MPX8005c

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. Citrix NetScaler MPX シリーズ

本章では、Citrix NetScaler MPX 8005c 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

サーバ証明書は、RSA 証明書のみが設定可能であり、RSA 証明書を設定した場合について記載する。

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	9
tls1.0	ON	サーバ	9
sslv3	ON	サーバ	9
sslv2	設定不可	－	－

- Citrix NetScaler MPX 8005c 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
0x00,0x15	TLS_DHE_RSA_WITH_DES_CBC_SHA				---	OFF	OFF	OFF	OFF	OFF
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
0x00,0x67	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
0x00,0x9e	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
0xc0,0x11	TLS_ECDHE_RSA_WITH_RC4_128_SHA				secp256r1	ON:14	ON:6	ON:6	ON:6	OFF
0xc0,0x12	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA				secp256r1	ON:13	ON:5	ON:5	ON:5	OFF
0xc0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON:8	ON:4	ON:4	ON:4	OFF
0xc0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON:7	ON:3	ON:3	ON:3	OFF

id	IANA 表記	高	推	例	鍵交換パラメータ	tls1.2	tls1.1	tls1.0	sslv3	sslv2
0xc0,0x27	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:9	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:11	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	ON:17	ON:9	ON:9	ON:9	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	---	ON:16	ON:8	ON:8	ON:8	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:15	ON:7	ON:7	ON:7	OFF
0x00,0x2f	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	---	ON:2	ON:2	ON:2	ON:2	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	---	ON:1	ON:1	ON:1	ON:1	OFF
0x00,0x3c	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	---	ON:4	OFF	OFF	OFF	OFF
0x00,0x3d	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	---	ON:3	OFF	OFF	OFF	OFF
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON:6	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON:5	OFF	OFF	OFF	OFF
0x00,0x03	TLS_RSA_EXPORT_WITH_RC4_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x06	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x08	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				---	OFF	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	―	―	―	―
heartbeat	15	非対応	非対応	非対応	―	―

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 Citrix NetScaler MPX 8005c の管理画面にログインし、(1) Configuration－ (2) Traffic Management－ (3) Load Balancing－ (4) Virtual Servers をクリックして、仮想サーバー覧を表示し、(5) 編集したい仮想サーバを選択し、(6) Edit ボタンを押下する。

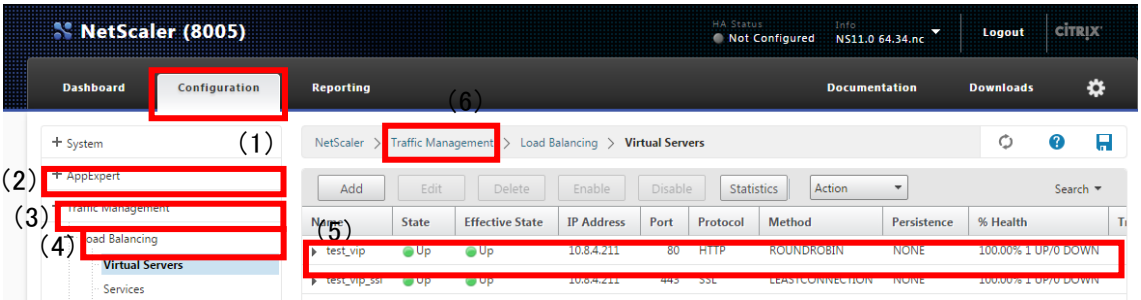

図 1.1.2-1 仮想サーバー覧画面-1

B) 仮想サーバ設定画面に遷移するので画面下の（7）「SSL Parameters」項目右側の（8）「ペン」アイコンを押下する。

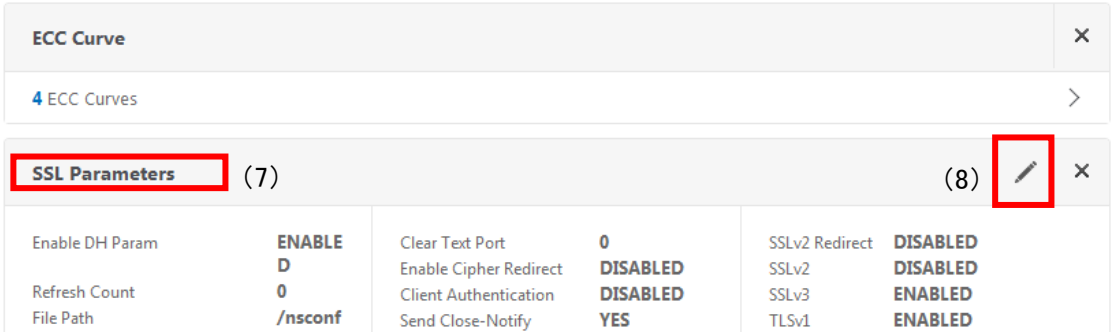

図 1.1.2-2　仮想サーバ設定画面（SSL パラメータ）

C) 「SSL Parameters」の設定を変更出来るようになるので、（9）「Protocol」」欄の有効にしたい（10）プロトコルのチェックボックスにチェックを入れ、（11）「OK」ボタンを押下し「SSL Parameters」の設定を完了して（12）「Done」ボタンを押下して Virtual Server の設定を完了する。

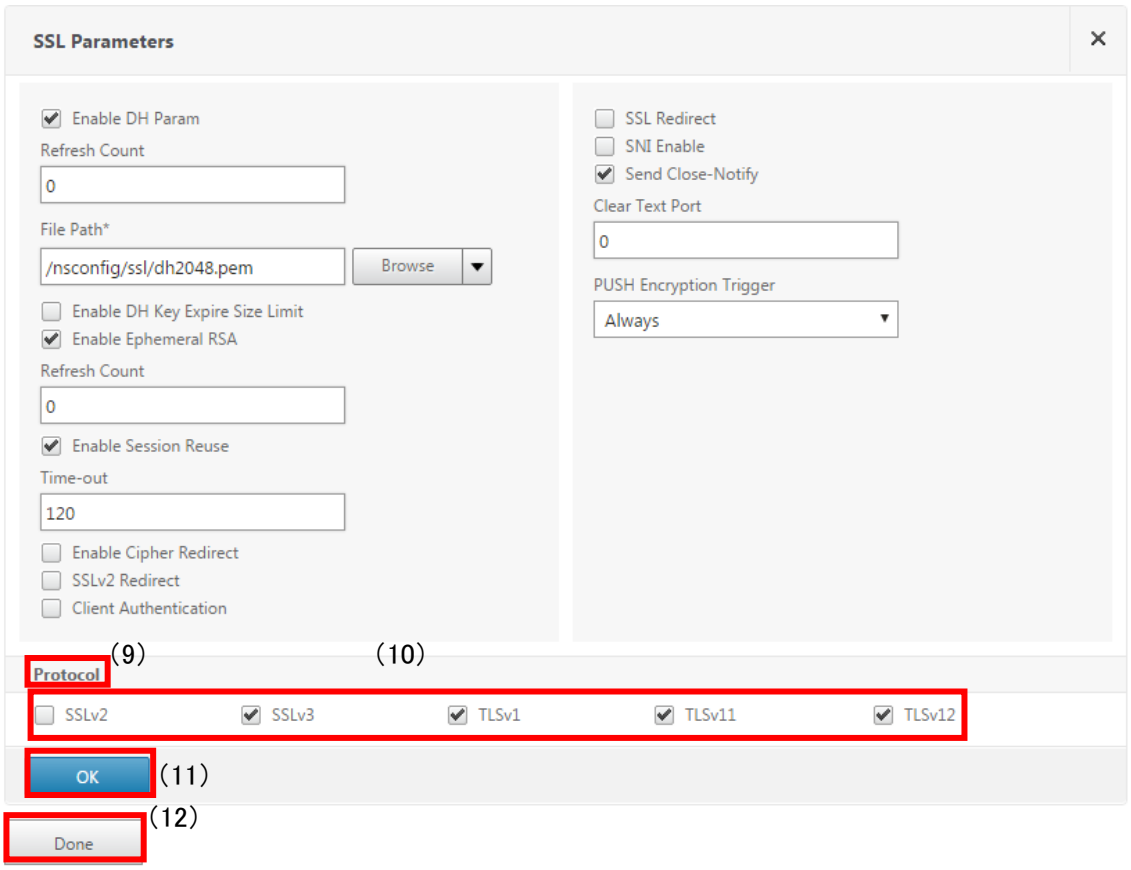

図 1.1.2-3　仮想サーバ設定画面（プロトコル）

D) 仮想サーバー覧画面に戻るので、右上の（13）「フロッピー」アイコンをクリックすると確認のダイアログが表示されるので、（14）「YES」を押下して設定を保存する。

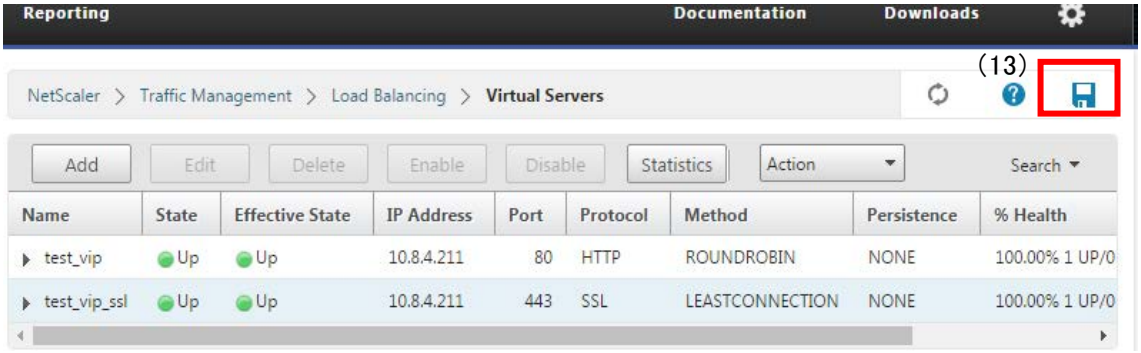

図 1.1.2-4　仮想サーバー一覧画面-2

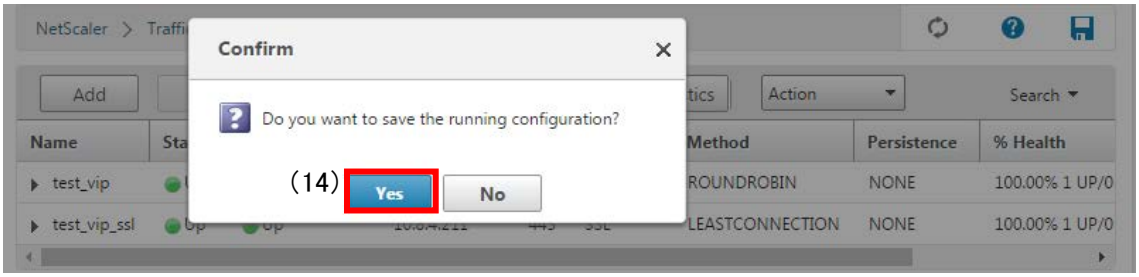

図 1.1.2-5　仮想 SSL サーバ設定確認画面-1

II.　暗号スイートの設定

A)　ブラウザで Citrix NetScaler MPX 8005c の管理画面にログインし、(1) Configuration－(2) Traffic Management－(3) Load Balancing－(4) Virtual Servers をクリックして、仮想サーバー覧を表示し、(5) 編集したい仮想サーバを選択し、(6) Edit ボタンを押下する。

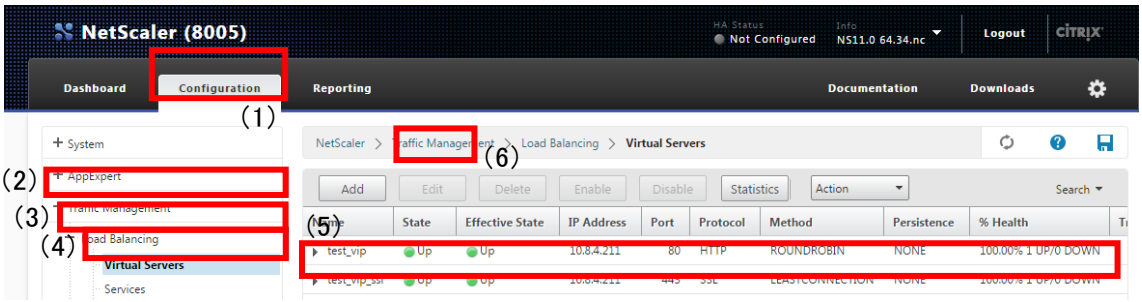

図 1.1.2-6　仮想サーバー覧画面-3

B)　仮想サーバ設定画面に遷移するので (7)「SSL Ciphers」右側の (8) ペンのボタンを押下し、表示される (9)「Add」ボタンを押下する。

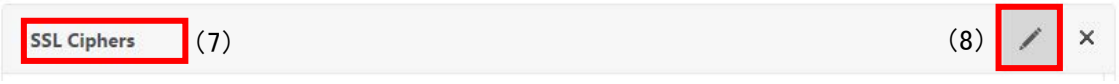

図 1.1.2-7　仮想サーバ設定画面（SSL 暗号）

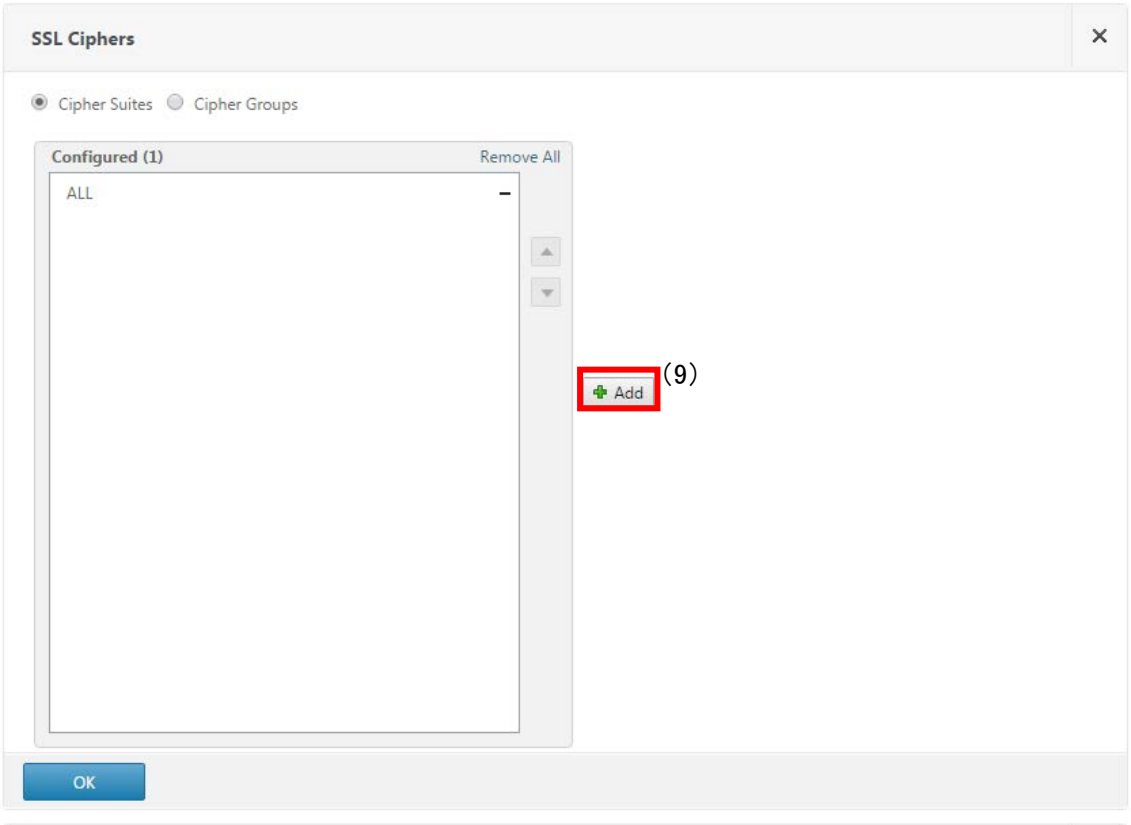

図 1.1.2-8　SSL 暗号編集画面

C)　（10）「Available」欄が表示されるので、（11）グループのツリーを展開し、有効にしたい暗号スイートに（12）チェックを入れ、（13）「右三角」ボタンを押下して（14）「Configured」欄へ移動させる。
優先順位は「Configured」欄の上から設定されるため、（15）暗号スイートを選択した上で右側の（16）「上三角」・「下三角」ボタンで順番を入れ替えることが可能。
設定し終わったら（17）「OK」ボタンと画面下の（18）「Done」ボタンを押下し、設定を完了する。

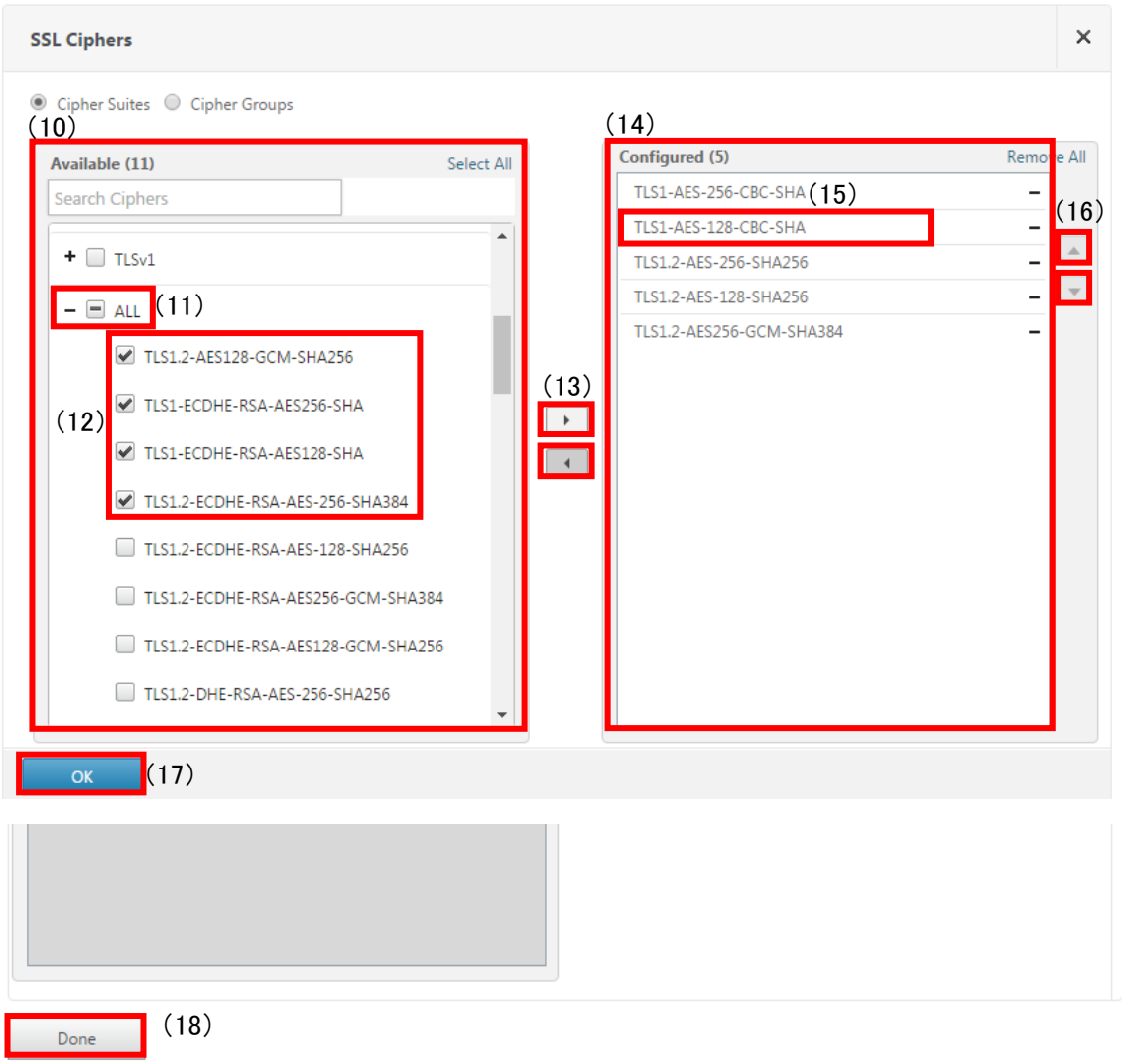

図 1.1.2-9　仮想 SSL サーバ設定画面（暗号スイート）

D)　仮想サーバー覧画面に戻るので、右上の（19）「フロッピー」アイコンをクリックすると確認のダイアログが表示されるので、（20）「YES」を押下して設定を保存する。

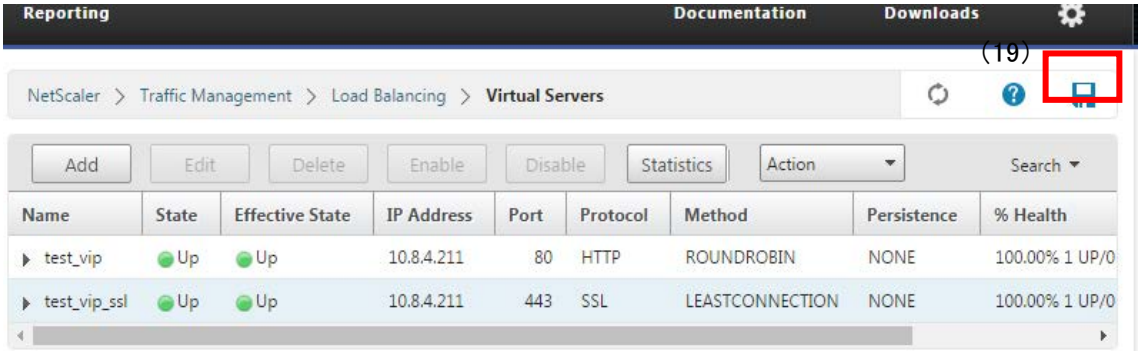

図 1.1.2-10　仮想サーバー一覧画面-4

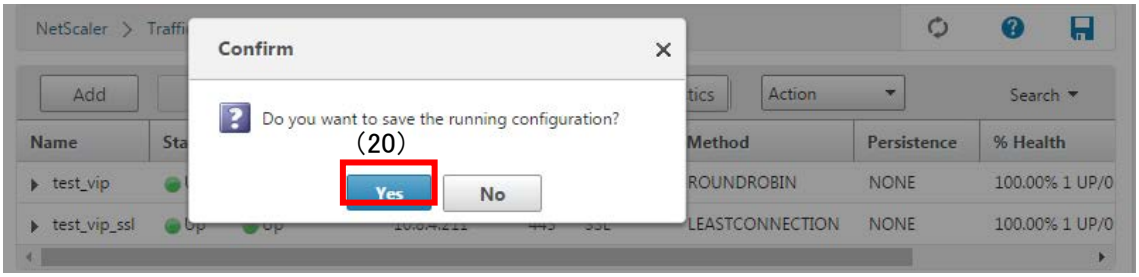

図 1.1.2-11　仮想 SSL サーバ設定確認画面-2

III.　DH/DHE、ECDH/ECDHE の鍵長の設定

DH/DHE：　6.12.2.I.C の図 1.1.2-3　仮想サーバ設定画面（プロトコル）にて、「Enable DH Param」にチェックを入れ、DH パラメータが記載された pem 形式のファイルを設定すると pem 形式ファイルの DH パラメータの鍵長で鍵交換が行われる。

対応している鍵長：256bit、512bit、1024bit、2048bit

ECDH/ECDHE：6.12.2.I.B の図 1.1.2-2　仮想サーバ設定画面（SSL パラメータ）にある「ECC Curve」の項目にて P_224（224bit）、P_256（256bit）、P_384（384bit）、P_521（521bit）が設定されており、設定から外すことも可能である(図 1.1.2-12　ECC Curve 設定画面 参照)。

複数設定している場合、優先されるのは 256bit となっている。

図 1.1.2-12　ECC Curve 設定画面

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
図 1.1.2-9　仮想 SSL サーバ設定画面（暗号スイート）の「Configured」欄へ、優先度上位の暗号スイートを上から順に設定する。

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

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、tls1.1、tls1.0、sslv3 が有効である。

※1.1.1 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

1.1.1 表 1.1.1-1 暗号設定内容（デフォルト）の Citrix NetScaler MPX 8005c 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：デフォルトでは設定 DH/DHE が含まれる暗号スイートなし。

ECDH/ECDHE：256bit(secp256r1)

IV. サーバクライアントの優先順位の設定

サーバ優先である。

※1.1.1 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

1.1.1 表 1.1.1-1 暗号設定内容（デフォルト）の Citrix NetScaler MPX 8005c 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 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、tls1.0、sslv3 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）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 15 個の暗号スイートが使用可能である。使用可能な 2 個の暗号スイートの優先順位は、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_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)	11	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_AES_256_CBC_SHA
		2	TLS_RSA_WITH_AES_128_CBC_SHA
		3	TLS_RSA_WITH_AES_256_CBC_SHA256
		4	TLS_RSA_WITH_AES_128_CBC_SHA256
		5	TLS_RSA_WITH_AES_256_GCM_SHA384
		6	TLS_RSA_WITH_AES_128_GCM_SHA256
		7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		8	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
		9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
		10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		13	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		14	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		15	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		16	TLS_RSA_WITH_RC4_128_SHA
		17	TLS_RSA_WITH_RC4_128_MD5

※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 をチェックし、TLS1.1、TLS1.0、SSLv3、SSLv2 のチェックを外す。

（図 1.1.2-3 参照）

II. 暗号スイート

1.1.2.II.C の手順にて SSL Ciphers 項目 Configured 欄に表 1.1.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定） の順番で設定する。

表 1.1.3.1-2　暗号スイートの設定（高セキュリティ型、個別指定）

Configured	暗号スイート
1	TLS1.2-DHE-RSA-AES256-GCM-SHA384
2	TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
3	TLS1.2-DHE-RSA-AES128-GCM-SHA256
4	TLS1.2-ECDHE-RSA-AES128-GCM-SHA256

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE：「Enable DH Param」にチェックを入れ、2048bit の pem 形式ファイルを設定する。

ECDH/ECDHE：「ECC Curve」の項目にて P_256（256bit）設定する。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先のため、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 1.1.3.1-3 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 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高セキュリティ型の順位と同じである。

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、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_RSA_WITH_AES_256_GCM_SHA384(α追加)	2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(α追加)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	3	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(β追加)	4	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。

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

差分あり。

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）　の「**設定ガイドラインの推奨セキュリティ型（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、推奨セキュリティ型に含まれない 5 個の暗号スイートが使用可能である。使用可能な 12 個の暗号スイートの優先順位は、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_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）	2	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	4	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	6	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	1	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	3	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	5	TLS_RSA_WITH_AES_256_GCM_SHA384（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	13	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		14	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		15	TLS_RSA_WITH_3DES_EDE_CBC_SHA
		16	TLS_RSA_WITH_RC4_128_SHA
		17	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、TLS1.0、TLS1.1 をチェックし、SSLv3、SSLv2 のチェックを外す。

（図 1.1.2-3 参照）

II. 暗号スイート

1.1.2.II.C の手順にて SSL Ciphers 項目 Configured 欄に表 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） の順番で設定する。

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）

Configured	暗号スイート
1	TLS1-DHE-RSA-AES-128-CBC-SHA
2	TLS1.2-DHE-RSA-AES128-SHA256
3	TLS1.2-DHE-RSA-AES128-GCM-SHA256
4	TLS1-ECDHE-RSA-AES128-SHA
5	TLS1.2-ECDHE-RSA-AES-128-SHA256
6	TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
7	TLS1-AES-128-CBC-SHA
8	TLS1.2-AES-128-SHA256
9	TLS1.2-AES-128-GCM-SHA256
10	TLS1-DHE-RSA-AES-256-CBC-SHA
11	TLS1.2-DHE-RSA-AES-256-SHA256
12	TLS1.2-DHE-RSA-AES256-GCM-SHA384
13	TLS1-ECDHE-RSA-AES256-SHA
14	TLS1.2-ECDHE-RSA-AES-256-SHA384
15	TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
16	TLS1-AES-256-CBC-SHA
17	TLS1.2-AES-256-CBC-SHA256
18	TLS1.2-AES-256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE：「Enable DH Param」にチェックを入れ、2048bit の pem 形式ファイルを設定する。

ECDH/ECDHE：「ECC Curve」の項目にて P_256（256bit）設定する。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先のため、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 1.1.3.2-3 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） の「**設定ガイドラインの推奨セキュリティ型（一部）」にある 18 個の**暗号スイートの使用が可能である。使用可能な 18 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）

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_RSA_WITH_AES_128_CBC_SHA(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(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_RSA_WITH_AES_128_GCM_SHA256(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	7	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	9	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	10	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	11	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	12	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	13	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	15	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)

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
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)	17	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。

I. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

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、1.1.3.1 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。

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 14 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 3 個の暗号スイートが使用可能である。使用可能な 14 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 1.1.3.3-1　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_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）

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）	2	TLS_RSA_WITH_AES_128_CBC_SHA（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	4	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	6	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
D	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	7	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	11	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
E	TLS_RSA_WITH_AES_256_CBC_SHA（E）	1	TLS_RSA_WITH_AES_256_CBC_SHA（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	3	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	5	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	16	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	15	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	13	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
		14	TLS_ECDHE_RSA_WITH_RC4_128_SHA
		17	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

SSLv3、TLS1.0、TLS1.1、TLS1.2 のチェックを入れる。　（図 1.1.2-3 参照）

II. 暗号スイート

1.1.2.II.C の手順にて SSL Ciphers 項目 Configured 欄に表 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） の順番で設定する。

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）

Configured	暗号スイート
1	TLS1-DHE-RSA-AES-128-CBC-SHA
2	TLS1.2-DHE-RSA-AES128-SHA256
3	TLS1.2-DHE-RSA-AES128-GCM-SHA256
4	TLS1-ECDHE-RSA-AES128-SHA

Configured	暗号スイート
5	TLS1.2-ECDHE-RSA-AES-128-SHA256
6	TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
7	TLS1-AES-128-CBC-SHA
8	TLS1.2-AES-128-SHA256
9	TLS1.2-AES-128-GCM-SHA256
10	TLS1-DHE-RSA-AES-256-CBC-SHA
11	TLS1.2-DHE-RSA-AES-256-SHA256
12	TLS1.2-DHE-RSA-AES256-GCM-SHA384
13	TLS1-ECDHE-RSA-AES256-SHA
14	TLS1.2-ECDHE-RSA-AES-256-SHA384
15	TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
16	TLS1-AES-256-CBC-SHA
17	TLS1.2-AES-256-CBC-SHA256
18	TLS1.2-AES-256-GCM-SHA384
19	SSL3-RC4-SHA
20	SSL3-EDH-RSA-DES-CBC3-SHA
21	SSL3-DES-CBC3-SHA

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE：「Enable DH Param」にチェックを入れ、2048bit の pem 形式ファイルを設定する。

ECDH/ECDHE：「ECC Curve」の項目にて P_256（256bit）設定する。

IV. サーバクライアントの優先順位の設定

既定でサーバ優先のため、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。

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） の「設定ガイドラインのセキュリティ例外型(一部)」にある 21 個の暗号スイートの使用が可能である。使用可能な 21 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）

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)	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_RSA_WITH_AES_128_CBC_SHA(A 追加)	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(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_RSA_WITH_AES_128_GCM_SHA256(A 追加)	6	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	7	TLS_RSA_WITH_AES_128_CBC_SHA(B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	8	TLS_RSA_WITH_AES_128_CBC_SHA256(B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	9	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	10	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	11	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	12	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)	13	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	15	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)	17	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)
G	TLS_RSA_WITH_RC4_128_SHA(G)	19	TLS_RSA_WITH_RC4_128_SHA(G)
H	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(H)	20	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA(H)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA(H)	21	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。

付属情報

- 製品情報
  Citrix NetScaler MPX 8005c ファームウェアバージョン: NS11.0 Build 64.34.nc

- 参考情報
  NetScaler 初期設定＆ロードバランサ機能設定ガイド Ver.1.6
  SSL Offload 機能設定ガイド Ver.1.6