

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

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書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

Netwiser

設定 機器情報

ホスト名: netwiser
ユーザ名: adm
権限: Admin権限

設定

- ネットワーク
- 冗長構成
 - VRRP
 - 情報同期実行
 - 強制/バックアップ
 - 同期設定
- SSL
- バランシング
- ヘルスチェック
- システム

同期設定

コマンド同期設定 ?

項目名	入力
コマンド同期	<input checked="" type="checkbox"/> 有効にする

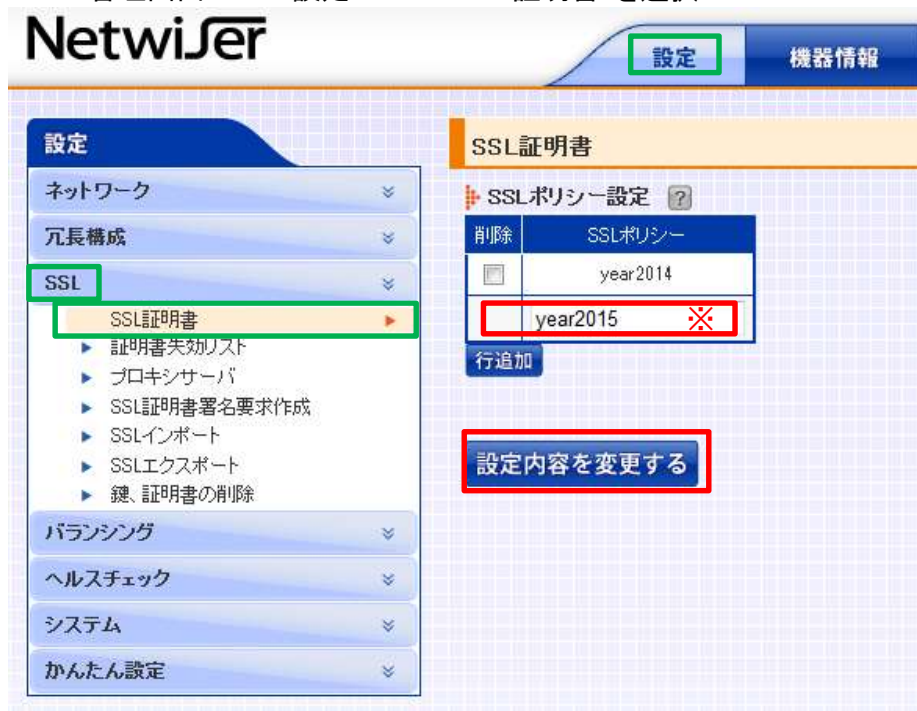
セッション同期設定 ?

項目名	入力
セッション同期	<input checked="" type="checkbox"/> 有効にする
起動時のセッション同期	<input checked="" type="checkbox"/> 有効にする

設定内容を変更する

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

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証明書署名要求作成

CSR (署名要求) 設定

SSLポリシー名	year2015
ECC証明書	<input checked="" type="checkbox"/> 有効 ※1
公開鍵長	2048
楕円曲線パラメータ	未選択
サーバのFQDN	
国名 (Country)	
都道府県 (State)	
区市町村 (Locality)	※2
組織名 (Organization)	
部門名 (Organization Unit)	
メールアドレス (Email Address)	

設定内容を変更する

- ※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

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エクスポート

ファイル選択

右クリックから保存してください。

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)	PKCS12形式
year2014	key	cert	chain				pkcs12
year2015	key ※3				csr ※4		

- ※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

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。

保存する

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				

ファイル選択 ?

SSLポリシー名	year2015 ※1
PKCS12形式	<input type="text"/> 参照...
秘密鍵	<input type="text"/> 参照...
パスフレーズ	<input type="text"/>
サーバ証明書	<input type="text"/> 参照... ※2
中間証明書	<input type="text"/> 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)	<input type="text"/> 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

※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。

Netwiser

設定 機器情報 リアルタイム情報 統計情報

設定

ネットワーク

冗長構成

SSL

- 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
- SSLEXポート
- 鍵、証明書の削除

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

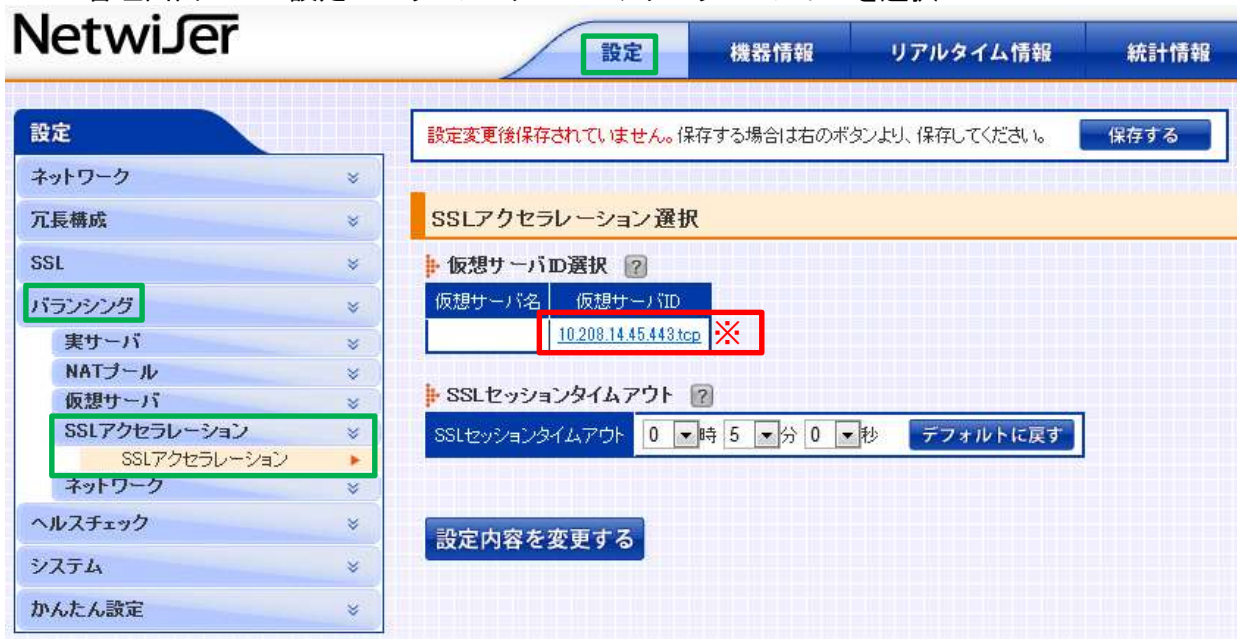
ファイル選択 ?

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 left sidebar has a menu with '設定' (Settings) at the top, followed by 'ネットワーク' (Network), '冗長構成' (Redundancy Configuration), 'SSL', 'バランシング' (Load Balancing), 'ヘルスチェック' (Health Check), 'システム' (System), and 'かんたん設定' (Easy Settings). The 'バランシング' menu is expanded, showing '実サーバ' (Real Server), 'NATプール' (NAT Pool), '仮想サーバ' (Virtual Server), 'SSLアクセラレーション' (SSL Acceleration), and 'ネットワーク' (Network). The 'SSLアクセラレーション' option is selected and highlighted in orange. The main content area is titled 'SSLアクセラレーション選択' (SSL Acceleration Selection). It contains a section for '仮想サーバID選択' (Virtual Server ID Selection) with a table for selecting a virtual server name and ID. The '仮想サーバID' field is set to '10.208.14.45.443.tcp' and is highlighted with a red box and a red 'X' icon. Below this is a section for 'SSLセッションタイムアウト' (SSL Session Timeout) with a dropdown menu set to '0' minutes and '0' seconds. A '保存する' (Save) button is at the top right. A '設定内容を変更する' (Change Settings) button is at the bottom.

※ 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 left sidebar is the same as in the previous screenshot. The main content area is titled 'SSLアクセラレーション設定' (SSL Acceleration Settings). It contains a section for 'SSL証明書の割り当て' (SSL Certificate Assignment) with a table for selecting a certificate name and adding it. The '証明書名' (Certificate Name) field is set to 'year2014 (default)' and is highlighted with a red box and a red 'X' icon. Below this is a section for 'SSLアクセラレーション詳細設定' (SSL Acceleration Detailed Settings) with a table for selecting SSL acceleration options. The table has columns for '項目名' (Item Name), '入力' (Input), and '削除' (Delete). The 'サーバが許可する暗号スイート' (Server Allowed Cipher Suites) section has a '全選択/解除' (Select All/Unselect) button. The 'クライアント証明書ヘッダ' (Client Certificate Header) and 'SSLセッションIDヘッダ' (SSL Session ID Header) sections have input fields. The 'クライアント認証失敗時処理' (Client Authentication Failure Handling) section has a dropdown menu set to 'SSLハンドシェイク強制終了' (Force SSL Handshake Termination) and a 'デフォルトに戻す' (Reset to Default) button. A '保存する' (Save) button is at the top right. A '設定内容を変更する' (Change Settings) button is at the bottom.

※ 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。

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

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	

- ※ 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。

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

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"/> 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	
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ハンドシェイク強制終了	<input type="checkbox"/>
	URL		

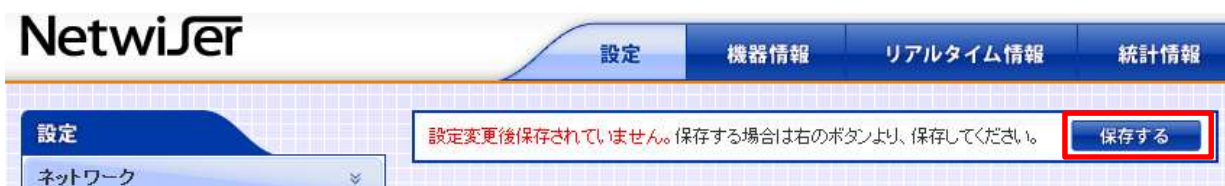
設定内容を変更する

- ※ 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。

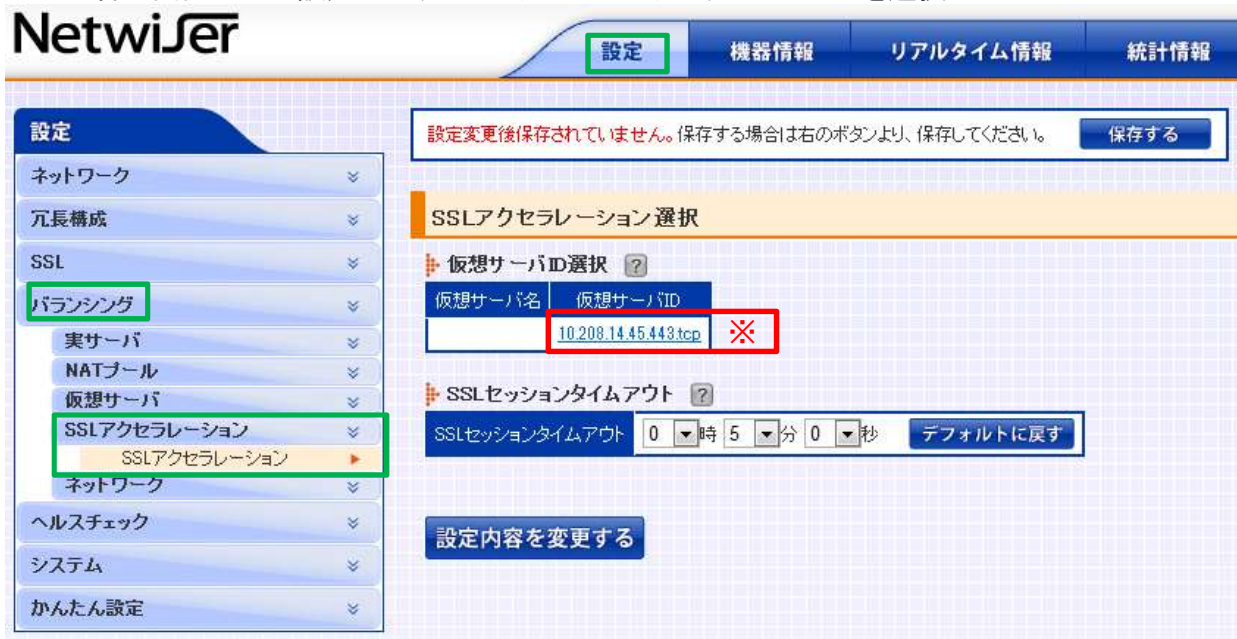
設定の保存を行う場合は「保存する」ボタンを押してください。



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できます。

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
機器情報
リアルタイム情報
統計情報

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
- 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。 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 <input type="checkbox"/> 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
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ハンドシェイク強制終了	<input type="checkbox"/>
	URL	

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
機器情報
リアルタイム情報
統計情報

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
- 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。 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

※ 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
機器情報
リアルタイム情報
統計情報

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
- 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。
 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

追加先

year2014 (default)

追加
削除

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"/>
	<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"/> 全選択/解除		
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	<input type="text" value="SSLハンドシェイク強制終了"/> デフォルトに戻す	<input type="checkbox"/>
	URL	<input type="text"/>	

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。