NEC

InterSec/CS400k

ユーザーズガイド

2017年8月　第1版

商標について

Microsoft、Windows、Windows Server、Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標 または 商標です。Adobe、Adobe ロゴ、Acrobat は、AdobeSystemsIncorporated（アドビシステムズ社）の登録商標または商標です。Linux®は LinusTorvalds 氏の日本およびその他の国における登録商標または商標です。RedHat®および Red Hat Enterprise Linux は、米国 RedHat,Inc.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。Java、JavaScript は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における商標または登録商標です。ALSI、InterSafe、InterSafe WebFilter は、アルプスシステムインテグレーション株式会社の登録商標です。TRENDMICRO、InterScanWebManager は、トレンドマイクロ株式会社の登録商標です。デジタルアーツ/DIGITAL ARTS、i-FILTER は、デジタルアーツ株式会社の登録商標です。その他記載の会社名および商品名は各社の商標または登録商標です。

オペレーティングシステムの表記ついて

Windows Server 2012 R2 は、Windows Server®2012 R2 Essentials operating system 、Windows Server®2012 R2 Standard operating system および Windows Server®2012 R2 Datacenter operating system の略称です。Windows Server 2012 は、Windows Server®2012 Standard operating system および Windows Server®2012 Datacenter operating system の略称です。Windows Server 2008 R2 は、Windows Server®2008 R2 Standard operating system および Windows Server®2008 R2 Enterprise operating system の略称です。Windows Server 2008 は、Windows Server®2008 Standard operating system および Windows Server®2008 Enterprise operating system の略称です。Windows Server 2003 x64 Editions は Windows®Server2003 R2、Standard x64 Edition operating system および Windows Server®2003 R2,Enterprise x64 Edition operating system または、Windows Server®2003,Standard x64 Edition operating system および Windows Server®2003,Enterprise x64 Edition operating system の略称です。Windows Server2003 は Windows Server®2003 R2 Standard Editionoperating system および Windows Server®2003 R2 Enterprise Edition operating system または、Windows Server®2003 Standard Edition operating system および Windows Server®2003 Enterprise Edition operating system の略称です。Windows8 は Microsoft® Windows®8 operating system の略称です。Windows7 は Microsoft® Windows®7 operating system の略称です。Windows Vista は Microsoft ® Windows Vista®Business operating system の略称です。Windows XP x64Edition は、Microsoft ® Windows® XP Professional x64 Edition operatingsystem の略称です。

Windows XP は Microsoft® Windows® XP Home Edition operating system および Microsoft® Windows® XP Professional operating system の略称です。

Red Hat Enterprise Linux 6 Server は、Red Hat Enterprise Linux 6 Server(x86)および Red Hat Enterprise Linux 6 Server(EMT64T)の総称です。サンプルアプリケーションで使用している名称は、すべて架空のものです。実在する品名、団体名、個人名とは一切関係ありません。本製品で使用しているソフトウェアの大部分は、BSD の著作と GNU のパブリックライセンスの条項に基づいて自由に配布することができます。ただし、アプリケーションの中には、その所有者に所有権があり、再配布に許可が必要なものがあります。

ご注意

(1)本書の内容の一部または全部を無断転載することは禁止されています。

(2)本書の内容に関しては将来予告なしに変更することがあります。

(3)弊社の許可なく複製・改変などを行うことはできません。

(4)本書は内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、お買い求めの販売店にご連絡ください。

(5)運用した結果の影響については(4)項にかかわらず責任を負いかねますのでご了承ください。

はじめに

このたびは、NEC の InterSec/CS400k(以後、InterSec/CS と記載)をお買い求めいただき、まことにありがとうございます。

本製品は、ネットワークに欠かせない各機能(メール/DNS・DHCP、プロキシ/Web フィルタリング、ロードバランサ)を、容易に構築し、効率的に運用できる、NEC のアプライアンスソフト InterSec の 1 つです。

用途に適したチューニングにより、堅牢なセキュリティを実現しつつ、高速なネットワーク環境を提供いたします。また、セットアップのわずらわしさをまったく感じさせない専用のセットアッププログラムやマネージメント Web アプリケーションは、お客様の一元管理の元でさらに細やかで高度なサービスを提供します。

本製品の持つ機能を最大限に引き出すためにも、ご使用になる前に本書をよくお読みになり、本製品の取り扱いを十分にご理解ください。

本書について

本書は、本製品を正しくセットアップし、使用できるようにするための手引きです。
安全に快適に使用していただくため、日常の利用、セットアップ、わからないことや不具合が起きた場合にご利用ください。
本書は常に本製品のそばに置いていつでも見られるようにしてください。

本文中の記号について

本書では巻頭で示した安全にかかわる注意記号の他に 3 種類の記号を使用しています。これらの記号と意味をご理解になり、本製品を正しくお取り扱いください。

	InterSec/CS の取り扱いや、ソフトウェアの操作で守らなければならない事柄や特に注意をすべき点を示します。
	InterSec/CS の取り扱いやソフトウェアを操作する上で確認をしておく必要がある点を示します。
	知っておくと役に立つ情報や、便利なことなどを示します。

本書の再入手について

ユーザーズガイドは、本製品ホームページからダウンロードすることができます。
「アプライアンスソフト InterSec　http://jpn.nec.com/intersec/」

目次

改版履歴

版数	改版日付	内容
1	2017 年 8 月	新規作成

1章 アプライアンスソフト InterSec について

本製品の特長や導入の際に知っておいていただきたい事柄について説明します。

・アプライアンスソフト InterSec とは

アプライアンスソフト InterSec の紹介と製品の特長・機能について説明しています。

・機能と特長

本ソフトウェア製品の機能と特長について説明します。

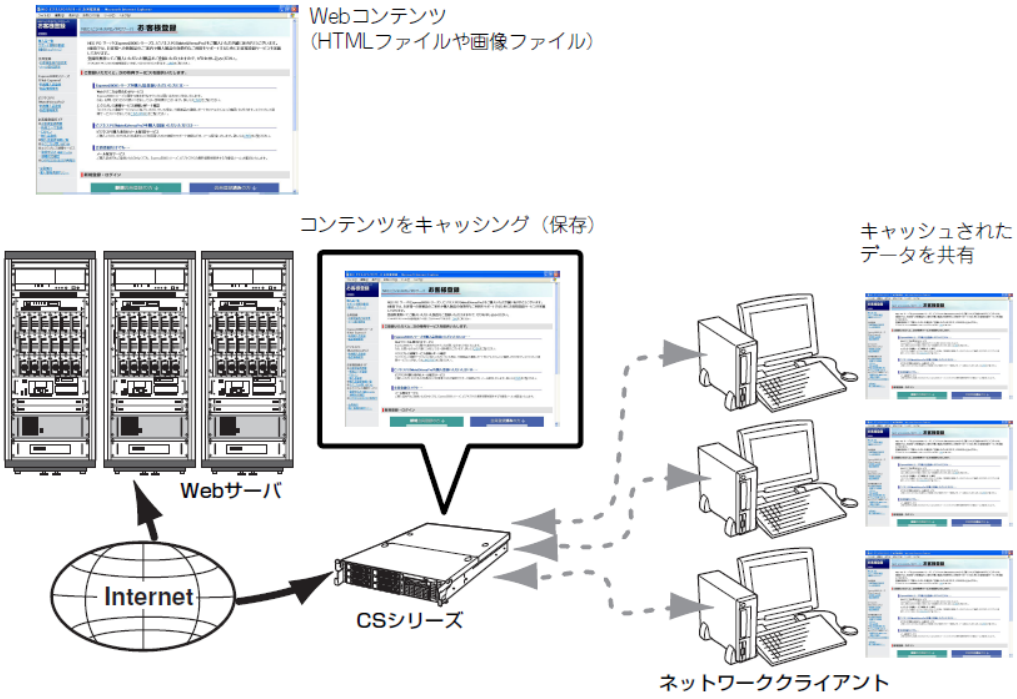
1.1. アプライアンスソフト InterSec とは

アプライアンスソフト InterSec は、お客様の運用目的に特化した設計で、必要のないサービス/機能を省くことでセキュリティホールの可能性を低減するなど、インターネットおよびイントラネットの構築時に不可欠なセキュリティについて考慮された、インターネットセキュリティ製品です。

- 高い拡張性
  専用のアプライアンスソフトとして、機能ごとに単体ユニットで動作させているために用途に応じた機能　拡張が容易に可能です。また、複数ユニットで冗長化構成にすることによりシステムを拡張していくことができます。
- コストパフォーマンスの向上
  運用目的への最適なチューニングが行われているため、単機能の動作において高い性能を確保できます。また、単機能動作に必要なモジュールのみ提供しているため、余剰がなく低コスト化が実現されています。
- 管理の容易性
  Web ベースの運用管理ツールから、環境設定や運用時における管理情報など、単機能が動作するために必要な設定のみを入力します。導入・運用管理が容易に行えます。

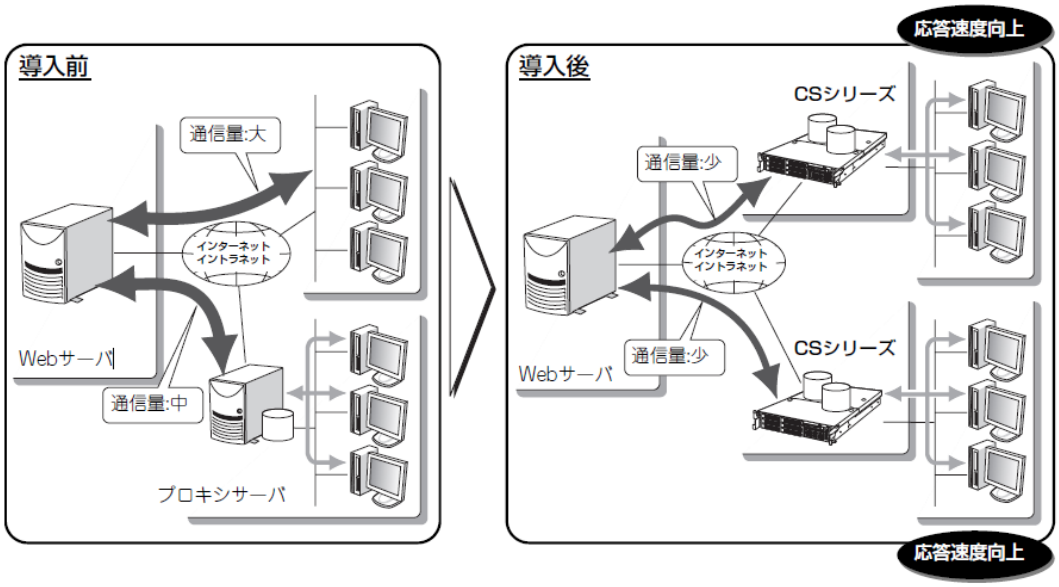
1.2. 機能と特徴

本製品は、社内から外部 Web サーバへのアクセスをより効率化するフォワードキャッシュと、WWW サーバの前段に設置し、WWW サーバの負荷軽減・コンテンツの保護を行うリバースキャッシュの機能をともにサポートします。運用管理ツール(Web ブラウザベース)やレポート機能を標準で装備し TCO 削減にも役立ちます。



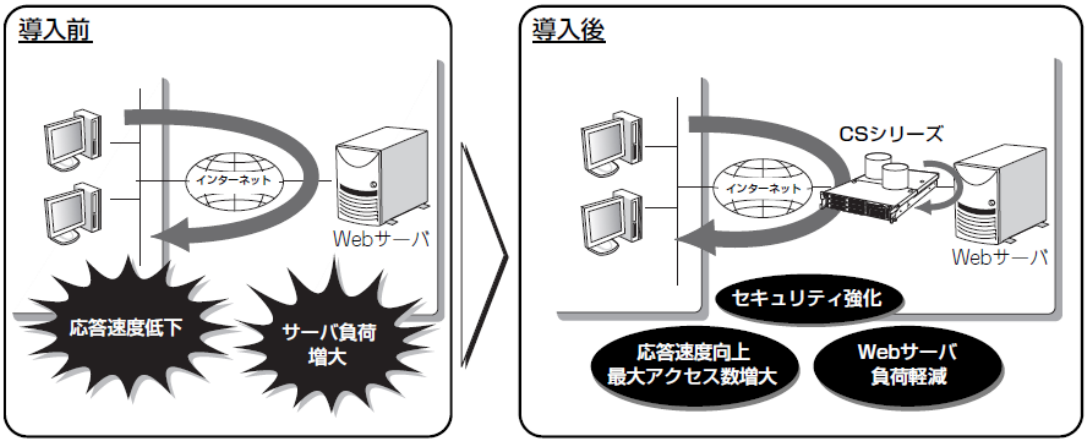
- **フォワードキャッシュ機能**

  クライアント側に Proxy サーバと新規/置換/併設して設置することにより、高性能キャッシュ機能を活かし、アクセスされたコンテンツを自動的に保存(キャッシュ)/再利用して、素早いレスポンスの提供と、回線コスト＆トラフィックを軽減/削減します。

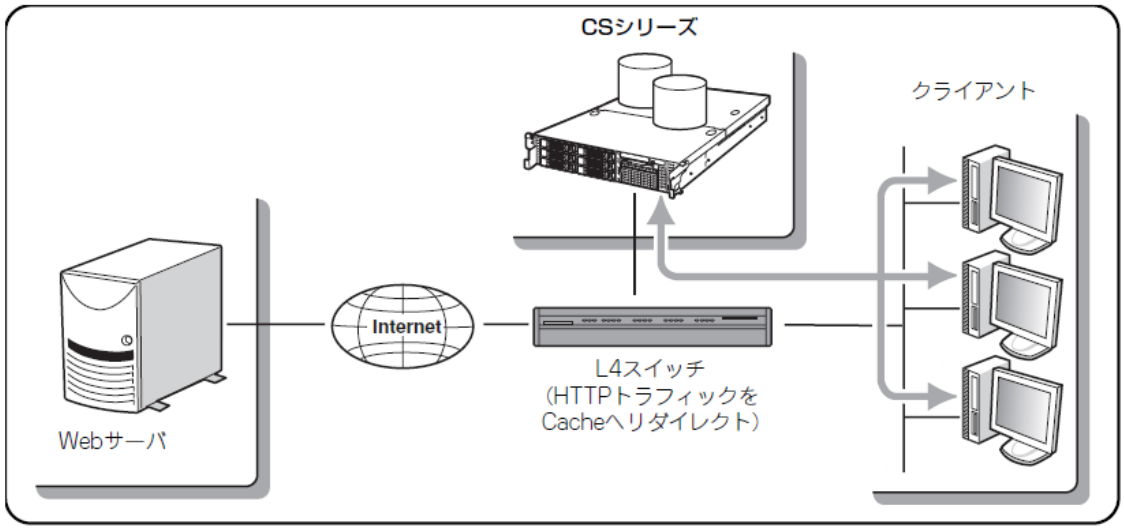


- **リバースキャッシュ機能**

  Web サーバ側の前段に設置しアクセス受付を代理させることで、高性能キャッシュ機能を活かし、コンテンツを自動でコピー保存(キャッシュ)し、複数台分の Web サーバと同じインターネットアクセス量を受け付けます。



- **運用管理機能**
  管理ツールは Web ブラウザ経由で GUI 化されています。
- **統計情報表示機能**
  アクセスログを解析し、統計情報をグラフ・表形式で表示します。また、この統計情報を元にダウンロードスケジュール、アクセス制限の指定を行うことも可能です。
- **スケジュールダウンロード機能**
  よく参照されるページをあらかじめ指定時刻にダウンロードし、キャッシュに格納しておくことが可能です。
- **IP フィルタリング機能**
  プロキシ機能を利用するクライアントを IP アドレスで制限し、部外者の不正な利用を防ぎます。
- **URL フィルタリング機能**
  フィルタ機能を利用すると、有害な Web などへのアクセスを制限します。
- **透過プロキシ機能**
  L4 スイッチを導入し、CS に透過プロキシ設定を行うことで、クライアントは、プロキシの設定をする必要がなくなります。



2章 システムのセットアップ

初期セットアップが完了した後に、システムのセットアップを行う必要があります。

2.1. セットアップ

2.1.1. 各種システムのセットアップについて

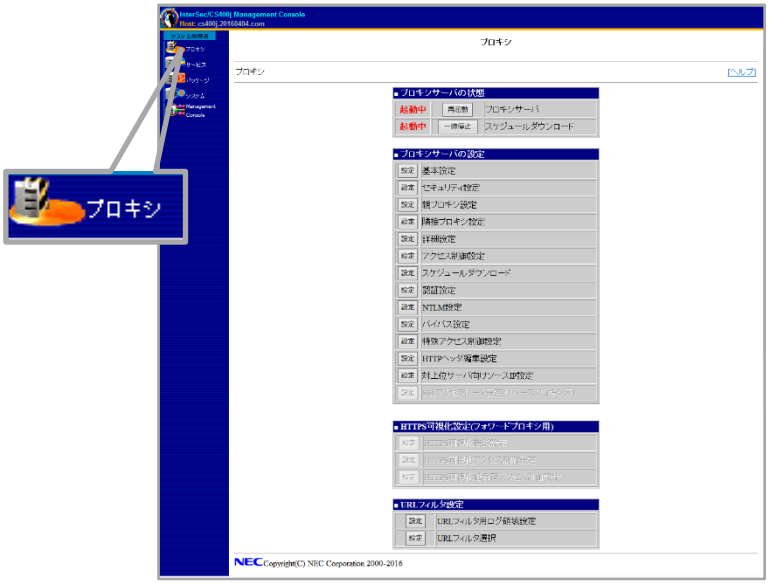
初期セットアップが完了したあとにシステムのセットアップを行ってください。

設定可能な機能の概要を Management Console 画面構成に従って説明します。

初期セットアップ後、初めて Management Console へログインする場合の手順については、「3.1.5. 初期ログイン」を参照してください。

2.1.1.1. プロキシ

InterSec/CS は頻繁にアクセスするページをキャッシングすることにより、次回、同じページにアクセスした際に、ブラウザの表示時間を短縮します。管理者は、Management Console から、有害な Web サイトなどへのアクセスの制限、不正なアクセスの制限などを設定することができます。また、頻繁に参照される Web ページをシステムに自動的にダウンロードさせ、システム内に格納しておくための設定もできます。これらの設定により、効率的なインターネットへのアクセスを実現します。



2.1.1.1.1. プロキシサーバ

プロキシサーバの起動状態を表示します。[再起動]をクリックするとプロキシサーバの再起動を行います(システムは再起動しません)。

2.1.1.1.2. スケジュールダウンロード

コンテンツを定期的にダウンロードしてキャッシュに格納するスケジュールダウンロードの状態を表示します。スケジュールダウンロードの使用を止める場合には、[一時停止]をクリックしてください。スケジュールダウンロードの再開は[起動]をクリックします。

2.1.1.1.3. 基本設定

ブラウザなどからの要求を受け付ける IP アドレスやポート番号など、プロキシサーバを動作させるための基本的な設定をサーバ種別に応じて設定します。

2.1.1.1.4. 基本設定(リバースプロキシ)

「プロキシ」画面の「基本設定」でサーバ種別設定を「Reverse」と選ぶことによって表示される画面です。この画面では、システムをリバースモードで運用する際の設定ができます(システムをリバースモードで運用するには DNS サーバとの連携が必須です)。

2.1.1.1.5. セキュリティ設定

クライアント IP アドレス制限と、CONNECT トラフィック制限を行います。

2.1.1.1.6. 親プロキシ設定

階層構造を形成する場合に親プロキシを設定することができます。親プロキシの指定と、親プロキシの選択方法を設定します。

2.1.1.1.7. 隣接プロキシ設定

階層構造を形成する場合にシステムの隣接プロキシを設定することができます。

2.1.1.1.8. 詳細設定

「プロキシ」画面の「詳細設定」でプロキシサーバとしての詳細な動作設定ができます。

2.1.1.1.9. アクセス制御設定

「プロキシ」画面の「アクセス制御設定」では、アクセス許可/禁止やキャッシュ許可/禁止、プロキシの使用許可/禁止というアクセスの制御が行えます。この設定は、最初に条件を持つリストを登録し、それぞれのリストに対しての動作条件(アクセス制御、非キャッシュ設定、no-cache リクエスト制御、プロキシ転送)を設定していくという流れになります。デフォルトは、リスト設定に「リスト名:all ,設定種別:src ,条件式:0.0.0.0/0.0.0.0 0::0/64」、「リスト名:cgi ,設定種別:url_pathregex ,条件式:¥.cgi$¥?」、アクセス制御設定に「allow/deny:allow ,リスト名:all」、非キャッシュ設定に「allow/deny:deny ,リスト名:cgi」です。

2.1.1.1.9.1. リスト設定

アクセス制御設定にリストの追加/編集/削除を行います。

- リストの追加
  リストを登録するには、アクセス制御の上画面に表示されている「リスト設定」画面から、[追加]をクリックします。
- リストの編集
  リストを編集するには、アクセス制御の上画面に表示されている[リスト設定]画面から編集したいリスト名の左横にある[編集]をクリックします。
- リストの削除
  リストを削除するには、アクセス制御の上画面に表示されている「リスト設定」画面から削除したいリスト名の左横にある[削除]をクリックします。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]をクリックしてください。

2.1.1.1.9.2. 動作条件の設定

アクセス制御の下画面では、登録したリストに対して動作条件の設定を行います。4 つの動作について設定することができます。

- アクセス制御設定
  登録したリストに対して、アクセスの許可/禁止を設定します。
- 非キャッシュ設定
  登録したリストに対して、キャッシュしてもよい/いけないを設定します。
- no-cache リクエスト制御設定
  登録したリストに対して、リクエストの Cache-Control ヘッダ、または Pragma ヘッダに指定されている“no-cache”に対応した処理をする/しないを設定します
- プロキシ転送設定
  登録したリストに対して、Web サーバへの接続を親プロキシ経由で転送するか、直接 Web サーバへ転送するかを設定します。

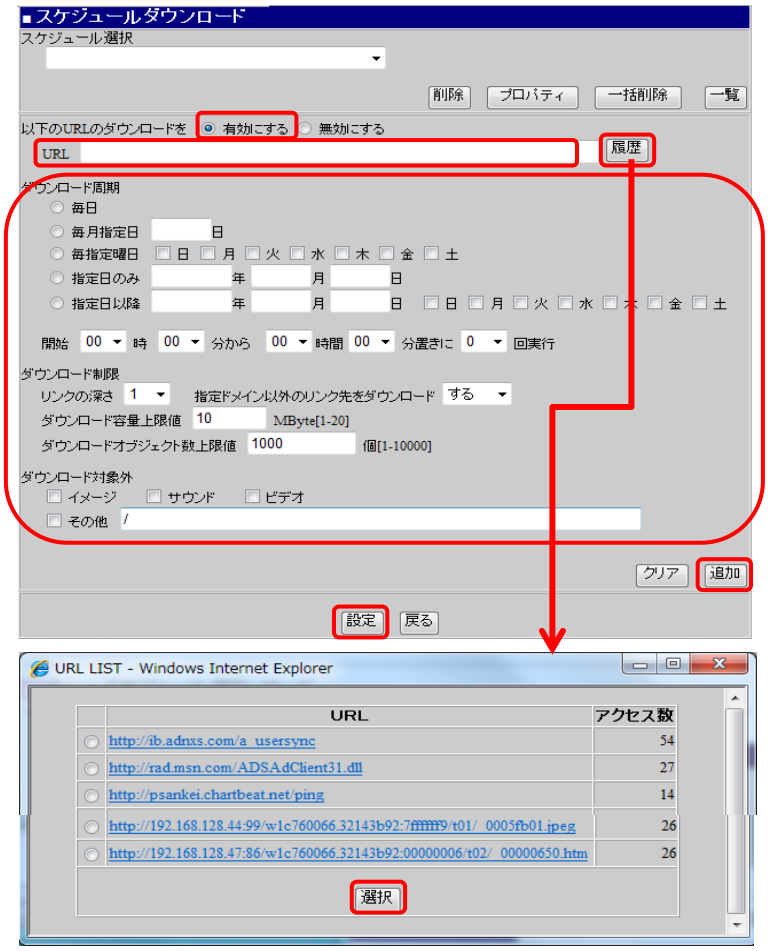
2.1.1.1.10. スケジュールダウンロード

スケジュールダウンロードとは、指定したページをあらかじめ指定時刻にダウンロードし、キャッシュ可能であればキャッシュする機能です。対象となる URL、ダウンロード周期などスケジュールダウンロードの設定ができます。

2.1.1.1.10.1. スケジュールの新規追加

スケジュールを追加するには、対象となる URL、ダウンロード周期などを設定し[追加]をクリックします。スケジュールは最大 100 件まで追加できます。

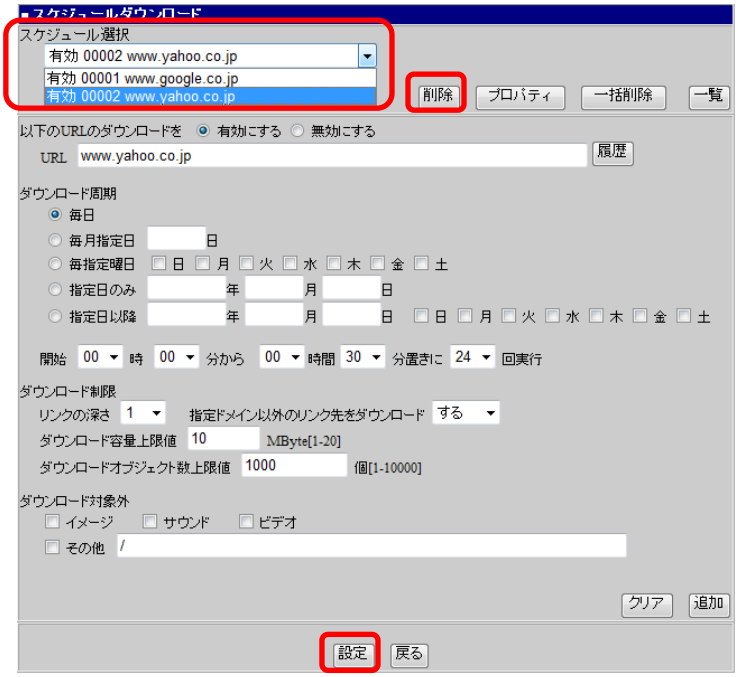
スケジュールを追加する手順は、以下ののとおりです。



1) 「有効にする」を選択する。
2) 以下のいずれかの方法で、ダウンロードする URL を指定する。
   - URL 欄に URL を入力する　　例） http://nec8.com/
   - [履歴]をクリックし、表示される「URL LIST」画面で URL を選択し、[選択]をクリックする
3) 「ダウンロード周期」「ダウンロード制限」「ダウンロード対象外」でダウンロードの条件を指定する。
4) [追加]をクリックしてダウンロードしたい URL を追加する。
5) [設定]をクリックする。

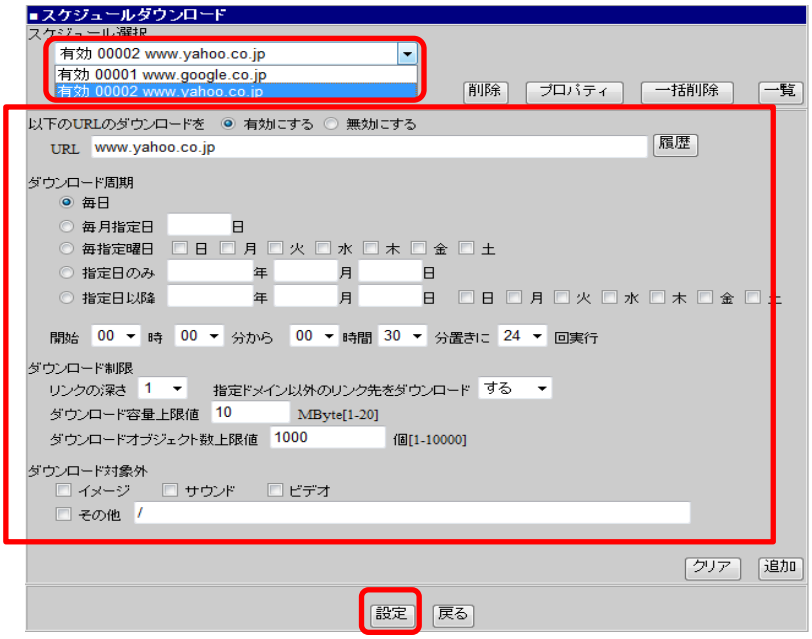
2.1.1.1.10.2. スケジュールの変更

スケジュールを変更するには、「スケジュール選択」欄からスケジュールを選択し、変更したい項目を編集し、[設定]をクリックします。



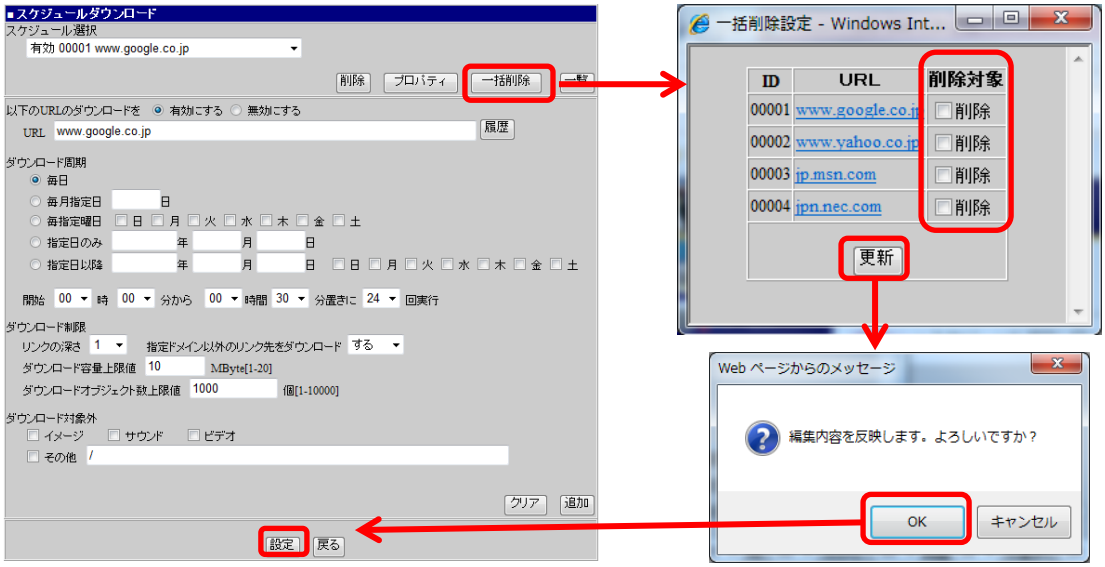
2.1.1.1.10.3. スケジュールの削除

スケジュールを削除するには、「スケジュール選択」欄からスケジュールを選択し、[削除]をクリックし、[設定]をクリックします。



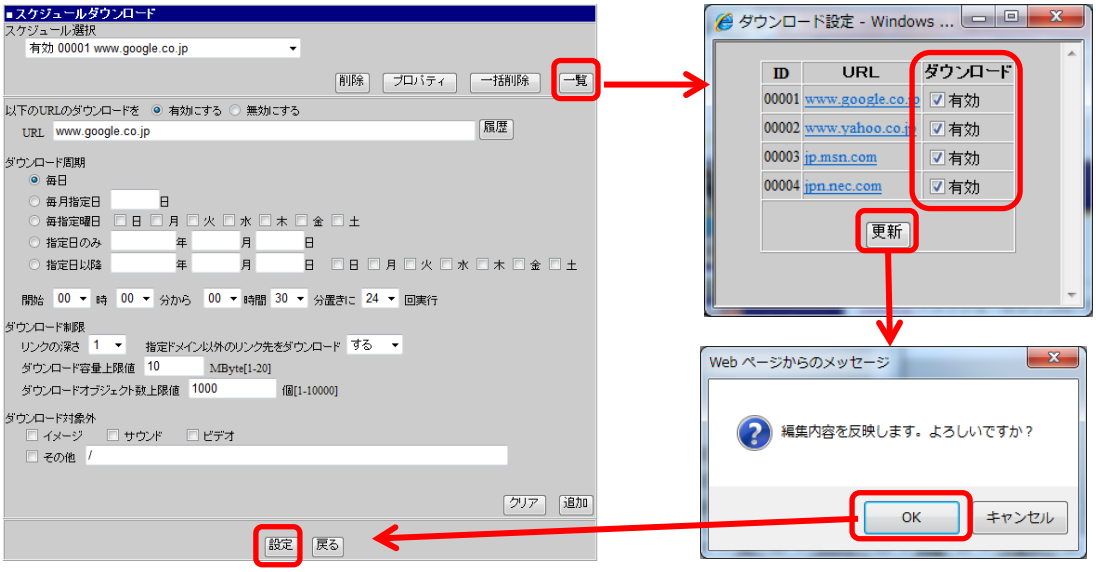
2.1.1.1.10.4. スケジュールの一括削除

[一括削除]をクリックすると、別ウィンドウで「一括削除設定」画面が開きます。「一括削除設定」画面で、削除したいスケジュールの「削除対象」をチェックし[更新]をクリックすると、確認ウィンドウが表示され、[OK]をクリックすると、「スケジュール選択」欄から削除されます。内容を確認し、問題なければ[設定]をクリックします。[設定]をクリックしなければ、変更内容は反映されませんのでご注意ください。



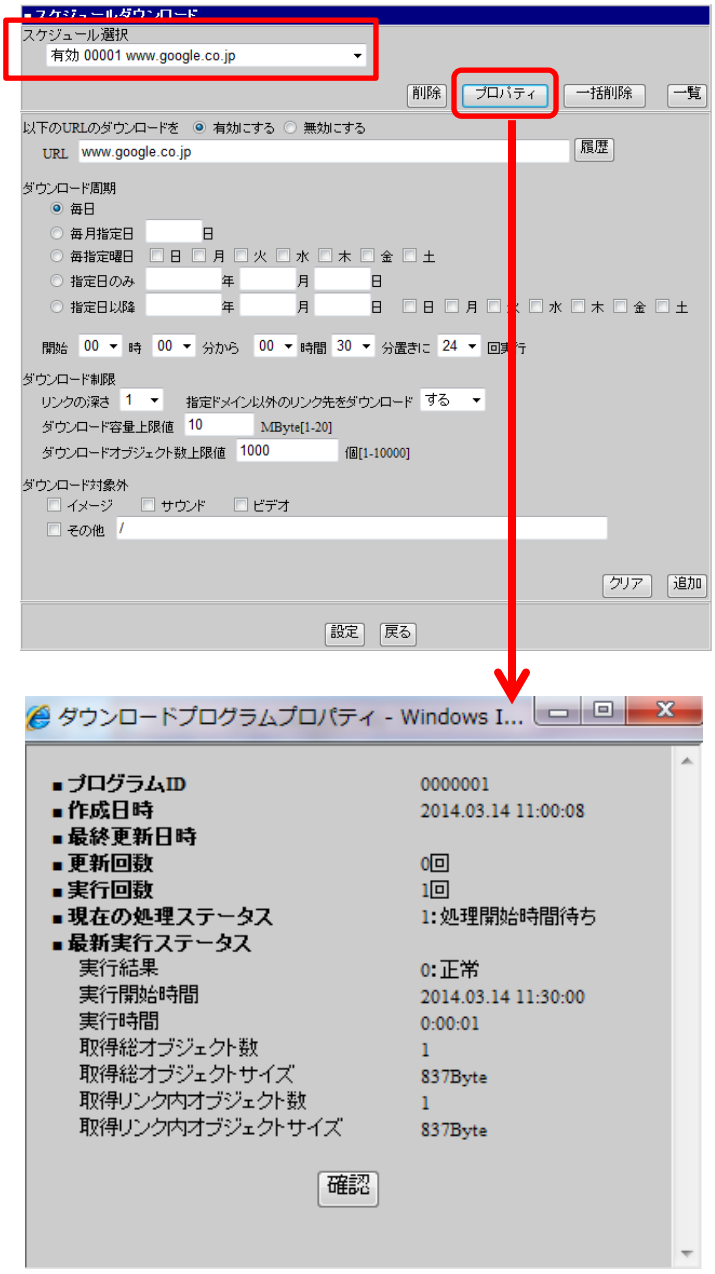
2.1.1.1.10.5. スケジュールの一括設定

[一覧]をクリックすると、別ウィンドウで「ダウンロード設定」画面が開きます。「ダウンロード設定」画面で、ダウンロードを実行したいスケジュールの「ダウンロード」をチェックし[更新]をクリックすると、確認ウィンドウが表示され、[OK]をクリックすると、「スケジュール選択」欄に反映されます。反映された内容を確認し、問題なければ[設定]をクリックします。[設定]をクリックしなければ、変更内容は反映されませんのでご注意ください。



2.1.1.1.10.6. スケジュールの確認

[プロパティ]をクリックすると、別ウィンドウにて選択したスケジュールの設定履歴や最新のダウンロード結果などを表示します。



2.1.1.1.11. 認証設定

「プロキシ」画面の「認証設定」で、サーバを使用するユーザを認証するための設定ができます。

2.1.1.1.12. NTLM 設定

NTLM(Windows NT LANManager)を利用して、クライアント情報のチェックと記録が行えます。

・ドメインコントローラとの連携無しで構築可能です。

・NTLM に非対応のクライアント AP については、許可・拒否・Ldap/Radius 認証を選択可能です。

・認証ユーザ名以外に、コンピュータ名、ドメイン名もログ出力可能です。

・InterSafe WebFilter/InterScan WebManager/i-FILTER(ICAP 版)との組み合わせで、ユーザ単位での設定やユーザ名のログ出力が可能です。

2.1.1.1.13. バイパス設定

「プロキシ」画面の「バイパス設定」では、システムを透過型プロキシとして動作させる際の、静的バイパス・動的バイパスの設定を行います。

2.1.1.1.14. 特殊アクセス制御設定

認証サービスをスキップさせる「認証スキップ設定」、URL フィルタリングソフトをスキップさせる「URL フィルタスキップ設定」、Keep-Alive 接続の方法について細かく指定する「Keep-Alive 設定」などの各種例外設定を行います。設定対象となるリストは、「アクセス制御設定」、「HTTP ヘッダ編集設定」、「対上位サーバ向けソース IP 設定」、「HTTPS 可視化アクセス制御設定」と共有します。

2.1.1.1.15. HTTP ヘッダ編集設定

HTTP ヘッダの扱いに関する設定を行います。

2.1.1.1.16. 対上位サーバ向けソース IP 設定

HTTP、HTTPS、FTP over HTTP アクセスに対して上位サーバへアクセスするソース IP の例外設定を行います。

2.1.1.1.17. SSL アクセラレータ設定(リバースプロキシ用)

リバースプロキシサーバで SSL アクセラレータ機能を使用する設定を行います。本機能は、オプション機能です。使用するためには、ライセンスをインストールしてください。

2.1.1.1.18. HTTPS 可視化設定(フォワードプロキシ用)

HTTPS 可視化機能に関する設定を行います。本機能は、オプション機能です。使用するためには、ライセンスをインストールしてください。

2.1.1.1.18.1. HTTPS 可視化機能設定

フォワードプロキシ(Forward,Forward(透過型Ｌ４スイッチ))で HTTPS 可視化機能を使用する設定を行います。

2.1.1.1.18.2. HTTPS 可視化アクセス制御設定

HTTPS 可視化機能の各機能について例外設定を行います。

2.1.1.1.18.3. HTTPS 可視化低負荷アクセス制御設定

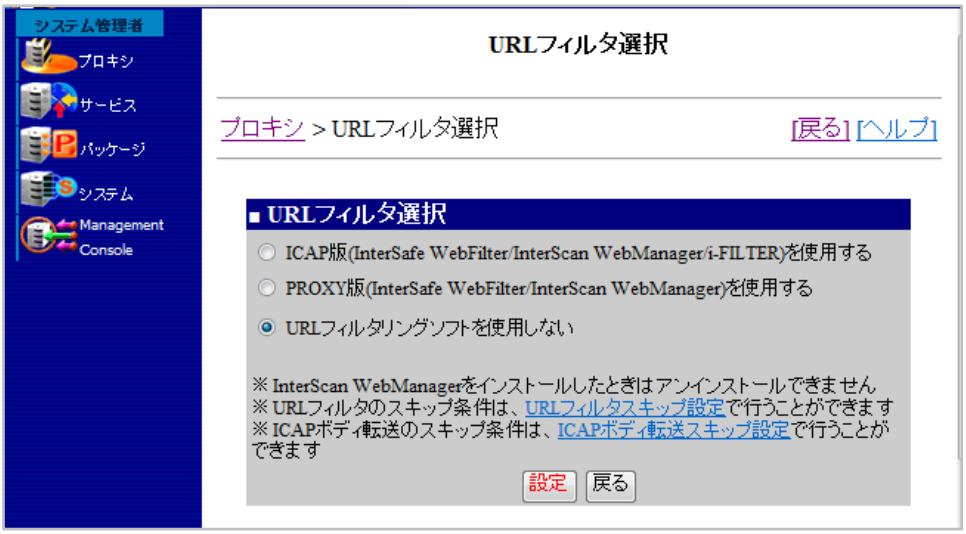
指定可能な条件を宛先 URL のホスト名部分のホスト名、ドメイン名に限定することで、大量に条件が存在する場合のアクセス制御の負荷を低減させます。

2.1.1.1.19. URL フィルタ用ログ領域設定

URL フィルタのログを保存する領域を指定できます。

2.1.1.1.20. URL フィルタ選択

「プロキシ」画面の「URL フィルタ選択」画面で、使用するフィルタリングソフトを選択することができます。



フィルタリングソフトは ICAP 版(InterSafe WebFilter/InterScan WebManager/i-FILTER)、または PROXY 版(InterSafe WebFilter/InterScan WebManager)を使用することができます。本システムには、ICAP 版(InterSafe WebFilter/i-FILTER)がプリインストールされておりますので、ICAP 版(InterSafe WebFilter/i-FILTER)は、InterSafe WebFIlter または i-FILTER のライセンス追加のみで、そのままご利用可能です。ICAP 版(InterScan WebManager)、PROXY 版(InterSafe WebFilter /InterScan WebManager)をご利用の際は、ICAP 版(InterSafe WebFilter)をアンインストールいただいた後、ご利用されるソフトのインストールとライセンスの追加が必要です。フィルタリングソフトの対応バージョンは、随時サポートサイトなどでご確認ください。ICAP 版使用時は、アクセスログへフィルタリングカテゴリ名およびフィルタリング結果を表示させることができます。

2.1.1.1.20.1. ログローテート設定

InterScan WebManager、InterSafe WebFilter、i-FILTER の各管理コンソールでログローテートの設定をする場合、その合計ファイルサイズに注意してください。なお、フィルタリングソフトのログ設定にて、ログの「自動削除」を有効にしていない場合、ディスクの空きがなくなる可能性がありますので、必ず設定を確認してください。

2.1.1.1.20.2. PROXY 版(InterSafe WebFilter/InterScan WebManager)設定

「プロキシ」画面の「フィルタ選択」画面の「URL フィルタ(PROXY 版)動作設定で、PROXY 版(InterSafe WebFilter/InterScan WebManager)の設定を行います。この設定は PROXY 版(InterSafe WebFilter /InterScan WebManager)を本システムで使用するときに必要ですので、必ず行ってください。IP アドレスとポート番号の指定は InterSafe WebFilter/InterScan WebManager で設定する内容に従って設定してください。なお、この画面で IP アドレスとポート番号を変更しても InterSafe WebFilter/InterScan WebManager には反映されません。

2.1.1.1.20.3. ICAP 版(InterSafe WebFilter/InterScan WebManager/i-FILTER)設定

「プロキシ」画面の「フィルタ選択」画面の「ICAP サーバ設定で、ICAP 版(InterSafe WebFilter/InterScan WebManager/i-FILTER)の設定を行います。この設定は ICAP 版(InterSafe WebFilter/InterScan WebManager/i-FILTER)を本システムで使用するときに必要ですので、必ず行ってください。 IP アドレスとポート番号などの指定は、「サービス」画面から InterSafe WebFilter/InterScan WebManager/i-FILTER 管理コンソールを起動し、表示する内容に従って設定してください。なお、本画面で IP アドレスとポート番号を変更しても InterSafe WebFilter/InterScan WebManager/i-FILTER 管理コンソールには反映されません。

2.1.1.1.20.4. InterSafe WebFilter/InterScan WebManager/i-FILTER インストール手順

本システムには、ICAP 版(InterSafeWebFiler/i-FILTER)がプリインストールされていますが、InterScan WebManager や PROXY 版を使用する際は、ICAP 版(InterSafe WebFilter/i-FILTER)をアンインストールした後、インストール作業を行います。手順の概要を示します。

なお、PROXY 版、ICAP 版もフィルタリングソフトのインストーラは共通です。

1) 「システム」画面の「保守用パスワード」で mainte ユーザのパスワードを設定する。
2) 「サービス」画面で「リモートログイン(telnetd)」を起動する。
3) 「サービス」画面の「リモートログイン(telnetd)」をクリックして「リモートログイン(telnetd)」画面へ遷移し、本システムにリモートログインできるように Telnet を許可するホストを設定する。
4) Telnet で mainte ユーザで本システムにリモートログインし、「su-」とコマンドラインに打ち込む。
5) パスワードを求められるので、ManagementConsole にログインするためのパスワード(admin のパスワード)を指定し、管理者ユーザになる。
6) InterSafe WebFilter/InterScan WebManager/i-FILTER のマニュアルに基づきインストールをする。
   インストール中にインストールディレクトリを聞かれた場合は、「/usr/local」を指定します。また、インストール中に、PROXY 版(スタンドアロン版)、ICAP 版のいずれかをインストールするか聞かれる場合がありますので、使用するモードを選択します。
7) インストール後、「プロキシ」画面の「URL フィルタ用ログ領域設定」画面の設定を確認し、インストールした URL フィルタ用のログ領域に関する設定がない場合は必ず設定を行う。
8) インストール後、「プロキシ」画面の「URL フィルタ選択」画面の設定を行う。
9) 「システム」画面にて[システムの再起動]を実行する。

2.1.1.2. サービス

管理者は、Management Console から以下のサービスの設定を行うことができます。

・i-FILTER
・InterSafe WebFilter
・actlog
・時刻調整(ntpd)
・ネットワーク管理エージェント(snmpd)
・リモートシェル(sshd)
・リモートログイン(telnetd)
・WPAD サーバ(wpad-httpd)

サービス画面では各機能の停止・起動を設定可能で、現在の稼動状況を表示します。さらにここから、各機能ごとの詳細な設定を行う画面に移ります。

2.1.1.2.1. i-FILTER

ICAP(Internet ContentAdaptationProtocol)による URL フィルタリングを行えます。(i-FILTER を ICAP サーバとして使用)。フィルタリングソフトウェアでのプロキシ動作が不要となるため、処理性能が向上します。

2.1.1.2.2. InterSafe WebFilter

ICAP(Internet ContentAdaptationProtocol)による URL フィルタリングを行えます。
(InterSafe を ICAP サーバとして使用)。フィルタリングソフトウェアでのプロキシ動作が不要となるため、処理性能が向上します。初めて利用する際は、右側の「InterSafe WebFilter」のリンクをクリックし、使用承諾契約書の内容をよく読んで[同意する]ボタンをクリックしてください。

2.1.1.2.3. 時刻調整(ntpd)

NTP(Network TimeProtocol)は、ネットワークで接続されたコンピュータ同士が連絡を取り合い、時計のずれを自動的に調整する仕組みです。本システムはこの仕組みを利用して、以下の機能を提供しています。

・他の PC が時計を本システムに合わせるのに必要な情報を提供する。
・インターネットの標準時刻サーバに、本システムの時計を合わせる。
・slew モードの有効/無効の設定

2.1.1.2.4. ネットワーク管理エージェト(snmpd)

SNMP(Simple Network ManagementProtocol)は、ネットワークに接続された機器の稼動状況を、ネットワークを通じて取得するための仕組みです。本システムは、ネットワークに接続された機器(エージェント)の側として、必要な情報をネットワークに発信する機能を提供しています。

2.1.1.2.5. リモートシェル(sshd)/リモートログイン(telnetd)

他のコンピュータ(ホスト)から本システムに接続(sshd は暗号化、telnetd は非暗号化)することを可能にする機能です。

Management Console では対応できない特別な操作を行いたい場合にだけこの機能を有効にします。通常の運用時に有効にする必要はありません。有効にしている間はセキュリティのレベルが低下しますので、通常は無効にしておくことをお勧めします。

「Telnet/SSH ログインを許可するホスト」画面にて、ログイン可能なホストを各種形式で指定します。カンマで区切って複数のホストを指定可能です。IP アドレスやホスト名以外にも各種指定形式をサポートしています。

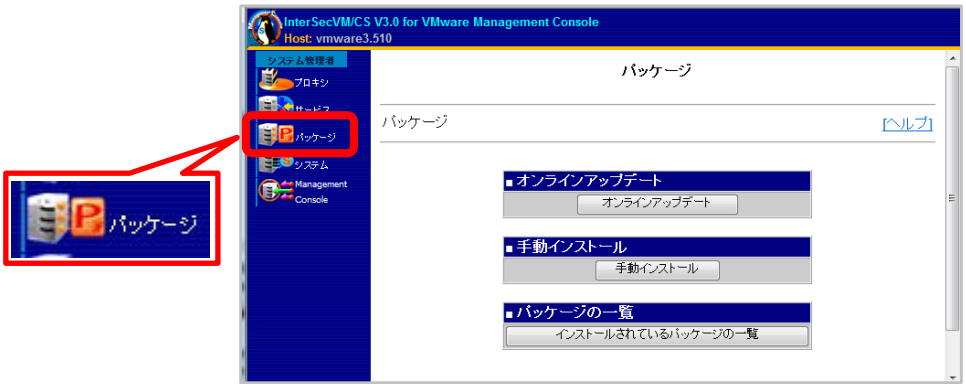
2.1.1.2.6. WPAD サーバ(wpad-httpd)

本システムをフォワードプロキシとして利用している際に、ブラウザ側でのプロキシ設定を自動化するための機能です。Internet Explorer6 以降で対応しています。本機能を利用するためには、ブラウザの参照している DNS サーバおよび DHCP サーバを適切に設定する必要があります。

「プロキシサーバ自動設定ファイル」画面で本システムに接続する際に使用するホスト名とポート番号を設定します。本システムを通さないで接続すべきマシンがあれば、ネットワークアドレス単位で指定することが可能です。

2.1.1.3. パッケージ

本システムにインストールされているアプリケーションなどのソフトウェアパッケージのアップデートやインストール、インストールされているパッケージの一覧を確認する画面です。



2.1.1.3.1. オンラインアップデート

オンラインアップデートを利用すると、Management Console から簡単にアップデートモジュールをインストールすることができます。アップデートモジュールとは、本システムに追加インストール(アップデート)可能なソフトウェアで、弊社で基本的な動作確認を行って公開しているものです。内容は、既存ソフトウェアの出荷後に発見された不具合修正や機能追加などが主ですが、新規ソフトウェアが存在することもあります。オンラインアップデートでは、現在公開されている本システム向けのアップデートモジュールの一覧を参照し、安全にモジュールをインストールすることができます。

2.1.1.3.2. 手動インストール

ローカルディレクトリのファイル名、または URL、PROXY、PORT を指定して RPM パッケージをインストールすることができます。

2.1.1.3.3. パッケージの一覧

現在本システムにインストールされている RPM パッケージの一覧を確認することができます。また、アンインストール作業を行うこともできます。

2.1.1.4. システム

Management Console 画面左の「システム」アイコンをクリックすると「システム」画面が表示されます。

2.1.1.4.1. システムの停止

[システムの停止]をクリックするとシステムを停止します。

2.1.1.4.2. システムの再起動

[システムの再起動」をクリックするとシステムを再起動します。

2.1.1.4.3. CPU／メモリ使用状況

メモリの使用状況と CPU の使用状況をグラフと数値で表示します。約 10 秒ごとに最新の情報に表示が更新されます。また、CPU 使用率と負荷、ネットワークについて、調節を行うことができます(上級者向け)。設定を変更する場合は、環境や使用状況にあわせて適切な値を設定してください。

2.1.1.4.4. ディスク使用状況

ディスクの使用状況を各ファイルシステムごとに数値とグラフで表示します。空き容量、使用率に注意してください。空き容量が足りなくなるとシステムが正常に動作しなくなる可能性があります。

2.1.1.4.5. プロセス実行状況

現在実行中のプロセスの一覧を表示します。プロセス実行状況の表の最上行の項目名をクリックすると、各項目で表示をソートすることができます。

2.1.1.4.6. 名前解決診断

ネットワーク設定で登録されている DNS サーバの動作を確認することができます。

「ホスト:」に適当なホスト名を入力して[診断]をクリックすると診断結果が表示されます。ホスト名に対して正しく「Name:」と「Address:」が表示されれば DNS サーバは正常に機能しています。

2.1.1.4.7. ネットワーク利用状況

ネットワーク利用状況を表示します。

「約 5 秒毎に画面をリフレッシュする」チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

2.1.1.4.8. ネットワーク接続状況

各ポートごとの接続状況を表示します。

「約 5 秒毎に画面をリフレッシュする」チェックボックスをチェックすると自動的に表示が最新状況に更新されます。

2.1.1.4.9. プロキシアクセス統計

アクセスの統計情報を表示します。

[プロキシアクセス動作設定]では、プロキシアクセス統計を有効にして動作させるかどうか設定します。動作させる際には優先度を設定してください。優先度は 1 から 19 まで設定可能であり、値が大きいほど優先度が低くなります。優先度を低くすることによりプロキシアクセス統計の動作による CPU の負荷を減らすことができます。

[プロキシアクセス統計表示」では、２世代（現在の情報、１世代前の情報）のうち、どちらかを選択し[表示]をクリックすると統計表示画面「Usage Statistics for ホスト名」が表示されます。

その画面中の表「Summary by Month」の「Month」の項目のリンクをクリックするとその月の詳細な統計情報を表示します。

[Webalizer 表示設定]では、sites はサイト別上位を、sites By KBytes はサイト別キロバイト上位を、URL's は URL 上位を、URL' s By KBytes はサイト別キロバイト上位を Entry Pages は入り口上位を、Exit Pages は出口別上位をいくつまで表示するか設定することができます。

2.1.1.4.10. 経路情報

「相手ホスト:」にホスト名を入力して[表示]をクリックすると、そのホストまでの経路情報を表示します。

2.1.1.4.11. システム情報

装置に割り当てたホスト名、および OS に関する情報を表示します。

2.1.1.4.12. AFT/ALB モード設定

AFT（Adapter FaultTolerance）/ALB（Adaptive LoadBalancing）モードの設定を行います。

2.1.1.4.13. ネットワーク

ネットワークの基本的な設定やネットワークインタフェース、ルーティングの設定を行います。

2.1.1.4.14. バックアップ/リストア

ファイルのバックアップおよびリストアの設定を行います。

「2.2. 再セットアップ」を参照してください。

2.1.1.4.15. 管理者パスワード

管理者名(admin)や管理者のパスワード、管理者宛のメール転送先を変更します。

管理者名は半角英小文字で始まる 1 文字以上 16 文字以下の半角英小文字数字、“_”、“-”で指定してください。各パスワードは 6 文字以上 14 文字以下の半角英数文字(半角記号を含む)を指定してください。省略すると、パスワードは変更されません。空のパスワードを指定することはできません。また、管理者宛のメールを転送する先を設定できます。管理者宛メールの転送先は正しく送信できるアドレスを指定してください。

2.1.1.4.16. アクセスログ取得(自動転送)

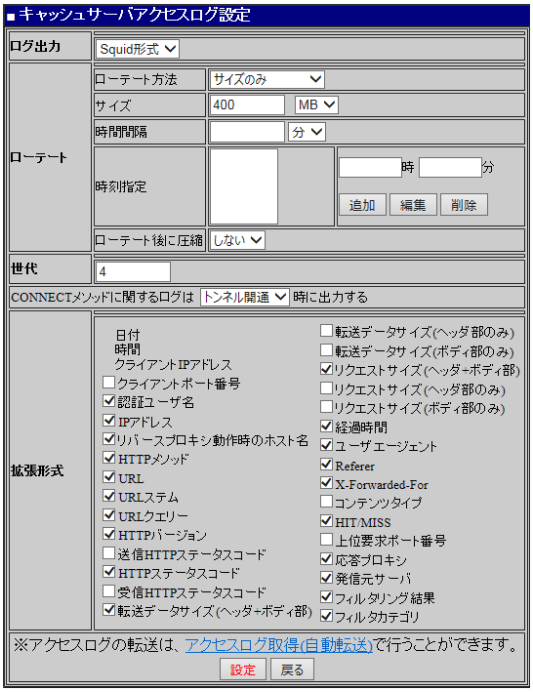
キャッシュサーバアクセスログを Samba または FTP で指定したホストを利用して転送します。

2.1.1.4.17. ログ管理

ログの表示、ログのローテートの設定を行います。ログの表示は表示したいログの[表示]をクリックするとローテートされたログの一覧が表示され、その中から表示したいログを選択して表示します。ログのローテートの設定は、ローテートを行うタイミングを周期またはファイルサイズで指定し、何世代までログを残すかを設定します。

2.1.1.4.17.1. キャッシュサーバアクセスログ

キャッシュサーバアクセスログの[設定]をクリックすると、「キャッシュサーバアクセスログ設定」画面が表示されます。この画面は、キャッシュサーバアクセスログの出力形式、ローテート(条件、サイズ、時間、時刻)、何世代までログを残すかなどを設定することができます。出力形式が拡張形式であったとき、拡張形式でチェックボックスにチェックを入れた項目がログ出力されます。



2.1.1.4.18. 保守用パスワード

保守用ユーザ(mainte)のパスワードを設定します。

設定を行ったあと、「mainte」ユーザでリモートログイン(telnet)サービス、リモートシェル(sshd)サービスを利用することができます。

2.1.1.4.19. キャッシュデータ削除

キャッシュされている全てのデータの削除を行います。

キャッシュされているデータを削除する際にプロキシサービスの再起動を実行します。

2.1.1.4.20. プロキシサーバ状態表示

本システムに関する様々な情報を表示させ、確認することができます。

情報種別	説明
一般情報	バージョン情報や運用時間等を表示します。
キャッシュ概要	現在の動作状況等を表示します。
キャッシュ情報	一定時間あたりの本システムへの接続数や、リクエスト数等を表示します。
クライアント要求	起動開始から現時点までに処理したさまざまな情報を表示します。
ICP 情報	隣接キャッシュサーバに関連する情報を表示します。
CERN 情報	親プロキシサーバに関連する情報を表示します。
FTP 情報	HTTP 経由での FTP プロトコルに関連する情報を表示します。 なお、以下の情報を表示しており、親プロキシ経由でリクエストを処理したリクエストについてはカウントの対象となりません。 ・FTP サーバと直接通信を行ったリクエストに関する情報 ・キャッシュから応答を返却したリクエストに関する情報

2.1.1.4.21. システム冗長化設定

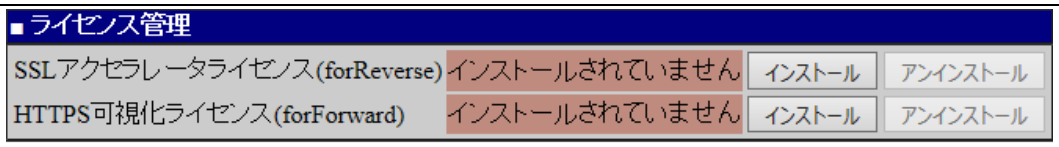
システム冗長化のシステム運用状況の表示、および各種情報設定を行います。主な設定項目は以下の通りです。

設定項目	説明
システム冗長化	システム冗長化する/しないを指定します。
本サーバ種別	システム冗長化する場合、本サーバ運用方法について稼動系/待機系を指定します。
相手サーバ実 IP アドレス	システム冗長化する場合、サーバ種別で稼働系を指定した場合は待機系の、待機系を指定した場合は稼動系の実 IP アドレスを指定します。
監視用ポート番号	システム冗長化する場合、稼動系～待機系間の死活監視用通信ポート番号を指定します。
監視間隔	システム冗長化する場合、稼動系～待機系間の死活監視間隔を指定します。
監視回数	システム冗長化する場合、稼動系～待機系間のフェイルオーバーを開始するまでの試行回数を指定します。

2.1.1.4.22. ライセンス管理

ライセンス製品のインストール/アンインストールを管理します。対象製品は以下の通りです。

- SSL アクセラレータライセンス(forReverse)
- HTTPS 可視化ライセンス(forForward)



2.1.1.4.23. 情報採取

障害調査などに必要な下記情報を採取することができます。

情報種別	説明
設定、状態管理情報	プロキシサーバの設定および状態管理情報を採取します。
システムログ情報	システムログ、ipmi のログ情報を採取します。
プロキシサービスログ情報	プロキシサービスのログ情報を採取します。
アクセスログ情報	キャッシュサーバアクセスログの情報を採取します。
actlog 情報	リソースの詳細情報を採取します。
sar 情報	sar の情報を採取します。
Management Console ログ情報	Management Console のログ情報を採取します。
URL フィルタ用ログ領域(移行済み)情報	URL フィルタ用ログ領域(移行済み)の情報を採取します。
パケットキャプチャデータ情報	パケットキャプチャデータ情報を採取します。
その他の情報	cron 等のログ情報を採取します。
ディレクトリ指定	採取するディレクトリを指定します。

2.1.1.4.24. シリアルポート設定

シリアルコンソールに接続をするシリアルポートの設定を行います。

シリアル接続の UPS を利用する場合は、シリアルポートの設定を行います。

2.1.1.4.25. パケットキャプチャ

tcpdump コマンドを使用して障害調査に必要なパケットキャプチャを採取します。

2.1.2. ESMPRO のセットアップ

2.1.2.1. ESMPRO/ServerAgentService のセットアップ

ESMPRO/ServerAgentService はシステムのセットアップ時にインストールされますが、ESMPRO の管理に必要な設定はされていません。各種ドキュメントを参照し、設定してください。

重要

ESMPRO/ServerAgentService(Linux)に関するドキュメント類の最新版は以下の URL に掲載されています。システム構築前に最新版を確認して取り寄せてください。

- ユーザーズガイド
- パラメータシート
- 必須パッケージ一覧
- アラート一覧
- プロセス情報
- 内部ログ情報

http://jpn.nec.com/esmsm/download.html?#sas_lin

[ダウンロード]より該当バージョンの ESMPRO/ServerAgentService(Linux)

ヒント

ESMPRO／ServerAgentService の他にも「エクスプレス通報サービス」がインストールされます。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

重要

シリアル接続の管理 PC から設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
# export LANG=C
```

2.1.2.2. ESMPRO/ServerManager のセットアップ

本装置をネットワーク上のコンピュータから管理・監視するためのアプリケーションとして、「ESMPRO/ServerManager」と「ESMPRO/ServerAgent Extension」が用意されています。
これらのアプリケーションを管理 PC にインストールすることによりシステムの管理が容易になるだけでなく、システム全体の信頼性を向上することができます。
ESMPRO/ServerManager と ESMPRO/ServerAgent Extension のインストールについては、ハードウェアに添付されているユーザーズガイドを参照してください。

2.1.3. オンラインアップデートの実行

オンラインアップデートは、システムソフトウェアを最新の状態に維持して、最高の機能・性能を発揮できるようにするために必要な手続きです。セットアップ後、および、再セットアップ後に必ず実行してください。

詳細は、「3.4. パッケージ」を参照してください。

2.2. 再セットアップ

2.2.1. システムの再インストール

再セットアップとは、システム異常などの原因でシステムが起動できなくなった場合などに、添付の「インストールディスク」を使って初期状態に戻してシステムを復旧するものです。
再セットアップ手順については、添付の「セットアップ手順説明書」に従い実施してください。

また、システムの故障、設定の誤った変更など思わぬトラブルからスムーズに復旧するために、定期的にシステムのファイルの「バックアップ」をとっておくことを強く推奨します。「バックアップ」しておいたファイルを「リストア」することによってバックアップを作成した時点の状態へシステムを復元することができます。

重要

再インストールを行うと、製品内の全データが消去され、出荷時の状態に戻ります。必要なデータが製品内に残っている場合は、データのバックアップを行ってから再インストールを実行してください。

重要

・アップデートが適用されている状態でバックアップを取得し、再セットアップ後にリストアを行うことでバックアップ時の設定に戻す処理を行う場合は、リストアを行った後、バックアップ時のアップデートか最新のアップデートを適用してください。バックアップ時のアップデートか最新のアップデートを適用するまで、システムの再起動は行わないでください。
・リストアは、バックアップ時と同一構成の装置に対して行う必要があります。

2.2.2. ESMPRO/ServerAgentService の再セットアップ

「システムの再インストール」で ESMPRO/ServerAgentService は自動的にインストールされますが、固有の設定がされていません。ESMPRO/ServerAgentService のドキュメントを参照し、セットアップをしてください。

ESMPRO／ServerAgent の他にも「エクスプレス通報サービス」がインストールされます。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

シリアル接続の管理 PC から設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
# export LANG=C
```

2.2.3. バックアップ

本製品では、システム内のファイルを以下の 5 つのグループに分類して、その各グループごとにファイルのバックアップのとり方を制御することができます。それぞれのグループのバックアップ対象ディレクトリおよび作成されるファイルの名称は「3.5.17. バックアップ/リストア」を参照してください。初期状態では、いずれのグループも「バックアップしない」設定になっています。お客様の環境にあわせて各グループのファイルのバックアップを設定してください。本製品では各グループに対して「ローカルディスク」「Samba」「FTP」の３種類のバックアップ方法を指定することができます。各方法には、それぞれ以下のような特徴があります。

バックアップ方法	特徴
ローカルディスク	ハードディスクの別の場所にバックアップをとります。 内蔵ハードディスクがクラッシュした場合、復元できませんのでご注意ください。
Samba、FTP	LAN に接続されている Windows マシンおよび FTP サーバのディスクにバックアップをとります。 内蔵ハードディスクがクラッシュしても復元を行うことができますが、あらかじめ、Windows マシンや FTP サーバに共有の設定をしておく必要があります。

バックアップ情報は、ローカルディスクに作成しないでください。再インストールを行うと、システム内の全データが消去され、バックアップ情報を使用することができません。

次ページより、Samba によるバックアップ設定手順について説明します。

2.2.3.1. Samba によるバックアップ設定手順

「Samba」を使用したバックアップの方法について説明します。

例として「workgroup」内に所属するマシン名「winpc」という Windows マシンの「C:ドライブ」にバックアップのためのフォルダ「cachebackup」を作成して「システムの設定ファイル」グループのファイルのバックアップを行う場合の操作手順を説明します。

バックアップファイルを置くマシン(winpc)でのバックアップ作業のためのユーザを「winpc」上にあらかじめ用意してください。

バックアップファイルの中にはシステムのセキュリティに関する情報などが含まれるため、バックアップのためのフォルダ(cachebackup)の読み取り、変更の権限などのセキュリティの設定には十分注意してください。(WindowsMe／98／95 ではセキュリティの設定ができません。そのためお客様の情報が第三者に盗まれる可能性があります。)

バックアップ作業のためのユーザは既存のユーザでもかまいませんが、以下の説明では「cacheadmin」というユーザをあらかじめ用意したという前提で説明します

次の順序で設定します。以降、順に設定例を説明していきます。

1) Windows マシンの共有フォルダの作成
2) システムのバックアップファイルグループの設定
3) バックアップの実行

バックアップ用に作成した共有フォルダの設定を不用意に変更するとシステムのバックアップおよび復元の機能が正常に動作しなくなるので注意してください。

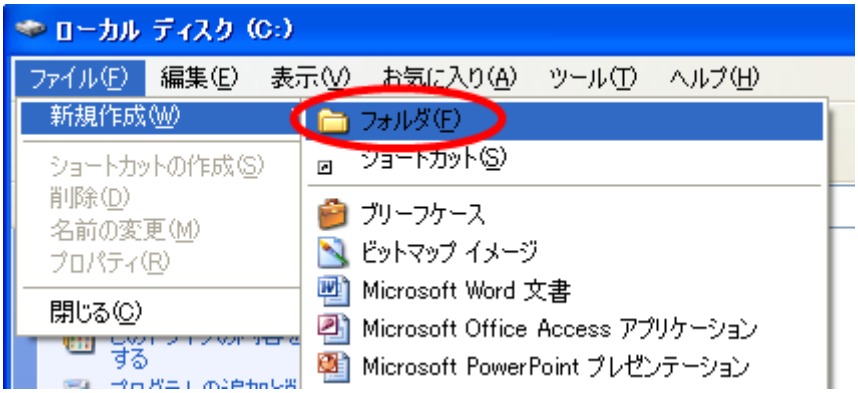
1) Windows マシンの共有フォルダの作成

まず、バックアップファイルを置いておくための共有フォルダを Windows マシンに作成します。ここでは、例として WindowsXP での作成方法を説明します。

・マシン「winpc」の「マイコンピュータ」画面を開く。

・開いた「マイコンピュータ」ウィンドウの「C：ドライブ」のアイコンをダブルクリックする。

・「ファイル」メニューの「新規作成」→「フォルダ」をクリックする。

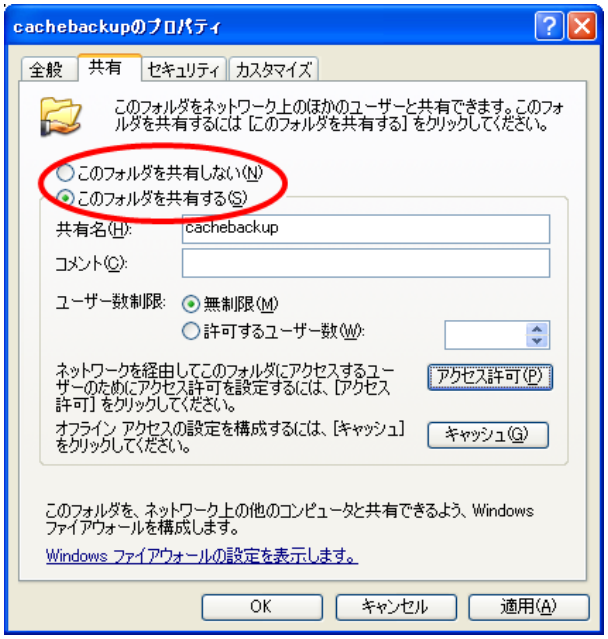


・「新しいフォルダ」の名前に「cachebackup」とキーボードから入力し<Enter>キーを押す。

・上記の手順で作成した「cachebackup」フォルダをクリックして選択する。

・「ファイル」メニューの「共有とセキュリティ」をクリックする。

「cachebackup のプロパティ」ウィンドウの「共有」シートが表示されます。



・「ネットワーク上での共有とセキュリティ」メニューで、「ネットワーク上でこのフォルダを共有する」のチェックボックスと「ネットワークユーザによるファイルの変更を許可する」にチェックをつける。
・[OK]をクリックして「cachebackup のプロパティ」のウィンドウを閉じる。
・「cachebackup」フォルダのアイコンが変わったことを確認する。

以上で共有フォルダの設定は完了です。

2) システムのバックアップファイルグループの設定

ここでは例として「システムの設定ファイル」グループのバックアップの設定手順を説明します。(他のグループも操作方法は同じです)

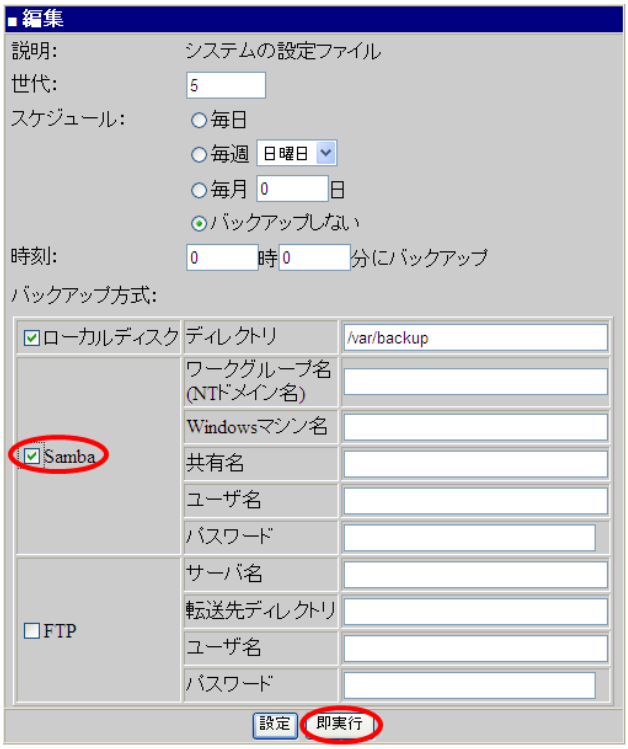
重要

システムの設定ファイル、およびプロキシサーバの設定ファイルは必ずバックアップを設定してください。

・Management Console 画面左の「システム」アイコンをクリックする。「システム」画面が表示されます。

・「システム」画面の「その他」一覧の[バックアップ/リストア]を押下する。「バックアップ/リストアー覧」画面が表示されます。

・一覧の「システムの設定ファイル」の左側の[編集]を押下する。バックアップ設定の「編集」画面が表示されます。



・「編集」画面のバックアップ方式の「Samba」をクリックして選択する。

・「Windows マシンの共有フォルダの作成」で行った設定に従って以下の項目を入力する。

項目	設定値
ワークグループ(NT ドメイン名)	Workgroup
Windows マシン名	Winpc
共有名	Cachebackup
ユーザ名	Cacheadmin
パスワード	ユーザ cacheadmin のパスワード

・正しく設定されていることを確認するため[即実行]を押下してバックアップを実行する。

・バックアップの確認ダイアログが表示されるので[OK]を押下する。

重要

Samba で転送する場合「共有名」配下にデフォルトゲートウェイに接続するインタフェースの実 IP アドレスの名前でフォルダを作成し、その配下にバックアップファイルを転送します。

定期的に自動的にバックアップを行うには次の設定を続けて行ってください。

・「編集」画面で「世代」、「スケジュール」、「時刻」を指定し、[設定]を押下する。

以上で、システムのバックアップファイルグループの設定は完了です。

重要

バックアップの処理は「システムのバックアップファイルグループの設定」で指定した日時に本製品とバックアップ先のマシンが起動していない場合は、バックアップされませんので注意してください。

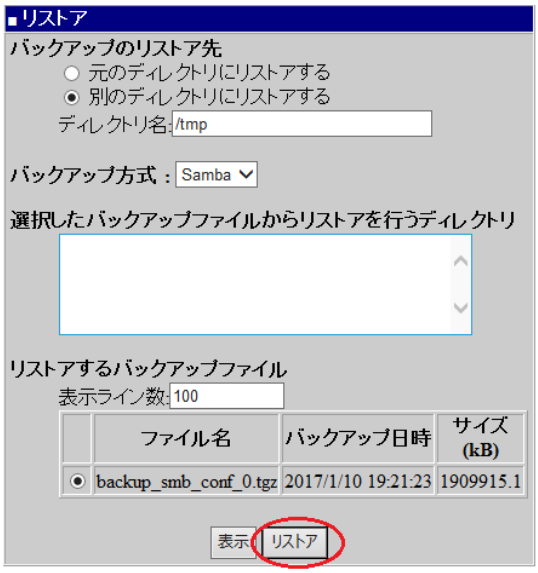
2.2.4. リストア手順

バックアップファイルは各バックアップファイルグループ毎にシステムにリストアすることができます。

ここでは例として、「2.2.3.1. Samba によるバックアップ設定手順」で設定を行った「システム設定のファイル」グループのファイルのバックアップファイルをシステムにリストアする際の操作手順の例を説明します。

1) Management Console 画面左の「システム」アイコンをクリックする。
2) 「システム」画面が表示されますので、「その他」一覧の[バックアップ/リストア]を押下する。
3) 「バックアップ/リストア一覧」画面が表示されますので、一覧の「システムの設定ファイル」の左側の[リストア]を押下する。

「リストア」画面が表示されます。



4) 「リストア」画面で「バックアップのリストア先」、「バックアップ方式」、「リストアするバックアップファイル」を指定し、[リストア]を押下する。
   通常は、デフォルトで最も新しいバックアップファイルが選択されています。そのまま実行すれば、最新のバックアップファイルがリストアされます。
5) 「リストアします。よろしいですか？」というダイアログボックスが表示されます。リストアする

場合は[OK]を押下します。

リストア結果が表示されれば、リストアは完了です。

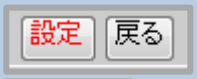
3章 Management Console

3.1. Management Console とは

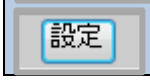
ネットワーク上のクライアントマシンから Web ブラウザを介して InterSec/CS のさまざまな設定の変更や状態の確認ができます。
この Web ベースの運用管理ツールのことを「Management Console」と呼びます。

重要

各画面にて項目の情報を入力後[設定]ボタンを押下することで、入力した情報の設定（書き込み）と反映を行います。



設定ボタンが赤字の場合、押下時にプロキシサービスの再起動をおこないます。



[設定]ボタンが黒字の場合は、プロキシサービスの再起動は行いません。

3.1.1. 利用者の権限

本製品の管理者は「システム管理者」と呼ばれ、さまざまな管理権限を持ちます。

システム管理者のユーザ名はデフォルトでは「admin」です。

3.1.2. 動作環境

Management Console は、以下のブラウザ環境での動作を確認しています。下記以外の Web ブラウザを利用した場合は、画面表示が乱れたり、予期せぬ動作をする場合があります。

- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 11

必ずブラウザの設定にて JavaScript を有効化したうえでご利用ください。

本製品は SSL3.0 で通信をおこなうことはできません。TLS1.0 以降をご利用ください。

Web ブラウザは、以下の OS 環境での動作を確認しています。

- Microsoft® Windows® 7
- Microsoft® Windows® 8

3.1.3. セキュリティモード

Management Console では日常的な運用管理のセキュリティを確保するため、2 つのセキュリティモードをサポートしています。

- **レベル 1(パスワード)**
  パスワード認証による利用者チェックを行います。ただし、パスワードや設定情報は暗号化せずに送受信します。
- **レベル 2(パスワード ＋SSL)**
  パスワード認証に加えて、パスワードや設定情報を SSL で暗号化して送受信します。自己署名証明書を用いていますので、ブラウザでアクセスする際に警告ダイアログボックスが表示されますが、[はい]などをクリックしてください。

デフォルトの設定では、「レベル 2」となっています。セキュリティレベルを変更する場合は、「3.6. Management Console」の「セキュリティモード」を変更してください。また、同画面で操作可能ホストを設定することにより、さらに高いレベルのセキュリティを保つことができます。

3.1.4. Management Console へのアクセス

Management Console へのアクセス手順は、セキュリティモードによって異なっています。クライアント側の Web ブラウザを起動し、下記の URL にアクセスしてください。

セキュリティモード	URL
レベル 2	https://<アドレス>:50453/
レベル 1	http://<アドレス>:50090/

※<アドレス>の部分には、InterSec/CS に割り当てた IP アドレスまたは FQDN を指定してください。

- Management Console へのアクセスには、プロキシを経由させないでください。
- Management Console へアクセスする場合にはブラウザのキャッシュ機能を使用しないようにしてください。
- 「3.1.2. 動作環境」に記述の環境で Management Console をご利用ください。

3.1.5. 初期ログイン

システムセットアップ後、初めて Management Console へログインする場合の手順を説明します。

1) 管理クライアントの Web ブラウザから以下の URL に接続します

https：//本システムに割り当てた FQDN：50453/

もしくは

https：//本システムに割り当てた IP アドレス：50453/

セキュリティモードの初期設定はレベル 2 となっていますので、「3.1.4. Management Console へのアクセス」のレベル 2 の URL にアクセスします。

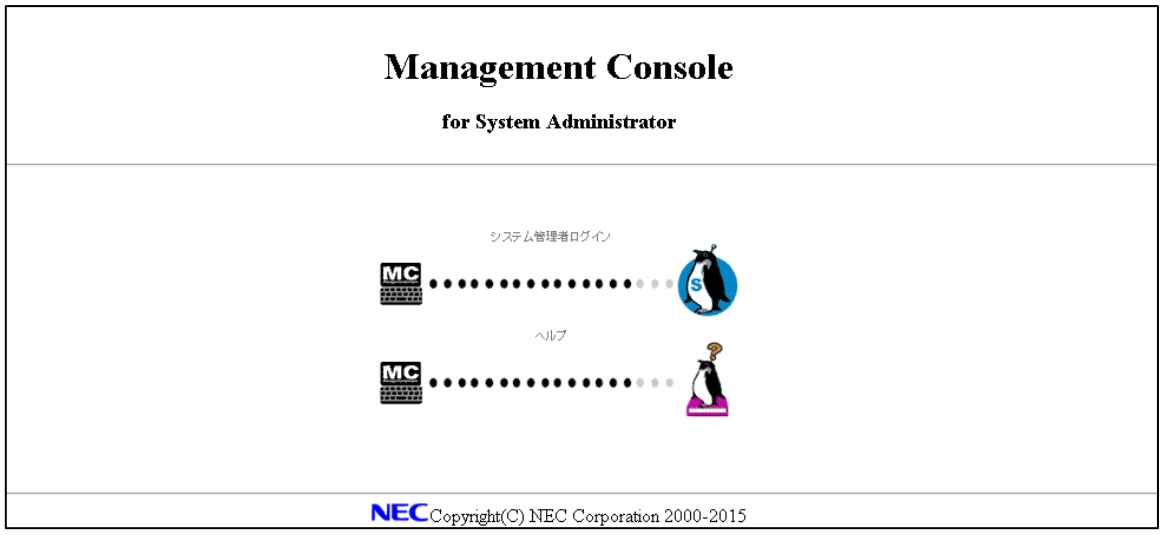
管理コンソールにログインする Management Console の URL にアクセスすると「セキュリティの警告」画面が表示されます。

例) Internet Explorer 8.0 の場合は、[このサイトの閲覧を続行する(推奨されません)]をクリックしてください。

Internet Explorer 8.0 の場合

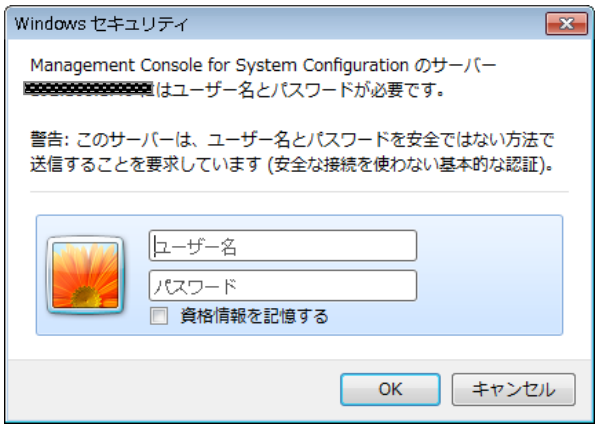
InterSec/CS では、暗号化を目的に、SSL を利用しているため、証明書は独自に生成しています。ログインにおいて警告が表示されますが、セキュリティにおいて問題はありません。

2) 管理コンソールのログイン画面が表示されます。“システム管理者ログイン” をクリックしてください。



ユーザ名にシステム管理者名、パスワードには、管理者パスワードを入力してください。システム管理者用のトップページが表示されます。初期値は以下です。

ユーザ名：admin パスワード：初期導入時に設定したパスワード



3) 管理者用のトップページが表示されます。 Web ブラウザに表示された画面から各種システムの設定ができます。

Management Console 管理者用トップページ

管理対象のホスト名が表示されます

ヒント

初回ログイン時は管理対象のホスト名部分は空白になっています。
ブラウザのリロード（最新の情報に更新など）をすれば、ホスト名が表示されます。

次ページより、Management Console の各画面の設定項目などについて説明します。

3.2. プロキシ

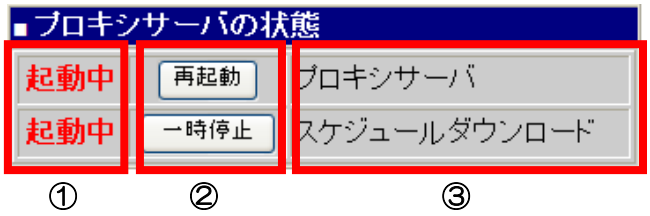
プロキシサービスの設定を行います。

プロキシは以下の画面に分かれています。

■プロキシサーバの状態
■プロキシサーバの設定
■HTTPS 可視化設定(フォワードプロキシ用)
■URL フィルタ設定

プロキシサーバの状態

プロキシサーバの状態を表示します。



◆ ①(状態表示)

プロキシサーバおよびスケジュールダウンロードのサービスの起動状態を表示します。起動状態を下記から表示します。

表示
起動中
停止中

◆ ②(操作)

✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

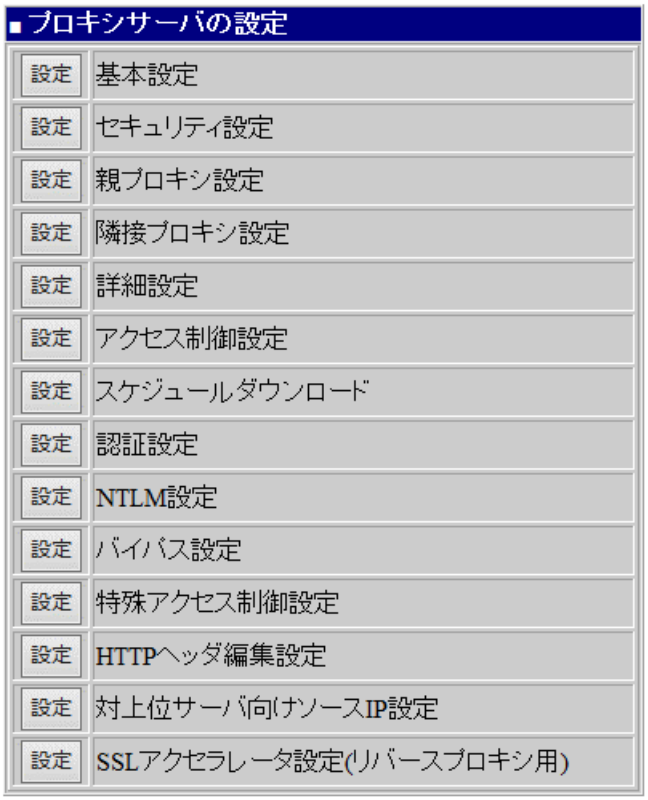
[再起動/起動]	[再起動]を押下することでプロキシサーバの再起動を、[起動] を押下することでプロキシサーバの起動を行います。
[一時停止/起動]	[一時停止]を押下することでスケジュールダウンロードの一時停止を、[起動]を押下することでスケジュールダウンロードの起動を行います。

◆ ③(サービス名の表示)

対象のサービスを列挙します。

プロキシサーバおよびスケジュールダウンロードを表示します。

プロキシサーバの設定

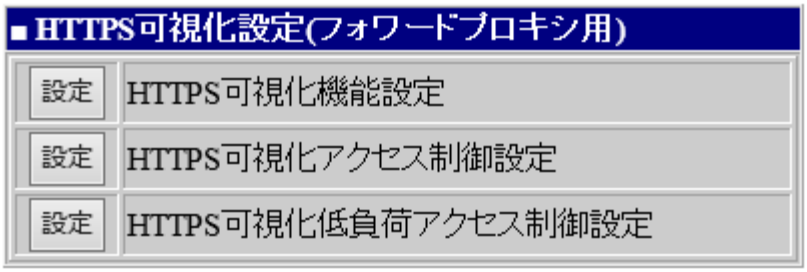


✓ ボタンの説明

[設定]	各機能の設定画面へ遷移します。 ・基本設定 →「3.2.1. 基本設定」 ・セキュリティ設定 →「3.2.2. セキュリティ設定」 ・親プロキシ設定 →「3.2.3. 親プロキシ設定」 ・隣接ロキシ設定 →「3.2.4. 隣接プロキシ設定」 ・詳細設定 →「3.2.5. 詳細設定」 ・アクセス制御設定 →「3.2.6. アクセス制御」 ・スケジュールダウンロード →「3.2.7. スケジュールダウンロード」 ・認証設定 →「3.2.8. 認証設定」 ・NTLM 設定 →「3.2.9. NTLM 設定」 ・バイパス設定 →「3.2.10. バイパス設定」 ・特殊アクセス制御設定 →「3.2.11. 特殊アクセス制御」 ・HTTP ヘッダ編集設定 →「3.2.12. HTTP ヘッダ編集設定」 ・対上位サーバ向けソース IP 設定 →「3.2.13. 対上位サーバ向けソース IP 設定」 ・SSL アクセラレータ設定(リバースプロキシ用) →「3.2.14. SSL アクセラレータ設定(リバースプロキシ用)」

HTTPS 可視化設定(フォワードプロキシ用)

HTTPS 通信の可視化設定をフォワードプロキシの各機能にて行うことができます。



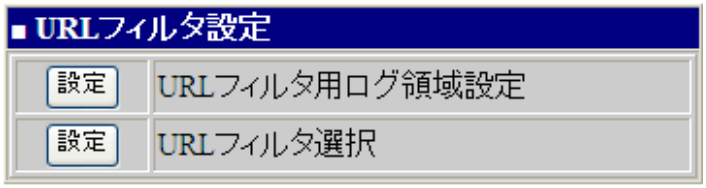
✓ ボタンの説明

[設定]	各機能の設定画面へ遷移します。	
	HTTPS 可視化機能設定	→「3.2.15. HTTPS 可視化機能設定」
	HTTPS 可視化アクセス制御設定	→「3.2.16. HTTPS 可視化アクセス制御設定」
	HTTPS 可視化低負荷アクセス制御設定	→「3.2.17. HTTPS 可視化低負荷アクセス制御設定」

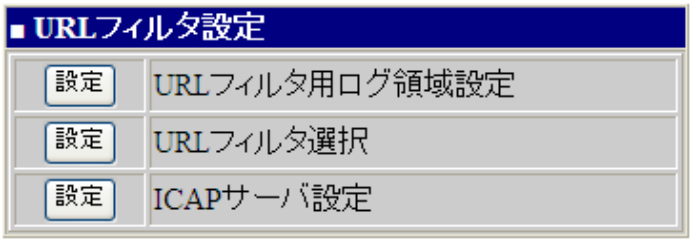
URL フィルタ設定

URL フィルタ設定画面は「3.2.19. URL フィルタ選択」にて、「ICAP 版」、「PROXY 版」、「URL フィルタリングを使用しない」のどれを選択したかで表示が変わり、それぞれの設定を行うことができます。

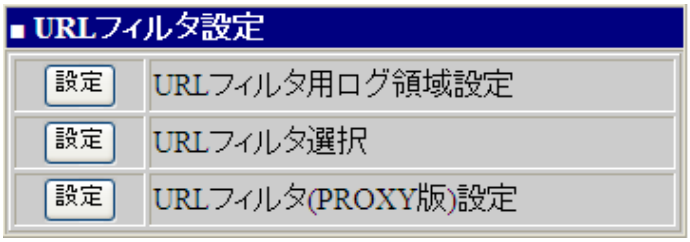
【URL フィルタリングを使用しない場合】



【ICAP 版フィルタリングを使用する場合】



【PROXY 版フィルタリングを使用する場合】



✓ ボタンの説明

[設定]	各機能の設定画面へ遷移します。 URL フィルタ用ログ領域設定　→「3.2.18. URL フィルタ用ログ領域設定」 URL フィルタ選択　→「3.2.19. URL フィルタ選択」 ICAP サーバ設定　→「3.2.20. ICAP サーバ設定」 URL フィルタ(PROXY 版)設定　→「3.2.21. URL フィルタ(PROXY 版)設定」

3.2.1. 基本設定

ブラウザなどからの要求を受け付ける IP アドレスやポート番号など、プロキシサーバを動作させるための基本的な設定をサーバ種別に応じて設定します。基本設定画面はサーバ種別設定にて「Forward」もしくは「Reverse」を選んだ時画面が変わり、各設定項目も変わります。

各設定項目の詳細は「3.2.1.1. 基本設定(Forward)」と「3.2.1.2. 基本設定(Reverse)」を参照してください。

3.2.1.1. 基本設定(Forward)

基本設定

サーバ種別設定にて「Forward」「Forward(透過型 L4 スイッチ)」を選択した場合、本画面に変わります。

◆ サーバ種別設定

プロキシサーバの動作種別について、以下の３種類から設定します。

設定値	説明
Forward	クライアント側にプロキシサーバを設置することにより、高性能キャッシュ機能を活かし、アクセスされたコンテンツを自動的に保存(キャッシュ)/再利用して、素早いレスポンスの提供と、回線コスト＆トラフィックを軽減/削減します。
Forward (透過型 L4 スイッチ)	L4 スイッチなどの機器を使用した場合、トランスペアレントキャッシュ機能により、クライアントブラウザ設定なしに Web アクセスのキャッシュが可能になります。
Reverse	本サーバを Web サーバ側に設置することにより Web サーバの負担を減らし、快適なサービスの提供を実現します。

重要

・「Forward」と「Reverse」の共存はできません。
・サーバ種別設定を変更するとアクセス制御設定のプロキシ転送設定が消去されます。
・サーバ種別にて「Reverse」設定時、SSL アクセラレータを使用せずに HTTPS 通信を行う場合、「HTTPS 通信用として使用する」にチェックを付けてください。
なお、キャッシュサーバポート番号の 443 ポートは「HTTPS 通信用として使用する」固定になります。

ヒント

・サーバ種別を「Forward(透過型 L4 スイッチ)」、「Reverse」に設定した場合 WPAD サーバを使用することができなくなります。
・「Forward(透過型 L4 スイッチ)」に設定した場合に透過で処理されるのは接続先の IP アドレスが「IPv4」でポート番号が「80」の HTTP アクセスのみになります。
HTTPS 可視化機能を使用することで「443」の HTTPS アクセスを透過で処理することも可能です。
HTTPS 可視化機能の詳細は「3.2.15. HTTPS 可視化機能設定」をご確認ください。

以降は、サーバ種別設定にて「Forward(透過型 L4 スイッチ含む)」を選択した際の設定項目となります。「Reverse」を選択した場合の設定項目は「3.2.1.2. 基本設定(Reverse)」をご確認ください。

◆ キャッシュサーバ設定

HTTP 接続を待ち受ける IP アドレスとポート番号の組を設定します。
キャッシュサーバ設定として、HTTP 接続を待ち受ける IP アドレスとポート番号の組の一覧が入力に従い表示されます。設定可能数は 256 までです。この中から設定変更、または削除する IP アドレスとポート番号の組の選択を行います。
一覧から IP アドレスとポート番号の組を選択すると、一覧の隣にキャッシュサーバ IP アドレス、キャッシュサーバポート番号など、設定内容の詳細が表示されます。この詳細を編集したあとに[編集]を押下することで設定内容を変更することが可能です。
また、キャッシュサーバ設定の追加を行うときは、キャッシュサーバ IP アドレスとキャッシュサーバポート番号を入力したあと、[追加]を押下してください。これにより一覧に新たなキャッシュサーバ設定が登録されます。
キャッシュサーバ設定の削除を行う場合には、削除したい IP アドレスとポート番号の組を選択後に[削除]を押下してください。

重要

追加/編集/削除の操作を行った場合であっても、画面下部の[設定]ボタンをクリックするまでは、サーバに設定内容は反映されません。

▶ キャッシュサーバ IP アドレス

ネットワークで設定した本サーバの IP アドレスの中から HTTP 接続を待ち受けるために使用する IP アドレスを選択します。

▶ キャッシュサーバポート番号

HTTP 接続を待ち受けるポート番号を指定します。1 つの IP アドレスに複数のポート番号を指定することができます。ポート番号は 80 および 1025 から 65535 まで指定可能です。デフォルトは 8080 です。

WPAD サーバが起動している場合、同じ番ポートを指定することはできません。

✓ ボタンの説明

[追加]	キャッシュサーバ設定の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択したキャッシュサーバ設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択したキャッシュサーバ設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ FTP プロキシ設定

FTP 接続を待ち受ける IP アドレスとポート番号の組を設定します。

本機能は、コマンドプロンプトや FTP クライアントツール等で使用される、HTTP でカプセル化されていない(Native)FTP のプロキシを実現するための機能です。

FTP プロキシ設定として FTP 接続を待ち受ける IP アドレスとポート番号の組の一覧が表示されます。設定可能数は 16 までです。この中から設定変更、または削除する IP アドレスとポート番号の組の選択を行います。

一覧から IP アドレスとポート番号の組を選択すると、一覧の隣に FTP プロキシ IP アドレス、FTP プロキシポート番号など、設定内容の詳細が表示されます。この詳細を編集したあとに[編集]を押下することで設定内容を変更することが可能です。

また、FTP プロキシ設定の追加を行うときは、FTP プロキシ IP アドレスと FTP プロキシポート番号を入力したあと、[追加]を押下してください。これにより一覧に新たな FTP プロキシ設定が登録されます。

FTP プロキシ設定の削除を行う場合には、削除したい IP アドレスとポート番号の組を選択後に[削除]を押下してください。

重要

追加/編集/削除の操作を行った場合であっても、画面下部の[設定]ボタンをクリックするまでは、サーバに設定内容は反映されません。

▶ FTP プロキシ IP アドレス

「3.5.15. ネットワーク」で設定した本サーバの IP アドレスの中から接続を待ち受けるために使用する IP アドレスを選択します。

▶ FTP プロキシポート番号

接続を待ち受ける FTP プロキシポート番号を指定します。1 つの IP アドレスに複数のポート番号を指定することができます。ポート番号は 21 および 1025 から 65535 まで指定可能です。WPAD サーバが起動している場合、同じ番ポートを指定することはできません。

✓ ボタンの説明

[追加]	FTP プロキシ設定の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した FTP プロキシ設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した FTP プロキシ設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

▶ デリミタ

FTP プロキシアクセスの際、ユーザ名に接続先 FTP サーバを埋め込む方法を用いる場合、ユーザ名と接続先 FTP サーバを区別するためにデリミタを使用します。

例えば、デリミタとして"@$"が指定されている場合は、ユーザ名に指定する文字列は"ユーザ名@接続先 FTP サーバ"あるいは"ユーザ名$接続先 FTP サーバ"となります。デリミタには最大 10 種類の半角文字を指定することができます。

FTP プロキシアクセスにはプロキシ認証を行う方法と行わない方法があります。

プロキシ認証を行わない場合、次の２つの方法があります。

- ユーザ名、パスワードによる認証を行った後、(一般的な FTP クライアントソフトウェアの場合は cd コマンドを使用して)"//接続先 FTP サーバ"の形式のパスへ移動する方法
- ユーザ名に接続先 FTP サーバを埋め込む方法

プロキシ認証を行う場合については「3.2.8. 認証設定」の「FTP プロキシ機能を使用する場合の認証手順」を参照してください。

▶ Active モード時にクライアントと接続するデータセッションのポート番号を指定

Active モードでのファイル転送実行時、本サーバ側からクライアント側へデータセッションの接続要求を行う際に使用する本サーバ側(接続元)のポート番号を限定する/しないを指定します。デフォルトは「しない」です。

設定値	説明
する	「限定するポート番号の範囲」のポート番号の範囲を使用します
しない	空いているポート番号が自動的に割り当てられるため、ポート番号は不定になります

▶ 限定するポート番号の範囲

「Active モード時にクライアントと接続するデータセッションのポート番号を限定する」と指定した場合に限定するデータセッションのポート番号の範囲を指定します。

ポート番号は 20 および 1025 から 65535 まで指定可能です。デフォルトは「20-20」です。

▶ 本サーバが独自に実行した PWD コマンドが失敗した際にエラーとして

本サーバが独自に実行した PWD コマンドが失敗した際にエラーとして扱わない/扱うを指定します。デフォルトは「扱う」です。 本サーバはカレントのパスを取得するために、独自に PWD コマンドを発行し、その結果を元に URL を生成し、アクセスログの出力、URL フィルタ、アクセス制御等処理に使用します。 従って、PWD コマンドが失敗した場合には絶対 URL が正しく生成されず、「/」直下へのアクセスとして処理される場合があります。

設定値	説明
扱わない	本サーバが独自に実行した PWD コマンドに対してエラー応答が返されると「/」が返された際と同じに扱います。そのため、処理対象の URL が実際のものとは異なる場合があります
扱う	本サーバが独自に実行した PWD コマンドに対するエラー応答を、そのままクライアント側へ返します

▶ 標準 FTP コマンドの先頭に'X'が付加された FTP コマンドを

標準 FTP コマンドの先頭に'X'が付加された FTP コマンドを受け付ける/受け付けないを指定します。デフォルトは「受け付けない」です。

設定値	説明
受け付ける	先頭に'X'が付加されていない標準 FTP コマンドと同じ意味と認識して処理を行います
受け付けない	本サーバが当該コマンドを拒否しクライアント側へエラー応答を返します

▶ FTP のアップロードサイズの上限値

HTTP でカプセル化されていない（Native）FTP のアップロードサイズの上限値を指定します。

指定したサイズを超えるデータをアップロードした場合、当該セッションを切断します。

デフォルトは「0 KB(無制限)」です。

1KB～無制限まで制御可能です。

▶ FTP のダウンロードサイズの上限値

HTTP でカプセル化されていない（Native）FTP のダウンロードサイズの上限値を指定します。

指定したサイズを超えるデータをダウンロードした場合、当該セッションを切断します。

デフォルトは「0 KB(無制限)」です。

1KB～無制限まで制御可能です。

▶ 親 FTP プロキシ

親 FTP プロキシを指定することができます。

➢ 親 FTP プロキシアドレス

親 FTP プロキシのホスト名または IP アドレスを指定します。

➢ 親 FTP プロキシポート番号

親 FTP プロキシのポート番号を指定します。

ポート番号は 1 から 65535 まで指定可能です。

◆ ICP ポート番号設定

「ICP 要求を受け付ける」を選択し、本サーバが受け付ける ICP のポート番号を設定します。

ポート番号は 1025 から 65535 まで指定可能です。通常は 3130 を指定します。

ICP 要求を受け付けないことも可能です。ICP 要求を受け付けない場合には「ICP 要求を受け付けない」を選択します。設定後、ICP ポート番号は空欄になります。

・本サーバにて ICP 要求を受け付ける場合、要求を受け付ける IP アドレスは、キャッシュサーバ設定で設定している全ての IP アドレスになります。

・一般的なブラウザのプロキシ設定画面で FTP 用として設定したプロキシに対しては、HTTP でカプセル化された FTP が使用されますので、ブラウザ側の設定では、キャッシュサーバ設定の IP アドレス：ポート番号を設定してください。ただし、ブラウザによっては仕様の異なる可能性があります。

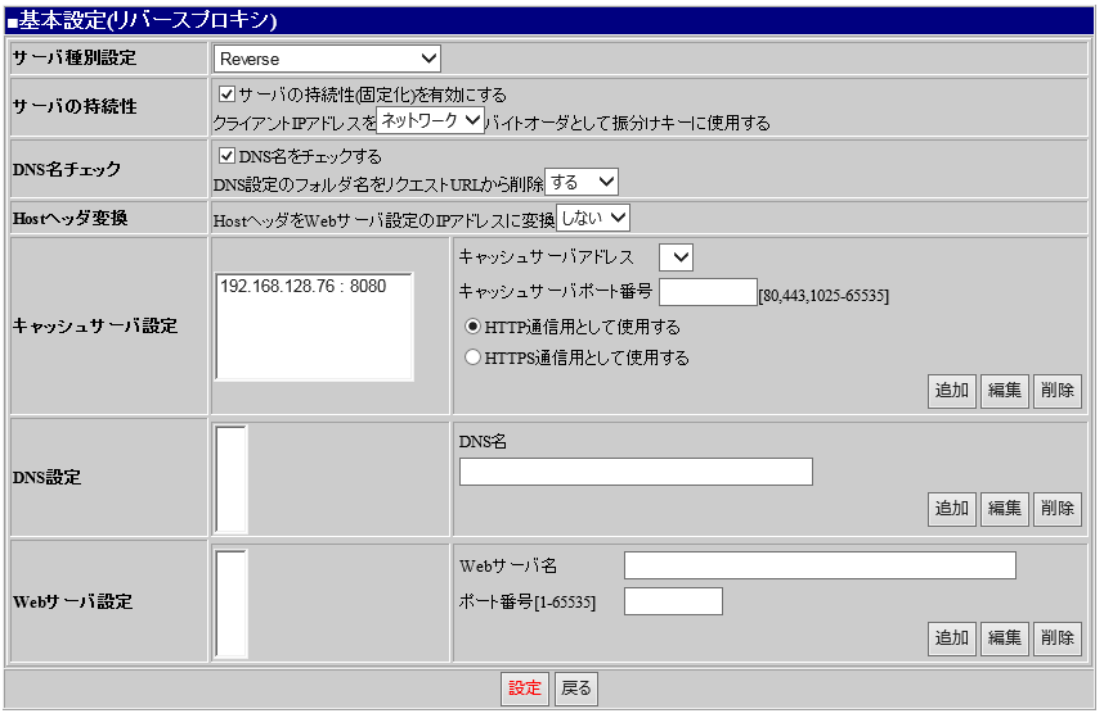
✓ ボタンの説明

[設定]	入力した内容を設定し、設定内容反映のためにプロキシサービスの再起動を行います。
[戻る]	前画面へ戻ります。

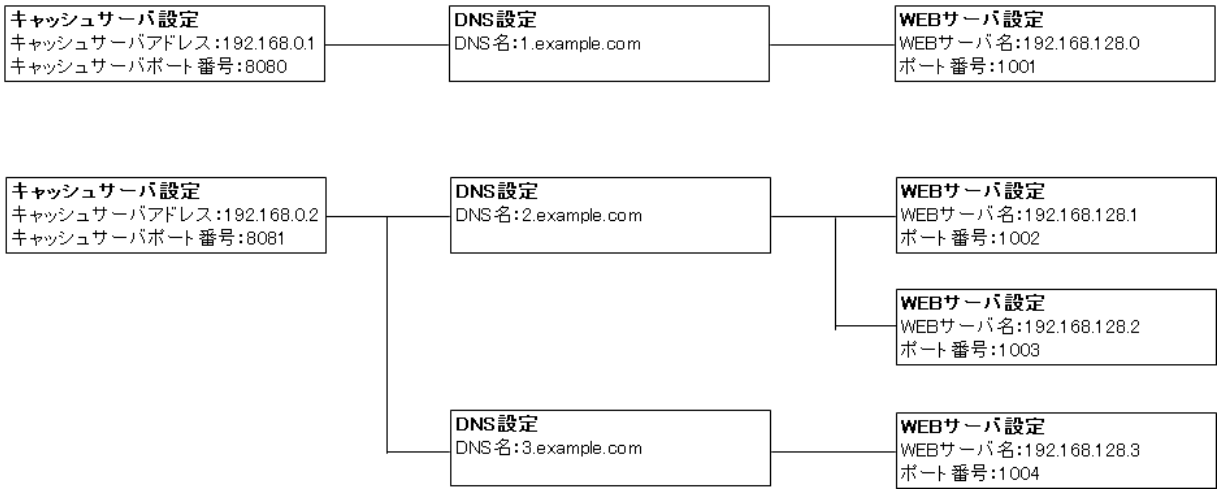
3.2.1.2. 基本設定(Reverse)

基本設定(リバースプロキシ)

サーバ種別設定にて「Reverse」を選択した場合、本画面に変わります。



リバースプロキシはキャッシュサーバ設定などで設定した待ち受けを使用して、アクセス制限を行うことにより、Web サーバのセキュリティを高めたり、Web サーバの負担を減らすことができます。更に Web サーバが複数台ある場合は負荷分散による振分けや冗長化を行うことができます。下記図の通り、キャッシュサーバ設定にクライアントからの待ち受けの IP アドレス等を設定します。その待ち受けに対して、DNS 設定に DNS 名を指定し、DNS 名毎に対応(クライアントからの要求を転送)する Web サーバを WEB サーバ設定に登録します。InterSafe WebFilter、InterScan WebManager、i-FILTER 使用時にサーバ種別設定で「Reverse」は指定できません。



◆ サーバの持続性

1 つの DNS 設定に対して複数の Web サーバ設定を行っている環境で、このチェックを ON にすると、本サーバにアクセスしたクライアントの IP アドレスを振分けのキーとして使用し、同じ IP アドレスからのアクセスを常に一意の Web サーバに振分けます。デフォルトは ON です。
このチェックを OFF にすると、当該アクセスをラウンドロビンで Web サーバに振分けを行います。

▶ サーバの持続性(固定化)を有効にする

設定値	説明
■チェックあり	持続性を有効にします。
□チェックなし	持続性を無効にします。

サーバの持続性は、HTTP の Keep-Alive に関する設定ではありません。

▶ クライアント IP アドレスを「ネットワーク/ホスト」オーダとして振分けキーに使用する

サーバの持続性(固定化)のチェックを ON にした場合に、Web サーバの振分けに使用するバイトオーダを下記から選択します。デフォルトは「ネットワーク」です。

設定値	説明
ネットワーク	同じネットワークからのアクセスを一意の Web サーバに振分ける傾向になります。 不特定多数のネットワーク(WAN 等)からのアクセスがメインの場合に、有効な設定です。
ホスト	同じネットワークからのアクセスを異なる Web サーバに振分ける傾向になります。 同じネットワーク(LAN 等)からのアクセスがメインの場合に、有効な設定です。

本サーバに直接接続して来ているクライアントの IP アドレスによって持続性を確保しているため、接続ルートが異なると持続性は確保されません。

◆ DNS 名チェック

本サーバが要求を受け付けたリクエストの URL が、DNS 設定にて設定した DNS 名と合致するかのチェックを行うか否かを指定します。デフォルトは「行う」です。DNS 名をチェックする場合、どの DNS 名とも合致しないリクエストは拒否されます。

▶ DNS 名をチェックする

設定値	説明
■チェックあり	DNS 名チェックを行います。
□チェックなし	DNS 名チェックを行いません。

▶ DNS 設定のフォルダ名をリクエスト URL から削除「する/しない」

DNS 設定でフォルダ名まで指定している場合に、リクエスト URL から当該フォルダ名部分を削除して Web サーバに転送するかどうか指定します。デフォルトは「する」です。以下の項目から選択します。

設定値	説明
する	DNS 設定のフォルダ名をリクエスト URL から削除する。
しない	DNS 設定のフォルダ名をリクエスト URL から削除しない。

指定しているフォルダ名が Web サーバ側のホームディレクトリ(Apache では DocumentRoot)であったり、Web サーバ上に実在しない識別のための仮想フォルダである場合等は、削除「する」を選択してください。

【削除する設定例】

DNS 設定	1.example.co.jp/sv1/
リクエスト URL	http://1.example.co.jp/sv1/index.html
転送時の URL	http://1.example.co.jp/index.html

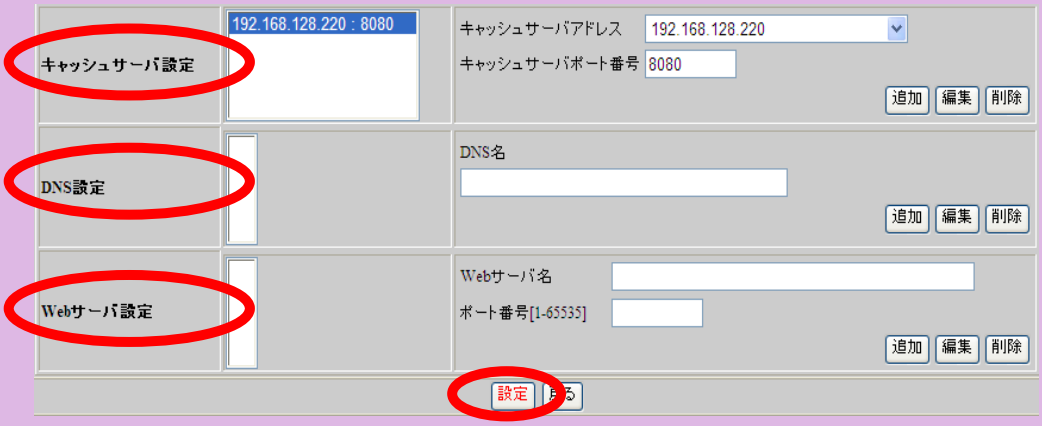
指定しているフォルダ名が Web サーバ側のホームディレクトリ直下のサブフォルダである場合は、削除「しない」を選択してください。

【削除しない設定例】

DNS 設定	1.example.co.jp/sv1/
リクエスト URL	http://1.example.co.jp/sv1/index.html
転送時の URL	http://1.example.co.jp/sv1/index.html

・リバースプロキシの設定方法

キャッシュサーバ設定にクライアントからの待ち受けの IP アドレス等を設定します。その待ち受けに対して、DNS 設定に DNS 名を指定し、DNS 名毎に対応(クライアントからの要求を転送)する Web サーバを WEB サーバ設定に登録します。



1) キャッシュサーバアドレス」と「キャッシュサーバポート番号」を入力して[追加]を押下する。
2) キャッシュサーバ設定にて追加された設定情報を選択し、DNS 名を入力後[追加]を押下する。
3) DNS 設定にて追加された設定情報を選択し、「Web サーバ名」と「ポート番号」を入力し、[追加]を押下する。
4) 1)～3)の手順後[設定]ボタンを押下する。

◆ Host ヘッダ変換

クライアントの HTTP リクエストの Host ヘッダが IP アドレスで構成されている場合において、Host ヘッダの IP バージョンと転送先 Web サーバの IP バージョンが異なる場合、 Host ヘッダを転送先 Web サーバアドレスに変換します。デフォルトは「しない」です。Web サーバ側の仕様によっては IP バージョンの異なるリクエストが拒否される場合がありますので、その場合は「する」に設定することでアクセスが拒否されなくなります。

※本設定は HTTP 通信のみ有効です。(HTTPS 通信では無効です)

◆ キャッシュサーバ設定

HTTP 接続を待ち受ける IP アドレスとポート番号の組を設定します。

キャッシュサーバ設定として、HTTP 接続を待ち受ける IP アドレスとポート番号の組の一覧が入力に従い表示されます。設定可能数は 256 までです。

ポート番号は 80,443,1025～65535 を指定可能です。

一覧から IP アドレスとポート番号の組を選択すると、一覧の隣にキャッシュサーバ IP アドレス、キャッシュサーバポート番号など、設定内容の詳細が表示されます。この詳細を編集したあとに[編集]を押下することで設定内容を変更することが可能です。

また、キャッシュサーバ設定の追加を行うときは、キャッシュサーバ IP アドレスとキャッシュサーバポート番号を入力したあと、[追加]を押下してください。これにより一覧に新たなキャッシュサーバ設定が登録されます。

キャッシュサーバ設定の削除を行う場合には、削除したい IP アドレスとポート番号の組を選択後に[削除]を押下してください。

▶ キャッシュサーバアドレス

ネットワークで設定した本サーバの IP アドレスの中から待ち受けるために使用する IP アドレスを選択します。

▶ キャッシュサーバポート番号

待ち受けるポート番号を指定します。1 つの IP アドレスに複数のポート番号を指定することができます。ポート番号は 80、443 および 1025 から 65535 まで指定可能です。

▶ 通信用途指定

当該待ち受けの用途を 1 つ選択します。

設定値	説明
HTTP 通信用として使用する	当該待ち受けを HTTP 通信用として使用します。
HTTPS 通信用として使用する	当該待ち受けを HTTPS 通信用として使用します。 SSL アクセラレータを使用せずに HTTPS 通信を行う場合にチェックします。

✓ ボタンの説明

[追加]	キャッシュサーバ設定の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	キャッシュサーバ設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	キャッシュサーバ設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ DNS 設定

Internet に公開する Web サーバのホスト名(DNS 名)を指定します。フォルダ名を指定することで同じホスト名で異なるサーバに振分けることが可能です。

1 つのキャッシュサーバに対して 16 個の DNS 名を設定することが可能です。ただし、「HTTPS 通信用として使用する」にチェックを付けているキャッシュサーバに対しては、DNS 名は 1 つのみです。

DNS名としてIPv6アドレスを指定する場合、IPアドレスの前後に"[]"をつけて設定してください。

DNS 設定は、キャッシュサーバで選択している待ち受けアドレスに対する設定となります。キャッシュサーバ設定の待ち受けアドレスの選択にしたがって、DNS 設定には対応する設定値を表示します。

▶ DNS 名

DNS 名を指定します。

DNS 名指定例:)

1.example.co.jp

1.example.co.jp/sv1/

1.example.co.jp/sv2/

重要

・フォルダ名を指定するときは"/"(スラッシュ)を最後に付けてください。

・別々のコンテンツを持つ複数の Web サーバに対して本サーバを使用する場合、Web サーバの数だけ DNS 名を指定してください。本サーバはホスト名を見分けて別々に処理することが可能です。

フォルダの階層が多段になっており上位階層のフォルダが同じ場合は階層が深い順に上から設定を行ってください。

DNS 名指定例
1.example.co.jp
1.example.co.jp/sv1/box1/
1.example.co.jp/sv1/

重要

逆に設定した場合は「1.example.co.jp/sv1/box1/」配下も「1.example.co.jp/sv1/」に該当することになります。

✓ ボタンの説明

[追加]	DNS 設定の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	DNS 設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	DNS 設定の削除を行います。削除後、[設定]を押下することで内容を反映しま

	す。

◆ Web サーバ設定

実際の Web サーバの IP アドレスまたはホスト名と、ポート番号を指定します。
本サーバは 1 つの DNS 名に対して 16 個の Web サーバを設定することが可能です。
Web サーバ設定は、キャッシュサーバで選択している待ち受けアドレスに対する設定となります。
キャッシュサーバ設定の待ち受けアドレスの選択にしたがって、対応する設定値を表示します。

重要

1 つの DNS 名に対して複数の Web サーバを設定する場合には、Web サーバは全て同一のコンテンツを提供する必要があります。

▶ Web サーバ名

アクセスを転送する Web サーバの IP アドレスまたはホスト名を指定します。

▶ ポート番号

アクセスを転送する Web サーバの待ち受けポート番号を指定します。

✓ ボタンの説明

[追加]	Web サーバ設定の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	Web サーバ設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	Web サーバ設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

重要

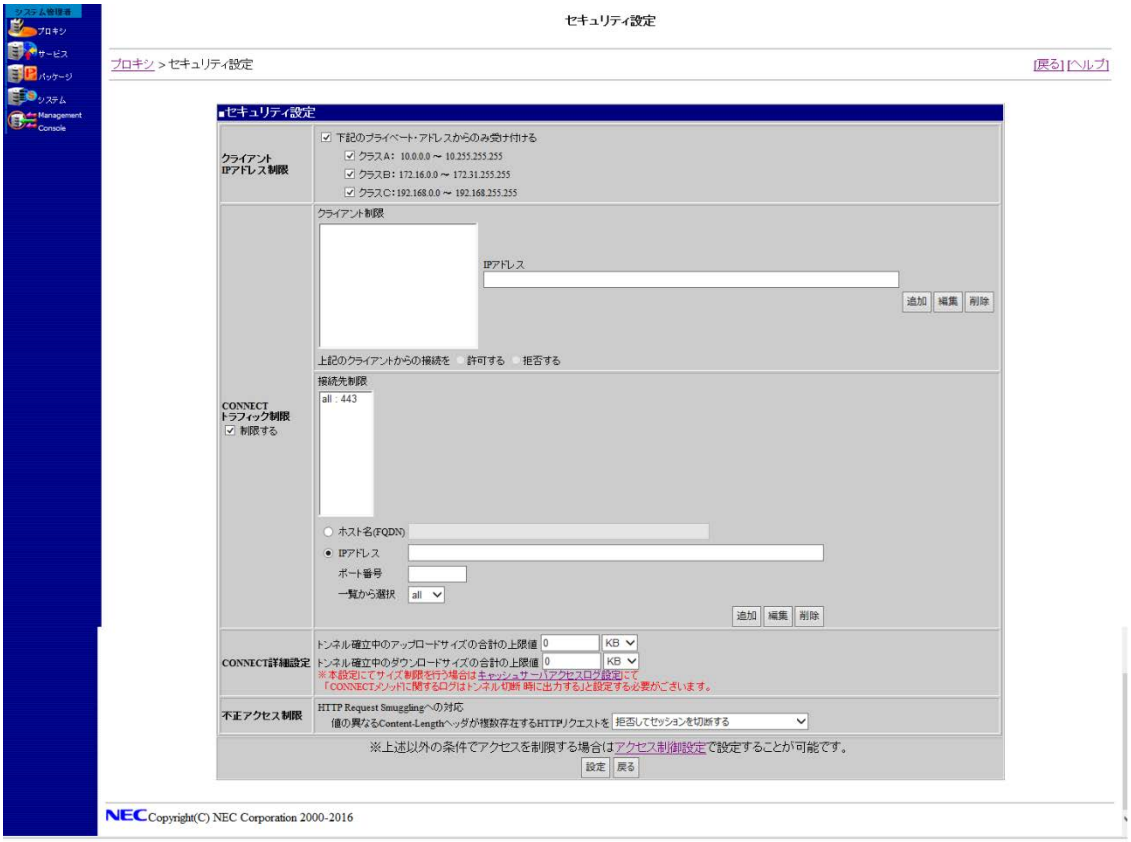
- 各リストボックスの設定項目を選択すると、リストボックス隣に設定内容が表示され、設定内容を編集した後に[編集]ボタンを押すことで設定内容を変更することが可能です。
- 各リストボックスに設定を追加する場合には、リストボックス隣で設定内容を入力後[追加]ボタンを押してください。
- 各リストボックスから設定を削除する場合には、リストボックスの削除したい設定を選択したあと[削除]を押してください。
- 追加/編集/削除の操作を行った場合であっても、画面下部の[設定]ボタンをクリックするまでは、サーバに設定内容は反映されません。
- サーバ種別設定を[Reverse]にする場合は DNS の設定を確認してください。
  今まで DNS で Web サーバのホスト名=Web サーバの IP アドレス と設定していた場合は Web サーバのホスト名=本サーバの IP アドレス と変更してください。

3.2.2. セキュリティ設定

セキュリティ設定

クライアント IP アドレス制限と、CONNECT トラフィック制限を行います。

更に細かい条件の設定を行いたい場合は「3.2.6. アクセス制御」で設定を行ってください。



◆ クライアント IP アドレス制限

本サーバに接続するクライアントを、IP アドレスのクラス別に制限します。

IPv4 に関してはクラス A～クラス C を選択してチェックを入れてください。

▶ 下記のプライベート・アドレスのみから受け付ける

デフォルトでは、全てのクラスに対して接続許可になっています。

「3.2.1.2. 基本設定(Reverse)」でサーバ種別設定に「Reverse」設定している場合は、この制限は無効となります。

設定値	説明
■チェックあり	クラスの指定に従い制限のチェックを行います。 クラスを選択していない場合は、全クライアント拒否になりますので注意してください。 クラスを選択した状態でも、チェックを外すと制限は無効になります。 また、この制限を設定していると、グローバル・アドレスから接続することはできません。
□チェックなし	制限を行いません。

➢ クラス A：10.0.0.0-10.255.255.255

設定値	説明
■チェックあり	クラス A の制限を行います。
□チェックなし	クラス A の制限の制限を行いません。

➢ クラス B：172.16.0.0-172.31.255.255

設定値	説明
■チェックあり	クラス B の制限を行います。
□チェックなし	クラス B の制限の制限を行いません。

➢ クラス C：192.168.0.0-192.168.255.255

設定値	説明
■チェックあり	クラス C の制限を行います。
□チェックなし	クラス C の制限の制限を行いません。

◆ CONNECT トラフィック制限

CONNECT メソッドは、プロキシでのトンネル接続を行うメソッドです。
トンネル接続は、どのようなアドレスやポートに対しても接続可能となっているため、外部からプロキシサーバを踏み台にして不正にアクセスされたり、内部から本来アクセスを許可していない外部のサービスにアクセスができる可能性があります。
CONNECT トラフィック制限は、CONNECT メソッドによる不正なアクセスを IP アドレスやポート番号で制限します。
「3.2.1.1. 基本設定(Forward)」のサーバ種別設定で「Forward」以外を設定している場合は、「制限する」にチェックを行い「クライアント制限」、「接続先制限」の設定を全て削除(拒否)することを推奨します。

設定値	説明
■チェックあり	指定に従いチェックを行います。
□チェックなし	チェックを行いません。

チェックを外している場合は、この設定は無効となり、追加/編集/削除の設定を行うことができません。

▶ クライアント制限

接続制限を行うクライアントを、IP アドレスを表示します。
デフォルトの設定はありません。

➢ IP アドレス

接続制限を行うクライアントを、IP アドレスで指定します。
何も設定していない場合は、「全ての IP アドレスの接続を許可」となります。アドレスマスクには最上位ビットから連続してビットが立つ値を指定してください。範囲指定の場合は、アドレスマスクを指定することができません。
全 IP アドレスを意味する設定(all、0.0.0.0 等)を指定することはできません。
形式)
ipaddress
ipaddress/mask
ipaddress1-ipaddress2
例)
192.168.0.1
192.168.0.0/24
192.168.0.0/255.255.255.0
192.168.0.1-192.168.0.50
2001:db8:20:3:1000:100:20:3
2001:db8:20:3::0 /32
2001:db8:20:3:1000:100:20:1-2001:db8:20:3:1000:100:20:50

✓ ボタンの説明

指定する IP アドレスの指定操作を行います。

[追加]	入力したアドレスの追加を行います。
[編集]	選択した設定の IP アドレスの編集を行います。
[削除]	選択した設定の IP アドレスの削除を行います。

▶ 接続先制限

アクセス制限を行う接続先のホスト名(FQDN)または IP アドレス、ポート番号を表示します。デフォルトでは「全接続先に対してポート番号 443 のみ許可(all:443)」が設定されています。ここで何も設定していない場合は、「全ての接続先への接続を拒否」となります。アドレスマスクには最上位ビットから連続してビットが立つ値を指定してください。

接続先としてホスト名(FQDN)を指定した場合は、一致するホスト名(FQDN)でリクエストが来た場合のみ接続を許可します。接続先を IP アドレスで指定した場合は、一致する IP アドレスでリクエストが来た場合のみ接続を許可します。

例)

all:all

192.168.0.1:8081

192.168.0.0/24:all

192.168.0.0/255.255.255.0:80

192.168.0.51-192.168.0.100:80

2001:db8:20:3:1000:100:20:3：8081

2001:db8:20:3::0/32：all

2001:db8:20:3:1000:100:20:1-2001:db8:20:3:1000:100:20:50：8081

1.example.co.jp:8080

➢ ホスト名(FQDN)

アクセス制限を行う接続先をホスト名を FQDN 形式にて指定する場合チェックし、ホスト名(FQDN)を指定します。

➢ IP アドレス

アクセス制限を行う接続先を、IP アドレスとポート番号で指定する場合チェックします。代表的な接続先は「一覧から選択」のリストから選択できます。「一覧から選択」にない接続先に関しては、「IP アドレス」と「ポート番号」の組み合わせで指定してください。全ての IP アドレス、ポート番号を指定する場合は、「all」を設定します。

「一覧から選択」内の代表的なポート番号一覧

ポート番号	名前
22	ssh
23	telnet
25	smtp
110	pop3
119	nntp
143	imap4
443	https

✓ ボタンの説明

該当行に対する操作をいます。

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ CONNECT 詳細設定

同じトンネルでアップ/ダウンロードを行ったサイズの合計の上限値を指定します。

▶ トンネル確立中のアップロードサイズの合計の上限値

同じトンネルでアップロードを行ったサイズの合計の上限値を指定します。(0 KB[無制限])

上限値を超えた場合、当該トンネルを切断します。

1KB～無制限(0)まで制御することが可能です。

▶ トンネル確立中のダウンロードサイズの合計の上限値

同じトンネルでダウンロードを行ったサイズの合計の上限値を指定します。(0 KB[無制限])
上限値を超えた場合、当該トンネルを切断します。
1KB～無制限(0)まで制御することが可能です。

重要

本設定にてサイズ制限を行う場合は「3.5.12.2. キャッシュサーバアクセスログ設定」にて「CONNECT メソッドに関するログはトンネル切断 時に出力する」と設定している場合に有効となります。

◆ 不正アクセス制限

値の異なる Content-Length ヘッダが複数存在する HTTP リクエストを本サーバが受信した際の処理を選択します。デフォルトは「拒否してセッションを切断する」です。本項目は HTTP Request Smuggling への対応になります。

▶ 値の異なる Content-Length ヘッダが複数存在する HTTP リクエストを「・・・」

設定値	説明
そのまま転送する	選択した場合は受信した HTTP リクエストをそのまま上位サーバに転送します。
拒否してセッションを切断する	選択した場合は受信した HTTP リクエストを上位サーバへ転送せずクライアント側にエラー応答を返しセッションを切断します。
上位サーバとの間のみ Keep-Alive を行わない	選択した場合は受信した HTTP リクエストを上位サーバへ転送しますが上位サーバ側のみ Kepp-Alive を行いません。
Keep-Alive を行わない	選択した場合は受信した HTTP リクエストを上位サーバへ転送しますがクライアント側、上位サーバ側で Kepp-Alive を行いません。

重要

「クライアント IP アドレス制限」と「CONNECT トラフィック制限」と「アクセス制御」の制限処理の順番は以下の通りです。
制限処理の順番によって設定が無効になる場合がありますので注意してください。

1) クライアント IP アドレス制限
2) CONNECT トラフィック制限
3) アクセス制御

✓ ボタンの説明

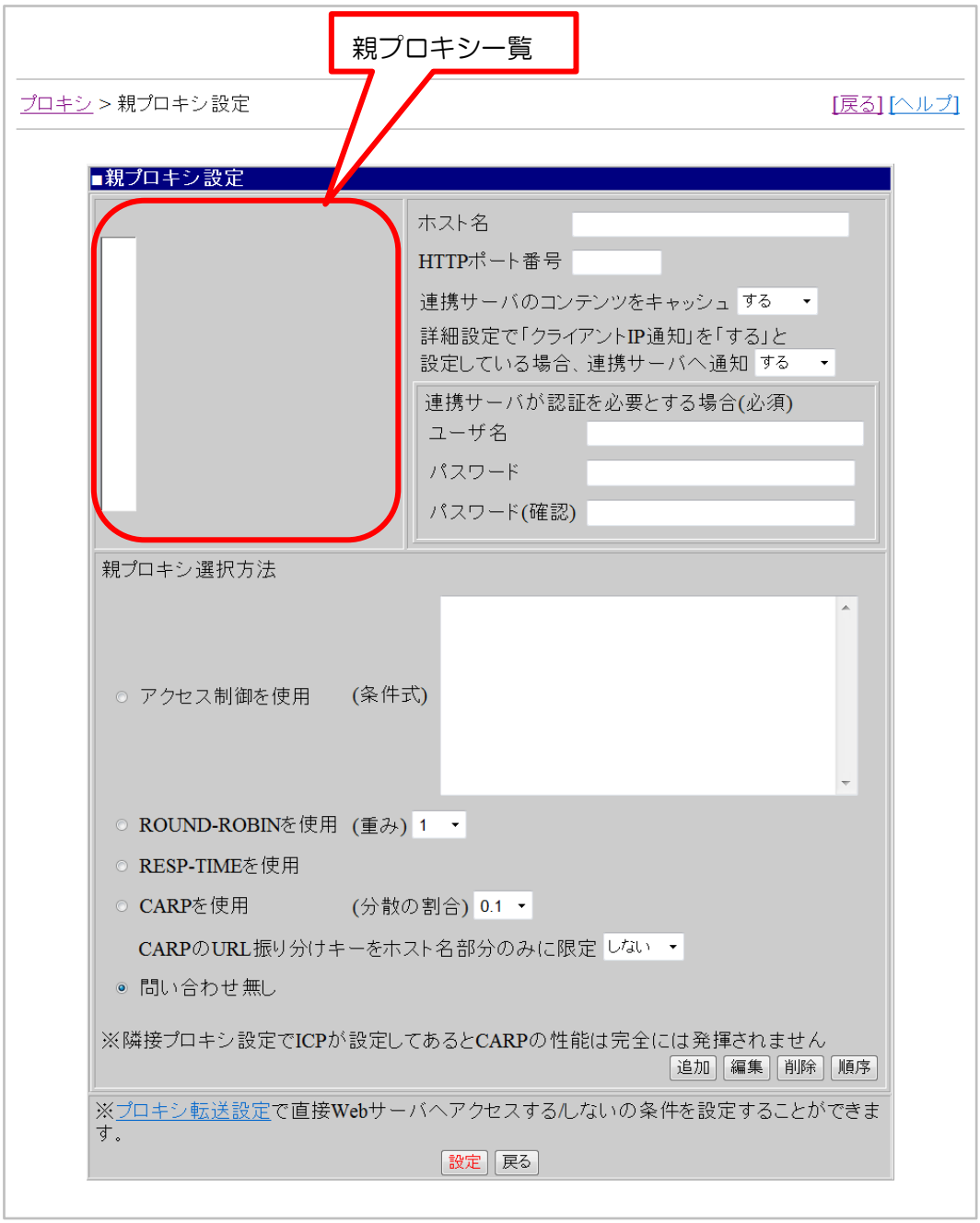
設定した項目の操作を行います。

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.3. 親プロキシ設定

親プロキシ設定

階層構造を形成する場合に親プロキシ(上位プロキシ)を設定することができます。親プロキシの指定と、親プロキシの選択方法を設定します。



◆ 親プロキシー覧

登録済の親プロキシの一覧が表示されます。設定可能数は 16 までです。
この中から設定変更、または削除する親プロキシの選択を行います。

親プロキシー覧の操作方法
- 一覧に表示されている親プロキシを選択すると、一覧の隣に親プロキシのホスト名、HTTP ポート番号などが、一覧の下部には親プロキシの選択方法に応じた詳細な情報が表示されます。
- 設定の編集後、「編集」を押下することで設定内容を変更することが可能です。
- 親プロキシの追加を行うときは、親プロキシのホスト名などの必要な設定を行ったあと、「追加」を押下してください。これにより一覧に新たな親プロキシが登録されます。
  親プロキシの削除を行う場合には、削除したい親プロキシを選択後に「削除」を押下してください。
- 親プロキシの順序を入れ換えたい場合には「順序」を押下してください。
- 順序を入れ換えることに意味がある親プロキシ選択方法はアクセス制御だけです。
- 追加/編集/削除/順序の操作を行った場合であっても、画面下部の「設定」を押下するまでは、サーバに設定内容は反映されません。

▶ ホスト名

親プロキシのホスト名または IP アドレスを指定します。隣接プロキシに設定してあるホスト名、IP アドレスは登録できません。アクセス制御を使用時、ホスト名には「login=」,「proxy-only」,tab を含む名前を指定することはできません。255 文字まで指定可能です。

▶ HTTP ポート番号

親プロキシのポート番号を指定します。

▶ 連携サーバのコンテンツをキャッシュ「する/しない」

キャッシュ可能な連携サーバからの応答をキャッシュするかどうかを指定します。

設定値	説明
する	応答をキャッシュします
しない	応答をキャッシュしません

▶ 詳細設定で「クライアント IP 通知を「する」と設定している場合、連携サーバへ通知する／しない

「3.2.5. 詳細設定」の「クライアント IP 通知」を「する」と設定している場合に付与される X-Forwarded-For ヘッダを連携サーバへ転送するかどうかを指定します。

設定値	説明
する	X-Forwarded-For ヘッダを付与して親プロキシへ転送します。
しない	X-Forwarded-For ヘッダを付与せず親プロキシへ転送します。

▶ 連携サーバが認証を必要とする場合(必須)

連携サーバ側でプロキシサーバの Basic 認証が有効となっている場合はユーザ名、パスワードの指定を行います。認証を必要としない場合には設定の必要はありません。

➢ ユーザ名

認証で使用するユーザ名を入力欄に指定します。「:」,tab を使用したユーザ名は指定できません。

➢ パスワード

認証で使用するパスワードを入力欄に指定します。「:」,tab を使用したパスワードは指定できません。

➢ パスワード確認

パスワードが誤っていないか確認用のパスワードを入力します。

◆ 親プロキシ選択方法

親プロキシの選択方法を、アクセス制御、ROUND-ROBIN、RESP-TIME、CARP の中から選択し設定をあわせて行います。選択された親プロキシ選択方法に応じて条件式や重みを指定します。サーバ種別を知りたい場合には親プロキシー覧(リストボックス)から親プロキシを選択して確認してください。

親プロキシ選択方法を複数同時に存在させることはできません。

▶ アクセス制御を使用

親プロキシへの接続方法にアクセス制御を用います。アクセス制御を用いる場合には条件式に制御方法を記述します。

➢ (条件式)

条件式には、指定された親プロキシへ接続を許可/不許可する宛先を記述します。

宛先をホスト名で指定する場合には「dn=ホスト名」で、IP アドレスで指定する場合には「ip=IP アドレス」と記述します。条件式に「login=」,「proxy-only」,「xff-notadd」を指定することはできません。

ホスト名での指定、IP アドレスでの指定はともにワイルドカード「*」を使用することができます。ただし、ワイルドカードはホスト名の方には"."にもマッチし、IP アドレスの方には"."にはマッチしません。

条件式には「!」を用いることも可能です。「!*. example.co.jp」という条件式があったとき、*. example.co.jp 以外の宛先を親プロキシに送ります。条件式に入力したタブと改行は空白文字に置き換えられます。

クライアント側 IP アドレスに対する制御(srcip)と、接続先ドメイン(dn)または IP アドレス(ip)に対する制御があります。

異なる種別の条件が同時に指定された場合(例えば srcip と dn など)は AND 条件、同じ種別の条件が同時に設定された場合(例えば ip と ip)の場合は OR 条件となります。

親プロキシの順序を入れ換えたい場合には「順序」を押下してください。

親プロキシ選択時には DNS 参照を行わないため、完全な制御を行うためには dn=,ip=の両方の指定が必要です。

親プロキシ指定１件で ip=, dn=, srcip= は各々64 個まで指定できます。
"="の前後にスペースを入れることはできません。

例 1)
http://www.ipc. example.co.jp/は、dn=*. example.co.jp にマッチします。
http://10.23.88.1/は、ip=10.*.*.*にマッチしますが、ip=10.*にはマッチしません。
1 つの条件式にスペース区切りで複数のホスト名、IP アドレスを記述することが可能です。

例 2)
dn=www. example.co.jp dn=!*. example.co.jp　ip=!10.*.*.*　ip=!192.*.*.*
複数の親プロキシの条件式にマッチした場合には、親プロキシ一覧の上位に書かれている設定が優先して適用されます。

例 3)
単一 IP アドレス指定: srcip=192.168.0.1
正規表現指定(*のみ): srcip=192.168.0.*
IP アドレス範囲指定: srcip=192.168.0.1-192.168.0.100
ネットマスク指定: srcip=192.168.0.0/255.255.255.0
例外指定: srcip=!192.168.0.1

▶ ROUND-ROBIN を使用

親プロキシへの接続方法に ROUND-ROBIN を用います。「サーバが接続された回数/重み」の値が最も小さい親プロキシが選択されます。

➢ (重み)

重みは 1 から 10 まで指定可能です。

▶ RESP-TIME を使用

親プロキシへの接続方法に RESP-TIME を用います。セッション接続にかかる時間が最も短い親プロキシが選択されます。

▶ CARP を使用

親プロキシへの接続方法に CARP(Cache Array Routing Protocol)を用います。CARP による親プロキシの負荷分散設定を行います。

➢ (分散の割合)

指定した親プロキシに対する負荷の分散値を 0.1 から 0.9 の範囲で(0.1 単位)指定します。
CARP のプロトコル規則では分散値の合計値が 1 になるよう決められていますが、本設定では合計値を 1 にする必要はありません。
合計値が 1 以外の場合、設定された分散値の比率に応じて内部的に分散値を変換します。
例えば、分散値が「0.1」の親プロキシが 4 台設定されている場合内部的には分散値は「0.25」として扱われます。

➢ CARP の URL 振分けキーをホスト名部分のみに限定する／しない

CARP の URL 振分けキーをホスト名部分のみに限定するかどうかを指定します。

設定値	説明
する	ホスト名部分が同じ URL へのアクセスは同じ親プロキシを使用します。
しない	ホスト名、パス部分が同じ URL へのアクセスは同じ親プロキシを使用します。

▶ 問い合わせ無し

親プロキシを１つしか指定しない場合には問い合わせ無しを指定してください。

親プロキシが１つのみの場合は、自動的に問い合わせ無しに設定されます。

重要

・隣接プロキシ設定で ICP が設定してあると CARP の性能は完全には発揮されません。
・下記のいずれかの条件に当てはまる場合、直接 Web サーバへ接続します。
1) アクセス制御を使用している場合、全ての条件式に一致しなかった
2) 対象になっている全ての親プロキシに接続できなかった
・直接 Web サーバへ接続させない場合、プロキシ転送設定で設定を行ってください。設定方法、デフォルトの設定値、注意事項に関しては「3.2.6. アクセス制御」の「■プロキシ転送設定」を参照

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。
[順序]	リストの順序を変更することができます。

◆ プロキシ転送設定

プロキシ転送設定のリンクをクリックすることで直接 Web サーバへアクセスする/しないの条件の設定を行うことができます。

→「3.2.6. アクセス制御」の「■プロキシ転送設定」

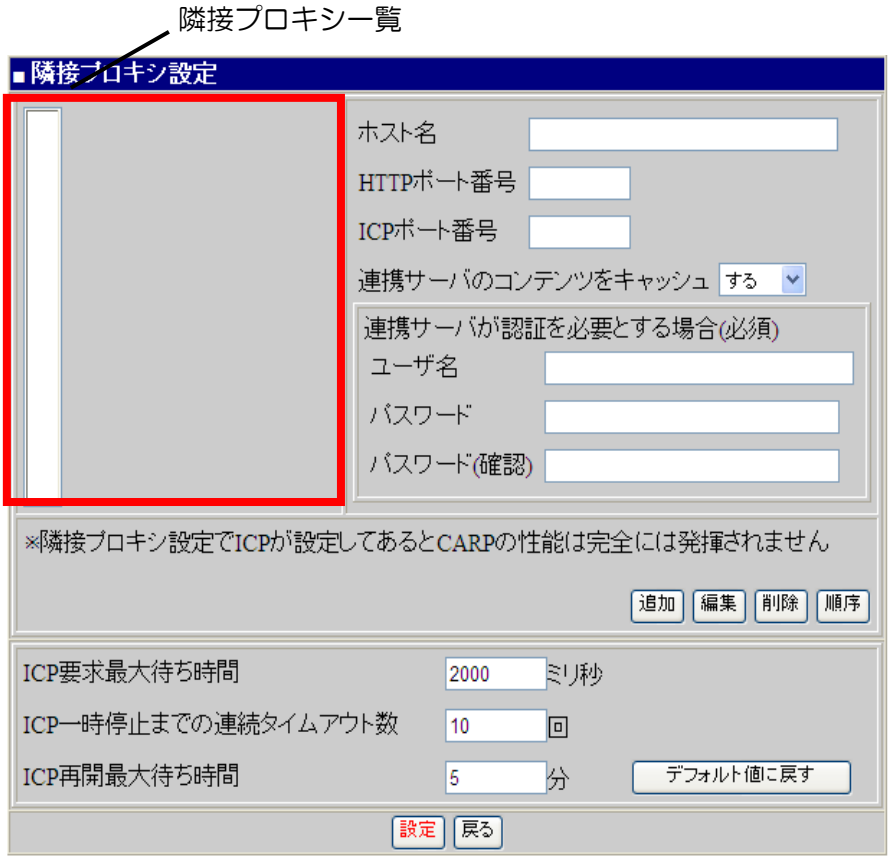
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.4. 隣接プロキシ設定

隣接プロキシ設定

階層構造を形成する場合にシステムの隣接プロキシを設定することができます。



◆ [隣接プロキシー覧]

登録済の隣接プロキシの一覧が表示されます。設定可能数は 16 までです。
この中から設定変更、または削除する隣接プロキシの選択を行います。

ヒント

隣接プロキシー覧の操作方法

- 一覧に表示されている隣接プロキシを選択すると、一覧の隣に隣接プロキシのホスト名、HTTP ポート番号などが表示されます。
- 設定の編集後、[編集]を押下することで設定内容を変更することが可能です。
- 隣接プロキシの追加を行うときは、隣接プロキシのホスト名などの必要な設定を行ったあと、[追加]を押下してください。これにより一覧に新たな隣接プロキシが登録されます。
- 隣接プロキシの削除を行う場合には、削除したい隣接プロキシを選択後に[削除]を押下してください。
- 追加/編集/削除の操作を行った場合であっても、画面下部の[設定]を押下するまでは、サーバに設定内容は反映されません。

▶ ホスト名

隣接プロキシのホスト名または IP アドレスを指定します。親プロキシに設定してあるホスト名、IP アドレスは指定できません。255 文字まで指定可能です。

▶ HTTP ポート番号

隣接プロキシのポート番号を指定します。

▶ ICP ポート番号

隣接プロキシへ問い合わせる ICP のポート番号を指定します。

▶ 連携サーバのコンテンツをキャッシュ「する/しない」

連携サーバのコンテンツをキャッシュするかどうかを指定します。

設定値	説明
する	コンテンツをキャッシュします。
しない	コンテンツをキャッシュしません。

▶ 連携サーバが認証を必要とする場合(必須)

連携サーバが認証を必要とする場合にユーザ名、パスワードの指定を行います。連携サーバが認証を必要とする場合にはユーザ名、パスワードの指定は必須です。認証を必要としない場合には設定の必要はありません。

➢ ユーザ名

認証で使用するユーザ名を入力欄に指定します。「:」,tab を使用したユーザ名は指定できません。

➢ パスワード

認証で使用するパスワードを入力欄に指定します。「:」,tab を使用したパスワードは指定できません。

➢ パスワード確認

パスワードが誤っていないか確認用のパスワードを入力します。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。
[順序]	リストの順序を変更することができます。

◆ ICP 要求最大待ち時間

連携サーバへのキャッシュデータの有無の問い合わせに対する待ち時間を設定します。10 ミリ秒から 5000 ミリ秒まで指定可能です。デフォルトは 2000 ミリ秒です。

◆ ICP 一時停止までの連続タイムアウト数

連携サーバへのキャッシュデータの有無の問い合わせが、ICP 一時停止までの連続タイムアウト数分連続でタイムアウトした場合、ICP 機能を一時停止します。1 回から 999 回まで指定可能で

す。デフォルトは 10 回です。

◆ ICP 再開最大待ち時間

一時停止した ICP 機能を再開するまでの待ち時間を設定します。1 分から 9999 分まで指定可能です。デフォルトは 5 分です。

ICP 要求最大待ち時間、ICP 一時停止までの連続タイムアウト数、ICP 再開最大待ち時間は、すべての隣接プロキシと共通の設定となります。隣接プロキシ設定で ICP が設定してあると CARP の性能は完全には発揮されません。

✓ ボタンの説明

[デフォルト値に戻す]	ICP 要求最大待ち時間、ICP 一時停止までの連続タイムアウト数、ICP 再開最大待ち時間をデフォルト値に戻します。

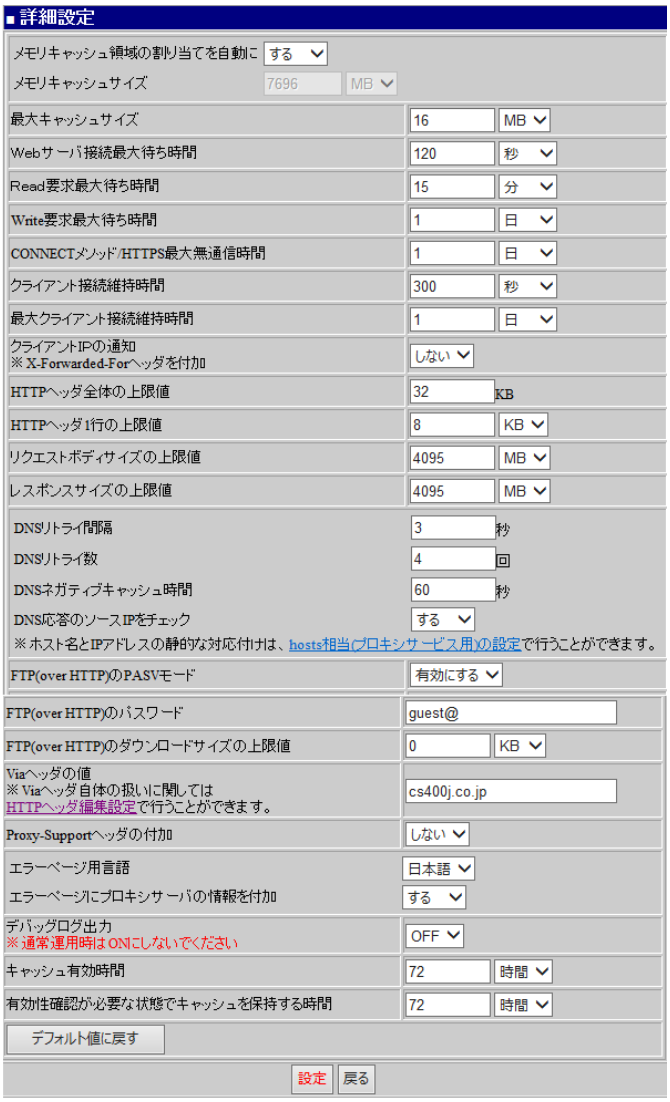
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.5. 詳細設定

詳細設定

プロキシサーバとしての詳細な動作設定ができます。



◆ メモリキャッシュ領域の割り当てを自動にする/しない

オブジェクトをキャッシュする領域のサイズを搭載メモリの容量から自動的に算出するかどうかを指定します。デフォルトは「する」です。

自動で算出する場合、十分にメモリの空きが確保できるように割り当てを行いますが、実際の運用において常に使用されない空きが存在しており、その空きをメモリキャッシュ領域に割り当てる場合は「しない」に変更し、再設定を行ってください。

本設定を変更した場合、設定反映のためにサーバのシステム再起動を行います。

◆ メモリキャッシュサイズ

メモリキャッシュ領域のサイズを指定します。

「3.5.3. CPU/メモリ使用状況」の「使用中」を参考に、慎重に設定を行ってください。

本設定は「メモリキャッシュ領域の割り当てを自動にしない」と設定した場合に指定可能です。

95MB から 99999GB の値で制御することができます。

※本設定を変更した場合、設定反映のためにサーバのシステム再起動を行います。

◆ 最大キャッシュサイズ

この設定よりも大きなオブジェクトはキャッシュされません。デフォルトは 16MB です。

1KB から 999MB までの値で制御することができます。0 を指定するとシステムの上限値(4095MB)になります。

◆ Web サーバ接続最大待ち時間

本サーバから Web サーバへのセッション接続要求に対し応答待ちをする時間を指定します。デフォルトは 120 秒です。 30 秒から 99 日までの値で制御することができます。

◆ Read 要求最大待ち時間

本サーバから Web サーバへの転送した HTTP リクエストに対し応答待ちをする時間を指定します。デフォルトは 15 分です。 30 秒から 99 日までの値で制御することができます。

◆ Write 要求最大待ち時間

本サーバが転送するデータをクライアント側が受信するまでの待ち時間を指定します。デフォルトは 1 日です。5 秒から 99 日までの値で制御することができます。

◆ クライアント接続維持時間

本サーバに対し、HTTP リクエストが送信されていない状態で本サーバ-クライアント間のコネクションを維持する最大無応答時間を指定します。デフォルトは 300 秒です。 30 秒から 99 日までの値で制御することができます。

◆ 最大クライアント接続維持時間

本サーバ-クライアント間でコネクションを維持する時間を指定します。デフォルトは 1 日です。30 秒から 99 日までの値で制御することができます。

◆ クライアント IP の通知

クライアントの IP アドレスをヘッダ情報として通知するかどうかを指定します。デフォルトは「しない」です。

◆ HTTP ヘッダ全体の上限値

1 つの HTTP リクエストの HTTP ヘッダ全体を格納するバッファサイズを 2KB から 999KB までの値で設定します。デフォルトは 32KB です。システムの仕様により 2 の累乗毎にバッファを確保するため、設定した値以上で一番近い 2 の累乗(2,4,8,16,32,64,128,256,512,1024KB)が実際の上限値になります。

例：「40KB」と設定した場合に実際のバッファの上限値は「64KB」になります。

◆ HTTP ヘッダ 1 行の上限値

HTTP ヘッダの 1 行のヘッダサイズの上限値を指定します。デフォルトは 8KB です。
512B から 999KB までの値で制御することができます。
HTTP ヘッダ全体の上限値未満の値を設定してください。

◆ リクエストボディサイズの上限値

クライアントからのリクエストボディサイズの上限値を 1KB から 9999GB までの値で指定します。
デフォルトは 4095MB です。

◆ レスポンスサイズの上限値

サーバからのレスポンスサイズの上限値を 1KB から 9999GB までの値で指定します。
デフォルトは 4095MB です。

◆ DNS リトライ間隔

DNS サーバからの応答待ち時間を指定します。デフォルトは 3 秒です。
この応答待ち時間が経過しても応答が返らない場合は、リトライを行います。
1 秒から 99 秒までの値で設定することができます。

◆ DNS リトライ数

DNS サーバへのリトライ回数を指定します。デフォルトは 4 回です。1 回から 99 回までの値で設定することができます。

◆ DNS ネガティブキャッシュ時間

DNS のネガティブキャッシュ時間を指定します。デフォルトは 60 秒です。
当該ホストに対して DNS 参照ができなかった場合は、その情報を本設定時間の間保持します。
0 秒から 999 秒までの値で設定することができます。

◆ DNS 応答のソース IP をチェック

DNS 参照時、リクエスト送信先の DNS サーバの IP アドレスと応答を返してきた DNS サーバの IP アドレスが同じであるかをチェックするかどうかを指定します。デフォルトは「する」です。

設定値	説明
する	IP アドレスが異なる場合は、不正な応答と判断します。セカンダリ以降の DNS サーバが存在する場合は、セカンダリ以降の DNS サーバへリトライします。全ての DNS サーバに対してリトライを行っても IP アドレスが異なる場合は、不正な応答と判断します。
しない	IP アドレスが異なる場合でも、応答はそのまま使用されます。 なお、ホスト名と IP アドレスの静的な対応付けは、 「3.5.15. ネットワーク」の hosts 相当(プロキシサービス用)の設定で行うことができます。

◆ FTP(over HTTP)の PASV モード

FTP の PASV モードを有効にするか無効にするかを指定します。デフォルトは「有効にする」です。HTTP でカプセル化された FTP 用の設定です。

設定値	説明
有効にする	設定を有効にします。
無効にする	設定を無効にします。

◆ FTP(over HTTP)のパスワード

anonymous FTP サーバへ接続する場合に、パスワード情報として送信される文字列を指定します。デフォルトは「guest@」です。

通常はメールアドレスを指定することが多いですが、この情報は FTP サーバに送信されるものであるため慎重に設定してください。

64 文字まで設定可能です。

HTTP でカプセル化された FTP 用の設定です。

◆ FTP(over HTTP)のダウンロードサイズの上限値

FTP サーバからのダウンロードサイズの上限値を指定します。(デフォルト:0 KB[無制限])

1KB から無制限までの値で制御することができます。

HTTP でカプセル化された FTP 用の設定です。

◆ Via ヘッダの値

HTTP の Via ヘッダに付加する文字列を指定します。

(初期値は初期導入で設定した本サーバのホスト名です。ただし、本サーバのホスト名を変更した場合はこの値は変更されません。)

Via ヘッダの値として HTTP プロトコルバージョンとここに指定した文字列を付加します。1～255 文字までの値を指定することができます。

「3.2.12. HTTP ヘッダ編集設定」にて Via ヘッダ自体の扱いに関して設定が可能です。

◆ Proxy-Support ヘッダの付加

オリジンサーバからの 401 応答に、
"Proxy-Support: Session-Based-Authentication"を付加するかどうかを指定します。デフォルトは「しない」です。

設定値	説明
しない	Proxy-Support ヘッダを付加しません。
する	指定することで、NTLM 認証(統合 Windows 認証)が必要なサイトへのアクセスが行えるようになります。 プロキシが多段構成となっている場合は、経路上の全てのサーバに対して以下の条件を満たす必要があります。設定を行う前に必ずご確認ください。 InterSec/CS に関しては、以下の条件は満たされています。 ・一経路上の全てのサーバが keep-alive 対応である事 NTLM はセッションセキュリティのプロトコルとなりますので、セッション単位で　認証を行う必要があります。 ・一経路上の全てのサーバが複数のセッションを束ねない事 経路上に複数セッションを束ねるサーバが存在すると、認証していないクライアントが認証済みと認識される可能性があります。

「する」に設定し、クライアントのブラウザ設定にて、ユーザ認証時に自動でログオンする設定にしている場合、信頼できるサイト以外から認証要求があった場合も自動でクライアントの情報が送信されてしまいますのでご注意ください。
一般的なブラウザのデフォルト設定はポップアップが表示される設定となっていますので、意図的に設定を変更しないことを推奨します。

◆ エラーページ用言語

アクセス制限時や内部エラーなど、本サーバにてエラーメッセージを通知する場合に表示する言語を選択します。
アップデートモジュールの適用状態によっては、以下に示す日本語以外の言語を選択できない場合があります。

設定値	説明
日本語	言語を日本語に選択します
英語	言語を英語に選択します

◆ エラーページにプロキシサーバの情報を付加

HTTP アクセスに対して、本サーバ自身がエラーメッセージを生成しエラー応答を返す場合にメッセージの下部に本サーバの情報を付加するかどうかを指定します。デフォルトは「する」です。

設定値	説明
しない	情報を付加しません。
する	情報を付加します。

指定することで、以下の形式にて本サーバの情報がメッセージに付加されます。

形式: Generated ＜日時＞ by ＜本サーバのホスト名＞ (＜製品名＞:＜romaパッケージのバージョン＞)
例: Generated 2015-01-15 18:00:00 by intersec.cs400i2.co.jp (InterSec/CS400i2:roma-12.5-17i)

◆ デバッグログ出力

キャッシュログにデバッグログを出力するか指定します。デフォルトは「OFF」です。

設定値	説明
OFF	デバックログを出力しません。
ON	デバックログを出力します。

OFF に設定してもエラー情報に関してはキャッシュログに出力されます。通常は ON にしないでください。

◆ キャッシュ有効時間

上位サーバ側から有効期限の指定や更新確認の指示がないキャッシュオブジェクトに関する設定を行います。

上位サーバ側へキャッシュの有効性確認を行わずにキャッシュから応答を返す時間を指定します。

0 秒から 99 時間までの値で設定することができます。

デフォルトは 72 時間です。

単位は「時間/分/秒」から選択可能です。

キャッシュした時点から設定された時間が経過する前に当該キャッシュオブジェクトへアクセスが行われた場合、上位サーバ側へキャッシュの有効性確認を行わずキャッシュから応答を返します。

上位サーバ側からの指示やキャッシュ有効時間の設定等とは無関係にキャッシュしない条件を指定したい場合は、「3.2.6. アクセス制御」の「■非キャッシュ設定」を参照してください。

◆ 有効性確認が必要な状態でキャッシュを保持する時間

有効期限が切れたキャッシュオブジェクトに関する設定を行います。
上位サーバ側へキャッシュが有効なのか確認する必要のある状態でキャッシュを保持する時間を指定します。デフォルトは 72 時間です。
0 秒から 99 時間までの値で設定することができます。
単位は「時間/分/秒」から選択可能です。
有効期限が切れた時点から設定された時間の間に当該キャッシュオブジェクトへアクセスが行われた場合、上位サーバ側にキャッシュの有効性を確認し、有効であれば保持しているキャッシュオブジェクトを返します。
有効でなければ、上位サーバ側から返されたオブジェクトをそのままクライアント側に返します。
有効期限に関しては、上位サーバ側から指示されたものかキャッシュ有効時間で指定されたものかの区別はなく、全てのキャッシュオブジェクトに対して有効な設定です。

✓ ボタンの説明

[デフォルト値に戻す]	表示内容をデフォルト値に戻します。 デフォルト値につきましては各項目の説明を参照してください。
[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.6. アクセス制御

リストを設定し、リスト毎にアクセスの制御、キャッシュする/しない、親プロキシを経由する/しない、"no-cache"に対応した処理をする/しないを指定することによりアクセスの制御を行います。

アクセス制御は以下の画面に分かれています。

■リスト設定
■アクセス制御設定
■非キャッシュ設定
■no-cache リクエスト制御設定
■プロキシ転送設定

ヒント

■リスト設定は「3.2.6. アクセス制御」「3.2.11. 特殊アクセス制御」「3.2.12. HTTP ヘッダ編集設定」、「3.2.13. 対上位サーバ向けソース IP 設定」、「3.2.16. HTTPS 可視化アクセス制御設定」で共通となります。

リスト設定

現在設定されているリスト設定の一覧を表示します。

※デフォルト値として予約している(編集、追加不可)リスト名は赤文字で表示されます。

■リスト設定

追加	リスト名	設定種別	条件式
編集 削除	all	src	0.0.0.0/0.0.0.0 0::0/64
編集 削除	cgi	urlpath_regex	\.cgi$ \?
編集 削除	MSIE-SKIP	browser_regex	MSIE
編集 削除	Google-Toolbar	browser_regex	GoogleToolbar

✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

[追加]	リストの追加を行います。→「3.2.6.1. リスト(追加)設定」
[編集]	リストの編集を行います。→「3.2.6.2. リスト(編集)設定」
[削除]	リストの削除を行います。→「3.2.6.3. リストの削除」

◆ リスト名

リスト名を英数字で表示します。大文字と小文字は区別しません。16 文字まで指定可能です。 編集の場合、リスト名の書き換えはできません。

デフォルト値として予約している(編集、追加不可)リスト名は赤文字で表示されます。

ヒント

デフォルトは、各種設定のデフォルトで使用するリストを設定しています。リスト名に"-"が含まれているリストは、デフォルト用のリストとして設定しています。そのため、リスト名に"-"が含まれているリストを作成、編集することはできません。設定されているデフォルトは、モジュールアップデート時、リストの意味合いの変更は行いませんが、内容を変更する可能性があります。

◆ 設定種別

設定種別を表示します。

詳細は、「3.2.6.1. リスト(追加)設定」の設定種別を参照してください。

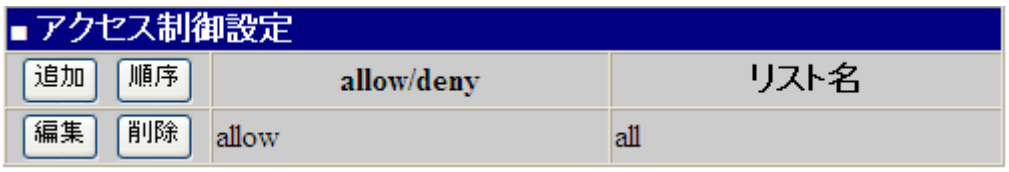
◆ 条件式

条件式は各設定種別に応じた条件式を表示します。

詳細は、「3.2.6.1. リスト(追加)設定」の条件式を参照してください。

アクセス制御設定

リスト毎にアクセスの制御を指定することによりアクセスの制御を行います。



✓ ボタンの説明

[追加]	アクセス制御設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

アクセスの許可/不許可を表示します。

表示	説明
allow	アクセスを許可
deny	アクセスを不許可

◆ リスト名

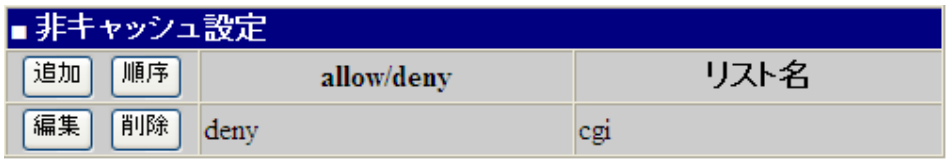
リスト設定で指定したリストの中からアクセスの許可/不許可を指定するリスト名を表示します。
リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

・アクセス制御設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

非キャッシュ設定

リスト設定で設定したリストに対し、キャッシュするかしないかを設定します。



✓ ボタンの説明

[追加]	非キャッシュ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

キャッシュする/しないを表示します。

表示	説明
allow	キャッシュする
deny	キャッシュしない。また、既存のキャッシュも使用しない。

◆ リスト名

リスト設定で指定したリストの中からキャッシュする/しないを指定するリスト名を表示します。
リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

ヒント

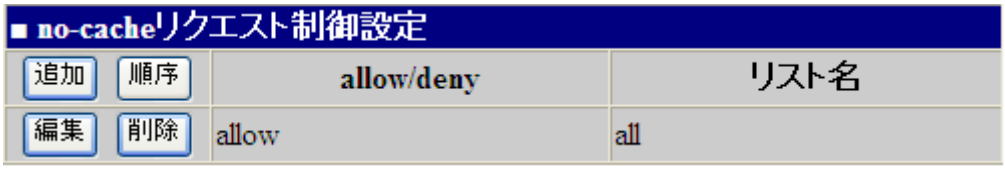
デフォルトの設定値
デフォルトはアクセス先の拡張子が「.cgi」のアクセスをキャッシュしない設定にしています。

重要

・非キャッシュ設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。
・キャッシュに関する基本的な設定は詳細設定を参照してください。

no-cache リクエスト制御設定

リスト設定で設定したリストに対し、リクエストの Cache-Control ヘッダ、または Pragma ヘッダに指定されている"no-cache"に対応した処理をする/しないを設定します。



✓ ボタンの説明

[追加]	no-cache リクエスト制御設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

no-cache に対応した処理をする/しないを表示します。

表示	説明
allow	no-cache に対応した処理をする
deny	no-cache に対応した処理をしない

◆ リスト名

リスト設定で指定したリストの中から no-cache に対応した処理をする/しないを指定するリスト名を表示します。 リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

ヒント

デフォルトの設定値
デフォルトで設定は行われていません。
設定がない場合は、"no-cache"に対応した処理を行います。

重要

・no-cache リクエスト制御設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

プロキシ転送設定

リスト設定で設定したリストに対し、Web サーバへの接続を親プロキシに転送するか/しないか、直接 Web サーバへ転送するか/しないかを指定します。

✓ ボタンの説明

[追加]	プロキシ転送設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ 転送種別

直接 Web サーバへ接続する/直接 Web サーバへ接続しない(親プロキシに転送する)を表示します。

表示	説明
Always_direct	常に、直接 Web サーバへ接続します。
Never_direct	常に、直接 Web サーバへ接続しません。

◆ allow/deny

転送する/しないを表示します。

表示	説明
Allow	転送します。
deny	転送しない。

◆ リスト名

リスト設定で指定したリストの中から直接 Web サーバへ接続する/直接 Web サーバへ接続しない(親プロキシに転送する)を指定するリスト名を表示します。 リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

ヒント

デフォルトの設定値
デフォルトで設定は行われていません。
設定がない場合、親プロキシの設定が行われていれば、基本的に親プロキシ経由で Web サーバへ接続を行いますが、親プロキシが接続できる状態でない場合、直接 Web サーバへ接続します。必ず親プロキシを経由してアクセスさせたい場合は、リスト all に対し、「Never_direct」「allow」を一番下に設定します。

重要

・プロキシ転送設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件との確認は行いません。順番には注意してください。順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

3.2.6.1. リスト(追加)設定

リスト(追加)設定

リストの追加設定を行うことができます。

設定内容は[設定]を押下しないと、システムに反映されません。

- **リスト名**

  リストの名前を入力してください。

  リスト名は、英数字で入力します。大文字と小文字は区別しません。16 文字まで指定可能です。

- **設定種別**

  設定種別を選択します。

  選択可能な設定種別に関しては「条件式」を参照してください。

- **条件式**

  「設定種別」に応じた条件式を入力します。

  区切り文字の空白を使用して複数の条件(値、文字列等)を記述することができます。複数の条件を記述した場合は OR 条件になります。

  条件式は 1024 文字(空白を含む)まで設定が可能です。正規表現を記述した場合は条件 1 つにつき 256 文字まで設定可能です。

  正規表現は POSIX 拡張正規表現を使用してください。

設定種別	条件式
src	本サーバへアクセスを行うホストの IP アドレスを指定します。 (※src/dst/myip 共通) 下記の条件式で単一の IP アドレスのほかにネットワーク、IP アドレスの範囲を設定することが可能です。 **条件式**：all ipaddress ipaddress/mask ipaddress1-ipaddress2 ipaddress1-ipaddress2/mask all を記載した場合、全ての IP アドレスが対象となります。 mask にはマスクビット数で表わすことができる最上位 bit から連続した bit が立つ値を指定してください。 **例**：all 10.32.113.0/24 10.32.113.0/255.255.255.0 10.32.113.1-10.32.113.34/32 10.32.113.1-10.32.113.34/255.255.255.255 2001:db8:20:3:1000:100:20:3 2001:db8:20:3::0/32 2001:db8:20:3:1000:100:20:1-2001:db8:20:3:1000:100:20:50/64
myip	プロキシサービスの待ち受けに設定されている IP アドレスを指定します。 **条件式**：src と同じです。
dst	リクエスト URL 内のドメイン(ホスト)名が IP アドレスの場合に IP アドレスを指定します。 dstdomain とは異なり、IP アドレスは数値として扱われるため IP アドレスの範囲指定が可能です。 **条件式**：src と同じです。

設定種別	条件式
dstdomain	リクエスト URL 内の Web サーバや FTP サーバのドメイン(ホスト)名または IP アドレスを指定します。 文字列として扱うため IP アドレスの範囲指定はできません。 **条件式**：domain ipaddress **例**：example.co.jp 192.168.128.0 2001:db8:20:3:1000:100:20:3
dstdom_regex	リクエスト URL 内の Web サーバや FTP サーバのドメイン(ホスト)名、または IP アドレスを正規表現で指定します。 空欄となる条件式"^$"は設定はできません。 **条件式**：domain ipaddress **例**：mail ※"mail"という文字列を含むホスト名 www.nec.com ※"www.nec.com"、"www%2Enec%2Ecom" という文字列を含むホスト名 ^192¥.168¥.128¥. ※先頭に”192.168.128.”、 "192%2E168%2E128%2E" という文字列を含むホスト名 ^2001:db8:20:3:: ※先頭に” 2001:db8:20:3::.” という文字列を含むホスト名
time	アクセス可、不可の時間を指定します。 **条件式**：曜日 時刻の範囲 曜日指定は下記の文字を使用してください。 S：日曜日 M：月曜日 T：火曜日 W：水曜日 H：木曜日 F：金曜日 A：土曜日 **例**：M T H F 9:00-20:00 日付をまたぐ指定はできません。20:00～02:00 と設定する場合、 20:00～24:00、0:00～2:00 の 2 つのリストを作成してください。

設定種別	条件式
url_regex	URL の正規表現を指定します。 空欄となる条件式"^$"は設定はできません。 "%xx"でエンコードされている部分に関しては文字に変換して比較します。URL のドメイン(ホスト)名部分のみが対象の場合は「dstdom_regex」で設定を行ってください。 **条件式**：URL の正規表現 **例**： ^http://www.nec.com/ ※http://www.nec.com/で始まる URL mail ※"mail"という文字列を含む URL www.nec.com ※"www.nec.com"、"www%2Enec%2Ecom" という文字列を含む URL https 通信の場合、通常は暗号化されているため、URL パス部分は対象になりませんが「3.2.15. HTTPS 可視化機能設定」の「HTTPS 可視化機能を有効に」を「する」と設定することで対象となります。
urlpath_regex	URL のパス部分の正規表現を指定します。 パス部分には、先頭の"/(スラッシュ)"は制御対象に含みません。 例えば、http://www.nec.com/**abc/def** の太字(abc/def)の部分をパスとみなします。"%xx"でエンコードされている部分に関しては文字に変換して比較します。 **条件式**：URL の正規表現 **例**：¥.gif$ ※.gif で終わる URL パス部分 www.nec.com ※"www.nec.com"、"www%2Enec%2Ecom"という文字列を含むパス部分 https 通信の場合、通常は暗号化されているため、URL パス部分は対象になりませんが「3.2.15. HTTPS 可視化機能設定」の「HTTPS 可視化機能を有効に」を「する」と設定することで対象となります。
port	URL 内のポート番号を指定します。 **条件式**：ポート番号 **例**：80
myport	本サーバのポート番号を指定します。 **条件式**：ポート番号 **例**：80
proto	プロトコル種別を HTTP,FTP,NFTP のうちどれか 1 つを指定します。 **条件式**：プロトコル種別 HTTP ※通常の HTTP アクセス FTP ※HTTP でカプセル化された FTP アクセス NFTP ※HTTP でカプセル化されていない FTP アクセス

設定種別	条件式
method	下記のいずれかを指定します。 通常の HTTP アクセス、および、HTTP でカプセル化された FTP アクセスについては RFC2518、2616 で定義されている HTTP メソッドを指定します。 **条件式**：HTTP メソッド名または FTP コマンド名 **例**：CONNECT HTTP でカプセル化されていない FTP アクセスについては RFC959 で定義されている FTP コマンドを指定します。 **条件式**：HTTP メソッド名または FTP コマンド名 **例**：STOR
browser_regex	ブラウザ種別(HTTP リクエストの User-Agent ヘッダのフィールド値)に関する条件を正規表現を用いて指定します。 User-Agent ヘッダの値の先頭から 128 文字までがチェック対象となりますので、その範囲内でチェックが行える条件式を指定してください。 **条件式**：ブラウザ名の正規表現 **例**：^MOZI FTP プロキシ機能を使用した場合のブラウザ名は"roma_nftp"となります。
proxy_auth	ユーザ名を指定します。 **条件式**：ユーザ名 **例**：tarou
proxy_auth_regex	ユーザ名を正規表現を用いて指定します。 空欄となる条件式"^$"は設定はできません。 **条件式**：ユーザ名の正規表現 **例**：^to
cookie_regex	HTTP リクエストの Cookie ヘッダのフィールド値に関する条件を正規表現を用いて指定します。 **条件式**：cookie の正規表現 **例**：ID=name.*
referer_regex	HTTP リクエストの Referer ヘッダのフィールド値に関する条件を正規表現を用いて指定します。 **条件式**：Referer の正規表現 **例**：^http://www.nec.com/

✓ ボタン操作

[設定]	設定値を入力後、[設定]を押下することで、「3.2.6. アクセス制御」のリスト設定にリストを追加し、前画面へ戻ります。
[戻る]	設定内容を保存せず前画面へ戻ります。

3.2.6.2. リスト(編集)設定

リスト編集設定

リスト設定画面にて編集を行いたいリストの編集を行います。
設定内容は[設定]を押下しないと、システムに反映されません。

◆ リスト名

リストの名前を表示します。

◆ 設定種別

設定種別を選択してください。選択する設定種別については「3.2.6.1. リスト(追加)設定」の「設定種別」「条件式」を参照してください。

◆ 条件式

条件式を入力してください。入力する条件式については「3.2.6.1. リスト(追加)設定」の「設定種別」「条件式」を参照してください。

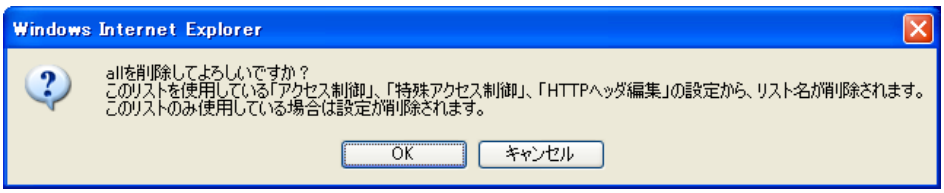
✓ ボタン操作

[設定]	設定値を入力後、[設定]を押下することで、選択したリストの内容を再設定し、前画面へ戻ります。
[戻る]	設定内容を保存せず前画面へ戻ります。

3.2.6.3. リストの削除

リストの削除

リストを削除するには、「3.2.6. アクセス制御」の上画面に表示されている「■リスト設定」画面から削除したいリスト名の左横にある[削除]を押下します。画面に削除するかどうかの確認を求めるダイアログボックスが表示されます。削除する場合は、[OK]を押下してください。



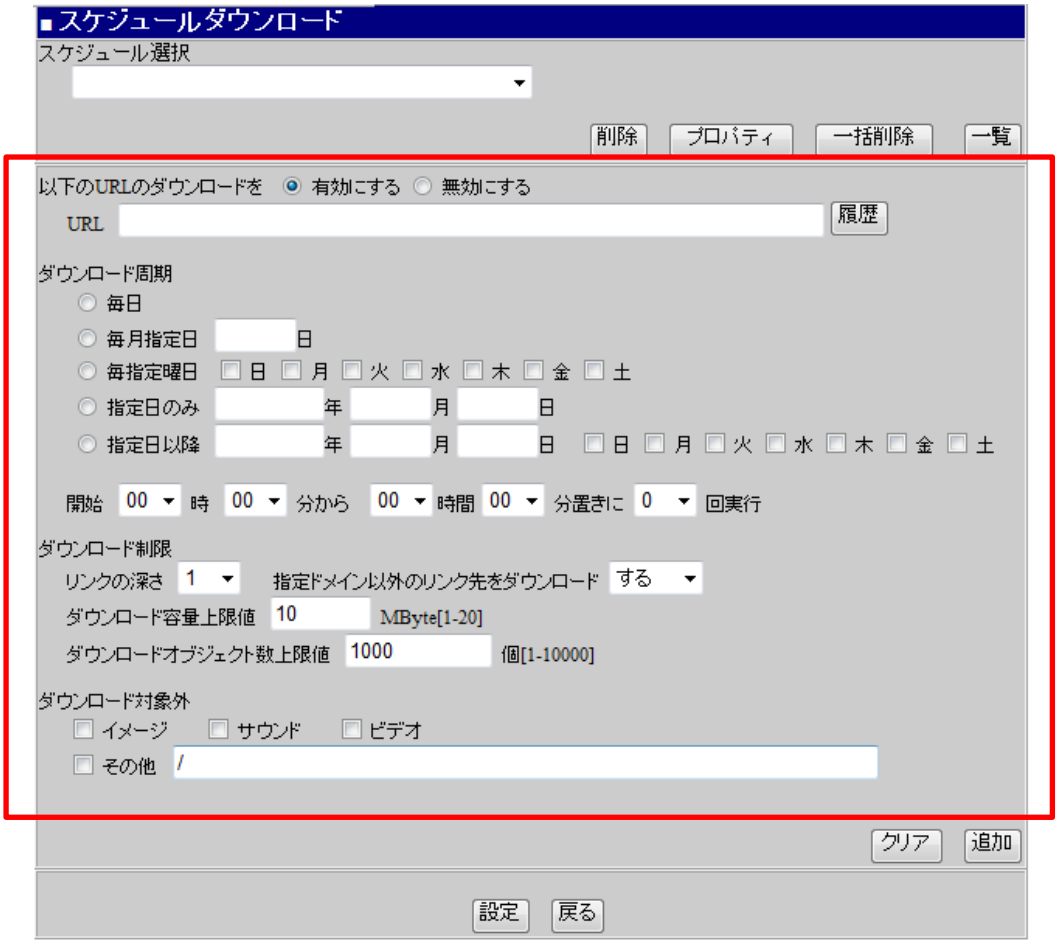
✓ ボタン操作

[OK]	選択したリストを削除し、全画面へ戻ります。
[キャンセル]	削除を行わず、前画面へ戻ります。

3.2.7. スケジュールダウンロード

スケジュールダウンロード

スケジュールダウンロードとは、指定したページをあらかじめ指定時刻にダウンロードし、キャッシュ可能であればキャッシュする機能です。対象となる URL、ダウンロード周期などスケジュールダウンロードの設定ができます。スケジュールは 100 件まで登録が可能です。



重要

・コンテンツの性質とサイズによってはキャッシュされないこともあります。
・対象コンテンツ(URL)がキャッシュ可能である場合は、対象コンテンツへのアクセスがアクセスログのキャッシュステータス結果で HIT になっています。

◆ スケジュール選択

登録されているスケジュールの一覧です。

選択されているスケジュールの詳細が赤枠の画面中央詳細部に表示されます。

✓ ボタンの説明

[削除]	選択したリストを削除します。削除後、[設定]を押下することで反映されます。
[プロパティ]	プロパティを表示します。 →「3.2.7.1. ダウンロードプログラムプロパティ」
[一括削除]	「3.2.7.2. 一括削除設定」へ遷移します。
[一覧]	「3.2.7.3. ダウンロード設定」へ遷移します。

◆ 画面中央詳細部

▶ 以下の URL のダウンロードを [有効にする/無効にする]

ダウンロードスケジュールの有効/無効を設定します。

ダウンロードを実行するときは「有効にする」を、実行しないときは「無効にする」を選んでください。

設定を残したまま(削除せずに)スケジュールダウンロードを実行しないときに「無効にする」を選択します。

➢ URL

ダウンロードの開始位置となる URL を指定します。

✓ ボタンの説明

[履歴]	アクセス頻度の高い URL 一覧画面を表示します。

▶ ダウンロード周期

以下の５種類からダウンロードするタイミングを選択します。

タイミング	説明
毎日	毎日ダウンロードを実行します。
毎月指定日	毎月の指定日にダウンロードを実行します。 月末にダウンロードするときは"31"日と指定してください。
毎指定曜日	毎週指定された曜日にダウンロードを実行します。
指定日のみ	指定された日付のみダウンロードを実行します。
指定日以降	指定された日付以降、毎週指定された曜日にダウンロードを実行します。 日付は 2000 年 1 月 1 日から 2038 年 1 月 19 日の範囲で設定してください。

➢ 開始 xx 時 xx 分から xx 時間 xx 分置きに xx 回実行

スケジュールダウンロードの実行開始時刻、実行間隔、実行回数を指定します。

実行間隔、実行回数 0 を指定すると、開始時刻に 1 回だけダウンロードを実行します。

実行間隔×実行回数は 24 時間以内になるように指定してください。

▶ ダウンロード制限

ダウンロードを行うときの制限事項を指定します。

➢ リンクの深さ

URL 欄の指定位置から何階層分ダウンロードを実行するかを指定します。

➢ 指定ドメイン以外のリンク先をダウンロード

URL 欄に指定したドメイン以外へのリンクに対するダウンロードの指定をします。

「する」を選ぶとリンクの深さで指定した階層分のみ指定ドメイン以外からのダウンロードを実行し、「しない」を選ぶと実行しません。

➢ ダウンロード容量上限値

ダウンロードするオブジェクトの総容量をメガバイト単位で指定します。

1 オブジェクトの容量制限はプロキシの詳細設定の最大キャッシュサイズで設定可能です。

1～20MB の範囲で指定してください。

➢ ダウンロードオブジェクト数上限値

ダウンロードするオブジェクトの総数を指定します。

1～10000 の範囲で指定してください。

▶ ダウンロード対象外

ダウンロードの対象としないオブジェクトの種別を指定します。

以下の 4 種別が指定できます。

種別	説明
イメージ	チェックしたときは以下の拡張子を持つ画像ファイルのダウンロードを実行しません。 .gif, .ief,.jpeg,.jpg,.tiff,.tif,.ras,.pnm,.pbm,.pgm,.ppm,.rgb,.xbm,.xpm,.xwd,.png
サウンド	チェックしたときは以下の拡張子を持つ音声ファイルのダウンロードを実行しません。 .au,.snd,.mp2,.mp3,.aif,.aiff,.aifc,.wav
ビデオ	チェックしたときは以下の拡張子を持つ映像ファイルのダウンロードを実行しません。 .mpeg,.mpg,.mpe,.qt,.mov,.avi,.movie
その他	上記以外の拡張子を持つファイルをダウンロードしないときに設定します。 "/"を区切り文字として最大 10 個まで指定できます。 例えば、.mid、.bmp、.txt をダウンロードしたくないときは以下のように設定します。 /mid/bmp/txt 拡張子は".(ピリオド)"を除き 5 文字分指定できます。

✓ ボタンの説明

[クリア]	詳細部の設定内容を初期状態へ戻します。
[追加]	詳細部の設定内容をスケジュール選択欄に新規登録します。 削除後[設定]を押下することで反映されます。

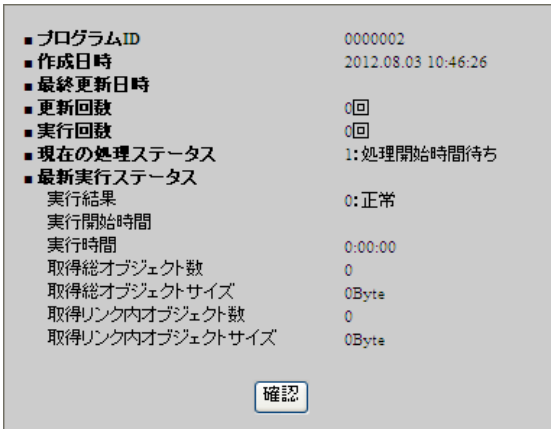
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	設定内容を保存せず前画面へ戻ります。

3.2.7.1. ダウンロードプログラムプロパティ

ダウンロードプログラムプロパティ

スケジュールの設定履歴、最新のダウンロード結果などを表示します。本画面は別ウィンドウで開きます。



- **プログラム ID**

  スケジュールダウンロードの登録 ID です。

- **作成日時**

  スケジュールダウンロードを作成した日時です。

- **最終更新日時**

  スケジュールダウンロードを最後に更新した日時です。

- **更新回数**

  スケジュールダウンロードを更新した回数です。

- **実行回数**

  スケジュールダウンロードを実行した回数です。

- **現在の処理ステータス**

  現在の処理ステータスを表示します。

表示
0:処理無し
1:処理開始時間待ち
2:処理開始待ち
3:全処理終了
256:処理実行中
512:設定エラー

◆ 最新実行ステータス

スケジュールダウンロードの最新の実行結果です。

▶ 実行結果

実行結果を表示します。

正常終了したときは「0：正常」を、エラーがあったときはその他のメッセージが表示されます。

エラーが複数発生したときは最も数値の小さいエラーが一種類表示されます。

表示
0：正常
1：データ(オブジェクト/ページ)が見つからない
2：総オブジェクトサイズ制限
4：総オブジェクト数制限
8：リンクの深さ制限
16：Proxy のアクセス制御による取得失敗
32：Proxy のキャッシュ制限によるキャッシュ失敗
64：取得データのキャッシュ制限によるキャッシュ失敗
128：Proxy の 1 オブジェクトサイズの制限によるキャッシュ失敗

▶ 実行開始時間

最新のダウンロードを開始した時間です。

▶ 実行時間

最新のダウンロードに要した時間です。

▶ 取得総オブジェクト数

最新のダウンロードで取得したオブジェクトの総数です。

▶ 取得総オブジェクトサイズ

最新のダウンロードで取得したオブジェクトの総サイズです。

▶ 取得リンク内総オブジェクト数

最新のダウンロードで取得したオブジェクトのうち、指定 URL 配下の総数です。

▶ 取得リンク内総オブジェクトサイズ

最新のダウンロードで取得したオブジェクトのうち、指定 URL 配下の総サイズです。

✓ ボタンの説明

[確認]	ウィンドウを閉じます。

3.2.7.2. 一括削除設定

一括削除設定

登録されているスケジュールの一覧が表示され、一括で削除することができます。本画面は別ウィンドウで開きます。

- **ID**

  スケジュールダウンロードの登録 ID です。

- **URL**

  ダウンロードの開始位置となる URL です。

  URL 部をクリックすると、新しいウィンドウにリンク先を表示します。

- **削除対象**

  削除するスケジュールダウンロードを指定する選択チェックボックスです。

  チェックされたスケジュールダウンロードが削除対象となります。

設定値	説明
■チェックあり	削除対象とします。
□チェックなし	削除対象としません。

✓ **ボタンの説明**

該当行に対する操作を行うための各種ボタンを表示します。

[更新]	ウィンドウを閉じ、設定結果をスケジュールダウンロード画面のスケジュール選択一覧に反映します。[更新]を押下だけでは、更新結果が反映されないので、反映させる場合は[更新]を押下後、「3.2.7. スケジュールダウンロード」にて[設定]ボタンを押下してください。

3.2.7.3. ダウンロード設定

ダウンロード設定

登録されているスケジュールの一覧が表示され、一括で有効/無効を指定することができます。

◆ ID

スケジュールダウンロードの登録 ID です。

◆ URL

ダウンロードの開始位置となる URL です。

URL 部をクリックすると、新しいウィンドウにリンク先を表示します。

◆ ダウンロード

スケジュールダウンロードの有効/無効を指定する選択チェックボックスです。

チェックされたスケジュールダウンロードが有効となります。

設定値	説明
■チェックあり	スケジュールダウンロードを有効とします。
□チェックなし	スケジュールダウンロードを無効とします。

✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

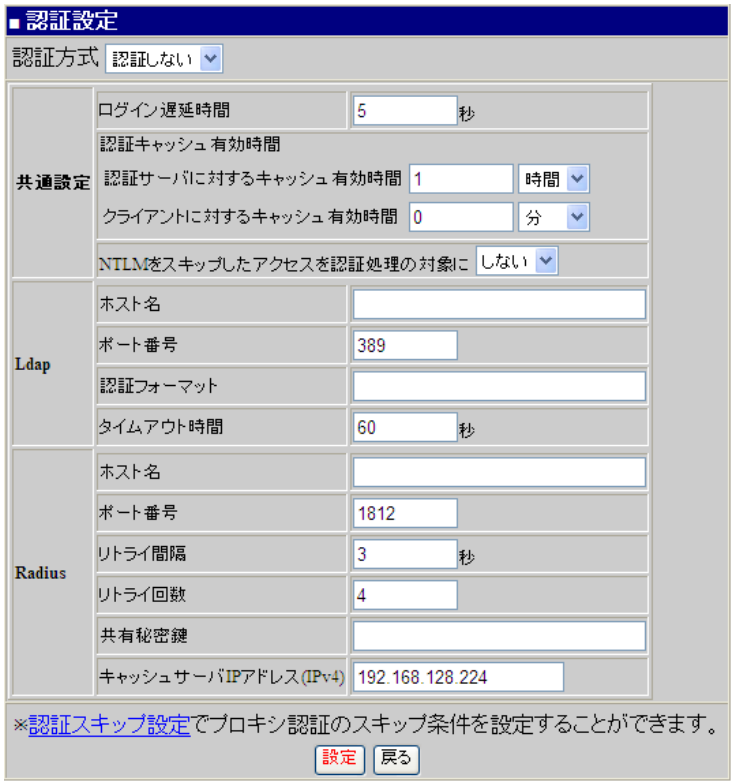
[更新]	ウィンドウを閉じ、設定結果をスケジュールダウンロード画面のスケジュール選択一覧に反映します。[更新]を押下だけでは、更新結果が反映されないので、反映させる場合は[更新]を押下後、「3.2.7. スケジュールダウンロード」にて[設定]ボタンを押下してください。

3.2.8. 認証設定

認証設定

本サーバを使用するユーザを Basic 認証するための設定ができます。

認証方式として、Ldap あるいは Radius のいずれか１つを選択できます。



◆ **認証方式**

ユーザ認証を行うために使用する方式を指定します。

設定値	説明
Ldap	認証方式として Ldap を使用します。
Radius	認証方式として Radius を使用します。
認証しない	ユーザ認証は行いません。

デフォルトは「認証しない」です。 使用可能なユーザ名は 258 文字以内です。

使用可能なパスワードは Ldap の場合 258 文字以内、Radius の場合 128 文字以内です。

アクセスログを拡張形式で取得する場合に出力できる認証ユーザ名は先頭から 63 文字までです。

◆ 共通設定項目

各認証方式で共通な項目の設定を行います。

▶ ログイン遅延時間

Ldap サーバや Radius サーバへのログイン時に認証エラーが発生した場合、クライアント側へのエラーの通知を遅延させる時間を指定します。

ブルートフォース等の攻撃が行われた場合に、短期間で何度も試行することができないようにするために設定に従ってエラーの通知を遅延させます。

1 秒から 99 秒まで指定可能です。デフォルトは 5 秒です。

▶ 認証サーバに対するキャッシュ有効時間

パスワードを本サーバが保持している時間を設定します。

1 分から 99 時間まで指定可能です。デフォルトは 1 時間です。

▶ クライアントに対するキャッシュ有効時間

クライアントの IP アドレスに関連付けたユーザ情報を本サーバが保持している時間を指定します。

0 分から 99 日まで指定可能です。デフォルトは 0 分です。

▶ NTLM をスキップしたアクセスを認証処理の対象にする/しない

NTLM スキップ設定により NTLM の処理を行わなかった場合、当該アクセスを認証処理の対象にする/しないを選択します。

設定値	説明
する	認証処理の対象にします。
しない	認証の対象にしません。

デフォルトは「する」です。

認証スキップ設定によりスキップすると判断したアクセスは、本設定とは関係なくスキップされます。

◆ Ldap

認証方式が Ldap の時の各種設定を指定します。

▶ ホスト名

Ldap サーバのホスト名を指定します。IP アドレスの指定も可能です。

▶ ポート番号

Ldap サーバとの接続に使用するポート番号を指定します。

1 から 65535 まで指定可能です。デフォルトは 389 です。

▶ 認証フォーマット

Ldap で認証を行う際、ユーザ名から「Distinguished Name」に変換するためのフォーマットを指定します。なお、クライアントで指定したユーザ名は、$u に変換されます。最大 500 文字まで指定可能です。

例)cn=$u,　dc=example,　dc=com

Ldap サーバとして「Active Directory」を使用している場合は「ユーザーログオン名」のドメインを指定することも可能です。

例)$u@exsample.co.jp

▶ タイムアウト時間

Ldap サーバとの通信タイムアウト時間を指定します。

1 秒から 99 秒まで指定可能です。デフォルトは 60 秒です。

◆ Radius

認証方式が Radius の時の各種設定を指定します。

▶ ホスト名

Radius サーバのホスト名を指定します。IP アドレスの指定も可能です。

▶ ポート番号

Radius サーバとの接続に使用するポート番号を指定します。

1 から 65535 まで指定可能です。デフォルトは 1812 です。

▶ リトライ間隔

Radius サーバからの応答待ち時間を指定します。

この応答待ち時間が経過しても応答が返らない場合は、リトライを行います。

1 秒から 99 秒まで指定可能です。デフォルトは 3 秒です。

▶ リトライ回数

Radius サーバへのリトライ回数を指定します。指定された回数まで接続を試みます。

1 回から 99 回まで指定可能です。デフォルトは 4 回です。

▶ 共有秘密鍵

Radius サーバと共有する秘密鍵を指定します。

最大 20 文字まで指定可能です。

▶ キャッシュサーバ IP アドレス

Radius サーバと通信を行うための本サーバの IP アドレスを指定します。

本サーバが複数の IP アドレスを指定している場合には、その中で Radius サーバとの通信に使用する IP アドレスを指定します。

FTP プロキシ機能を使用する場合の認証方法
本サーバまたは ICAP 版 InterSafe WebFilter で認証設定を行っていて FTP プロキシ機能を使用する場合、以下のシーケンスで FTP コマンドを送信することでオリジンサーバとの認証情報を区別することができます。
パターン１(USER コマンドを使用する方法)
1) 本サーバへ FTP 接続
2) USER および PASS コマンドで本サーバへの認証情報を送信
3) 「オリジンサーバのユーザ名@オリジンサーバ名」形式のパラメータを指定した USER コマンドを送信後、PASS コマンドでオリジンサーバのパスワードを指定
4) オリジンサーバへログイン完了
パターン２(SITE コマンドを使用する方法)
1) 本サーバへ FTP 接続
2) USER および PASS コマンドで本サーバへの認証情報を送信
3) SITE コマンドでオリジンサーバを指定
4) オリジンサーバへの接続が完了したら、再度 USER/PASS コマンドを使用し、オリジンサーバの認証情報を送信
FTP クライアントソフトウェアの種類(Windows コマンドプロンプトでの FTP コマンド等)によっては SITE コマンドをサポートしていない場合があります。
この場合は上記パターン１を使用してください。

・プロキシ認証に対応していないクライアントに対応させるなど、特定アクセスに対して認証を行わないような設定を認証スキップ設定のリンクから行うことができます。
・NTLM 機能と認証(Ldap/Radius)の両方を使用する場合、認証の処理が実行されるのは以下のアクセスのみです。
1) NTLM スキップ設定に従い、NTLM 機能をスキップしたアクセス。
2) NTLM 設定の「Ldap/Radius を行う」を選択した条件に該当するアクセス。
・NTLM スキップ設定をしたアクセスを認証の対象にしたくない場合は認証スキップにも NTLM スキップと同じ条件を追加してください。

✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

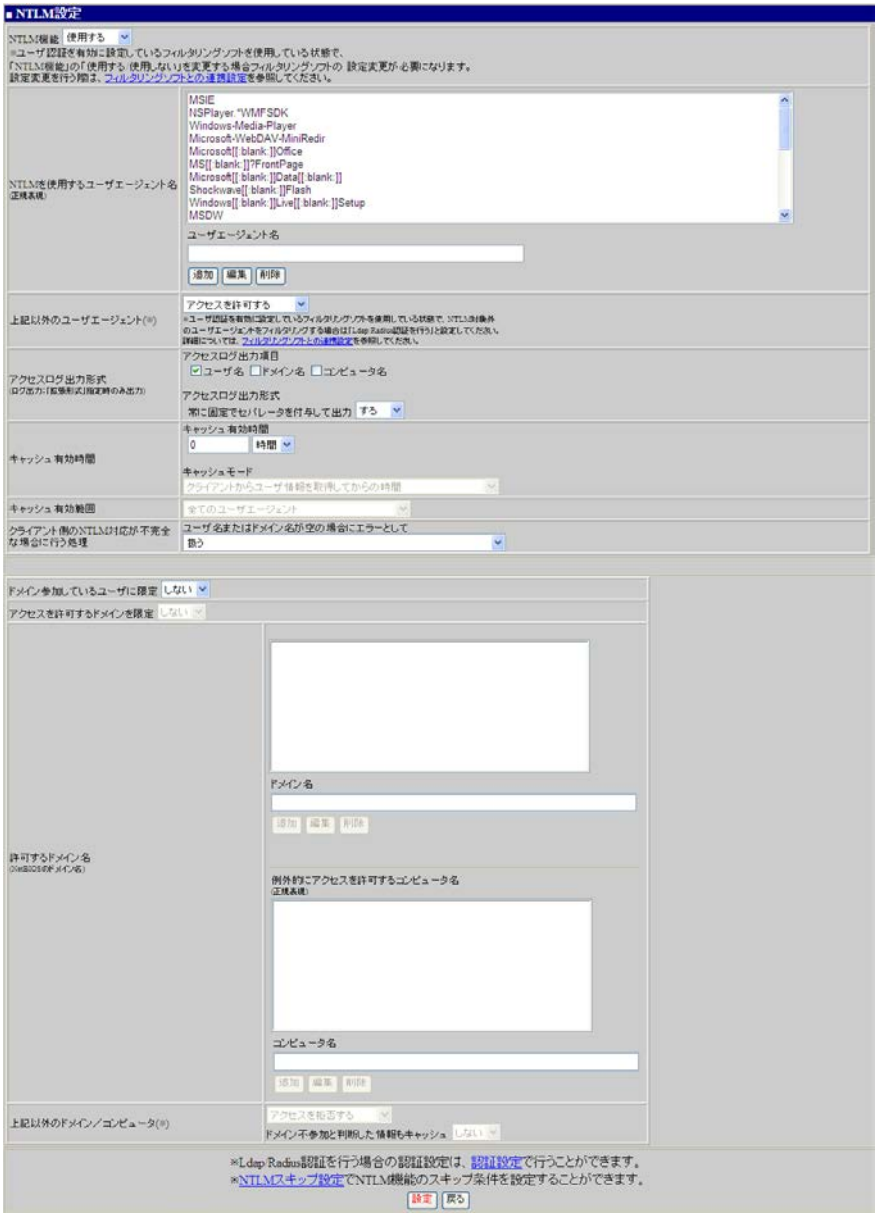
[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.9. NTLM 設定

NTLM 設定

本サーバで NTLM 機能を使用するための設定を行います。

透過型アクセスおよび FTP(HTTP でカプセル化された FTP アクセス)、NFTP(HTTP でカプセル化されていない FTP アクセス)では NTLM 機能を使用できません。



◆ NTLM 機能

NTLM 機能を使用するかを選択します。

「3.2.1. 基本設定」で「サーバ種別設定」を「Forward」に設定している場合のみ NTLM 機能を使用できます。デフォルトは「使用しない」です。

設定値	説明
使用する	NTLM 機能を使用します。
使用しない	NTLM 機能を使用しません。

ユーザ認証を有効に設定しているフィルタリングソフトを使用している状態で NTLM 機能の設定を変更する場合は、フィルタリングソフトと NTLM 機能の設定の同期が取れていないとフィルタリングが正しく動作しません。

NTLM 機能を使用する場合は、下記の項目について設定します。

◆ NTLM を使用するユーザエージェント名

NTLM 機能を使用するユーザエージェント名を正規表現で指定します。

設定できる条件は最大 255 文字です。

デフォルトは以下の条件を満たしたユーザエージェント名を設定しています。

実際にログオンしているクライアントのユーザ情報(ユーザ ID、パスワード、コンピュータ名、ドメイン名)を NTLM で通知するクライアント AP。
一般的に使用されているクライアント AP の中で 2014 年 1 月時点で上記の動作確認ができているもの

新たにユーザエージェント名を追加する場合は、クライアント AP の正常動作確認後本サーバに追加してください。

クライアント AP には一部の処理のみ NTLM に対応しているものもありますので注意して設定を行ってください。

▶ ユーザエージェント名

NTLM 機能を使用するユーザエージェント名を正規表現で指定します。

✓ ボタンの説明

[追加]	ユーザエージェント名の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択したユーザエージェント名の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択したユーザエージェント名の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ 上記以外のユーザエージェント

NTLM を使用するユーザエージェント名で指定した以外のユーザエージェントについてのアクセス可否を指定します。

デフォルトは「アクセスを許可する」です。

設定値	説明
アクセスを許可する	NTLM を使用するユーザエージェント名で指定した以外のユーザエージェントのアクセスを許可します。
アクセスを拒否する	NTLM を使用するユーザエージェント名で指定した以外のユーザエージェントのアクセスを拒否します。
Ldap/Radius 認証を行う	アクセスを許可する上で Ldap/Radius 認証を行います。

Ldap/Radius 認証を行う場合は、「3.2.8. 認証設定」から設定します。

ユーザ認証を有効に設定しているフィルタリングソフトを使用している状態で、フィルタリングソフトにユーザ名を送信する必要がある場合、ICAP サーバ設定でダミーのユーザ名を送信することが可能です。

設定の詳細は、「3.2.20. ICAP サーバ設定」を参照してください。

◆ アクセスログ出力形式

アクセス情報としての出力項目を選択及びアクセスログへの出力形式を選択します。

▶ アクセスログの出力項目

アクセスログへ出力する出力項目(ユーザ名/ドメイン名/コンピュータ名)を選択します。

デフォルトは「ユーザ名」のみ選択です。

本項目は、キャッシュサーバアクセスログの出力形式として「拡張形式」を指定した場合のみ出力されます。

キャッシュサーバアクセスログの出力形式を指定する場合は、「3.5.12. ログ管理」のキャッシュサーバアクセスログ設定より設定します。

▶ アクセスログ出力形式

アクセスログの「認証ユーザ名」に、アクセスログの出力項目で選択したユーザ名、ドメイン名、コンピュータ名を出力する際の出力形式を選択します。

デフォルトは「する」です。

設定値	説明
する	常に【ユーザ名¥ドメイン名¥コンピュータ名】の形式で出力します。アクセスログ出力項目の設定にかかわらずセパレータとして「¥」を２つ付加します。アクセスログの出力項目にて「ユーザ名」「コンピュータ名」を選択した場合、【ユーザ名¥¥コンピュータ名】で出力します。
しない	アクセスログ出力項目で選択した項目の間にのみセパレータとして「¥」を付加します。「ユーザ名」「コンピュータ名」を選択した場合、【ユーザ名¥コンピュータ名】の形式で出力します。

◆ キャッシュ有効時間

▶ キャッシュ有効時間

クライアントのIPアドレスに関連付けたユーザ情報を本サーバが保持している時間を設定します。

1分から99時間まで指定可能です。デフォルトは「0時間」です。

尚、本有効時間は「ユーザ情報を取得した時刻からの有効時間」となっています。有効時間が経過するまでは取得されたユーザ情報は更新されません。

そのため、キャッシュ有効時間の設定によって古い情報が使用されることがあります。有効時間以降にアクセスが行われるとユーザ情報を取得しなおします。

複数のクライアントにて1つのIPアドレスを利用する場合は、本有効時間は「0」に設定してください。

▶ キャッシュモード

キャッシュ有効時間の意味を下記から選択します。

デフォルトは「クライアントからユーザ情報を取得してからの時間」です。

・クライアントからユーザ情報を取得してからの時間

最後にNTLMのやり取りによりクライアント側からユーザ情報を取得した時刻がキャッシュ有効時間の基点となります。

・クライアントまたはキャッシュからユーザ情報を取得してからの時間

クライアントからユーザ情報を取得してからの時間のタイミングに加え、キャッシュからユーザ情報を取得した場合にも基点の時刻を更新します。

◆ キャッシュ有効範囲

キャッシュの有効範囲を指定します。

デフォルトは「全てのユーザエージェント」です。

設定値	説明
全てのユーザエージェント	「3.2.11. 特殊アクセス制御」の「NTLMスキップ設定」で、「deny」の対象になっていないアクセスに対してキャッシュを使用します。
使用するユーザエージェントのみ	「NTLMを使用するユーザエージェント名」で設定したユーザエージェントのみキャッシュを使用します。
全てのアクセス (NTLMスキップの対象も含む)	「3.2.11. 特殊アクセス制御」の「NTLMスキップ設定」で「deny」の対象となっているアクセスに対してもキャッシュを使用します。

◆ クライアント側の NTLM 対応が不完全な場合に行う処理

クライアント側のソフトが一応は NTLM に対応した動作をしているが、その動作になんらかの問題がある場合にどうするか処理の工程を選択します。

▶ ユーザ名またはドメイン名が空の場合にエラーとして

クライアント側から送付されたユーザ情報の内、ユーザ名またはドメイン名が空だった場合の処理を下記から選択します。デフォルトは「扱う」です。

選択肢	説明
扱う	エラーとします
扱わない(通常通りキャッシュする)	通常通りキャッシュします
扱わない(ユーザ名が空の場合のみキャッシュしない)	ユーザ名が空の場合のみキャッシュしません
扱わない(ユーザ名またはドメイン名が空の場合にキャッシュしない)	ユーザ名またはドメイン名が空の場合はキャッシュしません

◆ ドメイン参加しているユーザに限定

NTLM 機能を使用するユーザについて、ドメインに参加しているユーザに限定するかを選択します。 デフォルトは「しない」です。

設定値	説明
する	ドメイン参加しているユーザに限定する。
しない	ドメイン参加しているユーザに限定しない。

ドメイン参加しているユーザに限定する場合は、下記の項目について設定します。

◆ アクセスを許可するドメインを限定

ドメイン参加しているユーザに限定した上で、ドメインまで限定するかを選択します。
デフォルトは「しない」です。
許可するドメインを限定する場合は、許可するドメイン名(NetBIOS のドメイン名)について設定します。

設定値	説明
する	参加しているドメインを限定する。
しない	参加しているドメインを限定しない。

◆ 許可するドメイン名(NetBIOS のドメイン名)

アクセスを許可するドメイン名(NetBIOS)を指定します。
ドメイン名は、最大 64 文字まで指定可能となっておりますが、「NetBIOS 名の文字数は最長で 15 文字まで」の仕様から 16 文字以降の文字列については、チェック対象外となります。
従いまして、上記アクセスログに出力されるドメイン名につきましても、「15 文字まで」となります。

➢ ドメイン名

アクセスを許可するドメイン名(NetBIOS)を指定します。

✓ ボタンの説明

[追加]	ドメイン名の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択したドメイン名の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択したドメイン名の削除を行います。削除後、[設定]を押下することで内容を反映します。

▶ 例外的にアクセスを許可するコンピュータ名

上記で指定したドメインには参加してはいないものの、例外的にアクセスを許可するコンピュータ名を正規表現で指定します。

上記ドメイン名同様、最大 64 文字まで指定可能となっておりますが、16 文字以降の文字列については、チェック対象外となり、アクセスログに出力されるコンピュータ名につきましても、「15 文字まで」となります。

➢ コンピュータ名

ドメインには参加してはいないものの、例外的にアクセスを許可するコンピュータ名を正規表現で指定します。

✓ ボタンの説明

[追加]	コンピュータ名の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択したコンピュータ名の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択したコンピュータ名の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ 上記以外のドメイン/コンピュータ

「許可するドメイン名(NetBIOS のドメイン名)」で指定した以外のドメイン/コンピュータについてのアクセス可否を指定します。

デフォルトは「アクセスを拒否する」です。

設定値	説明
アクセスを拒否する	アクセスを拒否します。
Ldap/Radius 認証を行う	NTLM 認証はアクセス許可し、Ldap/Radius 認証を行います。 Ldap/Radius 認証は「3.2.8. 認証設定」から設定します。

▶ ドメイン不参加と判断した情報もキャッシュする/しない

ドメイン不参加と判断した場合にユーザ情報をキャッシュする/しないを選択します。

デフォルトは「しない」です。

設定値	説明
する	ドメイン不参加と判断した場合にユーザ情報をキャッシュします。
しない	ドメイン不参加と判断した場合にユーザ情報をキャッシュしません。

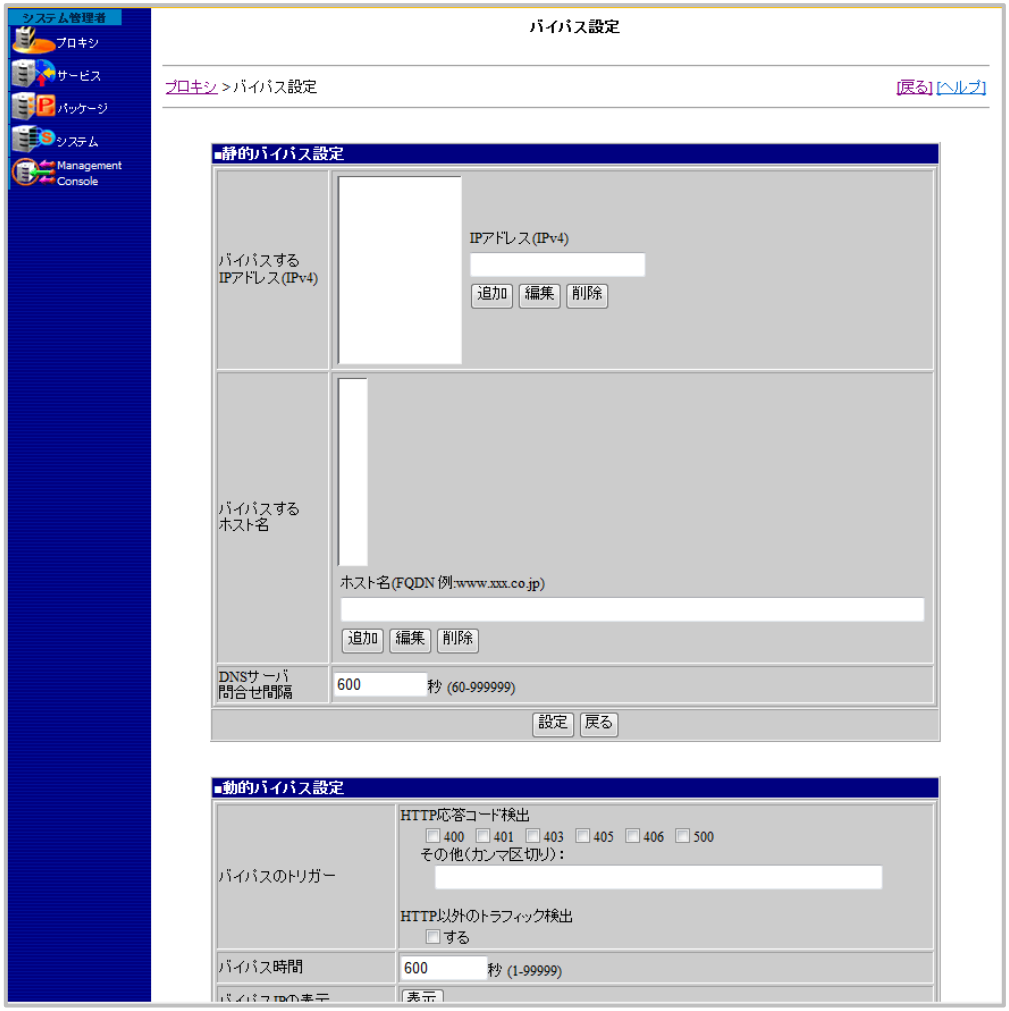
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.10. バイパス設定

システムを透過型プロキシとして動作させる際の、静的バイパス・動的バイパスの設定を行います。

「3.2.1. 基本設定」の「サーバ種別設定」にて「Forward(透過型Ｌ４スイッチ)」を選択している場合のみ有効な設定です。

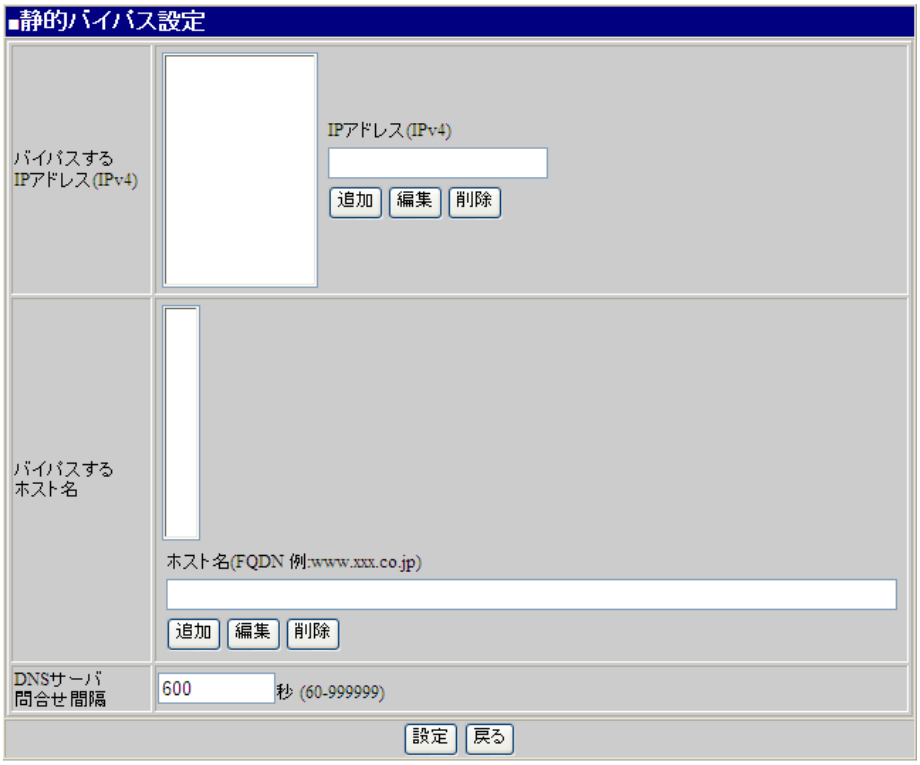


バイパス設定は以下の画面に分かれています。

■静的バイパス設定
■動的バイパス設定

静的バイパス設定

ホストの IP アドレス/ホスト名を指定して静的にバイパスを行います。
下記の追加/編集/削除の操作を行った場合であっても、静的バイパス用の「設定」を押下するまではサーバに設定内容は反映されません。



◆ バイパスする IP アドレス(IPv4)

静的にバイパスを行うホストの IP アドレス一覧が表示されます。
一覧に表示されている IP アドレスを選択すると、右の IP アドレス(IPv4)に選択された IP アドレスが表示されます。この IP アドレスを編集後に[編集]を押下することで設定内容が変更されます。
また、IP アドレスの追加を行う場合は、IP アドレス(IPv4)を入力後に、[追加]を押下してください。これにより、一覧に新たな IP アドレスが表示されます。最大 256 まで登録可能です。
IP アドレスの削除を行う場合は、削除したい IP アドレスを選択後に[削除]を押下してください。

▶ IP アドレス(IPv4)

IP アドレスを指定します。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ バイパスするホスト名

静的にバイパスを行うホスト名一覧が表示されます。

一覧に表示されているホスト名を選択すると、下のホスト名(FQDN)欄に選択されたホスト名が表示されます。このホスト名を編集後に[編集]を押下することで設定内容が変更されます。

また、ホスト名の追加を行う場合は、ホスト名を入力後に[追加]を押下してください。これにより、一覧に新たなホスト名が表示されます。最大 256 まで登録可能です。

ホスト名の削除を行う場合は、削除したいホスト名を選択後に[削除]を押下してください。

▶ ホスト名(FQDN 例:www.xxx.co.jp)

ホスト名(FQDN)を指定します。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ DNS サーバ問い合わせ間隔

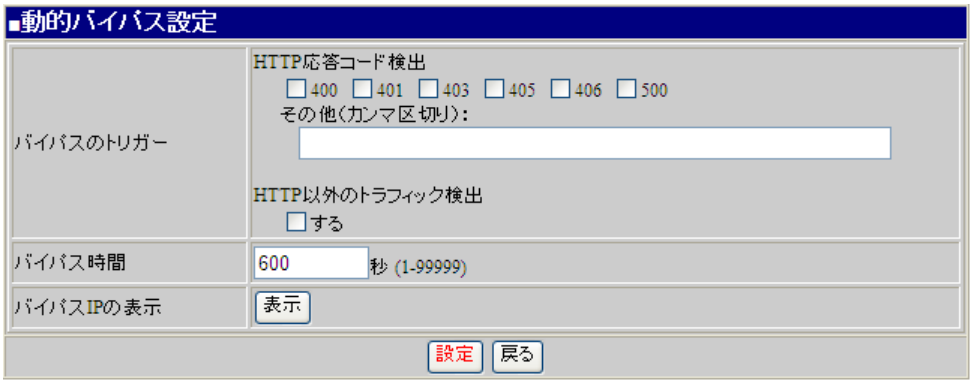
静的バイパスの設定をホスト名で行った場合、そのホスト名に対応する IP アドレスを DNS サーバに問い合わせる間隔を指定します。秒単位で指定してください。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

動的バイパス

動的にバイパスを行います。



◆ バイパスのトリガー

バイパスを行う条件を指定します。

▶ HTTP 応答コード検出

HTTP の応答コードの種類でバイパスを行います。条件に加える応答コードをチェックしてください。また、表示されていないコードを加える場合は、その他(カンマ区切り)欄に、コードの数値をカンマ区切りで入力してください。

▶ HTTP 以外のトラフィック検出

HTTP 以外のトラフィックをバイパスする場合はチェックを付けてください。

◆ バイパス時間

動的にバイパスを行う時間を指定します。秒単位で指定してください。

◆ バイパス IP の表示

現在バイパスされている IP アドレスまたはホスト名の表示を行います。

✓ ボタンの説明

[表示]	現在バイパスされている IP アドレスまたはホスト名を表示します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.11. 特殊アクセス制御

各種例外設定を行います。デフォルトで一部設定を行っています。

特殊アクセス制御は以下の画面に分かれています。

■リスト設定
■認証スキップ設定
■NTLM スキップ設定
■URL フィルタスキップ設定
■ICAP ボディ転送スキップ設定
■Keep-Alive 接続設定(クライアント側設定)
■Keep-Alive 接続設定(サーバ側設定)
■Keep-Alive 接続設定(データ読み飛ばし設定)
■Keep-Alive 接続設定(判断基準設定)
■Keep-Alive 接続設定(HTTP バージョン設定)
■Keep-Alive 接続設定(Connection ヘッダパラメータ設定)

■リスト設定は「3.2.6. アクセス制御」「3.2.11. 特殊アクセス制御」「3.2.12. HTTP ヘッダ編集設定」「3.2.13. 対上位サーバ向けソース IP 設定」「3.2.16. HTTPS 可視化アクセス制御設定」で共通となります。

リスト設定

現在設定されているリスト設定の一覧を表示します。

※デフォルト値として予約している(編集、追加不可)リスト名は赤文字で表示されます。

■リスト設定

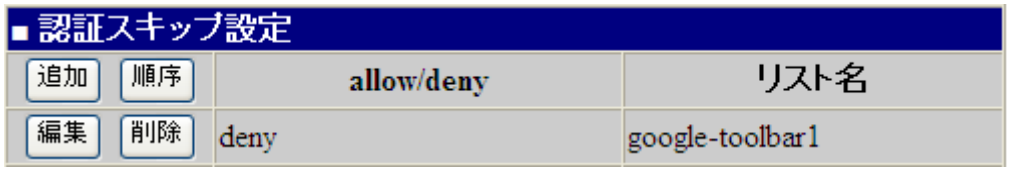
追加	リスト名	設定種別	条件式
編集 削除	all	src	0.0.0.0/0.0.0.0 0::0/64
編集 削除	cgi	urlpath_regex	\.cgi$ \?
編集 削除	MSIE-SKIP	browser_regex	MSIE
編集 削除	Google-Toolbar	browser_regex	GoogleToolbar

リスト設定は「3.2.6. アクセス制御」のリスト設定と共通となっています。

「3.2.6. アクセス制御」のリスト設定を参照ください。

認証スキップ設定

リスト設定で設定したリストに対し、認証処理を行う/行わない(allow/deny)を設定します。



✓ ボタンの説明

[追加]	認証スキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(認証する)、deny(認証しない)を表示します。

認証機能を使用している場合は、全てのアクセスに対して認証を行います。

本機能は、例外の指定としてご利用ください。

表示	説明
allow	認証する
deny	認証しない

◆ リスト名

リスト設定で指定したリストの中から、認証する/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞

認証の対応が不可もしくは不十分な特定のクライアント AP のアクセスは基本的にスキップの対象となります。

ただし、ユーザエージェントのみが条件ではセキュリティに問題があるため、デフォルトは他の条件と組み合わせて、範囲の絞込みが行えるアクセスを認証処理を行わない設定にしています。

他の条件と組み合わせて絞込みが行えないアクセスに関しては、環境に合わせて設定を追加してください。

例えば、"NSPlayer"は認証に対応していないクライアント AP ですが、他の条件と組み合わせて絞込みが行えないためデフォルトに設定しておりません。

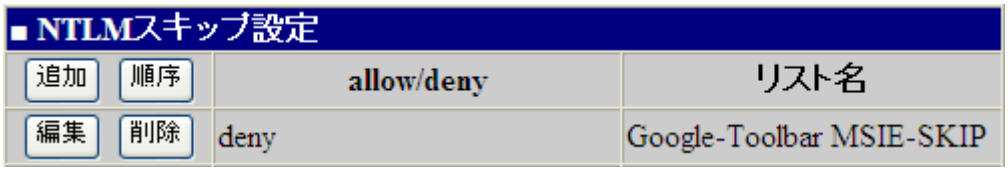
デフォルト値はバージョンによって異なる場合があります。

重要

・認証をスキップ設定したアクセスは、アクセスログに認証ユーザ名を出力させることができません。
・認証スキップ設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
・順番の変更はアクセス制御画面の「順序」ボタンを押すと出て来る編集画面で変更できます。
・設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。
・NTLM 機能と認証(Ldap/Radius)の両方を使用する場合、認証の処理が実行されるのは以下のアクセスのみです。
  1) NTLM スキップ設定に従い、NTLM 機能をスキップしたアクセス。
  2) 「3.2.9. NTLM 設定」で「Ldap/Radius を行う」を選択した条件に該当するアクセス。
・NTLM スキップ設定をしたアクセスを認証の対象にしたくない場合は認証スキップ設定にも NTLM スキップ設定と同じ条件を追加してください。

NTLM スキップ設定

リスト設定で設定したリストに対し、NTLM 処理を行う/行わない(allow/deny)を設定します。



✓ ボタンの説明

[追加]	NTLM スキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(NTLM 機能を使用する)、deny(NTLM 機能を使用しない)を表示します。

NTLM 機能を使用している場合は、「3.2.9. NTLM 設定」の「NTLM を使用するユーザエージェント名」で設定している全てのユーザエージェントに対して NTLM 処理を行います。

本機能は、例外の指定としてご利用ください。

表示	説明
allow	NTLM 機能を使用する
deny	NTLM 機能を使用しない

◆ リスト名

リスト設定で指定したリストの中から、NTLM 機能を使用する/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞

NTLM 設定の"NTLM を使用するユーザエージェント名"に設定されているデフォルトで、NTLM に対応しているクライアント AP を絞り込んでいます。

しかし、NTLM の対象となっているクライアント AP の中で一部のアクセスが NTLM に対応していない場合があります。

デフォルトは NTLM の対象となっているクライアント AP の中で、NTLM に対応していない一部のアクセスに対して NTLM 処理を行わない設定にしています。

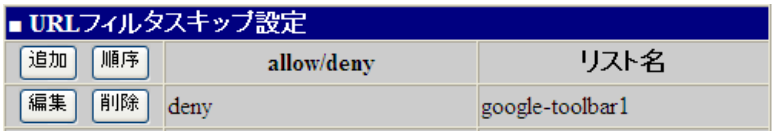
デフォルト値はバージョンによって異なる場合があります。

重要

- NTLM 機能をスキップしたアクセスは、アクセスログに NTLM ユーザ情報を出力させることができません。
- NTLM スキップ設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
- 順番の変更はアクセス制御画面の「順序」ボタンを押すと出て来る編集画面で変更できます。
- リスト設定の内容は、画面上部のリスト設定画面に表示しています。
- 設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。
- NTLM 機能と認証(Ldap/Radius)の両方を使用する場合、認証の処理が実行されるのは以下のアクセスのみです。
  1) NTLM スキップ設定に従い、NTLM 機能をスキップしたアクセス。
  2) 「3.2.9. NTLM 設定」で「Ldap/Radius を行う」を選択した条件に該当するアクセス。
- NTLM スキップ設定をしたアクセスを認証の対象にしたくない場合は認証スキップ設定にも NTLM スキップ設定と同じ条件を追加してください。

URL フィルタスキップ設定

リスト設定で設定したリストに対し、URL フィルタソフトでのフィルタリングを行う/行わない(allow/deny)を設定します。



✓ ボタンの説明

[追加]	URL フィルタスキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(フィルタリングする)、deny(フィルタリングしない)を表示します。

URL フィルタリングソフトを使用している場合は、全てのアクセスに対してフィルタリングを行います。

本機能は、例外の指定としてご利用ください。

表示	説明
allow	フィルタリングする
deny	フィルタリングしない

◆ リスト名

リスト設定で指定したリストの中から、フィルタリングする/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞
フィルタリングソフトでユーザ認証を行うことを想定し、デフォルトの設定を行っています。セキュリティを考慮し、デフォルトは下記の条件を満たすアクセスに対して、フィルタリングを行わない設定にしています。
・ユーザ情報の取得ができない(NTLM 及び認証への対応が不可もしくは不十分)アクセス
・条件を組み合わせて等フィルタリング処理を行わない範囲の絞込みが可能
・フィルタリング処理を行わなくても問題ないと思われるアクセス
例えば、上記の条件を満たすアクセスは、"Windows Update"が該当します。
上記の条件を満たしていないアクセスに対しては、環境に合わせて設定を追加してください。デフォルト値はバージョンによって異なる場合があります。
「3.2.16. ICAP サーバ設定」でダミーのユーザ名を送信する機能を使用する場合、デフォルト値又同様の目的で設定した値が不要になります。

・URL フィルタをスキップしたアクセスは、アクセスログにフィルタ結果、フィルタカテゴリを出力させることができません。
・URL フィルタスキップ設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
・順番の変更はアクセス制御画面の「順序」ボタンを押すと出て来る編集画面で変更できます。
・設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

ICAP ボディ転送スキップ設定

リスト設定で設定したリストに対し、ICAP ボディを転送する/転送しない(スキップする)(allow/deny)を設定します。

✓ ボタンの説明

[追加]	ICAP ボディ転送スキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(転送する)、deny(転送しない)を表示します。

「3.2.20. ICAP サーバ設定」で「ICAP サーバへボディを転送する」設定をしている場合は、全ての POST/PUT リクエストのボディを転送します。

特定の条件に該当するリクエストのボディを転送したくない場合に本機能をご利用ください。

表示	説明
allow	転送する
deny	転送しない

◆ リスト名

リスト設定で指定したリストの中から、フィルタリングする/しないを指定するリスト名を選択します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

ヒント

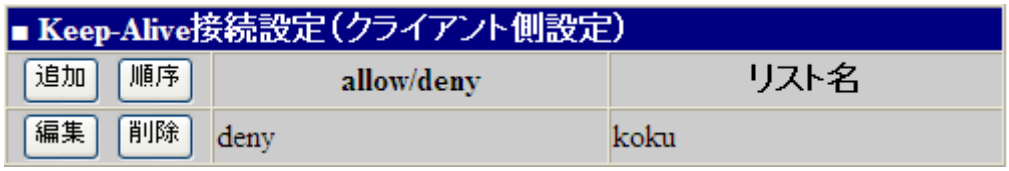
＜デフォルトの設定値に関して＞
デフォルトは設定されていないため、全ての POST/PUT リクエストのボディを転送します。

重要

・ICAP ボディ転送スキップ設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
・順番の変更はアクセス制御画面の「順序」ボタンを押すと出て来る編集画面で変更できます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

Keep-Alive 接続設定(クライアント側設定)

CS とクライアント側との接続で Keep-Alive 接続の指定があったときに、Keep-Alive を使用するかしないかを設定します。



✓ ボタンの説明

[追加]	Keep-Alive 接続設定(クライアント側設定)設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(Keep-Alive を使用する)、deny(Keep-Alive を使用しない)を表示します。

表示	説明
allow	CS とクライアント側との接続で Keep-Alive を使用する
deny	CS とクライアント側との接続で Keep-Alive を使用しない

◆ リスト名

リスト設定で指定したリストの中から、Keep-Alive を使用する/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、CS とクライアント側との接続で Keep-Alive 接続を使用する動作となります。

Keep-Alive 接続設定(サーバ側設定)

CS と上位サーバ側との接続で Keep-Alive 接続の指定があったときに、Keep-Alive を使用するかしないかを設定します。

✓ ボタンの説明

[追加]	Keep-Alive 接続設定(サーバ側設定)設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(Keep-Alive を使用する)、deny(Keep-Alive を使用しない)を表示します。

表示	説明
allow	CS と上位サーバ側との接続で Keep-Alive を使用する
deny	CS と上位サーバ側との接続で Keep-Alive を使用しない

◆ リスト名

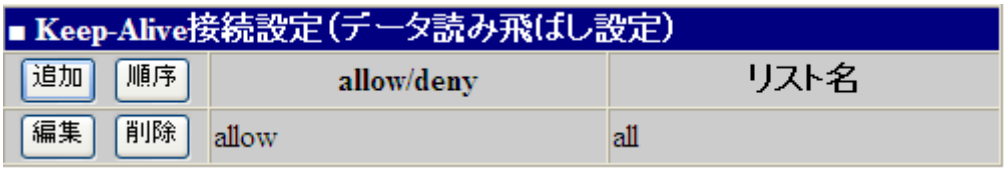
リスト設定で指定したリストの中から、Keep-Alive を使用する/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、CS と上位サーバ側との接続で Keep-Alive 接続を使用する動作となります。

Keep-Alive 接続設定(データ読み飛ばし設定)

リクエストの転送前に、上位サーバ側から送られてくる不正(余分)なデータを読み飛ばすことができます。



✓ ボタンの説明

[追加]	Keep-Alive 接続設定(データ読み飛ばし設定)設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(不正(余分)なデータを読み飛ばす)、deny(不正(余分)なデータを読み飛ばさない)を表示します。

表示	説明
allow	上位サーバ側から送られてくる不正(余分)なデータを読み飛ばす
deny	上位サーバ側から送られてくる不正(余分)なデータを読み飛ばさない

◆ リスト名

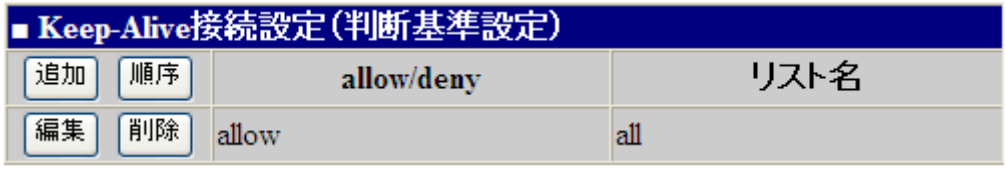
リスト設定で指定したリストの中から、不正(余分)なデータを読み飛ばす/読み飛ばさないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、上位サーバ側から送られてくる不正(余分)なデータを読み飛ばさない動作となります。

Keep-Alive 接続設定(判断基準設定)

Keep-Alive 接続を使用するかどうか決定する際に、FQDN を基準として使用するかどうかを指定します。



✓ ボタンの説明

[追加]	Keep-Alive 接続設定(判断基準設定)設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。
[追加]	アクセス制御設定の追加を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(FQDN を基準として使用する)、deny(FQDN を基準として使用しない)を表示します。

表示	説明
allow	FQDN を基準として使用する
deny	FQDN を基準として使用しない

◆ リスト名

リスト設定で指定したリストの中から、FQDN を基準として使用する/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、Keep-Alive 接続を使用するかどうか決定する際に、FQDN を基準として使用する動作となります。

Keep-Alive 接続設定(HTTP バージョン設定)

HTTP/1.0 で受けたリクエストを HTTP/1.1 に変換して転送するかどうかを指定します。

✓ ボタンの説明

[追加]	Keep-Alive 接続設定(HTTP バージョン)設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(アップグレードを行う)、deny(アップグレードを行わない)を表示します。

表示	説明
allow	アップグレードを行う(HTTP/1.1 に変換する)
deny	アップグレードを行わない(HTTP/1.1 に変換しない)

◆ リスト名

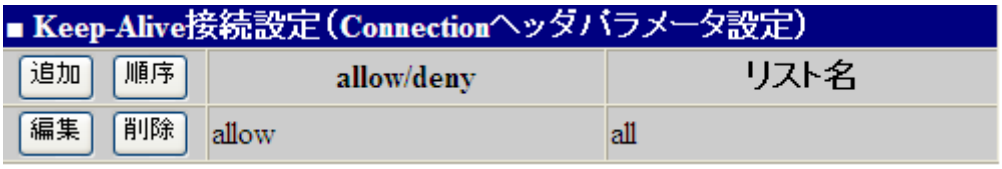
リスト設定で指定したリストの中から、HTTP/1.0 で受けたリクエストを HTTP/1.1 に変換して転送する/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、アップグレードを行う(HTTP/1.1 に変換する)動作となります。

Keep-Alive 接続設定(Connection ヘッダパラメータ設定)

Connection ヘッダに記載されている CS が解釈しないパラメータ値を削除するかどうかを指定します。



✓ ボタンの説明

[追加]	Keep-Alive 接続設定(Connection ヘッダパラメータ)設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(削除しない)、deny(削除する)を表示します。

表示	説明
allow	Connection ヘッダに記載されている CS が解釈しないパラメータ値を削除しない
deny	Connection ヘッダに記載されている CS が解釈しないパラメータ値を削除する

◆ リスト名

リスト設定で指定したリストの中から、Connection ヘッダに記載されている CS が解釈しないパラメータ値を削除する/しないを指定するリスト名を表示します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

ヒント

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、Connection ヘッダに記載されている CS が解釈しないパラメータ値を削除する動作となります。

重要

- 設定の追加を行いたい場合には各設定の[追加]ボタンを押してください。
- 設定の編集を行いたい場合には編集したい項目横の[編集]ボタンを押してください。
- 設定の削除を行いたい場合には各項目横の[削除]ボタンを押してください。
- 上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件との確認は行いません。
- 順序を変更を行いたい場合には[順序]ボタンを押して開く画面で順序を変更してください。

3.2.12. HTTP ヘッダ編集設定

HTTP ヘッダの扱いに関する設定を行います。

HTTP ヘッダ編集は以下の画面に分かれています。

■リスト設定
■X-Forwarded-For ヘッダ非付加設定
■Via ヘッダ非付加設定
■Via ヘッダ削除設定
■(任意のヘッダ名)ヘッダ削除設定

「■リスト設定」は「3.2.6. アクセス制御」「3.2.11. 特殊アクセス制御」「3.2.12. HTTP ヘッダ編集設定」「3.2.13. 対上位サーバ向けソース IP 設定」「3.2.16. HTTPS 可視化アクセス制御設定」で共通となります。

リスト設定

現在設定されているリスト設定の一覧を表示します。

※デフォルト値として予約している(編集、追加不可)リスト名は赤文字で表示されます。

■ リスト設定

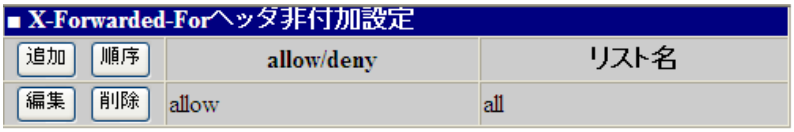
追加	リスト名	設定種別	条件式
編集 削除	all	src	0.0.0.0/0.0.0.0 0::0/64
編集 削除	cgi	urlpath_regex	\.cgi$ \?
編集 削除	MSIE-SKIP	browser_regex	MSIE
編集 削除	Google-Toolbar	browser_regex	GoogleToolbar

リスト設定は「3.2.6. アクセス制御」のリスト設定と共通となっています。

「3.2.6. アクセス制御」のリスト設定を参照ください。

X-Forwarded-For ヘッダ非付加設定

「3.2.5. 詳細設定」の「クライアント IP の通知」で「する」と設定している状態で直接 Web サーバへアクセスを行う場合、リスト設定で設定したリストに対して、X-Forwarded-For ヘッダを付加する/しない(allow/deny)を指定します。



✓ ボタンの説明

[追加]	X-Forwarded-For ヘッダ非付加設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(付加する)、deny(付加しない)を表示します。

表示	説明
allow	X-Forwarded-For ヘッダを付加する。
deny	X-Forwarded-For ヘッダを付加しない。

◆ リスト名

リスト設定で指定したリストの中から、付加する/しないを指定するリスト名を選択します。
リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

ヒント

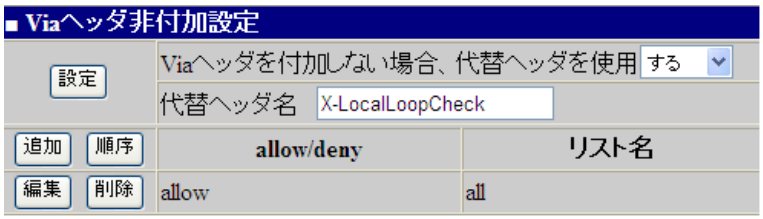
＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、「3.2.5. 詳細設定」の「クライアント IP の通知」で「する」と設定している状態で直接 Web サーバへアクセスする全てのアクセスに対して X-Forwarded-For ヘッダを付加します。

重要

- X-Forwarded-For ヘッダ非付加設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
- 順番の変更はアクセス制御画面の[順序]ボタンを押すと出て来る編集画面で変更できます。
- 設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。
- リスト設定の内容は、画面上部のリスト設定画面に表示しています。

Via ヘッダ非付加設定

リスト設定で設定したリストに対して、Via ヘッダを付加する/しない(allow/deny)を指定します。
また、Via ヘッダを付加しない場合に代替ヘッダを使用するかしないか、代替ヘッダ名の設定を行います。



✓ ボタンの説明

[設定]	「Via ヘッダを付加しない場合、代替ヘッダを使用する/しない」「代替ヘッダ名」の設定内容を入力し[設定]を押下することで、Via ヘッダ非付加設定を行います。
[追加]	Via ヘッダ非付加設定のリストの追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ Via ヘッダを付加しない場合、代替ヘッダを使用する/しない

Via ヘッダを付加しない場合に代替ヘッダを使用するかしないかを指定します。

設定値	説明
する	代替ヘッダを使用する
しない	代替ヘッダを使用しない

◆ 代替ヘッダ名

Via ヘッダの代わりに付加するヘッダ名を入力します。
空白文字、":"を含む文字列を設定することはできません。
また、削除ヘッダに設定しているヘッダ名を設定することはできません。
1～20 文字までの値を指定することができます。

◆ allow/deny

allow(付加する)、deny(付加しない)を表示します。

表示	説明
allow	Via ヘッダを付加する
deny	Via ヘッダを付加しない

◆ リスト名

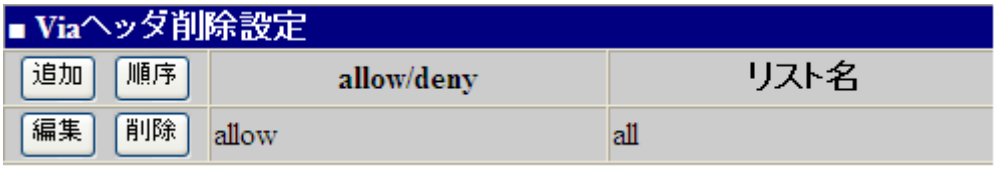
リスト設定で指定したリストの中から、付加する/しないを指定するリスト名を選択します。
リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

・Via ヘッダ非付加設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
・順番の変更はアクセス制御画面の[順序]ボタンを押すと出て来る編集画面で変更できます。
・設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

Via ヘッダ削除設定

リスト設定で設定したリストに対して、Via ヘッダを削除するかしないかを指定します。



✓ ボタンの説明

[追加]	Via ヘッダ削除設定のリストの追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

allow(削除しない)、deny(削除する)を指定します。

表示	説明
allow	Via ヘッダを削除しない
deny	Via ヘッダを削除する

◆ リスト名

リスト設定で指定したリストの中から、削除しない/するを指定するリスト名を選択します。
リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、Via ヘッダは削除しない動作となります。

・Via ヘッダ削除設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
・順番の変更はアクセス制御画面の[順序]ボタンを押すと出て来る編集画面で変更できます。
・設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。
・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

(任意のヘッダ名)ヘッダ削除設定

空欄のテキストボックスに削除対象のヘッダ名を入力し[追加]を押して条件を記載したリストを指定すると当該ヘッダの削除設定が作成されます。

✓ ボタンの説明

[追加]	(任意のヘッダ名)ヘッダ削除設定のリストの追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

追加された当該ヘッダの削除設定は「■via ヘッダ削除設定」と同様の操作が可能です。また、リスト設定を全て削除した場合、追加を行った当該ヘッダ削除設定の画面も削除されます。

例えばテキストボックスに「Referer」と入力し[追加]を押下した場合、「■Referer ヘッダ削除設定」が作成され、Referer ヘッダに関する条件の設定が可能になります。

追加可能なヘッダ削除設定は最大 32 個までです。(Via ヘッダ削除設定を含む)
リスト設定で設定したリストに対して、設定した任意のヘッダを削除しない/する (allow/deny)を指定します。

◆ allow/deny

allow(削除しない)、deny(削除する)を指定します。

表示	説明
allow	設定した任意のヘッダを削除しない
deny	設定した任意のヘッダを削除する

◆ リスト名

リスト設定で指定したリストの中から、削除しない/するを指定するリスト名を選択します。
リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

ヒント

＜デフォルトの設定値に関して＞
デフォルトは設定されておらず、設定した任意のヘッダは削除しない動作となります。

重要

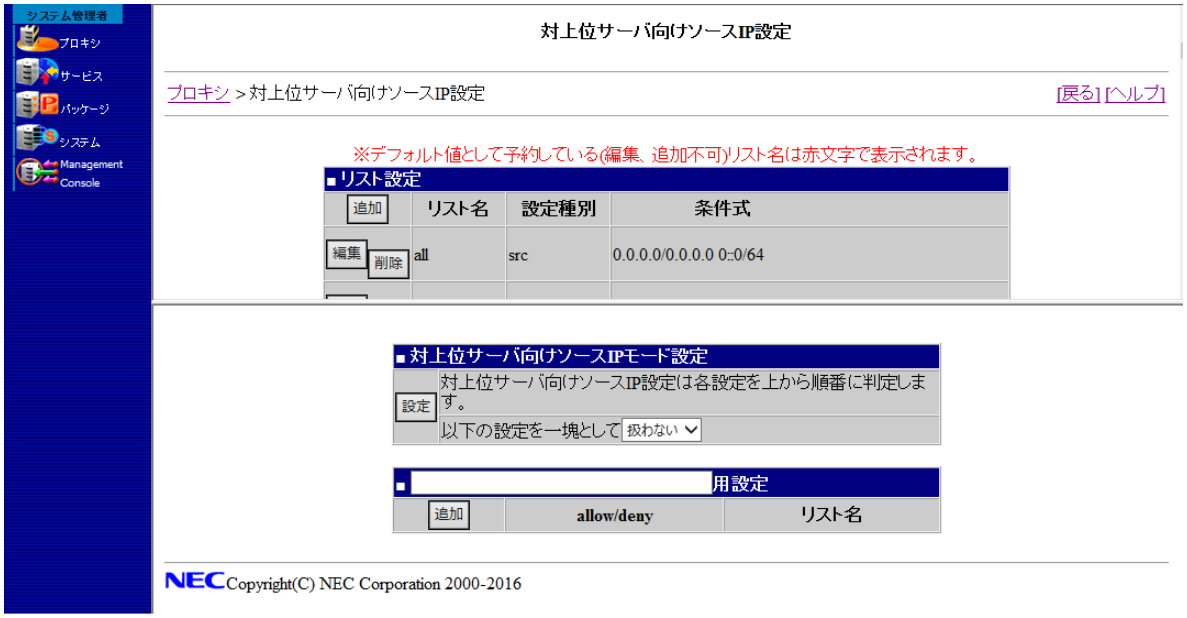
- (任意のヘッダ名)削除設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
- 順番の変更はアクセス制御画面の[順序]ボタンを押すと出て来る編集画面で変更できます。
- 設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。
- リスト設定の内容は、画面上部のリスト設定画面に表示しています。

3.2.13. 対上位サーバ向けソース IP 設定

HTTP、HTTPS、FTP over HTTP アクセスに対して上位サーバへアクセスするソース IP の例外設定を行います。

セッションベースで処理を行いますので、セッションを維持(keep-alive)している場合、セッション確立後の最初のアクセスでのみ条件判断を行います。

Revers プロキシとして使用している場合、HTTPS に関しては SSL アクセラレータ経由のアクセスのみが対象となります。



対上位サーバ向けソース IP 設定は以下の画面に分かれています。

■リスト設定
■対上位サーバ向けソース IP モード設定
■(IP アドレス)用設定

リスト設定

現在設定されているリスト設定の一覧を表示します。

※デフォルト値として予約している(編集、追加不可)リスト名は赤文字で表示されます。

■ リスト設定

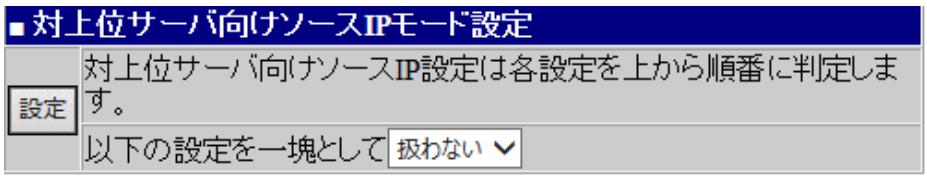
追加	リスト名	設定種別	条件式
編集 削除	all	src	0.0.0.0/0.0.0.0 0::0/64
編集 削除	cgi	urlpath_regex	\.cgi$ \?
編集 削除	MSIE-SKIP	browser_regex	MSIE
編集 削除	Google-Toolbar	browser_regex	GoogleToolbar

リスト設定は「3.2.6. アクセス制御」のリスト設定と共通となっています。

「3.2.6. アクセス制御」のリスト設定を参照ください。

対上位サーバ向けソース IP モード設定

以下の設定([IP アドレス]用設定)を一塊として扱う/扱わないを設定します。



✓ ボタンの説明

[設定]	「以下の設定を一塊として扱う/扱わない」の設定内容を入力し[設定]を押下することで、対上位サーバ向けソース IP モードの設定を行います。

「扱う」場合は「allow」の条件に該当した場合も、以降の判定を行わず、通常の実 IP アドレスがソース IP になります。

「扱わない」場合は「allow」の条件に該当した場合、次の IP アドレスの判定処理以降を継続します。

いずれの場合も「deny」に該当した場合、該当した IP アドレスがソース IP になります。

◆ 以下の設定を一塊として扱う/扱わない

以下の設定を一塊として扱う/扱わないを設定します。デフォルトは「扱わない」です。

設定値	説明
扱う	「allow」の条件に該当した場合も、以降の判定を行わず、通常の実 IP アドレスがソース IP になります。 「deny」に該当した場合、該当した IP アドレスがソース IP になります。
扱わない	「allow」の条件に該当した場合、次の IP アドレスの判定処理以降を継続します。 「deny」に該当した場合、該当した IP アドレスがソース IP になります。

(IP アドレス)用設定

空欄に上位サーバへアクセスするソース IP を入力し「追加」ボタンを押して条件を記載したリストを指定すると当該ソース IP 用設定が作成されます。

✓ ボタンの説明

[追加]	(IP アドレス)用設定のリストの追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

例： 「192.168.0.1」と入力した場合、「192.168.0.1 用設定」が作成され、「192.168.0.1」を上位サーバへアクセスするソース IP とする条件の設定が可能になります。

追加可能な対上位サーバ向けソース IP は最大 256 個までです。

◆ allow/deny

「allow」は「対上位サーバ向けソース IP モード設定」の設定によって動作が変わります。
「deny」は該当した IP アドレスをソース IP として使用します。

表示	説明
allow	「対上位サーバ向けソース IP モード設定」を「扱う」と設定している場合は「allow」の条件に該当した場合も、以降の判定を行わず、通常の実 IP アドレスがソース IP になります。 「扱わない」と設定している場合は「allow」の条件に該当した場合、次の IP アドレスの判定処理以降を継続します。
deny	該当した IP アドレスをソース IP として使用する

◆ リスト名

リスト設定で指定したリストの中から、上位サーバへアクセスするソース IP を指定するリスト名を選択します。

リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

＜デフォルトの設定値に関して＞

デフォルトは設定されておらず、通常の実 IP アドレスがソース IP になります。

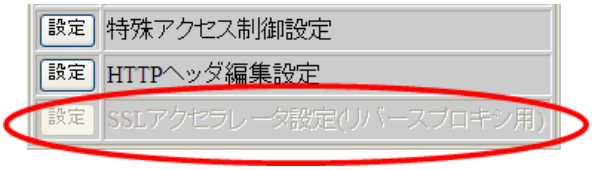
・順番の変更はアクセス制御画面の[順序]ボタンを押すと出て来る編集画面で変更できます。

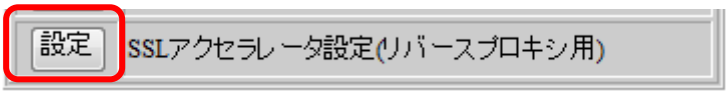
・「対上位サーバ向けソース IP モード設定」を「扱う」に設定し、設定の一番上に「allow/deny」に allow、「リスト名」に all を設定することで既存の設定を無効にすることができます。

・リスト設定の内容は、画面上部のリスト設定画面に表示しています。

3.2.14. SSL アクセラレータ設定(リバースプロキシ用)

リバースプロキシサーバで SSL アクセラレータ機能を使用する設定を行います。本機能は、オプション機能です。SSL アクセラレータライセンスがインストールされていない場合、「3.2. プロキシ」の「■プロキシサーバ設定」画面は以下の図の通り選択できない状態になっています。使用するためには、SSL アクセラレータライセンスをインストールしてください。



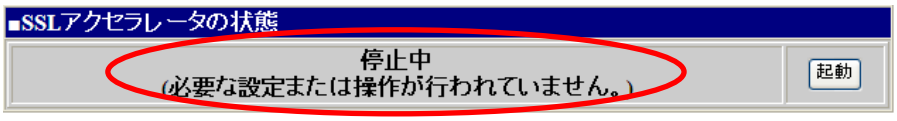


SSL アクセラレータ設定(リバースプロキシ用)は以下の画面に分かれています。

■SSL アクセラレータの状態
■SSL アクセラレータ設定

SSL アクセラレータの状態

SSL アクセラレータの起動状態を表示します。



状態(赤枠箇所)については、以下の組み合わせで表示します。

SSL アクセラレータの状態	待ち受け設定の有無(*1)	説明
起動中 (最新の設定で稼動中です。)	有り	最新の設定で SSL アクセラレータが稼動しています。
起動中 (最新の設定で稼動していません。)	有り	SSL アクセラレータで使用していない待ち受けが存在する状態で、稼動しています。設定した待ち受けを SSL アクセラレータで使用する場合は、「■SSL アクセラレータ設定」の[設定]、または本画面の[再起動]で SSL アクセラレータの再起動を行ってください。
	無し	SSL アクセラレータの設定変更後、SSL アクセラレータを再起動していないため変更前の設定で稼動しています。SSL アクセラレータの再起動を行った場合、設定不足のため SSL アクセラレータは停止します。
停止中 (必要な設定または操作が行われていません。)	有り	必要な設定を行った後、SSL アクセラレータを起動していません。現在の設定で SSL アクセラレータを起動させる場合は、「■SSL アクセラレータ設定」の[設定]、または本画面の[起動]を押下してください。
	無し	必要な設定が行われていないため、SSL アクセラレータが停止しています。必要な設定を行い、「■SSL アクセラレータ設定」の[設定]を押下してください。
停止中 (設定または SSL アクセラレータに異常が発生しました。)	有り	設定または SSL アクセラレータに異常があるため停止しています。設定または登録した証明書等を確認し、異常の原因を解決後に SSL アクセラレータの再起動を行ってください。

(*1) 「■SSL アクセラレータ 設定」でのアクセラレータ待ち受け設定に赤文字で表示の IP アドレス/TCP ポート番号の有無

チェック

本設定画面以外から設定及び SSL 証明書等を変更した場合は、SSL アクセラレータの再起動を行うまで起動状態にずれが生じる場合があります。

✓ ボタンの説明

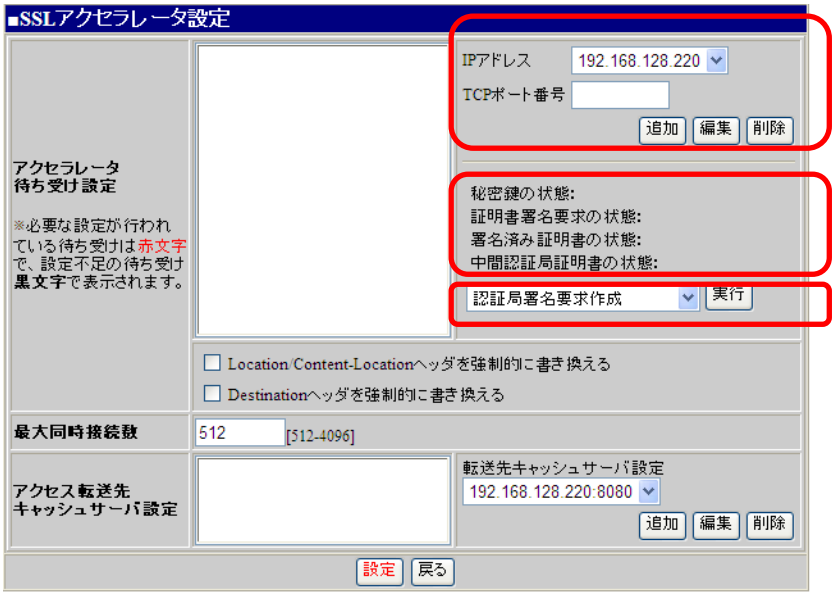
[起動]	SSL アクセラレータの起動を行います。
[再起動]	SSL アクセラレータの再起動を行います。

SSL アクセラレータが未起動時は[起動]、起動時は[再起動]が表示されます。

SSL アクセラレータ設定

SSL アクセラレータの待ち受けに対して、秘密鍵、証明書署名要求、署名済み証明書、中間認証局証明書の作成/登録を行います。

アクセラレータ待ちうけ設定に対してアクセス転送先キャッシュサーバの設定を行います。



①アクセラレータ
待ち受けに関する情報

②サーバ証明に関する情報

③証明書に関する操作

既存の秘密鍵、証明書の更新、インポートを行う際は「3.2.14.1. SSL 証明書更新手順」「3.2.14.2. SSL 証明書インポート手順」を参照してください。

◆ アクセラレータ待ち受け設定

以下で示す SSL アクセラレータの起動に必要な設定が行われている待ち受けは、設定済みの情報として赤文字で中央に表示されます。設定不足の場合は、黒文字のままとなります。

- IP アドレス/TCP ポート番号が設定済み
- 秘密鍵の状態、証明書署名要求の状態、署名済み証明書の状態が作成済み
- アクセス転送先分散グループ設定が設定済み

チェック

カーソルで選択(反転)している待ち受けは白文字で表示されるため、文字の色で状態の判別はできませんのでご注意ください。

▶ ①アクセラレータ待ち受けに関する情報

➢ IP アドレス

SSL アクセラレータ機能がクライアントからの HTTPS 接続を受け入れる待ち受け IP アドレスをプルダウンメニューから選択します。

➢ TCP ポート番号

SSL アクセラレータ機能がクライアントからの HTTPS 接続を受け入れる待ち受け TCP ポート番号を設定します。

✓ **ボタンの説明**

[追加]	設定した IP アドレス：ポート番号を待ち受けとして追加します。
[編集]	アクセラレータ待ち受け設定の一覧で選択した待ち受け IP アドレス：ポート番号を、新しい IP アドレス：ポート番号に編集(変更)します。
[削除]	アクセラレータ待ち受け設定の一覧で選択した待ち受け IP アドレス：ポート番号を削除します。

チェック

- 設定できる待ち受けは最大 16 個までです。
- 「3.2.1.2. 基本設定(Reverse)」のキャッシュサーバ設定で使用している IP アドレスと TCP ポート番号の組み合わせは設定できません。

▶ ②サーバ証明書に関する情報

リストから選択された IP アドレス、TCP ポート番号の SSL アクセラレータが使用するサーバ証明書に関する現在の状態が表示されます。待ち受け設定を追加後にサーバ証明書に関する操作を行ってください。

- 秘密鍵の状態

  当該待ち受け設定に対する、秘密鍵が存在する場合は作成済、存在しない場合は未作成と表示されます。

表示	説明
作成済	秘密鍵が存在する
未作成	秘密鍵が存在しない。

- 証明書署名要求の状態

  当該待ち受け設定に対する、証明書署名要求が存在する場合は作成済、存在しない場合は未作成と表示されます。

表示	説明
作成済	証明書署名要求が存在する
未作成	証明書署名要求が存在しない。

- 署名済み証明書の状態

  当該待ち受け設定に対する、署名済み証明書が存在する場合は作成済、存在しない場合は未作成と表示されます。

表示	説明
作成済	署名済み証明書が存在する
未作成	署名済み証明書が存在しない。

- 中間認証局証明書の状態

  当該待ち受け設定に対する、中間認証局証明書が存在する場合は作成済、存在しない場合は未作成と表示されます。

表示	説明
作成済	中間認証局証明書が存在する
未作成	中間認証局証明書が存在しない。

▶ ③証明書に関する操作

当該待ち受け設定に対して、実行する操作を選択します。

設定値	説明
認証局署名要求作成	秘密鍵と証明書署名要求を作成します。
署名済み証明書登録	認証局によって署名された証明書を登録します。
中間認証局証明書登録	認証局によって発行された中間認証局証明書を登録します。
自己署名証明書作成	自己で署名した、公的には証明されない証明書を作成します。 公的な認証局に署名要求書を提出している場合は、これを実行しないでください。認証局に署名された証明書が無効になります。
証明書署名要求表示	証明書署名要求を表示します。 署名済み証明書情報表示、当該待ち受け設定に対する署名済み証明書に関する情報を表示します。
署名済み証明書状態表示	署名済み証明書に関する情報を表示します。
中間認証局証明書情報表示	中間認証局証明書に関する情報を表示します。
証明書署名要求削除	秘密鍵と証明書署名要求を削除します。 公的な認証局に署名要求書を提出している場合は、これを実行しないでください。認証局に署名された証明書が無効になります。
署名済み証明書削除	署名済み証明書を削除します。
中間認証局証明書削除	中間認証局証明書を削除します。

チェック

秘密鍵、証明書署名要求、署名済み証明書、中間認証局証明書の削除を行った場合は、実際には削除せず以下のファイル名で「/opt/nec/roma/etc/bak_cert/配下」に移動させます。元に戻す場合は、「3.2.14.2. SSL 証明書インポート手順」を参考にしてください。

[ファイル名の規則]

秘密鍵：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).key

証明書署名要求：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).csr

署名済み証明書：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).crt

中間認証局証明書：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).mid

上記の待ち受けの IP アドレス/TCP ポート番号は秘密鍵、証明書署名要求、署名済み証明書、中間認証局証明書を使用していた設定になります。

✓ ボタンの説明

[実行]	上記③証明書に関する操作で選択している操作を実行します。

▶ Location/Content-Location ヘッダを強制的に書き換える

HTTP 応答内の当該ヘッダでアクセス転送先サーバ自身または間違ったプロトコル指定でのリスナが指している場合にヘッダを書き換えるかを設定します。

設定値	説明
■チェックあり	ヘッダを書き換えます。
□チェックなし	ヘッダを書き換えません。

例)ホスト名が「www.nec.co.jp(IP アドレス：192.168.0.1)」でアクセス転送先サーバの待ち受け(IP アドレス：192.168.0.1)で書き換えを行う場合、以下のように書き換えを行います。

変更前：Location: http://www.nec.co.jp/

変更後：Location: https://www.nec.co.jp/

▶ Destination ヘッダを強制的に書き換える

WebDAV で定義されている Destination ヘッダの URL を正しいプロトコルでアクセス転送先キャッシュサーバ自身を指すように書き換えるかを設定します。

設定値	説明
■チェックあり	ヘッダを書き換えます。
□チェックなし	ヘッダを書き換えません。

例)変更前：Destination: https://www.nec.co.jp/index.html

変更後：Destination: http://www.nec.co.jp/index.html

◆ 最大同時接続数

クライアント、SSL アクセラレータ間の最大同時接続数(システム全体での値)を設定します。

デフォルトは 512 になります。512～4096 の範囲で設定可能です。

◆ アクセス転送先キャッシュサーバ設定

SSL アクセラレータ機能が受け付けたクライアントからの HTTPS リクエストを転送するキャッシュサーバの IP アドレスと TCP ポート番号を設定します。

設定するキャッシュサーバの IP アドレスと TCP ポート番号は、SSL アクセラレータ機能がクライアントからの HTTPS 接続を受け入れる待ち受けに対し、1 つ設定してください。

▶ 転送先キャッシュサーバ設定

HTTPS リクエストを転送するキャッシュサーバを選択します。

「3.2.1.2. 基本設定(Reverse)」のキャッシュサーバ設定で「HTTPS 通信用として使用する」にチェックを付けている待ち受けは選択できません。

✓ ボタンの説明

[追加]	転送先 IP アドレス：ポート番号(転送先分散グループ)を追加設定します。
[編集]	アクセス転送先キャッシュサーバ設定の一覧で選択した転送先 IP アドレス：ポート番号(転送先キャッシュサーバ)を、新しい IP アドレス:ポート番号に編集(変更)します。
[削除]	アクセス転送先キャッシュサーバ設定の一覧で選択した転送先 IP アドレス：ポート番号(転送先分散グループ)を削除します。

✓ ボタンの説明

[設定]	「SSL アクセラレータ設定」で指定した内容を設定し、反映を行います。
[戻る]	プロキシ画面に戻ります。→「3.2. プロキシ」

設定した値は直ちに設定ファイル上に変更されますが、[設定]ボタンを押下されるまでは、変更した内容は動作に反映されません。
[設定]ボタンを押下することにより SSL アクセラレータサービスが再起動し、設定した内容が反映されます。

3.2.14.1. SSL 証明書更新手順

更新を行う際は、必要に応じて運用中の証明書のバックアップを「3.5.15. バックアップ/リストア」の「ディレクトリ指定」にて行ってください。

・バックアップ対象ディレクトリ： /opt/nec/roma/etc/cert

1) 本設定画面の「アクセラレータ待ち受け設定」にて、仮の待ち受け(ポートは重複しない任意の値)を追加します。
   ポートに指定する値は、プロキシサービスが使用する可能性の低い 8000～65535 以外が推奨されます。
2) 「アクセラレータ待ち受け設定」にて、「認証局署名要求作成」を実行します。
3) 2)で作成した CSR を認証局に送り、SSL 証明書の申請を行います。証明書を取得後、4)以降を実施します。
4) 本設定画面の「アクセラレータ待ち受け設定」にて、1)で追加した仮の待ち受けを選択し、「アクセラレータ待ち受け設定」にて、 「署名済みの証明書登録」、「中間認証局証明書登録(任意)」を実行します。
   中間認証局証明書以外の状態が全て作成済みとなっていることが必須です。
5) 本設定画面の「アクセラレータ待ち受け設定」にて、旧証明書が登録されている待ち受けを選択後、TCP ポート番号を重複しない 任意の値に変更し[編集]を押下します。
6) 4)で更新された、新しい証明書が登録されている待ち受け(”1)”で追加した仮の待ち受け)を選択後、TCP ポート番号を旧証明書が 登録されていた待ち受けと同じポート番号に変更し[編集]を押下します。
7) 1)で追加した仮の待ち受けを選択し、「アクセラレータ待ち受け設定」の以下 2 項目と「アクセス転送先キャッシュサーバ設定」を運用中の待ち受けと同じ設定にします。
   ・Location/Contrnt-Location ヘッダを強制的に書き換える。
   ・Destination ヘッダを強制的に書き換える。
8) [設定]を押下してください。

以上で、証明書の更新は完了となります。

3.2.14.2. SSL 証明書インポート手順

他機種で使用中の秘密鍵及び SSL 証明書を本サーバに取り込む際の手順となります。
既存の設定を流用する場合は、手順 1)、2)、3)、7)を飛ばし手順 4)から行ってください。

1) 本設定画面の「アクセラレータ待ち受け設定」にて、待ち受けを追加します。
2) 「アクセラレータ待ち受け設定」にて、「自己署名証明書作成」を実行します。
3) 中間認証局証明書が必要でない場合は、「中間認証局証明書削除」を実行します。
4) 本サーバの下記のディレクトリに存在している秘密鍵、証明書署名要求、署名済み証明書、中間認証局証明書(任意)を他機種で使用中の秘密鍵及び SSL 証明書で上書きします。
   ディレクトリ：/opt/nec/roma/etc/cert
   ・ファイル名の規則
   秘密鍵：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).key
   証明書署名要求：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).csr
   署名済み証明書：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).crt
   中間認証局証明書：(待ち受けの IP アドレス)_(待ち受けの TCP ポート番号).mid

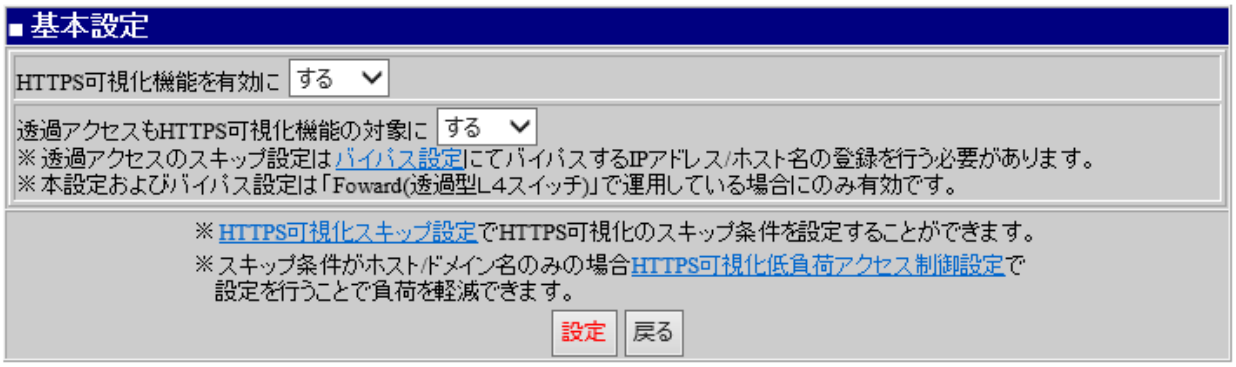
   上書きする待ち受けの IP アドレス/TCP ポート番号を使用してください
   例)待ち受けの IP アドレス 192.168.0.1、ポート番号 443 の場合、秘密鍵のファイル名は
   192.168.0.1_443.key
   になります。
5) 手順 4)で上書きした秘密鍵にパスフレーズが設定されている場合は、以下のコマンドを実行しパスフレーズを解除してください。
   # /usr/bin/openssl rsa -in (対象の秘密鍵のファイル名) -out (対象の秘密鍵のファイル名)
   コマンド実行後、パスフレーズの入力を求められますので対象の秘密鍵を作成したときのパスフレーズを入力してください。
   例)「192.168.0.1_443.key」のパスフレーズを解除する場合のコマンドは
   # /usr/bin/openssl rsa -in 192.168.0.1_443.key -out 192.168.0.1_443.key
   になります。
6) 1)で追加した待ち受けを選択し、「アクセラレータ待ち受け設定」の以下 2 項目と「アクセス転送先キャッシュサーバ設定」を設定します。
   ・Location/Contrnt-Location ヘッダを強制的に書き換える
   ・Destination ヘッダを強制的に書き換える
7) 本設定画面の[設定]を押下してください。

以上で、証明書のインポートは完了となります。

3.2.15. HTTPS 可視化機能設定

フォワードプロキシ用 HTTPS 可視化機能に関して設定を行います。

基本設定



◆ **HTTPS 可視化機能を有効にする/有効にしない**

HTTPS 通信可視化の機能を有効にする、しないの選択を行います(デフォルト：しない)。

「する」を選択した場合、暗号化された HTTPS 通信を復号化し、HTTP アクセスとして解析を行い、再度暗号化しアクセスを転送します。

「3.2.16. HTTPS 可視化アクセス制御設定」の「HTTPS 可視化スキップ設定」にて HTTPS 可視化のスキップ条件を設定することができます。

スキップする条件がホスト名/ドメイン名の場合、「3.2.17. HTTPS 可視化低負荷アクセス制御設定」にて通常より低負荷の制御設定を行うことができます。

◆ **透過アクセスも HTTPS 可視機能の対象にする/しない**

「3.2.1. 基本設定」の「サーバ種別設定」で「Forward(透過型Ｌ４スイッチ)」を選択し、本サーバを透過型として運用している場合に透過アクセスも HTTPS 可視化機能の対象にする、しないの選択します(デフォルト：しない)。

透過アクセスのスキップ設定を行う場合はバイパス設定にてバイパスする IP アドレス/ホスト名の登録を行う必要があります。

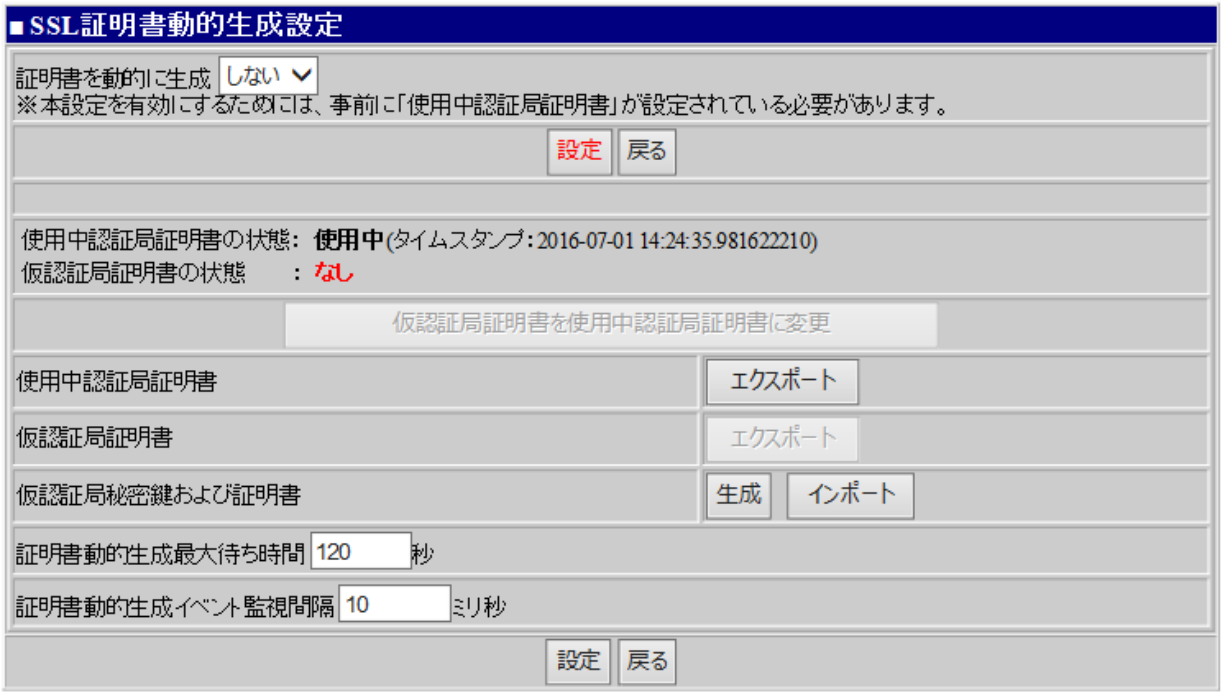
✓ **ボタンの説明**

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

SSL 証明書動的生成設定

HTTPS 可視化機能で使用する SSL 証明書の動的生成に関する設定を行います。
一旦、仮認証局証明書として生成(またはインポート)を行い「仮認証局証明書を使用中認証局証明書に変更」を押して状態を使用中に遷移させます。

CS 上で認証局秘密鍵および証明書を生成する場合、生成した認証局証明書を端末(ブラウザ)側の「信頼されたルート証明機関」にインポートしてください。
既存の認証局秘密鍵および証明書を使用する場合は[仮認証局秘密鍵および証明書]の[インポート]で CS 側に PEM 形式でインポートしてください。
※「Forward(透過型Ｌ４スイッチ)」で透過の対象となっているアクセスは本機能の対象外となります。



◆ 証明書を動的に生成する/しない

HTTPS 可視化機能の対象となっている SSL 通信で使用する証明書を動的に生成する/しないを指定します。 デフォルトは「しない」です。

使用中認証局証明書の設定が完了した後に「する」に変更してください。

本設定を「する」に変更するためには、事前に「使用中認証局証明書」が設定されている必要があります。

本機能を使用しない場合、ブラウザ側で警告画面が表示されたり、エラーとして扱われる場合がございますので必ず使用してください。

設定値	説明
する	SSL 通信で使用する証明書を動的に生成します。
しない	SSL 通信で使用する証明書に「対クライアント用の SSL 証明書」で登録した証明書を使用します。(デフォルト)

◆ 使用中認証局証明書の状態

SSL 証明書の動的生成で使用している認証局証明書の状態を表示します。

認証局証明書が存在している場合は「使用中(タイムスタンプ:2016-06-21 16:28:53.811712195)」のように表示されます。

認証局証明書が存在しない場合は「未使用」と表示されます。

◆ 仮認証局証明書の状態

一時的に保存している認証局証明書の状態を表示します。

仮認証局証明書が存在している場合は「あり(タイムスタンプ:2016-06-21 16:28:53.811712195)」のように表示されます。

仮認証局証明書が存在しない場合は「なし」と表示されます。

◆ 仮認証局証明書を使用中認証局証明書に変更

仮認証局証明書を使用中認証局証明書に変更します。

変更した場合、前回の認証局証明書で生成された SSL 証明書はすべて削除されます。

✓ ボタンの説明

[仮認証局証明書を使用中認証局証明書に変更]	仮認証局証明書を使用中認証局証明書に変更します。 その際に前回の認証局証明書で生成された SSL 証明書はすべて削除されます。

◆ 使用中認証局証明書

使用中認証局証明書に関する操作を行います。

▶ エクスポート

使用中認証局証明書を端末側にエクスポート(ダウンロード)します。

✓ ボタンの説明

[エクスポート]	使用中認証局証明書を端末側にエクスポート(ダウンロード)します。

◆ 仮認証局証明書

仮認証局証明書に関する操作を行います。

▶ エクスポート

仮認証局証明書を端末側にエクスポート(ダウンロード)します。

✓ ボタンの説明

[エクスポート]	仮認証局証明書を端末側にエクスポート(ダウンロード)します。

◆ 仮認証局秘密鍵および証明書

仮認証局秘密鍵および証明書に関する操作を行います。

▶ 生成

仮認証局の秘密鍵および証明書を生成します。

✓ ボタンの説明

[生成]	仮認証局の秘密鍵および証明書を生成します。→「3.2.15.3. 仮認証局秘密鍵および証明書生成」

▶ インポート

所持している認証局秘密鍵および証明書を仮認証局証明書として本サーバ上にインポートします。

[インポート]を押した後に表示される画面に、PEM 形式の認証局秘密鍵の内容をコピーし、[認証局証明書の登録に進む]を押し 表示される画面に PEM 形式の認証局証明書をコピーし[登録]を押してください。

✓ ボタンの説明

[インポート]	仮認証局の秘密鍵および証明書をインポートします。→「3.2.15.4. 仮認証局秘密鍵および証明書インポート」

◆ 証明書動的生成最大待ち時間

証明書が動的に生成される最大待ち時間を指定します。

デフォルトは 120 秒です。

1 秒から 999 秒まで指定可能です。

◆ 証明書動的生成イベント監視間隔

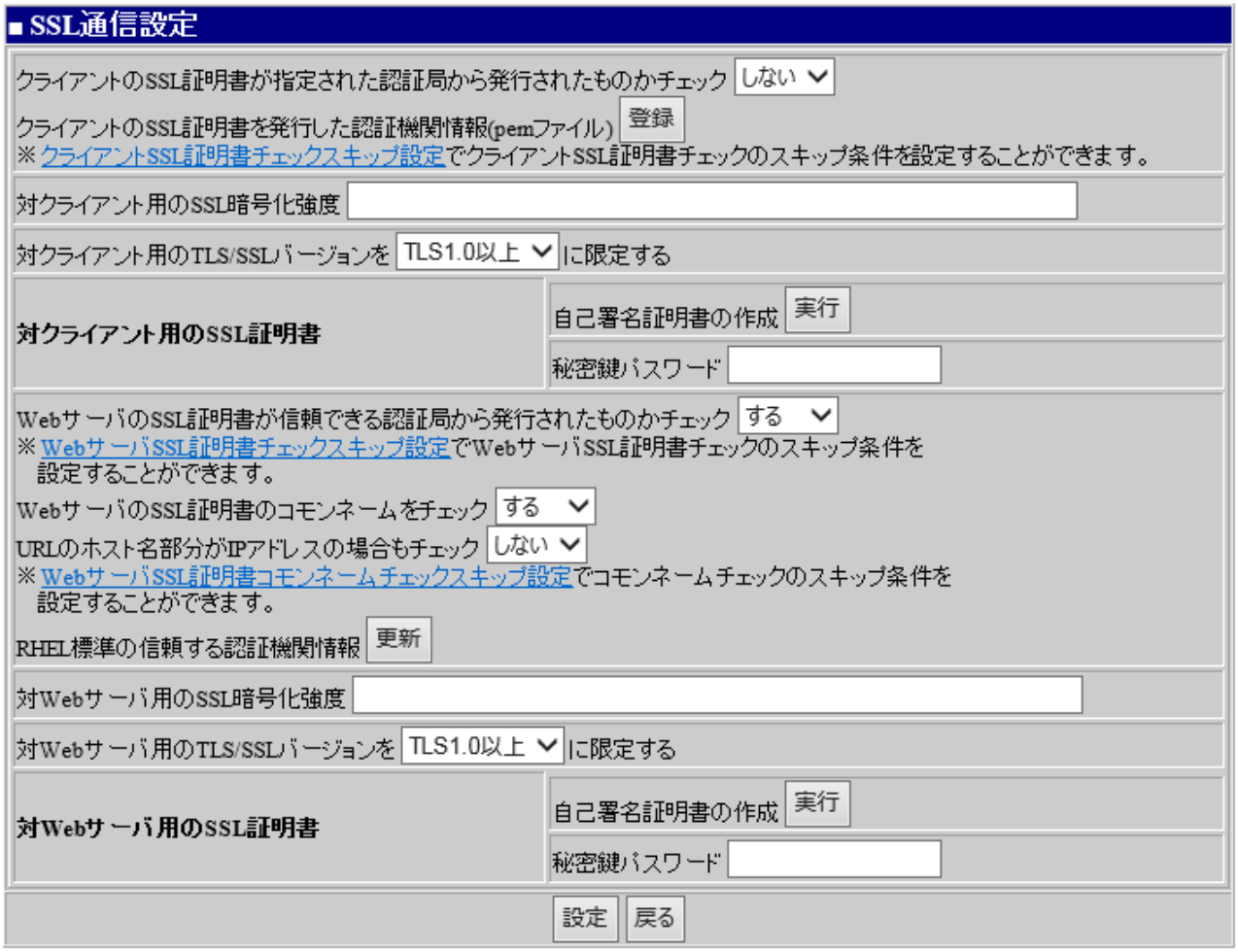
証明書を生成するイベントが発生しているか監視する間隔を指定します。

デフォルトは 10 ミリ秒です。

1 ミリ秒から 9999 ミリ秒まで指定可能です。

SSL 通信設定

HTTPS 可視化機能の対象となった SSL 通信に関する設定を行います。



◆ クライアントの SSL 証明書が指定された認証局から発行されたものかチェックするしない

クライアントが使用する SSL 証明書が「クライアントの SSL 証明書を発行した認証機関情報(pem ファイル)」の認証局から発行されたものかチェックする、しないを選択します。

「する」を選択した場合、クライアントが指定された認証局から発行された SSL 証明書を使用せずに SSL 通信を行った際にアクセスを拒否します。

クライアント SSL 証明書チェックスキップ設定にてクライアント SSL 証明書チェックのスキップ条件を設定することができます。

設定値	説明
する	SSL 証明書について認証局から発行されたものかをチェックします。
しない	SSL 証明書について認証局から発行されたものかをチェックしません(デフォルト)。

◆ クライアントの SSL 証明書を発行した認証機関情報(pem ファイル)

クライアントの SSL 証明書を発行した認証局のルート証明書(pem 形式)を登録します。

登録していない場合、RHEL 標準の信頼している認証機関情報を使用します。

✓ ボタンの説明

[登録]	証明書情報(pem ファイル)の登録を行います。→「3.2.15.1. 認証機関登録情報」

◆ 対クライアント用の SSL 暗号化強度

クライアントと本サーバ間の SSL 通信で使用する暗号化強度(OpenSSL の Cipher List)を指定します。

デフォルトは「ALL:!ADH:!EXPORT:+HIGH:!MEDIUM:!LOW:!3DES:!EDH」です。

◆ 対クライアント用の TLS/SSL バージョンを[ ]に限定する

クライアントと本サーバ間の SSL 通信で使用するを TLS/SSL バージョンを選択します。

クライアントが選択した TLS/SSL バージョン未満しか対応していない場合、当該クライアントからのアクセスは拒否されます。

設定値	説明
SSLv2 以上	—
SSLv3 以上	—
TLS1.0 以上	デフォルト値
TLS1.1 以上	—
TLS1.2 以上	—

◆ 対クライアント用の SSL 証明書

クライアントと本サーバ間で使用する SSL 証明書に関する設定を行います。

▶ 自己署名証明書の作成

クライアントと本サーバ間の SSL 通信で使用する、本サーバの自己署名証明書(SSL 証明書)を作成します。

✓ ボタンの説明

[実行]	証明の作成を実行します

▶ 秘密鍵パスワード

手持ちの SSL 証明書および秘密鍵を直接本サーバ上に格納した場合、秘密鍵に掛けているパスワードを設定します。

「自己署名証明書の作成」で SSL 証明書を作成する場合は本設定を「空欄」で設定します。

◆ Web サーバの SSL 証明書が信頼できる認証局から発行されたものかチェックする/しない

Web サーバの SSL 証明書が RHEL 標準の信頼している認証機関から発行されたものかチェックする、しないを選択します。Web サーバ SSL 証明書チェックスキップ設定にて Web サーバ SSL 証明書チェックのスキップ条件を設定することができます。

設定値	説明
する	信頼できる認証局から発行された SSL 証明書を使用していない Web サーバへのアクセスを拒否します(デフォルト)。
しない	信頼できる認証局から発行された SSL 証明書を使用していない Web サーバへのアクセスを拒否しません。

◆ Web サーバの SSL 証明書のコモンネームをチェックする/しない

アクセス先の Web サーバの SSL 証明書のコモンネームに宛先 URL のホスト名が含まれているかのチェックをする、しないを選択します。Web サーバ SSL 証明書コモンネームチェックスキップ設定にて Web サーバ SSL 証明書チェックのスキップ条件を設定することができます。

設定値	説明
する	Web サーバの SSL 証明書のコモンネームに含まれていないホスト名でのアクセスを拒否します(デフォルト)。
しない	Web サーバの SSL 証明書のコモンネームに含まれていないホスト名でのアクセスを拒否しません。

◆ URL のホスト名部分が IP アドレスの場合もチェックする/しない

「Web サーバの SSL 証明書のコモンネームをチェック」で「する」を選択した場合、宛先 URL のホスト名が IP アドレスでもチェックをする、しないを選択します。

設定値	説明
する	宛先 URL のホスト名が IP アドレスの場合も Web サーバの SSL 証明書のコモンネームに含まれているかチェックを行います(デフォルト)。
しない	宛先 URL のホスト名が IP アドレスの場合も Web サーバの SSL 証明書のコモンネームに含まれているかチェックを行いません。

◆ RHEL 標準の信頼する認証機関情報

「Web サーバの SSL 証明書が信頼できる認証局から発行されたものかチェック」で「する」を選択した場合に使用する信頼する認証局の情報を更新します。

✓ ボタンの説明

[更新]	信頼する証明書期間の情報を更新します。 →「3.2.15.2. 信頼する認証機関情報登録」

◆ 対 Web サーバ用の SSL 暗号化強度

本サーバと Web サーバ間の SSL 通信で使用する暗号化強度(OpenSSL の Cipher List)を指定します。

デフォルトは「ALL:!ADH:!EXPORT:+HIGH:!MEDIUM:!LOW:!3DES:!EDH」です。

◆ 対 Web サーバ用の TLS/SSL バージョンを[　]に限定する

本サーバと Web サーバ間の SSL 通信で使用するを TLS/SSL バージョンを選択します。

Web サーバが対応している TLS/SSL バージョン未満を選択した場合、本サーバからのアクセスが Web サーバから拒否されます。

サーバ用のバージョンを選択して限定します。

設定値	説明
SSLv2 以上	—
SSLv3 以上	—
TLS1.0 以上	デフォルト値
TLS1.1 以上	—
TLS1.2 以上	—

◆ 対 Web サーバ用の SSL 証明書

本サーバと Web サーバ間で使用する SSL 証明書に関する設定を行います。

▶ 自己署名証明書の作成

本サーバと Web サーバ間の SSL 通信で使用する、本サーバの自己署名証明書(SSL 証明書)を作成します。

✓　ボタンの説明

[実行]	証明の作成を実行します

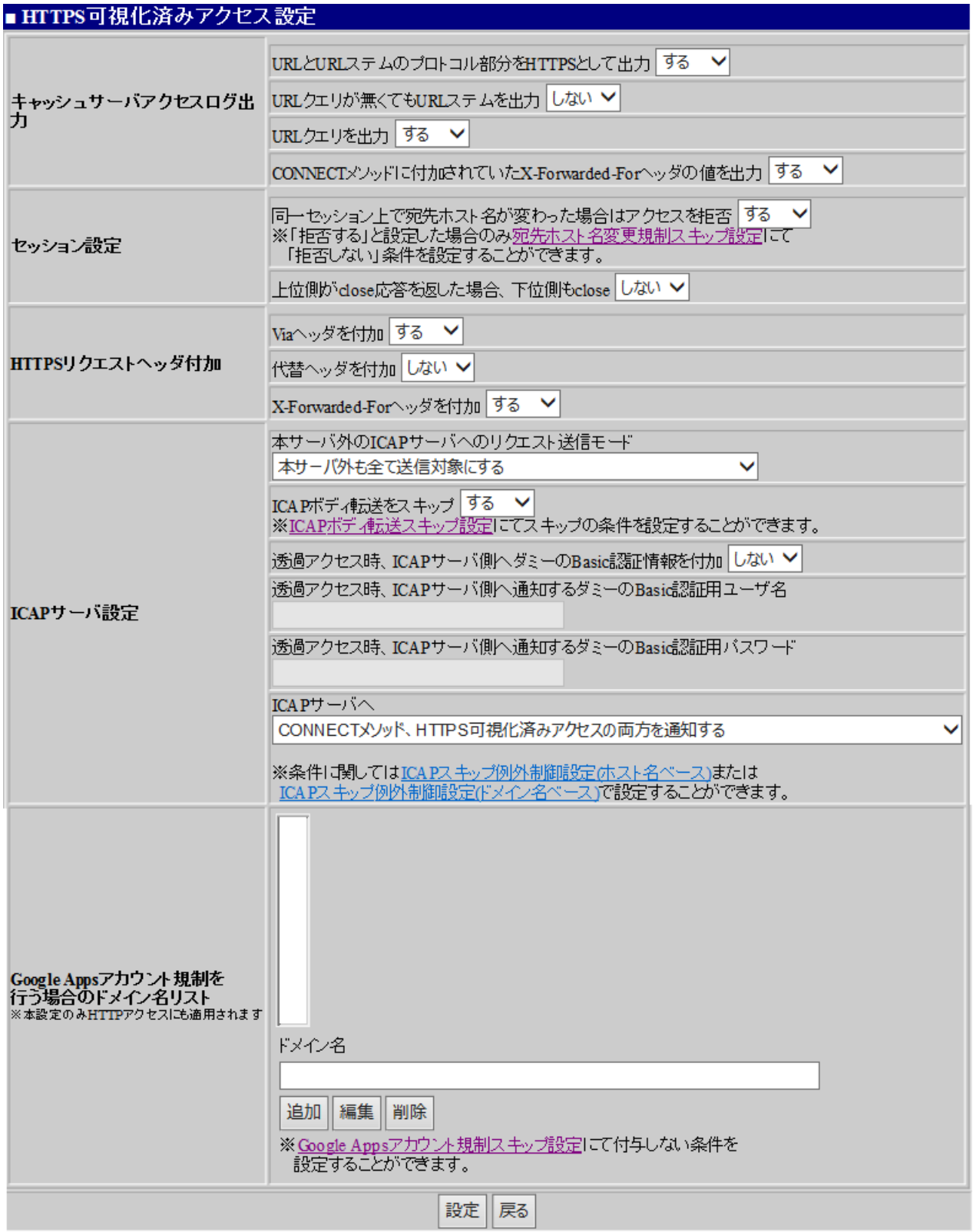
▶ 秘密鍵パスワード

手持ちの SSL 証明書および秘密鍵を直接本サーバ上に格納した場合、秘密鍵に掛けているパスワードを設定します。

「自己署名証明書の作成」で SSL 証明書を作成する場合は本設定を「空欄」で設定します。

HTTPS 可視化済みアクセス設定

復号化した HTTPS アクセスに関する設定を行います。



◆ キャッシュサーバアクセスログ出力

キャッシュサーバアクセスログ出力に関する設定を行います。

▶ URL と URL ステムのプロトコル部分を HTTPS として出力する/しない

キャッシュサーバアクセスログに出力する際に、URL と URL ステムのプロトコル部分を「HTTPS」に変更する、しないを選択します。

設定値	説明
する	URL と URL ステムのプロトコルを「HTTPS」に変更し、キャッシュサーバアクセスログに出力します(デフォルト)。
しない	URL と URL ステムのプロトコルを「HTTPS」に変更し、キャッシュサーバアクセスログに出力しません。

▶ URL クエリが無くても URL ステムを出力する/しない

キャッシュサーバアクセスログに出力する際に、URL クエリが無くても URL ステムを出力する、しないを選択します。

設定値	説明
する	URL クエリが無い場合も URL ステムをキャッシュサーバアクセスログに出力します。
しない	URL クエリが無い場合も URL ステムをキャッシュサーバアクセスログに出力しません(デフォルト)。

▶ URL クエリを出力する/しない

キャッシュサーバアクセスログに出力する際に、URL クエリを出力する、しないを選択します。

設定値	説明
する	URL クエリをキャッシュサーバアクセスログに出力します。(デフォルト)
しない	URL クエリをキャッシュサーバアクセスログに出力しません。

▶ CONNECT メソッドに付加されていた X-Forwarded-For ヘッダの値を出力する/しない

CONNECT メソッドに付加されていた X-Forwarded-For ヘッダの値をキャッシュサーバアクセスログに出力する、しないを選択します。

可視化された HTTPS リクエストに X-Forwarded-For ヘッダが付加されている場合は、その値が出力されます。

デフォルトは「する」です。

設定値	説明
する	CONNECT メソッドに付加されていた X-Forwarded-For ヘッダの値をキャッシュサーバアクセスログに出力します。(デフォルト)
しない	CONNECT メソッドに付加されていた X-Forwarded-For ヘッダの値をキャッシュサーバアクセスログに出力しません。

◆ セッション設定

セッションに関する設定を行います。

▶ 同一セッション上で宛先ホスト名が変わった場合はアクセスを拒否する/しない

同一セッション上で宛先ホスト名が変わった場合、アクセスを拒否する、しないを選択します。
宛先ホスト名変更規制スキップ設定にて「拒否しない」条件を設定することができます。

設定値	説明
する	同一セッション上でのアクセス中に宛先ホスト名が変わった場合、不正なアクセスが行われていると判断し、そのアクセス拒否します(デフォルト)。
しない	同一セッション上でのアクセス中に宛先ホスト名が変わった場合、不正なアクセスが行われていると判断し、そのアクセス拒否しません。

▶ 上位側が close 応答を返した場合、下位側も close する/しない

上位側がセッションを close する応答を行った場合、下位側も close する,しないを選択します。

設定値	説明
する	上位側がセッションを close する際に下位側のセッションも close します。
しない	上位側がセッションを close する際に下位側のセッションも close しません(デフォルト)。

◆ HTTPS リクエストヘッダ付加

HTTPS リクエストに付加するヘッダに関する設定を行います。

▶ Via ヘッダを付加する/しない

Via ヘッダを付加する、しないを選択します。

設定値	説明
する	Via ヘッダに詳細設定の「Via ヘッダの値」に設定されている値と HTTP プロトコルバージョンを付加します。
しない	Via ヘッダに詳細設定の「Via ヘッダの値」に設定されている値と HTTP プロトコルバージョンを付加しません（デフォルト）。

▶ 代替ヘッダを付加する/しない

Via ヘッダに付加する値を本サーバ独自のヘッダの値として付加する、しないを選択します。

設定値	説明
する	Via ヘッダに付加する値を本サーバ独自のヘッダの値として付加します。
しない	Via ヘッダに付加する値を本サーバ独自のヘッダの値として付加しません(デフォルト)。

▶ X-Forwarded-For ヘッダを付加する/しない

クライアントの IP アドレスを X-Forwarded-For ヘッダに付加する、しないを選択します。

設定値	説明
する	クライアントの IP アドレスを X-Forwarded-For ヘッダに付加します。
しない	クライアントの IP アドレスを X-Forwarded-For ヘッダに付加しません。(デフォルト)

◆ ICAP サーバ設定

ICAP サーバ設定にて連携している ICAP サーバに関する設定を行います。

▶ 本サーバ外の ICAP サーバへのリクエスト送信モード

サーバ用のバージョンを選択して限定します。URL フィルタスキップ設定にてスキップの条件を設定することができます。

設定値	説明
本サーバ外も全て送信対象にする	本サーバ外の ICAP サーバにもリクエストを送信します。
本サーバ上のみを送信対象とする	本サーバ上の ICAP サーバへのみリクエストを送信します（デフォルト）。
本サーバ上のがダウンしている場合のみ本サーバ外も送信対象にする	本サーバ上の ICAP サーバがダウンしている場合のみ、本サーバ外の ICAP サーバへリクエストを送信します。

▶ ICAP ボディ転送をスキップする/しない

ICAP サーバへ復号化した HTTPS リクエストのボディ部を ICAP サーバへ転送する、しないを選択します。

設定値	説明
する	連携している ICAP サーバにボディ部を転送する処理をスキップします（デフォルト）。一律で ICAP ボディ転送をスキップするため、条件を ICAP ボディ転送スキップ設定にてスキップの条件を設定することができます。
しない	連携している ICAP サーバにボディ部を転送する処理をスキップしません。

▶ 透過アクセス時、ICAP サーバ側へダミーの Basic 認証情報を付加する/しない

透過アクセス時に ICAP サーバ側へダミーの Basic 認証情報を付加する、しないを選択します。

設定値	説明
する	「透過アクセス時、ICAP サーバ側へ通知するダミーの Basic 認証用ユーザ名」、「透過アクセス時、ICAP サーバ側へ通知するダミーの Basic 認証用パスワード」を Basic 認証情報として ICAP サーバ側へ転送するリクエストに付加します。
しない	「透過アクセス時、ICAP サーバ側へ通知するダミーの Basic 認証用ユーザ名」、「透過アクセス時、ICAP サーバ側へ通知するダミーの Basic 認証用パスワード」を Basic 認証情報として ICAP サーバ側へ転送するリクエストに付加しません。(デフォルト）。

▶ 透過アクセス時、ICAP サーバ側へ通知するダミーの Basic 認証用ユーザ名

「透過アクセス時、ICAP サーバ側へダミーの Basic 認証情報を付加」で「する」を選択している場合、送信するダミーのユーザ名を指定します。

▶ 透過アクセス時、ICAP サーバ側へ通知するダミーの Basic 認証用パスワード

「透過アクセス時、ICAP サーバ側へダミーの Basic 認証情報を付加」で「する」を選択している場合、送信するダミーのパスワードを指定します。

▶ ICAP サーバへ

ICAP サーバへ CONNECT メソッド、HTTPS 可視化済みアクセスを通知する/しないに関する設定を行います。

設定値	説明
CONNECT メソッド、HTTPS 可視化済みアクセスの両方を通知する(デフォルト値)	本設定を指定している場合、CONNECT メソッドおよび HTTPS 可視化済みアクセスを全て通知します。 従来の CONNECT メソッドのフィルタリングに加えて、各アクセスの詳細もフィルタリングの対象になるため、最も厳しく URL フィルタリング処理が行われます。 ただし、URL の詳細まで判定対象にした場合には許可されるアクセスが CONNECT メソッドの判定の時点で拒否される可能性があります。
無条件に CONNECT メソッドは通知せず、HTTPS 可視化済みアクセスのみ通知する	本設定を指定している場合、CONNECT メソッドは一切通知せず、HTTPS 可視化済みアクセスのみ全て通知します。 各アクセスの詳細が全てフィルタリングの対象になりますが、CONNECT メソッドは全て対象外になるため、従来であれば拒否されていたアクセスが許可される可能性があります。
指定した条件に該当する CONNECT メソッドは通知せず、HTTPS 可視化済みアクセスのみ通知する	本設定を指定している場合、条件に該当した CONNECT メソッドは通知せず、HTTPS 可視化済みアクセスのみ全て通知します。 条件に該当しない場合は逆に CONNECT メソッドのみを通知し、HTTPS 可視化済みアクセスは通知しません。 条件に関しては「ICAP スキップ例外制御設定(ホスト名ベース)」または「ICAP スキップ例外制御設定(ドメイン名ベース)」で設定します。 必要に応じて適切にチェックを行うことが可能であり、フィルタリング処理の負荷も軽減することが可能ですが上記で条件を設定する必要があります。 条件に関しては「ICAP スキップ例外制御設定(ホスト名ベース)」または「ICAP スキップ例外制御設定(ドメイン名ベース)」で設定します。

◆ Google Apps アカウント規制を行う場合のドメイン名リスト

「google.com」宛のアクセスに付加する「X-GoogApps-Allowed-Domains ヘッダ」の値を登録します。Google Apps アカウント規制スキップ設定にて「X-GoogApps-Allowed-Domains ヘッダ」を付加する処理をスキップする条件を設定することができます。

▶ ドメイン名

ドメイン名が表示されます。

✓ ボタンの説明

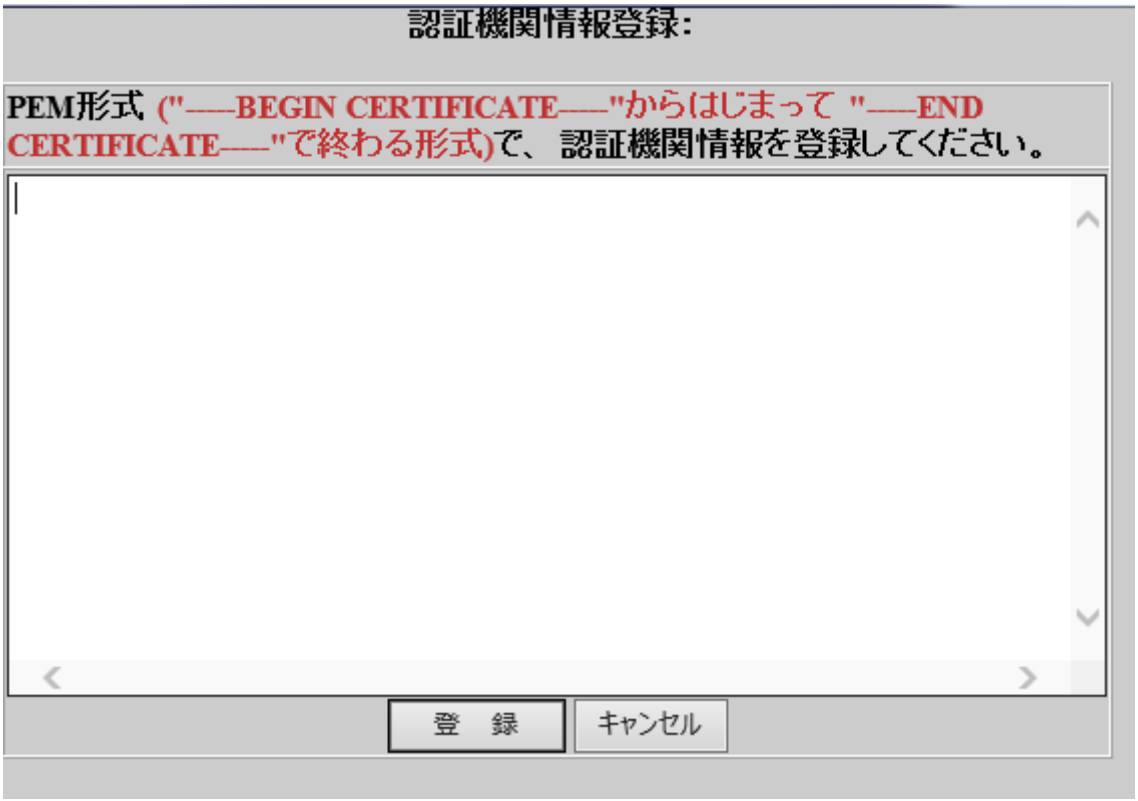
[追加]	ドメイン名の追加を行います。
[編集]	選択したドメイン名の編集を行います。
[削除]	指定したドメイン名を削除します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.15.1. 認証機関登録情報

認証機関情報登録を行います。

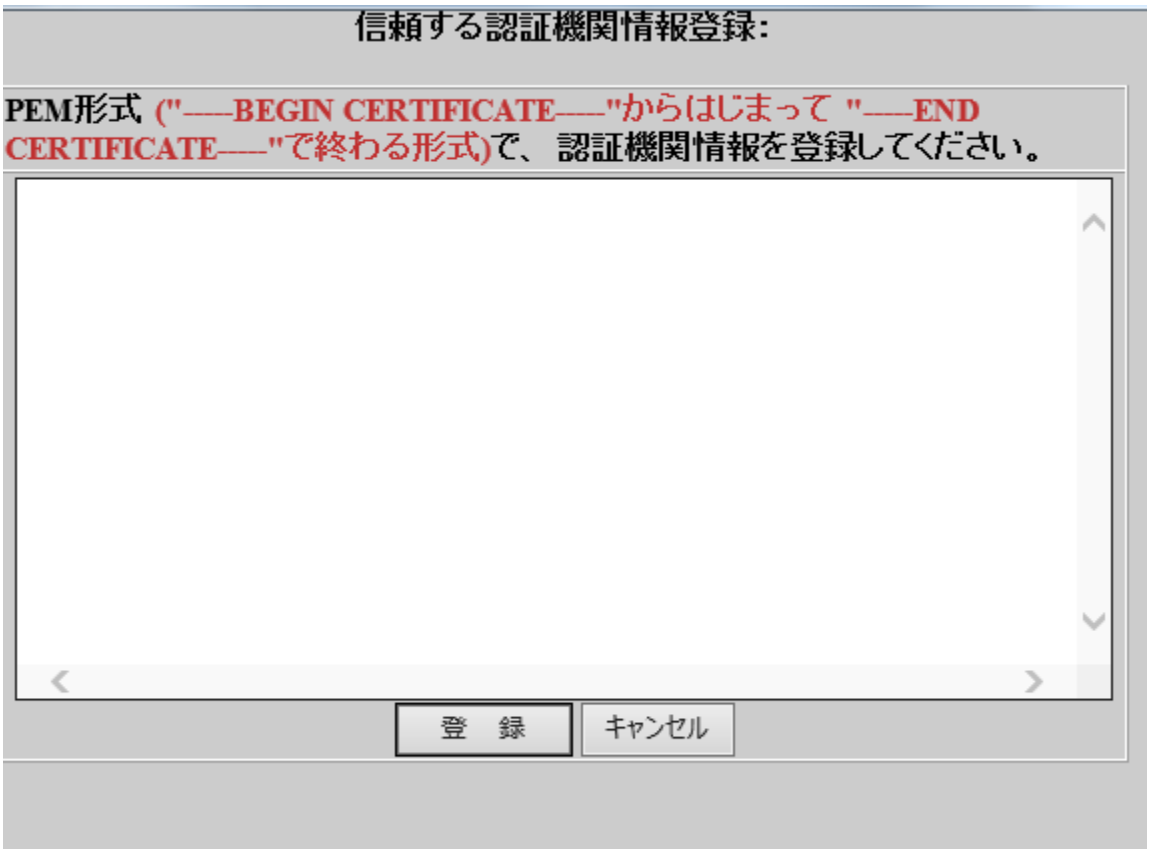


✓ ボタンの説明

[登録]	入力した内容を登録します。
[キャンセル]	前画面へ戻ります。

3.2.15.2. 信頼する認証機関情報登録

信頼する認証機関の報登録を行います。

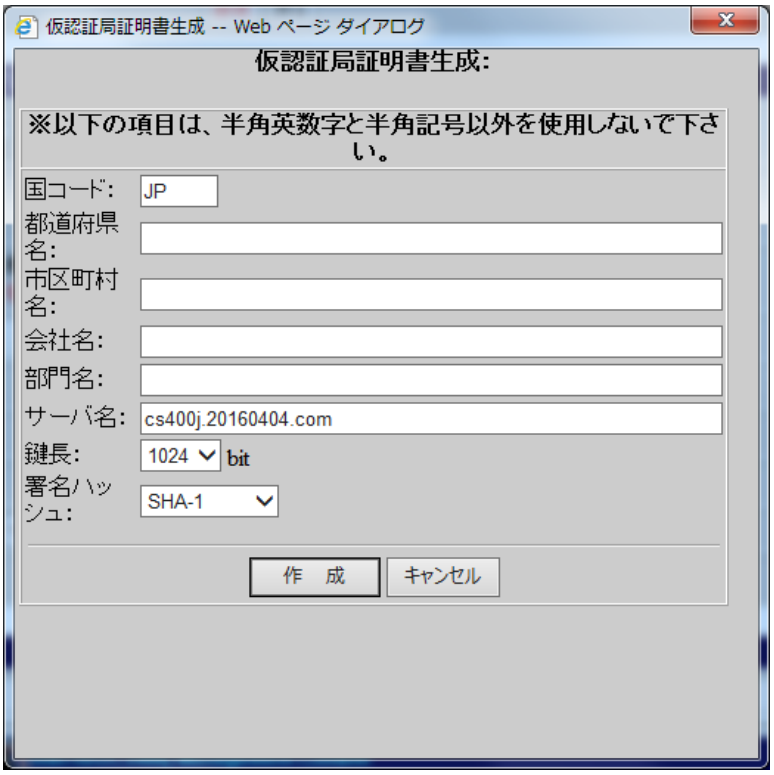


✓ ボタンの説明

[登録]	入力した内容を登録します。
[キャンセル]	前画面へ戻ります。

3.2.15.3. 仮認証局秘密鍵および証明書生成

仮認証局の秘密鍵および証明書を生成します。



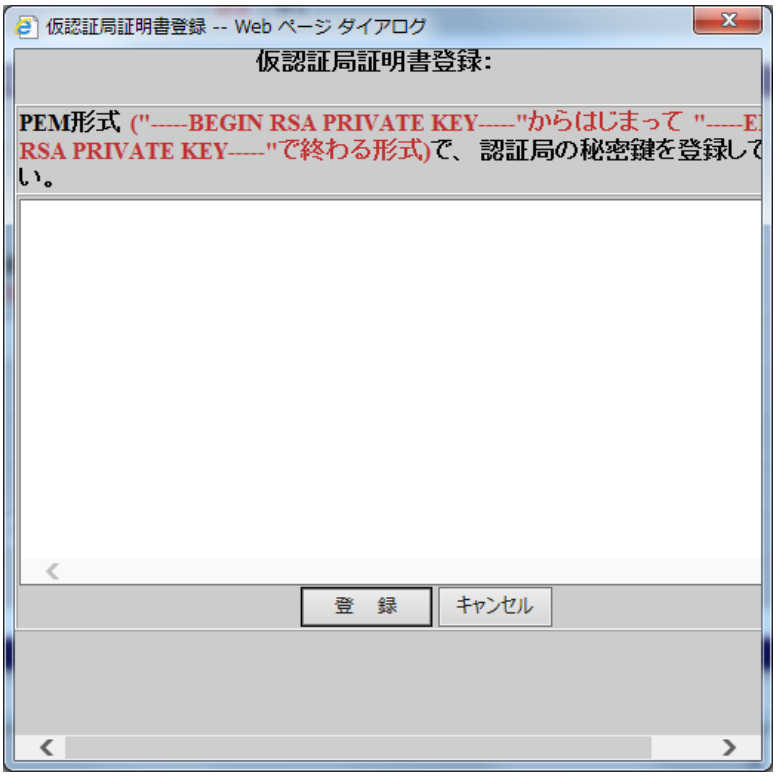
項目名	説明
国コード	仮認証局が所在する国コードを入力します。
都道府県	仮認証局が所在する都道府県を入力します。
市区町村名	仮認証局が所在する市区町村名を入力します。
会社名	仮認証局が所在する会社名を入力します。
部門名	仮認証局が所在する部門名を入力します。
サーバ名	仮認証局が所在するサーバ名を入力します。
鍵長	証明書の鍵長を指定します。
署名ハッシュ	証明書の署名ハッシュを指定します。

✓ ボタンの説明

[作成]	入力した内容で仮認証局の秘密鍵および証明書を生成します。
[キャンセル]	前画面へ戻ります。

3.2.15.4. 仮認証局秘密鍵および証明書インポート

所持している認証局秘密鍵(PEM 形式)および証明書(PEM 形式)を仮認証局証明書として本サーバ上にインポートします。



✓ ボタンの説明

[登録]	入力した内容を登録します。
[キャンセル]	前画面へ戻ります。

3.2.16. HTTPS 可視化アクセス制御設定

HTTPS 可視化済みアクセス設定

HTTPS 可視化アクセス制御は以下の画面に分かれています。

■リスト設定
■HTTPS 可視化スキップ設定
■クライアント SSL 証明書チェックスキップ設定
■Web サーバ SSL 証明書チェックスキップ設定
■Web サーバ SSL 証明書コモンチェックスキップ設定
■宛先ホスト名変更規制スキップ設定
■GoogleApp アカウント規制スキップ設定

ヒント

「■リスト設定」は「3.2.6. アクセス制御」「3.2.11. 特殊アクセス制御」「3.2.12. HTTP ヘッダ編集設定」「3.2.13. 対上位サーバ向けソース IP 設定」「3.2.16. HTTPS 可視化アクセス制御設定」で共通となります。

リスト設定

現在設定されているリスト設定の一覧を表示します。


※デフォルト値として予約している(編集、追加不可)リスト名は赤文字で表示されます。

■リスト設定

追加	リスト名	設定種別	条件式
編集 削除	all	src	0.0.0.0/0.0.0.0 0::0/64
編集 削除	cgi	urlpath_regex	\.cgi$ \?
編集 削除	MSIE-SKIP	browser_regex	MSIE
編集 削除	Google-Toolbar	browser_regex	GoogleToolbar

✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

[追加]	リストの追加を行います。→「3.2.6.1. リスト(追加)設定」
[編集]	リストの編集を行います。→「3.2.6.2. リスト(編集)設定」
[削除]	リストの削除を行います。→「3.2.6.3. リストの削除」

◆ リスト名

リスト名を英数字で表示します。大文字と小文字は区別しません。16 文字まで指定可能です。 編集の場合、リスト名の書き換えはできません。

デフォルト値として予約している(編集、追加不可)リスト名は赤文字で表示されます。

デフォルトは、各種設定のデフォルトで使用するリストを設定しています。リスト名に"-"が含まれているリストは、デフォルト用のリストとして設定しています。そのため、リスト名に"-"が含まれているリストを作成、編集することはできません。設定されているデフォルトは、モジュールアップデート時、リストの意味合いの変更は行いませんが、内容を変更する可能性があります。

◆ 設定種別

設定種別を表示します。

詳細は、「3.2.6.1. リスト(追加)設定」の設定種別を参照してください。

◆ 条件式

条件式は各設定種別に応じた条件式を表示します。

詳細は、「3.2.6.1. リスト(追加)設定」の条件式を参照してください。

HTTPS 可視化スキップ設定

HTTPS 可視化機能設定の「HTTPS 可視化機能を有効に」で「する」と設定している場合、リスト設定で設定したリストに対して、HTTPS 可視化を行う/行わない(allow/deny)を指定します。

✓ ボタンの説明

[追加]	HTTPS 可視化設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

HTTPS 可視化チェックの許可/不許可を表示します。

表示	説明
allow	HTTPS 可視化を許可
deny	HTTPS 可視化を不許可

◆ リスト名

リスト設定で指定したリストの中から HTTPS 可視化の許可/不許可を指定するリスト名を表示します。 リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

- デフォルトではインターネット(外部)への HTTPS アクセス(宛先ポート 443)のみを HTTPS 可視化機能の対象になっています。
- HTTPS 可視化設定は上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
- 順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
- リスト設定の内容が画面下部に表示されます。
- 「設定」ボタンが押下されることで設定が反映されます。

クライアント SSL 証明書チェックスキップ設定

HTTPS 可視化機能設定の「クライアントの SSL 証明書が指定された認証局から発行されたものかチェック」で「する」と設定している場合、リスト設定で設定したリストに対してクライアントの SSL 証明書が HTTPS 可視化機能設定の「クライアントの SSL 証明書を発行した認証機関情報(pem ファイル)」で登録した認証機関から発行されたものかチェックを行う/行わない(allow/deny)を指定します。

✓ ボタンの説明

[追加]	クライアント SSL 証明書チェックのスキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

クライアント SSL 証明書チェックの許可/不許可を表示します。

表示	説明
allow	クライアント SSL 証明書チェックを許可
deny	クライアント SSL 証明書チェックを不許可

◆ リスト名

リスト設定で指定したリストの中からクライアント SSL 証明書チェックの許可/不許可を指定するリスト名を表示します。 リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

- デフォルトは設定されていないため、HTTPS 可視化機能設定の「クライアントの SSL 証明書が指定された認証局から発行されたものかチェック」で「する」と設定している場合、全ての HTTPS アクセスに対してクライアントの SSL 証明書が指定された認証局から発行されたものかチェックを行います。
- クライアント SSL 証明書チェックは上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
- 順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
- リスト設定の内容が画面下部に表示されます。
- 「設定」ボタンが押下されることで設定が反映されます。

Web サーバ SSL 証明書チェックスキップ設定

HTTPS 可視化機能設定の「Web サーバの SSL 証明書が信頼できる認証局から発行されたものかチェック」で「する」と設定している場合、リスト設定で設定したリストに対して Web サーバの SSL 証明書が HTTPS 可視化機能設定の「RHEL 標準の信頼する認証機関情報」で信頼されているものかチェックを行う/行わない(allow/deny)を指定します。

✓ ボタンの説明

[追加]	Web サーバ SSL 証明書チェックのスキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

Web サーバ SSL 証明書チェックの許可/不許可を表示します。

表示	説明
allow	Web サーバ SSL 証明書チェックを許可
deny	Web サーバ SSL 証明書チェックを不許可

◆ リスト名

リスト設定で指定したリストの中から Web サーバ SSL 証明書チェックの許可/不許可を指定するリスト名を表示します。 リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

- デフォルトは設定されていないため、HTTPS 可視化機能設定の「Web サーバの SSL 証明書が信頼できる認証局から発行されたものかチェック」で「する」と設定している場合、全ての HTTPS アクセスに対して Web サーバの SSL 証明書が信頼している認証局から発行されたものかチェックを行います。
- Web サーバ SSL 証明書チェックは上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください
- 順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
- リスト設定の内容が画面下部に表示されます。
- 「設定」ボタンが押下されることで設定が反映されます。

Web サーバ SSL 証明書コモンチェックスキップ設定

HTTPS 可視化機能設定の「Web サーバの SSL 証明書のコモンネームをチェック」で「する」と設定している場合、リスト設定で設定したリストに対して宛先 URL のホスト名が Web サーバの SSL 証明書のコモンネームに存在しているかチェックを行う/行わない(allow/deny)を指定します。

✓ ボタンの説明

[追加]	Web サーバ SSL 証明書コモンチェックのスキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

Web サーバ SSL 証明書コモンチェックの許可/不許可を表示します。

表示	説明
allow	Web サーバ SSL 証明書コモンチェックを許可
deny	Web サーバ SSL 証明書コモンチェックを不許可

◆ リスト名

リスト設定で指定したリストの中から Web サーバ SSL 証明書コモンチェックの許可/不許可を指定するリスト名を表示します。 リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

- デフォルトは設定されていないため、HTTPS 可視化機能設定の「Web サーバの SSL 証明書のコモンネームをチェック」で「する」と設定している場合全ての HTTPS アクセスに対して、宛先 URL のホスト名が Web サーバの SSL 証明書のコモンネームに存在しているかチェックを行います。
- Web サーバ SSL 証明書コモンチェックは上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
- 順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
- リスト設定の内容が画面下部に表示されます。
- 「設定」ボタンが押下されることで設定が反映されます。

宛先ホスト名変更規制スキップ設定

HTTPS 可視化機能設定の「同一セッション上で宛先ホスト名が変わった場合はアクセスを拒否」で「する」と設定している場合、リスト設定で設定したリストに対して同一セッション上で宛先ホスト名が変わった場合はアクセスを拒否する/しない(allow/deny)を指定します。

✓ ボタンの説明

[追加]	宛先ホス名変更規制チェックのスキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

宛先ホス名変更規制の許可/不許可を表示します。

表示	説明
allow	宛先ホス名変更規制を許可
deny	宛先ホス名変更規制を不許可

◆ リスト名

リスト設定で指定したリストの中から宛先ホス名変更規制の許可/不許可を指定するリスト名を表示します。 リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

- デフォルトは設定されていないため、HTTPS 可視化機能設定の「宛先ホスト名変更規制スキップ設定」で「する」と設定している場合、全ての HTTPS アクセスに対して、同一セッション上で宛先ホスト名が変わった際にアクセスを拒否します。
- 宛先ホス名変更規制スキップは上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
- 順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
- リスト設定の内容が画面下部に表示されます。
- 「設定」ボタンが押下されることで設定が反映されます。

GoogleApp アカウント規制スキップ設定

HTTPS 可視化機能設定の「Google Apps アカウント規制を行う場合のドメイン名リスト」をリスト設定で設定したリストに対して、付加する/しない(allow/deny)を指定します。

✓ ボタンの説明

[追加]	Google Apps アカウント規制のスキップ設定の追加を行います。
[編集]	選択した設定の編集を行います。
[削除]	選択した設定の削除を行います。
[順序]	リストの順序を変更することができます。

◆ allow/deny

Google Apps アカウント規制の許可/不許可を表示します。

表示	説明
allow	Google Apps アカウント規制チェックを許可
deny	Google Apps アカウント規制チェックを不許可

◆ リスト名

リスト設定で指定したリストの中からチェックの許可/不許可を指定するリスト名を表示します。
リスト名は 30 個まで指定可能で、複数指定した場合には AND の処理が行われます。

重要

- デフォルトは設定されていないため、HTTPS 可視化機能設定の「Google Apps アカウント規制を行う場合のドメイン名リスト」のリストを全ての「google.com」ドメイン宛のリクエストに付加します。
- Google Apps アカウント規制のチェックは上位に記述されている条件から確認します。一致した場合、allow/deny の指定に関わらず以降の条件は確認しません。順番には注意してください。
  順番の変更は「順序」ボタンを押すと出て来る編集画面で変更できます。
- リスト設定の内容は、画面上部のリスト設定画面に表示しています。

3.2.17. HTTPS 可視化低負荷アクセス制御設定

HTTPS 可視化低負荷アクセス制御設定は以下の画面に分かれています。

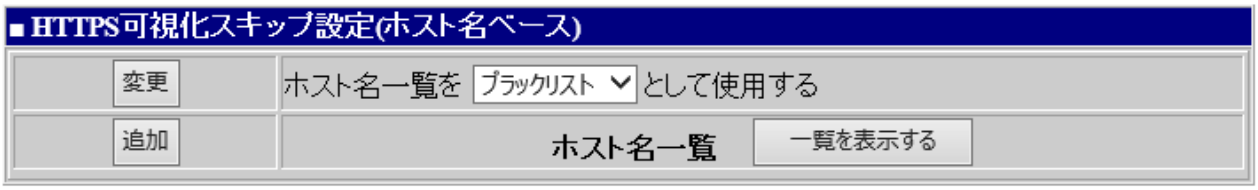
■設定状況
■HTTPS 可視化スキップ設定(ホスト名ベース)
■HTTPS 可視化スキップ設定(ドメイン名ベース)
■アクセス制御設定(ホスト名ベース)
■アクセス制御設定(ドメイン名ベース)
■ICAP スキップ例外制御設定(ホスト名ベース)
■ICAP スキップ例外制御設定(ドメイン名ベース)

設定状況

「設定」ボタンを押下すると、本画面で行った設定を反映します。設定が反映されている場合、黒文字で「反映済み」と表示します。 設定変更後に設定を反映していない場合、赤文字で「未反映」と表示します。

HTTPS 可視化スキップ設定(ホスト名ベース)

指定された条件に該当するアクセスに対して HTTPS 可視化機能の処理をスキップします。



◆ ホスト名一覧を[ ]として使用する

設定したホスト名の一覧をブラックリストとして扱うか、ホワイトリストとして扱うかを選択します。

設定値	説明
ブラックリスト	設定したホスト名宛のアクセスに対して、HTTPS 可視化機能の処理をスキップします。(デフォルト)
ホワイトリスト	設定したホスト名宛のアクセスに対してのみ、HTTPS 可視化機能の処理を行います。

◆ ホスト名一覧

設定したホスト名の一覧を表示します。

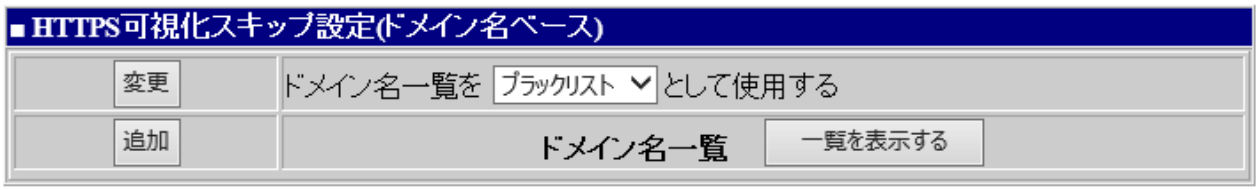
✓ **ボタンの説明**

該当行に対する操作を行うための各種ボタンを表示します。

[変更]	設定したホスト名を変更します。
[追加]	ホスト名を追加します。 →「3.2.17.1. HTTPS 可視化スキップ設定(ホスト名ベース)追加設定」
[編集]	設定したホスト名を編集します。
[削除]	設定したホスト名を削除します。
[一覧を非表示にする]	設定したホスト名の一覧を表示します。
[一覧を表示にする]	設定したホスト名の一覧を非表示にします。

HTTPS 可視化スキップ設定(ドメイン名ベース)

指定された条件に該当するアクセスに対して HTTPS 可視化機能の処理をスキップします。



◆ ドメイン名一覧を[ ]として使用する

設定したドメイン名の一覧をブラックリストとして扱うか、ホワイトリストとして扱うかを選択します。

設定値	説明
ブラックリスト	設定したドメイン名宛のアクセスに対して、HTTPS 可視化機能の処理をスキップします。(デフォルト)
ホワイトリスト	設定したドメイン名宛のアクセスに対してのみ、HTTPS 可視化機能の処理を行います。

◆ ドメイン名一覧

設定したホスト名の一覧を表示します。

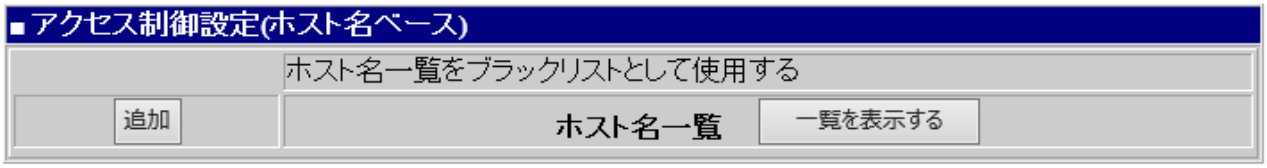
✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

[変更]	設定したドメイン名を変更します。
[追加]	ドメイン名を追加します。 →「3.2.17.2. HTTPS 可視化スキップ設定(ドメイン名ベース)追加設定」
[編集]	設定したドメイン名を編集します。
[削除]	設定したドメイン名を削除します。
[一覧を非表示にする]	設定したドメイン名の一覧を非表示にします。
[一覧を表示にする]	設定したドメイン名の一覧を表示します。

アクセス制御設定(ホスト名ベース)

指定された条件に該当するアクセスを拒否します。



◆ ホスト名一覧

設定したホスト名の一覧を表示します。

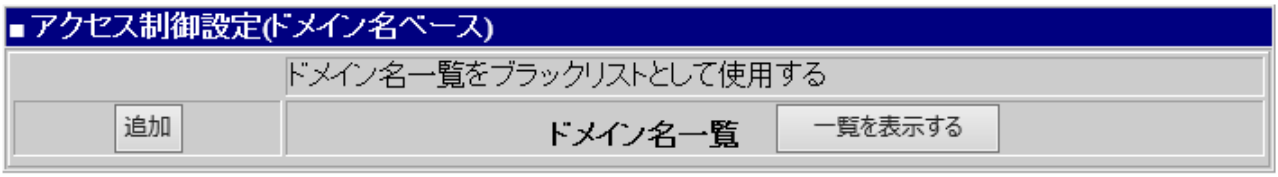
✓ **ボタンの説明**

該当行に対する操作を行うための各種ボタンを表示します。

[変更]	設定したホスト名を変更します。
[追加]	ホスト名を追加します。 →「3.2.17.3. アクセス制御設定(ホスト名ベース)追加設定」
[編集]	設定したホスト名を編集します。
[削除]	設定したホスト名を削除します。
[一覧を非表示にする]	設定したホスト名の一覧を非表示にします。
[一覧を表示にする]	設定したホスト名の一覧を表示します。

アクセス制御設定(ドメイン名ベース)

指定された条件に該当するアクセスを拒否します。



◆ ドメイン名一覧

設定したホスト名の一覧を表示します。

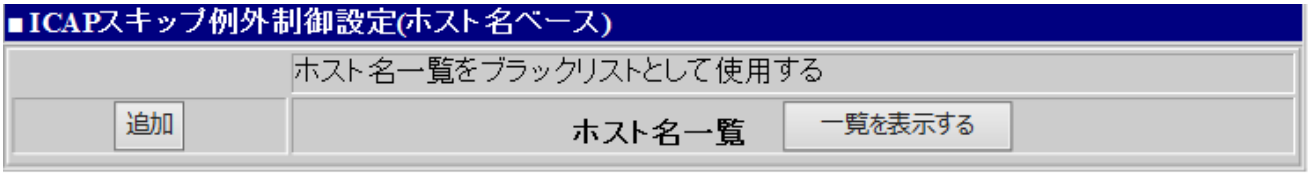
✓ **ボタンの説明**

該当行に対する操作を行うための各種ボタンを表示します。

[変更]	設定したドメイン名を変更します。
[追加]	ドメイン名を追加します。 →「3.2.17.4. アクセス制御設定(ドメイン名ベース)追加設定」
[編集]	設定したドメイン名を編集します。
[削除]	設定したドメイン名を削除します。
[一覧を非表示にする]	設定したドメイン名の一覧を表示します。
[一覧を表示にする]	設定したドメイン名の一覧を非表示にします。

ICAP スキップ例外制御設定(ホスト名ベース)

指定された条件に該当するアクセスを拒否します。



◆ ホスト名一覧

設定したホスト名の一覧を表示します。

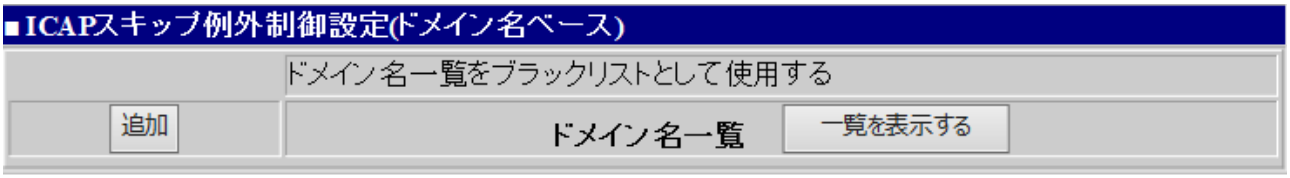
✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

[変更]	設定したホスト名を変更します。
[追加]	ホスト名を追加します。 →「3.2.17.5.　ICAP スキップ例外制御設定(ホスト名ベース)」
[編集]	設定したホスト名を編集します。
[削除]	設定したホスト名を削除します。
[一覧を非表示にする]	設定したホスト名の一覧を表示します。
[一覧を表示にする]	設定したホスト名の一覧を非表示にします。

ICAP スキップ例外制御設定(ドメイン名ベース)

指定された条件に該当するアクセスを拒否します。



◆ ホスト名一覧

設定したホスト名の一覧を表示します。

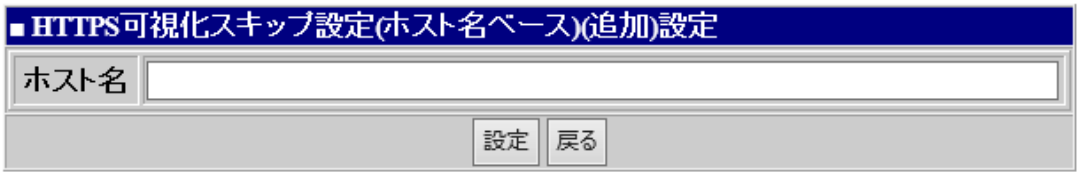
✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

[変更]	設定したホスト名を変更します。
[追加]	ホスト名を追加します。 →「3.2.17.6. ICAP スキップ例外制御設定(ドメイン名ベース)追加設定」
[編集]	設定したホスト名を編集します。
[削除]	設定したホスト名を削除します。
[一覧を非表示にする]	設定したホスト名の一覧を表示します。
[一覧を表示にする]	設定したホスト名の一覧を非表示にします。

3.2.17.1. HTTPS 可視化スキップ設定(ホスト名ベース)追加設定

一覧にホスト名を追加します。



✓ ボタン操作

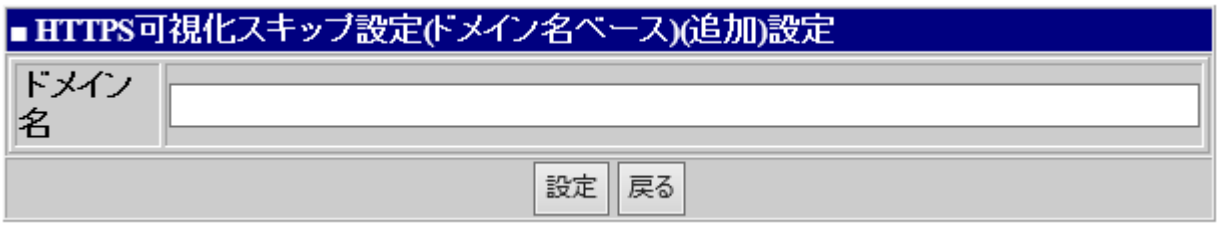
[設定]	設定したホスト名を追加します。
[戻る]	設定を行わず、前画面へ戻ります。

重要

・設定したホスト名は共通化されませんので、各制御設定毎に設定を行う必要があります。
・1 つのホスト名は最大 255 文字まで設定を行うことができます。
・区切り文字として空白(スペース)を使用することで、1 つのリストに最大 255 個まで設定を行うことができます。
・1 つのリストは最大 8000 文字まで設定を行うことができます。
・先頭に「.」を記述することはできません。

3.2.17.2. HTTPS 可視化スキップ設定(ドメイン名ベース)追加設定

一覧にドメイン名を追加します。



✓ ボタン操作

[設定]	設定したドメイン名を追加します。
[戻る]	設定を行わず、前画面へ戻ります。

重要

・設定したドメイン名は共通化されませんので、各制御設定毎に設定を行う必要があります。
・1 つのドメイン名は最大 253 文字まで設定を行うことができます。
・区切り文字として空白(スペース)を使用することで、1 つのリストに最大 255 個まで設定を行うことができます。
・1 つのリストは最大 8000 文字まで設定を行うことができます。
・先頭に「.」を記述することはできません。

3.2.17.3. アクセス制御設定(ホスト名ベース)追加設定

一覧にホスト名を追加します。

✓ ボタン操作

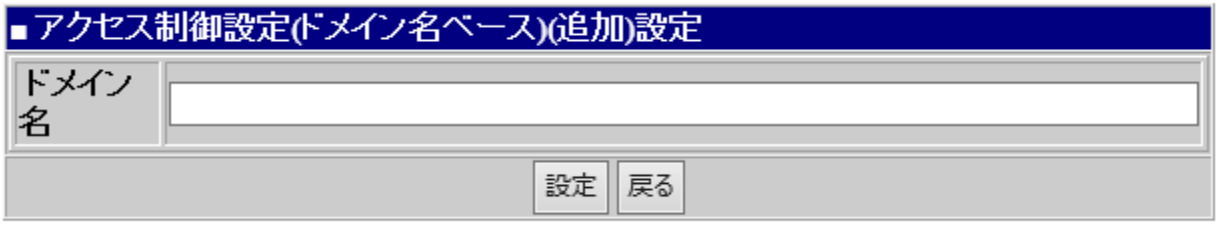
[設定]	設定したホスト名を追加します。
[戻る]	設定を行わず、前画面へ戻ります。

重要

・設定したホスト名は共通化されませんので、各制御設定毎に設定を行う必要があります。
・1 つのホスト名は最大 255 文字まで設定を行うことができます。
・区切り文字として空白(スペース)を使用することで、1 つのリストに最大 255 個まで設定を行うことができます。
・1 つのリストは最大 8000 文字まで設定を行うことができます。
・先頭に「.」を記述することはできません。

3.2.17.4. アクセス制御設定(ドメイン名ベース)追加設定

一覧にドメイン名を追加します。



✓ ボタン操作

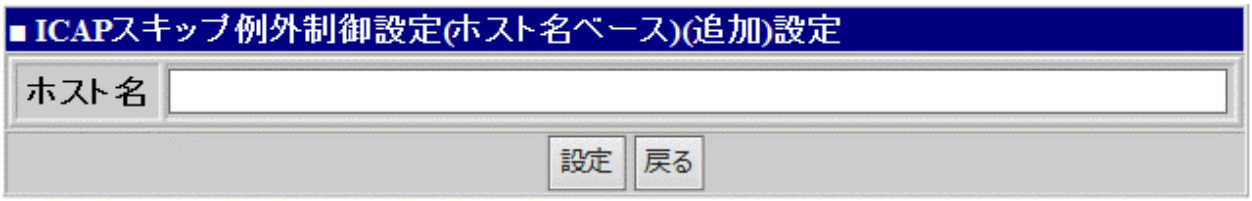
[設定]	設定したドメイン名を追加します。
[戻る]	設定を行わず、前画面へ戻ります。

重要

- 設定したドメイン名は共通化されませんので、各制御設定毎に設定を行う必要があります。
- 1 つのドメイン名は最大 253 文字まで設定を行うことができます。
- 区切り文字として空白(スペース)を使用することで、1 つのリストに最大 255 個まで設定を行うことができます。
- 1 つのリストは最大 8000 文字まで設定を行うことができます。
- 先頭に「.」を記述することはできません。

3.2.17.5. ICAP スキップ例外制御設定(ホスト名ベース)

一覧にホスト名を追加します。



✓ ボタン操作

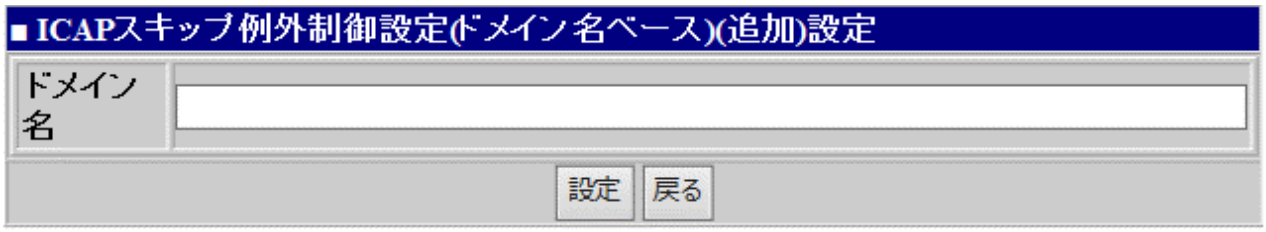
[設定]	設定したホスト名を追加します。
[戻る]	設定を行わず、前画面へ戻ります。

重要

・設定したホスト名は共通化されませんので、各制御設定毎に設定を行う必要があります。
・1 つのホスト名は最大 255 文字まで設定を行うことができます。
・区切り文字として空白(スペース)を使用することで、1 つのリストに最大 255 個まで設定を行うことができます。
・1 つのリストは最大 8000 文字まで設定を行うことができます。
・先頭に「.」を記述することはできません。

3.2.17.6. ICAP スキップ例外制御設定(ドメイン名ベース)追加設定

一覧にドメイン名を追加します。



✓ ボタン操作

[設定]	設定したドメイン名を追加します。
[戻る]	設定を行わず、前画面へ戻ります。

重要

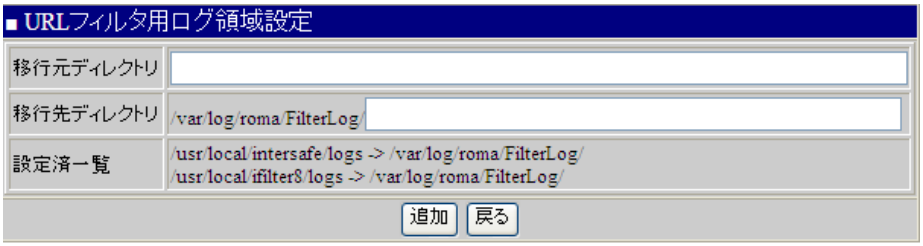
- 設定したドメイン名は共通化されませんので、各制御設定毎に設定を行う必要があります。
- 1 つのドメイン名は最大 253 文字まで設定を行うことができます。
- 区切り文字として空白(スペース)を使用することで、1 つのリストに最大 255 個まで設定を行うことができます。
- 1 つのリストは最大 8000 文字まで設定を行うことができます。
- 先頭に「.」を記述することはできません。

3.2.18. URL フィルタ用ログ領域設定

URL フィルタ用ログ領域設定

URL フィルタのログを保存する領域を指定できます。ログ領域の一部を使用します。以下で行うログ領域の移行設定は、基本的にはフィルタリングソフトのインストール後かつ運用開始前に実施してください。運用開始後にログファイルの移行を行う場合は、フィルタリングソフトのサービスを停止させて実施してください。 ログ出力中にログファイルの移行を行うと失敗する場合があります。また、ログファイルのサイズが大きいとファイルの移動に時間が掛かり失敗する場合があります。移行する際は、初期導入時に設定したログ領域("/var/log/roma")のサイズをオーバしないよう、フィルタリングソフトのログサイズと CS のログサイズ(世代数を含む)を考慮した上で実施してください。

・設定手順
  1) 移行元ディレクトリを入力
  2) 移行先ディレクトリを入力
  3) [追加]押下
・ログファイルの移行は以下の順で行われます。
  1) 移行元のディレクトリ配下のログファイルを移行先のディレクトリ配下に全て移動する。
  2) 移行元のディレクトリを削除する。
  3) 移行元と同じディレクトリ名で移行先のディレクトリへシンボリックリンクを貼る。



◆ 移行元ディレクトリ

InterSafe WebFilter/InterScan WebManager/i-FILTER のログファイルが格納されているディレクトリを指定します。InterSafe WebFilter/InterScan WebManager/i-FILTER のログファイルは、"<インストールディレクトリ>/logs" に保存されます。未設定状態でのデフォルトは、プリインストールの ICAP 版(InterSafe WebFilter Ver8.5)の"/usr/local/intersafe/logs"、ICAP 版(i-FILTER Ver9.0)の"/usr/local/ifilter9/logs"が表示されますので、必要に応じて変更してください。

◆ 移行先ディレクトリ

InterSafe WebFilter/InterScan WebManager/i-FILTER のログファイルを格納するディレクトリを指定します。格納するディレクトリは、初期導入時に設定したログ領域(/var/log/roma)の"FilterLog"ディレクトリ配下となるため、"/var/log/roma/FilterLog"は固定となります。"/var/log/roma/FilterLog"配下にディレクトリを追加することで、別のログファイルとの振分けを行うことも可能です。

◆ 設定済一覧

移行設定済のディレクトリの一覧が表示されます。移行元のディレクトリから移行先のディレクトリへシンボリックリンクが貼られた状態を表示します。移行後、シンボリックリンクの削除を行った際は一覧から削除されます。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[戻る]	前画面へ戻ります。

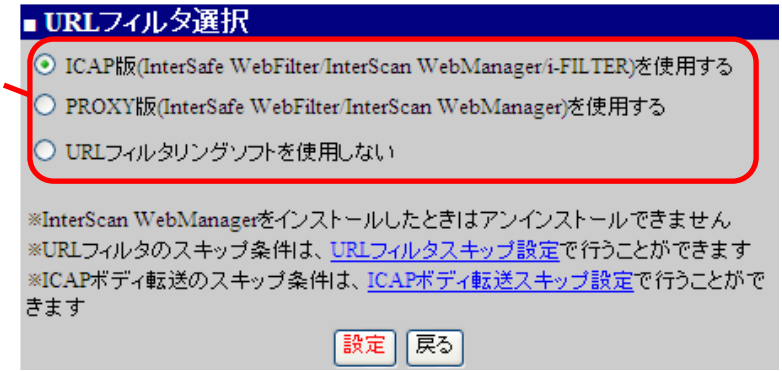
3.2.19. URL フィルタ選択

URL フィルタ選択

URL フィルタ選択画面で、使用するフィルタリングソフトを選択することができます。フィルタリングソフトはライセンス取得後、データベースファイルをダウンロードし利用します。
フィルタリングソフトは ICAP 版(InterSafe WebFilter/InterScan WebManage/i-FILTER)、または PROXY 版(InterSafe WebFilter/InterScan WebManager)を使用することができます。
また、「3.2.1. 基本設定」で本サーバのサーバ種別設定を「Forward(透過型 L4 スイッチ)」に設定した場合には PROXY 版は親プロキシとしてのみ使用できます。
本サーバのサーバ種別設定を「Reverse」に設定した場合にはフィルタリングソフトは使用できません。
本システムには、InterSafe WebFilter/i-FILTER の ICAP 版がプリインストールされておりますので、InterSafe WebFilter の ICAP 版は InterSafe WebFilter のライセンス追加、i-FILTER の ICAP 版は i-FILTER のライセンス追加のみで、そのままご利用可能です。
ICAP 版(InterScan WebManager/i-FILTER)、PROXY 版(InterSafe/InterScan WebManager)をご利用の際は、ICAP 版(InterSafe WebFilter)をアンインストールいただいた後、ご利用されるソフトのインストールとライセンスの追加が必要です。

・他のフィルタリングソフトをインストールする場合は各フィルタリングソフトのマニュアルを参照してください。
・フィルタリングソフトの対応バージョンは、随時サポートサイトなどでご確認ください。
・ICAP 版使用時は、本サーバのアクセスログへフィルタリングカテゴリ名およびフィルタリング結果を表示させることができます。
「3.5.12.2. キャッシュサーバアクセスログ設定」でログ出力形式に「拡張形式」を選択している場合は、カテゴリ「フィルタリング結果」と「フィルタカテゴリ」にチェックを入れます。ログ出力形式が「Squid 形式」の場合は、自動で出力されます。
なお、フィルタリングカテゴリ名を出力する場合は、以下の作業も行ってください。
1) InterSafe WebFilter／InterScan WebManager の管理画面が開いていれば閉じます。
2) コンソールや telnet などからログオンし、su コマンドで root ユーザになり、
(InterSafe の場合)/usr/local/intersafe/conf/proxy.inf、
(InterScan の場合)/usr/local/iswm/conf/proxy.inf
を以下のように修正します。
[CONTROL_CFG]セクション
ICAP_CATEGORY_NAME=TRUE
3) proxy.inf ファイルを上書きして閉じます。
4) Management Console の「サービス」画面、または InterSafe WebFilter／InterScan WebManager の管理コンソールより、InterSafe WebFilter／InterScan WebManager のサービスを再起動します。

①フィルタ選択



◆ ①フィルタ選択

使用するフィルタリングソフトを選択します。

重要

プレインストールされている InterSafe WebFilter、i-FILTER 以外の InterSafe WebFilter、i-FILTER または InterScan WebManager を使用する場合は「3.3.2. InterSafe WebFilter」の注意事項を参照してください。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。 「ICAP 版(InterSafe WebFilter/InterScan WebManage/i-FILTER)を使用する」を選択した場合→「3.2.20. ICAP サーバ設定」 「PROXY 版(InterSafe WebFilter/InterScan WebManage)を使用する」を選択した場合→「3.2.21. URL フィルタ(PROXY 版)設定」
[戻る]	前画面へ戻ります。

各フィルタリングソフトの利用方法は下記の通りです。

オプションソフト	利用方法	備考
ICAP 版 (InterSafe WebFilter)	出荷時にインストール済みです。 サービス画面にて使用許諾後にサービスとして起動可能になります。ICAP サーバと連携を行う場合は、ICAP サーバ設定画面から 設定します。ICAP 版(InterSafe WebFilter)自体の設定は InterSafe WebFilter の管理コンソールから行います。	HTTP でカプセル化されていない(Native)FTP もフィルタリング対象となります。
ICAP 版 (InterScan WebManager)	別途ソフトウェアを入手しインストールする必要があります。 ICAP サーバと連携を行う場合は、ICAP サーバ設定画面から設定します。ICAP 版(InterScan WebManager)自体の設定は InterScan WebManager の管理コンソールから行います。	HTTP でカプセル化されていない(Native)FTP もフィルタリング対象となります。
ICAP 版 (i-FILTER)	出荷時にインストール済みです。 ICAP サーバと連携を行う場合は、「プロキシ」→「ICAP サーバ設定」画面から設定します。 ICAP 版(i-FILTER)自体の設定は i-FILTER の管理コンソールから行います。	HTTP でカプセル化されていない(Native)FTP もフィルタリング対象となります。
PROXY 版 (InterSafe WebFilter)	別途ソフトウェアを入手しインストールする必要があります。 URL フィルタ(PROXY 版)設定画面にて利用方法(上位/下位)を指定します。PROXY 版 (InterSafe WebFilter)自体の設定は InterSafe WebFilter の管理コンソールから行います。	プリインストール時と同じディレクトリ (/usr/local/intersafe)にインストールしている場合は、サービス画面にて使用許諾後にサービスとして起動可能になります。
PROXY 版 (InterScan WebManager)	別途ソフトウェアを入手しインストールする必要があります。 URL フィルタ(PROXY 版)設定画面にて利用方法(上位/下位)を指定します。PROXY 版 (InterScan WebManager)自体の設定は InterScan WebManager の管理コンソールから行います。	

3.2.20. ICAP サーバ設定

ICAP サーバ設定

この設定は ICAP 版(InterSafe WebFilter/InteScan WebManager/i-FILTER)を本システムで使用するときに必要ですので、必ず行ってください。

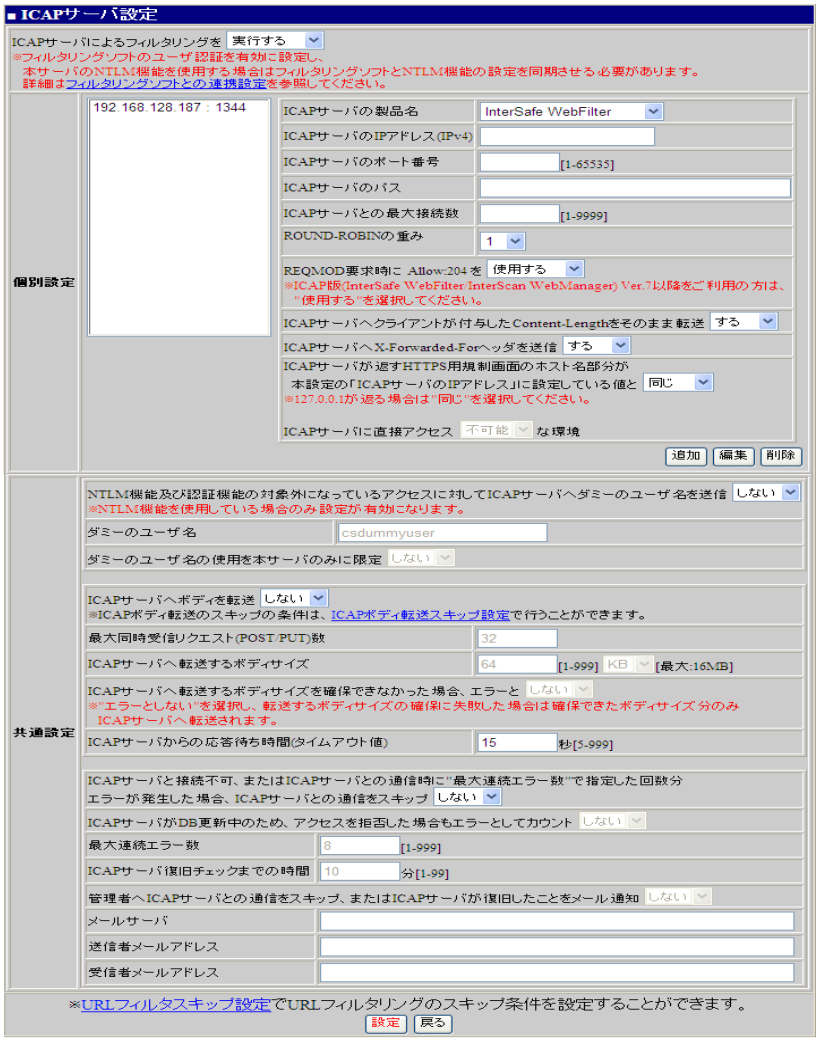
IP アドレスとポート番号などの指定は、「サービス」画面から InterSafe WebFilter/InterScan WebManager/i-FILTER 管理コンソールを起動し、表示する内容に従って設定してください。

なお、本画面で IP アドレスとポート番号を変更しても InterSafe WebFilter/InterScan WebManager /i-FILTER 管理コンソールには反映されません。

フィルタリング機能の対象となるプロトコルは、HTTP、HTTPS、FTP(HTTP でカプセル化された FTP アクセス)、NFTP(HTTP でカプセル化されていない FTP アクセス)になります。

基本設定画面で本サーバのサーバ種別設定を「Forward(透過型 L4 スイッチ)」に設定した場合には InterSafe WebFilter/InterScan WebManager は親プロキシとしてのみ使用可能です。

基本設定画面で本サーバのサーバ種別設定を「Reverse」に設定した場合には InterSafe WebFilter/InterScan WebManager/i-FILTER は使用できません。InterSafe WebFilter/InterScan WebManager/i-FILTER 管理コンソールで IP アドレスやポート番号を変更した場合には必ずこの画面の設定を変更して下さい。



◆ ICAP サーバによるフィルタリングを実行する/実行しない

キャッシュプログラムから InterSafe WebFilter/InterScan WebManager/i-FILTER によるフィルタリングを利用するか利用しないかを選択します。

◆ 個別設定

登録済の ICAP サーバの一覧が表示されます。設定可能数は 16 までです。

ICAP サーバを複数台設定する事で、ROUND-ROBIN による負荷分散と ICAP サーバダウン時の縮退(冗長化)を行うことが可能です。

例えば、CS の冗長化機能で 2 台の CS を使用している際に自 CS 上と相手側 CS 上の二つの ICAP サーバ両方を使用することが可能です。

ICAP サーバを複数台設定する場合は、"ROUND-ROBIN の重み"を選択してください。この中から設定変更、または削除する ICAP サーバの選択を行います。

一覧に表示されている ICAP サーバを選択すると、一覧の隣に ICAP サーバの IP アドレス、ICAP サーバのポート番号などが表示されます。設定の編集後、[編集]を押下することで設定内容を変更することが可能です。

また、ICAP サーバの追加を行うときは、ICAP サーバの IP アドレスなどの必要な設定を行った後、[追加]を押下してください。これにより一覧に新たな ICAP サーバが登録されます。

ICAP サーバの削除を行う場合には、削除したい ICAP サーバを選択後に[削除]を押下して下さい。

なお追加/編集/削除/順序の操作を行った場合であっても、画面下部の[設定]を押下するまでは、サーバに設定内容は反映されません。

本設定の一番上に設定されているものを「3.2.15. HTTPS 可視化機能設定」の[本サーバ外の ICAP サーバへのリクエスト送信モード xxxx]の本サーバとして扱います。

▶ ICAP サーバの製品名

ICAP サーバの製品名を選択します。

設定値	説明
InterSafe WebFilter	InterSafe WebFilter を使用します。
InterScan WebManager	InterScan WebManager を使用します。
i-FILTER Ver.7	i-FILTER Ver.7 を使用します。
i-FILTER Ver.8 以降	i-FILTER Ver.8 以降を使用します。
InterSafe WebFilter V8.5SP1 以降	InterSafe WebFilter V8.5SP1 以降を使用します。
InterScan WebManager V8.5SP1 以降	InterScan WebManager V8.5SP1 以降を使用します。

各製品ごとに ICAP の RFC に準拠していない独自のインタフェースが存在するため、実際の製品と異なる製品を選択した場合は正常な動作を行わない可能性があります。

▶ ICAP サーバの IP アドレス

ICAP サーバの IP アドレスを指定します。

重要

この設定画面で IP アドレスを設定しても InterSafe WebFilter/InterScan WebManager /i-FILTER には反映されません。別途 InterSafe WebFilter/InterScan WebManager /i-FILTER の管理コンソールで指定してください。

▶ ICAP サーバのポート番号

ICAP サーバのポート番号を指定します。InterSafe WebFilter/InterScan WebManager /i-FILTER の管理コンソールにて指定するポート番号を指定してください(通常、InterSafe WebFilter//InterSafe WebFilter v8.5SP1 以降/InterScan WebManager/ InterScan WebManager v8.5SP1 以降は 1344 を、i-FILTER Ver.7 は 13080、i-FILTER Ver.8 以降は 15080 を指定します)。

重要

この設定画面でポート番号を設定をしても InterSafe WebFilter/InterScan WebManager /i-FILTER には反映されません。別途 InterSafe WebFilter/InterScan WebManager /i-FILTER の管理コンソールで指定して下さい。

▶ ICAP サーバのパス

InterSafe WebFilter/InterScan WebManager/i-FILTER のパスを指定します。
URL フィルタリング側のデフォルト値は以下になっています
InterSafe WebFilter ：intersafe
InterSafe WebFilter V8.5SP1 以降：intersafe
InterScan WebManager：iswm
InterSafe WebManager V8.5SP1 以降：iswm
i-FILTER Ver.7：ifilter7icap
i-FILTER Ver.8 以降：ifilter8 (i-FILTER Ver.8 の場合)
i-FILTER Ver.8 以降：ifilter9 (i-FILTER Ver.9 の場合)
i-FILTER のパスは i-FILTER のバージョンによって違います。

重要

・NTLM 機能を使用する際はパスの値でユーザ情報の形式を判断していますので、必ず上記のデフォルト値を設定してください。
・i-FILTER のパスは i-FILTER のバージョンによって違います。

▶ ICAP サーバとの最大接続数

キャッシュプログラムから InterSafe WebFilter/InterScan WebManager/i-FILTER へ接続する TCP コネクションの最大接続数を指定します。

InterSafe WebFilter/InterScan WebManager/i-FILTER 側と制限値が異なる場合、より小さい値に制限されます。

1 から 9999 までの値で制御することができます。

重要

この設定画面で最大接続数を設定しても InterSafe WebFilter/InterScan WebManager /i-FILTER には反映されません。別途 InterSafe WebFilter/InterScan WebManager /i-FILTER の管理コンソールで指定して下さい。

▶ ROUND-ROBIN の重み

ICAP サーバの設定が複数台の場合は、「ROUND-ROBIN の重み」を指定します。重みは 0 から 10 まで指定可能です。この設定は ICAP サーバが複数台設定されている場合に有効となります。「サーバが接続された回数/ROUND-ROBIN の重み」の値が最も小さい ICAP サーバが選択されます。ICAP サーバをスタンバイ用として指定したい場合は、「ROUND-ROBIN の重み」を「0」に設定してください。「0」以外の ICAP サーバが全てダウンしたと判断した際に「0」と設定した ICAP サーバを使用します。

▶ REQMOD 要求時に Allow:204 を使用する/使用しない

ICAP 版(InterSafe WebFilter/InterScan WebManager)をご利用の方は、「使用する」を選択してください。デフォルトは「使用する」です。

設定値	説明
使用する	REQMOD 要求時に Allow:204 を使用する。
使用しない	REQMOD 要求時に Allow:204 を使用しない。

▶ ICAP サーバへクライアントが付与した Content-Length をそのまま転送する/しない

「共通設定」の「ICAP サーバへボディを転送」を「する」と設定している状態で、ボディ部のサイズが「ICAP サーバへ転送するボディサイズ」を超えている場合、クライアントが付与した Content-Length を ICAP サーバへそのまま転送する／しないを指定します。デフォルトは「する」です。

設定値	説明
する	Content-Length を ICAP サーバへそのまま転送する。
しない	Content-Length を ICAP サーバへそのまま転送せずに、実際に ICAP サーバへ転送するボディサイズに変更する。

▶ ICAP サーバへ X-Forwarded-For ヘッダを送信する/しない

ICAP サーバへ X-Forwarded-For でクライアンの IP アドレスを送信するかしないかを選択します。デフォルトは「する」です。

本サーバへアクセスを行ったクライアントの IP アドレスを ICAP サーバのクライアント IP アドレスとして使用する場合は「する」を選択します。

本サーバの IP アドレス自体を ICAP サーバのクライアント IP アドレスとして使用する場合は、「しない」を選択します。

設定値	説明
する	ICAP サーバへ X-Forwarded-For ヘッダを送信する。
しない	ICAP サーバへ X-Forwarded-For ヘッダを送信しない。

▶ ICAP サーバが返す HTTPS 用規制画面のホスト名部分が
本設定の「ICAP サーバの IP アドレス」に設定している値と異なる/同じ

ICAP サーバが返す HTTPS 用規制画面のホスト名部分が「ICAP サーバの IP アドレス」と同じか異なるかを選択します。デフォルトは「同じ」です。

「同じ」の場合、ICAP サーバが返す HTTPS 用規制画面のリダイレクト先は「ICAP サーバの IP アドレス」になります。

負荷分散装置(ロードバランサ)やルータ等が本サーバと ICAP サーバとの間に存在する場合、「異なる」可能性があります。

「異なる」の場合、ICAP サーバが返す HTTPS 用規制画面のリダイレクト先を「ICAP サーバに直接アクセス不可能/可能な環境」の設定によって変更します。

設定値	説明
異なる	ICAP サーバが返す HTTPS 用規制画面のホスト名部分が「ICAP サーバの IP アドレス」と異なる。
同じ	ICAP サーバが返す HTTPS 用規制画面のホスト名部分が「ICAP サーバの IP アドレス」と同じ。

▶ ICAP サーバに直接アクセス不可能/可能な環境

ICAP サーバに直接アクセス可能な環境かどうかを選択します。デフォルトは「不可能」です。

「不可能」の場合、ICAP サーバが返す HTTPS 用規制画面のリダイレクト先を「ICAP サーバの IP アドレス」に変更しアクセスします。

ネットワーク構成等により物理的に直接アクセス不可能な場合だけでなく、意図的に直接アクセスを禁止している場合も該当します。

「可能」の場合、ICAP サーバが返す HTTPS 用規制画面のリダイレクト先に従ってアクセスします。

設定値	説明
不可能	ICAP サーバに直接アクセス不可能な環境。
可能	ICAP サーバに直接アクセス可能な環境。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ 共通設定

各 ICAP サーバで共通な項目の設定を行います。

▶ NTLM 機能及び認証機能の対象外になっているアクセスに対して ICAP サーバへダミーのユーザ名を送信する/しない

NTLM 機能及び認証機能の対象になっていないアクセスに対して、ダミーのユーザ名を送信するかしないかを選択します。デフォルトは「しない」です。

ICAP サーバでユーザ認証を行う設定をされている場合のみ送信「する」を選択してください。送信「する」を選択した場合、ダミーのユーザ情報が送信されるため、URL フィルタスキップ設定のデフォルト値が不要になります。

設定値	説明
する	NTLM 機能及び認証機能の対象になっていないアクセスに対して、ダミーのユーザ名を送信する。
しない	NTLM 機能及び認証機能の対象になっていないアクセスに対して、ダミーのユーザ名を送信しない。

「3.2.9. NTLM 設定」で NTLM 機能「使用する」を選択している場合のみこの設定は有効になります。

▶ ダミーのユーザ名

「NTLM 機能及び認証機能の対象外になっているアクセスに対して ICAP サーバへダミーのユーザ名を送信」に「する」を指定している場合、送信するダミーのユーザ名を指定します。デフォルトは「csdummyuser」です。最大英数 20 文字まで設定することができます。

▶ ダミーのユーザ名の使用を本サーバのみに限定する/しない

ダミーのユーザ名の使用を本サーバのみに限定するかしないかを選択します。デフォルトは「しない」です。「しない」を選択した場合、ダミーのユーザ名でのアクセスを許可します。「する」を選択した場合、ダミーのユーザ名でのアクセスを拒否します。

設定値	説明
する	ダミーのユーザ名でのアクセスを拒否します。
しない	ダミーのユーザ名でのアクセスを許可します。

▶ ICAP サーバへボディを転送する/しない

ボディ部がある場合、当該データを ICAP サーバへ転送する/しないを指定します。
転送するを指定した場合、「最大同時受信リクエスト(POST/PUT)数」、「ICAP サーバへ転送するボディサイズ、「ICAP サーバへ転送するボディサイズを確保できなかった場合、エラーとする/しない」について設定してください。デフォルトは「転送しない」です。

設定値	説明
する	ICAP サーバへボディを転送する。
しない	ICAP サーバへボディを転送しない。

重要

ICAP サーバへボディを転送「する」に設定時、特定の条件でボディを送信したくない場合 ICAP ボディ転送スキップ設定でスキップ設定を行うことができます。

▶ 最大同時受信リクエスト(POST/PUT)数

想定される最大同時受信リクエスト(POST/PUT)数を指定します。デフォルトは 32 です。
「最大同時受信リクエスト(POST/PUT)数 × ICAP サーバへ転送するボディサイズ」の合計が、搭載メモリの 5%かつ 200MB まで設定可能です。

▶ ICAP サーバへ転送するボディサイズ

想定される ICAP サーバへ転送するボディサイズを指定します。デフォルトは 64KB です。
1B から 16MB までの値で制御することができます。指定された最大同時受信リクエスト(POST/PUT)数と ICAP サーバへ転送するボディサイズより転送用ボディバッファ(メモリ)を取得します。

▶ ICAP サーバへ転送するボディサイズを確保できなかった場合、エラーとする/しない

上記、最大同時受信リクエスト(POST/PUT)数と ICAP サーバへ転送するボディサイズより確保した転送用ボディバッファ(メモリ)にて、ICAP サーバへボディを転送するために必要となる容量が確保できなかった場合、確保できたサイズ分だけでも転送するか、エラー応答をクライアントへ返すかを指定します。デフォルトは「しない」です。

設定値	説明
する	エラーとする。(クライアントへエラー応答を返します)
しない	エラーとしない。(確保できたサイズ分ボディを転送します)

▶ ICAP サーバからの応答待ち時間(タイムアウト値)

本サーバから ICAP サーバへの要求に対し応答待ちをする時間を指定します。デフォルトは 15 秒です。5 秒から 999 秒までの値で制御することができます。応答待ち時間を超えた場合は、クライアントにエラー画面が返されます。

重要

・1～4 秒は、通常の遅延発生時にタイムアウトする可能性がある値のため設定できないようになっています。
・デフォルトは、「ICAP サーバが正常に応答できない」と判断出来る値を基準に設定しています。

▶ 当該アクセスにより ICAP サーバのプロセスがダウンした可能性がある場合、最大で xx 台までしかリトライしない

複数の ICAP サーバが登録されている環境で、当該アクセスが原因で ICAP サーバのプロセスがダウンした可能性があると判断した場合、他の ICAP サーバに対して最大で何台までリトライ処理を行うかを設定します。デフォルトは「15 台」です。

0 台から 15 台までの値で制御することができます。

ICAP サーバとの通信において異常を検出した場合、基本的に成功するか全て失敗するまで、登録されている他の ICAP サーバにリトライ処理を行います。

当該アクセスが要因で ICAP サーバのプロセスがダウンする場合、リトライ処理を行った他の ICAP サーバでも同様の現象が発生し、最悪の場合は全ての ICAP サーバのプロセスがダウンする可能性がありますが、リトライ処理を行う台数を制限することにより、その状態を防ぐことができます。

ICAP 要求送信後、ICAP サーバ側が ICAP 応答を返却せずに当該セッションを強制切断した場合に「当該アクセスにより ICAP サーバのプロセスがダウンした可能性がある」と判断します。

重要

設定変更等で ICAP サーバの再起動を行われた場合や他の要因で ICAP サーバ側でセッションの異常切断が発生した場合も、CS からの見え方に差分がないため同様に扱われます。他の異常に関しては、当該アクセスが要因となっている可能性がない、もしくは低いため、本制限の対象にはなりません。

登録している ICAP サーバの台数以上の値を設定した場合は「登録している ICAP サーバの台数 - 1」を設定されている場合と同じ意味になります。

▶ ICAP サーバと接続不可、または ICAP サーバとの通信時に「最大連続エラー数」で指定した回数分エラーが発生した場合 ICAP サーバとの通信をスキップする/しない

ICAP サーバと接続不可、または ICAP サーバとの通信時に「最大連続エラー数」で指定した回数分エラーが発生した場合 ICAP サーバとの通信を自動的にスキップするかを選択します。デフォルトは「しない」です。

設定値	説明
する	ICAP サーバとの通信を自動的にスキップする。
しない	ICAP サーバとの通信を自動的にスキップしない。

重要

「する」を選択すると ICAP サーバとの通信をスキップすることがあり、その場合一時的にフィルタリングが行なわれない状態になります。フィルタリングが必須の場合は「しない」を選択してください。

▶ ICAP サーバが DB 更新中のため、アクセスを拒否した場合もエラーとしてカウントする/しない

ICAP サーバが DB 更新中のため、アクセスを拒否した場合もエラーとしてカウントするかを選択します。デフォルトは「しない」です。

「ICAP サーバと接続不可、または ICAP サーバとの通信時に「最大連続エラー数」で指定した回数分エラーが発生した場合 ICAP サーバとの通信をスキップ」にて「する」を選択している場合に有効となります。

▶ 最大連続エラー数

ICAP サーバとの通信をスキップする判断基準として、最大連続エラー数を指定します。デフォルトは 8 です。

1 回から 999 回までの値で制御することができます。

応答タイムアウト、不正な応答内容、セッションの異常切断を検知した際にエラーとして ICAP サーバ毎にカウントします。

▶ ICAP サーバ復旧チェックまでの時間

ICAP サーバの復旧チェックを行なうまでの時間を指定することができます。デフォルトは 10 分です。1 分から 99 分までの値で制御することができます。

手動で ICAP サーバを復旧するまでは接続不可が続く可能性がありますので、大きめの値を設定してください。(設定例：10 分~60 分)ICAP サーバとの通信をスキップした際、自動的に ICAP サーバの復旧チェックを行ないます。

▶ システム管理者へ ICAP サーバとの通信をスキップ、または ICAP サーバが復旧したことをメール通知する/しない

ICAP サーバと接続不可、または ICAP サーバとの通信時に「最大連続エラー数」で指定した回数分エラーが発生した場合 ICAP サーバとの通信をスキップ「する」に設定した場合、システム管理者宛に ICAP サーバとの通信をスキップした、または ICAP サーバが復旧したことをメールで通知するかを選択します。デフォルトは「しない」です。

設定値	説明
する	メールで通知する。
しない	メールで通知しない。

▶ メールサーバ

メール通知先のメールサーバを IP アドレスまたはホスト名で指定します。

256 文字まで入力できます。

▶ 送信者のメールアドレス

メール通知する際の送信者メールアドレスを指定します。

320 文字まで入力できます。

@以降も必ず記入してください。

▶ 受信者のメールアドレス

メール通知先の際の送信者メールアドレスを指定します。
320 文字まで入力できます。
@以降も必ず記入してください。

重要

・本システムには、InterSafe WebFilter for ICAP、i-FILTER ICAP Server をインストールしています。ご利用の際はライセンスを購入して下さい。本製品添付のバックアップ DVD-ROM(/doc/intersafe/ ディレクトリ配下、/doc/ifilter/ディレクトリ配下)にマニュアルを格納していますので参照して下さい。
・InterSafe WebFilter/InterScan WebManager/i-FILTER の管理コンソールにてのポート番号を変更した場合、必ずこの画面の設定を変更してください。
・特定のアクセスに対してフィルタリング機能を使用しない設定を URL フィルタスキップ設定で行うことができます。設定方法、デフォルトの設定値、注意事項に関しては URL フィルタスキップ設定を参照してください。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.2.21. URL フィルタ(PROXY 版)設定

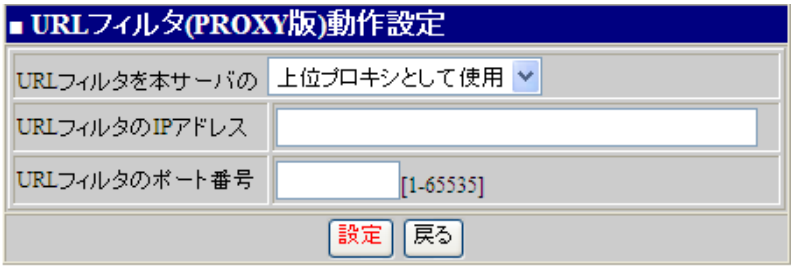
URL フィルタ(PROXY 版)設定

URL フィルタ(PROXY 版)動作設定で、PROXY 版(InterSafe WebFilter/InterScan WebManager)の設定を行います。

この設定は PROXY 版(InterSafe WebFilter/InterScan WebManager)を本システムで使用するときに必要ですので、必ず行ってください。

IP アドレスとポート番号の指定は InterSafe WebFilter/InterScan WebManager で設定する内容に従って設定してください。

なお、この画面で IP アドレスとポート番号を変更しても InterSafe WebFilter/InterScan WebManager には反映されません。



◆ URL フィルタを本サーバの上位プロキシとして使用/下位プロキシとして使用

InterSafe WebFilter/InterScan WebManager を本サーバの上位プロキシとして使用するか下位プロキシとして使用するかを選択します。 デフォルトは「上位プロキシとして使用」です。

設定値	説明
上位プロキシとして使用	URL フィルタを上位プロキシとして使用。
下位プロキシとして使用	URL フィルタを下位プロキシとして使用。

重要

InterSafe WebFilter/InterScan WebManager を上位プロキシとして使用する場合、アクセス制御のプロキシ転送と、隣接プロキシ設定の設定内容が削除されます。
InterSafe WebFilter/InterScan WebManager を上位プロキシとして使用する場合、この画面で設定した IP アドレスとポート番号に基づき InterSafe WebFilter/InterScan WebManager を親プロキシとして設定します。InterSafe WebFilter/InterScan WebManager 以外の親プロキシの設定は削除されます。

◆ URL フィルタの IP アドレス

InterSafe WebFilter/InterScan WebManager の IP アドレスを指定します。InterSafe WebFilter/InterScan WebManager で指定する IP アドレスを指定してください。

重要

この設定画面で IP アドレスを設定をしても InterSafe WebFilter/InterScan WebManager には反映されません。別途 InterSafe WebFilter/InterScan WebManager の管理コンソールで指定してください。

◆ URL フィルタのポート番号

InterSafe WebFilter/InterScan WebManager のポート番号を指定します。InterSafe WebFilter /InterScan WebManager で指定するポート番号を指定して下さい。

この設定画面でポート番号を設定をしても InterSafe WebFilter/InterScan WebManager には反映されません。別途 InterSafe WebFilter/InterScan WebManager の管理コンソールで指定してください。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。

3.3. サービス

サービス

CS で利用可能なサービスの起動状態や設定画面へのリンク一覧を表示します。

◆ OS 起動時の状態

システム起動時に、そのサービスを自動的に起動するかどうかを表示しています。

変更する場合は選択肢を変更して[設定]を押下してください。現在の状態が常に OS 起動時の状態になるものについては、変更ができないようになっています。

OS 起動時の状態を、以下から選択できます。

設定値	説明
起動	システム起動時に起動します。
停止	システム起動時に起動しません。

◆ 現在の状態

サービスの現在の状態を示します。

表示	説明
起動中	サービスが正常に起動している状態となります。
停止中	サービスが停止している状態となります。
-	サービスが使用できない状態です。

◆ (再)起動

✓ ボタンの説明

[起動]	サービスを起動します。
[再起動]	サービスを再起動(停止→起動)します。

◆ 停止

✓ ボタンの説明

[停止]	サービスを停止します。

◆ サービス

サービスの名前が表示されます。この欄をクリックすると、各サービスの詳細設定画面を表示します。

✓ ボタンの説明

[設定]	変更した設定内容を反映する場合に押下します。

InterSec/CS で利用可能なサービスと、初期設定の OS 起動時の状態は下記のとおりです。

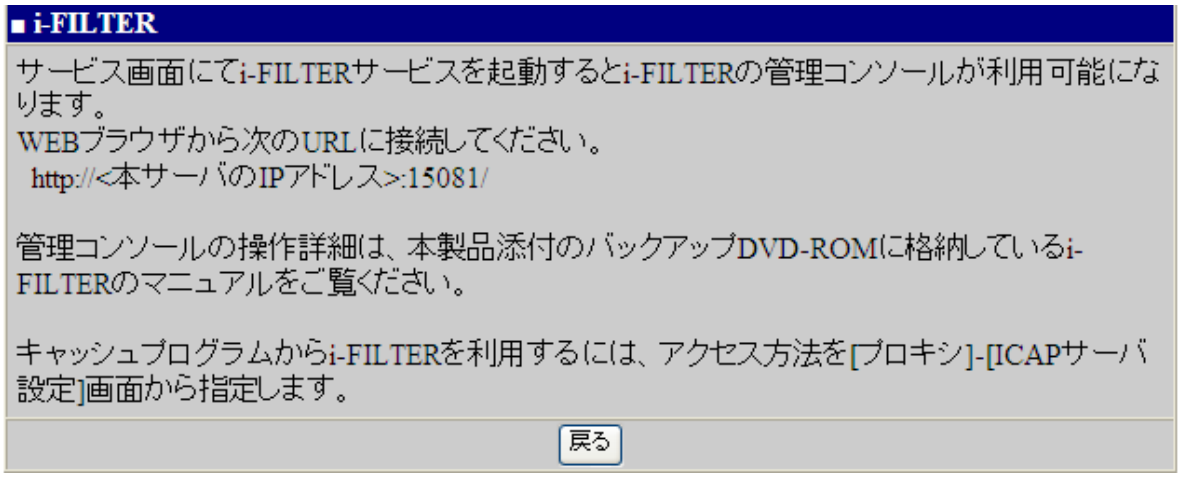
サービス名	初期状態
i-FILTER	停止
InterSafe WebFilter	-
actlog	起動
時刻調整(ntpd)	停止
ネットワーク管理エージェント(snmpd)	停止
リモートシェル(sshd)	停止
リモートログイン(telnetd)	停止
WPAD サーバ(wpad-httpd)	起動

運用形態によって異なる場合がありますので、注意してください。

次ページより各サービスの詳細設定画面について説明します。

3.3.1. i-FILTER

ICAP(Internet ContentAdaptationProtocol)による URL フィルタリングを行えます。(InterSafe WebFilter を ICAP サーバとして使用)。フィルタリングソフトウェアでのプロキシ動作が不要となるため、処理性能が向上します。



✓ ボタンの説明

[戻る]	前の画面へ戻ります。

重要

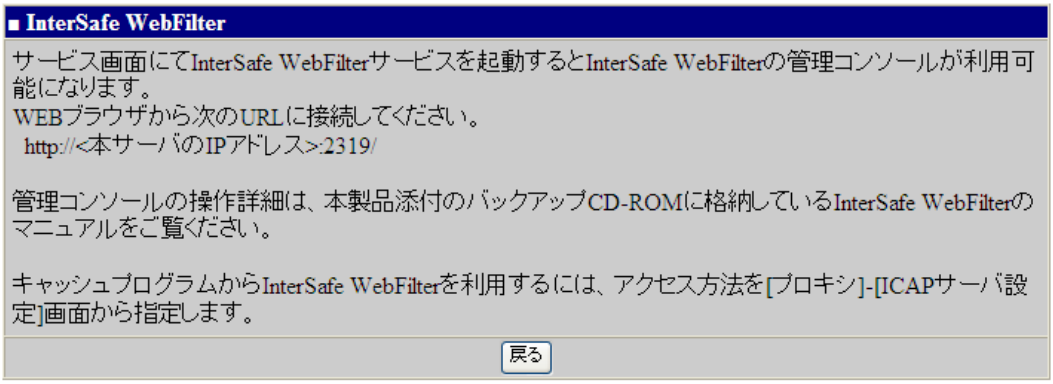
・本画面では、i-FILTER の起動／停止を設定することができます。i-FILTER を利用するには、URL フィルタ設定画面でも i-FILTER の設定が行われている必要があります。
・i-FILTER の使用をやめる場合は、「3.2.19. URL フィルタ選択」で変更を行い、サービス画面で i-FILTER を停止してください。

3.3.2. InterSafe WebFilter

InterSafe WebFilter

ICAP(Internet Content Adaptation Protocol)による URL フィルタリングを行えます。(InterSafe WebFilter を ICAP サーバとして使用)。フィルタリングソフトウェアでのプロキシ動作が不要となるため、処理性能が向上します。初めて利用する際は、右側の「InterSafe WebFilter」のリンクをクリックし、使用承諾契約書の内容をよく読んで「同意する」を押下してください。その後、別の使用承諾契約書が表示されますので同様に内容をよく読んで「同意する」を押下してください。その後、下記画面が表示されます。

【使用許諾に同意後】



✓ ボタンの説明

[戻る]	前画面へ戻ります。

重要

・本画面では、InterSafe WebFilter の起動／停止を設定することができます。
InterSafe WebFilter を利用するには、URL フィルタ設定画面でも InterSafe の設定が行われている必要があります。
・InterSafe WebFilter の使用をやめる場合は、「3.2.19. URL フィルタ選択」で変更を行い、サービス画面で InterSafe WebFilter を停止してください。

3.3.3. 時刻調整(ntpd)

NTP(Network TimeProtocol)は、ネットワークで接続されたコンピュータ同士が連絡を取り合い、時計のずれを自動的に調整する仕組みです。本システムはこの仕組みを利用して、以下の機能を提供しています。

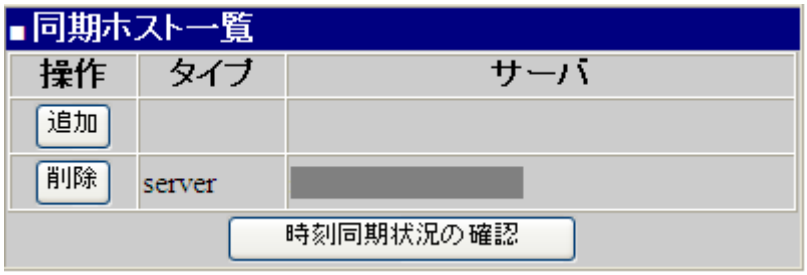
・他の PC が時計を本システムに合わせるのに必要な情報を提供する。
・インターネットの標準時刻サーバに、本システムの時計を合わせる。
・slew モードの有効/無効の設定

時刻調整(ntpd)は以下の画面に分かれています。

■同期ホスト一覧
■日付・時刻
■詳細設定

同期ホスト一覧

設定されているホスト(NTP サーバ)の一覧を示します。設定されていても同期に成功しているとは限りません。時刻同期の状態を確認するには「時刻同期状況の確認」を押下してください。
正しい時刻との時間差が大きいと同期することができません。あらかじめ時刻設定で正しい日時を設定の上、お使いください。



◆ 操作

✓ ボタンの説明

[追加]	新しい同期ホストを追加します。→「3.3.3.1. 時刻同期ホスト追加」
[削除]	同期ホストの削除を行います。

◆ タイプ

同期の方法を表示します。

設定値	説明
server	指定したホストの時刻に、自サーバの時刻を合わせます。
peer	指定したホストの時刻に自サーバの時刻を合わせると同時に、相手の時刻を自サーバに合わせます。

◆ サーバ

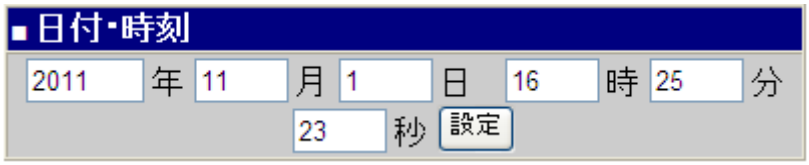
時刻同期を行っている NTP サーバを表示します。

✓ ボタンの説明

[時刻同期状況の確認]	設定されているホストとの時刻同期状況を確認します。新しいホストを追加した後は、同期に成功するまでに最低でも約 5 分程度は時間がかかります。

日付・時刻

このページを開いた時点の日時を表示します。[設定]を押すと、今表示されている時刻がシステムに設定されます。

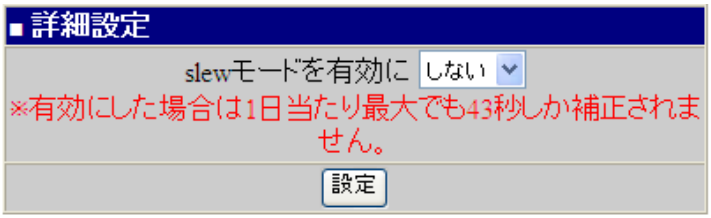


✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

詳細設定

NTP サービスに関する詳細な設定を行います。



◆ slew モードを有効にする/しない

時刻同期の際に少しずつ日付・時刻を修正するか一気に修正するかを選択します。「する」を選択した場合は少しずつ(1 秒毎に 0.0005 秒)日付・時刻を修正します。「しない」を選択した場合は同期している NTP サーバから取得した日付・時刻にそのまま修正します。 デフォルトは「しない」です。

「する」を選択する場合は設定を行う前に正確な日付・時刻を本サーバに設定してください。

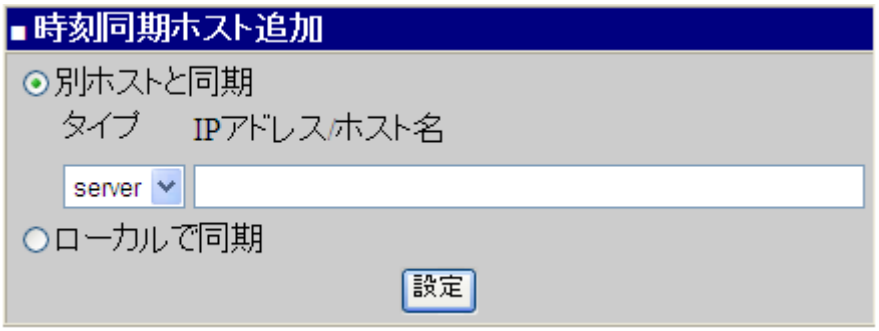
設定値	説明
する	少しずつ(1 秒毎に 0.0005 秒)日付・時刻を修正します。
しない	NTP サーバから取得した日付・時刻にそのまま修正します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

3.3.3.1. 時刻同期ホスト追加

同期を行う NTP サーバを追加します。



◆ 別ホストと同期

NTP サービスを提供している別のサーバと時刻同期を行います。

▶ タイプ

同期の方法を選択します。通常は「server」のままで構いません。

設定値	説明
server	指定したホストの時刻に、自サーバの時刻を合わせます。
peer	指定したホストの時刻に自サーバの時刻を合わせると同時に、相手の時刻を自サーバに合わせます。

▶ IP アドレス/ホスト名

同期ホストの IP アドレス または ホスト名 を入力してください。

◆ ローカルで同期

別のホストを指定せず、自サーバ内で同期を行います。

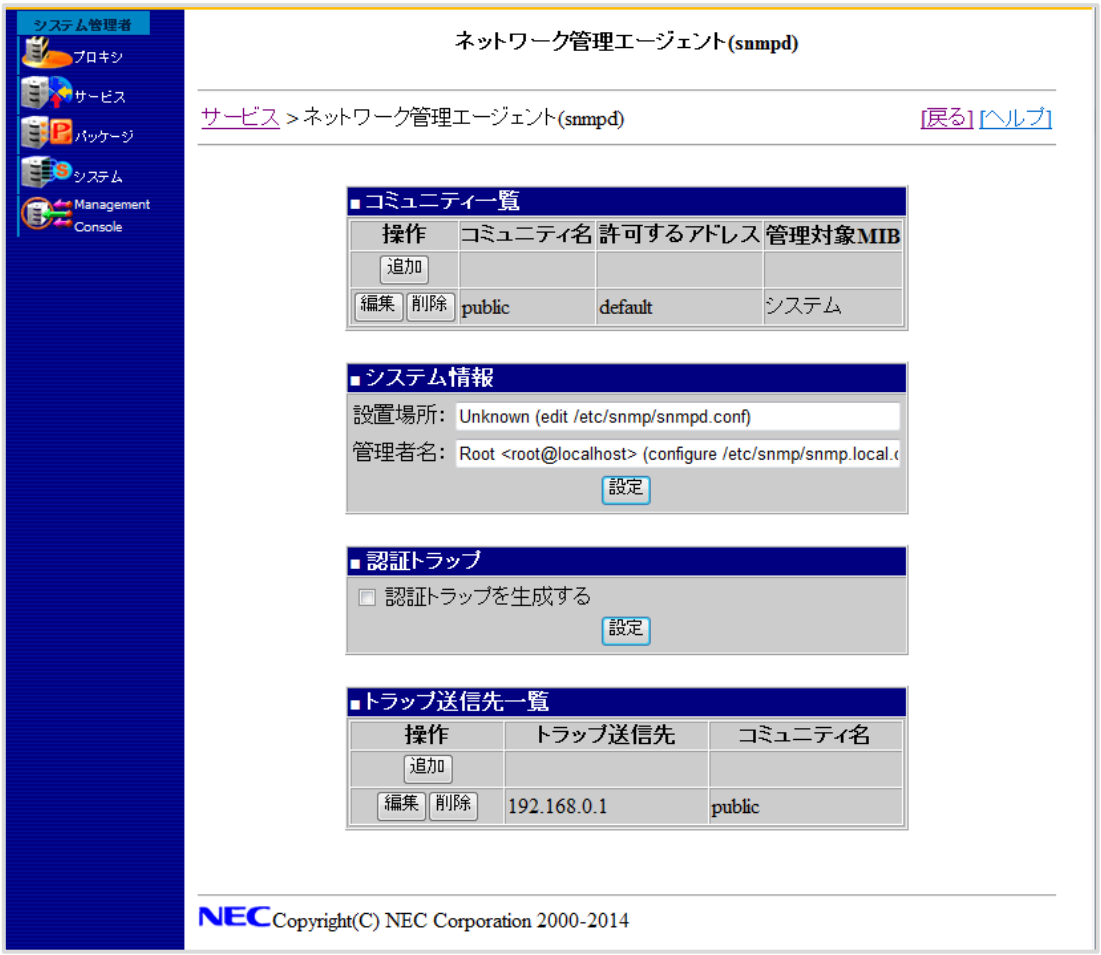
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

3.3.4. ネットワーク管理エージェント(snmpd)

NEC の ESMPRO シリーズや WebSAM シリーズなどの管理マネージャソフトから、このマシンを管理する際に必要となるエージェントソフトです。

管理マネージャからの情報取得要求に応えたり、トラップメッセージを管理マネージャに送信したりします。



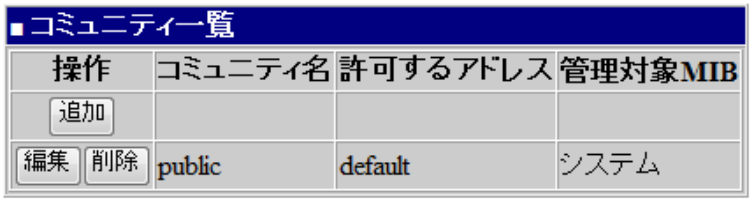
時刻調整(ntpd)は以下の画面に分かれています。

■コミュニティー覧
■システム情報
■認証トラップ
■トラップ送信先一覧

snmpd と ESMPRO/ServerAgentService は別のものとなります。
ネットワーク管理エージェント(snmpd)の設定は、CS にインストールされている snmpd に対して設定を行うものになり、ESMPRO/ServerAgentService に対して設定を行うものではありません。ESMPRO/ServerAgentService の設定を行いたい場合は、ESMPRO/ServerAgentService に対する設定を個別に行って頂く必要があります。

コミュニティー覧

このネットワーク管理エージェントにアクセス可能な管理マネージャマシンを登録します。



◆ 操作

✓ ボタンの説明

[追加]	コミュニティ名を追加します。→「3.3.4.1. コミュニティ追加/編集」
[編集]	コミュニティ名を編集します。→「3.3.4.1. コミュニティ追加/編集」
[削除]	コミュニティ名を削除します。

◆ コミュニティ名

コミュニティ名を表示します。

◆ 許可するアドレス

管理マネージャのアドレスを表示します。すべてのアドレスからのアクセスを許す場合は default と表示します。

◆ 管理対象 MIB

管理対象の MIB を下記から表示します。

表示	説明
システム	.iso.org.dod.internet.mgmt.mib-2.system 情報の読み込みを許可します。
MIB-II	.iso.org.dod.internet.mgmt.mib-2 情報の読み込み、書き込み、通知を許可します。
全て	.iso 情報の読み込み、書き込み、通知を許可します。

重要

- SNMP トラップの MIB 情報に関しては Linux 標準の MIB があります。Linux 標準の net-snmp については、/usr/share/snmp/mibs/以下のディレクトリに格納されています。
- ESMPRO/ServerAgentService の MIB ファイルについては、EXPRESSBUILDER 媒体に格納されています。詳細は、ESMPRO/ServerAgentService のユーザーズガイド(Linux 編)を参照してください。
- CS 独自の MIB 情報はありません。

システム情報

このマシンが設置されている場所や管理者のメールアドレスなどを記入しておいてください。この情報は必要に応じて管理マネージャから読み取られます。
日本語を用いると、マネージャ側で文字化けが発生することがあります。

◆ 設置場所

本装置の設置場所を指定します。

◆ 管理者名

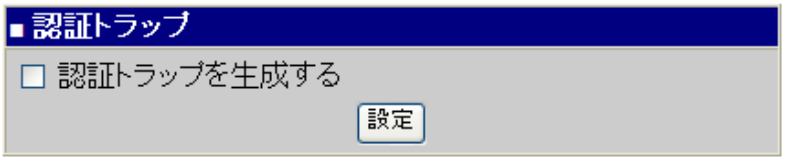
本装置の管理者名を指定します。

✓ ボタンの説明

[設定]	システム情報に指定した内容を設定します。

認証トラップ

不正な管理マネージャが不正なコミュニティ名でアクセスしてきたときに、その旨を正規の管理マネージャに通知するかどうかを指定します。



◆ 認証トラップを生成する

設定値	説明
■チェックあり	認証トラップを通知します。
□チェックなし	認証トラップを通知しません。

✓ ボタンの説明

[設定]	認証トラップに指定した内容を設定します。

トラップ送信先一覧

このマシンに何らかの障害が発生した際に、トラップメッセージを送信する先(管理マネージャ)の一覧を登録します。

◆ 操作

✓ ボタンの説明

[追加]	トラップ送信先を追加します。→「3.3.4.2. トラップ送信先追加/編集」
[編集]	トラップ送信先を編集します。→「3.3.4.2. トラップ送信先追加/編集」
[削除]	トラップ送信先を削除します。

◆ トラップ送信先

トラップ送信先アドレスを表示します。

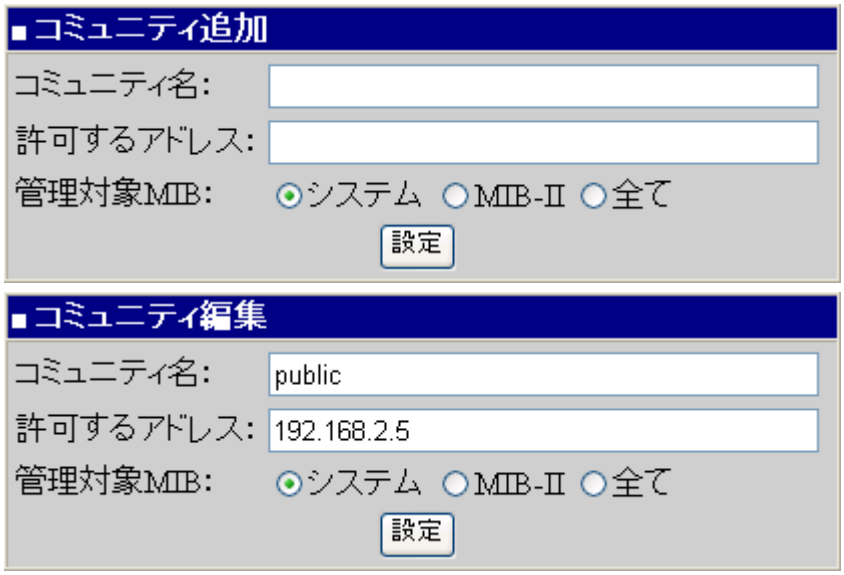
◆ コミュニティ名

コミュニティ名を表示します。

3.3.4.1. コミュニティ追加/編集

コミュニティ追加／コミュニティ編集

このネットワーク管理エージェントにアクセス可能な管理マネージャの登録/編集を行います。



◆ コミュニティ名

コミュニティ名は、管理マネージャと SNMP エージェントの間のパスワードのような役目を果します。

管理マネージャは、ここで設定されたコミュニティ名を知っておく必要があります。

◆ 許可するアドレス

アクセスを許可する管理マネージャのアドレスを指定してください。すべてのアドレスからのアクセスを許す場合は default と指定してください。アドレスとして、192.168.1.0/24 もしくは 192.168.1.0/255.255.255.0 のように記述することでサブネットを指定することも可能です。コミュニティ名の追加処理で追加できる「許可するアドレス」は一つまでとなっておりますので、複数の「許可するアドレス」の追加したい場合は、必要な数分同じコミュニティ名にて追加処理を実施してください。

◆ 管理対象 MIB

管理対象の MIB を下記から選択します。

表示	説明
システム	.iso.org.dod.internet.mgmt.mib-2.system 情報の読み込みを許可します。
MIB-II	.iso.org.dod.internet.mgmt.mib-2 情報の読み込み、書き込み、通知を許可します。
全て	.iso 情報の読み込み、書き込み、通知を許可します。

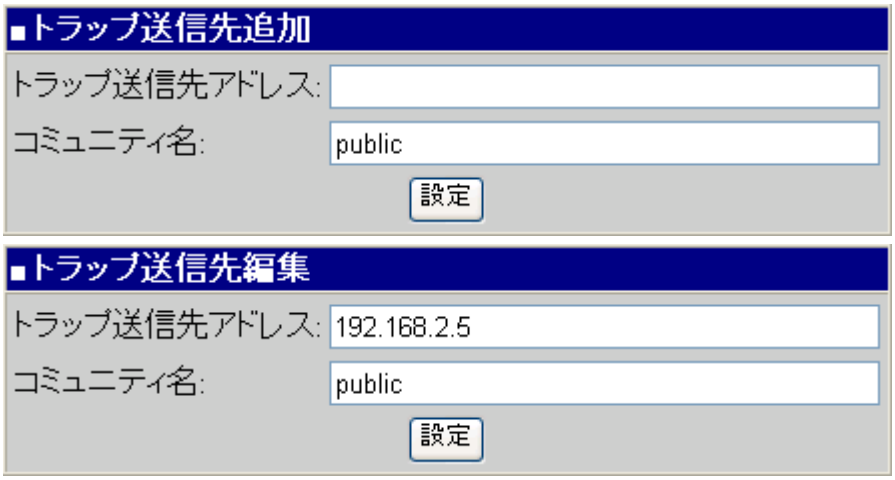
✓ ボタンの説明

[設定]	指定した内容を設定します。

3.3.4.2. トラップ送信先追加/編集

トラップ送信先の追加／トラップ送信先の編集

このマシンに何らかの障害が発生した場合などに、トラップメッセージを送信する先(管理マネージャ)の登録/編集を行います。



◆ トラップ送信先アドレス

トラップメッセージを送信する先のマシンの IP アドレスを指定してください。トラップ送信先の追加処理で追加できるトラップ送信先は一つまでとなっておりますので、複数のトラップ送信先を追加したい場合は、必要な数分トラップ送信先の追加処理を実施してください。

◆ コミュニティ名

適当なコミュニティ名を指定してください。

この名前は、管理マネージャ側でトラップメッセージを振り分ける際に使用されます。

「3.3.4. ネットワーク管理エージェント(snmpd)」の「■コミュニティー覧」で指定したものと別の名前でも構いません。

✓ ボタンの説明

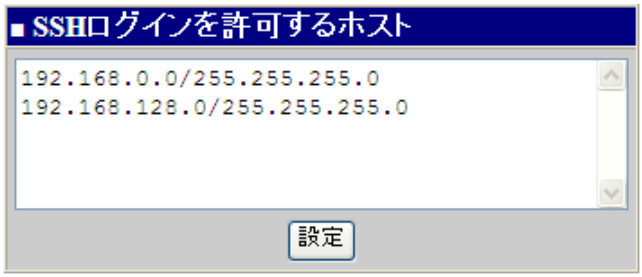
[設定]	指定した内容を設定します。

3.3.5. リモートシェル(sshd)

リモートシェル(sshd)

他のコンピュータ(ホスト)から本システムに接続(sshd は暗号化)することを可能にする機能です。Management Console では対応できない特別な操作を行いたい場合にだけこの機能を有効にします。通常の運用時に有効にする必要はありません。有効にしている間はセキュリティのレベルが低下しますので、通常は無効にしておくことをお勧めします。

ログイン可能なホストを各種形式で指定します。カンマで区切って複数のホストを指定可能です。IP アドレスやホスト名以外にも各種指定形式をサポートしています。



SSH ログインを許可するホストの追加・編集許可するホストを指定します。次のような形式でカンマ(,)で区切って列挙して指定できます。

設定値	説明
ALL	すべてを意味する ALL を指定できます。
ホスト名	DNS や/etc/hosts ファイルなどに登録されているホスト名を指定できます。
IP アドレス	クライアントの IP アドレスを指定できます。例えば、192.168.0.1 など。
ネットワークアドレスとサブネットマスク	ネットワークアドレスとサブネットマスクを使ってアドレスの範囲を指定できます。例えば、192.168.0.0/255.255.255.0 など(192.168.0.0 から 192.168.0.255 までの 256 個のアドレスにマッチします)。
ドメインに対するワイルドカード	ドメインに対してワイルドカードを指定できます。例えば、.example.co.jp など(example.co.jp に属するホスト名にマッチします)。最初の文字がドット(.)で始まることに注意してください。
ネットワークアドレスに対するワイルドカード	ネットワークアドレスに対してワイルドカードを指定できます。例えば、198.168.など(IP アドレスが 192.168.x.x であるホストにマッチします)。最後の文字がドット(.)で終わることに注意してください。

✓ **ボタンの説明**

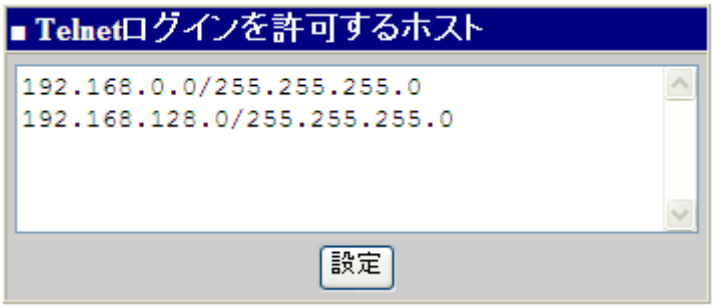
[設定]	入力した内容を設定し、内容を反映させます。

3.3.6. リモートログイン(tenlentd)

telnet ログインを許可するホスト

他のコンピュータ(ホスト)から本システムに接続(telnetd は非暗号化)することを可能にする機能です。Management Console では対応できない特別な操作を行いたい場合にだけこの機能を有効にします。通常の運用時に有効にする必要はありません。有効にしている間はセキュリティのレベルが低下しますので、通常は無効にしておくことをお勧めします。

「Telnet/SSH ログインを許可するホスト」画面にて、ログイン可能なホストを各種形式で指定します。カンマで区切って複数のホストを指定可能です。IP アドレスやホスト名以外にも各種指定形式をサポートしています。



設定内容は「3.3.5. リモートシェル(sshd)」と同じです。

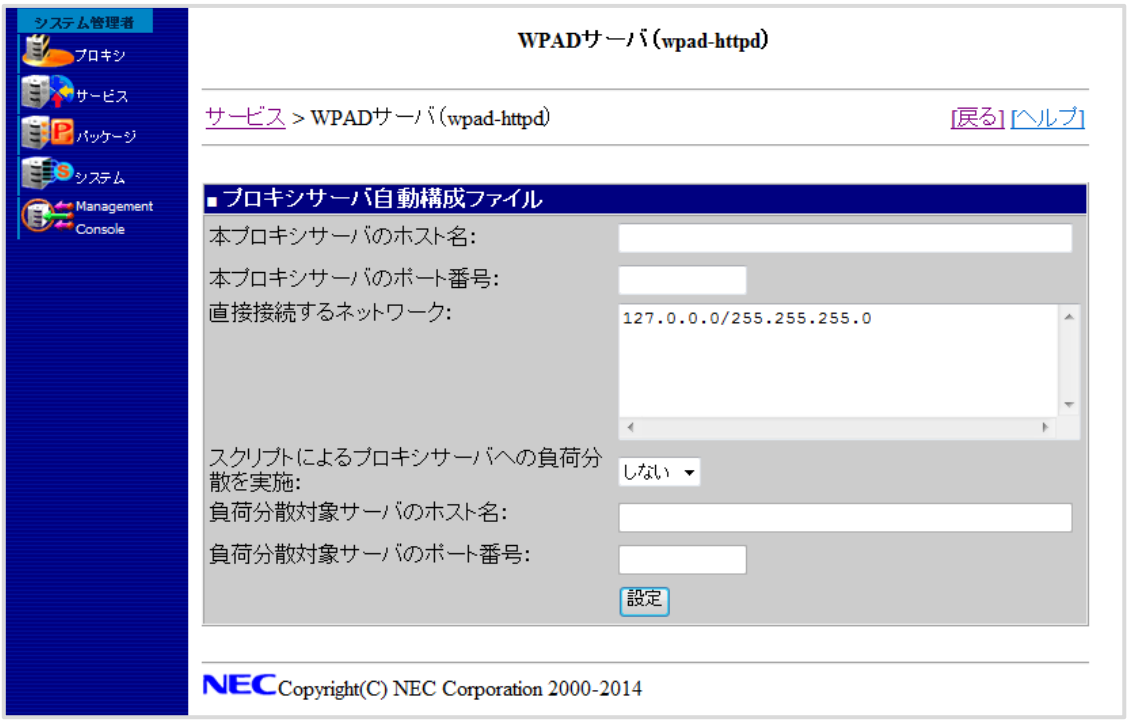
「3.3.5. リモートシェル(sshd)」の説明を参照ください。

3.3.7. WPAD サーバ(wpad-httpd)

プロキシサーバ自動構成ファイル

本システムをフォワードプロキシとして利用している際に、ブラウザ側でのプロキシ設定を自動化するための機能です。Internet Explorer 5.0 以降で対応しています。本機能を利用するためには、ブラウザの参照している DNS サーバおよび DHCP サーバを適切に設定する必要があります。

「プロキシサーバ自動構成ファイル」画面で本システムに接続する際に使用するホスト名とポート番号を設定します。本システムを通さないで接続すべきマシンがあれば、ネットワークアドレス単位で指定することが可能です。



重要

WPAD サーバは本システムのサーバ種別を「Forward」、「Forward（透過型 L4 スイッチ）」に設定したときにご利用いただけます。

WPAD(Web Proxy Auto-Discovery)とは、クライアント Web ブラウザのプロキシサーバ設定を自動化するためのプロトコルです。
Web ブラウザのプロキシサーバを設定するには、以下のような方法があります。

・手動で設定する
プロキシサーバのホスト名(IP アドレス)、ポート番号、直接接続するネットワーク等を手動で設定します。

・プロキシサーバ自動構成ファイルの URL を指定する
Netscape Communicator や Internet Explorer では、JavaScript で記述されたファイルを読み込んでプロキシサーバを自動設定することができます。システム管理者は、自動構成ファイルをイントラネット内の WWW サーバ上に配置しておき、クライアントではその URL を指定します。例えば「http://ホスト名/proxy.pac」などになります。

・WPAD で自動設定する
クライアントでの設定をさらに簡略化するための方法で、URL を指定する必要もありません。Internet Explorer 5 以降などで対応しています。WPAD 対応 Web ブラウザは、まず DHCP サーバから自動構成ファイルの URL を取得しようと試み、失敗した場合は「wpad」というホスト名のマシンから自動構成ファイル(Internet Explorer では「/wpad.dat」)を取得しようとします。システム管理者は、DHCP サーバと DNS サーバの設定を適切に行っておく必要があります。また自動構成ファイルは上記と同じものが利用できます。

WPAD サーバとは
本サーバに付属の WPAD サーバは、クライアントからの要求に応えて、プロキシサーバ自動構成ファイルを返すための専用サーバです。デフォルトはポート 80 番で動作します。

◆ 本プロキシサーバのホスト名

本プロキシサーバのホスト名(または IP アドレス)を指定してください。

◆ 本プロキシサーバのポート番号

本プロキシサーバのポート番号を指定してください。
ポート番号は 80 および 1025 から 65535 まで指定可能です。

◆ 直接接続するネットワーク

プロキシサーバを経由せず、直接接続するネットワークを指定してください。「IP アドレス/ネットマスク」の形式で指定します。その他の形式では指定できませんのでご注意ください。
例えば「127.0.0.0/255.255.255.0」などになります。

◆ スクリプトによるプロキシサーバへの負荷分散を実施

システム冗長化機能を使用している状態でスクリプトによる負荷分散を行う(アクティブ-アクティブ構成)場合は、両方(稼働系、待機系)に「する」を設定してください。
また、本画面の設定内容は両方(稼働系、待機系)同じに設定してください。
システム冗長化機能を使用している状態でスクリプトによる負荷分散を行わない(アクティブ-スタンバイ構成)場合は、両方(稼動系、待機系)に「しない」を設定してください。
クライアント自身の IP アドレスを振分けのキーとして、負荷分散を行います。

設定値	説明
する	スクリプトによる負荷分散を行います。
しない	スクリプトによる負荷分散を行いません。

◆ 負荷分散対象サーバのホスト名

負荷分散を実施する場合は、負荷分散対象サーバとなるホスト名(または IP アドレス)を指定してください。

◆ 負荷分散対象サーバのポート番号

負荷分散を実施する場合は、負荷分散対象サーバのポート番号を指定してください。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

3.4. パッケージ

本システムにインストールされているアプリケーションなどのソフトウェアパッケージのアップデートやインストール、インストールされているパッケージの一覧を確認する画面です。

パッケージは以下の画面に分かれています。

■オンラインアップデート
■手動インストール
■パッケージの一覧

オンラインアップデート

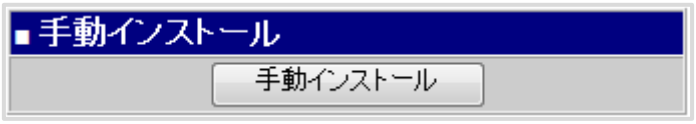
オンラインアップデートを利用すると、Management Console から簡単にアップデートモジュールをインストールすることができます。アップデートモジュールとは、本システムに追加インストール(アップデート)可能なソフトウェアで、弊社で基本的な動作確認を行って公開しているものです。内容は、既存ソフトウェアの出荷後に発見された不具合修正や機能追加などが主ですが、新規ソフトウェアが存在することもあります。オンラインアップデートでは、現在公開されている本システム向けのアップデートモジュールの一覧を参照し、安全にモジュールをインストールすることができます。

✓ ボタンの説明

[オンラインアップデート]	オンラインアップデートを行います。→「3.4.1. ユーザ認証」

手動インストール

ローカルディレクトリのファイル名、または URL、PROXY、PORT を指定して RPM パッケージをインストールすることができます。

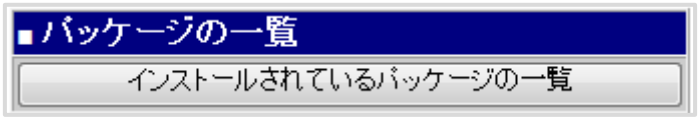


✓ ボタンの説明

[手動インストール]	手動インストールを行います。→「3.4.2. 手動インストール」

パッケージの一覧

現在本システムにインストールされている RPM パッケージの一覧を確認することができます。また、アンインストール作業を行うこともできます。



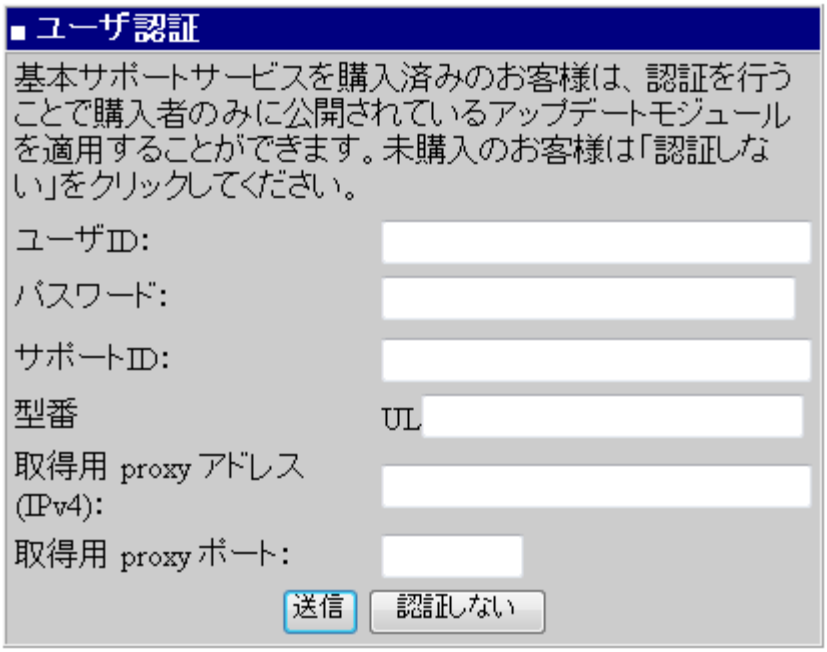
✓ ボタンの説明

[インストールされているパッケージの一覧]	パッケージの一覧を表示します。 →「3.4.3. パッケージ一覧」

3.4.1. ユーザ認証

ユーザ認証

基本サポートサービスを購入済みのお客様向け認証ページです。未購入のお客様は「認証しない」をクリックして次へ進んでください。基本サポートサービスを購入された客様は、認証することで全てのアップデートモジュールを参照することが可能です。未購入のお客様は、購入者向けに公開されているモジュールは参照できません。



- **ユーザ ID**

  ユーザ ID を入力します。

- **パスワード**

  パスワードを入力します。

- **サポート ID**

  契約の際に取得した、サポートＩＤを入力します。

- **型番**

  お客様でご利用になられているソフトウェア製品型番を入力します。

- **取得用 proxy アドレス(IPv4)**

  プロキシサーバのＩＰアドレスを入力します。

- **取得用 proxy ポート**

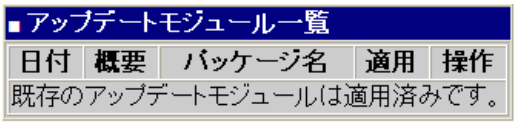
  外部との接続ができる proxy のポート番号を指定します。

✓ **ボタンの説明**

[送信]	ユーザ認証を行います。
[認証しない]	ユーザ認証を行わず、アップデートモジュールを取得します。

3.4.1.1. アップデートモジュール一覧

アップデートモジュール一覧



重要

・アップデートモジュールを適用後も適用状態が「未」と表示される場合は、モジュールの適用に失敗したか、システムの再起動を行っていない可能性があります。
・オンラインアップデート時は、本サーバがクライアントとなり、アップデート Web 用サーバへ接続します。「取得用 proxy アドレス」に本サーバを設定している場合、事前に以下の画面で自身からのアクセスを受け付ける設定にしておいてください。
「3.2.2. セキュリティ設定」
「3.2.6. アクセス制御」

◆ 日付

アップデートモジュールの公開日付を表示します。

◆ 概要

アップデートモジュールの概要を表示します。
[詳細情報]のリンクがある場合、アップデートモジュールの詳細情報を表示できます。

◆ パッケージ名

アップデートモジュールに含まれる主なパッケージを表示します。

◆ 適用

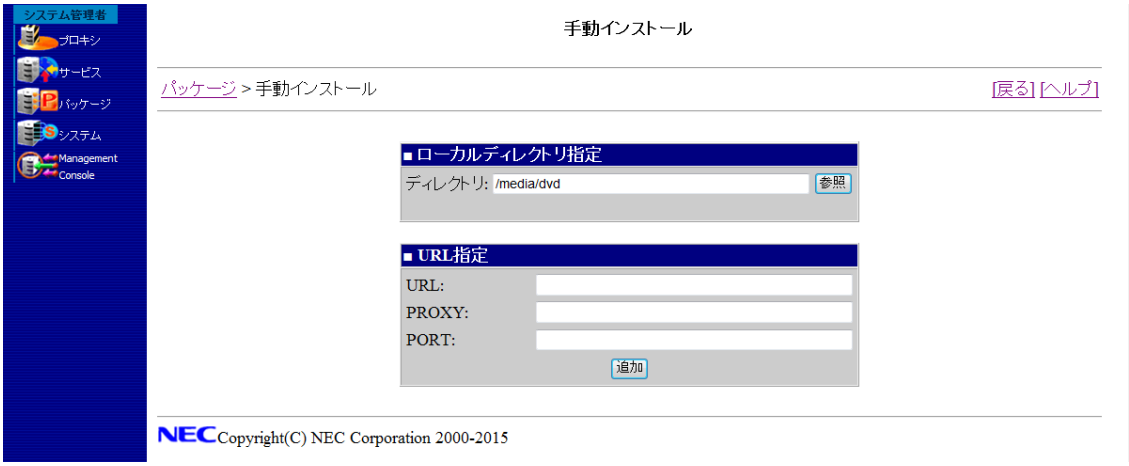
アップデート適用の有無を表示します。

✓ ボタンの説明

[適用]	取得したアップデートモジュールを[適用]を押下後に適用します。

3.4.2. 手動インストール

ローカルディレクトリのファイル名、または URL、PROXY、PORT を指定して RPM パッケージをインストールすることができます。



手動インストールは以下の画面に分かれています。

■ローカルディレクトリ指定
■URL 指定

開発元や販売店などで保証されているパッケージ以外をインストール、アップグレードした場合には、システムの動作保証を行うことができませんので、ご注意ください。

ローカルディレクトリ指定

DVD-ROM やローカルディスクから、パッケージのインストールを行います。

◆ ディレクトリ

パッケージが存在するディレクトリを指定します。パッケージ名を選択すると、選択したパッケージの情報が表示されます。

DVD-ROM からインストールする場合には「/media/dvd」で始まるディレクトリ名を指定してください。

✓ ボタンの説明

[参照]	ディレクトリ配下のディレクトリおよびパッケージ情報が表示されます。

URL 指定

Web サイトや FTP サイトからパッケージのインストールを行います。

◆ URL

URL 指定でパッケージをインストールするときはこちらを使用します。http://～や ftp://～で始まる URL でパッケージ名を指定することができます。

◆ PROXY

FTP もしくは HTTP をプロキシ経由で実行する場合に、プロキシサーバのアドレスを指定します。省略可能です。

◆ PORT

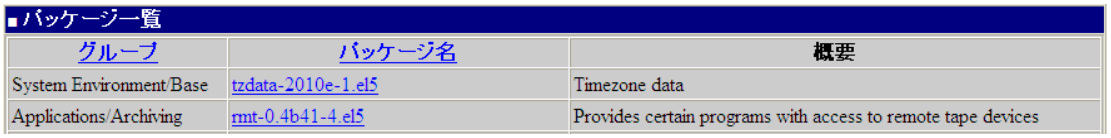
FTP もしくは HTTP をプロキシ経由で実行する場合に、プロキシサーバのポートを指定します。省略可能です。

✓ ボタンの説明

[追加]	パッケージのインストールが行われます。

3.4.3. パッケージ一覧

現在本システムにインストールされている RPM パッケージの一覧を確認することができます。また、アンインストール作業を行うこともできます。



■パッケージ一覧

グループ	パッケージ名	概要
System Environment/Base	tzdata-2010e-1.el5	Timezone data
Applications/Archiving	rmt-0.4b41-4.el5	Provides certain programs with access to remote tape devices

- **グループ**

  グループ名を表示します。

- **パッケージ名**

  パッケージ名を表示します。

  パッケージ名をクリックすると、パッケージ名順に並び替えます。

  各パッケージ名のリンクをクリックすると、該当パッケージ情報ページを表示し、アンインストールを行うことができます。

- **概要**

  パッケージの概要を表示します。

3.5. システム

システムの停止/再起動や本製品の状態確認、システムの管理を行います。

システムは以下の画面に分かれています。

■システム停止/再起動
■状態
■その他

システム停止/再起動

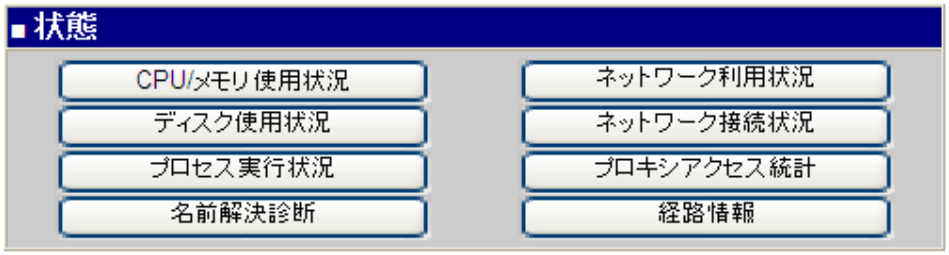
システムの停止・再起動を行います。

✓ ボタンの説明

[システムの停止]	システムを停止します。　→「3.5.1. システムの停止」
[システムの再起動]	システムを再起動します。　→「3.5.2. システムの再起動」

状態

本システムの各状況を表示します。

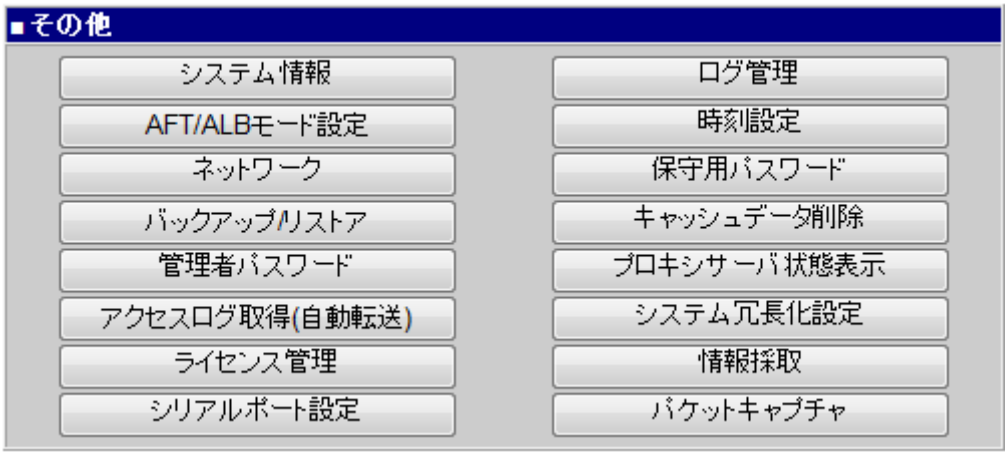


✓ ボタンの説明

[CPU/メモリ使用状況]	CPU/メモリ使用状況を表示します。 →「3.5.3. CPU/メモリ使用状況」
[ネットワーク利用状況]	ネットワーク利用状況を表示します。 →「3.5.4. ネットワーク利用状況」
[ディスク使用状況]	ディスク使用状況を表示します。 →「3.5.5. ディスク使用状況」
[ネットワーク接続状況]	ネットワーク接続状況を表示します。 →「3.5.6. ネットワーク接続状況」
[プロセス実行状況]	プロセス実行状況を表示します。 →「3.5.7. プロセス実行状況」
[プロキシアクセス統計]	プロキシアクセス統計を表示します。 →「3.5.8. プロキシアクセス統計」
[名前解決診断]	名前解決診断を表示します。 →「3.5.9. 名前解決診断」
[経路情報]	経路情報を表示します。 →「3.5.10. 経路情報」

その他

システムの停止・再起動を行います。



✓ ボタンの説明

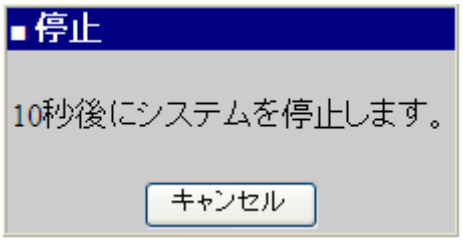
[システム情報]	システム情報を表示します。 →「3.5.11. システム情報」
[ログ管理]	ログの管理を行います。 →「3.5.12. ログ管理」
AFT/ALB モード設定	AFT（Adapter FaultTolerance）/ALB（Adaptive LoadBalancing）モードの設定を行います。 →「3.5.13. AFT/ALB モード設定」
[時刻設定]	NTP による時刻調整の設定を行います。 →「3.5.14. 時刻設定」
[ネットワーク]	ネットワークの設定を行います。 →「3.5.15. ネットワーク」
[保守用パスワード]	保守用ユーザのパスワードを設定します。 →「3.5.16. 保守用パスワード」
[バックアップ/リストア]	バックアップ/リストアを行います。 →「3.5.17. バックアップ/リストア」
[キャッシュデータ削除]	キャッシュデータの削除を行います。 →「3.5.18. キャッシュデータ削除」
[管理者パスワード]	管理者のパスワードを設定します。 →「3.5.19. 管理者パスワード」
[プロキシサーバ状態表示]	プロキシサーバの状態を表示します。 →「3.5.20. プロキシサーバ状態表示」
[アクセスログ取得(自動転送)]	アクセスログの転送設定を行います。 →「3.5.21. アクセスログ取得(自動転送)」
[システム冗長化設定]	冗長化設定を行います。 →「3.5.22. システム冗長化」

[ライセンス管理]	ライセンスのインストール/アンインストールを行います。 →「3.5.23. ライセンス管理」
[情報採取]	ログ情報などの採取を行います。 →「3.5.24. 情報採取」
[シリアルポート設定]	シリアルコンソールに接続をするシリアルポートを設定します。 →「3.5.25. シリアルポート設定」
[パケットキャプチャ]	パケットキャプチャを行います。 →「3.5.26. パケットキャプチャ」

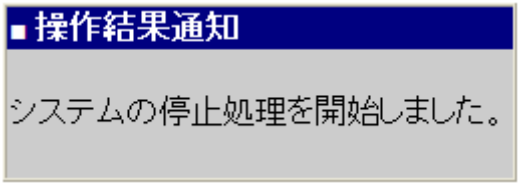
3.5.1. システムの停止

システムを停止(シャットダウン)します。システム停止確認ダイアログが表示されるので、[OK]押下で停止を行います。[キャンセル]押下で停止処理を中断できます。

システム停止待機画面にて[キャンセル]押下で停止処理を中断できます。



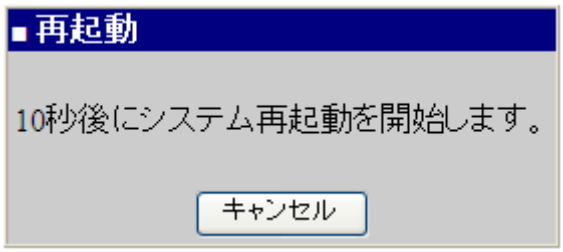
システム停止待機画面にて 10 秒間[キャンセル]を非押下で停止処理を開始します。



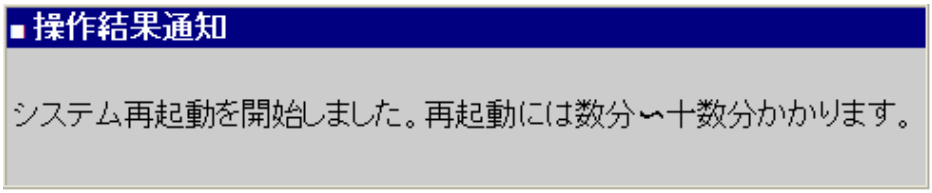
3.5.2. システムの再起動

システムを再起動（リブート）します。システム再起動確認ダイアログが表示されるので、[OK]押下で再起動を行います。[キャンセル]押下で再起動処理を中断できます。

システム再起動待機画面にて[キャンセル]押下で再起動処理を中断できます。



システム再起動待機画面にて 10 秒間[キャンセル]を押下しないと、以下のシステム再起動画面が表示されます。



しばらく待ち Management Console のどれかのメニューを選択して画面が表示されるようになれば、システムの再起動が完了したことになります。

3.5.3. CPU/メモリ使用状況

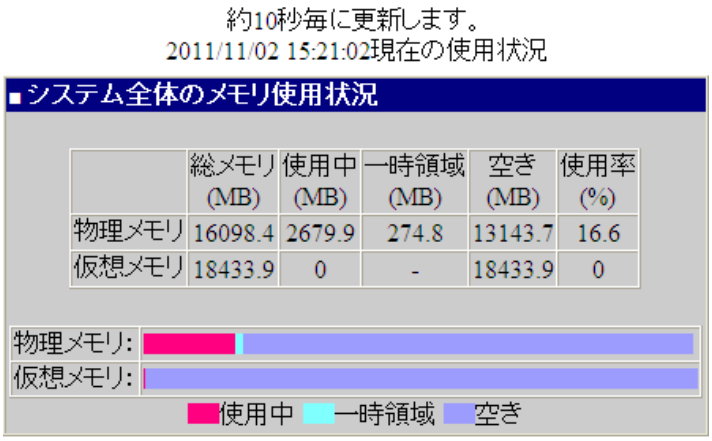
メモリの使用状況と CPU の使用状況をグラフと数値で表示します。約 10 秒ごとに最新の情報に表示が更新されます。また、CPU 使用率と負荷、ネットワークについて、調節を行うことができます(上級者向け)。設定を変更する場合は、環境や使用状況にあわせて値をチューニングしてください。

CPU/メモリ使用状況は以下の画面に分かれています。

■システム全体のメモリ使用状況
■システム全体の CPU 使用状況
■チューニングパラメータ

システム全体のメモリ使用状況

物理メモリ、仮想メモリについて、総容量、使用中、一時領域(物理メモリのみ)、空き容量、使用率を10 秒間隔で表示します。



- **総メモリ**

  物理メモリ、仮想メモリの総容量を表示します。

- **使用中**

  OS 及び稼動しているサービスが占有している物理メモリ、仮想メモリの容量を表示します。

- **一時領域**

  OS 及び稼動しているサービスが一時的に使用する物理メモリの容量を表示します。

  Linux の free コマンドで表示される buffers、cached の内、OS 及び稼動しているサービスが占有していないメモリの容量を表示します。

- **空き**

  物理メモリ、仮想メモリの空き容量を表示します。

  「総メモリ － 使用中 － 一時領域」の値が空き容量になります。

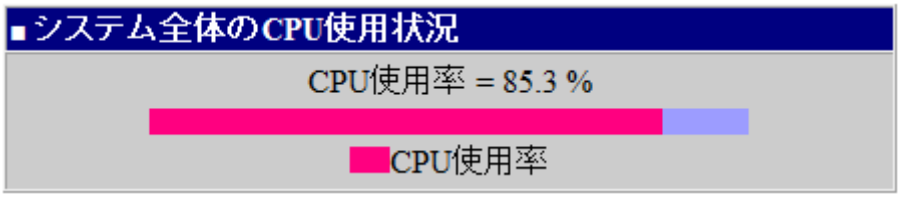
- **使用率**

  総メモリに対する使用中の割合を表示します。

システム全体の CPU 使用状況

CPU 使用状況を、10 秒間隔で表示します。

この CPU 使用状況は、特定のプロセスの CPU 負荷を表すものではなく、本サーバ全体の状況を表します。



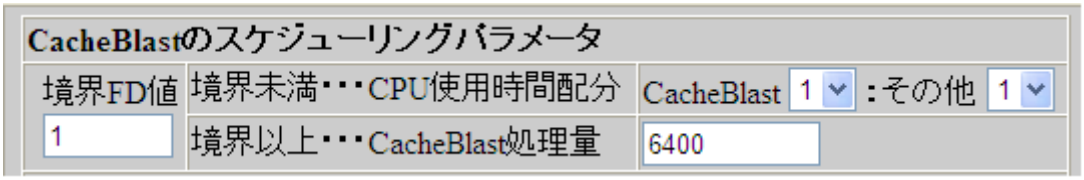
CacheBlast のスケジューリングパラメータ

本サーバ(CacheBlast)が使用するスケジューリングパラメータを調節することができます。
このパラメータを調整することで CPU 負荷と性能のバランスを調整できます。
本設定は、プロキシサービスを停止することなく動的に変更可能です。

CacheBlast は、以下のように 2 つのスケジューリングパターンを保持しており、境界 FD 値を元にどちらのパターンを使用するか決定します。
境界 FD 値は判定時のセッション数とお考えください。

- 処理中の接続数が境界 FD 値未満の場合・・・
  CacheBlast とそれ以外の CPU 使用時間配分が一定となるようにスケジューリングします。

- 処理中の接続数が境界 FD 値以上の場合・・・
  CacheBlast が一定量の処理を行ったあとに、一度 CPU を開放するようにスケジューリングします。



◆ 境界 FD 値

このパラメータは、CacheBlast が 2 つあるスケジューリングパターンのどちらを使用するのか決定するために使用されます。デフォルトは 1 です。
常に CPU 使用時間配分をベースとしたスケジューリングパターンを使用する場合は「16020」を、常に CacheBlast の処理量をベースとしたスケジューリングパターンを使用する場合は「1」を設定してください。

◆ 境界未満・・・CPU 使用時間配分

このパラメータは本サーバが境界 FD 値未満の接続を処理している際に、CacheBlast とそれ以外の部分がそれぞれ使用する CPU 時間の割合を設定します。1 ～9 まで指定可能です。デフォルトは 1 です。
1：1 と 2：2 では、割合は同じになりますが、後者は切り替わる間隔が 2 倍になります。

◆ 境界以上・・・CacheBlast 処理量

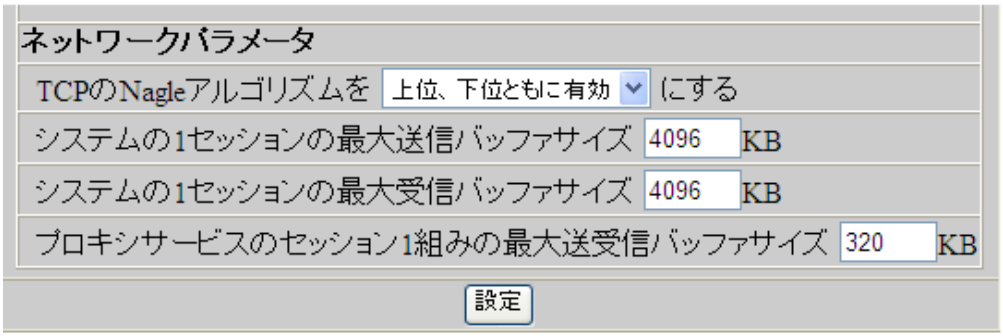
このパラメータは、本サーバが境界 FD 値以上の接続を処理している際に、CacheBlast が一度にどのくらい接続処理を実行するか指定します。

1～999999999 まで指定可能です。デフォルトは 6400 です。

フィルタリングソフトなど、本サーバ上で動作するアプリケーションソフト使用時は、CacheBlast の使用率が極端に高くならないようにご注意ください。
設定を変更する場合は、環境や値用状況にあわせて値をチューニングしてください。

ネットワークパラメータ

本サーバのネットワークに関するパラメータを設定することができます



◆ TCP の Nagle アルゴリズムを有効/無効にする

このパラメータは TCP セッションの Nagle アルゴリズムの有効/無効を指定します。

(デフォルト：上位、下位ともに有効にする)

◆ システムの 1 セッションの最大送信バッファサイズ

本サーバのシステム(OS)が 1 セッション当たりに使用する送信バッファの最大サイズを指定します。

4KB～4096KB まで制御可能です。

◆ システムの 1 セッションの最大受信バッファサイズ

本サーバのシステム(OS)が 1 セッション当たりに使用する受信バッファの最大サイズを指定します。

4KB～4096KB まで制御可能です。

◆ プロキシサービスのセッション 1 組みの最大送受信バッファサイズ

プロキシサービスがセッション 1 組み当たりに使用する送受信バッファの最大サイズを指定します。

28KB～8192KB まで制御可能です。

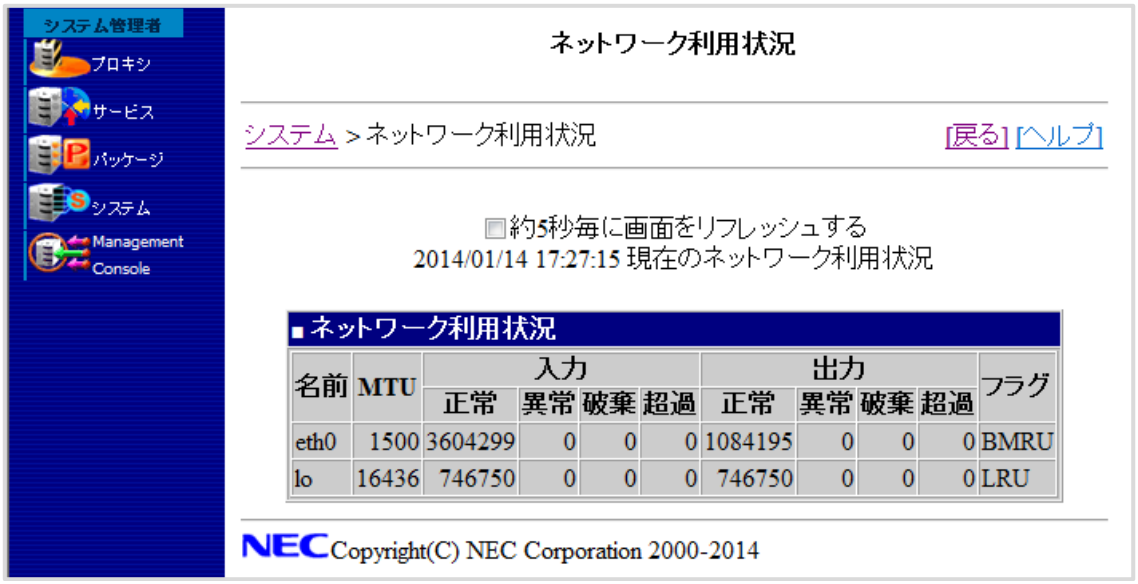
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

3.5.4. ネットワーク利用状況

ネットワーク利用状況

ネットワーク利用状況を表示します。



◆ 約 5 秒毎に画面をリフレッシュする

約 5 秒ごとに最新の情報に表示を更新するかを指定します。左側に表示情報の取得時刻を表示します。

設定値	説明
■チェックあり	約 5 秒毎に情報を更新します。
□チェックなし	情報の更新を行いません。

◆ 名前

インタフェースの名前です。

◆ MTU

最大転送単位(Maximum Transmission Unit)。

このネットワークに対して一度に送信できるパケットの最大サイズ(バイト数)です。

◆ 入力

▶ 正常

正常に受信したパケット数です。

▶ 異常

受信時に発生したエラーの数です。

▶ 破棄

受信時に破棄したパケット数です。

▶ 超過

超過(overrun)のため、破棄したパケット数です。

◆ 出力

▶ 正常

正常に送信したパケット数です。

▶ 異常

送信時に発生したエラーの数です。

▶ 破棄

送信時に破棄したパケット数です。

▶ 超過

超過(overrun)のため、破棄したパケット数です。

◆ フラグ

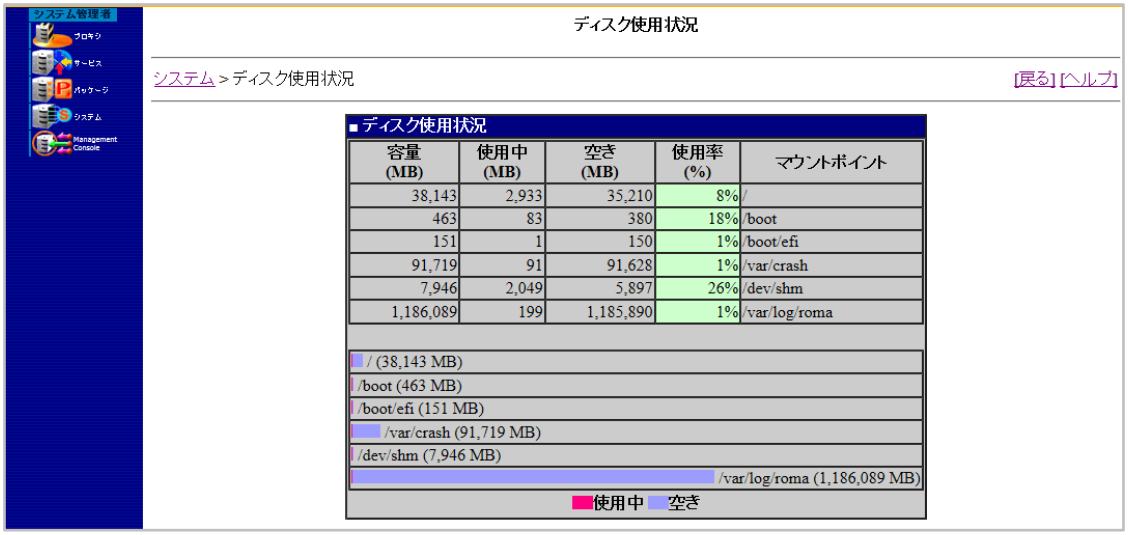
以下がフラグの詳細です。

表示	説明
B	ブロードキャストアドレスが設定済み
L	ループバックである
M	全受信モードである
N	トレイラーパケットは無効である
O	ARP がこのインタフェースでは無効である
P	Point-to-Point 接続である
R	インタフェースが Running 状態にある
U	インタフェースが Up している

3.5.5. ディスク使用状況

ディスクの使用状況

ディスクの使用状況を各ファイルシステムごとに数値とグラフで表示します。空き容量、使用率に注意してください。空き容量が足りなくなるとシステムが正常に動作しなくなる可能性があります。



- **容量**

  そのファイルシステムの容量を MB 単位で表示します。

- **使用中**

  使用中の容量を MB 単位で表示します。

- **空き**

  空き容量を MB 単位で表示します。

- **使用率**

  使用率をパーセント単位で表示します。

- **マウントポイント**

  このファイルシステムが、どのディレクトリにマウント(接続)されているかを示します。

3.5.6. ネットワーク接続状況

ネットワーク接続状況

各ポートごとの接続状況を表示します。

◆ 約 5 秒毎に画面をリフレッシュする

約 5 秒ごとに最新の情報に表示を更新するかを指定します。左側に表示情報の取得時刻を表示します。

設定値	説明
■チェックあり	約 5 秒毎に情報を更新します。
□チェックなし	情報の更新を行いません。

◆ プロトコル

使用しているプロトコル。

◆ 受信キュー

受信バッファに溜まっているデータのバイト数。

◆ 送信キュー

送信バッファに溜まっているデータのバイト数。

◆ 送信元アドレス

送信元のアドレスとポート番号。

*が表示されている場合は、接続待ち状態です。

◆ 宛先アドレス

宛先のアドレスとポート番号。

*が表示されている場合は、接続待ち状態です。

◆ 状態

コネクションの状態を表示します。

表示	説明
ESTABLISHED	接続中
LISTEN	接続待ち受け
CLOSE_WAIT	切断中

3.5.7. プロセス実行状況

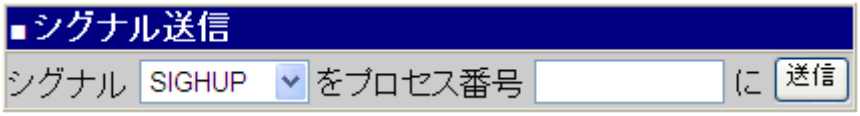
現在実行中のプロセスの一覧を表示します。プロセス実行状況の表の最上行の項目名をクリックすると、各項目で表示をソートすることができます。

プロセス実行状況は以下の画面に分かれています。

■シグナル送信
■プロセス実行状況

シグナル送信

シグナルをプロセスに送信します。



◆ シグナル

送信したいシグナルを指定します。

設定値	説明
SIGHUP	ハングアップシグナルを送ります。
SIGTERM	終了シグナルを送ります。
SIGKILL	強制終了シグナルを送ります。
SIGUSR1	USER1 シグナルを送ります。
SIGUSR2	USER2 シグナルを送ります。

◆ プロセス番号

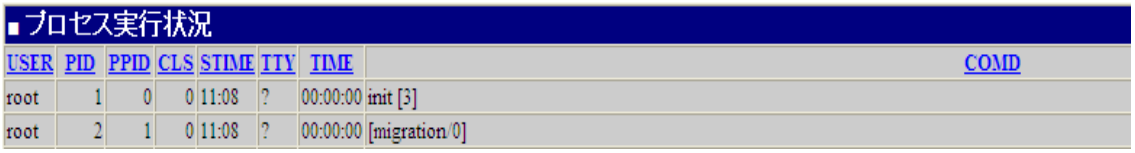
シグナルを送信したいプロセス番号を指定します。

✓ ボタンの説明

[送信]	選択したシグナルを入力したプロセスに送信します。

プロセス実行状況

マシン上で動作しているプロセスの一覧を表示します。USER などの項目名をクリックすると、その項目でソートして表示します。



■プロセス実行状況

USER	PID	PPID	CLS	STIME	TTY	TIME	COMD
root	1	0	0	11:08	?	00:00:00	init [3]
root	2	1	0	11:08	?	00:00:00	[migration/0]

- **USER**

  プロセスの実行ユーザ名を表示します。

  USER のリンククリックで USER にて並び替えて表示します。

- **PID**

  プロセス ID を表示します。

  PID のリンククリックで PID にて並び替えて表示します。

- **PPID**

  親プロセスのプロセス ID を表示します。

  PPID のリンククリックで PPID にて並び替えて表示します。

- **CLS**

  クラスを表示します。

  CLS のリンククリックで CLS にて並び替えて表示します。

- **STIME**

  プロセスの開始時刻を表示します。

  STIME のリンククリックで STIME にて並び替えて表示します。

- **TTY**

  プロセスが使用している TTY(端末ポート)を表示します。使用していない場合は、‘?’が表示されます。

  TTY のリンククリックで TTY にて並び替えて表示します。

- **TIME**

  プロセスが起動してから使用した CPU 時間を表示します。

  TIME のリンククリックで TIME にて並び替えて表示します。

- **COMD**

  コマンドラインの内容を表示します。

  COMD のリンククリックで COMD にて並び替えて表示します。

3.5.8. プロキシアクセス統計

プロキシサーバへのアクセスを Webalizer を使用して統計情報を表示します。

プロキシアクセス統計表示画面の「Summary byMonth」の表の「Month」の項目のリンクをクリックするとその月の詳細な統計情報を表示します。プロキシアクセス動作設定はプロキシアクセス統計を有効にして動作させるかどうか設定します。動作させる際には優先度を設定してください。優先度は 1 から 19 まで設定可能であり、値が大きいほど優先度が低くなります。優先度を低くすることによりプロキシアクセス統計の動作による CPU の負荷を減らすことができます。

Webalizer 表示設定では、sites はサイト別上位を、sites By KBytes はサイト別キロバイト上位を、URL's は URL 上位を、URL' s By KBytes はサイト別キロバイト上位を Entry Pages は入り口上位を、ExitPages は出口別上位をいくつまで表示するか設定することができます。

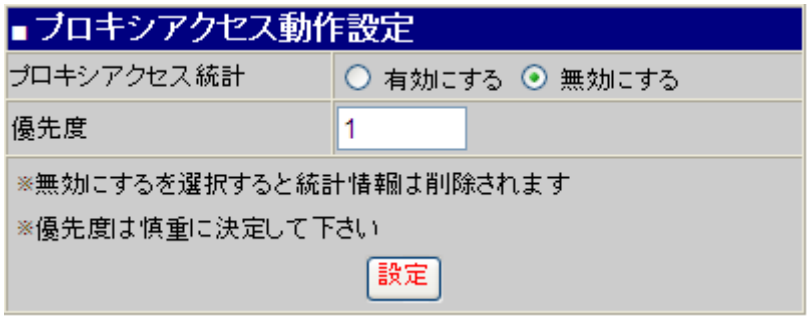
プロキシのアクセス統計は以下の画面に分かれています。

■プロキシアクセス動作設定
■プロキシアクセス統計表示
■プロキシアクセス統計設定
■Webalizer 表示設定

・プロキシアクセス統計を無効にするを選択するとそれまで作成されていた統計情報は削除されます。
・プロキシアクセス統計を動作させると性能低下がおこる可能性があります。
・優先度は慎重に決定してください。低い優先度を設定するとシステムの負荷状況によっては正常に統計情報が作成されない可能性があります。
・プロキシアクセス統計情報を動作させると、キャッシュサーバのアクセスログのログ出力形式は Squid に、ローテートサイズはいったん 100MB に設定されます。
・プロキシアクセス統計を動作させている時、ローテートサイズの扱いには注意してください。システムの性能およびプロキシアクセス統計の動作に影響を与えます。

・[初期値]をクリックすると、それぞれのテキストボックスに初期値が入ります。
・各テキストボックスは 0～99 まで入力することができます。
・統計情報はシステムのアクセスログがローテートされたときに作成されます。
・システムのアクセスログのローテートの設定はキャッシュサーバアクセスログの[設定]をクリックすることで表示される「3.5.12. ログ管理」のキャッシュサーバアクセスログ設定にて行えます。

プロキシアクセス動作設定



◆ プロキシアクセス統計

プロキシアクセス統計を有効にするか無効にするか指定します。

統計情報はキャッシュサーバアクセスログがローテートされた時に作成されます。キャッシュサーバアクセスログのローテートの設定は、「3.5.12. ログ管理」のキャッシュサーバアクセスログ設定にて行えます。

プロキシアクセス統計を有効にするとスケジュールダウンロードで履歴を使用できるようになります。また、キャッシュサーバアクセスログの出力形式は「Squid」に「ローテートサイズ」は 100MB に設定されます。

プロキシアクセス統計を無効にすると、それまで作成されていた統計情報は削除されます。 プロキシアクセス統計を有効にすると本サーバが性能低下を起こす可能性があります。

◆ 優先度

プロキシアクセス統計の動作の優先度を指定します。

1 から 19 まで設定可能で、値が大きいほど優先度が低くなります。優先度を低くすることによりプロキシアクセス統計処理による CPU の負荷を減らすことができます。

優先度は慎重に決定してください。あまりに低い優先度を指定すると正常にプロキシアクセス統計が動作しない可能性があります。

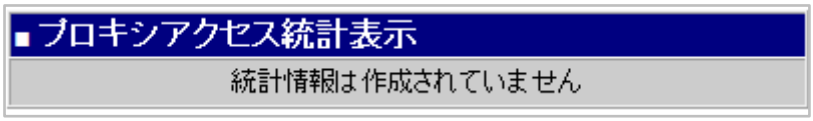
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

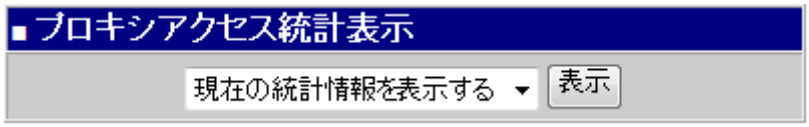
プロキシアクセス統計表示

プロキシアクセスの統計情報（表およびグラフ）を表示します。統計情報は２世代(現在の情報、１世代前の情報)のうち、どちらかを選択し、[表示]の押下で参照を行うことが可能です。

【プロキシアクセス統計情報なしの場合】



【プロキシアクセス統計情報ありの場合】

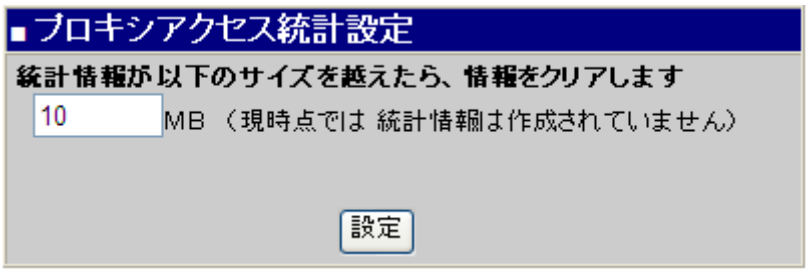


✓ ボタンの説明

[表示]	プロキシアクセス統計の表およびグラフの表示を行います。 →「3.5.8.1. プロキシアクセス統計グラフ」

プロキシアクセス統計設定

プロキシアクセスの統計情報は２世代で管理されています。
保存されている統計情報が指定したサイズ以上になったとき、ローテートが行われ、統計情報はクリアされます。
ローテートされる前の統計情報は１世代前の情報として、次のローテートが発生するまでの間は参照することが可能です。 デフォルトは 10MB です。



◆ 統計情報が以下のサイズを超えたら、情報をクリアします

統計情報がどの程度の大きさになったときクリア(ローテート)を行うかを MB 単位で指定します。
デフォルトは 10MB です。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

Webalizer 表示設定

◆ Sites

サイト別上位の表示数を指定します。デフォルトは 30 です。

◆ Sites By KBytes

サイト別キロバイト上位の表示数を指定します。デフォルトは 10 です。

◆ URL's

URL 別上位の表示数を指定します。デフォルトは 30 です。

◆ URL's By KBytes

URL 別キロバイト上位の表示数を指定します。デフォルトは 10 です。

◆ Entry Pages

入口別上位の表示数を指定します。デフォルトは 10 です。

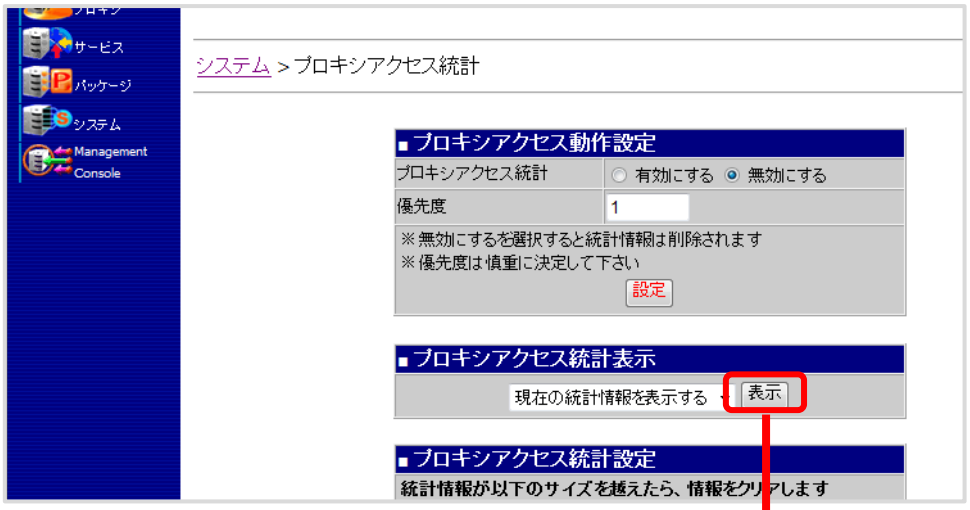
◆ Exit Pages

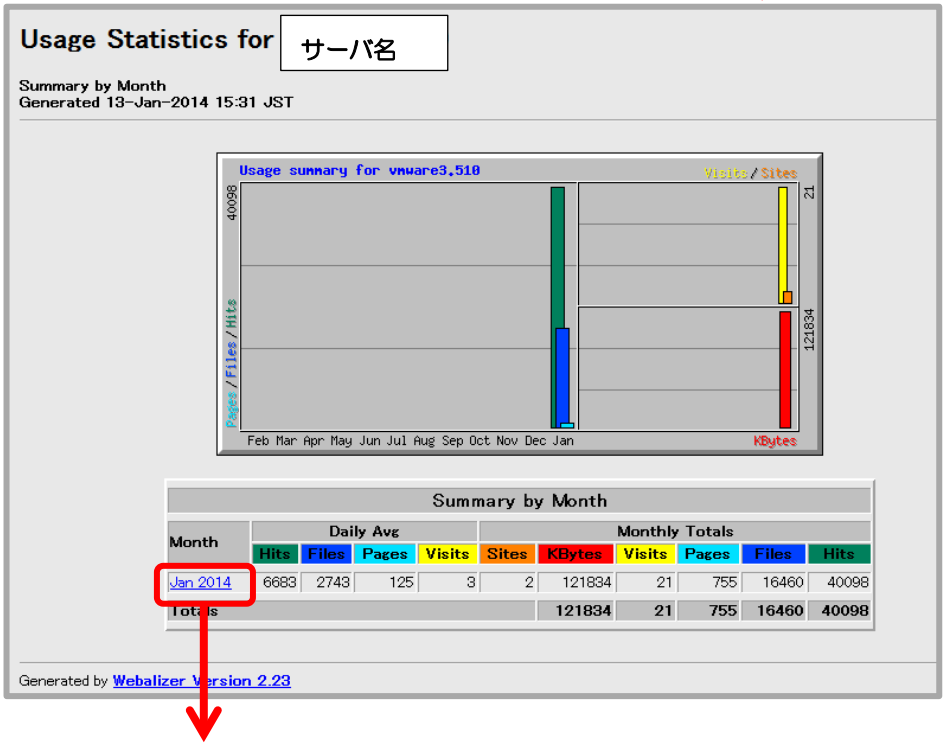
出口別上位の表示数を指定します。デフォルトは 10 です。

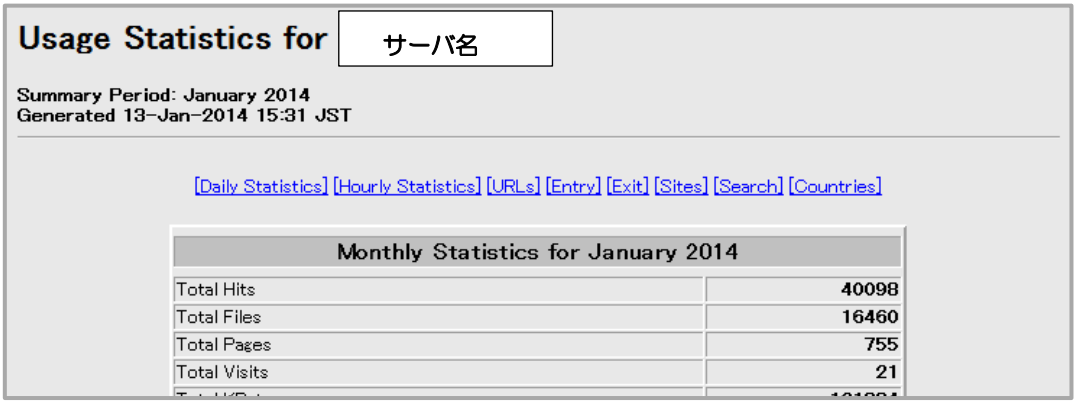
✓ ボタンの説明

[初期値]	各項目の値をデフォルトに変更します。デフォルト値は各項目の値を確認してください。[初期値]の押下後、[設定]ボタンを押下することで内容を反映します。
[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

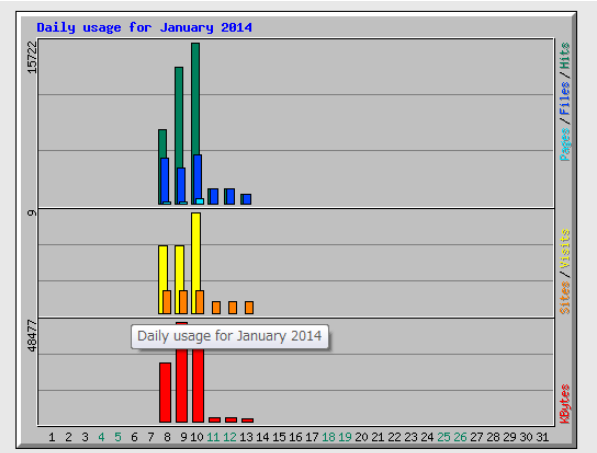
3.5.8.1. プロキシアクセス統計グラフ







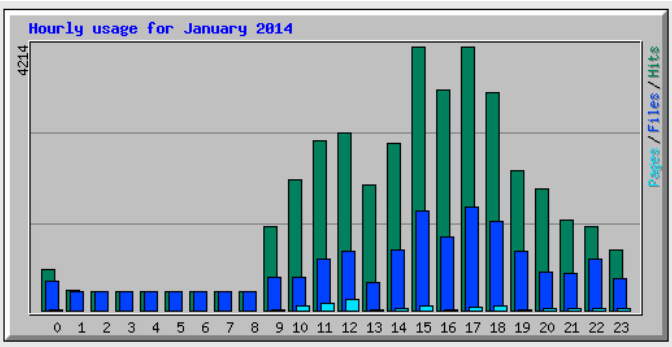
- 統計情報では Monthly Statistics、Daily Statistics、Hourly Statistics、URLs、Enrty(※1)、Exit(※2)、Sites、Search、Countries の種別毎に情報が表示されます。
- 「Monthly Statistics」の場合、Hits(※3)、Files(※4)、Pages、Visits(※5)、KBytes(※6)、Sites、URLs の項目について集計された表が表示されます。
- 「Daily Statistics」の場合、日毎の Hits、Files、Pages、Visits、Sites、KBytes の項目について表及びグラフが表示されます。



Daily Statistics for January 2014

Day	Hits		Files		Pages		Visits		Sites		KBytes	
8	7253	18.09%	4428	26.90%	111	14.70%	6	28.57%	2	100.00%	28507	23.40%
9	13312	33.20%	3482	21.15%	211	27.95%	6	28.57%	2	100.00%	48477	39.79%
10	15722	39.21%	4739	28.79%	433	57.35%	9	42.86%	2	100.00%	40413	33.17%
11	1440	3.59%	1440	8.75%	0	0.00%	0	0.00%	1	50.00%	1676	1.38%
12	1440	3.59%	1440	8.75%	0	0.00%	0	0.00%	1	50.00%	1676	1.38%
13	931	2.32%	931	5.66%	0	0.00%	0	0.00%	1	50.00%	1084	0.89%

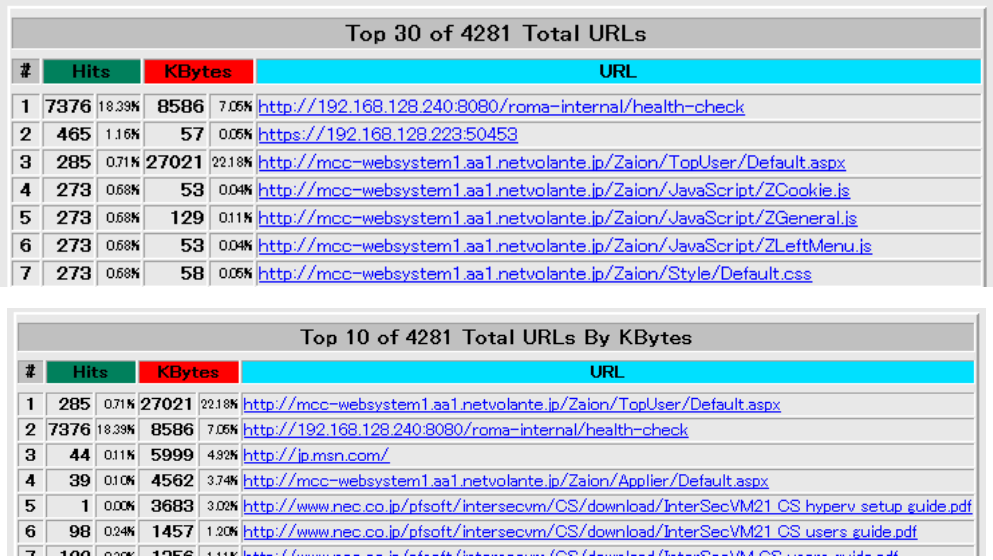
- 「Hourly Statistics」の場合、時間帯毎の Hits、Files、Pages、KBytes の項目からなる表及びグラフが表示されます。



Hourly Statistics for January 2014

Hour	Hits			Files			Pages			KBytes		
	Avg	Total		Avg	Total		Avg	Total		Avg	Total	
0	109	658	1.64%	77	467	2.84%	1	8	1.06%	391	2345	1.92%
1	53	323	0.81%	51	307	1.87%	0	0	0.00%	164	983	0.81%
2	50	300	0.75%	50	300	1.82%	0	0	0.00%	58	349	0.29%
3	50	300	0.75%	50	300	1.82%	0	0	0.00%	58	349	0.29%
4	50	300	0.75%	50	300	1.82%	0	0	0.00%	58	349	0.29%
5	50	300	0.75%	50	300	1.82%	0	0	0.00%	58	349	0.29%

- 「URL's」「URL's By KBytes」の場合、全 URL 中で Hits が多い順の上位サイトと KBytes が多い順の上位サイトについてそれぞれ Hits、KBytes、URL の項目が表示されます。



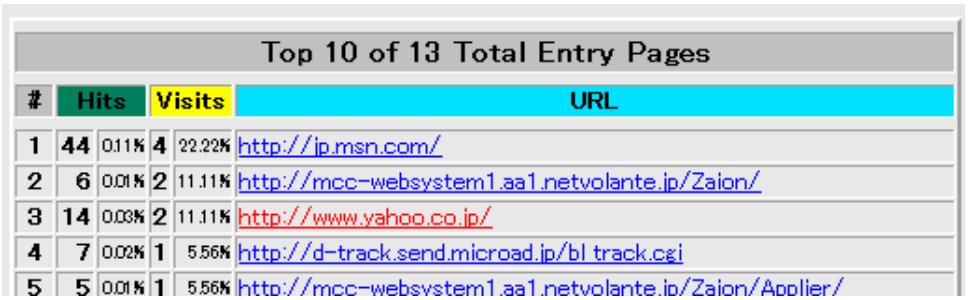
Top 30 of 4281 Total URLs

#	Hits		KBytes		URL
1	7376	18.39%	8586	7.05%	http://192.168.128.240:8080/roma-internal/health-check
2	465	1.16%	57	0.05%	https://192.168.128.223:50453
3	285	0.71%	27021	22.18%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/TopUser/Default.aspx
4	273	0.68%	53	0.04%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/JavaScript/ZCookie.js
5	273	0.68%	129	0.11%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/JavaScript/ZGeneral.js
6	273	0.68%	53	0.04%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/JavaScript/ZLeftMenu.js
7	273	0.68%	58	0.05%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/Style/Default.css

Top 10 of 4281 Total URLs By KBytes

#	Hits		KBytes		URL
1	285	0.71%	27021	22.18%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/TopUser/Default.aspx
2	7376	18.39%	8586	7.05%	http://192.168.128.240:8080/roma-internal/health-check
3	44	0.11%	5999	4.92%	http://jp.msn.com/
4	39	0.10%	4562	3.74%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/Applier/Default.aspx
5	1	0.00%	3683	3.02%	http://www.nec.co.jp/pfsoft/intersecvm/CS/download/InterSecVM21_CS_hyperv_setup_guide.pdf
6	98	0.24%	1457	1.20%	http://www.nec.co.jp/pfsoft/intersecvm/CS/download/InterSecVM21_CS_users_guide.pdf

- 「Entry」の場合、全 Entry Pages 中で Visits が多い順に上位サイトの Hits、Visits、URL の項目が表示されます。



Top 10 of 13 Total Entry Pages

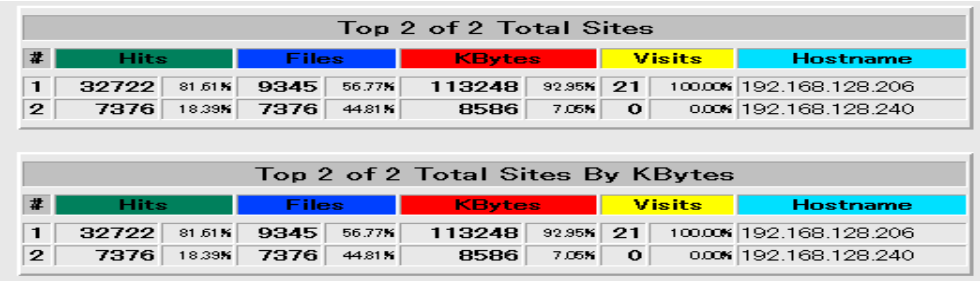
#	Hits		Visits		URL
1	44	0.11%	4	22.22%	http://jp.msn.com/
2	6	0.01%	2	11.11%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/
3	14	0.03%	2	11.11%	http://www.yahoo.co.jp/
4	7	0.02%	1	5.56%	http://d-track.send.microad.jp/bl_track.cgi
5	5	0.01%	1	5.56%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/Applier/

- 「Exit」の場合、全 Exit Pages 中で Visits が多い順に上位サイトの Hits、Visits、URL の項目が表示されます。

Top 10 of 16 Total Exit Pages

#	Hits		Visits		URL
1	14	0.03%	5	23.81%	http://www.yahoo.co.jp/
2	6	0.01%	2	9.52%	http://mcc-websystem1.aa1.netvolante.jp/Zaion/
3	30	0.07%	1	4.76%	http://192.168.128.222:50453/menu.cgi
4	11	0.03%	1	4.76%	http://192.168.128.223:50453/menu.cgi
5	1	0.00%	1	4.76%	http://blog.ustream-asia.jp/2013/04/ustream_9282.html

- 「Sites」「Sites By KBytes」の場合、全 Sites 中で Hits が多い順の上位サイトと KBytes が多い順の上位サイトについてそれぞれ Hits、Files、KBytes、Visits、Hostname の項目が表示されます。



Top 2 of 2 Total Sites

#	Hits		Files		KBytes		Visits		Hostname
1	32722	81.61%	9345	56.77%	113248	92.95%	21	100.00%	192.168.128.206
2	7376	18.39%	7376	44.81%	8586	7.05%	0	0.00%	192.168.128.240

Top 2 of 2 Total Sites By KBytes

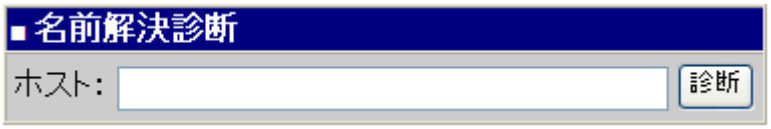
#	Hits		Files		KBytes		Visits		Hostname
1	32722	81.61%	9345	56.77%	113248	92.95%	21	100.00%	192.168.128.206
2	7376	18.39%	7376	44.81%	8586	7.05%	0	0.00%	192.168.128.240

(※1) 最初に閲覧したサイトを示します。
(※2) 最後に閲覧したサイトを示します。
(※3) 任意のリクエストに対しプロキシサーバ上で有効な html ページ、グラフィックのイメージ、オーディオ・ファイル、cgi スクリプトなどが存在した場合にヒットとして数えられます。
(※4) プロキシサーバからクライアントに送られたファイル数を示します。
(※5) サイトを閲覧したユーザ数を示します。(ただし、サイト参照のタイムアウト値は 30 分です。)
(※6) プロキシサーバよりクライアントに送られたデータの量を示します。(1 キロバイトは 1024 バイトです。)

3.5.9. 名前解決診断

名前解決診断

ネームサーバ(DNS サーバ)により正しく名前解決ができるかどうかの診断を行います。



◆ ホスト

名前解決の診断を行うホスト名を入力します。

✓ ボタンの説明

[診断]	「ホスト」に指定したホスト名の診断結果が表示されます。ホスト名に対して正しく「Name:」と Address:」が表示されれば DNS サーバは正常に機能しています。

3.5.10. 経路情報

経路情報

ネットワーク上のホストに届くパケットの経路を表示します。

◆ 相手ホスト

経路を表示する相手先ホストを指定します。ホスト名または FQDN または IP アドレスの形式で指定します。

✓ ボタンの説明

[表示]	中継地点のルータやゲートウェイの IP アドレスやそこに至るまでの到達時間が表示されます。

3.5.11. システム情報

システム情報

装置に割り当てたホスト名、および OS に関する情報を表示します。

- **ホスト名**
  マシンのホスト名。
- **OS 名**
  使用している OS 名。
- **OS リリース番号**
  カーネルのリリース番号。
- **OS バージョン**
  OS のバージョン。
- **ハードウェアの種類**
  ハードウェアの種類の表示。
- **プロセッサの種類**
  プロセッサの種類の表示。

✓ **ボタンの説明**

[戻る]	前画面へ戻ります。

3.5.12. ログ管理

ログ管理

現在、システムでロギングされているログファイルの一覧を示します。
ログファイルの種類と設定内容（ローテートのタイミングおよび世代数）が表示されます。
ログのローテートは毎日 0:00 とマシン起動時にチェックし、条件があっているものをローテートします。ログのローテートタイミングでのマシンの再起動を行う際はご注意下さい。

■ログ管理

操作	ログファイル	ローテート	世代
表示 設定	キャッシュサーバアクセスログ	100Mbyteごと	1
表示 設定	SSLアクセラレータアクセスログ	100Mbyteごと	5
表示 設定	システムログ	毎週	4
表示 設定	システムのセキュリティログ	毎週	4
表示 設定	システムのメールログ	毎週	4
表示 設定	システムのブートログ	毎週	4
表示 設定	クーロンログ	毎週	4
表示 設定	WPADサーバログ	毎週	4
表示	キャッシュログ	40Mbyteごと	1
表示 設定	Management Consoleログ	毎週	5
表示 設定	Management Consoleのアクセスログ	毎月	5
表示 設定	Management Consoleのエージェントログ	毎月	5
表示 設定	Management Consoleのエラーログ	毎月	5
表示 設定	Management Consoleの参照ログ	毎月	5
表示 設定	Management Console操作ログ	毎月	5

◆ 操作

✓ ボタンの説明

該当行に対する操作を行うための各種ボタンを表示します。

[表示]	各項目のログ表示選択画面へ遷移します。 →「3.5.12.1. ログファイルの表示」
[設定]	各項目の設定画面に遷移します。 ・キャッシュサーバアクセスログの場合 →「3.5.12.2. キャッシュサーバアクセスログ設定」 ・キャッシュサーバアクセスログ以外の場合 →「3.5.12.3. キャッシュサーバアクセス以外のログ設定」

◆ ログファイル

ログファイルのファイル内容を表示します。

◆ ローテート

ログファイルの世代更新の条件を表示します。

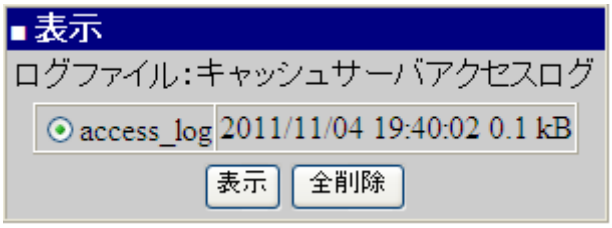
◆ 世代

ログファイルを保存する個数を表示します。

3.5.12.1. ログファイルの表示

表示

ログファイルの一覧を表示します。表には、ログファイルの最終更新時刻とファイルのサイズが表示されています。表示したいログファイルを選択して[表示]を押してください。



◆ ログファイル

ログファイルの種類が表示されます。

✓ **ボタンの説明**

選択行に対する操作を行うための各種ボタンを表示します。

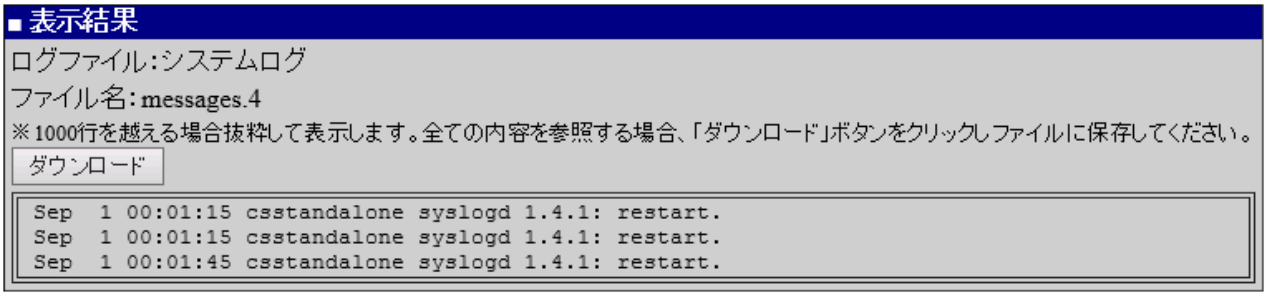
[表示]	選択されたログファイルを表示します。 →「3.5.12.1.1. ログファイルの表示結果」
[全削除]	カレントログファイルを除く全てのローテートログファイルが削除されます。

3.5.12.1.1. ログファイルの表示結果

表示結果

ログの内容を表示します。

ログが 1000 行を越える場合は抜粋して表示します。



◆ ログファイル

ログファイルのファイル内容を表示します。

◆ ファイル名

ログファイルの各世代のファイル名を表示します。

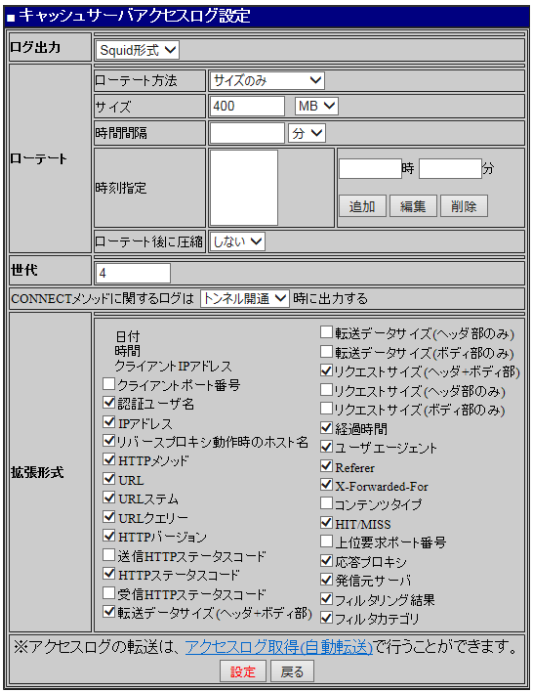
✓ ボタンの説明

[ダウンロード]	ログファイルをダウンロードします。

3.5.12.2. キャッシュサーバアクセスログ設定

キャッシュサーバアクセスログ設定

キャッシュサーバアクセスログの設定を行います。



◆ ログ出力

ログ出力パターンを以下の 4 つから 1 つ選択します。

設定値	説明
Squid 形式	ログを Squid 形式で出力します。
拡張形式	ログを拡張形式(独自形式)で出力します。出力の内容をカスタマイズすることができます。
CLF	ログを CLF(Common Log Format)形式で出力します。
出力しない	ログを出力しません。

プロキシアクセス統計を動作させると Squid 形式に固定されます。

アクセスログ取得(自動転送)が機能していると「出力しない」を指定できません。

◆ ローテート

ローテートに関する設定を行います。

▶ ローテート方法

ローテート方法を指定します。ローテート方法は「サイズのみ」,「サイズと時間間隔」,「サイズと時刻指定」を指定することができます。

設定値	説明
サイズのみ	サイズのみでローテートします。
サイズと時間間隔	サイズと時間間隔でローテートします。
サイズと時刻指定	サイズと時刻指定でローテートします。

▶ サイズ

ログをローテートさせるタイミングをログファイルのサイズで指定します。
100MB から 2GB まで指定可能です。デフォルトは 400MB です。
「3.5.8. プロキシアクセス統計」でプロキシアクセス統計を動作させると一旦 100MB に設定されます。
プロキシアクセス統計、アクセスログ取得(自動転送)動作時のローテートサイズの変更は注意して変更を行って下さい。本サーバの動作が不安定になる可能性があります。アクセスログ取得(自動転送)動作時は、(最大リトライキュー+1)×ローテートサイズがログ領域(/var/log/roma)以内に収まるように最大リトライキューとローテートサイズを設定してください。

▶ 時間間隔

ローテートの時間間隔を指定します。ローテート方法に「サイズと時間間隔」を指定した場合のみ有効となります。時間間隔は単位毎に次の値を指定できます。

・月指定の場合 1 から 99 まで
・週指定の場合 1 から 99 まで
・日指定の場合 1 から 99 まで
・時指定の場合 1 から 99 まで
・分指定の場合 10 から 999 まで

プロキシサービスが起動してから指定された時間が経過したのちログがローテートされますが、指定したサイズが先に有効になった場合はその時点でログがローテートされます。その後、改めて指定された時間が経過したのちログがローテートされます。

▶ 時刻指定

ローテートする時刻を指定します。ローテート方法に「サイズと時刻指定」を指定した場合のみ有効となります。

最大 144 個まで指定可能です。

複数指定する場合は 10 分以上間隔をあけてください。

指定時刻の直前に指定したサイズによるローテートが行われていた場合、直前のローテートより 10 分後にローテートします。

右側の「時」「分」に時刻を入力し[追加]でリストに時刻を追加します。

リストを選択すると、右側の時、分に選択した時刻が表示されます。

[編集]で選択している時刻を「時」「分」に入力している時刻に変更します。

[削除]で選択している時刻を削除します。

✓ ボタンの説明

[追加]	「時」「分」に指定の時刻を追加します。 追加後、[設定]を押下することで内容を反映します。
[編集]	選択している時刻を「時」「分」に入力している時刻に変更します。 編集後、[設定]を押下することで内容を反映します。
[削除]	選択している時刻を削除します。 削除後、[設定]を押下することで内容を反映します。

▶ ローテート後に圧縮

ログがローテートした際に圧縮して保持する/しないを指定します。

設定値	説明
する	ログがローテートした際に圧縮し保持する。
しない	ログがローテートした際に圧縮せずに保持する

◆ 世代

最大世代数を指定します。0 から 9999 まで指定可能です。デフォルトは 4 です。

(世代数+1)×ローテートサイズがログ領域(/var/log/roma)以内に収まるように世代数とローテートサイズを指定してください。世代数を現在の設定より小さくする場合、設定された世代以上のログファイルは削除されます。ログファイルが必要な場合、事前に別の場所へ退避させてください。

◆ CONNECT メソッドに関するログは トンネル開通/トンネル切断 時に出力する

CONNECT メソッドを使用したアクセスに関する情報をキャッシュサーバアクセスログに出力するタイミングをトンネル開通/切断時から選択します。デフォルトは「トンネル開通」になります。

トンネル開通時に出力する場合、トンネルが確立した時点で情報を出力するため、トンネル確立後に送受信されたデータのサイズは出力されません。

「経過時間」もトンネル開通時点までの時間になります。

トンネル切断時に出力する場合、トンネルを切断した時点で情報を出力するため、トンネル確立後に送受信されたデータのサイズも出力されます。

「経過時間」もトンネル切断時点までの時間になります。

CONNECT メソッドはクライアントが本サーバに対してトンネリング処理を要求する場合に使用されます。
トンネル開通までは HTTP での通信を行いますが、トンネル開通後は当該トンネルを利用してクライアントと上位サーバ間で HTTP 以外のプロトコルでの通信が可能になります。
「3.2.2. セキュリティ設定」の「トンネル確立中のアップロードサイズの合計の上限値」、「トンネル確立中のダウンロードサイズの合計の上限値」でサイズ制限を行う場合は「トンネル切断」を選択してください。

◆ 拡張形式

どの項目をログとして出力するか指定します。ログ出力で拡張形式を指定した場合に有効となります。日付、時間、IP アドレスは必ず出力します。チェックボックスにチェックを入れた項目がログに出力されます。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

＜Squid 形式のログフォーマット＞

出力例)

```
1252473144.804  139  192.168.250.1  TCP_HIT/200  14641
GET  http://www.express.nec.co.jp/sports?id=aaaa  -  DIRECT/192.168.250.2  text/html  ALLOW  "Sports¥Professional Sports"
```

出力例の左の項目から順に各出力項目を説明します。

・タイムスタンプ

アクセスが完了した時間です。UNIX 時間(1970 年 1 月 1 日からの秒数)で出力します。単位は秒です。

・経過時間

当該アクセスの受付けから終了までの時間(サーバ等からの応答待ち時間を含む)をミリ秒で出力します。

・クライアント IP アドレス

クライアント IP アドレスを出力します。

0.0.0.0 と記録されているアクセスは、処理中に接続が切れてしまった場合など、処理を正常に終了できなかったアクセスを表わしています。

・キャッシュステータス

本サーバがどのように要求を処理したかを表すタグ名と、HTTP のステータスコードを出力します。

詳細は後述の「＜拡張形式のログフォーマット＞」の「キャッシュステータス」をご覧ください。

HTTP のステータスコードに出力される「0xx」については、本サーバ独自のステータスコードになります。 基本的にはクライアント又はサーバが強制切断を行った場合に出力されます。

以下のステータスコードは本サーバに設定した制限に合致した場合に出力されます。

099・・・本サーバがタイムアウトを検出した。

083・・・ダウンロードサイズの上限値を超えた。

082・・・アップロードサイズの上限値を超えた。

080・・・HTTP ヘッダ全体のサイズの上限値を超えた。

・転送データサイズ

クライアントへ渡したデータの総バイト数を出力します。

ヘッダを含めたサイズです。

・HTTP メソッド

HTTP のメソッドを出力します。

また、ICP サーバとして本サーバを使用している場合は、ICP のメソッドも出力します。

・URL

アクセスを要求した Web ページの URL を出力します。

URL 長が 1KB を超える場合は、中略して出力します。

・出力無し
　必ず "-" が出力されます。
・階層構造データタグ/ホスト名
　オブジェクトの取得がどのように行われたかを表すタグ名と、接続先の IP アドレスを出力します。

＜Squid 形式のログフォーマット＞(続き)

・コンテンツタイプ

オブジェクトデータのコンテンツタイプを出力します。

コンテンツタイプが 47 文字を超える場合は、先頭から 47 文字までを出力します。

・フィルタリング結果

ICAP サーバから通知されるフィルタリング結果(ALLOW/DENY)を出力します。フィルタリング結果が通知されない場合は「-」を出力します。「URL フィルタスキップ設定」のスキップする条件に該当した場合、「SKIP」と出力します。ICAP サーバがダウンしているためににスキップした場合、「DSKIP」と出力します。

・フィルタカテゴリ

ICAP サーバから通知されたカテゴリ名を出力します。カテゴリ名が通知されない場合は「 - 」を出力します。

フィルタカテゴリをログに出力させる場合は「3.2.20. ICAP サーバ設定」の注意事項を参照してください。

i-FILTER を使用している場合は、カテゴリ名ではなくカテゴリ番号が表示されます。カテゴリ番号については i-FILTER の主管理者マニュアルもしくは i-FILTER の管理画面を参照してください。

＜拡張形式のログフォーマット＞

出力形式を「拡張形式」にすると下記の項目のうち日付、時間、IP アドレス以外の項目はユーザが出力するかしないかを指定することができます。

出力例)

```
2009-09-09 14:12:24 192.168.250.1 "USER_NAME" 192.168.250.3 -
GET http://www.express.nec.co.jp/sports?id=aaaa http://www.express.nec.co.jp/sports ?id=aaaa
HTTP/1.0 200 14641 457 139 "AAA/Browser(aaa)" "http://www.express.nec.co.jp"
"192.168.250.4"
```

出力例の左の項目から順に各出力項目を説明します。

・日付
　アクセスが完了した日付です。西暦-月-日のフォーマットで出力します。
・時間アクセスが完了した時刻です。時:分:秒のフォーマットで出力します。
・クライアント IP アドレス
　クライアント IP アドレスを出力します。0.0.0.0 と記録されているアクセスは、処理中に接続が切れてしまった場合など、処理を正常に終了できなかったアクセスを表わしています。
・クライアントポート番号
　クラインアントが使用したポート番号を出力します。
・認証ユーザ名
　NTLM 機能又は認証機能を使用したときのみユーザ名を出力します。NTLM 機能を使用した場合は、ユーザ名を 40 文字、ドメイン名を 15 文字、コンピュータ名を 15 文字まで出力します。 認証機能を使用した場合は、ユーザ名が 63 文字を超える場合、先頭から 63 文字までを出力します
・IP アドレス
　本サーバの IP アドレスを出力します。
・リバースプロキシ動作時のホスト名
　リバースプロキシ動作時のホスト名(または IP アドレス)を出力します。
・HTTP メソッド
　HTTP のメソッドを出力します。
　また、ICP サーバとして本サーバを使用している場合は、ICP のメソッドも出力します。
・URL
　アクセスを要求した Web ページの URL を出力します。
　URL 長が 1KB を超える場合は、中略して出力します。
・URL ステム
　URL に'?'が含まれた場合、'?'までの URL を出力します。
・URL クエリー
　URL に'?'が含まれた場合、'?'以降の URL を出力します。

＜拡張形式のログフォーマット＞（続き）

・HTTP バージョン
HTTP のバージョンを出力します。送信 HTTP ステータスコードクライアントへ送信した HTTP ステータスコードを出力します。クライアントへ HTTP ステータスコードを送信していない場合は「-」が出力されます。

・HTTP ステータスコード
HTTP ステータスコードを出力します。「0xx」(xx には任意の数字が入ります)は本サーバ独自のステータスコードになります。 基本的にはクライアント又はサーバが強制切断を行った場合に出力されます。
以下のステータスコードは本サーバに設定した制限に合致した場合に出力されます。
099・・・本サーバがタイムアウトを検出した。
083・・・ダウンロードサイズの上限値を超えた。
082・・・アップロードサイズの上限値を超えた。
080・・・HTTP ヘッダ全体のサイズの上限値を超えた。

・受信 HTTP ステータスコード
上位サーバから受信した HTTP ステータスコードを出力します。上位サーバから HTTP ステータスコードを受信していない場合は「-」が出力されます。

・転送データサイズ(ヘッダ+ボディ部)
本サーバからクライアントへ送信したデータの総バイト数を出力します。
転送データサイズ(ヘッダ部のみ)
本サーバからクライアントへ送信した HTTP ヘッダの総バイト数を出力します。

・転送データサイズ(ボディ部のみ)
本サーバからクライアントへ送信したボディデータの総バイト数を出力します。
SSL 通信(CONNECT メソッド)時は「CONNECT メソッドに関するログはトンネル開通時に出力する」と設定している状態でトンネル開通に成功した場合「-」を出力します。

・リクエストサイズ(ヘッダ+ボディ部)
本サーバから上位サーバ側に転送したデータの総バイト数を出力します。

・リクエストサイズ(ヘッダ部のみ)
本サーバから上位サーバ側に転送した HTTP ヘッダの総バイト数を出力します。

・リクエストサイズ(ボディ部のみ)
本サーバから上位サーバ側に転送したボディデータの総バイト数を出力します。SSL 通信(CONNECT メソッド)時は「CONNECT メソッドに関するログはトンネル開通時に出力する」と設定している状態でトンネル開通に成功した場合「-」を出力します。

・経過時間
当該アクセスの受付から終了までの時間(サーバ等からの応答時間を含む)をミリ秒で出力します。

・ユーザエージェント
ユーザが使用したブラウザ情報を出力します。ユーザエージェントが 128 文字を超える場合は、先頭から 128 文字までを出力します。Native-Ftp のアクセスは「roma_nftp」になります。
・Referer
参照 URL を出力します。
・X-Forwarded-For
発信元クライアント IP アドレスを出力します。
X-Forwarded-For が 31 文字を超える場合は、先頭から 31 文字までを出力します。
・コンテンツタイプ
オブジェクトデータのコンテンツタイプを出力します。
コンテンツタイプが 127 文字を超える場合は、先頭から 127 文字までを出力します。
出力する値が無い場合は「""」を出力します。

拡張形式のログフォーマット(続き)
・キャッシュステータス
キャッシュが HIT したか MISS したかを出力します。

TCP_HIT	二次メモリキャッシュ上のキャッシュデータに HIT した
TCP_MEM_HIT	一次メモリキャッシュ上のキャッシュデータに HIT した
TCP_IMS_HIT	クライアントからコンテンツの期限確認要求を受け、クライアントのキャッシュデータが有効期限内であったため CS か Web サーバが 304 応答(期限内)を返した
TCP_NEGATIVE_HIT	Web サーバからのエラー応答のキャッシュデータに HIT した
TCP_REFRESH_HIT	キャッシュデータが有効期限切の場合で、CS の期限確認要求に対して Web サーバが 304 応答(期限内)である
TCP_REFRESH_MISS	キャッシュデータが有効期限切の場合で、CS の期限確認要求に対して Web サーバが 304 以外の応答である
TCP_MISS	キャッシュデータが HIT しなかった

以下は、ICP 機能利用時のみ出力されるタグです。

UDP_HIT	要求されたオブジェクトが CS 上のキャッシュに存在した
UDP_MISS	要求されたオブジェクトが CS 上のキャッシュに存在しなかった
UDP_DENIED	要求されたアクセスは拒否された
UDP_INVALID	無効な要求を受信した

・上位要求ポート番号
本サーバが上位サーバへ接続した際に使用したポート番号を出力します。

・応答プロキシ
親プロキシ、隣接プロキシへリクエストを転送した場合のみ、当該プロキシの IP アドレスを出力します。
・発信元サーバ
親プロキシ、隣接プロキシへ転送せず、直接 Web サーバへリクエストを送信した場合のみ、当該 WEB サーバの IP アドレスを出力します。
・フィルタリング結果
ICAP サーバから通知されるフィルタリング結果(ALLOW/DENY)を出力します。フィルタリング結果が通知されない場合は「-」を出力します。「URL フィルタスキップ設定」のスキップする条件に該当した場合、「SKIP」と出力します。ICAP サーバがダウンしているためににスキップした場合、「DSKIP」と出力します。
・フィルタカテゴリ
ICAP サーバから通知されたカテゴリ名を出力します。カテゴリ名が通知されない場合は「-」を出力します。
フィルタカテゴリをログに出力させる場合は「3.2.20. ICAP サーバ設定」の注意事項を参照してください。
i-FILTER を使用している場合は、カテゴリ名ではなくカテゴリ番号が表示されます。
カテゴリ番号については i-FILTER の主管理者マニュアルもしくは i-FILTER の管理画面を参照してください。

＜CLF(Common Log Format)形式のログフォーマット＞

Apache の「共通ログフォーマット」で出力します。

出力例)

```
192.168.250.1 - "USER_NAME" [09/Sep/2009:14:12:24 +0900] "GET
http://www.express.nec.co.jp/sports?id=aaaa HTTP/1.0" 200 14641
```

出力例の左の項目から順に各出力項目を説明します

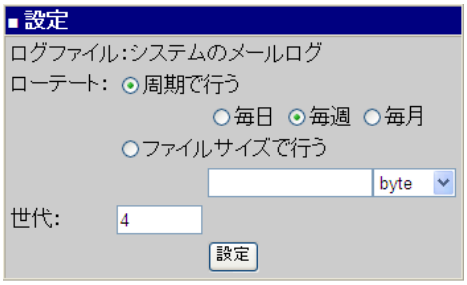
・クライアント IP アドレス
アクセスしたクライアントの IP アドレスを出力します。
・出力無し
必ず"-"が出力されます。
・認証ユーザ名
認証に使用されたユーザ ID を出力します。
・日時
アクセスが完了した日時です。以下の書式で出力されます。
日/月/年:時:分:秒 タイムゾーン
・リクエストの内容
クライアントからのリクエストの内容("メソッド URL のフルパス HTTP バージョン")を出力します。

・HTTP ステータスコード
HTTP ステータスコードを出力します。
「0xx」(xx には任意の数字が入ります)は本サーバ独自のステータスコードになります。
基本的にはクライアント又はサーバが強制切断を行った場合に出力されます
以下のステータスコードは本サーバに設定した制限に合致した場合に出力されます。
099・・・本サーバがタイムアウトを検出した。
083・・・ダウンロードサイズの上限値を超えた。
082・・・アップロードサイズの上限値を超えた。
080・・・HTTP ヘッダ全体のサイズの上限値を超えた。
・レスポンスサイズ
クライアントに転送したレスポンスのサイズを出力します。この中にヘッダ情報は含まれません。

3.5.12.3. キャッシュサーバアクセス以外のログ設定

設定

キャッシュサーバアクセス以外のログ設定を行います。



重要

「キャッシュログ」については、ログ管理の設定を行うことはできません。

◆ ログファイル

ログファイルの種類が表示されます。

◆ ローテート

ログファイルをローテート(それまでに記録したログファイルを退避して、新たにログを記録しはじめること)するタイミングを指定します。

設定値	説明
周期で行う	「毎日」、「毎週」、あるいは「毎月」1 回、ローテートを行います。
ファイルサイズで行う	ログファイルのサイズが、指定したサイズを越えた際に、ローテートを行います。

◆ 世代

何世代までのログファイルを残すかを指定します。0 を指定した場合、表示されているログファイルが上書きされます。

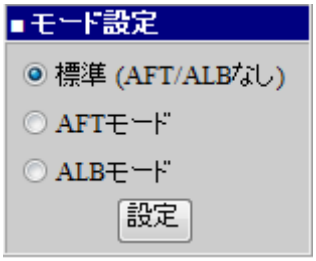
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

3.5.13. AFT/ALB モード設定

eth0/eth1 に対して、LAN 冗長化の動作モードの設定を行います。

※ eth2/eth3 に対しては、設定できません。



選択できる動作モードは、下記となります。

選択肢	説明
標準（AFT/ALB なし）	初期導入直後は、デフォルトとして本モードが選択されています。 冗長化を行わない場合は、こちらを選択してください。
AFT モード	動作モードを「AFT モード」に変更します。
ALB モード	動作モードを「ALB モード」に変更します。

◆ AFT モード（Adapter Fault Tolerance・active-backup）

AFT モードでは、eth0 と eth1 を 1 つの仮想アダプタ(bond0)として機能させることにより、プライマリポートが故障した場合、即座にバックアップポートに切り替え運用を継続させることができます(プライマリポートの IP アドレス及び MAC アドレスをバックアップポートが継承)。

※AFT モードの場合、接続するネットワーク集線機器は、リピータ・ハブ、スイッチング・ハブのどちらでも可。

◆ ALB モード（Adaptive Load Balancing・balance-alb）

ALB モードでは、eth0 と eth1 を 1 つの仮想アダプタ(bond0)として機能させることにより、各ポートに通信を分散し、スループットを向上させることができます。

※ALB モードの場合、スイッチング・ハブにのみ接続可。

■動作モード変更時の動作説明■

＜標準から AFT/ALB へ変更する際の動き＞

eth0 の設定が、仮想アダプタ(bond0)に引き継がれます。

eth1 に設定されている IP が、プロキシサーバの待ち受けとして使用されている場合は、エラーメッセージを表示します。「3.5.15.1. インタフェース」画面より eth1 の設定を削除するか、「3.2.1. 基本設定」画面でキャッシュサーバおよび FTP プロキシの設定を変更してください。

＜AFT/ALB から標準へ変更する際の動き＞

仮想アダプタ(bond0)の設定が、eth0 に引き継がれます。

eth1 は設定がされていない状態になりますので、必要があれば設定を行います。

重要

モードの設定を変更した際は、必ずシステム再起動が必要です。

✓ ボタンの説明

[設定]	指定した内容を設定します。
[戻る]	システム画面に戻ります。→「3.5. システム」

3.5.14. 時刻設定

時刻に関する設定を行います。

「3.3.3. 時刻調整(ntpd)」と同一の画面を表示します。

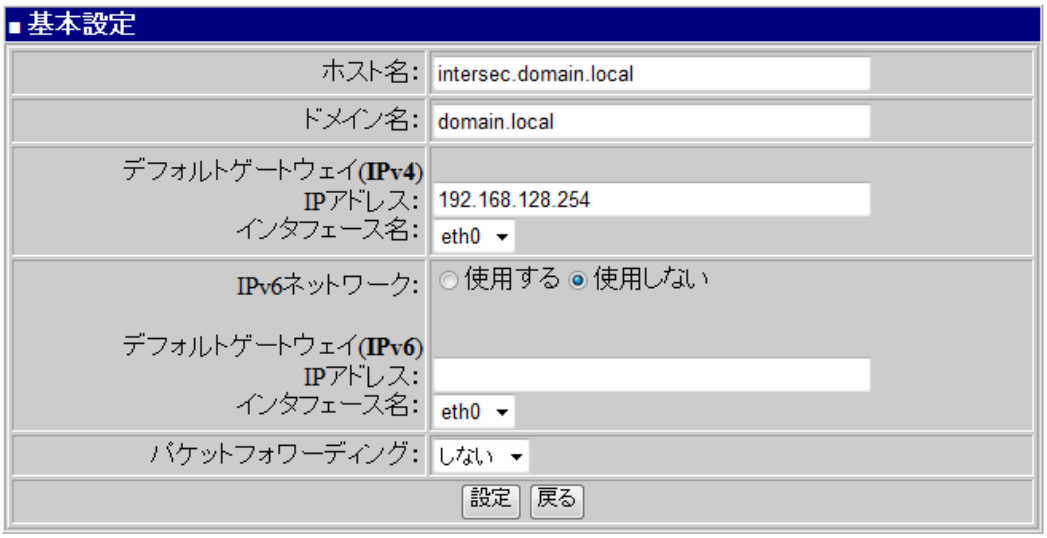
3.5.15. ネットワーク

ネットワークの基本的な設定やネットワークインタフェース、ルーティングの設定を行います。

ネットワークは以下の画面に分かれています。

■基本設定
■DNS 設定
■hosts 相当(プロキシサービス用)の設定
■ネットワーク設定

基本設定



◆ ホスト名

このマシンのホスト名を xxx.yyy.zz.jp のような完全なドメイン名(FQDN 形式)で指定します。

◆ ドメイン名

このマシンが所属しているドメイン名を指定します。

◆ デフォルトゲートウェイ(IPv4)

▶ IP アドレス

デフォルトゲートウェイの IPv4 アドレスを指定します。

▶ インタフェース名

デフォルトゲートウェイのインタフェース名を指定します。

◆ IPv6 ネットワーク

IPv6 ネットワークを使用するかしないか選択します。

設定値	説明
使用する	IPv6 ネットワークを使用します。
使用しない	IPv6 ネットワークを使用しない。

◆ デフォルトゲートウェイ(IPv6)

▶ IP アドレス

デフォルトゲートウェイの IPv6 アドレスを指定します。

▶ インタフェース名

デフォルトゲートウェイのインタフェース名を指定します。

◆ パケットフォワーディング

パケットをフォワーディングするか、しないかを指定します。

「3.2.1. 基本設定」のキャッシュサーバ設定に指定した IP アドレスに関しては、プロキシとしての機能が優先されます。

設定値	説明
する	パケットをフォワーディングする。
しない	パケットをフォワーディングしない。

「3.2.1. 基本設定」のサーバ種別が Forward(透過性 L4 スイッチ)で、バイパス設定を設定した場合、パケットフォワーディングは自動的に「する」が設定されます。この場合、「しない」への変更はできません。

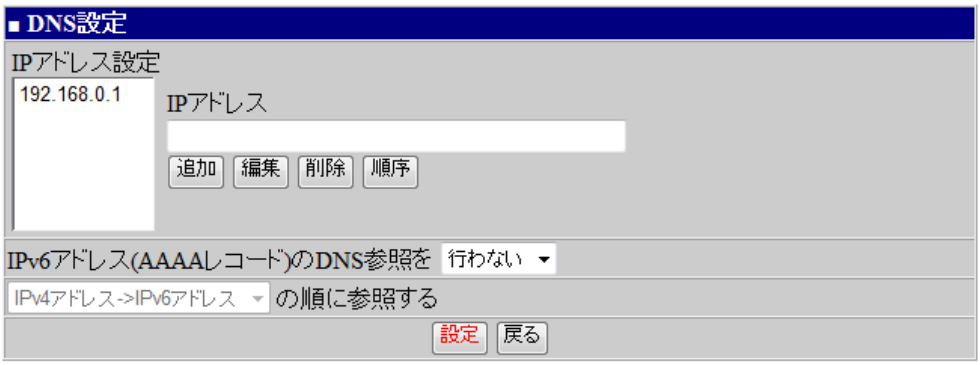
✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

設定はサーバを再起動しないと有効になりません。

DNS 設定

DNS の設定を行います。



◆ DNS 設定

DNS の一覧が表示されます。設定可能数は 16 までです。

この中から設定変更、または削除する DNS 設定の選択を行います。

一覧に表示されている DNS を選択すると、一覧の隣に DNS の IP アドレスが表示されます。DNS の IP アドレスを編集したあとに[編集]を押下することで設定内容を変更できます。

また、DNS の追加を行うときは、DNS の IP アドレスを入力したあと、[追加]を押下してください。これにより一覧に新たな DNS が登録されます。

DNS 設定の削除を行う場合には、削除したい DNS を一覧から選択後に[削除]を押下してください。

DNS は上位に表示されているものから優先的に使用されます。DNS の並びを変更する際には[順序]を押下し、表示される編集画面で変更してください。

なお、追加/編集/削除/順序の操作を行っても、画面下部の[設定]を押下しないと設定内容は反映されません。

▶ IP アドレス

DNS の IP アドレスを指定します。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。
[順序]	リストの順序を変更することが出来ます。→「xxx XXXX」

▶ IPv6 アドレス(AAAA レコード)の DNS 参照を行う／行わない

ホスト名に対応する IP アドレスの問い合わせを行う際、IPv6 アドレス(AAAA レコード)に関する問い合わせも行うかどうかを選択します。

設定値	説明
行わない	デフォルトは「行わない」です。
行う	IPv6 アドレス(AAAA レコード)に関する問い合わせも行います。

▶ IPv4 アドレス->IPv6 アドレス/IPv6 アドレス->IPv4 アドレスの順に参照する

「IPv6 アドレス(AAAA レコード)の DNS 参照を」「行う」場合に参照を行う順番を指定します。先に参照を行った方の結果が異常だった場合のみ後の方の問い合わせを行います。

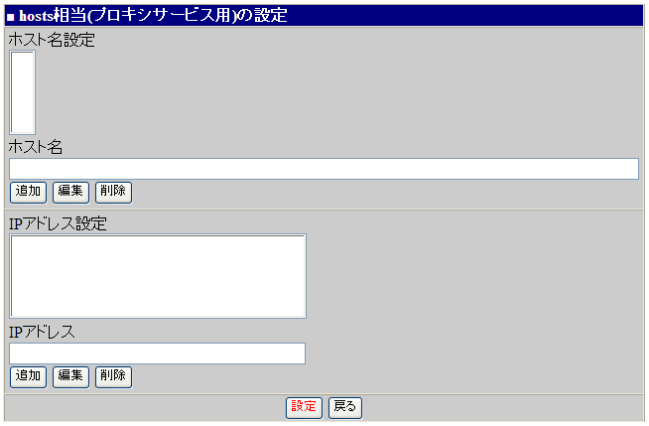
設定値	説明
IPv4 アドレス->IPv6 アドレス	IPv4 アドレス(A レコード)を先に参照します。デフォルトになります。
IPv6 アドレス->IPv4 アドレス	IPv6 アドレス(AAAA レコード)を先に参照します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

hosts 相当(プロキシサービス用)の設定

ホスト名と IP アドレスの静的な対応付けの設定を行います。
リクエストの URL に対して使用される機能になります。
本機能は、プロキシサービスの機能となりますので/etc/hosts ファイルの設定とは異なります。



◆ ホスト名設定

ホスト名の設定を行います。
ホスト名の一覧が表示されます。設定可能数は 512 までです。同じホスト名は登録できません。
ホスト名の追加を行うときは、ホスト名を入力したあと、[追加]を押下してください。これにより、一覧に新たなホスト名が登録されます。
ホスト名の編集を行うときは、一覧に表示されているホスト名を選択すると、一覧の隣にホスト名が表示されます。
ホスト名の編集をした後に[編集]を押下することで設定内容を変更できます。
ホスト名の削除を行うときは、削除したいホスト名を選択後に[削除]を押下してください。
なお、追加/編集/削除の操作を行っても、画面下部の[設定]を押下しないと設定内容は反映されません。

▶ ホスト名

ホスト名を指定します。255 文字まで入力できます。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

◆ IP アドレス設定

IP アドレスの設定を行います。

IP アドレスの一覧が表示されます。一つのホスト名に対して 16 個の IP アドレスを設定することが可能です。同じ IP アドレスは登録できません。

IP アドレスの追加を行うときは、IP アドレスを入力したあと、[追加]を押下してください。これにより、一覧に新たな IP アドレスが登録されます。

IP アドレスの編集を行うときは、一覧に表示されている IP アドレスを選択すると、一覧の隣に IP アドレスが表示されます。

IP アドレスの編集をした後に[編集]を押下することで設定内容を変更できます。

IP アドレスの削除を行うときは、削除したい IP アドレスを選択後に「削除」を押下してください。

なお、追加/編集/削除の操作を行っても、画面下部の[設定]を押下しないと設定内容は反映されません。

▶ IP アドレス

ホスト名に対する IP アドレスを指定します。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

ネットワーク設定

ネットワークのインタフェースとルーティングの設定を行います。

- インタフェース

  インタフェースをクリックすることで「3.5.15.1. インタフェース」を表示します。

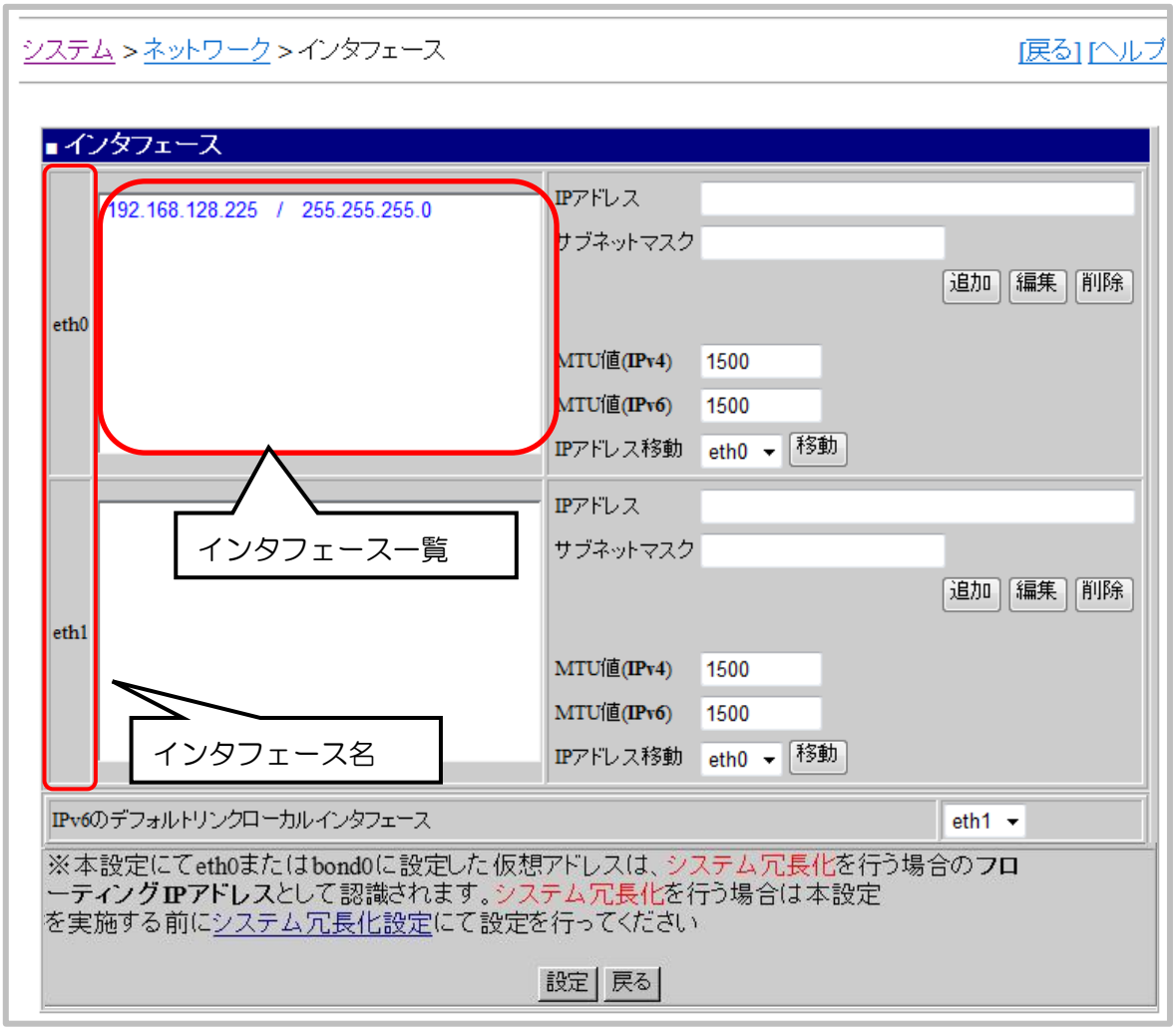
- ルーティング

  ルーティングをクリックすることで「3.5.15.2. ルーティング」を表示します。

3.5.15.1. インタフェース

インタフェース

NIC(Network Interface Card)、LAN ボードなどのネットワークインタフェースに関する設定を行います。



◆ インタフェース名

設定を行うインタフェース名を表示します。

利用可能なインタフェース分表示し、インタフェース毎に設定を行います。

◆ インタフェース一覧

各ネットワークインタフェース毎に割り当てたIPアドレスとサブネットマスクの組が表示されます。設定可能数は1つのネットワークインタフェースに対して256までです。この中から設定変更、または削除する設定の選択を行います。

一覧に表示されている設定を選択すると、一覧の隣に[IPアドレス]、[サブネットマスク]が表示されます。この[IPアドレス]と[サブネットマスク]を編集したあとに[編集]を押下することで設定内容を変更できます。

追加を行うときは、[IPアドレス]と[サブネットマスク]を入力したあと、[追加]を押下してください。これにより一覧の一番下に新たな設定が登録されます。

設定の削除を行う場合は、削除したい設定を選択後、[削除]を押下して下さい。

実IPアドレス(実在するネットワークデバイスのIPアドレス)は、一覧の一番上に青色で表示されています。

なお、追加/編集/削除の操作を行っても、画面下部の[設定]を押下しないと設定内容は反映されません。

▶ IPアドレス

追加/編集/削除するIPv4、IPv6アドレスを入力します。

IPv4アドレスが最低1つある状態でIPv6アドレスの設定を行ってください。

▶ サブネットマスク

IPアドレスが所属するネットワークのサブネットマスクを入力します。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[編集]	選択した設定の編集を行います。編集後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

▶ MTU値(IPv4)

このインタフェースに割り当てるMTU(最大転送単位)を指定してください。デフォルトは1500です。

100以上1500以下の整数を指定できます。

▶ MTU値(IPv6)

このインタフェースに割り当てるMTU(最大転送単位)を指定してください。デフォルトは1500です。

1280以上1500以下の整数を指定できます。

▶ IPアドレス移動

IPアドレスを他のネットワークインタフェースに移動します。移動するIPアドレスを指定し、移動先のインタフェース名を選択したあと、[移動]を押下します。

✓ ボタンの説明

[移動]	移動する IP アドレスを指定し、移動先のインタフェース名を選択したあと[移動]を押下することで IP アドレスを他のネットワークインタフェースに移動します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

・設定は[設定]ボタンをクリックした後、サーバを再起動しないと有効になりません。
・IP アドレスを変更または削除した場合、以下の各設定画面で設定している IP アドレスも連動して変更／削除します。
  ・「3.2.1. 基本設定」のキャッシュサーバ設定に指定している IP アドレス
  ・「3.2.1. 基本設定」の FTP プロキシ設定の IP アドレス
  ・「3.6. Management Console」のアクセス可能待ち受け IP
  ・「3.2.14. SSL アクセラレータ設定(リバースプロキシ用)」のアクセラレータ待ち受け(変更のみ連動します)
  ・「3.2.14. SSL アクセラレータ設定(リバースプロキシ用)」のアクセス転送先のキャッシュサーバ
  ・「ICAP サーバ設定 ICAP サーバ設定」の ICAP サーバの IP アドレスに設定されている IP アドレス
・「3.2.1. 基本設定」のキャッシュサーバ設定に指定している IP アドレスまたは FTP プロキシ設定の IP アドレスを削除せずに IP アドレスをネットワークインタフェース間で移動させたい時は、「IP アドレス移動」を使用して下さい。
・「3.2.1. 基本設定」のキャッシュサーバ設定に指定している IP アドレスが全て削除された場合、ゲートウェイデバイス(通常は eth0)にの実 IP アドレスをキャッシュサーバ設定に設定します。この時、サーバ種別が Reverse に設定されている場合には、Forward にサーバ種別が変更されます。
・実 IP アドレスの削除を行った場合、変わりに残った一覧の一番上の IP アドレスが実 IP アドレスとして設定されます。
・実 IP アドレス、キャッシュサーバ設定 IP アドレス、アクセス可能待ち受け IP が変更されることで Management Console への接続先アドレスが変更されることがあるのでご注意ください。
・システム冗長化用に設定するフローティング IP アドレスは、稼動系／待機系にて同じ IP アドレスを指定してください。

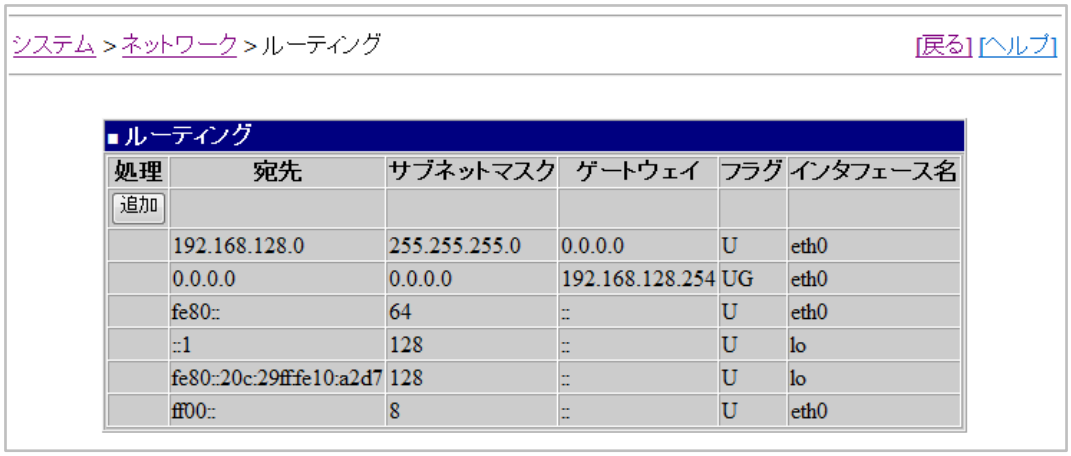
重要

- 「3.2.14. SSL アクセラレータ設定(リバースプロキシ用)」でアクセラレータ待ち受けに設定されている IP アドレスを[削除]ボタンを押して削除する場合、「3.2.14. SSL アクセラレータ設定(リバースプロキシ用)」でアクセラレータ待ち受けの削除を先に行ってください。
- 「3.2.20. ICAP サーバ設定」の ICAP サーバの IP アドレスに設定されている IP アドレスを[削除]ボタンを押して削除した場合、ゲートウェイデバイス(通常は eth0)の実 IP アドレスが ICAP サーバの IP アドレスに設定されます。
- 「3.2.20. ICAP サーバ設定」の ICAP サーバの IP アドレスに設定されている IP アドレスを[編集]ボタンで編集する際は、すでに設定されている待ちうけ(IP アドレス、ポート番号)と同じにならないようにしてください。

3.5.15.2. ルーティング

ルーティング

ルーティングテーブルは、パケットを目的のマシンに送信するためには、どのマシンに転送すればよいかを決定する情報を保持します。



- **処理**

  ✓ ボタンの説明

[追加]	ルーティングテーブルの追加を行います。 →「3.5.15.2.1. ルーティングテーブルの追加/編集」
[編集]	ルーティングテーブルの編集を行います。 →「3.5.15.2.1. ルーティングテーブルの追加/編集」
[削除]	ルーティングテーブルの削除を行います。

- **宛先**

  パケット送信の宛先を表示します。

- **サブネットマスク**

  サブネットマスクを表示します。

- **ゲートウェイ**

  ゲートウェイを表示します。

- **フラグ**

  フラグを表示します。経路の種類を意味します。

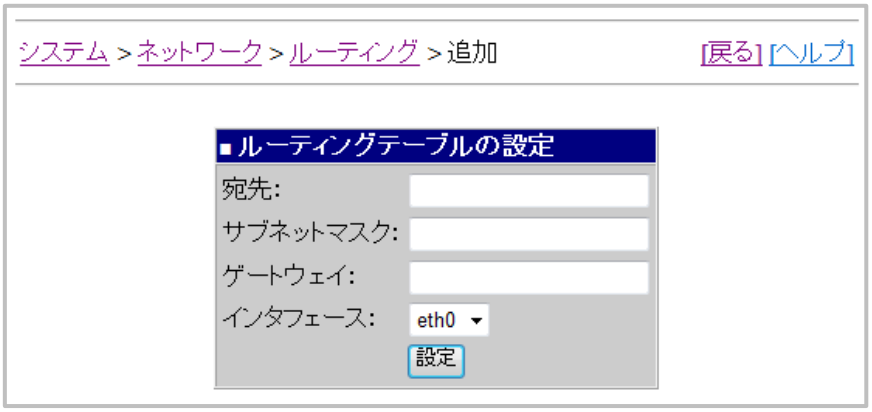
表示	説明
U	有効
H	ホスト
G	ゲートウェイ

- **インタフェース名**

  インタフェースを表示します。

3.5.15.2.1. ルーティングテーブルの追加/編集

ルーティングテーブルの追加/編集



- ◆ 宛先

  パケット送信先のネットワークアドレスまたはホストアドレスを指定します。

- ◆ サブネットマスク

  宛先がネットワークの場合はそのサブネットマスクを、宛先がホストの場合は 255.255.255.255 を指定します。

- ◆ ゲートウェイ

  このルーティングテーブルが選択された場合の、パケットの送信先の IP アドレスを指定します。ゲートウェイマシンは、このホストと同じネットワーク上に存在していなくてはなりません。宛先において自分自身が接続されているネットワークである場合、ゲートウェイには自分自身のインタフェースのアドレスを指定します。

- ◆ インタフェース

  このルーティングを設定するインタフェースを指定します。

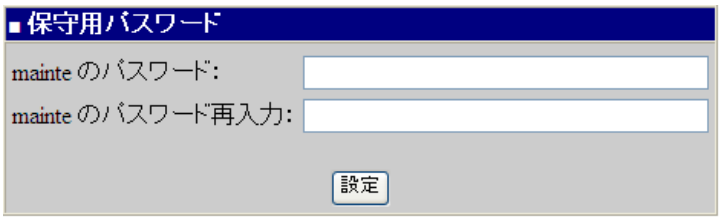
✓ ボタンの説明

[設定]	指定した内容を設定します。

3.5.16. 保守用パスワード

保守用パスワード

保守用ユーザ(mainte)のパスワードを設定します。設定を行った後、「mainte」ユーザでリモートログイン(telnet)サービス、リモートシェル(sshd)サービスを利用することができます。



- **mainte のパスワード**

  各パスワードは 6 文字以上 14 文字以下の半角英数文字（半角記号を含む）を指定してください。省略すると、パスワードは変更されません。空のパスワードを指定することはできません。

- **mainte のパスワード再入力**

  パスワード入力が誤っていないか確認するために、もう一度同じパスワードを入力します。

✓ **ボタンの説明**

[設定]	入力した内容を設定し、内容を反映させます。

3.5.17. バックアップ/リストア

バックアップ/リストア一覧

システムの故障、設定の誤った変更など思わぬトラブルからスムーズに復旧するために、定期的にシステムのファイルのバックアップをとっておくことを強く推奨します。バックアップしておいたファイルを「リストア」することによってバックアップを作成した時点の状態へシステムを復元することができるようになります。本製品では、システム内のファイルを以下の 5 つのグループに分類して、その各グループごとにファイルのバックアップのとり方を制御することができます。

■バックアップ/リストア一覧

操作	説明	世代数	タイミング
バックアップ 編集 リストア	システムの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシサーバの設定ファイル	5	バックアップしない
バックアップ 編集 リストア	各種ログファイル	5	バックアップしない
バックアップ 編集 リストア	プロキシアクセス統計情報	5	バックアップしない
バックアップ 編集 リストア	ESMPRO/SAのバックアップ	5	バックアップしない
バックアップ 編集 リストア	ディレクトリ指定	5	バックアップしない

重要

システムの設定ファイル、およびプロキシサーバの設定ファイルは必ずバックアップを設定してください。

各グループのバックアップ対象ディレクトリおよび作成されるファイルの名称は以下の通りです。

グループ	バックアップ対象
システムの設定ファイル	対象ディレクトリ: /etc 配下 /opt/nec/wpad/wpad.dat /opt/nec/wbmc/bin/wbmc_minute /root/.forward /opt/nec/wbmc/adm/.htaccess /home/users/mainte /opt/nec/.ssl.term.bkup /opt/nec/roma/etc/ip.conf 圧縮(ローカル): backup_conf_(世代).tgz 圧縮(Samba): backup_smb_conf_(世代).tgz 圧縮(FTP): backup_ftp_conf_(世代).tgz
プロキシサーバの設定ファイル	対象ディレクトリ : /etc/crontab、pound、/opt/nec/ catfish、 roma 配下 圧縮(ローカル): backup_proxy_(世代).tgz 圧縮(Samba): backup_smb_proxy_(世代).tgz 圧縮(FTP): backup_ftp_proxy_(世代).tgz
各種ログファイル	対象ディレクトリ: /var/lib/logrotate.status 配下 /var/log 配下 圧縮(ローカル): backup_log_(世代).tgz 圧縮(Samba): backup_smb_log_(世代).tgz 圧縮(FTP): backup_ftp_ log_(世代).tgz
プロキシアクセス統計情報	対象ディレクトリ : /home/webalizer/ 配下 圧縮(ローカル): backup_alizer_(世代).tgz 圧縮(Samba): backup_smb_alizer_(世代).tgz 圧縮(FTP): backup_ftp_alizer_(世代).tgz
ESMPRO/SA のバックアップ	対象ディレクトリ : /opt/nec/esmpro_sa/registry 配下、data 配下 圧縮(ローカル): backup_ESMPROSA_(世代).tgz 圧縮(Samba): backup_smb_ESMPROSA_(世代).tgz 圧縮(FTP): backup_ftp_ESMPROSA_(世代).tgz

（つづき）

グループ	バックアップ対象
ディレクトリ指定	対象ディレクトリ: 任意のディレクトリ ※例えば、フィルタリングソフト（InterSafe WebFilter）関連のファイルをまとめて指定する場合、/usr/local/intersafe/ を指定します。 InterSafe WebFilter の設定ファイルのみを指定する場合は、/usr/local/intersafe/conf/proxy.inf を指定します。 圧縮(ローカル): backup_dirinfo_(世代).tgz 圧縮(Samba): backup_smb_dirinfo_(世代).tgz 圧縮(FTP): backup_ftp_dirinfo_(世代).tgz

重要

ディレクトリ指定の「バックアップの対象となるディレクトリ」にローカルディスクの「ディレクトリ」が含まれる設定を行うことはできません。
「ディレクトリ」を空欄にする場合「/var/backup」が設定されている状態と同じになります。

◆ 操作

✓ ボタンの説明

[バックアップ]	設定に従ってバックアップを実行します。
[編集]	バックアップの設定を行います。 →「3.5.17.1. バックアップ/リストアの編集」
[リストア]	リストアを実行します。 →「3.5.17.2. リストア実行」

◆ 説明

バックアップ対象の説明を表示します。

◆ 世代数

バックアップファイルをいくつ残すかを表示します。

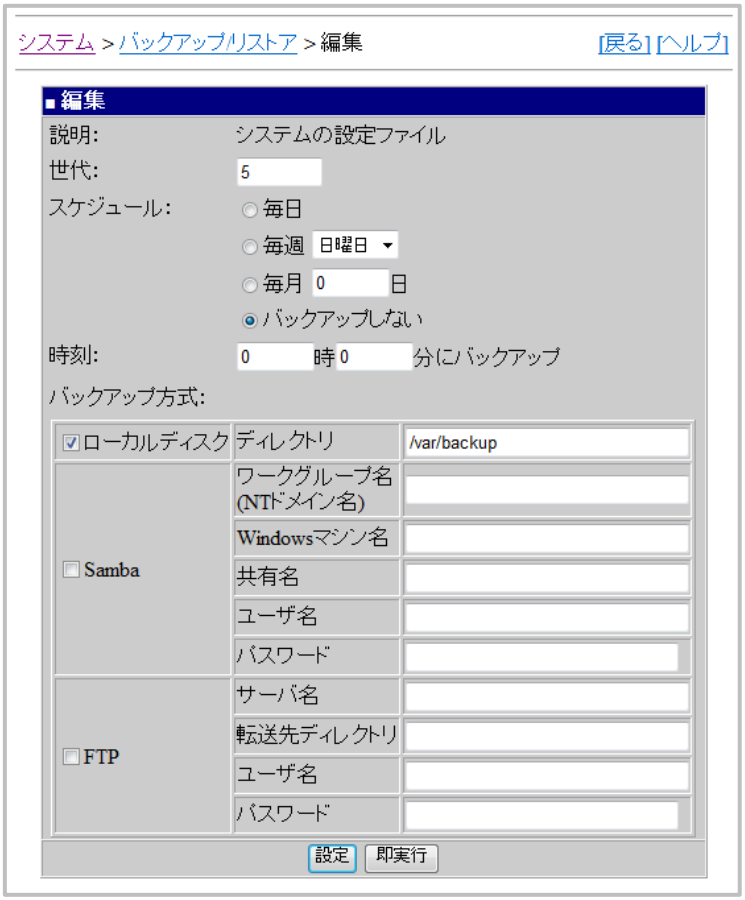
◆ タイミング

バックアップを実行するタイミングを表示します。

表示	説明
毎日	毎日バックアップを実行します。
毎週	毎週バックアップを実行します。
毎月	毎月バックアップを実行します。
バックアップしない	バックアップを行いません。

3.5.17.1. バックアップ/リストアの編集

編集



◆ 説明

バックアップ対象の説明を表示します。

◆ 世代

バックアップファイルをいくつ残すかを指定します。バックアップファイルを保管するディスクの容量と、必要性に応じて指定してください。世代を 1 にすると、バックアップを実行するたびに前回のバックアップ内容を上書きすることになります。

◆ スケジュール

バックアップを実行する日を指定します。

「毎日」、「毎週」、「毎月」、および「バックアップしない」から選択します。

デフォルトでは「バックアップしない」となっています。

設定値	説明
毎日	毎日バックアップを実行します。
毎週	毎週バックアップを実行します。右側の曜日も選択してください。
毎月	毎月バックアップを実行します。右側のテキストボックスに日付を入力してください。
バックアップしない	バックアップを行いません。

◆ 時刻

「スケジュール」で指定した日付の何時何分にバックアップを行うかを指定します。

重要 指定した時刻に本製品とバックアップ先のマシンが起動していない場合はバックアップできないので注意してください。

◆ バックアップ方式

「ローカルディスク」「Samba」「FTP」の 3 種類のバックアップ方法を指定することができます。

設定値	説明
ローカルディスク	本サーバのローカルディスクにバックアップを行います。 バックアップ先のディレクトリを指定します。既定ディレクトリは、/var/backup です。 Samba または FTP ではここで指定されたディレクトリにおいてバックアップ対象が圧縮されます。 ※空欄の場合は、"/var/backup"が設定されます。
Samba	Samba を利用して、Windows マシンにバックアップを行います。 実行前にあらかじめ Windows マシンに共有ディレクトリを設定する必要があります。 実行時は、最初にバックアップ対象が圧縮され、次に Windows マシンに設定した共有ディレクトリ配下に、デフォルトゲートウェイに接続するインタフェースの実 IP アドレスの名前でフォルダが作成され、最後に圧縮ファイルが Windows マシンへ転送されます。 Windows マシンの「ワークグループ名（NT ドメイン名）」「Windows マシン名」「共有名」「ユーザ名」「パスワード」を指定します。
FTP	FTP を利用して、FTP サーバにバックアップを行います。 FTP サーバの「サーバ名」「転送ディレクトリ」「ユーザ名」「パスワード」を指定します。

重要
- ローカルディスクへのバックアップは、他の方法に比べてリストアできない可能性が高くなります。なるべく Samba、FTP を使用して、別マシンへバックアップをとるようにしてください。
- Samba、FTP でのバックアップは、ローカルのハードディスクがクラッシュしても復元を行うことができますが、あらかじめ、バックアップ先のマシンに共有の設定をしておく必要がありますので注意してください。

重要 バックアップ方式にローカルディスクを指定する場合、ディスクフルを起こさないよう注意してください。ディスクフルになると、プロキシサービスが停止します。使用可能なデ

ィスク容量は、システムのディスク使用状況画面でマウントポイント「/」で表示されている容量です。標準構成の場合、以下の合計が使用可能なディスク容量を超えないよう、余裕を持たせた設定にしてください。

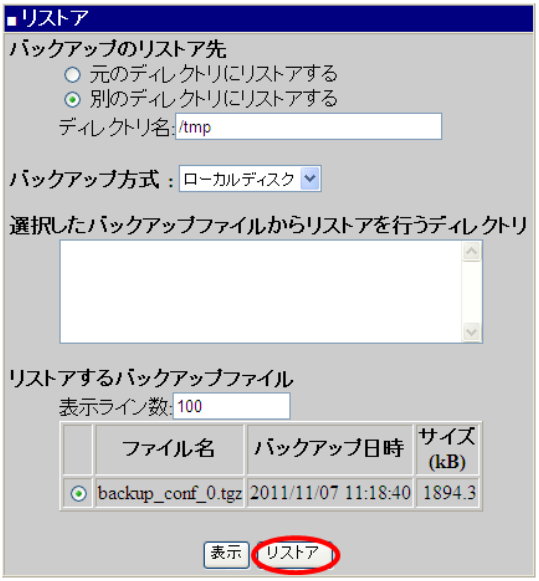
・万一の障害発生時のメモリダンプ採取用の空き領域(搭載メモリ分)
・InterScan WebManager、InterSafe WebFilter、
・i-FILTER のインストール用領域(約 100MB)
・InterScan WebManager、InterSafe WebFilter、i-FILTER のログファイル
・バックアップファイル
・システムのログ管理画面で設定できる各種ログファイル

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[即実行]	入力した内容を設定し、設定した内容に従ってバックアップを実行します。

3.5.17.2. リストア実行

リストア



◆ バックアップのリストア先

バックアップファイルのリストア先を指定します。

設定値	説明
元のディレクトリにリストアする	バックアップ時と同じディレクトリにリストアします。 現在の設定が、指定したバックアップファイルの内容に書き変わりますので注意してください。
別のディレクトリにリストアする	指定する別のディレクトリにリストアします。 「ディレクトリ名」で指定したディレクトリ配下にリストアを実行します。

◆ バックアップ方式

現在設定されているバックアップ方式の中から、リストアを行う方式を選択してください。

◆ 選択したバックアップファイルからリストアを行うディレクトリ

選択したバックアップファイルから特定のディレクトリまたはファイルをリストアする場合に指定します。ルートディレクトリ(/)から指定してください。

複数指定する場合は、スペース、改行、“,”(コンマ)のいずれかで区切ってください。

また、[表示]を押下してバックアップファイルの内容（ファイル名の一覧)で確認するようにしてください。

◆ リストアするバックアップファイル

どのバックアップファイルをリストアするかを指定します。
最新かどうかはバックアップ日時で確認してください。
バックアップデータのリストアは、バックアップ実行時のシステムへのアップデート適用状態と同じ状態にして実行してください。

► 表示ライン数

[表示]を押下した時に バックアップファイルの内容（ファイル名の一覧）を表示する行数を指定します。省略した場合は、全部表示されます。
指定可能な値は、1～18446744073709551615 です。

► ファイル名

バックアップファイル名です。

► バックアップ日時

バックアップを行った日時を表します。

► サイズ

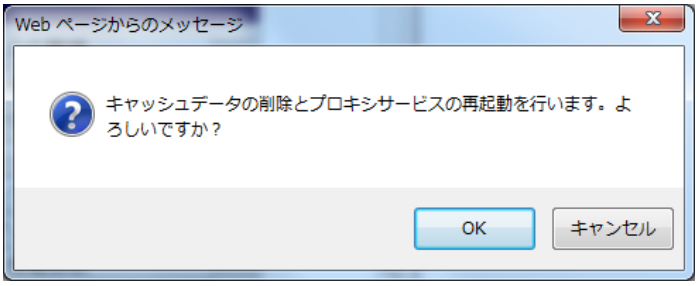
バックアップファイルにサイズを表示します。

✓ ボタンの説明

[表示]	指定したバックアップファイルの内容を表示します。リストアは実行されません。
[リストア]	指定したバックアップファイルを使用してリストアを実行します。元のディレクトリにリストアするを選択した場合、現在の設定がバックアップファイルの内容に書き変わりますので注意してください。

3.5.18. キャッシュデータ削除

キャッシュデータ削除確認ダイアログにて[OK]押下で、キャッシュされている全てのデータの削除とプロキシサービスの再起動を行います。



✓ ボタンの説明

[OK]	キャッシュデータの削除とプロキシサービスの再起動を行います。
[キャンセル]	キャッシュデータの削除とプロキシサービスの再起動をを行わず、前画面へ戻ります。

3.5.19. 管理者パスワード

管理者パスワード

システム管理者名(admin)やシステム管理者のパスワード、システム管理者宛のメール転送先を変更します。システム管理者名は半角英小文字で始まる１文字以上１６文字以下の半角英小文字数字、“_”、“-”で指定してください。各パスワードは 6 文字以上 14 文字以下の半角英数文字(半角記号を含む)を指定してください。省略すると、パスワードは変更されません。空のパスワードを指定することはできません。また、システム管理者宛のメールを転送する先を設定できます。システム管理者宛メールの転送先は正しく送信できるアドレスを指定してください。

- **admin の変更**

  システム管理者名は半角英小文字で始まる 1 文字以上 16 文字以下の半角英小文字数字，”_”，”-”で指定してください。

- **admin のパスワード**

  各パスワードは 6 文字以上 14 文字以下の半角英数文字（半角記号を含む）を指定してください。省略すると、パスワードは変更されません。空のパスワードを指定することはできません。

- **admin のパスワード再入力**

  パスワード入力が誤っていないか確認するために、もう一度同じパスワードを入力します。

- **メール転送先**

  バックアップなどの定期的に実行する処理の結果はシステムに保存されます。この結果をシステム外部のメールアドレスへ送る場合、転送先のメールアドレスを指定します(メール転送先を指定しない場合、システムに保存された結果は自動的に削除されます)。転送先を複数指定したいときは、スペース、改行、カンマ(,)のいずれかで区切ってその後ろに入力してください。

✓ **ボタンの説明**

[設定]	入力した内容を設定し、内容を反映させます。

重要

管理者のパスワードの変更を行うと、あわせてシステム管理者(root)のパスワードも変更します。

3.5.20. プロキシサーバ状態表示

本サーバに関する様々な情報を表示させ、確認することができます。

初期画面はプロキシサーバ状態表示(一般情報)です。

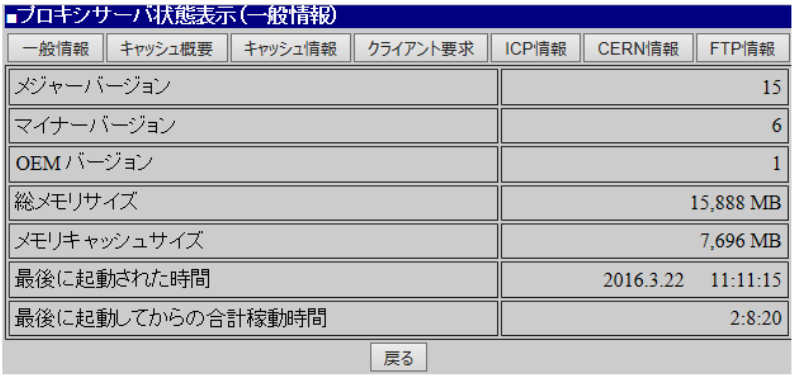
項目の中にある「単位時間」は 10 秒を単位とします。画面は 10 秒毎に更新されます。本画面で表示されるデータは、一般情報で表示される「最後に起動してからの合計稼働時間」内のデータで、プロキシサービスが再起動されるたびにリセットします。

プロキシサーバの状態表示は、画面上部のボタン(下記)押下で、対応する画面を表示します。

■プロキシサーバ状態表示(一般情報)
■プロキシサーバ状態表示(キャッシュ概要)
■プロキシサーバ状態表示(キャッシュ情報)
■プロキシサーバ状態表示(クライアント要求)
■プロキシサーバ状態表示(ICP 情報)
■プロキシサーバ状態表示(CERN 情報)
■プロキシサーバ状態表示(FTP 情報)

プロキシサーバ状態表示(一般情報)

本サーバのバージョン情報や運用時間等を表示します。



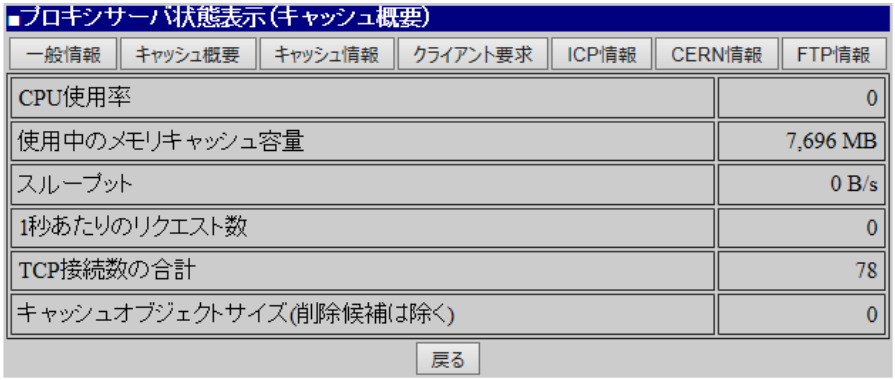
- **メジャーバージョン**
  プロキシサービスのメジャーバージョンです。
- **マイナーバージョン**
  プロキシサービスのマイナーバージョンです。
- **OEM バージョン**
  プロキシサービスの OEM バージョンです。
- **総メモリサイズ**
  本サーバのメモリサイズです。
- **メモリキャッシュサイズ**
  本サーバのメモリキャッシュサイズです。
- **最後に起動された時間**
  本サーバが最後に起動された時間です。
- **最後に起動してからの合計稼動時間**
  本サーバが最後に起動してから現在までの稼動経過時間です。

✓ **ボタンの説明**

[戻る]	前画面へ戻ります。

プロキシサーバ状態表示(キャッシュ概要)

本サーバの現在の動作状況等を表示します。



- **CPU 使用率**

  単位時間あたりの CPU 使用率です。

- **使用中のメモリキャッシュ容量**

  現在キャッシュ用として使用可能なメモリの容量です。

- **スループット**

  単位時間あたりのスループットです。B/s はバイト/秒です。

- **1 秒あたりのリクエスト数**

  直近 10 秒間の平均リクエスト数です。

- **TCP 接続数の合計**

  本サーバの TCP 接続数の合計です。

- **キャッシュオブジェクトサイズ(削除候補は除く)**

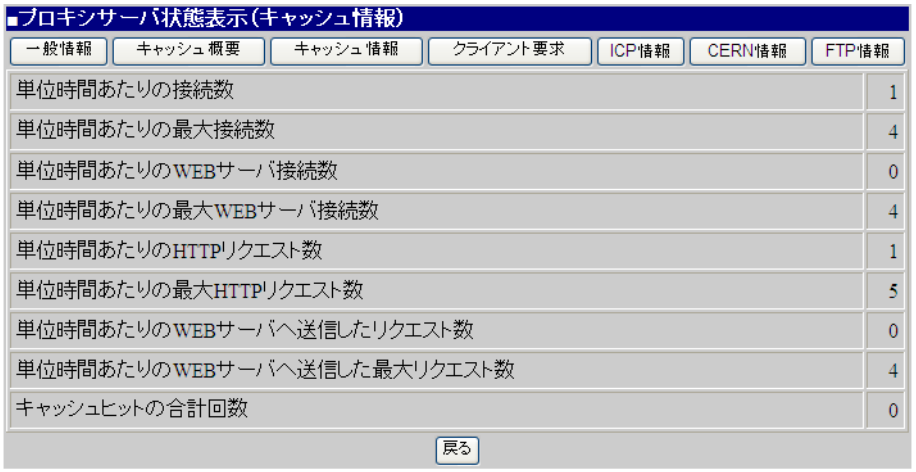
  本サーバで保持しているキャッシュのサイズです。

✓ **ボタンの説明**

[戻る]	前画面へ戻ります。

プロキシサーバ状態表示(キャッシュ情報)

一定時間あたりの本サーバへの接続数や、リクエスト数等を表示します。



- **単位時間あたりの接続数**

  単位時間あたりの接続数です。

- **単位時間あたりの最大接続数**

  最後に起動してから単位時間あたりの最大接続数です。

- **単位時間あたりの WEB サーバ接続数**

  単位時間あたりの WEB サーバ接続数です。

- **単位時間あたりの最大 WEB サーバ接続数**

  最後に起動してから単位時間あたりの最大 WEB サーバ接続数です。

- **単位時間あたりの HTTP リクエスト数**

  単位時間あたりの HTTP リクエスト数です。

- **単位時間あたりの最大 HTTP リクエスト数**

  最後に起動してから単位時間あたりの最大 HTTP リクエスト数です。

- **単位時間あたりの WEB サーバへ送信したリクエスト数**

  単位時間あたりの WEB サーバへ送信したリクエスト数です。

- **単位時間あたりの WEB サーバへ送信した最大リクエスト数**

  最後に起動してから単位時間あたりの WEB サーバへ送信した最大リクエスト数です。

- **キャッシュヒットの合計回数**

  最後に起動してからのキャッシュにヒットした合計回数です。

✓ **ボタンの説明**

[戻る]	前画面へ戻ります。

プロキシサーバ状態表示(クライアント要求)

本サーバが起動開始から現時点までに処理した様々な情報を表示します。

- **受信したリクエスト数**

  本サーバが受信したリクエスト数の合計です。

- **L4 スイッチ経由で受信したリクエスト数**

  本サーバが L4 スイッチ経由で受信したリクエスト数の合計です。

- **クライアントへ返した合計オブジェクトサイズ**

  本サーバがクライアントへ返したオブジェクトの合計サイズです。

- **クライアントから受信した合計リクエストサイズ**

  本サーバがクライアントから受信したリクエストの合計サイズです。

- **単位時間あたりの処理中リクエスト数**

  単位時間あたりの処理中のリクエスト数です。

- **WEB サーバに要求した合計リクエスト数**

  本サーバが WEB サーバに要求したリクエスト数の合計です。

- **エラーとして返した合計応答数**

  本サーバがエラーとして返した応答数の合計数です。

- **連携プロキシサーバに要求したリクエスト数**

  本サーバが連携プロキシサーバに要求したリクエスト数の合計です。

- **WEB サーバに送信したリクエストサイズ**

  本サーバが WEB サーバに送信したリクエストサイズの合計です。

◆ WEB サーバから受信したオブジェクトサイズ

本サーバが WEB サーバから受信したオブジェクトサイズの合計です。

◆ 接続に失敗した回数

本サーバが接続に失敗した回数の合計です。

◆ スケジュールダウンロードが送信したリクエスト数

本サーバのスケジュールダウンロードが送信したリクエスト数の合計です。

◆ WEB サーバから「304 Not Modified」で返された応答数

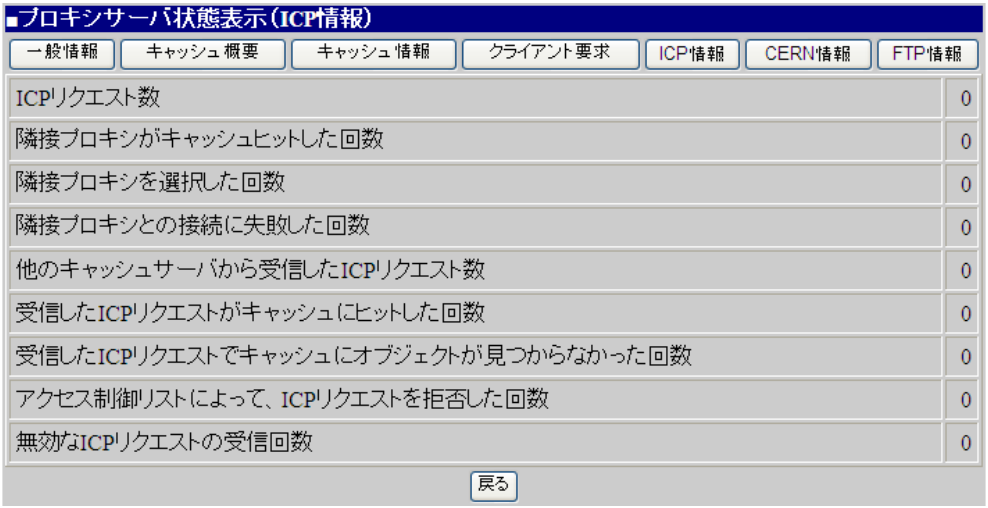
本サーバが WEB サーバから「304 Not Modified」(変更無し)で返された応答数の合計です。

✓ ボタンの説明

[戻る]	前画面へ戻ります。

プロキシサーバ状態表示(ICP 情報)

隣接キャッシュサーバに関連する情報を表示します。



- **ICP リクエスト数**

  本サーバの ICP リクエスト数の合計です。

- **隣接プロキシがキャッシュヒットした回数**

  隣接プロキシでキャッシュにヒットした回数の合計です。

- **隣接プロキシを選択した回数**

  本サーバが隣接プロキシを選択した回数の合計です。

- **隣接プロキシとの接続に失敗した回数**

  本サーバが隣接プロキシとの接続に失敗した回数の合計です。

- **他のキャッシュサーバから受信した ICP リクエスト数**

  本サーバが他のキャッシュサーバから受信した ICP リクエスト数の合計です。

- **受信した ICP リクエストがキャッシュにヒットした回数**

  受信した ICP リクエストが本サーバでキャッシュにヒットした回数の合計です。

- **受信した ICP リクエストでキャッシュにオブジェクトが見つからなかった回数**

  受信した ICP リクエストが本サーバでキャッシュにオブジェクトが見つからなかった回数の合計です。

- **アクセス制御リストによって、ICP リクエストを拒否した回数**

  本サーバのアクセス制御リストによって、ICP リクエストを拒否した回数の合計です。

- **無効な ICP リクエストの受信回数**

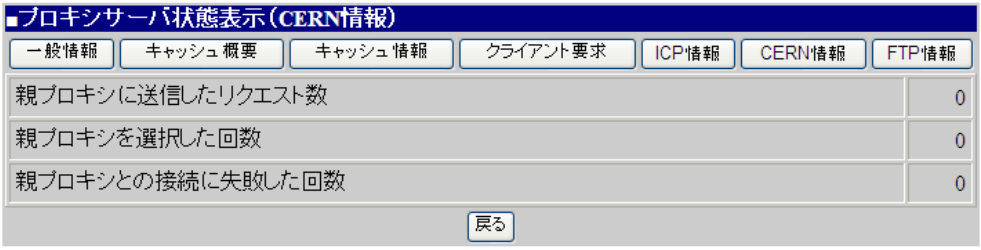
  無効な ICP リクエストの受信回数の合計です。

✓ **ボタンの説明**

[戻る]	前画面へ戻ります。

プロキシサーバ状態表示(CERN 情報)

親プロキシサーバに関連する情報を表示します。



◆ 親プロキシに送信したリクエスト数

本サーバが親プロキシに送信したリクエスト数の合計です。

◆ 親プロキシを選択した回数

本サーバが親プロキシを選択した回数の合計です。

◆ 親プロキシとの接続に失敗した回数

本サーバが親プロキシとの接続に失敗した回数の合計です。

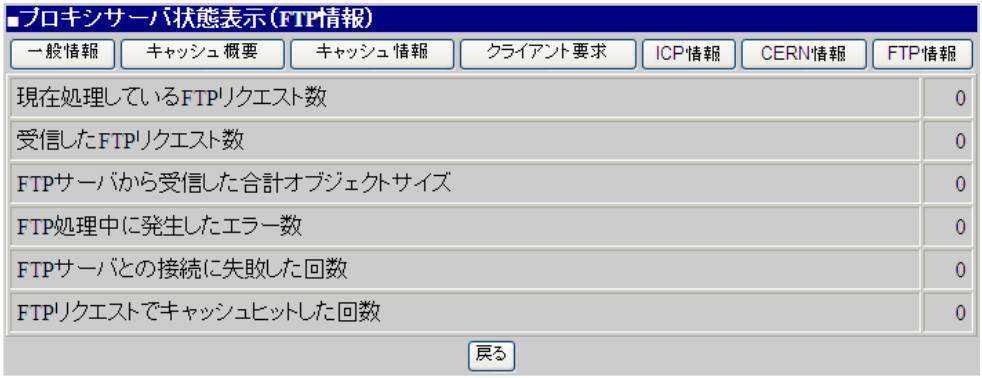
✓ ボタンの説明

[戻る]	前画面へ戻ります。

プロキシサーバ状態表示(FTP 情報)

HTTP 経由での FTP プロトコルに関連する情報を表示します。
以下の情報を表示していますので、親プロキシ経由でリクエストを処理したリクエストについてはカウントの対象となりません。

・本サーバが FTP サーバと直接通信を行ったリクエストに関する情報
・本サーバがキャッシュから応答を返却したリクエストに関する情報



◆ 現在処理している FTP リクエスト数

本サーバが現在処理している FTP リクエスト数の合計です。

◆ 受信した FTP リクエスト数

本サーバが受信した FTP リクエスト数の合計です。

◆ FTP サーバから受信した合計オブジェクトサイズ

本サーバが FTP サーバから受信した合計オブジェクトサイズです。

◆ FTP 処理中に発生したエラー数

本サーバが FTP 処理中に発生したエラー数の合計です。

◆ FTP サーバとの接続に失敗した回数

本サーバが FTP サーバとの接続に失敗した回数の合計です。

◆ FTP リクエストでキャッシュヒットした回数

本サーバが FTP リクエストでキャッシュにヒットした回数の合計です。

✓ ボタンの説明

[戻る]	前画面へ戻ります。

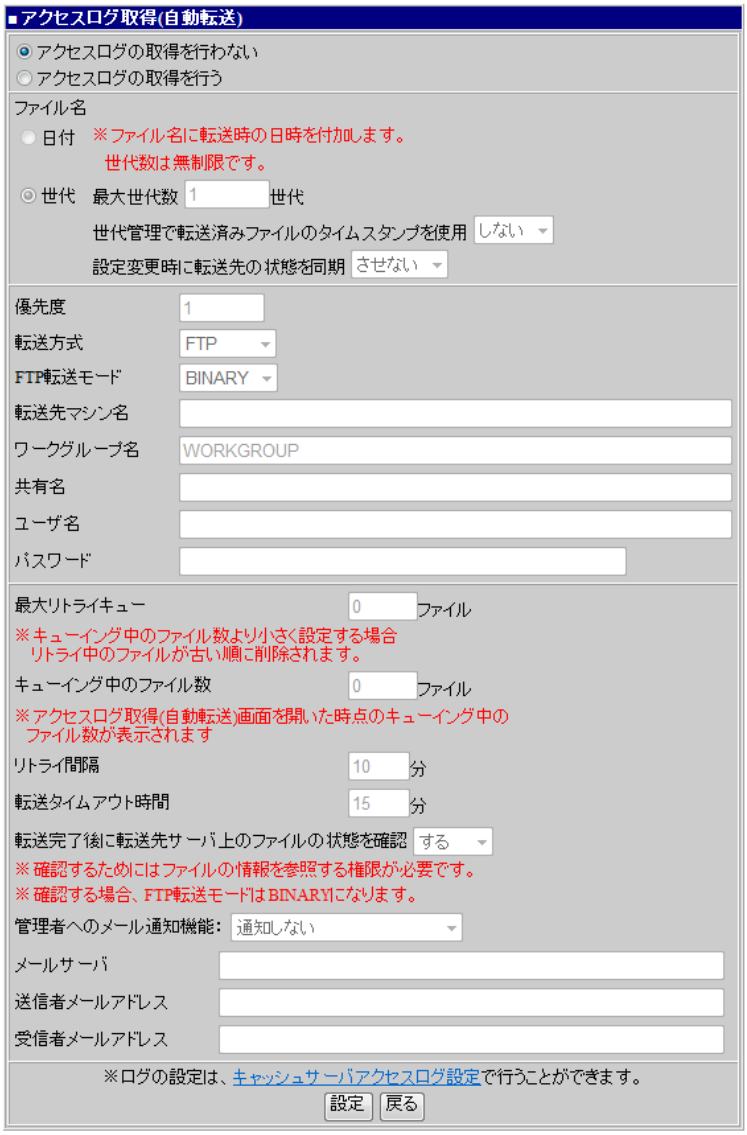
3.5.21. アクセスログ取得(自動転送)

アクセスログの取得(自動転送)

ログ管理のキャッシュサーバアクセスログを、ファイル名の形式、転送方式等を指定して別のサーバへ転送します。

アクセスログの転送はログのローテートが行われた直後(1 分以内)に開始されます。

ログ転送を行う際には「3.5.12. ログ管理」のキャッシュサーバアクセスログ設定にて出力形式を設定してください。ファイルサーバへアクセスログを転送する際に使用するアカウントにはファイルの書き込み及び参照の権限が必要です。



◆ アクセスログの取得を行わない/行う

アクセスログの取得を行うか、行わないかを選択します。

行わないを選択した場合、下記の設定内容は無効になり、キューイング中のファイルが存在する場合、全て削除されます。

行うを選択した場合、下記の項目に設定した条件にしたがって、アクセスログの取得を行います。

◆ ファイル名

転送するファイル名について設定します。

「日付」と「世代」から選択します。デフォルトは「世代」です。

▶ 日付

転送するアクセスログファイル名に日時を付加します。

転送先マシンに転送されるファイル名は「access(日時).log」の形式で転送されます。

(例：2008/1/1 3:30 にローテートされた場合ファイル名は、「access0801010330.log」となります。)

▶ 世代

転送するアクセスログファイル名に世代数を付加します。

転送先マシンに転送されるファイル名は「access(世代).log」の形式で転送されます。

(例：転送するファイルが 1 世代目の場合、ファイル名は「access1.log」になります。)

また、以下の設定を行なってください。

➢ 最大世代数

最大世代数を指定します。1 世代から 99 世代まで指定可能です。デフォルトは「1」世代です。

- 世代管理で転送済みファイルのタイムスタンプを使用する/しない

世代管理のため、転送済みファイルのタイムスタンプ情報を使用するか、しないかを選択します。デフォルトは「しない」です。

設定値	説明
する	世代管理に転送済みファイルのタイムスタンプ情報を使用する。
しない	世代管理に転送済みファイルのタイムスタンプ情報を使用しない。

世代管理の処理は、下記のタイミングで実施します。

・アクセスログを転送する時。
・転送先の状態を同期させる時。

「しない」を指定した場合、ローカルに保持している値を使用して世代管理を行います。「する」を指定した場合、転送先から取得したタイムスタンプを使用して新旧の判断を行います。「する」を指定する場合、以下の条件を満たす必要があります。

・転送先マシンに転送済みのファイルを上書きする等タイムスタンプを変更する作業を行わない。古いアクセスログを上書きした場合、新しいファイルとして認識されます。
・転送方式が FTP の場合、転送先マシンの一覧表示の出力フォーマットが UNIX、Windows、EPLF のいずれかである。
・転送先ディレクトリの参照ができる権限を持つユーザを設定する。
転送先のディレクトリを参照する権限がない場合、ディレクトリの中身が空の状態である時と同じ応答が返ってくる可能性があり、その場合転送済みの「access1.log」が上書きされます。

➢ 設定変更時に転送先の状態を同期させる/させない

設定変更時に転送先の状態を同期「させる」か「させないか」を選択します。
デフォルトは「させない」です。

設定値	説明
させない	転送先マシンのファイルの並び替え等を行いません。
させる	転送方式、転送先マシン名、ワークグループ名、共有名、ユーザ名、最大世代数のいずれかの変更が行われた場合、転送先マシンに転送したアクセスログの名前をタイムスタンプの新しい順番に並び替えます。 その際、転送先マシンに転送済みのアクセスログが最大世代数より多い場合、タイムスタンプが古い順に世代のローテート対象にならない形式(「元のファイル名_同期を行った時間(UNIX 時間)_項番」)にファイル名をリネームします。 「させる」と指定する場合以下の条件を満たす必要があります。 ・ファイル名の変更ができる権限を持つユーザを設定する。 ・転送先ディレクトリの参照ができる権限を持つユーザを設定する。 ・転送先マシンにプロキシサーバからアクセスが行える。 転送先の状態を同期できない場合、設定変更は行われません。

◆ 優先度

アクセスログ取得(自動転送)の優先度を指定します。
1 から 19 まで設定可能で、値が大きいほど優先度が低くなります。優先度を低くすることによりアクセスログ取得(自動転送)処理による CPU の負荷を減らすことができます。
あまりに低い優先度を指定すると正常にアクセスログ取得(自動転送)が動作しない可能性があります。デフォルトは 1 です。

◆ 転送方式

次の 2 つから選択します。デフォルトは FTP です。

設定値	説明
FTP	FTP で転送します。
SAMBA	SAMBA で転送します。

◆ FTP 転送モード

「転送方式」で FTP を選択した場合に、使用する転送モードを指定します。デフォルトは BINARY です。

設定値	説明
ASCII	ASCII モードでファイル転送を行います。サーバによっては転送したファイルの改行コード等が変換される可能性があります。
BINARY	BINARY モードでファイル転送を行います。

◆ 転送マシン名

転送先マシンの IP アドレスまたは、ホスト名を入力します。

◆ ワークグループ名

「転送方式」で SAMBA を選択した場合に、転送を行う際に使用するワークグループ名を指定します。NT ドメインに関しても有効です。

「転送方式」で FTP を選択した場合、本設定は無効となります。

◆ 共有名

転送方式が SAMBA の場合は、転送先マシンの共有されているディレクトリ名を入力します。

転送方式が FTP の場合は、転送先マシンのホームディレクトリ配下のディレクトリを指定します。

ブランクの場合はホームディレクトリになります。

◆ ユーザ名

ログイン時のユーザ名を入力します。

◆ パスワード

ログイン時のパスワードを入力します。

◆ 最大リトライキュー

アクセスログの転送失敗時にキューイングできるファイル数を指定します。

キューイング中のファイル数より小さく設定された場合、キューイングされているファイルが古い順に削除されます。

0 ファイルから 99 ファイルまで設定可能です。

(最大リトライキュー ＋1）× ローテートサイズがログ領域(/var/log/roma)のサイズ以内で収まるように設定を行ってください。

最大リトライキューの設定を大きくするとディスクフルの原因になるため下記の計算を参考に設定を行ってください。デフォルトは 0 です。

【計算方法】

ディスク使用状況のマウントポイントに/var/log/roma のパーティションが存在する場合

メモリダンプ(搭載メモリ × 0.25) ＋ ((最大リトライキュー ＋1）× ローテートサイズ)

※上記の合計がログ領域(/var/log/roma)のサイズ以内で収まるように設定を行ってください。

ディスク使用状況のマウントポイントに/var/log/roma のパーティションが存在しない場合

メモリダンプ(搭載メモリ × 1.25) ＋ アクセスログ以外の各種ログファイルの合計サイズ ＋ ((最大リトライキュー ＋1）× ローテートサイズ)

※InterSafe WebFilter/InterScan WebManager/i-FILTER をご利用の場合は以下のサイズも加えてください。

InterSafe WebFilter/InterScan WebManager/i-FILTER のプログラム(100MB) ＋ InterSafe WebFilter/InterScan WebManager/i-FILTER の各種ログサイズ

◆ キューイング中のファイル数

アクセスログ取得(自動転送)を開いた時点でキューイングされているアクセスログの数を表示します。

◆ リトライ間隔

アクセスログの転送失敗後、再度転送を行うまでの間隔を設定します
最大リトライキューを 0 に設定されている場合、リトライ間隔の設定は無効となります。
5 分から 99 分まで設定可能です。デフォルトは 10 分です。

◆ 転送タイムアウト時間

アクセスログ転送の待ち時間を設定します。待ち時間を超えた場合、転送処理を停止させます。
1 分から 99 分まで設定可能です。デフォルトは 15 分です。
あまりに小さい時間を設定した場合、アクセスログ転送が失敗する可能性があります。

◆ 転送完了後に転送先サーバ上のファイルの状態を確認する/しない

アクセスログ転送完了後に転送の成否を転送先サーバ上の当該アクセスログのサイズで判断するかどうかを指定します。

設定値	説明
する	本サーバ上と転送先サーバ上の当該アクセスログのサイズが同じであれば転送成功と判断します。 ※転送に使用するユーザに転送先サーバでファイルを参照できる権限が必要です ※確認する場合、FTP 転送モードは BINARY になります。
しない	本サーバ上と転送先サーバ上の当該アクセスログのサイズに関わらず転送成功と判断します。

◆ システム管理者へのメール通知機能

システム管理者へのメール通知を行うかを設定します。デフォルトは「通知しない」です。

設定値	説明
通知しない	アクセスログ転送の結果をシステム管理者へメール通知しません。
失敗時に通知する	アクセスログ転送が失敗又はアクセスログが削除されるたびにシステム管理者へメール通知します。
失敗時と成功時に通知する	アクセスログ転送が失敗(1 回目の失敗時のみ)、成功時又はアクセスログが削除されるたびにシステム管理者へメール通知します。

◆ メールサーバ

送信するメールサーバのホスト名又は IP アドレスを設定します。

256 文字まで設定可能です。

◆ 送信者メールアドレス

送信者にするメールアドレスを設定します。

320 文字まで設定可能です。

@以降も必ず設定してください。

◆ 受信者メールアドレス

転送結果を送信するメールアドレスを設定します。

320 文字まで設定可能です。

@以降も必ず設定してください。

重要

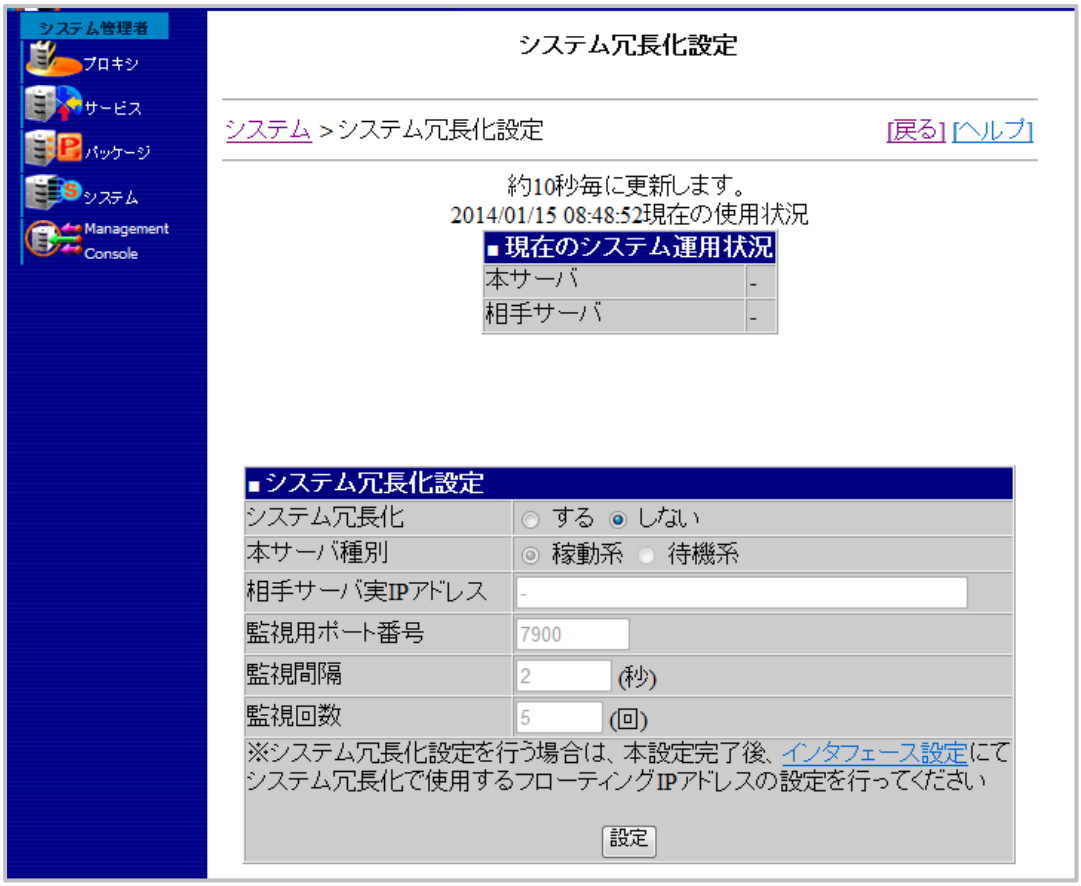
- アクセスログのローテートサイズの指定はキャッシュサーバアクセスログ設定にて行えます。
- アクセスログ取得(自動転送)を動作させている時は、アクセスログのローテートサイズの扱いに注意して下さい。性能低下を起こす可能性があります。
- 優先度は慎重に決定して下さい。あまりに低い優先度を設定すると正常に動作しない可能性があります。
- 転送先マシンにはおよそ最大世代数×ローテートサイズのディスク容量が必要となります。
- ファイル名に日付を付加する場合は転送先マシンにログファイルが無限に蓄積されます。
- プロキシサーバのアクセスログと同じ形式のファイル名で同じ場所にファイルを転送している場合、上書きされる可能性があります。
- アクセスログ取得(自動転送)を複数台のプロキシサーバで行っている場合(システム冗長化時も含む)、同じ場所にアクセスログを転送しないでください。転送したアクセスログが別のプロキシサーバから転送されたアクセスログに上書きされる場合があります。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。
[戻る]	前画面へ戻ります。

3.5.22. システム冗長化設定

システムの冗長化設定を行います。

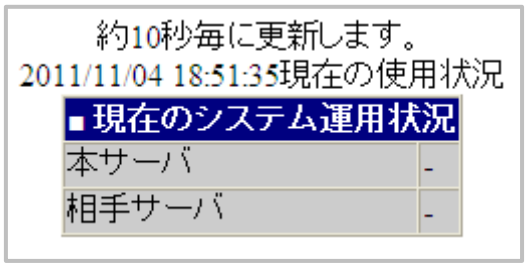


システム冗長化は以下の画面に分かれています。

■現在のシステム運用状況
■システム冗長化設定

現在のシステム運用状況

本サーバ/冗長化している相手サーバそれぞれの現在のシステム運用状況を表示します。システム冗長化を行っていない場合、"-"が表示されます。

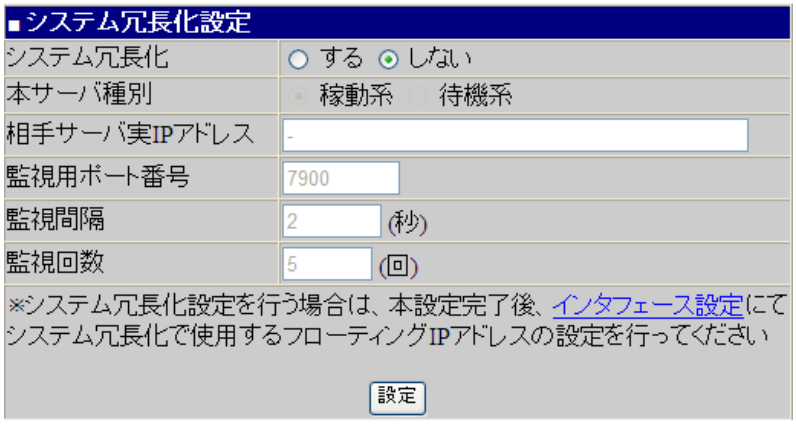


下記のメッセージを表示します。

本サーバ種別	相手サーバ種別	本サーバ運用状況	相手サーバ運用状況	説明
稼動系	待機系	稼動系として運用中です。	待機系として運用中です。	正常にシステム冗長化が行われています。
			通信異常の為状況不明です。	本サーバは正常に稼動していますが、相手サーバが停止している可能性があります。
		サービス停止中です。	稼動系として運用中です。	本サーバのプロキシサービスが停止している可能性があるため、相手サーバを稼動系とし運用しています。
			通信異常の為状況不明です。	システム冗長化するためのサービスが正常に動作していない可能性があります。
待機系	稼動系	待機系として運用中です。	稼動系として運用中です。	正常にシステム冗長化が行われています。
			通信異常の為状況不明です。	相手サーバが停止している可能性があるため、本サーバを稼動系として運用しています。
		サービス停止中です。	稼動系として運用中です。	本サーバのプロキシサービスが停止している可能性があるため、相手サーバを稼動系として運用しています。
			通信異常の為状況不明です。	システム冗長化するためのサービスが正常に動作していない可能性があります。

システム冗長化設定

システムを冗長化するにあたっての各種情報設定を行います。



◆ システム冗長化

システム冗長化する/しないを指定します。デフォルトは「しない」です。

設定値	説明
する	システム冗長化する。
しない	システム冗長化しない。

◆ 本サーバ種別

システム冗長化する場合、本サーバ運用方法について稼動系/待機系を指定します。デフォルトは「稼動系」です。

設定値	説明
稼動系	本サーバを稼動系とします。
待機系	本サーバを待機系とします。

◆ 相手サーバ実 IP アドレス

システム冗長化する場合、サーバ種別で稼働系を指定した場合は待機系の、待機系を指定した場合は稼動系の実 IP アドレスを指定します。

◆ 監視用ポート番号

システム冗長化する場合、稼動系～待機系間の死活監視用通信ポート番号を設定します。デフォルトは 7900 です。

1 から 65535 までの値で設定することができます。

通常は変更する必要はありません。他アプリケーションとポート番号が競合する場合などに変更します。設定を変更される場合、稼動系と待機系で同じポート番号を設定してください。

◆ 監視間隔

システム冗長化する場合、稼動系～待機系間の死活監視間隔を設定します。デフォルトは 2 秒です。 1 秒から 300 秒までの値で設定することができます。

◆ 監視回数

システム冗長化する場合、稼動系～待機系間のフェイルオーバーを開始するまでの試行回数を設定します。デフォルトは 5 回です。 1 回から 10 回までの値で設定することができます。

重要

・システム冗長化する場合、サーバ種別が稼動系のサーバ 1 台、待機系のサーバ 1 台の合計 2 台で運用してください。
・「3.5.21. アクセスログ取得(自動転送)」を行う場合、稼動系、待機系で異なる場所にアクセスログを転送してください。
(同じ場所に転送を行うと先に転送されているアクセスログが上書きされる場合があります)
・システム冗長化を使用して運用する場合、稼動系、待機系のモジュールのバージョンに差異がないようにしてください。
・システム冗長化のためのフローティング IP アドレスとして使用されるのは、eth0 に設定された仮想アドレスのみになります。
・稼働系の相手サーバ実 IP アドレスに待機系の IPv6 実 IP アドレスを指定した場合、待機系の相手サーバ実 IP アドレスも同様に稼働系の IPv6 実 IP アドレスを指定する必要があります

重要

・システム冗長化を構築している場合、稼働系のサーバが正常に稼働した時に自動的に切り替わります。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

3.5.23. ライセンス管理

ライセンス製品のインストール/アンインストールを管理します。対象製品は以下の通りです。

- SSL アクセラレータライセンス(forReverse)
- HTTPS 可視化ライセンス(forForward)

ライセンス管理

オプションライセンスのインストール及びアンインストールを行なうことが出来ます。

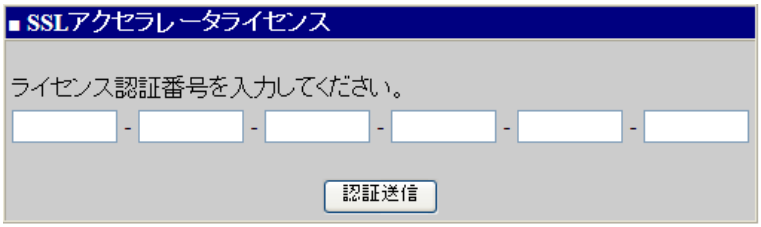
オプションライセンスの製品名を表示します。ライセンスの製品名の次に、ライセンスのインストール状態を表示します。

✓ **ボタンの説明**

[インストール]	ライセンスのインストールを行います。 →「3.5.23.1. ライセンスの登録」
[アンインストール]	ライセンスのアンインストールを行います。

3.5.23.1. ライセンスの登録

(登録するライセンス名)



◆ ライセンス認証番号を入力してください。

ライセンス認証番号を入力します。

✓ ボタンの説明

[認証送信]	指定した内容でライセンスの登録を行います。

3.5.24. 情報採取

情報採取

障害調査などに必要な情報を採取します。
基本的に障害発生時点の設定ファイル、障害が発生した時間を含んだログ情報を採取してください。
設定変更を行って運用している等の理由で、障害発生時点の設定ファイルが採取できない場合は、採取した設定ファイルと障害発生時点の設定ファイルの差分を(サポート窓口等へ)お伝えください。
必要な採取情報にチェックを行い、[実行]を押してください。
圧縮完了後に保存画面が表示されますので、「採取情報一覧」、「ファイルサイズ」を確認後、[保存]を押してクライアントに採取情報をダウンロードしてください。

✓ ボタンの説明

[実行]	チェックが入っている情報採取を実行します。

◆ ワークディスクの空き容量

情報採取画面を開いた時点のワークディスクの空き容量を表示します。

◆ 情報採取中にワークディスクの空き容量が[設定値]以下になったら情報採取を中断する

情報採取を中断するワークディスクの空き容量を設定します。

ワークディスクサイズの 1%を超える値から「ワークディスクの空き容量」の値まで設定可能です。

◆ 設定、状態管理情報

チェック時、プロキシサーバの設定および状態管理情報を採取します。システム管理者パスワードおよび秘密鍵等の機密性の高い情報は採取の対象になりません。

◆ システムログ情報

チェック時、システムログ、ipmi のログ情報を採取します。

◆ プロキシサービスログ情報

チェック時、プロキシサービスのログ情報を採取します。

キャッシュサーバアクセスログは非常にサイズが大きい可能性があるため、採取の対象なっておりません。

キャッシュサーバアクセスログが必要な場合は、「アクセスログ情報」を選択してください。

◆ アクセスログ情報

チェック時、キャッシュサーバアクセスログの情報を採取します。

◆ actlog 情報

チェック時、リソースの詳細情報を採取します。

actlog が起動している場合のみ、最新のリソースの詳細情報が採取されます。

デフォルトで actlog は起動しています。

◆ sar 情報

チェック時、sar の情報を採取します。

◆ Management Console ログ情報

チェック時、Management Console のログ情報を採取します。

◆ URL フィルタ用ログ領域(移行済み)情報

チェック時、URL フィルタ用ログ領域(移行済み)の情報を採取します。

URL フィルタ用ログ領域設定で移行を行っていない場合は、「ディレクトリ指定」で URL フィルタのログ領域を指定して採取してください。

◆ パケットキャプチャデータ情報

チェック時、パケットキャプチャデータ情報を採取します。

パケットキャプチャデータはパケットキャプチャにて採取することが可能です。

◆ その他の情報

チェック時、cron 等のログ情報を採取します。

◆ ディレクトリ指定

チェック時、指定したディレクトリの情報を採取します。

▶ 採取対象のディレクトリを指定します

採取するディレクトリを指定します。

複数指定する場合は、スペース、改行、カンマ(,)のいずれかで区切ってください。

例)

指定したディレクトリ配下の情報を採取

```
/var/log/roma/
```

指定したファイルを採取

```
/var/log/roma/access_log
```

指定した拡張子のファイルを採取

```
/var/log/roma/*.log
```

複数指定して採取

```
/var/log/roma/*.log /var/log/roma/*.txt
```

3.5.25. シリアルポート設定

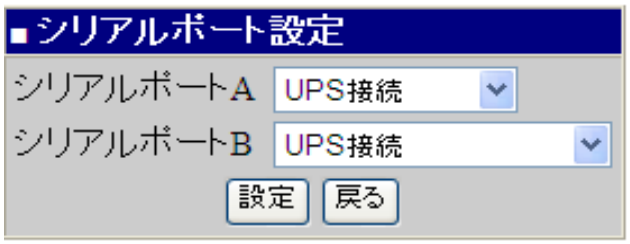
シリアルコンソールに接続するシリアルポートの設定を行います。

シリアル接続の UPS を利用する場合は、コンソールが利用するシリアルポートの設定を[UPS 接続]に設定してください。

シリアルポート経由にてログインする場合は、root アカウントにてログインすることはできません。

シリアルポート経由にてログインする場合は、保守用ユーザのパスワードの設定を行う必要があります。詳細は、「3.5.16. 保守用パスワード」をご確認ください。

なお、「シリアルポート A」と「シリアルポート B」には依存関係はありません。



◆ シリアルポート A

設定値	説明
コンソール接続	シリアルポート接続をコンソール接続に指定します。
UPS 接続	シリアルポート接続を UPS 接続に指定します。

◆ シリアルポート B

設定値	説明
コンソール接続	シリアルポート接続をコンソール接続に指定します。
UPS 接続	シリアルポート接続を UPS 接続に指定します。
ESMPRO コンソール接続	EXPRESSSCOPEエンジン3を利用の場合に選択します。本設定により、リモートコンソール機能の利用が可能となります。

✓ ボタンの説明

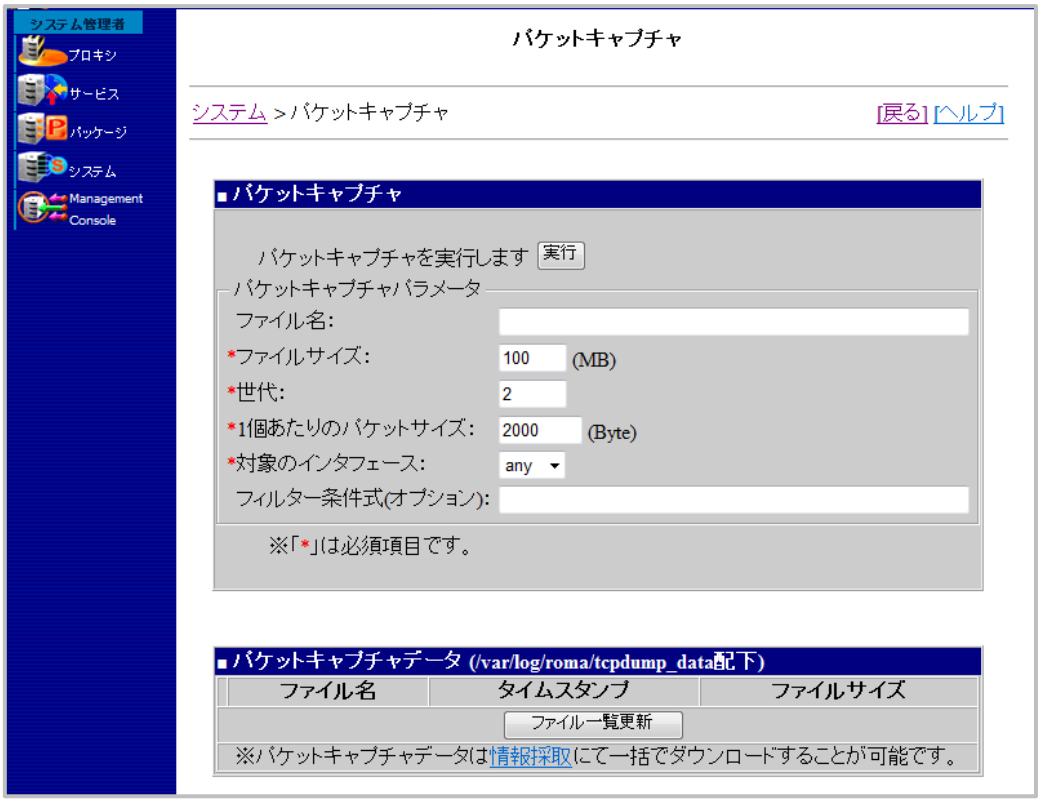
[設定]	指定した内容を設定します。
[戻る]	システム画面に戻ります。→「3.5. システム」

シリアルコンソールに接続する際のパラメータ値

パラメータ	パラメータ値
ボー・レート	19200bps
データ	8bit
パリティ	None
ストップ	1bit
フロー制御	none

3.5.26. パケットキャプチャ

tcpdump コマンドを使用して障害調査に必要なパケットキャプチャを採取します。



パケットキャプチャは以下の画面に分かれています。

■パケットキャプチャ
■パケットキャプチャデータ(/var/log/roma/tcpdump_data 配下)

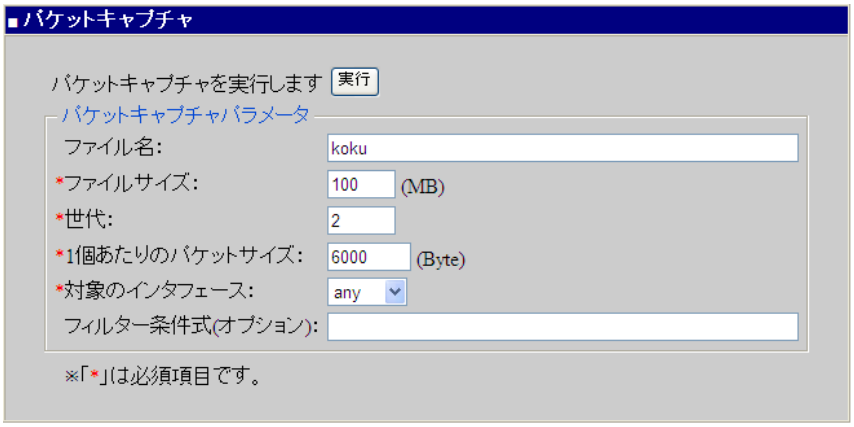
※パケットキャプチャは、実行前と実行後で表示内容が切り替わります。

重要

パケットキャプチャは、本サーバ上の通信パケットデータを取得する機能です。
取得するデータは、暗号化されているパケット以外はデータの内容をすべて参照できます。
採取や採取データの取り扱いについては十分注意してください。

パケットキャプチャ(実行前)

パケットキャプチャの実行前の画面です。



◆ パケットキャプチャを実行します

✓ ボタンの説明

[実行]	パケットキャプチャパラメータで指定した内容で、通信パケットデータの採取を開始します。 [実行]を押下すると「パケットキャプチャを開始します」のダイアログボックスを表示します。  パケットキャプチャを実行する場合は[OK]、実行しない場合は[キャンセル]を押下してください。 [OK]押下した場合は、パケットキャプチャ(実行後)の画面に切り替わります。

◆ パケットキャプチャパラメータ

採取するキャプチャデータのパラメータを指定します。

▶ ファイル名

キャプチャした情報を保存するファイル名を指定します。「ファイル名」を指定した場合、ファイル名は「(指定したファイル名)-(実行開始日時).cap(世代数)」となります。

「ファイル名」を指定しなかった場合、ファイル名は「(実行開始日時).cap(世代数)」となります。

キャプチャしたデータは /var/log/tcpdump_data ディレクトリに保存されます。

▶ ファイルサイズ

ファイル 1 個あたりのサイズの上限を MB 単位で指定します。(1MB = 1,000,000 Byte、デフォルト値：100)

キャプチャサイズがファイルサイズを超えた場合は、ローテートされます。

重要

・最大で「ファイルサイズの上限 * 世代」のディスク容量を使用することになりますので /var/log/roma パーティション を圧迫しないように設定して下さい。
・不要になったキャプチャデータは「削除」ボタンで削除してください。

▶ 世代

ローテートの最大世代数を指定します。2 から 99 まで指定可能です。(デフォルト：2)

▶ １個あたりのパケットサイズ

パケットあたりのキャプチャサイズを指定します。

あまり小さいと 1 パケットすべてを取得出来ない場合がありますので注意してください。デフォルトは、2000 バイトです。

▶ 対象のインタフェース

キャプチャ対象となるインタフェースを指定します。"any" を指定すると全てのインタフェースがキャプチャ対象となります。

重要

・SSL アクセラレータ利用時や二つ以上のインタフェース利用時のパケットをキャプチャする場合は必ず"any"を指定してください。

▶ フィルタ条件式(オプション)

パケットキャプチャフィルタの条件式を指定できます。

何も指定しない場合は、すべてのパケットをキャプチャします。

条件式は、tcpdump コマンドで指定できる条件式の以下の通りです。

条件種別	説明
ホスト名	ホスト名"xxx"に関連する全ての入出力パケットをキャプチャする場合は以下を指定します。 書式:host xxx [xxx はホスト名]
IP アドレス	IP アドレス"xxx.xxx.xxx.xxx"に関連する全ての入出力パケットをキャプチャする場合は、以下を指定します。 書式:host xxx.xxx.xxx.xxx [xxx.xxx.xxx.xxx は IP アドレス]
ホスト名とポート番号	ホスト名"xxx"、SMTP 通信(TCP ポート番号 25 番)で入出力パケットをキャプチャする場合は以下を指定します。 書式:host xxx port 25 [xxx はホスト名]
ホスト名と クライアント端末 あるいは ゲートウェイとの通信	ホスト名"xxx"、クライアントまたはゲートウェイの IP アドレス" yyy.yyy.yyy.yyy" で入出力パケットをキャプチャする場合は以下を指定します。 書式:host xxx and yyy.yyy.yyy.yyy [xxx はホスト名, yyy.yyy.yyy.yyy はクライアントまたは ゲートウェイの IP アドレス]

パケットキャプチャ(実行後)

パケットキャプチャの実行後の画面です。

◆ パケットキャプチャを実行中です(xxx)

表示されている数値(xxx の部分)は、パケットキャプチャ実行中のプロセス ID を示しています。プロセス ID による停止を行わないように注意してください。強制終了された場合は、正常に動作しません。

✓ ボタンの説明

[停止]	通信パケットデータの採取が開始されています。 [停止]を押下することで通信パケットデータの採取を停止し、パケットキャプチャデータに採取した情報を追加します。(「■パケットキャプチャデータ(/var/log/roma/tcpdump_data 配下)」に追加表示します。) パケットキャプチャ(実行前)の画面に切り替わります。

◆ パケットキャプチャパラメータ

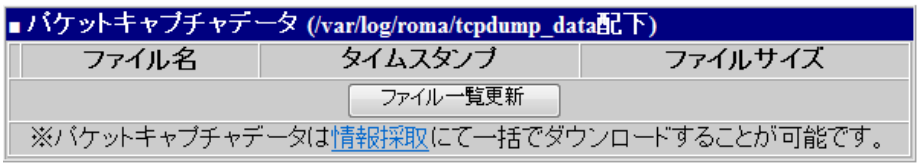
パケットキャプチャの実行前と同じ内容を表示します。

パケットキャプチャ(実行前)の説明を参照ください。

パケットキャプチャデータ(/var/log/roma/tcpdump_data 配下)

採取したパケットキャプチャデータの一覧表示および操作を行います。

キャプチャデータが存在しない場合



キャプチャデータが存在する場合

- ◆ ファイル名

  パケットキャプチャデータのファイル名を表示します。

- ◆ タイムスタンプ

  パケットキャプチャデータのタイムスタンプを表示します。

- ◆ ファイルサイズ

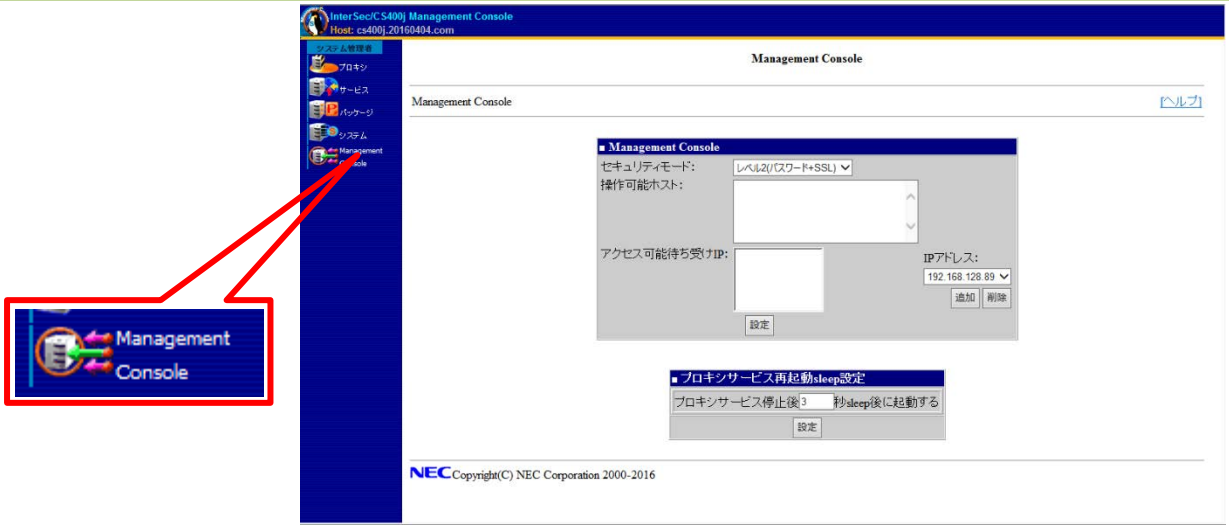
  パケットキャプチャデータのファイルサイズを表示します。

✓ ボタンの説明

[ダウンロード]	チェックしている採取したパケットキャプチャデータをダウンロードします。 表示されたメッセージに従い、ファイルを保存してください。
[ファイル一覧更新]	採取したパケットキャプチャデータの一覧を更新して表示します。 一覧に何も表示されていない場合はこのボタンのみ表示されます。
[削除]	チェックしている採取したパケットキャプチャデータを削除します。
[全削除]	採取したパケットキャプチャデータを全て削除します。

3.6. Management Console

Management Console



◆ セキュリティモード

Management Console を用いる際のセキュリティレベルを指定します。

設定値	説明
レベル 2(パスワード+SSL)	パスワード認証に加えて、パスワードや設定情報を SSL で暗号化して送受信します。このモードを用いる際は、http://xxx.xxx.xxx.xxx:50090/の代わりに https:// xxx.xxx.xxx.xxx:50453/ のアドレスでアクセスする必要があります。自己署名証明書を用いていますので、ブラウザでアクセスする際に警告ダイアログが表示されますが、[はい]を選択してください。
レベル 1(パスワード)	パスワード認証による利用者チェックを行います。 ただし、パスワードや設定情報は暗号化されません。(通常の TELNET による設定と同レベルのセキュリティです。)

◆ 操作可能ホスト

Management Console を使用可能なホストを限定する場合、そのアドレスを指定します。

・複数指定する場合は、半角スペースで区切って指定してください。
・IPv4 アドレスの場合は 192.168.1.1 の形式、192.168.1.0/24 の形式、192.168.1.0/255.255.255.0 の形式を使用できます。
・IPv6 アドレスの場合は「IP アドレス」のみか「IP アドレス/プレフィックス」の形式が使用できます。
・IP アドレスは[]で括らずに設定を行ってください。
・アルファベットは小文字のみ使用可能です。

ここで、適切なアドレスを指定しないと、Management Console にアクセスできなくなります。操作可能ホストを指定する場合は十分注意してください。

◆ アクセス可能待ち受け IP

Management Console にアクセス可能な本サーバへ登録されている IP アドレスを指定します。これにより、許可されていない IP アドレスを指定して Management Console へアクセスしようとしても、そのアクセスを拒否することが可能となります。アクセス可能待ち受け IP になにも登録されていない場合は、どの IP アドレスの Management Console へのアクセスも許可されます。

「IP アドレス」から追加登録したい IP アドレスを選択し[追加]押下します。

削除する場合は、削除したい IP アドレスを選択し[削除]押下します。

▶ IP アドレス

待ち受け可能な IP アドレスが選択可能となっています。

IP アドレスを選択し[追加]押下で、アクセス可能待ち受け IP に追加します。

✓ ボタンの説明

[追加]	入力した値の追加を行います。追加後、[設定]を押下することで内容を反映します。
[削除]	選択した設定の削除を行います。削除後、[設定]を押下することで内容を反映します。

✓ ボタンの説明

[設定]	入力した内容を設定し、内容を反映させます。

設定をした場合、設定内容を有効にするために Management Console のサーバを再起動します。すぐに再接続を行いたい場合は数秒待ってから接続してください。

プロキシサービス再起動 sleep 設定

◆ プロキシサービス停止後 xx 秒 sleep 後に起動する

プロキシサービスの再起動時にプロキシサービスの停止後、指定した時間 sleep した後、プロキシサービスを起動します。 デフォルトは「3 秒」です。

0～15 秒まで指定可能です。

各画面の赤字の[設定]ボタンを押下時にプロキシサービスの再起動を行います。

4章 トラブルシューティング

トラブルに当てはまる項目があるときは、その後の確認、処置に従ってください。
それでも正常に動作しない場合はサポートサービスをご利用ください。

4.1. 初期導入時

- **システム起動直後に、システムが停止**

  ほとんどの場合の原因は、パスワードの入力ミスが多いため、指定内容を確認してください。

- **Management Console が使用できない**

  InterSec/CS の起動には、数分かかります。念のため 5 分位経過してから、もう一度アクセスしてみてください。

4.2. 導入完了後

- **Management Console にアクセスできない**

・設定したアドレスが間違っていないことを確認してください。
・「3.1.2. 動作環境」の環境となっていることを確認してください。
・Management Console をアクセスする URL が間違っていないことを確認してください。
Management Console のセキュリティモードを変更した場合、アクセスする URL が変更されますので注意してください。
セキュリティモードを変更していない場合は、URL は「https://～」となっているか確認してください。
特に「https」の最後の「s」を入力しているか確認してください。
・Management Console へアクセスする URL(ポート番号)が間違っていないことを確認してください。
＜セキュリティモードが[レベル 2（パスワード+SSL）]の場合＞
https://<サーバの IP アドレスまたは FQDN>:50453/
＜セキュリティモードが[レベル 1（パスワード）]の場合＞
https://<サーバの IP アドレスまたは FQDN>:50090/
なお、ファイアウォール機器などを経由して接続する場合は、ポートの通過許可を行ってください。
・URL に、IP アドレスを使用してアクセスしてみてください。IP アドレスを使用したアクセスが成功する場合は、DNS の設定が誤っている可能性があります。設定を確認してください。
・Management Console の操作可能ホストを指定していないかどうか確認してください。操作可能ホストを指定している場合、Management Console を使用できるマシンは限定されます。

上記で問題が解決しない場合は、以下の手順で、ネットワーク接続を確認してください。

1) Windows マシンで MS-DOS(またはコマンドプロンプト)を起動する。
2) "ping ip-address"コマンドを実行する。(ip-address は、本製品に割り当てた IP アドレスです)
3) "Reply from ..."と表示される場合、ネットワークは正常です。この場合、仮想環境側より、システムの停止・起動処理を実行してください。起動後にもう一度アクセスしてみてください。
4) "Request timed out"と表示される場合、接続の確認は失敗です。続けて、他のマシンからも ping コマンドを実行してみてください。
一部のマシンから ping コマンドが失敗する場合は、失敗するマシンの設定の誤り、または故障です。
すべてのマシンから ping コマンドが失敗する場合は、仮想環境や HUB 装置などのネットワーク機器の設定を確認してください。ケーブルが外れていたり、電源が入っていなかったりすることがあります。ネットワーク機器の設定が誤っていない場合は、ネットワーク障害の可能性があります。

- **Management Console のログイン認証に失敗する(Authorization Required)**

  ・ユーザ ID を確認してください。管理者権限で Management Console を使用する時のユーザ ID の初期値は、admin(すべて小文字)です。
  ・初期導入設定において設定したパスワードを確認してください。パスワードの大文字と小文字は区別されるので注意してください。
  ・Management Console よりユーザ ID とパスワードの変更を行ったか確認してください。変更している場合は、変更したユーザ ID とパスワードでログインしてください。

- **Management Console 画面が文字化けする**

  ・ご使用のブラウザの文字コードのエンコード設定を確認してください。
  Management Console 画面の文字コードは、UTP-8 を使用しています。ブラウザのエンコードの設定を UTP-8 または自動判別にして確認してください。

- **サービスの応答が非常に遅い**

  ・Management Console を使用して、ディスクの使用状況を確認してください。いずれかのディスク使用率が、90%を超えている場合、不要なファイルの削除、「3.5.12. ログ管理」からログファイルの削減などの対処を行なってください。
  ・Management Console を使用して、ネットワークの利用状況を確認してください。正常の値に対して、異常/破棄/超過のいずれかが 10%を超える場合は、ネットワークに異常が発生していないかなどの確認を行なってください。

- **ブラウザから設定した変更内容に更新されない**

  設定の変更後、[適用]ボタン押下が必要です。[適用]ボタンを押下しているか確認してください。

- **OS のシステムエラーが発生**

  システムにアクセスできず、本製品のディスクアクセスが長く続く場合はシステムエラー(パニック)が発生している可能性があります。 パニック発生時にはダンプが採取され、その後自動的にシステムが再起動されます。
  システムエラーの障害調査には/var/crash 配下のファイルすべてと/var/log/messages ファイルを採取する必要があります。
  管理 PC(コンソール)から障害発生サーバにログインし、障害発生サーバから FTP で情報を採取し、サポートサービスへお問い合わせください。
  /var/crash 配下のファイルは、システムエラー(パニック)が発生するたび、自動的に更新されます。事前に削除したい場合は、/var/crash 配下の 127.0.0.1 で始まるディレクトリ毎削除してください。(他のファイルは削除しないでください)

5章 注意事項

5.1. Management Console 利用時の注意事項

- Management Console へ、複数ユーザが同時に接続し、操作を行って設定を行うと、設定ファイルが他でログインしたユーザの設定情報で上書きされるため、正常に設定が反映されない場合があります。
- Management Console の操作中に、ブラウザの[戻る]ボタンの操作を行った場合、表示されるデータが不正になったり、設定操作を行った情報が不正になる場合があります。
- Internet Explorer でショートカットキー操作による画面表示に関する操作を行うと表示が乱れることがあります。

  ・Ctrl +マウスのホイールを↓(画面の表示を縮小)
  ・Ctrl +マウスのホイールを↑(画面の表示を拡大)
- Internet Explorer で JavaScript を無効にしないでください。
  JavaScript を無効化した場合、設定操作行っても正しく動作しないため設定情報が不正になる場合があります。
- 設定動作を行うボタンをクリックした時は、結果画面が表示されるまで同様の操作(ボタンの連続押下)を行わないでください。設定情報が不正になる場合があります。
- Management Console 画面の文字コードは、UTF-8 を使用しています。ブラウザの文字エンコード設定によっては、文字化けが発生することがありますので、ブラウザの文字エンコード設定は UTF-8 が認識できるように指定してください。
- Windows Server 2008 以降の Internet Explorer ではセキュリティが強化されており、既定の設定では幾つかの Management Console の操作が正常に動作しません。
  このため、クライアント系の Windows をご利用頂くか、以下の設定変更にて使用してください。
  Internet Explorer の[ツール]-[インターネットオプション]-[セキュリティ]タブにある「レベルのカスタマイズ」をクリックし、「スクリプトレットの許可」を「有効にする」にチェックする。

5.2. 機能に関する注意事項

- 「3.5.17. バックアップ/リストア」で「システムの設定ファイル」のバックアップ/リストアにおいて、サービス(ネットワーク管理エージェント)の OS 起動時の状態が、正しくリストアできない場合があります。
  リストア実施後に、各サービスの起動状態を再確認してください。

6章 用語集

- **DHCP(Dynamic Host ConfigurationProtocol)**
  インターネットに一時的に接続するコンピュータに対し、IP アドレスなど必要な情報を自動的に割り当てるプロトコルです。DHCP サーバには、ゲートウェイサーバや DNS サーバの IP アドレスや、サブネットマスク、クライアントに割り当ててもよい IP アドレスの範囲などが設定されており、アクセスしてきたコンピュータにこれらの情報を提供することができます。
- **Management Console**
  Web ブラウザを利用した本製品のシステム設定ツールの名称です。Web-based Management Console の略称として WbMC と表記することもあります。
- **SNMP(ネットワーク管理エージェント)**
  NEC の ESMPRO シリーズや SystemScope シリーズなどの管理マネージャソフトから、本サーバを管理する際に必要となるエージェントソフトです。管理マネージャからの情報取得要求に応えたり、トラップメッセージを管理マネージャに送信します。
- **NTP(時刻調整)**
  ネットワークから協定世界時(UTC)を受信して、システム時刻の設定・維持を行うプロトコルです。
- **グローバルアドレス**
  インターネットに接続された機器に一意に割り当てられた IP アドレスです。インターネットの中での住所にあたり、インターネット上で通信を行うためには必ず必要です。IANA が一元的に管理しており、JPNIC などによって各組織に割り当てられます。
- **プライベートアドレス**
  グローバルアドレスを使用するには JPNIC などへの申請が必要ですが、組織内に閉じて使用することを条件に、無申請で利用可能な IP アドレスです。以下の範囲がプライベートアドレスとして定められています。

  ・10.0.0.0 ～ 10.255.255.255
  ・172.16.0.0 ～ 172.31.255.255
  ・192.168.0.0 ～ 192.168.255.255
- **FQDN(Fully Qualified Domain Name)**
  TCP/IP ネットワーク上で、ドメイン名やサブドメイン名、ホスト名を省略せずにすべて指定した記述形式のことです。
- **IP(Internet Protocol)**
  ネットワーク間でのデータの中継経路を決定するためのプロトコルです。通信プロトコルの体系において、TCP と IP は非常に重要なので、これら二つを合わせて TCP/IP とも呼ばれます。

- **IP(Internet Protocol)アドレス**
  TCP/IP 通信においてネットワーク上の各端末の位置を特定するために使用される 32 ビットのアドレスです。通常は 8 ビットずつ 4 つに区切って 0～255.0 ～255.0～255.0～255 という 10 進数の数字列で表される。
  例)130.158.60.5
- **SSL(Secure Socket Layer)**
  Web サーバが信頼できるかの認証を行ったり、Web ブラウザのフォームから送信する情報を暗号化するために用いられる技術です。SSL を用いるには、Web サーバに秘密鍵と証明書を設定する必要があります。証明書はベリサインなどの認証局に署名してもらうものと、自己署名のものがありますが、前者を用いるとサーバ認証と暗号化が、後者を用いると暗号化のみが有効になります。

The BSD Copyright

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it toyour programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:(1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope.The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program(independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program,and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.(Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from

the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program(or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License.
Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions.
You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.
If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted

interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different,write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation,write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>
> Copyright (C) 19yy <name of author>
>
> This program is free software; you can redistribute it and/or modify
> it under the terms of the GNU General Public License as published by
> the Free Software Foundation; either version 2 of the License, or
> (at your option) any later version.
>
> This program is distributed in the hope that it will be useful,
> but WITHOUT ANY WARRANTY; without even the implied warranty of
> MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
> GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License
> along with this program; if not, write to the Free Software
> Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

> Gnomovision version 69, Copyright (C) 19yy name of author
> Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
> This is free software, and you are welcome to redistribute it
> under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version,so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder.

Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library,so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files,plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of

any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the

copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler,kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any

other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions.You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANYKIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY

TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the library's name and a brief idea of what it does.>
> Copyright (C) <year> <name of author>
>
> This library is free software; you can redistribute it and/or
> modify it under the terms of the GNU Lesser General Public
> License as published by the Free Software Foundation; either
> version 2.1 of the License, or (at your option) any later version.
>
> This library is distributed in the hope that it will be useful,
> but WITHOUT ANY WARRANTY; without even the implied warranty of
> MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
> Lesser General Public License for more details.
>
> You should have received a copy of the GNU Lesser General Public
> License along with this library; if not, write to the Free Software
> Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option

4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your

reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying

under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate,

modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>
> Copyright (C) <year> <name of author>
>
> This program is free software: you can redistribute it and/or modify
> it under the terms of the GNU General Public License as published by
> the Free Software Foundation, either version 3 of the License, or
> (at your option) any later version.
>
> This program is distributed in the hope that it will be useful,
> but WITHOUT ANY WARRANTY; without even the implied warranty of
> MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
> GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License
> along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

> <program> Copyright (C) <year> <name of author>
> This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
> This is free software, and you are welcome to redistribute it
> under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an “about box”.

You should also get your employer (if you work as a programmer) or school, if any, to sign a “copyright disclaimer” for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

■　謝辞

LinusTorvalds 氏をはじめとする Linux に関わるすべての皆様に心より感謝いたします。

NEC
InterSec/CS400k
ユーザーズガイド

2017 年 8 月 第 1 版
日 本 電 気 株 式 会 社
東京都港区芝五丁目 7 番 1 号
TEL(03)3454-1111(大代表)