ASA5512

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

1. 調査結果詳細

※本書は「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」の1 部分を取り出したものである。調査の背景、調査方法等は報告書を参考にされたい。

1.x.1 章記載の表 1.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 1 暗号設定内容（デフォルト）の表記例

表 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 1 中の番号。

1.1. 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。**1.1.1 デフォルトでの暗号設定内容の調査**、および、**1.1.3 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。

1.1.1. デフォルトでの暗号設定内容の調査

表 1.1.1-1 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

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
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	ー	ー	ー	ー
heartbeat	15	対応	対応	対応	ー	ー

1.1.2. 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ー（2）Device Managementー（3）Advancedー（4）SSL settings をクリックして、（5）SSL settings 画面を表示する。

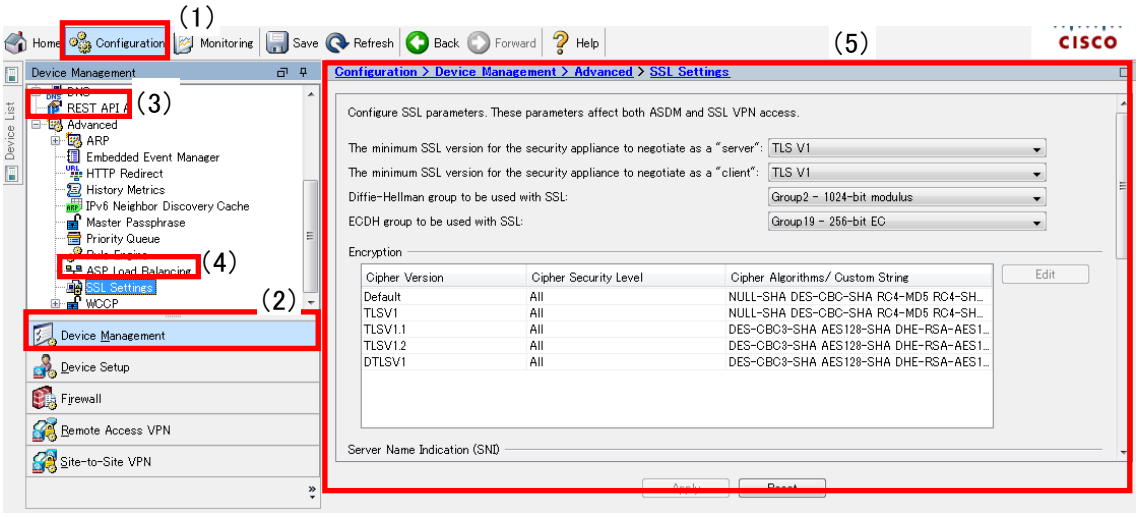

図 1.1.2-1 SSL Settings 画面-1

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。

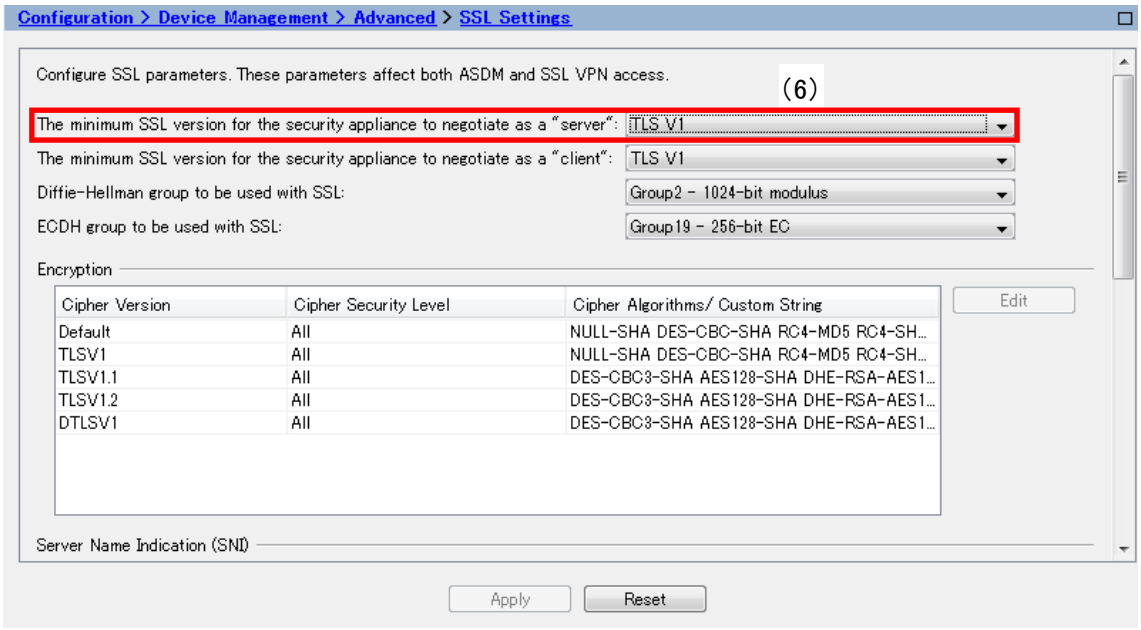

図 1.1.2-2　SSL Settings 画面（プロトコル）-1

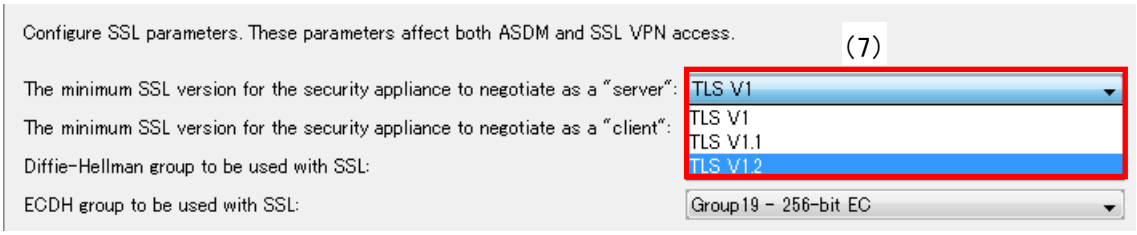

図 1.1.2-3　SSL Settings 画面-2

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。

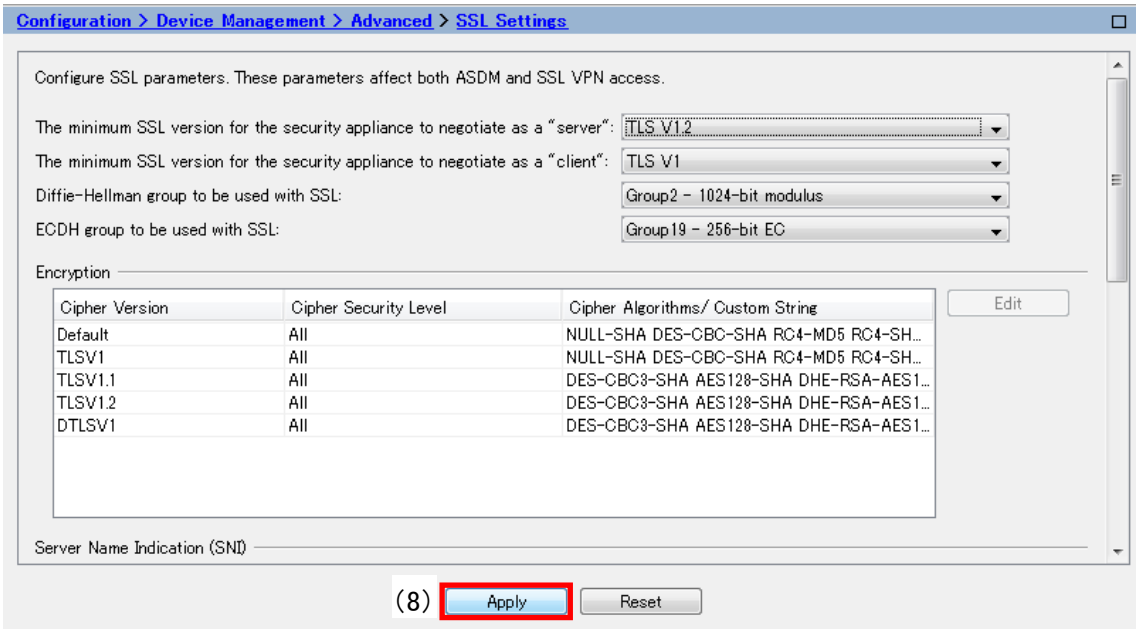

図 1.1.2-4　SSL Settings 画面（プロトコル）-2

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。

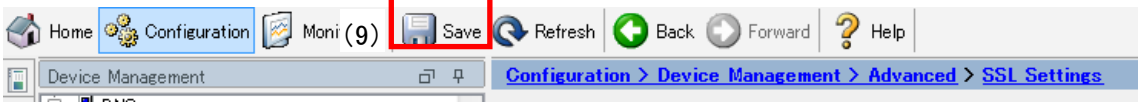

図 1.1.2-5　SSL Settings 画面（プロトコル）-3

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。

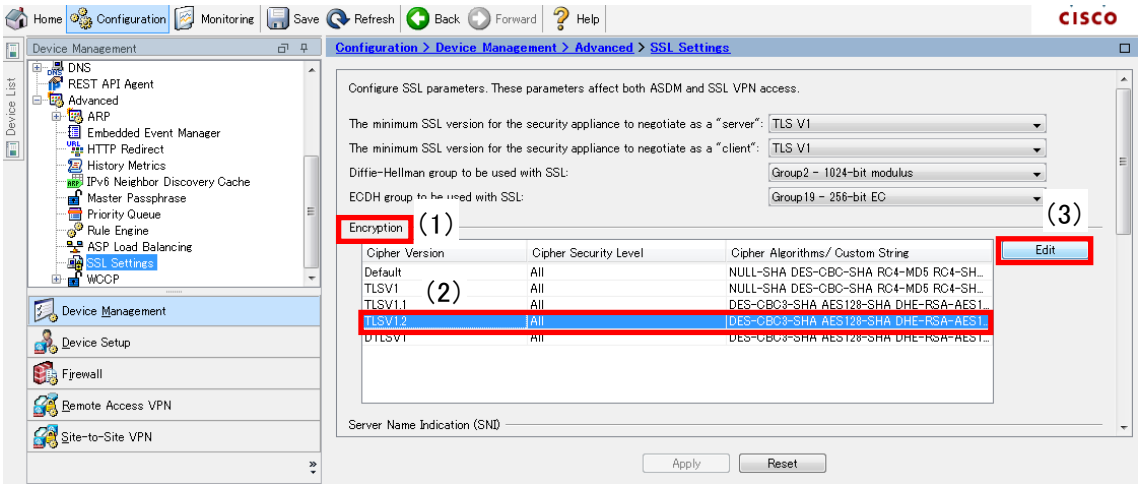

図 1.1.2-6　SSL Settings 画面（暗号スイート）-1

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。

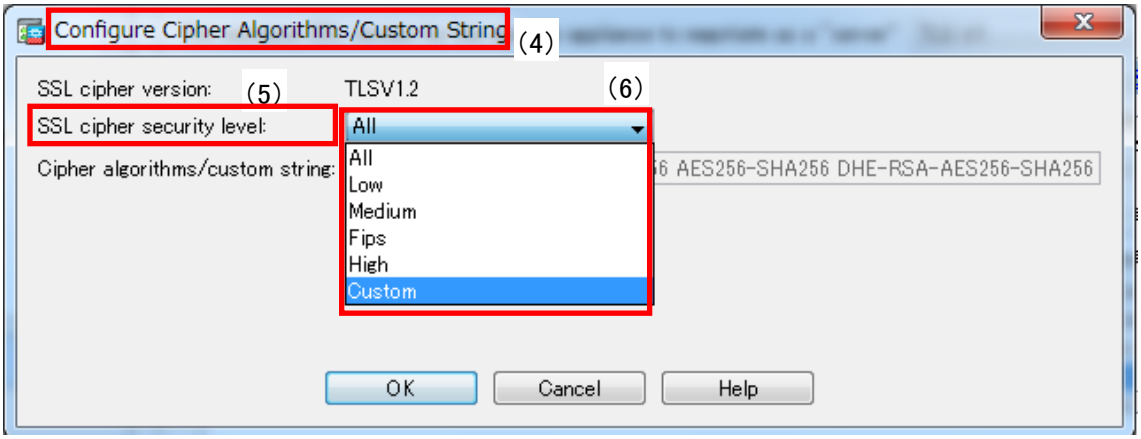

図 1.1.2-7　SSL Settings 画面（暗号スイート）-2

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。

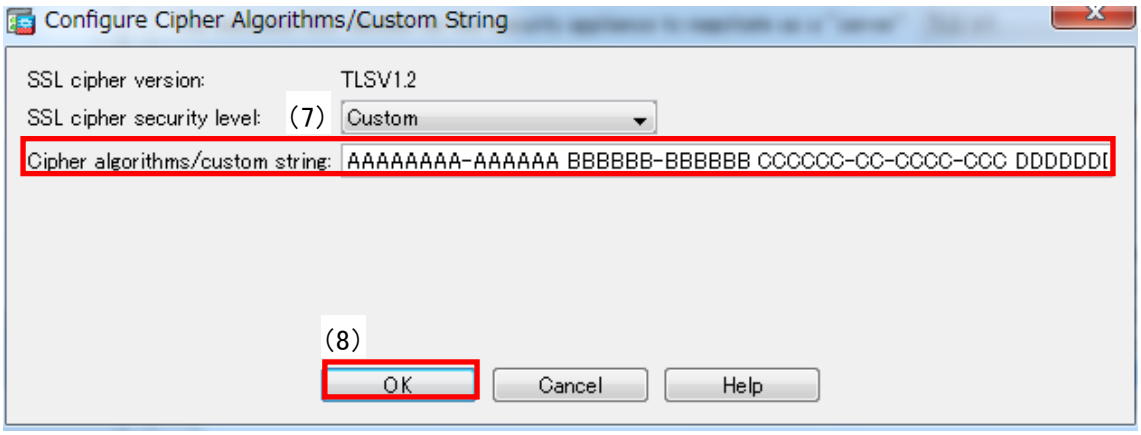

図 1.1.2-8　SSL Settings 画面（暗号スイート）-3

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。

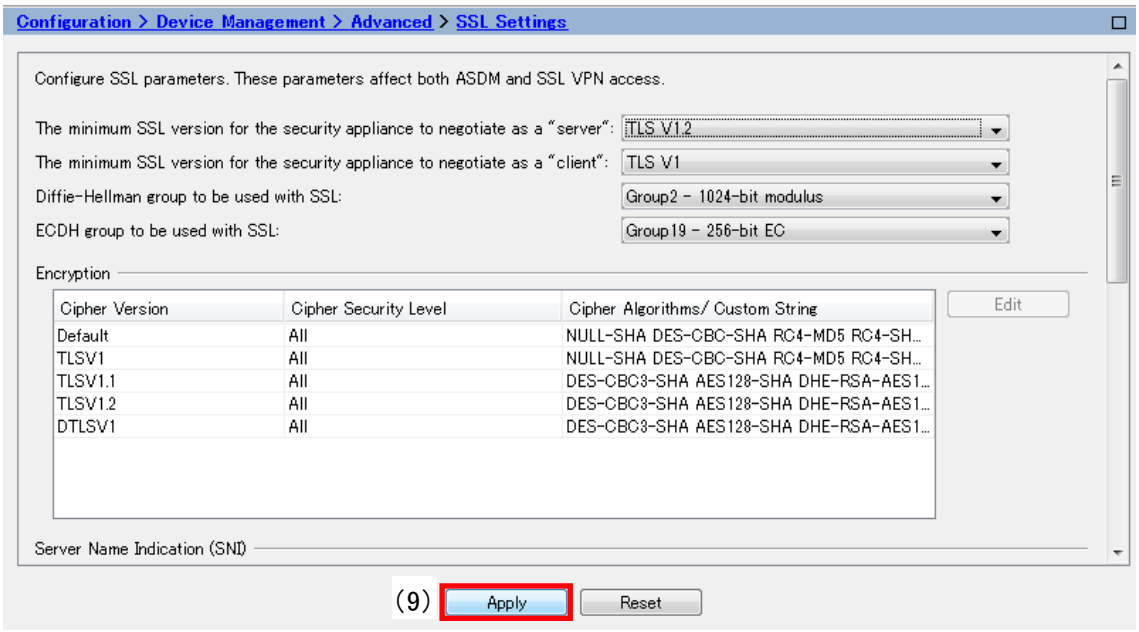

図 1.1.2-9　SSL Settings 画面（暗号スイート）-4

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 1.1.2-10　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」

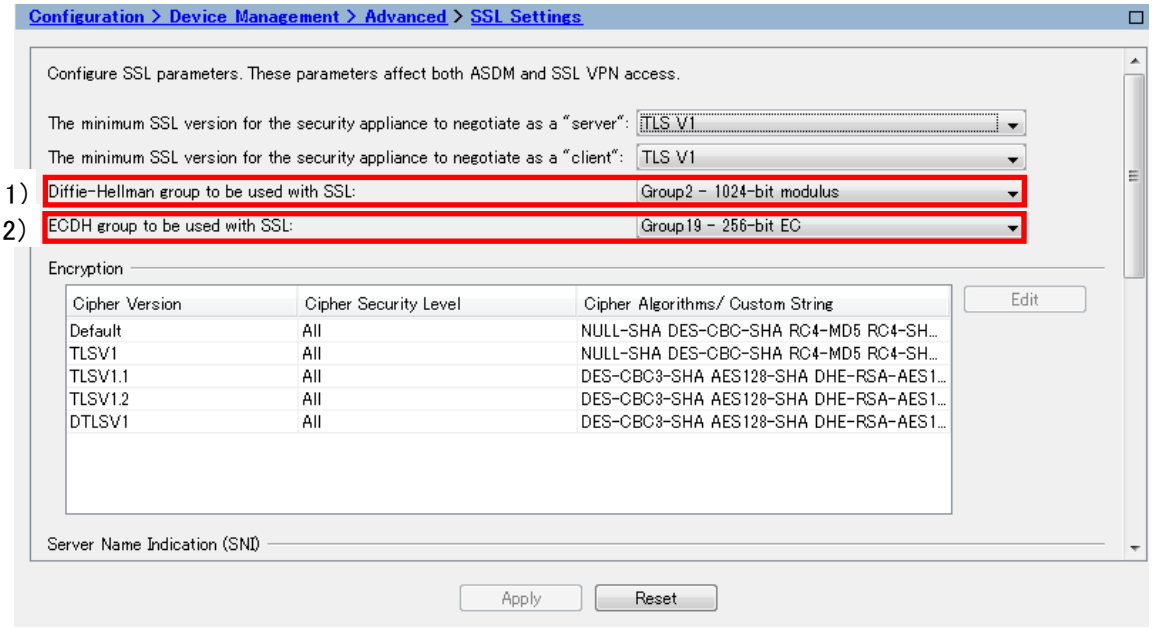

図 1.1.2-11　SSL Settings 画面（暗号スイート）-6

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。

1.1.3. 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

1.1.3.1. 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 1.1.2-3　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

1.1.2.II.A で TLSV1.2 を選択して、1.1.2.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

1.1.2.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 1.1.3.1-1　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 1.1.3.1-1　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 1.1.2-3　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 1.1.2-8　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-SHA256

III.　DH/DHE、ECDH/ECDHE の鍵長

図 1.1.2-11　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 1.1.3.1-2 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。

1.1.3.2. 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 1.1.2-3　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

1.1.2.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

1.1.2.III 図 1.1.2-11　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 1.1.3.2-1 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 1.1.2-3 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 1.1.2-8　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 1.1.2-11　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 1.1.3.2-2　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 1.1.3.2-2　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。

1.1.3.3. 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。

付属情報

- **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