



Web Beagle

Model 400 / 500 / 600

L4 & L7 ロードバランサのWeb Beagle をご利用いただきありがとうございます！
本製品の操作マニュアルになります。

第1章 Web Beagle とは

Web Beagle がどのようなものなのか、新しいモデルになって何ができるようになったかを解説します。

第2章 セットアップ

Web Beagle のセットアップの仕方について解説します。

第3章 冗長化構成

Web Beagle の冗長化構成の構築手順について解説します。

第4章 運用管理

Web Beagle の運用管理について解説します。

第5章 管理画面の機能説明

Web Beagle の管理画面について機能ごとに解説します。

第6章 コンソール管理

Web Beagle のコンソール接続時の機能について解説します。

第7章 保証とアフターサービス

Web Beagle の保証とアフターサービスになります。

付録

Web Beagle の付録です。

本マニュアルについて

本マニュアルについての注意事項になります。

第1章 Web Beagle とは

1. はじめに

このたびは株式会社エーティーワークスのWeb Beagle をお買い上げいただき、誠にありがとうございます。

Web Beagle は、オープンソースソフトウェアを使用した弊社が独自にカスタマイズしたロードバランサを搭載する、アプライアンスサーバです。筐体は弊社オリジナルの1/4U シャーシを採用しており、ラックを非常に効率よく使用することができます。専用の管理インターフェイスを搭載していますので、セットアップや運用管理を全てWeb ブラウザから行うことができます。

本書をよくお読みいただき、本製品の機能や使用方法を十分理解したうえで、本製品をご使用になってください。

2. 商標について

Linux は、Linus Torvalds の米国およびその他の国における登録商標あるいは商標です。

Microsoft、Windows は、米国Microsoft Corporation の米国およびその他の国における登録商標です。

その他、記載されている会社名、製品名は、各社の登録商標または商標です。

なお、本文中では、®、™ マークは明記しておりません。

3. Web Beagle の特徴

- **省スペース**
 - ラックを非常に有効に利用できる弊社オリジナルの1/4U シャーシを採用。
- **Web Beagle 機能**
 - L4負荷分散エンジンにオープンソースソフトウェアLinux Virtual Server (LVS) を採用
 - 以下の負荷分散方式をサポート
 - ラウンドロビン
 - 重み付けラウンドロビン
 - 最小コネクション
 - 重み付け最小コネクション
 - ソースハッシング
 - 最速応答時間
 - 負荷分散するトランスポートプロトコルをTCP、UDPから選択可能
 - 接続元IP アドレスによるセッション維持
 - 仮想IPのアクセス制限機能（ブラックリスト方式、ホワイトリスト方式）
 - 死活監視機能（TCP / HTTP / HTTPS / MySQL, ping / DNS）※ping / DNS はUDP上の通信を負荷分散時に選択可能
 - L7負荷分散エンジンにオープンソースソフトウェアHAProxyを採用
 - 以下の負荷分散方式をサポート
 - ラウンドロビン
 - 重み付けラウンドロビン
 - 最大接続数以下同一サーバー

- ソースハッシング
 - URIハッシング
- SSLオフロード機能
 - ノードサーバのSSL証明書のインストールが不要に
 - ノードサーバの負担減
- 以下のセッション維持方式をサポート
 - 接続元IP アドレス
 - cookie
 - スマートフォンでもセッション維持ができるように
 - SSLセッションID
- 仮想IPのアクセス制限機能（ブラックリスト方式、ホワイトリスト方式）
- 死活監視機能（TCP / HTTP / HTTPS）
- 様々なネットワーク構成に対応
 - Model 500, 600... DSR 型、NAT 型、透過型
 - Model 400... DSR 型のみ
- 待機サーバ機能
 - バックアップサーバとしての利用
 - ソーリーサーバとしての利用
- **運用管理**
 - Web ブラウザから操作できる専用管理インターフェースを搭載
 - 本製品の状態や死活監視の異常を即座に管理者にメール通知
 - SNMP エージェントとしてSNMP マネージャから管理可能
 - 負荷分散の拡張MIB取得をサポート
 - Web Beagle に蓄積された各種ログデータをグラフィカルに可視化
 - 管理画面よりWeb Beagle のログを一覧形式で確認可能
 - 外部Syslogサーバにログ転送可
- **保守性**
 - 設定情報のバックアップリストア機能
 - ファームウェアアップデート機能
 - 旧モデルバックアップファイルからの設定情報リストア機能
- **信頼性**
 - 本製品2 台にて冗長化構成に対応（アクティブ-スタンバイ構成）
 - ボンディングによるネットワークポートの冗長化（Model 600 のみ）
 - ネットワークポート故障時でも通信断が発生しない

4. 本文中に使用される記号について

本書では、本文中に以下の記号を使用しております。

- **注意**
装置の取り扱いや設定手順において守らなければならない事項や注意が必要な事項を記しています。
- ✂ **ポイント**
装置の取り扱いや設定手順において知っておくと便利な点を記述しています。
- 📖 **参照**
装関連する項目やページを記述しています。

5. ハードウェアの取り扱いについて

Model 400, 500 フロントパネルの説明

Model 400/500



図1-1 フロントパネル

- **電源スイッチ**
押下すると電源が投入されます。
- **リセットスイッチ**
押下するとリセットされます。
- **COM ポート**
シリアルポートです。
- **VGA 端子**
コンソールを接続する場合、モニタを接続します。
- **USB3.0**
USB3.0 ポートです。
- **ネットワークポート**
 - **DSR モード**
ポート1 を使用します。
 - **NAT モード(Model 500)**
WAN 側のネットワークにポート1 を接続します。
LAN 側のネットワークにポート2 を接続します。
 - **透過型モード(Model 500)**
外側のネットワークにポート1 を接続します。
内側のネットワークにポート2 を接続します。
- **アクセスランプ**
アクセスランプです。
- **電源ランプ**
電源ランプです。 【緑点灯】 電源ON 【消灯】 電源OFF
- **電源接続口**
付属の電源ケーブルを接続します。

❗ IPMI は使用しません。

Model 600 フロントパネルの説明

Model 600

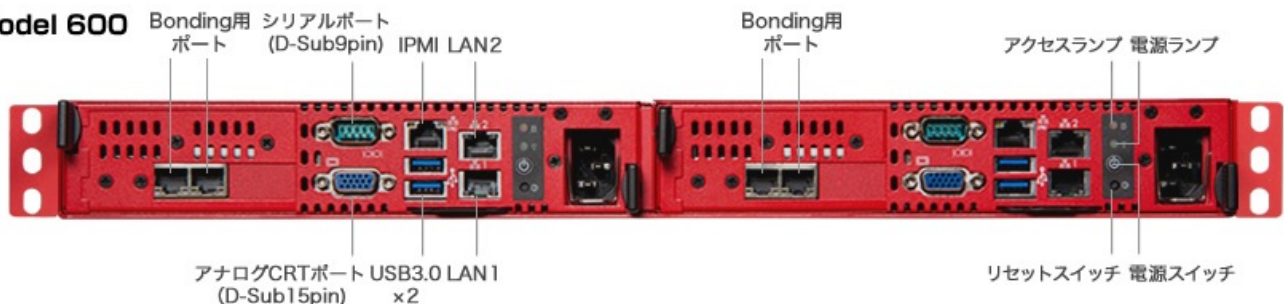


図1-2 フロントパネル

- **電源スイッチ**
押下すると電源が投入されます。
- **リセットスイッチ**
押下するとリセットされます。
- **COM ポート**
シリアルポートです。
- **VGA 端子**
コンソールを接続する場合、モニタを接続します。
- **USB3.0**
USB3.0 ポートです。
- **ネットワークポート**
 - **DSR モード**
ポート1, ポート3 を使用します。Bonding OFF 時はポート3 のみ使用します。
 - **NAT モード**
WAN 側のネットワークにポート1, ポート3 を接続します。Bonding OFF 時はポート3 のみ使用します。
LAN 側のネットワークにポート2, ポート4 を接続します。Bonding OFF 時はポート4 のみ使用します。
 - **透過型モード**
外側のネットワークにポート1, ポート3 を接続します。Bonding OFF 時はポート3 のみ使用します。
内側のネットワークにポート2, ポート4 を接続します。Bonding OFF 時はポート4 のみ使用します。
- **アクセスランプ**
アクセスランプです。
- **電源ランプ**
電源ランプです。 【緑点灯】 電源ON 【消灯】 電源OFF
- **電源接続口**
付属の電源ケーブルを接続します。

✂ ポート3, ポート4について

ポート3: 上図「Bonding用ポート」内の正面から見て左側ポート

ポート4: 上図「Bonding用ポート」内の正面から見て右側ポート

❗ IPMI は使用しません。

6. ハードウェア取り扱う上での注意事項

お客様や他の方への危害や損害を未然に防ぎ、本製品を安全にご使用いただくために必ずお守りいただきたい事項を記載しました。安全にご使用いただくために必ずお読みになり、内容をよく理解された上でご使用ください。

警告及び注意

- **付属品の電源コードを使用する**
付属品の電源コードを使用して下さい。
付属品の電源コードは他製品で使用しないで下さい。
付属品の電源コードはAC100V 専用です。AC100V で使用して下さい。
- **表示された電源電圧で使用する**
表示された電源電圧以外では使用しないでください。火災や感電の原因になります。
- **もし異常が起こったら**
本機から煙が出たり、変なにおいや音がしたら、直ちに安全にスイッチを切りコンセントからプラグ

を抜いてください。そのまま使用すると、火災や感電の原因となります。

(修理につきましては弊社にお問い合わせください)

- **濡れた手で本製品を触らないでください。また、濡れた手で電源プラグの抜き差しはしないでください**

本体及び周辺機器の電源プラグが入っているときに濡れた手で触れると、感電や故障の原因となります。

また、電源プラグが接続されていなくても故障の原因となります。

濡れた手で電源プラグの抜き差しをすると、感電をする恐れがありますので、必ず乾いた手で抜き差ししてください。

- **電源コードやプラグを破損させないでください**

無理に曲げて設置したりすると、電源コードやプラグが破損し、火災や感電につながります。

- **電源プラグは確実に差し込んでください**

電源プラグを確実に差し込まないと、接触不良により火災や感電につながりますので、必ず根元まで確実に差し込んでください。また、定期的にプラグの状態を確認してください。

- **電源コードのアース線は確実に配線してください**

- **雷が鳴っている時は、電源プラグに触れないでください**

落雷時に感電する恐れがあります。

- **電源プラグは定期的に埃などを取り除いてください**

電源プラグに埃がついたまま使用しますと、ショートや絶縁不良となり、火災や感電の原因となります。

埃を取り除く際は、プラグを抜き、乾いた布で拭き取ってください。

- **本体内部に、液体や異物を入れないでください**

本体内に液体や異物が入った状態で使用すると、火災や感電、故障につながる恐れがあります。液体や異物が内部に入った場合は、直ちに安全にスイッチを切り、コンセントからプラグを抜いてください。

(修理につきましては弊社にお問い合わせください)

- **高電圧機器の周辺で作業する場合、または高電圧機器を取り扱う場合は必ず2人以上で作業してください**

高電圧機器の周辺で作業する場合や、高電圧機器を取り扱う場合は、万一の場合にそなえ、必ず作業員以外に主電源を切断することができるように人員を配置してください。

また、予めブレーカーなどの主電源スイッチの場所を確認してください。

- **水分や湿気の多い場所でのご使用はお避けください**

火災や感電、故障の原因となります。

- **本体通気孔をふさがないでください**

本体通気孔をふさいだ状態で使用すると、本体内部の温度が上がり、故障ややけどの原因となります。

- **動作中のファンには指や異物を入れないでください**

けがや故障の原因となります。

- **本機の上に物をのせないでください。また、本機の上に乗らないでください**

落下して怪我をしたり、本機が破損する恐れがあります。本機の上に重量物を置くと、ケースが変形し、内部の機器が破損し、火災や感電の原因となる恐れがあります。

- **本製品を次のような場所に設置しないでください**

- 許容動作環境以外の場所
- 振動が発生する場所
- 平坦でない場所
- 強い磁界が発生する場所
- 直射日光が当たる場所
- 火気の近く、または高温になる場所
- 漏電や漏水の恐れのある場所（故障や感電の恐れがあります）
- 不安定な場所

- **本製品を落としたり、強い衝撃を与えないでください**

本製品は精密機械ですので、衝撃を与えないように慎重に取り扱ってください。強い衝撃を与えると

故障の原因となります。

- **本機を移動する際はコード類を取り外してください**

コードが破損し、火災や感電につながる恐れがありますので、必ずすべての接続をはずしてから移動してください。

- **静電気による破損を防ぐ為、以下のことをお守りください**

静電気によって、本製品が破損したり、データの損失、破損を引き起こす恐れがあります。

- 本製品に触れる前に、必ず身近な金属に触れ、身体の静電気を取り除いてください。
- メモリやその他部品の端子部分に手を触れないでください。

- **本製品を分解、修理、改造しないでください**

火災・感電・故障のおそれがあります (保証の対象外となります)

第2章 セットアップ

1. 設置計画

Web Beagle Model 500, 600 は3 種類のネットワーク構成に対応しています。ご利用のネットワーク構成にあわせて最適な構成を選択してWeb Beagle の導入を行ってください。Web Beagle Model 400 はDSR 型のみ対応していますのでDSR 型でネットワーク構成を行ってください。それぞれのネットワーク構成の特徴を説明します。

DSR 型

DSR 型の特徴

DSR (Direct Server Return) 型はサーバ直接応答とも呼ばれる方式で、次のような特徴があります。

- 受けたリクエストをWeb Beagle がノードサーバに転送します。転送時には通信内容に変更を加えません。
- 振り分けられたノードサーバは応答を直接リクエスト元へ送信します。

このため、DSR 型ではWeb Beagle はリクエストの振り分けのみを行う動作となり、Web Beagle の負担が少なくなります。

DSR 型は3 種類の動作方式の中で最も性能を発揮できるため、この方式でのご利用をお勧めします。

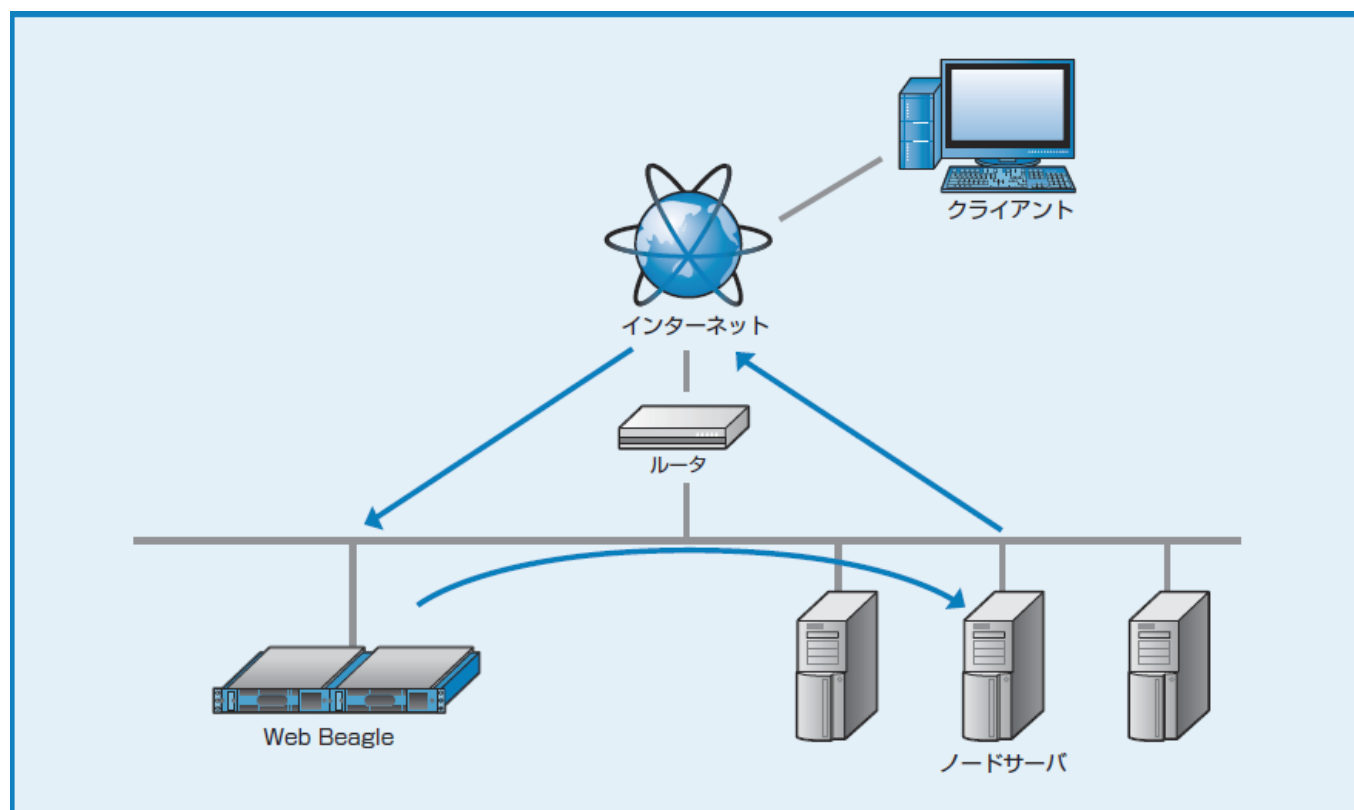


図2-1 DSR 型のネットワーク構成

❗ DSR 型を選択できないケース

DSR 型では、仮想IP アドレス宛のパケットはそのままノードサーバに転送されます。このため、ノードサーバでは仮想IP アドレス宛のパケットを受けつける特殊な設定が必要になります。ノードサーバがLinux ま

たはWindows の場合、「2章 - DSR 型における仮想IP アドレス宛の接続を受け付ける設定 (/chapter_2.html#dsr-型における仮想ip-アドレス宛の接続を受け付ける設定)」を参照し、設定を行ってください。ノードサーバでこの設定ができない場合は、DSR 型を利用することはできません。NAT 型または透過型でご利用ください。

④ DSR 構成におけるL7負荷分散の通信経路

L7負荷分散では、アプリケーションレベルでの負荷分散という性質のため、DSR 型ではありましても、

(1) リクエスト：クライアント ---> Web Beagle ---> ノードサーバ

(2) レスポンス：ノードサーバ ---> Web Beagle ---> クライアント

という通信経路になります。

NAT 型 (Model 500, Model 600)

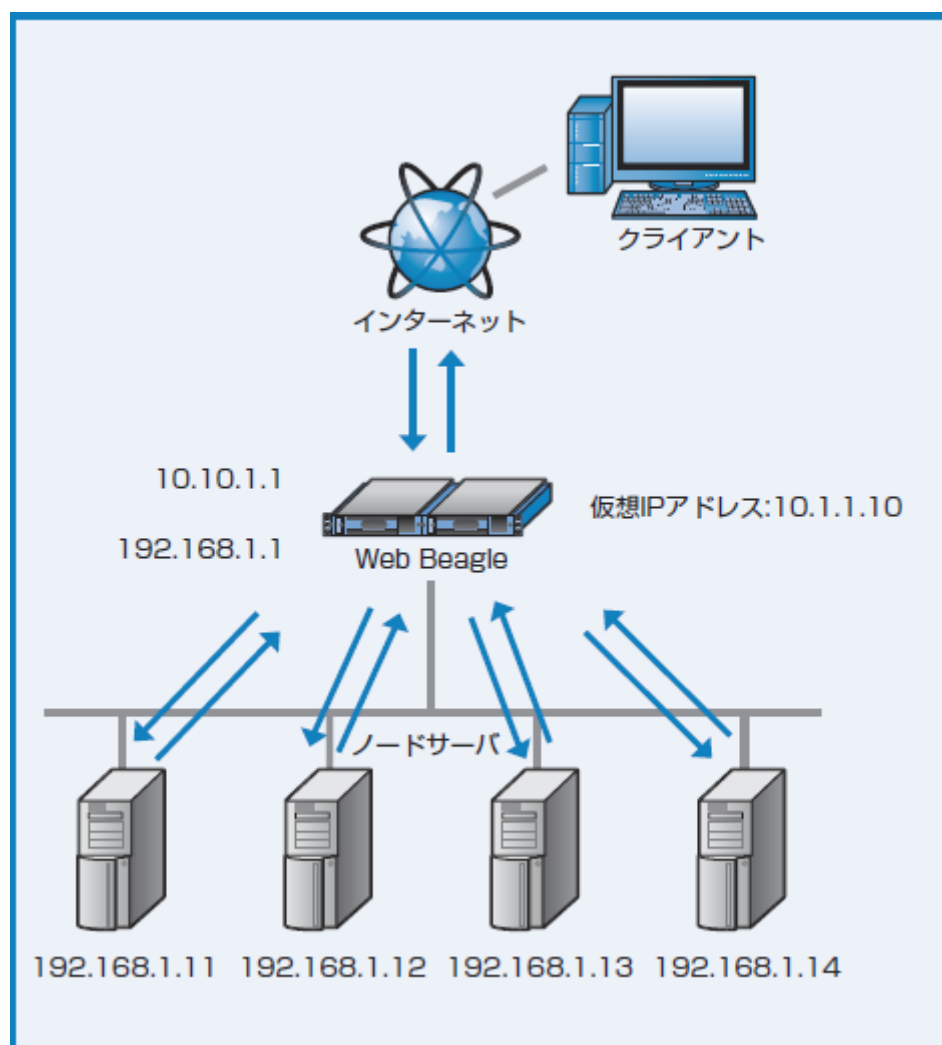
NAT 型の特徴

NAT 型は、ノードサーバにプライベートIP アドレスが設定されている等、Web Beagle の外側と内側のネットワークが異なる場合に利用します。

次のような特徴があります。

- ノードサーバにはプライベートIP アドレスを使用できるため、グローバルIPアドレスが少ないネットワークでも多くのノードサーバを利用できます。
- 外側からノードサーバへの通信はWeb Beagle でNAT を行わないと通信できないため、設定されていない通信は遮断することができます。

外側のネットワークから内側のネットワーク機器への接続手段として基本NAT 機能、NAPT (IP マスカレード) 機能があります。内側のネットワーク機器が外側のネットワークに接続することを可能にするソース NAT 機能も持っています。



透過型（Model 500, Model 600）

透過型の特徴

透過型は、導入対象が一つのネットワークで、DSR 型のようにノードサーバに特殊な設定ができない場合に有効な方法です。既存の運用システムに比較的容易に設置・導入することが可能となります。

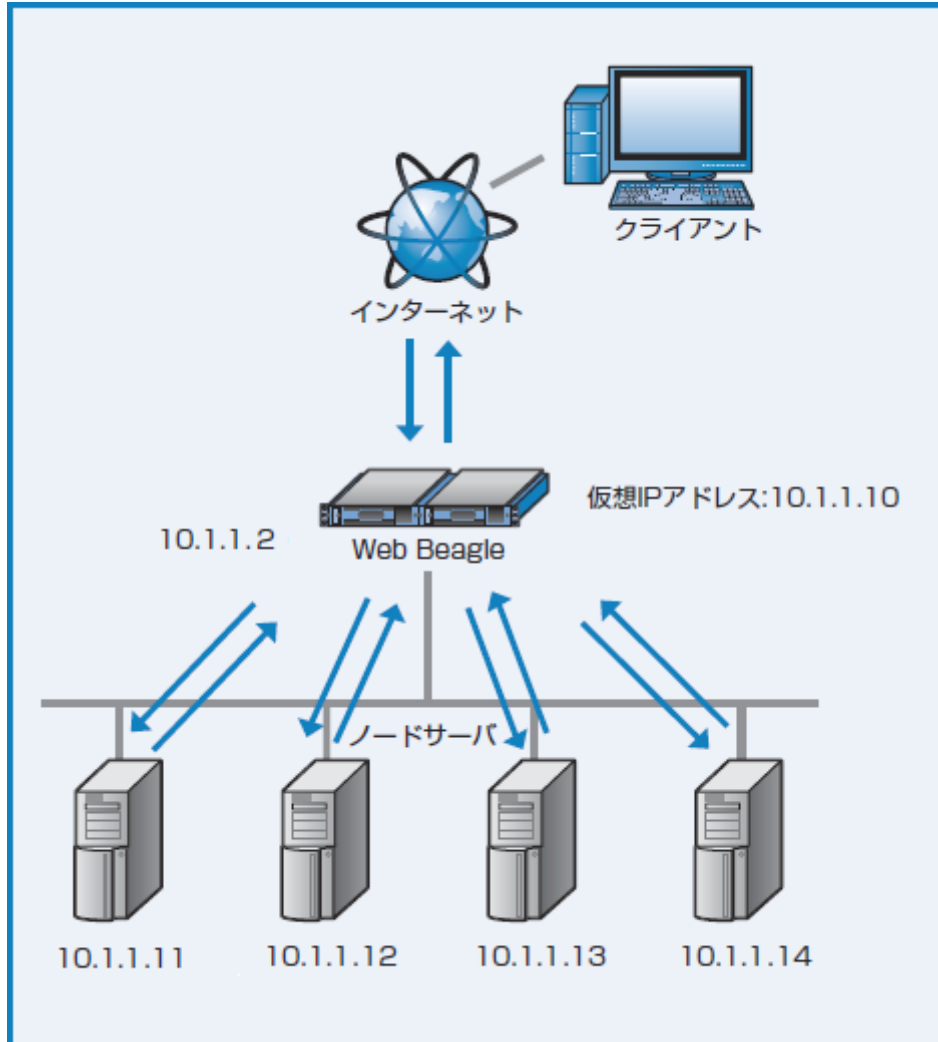


図2-3 透過型のネットワーク構成

分散方式について

Web Beagle ではL4の負荷分散とL7の負荷分散をサポートしています。

またL4の場合、負荷分散するトランスポートプロトコルをTCP、UDPから選択することができます。システム環境に合わせて最適な分散方式を選択してください。

ラウンドロビン（L4, L7）

各サーバに均等にリクエストを振り分ける方式です。ラウンドロビン方式は、次のようなシステム構成で効果的な方式となります。

- 各ノードサーバの処理能力が同じ。
- サイトの構成がhtml など静的なコンテンツが中心である。

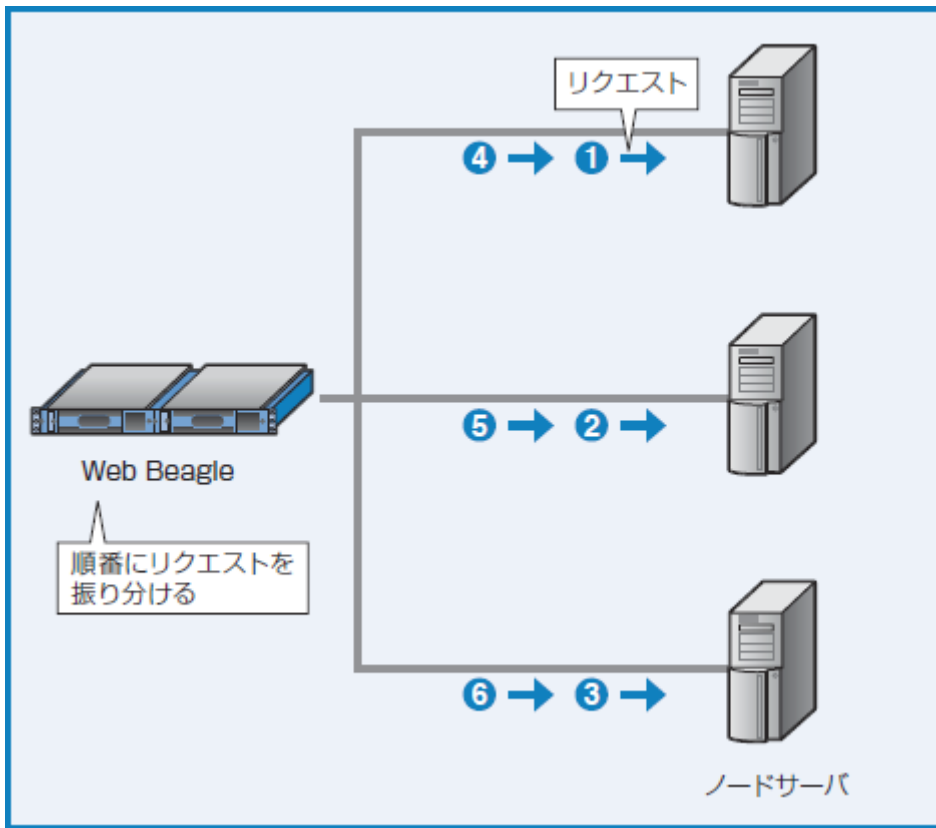


図2-4 ラウンドロビン

重み付けラウンドロビン (L4, L7)

サーバに優先順位を付け、その割合にしたがって、リクエストを振り分ける方式です。

例として、ノードサーバA、B、Cにおいて、サーバBはサーバAの2倍の処理能力、サーバCはサーバAの3倍の処理能力がある場合、各ノードサーバへの重み付けをA : B : C = 1 : 2 : 3 と設定することでサーバ負荷を均一にすることができます。次のようなシステム構成で効果的な方式となります。

- ノードサーバの処理能力に差がある。
- サイトの構成がhtml など静的なコンテンツが中心である。

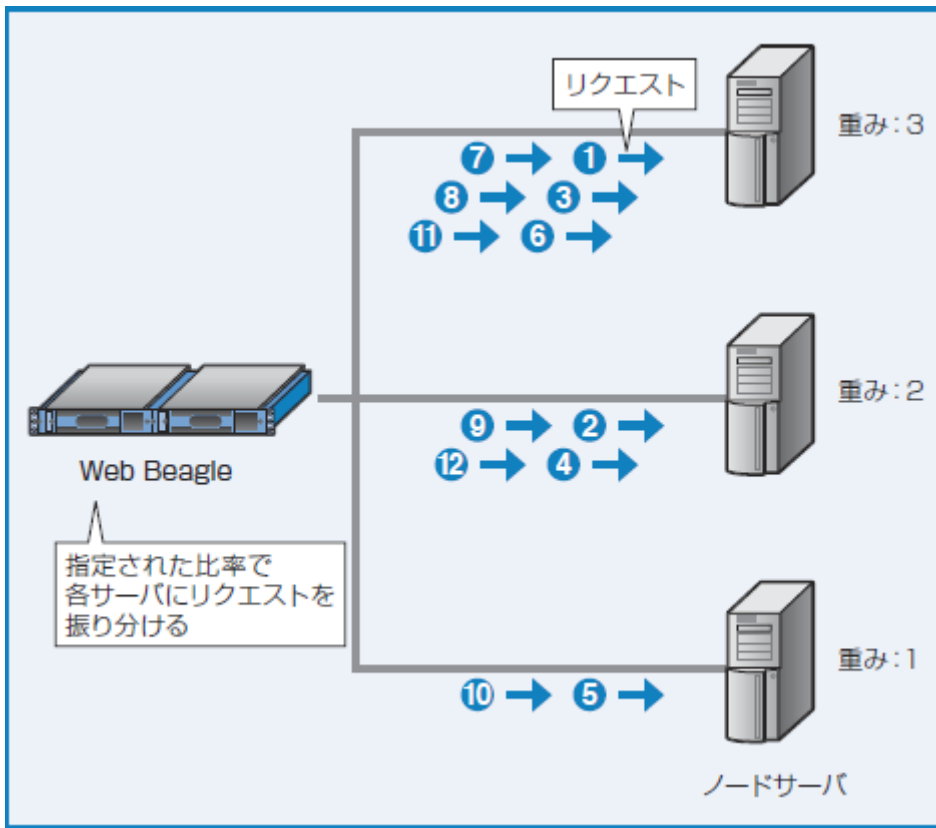


図2-5 重み付けラウンドロビン

最小コネクション (L4 のみ)

Web Beagle が各ノードサーバのコネクション状況を常に管理し、コネクション数が最も少ないサーバに振り分ける方式です。次のようなシステム構成で効果的な方式となります。

- 各ノードサーバの許容される同時接続数がほぼ同じ。
- サイトの構成がWeb アプリケーションなど動的なコンテンツ中心である。

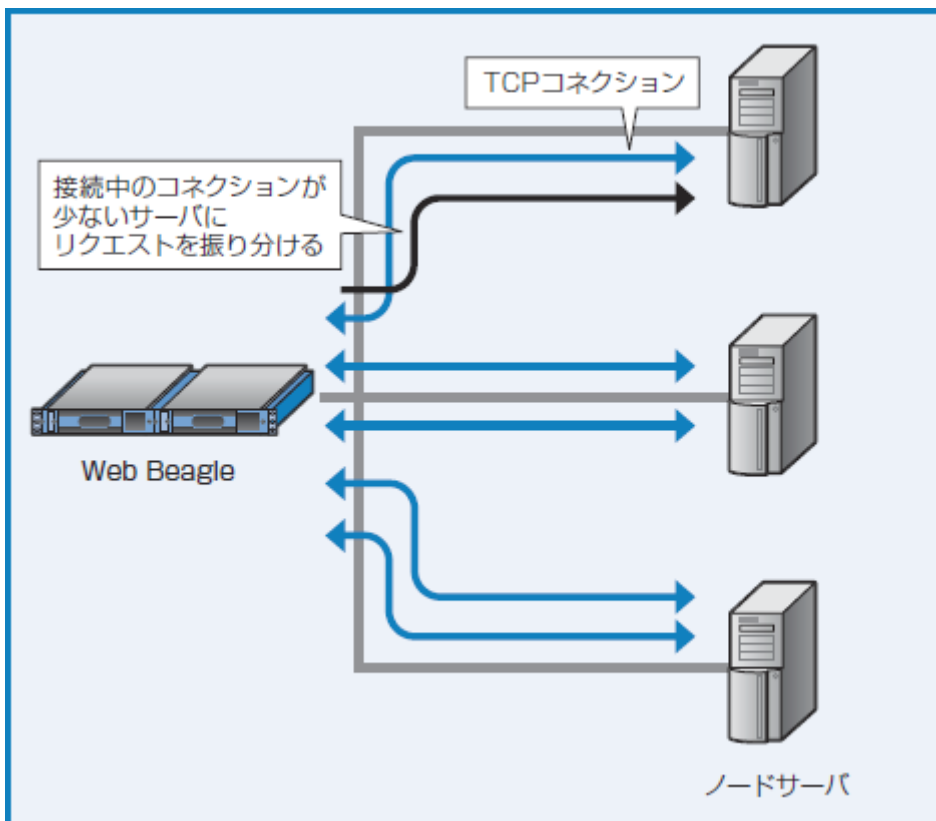


図2-6 最小コネクション

重み付け最小コネクション (L4 のみ)

Web Beagle が各ノードサーバのコネクション状況を常に管理し、コネクション数と各サーバの重み付けより最適なサーバに振り分ける方式です。次のようなシステム構成で効果的な方式となります。

- ノードサーバで許容される同時接続数が異なる。
- サイトの構成がWeb アプリケーションなど動的なコンテンツ中心である。

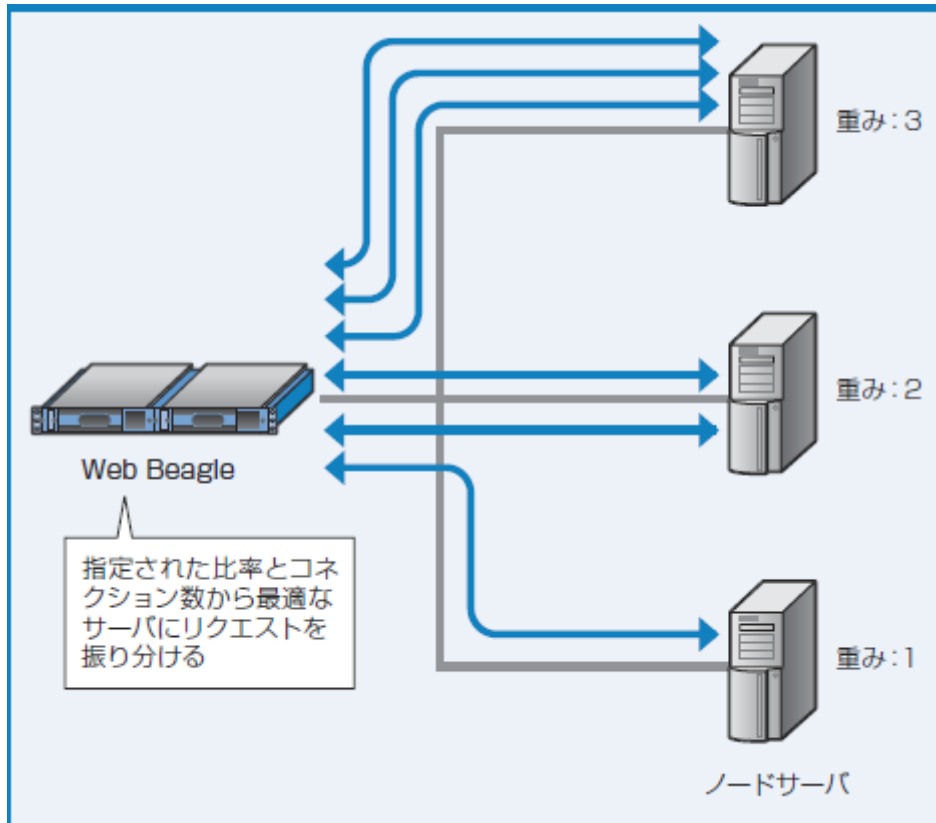


図2-7 重み付け最小コネクション

最大接続数以下同一サーバー (L7 のみ)

ノードサーバに設定した最大接続数を超過しない限り同一のノードサーバに振り分ける方式です。次のようなケースに効果的な方式となります。

- 低負荷の場合はノードサーバの電源をOFFにするなどしてノードサーバの数をできるだけ抑えたい。
- IMAPやRDPといった長いセッションの場合。

ソースハッシング (L4, L7)

接続元のIP アドレスから算出したハッシュテーブルに従って、次回同じIP アドレスからアクセスがあった場合、前回と同じノードサーバに振り分ける方式です。

keep-alive (接続維持) 機能と似ていますが、keep-alive は前回接続時から一定期間の接続を維持するのに対して、この方式はIP アドレスが同じであれば、常に同じノードサーバに振り分けます。

最速応答時間 (L4 のみ)

Web Beagle が各ノードサーバのコネクション状況を鑑み、パケットの遅延が最小と思われるノードサーバ、つまりもっとも応答速度が速いノードサーバに振り分ける方式です。最小コネクションと似ていますが、そちらは接続数で振り分けるのに対し、こちらは応答速度で振り分けま
す。最小コネクションと同様に次のようなシステム構成で効果的な方式となります。

- ノードサーバで許容される同時接続数が異なる。
- サイトの構成がWeb アプリケーションなど動的なコンテンツ中心である。

URIハッシング (L7 のみ)

URIから算出したハッシュテーブルにより、同じURIなら同じノードサーバに振り分ける方式です。この方式はプロキシサーバ向けです。

❗ クエリ文字列はURIに含みません。

2. 初期設定

Web Beagle の工場出荷時は、次のようにネットワークが設定されています。

- **動作方式**
DSR型
- **IP アドレス**
192.168.1.1
- **ネットマスク**
255.255.255.0
- **ゲートウェイ**
192.168.1.254

次のいずれかの方法でネットワークの設定を行ってください。メンテナンスPC を利用した方法では、ネットワーク以外の項目についても設定可能ですので、こちらの方法を推奨します。

2-1. メンテナンスPC を利用して設定する (推奨)

- **必要機器**
 - Web ブラウザ (Internet Explorer またはFirefox) が使用できるメンテナンスPC (Windows ノートPC など)
 - LAN ケーブルまたはHUB

1. Web Beagle とメンテナンスPC の接続

Web Beagle の初期設定用ポートとメンテナンスPCを、LAN ケーブルを使用して接続します。 Model 400/500 はポート1、 Model 600はポート3(Bonding左側)が初期設定用ポートとなります。

図2-8 のような状態となります。

HUB とLAN ケーブルを使用してWeb Beagle とメンテナンスPC それぞれを接続する方法でもかまいません (図2-9)。この場合、HUB にWeb Beagle、メンテナンスPC 以外を接続しないようにご注意ください。

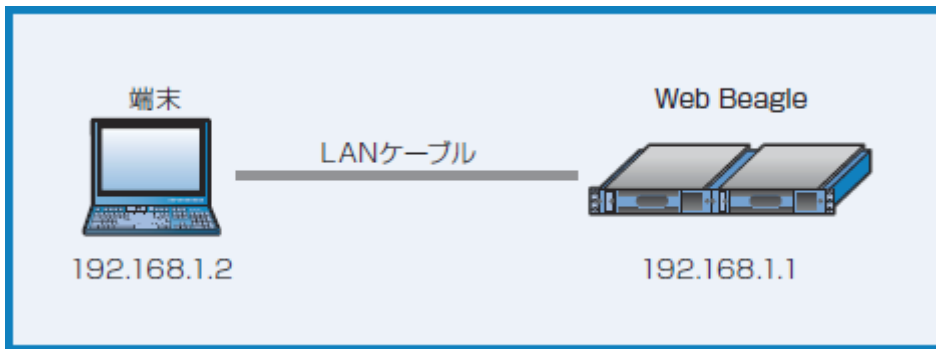


図2-8 メンテナンス端末との接続

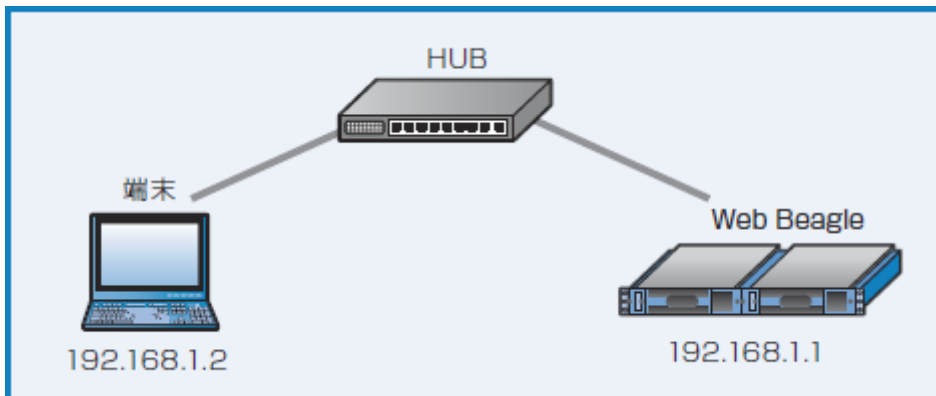


図2-9 HUB 接続時

2. メンテナンスPC のネットワーク設定

Web Beagle の工場出荷時のネットワーク設定は192.168.1.1 / 255.255.255.0 となっています。メンテナンスPC のネットワークを次のように設定します。

- **IP アドレス**
192.168.1.1
- **ネットマスク**
255.255.255.0
- **ゲートウェイ**
192.168.1.254 (任意)

3. Web Beagle の電源投入

Web Beagle のコンセントを電源に接続し、電源スイッチを押下します。

4. 管理画面へアクセス

メンテナンスPC 上のWeb ブラウザにて次のURL を開きます。

<https://192.168.1.1:18180/> (<https://192.168.1.1:18180/>)

図2-10 のログイン画面が表示されます。

電源投入後、システムが起動するまで約1 分程度の時間をおいてから、Web ブラウザによる接続を行ってください。

工場出荷時のログインIDおよび初期パスワードは、装置に添付されているシートのWeb 管理画面のログインID、パスワードを入力してください。



Copyright © 2016 A.T.WORKS, Inc.
All Rights Reserved.

図2-10 ログイン画面

❗ 図2-10 のログイン画面が表示されない場合は、次の確認を行ってください。

- Web Beagle が電源投入されているか（電源ランプの確認）
- Web Beagle とメンテナンスPC、HUB がケーブルでしっかり結線されているか
- メンテナンスPC のネットワーク設定が正しいか
- 入力したURL が正しいか

Web Beagle のネットワーク設定が変更されている場合、このURLでは接続ができません。

Web Beagle のネットワーク設定が不明な場合は、コンソール接続を利用してネットワークの再設定を行ってください。

5. ネットワーク設定

「2章 - ネットワーク構成例 (./chapter_2.html#ネットワーク構成例)」を参考にネットワーク設定を行います。

【基本設定】 → 【ネットワーク】 を選択します。

Model 500, Model 600

- 設置するシステム構成にあわせて動作方式を選択します。
- ネットワーク（IP アドレス、ネットマスク、ゲートウェイ）を設定します。
- 動作方式がNAT 型の場合、LAN 側のネットワークについても設定します。

Model 400

- ネットワーク（IP アドレス、ネットマスク、ゲートウェイ）を設定します。

⚠ ネットワークの編集については「5章 - ネットワーク (./chapter_5.html#ネットワーク)」を参照してください。

6. パスワード変更

工場出荷時は初期パスワードのため、必ずパスワード変更を行ってください。

【アクセス制限】 → 【パスワード変更】にてパスワード変更を行います。

☞ 管理者パスワードの変更については「5章 - パスワード変更 (./chapter_5.html#パスワード変更)」を参照してください。

7. 接続許可IPアドレスの制限

工場出荷時はどのIP アドレスからも管理画面への接続を許可する状態です。管理画面への接続のセキュリティを高めるため、接続を許可するIP アドレスを設定して制限することをお勧めします。

【アクセス制限】→【接続許可IP アドレス】にてWeb Beagle の管理画面への接続を許可するIP アドレスの制限を行います。接続許可IP アドレスの登録が無い場合は、IP アドレスによる制限は働きませんが、1 件以上登録されているときには、登録IP アドレス以外からの接続はできなくなります。

☞ 接続元IP アドレスの制限については「5章 - 接続許可IP アドレス (./chapter_5.html#接続許可ip-アドレス)」を参照してください。

8. Web Beagle の停止と設置

Web Beagle の電源ボタンを押して電源を切ります。

Web Beagle を使用するネットワークに設置し電源を入れると、設定したIP アドレスで起動します。

Web ブラウザでWeb Beagle に設定したIP アドレスを指定して管理画面を開き、設定を続けます。

https://【Web Beagle に設定したIP アドレス】:18180/

❗ Web Beagleがハングアップして応答がなくなってしまった場合、電源ボタンを長押し（4 秒程度）して電源を切ってください。

2-2. コンソール接続を利用して設定する

コンソール接続の場合、設定できるのは、ポート1インターフェイスのIPアドレス、ネットマスク、デフォルトゲートウェイのみになります。

コンソール接続による設定を行った後、メンテナンスPC を使用してWeb ブラウザからその他の項目の設定を行う必要があります。

• 必要機器

- モニタ (D-sub 15 ピン VGA 端子)
- キーボード (USB A 端子)

1. Web Beagle と機器の接続

Web Beagle のD-sub 端子にモニタを接続します。

Web Beagle のUSB 端子にキーボードを接続します。

2. Web Beagle の電源投入

Web Beagle のコンセントを電源に接続し、電源スイッチを押下します。

モニタにログインプロンプトが表示されますのでログインID とパスワードを入力します。

このログインID およびパスワードは、装置に添付されているシートのコンソールログインID、パスワードを入力してください。

❗ このログインID とパスワードはWeb Beagle の管理画面へのログインID、パスワードとは異なります。変更することはできません。

3. ネットワーク設定

ログインに成功するとメニューが表示されますので、ネットワーク設定を選択します。

本設定で設定可能な項目は、LAN1 ネットワークの次の項目に限定されます。

- IP アドレス
- ネットマスク
- ゲートウェイ

上記以外の設定項目はネットワーク設定後、メンテナンスPC を使用してWeb ブラウザから設定してください。

☞ コンソール管理からネットワーク設定を変更する方法は「6章 - コンソール管理 (./chapter_6.html#コンソール管理)」を参照してください。

4. Web Beagle の停止と設置

Web Beagle の電源ボタンを押し、電源を切ります。Web Beagle を使用するネットワークに設置し、電源を入れると設定したIP アドレスで起動します。Web ブラウザで次のURL を開き、設定を続けます。

https://【Web Beagle に設定したIP アドレス】:18180/

❗ 本手順では、管理者パスワードの変更、接続元IP アドレスの制限は行われておりません。

Web Beagle を使用するネットワークに設置後、Web ブラウザより管理画面にログインし、管理者パスワードの変更、接続元IP アドレスの制限を実施してください。

☞ 管理者パスワードの変更方法については「5章 - パスワード変更 (./chapter_5.html#パスワード変更)」を参照してください。

☞ 接続元IP アドレスの制限については「5章 - 接続許可IP アドレス (./chapter_5.html#接続許可ip-アドレス)」を参照してください。

ネットワーク構成例

DSR 型

DSR 型は図2-11 のようなネットワーク構成の場合に使用します。

❗ ネットワーク構成例のIP アドレスに便宜上、10.1.1.0/24 のネットワークのIP アドレスを使用しております。

✍ DSR 型では、Web Beagle はModel400/500ではポート1インターフェースのみ、Model 600でボンディングする場合はポート1とポート3(Bonding左側)を使用します。Model 600でボンディングしない場合はポート3(Bonding左側)のみを使用します。Web Beagle やノードサーバのIP アドレスは、同一ネットワークに属するIP アドレスとなります。

設定例

この例の場合、Web Beagle のネットワークを次のように設定します。

- **動作方式**
DSR型
- **IP アドレス**
10.1.1.2
- **ネットマスク**
255.255.255.0
- **ゲートウェイ**
10.1.1.1

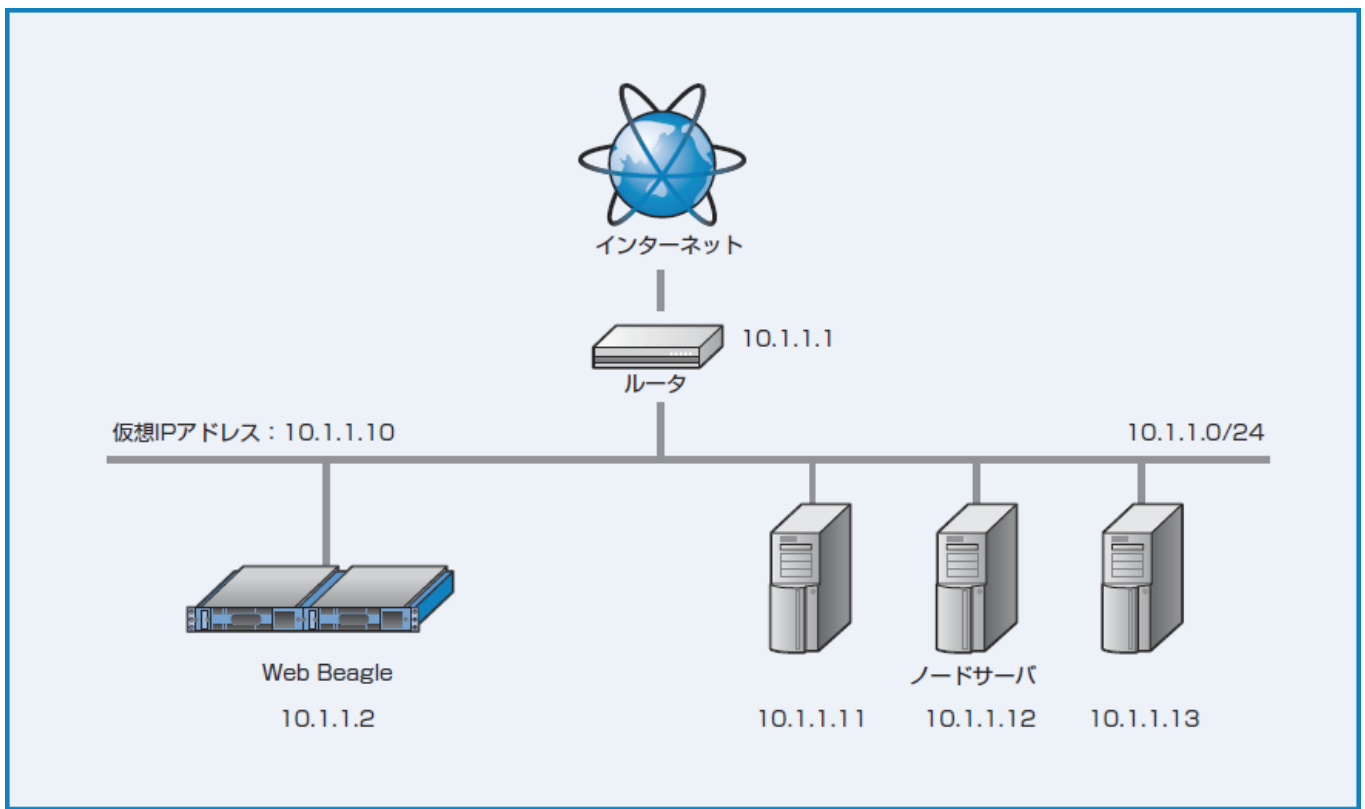


図2-11 DSR 型ネットワーク構成例

ノードサーバのIP アドレスには、ポート1 (Model 600 でボンディングする場合ポート3も使用) のネットワーク (この例の場合10.1.1.0/24) に属するIP アドレスを設定する必要があります。

❗ DSR 型の場合、各ノードサーバに仮想IP アドレス宛の接続を受け付けるように設定する必要があります。

ノードサーバに仮想IP アドレス宛の接続を受け付ける設定については「2章 - DSR 型における仮想IP アドレス宛の接続を受け付ける設定 (.chapter_2.html#dsr-型における仮想ip-アドレス宛の接続を受け付ける設定)」を参照してください。

NAT 型 (Model 500, Model 600)

NAT 型は図2-12 のようなネットワーク構成の場合に使用します。

✍ NAT 型の場合、Model 500 ではポート1、ポート2 インターフェイスはそれぞれ別のネットワークに接続します。Model 600 でボンディングする場合はポート1とポート3(Bonding左側)、ポート2とポート4(Bonding右側) の組み合わせでそれぞれ別のネットワークに接続します。Model 600 でボンディングしない場合はポート3(Bonding左側)、ポート4(Bonding右側) インターフェイスをそれぞれ別のネットワークに接続します。ポート2、ポート4 は通常、プライベートIP アドレスのネットワークを使用します。ノードサーバのデフォルトゲートウェイはポート2 インターフェイスのIP アドレスとします。

設定例

この例の場合、Web Beagle のネットワーク(ポート1)を次のように設定します。

- **動作方式**
NAT 型
- **IP アドレス**
10.1.1.2
- **ネットマスク**
255.255.255.0

- **ゲートウェイ**
10.1.1.1

この例の場合、Web Beagle のネットワーク(ポート2)を次のように設定します。

- **IP アドレス**
192.168.1.1
- **ネットマスク**
255.255.255.0

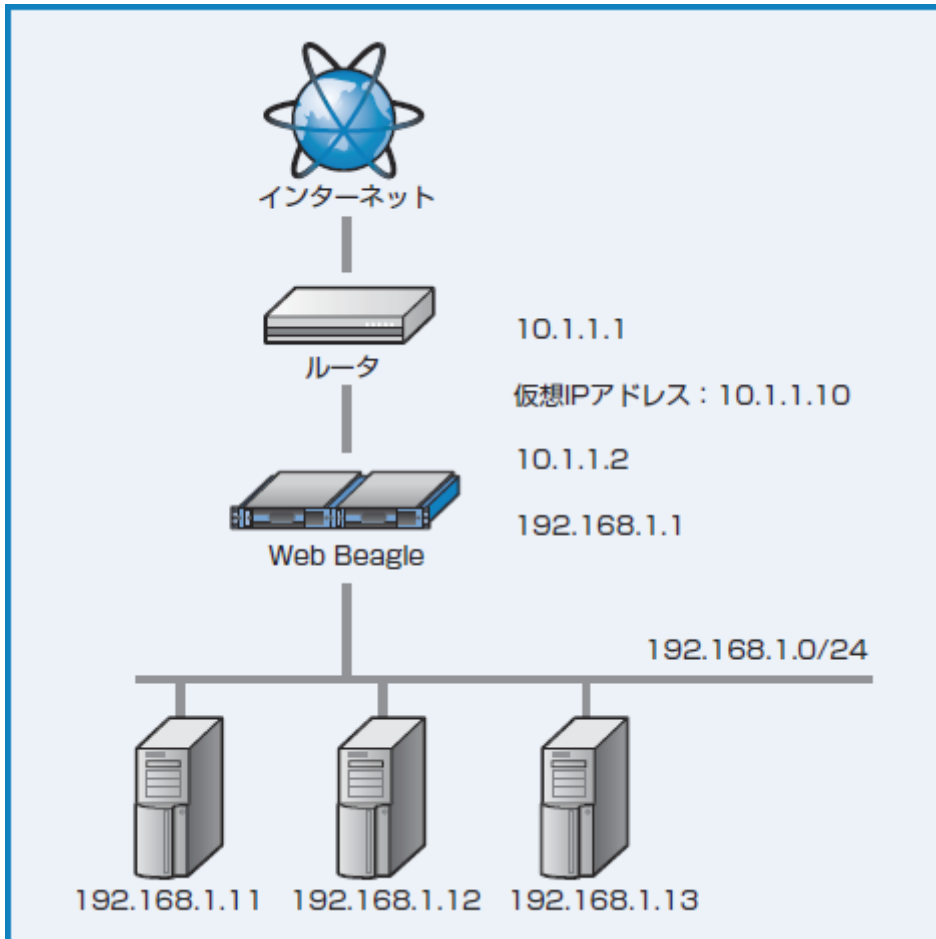


図2-12 NAT 型のネットワーク構成例

透過型 (Model 500, Model 600)

透過型は図2-13 のようなネットワーク構成の場合に使用します。

✂ 透過型では Model 500 の場合はポート2側がノードサーバが接続されるネットワークとなります。 Model 600 でボンディングする場合はポート2およびポート4(Bonding右)側がノードサーバが接続されるネットワークとなります。 Model 600 でボンディングしない場合はポート4(Bonding右)側がノードサーバが接続されるネットワークとなります。一方、外側ネットワークについては、Model 500 ではポート1には外側のネットワークと接続しているルータ等を接続します。 Model 600 でボンディングする場合はポート1およびポート3(Bonding左側)の組み合わせで外側ネットワークと接続します。 Model 600 でボンディングしない場合はポート3(Bonding左側)を外側ネットワークと接続します。

Web Beagle やノードサーバのIP アドレスは、同一ネットワークに属するIP アドレスとなります。

設定例

この例の場合、Web Beagle のネットワークを次のように設定します。

- **動作方式**
透過 型

- IP アドレス
10.1.1.2
- ネットマスク
255.255.255.0
- ゲートウェイ
10.1.1.1

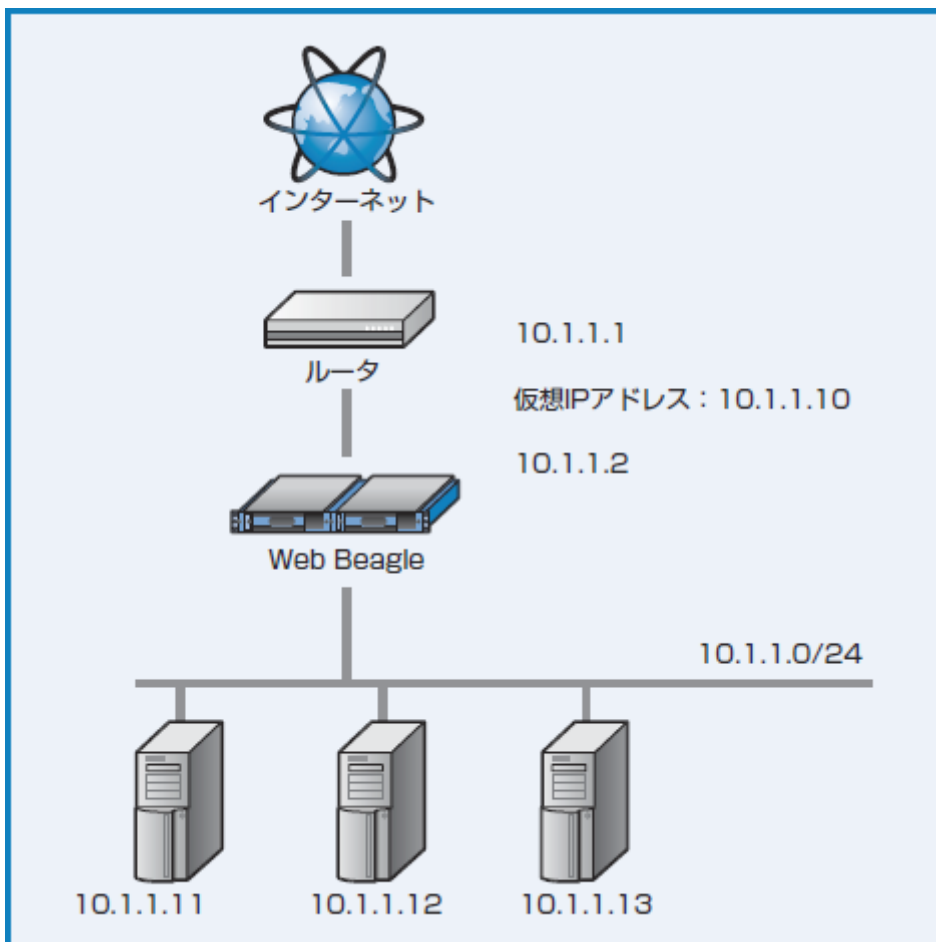


図2-13 透過型のネットワーク構成例

DSR 型における仮想IP アドレス宛の接続を受け付ける設定

ネットワーク構成がDSR 型の場合、各ノードサーバに仮想サービスのIP アドレスを受け取る設定が必要となります。

❗ ネットワークの構成変更により、仮想IP アドレスが変更になった場合も本手順を実施する必要があります。

設定例 1 OS がLinux の場合

以下のコマンドを実行します。

```
# iptables -t nat -A PREROUTING -d 仮想IP アドレス -j REDIRECT
```

ネットワーク構築例 (図2-11) の場合は、以下のコマンドを実行します。

```
# iptables -t nat -A PREROUTING -d 10.1.1.10 -j REDIRECT
```

設定例 2 OS がWindows Server 2008 の場合

1. ループバックデバイスを追加する

✎ ループバックデバイスがすでに追加されている場合は、次の手順へおすすみください。

1. 「スタート」 ボタンをクリックし、「コントロール パネル」 をクリックします。
2. クラシック表示を使用している場合は、左側のウィンドウで【コントロールパネル】 の下の「カテゴリの表示に切り替える」 をクリックします。
3. 「プリンタとその他のハードウェア」 をクリックします。
4. 左側のウィンドウにある【関連項目】 の下の「ハードウェアの追加」 をクリックし、「次へ」 をクリックします。
5. 「はい、ハードウェアを接続しています」 をクリックし、「次へ」 をクリックします。
6. 一覧の最後にある「新しいハードウェアデバイスの追加」 をクリックし、「次へ」 をクリックします。
7. 「一覧から選択したハードウェアをインストールする（詳細）」 をクリックし、「次へ」 をクリックします。
8. 「ネットワーク アダプタ」 をクリックし、「次へ」 をクリックします。
9. 【製造元】 ボックスの一覧の「Microsoft」 をクリックします。
10. 【ネットワークアダプタ】 ボックスの一覧の「Microsoft Loopback Adapter」 をクリックし、「次へ」 をクリックします。
11. 「次へ」 をクリックします。
12. 「完了」 をクリックします。

2. ループバックデバイスを設定する

1. 「スタート」 ボタンをクリックし「コントロールパネル」 をクリックします。
2. 「ネットワーク接続」 をクリックします。
3. デバイス名が「Microsoft Loopback Adapter」 の接続を右クリックし、プロパティを開きます。
4. インターネットプロトコル (TCP/IP) のプロパティを開きます。
5. 【次のIP アドレスを使う】 を選択し、IP アドレスに、仮想 IPアドレスを設定し「OK」 をクリックします (図2-14)

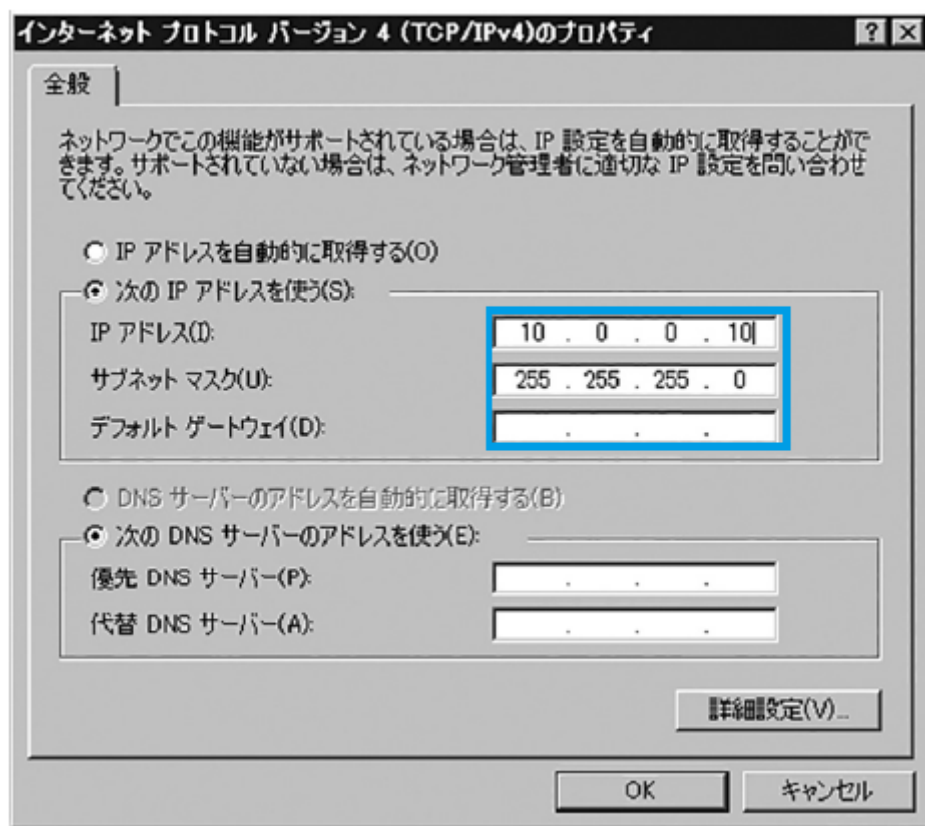


図2-14 インターネットプロトコル (TCP/IP) のプロパティ

3. ループバックデバイスを設定する

コマンドプロンプト上で下記のコマンドを実施してください。

```
C:¥> netsh interface ipv4 set interface "Local Area Connection" weakhostreceive=enabled
C:¥> netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
C:¥> netsh interface ipv4 set interface "loopback" weakhostsendsend=enabled
```

❗ “Local Area Connection” と “loopback” の部分は、お客様環境のネットワークデバイス名に置き換えてご変更ください。

Windows Server 日本語版だと “Local Area Connection” は「ローカルエリア接続」などで表記されております。

コントロールパネルから、「ネットワークとインターネット」→「ネットワーク接続」にて名前を確認してください。

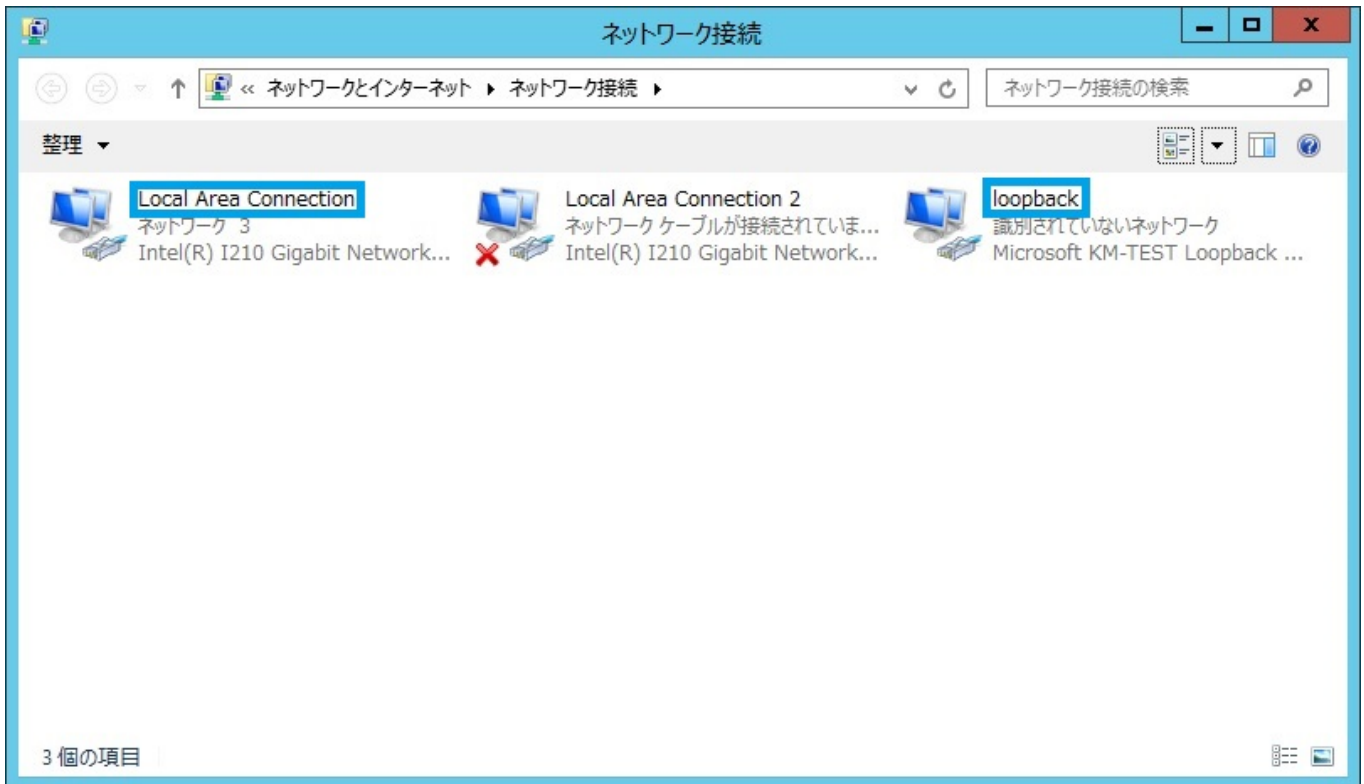


図2-14-1 ネットワーク接続の一例 青枠で囲まれたデバイス名を設定する

設定例 3 OS が Windows Server 2012 の場合

1. ループバックデバイスを追加する

✍ ループバックデバイスがすでに追加されている場合は、次の手順へおすすみください。

1. 「スタート」 ボタンをクリックし、「コンピューターの管理」 をクリックします。
2. 【コンピューターの管理】内の「デバイスマネージャー」 をクリックします。
3. 「デバイスマネージャー」 ツリーを右クリックして「レガシハードウェアの追加」 をクリックします。
4. ハードウェアの追加ウィザードが表示されます、「次へ」 をクリックします。
5. インストール方法を選んでくださいと表示されるので、「一覧から選択したハードウェアをインストールする」 にチェックを入れ「次へ」 をクリックします。
6. インストールするハードウェアの種類が表示されるので一覧から「ネットワークアダプター」 を選択し、「次へ」 をクリックします。
7. ネットワークアダプターを選択します、製造元を「Microsoft」、ネットワークアダプターを「Microsoft KM-TEST Loopback Adapter」 を選択し「次へ」 をクリックします。
8. インストールを開始しますと表示されるので「次へ」 をクリックします。
9. 「完了」 をクリックします。

2. ループバックデバイスを設定する

1. 「スタート」を右クリックし「コントロールパネル」をクリックします。
2. 「ネットワークとインターネット」をクリックします。
3. 「ネットワークの状態とタスクの表示」をクリックします。
4. デバイス名が「Microsoft KM-TEST Loopback Adapter」をクリックしプロパティを開きます。
5. インターネットプロトコルバージョン4（TCP/IP）のプロパティを開きます。
6. 【次のIP アドレスを使う】を選択し、IP アドレスに、仮想IP アドレスを設定し、「OK」をクリックします（図2-15）

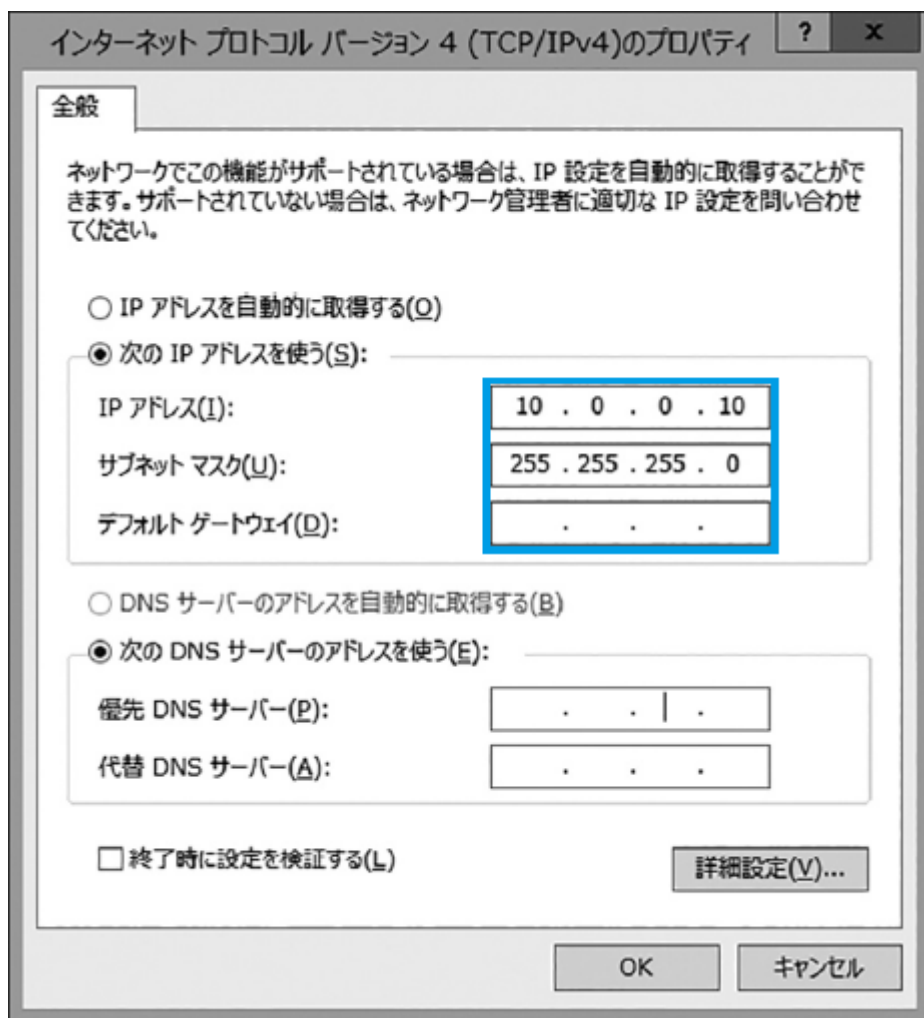


図2-15 インターネットプロトコル（TCP/IP）のプロパティ

3. ループバックデバイスを設定する

コマンドプロンプト上で下記のコマンドを実施してください。

```
C:¥> netsh interface ipv4 set interface "Local Area Connection" weakhostreceive=enabled  
C:¥> netsh interface ipv4 set interface "loopback" weakhostreceive=enabled  
C:¥> netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

❗ “Local Area Connection” と “loopback” の部分は、お客様環境のネットワークデバイス名に置き換えてご変更ください。

Windows Server 日本語版だと“Local Area Connection” は「ローカルエリア接続」などで表記されております。

コントロールパネルから、「ネットワークとインターネット」→「ネットワーク接続」にて名前を確認してください。

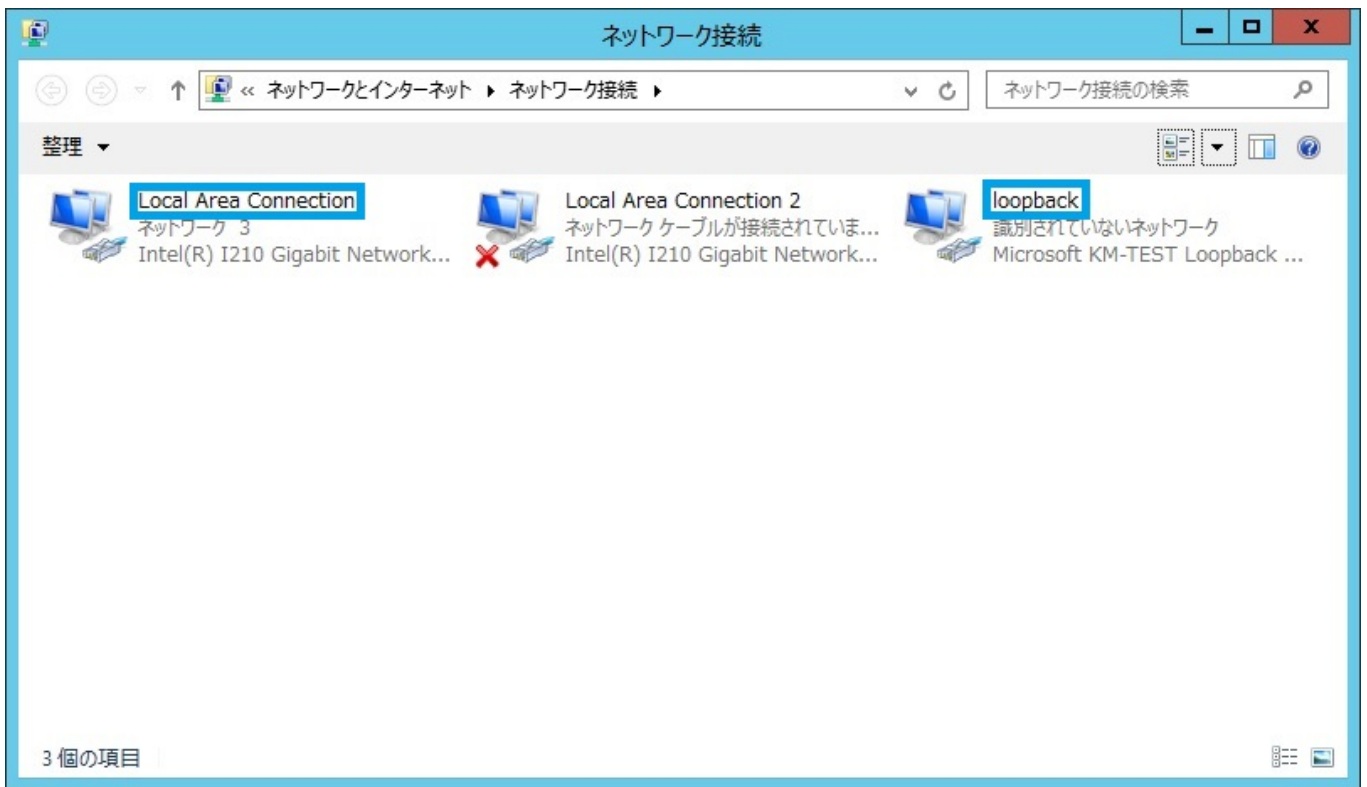


図2-15-1 ネットワーク接続の一例 青枠で囲まれたデバイス名を設定する

4. 仮想サービスの設定

仮想サービスの設定について、図2-12 DSR 型ネットワーク構成でTCPのポート80上の通信をL4負荷分散をする場合を例として説明いたします。説明中のIP アドレスも図2-12 の場合と同様の例で説明いたしますが、実際に使用するIP アドレスを設定してください。他のネットワーク構成の場合でも設定項目に違いはありません。

1. Web Beagle の管理画面にログインし 【L4負荷分散】 → 【L4仮想サービス】 を選択し「追加」ボタンをクリックします。（図2-16）



2. 仮想サービス追加の欄に次のように入力し「入力内容確認」ボタンをクリックします。（図2-17）

- 仮想IPアドレス
10.1.1.10
- ポート
80

- **プロトコル**
TCP
- **分散方式**
ラウンドロビン
- **待機サーバー**
- **バーチャルホスト名**
- **セッション維持**
ON 300 秒
- **有効**
有効
- **アクセス制限**
無効

分散方式については「2章 - 分散方式について (./chapter_2.html#分散方式について)」を参照してください。

L4ロードバランサ設定

仮想サービス追加/編集

仮想IPアドレス *	<input type="text" value="10.1.1.10"/>
ポート *	<input type="text" value="80"/>
プロトコル *	<input type="text" value="TCP"/>
分散方式 *	<input type="text" value="ラウンドロビン"/>
待機サーバ	<input type="text"/> : <input type="text" value="80"/>
バーチャルホスト名	<input type="text"/>
セッション維持	<input type="text" value="ON"/> <input type="text" value="300"/> 秒
有効 *	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
アクセス制限 *	<input type="text" value="無効"/>

キャンセル

入力内容確認

②

3. 入力した内容が図2-18 のように表示されます。問題がなければ「追加/編集」ボタンをクリックします。

L4ロードバランサ設定

仮想サービス追加/編集

仮想IPアドレス * 10.1.1.10
ポート * 80
プロトコル * TCP
分散方式 * ラウンドロビン
待機サーバ
バーチャルホスト名
セッション維持 ON: 300 秒
有効 * 有効
アクセス制限 * 無効

キャンセル

追加/編集

③

4. 仮想サービスが追加されると図2-19のように仮想サービスの詳細画面に遷移します。次に仮想サービスにノードサーバの追加するため「追加」ボタンをクリックします。

L4ノードサーバ設定

L4仮想サービス

編集

仮想IPアドレス * 10.1.1.10
ポート * 80/TCP
分散方式 * ラウンドロビン
待機サーバ
バーチャルホスト名
セッション維持 300 秒
有効 有効
アクセス制限 無効

ノードサーバ一覧

リフレッシュ

追加

④

10 件表示

検索:

ノードサーバ 死活監視 有効 アクティブ接続数 非アクティブ接続数

データはありません。

0 件中 0 から 0 まで表示

先頭

前

次

最終

5. ノードサーバの情報を次のように入力し「適用」ボタンをクリックします。(図2-20)

- IPアドレス
10.1.1.11
- ポート
80
- 有効
チェック

- 死活監視

TCP

- 接続タイムアウト

5 秒

☞ 死活監視機能については「4章 - 死活監視機能 (/chapter_4.html#死活監視機能)」を参照してください。

ノードサーバ設定

ノードサーバ追加/編集

IPアドレス *	<input type="text" value="10.1.1.11"/>
ポート *	<input type="text" value="80"/>
有効	<input checked="" type="checkbox"/>
死活監視 *	<input type="text" value="TCP"/>
接続タイムアウト	<input type="text" value="5"/> 秒

⑤

6. 入力した内容が図2-21 のように表示されます。問題がなければ「追加/編集」ボタンをクリックします。

ノードサーバ設定

ノードサーバ追加/編集

仮想IPアドレス *	10.1.1.11
ポート *	80
重み付け *	10
有効	有効
死活監視	TCP
接続タイムアウト	5

⑥

7. ノードサーバが図2-22 のように一覧に追加されます。必要に応じてノードサーバーを追加してください。

❶ ノードサーバの死活監視は追加直後から開始されます。状態がDOWNになっている場合、死活監視設定の見直しおよびノードサーバの状態を確認してください。

L4ノードサーバ設定

処理が成功しました！

L4仮想サービス

編集

仮想IPアドレス * 10.1.1.10
ポート * 80/TCP
分散方式 * ラウンドロビン
待機サーバ
バーチャルホスト名
セッション維持 300 秒
有効 有効
アクセス制限 無効

ノードサーバ一覧

リフレッシュ

追加

10 件表示

検索:

ノードサーバ	死活監視	有効	アクティブ接続数	非アクティブ接続数	
10.1.1.11:80	TCP	YES	0	0	編集 無効 削除

1 件中 1 から 1 まで表示

先頭

前

1

次

最終

以上で仮想サービスの設定は完了です。

5. Web Beagle 設置時の注意事項

上位SW がSTP（Spanning Tree Protocol）をサポートしている場合

Web Beagle を接続する上位スイッチがSTP をサポートしている場合、 STP がWeb Beagle の冗長化機能の packets を妨げ、フェイルバック発生時に一定期間仮想サービスへの通信が行われなくなる問題が発生します。この問題を回避するため、以下のいずれかの対策を実施してください。

- 上位スイッチのSTP 機能を無効にする
- 上位スイッチのWeb Beagle を接続するポートに対してPort Fast を有効にする

L4 の仮想サービスに 1 台のノードサーバを複数仮想サービスに登録する場合

L4 の仮想サービスに 1 台のノードサーバを複数仮想サービスに登録する場合、 ノードサーバを無効にする操作をおこなうと仮想サービス単位ではなく、 無効操作をしたノードサーバが属している全ての仮想サービスで無効になります。

1 台のノードサーバを複数の仮想サービスに登録している場合、 特定の仮想サービスでのみ、無効にすることはできないのでご注意ください。

1 台のノードサーバを複数の仮想サービスに登録している場合に、 特定の仮想サービスでのみ無効にする場合は、 ノードサーバの登録自体を削除する方法をとる必要があります。

❗ 上記の現象はL4 負荷分散エンジンのLVS の仕様となります。
L7 の仮想サービスの場合は上記のような現象は発生しません。

第3章 冗長化構成

1. 冗長化構成のメリット

Web Beagle を導入することにより、ノードサーバの負荷分散を図るとともに、一部のノードサーバに障害が発生してもシステム全体の動作を継続できるという利点があります。

しかし、図3-1のような構成では、Web Beagle 部分が冗長化構成になっておらず、この部分に障害が発生した場合、サービスが停止してしまいます。

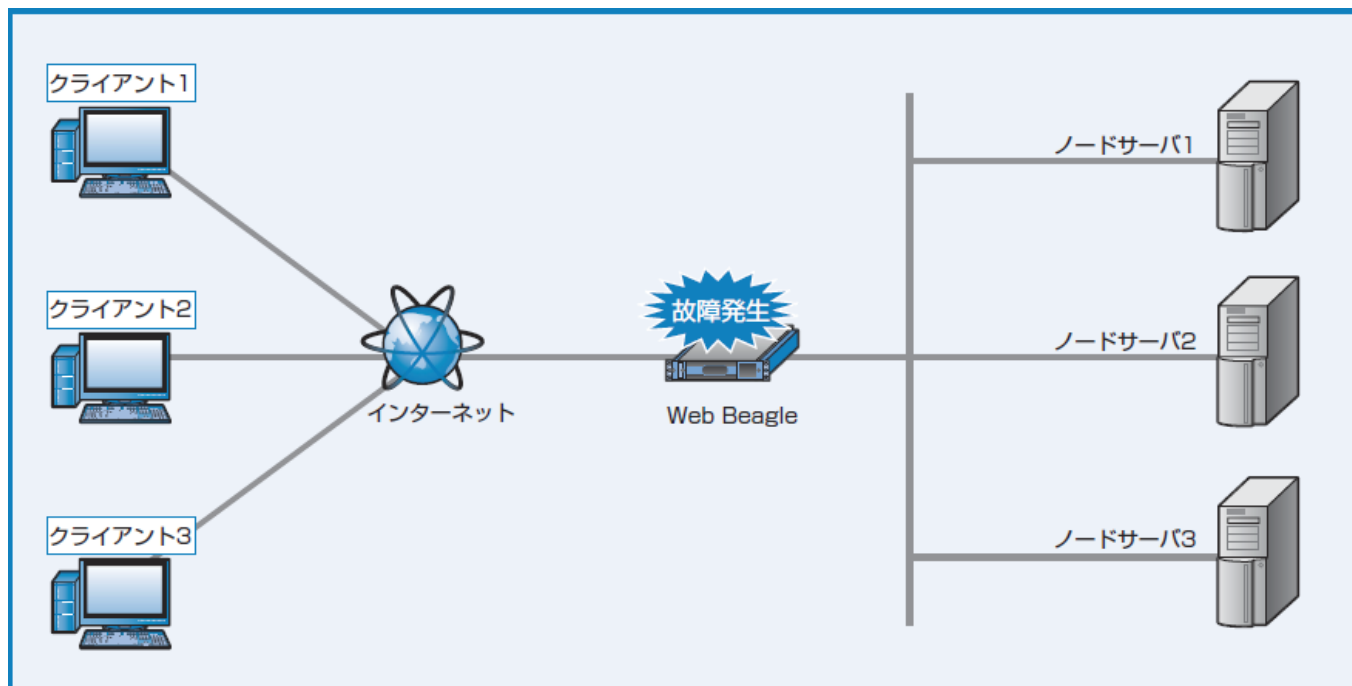


図3-1 単体構成のWeb Beagle 構成

Web Beagle は冗長化構成に対応していますので、同一の機種を2 台使用して冗長化構成を構築することができます。スタンバイ機はマスター機に障害が発生したことを検知すると、フェイルオーバーを行い、動作を継続します（図3-2）。

また、Web Beagle のメンテナンスなどを行う場合でも、動作の停止を最小限にとどめることができます。

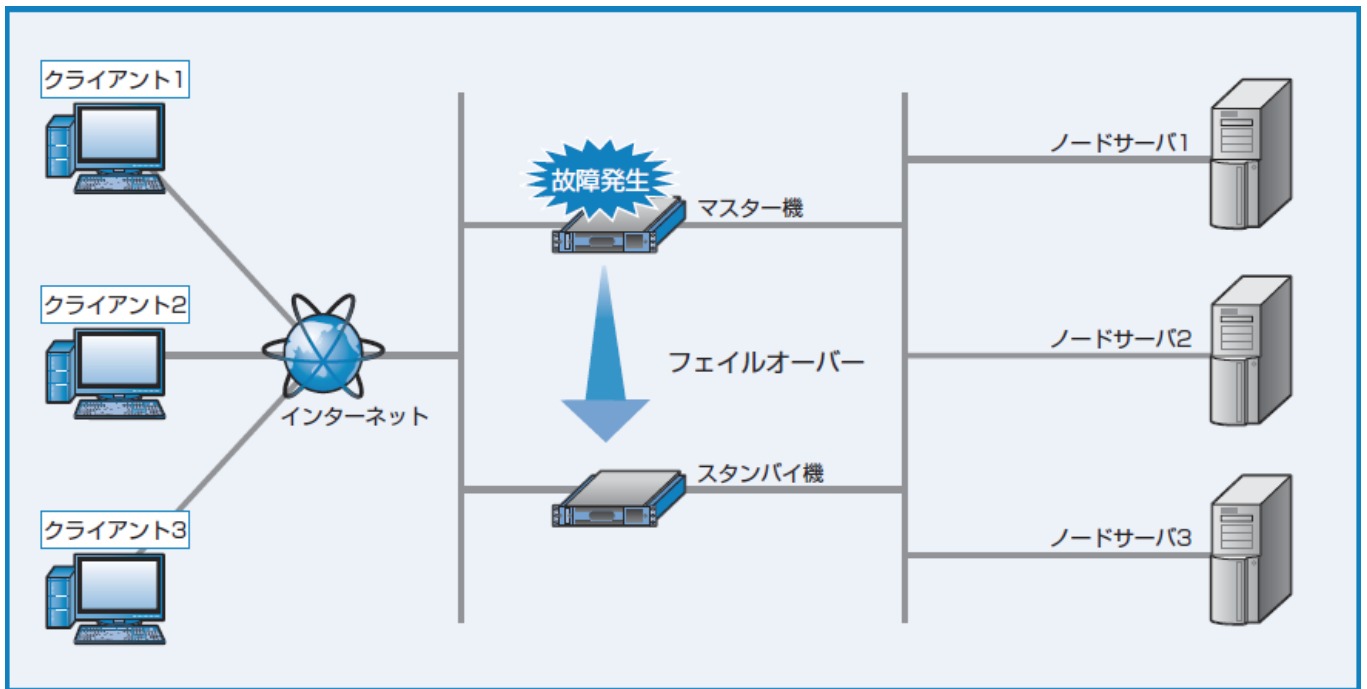


図3-2 冗長化構成のWeb Beagle 構成

Model 600 の場合は、ボンディングすることでネットワークポートの冗長化をすることも可能です。その場合はポート1 とポート3、ポート2 とポート4 がそれぞれペアになります。ボンディングのための特別な設定をする必要はありません。ペアとなるポートにどちらも接続されていれば自動的にボンディングされます。

2. 冗長化構成例

単体構成から冗長化構成への変更はWeb Beagle を2 台用意することでいつでも可能です。

ここでは2.3 章で導入したDSR 型のネットワーク構成に冗長化構成でWeb Beagle を導入する場合を例に説明します。DSR 型・NAT 型・透過型のいずれのネットワーク構成でも、冗長化構成を構築する手順は同一です。

1. DSR 型のセットアップ

「2章 - ネットワーク構成例 (./chapter_2.html#ネットワーク構成例)」に従い、まず図3-3 のようなDSR 型の構成を構築します。

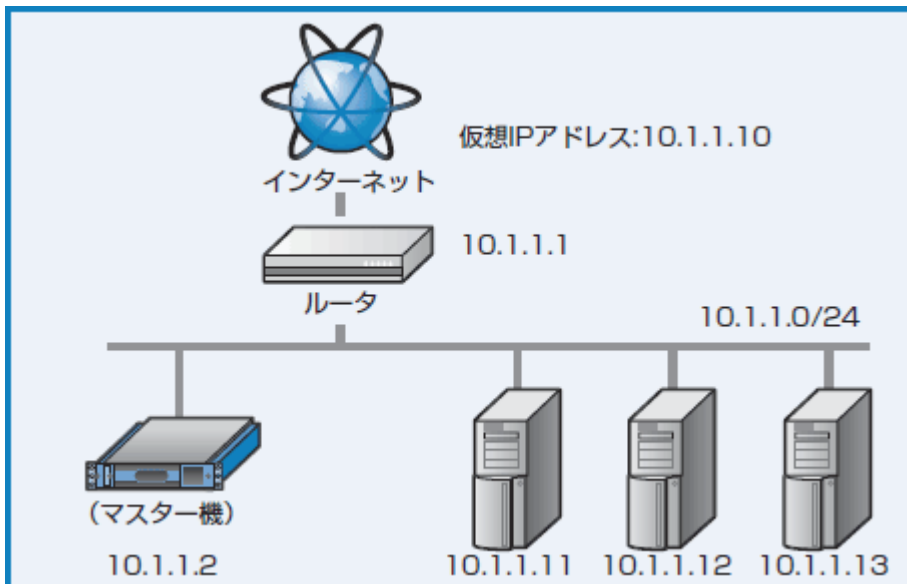


図3-3 DSR 型の単体構成

2. スタンバイ機の初期設定

「2章 - 初期設定 (./chapter_2.html#初期設定)」に従い、スタンバイ機のWeb Beagleの初期設定を行います。

本構成例では、スタンバイ機のIP アドレスは以下のように設定し、図3-4 のスタンバイ機の位置に、設置します。

- **動作方式**
DSR 型
- **IP アドレス**
10.1.1.3
- **ネットマスク**
255.255.255.0
- **ゲートウェイ**
10.1.1.1

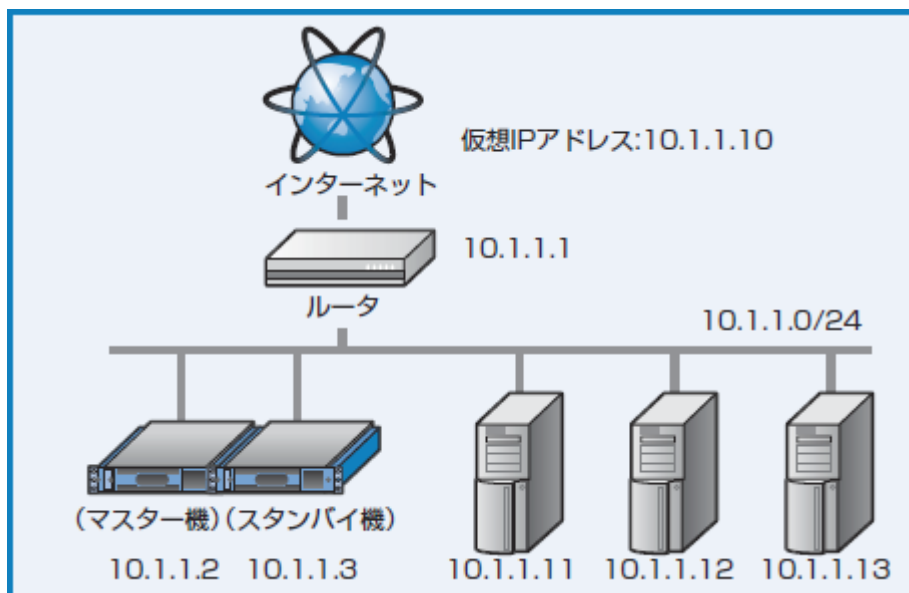


図3-4 DSR 型のHA 構成

3. マスター機の冗長化設定

現在、稼働しているWeb Beagle (10.1.1.2) をマスター機として動作するよう、冗長化構成の変更を行います。

Web Beagle (10.1.1.2) の管理画面にログインします。

【基本設定】 → 【冗長化設定】 を選択し、冗長化設定の「編集」を行います。

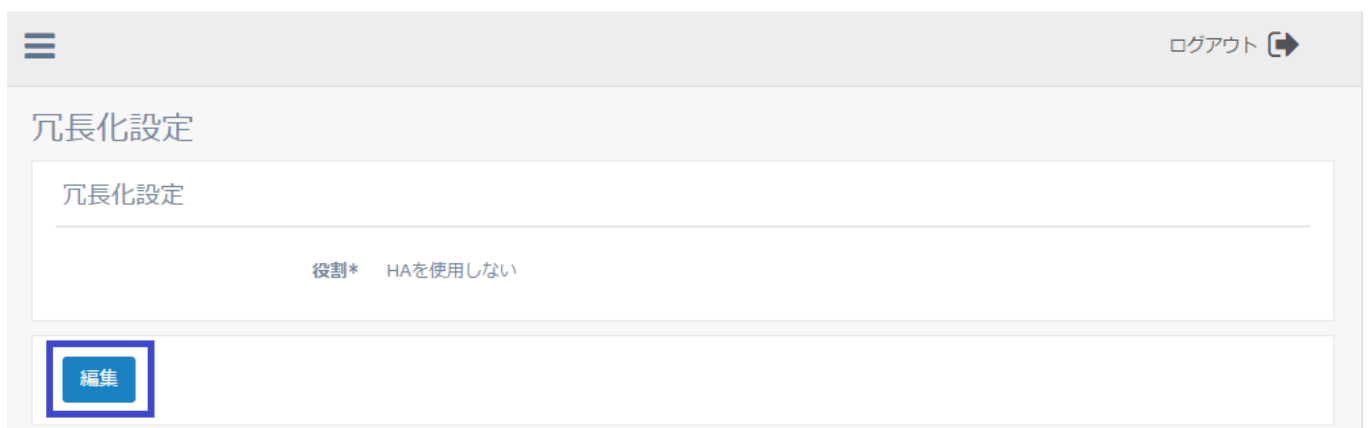


図3-5 冗長化設定画面

役割を「マスター」に変更すると、さらに設定項目が表示されます。
導入例では、以下のように設定します。

- **役割**
マスター
- **パートナーIP アドレス**
10.1.1.3
- **同期パスワード**
webbeaglesync
- **VRID**
111

冗長化設定編集

冗長化設定

役割 *	マスター
パートナーIPアドレス *	10.1.1.3
同期パスワード *	webbeaglesync
VRID *	111

キャンセル 入力内容確認

図3-6 冗長化設定編集画面（マスター）

☞ 冗長化設定については「5章 - 冗長化設定 (./chapter_5.html#冗長化設定)」を参照してください。

❗ 同期パスワードは、第三者に推測されにくい、独自の文字列を設定してください。
同期パスワードには、半角英数字のみ使用可能です。

❗ VRID は1 から255 までの整数を設定することができます。冗長化構成を行う機器同士には同じ値を設定します。

同一ネットワーク内の機器にVRRP を使用する機器がある場合には、設定されているVRID を調査の上、重複しないように設定してください。同一ネットワーク内に、冗長化構成の別のWeb Beagle を設置する場合にもVRID が重複しないように設定してください。

❗ 同一ネットワーク内の機器で重複したVRID を設定すると、通信異常などの不具合が発生することがあります。

「入力内容確認」をクリックし、内容に問題がなければ「更新」をクリックすると設定が反映されます。

更新後、冗長化設定が変更されていることを確認してください。

【ホーム】 → 【ダッシュボード】を選択してください。

- **現在の動作状態**
稼働中
- **役割**
マスター

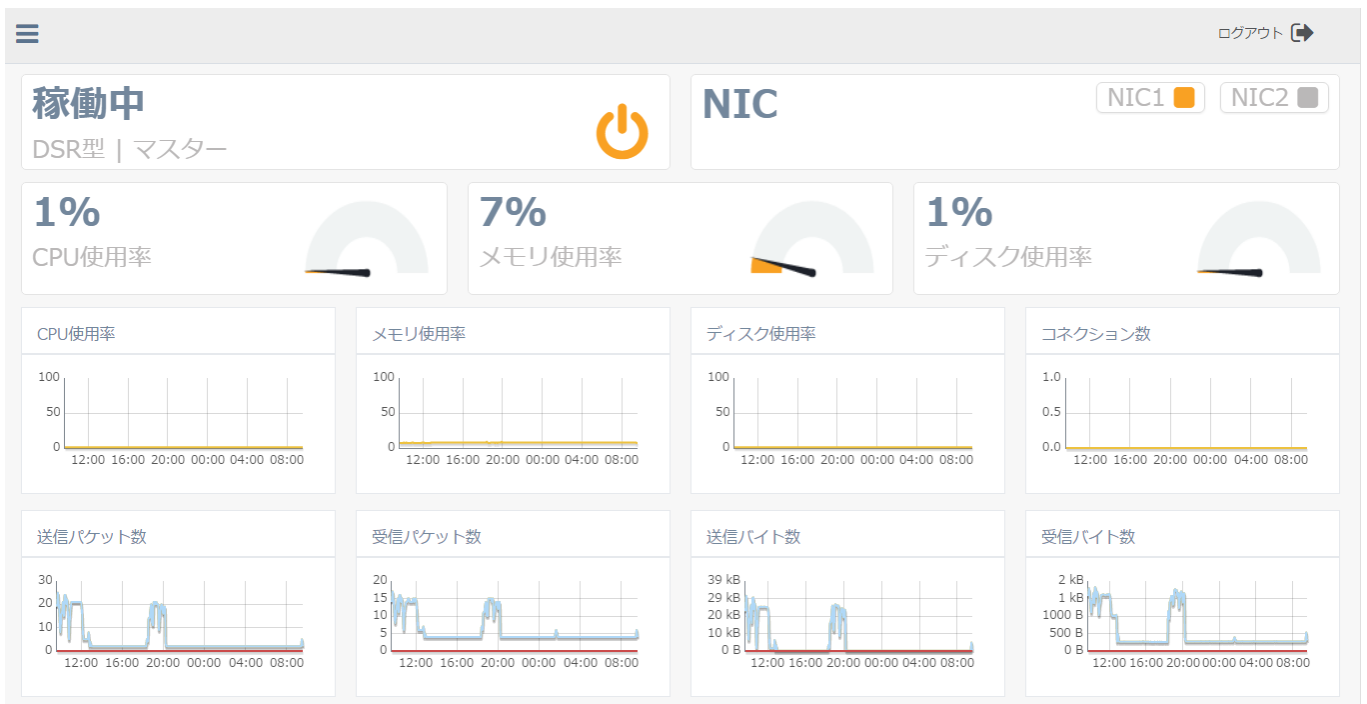


図3-7 装置の状態表示画面

4. スタンバイ機の冗長化設定

Web Beagle (10.1.1.3) をスタンバイ機として動作するよう、冗長化設定の変更を行います。

Web Beagle (10.1.1.3) の管理画面にログインします。

【基本設定】 → 【冗長化設定】 を選択し、冗長化設定の編集を行います。

役割を「スタンバイ」に変更すると、さらに設定項目が表示されます。導入例では、以下のように設定します。

- **役割**
スタンバイ
- **パートナーIP アドレス**
10.1.1.2
- **同期パスワード**
webbeaglesync
- **VRID**
111

図3-8 冗長化設定編集画面（スタンバイ）

👉 冗長化設定については「5章 - 冗長化設定 (./chapter_5.html#冗長化設定)」を参照してください。

🚨 同期パスワードおよびVRID はマスター機で設定したものと同じ値を設定してください。

「**入力内容確認**」をクリックして内容に問題なければ「**更新**」をクリックすると設定が反映されます。

更新後、冗長化設定が変更されていることを確認してください。

【ホーム】 → 【ダッシュボード】を選択してください。

- **現在の稼働状況**
待機中
- **役割**
スタンバイ

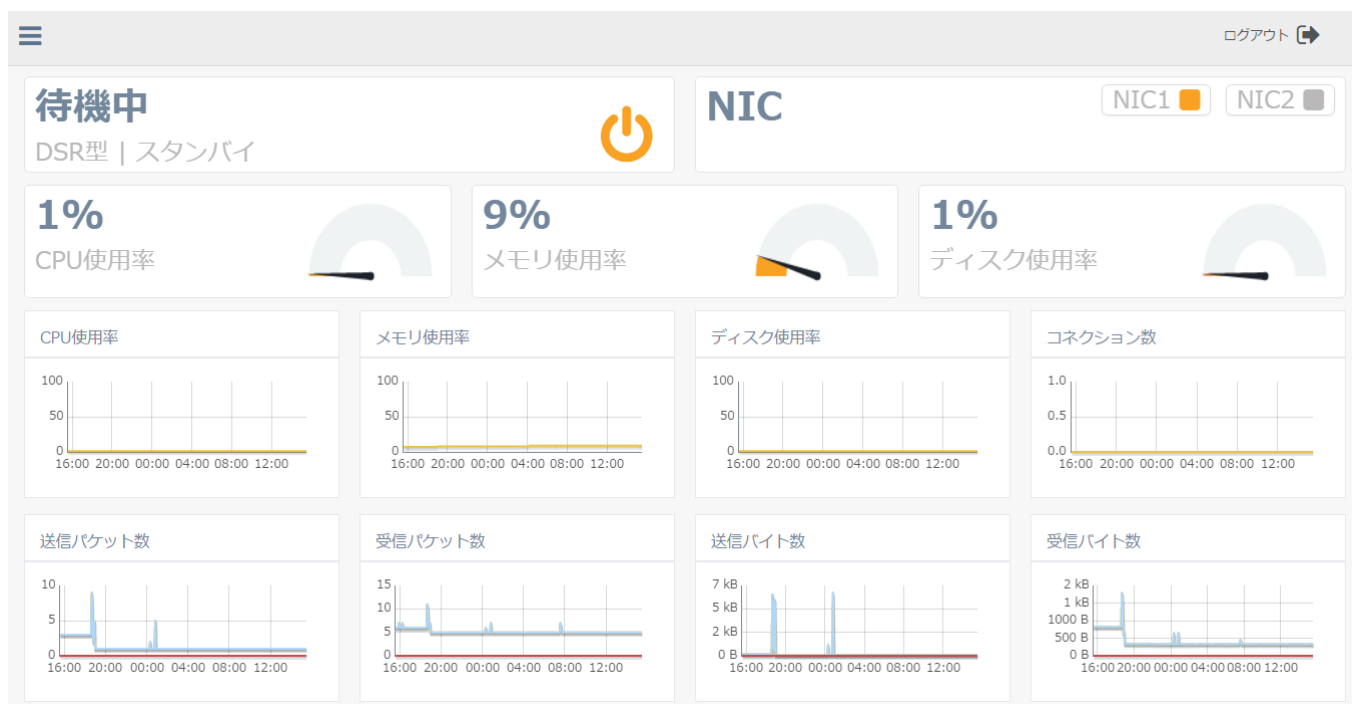


図3-9 装置の状態表示画面

このように表示されていれば、冗長化構成の構築が完了となります。

🚨 **同期が完了しなかった場合**

再起動後の状態が図3-10 の状態の場合

- **現在の稼働状況**
待機中（未同期）
- **役割**
スタンバイ

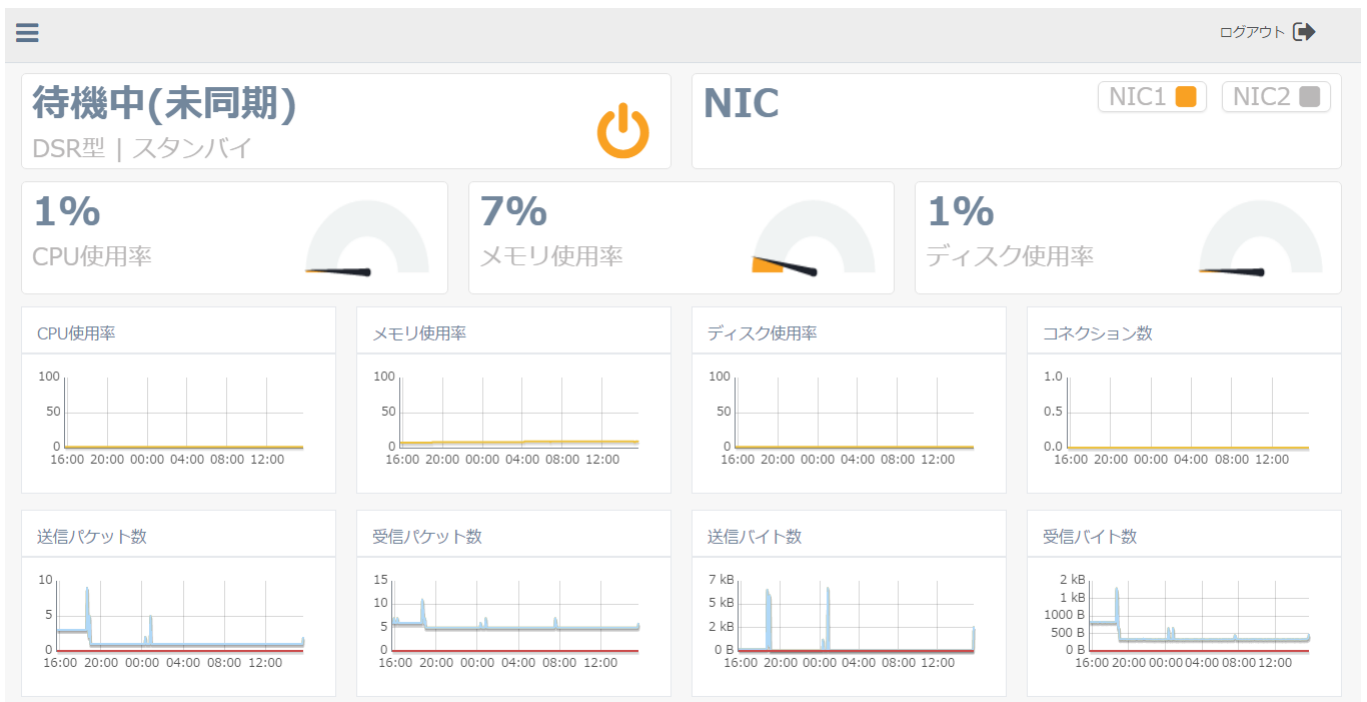


図3-10 装置の状態表示画面（未同期）

マスター機から情報の同期中という状態を表します。通常であれば、数分で同期処理が完了し、現在の動作状態は待機中に遷移します。しかし、しばらく待っても現在の動作状態が変更されない場合、以下の原因によって同期処理が正常に行われていないことが考えられます。

- マスター機およびスタンバイ機の冗長化設定が正しくない。
- パートナーIP アドレスにお互いのIP アドレスを設定していない。
- 同期パスワードが一致していない。
- VRID が一致していない。
- ネットワーク内に重複したVRID を設定している機器が存在する。

上記の点に注意して、再度両機の冗長化設定を確認してください。

3. 冗長化構成時の動作について

冗長化構成時のマスター機およびスタンバイ機がダウンした場合のフェイルオーバーの動作について説明します。

基本構成

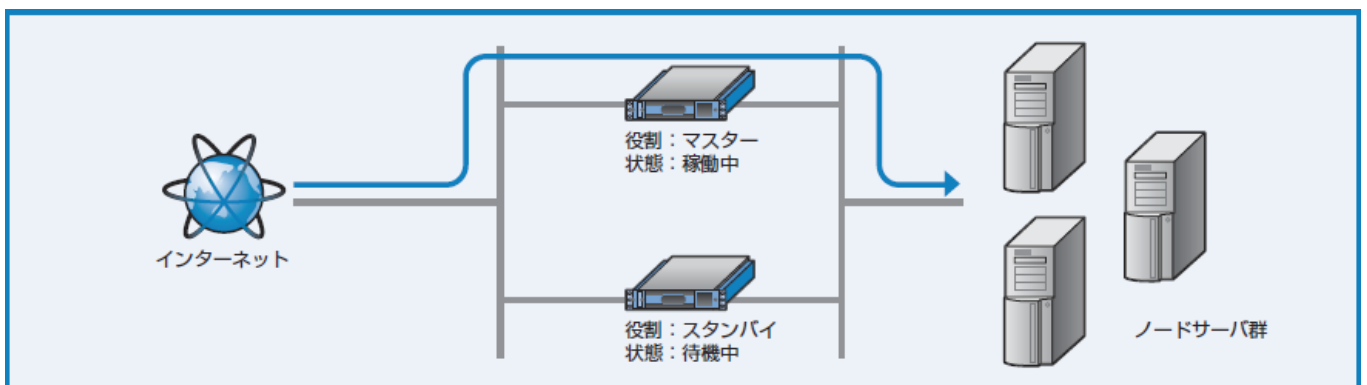


図3-11 基本構成

マスター機がダウンしたときの動作

マスター機がダウンした場合、ダウンしたことをスタンバイ機が自動的に検知し、スタンバイ機の動作状態が自動的に「稼働中」となり、動作を継続します。この動作を「フェイルオーバー」と呼びます（図3-12、図3-13）。

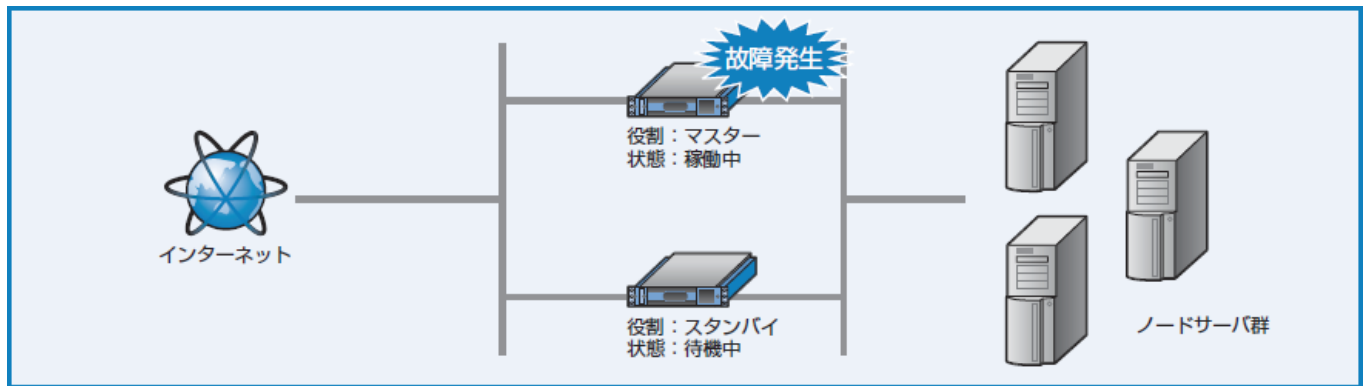


図3-12 マスター機で障害発生

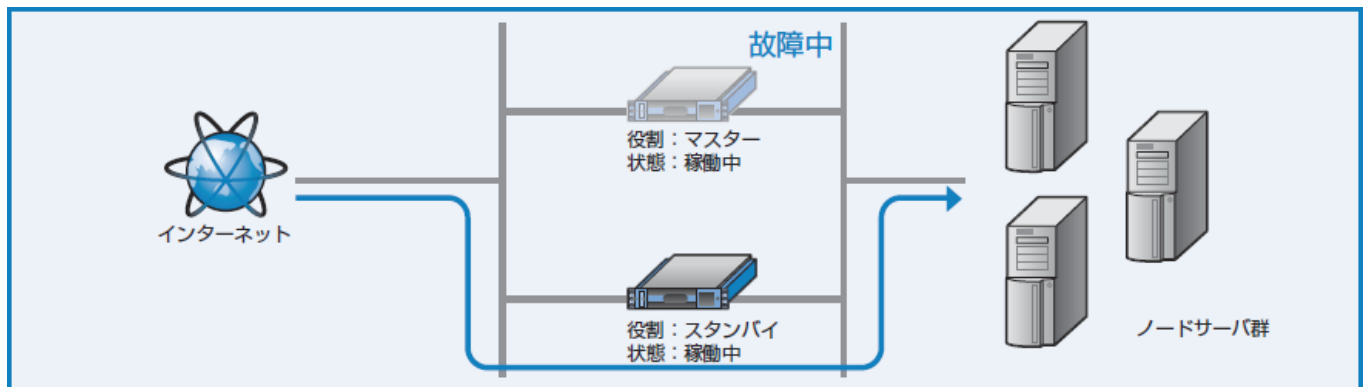


図3-13 フェイルオーバーが発生し、スタンバイ機で動作継続

マスター機が障害から復帰すると、再びスタンバイ機は「待機中」に遷移し、動作はマスター機で行われるようになります（図3-14、図3-15）

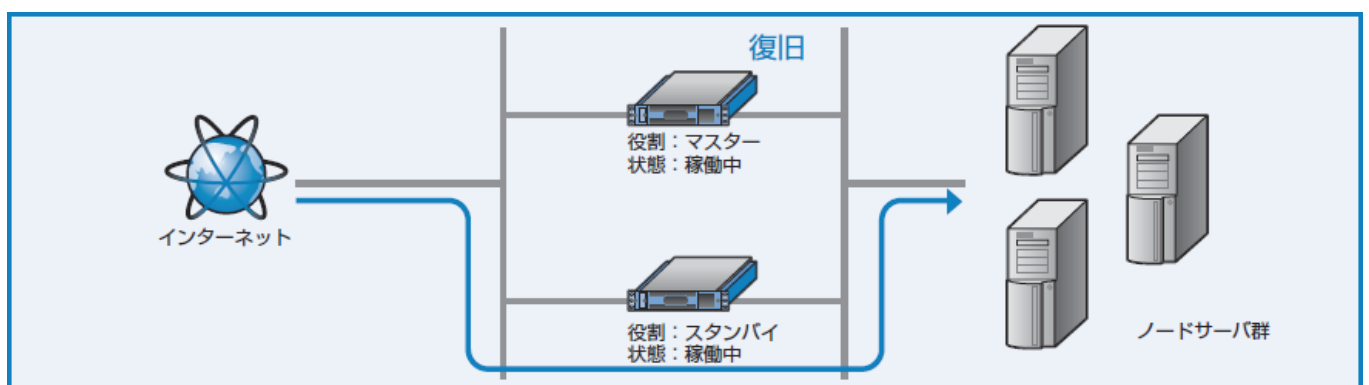


図3-14 マスター機が復帰

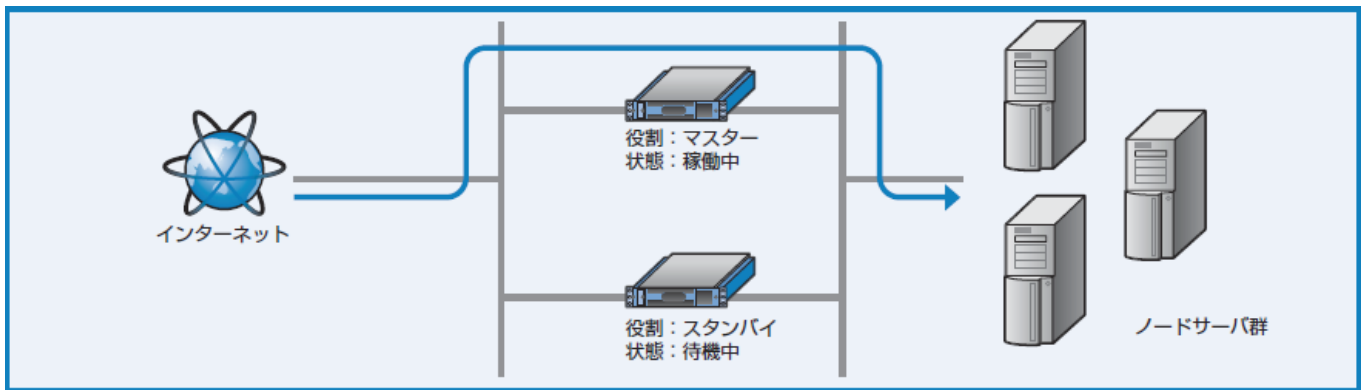


図3-15 再び通常構成で動作継続

スタンバイ機がダウンしたときの動作

スタンバイ機がダウンした場合、マスター機への影響はなく、引き続きマスター機で動作を継続します。スタンバイ機が復帰すると、自動的に基本構成にもどります（図3-16、図3-17）

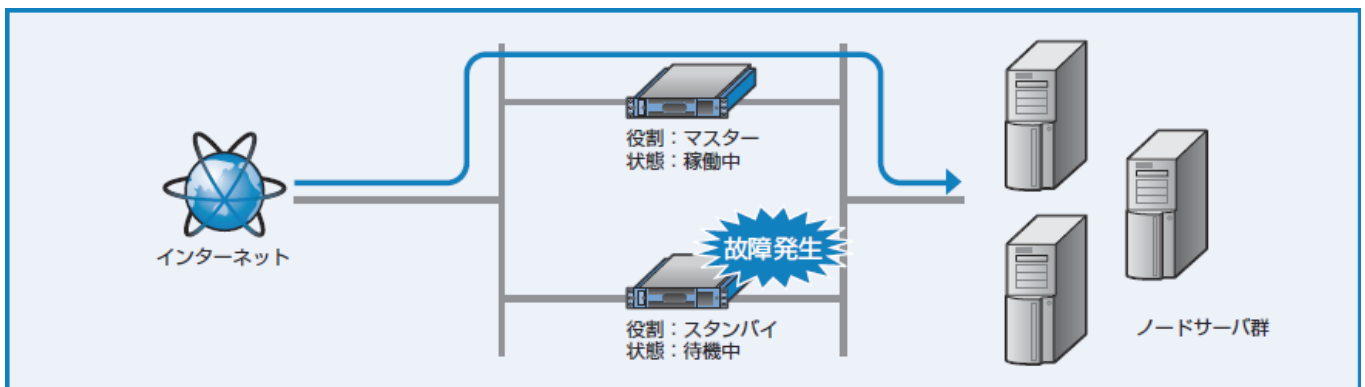


図3-16 スタンバイ機で障害が発生

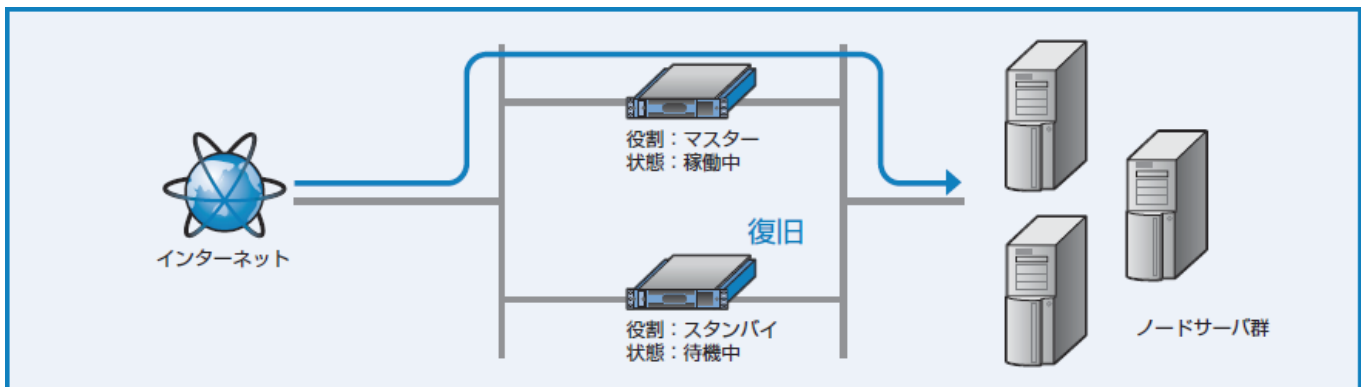


図3-17 スタンバイ機が復帰

プロモートについて

障害によりダウンしたマスター機がメンテナンスや部品交換などでただちに復旧できない場合、スタンバイ機で運用を継続する必要があります。

しかし、負荷分散設定変更はマスター機の管理インターフェイスからしか操作できないため、スタンバイ機のみでは負荷分散設定の変更はできません（図3-18）。負荷分散設定の変更を行う場合は、役割をスタンバイからマスターに昇格させる必要があります。この処理をプロモートと呼びます。プロモートによってスタンバイ機の役割をマスターに昇格させることで、マスター機として運用管理を続行することができます（図3-19）

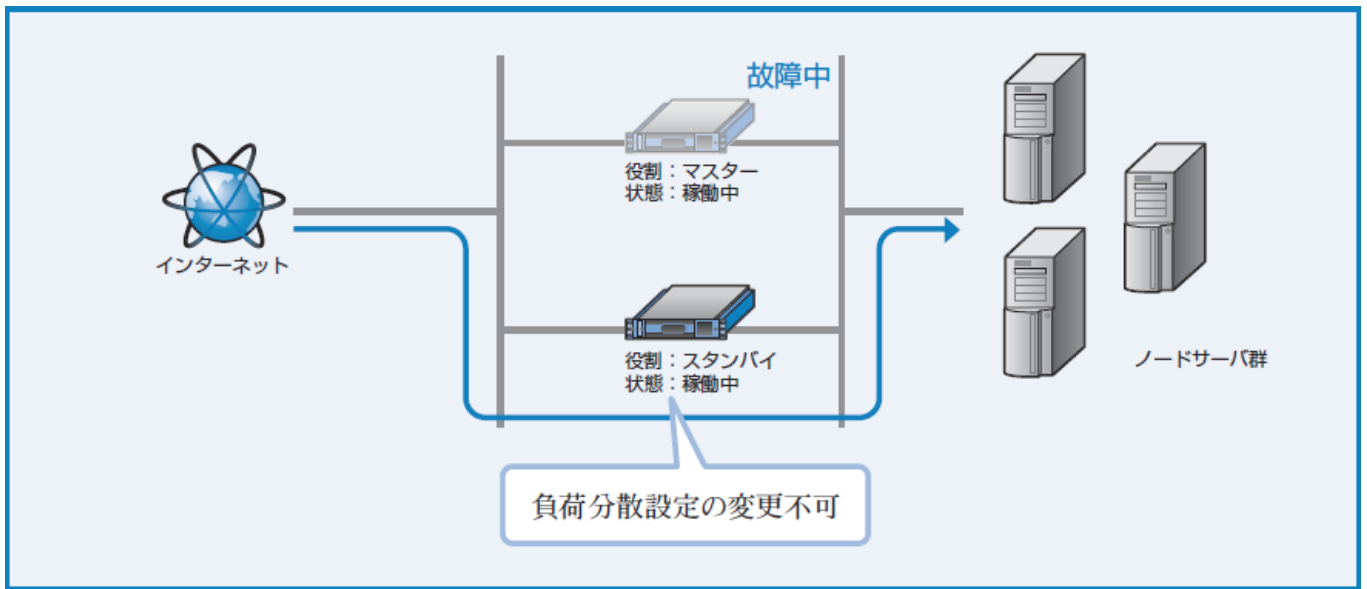


図3-18 スタンバイ機にフェイルオーバーした状況継続

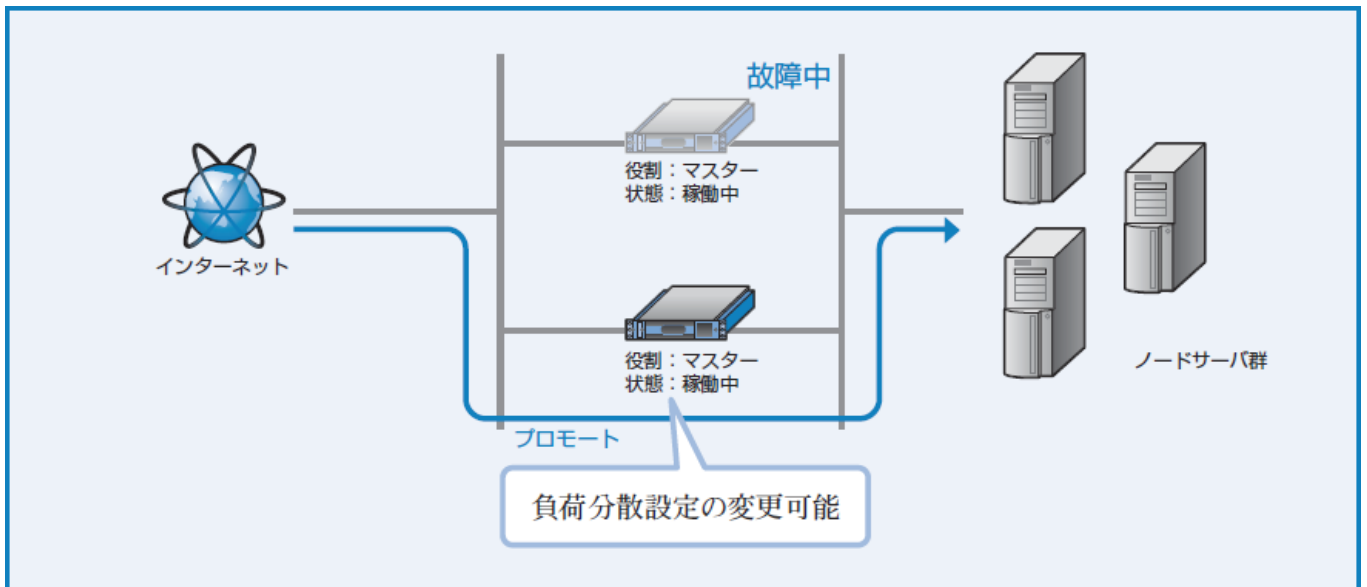


図3-19 プロモートにより、マスターに昇格

なお、プロモート操作を行うとスタンバイ機はマスター機に変更されます。故障していたマスター機をマスター機の設定のまま接続すると、マスター機が2台存在する状態となり冗長化構成が正常に動作しません（図3-20）。

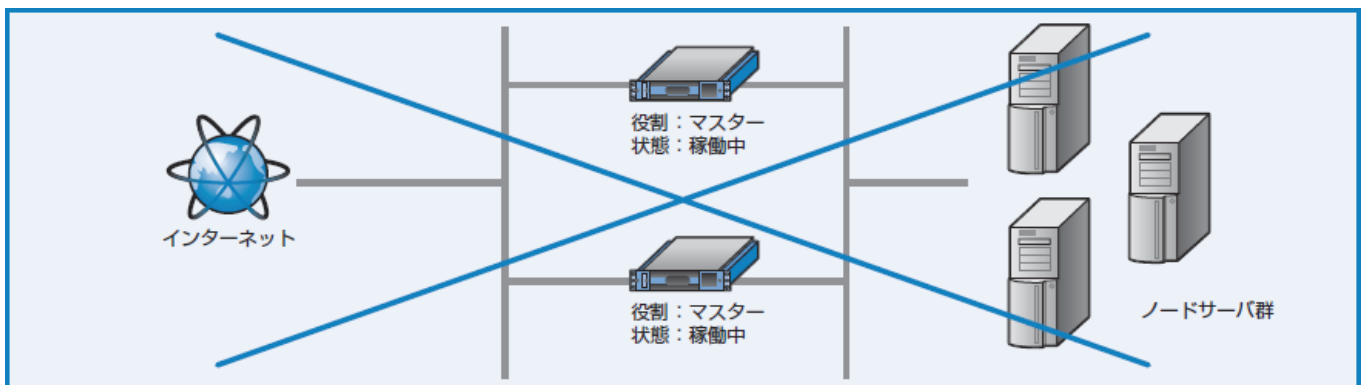


図3-20 誤った設置状態

プロモートを行いバックアップ機をマスター機に変更した場合は、役割を「スタンバイ」に設定したWeb Beagle を接続して冗長化構成を構築してください（図3-21）。自動的にマスター機の情報に同期し、それ以降、スタンバイ機として振舞います。

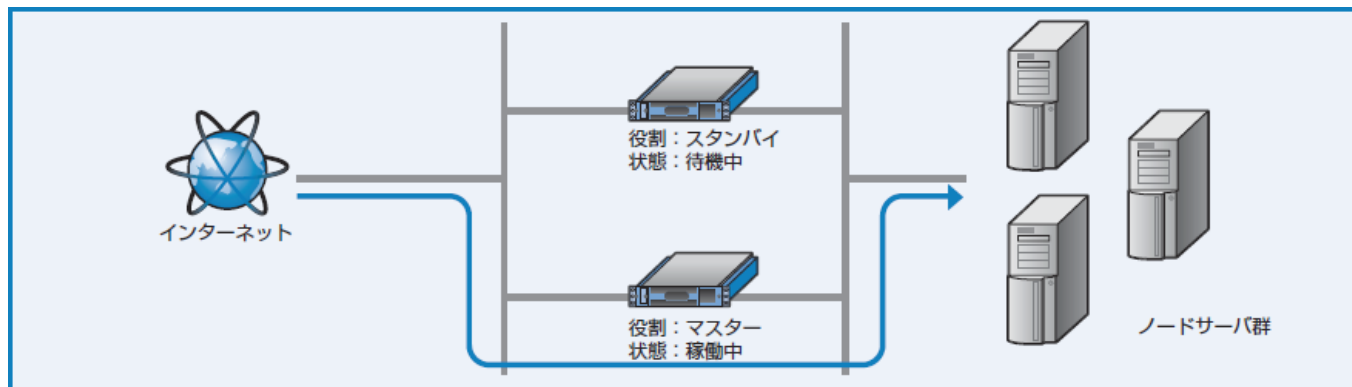


図3-21 スタンバイ機の設置

❗ Web Beagle が自動的にスタンバイに降格することはありません。

📖 冗長化設定については「5章 - 冗長化設定 (/chapter_5.html#冗長化設定)」を参照してください。

プロモート実行手順

【基本設定】 → 【冗長化設定】にて冗長化設定画面を表示します（図3-22）。

役割がスタンバイ、現在の動作状態が稼働中のときのみ、マスターに昇格ボタンが表示されます。

「**マスターに昇格**」ボタンをクリックすると、確認のダイアログが表示されますので「OK」を選択すると、即座に役割が【スタンバイ】 → 【マスター】に変更します（図3-23）。



図3-22 冗長化設定画面

第4章 運用管理

1. 死活監視機能

Web Beagle は、登録したノードサーバに異常が発生していないか、定期的に監視を行っています。これを死活監視機能といいます。この機能によって、運用中に障害が発生したノードサーバを分散対象から切り離し、残りのノードサーバで運用を継続します。

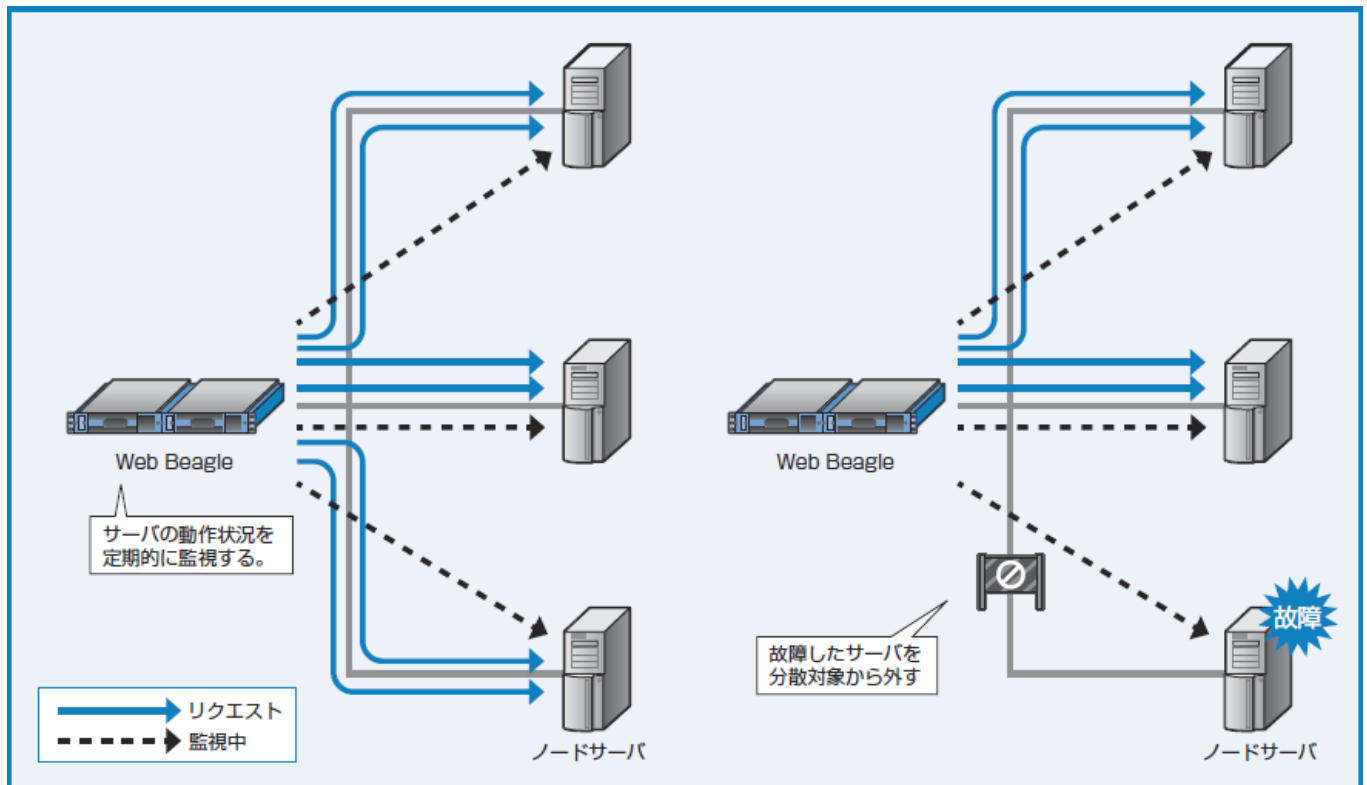


図4-1 死活監視機能

Web Beagle では、次の5種類の死活監視の方法をサポートしています。

- **TCPチェック (L4およびL7負荷分散、TCP上のあらゆるアプリケーションプロトコル通信の負荷分散時を想定し、Webサーバ/MySQLサーバだけでなくそれ以外のサーバへの負荷分散時に使用)**
ノードサーバのTCPポートに接続を試み、接続の可否でノードサーバの生存有無を判断する方式です。
レイヤー4レベル死活監視とも呼ばれます。
- **web (http、https) チェック (L4およびL7負荷分散、HTTPまたはHTTPS通信を負荷分散時を想定)**
web (http、https) チェックは、ノードサーバに指定のURIに対してhttpまたはhttpsリクエストを行い、正常な応答が得られるか確認する方式です。
レイヤー7レベル死活監視とも呼ばれます。
Webサーバからのステータスコードが200の応答が得られる場合、ノードサーバは正常に動作していると判定されます。分散先であるノードサーバのTCPポートに対してHTTPまたはHTTPSリクエストを行います。
❗ HTTPステータスコードが3xx (リダイレクション) の場合は正常動作とはみなされません。死活監視URIには正常時に200のステータスコードを返すURIを指定してください。

- MySQLチェック (L4負荷分散のみ、MySQLのクエリ通信の負荷分散時を想定)**
 指定のユーザ名・パスワードでWeb BeagleからノードサーバのMySQLやMariaDBなどのMySQL互換のデータベースにアクセスを行い、正常な応答が得られるか確認する方式です。分散先であるノードサーバのTCPポートに対してクエリ通信します。
- DNS queryチェック (L4負荷分散のみ、DNSサーバをノードサーバとしたDNS query通信の負荷分散時を想定)**
 監視設定したドメイン名に対するSOALレコードをノードサーバ(DNSサーバ)に問い合わせ、その存在有無をチェックする方式です。SOALレコードが得られれば、WebBeagleはノードサーバが生存していると見なします。分散先であるノードサーバのUDPポートに対して問い合わせされます。
- pingチェック (L4負荷分散のみ、あらゆるUDP上のアプリケーションプロトコル通信の負荷分散時を想定し、DNSサーバだけでなくそれ以外のサーバへの負荷分散時に使用)**
 pingを使用したICMPレベルの死活監視を行います。ping応答が正常に返答されれば、WebBeagleはノードサーバが生存していると見なします。

L4負荷分散の死活監視

TCP チェック

「ノードサーバ追加」または「ノードサーバ編集」にて死活監視に【TCP】を選択します (図4-2)

☞ 「ノードサーバ追加」「ノードサーバ編集」についてはそれぞれ「5章 - ノードサーバ追加 (/chapter_5.html#ノードサーバ追加)」「5章 - ノードサーバ編集 (/chapter_5.html#ノードサーバ編集)」を参照してください。

The screenshot shows the 'Node Server Settings' interface. At the top right, there is a 'Logout' button. The main heading is 'Node Server Settings'. Below it, the 'Node Server Addition/Editing' form is displayed. The form contains the following fields:

- IPアドレス *: 10.1.1.11
- ポート *: 80
- 重み付け *: 10
- 有効:
- 死活監視 *: TCP (This dropdown menu is highlighted with a blue border in the original image)
- 接続タイムアウト: 5 秒

At the bottom of the form, there are two buttons: 'キャンセル' (Cancel) and '入力内容確認' (Confirm Input).

図4-2 TCP チェックの選択

web (http、https) チェック

「ノードサーバ追加」または「ノードサーバ編集」にて死活監視で【HTTP】を選択します。

✂ 監視対象のURI のスキームがhttps であれば、「HTTPS」を選択します。

「死活監視URI」が入力できるようになりますので、死活監視に使用するURI を指定してください (図4-3)。

ノードサーバ設定

ノードサーバ追加/編集

IPアドレス *	<input type="text" value="10.1.1.11"/>
ポート *	<input type="text" value="80"/>
重み付け *	<input type="text" value="10"/>
有効	<input checked="" type="checkbox"/>
死活監視 *	<input type="text" value="HTTP"/>
接続タイムアウト	<input type="text" value="5"/> 秒
死活監視用URI	<input type="text" value="http://10.1.1.10/"/>

図4-3 HTTP チェックの選択

死活監視を特定のバーチャルドメインのURI に対して実施する場合には、 仮想サービスのバーチャルホスト名を設定してください（図4- 4）。

L4ロードバランサ設定

仮想サービス追加/編集

仮想IPアドレス *	<input type="text" value="10.1.1.10"/>
ポート *	<input type="text" value="80"/>
プロトコル *	<input type="text" value="TCP"/>
分散方式 *	<input type="text" value="重み付けラウンドロビン"/>
待機サーバ	<input type="text"/> : <input type="text" value="80"/>
バーチャルホスト名	<input type="text" value="virtual.example.com"/>
セッション維持	<input type="text" value="ON"/> <input type="text" value="300"/> 秒
有効 *	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
アクセス制限 *	<input type="text" value="無効"/>

図4-4 死活監視URI のホスト名指定

📖 L4仮想サービスの編集については「5章 - L4 仮想サービス追加 (./chapter_5.html#仮想サービス追加)」を参照してください。

✍️ 「仮想サービス」の死活監視URI のホスト名欄が空白の場合、「ノードサーバ追加」または「ノードサーバ編集」の死活監視URI のホスト名部分には、 仮想IP アドレスが表示されます。

バーチャルホスト名を設定すると、死活監視URI 欄にこれが表示されます。テキストボックスにパス名部分を入力し監視を行うページを指定してください（図4- 5）。

The screenshot shows the 'Node Server Settings' page with the following configuration:

- IPアドレス *: 10.1.1.11
- ポート *: 80
- 重み付け *: 10
- 有効:
- 死活監視 *: HTTP
- 接続タイムアウト: 5 秒
- 死活監視用URI: http://virtual.example.com/ []

Buttons: キャンセル, 入力内容確認

図4-5 バーチャルドメインのURI に対しての死活監視指定

MySQLチェック

「ノードサーバ追加」または「ノードサーバ編集」にて死活監視で【MySQL】を選択します。「DBユーザ名」と「パスワード」が入力できるようになりますので、死活監視対象のデータベースのユーザ名とパスワードを入力してください。（図4- 6）。

The screenshot shows the 'Node Server Settings' page with the following configuration:

- IPアドレス *: 10.1.1.11
- ポート *: 80
- 重み付け *: 10
- 有効:
- 死活監視 *: MySQL
- 接続タイムアウト *: 5 秒
- DBユーザ名: dbuser
- パスワード: dbpassword

Buttons: キャンセル, 入力内容確認

図4-6 MySQL チェックの選択

死活監視の確認

各ノードサーバの追加、または編集後、死活監視が働いているか確認します。

【L4負荷分散】 → 【対象の仮想サービス】 → 【ノードサーバー一覧】にて対象ノードサーバの状態を確認します。

ノードサーバ	死活監視	有効	アクティブ接続数	非アクティブ接続数	
192.168.24.190:80	TCP	YES	0	0	編集 無効 削除
192.168.24.191:80	TCP	YES	0	0	編集 無効 削除
192.168.24.192:80	TCP	YES	0	0	編集 無効 削除
192.168.24.193:80	TCP	YES	0	0	編集 無効 削除

図4-7 死活監視状態の確認

ノードサーバのステータスアイコンの色が緑であれば、対象ノードサーバは正常に稼働しています。赤であれば、TCP チェックの場合、対象ノードサーバで設定したTCP ポートに接続可能か確認してください。web (http、https) チェックの場合、死活監視URI に記述されたURI が正しいか、Web サーバがこれに回答しているか確認してください。MySQL チェックの場合、「DBユーザ名」「パスワード」に設定した値が正しいか確認してください。

✏️ 「L4負荷分散」の「L7仮想サービス一覧」にて仮想サービス毎のノードサーバの稼働状況や正常に稼働しているノードサーバ数を一覧で確認することができます（図4-8）

状態	仮想IPアドレス	ポート	分散方式	有効	稼働中 / 全ノードサーバ数	
■	192.168.24.198:80	80/TCP	ラウンドロビン	YES	2/2	フィルタ 編集 無効 削除

図4-8 仮想サービスの一覧画面

L7負荷分散の死活監視

TCP チェック

「L7仮想サービス追加/編集」にて死活監視に【TCP】を選択します（図4-9）

🔗 「L7仮想サービス追加/編集」については「5章 - L7 仮想サービス追加/編集 (./chapter_5.html#l7-仮想サービス追加)」を参照してください。

L7ロードバランサ設定

L7仮想サービス追加/編集

仮想IPアドレス *	<input type="text" value="10.1.1.10"/>
ポート *	<input type="text" value="80"/>
動作方式 *	<input type="text" value="HTTP"/>
分散方式 *	<input type="text" value="ラウンドロビン"/>
待機サーバ	<input type="text"/> : <input type="text" value="80"/>
バーチャルホスト名	<input type="text"/>
セッション維持方式 *	<input type="text" value="セッションを維持しない"/>
有効 *	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
死活監視 *	<input type="text" value="TCP"/>
アクセス制限 *	<input type="text" value="無効"/>

キャンセル

入力内容確認

図4-9 TCP チェックの選択

web (http、https) チェック

「L7仮想サービス追加/編集」にて死活監視で【HTTP】を選択します。

✎ 監視対象のURI のスキームがhttps であれば、「HTTPS」を選択します。

「死活監視URI」が入力できるようになりますので、死活監視に使用するURI を指定してください（図4-10）。

L7ロードバランサ設定

L7仮想サービス追加/編集

仮想IPアドレス *	<input type="text" value="10.1.1.10"/>
ポート *	<input type="text" value="80"/>
動作方式 *	<input type="text" value="HTTP"/>
分散方式 *	<input type="text" value="ラウンドロビン"/>
待機サーバ	<input type="text"/> : <input type="text" value="80"/>
バーチャルホスト名	<input type="text"/>
セッション維持方式 *	<input type="text" value="セッションを維持しない"/>
有効 *	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
死活監視 *	<input type="text" value="HTTP"/>
死活監視用URI	<input type="text" value="http://10.1.1.10/"/>
アクセス制限 *	<input type="text" value="無効"/>

キャンセル

入力内容確認

図4-10 HTTP チェックの選択

死活監視を特定のバーチャルドメインのURI に対して実施する場合には、仮想サービスのバーチャルホスト名を設定してください（図4- 11）。

L7ロードバランサ設定

L7仮想サービス追加/編集

仮想IPアドレス *	<input type="text" value="10.1.1.10"/>
ポート *	<input type="text" value="80"/>
動作方式 *	<input type="text" value="HTTP"/>
分散方式 *	<input type="text" value="ラウンドロビン"/>
待機サーバ	<input type="text"/> : <input type="text" value="80"/>
バーチャルホスト名	<input type="text" value="virtual.example.com"/>
セッション維持方式 *	<input type="text" value="セッションを維持しない"/>
有効 *	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
死活監視 *	<input type="text" value="HTTP"/>
死活監視用URI	http://virtual.example.com/ <input type="text"/>
アクセス制限 *	<input type="text" value="無効"/>

キャンセル

入力内容確認

図4-11 死活監視URI のホスト名指定

📖 L7仮想サービスの編集については「5章 - L7 仮想サービス編集 (./chapter_5.html#l7-仮想サービス編集)」を参照してください。

✎ 「L7仮想サービス」のバーチャルホスト名欄が空白の場合、死活監視用URI のホスト名部分には、仮想IPアドレスが表示されます。

バーチャルホスト名を設定すると、死活監視URI 欄にこれが表示されます。テキストボックスにパス名部分を入力し監視を行うページを指定してください (図4- 12) 。

L7ロードバランサ設定

L7仮想サービス追加/編集

仮想IPアドレス *	<input type="text" value="10.1.1.10"/>
ポート *	<input type="text" value="80"/>
動作方式 *	<input type="text" value="HTTP"/>
分散方式 *	<input type="text" value="ラウンドロビン"/>
待機サーバ	<input type="text"/> : <input type="text" value="80"/>
バーチャルホスト名	<input type="text" value="virtual.example.com"/>
セッション維持方式 *	<input type="text" value="セッションを維持しない"/>
有効 *	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
死活監視 *	<input type="text" value="HTTP"/>
死活監視用URI	<input type="text" value="http://virtual.example.com/"/>
アクセス制限 *	<input type="text" value="無効"/>

キャンセル

入力内容確認

図4-12 バーチャルドメインのURI に対しての死活監視指定

死活監視の確認

各ノードサーバの追加、または編集後、死活監視が働いているか確認します。

【L7負荷分散】 → 【対象の仮想サービス】 → 【ノードサーバー一覧】にて対象ノードサーバの状態を確認します。

ノードサーバ	有効	アクティブ接続数	非アクティブ接続数	
<input checked="" type="checkbox"/> 192.168.24.190:80	YES	0	0	編集 無効 削除
<input checked="" type="checkbox"/> 192.168.24.191:80	YES	0	0	編集 無効 削除
<input checked="" type="checkbox"/> 192.168.24.192:80	YES	0	0	編集 無効 削除
<input checked="" type="checkbox"/> 192.168.24.193:80	YES	0	0	編集 無効 削除

4 件中 1 から 4 まで表示

先頭 前 1 次 最終

図4-13 死活監視状態の確認

ノードサーバのステータスアイコンの色が緑であれば、対象ノードサーバは正常に稼働しています。赤であれば、TCP チェックの場合、対象ノードサーバで設定したTCP ポートに接続可能か確認してください。web (http、https) チェックの場合、死活監視URI に記述されたURI が正しいか、Web サーバがこれに応

答しているか確認してください。

✍ 「L7負荷分散」の「L7仮想サービス一覧」にて仮想サービス毎のノードサーバの稼働状況や正常に稼働しているノードサーバ数を一覧で確認することができます（図4-14）

L7ロードバランサ設定

L7仮想サービス一覧

リフレッシュ 追加

10 件表示 検索:

状態	仮想IPアドレス	分散方式	有効	稼働中 / 全ノードサーバ数
■	192.168.24.199:80	ラウンドロビン	YES	3/3

1 件中 1 から 1 まで表示

先頭 前 1 次 最終

フィルタ 編集 無効 削除

図4-14 仮想サービスの一覧画面

2. ノードサーバの有効化・無効化（一時的な切り離し）

Web Beagle では、管理画面からの操作でノードサーバを分散対象から切り離すことができます。Webサーバのメンテナンス時などで運用中にメンテナンスを行う場合などで一時的に切り離し、メンテナンス終了後元に戻す場合などに有効です（図4-15）。

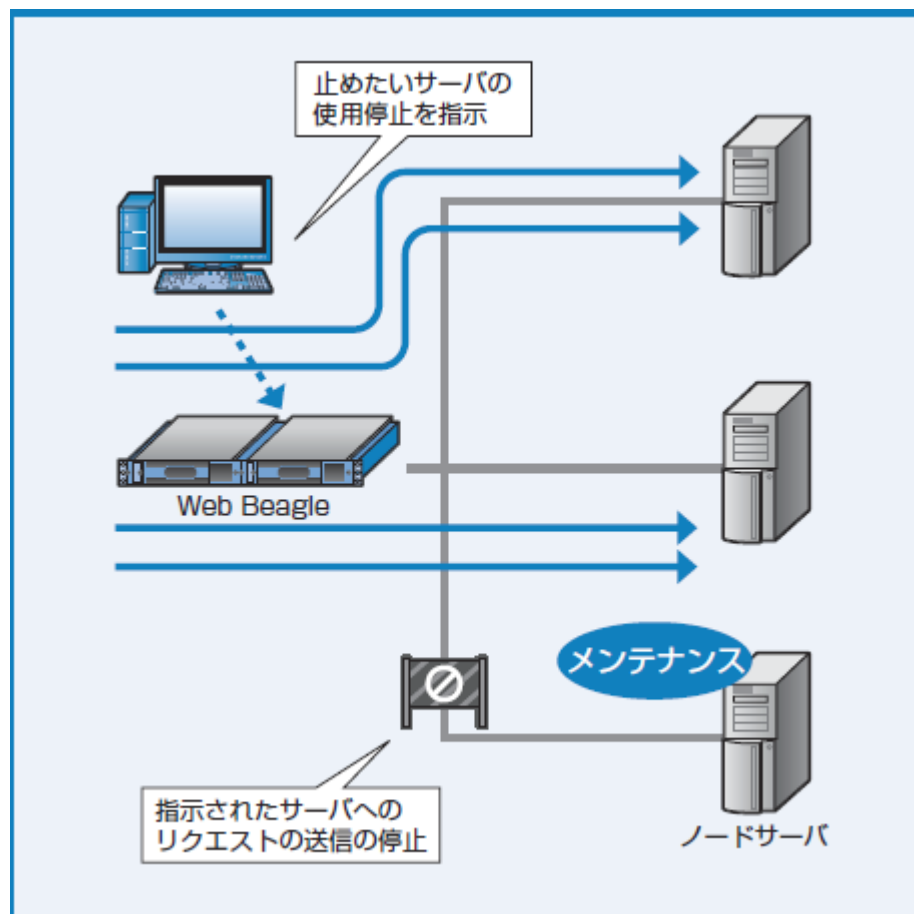


図4-15 ノードサーバの無効化

ノードサーバの無効化手順

❶ L4 負荷分散の場合もL7 負荷分散の場合も同様の手順となります。

1. 無効にしたいノードサーバがある【仮想サービス】を選択します。
2. ノードサーバ一覧から、分散対象から切り離したいノードサーバの「無効」をクリックします（図4-16）。

ノードサーバ一覧

10 件表示 検索:

ノードサーバ	死活監視	有効	アクティブ接続数	非アクティブ接続数	
192.168.24.190:80	TCP	YES	0	0	編集 無効 削除
192.168.24.191:80	TCP	YES	0	0	編集 無効 削除
192.168.24.192:80	TCP	YES	0	0	編集 無効 削除
192.168.24.193:80	TCP	YES	0	0	編集 無効 削除

4 件中 1 から 4 まで表示

先頭 前 1 次 最終

3. 対象ノードサーバの「状態」を確認し、分散対象から外れていることを確認します（図4-17）。

ノードサーバ一覧

10 件表示 検索:

ノードサーバ	死活監視	有効	アクティブ接続数	非アクティブ接続数	
192.168.24.190:80	TCP	YES	0	0	編集 無効 削除
192.168.24.191:80	TCP	YES	0	0	編集 無効 削除
192.168.24.192:80	TCP	YES	0	0	編集 無効 削除
192.168.24.193:80	TCP	NO	-	-	編集 有効 削除

4 件中 1 から 4 まで表示

先頭 前 1 次 最終

ノードサーバの有効化手順

❶ L4 負荷分散の場合もL7 負荷分散の場合も同様の手順となります。

切り離れたノードサーバを再び分散対象になるよう有効化します。

1. 有効にしたいノードサーバがある【仮想サービス】を選択します。
2. 図4-16 にて切り離れたノードサーバの「有効」をクリックします。
3. 対象ノードサーバの「状態」を確認し、UP になっていることを確認します（図4-18）。

ノードサーバー一覧						リフレッシュ	追加
10	件表示	検索:					
ノードサーバ	死活監視	有効	アクティブ接続数	非アクティブ接続数			
192.168.24.190:80	TCP	YES	0	0	編集	無効	削除
192.168.24.191:80	TCP	YES	0	0	編集	無効	削除
192.168.24.192:80	TCP	YES	0	0	編集	無効	削除
192.168.24.193:80	TCP	YES	0	0	編集	無効	削除

4 件中 1 から 4 まで表示

先頭 前 1 次 最終

3. 待機サーバ機能

Web Beagle では、通常負荷分散を行うノードサーバに加え、待機サーバを登録しておくことができます。待機サーバとは、通常の運用中はWeb Beagle からリクエストを振り分けられず、ノードサーバが停止（複数ノードサーバがある場合はすべて停止）した場合にのみリクエストが振り分けられるノードサーバです。仮想IP アドレス毎に一つの待機サーバを登録できます。

使用例 1) バックアップサーバとしての利用

この機能を用いることによって、通常の処理を行なっているノードサーバが停止した場合にのみ動作するサーバ（バックアップサーバ）を実現できます（図4-19）。

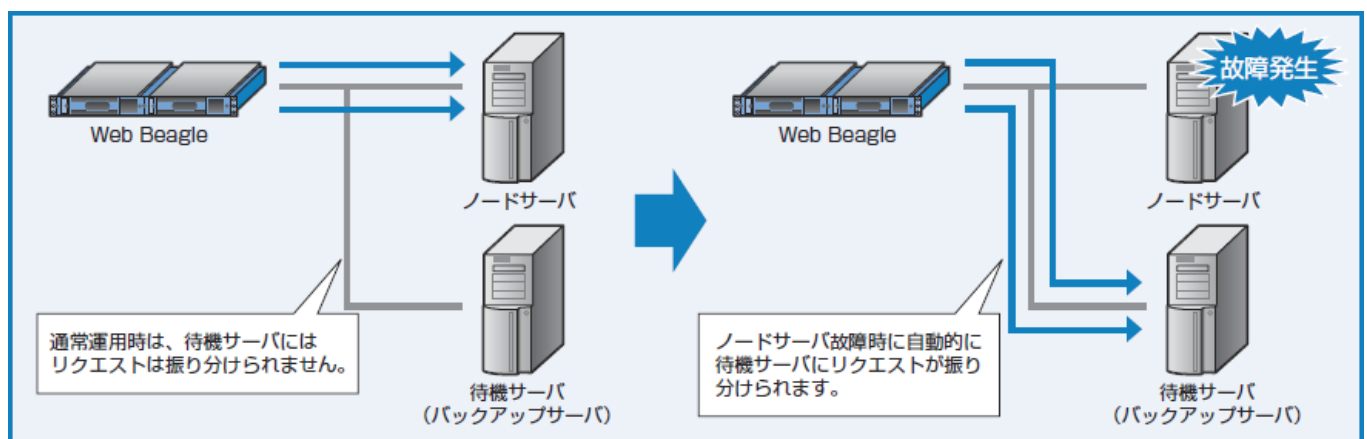


図4-19 スタンバイ機で障害が発生

使用例2) ソーリーサーバとしての利用

複数のWeb サーバに負荷分散することで、Web サーバの冗長性を高めることができますが、Web サーバがDB サーバやアプリケーションサーバに接続している場合、これらのバックエンドサーバに不具合が生じると、すべてのノードサーバが正常に動作しない状況が発生することが考えられます。

待機サーバには、システム障害を案内するコンテンツを設置しておく、またはバックエンドサーバを参照しない縮退運用コンテンツを設置しておくなどの事前準備をしておくことで、システムに不具合が発生した場合の対応を自動化することができます。

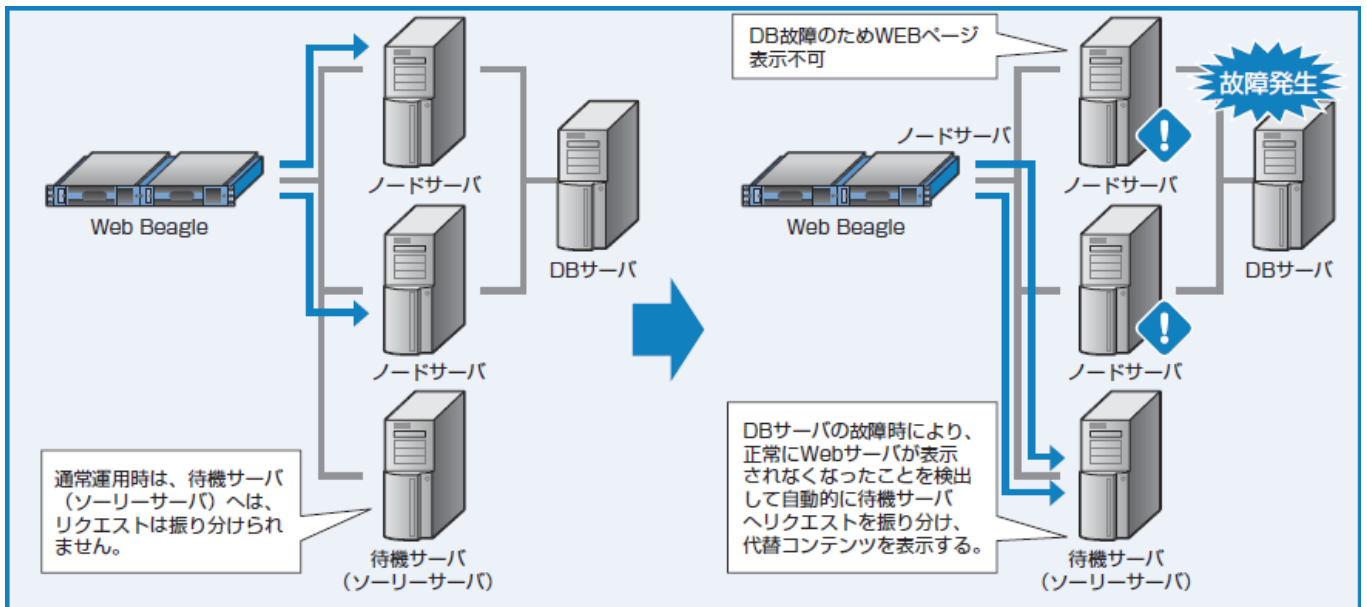


図4-20 スタンバイ機で障害が発生

待機サーバの設定手順

❗ L4 負荷分散の場合もL7 負荷分散の場合も同様の手順となります。

1. 待機サーバを設定したい【仮想サービス】を選択します。
2. 仮想サービスを新規追加する場合「追加」をクリックします。作成済みの仮想サービスに設定を行う場合は、対象の仮想サービスの「編集」をクリックします（図4-21）。

L4ロードバランサ設定

仮想サービス追加/編集

仮想IPアドレス *	10.1.1.10
ポート *	80
プロトコル *	TCP
分散方式 *	ラウンドロビン
待機サーバ	10.1.1.19 : 80
バーチャルホスト名	
セッション維持	ON 300 秒
有効 *	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
アクセス制限 *	無効

キャンセル 入力内容確認

図4-21 待機サーバの設定手順

3. 「待機サーバ」の項目に待機サーバのIP アドレスおよびポート番号を設定します。IPは実ノードサーバと同じネットワークアドレス上に配置したものを指定してください。ポート番号は仮想サービスのポートと同一値を設定してください。

4. 「適用」 をクリックします。

❗ 「待機サーバ」 が空白かつポートが「80」の場合は待機サーバ機能が無効であることを表します。

4. バックアップ・リストア手順

Web Beagle で設定した設定情報をバックアップすることができます。もちろん、バックアップファイルをリストアすることで以前の設定状態に戻すことができます。また、旧モデルのバックアップファイルから設定情報を復元することもできます。

バックアップ手順

1. 【運用管理】 → 【バックアップ／リストア】 を選択します（図4-22）
2. 「設定情報のバックアップ」の「バックアップ」 をクリックします。設定ファイルのダウンロードが開始されます（図4-22）。



図4-22 設定情報のバックアップ

❗ ご利用のブラウザによってはポップアップがブロックされバックアップファイルをダウンロードできない場合があります。

そのような場合はお手数ですが、ポップアップのブロックを解除して再度実行してください。

❗ ダウンロード手順はご使用のブラウザによって異なります。

❗ ダウンロードした設定ファイルをエディタなどで編集すると、正常にリストアできなくなります。そのため、設定ファイルの編集は行わないでください。

リストア手順

1. 【運用管理】 → 【バックアップ／リストア】 を選択します（図4-23）
2. バックアップ手順にて取得した設定ファイルを画面にドラッグするかクリックすると表示されるディレクトリー一覧からバックアップファイルを選択します。

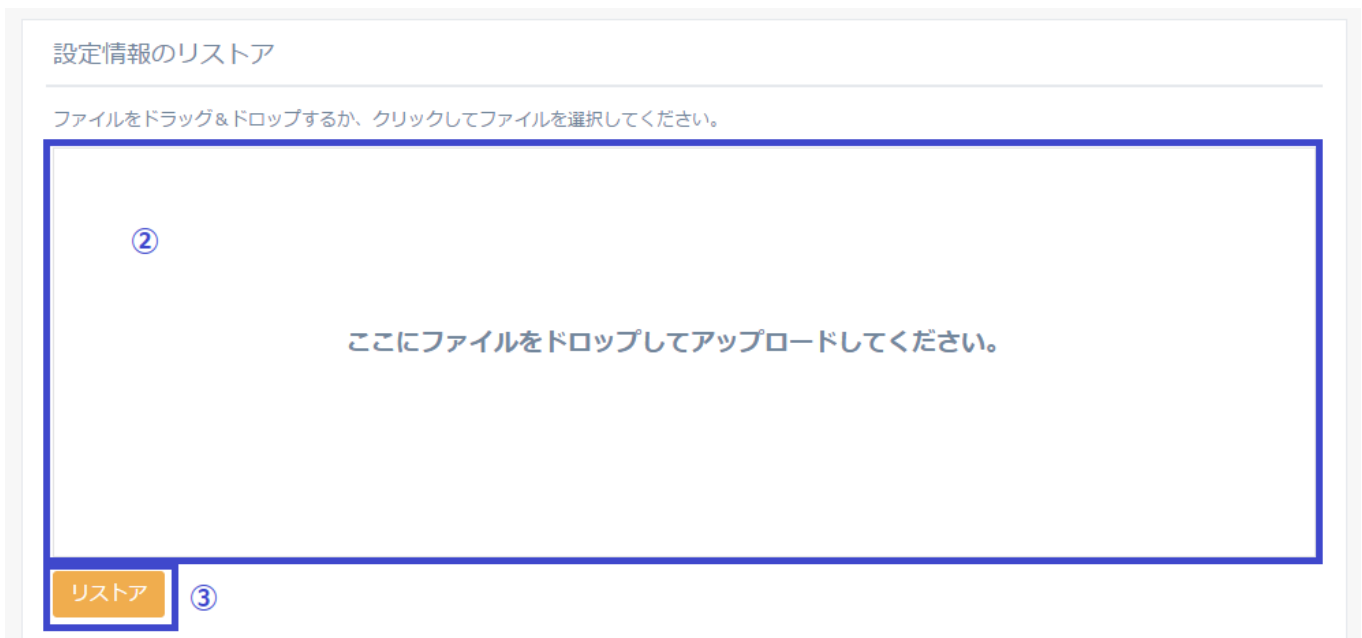


図4-23 設定情報のリストア

3. 「**リストア**」をクリックすると、設定情報のリストアが開始します。

✎ リストアされた設定情報は再起動後に有効になります。

❗ リストアに失敗した場合、以下の項目を確認してください。

- 指定したファイルがバックアップ手順で取得したファイルかどうか。
- 取得したファイルを編集していないか。

旧モデルからの設定情報のリストア手順

1. 【バックアップ/リストア】画面より【旧モデルからの設定情報のリストア】の【リストア画面へ移動】を選択します。（図4-24）

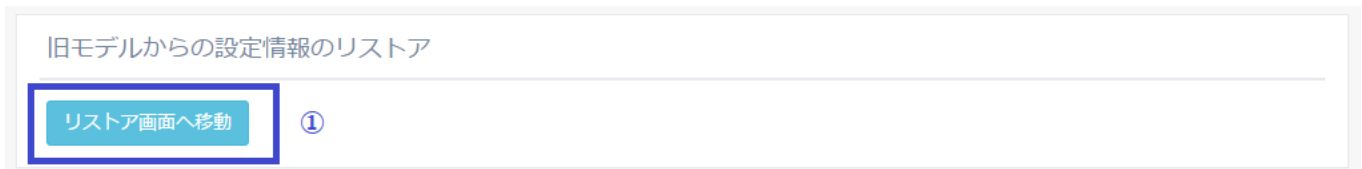


図4-24 旧モデルからの設定情報のリストアへの移動

2. 旧モデルのバックアップファイルを画面にドラッグするかクリックすると表示されるディレクトリー一覧から旧モデルのバックアップファイルを選択します。

旧モデルからの設定情報のリストア

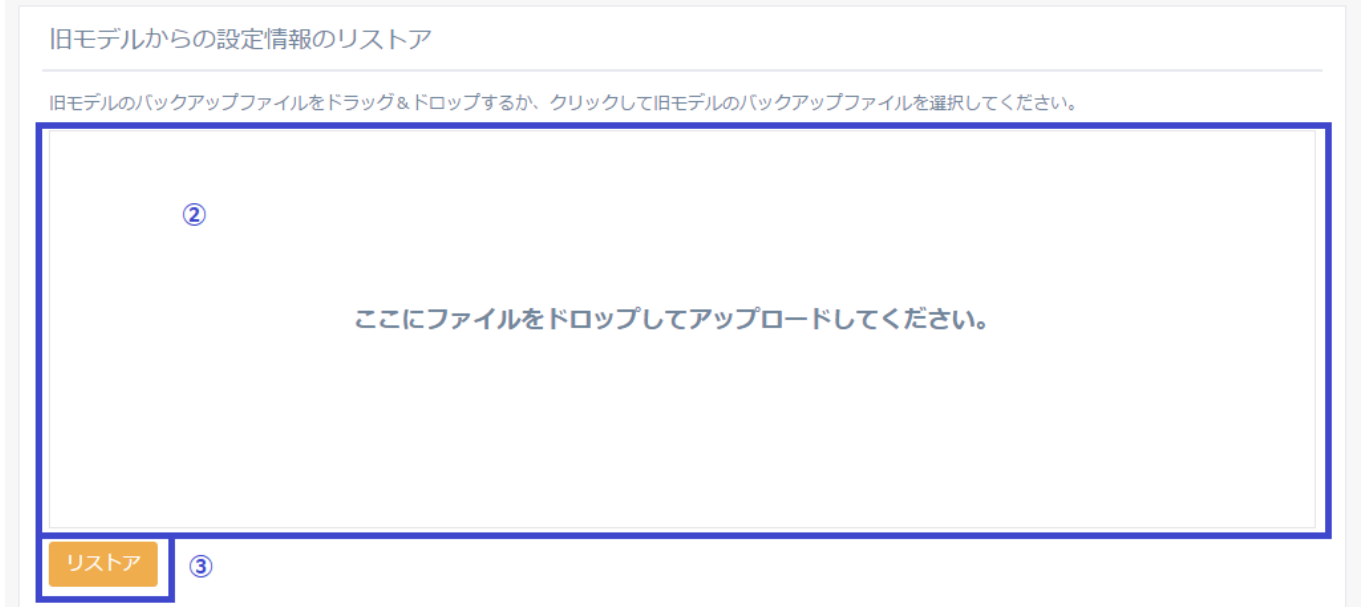


図4-25 旧モデルからの設定情報のリストア

3. 「**リストア**」をクリックすると、旧モデルからの設定情報のリストアが開始します。

✍ リストアされた設定情報は再起動後に有効になります。

❗ リストアに失敗した場合、以下の項目を確認してください。

- 指定したファイルが旧モデルのバックアップファイルかどうか。
- 取得したファイルを編集していないか。

5. ファームウェアアップデート

Web Beagle では、機能追加や不具合対応によりファームウェアの提供を行うことがあります。最新のファームウェアは弊社ウェブページをご確認の上、入手してください。

<https://store.atworks.co.jp> (<https://store.atworks.co.jp>)

❗ ファームウェアのアップデートを行う前に「設定情報のバックアップ」を実施し、設定情報を控えておいてください。

📖 「設定情報のバックアップ」については「5章 - 設定情報のバックアップ (./chapter_5.html#設定情報のバックアップ)」を参照してください。

❗ ファームウェアのアップデート中は、管理画面の操作、ブラウザの操作を行わないでください。ファームウェアのアップデート失敗やWeb Beagle 本製品の故障の原因となる場合があります。

ファームウェアバージョンの確認

Web Beagle のファームウェアのバージョンは下記の手順で確認することができます（図4-26）。

【運用管理】 → 【ファームウェア】 を選択してください。

ファームウェア

ファームウェア

モデル名 WebBeagle Model 600

バージョン 2.0.5

図4-26 バージョン表示画面

ファームウェアのアップデート

❶ 本手順はWeb Beagle の再起動が発生します。

1. 弊社ウェブページより、更新するファームウェアをダウンロードしてください。
<https://store.atworks.co.jp> (<https://store.atworks.co.jp>)
2. 【運用管理】 → 【ファームウェア】 を選択してください。
3. 取得したファームウェアを画面にドラッグするかクリックすると表示されるディレクトリ一覧からファームウェアを選択します。
4. ファームウェアを選択後、「**アップデート**」をクリックするとファームウェアのアップデートが開始されます（図4-27）。ファームウェアのアップデートに成功すると、自動的に再起動が実施されます。再起動後に再度「ファームウェアバージョンの確認」手順にてアップデートされたことを確認してください。

ファームウェアアップデート

ファイルをドラッグ&ドロップするか、クリックしてファイルを選択してください。

アップデート処理中の間は、このウィンドウ画面を閉じたり、本装置を再起動しないでください。

ここにファイルをドロップしてアップロードしてください。

アップデート

図4-27 ファームウェアアップデート画面

6.通知設定

Web Beagle では、機器の状態や仮想サービスの状態を通知する手段として、以下の通知設定をサポートしています。

- **メール通知**
- **SNMP**

- Syslog

メール通知

Web Beagle で検出したメッセージを管理者へメールで通知する機能です。

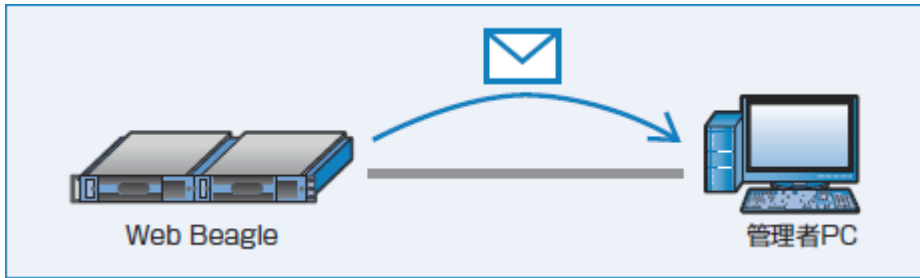


図4-28 メール通知

送信するメッセージは以下の内容です。

- Web Beagle 自身がマスター／スタンバイ状態で稼動開始したことの通知
- 仮想サービスに登録されているノードサーバの死活監視の異常／復旧通知
- 仮想サービスに登録されているノードサーバを管理画面から切り離し／復旧したときの通知

メール通知設定手順

1. 【通知設定】 → 【メール通知設定】を選択し、「編集」をクリックしてください（図4-29）。
2. 以下のように設定を行い、「入力内容確認」をクリックし内容に問題がなければ「更新」をクリックしてください。

- **メール通知**
 - 「有効」 チェックボックスにチェックをいれます。
- **SMTP サーバIP アドレス**
 - メール送信に用いる SMTP サーバの IP アドレスを設定します。
- **差出人アドレス**
 - 通知メールの差出人メールアドレスを設定します。
- **宛先アドレス**
 - 通知メールの宛先メールアドレスを設定します。

The screenshot shows the 'メール通知設定編集' (Edit Email Notification Settings) page. At the top, it says 'メール通知設定' (Email Notification Settings). Below this, there are four settings:

- メール通知 ***: A radio button is selected for '有効' (Enabled).
- SMTPサーバIPアドレス ***: A text input field containing '0.0.0.0'.
- 差出人アドレス ***: An empty text input field.
- 宛先アドレス ***: An empty text input field.

At the bottom of the form, there are two buttons: 'キャンセル' (Cancel) and '入力内容確認' (Check Input Content).

設定した宛先アドレスにメールが通知されることを確認してください。

❶ SMTP サーバに指定するメールサーバでは、宛先アドレスに指定したメールを受信または中継する設定になっている必要があります。

❷ 通知メールの内容については「付録 - 付録B. 通知メールの内容 (/appendix.html#付録b.-通知メールの内容)」を参照してください。

Syslog

Web Beagle が出力するSyslog をSyslog サーバに転送する機能です。

❗ Syslog の出力内容については、マニュアルにてサポートしておりません。

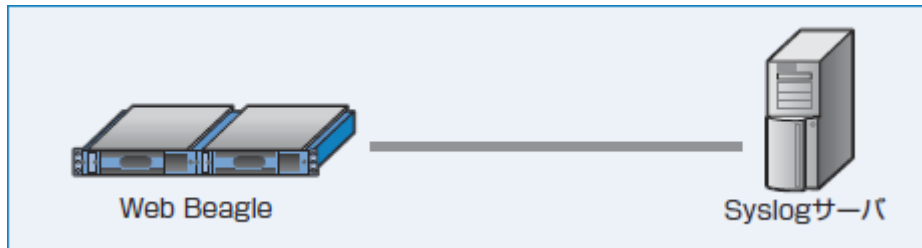


図4-30 Syslog サーバとの通信

Syslog 設定通知手順

1. 【通知設定】 → 【Syslog】を選択し、「編集」をクリックしてください。
2. 以下のように設定を行い、「入力内容確認」をクリックし内容に問題がなければ「更新」をクリックしてください。

Syslog を有効にする場合

- **ログを外部Syslogサーバに転送**
 - 「転送する」チェックボックスにチェックをいれます。
- **SyslogサーバIP アドレス**
 - Syslog の転送先サーバを設定します。
- **ファシリティ**
 - Syslog のファシリティ を設定します。
- **カーネルログ転送**
 - Web Beagle のカーネルログも採取する場合、「転送する」チェックボックスにチェックをいれます（通常は使用しません）。

The screenshot shows the 'Syslog設定編集' (Syslog Configuration Edit) page. The title is 'Syslog設定' (Syslog Configuration). There are four main settings:

- ログを外部Syslogサーバに転送 ***: A checkbox labeled '転送する' (Transfer) is checked.
- SyslogサーバIPアドレス ***: A text input field containing '0.0.0.0'.
- ファシリティ ***: A dropdown menu showing 'LOCAL0'.
- カーネルログ転送**: A checkbox labeled '転送する' (Transfer) is checked.

At the bottom, there are two buttons: 'キャンセル' (Cancel) and '入力内容確認' (Check Input Content).

図4-31 Syslog 設定画面

Syslog サーバの設定

Syslog サーバにて、Web Beagle のSyslog を受信できるよう設定してください。設定後、Web Beagle からのSyslog が受信されていることを確認してください。

第5章 管理画面の機能説明

❗ 入力画面の各項目名の後に記載されている「*」の文字は必須入力を意味します。もし入力がされない場合エラーメッセージが表示されます。

1. ログイン画面

1. Web Beagle のログイン画面を表示します。
ブラウザにて以下の URI を入力します。
https://【Web Beagle に設定したIP アドレス】:18180/
2. Web Beagle にログインします。
ログイン名・ログインパスワードを、入力してログインします。
❗ パスワードを忘れた場合は、「6章 - 管理者パスワードを忘れた場合 (./chapter_6.html#管理者パスワードを忘れた場合)」を参照してください。

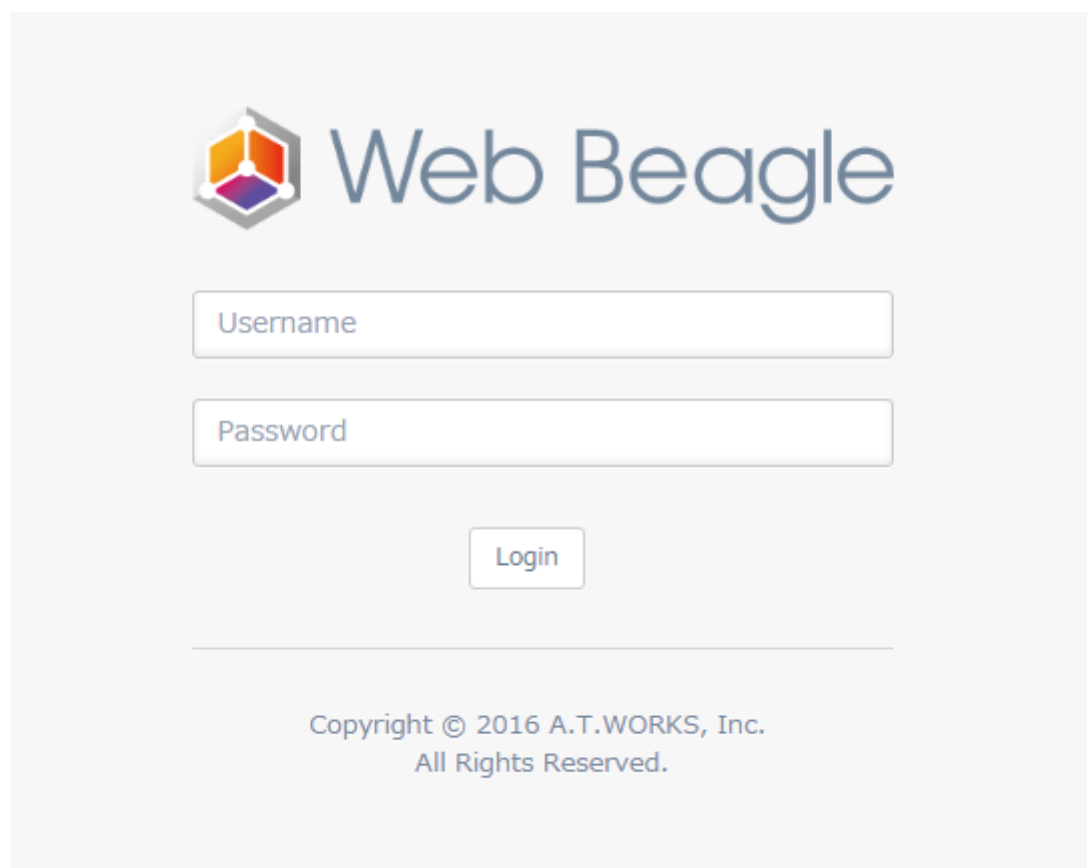


図5-1 ログイン画面

ログインに成功すると、管理画面が表示されます。

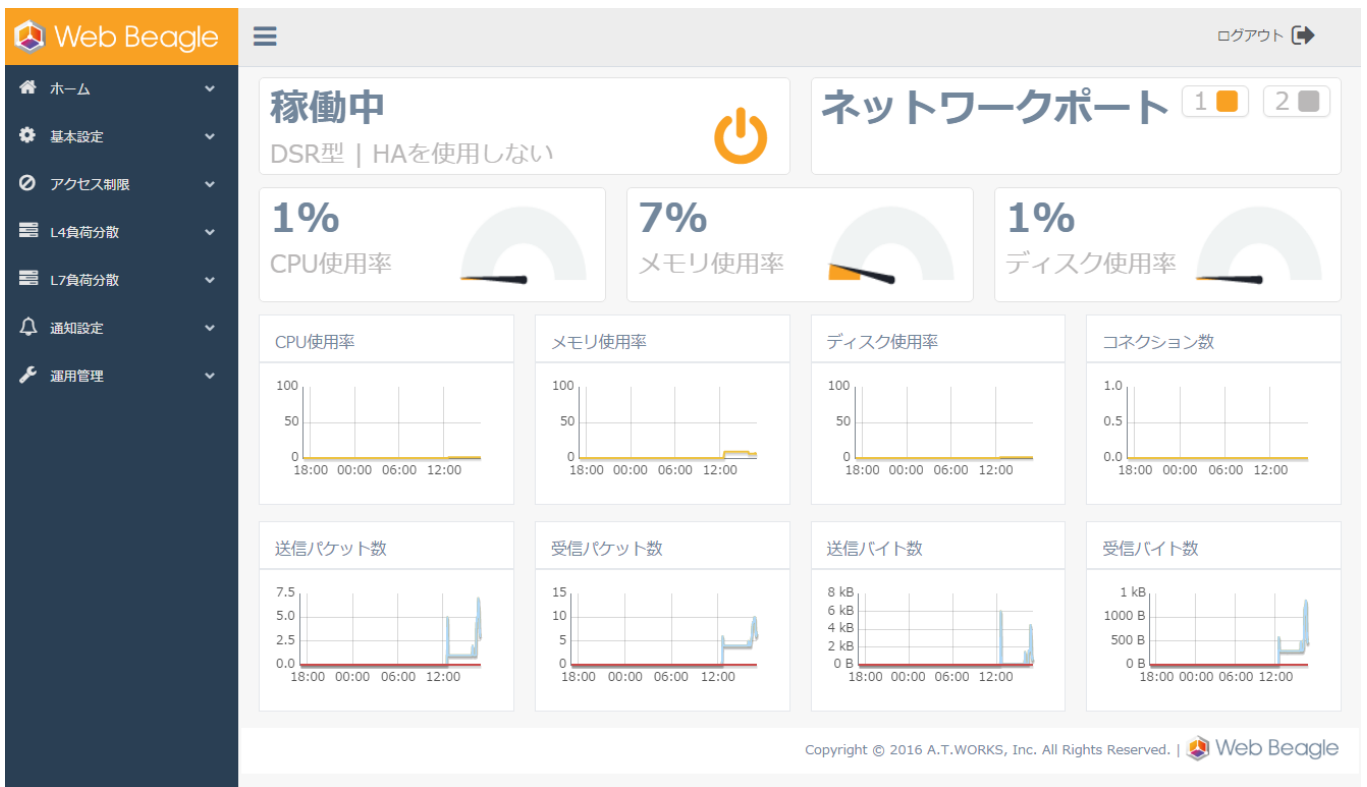


図5-2 管理画面

Web Beagle は以下のメニューで構成されています。

- **ホーム**
 - **ダッシュボード**
Web Beagle の機器の状態と接続数、パケット数、バイト数のグラフを表示します。
📄 「5章 - ダッシュボード (./chapter_5.html#ダッシュボード)」
- **基本設定**
 - **ネットワーク**
Web Beagle のネットワーク設定を表示・編集する場合に使用します。
📄 「5章 - ネットワーク (./chapter_5.html#ネットワーク)」
 - **NAT 設定**
Web Beagle のNAT 設定を表示・編集する場合に使用します。
✍️ 動作方式がNAT 型の場合のみ、表示されます。
📄 「5章 - NAT 設定 (./chapter_5.html#nat-設定)」
 - **冗長化設定**
Web Beagle の冗長化設定を表示・編集する場合に使用します。
📄 「5章 - 冗長化設定 (./chapter_5.html#冗長化設定)」
- **アクセス制限**
 - **パスワード変更**
Web Beagle の管理画面にログインするためのパスワードを変更する場合に使用します。
📄 「5章 - パスワード変更 (./chapter_5.html#パスワード変更)」
 - **接続許可IPアドレス**
Web Beagle の管理画面に接続を許可するIP アドレスの表示・変更する場合に使用します。
📄 「5章 - 接続許可IP アドレス (./chapter_5.html#接続許可ip-アドレス)」
- **L4負荷分散**
 - **L4仮想サービス**
Web Beagle のL4仮想サービスを表示・変更する場合に使用します。
📄 「5章 - L4 仮想サービス (./chapter_5.html#l4-仮想サービス)」

- **仮想サービスのIP アドレス**
Web Beagle のノードサーバを表示・変更する場合に使用します。
✍ 仮想サービスを作成後、表示されます。
📄 「5章 - L4 ノードサーバー一覧 (./chapter_5.html#l4-ノードサーバー一覧)」
- **L7負荷分散**
 - **L7仮想サービス**
Web Beagle のL7仮想サービスを表示・変更する場合に使用します。
📄 「5章 - L7 仮想サービス (./chapter_5.html#l7-仮想サービス)」
 - **仮想サービスのIP アドレス**
Web Beagle のノードサーバを表示・変更する場合に使用します。
✍ 仮想サービスを作成後、表示されます。
📄 「5章 - L7 ノードサーバー一覧 (./chapter_5.html#l7-ノードサーバー一覧)」
- **通知設定**
 - **Syslog**
Web Beagle のログをSyslog に転送する設定を表示・変更する場合に使用します。
📄 「5章 - Syslog (./chapter_5.html#syslog)」
 - **SNMP**
Web Beagle のSNMP 設定を表示・変更する場合に使用します。
📄 「5章 - SNMP (./chapter_5.html#snmp)」
 - **メール通知設定** Web Beagle の状態をメールで通知する設定を表示・変更する場合に使用します。
📄 「5章 - メール通知設定 (./chapter_5.html#メール通知設定)」
- **運用管理**
 - **ログ**
Web Beagle のログを管理画面から確認したい場合に使用します。
📄 「5章 - ログ (./chapter_5.html#ログ)」
 - **バックアップ/リストア**
Web Beagle の設定のバックアップとリストアを行う場合に使用します。
📄 「5章 - バックアップ/リストア (./chapter_5.html#バックアップリストア)」
 - **ファームウェア**
Web Beagle のファームウェア情報の表示・アップデートを行う場合に使用します。
📄 「5章 - ファームウェア (./chapter_5.html#ファームウェア)」
 - **サポート情報取得**
Web Beagle のサポート情報を取得する場合に使用します。
📄 「5章 - サポート情報取得 (./chapter_5.html#サポート情報取得)」
 - **再起動**
Web Beagle の再起動やシャットダウンを行う場合に使用します。
📄 「5章 - 再起動 (./chapter_5.html#再起動)」
 - **各種初期化**
Web Beagle のグラフデータやログの初期化する場合に使用します。
📄 「5章 - 各種初期化 (./chapter_5.html#各種初期化)」
- **ログアウト**
 - **ログアウト**
Web Beagle の管理画面からログアウトします。

2. ホーム

ダッシュボード

Web Beagle の機器の状態を表示します。

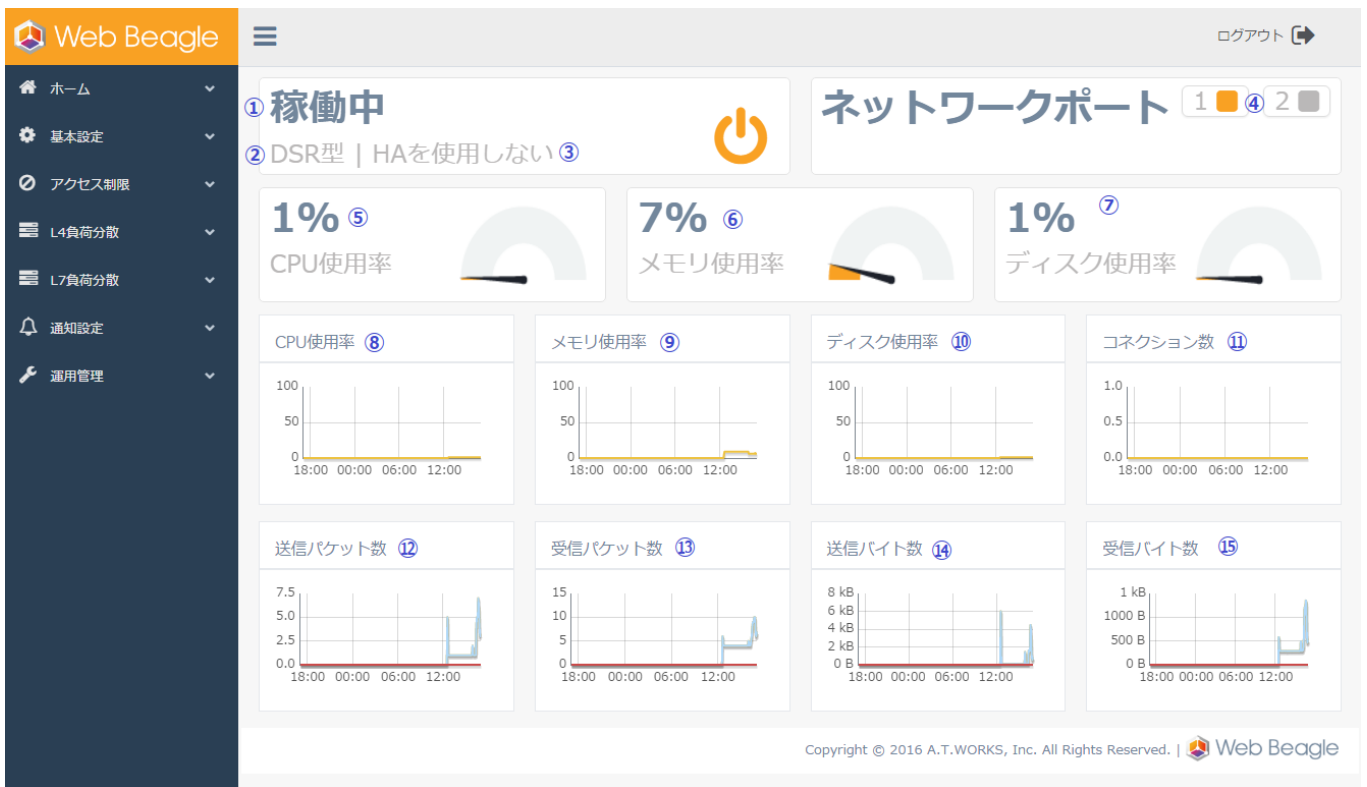


図5-3 ダッシュボード

1. 機器の動作状態

Web Beagle の現在の動作状態を表示します。稼働中、待機中、待機中(未同期)

2. 動作方式

Web Beagleの現在の動作方式を表示します。

DSR 型、NAT 型、透過型のいずれかとなります。

3. 役割

Web Beagle の現在の役割を表示します。

マスター、スタンバイ、HA を使用しないのいずれかとなります。

4. ネットワークポート

Web Beagle に接続されているネットワークポートの状態を表示します。

点灯している場合そのポートは接続されています。

※M600 では DSR でボンディングありの時にはポート2/4 は使用しませんが、それらのポートにネットワーク機器接続した場合にはLink 状態が接続状態(オレンジ色)に見えます。しかしポート2/4 を使ってWebBeagle が通信することはないため、実際の動作に支障はございません。

5. CPU 使用率

Web Beagle の現在のCPU 使用率を表示します。

6. メモリ使用率

Web Beagle の現在のメモリ使用率を表示します。

7. ディスク使用率

Web Beagle の現在のディスク使用率を表示します。

8. CPU 使用率グラフ

Web Beagle の直近24時間のCPU 使用率グラフを表示します。

クリックすると拡大されたグラフが表示されます。

9. メモリ使用率グラフ

Web Beagle の直近24時間のメモリ使用率グラフを表示します。

クリックすると拡大されたグラフが表示されます。

10. ディスク使用率グラフ

Web Beagle の直近24時間のディスク使用率グラフを表示します。

クリックすると拡大されたグラフが表示されます。

11. コネクション数グラフ

Web Beagle の直近24時間のコネクション数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

12. 送信パケット数

Web Beagle の直近24時間の送信パケット数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

13. 受信パケット数

Web Beagle の直近24時間の受信パケット数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

14. 送信バイト数

Web Beagle の直近24時間の送信バイト数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

15. 受信バイト数

Web Beagle の直近24時間の受信バイト数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

✂ 拡大されたグラフでは、日付を指定して検索することが可能です。

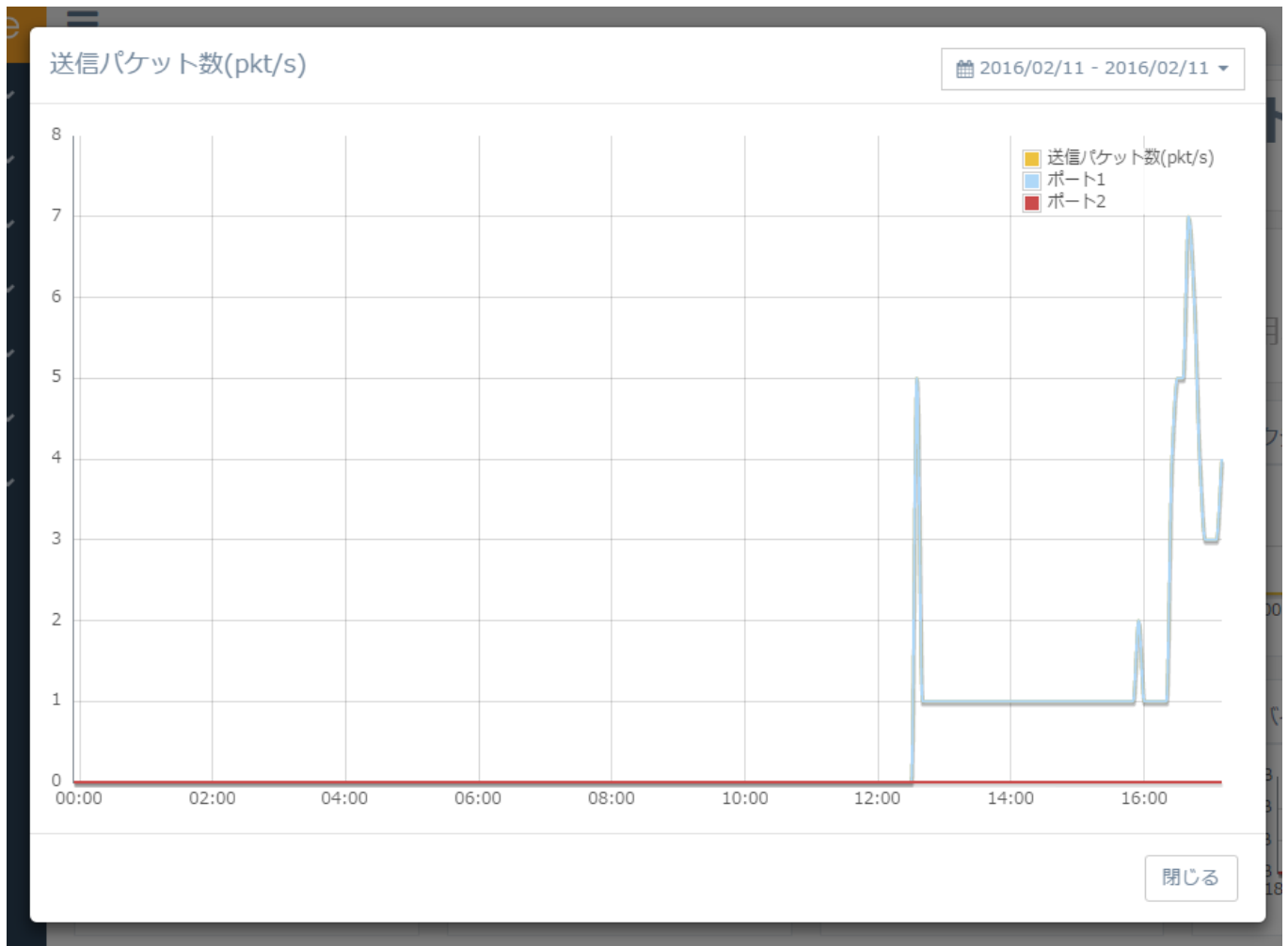


図5-4 拡大されたグラフ

❗ 同一の値の場合、後に描画される線が上に重なって表示されます。

2. 基本設定

ネットワーク

Web Beagle のネットワーク設定を表示・編集する場合に使用します。

ネットワーク設定表示

ネットワーク設定

ネットワーク

動作方式 *① NAT型

ホスト名 *② webbeagle

IPアドレス *③ 192.168.24.44

ネットマスク *④ 255.255.255.0

ゲートウェイ *⑤ 192.168.24.1

プライマリDNS ⑥ 192.168.24.100

セカンダリDNS ⑦ 192.168.24.101

NTPサーバ ⑧ ntp.nict.jp

管理画面接続ポート(SSL) ⑨ 18180

NAT内側のインタフェース

IPアドレス *⑩ 192.168.1.1

ネットマスク *⑪ 255.255.255.0

NAT内側から管理画面へのアクセス*⑫ 許可する

⑬ 編集

図5-5 ネットワーク設定表示

1. 動作方式

Web Beagleの現在の動作方式を表示します。
DSR 型、NAT 型、透過型のいずれかとなります。

2. ホスト名

Web Beagle のホスト名を表示します。

3. IP アドレス

Web Beagle のIP アドレスを表示します。

4. ネットマスク

Web Beagle のネットマスクを表示します。

5. ゲートウェイ

Web Beagle のゲートウェイを表示します。

6. プライマリDNS

Web Beagle の参照するプライマリDNS サーバを表示します。

7. セカンダリDNS

Web Beagle の参照するセカンダリDNS サーバを表示します。

8. NTP サーバ

Web Beagle の参照するNTP サーバを表示します。

9. 管理画面接続ポート (SSL)

Web Beagle の管理画面に接続するためのSSL ポートを表示します。

10. IP アドレス

NAT 内側のインターフェイスのIP アドレスを表示します。

(ここで設定するIPアドレスは仮想IPとなり、L4負荷分散の場合LAN側ネットワークのノードサーバはこれをゲートウェイとして通信を行いますので、ノードサーバにこのIPをゲートウェイとして設定してください。ただし、L7負荷分散の場合はその限りではありません。)

11. ネットマスク

NAT 内側のインターフェイスのネットマスクを表示します。

12. NATの内側から管理画面へのアクセス

NAT の内側から管理画面へのアクセスを許可するかどうかを表示します。

13. 【編集】

Web Beagleのネットワーク設定編集画面に移ります。

✎ ⑩、⑪、⑫の項目は動作方式がNAT 型の場合のみ表示されます。

📢 ⑥、⑦、⑧の項目は、メール通知を使用する場合に必要となります。

ネットワーク設定編集 (※役割がマスターまたはHA を使用しない場合)

ネットワーク編集

ネットワーク

動作方式 * ① DSR型 ▼

ホスト名 * ② webbeagle

IPアドレス * ③ 192.168.24.44

ネットマスク * ④ 255.255.255.0

ゲートウェイ * ⑤ 192.168.24.1

プライマリDNS ⑥ 192.168.24.100

セカンダリDNS ⑦ 192.168.24.101

NTPサーバ ⑧ ntp.nict.jp

管理画面接続ポート(SSL) ⑨ 18180

NAT内側のインタフェイス

IPアドレス * ⑩ 192.168.1.1

ネットマスク * ⑪ 255.255.255.0

NAT内側から管理画面へのアクセス * ⑫ 許可する

⑬ キャンセル ⑭ 入力内容確認

図5-6 ネットワーク設定編集

1. 動作方式

Web Beagleの現在の動作方式を設定します。

DSR 型、NAT 型、透過型のいずれかとなります。

- **Model 500, Model 600**
DSR 型・NAT 型・透過型のいずれか
- **Model 400**
DSR 型固定

2. ホスト名

Web Beagle のホスト名を設定します。

3. IP アドレス

Web Beagle のIP アドレスを設定します。

4. ネットマスク

Web Beagle のネットマスクを設定します。

5. ゲートウェイ

Web Beagle のゲートウェイを設定します。

6. プライマリDNS

Web Beagle の参照するプライマリDNS サーバを設定します。

7. セカンダリDNS

Web Beagle の参照するセカンダリDNS サーバを設定します。

8. NTP サーバ

Web Beagle の参照するNTP サーバを設定します。

9. 管理画面接続ポート (SSL)

Web Beagle の管理画面に接続するためのSSL ポートを設定します。

10. IP アドレス

NAT 内側のインターフェイスのIP アドレスを設定します。

(ここで設定するIPアドレスは仮想IPとなり、L4負荷分散の場合LAN側ネットワークのノードサーバはこれをゲートウェイとして通信を行いますので、ノードサーバにこのIPをゲートウェイとして設定してください。ただし、L7負荷分散の場合はその限りではありません。)

11. ネットマスク

NAT 内側のインターフェイスのネットマスクを設定します。

12. NATの内側から管理画面へのアクセス

NAT の内側から管理画面へのアクセスを許可するには、「許可する」にチェックを入れます。

13. 【キャンセル】

Web Beagleのネットワーク設定画面に戻ります。

14. 【入力内容確認】

Web Beagleのネットワーク設定編集入力内容確認画面に移ります。

✍ ⑩、⑪、⑫の項目は動作方式がNAT 型の場合のみ表示されます。

ネットワーク設定編集 (※役割がスタンバイの場合)

ネットワーク編集

ネットワーク

ホスト名 * ① wb2

IPアドレス * ② 192.168.24.41

ネットマスク * ③ 255.255.255.0

④ キャンセル ⑤ 入力内容確認

図5-7 ネットワーク設定編集(スタンバイ)

1. ホスト名

Web Beagle のホスト名を設定します。

2. IP アドレス

Web Beagle のIP アドレスを設定します。

3. ネットマスク

Web Beagle のネットマスクを設定します。

4. 【キャンセル】

Web Beagleのネットワーク設定画面に戻ります。

5. 【入力内容確認】

Web Beagleのネットワーク設定編集入力内容確認画面に移ります。

NAT 設定

Web Beagle のNAT 設定を表示・編集する場合に使用します。

動作方式がNAT 型のときのみ表示されます。

NAT設定の目的は、NAT構成を行うケースで、外側ネットワークのクライアントから内側ネットワークのノードサーバに対して、WebBeagleを経由しアクセスできる事に対応する為です。

想定されるユースケースとしましては、ノードサーバがWebサーバであり、そのサーバの定期的なメンテナンス目的のために 外側ネットワークまたは更に その外側にあるクライアントから ssh にてWebサーバへアクセスしたり、Webアプリコンテンツを転送するために、外側のクライアントからftpでアクセスする等があります。

これを実現するために、基本NATまたはNAPT(IPマスカレード)の設定機能を用意しています。

基本NAT

外側IP アドレスと内側IP アドレスを1 対1 で対応させます。

基本NAT設定にて、

- 外側IPアドレス ※ 1 (外側ネットワークで空きのある適当なアドレスで、負荷分散用とは別の仮想IP の様なものとなります)
- 内側IPアドレス (内側ネットワークにあるノードサーバのIPアドレス)

としておき、外側ネットワークにあるクライアントから <※ 1 のIP> でアクセスすれば、WebBeagle が <内側IPアドレス> へ橋渡しします。(このとき通信ポートはWebBeagleで変換しません)

❗ 基本NATでは外側IPアドレスと内側ネットワークにあるノードサーバのIPを一对一で紐づけるため、ノードサーバの数分だけ外側IPアドレスを用意する必要があります。

NAT設定編集

基本NAT

外側IPアドレス * ①

内側IPアドレス * ②

③

外側IPアドレス	内側IPアドレス	
10.1.1.11	192.168.1.11	<input type="button" value="編集"/> <input type="button" value="削除"/>

④ ⑤

図5-8 基本NAT

1. 外側IP アドレス

外側のIP アドレスを設定します。外側ネットワークに空きのあるIPアドレスを設定して下さい。

2. 内側IP アドレス

内側のIP アドレスを設定します。対応させるノードサーバのIPアドレスを設定して下さい。

3. 【追加】

基本NAT を基本NAT 一覧に追加します。

4. 【編集】

選択した基本NAT を編集します。

クリックすると入力エリアに値が表示されますので値を編集後、追加ボタンを押して下さい。

5. 【削除】

基本NAT を削除します。

NAPT (IP マスカレード)

外側のポートに対するアクセスを内側IP アドレスのポートに転送します。

NAPT設定にて、

- 外側ポート (システムで使える適当なポート、well-known以外が望ましい)
- 内側IPアドレス (ノードサーバのIPアドレス)
- 内側ポート (外側ポートから変換する内側ポートで、通信したいアプリケーションプロトコルに対応したポートを指定)
- プロトコル (通信したいアプリケーションプロトコルに応じて、ALL/TCP/UDPから選びます)

としておき、外側ネットワークにあるクライアントから <WebBeagleの外側の実IP:外側ポート> でアクセスすると、WebBeagle が <内側IP:内部ポート> へ通信を橋渡しします。

❗ NAPTではNATと違い対応させる外側IPアドレスを消費しないのがメリットです。但し、WebBeagleに対してノードサーバの数分だけ外側ポートを用意する必要があります。

NAPT

外側ポート * ① 3129

内側IPアドレス * ② 192.168.1.13

内側ポート * ③ 8081

プロトコル * ④ TCP

⑤ 追加

外側ポート	内側IPアドレス	内側ポート	プロトコル	
3128	192.168.1.12	8080	ALL	編集 削除

⑥ ⑦

図5-9 NAPT (IP マスカレード)

1. 外側ポート

外側のポートを設定します。構成するネットワークで使える適当なポートを割り当てて下さい。

2. 内側IP アドレス

内側のIP アドレスを設定します。対応させるノードサーバのIPアドレスを設定して下さい。

3. 内側ポート

内側のポートを設定します。通信したいアプリケーションプロトコルに対応したポートを指定して下さい。

さい。

4. プロトコル

NAPT を行うプロトコルを設定します。ALL、TCP、UDP のいずれかとなります。通信したいアプリケーションプロトコルに応じて選択して下さい。

5. 【追加】

NAPT をNAPT 一覧に追加します。

6. 【編集】

選択したNAPT を編集します。

クリックすると入力エリアに値が表示されますので値を編集後、追加ボタンを押してください。

7. 【削除】

NAPT を削除します。

NAT 内から外への通信許可

The screenshot shows a web interface for configuring NAT settings. At the top, the title 'NAT内から外への通信許可' is displayed. Below the title, there is a section with a sub-title 'NAT内から外への通信許可' and a checkbox labeled '許可する'. A circled '1' is placed above the checkbox. Below this section, there is a blue button labeled '入力内容確認' with a circled '2' above it.

図5-10 NAT 内から外への通信許可

1. NAT 内から外への通信許可

NAT 内から外への通信許可するには、このチェックボックスにチェックを入れます。

2. 【入力内容確認】

NAT 設定の入力内容確認画面に移ります。

❗ 入力内容確認画面で「更新」をクリックすると、Web Beagle に設定が反映されます。

冗長化設定

Web Beagle の冗長化設定を表示・編集する場合に使用します。

冗長化設定の表示

冗長化設定

冗長化設定

役割***①** マスター

パートナーIPアドレス ***②** 192.168.24.41

同期パスワード ***③** syncpassword

VRID ***④** 100

NAT内側の管理画面のIPアドレス***⑤** 192.168.1.8
*

現在の動作状態**⑥** 稼働中

⑦

編集

図5-11 冗長化設定の表示

1. 役割

Web Beagleの現在の役割を表示します。HA を使用しない、マスター、スタンバイのいずれかとなります。

2. パートナーIP アドレス

パートナー機のIP アドレスを表示します。

3. 同期パスワード

パートナー機と情報を同期するためのパスワードを表示します。

4. VRID

VRRP で使用するVRID を表示します。

5. NAT 内側の管理画面のIP アドレス

NAT の内側から管理画面へのアクセスするためのIP アドレスを表示します。


(ここに表示されるIPアドレスは、Web BeagleのLAN側ネットワークポートの実IPです。)

6. 現在の動作状態

Web Beagleの現在の動作状態を表示します。稼働中、待機中、待機中(未同期)のいずれかとなります。

7. 【編集】

Web Beagleの役割の変更画面に移ります。

 **⑤**の項目は動作方式がNAT 型の場合のみ表示されます。

現在の動作状態が待機中の場合

冗長化設定

冗長化設定

役割*	スタンバイ
パートナーIPアドレス *	192.168.24.44
同期パスワード *	syncpassword
VRID *	100
現在の動作状態	待機中

同期情報のクリア ⑧

編集

図5-12 現在の動作状態が待機中の場合

8. 同期情報のクリア

マスターとの同期情報をクリアします。クリアを行うとマスター機から同期情報が再送されます。マスター機が変更になった場合など、強制的にスタンバイ機の同期情報を更新する場合に使用します。

役割がスタンバイの場合かつ現在の動作中が稼働中の場合

冗長化設定

役割*	スタンバイ
パートナーIPアドレス *	192.168.24.44
同期パスワード *	syncpassword
VRID *	100
現在の動作状態	稼働中

編集 マスターに昇格 ⑨

図5-13 役割がスタンバイの場合かつ現在の動作中が稼働中の場合

9. マスターに昇格します【実行】

Web Beagleの役割をバックアップからマスターに変更します。
元のマスターであったパートナー機については、手動で役割をスタンバイに変更してください。

冗長化設定の編集

冗長化設定編集

冗長化設定

役割 * ① マスター

パートナーIPアドレス * ② 192.168.24.41

同期パスワード * ③ syncpassword

VRID * ④ 100

NAT内側の管理画面のIPアドレス * ⑤ 192.168.1.8

⑥ キャンセル ⑦ 入力内容確認

図5-14 冗長化設定の編集

1. 役割

Web Beagleの現在の役割を変更します。HAを使用しない、マスター、スタンバイのいずれかとなります。

マスターおよびスタンバイの場合はさらにパートナーIPアドレス、同期パスワード、VRIDを設定します。

2. パートナーIPアドレス

パートナー機のIPアドレスを変更します。

Web Beagleがマスター機の場合は同期対象のスタンバイ機のIPアドレスを、Web Beagleがスタンバイ機の場合は同期対象のマスター機のIPアドレスを入力してください。

3. 同期パスワード

パートナー機と情報を同期するためのパスワードを変更します。

マスター機とスタンバイ機で同じパスワードを入力してください。

❶ 同期パスワードは、第三者に推測されにくい、独自の文字列を設定してください。

同期パスワードには、半角英数字のみ使用可能です。

4. VRID

VRIDで使用するVRIDを変更します。

マスター機とスタンバイ機で同じVRIDを入力してください。

❶ VRIDは1から255までの整数を設定することができます。冗長化構成を行う機器同士には同じ値を設定します。同一ネットワーク内の機器にVRRPを使用する機器がある場合には、設定されているVRIDを調査の上、重複しないように設定してください。同一ネットワーク内に、冗長化構成の別のWeb Beagleを設置する場合にもVRIDが重複しないように設定してください。

5. NAT内側の管理画面のIPアドレス

NATの内側から管理画面へのアクセスするためのIPアドレスを設定します。

(ここで設定するIPアドレスは、Web BeagleのLAN側ネットワークポートの実IPです。)

6. 【キャンセル】

編集を中止します。

7. 【入力内容確認】

入力された内容に問題がなければ入力内容確認画面に移ります。

✎ ⑤の項目は動作方式がNAT型の場合のみ設定できます

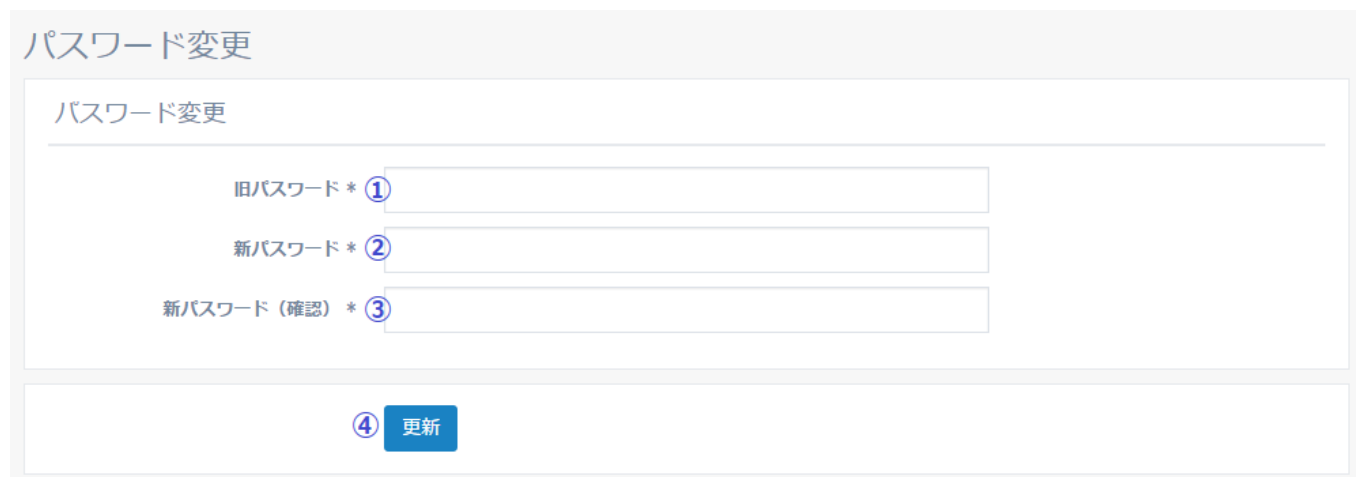
✎ ⑦のボタンクリック後、「更新」ボタンをクリックすると値が反映されます。

機器の再起動は必要ありません。

3. アクセス制限

パスワード変更

Web Beagle のネットワーク設定を表示・編集する場合に使用します。



パスワード変更

パスワード変更

旧パスワード * ①

新パスワード * ②

新パスワード (確認) * ③

④ 更新

図5-15 パスワード変更

1. 旧パスワード

現在のパスワードを入力します。パスワードが一致しなければ変更できません。

2. 新パスワード

新しいパスワードを入力します。

3. 新パスワード (再入力)

新しいパスワードを再入力します。

新パスワードと再入力したパスワードが一致しなければ変更できません。

4. 【更新】

Web Beagleにパスワードの変更を適用します。

接続許可IP アドレス

Web Beagle の管理画面への接続を許可するIP アドレスを表示・設定する場合に使用します。

❗ 工場出荷時はどのIP アドレスからも管理画面へ接続を許可する状態です。

接続許可IP アドレス

Web Beagle の管理画面に接続を許可するIP アドレスを表示します。

接続許可IPアドレス

接続許可IPアドレス

① IPアドレス	② ネットマスク
192.168.23.143	255.255.255.0

③
編集

図5-16 接続許可IP アドレス

1. IP アドレス

管理画面に接続を許可するIP アドレスを表示します。

2. ネットマスク

管理画面に接続を許可するネットマスクを表示します。

3. 【編集】

管理画面に接続を許可するIP アドレスの一覧を編集します。

接続許可IP アドレス一覧編集

Web Beagle の管理画面に接続を許可するIP アドレスの一覧を編集します。

接続許可IPアドレス

接続許可IPアドレス

IPアドレス * ①

ネットマスク * ②

③ 追加

IPアドレス	ネットマスク		
192.168.23.143	255.255.255.0	編集	削除

④ ⑤

⑥
入力内容確認

図5-17 接続許可IP アドレス一覧編集

1. IP アドレス

追加または編集するIP アドレスを指定します。

2. ネットマスク

追加または編集するネットマスクを指定します。

3. 【追加】

Web Beagleの管理画面に接続を許可するIP アドレスを下記の一覧に追加します。

4. 【編集】

選択したIP アドレスを入力エリアに設定します。

5. 【削除】

選択したIP アドレスを一覧から削除します。

6. 【入力内容確認】

入力内容確認画面に移ります。

① 入力内容確認画面で「更新」 ボタンをクリックすると設定はただちに反映されます。

4. L4 負荷分散

L4 仮想サービス

Web Beagle のL4 仮想サービスを表示・変更する場合に使用します。

L4 仮想サービス一覧

L4 仮想サービスの一覧を表示します。

The screenshot shows the 'L4ロードバランサ設定' (L4 Load Balancing Settings) page. At the top, there are two numbered callouts: ① pointing to the 'L4仮想サービス一覧' (L4 Virtual Service List) title and ② pointing to the 'リフレッシュ' (Refresh) and '追加' (Add) buttons. Below the title, there is a search bar with a search icon and a search input field (callout ④). To the left of the search bar is a dropdown menu for '件表示' (Items per page) set to '10' (callout ③). The main content is a table with columns: '状態' (Status), '仮想IPアドレス' (Virtual IP Address), 'ポート' (Port), '分散方式' (Distribution Method), '有効' (Enabled), and '稼働中 / 全ノードサーバ数' (Operational / Total Node Server Count). The table contains two rows. The first row has a grey status icon (callout ⑤), IP '192.168.24.213' (callout ⑥), port '80/TCP' (callout ⑦), distribution method '重み付けラウンドロビン' (callout ⑧), status 'NO' (callout ⑨), and count '0/1' (callout ⑩). To the right of this row are buttons: 'フィルタ' (Filter), '編集' (Edit), '有効' (Enable), and '削除' (Delete), with callouts ⑪, ⑫, ⑬, and ⑭ respectively. The second row has a green status icon, IP '192.168.24.38', port '80/TCP', distribution method 'ラウンドロビン', status 'YES', and count '4/4'. Below the table, there is a pagination bar showing '2件中 1 から 2 まで表示' (Showing 1 to 2 of 2 items) with callout ⑮. At the bottom right, there are navigation buttons: '先頭' (First), '前' (Previous), '1' (Current page), '次' (Next), and '最終' (Last), with callouts ⑯, ⑰, ⑱, and ⑲ respectively. At the very bottom, there are additional callouts ⑳ and ㉑ pointing to the bottom of the page.

図5-18 L4 仮想サービス一覧

1. 【リフレッシュ】

仮想サービスの状態の表示を更新します。

2. 【追加】

仮想サービスを追加します。

3. 表示件数

一覧に表示するデータの数を指定します。

4. 検索条件

一覧に表示するデータの検索条件を指定します。

5. 状態

仮想サービスの状態を表示します。

- 緑：全てのノードサーバが稼働中です。
- 黄：いくつかのノードサーバがダウンしています。
- 赤：全てのノードサーバがダウンしています。
- 灰：仮想サービスが無効です。
のいずれかの色で表されます。

6. 仮想IP アドレス

仮想サービスの仮想IP アドレスを表示します。

7. ポート

仮想サービスのポート、プロトコル表示します。

8. 分散方式

仮想サービスの分散方式を表示します。

- ラウンドロビン
 - 重み付けラウンドロビン
 - 最小コネクション
 - 重み付け最小コネクション
 - ソースハッシング
 - 最速応答時間
- のいずれかとなります。

9. **有効**

仮想サービスが有効ならばYES、無効ならばNO

10. **稼動中/全ノードサーバ数**

全ノードサーバ中、稼動中のサーバ数を表示します。

11. **【フィルタ】**

仮想サービスのIPフィルタ設定画面を表示します。

12. **【編集】**

仮想サービスの編集画面を表示します。

13. **【無効】・【有効】**

有効な仮想サービスを無効にします。

無効な仮想サービスは有効にします。

14. **【削除】**

仮想サービスを削除します。

15. **【件数】**

一覧に表示中の件数の範囲を表示します。

16. **【先頭】**

一覧の先頭のページを表示します。

17. **【前】**

前のページを表示します。

18. **【ページ番号】**


選択したページを表示します。

19. **【次】**

次のページを表示します。

20. **【最終】**

最終ページを表示します。

 本画面では、仮想サービスの状態を更新するために60秒に1回画面をリフレッシュします。

仮想サービス追加／編集

L4ロードバランサ設定

仮想サービス追加/編集

仮想IPアドレス * ① 192.168.24.38

ポート * ② 80

プロトコル * ③ TCP

分散方式 * ④ ラウンドロビン

待機サーバ ⑤ : 80

バーチャルホスト名 ⑥

セッション維持 ⑦ OFF

有効 * ⑧ 有効 無効

アクセス制限 * ⑨ 無効

⑩ キャンセル ⑪ 入力内容確認

図5-19-1 仮想サービス追加/編集 (プロトコルにTCPを選択時)

1. 仮想IP アドレス

仮想サービスの仮想IP アドレスを設定します。

2. ポート

仮想サービスのポートを設定します。

3. プロトコル

仮想サービスのプロトコルを設定します。

4. 分散方式

仮想サービスの分散方式を設定します。

- ラウンドロビン
 - 重み付けラウンドロビン
 - 最小コネクション
 - 重み付け最小コネクション
 - ソースハッシング
 - 最小応答時間
- のいずれかとなります。

5. 待機サーバ

待機サーバのIPアドレスおよびポートを設定します。

6. バーチャルホスト名

HTTP によるノードサーバ死活監視用のバーチャルホスト名を設定します。

7. セッション維持

セッション維持の有効/無効を設定します。有効の場合、セッション維持時間(300~9999秒)も設定します。

実際のセッション維持時間は設定値+最大1分となる事がございます。

8. 有効

仮想サービスの有効/無効を設定します。

9. アクセス制限

仮想サービスのアクセス制限を設定します。

- 無効
- ブラックリスト方式
- ホワイトリスト方式

10. 【キャンセル】

仮想サービスの編集を中止します。

11. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「追加/編集」をクリックするとWeb Beagle に設定を適用します。

L4ロードバランサ設定

仮想サービス追加/編集

仮想IPアドレス * ① 192.168.24.38

ポート * ② 80

プロトコル * ③ UDP

分散方式 * ④ ラウンドロビン

待機サーバ ⑤ : 80

監視ドメイン名(空欄時はpingによる監視) ⑥

セッション維持 ⑦ OFF

有効 * ⑧ 有効 無効

アクセス制限 * ⑨ 無効

⑩ キャンセル ⑪ 入力内容確認

図5-19-2 仮想サービス追加/編集 (プロトコルにUDPを選択時)

6. **監視ドメイン名(空欄時はpingによる監視)** DNSクエリによるノードサーバ死活監視用のドメイン名を設定します。
空欄時はpingによる監視を行います。

L4 負荷分散・ノードサーバ編集

Web Beagle のL4 負荷分散の仮想IPに紐づくノードサーバを表示・変更する場合に使用します。

L4 仮想サービス

L4ノードサーバ設定

L4仮想サービス

⑨ 編集

仮想IPアドレス * ① 192.168.24.211

ポート * ② 80/TCP

分散方式 * ③ ラウンドロビン

待機サーバ ④ 192.168.24.42:80

バーチャルホスト名 ⑤ virtual.example.com

セッション維持 ⑥ 300 秒

有効 ⑦ 無効

アクセス制限 ⑧ ブラックリスト方式

図5-20 L4 仮想サービス

1. 仮想IP アドレス

仮想サービスの仮想IP アドレスを表示します。

2. ポート

仮想サービスのポートとプロトコルを表示します。

3. 分散方式

仮想サービスの分散方式を表示します。

- ラウンドロビン
 - 重み付けラウンドロビン
 - 最小コネクション
 - 重み付け最小コネクション
 - ソースハッシング
 - 最速応答時間
- のいずれかとなります。

4. バーチャルホスト名

HTTP によるノードサーバ死活監視用のバーチャルホスト名を表示します。

5. 待機サーバ

待機サーバのIPアドレスおよびポートを表示します。

6. セッション維持

セッション維持の有効/無効を表示します。有効の場合、セッション維持時間を表示します。

7. 有効

仮想サービスの有効/無効を表示します。

8. アクセス制限

仮想サービスのアクセス制限状態を表示します。

- 無効
- ブラックリスト方式
- ホワイトリスト方式

9. 【編集】

仮想サービスの編集画面に移ります。

L4 ノードサーバー一覧


③	10	件表示	④	検索:	①	②							
⑤	⑥	ノードサーバ	⑦	死活監視	⑧	有効	⑨	アクティブ接続数	⑩	非アクティブ接続数	⑪	⑫	⑬
⑤	⑥	192.168.24.190:80	⑦	TCP	⑧	YES	⑨	0	⑩	0	編集	無効	削除
		192.168.24.191:80		TCP		YES		0		0	⑪	⑫	⑬
		192.168.24.192:80		TCP		YES		0		0	編集	無効	削除
		192.168.24.193:80		TCP		YES		0		0	編集	無効	削除

4 件中 1 から 4 まで表示 ⑭

⑮ 先頭 ⑯ 前 1 次 ⑰ 最終

図5-21 L4 ノードサーバー一覧

1. **【リフレッシュ】**
ノードサーバの状態の表示を更新します。
2. **【追加】**
ノードサーバを追加します。
3. **表示件数**
一覧に表示するデータの数を指定します。
4. **検索条件**
一覧に表示するデータの検索条件を指定します。
5. **状態**
ノードサーバの状態を表示します。L4ロードバランサ設定にて変更を行った場合、この状態が現状の状態に落ち着くまでには数秒掛かります。60秒のリフレッシュを待つかリフレッシュボタンにて状態を更新してください。
6. **ノードサーバ**
ノードサーバのIP アドレスとポートを表示します。
7. **死活監視**
ノードサーバの死活監視プロトコルを表示します。
8. **有効**
ノードサーバが有効ならばYES、無効ならばNO
9. **アクティブ接続数**
ノードサーバに実際に接続している数を表示します。
10. **非アクティブ接続数**
ノードサーバの通信完了を待っている接続数を表示します。
11. **【編集】**
ノードサーバを編集します。
12. **【無効】・【有効】**
有効なノードを無効にします。
無効なノードは有効にします。
13. **【削除】**
ノードサーバを削除します。
14. **【件数】**
一覧に表示中の件数の範囲を表示します。
15. **【先頭】**
一覧の先頭のページを表示します。
16. **【前】**
前のページを表示します。
17. **【ページ番号】**
選択したページを表示します。
18. **【次】**
次のページを表示します。
19. **【最終】**
最終ページを表示します。

 本画面では、ノードの状態を更新するために60秒に1回画面をリフレッシュします。

ノードサーバ設定

ノードサーバ追加/編集

IPアドレス * ① 192.168.24.190

ポート * ② 80

重み付け * ③ 10

有効 ④

死活監視 * ⑤ HTTP

接続タイムアウト * ⑥ 5 秒

死活監視用URI ⑦ http://virtual.example.com/

⑩ キャンセル ⑪ 入力内容確認

図5-22 ノードサーバ追加/編集

1. IP アドレス

ノードサーバのIP アドレスを表示します。

2. ポート

ノードサーバのポートを表示します。

3. 重み付け

分散方式が重み付けラウンドロビンと重み付け最小コネクションの場合の重み付けを設定します。

4. 有効

ノードサーバの有効/無効を設定します。

5. 死活監視

ノードサーバの死活監視プロトコルを設定します (UDPの負荷分散時は選択できません)。

6. 接続タイムアウト

ノードサーバの死活監視タイムアウトを設定します。単位は秒です。

7. 死活監視用URI

HTTP またはHTTPS によるノードサーバ死活監視用のURI を設定します (UDPの負荷分散時は選択できません)。

8. DBユーザ名

MySQL によるノードサーバ死活監視用のDBユーザ名 を設定します。

9. パスワード

MySQL によるノードサーバ死活監視用のパスワード を設定します。

10. 【キャンセル】

ノードサーバの編集を中止します。

11. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「追加/編集」をクリックするとWeb Beagle に設定を適用します。

- ✎ ③の項目は分散方式が重み付けラウンドロビンか重み付け最小コネクションの場合のみ表示されます。
- ✎ ⑦の項目は死活監視がHTTP かHTTPS の場合のみ表示されます。
- ✎ ⑧、⑨の項目は死活監視がMySQL の場合のみ表示されます。

IPフィルタ設定 - 192.168.24.211:80/TCP

フィルタリング

仮想IPアドレス ① 192.168.24.211:80/TCP

フィルタリング* ② ブラックリスト方式

IPフィルター一覧

③ クリア

IPアドレス* ④ 54.223.46.128

ネットマスク* ⑤ 255.255.255.255

⑥ 追加 / 編集

IPアドレス	ネットマスク	
54.223.46.122	255.255.255.255	編集 削除

⑦ ⑧

入力内容確認 ⑨

図5-23 L4 IPフィルタ設定

1. 仮想IPアドレス

IPフィルタを設定する仮想IPアドレスを表示します。

2. フィルタリング

フィルタリングの種類を無効、ブラックリスト方式、ホワイトリスト方式、の中から選択します。

3. 【クリア】

フィルタリング一覧のデータをクリアします。

4. IPアドレス

フィルタリング対象とされたIPアドレスです。

5. ネットマスク

フィルタリング対象とされたネットマスクです。

6. 【追加 / 編集】

入力したIPアドレスとネットマスクを一覧に追加します。

7. 【編集】

選択したデータを編集します。

8. 【削除】

選択したデータを削除します。

9. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「追加/編集」をクリックするとWeb Beagle に設定を適用します。

✎ ④、⑤の項目はフィルタリングがブラックリスト方式かホワイトリスト方式の場合のみ表示されます。

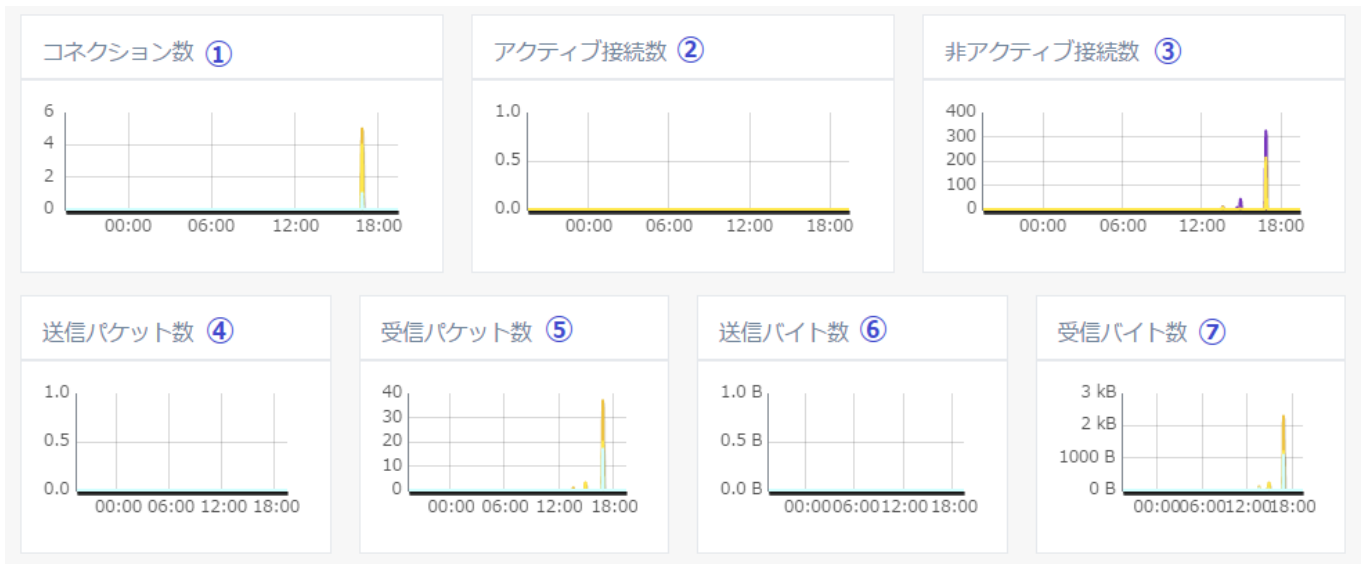


図5-24 L4 仮想サービス状態グラフ

1. コネクション数グラフ

仮想サービスの直近24時間のコネクション数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

2. アクティブ接続数グラフ

仮想サービスの直近24時間のアクティブ接続数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

3. 非アクティブ接続数グラフ

仮想サービスの直近24時間の非アクティブ接続数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

4. 送信パケット数

仮想サービスの直近24時間の送信パケット数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

5. 受信パケット数

仮想サービスの直近24時間の受信パケット数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

6. 送信バイト数

仮想サービスの直近24時間の送信バイト数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

7. 受信バイト数

仮想サービスの直近24時間の受信バイト数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

✎ 拡大されたグラフでは、日付を指定して検索することが可能です。

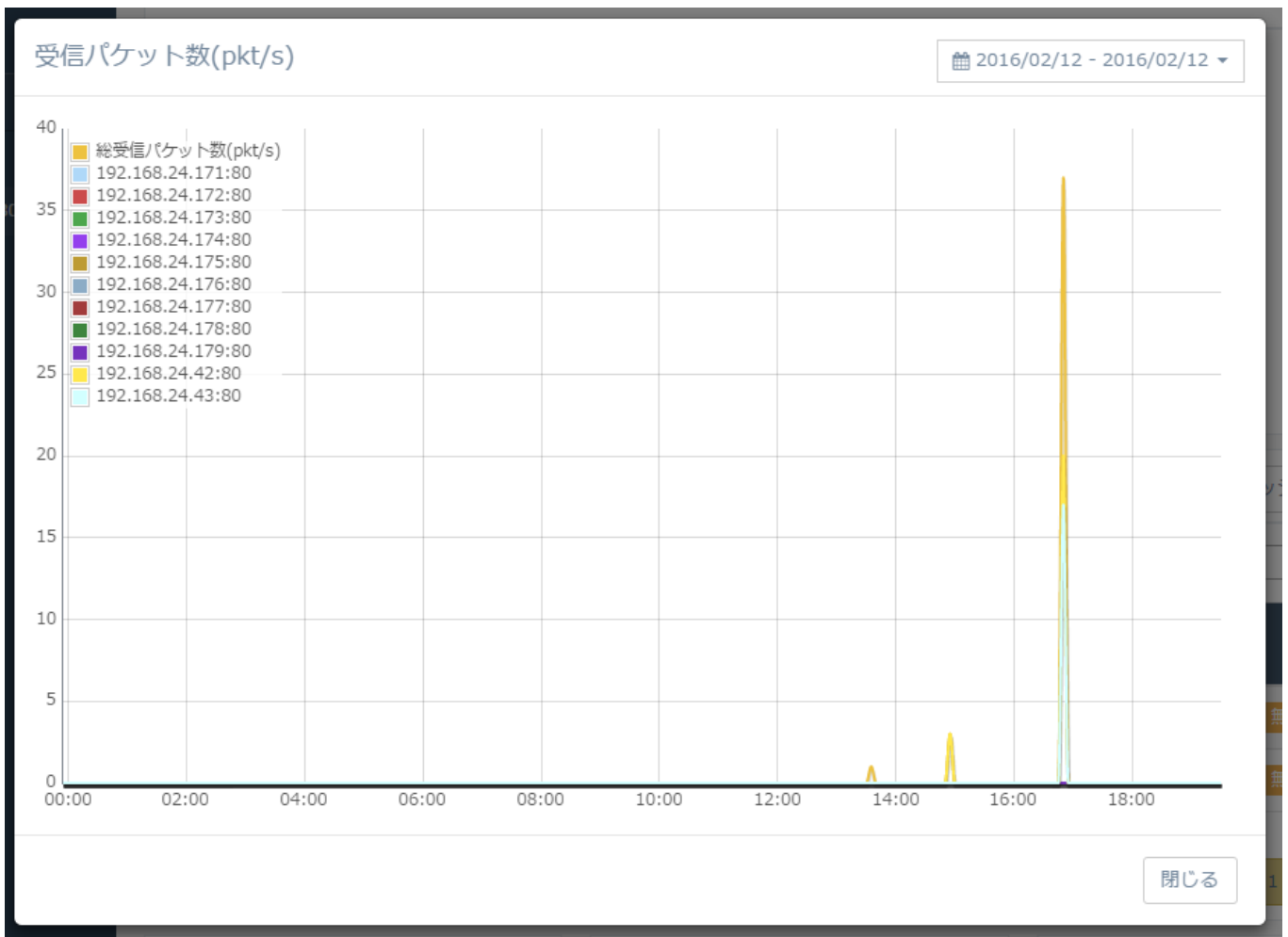


図5-25 拡大されたグラフ

- ❗ 同一の値の場合、後に描画される線が上に重なって表示されます。
- ✂ 拡大グラフを表示中の際は画面の定期的なリフレッシュは一時停止します。

5. L7 負荷分散

L7 仮想サービス

Web Beagle のL7 仮想サービスを表示・変更する場合に使用します。

L7 仮想サービス一覧

L7 仮想サービスの一覧を表示します。

L7ロードバランサ設定



状態	仮想IPアドレス	分散方式	有効	稼働中 / 全ノードサーバ数	
緑	192.168.24.199:80	ラウンドロビン	YES	3/3	フィルタ 編集 無効 削除
灰	192.168.24.211:80	URIハッシング	NO	0/0	フィルタ 編集 有効 削除
黄	192.168.24.212:80	ソースハッシング	YES	1/2	フィルタ 編集 無効 削除
赤	192.168.24.213:80	重み付けラウンドロビン	YES	0/1	フィルタ 編集 無効 削除

図5-26 L7 仮想サービス一覧

1. 【リフレッシュ】

仮想サービスの状態の表示を更新します。

2. 【追加】

仮想サービスを追加します。

3. 表示件数

一覧に表示するデータの数を指定します。

4. 検索条件

一覧に表示するデータの検索条件を指定します。

5. 状態

仮想サービスの状態を表示します。

- 緑：全てのノードサーバが稼働中です。
- 黄：いくつかのノードサーバがダウンしています。
- 赤：全てのノードサーバがダウンしています。
- 灰：仮想サービスが無効です。
のいずれかの色で表されます。

6. 仮想IP アドレス

仮想サービスの仮想IP アドレスを表示します。

7. 分散方式

仮想サービスの分散方式を表示します。

- ラウンドロビン
- 重み付けラウンドロビン
- 最大接続数以下同一サーバー
- ソースハッシング
- URI ハッシング
のいずれかとなります。

8. 有効

仮想サービスが有効ならばYES、無効ならばNO

9. 稼働中/ 全ノードサーバ数

全ノードサーバ中、稼働中のサーバ数を表示します。

10. 【フィルタ】

仮想サービスのIPフィルタ設定画面を表示します。

11. 【編集】

仮想サービスの編集画面を表示します。

12. 【無効】・【有効】

有効な仮想サービスを無効にします。
無効な仮想サービスは有効にします。

13. 【削除】

仮想サービスを削除します。

14. 【件数】

一覧に表示中の件数の範囲を表示します。

15. 【先頭】

一覧の先頭のページを表示します。

16. 【前】

前のページを表示します。

17. 【ページ番号】

選択したページを表示します。

18. 【次】

次のページを表示します。

19. 【最終】

最終ページを表示します。

✂ 本画面では、仮想サービスの状態を更新するために60秒に1回画面をリフレッシュします。

L7 仮想サービス追加／編集

L7ロードバランサ設定

L7仮想サービス追加/編集

仮想IPアドレス * ① 192.168.24.38

ポート * ② 80

動作方式 * ③ HTTPS 証明書あり ▼ SSL オフロード設定

分散方式 * ④ ラウンドロビン ▼

待機サーバ ⑤ 192.168.24.100 : 80

バーチャルホスト名 ⑥ virtual.example.com

セッション維持方式 * ⑦ セッションを維持しない ▼

有効 * ⑧ 有効 無効

死活監視 * ⑨ HTTP

死活監視用URI ⑩ http://virtual.example.com/

アクセス制限 * ⑪ ブラックリスト方式 ▼

⑫ キャンセル ⑬ 入力内容確認

図5-27 L7 仮想サービス追加／編集

1. 仮想IP アドレス

仮想サービスの仮想IP アドレスを設定します。

2. ポート

仮想サービスのポートを設定します。

3. 動作方式

仮想サービスの動作方式を設定します。

- HTTP
- HTTPS 証明書あり
- HTTPS 証明書なし

のいずれかとなります。

✎ HTTPS 証明書ありを選択した場合、SSL オフロードの設定をしなければなりません。
「SSL オフロード設定」ボタンより設定をしてください。

4. 分散方式

仮想サービスの分散方式を設定します。

- ラウンドロビン
- 重み付けラウンドロビン
- 最大接続数以下同一サーバー
- ソースハッシング
- URI ハッシング

のいずれかとなります。

✎ URI ハッシングは動作方式がHTTP かHTTPS 証明書ありの場合表示されます。

5. 待機サーバ

待機サーバのIPアドレスおよびポートを設定します。

6. バーチャルホスト名

HTTP によるノードサーバ死活監視用のバーチャルホスト名を設定します。

7. セッション維持

セッションの維持方式を設定します。

- セッションを維持しない
- 接続元IP アドレス

✎ 接続元IP アドレスを選択した場合、セッション維持タイムアウトも設定します。

- cookie

✎ cookie を選択した場合、cookie 名も設定します。

cookie は動作方式にHTTP、またはHTTPS 証明書ありを選択した場合表示されます。

- SSL セッションID

✎ SSL セッションID は動作方式にHTTPS 証明書なしを選択した場合表示されます。

8. 有効

仮想サービスの有効/無効を設定します。

9. 死活監視

ノードサーバの死活監視プロトコルを設定します。

10. 死活監視用URI

HTTP またはHTTPS によるノードサーバ死活監視用のURI を設定します。

11. アクセス制限

仮想サービスのアクセス制限を設定します。

- 無効
- ブラックリスト方式
- ホワイトリスト方式

12. 【キャンセル】

仮想サービスの編集を中止します。

13. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「追加/編集」をクリックするとWeb Beagle に設定を適用します。

✎ ⑩の項目は死活監視がHTTP かHTTPS の場合のみ表示されます。

SSL オフロード設定

SSL 証明書

サーバ証明書 * ①

秘密鍵 * ②

中間証明書 ③

パスフレーズ ④

⑤ キャンセル ⑥ 仮想サービスの設定を続ける

図5-28 SSL オフロード設定

1. サーバ証明書

SSL オフロードで使用するサーバ証明書を設定します。

2. 秘密鍵

SSL オフロードで使用する秘密鍵を設定します。

3. 中間証明書

SSL オフロードで使用する中間証明書を設定します。

4. パスフレーズ

SSL オフロードで使用する秘密鍵のパスフレーズを設定します。

5. 【キャンセル】

SSL オフロード設定の編集を中止します。

6. 【仮想サービスの設定を続ける】

入力した内容に決定し、L7仮想サービスの追加/編集画面に移ります。

値はL7仮想サービス追加/編集の確認画面で「追加/編集」をクリックすることで反映されます。

L7 負荷分散・ノードサーバ編集

Web Beagle のL7 負荷分散の仮想IPに紐づくノードサーバを表示・変更する場合に使用します。

L7 仮想サービス

L7ノードサーバ設定

L7仮想サービス ⑫ 編集

仮想IPアドレス * ① 192.168.24.213

ポート * ② 80

動作方式 * ③ HTTP

分散方式 * ④ ラウンドロビン

待機サーバ ⑤ 192.168.24.100:80

バーチャルホスト名 ⑥ virtual.example.com

セッション維持方式 ⑦ セッションを維持しない

有効 * ⑧ 有効

死活監視 * ⑨ HTTP

死活監視用URI * ⑩ http://virtual.example.com/

アクセス制限 * ⑪ ブラックリスト方式

図5-29 L7 仮想サービス

1. 仮想IP アドレス

仮想サービスの仮想IP アドレスを表示します。

2. ポート

仮想サービスのポートを表示します。

3. 動作方式

仮想サービスの動作方式を表示します。

- HTTP
- HTTPS 証明書あり
- HTTPS 証明書なし

のいずれかとなります。

4. 分散方式

仮想サービスの分散方式を表示します。

- ラウンドロビン
- 重み付けラウンドロビン
- 最大接続数以下同一サーバー
- ソースハッシング
- URI ハッシング

のいずれかとなります。

5. 待機サーバ

待機サーバのIPアドレスおよびポートを表示します。

6. バーチャルホスト名

HTTP によるノードサーバ死活監視用のバーチャルホスト名を表示します。

7. セッション維持

セッションの維持方式を表示します。

接続元IP アドレスの場合、セッション維持タイムアウトも表示します。

cookie の場合、cookie 名も表示します。

8. 有効

仮想サービスの有効/無効を表示します。

9. 死活監視

ノードサーバの死活監視プロトコルを表示します。

10. 死活監視用URI

HTTP またはHTTPS によるノードサーバ死活監視用のURI を表示します。

11. アクセス制限

仮想サービスのアクセス制限状態を表示します。

- 無効
- ブラックリスト方式
- ホワイトリスト方式

12. 【編集】

仮想サービスの編集画面に移ります。

L7 ノードサーバー一覧

ノードサーバ	有効	アクティブ接続数	非アクティブ接続数	
192.168.24.190:80	YES	0	0	編集 無効 削除
192.168.24.191:80	YES	0	0	編集 無効 削除
192.168.24.192:80	YES	0	0	編集 無効 削除
192.168.24.193:80	YES	0	0	編集 無効 削除

図5-30 L7 ノードサーバー一覧

1. 【リフレッシュ】

ノードサーバの状態の表示を更新します。

2. 【追加】

ノードサーバを追加します。

3. 表示件数

一覧に表示するデータの数指定します。

4. 検索条件

一覧に表示するデータの検索条件を指定します。

5. 状態

ノードサーバの状態を表示します。L7ロードバランサ設定にて変更を行った場合、この状態が現状の状態に落ち着くまでには数秒掛かります。60秒のリフレッシュを待つかリフレッシュボタンにて状態を更新してください。

6. ノードサーバ

ノードサーバのIPアドレスとポートを表示します。

7. 有効

ノードサーバが有効ならばYES、無効ならばNO

8. アクティブ接続数

ノードサーバに実際に接続している数を表示します。

9. 非アクティブ接続数

ノードサーバの通信完了を待っている接続数を表示します。

10. 【編集】

ノードサーバを編集します。

11. **【無効】・【有効】**
有効なノードを無効にします。
無効なノードは有効にします。
12. **【削除】**
ノードサーバを削除します。
13. **【件数】**
一覧に表示中の件数の範囲を表示します。
14. **【先頭】**
一覧の先頭のページを表示します。
15. **【前】**
前のページを表示します。
16. **【ページ番号】**
選択したページを表示します。
17. **【次】**
次のページを表示します。
18. **【最終】**
最終ページを表示します。

✂ 本画面では、ノードの状態を更新するために60秒に1回画面をリフレッシュします。

ノードサーバ追加／編集

L7ノードサーバ一覧

L7ノードサーバ追加/編集

IPアドレス * ① 192.168.24.190

ポート * ② 80

重み付け * ③ 10

有効④

接続タイムアウト⑤ 5 秒

⑥ キャンセル ⑦ 入力内容確認

図5-31 L7 ノードサーバ追加／編集

1. IP アドレス

ノードサーバのIP アドレスを表示します。

2. ポート

ノードサーバのポートを表示します。

3. 重み付け

分散方式が重み付けラウンドロビンの場合の重み付けを設定します。

4. 有効

ノードサーバの有効／無効を設定します。

5. 接続タイムアウト

ノードサーバの死活監視タイムアウトを設定します。単位は秒です。

6. 最大同時接続数

ノードサーバの最大で同時接続できる数を設定します。0を設定時は同時接続数は無制限となります。

7. 【キャンセル】

ノードサーバの編集を中止します。

8. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「追加/編集」をクリックするとWeb Beagle に設定を適用します。

✎ ③の項目は分散方式が重み付けラウンドロビンの場合のみ表示されます。

L7 IPフィルタ設定

IPフィルタ設定 - 192.168.24.211:80/TCP

フィルタリング

仮想IPアドレス ① 192.168.24.211:80/TCP

フィルタリング * ② ブラックリスト方式

IPフィルター一覧

③ クリア

IPアドレス * ④ 54.223.46.128

ネットマスク * ⑤ 255.255.255.255

⑥ 追加 / 編集

IPアドレス	ネットマスク	
54.223.46.122	255.255.255.255	編集 削除

⑦ ⑧

入力内容確認 ⑨

図5-32 L7 IPフィルタ設定

1. 仮想IPアドレス

IPフィルタを設定する仮想IPアドレスを表示します。

2. フィルタリング

フィルタリングの種類を無効、ブラックリスト方式、ホワイトリスト方式、の中から選択します。

3. 【クリア】

フィルタリング一覧のデータをクリアします。

4. IPアドレス

フィルタリング対象とされたIPアドレスです。

5. ネットマスク

フィルタリング対象とされたネットマスクです。

6. 【追加 / 編集】

入力したIPアドレスとネットマスクを一覧に追加します。

7. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「追加/編集」をクリックするとWeb Beagle に設定を適用します。

✎ ④、⑤の項目はフィルタリングがブラックリスト方式かホワイトリスト方式の場合のみ表示されます。

L7 仮想サービス状態グラフ

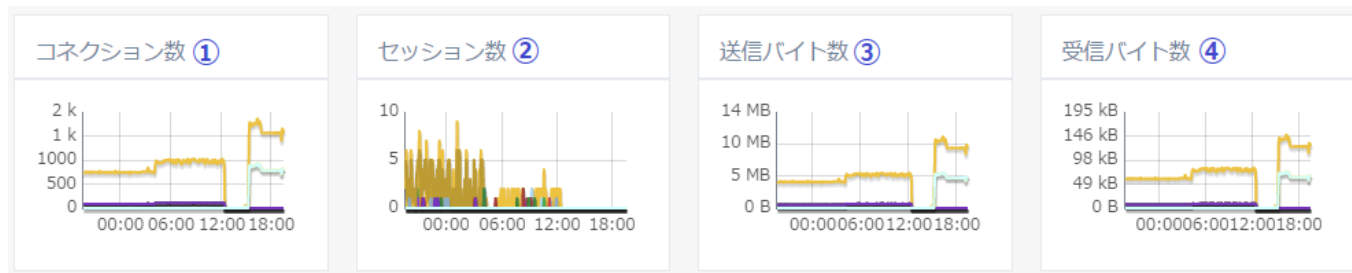


図5-33 L7 仮想サービス状態グラフ

1. コネクション数グラフ

仮想サービスの直近24時間のコネクション数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

2. セッション数グラフ

仮想サービスの直近24時間のセッション数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

3. 送信バイト数

仮想サービスの直近24時間の送信バイト数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

4. 受信バイト数

仮想サービスの直近24時間の受信バイト数グラフを表示します。
クリックすると拡大されたグラフが表示されます。

✂ 拡大されたグラフでは、日付を指定して検索することが可能です。

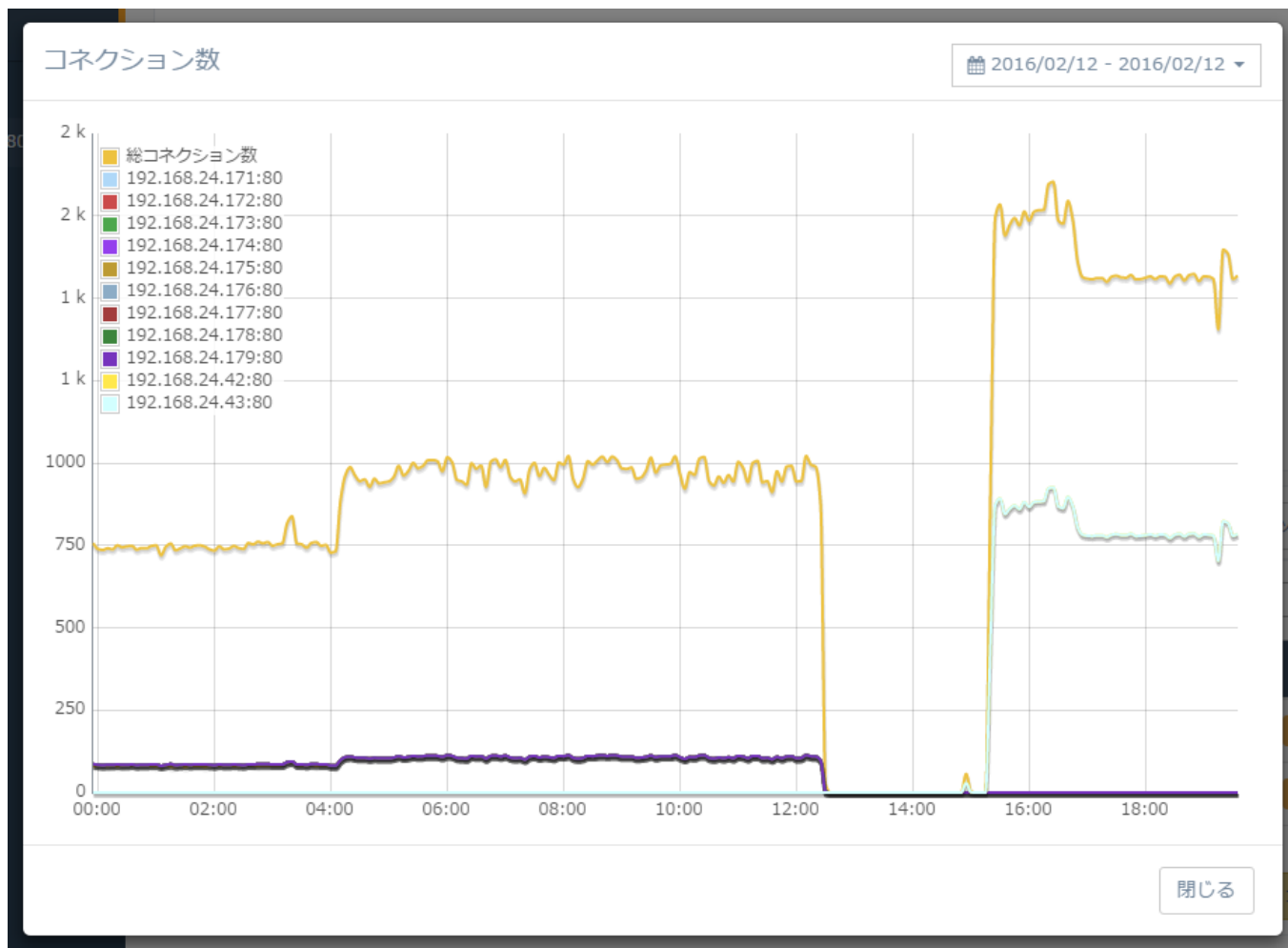


図5-34 拡大されたグラフ

- ① 同一の値の場合、後に描画される線が上に重なって表示されます。
- ✎ 拡大グラフを表示中は画面の定期的なリフレッシュは一時停止します。

6. 通知設定

Syslog

Web Beagle のログをSyslog に転送する設定を表示・変更する場合に使用します。

Syslog 設定

図5-35 Syslog 設定

1. ログを外部Syslog サーバに転送

Web BeagleのログをSyslog サーバに転送するには、このチェックボックスにチェックを入れます。

2. Syslog サーバIP アドレス

Web Beagleのログの転送先Syslog サーバのIP アドレスを設定します。

3. ファシリティ

Web Beagleのログのファシリティを設定します。

4. カーネルログ転送

Web BeagleのカーネルログをSyslogサーバに転送するには、このチェックボックスにチェックを入れます。

5. 【キャンセル】

Syslog 設定の編集を中止します。

6. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「更新」をクリックするとWeb Beagle に設定を適用します。

SNMP

Web Beagle のSNMP 設定を表示・変更する場合に使用します。

SNMP

SNMP設定編集

SNMP

SNMP機能 有効

コミュニティ名 * public

SNMP接続許可IPアドレス

IPアドレス * 192.168.23.0

ネットマスク * 255.255.255.0

追加/編集

IPアドレス	ネットマスク	
192.168.23.0	255.255.255.0	編集 削除

キャンセル 入力内容確認

図5-36 SNMP

1. SNMP 機能

Web BeagleのログをSNMP サーバに転送するには、このチェックボックスにチェックを入れます。

2. コミュニティ名

SNMP のコミュニティ名を設定します。

3. IP アドレス

SNMP に接続を許可するIP アドレスを設定します。

4. ネットマスク

SNMP に接続を許可するネットマスクを設定します。

5. 【追加/編集】

入力したSNMP接続を許可するIP アドレスを一覧に追加します。

6. 【編集】

選択したSNMP接続許可IP アドレスを編集します。

クリックすると入力エリアに値が表示されますので値を編集後、追加/編集ボタンを押してください。

7. 【削除】

SNMP接続許可IP アドレスを一覧から削除します。

8. 【キャンセル】

SNMP の編集を中止します。

9. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「更新」をクリックするとWeb Beagle に設定を適用します。

① 設定はただちに反映されます。

メール通知設定

Web Beagle の状態をメールで通知する設定を表示・変更する場合に使用します。

メール通知設定

メール通知設定編集

メール通知設定

メール通知 ***①** 有効

SMTPサーバIPアドレス * **②** 192.168.24.10

差出人アドレス * **③** webbeagle@example.co.jp

宛先アドレス * **④** admin@example.co.jp

⑤ キャンセル **⑥** 入力内容確認

図5-37 メール通知設定

1. メール通知

メールによる状態の通知を行うには、このチェックボックスにチェックを入れます。

2. SMTP サーバIP アドレス

メールの送信に用いるSMTP サーバのIP アドレスを設定します。

3. 差出人アドレス

通知メールの差出人メールアドレスを設定します。

4. 宛先アドレス

通知メールの宛先メールアドレスを設定します。

5. 【キャンセル】

メール通知設定 の編集を中止します。

6. 【入力内容確認】

入力内容確認画面に移ります。確認画面で「更新」をクリックするとWeb Beagle に設定を適用します。

7. 運用管理

ログ

Web Beagle のログを管理画面から確認する場合に使用します。

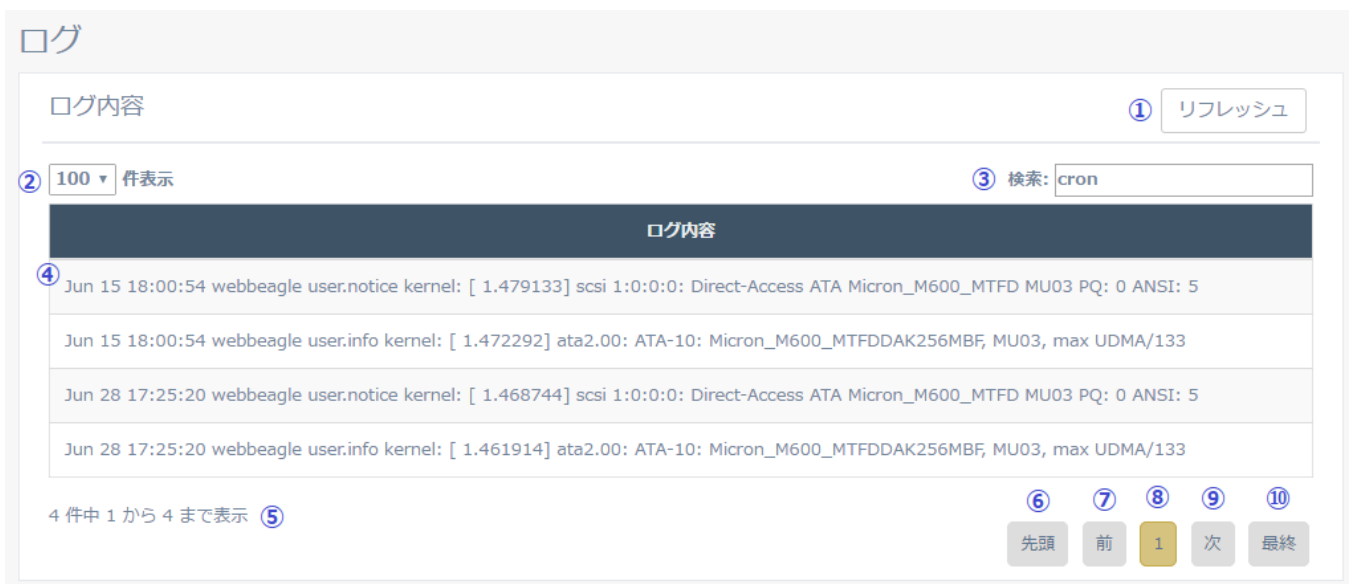


図5-38 ログ

1. **【リフレッシュ】**
ログの表示を更新します。
2. **表示件数**
一覧に表示するデータの数を指定します。
3. **検索**
ログ一覧の検索条件を入力します。
4. **ログ内容**
ログを一覧で表示します。
5. **【件数】**
一覧に表示中の件数の範囲を表示します。
6. **【先頭】**
一覧の先頭のページを表示します。
7. **【前】**
前のページを表示します。
8. **【ページ番号】**
選択したページを表示します。
9. **【次】**
次のページを表示します。
10. **【最終】**
最終ページを表示します。

バックアップ／リストア

Web Beagle の設定のバックアップとリストアを行う場合に使用します。

設定情報のバックアップ

Web Beagleの設定情報をバックアップします。

「**バックアップ**」 ボタンをクリックすると、Web Beagleの設定情報がダウンロードできます。

旧モデルからの設定情報のリストア



図5-39 設定情報のバックアップ

1. 【バックアップ】

Web Beagle の設定情報をバックアップします。

❗ ご利用のブラウザによってはポップアップがブロックされバックアップファイルをダウンロードできない場合があります。

そのような場合はお手数ですが、ポップアップのブロックを解除して再度実行してください。

設定情報のリストア

バックアップしたWeb Beagle の設定情報をリストアします。

Web Beagle の設定情報のバックアップファイルをアップロードコンテナにドラッグするか、コンテナをクリックしてバックアップファイルを指定します。

「リストア」 ボタンをクリックすると、指定したバックアップファイルを用いて、 Web Beagle の設定情報がリストアできます。

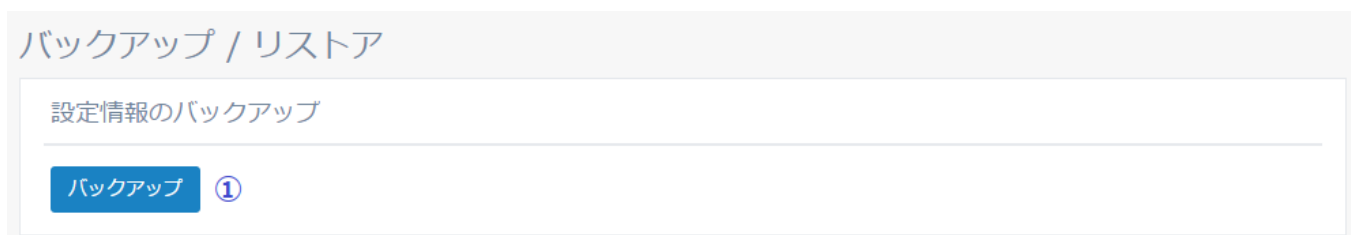


図5-40 設定情報のリストア

1. 【アップロードコンテナ】

Web Beagle の設定情報のバックアップファイルを指定します。

2. 【リストア】

Web Beagle の設定情報のリストアします。

旧モデルからの設定情報のリストア

旧モデルのバックアップファイルからWeb Beagle の設定情報をリストアします。

【バックアップ/リストア】ページの【旧モデルからの設定情報のリストア】の【リストア画面へ移動】を選択します。



図5-41 旧モデルからの設定情報のリストアへの移動

旧モデルからの設定情報のリストア画面が表示されますので、旧モデルのWeb Beagle の設定情報のバックアップファイルをアップロードコンテナにドラッグするか、コンテナをクリックしてバックアップファイルを指定します。

「リストア」ボタンをクリックすると、指定したバックアップファイルを用いて、Web Beagle の設定情報がリストアできます。

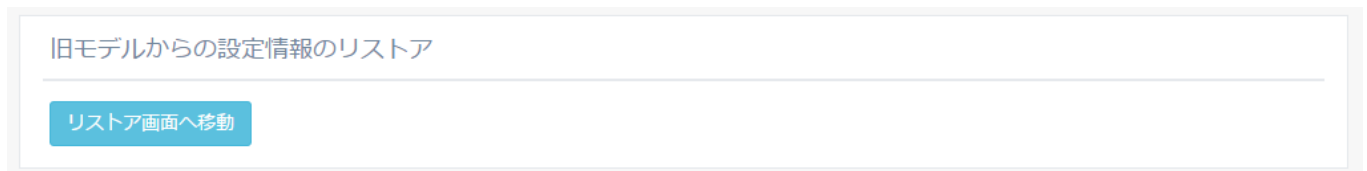


図5-42 旧モデルからの設定情報のリストア

1. 【アップロードコンテナ】

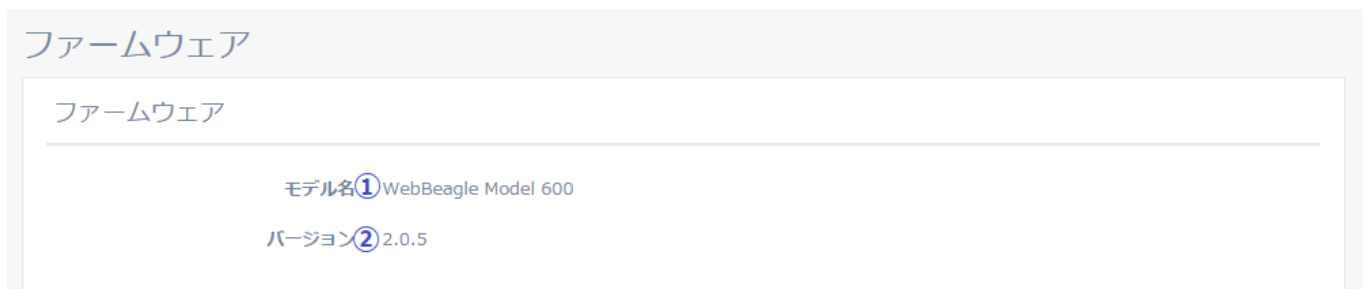
旧モデルのWeb Beagle の設定情報のバックアップファイルを指定します。

2. 【リストア】

旧モデルのWeb Beagle の設定情報のリストアします。

ファームウェア

Web Beagle のファームウェア情報の表示・アップデートを行う場合に使用します。



第6章 コンソール管理

1. コンソール管理

Web Beagle のコンソール管理画面をお使いいただくための手順を説明します。

Web Beagle にモニタ、キーボードを接続してください。

Web Beagle のフロントパネルについては「1章 - ハードウェアの取り扱いについて (./chapter_1.html#ハードウェアの取り扱いについて)」を参照してください。

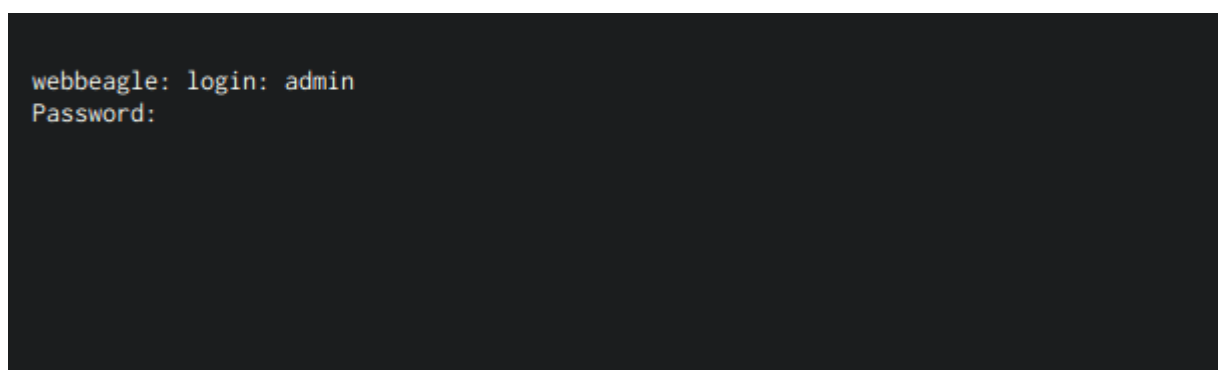


図6-1 ログイン画面

Web Beagle のコンセントを電源に接続し、電源スイッチを押下します。

モニタにログインプロンプトが表示されますのでログインID とパスワードを入力します。

このログインID およびパスワードは、装置に添付されているシートのコンソールログインID、パスワードを入力してください。

! このログインID とパスワードはWeb Beagle の管理画面へのログインID、パスワードとは異なります。変更することはできません。

ログインすると、コンソール管理メニューが表示されます。

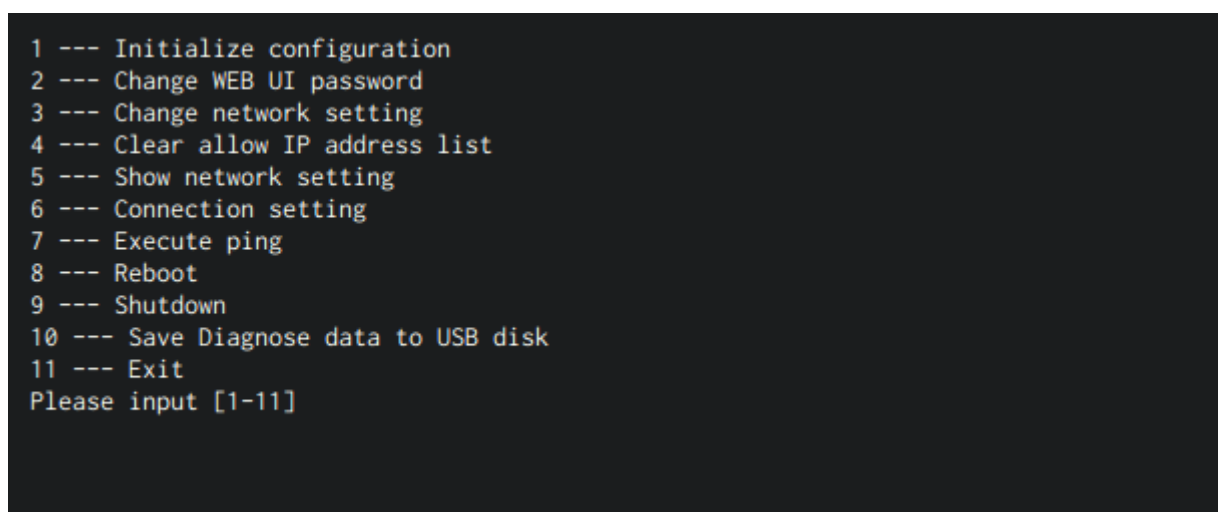


図6-2 コンソール管理メニュー

工場出荷時設定に戻したい場合

Web Beagle の設定を工場出荷時に戻す場合、管理メニューにて 1 を入力します。
設定を初期化するか確認を求められますので、よろしければ y を入力してください。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 1

Do you want to initialize the configuration?[y/n]:y
Configuration initialized
```

図6-3 設定の初期化

管理者パスワードを忘れた場合

Web インターフェイスの管理者パスワードを忘れた場合、管理メニューにて 2 を入力します。
新しいパスワードの入力を求められますので、パスワードの再設定を行います。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 2

Input new password: newpassword
```

図6-4 パスワードの再設定

ネットワーク設定を変更したい場合

Web Beagle のネットワーク設定を変更する場合、管理メニューにて 3 を入力します。
新しいIP アドレス、ネットマスク、ゲートウェイを入力し、再設定を行ってください。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 3

Input new IP address: 10.1.1.2
Input new Netmask: 255.255.255.0
Input new Gateway: 10.1.1.1
```

図6-5 ネットワーク設定の変更

管理画面へのアクセス制限をクリアしたい場合

Web Beagle のWeb インターフェイスへのアクセス制限をクリアする場合、管理メニューにて 4 を入力します。

アクセス制限をクリアするか確認を求められますので、よろしければ y を入力してください。

ただちにアクセス制限は解除されますので、Web インターフェイスにて再度アクセス制限を行ってください。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 4

Do you want to clear allowd IP?[y/n]: y

Allowed IP cleared.
```

図6-6 アクセス制限のクリア

ネットワーク設定を確認したい場合

ネットワーク設定を確認したい場合、管理メニューにて 5 を入力します。

現在のネットワーク状態とネットワーク設定が表示されます。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 5

Current Setting:
IP Address:      10.1.1.2
Net Mask:       255.255.255.0
Default Gateway: 10.1.1.1
```

図6-7 ネットワーク設定確認

接続設定を変更したい場合

Web Beagle の接続設定を変更したい場合、管理メニューにて6を入力します。

現在の設定が表示され、変更したい設定を入力を求められます。

BONDING 設定を変更する場合は1を、TSO 設定を変更する場合は2を、NIC 設定(ネットワークポート設定)を変更する場合は3を、管理メニューに戻る場合は4を入力します。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 6

BONDING: off

TSO: off
eth0: auto
eth1: auto

1 --- Change BONDING setting
2 --- Change TSO setting
3 --- Change NIC setting
4 --- Return
Please input [1-4]:
```

図6-8 接続設定の変更

1. BONDING 設定

BONDING の設定値を以下から選択することができます。

- o 0 --- off
- o 1 --- balance-rr
- o 2 --- active-backup
- o 3 --- balance-xor
- o 4 --- broadcast
- o 5 --- 802.3ad
- o 6 --- balance-tlb
- o 7 --- balance-alb

```
1 --- Change BONDING setting
2 --- Change TSO setting
3 --- Change NIC setting
4 --- Return
Please input [1-4]: 1

0 --- off
1 --- balance-rr
2 --- active-backup
3 --- balance-xor
4 --- broadcast
5 --- 802.3ad
6 --- balance-tlb
7 --- balance-alb
Please input [0-7]:
```

図6-9 BONDING 設定

2. TSO 設定

TSO の「on」「off」を入力することができます。

```
1 --- Change BONDING setting
2 --- Change TSO setting
3 --- Change NIC setting
4 --- Return
Please input [1-4]: 2

Change TSO setting
1 --- on
2 --- off[default]
Please input [1-2]:
```

図6-10 TSO 設定

3. NIC 設定

変更したいNIC(ネットワークポート)に該当する数字を入力します。
画面に表示されている設定の数字を入力して、設定を変更します。

```
1 --- Change BONDING setting
2 --- Change TSO setting
3 --- Change NIC setting
4 --- Return
Please input [1-4]: 3

Select NIC
1 --- eth0
2 --- eth1
Please input [1-2]: 1

Select Connection setting
1 --- auto[default]
2 --- 1000M full
3 --- 100M full
4 --- 10M full
5 --- 100M half
6 --- 10M half
Please input [1-6]:
```

図6-11 NIC 設定

ネットワークの疎通を確認したい場合

WebBeagle のネットワークの疎通を確認したい場合、管理メニューにて 7 を入力します。

対象のIP アドレスとの疎通結果が表示されます。

もし疎通結果が失敗していた場合（図6-9）、WebBeagle のネットワーク設定やネットワークの配線をみなおしてください。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 7

Input destination IP address:
PING 10.1.1.1 (10.1.1.1) 56(86) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=0.072 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=0.069 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=0.058 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=64 time=0.070 ms

--- 10.1.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.058/0.067/0.072/0.008 ms
```

図6-12 ネットワーク疎通確認(疎通成功)

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 7

Input destination IP address:
PING 10.1.1.1 (10.1.1.1) 56(86) bytes of data.

--- 10.1.1.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss
```

図6-13 ネットワーク疎通確認(疎通成功)

Web Beagle を再起動したい場合

Web Beagle を再起動する場合、管理メニューにて8を入力します。再起動するか確認を求められますので、よろしければ y を入力してください。ただちにWeb Beagle は再起動されます。

```
1 --- Initialize configuration
2 --- Change WEB UI password
3 --- Change network setting
4 --- Clear allow IP address list
5 --- Show network setting
6 --- Connection setting
7 --- Execute ping
8 --- Reboot
9 --- Shutdown
10 --- Save Diagnose data to USB disk
11 --- Exit
Please input [1-11] 8

Do you want to reboot the system?[y/n]:
```

図6-14 Web Beagle の再起動

Web Beagle をシャットダウンしたい場合

Web Beagle をシャットダウンする場合、管理メニューにて9を入力します。シャットダウンするか確認を求められますので、よろしければ y を入力してください。ただちにWeb Beagle はシャットダウンされます。

第7章 保証とアフターサービス

1. 初期不良交換期間

本製品の初期不良交換期間につきましては、発送日の翌日より30日間とさせていただきますので、期間内にご連絡いただいた上で、弊社宛にお送りください。定められた期間を過ぎての初期不良交換には一切応じられませんのでご了承ください。なお、お送りいただく際には、保証書及び製品（付属品、外箱）がすべてそろっている必要がございます。万が一、欠品若しくは外箱に著しい破損が見受けられる場合には交換いたしかねますのでご了承ください。

2. 初期不良交換

初期不良品としてお送りいただいた商品につきましては、弊社にて動作チェックを行った上で判断させていただきます。動作チェックには数日お時間をいただきますので、お送りいただきまして即日の交換は致しかねますのであらかじめご了承ください。交換は致しかねますのであらかじめご了承ください。但し、下記項目の条件に当てはまる場合には、初期不良交換の対象外とさせていただきます。

- 周辺機器の相互間の相性による動作不良
- 各機器のメーカーが責を追うべきハードウェア及びソフトウェアの不具合による動作不良
- 本製品環境条件以外での使用または警告、注意事項を無視した事による故障
- お客様の責による設定及び破壊による動作不良

3. 無償修理保証期間

製品メーカーの保証規定の無い場合、弊社発送日の翌日より一年間の無償修理を保証いたします。ただし、以下の場合には有償修理扱いとなりますので、あらかじめご了承ください。

- 保証書が無い場合
- 天災、公害、事故、火事等による故障及び損傷
- お買い上げ後の輸送中もしくは移動中にお取り扱いが不適切な為に生じた故障及び損傷
- 使用上不適切なお取り扱いをされた場合
- 本製品環境条件以外での使用または警告、注意事項を無視した事による故障
- 消耗品の交換を必要とする場合

4. 返品に関して

お買い上げいただきました商品に関しましては、以下の場合にご購入後7日間に限り、返品・交換に応じません。

- 不良品
- 商品説明との著しい機能相違
- 発送間違い

5. 追記事項

- 本製品の使用または使用不能によって生じたいかなる損害につきましても、弊社では一切の責任を負わないものとします。
- 修理をご依頼される場合には、必ず事前にご連絡いただいた上で、販売元もしくは弊社へご発送下さい。但し弊社へ修理をご依頼される場合の送料は、お客様負担となります。弊社からお客様あてに返送する場合の送料は弊社負担となりますので、あらかじめご了承ください。
- お買い上げいただきました商品を改造、または部品交換等をなされた場合には本保証の対象外とさせていただきます。
- 本保証は日本国内においてのみ有効です。
This warranty is valid only in Japan.

付録

付録A. 仕様

	Model 400	Model 500	Model 600
ネットワークインターフェース	1000BASE-T (2ポート) ※1		1000BASE-T (4ポート) ※2
ネットワークポートのボンディング	×		○
機能	レイヤー4 ロードバランシング レイヤー7 ロードバランシング		
プロトコル	レイヤー4 TCP, UDP レイヤー7 TCP		
L4 対応負荷分散方式	ラウンドロビン		
	最小コネクション		
	重み付けラウンドロビン		
	重み付け最小コネクション		
	ソースハッシング		
	最速応答時間		
L7 対応負荷分散方式	ラウンドロビン		
	重み付けラウンドロビン		
	最大接続数以下同一サーバー		
	ソースハッシング		
	URIハッシング ※3		
セッション維持	(L4) セッション維持タイムアウト値による維持		
	(L7) 接続元IP アドレスによる維持		
	(L7) cookie による維持 ※3		
	(L7) SSL セッションID による維持 ※4		

	Model 400	Model 500	Model 600
死活監視方式	TCP / HTTP / HTTPS / MySQL, ping / DNS ※5		
仮想サービス数	8 (最大) ※6	16 (最大) ※6	32 (最大) ※6
ノード数	32 ※7	256 ※7	256 ※7
対応ネットワーク構成	DSR 型	DSR 型 / NAT 型 / 透過型	DSR 型 / NAT 型 / 透過型
冗長化構成	アクティブ / スタンバイの冗長化構成が可能(同一機種を2台用意)		
使用電力	AC100V ± 10V (50 / 60Hz)		
平均電力消費量	単体: 35W 冗長構成時: 70W(2台の合計消費電力)		
寸法	単体: 42.2(H) × 217(W) × 365(D)mm 冗長構成時 43.8 (H) × 447.8 (W) × 371.6 (D) mm (ラックマウントキットを含む)		
質量	単体 : 約3.8kg 冗長構成時 : 約10.6kg (ラックマウントキット含む)		
付属品	電源ケーブル、ラックマウントキット、Web Beagle 操作マニュアル		
管理UIの動作検証済みブラウザ	IE 11 (11.0.9600.18427) Chrome (52.0.2743.116 m) FireFox (46.0.1) Microsoft Edge (20.10240.17146.0)		

- ✂ ※1 DSR 型の場合は、ポート1 のみ使用します。
- ✂ ※2 ボンディング接続時、ポート1 とポート3、ポート2 とポート4 がそれぞれペアになります。DSR 型の場合はポート1 とポート3 を使用します。
- ✂ ※3 L7で動作方式がHTTP, HTTPS 証明書ありの場合のみ
- ✂ ※4 L7で動作方式がHTTPS 証明書なしの場合のみ
- ✂ ※5 L4のみMySQL(TCP上の通信を負荷分散時)が選択可能。ping / DNS はL4でUDP上の通信を負荷分散時で選択可能。
- ✂ ※6 L4とL7の全仮想サービスの合計最大数です。
- ✂ ※7 L4とL7の全仮想サービスで使用するノードサーバの合計最大数です。

付録B. 通知メールの内容

✂ ノード切り離しの通知メールはL4 負荷分散(LVS)特有の機能となります。
L7 負荷分散(HAProxy)にノード切り離しの通知メールはございません。

- 件名
[ホスト名] - Entering MASTER state
- 本文
=> Message Code 001: Device is now owning VIPs <=

- **内容説明**

Web Beagle (ホスト名) がサービス可能な状態になりました。

冗長化構成の場合、対象ホスト名のWeb Beagle がマスター状態で稼働していることを表します。

もし対象ホストがスタンバイ状態で動作していた場合、フェイルオーバーが発生してマスター状態に遷移したことを意味します。

- **件名**

[ホスト名] - Entering BACKUP state

- **本文**

=> Message Code 002: Device is no longer owning VIPs <=

- **内容説明**

Web Beagle (ホスト名) がスタンバイ状態で稼働していることを表します。

本メールは冗長化構成時にのみ、通知されます。

- **件名**

[ホスト名] - Realserver ノードサーバーのIP アドレス - DOWN

- **本文**

=> Message Code 003: The realserver is disabled by user <=

- **内容説明**

管理者が、対象ノードサーバが無効になるよう操作したため、Web Beagle (ホスト名) が管理しているノードサーバ (ノードサーバのIP アドレス) が分散対象から切り離されました。

- **件名**

[ホスト名] - Realserver ノードサーバーのIP アドレス - UP

- **本文**

=> Message Code 004: The realserver is enabled by user <=

- **内容説明**

管理者が、対象ノードサーバが有効になるよう操作したため、Web Beagle (ホスト名) が管理しているノードサーバ (ノードサーバのIP アドレス) が分散対象に復旧しました。

- **件名**

[ホスト名] - Realserver ノードサーバーのIP アドレス - DOWN

- **本文**

=> Message Code 005: TCP CHECK failed on service <=

- **内容説明**

Web Beagle (ホスト名) が管理しているノードサーバ (ノードサーバのIP アドレス) の死活監視 (TCP チェック) で異常を検出したため分散対象から切り離されました。

- **件名**

[ホスト名] - Realserver ノードサーバーのIP アドレス - UP

- **本文**

=> Message Code 006: TCP CHECK succeed on service <=

- **内容説明**

Web Beagle (ホスト名) が管理しているノードサーバ (ノードサーバのIP アドレス) が分散対象に復旧しました。

付録C. Web Beagle MIB 仕様

L4 負荷分散エンジン MIB (LVS MIB)

- **Root OID**

.1.3.6.1.4.1.8255(WebBeagleL4).4711(lvs)

OID	名前	文法	アクセス	説明
LVS テーブル				
lvs 1	lvsVersion	OCTET STRING (SIZE(0..1024))	read-only	Version of the LVS kernel modules
lvs 2	lvsNumServices	INTEGER	read-only	Number of lvs services
lvs 3	lvsHashTableSize	INTEGER	read-only	Hashtable Size
lvs 4	lvsTcpTimeOut	TimeInterval	read-only	TCP Timeout in 1/100 s
lvs 5	lvsTcpFinTimeOut	TimeInterval	read-only	TCP_FIN Timeout in 1/100 s
lvs 6	lvsUdpTimeOut	TimeInterval	read-only	UDP_FIN Timeout in 1/100 s
lvs 7	lvsDaemonState	INTEGER none(0), master(1), backup(2)	read-only	Daemon state
lvs 8	lvsMcastInt	OCTET STRING (SIZE(0..16))	read-only	Multicast Interface Name
lvs 17	lvsServiceTable	SEQUENCE OF lvsServiceEntry	-	A table containing lvs service-specific information.
lvs 18	lvsRealTable	SEQUENCE OF lvsRealEntry	-	A table containing per realserver information.
LVS serviceテーブル				
lvsServiceTable 1	LvsServiceEntry	-	-	information about a lvs service

OID	名前	文法	アクセス	説明
lvsServiceEntry 1	lvsServiceNumber	INTEGER (0..65535)	read-only	The lvs service number
lvsServiceEntry 2	lvsServiceSchedType	OCTET STRING (SIZE(0..16))	read-only	Scheduler Type
lvsServiceEntry 3	lvsServiceProto	INTEGER fwmark(-1), tcp(6), udp(17),	read-only	Protocol (tcp/udp) or packets marked by fwmark
lvsServiceEntry 4	lvsServiceAddr	IpAddress	read-only	IP Address of the Service a.k.a Virtual IP (VIP)
lvsServiceEntry 5	lvsServicePort	INTEGER { fwmark(-1)	read-only	The port number of the service
lvsServiceEntry 6	lvsServiceFWMark	INTEGER { undefined(0);	read-only	The Firewall Mark which tags connections to be processed by this lvs service
lvsServiceEntry 7	lvsServicePersistTimeout	TimeInterval	read-only	The Timeout of persistent connections in 1/100 s
lvsServiceEntry 8	lvsServicePersistNetmask	IpAddress	read-only	The netmask of persitent connections
lvsServiceEntry 9	lvsServiceNumDests	INTEGER (0..65535)	read-only	the number of realservers for this virtual server
lvsServiceEntry 10	lvsServiceStatsConns	Counter32	read-only	the total number of connections which has been handled by this lvs service since the beginning
lvsServiceEntry 11	lvsServiceStatsInPkts	Counter32	read-only	the total number of incomming pakets to this lvs service
lvsServiceEntry 12	lvsServiceStatsOutPkts	Counter32	read-only	the total number of outgoing pakets from this lvs service (always 0 for LVS-DR)

OID	名前	文法	アクセス	説明
lvsServiceEntry 13	lvsServiceStatsInBytes	Counter32	read-only	the total number of incoming bytes from this lvs service
lvsServiceEntry 14	lvsServiceStatsOutBytes	Counter32	read-only	the number of outgoing bytes from this lvs service (always 0 for LVS-DR)
lvsServiceEntry 15	lvsServiceRateCps	Gauge32	read-only	the current connection rate
lvsServiceEntry 16	lvsServiceRateInPPS	Gauge32	read-only	the current in packet rate
lvsServiceEntry 17	lvsServiceRateOutPPS	Gauge32	read-only	the current out packet rate
lvsServiceEntry 18	lvsServiceRateInBPS	Gauge32	read-only	the current in byte rate
lvsServiceEntry 19	lvsServiceRateOutBPS	Gauge32	read-only	the current out byte rate
LVS RealServerテーブル				
lvsRealTable 1	lvsRealEntry	-	-	information about a lvs real server
lvsRealEntry 1	lvsRealServiceNumber	INTEGER (0..65535)	read-only	The lvs service number
lvsRealEntry 2	lvsRealServerNumber	INTEGER (0..65535)	read-only	The lvs realserver number
lvsRealEntry 3	lvsRealServerAddr	IpAddress	read-only	The lvs realserver IP
lvsRealEntry 4	lvsRealServerPort	INTEGER (0..65535)	read-only	The lvs realserver Port
lvsRealEntry 5	lvsRealServerFlags	INTEGER{ masq(0), local(1), tunnel(2), route(3)	read-only	The lvs realserver Flags
lvsRealEntry 6	lvsRealServerWeight	INTEGER (0..65535)	read-only	The lvs realserver weight

OID	名前	文法	アクセス	説明
lvsRealEntry 7	lvsRealStatsConns	Counter32	read-only	the total number of connections which has been handled by this lvs realserver since the beginning
lvsRealEntry 8	lvsRealStatsInPkts	Counter32	read-only	the total number of incoming packets to this lvs realserver
lvsRealEntry 9	lvsRealStatsOutPkts	Counter32	read-only	the total number of outgoing packets from this lvs realserver (always 0 for LVS-DR)
lvsRealEntry 10	lvsRealStatsInBytes	Counter64	read-only	the total number of incoming bytes from this lvs realserver
lvsRealEntry 11	lvsRealStatsOutBytes	Counter64	read-only	the number of outgoing bytes from this lvs realserver (always 0 for LVS-DR)
lvsRealEntry 12	lvsRealRateCps	Gauge32	read-only	the current connection rate
lvsRealEntry 13	lvsRealRateInPPS	Gauge32	read-only	the current in packet rate
lvsRealEntry 14	lvsRealRateOutPPS	Gauge32	read-only	the current out packet rate
lvsRealEntry 15	lvsRealRateInBPS	Gauge32	read-only	the current in byte rate
lvsRealEntry 16	lvsRealRateOutBPS	Gauge32	read-only	the current out byte rate

L7 負荷分散エンジン MIB (HAProxy MIB)

- **Root OID**

.1.3.6.1.4.1.29385(WebBeagleL7).106(haproxy)

OID	名前	文法	アクセス	説明
haproxy Stats テーブル				
haproxy 1	haproxyStats	-	-	-
haproxy Stats FrontEnd テーブル				

OID	名前	文法	アクセス	説明
haproxyStats 0	haproxyFE	-	-	-
haproxyFE 0	haproxyFEpxname	STRING	read-only	Proxy Name
haproxyFE 1	haproxyFEsvname	STRING	read-only	Service Name
haproxyFE 2	haproxyFEqcur	STRING	read-only	Current Queue
haproxyFE 3	haproxyFEqmax	STRING	read-only	Max Queue
haproxyFE 4	haproxyFEscur	STRING	read-only	Current Sessions
haproxyFE 5	haproxyFEsmax	STRING	read-only	Max Sessions
haproxyFE 6	haproxyFEslim	STRING	read-only	Limit Sessions
haproxyFE 7	haproxyFEstot	STRING	read-only	Total Sessions
haproxyFE 8	haproxyFEbin	STRING	read-only	In Bytes
haproxyFE 9	haproxyFEbout	STRING	read-only	Out Bytes
haproxyFE 10	haproxyFEdreq	STRING	read-only	Request Denied
haproxyFE 11	haproxyFEdresp	STRING	read-only	Response Denied
haproxyFE 12	haproxyFEereq	STRING	read-only	Request Errors
haproxyFE 13	haproxyFEecon	STRING	read-only	Connection Errors
haproxyFE 14	haproxyFEeresp	STRING	read-only	Response Errors
haproxyFE 15	haproxyFEwretr	STRING	read-only	Retr Warnings
haproxyFE 16	haproxyFEwredis	STRING	read-only	Redis Warnings

OID	名前	文法	アクセス	説明
haproxyFE 17	haproxyFEstatus	STRING	read-only	Server Status
haproxyFE 18	haproxyFEweight	STRING	read-only	Server Weight
haproxyFE 19	haproxyFEact	STRING	read-only	Active Server
haproxyFE 20	haproxyFEbck	STRING	read-only	Backup Server
haproxyFE 21	haproxyFEchkfail	STRING	read-only	check fail
haproxyFE 22	haproxyFEchkdown	STRING	read-only	check down
haproxyFE 23	haproxyFElastchg	STRING	read-only	last change
haproxyFE 24	haproxyFEdowntime	STRING	read-only	downtime
haproxyFE 25	haproxyFEqlimit	STRING	read-only	Limit Queue
haproxyFE 26	haproxyFEpid	STRING	read-only	proces id
haproxyFE 27	haproxyFEiid	STRING	read-only	proxy id
haproxyFE 28	haproxyFEsid	STRING	read-only	service id
haproxyFE 29	haproxyFEthrottle	STRING	read-only	throttle
haproxyFE 30	haproxyFElbtot	STRING	read-only	lbtot
haproxyFE 31	haproxyFEtracked	STRING	read-only	tracked
haproxyFE 32	haproxyFEtype	STRING	read-only	type
haproxyFE 33	haproxyFERate	STRING	read-only	rate

OID	名前	文法	アクセス	説明
haproxyFE 34	haproxyFEratelim	STRING	read-only	limit rate
haproxyFE 35	haproxyFEratemax	STRING	read-only	max rate
haproxyFE 36	haproxyFEcheckstatus	STRING	read-only	check status
haproxyFE 37	haproxyFEcheckcode	STRING	read-only	check code
haproxyFE 38	haproxyFEcheckduration	STRING	read-only	check duration
haproxyFE 39	haproxyFEhrsp1xx	STRING	read-only	http responses with 1xx code
haproxyFE 40	haproxyFEhrsp2xx	STRING	read-only	http responses with 2xx code
haproxyFE 41	haproxyFEhrsp3xx	STRING	read-only	http responses with 3xx code
haproxyFE 42	haproxyFEhrsp4xx	STRING	read-only	http responses with 4xx code
haproxyFE 43	haproxyFEhrsp5xx	STRING	read-only	http responses with 5xx code
haproxyFE 44	haproxyFEhrspother	STRING	read-only	http responses with other code
haproxyFE 45	haproxyFEhanafail	STRING	read-only	hanafail
haproxyFE 46	haproxyFEreqrate	STRING	read-only	request rate
haproxyFE 47	haproxyFEreqratemax	STRING	read-only	request max rate
haproxyFE 48	haproxyFEreqtot	STRING	read-only	request total
haproxyFE 49	haproxyFEcliabrt	STRING	read-only	cli abort
haproxyFE 50	haproxyFEsvabrt	STRING	read-only	srv abrt

OID	名前	文法	アクセス	説明
haproxyFE 51	haproxyFEcompin	STRING	read-only	comp in
haproxyFE 52	haproxyFEcompout	STRING	read-only	comp out
haproxyFE 53	haproxyFEcompbyp	STRING	read-only	comp byp
haproxyFE 54	haproxyFEcomprsp	STRING	read-only	comp rsp
haproxy Stats BackEnd テーブル				
haproxyStats 1	haproxyBE	-	-	-
haproxyBE 0	haproxyBEpxname	STRING	read-only	Proxy Name
haproxyBE 1	haproxyBEsvname	STRING	read-only	Service Name
haproxyBE 2	haproxyBEqcur	STRING	read-only	Current Queue
haproxyBE 3	haproxyBEqmax	STRING	read-only	Max Queue
haproxyBE 4	haproxyBEscur	STRING	read-only	Current Sessions
haproxyBE 5	haproxyBEsmax	STRING	read-only	Max Sessions
haproxyBE 6	haproxyBEslim	STRING	read-only	Limit Sessions
haproxyBE 7	haproxyBEstot	STRING	read-only	Total Sessions
haproxyBE 8	haproxyBEbin	STRING	read-only	In Bytes
haproxyBE 9	haproxyBEbout	STRING	read-only	Out Bytes
haproxyBE 10	haproxyBEDreq	STRING	read-only	Request Denied
haproxyBE 11	haproxyBEDresp	STRING	read-only	Response Denied

OID	名前	文法	アクセス	説明
haproxyBE 12	haproxyBEereq	STRING	read-only	Request Errors
haproxyBE 13	haproxyBEecon	STRING	read-only	Connection Errors
haproxyBE 14	haproxyBEeresp	STRING	read-only	Response Errors
haproxyBE 15	haproxyBEwretr	STRING	read-only	Retr Warnings
haproxyBE 16	haproxyBEwredis	STRING	read-only	Redis Warnings
haproxyBE 17	haproxyBEstatus	STRING	read-only	Server Status
haproxyBE 18	haproxyBEweight	STRING	read-only	Server Weight
haproxyBE 19	haproxyBEact	STRING	read-only	Active Server
haproxyBE 20	haproxyBEbck	STRING	read-only	Backup Server
haproxyBE 21	haproxyBEchkfail	STRING	read-only	check fail
haproxyBE 22	haproxyBEchkdown	STRING	read-only	check down
haproxyBE 23	haproxyBElastchg	STRING	read-only	last change
haproxyBE 24	haproxyBEDowntime	STRING	read-only	downtime
haproxyBE 25	haproxyBEqlimit	STRING	read-only	Limit Queue
haproxyBE 26	haproxyBEpid	STRING	read-only	proces id
haproxyBE 27	haproxyBEiid	STRING	read-only	proxy id
haproxyBE 28	haproxyBEsid	STRING	read-only	service id

OID	名前	文法	アクセス	説明
haproxyBE 29	haproxyBEthrottle	STRING	read-only	throttle
haproxyBE 30	haproxyBElbtot	STRING	read-only	lbtot
haproxyBE 31	haproxyBEtracked	STRING	read-only	tracked
haproxyBE 32	haproxyBEtype	STRING	read-only	type
haproxyBE 33	haproxyBERate	STRING	read-only	rate
haproxyBE 34	haproxyBERatelim	STRING	read-only	limit rate
haproxyBE 35	haproxyBERatemax	STRING	read-only	max rate
haproxyBE 36	haproxyBEcheckstatus	STRING	read-only	check status
haproxyBE 37	haproxyBEcheckcode	STRING	read-only	check code
haproxyBE 38	haproxyBEcheckduration	STRING	read-only	check duration
haproxyBE 39	haproxyBEhrsp1xx	STRING	read-only	http responses with 1xx code
haproxyBE 40	haproxyBEhrsp2xx	STRING	read-only	http responses with 2xx code
haproxyBE 41	haproxyBEhrsp3xx	STRING	read-only	http responses with 3xx code
haproxyBE 42	haproxyBEhrsp4xx	STRING	read-only	http responses with 4xx code
haproxyBE 43	haproxyBEhrsp5xx	STRING	read-only	http responses with 5xx code
haproxyBE 44	haproxyBEhrspother	STRING	read-only	http responses with other code
haproxyBE 45	haproxyBEhanafail	STRING	read-only	hanafail

OID	名前	文法	アクセス	説明
haproxyBE 46	haproxyBEreqrate	STRING	read-only	request rate
haproxyBE 47	haproxyBEreqratemax	STRING	read-only	request max rate
haproxyBE 48	haproxyBEreqtot	STRING	read-only	request total
haproxyBE 49	haproxyBEcliabrt	STRING	read-only	cli abort
haproxyBE 50	haproxyBESrvabrt	STRING	read-only	srv abrt
haproxyBE 51	haproxyBEcompin	STRING	read-only	comp in
haproxyBE 52	haproxyBEcompout	STRING	read-only	comp out
haproxyBE 53	haproxyBEcompbyp	STRING	read-only	comp byp
haproxyBE 54	haproxyBEcomprsp	STRING	read-only	comp rsp
haproxyBE 55	haproxyBElastsess	STRING	read-only	last sessions
haproxyBE 56	haproxyBElastchk	STRING	read-only	last check
haproxyBE 57	haproxyBElastagt	STRING	read-only	last agt
haproxyBE 58	haproxyBEqtime	STRING	read-only	qtime
haproxyBE 59	haproxyBEctime	STRING	read-only	ctime
haproxyBE 60	haproxyBERtime	STRING	read-only	rtime
haproxyBE 61	haproxyBETIME	STRING	read-only	ttime

haproxy Stats Server テーブル

haproxyStats 2	haproxySV	-	-	-
----------------	-----------	---	---	---

OID	名前	文法	アクセス	説明
haproxySV 0	haproxySVpxname	STRING	read-only	Proxy Name
haproxySV 1	haproxySVsvname	STRING	read-only	Service Name
haproxySV 2	haproxySVqcur	STRING	read-only	Current Queue
haproxySV 3	haproxySVqmax	STRING	read-only	Max Queue
haproxySV 4	haproxySVscur	STRING	read-only	Current Sessions
haproxySV 5	haproxySVsmax	STRING	read-only	Max Sessions
haproxySV 6	haproxySVslim	STRING	read-only	Limit Sessions
haproxySV 7	haproxySVstot	STRING	read-only	Total Sessions
haproxySV 8	haproxySVbin	STRING	read-only	In Bytes
haproxySV 9	haproxySVbout	STRING	read-only	Out Bytes
haproxySV 10	haproxySVdreq	STRING	read-only	Request Denied
haproxySV 11	haproxySVdresp	STRING	read-only	Response Denied
haproxySV 12	haproxySVereq	STRING	read-only	Request Errors
haproxySV 13	haproxySVecon	STRING	read-only	Connection Errors
haproxySV 14	haproxySVeresp	STRING	read-only	Response Errors
haproxySV 15	haproxySVwretr	STRING	read-only	Retr Warnings
haproxySV 16	haproxySVwredis	STRING	read-only	Redis Warnings

OID	名前	文法	アクセス	説明
haproxySV 17	haproxySVstatus	STRING	read-only	Server Status
haproxySV 18	haproxySVweight	STRING	read-only	Server Weight
haproxySV 19	haproxySVact	STRING	read-only	Active Server
haproxySV 20	haproxySVbck	STRING	read-only	Backup Server
haproxySV 21	haproxySVchkfail	STRING	read-only	check fail
haproxySV 22	haproxySVchkdown	STRING	read-only	check down
haproxySV 23	haproxySVlastchg	STRING	read-only	last change
haproxySV 24	haproxySVdowntime	STRING	read-only	downtime
haproxySV 25	haproxySVqlimit	STRING	read-only	Limit Queue
haproxySV 26	haproxySVpid	STRING	read-only	proces id
haproxySV 27	haproxySViid	STRING	read-only	proxy id
haproxySV 28	haproxySVsid	STRING	read-only	service id
haproxySV 29	haproxySVthrottle	STRING	read-only	throttle
haproxySV 30	haproxySVlbtot	STRING	read-only	lbtot
haproxySV 31	haproxySVtracked	STRING	read-only	tracked
haproxySV 32	haproxySVtype	STRING	read-only	type
haproxySV 33	haproxySVrate	STRING	read-only	rate

OID	名前	文法	アクセス	説明
haproxySV 34	haproxySVratelim	STRING	read-only	limit rate
haproxySV 35	haproxySVratemax	STRING	read-only	max rate
haproxySV 36	haproxySVcheckstatus	STRING	read-only	check status
haproxySV 37	haproxySVcheckcode	STRING	read-only	check code
haproxySV 38	haproxySVcheckduration	STRING	read-only	check duration
haproxySV 39	haproxySVhrsp1xx	STRING	read-only	http responses with 1xx code
haproxySV 40	haproxySVhrsp2xx	STRING	read-only	http responses with 2xx code
haproxySV 41	haproxySVhrsp3xx	STRING	read-only	http responses with 3xx code
haproxySV 42	haproxySVhrsp4xx	STRING	read-only	http responses with 4xx code
haproxySV 43	haproxySVhrsp5xx	STRING	read-only	http responses with 5xx code
haproxySV 44	haproxySVhrspother	STRING	read-only	http responses with other code
haproxySV 45	haproxySVhanafail	STRING	read-only	hanafail
haproxySV 46	haproxySVreqrate	STRING	read-only	request rate
haproxySV 47	haproxySVreqratemax	STRING	read-only	request max rate
haproxySV 48	haproxySVreqtot	STRING	read-only	request total
haproxySV 49	haproxySVcliabrt	STRING	read-only	cli abort
haproxySV 50	haproxySVsvabrt	STRING	read-only	srv abrt

OID	名前	文法	アクセス	説明
haproxySV 51	haproxySVcompin	STRING	read-only	comp in
haproxySV 52	haproxySVcompout	STRING	read-only	comp out
haproxySV 53	haproxySVcompbyp	STRING	read-only	comp byp
haproxySV 54	haproxySVcomprsp	STRING	read-only	comp rsp
haproxySV 55	haproxyBElastsess	STRING	read-only	last sessions
haproxySV 56	haproxyBElastchk	STRING	read-only	last check
haproxySV 57	haproxyBElastagt	STRING	read-only	last agt
haproxySV 58	haproxyBEqtime	STRING	read-only	qtime
haproxySV 59	haproxyBEctime	STRING	read-only	ctime
haproxySV 60	haproxyBERtime	STRING	read-only	rtime
haproxySV 61	haproxyBETtime	STRING	read-only	ttime
haproxy Info テーブル				
haproxy 2	haproxyInfo	-	-	-
haproxy Info Nameテーブル				
haproxyInfo 0	haproxyInfoName	-	-	-
haproxyInfoName 0	haproxyINName	STRING	read-only	Name
haproxyInfoName 1	haproxyINVersion	STRING	read-only	Version
haproxyInfoName 2	haproxyINReleaseDate	STRING	read-only	Release date
haproxyInfoName 3	haproxyINNbproc	STRING	read-only	Nbproc

OID	名前	文法	アクセス	説明
haproxyInfoName 4	haproxyINProcessNum	STRING	read-only	Process num
haproxyInfoName 5	haproxyINPid	STRING	read-only	Pid
haproxyInfoName 6	haproxyINUptime	STRING	read-only	Uptime
haproxyInfoName 7	haproxyINUptimeSec	STRING	read-only	Uptime sec
haproxyInfoName 8	haproxyINMemmaxMB	STRING	read-only	Memmax MB
haproxyInfoName 9	haproxyINUlimit-n	STRING	read-only	Ulimit-n
haproxyInfoName 10	haproxyINMaxsock	STRING	read-only	Maxsock
haproxyInfoName 11	haproxyINMaxconn	STRING	read-only	Maxconn
haproxyInfoName 12	haproxyINMaxpipes	STRING	read-only	Maxpipes
haproxyInfoName 13	haproxyINCurrConns	STRING	read-only	CurrConns
haproxyInfoName 14	haproxyINPipesUsed	STRING	read-only	PipesUsed
haproxyInfoName 15	haproxyINPipesFree	STRING	read-only	PipesFree
haproxyInfoName 16	haproxyINTasks	STRING	read-only	Tasks
haproxyInfoName 17	haproxyINRunQueue	STRING	read-only	Run queue
haproxyInfoName 18	haproxyINnode	STRING	read-only	node
haproxyInfoName 19	haproxyINdescription	STRING	read-only	description
haproxy Info Valueテーブル				
haproxyInfo 1	haproxyInfoValue	-	-	-

OID	名前	文法	アクセス	説明
haproxyInfoValue 0	haproxyIVName	STRING	read-only	Name
haproxyInfoValue 1	haproxyIVVersion	STRING	read-only	Version
haproxyInfoValue 2	haproxyIVReleaseDate	STRING	read-only	Release date
haproxyInfoValue 3	haproxyIVNbproc	STRING	read-only	Nbproc
haproxyInfoValue 4	haproxyIVProcessNum	STRING	read-only	Process num
haproxyInfoValue 5	haproxyIVPid	STRING	read-only	Pid
haproxyInfoValue 6	haproxyIVUptime	STRING	read-only	Uptime
haproxyInfoValue 7	haproxyIVUptimeSec	STRING	read-only	Uptime sec
haproxyInfoValue 8	haproxyIVMemmaxMB	STRING	read-only	Memmax MB
haproxyInfoValue 9	haproxyIVUlimit-n	STRING	read-only	Ulimit-n
haproxyInfoValue 10	haproxyIVMaxsock	STRING	read-only	Maxsock
haproxyInfoValue 11	haproxyIVMaxconn	STRING	read-only	Maxconn
haproxyInfoValue 12	haproxyIVMaxpipes	STRING	read-only	Maxpipes
haproxyInfoValue 13	haproxyIVCurrConns	STRING	read-only	CurrConns
haproxyInfoValue 14	haproxyIVPipesUsed	STRING	read-only	PipesUsed
haproxyInfoValue 15	haproxyIVPipesFree	STRING	read-only	PipesFree
haproxyInfoValue 16	haproxyIVTasks	STRING	read-only	Tasks

OID	名前	文法	アクセス	説明
haproxyInfoValue 17	haproxyIVRunQueue	STRING	read-only	Run queue
haproxyInfoValue 18	haproxyIVnode	STRING	read-only	node
haproxyInfoValue 19	haproxyIVdescription	STRING	read-only	description

本マニュアルについて

注意事項

株式会社エーティーワークスは本マニュアルの記述のいかなる誤りに対しても責任を負うものではありません。

また、株式会社エーティーワークスは本マニュアルの記述の使用によるいかなる結果に対しても責任を負うものではありません。本マニュアルはお客様の責任で使用してください。

本マニュアルの内容は情報提供のみを目的としており、予告なしに変更される場合があります。

事前に株式会社エーティーワークスによる許可がない限り、本マニュアルのいかなる部分も複製することはできません。

また、株式会社エーティーワークスによる許可がない限り、本マニュアルを配布することはできません。

変更履歴

- 2016/02/22 初版
- 2016/08/22 第2版
 - L4 負荷分散でプロトコルを選択できるようになったことによる修正
 - L4 負荷分散の死活監視方式にMySQLが追加になったことによる修正
 - L7 負荷分散方式に最大接続数以下同一サーバーが追加になったことによる修正
 - 【L4 IPフィルタ設定】 ページ追加による修正
 - 【L7 IPフィルタ設定】 ページ追加による修正
 - 【旧モデルからの設定情報のリストア】 ページ追加による修正
 - 【ログ】 メニュー追加による修正
- 2016/09/12 第3版
 - Model 600 の説明を修正 (第1章 Model 600 フロントパネルの説明)
 - Web Beagle の特徴を修正 (第1章 3. Web Beagle の特徴)
 - 透過型 (Model 500, Model 600) の図を修正 (第2章 1. 設置計画 透過型 (Model 500, Model 600))
 - DSR 型の説明を修正 (第2章 2. 初期設定 ネットワーク構成例 DSR 型)
 - NAT 型の説明を修正 (第2章 2. 初期設定 ネットワーク構成例 NAT 型 (Model 500, Model600))
 - 透過型の説明を修正 (第2章 2. 初期設定 ネットワーク構成例 透過型 (Model 500, Model600))
 - 仮想サービスの設定を修正 (第2章 4. 仮想サービスの設定)
 - DSR 型の単体構成の図を修正 (第3章 2. 冗長化構成例 1. DSR 型のセットアップ)
 - 設置状態の図を修正 (第3章 3. 冗長化構成時の動作について)
 - 死活監視機能の説明を修正 (第4章 1. 死活監視機能)
 - NAT 設定の説明を修正 (第5章 2. 基本設定 NAT 設定)
 - 基本NAT, NAPT, IP マスカレードの説明を追記 (第5章 2. 基本設定 NAT 設定)
 - 冗長化設定の説明を修正 (第5章 2. 基本設定 冗長化設定)
 - L4 仮想サービスの説明を修正 (第5章 4. L4 負荷分散 L4 仮想サービス)
 - 付録の仕様を追記 (付録 付録A. 仕様)
- 2016/11/22 第4版
 - 設定例2 OS がWindows Server 2008 の場合の説明を修正 (第2章 ネットワーク構成例 設定例2 OS がWindows Server 2008 の場合)
 - 設定例3 OS がWindows Server 2012 の場合の説明を修正 (第2章 ネットワーク構成例 設定例3 OS がWindows Server 2012 の場合)

- 待機サーバの設定手順を修正 (第4章 3. 待機サーバ機能 待機サーバの設定手順)
- L4 ノードサーバー一覧の説明を修正 (第5章 4. L4 負荷分散 L4 ノードサーバー一覧)
- L7 ノードサーバー一覧の説明を修正 (第5章 5. L7 負荷分散 L7 ノードサーバー一覧)
- L7 ノードサーバ追加／編集の説明を修正 (第5章 5. L7 負荷分散 L7 ノードサーバ追加／編集)
- 付録の仕様を追記 (付録 付録A. 仕様)
- 2017/01/06 第5版
 - フロントパネルの図の説明を修正 (第1章 5. ハードウェアの取り扱いについて)
 - Web Beagle とメンテナンスPC の接続の説明を修正 (第2章 2. 初期設定 2-1. メンテナンスPC を利用して設定する (推奨))
 - DSR 型の説明を修正 (第2章 2. 初期設定 ネットワーク構成例 DSR 型)
 - NAT 型の説明を修正 (第2章 2. 初期設定 ネットワーク構成例 NAT 型 (Model 500, Model600))
 - 透過型の説明を修正 (第2章 2. 初期設定 ネットワーク構成例 透過型 (Model 500, Model600))
 - ネットワークポートの説明を修正 (第5章 2. ホーム ダッシュボード)
 - 付録の管理UIの動作検証済みブラウザを追記 (付録 付録A. 仕様)
- 2017/02/20 第6版
 - 第7章 保証とアフターサービスを追加 (第7章 保証とアフターサービス)
- 2017/06/21 第7版
 - セットアップの説明を修正 (第2章 ネットワーク構成例 DSR型における仮想IPアドレス宛の接続を受け付ける設定 設定例 1)
 - DSR型の説明に追記 (第2章 DSR型 DSR構成におけるL7負荷分散の通信経路)
 - ネットワークの説明に追記 (第5章 基本設定 ネットワーク ネットワーク設定表示・ネットワーク設定編集)
 - 冗長化の説明に追記 (第5章 冗長化設定 冗長化設定の表示・冗長化設定の編集)
 - 付録の記載を修正 (付録 表中の項目「冗長化構成」の説明)