Alteon VA

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. 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。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	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

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	---	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
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

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	---	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

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)「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。

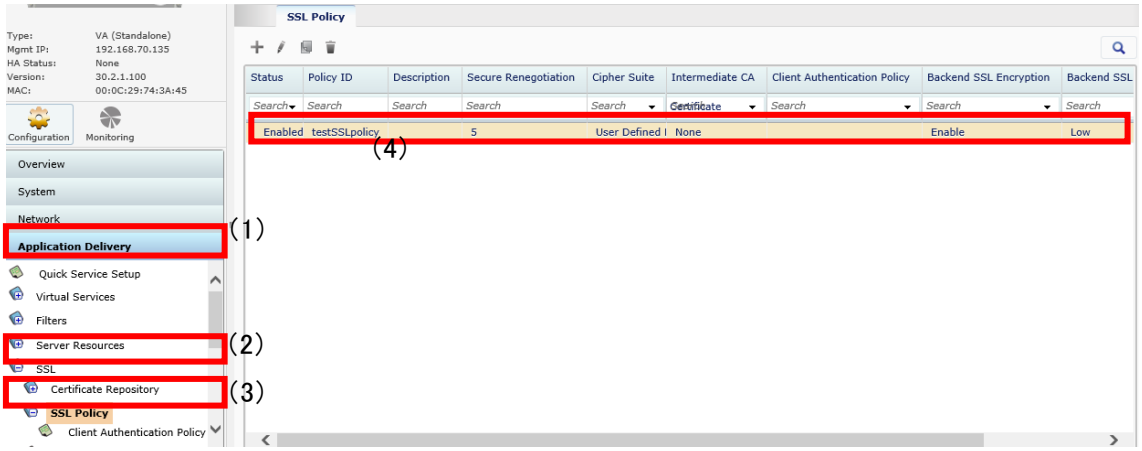

図 6.4.2-1　SSL Policy 一覧画面-1

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。

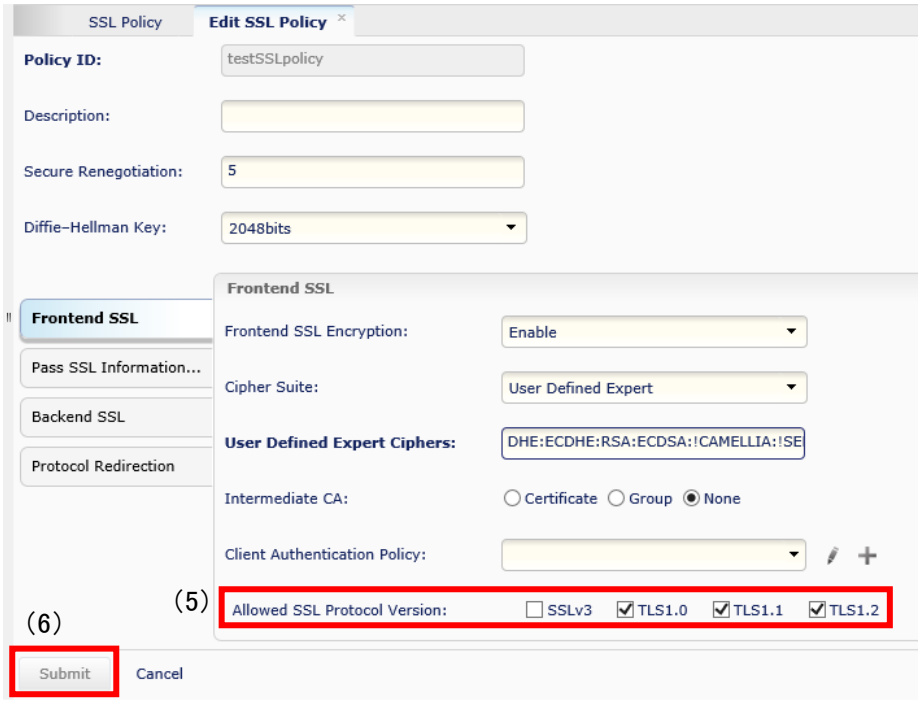

図 1.1.2-2　SSL Policy 編集画面-1

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。

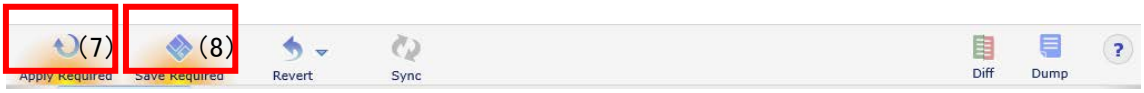

図 1.1.2-3 SSL Policy 編集画面-2

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。

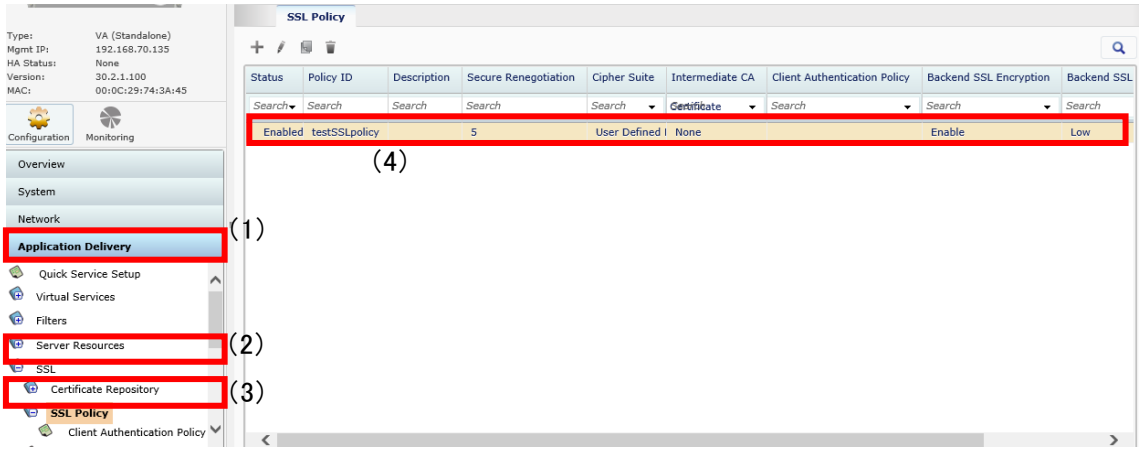

図 1.1.2-4 SSL Policy 一覧画面-2

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。

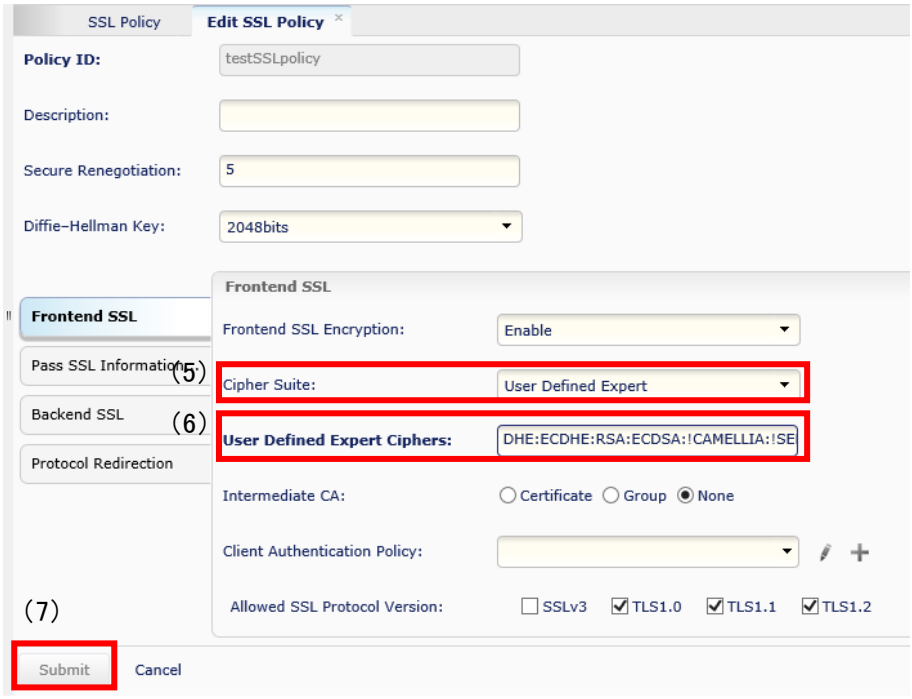

図 1.1.2-5　SSL Policy 編集画面-3

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。

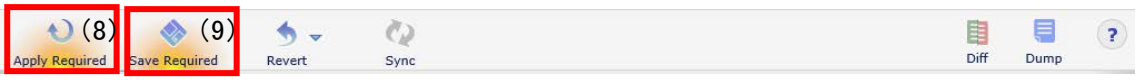

図 1.1.2-6　SSL Policy 編集画面-4

III. DH/DHE、ECDH/ECDHE の鍵長の設定

DH/DHE の鍵長は、図 1.1.2-5　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。

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

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 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-5　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 1.1.2-5　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 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。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 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）

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号スイート	1	TLS_RSA_WITH_AES_128_GCM_SHA256
		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 1.1.2-2 参照）

II.　暗号スイート

図 1.1.2-5　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 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 1.1.3.1-2 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)
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。

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

TLS1.2、TLS1.1、TLS1 のチェックを入れる。

SSLv3 のチェックを外す。

（図 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-5 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 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） 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 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） 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）

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 1.1.2-5　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

1.1.3.3. 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 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-5　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 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） 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 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）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）

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）

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_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）
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 1.1.2-2 参照）

II. 暗号スイート

図 1.1.2-5　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 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） 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 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）のとおりである。

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）

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）

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_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）
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 1.1.2-5　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。

付属情報

- 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