InterSec VM/LB V3.0 for VMware

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. 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、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、RSA 証明書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、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

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
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
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	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) SSH または vSphere Client で直接（1）「/etc/pound/mkpoundcfg.sh」を編集(図 1.1.2-1　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 1.1.2-2　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。

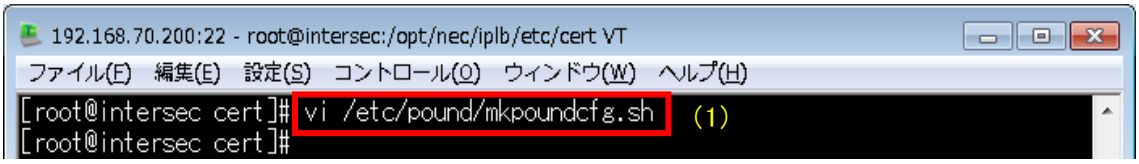

図 1.1.2-1　プロトコルバージョン指定画面-1

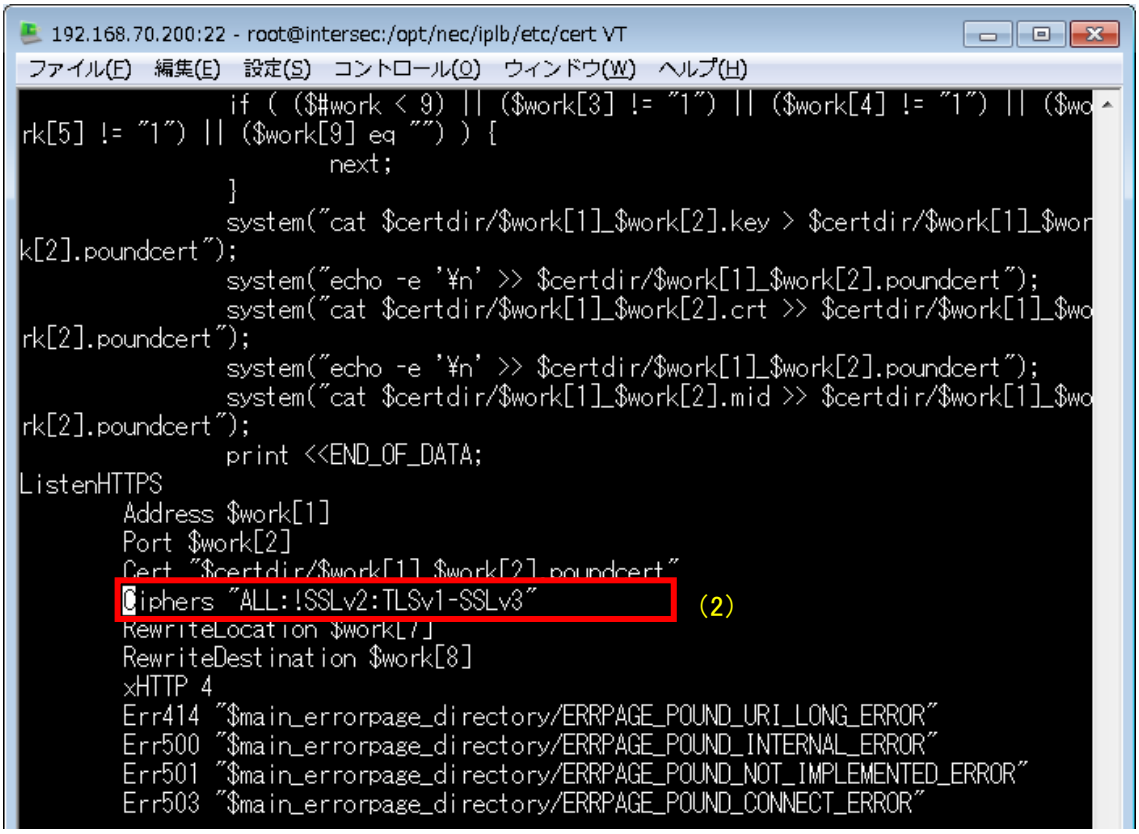

図 1.1.2-2　プロトコルバージョン指定画面-2

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。

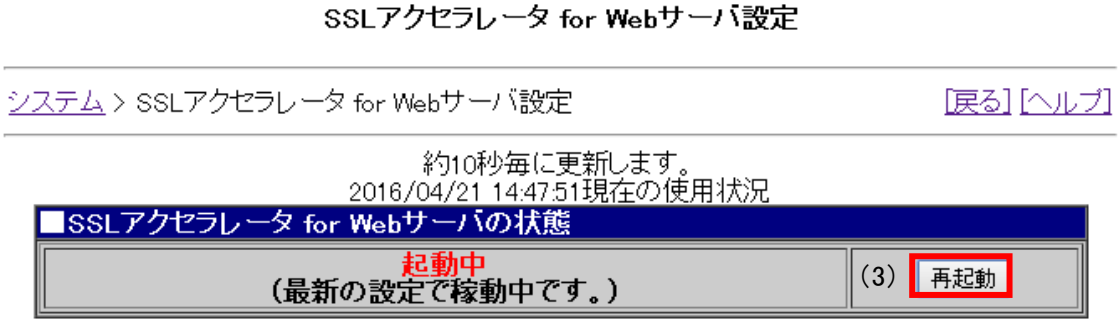

図 1.1.2-3　SSL アクセラレータ for Web サーバの状態画面（プロトコル設定）

II.　暗号スイートの設定

A)　1.1.2.I.A)と同様、SSH または vSphere Client で直接（1）「/etc/pound/mkpoundcfg.sh」を編集(図 1.1.2-4　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）。

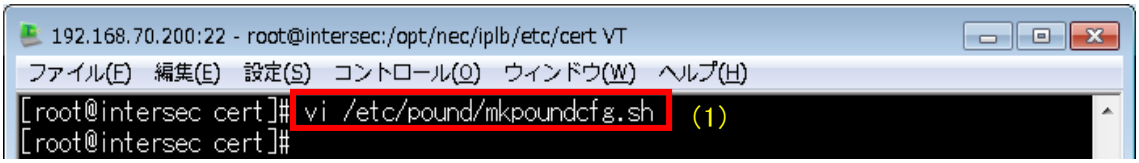

図 1.1.2-4 暗号スイート設定画面-1

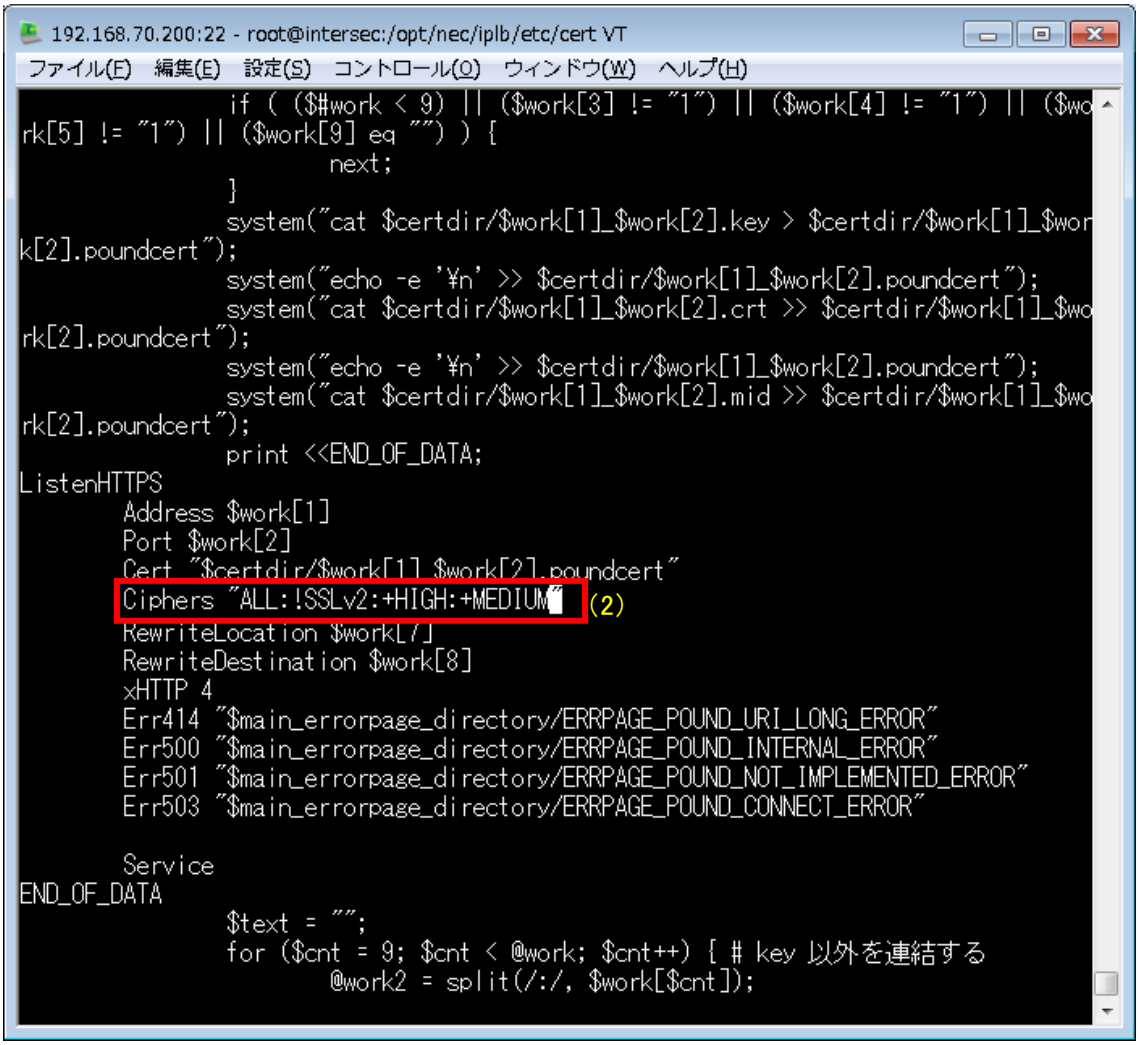

図 1.1.2-5 暗号スイート設定画面-2

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。

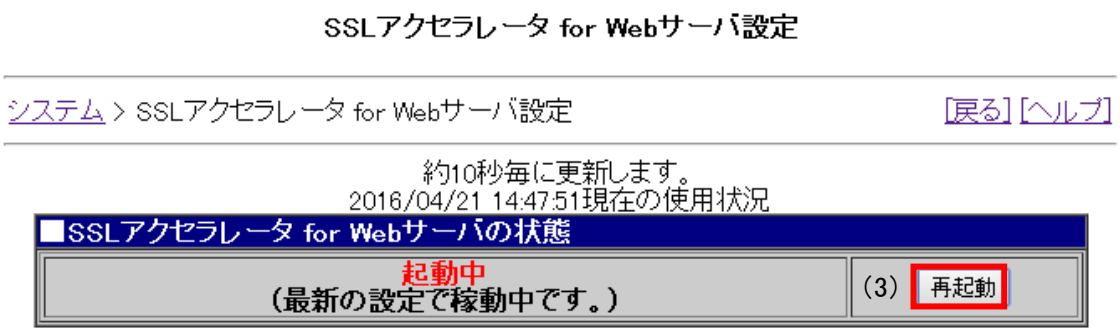

図 1.1.2-6　SSL アクセラレータ for Web サーバの状態画面（暗号スイート）

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。

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

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。

1.1.3.2. 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

1.1.2.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

1.1.2.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 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 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 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）	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

1.1.2.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

1.1.2.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 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 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 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）	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。

1.1.3.3. 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

1.1.2.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

1.1.2.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 1.1.3.3-1　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 1.1.3.3-1　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

1.1.2.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

1.1.2.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 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） 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 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）	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。

付属情報

- 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