APV2600

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

2

※XXXXXXXは機種名

- 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	―	―

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. 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、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**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。

1.1.1. 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 1.1.1-1 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	―	―
tls1.0	ON	サーバ	7
sslv3	OFF	―	0
sslv2	設定不可	―	―

- 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 1.1.1-2　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

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)　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 1.1.2-1　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 1.1.2-2　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ー(2)SSL 設定ー(3)SSL 仮想リストー(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 1.1.2-3　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。

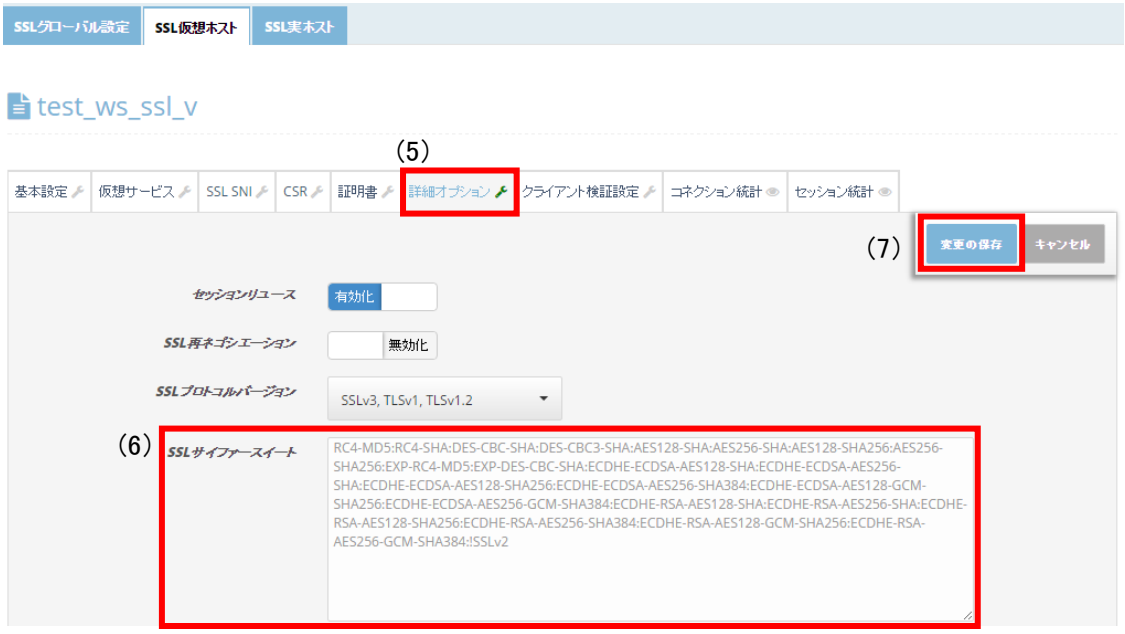

図 1.1.2-4　SSL サイファースイート設定画面

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
1.1.2.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。

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) 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。
※1.1.1 (1)RSA 証明書設定時 表 1.1.1-1 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
1.1.1 (1)RSA 証明書設定時 表 1.1.1-1 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
1.1.1 (1)RSA 証明書設定時 表 1.1.1-1 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

1.1.1 (1)RSA 証明書設定時 表 1.1.1-1　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 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、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 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、RSA 証明書設定時）のとおりである。

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、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 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-4　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 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、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 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、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。
※1.1.1 (2)ECDSA 証明書設定時 表 1.1.1-2 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
1.1.1 (2)ECDSA 証明書設定時 表 1.1.1-2 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。
※1.1.1 (2) ECDSA 証明書設定時 表 1.1.1-2 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
1.1.1 (2)ECDSA 証明書設定時 表 1.1.1-2 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
1.1.1 (2) ECDSA 証明書設定時 表 1.1.1-2 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 1.1.3.1-3　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 1.1.3.1-3　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 1.1.3.1-3　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 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-4　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 1.1.3.1-4 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 1.1.3.1-4 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。

1.1.3.2. 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、1.1.3.1 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 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、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 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、RSA 証明書設定時）のとおりである。

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、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 1.1.2-2 参照）

II. 暗号スイート
図 1.1.2-4 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 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、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 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、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、1.1.3.1 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 1.1.3.2-3　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

1.1.3.2-3　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 1.1.3.2-3 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 1.1.3.2-3　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 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-4　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 1.1.3.2-4 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 1.1.3.2-4 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。

1.1.3.3. 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、1.1.3.1 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 1.1.3.3-1　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 1.1.3.3-1　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 1.1.3.3-1　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 1.1.2-2 参照）

II. 暗号スイート
図 1.1.2-4　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 1.1.3.3-2　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 1.1.3.3-2　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、1.1.3.1 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 1.1.3.3-3　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 1.1.3.3-3　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 1.1.3.3-3　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 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-4　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 1.1.3.3-4 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 1.1.3.3-4 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。

付属情報

- 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