Coyote Point Systems

Equalizer E350si/E450si

XCEL カードインストール・CSR 作成・サーバ証明書インストール手順書

2009/11/24 版 (Ver. 2.1)

[Equalizer E350si/E450si v7.2.3c 対応 総合版]

Networld

本書の内容は予告なく変更することがあります。

本書の内容について、(株)ネットワールドは如何なる責任を負うものではありません。

本書の内容の無断転写はできません。

バージョンによって画面イメージが異なる場合があります。 ご了承下さい。

Equalizer™ は米 Coyote Point Systems 社の登録商標です。

目次

はじめに

本手順書は大きく分けて 3 つのセクションに分かれています。 何れも HTTPS クラスタ使用に伴って手順が必要になるものです。 XCEL カードのインストール、CSR 作成手順、及び HTTPS クラスタへの証明書インストールの 3 つの手順書になります。

各バージョンの違いによりウェブ管理インターフェースのデザインが若干異なる場合が御座いますが、基本的手順に大きな差異は御座いません。

(XCEL インストール手順)

Equalizer XCEL をインストールするには、E350si/450si のバージョン確認を行い、そのバージョンに合った XCEL アップグレードファイルを適用して下さい。 現在のバージョン確認方法はシリアル接続にて root でログインして、cat /.version/eq にてご確認頂くか、ウェブ管理インターフェースにログインして頂き、画面左の Equalizer をクリックして頂くと画面中央に表示されます。

この作業を行うには事前に登録とアップグレードファイルのダウンロードが必要になりますので、Tec-world (https://hds.networld.co.jp/helpdesk/support/login.jsp) へご投稿が必要になります。詳細は XCEL インストール手順をご参照下さい。

(CSR 作成手順)

この資料は、Equalizer E350si/450si v7.2.x 上で CSR を作成する手順について記述しています。作成する CSR は RSA 3DES 1024bit で暗号化することを前提としています。 CSR を提出する CA によってこの暗号化をサポートしていない場合は、暗号化の鍵長や暗号化アルゴリズムを変更する必要があります。 Equalizer 上で Openssl のオンラインマニュアル等を参照し、手順内容を変更して下さい。 XCEL-I カードをご利用のお客様につきましては 1024 bits での鍵長で作成を行って下さい。

(サーバ証明書インストール手順)

本手順書は CA へサーバ証明書発行依頼後のサーバ証明書を Equalizer へアップロードする手順について説明しています。 サーバ証明書を CA へ発行申請する場合の手順書につきましては「CSR 作成手順書」をご確認頂き、サーバ証明発行依頼を行って下さい。

Equalizer で使用される HTTPS クラスタを有効にする場合にそのクラスタへサーバ証明書をアップロードする必要があります。 その際にアップロードするファイルを Equalizer では「Composite ファイル」と呼んでいます。

Composite ファイルとは CA より発行されたサーバ証明書と CSR 作成時に作成した秘密鍵とを張り合わせたファイルになります。 上記に加え、中間証明書のインストールが必要な場合には、サーバ証明書、秘密鍵、中間証明書を順に張り合わせた 1 つのファイルになります。 中間証明書を含む証明書を HTTPS クラスタへアップロードが必要な場合はこの 3 つを張り合わせたファイルを「Composite ファイル」と呼びます。

Equalizer XCEL インストール手順

1. ハードウェアのインストール

****

作業の前に

■ Equalizer の電源プラグを必ず抜いて下さい。

■ 金属に触れるなどして、体内の静電気を放電して下さい。

■ 濡れた手では絶対に作業を行わないで下さい。

■ XCEL の基盤部分、スロット差込口の金属部分には触れないで下さい。

■ アップグレードファイルをダウンロードするには事前に登録が必要になります。 Tec-world に Equalizer のシリアル番号、ifconfig のアウトプット、XCEL カードのシリアル番号を「XCEL カードライセンス発行申請」の件名でご投稿下さい。 HA (冗長化) 構成のお客様は上記 3 点の情報を組みにしてご投稿下さい。

****

(ア) PCI スロット位置の確認

Equalizer XCEL を差し込む PCI スロットがどこに有るかを確認します。 上面パネルを固定しているネジを確認して下さい。

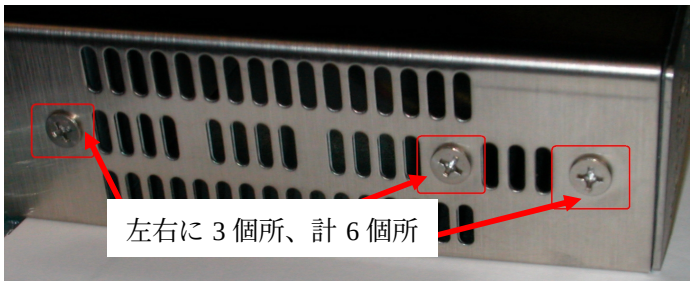

図 1

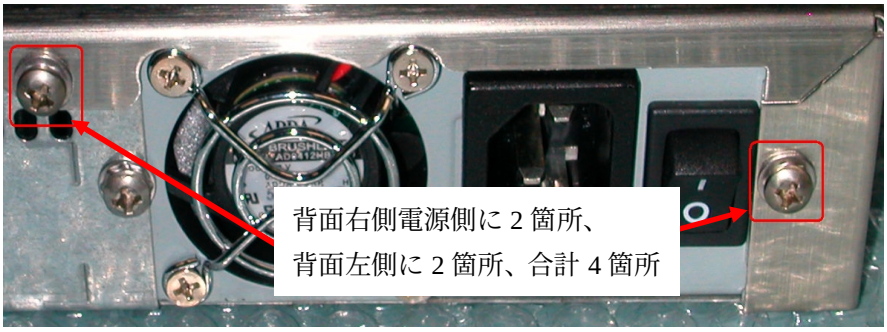

図 2

左右合計 6 箇所、背面 4 箇所のネジを外して、上面パネルを手前に引き出してから、上へ持ち上げて取り外します。 上面パネルを外すと、スロットを確認出来ます。 XCEL カードを差し込むスロットはメモリーが差し込まれている側になります。

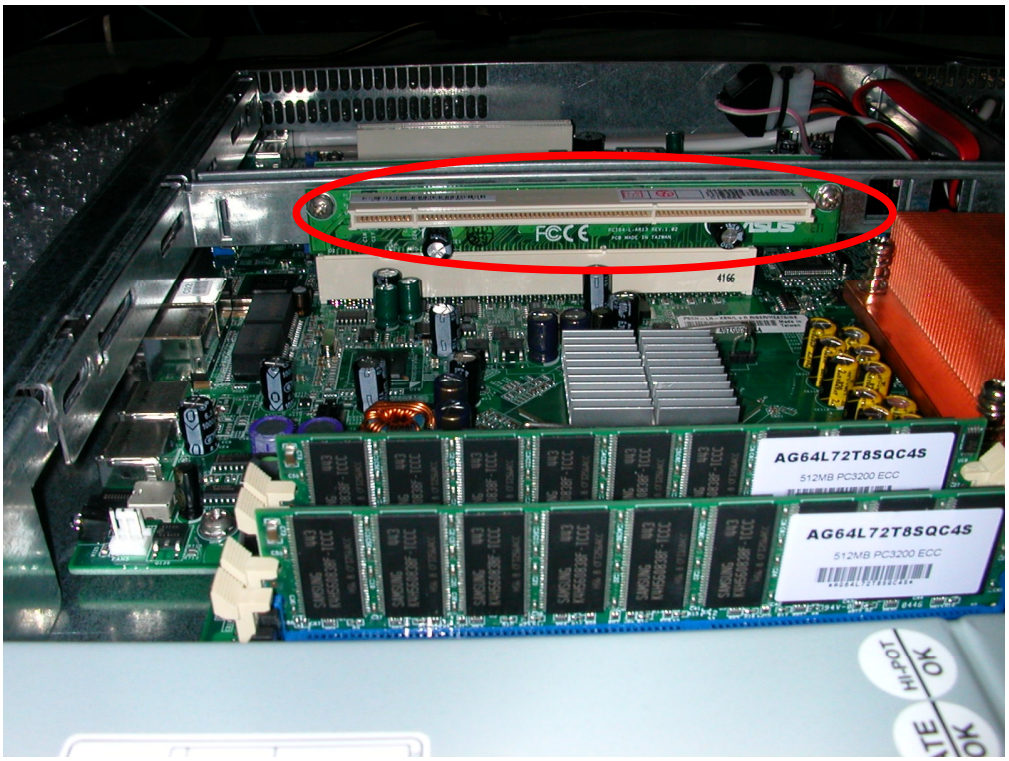

図 3

(イ) XCEL の PCI スロットへの差し込み

① Equalizer XCEL を準備します。

※XCEL の基盤、スロット差し込み口の金属部分には触れないで下さい。

図 4

② 空きスロットに、XCEL を差し込みます。〔XCEL カードが差し難い場合があるので、縦に差し込まれているカードを取り外す事をお勧めします。〔図 5 参照〕〕
※基盤、スロット差し込み口の金属部分には触れないで下さい

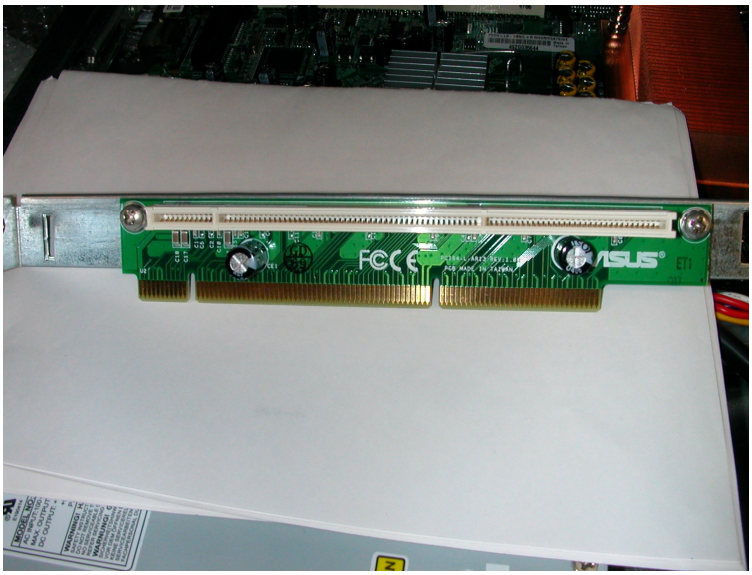

図 5

③ XCEL の裏表を確認して、空き PCI スロットに対して垂直に差し込みます。 多少堅かったり、きつかったりしますが、ゆっくり丁寧に力強く、最後まで差し込んでください。

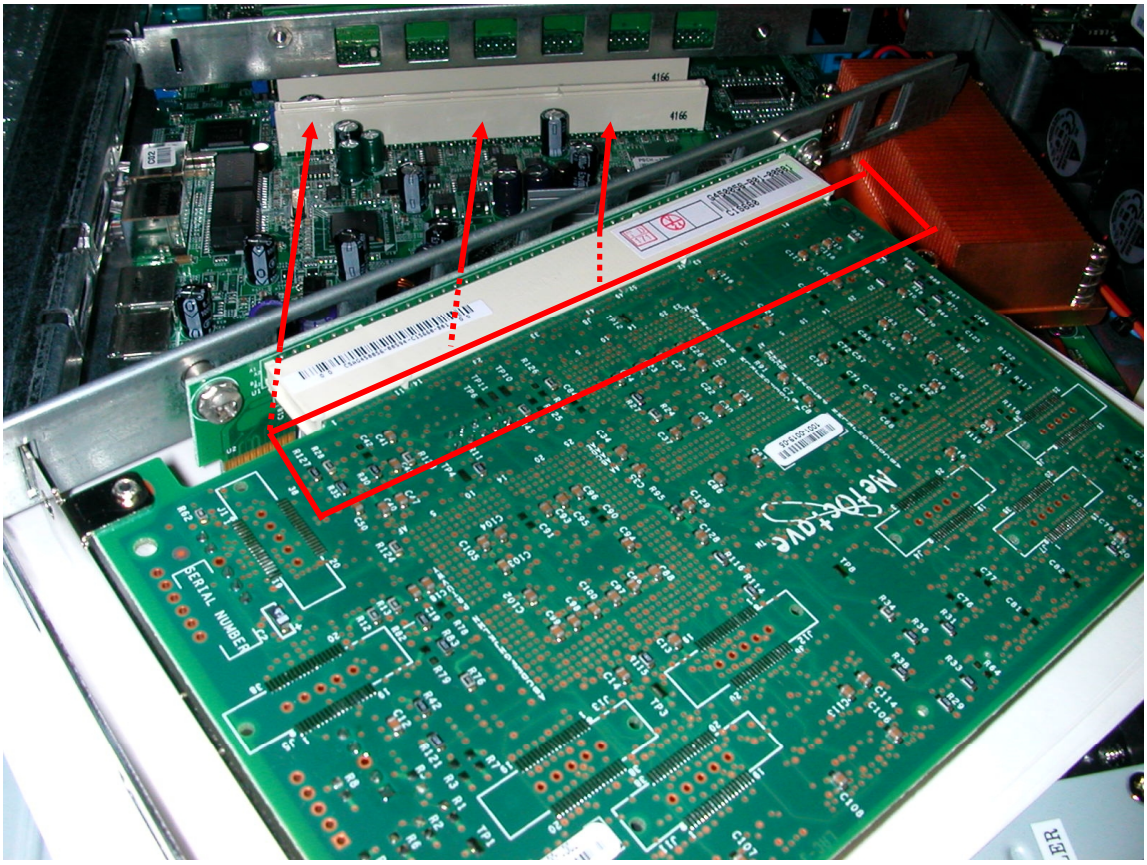

図 6

④　元の場所に差し直して、上面パネルカバーを元に戻して左右面と背面の固定ネジ合計10箇所を止めて下さい。

⑤　以上が XCEL カードインストールになります。

2. XCEL ドライバのアップグレード

最新の XCEL ドライバへアップグレードします。

① Equalizer の Serial ポートに端末を接続します。

② eqadmin で Login します。

③ メニューから「8 Upgrade　　Install new software」を選択します。

④ 「 1 FTP　　FTP to Coyote Point upgrade server 」を選択します。

⑤ FTP サーバ上の XCEL ドライバ upgrade ファイルのパスを指定します。

＊ **XCEL ドライバのアップグレードには事前に登録が必要です。 登録作業には 3 営業日を頂いております。 スケジュール管理にご注意下さい。**

＊ **設定の際は、事前に Tec-world へ件名「XCEL カードアップグレード申請」で、下記項目をご連絡下さい。 ご連絡頂く情報は**

1) **Equalizer シリアル番号**
2) **ifconfig のアウトプット**
3) **XCEL カードのシリアル番号**
4) **HA (冗長化) 構成の場合は上記 1) ～ 3) を組みにしてご連絡下さい。**

＊ **アップグレード時にはメーカー・ライセンスサーバへインターネットアクセスで接続出来る環境が必要です。 Tec-world ご投稿先リンクは https://hds.networld.co.jp/helpdesk/support/login.jsp になります。**

⑥ ローカル FTP サーバに接続後、自動的にデータのダウンロードが開始され、ダウンロード終了後、アップグレードが開始します。

⑦ アップグレード終盤に、

To improve security, we recommend that you disable version 1
of the SSH protocol.
If you do disable this, you may find that certain older SSH
clients such as TTSSH will no longer be able to communicate
with the Equalizer.

Do you wish to disable SSH protocol version 1?

のように SSH バージョン 1 について無効にするか否かを聞かれますので、バージョン 1 を無効に設定する際は「y」として Enter を押して下さい。 処理後の変更は出来ませんので注意を

して設定して下さい。 その後、再起動を行うかを聞かれますので、「y」として Enter を押して下さい。

⑧ reboot 後、XCEL が Equalizer の OS 上から正しく認識されていることを確認します。nspstats コマンドを実行し、XCEL のステータスメッセージが出力される事をご確認下さい。

※ シリアルコンソール接続し、CLI から確認します。

1. Equalizer に電源を投入します。
2. シリアルコンソール接続し、ブート後、**root**（デフォルトで password なし）で Login します。
3. **nspstats** コマンドを実行して XCEL が正しく認識されているか確認します。XCEL が正しく認識されていれば下記のような XCEL のステータスメッセージが出力されます。

```
eq-ext# nspstats
NSP2000 Instance #0:
PK Hardware Errors                  = 0
 PK Requests:   Queued              = 0
 Completed                          = 0
 Checks Called                      = 0
 Preempted                          = 0
 EA Hardware Errors                 = 0
 EA Requests:   Queued              = 0
                Completed           = 0
                Checks Called       = 0
                Preempted           = 0
RN Requests:    Queued              = 0
                Underruns           = 0

NSP2000 Memory statistics:
EA buffers:     current allocation - 0 / 4048 0%
                maximum allocation - 0 / 4048 1%
PK buffers:     current allocation - 0 / 506 0%
                maximum allocation - 0 / 506 0%
```

＊ 認識されていなければ、下記のようなエラーメッセージが表示されます。

eq-ext # nspstats
nspstats: driver open failure – 33

正しく認識されていることが確認できればハードウェアのインストール作業の完了です。

⑨ XCEL ドライバのアップグレードは完了です。

3. Web 管理画面から動作を確認

(1) Web ブラウザで Equalizer の WEB 管理インターフェースにアクセスします。
(2) touch/look でログオンします。
(3) ログイン直後の画面中央に E350si または、E450si と表示されているのを確認します。
(4) 画面左上の「Equalizer」をクリックすると Equalizer status が表示されます。 その際、Equalizer version の確認と SSL acceleration が「enable」になっているか確認します。

＊ SSL acceleration が enable と表示されていない場合は正しくXCEL ライセンスがアップグレードされていない可能性があります。 ライセンスアップグレードの手順 を再度実行して下さい。それでも上手くいかない場合は、Tech-World へご質問下さい。

Equalizer E350si/450si CSR 作成手順

1. CSR 作成時の注意

CSR 作成の手順は基本的に証明書を発行する CA の指定に従ってください。 本手順書の内容が CA の推奨する手順と異なる場合は、本手順を遵守する必要ありません。

SI シリーズのモデルからパスフレーズを使用してのサーバ証明書のアップロードが可能になりました。 パスフレーズを無効にする場合は下記手順の 5 を行って下さい。

2. E350si/450si で CSR を作成する手順

1. Root でログオンします。

2. 作業ディレクトリに移動します

   #cd /tmp

3. 秘密鍵作成のための擬似乱数を作成します

   #openssl md5 * > rand.dat

   rand.dat=出力する擬似乱数。任意のファイル名。

4. 1024bit 3DES により秘密鍵を生成します

   #openssl genrsa -rand rand.dat -des3 1024 > key.pem

   パスフレーズの入力を求められます。任意の文字列を入力して下さい。
   1024=鍵長
   (key.pem=パスフレーズの必要な秘密鍵。任意のファイル名。)

5. パスフレーズを無効にする場合は下記を実行します。 パスフレーズを無効にしない場合は 6 へお進み下さい。

   #openssl rsa -in key.pem -out keyout.pem

   パスフレーズの入力を求められます。先ほどの文字列を入力して下さい。
   (keyout.pem=無効化して出力する秘密鍵。任意のファイル名)

6. 生成した秘密鍵によって CSR を作成します。

(ア) 5 でパスフレーズを無効にした場合:
#openssl req -new -key keyout.pem -out csr.pem
(csr.pem=出力する CSR。任意のファイル名)

(イ) 5 でパスフレーズを無効にしない場合:
#openssl req –new –key key.pem –out csr.pem
(csr.pem=出力する CSR。任意のファイル名)

Enter pass phrase for key.pem: (4 で入力したパスフレーズを入力します。)

CSR 作成時に証明書情報(ディスティングイッシュネーム)の問い合わせがあります。
CA に申請する情報に従って入力して下さい。

Country Name	<国>
State of Province Name	<都道府県名>
Locality Name	<市区町村名>
Organization Name (eg, company)	<正式英語組織名>
Organizational Unit Name (eg, section)	<部門名>
Common Name (eg, YOUR name)	<URL<FQDN>>
Email Address	<管理者のメール<省略可>>
A challenge password	<省略>
An optional company name	<省略>

※A challenge password、An optional company name の入力は省略して下さい。 Blank で Enter。

7. 作成した CSR を FTP でローカルマシンにアップロードし、CA へサーバ証明書の申請を行ってください。

※ HTTPS クラスタへサーバ証明書をインストールするには、CSR 作成時に用いた秘密鍵も必要です。 CSR と一緒にこの秘密鍵もローカルマシンにアップロードして管理して下さい。

※ HTTPS クラスタへインストールする証明書ファイル(composite ファイル)は、CA から発行された証明書(テキスト)と秘密鍵(テキスト)を同一テキストファイルに張り合わせたものです。 加えて、中間証明書が必要な場合には、サーバ証明書、秘密鍵、中間証明書を同一ファイルに順に張り合わせたものを composite ファイルと

呼びます。

参考

SSL アクセラレータ使用時に申請する証明書の枚数に関しましては証明書を発行する CA にお問い合わせ下さい。CA によって申請の際の制約が異なります。 日本 Verisign では同一 Common Name で実際のサーバ台数分の申請が必要なようです。

http://www.verisign.co.jp/server/help/faq/100020/index.html

（リンク切れの場合はご容赦願います）

サーバ証明書インストール手順

Composite ファイルの作成手順

1. Composite ファイルの作成

サーバ証明書と秘密鍵をテキストで貼り付けた Composite ファイルを作成します。 Composite ファイルは下記の様に表示されます。

```
-----BEGIN CERTIFICATE-----
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZa=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJkLmNoPqRsTuVwXyZAwaBcDeFgH
aBcDeFgHiJkLmNoPqRsTuVwXyZaBcDeFgHiJ
-----END RSA PRIVATE KEY-----
```

図 7

2. 中間証明書を含む Composite ファイルの作成

サーバ証明書、秘密鍵、中間証明書を一枚の Composite ファイルとして保存します。 上記例の中間証明書が追加されます。

サーバ証明書部分

-----BEGIN CERTIFICATE----- から

-----END CERTIFICATE----- まで

秘密鍵部分

----BEGIN RSA PRIVATE KEY----- から

-----END RSA PRIVATE KEY----- まで

中間証明書部分

-----BEGIN CERTIFICATE ----- から

-----END CERTIFICATE ----- まで

Composite ファイルのインストール

HTTPS クラスタの選択

1. ウェブ管理インターフェースに touch でログインを行ない、サーバ証明書をアップロードしたい HTTPS クラスタをクリックします。（サーバ証明書がアップロードされていないクラスタは赤色で表示され、クラスタが無効の状態です。）

   画面中央にクラスタ情報が表示されるので、 クラスタ情報画面の右上の menu から「Manage SSL Certificates」を選択します。

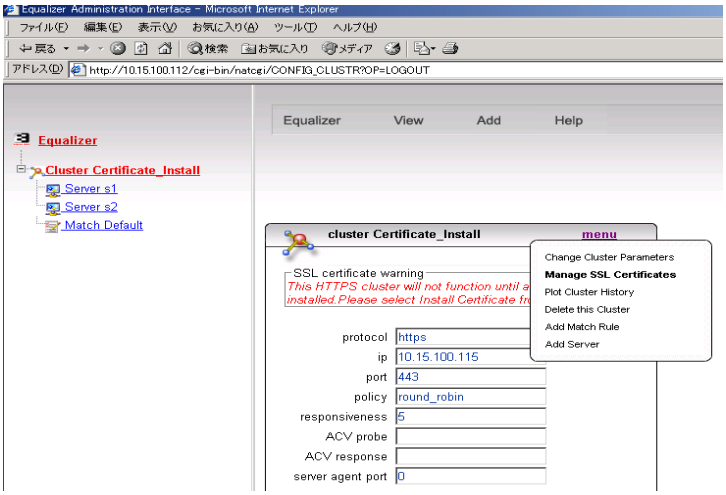

図 8

Composite ファイルのアップロード

2. cluster にチェックが入っている事を確認し、参照ボタンから Composite ファイルを選択して「upload」をクリックします。

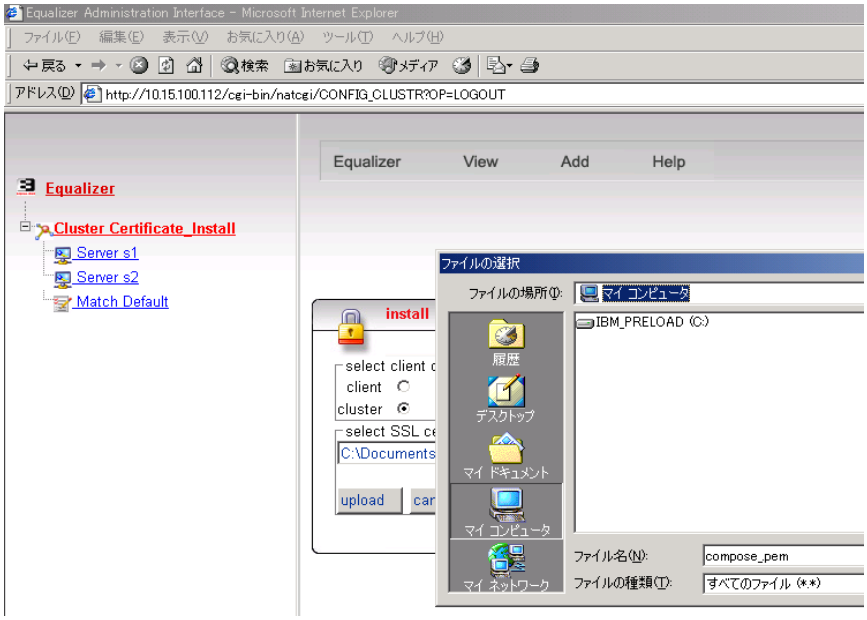

図 9

3. ここで、CSR 作成時にパスフレーズの設定がある秘密鍵の場合には、そのパスフレーズを入力します。 パスフレーズを無効にした場合にはそのままアップロードされます。

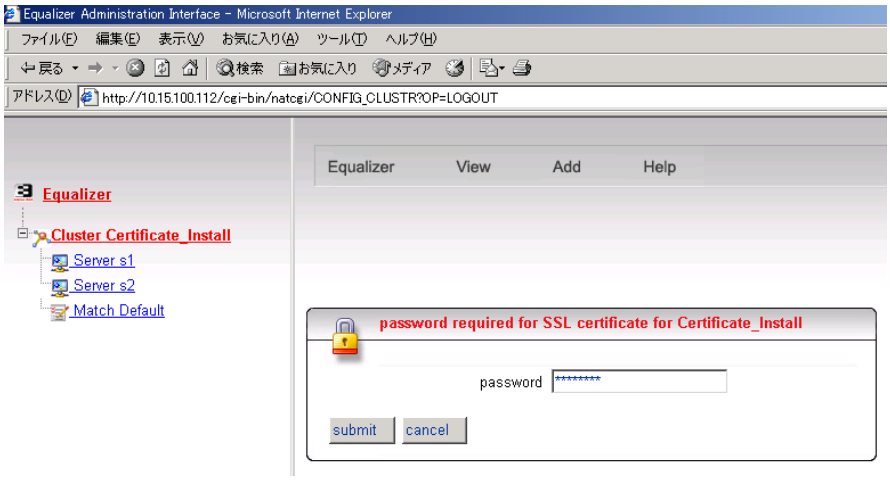

図 10

4. サーバ証明書がインストールされると赤色で表示されていたクラスタ名が緑色に変わります。 これでサーバ証明書のインストールは終了になります。

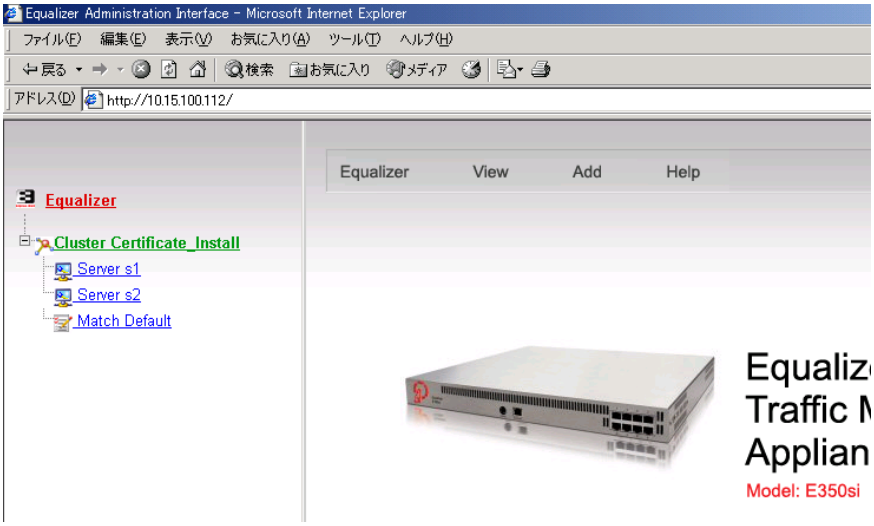

図 11

クライアント証明書のインストール

クライアント証明書をアップロードする HTTPS クラスタをクリックします。「Manage SSL Certificates」を選択して下記画面が表示されます。 client にチェックを入れ、参照ボタンからクライアント証明書を選択して「upload」をクリックするとアップロードされます。以上でクライアント証明書インストールが終了です。

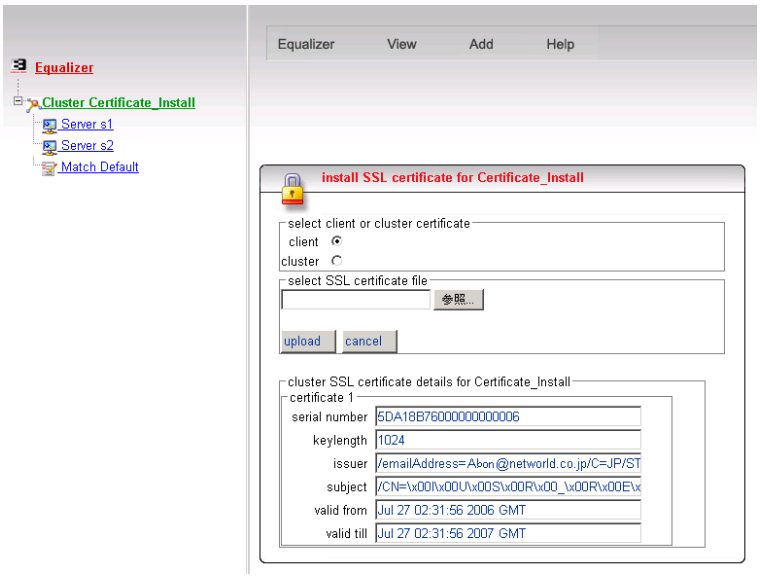

図 12