

SX-39、SX-38シリーズ技術資料

SSL証明書更新手順書

GUI操作編

対象機種:SX-39、SX-38シリーズ全機種

2019年2月

セイコーソリューションズ株式会社

はじめに

本手順書では新規証明書で不具合が発生した場合を考慮し、新規にSSLポリシー名を作成して新規証明をインポートする手順となっております。

既存のSSLポリシー名に新規証明書をインポートすることも可能ですが既存の証明書はクリアされてしましますのでご注意ください。

冗長構成の場合、『コマンド同期』設定が「有効」に設定されていれば、1台の機器を操作するだけ相手機器側にも設定が反映されます。

『コマンド同期』の設定は下記操作にて確認することが出来ます。

”WEB管理画面TOP→設定→冗長構成→同期設定”を選択

The screenshot shows the Netwiser web management interface. At the top, there are tabs for 'Setting' and 'Machine Information'. On the left, a sidebar titled 'Setting' lists several options: 'Network', 'Redundant Configuration', 'SSL', 'Balancing', 'Health Check', and 'System'. Under 'Redundant Configuration', 'Sync Setting' is selected. The main content area is titled 'Sync Setting' and contains two sections: 'Command Sync Setting' and 'Session Sync Setting'. In the 'Command Sync Setting' section, there is a table with one row:

Item Name	Input
Command Sync	<input checked="" type="checkbox"/> Enable

In the 'Session Sync Setting' section, there are two rows:

Item Name	Input
Session Sync	<input checked="" type="checkbox"/> Enable
Session Sync at Startup	<input checked="" type="checkbox"/> Enable

A blue button at the bottom right says 'Change setting content'.

1) 新規にSSLポリシー名を作成

”WEB管理画面TOP→設定→SSL→SSL証明書”を選択

The screenshot shows the Netwiser web management interface. The top navigation bar has tabs for '設定' (Setting) and '機器情報' (Device Information). The main left sidebar menu under '設定' includes 'ネットワーク', '冗長構成', 'SSL' (which is selected and highlighted in green), and 'パラシング', 'ヘルスチェック', 'システム', and 'かんたん設定'. The right panel is titled 'SSL証明書' (SSL Certificate) and contains a sub-menu 'SSLポリシー設定'. It lists two entries: 'year2014' and 'year2015'. The entry 'year2015' is highlighted with a red border. Below the list is a blue button labeled '行追加' (Add Row). At the bottom of the right panel is a large red-bordered button labeled '設定内容を変更する' (Change Configuration Content).

※ 上記例(year2015)のように、新たなSSLポリシー名を入力してください。
入力後、「設定内容を変更する」ボタンを押してください。

NetwiserでSSL証明書署名要求作成(CSR)を行う必要が無い場合は
2)の操作は不要です。3)SSL証明書及び鍵のインポート操作に進んでください。

2) SSL証明書署名要求(CSR)及び秘密鍵の作成

"WEB管理画面TOP→設定→SSL→SSL証明書署名要求作成"を選択

The screenshot shows the Netwiser web management interface. The top navigation bar includes tabs for '設定' (Setting), '機器情報' (Machine Information), and 'リアルタイム情報' (Real-time Information). The left sidebar under the '設定' tab has a 'SSL' section highlighted with a green box, containing options like 'SSL証明書', '証明書失効リスト', 'プロキシサーバ', 'SSL証明書署名要求作成' (which is also highlighted with a yellow box), 'SSLインポート', 'SSLエクスポート', and '鍵、証明書の削除'. The main content area is titled 'SSL証明書署名要求作成' and contains a 'CSR (署名要求) 設定' section. This section includes fields for 'SSLポリシー名' (set to 'year2015'), 'ECC証明書' (checkbox '有効' checked, marked with '※1'), '公開鍵長' (set to '2048'), '楕円曲線パラメータ' (set to '未選択'), 'サーバのFQDN' (empty), '国名 (Country)' (empty), '都道府県 (State)' (empty), '区市町村 (Locality)' (empty, marked with '※2'), '組織名 (Organization)' (empty), '部門名 (Organization Unit)' (empty), and 'メールアドレス (Email Address)' (empty). A red box highlights the '年' dropdown in the SSL policy name field and the 'Locality' field.

※1 1)にて作成したSSLポリシー名及び公開鍵長を選択してください。

ECC証明書を利用する場合は「有効」にチェックをして、楕円曲線パラメータの項目を選択してください。

(SX-3920、SX-3820はECC証明書を利用することはできません)

※2 CA局で必要とされる項目の登録を行って下さい。

設定後、「設定内容を変更する」ボタンを押してください。

"WEB管理画面TOP→設定→SSL→SSエクスポート"を選択

The screenshot shows the Netwiser web management interface. The top navigation bar includes tabs for '設定' (Setting), '機器情報' (Machine Information), 'リアルタイム情報' (Real-time Information), '統計情報' (Statistics Information), and 'ログ参照' (Log Reference). The left sidebar under the '設定' tab has a 'SSL' section highlighted with a green box, containing options like 'SSL証明書', '証明書失効リスト', 'プロキシサーバ', 'SSL証明書署名要求作成', 'SSLインポート', 'SSLエクスポート' (which is also highlighted with a yellow box), and '鍵、証明書の削除'. The main content area is titled 'SSLエクスポート' and contains a 'ファイル選択' (File Selection) section. It shows a table with columns: 'SSLポリシー名', '秘密鍵', '証明書', '中間証明書', 'CA局証明書(クライアント認証)', 'CSR(署名要求)', 'CRL(失効リスト)', and 'PKCS12形式'. There are two rows: one for 'year2014' (secret key 'key', certificate 'cert', intermediate certificate 'chain') and another for 'year2015' (secret key 'key', certificate 'cert', intermediate certificate 'chain', CSR file 'csr' marked with '※3'). A red box highlights the 'csr' file in the 'CSR(署名要求)' column for the 'year2015' row.

※3 CSRをマウスで右クリックして「対象ファイルに保存」を選択、CSRファイルを取得してください。

取得したCSRファイルをCA局へ申請し、証明書を受け取ってください。

3) SSL証明書及び鍵のインポート

"WEB管理画面TOP→設定→SSL→SSLインポート"を選択

The screenshot shows the Netwiser web management interface. The top navigation bar includes tabs for '設定' (Setting), '機器情報' (Equipment Information), 'リアルタイム情報' (Real-time Information), and '統計情報' (Statistics Information). The '設定' tab is currently selected.

The left sidebar contains a tree view of settings categories: ネットワーク, 冗長構成, SSL, バランシング, ヘルスチェック, システム, and かんたん設定. The 'SSL' category is expanded, and the 'SSLインポート' (SSL Import) option is highlighted with a green border.

The main content area is titled 'SSLインポート' (SSL Import). It displays '鍵、証明書情報' (Key, Certificate Information) with a table:

ポリシー名	サーバ証明書	中間証明書	CA証明書	秘密鍵
year2014	valid	valid		2048
year2015				

Below this is the 'ファイル選択' (File Selection) section, which is highlighted with a red box. It lists fields for selecting files:

- SSLポリシー名: year2015 (marked with an error icon)
- PKCS12形式: (input field with a browse button)
- 秘密鍵: (input field with a browse button)
- パスフレーズ: (input field)
- サーバ証明書: (input field with a browse button)
- 中間証明書: (input field with a browse button)
- CA局証明書(クライアント認証): (input field with a browse button)

A large blue button at the bottom of this section is labeled 'ファイルをインポートする' (Import File).

※1 1)で作成したSSLポリシー名(year2015)を選択してください。

※2 新規にインポートするファイルを選択し「ファイルをインポートする」ボタンを押してください。

- ・インポートするファイルがPKCS12形式(鍵、証明書が1つのファイル)の場合は、鍵、証明書欄を選択する必要はありません。
- ・鍵ファイル、証明書ファイルが別ファイルの場合はPKAS12形式欄を選択する必要ありません。各ファイルを選択し、まとめてインポートすることができます。
- ・中間証明書を2つインポートする必要がある場合は1つ目をインポートした後に、2つ目をインポートする際「階層化」を選択してください。
「上書き」を選択すると1つ目のファイルが削除されます。
- ・NetwiserにてSSL証明書署名要求(CSR)を行った場合は、秘密鍵は作成されていますので秘密鍵をインポートする必要はありません。

4) 証明書ファイルインポート結果の確認

インポートが正常に行われると下記例の様に証明書関係は「valid」
秘密鍵は鍵長(例では2048)が表示されます。

下記画面は中間証明書が階層化され2つのファイルがインポートされている例となります。

The screenshot shows the Netwiser configuration interface. The left sidebar has a 'SSL' section expanded, with 'SSLインポート' (SSL Import) selected. The main area displays the 'SSLインポート' (SSL Import) configuration. It includes a table for '鍵、証明書情報' (Key, Certificate Information) and a 'ファイル選択' (File Selection) table.

SSLインポート

鍵、証明書情報

ポリシー名	サーバ証明書	中間証明書	CA証明書	秘密鍵
year2014	valid	valid valid		2048
year2015	valid	valid valid		2048

ファイル選択

SSLポリシー名	未選択
PKCS12形式	[参照...]
秘密鍵	[参照...]
パスフレーズ	
サーバ証明書	[参照...]
中間証明書	[参照...] <input type="radio"/> 上書き <input checked="" type="radio"/> 階層化
CA局証明書(クライアント認証)	[参照...] <input type="radio"/> 上書き <input checked="" type="radio"/> 階層化

ファイルをインポートする

5)新たに作成したSSLポリシー名を仮想サーバに割り当てます。

”WEB管理画面TOP→設定→バランシング→SSLアクセラレーション”を選択

The screenshot shows the 'Netwiser' web management interface. The top navigation bar includes tabs for '設定' (Setting), '機器情報' (Equipment Information), 'リアルタイム情報' (Real-time Information), and '統計情報' (Statistics). The left sidebar under the '設定' tab has several sections: ネットワーク, 元長構成, SSL, バランシング, 実サーバ, NATプール, 仮想サーバ, SSLアクセラレーション, and システム. The 'SSLアクセラレーション' section is highlighted with a green border. The main content area is titled 'SSL Acceleration Selection'. It contains two sections: 'Virtual Server ID Selection' and 'SSL Session Timeout Out'. In the 'Virtual Server ID Selection' section, there is a text input field containing '10.208.14.45:443.tcp' with a red box around it, and a delete button (X). Below these sections is a blue button labeled '設定内容を変更する' (Change settings).

※ SSL証明書を割り当てる仮想サーバIDを選択してください。

The screenshot shows the 'Netwiser' web management interface. The top navigation bar includes tabs for '設定' (Setting), '機器情報' (Equipment Information), 'リアルタイム情報' (Real-time Information), and '統計情報' (Statistics). The left sidebar under the '設定' tab has several sections: ネットワーク, 元長構成, SSL, バランシング, 実サーバ, NATプール, 仮想サーバ, SSLアクセラレーション, and システム. The 'SSLアクセラレーション' section is highlighted with a green border. The main content area is titled 'SSL Acceleration Configuration'. It contains two sections: 'SSL Certificate Assignment' and 'SSL Acceleration Detailed Settings'. In the 'SSL Certificate Assignment' section, there is a 'Add' section with a dropdown menu '証明書名' (Certificate Name) and an 'Add' button, and a 'Target' section with a list containing 'year2014 (default)' with a red box around it, and a 'Delete' button. Below these sections is a blue button labeled '設定内容を変更する' (Change settings). The 'SSL Acceleration Detailed Settings' section contains a table with columns for '項目名' (Item Name), '入力' (Input), and '削除' (Delete). The table rows include: 'サーバが許可する暗号スイート' (Ciphersuites allowed by server) with checkboxes for EXP-DES-CBC-SHA, DES-CBC-SHA, RC4-MD5, AES128-SHA, and AES256-SHA; 'クライアント証明書ヘッダ' (Client certificate header) with an input field; 'SSLセッションIDヘッダ' (SSL session ID header) with an input field; and 'クライアント認証失敗時処理' (Client authentication failure handling) with options for '動作' (Action) set to 'SSLハンドシェーク強制終了' (Force SSL handshake termination) and 'URL'.

※ 既存の証明書名(year2014)を選択してください。
選択後、「削除」ボタンを押してください。

設定	
ネットワーク	▼
冗長構成	▼
SSL	▼
バランシング	▼
実サーバ	▼
NATプール	▼
仮想サーバ	▼
SSLアクセラレーション	▼
SSLアクセラレーション	▶
ネットワーク	▼
ヘルスチェック	▼
システム	▼
かんたん設定	▼

設定変更後保存されません。保存する場合は右のボタンより、保存してください。

保存する

SSLアクセラレーション設定

SSL証明書の割り当て

追加元

year2015



追加

追加先



デフォルト証明書にセットする

SSLアクセラレーション詳細設定

項目名	入力	削除
サーバが許可する暗号スイート	<input type="checkbox"/> EXP-DES-CBC-SHA <input type="checkbox"/> EXP-RC4-MD5 <input type="checkbox"/> DES-CBC-SHA <input checked="" type="checkbox"/> DES-CBC3-SHA <input checked="" type="checkbox"/> RC4-MD5 <input checked="" type="checkbox"/> RC4-SHA	<input type="checkbox"/>

※ 1)で新規に作成したSSLポリシー名(year2015)を選択してください。

選択後、「追加」ボタンを押してください。

設定	
ネットワーク	▼
冗長構成	▼
SSL	▼
バランシング	▼
実サーバ	▼
NATプール	▼
仮想サーバ	▼
SSLアクセラレーション	▼
SSLアクセラレーション	▶
ネットワーク	▼
ヘルスチェック	▼
システム	▼
かんたん設定	▼

設定変更後保存されません。保存する場合は右のボタンより、保存してください。

保存する

SSLアクセラレーション設定

SSL証明書の割り当て

追加元

証明書名



year2015 (default)

追加先



デフォルト証明書にセットする

SSLアクセラレーション詳細設定

項目名	入力	削除
サーバが許可する暗号スイート	<input type="checkbox"/> EXP-DES-CBC-SHA <input type="checkbox"/> EXP-RC4-MD5 <input type="checkbox"/> DES-CBC-SHA <input checked="" type="checkbox"/> DES-CBC3-SHA <input checked="" type="checkbox"/> RC4-MD5 <input checked="" type="checkbox"/> RC4-SHA <input checked="" type="checkbox"/> 全選択/解除 <input type="checkbox"/> AES128-SHA <input checked="" type="checkbox"/> AES128-SHA256 <input checked="" type="checkbox"/> AES256-SHA <input checked="" type="checkbox"/> AES256-SHA256	<input type="checkbox"/>
クライアント証明書ヘッダ	<input type="text"/>	<input type="checkbox"/>
SSLセッションIDヘッダ	<input type="text"/>	<input type="checkbox"/>
クライアント認証失敗時処理	動作: <input type="button" value="SSLハンドシェーク強制終了"/> URL: <input type="text"/>	<input type="button" value="デフォルトに戻す"/> <input type="checkbox"/>

設定内容を変更する

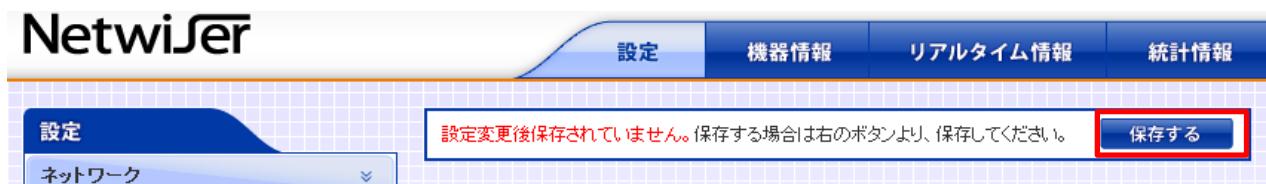
※ 新規に作成した証明書名が追加先に登録されますので確認してください。

確認後、「設定内容を変更する」ボタンをしてください。

6) 設定の保存

「保存する」ボタンを押さなくとも設定は反映されていますが、リブートを行った際に変更した設定がクリアされてしまいます。

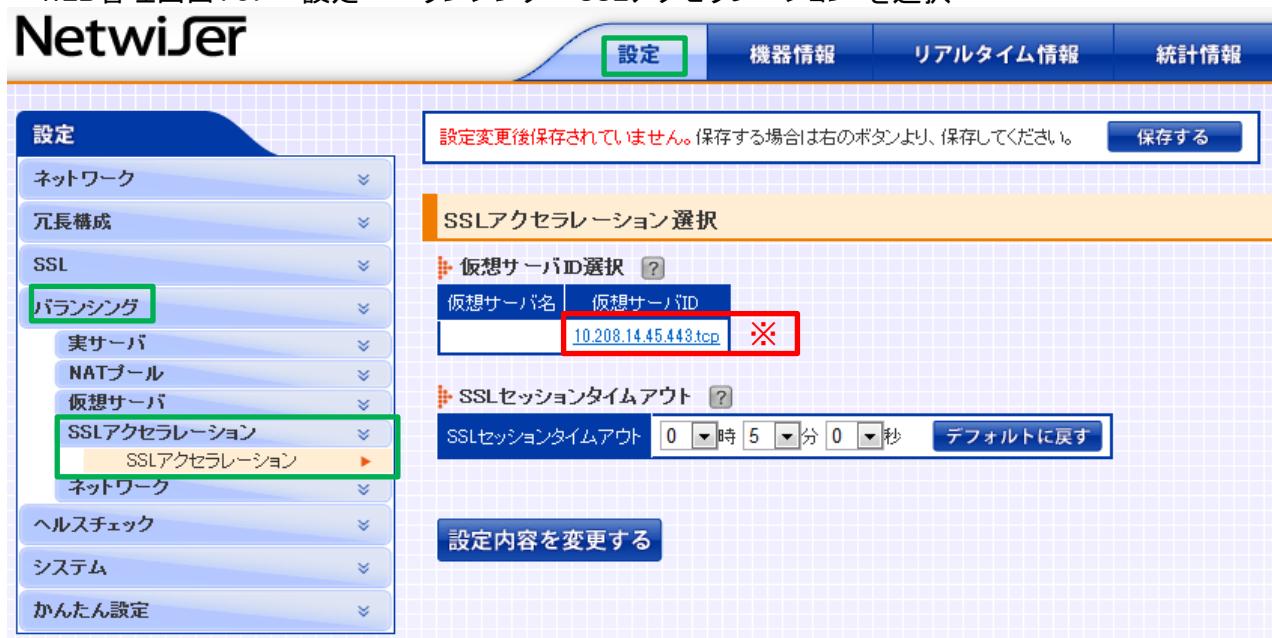
設定の保存を行う場合は「保存する」ボタンを押してください。



新規証明書で不具合が発生した際は、以降の手順で元の証明書に戻すことが出来ます。

7) 既存SSL証明書へ戻す設定方法

"WEB管理画面TOP→設定→バランシング→SSLアクセラレーション"を選択



※ 元の証明書に戻す仮想サーバIDを選択してください。

設定

ネットワーク
冗長構成
SSL
バランシング
実サーバ
NATプール
仮想サーバ
SSLアクセラレーション
SSLアクセラレーション
ネットワーク
ヘルスチェック
システム
かんたん設定

設定変更後保存されません。保存する場合は右のボタンより、保存してください。

保存する

SSLアクセラレーション設定

SSL証明書の割り当て

追加元	証明書名	追加	追加先
	year2015 (default)		※

削除

デフォルト証明書にセットする

SSLアクセラレーション詳細設定

項目名	入力	削除
サーバが許可する暗号スイート ■ 全選択/解除	<input type="checkbox"/> EXP-DES-CBC-SHA <input type="checkbox"/> EXP-RC4-MD5 <input type="checkbox"/> DES-CBC-SHA <input checked="" type="checkbox"/> DES-CBC3-SHA <input checked="" type="checkbox"/> RC4-MD5 <input checked="" type="checkbox"/> RC4-SHA <input checked="" type="checkbox"/> AES128-SHA <input checked="" type="checkbox"/> AES128-SHA256 <input checked="" type="checkbox"/> AES256-SHA <input checked="" type="checkbox"/> AES256-SHA256	<input type="checkbox"/>
クライアント証明書ヘッダ		<input type="checkbox"/>
SSLセッションIDヘッダ		<input type="checkbox"/>
クライアント認証 失敗時処理	動作 SSLハンドシェーク強制終了	デフォルトに戻す
URL		<input type="checkbox"/>

設定内容を変更する

※ 新規証明書名(year2015)を選択してください。
選択後、「削除」ボタンを押してください。

設定

ネットワーク
冗長構成
SSL
バランシング
実サーバ
NATプール
仮想サーバ
SSLアクセラレーション
SSLアクセラレーション
ネットワーク
ヘルスチェック
システム
かんたん設定

設定変更後保存されません。保存する場合は右のボタンより、保存してください。

保存する

SSLアクセラレーション設定

SSL証明書の割り当て

追加元	year2014	×	追加	追加先

削除

デフォルト証明書にセットする

SSLアクセラレーション詳細設定

項目名	入力	削除
サーバが許可する暗号スイート	<input type="checkbox"/> EXP-DES-CBC-SHA <input type="checkbox"/> EXP-RC4-MD5 <input type="checkbox"/> DES-CBC-SHA <input checked="" type="checkbox"/> DES-CBC3-SHA <input checked="" type="checkbox"/> RC4-MD5 <input checked="" type="checkbox"/> RC4-SHA	<input type="checkbox"/>

※ 既存のSSLポリシー名(year2014)を選択してください。
選択後、「追加」ボタンを押してください。

設定変更後保存されていません。保存する場合は右のボタンより、保存してください。

SSLアクセラレーション設定

SSL証明書の割り当て

追加元	追加先
証明書名	year2014 (default) ×

SSLアクセラレーション詳細設定

項目名	入力	削除
サーバが許可する暗号スイート 全選択/解除	<input type="checkbox"/> EXP-DES-CBC-SHA <input type="checkbox"/> DES-CBC-SHA <input checked="" type="checkbox"/> RC4-MD5 <input checked="" type="checkbox"/> AES128-SHA <input checked="" type="checkbox"/> AES256-SHA <input type="checkbox"/> EXP-RC4-MD5 <input checked="" type="checkbox"/> DES-CBC3-SHA <input checked="" type="checkbox"/> RC4-SHA <input checked="" type="checkbox"/> AES128-SHA256 <input checked="" type="checkbox"/> AES256-SHA256	<input type="button" value="削除"/>
クライアント証明書ヘッダ	<input type="text"/>	<input type="button" value="削除"/>
SSLセッションIDヘッダ	<input type="text"/>	<input type="button" value="削除"/>
クライアント認証 失敗時処理	動作: <input type="button" value="SSLハンドシェーク強制終了"/> URL: <input type="text"/>	<input type="button" value="デフォルトに戻す"/> <input type="button" value="削除"/>

設定内容を変更する

※ 既存の証明書名が追加先に登録されますので確認してください。
確認後、「設定内容を変更する」ボタンをしてください。

「保存する」ボタンを押さなくても設定は反映されていますが
リブートを行った際に変更した設定がクリアされてしまいます。

設定の保存を行う場合は「保存する」ボタンを押してください。