SSL/TLS アプライアンス製品の
暗号設定方法等の調査報告書

2016 年 11 月

独立行政法人 情報処理推進機構
セキュリティセンター

目次

1. 背景・目的

独立行政法人情報処理機構（以下、「IPA」という。）では、暗号技術評価プロジェクト CRYPTREC(*1)の活動を通じ、オンラインショッピング、インターネットバンキング、ネットトレードなどのサービスで使用する SSL（Secure Socket Layer）/TLS（Transport Layer Security）プロトコルの適正な利用促進を目的として、SSL/TLS サーバの構築者や運営者が適切なセキュリティを考慮した暗号設定ができるようにするための SSL/TLS 暗号設定ガイドライン（以下「設定ガイドライン」という。）を公開(*2)した。

本調査では、一般に販売されている SSL/TLS を利用するアプライアンス製品（以下、SSL/TLS 製品という）を対象とし、SSL/TLS に関してどのような設定が可能であるか、及び設定ガイドラインにどの程度準拠した設定が可能であるかを明らかにする。調査の結果を公開することにより、製品レベルでの具体的な設定に基づく SSL/TLS プロトコルの適正な利用促進を図ることを目的としている。

*1: CRYPTREC ホームページ：http://www.cryptrec.go.jp/
*2:「SSL/TLS 暗号設定ガイドライン～安全なウェブサイトのために（暗号設定対策編）～」の公開：
https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

2. 業務内容

2.1. 業務内容概要

一般に販売されている SSL/TLS 製品（SSL/TLS を終端する SSL/TLS アクセラレータ製品、SSL/TLS ロードバランサ製品、WAF（Web Application Firewall）製品、セキュリティ統合製品等）について、以下の業務を行い、具体的な暗号設定状況の実情を明らかにする。

① デフォルトでの暗号設定内容の調査
② 暗号設定方法の調査
③ 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

2.2. 業務内容詳細

2.2.1. デフォルトでの暗号設定内容の調査

一般に販売されている SSL/TLS 製品について、実際に動作環境を構築し、初期状態での暗号設定内容を、以下の要件Ⅰ及び要件Ⅱに基づいて調査する。

要件Ⅰ：プロトコルバージョンごとに接続可否を調査する。

1. プロトコルバージョンとして SSL2.0、SSL3.0、TLS1.0、TLS1.1、TLS1.2 を対象とし、個々のプロトコルバージョンごとに接続可否を調査する。
2. プロトコルバージョンごとの接続可否の結果は一覧として記載する。

要件Ⅱ：暗号スイートごとに接続可否を調査する。

1. IANA が管理する TLS Cipher Suite Registry(本報告書では 2016.2.3 現在のものを使用)に記載のすべての暗号スイートを対象とし、個々の暗号スイートごとに接続可否を調査する。
2. 暗号スイートごとの接続可否の結果は一覧として記載する。
3. 鍵交換での種類ごとに暗号スイートを、RSA, DH, DHE, ECDH, ECDHE, KRB5, PSK, SRP, NULL の 9 つにグルーピングしてまとめる。
4. DH/DHE、ECDH/ECDHE が利用可能である場合は、利用する鍵長を調査する。
5. 設定ガイドラインに記載の接続可否の設定要求と、実際の接続可否の状態が異なる暗号スイートについて違いを明示する。

2.2.2. 暗号設定方法の調査

2.2.1.での要件Ⅰ及び要件Ⅱに記載の内容に関連して、どのような暗号設定が可能であるかを調査し、その設定方法を取りまとめる。

その際、プロトコルバージョンの接続可否についての設定方法、暗号スイートの接続可否についての設定方法、暗号スイートの優先順位についての設定方法を明確に区別したうえで、どのように設定するか（もしくは設定できないか）を調査する。また、暗号スイートの設定方法については、暗号アルゴリズム名を具体的に指定して、接続可否の設定や優先順位の設定が可能であるか否かも調査する。

DH/DHE、ECDH/ECDHE が利用可能である場合には、鍵長をどのように設定するか（もしくは設定できないか）についても調査する。

2.2.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

2.2.2.で調べた暗号設定方法のうち、暗号スイートの接続可否や優先順位に係わる暗号設定方法があるものについては、以下の手順及び 2.2.1.での要件Ⅰ及び要件Ⅱに基づいて、
設定ガイドラインでの設定要求にもっとも準拠していると思われる暗号設定内容になる暗号設定方法を調査し、実際の暗号設定内容と設定ガイドラインの設定要求との差分の分析を行う。

その際、設定ガイドラインに記載の高セキュリティ型、推奨セキュリティ型、セキュリティ例外型の３種類すべての設定要求について、各々調査・分析を行う。

なお、暗号スイートの接続可否や優先順位に係わる暗号設定方法がないものについては、デフォルトでの暗号設定内容について下記の手順②の分析のみを行う。

手順①　設定ガイドラインでの設定要求にもっとも準拠していると思われる暗号設定内容になる暗号設定方法を調査する。なお、この段階では、「暗号スイート名」を具体的にしているコマンドは利用しない。（個別の暗号スイート名ではなく、例えば、グループとして指定する方法を利用する。）

手順②　以下の点について、手順①で選択した暗号設定内容と設定ガイドラインでの設定要求との差分を分析する。

- プロトコルバージョンが設定ガイドラインでの設定要求に合っているか。
- 設定ガイドラインでは接続不可を要求しているが、手順①で選択した暗号設定内容では接続可能となっている暗号スイートが存在するか。
- DH/DHE、ECDH/ECDHE が利用可能である場合の鍵長が設定ガイドラインでの要求設定に合っているか。

手順③　暗号設定方法で「暗号スイート名」を具体的に指定するコマンドが利用できる場合には、それらのコマンドも含めた暗号設定方法による暗号設定内容を調査し、設定ガイドラインでの設定要求に完全準拠、または手順②よりも適切な暗号設定内容とすることが可能となるかを分析する。もし可能となる暗号設定内容があれば、その時の暗号設定方法と暗号設定内容を明らかにする。分析内容は手順②と同様である。

3. 調査対象製品

調査対象製品の一覧を　表 3-1　調査対象製品一覧　に示す。

表 3-1　調査対象製品一覧

項番	メーカー	機種名	ファームウェアバージョン	代理店	備考
1	Cisco	ASA 5512	9.5(2)5	シスコシステムズ	・ASA シリーズ
2	F5 ネットワークス	BIG-IP 3900	12.0.0	F5 ネットワークスジャパン	・BIG-IP シリーズ
3	A10 ネットワークス	3030S	-	A10 ネットワークス	・Thunder シリーズ ・ソフトウェアバージョン：2.7.2-P7-SP3
4	日本ラドウェア	Alteon VA	-	日本ラドウェア	・Alteon シリーズ ・ソフトウェア製品 (バージョン：30.2.1.100)
5	富士通	IPCOM EX2700 IN	E20L32 NF0201 B01	富士通	・IPCOM シリーズ
6	NEC	InterSecVM/LB V3.0 for VMWare	-	NEC	・InterSec シリーズ ・ソフトウェア製品(アップデートモジュール Rel 1.0)
7	Array Networks	APV2600	-	Array Networks	・APV シリーズ ・ソフトウェアバージョン : ArrayOS Rel.APV.8.6.0.14
8	日立製作所	Hitachi LoadBalaner EL130	-	日立製作所	・A10 ネットワークス Thunder 1030S の OEM 製品 ・ソフトウェアバージョン：2.7.1-P6
9	バラクーダネットワークス	Barracuda Load Balancer ADC モデル 340	6.0.0.005	バラクーダネットワークスジャパン	・ Load Balancer ADC シリーズ
10	バラクーダネットワークス	Barracuda WAF モデル 360	8.1.0.009	バラクーダネットワークスジャパン	・WAF シリーズ
11	Citrix	MPX8005c	NS11.0 Build 64.34.nc	マクニカネットワークス	・ NetScaler MPX シリーズ
12	セイコーソリューションズ	Netwiser SX-3850	7.3.20	セイコーソリューションズ	・Netwiser シリーズ
13	Cisco	WSA S370	8.8.0-085	シスコシステムズ	・WSA シリーズ
14	Imperva	SecureSphere X2010	11.0.0.30	マクニカネットワークス	・SecureSphere シリーズ

4. 調査環境

調査環境を 図 4-1 調査環境 に示す。図中の調査対象製品は 表 3-1 調査対象製品一覧 を参照のこと。

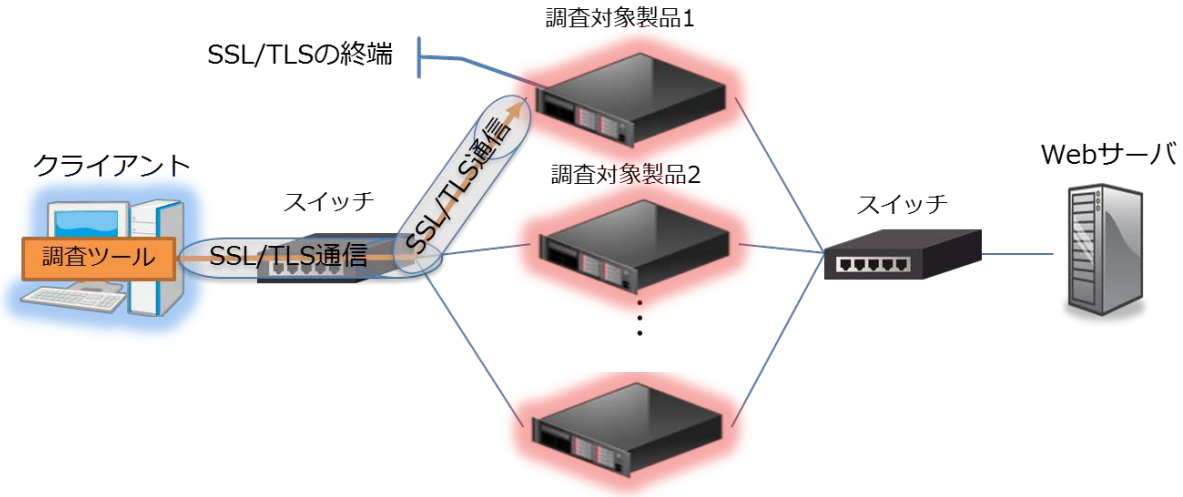

図 4-1 調査環境

※図中の「調査ツール」は NTT ソフトウェア株式会社所有の「TLS 暗号設定確認ツール」を使用している。

5. 調査結果概要

5.1. 調査結果一覧

本報告書では、調査を行った 14 製品のうち、SSL/TLS の設定方法が本調査で想定する調査条件と異なる 2 製品については解説から除外し、12 製品についての結果を解説する。

なお、調査時の証明書の設定については、次の 3 通りである。

- RSA 証明書と ECDSA 証明書の両方を同時に設定できる製品については両方を設定して調査。
- RSA 証明書と ECDSA 証明書のどちらか一方しか設定できない製品については、それぞれ 1 種を設定した状態で調査（結果も 2 種類記載）。
- RSA 証明書のみが設定できる製品については RSA 証明書を設定して調査。

デフォルト設定における「設定ガイドライン」の要求設定への準拠状況を表 5.1-1 に示す。通常、SSL/TLS アプライアンス製品のデフォルト設定は安全性よりも相互接続性を重視しており、調査結果から、表 5.1-1 のように、推奨セキュリティ型の要求設定項目に 11 製品が準拠していないこと[1]、また高セキュリティ型の要求設定項目に 12 製品すべてが準拠していないことが裏付けられた。

表 5.1-1　デフォルト設定での「設定ガイドライン」の要求設定への対応

項番	調査対象製品	高セキュリティ	推奨セキュリティ	セキュリティ例外
1	Cisco ASA シリーズ	*RSA 証明書及び ECDSA 証明書の両方を同時に設定時*		
		準拠していない	準拠していない	準拠していない
2	F5 ネットワークス BIG-IP シリーズ	*RSA 証明書及び ECDSA 証明書の両方を同時に設定時*		
		準拠していない	準拠していない	準拠していない
3	A10 ネットワークス Thunder シリーズ	*RSA 証明書設定時（※片方のみ設定可）*		
		準拠していない	準拠していない	準拠していない
		ECDSA 証明書設定時（※片方のみ設定可）		
		準拠していない	準拠している	準拠していない
4	日本ラドウェア Alteon シリーズ	*RSA 証明書及び ECDSA 証明書の両方を同時に設定時*		
		準拠していない	準拠していない	準拠していない
5	富士通 IPCOM シリーズ	*RSA 証明書設定時*		
		準拠していない	準拠していない	準拠していない
6	NEC InterSec シリーズ	*RSA 証明書設定時*		
		準拠していない	準拠していない	準拠していない
7	Array Networks APV シリーズ	*RSA 証明書設定時（※片方のみ設定可）*		
		準拠していない	準拠していない	準拠していない
		ECDSA 証明書設定時（※片方のみ設定可）		
		準拠していない	準拠していない	準拠していない
8	日立製作所 Hitachi Load Balancer EL130	*RSA 証明書設定時*		
		準拠していない	準拠していない	準拠していない

[1] A10 Thunder については、ECDSA 証明書を設定すれば、「設定ガイドライン」の推奨セキュリティに準拠できるため、準拠している製品としてカウントしている。

9	バラクーダネットワークス Barracuda Load Balancer ADC シリーズ	*RSA 証明書を設定時*		
		準拠していない	準拠していない	準拠していない
10	バラクーダネットワークス Barracuda WAF シリーズ	*RSA 証明書を設定時*		
		準拠していない	準拠していない	準拠していない
11	Citrix NetScaler MPX シリーズ	*RSA 証明書設定時*		
		準拠していない	準拠していない	準拠していない
12	セイコーソリューションズ Netwiser シリーズ	*RSA 証明書設定時*		
		準拠していない	準拠していない	準拠していない

一方で、設定ガイドラインにもっとも準拠していると思われる設定への変更後における「設定ガイドライン」の要求設定への準拠状況準拠状況を表 5.1-2 に示している。設定を変更することで、12 製品が推奨セキュリティ型に準拠できること、及び、9 製品が高セキュリティ型の要求設定項目に準拠できることがわかった。なお、セキュリティ例外型では、サポート外[2]の 1 製品を除いた 11 製品すべてで準拠可能となっている。

表 5.1-2 「設定ガイドライン」の要求設定への対応

項番	調査対象製品	高セキュリティ	推奨セキュリティ	セキュリティ例外
1	Cisco ASA シリーズ	*RSA 証明書及び ECDSA 証明書の両方を同時に設定時*		
		設定（準拠）できる	設定（準拠）できる	設定できない
2	F5 ネットワークス BIG-IP シリーズ	*RSA 証明書及び ECDSA 証明書の両方を同時に設定時*		
		EC 系のみに設定すれば準拠できる	設定（準拠）できる	設定（準拠）できる
3	A10 ネットワークス Thunder シリーズ	*RSA 証明書設定時（※片方のみ設定可）*		
		EC 系のみに設定すれば準拠できる	設定（準拠）できる	設定（準拠）できる
		ECDSA 証明書設定時（※片方のみ設定可）		
		設定できない	設定（準拠）できる	設定できない
4	日本ラドウェア Alteon シリーズ	*RSA 証明書及び ECDSA 証明書の両方を同時に設定時*		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
5	富士通 IPCOM シリーズ	*RSA 証明書設定時*		
		設定できない	設定（準拠）できる	設定（準拠）できる
6	NEC InterSec シリーズ	*RSA 証明書設定時*		
		設定できない	設定（準拠）できる	設定（準拠）できる
7	Array Networks APV シリーズ	*RSA 証明書設定時（※片方のみ設定可）*		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる

[2] SSL3.0 を設定できないため、そもそもセキュリティ例外型をサポートしていないと判断している。

		ECDSA 証明書設定時（※片方のみ設定可）		
		設定（準拠）できる	デフォルトで準拠できる	設定（準拠）できる
8	日立製作所 Hitachi Load Balancer EL130	*RSA 証明書設定時*		
		設定できない	設定（準拠）できる	設定（準拠）できる
9	バラクーダネットワークス Barracuda Load Balancer ADC シリーズ	*RSA 証明書及びECDSA 証明書の両方を同時に設定時*		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
10	バラクーダネットワークス Barracuda WAF シリーズ	*RSA 証明書及びECDSA 証明書の両方を同時に設定時*		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
11	Citrix NetScaler MPX シリーズ	*RSA 証明書設定時*		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる
12	セイコーソリューションズ Netwiser シリーズ	*RSA 証明書設定時*		
		設定（準拠）できる	設定（準拠）できる	設定（準拠）できる

※調査対象製品の具体的な機種名等は表 3-1　調査対象製品一覧表 3-1　調査対象製品一覧 参照。
※EC 系：楕円曲線暗号が含まれる暗号スイート。

6. 調査結果詳細

6章では、12 製品については個別の調査結果詳細を示す。

ここでは、6.x.1 章記載の表 6.x.1-1 暗号設定内容（デフォルト） の見方を以下に示す。

- CipherSuite 選択優先権

プロトコル	設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	7
tls1.1	OFF	–	0
tls1.0	ON	クライアント	5
sslv3	OFF	–	0
sslv2	設定不可	–	–

1

- XXXXXXX で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	ON	OFF	ON	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	----	ON	OFF	ON	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	----	ON	OFF	ON	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	----	ON	OFF	ON	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	----	ON	OFF	ON	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	----	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	----	ON	OFF	OFF	OFF	OFF

※XXXXXXXは機種名

2

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

3

図 6-1 暗号設定内容（デフォルト）の表記例

表 6-1 暗号設定内容（デフォルト）の表の見方

項番	項目	説明
1	CipherSuite 選択優先権	・「設定状況」欄：設定されていれば「ON」、設定されていなければ「OFF」、設定不可であれば「設定不可」。 ・「CipherSuite 選択優先権」欄：暗号スイートの優先権がサーバにあるかクライアントにあるか。 「サーバ」：サーバ優先。 「クライアント」：クライアント優先。 「-」：当該プロトコルが使用できない場合。 ・「CipherSuite 数」欄：該当する暗号スイートの数（reserved または unassigned の暗号スイートで、有効な数を含む）。
2	使用可能な暗号スイート ※Appendix2 の表も同様	・IANA で規定されている全ての暗号スイートに対してプロトコル毎に「ON」(使用可能)「OFF」(使用不可)を示す。項番 1 の CipherSuite 選択優先権がサーバ優先で、且つ「ON」であった場合、「ON」の隣に暗号スイートの優先順位を示す（例：「ON：1」）。 ・「高」「推」「例」欄：それぞれ設定ガイドラインの「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」のいずれのグループに属するかを示す。いずれにも属さない場合は空欄。 「α」「β」「A」～「H」：設定ガイドラインの要求設定のグループを示す。 「α追加」「β追加」「A 追加」～「F追加」：設定ガイドラインの各グループへの追加または代替を示す。 ・「鍵交換パラメータ」欄：鍵交換の暗号が DH/DHE、ECDH/ECDHE 且つ「ON」であった場合は、複数の鍵長の設定値から通信時のネゴシエーションによって選択された DH/DHE の鍵長、または、ECDH/ECDHE の namedcurve の名前のうち、一つを例示している。該当しない場合は「---」。 ・二重線は鍵交換の種類(DH, DHE, ECDH, ECDHE, KRB5, NULL, PSK, RSA, SRP)の区切りを示す。
3	Extension	・サーバの Extension（拡張機能）の情報をプロトコル毎に「対応」、「非対応」または「-」で示す。 「-」の場合はプロトコルで拡張機能自体がない場合を示す。 「signature_algorithms」：クライアントの使用可能な署名アルゴリズムを受入可否。「対応」の場合で、クライアントが安全性の低い署名アルゴリズムしか受け入れられない場合は、TLS/SSL 通信で使用される暗号がダウングレードする可能性がある。 「heartbeat」：サーバ側での Heartbeat（死活監視）機能が有効か否か。Heartbeat 機能が有効な場合、HeartBleed 攻撃を受ける可能性がある。

※項番は図 6-1 中の番号。

6.1. Cisco ASA シリーズ

本章では、ASA 5512 について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能である。RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なり、両方の証明書を設定した場合は、両方の暗号スイートが有効になる。**6.1.1 デフォルトでの暗号設定内容の調査**、および、**6.1.3 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**は、RSA 証明書と ECDSA 証明書の両方を設定した場合について記載する。

6.1.1. デフォルトでの暗号設定内容の調査

表 6.1.1-1　暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	21
tls1.1	ON	サーバ	5
tls1.0	ON	サーバ	5
sslv3	設定不可	ー	ー
sslv2	設定不可	ー	ー

- Cisco ASA 5512 で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON:19	ON:3	ON:3	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON:17	ON:1	ON:1	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON:15	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON:7	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON:11	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON:3	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:13	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:5	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:14	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:6	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:9	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:1	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:10	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:2	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	----	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	----	ON:21	ON:5	ON:5	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	----	ON:20	ON:4	ON:4	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	----	ON:18	ON:2	ON:2	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	----	ON:16	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	----	ON:8	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	----	ON:12	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	----	ON:4	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	―	―	―	―
heartbeat	15	対応	対応	対応	―	―

6.1.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ASDM という接続用設定ツールで設定画面にログインし、（1）Configuration－（2）Device Management－（3）Advanced－（4）SSL settings をクリックして、（5）SSL settings 画面を表示する。

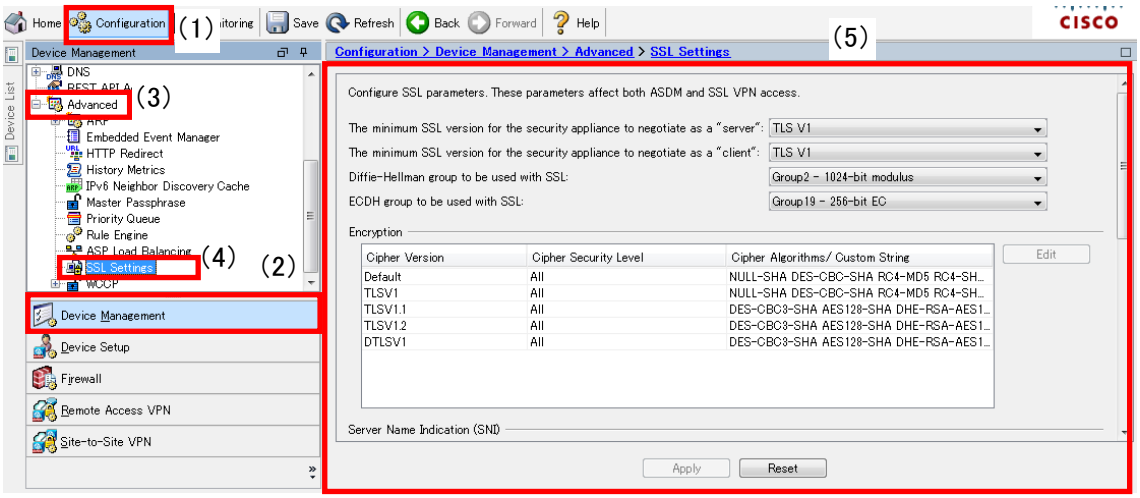

図 6.1.2-1 SSL Settings 画面-1

B) （6）「The minimum SSL version for the security appliance to negotiate as a “server”」の（7）プルダウンメニューから、有効にしたいバージョン以上のプロトコルを選択する。
※選択したプロトコル未満のバージョンは使用されない。
※SSLv2 と SSLv3 は使用不可。

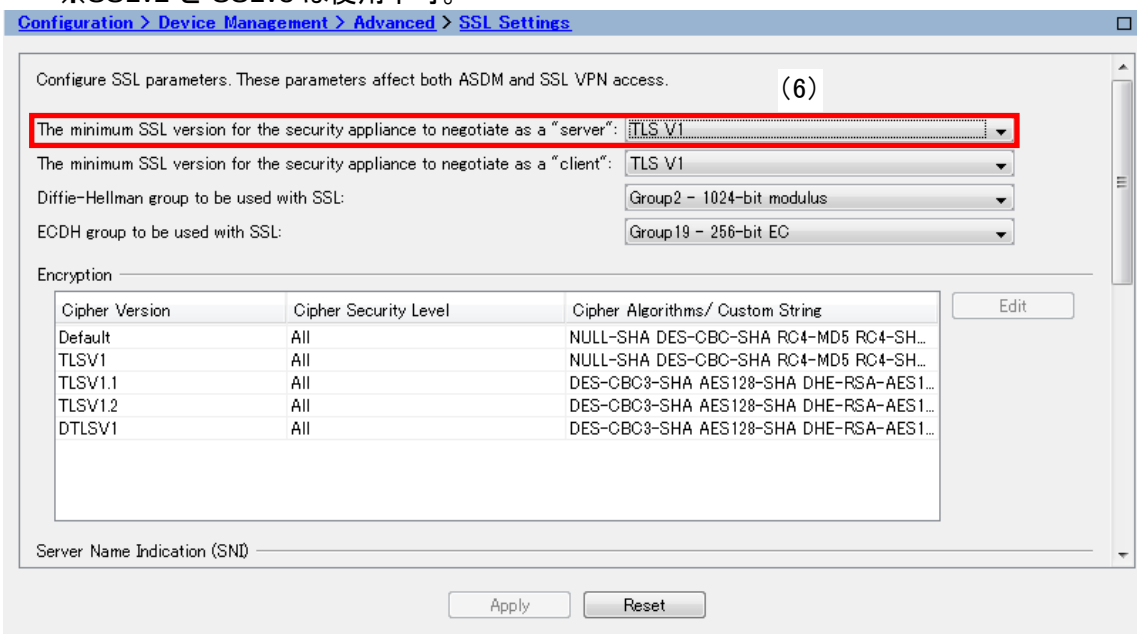

図 6.1.2-2 SSL Settings 画面（プロトコル）-1

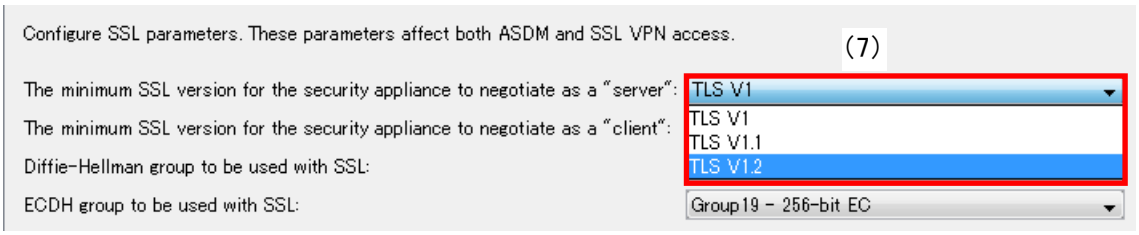

図 6.1.2-3　SSL Settings 画面-2

C)　設定が完了したら（8）「Apply」ボタンを押下して変更を適用する。

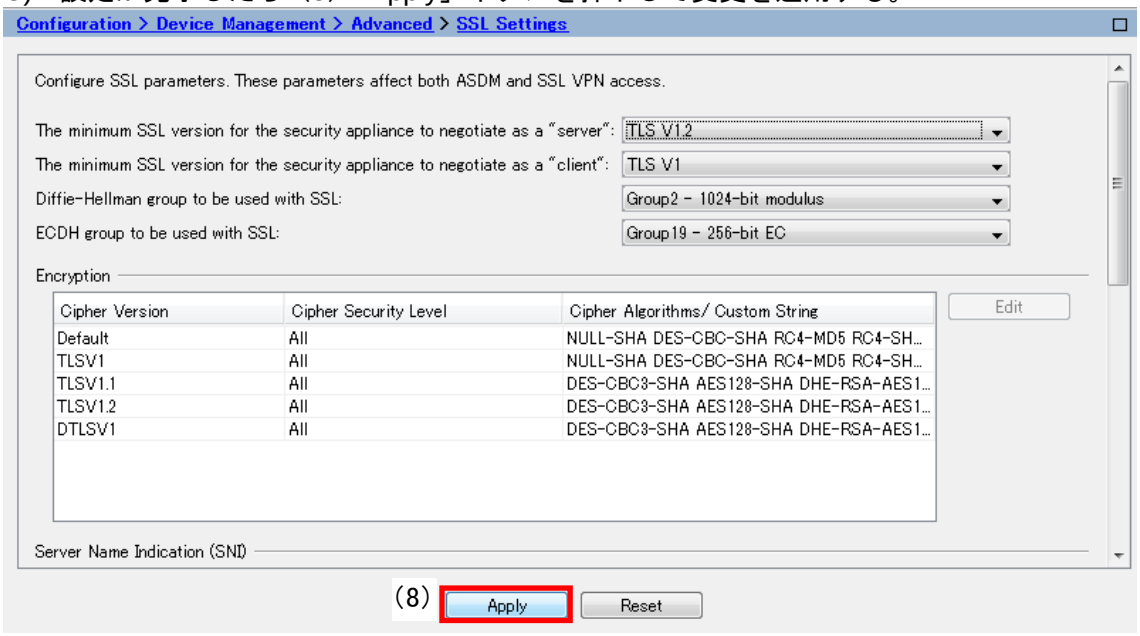

図 6.1.2-4　SSL Settings 画面（プロトコル）-2

D)　設定が完了したら画面上の（9）「Save」ボタンを押下して設定を保存する。

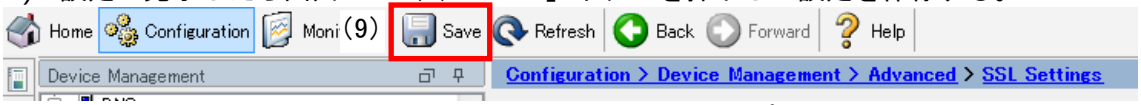

図 6.1.2-5　SSL Settings 画面（プロトコル）-3

II.　暗号スイートの設定

A)　6.1.2.I.A で表示した「SSL Settings」画面の（1）「Encryption」で（2）設定したい「Cipher Version」を選択し、（3）「Edit」ボタンを押下する。

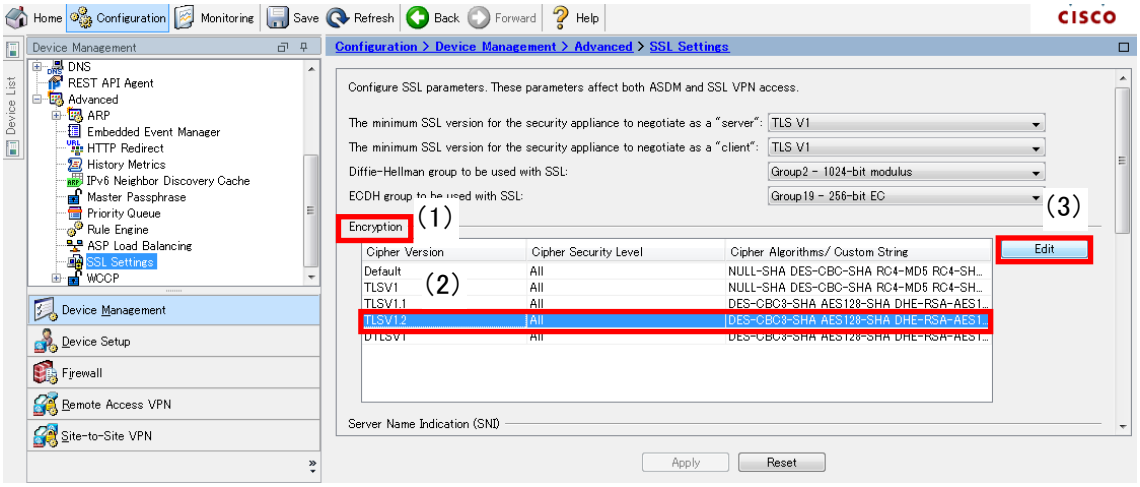

図 6.1.2-6　SSL Settings 画面（暗号スイート）-1

B)　（4）「Configure Cipher Algorithms/Custom String」画面が表示されるので、（5）「SSL cipher security level」の（6）プルダウンメニューから「Custom」を選択する。

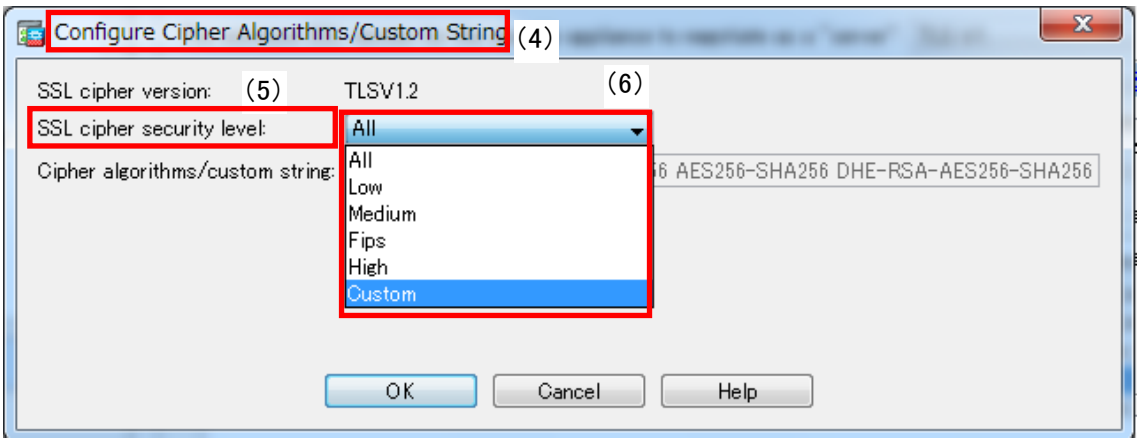

図 6.1.2-7　SSL Settings 画面（暗号スイート）-2

C)　（7）「Cipher algorithms/custom string」欄に使用したい暗号スイート順に入力したら（8）「OK」ボタンを押下する。

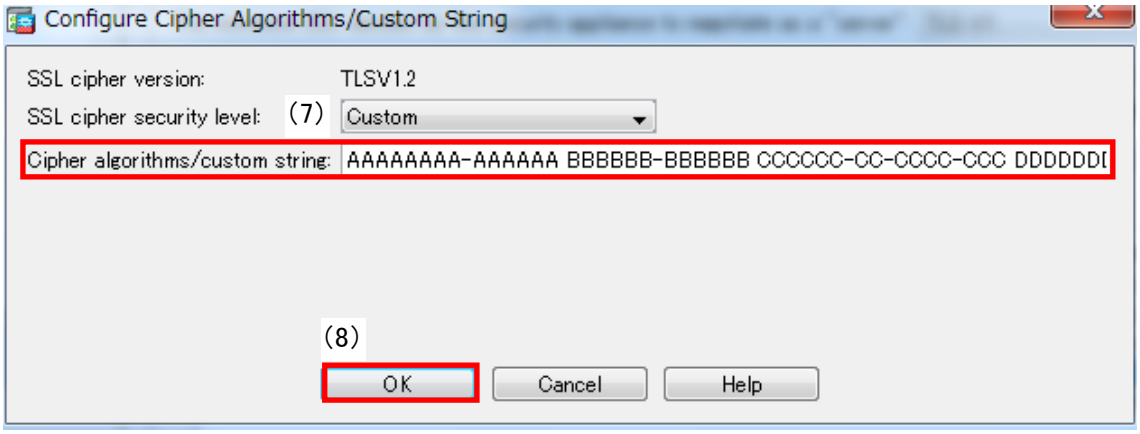

図 6.1.2-8　SSL Settings 画面（暗号スイート）-3

D)　設定が完了したら（9）「Apply」ボタンを押下して変更を適用する。

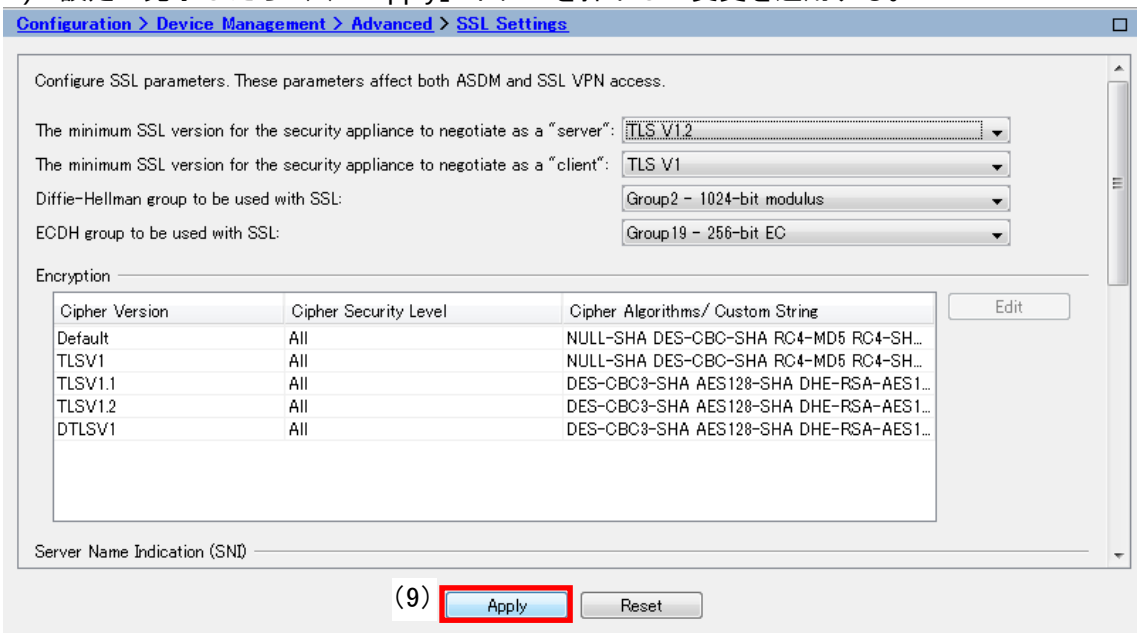

図 6.1.2-9　SSL Settings 画面（暗号スイート）-4

E)　設定が完了したら画面上の（10）「Save」ボタンを押下して設定を保存する。

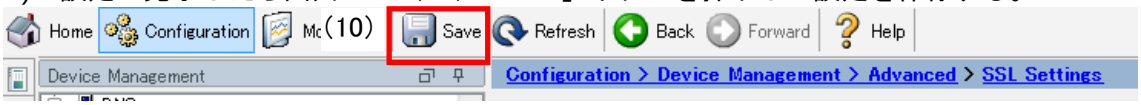

図 6.1.2-10　SSL Settings 画面（暗号スイート）-5

III.　DH/DHE、ECDH/ECDHE の鍵長の設定

DH/DHE、ECDH/ECDHE の鍵長の設定は 6.1.2.I.A 図 6.1.2-1　SSL Settings 画面-1 にて設定可能である。

（11）「Diffie-Hellman group to be used with SSL」では DH/DHE の鍵長が設定可能であり、（12）「ECDH group to be used with SSL」では ECDH/ECDHE の鍵長が設定可能である（設定箇所は図 6.1.2-11　SSL Settings 画面（暗号スイート）-6 参照）。

設定可能な鍵長は以下の通り。

Diffie-Hellman group to be used with SSL：

「Group1 - 768-bit modules」

「Group2 - 1024-bit modules」（デフォルト）

「Group5 - 1536-bit modules」

「Group14 - 2048-bit modules, 224-bit prime order」

「Group24 - 2048-bit modules, 256-bit prime order」

ECDH group to be used with SSL：

「Group19 - 256-bit EC」（デフォルト）

「Group20 - 384-bit EC」

「Group21 - 521-bit EC」

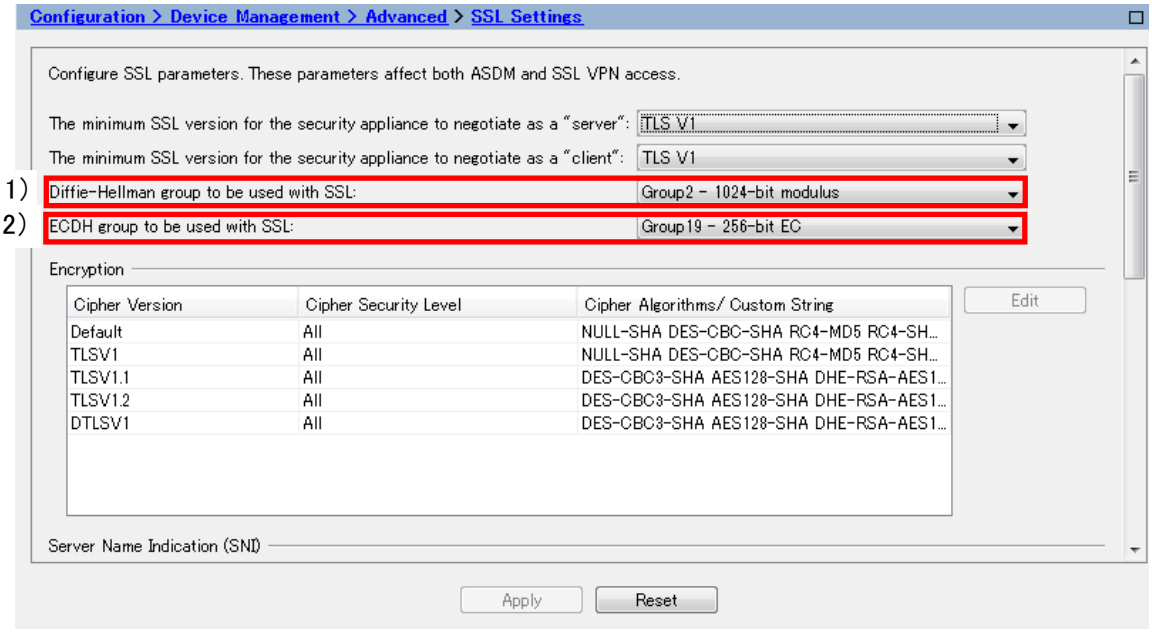

図 6.1.2-11　SSL Settings 画面（暗号スイート）-6

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
6.1.2.II.B、C と同様、「SSL cipher security level」のプルダウンメニューから「Custom」を選択し、「Cipher algorithms/custom string」欄に優先順位の順に暗号スイートを入力する。

VI. Extension の設定
設定方法なし。

※証明書について
証明書は RSA 証明書と ECDSA 証明書がインポート可能である。
また、ECDSA 証明書のみを設定する場合は、設定した ECDSA 証明書とあわせて、機器にプリインストールされている RSA 証明書も有効となる。

6.1.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.1.3.1. 高セキュリティ型

①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
図 6.1.2-3　SSL Settings 画面-2 の「minimum SSL version for the security appliance to negotiate as a “server”」で TLS V1.2 を選択する。

II. 暗号スイート
6.1.2.II.A で TLSV1.2 を選択して、6.1.2.II.C の「Cipher algorithms/custom string」欄に、以下の文字列を設定する。
AESGCM!kRSA

III. DH/DHE、ECDH/ECDHE の鍵長
6.1.2.III.の「Diffie-Hellman group to be used with SSL」で、「Group14 - 2048-bit modules, 224-bit

prime order」を選択し、「ECDH group to be used with SSL」で、「Group19 – 256bit EC」を選択する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

② ①の設定とガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.1.3.1-1 設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型(一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.1.3.1-1 設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追)	2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追)	3	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追)	6	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に指定する方法）

I. プロトコルバージョン
図 6.1.2-3 SSL Settings 画面-2 の「minimum SSL version for the security appliance to negotiate as a “server”」で TLS V1.2 を選択する。

II. 暗号スイート
プロトコルバージョンごとに、図 6.1.2-8 SSL Settings 画面（暗号スイート）-3 の「Cipher algorithms/custom string」欄に、以下の文字列を設定する。暗号スイートの間には半角スペースを挿入する。

DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-S

HA256

III. DH/DHE、ECDH/ECDHE の鍵長
図 6.1.2-11　SSL Settings 画面（暗号スイート）-6 の「Diffie-Hellman group to be used with SSL」で、「Group14 - 2048-bit modules, 224-bit prime order」を選択し、「ECDH group to be used with SSL」で、「Group19 – 256bit EC」を選択する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定とガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.1.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定） の「設定ガイドラインの高セキュリティ型(一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.1.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追)	2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追)	3	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	4	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.1.3.2. 推奨セキュリティ型

①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

①　プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
図 6.1.2-3　SSL Settings 画面-2 の「minimum SSL version for the security appliance to

negotiate as a “server”」で、TLS V1 を設定する。

II. 暗号スイート
6.1.2.II.C の「Cipher algorithms/custom string」欄に、以下の文字列を設定する。

- TLS V1.2
  DH+AES128 ECDH+AES128 RSA+AES128 DH+AES256 ECDH+AES256 RSA+AES256
- TLS V1.1
  ALL !3DES
- TLS V1
  ALL !3DES !RC4 !DES !NULL

III. DH/DHE 、ECDH/ECDHE の鍵長
6.1.2.III 図 6.1.2-11　SSL Settings 画面（暗号スイート）-6 の「Diffie-Hellman group to be used with SSL」で、「Group2 - 1024-bit modulus」を選択し、「ECDH group to be used with SSL」で、「Group19 – 256bit EC」を選択する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.1.3.2-1 設定ガイドラインとの差分（推奨セキュリティ型） の設定ガイドラインの推奨セキュリティ型（一部）にある 20 個の暗号スイートの使用が可能である。使用可能な 20 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティ型の順位と同じである。

表 6.1.3.2-1 設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）	3	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）	2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）	1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）	7	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	10	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	9	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	8	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）	13	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）	12	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）	11	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）	17	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	16	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）	15	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	14	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	20	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	19	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	18	TLS_RSA_WITH_AES_256_GCM_SHA384（E）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE 、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に指定する方法）

I. プロトコルバージョン
図 6.1.2-3 SSL Settings 画面-2 の「minimum SSL version for the security appliance to negotiate as a “server”」で、TLS V1 を設定する。

II. 暗号スイート
プロトコルバージョンごとに、「Cipher algorithms/custom string」欄に、優先度上位の暗号スイートから順に設定する（図 6.1.2-8　SSL Settings 画面（暗号スイート）-3 参照）。暗号スイートの間には半角スペースを挿入する。

- TLS V1.2
  DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES128-GCM-SHA256 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 AES256-SHA AES256-SHA256 AES256-GCM-SHA384
- TLS V1.2
  DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA256 DHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 AES128-SHA AES128-SHA256 AES128-GCM-SHA256 DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA256 DHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 AES256-SHA AES256-SHA256 AES256-GCM-SHA384
- TLS V1.1、TLS V1
  DHE-RSA-AES128-SHA AES128-SHA DHE-RSA-AES256-SHA AES256-SHA

III. DH/DHE 、ECDH/ECDHE の鍵長
図 6.1.2-11　SSL Settings 画面（暗号スイート）-6 の「Diffie-Hellman group to be used with SSL」で、「Group2 - 1024-bit modulus」を選択し、「ECDH group to be used with SSL」で、「Group19 – 256bit EC」を選択する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.1.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型、個別指定） の設定ガイドラインの推奨セキュリティ型（一部）にある 20 個の暗号スイートの使用が可能である。使用可能な 20 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティ型の順位と同じである。

表 6.1.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）	1	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）	2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	5	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）	6	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	7	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	8	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	9	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	10	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）	11	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）	12	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）	13	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）	14	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	15	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）	26	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	17	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	18	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	19	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	20	TLS_RSA_WITH_AES_256_GCM_SHA384（E）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.1.3.3. セキュリティ例外型

SSLv3 を有効にできないため、セキュリティ例外型は設定できない。

6.2. F5 ネットワークス BIG-IP シリーズ

本章では、BIG-IP3900 について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能である。RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なり、両方の証明書を設定した場合は、両方の暗号スイートが有効になる。6.2.1 **デフォルトでの暗号設定内容の調査**、および、6.2.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**は、RSA 証明書と ECDSA 証明書の両方を設定した場合について記載する。

6.2.1. デフォルトでの暗号設定内容の調査

表 6.2.1-1　暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	21
tls1.1	ON	サーバ	9
tls1.0	ON	サーバ	9
sslv3	OFF	ー	0
sslv2	設定不可	ー	ー

- BIG-IP3900 で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	1024bit	ON:7	ON:3	ON:3	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON:6	ON:2	ON:2	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON:4	ON:1	ON:1	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON:5	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON:3	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON:2	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON:1	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON:21	ON:9	ON:9	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:20	ON:8	ON:8	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:18	ON:7	ON:7	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:19	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:17	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:16	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:15	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:14	ON:6	ON:6	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:13	ON:5	ON:5	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:11	ON:4	ON:4	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:12	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:10	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:9	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:8	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.2.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで BIG-IP Configuration Utility にログインし、(1) Local Traffic－(2) Profiles－(3) SSL－(4) Client をクリックしてプロファイル一覧を表示し、(5) 現在有効な Profile を選択する。

※プロファイルでは、仮想サーバでトラフィックをどのように処理するかを定義する。仮想サーバアドレス・ポート、あらかじめ用意されている HTTP・SSL 等のプロファイル、SNAT 等を指定する。

※例えば SSL プロファイルではあらかじめ用意されているクライアントプロファイル(clientssl)かサーバプロファイル(serverssl)を選択する。詳細を変更したい場合はクライアント／サーバプロファイルをベースにカスタマイズする。

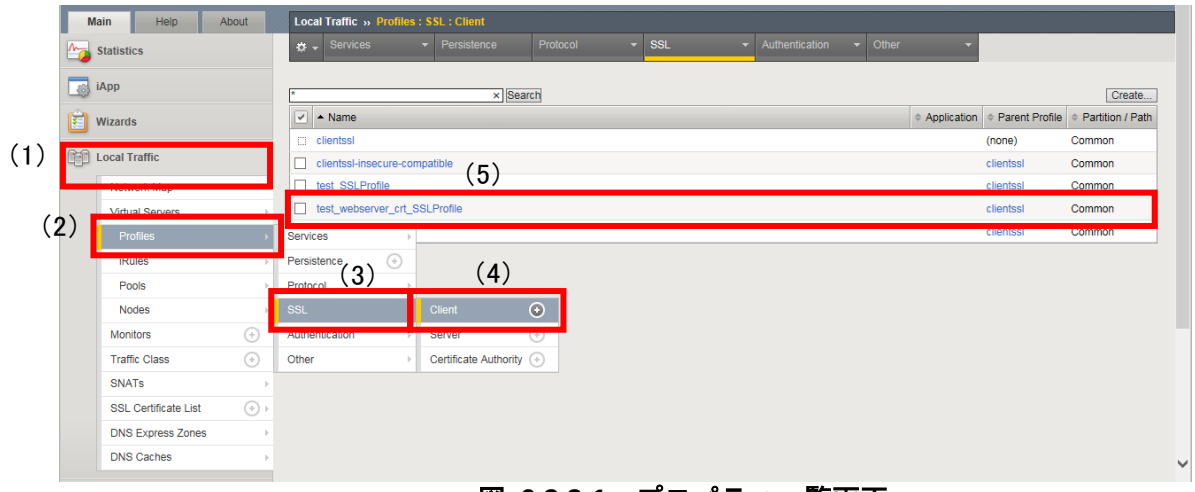

図 6.2.2-1 プロパティー覧画面

B)　プロパティ編集画面の Option 欄で、(6) 編集を有効にするチェックボックスを選択し、Available Options 欄の一覧から No SSLv2、No SSLv3、No TLSv1 を選択して、(8) Enable ボタンを使用して（7）Enabled Options 欄へ追加して有効にする。無効にする場合は（9）Disable ボタンで Enable Options 欄から削除する。

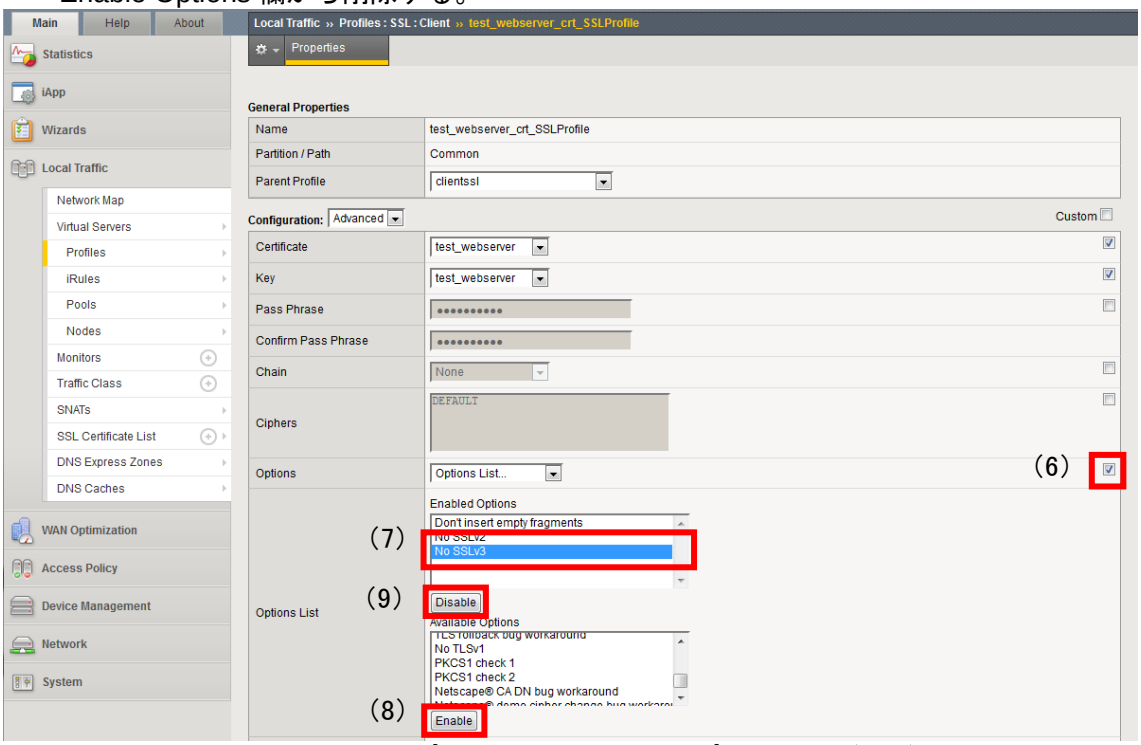

図 6.2.2-2　プロパティ編集画面（プロトコルバージョン）

II.　暗号スイートの設定

A)　プロパティ編集画面の Ciphers 欄に、OpenSSL 表記で暗号スイートを指定する。

注）OpenSSL 表記とは、OpenSSL の ciphers コマンドの表記にしたがい、指定された文字列と指定された記号を用いる。

例：ALL:!MD5

参考：https://www.openssl.org/docs/man1.0.2/apps/ciphers.html

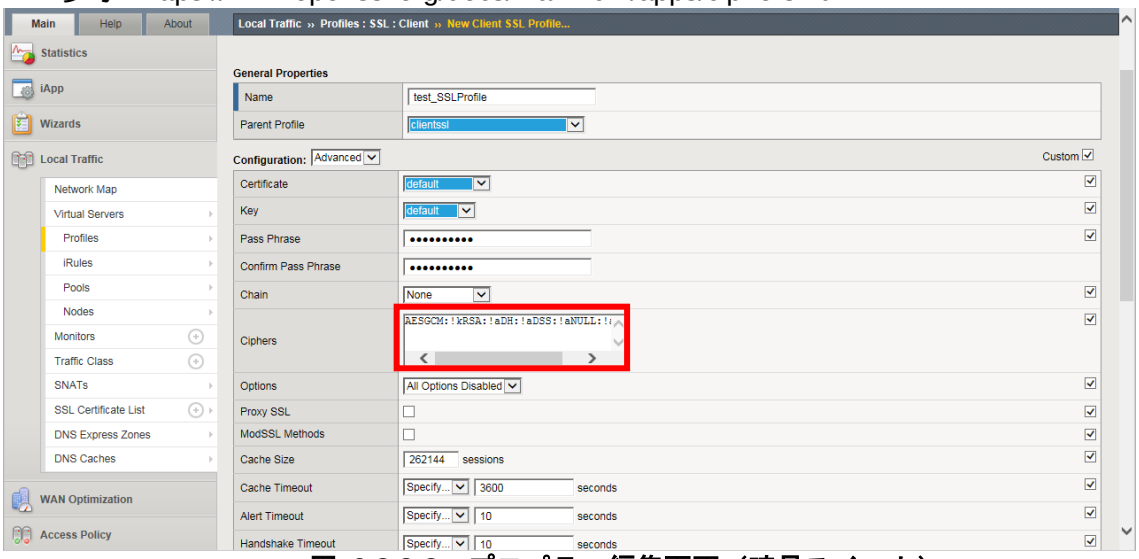

図 6.2.2-3　プロパティ編集画面（暗号スイート）

III. DH/DHE、ECDH/ECDHE の鍵長の設定
設定方法なし。
DHE の鍵長は、既定で 1024bit である。
ECDHE の鍵長は、既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II 暗号スイートの設定で設定した結果による。

VI. Extension の設定
設定方法なし。

6.2.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.2.3.1. 高セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。ただし、EC 系（楕円曲線暗号が含まれる暗号スイート）のみに設定した場合に限る。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
図 6.2.2-2 プロパティ編集画面（プロトコルバージョン）で、No SSLv2、No SSLv3、No TLSv1、No TLSv1.1 を有効にする。

II. 暗号スイート
図 6.2.2-3 プロパティ編集画面（暗号スイート）の Ciphers 欄に、以下の文字列を設定する。
AES-GCM:!ADH:!RSA

III. DH/DHE、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は既定で 1024bit である。
ECDHE の鍵長は既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分あり。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.2.3.1-1 設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型（一部）」にある 6 個の暗号

スイートの使用が可能である。
ただし、ECDH が除外できないため、高セキュリティ型に含まれない 2 個の暗号スイートが含まれる。使用可能な 6 個の暗号スイートと「設定ガイドラインの高セキュリティ型（一部）」の優先順位の違いは、表 6.2.3.1-1　設定ガイドラインとの差分（高セキュリティ型）のとおりである。

表 6.2.3.1-1　設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）設定	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）	8	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α 追加）	4	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α 追加）	3	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α 追加）
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）	2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β 追加）	1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β 追加）	7	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β 追加）
－	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	6	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
		5	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384

※設定ガイドラインの高セキュリティ（一部）設定の同優先順位内の優先順位は順不同
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
DHE の鍵長が 1024bit である。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
図 6.2.2-2　プロパティ編集画面（プロトコルバージョン）で、No SSLv2、No SSLv3、No TLSv1、No TLSv1.1 を有効にする。

II. 暗号スイート
図 6.2.2-3　プロパティ編集画面（暗号スイート） の Ciphers 欄に、以下の文字列を設定する。
DHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-GCM-SHA384:
ECDHE-ECDSA-AES256-GCM-SHA384: DHE-RSA-AES128-GCM-SHA256:
ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256

III. DH/DHE、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は既定で 1024bit である。
ECDHE の鍵長は既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち､表 6.2.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定） の「設定ガイドラインの高セキュリティ型（一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.2.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定）

グループ	設定ガイドラインの高セキュリティ型（一部）設定	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α追加）	3	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α追加）
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）	4	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）	5	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β追加）	6	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β追加）

※設定ガイドラインの高セキュリティ（一部）設定の同優先順位内の優先順位は順不同
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分あり。
DHE の鍵長が 1024bit である。

6.2.3.2. 推奨セキュリティ型

①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
図 6.2.2-2　プロパティ編集画面（プロトコルバージョン） で、No SSLv2、No SSLv3 を有効にする。

II. 暗号スイート
図 6.2.2-3　プロパティ編集画面（暗号スイート） の Ciphers 欄に、以下の文字列を設定する。
SHA256:SHA:SHA384:!ADH:!3DES:!RC4:!DES

III. DH/DHE、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は 1024bit である。
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.2.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）　の「設定ガイドラインの推奨セキュリティ型（一部）」にある 34 個の暗号スイートの使用が可能である。使用可能な 34 個の暗号スイートと設定ガイドラインの推奨セキュリティ型（一部）の優先順位の違いは、表 6.2.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）　のとおりである。

表 6.2.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）設定	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）	20	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA（A）	25	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）	8	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）	7	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）	19	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	18	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）	6	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	5	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）	4	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	3	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	22	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	12	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）	26	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	11	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
C	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA（C 追加）	21	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA（C 追加）
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256（C 追加）	10	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256（C 追加）
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256（C 追加）	9	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256（C 追加）
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）	15	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）	1	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA（D）	23	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）	31	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）	14	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	13	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）	30	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	29	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）	28	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	27	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	17	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	2	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	24	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	34	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
F	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）	16	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）	33	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）	32	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）

※設定ガイドラインの推奨セキュリティ（一部）設定の同優先順位内の優先順位は順不同
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
図 6.2.2-2 プロパティ編集画面（プロトコルバージョン） で、No SSLv2、No SSLv3 を有効にする。

II. 暗号スイート
図 6.2.2-3 プロパティ編集画面（暗号スイート） の Ciphers 欄に、以下の文字列を設定する。
DHE-RSA-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-CBC-SHA:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA:AES128-SHA256:CAMELLIA128-SHA:AES128-GCM-SHA256:ECDH-ECDSA-AES128-SHA:ECDH-ECDSA-AES128-SHA256:ECDH-ECDSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA256-SHA:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-CBC-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA:AES256-SHA256:CAMELLIA256-SHA:AES256-GCM-SHA384:ECDH-ECDSA-AES256-SHA:ECDH-ECDSA-AES256-SHA384:ECDH-ECDSA-AES256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は既定で 1024bit である。
ECDHE の鍵長は既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち､表 6.2.3.2-2 設定ガイドラインとの差分（推奨セキュリティ型、個別指定） の「設定ガイドラインの推奨セキュリティ型（一部）」にある 34 個の暗号スイートの使用が可能である。使用可能な 34 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティ型の順位と同じである。

表 6.2.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）設定	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	1	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	2	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	3	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	4	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)	7	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)	9	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	10	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	11	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	12	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	13	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	14	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
C	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)	15	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)	16	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)	17	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	18	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	19	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	20	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	21	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)	22	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	23	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)	24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)	25	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)	26	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	27	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	28	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	29	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	30	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	31	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
F	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (F 追加)	32	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (F 追加)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (F 追加)	33	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (F 追加)
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (F 追加)	34	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (F 追加)

※設定ガイドラインの推奨セキュリティ（一部）設定の同優先順位内の優先順位は順不同
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.2.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
図 6.2.2-2　プロパティ編集画面（プロトコルバージョン） で、No SSLv2 を有効にする。

II. 暗号スイート
図 6.2.2-3　プロパティ編集画面（暗号スイート） の Ciphers 欄に、以下の文字列を設定する。
SHA256:SHA:SHA384:!ADH:!DES:!EXPORT:+RC4:+3DES

III. DH/DHE、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は既定で 1024bit である。
ECDHE の鍵長は既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分あり。
セキュリティ例外型に含まれる暗号スイート 67 個のうち､表 6.2.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）　の「設定ガイドラインのセキュリティ例外型（一部）」にある 37 個の暗号スイートの使用が可能である。
ただし、セキュリティ例外型に含まれない 3 個の暗号スイートが含まれる。使用可能な 37 個の暗号スイートと「設定ガイドラインのセキュリティ例外型（一部）」の優先順位の違いは、表 6.2.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）　のとおりである。

表 6.2.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）設定	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	39	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	37	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	36	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	20	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)	25	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)	7	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	19	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)	18	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	5	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	4	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	3	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	22	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
C	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)	12	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)	26	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)	11	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	21	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	10	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	9	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	15	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	23	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)	31	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)

グループ	設定ガイドラインのセキュリティ例外型（一部）設定	優先順位	暗号スイート設定結果
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）	13	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	29	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	28	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	27	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	17	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
F	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）	2	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）	24	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）	34	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）
G	TLS_RSA_WITH_RC4_128_SHA（G）	16	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	33	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA（H）	32	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA（H）
－	設定ガイドラインのセキュリティ例外型に該当しない暗号スイート	35	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
		40	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
		38	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

※設定ガイドラインのセキュリティ例外型（一部）設定の同優先順位内の優先順位は順不同
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
図 6.2.2-2　プロパティ編集画面（プロトコルバージョン）で、No SSLv2 を有効にする。

II. 暗号スイート
図 6.2.2-3　プロパティ編集画面（暗号スイート）の Ciphers 欄に、以下の文字列を設定する。
DHE-RSA-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-CBC-SHA:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA:AES128-SHA256:CAMELLIA128-SHA:AES128-GCM-SHA256:ECDH-ECDSA-AES128-SHA:ECDH-ECDSA-AES128-SHA256:ECDH-ECDSA-AES128-GCM-SHA256:DHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-CAMELLIA256-SHA:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-CBC-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA:AES256-SHA256:CAMELLIA256-SHA:AES256-GCM-SHA384:ECDH-ECDSA-AES256-SHA:ECDH-ECDSA-AES256-SHA384:ECDH-ECDSA-AES256-GCM-SHA384
※文字列制限（768 文字）のため、残りの
:RC4-SHA:ECDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA
が設定できない。

III. DH/DHE、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は既定で 1024bit である。
ECDHE の鍵長は既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定

II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち､表 6.2.3.3-2　設定ガイドラインとの差分（セキュリティ例外型、個別指定） の「設定ガイドラインのセキュリティ例外型（一部)」にある 34 個の暗号スイートの使用が可能である。
ただし、使用可能な 34 個の暗号スイートの優先順位は、設定ガイドラインのセキュリティ例外型の順位と同じである。

表 6.2.3.3-2　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	1	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	2	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	3	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	4	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)	7	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)	9	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	10	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	11	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	12	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	13	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	14	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
C	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)	15	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)	16	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)	17	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	18	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	19	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	20	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	21	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)	22	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	23	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)	24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)	25	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)	26	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	27	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	28	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	29	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	30	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	31	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
F	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (F 追加)	32	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (F 追加)
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (F 追加)	33	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (F 追加)

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）	34	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）
G	TLS_RSA_WITH_RC4_128_SHA（G）		
H	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA（H） TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）		

※設定ガイドラインのセキュリティ例外型（一部）設定の同優先順位内の優先順位は順不同
※括弧内は設定ガイドラインのグループ名。
※グループ G、H の 3 つの暗号スイートが機能的には使用可能だが、文字列制限（768 文字）のため「暗号スイート設定結果」欄記載の 34 個分の暗号スイートしか設定できない。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.3. A10 ネットワークス Thunder シリーズ

本章では、Thunder 3030S について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能である。RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なり、両方の証明書を設定した場合は、両方の暗号スイートが有効になる。RSA 証明書と ECDSA 証明書の両方を設定することができないため、6.3.1 **デフォルトでの暗号設定内容の調査**、および、6.3.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、 (1) RSA 証明書設定時、(2) ECDSA 証明書設定時に分けて記載する。

6.3.1. デフォルトでの暗号設定内容の調査

(1) RSA 証明書設定時

表 6.3.1-1　暗号設定内容（デフォルト、RSA 証明書設定時）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	20
tls1.1	ON	クライアント	9
tls1.0	ON	クライアント	10
sslv3	ON	クライアント	8
sslv2	設定不可	ー	ー

- A10 ネットワークス Thunder 3030S で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON	ON	ON	ON	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON	ON	ON	ON	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON	ON	ON	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON	ON	ON	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β 追加	A 追加	A 追加	secp256r1	ON	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α 追加	D 追加	D 追加	secp256r1	ON	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON	ON	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	ON	ON	ON	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	ON	ON	ON	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	ON	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	ON	ON	ON	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON	OFF	OFF	OFF	OFF

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

(2) ESDSA 証明書設定時

表 6.3.1-2　暗号設定内容（デフォルト、ECDSA 証明書設定時）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	5
tls1.1	ON	クライアント	4
tls1.0	ON	クライアント	4
sslv3	OFF	ー	0
sslv2	設定不可	ー	ー

- A10 ネットワークス Thunder 3030S で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON	ON	ON	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON	ON	ON	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β 追加	A 追加	A 追加	secp256r1	ON	ON	ON	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α 追加	D 追加	D 追加	secp256r1	ON	ON	ON	OFF	OFF

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.3.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで管理画面にログインし、(1) コンフィグ－ (2) SLB－ (3) テンプレート－ (4) SSL－ (5) 作成してあるクライアント SSL テンプレート（例：test_ws_ssl）をクリックする。

図 6.3.2-1 クライアント SSL リスト画面

B) SSLv3 を無効にする場合は、クライアント SSL 内の (6)「SSLv3 のクライアントを拒否する」の (7) 有効にチェックを入れる。

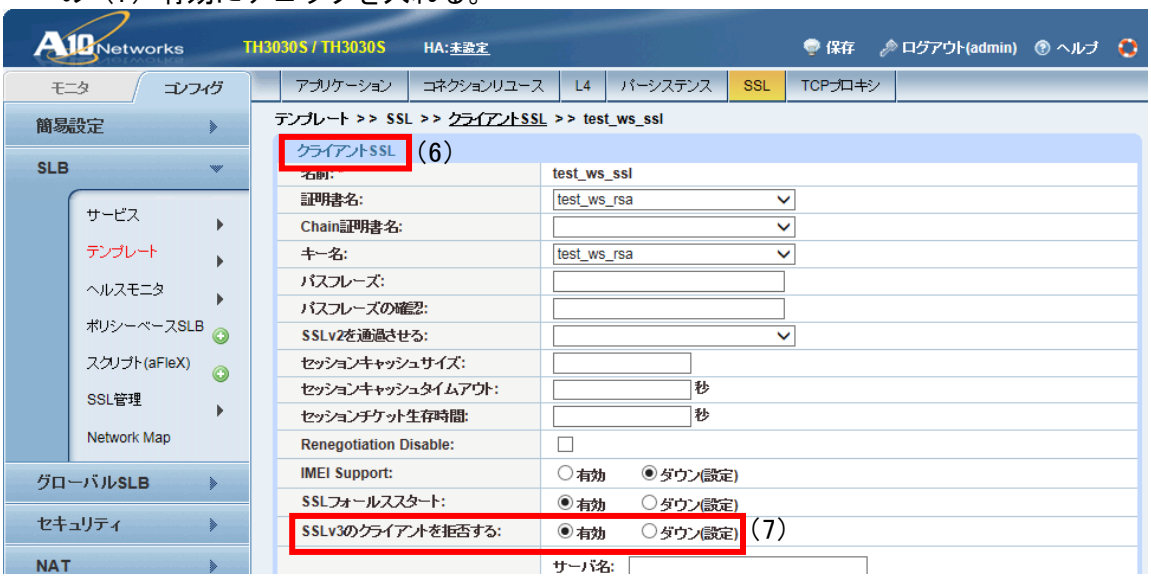

図 6.3.2-2 クライアント SSL 設定画面-1

C) 設定が完了したら (8)「OK」ボタンを押下する。

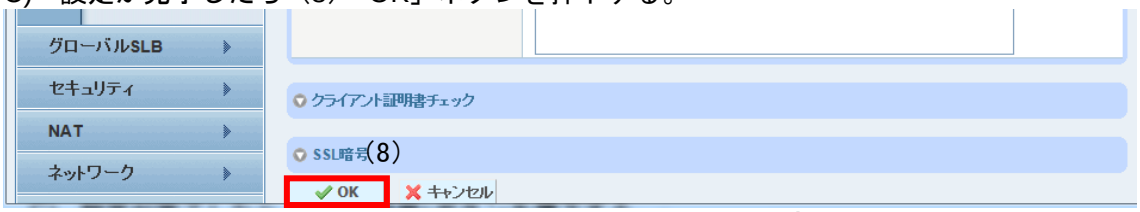

図 6.3.2-3 クライアント SSL 設定画面-2

D) 画面上の電球のアイコンが点滅するので、(9)「保存」をクリックして設定を保存する。

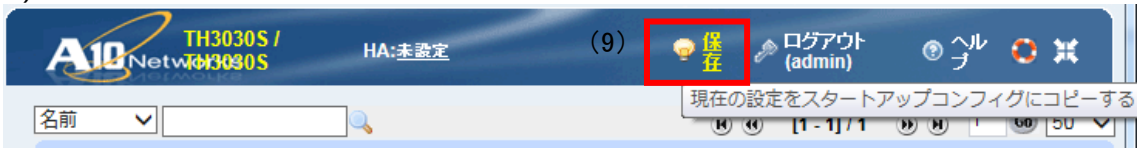

図 6.3.2-4 設定保存画面

II. 暗号スイートの設定

A) ブラウザで管理画面にログインし、(1) コンフィグ－ (2) SLB－ (3) テンプレート－ (4) SSL－ (5) SSL 暗号をクリックする。

図 6.3.2-5 SSL 暗号追加メニュー画面

B) SSL 暗号リスト画面が表示されたら (6)「追加」ボタンを押下する。

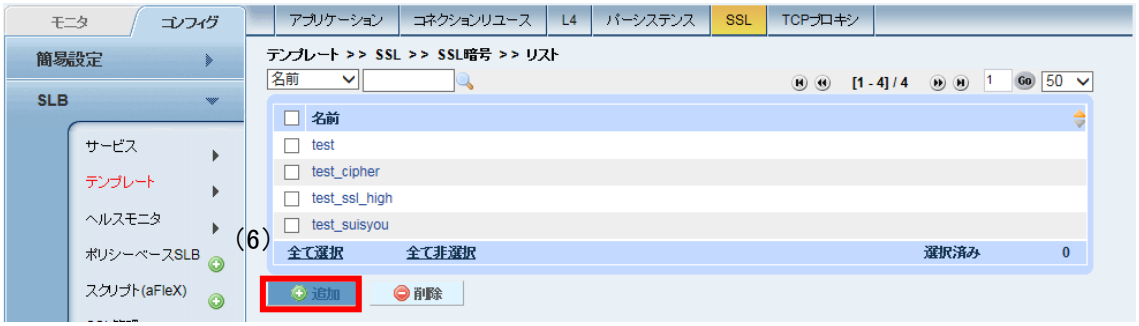

図 6.3.2-6 SSL 暗号リスト画面

C) SSL 暗号新規作成画面が表示されたら (7) 名前を入力し、追加したい (8) SSL 暗号をドロップダウンリストから選択し、(9)「プライオリティー」欄で優先度を入力してから (10)「追加」ボタンを押下する。
更に追加したい SSL 暗号が有る場合は (8) ～ (10) を繰り返す。
追加し終わったら (11)「OK」ボタンを押下する。
※プライオリティーの値が大きいものが優先される。
※RSA を含む暗号スイートは、RSA 証明書を設定しないと使用できない。
※ECDSA を含む暗号スイートは、ECDSA 証明書を設定しないと使用できない。
※証明書は RSA、ECDSA のどちらか一方しか設定できない。

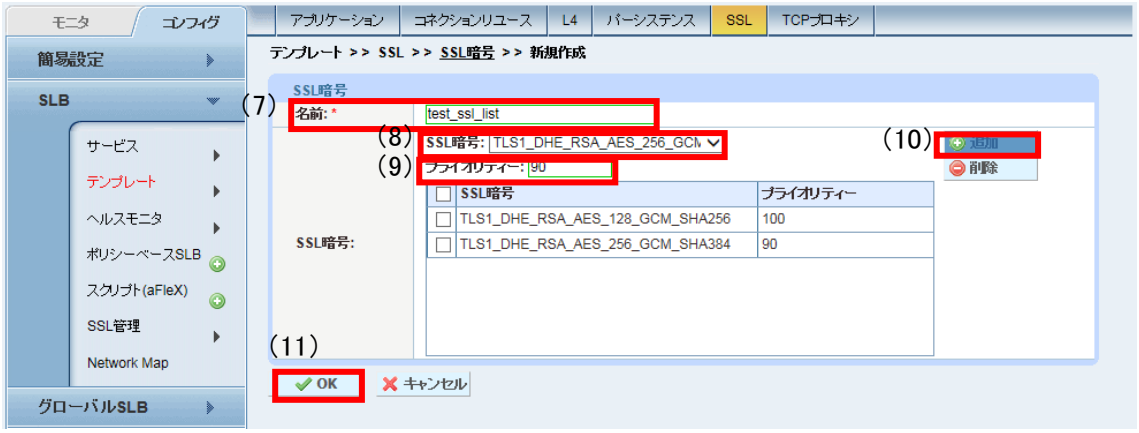

図 6.3.2-7　SSL 暗号新規作成画面

D)　図 6.3.2-1　クライアント SSL リスト画面 で設定したクライアント SSL を開き、(12)「SSL 暗号」内の（13）クラスで「SSL サイファーテンプレート」を選択し、(14) SSL サイファーテンプレートで図 6.3.2-7　SSL 暗号新規作成画面 で作成した SSL 暗号（例 : test_ssl_list）を選択する。あるいは、クラスで「SSL 暗号」を選択し、(15) SSL 暗号で暗号スイートを個別に選択する。
設定が完了したら（16）「OK」ボタンを押下する。

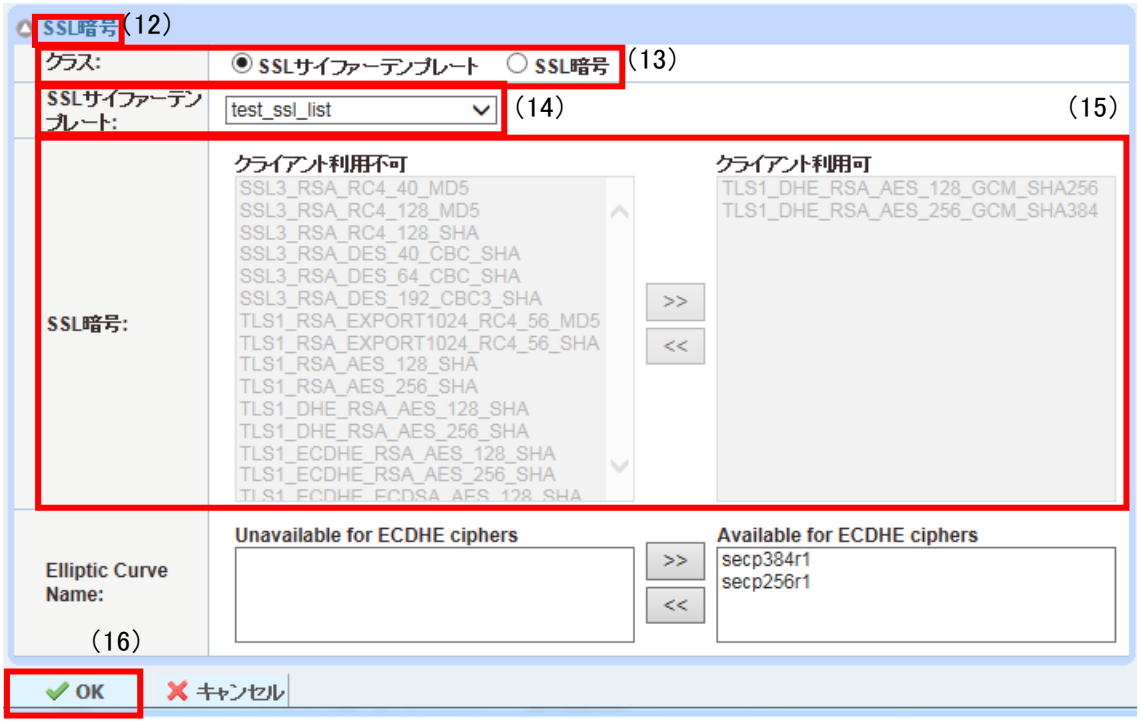

図 6.3.2-8　SSL 暗号画面

E)　クライアント SSL リスト画面に戻るので、(17) 保存ボタンを押下する。

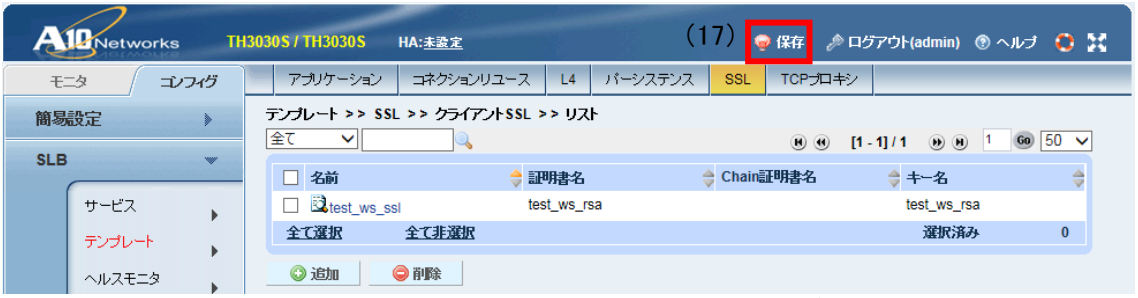

図 6.3.2-9　クライアント SSL リスト（保存ボタン点滅）画面

III. DH/DHE、ECDH/ECDHE の鍵長の設定
DH/DHE の鍵長は設定方法なし。
※DHE の鍵長は 1024bit である。
ECDHE の鍵長は 6.3.1.II.D 図 6.3.2-8 SSL 暗号画面 にて、「Elliptic Curve Name:」の「Available for ECDHE ciphers」欄に secp384r1 もしくは secp256r1 を選択することで、384bit(secp384r1) または 256bit(secp256r1)が設定される。
※「Available for ECDHE ciphers」欄の上位の設定が優先される。

IV. サーバクライアントの優先順位の設定
図 6.3.2-8 SSL 暗号画面 ですべての暗号スイートを選択した場合は、クライアント優先になる。既定は、すべての暗号スイートを 6.4.2II.D の画面で選択した状態であり、クライアント優先である。6.3.1.II.D の手順にて SSL サイファーテンプレートを設定した場合、図 6.3.2-8 SSL 暗号画面 で暗号スイートを一部選択した場合は、サーバ優先となる。

V. 暗号スイートの優先順位の設定
6.3.1.II.D の手順にて SSL サイファーテンプレートを設定した場合にのみ、リストに設定された暗号スイートのプライオリティーの値が高いものから優先順位が設定される。

VI. Extension の設定
設定方法なし。

6.3.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.3.3.1. 高セキュリティ型

(1) RSA 証明書設定時

③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。ただし、鍵交換を EC 系（楕円曲線暗号が含まれる暗号スイート）のみに設定した場合に限る。

※TLS1.0、TLS1.1 の設定を変更する操作はできないため、プロトコルバージョンの設定で TLS1.2 のみに設定することはできないが、TLS1.2 以外で使用可能な暗号スイートが無いように暗号スイートを設定できるため、実質的に高セキュリティ型に準拠が可能である。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

I. プロトコルバージョン

tls1.2、tls1.1、tls1.0、sslv3 が有効である。

※6.3.1⑴RSA 証明書設定時 表 6.3.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）の CipherSuite 選択優先権 のとおり。

II. 暗号スイート

6.3.1⑴RSA 証明書設定時 表 6.3.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）の A10 ネットワークス Thunder 3030S で使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE：1024bit

ECDH/ECDHE：256bit(secp256r1)

IV. サーバクライアントの優先順位の設定

クライアント優先である。

※6.3.1⑴RSA 証明書設定時 表 6.3.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）の CipherSuite 選択優先権 のとおり。

V. 暗号スイートの優先順位の設定

クライアント優先であるため、優先順位はなし。

VI. Extension の設定

6.3.1⑴RSA 証明書設定時 表 6.3.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

tls1.1、tls1.0、sslv3 が有効である。

II. 暗号スイート

差分あり。

高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.3.3.1-1 設定ガイドラインとの差分（高セキュリティ型、RSA 証明書設定時） の「設定ガイドラインの高セキュリティ型(一部)」にある 4 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 17 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.3.3.1-1　設定ガイドラインとの差分（高セキュリティ型、RSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型（一部）	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）
－	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5
		TLS_RSA_WITH_DES_CBC_SHA
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		TLS_RSA_WITH_AES_128_CBC_SHA
		TLS_RSA_WITH_AES_128_CBC_SHA256
		TLS_RSA_WITH_AES_128_GCM_SHA256
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		TLS_RSA_WITH_AES_256_CBC_SHA
		TLS_RSA_WITH_AES_256_CBC_SHA256
		TLS_RSA_WITH_AES_256_GCM_SHA384
		TLS_RSA_WITH_RC4_128_SHA
		TLS_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE の鍵長が 1024bit である。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSLv3 のクライアントを拒否する: 有効　（図 6.3.2-2 参照）
TLS1.0、TLS1.1 の設定はない。

II. 暗号スイート
6.3.1.II.D の手順にて SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティーの値を表 6.3.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定、RSA 証明書設定時） の様に設定する。

表 6.3.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定、RSA 証明書設定時）

プライオリティー	暗号スイート
100	TLS1_DHE_RSA_AES_256_GCM-SHA_384
100	TLS1_ECDHE_RSA_AES_256_GCM_SHA_384
90	TLS1_DHE_RSA_AES_128_GCM_SHA256
90	TLS1_ECDHE_RSA_AES_128_GCM_SHA256

※「プライオリティー」は 1～100 の範囲で指定。100 が最も優先度が高い。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。
ECDH/ECDHE：6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 にて、「Elliptic Curve Name:」の「Available for ECDHE ciphers」欄に secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定
6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
※TLS1.0、TLS1.1 の設定はないが、6.3.3.1(1)③Ⅱ.暗号スイートで設定した暗号スイートが使えるプロトコルバージョンが TLS1.2 のみであるため、結果として TLS1.2 のみ有効になる。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.3.3.1-3　設定ガイドラインとの差分（高セキュリティ型、個別指定、RSA 証明書設定時） の「設定ガイドラインの高セキュリティ型（一部）」にある 4 個の暗号スイートの使用が可能である。使用可能な 4 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.3.3.1-3　設定ガイドラインとの差分（高セキュリティ型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分あり。
DH/DHE の鍵長が 1024bit である。

(2) ECDSA 証明書設定時

TLS1.2 のみ有効にできないため、設定ガイドラインの高セキュリティ型に設定することはできない。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

I. プロトコルバージョン

tls1.2、tls1.1、tls1.0 が有効である。

※6.3.1 ⑵ECDSA 証明書設定時 表 6.3.1-2 暗号設定内容（デフォルト、ECDSA 証明書設定時）の CipherSuite 選択優先権 のとおり。

II. 暗号スイート

6.3.1 ⑵ECDSA 証明書設定時 表 6.3.1-2 暗号設定内容（デフォルト、ECDSA 証明書設定時）の A10 ネットワークス Thunder 3030S で使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDH/ECDHE：256bit(secp256r1)

IV. サーバクライアントの優先順位の設定

クライアント優先である。

※6.3.1（2）ECDSA 証明書設定時 表 6.3.1-2 暗号設定内容（デフォルト、ECDSA 証明書設定時）の CipherSuite 選択優先権 のとおり。

V. 暗号スイートの優先順位の設定

クライアント優先であるため、優先順位はなし。

VI. Extension の設定

6.3.1 ⑵ ECDSA 証明書設定時 表 6.3.1-2 暗号設定内容（デフォルト、ECDSA 証明書設定時）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

tls1.1、tls1.0 が有効である。

II. 暗号スイート

差分あり。

高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.3.3.1-4 設定ガイドラインとの差分（高セキュリティ型、ECDSA 証明書設定時） の「設定ガイドラインの高セキュリティ型（一部）」にある 2 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 3 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.3.3.1-4　設定ガイドラインとの差分（高セキュリティ型、ECDSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型（一部）	暗号スイート設定結果
α	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)
-	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③　プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSLv3 のクライアントを拒否する: 有効　（図 6.3.2-2 参照）
※TLS1.0、TLS1.1 は有効のままで、変更できない。

II. 暗号スイート
6.3.1.II.D の手順にて SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティーの値を表 6.3.3.1-5　暗号スイートの設定（高セキュリティ型、個別指定、ECDSA 証明書設定時）の様に設定する。

表 6.3.3.1-5　暗号スイートの設定（高セキュリティ型、個別指定、ECDSA 証明書設定時）

プライオリティー	暗号スイート
100	TLS1_ECDHE_ECDSA_AES_256_GCM_SHA384
90	TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256

※「プライオリティー」は 1～100 の範囲で指定。100 が最も優先度が高い。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE : 6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 にて、「Elliptic Curve Name:」の「Available for ECDHE ciphers」欄に secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定
6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLS1.0、TLS1.1 が有効である。

II. 暗号スイート

差分なし。

高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.3.3.1-6　設定ガイドラインとの差分（高セキュリティ型、個別指定、ECDSA 証明書設定時）の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。使用可能な 2 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.3.3.1-6　設定ガイドラインとの差分（高セキュリティ型、個別指定、ECDSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)	1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)	2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

※6.3.1.II.D の画面にて設定した値となる。

6.3.3.2. 推奨セキュリティ型

(1) RSA 証明書設定時

③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.3.3.1 高セキュリティ型 と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

sslv3 が有効である。

II. 暗号スイート

差分あり。

推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.3.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型、RSA 証明書設定時）の「設定ガイドラインの推奨セキュリティ型(一部)」にある 17 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 4 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.3.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型、RSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5
		TLS_RSA_WITH_RC4_128_SHA
		TLS_RSA_WITH_DES_CBC_SHA
		TLS_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSLv3 のクライアントを拒否する: 有効　（図 6.3.2-2 参照）

II. 暗号スイート
6.3.1.II.D の手順にて暗号スイートを設定する際にプライオリティーの値を表 6.3.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定、RSA 証明書設定時）の様に設定する。

表 6.3.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定、RSA 証明書設定時）

プライオリティー	暗号スイート
100	TLS1_DHE_RSA_AES_128_SHA
100	TLS1_DHE_RSA_AES_128_SHA256
100	TLS1_DHE_RSA_AES_128_GCM_SHA256
100	TLS1_ECDHE_RSA_AES_128_SHA
100	TLS1_ECDHE_RSA_AES_128_SHA256
100	TLS1_ECDHE_RSA_AES_128_GCM_SHA256
90	TLS1_RSA_AES_128_SHA
90	TLS1_RSA_AES_128_SHA256
90	TLS1_RSA_AES_128_GCM_SHA256

プライオリティー	暗号スイート
70	TLS1_DHE_RSA_AES_256_SHA
70	TLS1_DHE_RSA_AES_256_SHA256
70	TLS1_DHE_RSA_AES_256_GCM_SHA384
70	TLS1_ECDHE_RSA_AES_256_SHA
70	TLS1_ECDHE_RSA_AES_256_GCM_SHA384
60	TLS1_RSA_AES_256_SHA
60	TLS1_RSA_AES_256_SHA256
60	TLS1_RSA_AES_256_GCM_SHA384

※「プライオリティー」は 1～100 の範囲で指定。100 が最も優先度が高い。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。
ECDH/ECDHE : 6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 にて、「Elliptic Curve Name:」の「Available for ECDHE ciphers」欄に secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定
6.3.1.II.D 図 6.3.2-8　SSL 暗号画面の画面で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.3.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、RSA 証明書設定時） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 17 個の暗号スイートの使用が可能である。使用可能な 17 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティ型の順位と同じである。

表 6.3.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	6	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	3	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	5	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	9	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	7	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	14	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	12	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	11	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	13	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	10	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	17	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	16	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	15	TLS_RSA_WITH_AES_256_GCM_SHA384(E)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

(2) ECDSA 証明書設定時
①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.3.3.1 高セキュリティ型 (2)ECDSA 証明書設定時
と同じである。

② ①の設定と設定ガイドラインの設定内容との差分
I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.3.3.2-4 設定ガイドラインとの差分（推奨セキュリティ型、ECDSA 証明書設定時） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 5 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.3.3.2-4　設定ガイドラインとの差分（推奨セキュリティ型、ECDSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。
※ECDH/ECDHE の場合、図 6.3.2-8　SSL 暗号画面で設定した値となる。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSLv3 のクライアントを拒否する: 有効　（図 6.3.2-2 参照）
※TLS1.0、TLS1.1 は有効のままで、変更できない。

II. 暗号スイート
6.3.1.II.D の手順にて SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティーの値を以下の様に設定する。

表 6.3.3.2-5　暗号スイートの設定（推奨セキュリティ型、個別指定、ECDSA 証明書設定時）

プライオリティー	暗号スイート
100	ECDHE-ECDSA-AES128-SHA
100	ECDHE-ECDSA-AES128-SHA256
100	ECDHE-ECDSA-AES128-GCM-SHA256
70	ECDHE-ECDSA-AES256-SHA
70	ECDHE-ECDSA-AES256-GCM-SHA384

※「プライオリティー」は 1～100 の範囲で指定。100 が最も優先度が高い。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE : 6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 にて、「Elliptic Curve Name:」の「Available for ECDHE ciphers」欄に secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定
6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.3.3.2-6　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、ECDSA 証明書設定時） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 5 個の暗号スイートの使用が可能である。使用可能な 5 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティの順位と同じである。

表 6.3.3.2-6　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、ECDSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
D	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	4	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.3.3.3. セキュリティ例外型

(1) RSA 証明書設定時
③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.3.3.1 高セキュリティ型 (1)RSA 証明書設定時
と同じである。

② 設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分あり。
セキュリティ例外型に含まれる暗号スイート 67 個のうち､表 6.3.3.3-1　設定ガイドラインとの差分（セキュリティ例外型、RSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型(一部)」にある 19 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 2 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.3.3.3-1　設定ガイドラインとの差分（セキュリティ例外型、RSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)
_	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5
		TLS_RSA_WITH_DES_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）
6.3.1.II.D の手順にて暗号スイートを設定する際にプライオリティーの値を以下の様に設定する。

I. プロトコルバージョン
SSLv3 のクライアントを拒否する: ダウン（設定）　（図 6.3.2-2 参照）

II. 暗号スイート
6.3.1.II の手順で表 6.3.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定、RSA 証明書設定時）の暗号スイートを追加する。

表 6.3.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定、RSA 証明書設定時）

プライオリティー	暗号スイート
100	TLS1_DHE_RSA_AES_128-SHA
100	TLS1_DHE_RSA_AES_128_SHA256
100	TLS1_DHE_RSA_AES_128_GCM_SHA256

プライオリティー	暗号スイート
100	TLS1_ECDHE_RSA_AES_128_SHA
100	TLS1_ECDHE_RSA_AES_128_SHA256
100	TLS1_ECDHE_RSA_AES_128_GCM_SHA256
90	TLS1_RSA_AES_128_SHA
90	TLS1_RSA_AES_128_SHA256
90	TLS1_RSA_AES_128_GCM_SHA256
70	TLS1_DHE_RSA_AES_256_SHA
70	TLS1_DHE_RSA_AES_256_SHA256
70	TLS1_DHE_RSA_AES_256_GCM_SHA384
70	TLS1_ECDHE_RSA_AES_256_SHA
70	TLS1_ECDHE_RSA_AES_256_GCM_SHA384
60	TLS1_RSA_AES_256_SHA
60	TLS1_RSA_AES_256_SHA256
60	TLS1_RSA_AES_256_GCM_SHA384
40	SSL3_RSA_RC4_128_SHA
30	SSL3_RSA_DES_192_CBC3_SHA

※「プライオリティー」は 1～100 の範囲で指定。100 が最も優先度が高い。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。
ECDH/ECDHE : 6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 にて、「Elliptic Curve Name:」の「Available for ECDHE ciphers」欄に secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定
6.3.1.II.D 図 6.3.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.3.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定、RSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型（一部）」にある 19 個の暗号スイートの使用が可能である。使用可能な 19 個の暗号スイートの優先順位は、設定ガイドラインのセキュリティ例外型の順位と同じである。

表 6.3.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）	6	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）	3	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）	2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	5	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	9	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	8	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	7	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）	14	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）	12	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）	11	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	13	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	10	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	17	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	16	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	15	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	18	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	19	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

IV. DH/DHE、ECDH/ECDHE の鍵長
差分なし。
※ECDH/ECDHE の場合、6.3.1.II.D の画面にて設定した値となる。

(2) ECDSA 証明書設定時
SSLv3 で使用できる暗号スイートがないため、セキュリティ例外型は設定できない。

6.4. 日本ラドウェア Alteon シリーズ

本章では、Alteon VA について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能である。RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なり、両方の証明書を設定した場合は、両方の暗号スイートが有効になる。6.4.1 **デフォルトでの暗号設定内容の調査**、および、6.4.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**は、RSA 証明書と ECDSA 証明書の両方を設定した場合について記載する。

6.4.1. デフォルトでの暗号設定内容の調査

表 6.4.1-1 暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	17
tls1.1	ON	サーバ	13
tls1.0	ON	サーバ	13
sslv3	ON	サーバ	13
sslv2	設定不可	ー	ー

※プロトコルごとの CipherSuite 数は、日本ラドウェア Alteon VA で使用可能な暗号スイート表で ON の暗号スイートの数に unassigned（IANA の一覧で unassigned となっている暗号スイートの id）の暗号スイート 2 個（0x00,0x62、0x00,0x64）を含む。

- 日本ラドウェア Alteon VA で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:11	ON:7	ON:7	ON:7	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:10	ON:6	ON:6	ON:6	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	ON:13	ON:9	ON:9	ON:9	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:12	ON:8	ON:8	ON:8	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:7	ON:3	ON:3	ON:3	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:3	ON:1	ON:1	ON:1	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:2	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON:9	ON:5	ON:5	ON:5	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON:4	ON:2	ON:2	ON:2	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	ON:8	ON:4	ON:4	ON:4	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:5	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:1	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	ON:15	ON:11	ON:11	ON:11	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	ON:14	ON:10	ON:10	ON:10	OFF

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.4.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで管理画面にログインし、(1)「Application Delivery」ー(2)「SSL」ー(3)「SSL Policy」ーと遷移し、一覧の（4）「SSL Policy」（例：testSSLpolicy）をクリックする。

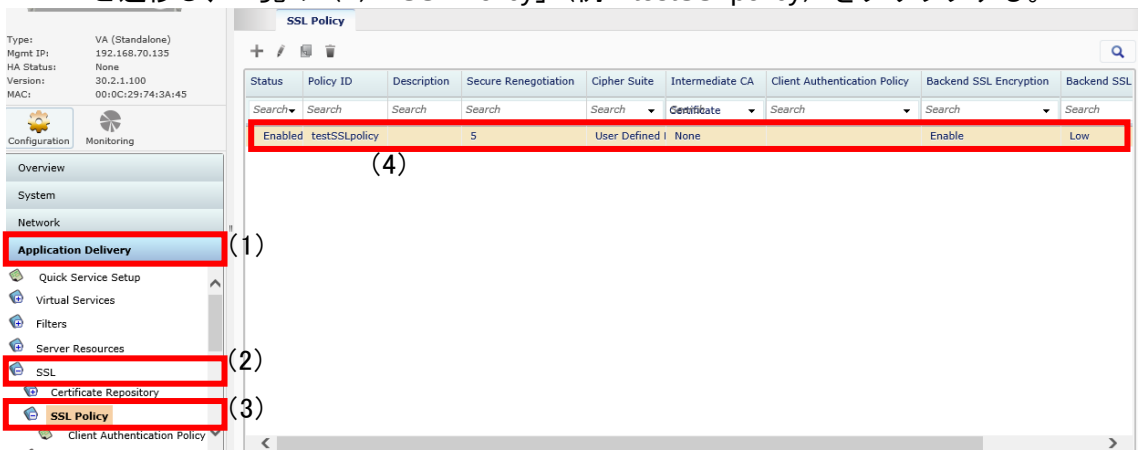

図 6.4.2-1 SSL Policy 一覧画面-1

B) 「SSL Policy 編集画面」が表示されたら（5）「Allowed SSL Protocol Version」の使用したいプロトコルにチェックを入れ、設定が完了したら（6）「Submit」ボタンを押下する。

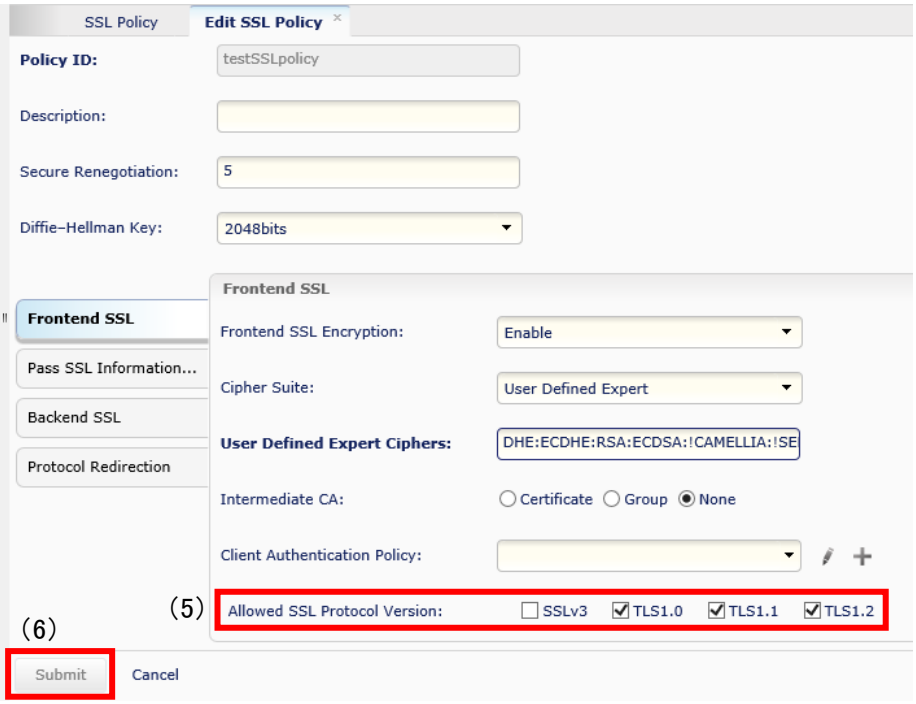

図 6.4.2-2 SSL Policy 編集画面-1

C) 設定が完了したら、画面上の（7）「Apply Required」ボタンと（8）「Save Required」ボタンを押下して設定を適用・保存する。

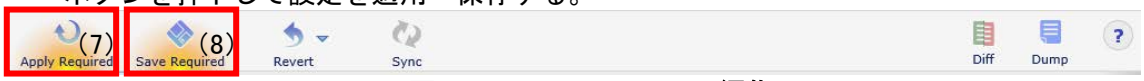

図 6.4.2-3 SSL Policy 編集画面-2

II. 暗号スイートの設定

A) ブラウザで管理画面にログインし、(1)「Application Delivery」ー（2）「SSL」ー（3）「SSL Policy」ーと遷移し、一覧の（4）「SSL Policy」（例：testSSLpolicy）をクリックする。

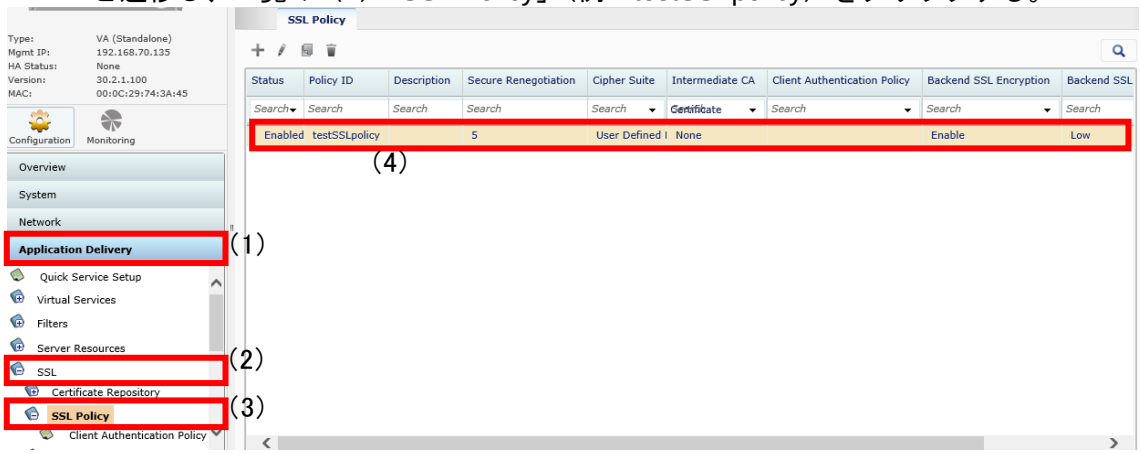

図 6.4.2-4 SSL Policy 一覧画面-2

B) 「SSL Policy 編集画面」が表示されたら（5）「Cipher Suite」欄で「User Defined Expert」を選択し、(6)「User Defined Expert Ciphers」欄に使用したい暗号スイートを OpenSSL 表記で設定し、(7)「Submit」ボタンを押下する。

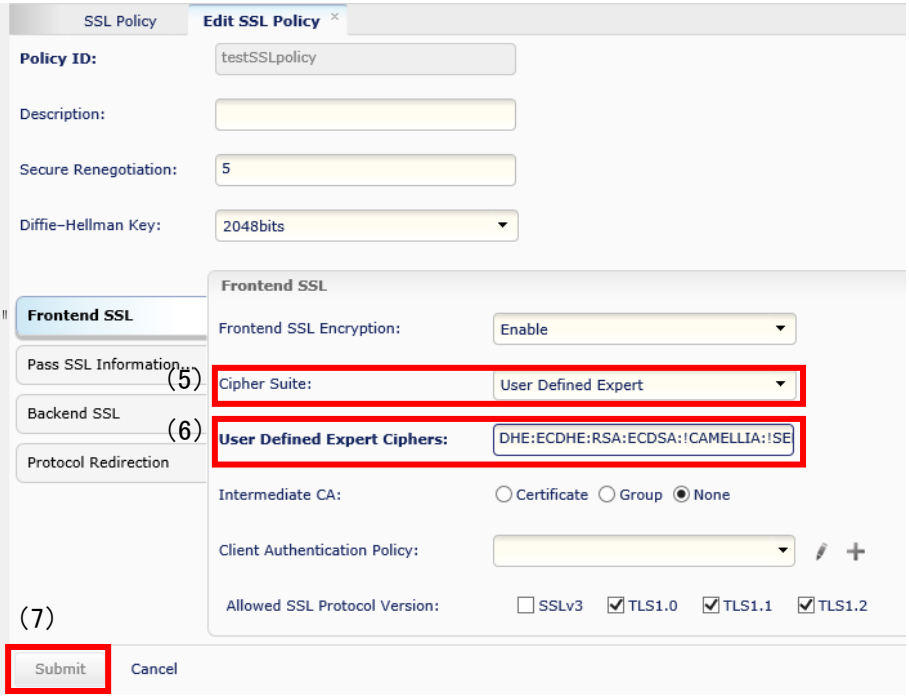

図 6.4.2-5 SSL Policy 編集画面-3

C) 設定が完了したら、画面上の（8）「Apply Required」ボタンと（9）「Save Required」ボタンを押下して設定を適用・保存する。

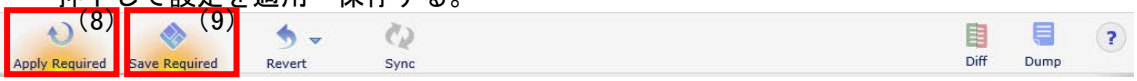

図 6.4.2-6　SSL Policy 編集画面-4

III. DH/DHE、ECDH/ECDHE の鍵長の設定
DH/DHE の鍵長は、図 6.4.2-5　SSL Policy 編集画面-3 の「Diffie-Hellman Key:」欄で 1024bits または 2048bits を選択する。
ECDH/ECDHE の鍵長は、設定方法なし。既定で secp256r1 が設定される。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで暗号スイートを設定した順位になる。
※グループ名で設定した際の優先順位については強度が高い順になる。

VI. Extension の設定
設定方法なし。

6.4.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.4.3.1. 高セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
TLS1.2 のチェックを入れる。
TLS1.1、TLS1.0、SSLv3.0 のチェックを外す。
（図 6.4.2-2 参照）

II. 暗号スイート
図 6.4.2-5　SSL Policy 編集画面-3 の「User Defined Expert Ciphers」欄に、以下の文字列を設定する。
AESGCM:!ADH

III. DH/DHE、ECDH/ECDHE の鍵長
図 6.4.2-5　SSL Policy 編集画面-3 の「Diffie-Hellman Key:」欄で 2048bits を選択する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分あり。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.4.3.1-1　設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型(一部)」にある 6 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 4 個の暗号スイートの使用が可能となる。優先順位は、表 6.4.3.1-2　設定ガイドラインとの差分（高セキュリティ型）のとおりである。

表 6.4.3.1-1　設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）	3	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α追加）	5	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）	9	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）	2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β追加）	4	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）	8	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）
－	設定ガイドラインの高セキュリティ型に該当しない暗	1	TLS_RSA_WITH_AES_128_GCM_SHA256

	号スイート	6	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
		7	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
		10	TLS_RSA_WITH_AES_256_GCM_SHA384

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLS1.2 のチェックを入れる。
TLS1.1、TLS1.0、SSLv3.0 のチェックを外す。
（図 6.4.2-2 参照）

II. 暗号スイート
図 6.4.2-5 SSL Policy 編集画面-3 の「User Defined Expert Ciphers」欄に、以下の文字列を設定する。
AESGCM:!ADH:!AES128-GCM-SHA256:!AES256-GCM-SHA384:!ECDH-ECDSA-AES128-GCM-SHA256:!ECDH-ECDSA-AES256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：2048bit
ECDH/ECDHE：既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.4.3.1-1 設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型(一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.4.3.1-2 設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (α追加)	2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)	3	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	6	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

上記設定で、暗号スイートを優先順位も含めて高セキュリティ型に設定することができる。以下のように個別に暗号スイートを設定しても同様である。

DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.4.3.2. 推奨セキュリティ型

①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
TLS1.2、TLS1.1、TLS1 のチェックを入れる。
SSLv3 のチェックを外す。
（図 6.4.2-2 参照）

II. 暗号スイート
図 6.4.2-5 SSL Policy 編集画面-3 の「User Defined Expert Ciphers」欄に、以下の文字列を設定する。
ALL:!ADH:!SEED:!EXP:!NULL:!RC4:!DES:!DES:!3DES:!AECDH

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：2048bit
ECDH/ECDHE：既定で 256bit(secp256r1)となる。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。

推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.4.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 34 個の暗号スイートの使用が可能である。使用可能な 34 個の暗号スイートの優先順位は、表 6.4.3.2-1 設定ガイドラインとの差分（推奨セキュリティ型） のとおりである。

表 6.4.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）	26	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA（A）	27	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）	25	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）	24	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）	23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	22	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）	21	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	20	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）	19	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	18	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	33	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	32	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）	34	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	31	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
C	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA（C 追加）	30	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA（C 追加）
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256（C 追加）	29	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256（C 追加）
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256（C 追加）	28	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256（C 追加）
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）	9	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）	8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA（D）	10	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）	7	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）	6	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）	4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）	2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	16	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	15	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	17	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	14	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
F	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）	13	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）	12	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）	11	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）
①と同様である。

④ ③の設定と設定ガイドラインの設定内容との差分
②設定ガイドラインの設定内容との差分と同様である。
①プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定の暗号スイートは、推奨セキュリティ型のもののみに設定できるが優先順位が異なる。以下のように個別に暗号スイートを個別に設定することで、優先順位も推奨セキュリティ型に設定することができる。
ただし、「User Defined Expert Ciphers」欄の入力文字列制限（256 文字まで）により、推奨セキュリティ型の 34 個の暗号スイートのうち、11 個の暗号スイートまでしか設定できない。

図 6.4.2-5 SSL Policy 編集画面-3 の「User Defined Expert Ciphers」欄に以下の様に記述する。

DHE-RSA-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA

6.4.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
TLS1.2、TLS1.1、TLS1、SSL3 のチェックを入れる。 （図 6.4.2-2 参照）

II. 暗号スイート
図 6.4.2-5 SSL Policy 編集画面-3 の「User Defined Expert Ciphers」欄に、以下の文字列を記載する。
ALL:!ADH:!SEED:!EXP:!NULL:!DES:!DES:!AECDH:!MD5

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：2048bit
ECDH/ECDHE：既定で 256bit(secp256r1)となる。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

II. 暗号スイート

差分あり。

セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.4.3.3-1　設定ガイドラインとの差分（セキュリティ例外型） の「設定ガイドラインのセキュリティ例外型（一部）」にある 37 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 6 個の暗号スイートが使用可能である。優先順位は、表 6.4.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）のとおりである。

表 6.4.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	26	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	27	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	25	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	24	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)	23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	22	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)	21	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	20	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)	19	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	18	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	33	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	32	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	34	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	31	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
C	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)	30	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)	29	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)	28	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	9	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	10	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	7	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)	6	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)	4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)	2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	16	TLS_RSA_WITH_AES_256_CBC_SHA (E)

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	15	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	17	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	14	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
F	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）	13	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）	12	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）	11	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）
G	TLS_RSA_WITH_RC4_128_SHA（G）	38	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	43	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA（H）	41	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA（H）
－	設定ガイドラインのセキュリティ例外型に該当しない暗号スイート	37	TLS_ECDH_ECDSA_WITH_RC4_128_SHA
		42	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
		36	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
		40	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
		35	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		39	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLS1.2、TLS1.1、TLS1、SSL3 のチェックを入れる。　（図 6.4.2-2 参照）

II. 暗号スイート
図 6.4.2-5　SSL Policy 編集画面-3 の「User Defined Expert Ciphers」欄に、以下の文字列を設定する。
ALL:!ADH:!SEED:!EXP:!NULL:!DES:!DES:!AECDH:!MD5:!ECDH-ECDSA-RC4-SHA:!ECDH-ECDSA-DES-CBC3-SHA:!ECDHE-ECDSA-RC4-SHA:!ECDHE-ECDSA-DES-CBC3-SHA:!ECDHE-RSA-RC4-SHA:!ECDHE-RSA-DES-CBC3-SHA

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：2048bit
ECDH/ECDHE：既定で 256bit(secp256r1)となる。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定方法なし。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

II. 暗号スイート

差分なし。

セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.4.3.3-1　設定ガイドラインとの差分（セキュリティ例外型） の「設定ガイドラインのセキュリティ例外型(一部)」にある 37 個の暗号スイートの使用が可能である。使用可能な 37 個の暗号スイートの優先順位は、表 6.4.3.3-1 設定ガイドラインとの差分（セキュリティ例外型）のとおりである。

表 6.4.3.3-2　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	26	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	27	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	25	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	24	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)	23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	22	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)	21	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	20	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)	19	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	18	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	33	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	32	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	34	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	31	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
C	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)	30	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)	29	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (C 追加)
	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)	28	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (C 追加)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	9	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	10	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	7	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)	6	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)	4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)	2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	16	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	15	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	17	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	14	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
F	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）	13	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）	12	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384（F 追加）
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）	11	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384（F 追加）
G	TLS_RSA_WITH_RC4_128_SHA（G）	35	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	37	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA（H）	36	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA（H）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

①プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定の暗号スイートは、セキュリティ例外型のもののみに設定できるが優先順位が異なる。以下のように個別に暗号スイートを個別に設定することで、優先順位もセキュリティ例外型に設定することができる。
ただし、「User Defined Expert Ciphers」欄の入力文字列制限（256 文字まで）により、セキュリティ例外型の 37 個の暗号スイートのうち、11 個の暗号スイートまでしか設定できない。

図 6.4.2-5　SSL Policy 編集画面-3 の「User Defined Expert Ciphers」欄に以下の様に記述する。

DHE-RSA-AES128-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.5. 富士通 IPCOM シリーズ

本章では、IPCOM EX2700 IN について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書のみが設定可能であり、6.5.1 **デフォルトでの暗号設定内容の調査**、および、6.5.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、RSA 証明書を設定した場合について記載する。

6.5.1. デフォルトでの暗号設定内容の調査

表 6.5.1-1 暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	7
tls1.1	OFF	ー	0
tls1.0	ON	クライアント	5
sslv3	ON	クライアント	5
sslv2	OFF	ー	0

- 富士通 IPCOM EX2700 IN で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	----	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				----	ON	OFF	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	----	ON	OFF	ON	ON	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	----	ON	OFF	ON	ON	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	----	ON	OFF	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	----	ON	OFF	ON	ON	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	----	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	----	ON	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.5.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで IPCOM EX2700 IN WEB コンソールにログインし、(1) 設定－ (2) 装置設定－ (3) SSL アクセラレータ (4) 仮想 SSL サーバをクリックして、(5) 仮想 SSL サーバー覧を表示し、編集したい仮想サーバを選択し、(6) 仮想 SSL サーバ設定項目を表示する。

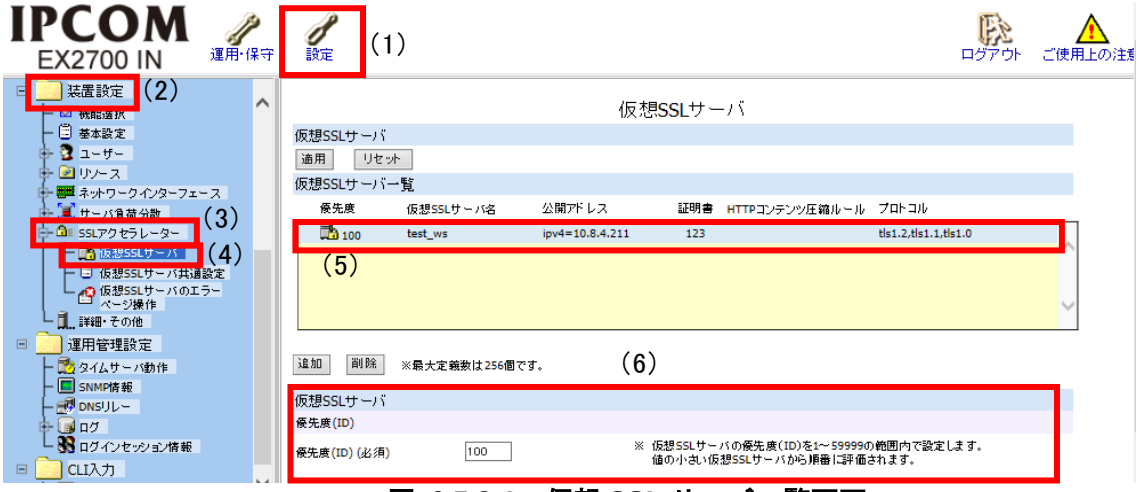

図 6.5.2-1 仮想 SSL サーバー覧画面

B) 仮想 SSL サーバ設定項目にある (7)「詳細設定」ボタンを押下し、(8) プロトコル一覧の有効にしたいプロトコルバージョンに (9) チェックを入れる。

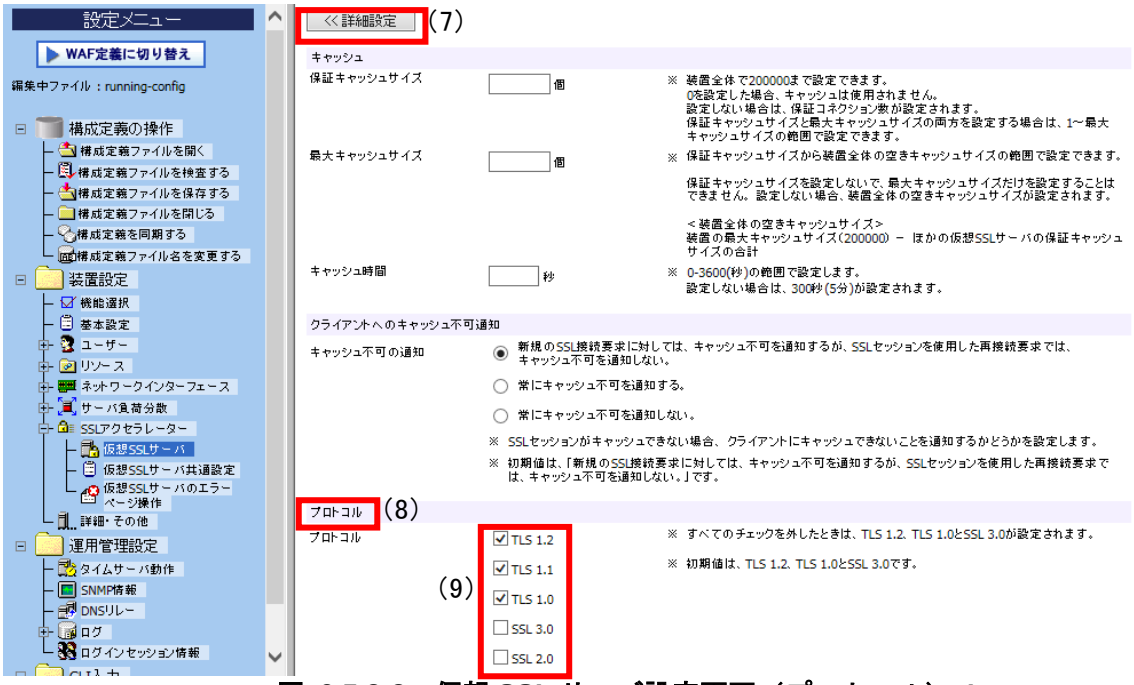

図 6.5.2-2 仮想 SSL サーバ設定画面（プロトコル）-1

C) 設定が完了したら (10)「適用」ボタンを押下する。

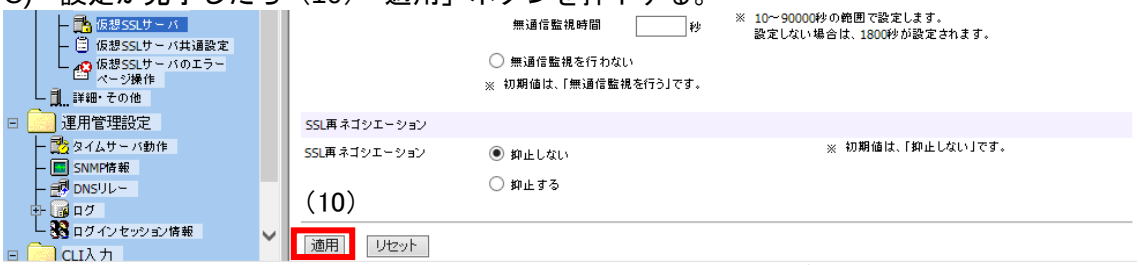

図 6.5.2-3 仮想 SSL サーバ設定画面（プロトコル）-2

D) 構成の保存を促すポップアップが表示されるので（11）「OK」ボタンを押下してポップアップを閉じる。

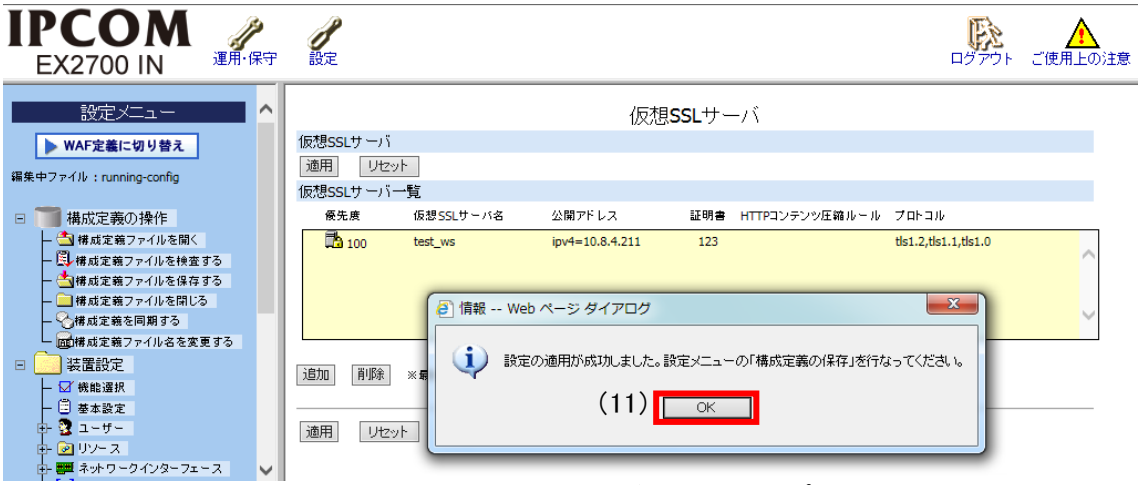

図 6.5.2-4　仮想 SSL サーバ設定画面（プロトコル）-3

E)　（12）構成定義の操作ー（13）構成定義ファイルを保存するをクリックして、（14）「構成定義ファイルの保存」ポップアップを表示し、（15）「即時反映（running-config）と再起動時に反映（startup-config）」にチェックを入れ、（16）「OK」ボタンを押下して保存する。

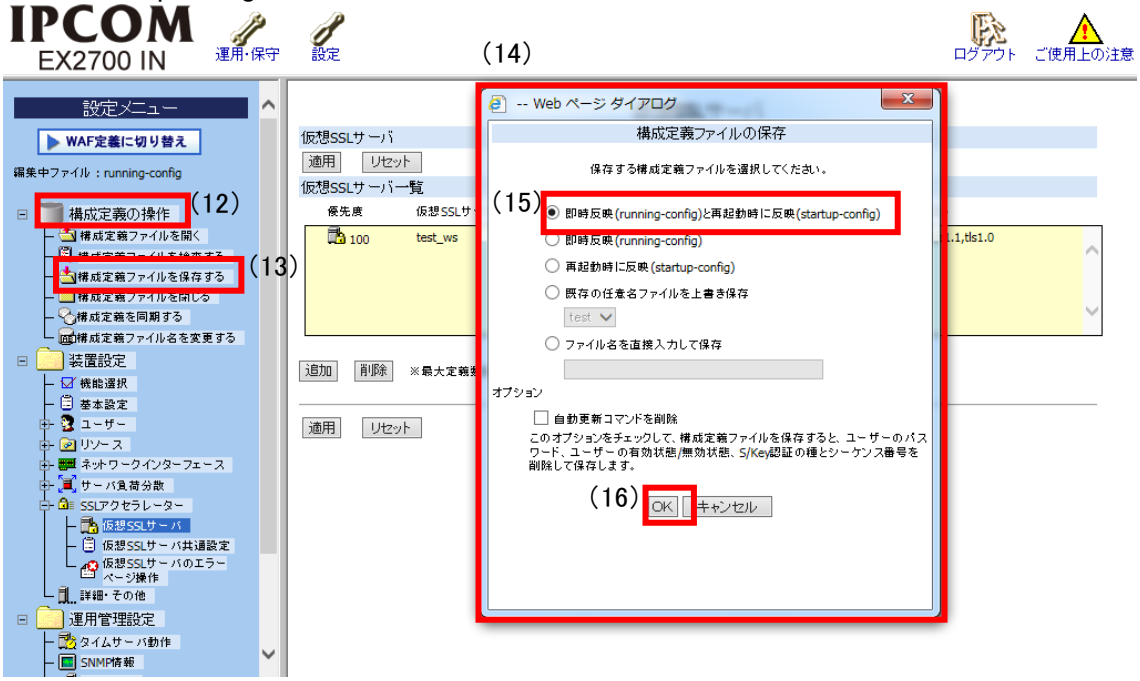

図 6.5.2-5　構成定義ファイル保存画面-1

II. 暗号スイートの設定

A) 図 6.5.2-6 仮想 SSL サーバ設定画面（暗号スイート）の（1）「暗号スイート」で（2）「設定する」を選択し、（3）「設定」ボタンを押下する。

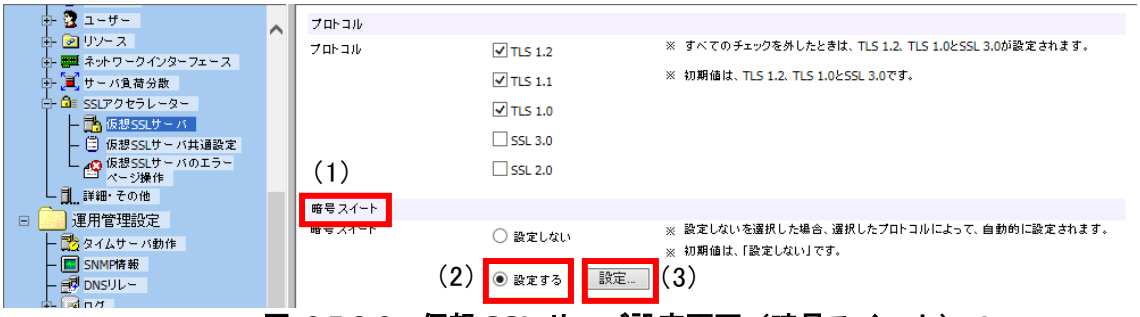

図 6.5.2-6 仮想 SSL サーバ設定画面（暗号スイート）-1

B) （4）「仮想 SSL サーバ暗号スイート選択」画面が表示されるので、（5）「暗号スイートを選択」の一覧から有効にしたい「暗号スイート」もしくは「グループ化文字列」にチェックを入れ、（6）「←＋」ボタンで有効、（7）「→」ボタンで無効を選択する。選択した暗号スイートは（8）「選択した暗号スイート」欄に表示され、現在有効になっている暗号スイートは（9）「選択した暗号スイートの展開結果」欄に表示される。選択が完了したら（10）「OK」ボタンを押下して画面を閉じる。

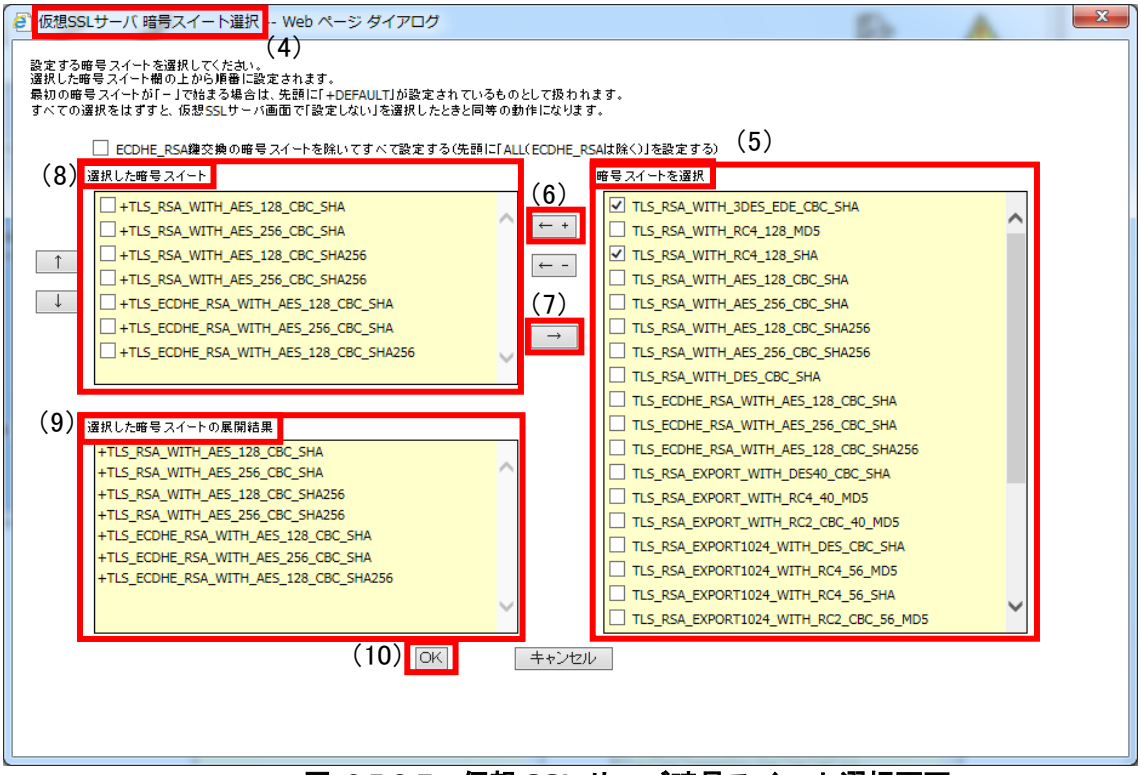

図 6.5.2-7 仮想 SSL サーバ暗号スイート選択画面

C)　設定が完了したら（11）「適用」ボタンを押下する。

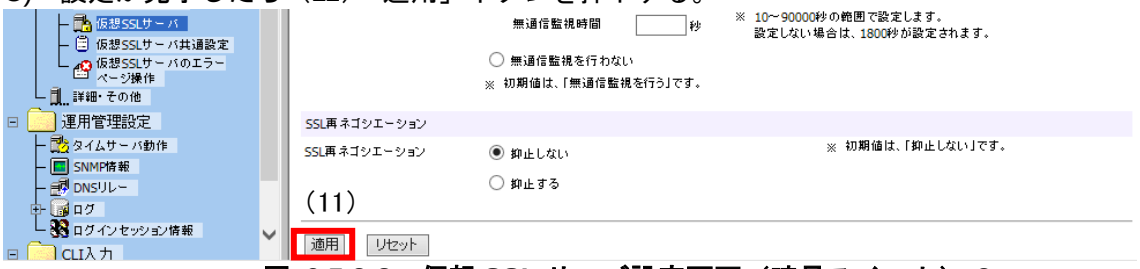

図 6.5.2-8　仮想 SSL サーバ設定画面（暗号スイート）-2

D)　構成の保存を促すポップアップが表示されるので（12）「OK」ボタンを押下してポップアップを閉じる。

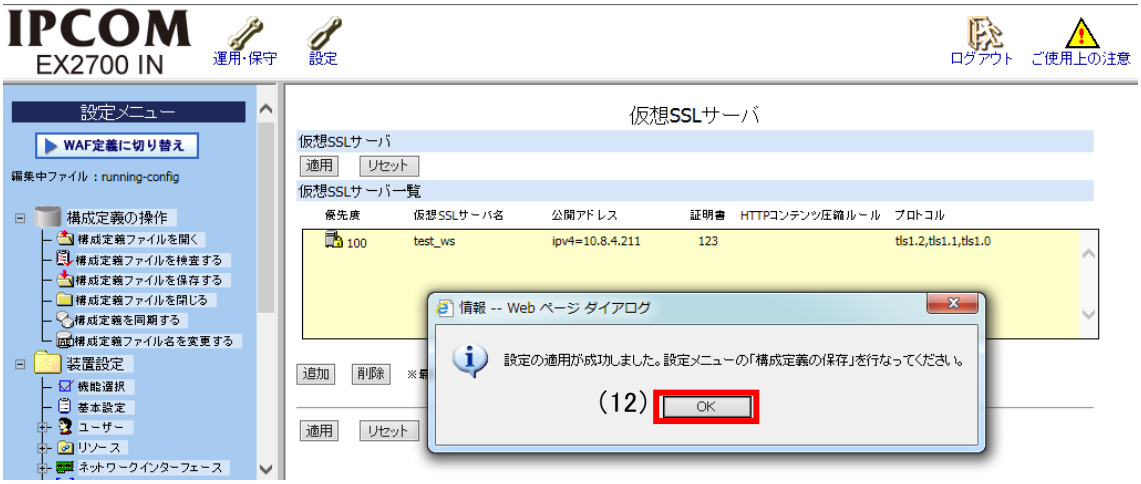

図 6.5.2-9　仮想 SSL サーバ設定画面（暗号スイート）-3

E)　（13）構成定義の操作ー（14）構成定義ファイルを保存するをクリックして、（15）「構成定義ファイルの保存」ポップアップを表示し、（16）「即時反映（running-config）と再起動時に反映（startup-config）」にチェックを入れ、（17）「OK」ボタンを押下して保存する。

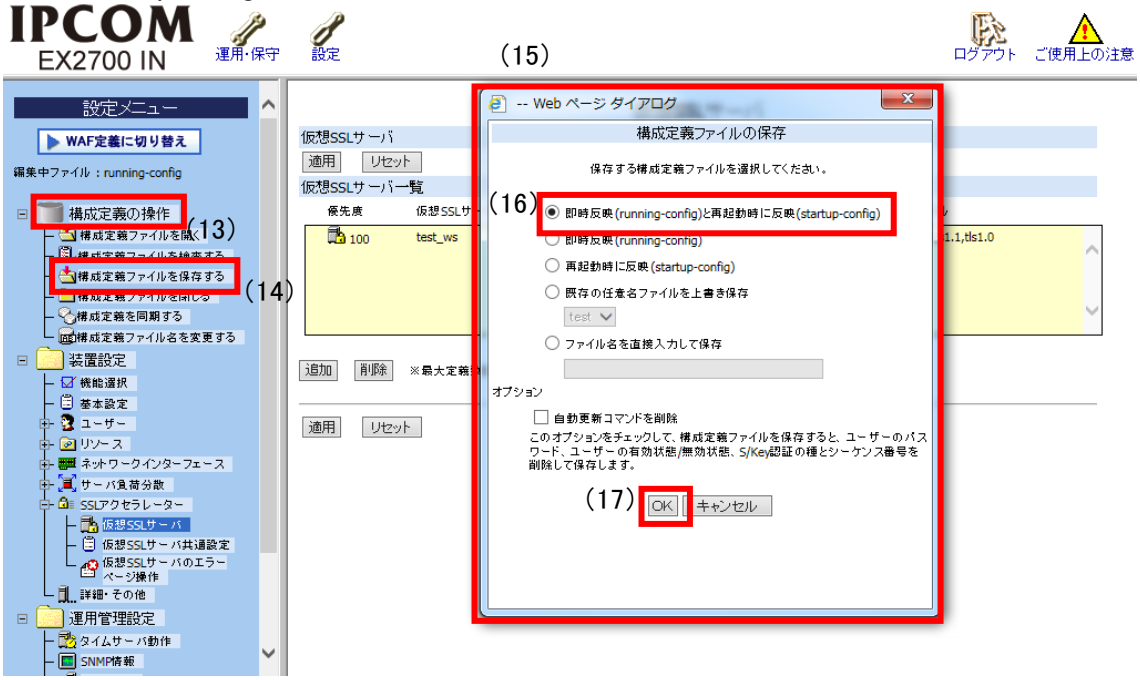

図 6.5.2-10　構成定義ファイル保存画面-2

III. DH/DHE、ECDH/ECDHE の鍵長の設定
設定方法なし。
ECDHE の鍵長は、既定で 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定方法なし。

6.5.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.5.3.1. 高セキュリティ型

高セキュリティ型の暗号スイートが使用できないため、設定ガイドラインの高セキュリティ型に設定することはできない。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
高セキュリティ型の暗号スイートが使用できない。

② ①の設定と設定ガイドラインの設定内容との差分
高セキュリティ型に含まれる 12 個の暗号スイートがすべて使用できない。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）
高セキュリティ型の暗号スイートが使用できない。

④ ③の設定と設定ガイドラインの設定内容との差分
高セキュリティ型に含まれる 12 個の暗号スイートがすべて使用できない。

6.5.3.2. 推奨セキュリティ型

①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
SSL プロトコル：チェック有：TLS1.0、TLS1.1、TLS1.2
チェック無：SSL2.0、SSL3.0
（図 6.5.2-2 参照）

II. 暗号スイート
図 6.5.2-7 仮想 SSL サーバ暗号スイート選択画面 の「選択した暗号スイート」欄に、表 6.5.3.2-1 暗号スイートの設定（推奨セキュリティ型、文字列指定） に示す「グループ化文字列」を「追加」する。

表 6.5.3.2-1 暗号スイートの設定（推奨セキュリティ型、文字列指定）

優先順位	グループ化文字列
-	ECDHE_RSA
	AES

※優先順位は考慮されないため順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.5.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 7 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.5.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA（B）	TLS_RSA_WITH_AES_128_CBC_SHA（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_CBC_SHA（E）	TLS_RSA_WITH_AES_256_CBC_SHA（E）

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：チェック有：TLS1.0、TLS1.1、TLS1.2
チェック無：SSL2.0、SSL3.0
（図 6.5.2-2 参照）

II. 暗号スイート
図 6.5.2-7　仮想 SSL サーバ暗号スイート選択画面　の「選択した暗号スイート」欄に、表 6.5.3.2-3　暗号スイートの設定（推奨セキュリティ型、個別指定） の暗号スイートを「追加」する。

表 6.5.3.2-3　暗号スイートの設定（推奨セキュリティ型、個別指定）

優先順位	暗号スイート
-	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA

※優先順位は考慮されないため順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり､暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.5.3.2-4　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）の「設定ガイドラインの推奨セキュリティ型(一部)」にある 7 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.5.3.2-4　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA（B）	TLS_RSA_WITH_AES_128_CBC_SHA（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_CBC_SHA（E）	TLS_RSA_WITH_AES_256_CBC_SHA（E）

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.5.3.3. セキュリティ例外型

①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
SSL プロトコル：チェック有：SSL3.0、TLS1.0、TLS1.1、TLS1.2
チェック無：SSL2.0
（図 6.5.2-2 参照）

II. 暗号スイート
A) 図 6.5.2-7 仮想 SSL サーバ暗号スイート選択画面の「選択した暗号スイート」欄に、表 6.5.3.3-1 暗号スイートの設定（セキュリティ例外型、文字列指定Ａ） の「グループ化文字列」を「追加」する。

表 6.5.3.3-1 暗号スイートの設定（セキュリティ例外型、文字列指定Ａ）

優先順位	グループ化文字列
-	ECDHE_RSA
	AES
	3DES
	RC4
	－MD5
	－EXPORT

※先頭に「－」が付与されているものは「←－」ボタンで除外設定を行う。
※優先順位は考慮されないため順不同。

B) 図 6.5.2-7 仮想 SSL サーバ暗号スイート選択画面の「選択した暗号スイート」欄に、表 6.5.3.3-2 暗号スイートの設定（セキュリティ例外型、文字列指定Ｂ） の「グループ化文字列」と「暗号スイート」を「追加」する。

表 6.5.3.3-2 暗号スイートの設定（セキュリティ例外型、文字列指定Ｂ）

優先順位	グループ化文字列＋暗号スイート
-	ECDHE_RSA
	AES
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA

※優先順位は考慮されないため順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
A)、B)ともに、セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.5.3.3-3　設定ガイドラインとの差分（セキュリティ例外型） の「設定ガイドラインのセキュリティ例外型(一部)」にある 9 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.5.3.3-3　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA（B）	TLS_RSA_WITH_AES_128_CBC_SHA（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_CBC_SHA（E）	TLS_RSA_WITH_AES_256_CBC_SHA（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：チェック有：SSL3.0、TLS1.0、TLS1.1、TLS1.2
チェック無：SSL2.0
（図 6.5.2-2 参照）

II. 暗号スイート
図 6.5.2-7　仮想 SSL サーバ暗号スイート選択画面の「選択した暗号スイート」欄に、表 6.5.3.3-4　暗号スイートの設定（セキュリティ例外型、個別指定） の暗号スイートを「追加」する。

表 6.5.3.3-4　暗号スイートの設定（セキュリティ例外型、個別指定）

優先順位	暗号スイート
-	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA

※優先順位は考慮されないため順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
A)、B)ともに、セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.5.3.3-5　設定ガイドラインとの差分（セキュリティ例外型、個別指定）の「設定ガイドラインのセキュリティ例外型（一部）」にある 9 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.5.3.3-5　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA（B）	TLS_RSA_WITH_AES_128_CBC_SHA（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	TLS_RSA_WITH_AES_256_CBC_SHA256（E）

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

6.6. NEC InterSec シリーズ

本章では、InterSecVM/LB V3.0 for VMWare について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書のみが設定可能であり、6.6.1 **デフォルトでの暗号設定内容の調査**、および、6.6.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、RSA 証明書を設定した場合について記載する。

6.6.1. デフォルトでの暗号設定内容の調査

表 6.6.1-1　暗号設定内容（デフォルト、RSA 証明書設定時）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	設定不可	ー	ー
tls1.1	設定不可	ー	ー
tls1.0	ON	クライアント	20
sslv3	ON	クライアント	20
sslv2	OFF	ー	0

- NEC InterSecVM/LB V3.0 for VMWare で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				512bit	OFF	OFF	ON	ON	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	OFF	OFF	ON	ON	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	ON	ON	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	OFF	OFF	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	OFF	OFF	ON	ON	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	ON	ON	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	ON	ON	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	ON	ON	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	ON	ON	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	ON	ON	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	―	―	―	―
heartbeat	15	非対応	非対応	非対応	―	―

6.6.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) SSH または vSphere Client で直接（1）「/etc/pound/mkpoundcfg.sh」を編集(図 6.6.2-1　プロトコルバージョン指定画面-1 参照)し、(2)「Ciphers」プロパティを追加し、禁止したいプロトコルを指定する(図 6.6.2-2　プロトコルバージョン指定画面-2 参照)。

例：Ciphers “ XXXX:XXXX:!SSLv2:!SSLv3:XXXX:XXXX:XXXXX”

※Ciphers 属性で SSLv3 を無効化すると TLS1.0 も無効になる。

※Ciphers 属性に TLSv1.0-SSLv3 と指定しても TLS1.0 と SSLv3 が有効になる。

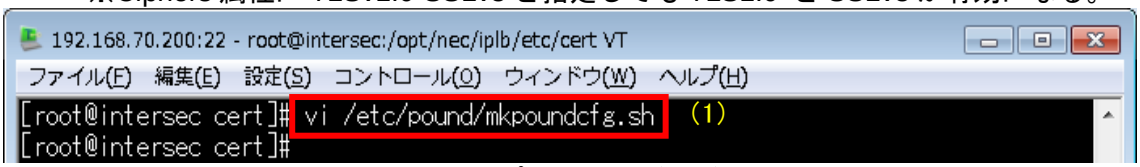

図 6.6.2-1　プロトコルバージョン指定画面-1

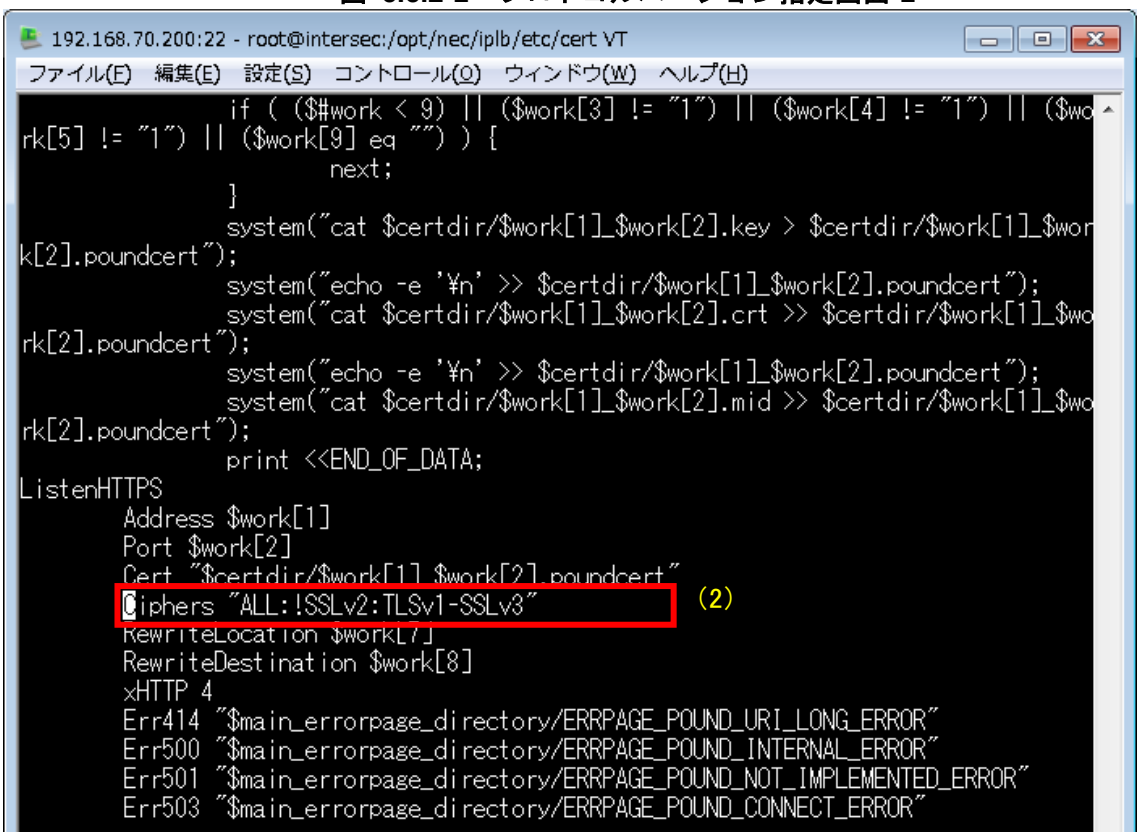

図 6.6.2-2　プロトコルバージョン指定画面-2

B) 設定変更後、ブラウザで「SSL アクセラレータ for Web サーバの状態」画面を表示し、(3)「再起動」ボタンを押下する。

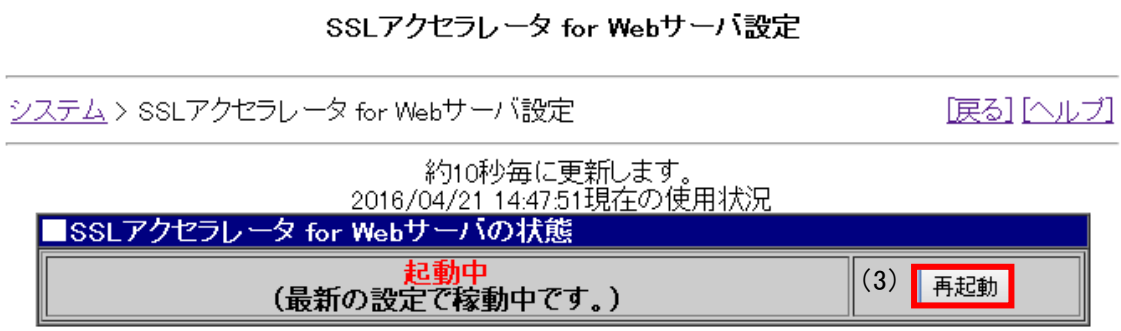

図 6.6.2-3　SSL アクセラレータ for Web サーバの状態画面（プロトコル設定）

II.　暗号スイートの設定

A)　6.6.2.I.A)と同様、SSH または vSphere Client で直接（1）「/etc/pound/mkpoundcfg.sh」を編集(図 6.6.2-4　暗号スイート設定画面-1 参照)し、（2）「Ciphers」プロパティを追加し、Apache の Ciphers と同様に暗号スイートを指定する(図 6.6.2-5　暗号スイート設定画面-2 参照)。

例：Ciphers　“ ALL:!SSLv2:+HIGH:+MEDIUM”

※Ciphers 属性で SSLv3 を無効化すると TLS1.0 も無効になる。

※Ciphers 属性に TLSv1.0-SSLv3 と指定しても TLS1.0 と SSLv3 が有効になる。

※証明書の暗号によって設定できる暗号スイートが異なる。

※ECDSA 証明書は設定できない（SSL アクセラレータ機能が起動しなくなる）。

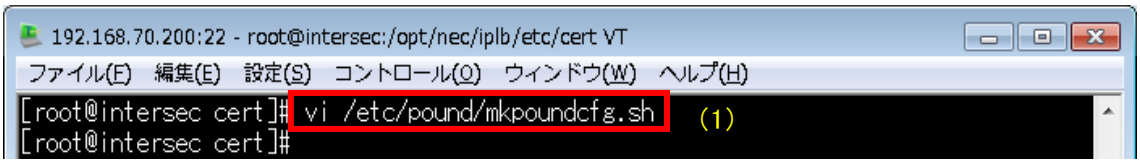

図 6.6.2-4　暗号スイート設定画面-1

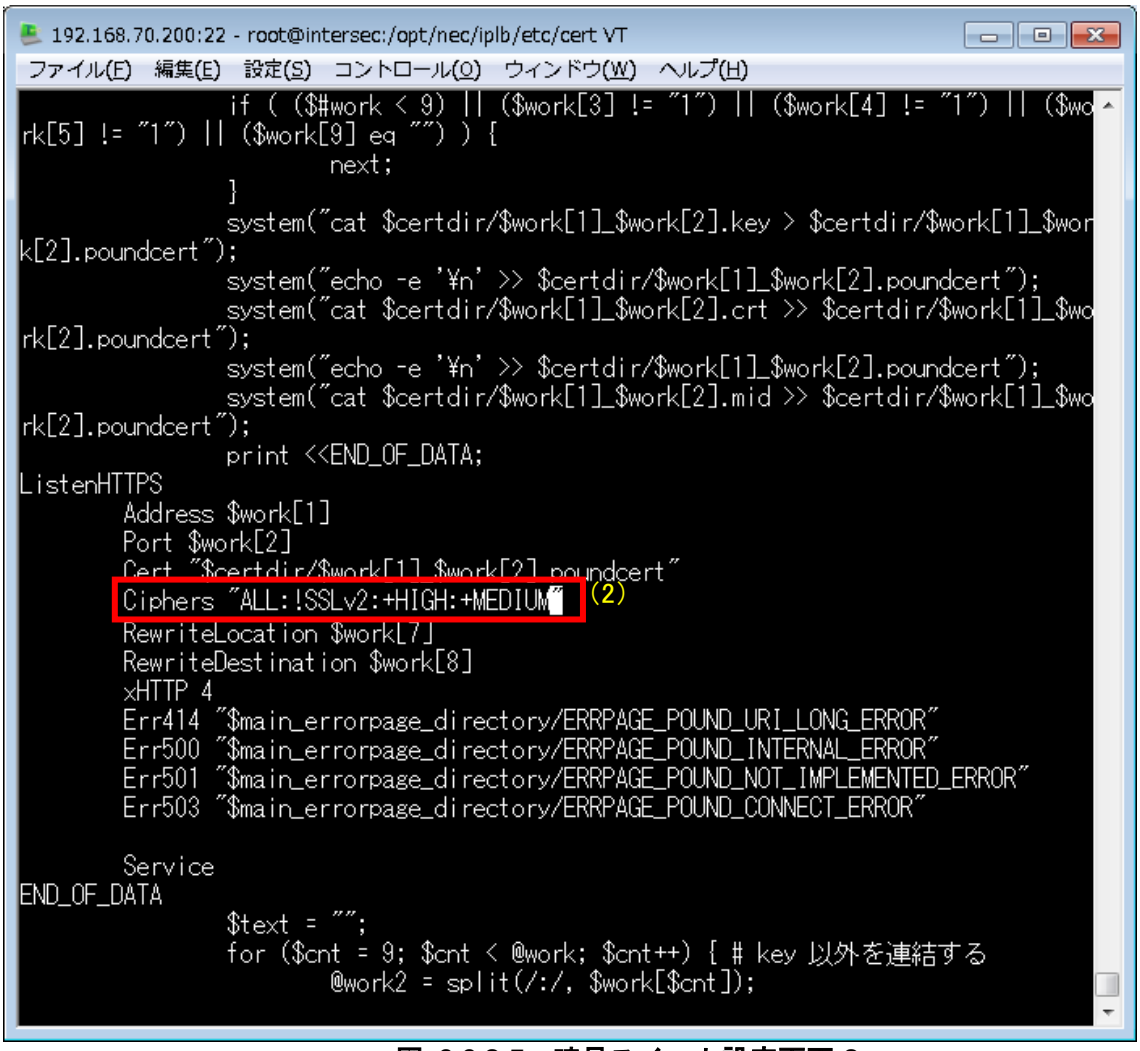

図 6.6.2-5 暗号スイート設定画面-2

B) 設定変更後、ブラウザで「SSL アクセラレータ for Web サーバの状態」画面を表示し、(3)「再起動」ボタンを押下する。

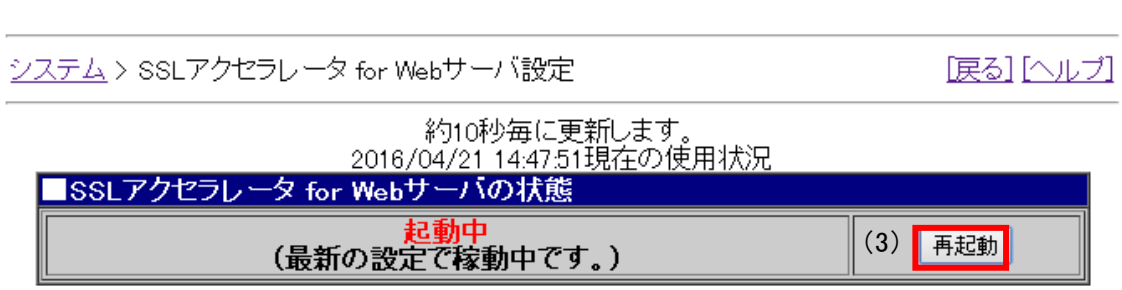

図 6.6.2-6 SSL アクセラレータ for Web サーバの状態画面（暗号スイート）

III. DH/DHE、ECDH/ECDHE の鍵長の設定

設定方法なし。

DH/DHE の鍵長は、1024bit または 512bit が使用される。

※以下の EXPORT 暗号を含む暗号スイートの場合、512bit となる。

・TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

・TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

・TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定方法なし。

6.6.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.6.3.1. 高セキュリティ型

高セキュリティ型の暗号スイートが使用できないため、設定ガイドラインの高セキュリティ型に設定することはできない。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
高セキュリティ型に含まれる 12 個の暗号スイートが使用できない。

② ①の設定と設定ガイドラインの設定内容との差分
高セキュリティ型に含まれる 12 個の暗号スイートがすべて使用できない。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）
高セキュリティ型に含まれる 12 個の暗号スイートがすべて使用できない。

④ ③の設定と設定ガイドラインの設定内容との差分
高セキュリティ型に含まれる 12 個の暗号スイートがすべて使用できない。

6.6.3.2. 推奨セキュリティ型

SSLv3 を無効にすることができないため、設定ガイドラインの推奨セキュリティ型に設定することはできない。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
6.6.2.I.A「/etc/pound/mkpoundcfg.sh」に「Ciphers」プロパティを追加し「:!SSLv2」を記述する。
※!SSLv3 を記述すると TLSv1.0 も無効になるため、!SSLv3 は記述しない。

II. 暗号スイート
6.6.2.II.A「/etc/pound/mkpoundcfg.sh」の「Ciphers」プロパティに、以下を一行で記述する。
RSA+AES:RSA+CAMELLIA:DH+AES:DH+CAMELLIA:!ADH

※プロトコルバージョンと合わせて、以下のように記述する。
“:!SSLv2: RSA+AES:RSA+CAMELLIA:DH+AES:DH+CAMELLIA:!ADH”

III. DH/DHE 、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は 1024bit である。

IV. サーバクライアントの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLS1.2、TLS1.1 が無効である。
SSLv3 が有効である。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.6.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）　の「設定ガイドラインの推奨セキュリティ型(一部)」にある 8 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.6.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	各暗号スイートを設定
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に指定する方法）

I. プロトコルバージョン
6.6.2.I.A「/etc/pound/mkpoundcfg.sh」に「Ciphers」プロパティを追加し「:!SSLv2」を記述する。
※!SSLv3 を記述すると TLSv1.0 も無効になるため、!SSLv3 は記述しない。

II. 暗号スイート
6.6.2.II.A「/etc/pound/mkpoundcfg.sh」の「Ciphers」プロパティに、以下を一行で記載する。
DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-CAMELLIA256-SHA:AES128-SHA:AES256-SHA:CAMELLIA128-SHA:CAMELLIA256-SHA

※プロトコルバージョンと合わせると以下のように記述することになる。
"!SSLv2:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-CAMELLIA256-SHA:AES128-SHA:AES256-SHA:CAMELLIA128-SHA:CAMELLIA256-SHA"

III. DH/DHE 、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は 1024bit である。

IV. サーバクライアントの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため

設定できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLS1.2、TLS1.1 が無効である。
SSLv3 が有効となる。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.6.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型、個別指定） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 8 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.6.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	各暗号スイートを設定
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.6.3.3. セキュリティ例外型

①暗号スイートを具体的に設定しない方法、および、③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

I. プロトコルバージョン
6.6.2.I.A の「/etc/pound/mkpoundcfg.sh」に「Ciphers」プロパティを追加し「:!SSLv2」を記述する。

II. 暗号スイート
6.6.2.II.A の「/etc/pound/mkpoundcfg.sh」の「Ciphers」プロパティに、以下を一行で記述する。
RSA+AES:RSA+CAMELLIA:DH+AES:DH+CAMELLIA:RSA+3DES:DH+3DES:RC4-SHA:!ADH:!MD5

※プロトコルバージョンと合わせると以下のように記述することになる。
“:!SSLv2:RSA+AES:RSA+CAMELLIA:DH+AES:DH+CAMELLIA:RSA+3DES:DH+3DES:RC4-SHA:!ADH:!MD5“

III. DH/DHE 、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は 1024bit である。

IV. サーバクライアントの優先順位の設定
設定できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.2、TLS1.1 が無効である。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.6.3.3-1　設定ガイドラインとの差分（例外セキュリティ型）の 「設定ガイドラインのセキュリティ例外型（一部）」にある 11 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.6.3.3-1　設定ガイドラインとの差分（例外セキュリティ型）

グループ	設定ガイドラインの例外セキュリティ型（一部）	各暗号スイートを設定
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (H)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
6.6.2.I.A の「/etc/pound/mkpoundcfg.sh」に「Ciphers」プロパティを追加し「:!SSLv2」を記述する。

II. 暗号スイート
6.6.2.II.A「/etc/pound/mkpoundcfg.sh」の「Ciphers」プロパティに、以下を一行で記載する。
DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-CAMELLIA256-SHA:AES128-SHA:AES256-SHA:CAMELLIA128-SHA:CAMELLIA256-SHA:RC4-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA

※プロトコルバージョンと合わせると以下のように記述することになる。
"!SSLv2:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-CAMELLIA128-SHA:DHE-RSA-CAMELLIA256-SHA:AES128-SHA:AES256-SHA:CAMELLIA128-SHA:CAMELLIA256-SHA:RC4-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA"

III. DH/DHE 、ECDH/ECDHE の鍵長
設定方法なし。
DHE の鍵長は 1024bit である。

IV. サーバクライアントの優先順位の設定
設定できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.2、TLS1.1 が無効である。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.6.3.3-2　設定ガイドラインとの差分（セキュリティ例外型、個別指定） の「設定ガイドラインのセキュリティ例外型（一部）」にある 11 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため優先順位は考慮されない。

表 6.6.3.3-2　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインのセキュリティ例外型（一部）	各暗号スイートを設定
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)

グループ	設定ガイドラインのセキュリティ例外型（一部）	各暗号スイートを設定
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (H)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

6.7. Array Networks APV シリーズ

本章では、APV 2600 について調査した結果を示す。

サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能であり、RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なる。RSA 証明書と ECDSA 証明書の両方を設定することができないため、6.7.1 **デフォルトでの暗号設定内容の調査**、および、6.7.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、 (1) RSA 証明書設定時、(2) ECDSA 証明書設定時に分けて記載する。

6.7.1. デフォルトでの暗号設定内容の調査

(1) RSA 証明書設定時

表 6.7.1-1　暗号設定内容（デフォルト、RSA 証明書設定時）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	13
tls1.1	設定不可	ー	ー
tls1.0	ON	サーバ	7
sslv3	OFF	ー	0
sslv2	設定不可	ー	ー

- Array Networks APV 2600 で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:8	OFF	ON:6	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:9	OFF	ON:7	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:10	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:11	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:12	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:13	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:1	OFF	ON:1	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:2	OFF	ON:2	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:3	OFF	ON:3	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:4	OFF	ON:4	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:5	OFF	ON:5	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:7	OFF	OFF	OFF	OFF

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

(2) ECDSA 証明書設定時

表 6.7.1-2　暗号設定内容（デフォルト、ECDSA 証明書設定時）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	6
tls1.1	設定不可	ー	ー
tls1.0	ON	サーバ	2
sslv3	OFF	ー	0
sslv2	設定不可	ー	ー

- Array Networks APV 2600 で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON：1	OFF	ON：1	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON：2	OFF	ON：2	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON：3	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON：4	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON：5	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON：6	OFF	OFF	OFF	OFF

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.7.2. 暗号設定方法の調査

I.　プロトコルバージョンの指定

A)　ブラウザで管理画面にログインし、(1)SLBー(2)SSL 設定ー(3)SSL 仮想リストー(4)変更したい SSL ホスト(例：test_ws_ssl_v)をクリックする。

図 6.7.2-1　SSL 仮想ホスト画面-1

B)　(5)「詳細オプション」タブをクリックし、(6)SSL プロトコルバージョンのボタンをクリックし、(7)プルダウンメニューにある有効にしたいプロトコルバージョンにチェックを入れる。変更が完了したら(8)変更の保存ボタンを押下する。

図 6.7.2-2　SSL プロトコルバージョン設定画面

II.　暗号スイートの設定

A)　ブラウザで管理画面にログインし、(1)SLB－(2)SSL 設定－(3)SSL 仮想リスト－(4)暗号スイートを設定したい SSL ホスト(例：test_ws_ssl_v)をクリックする。

図 6.7.2-3　SSL 仮想ホスト画面-2

B)　(5)「詳細オプション」タブをクリックし、(6)SSL サイファースイート欄に有効にしたい順で記載する。設定が完了したら(7)変更の保存ボタンを押下する。

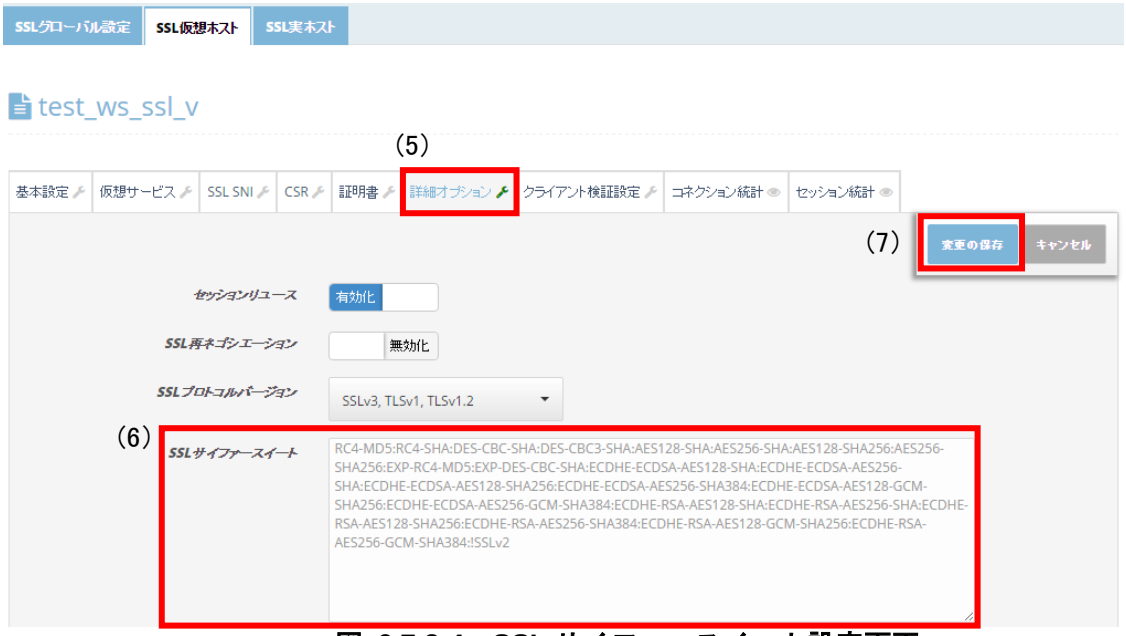

図 6.7.2-4　SSL サイファースイート設定画面

III. DH/DHE、ECDH/ECDHE の鍵長の設定
設定方法なし。
DH/DHE： DH/DHE が含まれる暗号スイートが使用できない。
ECDH/ECDHE：既定で secp256r1 である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
6.7.2.II.B の手順にて優先順位を上位のものにしたい暗号スイートから SSL サイファースイート欄へ記載する。

VI. Extension の設定
設定方法なし。

6.7.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.7.3.1. 高セキュリティ型

(1) RSA 証明書設定時

③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

I. プロトコルバージョン

tls1.2、tls1.0 が有効である。

※6.7.1 (1)RSA 証明書設定時 表 6.7.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）の CipherSuite 選択優先権 のとおり。

II. 暗号スイート

6.7.1 (1)RSA 証明書設定時 表 6.7.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）の Array Networks APV 2600 で使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDH/ECDHE：secp256r1

IV. サーバクライアントの優先順位の設定

既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定

6.7.1 (1)RSA 証明書設定時 表 6.7.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）Array Networks APV 2600 で使用可能な暗号スイート の優先順位とおり。

VI. Extension の設定

6.7.1 (1)RSA 証明書設定時 表 6.7.1-1 暗号設定内容（デフォルト、RSA 証明書設定時）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

TLSv1.0 が有効である。

II. 暗号スイート

差分あり。

高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.7.3.1-1 設定ガイドラインとの差分（高セキュリティ型、RSA 証明書設定時） の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 11 個の暗号スイートが使用可能である。優先順位は表 6.7.3.1-1 設定ガイドラインとの差分（高セキュリティ型、RSA 証明書設定時）のとおりである。

表 6.7.3.1-1　設定ガイドラインとの差分（高セキュリティ型、RSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型(一部)	優先順位	暗号スイート設定結果
α	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α 追加)	13	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α 追加)
β	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β 追加)	12	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β 追加)
-	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	1	TLS_RSA_WITH_RC4_128_MD5
		2	TLS_RSA_WITH_RC4_128_SHA
		3	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		4	TLS_RSA_WITH_AES_128_CBC_SHA
		5	TLS_RSA_WITH_AES_256_CBC_SHA
		6	TLS_RSA_WITH_AES_128_CBC_SHA256
		7	TLS_RSA_WITH_AES_256_CBC_SHA256
		8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
		9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLSv1.2 をチェックし、TLS1.0、SSLv3 のチェックを外す。　（図 6.7.2-2 参照）

II. 暗号スイート
図 6.7.2-4　SSL サイファースイート設定画面 の SSL サイファースイート欄に、以下の文字列を設定する。
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE：既定で secp256r1 である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.7.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定、RSA 証明書設定時） の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。使用可能な 2 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.7.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型(一部)	優先順位	暗号スイート設定結果
α	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α 追加)	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α 追加)
β	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β 追加)	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β 追加)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし

(2)　ECDSA 証明書設定時
③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
暗号スイートを具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

I. プロトコルバージョン
TLSv1.2、TLSv1.0 が有効である。
※6.7.1 (2)ECDSA 証明書設定時 表 6.7.1-2　暗号設定内容（デフォルト、ECDSA 証明書設定時）の CipherSuite 選択優先権 のとおり。

II. 暗号スイート
6.7.1 (2)ECDSA 証明書設定時 表 6.7.1-2　暗号設定内容（デフォルト、ECDSA 証明書設定時）の Array Networks APV 2600 で使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE：secp256r1

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。
※6.7.1 (2) ECDSA 証明書設定時 表 6.7.1-2　暗号設定内容（デフォルト、ECDSA 証明書設定時）の CipherSuite 選択優先権 のとおり。

V. 暗号スイートの優先順位の設定
6.7.1 (2)ECDSA 証明書設定時 表 6.7.1-2　暗号設定内容（デフォルト、ECDSA 証明書設定時）の Array Networks APV 2600 で使用可能な暗号スイート の優先順位のとおり。

VI. Extension の設定
6.7.1 (2) ECDSA 証明書設定時 表 6.7.1-2　暗号設定内容（デフォルト、ECDSA 証明書設定時）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLSv1.0 が有効である。

II. 暗号スイート
差分あり。
高セキュリティ型に含まれる暗号スイート 12 個のうち､表 6.7.3.1-3　設定ガイドラインとの差分（高セキュリティ型、ECDSA 証明書設定時） の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 4 個の暗号スイートが使用可能である。暗号スイートの優先順位は、表 6.7.3.1-3　設定ガイドラインとの差分（高セキュリティ型、ECDSA 証明書設定時） のとおりである。

表 6.7.3.1-3　設定ガイドラインとの差分（高セキュリティ型、ECDSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型(一部)	優先順位	暗号スイート設定結果
α	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α 追加)	6	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α 追加)
β	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β 追加)
-	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
		2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
		3	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
		4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLSv1.2 をチェックし、TLS1.0、SSLv3 のチェックを外す。　（図 6.7.2-2 参照）

II. 暗号スイート
図 6.7.2-4　SSL サイファースイート設定画面の SSL サイファースイート欄に、以下の文字列を設定する。
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE：既定で secp256r1 である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.7.3.1-4　設定ガイドラインとの差分（高セキュリティ型、個別指定、ECDSA 証明書設定時）の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。使用可能な 2 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.7.3.1-4　設定ガイドラインとの差分（高セキュリティ型、個別指定、ECDSA 証明書設定時）

グループ	設定ガイドラインの高セキュリティ型(一部)	優先順位	暗号スイート設定結果
α	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α 追加)
β	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)	2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.7.3.2. 推奨セキュリティ型

(1) RSA 証明書設定時
③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.7.3.1 高セキュリティ型と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLSv1.1 が無効である。

II. 暗号スイート
差分あり。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.7.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型、RSA 証明書設定時） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 10 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 3 個の暗号スイートが使用可能である。暗号スイートの優先順位は、表 6.7.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型、RSA 証明書設定時）のとおりである。

表 6.7.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型、RSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	3	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	4	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	5	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	6	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	8	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	9	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	10	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	11	TLS_RSA_WITH_RC4_128_MD5
		12	TLS_RSA_WITH_RC4_128_SHA
		13	TLS_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLSv1.2、TLSv1.0 をチェックし、SSLv3 のチェックを外す。　（図 6.7.2-2 参照）

II. 暗号スイート
図 6.7.2-4　SSL サイファースイート設定画面 の SSL サイファースイート欄に、以下の文字列を設定する。
ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA:AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA:AES256-SHA256

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE：既定で secp256r1 である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

TLSv1.1 が無効である。

II. 暗号スイート

差分なし。

推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.7.3.2-2 設定ガイドラインとの差分（推奨セキュリティ型、個別指定、RSA 証明書設定時）の「設定ガイドラインの推奨セキュリティ型(一部)」にある 10 個の暗号スイートの使用が可能である。使用可能な 10 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティ型の順位と同じである。

表 6.7.3.2-2 設定ガイドラインとの差分（推奨セキュリティ型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	3	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	4	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	5	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	6	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	8	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	9	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	10	TLS_RSA_WITH_AES_256_CBC_SHA256(E)

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

(2) ECDSA 証明書設定時

デフォルトの設定で、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.7.3.1 高セキュリティ型 (2)ECDSA 証明書設定時と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

TLSv1.1 が無効である。

II. 暗号スイート

差分なし。

推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.7.3.2-3 設定ガイドラインと

の差分（推奨セキュリティ型、ECDSA 証明書設定時）の「設定ガイドラインの推奨セキュリティ型(一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は表 6.7.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、ECDSA 証明書設定時）表 6.7.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、ECDSA 証明書設定時） のとおりである。

表 6.7.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、ECDSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
D	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	6	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具田的に設定する方法）

I. プロトコルバージョン
SSLv3 のチェックを外す。　（図 6.7.2-2 参照）

II. 暗号スイート
図 6.7.2-4　SSL サイファースイート設定画面 の SSL サイファースイート欄に、以下の文字列を設定する。
ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE：既定で secp256r1 である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLSv1.1 が無効である。

II. 暗号スイート

差分なし。

推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.7.3.2-4　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、ECDSA 証明書設定時） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティの順位と同じである。

表 6.7.3.2-4　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、ECDSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
D	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	6	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

6.7.3.3. セキュリティ例外型

(1)RSA 証明書設定時

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.7.3.1 高セキュリティ型 (1)RSA 証明書設定時と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

TLSv1.1、SSLv3 が無効である。

II. 暗号スイート

差分あり。

セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.7.3.3-1　設定ガイドラインとの差分（セキュリティ例外型、RSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型(一部)」にある 12 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 1 個の暗号スイートが使用可能である。暗号スイートの優先順位は、表 6.7.3.3-1　設定ガイドラインとの差分（セキュリティ例外型、RSA 証明書設定時） のとおりである。

表 6.7.3.3-1　設定ガイドラインとの差分（セキュリティ例外型、RSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	12	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	4	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	6	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	13	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	5	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	7	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	2	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	3	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）
－	設定ガイドラインのセキュリティ例外型に該当しない暗号スイート	1	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLS1.2、TLS1、SSLv3 のチェックを入れる。　（図 6.7.2-2 参照）

II. 暗号スイート
図 6.7.2-4　SSL サイファースイート設定画面 の SSL サイファースイート欄に、以下の文字列を設定する。
ECDHE-RSA-AES128-SHA: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-GCM-SHA256: AES128-SHA: AES128-SHA256:ECDHE-RSA-AES256-SHA: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-GCM-SHA384: AES256-SHA: AES256-SHA256: RC4-SHA: DES-CBC3-SHA

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE：既定で secp256r1 である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.1 が無効である。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち､表 6.7.3.3-2 設定ガイドラインとの差分（セキュリティ例外型、個別指定、RSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型(一部)」にある 12 個の暗号スイートの使用が可能である。使用可能な 12 個の暗号スイートの優先順位は、設定ガイドラインのセキュリティ例外型の順位と同じである。

表 6.7.3.3-2 設定ガイドラインとの差分（セキュリティ例外型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	3	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	4	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	5	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	6	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	8	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	9	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	10	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
G	TLS_RSA_WITH_RC4_128_SHA(G)	11	TLS_RSA_WITH_RC4_128_SHA(G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)	12	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

(2) ECDSA 証明書設定時
③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.7.3.1 高セキュリティ型 (2)ECDSA 証明書設定時と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLSv1.1、SSLv3 が無効である。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.7.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、ECDSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型(一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、表 6.7.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、ECDSA 証明書設定時）のとおりである。

表 6.7.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、ECDSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
D	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	6	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLS1.2、TLS1、SSLv3 のチェックを入れる。　（図 6.7.2-2 参照）

II. 暗号スイート
図 6.7.2-4　SSL サイファースイート設定画面 の SSL サイファースイート欄に、以下の文字列を設定する。
ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長
ECDH/ECDHE：既定で secp256r1 である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した内容による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

TLS1.1 が無効である。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.7.3.3-4　設定ガイドラインとの差分（セキュリティ例外型、個別指定、ECDSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型(一部)」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、設定ガイドラインのセキュリティ例外型の順位と同じである。

表 6.7.3.3-4　設定ガイドラインとの差分（セキュリティ例外型、個別指定、ECDSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型(一部)	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	2	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
D	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	4	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	6	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.8. 日立製作所 Hitachi Load Balancer EL130

本章では、Hitachi Load Balancer EL130 について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書のみが設定可能であり、6.8.1 **デフォルトでの暗号設定内容の調査**、および、6.8.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、RSA 証明書を設定した場合について記載する。

6.8.1. デフォルトでの暗号設定内容の調査

表 6.8.1-1 暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	7
tls1.1	設定不可	ー	ー
tls1.0	ON	クライアント	6
sslv3	ON	クライアント	6
sslv2	設定不可	ー	ー

- 日立製作所 Hitachi Load Balancer EL130 で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON	OFF	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	OFF	ON	ON	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	OFF	ON	ON	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	OFF	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	OFF	ON	ON	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.8.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで管理画面にログインし、(1) コンフィグ ー (2) SLB ー (3) テンプレート ー (4) SSL ー (5) 作成してあるクライアント SSL テンプレート（例：test_ssl_rsa）をクリックする。

図 6.8.2-1 クライアント SSL リスト画面

B) SSLv3 を無効にする場合は、クライアント SSL 内の（6）「SSLv3 のクライアントを拒否する」の（7）有効にチェックを入れる。

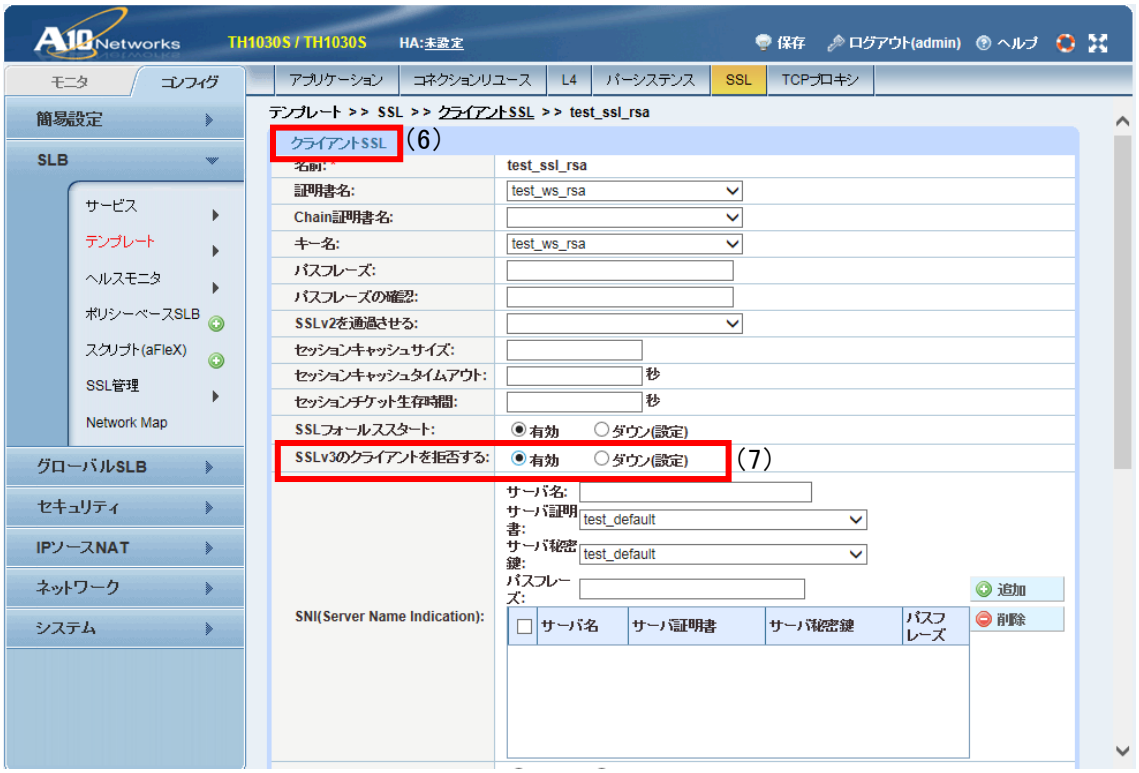

図 6.8.2-2　クライアント SSL 設定画面-1

C)　設定が完了したら（8）「OK」ボタンを押下する。

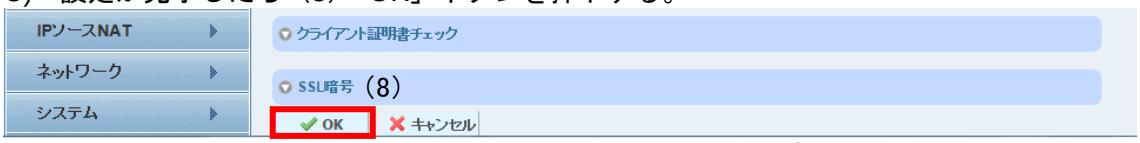

図 6.8.2-3　クライアント SSL 設定画面-2

D)　画面上の電球のアイコンが点滅するので、（9）「保存」をクリックして設定を保存する。

図 6.8.2-4　設定保存画面

II.　暗号スイートの設定

A)　ブラウザで管理画面にログインし、(1) コンフィグ－ (2) SLB－ (3) テンプレート－ (4) SSL－ (5) SSL 暗号をクリックする。

図 6.8.2-5　SSL 暗号追加メニュー画面

B)　SSL 暗号リスト画面が表示されたら (6)「追加」ボタンを押下する。

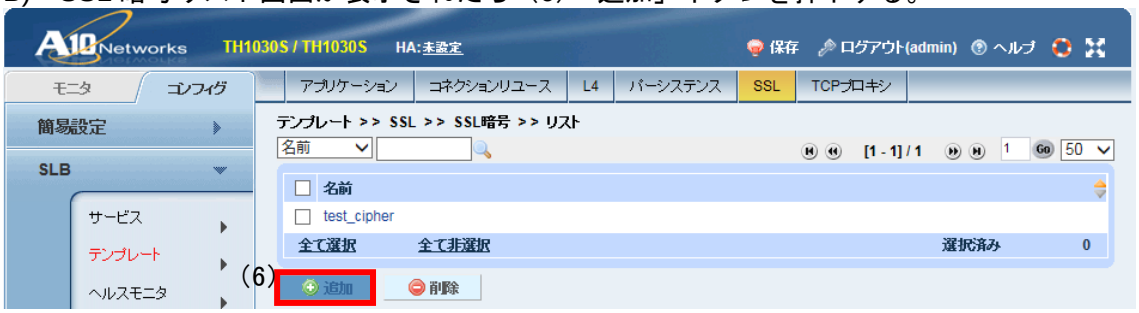

図 6.8.2-6　SSL 暗号リスト画面

C)　SSL 暗号新規作成画面が表示されたら (7) 名前を入力し、追加したい (8) SSL 暗号をドロップダウンリストから選択し、(9)「プライオリティー」欄で優先度を入力してから (10)「追加」ボタンを押下する。
更に追加したい SSL 暗号が有る場合は (8) ～ (10) を繰り返す。
追加し終わったら (11)「OK」ボタンを押下する。
※プライオリティーの値が大きいものが優先される。
※ECDSA 証明書は設定が可能だが、有効な暗号スイートが無いため利用できない。

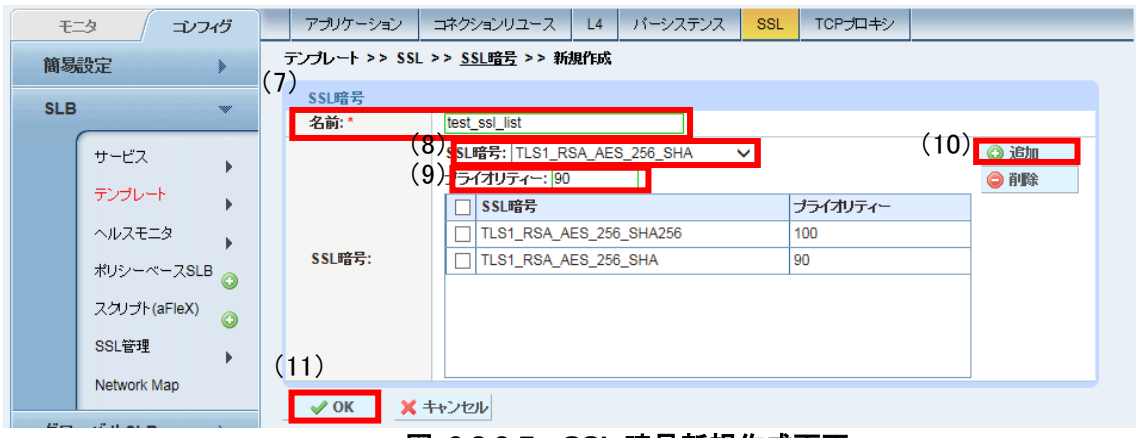

図 6.8.2-7　SSL 暗号新規作成画面

D) 6.8.1.I.B で設定したクライアント SSL を開き、(12)「SSL 暗号テンプレート」内の（13）クラスで「SSL サイファーテンプレート」にチェックを入れ、(14) SSL サイファーテンプレートで 6.8.1.II.C で作成した SSL 暗号（例 : test_ssl_list）を選択する。あるいは、クラスで「SSL 暗号」を選択し、(15) SSL 暗号で暗号スイートを個別に選択する。
設定が完了したら（16）「OK」ボタンを押下する。

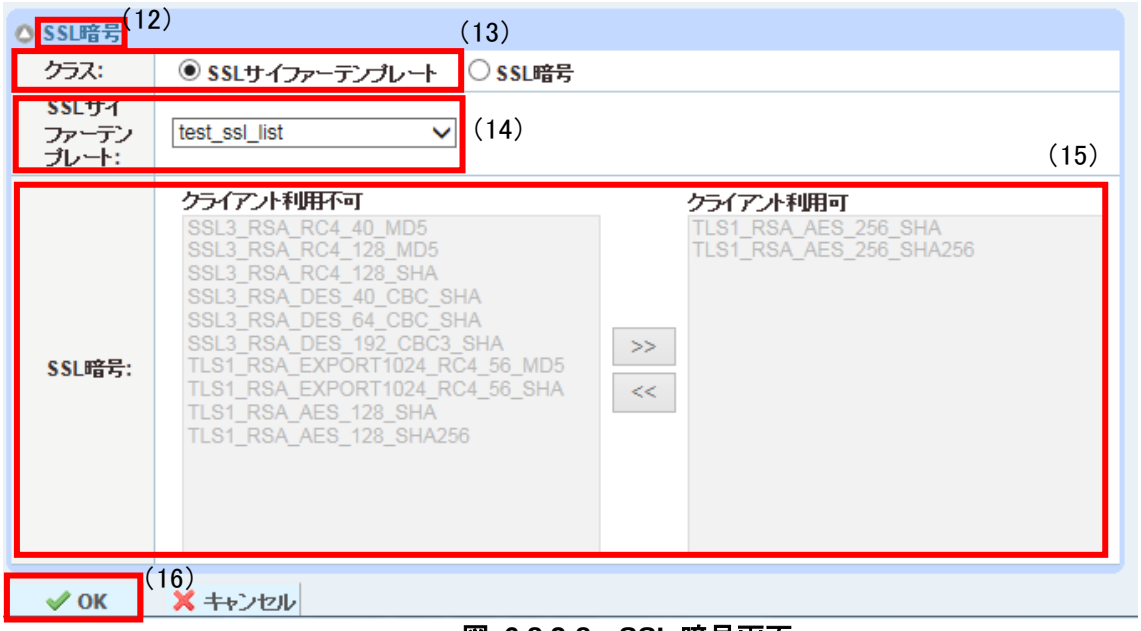

図 6.8.2-8 SSL 暗号画面

E) クライアント SSL リスト画面に戻るので、(17) 保存ボタンを押下する。

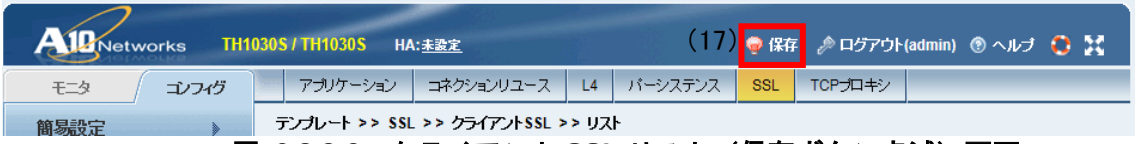

図 6.8.2-9 クライアント SSL リスト（保存ボタン点滅）画面

III. DH/DHE、ECDH/ECDHE の鍵長の設定
設定方法なし。

IV. サーバクライアントの優先順位の設定
6.8.2.II.D 図 6.8.2-8 SSL 暗号画面 ですべての暗号スイートを選択した場合は、クライアント優先になる。既定は、すべての暗号スイートを 6.8.2.II.D 図 6.8.2-8 SSL 暗号画面 で選択した状態であり、クライアント優先である。6.8.2.II.D の手順にて SSL サイファーテンプレートを設定した場合、6.8.2.II.D 図 6.8.2-8 SSL 暗号画面 で暗号スイートを一部選択した場合は、サーバ優先となる。

V. 暗号スイートの優先順位の設定
6.8.2.II.D の手順にて SSL サイファーテンプレートを設定した場合にのみ、リストに設定された暗号スイートのプライオリティーの値が高いものから優先順位が設定される。

VI. Extension の設定
設定方法なし。

6.8.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.8.3.1. 高セキュリティ型

設定ガイドラインの高セキュリティ型に設定することはできない。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

高セキュリティ型の暗号スイートが使用できない。

② ①の設定と設定ガイドラインの設定内容との差分

高セキュリティ型に含まれる 12 個の暗号スイートがすべて使用できない。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

高セキュリティ型の暗号スイートが使用できない。

④ ③の設定と設定ガイドラインの設定内容との差分

高セキュリティ型に含まれる 12 個の暗号スイートがすべて使用できない。

6.8.3.2. 推奨セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

I. プロトコルバージョン

tls1.2、tls1.0 が有効である。

※表 6.8.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

II. 暗号スイート

表 6.8.1-1　暗号設定内容（デフォルト）日立製作所 Hitachi Load Balancer EL130 で使用可能な暗号スイートで使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE、ECDH/ECDHE を含む暗号スイートがないためなし。

IV. サーバクライアントの優先順位の設定

クライアント優先である。

※表 6.8.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

V. 暗号スイートの優先順位の設定

クライアント優先であるため、優先順位はなし。

VI. Extension の設定

表 6.8.1-1　暗号設定内容（デフォルト）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

TLS1.1 が無効である。

SSLv3 が有効である。

II. 暗号スイート

差分あり。

推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.8.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型、RSA 証明書設定時） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 4 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 3 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.8.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型、RSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
－	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5
		TLS_RSA_WITH_RC4_128_SHA
		TLS_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE、ECDH/ECDHE を含む暗号スイートが有効でないため、比較できない。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン

SSLv3 のクライアントを拒否する: 有効　（図 6.8.2-2 参照）

II. 暗号スイート

6.8.2.II.D の手順で暗号スイートを設定する際にプライオリティーの値を以下の様に設定する。

表 6.8.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定、RSA 証明書設定時）

プライオリティー	暗号スイート
100	TLS1_RSA_AES_128_SHA
100	TLS1_RSA_AES_128_SHA256
90	TLS1_DHE_RSA_AES_256_SHA
90	TLS1_DHE_RSA_AES_256_SHA256

※「プライオリティー」は 1～100 の範囲で指定。100 が最も優先度が高い。

III. DH/DHE、ECDH/ECDHE の鍵長

設定できない。

IV. サーバクライアントの優先順位の設定
6.8.2.II.D 図 6.8.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.1 が無効である。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.8.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、RSA 証明書設定時） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 4 個の暗号スイートの使用が可能である。使用可能な 4 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティ型の順位と同じである。

表 6.8.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	1	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	2	TLS_RSA_WITH_AES_128_CBC_SHA (B)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	3	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	4	TLS_RSA_WITH_AES_256_CBC_SHA (E)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE、ECDH/ECDHE を含む暗号スイートが有効でないため、比較できない。

6.8.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

①　プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.8.3.2 推奨セキュリティ型と同じである。

②　①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.1 が無効である。

II. 暗号スイート
差分あり。

セキュリティ例外型に含まれる暗号スイート 67 個のうち､表 6.8.3.3-1　設定ガイドラインとの差分（セキュリティ例外型、RSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型(一部)」にある 6 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 1 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.8.3.3-1　設定ガイドラインとの差分（セキュリティ例外型、RSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE、ECDH/ECDHE を含む暗号スイートが有効でないため、比較できない。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSLv3 のクライアントを拒否する: ダウン（設定）　（図 6.8.2-2 参照）

II. 暗号スイート
6.8.2.II.D の手順で表 6.8.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定、RSA 証明書設定時） の暗号スイートを追加する。

表 6.8.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定、RSA 証明書設定時）

プライオリティー	暗号スイート
100	TLS1_RSA_AES_128_SHA
100	TLS1_RSA_AES_128_SHA256
90	TLS1_RSA_AES_256_SHA
90	TLS1_RSA_AES_256_SHA256
80	SSL3_RSA_RC4_128_SHA
70	SSL3_RSA_DES_192_CBC3_SHA

※「プライオリティー」は 1～100 の範囲で指定。100 が最も優先度が高い。

III. DH/DHE、ECDH/ECDHE の鍵長
設定できない。

IV. サーバクライアントの優先順位の設定
6.8.2.II.D 図 6.8.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.1 が無効である。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.8.3.3-3 設定ガイドラインとの差分（セキュリティ例外型、個別指定、RSA 証明書設定時） の「設定ガイドラインのセキュリティ例外型（一部）」にある 6 個の暗号スイートの使用が可能である。使用可能な 6 個の暗号スイートの優先順位は、設定ガイドラインのセキュリティ例外型の順位と同じである。

表 6.8.3.3-3 設定ガイドラインとの差分（セキュリティ例外型、個別指定、RSA 証明書設定時）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	1	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	2	TLS_RSA_WITH_AES_128_CBC_SHA (B)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	3	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	4	TLS_RSA_WITH_AES_256_CBC_SHA (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	5	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	6	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE、ECDH/ECDHE を含む暗号スイートが有効でないため、比較できない。

6.9. バラクーダネットワークス Barracuda Load Balancer ADC シリーズ

本章では、Barracuda Load Balancer ADC について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能である。RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なり、両方の証明書を設定した場合は、両方の暗号スイートが有効になる。6.9.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、RSA 証明書と ECDSA 証明書の両方を設定した結果について記載する。ただし、デフォルト設定では RSA 証明書のみの設定になっているため、6.9.1 **デフォルトでの暗号設定内容の調査**については、RSA 証明書のみを設定した結果について記載する。

6.9.1. デフォルトでの暗号設定内容の調査

デフォルトでは ECDSA 証明書の設定は無効になっているため、RSA 証明書のみ設定した場合について記載する。

表 6.9.1-1　暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	25
tls1.1	ON	サーバ	13
tls1.0	ON	サーバ	13
sslv3	OFF	ー	0
sslv2	設定不可	ー	ー

- Barracuda Load Balancer ADC で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	2048bit	ON:24	ON:12	ON:12	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	2048bit	ON:17	ON:7	ON:7	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	2048bit	ON:8	ON:2	ON:2	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	2048bit	ON:18	ON:8	ON:8	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	2048bit	ON:16	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	2048bit	ON:7	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	2048bit	ON:9	ON:3	ON:3	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	2048bit	ON:3	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	2048bit	ON:1	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON:23	ON:11	ON:11	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:15	ON:6	ON:6	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:6	ON:1	ON:1	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:14	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:5	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:4	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:2	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	OFF	OFF	OFF	OFF	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:25	ON:13	ON:13	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:21	ON:9	ON:9	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:12	ON:4	ON:4	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:20	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:11	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON:22	ON:10	ON:10	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON:13	ON:5	ON:5	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:19	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:10	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.9.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで Barracuda Load Balancer ADC にログインし、(1) 基本設定ー (2) サービスー (3) 該当のサービスをクリックして (4) サービス設定を表示する。

図 6.9.2-1 プロパティー覧画面

B) (5) SSL Setting の (6) SSL プロトコルで有効にしたいプロトコルバージョンにチェックを入れ、(7) 変更の保存ボタンを押下する。

図 6.9.2-2　プロパティ編集画面（プロトコルバージョン）

II.　暗号スイートの設定

A)　サービス設定項目の（1）証明書欄にある（2）Enable ECDSA Ciphers を（3）「オン」にし、（4）プルダウンメニューから ECDSA 形式の証明書を選択する。
※ECDSA 暗号の有効化でオンを選択し、ECDSA 証明書を選択しないと ECDSA を含む暗号スイートが有効にならない。

図 6.9.2-3　プロパティ編集画面（暗号スイート）-1

B)　（5）SSL Settings の（6）高度なオプションを（7）「表示」し、（8）Enable Perfect Forward Secrecy の（9）「はい」を選択する。

図 6.9.2-4　プロパティ編集画面（暗号スイート）-2

C) 高度なオプション内（10）SSL Ciphers 項目の Use Ciphers にある（11）「選択した暗号」欄に（12）「使用可能な暗号」欄から『優先度を高くしたい暗号スイート順』に（13）「追加」ボタンと（14）「削除」ボタンを使用して設定する。設定が終わったら画面右上の（15）「変更の保存」ボタンを押下する。
※Enable Perfect Forward Secrecy で「はい」を選択しておかないと ECDHE を含む暗号スイートは選択しても有効にならない。
※デフォルトでは以下の暗号スイート以外は全て「選択した暗号」欄に追加されている。
・DHE-RSA-SEED-SHA
・SHEED-SHA
・IDEA-CBC-SHA
・ECDHE-RSA-RC4-SHA
・ECDHE-ECDSA-RC4-SHA
・RC4-SHA
・RC4-MD5
※優先度は「選択した暗号」欄の上から順となるため、一度全て「使用可能な暗号」欄に移動する必要がある。

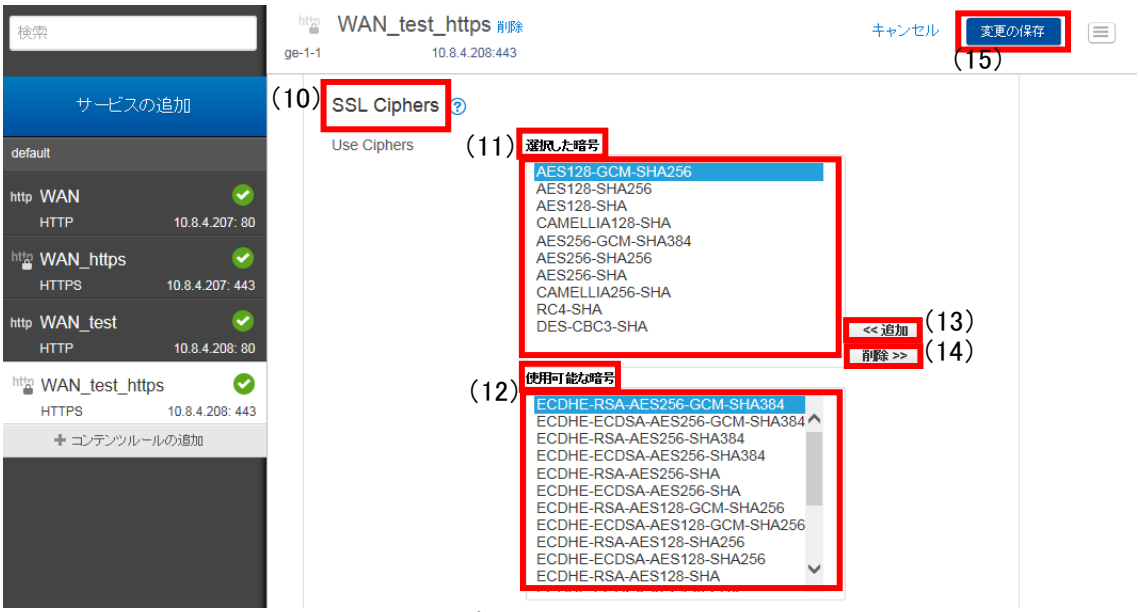

図 6.9.2-5　プロパティ編集画面（暗号スイート）-3

III. DH/DHE、ECDH/ECDHE の鍵長の設定
設定方法なし。
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II 暗号スイートの設定した結果による。

VI. Extension の設定
設定方法なし。

6.9.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.9.3.1. 高セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容の調査結果を以下に示す。

I. プロトコルバージョン
TLS1.2、TLS1.1、TLS1.0 が有効である。
※6.9.1 表 6.9.1-1 暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

II. 暗号スイート
6.9.1 表 6.9.1-1 暗号設定内容（デフォルト）の Barracuda Load Balancer ADC で使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。
※6.9.1 表 6.9.1-1 暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

V. 暗号スイートの優先順位の設定
6.9.1 表 6.9.1-1 暗号設定内容（デフォルト）の Barracuda Load Balancer ADC で使用可能な暗号スイート のとおり。

VI. Extension の設定
6.9.1 表 6.9.1-1 暗号設定内容（デフォルト）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLS1.1、TLS1.0 が有効である。

II. 暗号スイート
差分あり。
高セキュリティ型に含まれる 12 個の暗号スイートのうち､表 6.9.3.1-1 設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型（一部）」にある 4 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 21 個の暗号スイートが使用可能である。優先順位についても表 6.9.3.1-1 設定ガイドラインとの差分（高セキュリティ型） のとおりである。

表 6.9.3.1-1 設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)
–	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
		6	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		7	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
		8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
		9	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
		10	TLS_RSA_WITH_AES_256_GCM_SHA384
		11	TLS_RSA_WITH_AES_256_CBC_SHA256
		12	TLS_RSA_WITH_AES_256_CBC_SHA
		13	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
		14	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		15	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
		16	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
		17	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
		18	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
		19	TLS_RSA_WITH_AES_128_GCM_SHA256
		20	TLS_RSA_WITH_AES_128_CBC_SHA256
		21	TLS_RSA_WITH_AES_128_CBC_SHA
		22	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
		23	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		24	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
		25	TLS_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：チェック有：TLS1.2
チェック無：SSL3.0、TLS1.0、TLS1.1
（図 6.9.2-2 参照）

II. 暗号スイート
6.9.2 II 図 6.9.2-5　プロパティ編集画面（暗号スイート）の「選択した暗号」欄に、表 6.9.3.1-2 暗号スイートの設定（高セキュリティ型、個別指定）の順番で「追加」する。

表 6.9.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定）

優先順位	暗号スイート
1	DHE-RSA-AES256-GCM-SHA384
	ECDHE-ECDSA-AES256-GCM-SHA384
	ECDHE-RSA-AES256-GCM-SHA384
2	DHE-RSA-AES128-GCM-SHA256

優先順位	暗号スイート
	ECDHE-ECDSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-GCM-SHA256

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる 12 個の暗号スイートのうち､表 6.9.3.1-3　設定ガイドラインとの差分（高セキュリティ型、個別指定） の「設定ガイドラインの高セキュリティ型（一部)」にある 6 個の暗号スイートの使用が可能である。優先順位についても表 6.9.3.1-3　設定ガイドラインとの差分（高セキュリティ型、個別指定） のとおりである。

表 6.9.3.1-3　設定ガイドラインとの差分（高セキュリティ型、個別指定）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)	2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(α追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)	3	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	4	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(β追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.9.3.2. 推奨セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容となる。調査結果は**高セキュリティ型**と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分あり。
推奨セキュリティ型に含まれる 64 個の暗号スイートのうち､表 6.9.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型（一部)」にある 22 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 3 個の暗号スイートが使用可能である。

表 6.9.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	17	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	18	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	16	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	15	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	14	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	21	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	20	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	22	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	19	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	7	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	9	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	6	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	12	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	11	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	13	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	10	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	23	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		24	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
		25	TLS_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：チェック有：TLS1.0、TLS1.1、TLS1.2
チェック無：SSL3.0
（図 6.9.2-2 参照）

II. 暗号スイート
図 6.9.2-5 プロパティ編集画面（暗号スイート）の「選択した暗号」欄に、表 6.9.3.2-2 暗号スイートの設定（推奨セキュリティ型、個別指定） の順番で「追加」する。

表 6.9.3.2-2 暗号スイートの設定（推奨セキュリティ型、個別指定）

優先順位	暗号スイート
1	DHE-RSA-AES128-GCM-SHA256
	DHE-RSA-AES128-SHA256
	DHE-RSA-AES128-SHA
	DHE-RSA-CAMELLIA128-SHA
	ECDHE-ECDSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-ECDSA-AES128-SHA256
	ECDHE-RSA-AES128-SHA256
	ECDHE-ECDSA-AES128-SHA
	ECDHE-RSA-AES128-SHA
2	AES128-GCM-SHA256
	AES128-SHA256
	AES128-SHA
	CAMELLIA128-SHA
3	DHE-RSA-AES256-GCM-SHA384
	DHE-RSA-AES256-SHA256
	DHE-RSA-AES256-SHA

優先順位	暗号スイート
	DHE-RSA-CAMELLIA256-SHA
	ECDHE-ECDSA-AES256-GCM-SHA384
	ECDHE-RSA-AES256-GCM-SHA384
	ECDHE-ECDSA-AES256-SHA384
	ECDHE-RSA-AES256-SHA384
	ECDHE-ECDSA-AES256-SHA
	ECDHE-RSA-AES256-SHA
4	AES256-GCM-SHA384
	AES256-SHA256
	AES256-SHA
	CAMELLIA256-SHA

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。
※ECDSA（256bit）の証明書を設定した場合 256bit(secp256r1)が使用される。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる 64 個の暗号スイートのうち､表 6.9.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定） の「設定ガイドラインの推奨セキュリティ型（一部）」にある 28 個の暗号スイートの使用が可能である｡優先順位についても表 6.3.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定、RSA 証明書設定時） のとおりである。

表 6.9.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）	3	TLS_DHE_RSA_WITH_AES_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA（A）	4	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA（A）
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）	2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256（A）
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）	1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（A）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）	9	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）	7	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256（A 追加）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	13	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	12	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）	14	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	11	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）	17	TLS_DHE_RSA_WITH_AES_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）	16	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256（D）
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA（D）	18	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA（D）
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）	15	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（D）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）	23	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	24	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）	21	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	22	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）	19	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	20	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	27	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	26	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	28	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	25	TLS_RSA_WITH_AES_256_GCM_SHA384（E）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.9.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容となる。調査結果は**高セキュリティ型**と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分あり。
セキュリティ例外型に含まれる 67 個の暗号スイートのうち表 6.9.3.3-1　設定ガイドラインとの差分（セキュリティ例外型） の「設定ガイドラインのセキュリティ例外型（一部）」にある 24 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 1 個の暗号スイートが使用可能である。

表 6.9.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	17	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)	18	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	16	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)	15	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)	14	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	21	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	20	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)	22	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	19	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	8	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	7	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)	9	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	6	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	12	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	11	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)	13	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	10	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
H	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (H)	24	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (H)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	25	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)
-	設定ガイドラインのセキュリティ例外型に該当しない暗号スイート	23	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：チェック有：SSL3.0、TLS1.0、TLS1.1、TLS1.2　（図 6.9.2-2 参照）

II. 暗号スイート
図 6.9.2-5　プロパティ編集画面（暗号スイート）の「選択した暗号」欄に、表 6.9.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定） の順番で「追加」する。

表 6.9.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定）

優先順位	暗号スイート
1	DHE-RSA-AES128-GCM-SHA256
	DHE-RSA-AES128-SHA256

優先順位	暗号スイート
	DHE-RSA-AES128-SHA
	DHE-RSA-CAMELLIA128-SHA
	ECDHE-ECDSA-AES128-GCM-SHA256
	ECDHE-RSA-AES128-GCM-SHA256
	ECDHE-ECDSA-AES128-SHA256
	ECDHE-RSA-AES128-SHA256
	ECDHE-ECDSA-AES128-SHA
	ECDHE-RSA-AES128-SHA
2	AES128-GCM-SHA256
	AES128-SHA256
	AES128-SHA
	CAMELLIA128-SHA
3	DHE-RSA-AES256-GCM-SHA384
	DHE-RSA-AES256-SHA256
	DHE-RSA-AES256-SHA
	DHE-RSA-CAMELLIA256-SHA
	ECDHE-ECDSA-AES256-GCM-SHA384
	ECDHE-RSA-AES256-GCM-SHA384
	ECDHE-ECDSA-AES256-SHA384
	ECDHE-RSA-AES256-SHA384
	ECDHE-ECDSA-AES256-SHA
	ECDHE-RSA-AES256-SHA
4	AES256-GCM-SHA384
	AES256-SHA256
	AES256-SHA
	CAMELLIA256-SHA
5	RC4-SHA
6	EDH-RSA-DES-CBC3-SHA
	DES-CBC3-SHA

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。
※ECDSA（256bit）の証明書を設定した場合 256bit(secp256r1)が使用される。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる 67 個の暗号スイートのうち表 6.9.3.3-3 設定ガイドラインとの差分（セキュリティ例外型、個別指定） の「設定ガイドラインのセキュリティ例外型（一部）」にある 31 個の暗号スイートの使用が可能である。優先順位についても表 6.9.3.3-1 設定ガイドラインとの差分（セキュリティ例外型） のとおりである。

表 6.9.3.3-3 設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	3	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(A)	4	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA(A)
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	7	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	9	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
B	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	11	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	12	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA(B)	13	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)	14	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)
D	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	15	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	16	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	17	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(D)	18	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA(D)
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	19	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	20	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	21	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	22	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	23	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	24	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
E	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	25	TLS_RSA_WITH_AES_256_GCM_SHA384(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	26	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_CBC_SHA(E)	27	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)	28	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)
G	TLS_RSA_WITH_RC4_128_SHA(G)	29	TLS_RSA_WITH_RC4_128_SHA(G)
H	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(H)	30	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(H)

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)	31	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.10. バラクーダネットワークス Barracuda WAF シリーズ

本章では、Barracuda WAF について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書と ECDSA 証明書が設定可能である。RSA 証明書を設定した場合と ECDSA 証明書を設定した場合で有効となる暗号スイートが異なり、両方の証明書を設定した場合は、両方の暗号スイートが有効になる。6.10.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、RSA 証明書と ECDSA 証明書の両方を設定した結果について記載する。ただし、デフォルト設定では RSA 証明書のみの設定になっているため、6.10.1 **デフォルトでの暗号設定内容の調査**については、RSA 証明書のみを設定した結果について記載する。

6.10.1. デフォルトでの暗号設定内容の調査

デフォルトでは ECDSA 証明書の設定は無効になっているため、RSA 証明書のみ設定した場合について記載する。

表 6.10.1-1　暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	20
tls1.1	ON	サーバ	13
tls1.0	ON	サーバ	13
sslv3	ON	サーバ	4
sslv2	設定不可	ー	ー

- Barracuda WAF で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256r1	ON:9	ON:10	ON:10	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON:12	ON:12	ON:12	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:13	ON:11	ON:11	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:11	ON:13	ON:13	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:4	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:3	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:2	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:1	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:20	ON:1	ON:1	ON:1	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:10	ON:9	ON:9	ON:4	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	ON:2	ON:2	ON:2	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:16	ON:6	ON:6	ON:3	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:17	ON:5	ON:5	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:14	ON:8	ON:8	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:8	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:7	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON:19	ON:3	ON:3	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON:15	ON:7	ON:7	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	ON:18	ON:4	ON:4	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:5	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	対応	対応	対応	ー	ー

6.10.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで管理画面にログインし、(1) 基本設定ー (2) サービスをクリックしてサービス一覧を表示し、(3) 現在有効なサービスの「Edit」をクリックする。

図 6.10.2-1 サービス一覧画面

B) サービス編集画面の SSL 欄で、(4)「高度な設定を非表示」を選択する。(5) ECDSA Certificate で (6) 使用する証明書を選択する。(7) SSL プロトコル欄の SSL 3.0、TLS 1.0、TLS1.1、TLS1.2 を選択して、有効にするか無効にするかを (8) 有効化 (9) 無効化にチェックを入れ、(10) 保存ボタンで確定する。

※ECDSA 暗号の有効化でオンを選択し、ECDSA 証明書を選択しないと ECDSA を含む暗号スイートが有効にならない。

※ECDSA 証明書のみは設定できず、RSA 証明書を設定することが前提となる。

図 6.10.2-2 サービス編集画面（プロトコルバージョン）

II. 暗号スイートの設定

A) サービス編集画面の（1）PFS（Perfect Forward Secrecy）の有効化で（2）はいを選択する。（3）暗号欄で（4）カスタムにチェックを入れると（5）Selected Ciphers 欄と（6）Available Ciphers 欄が表示されるので、（7）追加ボタンと（8）削除ボタンで Selected Ciphers 欄に追加し、（9）保存ボタンで確定する。

※PFS（Perfect Forward Secrecy）を有効化しないと ECDHE を含む暗号スイートは選択しても有効にならない。

※デフォルトでは全て Selected Ciphers 欄に追加されている。

※優先度は Selected Ciphers 欄の上から順となるため、一度全て Available Ciphers 欄に移動する必要がある。

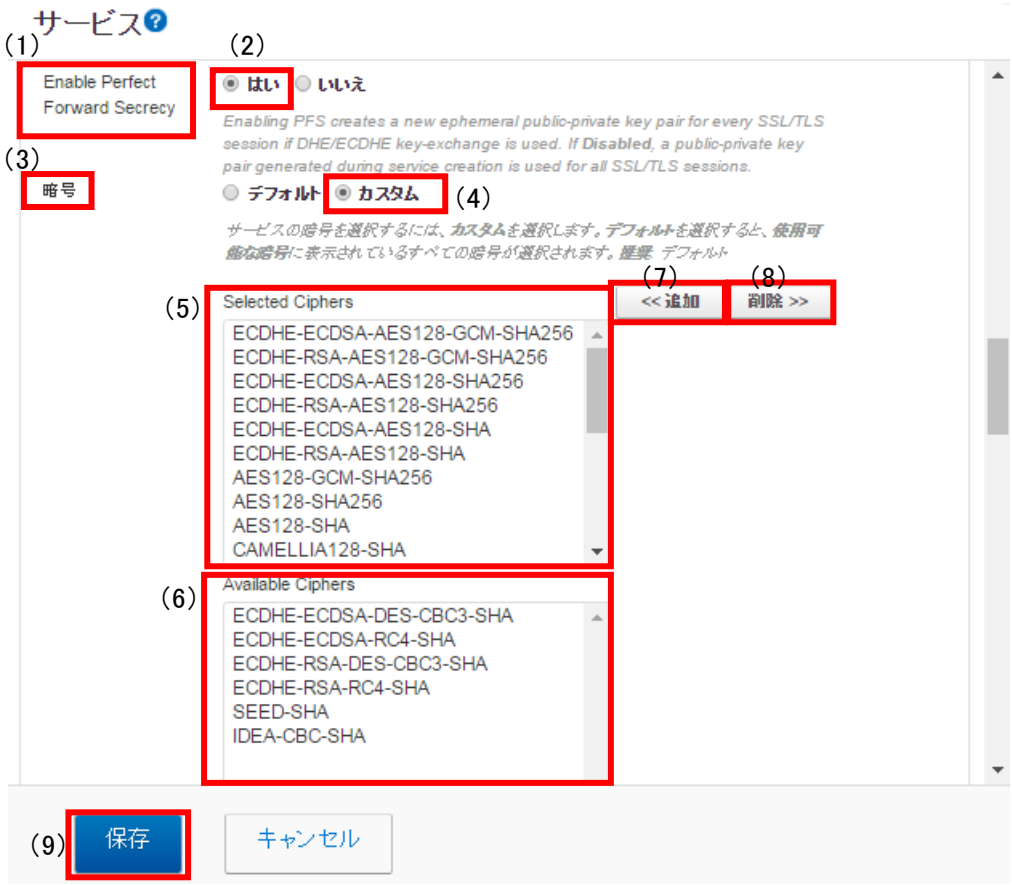

図 6.10.2-3 サービス編集画面（暗号スイート）

III. DH/DHE、ECDH/ECDHE の鍵長の設定

設定方法なし。

ECDHE の鍵長は、既定で 256bit(secp256r1)である。

※ECDSA512bit の証明書を設定した場合でも secp256r1 が使用される。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定

II 暗号スイートの設定した結果による。

VI. Extension の設定

設定方法なし。

6.10.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.10.3.1. 高セキュリティ型

③「暗号スイートを具体的に設定する方法」により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

暗号スイートを具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容の調査結果を以下に示す。

I. プロトコルバージョン
TLS1.1、TLS1.0、SSL3.0 が有効である。

II. 暗号スイート
6.10.1 表 6.10.1-1　暗号設定内容（デフォルト）の Barracuda WAF で使用可能な暗号スイートのとおり。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。
※6.10.1 表 6.10.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

V. 暗号スイートの優先順位の設定
6.10.1 表 6.10.1-1　暗号設定内容（デフォルト）の Barracuda WAF で使用可能な暗号スイートのとおり。

VI. Extension の設定
6.10.1 表 6.10.1-1　暗号設定内容（デフォルト）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
TLS1.1、TLS1.0、SSL3.0 が有効である。

II. 暗号スイート
差分あり。
高セキュリティ型に含まれる 12 個の暗号スイートのうち、表 6.10.3.1-1 設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型（一部）」にある 2 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 18 個の暗号スイートが使用可能である。優先順位についても表 6.10.3.1-1 設定ガイドラインとの差分（高セキュリティ型） のとおりである。

表 6.10.3.1-1 設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）
β	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）
–	設定ガイドラインの高セキュリティ型に該当しない暗号スイ	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
	ート	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		5	TLS_RSA_WITH_AES_256_GCM_SHA384
		6	TLS_RSA_WITH_AES_128_GCM_SHA256
		7	TLS_RSA_WITH_AES_256_CBC_SHA256
		8	TLS_RSA_WITH_AES_128_CBC_SHA256
		9	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		10	TLS_RSA_WITH_RC4_128_SHA
		11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
		14	TLS_RSA_WITH_AES_256_CBC_SHA
		15	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
		16	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		17	TLS_RSA_WITH_AES_128_CBC_SHA
		18	TLS_RSA_WITH_SEED_CBC_SHA
		19	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
		20	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：有効化：TLS1.2
無効化：SSL3.0、TLS1.0、TLS1.1
（図 6.10.2-2 参照）

II. 暗号スイート
6.10.2 II 図 6.10.2-3　サービス編集画面（暗号スイート）の「暗号」「Select Ciphers」欄に、表 6.10.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定）の順番で「追加」する。

表 6.10.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定）

優先順位	暗号スイート
1	ECDHE-ECDSA-AES256-GCM-SHA384
2	ECDHE-RSA-AES256-GCM-SHA384
3	ECDHE-ECDSA-AES128-GCM-SHA256
4	ECDHE-RSA-AES128-GCM-SHA256

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる 12 個の暗号スイートのうち､表 6.3.3.1-3 設定ガイドラインとの差分（高セキュリティ型、個別指定、RSA 証明書設定時） の「設定ガイドラインの高セキュリティ型（一部）」にある 4 個の暗号スイートの使用が可能である。優先順位についても表 6.10.3.1-3 設定ガイドラインとの差分（高セキュリティ型、個別指定） のとおりである。

表 6.10.3.1-3 設定ガイドラインとの差分（高セキュリティ型、個別指定）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α追加）	1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384（α追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（α追加）
β	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β追加）	3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256（β追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（β追加）

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.10.3.2. 推奨セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

暗号スイートを具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.10.3.1 **高セキュリティ型**と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
SSL3.0 が有効である。

II. 暗号スイート
差分あり。
推奨セキュリティ型に含まれる 64 個の暗号スイートのうち、表 6.10.3.2-1 設定ガイドライン

との差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型（一部）」にある 14 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 6 個の暗号スイートが使用可能である。

表 6.10.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	17	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	8	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）	19	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	6	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	14	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	7	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	15	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	5	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	9	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		10	TLS_RSA_WITH_RC4_128_SHA
		12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		16	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		18	TLS_RSA_WITH_SEED_CBC_SHA
		20	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：有効化：TLS1.0、TLS1.1、TLS1.2
無効化：SSL3.0
（図 6.10.2-2 参照）

II. 暗号スイート
6.10.2 II 図 6.10.2-3　サービス編集画面（暗号スイート）の「暗号」「Select Ciphers」欄に、表 6.10.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定）の順番で「追加」する。

表 6.10.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定）

優先順位	暗号スイート
1	ECDHE-ECDSA-AES128-GCM-SHA256
2	ECDHE-RSA-AES128-GCM-SHA256
3	ECDHE-ECDSA-AES128-SHA256
4	ECDHE-RSA-AES128-SHA256
5	ECDHE-ECDSA-AES128-SHA
6	ECDHE-RSA-AES128-SHA
7	AES128-GCM-SHA256
8	AES128-SHA256
9	AES128-SHA
10	CAMELLIA128-SHA
11	ECDHE-ECDSA-AES256-GCM-SHA384
12	ECDHE-RSA-AES256-GCM-SHA384
13	ECDHE-ECDSA-AES256-SHA384
14	ECDHE-RSA-AES256-SHA384
15	ECDHE-ECDSA-AES256-SHA
16	ECDHE-RSA-AES256-SHA
17	AES256-GCM-SHA384
18	AES256-SHA256
19	AES256-SHA
20	CAMELLIA256-SHA

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。
※ECDSA（256bit）の証明書を設定した場合 256bit(secp256r1)が使用される。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる 64 個の暗号スイートのうち、表 6.10.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型（一部）」にある 20 個の暗号スイートの使用が可能である。優先順位についても表 6.10.3.2-1　設定ガイドライ

ンとの差分（推奨セキュリティ型） のとおりである。

表 6.10.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
B	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	7	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA(B)	9	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)	10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)
D	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	11	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	12	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	13	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	15	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)	16	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)
E	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	17	TLS_RSA_WITH_AES_256_GCM_SHA384(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	18	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_CBC_SHA(E)	19	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)	20	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.10.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に設定方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.10.3.1 **高セキュリティ型**と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート

差分あり。
セキュリティ例外型に含まれる 67 個の暗号スイートのうち、表 6.10.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）の「設定ガイドラインのセキュリティ例外型（一部）」にある 16 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 4 個の暗号スイートが使用可能である。

表 6.10.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	17	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	8	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）	19	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	6	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	14	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	7	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）	15	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	5	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	10	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	16	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）
-	設定ガイドラインのセキュリティ例外型に該当しない暗号スイート	9	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		18	TLS_RSA_WITH_SEED_CBC_SHA
		20	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL プロトコル：有効化：SSL3.0、TLS1.0、TLS1.1、TLS1.2　（図 6.10.2-2 参照）

II. 暗号スイート
6.10.2 II 図 6.10.2-3　サービス編集画面（暗号スイート）の「暗号」「Select Ciphers」欄に、表 6.10.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定）の順番で「追加」する。

表 6.10.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定）

優先順位	暗号スイート
1	ECDHE-ECDSA-AES128-GCM-SHA256
2	ECDHE-RSA-AES128-GCM-SHA256
3	ECDHE-ECDSA-AES128-SHA256

優先順位	暗号スイート
4	ECDHE-RSA-AES128-SHA256
5	ECDHE-ECDSA-AES128-SHA
6	ECDHE-RSA-AES128-SHA
7	AES128-GCM-SHA256
8	AES128-SHA256
9	AES128-SHA
10	CAMELLIA128-SHA
11	ECDHE-ECDSA-AES256-GCM-SHA384
12	ECDHE-RSA-AES256-GCM-SHA384
13	ECDHE-ECDSA-AES256-SHA384
14	ECDHE-RSA-AES256-SHA384
15	ECDHE-ECDSA-AES256-SHA
16	ECDHE-RSA-AES256-SHA
17	AES256-GCM-SHA384
18	AES256-SHA256
19	AES256-SHA
20	CAMELLIA256-SHA
21	RC4-SHA
22	DES-CBC3-SHA

※グループ内の順番は順不同。

III. DH/DHE、ECDH/ECDHE の鍵長
ECDHE の鍵長は 256bit(secp256r1)である。
※ECDSA（256bit）の証明書を設定した場合 256bit(secp256r1)が使用される。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる 67 個の暗号スイートのうち、表 6.10.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定）の「設定ガイドラインのセキュリティ例外型（一部）」にある 22 個の暗号スイートの使用が可能である。優先順位についても表 6.10.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）のとおりである。

表 6.10.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)	1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(A 追加)

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)	3	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)	5	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
B	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	7	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_CBC_SHA(B)	9	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)	10	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA(B)
D	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)	11	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	12	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)	13	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)	15	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)	16	TLS_ECDHE_RSA_AES_256_CBC_SHA(D 追加)
E	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	17	TLS_RSA_WITH_AES_256_GCM_SHA384(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	18	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_CBC_SHA(E)	19	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)	20	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA(E)
G	TLS_RSA_WITH_RC4_128_SHA(G)	21	TLS_RSA_WITH_RC4_128_SHA(G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)	22	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.11. Citrix NetScaler MPX シリーズ

本章では、Citrix NetScaler MPX 8005c について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書のみが設定可能であり、6.11.1 **デフォルトでの暗号設定内容の調査**、および、6.11.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、RSA 証明書を設定した場合について記載する。

6.11.1. デフォルトでの暗号設定内容の調査

サーバ証明書は､RSA 証明書のみが設定可能であり､RSA 証明書を設定した場合について記載する。

表 6.11.1-1　暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	サーバ	17
tls1.1	ON	サーバ	9
tls1.0	ON	サーバ	9
sslv3	ON	サーバ	9
sslv2	設定不可	ー	ー

- Citrix NetScaler MPX 8005c で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256r1	ON:14	ON:6	ON:6	ON:6	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON:13	ON:5	ON:5	ON:5	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:8	ON:4	ON:4	ON:4	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:7	ON:3	ON:3	ON:3	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:10	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:9	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:12	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:11	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:17	ON:9	ON:9	ON:9	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:16	ON:8	ON:8	ON:8	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:15	ON:7	ON:7	ON:7	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:2	ON:2	ON:2	ON:2	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:1	ON:1	ON:1	ON:1	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:4	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:3	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:5	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF:デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.11.2. 暗号設定方法の調査

I. プロトコルバージョンの指定

A) ブラウザで Citrix NetScaler MPX 8005c の管理画面にログインし、(1) Configurationー (2) Traffic Managementー（3）Load Balancingー（4）Virtual Servers をクリックして、仮想サーバー覧を表示し、(5）編集したい仮想サーバを選択し、(6）Edit ボタンを押下する。

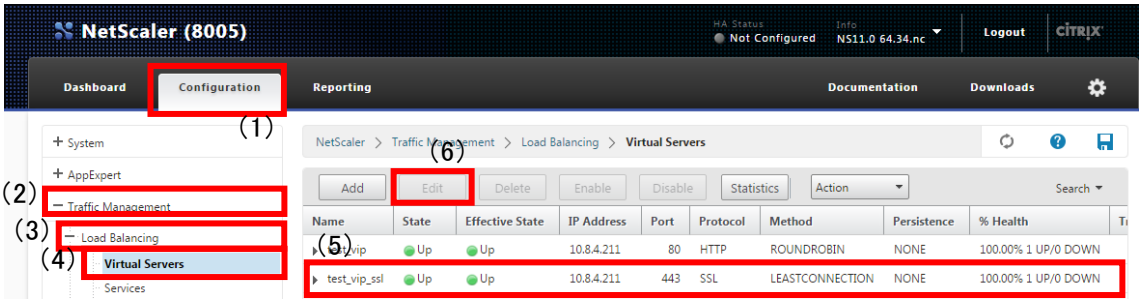

図 6.11.2-1 仮想サーバー覧画面-1

B) 仮想サーバ設定画面に遷移するので画面下の（7）「SSL Parameters」項目右側の（8）「ペン」アイコンを押下する。

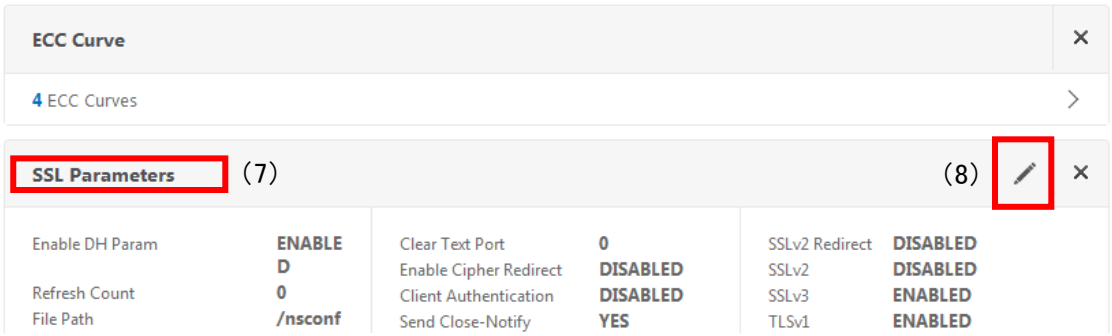

図 6.11.2-2 仮想サーバ設定画面（SSL パラメータ）

C) 「SSL Parameters」の設定を変更出来るようになるので、(9)「Protocol」」欄の有効にしたい(10)プロトコルのチェックボックスにチェックを入れ、(11)「OK」ボタンを押下し「SSL Parameters」の設定を完了して（12）「Done」ボタンを押下して Virtual Server の設定を完了する。

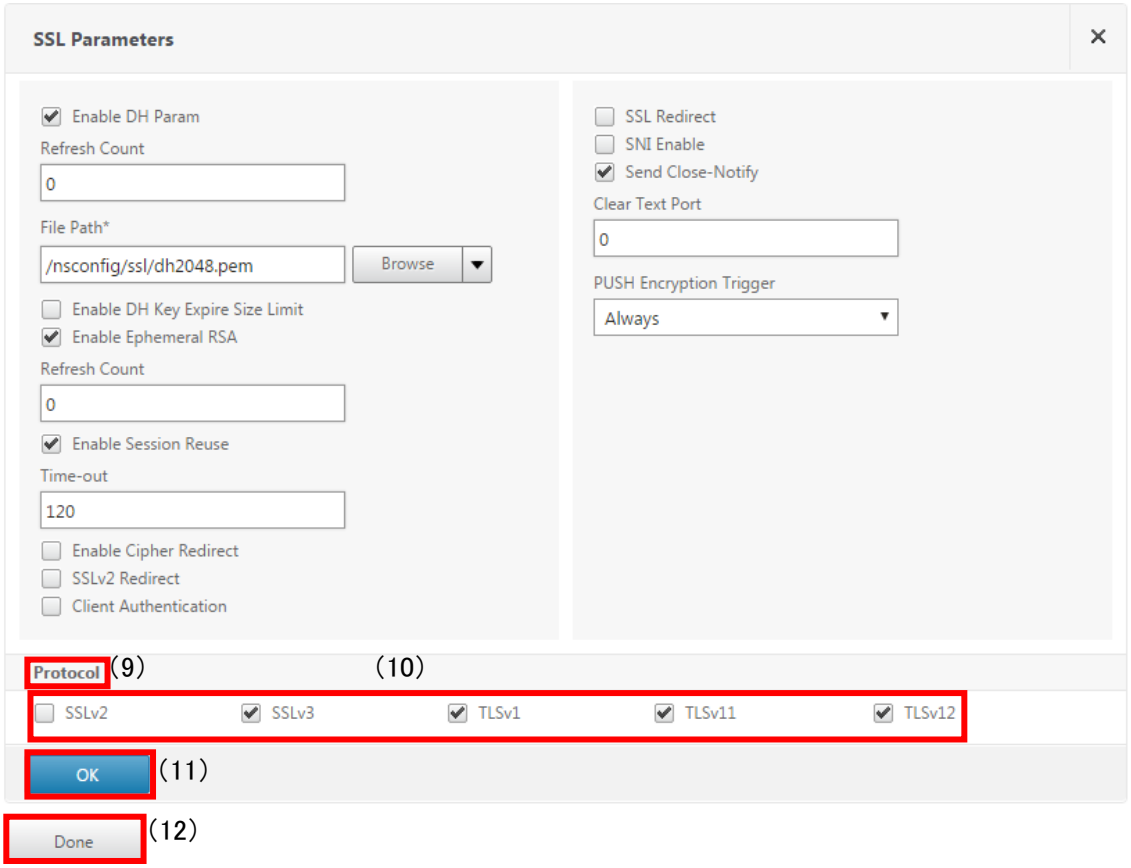

図 6.11.2-3　仮想サーバ設定画面（プロトコル）

D)　仮想サーバー覧画面に戻るので、右上の（13）「フロッピー」アイコンをクリックすると確認のダイアログが表示されるので、（14）「YES」を押下して設定を保存する。

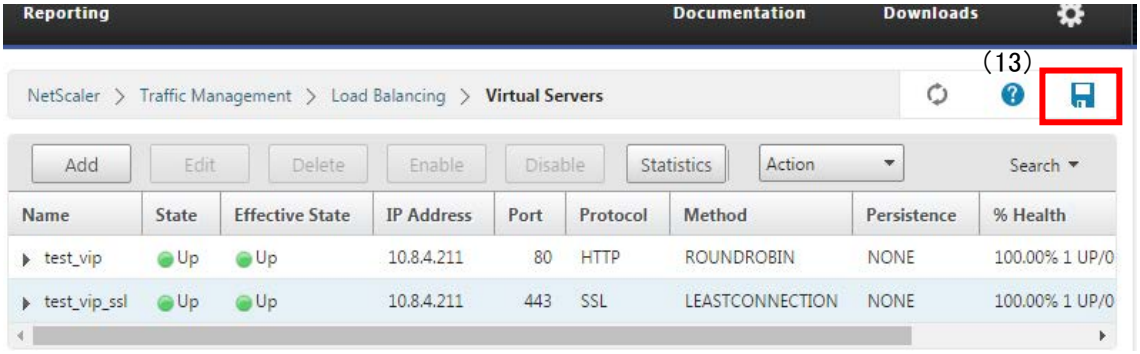

図 6.11.2-4　仮想サーバー覧画面-2

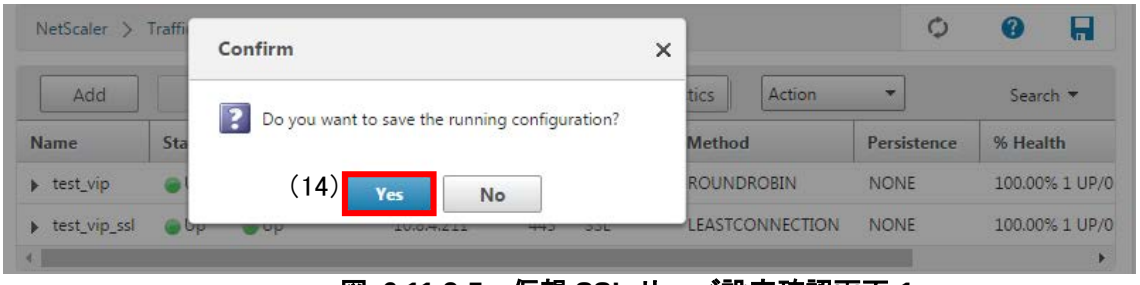

図 6.11.2-5　仮想 SSL サーバ設定確認画面-1

II. 暗号スイートの設定

A) ブラウザで Citrix NetScaler MPX 8005c の管理画面にログインし、(1) Configuration－(2) Traffic Management－（3）Load Balancing－（4）Virtual Servers をクリックして、仮想サーバー覧を表示し、(5）編集したい仮想サーバを選択し、(6）Edit ボタンを押下する。

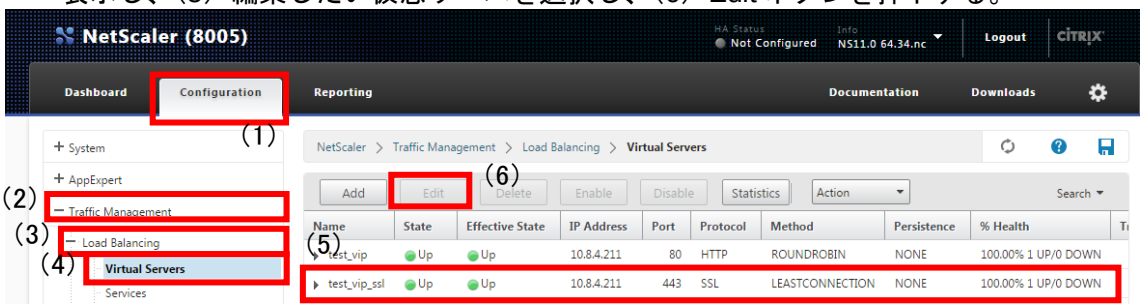

図 6.11.2-6 仮想サーバー覧画面-3

B) 仮想サーバ設定画面に遷移するので（7）「SSL Ciphers」右側の（8）ペンのボタンを押下し、表示される（9）「Add」ボタンを押下する。

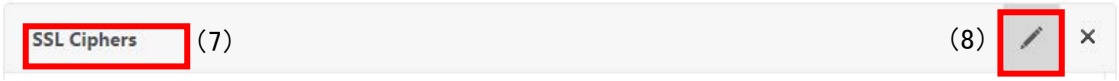

図 6.11.2-7 仮想サーバ設定画面（SSL 暗号）

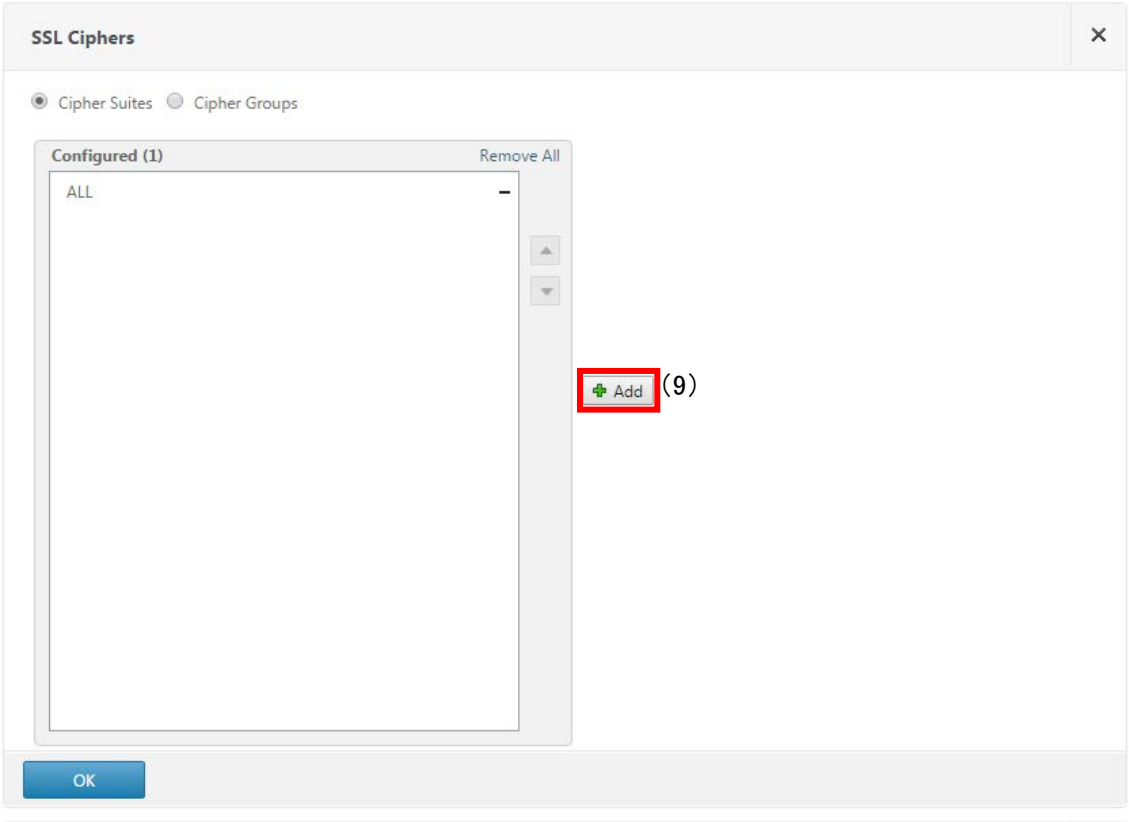

図 6.11.2-8 SSL 暗号編集画面

C)　（10）「Available」欄が表示されるので、（11）グループのツリーを展開し、有効にしたい暗号スイートに（12）チェックを入れ、（13）「右三角」ボタンを押下して（14）「Configured」欄へ移動させる。
優先順位は「Configured」欄の上から設定されるため、（15）暗号スイートを選択した上で右側の（16）「上三角」・「下三角」ボタンで順番を入れ替えることが可能。
設定し終わったら（17）「OK」ボタンと画面下の（18）「Done」ボタンを押下し、設定を完了する。

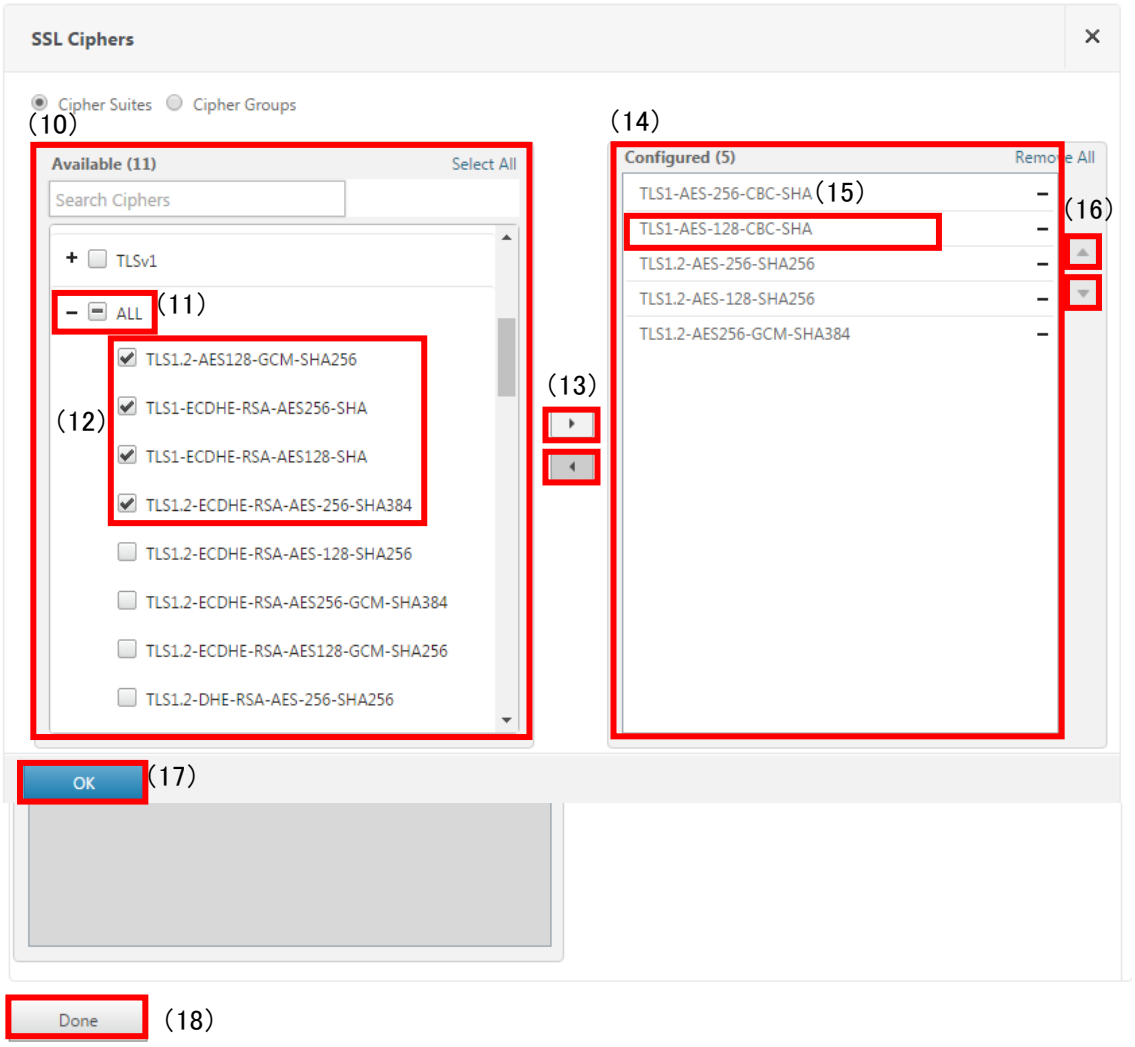

図 6.11.2-9　仮想 SSL サーバ設定画面（暗号スイート）

D)　仮想サーバー覧画面に戻るので、右上の（19）「フロッピー」アイコンをクリックすると確認のダイアログが表示されるので、（20）「YES」を押下して設定を保存する。

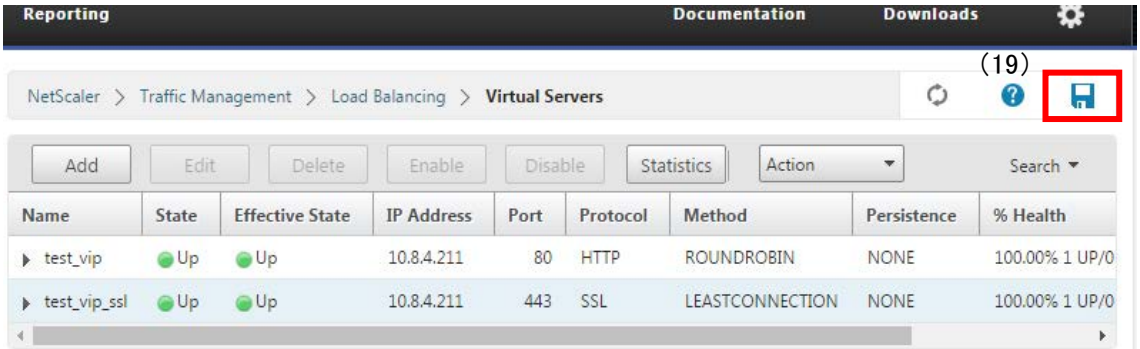

図 6.11.2-10　仮想サーバー覧画面-4

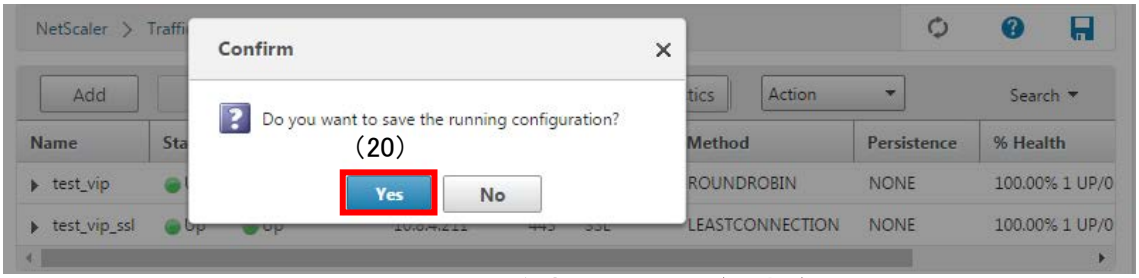

図 6.11.2-11　仮想 SSL サーバ設定確認画面-2

III. DH/DHE、ECDH/ECDHE の鍵長の設定
DH/DHE： 6.11.2.I.C の図 6.11.2-3　仮想サーバ設定画面（プロトコル）にて、「Enable DH Param」にチェックを入れ、DH パラメータが記載された pem 形式のファイルを設定すると pem 形式ファイルの DH パラメータの鍵長で鍵交換が行われる。
対応している鍵長：256bit、512bit、1024bit、2048bit

ECDH/ECDHE : 6.11.2.I.B の図 6.11.2-2　仮想サーバ設定画面（SSL パラメータ）にある「ECC Curve」の項目にて P_224（224bit）、P_256（256bit）、P_384（384bit）、P_521（521bit）が設定されており、設定から外すことも可能である(図 6.11.2-12　ECC Curve 設定画面 参照)。
複数設定している場合、優先されるのは 256bit となっている。

図 6.11.2-12　ECC Curve 設定画面

IV. サーバクライアントの優先順位の設定
既定でサーバ優先であり、変更できない。

V. 暗号スイートの優先順位の設定
図 6.11.2-9　仮想 SSL サーバ設定画面（暗号スイート）の「Configured」欄へ、優先度上位の暗号スイートを上から順に設定する。

VI. Extension の設定
設定方法なし。

6.11.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.11.3.1. 高セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

I. プロトコルバージョン
tls1.2、tls1.1、tls1.0、sslv3 が有効である。
※6.11.1 表 6.11.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権 のとおり。

II. 暗号スイート
6.11.1 表 6.11.1-1　暗号設定内容（デフォルト）の Citrix NetScaler MPX 8005c で使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：デフォルトでは設定 DH/DHE が含まれる暗号スイートなし。
ECDH/ECDHE：256bit(secp256r1)

IV. サーバクライアントの優先順位の設定
サーバ優先である。
※6.11.1 表 6.11.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権 のとおり。

V. 暗号スイートの優先順位の設定
6.11.1 表 6.11.1-1　暗号設定内容（デフォルト）の Citrix NetScaler MPX 8005c で使用可能な暗号スイートの優先順位 のとおり。

VI. Extension の設定
6.11.1 表 6.11.1-1　暗号設定内容（デフォルト）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
tls1.1、tls1.0、sslv3 が有効である。

II. 暗号スイート
差分あり。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.12.3.1-1　設定ガイドラインとの差分（高セキュリティ型） の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 15 個の暗号スイートが使用可能である。使用可能な 2 個の暗号スイートの優先順位は、表 6.11.3.1-1　設定ガイドラインとの差分（高セキュリティ型） のとおりである。

表 6.11.3.1-1　設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)	11	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	12	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
-	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	1	TLS_RSA_WITH_AES_256_CBC_SHA
		2	TLS_RSA_WITH_AES_128_CBC_SHA
		3	TLS_RSA_WITH_AES_256_CBC_SHA256
		4	TLS_RSA_WITH_AES_128_CBC_SHA256
		5	TLS_RSA_WITH_AES_256_GCM_SHA384
		6	TLS_RSA_WITH_AES_128_GCM_SHA256
		7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
		9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
		10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		13	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		14	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		15	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		16	TLS_RSA_WITH_RC4_128_SHA
		17	TLS_RSA_WITH_RC4_128_MD5

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLS1.2 をチェックし、TLS1.1、TLS1.0、SSLv3、SSLv2 のチェックを外す。
（図 6.11.2-3 参照）

II. 暗号スイート
6.11.2.II.C の手順にて SSL Ciphers 項目 Configured 欄に表 6.11.3.1-2　暗号スイートの設定(高セキュリティ型、個別指定） の順番で設定する。

表 6.11.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定）

Configured	暗号スイート
1	TLS1.2-DHE-RSA-AES256-GCM-SHA384
2	TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
3	TLS1.2-DHE-RSA-AES128-GCM-SHA256
4	TLS1.2-ECDHE-RSA-AES128-GCM-SHA256

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：「Enable DH Param」にチェックを入れ、2048bit の pem 形式ファイルを設定する。
ECDH/ECDHE：「ECC Curve」の項目にて P_256（256bit）設定する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先のため、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.11.3.1-3 設定ガイドラインとの差分（高セキュリティ型、個別指定）の「設定ガイドラインの高セキュリティ型(一部)」にある 4 個の暗号スイートの使用が可能である。使用可能な 4 個の暗号スイートの優先順位は、設定ガイドラインの高セキュリティ型の順位と同じである。

表 6.11.3.1-3 設定ガイドラインとの差分（高セキュリティ型、個別指定）

グループ	設定ガイドラインの高セキュリティ型（一部）	優先順位	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	1	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	4	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.11.3.2. 推奨セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.11.3.1 高セキュリティ型と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
sslv3 が有効である。

II. 暗号スイート
差分あり。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.11.3.2-1 設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 12 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 5 個の暗号スイートが使用可能である。使用可能な 12 個の暗号スイートの優先順位は、表 6.11.3.2-1 設定ガイドラインとの差分（推奨セキュリティ型） のとおりである。

表 6.11.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	12	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	2	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	4	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	6	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	1	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	3	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	5	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	13	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		14	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		15	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		16	TLS_RSA_WITH_RC4_128_SHA
		17	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
TLS1.2、TLS1.0、TLS1.1 をチェックし、SSLv3、SSLv2 のチェックを外す。
（図 6.11.2-3 参照）

II. 暗号スイート
6.11.2.II.C の手順にて SSL Ciphers 項目 Configured 欄に表 6.11.3.2-2　暗号スイートの設定(推奨セキュリティ型、個別指定） の順番で設定する。

表 6.11.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定）

Configured	暗号スイート
1	TLS1-DHE-RSA-AES-128-CBC-SHA
2	TLS1.2-DHE-RSA-AES128-SHA256
3	TLS1.2-DHE-RSA-AES128-GCM-SHA256
4	TLS1-ECDHE-RSA-AES128-SHA
5	TLS1.2-ECDHE-RSA-AES-128-SHA256
6	TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
7	TLS1-AES-128-CBC-SHA

Configured	暗号スイート
8	TLS1.2-AES-128-SHA256
9	TLS1.2-AES-128-GCM-SHA256
10	TLS1-DHE-RSA-AES-256-CBC-SHA
11	TLS1.2-DHE-RSA-AES-256-SHA256
12	TLS1.2-DHE-RSA-AES256-GCM-SHA384
13	TLS1-ECDHE-RSA-AES256-SHA
14	TLS1.2-ECDHE-RSA-AES-256-SHA384
15	TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
16	TLS1-AES-256-CBC-SHA
17	TLS1.2-AES-256-CBC-SHA256
18	TLS1.2-AES-256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：「Enable DH Param」にチェックを入れ、2048bit の pem 形式ファイルを設定する。
ECDH/ECDHE：「ECC Curve」の項目にて P_256（256bit）設定する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先のため、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した結果による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.11.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 18 個の暗号スイートの使用が可能である。使用可能な 18 個の暗号スイートの優先順位は、設定ガイドラインの推奨セキュリティ型の順位と同じである。

表 6.11.3.2-3　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	1	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	5	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	7	TLS_RSA_WITH_AES_128_CBC_SHA(B)

グループ	設定ガイドラインの推奨セキュリティ型（一部）	優先順位	暗号スイート設定結果
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	9	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	10	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	11	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	12	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	13	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	15	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	16	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	17	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	18	TLS_RSA_WITH_AES_256_GCM_SHA384(E)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

IV. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.11.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.11.3.1 高セキュリティ型と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分あり。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.11.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）　の「設定ガイドラインのセキュリティ例外型(一部)」にある 14 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 3 個の暗号スイートが使用可能である。使用可能な 14 個の暗号スイートの優先順位は、表 6.11.3.3-1　設定ガイドラインとの差分（セキュリティ例外型） のとおりである。

表 6.11.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）	12	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
B	TLS_RSA_WITH_AES_128_CBC_SHA（B）	2	TLS_RSA_WITH_AES_128_CBC_SHA（B）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	4	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	6	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)	9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)	11	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	1	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	3	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	5	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	16	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	15	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	13	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		14	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		17	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSLv3、TLS1.0、TLS1.1、TLS1.2 のチェックを入れる。 （図 6.11.2-3 参照）

II. 暗号スイート
6.11.2.II.C の手順にて SSL Ciphers 項目 Configured 欄に表 6.11.3.3-2 暗号スイートの設定(セキュリティ例外型、個別指定） の順番で設定する。

表 6.11.3.3-2 暗号スイートの設定（セキュリティ例外型、個別指定）

Configured	暗号スイート
1	TLS1-DHE-RSA-AES-128-CBC-SHA
2	TLS1.2-DHE-RSA-AES128-SHA256
3	TLS1.2-DHE-RSA-AES128-GCM-SHA256
4	TLS1-ECDHE-RSA-AES128-SHA
5	TLS1.2-ECDHE-RSA-AES-128-SHA256
6	TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
7	TLS1-AES-128-CBC-SHA
8	TLS1.2-AES-128-SHA256
9	TLS1.2-AES-128-GCM-SHA256
10	TLS1-DHE-RSA-AES-256-CBC-SHA
11	TLS1.2-DHE-RSA-AES-256-SHA256
12	TLS1.2-DHE-RSA-AES256-GCM-SHA384

Configured	暗号スイート
13	TLS1-ECDHE-RSA-AES256-SHA
14	TLS1.2-ECDHE-RSA-AES-256-SHA384
15	TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
16	TLS1-AES-256-CBC-SHA
17	TLS1.2-AES-256-CBC-SHA256
18	TLS1.2-AES-256-GCM-SHA384
19	SSL3-RC4-SHA
20	SSL3-EDH-RSA-DES-CBC3-SHA
21	SSL3-DES-CBC3-SHA

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：「Enable DH Param」にチェックを入れ、2048bit の pem 形式ファイルを設定する。
ECDH/ECDHE：「ECC Curve」の項目にて P_256（256bit）設定する。

IV. サーバクライアントの優先順位の設定
既定でサーバ優先のため、変更できない。

V. 暗号スイートの優先順位の設定
II.暗号スイートで設定した内容による。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。

II. 暗号スイート
差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.11.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定） の「設定ガイドラインのセキュリティ例外型(一部)」にある 21 個の暗号スイートの使用が可能である。使用可能な 21 個の暗号スイートの優先順位は、設定ガイドラインのセキュリティ例外型の順位と同じである。

表 6.11.3.3-3　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	1	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	2	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)	5	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	7	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	9	TLS_RSA_WITH_AES_128_GCM_SHA256(B)

グループ	設定ガイドラインのセキュリティ例外型（一部）	優先順位	暗号スイート設定結果
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	10	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	11	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	12	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	13	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	15	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	16	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	17	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	18	TLS_RSA_WITH_AES_256_GCM_SHA384(E)
G	TLS_RSA_WITH_RC4_128_SHA(G)	19	TLS_RSA_WITH_RC4_128_SHA(G)
H	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(H)	20	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(H)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)	21	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III.DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.12. セイコーソリューションズ Netwiser シリーズ

本章では、Netwiser SX-3850 について調査した結果を示す。

なお、サーバ証明書は、RSA 証明書のみが設定可能であり、6.12.1 **デフォルトでの暗号設定内容の調査**、および、6.12.3 **暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析**については、RSA 証明書を設定した場合について記載する。

6.12.1. デフォルトでの暗号設定内容の調査

表 6.12.1-1　暗号設定内容（デフォルト）

- CipherSuite 選択優先権

プロトコル	プロトコル設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	15
tls1.1	設定不可	ー	ー
tls1.0	ON	クライアント	5
sslv3	OFF	ー	0
sslv2	設定不可	ー	ー

- Netwiser SX-3850 で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON	OFF	ON	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	OFF	ON	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	OFF	ON	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	OFF	ON	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	OFF	ON	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON	OFF	OFF	OFF	OFF

※tls1.2～sslv2 欄が全て OFF：デフォルトでは設定可能になっていない暗号スイート。

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

6.12.2. 暗号設定方法の調査

I.　プロトコルバージョンの指定

A)ブラウザで WEB 管理画面にログインし、(1) 設定ー (2) バランシングー (3) SSL アクセラレーションー (4) SSL アクセラレーションをクリックして SSL アクセラレーション選択画面を表示する。

SSL アクセラレーション選択画面の (5) SSL3.0 有効/無効欄のチェックボックスを選択して、SSL3.0 を有効にするか無効にするかを操作する。

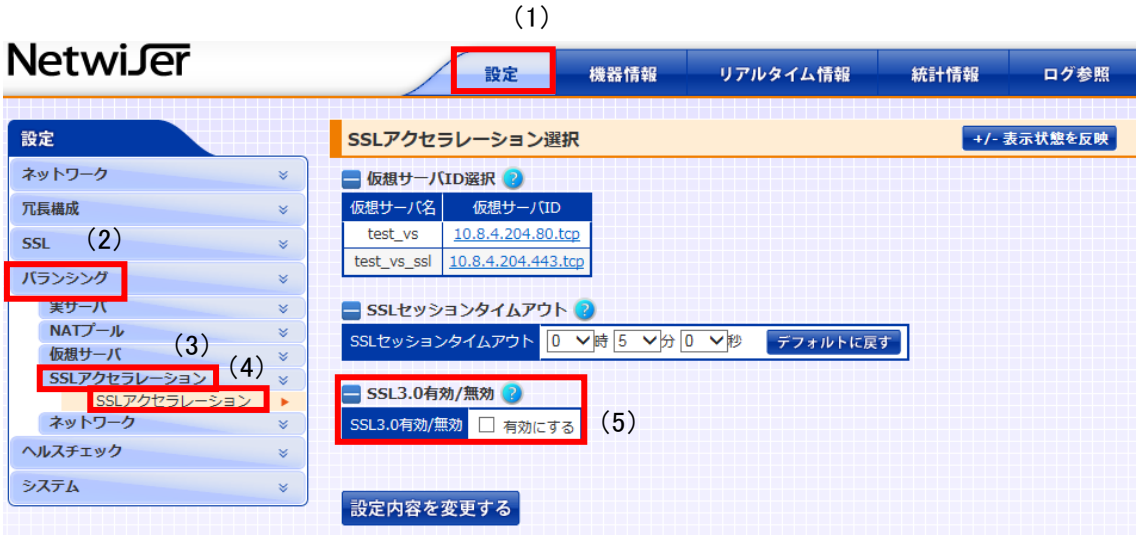

図 6.12.2-1　SSL アクセラレーション選択画面-1

II.　暗号スイートの設定

A)SSL アクセラレーション選択画面で設定したい (6) 仮想サーバ ID を選択する。

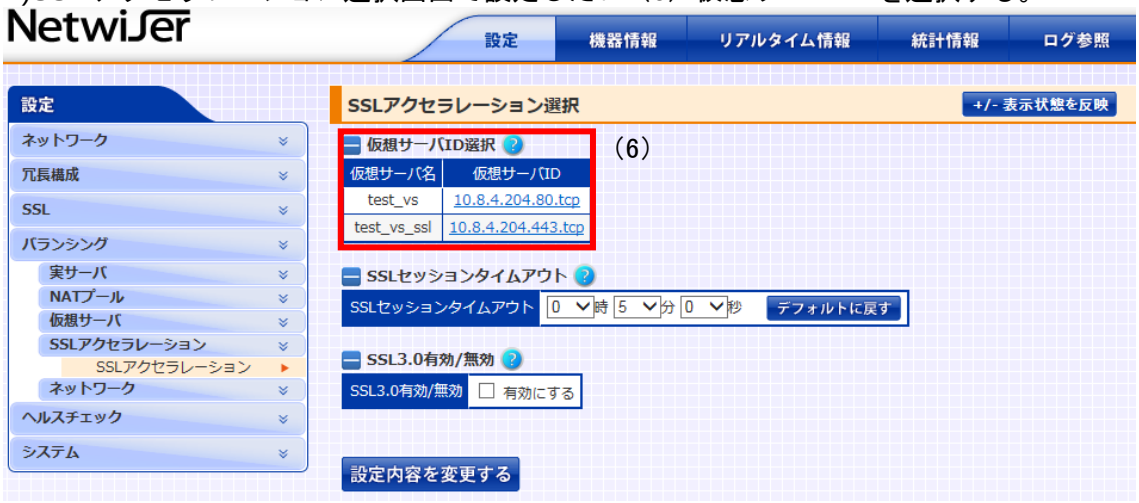

図 6.12.2-2　SSL アクセラレーション選択画面-2

B)SSL アクセラレーション設定画面の（7）SSL アクセラレーション詳細設定欄に、設定したい暗号スイートのチェックボックスにチェックを入れて暗号スイートを指定する。

図 6.12.2-3　SSL アクセラレーション設定画面

※デフォルトで有効になっている暗号スイート：RC4-MD5、RC4-SHA、DES-CBC3-SHA、AES128-SHA、DHE-AES128-SHA、AES256-SHA、DHE-AES256-SHA、AES128-SHA256、AES256-SHA256、DHE-AES128-SHA256、DHE-AES256-SHA256、AES128-GCM-SHA256、AES256-GCM-SHA384、DHE-RSA-AES128-GCM-SHA256、DHE-RSA-AES256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長の設定
製品独自の設定方法なし

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
サーバクライアントの優先順位がクライアント優先であり、暗号スイートの優先順位がないため設定できない。

VI. Extension の設定
設定方法なし。

6.12.3. 暗号設定内容と設定ガイドラインでの設定要求との差分の調査・分析

6.12.3.1. 高セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの高セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容の調査結果を以下に記載する。

I. プロトコルバージョン
tls1.2、tls1.0 が有効である。
※6.12.1 表 6.12.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

II. 暗号スイート
6.12.1 表 6.12.1-1　暗号設定内容（デフォルト）Netwiser SX-3850 で使用可能な暗号スイートで使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：1024bit

IV. サーバクライアントの優先順位の設定
クライアント優先である。
※6.12.1 表 6.12.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

V. 暗号スイートの優先順位の設定
クライアント優先であるため、優先順位はなし。

VI. Extension の設定
6.12.1 表 6.12.1-1　暗号設定内容（デフォルト）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分あり。
tls1.0 が有効である。

II. 暗号スイート
差分あり。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.12.3.1-1　設定ガイドラインとの差分（高セキュリティ型）の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。その他、高セキュリティ型に含まれない 13 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.12.3.1-1　設定ガイドラインとの差分（高セキュリティ型）

グループ	設定ガイドラインの高セキュリティ型（一部）	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)
-	設定ガイドラインの高セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5
		TLS_RSA_WITH_RC4_128_SHA
		TLS_RSA_WITH_3DES_EDE_CBC_SHA

グループ	設定ガイドラインの高セキュリティ型（一部）	暗号スイート設定結果
		TLS_RSA_WITH_AES_128_CBC_SHA
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA
		TLS_RSA_WITH_AES_256_CBC_SHA
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA
		TLS_RSA_WITH_AES_128_CBC_SHA256
		TLS_RSA_WITH_AES_256_CBC_SHA256
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
		TLS_RSA_WITH_AES_128_GCM_SHA256
		TLS_RSA_WITH_AES_256_GCM_SHA384

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL3.0 有効/無効：（チェックを外す）
TLS1.0、TLS1.1 の設定はない。
（図 6.12.2-1 参照）

II. 暗号スイート
6.12.2.II.B 図 6.12.2-3　SSL アクセラレーション設定画面 の SSL アクセラレーション詳細設定で下記暗号スイートのチェックボックスにチェックを入れる。
DHE-AES256-GCM-SHA384、DHE-AES128-GCM-SHA256

※クライアント優先のため、優先順位は設定されない。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
クライアント優先であるため、優先順位はなし。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
※TLS1.0 の設定はないが、6.12.3.1 ③Ⅱ.暗号スイートで設定した暗号スイートが使えるプロトコルバージョンが TLS1.2 のみであるため、結果として TLS1.2 のみ有効になる。

II. 暗号スイート
差分なし。
高セキュリティ型に含まれる暗号スイート 12 個のうち、表 6.12.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定） の「設定ガイドラインの高セキュリティ型(一部)」にある 2 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.12.3.1-2　設定ガイドラインとの差分（高セキュリティ型、個別指定）

グループ	設定ガイドラインの高セキュリティ型（一部）	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.12.3.2. 推奨セキュリティ型

③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）
「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.12.3.1 高セキュリティ型と同じである。

② ①の設定と設定ガイドラインの設定内容との差分
I. プロトコルバージョン
差分なし。
TLS1.1 が無効である。

II. 暗号スイート
差分あり。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 6.12.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型） の「設定ガイドラインの推奨セキュリティ型(一部)」にある 12 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 3 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.12.3.2-1　設定ガイドラインとの差分（推奨セキュリティ型）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	TLS_RSA_WITH_AES_256_CBC_SHA(E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	TLS_RSA_WITH_AES_256_CBC_SHA256(E)
	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	TLS_RSA_WITH_AES_256_GCM_SHA384(E)
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5
		TLS_RSA_WITH_RC4_128_SHA
		TLS_RSA_WITH_3DES_EDE_CBC_SHA

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL3.0 有効/無効: （チェックを外す） （図 6.12.2-1 参照）

II. 暗号スイート
図 6.12.2-3 SSL アクセラレーション設定画面 の SSL アクセラレーション詳細設定で下記暗号スイートのチェックボックスにチェックを入れる。
AES128-SHA、AES128-SHA256、AES256-SHA、AES256-SHA256、AES128-GCM-SHA256、AES256-GCM-SHA384、DHE-AES128-SHA、DHE-AES128-SHA256、DHE-AES128-GCM-SHA256、DHE-AES256-SHA、DHE-AES256-SHA256、DHE-AES256-GCM-SHA384

※クライアント優先のため、優先順位は設定されない。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
クライアント優先であるため、優先順位はなし。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.1 が無効である。

II. 暗号スイート
差分なし。
推奨セキュリティ型に含まれる暗号スイート 64 個のうち、下の表 6.12.3.2-2 設定ガイドラインとの差分（推奨セキュリティ型、個別指定）の「設定ガイドラインの推奨セキュリティ型(一部)」にある 12 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため、優先

順位は考慮されない。

表 6.12.3.2-2　設定ガイドラインとの差分（推奨セキュリティ型、個別指定）

グループ	設定ガイドラインの推奨セキュリティ型（一部）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

6.12.3.3. セキュリティ例外型

③暗号スイートを具体的に設定する方法により、設定ガイドラインのセキュリティ例外型に設定（準拠）することができる。

① プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定しない方法）

「暗号アルゴリズム」を具体的に指定する以外に方法がないため、デフォルトでの暗号設定内容となる。調査結果は、6.12.3.1 高セキュリティ型 と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン
差分なし。
TLS1.1 が無効である。

II. 暗号スイート
差分あり。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.12.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）の「設定ガイドラインのセキュリティ例外型(一部)」にある 14 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 1 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.12.3.3-1　設定ガイドラインとの差分（セキュリティ例外型）

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)
-	設定ガイドラインの推奨セキュリティ型に該当しない暗号スイート	TLS_RSA_WITH_RC4_128_MD5

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

③ プロトコルバージョン、暗号スイート、DH/DHE、ECDH/ECDHE の鍵長がもっとも設定ガイドラインの設定要求に準拠していると思われる設定（暗号スイートを具体的に設定する方法）

I. プロトコルバージョン
SSL3.0 有効/無効: （チェックを入れる） （図 6.12.2-1 参照）

II. 暗号スイート
6.12.2.II.B 図 6.12.2-3 SSL アクセラレーション設定画面 の SSL アクセラレーション詳細設定で下記暗号スイートのチェックボックスにチェックを入れる。
RC4-SHA、DES-CBC3-SHA、AES128-SHA、AES128-SHA256、AES256-SHA、AES256-SHA256、AES128-GCM-SHA256、AES256-GCM-SHA384、DHE-AES128-SHA、DHE-AES128-SHA256、DHE-AES128-GCM-SHA256、DHE-AES256-SHA、DHE-AES256-SHA256、DHE-AES256-GCM-SHA384

※クライアント優先のため、優先順位は設定されない。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。

IV. サーバクライアントの優先順位の設定
既定でクライアント優先であり、変更できない。

V. 暗号スイートの優先順位の設定
クライアント優先であるため、優先順位はなし。

VI. Extension の設定
設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。
TLS1.1 が無効である。

II. 暗号スイート

差分なし。
セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 6.12.3.3-2　設定ガイドラインとの差分（セキュリティ例外型、個別指定） の「設定ガイドラインのセキュリティ例外型(一部)」にある 14 個の暗号スイートの使用が可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

表 6.12.3.3-2　設定ガイドラインとの差分（セキュリティ例外型、個別指定）

グループ	設定ガイドラインのセキュリティ例外型（一部）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	TLS_RSA_WITH_AES_256_CBC_SHA (E)
G	TLS_RSA_WITH_RC4_128_SHA (G)	TLS_RSA_WITH_RC4_128_SHA (G)
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (H)

※グループ内の順番は順不同。
※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

Appendix

・1. 本書の見方
・2. IANA で定義された暗号スイートに対する対応表
・3. 付属情報

1. 本書の見方

6.x.1 章記載の表 6.x.1-1 暗号設定内容(デフォルト) の見方を以下に示す。

- CipherSuite 選択優先権

プロトコル	設定状況	CipherSuite 選択優先権	CipherSuite 数
tls1.2	ON	クライアント	7
tls1.1	OFF	-	0
tls1.0	ON	クライアント	5
sslv3	OFF	-	0
sslv2	設定不可	-	-

1

- XXXXXXX で使用可能な暗号スイート

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	ON	OFF	ON	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	OFF	ON	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	OFF	ON	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	OFF	ON	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	OFF	ON	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF

※XXXXXXXは機種名

2

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	非対応	ー	ー	ー	ー
heartbeat	15	非対応	非対応	非対応	ー	ー

3

付図 **1-1** 暗号設定内容(デフォルト)の表記例

付表 **1-1** 暗号設定内容(デフォルト)の表の見方

項番	項目	説明
1	CipherSuite 選択優先権	・「設定状況」欄:設定されていれば「ON」、設定されていなければ「OFF」、設定不可であれば「設定不可」。 ・「CipherSuite 選択優先権」欄:暗号スイートの優先権がサーバにあるかクライアントにあるか。 「サーバ」:サーバ優先。 「クライアント」:クライアント優先。 「-」:当該プロトコルが使用できない場合。 ・「CipherSuite 数」欄:該当する暗号スイートの数(reserved または unassigned の暗号スイートで、有効な数を含む)。
2	使用可能な暗号スイート ※Appendix2 の表も同様	・IANA で規定されている全ての暗号スイートに対してプロトコル毎に「ON」(使用可能)「OFF」(使用不可)を示す。項番 1 の CipherSuite 選択優先権がサーバ優先で、且つ「ON」であった場合、「ON」の隣に暗号スイートの優先順位を示す(例:「ON:1」)。 ・「高」「推」「例」欄:それぞれ設定ガイドラインの「高セキュリティ型」「推奨セキュリティ型」「セキュリティ例外型」のいずれのグループに属するかを示す。いずれにも属さない場合は空欄。 「α」「β」「A」~「H」:設定ガイドラインの要求設定のグループを示す。 「α追加」「β追加」「A 追加」~「F追加」:設定ガイドラインの各グループへの追加または代替を示す。 ・「鍵交換パラメータ」欄:鍵交換の暗号が DH/DHE、ECDH/ECDHE 且つ「ON」であった場合は、複数の鍵長の設定値から通信時のネゴシエーションによって選択された DH/DHE の鍵長、または、ECDH/ECDHE の namedcurve の名前のうち、一つを例示している。該当しない場合は「---」。 ・二重線は鍵交換の種類(DH, DHE, ECDH, ECDHE, KRB5, NULL, PSK, RSA, SRP)の区切りを示す。
3	Extension	・サーバの Extension(拡張機能)の情報をプロトコル毎に「対応」、「非対応」または「-」で示す。 「-」の場合はプロトコルで拡張機能自体がない場合を示す。 「signature_algorithms」:クライアントの使用可能な署名アルゴリズムを受入可否。「対応」の場合で、クライアントが安全性の低い署名アルゴリズムしか受け入れられない場合は、TLS/SSL 通信で使用される暗号がダウングレードする可能性がある。 「heartbeat」:サーバ側での Heartbeat(死活監視)機能が有効か否か。Heartbeat 機能が有効な場合、HeartBleed 攻撃を受ける可能性がある。

※項番は付図 1-1 中の番号。

2. IANA で定義された暗号スイートに対する対応表

IANA で定義された暗号スイート(2016.2.3 現在)への各製品の対応状況を以下に示す。
なお、TLS_EMPTY_RENEGOTIATION_INFO_SCS (0x00,0xff) については、その他の暗号スイートと扱いが異なり、ON になることはない。

2.1 Cisco ASA 5512

付表 **2.1-1 IANA** で定義された暗号スイートへの対応(**Cisco ASA 5512**)

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON:19	ON:3	ON:3	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON:17	ON:1	ON:1	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON:15	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON:7	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON:11	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON:3	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:13	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:5	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:14	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:6	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	追加	A 追加	A 追加	secp256r1	ON:9	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON：1	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON：10	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON：2	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	ON:9	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	ON:7	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	OFF	OFF	ON:6	OFF	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON:8	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:21	ON:5	ON:5	OFF	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:20	ON:4	ON:4	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:18	ON:2	ON:2	OFF	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:16	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:8	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:12	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:4	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.1.1 参照のこと。

2.2 F5 ネットワークス BIG-IP3900

付表 **2.3-1 IANA** で定義された暗号スイートへの対応（**F5** ネットワークス **BIG-IP3900**）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				1024bit	OFF	OFF	ON：19	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				1024bit	OFF	OFF	ON：23	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				1024bit	OFF	OFF	ON：10	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				1024bit	OFF	OFF	ON：16	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				1024bit	OFF	OFF	ON：4	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				1024bit	ON：31	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				1024bit	ON：10	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				1024bit	ON：40	ON：18	ON：22	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	1024bit	ON：19	ON:8	ON:9	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON：30	ON：13	ON：15	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON:9	ON:3	ON:3	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	1024bit	ON：43	ON：22	ON：27	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON：29	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON:8	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	1024bit	ON：41	ON：20	ON：25	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	*β*	A	A	1024bit	ON：28	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	*α*	D	D	1024bit	ON:7	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	ON：20	ON:9	ON：11	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	ON：34	ON：14	ON：17	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	ON：13	ON:4	ON:5	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	ON：33	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	ON：12	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	ON：32	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	ON：11	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON：18	ON：7	ON：8	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON：27	ON：12	ON：14	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON：6	ON：2	ON：2	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON：17	ON：6	ON：7	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON：26	ON：11	ON：13	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:5	ON:1	ON:1	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON：25	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:4	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON：24	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:3	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON：23	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:2	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON：22	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:1	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON：39	ON：17	ON：21	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON：38	ON：16	ON：20	OFF	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	ON：19	ON：24	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON：21	ON：10	ON：12	OFF	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON：37	ON：15	ON：18	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON：16	ON：5	ON：6	OFF	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON：36	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON：15	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON：44	ON：23	ON：28	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON：42	ON：21	ON：26	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON：35	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON：14	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00, 0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00, 0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.2.1 参照のこと。

2.3 A10 ネットワークス Thunder 3030S

付表 **2.4-1 IANA** で定義された暗号スイートへの対応
（A10 ネットワークス Thunder 3030S、RSA 証明書設定時）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	----	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON	ON	ON	ON	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON	ON	ON	ON	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	----	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp384r1	ON	ON	ON	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp384r1	ON	ON	ON	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp384r1	ON	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp384r1	ON	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp384r1	ON	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON	ON	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	ON	ON	ON	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	ON	ON	ON	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	ON	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	ON	ON	ON	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.3.1(1)参照のこと。

付表 **2.4-2 IANA** で定義された暗号スイートへの対応
（A10 ネットワークス Thunder 3030S、ECDSA 証明書設定時）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp384r1	ON	ON	ON	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp384r1	ON	ON	ON	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp384r1	ON	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp384r1	ON	ON	ON	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp384r1	ON	ON	ON	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	OFF	OFF	OFF	OFF	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				----	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.3.1(2)参照のこと。

2.4 日本ラドウェア Alteon VA

付表 **2.5-1 IANA** で定義された暗号スイートへの対応（日本ラドウェア **Alteon VA**）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				2048bit	ON：67	ON：42	ON：42	ON：42	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				2048bit	ON：71	ON：46	ON：46	ON：46	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				2048bit	ON：69	ON：44	ON：44	ON：44	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				2048bit	ON：64	ON：39	ON：39	ON：39	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				2048bit	ON：55	ON：34	ON：34	ON：34	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				2048bit	ON：66	ON：41	ON：41	ON：41	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				2048bit	ON：63	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				2048bit	ON：54	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				2048bit	ON：56	ON：35	ON：35	ON：35	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				2048bit	ON：65	ON：40	ON：40	ON：40	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				2048bit	ON：62	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				2048bit	ON：53	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				512bit	ON：76	ON：51	ON：51	ON：51	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				512bit	ON：75	ON：50	ON：50	ON：50	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				2048bit	ON：70	ON：45	ON：45	ON：45	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	2048bit	ON：68	ON：43	ON：43	ON：43	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	2048bit	ON：59	ON：36	ON：36	ON：36	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	2048bit	ON：51	ON：32	ON：32	ON：32	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	2048bit	ON：61	ON：38	ON：38	ON：38	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	2048bit	ON：58	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	2048bit	ON：50	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	2048bit	ON：52	ON：33	ON：33	ON：33	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				2048bit	ON：60	ON：37	ON：37	ON：37	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	2048bit	ON：57	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	2048bit	ON：49	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				512bit	ON：74	ON：49	ON：49	ON：49	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	ON：45	ON：29	ON：29	ON：29	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	ON：33	ON：17	ON：17	ON：17	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	ON：39	ON：23	ON：23	ON：23	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	ON：24	ON：10	ON：10	ON：10	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	ON：10	ON：4	ON：4	ON：4	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				secp256k1	ON：44	ON：28	ON：28	ON：28	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				secp256k1	ON：32	ON：16	ON：16	ON：16	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				secp256k1	ON：38	ON：22	ON：22	ON：22	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				secp256k1	ON：21	ON：9	ON：9	ON：9	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				secp256k1	ON：7	ON：3	ON：3	ON：3	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	ON：23	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	ON：9	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	ON：22	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	ON：8	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				secp256k1	ON：43	ON：27	ON：27	ON：27	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				secp256k1	ON：31	ON：15	ON：15	ON：15	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				secp256k1	ON：37	ON：21	ON：21	ON：21	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256k1	ON：20	ON：8	ON：8	ON：8	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256k1	ON：6	ON：2	ON：2	ON：2	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				secp256k1	ON：42	ON：26	ON：26	ON：26	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256k1	ON：30	ON：14	ON：14	ON：14	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256k1	ON：36	ON：20	ON：20	ON：20	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256k1	ON：19	ON：7	ON：7	ON：7	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256k1	ON：5	ON：1	ON：1	ON：1	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256k1	ON：18	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256k1	ON：4	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256k1	ON：17	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256k1	ON：3	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256k1	ON：16	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256k1	ON：2	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256k1	ON：15	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256k1	ON：1	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	ON：48	ON：31	ON：31	ON：31	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	ON：47	ON：30	ON：30	ON：30	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON：35	ON：19	ON：19	ON：19	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON：34	ON：18	ON：18	ON：18	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	ON：41	ON：25	ON：25	ON：25	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON：40	ON：24	ON：24	ON：24	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON：27	ON：11	ON：11	ON：11	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON：13	ON:5	ON:5	ON:5	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	ON：46	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON：26	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON：12	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON：29	ON：13	ON：13	ON：13	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON：14	ON:6	ON:6	ON:6	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	ON：28	ON：12	ON：12	ON：12	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON：25	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON：11	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	ON：73	ON：48	ON：48	ON：48	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	ON：72	ON：47	ON：47	ON：47	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.4.1 参照のこと。

2.5 富士通 IPCOM EX2700 IN

付表 **2.6-1 IANA** で定義された暗号スイートへの対応（富士通 **IPCOM EX2700 IN**）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON	ON	ON	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON	ON	ON	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON	ON	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	ON	ON	ON	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	ON	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	ON	ON	ON	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	ON	ON	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	ON	ON	OFF	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	ON	ON	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	ON	ON	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.5.1 参照のこと。

2.6 NEC InterSecVM/LB V3.0 for VMWare

付表 2.7-1 IANA で定義された暗号スイートへの対応
（NEC InterSecVM/LB V3.0 for VMWare、RSA 証明書設定時）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				512bit	OFF	OFF	ON	ON	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				512bit	OFF	OFF	ON	ON	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	1024bit	OFF	OFF	ON	ON	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				1024bit	OFF	OFF	ON	ON	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				512bit	OFF	OFF	ON	ON	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	ON
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	OFF	OFF	ON	ON	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	ON	ON	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	OFF	OFF	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	OFF	OFF	ON	ON	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	ON	ON	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	ON	ON	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	ON
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	ON
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	ON	ON	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				----	OFF	OFF	ON	ON	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	ON	ON	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				----	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.6.1 参照のこと。

2.7 Array Networks APV 2600

付表 **2.8-1 IANA** で定義された暗号スイートへの対応
（**Array Networks APV 2600**、**RSA** 証明書設定時）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:8	OFF	ON:7	ON:7	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:9	OFF	ON:8	ON:8	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:10	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:11	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:12	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:13	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:1	OFF	ON:1	ON:1	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:2	OFF	ON:2	ON:2	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON:3	ON:3	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:3	OFF	ON:4	ON:4	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:4	OFF	ON:5	ON:5	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:5	OFF	ON:6	ON:6	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:7	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	----	OFF	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				----	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.7.1(1)参照のこと。

付表 **2.8-2 IANA** で定義された暗号スイートへの対応
(Array Networks APV 2600、ECDSA 証明書設定時**)**

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	----	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	----	OFF	OFF	OFF	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	----	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:1	OFF	ON:1	ON:1	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:2	OFF	ON:2	ON:2	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:3	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:4	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:5	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:6	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	OFF	OFF	OFF	OFF	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				----	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.7.1(2)参照のこと。

2.8 日立製作所 Hitachi Load Balancer EL130

付表 **2.14-1 IANA** で定義された暗号スイートへの対応
（日立製作所 **Hitachi Load Balancer EL130**）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON	OFF	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	OFF	ON	ON	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	OFF	ON	ON	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	OFF	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	OFF	ON	ON	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				----	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				----	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.8.1 参照のこと。

2.9 Barracuda Load Balancer ADC

付表 **2.10-1 IANA** で定義された暗号スイートへの対応（**Barracuda Load Balancer ADC**）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	2048bit	ON : 31	ON : 15	ON : 15	ON : 1	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	2048bit	ON : 23	ON : 9	ON : 9	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	2048bit	ON : 12	ON : 3	ON : 3	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	2048bit	ON : 24	ON : 10	ON : 10	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	2048bit	ON : 22	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	2048bit	ON:11	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	2048bit	ON : 13	ON : 4	ON : 4	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				2048bit	ON : 33	ON : 17	ON : 17	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	2048bit	ON : 4	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	2048bit	ON : 1	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				secp256r1	ON : 36	ON : 21	ON : 21	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON : 30	ON : 14	ON : 14	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON : 21	ON : 8	ON : 8	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON : 10	ON : 2	ON : 2	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256r1	ON : 35	ON : 20	ON : 20	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON : 29	ON : 13	ON : 13	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON : 20	ON : 7	ON : 7	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON : 9	ON : 1	ON : 1	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON : 19	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON : 8	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON : 18	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON : 7	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β 追加	A 追加	A 追加	secp256r1	ON : 5	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α 追加	D 追加	D 追加	secp256r1	ON : 2	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β 追加	A 追加	A 追加	secp256r1	ON : 6	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α 追加	D 追加	D 追加	secp256r1	ON : 3	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β 追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α 追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β 追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α 追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON : 38	ON : 23	ON : 23	ON : 5	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON : 37	ON : 22	ON : 22	ON : 4	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	ON : 19	ON : 19	ON : 3	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON : 32	ON : 16	ON : 16	ON : 2	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON : 27	ON : 11	ON : 11	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON : 16	ON : 5	ON : 5	OFF	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON : 26	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON : 15	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON : 28	ON : 12	ON : 12	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON : 17	ON : 6	ON : 6	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	ON : 34	ON : 18	ON : 18	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON : 25	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON : 14	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.9.1 参照のこと。

2.10 Barracuda WAF

付表 **2.11-1 IANA** で定義された暗号スイートへの対応（**Barracuda WAF**）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				secp256r1	ON : 13	ON : 14	ON : 14	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON : 18	ON : 16	ON : 16	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON : 20	ON : 15	ON : 15	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON : 16	ON : 17	ON : 17	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256r1	ON : 14	ON : 10	ON : 10	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON : 19	ON : 12	ON : 12	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON : 21	ON:11	ON:11	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON : 17	ON : 13	ON : 13	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON : 7	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON : 5	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON : 8	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON : 6	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β 追加	A 追加	A 追加	secp256r1	ON : 3	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α 追加	D 追加	D 追加	secp256r1	ON : 1	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β 追加	A 追加	A 追加	secp256r1	ON : 4	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α 追加	D 追加	D 追加	secp256r1	ON : 2	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β 追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α 追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β 追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α 追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON : 28	ON : 1	ON : 1	ON : 1	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON : 15	ON : 9	ON : 9	ON : 4	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	ON : 2	ON : 2	ON : 2	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON : 24	ON : 6	ON : 6	ON : 3	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON : 25	ON : 5	ON : 5	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON : 22	ON : 8	ON : 8	OFF	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON : 12	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON : 11	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	ON : 27	ON : 3	ON : 3	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	ON : 23	ON : 7	ON : 7	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	ON : 26	ON : 4	ON : 4	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON : 10	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON：9	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.10.1 参照のこと。

2.11 Citrix NetScaler MPX 8005c

付表 **2.12-1 IANA** で定義された暗号スイートへの対応
（**Citrix NetScaler MPX 8005c**、**RSA** 証明書設定時）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				2048bit	ON:30	ON:18	ON:18	ON:18	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				2048bit	ON:32	ON:20	ON:20	ON:20	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				2048bit	ON:31	ON:19	ON:19	ON:19	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				2048bit	ON:33	ON:21	ON:21	ON:21	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				2048bit	ON:34	ON:22	ON:22	ON:22	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x17	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				2048bit	ON:29	ON:17	ON:17	ON:17	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	2048bit	ON:20	ON:8	ON:8	ON:8	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	2048bit	ON:18	ON:6	ON:6	ON:6	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	2048bit	ON:17	ON:5	ON:5	ON:5	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	2048bit	ON:14	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	2048bit	ON:13	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	2048bit	ON:16	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	2048bit	ON:15	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	----	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				----	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	----	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				----	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256r1	ON:21	ON:9	ON:9	ON:9	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON:19	ON:7	ON:7	ON:7	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:8	ON:4	ON:4	ON:4	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:7	ON:3	ON:3	ON:3	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON:10	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	secp256r1	ON:9	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON:12	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON:11	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:24	ON:12	ON:12	ON:12	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:23	ON:11	ON:11	ON:11	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	ON:25	ON:13	ON:13	ON:13	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON:22	ON:10	ON:10	ON:10	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:2	ON:2	ON:2	ON:2	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:1	ON:1	ON:1	ON:1	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:4	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:3	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:5	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	ON:26	ON:14	ON:14	ON:14	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	ON:28	ON:16	ON:16	ON:16	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	ON:27	ON:15	ON:15	ON:15	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.11.1 参照のこと。

2.12　セイコーソリューションズ　Netwiser SX-3850

付表 **2.13-1 IANA** で定義された暗号スイートへの対応
（セイコーソリューションズ **Netwiser SX-3850**）

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0x0c	TLS_DH_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0d	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0f	TLS_DH_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x10	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x18	TLS_DH_anon_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1a	TLS_DH_anon_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1b	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x30	TLS_DH_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x31	TLS_DH_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x34	TLS_DH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x36	TLS_DH_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x37	TLS_DH_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3a	TLS_DH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3e	TLS_DH_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3f	TLS_DH_RSA_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x42	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x43	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x46	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x68	TLS_DH_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x69	TLS_DH_RSA_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6c	TLS_DH_anon_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6d	TLS_DH_anon_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x85	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x86	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x89	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x97	TLS_DH_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x98	TLS_DH_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9b	TLS_DH_anon_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa0	TLS_DH_RSA_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa1	TLS_DH_RSA_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa4	TLS_DH_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa5	TLS_DH_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa6	TLS_DH_anon_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa7	TLS_DH_anon_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbb	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbc	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbf	TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc1	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc2	TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc5	TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3e	TLS_DH_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3f	TLS_DH_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x40	TLS_DH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x41	TLS_DH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x46	TLS_DH_anon_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x47	TLS_DH_anon_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x54	TLS_DH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x55	TLS_DH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x58	TLS_DH_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x59	TLS_DH_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5a	TLS_DH_anon_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5b	TLS_DH_anon_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7e	TLS_DH_RSA_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7f	TLS_DH_RSA_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x82	TLS_DH_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x83	TLS_DH_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x84	TLS_DH_anon_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x85	TLS_DH_anon_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0b	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x0e	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x19	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x12	TLS_DHE_DSS_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x13	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA			H	---	OFF	OFF	OFF	OFF	OFF
0x00,0x2d	TLS_DHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x32	TLS_DHE_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x38	TLS_DHE_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x40	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x44	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x45	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x6a	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x87	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x88	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA		D	D	---	OFF	OFF	OFF	OFF	OFF
0x00,0x8e	TLS_DHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8f	TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x99	TLS_DHE_DSS_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9a	TLS_DHE_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0xa2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaa	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xab	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0x00,0xb2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb4	TLS_DHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb5	TLS_DHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbd	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xbe	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A	A	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc3	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xc4	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256		D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x42	TLS_DHE_DSS_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x43	TLS_DHE_DSS_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x44	TLS_DHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x45	TLS_DHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x52	TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x53	TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x56	TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x57	TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x66	TLS_DHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x67	TLS_DHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6c	TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6d	TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7c	TLS_DHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β	A	A	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7d	TLS_DHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α	D	D	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x80	TLS_DHE_DSS_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x81	TLS_DHE_DSS_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x90	TLS_DHE_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x91	TLS_DHE_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x96	TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x97	TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9e	TLS_DHE_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9f	TLS_DHE_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa2	TLS_DHE_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa3	TLS_DHE_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa6	TLS_DHE_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa7	TLS_DHE_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaa	TLS_PSK_DHE_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xab	TLS_PSK_DHE_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x11	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x14	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x01	TLS_ECDH_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x02	TLS_ECDH_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x03	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x04	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x05	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0b	TLS_ECDH_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0c	TLS_ECDH_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0d	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x0e	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0f	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x15	TLS_ECDH_anon_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x16	TLS_ECDH_anon_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x17	TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x18	TLS_ECDH_anon_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x19	TLS_ECDH_anon_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x25	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x26	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x29	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2a	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2d	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2e	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x31	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x32	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4a	TLS_ECDH_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4b	TLS_ECDH_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4e	TLS_ECDH_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4f	TLS_ECDH_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5e	TLS_ECDH_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5f	TLS_ECDH_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x62	TLS_ECDH_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x63	TLS_ECDH_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x74	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x75	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x78	TLS_ECDH_RSA_WITH_CAMELLIA_128_CBC_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x79	TLS_ECDH_RSA_WITH_CAMELLIA_256_CBC_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x88	TLS_ECDH_ECDSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x89	TLS_ECDH_ECDSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8c	TLS_ECDH_RSA_WITH_CAMELLIA_128_GCM_SHA256		C 追加	C 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8d	TLS_ECDH_RSA_WITH_CAMELLIA_256_GCM_SHA384		F 追加	F 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x06	TLS_ECDHE_ECDSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x07	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x08	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x10	TLS_ECDHE_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x2f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x33	TLS_ECDHE_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x34	TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x39	TLS_ECDHE_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3a	TLS_ECDHE_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3b	TLS_ECDHE_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x48	TLS_ECDHE_ECDSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x49	TLS_ECDHE_ECDSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4c	TLS_ECDHE_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x4d	TLS_ECDHE_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5c	TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x5d	TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x60	TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x61	TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x70	TLS_ECDHE_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x71	TLS_ECDHE_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x72	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x73	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x76	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256		A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x77	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384		D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x86	TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x87	TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8a	TLS_ECDHE_RSA_WITH_CAMELLIA_128_GCM_SHA256	β追加	A 追加	A 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8b	TLS_ECDHE_RSA_WITH_CAMELLIA_256_GCM_SHA384	α追加	D 追加	D 追加	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9a	TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9b	TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xac	TLS_ECDHE_ECDSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xad	TLS_ECDHE_ECDSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xae	TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xaf	TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1e	TLS_KRB5_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x1f	TLS_KRB5_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x20	TLS_KRB5_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x21	TLS_KRB5_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x22	TLS_KRB5_WITH_DES_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x23	TLS_KRB5_WITH_3DES_EDE_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x24	TLS_KRB5_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x25	TLS_KRB5_WITH_IDEA_CBC_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x26	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x27	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x28	TLS_KRB5_EXPORT_WITH_RC4_40_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x29	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2a	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2b	TLS_KRB5_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x00	TLS_NULL_WITH_NULL_NULL				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2c	TLS_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8a	TLS_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8b	TLS_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8c	TLS_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x8d	TLS_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa8	TLS_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xa9	TLS_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xae	TLS_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xaf	TLS_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb0	TLS_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb1	TLS_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x64	TLS_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x65	TLS_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6a	TLS_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6b	TLS_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8e	TLS_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x8f	TLS_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x94	TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x95	TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa4	TLS_PSK_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa5	TLS_PSK_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa8	TLS_PSK_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa9	TLS_PSK_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x01,0x00,0x80	SSL_RC4_128_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x03,0x00,0x80	SSL_RC2_CBC_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x05,0x00,0x80	SSL_IDEA_128_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x06,0x00,0x40	SSL_DES_64_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x07,0x00,0xc0	SSL_DES_192_EDE3_CBC_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x01	TLS_RSA_WITH_NULL_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x02	TLS_RSA_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON	OFF	ON	ON	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON	OFF	ON	ON	OFF
0x00,0x07	TLS_RSA_WITH_IDEA_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x09	TLS_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	ON	ON	OFF
0x00,0x0a	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H	---	ON	OFF	ON	ON	OFF
0x00,0x2e	TLS_RSA_PSK_WITH_NULL_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON	OFF	ON	ON	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON	OFF	ON	ON	OFF
0x00,0x3b	TLS_RSA_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0x41	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0x84	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA		E	E	---	OFF	OFF	OFF	OFF	OFF
0x00,0x92	TLS_RSA_PSK_WITH_RC4_128_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x93	TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x96	TLS_RSA_WITH_SEED_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON	OFF	OFF	OFF	OFF
0x00,0xac	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xad	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb8	TLS_RSA_PSK_WITH_NULL_SHA256				---	OFF	OFF	OFF	OFF	OFF
0x00,0xb9	TLS_RSA_PSK_WITH_NULL_SHA384				---	OFF	OFF	OFF	OFF	OFF
0x00,0xba	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0x00,0xc0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3c	TLS_RSA_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x3d	TLS_RSA_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x50	TLS_RSA_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x51	TLS_RSA_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x68	TLS_RSA_PSK_WITH_ARIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x69	TLS_RSA_PSK_WITH_ARIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6e	TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x6f	TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x7a	TLS_RSA_WITH_CAMELLIA_128_GCM_SHA256		B	B	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x7b	TLS_RSA_WITH_CAMELLIA_256_GCM_SHA384		E	E	---	OFF	OFF	OFF	OFF	OFF
0xc0,0x92	TLS_RSA_PSK_WITH_CAMELLIA_128_GCM_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x93	TLS_RSA_PSK_WITH_CAMELLIA_256_GCM_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x98	TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x99	TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9c	TLS_RSA_WITH_AES_128_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x9d	TLS_RSA_WITH_AES_256_CCM				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa0	TLS_RSA_WITH_AES_128_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0xc0,0xa1	TLS_RSA_WITH_AES_256_CCM_8				---	OFF	OFF	OFF	OFF	OFF
0x02,0x00,0x80	SSL_RC4_128_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x04,0x00,0x80	SSL_RC2_CBC_128_CBC_EXPORT40_WITH_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1a	TLS_SRP_SHA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1b	TLS_SRP_SHA_RSA_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1c	TLS_SRP_SHA_DSS_WITH_3DES_EDE_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1d	TLS_SRP_SHA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1e	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x1f	TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0xc0,0x22	TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
0x00,0xff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV				---	OFF	OFF	OFF	OFF	OFF

※デフォルトの設定は 6.12.1 参照のこと。

3. 付属情報

3.1 Cisco ASA 5512

- 製品情報
  CISCO ASA 5512 ASA Version: 9.5(2)5

- 参考情報
  ASDM を使用した Cisco ASA 5500 シリーズ コンフィギュレーション ガイド
  Cisco ASA 5505 クイック スタート ガイド Version 8.0
  Cisco ASA Series General Operations ASDM Configuration Guide, 7.5
  Cisco ASA Series VPN ASDM Configuration Guide, 7.5

3.2 F5 ネットワークス BIG-IP3900

- 製品情報
  BIG-IP 3900 Ver.12.0.0

- 参考情報
  BIG-IP LTM セットアップガイド（v15.5.1 対応）PEOLD.ver2.0

3.3 A10 ネットワークス Thunder 3030S

- 製品情報
  A10 ネットワークス Thunder 3030S ソフトウェアバージョン: 2.7.2-P7-SP3(build: 3)

- 参考情報
  A10networks Thunder クイックスタートガイド
  A10-DG-Apache_Web_Server_2.2.pdf
  A10_Thunder_272_GUI_Ref-2014_06_16.pdf
  A10_Thunder_272_CLI_Ref-2015_05_14.pdf

- 今後のサポート予定
  サポート暗号化スイートは、今後のリリースにて拡張予定。

3.4 日本ラドウェア Alteon VA

- 製品情報
  日本ラドウェア Alteon VA Version: 30.2.1.100

- 参考情報
  Radware Alteon Installation and Maintenance Guide
  Alteon Command Line Interface Application Guide
  Alteon Command Line Interface Reference Guide
  Alteon Web Based Management Application Guide

3.5 富士通 IPCOM EX2700 IN

- 製品情報
  富士通 IPCOM EX2700 IN ファームウェア版数: E20L32 NF0201 B01
  (搭載オプション 1000BASE-T インターフェースカード B、暗号カード C、SSL アクセラレータオプション)

  SSL アクセラレータ機能を使用するには､暗号カードと SSL アクセラレータオプションが必要。

  暗号カードには 3 種類あり、今回は「暗号カード C」を搭載している。
  「暗号カード A2」「暗号カード B」では以下の暗号スイートが未サポートとなる。
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

  ・以下の機種の SSL アクセラレータ機能で「暗号カード A2」「暗号カード B」「暗号カード C」を利用可能。
  IPCOM EX2700 SC、IPCOM EX2700 LB、IPCOM EX2700 IN、
  IPCOM EX2500 SC、IPCOM EX2500 LB、IPCOM EX2500 IN

  ・以下の機種の SSL アクセラレータ機能で「暗号カード A2」「暗号カード B」を利用可能。
  IPCOM EX2300 SC、IPCOM EX2300 LB、IPCOM EX2300 IN

- 参考情報
  FUJITSU Network IPCOM EX2700 クイックスタートガイド(E20L32 Rev.1)
  FUJITSU Network IPCOM EX シリーズ ユーザーズガイド E20L32
  FUJITSU Network IPCOM EX シリーズ コンソールリファレンスガイド E20L32

- 今後のサポート予定
  ・2016 年 9 月以降にサポート予定の暗号スイート
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (暗号カード C のみ)
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (暗号カード C のみ)
  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (暗号カード C のみ)
  TLS_RSA_WITH_AES_128_GCM_SHA256
  TLS_RSA_WITH_AES_256_GCM_SHA384

  ・2016 年 9 月以降にサポート予定の機能
  サーバクライアントの優先順位の設定機能
  暗号スイートの優先順位の設定機能

3.6 NEC InterSecVM/LB V3.0 for VMWare

- 製品情報
  NEC InterSecVM/LB V3.0 for VMware
  InterSecVM/LB V3.0 for VMware 用アップデートモジュール Rel 1.0 適用済
  ※InterSecVM/LB V3.0 for VMware 用 アップデートモジュール Rel 3.1 を適用することで TLS1.1、TLS1.2 が利用可能となる。

- 参考情報
  InterSecVM/LB V3.0 for VMware セットアップ手順説明書
  InterSecVM/LB V3.0 for VMware ユーザーズガイド

3.7 Array Networks APV 2600

- 製品情報
  Array Networks APV 2600
  ソフトウェアビルド情報 ArrayOS Rel.APV.8.6.0.14 build on Thu Mar 3 08:30:21 2016

- 参考情報
  ArrayOS APV 8.6 User Guide

3.8 日立製作所 Hitachi Load Balancer EL130

- 製品情報
  日立製作所 Hitachi Load Balancer EL130 ソフトウェアバージョン: 2.7.1-P6(build: 143)

- 参考情報
  クイックスタートガイド

3.9 Barracuda Load Balancer ADC

- 製品情報
  Barracuda Load Balancer ADC 340 ファームウェアバージョン: 6.0.0.005 (2016-04-20 05:29:37)

- 参考情報
  Barracuda Load Balancer ADC クイックスタートガイド
  Barracuda Load Balancer ADC オンラインマニュアル

3.10 Barracuda WAF

- 製品情報
  Barracuda Web Application Firewall 360 ファームウェアバージョン: 8.1.0.009 (2016-05-04 22:58:07)

- 参考情報
  Barracuda Web Application Firewall　日本語セットアップガイド

3.11　Citrix NetScaler MPX 8005c

- 製品情報
  Citrix NetScaler MPX 8005c ファームウェアバージョン: NS11.0 Build 64.34.nc

- 参考情報
  NetScaler 初期設定＆ロードバランサ機能設定ガイド Ver.1.6
  SSL Offload 機能設定ガイド Ver.1.6

3.12 セイコーソリューションズ Netwiser SX-3850

- 製品情報
  Netwiser SX-3850 ファームウェアバージョン v7.3.20 built on 2016/03/16 17:03 (secondary v7.3.20)

- 参考情報
  SX-3840,45,50 取扱説明書(第 1.1 版)
  Netwiser SX-38 シリーズ　導入・運用の手引(第 2.1 版)
  Netwiser SX-38 シリーズ コマンドリファレンス(第 1.4 版)

- 製品シリーズについて
  下記製品は SX-38xx シリーズ共通。
  SX-3850/SX-3845/SX-3840/SX-3820

3.13 Imperva SecureSphere X2010

- 製品情報
  Imperva SecureSphere X2010　バージョン:11.0.0.30 Enterprise Edition

- 参考情報
  Imperva SecureSphere スタートアップガイド
  Configuring Common Criteria Compliance
  v11.0-Administration-Guide
  v11.0-Web-Security-User-Guide

※本製品には「ブリッジモード（透過モード）」と「リバースプロキシモード」があり、通常は「ブリッジモード」で使用する（「リバースプロキシモード」は非推奨）。
但し、「ブリッジモード」は暗号関連の設定が Web サーバの設定に依存するため、以降の調査結果は、「リバースプロキシモード」で調査した結果を記載している。「リバースプロキシモード」における制約事項は下記を参照のこと。

- リバースプロキシモードでの制約事項
  ・2MB 以上の非マルチパート Post リクエストは、リバースプロキシ構成では処理できず Drop される挙動となる。
  ・Referer ヘッダに大文字が含まれていた場合、SecureSphere はこれらを小文字に書き換える。
  ・Tag Vlan, リンクアグリゲーション、ハードウェアバイパスは未サポート。
  ・高負荷時には SecureSphere は通信を Drop する挙動となる。
  ※代理店（マクニカネットワークス株式会社）による経験値。