IPCOM EX2-3500

（IPCOM EX2-3000 IN ソフトウェア V01）

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

※調査の背景、調査方法等は「SSL/TLS を利用するサーバアプライアンス製品における暗号設定方法等の調査報告書」を参考にされたい。

1.1.1 章記載の表 1.1.1-1 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	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。 「αl「βl「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. 富士通 IPCOM シリーズ

本章では、IPCOM EX2-3500 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	OFF	ー	0
tls1.0	ON	クライアント	3
sslv3	OFF	ー	0
sslv2	設定不可	ー	－

- 富士通 IPCOM EX2-3500 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	---	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
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
0xc0,0x2f	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
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	OFF	OFF	OFF	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G 追加	---	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
0x00,0x9c	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	---	ON	OFF	OFF	OFF	OFF
0x00,0x9d	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	---	ON	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	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 IPCOM EX2-3500 WEB コンソールにログインし、(1) 設定－ (2) 装置設定－ (3) SSL アクセラレータ (4) 仮想 SSL サーバをクリックして、(5) 仮想 SSL サーバ一覧を表示し、編集したい仮想サーバを選択し、(6) 仮想 SSL サーバ設定項目を表示する。

図 1.1.2-1 仮想 SSL サーバー覧画面

B) 仮想 SSL サーバ設定項目にある (7)「詳細設定」ボタンを押下し、(8) プロトコル一覧の有効にしたいプロトコルバージョンに (9) チェックを入れる。

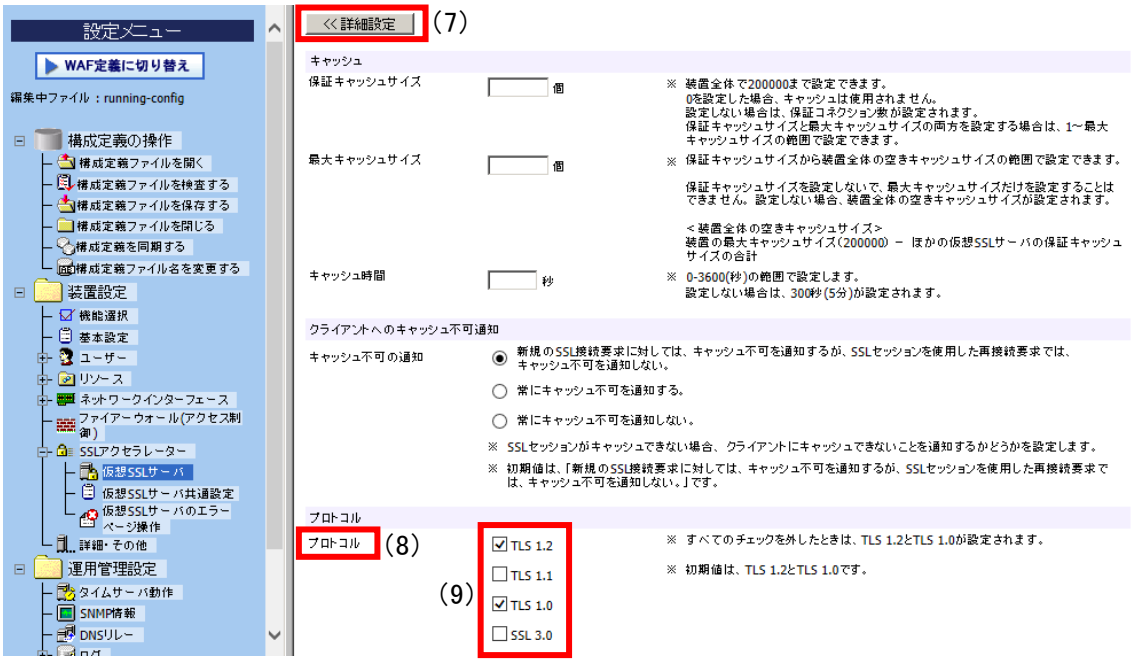

図 1.1.2-2 仮想 SSL サーバ設定画面（プロトコル）-1

C) 設定が完了したら（10）「適用」ボタンを押下する。

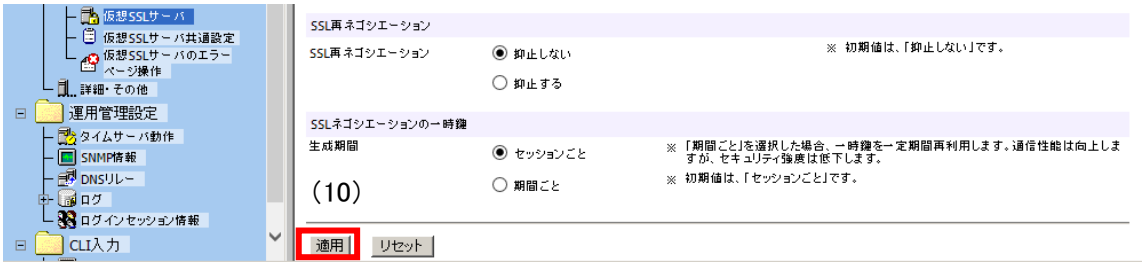

図 1.1.2-3 仮想 SSL サーバ設定画面（プロトコル）-2

D) 構成の保存を促すポップアップが表示されるので（11）「OK」ボタンを押下してポップアップを閉じる。

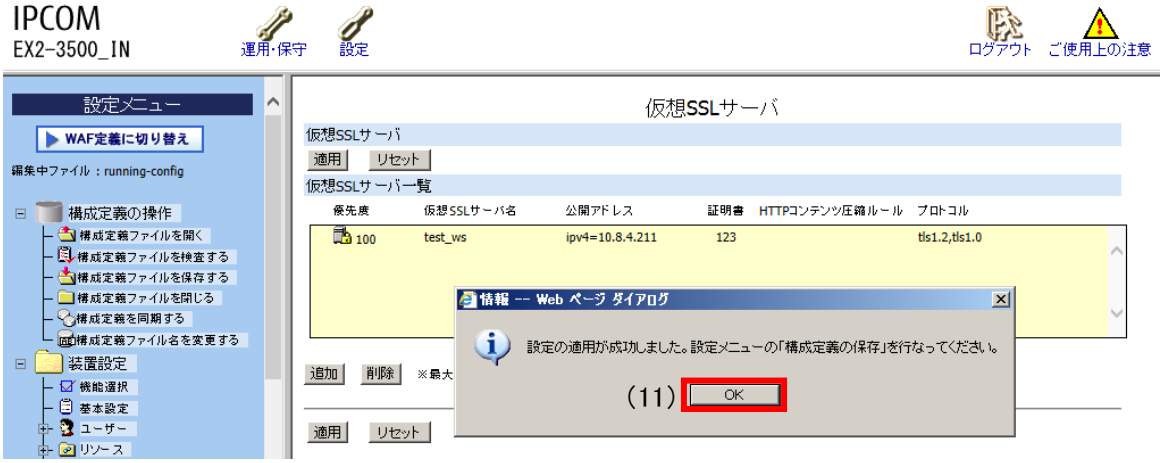

図 1.1.2-4 仮想 SSL サーバ設定画面（プロトコル）-3

E) （12）構成定義の操作ー（13）構成定義ファイルを保存するをクリックして、（14）「構成定義ファイルの保存」ポップアップを表示し、（15）「即時反映（running-config）と再起動時に反映（startup-config）」にチェックを入れ、（16）「OK」ボタンを押下して保存する。

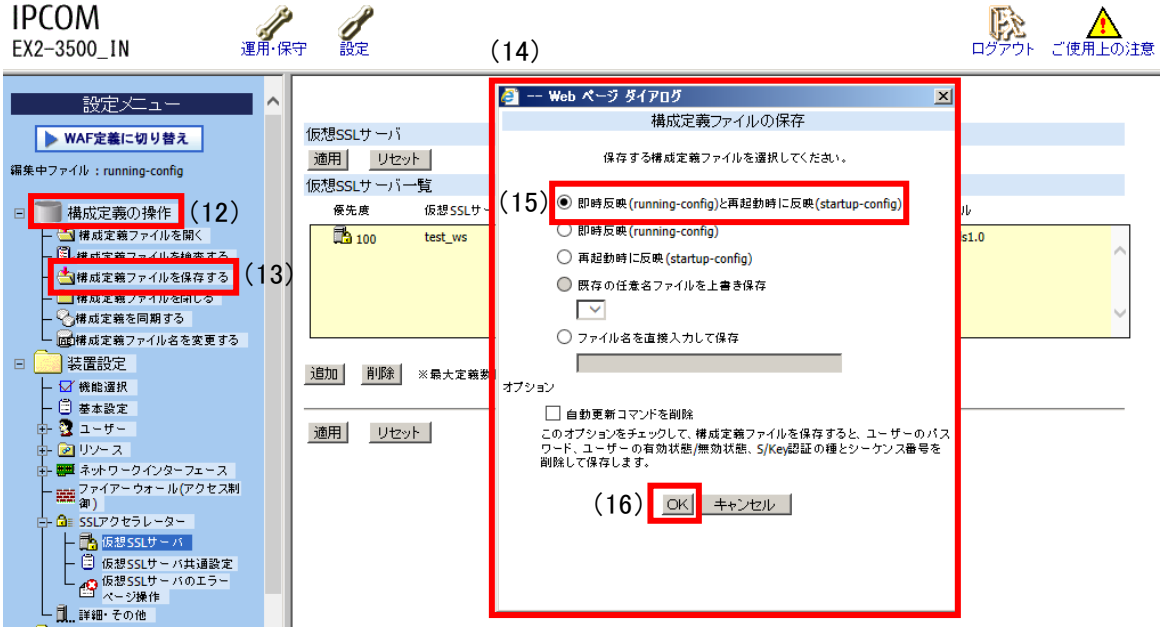

図 1.1.2-5　構成定義ファイル保存画面-1

II. 暗号スイートの設定

A) 図 1.1.2-6 仮想 SSL サーバ設定画面（暗号スイート）の（1）「暗号スイート」で（2）「設定する」を選択し、（3）「設定」ボタンを押下する。

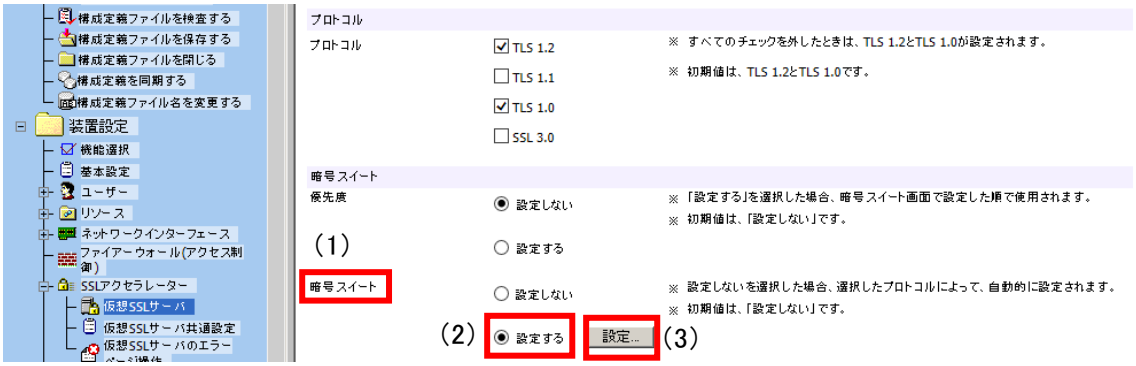

図 1.1.2-6 仮想 SSL サーバ設定画面（暗号スイート）-1

B) （4）「仮想 SSL サーバ暗号スイート選択」画面が表示されるので、（5）「暗号スイートを選択」の一覧から有効にしたい「暗号スイート」もしくは「グループ化文字列」にチェックを入れ、（6）「←＋」ボタンで有効、（7）「→」ボタンで無効を選択する。選択した暗号スイートは（8）「選択した暗号スイート」欄に表示され、現在有効になっている暗号スイートは（9）「選択した暗号スイートの展開結果」欄に表示される。選択が完了したら（10）「OK」ボタンを押下して画面を閉じる。

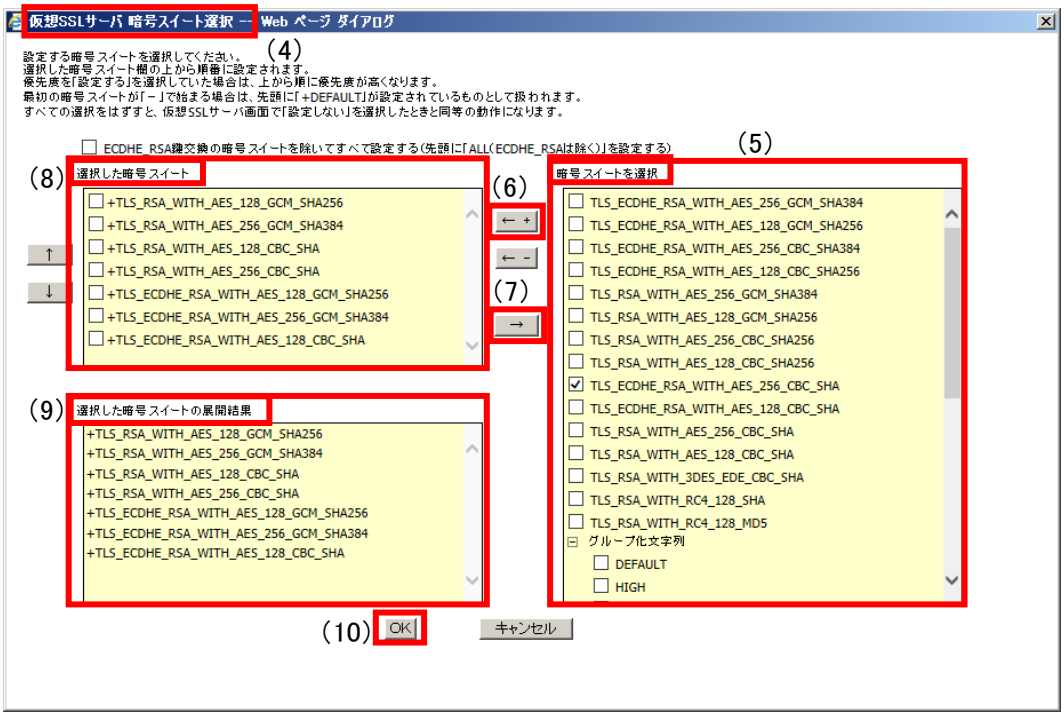

図 1.1.2-7 仮想 SSL サーバ暗号スイート選択画面

C) 設定が完了したら（11）「適用」ボタンを押下する。

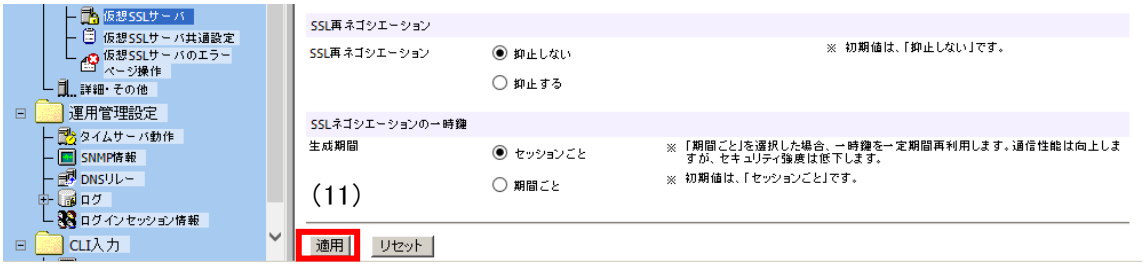

図 1.1.2-8 仮想 SSL サーバ設定画面（暗号スイート）-2

D) 構成の保存を促すポップアップが表示されるので（12）「OK」ボタンを押下してポップアップを閉じる。

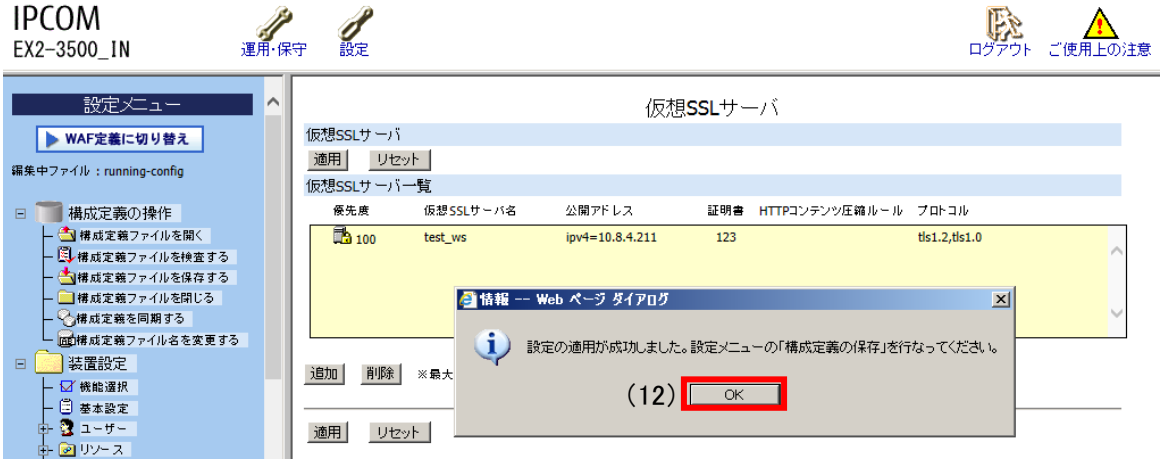

図 1.1.2-9 仮想 SSL サーバ設定画面（暗号スイート）-3

E) （13）構成定義の操作ー（14）構成定義ファイルを保存するをクリックして、（15）「構成定義ファイルの保存」ポップアップを表示し、（16）「即時反映（running-config）と再起動時に反映（startup-config）」にチェックを入れ、（17）「OK」ボタンを押下して保存する。

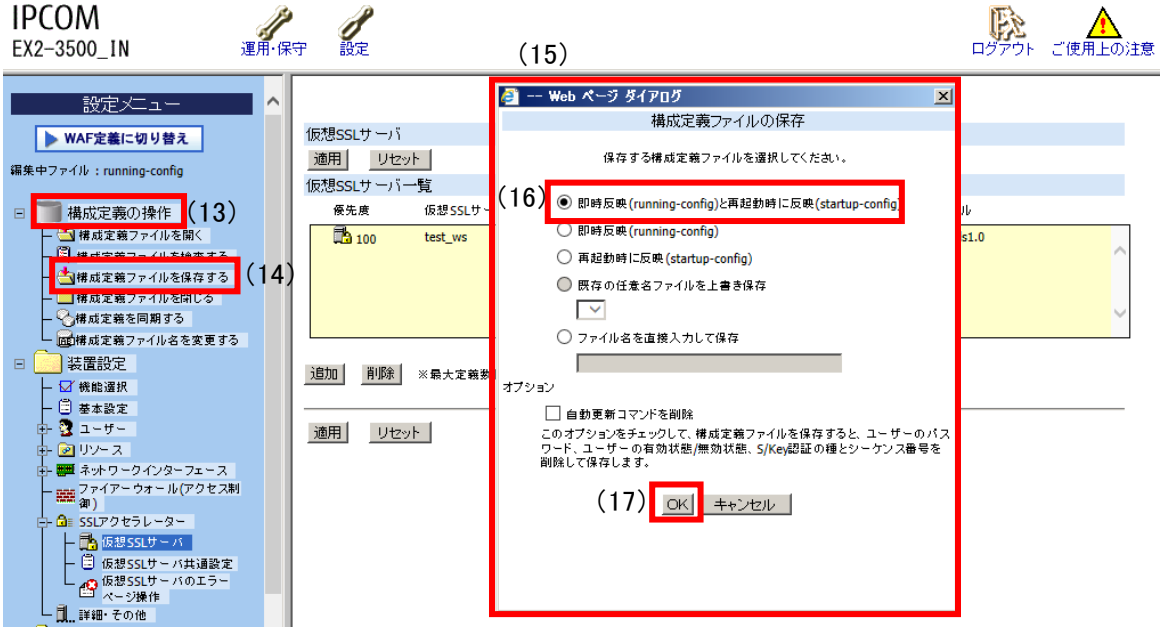

図 1.1.2-10　構成定義ファイル保存画面-2

III. DH/DHE、ECDH/ECDHE の鍵長の設定

設定方法なし。

ECDHE の鍵長は 256bit(secp256r1)または 384bit(secp384r1)である。

IV. サーバクライアントの優先順位の設定

A) 図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1 の（1）「優先度」で（2）サーバ優先の場合は「設定する」、クライアント優先の場合は「設定しない」を選択する。

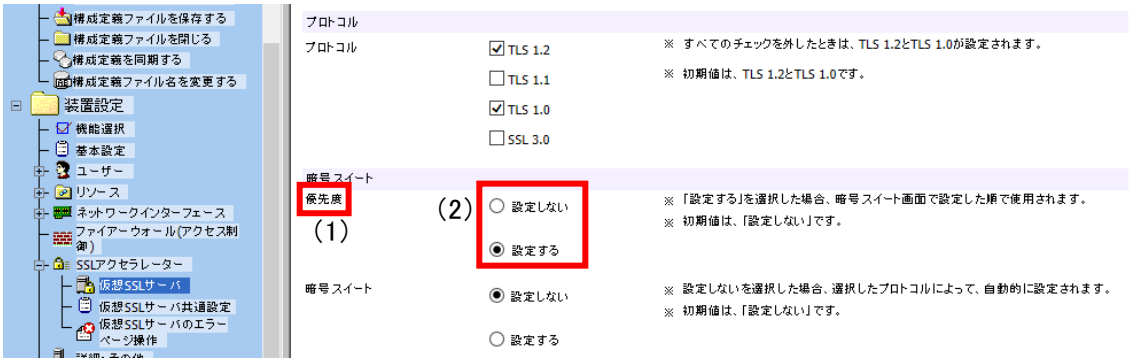

図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1

B) 設定が完了したら（3）「適用」ボタンを押下する。

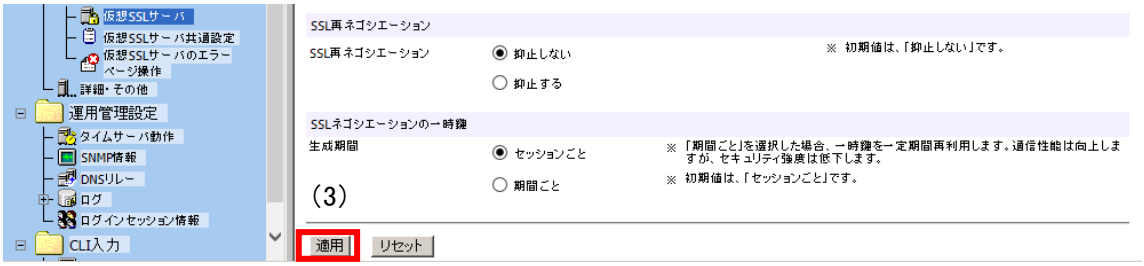

図 1.1.2-12　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-2

C) 構成の保存を促すポップアップが表示されるので（4）「OK」ボタンを押下してポップアップを閉じる。

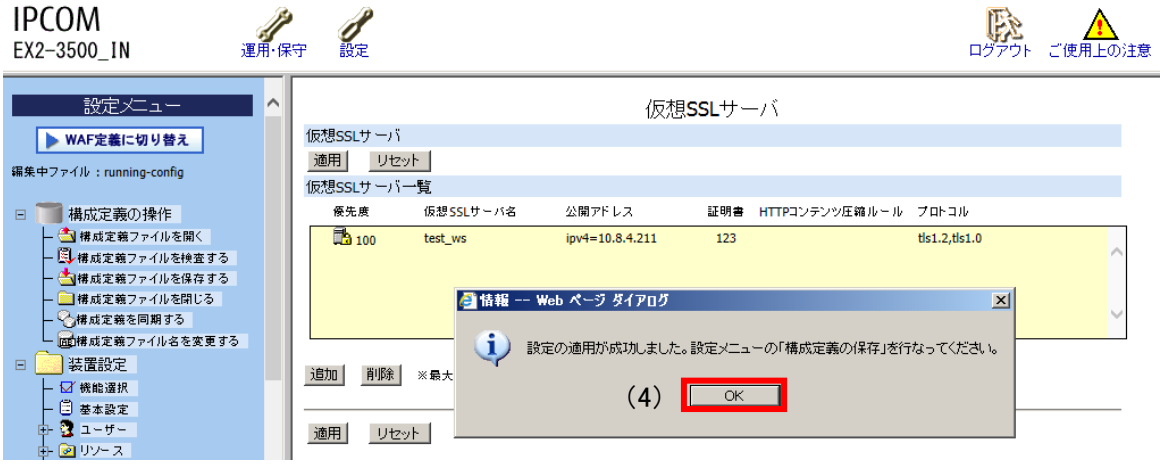

図 1.1.2-13　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-3

D)　（5）構成定義の操作ー（6）構成定義ファイルを保存するをクリックして、（7）「構成定義ファイル

の保存」ポップアップを表示し、(8)「即時反映(running-config)と再起動時に反映(startup-config)」にチェックを入れ、(9)「OK」ボタンを押下して保存する。

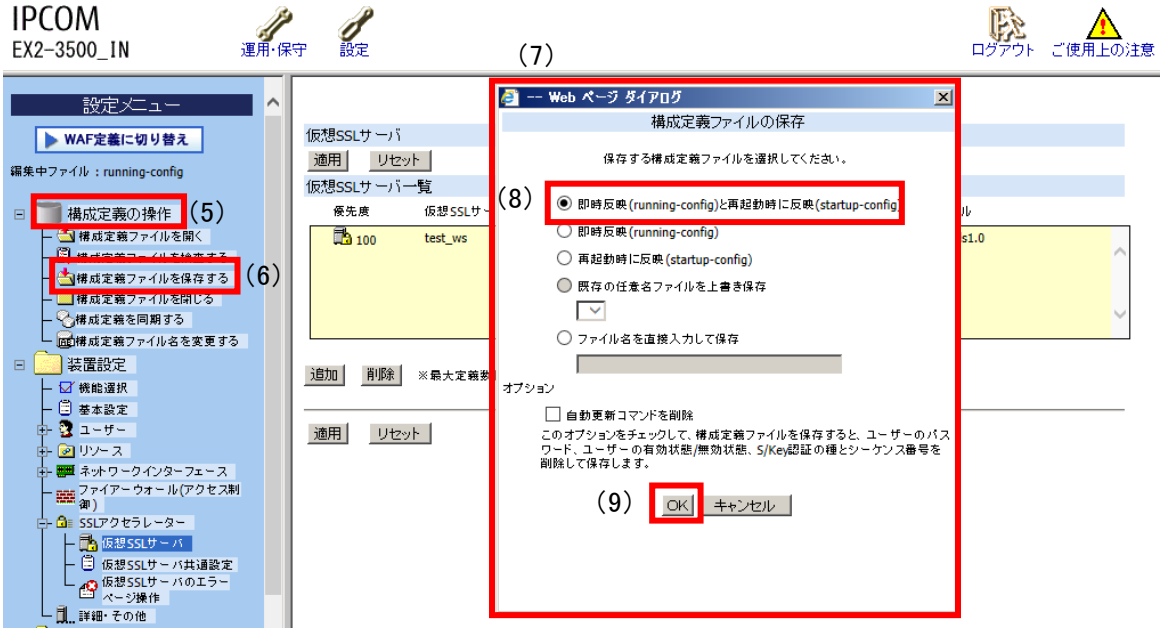

図 1.1.2-14　構成定義ファイル保存画面-3

V.　暗号スイートの優先順位の設定

1.1.2.IV.A の手順にて「優先度」を「設定する」に設定した場合のみ、1.1.2.II.B の「仮想 SSL サーバ暗号スイート選択」画面で「選択した暗号スイート」の上から順に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

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)する事が出来る。

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設定しない場合、意図しないスイートが入る事がある為、③の暗号スイートを具体的に設定する方法を推奨する

I. プロトコルバージョン

SSL プロトコル：チェック有： TLS1.2

チェック無：TLS1.0、TLS1.1、SSL3.0

（図 1.1.2-2　仮想 SSL サーバ設定画面（プロトコル）-1 参照）

II. 暗号スイート

図 1.1.2-7　仮想 SSL サーバ暗号スイート選択画面　の「選択した暗号スイート」欄に、表 1.1.3.1-1　暗号スイートの設定（高セキュリティ型、文字列指定） に示す「グループ化文字列」を「追加」する。

表 1.1.3.1-1　暗号スイートの設定（高セキュリティ型、文字列指定）

優先順位	グループ化文字列
-	ECDHE_RSA

※優先順位を付与する設定を行った場合、グループ化文字列に対して優先度が付与されます。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)または 384bit(secp384r1)である。

IV. サーバクライアントの優先順位の設定

図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1 によりサーバ優先に設定する。

V. 暗号スイートの優先順位の設定

暗号スイートに優先順位を付与する設定を行った場合、設定したグループの順番に従って優先度が付与される。ただし、グループ内の順位は制御出来ない(詳細な制御は、③の設定が必要)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

①の通り、本製品では暗号スイートを具体的に設定する必要がある。

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 1.1.3.1-2　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。ただし、ECDHE は、除外できないため高セキュリティ型に含まれない 4 個の暗号スイートが含まれる。使用可能な 2 個の暗号スイートと「設定ガイドラインの高セキュリティ型（一部)」の優先順位の違いは、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）の通りである。

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_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）
	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	3	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
		4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
		5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
		6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

※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

SSL プロトコル：チェック有：TLS1.2

チェック無：TLS1.0、TLS1.1、SSL3.0

（図 1.1.2-2　仮想 SSL サーバ設定画面（プロトコル）-1 参照）

II. 暗号スイート

図 1.1.2-7　仮想 SSL サーバ暗号スイート選択画面　の「選択した暗号スイート」欄に、表 1.1.3.1-3

暗号スイートの設定（高セキュリティ型、個別指定）の暗号スイートを「追加」する。

表 1.1.3.1-3　暗号スイートの設定（高セキュリティ型、個別指定）

優先順位	暗号スイート
-	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

※優先順位は、別の設定で指定。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)または 384bit(secp384r1)である。

IV. サーバクライアントの優先順位の設定

図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1 によりサーバ優先に設定する。

V. 暗号スイートの優先順位の設定

暗号スイートに優先順位を付与する設定を行った場合、設定したグループの順番に従って優先度が付与される。

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）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。設定可能な 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）

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）

※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

SSL プロトコル：チェック有：TLS1.0、TLS1.1、TLS1.2

チェック無：SSL3.0

（図 1.1.2-2　仮想 SSL サーバ設定画面（プロトコル）-1 参照）

II. 暗号スイート

図 1.1.2-7　仮想 SSL サーバ暗号スイート選択画面　の「選択した暗号スイート」欄に、表 1.1.3.2-1 暗号スイートの設定（推奨セキュリティ型、文字列指定） に示す「グループ化文字列」を「追加」する。

表 1.1.3.2-1　暗号スイートの設定（推奨セキュリティ型、文字列指定）

優先順位	グループ化文字列
-	ECDHE_RSA
	AES_GCM
	AES

※優先順位を付与する設定を行った場合、グループ化文字列に対して優先度が付与されます。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)または 384bit(secp384r1)である。

IV. サーバクライアントの優先順位の設定

図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1 によりサーバ優先に設定する。

V. 暗号スイートの優先順位の設定

暗号スイートに優先順位を付与する設定を行った場合、設定したグループの順番に従って優先度が

付与される。ただし、グループ内の順位は制御出来ない(詳細な制御は、③の設定が必要)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。

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） 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。使用可能な 12 個の暗号スイートと設定ガイドラインの推奨セキュリティ型（一部）の優先順位の違いは、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）の通りである。

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）

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_GCM_SHA256（A 追加）	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
B	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	8	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	10	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA（B）	12	TLS_RSA_WITH_AES_128_CBC_SHA（B）
D	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_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_RSA_WITH_AES_256_CBC_SHA（D 追加）	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
E	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	7	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	9	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_CBC_SHA（E）	11	TLS_RSA_WITH_AES_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設定する方法）

I. プロトコルバージョン

SSL プロトコル：チェック有：TLS1.0、TLS1.1、TLS1.2

チェック無：SSL3.0

（図 1.1.2-2　仮想 SSL サーバ設定画面（プロトコル）-1 参照）

II. 暗号スイート

図 1.1.2-7　仮想 SSL サーバ暗号スイート選択画面　の「選択した暗号スイート」欄に、表 1.1.3.2-3 暗号スイートの設定（推奨セキュリティ型、個別指定）　の暗号スイートを「追加」する。

表 1.1.3.2-3　暗号スイートの設定（推奨セキュリティ型、個別指定）

優先順位	暗号スイート
-	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_256_GCM_SHA384
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA

※優先順位は、別の設定で指定。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)または 384bit(secp384r1)である。

IV. サーバクライアントの優先順位の設定

図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1 によりサーバ優先に設定する。

V. 暗号スイートの優先順位の設定

暗号スイートに優先順位を付与する設定を行った場合、設定したグループの順番に従って優先度が

付与される。

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 1.1.3.2-4　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）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。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推奨セキュリティ型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）

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_GCM_SHA256 (A 追加)	1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (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_CBC_SHA (A 追加)	3	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (A 追加)
B	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	4	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	5	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA (B)	6	TLS_RSA_WITH_AES_128_CBC_SHA (B)
D	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)	7	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)	8	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(D 追加)
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)	9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (D 追加)
E	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	10	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	11	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA (E)	12	TLS_RSA_WITH_AES_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

SSL プロトコル：チェック有：SSL3.0、TLS1.0、TLS1.1、TLS1.2

チェック無：

（図 1.1.2-2　仮想 SSL サーバ設定画面（プロトコル）-1 参照）

II. 暗号スイート

図 1.1.2-7　仮想 SSL サーバ暗号スイート選択画面の「選択した暗号スイート」欄に、表 1.1.3.3-1 暗号スイートの設定（セキュリティ例外型、文字列指定） の「グループ化文字列」を「追加」する。

表 1.1.3.3-1　暗号スイートの設定（セキュリティ例外型、文字列指定）

優先順位	グループ化文字列
-	ECDHE_RSA
	AES_GCM
	AES
	SHA

※優先順位を付与する設定を行った場合、グループ化文字列に対して優先度が付与されます。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)または 384bit(secp384r1)である。

IV. サーバクライアントの優先順位の設定

図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1 によりサーバ優先に設定する。

V. 暗号スイートの優先順位の設定

暗号スイートに優先順位を付与する設定を行った場合、設定したグループの順番に従って優先度が付与される。ただし、グループ内の順位は制御出来ない(詳細な制御は、③の設定が必要)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。

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） 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。使用可能な 14 の暗号スイートと設定ガイドラインのセキュリティ例外型の優先順位の違いは、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）の通りである。

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）

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_GCM_SHA256（A 追加）	2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（A 追加）	4	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256(A 追加)
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）	6	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
B	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	8	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	10	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA（B）	12	TLS_RSA_WITH_AES_128_CBC_SHA（B）
D	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	1	TLS_ECDHE_RSA_WITH_AES_256_GCM_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_RSA_WITH_AES_256_CBC_SHA（D 追加）	5	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
E	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	7	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	9	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_CBC_SHA（E）	11	TLS_RSA_WITH_AES_256_CBC_SHA（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	14	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	13	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

SSL プロトコル：チェック有：SSL3.0、TLS1.0、TLS1.1、TLS1.2

チェック無：

（図 1.1.2-2　仮想 SSL サーバ設定画面（プロトコル）-1 参照）

II. 暗号スイート

図 1.1.2-7　仮想 SSL サーバ暗号スイート選択画面の「選択した暗号スイート」欄に、表 1.1.3.3-3 暗号スイートの設定（セキュリティ例外型、個別指定）の暗号スイートを「追加」する。

表 1.1.3.3-3　暗号スイートの設定（セキュリティ例外型、個別指定）

優先順位	暗号スイート
-	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_RSA_WITH_AES_128_GCM_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA256
	TLS_RSA_WITH_AES_128_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_256_GCM_SHA384
	TLS_RSA_WITH_AES_256_CBC_SHA256
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_RC4_128_SHA
	TLS_RSA_WITH_3DES_EDE_CBC_SHA

※優先順位は、別の設定で指定。

III. DH/DHE、ECDH/ECDHE の鍵長

ECDHE の鍵長は 256bit(secp256r1)または 384bit(secp384r1)である。

IV. サーバクライアントの優先順位の設定

図 1.1.2-11　仮想 SSL サーバ設定画面（サーバクライアントの優先順位）-1 によりサーバ優先に設定する。

V. 暗号スイートの優先順位の設定
暗号スイートに優先順位を付与する設定を行った場合、設定したグループの順番に従って優先度が付与される。

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 1.1.3.3-4 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）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。使用可能な 14 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）

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_GCM_SHA256（A 追加）	1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（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_CBC_SHA（A 追加）	3	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA（A 追加）
B	TLS_RSA_WITH_AES_128_GCM_SHA256（B）	4	TLS_RSA_WITH_AES_128_GCM_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA256（B）	5	TLS_RSA_WITH_AES_128_CBC_SHA256（B）
	TLS_RSA_WITH_AES_128_CBC_SHA（B）	6	TLS_RSA_WITH_AES_128_CBC_SHA（B）
D	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）	7	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）	8	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（D 追加）
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）	9	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（D 追加）
E	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	10	TLS_RSA_WITH_AES_256_GCM_SHA384（E）
	TLS_RSA_WITH_AES_256_CBC_SHA256（E）	11	TLS_RSA_WITH_AES_256_CBC_SHA256（E）
	TLS_RSA_WITH_AES_256_CBC_SHA（E）	12	TLS_RSA_WITH_AES_256_CBC_SHA（E）
G	TLS_RSA_WITH_RC4_128_SHA（G）	13	TLS_RSA_WITH_RC4_128_SHA（G）
H	TLS_RSA_WITH_3DES_EDE_CBC_SHA（H）	14	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

  富士通 IPCOM EX2-3500

  (IPCOM EX2-3000 IN ソフトウェア V01 ソフトウェア版数: V01L03)

  搭載オプション

  1000BASE-T インターフェースカード 2

  暗号カード B

  IPCOM EX2-3500／3200 用 HDD1

  SSL アクセラレータオプション

  SSL アクセラレータ機能を使用するには、暗号カードと SSL アクセラレータオプションが必要。
  暗号カードには 2 種類あり、今回は「暗号カード B」を搭載している。
  「暗号カード A」「暗号カード B」でサポートされる暗号スイートは同一である。

  ・以下の機種の SSL アクセラレータ機能で「暗号カード A」「暗号カード B」を利用可能。
  IPCOM EX2-3200(EX2-3000 SC ソフトウェア／LB ソフトウェア／IN ソフトウェア)
  IPCOM EX2-3500(EX2-3000 SC ソフトウェア／LB ソフトウェア／IN ソフトウェア)

- 参考情報

  FUJITSU Network IPCOM EX2 ソフトウェアシリーズ V01L03 コマンドリファレンスガイド
  FUJITSU Network IPCOM EX2 ソフトウェアシリーズ V01L03 ユーザーズガイド
  FUJITSU Network IPCOM EX2 ソフトウェアシリーズ V01L03 コンソールリファレンスガイド