Thunder 3030S

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 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」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 1-1 暗号設定内容の表記例

表 1-1 暗号設定内容の表の見方

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 1-1 中の番号。

1.1. A10 ネットワークス Thunder シリーズ

本章では、Thunder 3030S 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。両方の証明書を一つの仮想サーバに設定した場合、ECDSA 証明書の暗号スイートが優先される。Thunder シリーズは SSL/TLS プロトコルバージョンおよび暗号スイートの選択が可能である。そのため、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・分析を (1) RSA 証明書設定時、(2) ECDSA 証明書設定時に分けて記載する。

1.1.1. デフォルトでの暗号設定内容の調査

(1) RSA 証明書設定時

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	ON	クライアント	13
tls1.1	ON	クライアント	6
tls1.0	ON	クライアント	6
sslv3	OFF	ー	ー
sslv2	設定不可	ー	ー

- A10 ネットワークス Thunder 3030S 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
0xC0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA		A追加	A追加	secp256r1	ON	ON	ON
0xC0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		A追加	A追加	secp256r1	ON	OFF	OFF
0xC0,0x2F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	β追加	A追加	A追加	secp256r1	ON	OFF	OFF
0xC0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA		D追加	D追加	secp256r1	ON	ON	ON
0xC0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	α追加	D追加	D追加	secp256r1	ON	OFF	OFF
0x00,0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA			H追加	-	ON	ON	ON
0x00,0x2F	TLS_RSA_WITH_AES_128_CBC_SHA		B	B	-	ON	ON	ON
0x00,0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256		B	B	-	ON	OFF	OFF
0x00,0x9C	TLS_RSA_WITH_AES_128_GCM_SHA256		B	B	-	ON	OFF	OFF
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA		E	E	-	ON	ON	ON
0x00,0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256		E	E	-	ON	OFF	OFF
0x00,0x9D	TLS_RSA_WITH_AES_256_GCM_SHA384		E	E	-	ON	OFF	OFF
0x00,0x05	TLS_RSA_WITH_RC4_128_SHA			G	-	ON	ON	ON

- Extension

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

(2) ECDSA 証明書設定時

表 1.1.1-2　暗号設定内容（デフォルト、ECDSA 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	ON	クライアント	5
tls1.1	ON	クライアント	4
tls1.0	ON	クライアント	4
sslv3	OFF	ー	ー
sslv2	設定不可	ー	ー

- A10 ネットワークス Thunder 3030S 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
0xc0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		A 追加	A 追加	secp256r1	ON	ON	ON
0xc0,0x0a	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA		D 追加	D 追加	secp256r1	ON	ON	ON
0xc0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		A 追加	A 追加	secp256r1	ON	OFF	OFF
0xc0,0x2b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	β追加	A 追加	A 追加	secp256r1	ON	ON	ON
0xc0,0x2c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	α追加	D 追加	D 追加	secp256r1	ON	ON	ON

- Extension

name	id	tls1.2	tls1.1	tls1.0	sslv3	sslv2
signature_algorithms	13	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方法

A) ターミナルソフトより機器にログインし、コンフィグレーションモードに入る。

B) 対象のクライアント SSL テンプレート名を入力し、テンプレート設定モードに入る。

C) 「version」コマンドにてセキュリティバージョンを設定する。

```
Thunder>
Thunder>enable
Password:
Thunder#
Thunder#configure terminal
Thunder(config)#
Thunder(config)#slb template client-ssl test-clssl
Thunder(config-client ssl)#
Thunder(config-client ssl)#version 33 30
Thunder(config-client ssl)#
```

※セキュリティバージョンと設定値の対応は下記の通り。

30: SSLv3.0

31: TLSv1.0

32: TLSv1.1

33: TLSv1.2

II.　暗号スイートの指定方法

A)　ブラウザで管理画面にログインし、「ADC」－「テンプレート」をクリックする。

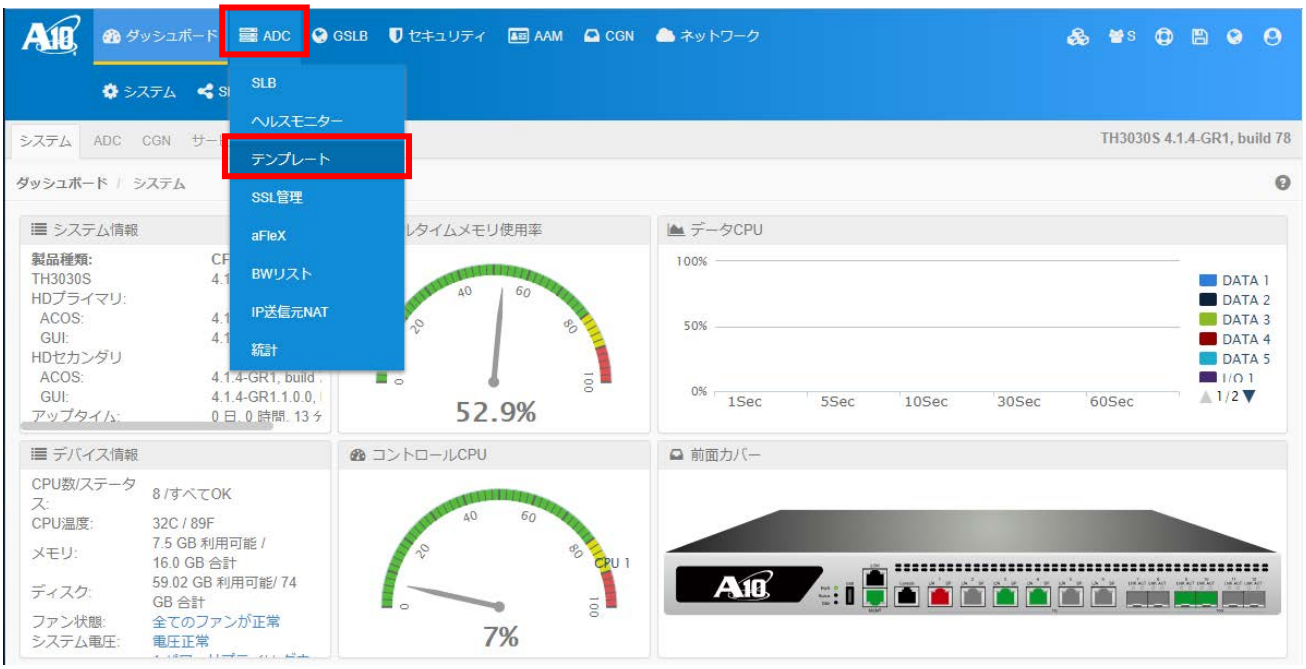

図 1.1.2-1　Thunder 管理画面

B)　SLB テンプレート一覧画面が表示されたら「SSL」をクリックする。

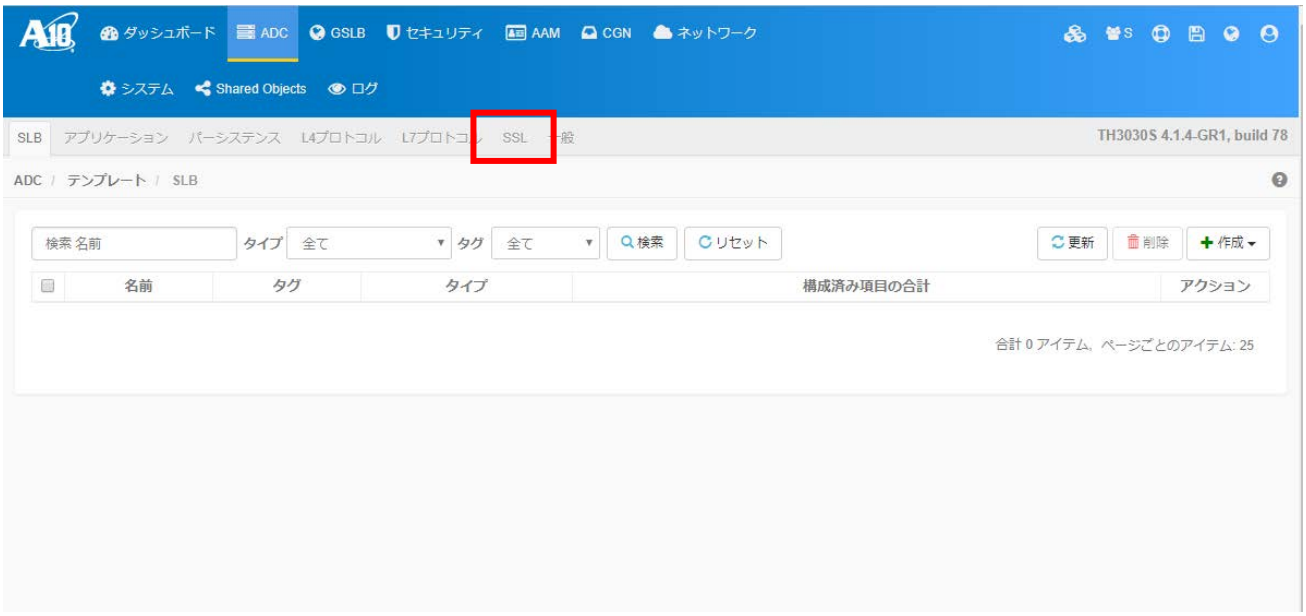

図 1.1.2-2　SLB テンプレート一覧画面

C) SSL テンプレートー覧画面が表示されたら「作成」ー 「SSL 暗号」をクリックする。

図 1.1.2-3 SSL テンプレートー覧画面

D) SSL サイファーテンプレート画面が表示されたら、「名前」欄に名前を入力する。

E) 「追加」ボタンを押下し暗号リストを追加し、SSL スイートをドロップダウンリストから選択し、「プライオリティ」欄で優先度を入力してからフロッピーディスクのアイコンを押下し確定する。

F) さらに追加で暗号スイートを増やしたい場合は E)の手順を繰り返し、追加し終えたら「はい」ボタンを押下する。

図 1.1.2-4 SSL サイファーテンプレート画面

G) SSL テンプレート一覧画面で設定したクライアント SSL テンプレートの「編集」をクリックする。

図 1.1.2-5 SSL テンプレート一覧画面

H) 「一般的なフィールド」内の「Cipher の選択」で「Cipher テンプレート」のラジオボタンを有効にし、「Cipher テンプレート」のリストで作成した SSL サイファーテンプレート（例：cipher-list）を選択する。

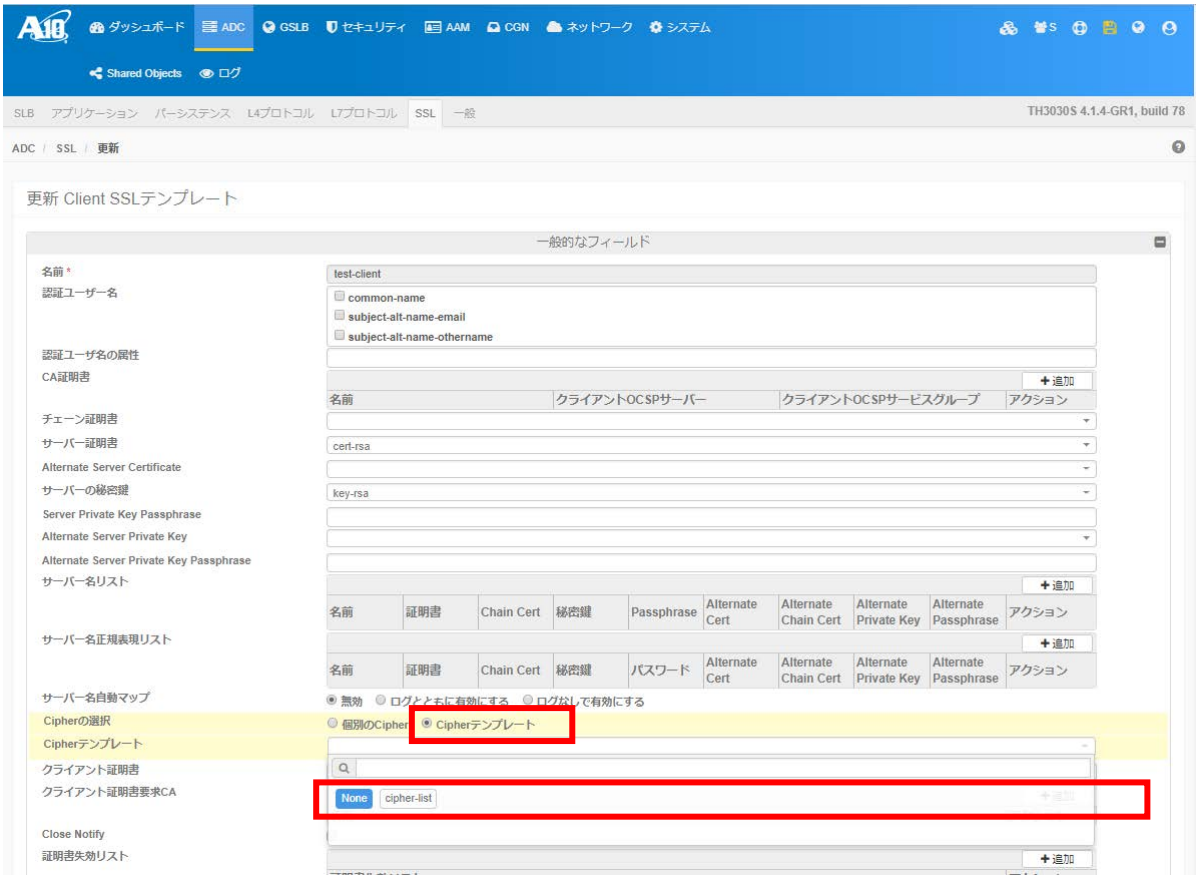

図 1.1.2-6 クライアント SSL テンプレート設定画面

I)　設定が完了したら、画面下部にある「更新」ボタンを押下する。

図 1.1.2-7　クライアント SSL テンプレート設定画面

J)　SSL テンプレート一覧画面に戻るのでフロッピーディスクのアイコンをクリックし、設定を保存する。

図 1.1.2-8　SSL テンプレート一覧画面

III. DH/DHE、ECDH/ECDHE の鍵長の設定方法

A) クライアント SSL テンプレート画面にて、ECDHE の鍵長は「EC Name list」欄の「追加」を押下し EC 名リストを追加し、EC 名をドロップダウンリストから選択してから、フロッピーディスクのアイコンをクリックする。
DHE の鍵長は「Diffie-Hellman パラメータ」欄のドロップダウンリストより選択する。

B) 選択し終えたら画面下部の「更新」ボタンをクリックする。

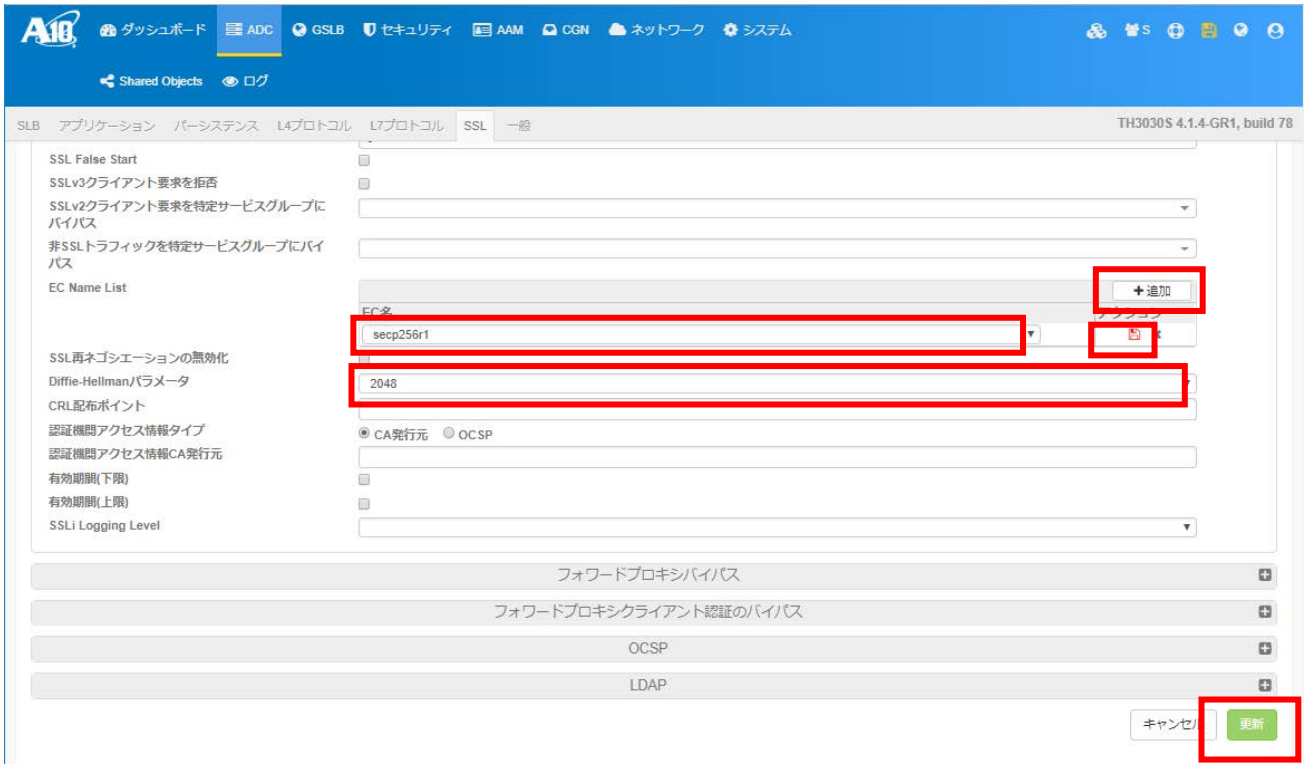

図 1.1.2-9　クライアント SSL テンプレート画面

C) 図 1.1.2-8　SSL テンプレート一覧画面に戻るのでフロッピーディスクのアイコンをクリックし、設定を保存する。

IV. サーバクライアントの優先順位の設定
既定は、クライアント優先である。
SSL サイファーテンプレートを設定した場合、サーバ優先となる。

V. 暗号スイートの優先順位の設定
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

(1) RSA 証明書設定時

暗号スイート、プロトコルバージョン、DH/DHE,ECDH/ECDHE の鍵長を具体的に設定する方法によって、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た設定

I. プロトコルバージョン

プロトコルバージョン設定により TLS1.2 のみ有効にする。

II. 暗号スイート

SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティの値を表 1.1.3.1-1 暗号スイートの設定(高セキュリティ型、RSA 証明書設定時)の様に設定する。

表 1.1.3.1-1 暗号スイートの設定(高セキュリティ型、RSA 証明書設定時)

プライオリティ	暗号スイート
100	TLS1_DHE_RSA_AES_256_GCM_SHA384
100	TLS1_ECDHE_RSA_AES_256_GCM_SHA384
90	TLS1_DHE_RSA_AES_256_GCM_SHA384
90	TLS1_ECDHE_RSA_AES_256_GCM_SHA384

※「プライオリティ」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

DH/DHE： 2048 を設定する。

ECDH/ECDHE：secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定

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。

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。

高セキュリティ型に含まれる暗号スイート 12 個のうち、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。なお、設定ガイドラインのグループ内の優先順位は考慮しない。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし

(2) ECDSA 証明書設定時

暗号スイート、プロトコルバージョン、DH/DHE,ECDH/ECDHE の鍵長を具体的に設定する方法によって、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た設定

I. プロトコルバージョン

プロトコルバージョン設定により TLS1.2 のみ有効にする。

II. 暗号スイート

SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティの値を表 1.1.3.1-2 暗号スイートの設定(高セキュリティ型、ECDSA 証明書設定時)の様に設定する。

表 1.1.3.1-2 暗号スイートの設定(高セキュリティ型、ECDSA 証明書設定時)

プライオリティ	暗号スイート
100	TLS1_ECDHE_ECDSA_AES_256_GCM_SHA384
90	TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256

※「プライオリティ」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

ECDH/ECDHE：secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定

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。

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。

高セキュリティ型に含まれる暗号スイート 12 個のうち、2 個の暗号スイートの使用が可能である。使用可能な 2 個の暗号スイートの優先順位は、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。なお、設定ガイドラインのグループ内の優先順位は考慮しない。

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) RSA 証明書設定時

暗号スイート、プロトコルバージョン、DH/DHE,ECDH/ECDHE の鍵長を具体的に設定する方法によって、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た設定

I. プロトコルバージョン

プロトコルバージョン設定より TLS1.2、TLS1.1、TLS1.0 のみ有効にする。

II. 暗号スイート

SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティの値を表 1.1.3.2-1 暗号スイートの設定(推奨セキュリティ型、RSA 証明書設定時)の様に設定する。

表 1.1.3.2-1 暗号スイートの設定(推奨セキュリティ型、RSA 証明書設定時)

プライオリティ	暗号スイート
100	TLS1_DHE_RSA_AES_128_GCM_SHA256
100	TLS1_DHE_RSA_AES_128_SHA256
100	TLS1_DHE_RSA_AES_128_SHA
100	TLS1_ECDHE_RSA_AES_128_GCM_SHA256
100	TLS1_ECDHE_RSA_AES_128_SHA256
100	TLS1_ECDHE_RSA_AES_128_SHA
90	TLS1_RSA_AES_128_GCM_SHA256
90	TLS1_RSA_AES_128_SHA256
90	TLS1_RSA_AES_128_SHA
80	TLS1_DHE_RSA_AES_256_GCM_SHA384
80	TLS1_DHE_RSA_AES_256_SHA256
80	TLS1_DHE_RSA_AES_256_SHA
80	TLS1_ECDHE_RSA_AES_256_GCM_SHA384
80	TLS1_ECDHE_RSA_AES_256_SHA384
80	TLS1_ECDHE_RSA_AES_256_SHA
70	TLS1_RSA_AES_256_SHA256
70	TLS1_RSA_AES_256_SHA

※「プライオリティ」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

DH/DHE： 2048 もしくは 1024 を設定する。

ECDH/ECDHE：secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定

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。

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、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。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

(2) ECDSA 証明書設定時

暗号スイート、プロトコルバージョン、DH/DHE,ECDH/ECDHE の鍵長を具体的に設定する方法によって、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た設定

I. プロトコルバージョン

プロトコルバージョン設定より TLS1.2、TLS1.1、TLS1.0 のみ有効にする。

II. 暗号スイート

SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティの値を表 1.1.3.2-2 暗号スイートの設定(推奨セキュリティ型、ECDSA 証明書設定時)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、ECDSA 証明書設定時)

プライオリティ	暗号スイート
100	TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256
100	TLS1_ECDHE_ECDSA_AES_128_SHA256
100	TLS1_ECDHE_ECDSA_AES_128_SHA
80	TLS1_ECDHE_ECDSA_AES_256_GCM_SHA384
80	TLS1_ECDHE_ECDSA_AES_256_SHA

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

VII. DH/DHE、ECDH/ECDHE の鍵長

ECDH/ECDHE：secp384r1 もしくは secp256r1 を設定する。

VIII. サーバクライアントの優先順位の設定

サーバ優先となる。

IX. 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。

X. 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、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推奨セキュリティ型の順位と同じである。

IV. 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) RSA 証明書設定時

暗号スイート、プロトコルバージョン、DH/DHE,ECDH/ECDHE の鍵長を具体的に設定する方法によって、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た設定

I. プロトコルバージョン

プロトコルバージョン設定より TLS1.2、TLS1.1、TLS1.0、SSL3.0 のみ有効にする。

II. 暗号スイート

SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティの値を表 1.1.3.3-1 暗号スイートの設定(セキュリティ例外型、RSA 証明書設定時)の様に設定する。

表 1.1.3.3-1 暗号スイートの設定(セキュリティ例外型、RSA 証明書設定時)

プライオリティ	暗号スイート
100	TLS1_DHE_RSA_AES_128_GCM_SHA256
100	TLS1_DHE_RSA_AES_128_SHA256
100	TLS1_DHE_RSA_AES_128_SHA
100	TLS1_ECDHE_RSA_AES_128_SHA256
100	TLS1_ECDHE_RSA_AES_128_SHA
90	TLS1_RSA_AES_128_GCM_SHA256
90	TLS1_RSA_AES_128_SHA256
90	TLS1_RSA_AES_128_SHA
80	TLS1_DHE_RSA_AES_256_GCM_SHA384
80	TLS1_DHE_RSA_AES_256_SHA256
80	TLS1_DHE_RSA_AES_256_SHA
80	TLS1_ECDHE_RSA_AES_256_GCM_SHA384
80	TLS1_ECDHE_RSA_AES_256_SHA
70	TLS1_RSA_AES_256_GCM_SHA384
70	TLS1_RSA_AES_256_SHA256
70	TLS1_RSA_AES_256_SHA
60	SSL3_RSA_RC4_128_SHA
50	SSL3_RSA_DES_192_CBC3_SHA

※「プライオリティ」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
DH/DHE： 2048 もしくは 1024 を設定する。
ECDH/ECDHE：secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定
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。

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 67 個のうち、19 個の暗号スイートの使用が可能である。使用可能な 19 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。

V. DH/DHE、ECDH/ECDHE の鍵長
差分なし。

(2) ECDSA 証明書及び RSA 証明書(RC4 暗号スイート用)設定時

暗号スイート、プロトコルバージョン、DH/DHE,ECDH/ECDHE の鍵長を具体的に設定する方法によって、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た設定

I. プロトコルバージョン

プロトコルバージョン設定より TLS1.2、TLS1.1、TLS1.0、SSL3.0 のみ有効にする。

II. 暗号スイート

SSL サイファーテンプレートで暗号スイートを設定する際にプライオリティの値を表 1.1.3.3-2 暗号スイートの設定(セキュリティ例外型、ECDSA 証明書及び RSA 証明書(RC4 暗号用)設定時)の様に設定する。

表 1.1.3.3-2 暗号スイートの設定(セキュリティ例外型、ECDSA 証明書及び RSA 証明書(RC4 暗号用)設定時)

プライオリティ	暗号スイート
100	TLS1_ECDHE_ECDSA_AES_128_GCM_SHA256
100	TLS1_ECDHE_ECDSA_AES_128_SHA256
100	TLS1_ECDHE_ECDSA_AES_128_SHA
80	TLS1_ECDHE_ECDSA_AES_256_GCM_SHA384
80	TLS1_ECDHE_ECDSA_AES_256_SHA
60	SSL3_RSA_RC4_128_SHA

※「プライオリティ」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

ECDH/ECDHE：secp384r1 もしくは secp256r1 を設定する。

IV. サーバクライアントの優先順位の設定

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。

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 64 個のうち、7 個の暗号スイートの使用が可能である。使用可能な 7 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。

III. DH/DHE、ECDH/ECDHE の鍵長

差分なし。

付属情報

- **製品情報**
  A10 ネットワークス Thunder 3030S ソフトウェアバージョン: 4.1.4-GR1

- **参考情報**
  A10_4.1.4-GR1_CLI.pdf
  A10_4.1.4-GR1_CLI-SLB.pdf