Netwiser SX-3850

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

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。 「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. セイコーソリューションズ Netwiser シリーズ

本章では、Netwiser SX-3850 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	15
tls1.1	設定不可	ー	ー
tls1.0	ON	クライアント	5
sslv3	OFF	ー	0
sslv2	設定不可	ー	ー

- Netwiser SX-3850 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
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256		A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x6b	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256		D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9e	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	β	A	A	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x9f	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	α	D	D	1024bit	ON	OFF	OFF	OFF	OFF
0x00,0x04	TLS_RSA_WITH_RC4_128_MD5				---	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
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 WEB 管理画面にログインし、(1) 設定ー (2) バランシングー (3) SSL アクセラレーションー (4) SSL アクセラレーションをクリックして SSL アクセラレーション選択画面を表示する。SSL アクセラレーション選択画面の (5) SSL3.0 有効/無効欄のチェックボックスを選択して、SSL3.0 を有効にするか無効にするかを操作する。

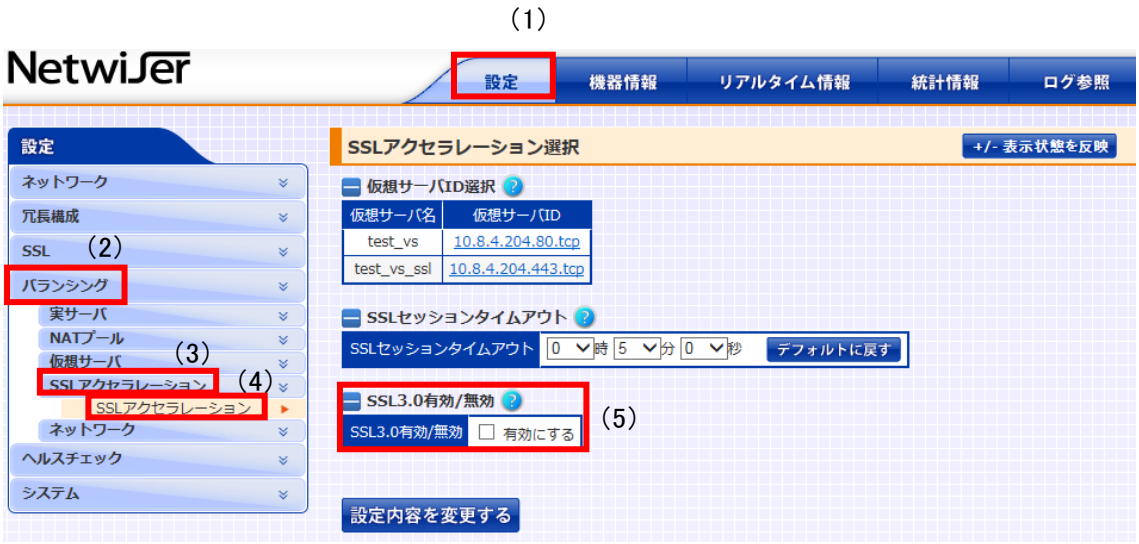

図 1.1.2-1　SSL アクセラレーション選択画面-1

II.　暗号スイートの設定

A)SSL アクセラレーション選択画面で設定したい (6) 仮想サーバ ID を選択する。

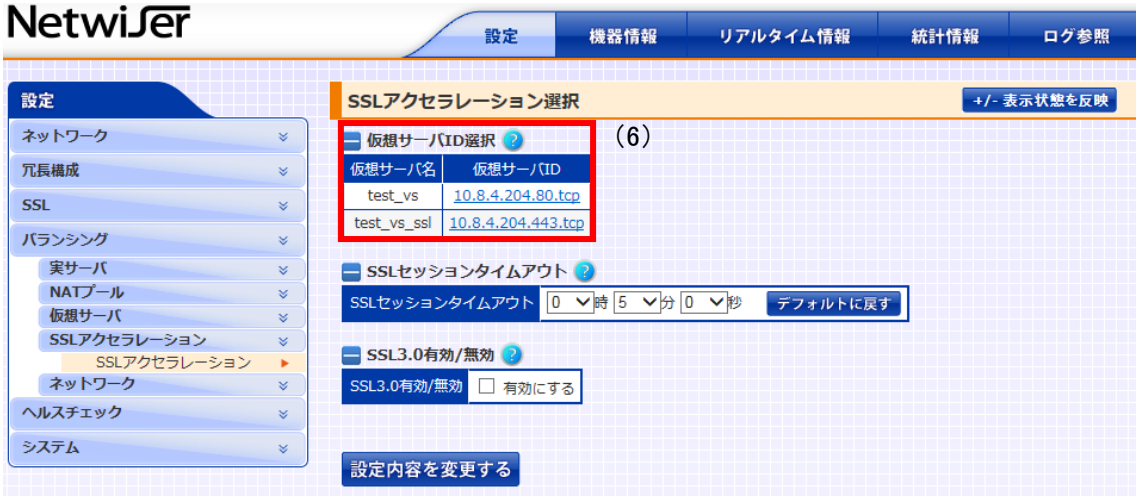

図 1.1.2-2　SSL アクセラレーション選択画面-2

B)SSL アクセラレーション設定画面の（7）SSL アクセラレーション詳細設定欄に、設定したい暗号スイートのチェックボックスにチェックを入れて暗号スイートを指定する。

図 1.1.2-3　SSL アクセラレーション設定画面

※デフォルトで有効になっている暗号スイート：RC4-MD5、RC4-SHA、DES-CBC3-SHA、AES128-SHA、DHE-AES128-SHA、AES256-SHA、DHE-AES256-SHA、AES128-SHA256、AES256-SHA256、DHE-AES128-SHA256、DHE-AES256-SHA256、AES128-GCM-SHA256、AES256-GCM-SHA384、DHE-RSA-AES128-GCM-SHA256、DHE-RSA-AES256-GCM-SHA384

III. DH/DHE、ECDH/ECDHE の鍵長の設定

製品独自の設定方法なし

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

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、tls1.0 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）Netwiser SX-3850 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：1024bit

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。

※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

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

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。

tls1.0 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 13 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 1.1.3.1-1　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）	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(α)
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(β)
-	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	TLS_RSA_WITH_RC4_128_MD5
		TLS_RSA_WITH_RC4_128_SHA
		TLS_RSA_WITH_3DES_EDE_CBC_SHA
		TLS_RSA_WITH_AES_128_CBC_SHA
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA
		TLS_RSA_WITH_AES_256_CBC_SHA
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA
		TLS_RSA_WITH_AES_128_CBC_SHA256
		TLS_RSA_WITH_AES_256_CBC_SHA256
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
		TLS_RSA_WITH_AES_128_GCM_SHA256
		TLS_RSA_WITH_AES_256_GCM_SHA384

※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

SSL3.0 有効/無効：(チェックを外す)

TLS1.0、TLS1.1 の設定はない。

（図 1.1.2-1 参照）

II. 暗号スイート

1.1.2.II.B 図 1.1.2-3　SSL アクセラレーション設定画面 の SSL アクセラレーション詳細設定で下記暗号スイートのチェックボックスにチェックを入れる。

DHE-AES256-GCM-SHA384、DHE-AES128-GCM-SHA256

※クライアント優先のため、優先順位は設定されない。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。

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
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
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。
※TLS1.0 の設定はないが、1.1.3.1 ③Ⅱ.暗号スイートで設定した暗号スイートが使えるプロトコルバージョンが TLS1.2 のみであるため、結果として TLS1.2 のみ有効になる。

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 1.1.3.1-2　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 2 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 1.1.3.1-2　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）	暗号スイート設定結果
α	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384（α）
β	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256（β）

※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

差分なし。

TLS1.1 が無効である。

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 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）

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
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)
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)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	TLS_RSA_WITH_AES_128_GCM_SHA256(B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA(D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256(D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)
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)
	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	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	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

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

SSL3.0 有効/無効: （チェックを外す）　（図 1.1.2-1 参照）

II. 暗号スイート

図 1.1.2-3　SSL アクセラレーション設定画面 の SSL アクセラレーション詳細設定で下記暗号スイートのチェックボックスにチェックを入れる。

AES128-SHA、AES128-SHA256、AES256-SHA、AES256-SHA256、AES128-GCM-SHA256、AES256-GCM-SHA384、DHE-AES128-SHA、DHE-AES128-SHA256、DHE-AES128-GCM-SHA256、DHE-AES256-SHA、DHE-AES256-SHA256、DHE-AES256-GCM-SHA384

※クライアント優先のため、優先順位は設定されない。

III. DH/DHE、ECDH/ECDHE の鍵長

DH/DHE：設定がなく、既定で 1024bit である。

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
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
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、下の表 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 12 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）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA(B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256(B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256(B)	TLS_RSA_WITH_AES_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_AES_256_CBC_SHA256(D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA(E)	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256(E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384(E)	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

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。

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）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 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）

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
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
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)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
D	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (D)
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)

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
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）
	TLS_RSA_WITH_AES_256_GCM_SHA384（E）	TLS_RSA_WITH_AES_256_GCM_SHA384（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
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
SSL3.0 有効/無効: （チェックを入れる）　（図 1.1.2-1 参照）

II. 暗号スイート
1.1.2.II.B 図 1.1.2-3　SSL アクセラレーション設定画面 の SSL アクセラレーション詳細設定で下記暗号スイートのチェックボックスにチェックを入れる。
RC4-SHA、DES-CBC3-SHA、AES128-SHA、AES128-SHA256、AES256-SHA、AES256-SHA256、AES128-GCM-SHA256、AES256-GCM-SHA384、DHE-AES128-SHA、DHE-AES128-SHA256、DHE-AES128-GCM-SHA256、DHE-AES256-SHA、DHE-AES256-SHA256、DHE-AES256-GCM-SHA384

※クライアント優先のため、優先順位は設定されない。

III. DH/DHE、ECDH/ECDHE の鍵長
DH/DHE：設定がなく、既定で 1024bit である。

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

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

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 1.1.3.3-2　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 14 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）	暗号スイート設定結果
A	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (A)
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (A)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (A)
B	TLS_RSA_WITH_AES_128_CBC_SHA (B)	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)	TLS_RSA_WITH_AES_128_CBC_SHA256 (B)
	TLS_RSA_WITH_AES_128_GCM_SHA256 (B)	TLS_RSA_WITH_AES_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_AES_256_CBC_SHA256 (D)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (D)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (D)
E	TLS_RSA_WITH_AES_256_CBC_SHA (E)	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)
	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)	TLS_RSA_WITH_AES_256_CBC_SHA256 (E)
	TLS_RSA_WITH_AES_256_GCM_SHA384 (E)	TLS_RSA_WITH_AES_256_CBC_SHA (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)

※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。

1.2. 付属情報

- 製品情報
  Netwiser SX-3850 ファームウェアバージョン v7.3.20 built on 2016/03/16 17:03 (secondary v7.3.20)

- 参考情報
  SX-3840,45,50 取扱説明書(第 1.1 版)
  Netwiser SX-38 シリーズ　導入・運用の手引(第 2.1 版)
  Netwiser SX-38 シリーズ コマンドリファレンス(第 1.4 版)

- 製品シリーズについて
  下記製品は SX-38xx シリーズ共通。
  SX-3850/SX-3845/SX-3840/SX-3820