Hitachi LoadBalancer EL130

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. 日立製作所 Hitachi Load Balancer EL130

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

なお、サーバ証明書は、RSA 証明書のみが設定可能であり、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）

- CipherSuite 選択優先権

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

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

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

- Extension

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

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）コンフィグー（2）SLBー（3）テンプレートー（4）SSLー（5）作成してあるクライアント SSL テンプレート（例：test_ssl_rsa）をクリックする。

図 1.1.2-1　クライアント SSL リスト画面

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

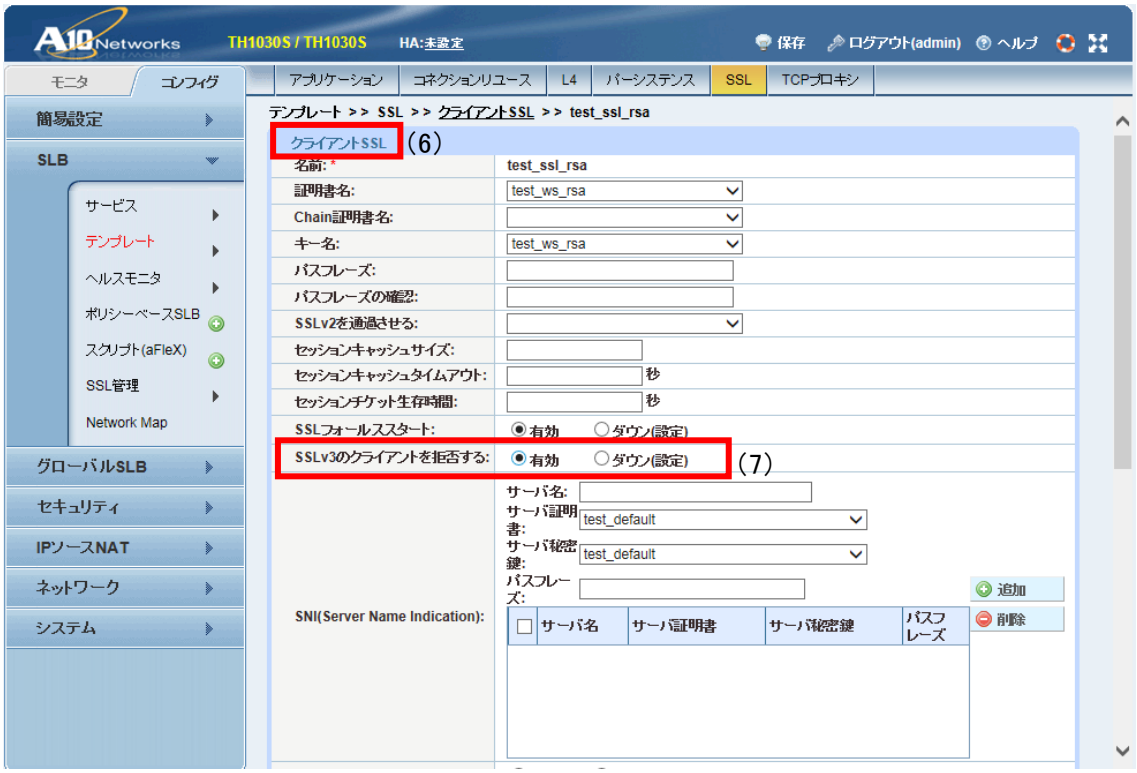

図 1.1.2-2　クライアント SSL 設定画面-1

C)　設定が完了したら（8）「OK」ボタンを押下する。

図 1.1.2-3　クライアント SSL 設定画面-2

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

図 1.1.2-4　設定保存画面

II.　暗号スイートの設定

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

図 1.1.2-5　SSL 暗号追加メニュー画面

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

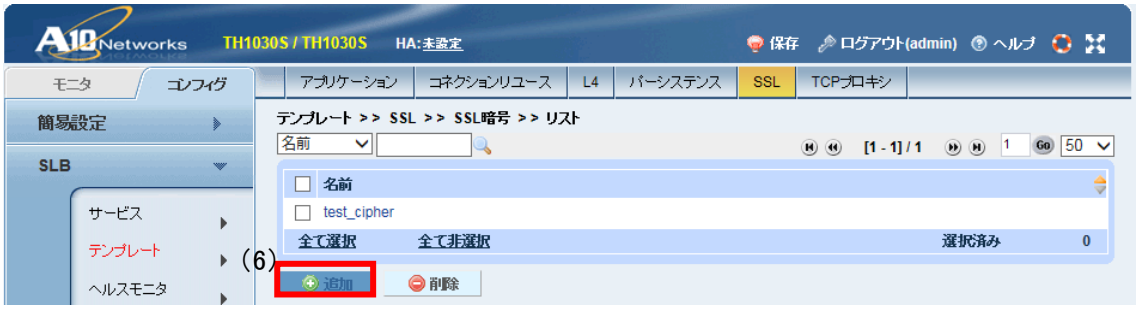

図 1.1.2-6　SSL 暗号リスト画面

C)　SSL 暗号新規作成画面が表示されたら (7) 名前を入力し、追加したい (8) SSL 暗号をドロップダウンリストから選択し、(9)「プライオリティー」欄で優先度を入力してから (10)「追加」ボタンを押下する。

更に追加したい SSL 暗号が有る場合は (8) ～ (10) を繰り返す。

追加し終わったら (11)「OK」ボタンを押下する。

※プライオリティーの値が大きいものが優先される。

※ECDSA 証明書は設定が可能だが、有効な暗号スイートが無いため利用できない。

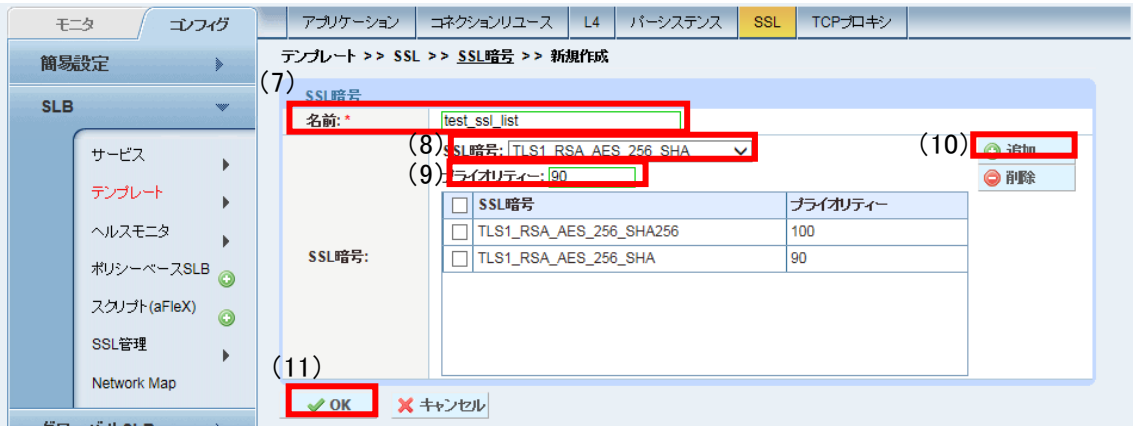

図 1.1.2-7　SSL 暗号新規作成画面

D)　1.1.1.I.B で設定したクライアント SSL を開き、(12)「SSL 暗号テンプレート」内の（13）クラスで「SSL サイファーテンプレート」にチェックを入れ、(14) SSL サイファーテンプレートで 1.1.1.II.C で作成した SSL 暗号（例：test_ssl_list）を選択する。あるいは、クラスで「SSL 暗号」を選択し、（15）SSL 暗号で暗号スイートを個別に選択する。
設定が完了したら（16）「OK」ボタンを押下する。

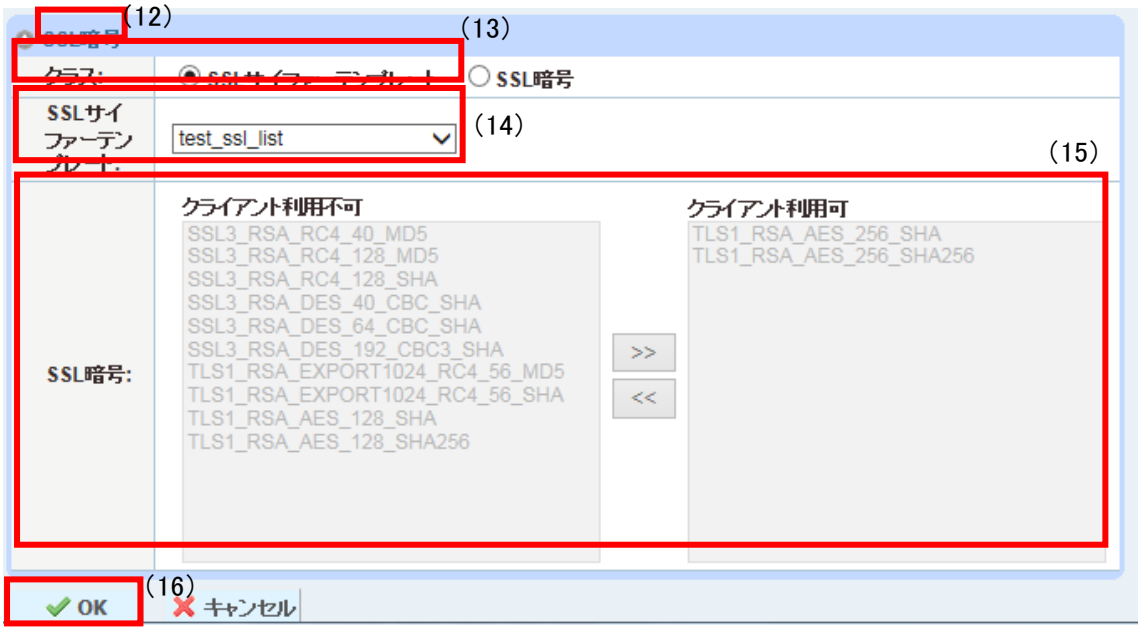

図 1.1.2-8　SSL 暗号画面

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

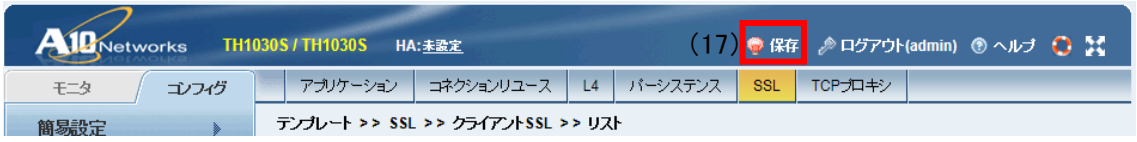

図 1.1.2-9　クライアント SSL リスト（保存ボタン点滅）画面

III.　DH/DHE、ECDH/ECDHE の鍵長の設定

設定方法なし。

IV. サーバクライアントの優先順位の設定
1.1.2.II.D 図 1.1.2-8　SSL 暗号画面 ですべての暗号スイートを選択した場合は、クライアント優先になる。既定は、すべての暗号スイートを 1.1.2.II.D 図 1.1.2-8　SSL 暗号画面 で選択した状態であり、クライアント優先である。1.1.2.II.D の手順にて SSL サイファーテンプレートを設定した場合、1.1.2.II.D 図 1.1.2-8　SSL 暗号画面 で暗号スイートを一部選択した場合は、サーバ優先となる。

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

VI. Extension の設定
設定方法なし。

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
設定ガイドラインの高セキュリティ型に設定することはできない。

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

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

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

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

1.1.3.2. 推奨セキュリティ型
③暗号スイートを具体的に設定する方法により、設定ガイドラインの推奨セキュリティ型に設定（準

拠）することができる。

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

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

I. プロトコルバージョン

tls1.2、tls1.0 が有効である。

※表 1.1.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

II. 暗号スイート

表 1.1.1-1　暗号設定内容（デフォルト）日立製作所 Hitachi Load Balancer EL130 で使用可能な暗号スイートで使用可能な暗号スイート のとおり。

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE、ECDH/ECDHE を含む暗号スイートがないためなし。

IV. サーバクライアントの優先順位の設定

クライアント優先である。

※表 1.1.1-1　暗号設定内容（デフォルト）の CipherSuite 選択優先権のとおり。

V. 暗号スイートの優先順位の設定

クライアント優先であるため、優先順位はなし。

VI. Extension の設定

表 1.1.1-1　暗号設定内容（デフォルト）の Extension のとおり。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分あり。

TLS1.1 が無効である。

SSLv3 が有効である。

II. 暗号スイート

差分あり。

推奨セキュリティ型に含まれる暗号スイート 64 個のうち、表 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 4 個の暗号スイートの使用が可能である。その他、推奨セキュリティ型に含まれない 3 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

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

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

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

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

I. プロトコルバージョン

SSLv3 のクライアントを拒否する: 有効　（図 1.1.2-2 参照）

II. 暗号スイート

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

表 1.1.3.2-2　暗号スイートの設定（推奨セキュリティ型、個別指定、RSA 証明書設定時）

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

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

III. DH/DHE、ECDH/ECDHE の鍵長

設定できない。

IV. サーバクライアントの優先順位の設定

6.8.2.II.D 図 1.1.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V.　暗号スイートの優先順位の設定

II.暗号スイートで設定した結果による。

VI.　Extension の設定

設定できない。

④　③の設定と設定ガイドラインの設定内容との差分

I.　プロトコルバージョン

差分なし。

TLS1.1 が無効である。

II.　暗号スイート

差分なし。

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

表 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、個別指定、RSA 証明書設定時）

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

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III.　DH/DHE、ECDH/ECDHE の鍵長

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

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）

「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、1.1.3.2 推奨セキュリティ型と同じである。

② ①の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

TLS1.1 が無効である。

II. 暗号スイート

差分あり。

セキュリティ例外型に含まれる暗号スイート 67 個のうち、表 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 6 個の暗号スイートの使用が可能である。その他、セキュリティ例外型に含まれない 1 個の暗号スイートが使用可能である。ただし、クライアント優先であるため、優先順位は考慮されない。

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

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

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

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

I. プロトコルバージョン

SSLv3 のクライアントを拒否する: ダウン（設定）　（図 1.1.2-2 参照）

II. 暗号スイート

6.8.2.II.D の手順で表 1.1.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定、RSA 証明書設定時） の暗号スイートを追加する。

表 1.1.3.3-2　暗号スイートの設定（セキュリティ例外型、個別指定、RSA 証明書設定時）

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

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

III. DH/DHE、ECDH/ECDHE の鍵長

設定できない。

IV. サーバクライアントの優先順位の設定

6.8.2.II.D 図 1.1.2-8　SSL 暗号画面 で暗号スイートを一部選択するため、サーバ優先となる。

V. 暗号スイートの優先順位の設定

II.暗号スイートで設定した結果による。

VI. Extension の設定

設定できない。

④ ③の設定と設定ガイドラインの設定内容との差分

I. プロトコルバージョン

差分なし。

TLS1.1 が無効である。

II. 暗号スイート

差分なし。

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

表 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、個別指定、RSA 証明書設定時）

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

※グループ内の順番は順不同。

※括弧内は設定ガイドラインのグループ名。

III. DH/DHE、ECDH/ECDHE の鍵長

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

付属情報

- **製品情報**
  日立製作所 Hitachi Load Balancer EL130 ソフトウェアバージョン: 2.7.1-P6(build: 143)

- **参考情報**
  クイックスタートガイド