



## **Coyote Point Systems**

**Equalizer E250GX**

**Equalizer 簡易設定手順書**

Firmware 8.5.1c 対応版 Rev.1.2

[2010/06/24]





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ります。ご了承下さい。

Copyright 2010 Networld, Corp. All right reserved.

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

— 目次 —

EQUALIZER簡易設定手順書について .....	9
<b>セクション1 EQUALIZER設定の準備 .....</b>	<b>10</b>
1-0 機器の設置 .....	10
1-1 ターミナルエミュレーターの設定 .....	10
1-2 初期設定 .....	11
1-2-1 Interfaces (ネットワーク設定) .....	13
1-2-2 Time Zone (タイムゾーン設定) .....	15
1-2-3 Clock (時刻設定) .....	16
1-2-4 Manage users (Web管理画面アカウント作成) .....	17
1-2-5 Console (eqadminアカウントのパスワード変更) .....	18
1-2-6 Commit (設定の適用・再起動) .....	19
1-2-7 Shutdown (機器のシャットダウン) .....	19
1-2-8 Upgrade (ファームウェアアップグレード) .....	19
1-2-9 Manage 'eqsupport' (リモートアカウント接続設定) .....	20
1-2-10 Reset Switch .....	21
1-3 アカウント・パスワード一覧 .....	21
1-3-1 ROOTパスワードの変更方法 .....	21
<b>セクション2 WEB管理画面の操作 .....</b>	<b>23</b>
2-1 EQUALIZER WEB管理画面について .....	23
2-1-1 Equalizer Web管理画面にアクセスする .....	23
2-1-2 Web管理画面の概要 .....	24
2-1-3 機器の詳細情報を表示 .....	24
2-1-4 Helpメニューの利用 .....	26
2-1-5 設定追加・変更の決定ボタンについて .....	27
2-1-6 Web管理画面のメッセージ表示について .....	27
2-1-7 Web管理画面からのログアウト .....	28
2-1-8 Equalizerのライセンス表示について .....	28
<b>セクション3 機器のグローバル設定 .....</b>	<b>29</b>

<b>3-1 “CLUSTERS” タブ設定</b> .....	30
3-1-1 “General” .....	30
3-1-2 “Probes” .....	31
3-1-3 “VLB” .....	32
3-1-4 “Networking” .....	32
3-1-4-1 Send buffer/ Receive buffer について .....	34
3-1-4-2 Outbound NAT通信について .....	34
3-1-4-3 “allow extended chars” 設定について .....	35
<b>3-2 “STATUS” タブ設定</b> .....	36
3-2-1 “Cluster Summary” .....	36
3-2-2 “Statistics” .....	37
3-2-3 “Event Log” .....	39
3-2-4 “Plot” .....	40
<b>3-3 “MONITORING” タブ設定</b> .....	42
3-3-1 “Events” .....	42
3-3-1-1 “logging” .....	42
3-3-1-2 “handling” .....	42
3-3-1-3 “email notification” .....	43
3-3-2 “Export to CSV” .....	44
<b>3-4 “PERMISSIONS” タブ設定</b> .....	45
3-4-1 “Users” .....	45
3-4-1-1 ユーザアカウントの追加 .....	45
3-4-1-2 ユーザアカウント設定の変更 .....	46
3-4-1-3 ユーザアカウントの削除 .....	46
3-4-2 “GUI Access” .....	47
3-4-3 “SSH Access” .....	47
<b>3-5 “MAINTENANCE” タブ設定</b> .....	48
3-5-1 “General” .....	48
3-5-1-1 “backup” .....	48
3-5-1-2 “restore” .....	49
3-5-1-3 “shutdown” .....	49
3-5-1-4 “reboot” .....	50
3-5-1-5 “save state” .....	50
3-5-2 “System Time” .....	51
3-5-2-1 “timezone setting” .....	51
3-5-2-2 “date and time” .....	51

3-5-3	“License Information”	52
3-5-3-1	“license information”	52
3-5-3-2	“Offline License”	53
3-5-3-3	“Online License”	53
3-5-4	“Certificates”	54
3-5-5	“Static Routes”	54
3-5-5-1	スタティックルートの追加	55
3-5-5-2	スタティックルートの変更	55
3-5-5-3	スタティックルートの削除	55
<b>セクション4 クラスタ・サーバ設定手順</b>		<b>56</b>
4-1	クラスタとサーバの関係	56
4-1-1	クラスタの定義について	56
4-1-2	サーバの定義について	56
4-1-3	サーバに対するEqualizerの監視について	57
4-1-4	Equalizerを通過する通信について	57
4-1-5	サーバのデフォルトゲートウェイについて	57
4-1-6	spoof設定について(SNAT設定)	57
4-1-6-1	spoofとは	57
4-1-6-2	SNAT(Source NAT)の動作	58
4-1-6-3	なぜSNATを使用するのか	59
4-1-6-4	SNATのデメリット	60
4-1-6-5	“X-Forwarded-For”ヘッダ追加について	60
4-1-7	ポート変換機能について	60
4-1-8	HTTPSクラスタの動作について	61
4-2	ネットワーク構成について	62
4-3	クラスタ作成	63
4-3-1	クラスタ作成ウィザードの起動	63
4-3-2	L4クラスタの作成	63
4-3-3	L7クラスタの作成	65
4-3-4	クラスタの削除	65
4-4	L4クラスタパラメータ設定	65
4-4-1	“Configuration”タブ	65
4-4-1-1	“Required”	66
4-4-1-2	“Probes”	66

4-4-1-3 “Persistence” .....	68
4-4-1-4 “LB Algorithm” .....	68
<b>4-4-2 “Servers” タブ</b> .....	69
<b>4-4-4 “Reporting” タブ</b> .....	69
4-4-3-1 “Statistics” .....	69
4-4-3-2 “Plots” .....	70
<b>4-4-5 FTPサービスを提供する場合のクラスタ設定</b> .....	70
<b>4-5 L7/HTTPクラスタパラメータ設定</b> .....	72
<b>4-5-1 “Configuration” タブ</b> .....	72
4-5-1-1 “Required” .....	72
4-5-1-2 “Probes” .....	73
4-5-1-3 “Persistence” .....	73
4-5-1-4 “LB Algorithm” .....	74
4-5-1-5 “Networking” .....	74
<b>4-5-2 “Reporting” タブ</b> .....	75
<b>4-6 L7/HTTPSクラスタパラメータ設定</b> .....	76
<b>4-6-1 “Security&gt; Certificates”</b> .....	76
<b>4-6-2 “Security &gt; SSL”</b> .....	77
<b>4-7 L4/L7 クラスタ共通パラメータ詳細</b> .....	79
<b>4-7-1 “Configuration &gt; Require &gt; Policy”</b> .....	79
<b>4-7-2 “Configuration &gt; Require &gt; Responsiveness”</b> .....	81
<b>4-7-3 “Configuration &gt; Probes &gt; ACV probe / response”</b> .....	81
4-7-3-1 “ACV probe” .....	82
4-7-3-2 “ACV response” .....	82
<b>4-8 サーバ設定</b> .....	83
<b>4-8-1 サーバ作成</b> .....	83
<b>4-8-2 サーバ作成ウィザードの入力</b> .....	83
<b>4-8-3 サーバ パラメータ設定変更</b> .....	84
<b>4-8-4 Configuration タブ設定</b> .....	84
4-8-4-1 “Required” .....	84
4-8-4-2 “Outbound NAT” .....	85
<b>4-8-5 “max connection” 設定</b> .....	87
<b>4-8-6 “hotspare” 設定</b> .....	87
<b>4-8-7 “quiesce” 設定</b> .....	88
<b>4-8-8 “dont probe” 設定</b> .....	88
<b>4-8-9 “dont persist” 設定</b> .....	88

<b>セクション5 冗長化設定手順</b> .....	<b>89</b>
<b>5-1 FAILOVER動作の基本概念について</b> .....	<b>89</b>
<b>5-2 PRIMARY / BACKUPの関係について</b> .....	<b>90</b>
5-2-1 Primary”役”、 Backup”役”とは.....	90
5-2-2 切り戻し動作(Failback) について.....	90
5-2-3 冗長化の通信(sibling) について.....	91
5-2-4 Gratuitous ARPについて.....	91
5-2-5 Failoverペア同士のコンフィグ同期について.....	91
5-2-6 Failover Aliasについて.....	92
<b>5-3 FAILOVER設定</b> .....	<b>93</b>
5-3-1 Failover設定画面.....	94
5-3-2 “Peers” タブ (Failoverペアテーブル).....	94
5-3-3 Failover Peer登録ウィザード.....	94
5-3-3-1 設定している機器をPeerとして登録.....	94
5-3-3-2 設定している機器の詳細情報登録.....	94
5-3-3-3 登録の確認.....	95
5-3-3-4 Peerの登録.....	95
5-3-3-5 Peerの詳細情報登録.....	95
5-3-3-6 Peerの詳細情報登録.....	95
5-3-3-7 Peerの変更・削除.....	96
5-3-4 “Parameters” タブ.....	96
5-3-4-1 Failover Alias設定.....	96
5-3-4-2 Failover Timing設定.....	96
5-3-4-3 コンフィグ同期設定.....	97
5-3-4-4 設定の決定、再起動(commit & reboot).....	97
5-3-5 Failover設定完了の確認.....	97
<b>APPENDIX A セッション維持動作解説</b> .....	<b>99</b>
A-1 セッション維持とは.....	99
A-2 EQUALIZERが提供するセッション維持方法.....	99
A-3 STICKY TIMEによるセッション維持.....	100
A-3-1 sticky timeの設定.....	100
A-3-2 sticky timeの注意点.....	100
A-3-3 inter-cluster sticky設定について.....	101

A-3-4 sticky network aggregation設定について .....	101
A-3-5 sticky テーブル情報の同期について.....	101
A-3-6 サーバ単位のセッション維持設定について.....	101
A-4 COOKIEによるセッション維持 .....	102
A-4-1 cookieの設定 .....	102
A-4-2 Equalizerのcookieとサーバのcookieの違い .....	102
A-4-3 Equalizerのcookieの詳細解説.....	102
A-4-4 複数クラスタ間のcookie動作について.....	103
A-4-5 冗長化構成時のcookie動作について.....	103
A-4-6 once only使用時のcookie動作について.....	103
A-4-7 サーバ単位のセッション維持設定について.....	104
 APPENDIX B CSR作成手順.....	 105
B-1 EQUALIZER サーバ証明書インストール手順について .....	105
B-2 CSR作成手順 .....	105
B-3 COMPOSITEファイル 作成手順.....	107
B-4 COMPOSITEファイル アップロード手順.....	108
B-5 サーバ証明書に関する注意事項 .....	110
 改定履歴.....	 111



## Equalizer簡易設定手順書について

簡易設定手順書を使用することで、Equalizer の設置・設定・運用を行うことができます。頻繁にお問い合わせ頂く機能・設定箇所については、より詳細に解説しています。また、Equalizer をより簡単に設定し運用を行えるように、Equalizer が提供する機能についての個別解説も盛り込まれています(その為、文書構成や記述内容はメーカーから提供されている Equalizer 英文マニュアルとは異なります)。

より詳細な説明につきましてはEqualizer英文マニュアルをご参照頂きます様お願い致します。Equalizer英文マニュアルはWeb管理画面の上部メニューから“Help > View Guide(PDF)”を選択することでダウンロードが可能です(セクション [2-1-4](#) を参照下さい)。

簡易設定手順書は、予告なしに記載内容に変更がある場合がありますので、あらかじめご了承下さい。また、改定内容については改定履歴をご確認下さい。

## セクション1 Equalizer設定の準備

### 1-0 機器の設置

Equalizer のインストールは以下の手順でお願いします。

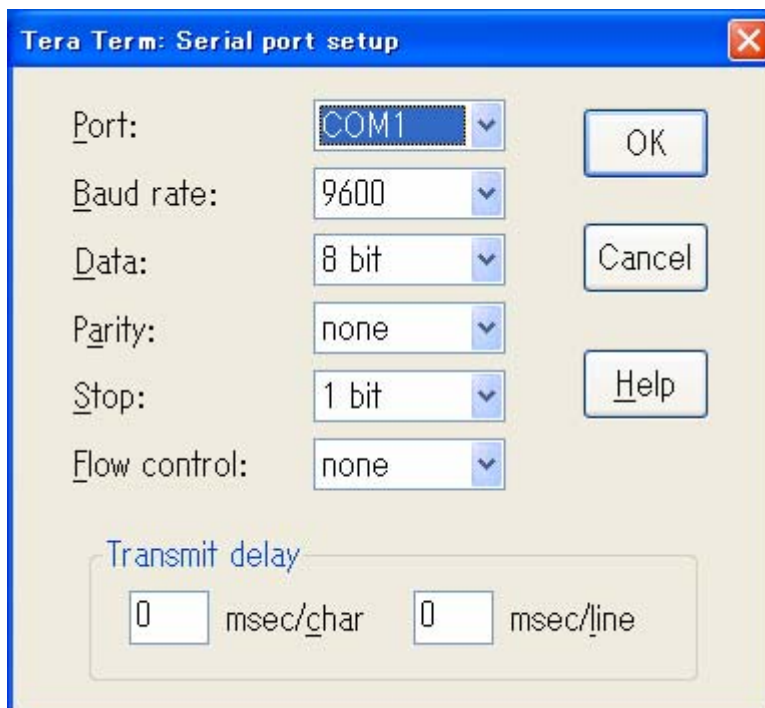
1. 同封されているラックマウント用の金具やケーブル等を箱から取り出します。同封されていたパッケージはそのまま捨てずに保存して下さい。機器初期不良などの理由で機器を返送する際、**オリジナルのパッケージが揃っていないと対応出来ない場合が御座います**ので、ご了承下さい。また、ハード機器に変更点を確認された場合、保証対象にならない場合が御座います。）
2. 平らな場所を選んで Equalizer を設置します。
3. 同封されているシリアルケーブルを使用する際に、Equalizer の前面に「Serial」と書かれている差込み口がありますので、そこに付属のシリアルケーブルを差込みます。TeraTerm Pro 等のターミナル・エミュレータ・ソフトウェア等を使用して設定を行います。
4. カテゴリー5 以上の LAN ケーブルを使用し、Equalizer を LAN に接続して下さい。
  - イ) Equalizer を上・下層ネットワークの中継として使用する場合(デュアルネットワーク構成として使用する場合)、External ポートに RJ-45LAN ケーブルを差して上部ネットワークと接続します。Internal ポートは下部ネットワークと接続します。
  - ロ) シングルネットワーク構成で利用する場合、Internal ポートをそのネットワークへ接続します。
5. Equalizer に同封されている電源コードを使用して、適切な電源へ接続して下さい。この Equalizer 電源ユニットは 50Hz/60Hz、100~240 VAC 入力に対応しています。
6. 後面パネルにある電源スイッチをオンにして、電源を投入します。

### 1-1 ターミナルエミュレーターの設定

Equalizer 機器を設置し電源を投入した後、ターミナルもしくはターミナルエミュレーターを使用して設定を行います。Equalizer 機器の設定に必要なターミナルもしくはターミナルエミュレーターの設定値は以下の通りです。

- 9600 baud rate
- 8 data bit

- no parity
- 1 stop bit
- VT100 emulation



(TeraTerm 設定例)

Windows デフォルトのターミナルエミュレーター、HyperTerminal、を使用する場合、keyboard application mode と cursor keypad mode を有効にする必要があります。

もしご利用のターミナルソフトウェアでシリアルラインのハングアップ設定のサポートがある場合、ハングアップを無視するよう設定して下さい。設定する事で、Equalizer が再起動してもシングルターミナルセッションとして使用する事が出来ます。

Coyote Point Systems社では [TeraTerm](#)をEqualizer機器設定でのエミュレーターとして推奨しています。

## 1-2 初期設定

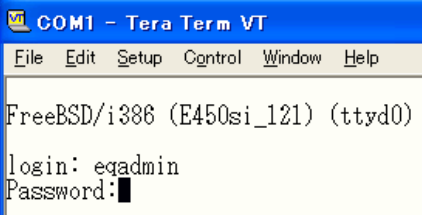
Equalizer が起動すると、デバイス情報や起動中である旨のメッセージがターミナルに表示されます。通常、これらの表示については確認をする必要はありません。しかし、ターミナルエミュレーションソフトウェアでハングアップを無視するように設定していない場合、起動中にターミナルのセッションが2重に存在してしまう可能性があるため、そのような場合はターミナルのセッションを起動し直して下さい。

1. Equalizer の起動処理が終了すると、ログインプロンプトが表示されます。ここで、eqadmin

と入力し <Enter> を押します。Equalizer へのログインアカウントとして、root を選択することも可能です(初期パスワードは設定されておりません)。 root ユーザとしてログインすると Equalizer 内部システム(FreeBSD ベース)へアクセスすることができます。

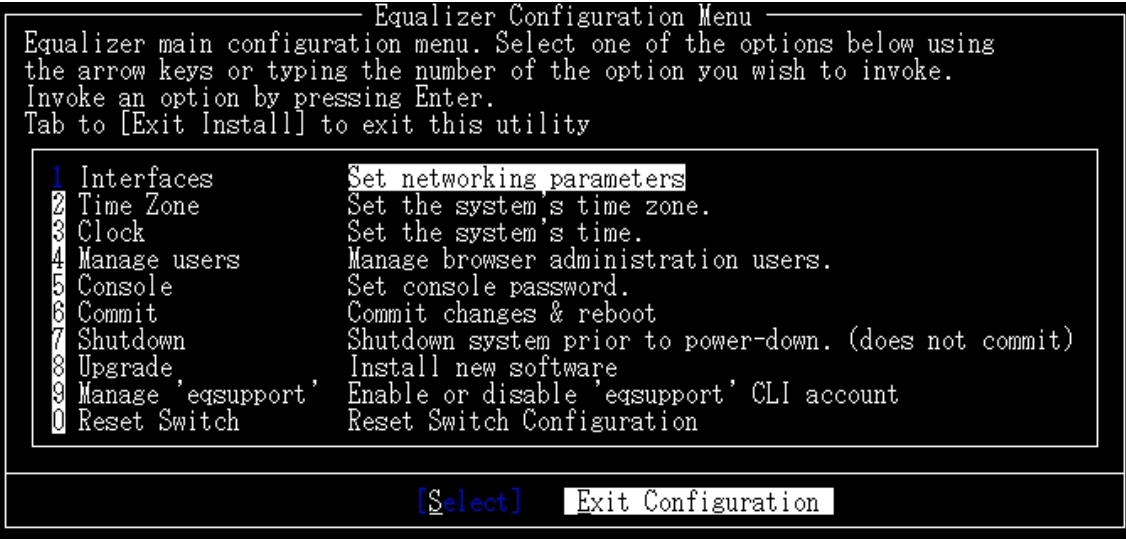
※ ファイルを直接編集すると機器不具合の原因にもなりますので、弊社サポートからご依頼させて頂く場合以外の利用はお控え頂きます様お願い致します。

2. パスワードを要求されますので、デフォルトの equalizer を入力します。



```
COM1 - Tera Term VT
File Edit Setup Control Window Help
FreeBSD/i386 (E450si_121) (ttyd0)
login: eqadmin
Password: █
```

3. Equalizer の基本設定(変更)用の CLI 「Equalizer Configuration Utility」が起動します。



```
Equalizer Configuration Menu
Equalizer main configuration menu. Select one of the options below using
the arrow keys or typing the number of the option you wish to invoke.
Invoke an option by pressing Enter.
Tab to [Exit Install] to exit this utility

1 Interfaces          Set networking parameters
2 Time Zone           Set the system's time zone.
3 Clock               Set the system's time.
4 Manage users        Manage browser administration users.
5 Console             Set console password.
6 Commit              Commit changes & reboot
7 Shutdown            Shutdown system prior to power-down. (does not commit)
8 Upgrade             Install new software
9 Manage 'eqsupport' Enable or disable 'eqsupport' CLI account
0 Reset Switch        Reset Switch Configuration

[Select] Exit Configuration
```

#### TeraTerm Pro を使用時の画面

4. Configuration Utility でメニューを選ぶ時は矢印キーで上下に設定・変更したいメニュー項目を選びます。 選択されたメニューはハイライトで確認する事が出来ます。

使用しているターミナルエミュレーターで矢印キーが使用出来ない場合は <CTRL> + n で次のメニュー項目、 <CTRL> + p で前のメニュー項目を選択することが出来ます。 矢印キーの左右でモードを選択します。「Select」でメニュー項目を選択出来る状態になります。

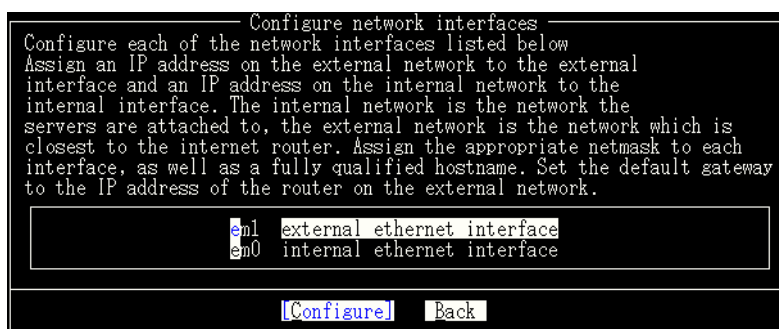
「Exit Configuration」を選択すると Configuration Utility が終了し、元のログインプロンプトが表示されます。 使用しているターミナルエミュレーターで矢印キーが使用出来ない場合は <Tab> で同様の動作を行う事が出来ます。

項番	項目名	設定内容
1	Interfaces	ネットワークパラメータの設定を行います
2	Time Zone	タイムゾーンの設定を行います
3	Clock	日時の設定を行います
4	Manage users	ウェブ管理画面のユーザ登録
5	Console	コンソールパスワードを変更します
6	Commit	設定パラメータの変更を決定(再起動を伴います)
7	Shutdown	機器のシャットダウン (設定パラメータの更新は反映されません)
8	Upgrade	ファームウェアのアップグレードを行います
9	Manage 'eqsupport'	SSH によるコンソール画面へのアクセスを設定します
0	Reset Switch	E250GX シリーズでは使用しません。

## 1-2-1 Interfaces (ネットワーク設定)

このメニューから、機器のホスト名、ネットワークインターフェース、デフォルトルート、そして DNS サーバなど、ネットワークに関連する設定を行うことができます。

1. Configuration Menu ウィンドウの 1 番目のオプション **Interfaces** を選択し <Enter> を押すと、「Configuration network interfaces」ウィンドウが表示されます。

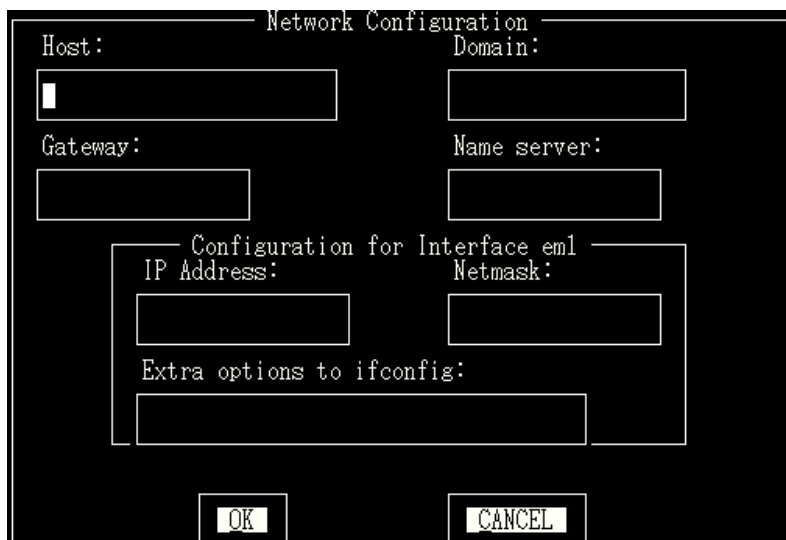


External インターフェースを選択すると、ホスト名や DNS サーバなど機器全体の設定を行うことができます。Internal インターフェースを選択すると Internal インターフェースの IP アドレスの設定を行うことができます。

ネットワークインターフェースの設定注意点として Equalizer を シングルネットワーク構成で使用する場合には、External インターフェース では機器全体の設定のみを行い IP アドレス設定は行わないで下さい。Internal インターフェース IP アドレスのみ設定します。

2. 上下の矢印キーで **external ethernet interface** を選択し、上記の図の様にハイライトさ

せませす。 <Enter> を押すと、下記図の様に「Network Configuration」が表示されます。デュアルネットワーク構成かシングルネットワーク構成かを問わず、Host、Domain、Gateway、そしてName server の項目は external ethernet interface に設定する必要があります。 internal ethernet interface の設定では、これらの項目は含まれません。



```

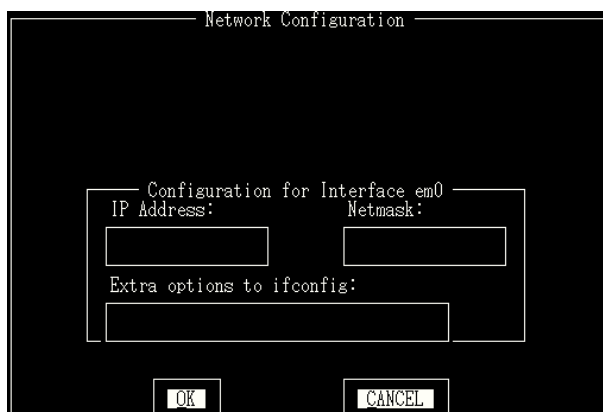
Network Configuration
Host: [ ] Domain: [ ]
Gateway: [ ] Name server: [ ]
Configuration for Interface em1
IP Address: [ ] Netmask: [ ]
Extra options to ifconfig: [ ]
OK CANCEL
  
```

**備考:** 各設定項目を入力したら、必ず <Enter> を押して下さい。決して、矢印キーや <Tab> 等で項目入力後に項目移動しない様にご注意下さい。Network Configuration 内で設定が反映されない事があります。

3. Host の項目はお客様ネットワーク環境での Equalizer の名前を入力します。( <Tab> を押す事で、各項目を移動する事が出来ます。)
4. Domain の項目は Equalizer のドメイン名を入力します。  
 ・例えば、FQDN で、equalizer.mydomain.com だとすると、Host の項目には equalizer を入力し、Domain の項目には mydomain.com を入力します。  
 (Host の項目で、equalizer.mydomain.com と入力すると、Domain の項目には自動的に mydomain.com が入力されます。)
5. Gateway の項目では External 側ネットワークのデフォルトゲートウェイ IP アドレスを設定して下さい。 Equalizer が External ネットワークから外部へ送信するすべてのパケットはこのゲートウェイを通ります。
6. Name server の項目は Equalizer が使用する DNS サーバの IP アドレスを入力します。  
**DNS が存在しない場合は「0.0.0.0」を入力して下さい。**
7. External ポートを使用する場合(デュアルネットワーク構成のスイッチ型 Equalizer を利用する場合、もしくは 2 ポート Equalizer を使用したデュアル・シングルネットワーク構成での設定の場合)、External 側インターフェースに唯一固有の IP アドレスを設定します。  
 (IP Address と Netmask の項目では External 側ネットワークに対応した数値を入力して

下さい。設定前にはネットワーク構成図等を利用して設定を事前にご確認下さい。) シングルネットワーク構成時は Internal 側アドレスのみ設定します。External 側の IP アドレスは空白の状態です。〈Enter〉を押して、何も入力されていない事をご確認下さい。

8. 設定が終了したら、OK を選択し 〈Enter〉 を押して下さい。
9. Internal インターフェースのパラメータを設定する場合は **internal ethernet interface** を選択し、〈Enter〉 を押して下さい。



10. IP Address と Netmask を入力します。
11. 設定が終了したら、OK を選択し 〈Enter〉 を押して下さい。
12. **Back** を選択し 〈Enter〉 を押すと、メインの Configuration メニュー、Equalizer Configuration Menu に戻ります。  
(設定を更新させるには、Equalizer Configuration Menu の 6 番目、Commit を選択します。その後、Equalizer 機器が再起動します。)

**注意:** 各インターフェースにある “Extra options to ifconfig” では、ポートの Duplex や Speed を選択することが可能です。デフォルトでは全て Auto で動作していますが、固定にする場合はこちらに記入します。書式については TEC-World の FAQ をご参照下さい。

## 1-2-2 Time Zone (タイムゾーン設定)

現在のタイムゾーンを変更するには、次の順序で行います。また、同設定は Web 管理画面からも行なうことが可能です。

※本設定に再起動は必要ありません。

1. Equalizer Configuration Menu ウィンドウで 2 番目の項目、Time Zone を選択して 〈Enter〉 を押します。

2. メニューバーから設定したいタイムゾーンを選択します。



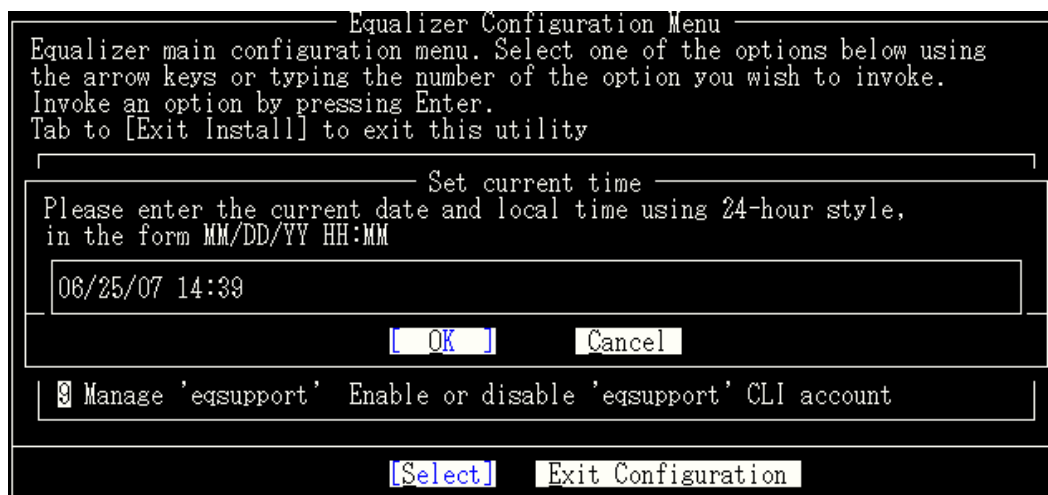
3. 設定が終了したら、OK を選択し <Enter> を押して下さい。  
(更新を行うには再起動が必要です。設定パラメータの更新をご参照下さい。)

### 1-2-3 Clock (時刻設定)

現在の日付、時間を設定するには、次の順序で行います。

※ 本設定に再起動は必要ありません。

1. Equalizer Configuration Menu ウィンドウで 3 番目の項目、Time を選択して <Enter> を押します。
2. 24 時間での時間を、月/日/年 時:分 で設定します。



3. 設定が終了したら、OK を選択し <Enter> を押して下さい。



**備考:** 日時の設定は CLI で行うことも可能です。root でログインして頂き、date YYYYMMDDHHMM で <Enter> を押して下さい。

例) date 200711011957 で <Enter> 直後に 2007 年 11 月 01 日 19 時 57 分 00 秒で設定されます。)

## 1-2-4 Manage users (Web管理画面アカウント作成)

eqadmin で基本設定を行った後は、Web ブラウザから機器設定を行い、この画面は Web 管理画面と呼ばれます。デフォルトで設定されているアカウント名は:

touch (設定可能ユーザ。デフォルトパスワード: touch )

look (Read Only ユーザ。デフォルトパスワード: look )

の2つです。

上記以外のユーザ作成を行なう際はこのメニューを使用します。

**備考:** 同様の作業は Web 管理画面からも行なうことが出来ます。しかし、Web 管理画面へのログインパスワードを紛失した場合などは、ここからユーザを新規作成することで Web 管理画面へのアクセスが必要になります。

touch パスワードはブラウザで Equalizer にアクセスした際に、編集モード(touch)でログインする際のパスワードになります。パスワードに使用出来る文字はスペース以外のプリント可能な文字列の組み合わせになります。また、文字列の長さは 20 文字までで、大文字小文字は区別されます。パスワード変更を行うには次の手順で行います。

1. Equalizer Configuration Menu ウィンドウで 4 Manage users を選択して <Enter> を押します。
2. 編集可能ユーザ(Full Access) または Read Only ユーザを作成するかを選択します。



3. 以下の項目が表示されますので、入力します。

- Enter username: アカウント名を設定します。
- Enter full name: your user アカウント名の説明を設定します
- Enter password: パスワードを設定します、確認を含め2回入力します

### 1-2-5 Console (eqadminアカウントのパスワード変更)

現在設定作業をしている Configuration Utility にアクセスする為にアカウント eqadmin に対するパスワードの変更になります(初期パスワードは equalizer 設定されています)。パスワードに使用出来る文字はスペース以外のプリントが可能な文字列の組み合わせになります。パスワード変更を行うには次の手順で行います。

1. Equalizer Configuration Menu ウィンドウで 5 番目の項目、Console を選択して <Enter> を押します。

```

Equalizer Configuration Menu
Equalizer main configuration menu. Select one of the options below using
the arrow keys or typing the number of the option you wish to invoke.
Invoke an option by pressing Enter.
Tab to [Exit Install] to exit this utility

1 Interfaces      Set networking parameters
2 Time Zone      Set the system's time zone.
3 Clock          Set the system's time.
4 Manage users   Manage browser administration users.
5 Console        Set console password.
6 Commit         Commit changes & reboot
7 Shutdown      Shutdown system prior to power-down. (does not commit)
8 Upgrade        Install new software
9 Manage 'egsupport' Enable or disable 'egsupport' CLI account

[Select] Exit Configuration
  
```

2. 以下の項目が表示されますので、入力します。パスワードの変更はこの作業後、直ぐに適用されます。

- Changing local password for eqadmin.  
New password:
- Retype new password:

## 1-2-6 Commit（設定の適用・再起動）

設定変更したコンフィギュレーションを適用更新するには、Equalizer を再起動させる必要があります。設定変更を適用させるには、次の順序で行います。

1. Equalizer Configuration Menu ウィンドウで 6 番目の項目、Commit を選択して <Enter> を押します。
2. 再起動の処理が終了したら設定の更新がされているか、再度確認します。

**備考：** この作業を行わないと Equalizer に変更したコンフィギュレーションを適用させる事が出来ません。 eqadmin で設定変更を行った際には必ずこの処理を行って下さい。ただし、パスワード変更とリモートアクセスの設定についてはこの再起動は必要ありません。

## 1-2-7 Shutdown（機器のシャットダウン）

Configuration Utility を使用して Equalizer をシャットダウンさせる事が出来ます。シャットダウンの動作自体は Equalizer の設定更新を行いません。シャットダウンを行うには次の手順で行います。

**備考：** 機器の電源を落とす場合は、かならずシャットダウンを行なってください(機器が故障する場合があります)。シャットダウンは Web 管理画面からも行なうことが可能です。

1. Equalizer Configuration Menu ウィンドウで 7 番目の項目、Shutdown を選択して <Enter> を押します。
2. シャットダウンの処理が終了したら、機器の電源を切って下さい。

## 1-2-8 Upgrade（ファームウェアアップグレード）

Coyote Point Systems 社から最新の Equalizer のソフトアップグレードを行うには Equalizer Configuration Utility を使用して行います。

ファームウェアの提供は弊社より行われ、最新ファームウェアご提供の連絡は保守契約お客様へメールにて行なわれます。ファームウェアの提供依頼などについてはそちらのメールをご確認下さい。

## 1-2-9 Manage 'eqsupport' (リモートアカウント接続設定)

Equalizer へのリモートアクセスのアカウントを有効にした場合、Equalizer ヘシステム確認を目的として遠隔アクセスが可能です。Equalizer Configuration Utility リモートアクセスを有効にすると、Equalizer システム確認を目的としてリモートアクセスで接続する事が可能です。利用するアカウントは eqsupport のみとなりアカウント追加は出来ません。

**注意:** eqsupport アカウントの無効化やアップグレード処理を遠隔から行うと、SSH にてアクセス出来なくなる場合が御座いますので、編集を伴う処理を行う場合にはシリアル接続にて処理を行って下さい。

**注意:** eqsupport アカウントは初期状態では無効に設定されています、またパスワードも設定されておきませんので、ご利用になる場合は有効化(Enable)し、パスワードの設定が必要になります。

リモートアクセスアカウント設定手順は以下の通りになります。

1. 9番目の「Manage 'eqsupport'」を選んで、<Enter> を押します。
2. Equalizer CLI eqsupport account selection が下記画面のように表示されるので、オプション3の Password を選択します。

New Password:

Retype New Password:

と表示されますので、従ってパスワードを2回入力します。パスワードが合致し、設定が完了するとメニュー画面に戻ります。

```

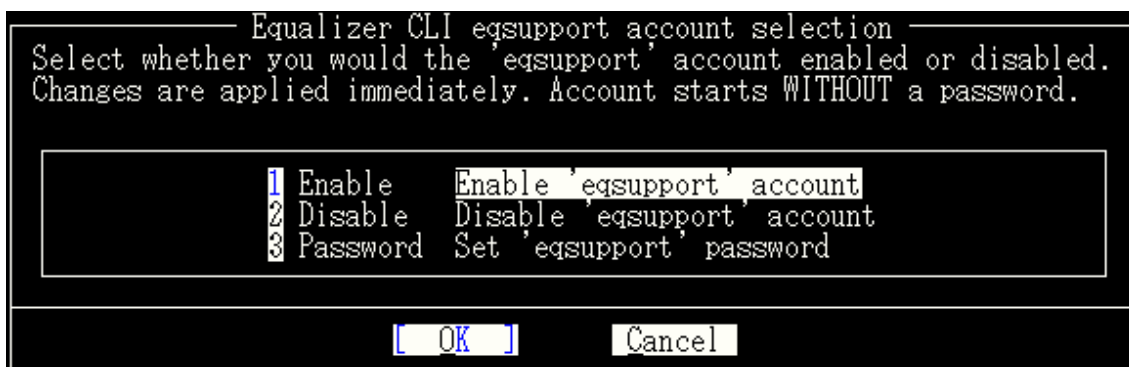
Equalizer CLI eqsupport account selection
Select whether you would the 'eqsupport' account enabled or disabled.
Changes are applied immediately. Account starts WITHOUT a password.

  1 Enable   Enable 'eqsupport' account
  2 Disable  Disable 'eqsupport' account
  3 Password Set 'eqsupport' password

Changing local password for eqsupport.
New password:
Retype n
ew password:

```

3. オプション1の Enable をハイライトして <Enter> を押します。これで、リモートアカウントが有効になります。



4. リモートアクセスアカウントを無効化する場合は、メニュー画面からオプション2 Disable を選択します。
5. パスワードを変更したい場合は手順1と同様、メインメニューから Manage 'eqsupport' を選択し、パスワードを再度入力します。  
※既存のパスワード再入力は求められません。

### 1-2-10 Reset Switch

Equalizer E250GX では使用しません。

## 1-3 アカウント・パスワード一覧

Equalizer のアカウントおよびパスワードの初期設定一覧は以下の通りです。

アカウント名	CLI(コンソール)	Web 管理画面	初期設定	変更方法
root	○	—	(設定なし)	1-3-1 を参照
eqadmin	○	—	equalizer	<a href="#">1-2-5</a> を参照
eqsupport	○(SSH)	—	(設定なし)	<a href="#">1-2-9</a> を参照
touch	—	○	touch	<a href="#">3-4-1-2</a> を参照
look	—	○	look	<a href="#">3-4-1-2</a> を参照
カスタム	—	○	(設定なし)	<a href="#">3-4-1-2</a> を参照

### 1-3-1 rootパスワードの変更方法

1. root アカウントでコンソール画面へログインします。
2. 以下のコマンドを実行します

passwd root

3. パスワードの入力、および再入力を求められますので、入力し決定します。
4. 設定を反映するには機器の再起動が必要ですので、1-2-6 の Commit changes & reboot を実行し機器の再起動を実施して下さい。

**備考:** root パスワードを紛失した場合、パスワードのリセットが必要になります、方法は TEC-World の FAQ をご確認ください。この作業には機器の再起動が必要になりますので、サービスの提供に影響します。

## セクション2 Web管理画面の操作

### 2-1 Equalizer Web管理画面について

セクション1にて初期設定の完了後は、Equalizer のサービスの設定・管理等は Web 管理画面より行ないます。JavaScript が有効なウェブブラウザを使用しログインします。

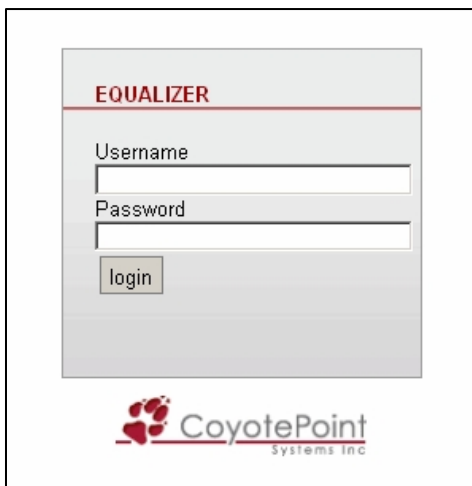
#### 2-1-1 Equalizer Web管理画面にアクセスする

管理画面で Equalizer にアクセスする為に、ブラウザは JavaScript が有効になっている事を確認下さい。

1. ブラウザ画面にEqualizerのIPアドレスを入力します。 External側・Internal側どちらのポートであってもIPアドレスが設定されていればログインが可能です(アクセス制限を行う場合は [3-4-2](#) を参照下さい)。

冗長化構成の場合、2台が共有するFailover AliasのIPアドレスを使用してログインすることも可能です。 この場合、Primaryとして動作している機器に接続されます。

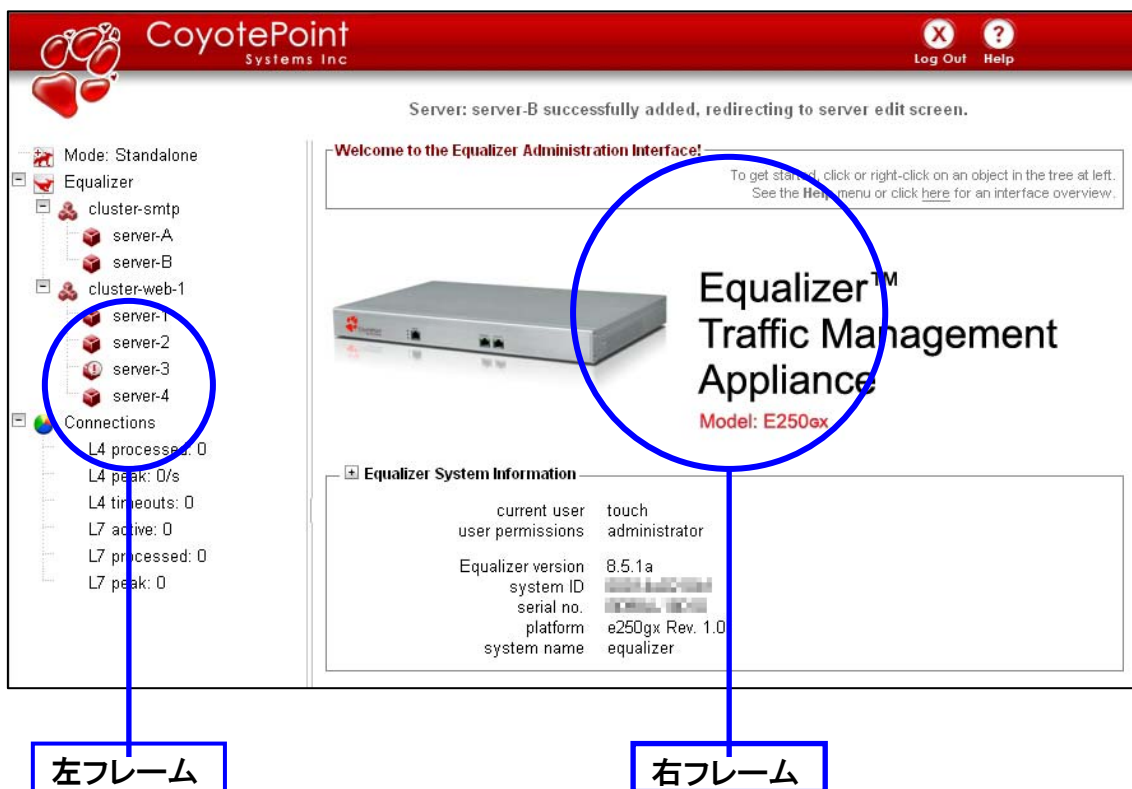
2. ログイン画面が表示されます。 [1-2-4](#) で作成したアカウント、あるいはデフォルトで設定されているtouchまたはlookアカウントにてログインを行ないます。



**備考:** パスワードを忘れてしまった場合は、Equalizerにシリアル接続してアカウントを作成する事が可能です。詳しくは [1-2-4](#) を参照下さい。

## 2-1-2 Web管理画面の概要

Web 管理画面へログインすると、以下の画面が表示されます



Web 管理画面は2つフレームで構成されています。

左フレームは、メインメニュー、設定したクラスター・サーバなどが表示されます。

右フレームは、左フレームで選択した項目の詳細情報が表示されます。右フレーム内に表示されるタブを選択することで、より詳細な項目を設定することが出来ます。

## 2-1-3 機器の詳細情報を表示

ログイン後、右フレーム下のボックス上にマウスを乗せることで機器の詳細情報を表示することができます。



Equalizer System Information

current user	touch
user permissions	administrator
Equalizer version	8.5.1a
system ID	XXXXXXXXXX
serial no.	XXXXXXXXXX
platform	e250gx Rev. 1.0
system name	equalizer
external interface	em1
internal interface	em0
external address	10.15.2.201
internal address	10.15.101.211
failover mode	standalone
sequence number	9
Envoy geographic load balancing	not available on this hardware
SSL acceleration	not available on this hardware
hardware GZIP compression	not available on this hardware
Virtualization Load Balancing	VLB Basic

- **current user**  
現在ログインしているユーザ名を表示します。
- **user permissions**  
現在ログインしているユーザの権限を表示します。
- **Equalizer version**  
機器のファームウェアバージョンを確認することができます。
- **systemID**  
機器の SystemID を表示します。この情報はファームウェアアップグレード時などメーカに機器の登録を行なう際に必要になります。
- **serial no.**  
機器のシリアル番号が表示されます。
- **platform**  
機器のハードウェアプラットフォーム情報が表示されます。
- **system Name**  
スタンドアロンで動作している場合はホスト名([1-2-1 参照](#))が、冗長化構成の場合はPeer name([5-3-3-2 参照](#))が表示されます。
- **external interface**  
External 側のインターフェース名が表示されます、これは機器により異なります。
- **internal interface**  
Internal 側のインターフェース名が表示されます、これは機器により異なります。

- external address  
External 側の IP アドレスが表示されます。
- internal address  
Internal 側の IP アドレスが表示されます。
- failover mode  
機器のフェイルオーバー状態が表示されます。
  - standalone → 機器は単体で動作しています(Failover 設定がない状態)
  - primary → 機器は Primary 役で動作しています。
  - backup → 機器は Backup 役で動作しています。
  - initializing → Failover Mode を認識中に表示されます(機器起動直後など)。  
また、ネットワークに問題があり、機器がポージング状態になっている場合でも表示されます。 その場合は上位ネットワーク、  
負荷分散対象サーバの接続を確認して下さい。
- sequence number  
機器のsequence値が表示されます。 sequence値については [セクション5-2-5](#)をご参照下さい
- Envoy geographic load balancing  
E250GX では Envoy 機能を使用することは出来ません。
- SSL acceleration  
E250GX では XCEL カードを使用することは出来ません。
- Hardware GZIP compression  
E250GX ではハードウェアによる HTTP 圧縮を行うことは出来ません。
- Virtualization Load Balancing  
E250GX では VLB Basic のみ使用することが出来ます。

## 2-1-4 Helpメニューの利用

Web 管理画面右上にある Help メニューから Equalizer に関する情報を確認することが出来ます。 確認できるドキュメントは Equalizer 内部からダウンロードしていますので、インターネットへの接続は必要ありません。



- View Guide(PDF)  
Equalizer のマニュアル(英語)をダウンロードできます。
- View Release Notes(PDF)  
使用しているファームウェアのリリースノートを確認することができます。
- View Transition Guide (PDF)  
ファームウェアバージョン7と8の差異について確認することができます。
- Context Help(PDF)  
Equalizer の Web 管理画面についてマニュアルがダウンロードできます。
- About  
ログイン直後の画面へ移動します。

### 2-1-5 設定追加・変更の決定ボタンについて

Web 管理画面で設定の追加または変更を行った場合は、必ず決定ボタンを押して反映させる必要があります。この動作を行わない場合、変更内容が失われますのでご注意ください。

決定ボタンは  です。

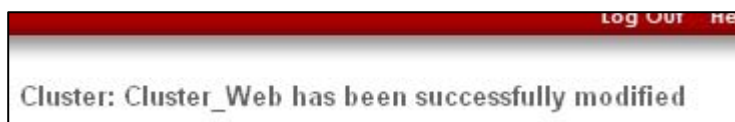
### 2-1-6 Web管理画面のメッセージ表示について

Web 管理画面では、設定画面のステータスメッセージが画面右上に表示されます。現在選択している画面の情報や、設定変更が正常に行われたかなどはメッセージをご確認下さい。

右図の例では、クラスター “Cluster\_Web” をクリックした際に表示されるメッセージです、[4-4-1-1](#) で説明されている “required” の設定画面が選択されていることを示しています。



2-1-5 の操作を行い設定を変更した場合には、右図のように、正常に設定が反映された旨のメッセージが表示されます。



## 2-1-7 Web管理画面からのログアウト

Web 管理画面からログアウトするには、画面右上から Log Out を選択します。



## 2-1-8 Equalizerのライセンス表示について

Equalizer のライセンスは出荷時に有効になっていますが、なんらかの理由でライセンスが無効になった場合には、Web 管理画面のトップページから確認ができます。

下記図のように筐体画像が変化した場合はヘルプデスクへご連絡下さい。



## セクション3 機器のグローバル設定

Equalizer のグローバル設定について項目別に設定を行います。全ての設定はWeb 管理画面から行います。

左フレームから Equalize を選択すると、右フレームにタブが表示されます。タブを選択することで各設定各設定画面を表示させることができます。

Failover設定(5-3)を行った場合、  
"Equalizer" の代わりに機器に設定したPeer Nameが表示されます。



表示される右フレームは以下ようになります。

タブ(Clusters, Status, Monitoring, Permissions, Maintenance)をクリックするとそれぞれのセクションが表示されます。



## 3-1 “Clusters” タブ設定



### 3-1-1 “General”

Name	Type	IP Address	Port	Servers	Actions
cl_K_172_ps	HTTPS	10.15.100.172	443	4  1  0	
HTTPS_Web	HTTP	10.15.100.173	80	3  1  0	
cl01	L4 TCP	10.15.100.176	80	0  0  0	

設定されているクラスタ(4-3 を参照)を一覧表示します、また所属しているサーバの状態も簡易表示することが可能です。

- Name  
クラスタの名称を表示します。
- Type  
tcp\_L4, udp\_L4, HTTP, HTTPS のクラスタタイプを表示します。
- IP Address  
クラスタの IP アドレスが表示されます。
- Port  
クラスタのポート番号が表示されます。
- Servers  
所属しているサーバの状態が表示されます。  
左から Up, Down, dont probe のサーバ数がそれぞれ表示されます。
- Actions  
クラスタの削除、変更、新規作成を行うことができます。

項目	内容
	該当クラスタを削除します。
	該当クラスタ設定を変更します。
	クラスタ作成ウィザードを起動します。

### 3-1-2 “Probes”

Equalizer のヘルスチェック設定を変更します。

probe parameters

probe interval	20.0
probe timeout	10.0
strikeout threshold	3
probe delay	10.0
agent delay	10.0

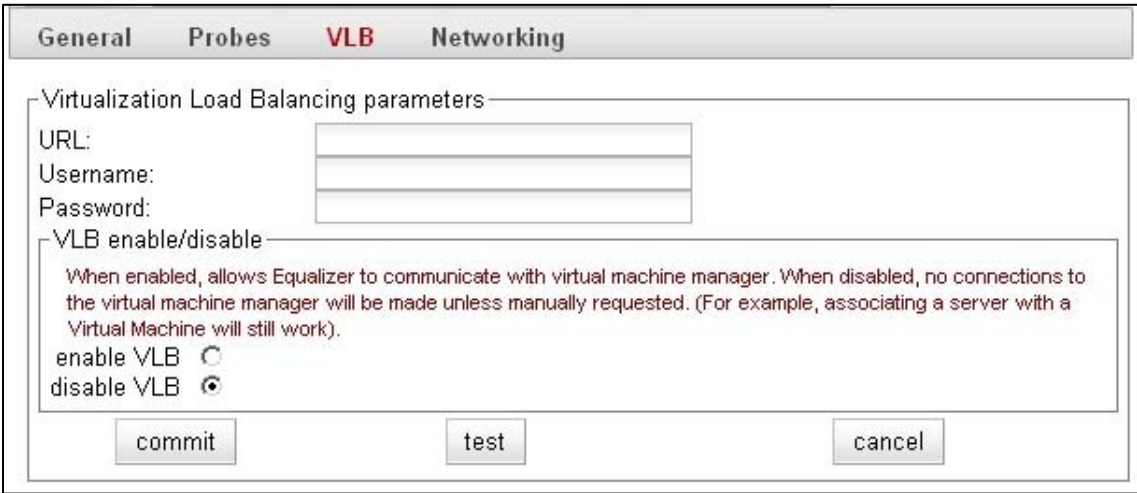
require agent response 
     
 ICMP probe

commit
show defaults
reset

項目	設定内容
probe interval	TCP ハンドシェイク(および ACV)が1度失敗した後、2 回目以降のヘルスチェックは Probe Interval で設定した間隔(秒)で行われます。 デフォルト 20 秒
probe timeout	TCP ハンドシェイク(および ACV)のタイムアウト時間(秒)を設定します。 デフォルト 10 秒
strikeout threshold	Equalizer がサーバを Down と認識するまでの失敗許容回数です。単位は回。 デフォルトは 3、設定可能範囲は 1~6 です。
probe delay	サーバヘルスチェックの間隔(秒)を設定します。 TCP ハンドシェイク(および ACV)はこの間隔行なわれます。 デフォルトは 10 秒です。 設定可能範囲は 0 秒から 60 秒までですが、5 秒以下を設定した場合には自動的に 5 秒間隔になります。
agent delay	VLB や Server Agent を使用したロードバランス時に設定が必要になります。 Equalizer がサーバ上の Agent を確認する間隔(秒)を設定します。 デフォルトは 10 秒、設定可能範囲は 1 ~60 秒です。
require agent response	Server Agent を使用した際にのみ設定します。 設定した場合に Server Agent からの応答がないと、サーバをダウンと判定します。
ICMP probe	ICMP によるヘルスチェックを行いません。 間隔の指定はできません、5 秒間隔で行なわれます。

### 3-1-3 “VLB”

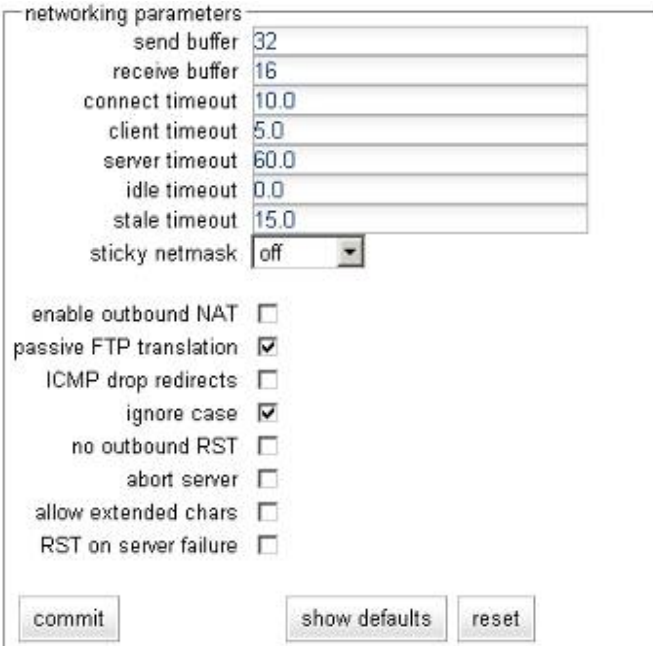
VLB を使用し負荷分散を行なう際に設定を行います。



項目	設定内容
URL	VMware API コネクション用の Virtual Center(または ESX サーバ上)の URL を設定します。 デフォルトでは https:// を使用し、 /sdk を指定します。 サンプルは上図をご参照下さい。
Username	VMware Virtual Center または ESX サーバへログインする際のユーザアカウントを指定します。
Password	VC User のパスワードを入力します。

### 3-1-4 “Networking”

ネットワークについての設定を行います。





項目	設定内容
send buffer	L7 での送信ソケットバッファサイズです。単位はキロバイト。デフォルトは 32KB です。最大値は 128 です。詳細は 3-1-4-1 を参照して下さい。
receive buffer	L7 での受信ソケットバッファサイズです。単位はキロバイト。デフォルトは 16KB です。最大値は 128 です。詳細は 3-1-4-1 を参照して下さい。
connect timeout	ACV によるヘルスチェックの接続要求に対するサーバ応答タイムアウト値(秒)です。デフォルトは 10 秒です、1~60 秒の範囲で設定が可能です。
client timeout	L7 クラスタのみ反映されます。クライアントのアイドル接続の終了までの時間です。単位は秒で、デフォルトは 5 秒です。設定値は 1.0 秒から設定可能です。
server timeout	L7 クラスタのみ反映されます。サーバのアイドル接続の終了までの時間です。単位は秒。デフォルトは 60 秒です。設定値は 1.0 秒から設定可能です。
idle timeout	L4 クラスタへの設定値で、アイドル状態にある TCP コネクションを Equalizer が切断するまでのタイムアウト時間を設定します。
stale timeout	L4 クラスタへの設定値で、ハーフオープン接続として存在している L4 接続をタイムアウトさせる設定時間(秒)になります。
sticky netmask	Sticky Persistence を使用時のアクセス IP に対するネットマスクの設定になります。デフォルトは「Off」です。クラスフルな設定になります。詳細は APPENDIX A を参照して下さい。
enable outbound NAT	Outbound NAT の有効・無効を設定可能です、これはデュアルネットワーク設定でのみ使用可能です。 有効にすると、Equalizer をゲートウェイとして Internal ネットワークの端末から External ネットワークへ通信する際、端末の送信元 IP アドレスを Equalizer の External 側 IP アドレスに NAT します。 無効の状態では送信元 IP アドレスは端末の IP アドレスのまま通信を行いません。詳細は 3-1-4-2 を参照して下さい。
passive FTP translation	passive FTP translation を有効にする場合チェックを入れて下さい。詳細は <a href="#">4-4-4</a> を参照して下さい。
ICMP drop redirects	Equalizer を経由する ICMP redirect メッセージを破棄します。
ignore case	チェックを入れ有効にすると、Match Rules での大文字・小文字の区別をしません。各クラスタ・各 Match Rule に対して設定する事も出来ます。 <b>(E250GX では使用しません)</b>

no outbound RST	チェックを入れ有効にすると、変換されない TCP RESET パケットを転送させないようにします。
abort server	クローズする際にサーバに対し不意に接続を落とします。
allow extended chars	URI やヘッダ内の ASCII や UTF-8 の透過設定です。デフォルトではチェックが外れて無効の状態です。
RST on server failure	L4 クラスタに適用されます。TCP セッションが確立した後に負荷分散先サーバがダウンした場合、クライアントに対して RST(リセット)パケットを送付します。

### 3-1-4-1 Send buffer/ Receive buffer について

L7クラスタではディレイドバインディングによるセッション管理が行なわれるため、バッファサイズを使用しデータを一時的に保持します。大きなファイルサイズ(1MB 以上など)をやり取りする場合は、バッファサイズがボトルネックになることがありますので、サイズを Send:Receive = 64:32 などのサイズに変更して下さい。

サイズが大きくなった場合、セッション毎にメモリが消費されます。セッション数が多い環境においてはメモリ容量が不足する場合があります、ご注意ください。

### 3-1-4-2 Outbound NAT通信について

デュアルネットワーク構成時、Internal セグメントから External セグメントへ通信を行なう際 Equalizer は IP アドレスの変換を行ないませんので、Internal セグメントのノードは自身の IP アドレスで通信を行なうことができます。しかしながら、External セグメントがグローバル IP セグメントである場合などでは、Outbound NAT を有効にすることで Equalizer が保持する External セグメントの IP アドレスへ NAT 変換することができます、こうすることで Internal セグメントのノードは External 側(およびその上位)セグメントへ通信を行なうことが可能になります。

デフォルトで Outbound NAT を有効にした状態では、Equalizer の External リアル IP アドレスに NAT 変換されるため、Equalizer を 2 台使用する冗長化構成の場合、どちらの機器が Primary 役として動作しているかによって、NAT される IP アドレスが変化してしまいます(冗長化については [5-1](#) を参照)。この場合、各サーバで Outbound NAT 設定を行うことで、NAT する IP アドレスを機器の External 側 IP アドレスではなく クラスタ IP アドレス や External 側の Failover Alias に設定が可能です。クラスタ IP アドレスは両機器で共有している IP アドレスであることから、どちらの機器が Primary 役であったとしても外部に通信する際の IP アドレスは共通になります。

通信するアプリケーションやサーバによっては必ず同一 IP アドレスで通信を行なう必要がある場合がありますので、そういった状況では各サーバで Outbound NAT を設定下さい。設定は各サーバのパラメータから行います、詳細は [4-8-4-2](#) をご確認ください。

### 3-1-4-3 “allow extended chars” 設定について

URI や HTTP ヘッダ上に 2 バイト文字が含まれるコンテンツでは、Equalizer 内で正常に処理ができず正常に表示されない場合があります、Equalizer ログに “parameter error” として表示されます。

上記の事象が発生した場合は、“allow extended chars” を有効にし、2 バイト文字を透過的に処理する設定を施すことでこの問題を回避することが可能です。

## 3-2 “Status” タブ設定

Equalizer の機器情報、クラスタ・サーバ情報、ログ情報などを確認します。



### 3-2-1 “Cluster Summary”







それぞれのクラスタ・および所属サーバの状況を確認できます。クラスタ名をクリックすると所属するサーバの状況が表示されます。

下図は L4クラスタ “Cluster\_Web\_2” をクリックした表示です。

Cluster_Web_2							
Servers	Status	Flags	Initial Weight	Current Weight	Processed	Active	Sticky
server_1	↑		Not used	Round Robin	0	0	0
server_2	↑		Not used	Round Robin	0	0	0

項目	内容
Servers	サーバ名を表示します。
Status	サーバ状態がアイコン表示されます。それぞれの意味については下記 Status アイコン表をご確認下さい。
Flags	サーバに設定されたフラグの状態が表示されます。
Initial Weight	サーバに設定された initial weight 値を表示します。Round Robin を負荷分散ポリシーとして選択した場合は Not used と表示されます。Round Robin および Static Weight 以外の、動的負荷分散ポリシーを選択した場合、現在の動的 Weight 値は Current Weight として表示されます。
Current Weight	サーバの動的 weight 値を表示します。Round Robin を負荷分散ポリシーとして選択した場合は Not used と表示されます。動的負荷分散ポリシーを選択している場合、この weight 値によってサーバへの振り分けが行われます。
Processed	完了したセッション数が表示されます。
Active	現在アクティブなセッション数が表示されます。

Sticky	Sticky によるセッション維持が行なわれているユーザ数を表示します。
--------	--------------------------------------

Status アイコン	内容
	ヘルスチェックに成功し、サーバはアップしています。
	ヘルスチェックに失敗し、サーバはダウンしています。
	ヘルスチェックに成功していますが、サーバのWeight値が0に設定されているか、 <a href="#">quiesce設定</a> が有効になっています。
	ヘルスチェックに失敗しており、また、サーバのWeight値が0に設定されているか、 <a href="#">quiesce設定</a> が有効になっています。
	<a href="#">hot spare設定</a> が有効になっています。
	該当サーバに対するヘルスチェックが無効に設定され、サーバのステータスを確認することが出来ない状態です。

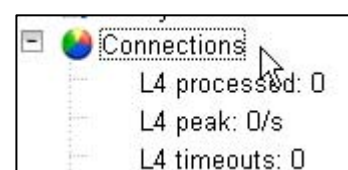
また、L7クラスタの表示項目は以下のようになります。

clst_123						
Servers	Status	Flags	Initial Weight	Current Weight	Processed	Active
sv161			Not used	Round Robin	0	0
sv162			Not used	Round Robin	0	0

### 3-2-2 “Statistics”

サービス全体の統計情報を確認することが出来ます。

この画面へは左フレームの“Connections”を選択しても移動することが可能です(右図参照)



確認できる情報は大きく Basic Statistics と Advanced Statistics に分けられます。

Basic Statistics	
L4 total connections processed	0
L4 peak connections processed	53 per second
L4 stale connections timed-out	0
L4 idle connections timed-out	0
L7 current active connections	0
L7 total connections processed	13817
L7 peak connections processed	40

項目	内容
L4 total connections processed	L4クラスタで処理されたコネクション数の総数です。
L4 peak connections processed	L4クラスタで1秒間で処理された最大のコネクション数です。
L4 connections timed-out	L4クラスタでタイムアウトしたコネクションの数です。
Envoy status	E650GX のみ表示されます。
L7 current active connections	L7クラスタに於いて、現在アクティブなコネクション数です。
L7 total connections processed	L7クラスタで処理されたコネクション数の総数です。
L7 peak connections processed	L7クラスタで1秒間に処理された最大のコネクション数です。

Advanced Statistics	
L7 client connections acceptable	0
L7 connections timed out	0
L7 request bytes from clients	0
L7 response bytes to clients	0
L7 complete requests	0
L7 min. usec to complete request	0
L7 max. usec to complete request	0
L7 avg. usec to complete request	0
L7 maximum headers exceeded by client	0
L7 total client connections	0
L7 current client connections	0
L7 requests processed	0
L7 responses processed	0
L7 server conx reused	0
L7 cookies stuffed	0
requests in error	0
L7 responses in error	0
L7 client request timeouts	0
L7 server connect timeouts	0
server response timeouts	0
L7 avg. usec to connect to server	0

項目	内容
L7 client connections acceptable	開始された L7コネクション数です。
L7 connections timed out	Client timeout 値、Connect timeout 値、Server timeout 値等を過ぎたことでタイムアウトした L7コネクション数です。
L7 request bytes from client	クライアントから受け取ったデータをバイト数で表示します。
L7 response bytes to client	サーバから受け取ったデータをバイト数で表示します。
L7 complete requests	L7クラスタで完了したクライアントリクエスト数を表示します (Client timeout 値に達する前に処理したリクエスト)
L7 min. usec to complete request	クライアントリクエストの受付完了までにかかった最小時間をマイクロ秒で表示します。
L7 max. usec to complete request	クライアントリクエストの受付完了までにかかった最大時間をマイクロ秒で表示します。

L7 avg. usec to complete request	クライアントリクエストの受付完了までにかかった平均時間をマイクロ秒で表示します。
L7 maximum headers exceeded by client	Equalizer がサポートする最大64ヘッダを超えた L7クライアントリクエスト数を表示します(Equalizer は64ヘッダを超えたクライアントリクエストはドロップします)
L7 total client connections	受け付けた L7クライアントコネクション数を表示します(必ずしも完了した(Processed)コネクションではありません)
L7 current client connections	現在のアクティブな L7コネクション総数を表示します。
L7 request processed	完了した L7クライアントリクエスト総数を表示します。
L7 response processed	完了した L7サーバレスポンス総数を表示します。
L7 server conx refused	クローズせず、再度 Equalizer で利用されたサーバーコネクション数を表示します。
L7 cookies stuffed	Equalizer が L7パケットにセッション維持用 Cookie を付与した回数を表示します。
requests in error	エラーが発生した L7リクエストの総数を表示します。
L7 responses in error	エラーが発生した L7レスポンスの総数を表示します。
L7 client requests timeouts	Client timeout 値に達したためドロップされた L7リクエスト総数を表示します。
L7 server connect timeouts	Connect timeout 値に達したためドロップされた L7リクエスト総数を表示します。
server response timeouts	Server timeout 値に達したためドロップされた L7リクエスト総数を表示します。
L7 avg. used to connect to server	Equalizer がサーバへのコネクション確立に要する平均時間(秒)

### 3-2-3 “Event Log”

Equalizer のログ情報を確認する事が出来ます。 ログは大きく3種類に分かれています。

- equalizer  
 負荷分散、ヘルスチェック、Failover 等、サービスに関するログが表示されます。
- operating system  
 Equalizer の内部 OS ログ、NTP、ポート状態などのログが表示されます。
- クラスタ別ログ  
 Equalizer Log から、指定したクラスタのログを抜粋して表示します。

max lines:  log type:  Refresh

```

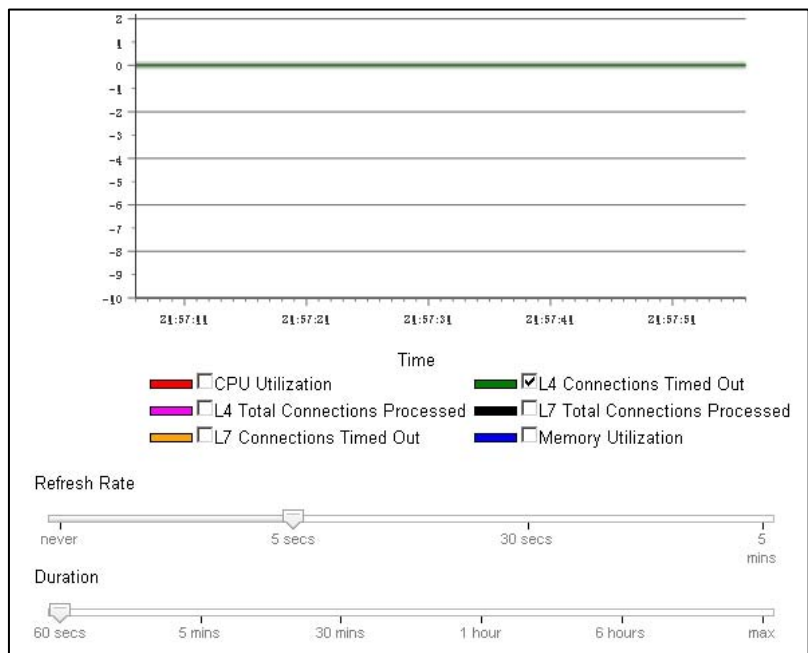
Sep 29 03:41:01!envoyadm equalizer daemon no
Sep 29 03:41:11!envoyadm equalizer-Cluster-1 daemon no
Sep 29 03:41:21!envoyadm equalizer-Cluster-2 daemon no
Sep 29 03:41:31!envoyadm operating system daemon no
  
```

項目	内容
max lines	ボックス内に表示するログの行数を指定します。 デフォルト20行、最大1000行まで指定が可能。
log type	equalizer, operating system, クラスタ別ログから種類を指定します。
Refresh	ログを最新の状態に更新します。

ボックス内に表示されたログは、テキストとしてコピーすることが可能です。 サポートなどでログ採取を行なう場合には、こちらから行って下さい。

### 3-2-4 “Plot”

Equalizer の状態をグラフ表示します。



項目	内容
CPU Utilization	CPU 使用率を表示します。
L4 Connections Timed Out	タイムアウトした L4接続数を表示します。



L4 Total Connections Processed	処理された L4コネクション数を表示します(全 L4 クラスタ合計)
L7 Total Connections Processed	処理された L7コネクション数を表示します(全 L7クラスタ合計)
L7 Connections Timed Out	タイムアウトした L7コネクション数を表示します。
Memory Utilization	メモリ使用率を表示します。
Refresh Rate	更新する間隔を設定します。
Duration	表示する時間の範囲を選択します。

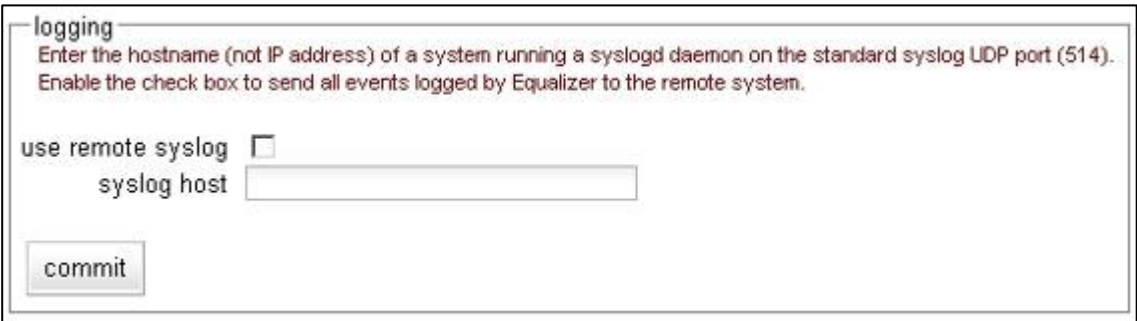
### 3-3 “Monitoring” タブ設定

Equalizer による監視・トラップ設定を行います。



#### 3-3-1 “Events”

##### 3-3-1-1 “logging”

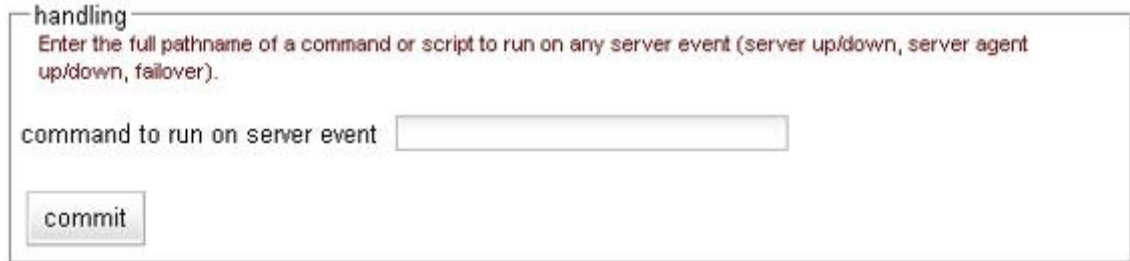


Logging 設定では、Equalizer のログを Syslog サーバへ出力する場合に設定します。Syslog サーバへの通信は UDP/514 ポートにて行なわれます。

“use remote syslog” にチェックを入れ、“syslog host” に Syslog サーバの IP アドレスを入力します。

**注意： ファシリティ設定、メッセージレベル設定は行うことができません。**

##### 3-3-1-2 “handling”



Handling 設定は、イベント発生時に入力されたコマンドやシェルを実行します。サポート外項目になりますので、詳細は英文マニュアルをご参照下さい。

### 3-3-1-3 “email notification”

email notification

Enter from and to addresses in "user@example.com" or "<user@example.com>" format. The SMTP server can be specified as an IP address or hostname. Enable the check box to send email on any server event.

enable email notification

from

to

SMTP server

Email Notification は、イベント発生時にアラートメールを送付します。

項目	内容
enable email notification	メール送付設定を有効にします。
from	メールを送付の際に使用する From アドレスを指定します。SMTP サーバのセキュリティなどに問題がなければ特に制限なく指定可能です。
to	メールの送付先アドレスです、複数の宛て先を指定する場合はメールアドレスを “<” “>” で囲み、メールアドレスの間にスペースを入れて下さい。 例： <first@email.com> <second@email.com>
SMTP server	使用する SMTP サーバを指定します。Equalizer に DNS 設定がある場合はドメインによる指定も可能です。

メールが送付されるイベントは大きく分けて以下の 2 種類です

- サーバのヘルスチェックが失敗した時、また再度成功した時
- Failover が発生した時

### 3-3-2 “Export to CSV”

export to csv

Create a comma separated value (CSV) file containing the data used by Equalizer to plot cluster and server histories.  
 Note: Exported file size may be large when a long time period is selected.

time period:

クラスタの統計データおよびサーバヒストリを含む稼動統計、また機器の統計を5秒間隔で出力することができます。出力する時間は Time Period から指定することが出来、直近5分間から保存している全てのデータまで範囲の指定が可能です。

#### クラスタ・サーバ統計

項目	内容
Delay	サーバの平均サービスタイム。 サービスタイムとはクライアントリクエストをうけてから、サーバがリプライパケットを送信開始するのにかかる時間です。
Agent	サーバから返すサーバエージェント値の平均 (※負荷分散 Policy として Server Agent を使用していない場合は関係ございません)
Connections	サーバのアクティブコネクションの平均数
Load	サーバ負荷。
Total	サーバにより処理されたコネクション総数
Time	サーバのアップタイム
Weight	サーバの Weight 値

#### 機器情報統計

項目	内容
Total Connections Processed	処理されたコネクションの総数
Peak Connections Processed	1 秒あたりに処理された最大のコネクション数
Connections over last sec	最後の 1 秒間に処理されたコネクション数
Connections Timed Out	コネクションタイムアウト値を超え、ドロップされたコネクション数
CPU Utilization	使用されている CPU 容量のパーセンテージ

## 3-4 “Permissions” タブ設定



### 3-4-1 “Users”

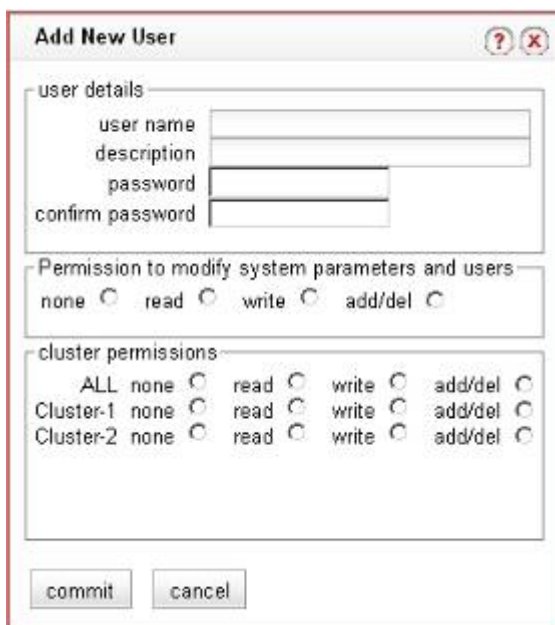
Web管理画面へのログインアカウントを管理します。 [1-2-4](#) で作成したアカウントはこちらで表示され管理することが可能です。

管理できる内容は以下のようになっております

- ・ アカウントの作成・削除
- ・ パスワードの変更
- ・ 権限(グローバル・各クラスタ)の変更

#### 3-4-1-1 ユーザアカウントの追加

ユーザテーブルの最下部にある  ボタンを押すと、以下のようなアカウント登録ウィザードが表示されます。



「user details」の項目では、作成するアカウント情報を入力します。

- user name  
アカウント名を入力します。
- description  
[1-2-4](#) の enter fullnameと同一項目です、アカウントの詳細を任意で入力します。
- password / confirm password  
アカウントに対するパスワードを入力します。

「Permission to modify system parameters and users」ではグローバル設定画面に対しての権限設定を行います。また「cluster permissions」では全体クラスタ(ALL) または 各クラスタ設定(各クラスタ名)に対する権限の設定を行います。

権限の内容は以下をご参照下さい。

権限	内容
none	アクセスする権限がありません。 グローバル設定を確認することは出来なくなり、各クラスタが Web 管理画面上に表示されなくなります。
read	グローバル設定・各クラスタ設定を読み取ることが可能です、変更する権限はありません。
write	グローバル設定・各クラスタ設定を読み取り・変更することが可能です。 新規作成(クラスタなど)を行なうことは出来ません。
add/del	グローバル設定・各クラスタ設定に対し、全ての権限を保持します。

#### クラスタ権限の設定例)

```

cluster permissions
  ALL none  read  write  add/del 
Cluster-1 none  read  write  add/del 
Cluster-2 none  read  write  add/del 
  
```

左の例では、Cluster-1 に対しては全ての権限がありますが、それ以外のクラスタについては ALL の設定が有効ですので、読み取り専用となります。

### 3-4-1-2 ユーザアカウント設定の変更

ユーザアカウントのパスワードや権限を変更する為には、write 以上の権限を持ったユーザによってのみ行なうことが可能です。

ユーザテーブルの Action の欄から  ボタンを選択すると変更ウィンドウが表示されますので、変更を行って下さい。

### 3-4-1-3 ユーザアカウントの削除

ユーザアカウントを削除する場合は、グローバル設定に add/del の権限を持ったユーザが削除

を行なうことが可能です。

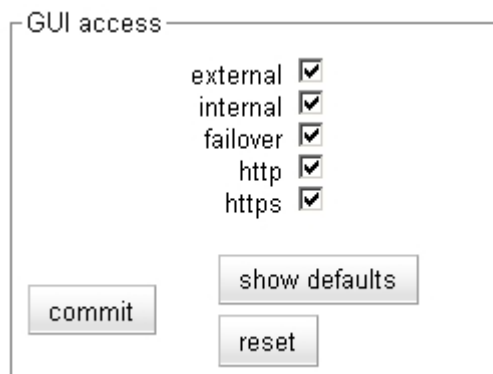
ユーザテーブルの Action の欄から  ボタンを選択すると変更ウィンドウが表示されますので、変更を行って下さい。

### 3-4-2 “GUI Access”

Equalizer の Web 管理画面へアクセス制御を行なうことが出来ます。

インターフェース項目としてはExternal, Internal, Failover の3種類があり、チェックを外すことで該当するインターフェースからのアクセスを禁止します。Failoverは冗長化構成のときのみ使用できるものです([5-3-4-1](#)を参照下さい)

Web 管理画面へはHTTPまたはHTTPSでのログインが可能です。それぞれのチェックを外すことでアクセスを禁止することが可能です。



GUI access

- external
- internal
- failover
- http
- https

commit      show defaults

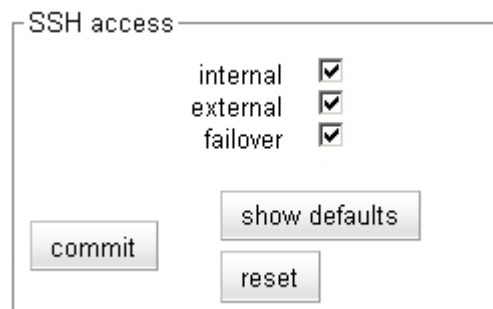
                  reset

**注意： 現在アクセスしているインターフェース/プロトコルを禁止することは出来ませんので、禁止設定は必ず別のインターフェース/プロトコルから行う必要があります。**

### 3-4-3 “SSH Access”

Equalizer への SSH アクセス制御設定が出来ます。

インターフェース項目としてはExternal, Internal, Failover の3種類があり、チェックを外すことで該当するインターフェースからのアクセスを禁止します。Failoverは冗長化構成のときのみ使用できるものです([5-3-4-1](#)を参照下さい)



SSH access

- internal
- external
- failover

commit      show defaults

                  reset

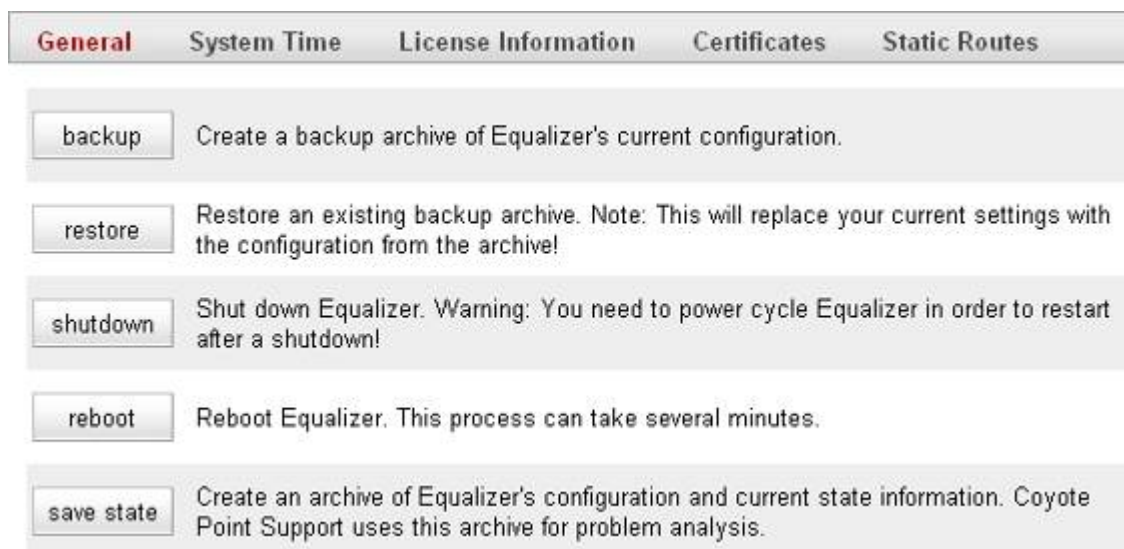
## 3-5 “Maintenance” タブ設定



このタブでは機器の設定・管理について設定を行います。

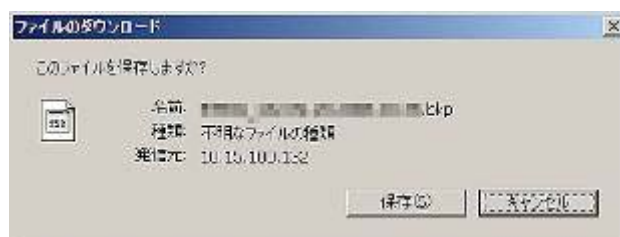
### 3-5-1 “General”

General のセクションでは、機器のシャットダウン・リブートやコンフィグに関する運用管理を行います。



#### 3-5-1-1 “backup”

Equalizer の設定コンフィグ(バックアップファイル)を保存します。 ボタンを押すと以下のようなウィンドウ(ブラウザの種類により異なります)が表示されますので、アクセス端末に保存して下さい。





ファイル名はお客様の設定や取得した日時により異なります。

形式は [Hostname]-[MM].[DD].[YYYY]-[HH].[MM].bkp となります。

例) Equalizer1-09.20.2008-10.50.bkp

上記はホスト名(1-2-1を参照)“Equalizer1”の機器上で

2008年9月20日 10時50分に取得されたバックアップファイルです。

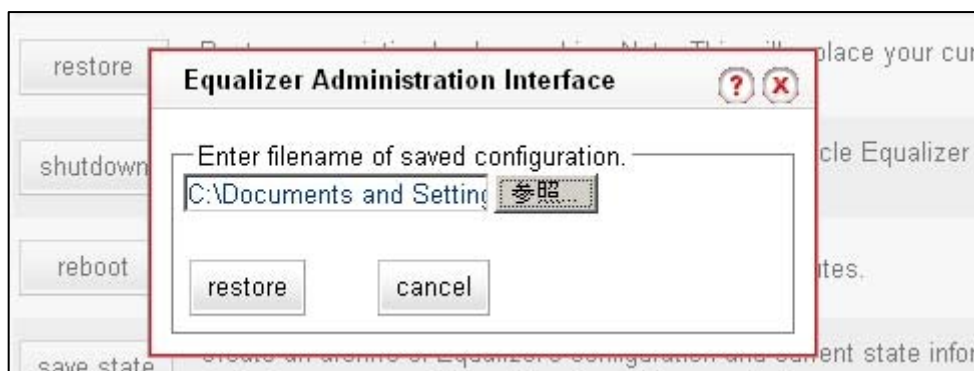
**注意:** 設定を変更した場合は必ずバックアップファイルを新規で保存して下さい。機器故障により交換した場合は、バックアップファイルがないと復旧させることが出来なくなります。

**注意:** 冗長化構成の場合は、両機器からバックアップファイルを取得して下さい。IPアドレスなどの情報も含まれるため、冗長構成であったとしても両機器には差異があります。

### 3-5-1-2 “restore”

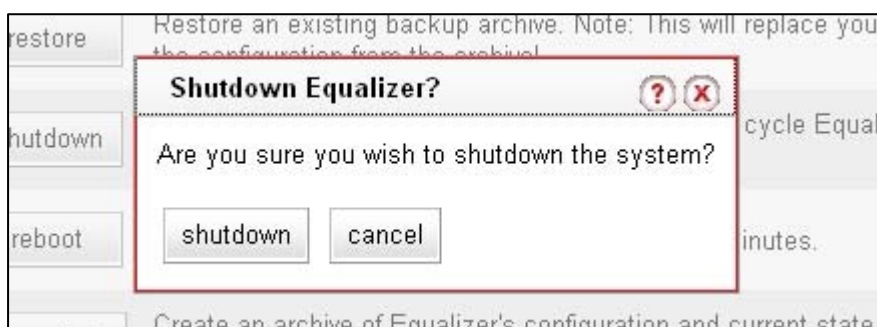
Equalizer に対して、3-5-1-1 で取得したバックアップファイルをリストアする際に使用します。リストアすると機器は再起動し、リストアしたコンフィグにて起動します。

ボタンを選択すると下図のウィンドウが表示されますので、ファイルを端末から選択して下さい。



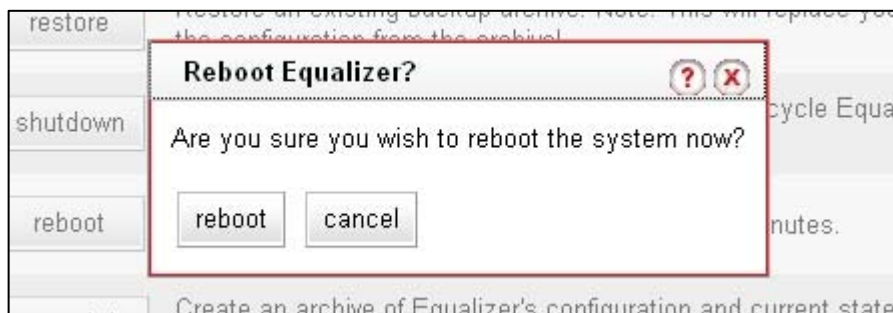
### 3-5-1-3 “shutdown”

Equalizer の電源を切る際は、Shutdown をまず行なう必要があります。ボタンを選択すると、下図の確認メッセージが表示されますので、shutdown を再度選択すると実行されます。



### 3-5-1-4 “reboot”

Equalizer を再起動させる場合はこちらから行ないます。 ボタンを選択すると下図のメッセージが表示されますので、reboot を再度選択すると reboot を行ないます。

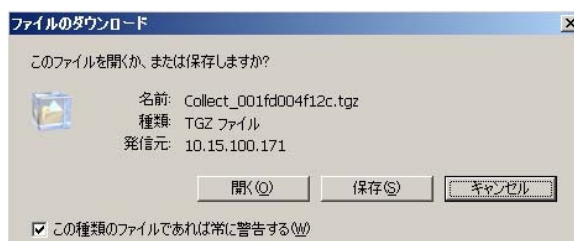


決定すると、再起動が完了するまで下記のウィンドウが表示されます。完了するとウィンドウは自動的に閉じられます。



### 3-5-1-5 “save state”

Equalizer の機器の状態を一括でダウンロードすることができます。 ヘルプデスク等にご連絡頂いた場合などではこちらのファイルを取得するご依頼をさせて頂く事がございます。 このボタンを押すと以下のようなウィンドウ(ブラウザの種類により異なります)が表示されますので、アクセス端末に保存して下さい(ファイル名は “Collect\_[機器の SystemID].tgz”)。



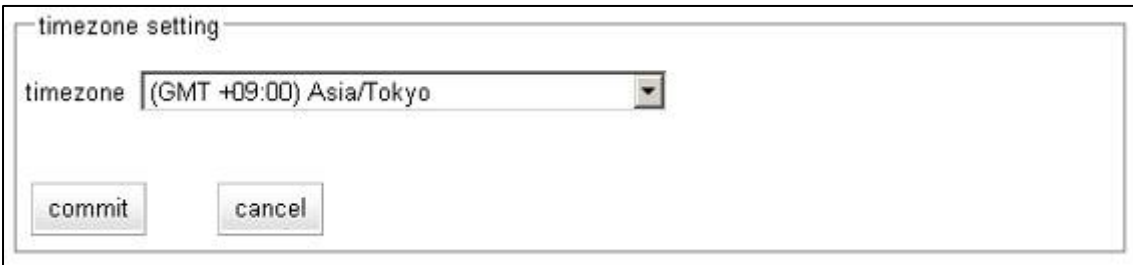
取得できるデータにはコンフィグやログなどのデータが含まれておりますが、リストア時に使用することは出来ません。コンフィグの保存は 3-4-1-1 に沿って行なって下さい。

**注意：ファイル取得時には、一時的ではありますが CPU 使用率が上昇します。可能であれば、サービスへのアクセスが少ない時間に行なって頂くことが推奨されております。**

## 3-5-2 “System Time”

機器の現在時刻、タイムゾーン、および NTP サーバの設定を行います。

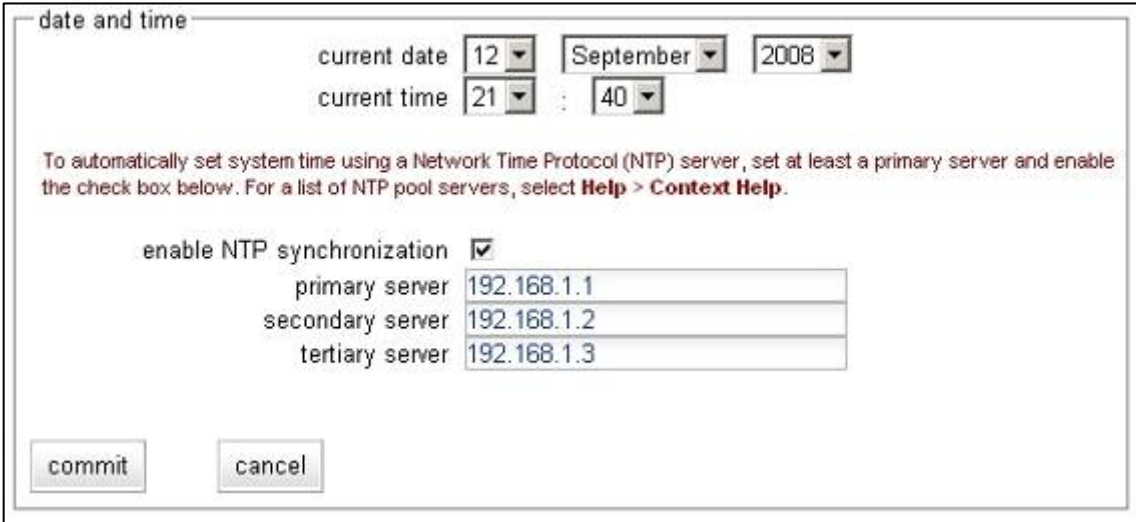
### 3-5-2-1 “timezone setting”



「timezone setting」のセクションでは、機器のタイムゾーンを設定することができます。

### 3-5-2-2 “date and time”

「date and time」のセクションでは日時設定 および NTP 設定を行うことができます。NTP は 3 つまで登録が可能です。commit ボタンを押すと reboot の実行を求められますので、実行します。再起動後、時刻の設定および NTP 設定は有効になります。



追記：時刻の設定のみであれば、再起動せずに行うことが可能です。時刻を設定変更後、commit ボタンを押します。reboot 実行の確認メッセージが表示されますが、ここで cancel を選択すると、時刻の設定は変更されます。

### 3-5-3 “License Information”

Equalizer の負荷分散機能を使用するためにはライセンスを取得する必要があります。弊社から出荷された Equalizer はライセンスが取得された状態になっており、再度ライセンスを取得頂く必要は通常ございません(ファームウェアのアップグレード時など、ライセンスを再度確認する必要が発生する場合がございます)。

ライセンスの取得・確認はインターネット経由でメーカーのライセンスサーバへ通信することで行なわれます、使用するポート番号は TCP/80 番になります。

#### 3-5-3-1 “license information”

```
license information
                product  e250
servers per cluster  16
supported clusters  64
                serial no.  [REDACTED]
                system ID  [REDACTED]
```

Please register your Equalizer using the link below, before using either the Online License or Offline License tabs to license Equalizer.

[www.coyotepoint.com/register.htm](http://www.coyotepoint.com/register.htm)

ライセンスが正常に取得・認識されている機器では、上記のようにシリアル番号などの情報が表示されます。ライセンスが正常に取得または認識されていない場合は、下記のように “unlicensed” と表示されます。

```
license information
                product  **unlicensed
                system ID  [REDACTED]
```

Please register your Equalizer using the link below, before using either the Online License or Offline License tabs to license Equalizer.

[www.coyotepoint.com/register.htm](http://www.coyotepoint.com/register.htm)

注意：ライセンスが取得・認識できていない Equalizer では負荷分散の機能を使用することが出来ません。製品を正常に使用するには、ライセンスが必要になります。

### 3-5-3-2 “Offline License”

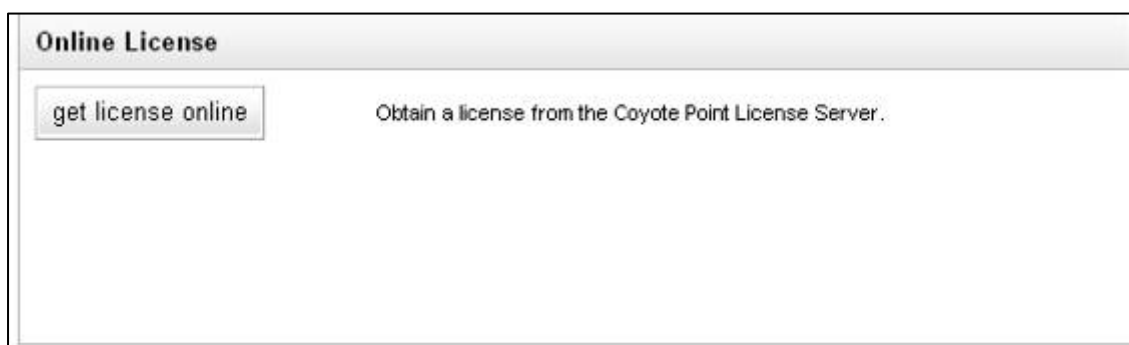


ライセンスを取得するには、通常インターネット経由でライセンスサーバにアクセスする必要がありますが(3-5-3-3 参照)、オフライン環境の場合は、Offline License 申請を行なうことでライセンス申請を行なう事が可能です。

上図の“create license request file”を選択すると、申請ファイルを端末に保存することができます。こちらのファイルを弊社 TEC-World 宛にご送付下さい(インシデント消費はございません)。

メーカーより発行されたライセンスファイルをインストールするには、上図の“install signed license file”を選択し、ライセンスファイルを選択します。機器の再起動を行う旨メッセージが表示されますので、決定します。再起動後、ライセンスファイルが正常に取得できたかを 3-5-3-1 からご確認下さい。

### 3-5-3-3 “Online License”



インターネット経由でライセンスを取得するには、上図“get license online”を選択します。Equalizer はポート 80 番を使用しライセンスサーバへアクセスを行ないます。正常に取得できた場合は、再起動を行う旨メッセージが表示されますので、決定します。再起動後、ライセンスファイルが正常に取得できたかを 3-5-3-1 からご確認下さい。

### 3-5-4 “Certificates”

EqualizerのWeb管理画面へアクセスする際にSSLサーバ証明書を使用する場合、こちらから証明書のアップロードを行なうことができます。サーバ証明書を申請するためのCSRの作成方法などの手順については [こちらの資料](#)をご参照下さい。

select SSL certificate file

Upload a certificate for the Equalizer Administration Interface. Clients use this certificate to authenticate a connection with the interface. The certificate file must be in PEM (.pem) or PKCS12 (.pfx) format, and must contain the private key and the entire certificate chain.

**注意：** サービス用のサーバ証明書とは別になります。SSLでサービスを行なう際は、別途クラスタ毎にサーバ証明書のインストールが必要になります。詳細につきましては [4-6-1](#) をご参照下さい。

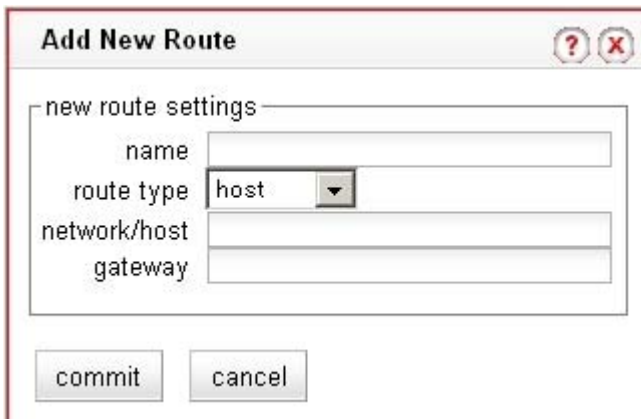
### 3-5-5 “Static Routes”


スタティックルートの設定・変更・削除を行います。

Use this table to define static routes on Equalizer. This is usually necessary only when a client or server is not on the same subnet as Equalizer's external or internal interfaces.

Name	Type	Network/Host	Gateway	Actions
192segment	-net	192.168.1/24	10.15.100.5	<input type="button" value="trash"/> <input type="button" value="wrench"/>
				<input type="button" value="plus"/>


### 3-5-5-1 スタティックルートの追加




スタティックルートを追加するにはルートテーブル画面から  を選択します。上記のウィンドウが表示されますので、パラメータを記載します。

- name  
作成するルートに名称を設定します。  
例)route1 route2
- route type  
ネットワークを設定するには network 、ホストを設定するには host を選択します。
- network/host  
あて先ネットワーク/ホストを指定します。  
例)192.168.1/24 , 10.10/16 , 192.168.1.100/32
- gateway  
宛先のゲートウェイアドレスを指定します。  
例)172.16.100.1, 10.10.50.1

### 3-5-5-2 スタティックルートの変更

作成したスタティックルート情報を変更するにはルートテーブル画面から  を選択します。3-5-5-1 と同様のウィンドウが表示されますので、設定を変更し、決定します。

### 3-5-5-3 スタティックルートの削除

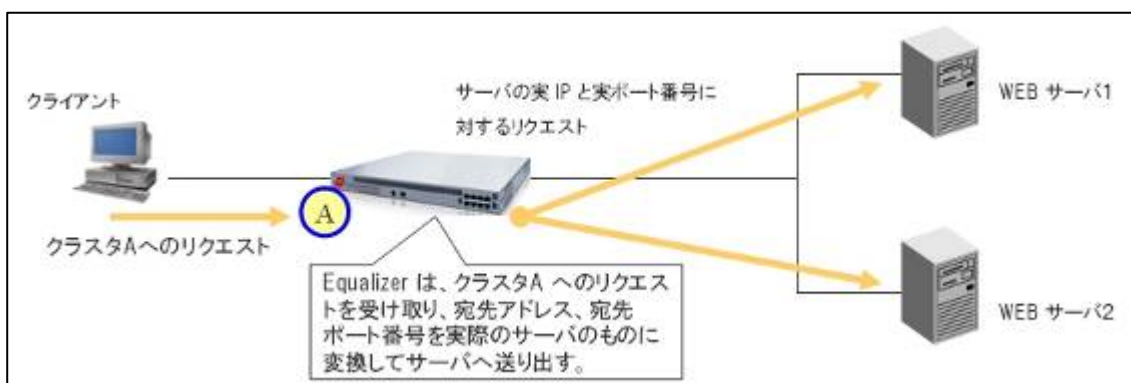
作成したスタティックルート情報を削除するにはルートテーブル画面から  を選択します。確認のウィンドウが表示されますので、決定を選択するとルート情報は削除されます。

## セクション4 クラスタ・サーバ設定手順

### 4-1 クラスタ と サーバの関係

このセクションでは、サービスを提供するために必要なクラスタ、およびクラスタに所属するサーバについて、その設定手順を説明致します。

#### 4-1-1 クラスタの定義について



Equalizer で実際のサービスを行なう IP アドレスは、Equalizer のリアル IP アドレスではなく別途作成される仮想 IP アドレスです。この**仮想 IP アドレス (Virtual IP, VIP)** に受け付ける**ポート番号**を組み合わせたものが**クラスタ**と呼ばれます(上図参照)。

**注意:** クラスタ IP アドレスに到達した通信でも、クラスタのポート番号とリクエストのポート番号が違う場合 Equalizer は通信を受け付けません。

#### 4-1-2 サーバの定義について

クラスタの IP アドレス・ポート番号に到達した通信は、実際に**サービスを提供するサーバ**に割り振られます。Equalizer ではサーバは各クラスタに所属していますので、各クラスタに対してサーバ追加を行う設定になります。

**注意:** 別クラスタで受け付けた通信を同一サーバに振り分ける場合は、クラスタを複数作成し、各クラスタに同じサーバを所属させます。



### 4-1-3 サーバに対するEqualizerの監視について

Equalizer はサービスを継続して行なう為に、サーバに対してヘルスチェック(死活監視)を行ないます。ヘルスチェックに失敗したサーバは「ダウン」とみなされ、リクエストの振り分けは行なわれません。

### 4-1-4 Equalizerを通過する通信について

4-1-1 で、クラスタに到達した通信は所属するサーバに割り振られるという説明がありましたが、クラスタ IP アドレス、Equalizer のリアル IP アドレス、Failover Alias IP アドレス以外に対する通信については、Equalizer はルーティング処理を行ない処理します。従って、デュアルネットワーク構成(4-2 参照)においても Equalizer 上位・下位をまたぐ通信が可能になります。

### 4-1-5 サーバのデフォルトゲートウェイについて

Equalizer を使用する際に、負荷分散対象サーバのデフォルトゲートウェイは Equalizer のリアル IP アドレスを指定します。これは、Equalizer が負荷分散通信を行なう際に IP アドレスを NAT している為です、この NAT された IP アドレスを再変換するためにサーバからの応答通信は Equalizer へ戻される必要があります(4-1-6 も併せてご確認ください)。

冗長化構成の場合は、2台のEqualizerが共有するFailover Aliasをゲートウェイとして設定します(5-2-6)。

### 4-1-6 spoof設定について(SNAT設定)

4-1-5 のように負荷分散サーバのデフォルトゲートウェイは通常 Equalizer に向ける必要がありますが、spoof の設定を変更することで別の機器をデフォルトゲートウェイとして設定し、かつ負荷分散通信も行うことが可能になります。

#### 4-1-6-1 spoofとは

spoofは各クラスタに個別で行なう設定で、機器全体に対する設定ではありません。デフォルトは有効になっていますが、無効にすることでEqualizerはSNAT(Source NAT) の動作をします。設定箇所については [4-4-1-1](#)、[4-5-1-1](#) をご参照ください。

SNAT 動作を行なうと、クライアントからの通信を Equalizer がサーバに振り分ける際に、クライアントの送信元 IP アドレスを Equalizer のリアル IP アドレスに NAT 変換します。

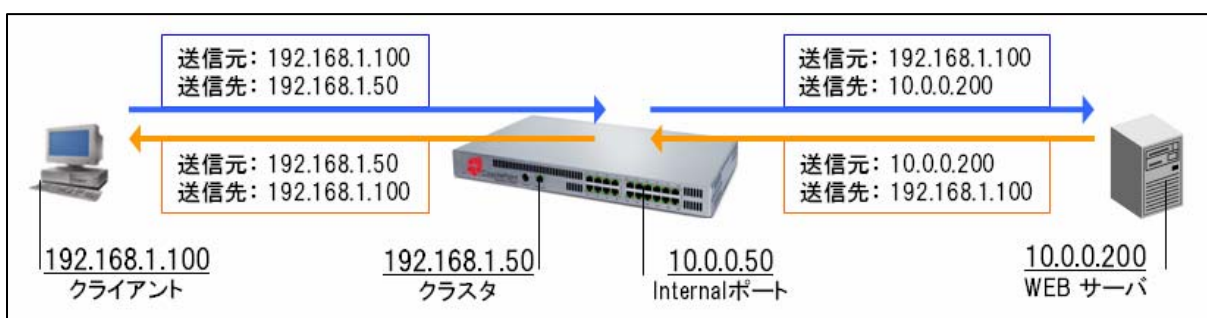
spoof 設定と SNAT 動作の関係については以下の表をご参照下さい。

spoof 設定	SNAT 動作
有効(デフォルト)	しない
無効	する

## 4-1-6-2 SNAT(Source NAT)の動作

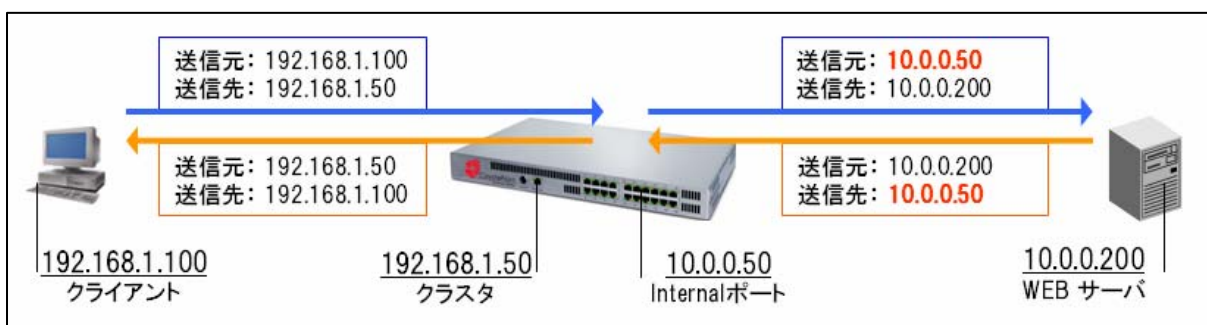
デュアル・シングル両ネットワーク構成において、SNAT の動作がどのように行なわれるのか、以下の図で解説します。

### ■デュアルネットワーク構成、spoof 有効(SNAT 無効)の状態



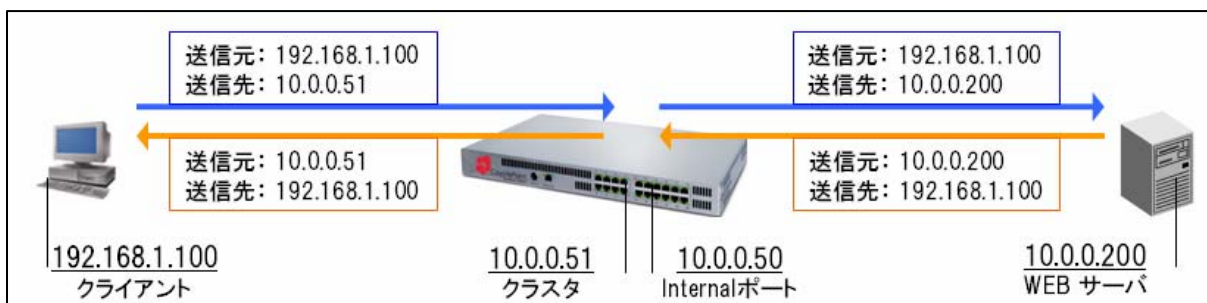
Equalizer はクライアントのリクエストを受け付け、送信先 IP アドレスをサーバの IP アドレスに変換し通信をおこないます。しかし送信元 IP アドレスは変換せず、クライアントの IP アドレスがそのままサーバへ到達しています。

### ■デュアルネットワーク構成、spoof 無効(SNAT 有効)の状態

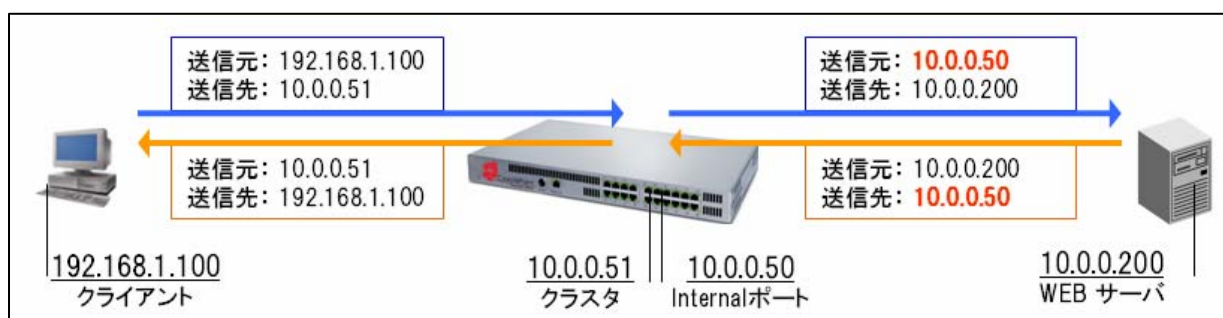


Equalizer がサーバへ通信を行なう際、送信元 IP アドレスを Equalizer のリアル IP アドレスへ変換 (NAT)していることが分かります。

### ■シングルネットワーク構成、spoof 有効(SNAT 無効)の状態



■シングルネットワーク構成、spoof 無効(SNAT 有効)の状態



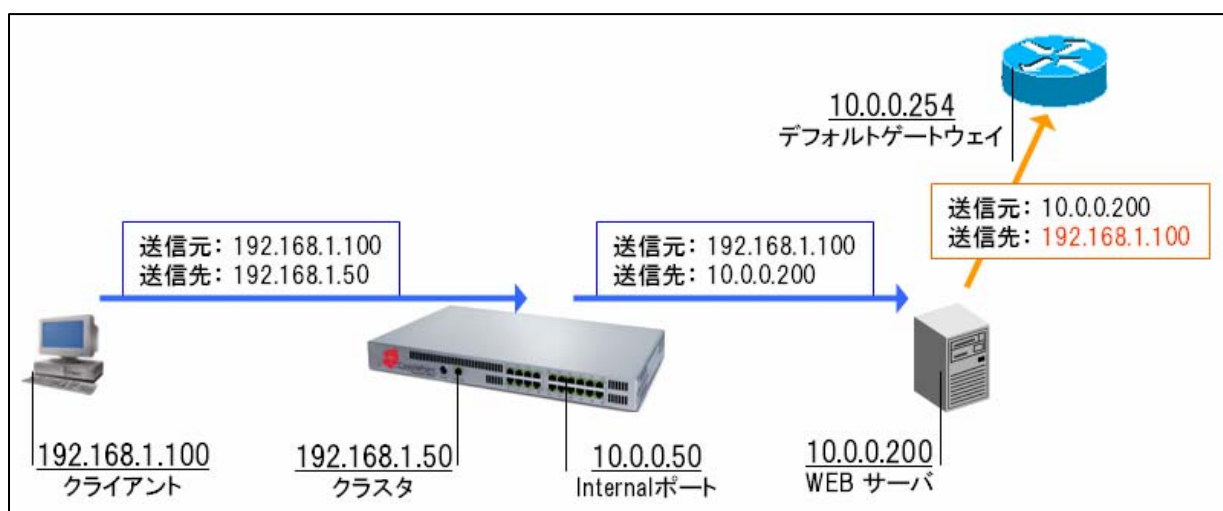
上記例のように、spoof を無効にし SNAT 動作を行なうことで、サーバへのアクセスは全て Equalizer のリアル IP アドレスから行なわれるようになります。

### 4-1-6-3 なぜSNATを使用するのか

4-1-5 では、通常サーバのデフォルトゲートウェイは Equalizer へ指定し、Equalizer へ通信を戻す理由について説明致しましたが、ネットワーク環境などによってはサーバのデフォルトゲートウェイを Equalizer 以外の機器に向ける必要があるケースがあります。

このようなケースでは spoof を無効(SNAT を使用)にし、サーバへのアクセスは必ず同一セグメントである Equalizer から行なうようにします。同一セグメント内の通信になるため、サーバはデフォルトゲートウェイを使用せずに応答通信を Equalizer へ戻すことが可能になり、負荷分散の通信が確立します。

下記図では、サーバのデフォルトゲートウェイが Equalizer 以外に向いているため、他セグメントである 192.168.1.100 から到達したリクエストはデフォルトゲートウェイに向かって送信されています。このような状況では SNAT を使用することで、通信を正常に行うことが可能になります。



#### 4-1-6-4 SNATのデメリット

4-1-6-3 のように、SNAT を使用することでサーバのデフォルトゲートウェイを意識せずに通信を行なうことが可能ですが、全アクセスの送信元 IP アドレスが Equalizer のリアル IP アドレスになります。サーバで送信元 IP のログ収集を行なうことが出来なくなりますので注意が必要です。この問題を解決するため、Equalizer は X-Forwarded-For ヘッダを追加する機能を備えています。詳細は 4-1-6-5 をご確認ください。

また Equalizer を冗長化構成で使用している場合は、Primary 役として処理を行なっている Equalizer の IP アドレスが送信元 IP アドレスになります。

#### 4-1-6-5 “X-Forwarded-For” ヘッダ追加について

L7/HTTP、L7/HTTPS クラスタを使用した場合、Equalizer がクライアントリクエストをサーバへ振り分ける際にクライアントの送信元 IP アドレスを X-Forwarded-For ヘッダとして追加することが可能です。サーバで X-Forwarded-For ヘッダを確認することで、クライアントの送信元 IP アドレスを取得することが可能になります。設定方法は [4-5-1-5](#) をご確認ください。

#### 4-1-7 ポート変換機能について

通常では、クラスタが受け付けるポート番号とサーバが受け付けるポート番号は同じです。例えば、TCP/80 番でサービスを提供しているクラスタに所属するサーバのポート番号は、同じく TCP/80 番になっています。

Equalizer ではポートリダイレクション機能が提供されていて、サーバのポート番号をクラスタとは別に設定することが可能です。以下の設定ではサービスの提供は TCP/80 番で行なっていますが、Equalizer とサーバ間の通信は TCP/8080 番で行なっています。

##### ■クラスタ “Cluster\_Web” (ポート: TCP/80)

サーバ1:192.168.1.10 (ポート:TCP/8080)

サーバ2:192.168.1.11 (ポート:TCP/8080)

Equalizer は自動的にポートを変換しています。この設定はサーバを作成する際に(4-8 参照)ポート番号を指定するだけで行なうことができます。サーバ作成後は、サーバのポート番号に対して TCPヘルスチェックが開始されます。

サーバのポート番号とは別のポート番号を使用してヘルスチェックを行ないたい場合は、[4-8-3](#) の probe port 設定を行ってください。

#### 4-1-8 HTTPSクラスタの動作について

HTTPSクラスタを使用した場合、SSL通信をクラスタで受け付け処理することが可能になります。HTTPSクラスタにはSSLサーバ証明書がインストールされており(4-6-1を参照) SSLの複号処理を行なった後、サーバに対してはHTTP通信を行ないます。

サーバからの戻り通信は、Equalizer まで HTTP 通信で行なわれた後、Equalizer が再度 SSL 暗号処理を行い、クライアントに対して通信を行ないます。この動作によって、クライアントと Equalizer の間はセキュアなコネクションが保たれます。



補足： HTTPSクラスタ作成時のデフォルトポート番号は443、HTTPSクラスタのサーバデフォルトポート番号は80に設定されています。

## 4-2 ネットワーク構成について

Equalizerで実現可能なネットワーク構成について、また構成によるクラスターサーバのIPアドレス体系などにつきましては、[弊社サポートページ](#)をご確認下さい。

## 4-3 クラスタ作成

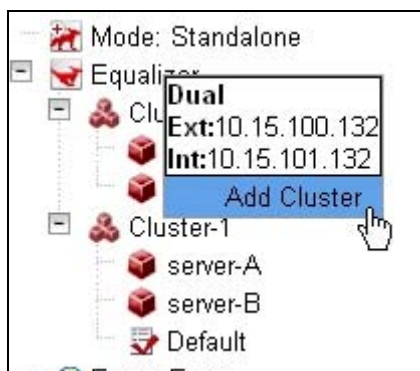
Equalizer で作成できるクラスタは、以下の4種類になります。

モデル	L4/TCP	L4/UDP	L7/HTTP	L7/HTTPS
E250GX	○	○	○	○


**アドバイス:** 冗長化構成では、まず冗長化設定(セクション5参照)を行うことを推奨しています。これは、冗長化構成の Equalizer はデフォルトではクラスタ・サーバの設定は同期する為で、同期させることで片側機器のみ設定を行うともう一方の機器に設定が自動でコピーされます。

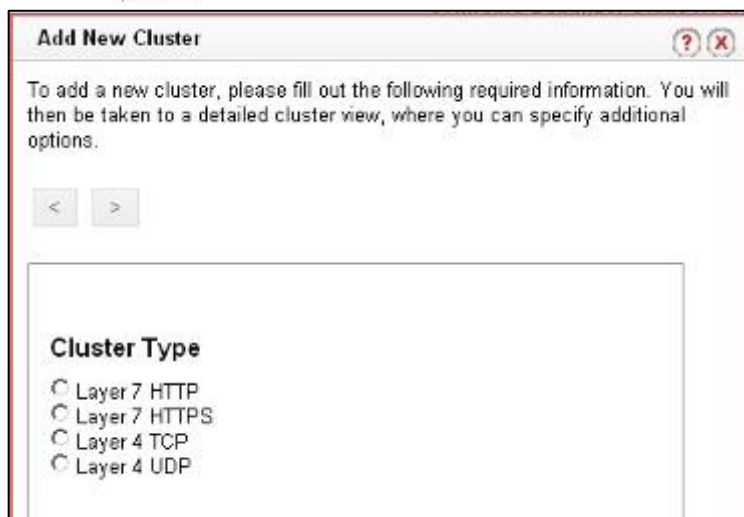
### 4-3-1 クラスタ作成ウィザードの起動

クラスタの作成は、クラスタ作成ウィザードから行ないます。左フレームを右クリックすると、メニューが表示されます(下図)。メニューから“Add Cluster”を選択し、ウィザードを起動します。



### 4-3-2 L4クラスタの作成

L4クラスタを作成する場合は、ウィザードで“Layer 4 TCP”または“Layer 4 UDP”を選択し  ボタンを押して次に進みます。



**Add New Cluster**

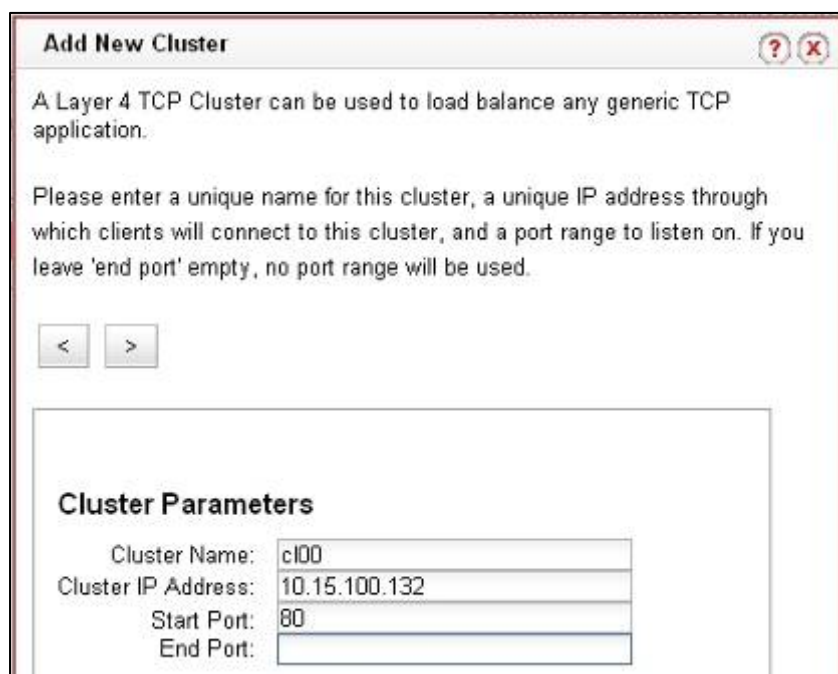
To add a new cluster, please fill out the following required information. You will then be taken to a detailed cluster view, where you can specify additional options.

< >

**Cluster Type**

Layer 7 HTTP  
 Layer 7 HTTPS  
 Layer 4 TCP  
 Layer 4 UDP

次画面にて作成するクラスタの詳細情報を入力します。



**Add New Cluster**

A Layer 4 TCP Cluster can be used to load balance any generic TCP application.

Please enter a unique name for this cluster, a unique IP address through which clients will connect to this cluster, and a port range to listen on. If you leave 'end port' empty, no port range will be used.

< >

**Cluster Parameters**


Cluster Name:	c100
Cluster IP Address:	10.15.100.132
Start Port:	80
End Port:	

- **Cluster Name**  
クラスタの名称設定です、アルファベットから始まる必要があります。
- **Cluster IP Address**  
クラスタの IP アドレスを入力します。
- **Start Port**  
受付ポートの開始ポートを設定します。
- **End Port**  
受付ポート番号の範囲指定を行なう場合は終点ポートの設定をします。 単一ポートのみの設定であれば空欄にします。



次の画面で設定内容を確認し commit すると新規 L4クラスタが左フレームに追加されます。

### 4-3-3 L7クラスタの作成

L7クラスタを作成する場合は、ウィザードで “Layer 7 HTTP” または “Layer 7 HTTPS” を選択し  ボタンを押して次に進みます。

次画面では 4-3-2 と同じくクラスタ情報を入力します。L4クラスタと違い、設定するポート番号は1つです。設定内容を確認し commit すると新規 L7クラスタが左メニューに追加されます。

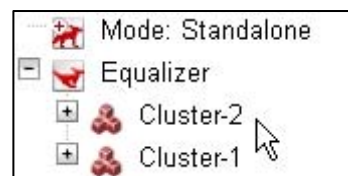
### 4-3-4 クラスタの削除

作成したクラスタを削除するには、左フレームで削除したいクラスタを選択し右クリックします。表示されるメニューから Delete Cluster を選択すると、確認画面が表示されますので、決定を押すと削除完了です。

または、3-1-1 で削除ボタンを使用することで行なうことも可能です。

## 4-4 L4クラスタパラメータ設定

クラスタのパラメータを設定します。作成したクラスタを左メニューから選択することでパラメータ設定画面へ移行することが出来ます(右図)。



**注意：一部のパラメータは [3-1](#) と同様のものです。3-1 の設定内容はグローバル設定として、すべてのクラスタに適用されます。3-1 と同様のパラメータを各クラスタに個別設定した場合はグローバル設定よりも優先されます。**

### 4-4-1 “Configuration” タブ



クラスタ動作に必要な設定を行うタブです。以下4つに分類されています。

#### 4-4-1-1 “Required”

cluster parameters

protocol	<input type="text" value="Layer 4 TCP"/>
ip	<input type="text" value="192.168.1.1"/>
start port	<input type="text" value="80"/>
end port	<input type="text" value="80"/>
idle timeout	<input type="text" value="0.0"/>
disable	<input type="checkbox"/>
spooF	<input type="checkbox"/>
direct server return	<input type="checkbox"/>

項目	内容
protocol	4-3-2 で作成したクラスタ種類が表示されます（変更は出来ません）
ip	4-3-2 で作成した IP アドレスが表示されます（変更可能です）
start port	4-3-2 で作成したポート番号が表示されます（変更可能です）
end port	同上
idle timeout	L4 クラスタへの設定値で、アイドル状態にある TCP コネクションを Equalizer が切断するまでのタイムアウト時間を設定します。
disable	クラスタサービス無効にする設定です。試験的にクラスタ導入を行い、検証時間外にリクエストを受け付けたくない場合等に、有効にします。
spooF	有効の場合、アクセスするクライアントの送信元 IP アドレスをクラスタ所属サーバにそのまま振り分けます。 無効の場合、アクセスするクライアントの送信元 IP アドレスは Equalizer のインターフェースに NAT されサーバに振り分けが行なわれます。 詳細は <a href="#">4-1-6</a> を参照して下さい。
direct server return	DSR 構成を行なう際、有効にします。

#### 4-4-1-2 “Probes”

cluster parameters

probe port

ACV probe

ACV response

probe delay

server agent port

agent probe

probe ssl

---

agent type

Server agent requires custom agent running on each server. Virtualization Load Balancing (VLB) agent uses Virtual Center configuration to monitor servers.

server agent

VLB

none

項目	内容
probe port	サーバヘルスチェックのポート番号を指定します。 デフォルトでは0と表示され、クラスタの受付ポートが使用されます。
ACV probe	ACVによるサーバヘルスチェックを行なう際に使用します、詳細は <a href="#">4-7-3</a> をご確認ください。
ACV response	ACVによるサーバヘルスチェックを行なう際に使用します、詳細は <a href="#">4-7-3</a> をご確認ください。
probe delay	<a href="#">3-1-2</a> と同様の設定になります。
server agent port	Server agent を使用するとサーバからパフォーマンス統計を収集し、その情報に基づき負荷分散を行ないますが、サーバ上でエージェントデーモンを走らせる必要があります(日本国内サポート外機能です)。 agent type の設定を server agent を選択するとこのパラメータは有効になります。
agent probe	サーバ側の agent に対して通信を行なう際のポート番号を指定します。 デフォルトでは 1510 を使用します。
probe ssl	SSL 通信を提供しているクラスタで ACV の設定がされている場合に有効にします。
agent type	server agent や VLB を使用した負荷分散を行なう場合に、該当する箇所を有効にします。

### 4-4-1-3 “Persistence”

セッション維持の動作設定を行います。L4 クラスタに於けるセッション維持動作については [APPENDIX A](#) をご参照下さい。



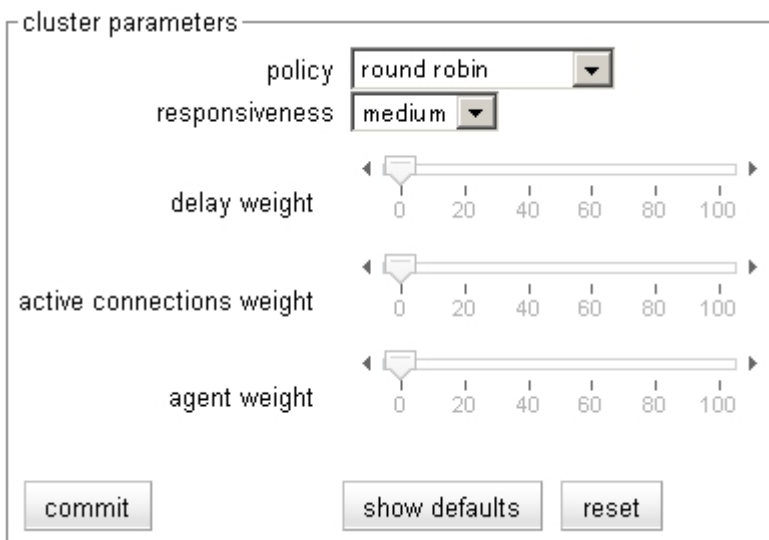
項目	内容
sticky time	クライアントの送信元 IP アドレスを利用してセッションを維持させる為の時間設定(秒)です。アクセスがあった送信元 IP は Sticky レコードに記録され、時間設定以内に再度通信が行なわれた場合は同じサーバに対して振り分けが行なわれます。セッション維持が必要ではない場合、0 秒を設定して下さい。
inter-cluster sticky	L4 クラスタを使用し、同じ IP を持つ複数のクラスタが同一サーバが設定されている状況で、そのクラスタをまたがった通信でセッション維持を行ないたい場合にはチェックを入れます。

**注意:** Sticky レコードを保持するためにはメモリを使用します。アクセスが多い環境などで Sticky 設定時間が長すぎる場合には機器メモリがひっ迫する可能性がありますので、ご注意下さい。600秒程度がメーカーの推奨値となっております。

### 4-4-1-4 “LB Algorithm”

このクラスタ内で使用される負荷分散ポリシーを選択します。各ポリシーの詳細は [4-7-1](#) を参照下さい




動的負荷分散の反応速度もこの画面から設定します、詳細は [4-7-2](#) を参照下さい



## 4-4-2 “Servers” タブ



クラスタ所属のサーバー一覧が表示されます。

項目	内容
Name	設定したクラスタ名が表示されます。
IP Address	設定した IP アドレスが表示されます。
Port	設定したポート番号が表示されます。
Status	サーバの状態がアイコンで表示されます。各アイコンの意味については、 <a href="#">3-2-1</a> を参照して下さい。
Actions	該当するサーバの削除  、変更  を行うことができます。サーバ新規作成を行なう場合には  を選択します。

## 4-4-4 “Reporting” タブ



クラスタに対する通信の状況などを確認することができます。

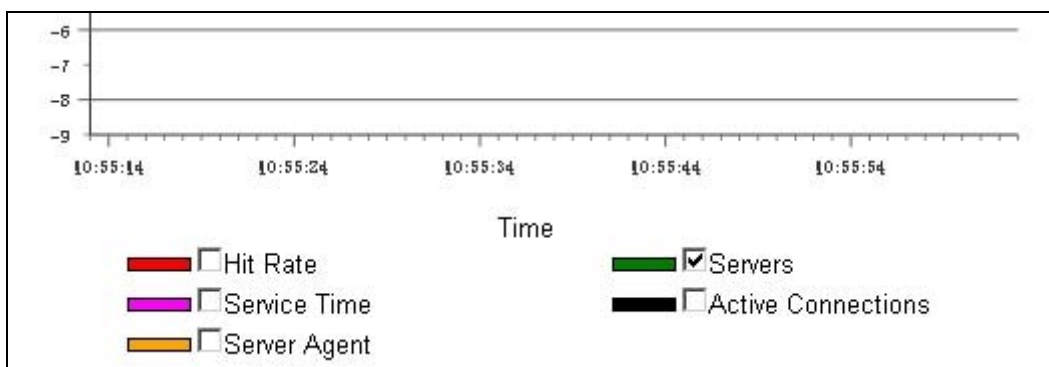
### 4-4-3-1 “Statistics”

クラスタに対する通信の統計を簡単に確認することが可能です(右図)。各パラメータについては以下をご参照下さい。

Cluster Statistics
total number of servers: 2
server active connections: 0
total connections served: 754
active sticky records: 0

項目	内容
total number of servers	クラスタに設定されているサーバ数が表示されます。
server active connections	3-2-1 で確認できる Active の項目と同様です。現在アクティブなセッション数を表示します。
total connections served	3-2-1 で確認できる Processed の項目と同様です。処理されたセッション数を表示します。
active sticky records	3-2-1 で確認できる Sticky の項目と同様です。クラスタが保持している Sticky 数を表示します。

#### 4-4-3-2 “Plots”



クラスタ・サーバについての統計をグラフ表示することが出来ます。

#### 4-4-5 FTPサービスを提供する場合のクラスタ設定

Equalizer でFTP サービスを提供する場合は、以下の設定を参照して下さい。FTP は複数のポートを使用し、かつFTP が行なう NAT 動作を正常に処理するため、Equalizer は特別な仕様になっています。

クラスタの作成方法などは通常と同じですが、FTP クラスタ用の設定については以下の表を参照して下さい。

設定項目	使用するパラメータ
クラスタ	L4/TCP クラスタ
ポート番号	21
spoof	有効

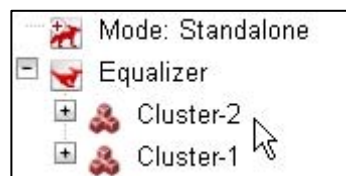
外部からアクセス出来ないネットワークセグメントにサーバ群が設定されている場合 passive FTP translation のオプションを有効にすることが必要な場合があります(3-1-4を参照)。有効にした場合、Equalizer はサーバの IP アドレスではなくクラスタ IP アドレスを含めるようにサーバから外部への FTP PASV コントロールメッセージを書き直します。この設定を有効にした場合は、クライアントは passive モード(PASV)のみでしかクラスタにアクセスできなくなります。

FTP クラスタを使用する際には、以下の点にも留意して下さい。

- Equalizer のポート変換機能は使用できません。クラスタで設定されたポート番号と、サーバで設定されたポート番号は同じでなければなりません。
- FTP クラスタは前述の通りポート21番で設定する必要があります。ポートの範囲指定機能を使用し、例えばポート19番～50番を設定したとしても Equalizer は FTP クラスタとは認識しません。
- FTP のデータコネクションは Equalizer の内部動作として sticky time は1秒として処理されています。これは、多くの Web ブラウザで使用されている Passive モードのデータコネクションをサポートするためです。
- FTP クラスタは Web 管理画面には1つのクラスタのみ表示されますが、内部動作としては2つのクラスタスロットを使用しています。こうすることでサーバからの FTP データコネクションを正常に NAT し外部へ通信させることが出来ます。

## 4-5 L7/HTTPクラスタパラメータ設定

クラスタのパラメータを設定します。作成したクラスタを左メニューから選択することでパラメータ設定画面へ移行することができます(右図)。



### 4-5-1 “Configuration” タブ



クラスタ動作に必要な基本設定を行うタブです。以下5つのセクションに分かれています。

#### 4-5-1-1 “Required”

cluster parameters

protocol	Layer 7 HTTP
ip	10.15.100.173
port	80
netmask	0xffffffff
disable	<input type="checkbox"/>
ignore case	<input checked="" type="checkbox"/> (inherit from global: <input checked="" type="checkbox"/> )
spooof	<input checked="" type="checkbox"/>

commit
show defaults
reset

項目	内容
protocol	4-3-2 で作成したクラスタ種類が表示されます (変更は出来ません)
ip	4-3-2 で作成した IP アドレスが表示されます (変更可能です)
responsiveness	動的負荷分散の反応速度を設定します、詳細は <a href="#">4-7-2</a> を参照下さい
netmask	External ポートで定義されているサブネットマスクとは異なるサブネットがクラスタ IP のサブネットに適用されている場合のネットマスクの値になります。これはお客様が適切なルーティングをクラスタが複数 IP サブネットにアクセス出来るように設定されている事が条件になります。
disable	クラスタサービス無効にする設定です。試験的にクラスタ導入を行い、検証時間外にリクエストを受け付けたくない場合等に、有効にします。



ignore case	有効な場合 Match Rules で精査する内容で大文字・小文字の判別を行いません。 <b>(E250GX では使用しません)</b>
spooof	有効の場合、アクセスするクライアントの送信元 IP アドレスをクラスタ所属サーバにそのまま振り分けます。 無効の場合、アクセスするクライアントの送信元 IP アドレスは Equalizer のインターフェースに NAT されサーバに振り分けが行なわれます。 詳細は <a href="#">4-1-6</a> を参照して下さい。

### 4-5-1-2 “Probes”

[4-4-1-2](#) と同様の設定になります、そちらのセクションをご参照下さい。

### 4-5-1-3 “Persistence”

セッション維持の動作設定を行います。L7クラスタに於けるセッション維持動作については APPENDIX A をご参照下さい。

cluster parameters

cookie age

cookie scheme

cookie generation

cookie domain

cookie path

persist

always

項目	内容
cookie age	Equalizer のセッション維持用 Cookie の有効期限を秒で指定します。有効時間を過ぎたセッション維持用 Cookie を持って通信が行なわれた場合は、Equalizer はセッション維持動作を行いません。 設定する場合は、クライアント・Equalizer・サーバが同じ時刻に設定されていることを確認して下さい。時刻設定に差異がある場合、正常に動作しないことがあります。
cookie scheme	cookie scheme は 0~2 の値で設定し、クラスタで使用されるセッション維持用 cookie のフォーマットを指定します(通常はデフォルトの 2 で問題ありません)。 0 = cookie にはクラスタの IP アドレスおよびポート番号、またサーバの IP アドレスおよびポート番号が保存されます。

	<p>1 = cookie にはクラスタの IP アドレス、またサーバの IP アドレスおよびポート番号が保存されます。</p> <p>2 = cookie にはクラスタの IP アドレス、またサーバの IP アドレスが保存されます。</p>
cookie generation	cookie scheme が 2 もしくはそれ以上の場合に追加します。適切な cookie として認識させる為に cookie generation 値はブラウザに保存されるその数値と一致しなければなりません。逆に古い cookie を適用させたくない場合にはこの数値を加算します。
cookie domain	設定されたドメイン名でアクセスするクライアントのブラウザにのみ セッション維持用 cookie の付与を行いません。 (例えば www.coyotepoint.com や my.coyotepoint.com)。
cookie path	リクエスト URI 内に設定されたパスが存在する場合に セッション維持用 cookie をブラウザに付与します。(例えば、/store/と設定し、http://www.hogehoge.com/store/mypage.html にアクセスした場合にはセッション維持用 cookie がブラウザに保存されます。http://www.hogehoge.com/goods/information.html ではセッション維持用 cookie はブラウザに保存されません)
persist	Cookie を使用したサーバセッション維持を行なう際に有効にします。
always	無効の場合、サーバが set cookie を行ったかを確認し、行っていればセッション維持用 Cookie を Equalizer も付与し、行っていないければ Equalizer はセッション維持用 Cookie を付与しません。 有効の場合は、必ずセッション維持用 Cookie を付与します。

#### 4-5-1-4 “LB Algorithm”

[4-4-1-4](#)と同様の設定になります、そちらのセクションをご参照下さい。

#### 4-5-1-5 “Networking”

L7クラスタ固有のタイムアウト値などの設定を行います。

cluster parameters

send buffer	32
receive buffer	16
request max	32
response max	32
custom header	
connect timeout	10.0
client timeout	5.0
server timeout	60.0
abort server	<input type="checkbox"/> (inherit from global: <input checked="" type="checkbox"/> )
once only	<input type="checkbox"/>
insert client IP	<input type="checkbox"/>

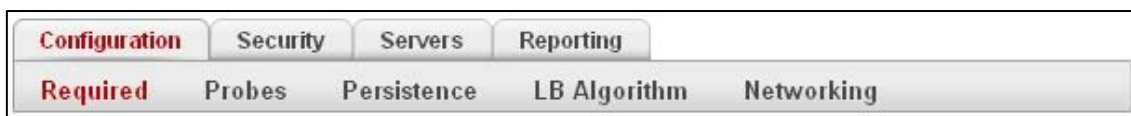
commit
show defaults
reset

項目	内容
send buffer	ネットワークインターフェースから送信される直前のデータが L7プロキシ処理を行う為に確保するメモリ領域をキロバイトで設定する値になります。
receive buffer	ネットワークインターフェースに受信されているデータを L7プロキシ処理する為に確保するメモリ領域をキロバイトで設定する値になります。
request max	キロバイトでの最大 HTTP リクエストヘッダの取得サイズになります。
response max	キロバイトでの最大 HTTP レスポンスヘッダの取得サイズになります。
custom header	Equalizer で受け付けるリクエストに対して、カスタムの HTTP ヘッダを挿入します。
connect timeout	接続要求に対してサーバがレスポンスを返すまでの Equalizer のタイムアウト値になります。
client timeout	Equalizer がクライアントリクエストの終了を待つまでのタイムアウト設定値になります。
server timeout	Equalizer がサーバへリクエストを投げてから次のリクエストを受けるまでの接続をタイムアウトとして判定するまでの設定値になります。
abort server	クローズする際にサーバに対し不意に接続を落とします。
once only	1 つの TCP セッションに対して複数のリクエスト投げるようなクライアント通信で最初のリクエストのみ Equalizer cookie を確認してセッション維持を行います。また、HTTP/1.1 でのプロキシサーバ経由通信が multiplexing で動作する場合には無効にする必要がある場合があります。
insert client IP	有効にした場合、クライアントリクエストをサーバへ送付する際に、HTTPヘッダ “X-Forwarded-For” をEqualizerが付与します。このヘッダにはクライアントIPアドレスが記載されています。詳細については <a href="#">4-1-6-5</a> を参照して下さい。

#### 4-5-2 “Reporting” タブ

[4-4-4](#) と同様の設定になりますので、そちらのセクションをご参照下さい。

## 4-6 L7/HTTPSクラスタパラメータ設定



SSL 通信を Equalizer で終端させる場合は、L7/HTTPS クラスタを作成します。作成手順については 4-3-3 をご参照下さい。また、基本的な設定内容は L7/HTTP クラスタと同じですので、このセクションでは L7/HTTPS にのみ存在するパラメータについて説明致します。

L7/HTTPS クラスタ作成後は、下記のようなエラーが表示されます。




「L7/HTTPS クラスタはサーバ証明書をインストールしないと使用できません」という旨のエラーになり、これは 4-6-1 の手順でサーバ証明書をインストールすることで表示されなくなります。

### 4-6-1 “Security> Certificates”

SSL サーバ(クライアント)証明書のインストール・更新を行い、インストールした証明書の内容を確認することが出来ます。CSR 作成手順につきましては [APPENDIX B](#) をご参照下さい。

- select client or cluster certificate  
インストールする証明書がサーバ証明書であれば cluster、クライアント証明書であれば client を選択します。
- select SSL certificate file  
インストールする証明書を選択し、決定します。

 を押し決定すると、選択された証明書の内容が表示されます。サーバ証明書にパスワードが設定されている場合には、右図のようにパスワード入力画面が表示されます。



サーバ証明書の内容は下記のように表示されます。下の例ではサーバ証明書と中間証明書が

組み込まれた Composite ファイルなので、2つの証明書情報 がそれぞれ記載されております。選択したいサーバ証明書であると確認後、  を押して決定します。



画面が更新され、サーバ証明書の内容が表示されることを確認します。

#### 4-6-2 “Security > SSL”

SSL 関連の設定はこちらから行います。各パラメータの詳細については下記をご確認下さい。

cluster parameters	
cipher suite	<input type="text" value="AES128-SHA:DES-CBC3-SHA"/>
session cache timeout	<input type="text" value="60.0"/>
session cache kbytes	<input type="text" value="256"/>
client verification depth	<input type="text" value="2"/>
certify client	<input type="checkbox"/>
require certificate	<input type="checkbox"/>
verify once	<input type="checkbox"/>
ssl unclean shutdown	<input type="checkbox"/>
no header rewrite	<input type="checkbox"/>
<input type="button" value="commit"/> <input type="button" value="show defaults"/> <input type="button" value="reset"/>	

項目	内容
cipher suite	L7 HTTPS クラスタの設定値で、サーバによって提供される cipher suite を制限します。 XCEL カードが認識された時、XCEL カードで

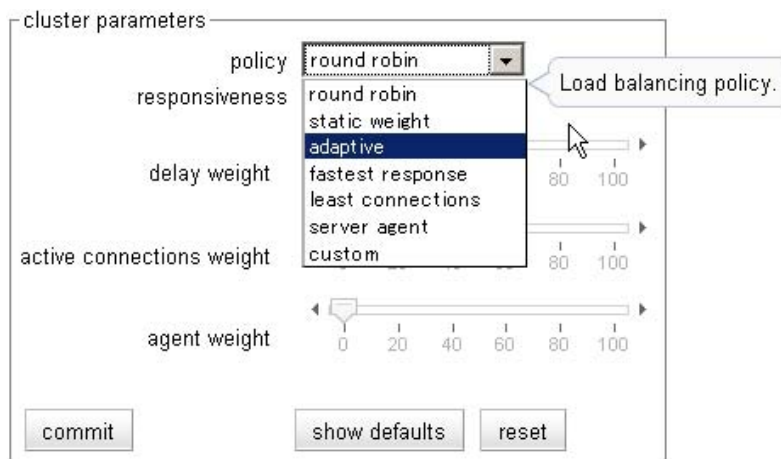
	アクセラレートされるデフォルトの cipher suite が設定されます。
session cache timeout	SSL セッションキャッシュで確保された領域を破棄する設定秒数になります。
session cache kbyte	SSL セッションキャッシュで領域確保されるキロバイトでの最大値になります。
client verification depth	L7 HTTPS クラスタの設定値で、例えば、デフォルトの 2 という数値はクライアント証明(Level 0)と2階層上(Level 1、Level 2)を確認します。Level 2 より大きい証明パスは無視されます。
certify client	クライアントのリクエストを Equalizer が受けた際にクライアント証明書をサーバに代わって確認するか否かの設定項目になります
require certificate	クライアントのリクエストを Equalizer が受けた際にクライアント証明書を Equalizer が要求するか否かの設定になります。
verify once	たとえ SSL で再認証されたとしても、Equalizer はクライアントの最初のリクエストのみ証明確認します。
ssl unclean shutdown	L7 HTTPS クラスタの設定値で、HTTP/1.1 での HTTPS 接続維持を行う際にエラーが表示される場合にはチェックを付けてお試し下さい。この問題は Internet Explore と Apache サーバとの接続時に依存する問題で、通常断続的に起きるようです。
allow unsafe renegotiation	HTTPS クラスタでは SSL renegotiation 機能はデフォルトで無効になっています。この設定を有効にすることで、SSL renegotiation を行うことが可能になります(セキュリティの観点から無効にしておくことが推奨されています)。
no header rewrite	サーバからクライアントへのレスポンスをそのまま通す設定になります。通例 Equalizer の L7 HTTPS クラスタの設定を行うと、その所属サーバの待ち受けポートは HTTP として処理されます。Equalizer はクライアントと SSL で通信していますので、仮にサーバが Location: header を使用し HTTP リダイレクトを送信すると、この URL は https: が含まれないプロトコルとなります。Equalizer はそれが HTTPS になるようにサーバからのレスポンドを自動で書き換えますが、この書き換えを Equalizer に行わせたくない場合に、この項目にチェックを付けて有効にします。

## 4-7 L4/L7 クラスタ共通パラメータ詳細

### 4-7-1 “Configuration > Require > Policy”

クラスタ負荷分散アルゴリズムの設定を行います。ポリシー設定は各クラスタ個別で行ないます。

各アルゴリズムの内容は下記をご確認下さい。



項目	内容
round robin	<p>Equalizer デフォルトの負荷分散アルゴリズムです。設定ファイルの該当クラスタ所属サーバの登録順に上から順に振り分けが行われ、最後のサーバまで振り分けが行われると最初の登録サーバに戻って通信を処理します。サーバが Down した場合にはそのサーバを負荷分散サーバのリストから除外して負荷分散処理を継続します。</p> <p>round robin はサーバの weight 値には影響されず負荷分散を行なう静的なアルゴリズムです。サーバのレスポンス時間やコネクション数に関わらず動作します。</p>
static weight	<p>各サーバ個別に設定された weight 値を基に負荷分散を行います。高い weight 値が設定されたサーバに対しては高い割合でリクエストが振り分けられます。設定された weight 値を考慮しランダムに振り分けを行なうイメージです。</p>
adaptive	<p>Equalizer 独自のアルゴリズムになり、以下3つの要素を基に最適な振り分け先サーバを判断します。</p> <ul style="list-style-type: none"> <li>• Server response time サーバからの応答時間です。</li> <li>• Active connection count サーバに振られているアクティブ接続数です。</li> <li>• Server agent value サーバで起動しているサーバエージェントデーモンによって返</li> </ul>

	される数値です
fastest response	<p>サーバのレスポンス時間がもっとも短いサーバに対して高い確率で負荷分散されます。ただし、仮に Equalizer が一度にそのリクエストを対象サーバに振ってしまうと、そのサーバの負荷が一度に上がってサーバのレスポンス時間が遅くなる結果を招く可能性があります。この事から Equalizer はクラスタ単位でこのレスポンス時間を最適化します。</p> <p>この負荷分散アルゴリズムでは Equalizer はアクティブ接続数と(設定がされていれば)サーバエージェント値を確認します。しかし両数値が adaptive で運用するよりも小さな影響になります。あるサーバのレスポンス時間がそのクラスタ内で一番早かったとしてもアクティブ接続数が大きい場合やサーバエージェント値が高い数値の場合には Equalizer は新規セッションをそのサーバに振らない事があります。</p>
least connections	<p>サーバのアクティブ接続数がもっとも少ないサーバに対して高い確率で負荷分散されます。ただし、fastest response の様に Equalizer は該当するサーバがこの振り分けによってレスポンスを落とさない様にサーバのアクティブ接続数やサーバエージェント値を確認しています。Least connection もクラスタワイドでサーバへの接続振り分けを最適化しています。</p>
server agent	<p>サーバエージェント値のもっとも低いサーバに対して高い確率で負荷分散されます。fastest response と同様にアクティブ接続数とレスポンス時間を確認しています。server agent はサーバエージェント機能が有効になっている時のみ動作します <b>(日本でのサポートは現状御座いません)</b>。</p>
custom	<p>サーバのレスポンス時間、サーバのアクティブ接続数、サーバエージェント値の3点をカスタマイズ設定することが可能です。</p>

#### サーバエージェントの利用について

サーバエージェントはサーバのパフォーマンスの統計情報を収集します。サーバエージェントを使用する設定をクラスタに行った場合、Equalizer は定期的にサーバエージェントデーモンが起動しているクラスタ所属サーバにアクセスしてパフォーマンス統計情報を収集します。

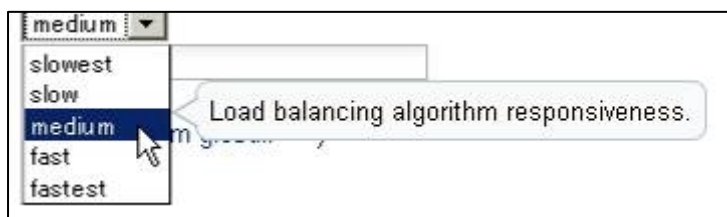
また、サーバエージェントをカスタマイズしてサーバリソースをサーバエージェントへ通知させる仕組みを作ることで、Equalizer はデータベースやその他のサーバリソースが提供状況にない場合にサーバに対してリクエストを振り分けしなくなります。

備考： 負荷分散アルゴリズムを server agent に設定した場合には、各クラスタ所属サーバはサーバエージェントデーモンがパフォーマンス統計情報を収集する為、起動している必要があります。もし負荷分散アルゴリズムを server agent に設定し、クラスタ所属サーバにサーバエージェ



ントデーモンが起動していない場合でクラスタパラメータの pedantic agent が無効の状態であれば、Equalizer はサーバエージェントデーモンが返す数値無しで負荷分散を行います。 pedantic agent が有効の場合で、サーバエージェントデーモンがサーバで起動していない場合にはそのサーバは DOWN 判定を受けます。

#### 4-7-2 “Configuration > Require > Responsiveness”



responsiveness の設定は Equalizer がサーバの動的 weight 値をどのくらい頻繁に調整するかの設定になります。 Equalizer は slowest、slow、medium、fast、fastest の 5 つのレスポンス設定を提供しています。 このレスポンス設定は adaptive、least connections、fastest response 負荷分散アルゴリズムを使用する際に影響を与えます。

#### 動的 weight 値による負荷分散

クラスタ内の各サーバの静的 weight 値を適切に設定した後に Equalizer が各サーバの動的 weight 値を調整していない事があります。 つまり負荷が高いのにも関わらず動的 weight 値に変化が無い場合ですが、このような場合にはクラスタのレスポンスのパラメータを fast へ変更します。 Equalizer はサーバのパフォーマンスを最適化します。 これにより、クラスタワイドのパフォーマンスの改善が図られるでしょう。

#### Dynamic Weight Oscillations

特定サーバの動的 weight 値が振幅している場合(例えば、動的 weight 値が 100[デフォルトの静的 weight 値]を基準にした時に時間軸に対して振幅が上下に激しい場合など)には、クラスタのレスポンスを slow へ変更します。 同時にサーバのアプリケーションが不適切な動作をしていないか確認を行います。

#### 4-7-3 “Configuration > Probes > ACV probe / response”

コンテンツレベルでサーバのヘルスチェックを行なう場合に設定を行います。

probe port	443
ACV probe	GET /equalizer/check.html HTTP
ACV response	Server OK
probe delay	10.0

ACVは各クラスタ個別で設定されます。ACVが設定された状態では、HTTPリクエストをサーバに対して行い、応答される文字列によってサーバ状態を確認しています。

テキストベースでのリクエスト/レスポンスに対応するプロトコルでACV設定が可能です。ただしL4/UDPクラスタではACVの設定は出来ません。

設定項目は2箇所です。

#### 4-7-3-1 “ACV probe”

■L4 クラスタの場合：GET /<URL Path> HTTP/1.0(1.1)¥r¥nHost:<hostname>¥r¥n¥r¥n と設定します。

例) GET /index.htm HTTP/1.1¥r¥nHost:www.coyotepoint.com¥r¥n¥r¥n

L4 クラスタでは設定されるサービスがHTTPとは限らない為、改行コードが必要になります。また、サーバによってこの改行コードが当てはまらない場合がありますので、サーバ側の設定をご確認下さい。

■L7 クラスタの場合：GET /<URL path> HTTP/1.0(1.1)¥r¥nHost:<hostname> と設定します。

例) GET /index.html HTTP/1.1¥r¥nHost:www.networld.co.jp

(最後の「¥r¥n¥r¥n」のような改行コードは必要ありません。自動で入力されます。ただし、サーバによって自動で付加される改行コードが当てはまらない場合がありますので、サーバ側の設定をご確認下さい。)

#### 4-7-3-2 “ACV response”

サーバからあるべき応答の文字列を指定します。ACV string で取得するファイルの先頭 1024 バイト目までを確認しますので、ACV response で指定する文字列は必ずこの 1024 バイトに含まれている必要があります。


[例] welcome

## 4-8 サーバ設定

クラスタ設定後、サーバを追加します。

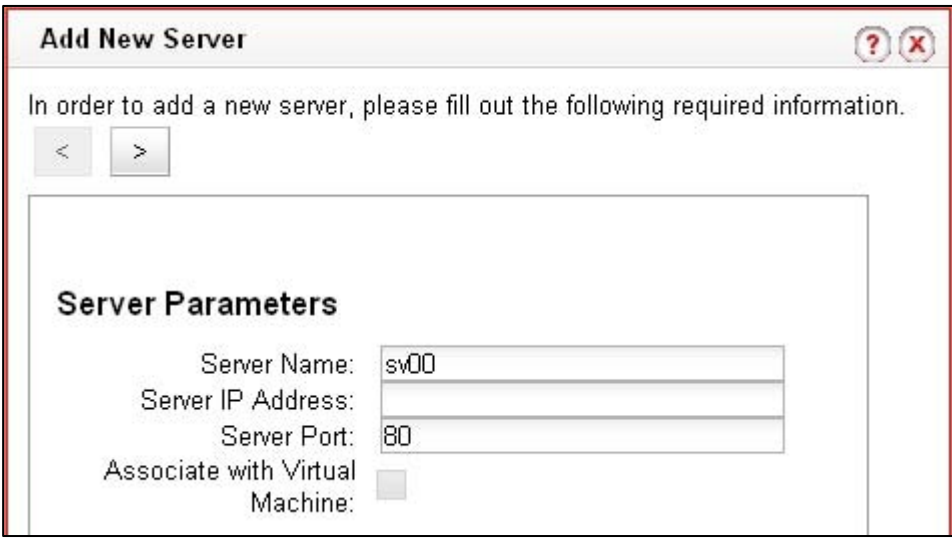
### 4-8-1 サーバ作成

左メニューから新規サーバを所属させるクラスタ上で右クリックすると、メニューが表示されますので“Add Server”を選択するとサーバ作成ウィザードが表示されます。

同様のことを [4-4-3](#) のサーバー一覧画面から行なうことができます。サーバテーブルから  を選択します。



### 4-8-2 サーバ作成ウィザードの入力

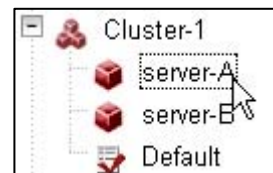


サーバ作成ウィザードにて、サーバ情報を入力します。

- Server Name  
サーバの名称設定です、アルファベットから始まる必要があります。
- Server IP Address  
サーバの IP アドレスを入力します。
- Server Port  
サーバのサービス受付ポート設定です。デフォルトではクラスタのポート番号が自動で設定されますが、クラスタの受け付けポートとは別に任意の番号へ変更することが可能です([4-1-7](#)を参照下さい)。
- Associate with Virtual Machine: (E250GX では使用しません)  
VLB 機能を有効にしたクラスタに、仮想サーバを追加する場合チェックを入れます。

### 4-8-3 サーバ パラメータ設定変更

左フレームのリストからサーバを選択することで、詳細情報を確認することができます(右図)。



### 4-8-4 Configuration タブ設定



#### 4-8-4-1 “Required”

Server parameters

ip	<input type="text" value="192.168.10.10"/>
port	<input type="text" value="80"/>
probe port	<input type="text" value="0"/>
max connections	<input type="text" value="0"/>
initial weight	<input type="text" value="100"/>
hot spare	<input type="checkbox"/>
quiesce	<input type="checkbox"/>
dont probe	<input type="checkbox"/>
dont persist	<input type="checkbox"/>

サーバの基本パラメータ設定を行うことが可能です。

**注意: Server Name については変更することが出来ません。**

項目	内容
ip	サーバの IP アドレスを入力します。
port	サーバのポート番号を入力します。
probe port	ヘルスチェックを行なうポート番号を別途指定する場合は設定します。デフォルトは 0 と表示され、この場合はサーバのポート番号を使用します。
max connections	サーバに振り分ける最大同時接続数を設定します。詳細は 4-8-5 を参照下さい。
Initial weight	サーバの初期 Weight 値を設定します。設定範囲は 20 ~ 200 です。例えば、サーバ2台を 50:100 の割合にした場合はおよそ 1:2の割合

	でリクエストが割り振られます。
hot spare	バックアップサーバや Sorry サーバとして使用する際に有効にします。詳細は 4-8-6 を参照下さい。
quiesce (クワイエンス)	メンテナンス時などサーバを使用停止する際に、クライアントからのコネクションを維持しながら行なう際に使用します。詳細については 4-8-7 を参照下さい。
dont probe	サーバに対して TCP ハンドシェイク(および ACV)によるヘルスチェックを行わない場合は、この設定を有効にします。詳細は 4-8-8 を参照下さい。
dont persist	サーバ個別に対してセッション維持を無効にする場合は、この設定を有効にします。詳細は 4-8-9 を参照下さい。

#### 4-8-4-2 “Outbound NAT”

<b>Configuration</b>	Reporting
Required	<b>Outbound NAT</b>

Outbound NAT機能([3-1-4-2](#) を参照)の詳細設定を行います。デフォルトではEqualizerのExternal側IPアドレスにNATされますが、本設定を行うことで、NATするIPアドレスをサーバIPアドレスごとに設定可能になります。

本設定を行う理由として、以下のようなケースがあります。

- ・ 冗長化構成時に、Equalizer の Failover が発生すると Outbound NAT 時に使用される IP アドレスも併せて変更されるため、一意の IP アドレスに NAT することが出来ない。Failover Alias に NAT させることで、どちらの機器が Primary 役であっても同一 IP アドレスで外部へアクセスすることが出来る。
- ・ アプリケーションの仕様上、サーバからクライアントへ通信を行う必要があるが、通常の Outbound NAT ではクラスタ IP アドレスとは異なってしまうため、クライアントと正常に通信ができない。クラスタ IP アドレスに NAT させることで、サーバからクライアントへの通信を、サービスとして提供している IP アドレスから行うことが出来る。

**注意:** 本設定を使用するには、事前にグローバル設定でOutbound NATが有効になっている必要があります。設定方法は [3-1-4](#) をご参照下さい。

**参考:** 同一 IP アドレスのサーバが、複数クラスタに所属している場合は、最後に変更された設定が適用されます(最後に更新された時点で、別クラスタに所属する同一 IP アドレスのサーバが自動的に Default address に変更されます)。

Default address  
This option will set the outbound NAT address to the Default setting. This means that if this server's outbound NAT option is not set explicitly in another cluster, the Equalizer's address will be used. If it is set explicitly in another cluster, that address (either Failover or Cluster) will be used.

Equalizer address  
This option will set the outbound NAT address for this server (in this and all other clusters) to use the Equalizer's administrative IP address as the source address for outbound traffic.

Failover address  
This option will set the outbound NAT address for this server (in this and all other clusters) to use the Failover IP address as the source address for outbound traffic.

Cluster c100's address  
This option will set the outbound NAT address for this server (in this and all other clusters) to use the IP address of this cluster. This means that if this server (a server with the same IP address) exists in another cluster, that server's Outbound NAT option will be reset to use this address.

項目	内容
Default address	通常の Outbound NAT と同様、Equalizer の External 側 IP アドレスに NAT します。冗長化している環境では、Primary 役として動作している機器の IP アドレスに NAT されます。同一 IP アドレスのサーバが別クラスタに存在し、Default address 以外の設定であった場合は、その設定が優先されます。（デフォルトでこの設定が有効になっています）
Equalizer address	動作としては Default address と同様です。一度 Default address から設定変更を行い、それから再度 Default address の状態に戻すために使用します。そのサーバが1クラスタにのみ設定されている場合は Default address に設定し直せば問題ありませんが、サーバが複数のクラスタにまたがっている場合は明示的に Equalizer address を指定する必要があります。
Failover address	External側のFailover Aliasとして設定されているIPアドレスを使用します。設定方法については <a href="#">5-3-4-1</a> をご参照下さい。この設定は冗長化構成の時のみ設定可能です。
Cluster [クラスタ名]'s address	サーバが所属するクラスタ IP アドレスを使用します。 <b>L4クラスタ使用時に受付ポート番号の範囲指定を行なった場合は、サーバが使用した送信元ポート番号がクラスタの受付ポート番号の範囲外である必要があります。ポート番号が重複した場合、正常に通信ができなくなります。</b>

#### 4-8-5 “max connection” 設定

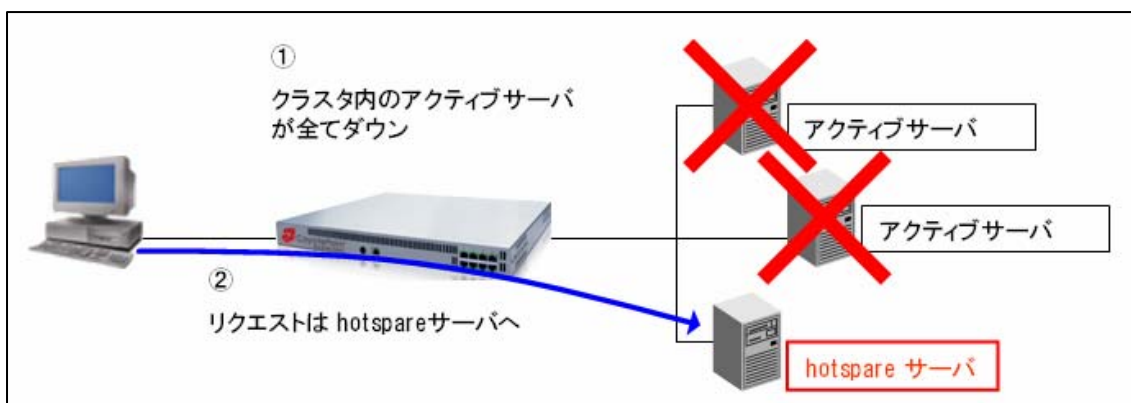
各サーバが同時に受け付けることが出来るアクティブコネクション数の上限を設定します、これは L4/ L7 クラスタに設定可能なパラメータです。 上限を超えたコネクションリクエストが行なわれた場合、そのサーバへの振り分けは行なわれず、クラスタ内の他サーバに割り振られます。

例外として、サーバのアクティブコネクションが 設定された max connection 値に達していた場合においても、クライアントが Equalizer のセッション維持用 cookie を持ってリクエストを行なった場合にはセッション維持されたサーバへ振り分けられます。 しかしながら、L4 クラスタで使用される sticky によるセッション維持された通信は max connection によってサーバへの接続が制限されます。

クラスタに hot spare サーバを設定することで、振り分け先サーバ全てが max connection に達した場合に、リクエストを hot spare サーバや Responders に処理させる事が可能です。 例えば「現在混み合っております」などのページを表示することが可能になります。

#### 4-8-6 “hot spare” 設定

バックアップサーバや sorry サーバを設定する際に使用します。 hot spare に設定したサーバに対しては通常リクエストが振り分けられることはありませんが、クラスタ内のアクティブなサーバが全てダウンと判定された場合に hot spare サーバへの振り分けが開始されます。



セッション維持された通信は hot spare サーバに対しても優先的に振り分けが行なわれます。 例えば、アクティブサーバがダウンし hot spare へ振り分けられたクライアントは hot spare サーバとセッション維持を行ないます。 この場合、アクティブサーバが復旧したとしてもセッション維持されたクライアントは hot spare サーバへ振り分けられてしまいます。 この状況はサーバ個別にセッション維持を無効にすることで回避が可能です、詳細は 4-8-8 を参照下さい。

#### 4-8-7 “quiesce” 設定

メンテナンス時などサーバを使用停止する際に、クライアントからの接続を維持しながら、緩やかにサーバへの接続を減少させる際に使用します。quiesce に設定されたサーバに対しては既存で確立しているセッションは振り分けられますが、新規リクエストは振り分けられません。接続が減少した後、サーバメンテナンスを行なうことでサービスへの影響を最小限に抑えることが可能になります。

クラスタ内で quiesce 設定されたサーバのみが存在し、その他アクティブなサーバが全てダウンしている状況に於いては、サービスの継続を優先させるため Equalizer は例外的に新規リクエストも quiesce サーバに振り分けを行いません。

セッション維持された通信については、Equalizer は quiesce サーバに対して振り分けを行いません。

#### 4-8-8 “dont probe” 設定

サーバに対するEqualizerのヘルスチェックはデフォルトでクラスタ内の全サーバに対して行なわれています。クラスタ内特定サーバへのヘルスチェックを無効にする場合にこの設定を行います。この設定を有効にしてもICMPによるヘルスチェック([3-1-2](#) 参照)は行なわれませんが、L4レベル以上のヘルスチェック(ACVを含む)は行なわれません。

**注意： ICMP によるヘルスチェックを無効にしている場合、サーバへのヘルスチェックが全て無効になってしまい、サーバのダウンを検知できなくなりますのでご注意ください。**

#### 4-8-9 “dont persist” 設定

セッション維持の設定はクラスタ単位で行なわれ、クラスタ所属のサーバ全てに対して有効になりますが、この設定を有効にすることでサーバ単位のセッション維持を無効にすることが可能です。

hot spare サーバを設定している場合にこの設定を使用することで、望まれないセッション維持を回避することが可能になります。



## セクション5 冗長化設定手順

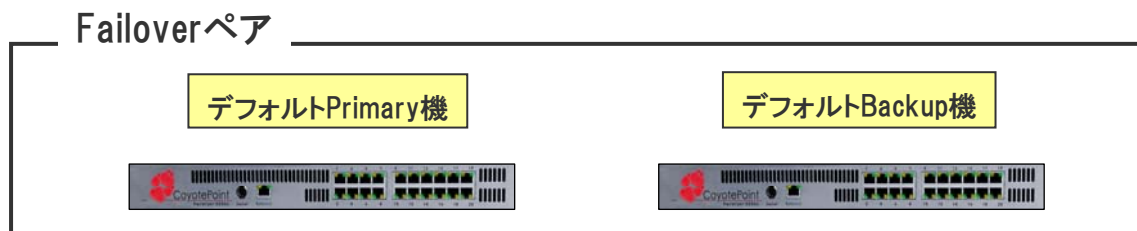
Equalizer は全てのモデルにおいて冗長化することが可能です。冗長化を行なうことでどちらかの機器に障害が発生した場合に於いてもサービスを継続させることが可能になります。

補足: Equalizer の設定上、冗長化は "Failover" と呼ばれます。本マニュアルに於きましても冗長化、Failover という2つの呼称を併用します。  
2台の機器がアクティブ・ホットスタンバイとして動作する概念は同一です。

### 5-1 Failover動作の基本概念について

Failover を組んでいる2台の Equalizer は Failover ペアと呼ばれ、役割としては以下の2種類どちらかになります。

- ・ デフォルト Primary 機
- ・ デフォルト Backup 機



上記のように Equalizer は Primary と呼ばれる機器がアクティブ機器として動作しサービスを行います。デフォルト Primary 機に障害が発生した場合は、デフォルト Backup 機が検知し、サービス提供を引き継ぎます。

## 5-2 Primary / Backupの関係について

Primary / Backup の関係について、以下の点にご注意頂く必要があります。

### 5-2-1 Primary”役”、 Backup”役” とは

5-1 のように、Failover ペアを組む2台の Equalizer は「デフォルト Primary 機」「デフォルト Backup 機」と設定されます。デフォルト Primary 機に障害が発生した場合、デフォルト Backup 機が Primary として動作しますが、この場合『デフォルト Backup 機が「Primary 役」として動作する』と表現します。

このようにデフォルト設定に関わらず Primary/Backup として動作している事は「役」と呼ばれます。運用中に**どちらの機器が実際の Primary として動作しているのか**については、各機器の「役」を確認する必要があります。下記表のような組み合わせになる可能性があります。

■デフォルトの Primary/Backup 設定と、Primary/Backup 役の組み合わせ

パターン	デフォルト設定	Primary 役	Backup 役
1	デフォルト Primary	○	
	デフォルト Backup		○
2	デフォルト Primary		○
	デフォルト Backup	○	

### 5-2-2 切り戻し動作(Failback) について

Primary 役として動作している機器に障害が発生すると、Backup 役であった機器が Primary 役に切り替わり(Failover)、サービス提供を開始します。その後、Primary 役として動作していた機器が復旧した場合は、Primary 役としてではなく Backup 役として動作を開始します。

このように、一度切り替わり動作(Failover)が発生すると、Primary 役の機器が入れ替わり、その状態のまま引き続き運用が行われます。言い換えると、Equalizer では切り戻し動作(Failback)は行なわれません。

補足: Primary 役/Backup 役を意図的に入れ替えたい場合は、Primary 役として動作している機器を再起動させることで可能です。相手機器がいなくなったことを検知した Backup 役の Equalizer は Primary 役へ移行します。

### 5-2-3 冗長化の通信(sibling) について

Failover ペアの Equalizer 間では互いの生存確認を行う sibling と呼ばれる通信をネットワークを介して行なっています。この通信によってペア同士は切り替わりなど Failover の状態確認を行います。

この通信は TCP/7342 によって行なわれます。デュアルネットワークの場合は External/Internal 側の両セグメントで行なわれます。

**注意:** Equalizer の周辺ネットワークは sibling 通信が正常に行えるように設計する必要があります。Equalizer 上位・下位のスイッチは STP 機能をポート単位で OFF にするなど、必ず sibling 通信を妨げないようにして下さい。Equalizer がファイアウォールに直接接続されている場合なども、問題になるケースがございますので、十分にご注意下さい。

### 5-2-4 Gratuitous ARPについて

Failover 動作が発生すると、Primary 役として動作を開始した Equalizer は以下の IP アドレスを自分の MAC アドレスを紐付けるために Gratuitous ARP を送出します。

- ・ クラスタ IP アドレス
- ・ External 側 Failover Alias IP アドレス
- ・ Internal 側 Failover Alias IP アドレス

Equalizer 同士、および上位・下位のネットワーク機器は上記の Gratuitous ARP を正常に受け取ることが出来る環境である必要があります。

### 5-2-5 Failoverペア同士のコンフィグ同期について

Failover ペアを組む Equalizer はコンフィグの同期を行いません。

機器設定の追加/変更/削除を実施すると、機器の sequence 値が増加します。Failover ペアを組んでいる機器間で sequence 値を比較し、値が大きい機器のコンフィグを最新と判断し、もう一方の機器に同期させます。従って、デフォルト Primary 機・デフォルト Backup 機のどちらの設定を更新してもコンフィグ同期が実施されません。

同期対象となる設定項目については以下の通りです。

- ・ Failover 設定
- ・ グローバル設定
- ・ クラスタ設定
- ・ サーバ設定
- ・ メール送付設定([3-3-1-3](#))
- ・ Handing設定([3-3-1-2](#))

同期対象ではないコンフィグは以下の通りです。

設定については Failover ペアを組んでいたとしても必ず両機器に設定する必要があります。

- Logging設定([3-3-1-1](#))
- SSL サーバ証明書
- ログ情報
- Sticky テーブル情報
- Host 名
- Domain 名
- DNS サーバ設定
- Default Gateway 設定
- Equalizer IP アドレス
- Time Zone 設定
- 時刻設定
- NTP サーバ設定

補足: コンフィグの同期はデフォルトで有効になっていますが、無効にするには [5-3-4-3](#) をご参照下さい。

## 5-2-6 Failover Aliasについて

Failover ペアを組む Equalizer は Failover Alias と呼ばれる IP アドレスを共有します。これは冗長構成にのみ使用する IP アドレスとなり、Equalizer 1 台の構成では使用しません。

通常、負荷分散対象サーバのデフォルトゲートウェイは Equalizer のリアル IP に設定しますが ([4-1-5](#))、冗長化構成の場合は Equalizer 2 台それぞれにリアル IP アドレスが存在するため、2 台の Equalizer が共有する仮想 IP アドレスを設定する必要があります。

デュアルネットワーク構成の場合は External 側にも Failover Alias IP アドレスを設定します。これは External セグメント(およびその上位)から Internal セグメントへ通信を行なう際のゲートウェイアドレスになります。この IP アドレスは固有のものである必要があります。

## 5-3 Failover設定

5-2-4 の通り Failover 設定はコンフィグ同期の対象になっています、つまり Failover 設定は両ペアで全く同一になります。5-3-1 から Failover 設定を行いますが、この設定を両機器に対して行う流れになります。

### 注意！

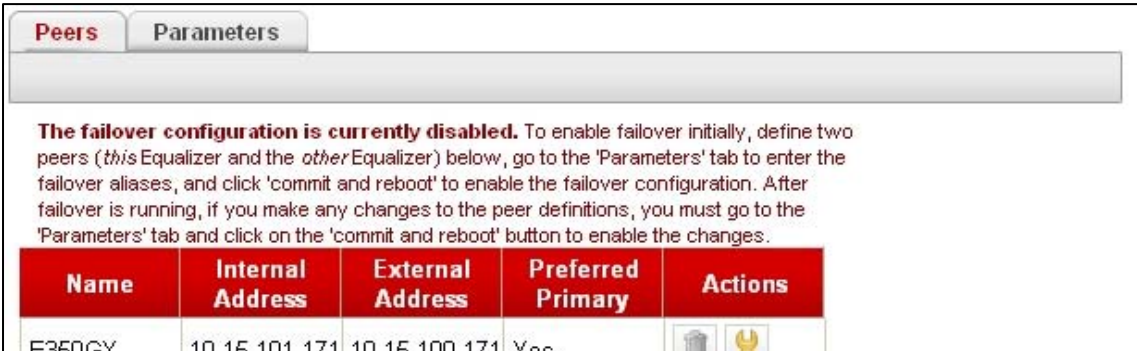
Failover 設定画面を開くと、登録されている Equalizer の情報が下記のように表示されます。Failover の設定が行われていたとしても、Failover 設定に変更を加えた場合には、Failover 設定が無効になり再起動が必要になることがあります。その場合は、5-3-4-4 の手順で再起動を行って下さい。



再起動が必要かどうかは、Failover 設定画面で

**The Failover configuration is currently disabled**

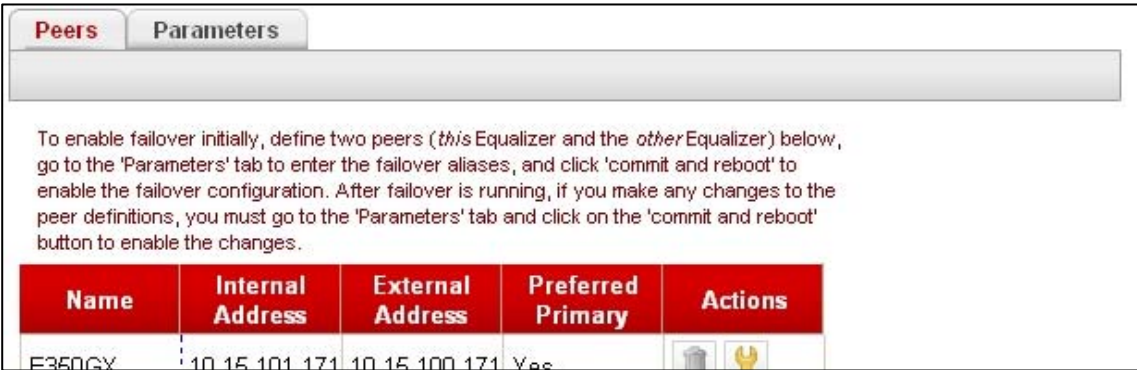
という表示をご確認下さい。表示されている場合は、再起動が必要で、表示されていない場合は再起動は必要ありません。



#### 【Failover 設定が無効になっており、再起動が必要であるケース】



Name	Internal Address	External Address	Preferred Primary	Actions
E350GY	10.15.101.171	10.15.100.171	Yes	 

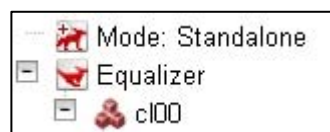
#### 【Failover 設定が有効になっており、再起動が必要ではないケース】



Name	Internal Address	External Address	Preferred Primary	Actions
E350GY	10.15.101.171	10.15.100.171	Yes	 

### 5-3-1 Failover設定画面

左フレームの最上部に“Mode: Standalone”と表示されているアイコンがあります。Failover ペアとしてではなく、単体で動作している機器はこのように Standalone と表示されます。このアイコンを選択し、Failover ペア登録を行ないます。




ペアとして登録される Equalizer は **Peer** と呼称され、識別のため Peer Name を設定します。

### 5-3-2 “Peers” タブ (Failoverペアテーブル)

右図のように Peers タブが表示されます。このタブにペアとなる Equalizer 2 台を登録します。

登録される Equalizer は

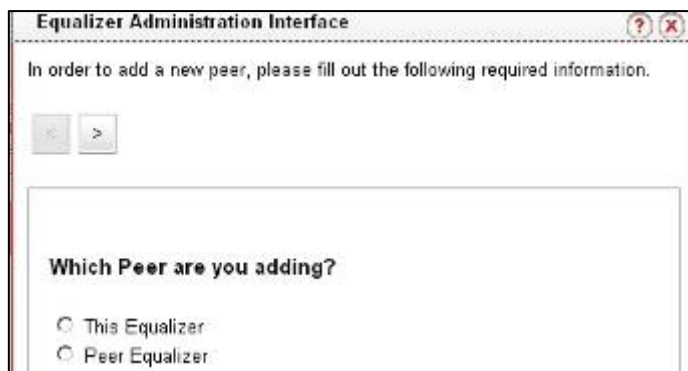
Peer テーブルの Actions から ボタンを  選択すると Peer 登録ウィザードが起動します。



### 5-3-3 Failover Peer登録ウィザード

#### 5-3-3-1 設定している機器をPeerとして登録

右図で現在設定している機器を Peer として登録します。“This Equalizer”を選択して次に進みます。

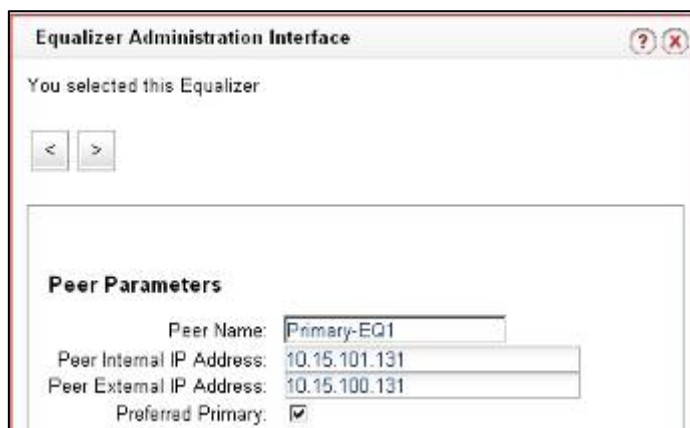


#### 5-3-3-2 設定している機器の詳細情報登録

右図のように

- Peer Name
- External 側 IP
- Internal 側 IP
- Preferred Primary

を入力します。



“Preferred Primary” は、デフォルト Primary 機器であることを設定するものですので、チェックを入れます。

#### ■本セクションで設定する Equalizer の情報

デフォルト設定	External 側 IP アドレス	Internal 側 IP アドレス	Peer Name
デフォルト <b>Primary</b>	10.15.100.131	10.15.101.131	Primary-EQ1
デフォルト <b>Backup</b>	10.15.100.132	10.15.101.132	Backup-EQ2

入力し、次に進むと確認画面が表示されますので、決定します。

補足: Failover 設定を行うと、2-1-3 で表示される system name が Peer Name で設定した名称に置き換えられます。機器の確認を容易にするため、Peer Name はそれぞれのホスト名を設定することを推奨します。

#### 5-3-3-3 登録の確認

Failover ペアテーブルに先ほど登録した Equalizer 情報が正しく登録されているか、確認します。

Name	Internal Address	External Address	Preferred Primary	Actions
Primary-EQ1	10.15.101.131	10.15.100.131	Yes	 
				

#### 5-3-3-4 Peerの登録

Failover ペアを組む Equalizer の情報を Peer として登録します。5-3-2 と同じ手順でウィザードを起動し、右図のように “Peer Equalizer” を選択します。

Which Peer are you adding?

- This Equalizer  
 Peer Equalizer

#### 5-3-3-5 Peerの詳細情報登録

5-3-3-2 と同様の手順で Peer 登録を行ないます。注意すべき点はデフォルト Backup の機器なので Preferred Primary のチェックは外す必要があります。決定し、次に進みます。

**Peer Parameters**

Peer Name:

Peer Internal IP Address:

Peer External IP Address:

Preferred Primary:

#### 5-3-3-6 Peerの詳細情報登録



Failover ペアテーブルが表示されますので、登録した Peer 情報を再度確

Name	Internal Address	External Address	Preferred Primary	Actions
Primary-EQ1	10.15.101.131	10.15.100.131	Yes	 
Backup-EQ2	10.15.101.132	10.15.100.132	No	 

認めます。

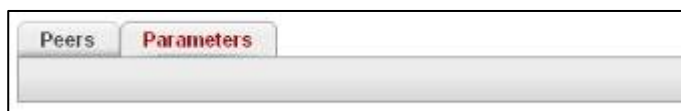
問題がなければ、同様の作業をもう1台の Equalizer にも行ないます、全く同じ設定手順ですが、5-3-3-1 の “This Equalizer” で自動設定登録される Equalizer は異なりますので、注意して下さい。

### 5-3-3-7 Peerの変更・削除

設定ウィザードから行なった Peer については設定後に変更・削除が可能です。Failover テーブルの Action から、 や  を使用して行ないます。

### 5-3-4 “Parameters” タブ

Failover ペアを組む Equalizer を Peer として登録後は、Parameter タブにある項目について設定を行います。



#### 5-3-4-1 Failover Alias設定

Failover Alias(5-2-6) の設定を行います。右図はデュアルネットワーク時の設定画面です(External側/Internal側、それぞれの項目が表示されます)。シングルネットワーク構成の場合はInternal側のみが表示されます。

configure failover aliases

internal address	10.15.101.133
internal netmask	255.255.255.0
external address	10.15.100.133
external netmask	255.255.255.0

dual network mode

#### 5-3-4-2 Failover Timing設定

Sibling 通信のタイムアウト時間などを設定します。

項目	内容
receive timeout	sibling 通信に対する相手 Peer からの応答を待つタイムアウト時間です(秒)
connection timeout	ペアの sibling 通信に対するタイムアウト時間です(秒)。



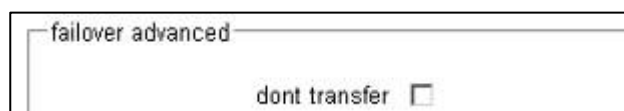
probe interval	sibling 通信を行なう間隔です(秒)。
----------------	------------------------

Backup 役の機器で、receive timeout または connection timeout のどちらかが発生した場合、1 回目の Strikeout として計算されます。この Strikeout が3回に達すると Backup 役は Primary 役へと切り替わり動作を行ないません。」

**補足： 通常の運用では、タイムアウト値はデフォルト設定で問題ありません。**

### 5-3-4-3 コンフィグ同期設定

Sibling を行なっている Equalizer 同士でコンフィグの同期を行なうかどうか、設定します。通常の設定では自動で行ないませんが、“dont transfer” を有効にすることで、コンフィグ同期は行ないません。



コンフィグ同期の詳細は [5-2-5](#) を参照下さい。

dont transfer 設定変更を行うには、設定変更後に 5-3-4-4 で説明されている commit & reboot ボタンを押します。“Reboot Equalizer?” と再起動実行の確認メッセージが表示されますが、ここで cancel を選択して下さい。

**補足： dont transfer の設定変更のみを行うのであれば再起動は必要ありません。**

### 5-3-4-4 設定の決定、再起動(commit & reboot)

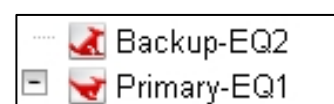
Failover の設定を行った場合、また、設定を変更した場合、必ず右のボタンを押して決定を行なう必要があります。また、この作業は再起動を伴います。



### 5-3-5 Failover設定完了の確認

再起動後、Web 管理画面へログインします。

左フレームを確認すると、5-3-1 では Standalone と表示されていた箇所にも 5-3-3-2 および 5-3-3-4 で登録した両 Peer Name が表示されていることをご確認下さい(右図)。



どちらの Peer が Primary 役として動作しているのか、についての確認方法はアイコンから行なうことができます。上図では、Primary-EQ1 のアイコンは『走っている Coyote』なので、Primary 役であると分かります。逆に Backup-EQ2 のアイコンは『座っている Coyote』なので、Backup 役として待機していることが分かります。

(※ [2-1-3](#) の “failover mode” でも同様の確認が可能です)

## APPENDIX A セッション維持動作解説

### A-1 セッション維持とは

Equalizerは負荷分散を行なうため、クラスタへ到達したクライアントのリクエストをクラスタ所属のサーバに対して振り分けます。4-7-1にある負荷分散ポリシーによって、振り分け先サーバはアクセスした瞬間に決定されます。

しかし各サーバが、以前に行なった通信のユーザ情報を個別に参照しなくてはいけないケースがあります。例えばショッピングサイトで買い物を行なっている場合など、ユーザのログイン情報やユーザがどの品物をショッピングカートに入れたかという情報は、サーバとクライアントが共有しなくてはなりません。

このようにサーバが固有情報を保持し、あるクライアントは常に同一サーバにアクセスする必要がある場合、負荷分散ポリシーによってランダムにサーバを選択することは出来ません。この、以前にアクセスしたサーバに次回以降も引き続いてアクセスを行なう動作をセッション維持といいます。

**注意： Equalizer はユーザのログイン情報や、ショッピングカートの情報などのセッション情報を認識することはありません。 Equalizer が提供する「セッション維持」とはアクセスするクライアントと振り分けられるサーバとの紐付けです。**

**これは、同一ユーザが前回のアクセス時とは別の TCP セッションを使用しクラスタにアクセスした場合でも、そのユーザが特定のサーバに振り分けられる必要があると IP レベル・HTTP レベルで判断するということです。**

### A-2 Equalizerが提供するセッション維持方法

Equalizer が提供するセッション維持機能は、クラスタによって異なります。

クラスタ	セッション維持方法	セッション維持動作	解説
L4/TCP L4/UDP	sticky time	クライアントの送信元 IP アドレスを判別しセッション維持を行なう	A-3
L7/HTTP L7/HTTPS	cookie	Equalizer がセッション維持用 Cookie をクライアントに付与することでセッション維持を行なう	A-4

sticky time や cookie によるセッション維持は、Hot Spare や Quiesce として設定したサーバに対しては優先して適用されます。例えば、クライアントがサーバへセッション維持されている状態で該当サーバを Hot Spare に設定変更した場合、通常(他にアクティブなサーバがクラスタ内に存在する場合)では Hot Spare サーバへは通信が振り分けられませんが、セッション維持されたクライアントは Hot Spare サーバへ振り分けられます。

## A-3 sticky timeによるセッション維持

L4クラスタの動作では、Equalizer はリクエストしてくるクライアントの送信元 IP アドレスを Sticky テーブル情報として記録します。次回以降のリクエスト送信元 IP アドレスがこの Sticky テーブルに記載されている場合は、前回振り分けたサーバに再度振り分けを行なうことでセッション維持動作を実現します。

### A-3-1 sticky timeの設定

設定は各クラスタ個別に行いません、設定箇所は [4-4-1-3](#) を参照して下さい。

sticky time は秒数で指定しますが、これは初回のアクセス時からの秒数ではありません。最終的に行なわれたアクセスからの秒数になります。さらに厳密には TCP セッションが終了してから秒数のカウントダウンが開始しますので、HTTP/1.1 の KeepAlive などにより TCP セッションが KeepAlive タイムアウト時間内でクローズされずに残っている場合はカウントが開始されず、TCP セッションが終了してからカウントが行なわれます。

### A-3-2 sticky timeの注意点

クライアントの送信元 IP アドレスを判別しセッション維持を行なうことから、クライアントの IP アドレスが同一になってしまう環境などに於いては sticky によるセッション維持を行なうことは難しくなります。以下の例を参照して頂き、該当する場合は L7 クラスタを使用するなど、別途セッション維持の方法をご検討下さい。

- ・ クライアントと Equalizer の間にリバース Proxy 等が存在し、クラスタへアクセスする IP アドレスが特定の IP アドレスに NAT 変換されてしまう場合。
- ・ 携帯電話からのアクセスは、通信キャリアのゲートウェイアドレスに変換されてしまうため、送信元 IP アドレスが偏る可能性があります。
- ・ 移動している携帯電話などは、通信する基地局が切り替わった際に送信元 IP アドレスが切り替わる場合があります。このように送信元 IP アドレスが途中で変わる状況に

おいては、sticky によるセッション維持に問題が出る可能性があります。

### A-3-3 inter-cluster sticky設定について

複数のクラスタで同一の IP アドレスを使用し、個別のポート番号でサービスを行なっている場合にクラスタ間で sticky テーブル情報を共有することが可能です。sticky time によるセッション維持を設定している場合にのみ設定可能になります。以下の例では 80 番(HTTP)および 443(HTTPS)のサービスを行なっている2つのクラスタがあります。

■クラスタ “WebHTTP” (192.168.200.1 :80)

サーバ1:192.168.1.10

サーバ2:192.168.1.11

■クラスタ “WebHTTPS” (192.168.200.1 :443)

サーバ1:192.168.1.10

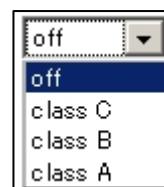
サーバ2:192.168.1.11

上記例に於いてinter-cluster stickyを有効にすることで、“WebHTTP” に対して80番でアクセスしたクライアントが、その後 “WebHTTPS” に443番でアクセスした場合に同じサーバへ割り振ることが可能になります。

### A-3-4 sticky network aggregation設定について

クライアントの送信元 IP アドレスをネットワークセグメント単位で判断し、同一のサーバへ割り振る際に使用します。例えば複数の Proxy サーバが存在し送信元 IP アドレスが固定されない場合などに使用します。

クラスA, B, Cから選択します。設定箇所は [3-1-4](#) を参照して下さい。



### A-3-5 sticky テーブル情報の同期について

冗長化構成時、2台のEqualizer間ではStickyテーブル情報は同期されません([5-2-5](#) も併せて参照下さい)。EqualizerがFailoverすると、既存で行なわれていた通信も新規リクエストとして処理されます。

### A-3-6 サーバ単位のセッション維持設定について

通常、セッション維持はクラスタ単位で設定しますが、サーバ単位でセッション維持動作の有効・無効を選択することが可能です。詳細は [4-8-8](#) のdont persist解説をご参照下さい。

## A-4 cookieによるセッション維持

L7/HTTP・HTTPS クラスタでは、セッション維持方法として cookie を付与します。初回のリクエストで Equalizer が付与した cookie を次回リクエストの HTTP ヘッダに埋め込んで通信が行なわれるため、Equalizer は cookie 情報を確認し同じサーバへ振り分けることが実現できます。

L7/HTTPS クラスタの場合は、SSL 複合処理を行ってから cookie 情報を確認し、クライアントへ通信を戻す際には cookie を付与してから SSL 暗号処理を行いません。従って L7/HTTP クラスタと同様に cookie によるセッション維持動作を行なうことが可能です。

### A-4-1 cookieの設定

設定箇所およびパラメータについては [4-5-1-3](#) を参照下さい。デフォルトでは cookie によるセッション維持は有効になっています。

### A-4-2 Equalizerのcookieとサーバのcookieの違い

Equalizer が付与する cookie はセッション維持に使用する cookie ですので、サーバが発行する cookie とは使用目的が違います。Equalizer はサーバの cookie に対しては書き換え・削除等の動作は一切行わず、自身が付与した cookie のみ確認を行います。

サーバが set-cookie をした場合にのみ、Equalizer が cookie を付与する設定は [4-5-1-3](#) の always 設定をご確認下さい。

### A-4-3 Equalizerのcookieの詳細解説

Equalizer が付与する cookie には クラスタ・サーバの情報が記載されていますので、クライアントが cookie を保持した状態でリクエストをすることで、Equalizer は振り分け先サーバを判別することが可能です。実際に付与される Equalizer の cookie は例えば以下のようになります。

Coyote-2-a0f648f=a0f65d2

cookie が付与される際の通信フローについては以下の図を参照して下さい。



#### A-4-4 複数クラスタ間のcookie動作について

A-4-3 の解説の通り、cookie にはクラスタ・サーバの情報が記載されていますが、ポート番号については認識していません。従って、同一 IP アドレスの L7/HTTP・HTTPS クラスタが複数ポート番号にまたがってサービスを提供している場合は同じ cookie を使用することができます(サーバ IP アドレスが同一である必要があります)。A-3-3 と同じ例ですが、下記のように2つのクラスタが同一サーバを所属させてサービスをしている場合、クラスタ “WebHTTP” で発行された cookie は、クラスタ “WebHTTPS” でも認識することができます。

■クラスタ “WebHTTP” (192.168.200.1 :80)

サーバ1:192.168.1.10

サーバ2:192.168.1.11

■クラスタ “WebHTTPS” (192.168.200.1 :443)

サーバ1:192.168.1.10

サーバ2:192.168.1.11

#### A-4-5 冗長化構成時のcookie動作について

cookie にはクラスタ・サーバ情報が含まれている為、冗長化構成時に Equalizer が Failover したとしてもクライアントが cookie を HTTP リクエストヘッダ内に挿入していれば問題なく Equalizer は判断し同じサーバへ振り分けることが出来ます。

L4クラスタの sticky の設定では、sticky テーブル情報を Failover ペアが共有しないために Failover 後はセッション維持を行なうことが出来ませんが、L7クラスタの cookie を使用することで実現が可能です。

#### A-4-6 once only使用時のcookie動作について

L7HTTP/HTTPSクラスタではonce onlyと呼ばれる設定パラメータがあります([4-5-1-5 参照](#))。once only を有効にした状態で、1つのTCPセッション内で複数のHTTPリクエストが行なわれた場合、Equalizerは先頭リクエストのヘッダ情報のみ確認します。また、先頭リクエストに対してのみcookieを付与します。

複数クライアントの HTTP リクエストが1つの TCP セッション内にまとめられてしまう環境などでは、正常にセッション維持を行なう為に once only の設定を無効にする必要があります。

また先頭リクエストに対してのみ cookie 付与が行われる為、cookie age 設定で有効期限を設定している場合に、1つの TCP セッションで通信を行なっている最中に cookie 有効期限が過ぎてしまうことがあります。ブラウザは有効期限が過ぎた cookie をリクエストヘッダに挿入しない

ため、同一のクラスタに対して新規に TCP セッションを開いた場合にセッション維持が行なえなくなります。

once only 設定を無効にする、あるいは cookie age 設定を 0 秒にすることで、このようなケースを防ぐことが可能です。

#### A-4-7 サーバ単位のセッション維持設定について

通常、セッション維持はクラスタ単位で設定しますが、サーバ単位でセッション維持動作の有効・無効を選択することが可能です。詳細は [4-8-8](#) の dont persist 解説をご参照下さい。



## APPENDIX B CSR作成手順

### B-1 Equalizer サーバ証明書インストール手順について

HTTPS クラスタへサーバ証明書をインストールする手順について説明します。  
作成する CSR(Certificate Server Request) は RSA 3DES 2048bit で暗号化することを前提として  
います。CSR を提出する CA(認証局) が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ので、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。

### B-2 CSR作成手順

サーバ証明書を発行するには CSR を作成し CA へ提出する必要があります。CSR 作成は  
Equalizer 上で行うことができます。CA が提示している作成手順と異なる場合は、その手順にて  
作成してください。

1. シリアルコンソール画面へシリアルケーブル または SSH にてログインします、ログインは  
root にて行って下さい。(SSH の場合はログイン後に su にて root 権限に切り替えます)。
2. ディレクトリを移動します。  
# 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)  
※下記エラーが表示されますがrand.dat が作成されていれば作業に問題はございません。  
snmpctl: Operation not supported  
switchc\_server.sock: Operation not supported  
switchd\_server.sock: Operation not supported
4. 2048bit 3DES により秘密鍵を生成します  
# openssl genrsa -rand rand.dat -des3 2048 > 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ます。  
※ 鍵長を 1024bit で作成する場合は以下のように入力します  
# openssl genrsa -rand rand.dat -des3 1024 > key.pem  
※ XCEL カードが搭載された SI シリーズ筐体で 2048bit 鍵長の秘密鍵を使用する場合は、  
Composite ファイルをアップロードする際 “use secure key storage”を無効化して下さい。

- ※ 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 へ進みます。)  
# 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。
    - 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
    - 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
  7. 4 で入力したパスフレーズを入力します  
証明書情報(ディスティングイッシュネーム)を入力します。  
CA に申請する情報を入力します。

### 参考例

表示される項目	日本語訳	入力例
Country Name(2 letter code)	<国>	JP
State or Province Name	<都道府県名>	Tokyo
Locality Name	<市区町村名>	Chiyoda-ku
Organization Name (eg, company)	<正式英語組織名>	Example Inc.,
Organizational Unit Name (eg, section)	<部門名>	System 1
Common Name (eg, YOUR name)	<URL<FQDN>>	www.example.com
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 の入力は省略します。

何も入力せず Enter キーを押し決定します。

Equalizer 上から FTP コマンドを使用し、作成した CSR および 秘密鍵 を外部へ転送します上  
記 CSR を元に、CA へサーバ証明書の発行を申請します。

また 次のコマンドにて表示されるテキストをコピー&ペーストしていただくことでも可能です。

```
# cat key.pem
# cat csr.pem
```

必要な証明書の枚数などは CA により異なりますので、申請先 CA へ直接お問い合わせ下さい。

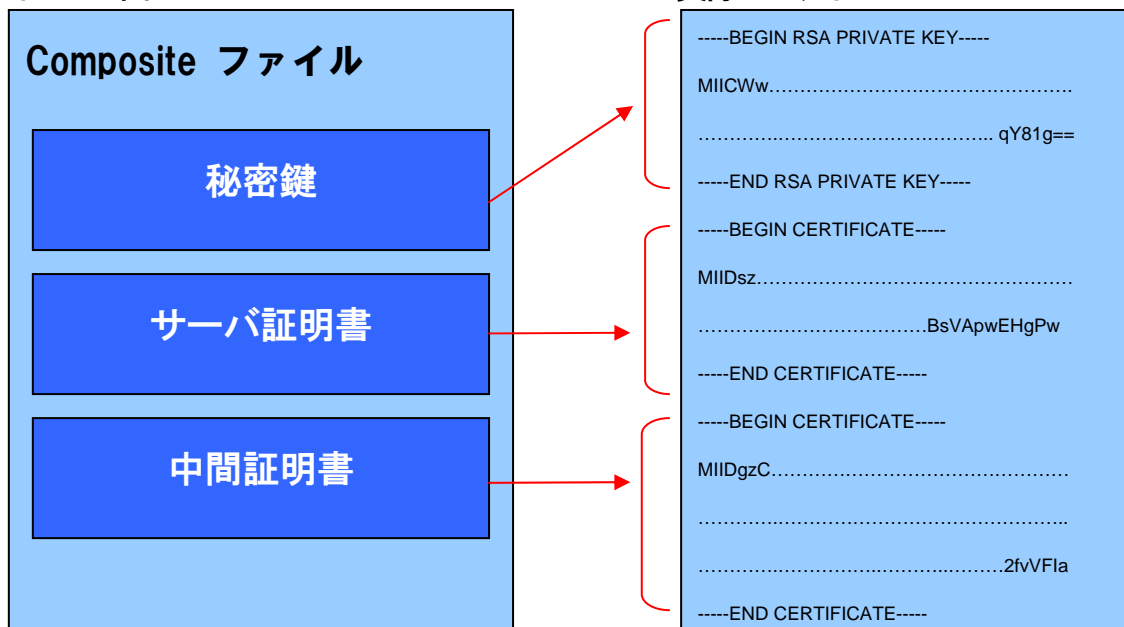
### B-3 Compositeファイル 作成手順

Equalizer へアップロードするファイルは Composite ファイル と呼ばれます。

これは次の3点をあわせたテキスト形式ファイルです。拡張子 “.pem” にて保存します。

- ・ 秘密鍵
- ・ CA より発行されたサーバ証明書
- ・ 中間証明書

イメージ図

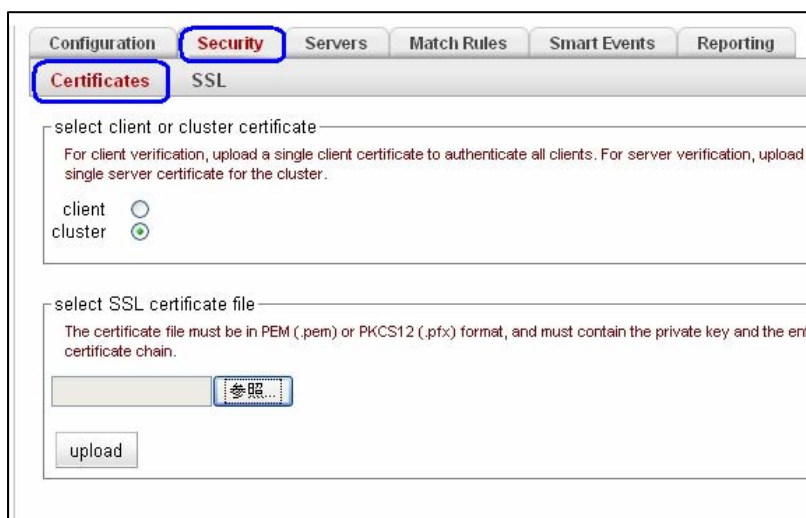


## B-4 Compositeファイル アップロード手順

Composite ファイル は Equalizer の Web 管理画面からアップロードします。  
 ブラウザから ユーザ touch または編集ユーザ にて Equalizer へログインして下さい。左フレームから、該当 HTTPS クラスタを選択します。SSL サーバ証明書が無い状態では、SSL certificate warning が表示されます。



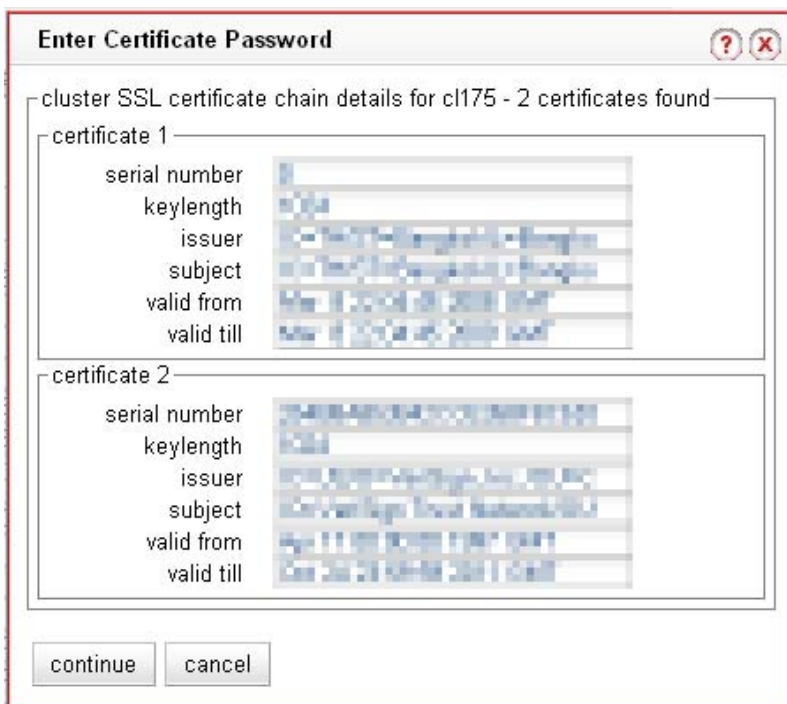
表示された画面から Security タブから Certificates を選択すると、下記のように“参照”ボタンが表示されますので、ローカル PC 上から Composite ファイルを選択し、“upload” ボタンを押します。



CSR 作成時にパスフレーズを有効にした場合は、アップロード時にパスフレーズ入力画面が表示されます(右図)。



continue をクリックすると、インストールする証明書の内容が表示されますので、確認します。



continue を押して決定することで、サーバ証明書のアップロードは完了です。

クラスタ内のサーバ証明書情報を確認すると Certificate が反映されています。certificate 1 がサーバ証明書、certificate 2 が中間証明書 となります。 証明書の内容や、有効期限なども確認可能です。

サーバ証明書をアップロード後、該当クラスタに SSL certificate warning が表示されなくなったことを確認します。



## B-5 サーバ証明書に関する注意事項

- ・ HA 構成の場合、サーバ証明書情報は同期対象ではないため Primary/Backup 両方にアップロードする必要があります。
- ・ 機器のコンフィグ情報である「バックアップファイル」にはアップロードしたサーバ証明書の情報はセキュリティの観点から含まれません。
- ・ SI シリーズで Xcel カードを使用している場合は、デフォルト設定で秘密鍵は Xcel カード内に格納されます。このため、Web 管理画面・コンソール画面から秘密鍵情報を参照することは出来ません。GX シリーズでは Equalizer の内部に保存されます。
- ・ ハードウェア故障などで、機器交換を行った場合は「バックアップファイル」にて設定をリストアした後、サーバ証明書を再度アップロードする必要があります。

## 改定履歴

改定番号	改定内容	改定日
1.0	新規作成しました。	2009/09/01
1.1	ファームウェア 8.5.1c に対応しました。 APPENDIX B の内容を更新しました。 文書内のリンクを一部修正しました。	2010/03/12
1.2	APPENDIX B の内容を更新しました。	2010/06/24