



# ロードマスターシリーズ バージョン 5.1 用

## アプリケーション、設置&設定ガイド

**Revision 1.0**

1. Revision 1.0 発行 (初版)

2011年2月21日

商標

Copyright © 2000 – 2010 KEMP Technologies, Inc. All rights reserved.

ロードマスター製品のソフトウェアと関係文書の全ての所有権は、KEMP テクノロジー社が保有しています。

ロードマスター負荷分散装置の使用は、ライセンス契約の対象になります。

ここに記載されている内容については、事前の連絡なしで変更されることがあります。

会社名の使用例は、注意書きが無い限り創作によるものです。

Sun, Sun Microsystems, Sun のロゴ, Solaris, SunOS 及び Java は、米国、もしくは他の国の Sun マイクロシステムズ (株) の商標、もしくは商標として登録されています。

UNIX は、X/Open Company Ltd の商標です。 .

IBM は、International Business Machines Corporation の商標です。

Microsoft (マイクロソフト) , Windows (ウィンドウズ) 及び Windows NT (ウィンドウズ NT) は、Microsoft Corporation の商標です。

Linux は、Linus Torvalds の登録商標です。

Intel (インテル) と Pentium (ペンティアム) は、Intel Corporation の登録商標です。

他の全ての商標、もしくは登録商標は各々の所有者の所有物です。

<b>I.</b>	<b>アプリケーションガイド</b> .....	<b>9</b>
<b>1</b>	<b>はじめに</b> .....	<b>9</b>
1.0	感謝の意.....	9
1.1	このガイドの構成について.....	9
1.2	実モデルとこのガイド内で使われているモデルの違い.....	9
1.3	使用されている用語と略語.....	9
<b>2</b>	<b>ロードマスターの概要</b> .....	<b>12</b>
2.1	負荷分散とその利益.....	12
2.2	付設を始める前の考慮点.....	13
2.3	シンプルな負荷分散構成.....	15
2.4	ロードマスター負荷分散機能.....	16
<b>3</b>	<b>ロードマスター・ネットワーク・トポロジー</b> .....	<b>19</b>
3.1	1アーム・バランサー.....	19
3.2	2アーム、マルチアーム・バランサー.....	21
3.3	ダイレクト・サーバ・リターン (DSR) の一例.....	24
<b>4</b>	<b>その他のネットワーク問題点</b> .....	<b>34</b>
4.1	S-NAT.....	34
4.2	デフォルト・ゲートウェイと追加ルート.....	35
4.2	デフォルトゲートウェイのイーサポート指定.....	37
4.3	リモート・リアルサーバのサポート.....	37
<b>5</b>	<b>シングル/デュアル ユニット構成</b> .....	<b>39</b>
5.1	シングル・ユニット構成.....	39
5.2	ハイ・アベイラビリティ (HA) 構成.....	39
<b>6</b>	<b>負荷分散方式 (Scheduling Method)</b> .....	<b>42</b>
6.1	ラウンドロビン (Round Robin).....	42
6.2	重み付けラウンドロビン (Weighted Round Robin).....	42
6.3	最小接続 (Least Connection).....	42
6.4	重み付け最小接続 (Weighted Least Connection).....	43
6.5	エージェント・ベースのアダプティブ配分 (Adaptive).....	43
6.6	固定重み付け配分 (Fixed Weighted).....	44
<b>7</b>	<b>パーシステンス (Persistence)</b> .....	<b>45</b>
7.1	パーシステンスの概要.....	45
7.2	パーシステンスの必要性.....	46
7.3	設定.....	46
7.4	タイムアウト (Timeout).....	47
7.5	レイヤ4パーシステンス方式.....	48
7.6	レイヤ7パーシステンス方式.....	49
7.7	パーシステンスと HTTPS/SSL.....	52
7.8	ポート・フォローウィング (Port Following).....	53

<b>8</b>	<b>アプリケーション・フロントエンド (AFE)</b> .....	<b>55</b>
8.1	ネットワーク侵入防止システム (IPS) .....	55
8.2	キャッシング .....	58
8.3	データ圧縮 .....	60
<b>9</b>	<b>ルールベースのコンテンツ・スイッチ</b> .....	<b>63</b>
9.1	用語 .....	64
9.2	コンテンツスイッチの制約 .....	64
9.3	コンテンツスイッチの使用 .....	64
9.4	コンテンツルールのセットアップ .....	64
9.5	バーチャルサービスへの適用 .....	66
<b>10</b>	<b>ヘルスチェック</b> .....	<b>68</b>
10.1	サービス、ノンサービス・ベースのヘルスチェック .....	68
<b>11</b>	<b>SNMP サポート</b> .....	<b>71</b>
11.1	SNMP 経由のロードマスター・パフォーマンス・マトリックス .....	71
11.2	SNMP を介してのロードマスター・イベント・トラップ .....	72
11.3	参考 .....	73
<b>12</b>	<b>ロードマスターのソフトウェア・アップグレード</b> .....	<b>74</b>
12.1	オンラインによるアップグレード .....	74
<b>13</b>	<b>Miscellaneous</b> .....	<b>75</b>
13.1	リモート Syslogd サポート .....	75
13.2	ライセンスの入手方法 .....	75
13.3	バックアップとリストア .....	77
13.4	システム・リカバリー .....	78
13.5	L4 と L7 のバーチャルサービス間の相互可動性 .....	79
13.6	Web ユーザーインターフェース (WUI) ルート証明書のインストール .....	79
13.7	ログ情報 .....	79
<b>14</b>	<b>ユーザ管理</b> .....	<b>82</b>
14.1	Roles/Permission .....	82
<b>15</b>	<b>ボンディングと VLAN</b> .....	<b>84</b>
15.1	概要 .....	84
15.2	必要とする規格 (スイッチ側) .....	84
15.2.1	スイッチ側の設定 .....	84
15.3	ボンディング／チーミング (802.3ad/Active-Backup) .....	85
15.3.1	ボンディング／チーミング設定方法 .....	85
15.3.2	ボンディング／チーミングの解除 .....	86
15.4	VLAN タギング .....	87
15.4.1	VLAN タギングの設定方法 .....	87
15.4.2	VLAN タグの削除 .....	87
<b>16</b>	<b>付録 I</b> .....	<b>88</b>
16.1	エージェントベースのアダプティブ負荷分散用 API .....	88

16.2	HTTP サーバでのサーバクッキーサポート .....	91
16.3	MIB ツリー .....	91
<b>II.</b>	<b>インストール&amp;設定ガイド.....</b>	<b>92</b>
<b>A.</b>	<b>開始前に.....</b>	<b>92</b>
1	ロードマスター装置 .....	92
1.1	送付品 .....	92
1.2	ロードマスター2200 ハードウェア .....	92
1.3	ロードマスター2600 ハードウェア .....	93
1.4	ロードマスター3600 ハードウェア .....	94
1.5	ロードマスター5500 ハードウェア .....	95
2	ハードウェアの接続 .....	96
2.1	eth0 の接続 .....	96
2.2	eth1 の接続 .....	96
<b>B.</b>	<b>シングル構成の初期設定 (non-HA) .....</b>	<b>96</b>
1	ログインとライセンスキー入力 .....	96
<b>C.</b>	<b>ハイアビリティ構成での初期設定 (HA).....</b>	<b>97</b>
1	HA-1 のログインとライセンスキー入力.....	97
2	HA-2 へのログインとライセンスキー入力.....	97
<b>D.</b>	<b>クイック・セットアップ (Quick Setup) .....</b>	<b>98</b>
<b>E.</b>	<b>メインメニュー.....</b>	<b>100</b>
1	設定メニューの基本 .....	101
1.1	Quick Setup “クイックセットアップ” .....	101
2	Service Management (CLI) “サービス・マネージメント” .....	101
3	Local Administration “ローカル・アドミニストレーション” .....	102
3.1	Set Password “パスワードのセット” .....	102
3.2	Set Date/Time “日時の設定” .....	102
3.3	Set Keyboard Map “キーボードのマッピング” .....	102
3.4	Backup/Restore “バックアップ/リストア” .....	103
3.5	Remote Access Control “リモート・アクセス・コントロール” .....	103
4	Basic Setup “基本設定” .....	104
4.1	Network configuration “ネットワーク設定” .....	104
4.2	Hostname Configuration “ホスト名の設定” .....	104
4.3	DNS configuration “DNS 設定” .....	104
4.4	Routing Configuration “ルーティング設定” .....	105
4.5	Email Configuration “E メールの設定” .....	105
4.6	Enable L7 transparency “L7 モードのトランスペアレンシー設定” .....	106
4.7	Using X-Forwarded-For Header “「X-Forwarded-For」のヘッダーへの挿入” .....	106
4.8	Adding/No Port Added to Active Cookie “アクティブクッキーへのポート番号付与” .....	107

4.9	Support VS/Subnet Originating Requests “ソース IP アドレスの VS への変更をサポート”	107
5	Extended Configuration “拡張設定”	107
5.1	Interface Control “インターフェース・コントロール”	107
5.2	Enable/Disable S-NAT “S-NAT 機能の有効/無効化”	107
5.3	Syslogd Configuration “シスログ・サーバ設定”	108
5.4	SNMP metrics “SNMP メトリックス”	108
5.5	SNMP traps “SNMP トラップ”	109
5.6	Enable/Disable L7 persistency state failover “L7 パーシステンスのステータスフル・フェイルオーバーの有効/無効化”	109
5.7	Enable/Disable L4 connection state failover “L4 接続ステータスフル・フェイルオーバーの有効/無効化”	109
5.8	Multicast Configuration “マルチキャスト設定”	110
5.9	HA Parameters “HA 関連パラメータ”	110
6	Packet Filter & BalckLists “パケットフィルターとアクセス管理”	111
6.1	Access control Lists “アクセス・コントロール・リスト”	111
7	Utilities “ユーティリティ”	113
7.1	Software Upgrade “ソフトウェアの更新”	113
7.2	Transfer Protocol “転送用プロトコール”	113
7.3	Network Time Protocol Host “NTP サーバの設定”	114
7.4	SSL certificate administration “SSL 証明書管理”	114
7.5	Update License “ライセンスの更新”	114
7.6	L7 Idle Timeout “L7 セッション用アイドルタイマー”	114
7.7	Diagnostics “診断ツール”	115
8	Reboot “リブート”	115
9	Exit LoadMaster Config “設定画面よりの退出”	116
<b>F.</b>	<b>ロードマスター設置用質問表</b>	<b>117</b>
1	単一ロードマスター・バランサー・ソリューション	117
2	HA デュアル・ロードマスター・バランサー・ソリューション	117
<b>III.</b>	<b>コマンドライン・インターフェース参照ガイド</b>	<b>118</b>
1	最上階層のコマンド	118
2	“Adaptive” のコマンドセット	119
3	“Healthcheck” のコマンドセット	120
4	“Rules” のコマンドセット	121
5	“Rules” 編集コマンドレベル	122
6	“VIP” のコマンドレベル	123
7	“Real Server” コマンドレベル	127
<b>IV.</b>	<b>ウェブ・ユーザ・インターフェース (WUI) 設定ガイド</b>	<b>129</b>
<b>A.</b>	<b>用語と略語</b>	<b>129</b>
<b>B.</b>	<b>ファーストトラック (Fast Track)</b>	<b>130</b>
1	ログインの仕方	130

2	シンプルなバーチャルサービス作成.....	131
3	コンテンツルールの作成.....	134
4	SSL アクセラレーション.....	138
5	マイクロソフト・ターミナル・サービス負荷分散.....	139
<b>C.</b>	<b>全メニューツリー.....</b>	<b>144</b>
1	Home.....	144
2	Virtual Services (バーチャルサービス).....	144
2.1	Add New (追加).....	144
2.2	View/Modify Existing (Generic Service Type) “既存の表示/変更 (一般サービスタイプ)”.....	145
2.3	View/Modify Existing (HTTP/HTTPS Service Type) “既存の表示/変更 (HTTP/HTTPS サービスタイプ)”.....	150
2.4	View/Modify Existing (Remote Terminal Service Type) “既存の表示/変更 (リモートターミナルサービスタイプ)”.....	154
2.5	Real Server for this Virtual Service (リアルサーバのアサイン).....	156
3	Statistics (統計情報).....	158
3.1	Global Metrics (システム統計).....	158
3.2	Real Server Metrics (リアルサーバ統計).....	158
3.3	Virtual Service Metrics (バーチャルサーバ統計).....	158
4	Real Servers (リアルサーバ).....	158
5	Rule & Checking (ルールとチェック).....	159
5.1	Content Rules (コンテンツスイッチ用ルール).....	159
5.2	Check Parameters (アダプティブ、ヘルスチェック用パラメータ).....	160
6	Certificate (証明書).....	161
6.1	Intermediate Certs. (インターミディエート証明書).....	161
6.2	Generate CSR (CSR 作成).....	161
6.3	Backup/Restore Certs. (証明書のバックアップ/リストア).....	161
7	System Configuration (システム用設定).....	162
7.1	Interface s (インターフェース).....	162
7.2	Local DNS Configuration (ローカル DNS 設定).....	162
7.3	Route Management (ルート管理).....	163
7.4	Access Control (アクセス管理).....	163
7.5	System Administration (システム管理).....	164
7.6	Logging Options (ログオプション).....	166
7.7	Miscellaneous (その他).....	170

# I. アプリケーションガイド

## 1 はじめに

### 1.0 感謝の意

この度は、KEMPテクノロジー社のロードマスターシリーズをお買い上げ頂きまして、誠に有難うございます！

私たち KEMP テクノロジー社及び当社パートナー各社の社員一同、ロードマスターが貴社ビジネスの成功に貢献できますことを願っております。

### 1.1 このガイドの構成について

ロードマスターシリーズ アプリケーション、設置&設定ガイドは4つの大きなセクションにより構成されています。

**アプリケーションガイド:** 負荷分散の主な機能と、ロードマスターのハードウェア構成要素のセットアップについて述べられています。

**設置&設定ガイド:** ロードマスターを、インストールする方法と設定を行う各パラメータについて説明をしています。

**コマンドライン・インターフェース:** コマンドラインを使って設定を行う方法について説明しています。

**WUI 設定ガイド:** ウェブユーザインターフェース (WUI) を使って管理する方法について説明しています。

### 1.2 実モデルとこのガイド内で使われているモデルの違い

このガイドで使用されているスクリーンショットや写真は、お買い上げ頂いたモデルと同じでない部分があるかもしれませんがご了承ください。

### 1.3 使用されている用語と略語

アクセスコード: アクセスコードは、ロードマスターが初期設定中に生成する各ハード特有のユニークなコード。ライセンスキーを申請する場合には、このコードが必要になります。

AFE: キャッシング、圧縮、及び侵入防止機能等のアドバンス・フロントエンド機能。

balancer、分散装置: ネットワークより入ってくるトラフィックをサーバに振り分けるネットワーク装置、もしくは概念。

ファームサイド、ファーム側: ロードマスターの、サーバファームに接続されているネットワークインターフェース。

フラットベース: バーチャルサービスとリアルサーバが同じサブネットにあるネットワーク形態。

HA: ハイ・アベイラビリティ、冗長構成。

ICMP: Internet Control Message Protocol

MIB: Management Information Base の略で、OID (object definitions) のデータベースオブジェクト定義を監視する SNMP マネージャーに必要な詳細情報。

NAT: Network Address Translation

NAT ベース: ロードマスターで、受信したリクエストの宛先 IP アドレスをリアルサーバの IP アドレスに変換するネットワーク形態。リアルサーバからの帰りのトラフィックは、ロードマスターを介して戻らなければならない。そして、その帰りのソース IP アドレスは、バーチャルサービス・アドレス (VIP) へ変換される。

ネットワークサイド、ネットワーク側: ロードマスターで、バーチャルサービスを収容しクライアントのリクエストを受け取るネットワーク・インターフェース。

1 アーム: 内向け、外向けの両方のトラフィックを 1 つのイーサポートを使って行うネットワーク形態 (フラットベースと同義)。

RS: リアルサーバ。サーバファームを構成する物理的なサーバマシン。

サービス: ネットワークに接続されるアプリケーション。

シェアード IP: 特定のインターフェース(例えばイーサ 0、イーサ 1)上で、保障された利用可能アドレス。HA 構成の場合のみ使用する。

SCP: SSH 接続時の Secure copy command

SNMP: Simple Network Management Protocol。TCP/IP ネットワークを管理するネットワーク・プロトコル。このプロトコルは、MIB によって与えられるデータオブジェクトへのアクセスを可能にする機能を持っている。

S-NAT: ソース IP アドレスのネットワークアドレス変換。

SSH: Secure Shell Protocol

2 アーム: バーチャルサービス・アドレス (VIP) とリアルサーバのサブネットが異なるネットワーク形態。

UTC: Universal Time Coordinated

- VIP:** Virtual IP Address: ロードマスター上で定義されるサービスの IP アドレス。
- VS:** バーチャルサービス。ロードマスター上でサーバファームのサービスに到着させるためのエントリー（クラスター）。
- WUI:** Web User Interface。ウェブブラウザを介してロードマスターを管理するインターフェース。

## 2 ロードマスターの概要

### 2.1 負荷分散とその利益

インターネットとネットワークベースのアプリケーションは、日々より精巧になっており、これらのサービスとアプリケーションの管理も、それに従いカバーする範囲がより広く、複雑になって来ています。その結果、ユーザが期待、要求している下記のサービス品質に対して、どのように対応するかがキーポイントになっています。

- ▶ サーバマシンの拡張性 – サービスとアプリケーションの拡張の必要性が発生した時、それらを提供するマシンのハードウェア増強をどれだけ容易に行えるかの要求については限りがありません。そして、ハードウェアの拡張制限（限界）に遭遇しても継続的に使用できることや、それらの拡張を行うときにシステム停止したくないというのがユーザの希望です。
- ▶ サービスとアプリケーションの冗長性 – サービスの可用性が容易にビジネスの成功を決定する銀行、B2B や、VoIP などのミッションクリティカルなインターネットをベースとしたネットワークでは、1つのハードウェアの故障でも引き続きサービスの提供が行われることが要求されます。
- ▶ 高い柔軟性– インターネットサービスとアプリケーションの多様性とその数の増大に対して、環境の強固性を危険にさらすことなく、その要求に対するリソースを素早く、又、巧みに行える環境を持つことが、ネットワーク管理者にとって必須です。
- ▶ パフォーマンスの向上性 –ほんの少しの違いかもしれませんが、ミッションクリティカルなサービスやアプリケーションは、シビアなレスポンス時間の競争を要求します。

### ソリューション

負荷分散装置は、ネットワークを非常に強力にする装置です。それは、幾つかのマシンをあたかも1つのように見せる効力を持っているからです。これにより、1つのネットワークのサービスがずらりと並んだ実際のマシン群（サーバ、もしくはアプリケーションファームとも呼ばれる）に分配されます。負荷分散装置は、1つのネットワークサービスへのリクエストを、多彩でインテリジェントな負荷分散方式を使って特定のサーバへと流します。このように、近年幅広く採用されて成功している負荷分散技術は、数々の利益をもたらします。

- ▶ サーバマシンの拡張性 – サービス追加の要求に対して、ファーム内にサーバマシンを追加するだけで達成できる。前もって、かなりのトラフィックを想定したリソースの多い高価なサーバに投資して、後で結局それほどリソースが使われないということを防げる。
- ▶ サービスとアプリケーションの高可用性 – ファーム内の複数のサーバマシンにより、サービスが提供されることで一台のサーバがダウンしてもサービスそのものが停止したり、パフォーマンスが急激に悪化することなく継続してサービスを提供できる。

- ▶ 柔軟性の拡張 – 要求に合わせて、ファーム内のサーバ追加やサーバの撤去など容易に実施することが可能であり、効果が直ぐに発揮される。サービス（負荷分散装置が使われている環境では、バーチャルサービスとも呼ばれる）でのリソースの利用を最大にできる。
- ▶ パフォーマンスの改善 – インテリジェントな負荷分散アルゴリズムが、サーバファーム内で最も効率的に処理するマシンにリクエストを振り分けるように保障する。

ロードマスターは、高トラフィック負荷とミッションクリティカルなアプリケーションに対して、更なる信頼性、柔軟性、及び高い費用対効果ソリューションを提供し、結果として低いTCOで高いサービス品質（QoS）を実現させます。

## 2.2 付設を始める前の考慮点

もし、既にサーバと負荷分散装置の組み合わせによるセットアップ方法と基礎的な負荷分散装置の機能について理解している場合は、このセクションはスキップしてください。

インストール&設定ガイドに、ロードマスターによってサポートされている負荷分散用サービス（バーチャルサービス）のインストールと設定について、その方法を説明しています。もし、初めてロードマスターを設置する場合は、事前に下記のロードマスターのドキュメントでカバーされている内容を理解されることをお勧めします。

どのロードマスターのネットワークトポロジーが自分のアプリケーションに最適か？

「このガイドのセクション3を参照」

リアルサーバは、公にルーティングできるIPアドレスを必要としているか、それともプライベートなネットワークセグメント上でロードマスターの後ろに隠れたものでよいか？

「このガイドのセクション3を参照」

負荷分散をしようとしているアプリケーションは、装置とリアルサーバが同じサブネット（フラットベース）内に共存するネットワーク形態を必要としているか？

「このガイドのセクション3を参照」

ネットワーク接続は、外部からファーム内に向かって行われると共に、ファーム内から外部に向かっても行われるか？

「このガイドのセクション4を参照」

アクティブ/スタンバイの冗長構成によるハイ・アベイラビリティのサポートが必要かどうか？「このガイドのセクション5を参照」

どのように今のアプリケーションを複数のリアルサーバに配置しようとしているか？

現状のアプリケーションのためには、どのようなバーチャルサービスが最適か？

「このガイドのセクション6を参照」

リアルサーバへの負荷分散は、ラウンドロビン方式でよいか、それともアプリケーションの見地からレポートを採取し、考慮点などをおかみ合わせて他の方法を選択すべきかどうか判断する？

「このガイドのセクション6を参照」

セッション維持は今のアプリケーションに必要なかどうか？

「このガイドのセクション7 & 8を参照」

IP アドレスによるセッション維持だけで十分だろうか、それともレイヤ7の見地から考慮した方法を取るべきかどうか？

「このガイドのセクション7 & 8を参照」

現在の SNMP 環境に、ロードマスターを統合させるべきかどうか？

「このガイドのセクション13を参照」

今のアプリケーションには、どのヘルスチェック方法が最適か？

「このガイドのセクション12を参照」

バーチャルサービスの設定にコマンドラインを使うのが良いか、それともウェブベースのインターフェースを使う必要があるか？

「コマンドラインインターフェース参照ガイドのセクション6とウェブユーザインターフェース (WUI) 設定ガイドを参照」

ロードマスターのイベントを既存の Syslog サーバにレポートしたいかどうか？

「このガイドのセクション15を参照」

CLI (コマンドラインインターフェース) でのリモートからのアクセスは必要か？

「インストール&設定ガイドのセクション3.5を参照」

ロードマスターの保守のために KEMP テクノロジー社のサイトへのアクセスを許可しておくべきか？

「インストール&設定ガイドのセクション3.5を参照」

## 2.3 シンプルな負荷分散構成

前述の各項目を考慮した負荷分散サイトの一例を下記に示します。

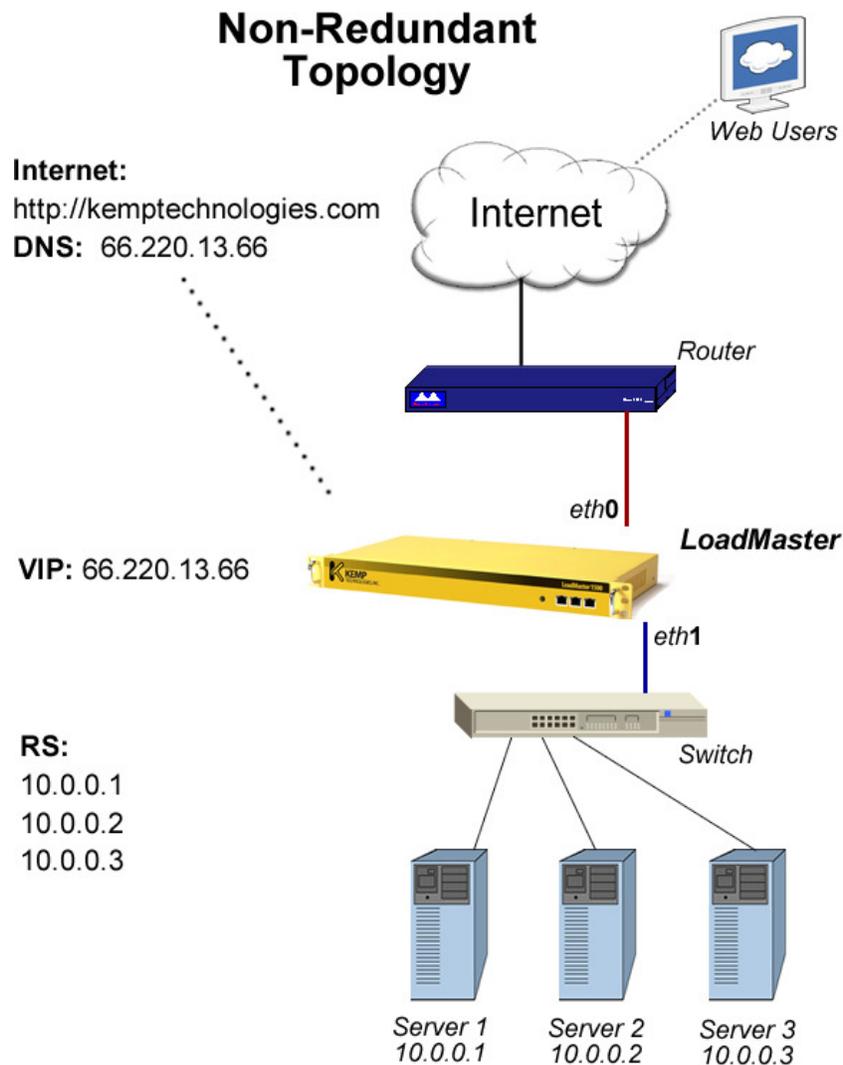


図 1: シンプルな負荷分散構成の一例

1つのバーチャルサービスが、HTTP サービスのために IP アドレス 66.220.13.66 を使って作成されています。

このバーチャルサービスは、入ってくるトラフィックを RS (リアルサーバ) 1、2、及び 3 へと分散されるように設定されています。

クライアントは、<http://www.kemptechnologies.com> へリクエストします。

リクエストされた URL が DNS サーバにより 66.220.13.66 に変換されます。

リクエストは、ロードマスターのネットワーク・インターフェース”eth0”を介してロードマスターへとルーティングされます。

ロードマスターは、ネットワーク・インターフェース “eth1”を介してサーバファームである 10.0.0.0 のサブネットに接続されています。

ロードマスターは、アドレス 66.220.13.66 のリクエストに対してコンテンツを返してくれる三台のリアルサーバがそのサブネット内にあることを知っています。

ロードマスターは、設定された負荷分散方式（例えば、重み付けラウンドロビン）に従って、3台の内の1台のリアルサーバへリクエストを振分けます。

## 2.4 ロードマスター負荷分散機能

ロードマスター負荷分散装置は、 balancer OS とウェブ・ユーザ・インターフェース (WUI) により、下記の機能を提供します。

### 2.4.1 バランサーOSベーシック

- TCP/UDP ベースのプロトコルのためのサーバ負荷分散
- NAT ベース・フォワーディングによるマルチアームの balancer /サーバファームのネットワーク・トポロジー。 NOTES 1. 参照.
- OS はフラッシュディスクよりブート。
- マルチアームでの S-NAT サポート。 NOTE2. 参照
- 1アームによる balancer とサーバファームのフラットベース・ネットワーク形態。
- ダイレクト・サーバ・リターン (DSR) のサポート。
- balancer のイーサポートの強制デュプレックスモード・オプション。
- 保守目的のリモート・アクセス許可オプション。
- VLAN タグのサポート。
- 外部サブネット上のリアルサーバサポート
- 設定変更可能なフレキシブルな HA 構成

- SSL 証明書管理
- リアルタイムな詳細統計と履歴
- 複数の管理用ユーザのサポート
- WUI 画面上のホバーヘルプ機能（英語）
- WUI による診断、及びデバッグ機能
- L4 及び L7 の接続／ユーザのドレイン停止
- HTTP ヘッダー・インジェクション
- ボンディング／リンク・アグリゲーション

**NOTES:**

1. リアルサーバとバーチャルサービスは、NAT のようなフォワーディング・メカニズムを使用して、お互いに論理上異なったネットワーク上に設置／設定されます。このために、ロードマスターは2つのイーサポートを使用します（2アームと呼ばれる）。又、外部ネットワークへの NAT 機能を用いることで、自身のポートにアサインしているサブネット以外のサーバもリアルサーバとして取り込めます。
2. S-NAT を有効にしていた場合リアルサーバからのインターネットへの接続時にソース IP アドレスとして、ロードマスターのイーサポート、もしくは VS に割当てられた IP アドレスを使うように指定できます。
3. フラットベース・トポロジーでは、リアルサーバとバーチャルサービスが同じ論理ネットワーク上に構成されます。
4. フル・デュプレックス・モード。

**2.4.2 負荷分散 (Scheduling) と L4/L7 セッション維持 (Persistence)**

- 5つの静的負荷分散方式
- エージェントベースの API による自動適応負荷分散方式
- 下記のセッション維持方式（パーシステンス）：

ソース IP アドレス

スーパーHTTP

サーバ（パッシブ）クッキー

サーバ（パッシブ）クッキー／IP アドレス

アクティブ（インサート）クッキー

アクティブ（インサート）クッキー／IP アドレス

ハッシュ全クッキー

ロードマスターシリーズ アプリケーション、インストレーション&設定ガイド

© 2011 KEMP Technologies Inc.

ハッシュ全クッキー/IP アドレス

URL ハッシュ

HTTP ホストヘッダー

HTTP クエリ部分ハッシュ

SSL セッション ID

ターミナルサービス (MS Windows Terminal Server 用)

ターミナルサービス/IP アドレス (MS Windows Terminal Server 用)

- セッション維持のためのポート・フォロワー (HTTP/HTTPS 用)
- SSL アクセラレーション

### 2.4.3 ヘルスチェックと可用性

- ICMP/TCP を用いたサーバマシンのヘルスチェック
- DNS, FTP, HTTP (1.0/1.1) , HTTPS, IMAP, NNTP, POP3, SMTP, TELNET、RDP のサービスチェック
- リアルサーバ障害時のサーバリストの自動再設定
- オプションによる HA 構成時のアクティブ/スタンバイ設定
- クッキー、もしくは TCP 接続のステートフル/ステートレス・フェイルオーバー (HA 構成で待機系への切り替え時のパーシステンスを保持する、もしくは保持しない接続)
- 高度な HTTP ヘルスチェック

### 2.4.4 管理

- ウェブベース・インターフェース (WUI) によるバーチャルサービスの作成、削除、及び編集
- コマンドライン・インターフェース (CLI) によるバーチャルサービスの作成、削除、及び編集
- パケット・フィルタ機能
- リモート Syslog サーバのサポート
- システム・イベントの E メールによる報知
- ロードマスター管理操作のためのリモートアクセス

- ▶ バックアップからのリストアの情報（全部かロードマスターの設定のみ、またはバーチャルサービスの設定のみ）の選択
- ▶ ロードマスターファームウェアのオンライン・アップグレード
- ▶ イベント・トラップ目的の SNMP、E メールサポート
- ▶ SNMP パフォーマンス・メトリックス
- ▶ MS IIS サーバ用 PFX フォーマット SSL 証明書のインポート

#### 2.4.5 その他

- ▶ タイムゾーンと NTP サーバのサポート
- ▶ 管理ユーザ “bal” 用パスワード変更機能
- ▶ ユーザ “bal” のパスワード・リカバリー機能
- ▶ マルチ言語キーボードのサポート
- ▶ リアルサーバの DNS リバースルックアップ（逆引き）

### 3 ロードマスター・ネットワーク・トポロジー

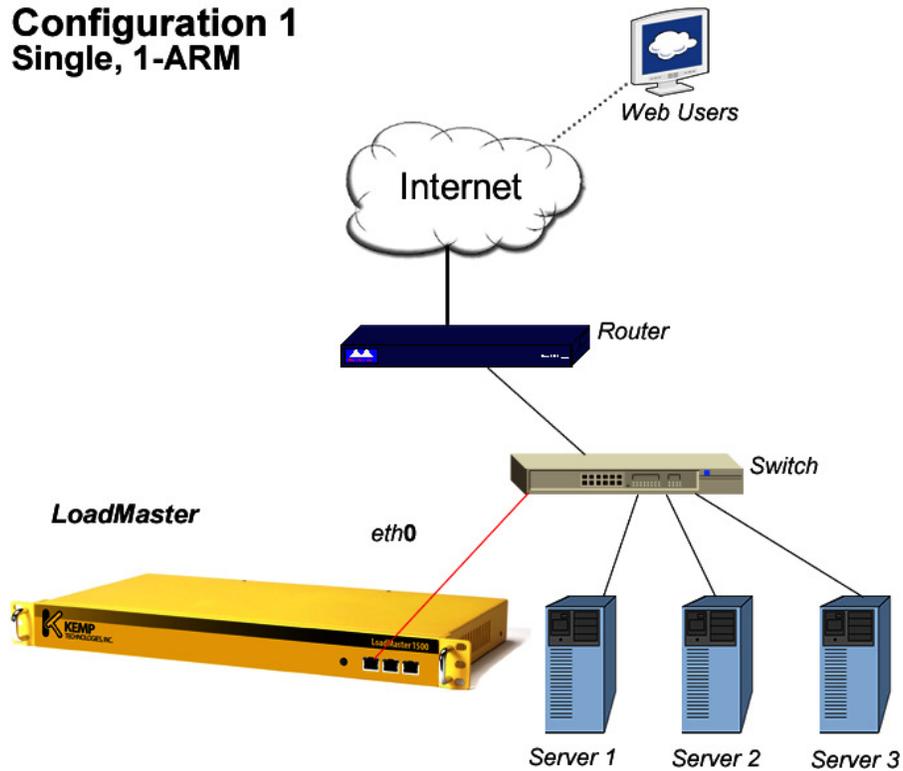
#### 3.1 1アーム・バランサー

もし、1アーム構成を選択したならば、下記の事柄が適用されます。

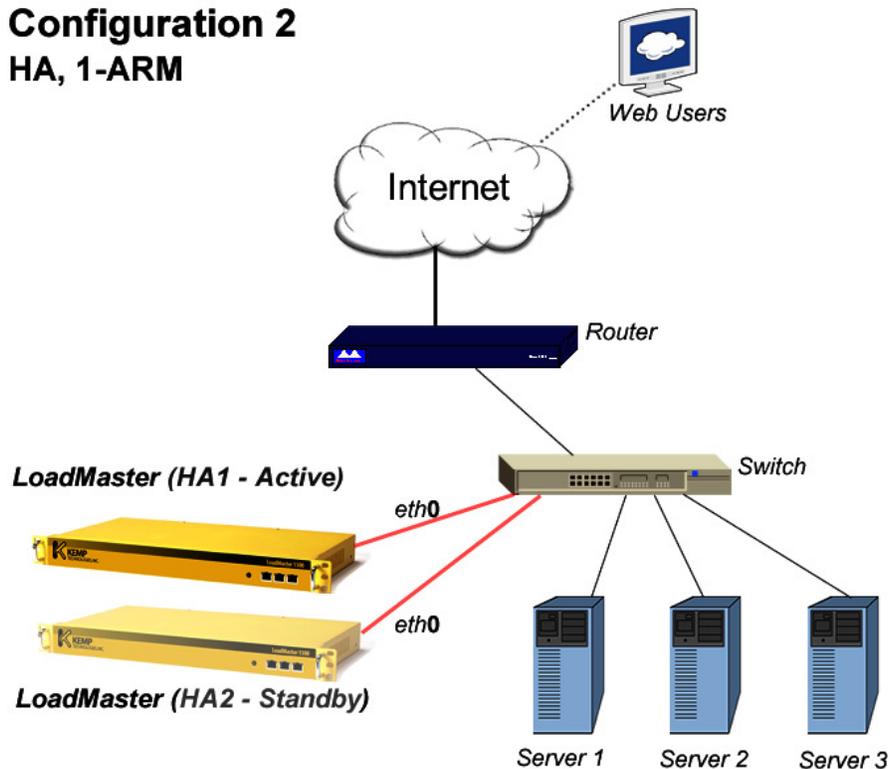
- ▶ イーサポート0だけが使用されます（受送信の両方のトラフィックで）。
- ▶ リアルサーバとバーチャルサービスは、同じ論理ネットワーク上の構成品となります。時々、フラットベースとも呼ばれます。もしサービスがインターネット上で使用されるならば、リアルサーバとバーチャルサービスの両方とも、パブリック IP アドレスであることを暗示しています。
- ▶ S-NAT は、1アーム構成時では無意味です。
- ▶ リアルサーバは、デフォルトではダイレクト・サーバ・リターン（DSR）の設定にはなっていません。
- ▶ ロードマスターとクライアントが同じ論理ネットワークに位置している場合、IP アドレスの透過モードを使用するとバーチャルサービスへのアクセスが出来ませ

ん。DSR（ダイレクト・サーバ・リターン）構成にすることでアクセスが出来るようになります。

### Configuration 1 Single, 1-ARM



## Configuration 2 HA, 1-ARM



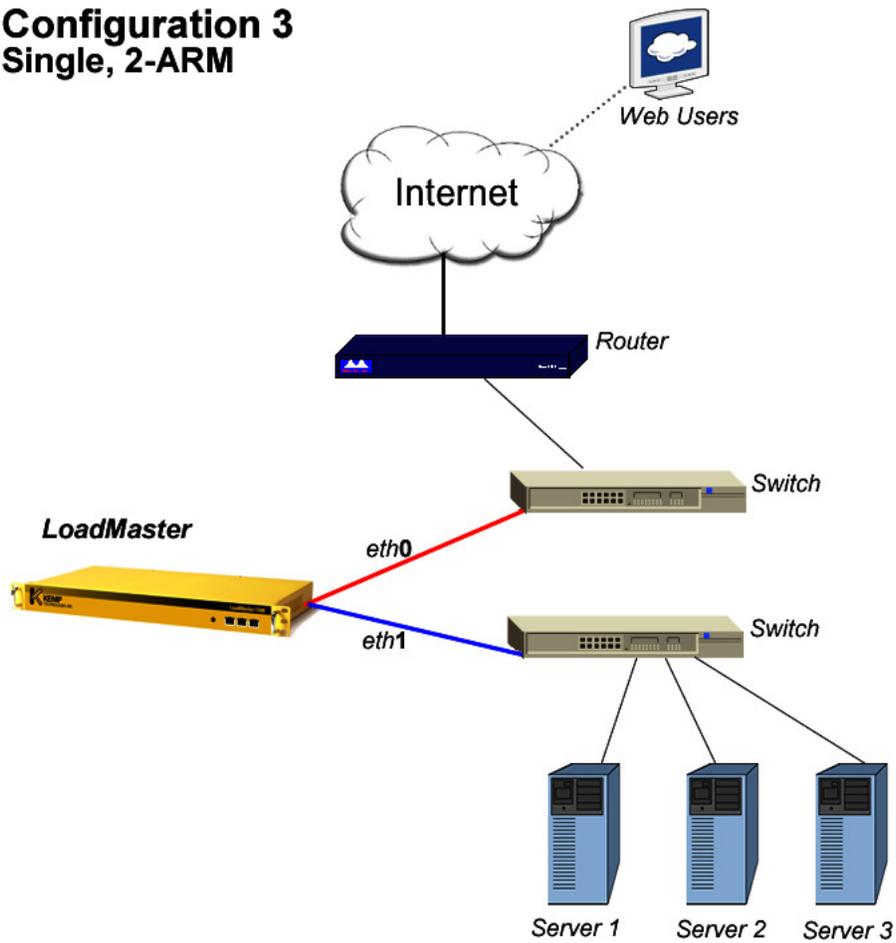
### 3.2 2アーム、マルチアーム・バランサー

もし、2アーム、マルチアーム構成を選択したならば、下記の事項が適用されます。

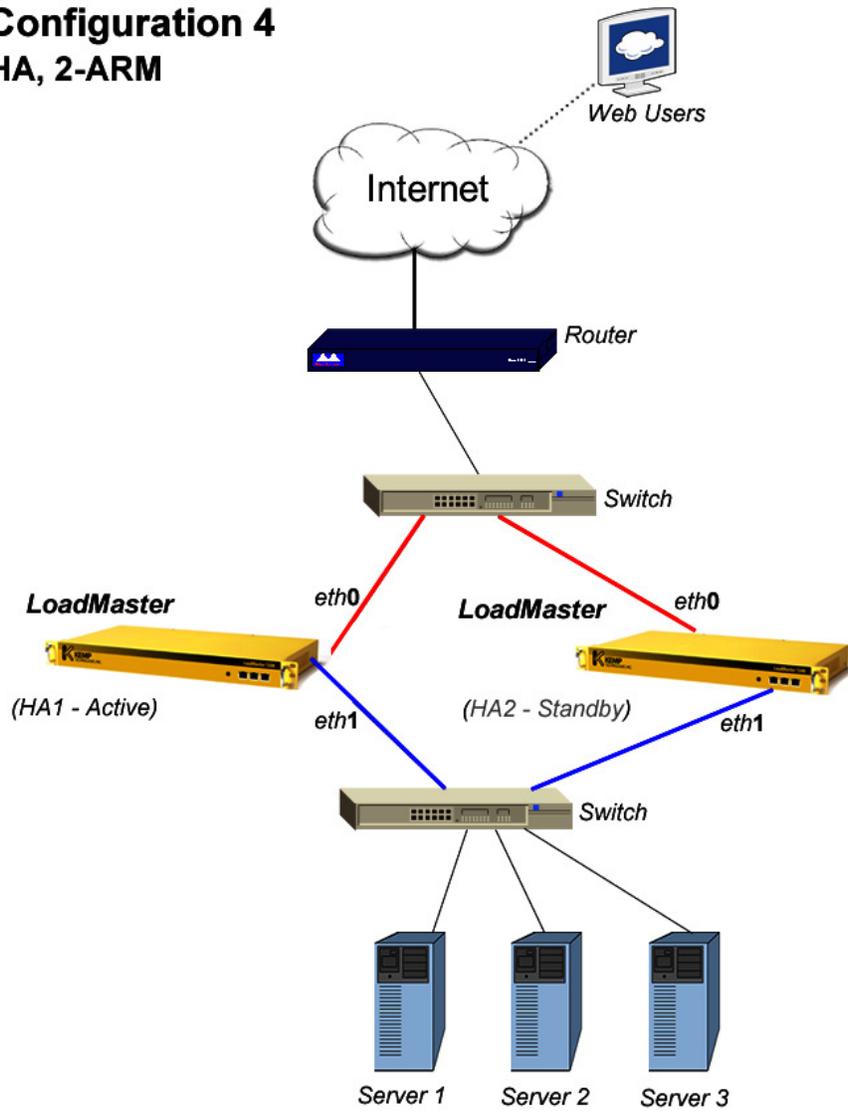
- イーサポート0（ネットワーク側）とイーサポート1（ファーム側）の両方のインターフェースが使用されます。マルチアームでは、他のイーサポートがファーム用として追加されます。
- ロードマスター（イーサポート0）とサーバファームは、別々の論理ネットワークに位置します。NAT ベース・トポロジとも呼ばれることがあります。
- サーバファームは、ルーティング出来ない IP アドレス（RFC1918）が使われます。
- この構成では、S-NAT 機能は有益です。
- ロードマスターとクライアントが同じ論理ネットワークに位置している場合、IP アドレスが透過モード（トランスペアレンシー）でもバーチャルサービスへのアクセスは正しく機能します。
- バーチャルサービスは、どのイーサポートのサブネットを使用しても作成可能です。
- リアルサーバは、どのイーサポートにでも存在できます。しかしながら、イーサポート0への設定は、2アーム構成時には推奨されません。

- ▶ 1アーム、2アームに関係なく、各ポートに外部サブネットを追加可能です。

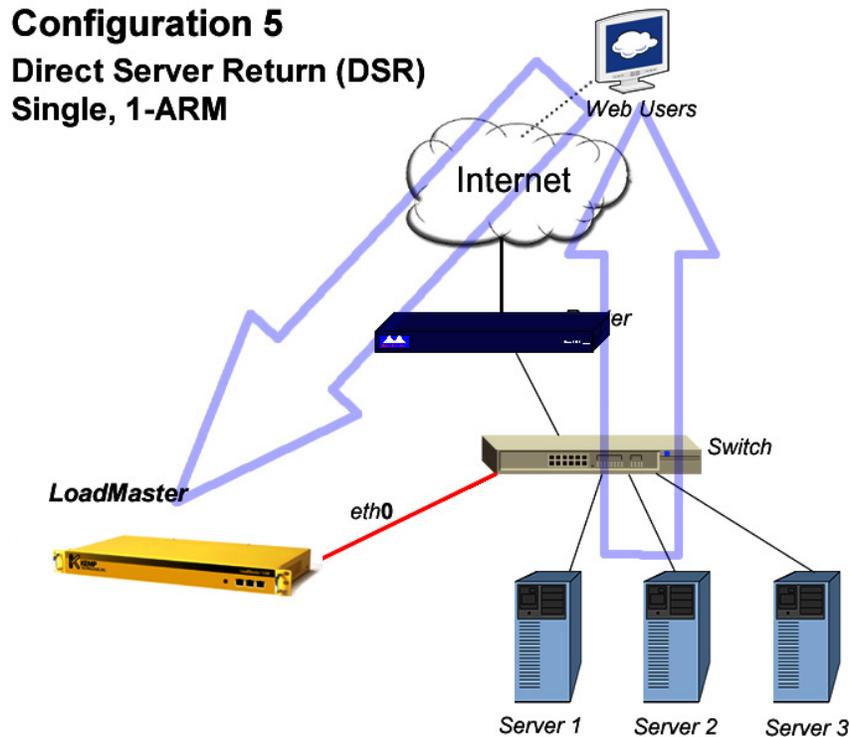
### Configuration 3 Single, 2-ARM



### Configuration 4 HA, 2-ARM



### 3.3 ダイレクト・サーバ・リターン(DSR)の一例



- 1- ロードマスターが、インカミング・リクエストを受信
- 2- サーバ1へとルーティング
- 3- サーバ1よりレスポンスを送信  
 レスポンスは、ロードマスターを介さずにクライアントに直接返されます

上図：ダイレクト・サーバ・リターン構成例

この機能は、リアルサーバがロードマスターを介さずに、直接クライアントにレスポンスを返す必要があるときにだけ設定してください。この構成では、リアルサーバはクライアントへの直接パス（例えば、ロードマスターと併設されたルータを介した）を持っていない限りなりません。

**注意：**DSR 構成時には、パーシステンス（セッション維持）はソース IP オプションだけが指定可能です。又、バーチャルサービス（VS）の設定は、L4の透過モードにしなければなりません。非透過モード(L7)では、クライアントのソース IP アドレスが RS に送られないので、この機能は動作しません。

DSRには、MAT (MAC アドレス・トランスレーション) とリアルサーバ (RS) 設定変更のコンビネーションが使われます。RSには、通常のIPアドレスを設定しますが、VS用のIPアドレス (VIP) も設定する必要があります。通常では、VIPアドレスはロードマスター以外の機器に重複して設定することはできません。この問題を解決するためには、リアルサーバへ設定するVIPアドレスが、ARPリクエストに対してレスポンスを返さないようにする必要があります。現状でカーネル 2.6 バージョンをもつLinuxでは、ループバック・インターフェース上にIPエリアスとしてVIPアドレスを設定することで対応が可能です。

VSを作成して各リアルサーバを設定する時、“Forwarding Method”として“route”を選択する必要があります。これは、ロードマスターがクライアントからのパケットの宛先IPアドレスを変更することなくRSにルーティングすることを意味します (下記のステップ1と2に相当。ClientのIPアドレスは216.139.43.10、VIPは195.30.70.200、RSの実際のIPアドレスは195.30.70.100とします)。リアルサーバ (RS) は、パケットが宛先としてVIPアドレスを持っていたとしても、ループバック・インターフェースにこのVIPアドレスをIPエリアスとして設定してあるので受け付けます。リアルサーバは、リクエストしてきたクライアントに、VIPアドレスをソースIPアドレスとしてリプライを返します (下記のステップ3に相当)。

ステップ	ソース IP	宛先 IP	MAC アドレス
1. (Client→LM) (LM)	216.139.43.10 (Client)	195.30.70.200 (VS)	Dest: 00:00:00:00:00:aa
2. (LM→RS) (RS)	216.139.43.10 (Client)	195.30.70.200 (RS)	Dest: 00:00:00:00:00:bb
3. (RS→Client)	195.30.70.200 (RS)	216.139.43.10 (Client)	Source: 00:00:00:00:00:bb(RS)

LM ロードマスター、VS バーチャルサービス、もしくはVIP、RS リアルサーバ

### リアルサーバでのDSR設定方法

DSRがネットワーク側で問題なく動作するには、サーバは宛先としてVIPアドレスが設定されたクライアントからのリクエストを受け付けなければなりません。しかし、同じネットワーク内で同一のIPアドレスを2つの機器に設定することはできません。

この問題は、2つの方法で解決できます。1つは、エリアスとしてインターフェースにVIPアドレスを設定する方法で、管理上ダウンさせていなければなりません。もう1つの方法は、ループバック・インターフェース上にエリアスを設定します。そして、サーバは他の機器がバーチャルサービスのIPアドレスをARPリクエストで問い合わせして来てもレスポンスを返さないようにしなければなりません。もし、レスポンスを返してしまうと、サービスのリクエストがバーチャルサービスではなく、リアルサーバへ直接送信されてしまうようになってしまいます。

### Linux でVIP アドレスをループバック・インターフェースに設定する例

1. “ifconfig -a” コマンドを使用して現状の設定を確認：

```
root@RS1 $ ifconfig -a
eth0  Link encap:Ethernet HWaddr 00:00:00:00:00:bb inet addr: 195.30.70.11 Bcast: 195.30.70.255
      Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX
      packets:96561817 errors:526 dropped:0 overruns:5 frame:0 TX packets:97174301 errors:0
      dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:100 Interrupt:10 Base address:0x4000
lo    Link encap:Local Loopback inet addr: 127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING
      MTU:3924 Metric:1 RX packets:3985923 errors:0 dropped:0 overruns:0 frame:0 TX
      packets:3985923 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0
```

2. “ifconfig”コマンドを使って IP エリアスとしてのループバック・インターフェースを作成：

```
root@RS1 $ ifconfig lo:1 195.30.70.200 broadcast 195.30.70.200 \ netmask 255.255.255.255
root@RS1 $ ifconfig lo:1
lo:1  Link encap:Local Loopback inet addr:195.30.70.200 Mask:255.255.255.255 UP LOOPBACK
      RUNNING MTU:3924 Metric:1
```

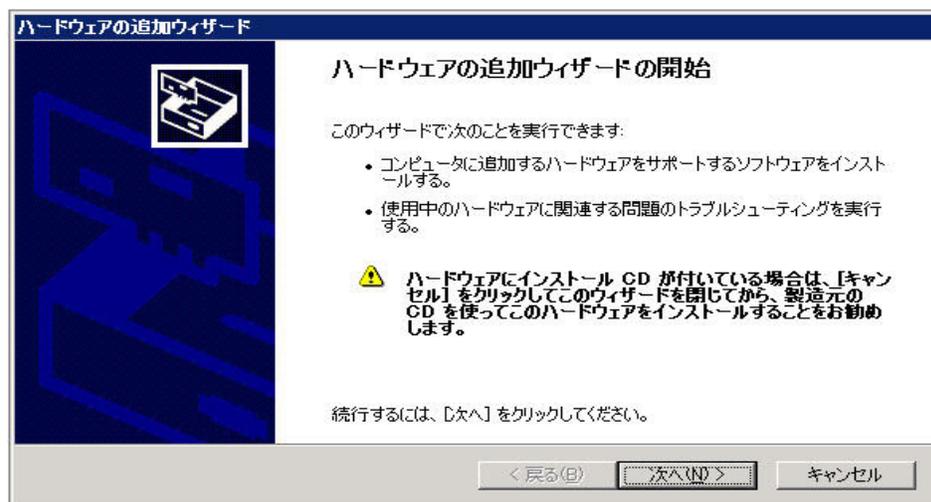
3. ループバック・インターフェースが ARP へのリプライを返さないようにします。  
“etc/sysctl.conf” ファイルに下記のパラメータを追加します。

```
net.ipv4.conf.all.arp_ignore=1
net.ipv4.conf.eth0.arp_ignore=1
net.ipv4.conf.eth1.arp_ignore=1
net.ipv4.conf.all.arp_announce=2
net.ipv4.conf.eth0.arp_announce=2
net.ipv4.conf.eth1.arp_announce=2
```

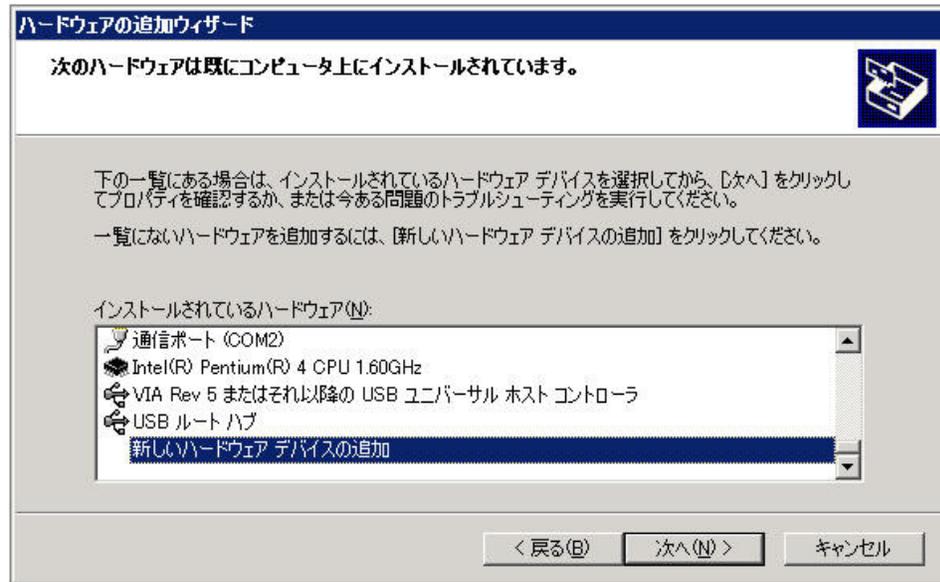
### Windows 2003 Server でVIPアドレスをループバック・インターフェースに設定する例

Windowsサーバでは、ループバック・アダプターを使用するのが一般的です。ループバック・アダプターを設定し、VIPアドレスを割当てる方法を示します。

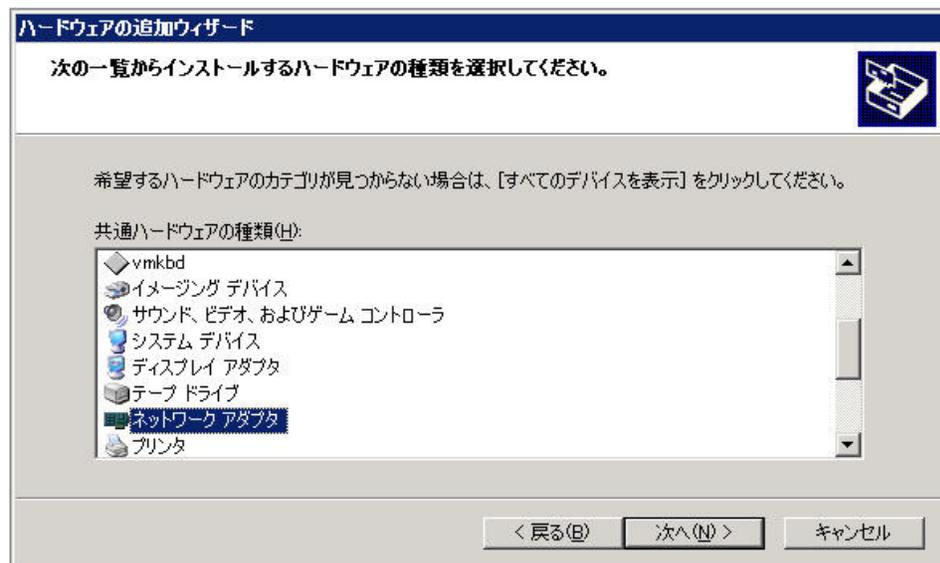
1. コントロールパネルの“ハードウェアの追加”を選択します。



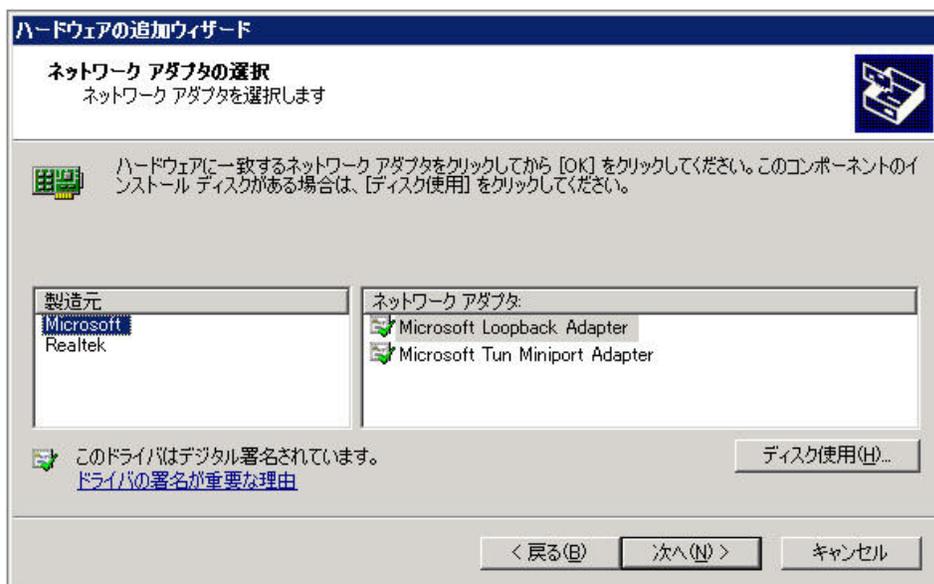
2. “次へ” をクリックすると、ウィザードは新しいハードウェアを探します。そして、“概にこのハードウェアをコンピュータに接続していますか？”と問い合わせてきます。“はい、——” を選択し “次へ” をクリックします。ハードウェアのリストが表示されるので、スクロールダウンして “新しいハードウェアデバイスの追加” を選択します。



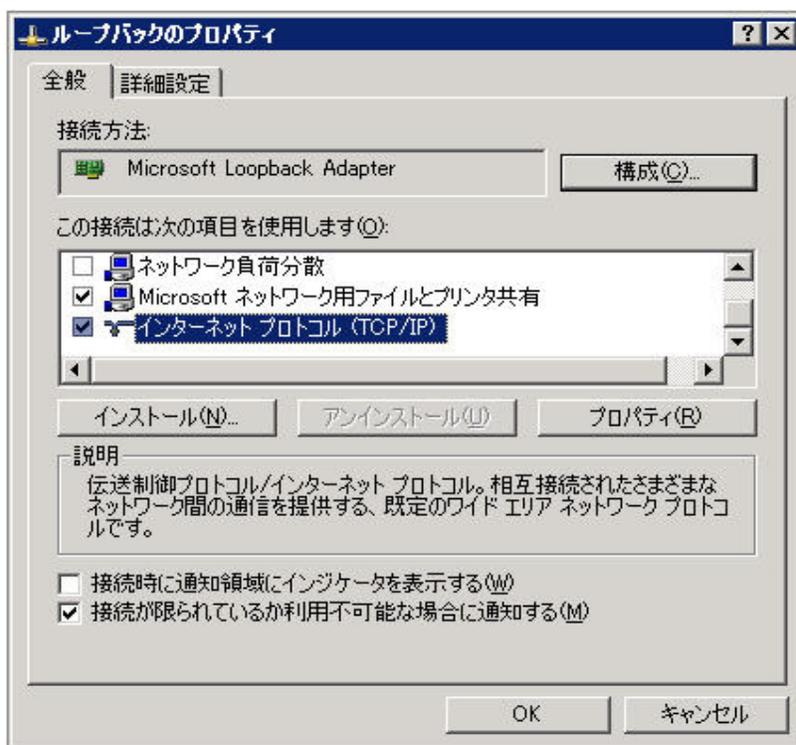
3. 次の画面で “一覧から選択したハードウェアをインストールする” を選択し “次へ” をクリックします。リストから “ネットワークアダプタ” をダブルクリックします。



4. 次の画面で、ネットワークインターフェースのベンダー名がリストされますので、“Microsoft” の中から “Microsoft Loopback Adapter” をダブルクリックします。

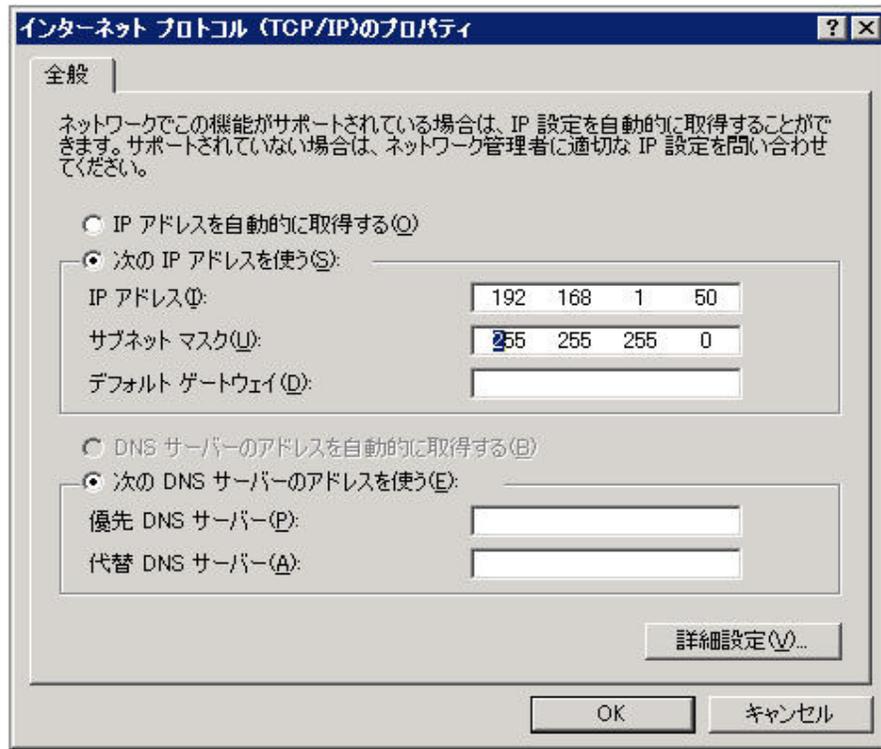


5. “次へ” をクリックし、アダプターをインストールします。問題なくインストールされると、完了画面が表示されますので、“完了” をクリックします。
6. コントロールパネルの“ネットワーク接続”を選択すると、“ローカルエリア接続 2”が追加されていますので、名前を“ループバック”に変更しておく管理上便利かもしれません。そして、その状態画面から“プロパティ”をクリックし、“インターネット プロトコル(TCP/IP)”を選択します。

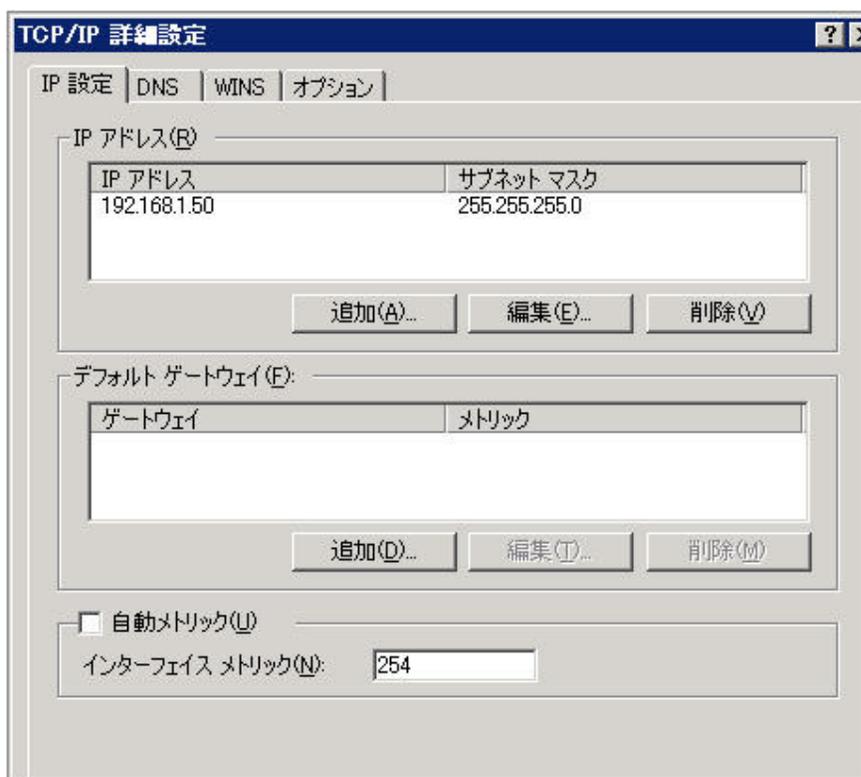


7. “プロパティ” をクリックし、IP アドレスに VIP アドレスを入力します。この例

では、VIP アドレスは ‘92.168.1.50’ です。サブネットマスクを入力し、“詳細設定” をクリックします。



8. TCP/IP 詳細画面の中の“自動メトリック”のチェックを外します。そして、ARP リクエストが来てもレスポンスを返さないように ‘2 5 4’ と入力します。  
“OK” ボタンをクリックし変更を終了させます。



9. TCP/IP 詳細設定画面に戻りますので、“OK” ボタンをクリックし完了させます。

#### Windows 2000 Server でVIPアドレスをループバック・インターフェースに設定する例 ハードウェアの追加

- 1) スタート→設定 (s) →コントロールパネル (c) →ハードウェアの追加と削除
- 2) ハードウェアの追加と削除ウィザードの開始→次へ
- 3) デバイスの追加／トラブルシューティング→次へ
- 4) 新しいデバイスの追加→次へ→いいえ、一覧からハードウェアを選択します
- 5) ネットワークアダプタ→次へ→Microsoft→Microsoft Loopback Adapter→次へ
- 6) 完了

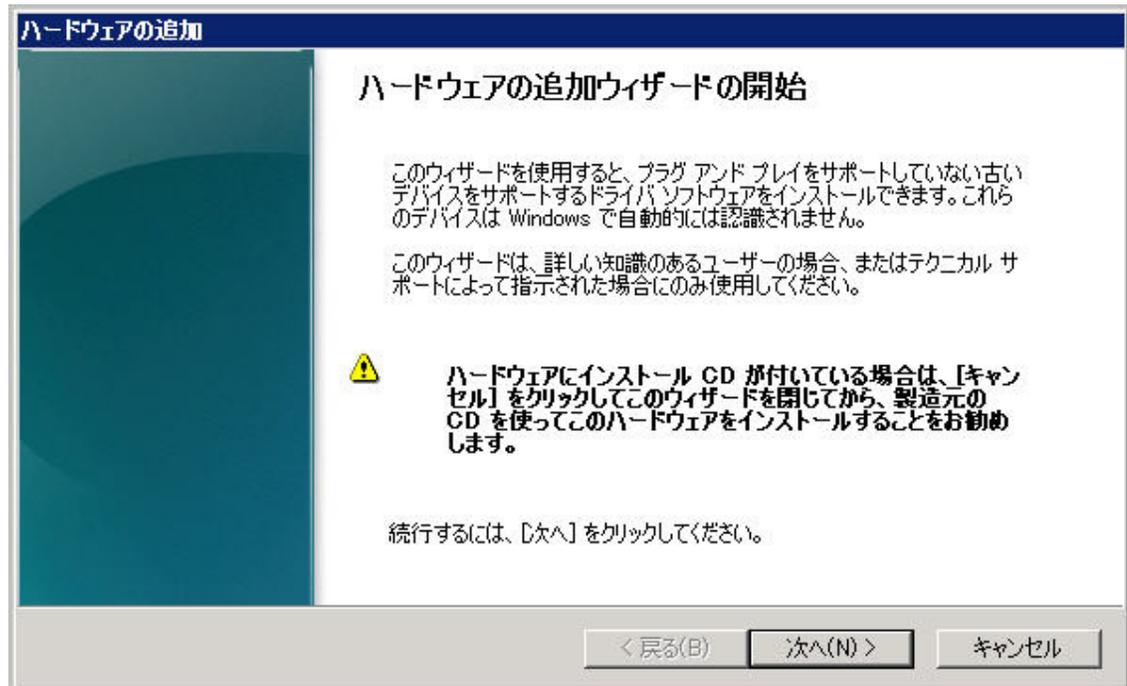
#### ループバック・アダプターの設定

- 1) スタート→設定 (s) →コントロールパネル (c) →ネットワークとダイヤルアップ接続
- 2) Loopback Adapter を右クリックしプロパティを選択
- 3) インターネットプロトコル (TCP/IP) のみ選択し、後は選択しない。
- 4) インターネットプロトコル (TCP/IP) をハイライトにして、プロパティをクリックします。
- 5) バーチャルサービスの IP アドレスとサブネットマスクのみを入力します。デフォルト・ゲートウェイは入力しないでください。

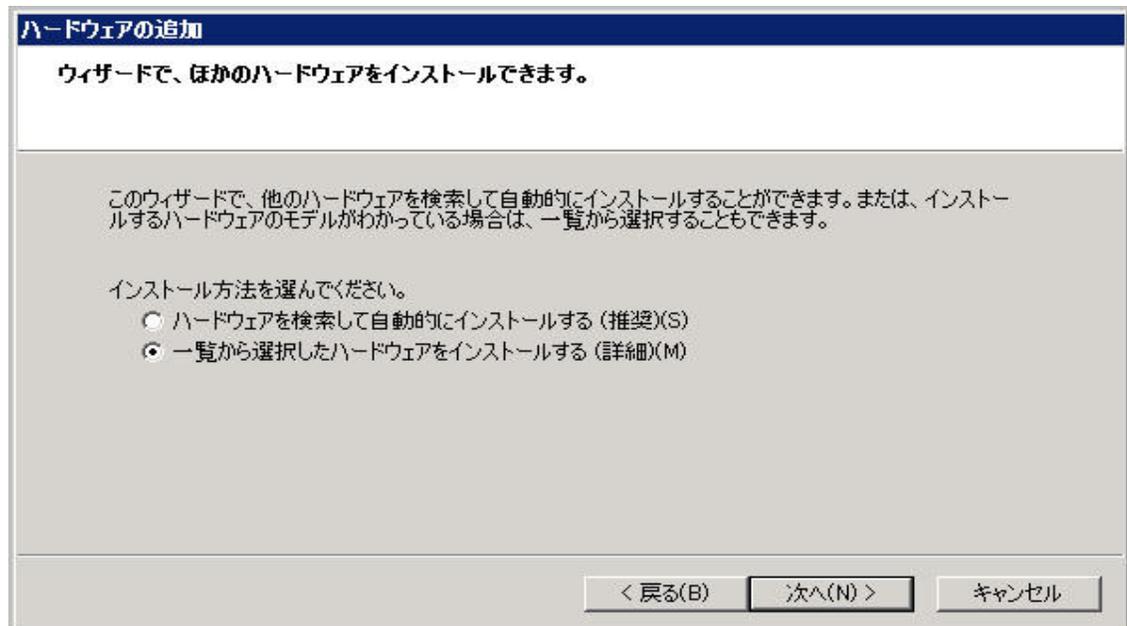
6) OK ボタンを押して完了。

*Windows 2008 Server* でVIPアドレスをループバック・インターフェースに設定する例  
Windowsサーバでは、ループバック・アダプターを使用するのが一般的です。ループバック・アダプターを設定し、VIPアドレスを割当てる方法を示します。

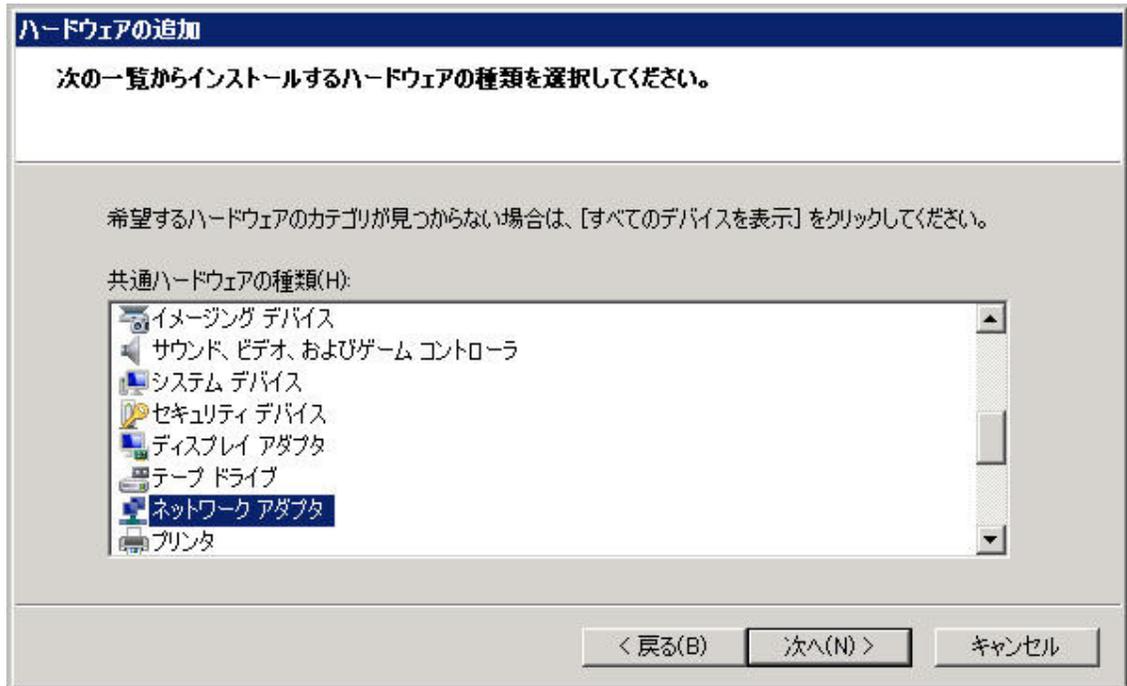
1. コントロールパネルの“ハードウェアの追加”を選択します。



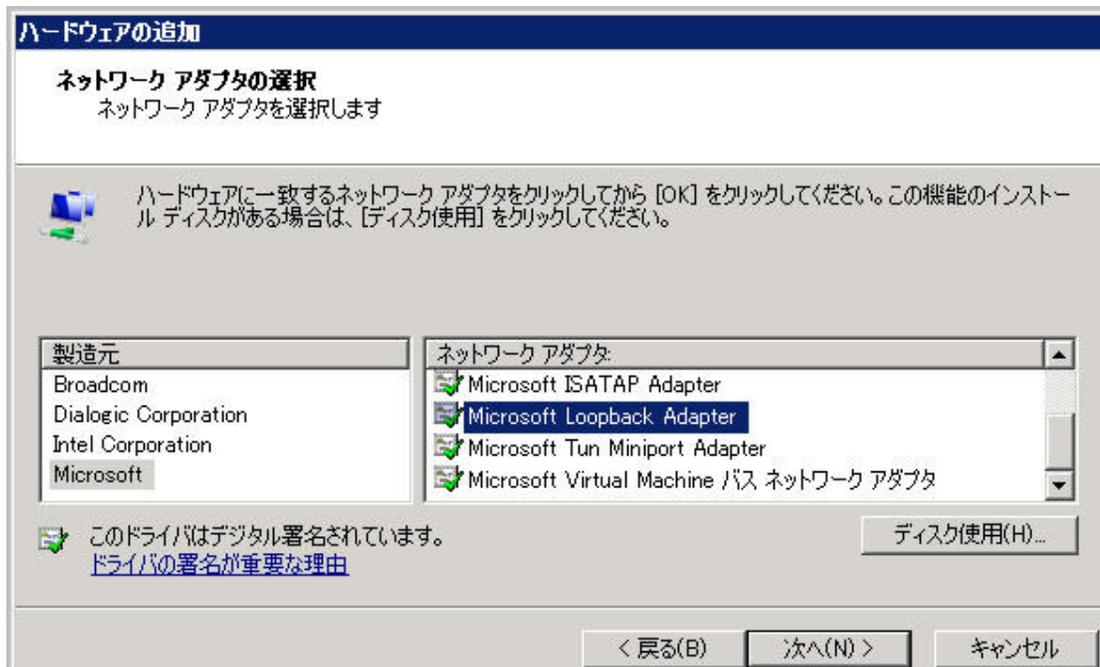
2. “次へ” をクリックして、インストール方法として“一覧から選択したハードウェアをインストール”を選択し、次へをクリックします。



- 表示された共通ハードウェアの種類一覧から“ネットワークアダプタ”をダブルクリックします。

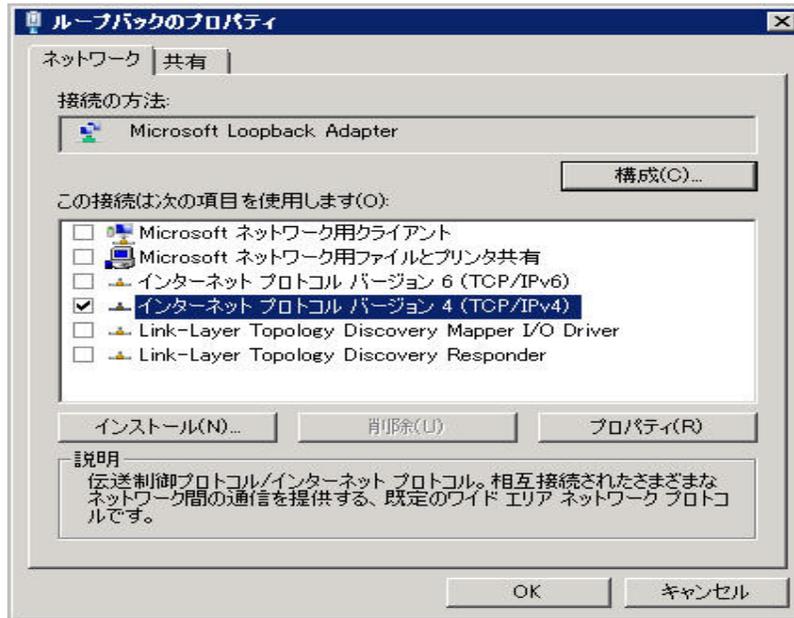


- 次の画面で、ネットワークインターフェースのベンダー名がリストされますので、“Microsoft”の中から“Microsoft Loopback Adapter”をダブルクリックします。

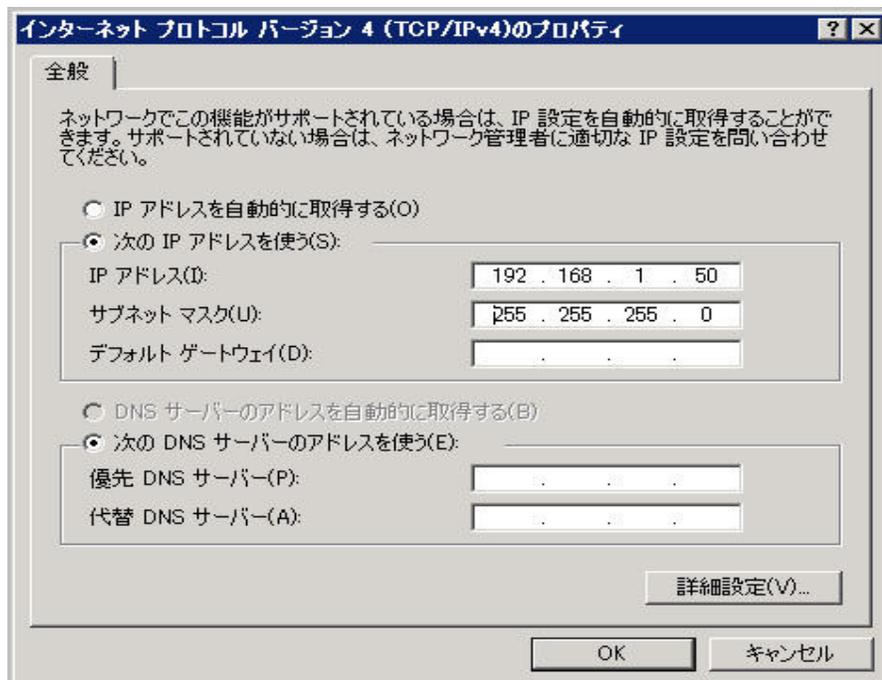


- “次へ”をクリックし、アダプターをインストールします。問題なくインストールされると、完了画面が表示されますので、“完了”をクリックします。
- コントロールパネルの“ネットワークと共有センター”に行き、ネットワーク接続を選択します。“ローカルエリア接続 2”が追加されていますので、名前を“ループバック”に変更しておく管理上便利かも知れません。そして、ループ

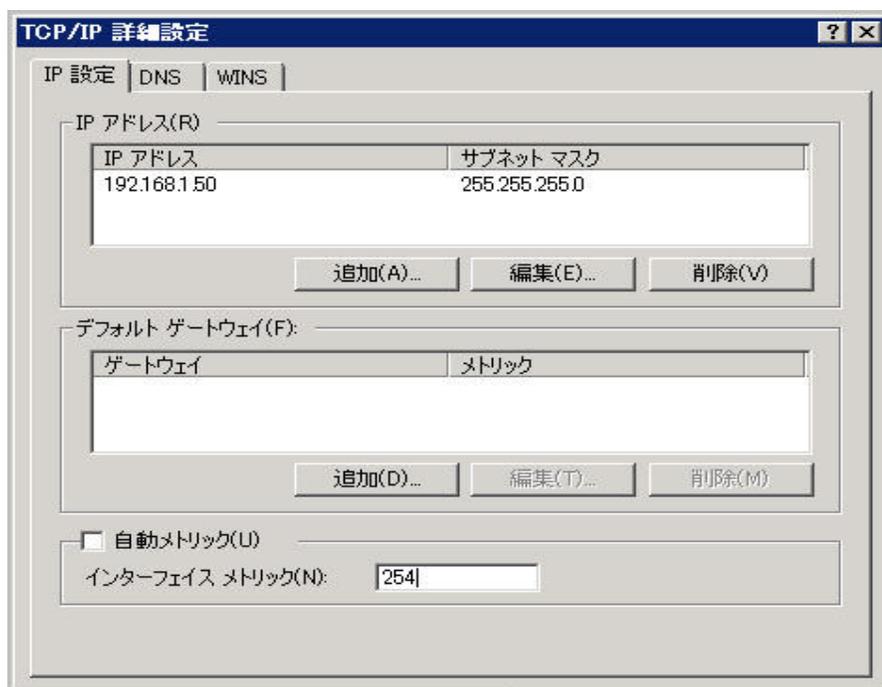
バックを右クリックし“プロパティ”を選択し、“インターネットプロトコルバージョン 4 (TCP/IP v 4)” のみにチェックマークを入れます。他のチェックマークは抜いてください。



7. “プロパティ” をクリックし、IP アドレスに VIP アドレスを入力します。この例では、VIP アドレスは ‘92.168.1.50’ です。サブネットマスクを入力し、“詳細設定” をクリックします。



8. TCP/IP 詳細画面の中の“自動メトリック”のチェックを外します。そして、ARP リクエストが来てもレスポンスを返さないようにするために ‘254’ と入力します。そして、“OK” ボタンをクリックし変更を終了させます。



9. TCP/IP 詳細設定画面に戻りますので、“OK” ボタンをクリックし、ループバックのプロパティ画面を閉じれば完了です。

10. コマンドラインにて、下記を入力します。

```
netsh interface ipv4 set interface "Local Area Connection" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

## 4 その他のネットワーク問題点

### 4.1 S-NAT

2アーム、マルチアームのネットワーク構成を使用する時、リアルサーバからインターネットへアクセスできることは場合によっては有益です。この場合、リアルサーバのデフォルトルートは、ロードマスターを介するものです。しかしながら、リアルサーバがプライベートのIPアドレスを使っていれば、インターネットへのアクセスはできません。

この場合、S-NAT機能を使うことにより、ロードマスターはリアルサーバからのアクセスに対して、イーサポート0、もしくはVIPアドレスをマップしてロードマスターからのアクセスのように動作します。リアルサーバは、これによりあたかも直接アクセスしているかのようにインターネットを使用できます。そして、この方法はインターネットからはリアルサーバへ直接接続できないという追加的なセキュリティをもたらします。

S-NATの使用は、1アーム構成では推奨できません。

この S-NAT 機能は、コンソールメニュー、もしくはウェブ・ユーザ・インターフェース (WUI) よりオン、もしくはオフに設定することができます。

S-NAT 用 IP アドレスは、設定により選択可能です。設定変更は、SSH 接続した設定ユーティリティ、もしくは WUI を使って行います。

### SSH 接続経由の設定ユーティリティを使用する場合

メニュー画面の “2. Service Management (CLI)” を選択します。  
"#" プロンプトが表示されたら、次のコマンドを入力します。

```
vip <IPaddress>:<port> <enter>
```

<IP address>は、インターネットへアクセスするリアルサーバ (RS) が属するバーチャルサービスの IP アドレスです。そして <port> は、そのバーチャルサービスのポート番号です。このコマンドを入力すると、新たな “#” プロンプトが表示されますので、次のコマンドを入力します。

```
useforsnat <enter>
```

このコマンド入力により、リアルサーバは Internet へのアクセス時にバーチャルサービスにアサインされている IP アドレスを使用するようになります。設定を確認するために、下記のコマンドを入力します。

```
show <enter>
```

該当 VIP の属性が表示され、usefornet がその中にあることを確認します。そして、コマンド入力画面から抜けるために下記のようにコマンドを入力します。

```
exit <enter>
```

```
exit <enter>
```

and tab to the exit button at the bottom of the screen to commit the change

### WUI を使用する場合

インターネットへアクセスするリアルサーバが属するバーチャルサービスの Properties 画面を、“Virtual Service” サブメニューの “View/Modify Services” から、特定バーチャルサービスの “Modify” ボタンをクリックして開きます。表示された Properties 画面の中の “Basic Properties” の中にある “Use Address for SNAT” にチェックマークを入れます。



## 4.2 デフォルト・ゲートウェイと追加ルート

外部へのルートが1つだけのネットワークにロードマスターが設置されているような単純な構成では、システムに1つのデフォルト・ゲートウェイを設定するだけです。ロードマスターから外部への全てのトラフィックは、このゲートウェイを介してルーティングされます。図-Aに、その構成例を示します。

ロードマスターが、もっと複雑なネットワーク構成内に設置された場合（例えば図-Bに示しているような）、特定サブネットがシステム以外の別のゲートウェイを介するルートを持っている場合は、ルーティングテーブルにそのルートを追加しなければなりません。例えば、この図-Bでは追加ルートとしてプライベート・ネットワークか、もしくは2つ目のISP Link 2を介するようにルーティングテーブルを追加設定しなければなりません。

静的なルーティングだけが、ロードマスター上に設定可能です。（このマニュアル内のインストール&設定ガイドを参照）ロードマスターは、現状ではダイナミック・ルーティングはサポートしていません。

### Configuration 3 Single, 2-ARM

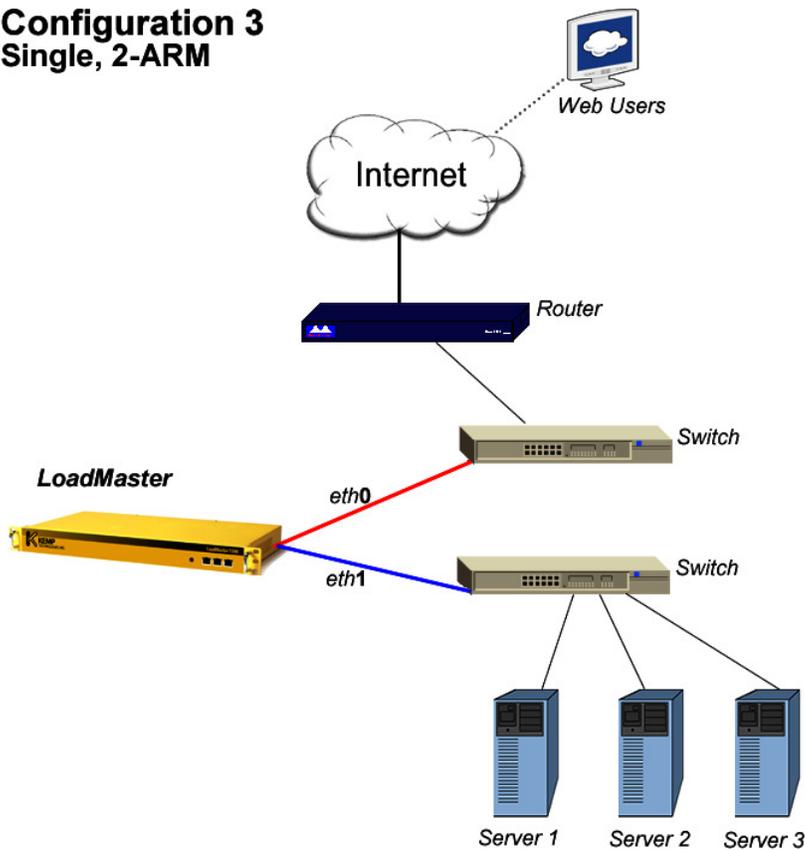


図-A

### Configuration 6 Single, 2-ARM

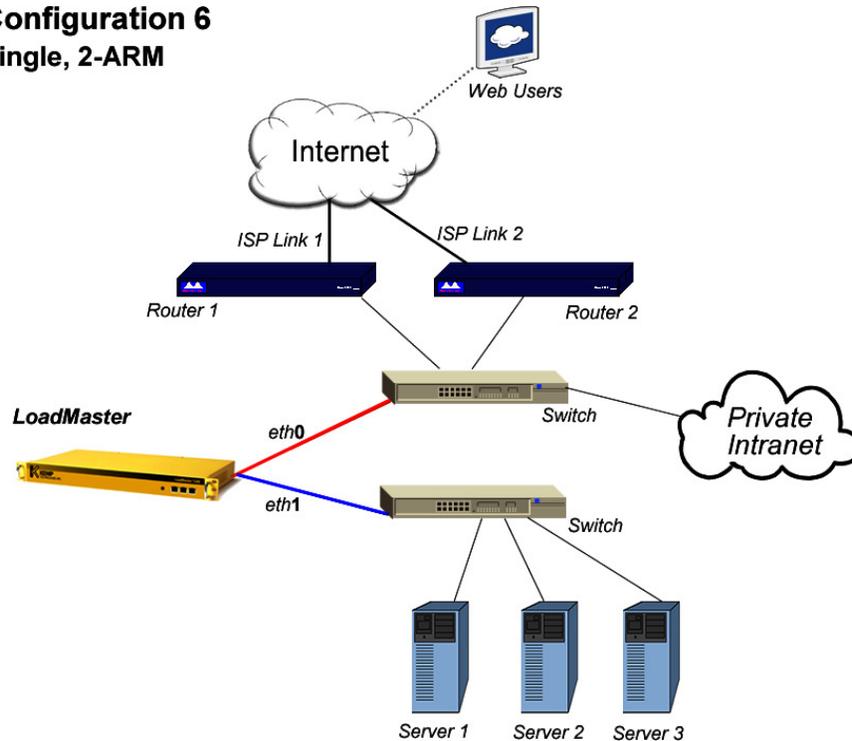


図- B

## 4.2 デフォルトゲートウェイのイーサポート指定

デフォルト設定では、システムのデフォルトゲートウェイはイーサポート 0 上のサブネットに存在するデバイス（ルーターやファイヤーウォール）しか許可されません。マルチアームを構成して、イーサポート 0 以外のポートにあるデバイスをシステムのデフォルトゲートウェイとして設定したい場合は、“System Configuration” サブメニューの

“Miscellaneous Options” オプション下の “Network Options” の “Enable Alternate GW support” を ‘Yes’ にすることで可能です。その後、デフォルトゲートウェイに使用する “Network Interface” の設定で、“Use for Default Gateway” にチェックマークを付けます。システムのデフォルトゲートウェイが存在するイーサポート以外のサブネットアドレスを使用してバーチャルサービスを作成し、システムのデフォルトゲートウェイ以外のデバイスをデフォルトゲートウェイとして使用する場合、バーチャルサービス設定のパラメータ “Default Gateway” にそのデバイスを指定して下さい。

## 4.3 リモート・リアルサーバのサポート

バーチャルサービスが非透過モードであるならば、ローカルなネットワーク以外に存在するサーバをリアルサーバとして負荷分散の対象に参加させることが可能です。バーチャルサービスを非透過モードに設定するには、WUI からバーチャルサービスの Properties 画面で、“Force L7” をオンにする必要があります。更に、この設定をオンにすることで表示される “L7 Transparency” はオフにしなければなりません。

デフォルトでは、リモート・リアルサーバの追加はできない設定になっていますので、WUI の “System Configuration” サブメニュー下の “System Administration” → “Miscellaneous Options” → “L7 Configuration” 内の “Enable Non-Local Real Servers” をオンにします。次に、バーチャルサービスの Properties 画面でリアルサーバを追加します。表示された “Please Specify the Parameters for the Real Server” 画面の “Allow Remote Addresses” をオンにします。そして、リモート・リアルサーバの IP アドレスを入力します。

**Please Specify the Parameters for the Real Server**

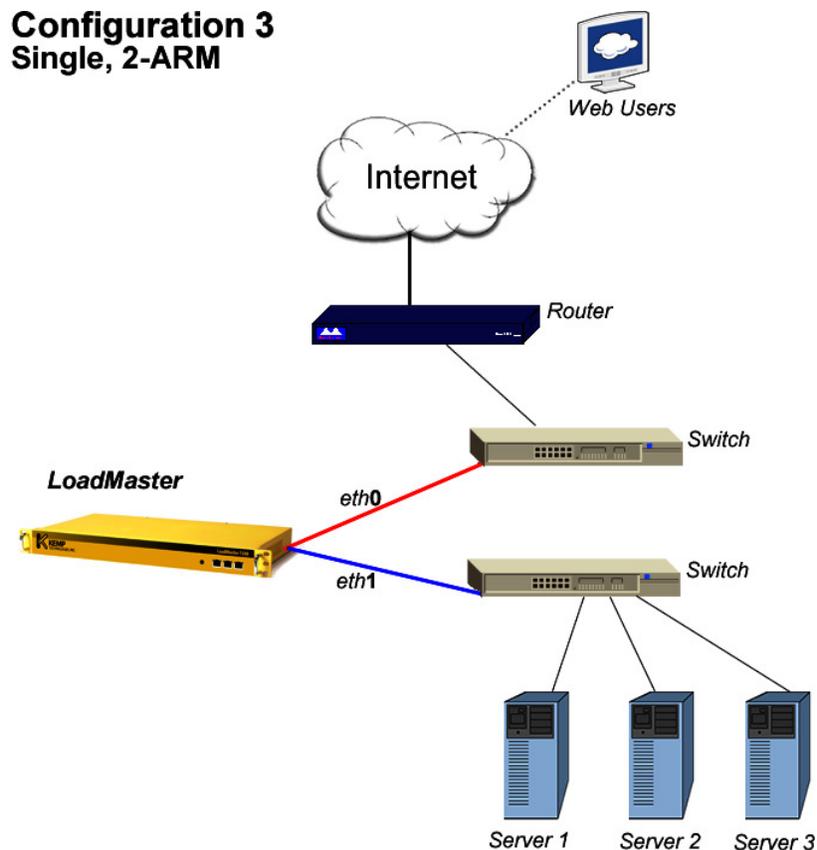
Allow Remote Addresses	<input checked="" type="checkbox"/>
Real Server Address	<input style="width: 100%;" type="text"/>
Port	<input style="width: 50%;" type="text" value="80"/>
Forwarding method	<input type="text" value="nat"/>
Weight	<input style="width: 50%;" type="text" value="1000"/>

<-BackAdd This Real Server

## 5 シングル/デュアル ユニット構成

### 5.1 シングル・ユニット構成

スタンドアローン・モードでの構成は下図のようになります。



### 5.2 ハイ・アベイラビリティ(HA)構成

ロードマスターのハイ・アベイラビリティ機能 (HA) は、システム上のサービスの可用性を保障するものです。HA は、ホット-スタンバイ、及びフェイルオーバー・メカニズムにより実現されます。2つのまったく同じロードマスターのユニットが、ネットワーク上で融合されます。1台のユニットがアクティブ・バランサーとして、2台目がスタンバイ・バランサーとして、アクティブ・バランサーに障害が発生した時にいつでも活動を引き継げるように、準備状態になっています。この2ユニット・クラスターは、ネットワークサイドとサーバファームの両方からは、シングルの論理ユニットとして見えます。

**注意：** 2つのロードマスターが、相互に監視しあって構成されている HA クラスターとして稼動中ならば、各ネットワーク・インターフェースは独自の IP アドレスとシェアード・IP アドレス (フローティングとも呼ばれる) を持ちます。シェアード IP アドレスは、両方のロ

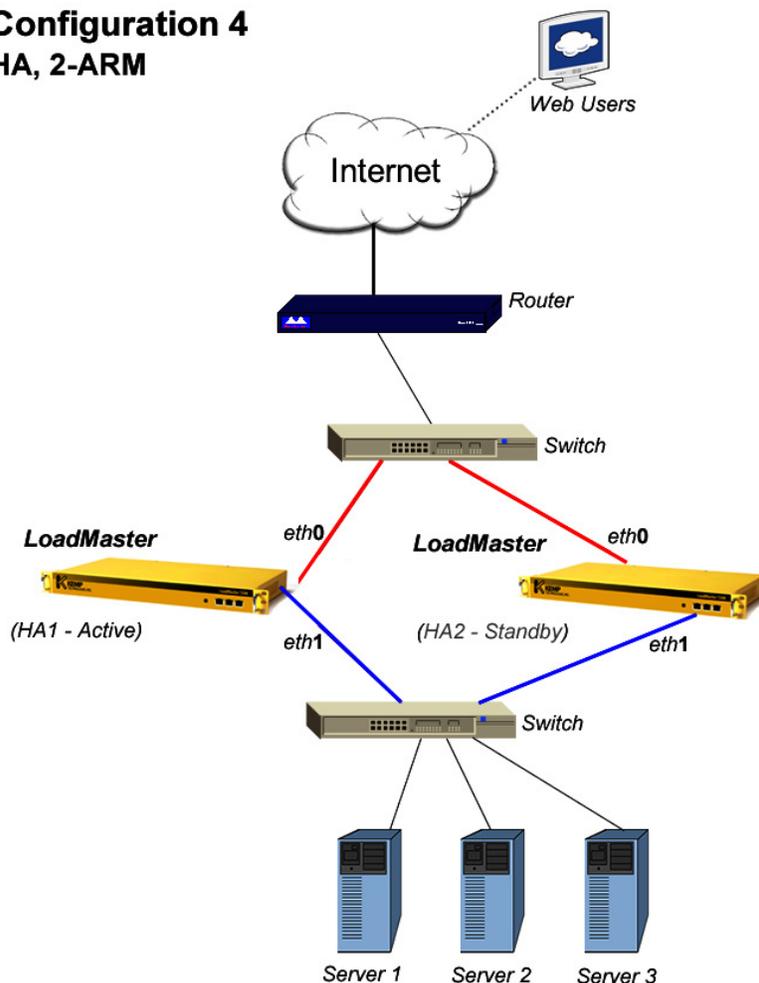
ードマスター・ノードで共用されます。しかし、アクティブなロードマスター装置だけにこのアドレスの実使用が許されます。

通常稼動中は、各ノードが一定周期で相手のマシンの可用性を2つの接続（イーサポート0と1）を介してハートビート・メッセージ（hb方式）、もしくはブロードキャスト（carp方式）を送ることで相互にチェックし合っています。何らかの異変が起こり、アクティブのロードマスターがダウンしたならば、スタンバイ・マシンがアクティブとなり、負荷分散の全タスクを引き継ぎます。

1アーム構成時は、HA クラスタを構成する2つのユニットはイーサポート1同士をクロスオーバーケーブル（LM1500のみ必須）、もしくはストレートケーブルにて接続する必要があります。この場合のイーサポート1の設定は、システムが172.31.255.0/24のアドレススペースの中から自動的に行いますので必要ありません。特別な場合を除いて、何の設定も行わないでください。このケーブルが正しく付設されていない場合は、ファイルオーバーを行うトリガーを間違えて検出して不必要な切り替えが発生しますのでご注意ください。

HA モードでのトポロジーは下図のようになります。

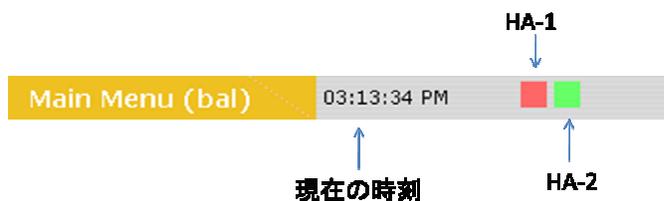
**Configuration 4**  
**HA, 2-ARM**



**注意：** 2アーキ構成の冗長構成では、リアルサーバは、デフォルト・ゲートウェイとしてロードマスターのファーム側のシェアード IP アドレスを設定しなければなりません。

### HAの状態

HAクラスターの状態は、下図のように WUI の左上に 2つの四角の色アイコンでリアルタイムに表示されます。左のアイコンが HA-1 用で、右が HA-2 用です。シェアード IP アドレス、もしくはアクティブ側のロードマスターへ WUI で接続した時のみ正しい状態が表示されます。スタンバイ側のロードマスターへ WUI で接続しても正しい状態が表示されませんので注意が必要です。



色	状態
緑	正常
赤	停止
青	アクティブーアクティブ (異常)
灰	システムロック

## 6 負荷分散方式 (Scheduling Method)

ロードマスターには、“スケジューリングルール (Scheduling Rules)” もしくは、“アルゴリズム” として一般的に知られている分散方式が多種備わっています。

### 6.1 ラウンドロビン(Round Robin)

この方式では、入ってくるリクエストはサーバファーム群のなかの可用なサーバへ順番に分配されます。

もし、全てのサーバが同等のパフォーマンスを持っていて、サービスへの同じような負担を抱えているのであればこの方式を選択してください。このような前提条件ならば、ラウンドロビンはシンプルで効果的な分配方式です。

しかしながら、もしサーバが異なるパフォーマンスを持っているならば、ラウンドロビン方式を使うことにより非力なサーバが現在の処理を終了する前に次の要求を受けるようになってしまいます。これは、非力なサーバがオーバーロードとなる原因になります。

### 6.2 重み付けラウンドロビン(Weighted Round Robin)

この方式は、シンプルなラウンドロビンの弱みを補ってくれます。入ってきたリクエストは、前もってサーバ毎にアサインした静的重みを計算しながら、サーバ群の各サーバに順番に配分されます。

管理者は、サーバの重みをサーバのパフォーマンスに合わせて容易に設定出来ます。はるかに能率が劣るサーバ B の重みを “50” とすると同時に、最も能率的なサーバ A には、例えば重み “100” を与えます。これは、サーバ B が最初のリクエストを受け取る前に、サーバ A が2つ続けてリクエストを受け付けることになります。そしてこのパターンを繰り返します。

### 6.3 最小接続(Least Connection)

前述のラウンドロビン方式は、一定時間内にいくつの接続が持続されているかの評価を配分計算に取り入れません。それにより、サーバ A より少ないリクエストを受け取っているサーバ B がオーバーロードになることがあります。何故ならば、サーバ B へ配分されたユーザが、接続を長く持続している場合があるからです。持続している接続数が多いとサーバへのリクエストが多くなり負荷も増加します。

この潜在的な問題は、最小接続方式により防げます。この方式では、リクエストは全てのサーバが現在持続している接続数を基に計算されて配分されるからです。クラスター内のサーバで、アクティブな接続数が一番少ないものが、次のリクエストを自動的に受け取るようになります。パフォーマンスに対しては、基本的には単純なラウンドロビンと同じ原理です。

従って、この方式に関係するサーバは、同じようなパフォーマンスのリソースを持つことが理想的です。

## 6.4 重み付け最小接続(Weighted Least Connection)

もしサーバが、異なるパフォーマンスのリソースを持っている場合、重み付け最小接続方式 (“weighted least connection”) は最も適切な方法です。アクティブな接続数と管理者によって設定された個別の重みとの組み合わせは、最小接続と重み付けの両方の長所を採用することで、一般的にサーバ負荷が平準化された結果をもたらします。

概して、この方式は接続数とサーバの重み付けの混合比率を使用するので、正当な配分方法といえます。クラスター内の最低比率を持ったサーバが自動的に次のリクエストを受け取ることとなります。

## 6.5 エージェント・ベースのアダプティブ配分(Adaptive)

上記の方式の他に、ロードマスターは一定期間毎にサーバの状態をチェックし、動的に重み付けを行うことが出来る適応性の高い方式をサポートしています。

極めて強力なエージェントベースのアダプティブ配分方式は、 balancer が周期的にファーム内、全サーバのシステム負荷をチェックします。各サーバマシンは、自分自身の実際の負荷を 0 から 102 までの数値 (0 = アイドル、99 = オーバーロード、101 = 失敗、102 = 管理的に使用負荷) で表わすファイルを用意する必要があります。 balancer は、このファイルを HTTP GET により取得します。実際の負荷値を格納した ASCII ファイルを用意してロードマスターに返すのはサーバの役割です。サーバがどのようにこの情報を査定するかについては、必須条件はありません。

この方式がシステムに問題を発生させないために、“Rules & Checking” サブメニューの “Check Parameters” 内にある “Min. Control Variable Value(%)” を調整することを推奨します。

“Min. Control Variable Value(%)” (最低制御変化値) を変更する場合は、“Min. Control Variable Value (%)” の矢印をクリックし、リストの中から適切な値を選択します。このパラメータは、負荷分散対象の各リアルサーバの重みの割り当てを、パフォーマンスエージェントが読み込んだパフォーマンス値に従わせるのを開始するための閾値です。バーチャルサービスにアサインされている全てのリアルサーバのパフォーマンス値がこの閾値を超えない限りは、リアルサーバの重みに従ったトラフィックの割り当ては、静的に設定されている値を使用して行われます。この場合の負荷分散方式は、静的分散方式である重み付けラウンドロビン方式が使用されます。デフォルトの閾値は 5 % です。

## 6.6 固定重み付け配分 (Fixed Weighted)

この方式では、重み付けが一番高いリアルサーバのみが使用されます。もし、一番重み付けの高いサーバが使用不可となった場合は、次に重み付けの高いサーバがクライアントからのリクエストを処理し応答します。全てのリアルサーバは、どのサーバが優先的にクライアントからのリクエストを処理するかの順番に従って異なる重み付けをする必要があります。

## 7 パーシステンス (Persistence)

### 7.1 パーシステンスの概要

アフィニティ、サーバアフィニティ、もしくはサーバスティッキーとも呼ばれるパーシステンスは、個々のクライアントからのリクエストをサーバファームの同じサーバに送るようにする機能です。パーシステンスは、デフォルトでは設定されていませんが、各バーチャルサービスを作成するときに設定可能なオプションです。

パーシステンスなしでは、ロードマスターはラウンドロビン方式や、重み付けラウンドロビン方式などの負荷分散アルゴリズムに従ってトラフィックをサーバに導きます。(図-1)

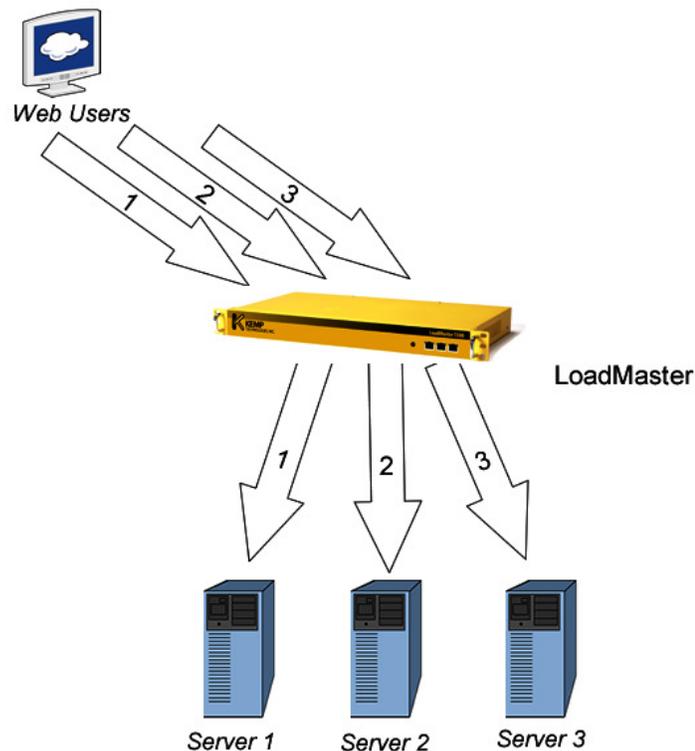


図-1 : パーシステンスなしの負荷分散

パーシステンスを利用すると、ロードマスターは新しいリクエストは負荷分散アルゴリズムにより特定のサーバへと導きますが、次のリクエストは前回と同じサーバへ導きます。(図-2)

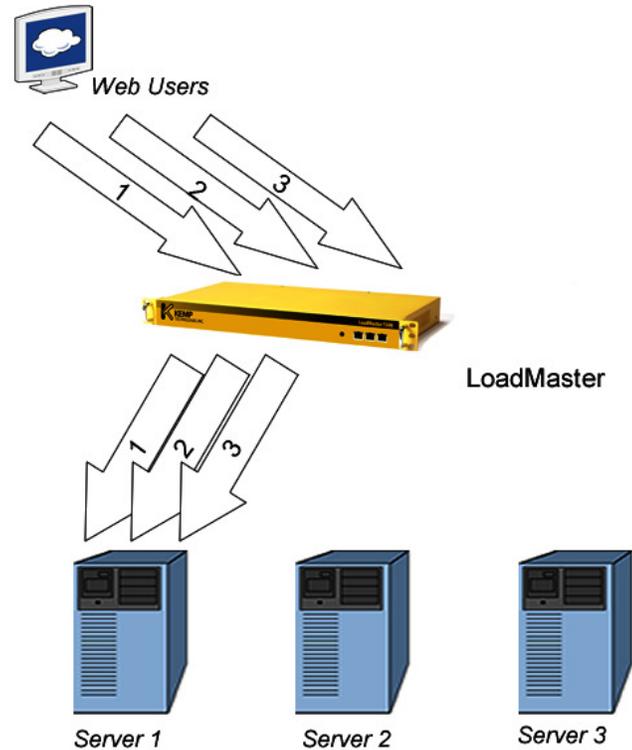


図-2：パーシステンス有りの負荷分散

## 7.2 パーシステンスの必要性

もし、稼働中のサイトがインタラクティブなサイトであればパーシステンスの必要性が高まります。ログインを求めてくるサイトですと殆ど必要です。もし、静的なテキストやイメージだけを提供するサイトであれば、パーシステンスの必要性はないかも知れません。ほとんどの場合、必要がないとしてもパーシステンスが悪い影響を与えることはありません。

ASPやPHP等の多数のウェブサイト用プログラム言語のセッションをハンドルするメカニズムは、ステートフル（状態保持）として知られ、ユーザのためにユニークなセッションを張り、その状態を同一のサーバに保存します。ログイン時のユーザ証明からショッピングカートの中身まで含んだこのステートフル（状態保持）情報は、一般的にサーバ間では共有しません。よって、複数のサーバを使用する場合は、各ユーザがインタラクティブにサーバとのやり取りを行っている間は、特定のサーバとの接続を保持することが重要で、パーシステンスは正にこのためにあります。

## 7.3 設定

パーシステンスは、バーチャルサービス毎にバーチャルサービス編集画面の **Basic Properties** グループ内で設定されます。この画面では、パーシステンスのために可能な全てのオプションがドロップダウンメニューで表示されます。(図-3)

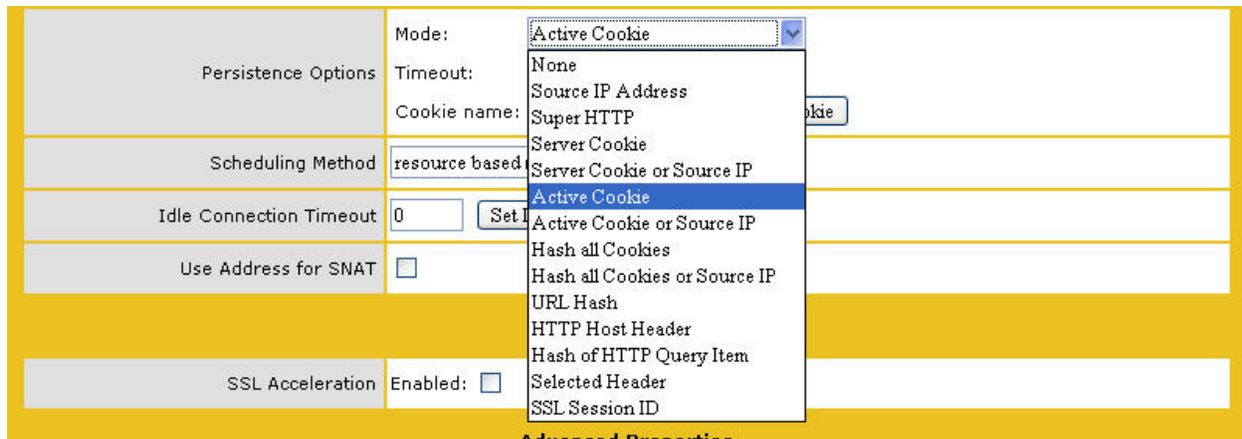


図- 3 : パーシステンス・モードのドロップダウン

**注意：** もし、VS がコンテンツスイッチを有効としている場合、このパーシステンス・メニューにはレイヤ7用の全てのオプションが表示されます。しかし、レイヤ7オプション（None,もしくは Source IP 以外）を選択した場合は、コンテンツスイッチは自動的に無効となります。そして、もし、ルールを既にリアルサーバへ適用している場合は、それらの設定は削除されます。

## 7.4 タイムアウト(Timeout)

各パーシステンス・モードには、各ユーザにどれだけのセッション維持時間が与えられるかを指定する、1分から24時間までの選択可能なタイムアウト値があります。(図-4)

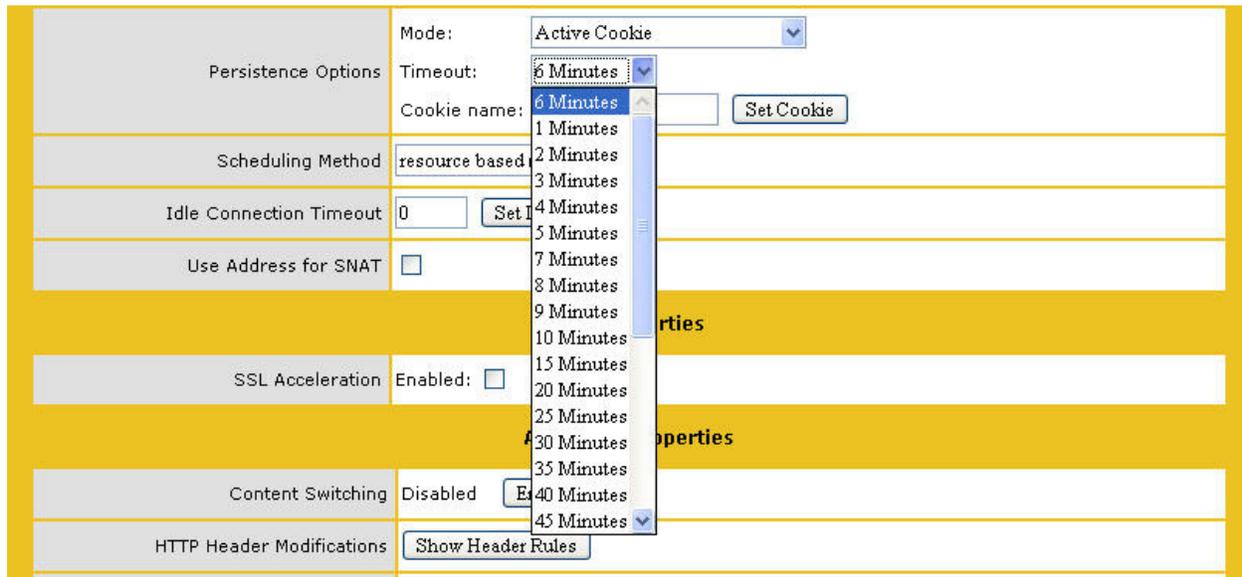


図- 4: タイムアウトの設定

このタイムアウトの時間は、直近のアクティブとなった接続の開始時間よりカウントされます。もし、クライアントがタイムアウト時間内に何度もバーチャルサービスにリクエストをした場合は、確実にセッションが同じサーバに維持されます。

例えば、もしバーチャルサービスのタイムアウト値を10分とし、そしてユーザが幾つかのリクエストを20分内で行ったとしても、各リクエストの間隔がいつも10分以内であればパーシステンスは有効です。もし、ユーザが20分間のアイドルを取った場合、次の接続は新しいセッションとしてカウントされ、リクエストは前回とは違うサーバへ送られるかもしれません。このようにタイムアウト値が十分な時間でない場合は、もっと長い値をセットする必要があります。基本的には、アプリケーション側の Timeout 値と同じにすることを推奨します。

## 7.5 レイヤ 4 パーシステンス方式

サーバファーム内にあるウェブサーバとの間でロードマスターがパーシステンスを可能にするには幾つかの方法があります。全ての方法が、基本的に各ユーザを同じサーバに維持するためですが、その方法は下記のように区別されています。

### 7.5.1 ソースIPアドレス・パーシステンス (Source IP Address Persistence)

ソース IP アドレス・パーシステンスは、入ってくるリクエストにあるソース IP アドレスをユーザの識別に使用します。これは、パーシステンスの一番シンプルな方式で、HTTP に関連しないものも含めて、全ての TCP プロトコルで働きます。

ソース IP パーシステンスは、コンテンツスイッチ、及びダイレクト・サーバ・リターン (DSR) と一緒に使用できる唯一のパーシステンスのオプションです。

### 7.5.2 ソースIPネットマスク (Source IP Netmask)

ソース IP パーシステンス方式のために、タイムアウト値の他にネットマスク設定オプションがあります (図-5 を参照)。これは、ロードマスターがパーシステンスを決定する際に IP アドレスをいかに細かく識別するかを決めるためのものです。この細やかさは、1人のユニークなユーザのための各単独 IP アドレスから(255.255.255.255)、各クラス A ネットワークを1つのシングルユーザとして扱うレンジ (207.0.0.0/8 のように1つ目のオクテット) までが可能です。

Persistence Options	Mode:	Source IP Address
	Timeout:	6 Minutes
	Netmask:	255.255.255.255

図-5 : ネットマスク設定

例えば、ネットマスクのセッティングを 255.255.255.255 としている場合、IP アドレス 192.168.0.100 と 192.168.0.101 は2つの異なるユーザとして扱われます。ネットマスクを

255.0.0.0 としている場合は、IP アドレス 207.0.10.10 と 207.200.234.10 は、両方とも 207.0.0.0/8 のネットワーク上のアドレスのために、同じユーザとして扱われます。

デフォルトのセッティング、255.255.255.255 は、一般的にほとんどの環境において十分といえます。

### ソース IP パーシシステムの欠点

ソース IP パーシシステムは、セッションを正しく維持するためには望ましくない、もしくは有効的でない状態があります。それらの状態に含まれるのは；

- ▶ ほとんど、もしくは全てのユーザが単一の IP アドレスを使う時
- ▶ ユーザが自信の IP アドレスを切り替える場合

最初のケースは、しばしば、多数のユーザが単一のプロキシを経由してリクエストしてきて、あたかもシングル IP から来たような状況に遭遇するものです。ソース IP パーシシステムでは、全てのこれらのユーザがシングルユーザに見えてしまいます。他にも同じようなことが起こるケースとしては、インターネットを経由して1つのオフィスから全てのクライアントのリクエストが来る場合です。オフィスで使用しているルータは、一般的に全てのオフィスのシステムを1つの IP アドレスに NAT してしまいます。そして全てのリクエストがシングルユーザからのように見えてしまいます。これは、新しいユーザ・リクエストが来ても、全てを分散しないで同じリアルサーバへと導き、偏った負荷分散の結果を招いてしまいます。

2つ目のケースは、歴史的に大きな憂慮点であるメガ-ISP（例えば Nifty や NTT）の幾つかでプロキシサーバを使っている場合です。このような場合、全てではないと思われませんが、使用しているプロキシの設定によって、もしくはネットワークの問題によって時々 IP アドレスをスイッチするケースが発生します。IP アドレスが変更されてしまうと、ソース IP パーシシステムでは、同じユーザが違ったユーザに見えてしまいます。

これらの各ケースは、どのような IP アドレスから来ても異なったユーザ毎にユニークなクッキー値を使うレイヤ7パーシシステムにより問題を解決出来ます。しかしながら、これは HTTP プロトコルのみにも働きます（HTTPS/SSL プロトコルで、セッションをロードマスターで終端した場合も）。

## 7.6 レイヤ7パーシシステム方式

IP アドレス、ポート以外に、HTTP プロトコルでは色々な情報をセッション維持のために使用する方法があります。

### 7.6.1 スーパーHTTP (Super HTTP)

スーパーHTTP オプションは、HTTP リクエストの中の “User-Agent” フィールドをハッシュ化した値を使用します。HTTP リクエスト内に同じ値が含まれているならば、前回接続したリアルサーバへと接続します。もし、HTTP リクエストの中に ‘MSRPC’ という MS Exchange サーバで使用する文字列が含まれていた場合は、“Authorization” フィールドも含め

てハッシュ化します。このオプションは、MS Exchange サーバの CAS サービス用バーチャルサービスを作成する時に利用されることを推奨します。

### 7.6.2 サーバクッキーパーシステンス (Server Cookie Persistence)

サーバクッキーオプションは、どのサーバに HTTP リクエストを送るかを決定する際に、サーバが作成した既存のクッキーを使うレイヤ7機能の1つです。この方式は、パッシブクッキーとも呼ばれ、ロードマスターはクッキーの作成や管理をしないで、単に HTTP パケットストリームの中の指定されたクッキーをモニターします。

Persistence Options	Mode:	Server Cookie
	Timeout:	6 Minutes
	Cookie name:	PHPSESSIONID
		Set Cookie

図-6：クッキー名のセッティング

サーバクッキーパーシステンスでは、ロードマスターがどのクッキーを参照すればよいかを知るために、クッキー名オプション（図-6）を設定する必要があります。サーバクッキーパーシステンスが問題なく働くためには、サーバによって作り出されるクッキーが、個々のユーザのためにユニークな値を持っている必要があります。

許容できるクッキーの一例として、クッキー名が **PHPSESSIONID** で、その値が **fc8613d118daa515203428777360e4ca** とすると、HTTP ヘッダーの中ではこのようになります。Cookie: **PHPSESSID=fc8613d118daa515203428777360e4ca**

“=” の後のストリングは、ユーザ毎にユニークで、サーバクッキーパーシステンスのために認識出来るものでなければなりません。

### 7.6.3 アクティブクッキーパーシステンス (Active Cookie Persistence)

アクティブクッキーパーシステンス方式は、サーバクッキーオプション方式と同じようにクッキーを使用するレイヤ7機能の1つですが、アクティブクッキーはサーバではなく、ロードマスターによりクッキーが作り出されます。

アクティブクッキーパーシステンス方式を設定したバーチャルサービスに接続要求があった時、ロードマスターは特定のクッキーを見つけ出そうとします。もし、そのクッキーがない場合は、サーバからのレスポンスをクライアントに返す時に、HTTP パケット内に **Set-Cookie** ディレクティブとしてクッキーを挿入します。既にレスポンス内にサーバからのクッキーが存在した場合でも、そのクッキーの破棄、改ざん等は行わずに新たにクッキーを追加します。

アクティブクッキーの値は、ロードマスターがユーザを識別するためにユーザ毎にユニークです。

この方式の長所は、サーバでクッキーを作成、管理する必要がなくサーバ設定の負担を軽減できることです。

共通のプロキシサーバなどを経由してクライアントからの HTTP セッションが張られる場合は、違うユーザでも同じクッキーが使用されて負荷が正常に分散されません。この場合は、

各セッション毎にアサインされるポート番号をクッキーに挿入させる “Add Port to Active Cookie” 機能をオンにしてください。

#### **7.6.4 サーバクッキー、もしくはソースIPパーシステンス (Server Cookie or Source IP Persistence)**

サーバクッキー、もしくはソース IP のセッティングは、サーバクッキー・パーシステンスと同じです。もし、何らかの理由で期待していたクッキーが検出出来なかった時（例えばユーザがクッキーの使用を許可していない時に起こり得ます）、パーシステンスの決定にソース IP アドレスが使用されます。

#### **7.6.5 アクティブクッキー、もしくはソースIPパーシステンス (Active Cookie or Source IP Persistence)**

アクティブクッキー、もしくはソース IP のセッティングは、アクティブクッキー・パーシステンスと同じです。もし、何らかの理由で期待していたクッキーが検出出来なかった時、パーシステンスの決定にソース IP アドレスが使用されます。

もし、特別な条件が無く、レイヤ7のパーシステンスの使用を意図するならばこの方式を推奨します。サーバでの設定は必要ありませんし、ロードマスターがクッキー関連の全ての管理を行うことと、クライアントがクッキーを許可しない設定を行っている場合、ソース IP アドレスを使用することが可能だからです。

#### **7.6.6 ハッシュ全クッキー・パーシステンス (Hash All Cookies Persistence)**

ハッシュ全クッキー方式は、HTTP ストリームの中の全クッキーの値を用いてハッシュを作り出します。もしこの値が異なったら、まったく新しい接続として扱います。そして、リクエストは負荷分散アルゴリズムに従ってサーバへと配分されます。

#### **7.6.7 ハッシュ全クッキー、もしくはソースIPパーシステンス (Hash All Cookies or Source IP Persistence)**

ハッシュ全クッキー、もしくはソース IP は、ハッシュ全クッキーと同じですが、HTTP リクエスト内にクッキーがなかった場合にパーシステンスにソース IP アドレスが使用されます。

#### **7.6.8 URLハッシュ・パーシステンス (URL Hash Persistence)**

URL ハッシュパーシステンス方式を用いると、ロードマスターは同じ URL のリクエストを同じサーバへ送ります。

#### **7.6.9 HTTPホスト・ヘッダー・パーシステンス (HTTP Host Header Persistence)**

HTTP ホスト・ヘッダー・パーシステンス方式を用いると、ロードマスターは HTTP ヘッダーの “Host” の中に同じ値を含む全てのリクエストを同じサーバへ送ります。

### 7.6.10 SSLセッションIDパーシステンス (SSL Session ID Persistence)

SSLセッションIDパーシステンスのために、ロードマスターは各SSL接続間に存在するSSLセッションIDを使用します。SSLセッションIDは、ユーザ毎にユニークなために、ロードマスターはこれをユーザ識別に使い、同じユーザを同一サーバへと接続します。この方式は、SSLトラフィックに対してのみ有効です。

残念ながら、この方式は現在あまり有益性をもたらしてくれません。特定のOSとブラウザの組み合わせでは、SSLセッションIDを2分おきに変更するために、ロードマスターが同じユーザにも関わらず別のユーザとして識別してしまうためです。

### 7.6.11 ハッシュHTTPクエリ項目パーシステンス (Hash of HTTP Query Item Persistence)

この方式は、URLハッシュパーシステンスとまったく同じように働きますが、ネーム項目の代わりにURLのクエリ文内のクエリ項目を判別します。同じクエリ項目値を持った全てのリクエストは、同じサーバへと送られます。

### 7.6.12 Selected Header (指定ヘッダー)

特定のHTTPヘッダーを指定して、そのヘッダーによるパーシステンスを行います。

### 7.6.13 ターミナルサービス (Terminal Service)

この方式は、マイクロソフト・ターミナル・サービス負荷分散用にのみ適用可能です。詳細は“9. マイクロソフト・ターミナル・サービス負荷分散”の項を参照してください。

### 7.6.14 ターミナルサービス、もしくはソースIPアドレス (Terminal Service or Source IP)

この方式は、マイクロソフト・ターミナル・サービス負荷分散用にのみ適用可能です。詳細は“9. マイクロソフト・ターミナル・サービス負荷分散”の項を参照してください。

## 7.7 パーシステンスとHTTPS/SSL

HTTPS/SSLでは、幾つかの考慮点があります。もし、SSLアクセラレーション機能を使用しない (SSLセッションをロードマスターで終端しない) 場合、選択できるオプションはソースIPアドレスかセッションID (あまり効果が期待できない) のみとなってしまいます。これは、SSLセッションを終端しない事によりパケットが暗号化されたままであり、ロードマスターはHTTPヘッダー、もしくはレイヤ7情報を見ることが出来ないためです。

もし、ロードマスターでSSLアクセラレーション機能によりHTTPS/SSLを終端するならば、ロードマスターがサポートしているどのパーシステンスのオプションでも使用することが可能です。HTTP/SSLセッションが終端されると、ロードマスターは復号化された全てのトラフィックを見ることが可能で、もちろんHTTPストリームも見ることが出来ます。これは、

HTTPS/SSL セッションを一旦ロードマスターで終端し、再度リアルサーバとの間で SSL セッションを確立する SSL リバースの場合も同様です。

## 7.8 ポート・フォローイング (Port Following)

ユーザが商品を選択、又はリストに追加するショッピングカートを使用する時は、一般には HTTP 用バーチャルサービスにより行われますので、上記のどのパーシステンス方式でも使用可能です。ユーザがそれらの商品に対して購入を決定した後、クレジットカードなどによる支払い処理では、一般的にはセキュアな SSL (https) 用バーチャルサービスに切り替わり実行されます。バーチャルサービスが、HTTP 用から HTTPS 用に切り替わる時に、2つのサービス間で同じリアルサーバに接続を継続させる機能がポートフォローイングです。ポートフォローイングがオンになっていれば、ショッピングカートに入れた商品を購入しようとしてクレジットカードなどによる支払い処理のために、SSL セッションに切り替わっても引き続き処理が継続されるはずですが、もし、ポートフォローイング機能が HTTP 用と HTTPS 用バーチャルサービス間でオンになっていなければ、サービスが切り替わった時に今までのショッピングカートの商品リストの情報を保持したリアルサーバ以外のサーバに接続され、支払い処理時その情報が取得できないという問題が発生する場合があります。

ポートフォローイングをオンにした接続試験例として、オンラインショッピングサイト “[www.onlineshop.com](http://www.onlineshop.com)” の為に HTTP と HTTPS 用バーチャルサービスを設定しているとします。最初に URL ‘<http://www.onlineshop.com>’ に HTTP サービスのアクセスを行います。その後、今度は ‘<https://www.onlineshop.com>’ に HTTPS による SSL 接続を行います。SSL セッションは初めの HTTP サービスを提供した同じサーバと接続されるはずですが。

**注意：**この機能は、両バーチャルサービスに同じリアルサーバが設定されており、両方のバーチャルサービスが同じ L7 パーシステンスオプションを選択している場合のみ有効になります。

### ポートフォローイングの設定

1. HTTP (ポート番号 80)、及び HTTPS 用 (ポート番号 443) バーチャルサービスを作成します。HTTPS 用バーチャルサービスは、SSL Acceleration 機能をオンにして、SSL オフローディングとしなければなりません。SSL Acceleration 機能なしでは、クッキーが判読できないためにこの機能が使用出来ません。
2. **Virtual Services** サブメニューの **View/Modify Existing** オプションを選択して **Properties** をチェックします。
3. ポート 80 と 443 の両方のパーシステンスオプションが同じクッキーに設定されていて、“**Timeout**”、及び “**Cookie Name**” も同じであることを再確認します。
4. 両方のバーチャルサービスの属性 (Prpperties) で、**Advanced Properties** セクションにある “**Port Following**” をオンにします。そして、リストの中から相手のバーチャルサービスを選択します。

5. 10秒待つか、**Basic Properties** セクションにある “**Activate or Deactivate Service**” のチェックマークをオフ/オンして、新しい設定を有効とします。

## 8 アプリケーション・フロントエンド (AFE)

アプリケーション・フロントエンド (AFE) は、ウェブアプリのデータ配信とネットワークの効率を高めるためのグループ機能です。ロードマスターは、AFE を新たに実装することにより、既に実装済みの容易な管理、透明的な高パフォーマンスの負荷分散機能を損なわずに、より一層高いスループットとサーバのパフォーマンス向上という誰もが求める基本的な要求を満たします。ロードマスターの AFE サービスは、下記の機能を含んでいます。

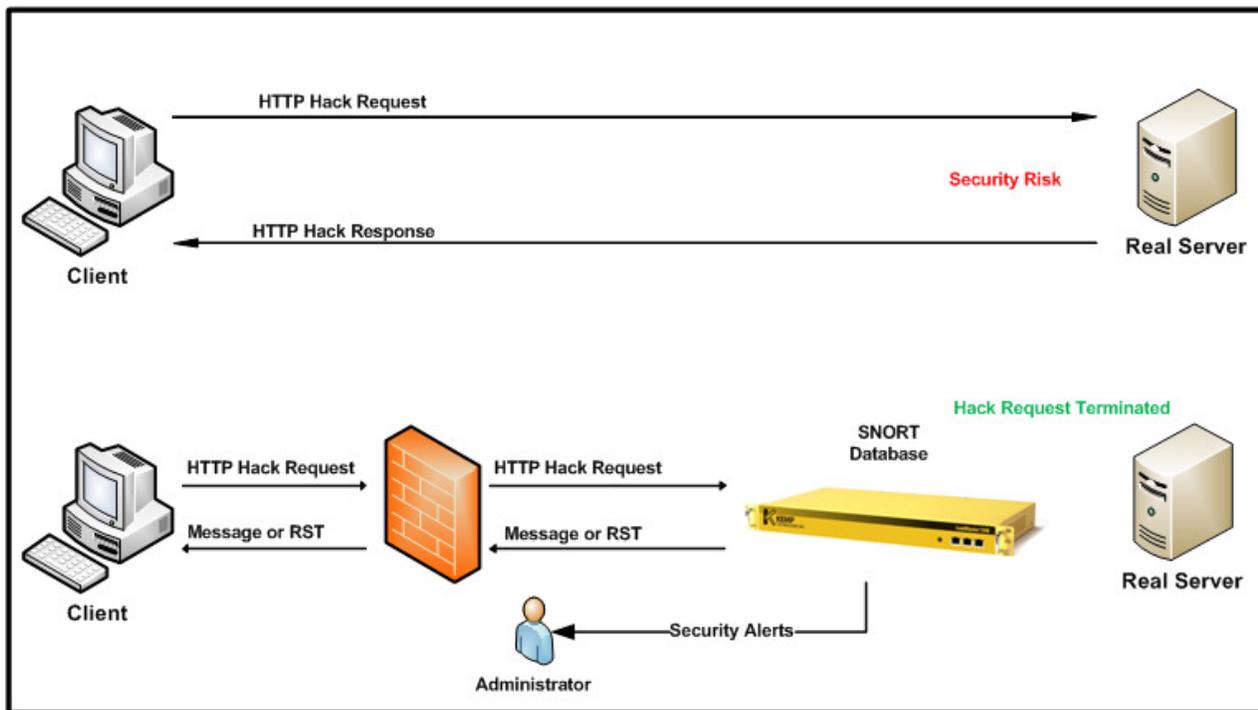
- ネットワーク侵入防止システム (IPS)
- キャッシング
- データ圧縮

各機能は、バーチャルサービス毎に設定することが可能です。

注: AFE 機能は、ライセンスで制御されます。もし LM2000、及びそれ以上のモデルでこの機能が使えないならば、弊社代理店までご連絡ください。新しいライセンスキーを発行します。

### 8.1 ネットワーク侵入防止システム (IPS)

ロードマスターは、この HTTP 侵入防止機能を有効にすることで一層強固なインターネット装置となります。従来の SSL に、この IPS が持つ DoS 攻撃防御が追加されることで、リアルタイムに攻撃を軽減するだけでなく、クリティカルな攻撃にはリアルサーバを切り離すことで守ります。侵入防止システムは、業界標準である SNORT データベースをベースにしており、侵入が検知されたらリアルタイムで警告を発します。



### バーチャルサービスの設定

IPS 機能は、HTTP と SSL アクセラレーション（オフローディング）を有効にした HTTPS 用バーチャルサービスで有効に出来ます。この機能を設定するためには、バーチャルサービスの“Service Type”が‘HTTP/HTTPS’であることを確認後、下図のように“Advanced Properties”内の“Detect Malicious Requests”にチェックマークを入れます。

Advanced Properties	
Healthcheck URL	<input type="text"/> <input type="button" value="Set URL"/>
HTTP Healthcheck Method	HEAD ▾
Content Switching	Disabled <input type="button" value="Enable"/>
Enable Caching	<input type="checkbox"/>
Enable Compression	<input type="checkbox"/>
Detect Malicious Requests	<input checked="" type="checkbox"/> Intrusion Handling <input type="button" value="Drop Connection"/> ▾ Warnings <input checked="" type="checkbox"/>

“SNORT” ルールにマッチしたリクエストの扱いには、2つのオプションがあります。‘Drop Connection’か‘Send Reject’です。両オプションとも、RS への到達を許さず、侵入を試みたクライアントに対してレスポンスを返すか否かを設定します。

### Drop Connection

“SNORT” ルールにマッチした場合、HTTP レスポンスを返しません。TCP 接続は切断され、結果的に HTML コンテンツのクライアントへの返信はありません。

## Send Reject

“SNORT” ルールにマッチした場合は、ロードマスターは侵入を試みたクライアントへ HTTP 400 “Invalid Request” と、マッチした内容を示すメッセージを HTML 形式で返信します。参考例を以下に示します。

サンプルリクエスト : `http://<VIP>/modules/articles/index.php?cat_id=SQL`

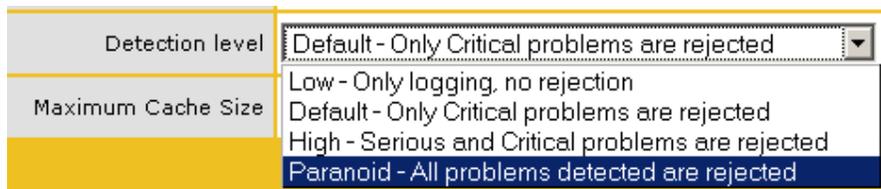
サンプルレスポンス : `<html><head><title>400 Invalid Request</title></head><body>Invalid Request: COMMUNITY WEB-PHP Xoops module Articles SQL Injection Exploit</body>`

## Detection level

ルールがマッチングするレベルを、システムとして下記のようなレベルに設定変更が可能です。詳細につきましては、[‘http://www.snort.org/docs/snort\\_manual/node220.html’](http://www.snort.org/docs/snort_manual/node220.html) を参照ください。

Default = 高セキュリティのルールにマッチしたリクエストをブロックし、記録します。  
 High = 高、及び中セキュリティのルールにマッチしたリクエストをブロックし、記録します。  
 Paranoid = 全てのセキュリティレベルにマッチしたルールをブロックし、記録します。

設定方法 : WUI にアクセスし、System Configuration -> Miscellaneous Options -> L7 Configuration



## 警告

侵入防止機能は、悪意のあるアクセスと判断した接続を切断しますが、しかしながらいくつかのものは明確には判断出来ない場合があります。これらに対しては、デフォルトではブロックせず記録も残しませんが、“WARNING” オプションを有効にすればログに記録します。SNORT のルールファイルの中で、これらのマイナーなアクティビティとして指定されている、危険でないオペレーションリクエストの例を下記に示します。

Uri: `"/OvCgi/OpenView5.exe?Context=Snmp&Action=Snmp&Host=&Oid="`  
 which is described as "WEB-MISC HP OpenView Manager DOS" and is only suspicious

## 侵入警告

全ての侵入警告は、“System” と “Warning” ログの中に記録されます。又、警告通知は、Syslog サーバ、及び E-Mail として SMTP サーバに、最低レベル “Notice” として送信可能で

す。侵入警告は、重要警告として記録維持のために Syslog サーバによって記録されることを推奨します。

## SNORT設定

新しいルールは、“[www.snort.org](http://www.snort.org)”よりダウンロードが出来ます。新しいルールセットを取得、もしくは作成したら、WUIの“System Configuration”サブメニューの“Miscellaneous Options”下の“L7 Configuration”オプションの“Detection Rules”を使ってシステムへの取り込みを行う必要があります。“Browse”ボタンをクリックして、ダウンロード、もしくは作成したルール用ファイルを選択します。ルール用ファイルは、“Tar”、もしくは“Gzip”でエンコードされたもので“tar.gz”の拡張子を持っていて、“rules”のディレクトリー下にファイルが存在しなければなりません。ロードマスターは、このファイルを解凍して新しいルールとして既存のルールをリプレースします。因みに、“tar.gz”の拡張子は、[www.snort.org](http://www.snort.org)より新しいルールをダウンロードするときのファイルのスタンダードです。ロードマスターの出荷時は、GPLに準拠した共通ルールをインストールしています。

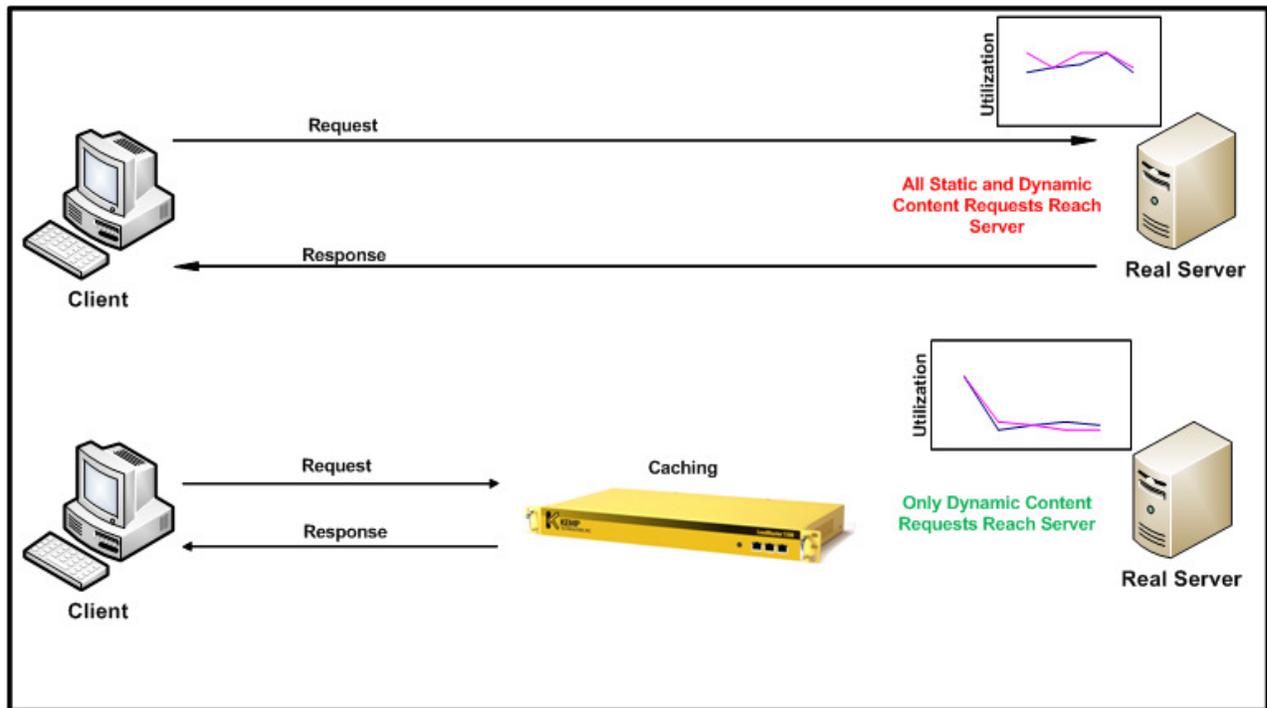


## 8.2 キャッシング

ロードマスターの持つ先進的なキャッシング用エンジンは、リアルサーバの貴重な処理能力とネットワーク帯域使用を節約し、クリティカルなコアビジネス用アプリケーションだけに威力を発揮出来るように専念させます。

キャッシング機能は、際立ったサーバのパフォーマンス向上をもたらすことに貢献します。クライアントとサーバが頻繁に相互通信をする HTTP のようなプロトコルでは、静的なリソースをフェッチするために、ネットワークとリアルサーバ上の不必要なリソース使用を抑えるために接続と切断がひっきりなしに繰り返されます。

一般的に、アプリケーションの威力をより発揮させるために、キャッシング機能を有効にし、ネットワーク帯域とそれに関連するリソースの使用を適正化します。ロードマスターでは、キャッシング機能を利用することで、リアルサーバへのウェブ用トラフィックを減少させ、結果的にリアルサーバ接続の帯域とサーバ上のリソース使用を節約し、アプリケーションの処理能力を向上させます。



### バーチャルサービスの設定

キャッシング機能は、HTTP と SSL オフローディング用 HTTPS のバーチャルサービスで有効に出来ます。この機能を設定するには、バーチャルサービスの“Service Type”が‘HTTP/HTTPS’であることが前提です。それを確認後、“Advanced Properties”内の“Enable Caching”にチェックマークを入れます。キャッシングは、静的なコンテンツだけを蓄積します。

注：“no-cache”ヘッダーを持つHTTP/HTTPS リクエストは、キャッシング機能をバイパスします。キャッシュ処理は、メモリーへの蓄積を行うのに少し時間を必要としますので、静的なコンテンツが正しくキャッシュされるまで最大で30秒間待つ必要があります。

Advanced Properties	
Healthcheck URL	<input type="text"/> <input type="button" value="Set URL"/>
HTTP Healthcheck Method	HEAD ▼
Content Switching	Disabled <input type="button" value="Enable"/>
Enable Caching	<input checked="" type="checkbox"/> Maximum Cache usage <input type="button" value="No Limit"/> ▼

### Maximum cache usage (最大キャッシュ使用)

このオプションは、キャッシュメモリーのサイズに制限を設けるのを目的としています。この制限は、バーチャルサービス毎に設定します。例えば、2つのバーチャルサービスが最大

キャッシュのメモリー使用制限を50%ずつに設定したとすると、合計で100%のキャッシュメモリーを使用することになります。

デフォルトは‘No Limit’となっていますが、メモリーが均等に使用されないことを防止するためにこの最大キャッシュ使用制限を設定することを推奨します。各バーチャルサービスが正しくキャッシングメモリーを使えるように、この“Maximum cache usage”を調整してください。もし設定が正しくなくメモリーに空きがない場合は、このサービスではコンテンツのキャッシュが行われません。

### キャッシュのフラッシング

ロードマスターは、リアルサーバのファイルが更新されるのをモニターしていません。よって、もしファイルが更新されても、キャッシュメモリー内にストアされている内容を自動的に更新しません。内容を更新させるためには、この機能を一旦無効にしてから再度有効にしてメモリーのフラッシングを行わせる必要があります。但し、キャッシングされたファイルは、もし期限が限定されていなければ1時間で消去されます。

### Maximum Cache Size (最大キャッシュサイズ)

システム全体で使用出来るキャッシュ用メモリーサイズの最大値を設定します。この値は、実際実装されているメモリーサイズに連動しています。(基本的な最大設定値は、システムが実装しているメモリーサイズの5分の一です。) WUIの“System Configuration”->“Miscellaneous Options”->“L7 Configuration”から設定可能です。

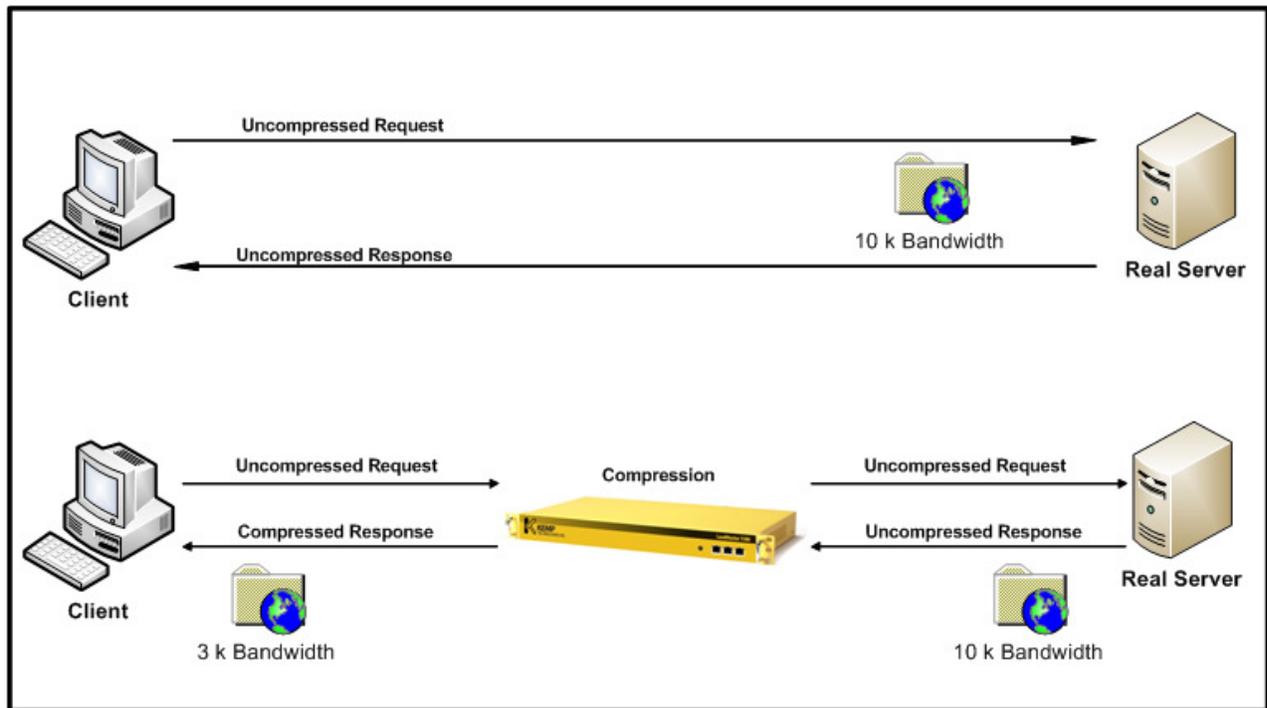
Maximum Cache Size	<input type="text" value="100"/>	(Valid values:1 - 102)
--------------------	----------------------------------	------------------------

(注：単位はMBです)

## 8.3 データ圧縮

ロードマスターのデータ圧縮機能は、一般的なブラウザで利用出来る“gzip”圧縮を使用することで、転送するHTTPオブジェクトのデータ量を減らします。Lempel-Ziv(LZ)とHTTP/1.1 GNU zip (gzip)のコンテンツ圧縮/エンコーディングにより、Textファイル (HTML、CSS、JavaScript)を高圧縮することでネットワークの使用帯域を減少させます。

データ圧縮は、圧縮する内容の品質を落とすことなく、アプリケーションのリクエストパケット毎のペイロードを圧縮することが可能なために、その結果、ネットワークの使用帯域を少なくし、ユーザのレスポンスに対する満足度を向上させます。圧縮率は、ファイルの種類により変化します。



注：圧縮は、ファイルを一旦ロードマスターで完全に受け取った後で処理を行うために、リアルタイム処理に遅延が出る可能性があります。リアルサーバからのファイル受信処理を減少させるキャッシュ機能を併用して使用することで、圧縮機能がサービスのスループットのボトルネックになるのを防げます。

### バーチャルサービスの設定

データ圧縮は、HTTP、及びHTTPS（SSL オフローディング）用バーチャルサービスで有効に出来ます。この機能を有効にするには、バーチャルサービスのサービスタイプが‘HTTP/HTTPS’になっている必要があります。その設定を確認後、“Advanced Properties”内の“Enable Compression”ボックスにチェックマークを入れます。

Advanced Properties	
Content Switching	Disabled <input type="button" value="Enable"/>
HTTP Header Modifications	<input type="button" value="Show Header Rules"/>
Enable Caching	<input checked="" type="checkbox"/> Maximum Cache usage <input type="button" value="No Limit"/>
Enable Compression	<input checked="" type="checkbox"/>
Detect Malicious Requests	<input type="checkbox"/>

圧縮は、ブラウザ側で“gzip”をサポートしているかどうかによります。ブラウザとロードマスター間で圧縮が行われているかどうかは、HTTP トラフィックをトレースすること

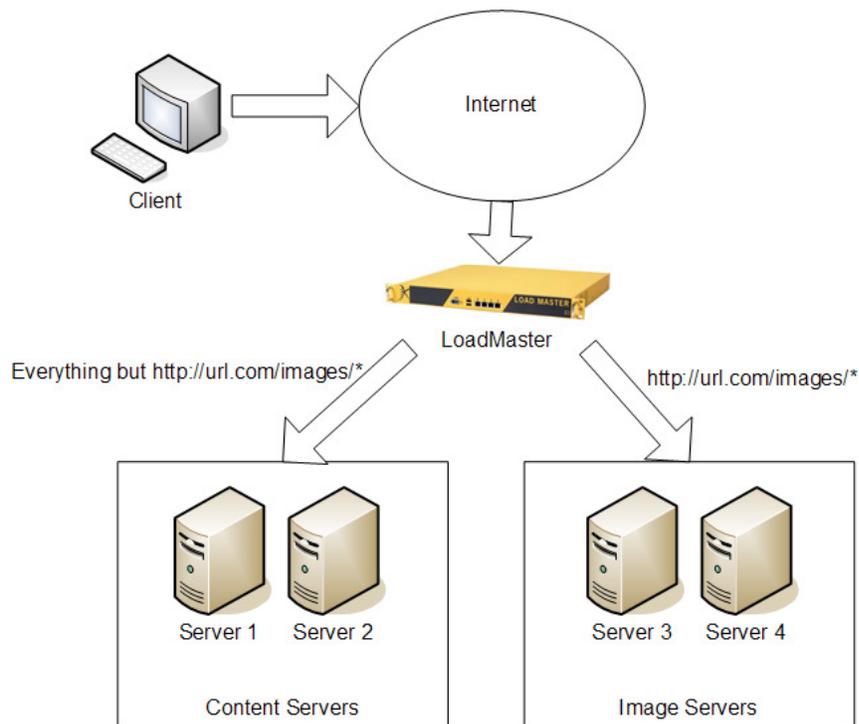
で確認が出来ます。下記の **HTTP** ヘッダーがブラウザからロードマスターへのパケットトレースに含まれていたら、圧縮が行われています。

**Content-Encoding: gzip**

## 9 ルールベースのコンテンツ・スイッチ

ロードマスターシリーズでは、一般的に URL スイッチングと呼ばれるコンテンツ・スイッチをサポートしています。これは、リクエストされた URL の内容を基に、ロードマスターが特定のリクエストを特定のリアルサーバへ導くものです。

例えば、1つのグループはイメージだけ提供するサーバ群で、他のグループはそれ以外の全ての内容を提供する2つのグループのサーバ群を持っていたとすると、2つの種類のリクエストを分けるためのコンテンツルールを作成することが出来ます（図—25）。



図—25：コンテンツスイッチの概要

/images を含んだ URL、例えば“<http://url.com/images/party.jpg>” や <http://url.com/images/dogs.jpg> は、サーバ3と4に導かれ、他はサーバ1と2に導かれるようにします。

これは、アプリケーション・サーバ、スタティック・コンテンツ・サーバ、マッピング・サーバや特定コンテンツ作成サーバなどの、同じホストネーム下（例えば [www.websitename.co.jp](http://www.websitename.co.jp)）で異なる機能のサーバを持っている時に役立ちます。

## 9.1 用語

注意：コンテンツスイッチの用語は、レイヤ2スイッチが絡むプロセスを表わしたものではありません。それよりも、異なるサーバ間でリクエストされたコンテンツに応じてトラフィックをスイッチするといった方が良いでしょう。

## 9.2 コンテンツスイッチの制約

コンテンツスイッチを有効にしたバーチャルサービスでは、クッキー・パーシステンスなどの他のレイヤ7機能が使用出来ません。1つのバーチャルサービスでコンテンツスイッチを使用し、他のバーチャルサービスでレイヤ7クッキー・パーシステンスを使用するようには出来ませんが、同じバーチャルサービスで両方を有効には出来ません。

## 9.3 コンテンツスイッチの使用

コンテンツスイッチを設定するためには、コンテンツルールとバーチャルサービスの2つの設定箇所があります。コンテンツルールは、ロードマスター上でシステム規模で設定します。そして、バーチャルサービス下の特定リアルサーバへそれらのルールを適用します。最初に行わなければならないのはルールの作成です。

## 9.4 コンテンツルールのセットアップ

WUI画面の左側のメインメニューから、**Rules&Checking** を選びます。その配下の **Content Rules** をクリックすると、現状で作成してある全てのコンテンツルールのリストが表示されます（図—26）。



Content Matching Rules				
Operation	Name	Match Type	Options Header	Pattern

図—26：コンテンツルール管理

隠れたルールとして、全てにマッチして編集が出来ない **default** というルールがあります。コンテンツルールを作成するために、“Create New...”ボタンをクリックすると **Create Rule** 画面に移動します（図—27）。

Rule Name	Images
Rule Type	Content Matching ▼
Match Type	Prefix ▼
Header Field	
Match String	/images/*
Negation	<input type="checkbox"/>
Ignore Case	<input type="checkbox"/>
Include Host in URL	<input type="checkbox"/>
Include Query in URL	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Create Rule"/>	

図一 2 7 : Create Rule 画面

1つのサーバグループのルールパスである/images/を持つ全てのURLリクエストを送るルールを作成するために、Match String フィールドに“/images/\*”と入力します。ストリング（文）を基にマッチさせるか、排他するかの提示タイプなのでこの入力にはレギュラー・エクスプレッションで行います。レギュラー・エクスプレッションでは“\*”は全てにマッチする意味となります。

レギュラー・エクスプレッションは、文字の連続です。スペシャル文字でないどの文字もそれ自身とマッチします。スペシャル文字として下記があります。

- “^” これは文字列の最初にしか適用されません。  
URLの最初の文字とマッチしなければなりません。
- “\$” これは、文字列の最後にしか適用されません。  
URLの最後の文字とマッチしなければならないことを意味しています。
- “?” これは、どの単一文字ともマッチします。
- “\*” これは、0バイトもしくはそれ以上の文字とマッチします。
- “[” これは、記号のセットの始まりを意味します。セットされた内容の単一文字とマッチします。もしこれが“^”で始まるなら、セットにないどの単一文字ともマッチします。  
例えば、 “[0-9]” は一桁のどの数字ともマッチします。  
 “[^abf]” は、“a”、“b”、“f”以外のどの単一文字ともマッチします。  
 “^[^a-z]” は、URLの最初の文字が小英文字以外であればマッチします。

<例>

ここに幾つかの例を挙げます。

“/home/\*.gif” これは、/home ディレクトリーの.gif の拡張子を持った全てのファイルを指している URL とマッチします。

“[gG][iI][fF]” これは、文字列に“gif”、“GIF”、“gIF”、“giF”、“GiF”等を含んだ全ての URL にマッチします。

**注意：** “/home/cgi-bin/XXX.cmd?value=hello”のように入力用 URL が与えられた場合の文字列の最後の文字は”?”の前となります。例えば、postfix として”cmd”はこの URL でマッチしますが、”hello”はマッチしません。

URL の中に Host を含ませるかはオプションです (support.kemptechnologies.jp をマッチさせるかどうかのように)。

他のオプションとして Negation が有ります。Negation なしでは、“/images/”を含む全てのリクエストは上記のルールにマッチしますが、Negation をオンにすると、“/images/”を含まない全てのリクエストがこのルールのマッチ対象となります。

“Include query”オプションは、URL クエリのように “?” の後の文字列も含ませてマッチングを行います。1つの例えとして、

<http://support.kemptechnologies.com/images/imagid.jsp?item=1> は、“item=1”がクエリ項目です。

“Commit” ボタンをクリックするとルールは追加されますが、どのバーチャルサービスもその影響を受けることはありません。一度ルールが追加された後、各バーチャルサービス内のリアルサーバへそれを適用する必要があります。

## 9.5 バーチャルサービスへの適用

コンテンツスイッチをバーチャルサービスへ適用する最初のステップは、パーシステンス・オプションが“None”もしくは“Source IP” (レイヤ4パーシステンス・オプション) になっているか確かめることです。

パーシステンスが正しいオプションに設定されているならば、コンテンツスイッチを有効にするパラメータが“Content Switching”が“Advanced Properties”内にあるはず (図—28)。



図—28 : コンテンツスイッチの有効化

これを有効にすると、どのリアルサーバも右側に新しい欄 “Rules”が追加されたのが見えるはず (図—29)。

Operation			IP Address	Port	Forwarding method	Weight	Status	Rules
Disable	Modify	Delete	192.168.3.25	80	nat	1000	Enabled	None
Disable	Modify	Delete	192.168.3.31	80	nat	1000	Enabled	None

図一 2 9 : Rules 欄の追加

コンテンツスイッチを有効にただけでは、ルールはアクティブになりません。1つのバーチャルサービスに設定されている4つのウェブサーバを例にして見てみましょう。これらのサーバは、192.168.1.100, 101, 102, と 103 とします。図の25のように、100と101のサーバは全般のコンテンツ用で、102と103はイメージ用のサーバとします。

各サーバの“None”ボタンをクリックします。この時、どのサーバにも複数のルールを追加する機会が与えられます。しかし、この例では各サーバに1つのみルールを設定します。前のセクションで作成したルールをサーバ102、103へ、そして100と101にデフォルトルールを適用します（図一30）。



図一 3 0 : ルールの追加

Operation			IP Address	Port	Forwarding method	Weight	Status	Rules
Disable	Modify	Delete	192.168.1.100	80	nat	1000	Enabled	1
Disable	Modify	Delete	192.168.1.101	80	nat	1000	Enabled	1
Disable	Modify	Delete	192.168.1.102	80	nat	1000	Enabled	1
Disable	Modify	Delete	192.168.1.103	80	nat	1000	Enabled	1

図一31 : ルールの追加後

4つのサーバのルール欄に、1つずつのルールが設定されたことが確認できます（図一31）。この時点で、この設定が正しく動作するかテストが行えます。

**注：**コンテンツスイッチ機能が正しく働くために、リアルサーバのHTTP Keepalive機能を無効にする必要があります。この機能を無効にすることで発生するインパクトについては、RFC 2616を参照願います。

## 10 ヘルスチェック

ロードマスターは、レイヤ3、レイヤ4、及びレイヤ7のヘルスチェックをリアルサーバとバーチャルサービスの可用性確認のために使用します。1つのサーバがヘルスチェックの応答を定義された時間間隔とリトライ回数以内に返さない場合は、サーバの重みがゼロに設定されます。この重みゼロは、リアルサーバがオンラインに戻ったことが確認されるまで、バーチャルサービス設定から外されることを意味します。

ロードマスターが使うこれらのレイヤ3、レイヤ4、レイヤ7のヘルスチェックの設定は、WUIもしくはコンソールからCLIを介して行うことができます。ロードマスターは、下記のポートに対して最も可能性の高いヘルスチェック方式を、デフォルトとしてバーチャルサービスに関連付けます。

サービス	ポート	プロトコル
FTP	21	TCP
TELNET	23	TCP
SMTP	25	TCP
HTTP	80	TCP
HTTPS	443	TCP
POP3	110	TCP
NNTP	119	TCP
IMAP	143	TCP
DNS	53	UDP
RDP	3389	TCP

これ以外のポートに対しては、ロードマスターはTCPサービスならばレイヤ4ヘルスチェック、UDPサービスであればレイヤ3のヘルスチェックを使用します。ヘルスチェックのセッティングは、バーチャルサービスのプロパティでデフォルトからスタンダードでない設定へと調整できます。例えば、HTTPサービスがポート80ではなく8080で稼動している場合、デフォルトのレイヤ4ヘルスチェック方式よりHTTPに変更できます。

注意：ヘルスチェックのタイムアウト、リトライ回数の設定は、システム全体の共通のものでサーバ毎に違う値の設定は出来ません。

ロードマスターでは、バーチャルサービスを定義するときに、必ず1つのサービスチェックのオプションを使用するようにしなければなりません。

### 10.1 サービス、ノンサービスベースのヘルスチェック

レイヤ3ヘルスチェックは、リアルサーバをネットワークを通してチェックするためにICMPベースのエコーリクエスト（ping）を使います。レイヤ3チェック方式は、バーチャルサービスに頼らないもので、これが失敗すると該当するリアルサーバは、そのサーバを定義している全てのバーチャルサービスから外されます。

サービスベースのヘルスチェック方式は、レイヤ3ヘルスチェックと対照に、レイヤ4、レイヤ7の両方の方式でバーチャルサービスに関連付けられています。リアルサーバがそのよ

うなサービスチェックに失敗した場合は、該当するバーチャルサービスのみ外され、その他のバーチャルサービスでは同じリアルサーバでも影響を受けません。

<u>レイヤ</u>	<u>タイプ</u>	<u>詳細</u>
3	ICMP	ロードマスターは、リアルサーバに ICMP エコーリクエスト (ping) を送ります。リアルサーバは、設定してあるリトライ回数内でタイムアウト時間内に ICMP エコーレスポンスを返さないとチェックに失敗します。
4	TCP	ロードマスターは、設定されているリアルサーバのサービスポートに TCP 接続を開きます。サーバの設定ポートに TCP SYN パケットを送付します。サーバが、TCP SYN ACK を設定してあるリトライ回数内でタイムアウト時間内に返すとチェックはパスします。この場合は、ロードマスターは TCP RESET パケットを送り接続を閉じます。もし、時間内にレスポンスがないとチェックが失敗し、サーバはダウンしているものとみなします。
7	FTP	ロードマスターは、リアルサーバのサービスポート (ポート 21) 上に TCP 接続を開きます。もしサーバが、ステータス・コード 220 と一緒にグリーティング・メッセージを返すと、ロードマスターは QUIT コマンドをサーバに送り接続を閉じて、サーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。
7	TELNET	ロードマスターは、リアルサーバのサービスポート (ポート 23) に TCP 接続を開きます。もし、サーバが char '0xff' で始まるコマンド文字を返すと、ロードマスターは接続を閉じサーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うコマンド文字が返すとサーバはダウンしているものとみなします。
7	SMTP	ロードマスターは、リアルサーバのサービスポート (ポート 25) に TCP 接続を開きます。もしサーバが、ステータス・コード 220 と一緒にグリーティング・メッセージを受け取ると、ロードマスターは QUIT コマンドをサーバに送り接続を閉じて、サーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。
7	HTTP	ロードマスターは、リアルサーバのサービスポート (ポート 80) に TCP 接続を開きます。ロードマスターは、ページ "/" に HTTP/1.0 HEAD リクエストを送付します。もし、サーバが HTTP レスポンスをステータス・コード 2xx (200-299)、301,302 もしくは 401 と共に返すと、ロードマスターは接続を閉じサーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さな

いか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。

- 7      **HTTPS**      ロードマスターは、**SSL** 接続をリアルサーバのサービスポート（ポート 443）に開きます。ロードマスターは、ページ “/” に **HTTP/1.0 HEAD** リクエストを送付します。もし、サーバが **HTTP** レスポンスをステータス・コード 2xx（200–299）、301,302 もしくは 401 と共に返すと、ロードマスターは接続を閉じサーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。
- 7      **POP3**      ロードマスターは、リアルサーバのサービスポート（ポート 110）に **TCP** 接続を開きます。もしサーバが、“+OK” で始まるグリーティング・メッセージを返すと、ロードマスターは **QUIT** コマンドをサーバに送り接続を閉じて、サーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。
- 7      **NNTP**      ロードマスターは、リアルサーバのサービスポート（ポート 119）上に **TCP** 接続を開きます。もしサーバが、ステータス・コード 200、201 と一緒にグリーティング・メッセージを返すと、ロードマスターは **QUIT** コマンドをサーバに送り接続を閉じて、サーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。
- 7      **IMAP**      ロードマスターは、リアルサーバのサービスポート（ポート 143）に **TCP** 接続を開きます。もしサーバが、“+OK” か “\*OK” で始まるグリーティング・メッセージを返すと、ロードマスターは **LOGOUT** コマンドをサーバに送り接続を閉じて、サーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。
- 7      **DNS**      ロードマスターは、リアルサーバのサービスポート（ポート 53/UDP）に **Source-of-Authority (SOA)** リクエストを送ります。サーバが **SOA** リクエストに対して成功裏にレスポンスを返すと、ロードマスターはサーバをアクティブとします。もし、サーバが設定してあるリトライ回数内でタイムアウト時間内にレスポンスを返さないか、もしくは違うステータス・コードを返すとサーバはダウンしているものとみなします。
- 7      **Remote Terminal Protocol**

ロードマスターは、リアルサーバにポート番号 3389 に対して TCP 接続を開き、RDP プロトコルによる “X.224 Connection Request” パケットを送信します。もし受信側から、“x.224 Connection Confirm” パケットが返信されてきたら、リモートクライアントからのリクエストに対して接続を許可できる Microsoft のターミナルサーバとして、サーバをアクティブとします。それ以外は、サーバに何らかの異常があると見なし、サーバをダウンとします。

- 0        None        ロードマスターは、リアルサーバに対してヘルスチェックを行いません。結果として常時サーバがアップとみなしてトラフィックを転送します。

バランサーのヘルスチェック最良設定については、セクション III のコマンドライン・インターフェース・リファレンスガイドを参照ください。

## 11 SNMP サポート

Simple Network Management Protocol (SNMP) は、リモート管理ステーション (SNMP マネージャ) よりネットワークを介して多くのネットワーク構成部品を管理するのを可能にするプロトコルです。

管理ステーション (SNMP マネージャ) は、被管理ステーション (SNMP エージェント) にデータをリクエストしたり、エージェントのデータを変更できます。

SNMP エージェントは、ユニットのフェイルオーバー等の予め定義してあるイベントに対して警告を出すようにセットアップ出来ます。警報メカニズムには、イベントトラップを用います。

SNMP スタンドアロンの説明については、リファレンス (セクション 12.3) を参照ください。現在のバージョンは SNMPv2c (community-based SNMPv2) です。他の主なバージョンは、SNMPv1 です。

ロードマスターの SNMP は SNMPv2c をベースにしていますが、上記の 2 つのバージョンを使用できます。しかしながら、SNMPv1 はロードマスターが使用している 64 ビット値をサポートしていないために、SNMPv2c の使用を推奨します。

**注：HA 構成をモニターする場合は、シェアード IP アドレスではなく必ず各ユニットに与えられた個別の IP アドレスを使用してください。**

### 11.1 SNMP 経由のロードマスター・パフォーマンス・マトリックス

全てのロードマスター特定データオブジェクトに関する情報は、下記の 3 つのエンタープライズ特定 MIBs (Management Information Base) に用意されています。

**ONE4NET-MIB.txt**                      エンタープライズ id

<b>IPVS-MIB.txt</b>	バーチャルサーバ状態
<b>B-100-MIB.txt</b>	ロードマスター設定情報

これらの MIBs（ロードマスターの CD 内にあります）は、SNMP によるパフォーマンス／設定情報をリクエストできるように、SNMP マネージャーにインストールされなければなりません。

カウンターの詳細は、ロードマスタ MIBs より取得出来ます（条項詳細）。

個々のフォームの MIB 情報の取得は、Linux（NAD UCD-SNMP）で下記のコマンドで行えます。

```
snmptranslate -Td -OS <oid>
```

<oid>は入手したい object identifier

**例:** <oid> = .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns

```
snmptranslate -Td -Ov .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns
```

```
.1.3.6.1.4.1.12196.12.2.1.12
RSConns          OBJECT-TYPE
-- FROM          IPVS-MIB
SYNTAX           Counter32
MAX-ACCESS       read-only
STATUS           current
DESCRIPTION      "the total number of connections for this RS"
 ::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) one4net(12196) ipvs(12) ipvsRSTable(2)
rsEntry(1) 12 }
```

ロードマスターの MIBs の中で定義されているデータオブジェクトは、WUI によって表示されるカウンターのスーパーセットです。

**注意：**ロードマスターのデータオブジェクトは、書き込み不可能ですので GET リクエスト（GET, GET-NEXT, GET-BULK,..）のみ使用されます。

ロードマスターの SNMP サポートの設定に関する説明は、インストール・ガイドを参照ください。SNMP サポートは、デフォルトでは無効となっています。

## 11.2 SNMPを介してのロードマスター・イベント・トラップ

ロードマスターは、SNMPv1 と SNMPv2 トラップの出力をサポートしています。

この機能を有効にすると、下記のようなトラップを出力します。

<b>ColdStart</b>	一般 (SNMP サブシステムの開始／停止)
<b>VsStateChange</b>	(バーチャルサービスの状態変更)
<b>RsStateChange</b>	(リアルサーバ状態変更)

**HaStateChange** (HA 構成システムのみ：ロードマスターフェイルオーバー)

トラップ機能の設定に関しては、インストールガイドを参照ください。  
トラップ出力は、デフォルトでは無効となっています。

**11.3 参考**

## SNMPv1:

RFC 1155 TCP/IP ベースのインターネット用管理情報の構造と確認

RFC 1157 SNMP

RFC 1212 簡明 MIB 定義

## SNMPv2c:

RFC 1901 コミュニティベース SNMP の紹介

RFC 1902 SNMP バージョン 2 (SNMPv 2) 用管理情報構造

RFC 1903 SNMP バージョン 2 (SNMPv 2) 用原文改造

RFC 1904 SNMP バージョン 2 (SNMPv 2) 用符号陳述

RFC 1905 SNMP バージョン 2 (SNMPv 2) 用プロトコル操作

RFC 1906 SNMP バージョン 2 (SNMPv 2) 用トランスポート・マッピング

RFC 1907 SNMP バージョン 2 (SNMPv 2) 用 MIB

## SNMPv3:

RFC 2570 インターネット-スタンダード・ネットワーク管理構成バージョン 3 の紹介

RFC 2571 SNMP 管理用枠組みを供述するための構造

RFC 2572 SNMP のためのメッセージ処理と出力

RFC 2573 SNMP アプリケーション

RFC 2574 SNMP バージョン 3 (SNMPv 3) のためのユーザベースのセキュリティモデル

RFC 2575 SNMP のためのビューベース・アクセス・コントロール・モデル

RFC 2576 インターネット-スタンダード・ネットワーク管理構成バージョン 1, 2, 3 の共存

## 12 ロードマスターのソフトウェア・アップグレード

### 12.1 オンラインによるアップグレード

ロードマスターは、ソフトウェアのアップデートとアップグレードを、オンラインで行う機能をサポートしています。パッチは、KEMPテクノロジーにより作成されます。これらのパッチは、一旦ローカルディスクへダウンロードした後に、WUIからインストール出来ます。又、コンソールを使って、FTP、HTTP、もしくはSSHデーモンをサポートしているマシンからインストールする事も可能です。どちらの場合も、一旦ロードマスタをリブートして、ダウンロードするメモリーのスペースを作ってから行うべきです。又、設定ファイルのバックアップをとってから行うことも重要です。

パッチは、チェックサム (MD5) と暗号化でデータ破壊と改ざんに対してプロテクトされています。

WUIの左側にあるメインメニューの“System Configuration”内の”System Administration”下の”Update Software”から行います。

コンソールを使用する時には、設定メニュー (utilities->software upgrade)を使って、サーバマシン (FTP、SCP、もしくはHTTPプロトコルを使用している) からパッチを一旦ダウンロードしてから行います。又、HTTPプロトコルを使用して、直接KEMPテクノロジーのサーバからロードマスターへダウンロードすることも出来ます。パッチがダウンロードされると、解凍と整合性チェックが行われます。

もし、パッチが正当ならばバージョンが表示され、ユーザはこのパッチをインストールするかどうかは問われます。パッチが問題なくインストールされたならば、ロードマスターは新しいバージョンをアクティブするためにリブートされなければなりません。

もし、何らかの理由でパッチが要求通りに動作しなかった場合には、設定メニューから以前のバージョンへのロールバックを行えます。

設定メニューの Utilities->Update License から、30-60日間しか有効でない評価用ライセンスからフルライセンスに切り替えてください。評価用ライセンスは評価期間が過ぎるとシステムが起動しなくなります。

ライセンスキーのアップデートは、WUIの“System Configuraiton” → “System Adminisration” → “Update License”より実施可能です。新しいキーにアップデートしてもロードマスターのリブートは必要ありません。

パッチを当てるためのファームウェアの更新は、ライセンスにより期限が限られています。基本的には、この更新の有効期間は1年です。無償保障期間が過ぎて保守契約を締結した場合には、新しいライセンスキーをインストールしなければなりません。もしこの有効期限が切れた場合は、下図のようなエラーがファームウェアの更新時に出力されますので、ライセンスの更新のために、システムを購入した販売店にお問合せください。

Updates not permitted - Please install new license

OK

## 13 Miscellaneous

### 13.1 リモート Syslogd サポート

ロードマスターは、syslog プロトコルを使い、色々な警告とエラーメッセージを出力できます。これらのメッセージは、普通ローカルメモリーに蓄積され、WUI の “System Configuration” メニューの “logging Options” 下の “log Files” からか、コンソールの診断メニューを介して表示することが出来ます。又、ロードマスターがこれらのエラーメッセージをリモート syslog サーバへ送信するように設定することも可能です。6つの異なるレベルのエラーメッセージが定義されています。各レベルのメッセージを、異なるサーバへと送れます。レベルは；

INFO  
NOTICE  
WARN  
ERROR  
CRITICAL  
EMERGENCY

注意：メッセージは、情報が送られるだけです。Emergency メッセージは、通常早急なアクションを必要とします。

**ヒント：**リモート Linux サーバでロードマスターの syslog メッセージを受けられるように syslog プロセスを有効にするためには、syslog を “-r” フラグを立てて起動しなければなりません。

### 13.2 ライセンスの入手方法

リブート後、ログイン用プロンプトが現れますので、'bal'（パスワード'1fourall'）でログインします。

ロードマスターのソフトウェアをアンロックするためには、ライセンスキーが必要です。ライセンスキーは、各単一ロードマスターインスタンスにハードウェア依存のアクセスコードを結合させて、個々に生成します。

ロードマスター用に入手できるライセンスは、下記の3種類です。

- a) 評価用ライセンス。これは最長 30 日間有効なフル機能用ライセンスです。
- b) 期限なし（フル）のスタンドアロン用ライセンス。

c) 期限なし（フル）の HA クラスター構成用ライセンス。HA-1 と HA-2 に分かれています。

評価用ライセンスは、フルのスタンドアローンか HA 用にアップグレードが出来ます。

### 13.2.1 30 日間評価用ライセンスの入手

1. 通常、評価を目的に送られてくるロードマスターには、既に評価用ライセンスのキーがプリントされたシートが添付されてきます。先ず、このシートの有無をチェックしてください。
2. ロードマスターに、VGA モニターと USB 用キーボードを接続します。又は、ターミナルエミュレーターのソフトウェア（Hyper Terminal 等）が使用できる PC にヌルモデムケーブルで COM+ポート同士（115200,8,N,1）を接続します。リブート後、'bal' (password '1fourall')でログインします。アクセスコードが画面に表示されて、ライセンスキーの入力を問われます。
1. 上記 1 項のライセンスキーを入力します。HA 構成の場合は、間違わないようにしてください。もし、キーがない場合は、KEMP テクノロジー社の代理店までアクセスコードを添えて評価用ライセンスキーの申請を行ってください。

### 13.2.2 フルライセンスの入手

1. もし、ロードマスターを既に購入された場合は、フルライセンス用キーが販売店のほうから送られて来ているはずです。もし入手されていないようでしたら、購入された販売店の方に問い合わせをしてください。
2. 入手後、もし初めてライセンスキーを入力する場合は、上記評価用ライセンスキーの入力に従います。
3. 評価用ライセンスが既にインストールされている場合は、次のセクションのライセンスのアップグレードに従ってください。

### 13.2.3 HA用フルライセンスの入手

1. ロードマスターを購入された場合は、製品の納品日から 40 日間以内にフルライセンス用キーが販売店から送られてきます。もし、40 日間過ぎてもフルライセンス用キーを受取っていない場合は、購入された販売店に問い合わせてください。
2. 入手後、もし初めてライセンスキーを入力する場合は、上記評価用ライセンスキーの入力に従います。HA-1 の方からライセンスキーを入力し、評価用環境に合わせた設定を行います。きちんと WUI が表示されることを確認ください。
3. HA-2 に、VGA モニターと USB 用キーボードを接続します。又は、ターミナルエミュレーターのソフトウェア（Hyper Terminal 等）が使用できる PC にヌルモデムケーブルで COM+ポート同士（115200,8,N,1）を接続します。リブート後、'bal' (password



メニューの”System Administration”下の”Backup/Restore”に行きます。そして、”Create Backup File”ボタンをクリックして特定の場所を指定してください。コンソールから行うときは、FTP か、SSH デーモンが走っているサーバへセーブします。’7’ Utilities から’2’ Transfer protocol へ行き、サーバに対応したプロトコルを選択します。その後、“q”を選んでメインメニューに戻り、’3’ Local Administration から’4’ Backup/Restore に行きます。’1’ Save Backup to Remote Host を選択し、プロンプトに従いサーバの情報を入力します。

設定をリストアする時、下記のどのポーションをリストアするか問われます。

VS Configuration only,

LM Configuration only,

All LM + VS Configuration Values.

“LM” 設定は、ロードマスターの IP アドレス等の全てのインターフェース情報や基本的な設定が含まれます。

“VS”設定は、バーチャルサービスとリアルサーバの全ての情報が含まれています。

注意： HA クラスターのスタンバイマシンに設定をリストアした場合は、LM 情報だけがリストアされます。バーチャルサービスの設定はアクティブ側から提供されます。

### 13.3.1 SSL証明書のバックアップ

WUI にアクセスし、“Certificate” → “Backup/Restore Certs.” に行きます。そして、“Certificate Back” のところの “Passphrase” に任意のパスワードを入力し、“Create Backup File” をクリックします。ダウンロード画面が現れたら、“Open” をクリックし、任意のディレクトリ下に任意の名前でセーブします。

## 13.4 システム・リカバリー

コンパクト・フラッシュメモリーのファイルが壊れた時などにはシステムのリカバリーが必要です。

- 設定のバックアップファイルと、もし SSL 証明書をバックアップしていたらそのファイルを用意します。
- ライセンスキーを用意します。
- 販売店に連絡し、リカバリーが出来るかどうかを確認します。  
もし、出来るようであれば；
- 基本的な設定を行います。（ライセンス入力、初期設定）

- ▶ 設定をバックアップファイルからリストアします。

## 13.5 L4とL7のバーチャルサービス間の相互可動性

パーシステンス方式を他の方式に変更した場合、全ての VS/RS の統計情報がリセットされます。バイト用統計値がテラバイトからゼロに変更された時、関連する値 (Byte/sec など) をグラフ表示をしていると最大値と最小値が大きくかけ離れていることから表示に影響が出ます。

## 13.6 Webユーザインターフェース(WUI)ルート証明書のインストール

ロードマスターは、デフォルトでは管理者がセキュアな HTTPS で WUI へアクセス出来るように、セルフサインの SSL 証明書を使用するように設計されています。しかしながら、殆どのブラウザは、そのような SSL 証明書の使用に対して警告を表示します。警告が表示されないようにするには、証明書のインストールを行う必要があります。そのためには、警告を無理して“サイトの閲覧を続行する”を選択して WUI に接続します。そして、“証明書のエラー”をクリックして、証明書の表示を行って“証明書のインストール”を選択します。問題なく証明書がインポート出来たならば、次回からはこの警告は表示されなくなります。

## 13.7 ログ情報

ログ情報は、WUI の “System Configuration” サブメニュー下の “Logging Options” オプションの “Log Files” から閲覧可能です。

### スタンドアローン構成

**Boot.msg File:** Linux の一般的なブート情報が含まれています。

**Warning Message File:** コアの負荷分散エンジンが出力したイベントを含んでいます。L4 の関連です。

**System Message File:** Linux の OS とコアな負荷分散エンジン (L7) が出力したイベントを含んでいます。

### HA 構成 (CARP 設定)

**Boot.msg File:** Linux の一般的なブート情報が含まれています。

**Warning Message File:** コアの負荷分散エンジンが出力したイベントを含んでいます。L7 の関連です。

**System Message File:** Linux の OS とコアな負荷分散エンジン (L4) 、及び HA エンジンが出力したイベントを含んでいます。

### HA 構成 (HB 設定)

**Boot.msg File:** Linux の一般的なブート情報が含まれています。

**Warning Message File:** コアの負荷分散エンジンが出力したイベントを含んでいます。L7 の関連です。

**System Message File:** Linux の OS とコアな負荷分散エンジン (L4) 、及び HA エンジンが出力したイベントを含んでいます。

**Heartbeat Message:** HA のハートビートエンジンの出力したイベントを含んでいます。

注：ログ情報は、限られたメモリー容量を使用しているため、上書きされてしまいます。又、システムがハングアップしてしまった場合は参照できません。Syslog サーバや SNMP マネージャーを使用して、イベント情報が残るようにすることを推奨します。

### 13.8 デバッグ機能

この機能は、WUI の “System Configuration” サブメニュー下の “Logging Optios” オプション内の “Debug Options” の下記を選択することで実施可能です。特定の問題を解決するために、KEMP 社の販売店サポート技術要員の指示により使用することをお勧めします。

#### **Disable All Transparency**

全てのバーチャルサービスのトランスペアレンシーを変更します。KEMP 社の販売店サポート要員の承諾を得た上でオンにしてください。

#### **Enable L7 Debug Traces**

“System Messages” 内に、追加的な L7 アクセスのデバッグ情報を出力します。

#### **Perform a l7 adm**

L7 のバーチャルサービスの詳細情報をテーブル形式で表示します。

#### **Perform a PS**

システムのプロセス状態をレポートします。

#### **Display Meminfo**

システムのメモリー使用状況を表示します。

#### **Display Slabinfo**

システム全体のスラブキャッシュを表示します。

#### **Ping Host**

ICMP をサポートしている IPv4 デバイスへの ICMP エコーリクエスト (PING) を発信します。

#### **TCP dump**

イーサネットポート上のパケットトレースを行い、その結果をファイルとしてダウンロード出来ます。フィルターとして、イーサネットポート、IP アドレス、ポート番号を指定出来ます。Start ボタンを押すことでトレースが開始され、Stop ボタンをクリックするまで継続され

ます。トレースの停止後に“Download” ボタンをクリックすることでローカルディスクへ保存するか、WireSharkなどで直接開いてパケットの解析を行うことができます。

## 14 ユーザ管理

ロードマスターは、異なるアクセスレベルのログインが可能な複数の管理ユーザをサポートしています。ユーザ管理は、WUIの“System Administration”サブメニューの“User Management”オプションから行います。追加する各ユーザ名は、3文字以上で10文字以下でなければなりません。パスワードは、半角文字で8文字から16文字までの範囲で指定できます。使用できる文字は英字（大文字、小文字）、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めて下さい。

### パスワード指定例

- ・ 英小文字のみ : 9文字以上 `abcdefghi`
- ・ 英小文字と数字の混在 : 8文字以上 `1abcdefg`
- ・ 英大文字と英小文の混在 : 8文字以上 `Abcdefgh`
- ・ 英小文字、記号、数字の混在 : 8文字以上 `ab!12345`
- ・ 数字のみ : 13文字以上 `0123456789012`

ユーザの追加は、WUIからしか許可されていませんので、SSH通信での設定ユーティリティでは行えません。

### 14.1 Roles/Permission

デフォルトのファクトリ設定では、管理者ユーザ名は“**bal**”でパスワードは“**1fourall**”です。このユーザは、最高レベルのアクセスが行える権利を有しています。追加出来るユーザには、この“**bal**”のサブセットとなるアクセス権利を与えることが可能です。各ユーザのロールの変更は、リアルタイムで有効となります。ロールは、複数を結合指定で互いのロールは干渉しません。

新しく作成するユーザのデフォルトのアクセス権限は、WUIへの“**read**”のみ、SSL証明書用CSR作成、ログファイルの読む込み、及び基本的なデバッグ機能の実行だけです。

#### 14.1.1 Real Servers

このロールは、リアルサーバの“**Enable**”と“**Dosable**”を行う権限を持ちます。

#### 14.1.2 Virtual Services

このロールは、バーチャルサービスの管理権限を持ちます。バーチャルサービスの変更、追加、削除、及びサブネットの変更が可能です。

#### 14.1.3 Rules

このロールは、ルール管理権限を持ちます。ルールの変更、追加、削除が可能です。

#### 14.1.4 System Backup

このロールは、設定ファイルのバックアップ権限を持ちます。設定ファイルのバックアップファイルの作成、及びリストアが可能です。

#### 14.1.5 Certificate Creation

このロールは、SSL 証明書の管理権限を持ちます。SSL 証明書のインストール、削除が可能です。

#### 14.1.6 Intermediate Certificates

このロールは、第三者 SSL 証明書（インターミディエート）の管理権限を持ちます。第 3 者 SSL 証明書のインストール、削除が可能です。

#### 14.1.7 Certificate Backup

このロールは、SSL 証明書のバックアップ作成権限を持ちます。証明書のバックアップ（エクスポート）、リストア（インポート）が可能です。

#### 14.1.7 All Permissions

このロールは、すべての権限を持ちます。このロールを持ったユーザはデフォルトユーザの 'bal' と同じ権限が与えられます。

#### 14.1.8 Allowed Network

このロールは、設定されたサブネットのうち、どのサブネットを管理出来るようにするかを選択するものです。選択されたサブネットだけに属するバーチャルサービスとそのリアルサーバの参照が可能になります。変更、追加を行うためには、他のロールと併せた許可が必要です。

## 15 ボンディングと VLAN

### 15.1 概要

ロードマスターのボンディング/VLAN タギングは、この機能を使用するために必要とされる規格に合っているならば WUI より簡単に設定が行えます。このガイドは、ロードマスター上のインターフェースのボンディングと VLAN 設定を行うためにデザインされたものです。ボンディングのサポートは、全てのネットワークモジュールで利用可能です。

### 15.2 必要とする規格 (スイッチ側)

1. VLAN タギング
  - a. IEEE 802.1Q
2. ボンディング (Bonding) /チーミング (Teaming)
  - a. IEEE 802.1AX/IEEE 802.3ad/LACP

#### 15.2.1 スイッチ側の設定

ボンディング機能の内、Active/Backup モードでの設定には、スイッチ側でのボンディング/チーミングの設定は必要ありません。単に、一般のポートをロードマスターに接続するだけで OK です。しかし、802.3ad ボンディングモードを使用するには、スイッチ側のポートが 802.1AX (802.3ad) に準拠していて、尚且つそれらのポートをボンディング/チーミングに設定する必要があります。スイッチがこの仕様に準拠しているかどうかは、スイッチ側の仕様を確認してください。各ベンダーでこの機能名が違うかもしれませんので、“リンク・アグリゲーション (link aggregation)”、“イーサネットトランク (Ethernet trunk)”、“NIC チーミング (NIC teaming)”、“ポートチャンネル (port channel)”、“ポートチーミング (port teaming)”、“ポートトランキング (port Trunking)”、“リンクバンドリング (link bundling)”、“イーサネットチャンネル (EtherChanne)”、“マルチリンクトランキング (Multi-Link Trunking 「MLT」)”、“NIC ボンディング (NIC bonding)”、“ネットワーク・フォルトトーレランス (Network Fault Tolerance 「NFT」)”、“LAG”などでチェックしてみてください。

スイッチ側の VLAN トランキング機能を可能にする時は、スイッチの各ポートが一般、アクセス、トランキングの各専用モードをサポートしているか確認ください。一般モードは、ポートを VLAN に属させ、タグあり、タグなしの設定が可能 (802.1Q フルモード) で、アクセスモードは、シングルタグなし VLAN に属させます。トランクモードは、ポートを全てのポートがタグありの VLAN に属させます。

## 15.3 ボンディング／チーミング (802.3ad/Active-Backup)

ボンディング機能を設定するためのキーポイントを下記します。

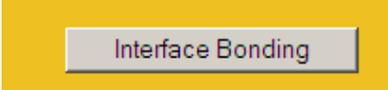
1. ボンディングをするポートは、親ポートより高い番号のポートでなければなりません。例えば、ボンディングをポート# 10より始める場合、追加するポートは# 11、もしくはそれより高い番号のポートでなければなりません。
2. ボンディングと VLAN タギングを併用する場合は、ボンディングを設定し終えてから VLAN タギングを設定しなければなりません。
3. ポート# 1 は、ボンディング用ポートとしては使用出来ません。
4. もし IP アドレスが設定されているポートをボンディングに追加する場合は、全ての IP アドレスを削除してから行う必要があります。
5. ボンディング機能の中で “Active/Backup” の設定については、スイッチ側には 802.3ad 関連のいずれの仕様も必要ありません。

ヒント:

1. ボンディングに使用するポートは、スイッチ側、ロードマスター側両方で全て同じスピード、Duplex モードである必要があります。
2. ポート# 0 をボンディングとして設定した場合、WUI 接続が切れてしまいます。再接続をするためには、システムを一旦リブートする必要があります。もし、他のポートにアクセス可能ならば、WUI よりリブートを可能にするためにそのポートに WUI を仮に移すことを推奨します。

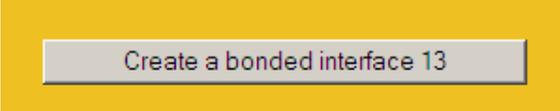
### 15.3.1 ボンディング／チーミング設定方法

1. WUI にアクセスし、メニューから ▶ **System Configuration** ▶ **Interfaces** | に行き、ボンディングを開始するポートに相当する ▶ **ethX** を選択し、下記の “Interface Bonding” ボタンをクリックします。



Interface Bonding

2. ポートをボンディング用ポートにするための確認ボタンをクリックします。



Create a bonded interface 13

3. ポートがボンディング用ポートとなった結果が表示されますので、“Continue” ボタンをクリックします。



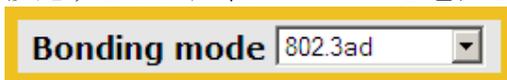
Converted Interface to be used as bonded device

Continue

- メニューから ▶ **System Configuration** ▶ **Interfaces** へ行き、作成されたボンディングポート ▶ **bndX** を選択します。表示された “Network Interface X” 画面の中の “Bonded Device” ボタンをクリックします。



- 設定するボンディングモードを選択します。



- このボンディングに追加するポートを選択します。



- ポートがボンディングされた旨が表示されますので、“Continuos” をクリックします。



- メニューから ▶ **System Configuration** ▶ **Interfaces** へ行き、作成されたボンディングポート ▶ **bndX** を選択します。表示された “Network Interface X” 画面に必要な IP アドレス情報を設定します。

### 15.3.2 ボンディング／チーミングの解除

ボンディングポートに VLAN が設定されている場合は、先ずこれらの設定を削除します。これらを削除しないとボンディングを解除したポートの最初の親ポートにこれらの設定が残ります。

- WUI にアクセスし、メニューから ▶ **System Configuration** ▶ **Interfaces** に行き、解除するボンディングポートに相当する ▶ **bndX** を選択します。表示された “Network Interface ethX” 画面の中の “Bonded Devices” ボタンをクリックします。



- 表示された “Bonded Device Management” 画面からボンディングを解除するグループから子ポートの “Unbind Port” ボタンをクリックします。



- 子ポートのボンディングを全て解除し終わると、下図のように親ポートだけが残りますので、“Unbond this interface” ボタンをクリックします。



## 15.4 VLAN タギング

VLAN を設定するに当たり、下記を考慮しておいてください。

1. VLAN タギングを設定する場合は、スイッチ側の設定を先に済ませておいてください。
2. ボンディング/チーミングを VLAN タギングと併用する場合は、ロードマスター側ではまずボンディングの設定を行った上で VLAN タギングの設定を行ってください。

ヒント:

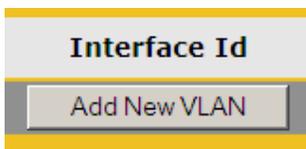
1. VLAN タグは、一般の物理ポート、もしくはボンディングポートの両方で設定可能です。

### 15.4.1 VLANタギングの設定方法

1. WUI へアクセスし、メニューから ▶ **System Configuration** ▶ **Interfaces** を選択し、VLAN タグを設定するポートに該当する ▶ **ethX** もしくは **bndX** をクリックします。表示された “Network Interface” 画面上の “VLAN Configuration” ボタンをクリックします。



2. 表示された “VLAN Management” 画面上の “Add New VLAN” ボタンをクリックします。



3. 追加する VLAN タグにより上記の操作を繰り返します。設定後は、メニューから ▶ **System Configuration** ▶ **Interfaces** に行き、▶ **Virtual LAN** の矢印をクリックし VLAN タグが追加されているのを確認します。

### 15.4.2 VLANタグの削除

1. 特定の VLAN タグを削除するには、メニューから ▶ **System Configuration** ▶ **Interfaces** ▶ を選択し、**Virtual LAN** の矢印をクリックし削除する VLAN タグを選択します。
2. 表示された “Network Interface X” 画面上の該当 VLAN の IP アドレスを削除します。IP アドレスが完全に削除されると、下図の “Delete this VLAN” ボタンが現れますのでク

リックします。その後、削除された旨の通知画面が現れますので“Continue” ボタンをクリックします。



- 追加の VLAN タグの削除が必要ならば、上記を繰り返します。削除の確認は、メニューから ▶ **System Configuration** ▶ **Interfaces** に行き、▶  の矢印をクリックして行ってください。

## 16 付録 I

### 16.1 エージェントベースのアダプティブ負荷分散用API

アダプティブ方式の負荷分散のために、ロードマスターはファーム内の対応するリアルサーバのシステム負荷を定期的にチェックしています。各リアルサーバは、自サーバの実際の負荷を 0 から 102 で表わす数字のファイル（0=空、99=過負荷、101=サーバダウン、102=管理的に不可用）を用意する必要があります。ロードマスターは、このファイルを HTTP GET 操作で取得します。このファイル（ASCII 形式）を用意するのは、各サーバの役割です。どのようにサーバが自分の負荷を評価するかは自由です。但し、幾つか守らなければならない下記の制約があります。

- ▶ 最初の行に 0 から 102 までの数字を示す ASCII ファイルがなければなりません。
- ▶ ファイルは、ロードマスターより HTTP GET でアクセス出来なければなりません。
- ▶ 全てのサーバで、同じ URL でなければなりません。
- ▶ このファイルのロケーションを指定するパラメーター “Adaptive URL” (“Rules & Checking”メニューの”Check Parameter”画面内)に入力した場所にファイルはなければなりません。

下記は、LINUX サーバで負荷情報を決定し、表示させるためのスクリプト例です。

```
get load() {
    awk '/^cpu0/ {printf "%d %d %d %d\n", $2, $3, $4, $5}' \
        /proc/stat > /tmp/cpload
    read USR SYS IOWAIT IDLE < /tmp/cpload
    # echo $USR $SYS $IOWAIT $IDLE
}

INTV=5
DOCUMENTROOT=/usr/local/httpd/htdocs/
LOADFILE="$DOCUMENTROOT/load"

main() {
    while true; do
        USR1=$USR
        SYS1=$SYS
        IOWAIT1=$IOWAIT
        IDLE1=$IDLE
        get load
        SUM=$(( $USR+$SYS+$IOWAIT+$IDLE ))
        PUSR=$(( (USR-USR1)/$INTV ))
        PSYS=$(( (SYS-SYS1)/$INTV ))
        PIOWAIT=$(( (IOWAIT-IOWAIT1)/$INTV ))
        PIDLE=$(( (IDLE-IDLE1)/$INTV ))
        echo "$(( 100-PIDLE ))" > $LOADFILE
        sleep $INTV
    done
}
get load
main
```

下記は、MS Windows 2000, 2003 サーバで負荷情報を決定し、表示させるための C プログラムの例です。

```

#include <windows.h>
#include <stdio.h>
#include <conio.h>
#
#define CPU 0      0      /*processor 0*/
#define INTERVAL MS 3000 /*three seconds as interval*

/*counter path for Windows NT 4.0 and 2000*/
#define COUNTER_PATH NT TEXT("\\\\\\%s\\Prozessor{%d}\\%s Prozessorzeit
(
v
HQUERY      hQuery
F
Yo
{
TCHAR      c name[MAX COMPUTERTNAME LEN
TCHAR      counter path
DWORD      ctrType;
DWORD      size=MAX COMP
HCOUNTER    hCounter;
PDH STATUS  pdhStatus;

if(!GetCo
{
fprintf(stderr
.
exi

pdhStatus = PdhOpenQuery(0,0
if(pdhStatus!=NO

if((GetVersion() & 0xFF) >= 5)
sprint
else
sd

pdhStatus=PdhAddCounter(hQue
if(pdhStatus!=NO
exit{

while(
{
fp=fopen(COU
if(!fp
{
fprintf(stderr,"ERROR: Couldn't open counter file!\n");
.
exi
}

pdhStatus=PdhCollectQueryDat
if(pdhStatus!=NO
exit(1);
pdhStatus =
PdhGetFormattedCounterValue(hCounter,PDH_FMT_DOUBLE,&ctrType,&fmt
fprintf(fp,TEXT{
fclose(fp);
.
Sle
}
Yo
{
if(hQuery!=INVALID_HANDLE_VALUE
.

```

このコードは、Windows 2000 から CPU 負荷を得るためのプログラム例です。これは、Performance Data Helper (PDH) API を使い、pdh.lib にリンクしていなければなりません。

PDH Dynamic Link Library (DLL) pdh.dll をシステムにインストールしなければなりません。又、Windows 2000 のカウンターパスをインストールされている言語に合わせて変更してください。

KEMP テクノロジーでは、Windows2000, 2003, 2008 サーバ用に作成したエージェントを用意しています。このエージェントの使用を検討されている場合は、ロードマスター販売店までお問い合わせください。

## 16.2 HTTPサーバでのサーバクッキーサポート

この短いサンプルでは、リアルサーバでどのようにクッキーをセットするかを示します。

```
#!/usr/bin/perl
#####
$VERSION="set-cookie.pl v1.0; #Jun 18 2002 Brain Force GmbH
#-----
#
# Simple set cookie demo.
#-----
#- User configurable variables -----#
#set cookie name
$name = "cookie-name";
#set cookie value
$value = "demo-cookie";
#set expiry date for the cookie
$expDate = "09-Nov-2002 00:00:00 GMT";
#set this to your domain prepended with a .
$domain = ".qmr.de";
#set path for the cookie
$path = "/";
#set to one if you want the cookie to be sent over a secure connection(ssl)
$secure = "0";
#-----#

#main command to set cookie on a client side
&setCookie($name, $value, $expDate, $path, $domain);

# be sure to print a MIME type AFTER cookie headers and follow with a blank line
print "Content-type: text/html\n\n";

%cookies = &getCookies; # store cookies in %cookies
#-----#

#- Set Cookie -----#
sub setCookie {
    # end a set-cookie header with the word secure and the cookie will only
    # be sent through secure connections
    local($name, $value, $expiration, $path, $domain, $secure) = @_;

    print "Set-Cookie: ";
    print ($name, "=", $value, "; expires=", $expiration,
           "; path=", $path, "; domain=", $domain, "; ", $secure, "\n");
}
#-----#

#- Retrieve Cookies From ENV -----#
sub getCookies {
    # cookies are separated by a semicolon and a space, this will split
    # them and return a hash of cookies
    local(@rawCookies) = split (/; /, $ENV{'HTTP_COOKIE'});
    local(%cookies);

    foreach(@rawCookies){
        ($key, $val) = split (/=/, $);
        $cookies{$key} = $val;
    }

    return %cookies;
}
#-----#
```

## 16.3 MIBツリー

SNMP マネージャー用 MIBs (ONE4NET-MIB, B100-MIB, IPV6-MIB) ファイルは、装置に添付されている CD に含まれています。SNMP にて MIB 情報による各種統計情報を取得するには、これら 3 ファイルを使用しなければなりません。

## II. インストール&設定ガイド

### A. 開始前に

ロードマスターを始めてセットアップするには、ターミナルエミュレータソフトが起動しているパソコンとロードマスターの COM ポートを接続する必要があります。又は、VGA モニターUSB キーボードを直接ロードマスターに接続します。

パソコンとロードマスターを接続するケーブルはヌル・モデムケーブルを使い、COM ポートの設定は 115,200、8、N,1 とします。

ブートが正しく行われるとログイン画面が現れますので、ログインユーザ名'bal'、パスワード'1fourall'でログインします。ログインが正しいとアクセスコードが表示され、ライセンス用キーの入力を問われます。

### 1 ロードマスター装置

#### 1.1 送付品

- ▶ 送付される各ロードマスターには下記構成が含まれています。
  - A/C 電源用ケーブル
  - ロードマスターのソフトウェアと、マニュアル 1 式 (PDF 形式) が含まれた一枚の CD
  - 19 インチ用ラック搭載用キット
  - COM ポート用ヌル・モデムケーブル

#### 1.2 ロードマスター2200 ハードウェア



LM-2200 ハードウェア :

Intel Pentium M プロセッサ  
 1 GB RAM メモリー  
 ブータブル DOM (ハードディスクなし)

ポート :

4 x GbE LAN ポート  
 1 x COM+ コンソール用シリアルポート

1 VGA ポート (裏面)

2 x USB ポート

**寸法:**

426(W) x 419(D) x 44(H) mm

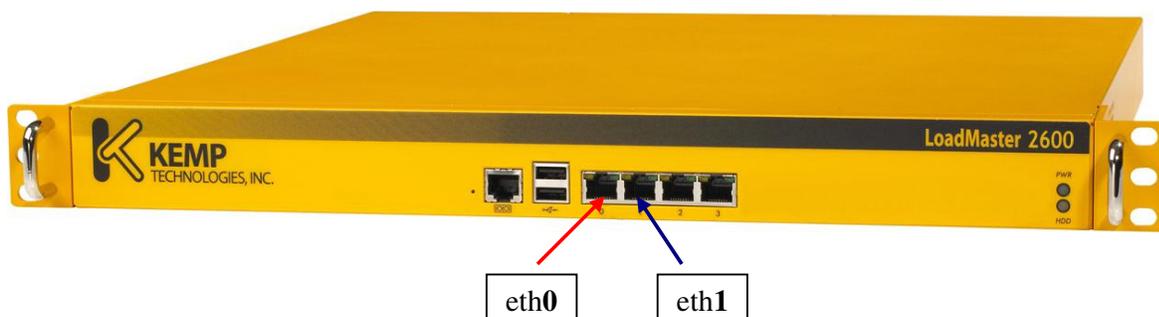
**電源:**

180W ATX 電源ユニット AC/DC 90 ~ 264V フルレンジ@ 47 ~ 63 H

**重量:** ~6 Kg

CE/FCC 認定、UL 登録、RoHS 準拠

### 1.3 ロードマスター2600 ハードウェア



**LM-2600 ハードウェア:**

**Intel Dual Core Processor**

**2 GB RAM メモリー**

**ブータブル DOM (ハードディスクなし)**

**ポート:**

4 x GbE LAN ポート

1 x COM+ コンソール用シリアルポート

1 VGA ポート (裏面)

2 x USB ポート

**寸法:**

426 (W) X 365 (D) X 44 (H) mm

**電源:**

200W ATX Power supply, AC/DC 90-264V フルレンジ@47~63 Hz

**重量:** ~7 kg

CE/FCC 承認、UL 登録、RoHS 準拠

## 1.4 ロードマスター3600 ハードウェア



**LM-3600 ハードウェア :**

**Intel Quad Core プロセッサ**  
**4GB RAM メモリ**  
**ブータブル DOM (ハードディスクなし)**

**ポート :**

8 x GbE LAN ポート  
1 x COM+ コンソール用シリアルポート  
1 VGA ポート  
2 x USB ポート

**寸法 :**

426(W) X 365 (D) X 44 (H) mm

**電源 :**

200W ATX Power supply, AC/DC 90-264V フルレンジ@47~63 Hz

**重量 :** ~7.0 kg

CE/FCC 承認、 UL 登録、 RoHS 準拠

## 1.5 ロードマスター5500 ハードウェア



### LM-5500 ハードウェア :

注：標準のハードウェア設定では、18 の GbE ポートと SSL 通信用 ASIC カードが搭載されます。24 の GbE ポートの実装も可能ですが、その場合は SSL 通信用 ASIC カードが搭載出来ませんので、SSL 通信のパフォーマンスが劣化します。詳細は販売店までお問い合わせください。

2 x Intel Quad-Core Xeon プロセッサ  
 4GB RAM メモリー  
 ブータブル DOM (ハードディスクなし)

#### ポート :

18 x GbE LAN ポート (SSL 用 ASIC ボード搭載) 、 24 x GbE LAN ポート (SSL 用 ASIC ボード非搭載)、 **最大 8 x SFP ファイバーポート**  
 1 x COM+ コンソール用シリアルポート  
 1 VGA ポート (裏面)  
 2 x USB ポート

#### 寸法 :

427(W) X 600 (D) X 88 (H) mm

#### 電源 :

460W ATX Redundant Power supply, AC/DC 90-264V フルレンジ@47-63 Hz

#### 重量 :

~25 kg  
 CE/FCC 承認、 UL 登録、 RoHS 準拠

## 2 ハードウェアの接続

### 2.1 eth0の接続

カテゴリ5以上のイーサケーブルの一方の終端を、“eth0”とマップされている LAN ポートに接続し、他方終端をデフォルトゲートウェイが収容されているハブ/スイッチに接続します。

### 2.2 eth1 の接続

カテゴリ5以上のイーサケーブルの一方の終端を、“eth1”とマップされている LAN ポートに接続し、他方終端をサーバファームにインターフェースしているハブ/スイッチに接続します。

HA構成で、1アームのネットワーク形体の場合は、必ずHA-1とHA-2の両方のこのポートをお互いにストレート、もしくはクロスオーバーケーブルで接続してください。これは、設定情報の同期と相手の状態を監視するために必要です。又、以下に案内しているQuick Setupでイーサポート設定とパスワード変更が終了し、システムをリブートした後、ブラウザからウェブ・ユーザ・インターフェース (WUI) に接続が可能になります。WUIの“System Configuration”サブメニュー下の“Interfaces”の“1”を開き、“Use for HA checks”にチェックマークがあることを確認してください。もしチェックマークがない場合は、チェックする必要があります。この場合、イーサポート1の設定は一切不要です。

2アーム構成では、ネットワークを介してHA同士が同期を取りますので、同じくイーサポート1、もしくは他のポートの“Use for HA checks”にチェックマークがあるのを確認してください。

**注：** システムのデフォルトゲートウェイは、デフォルトではeth0サブネット上のデバイスだけが設定可能ですので、eth0はネットワーク側になるようにしてください。他のポートはユニバーサルですので、ネットワークでもサーバファームのどちらでも構いません。もし、デフォルトゲートウェイをEth0以外のサブネットに存在するデバイスに変更したい場合は、System Configuration-> Miscellaneous Options-> Network Options 内の Enable Alternate GW support を‘Yes’にしてリブートをする必要があります。その後、デフォルトゲートウェイを設定する“Interface”の“Use for Default Gateway”をオンにしてください。

## B. シングル構成の初期設定 (non-HA)

### 1 ログインとライセンスキー入力

コンソールが使用できるように、VGA モニターと USB キーボードをユニットへ接続します。シリアルポートも使用可能です。シリアルポートよりコンソールを立ち上げる場合は、ヌル・モデムケーブルを使い、ターミナル・エミュレータ・ソフトが使えるパソコンの COM ポートとロードマスターの前面にある COM ポートを接続します。(COM ポートの設定は 115,200、8、N,1 とします)。

電源を投入すると、ブートプロセスが実行されログイン画面が表示されます。最初のログインは、ユーザ名” bal”、パスワード” 1fourall”と入力します。ログインに成功すると、ライセンスキーを要求する下記のメッセージが表示されます：

"Thank you for purchasing LoadMaster. Please contact your KEMP representative to receive a License Key and unlock your LoadMaster".

ライセンスキーは、ロードマスターの梱包内に一枚の紙で案内してあります。もし、見つからないようでしたら購入した販売店まで問い合わせてください。

**注意：**キーボードは、US/ASCII 用マッピングになっています。ライセンスキーを入力する時、もし数字用キーパッド部分を使用する場合は、マイナス（-）文字は、、 “NumLock” キーをオンにする必要があります。

クイック・セットアップ中に、キーボード用マッピングを、実際使用している正しいものに変更する設定があります。

**ヒント：**販売店にライセンスキーを問い合わせる前に、評価目的か、又は既に購入済（支払い済み）かをチェックした上で、アクセスコードを用意してください。評価目的、もしくは支払いがなされていない場合は、45 日間有効の仮ライセンスの発行となります。

ライセンスキーは、ロードマスターの各ハードウェアに対して固有ですので、他のハードウェアでの流用は出来ません。

有効なライセンスキーが入力されると、クイック・セットアップがスタートします。クイック・セットアップの詳細については、“Quick Setup”のセクションを参照ください。

## C. ハイアビリティ構成での初期設定 (HA)

### 1 HA-1 のログインとライセンスキー入力

冗長構成の為に2台購入された場合は、HA-1 と HA-2 というユニットの組み合わせとなります。ライセンスキーを案内している紙に、対応するユニットのシリアル番号が明記されていますので、どちらが HA-1 用ユニットか確認します。

HA-1 が確認できたら、上記のシングル構成用ユニットと同じ要領にて電源を投入し、ライセンスキーを投入します。

有効なライセンスキーが入力されると、クイック・セットアップがスタートします。クイック・セットアップの詳細については、“Quick Setup”のセクションを参照ください。

### 2 HA-2 へのログインとライセンスキー入力

HA-2 への電源投入、ログインは、HA-1 のクイック・セットアップが正常に終了し終えた後に行います。事前に、HA-1 への PING や WUI への接続が問題なく行えることを確認してください。

HA-2の電源を投入し、ログインします。アクセスコードが表示され、ライセンスキーの入力を促されますので、HA-2用のものを入力します。

ライセンスキーが正しいと、クイックセットアップが開始され、イーサポート0 “eth0” 用 IP アドレスの入力を促されます。そして、HA-1 の “eth0” の IP アドレスの入力を促されます。

もし、入力した IP アドレスとネットワーク接続が正常であれば、他の設定は HA-1 より転送されてきて、下記のメッセージが表示されます：

“Most of the configuration parameters have been received from the partner LoadMaster.  
Only the local network interfaces must now be configured.”。

“eth0”以外のローカル IP アドレスを入力してください。シェアード IP アドレスが案内のために表示されます。

各ローカルアドレスの入力が終わると、設定が有効になります。これで HA 構成での稼動が可能です。

もし、設定情報を HA-1 より受信できない場合は、HA-1 と行った同じ各パラメータへの入力が必要です。出来るならば、転送が成功するように HA-1 と HA-2 のネットワークへの接続と IP アドレスの設定が正しいか確認してください。

HA-2 に手動で設定を行った場合は、ネットワークが正常で IP アドレスに問題がなければ、リブートすることにより HA-1 の設定が上書きされます。

**ヒント：**両方の IP アドレスとシェアード IP アドレスを、PING により確認してください。

## D. クイック・セットアップ (Quick Setup)

ロードマスターへ初めてログインし、ライセンスキーを入力し終わると、クイック・セットアップが始まります。

クイック・セットアップは、コンソールのメインメニューからもアクセス可能です。

クイック・セットアップは、ロードマスターが WUI (ウェブ・ユーザ・インターフェース) や、SSH 接続でバーチャルサービスの設定を開始出来るようにするための、基本的なパラメータを簡単に設定するのを可能にします。一度設定したパラメータは、メニュー画面より変更が可能です。

クイック・セットアップは、下記の “ようこそ” メッセージを表示します：

"This menu will allow you to quickly set up the balancer. The first step is to set up the network interfaces, then the hostname(s) of your LoadMaster(s) and finally the default gateway and DNS parameters."

クイック・セットアップ手順は、下記のパラメータの設定を可能とします。

- イーサポート0 –IP アドレス
- イーサポート1 –IP アドレス

- ▶ ホスト名- ローカル用 (HA 構成であればパートナー側の分も含めて)
- ▶ DNS 用パラメータ
- ▶ ドメイン用パラメータ
- ▶ デフォルト・ゲートウェイ

これらのパラメータがセットされれば、設定は有効となります。そして、ロードマスターは稼働準備が整ったこととなります。

注意：もしパラメータの入力が正しくなかった場合は、メインメニューに表れている [CANCEL] ボタンを使用してください。クイック・セットアップが再度開始されますので、間違いを訂正出来ます。

### イーサポート 0 – IP アドレス “Ethernet IP address(s) – eth0”

ユーザは、イーサネット 0 (ネットワーク側) の IP アドレスの入力を問われます。ドット (.) で区切られた 4 組の数字を、下記のようにネットワーク・スペシフィヤ (/ 2 4) と共に入力します。

<例> : 192.168.200.12/24

もし、ネットワーク・スペシフィヤが入力に含まれていない場合は、ネットマスクの入力を問われます。ネットワークスペファイヤの / 2 4 かドットで区切られた 4 組の数字 (例えば 255.255.255.0) を入力してください。

次に、このインターフェース用 VLAN タグ ID を入力できます。もし、VLAN が使用されていなければブランクのままとします。VLAN タグ ID は、1 から 4095 までの間の値が使用できます。

**注：**VLAN タグに “1” を使用することは、他のネットワーク構成品との間で問題を引き起こし得るので推奨しかねます。

HA 構成を行う時は、シェアード IP アドレスが必要になります。これは、“eth0” にアサインした IP アドレスと同じネットワークにあるアドレスでなければなりません。

### イーサポート 1 – IP アドレス “Ethernet IP address(s) – eth1”

ユーザは、今度はファーム側イーサネットである “eth1” の IP アドレス入力を問われます。1 アーム構成の場合は、この入力はブランクのままとしてください。

入力フォーマットは、“eth0” と同じです。ここでアサインするアドレスは、“eth0” と異なるネットワークでなければなりません。

### ホスト名 “Hostname(s)”

ロードマスターのホスト名をここでセットします。標準な名前が推奨されます。このホスト名は、もし、これが HA 構成の 1 ユニットではなく、もしくは同じネットワーク・ブロードキ

キャスト内に別のロードマスター・クラスター (HA ペア) が存在しなければ、デフォルトからの変更は必要ありません。

### DNS 設定 “Name Server IP Addresses ”

DNS リゾルバーを設定します。3 つまでの DNS サーバの指定が可能です (アドレスは、ドットで仕切られた 4 組の数字のシンタックスでなければなりません)。

### ドメインの設定 “Domain List”

サーチするドメインのリストを入力します。6 つまでのドメインが指定可能です。

### デフォルト・ゲートウェイ “Default Gateway”

ネットワーク側のデフォルト・ゲートウェイを設定します。

## E. メインメニュー

ロードマスターが持つ多くの機能を、メニューシステムを使って設定できます。メニューシステムは、コンソールを使うか、もしくはリモートから SSH 接続を用いて ‘bal’ ユーザ名でログインすることにより利用できます。

**重要:** リモートアクセスは、SSH 接続が許可されていて (デフォルト) ‘bal’ ユーザのパスワードがデフォルトから変更されている時だけ可能です。もし、パスワードがデフォルト値より変更されていない場合は、直接接続のコンソールよりのみ可能です。

**注意:** もし、‘bal’ のパスワードを忘れた場合は、コンソールより ‘pwreset’ 名でログインします。パスワードは、‘1pwreset’ です。これは、‘bal’ の既存パスワードをリブートされるまで ‘1fourall’ にリセットします。もし、ユニットがリブートされたならば、パスワードは忘れてしまった古いものに戻ってしまいます。リブートをするまでに、設定メニューからパスワードの変更を行うべきです。

## 1 設定メニューの基本

設定用メニューシステムは、機能別の幾つかの階層メニューへ分割されています。メニューをナビゲートするには Up と Down カーソルキーか、‘+’ と ‘-’ キーを用います。メニュー上で番号で案内にしているエントリは、番号入力で選択できます。

**<例>**：キーボードのマッピングを変更しようとする場合、ユーザは“Local Administration”上で、3 <CR>とタイプすることで、メニューの“3. Set keyboard map”を選択することが出来ます。

‘q’ <CR> or ‘ESCAPE’、もしくは[CANCEL] ボタンを使って、1階層前のメニューに戻ります。

**ヒント**：[OK]か [CANCEL] ボタンにアクセスするためには、TAB キーを使うことでメニューからボタンへ切り替えられます。

メインメニューから[CANCEL] ボタンを使うと、変更した設定は無効となります。

メインメニューから[OK] ボタンを押すと、ハイライトされているメニューに切り替わります。

**重要**：ロードマスターが HA クラスタとして構成されている時、そしてスタンバイマシンへログインしている場合は、ローカル・ユーザ・インターフェース、ローカルパスワードの変更、及びバックアップ/リストアだけしか実行できません。その他の設定は、アクティブマシンでしか変更が出来ません。メインメニューから、下記のオプションが可能です。

### 1.1 Quick Setup “クイックセットアップ”

これは、ユーザがロードマスターのイーサネット IP アドレス、ローカルゲートウェイ、ネームサーバなどの基本設定パラメータを素早く設定出来るようにします。

初期設定の“クイック・セットアップ”セクションを参照ください。

## 2 Service Management (CLI) “サービス・マネージメント”

このメニューは、ユーザがロードマスターで利用できるバーチャルサービスを管理するための CLI (コマンドライン・インターフェース) を始められます。各コマンド用シンタックスは、セクション III を参照ください。

CLI より抜ける場合は、“exit”とタイプします。もしくは、エスケープか CTRL-D キーを使用します。

このバージョンのロードマスターは、以前の Utilities -> Diagnostics 下の“Use MML format CLI”メニューからの選択に替わるものです。

### 3 Local Administration “ローカル・アドミニストレーション”

このメニューは、現在のロードマスターの管理用タスクを実行します。下記のオプションが利用可能です。

#### 3.1 Set Password “パスワードのセット”

このオプションを使い、ユーザ”bal”のパスワードを変更します。パスワードは、セキュリティのため変更すべきです。SSH 接続を介してのリモートからのアクセスは、このパスワードを変更しない限り許可されません。パスワードは、半角文字で 8 文字から 16 文字までの範囲で指定できます。使用できる文字は英字（大文字、小文字）、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めて下さい。

##### パスワード指定例

- |                |           |               |
|----------------|-----------|---------------|
| ・英小文字のみ        | : 9 文字以上  | ancdefghi     |
| ・英小文字と数字の混在    | : 8 文字以上  | 1abcdefg      |
| ・英大文字と英小文の混在   | : 8 文字以上  | Abcdefgh      |
| ・英小文字、記号、数字の混在 | : 8 文字以上  | ab!12345      |
| ・数字のみ          | : 13 文字以上 | 0123456789012 |

**重要：**パスワードは、バックアップではセーブされません。よって、リストア時もリプレイスされることはありません。

もし、ロードマスターが HA モードで稼働している場合、各ロードマスターは別々のパスワードを持つことが出来ます。パスワードの情報は、HA クラスタ内では転送されることはありません。

#### 3.2 Set Date/Time “日時の設定”

このオプションは、タイムゾーンとローカル日時をセットします。

タイムゾーンがリストアップされますが、一番初めのゾーンが現在選択されているゾーンです。要求に応じて他のゾーンの選択を行ってください。

日付は、下記のフォーマットで入力します。

02-12-03 (Year-Month-Day)

時間は、下記のフォーマットです。

10:57:15 (Hours:Minutes:Seconds)

**注：**納入されたロードマスターは、UTC タイムゾーンが選択されています。

#### 3.3 Set Keyboard Map “キーボードのマッピング”

このオプションは、異なる言語をサポートしているキーマッピングへの変更を行います。サポートしているマッピングがリストされます。現在選択されているマッピングは、リストの先頭にあるものです。

**注意：**デフォルトのキーボードマッピングは、US/ASCII です。

このマッピング変更は、管理者が SSH 接続でリモート・ログインしている間は有効になりません。一度接続を切り、再接続したときに有効となります。

新しいキーボード・マッピングが選択されると、管理者はそのマッピングが間違いないかチェックするように問われます。もし、キーボードマッピングが正しくない場合は、[CANCEL] ボタンを押して、他の選択が行えます。

### 3.4 Backup/Restore “バックアップ/リストア”

このオプションは、ロードマスターの設定ファイルをリモートマシンへセーブすることを可能にします。

このメニューでは、リモートマシンは FTP か SSH デーモンが動いているサーバでなければなりません。

リモートマシンからリストアを実行する時、管理者はリストアされる設定情報を選択することが出来ます。

#### “Only the Virtual Service configuration”

バーチャルサービスに関する設定情報だけをリストアします。SSL 証明書がインストールしている場合は、この情報はバックアップされていませんので、リストア対象から外れます。

#### “Only the LoadMaster Base Configuration”

バーチャルサービス関連でない他の設定情報だけをリストアします。

#### “Both the Virtual Service and Base Configuration information”

ロードマスターの全ての設定情報をリストアします。

**重要：**HA 構成時のスタンバイ・ロードマスターからのリストアは、許可されていません。これは、バーチャルサービスの設定がいつもアクティブ・ロードマスターによりハンドルされていて、尚且つリストアされる設定情報が上書きされるからです。

### 3.5 Remote Access Control “リモート・アクセス・コントロール”

このオプションは、ロードマスターへのリモートからのアクセスを許可/禁止するものです。

#### Enable/Disable Remote SSH access “SSHアクセスの許可/禁止”

このオプションは、SSH 接続を介してのロードマスターへのアクセスを許可/禁止します。もし、このオプションが禁止されていると、設定メニューへのアクセスはコンソールだけから

可能となります。‘bal’ ユーザのパスワードが設定されていない場合は、SSH 接続を介したログインは出来ません。

### Enable/Disable Remote Web access “WUIへのリモートアクセス許可/禁止”

WUI（ウェブユーザインターフェース）のアクセスを許可/禁止します。

### Change SSHD Address “SSHアクセスの変更”

ロードマスターは、全てのイーサポートにアクセス出来るように設定されて納入されています。このオプションを使い、特定のイーサポートからのみアクセスを許可するように変更が出来ます。

### Change Web Address “ウェブアクセスの変更”

ロードマスターは、ネットワーク側のアドレスを使ってのみアクセス出来るように設定されて納入されています。このオプションを使い、ファームからのみアクセスを許可するように変更が出来ます。又、デフォルトのポート番号443から他のポートへの変更も可能です。

## 4 Basic Setup “基本設定”

このメニューから、管理者がクイック・セットアップの各ステップを別々に実行させることが出来ます。

### 4.1 Network configuration “ネットワーク設定”

イーサネットへの様々なIPアドレスの設定が可能です。

ロードマスターを1アーム構成で使用する時、2つ目のインターフェースは設定する必要はありません。2番目のインターフェース“eth1”の入力を問われたら、何のアドレスも入力しないで[OK] ボタンを押してください。

ロードマスターの他のイーサネット・インターフェースを利用可能にするには、それらのインターフェースをこのメニューから設定可能です。

### 4.2 Hostname Configuration “ホスト名の設定”

ロードマスターのホスト名は、変更が可能です。システムが、HA クラスタとして構成されるいけば、パートナーのホスト名も変更可能です。

**ヒント：**ロードマスターのホスト名は、同じブロードキャストネットワーク内に他のHA クラスタが存在しない限り変更する必要はありません。

### 4.3 DNS configuration “DNS設定”

このオプションは、ロードマスターのネームリゾルバー (DNS) の設定を行うものです。もし、ここで DNS サーバの指定を行わない場合は、ロードマスターはドットで区切られた 4 組の数字 (IP アドレス) でしか実行できません。

このオプションは、3 つまでの DNS サーバの設定を許します。これらは、ドットで区切られた 4 組の数字によるフォーマットでなければなりません。

3 つまでの DNS サーバが、スペースで区切られて指定出来ます。

#### 4.4 Routing Configuration “ルーティング設定”

このオプションは、デフォルトとスタティックのルート設定を許します。

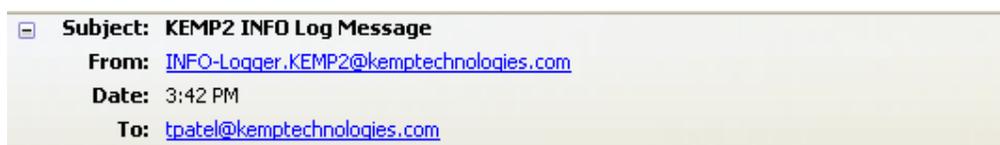
ロードマスターは、インターネットと通信するためのデフォルト・ゲートウェイを要求します。詳細については、アプリケーションガイドを参照ください。

他のルートを、このメニューを使って指定できます。それらのルートは、スタティックでそのゲートウェイは、ロードマスターと同じネットワークにある必要があります。

#### 4.5 Email Configuration “Eメールの設定”

このオプションは、ロードマスターの発するイベントを E メールにて警告として通知するための設定を可能にします。Eメールの通知は、6つの定義レベルに分かれて配信されます。レベル毎に異なる受信者を設定出来、各レベルは複数の受信者を設定出来ます。Eメール警告は、メールサーバによりますが、ノンセキュア、もしくはセキュア (SSL) 両方の通信をサポートしています。設定と発信試験は、WUI の “System Configuration” サブメニュー下の “System Administration” オプションの “E-Mail Options” から行えます。

Eメール警告のサンプル：



Oct 22 19:42:16 KEMP2 logger: This is a test from the Load Master

##### 4.5.1 Set SMTP Server

FQDN フォーマット、もしくは IP アドレスで SMTP サーバを指定します。FQDN フォーマットで指定を行う場合は、DNS サーバの設定を行う必要があります。

##### 4.5.2 Set Authorized User

指定した SMTP サーバが、メール配信を行うために特定権限を必要とするならば、その権限を持ったユーザ名を入力します。もし権限を必要としないならば空白のままとします。

### 4.5.3 Set Authorized Users Password

上記ユーザのためのパスワードを入力します。パスワードは、半角文字で 8 文字から 16 文字までの範囲で指定できます。使用できる文字は英字（大文字、小文字）、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めて下さい。

#### パスワード指定例

- ・英小文字のみ : 9 文字以上 `abcdefghi`
- ・英小文字と数字の混在 : 8 文字以上 `1abcdefgh`
- ・英大文字と英小文の混在 : 8 文字以上 `Abcdefgh`
- ・英小文字、記号、数字の混在 : 8 文字以上 `ab!12345`
- ・数字のみ : 13 文字以上 `0123456789012`

### 4.5.4 Set Local Domain

SMTP サーバが、ドメインに属しているならば最上位のドメイン名を入力します。必要がなければ空白のままとします。

### 4.5.5 Set E-mail Recipient

各警告レベルに応じた E メールを受信者のアドレスを入力します。各レベルには、コンマで区切って複数の受信者を設定可能です。例：

[support@kemptechnologies.com](mailto:support@kemptechnologies.com),[info@kemptechnologies.com](mailto:info@kemptechnologies.com)

## 4.6 Enable L7 transparency “L7 モードのトランスペアレンシー設定”

このトグル・オプションは、システム全体の L7 モードにおけるネットワークのトランスペアレンシー設定を許します。

各 VS で、ネットワーク・トランスペアレンシーの独自設定が出来ますが、ここではデフォルトの設定を行います。

この設定をオンにすると、このパラメータは “Disable L7 Transparency” に変わります。

## 4.7 Using X-Forwarded-For Header “「X-Forwarded-For」のヘッダーへの挿入”

このオプションは、VS が L7 モードで稼動していて、ネットワーク設定をノン・トランスペアレンシーに設定している時（必然的に L7 モードとなる）、HTTP ヘッダー内にクライアントの IP アドレスを “X-Forwarded-For” として挿入します。

このオプションをオンにしなければ、ロードマスターはクライアント IP アドレスのために “X-ClientSide” をヘッダーに挿入します。

このパラメータをオンにすると、オプションは “Using X-ClientSide Header” に変わります。

## 4.8 Adding/No Port Added to Active Cookie “アクティブクッキーへのポート番号付与”

このオプションをオンにすると、ロードマスターが作成するアクティブクッキー内に TCP ソースポート番号の付与を行います。NAT 下に設置したロードマスターからのリアルサーバへのアクセスでは、全てのソース IP アドレスが同じになり、クライアントに返信する時に追加するアクティブクッキーもクライアントが違って同じになってしまいます。そこで、クライアント毎にユニークなクッキーを生産するために、ソースポート番号を付与します。

## 4.9 Support VS/Subnet Originating Requests “ソースIPアドレスのVSへの変更をサポート”

L7 モードで作成された VS は、非透過モードではその配下にある RS との通信時に VS にアサインされた IP アドレス (VIP) を使用します。例えば、2 アーム/マルチアームネットワーク構成下で、もし RS が同じサブネットからのみのアクセスしか許可しない場合、このパラメータをオンにすることで VIP では RS の属するイーサポートの IP アドレスをソース IP アドレスとしてアクセスを行わせることを可能とします。

注：このパラメータは、L4 モードでの VS では有効になりません。又、このパラメータを変更する場合は、システムのリブートが必要です。

# 5 Extended Configuration “拡張設定”

このメニューでは、管理者が主機能には直接影響を及ぼさずに、管理を容易にする設定が行えます。

## 5.1 Interface Control “インターフェース・コントロール”

このオプションは、Web User Interface (WUI) を使用できるイーサネットポートを選択します。デフォルトはポート 0 です。それ以外のポートを経由して WUI を使用したい場合には、このオプションで変更可能です。

## 5.2 Enable/Disable S-NAT “S-NAT機能の有効/無効化”

このトグル・オプションは、ロードマスターの S-NAT 機能の有効、もしくは無効化を行うものです。

S-NAT が有効の時、リアルサーバはロードマスターをゲートウェイとしてインターネットへのアクセスが出来ます。ロードマスターは、マスケラードを使いロードマスターがあたかも発信したかのようにして、リアルサーバからの接続をリクエストします。これは、リアルサーバがプライベート・ネットワーク上にいながらインターネットへのアクセスが出来ることを意味しています。

S-NAT が無効の時は、ロードマスターはマスケラードを実行しませんので、リアルサーバはインターネットへのアクセスが出来ません。

1 アーム構成では、S-NAT は何も機能しません。

### 5.3 Syslogd Configuration “シスログ・サーバ設定”

このオプションを使うことにより、ログメッセージは syslogd プロトコルを使って異なるホストへ送られます。

6つの異なるレベルのホストを指定出来ます：

INFO	このホストは、ロードマスターの全てのメッセージを受信します。
NOTICE	このホストは、ロードマスターの INFO (情報) レベル以外の全てのメッセージを受信します。
WARN	このホストは、NOTICE、INFO レベル以外の全てのメッセージを受信します。
ERROR	このホストは、ERROR,CRITICAL,及び EMERGENCY メッセージを受信します。
CRITICAL	このホストは、CRITICAL、及び EMERGENCY メッセージを受信します。
EMERGENCY	このホストは、EMERGENCY メッセージだけを受信します。

### 5.4 SNMP metrics “SNMPメトリックス”

このメニューより、SNMP 設定を変更できます。SNMP の情報については、アプリケーションガイドを参照ください。

#### Enable/Disable SNMP metrics “SNMP メトリックスの有効/無効”

このトグルオプションは、SNMP メトリックスを有効/無効にするものです。このオプションを有効にすると、SNMP リクエストに対して応答します。

**注：**この設定は、デフォルトでは無効になっています。

#### Configure SNMP Clients “SNMP クライアント設定”

このオプションにより、管理者はロードマスターがどの SNMP 管理ホストへ応答を返すかの指定を行います。

**重要：**もし、クライアントを指定しない場合は、ロードマスターは SNMP 管理リクエストに対しての応答を、不特定のホストへ返します。

#### Configure SNMP Community String “SNMP コミュニティ名の設定”

このオプションは、SNMP コミュニティ・ストリングの変更を許します。デフォルト値は、“public” です。

#### Configure SNMP Contact “SNMP コンタクトの設定”

このオプションは、SNMP コンタクト名列の変更を許します。例えば、ロードマスター管理者の E-Mail アドレスなどです。

### **Configure SNMP Location “SNMP ロケーションの設定”**

このオプションは、SNMP ロケーション名列の変更を許します。

## **5.5 SNMP traps “SNMPトラップ”**

ロードマスターのバーチャルサービスやリアルサーバへの重要なイベントが発生した場合、トラップが作られます。これらは、SNMP トラップシンクへ送られます。

### **Enable/Disable SNMP Traps “SNMP トラップの有効/無効化”**

このトグルオプションは、SNMP トラップの送信を有効/無効にします。

**注：**SNMP トラップは、デフォルトでは無効です。

### **Configure SNMP Trap Sink1 “SNMP トラップシンク 1 の設定”**

このオプションは、管理者がトラップの発生時に、SNMPv1 トラップをどのホストに送信するかを指定します。

### **Configure SNMP Trap Sink2 “SNMP トラップシンク 2 の設定”**

このオプションは、管理者がトラップの発生時に、SNMPv2 トラップをどのホストに送信するかを指定します。

## **5.6 Enable/Disable L7 persistency state failover “L7 パーシステンスのステータスフル・フェイルオーバーの有効/無効化”**

**注：**この機能は、HA クラスタ構成だけで利用可能です。

L7 パーシステンス・オプションが有効になっている時、アクティブ側ロードマスターは、接続情報を自動的にスタンバイマシンへ送信します。これにより、もしアクティブ側が障害でダウンした場合、スタンバイ側ロードマスターはあたかも何も起こらなかったかのようにリクエスト処理を引き継ぎます。この接続情報は、マルチキャスト・プロトコルを使って送られます。この送信先は、パラメータ“Multicast Configuration”により選択可能です。

このトグル・L7 オプションは、接続情報の送信を有効か無効にします。もし、この機能が通信帯域を取りすぎるか、もしくは必要としなければ、リソース保護のために無効にしたままとすることを推奨します。

## **5.7 Enable/Disable L4 connection state failover “L4 接続ステータスフル・フェイルオーバーの有効/無効化”**

**注意：**この機能は、HA クラスタ構成だけで利用可能です。

バーチャルサービスが、パーシステンスを使っていないか、もしくはソース IP アドレスパーシステンスのみ使っている時、アクティブ側ロードマスターは、接続情報を自動的にスタンバイマシンへ送信します。これにより、もしアクティブ側が障害でダウンした場合、スタンバイ側ロードマスターはあたかも何も起こらなかったかのようにリクエスト処理を引き継ぎます。この接続情報は、マルチキャスト・プロトコルを使って送られます。この送信先は、パラメータ“Multicast Configuration”により選択可能です。

このトグル・オプションは、レイヤ4 接続情報の送信を有効か無効にします。もし、この機能が通信帯域を取りすぎるか、もしくは必要としなければ、リソース保護のために無効にしたままとすることを推奨します。

## 5.8 Multicast Configuration “マルチキャスト設定”

**注：**このオプションは、HA クラスタ構成で、尚且つ“L4 connection state failover”、もしくは“L7 persistency state failover”機能のどちらかを有効にしている時にだけ利用可能です。

このオプションにより、接続情報を送信するために使用する、イーサネット・インターフェースとマルチキャスト・アドレス変更が出来ます。ロードマスターを、1 アームモードで使用している時、イーサネットインターフェースは変更出来ません。

## 5.9 HA Parameters “HA関連パラメータ”

**注：**このオプションは、HA クラスタ構成だけで利用可能です。この設定を両方のシステムに反映させるためには、シェアード IP アドレスに WUI からアクセスしてください。システムの一方だけの変更を行うには、各ユニットに与えられているローカル IP アドレスに WUI からアクセスしてください。

### 5.9.1 Set HA Timeout “HAタイムアウト”

このオプションにより、HA クラスタの機能不全検出時間を調整出来ます。設定値は1 から5 までです。デフォルト値は1 です。低い値ほど機能不全を早く検出しますが、DoS 攻撃には高い値が良い防止策になります。

### 5.9.2 Set HA Initial Wait Time “HAクラスタのイニシャル待ち時間”

リブートが行われるとき、実際のリブートが終了してからアクティブモードになる時間を設定します。ロードマスターがリブートする際にスイッチ側にイニシャルを掛けますが、リンクが復旧するまでに遅延が発生するときは、この待ち時間を調整します。調整時間が悪いと、ロードマスターがブートを終了しアクティブ用オペレーションを開始しようとしても、リンクダウンを検出してしまい、その結果、再度のリブートが発生します。スタンバイ側では、この設定は無視されます。

### 5.9.3 Set Preferred Host “優先ホストの設定”

HAクラスターにおける、常時アクティブマシンの設定を行います。この設定を行うことで、仮に設定されたアクティブマシンが機能不全でスタンバイへ切り替わっても、復旧後はこのマシンへアクティブが戻ります。

デフォルトは、どちらも優先権を持っていません。

#### 5.9.4 Set HA update Interface “設定情報更新用インターフェース設定”

アクティブ側が、設定情報の更新が発生した場合の、スタンバイへの情報送信に使用するインターフェースを設定します。

#### 5.9.5 Set HA Virtual ID “HAのID設定”

同じブロードキャストのネットワーク上で、一組以上のHAクラスターを設置する場合、各HAペアにユニークなIDを付与することで情報の混信を防止します。

1組以上のHAペアが存在しなければ、デフォルト値の“1”を変更する必要はありません。

#### 5.9.6 Enable use of Virtual MAC Addresses “バーチャルMACアドレスの無効/有効化”

ファイヤーウォール等で、各IPアドレスに該当するMACアドレスが直ぐに変更できないようにARPテーブルのキャッシュメモリのフラッシュ時間をかなり長く設定されている場合、このバーチャルMACを有効にすることで、HA-1とHA-2両方がアクティブになった時に同じMACアドレスがアサインされるようにします。この機能をオンにした場合は、両方のユニットのリブートが必要です。

## 6 Packet Filter & BalckLists “パケットフィルターとアクセス管理”

### 6.1 Access control Lists “アクセス・コントロール・リスト”

ロードマスターは、“ブラックリスト”アクセス・コントロール・リストをサポートします。このリストに入っているホスト、もしくはネットワークは、ロードマスターによる一切のサービスの提供を受けることが出来ません。

ロードマスターは、更にパケットフィルターを持っています。パケットフィルターを有効にすると、バーチャルサービスで設定してあるポート以外のIPパケットは全てブロックされます。

アクセス・コントロール・リストは、このパケットフィルターを有効にしないと機能しません。デフォルトでは、アクセス・コントロール・リストは無効です。全てのソースIPアドレスが、バーチャルサービスへのアクセスが許容されることを意味します。

注：この機能は、1アーム、2アーム構成に関係なくVSへのアクセスを制御できます。RSへの制御は、2アーム構成に限ってのみ可能ですが、全て許容するか拒否するかの設定のみになります。

### Enable Access Control Lists “アクセス・コントロール・リストの有効／無効化”

このトグルオプションは、パケットフィルター／アクセスコントロールリストの有効化、無効化を行います。有効にすると VS へのアクセスは、Blocked/Allowed list によって制御されます。RS への直接のアクセスは規制されず (2 アーム構成のみ)。

### Show blocked addresses “ブロックアドレスの表示”

このオプションは、現在のバーチャルサービスへのアクセスが規制されているホスト／ネットワークの表示を行います。

### Add address to blocked list “ブロックリストへのアドレス追加”

このオプションは、管理者がアクセスコントロールリストへホスト、もしくはネットワーク IP アドレスの追加を行うのを許します。ドットで区切られた 4 数字の IP アドレスだけが有効です。ネットワークの場合は、ネットワーク・スペシファイヤを使用します。

<例> 192.168.200 の全てのホストをブロックする場合は 192.168.200.0/24 とします。

### Delete address from blocked list “ブロックリストからの削除”

このオプションは、アクセスコントロールリストから IP アドレス、もしくはネットワークの削除を許します。

### Show Allowed address “許容アドレスの表示”

ネットワークをブロックリストに追加した場合、もしその中で特定ホストからのバーチャルサービスへのアクセスを許容させたい時に、“Add address to allowed list” オプションでそのアドレスを追加できます。その許容されたホストの IP アドレスを表示させたい場合、このオプションを使用します。

### Add address to allowed list “許容アドレスの追加”

ネットワークをブロックリストに追加した場合、もしその中で特定ホストからのバーチャルサービスへのアクセスを許容させたい時に、このオプションを使用してその IP アドレスを追加します。

### Delete address from allowed list “許容アドレスの削除”

許容アドレスを削除する時に、このオプションを使用して行います。

### Reject/Drop blocked packets “ブロックリスト・ホストからのパケットのリジェクト／ドロップ”

ブロックリストのホストから接続リクエストを受けた時、そのリクエストは通常無視 (Drop) されます。ロードマスターは、無視する代わりに ICMP リジェクトパケットを返す

ように設定が出来ます。セキュリティのためには、ブロックされた IP アドレスのリクエストは無視するのが最良です。

## 7 Utilities “ユーティリティ”

### 7.1 Software Upgrade “ソフトウェアの更新”

このオプションを使用することで、ロードマスターのソフトウェアのパッチがインストール、もしくは削除されます。

#### Install Update “アップデート”

このオプションで、パッチがリモートサーバからロードマスターへダウンロードされます。サーバは、SSH デーモンが走っている必要があります。

パッチが一旦ダウンロードされると、アンパックされると共に内容の確認が行われます。もしパッチが正しいことが確認されると、パッチ名が表示され、管理者はそのパッチをインストールするかどうか問われます。後で “rollback update” でリカバリーするときのために、現在の OS のコピーが新しいパッチのインストール前にセーブされます。

#### Rollback Update “アップデートのロールバック”

もし、新しいパッチを削除する必要があるれば、このオプションが以前の OS バージョンへのリカバリーを行います。リカバリー OS は、1 つのみ利用可能です。よって、一旦 OS のリカバリーを行った後では、それ以前のバージョンへのリカバリーは不可能です。

#### Reset to Factory Default “設定の出荷時へのリセット”

このオプションを使い、全ての設定を工場出荷時の設定にリセットします。

### 7.2 Transfer Protocol “転送用プロトコル”

このオプションは、ロードマスターがリモートサーバからデータの転送を行う時にどの転送方法を使うかの指定を行うのを許します。選択された方法は、パッチをリモートサーバからダウンロードするか、設定ファイルのリモートサーバへのバックアップ時に使用されます。デフォルト方法は、“ftp”です。

#### Use ftp protocol “ftp プロトコルの使用”

このオプションを使用して、インターネットのスタンダードである FTP プロトコルに設定します。ほとんどのサーバがこのプロトコルをサポートします。

#### Use scp protocol “scp プロトコルの使用”

“scp” セキュアコピー転送モードが選択されます。これは、FTP よりもっとセキュアですが、通常 UNIX サーバのみでサポートされています。もし、このモードが選択されると、SSL 証

明書はウェブインターフェースを介してではなく、メニューシステムからしかインストール出来ません。

### Use http protocol “http プロトコルの使用”

この転送方法を使って、リモートサーバへの設定ファイルのバックアップは実行出来ません。ソフトウェアパッチだけは、どのウェブサーバからでもこの方法でダウンロード出来ます。

### 7.3 Network Time Protocol Host “NTPサーバの設定”

ロードマスターの時間を、NTP サーバと同調出来ます。時間は、ブート時と一時間ごとに同調します。このオプションを使用し、NTP サーバのアドレスを指定します。

### 7.4 SSL certificate administration “SSL証明書管理”

このオプションは、現在インストールされているSSL証明書の管理を可能にします。SSLアクセスレーションが有効になっているバーチャルサービスがリストされます。バーチャルサービスを選択することにより、証明書の管理サービスを許します。ローカルオプションの選択により、ウェブインターフェースのために使用される証明書の再作成を許可します。

#### Get a certificate file “証明書のダウンロード”

このオプションは、管理者がバーチャルサービスのための証明書ファイルをダウンロードするのを許します。

注意：証明書ファイルの転送は、SCP プロトコルの使用を推奨します。

#### Get a key file “プライベートキーのダウンロード”

このオプションは、バーチャルサービスのプライベートキーをダウンロードするのを許します。もし、プライベートキーが証明書ファイルに含まれているならば、追加的なプライベートキーは要求されません。

#### Delete the key and certificate files “プライベートキーと証明書ファイルの削除”

管理者が、指定されたバーチャルサービスの証明書とプライベートキーを削除するのを許します。

### 7.5 Update License “ライセンスの更新”

このオプションは、新しいライセンスキーの入力を許可します。

<例> 評価用からフルライセンスに更新する時。

### 7.6 L7 Idle Timeout “L7 セッション用アイドルタイマー”

このオプションは、L7 セッションにおけるアイドル時のタイムアウトの設定を行うのを許します。デフォルト値は660秒です。（表示上は“0”）

## 7.7 Diagnostics “診断ツール”

このサブメニューは、管理者がロードマスターの診断機能を実行するのを許します。

### Ping Remote Host “リモートホストへの PING”

リモートホストは、このオプションで PING されます。

### Self Test “自己診断”

このオプションを使用して、自己診断プログラムを起動します。4 つの診断項目が全て Up & Running になっている必要があります。

### View Log Files “ログファイルの取得”

システムのログを見るためのオプションです。ブートメッセージ、警告メッセージ、システムメッセージ、HA ログファイル (HA 構成時のみ) を取得できます。

### Software Versions “ソフトウェアのバージョン情報”

現在の OS バージョンを表示します。

### Show Partner IP Address “パートナーマシンの IP アドレスチェック”

HA クラスタ構成時のパートナーマシンの IP アドレスを表示します。設定されていない場合は、パートナーアドレスを入力出来ます。変更も可能です。

### Enable Diagnostic login “診断ユーザログインの有効/無効化”

重要：このオプションは、KEMP テクノロジー社のサポート要員がリクエストした場合にのみ有効にすべきです。

もし、このオプションが通常オペレーションで有効化されると、許可されていないアクセスを受ける可能性があります。診断ユーザログインは、ロードマスターのリブートにより無効になります。又、有効になっていると、このパラメータから無効にすることが可能です。

### Restart Daemon “デーモンのリスタート”

ロードマスターが使用しているデーモンを全てリスタートさせます。

### Diagnostic Shell

診断のために、シェルを起動するオプションです。“tcpdump”、“ftp”などが使用できます。

## 8 Reboot “リブート”

このオプションは、ロードマスターをリブートします。全ての設定変更は、リブートする前にセーブされます。

**注意：**HA クラスター構成で稼動しているとき、スタンバイ側マシンはアクティブ側より更新された設定情報をリブート前に受け取っています。よって、アクティブ側のリブートの結果、スタンバイ側に切り替わっても、最新の設定で稼動します。

## 9 Exit LoadMaster Config “設定画面よりの退出”

このオプションは、管理者が設定メニューより退出するのを許します。

もし、何らかのパラメータが変更されていたら、管理者はその変更を有効にさせるかどうか聞かれます。“Yes”の確認が行われると、変更は有効になります。もし、管理者が変更を有効にしたいくなければ、後で有効にするためにセーブするかどうかを問われます。確認が “No” の場合は、変更は全て削除されます。

## F. ロードマスター設置用質問表

### 1 単一ロードマスター・バランサー・ソリューション

マシン 1

ネットワーク側: eth0

IPアドレス

---

ネットマスク

---

ファーム側: eth1

IPアドレス

---

ネットマスク

---

ホスト名

---

DNSサーバ

(3つまで)

---

サーチドメイン

(2つまで)

---

デフォルトG/W

IPアドレス

---

### 2 HAデュアル・ロードマスター・バランサー・ソリューション

マシン 1

マシン 2

ネットワーク側: eth0

IPアドレス

---

ネットマスク

---

シェアードIPアドレス

---

ファーム側: eth1

IPアドレス

---

ネットマスク

---

シェアードIPアドレス

---

ホスト名

---

DNSサーバ

(3つまで)

---

サーチドメイン

(2つまで)

---

デフォルトG/W

IPアドレス

---

### III. コマンドライン・インターフェース参照ガイド

コマンドライン・シンタックスは、他のロードバランサー・メーカーによって使用されている業界標準シンタックスを基にしていますが、厳密ではありません。

コマンドインターフェースは、ラインベースで、階層的なコマンドセットを持っています。設定の変更は、階層の最初のレベルまで戻らないと有効になりません。

ヒント：ポートは、数字か、又は記号名で指定します。下記の記号名が認知されています。

DNS	53
FTP	21
HTTP	80
IMAP4	143
LDAP	389
POP2	109
POP3	110
SMTP	25
SNMP	161
SSL	443
TELNET	23
TFTP	69

## 1 最上階層のコマンド

最上階層で、下記のコマンドを指定できます。

### 1.1 Adaptive

このコマンドは、負荷分散方式の Adaptive 用パラメータの幾つかのコマンドセットへ入り込むための切り替えを行います。

### 1.2 Delete <VS 名/VIP アドレス>

このコマンドで特定の VIP を削除できます。

### 1.3 Disable\_rs <IP 指定>

このコマンドは、特定のリアルサーバを利用不可能にします。<例> 特定リアルサーバへのトラフィックを止めたい場合。このコマンドは、全てのバーチャルサービスに設定してある同じリアルサーバを利用不能にします。

### 1.4 Enable\_rs <IP 指定>

このコマンドは、特定のリアルサーバを利用可能状態に戻します。全てのバーチャルサービスにおいて、このリアルサーバは利用可能状態になります。

### 1.5 Healthcheck

このコマンドは、ヘルスチェック用パラメータのコマンドセットへ入り込むための切り替えを行います。

## 1.6 Rules

このコマンドは、ルール設定用パラメータのコマンドセットへ入り込むための切り替えを行います。“Rules”は、L7 オプションを利用可能にした場合に利用出来ます。

## 1.7 Show <バーチャルサービス名/VIP>

このコマンドは、指定されたバーチャルサービスに関連する全ての情報を表示します。もし、バーチャルサービスが指定されなかった場合は、全てのバーチャルサービスの情報が表示されます。

## 1.8 Vip <バーチャルサービス名/VIP>

このコマンドは、バーチャルサービスのコマンドセットへ入り込むための切り替えを行います。VIPは、バーチャルサービスのIPアドレスです。もし、バーチャルサービスのIPアドレス、もしくはサービス名が指定されない場合は、新しいバーチャルサービスが作成されます。コマンドセットで設定を変更しても、このCLIの最初のレベルまで戻らなければ、その変更は有効にはなりません。

## 1.9 Help

現レベルでのコマンドセットを表示します。

## 1.10 End

CLIのセッションを終了させます。

## 1.11 Exit

コマンドレベルを1つ戻します。最初のレベルに戻ってからは、このコマンドでは何も行われません。

## 2 “Adaptive” のコマンドセット

下記のコマンドが、“Adaptive”レベルで利用可能です。CLI階層の最初に戻ってきたときに変更が有効になります。最初のレベルに戻るには、exitコマンドを繰り返します。

### 2.1 Interval <Integer>

このコマンドにより、リアルサーバへの負荷値の採取周期時間<Integer>秒をセットします。

### 2.2 Min <Integer>

アダプティブ負荷分散方式が作動するための、最低の負荷値 (%) を <Integer> でセットします。もし、負荷がこの境界値より低くなったら、バーチャルサービスはこのサーバをアイドル状態とし、重み付けを静的に設定している値に戻します。

### 2.3 Port <ポート番号>

アダプティブ負荷分散方式が可能なサーバより、負荷値を採取する時に接続するポート番号を指定します。

### 2.4 Show

アダプティブ方式の、現在のパラメータ設定値を表示します。

### 2.5 Url <String>

アダプティブ方式で、負荷値を採取する URL を指定します。この URL で指定する負荷値の内容は、0 が負荷が何もない状態で、100 が最大負荷状態を示します。

詳細については、アプリケーションガイドの 6.5 エージェントベースのアダプティブ配分を参照ください。

### 2.6 Weight <Integer>

重み付けの静的最小値を指定します。

アダプティブ分配方式は、サーバの重みをこれ以下には調整しません。

### 2.7 Help

アダプティブ用コマンドレベルで利用可能なコマンドを表示します。

### 2.8 End

CLI セッションを終了します。変更した設定は、全て削除されてしまいます。

### 2.9 Exit

1 つ前の CLI 階層へ戻ります。最後の階層へ戻ると、変更した設定が設定ファイルにセーブされ、システムがその変更を有効にします。

## 3 “Healthcheck” のコマンドセット

### “Healthcheck” コマンドレベル

#### 3.1 Interval <Integer>

リアルサーバの、死活チェックの周期間隔を指定します。

#### 3.2 Retry <Integer>

リアルサーバの死活チェックでレスポンスがない場合に、何回再試行を行うかを指定します。

### 3.3 Show

Healthcheck パラメータの現状設定を表示します。

### 3.4 Timeout <Integer>

リアルサーバからの応答時間を指定します。ロードマスターは、Timeout 値 x Retry 値までにサーバからの応答がない場合は、ダウンとみなします。

### 3.5 Help

Healthcheck コマンドレベルのコマンドセットをリストします。

### 3.6 End

CLI セッションを終了します。Healthcheck レベルで変更をした設定は、全て無視されます。

### 3.7 Exit

Healthcheck コマンドレベルを離れ、変更を加えた設定がシステムにセーブされ有効となります。

## 4 “Rules”のコマンドセット

下記のコマンドが、Rules コマンドレベルで実行できます。

### 4.1 Add <ルール名>

このコマンドは、新しいルール<ルール名>を作成します。そして、ルール編集コマンドレベルへスイッチします。Rules コマンドレベルへ戻ることで、別のルールの作成、もしくは変更が出来ます。

ルールは、リアルサーバへアサインする前に作成する必要があります。

### 4.2 Modify <ルール名>

このコマンドは、ルール編集コマンドレベルへスイッチさせます。rule <ルール名> で既存のルールを編集出来ます。

### 4.3 Delete <ルール名>

これは、特定のルールを削除します。このルールをアサインしている全てのリアルサーバから、このルールは削除されます。

### 4.4 Show [ <ルール名> ]

ルール名を指定して設定を表示させます。ルール名の指定がなければ、全てのルールを表示します。

#### 4.5 Help

現在の階層で使用できる全てのコマンドをリストアップします。

#### 4.6 End

CLIセッションを終了します。ルールコマンドレベルで作成、変更した設定は全て失われます。

#### 4.7 Exit

1つ前の階層に戻ります。一番最初の階層に戻ると、このコマンド層で作成、変更した設定が有効になります。

### 5 “Rules”編集コマンドレベル

Rule 編集コマンドレベルでは、下記のコマンドが実行できます。

#### 5.1 value <string>

このオプションで、マッチするルール文をセット出来ます。スペースは意味を持ちます。デフォルトでは、文はレギュラー表現として扱われます。もし <プレフィックス>、もしくは<ポストフィックス>がセットされると、受信するめいめいの URL の初めか終わりにマッチするための一語一語の文と扱われます。

#### 5.2 [no] negation

このコマンドは、ルールの意図を反対にします。もし、no ならば従来の意図に戻ります。例えば、negation がセットされると、ルールにあった文をもつ URL を受け取ったとしてもマッチせず、反対にルールにあった文がない URL がマッチすることになります。

#### 5.3 [no] prefix

これは、ルール文のマッチを、受け取った URL 文の初めの部分で行うように指定します。“no” は、このセットをリセットします。

#### 5.4 [no] postfix

これは、ルール文のマッチを、受け取った URL 文の終わりの部分で行うように指定します。“no” は、このセットをリセットします。

#### 5.5 [no] regex+host

これは、ルール文のマッチを、受け取った URL 文とホスト名の連鎖で行わせるように指定します。“no” は、このセットをリセットします。

## 5.6 [no] prefix+host

これは、ルール文のマッチを、受け取った URL 文の初めの部分とホスト名の連鎖で行わせるように指定します。“no”は、このセットをリセットします。

## 5.7 [no] postfix+host

これは、ルール文のマッチを、受け取った URL 文の終わりの部分とホスト名の連鎖で行わせるように指定します。“no”は、このセットをリセットします。

**注意：**“no”を全てのオプションで選んだ場合は、デフォルトであるホスト名を含ませない Regular 表現でのマッチに戻ります。

## 5.8 Show

現在のルール値を表示します。

## 5.9 Help

ルール編集コマンドレベル層で利用可能なコマンドをリストします。

## 5.10 End

CLI セッションを終了します。ルールコマンドレベルで作成、変更した設定は全て失われます。

## 5.11 Exit

1 つ前の階層に戻ります。一番最初の階層に戻ると、このコマンド層で作成、変更した設定が有効になります。

# 6 “VIP”のコマンドレベル

下記のコマンドが、Virtual Service コマンドレベルで利用可能です。“exit”コマンドで、最初の CLI 階層に戻ることで、設定が有効になります。もし VIP がなんらかのエラーを含んでいると、管理者はその VIP を破棄するかどうか聞かれます。もし VIP を破棄したならば、最初の層に戻ります。VIP を破棄しない場合は、Virtual Service コマンド階層に留まりますが、エラーを修正する必要があります。

## 6.1 [no] Adaptive <String>

このバーチャルサービスが、Adaptive 負荷分散方式を使うかどうか指定します。現状では、”  
http\_rs “方式だけが利用可能です。利用不可にする場合は、no adaptive コマンドを使用します。

## 6.2 Add <IP アドレス>

このコマンドは、バーチャルサービスに<IP アドレス>で指定したリアルサーバを追加します。又、この入力で、リアルサーバ・コマンドレベルにスイッチします。リアルサーバ・コマンドレベルより戻ると、次のリアルサーバを追加できます。

### 6.3 Address <IP アドレス>

新しく作成するバーチャルサービスの IP アドレスを指定します。

### 6.4 [no] Cookie <String>

クッキーベースのパーシステンシー方式を使用するときは、このコマンドでクッキーを指定出来ます。このコマンドは、ロードマスターが L7 オプションを有効にしていると使用できます。<passive-cookie> と <passive-cookie-src> パーシステンシー方式を使用するならば、<string>は必須です。設定した<string>を削除する場合は、“no cookie” コマンドを使用します。

### 6.5 Delete <IP アドレス>

バーチャルサービスよりリアルサーバを削除する場合に、<IP アドレス>で指定します。バーチャルサービスは、最低1つのリアルサーバを持たなければなりません。

### 6.6 Disable

バーチャルサービスを利用不可にします。これは、バーチャルサービスが新しいリクエストを受け付けなくなることを意味します。

### 6.7 Enable

バーチャルサービスを再利用可能にします。バーチャルサービスは、再び新しいリクエストを受け付けるようになります。

### 6.8 Follow <ポート番号>

このコマンドは、ロードマスターが L7 オプションを有効にしている時のみ働きます。これは、HTTP と HTTPS 用バーチャルサービスが、同じリアルサーバに接続されるように、ポート番号が違ってここで指定したポートへの接続ならば前の接続をフォローします。ポート 80 (HTTP) から 443 (HTTPS) へのポートフォローがその例です。

### 6.9 Mask <IP マスク>

L4 モードのバーチャルサービスで、ソース IP パーシステンシー方式を使う場合、ソース IP アドレスのグループ化をどのように行うか指定します。デフォルトは、255.255.255.255 で全ての IP アドレスを個別に扱います。

### 6.10 [no] Name <ニック名>

バーチャルサービスのニック名を指定します。ニック名を削除する場合は、“no name” コマンドを使用します。

### 6.11 Healthcheck <String>

バーチャルサービスに与えるヘルスチェック方式を指定します。もし、バーチャルサービスが一般的なポート番号ならば、それにあつた方式が自動的に設定されます。下記のヘルスチェックが指定可能です。

http	Http
https	Https (SSL)
smtp	Simple mail transfer protocol
nntp	Nnetwork news transfer protocol
ftp	File transfer protocol
telnet	Telnet protocol
pop3	Postoffice - mail client protocol
imap	Imap - mail client protocol
tcp	基本的なTCP接続
dns	DNSリクエストをリアルサーバのポートに送信します。これはUDPプロトコルでのみ有効です。
udp	ダミーの0バイトの UDP パケットをリアルサーバのポートに送信します。
icmp	ICMP ping をリアルサーバへ送信します。

### 6.12 [no] Persist < パーシステンシー方式>

このコマンドは、バーチャルサービスがどのパーシステンシー方式を使用するか指定します。どのパーシステンシー方式も使用しないならば、“no persist” コマンドを使用します。下記のパーシステンシー方式が指定可能です。もし、L7 オプションが有効になっていないと、< s r c >パーシステンシー方式だけが利用可能です。

ssl	SSL接続で、セッションIDを利用してリアルサーバへのパーシステンシーを維持します。
cookie	サーバが作ったクッキーを使用します。
active-cookie	ロードマスターが作ったクッキーを使用します。
url	同じURLのリクエストを、いつも同じリアルサーバへ行くようにします。
host	同じホストへのリクエストを、同じリアルサーバへと行かせます。
src	IPベースのパーシステンシーを有効にします。
cookie- src	サーバが作ったクッキーを優先的にパーシステンシーで使用しますが、もしクッキーがリクエストに含まれていない時は、クライアントのIPアドレスを使います。
active- cook-src	ロードマスターが作ったクッキーを優先的にパーシステンシーに使用しますが、もしクッキーがリクエストに含まれていない時は、クライアントのIPアドレスを使います。
cookie- hash	同じクッキーのセットを持つリクエストは、いつも同じリアルサーバへ送られます。クッキーがない場合には、負荷分散方式に沿って次のサーバへ送られます。

### 6.13 Port <ポート番号>

バーチャルサービスが使用するポート番号を指定します。ヘルスチェック方式を指定しなくても、一般的なポート番号ならば該当する方式が自動的に選択されます。

### 6.14 Precedence <ルール名> <番号>

ルールの優先順位<番号>をセットします。番号1は、ルールリストの中で最初にチェックするルールです。高い番号ほど優先順位が下がります。もし、<default>ルールがリアルサーバで指定されたら、この Precedence ルールは、どの定義されたルールよりも高い順位となります。よって、<default>ルールは、全ての他のルールの後にチェックされます。

### 6.15 Protocol <tcp/udp>

バーチャルサービスで使用するプロトコルを指定します。これは、<tcp> か <udp> になります。デフォルトは <tcp> です。

### 6.16 Ptimeout <Integer>

ロードマスターが、接続のパーシステンシーを維持するための情報を、どれだけ長く記憶するかを指定します。この値は、秒で指定されます。

### 6.17 Schedule <負荷分散方式>

これは、リアルサーバへの負荷分散方式を指定します。下記の分散方式が指定出来ます。

rr	ラウンドロビン (デフォルト)
wrr	重み付けラウンドロビン
lc	最小接続
llc	重み付け最小接続

### 6.18 Server <IP アドレス>

このコマンドは、リアルサーバを指定して、リアルサーバ・コマンドレベルへ入ります。リアルサーバは、バーチャルサービスへ既にアサインされている必要があります。

### 6.19 [no] cache

該当するバーチャルサービスのキャッシュをオン/オフします。

### 6.20 [no] compress

該当するバーチャルサービスの圧縮機能をオン/オフします。

### 6.21 [no] urlverify <0-7>

該当するバーチャルサービスの IPS 機能をオン (1 - 7) / オフ (0) します。

### 6.22 [no] dftgw <IP アドレス>

該当するバーチャルサービスのデフォルト・ゲートウェイを設定します。

### 6.23 Show

現状のバーチャルサービスの全てのパラメータを表示します。

### 6.24 Help

バーチャルサービス・コマンドレベルの、全てのコマンドのリストアップを行います。

## 6.25 End

CLI セッションを終了します。バーチャルサービス・コマンドレベル、もしくは下位層で作成、変更した設定は全て失われます。

## 6.26 Exit

最上階層へ戻ります。バーチャルサービスへの変更がセーブされます。もし、バーチャルサービスの設定にエラーが検出されたら、システムがエラーをレポートし、バーチャルサービスを破棄するかどうか聞いてきます。もしそのバーチャルサービスが破棄されなかった場合は、同じコマンドレベルに残り、エラーの修正を行えます。

# 7 “Real Server”コマンドレベル

このコマンドレベルで、特定のリアルサーバを設定できます。下記のコマンドが、このレベルで利用可能です。

## 7.1 Addrule <ルール名>

このコマンドは、リアルサーバヘルール<ルール名>を追加します。もし、これが最初のルールのアサインならば、優先順位リストの最下位ユーザ定義ルールとして置かれます。優先順位を変更するには、VIP コマンド層の **Precedence** コマンドを使用します。

## 7.2 Delrule <ルール名>

このコマンドは、リアルサーバからルール<ルール名>の関連付けを取り除きます。もし、バーチャルサービスで他のリアルサーバがこのルールを関連付けていなければ、バーチャルサービスの優先順位リストから削除されます。

## 7.3 Disable

現在のリアルサーバを利用不可にします。リアルサーバは、このバーチャルサービスだけで利用不可になります。他のバーチャルサービスに関連付けられている同リアルサーバは、影響を受けません。

## 7.4 Enable

バーチャルサービスのリアルサーバを利用可能状態に戻します。もし、リアルサーバが他のバーチャルサービスにも設定されていても、このバーチャル以外に影響を受けません。

## 7.5 Forward <フォワード方式>

これは、リアルサーバへのアクセス方法として使用されるフォワード方式を指定します。フォワード方式は、<nat> か <route> です。デフォルト方式は、<nat> で、<route> は **Direct Server Return** を使用するときを選択されます。

## 7.6 Port <ポート番号>

リアルサーバが使用すべきポート番号を指定します。もし、ポート番号が指定されないと、バーチャルサービスのポート番号が使用されます。

### 7.7 Show

現在のリアルサーバのパラメータを表示します。

### 7.8 Weight <integer>

リアルサーバの重みを指定します。これは、リアルサーバの重みを使用する幾つかの分配方式を使う時に使用されます。

### 7.9 Help

この階層で利用出来るコマンドをリストアップします。

### 7.10 End

CLIセッションを終了します。VIP、及び Real Server コマンド層で行われた変更はセーブされません。

### 7.11 Exit

VIP コマンドレベルへ戻ります。現在のバーチャルサービスの編集が完了しないと、変更はセーブされません。

## IV. ウェブ・ユーザ・インターフェース (WUI) 設定ガイド

### A. 用語と略語

アクセスコード: アクセスコードは、ロードマスターが初期設定中に発生するハード特有のユニークなコードです。このコードを基に、販売代理店の方からフルライセンスの供給を受けることができます。

balancer、分散装置: ネットワークより入ってくるトラフィックをサーバに振り分けるネットワーク装置、もしくは論理。

ファームサイド、ファーム側: ロードマスターの、サーバファームに接続されているネットワークインターフェース。

フラットベース: バーチャルサービスとリアルサーバが同じサブネットにあるネットワーク形態。

HA: ハイ・アベイラビリティ、冗長構成

ICMP: Internet Control Message Protocol

MIB: Management Information Base の略で、OID (object definitions) のデータベース。オブジェクト定義を監視する SNMP マネージャーに必要な詳細情報。

NAT: Network Address Translation

NAT ベース: ロードマスターで受信したリクエストの宛先 IP アドレスをリアルサーバの IP アドレスに変換するネットワーク形態。リアルサーバからの帰りのトラフィックは、ロードマスターを介して戻らなければならない。そして、その帰りのソース IP アドレスは、バーチャルサービス・アドレス (VIP) へ変換される。

ネットワークサイド、ネットワーク側: ロードマスターで、バーチャルサービスを収容しクライアントのリクエストを受け取るネットワーク・インターフェース。

1 アーム: 内向け、外向けの両方のトラフィックを1つのイーサポートを使って行うネットワーク形態。フラットベースとも言われる。

RS: リアルサーバ: サーバファームを構成する物理的なサーバマシン。

サービス: ネットワークに接続されるアプリケーション。

シェアードIP: 特定のインターフェース (例えばイーサ0、イーサ1)上で、保障された利用可能アドレス。HA 構成の場合のみ使用する。

SCP: SSH 接続時の Secure copy command

- SNMP:** Simple Network Management Protocol。TCP/IP ネットワークを管理するネットワーク・プロトコル。このプロトコルは、MIB によって与えられるデータオブジェクトへのアクセスを可能にする機能を持っている。
- S-NAT:** ソース IP アドレスのためのネットワークアドレス変換。
- SSH:** Secure Shell Protocol
- 2 アーム:** バーチャルサービス・アドレス (VIP) とリアルサーバのサブネットが異なるネットワーク形態。
- UTC:** Universal Time Coordinated
- VIP:** Virtual IP Address: ロードマスター上で定義されるサービスの IP アドレス。
- VS:** バーチャルサービス: ロードマスター上でサーバファームのサービスに到着させるためのエントリ。(クラスター)
- WUI:** Web User Interface。ウェブブラウザを介してロードマスターを管理するインターフェース。

## B. ファーストトラック (*Fast Track*)

下記セクションでは、バーチャルサービスを作成するために要求されるステップを、最初から最後まで紹介します。

### 1 ログインの仕方

好きなブラウザをスタートし、管理しようとしているロードマスターの URL を入力します。下記の図では、192.168.1.101 がロードマスターのイーサネット 0 のアドレスで、URL は：

<https://192.168.1.101> となります。

そうすると、ユーザ証明を聞かれます。デフォルトのユーザ名は 'bal' で、仮定義されているパスワードは '1fourall' です。

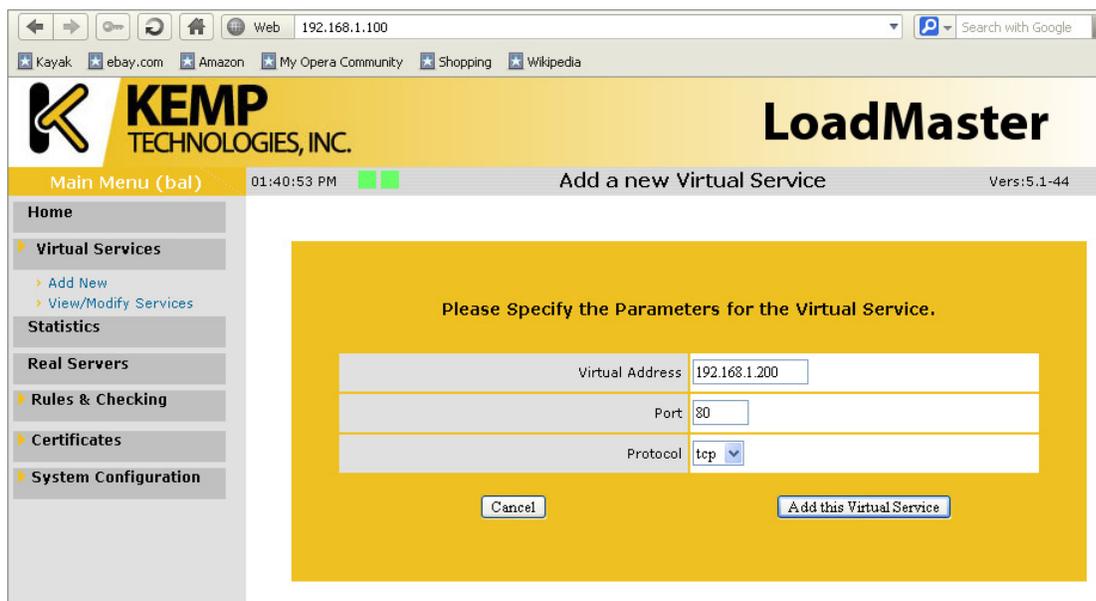
**注意：**ユーザ 'bal' のパスワードは、初期設定でコンソールから変更されている必要があります。その変更されたパスワードが、この WUI 接続で使用されなければなりません。



## 2 シンプルなバーチャルサービス作成

このセクションは、2つのリアルサーバを持つシンプルなバーチャルサービスの作成に必要なステップを通します。

バーチャルサービス作成プロセスを始めるには、左の“Virtual Service”サブメニューを選択し、次に“Add New”メニュー項目をクリックします。ここで、バーチャル IP (VIP) アドレスとポート番号、及びプロトコルを入力すると、バーチャルサービスのパラメータページが開きます。



例えば、顧客の“[www.a-domain.com](http://www.a-domain.com)”の IP アドレス **192.168.1.200** を **VIP** アドレスとして入力します。ポート番号は、HTTP サービスの場合は、通常 80 です。プロトコルは、TCP もしくは UDP の選択値がありますが、TCP がほとんどのケースで一般的です。

入力した VIP アドレス、ポート番号、プロトコルが正しければ、バーチャルサービス属性画面に移るために“Add This Virtual Service”ボタンをクリックします。そして、パーシステン

シーなし、コンテンツスイッチなしとし、負荷分散方式をデフォルトのラウンドロビン方式のままとして、何も特別の機能を必要としないものとします。

The screenshot displays the 'Properties of VIP tcp/192.168.1.200:80' configuration page in the Kemp LoadMaster WUI. The interface is yellow and white. The main content area is titled 'Properties for 192.168.1.200:80 - Operating at Layer 7'. It contains several sections:

- Basic Properties:** Includes checkboxes for 'Activate or Deactivate Service' (checked), 'L7 Transparency' (unchecked), and 'Use Address for SNAT' (unchecked). It also has dropdowns for 'Service Type' (HTTP/HTTPS), 'Scheduling Method' (round robin), and 'HTTP Method' (HEAD). Input fields are provided for 'Port Range' (80-), 'Extra Ports', 'Checked Port', 'URL', and 'Idle Connection Timeout' (0).
- Real Server Check Parameters:** Includes a 'Set Check Port' button, a 'Set URL' button, and a 'Use HTTP/1.1' checkbox (unchecked).
- Service Nickname:** Includes a 'Set Nickname' button.
- Persistence Options:** Includes a 'Mode' dropdown set to 'None'.
- SSL Properties:** Includes an 'SSL Acceleration' checkbox (unchecked).
- Advanced Properties:** Includes a 'Content Switching' checkbox (checked) and buttons for 'Rule Precedence' and 'Disable'.

最後に実行するアクションは、リアルサーバの追加です。リアルサーバのパラメータページに移るために、リアルサーバテーブルの“Add New...” ボタンをクリックします。ここで、追加したいリアルサーバの IP アドレスを指定し、そのポート番号とフォワード方式を入力します。もし、追加するリアルサーバがローカルネットワーク以外にある場合は、“System Configuration” サブメニューの“Miscellaneous Options” オプション下の“Network Option”内の“Enable Non-Local Real Server”を‘Yes’にする必要があります。このパラメータを‘Yes’にすることで下図のリアルサーバ追加画面に“Allow Remote Addresses”が表示されます。(注：Transparency モードではこの機能は使用できません。VS の“Force L7”をオンにして“L7 Transparency”をオフにする必要があります。)

**Please Specify the Parameters for the Real Server**

Allow Remote Addresses	<input type="checkbox"/>
Real Server Address	<input type="text" value="192.168.1.30"/>
Port	<input type="text" value="80"/>
Forwarding method	<input type="text" value="nat"/>
Weight	<input type="text" value="1000"/>

この例では、リアルサーバは、同じネットワーク 192.168.1.0 上にあると仮定し、リアルサーバの IP アドレスを ‘192.168.1.30’ を “Real Server Address” 欄に入力します。この時点では、ポート番号 (Port)、フォワード方式 (Forwarding method)、重み (Weight) は考慮する必要はありません。登録を完了するために、“Add This Real Server” ボタンをクリックします。リアルサーバを追加する旨のポップアップ画面が表示されますので OK ボタンを押します。他のリアルサーバを追加するには、同じ手順で他のリアルサーバの IP アドレスを登録します。

全ての変更は、リアルタイムで有効になりますので、このバーチャルサービスは作成され稼動し始めています。作成したバーチャルサービスのサマリーを見るために、左の “Virtual Services” サブメニュー下の “View/Modify Existing” をクリックします。バーチャルサービス・テーブルに、今作成したバーチャルサービスがリストされているはずで

Virtual IP Address	Prot	Name	Layer	Certificate Installed	Scheduler	Status	Real Servers	
192.168.1.200:80	tcp		L7		round robin	Up	192.168.1.30	<input style="margin-right: 5px;" type="button" value=" Modify "/> <input style="margin-left: 5px;" type="button" value=" Delete "/>

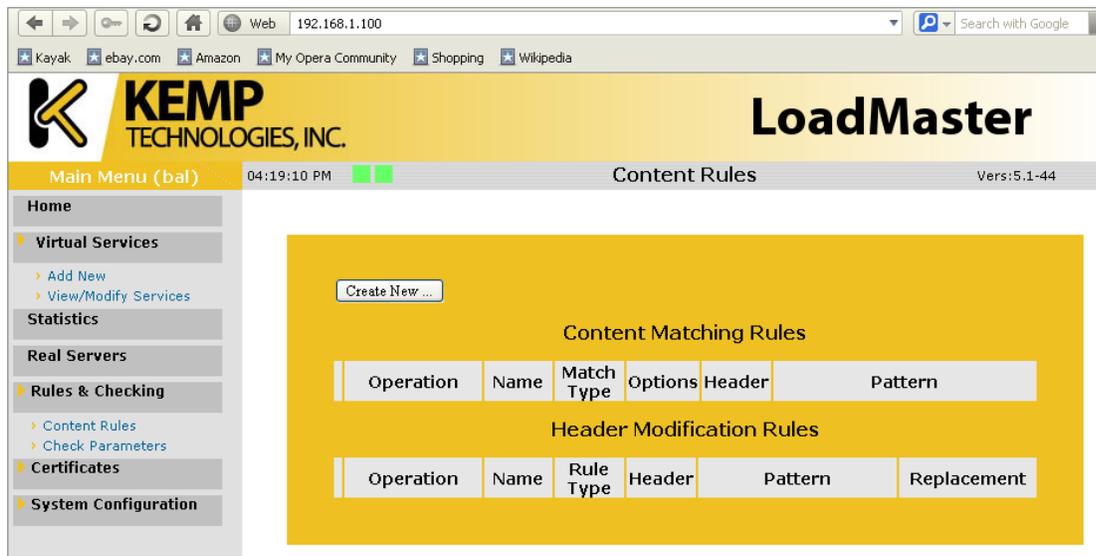
### 3 コンテンツルールの作成

このセクションでは、コンテンツスイッチを使用するバーチャルサービスの作成に必要なルールの作成とその使用方法について説明します。コンテンツスイッチは、ルールに沿って、HTTP リクエストを該当するサーバに転送します。ルールには、下記の種類があります。

コンテンツ・マッチング・ルール  
ヘッダー・モディフィケーション・ルール  
Add Header  
Delete Header  
Replace Header  
Modify URL

#### コンテンツ・マッチング・ルール

このステップを始めるには、最低1つのルールを作成する必要があります。WUIでのコンテンツルール管理セクションは、“Rules & Checking”サブメニュー下にあります。“Content Rules”をクリックすると既存のコンテンツルールのサマリーリストを見ることが出来ます。



新しいコンテンツルールを作成するルール作成ページを開くために、“Create New...”ボタンをクリックします。“CreateRule”画面が表示されますので、“Rule Type”に‘Content Matching’が選択されていることを確認します。ルールをセットするために、8つのパラメータがありますが、“Rule Name”、“Match Type”と“Match String”だけが必須項目ですので、ここでは他パラメータ“Header Filed”、“Negation”、“Include Host in URL”、と“Include Query”は使用しません。

“Rule Name”フィールドに、識別用のルール名を入力します。この例では、ルール名を“testrule”とします。次に、ルールタイプ“Prefix”、“Postfix”、もしくは“Regular Expression”を選択します。これらのタイプの詳細は、次の章で説明されますので、この例では“Postfix”を選択します。最後に、ロードマスターがマッチングを試みるためのテキストを入力します。この例では、JPEG グラフィック・ファイルの入手リクエスト (HTTP

GET) がきたらコンテンツスイッチを実施させるために、“jpg”と入力します。ルール作成を終えるために、“Commit” ボタンをクリックします。コンテンツルール管理ページに戻り、今作ったルールがリストされるはずです。

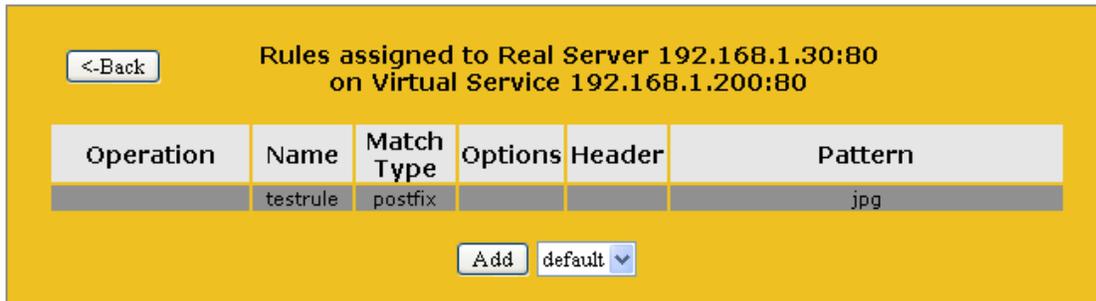
Rule Name	<input type="text" value="testrule"/>
Rule Type	Content Matching ▼
Match Type	Postfix ▼
Header Field	<input type="text"/>
Match String	<input type="text" value="jpg"/>
Negation	<input type="checkbox"/>
Ignore Case	<input type="checkbox"/>
Include Host in URL	<input type="checkbox"/>
Include Query in URL	<input type="checkbox"/>

次のステップは、バーチャルサービスがコンテンツスイッチを行えるようにする事です。もし、このルールを新しいバーチャルサービスのコンテンツスイッチのために使用したいならば、この前のセクションで説明している方法に沿って、新しいバーチャルサービスを作成してください。既存のバーチャルサービスにコンテンツスイッチを追加するのであれば、バーチャルサービス・テーブルの該当バーチャルサービスの“Modify” ボタンをクリックします。属性ページで、“Advanced Properties” セクション内に“Content switching: disabled”のパラメータと“Enable” ボタンがあるのに気がつくはずです。

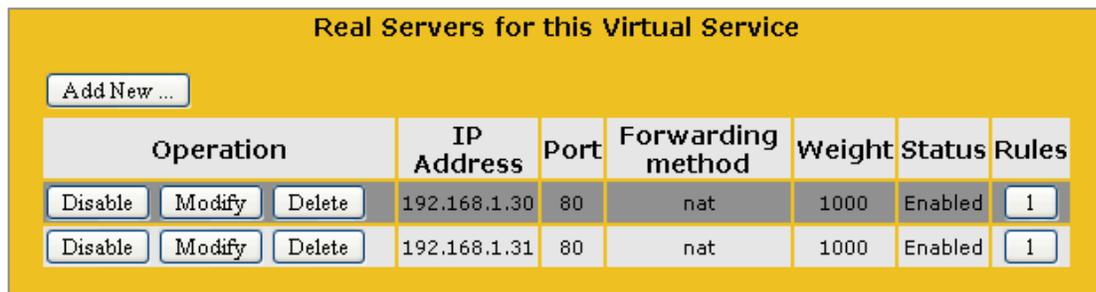
この Enable ボタンをクリックします。リアルサーバにアサインされているルール数を示すボタンを含む“Rule” 欄が、“Real Server” テーブルに追加されます。今回の場合、このボタンには“None”と表示されるはずです。リアルサーバにルールを追加するためには、このボタンをクリックします。例えば、もし、リアルサーバ 192.168.1.30 が全ての JPEG ファイルを持っているならば、” testrule “をこのリアルサーバへ追加すべきです。

Real Servers for this Virtual Service								
<input type="button" value="Add New ..."/>								
Operation			IP Address	Port	Forwarding method	Weight	Status	Rules
<input type="button" value="Disable"/>	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>	192.168.1.30	80	nat	1000	Enabled	<input type="button" value="None"/>
<input type="button" value="Disable"/>	<input type="button" value="Modify"/>	<input type="button" value="Delete"/>	192.168.1.31	80	nat	1000	Enabled	<input type="button" value="None"/>

“Rule Management” ページに、リアルサーバにアサインされているルールが表示され、プールダウン・リストには、既に定義されていてこのリアルサーバへアサインされていない他のルールが見えるはずですが、“default” ルールは、そのリストの中に必ず存在し、どのルールにもマッチしないリクエストをハンドルします。“testrule” を選択し、“Add” ボタンをクリックします。“testrule” がリストに加えられたのが見えるはずですが。バーチャルサービスの属性ページへ帰るためには、左上の“<-Back>” ボタンをクリックします。全てのリアルサーバへルールをアサインするプロセスを繰り返します。特定のルールが必要ないリアルサーバへは、“default” ルールをアサインしなくてはなりません。そうしないと、そのリアルサーバへは何のリクエストも分配されずに、使われなくなります。



コンテンツスイッチは、このバーチャルサービスで有効になりました。バーチャルサービステーブルに戻るには、左上の“Virtual Service” サブメニュー下の“View/Modify Existing” をクリックします。



## ヘッダー・モディフィケーション・ルール

### Add Header

HTTP リクエスト内に新しいヘッダーを挿入するためのルールです。

新しいルールを作成するルール作成ページを開くために、“Create New...” ボタンをクリックします。“CreateRule” 画面が表示されますので、“Rule Type” に‘Add Header’ を選択します。

“Rule Name” フィールドに、識別用のルール名を入力します。この例では、ルール名を“addrule” とします。次に、“Header Field to be Added” に挿入するヘッダー名“test”を入力します。そしてそのヘッダー値として‘10’を“Value of Header Field to be Added”に入力し、“Create Rule” をクリックします。

Rule Name	<input type="text" value="addrule"/>
Rule Type	<input type="text" value="Add Header"/>
Header Field to be Added	<input type="text" value="addrule"/>
Value of Header Field to be Added	<input type="text" value="10"/>

### Delete Header

HTTP リクエスト内の特定ヘッダーをサーチして、そのヘッダーを削除して RS へ転送するためのルールです。

新しいルールを作成するルール作成ページを開くために、“Create New...” ボタンをクリックします。“Create Rule” 画面が表示されますので、“Rule Type” に ‘Delete Header’ を選択します。

“Rule Name” フィールドに、識別用のルール名を入力します。この例では、ルール名を “deleterule” とします。次に、“Header Field to be Deleted” に削除されるヘッダー名 “test” を入力し、“Create Rule” をクリックします。

Rule Name	<input type="text" value="deleterule"/>
Rule Type	<input type="text" value="Delete Header"/>
Header Field to be Deleted	<input type="text" value="test"/>

### Replace Header

HTTP リクエスト内の特定ヘッダーをサーチして、そのヘッダーの値を変更して RS へ転送するためのルールです。新しいルールを作成するルール作成ページを開くために、“Create New...” ボタンをクリックします。“CreateRule” 画面が表示されますので、“Rule Type” に ‘Replace Header’ を選択します。

“Rule Name” フィールドに、識別用のルール名を入力します。この例では、ルール名を “replacerule” とします。次に、“Header Field” に値を変更するヘッダー名 ‘test’ を入力します。マッチする値 ‘10’ を入力し、変更する値 ‘20’ を “Value of Header Field to be replaced” に入力し、“Create Rule” をクリックします。

Rule Name	<input type="text" value="replacerule"/>
Rule Type	<input type="text" value="Replace Header"/>
Header Field	<input type="text" value="test"/>
Match String	<input type="text" value="10"/>
Value of Header Field to be replaced	<input type="text" value="20"/>

### Modify URL

HTTP リクエストの URL を変更して RS へ転送するためのルールです。新しいルールを作成するルール作成ページを開くために、“Create New...” ボタンをクリックします。

“CreateRule” 画面が表示されますので、“Rule Type” に ‘Modify URL’ を選択します。この例では、‘http://www.kemptechnologies.com’ を ‘http://www.yourcompany.com’ に変更するルールを作成します。

“Rule Name” フィールドに、識別用のルール名を入力します。この例では、ルール名を “replaceurl” とします。次に、“Match String” に変更の対象となる URL 内の文字列 ‘kemptechnologies’ を入力します。そして、‘yourcompany’ を “Modified URL” に入力し、“Create Rule” をクリックします。

Rule Name	<input type="text" value="replaceurl"/>
Rule Type	<input type="text" value="Modify URL"/>
Match String	<input type="text" value="kemptechnologies"/>
Modified URL	<input type="text" value="yourcompany"/>

これらのルールをVSに展開する方法は、上記のコンテンツ・マッチング・ルールで説明している方法と同じです。

## 4 SSLアクセラレーション

このセクションは、どのようにして SSL アクセラレーションが利用可能なバーチャルサービスの作成を行うかを説明します。

SSL アクセラレーションは、SSL 処理をリアルサーバからロードマスターへ移行します。この機能を使用することで、リアルサーバ毎に必要としていた SSL 証明書のインストールはバーチャルサービスに一回だけインストールするのみで済みます。

**注意：**SSL アクセラレーションを有効にすると、ロードマスターからリアルサーバへの通信は暗号化されません。

最初に、前述のセッションを参考にして新しいバーチャルサービスをポート 443 (HTTPS) で作成します。パーシステンシーには SSL セッション ID 以外のオプションを推奨します。理由は、最近のブラウザが短い時間内にセッション ID を変更する為にパーシステンシーが正常に機能しないためです。リアルサーバも上記に従い追加します。そして、SSL アクセラレーション機能を有効にするために、“SSL Acceleration” にチェックマークを入れます。



もし、未だバーチャルサービスに SSL 証明書がインストールされていない場合は、ロードマスターが持っている証明書が仮にインストールされるメッセージが表示されます。



SSL アクセラレーションを有効にした場合、下記 2 点について注意してください。

1. このバーチャルサービスにアサインされるリアルサーバは、ポート番号 80 をデフォルトで使用するよう設定されます。
2. リアルサーバへのサービスチェックは、一般的な場合の HTTPS ではなく HTTP が使われるよう設定されます。

## 5 マイクロソフト・ターミナル・サービス負荷分散

マイクロソフト・ターミナル・サーバの分散用バーチャルサービスのセッティングは、他のサービス用バーチャルサービスのセッティング方法と似ています。ロードマスターは、バーチャルサービスのポート番号を基にバーチャルサービスのタイプを検出します。

**Please Specify the Parameters for the Virtual Service.**

Virtual Address	<input type="text" value="192.168.1.200"/>
Port	<input type="text" value="3389"/>
Protocol	<input type="text" value="tcp"/>

ポート番号3389を入力すると、ロードマスターは自動的にサービスタイプとしてリモートターミナルを選択します。

バーチャルサービスに、ポート番号80、8080、もしくは443を指定すると、HTTP/HTTPS サービスを選択します。もし、ポート番号3389を指定すると、ターミナルサービスを選択します。もし、ロードマスターで自動認識しないポート番号が指定された場合、サービスは “一般 (Generic) ” が選択されます。

**Properties for 192.168.1.200:3389 - Operating at Layer 7**

**Basic Properties**         

Activate or Deactivate Service	<input checked="" type="checkbox"/>
Service Type	Remote Terminal ▼
Port Range	3389- <input type="text"/> <input type="button" value="Set Range"/>
Extra Ports	<input type="text"/> <input type="button" value="Set Extra Ports"/>
L7 Transparency	<input checked="" type="checkbox"/>
Real Server Check Parameters	Remote Terminal Protocol ▼    Checked Port <input type="text"/> <input type="button" value="Set Check Port"/>
Service Nickname	<input type="text"/> <input type="button" value="Set Nickname"/>
Persistence Options	Mode: Terminal Service or Source IP ▼ Timeout: 6 Minutes ▼ Netmask: /32 ▼
Scheduling Method	round robin ▼
Idle Connection Timeout	0 <input type="text"/> <input type="button" value="Set Idle Timeout"/>
Use Address for SNAT	<input type="checkbox"/>

**Advanced Properties**

Not Available Server	<input type="text"/> <input type="button" value="Set Server Address"/>
Default Gateway	<input type="text"/> <input type="button" value="Set Default Address"/>

**Real Servers for this Virtual Service**

Operation	IP Address	Port	Forwarding method	Weight	Status
-----------	------------	------	-------------------	--------	--------

注意：サービスタイプは、選択オプションから手動で変更可能です。

この設定では、ロードマスターが複数のサーバ間でマイクロソフトのターミナルサービス用負荷分散を有効にします。最初の接続は、デフォルトのラウンドロビン、もしくは、最小接続、アダプティブなどの負荷分散方式に従って任意のサーバに割り振られます。

ユーザがログアウトをしないでセッションが切断された場合は、それまで接続されていたサーバへ再接続されることが望めます。これは、切断時にユーザが使用していたウィンドウとアプリケーションの画面に戻れるからです。

これが、バランサーを介してターミナルサービスを利用している時にパーシステンシーが必要になる理由です。パーシステンシーが正しく機能すると、ユーザが再接続してきた時にロードマスターは同じサーバにセッションを張ります。これは下記の3つの方法のうちの1つで行われます：

1. ターミナルサーバは、クライアント側が RDP バージョン 6.1 以降の Remote Desktop Connection を使用するならば、セッション・ディレクトリー (2003 Server) / セッションブローカ (2008 Server) / RD コネクションブローカ (2008 R2 Server) との併用が必要です。ロードマスターはセッション・ディレクトリー / セッションブローカ / RD コネクションブローカが正しいホストの選択決定を行うための“ルーティング・トークン”を使用します。ロードマスターで設定されているパーシステンシー用タイムアウト値はここでは無意味です。この方式では、セッション・ディレクトリーがタイムアウトを受け持ちます。  
**注：セッション・ディレクトリー設定の中の“IP アドレス・リダイレクト (ルーティング・トークン・リダイレクトにはオフ) (I)”のチェックマークは、はずさなければなりません。**
2. RDP6.0 もしくはそれ以前のバージョンをクライアントが使用するならば、セッション・ディレクトリーは、パーシステンシーに関する限りロードマスターではオプションです。デフォルトでは、ユーザ名 (ドメイン名 + ユーザ名の 9 文字のみ) を使用します。もし、クライアントが最初のリクエストでユーザ名とパスワード (図-7 参照) を入力したら、この情報はロードマスター内部に記憶されます。再接続時に、これらのフィールドに前の情報が存在する限り、ロードマスターは記憶したデータから該当するユーザ名を調べて、最初の接続と同じサーバへと再接続します。パーシステンス用タイムアウトは、この情報をロードマスターが記憶するタイムリミットとして使用されます。クライアントが、RDP 6.1 もしくはそれ以降のバージョンを使用するならば、セッション・ディレクトリー / セッションブローカ / RD コネクションブローカを使用しなければなりません。

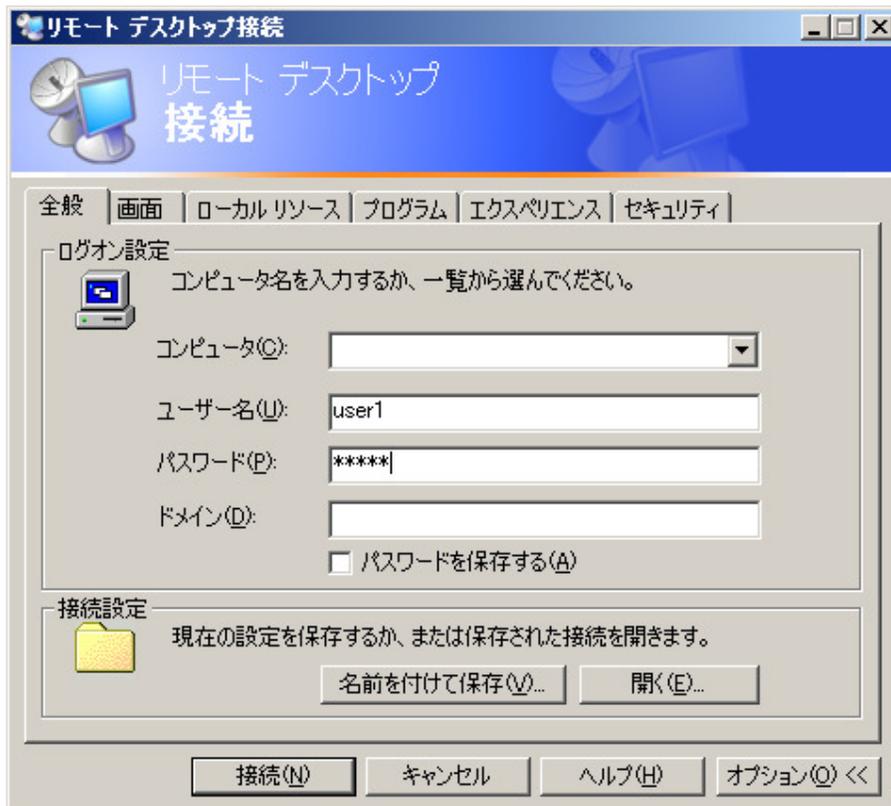


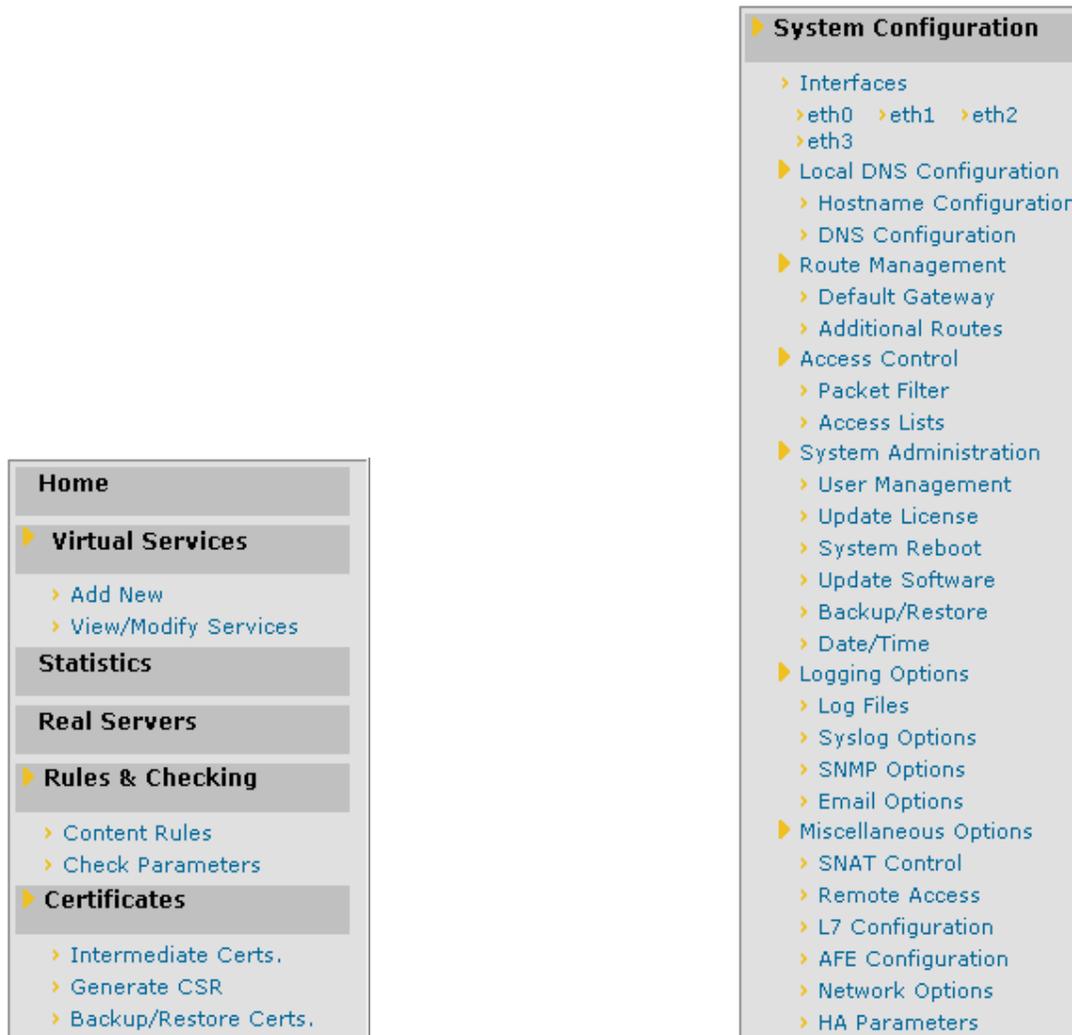
図-7 埋め込まれたユーザ名とパスワード

- もし “ターミナル・サービス、もしくはソース IP (Terminal-Service or source IP)” モードのパーシステンス方式を選択していて、上記の1)、及び2)のユーザ、もしくはトークン情報が得られなければ、ソース IP アドレスがパーシステンスに使用されます。

## C. 全メニューツリー

このセクションは、必要なパラメータを捜し出すのを助けるための、ロードマスターの WUI メニュー構成のクイック参照です。

画面左側上に、折りたたみ可能なサブメニューグループにより構成されたメインメニューがあります。



### 1 Home

システムの概要が表示されます。

### 2 Virtual Services (バーチャルサービス)

バーチャルサービスのリストアップ、各属性の表示、変更、及びサービスの作成、削除が行えます。

#### 2.1 Add New(追加)

新しいバーチャルサービス作成が行えます。バーチャル IP (VIP) アドレス、ポート番号をテキストフィールドに手書きで入力し、プロトコルタイプをプルダウンリストから選択します。

## 2.2 View/Modify Existing (Generic Service Type) “既存の表示/変更 (一般サービスタイプ)”

バーチャルサービスのテーブルが表示されます。“Delete”ボタンで該当バーチャルサービスの削除が行えます。”Modify”ボタンで属性ページを表示します。

### Duplicate VIP

同じ設定の VS を複製できます。VIP アドレスは、実際の複製を行う前に変更するように促されます。

### Change Address

既存 VS の IP アドレス (VIP) の変更が行えます。

### Activate or Deactivate Service (サービスの有効/無効)

このチェックボックスは、バーチャルサービスの有効、無効を指定できます。デフォルトは、有効です。

### Service Type (サービスタイプ)

アプリケーションのタイプにより、下記の 3 種類の中からプルダウンリストで選択可能です。

HTTP/HTTPS	ウェブサービス
Generic	ウェブサービス、ターミナルサービス以外
RemoteTerminal	ターミナルサービス

### Port Range

VS がサービスを受け付けるポート番号が複数で尚且つ連続番号であるならば、このパラメーターに最老番のポート番号を入力します。各ポート番号毎に VS を作成する手間を省くことが出来ます。

### Extra Ports

VS がサービスを受け付けるポート番号が複数で尚且つ非連続番号であるならば、このパラメーターに追加のポート番号を入力します。一つ以上入力する場合はスペースで区切って入力して下さい。各ポート番号毎に VS を作成する手間を省くことが出来ます。

### Force L7 (強制レイヤ 7)

モードを強制的にレイヤ 7 にします。クッキー・パーシステンシーや SSL アクセラレーションなどのレイヤ 7 オプションを有効にすると、このパラメータは現れなくなってしまう。

**L7 Transparency (レイヤ7透過モード)**

上記の“Force L7”、もしくはL7用パーシステンスオプション等を設定した場合のネットワーク透過モードの設定を行います。

**Allow Server Initiating Protocols (サーバ発信プロトコル許可)**

このパラメータは、“Service Type”として‘Generic’が選択され、尚且つVSがレイヤ7に設定された時のみ表示されます。

一般的に、RSはロードマスターとの間でTCP接続を確立した後、ロードマスター側からレイヤ7（アプリケーションレベル）プロトコルの発信を受けます、そして、RSはその発信に対して応答を返信します。HTTP/HTTPSは、その典型的なプロトコルです。ロードマスターは、TCP接続確立後、HTTPリクエストを送信しRSはページを返信します。しかしながら、SSH、FTP、SMTPなどのプロトコルでは、ロードマスターはVSがL7モードであるならばクライアントとのTCP接続が確立した後に、クライアントからのアプリケーションレイヤーの発信を受けますが、RSへの転送を行いません。この為にアプリケーションレイヤーでの応答をクライアントに返すことが出来ずにタイムアウトなってしまいます。このパラメータをオンにすることで、ロードマスターはクライアントからのアプリケーションレイヤーの発信をRSへ転送し、その応答をクライアントへ返信しますので、その後のデータのやり取りをスムーズに行わせることが出来ます。SMTP、SSH、IMAP4、MySQL用サービスの場合は、このプロトコルを指定する必要があります。これ以外のサービスの場合は、‘Other Server Initiating’を選択してください。L4ではこのパラメータは不要ですので表示されません。

**Real Server Check Protocol (リアルサーバ・チェック用プロトコル)**

このプールダウン・リストで、リアルサーバの死活チェックを行う方法を選択します。良く知られるサービスから、下位レベルのTCP/UDP、もしくはICMP方式まであります。ここで選択された方式で、リアルサーバの可用性がチェックされます。TCP/UDP方式は、単に接続を試みるだけのチェックを行います。

下記のヘルスチェック方式が指定出来ます。

ICMP Ping	Pingをリアルサーバへ送信します
HTTP Protocol	HTTP GET/HEAD リクエストを送信します
HTTPS Protocol	SSL通信でHTTP GET/HEADリクエストを送信します
TCP Connection Only	TCP接続を試みます
Mail (SMTP) Protocol	ポート25 (又は設定ポート) にTCP接続を試みます
Network News (NNTP) Protocol	ポート119 (又は設定ポート) にTCP接続を試みます
File Transfer (FTP) Protocol	ポート21 (又は設定ポート) にTCP接続を試みます
Telnet Protocol	ポート23 (又は設定ポート) にTCP接続を試みます
Mailbox (POP3) Protocol	ポート110 (又は設定ポート) にTCP接続を試みます
Mailbox (IMAP) Protocol	ポート143 (又は設定ポート) にTCP接続を試みます
Remote Terminal Protocol	ポート3389にRDP接続を試みます
None	ヘルスチェックを行いません。

HTTP/HTTPSを指定した場合は、そのポート番号を“Checked Port”に指定して、RSに設定したポート以外に変更することが可能です。又、デフォルトページ以外へのヘルスチェッ

クを行わせる場合は、‘URL’欄にそのURLを指定してください。デフォルトページを持たない場合、存在するページを‘URL’欄に指定しなければ、VSがアップ状態になりません。ウェブサーバーが、Host名を要求するHTTP/1.1バージョンでは“Use HTTP/1.1”をオンにして、Host名を指定する必要があります。又、デフォルトのヘルスチェックでは、通信するデータを最小限にするためにHTTP HEADモードでリクエストを出しますが、リプライ内の特定文字列をサーバの状態監視に使用するならば、“HTTP Method”を‘GET’モードに変更し、“Reply 200 Patern”欄にその文字列を指定してください。

### **URL (ヘルスチェック用URL)**

ロードマスターの、ウェブサーバへのヘルスチェックをデフォルトのページではなく、このパラメータで指定したURLに対して行います。

### **Use HTTP/1.1**

ウェブサーバのヘルスチェックで、ホスト名を指定できるHTTP1.1プロトコルを使用します。このパラメータをオンにすると“Host”フィールドが現れますので、ホスト名を入力します。

### **HTTP Healthcheck Method (HTTPヘルスチェック方法)**

HTTPプロトコルでのヘルスチェックは、デフォルトではHTTP HEADリクエストで行われます。これをHTTP GETに変えて、レスポンスの中身をチェックする場合はこのプルダウンリストを使って変更します。GETを選択すると、“HTTP Reply 200 Pattern”テキストフィールドが追加されます。

### **HTTP Reply 200 Pattern (HTTPレスポンス200のパターン)**

HTTP GETリクエストのレスポンスとして2xxが帰ってきた場合、そのコンテンツに含まれる特定のパターン文により、サーバのサービスチェックを行うことができます。パターン文は、このフィールドにレギュラー表現で入力します。

### **Service Nickname (サービス名)**

このテキストフィールドでは、バーチャルサービスのニックネームの設定、変更が行えます。

### **Persistence Options (パーシステンス・オプション)**

このパラメータでは、対応するバーチャルサービスのパーシステンス方式の選択が可能です。又、タイムアウト時間の設定やクッキー名の入力も行えます。

もし、パーシステンスが有効になったら、クライアントの接続が特定のリアルサーバへ行われるように維持されます。言い換えると、同じクライアントは、同じリアルサーバへと接続されます。タイムアウト値は、ロードマスターがどれぐらいこの特定接続を記憶しておくかを指定するものです。

パーシステンスの選択は、プルダウン・リストの下記方式から行います。

**Source IP Address (ソース IP アドレス)**

クライアントからのリクエストにあるソース IP アドレスが、このパーシステンス方式のキーとして使用されます。ネットマスクは、いかにロードマスターが、クライアントの環境に合わせてパーシステンスを行うかの決定をします。例えば、

ネットマスクが 255.255.255.25 (デフォルト) に設定されていると、個々の IP アドレス全てが、正当なパーシステンス用判断材料としての資格を得ます。よって、IP アドレス 200.190.125.67 が接続されると、そのアドレスが特定サーバとの接続のために記憶されます。そして、そのクライアントのセッションが終わり、切断されます。少し経った後で、そのクライアントが新しいセッションを開始した時、IP アドレスが同じであればその前と同じサーバへと接続されますが、200.190.125.44 のような別の IP アドレスがアサインされていたとすると、以前と同じリアルサーバへの接続は保証されません。

しかしながら、この場合、ネットマスクが 255.255.255.0 とセットされていたら、200.190.125.X のアドレスが 1 つのグループとして見なされるので、同じリアルサーバへと接続されます。この新しい接続は、前回切断されたときから測ってタイムアウト時間内である必要があります。

**Scheduling method (負荷分散方式)**

このパラメータは、ロードバランサーが特定のサービスのためにリアルサーバを選択する方式を指定し、負荷のリアルサーバへの分散を可能にします。下記の分散方式が選択できます。

**Round Robin (ラウンドロビン)**

ラウンドロビンは、最初のセッションをリアルサーバ 1 へ、2 番目をリアルサーバ 2 へとという様に、新しいセッションを順番にリアルサーバへアサインします。この方式では、不可を特定サーバに偏らせることは出来ません。

**Weighted Round Robin (重み付けラウンドロビン)**

この方式は、新しいセッションがどのリアルサーバにアサインされるべきか、リアルサーバの重みによって決定されます。高い重みを持つリアルサーバほど、その重みに比例して多い接続を引き受けさせられます。

**Least Connection (最小接続)**

この方式では、現状で一番接続数が少ないリアルサーバが、新しいセッションにアサインされます。

**Weighted Least Connection (重み付け最小接続)**

最小接続と同じですが、重みをバイアスにして計算した結果でリアルサーバをアサインします。

### **Resources Base (Adaptive) (アダプティブ)**

アダプティブ分配方式は、リアルサーバの実際の負荷を定期的にモニターしてそのレシオに基づいてリアルサーバをアサインします。結果的に非常にバランスの取れた配分が出来ます。詳細は、グローバル設定のセクションを参照ください。

### **Fixed Weighting (固定重み)**

優先的に1つのサーバをいつもアサインします。その優先サーバがダウンした場合は、次優先順位のサーバをアサインします。優先順位は、重みの値が大きいほど高くなります。

### **Idle Connection Timeout (アイドル・コネクション・タイムアウト)**

システムの持っているアイドル・コネクション・タイムアウトを共用したくない場合は、ここにこの VS 特有のタイムアウト値を設定します。

### **Use Address for SNAT**

2アーム、もしくはマルチアーム構成で RS より外部ネットワークへ接続する場合、システムで設定してあるデフォルトゲートウェイの属するイーサポートアドレスをソース IP アドレスとして使用しますが、VIP アドレスを使用したい場合はこのパラメータをオンにします。

### **SSL Properties (SSL属性)**

#### **SSL Acceleration (SSL アクセラレーション)**

このオプションは、バーチャルサービスを SSL アクセラレーションする時に “Enabled” チェックボックスをオンにします。SSL アクセラレーションについては、B 章のファーストトラックを参照ください。もし、バーチャルサービスに証明書がインストールされていない場合は、インストールを促すメッセージが現れます。そして、“Enable” の横に、“Reversed” という新しいチェックボックスが現れます。又、“Certificate” と “Rewrite” の新しい欄が追加されます。

#### **Reversed (リバース SSL)**

このオプションは、HTTP 用バーチャルサービスに入ってくる HTTP プロトコルを HTTPS に変換します。よってリアルサーバとの通信は SSL 通信となり、リアルサーバには SSL 証明書のインストールが必要です。SSL 用バーチャルサービスを一旦ロードマスターで終端した後、このリバース SSL オプションを持つバーチャルサービスと連結接続することで、クライアントからリアルサーバまで全てが SSL 通信となります。この方式は、全通信が SSL でもクッキーなどの L7 パーシステンスオプションを使用したい場合に有効です。この場合の

SSL アクセラレーション用バーチャルサービスは、リアルサーバとしてダミーの IP アドレスを使用し、ダミー IP アドレスをこのリーバース SSL 用バーチャルサービスの VIP として使用します。

### **Certificates (証明書)**

“Add New”ボタンを押すことで、新しい証明書をインストール出来ます。コピー&ペーストで、SSL 証明書とプライベートキーをインストールするページに移ります。証明書によっては、インターミディエート証明書を必要とするものがあります。インターミディエート証明書をインストールする場合は、” Add 3<sup>rd</sup> Party Cert “ボタンをクリックし、証明書を貼り付けるページにコピー&ペーストを行います。

SSL 証明書のインストールは、各バーチャルサービスで必要ですが、インターミディエート証明書は、同じ CA 用ならシステムに一回インストールするだけで、全てのバーチャルサービスでシェアされます。

### **Rewrite Rule (プロトコル変更)**

リアルサーバからのリダイレクトを行う URL ロケーションの、プロトコル (HTTP/HTTPS) を一つに統一する必要がある場合は、このプルダウンリストで選択します。

### **Advanced Properties (アドバンス属性)**

#### **Default Gateway (デフォルト G/W)**

各バーチャルサービスの特定デフォルト G/W を設定出来ます。ここで何も入力がない場合は、システムの設定 (System Configuration サブメニューの Route Management) が利用されます。

## **2.3 View/Modify Existing (HTTP/HTTPS Service Type) “既存の表示/変更 (HTTP/HTTPSサービスタイプ)”**

上記の Generic Service Type に無い HTTP/HTTPS バーチャルサービス用パラメータです。

### **Persistency Options**

#### **Super HTTP**

スーパーHTTP オプションは、HTTP リクエストの中の “User-Agent” フィールドをハッシュ化した値を使用します。HTTP リクエスト内に同じ値が含まれているならば、前回接続したリアルサーバへと接続します。もし、HTTP リクエストの中に ‘MSRPC’ という MS Exchange サーバで使用する文字列が含まれていた場合は、“Autorization” フィールドも含めてハッシュ化します。このオプションは、MS Exchange サーバの CAS サービス用バーチャルサービスを作成する時に推奨します。

#### **URL Hash (URL ハッシュ)**

同じ URL へのリクエストは、同じサーバへと配分されます。

### **Server Cookie (サーバクッキー)**

リクエストの HTTP ヘッダー内に同じクッキーが存在すると、前回と同じサーバへとリクエストを分配します。このクッキーはサーバによって作られる必要があります。

### **Server Cooki or Source IP (サーバクッキー、もしくはソース IP)**

リクエストの HTTP ヘッダー内に同じクッキー (リアルサーバが作成した) が存在すると、前回と同じサーバへとリクエストを分配します。クッキーが存在しない場合には、ソース IP アドレスを使ってパーシステンスを試みます。

### **Active Cookie (アクティブクッキー)**

ロードマスターが独自のクッキーを作成します。それと同じクッキーがリクエストに含まれていると、ロードマスターはそのリクエストを前回と同じリアルサーバへと導きます。

### **Active Cookie or Source IP (アクティブクッキー、もしくはソース IP)**

リクエストの HTTP ヘッダー内に同じクッキー (ロードマスターが作成した) が存在すると、前回と同じサーバへとリクエストを配分します。クッキーが存在しない場合には、ソース IP アドレスを使ってパーシステンスを試みます。

### **Hash All Cookie (ハッシュ全クッキー)**

リクエストの HTTP ヘッダー内に同じクッキーセット (サーバが作成した) が存在すると、前回と同じサーバへとリクエストを配分します。

### **Hash All Cookie or Source IP (ハッシュ全クッキー、もしくはソース IP)**

リクエストの HTTP ヘッダー内に同じクッキーセット (サーバが作成した) が存在すると、前回と同じサーバへとリクエストを配分します。クッキーが存在しない場合には、ソース IP アドレスを使ってパーシステンスを試みます。

### **HTTP Host Header (HTTP ホストヘッダー)**

同じホストへのリクエストは、前回と同じサーバへと配分されます。

### **Hash of HTTP Query Item (HTTP クエリ項目ハッシュ)**

同じクエリ項目を含むリクエストは、前回と同じサーバへと配分されます。

### **SSL Session ID (SSL セッション ID)**

SSL セッション ID が同じならば、前回と同じサーバへと導きます。

注意：メジャーなブラウザは、一定間隔でこの ID を入れ替えてしまうので、一般の SSL 通信用には使用できません。

### **Selected Header (指定ヘッダー)**

特定の HTTP ヘッダーを指定して、そのヘッダーによるパーシステンシーを行います。ヘッダーの値がマッチングしたら前回と同じ RS へ接続します。

### **Content switching (コンテンツスイッチ)**

このバーチャルサービスのルールベースのコンテンツスイッチ機能を有効にします。このパラメータをオンにした後に、該当するリアルサーバルールをアサインする必要があります。ルールは、事前に作成されている必要があり、各リアルサーバに追加された “Rules” 欄の “None” ボタンをクリックした後に現れるリストから選択します。ルール作成とコンテンツスイッチの設定方法についてはアプリケーションガイドを参照して下さい。

### **Rule Precedence**

コンテンツスイッチ用ルールの優先順位を設定します。このパラメータは、コンテンツスイッチ機能を有効にして RS にルールが適用されている場合のみ表示されます。このボタンをクリックすると、対応するバーチャルサービスにアサインされたルール全てがリストされず。各ルールの “Promote” ボタンをクリックすることで優先順位を上げることが出来ます。

### **HTTP Header Modifications**

VSに使用できるヘッダー・モディフィケーション・ルールを表示します。

### **Port Following (ポートフォロウイング)**

ポートフォロウイングは、HTTP/HTTPS から HTTPS (SSL) /HTTP 接続へスイッチする時に、同じリアルサーバへの接続維持 (パーシステンス) を提供します。ポートフォロウイングは、スイッチするサービスが HTTP/HTTPS サービスであり、HTTP サービスと HTTPS サービスが同じ IP アドレスを使用し、パーシステンシーや RS などの設定が同じである時のみ設定可能です。HTTP から HTTPS へパーシステンスを必要とするときは、この機能を HTTP 用バーチャルサービスで有効にし、HTTPS から HTTP へのパーシステンスが必要などときには、HTTPS 用バーチャルサービスでも有効にする必要があります。設定は、プルダウンリストから行い、同じリアルサーバを使っているバーチャルサービスを選択する必要があります。又、この機能を使うためには、L7 モードで、尚且つ両方のバーチャルサービスのパーシステンス方式と分散方式が同じ設定であることが要求されます。又、HTTPS 用バーチャルサービスは、パケットの中身を見られるように SSL アクセラレーションを有効にする必要があります。

### **Enable Caching (キャッシング有効化)**

キャッシュ機能が使用できるようにします。キャッシュされるファイルは下記の条件を満たしている必要があります。

HTTP GET で採取されたコンテンツで；

1. コンテンツのレンジをパラメタなどで指定していないもの。
2. アクセスの許可を必要としないもの。
3. GET に Query を含んでいないもの。（例：/cgi/fred?value）
4. ".shtml" もしくは ".php" の拡張子以外のもの。
5. RS からの応答が 200, 203, 300, 301, 410 のもの。
6. "Cache-control:" もしくは "pragma: no-cache" HTTP ヘッダーを含んでいないもの。
7. Modify (Date - LastModified) が 60 秒以上のもの。
8. "Expires"ヘッダーを含んでいる場合は、期限がきれていないもの。
9. ファイルのサイズが各 VS に割り当てられているキャッシュサイズの 50%を超えないもの。

キャッシュされたファイルは、期限が1時間としてマークされます。1時間が過ぎるとキャッシュから削除されます。RS が期限を指定している場合は、1時間以内の期限だけが有効となります。仮に RS でキャッシュ期限 (Expiry Date)指定が 30分だったとしたら、RS の期限が有効になります。90分と指定された場合は、RS の期限指定は無効となり、ロードマスターがマークする 60分が期限となります。

### Enable Compression (圧縮の有効化)

RS、及びクライアント間で送受するファイルを圧縮します。

### Detect Malicious Requests (IDS 機能の追加)

クライアントからの悪意のある HTTP リクエスト、ポストパケットを検出します。検出には米国 Snort 社の Snort を使用しています。悪意のあるパケットは Reject、もしくは Drop を指定できます。又、これらのパケットの検出をログに出力する事も可能です。

### Add Header to Request (HTTP リクエストへのヘッダー追加)

クライアントからの HTTP リクエストにヘッダーを追加して RS へ転送することを可能とします。

### Not Available Server (緊急用サーバ)

もし、全てのリアルサーバが使用できなくなった時に、緊急用サーバで仮応答するときこのサーバをアサインします。指定できるのは IP アドレスのみです。

### Not Available Redirection Handling (リダイレクション)

リアルサーバより帰ってきたエラーにより、リダイレクトするロケーションを設定出来ます。HTTP リクエストを無条件に HTTPS にするには、“Error Code” に 302 を選択し、“Redirect URL” 欄に ‘ホスト名+ドメイン名+%s’ <例えば ‘www.kemptechnologies.com%s’ >と入力します。もしくは、ホスト名+ドメイン名を指定しないでクライアントからのものをそのまま使用する時は ‘%h%s’ と入力します。この場合は、リアルサーバのアサインは必要

ありません。当然、リダイレクト先のバーチャルサービスがなければなりません。URL の代わりに、バーチャルサービスの IP アドレスでも働きます。

**Error Code:** リアルサーバが利用不可能な場合、ロードマスターは HTTP エラーコードに従って、接続を終端することが出来ます。

**Redirect URL:** リアルサーバが利用不可能な場合、エラーをクライアントに返信すると共にここで設定した URL へのリダイレクトを指定出来ます。

### Default Gateway (VS 専用デフォルトゲートウェイ)

システムに設定されているデフォルトゲートウェイではなく、他のゲートウェイを使用しなければならない時には、ここにその IP アドレスを指定できます。

## 2.4 View/Modify Existing (Remote Terminal Service Type) “既存の表示／変更 (リモートターミナルサービスタイプ)”

リモートターミナル特有のバーチャルサービス用パラメータです。

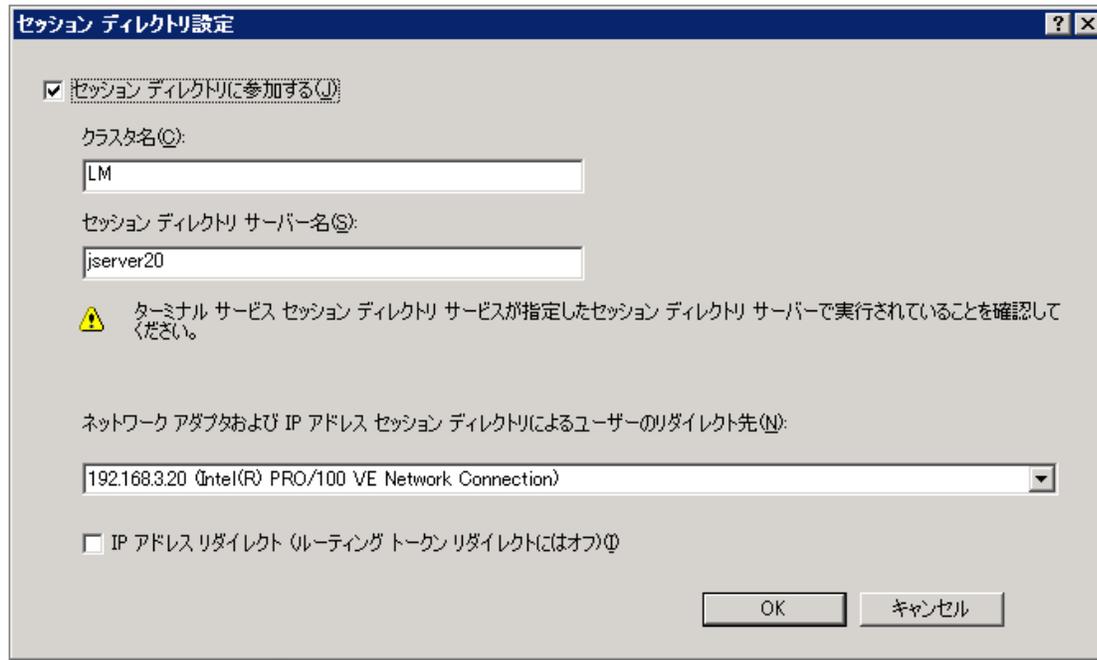
### Real Server Check Protocol

ターミナルサービス用バーチャルサービスでは、リアルサーバのチェック用として ICMP、TCP、もしくは RDP のオプションがあります。RDP (Remote Terminal Protocol) オプションでは、ロードマスターはポート番号 3389 に TCP 接続を行います。そして、ターミナルサーバに対して a1110 コード (接続リクエスト) を送信します。もし、サーバが a1101 コードを返信してきたならば、接続を閉じサーバをアクティブとします。もし、サーバが設定してあるタイムアウト時間 x リトライ回数以内に返信して来ない、もしくは違うコードでの返信をしてきたならば、サーバは使用不可能と見なします。

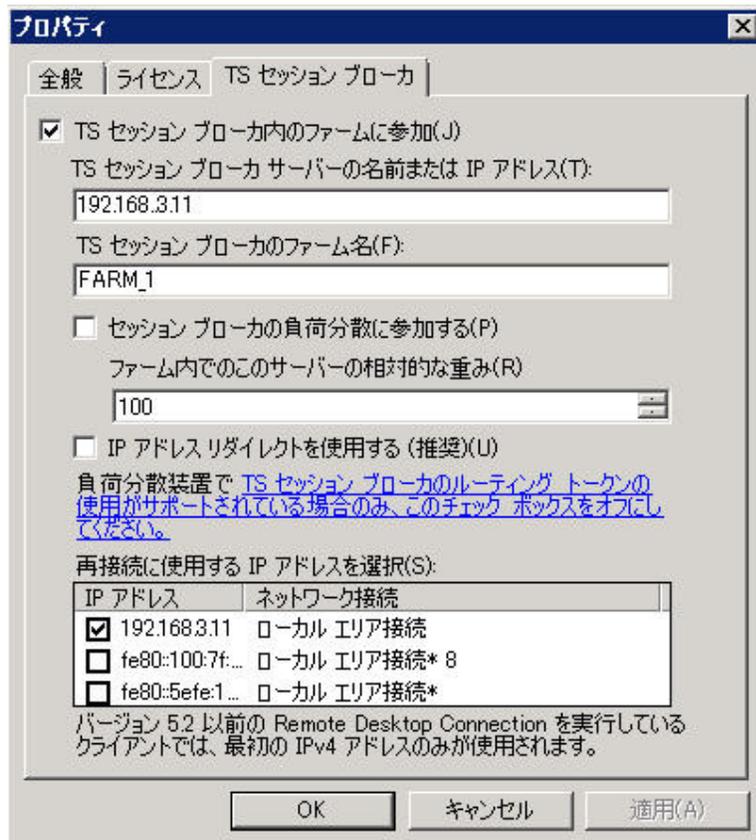
### Persistence Option

もしターミナルサービスが、セッションディレクトリ (2003 サーバ) / TS セッションブローカー (2008 サーバ) / RD コネクションブローカー (2008R2 サーバ) を使用しているならば、ロードマスターは接続するホストへのセッション維持のためにそれらのサーバからユーザ ID として発行される “Routing Token” を使用します。この場合は、ロードマスターのセッション維持のタイムアウト用パラメータは無効です。パーシステンシーのタイムアウトは、セッションディレクトリサーバ (2003 サーバ) / TS セッションブローカー (2008 サーバ) / RD コネクションブローカー (2008R2 サーバ) 側で設定する必要があります。

**注:** 2003 サーバの場合、セッションディレクトリ設定の “IP アドレスリダイレクト (ルーティングトークンリダイレクトにはオフ) (I)” のチェックマークは、外さなければなりません。



2008 サーバの場合は、TS セッションブローカの設定時に“IP アドレスリダイレクトを使用する (推奨)”のチェックマークを外す必要があります。



2008R2 サーバの場合は、Remote Desktop Session Host Configuration の RS Connection Broker の Properties 内で ‘Token redirection only’ を選択します。デフォルトは、Use IP address redirection (recommended) になっていますので、プルダウンメニューより変更してください。

リモートデスクトップ接続等のクライアントが、RDP バージョン 6. 1 もしくはそれ以降のバージョンを使用していて、パーシステンシーが必要ならばセッションディレクトリ/セッションブローカ/RD コネクションブローカとの併用を行わなければなりません。RDP 6. 0 もしくはそれ以前のバージョンを使用しているならば、セッションディレクトリ/セッションブローカ/RD コネクションブローカの使用はオプションとなります。このバージョンを使用しているクライアントが、リモートデスクトップ接続のユーザ名とパスワード欄に特定情報を入力している状態でイニシャルリクエストを発するならば、ロードマスターはドメイン+ユーザ名の最大 9 文字の情報をセーブします。再接続時に、この欄に同じ情報を使用する限りは、ロードマスターは前回のターミナルサーバ接続情報を基に同じサーバへの接続を行います。この場合は、パーシステンシーのタイムアウトはロードマスターに設定してある値が有効となります。

注：RDP 6. 0、もしくはそれ以前のバージョンでのユーザ名は、ドメイン名を含めて 9 文字までが識別可能です。もし長いドメイン名を使用している場合で、ユーザ名にドメイン名を含ませる必要があるならば、ユーザ名の識別が出来ない場合が出てきます。これが原因で負荷分散が偏る場合には、セッションディレクトリ (2003 サーバ) や、セッションブローカ (2008 サーバ)、RD コネクションブローカ (2008R2 サーバ) の使用をお願いします。又、RDP 6. 1、もしくはそれ以降のバージョンでも、セッションディレクトリ (2003 サーバ) や、セッションブローカ (2008 サーバ)、RD コネクションブローカ (2008R2 サーバ) の使用をお願いします。

### **Terminal Service (RDP ユーザ)**

MS のターミナルサーバ用 RDP プロトコルで使用されるユーザ情報、もしくはセッションディレクトリ/セッションブローカが発生させるトークンによるセッション維持を可能にします。同じユーザからの接続リクエストは、前回と同じターミナルサーバへと配信されます。

注：このパラメータは、“Service Type” を ‘Remote Terminal ‘ に設定しないと表示されません。

### **Terminal Service or Source IP (RDP ユーザ、もしくはソース IP アドレス)**

MS のターミナルサーバ用 RDP プロトコルで使用されるユーザ情報、セッションディレクトリ/セッションブローカが発生させるトークン、もしくはソース IP アドレスによるセッション維持を可能にします。RDP のユーザ情報、もしくはセッションディレクトリ/セッションブローカが発生させるトークンが取得できない場合は、TCP 接続のソース IP アドレスをセッション維持に使用します。

注：このパラメータは、“Service Type” を ‘Remote Terminal ‘ に設定しないと表示されません。

## **2.5 Real Server for this Virtual Service (リアルサーバのアサイン)**

このセクションは、バーチャルサービスにアサインされているリアルサーバをリストアップします。アサインされていない場合は、追加、又、アサインされている場合は、リアルサーバ属性の要約が表示され、そしてリアルサーバの追加、削除、及び属性変更が可能です。コンテンツスイッチが有効になっていると、各リアルサーバへのルール of の追加、削除もこのセクションで行えます。

### Add New (リアルサーバの追加)

ここで新しいリアルサーバの下記属性をセットします。

**Real Server Address:** リアルサーバ IP アドレス (この属性は編集不可能です)。

**Port:** リアルサーバのフォワーディング・ポートを設定します。編集可能です。

**Forwarding method :** DSR (ダイレクト・サーバ・リターン) の時には “Route” を選び、それ以外は “NAT” のままとします。

**Weight:** サーバの重みを設定します。これは重み付け負荷分散方式 (Weighted Round Robin, Weighted Least Connection 及び Adaptive) で使用されます。デフォルトの初期設定値は 1000 で、最高 65535、最低 1 までの値への変更が可能です。これには、リアルサーバの処理スピードに比例した値をアサインすると良い基準となります。例えば、サーバ 2 が、サーバ 1 と比較して 4 倍の CPU 性能だとすると、サーバ 2 を 4000 とし、サーバ 1 はデフォルト値の 1000 のままとします。

**Allow Remote Addresses :** イーサポートにアサインされたローカルサブネット以外のリモートネットワーク上の RS を追加する時にチェックマークをオンにします。但し非透過モードの VS のみでしか稼動しません。透過モードに設定すると、HTTP リクエストパケットのソース IP アドレスがクライアントの IP アドレスとなり、返信パケットがロードマスターへ帰らず直接クライアントへ返信されのがその理由です。

注：この機能を使用するためには “System Administration” サブメニュー下の “Miscellaneous Options” の “Network Options” 内の “Enable Non-Local Real Servers” を ‘Yes’ にしなければなりません。そして、VS を L7 (Force L7 をオン) で Non-Transparency (L7 Transparency をオフ) モードにしなければこのパラメータは表示されません。

### Modify (リアルサーバ属性変更)

リアルサーバの Port, Forwarding Method、及び Weight 値の変更が可能です。

### Disable (一次休止)

リアルサーバを一時的に利用不可とします。パーシステンスのタイムアウトしていないリクエストは接続されます。

### Delete (削除)

リアルサーバをこのバーチャルサービスより削除します。

### 3 Statistics (統計情報)

この統計セクションでは、ロードマスターのパフォーマンスに関連する情報を提供します。そして、15秒おきにリアルタイムの情報に更新します。これは、最上のパフォーマンスを与えるためにサーバファーム上の負荷分散をチューニングする時や、障害対応、及びエラーの検出にとっても役立ちます。更に、この機能は、バーチャルサービスとリアルサーバにまたがったパフォーマンス比較のために非常に貴重です。

#### 3.1 Global Metrics (システム統計)

##### *CPU activity* (CPU アクティビティ)

このグラフは、ロードマスターの以下のCPU使用率を表示します。

Use	ユーザモードでの処理で消費されるCPU使用率
System	システムモードでの処理で消費されるCPU使用率
Idle	空きのCPU使用率
I/O Waiting	I/O処理が完了するまで待っているために消費されるCPU使用率

**注意** : User + System + I/O Waiting + Idle = 100%

##### *Memory usage* (メモリー使用率)

この棒グラフは、ロードマスターのシステム上でのメモリーの使用率 (Used) と空き率 (Available) の総計を表わします。

##### *Network Activity* (ネットワーク・アクティビティ)

この棒グラフは、各インターフェースのネットワーク・スループットを示します。

#### 3.2 Real Server Metrics (リアルサーバ統計)

これらのグラフは、リアルサーバによってハンドルされている接続数、バイト数、もしくはパケット数 (画面右上の各対応ボタンを押すことで表示が切り替わる) を表示します。この値は、リアルサーバをアサインしている全バーチャルサービスの合計です。そして、装置全体に対する各リアルサーバの度合いを%欄に表わします。

#### 3.3 Virtual Service Metrics (バーチャルサーバ統計)

これらのグラフは、各バーチャルサービスの接続数、もしくはバイト数のトータル数を表示します。そして、各バーチャルサービスにアサインされているリアルサーバが、そのバーチャルサービス内でそのトータル数に対して、どれぐらいの度合いを占したかを%欄に表示します。

### 4 Real Servers (リアルサーバ)

バーチャルサービスにアサインされた、全てのリアルサーバのリストが表示されます。



? - 文字の1つのどれかにマッチ  
\* - ゼロ、もしくはそれ以上の桁のいずれの文字にもマッチ  
\$ - 行の最後の文字  
^ - 行の最初の文字  
[- セットのスタートで、]で終わるセットの中の一文字とマッチ  
^ - セットのスタートで、セット内にはない文字とマッチ  
\\ - 次の文字にエスケープ

### **Negation (逆転)**

マッチングの定義を否定します。例えば、“test”がPrefixでマッチするルールを作成したとすると、このNegationを使うことで“test”以外ならマッチすることになります。

### **Ignore Case (文字ケースの無視)**

大文字、小文字の区別をなくします。

### **Include Host in URL(ホスト名を含む)**

ホスト名を含んでURL文字列をサーチします。このパラメータがオフになっている場合はホスト名は省いてマッチング処理が行われます。

### **Include Query in URL (クエリを含む)**

URLのクエリ部分まで含めてルールのマッチングを行います。

## **5.2 Check Parameters (アダプティブ、ヘルスチェック用パラメータ)**

アダプティブ負荷分散とヘルスチェック用パラメータを設定します。

### **5.2.1 Adaptive Parameters (アダプティブ負荷分散方式用パラメータ)**

#### **Adaptive Interval(sec) (インターバル)**

アダプティブ負荷分散方式を使用するときの、ロードマスターがリアルサーバの負荷をチェックする周期時間(秒)を設定します。デフォルトは10秒で、最長60秒まで設定可能です。

#### **Adaptive URL (アダプティブURL)**

リアルサーバが、自身の負荷値を記録するURLロケーションを指定します。デフォルトは“/load”です。1つのバーチャルサービスにアサインされている全てのリアルサーバで同じロケーションである必要があります。

#### **Port (ポート)**

ロードマスターが、リアルサーバの負荷値をHTTP GETで採取する時のポート番号を指定します。デフォルトは80です。

#### **Min. Control Variable Value (%) (アダプティブ開始最低重み値)**

アダプティブが、リアルサーバの負荷値を基に重み付けを行う時の最小負荷値を設定します。この設定値より以下では、リアルサーバに設定してある静的重み値を使った重み付けラウンドロビン方式が使用されます。

### 5.2.2 Service Check Parameter (サービスチェック用パラメータ)

ヘルスチェック用パラメータの変更が行えます。

#### **Check Interval (sec) (チェック周期)**

ヘルスチェックの周期時間を変更できます。デフォルト値は9秒です。

#### **Connect Timeouts (sec) (接続タイムアウト)**

RS へのサービスチェックは2つのタイプがあります。サーバと接続を確立させるだけの L4 タイプ (例えば TCP 接続を指定した場合) と、そしてアプリケーションレイヤでアクセスしその応答を促すタイプです (例えば L7 の HTTP/HTTPS を指定した場合)。このタイムアウトは、L4 レイヤでは TCP 接続が確立されるまで、また L7 ではアプリケーションレイヤのアクセスが確立されるまでどれだけ待つかの設定です。デフォルトは4秒に設定してあります。

#### **Re-try Count (リトライ回数)**

これは、サーバのヘルスチェックでタイムアウトが発生した時にリトライする回数を指定します。デフォルト値は“2”で、それ以下の設定は出来ません。

## 6 Certificate (証明書)

### 6.1 Intermediate Certs. (インターミディエート証明書)

現在インストールされているインターミディエート証明書をリストアップします。新しいインターミディエート証明書のインストールを行うには、“Add New” ボタンをクリックし、現れたテキスト入力画面に証明書をコピー&ペーストします。この証明書は、CA 局毎に1回だけインストールします、全てのバーチャルサービスにインストールされたパブリック証明書は、インターミディエート証明書により各 CA のルート証明書までチェーン化されます。

### 6.2 Generate CSR (CSR作成)

SSL 証明書を CA 機関に申請する時に、ここで CSR とそのプライベートキーの作成を行うことが可能です。作成後は、必ず両方ともファイルにコピーして保存してください。ロードマスターは、作成後これらの情報を維持せず、メニュー切り替え時に破棄しますので注意してください。

### 6.3 Backup/Restore Certs. (証明書のバックアップ/リストア)

このセクションでは、SSL 証明書のバックアップとリストアが行えます。通常の設定ファイルのバックアップでは、SSL 証明書はバックアップされませんので、証明書のバックアップ

を行いたいときには、別途このメニューより行う必要があります。リストアを行う場合は、VS 設定ファイルのリストア後に、SSL 証明書のリストアを行います。

## 7 System Configuration (システム用設定)

### 7.1 Interfaces (インターフェース)

各イーサポートの設定確認と、変更、追加が可能です。設定を更新した場合、リブートが必要です。

#### 7.1.1 Network Interface X (ネットワークインターフェース)

<b>Interface Address</b> ( <i>xx.xx.xx.xx[/ss]</i> )	管理用ローカル IP アドレス/ネットマスク
<b>HA Shared IP address</b>	HA 構成時のシェアード IP アドレス
<b>HA Partner IP address</b>	HA 構成時のペアとなるユニットの IP アドレス
<b>Use for HA check</b>	HA 構成時でペアとなるユニットの状態チェックに使用する／しない
<b>Link Status</b>	手動で通信速度、通信モードを設定する場合、プルダウンリストより選択

**VLAN Configuration** VLAN タグを使用する時に VLAN ID の設定を行います。複数の VLAN タグを扱うことが出来る VLAN トランク (802.1Q) が可能です。設定の詳細はアプリケーションガイドを参照下さい。

**Interface Bonding** イーサネットポートを複数束ねるボンディング/チーミング (802.1AX, 802.3ad) の設定を行います。設定の詳細はアプリケーションガイドを参照下さい。

#### 7.1.2 Subnets on this Interface (インターフェースのサブネット)

イントラネット内の他のサブネットにリアルサーバが存在するとき、そのネットワークをここで設定します。

**Subnet :** サブネット (例えば 10.1.0.0/8, 192.168.2.0/24)  
**Local Address:** このサブネットの管理用ローカルアドレスで RS はこのアドレスをデフォルトゲートウェイとして使用しなければなりません。

### 7.2 Local DNS Configuration (ローカルDNS設定)

#### 7.2.1 Hostname Configuration (ホスト名設定)

ロードマスターにホスト名前をアサインします。

#### 7.2.2 DNS Configuration (DNS設定)

### **DNS NameServer (IP Address) (DNS サーバ)**

ロードマスターが使用する DNS サーバを、最高 3 台まで設定出来ます。

### **DNS Search Domains (DNS サーチ ドメイン)**

ロードマスターがホストをサーチする場合のドメインを、最高 6 つまで設定出来ます。

## **7.3 Route Management (ルート管理)**

このオプションは、システムのデフォルト・ゲートウェイと静的ルーティングを設定出来ます。

ロードマスターは、インターネット/リモートネットワークへの通信を行うためにデフォルト・ゲートウェイを設定する必要があります。そして、更なるルーティングが追加できます。追加するルーティングは静的なもので、ゲートウェイは、ロードマスターと同じサブネットになければなりません。

## **7.4 Access Control (アクセス管理)**

### **7.4.1 Packet Filter (パケットフィルター)**

このトグルオプションは、パケットのフィルターを有効 [Enable] / 無効 [Disable] にすることが出来ます。もし、フィルターが有効になっていなければ、2 アーム構成ではロードマスターは単に IP パケットをファーム側にフォワードします。フィルターが有効になっていれば、バーチャルサービスのアドレスだけが処理され、その他のアドレスはブロックされます。1 アームではこの機能は働きません。

### **Rejection method (リジェクト方法)**

アクセスリストでブロック (遮断) されているホストより接続リクエストを受けた時、そのリクエストはロードマスターでは通常無視 (Dropped) されます。しかし、設定を “Reject” に変更することで、ICMP リジェクト・パケットを返すことが出来ます。セキュリティのためには、“Drop” の設定にしておく方を推奨します。

### **7.4.2 Access Lists (アクセス管理リスト)**

ロードマスターは、“ブラックリスト” アクセス管理システムをサポートします。

### **Blacklist (ブラックリスト)**

“ブラックリスト” に入力されたいずれのホスト、ネットワークからの、ロードマスターが提供するバーチャルサービスへのアクセスがブロックされます。

“Access List” は、“Packet Filter” が有効になっている時のみ有効です。

### **Whitelist (ホワイトリスト)**

“ホワイトリスト”は、“ブラックリスト”で規制されたネットワークの中の特定ホスト、ネットワークからの、ロードマスターが提供するバーチャルサービスへのアクセスを許します。

## 7.5 System Administration (システム管理)

### 7.5.1 User Management (ユーザ管理)

#### Change Password (パスワード変更)

システム管理用ユーザ “bal “のパスワード変更をします。現在のパスワードと新しいパスワードの入力が必要です。パスワードは、半角文字で 8 文字から 16 文字までの範囲で指定できます。使用できる文字は英字 (大文字、小文字)、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めて下さい。

#### パスワード指定例

- ・英小文字のみ : 9 文字以上    `abcdefghi`
- ・英小文字と数字の混在 : 8 文字以上    `1abcdefg`
- ・英大文字と英小文の混在 : 8 文字以上    `Abcdefgh`
- ・英小文字、記号、数字の混在 : 8 文字以上    `ab!12345`
- ・数字のみ : 13 文字以上    `0123456789012`

#### Other Users (他管理ユーザの作成)

違う権利を持つ管理ユーザを作成できます。又、デフォルトの管理ユーザである ‘bal’ ユーザと同じ権限を持つユーザも作成できます。ユーザをロードマスターで管理しないで RADIUS サーバにて行うことも可能です。

### 7.5.2 Update License (ライセンスキーの更新)

システムのライセンスキーを更新します。評価用仮ライセンスを使用している場合は、ここで永久ライセンスに更新しなければ、システムが停止してしまいます。何時システムが停止するかは、この画面でライセンスの有効期限を確認することで分かります。

### 7.5.3 System Reboot (システムリブート)

システムのリブート、シャットダウンと、設定を工場出荷時のデフォルトへ戻せる “Reset To Factory Defaults” があります。

### 7.5.4 Update Software (ファームウェア更新)

ファームウェアの更新を行えます。パッチは、新しいファームウェアとしてリリースされるので、一旦ローカルディスクへダウンロードした後、ここにそのロケーションを指定します。“Update Machine” ボタンをクリックすると、ダウンロード、内容確認が行われ、インストールが行われますが、最後にリブートを要求されます。

## Restore Software (ファームウェア復旧)

ファームウェアが更新されると、必ず1つ前のファームウェアバージョンはシステム内にセーブされます。もし、そのファームウェアバージョンに戻したい場合は、“Restore Software” をクリックします。セーブできるファームウェアは1つだけです。

### 7.5.5 Backup/Restore (設定バックアップ/リストア)

設定ファイルのバックアップとリストアが行えます。“Create Backup File” をクリックし、セーブ先を指定します。

リストアは、“Choose” をクリックしセーブされている設定ファイルを指定して、右側の設定グループを選択し “Restore Configuration” をクリックします。全部の設定をリストアしたい場合は、両方のグループを選択します。

- LoadMaster Base Configuration : VS 関連以外の設定のみ (インターフェース、システム関連設定)
- VS Configuration Only: VS 関連の設定のみ

### 7.5.6 Date/Time (日付/時間)

時間、日付の設定が行えます。NTP ホストを指定することで、精度の高い時刻を保つことが可能です。HA 構成時で時間の設定がユニット間で異なると、正常な設定ファイルやログファイルの更新が出来なくなりますので、必ず有効な NTP ホストを設定し両方のユニットの時間が合うように留意ください。日本時間にするためには、“Set Time Zone” に ‘JST’ を選択します。

## 7.6 Logging Options (ログオプション)

### 7.6.1 Log Files (ログファイル)

システムブート時のメッセージ、警告メッセージ、システムメッセージ、ハートビート・メッセージを見ることが可能です。セーブ、転送したいときは、“Download Log Files”をクリックします。ファイルは圧縮されますので、内容を見る場合は解凍する必要があります。

#### **Boot.msg File**

システムがブートした時のメッセージを記録したファイルをレビュー出来ます。

#### **Warning Message File**

コアの負荷分散エンジンが排出したイベントを含んでいます。L4 の関連です。

#### **System Message File**

Linux の OS とコアな負荷分散エンジン (L7) が排出したイベントを含んでいます。

#### **Reset Logs**

全てのメッセージを消去します。

#### **Debug Options**

##### ***Disable All Transparency***

全てのバーチャルサービスのトランスペアレンシーを変更します。KEMP 社の販売店サポート要員の承諾を得た上でオンにしてください。

##### ***Enable L7 Debug Traces***

“System Messages” 内に、追加的な L7 アクセスのデバッグ情報を出力します。

##### ***Perform a l7 adm***

L7 のバーチャルサービスの詳細情報をテーブル形式で表示します。

##### ***Perform a PS***

システムのプロセス状態をレポートします。

##### ***Perform a l7 adm***

L7 のバーチャルサービスの詳細情報をテーブル形式で表示します。

### **Display Meminfo**

システムのメモリー使用状態を表示します。

### **Display Slabinfo**

システムの Slab 情報を表示します。

### **Perform an Ifconfig**

システムが持つ全てのイーサネットポートの情報を表示します。

### **Ping Host**

ICMP をサポートしている IPv4 デバイスへの ICMP エコーリクエスト (PING) を発信します。

### **TCP dump**

トレースを取得するための tcpdump コマンドを使用できます。フィルターは、イーサポート、IP アドレス、TCP/UDP のポート番号のみです。Start、Stop 後 “download” でローカルホストなどへファイルとしてセーブするか WireShark で直接開くことができます。

## **7.6.2 Syslog Options (シスログ・オプション)**

ロードマスターは、syslog プロトコルを使い、色々な警告とエラーメッセージを出力できます。これらのメッセージは、普通ローカルメモリーに蓄積され、WUI の “System Configuration” メニューの “logging Options” 下の “log Files” からか、コンソールの診断メニューを介して表示することができます。又、ロードマスターがこれらのエラーメッセージをリモート syslog サーバへ送信するように設定することも可能です。6つの異なるレベルのエラーメッセージが定義されています。各レベルのメッセージを、異なるサーバへと送れます。レベルは；

INFO  
NOTICE  
WARN  
ERROR  
CRITICAL  
EMERGENCY

注意：メッセージは、情報が送られるだけです。Emergency メッセージは、通常早急なアクションを必要とします。

ヒント：リモート Linux サーバでロードマスタの syslog メッセージを受けられるように syslog プロセスを有効にするためには、syslog を “-r” フラグを立てて起動しなければなりません。

## **7.6.3 SNMP Options (SNMPオプション)**

システムの各種警告を受けとる SNMP サーバの設定が行えます。

**Enable SNMP “SNMP メトリックスの有効/無効”**

このトグル・オプションは、SNMP メトリックスを有効/無効にするものです。このオプションを有効にすると、SNMP リクエストに対して応答します。

**注：**この設定は、デフォルトでは無効になっています。

**SNMP Clients “SNMP クライアント設定”**

このオプションにより、管理者はロードマスターが特定の SNMP 管理ホストへ応答を返すかの指定を行います。1 つ以上のホストを指定する場合は、空白で区切って入力します。

**重要：**もし、クライアントを指定しない場合は、ロードマスターは SNMP 管理リクエストに対しての応答を、不特定のホストへ返します。

**Community String “SNMP コミュニティ名の設定”**

このオプションは、SNMP コミュニティ・ストリングの変更を許します。デフォルト値は、“public” です。

**Contact Address “SNMP コンタクトの設定”**

このオプションは、SNMP コンタクト名列の変更を許します。例えば、ロードマスター管理者の E-Mail アドレスなどです。

**Location “SNMP ロケーションの設定”**

このオプションは、SNMP ロケーション名列を入力します。

**SNMP traps “SNMP トラップ”**

ロードマスターのバーチャルサービスやリアルサーバへの重要なイベントが発生した場合、トラップが作られます。これらは、SNMP トラップシンクへ送られます。

**Enable/Disable SNMP Traps “SNMP トラップの有効/無効化”**

このトグル・オプションは、SNMP トラップの送信を有効/無効にします。

**注：**SNMP トラップは、デフォルトでは無効です。

**Configure SNMP Trap Sink1 “SNMP トラップシンク 1 の設定”**

このオプションは、管理者がトラップの発生時に、SNMPv1 トラップをどのホストに送信するかを指定します。

**Configure SNMP Trap Sink2 “SNMP トラップシンク 2 の設定”**

このオプションは、管理者がトラップの発生時に、SNMPv2 トラップをどのホストに送信するかを指定します。

#### 7.6.4 Email Options (E-Mailオプション)

このオプションは、ロードマスターの発するイベントを E メールにて警告として通知するための設定を可能にします。Eメールの通知は、6つの定義レベルに分かれて配信されます。レベル毎に異なる受信者を設定出来、各レベルは複数の受信者を設定出来ます。Eメール警告は、メールサーバによりますが、ノンセキュア、もしくはセキュア (SSL) 両方の通信をサポートしています。

Eメール警告のサンプル：



Oct 22 19:42:16 KEMP2 logger: This is a test from the Load Master

#### Enable Email Logging

Eメール警告オプションをオン/オフします。

#### Set SMTP Server

FQDN フォーマット、もしくは IP アドレスで SMTP サーバを指定します。FQDN フォーマットで指定を行う場合は、DNS サーバの設定を行う必要があります。

#### Set Authorized User

指定した SMTP サーバが、メール配信を行うために特定権限を必要とするならば、その権限を持ったユーザ名を入力します。もし権限を必要としないならば空白のままとします。

#### Set Authorized Users Password

上記ユーザのためのパスワードを入力します。パスワードは、半角文字で 8 文字から 16 文字までの範囲で指定できます。使用できる文字は英字 (大文字、小文字)、数字、英数字以外の記号文字で、これらの文字を任意に組合わせて指定できます。ロードマスターは指定された文字列の強度を自動的に計算して、パスワードの強度が弱い場合はメッセージを表示します。メッセージが表示されたら文字種類を変更するか桁数を増やしてパスワードの強度を高めて下さい。

#### パスワード指定例

- ・英小文字のみ : 9 文字以上 `ancdefghi`
- ・英小文字と数字の混在 : 8 文字以上 `1abcdefg`
- ・英大文字と英小文の混在 : 8 文字以上 `Abcdefgh`
- ・英小文字、記号、数字の混在 : 8 文字以上 `ab!12345`
- ・数字のみ : 13 文字以上 `0123456789012`

### Set Local Domain

SMTP サーバが、ドメインに属しているならば最上位のドメイン名を入力します。必要がなければ空白のままとします。

### Set E-mail Recipient

各警告レベルに応じた E メールを受信者のアドレスを入力します。各レベルには、コンマで区切って複数の受信者を設定可能です。例：

[support@kemptechnologies.com](mailto:support@kemptechnologies.com),[info@kemptechnologies.com](mailto:info@kemptechnologies.com)

### Reset

システムの全ての E メール警告の設定を新たに入力した情報にリセットします。

### Change Email Recipients

E メール警告受信者を新たに入力した情報にリセットします。

### Send Test Email to All Recipients

テストメッセージを登録した全ての E メール受信者に送信します。

## 7.7 Miscellaneous (その他)

### 7.7.1 SNAT Control (SNAT管理)

このオプションは、ロードマスターの S-NAT 機能を有効、無効に出来ます。2 アーム構成で S-NAT を有効にすると、リアルサーバはロードマスターをゲートウェイにしてインターネットへのアクセスが可能になります。ロードマスターは、リアルサーバからのリクエストをあたかもロードマスターが発信したかのように見せかけ (マスケラード) ます。これは、リアルサーバがプライベートネットワーク内にあっても、インターネットへのアクセスが出来ることを意味します。

S-NAT を無効にすると、ロードマスターは “マスケラード” を実行せず、プライベートネットワークのリアルサーバからのインターネットへのアクセスは出来なくなります。

1 アームでのネットワーク構成では、S-NAT は何の機能も提供しません。

### 7.7.2 Remote Access (リモートアクセス)

システム管理を、リモートで行うための設定を変更出来ます。

Allow Remote SSH Access	<input checked="" type="checkbox"/> Using: All Networks Port: 22 <input type="button" value="Set Port"/>
	Disable SSH-V1 Prot <input checked="" type="checkbox"/>
Allow Web Administrative Access	<input checked="" type="checkbox"/> Using: eth0: 192.168.1.100 Port: 443 <input type="button" value="Set Port"/>
Administrative Default Gateway	<input type="text"/> <input type="button" value="Admin Default Gateway"/>
Radius Server	<input type="text"/> <input type="button" value="Radius Server"/> Shared Secret: <input type="text"/> <input type="button" value="Set Secret"/>
Enable Hover Help	<input checked="" type="checkbox"/>
Enforce Strict IP Routing	<input type="checkbox"/>
Remote GEO LoadMaster Access	<input type="text"/> <input type="button" value="Set GEO LoadMaster access"/>
GEO LoadMaster Port	22 <input type="button" value="Set GEO LoadMaster Port"/>

### Allow Remote SSH access “SSH アクセスの許可／禁止”

このオプションは、SSH 接続を介したロードマスターへのアクセスを許可／禁止します。もし、このオプションが禁止されていると、設定メニューへのアクセスはコンソールだけから可能となります。‘bal’ ユーザのパスワードが設定されていない場合は、SSH 接続を介したログインは出来ません。

### Allow web Administrative Access “WUI へのリモートアクセス許可／禁止”

WUI (ウェブユーザインターフェース) のアクセスを許可／禁止します。又、デフォルトのイーサポート 0 より他のイーサポートへの変更、及びポート番号の変更が可能です。

### Administrative Default Gateway

WUI のための特定ゲートウェイ装置を設定して、システムのグローバルゲートウェイとは違うルーティングを行わせることが可能です。WUI 以外のアクセスでは、この設定は使用されません。

### Radius Server

管理用ユーザを RADIUS と連携させられます。サーバの登録がここに必要です。

### Enable Hover Help

WUI 上に表示されるヘルプ機能を有効、無効にします。

### Enforce Strict IP Routing

WUI へのアクセス時、ストリクト・ソース・ルーティングのみしか受け付けないようにします。

## Remote GEO LoadMaster Access

LoadMaster-GEO, LoadMaster-DR, もしくは VLM-DR と併用して使用するときに状態監視を受け付けるために相手の IP アドレスを設定します。

## GEO LoadMaster Port

上記 “Remote GEO LoadMaster Access” のポート番号を設定します。SSH プロトコールが使用されますので、通常ポート番号 22 を使用します。

### 7.7.3 L7 Configuration (レイヤ 7 設定)

L7 Transparency	Non Transparent ▼
Allow connection scaling over 64K Connections	No ▼
L7 Connection Drain Time (secs)	300 <input type="button" value="Set Time"/> (Valid values:60 - 86400)
Additional L7 Header	X-ClientSide ▼
Add Port to Active Cookie	No ▼
L7 Connection Timeout (secs)	0 <input type="button" value="Set Time"/> (Valid values:0, 60-86400)
Always Check Persist	No ▼
Assume Expect-100	No ▼
Conform to RFC	Yes ▼

#### L7 Transparency (レイヤ 7 トランスペアレンシー)

システム全体で、追加するバーチャルサービスのデフォルトのトランスペアレンシーの設定を変更できます。デフォルトは “Non Transparent” です。

#### Allow connection scaling over 64K Connections

高トラフィックにおいては、VS毎のTCP接続数が 1 ポートの上限である 64,000 以上必要になることがあります。このオプションを使用することで、他のIPアドレスのポートを振り分けることで上限を拡張できます。他のIPアドレスの指定は、バーチャルサービスの属性パラメータの “Alternate Source Addresses” 内に指定できます。1 つ以上のIPアドレスを指定する場合は、空白で区切って入力します。

#### L7 Connection Drain Time (secs)

リアルサーバは、Disableにしてもパーシステンシー機能のタイムアウト時間以内であれば、前回のユーザの再接続を許します。このパラメータは、指定した時間でパーシステンシーのタイムアウト時間を一時的に書き換えることで、タイムアウトを強制的に発生させることが

できます。これにより、サーバの保守作業を行う場合などにユーザを他のリアルサーバへ早期に導くことができます。

### **Additional L7 Header (レイヤ7 追加ヘッダー)**

バーチャルサービスをトランスペアレントに設定しない場合は、L7 モードだけが可能です。又、その場合は、クライアントの IP アドレスは、バーチャルサービスのアドレスへとロードマスターが変換してリアルサーバへアクセスします。よって、その場合はクライアントのアドレスは、バーチャルサービスのアドレスのみがサーバのアクセスログへ書かれ、実際のクライアントアドレスは書かれない事になります。この機能を使用することで、HTTP ヘッダー内へ X-ClientSide、もしくは X-Forwarded-For としてクライアントアドレスを挿入します。

### **Add Port to Active Cookie (アクティブクッキーへのポート番号追加)**

ロードマスターが発生させるクッキーに、ソース TCP ポートを追加しユニークなクッキーにさせる事が可能です。

通常、NAT 下の LAN 側にロードマスターを置いた場合、ソース IP アドレスが統一され同じリアルサーバへの接続がなされると、違うクライアントのアクセスでもクッキー内容が同じになってしまいます。この結果、パーシステンスの時間切れ後にアクセスしたとしても、他のクライアントが接続した時間を基点としてしまい、パーシステンスの時間切れがなくなり、同じリアルサーバへと接続されてしまいます。これが重なると、結果的に1つのサーバへの接続のみに偏ってしまいます。これを防ぐために、リクエストを受けた時のソースポートをクッキーに加えることでユニークなものにし、クライアント毎のパーシステンスが可能となります。

### **L7 Connection Timeout (sec) (レイヤ7 接続タイムアウト)**

L7 モードの接続時間の調整ができます。デフォルトの“0”は、660 秒 (11 分) です。これ以上の接続持続性を必要とする場合は、その時間に更新します。時間を入力した後に“Enter”キーを押す必要があります。又、新しい設定を有効にするためにはシステムリブートが必要です。

### **Always Check Persist (全リクエスト・パーシステンシー)**

デフォルト設定での HTTP/1.1 のリクエストは、同一セッション中最初のリクエストのみがパーシステンシー・オプションに沿って同一サーバへのセッション維持が行われます。このオプションを使用すると、同一セッションの全てのリクエストがパーシステンシー・オプションに沿ってセッションを同一 RS に維持しようとします。

### **Assume Expect-100**

クライアントが HTTP リクエストの送出時、“100-continue”ヘッダーを要求してきた場合に、100(Continue) status を返して通信を継続させます。

### **Conform to RFC**

システムで使用する HTTP プロトコールを RFC2616 に準拠させます。

#### 7.7.4 AFE Configuration (アプリケーション・フロント・エンド機能設定)

Cache Configuration	
Maximum Cache Size	100 <input type="button" value="Set Size"/> (Valid values:1 - 101)
Cache Virtual Hosts	Yes <input type="button" value="v"/>
File extensions that should not be cached:	<input type="text"/> <input type="button" value="Add"/>
.aspx .jsp .php .shtml	<input type="button" value="No Entry"/> <input type="button" value="Delete"/>
Compression Options	
File extensions that should not be compressed:	<input type="text"/> <input type="button" value="Add"/>
.asf .gif .gz .jpeg .jpg .mov .mp3 .mp4 .mpe .mpeg .mpg .pdf .png .swf .tgz .wav .wma .wmv .z .zip	<input type="button" value="No Entry"/> <input type="button" value="Delete"/>
Intrusion Detection Options	
Detection Rules	<input type="text"/> <input type="button" value="Choose..."/> <input type="button" value="Install new Rules"/>
Detection level	Default - Only Critical problems are rejected <input type="button" value="v"/>

#### Cache Configuration (キャッシュ機能オプション設定)

システムで使用する最大キャッシュメモリーの設定、及び VS 毎のキャッシュメモリー (Cache Virtual Hosts) 機能のオン/オフ、及びキャッシュしないファイルの種類を指定できます。

#### Compression Options (圧縮機能オプション設定)

圧縮するファイルの種類を指定します。

#### Intrusion Detection Options (IDS 機能オプション設定)

侵入防止システムのルールのアップグレード、及び検出レベルの設定変更を行えます。

#### 7.7.5 Network Options (ネットワーク関連オプション設定)

Enable Non-Local Real Servers	Yes ▼
Enable Alternate GW support	Yes ▼
Enable TCP Timestamps	No ▼
Enable TCP Keepalives	Yes ▼
Enable Reset on Close	No ▼
Subnet Originating Requests	No ▼

### Enable Non-Local Real Server (リモートサーバの有効化)

非透過モード (Non Transparent) バーチャルサービスで、ローカルサブネット以外のサーバを、リアルサーバとして追加できます。透過モード (Transparent) のバーチャルサービスへは有効になりません。このパラメータを “Yes” にすると、VS 内の RS 追加時に新たなパラメータとして “Allow Remote Addresses” が表示されますので、チェックマークをいれた後でリモート RS の IP アドレスを入力します。

### Enable Alternate GW support (ポート 0 以外のゲートウェイの有効化)

システムのデフォルト・ゲートウェイは、通常ポート 0 のサブネットに属する機器しかアサイン出来ません。ポート 0 以外のネットワークに属する機器をデフォルト・ゲートウェイとしてアサインしたい場合は、このパラメータをオンにして、該当するポートの属性パラメータである “Use for Default Gateway” もオンにする必要があります。その後、デフォルト・ゲートウェイを変更します。

### Enable L7 Timestamps (L7 タイムスタンプの有効化)

ロードマスターは、デフォルトにおいて TCP 接続パケット (SYN) にタイムスタンプを含みません。L7 モードでの接続で、パフォーマンス試験などでタイムスタンプの必要がある時は、On にしてください。それ以外の一般の通常オペレーションでは、このパラメータはオフにしておくことを推奨します。

### Always Check Persist (全リクエスト・パーシステンシー)

デフォルト設定での HTTP/1.1 のリクエストは、同一セッション中最初のリクエストのみがパーシステンシー・オプションに沿って同一サーバへのセッション維持が行われます。このオプションを使用すると、同一セッションの全てのリクエストがパーシステンシー・オプションに沿ってセッションを同一 RS に維持しようとします。

### Enable TCP Keepalives (TCP 接続のキープアライブの有効化)

アプリケーションによっては、TCP を開いたままではタイムアウトを起してしまうものがあります。この機能をオンにすることで定期的にキープアライブを発信し TCP 接続を継続させます。(MS-Exchange サーバでは必須)

**Enable Reset on Close (Reset 使用による TCP 接続クローズの有効化)**

このパラメータをオンにすることで TCP 接続でクライアントを Reset にて強制的にクローズ出来るようにします。

**Subnet Originating Requests (非透過モードでのソースアドレス変更)**

2 アーム構成時、非透過モードでのサービスのリアルサーバへのアクセスは、VS のアドレスがソース IP アドレスとなります。セキュリティ上、ソース IP アドレスが同じサブネット上のアドレスでなければならない場合、この機能を有効にします。有効にした場合は、RS の属するイーサポートにアサインされている IP アドレスをソース IP アドレスとして RS をアクセスします。

**7.7.4 HA Parameters (HA用パラメータ)**

HA Mode	HA (Second) Mode
HA version	Upgraded (carp)
HA Timeout	15 Seconds
HA Initial Wait Time	10 <input type="button" value="Set Delay"/> ( Valid Values: 0, 16-180)
HA Virtual ID	1 <input type="button" value="Set Virtual ID"/> ( Valid Values: 1-255)
Switch to Preferred Server	No Preferred Host
HA Update Interface	eth0: 192.168.1.100
Force Partner Update	<input type="button" value="Force Update"/>
Inter HA L4 TCP Connection Updates	<input type="checkbox"/>
Inter HA L7 Persistency Updates	<input type="checkbox"/>
Use Virtual MAC addresses	<input type="checkbox"/>

**HA Mode (HA 構成モード)**

スタンドアロン、HA-1、もしくは HA-2 の選択が出来ます。構成を変更するときにはシステムリブートが必要です。

**HA version (HA バージョン)**

HA でお互いを監視するプロトコルを選択できます。ハートビート (h b) 方式は古いバージョン (4.1/4.2) で使用されていたもので、carp プロトコルは更新された方式です。この方式を変更した場合は、2つのユニットのリブートが必要です。

**HA Timeout (sec) (HA タイムアウト)**

このオプションは、HA クラスターの故障を検出する時間を調整出来ます。3-15 秒の間で設定出来、デフォルトは 9 秒です。短い値ほど故障をすばやく検出出来、長い値ほど DOS 攻撃に対して防御を与えます。

### HA Initial Wait Time (sec) (HA 起動待機時間)

このオプションは、システムがリブートした時、どのぐらい待ってから稼動状態にするかを指定出来ます。これは、スイッチがセキュリティ対策のために、イニシャルが掛かった時リンクを張るのを遅くしている場合に、リンクが完全に張られるのを待ってシステムを稼動状態にするという目的のためです。これにより、ネットワークのリンクが張られる前にシステムが稼動状態になってしまったために、リンクダウンの原因で再度システムがリブートを繰り返すのを防止出来ます (h bモード時)。“carp”モードでも、システムが稼動状態になった時、スイッチのリンク状態をチェックしますが、もしリンクが張られていなくても自主的なリブートは行いません。

### HA Virtual ID (HA 仮想 ID)

このオプションは、同じネットワーク上に1つ以上の HA ペアが設置されていて、間違った干渉が起こるのを防止するために必要です。必ずそういう場合は、HA ペアに異なる ID 番号を設定するようにしてください。

### Switch to Preferred Server (アクティブ固定)

HA 構成時のアクティブ側ユニットを固定化します。この設定を特定のユニットに指定した場合は、故障時には他のユニットがアクティブとなりますが、このユニットが復旧するとすぐアクティブに戻ります。

注：この設定の変更時は、システムのリブートが必要です。

### HA Update Interface (HA 情報転送インターフェース)

この設定は、HA 間の情報転送にどのインターフェースを使用するかを指定出来ます。1 アーム構成では他の選択は出来ませんが、2 アーム、マルチアームでは他のインターフェースへの変更が出来ます。

### Force Partner Update

このパラメータは、スタンバイ側だけで使用できます。“Force Update” ボタンをクリックすると、アクティブ側の設定ファイルをスタンバイ側へ強制的に上書きします。

### Inter HA L4 TCP Connection Updates (L4 ステータスフル切り替え)

このオプションは、HA 構成時にシステムが故障で他のユニットへ切り替わっても、TCP 接続を継続するためのものです。追加のメモリー使用量と CPU 処理量が発生しますので、必要性が高くない場合はこのオプションの使用は推奨出来ません。

注：このパラメータをオンにしたらシステムのリブートが必要です。

### Inter HA L7 Persistency Updates (L7 ステータスフル切り替え)

このオプションは、HA 構成時にシステムが故障で他のユニットへ切り替わっても、L7 パーシステンスを継続するためのものです。追加のメモリー使用量と CPU 処理量が発生しますので、必要性が高くない場合はこのオプションの使用は推奨出来ません。

注：このパラメータをオンにしたらシステムのリブートが必要です。

### HA Multicast Interface (HA ステータスフル・インターフェース)

このパラメータは、上記の *Inter HA L4 TCP Connection Updates*、及び *Inter HA L7 Persistency Updates* をオンにすると表示されます。ステータスフル情報を HA 同士で同期を取るためのパスを選択します。

### HA Initial Network Checks (HA イニシャル時のネットワークチェック)

HA 構成時に、ユニットのイニシャルが発生した場合、追加的なネットワークのチェックを行います。一般的なネットワークでは必要ありませんので、このオプションの使用は推奨しません。

**注意：**このパラメータは、“HA Version”として‘Legacy(hb)’を選択した時のみ表示されます。

### Use Virtual MAC addresses (バーチャル MAC アドレスの使用)

現在の多くの Firewall は、IP アドレスから MAC アドレスを探した結果をセーブする ARP テーブルを持っていますが、セキュリティ対策のために例え MAC アドレスが変わったという結果が得られても、テーブル内の情報を 60 分以内には変更しません (Long Arp Cache)。この場合は、HA システムが 1 つのシェアード IP アドレスを使ってスタンバイ側へ切り替わる時に MAC アドレスを変更してトラフィックの行き先を切り替えているアルゴリズムが使えなくなってしまう。レガシーな HA バージョンであるハートビート (Heart Beat) 方式では、この問題解決のために Firewall の Arp 用キャッシュ保持時間を最短にってもらうようお願いしていました。しかし、このパラメータを追加したことで、HA のイーサポートが共通バーチャル MAC アドレスを使えるようになりました。例えば、HA-1 がマスターで MAC アドレスは AA だとします。このパラメータをオンにすることで、バーチャル MAC アドレス BB を HA-1 に宛がいます。そして、HA-2 に切り替わった時に HA-2 が持っていた本来の CC という MAC アドレスに変わりバーチャル MAC アドレス BB を HA-2 に移し替えます。スタンバイとなった HA-1 は本来の AA に戻ります。これにより、シェアード IP アドレスに対する MAC アドレスがいつも同じバーチャル MAC アドレスのままとなり Firewall の Long Arp Cache の問題が解決されます。

只、この機能をオンにすると本当の MAC アドレスが隠れてしまい、障害解析を行う時に技術者を混乱させてしまうかもしれません。よって、もし Firewall 側でキャッシュ保持時間を最短に変更できるのであればこのパラメータを使用しないことを薦めます。この保持時間の値が、実際の VS トラフィックの切り替え時間となりますので、アクティブが切り替わったとしても、この値が 1 分とすると 1 分後に実際の VS トラフィックは新しいマスター側へ流れるようになります。

**注意：**このパラメータは、“HA Version”を‘carp’に設定した時のみ表示されます。又、このパラメータをオンにした場合は、HA 両方のユニットをリブートする必要があります。

**End**