Express5800/MW シリーズ

Web サービスにおける

SSL サーバ証明書発行機関から取得した証明書の更新方法

および

中間 CA 証明書の設定･更新方法

2009/03/17 第 2 版

更新履歴

版数	作成日	内容
1	**2004/09/24**	初版
2	**2009/03/17**	・設定ファイルの退避手順を追記 ・**SSL** の使用の有効化・無効化の手順を追記 ・**SSL** 関連のログ設定内容の確認・復元の手順を追記 ・中間 **CA** 証明書の設定・更新方法を追記

1．SSL サーバ証明書発行機関から取得した証明書の更新方法

SSL サーバ証明書の第三者発行機関から取得した証明書を更新する場合には、以下の手順により行ってください。

鍵ペアと CSR を再作成します。
既存の証明書と鍵ペアをバックアップしておき、再作成後リストアします。
なお、鍵ペア と CSR のバックアップ/リストア作業は、MW サーバにログイン後、root アカウントにて行ってください。フェイルオーバクラスタ構成の場合、稼働系にて行ってください。

(1) Web サービスの停止

Management Console(システム管理者)のサービス画面より、Web サーバ(httpd) を、[停止]します。

(2) 更新前の設定ファイルの退避

不測の事態に備え、更新前の設定ファイルを別サーバへ退避しておいてください。
もし、更新作業中に問題発生し、更新前の状態に復元したい場合は、退避した設定ファイルをリストアしてください。

(2)-1. 設定ファイルの退避手順

```
# mkdir -p /tmp/ssl
# cd /etc/httpd/conf
# tar czf /tmp/ssl/httpdconf.tgz *
# cd /etc/logrotate.d
# tar czf /tmp/ssl/ssllogconf.tgz apache
```

上記手順にて作成した httpdconf.tgz、および、ssllogconf.tgz を ftp コマンド等を利用し、別サーバへ転送し、別サーバにてファイルを保存しておいてください。
なお、Management Console(システム管理者)にて、ディレクトリ指定で、samba サーバやテープ装置にファイルをバックアップすることも可能です。

(2)-2. 設定ファイルのリストア手順

何らかの問題が発生し、更新前の状態に復元したい場合は、以下の手順にて設定ファイルのリストアを行ってください。なお、以下の手順では、/tmp/ssl 配下に、httpdconf.tgz、および、ssllogconf.tgz が格納されていることを前提としています。

```
# cd /etc/httpd/conf
# tar xzf /tmp/ssl/httpdconf.tgz
# cd /etc/logrotate.d
# tar xzf /tmp/ssl/ssllogconf.tgz
```

(3) 証明書と鍵ペアのバックアップ

以下のファイルを、適当なディレクトリにコピーします。

・/etc/httpd/conf/ssl.crt/crt_ドメイン名-ssl.pem (証明書)
・/etc/httpd/conf/ssl.key/key_ドメイン名-ssl.pem (鍵ペア)

(例)ドメイン名が、hoge.co.jp の場合

```
# mkdir -p /tmp/ssl/hoge.co.jp
# mkdir -p /tmp/ssl/hoge.co.jp/old
# cp -p /etc/httpd/conf/ssl.crt/crt_hoge.co.jp-ssl.pem /tmp/ssl/hoge.co.jp/old
# cp -p /etc/httpd/conf/ssl.key/key_hoge.co.jp-ssl.pem /tmp/ssl/hoge.co.jp/old
```

(4) SSL 関連のログ設定内容確認

ログのローテート間隔や世代の設定をデフォルト設定から変更している場合は、Management Console(システム管理者)にて、設定内容をメモ用紙等に控えておいてください。
SSL の使用を無効化した際、設定内容は削除されますので、必ずログの設定内容を確認するようにしてください。

Management Console(システム管理者)
「システム > ログ管理」画面

Web サーバ(httpd)のエラーログ（ドメイン名-ssl）
Web サーバ(httpd)のアクセスログ（ドメイン名-ssl）

上記該当ファイルの「設定」をクリック後に表示される画面にて、設定内容を確認してください。

(5) SSL の使用の無効化

Management Console(システム管理者)にて、SSL の使用を無効にしてください。

Management Console(システム管理者)
「ドメイン情報」画面

(5)-1. SSL の使用を無効化するドメインの「編集」をクリック。
(5)-2.「□SSL を使用する」のチェックをはずす。
(5)-3.「設定」をクリック。

(6) 鍵ペアと CSR の再作成

Management Console(システム管理者)にて、鍵ペアと CSR の再作成を行ってください。

Management Console(システム管理者)
「ドメイン情報」画面

(6)-1. 再作成するドメインの「編集」をクリック。
(6)-2.「■ SSL」の「SSL 設定」をクリック。
(6)-3.「秘密鍵と証明書署名要求を作る」を選択し、「設定」をクリック。
(6)-4.「■ 証明書署名要求作成」画面にて、お客様環境に応じた適切な値を入力し、「設定」をクリック。
(6)-5.「■ 証明書署名要求表示」画面にて、「戻る」をクリック。

(7) 再作成した、鍵ペアと CSR のバックアップ

以下のファイルを、適当なディレクトリにコピーします。なお、(3)でコピーしたディレクトリとは違うディレクトリにコピーしてください。

・/etc/httpd/conf/ssl.csr/csr_ドメイン名-ssl.pem (CSR)
・/etc/httpd/conf/ssl.key/key_ドメイン名-ssl.pem (鍵ペア)

(例)ドメイン名が、hoge.co.jp の場合

```
# mkdir -p /tmp/ssl/hoge.co.jp/new
# cp -p /etc/httpd/conf/ssl.csr/csr_hoge.co.jp-ssl.pem /tmp/ssl/hoge.co.jp/new
# cp -p /etc/httpd/conf/ssl.key/key_hoge.co.jp-ssl.pem /tmp/ssl/hoge.co.jp/new
```

(8) (3)、(7)でバックアップしたファイルの退避

不測の事態に備え、(3)、(7)でバックアップしたファイルを別サーバへ退避しておいてください。
もし、何らかの問題が発生し、(3)、(7)でバックアップしたファイルを復元したい場合は、
退避したファイルをリストアしてください。

(8)-1. 退避手順

```
# cd /tmp
# tar czf sslfileback.tgz ssl
```

上記手順にて作成した sslfileback.tgz を ftp コマンド等を利用し、別サーバへ転送し、
別サーバにてファイルを保存しておいてください。
なお、Management Console(システム管理者)にて、ディレクトリ指定で、samba サーバや
テープ装置にファイルをバックアップすることも可能です。

(8)-2. リストア手順
何らかの問題が発生し、(3)、(7)でバックアップしたファイルを復元したい場合は、以下
の手順にてリストアを行ってください。なお、以下の手順では、/tmp 配下に、sslfileback.tgz
が格納されていることを前提としています。

```
# cd /tmp
# tar xzf sslfileback.tgz
```

sslfileback.tgz を解凍することにより、/tmp/ssl 配下 に、(3)、(7)でバックアップした
ファイルが復元されます。

(9) (3) でバックアップした証明書と鍵ペアのリストア

バックアップしたファイルを以下のファイルにコピーしてください。

・/etc/httpd/conf/ssl.crt/crt_ドメイン名-ssl.pem (証明書)
・/etc/httpd/conf/ssl.key/key_ドメイン名-ssl.pem (鍵ペア)

(例)ドメイン名が、hoge.co.jp の場合

```
# cd /tmp/ssl/hoge.co.jp/old
# cp -p crt_hoge.co.jp-ssl.pem /etc/httpd/conf/ssl.crt/crt_hoge.co.jp-ssl.pem
# cp -p key_hoge.co.jp-ssl.pem /etc/httpd/conf/ssl.key/key_hoge.co.jp-ssl.pem
```

(10) SSL の使用の有効化

Management Console(システム管理者)にて、SSL の使用を有効にしてください。

Management Console(システム管理者)
「ドメイン情報」画面

(10)-1. SSL の使用を有効化するドメインの「編集」をクリック。
(10)-2.「□SSL を使用する」にチェックを入れる。
(10)-3.「設定」をクリック。

(11) SSL 関連のログ設定内容復元

(4) でメモ用紙等に控えたログの設定内容を復元します。
Management Console(システム管理者)にて、設定内容の復元を行ってください。

Management Console(システム管理者)
「システム > ログ管理」画面

Web サーバ(httpd)のエラーログ（ドメイン名-ssl）
Web サーバ(httpd)のアクセスログ（ドメイン名-ssl）

上記該当ファイルの「設定」をクリック後に表示される画面にて、再設定してください。
なお、画面表示されている設定内容とメモ用紙等に控えた設定内容が同じ場合、再設定する必要はありません。

(12) 中間 CA 証明書を使用する必要がある場合は、別途、「**２．中間 CA 証明書の設定・更新方法**」を参照し、中間 CA 証明書の設定を行ってください。

(13) Web サービスの起動

Management Console(システム管理者)のサービス画面より、Web サーバ(httpd) を、[起動]します。

以上で、鍵ペアと CSR の再作成は終了です。
(7) でバックアップしたファイルで、証明書の発行を依頼してください。

以下、新しいサーバ証明書の登録方法となります。
新しいサーバ証明書が発行されましたら作業してください。

(14) Web サービスの停止

Management Console(システム管理者)のサービス画面より、Web サーバ(httpd) を、[停止]します。

(15) 登録前の設定ファイルの退避

不測の事態に備え、登録前の設定ファイルを別サーバへ退避しておいてください。
もし、登録作業中に問題発生し、登録前の状態に復元したい場合は、退避した設定ファイルをリストアしてください。

(15)-1. 設定ファイルの退避手順

```
# cd /etc/httpd/conf
# tar czf /tmp/httpdconf-15.tgz *
# cd /etc/logrotate.d
# tar czf /tmp/ssllogconf-15.tgz apache
```

上記手順にて作成した **httpdconf-15.tgz**、および、**ssllogconf-15.tgz** を **ftp** コマンド等を利用し、別サーバへ転送し、別サーバにてファイルを保存しておいてください。
なお、**Management Console(**システム管理者**)**にて、ディレクトリ指定で、**samba** サーバやテープ装置にファイルをバックアップすることも可能です。

(15)-2. 設定ファイルのリストア手順
何らかの問題が発生し、登録前の状態に復元したい場合は、以下の手順にて設定ファイルのリストアを行ってください。なお、以下の手順では、**/tmp** 配下に、**httpdconf-15.tgz**、および、**ssllogconf-15.tgz** が格納されていることを前提としています。

```
# cd /etc/httpd/conf
# tar xzf /tmp/httpdconf-15.tgz
# cd /etc/logrotate.d
# tar xzf /tmp/ssllogconf-15.tgz
```

(16) SSL 関連のログ設定内容確認

ログのローテート間隔や世代の設定をデフォルト設定から変更している場合は、**Management Console(**システム管理者**)**にて、設定内容をメモ用紙等に控えておいてください。
SSL の使用を無効化した際、設定内容は削除されますので、必ずログの設定内容を確認するようにしてください。

Management Console(システム管理者**)**
「システム **>** ログ管理」画面

Web サーバ**(httpd)**のエラーログ（ドメイン名**-ssl**）
Web サーバ**(httpd)**のアクセスログ（ドメイン名**-ssl**）

上記該当ファイルの「設定」をクリック後に表示される画面にて、設定内容を確認してください。

(17) SSL の使用の無効化

Management Console(システム管理者**)**にて、**SSL** の使用を無効にしてください。

Management Console(システム管理者**)**
「ドメイン情報」画面

(17)-1. SSL の使用を無効化するドメインの「編集」をクリック。
(17)-2.「□**SSL** を使用する」のチェックをはずす。
(17)-3.「設定」をクリック。

(18) (7) でバックアップした鍵ペアと **CSR** のリストア

バックアップしたファイルを以下のファイルにコピーしてください。

・/etc/httpd/conf/ssl.csr/csr_ドメイン名-ssl.pem (CSR)
・/etc/httpd/conf/ssl.key/key_ドメイン名-ssl.pem (鍵ペア)

(例)ドメイン名が、hoge.co.jp の場合

```
# cd /tmp/ssl/hoge.co.jp/new
# cp -p csr_hoge.co.jp-ssl.pem /etc/httpd/conf/ssl.csr/csr_hoge.co.jp-ssl.pem
# cp -p key_hoge.co.jp-ssl.pem /etc/httpd/conf/ssl.key/key_hoge.co.jp-ssl.pem
```

(19) 新しいサーバ証明書の登録

Management Console(システム管理者)にて、新しいサーバ証明書の登録を行ってください。

Management Console(システム管理者)
「ドメイン情報」画面

(19)-1. 登録するドメインの「編集」をクリック。
(19)-2.「■ SSL」の「SSL 設定」をクリック。
(19)-3.「署名済みの証明書を登録する」を選択し、「設定」をクリック。
(19)-4.「■ 証明書登録」画面にて、取得したサーバ証明書の内容を入力し、「設定」をクリック。

(20) SSL の使用の有効化

Management Console(システム管理者)にて、SSL の使用を有効にしてください。

Management Console(システム管理者)
「ドメイン情報」画面

(20)-1. SSL の使用を有効化するドメインの「編集」をクリック。
(20)-2.「□SSL を使用する」にチェックを入れる。
(20)-3.「設定」をクリック。

(21) SSL 関連のログ設定内容復元

(16) でメモ用紙等に控えたログの設定内容を復元します。
Management Console(システム管理者)にて、設定内容の復元を行ってください。

Management Console(システム管理者)
「システム > ログ管理」画面

Web サーバ(httpd)のエラーログ（ドメイン名-ssl）
Web サーバ(httpd)のアクセスログ（ドメイン名-ssl）

上記該当ファイルの「設定」をクリック後に表示される画面にて、再設定してください。
なお、画面表示されている設定内容とメモ用紙等に控えた設定内容が同じ場合、再設定する必要はありません。

(22) 中間 CA 証明書を使用する必要がある場合は、別途、「２．中間 CA 証明書の設定・更新方法」を参照し、中間 CA 証明書の設定を行ってください。

(23) Web サービスの起動

Management Console(システム管理者**)**のサービス画面より、**Web** サーバ**(httpd)** を、**[**起動**]** します。

以上で、新しいサーバ証明書の登録は終了です。

新しい証明書で、**SSL** 接続できることをご確認ください。
なお、新しい証明書で、**SSL** 接続ができるまで、バックアップした全てのファイルは、必ず保存しておいてください。

２．中間 CA 証明書の設定・更新方法

SSL サーバ証明書の発行元から取得した中間 CA 証明書を MW サーバで使用、もしくは、更新する場合には、以下の手順により行ってください。

２．１． 新規に中間 CA 証明書を利用する、もしくは、サーバ証明書を更新する場合

Management Console では、Web サーバの中間 CA 証明書のインストール機能を提供しておりません。
Web サーバとしては、中間 CA 証明書を利用すること(の設定)は可能です。恐れ入りますが、
Web サーバの設定ファイル(/etc/httpd/conf/wbmc.conf)の直接編集をお願いします。
作業は、MW サーバにログイン後、root アカウントにて行ってください。

なお、サーバ証明書の更新を行う場合、更新作業の過程(SSL の使用の無効化作業時)において、一旦、SSL に関する設定が、wbmc.conf より削除されます。そのため、サーバ証明書の更新を行った後に、再度、中間 CA 証明書の設定を行う必要があります。

また、不測の事態に備え、あらかじめ wbmc.conf のバックアップを行った上で作業を行ってください。

```
# cp -p /etc/httpd/conf/wbmc.conf /etc/httpd/conf/wbmc.conf.bak
```

(1) Web サービスの停止

Management Console(システム管理者)のサービス画面より、Web サーバ(httpd) を、[停止]します。

(2) 中間 CA 証明書の MW サーバへの格納

サーバ証明書の発行元より入手した中間 CA 証明書を、以下のディレクトリ配下に格納してください。格納するファイル名につきましては、任意ですが、サーバ証明書ファイルと重複しないようにご注意ください。

格納先ディレクトリ名： /etc/httpd/conf/ssl.crt

(3) 設定ファイル(/etc/httpd/conf/wbmc.conf)の編集

/etc/httpd/conf/wbmc.conf ファイルを以下のように編集します。

[ファイル名]としている所は、(2)で指定したファイル名を記述してください。

該当する<VirtualHost [該当ドメインの IP]:443>内に追記します。(*1)

SSLCertificateChainFile /etc/httpd/conf/ssl.crt/[ファイル名]

(*1)"[該当ドメインの IP]:443"と記述していますが、これは、SSL 使用時のアクセスポート番号として、443 を使用していることを前提としています。
お客様環境にて、別のポート番号を使用されている場合は、443 をお客様環境で使用されている番号に読み替えてください。

例)

```
---------
SSLCertificateChainFile /etc/httpd/conf/ssl.crt/ca_ドメイン名-ssl.pem ← 追加
SSLCertificateFile /etc/httpd/conf/ssl.crt/crt_ドメイン名-ssl.pem
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/key_ドメイン名-ssl.pem
---------
```

上記の例ですと、ファイル名は、**"ca_ドメイン名-ssl.pem"** となります。

(4) Web サービスの起動

Management Console(システム管理者**)**のサービス画面より、**Web** サーバ**(httpd)** を、**[**起動**]** します。

２．２． 中間 CA 証明書のみを更新する場合

現在、サーバ証明書、および、中間 **CA** 証明書を使用中で、中間 **CA** 証明書のみを更新する場合、以下の手順にて中間 **CA** 証明書の更新を行ってください。

(1) Web サービスの停止

Management Console(システム管理者**)**のサービス画面より、**Web** サーバ**(httpd)** を、**[**停止**]** します。

(2) サーバ証明書の発行元より、最新の中間 **CA** 証明書を入手します。

(3) 現在使用している中間 **CA** 証明書を最新の中間 **CA** 証明書と置き換えます。

(4) Web サービスの起動

Management Console(システム管理者**)**のサービス画面より、**Web** サーバ**(httpd)** を、**[**起動**]** します。