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シーリーズ全機種

2024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。

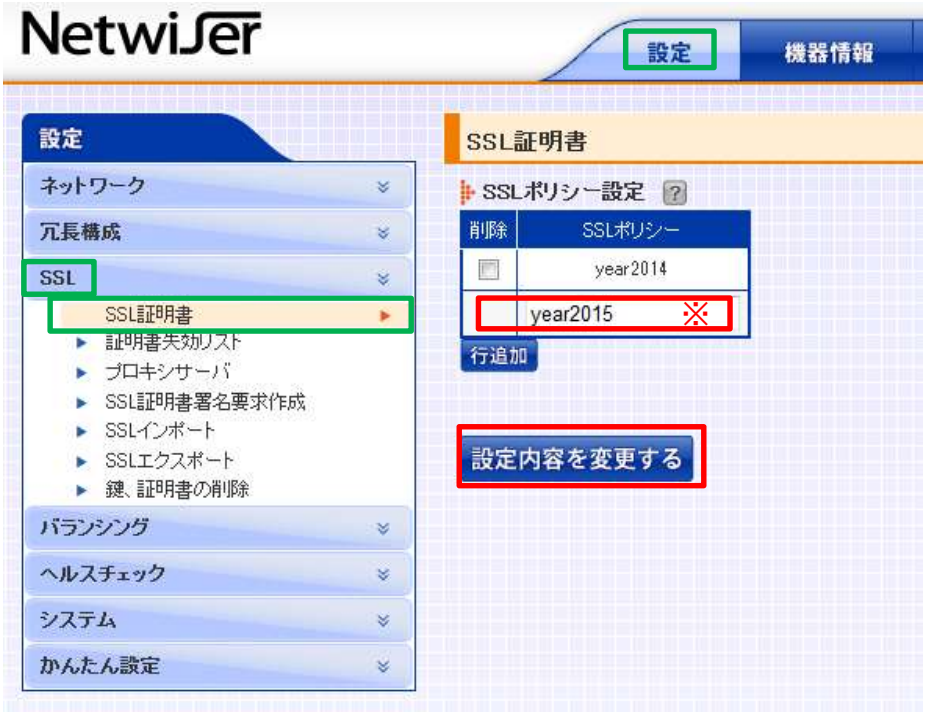
既存のSSLポリシー名に新規証明書をインポートすることも可能ですが既存の証明書は
クリアされてしまいますのでご注意ください。

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で
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

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



※ 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。

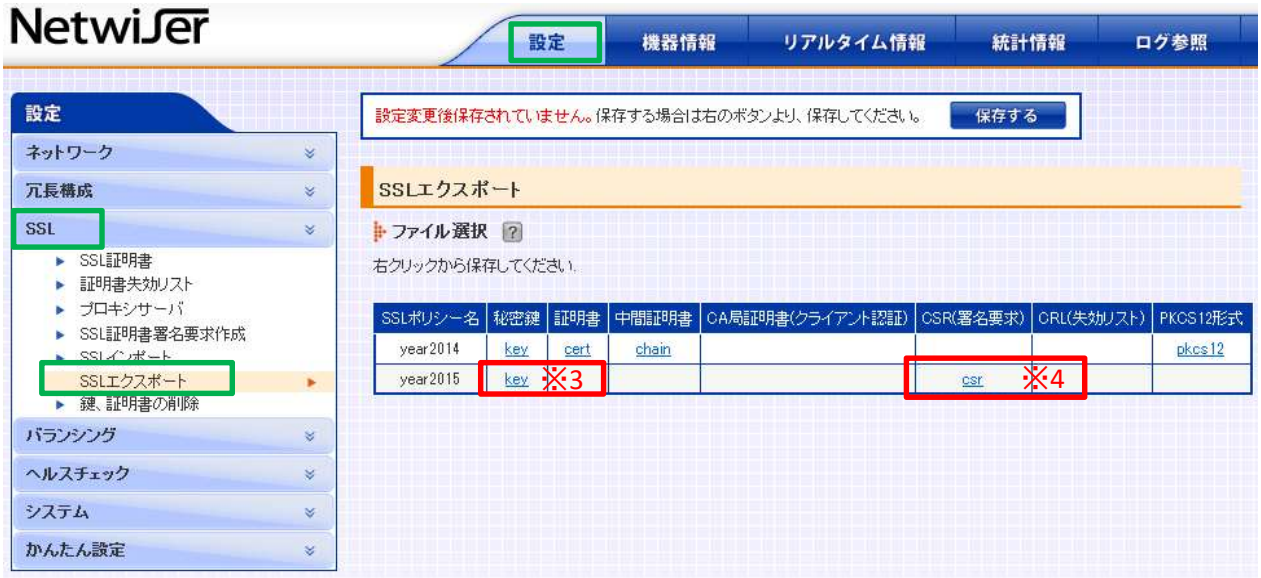
NetwiserでSSL証明書署名要求作成(CSR)を行う必要が無い場合は
2)の操作は不要です。3)SSL証明書及び鍵のインポート操作に進んでください。

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

※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。

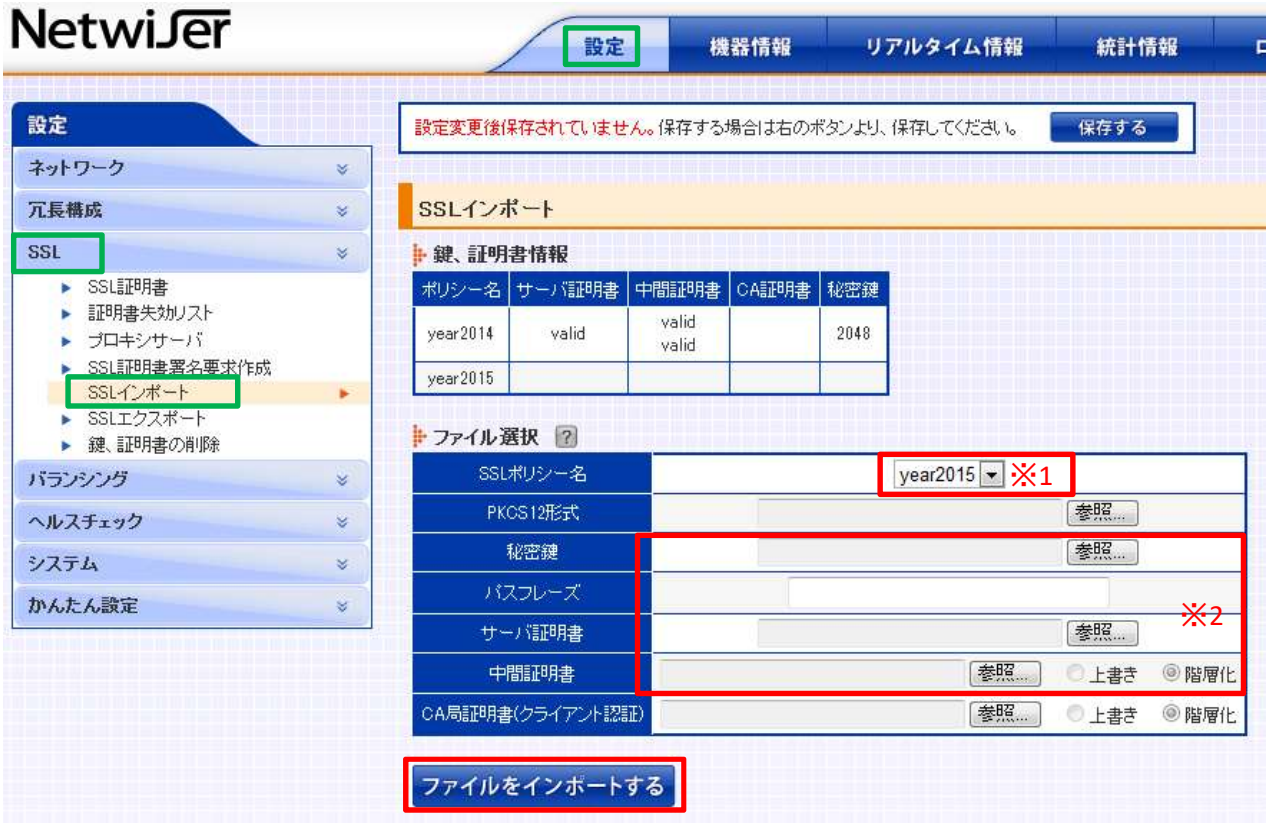
”WEB管理画面TOP→設定→SSL→SSエクスポート”を選択



※3　keyをマウスで右クリックして対象ファイルを保存してください。
　　keyを削除してしまうと再度CSRを行う必要があります。
　　不測の事態が発生した際に戻せるよう、keyファイルを保管しておいてください。
※4　CSRをマウスで右クリックして対象ファイルを保存してください。
　　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



※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。

・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。

・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。
秘密鍵にパスフレーズが設定されている場合は、パスフレーズを入力してください。

・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。

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、
「PKCS12形式」でファイルを選択してください。
鍵、証明書欄を選択する必要はありません。

クライアント認証を行う際は「CA局証明書」にてクライアント証明書を選択してください。

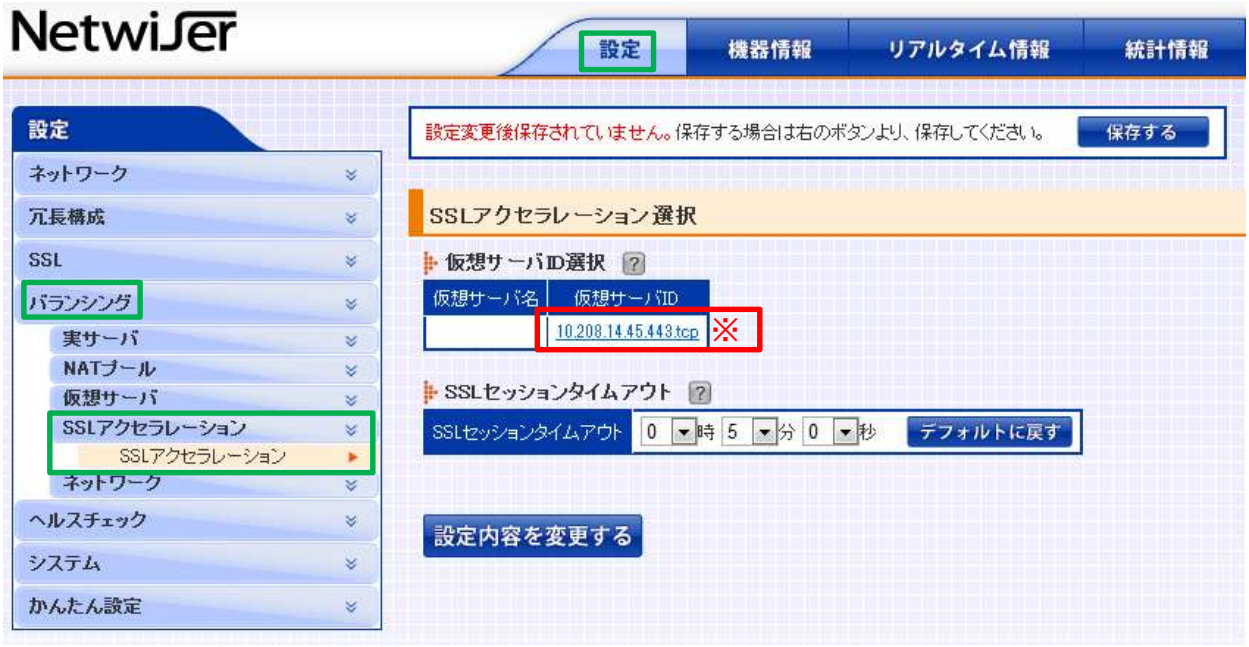
4）証明書ファイルインポート結果の確認

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。

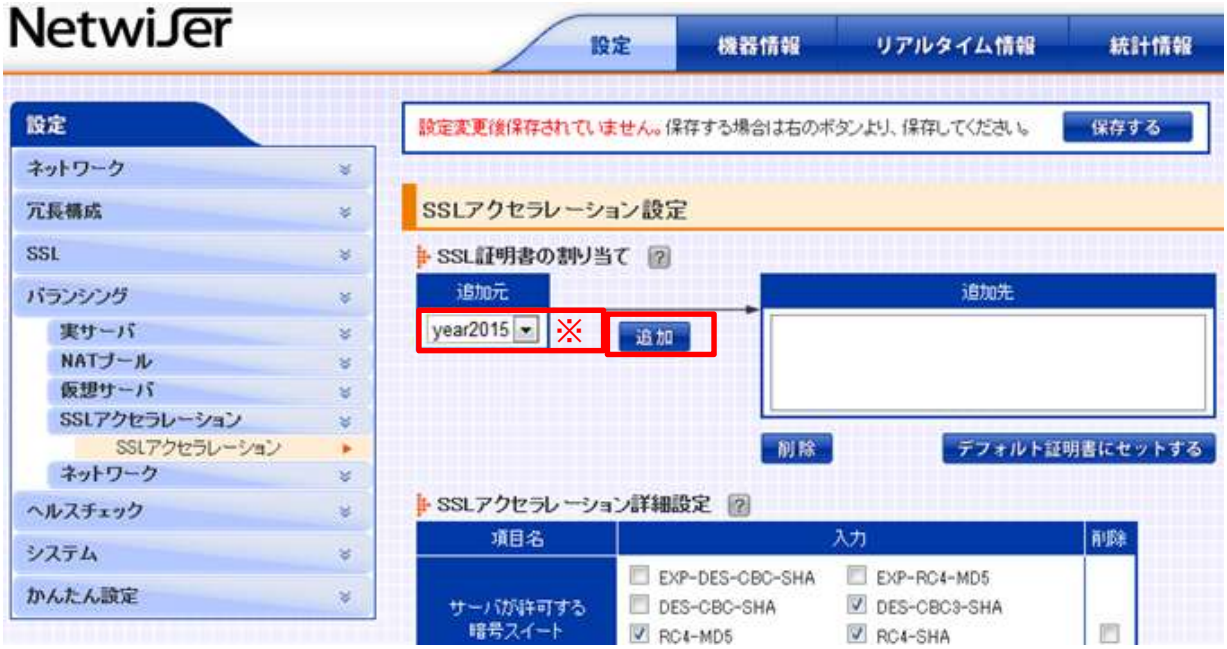
5）新たに作成したSSLポリシー名を仮想サーバに割り当てます。

”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



※　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。

※　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。



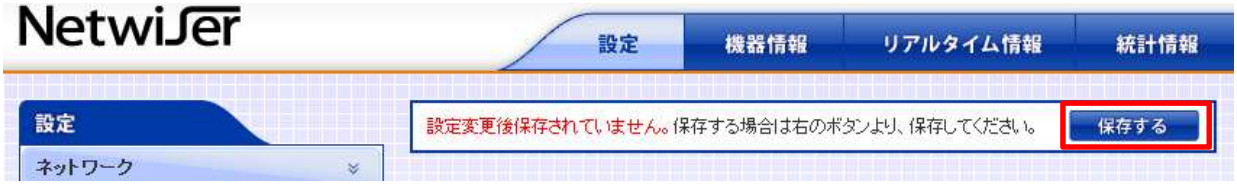
※　1）で新規に作成したSSLポリシー名（year2015）を選択してください。
　　選択後、「追加」ボタンを押してください。

※　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。

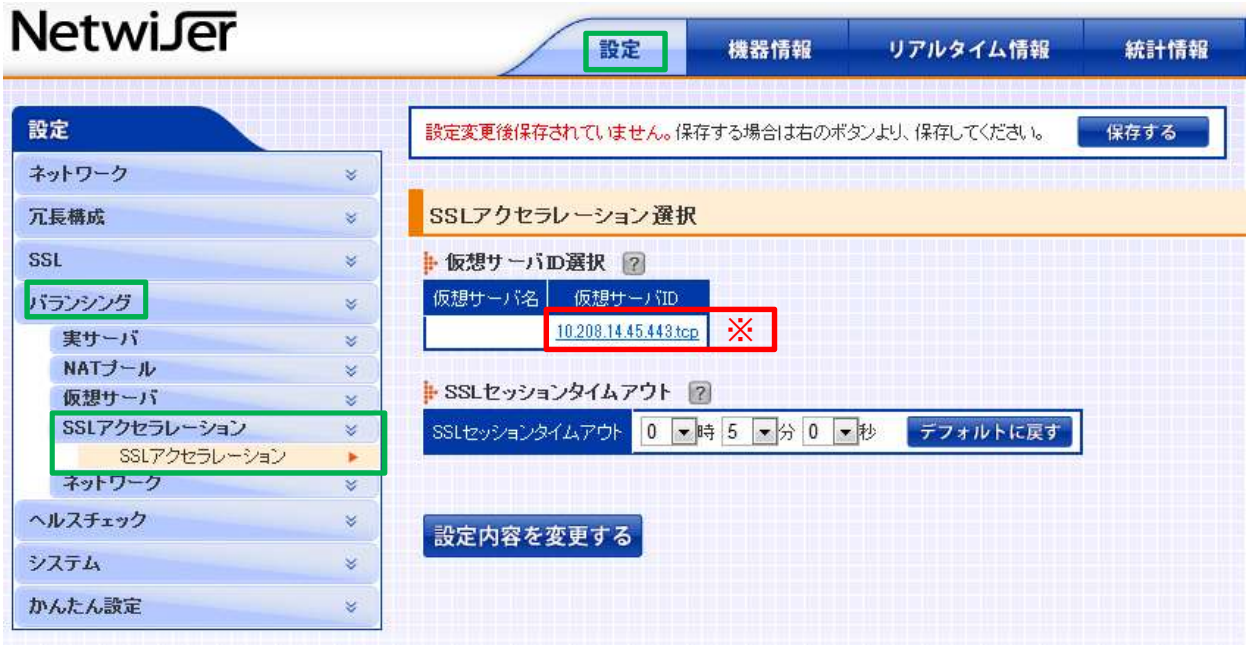
設定の保存を行う場合は「保存する」ボタンを押してください。



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。

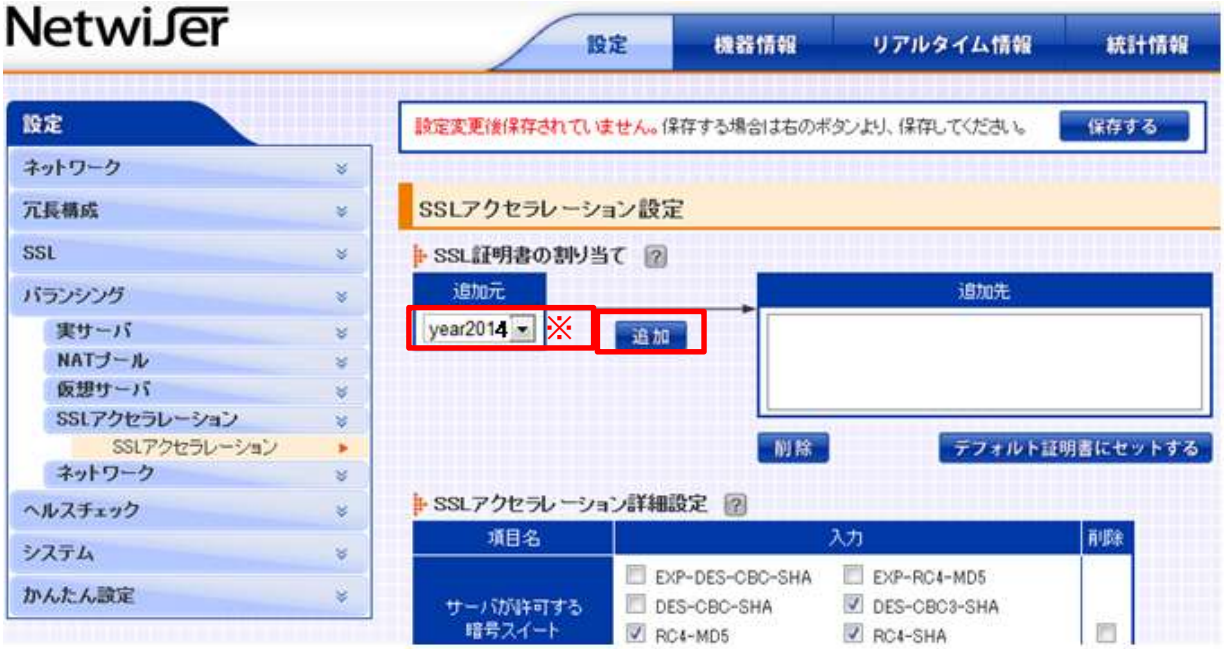
7）既存SSL証明書へ戻す設定方法

”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。

※　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。



※　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。

※　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。