Trend Micro InterScan WebManager™

管理者ガイド

TREND MICRO™

Securing Your Connected World

■ 著作権

■マニュアルの構成

● クイックスタートガイド

クイックスタートガイドでは、Trend Micro InterScan WebManager で Web フィルタリングを行うための基本的な設定と、運用の流れについて説明しています。

Trend Micro InterScan WebManager を初めて導入するときにお読みください。

● 管理者ガイド (本書)

管理者ガイドでは、Trend Micro InterScan WebManager で設定できるさまざまなフィルタリング機能の設定について詳しく説明しています。

また、Linux 版のシステム構築・設定、LDAP 認証サーバとの連携方法など大規模なシステムでの運用方法についても説明しています。

Trend Micro InterScan WebManager の運用形態に応じて、必要項目を参照してください。

■ マニュアルに掲載している画面

マニュアルでは、スタンドアロン版のシステム管理者用の管理画面を例に説明しています。
表示された画面が、マニュアルに掲載されている画面と異なる場合は、実際の画面に従って操作してください。
画面は、改善のため予告なく変更することがあります。

目次

インストールと使用の準備

1. システム運用までの流れ

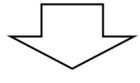
Trend Micro InterScan WebManager(以下、ISWM)の基本的なフィルタリングサービスを利用するには、次の手順に従って製品をインストール、設定してください。

注意: [設定情報管理]-[保存 / 復旧 / 同期]-[レプリカサーバ同期] で、[設定変更時に自動で同期を行う] チェックボックスをオンにしている場合は、設定変更の際、プライマリサーバとレプリカサーバは常に同期を取るため、システムの規模によってはネットワークの負荷が高くなります。複数のレプリカサーバを登録して運用する場合は、レプリカサーバを登録する前に、プライマリサーバの設定やグループ / ユーザの登録、フィルタリングルールの設定を完了してください。

1-1. 基本的な運用

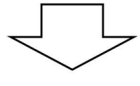
1. ISWMのインストール

ISWM を運用するサーバに、ISWM をインストールします。
インストール方法は、お使いになる OS やネットワークの構成によって異なります。
インストールの手順→「第 1 章 インストールと使用の準備」(1 ページ)



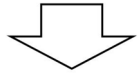
2. 連携するICAPクライアントの設定(ICAP版のみ)

ISWM と連携して動作する ICAP クライアントの設定をします。
スタンドアロン版では、設定する必要はありません。
ICAP 版の場合→「5. ICAP クライアントの設定」(14 ページ)



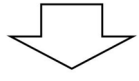
3. データベースのダウンロード

管理画面にログインし、データベースをダウンロードします。
管理画面へのログイン→「8. 管理画面へのログイン / ログアウト」(32 ページ)
データベースのダウンロード→「1-2. データベースのダウンロード」(40 ページ)



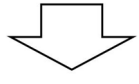
4. レプリカサーバの登録(複数サーバで運用する場合のみ)

管理画面にログインし、プライマリサーバに、連携するレプリカサーバを登録します。
管理画面へのログイン→「8. 管理画面へのログイン / ログアウト」(32 ページ)
レプリカサーバの登録→「2-3. 新規レプリカサーバを登録する」(43 ページ)



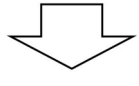
5. サーバの設定

ISWM をインストールしたプライマリサーバの設定をします。
ご利用になるネットワーク環境にあわせて、フィルタリングするリクエストのポート番号や、上位プロキシサーバなどの設定をします。
サーバの設定→「第 2 章 サーバの設定と管理」(40 ページ)



6. グループとユーザの登録

ISWM でフィルタリングするユーザとグループを登録します。
複数のグループでフィルタリングする場合、ユーザ認証の設定が必要になります。
グループとユーザの管理→「第 3 章 グループとユーザの管理」(111 ページ)
ユーザ認証の設定→「5. ユーザ認証 /LDAP の設定」(60 ページ)



7. フィルタリングの設定

ISWM のフィルタリング設定をします。
フィルタリングの設定→「第 4 章 フィルタリングの設定」(158 ページ)

注意: HTTPS 規制をサーバデコード方式で使用する場合、認証コードが必要になります。詳細については、「2-1. HTTPS 規制の設定」(180 ページ)を参照してください。

以上で、基本的な運用設定は完了です。

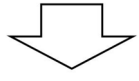
2. インストールの流れ

ISWMはご利用になるネットワーク環境や、サーバOSによってインストール手順が異なります。
旧バージョンのISWMからバージョンアップする場合、「F. バージョンアップインストールについて」(484ページ)を参照してください。

2-1. Windowsサーバへのインストール

1. プライマリサーバにISWMをインストールする

ISWM のシステム設定やグループ / ユーザの管理、フィルタリングの設定をするプライマリサーバに、ISWM をインストールします。
詳しくは、「3. Windows へのインストール」(7 ページ)を参照してください。



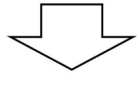
2. レプリカサーバに ISWM をインストールする (複数サーバで運用する場合のみ)

複数のサーバでフィルタリングサービスの負荷を分散して運用する場合は、負荷分散用のサーバにも ISWM をインストールします。
レプリカサーバへインストールする場合はインストール画面でインストールタイプをレプリカサーバに設定し、インストール完了後に管理画面でプライマリサーバに登録してください。

2-2. Linux サーバへのインストール

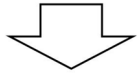
1. プライマリサーバにISWMをインストールする

ISWM のシステム設定やグループ / ユーザの管理、フィルタリングの設定をするプライマリサーバに、ISWM をインストールします。
詳しくは、「4. Linux へのインストール (スタンドアロン版、ICAP 版)」(10 ページ)を参照してください。



2. ICAPクライアントの設定をする(ICAP版のみ)

「5. ICAP クライアントの設定」(14 ページ)を参照して ICAP クライアントの設定をしてください。



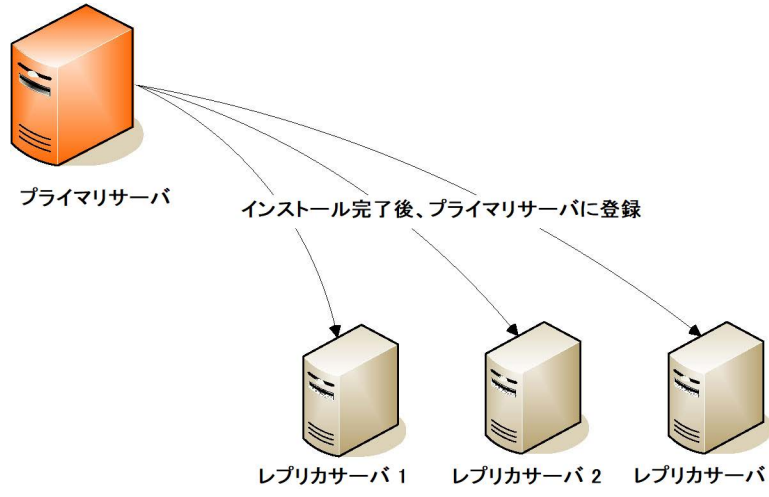
3. レプリカサーバに ISWM をインストールする (複数サーバで運用する場合のみ)

複数のサーバでフィルタリングサービスの負荷を分散して運用する場合は、負荷分散用のサーバにも ISWM をインストールします。
レプリカサーバへインストールする場合はインストール画面でインストールタイプをレプリカサーバに設定し、インストール完了後に管理画面でプライマリサーバに登録してください。

2-3. 複数サーバでの負荷分散運用

ISWMでは複数のサーバを1台のプライマリサーバで管理します。プライマリサーバとしてインストールするか、レプリカサーバとしてインストールするかは、インストール中に選択します。
インストール直後の状態では、レプリカサーバは、プライマリサーバと関連付けられていません。
プライマリサーバの設定完了後に、必ずISWMの管理画面からレプリカサーバの登録をしてください。

サーバ構成例



注意:
- プライマリサーバとすべてのレプリカサーバは、同一の OS・バージョンで運用してください。
- インストール完了後は、サーバ種別 (プライマリサーバ、レプリカサーバ) と、インストール時に選択した IP アドレスの変更はできません。変更する場合は、再インストールが必要です。
- 管理画面は、サーバタイプをプライマリサーバとしてインストールしたサーバで提供されます。レプリカサーバでは提供されません。

3. Windowsへのインストール

インストールに必要なシステム要件は、製品付属のReadmeを参照してください。
WindowsサーバへISWMをインストールする場合は、次の手順でインストールしてください。

注意:
- インストール作業前に、すべてのアプリケーションを終了してください。
- すでに旧バージョンの ISWM をお使いの場合、設定を引き継いでバージョンアップインストールします。
  万が一の場合に備えて、以下のフォルダにある設定ファイルをバックアップしてください。
  ＜インストールフォルダ＞ ¥conf
  バージョンアップインストールについては、「F. バージョンアップインストールについて」(484 ページ)を参照してください。

1. インストールを実行するコンピュータに、管理者権限を持つログインユーザでログインします。
2. インストールメディアを挿入し、セットアッププログラム「setup.exe」を実行します。

   セットアッププログラムは、< インストールメディア >¥program¥windows¥ にあります。インストール開始画面が表示されます。
3. [次へ] ボタンをクリックします。

   使用許諾契約画面が表示されます。
4. [使用許諾契約の条項に同意する] をクリックして選択し、[次へ] ボタンをクリックします。

   使用許諾契約の内容に同意いただけない場合は、[使用許諾契約の条項に同意しない] をクリックしてインストールを中止してください。
5. インストールするフォルダを確認して [次へ] ボタンをクリックします。

   インストールが開始されます。
   初期設定では、Windows がインストールされているドライブ (通常は C ドライブ) の「ISWM」フォルダにインストールされます。インストール先フォルダを変更する場合は [選択] ボタンをクリックしてインストール先フォルダを変更してください。

注意:
- 旧バージョンの ISWM の設定ファイルを引き継ぎたい場合は、旧バージョンがインストールされていたフォルダにインストールしてください。
- フォルダ名は半角英数字、'_'、'-' のみを使用してください。また、フォルダ名全体の長さが 128 文字を超えないようにしてください。

6. インストールタイプをクリックして選択し、[次へ] ボタンをクリックします。

注意: ここで選択したサーバのインストールタイプは後から変更できません。変更する場合は、再インストールが必要になります。プライマリサーバ、レプリカサーバについては、「2. インストールの流れ」(4 ページ) を参照してください。

7. 利用するサーバの IP アドレスを選択して [次へ] ボタンをクリックします。

インストール設定の内容が表示されます。

注意:
- レプリカサーバの場合、IP アドレスの選択手順はありません。次の手順へ進んでください。
- サーバの IP アドレスが複数設定されている場合、ISWM として利用する IP アドレスを選択してください。初期値で使用する場合、そのまま次の手順へ進んでください。

8. [インストール] ボタンをクリックします。

インストールが始まります。
インストールが完了するとインストール完了の画面が表示されます。

9. [次へ] ボタンをクリックします。

OS パラメータの最適化を確認する画面が表示されます。

10. [はい] をクリックして選択し、[次へ] ボタンをクリックします。

設定が完了すると、メッセージが表示されます。

11. [次へ] ボタンをクリックします。

再起動を促すメッセージが表示されます。

12. [システムを再起動する] をクリックして選択し、[次へ] ボタンをクリックします。

再起動すると ISWM のサービスが有効になり、ISWM のサービスが自動的に開始されます。

注意: OSパラメータの最適化を実行しなかった場合、コマンドラインからサーバのチューニングを実行できます。「A-22. amstune[サーバのチューニング]」(437ページ)を参照してください。

以上で、ISWMのインストールは完了です。

4. Linuxへのインストール(スタンドアロン版、ICAP版)

インストールに必要なシステム要件は、製品付属のReadmeを参照してください。
Linuxサーバへ ISWM(スタンドアロン版またはICAP版)をインストールする場合は、次の手順でインストールしてください。
ICAP版の場合は、インストールが完了したら、続けて「5. ICAPクライアントの設定」(14ページ)を参照して、お使いになるICAPクライアントを設定してください。

注意:
- インストール作業前に、すべてのアプリケーションを終了してください。
- すでに旧バージョンの ISWM をお使いの場合、設定を引き継いでバージョンアップインストールします。万が一の場合に備えて、以下のフォルダにある設定ファイルをバックアップしてください。
  <インストールディレクトリ> /conf
  バージョンアップインストールについては、「F. バージョンアップインストールについて」(484 ページ)を参照してください。
- ISWM を実行する環境には、日本語環境が必要です。日本語表示可能なコンソール、またはウィンドウシステムを使用してください。

1. インストールメディアをマウントし、解凍後セットアッププログラム「setup.sh」を実行します。

インストーラのイントロダクションが表示されます。
セットアッププログラムは以下のフォルダにあります。
- <インストールメディア >/program/linux/

注意:
- インストールは root ユーザで実行してください。
- インストールは、コマンドラインで実行してください。
- インストール中に ISWM に IP アドレスを設定するため、ネットワークサービスが起動している必要があります。ネットワークサービスを起動してからインストールを実行してください。
- back と入力して <Enter> を押すと、1 つ前の手順に戻ります。また、quit と入力して <Enter> を押すと、インストールプログラムを終了することができます。

2. インストーラのイントロダクションが表示された後、<Enter> を押してインストール作業を続行します。

使用許諾契約が表示されます。

3. 「Y」を入力して <Enter> を押します。使用許諾契約の内容に同意いただけない場合は、「N」を入力してインストールを中止してください。

注意: 使用許諾契約の内容は日本語で表示されます。日本語の設定がされていない場合、使用許諾契約の内容を表示することができません。

4. インストールディレクトリを指定し、<Enter> を押します。

```
Only normal-width Alphanumeric character and '_' or '-' are allowed to use as install folder name.
Whole folder path's length is restricted within 128 characters.

Select install folder. Where Would You Like to Install?
Default Install Folder: /usr/local/iswm
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

初期設定では、次のディレクトリにインストールされます。インストールディレクトリを変更する場合は、絶対パスで入力して <Enter> を押してください。

- /usr/local/iswm

5. スタンドアロン版をインストールする場合は「1」、ICAP 版をインストールする場合は「2」と入力して <Enter> を押します。

```
Please Choose the Install Set to be installed by this installer.
->  1- Standalone
    2- ICAP
ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

6. サーバのインストールタイプを選択し、<Enter> を押します。

ISWM をインストールするサーバをプライマリサーバとして動作させるか、レプリカサーバとして動作させるかを決定します。「1」(プライマリサーバ) または「2」(レプリカサーバ) を入力して <Enter> を押してください。

```
Please select server type
->  1- Primary Server
    2- Replica Server
ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

注意: ここで選択したサーバのインストールタイプは後から変更できません。変更する場合は、再インストールが必要になります。プライマリサーバ、レプリカサーバについては「2. インストールの流れ」(4 ページ)を参照してください。

7. ISWM をインストールするサーバの IP アドレスを選択して <Enter> を押します。

IP アドレスを確認するメッセージが表示されます。

```
Please select the IP address which it utilizes as Primary
-> 1- 192.168.11.108
ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

注意:
- レプリカサーバの場合、IP アドレスの選択手順はありません。次の手順へ進んでください。
- サーバの IP アドレスが複数設定されている場合、ISWM として利用する IP アドレスを数値で指定して <Enter> を押してください。初期値で使用する場合、そのまま <Enter> を押してください。

8. 確認のメッセージが表示されるので、「Y」を入力して <Enter> を押します。

ISWM の設定を確認するメッセージが表示されます。

9. ISWM 実行ユーザを自動設定するか選択し、<Enter> を押します。

ユーザとグループの設定が表示されます。

```
When automatic setting is selected, the iswm group and the iswm user are drawn up
->  1- Automatic setting
    2- Manual setting
ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

10. ユーザとグループの設定が正しいか確認し、<Enter> を押します。

ISWM の起動設定を確認するメッセージが表示されます。

```
The owner is set in the user and the group below
User:iswm
Group:iswm
PRESS <ENTER> TO CONTINUE:
```

11. ISWM を自動起動するか選択して <Enter> を押します。

インストール設定内容が表示されます。

```
-> 1- Automatic start registers
   2- Automatic start does not register
ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT DEFAULT:
```

注意: ISWM の自動起動を設定した場合、コンピュータが起動すると自動的に ISWM のサービスが起動します。

12. ISWM のインストール設定内容を確認します。

<Enter> を押すと ISWM のインストールが始まります。ISWM のインストールが完了すると、OS パラメータの最適化を確認するメッセージが表示されます。

注意: コマンドプロンプトに戻る前に <Ctrl>+<C> を押してインストール処理を中断しないでください。

13. 「1」を入力して <Enter> を押します。

設定が完了すると、ISWM サービスの起動を促すメッセージが表示されます。

14. 「1」を入力して <Enter> を押します。

ISWM のサービスが自動的に開始されます。

注意: OSパラメータの最適化を実行しなかった場合、コマンドラインからサーバのチューニングを実行できます。「A-22. amstune[サーバのチューニング]」(437ページ) を参照してください。

以上で、ISWMのインストールは完了です。

5. ICAPクライアントの設定

ICAP 版をご利用になる場合、ICAP クライアントと連携する設定が必要になります。ご利用の環境にあわせて設定をしてください。
各ICAPクライアントの詳細説明ページについては、次の表を参照してください。。

5-1. BlueCoatとの連携

ICAPクライアントとしてBlueCoatを利用する場合、ICAPサービスファームの登録とポリシーの設定を行ってください。

注意: ISWM を BlueCoat と連携させて動作させるために BlueCoat 側で必要な設定をします。詳しくは BlueCoat のマニュアルを参照してください。

■ 管理画面へのログイン

次の手順でBlueCoat管理画面にログインしてください。
ここでは、BlueCoat SGOS 6.7.4.10の場合を例に説明します。

1. ブラウザから https://<bluecoat-server>:<bluecoat-adminport>/ にアクセスします。

   <bluecoat-server> : BlueCoat 稼動サーバ名 /IP アドレス
   <bluecoat-adminport>: BlueCoat 管理画面用ポート番号 (初期設定では 8082)
   WWW 認証ダイアログが表示されます。

2. BlueCoat 管理者アカウント、パスワードを入力して [OK] ボタンをクリックします。

   BlueCoat 管理画面が表示されます。

続けてICAPサービスファームの設定をします。

■ ICAP サービスファームの登録

ISWMとの連携のためにICAPサービスの登録、ポリシーの設定を行います。ICAPサービスを登録

するには、次の手順に従ってください。

1. [Configuration] タブを選択し、画面左のメニューの [Content Analysis]-[ICAP] をクリックします。

   ICAP サービスの設定画面が表示されます。

2. [ICAP Services] タブを選択し、[New] ボタンをクリックします。

   「サービス登録用」ダイアログが表示されます。

3. 登録するサービス名を入力して [OK] ボタンをクリックします。

   ICAP サービスが一覧に登録されます。
   複数の ICAP サーバを使用する場合には、使用するサーバごとにサービスを登録してください。

4. 登録されたサービスを一覧から選択し、[Edit] ボタンをクリックします。

   ICAP サービス設定ダイアログが表示されます。

5. 次の項目を設定します。

ICAP version	1.0
Service URL	環境にあわせて IP アドレス、ホスト名、ICAP ポート番号を指定します。 記入例） icap://<ISWM-Server>:<ICAP-Port>/ <ISWM-Server>: ISWM ICAP版を導入しているサーバの IP アドレス / ホスト名 <ICAP-Port>: LISTEN している ICAP ポート番号
Maximum number of connections	設定変更不要です。初期値は 5 ですが、ISWM と連携時に、「ISWM のプロセス数」の二分の一が自動的に設定されます。ISWM のプロセス数は、設定ファイル（proxy.inf）の [CONTROL_CFG] セクションの SERVER_PROCESS キーで設定します。
Connection timeout(seconds)	70
Method supported	request modification
Health Checks Options	ISWM の状態監視を実施します。

注意: [Sense settings]ボタンをクリックするとICAPサーバとの接続を確認し、ICAPサーバに適合した設定へ変更できます。

6. [OK] ボタンをクリックしてサービスの設定を BlueCoat に保存します。
7. [Apply] ボタンをクリックして BlueCoat に設定を反映します。

注意: [Apply] ボタンをクリックしないと設定は反映されません。必ず [Apply] ボタンをクリックしてください。

続けてポリシーの設定をします。

■ ポリシーの設定

1. 画面左のメニューの [Policy]-[Visual Policy Manager] をクリックします。
   Policy サービスの登録画面が表示されます。
2. [Visual Policy Manager] タブを選択し、[Launch Legacy Java VPM] ボタンをクリックします。
   Visual Policy Manager 画面が表示されます。
3. メニューバーの [Policy] をクリックし、表示されるプルダウンメニューから [Add Web Access Layer] をクリックします。
4. レイヤー名を入力し、[OK] ボタンをクリックします。
   レイヤーが追加されます。
5. 追加されたレイヤーの [Action] のセルを右クリックし、[Set] をクリックします。
   [Set Action Object] ダイアログが表示されます。
6. [New...] ボタンをクリックし、[Set ICAP Request Service...] をクリックします。
   [ADD ICAP Request Service Object] ダイアログボックスが表示されます。
7. 次の項目を設定し、[OK] ボタンをクリックします。
   - Use ICAP request service: 登録した ICAP サービスを選択
   - Error handling: [Deny the client request] を選択

   [Action] 一覧に ICAP サービスが追加されます。

8. [Set Action Object] に追加された ICAP サービスを選択し、[OK] ボタンをクリックします。

   ポリシーの Action が有効になります。

9. [Install Policy] ボタンをクリックします。

   Visual Policy Manager で設定したポリシー設定が BlueCoat に反映されます。

以上で、ISWMとBlueCoatのICAP連携の設定は完了です。

■ HTTPS デコードを行う場合

BlueCoatと連携した上でHTTPSデコードを行うには、BlueCoatのSSL Proxy機能を有効にします。

注意: 詳しくは BlueCoat の Web サイトを参照してください。

1. ICAP クライアントの動作により、HTTPS デコードの前と後で 2 段階のフィルタリング判定が行われる場合があります。デコード前の判定 (ドメイン単位) をスキップし、デコード後の判定 (ディレクトリ / ファイル単位) を優先するには、以下の設定を追加してください。

   BlueCoat の管理画面にアクセスし、Service URL を「icap://<ISWM-Server>:<ICAP-Port>/skip_connect_reqmod」として新しい ICAP サービスファームを追加します。デコード前の判定をスキップしたいリクエストは、この ICAP サービスへ転送するようにポリシーを設定してください。

2. ISWM の設定ファイル proxy.inf の [CONTROL_CFG] セクションの ICAP_CLIENT_TYPE キーに「BLUECOAT」を設定します。

   ファイルの保存場所

   Linux 版＜インストールディレクトリ >/conf/proxy.inf

   ICAP_CLIENT_TYPE キーに「BLUECOAT」を設定した場合、デコードされたリクエストに含まれる「Authorization」ヘッダの値を使用して認証を行います。

   注意: ICAP_CLIENT_TYPE キーが「DEFAULT」の場合、正しく認証が行えません。

■ 通信シーケンスログの出力を行う場合

BlueCoat と連携した上で通信シーケンスログの出力を行う場合は、追加の ICAP サービスの登録とポリシーの設定を行います。ICAPサービスを登録するには、次の手順に従ってください。

注意: 通信シーケンスログについては「2. ログファイルの設定」(359 ページ)を参照してください。

1. [Configuration] タブを選択し、画面面左のメニューの [Content Analysis]-[ICAP] をクリックします。

   ICAP サービスの設定画面が表示されます。

2. [ICAP Services] タブを選択し、[New] ボタンをクリックします。

   「サービス登録用」ダイアログが表示されます。

3. 登録するサービス名を入力して [OK] ボタンをクリックします。

   ICAP サービスが一覧に登録されます。
   複数の ICAP サーバを使用する場合には、使用するサーバごとにサービスを登録してください。

4. 登録されたサービスを一覧から選択し、[Edit] ボタンをクリックします。

   ICAP サービス設定ダイアログが表示されます。

5. 次の項目を設定します。

ICAP version	1.0
Service URL	環境にあわせて IP アドレス、ホスト名、ICAP ポート番号を指定します。 記入例） icap://<ISWM-Server>:<ICAP-Port>/ <ISWM-Server>: ISWM ICAP版を導入しているサーバの IP アドレス / ホスト名 <ICAP-Port>: LISTEN している ICAP ポート番号
Maximum number of connections	設定変更不要です。初期値は 5 ですが、ISWM と連携時に、「ISWM のプロセス数」の二分の一が自動的に設定されます。ISWM のプロセス数は、設定ファイル（proxy.inf）の [CONTROL_CFG] セクションの SERVER_PROCESS キーで設定します。
Connection timeout(seconds)	70

Method supported	response modification
Preview size (bytes)	enabled のチェックを外します。
Health Checks Options	設定した場合に Health Check による通信が通信シーケンスログに出力されるため設定しないことを推奨します。

注意: [Sense settings]ボタンをクリックするとICAPサーバとの接続を確認し、ICAPサーバに適合した設定へ変更できます。
通信シーケンスログの出力を行う場合は、BlueCoat の Method supported が request modification としている ICAP サービス側でも、Health Check を設定しないことを推奨します。

6. [OK] ボタンをクリックしてサービスの設定を BlueCoat に保存します。

7. [Apply] ボタンをクリックして BlueCoat に設定を反映します。

注意: [Apply] ボタンをクリックしないと設定は反映されません。必ず [Apply] ボタンをクリックしてください。

続けてポリシーの設定をします。

■ ポリシーの設定

1. 画面左のメニューの [Policy]-[Visual Policy Manager] をクリックします。
   Policy サービスの登録画面が表示されます。

2. [Visual Policy Manager] タブを選択し、[Launch Legacy Java VPM] ボタンをクリックします。
   Visual Policy Manager 画面が表示されます。

3. メニューバーの [Policy] をクリックし、表示されるプルダウンメニューから [Add Content Access Layer] をクリックします。

4. レイヤー名を入力し、[OK] ボタンをクリックします。
   レイヤーが追加されます。

5. 追加されたレイヤーの [Action] のセルを右クリックし、[Set] をクリックします。
   [Set Action Object] ダイアログが表示されます。

6. [New...] ボタンをクリックし、[Set ICAP Response Service...] をクリックします。

   [ADD ICAP Response Service Object] ダイアログボックスが表示されます。

7. 次の項目を設定し、[OK] ボタンをクリックします。

   - Use ICAP response service: 登録した ICAP サービスを選択
   - Error handling: [Deny the client request] を選択

   [Action] 一覧に ICAP サービスが追加されます。

8. [Set Action Object] に追加された ICAP サービスを選択し、[OK] ボタンをクリックします。

   ポリシーの Action が有効になります。

9. [Install Policy] ボタンをクリックします。

   Visual Policy Manager で設定したポリシー設定が BlueCoat に反映されます。

以上で、設定は完了です。

5-2. Squid との連携

ICAPクライアントとしてSquidを利用する場合、squid.confを設定してください。
ここでは、Squid version3.1.8の場合を例に説明します。

注意:
- Squid で ICAP クライアント機能を有効にするには、Squid インストール時の configure のオプションで "--enable-icap-client" を追加する必要があります。
- Squid 2.7/3.0 は非サポートです。
- 詳しくは Squid の Web サイトを参照してください。

1. 「squid.conf」に以下の設定を追加します。

   「acl CONNECT method CONNECT」と記述されている行の後に、以下の設定を追加します。

```
acl filtering_server dst <ISWM の IP アドレス >
acl block_message port 443
acl block_message port 21128
acl mng_web_port port <ISWM の管理画面のポート (2319)>
http_access allow filtering_server mng_web_port
always_direct allow filtering_server mng_web_port
always_direct allow filtering_server block_message
```

2. 「squid.conf」の最終行に以下の設定を追加します。

   通信シーケンスログを出力しない場合は以下の設定を追加します。

```
icap_enable on
icap_service service_1 reqmod_precache bypass=off icap://<ISWM の IP アドレス >:1344
adaptation_service_set service_set_1 service_1
adaptation_access service_set_1 deny filtering_server mng_web_port
adaptation_access service_set_1 allow all
icap_send_client_ip on
```

   通信シーケンスログを出力する場合は以下の設定を追加します。

```
icap_enable on
icap_service service_req reqmod_precache bypass=off icap://<ISWM の IP アドレス >:1344/reqmod
adaptation_service_set service_set_req service_req
adaptation_access service_set_req deny filtering_server mng_web_port
adaptation_access service_set_req allow all
icap_service service_resp respmod_precache bypass=off icap://<ISWM の IP アドレス >:1344/respmod
adaptation_service_set service_set_resp service_resp
adaptation_access service_set_resp deny filtering_server mng_web_port
adaptation_access service_set_resp allow all
icap_send_client_ip on
```

キー名	説明
icap_enable	Squid で ICAP クライアント機能を有効にします。

キー名	説明
icap_service	ISWM がインストールされているサーバとの連携方法を指定します。 ・フォーマット icap_service< サービス名 ><ICAP メソッド>< オプション>< サービス URL> < サービス名 >: 任意のサービス名を設定します。 <ICAP メソッド>: reqmod_precache を設定します。通信シーケンスログを出力する場合は、reqmod_precache と respmod_precache の各々を設定した icap_service が必要です。 < オプション >: bypass=off を指定します。 < サービス URL>: 記入例)icap://<ISWM-Server>:<ICAP-Port>
adaptation_service_set	icap_service で設定した ICAP サービスを ICAP サービスセットとして設定します。 ・フォーマット adaptation_service_set< サービスセット名 >< サービス名 > < サービスセット名 >: 任意のサービスセット名を設定します。 < サービス名 >: icap_service で設定したサービス名を指定します。
adaptation_access	Squid で受信した HTTP 通信を ISWM に送信するように設定します。 ・フォーマット adaptation_access< サービスセット名 > allow all < サービスセット名 >: adaptation_service_set キーで設定した ICAP サービスセットを指定します。
icap_send_client_ip	クライアントの IP アドレスを ISWM に通知するように設定します。

注意: ISWM と Squid を同じサーバにインストールしている場合、「icap_service」キーにループバックアドレス(127.0.0.1)を指定しないでください。必ず ISWM をインストールしたサーバの IP アドレスを指定してください。

3. ユーザ名で認証させる場合は「squid.conf」の最終行に以下の設定を追加します。

```
icap_send_client_username on
icap_client_username_encode on
icap_client_username_header X-Authenticated-User
```

4. Squid を再起動します。

以上で、ISWMとSquidのICAP連携の設定は完了です。

注意: ICAP クライアントでの NTLM 認証については、「C. ICAP クライアントでの NTLM 認証」(476 ページ)を参照してください。

■ HTTPS デコードを行う場合

Squidと連携した上でHTTPSデコードを行うには、SquidのSSLBump機能を有効にします。

注意:
- Squid で SSLBump 機能を有効にするには、サーバ証明書ファイルと秘密鍵ファイルを準備してください。また、Squid インストール時の configure のオプションで "--enable-ssl" を追加する必要があります。
- 詳しくは Squid の Web サイトと SSL サーバを参照してください。

1. Squid がインストールされているサーバにアクセスし、Squid の設定ファイル「squid.conf」の http_port に以下を追加します。設定は、ご使用の環境に合わせて修正してください。

   squid.conf の設定例

```
# Squid normally listens to port 3128
#http_port 3128 < 削除またはコメントアウト >
ssl_bump deny filtering_server mng_web_port
ssl_bump deny filtering_server block_message
ssl_bump allow all
http_port 3128 ssl-bump generate-host-certificates=on cert=< サーバ証明書ファイルパス > key=< 秘密鍵ファイルパス >
```

2. ICAP クライアントの動作により、HTTPS デコードの前と後で 2 段階のフィルタリング判定が行われる場合があります。デコード前の判定 (ドメイン単位) をスキップし、デコード後の判定 (ディレクトリ / ファイル単位) を優先するには、以下の設定を追加してください。

   「squid.conf」に新しい icap_service として「icap://<ISWM-Server>:<ICAP-Port>/skip_connect_reqmod」を追加します。デコード前の判定をスキップしたいリクエストは、こ

の ICAP サービスへ転送するように acl を設定してください。

3. ISWM の設定ファイル proxy.inf の [CONTROL_CFG] セクションの ICAP_CLIENT_TYPE キーに「SQUID」を設定します。

ファイルの保存場所

Linux 版＜インストールディレクトリ >/conf/proxy.inf

ICAP_CLIENT_TYPE キーに「SQUID」を設定した場合、デコードされたリクエストに含まれる「Authorization」ヘッダの値を使用して認証を行います。

注意: ICAP_CLIENT_TYPE キーが「DEFAULT」の場合、正しく認証が行えません。

5-3. Thunder との連携

ICAPクライアントとしてA10 Thunderを利用する場合、以下の手順で設定します。

注意: ISWM を Thunder と連携させて動作させるために、Thunder のコンフィグレーションモードで必要な設定をします。詳しくは Thunder のマニュアルを参照してください。

1. コンフィグレーションモードで下記コマンドを実行し、ISWM のサーバを登録します。

```
# slb server [ 任意のサーバ名 ] [ISWM の IP アドレス ]
# port [ISWM のポート番号 ] tcp
```

2. コンフィグレーションモードで下記コマンドを実行し、ISWM のサービスグループを作成します。

```
# slb service-group [ 任意のグループ名 ] tcp
# member [ 設定したサーバ名 ] [ 設定したポート番号 ]
```

3. コンフィグレーションモードで下記コマンドを実行し、REQMOD の ICAP テンプレートを作成しますす。

```
# slb template reqmod-icap [ 任意の設定名 ]
# include-protocol-in-uri
# preview 1
# service-url icap://[ISWM の IP またはホスト名 ]:[ISWM のポート番号 ]/
# service-group [ 設定したグループ名 ]
```

注意: POST データの preview サイズを「1byte」に設定する必要があります。
ISWM で 2byte 以降のデータを取得できないため、POST ログの出力と書込みキーワード規制機能は使用できません。

4. 作成した ICAP テンプレートを HTTP/HTTPS 通信に適用します。

5. Thunder 経由で行う Web アクセスが、ISWM のフィルタリングルールで許可 / 規制されること、および ISWM のアクセスログ（http.log）が出力されることをご確認ください。

■ Thunder の設定例

2 台の ISWM を登録する場合、以下のコマンドを実行します。

```
!
slb server iw1 10.10.224.100
  port 1344 tcp
!
slb server iw2 10.10.224.101
  port 1344 tcp
!
slb service-group t1344 tcp
  member iw1 1344
  member iw2 1344
!
slb template reqmod-icap rq1
  include-protocol-in-uri
  preview 1
  service-url icap://iswf:1344/
  service-group t1344
!
```

管理画面の表示例は以下のようになります。

■ HTTPS デコードを行う場合

Thunderと連携した上でHTTPSデコードを行うには、Thunderの設定とISWMの設定を変更します。

注意:
- Squid で SSLBump 機能を有効にするには、サーバ証明書ファイルと秘密鍵ファイルを準備してください。また、Squid インストール時の configure のオプションで "--enable-ssl" を追加する必要があります。
- 詳しくは Squid の Web サイトと SSL サーバを参照してください。

1. Thunder で SSL 復号化機能を有効にします。

詳しくは Thunder のマニュアル等を参照してください 。

2. ISWM の設定ファイル proxy.inf の [CONTROL_CFG] セクションの ICAP_CLIENT_TYPE キーに「SQUID」を設定します。

ファイルの保存場所

Linux 版＜インストールディレクトリ >/conf/proxy.inf

ICAP_CLIENT_TYPE キーに「SQUID」を設定した場合、デコードされたリクエストに含まれる「Authorization」ヘッダの値を使用して認証を行います。

注意: ICAP_CLIENT_TYPE キーが「DEFAULT」の場合、正しく認証が行えません。

6. ISWMの起動と停止

ISWMは通常、インストール完了後からサーバを再起動すると自動的にサービスを実行するように設定されます。ここでは、何らかの原因でサービスの再起動や停止をする場合の起動と停止について説明します。

6-1. Windowsの場合

Windows版でサービスを起動/停止するには、Windowsの[コントロールパネル]の[サービス]を使用します。次の手順でサービスの起動と停止をします。

1. サービスの起動と停止を実行可能なユーザアカウントで Windows にログインします。
2. [スタート] ボタン→ [設定] → [コントロールパネル] → [管理ツール] の順に選択し、[サービス] をダブルクリックします。
3. 停止または開始したいサービスを選択して [操作] メニューの [開始] または [停止] を実行します。

   ISWM には、4 つのサービスがあります。
   ISWMAdminControl : 管理サービス
   ISWMWebService : 拡張 Web サービス
   ISWMProxyControl : フィルタリングサービス
   ISWMDataCollectorControl : 集計サービス

注意: 集計サービスはプライマリサーバのみにあります。レプリカサーバにはありません。

6-2. Linux の場合

Linux 版の ISWM のサービスを起動または停止する場合は、対象とするサービスごとにターミナルで、次のコマンドを実行します。

注意: 起動と停止は root ユーザで実行してください。

管理サービス

起動: <インストールディレクトリ>/bin/amsadmin start
停止: <インストールディレクトリ>/bin/amsadmin stop

拡張Webサービス

起動: <インストールディレクトリ>/bin/amsweb start
停止: <インストールディレクトリ>/bin/amsweb stop

フィルタリングサービス

起動: <インストールディレクトリ>/bin/amsproxy start
停止: <インストールディレクトリ>/bin/amsproxy stop

集計サービス

起動: <インストールディレクトリ>/bin/amscollector start
停止: <インストールディレクトリ>/bin/amscollector stop

注意:

- 拡張Webサービスの起動/停止に、<インストールディレクトリ>/tomcat/bin/startup.shを実行しないでください。実行してしまった場合には、<インストールディレクトリ>/tomcat/work 以下のディレクトリとファイルをすべて削除してください。
- すべてのサービスを同時に起動 / 停止する場合は、次のコマンドを実行します。
  起動: <インストールディレクトリ>/bin/amsmain start
  停止: <インストールディレクトリ>/bin/amsmain stop
- 集計サービスはプライマリサーバのみ起動または停止できます。

7. アンインストール

7-1. Windowsの場合

Windows版をアンインストールする場合、Windowsの[コントロールパネル]の[プログラムの追加と削除]を使用します。

1. アンインストールを実行するコンピュータに、管理者権限を持つログインユーザでログインします。
2. [スタート] ボタン→ [設定] → [コントロールパネル] の順に選択し、[プログラムの追加と削除] をダブルクリックします。
3. ISWM を選択して [変更と削除] ボタンをクリックします。

   アンインストールの確認画面が表示されます。
4. [次へ] ボタンをクリックします。

   設定情報のアンインストール画面が表示されます。
5. 設定ファイルとログファイルを保存する場合は選択し、[アンインストール] ボタンをクリックします。

   アンインストールが完了するとアンインストール完了画面が表示されます。

   注意:
   - 現在の設定情報を保存したい場合は [設定ファイル] チェックボックスをオンにします。
   - ISWM で収集したログファイルを保存したい場合は、[ログファイル] チェックボックスをオンにします。
   - すべてのファイルをアンインストールしたい場合は、両方のチェックボックスをオフにしてください。
   - ここで保存した設定ファイルやログファイルは、再インストール時に読み込んで新しくインストールする ISWM に反映されます。
   - コマンドラインからサーバのチューニングを実行した場合、アンインストール完了後、再起動を促すメッセージが表示されます。
6. [完了] ボタンをクリックします。

以上で、ISWMのアンインストールは完了です。

7-2. Linux の場合

ISWMは、次の手順でアンインストールしてください。

注意: ISWM のアンインストールは root ユーザで実行してください。

1. ISWM のすべてのサービスを停止します。

ターミナルから次のコマンドを実行して、サービスを停止します。

管理サービスの停止

<インストールディレクトリ>/bin/amsadmin stop

拡張 Web サービスの停止

<インストールディレクトリ>/bin/amsweb stop

フィルタリングサービスの停止

<インストールディレクトリ>/bin/amsproxy stop

集計サービスの停止

<インストールディレクトリ>/bin/amscollector stop

初期設定では、次のディレクトリにインストールされています。
- /usr/local/iswm

2. ターミナルから < インストールディレクトリ >/bin/uninstall.sh を実行します。

アンインストールの確認メッセージが表示されます。

3. <Enter> を押します。

各種設定情報ファイルの保存を確認するメッセージが表示されます。

4. 削除したいファイルを選択して <Enter> を押します。

```
Check items you want to uninstall.
  1- Setting file
  2- Log file
```

アンインストールが開始されます。

注意: 設定ファイル (Setting file) とログファイル (Log file) の両方を削除したい場合は、「1,2」と (半角カンマで) 区切って入力し、<Enter> を押します。

8. 管理画面へのログイン/ログアウト

ISWM の設定をするときは、ブラウザからプライマリサーバの管理画面にログインしてください。

注意:
- ISWM の管理画面では、セッション情報管理に Cookie を使用しています。Cookie が使用できる環境でログインしてください。
- Microsoft Edge の設定で、[Cookie とサイトのアクセス許可] → [Cookie とサイトデータの管理と削除] → [Cookie データの保存と読み取りをサイトに許可する (推奨)] をオフに設定するとCookieが使用できなくなり、管理画面にログインできなくなります。

8-1. 管理画面へのログイン

管理画面へのログインは次の手順で行います。

1. ブラウザで管理画面にアクセスします。

プライマリサーバの IP アドレスが 192.168.1.1、ポートが 2319 の場合、
http://192.168.1.1:2319/index.html と入力します。
ログイン画面が表示されます。

注意:
- ISWM をインストールしたサーバ以外の端末からネットワーク経由で管理画面にログインできます。
- Windows 版の場合、[スタート] ボタン→ [すべてのプログラム] → [InterScanWebManager] → [InterScanWebManager] をクリックするとログイン画面を表示できます。
- 管理画面情報でポート番号を変更している場合、設定にあわせて URL のポート番号部分 (2319) を変更してください。

2. アカウントとパスワードを入力し、[ログイン] ボタンをクリックします。

[ホーム] 画面が表示されます。

注意:
- ISWM をインストールした直後は、アカウント [root]、パスワード [root] でログインしてください。
- 第 1 階層グループごとにアカウントの管理をしている場合は、アカウントに「ADMIN¥root」と入力してログインしてください。
- 言語で [English] を選択した場合は、画面の項目が英語で表示されます。日本語で作成したグループ名やカテゴリ名は、日本語のままで表示されます。
- ログイン後は、ブラウザなどの [戻る] ボタンなどで、ページを切り替えないでください。また、管理画面を終了させるときは、必ず画面右上の [ログアウト] でログアウトしてから [閉じる] ボタンなどでブラウザを終了させてください。ログアウトしないでブラウザを終了した場合、ログインしたままの状態になります。

■ ログインするアカウントについて

管理画面はログインするアカウントによって設定できる項目や表示される画面が異なります。アカウント種別と、それぞれのアカウントで設定や表示ができる項目については、次の表を参照してください。

アカウント種別	説明
システム管理者	システムの管理者です。 管理画面上ですべての設定が可能です。
システム管理者 (制限付き)	制限付きのシステムの管理者です。 グループ / ユーザ管理、共通アクセス管理、個別アクセス管理、規制解除申請管理の設定が可能です。 サーバ管理、設定情報管理、ログ管理の設定情報の閲覧のみが可能です。
システム管理者 (閲覧のみ)	閲覧のみのシステムの管理者です。 管理画面上ですべての設定情報の閲覧のみが可能です。
システム管理者 (例外 URL 設定のみ)	例外 URL 設定のみのシステムの管理者です。 すべてのグループの例外 URL の設定のみが可能です。 ユーザ自身のパスワード、メールアドレスの変更ができます。

アカウント種別	説明
グループ管理者	グループの管理者です。 所属グループと下位グループのグループ / ユーザ管理、個別アクセス管理、規制解除申請管理の設定が可能です。 第一階層のグループ管理者だけがアクセスログの閲覧が可能です。
グループ管理者 (制限付き)	制限付きのグループの管理者です。 所属グループと下位グループのグループ / ユーザ管理、個別アクセス管理、規制解除申請管理の設定が可能です。 第一階層のグループ管理者だけがアクセスログの閲覧が可能です。
グループ管理者 (閲覧のみ)	閲覧のみのグループの管理者です。 所属グループと下位グループのグループ / ユーザ管理、個別アクセス管理、規制解除申請管理、設定情報管理、ログ管理の設定情報の閲覧のみが可能です。 第一階層のグループ管理者だけがアクセスログの閲覧が可能です。
グループ管理者 (例外 URL 設定のみ)	例外 URL 設定のみのグループの管理者です。 所属グループと下位グループの例外URLの設定のみが可能です。 ユーザ自身のパスワード、メールアドレスの変更ができます。
一般ユーザ	各グループに所属する一般ユーザです。 ユーザ自身のパスワード、メールアドレスの変更ができます。

注意:
- 一般ユーザのアカウントは、ユーザ認証の設定で LDAP 連携をしている場合、パスワードの変更はできません。パスワードは LDAP サーバで変更してください。
- 第一階層のグループ管理者 (制限付き) およびグループ管理者 (閲覧のみ) で管理画面にアクセスした場合、自分の所属するグループのアクセスログの閲覧は可能です。ただし、ローテート済みのログの削除はできません。グループ管理者 (制限なし) だけがログを削除できます。

8-2. 管理画面からのログアウト

管理画面からログアウトする場合は、画面右上にある[ログアウト]をクリックしてください。

注意: 管理画面はブラウザの [閉じる] ボタンで終了しないでください。ISWM にセッションが残ったままになるので、サーバのメモリを消費します。また、セッション情報が残るのでセキュリティ維持のためにも、必ずログアウトしてください。

1. 画面右上にある [ログアウト] をクリックします。
   確認のダイアログが表示されます。
2. [OK] ボタンをクリックします。

9. [ホーム]画面の各部名称

管理画面にログインすると[ホーム]画面が表示されます。
ここでは、[ホーム]画面の各部の名称と基本的な操作について説明します。

9-1. [ホーム]画面

ISWMにログインすると[ホーム]画面が表示されます。
[ホーム]画面では「ログイン情報」、「簡易設定」、「URLカテゴリ確認」、「Geoスコープ」、「サーバ情報」が表示されます。

■ ログイン情報

現在ログインしているアカウントのグループ、ユーザ、権限、前回ログイン日時を確認できます。

■ 簡易設定

簡易設定のリンクがあります。
[簡易設定]をクリックすると、運用に必要な最小限の設定をする[簡易設定]画面を表示します。簡易設定は、すべてのユーザに一括してフィルタリングルールを設定します。
初めてISWMをご利用になる場合や、テスト環境での動作確認時などにご利用ください。

■ URL カテゴリ確認

URLカテゴリ確認システムのリンクがあります。
[URLカテゴリ確認システム]をクリックすると、URLカテゴリ確認システムに接続します。
URLカテゴリ確認システムでは、次のサービスを提供しています。

規制 URL のカテゴリ確認	URL がどのカテゴリに分類登録されているのか調べることができます。 フィルタリングルールを作成するときに参照してください。
規制 URL の申請	データベースに登録を希望する URL をネットスター社のデータベース登録セクションに申請することができます。

注意: URL カテゴリ確認システムに URL を送信した場合、受付確認および、登録・解除・変更等の結果連絡が、メールで送信されます。
メールの送信先は、データベース候補リスト登録時に入力したメールアドレスとなります。

■ Geo スコープ

Geoスコープは、地域別のアクセスグラフを表示する画面です。地域・カテゴリ・プロトコル・期間(日・週・月) などのアクセス数を集計したログをグラフで表示します。

1. ホーム画面の [Geo スコープ] をクリックすると、別画面で Geo スコープが表示されます。
2. Geo スコープの右上にある「アクセス集計」をクリックして [ON] にすると、集計が開始され、グラフが表示されます。
3. 表示条件(集計単位や期間など)を変更する場合は、画面左側にある各項目を設定してください。

■ 地域別規制

地域を選択し、[地域別規制]をクリックすると、選択した地域の未分類カテゴリのアクセスをブロックします。

1. Geo スコープ右上の [地域別規制] をクリックして [ON] にします。
2. 画面の地球儀上をクリックして地域を選択すると、画面右側に選択された地域の情報が表示されます。
3. [アクセスブロック] をクリックして [ON] にします。
4. 未分類のみをブロックする場合は、[未分類のみ対象] を [ON] にします。

注意:
- 地域別規制を解除する場合は、アクセスブロックを [OFF] にします。
- Geo スコープ表示画面は、一般ユーザ、グループ管理者は表示できません。ただし、ログ出力設定でログの出力単位を「グループ別」に設定している場合は、第一階層のグループ管理者にも表示されます。

■ サーバ情報

ISWMとして稼動しているプライマリサーバ、およびレプリカサーバの状態を確認できます。[パフォーマンスモニタ]の[表示]をクリックすると、各種リソース状況などのパフォーマンス情報を、グラフを使って別画面に表示します。表示期間は、1時間、1日、1週間から設定してください。表示内容は、1分毎に更新されます。

■ メインメニュー

7つのカテゴリに分類された設定項目を表示します。

各メインメニューにマウスのポインタを合わせると、カテゴリごとに設定可能な項目がサブメニューとして表示されます。サブメニューをクリックすると、対応する画面が表示されます。画面名称と詳細説明ページについては、次の表を参照してください。

[グループ / ユーザ管理] 画面	「2. [グループ / ユーザ管理] 画面でできること」(127 ページ)
[共通アクセス管理] 画面	「2. [共通アクセス管理] 画面でできること」(180 ページ)
[個別アクセス管理] 画面	「3. [個別アクセス管理] 画面でできること」(183 ページ)
[規制解除申請管理] 画面	「1. [規制解除申請管理] 画面でできること」(336 ページ)
[サーバ管理] 画面	「1. [サーバ管理] 画面でできること」(40 ページ)
[設定情報管理] 画面	「1. [設定情報管理] 画面でできること」(352 ページ)
[ログ管理] 画面	「1. [ログ管理] 画面でできること」(357 ページ)

■ ヘルプ

管理画面の  をクリックすると、『Trend Micro InterScan WebManager管理者マニュアル』(本書)の該当ページが表示されます。

サーバの設定と管理

1. [サーバ管理]画面でできること

レプリカサーバの登録やISWMの設定変更などのほかに、ユーザ認証方法やメール通知設定など、サーバ共通の設定ができます。

1-1. サーバの設定と登録

レプリカサーバの新規登録や、ISWMのIPアドレスや各ポートに設定されたポート番号を参照できます。また、各サーバのフィルタリングサービスの起動/終了、再起動、ウィルスチェック連携機能の設定もできます。
レプリカサーバは、単独では動作しません。必ず、管理画面で新規サーバの登録をしてください。
ISWMに登録されているサーバは、管理画面で設定を変更したときに自動的に一括して設定を同期しますが、何らかの問題で同期に失敗している場合、サーバ名が赤く表示されます。
設定の復旧に失敗している場合には青く表示されます。
設定の反映に失敗している場合には橙で表示されます。
この場合、同期/復旧/反映に失敗しているサーバと通信し、修復を試みることができます。
→「2. サーバの設定と登録」(42ページ)

注意: 管理画面で設定を変更し、今すぐにレプリカサーバに反映したいとき、[設定情報管理]-[保存/復旧/同期]-[レプリカサーバ同期]で、[今すぐ同期を実行]ボタンをクリックしてください。
なお、管理画面で設定を変更したとき、プライマリサーバへの反映、レプリカサーバへの反映は自動的に行います。管理画面で設定を変更したとき、自動的にプライマリサーバとレプリカサーバが同期しないように設定したい場合は、[設定情報管理]-[保存/復旧/同
期]-[レプリカサーバ同期]で、[設定変更時に自動で同期を行う]チェックボックスをオフにしてください。

1-2. データベースのダウンロード

フィルタリング用データベースのライセンスキーの設定やダウンロード時の各種設定ができます。また、データベースのダウンロードと各サーバへの適用状況を確認できます。
→「3. データベースのダウンロード」(53ページ)

1-3. 信頼済み証明書設定

SSLサーバの証明書を検証するために使用する認証局証明書の管理が行えます。
→「4. 信頼済み証明書設定」(57ページ)

1-4. ユーザ認証 /LDAP の設定

フィルタリングサービスをグループごとにする場合のユーザ認証の方法を設定します。LDAP連携やLDAP同期も設定できます。
→「5. ユーザ認証/LDAPの設定」(60ページ)

1-5. メール通知設定

管理者宛てに、ISWMのライセンス期限切れの事前通知やサーバの動作状況をメールで通知できます。
→「6. メール通知設定」(98ページ)

1-6. 上位プロキシ設定

上位プロキシの使用可否や、アクセスする先に応じて使用する上位プロキシの設定を管理画面から柔軟に行うことができます。
→「7. 上位プロキシ設定」(100ページ)

1-7. 一般設定

管理画面の[サーバ管理]-[一般設定]で、以下の設定を行うことができます。

- セーフサーチロック
- アクセス制御設定
- フィルタリングバイパス設定
- 保存 / 復旧設定
- 通知設定
- 例外 URL 自動登録設定
- 例外 URL 自動削除設定
- ARMS(Automatic registration service for Malware Site) 設定

→「8. 一般設定」(104ページ)

2. サーバの設定と登録

2-1. サーバ情報を確認する

ISWMでは複数のサーバを一元管理します。
「サーバ設定」では、ISWM として稼動しているプライマリサーバ、およびレプリカサーバの状態や設定を確認できます。

1. [サーバ管理]-[サーバ設定]をクリックします。

[サーバ設定]が表示されます。

注意: 赤く表示されているサーバは、設定の同期に失敗しているサーバです。
青く表示されているサーバは、設定の復旧に失敗したサーバです。
橙で表示されているサーバは、設定の反映に失敗したサーバです。
ネットワーク設定などに問題がないか確認してください。

2-2. サーバの起動と停止

ISWM では登録されているプライマリサーバやレプリカサーバのフィルタリングサービスを個別に起動したり、停止できます。[サーバ設定]では、メンテナンス時に一時的にサーバを停止したり、設定を反映するためにフィルタリングサービスを再起動できます。

注意: 管理画面から再起動できるのは「フィルタリングサービス」のみです。「管理サービス」および「拡張Webサービス」は再起動できません。

1. [サーバ管理]-[サーバ設定]をクリックします。

[サーバ設定]が表示されます。

2. フィルタリングサービスの状態を変更します。

再起動、起動、終了の中から変更したい状態をクリックします。

2-3. 新規レプリカサーバを登録する

ISWMは、最大10台までのレプリカサーバを管理できます。サーバにレプリカサーバを登録するときは、次の手順で新規サーバ登録をしてください。

注意:
- [サーバ登録] では、ISWM インストール時に設定した IP アドレスを設定してください。インストール後の変更はできません。
  サーバ名は、任意の名前を設定し、運用途中で変更することもできます。
- ロードバランサやICAPクライアントなどを使用して、ラウンドロビンによる負荷分散を行っている環境では、規制画面の表示や一時解除、警告解除が正常に動作しないため、[サーバ管理]-[サーバ設定]より、[ロードバランサ補助設定]を有効にしてください。

1. [サーバ管理]-[サーバ設定]をクリックします。

[サーバ設定]が表示されます。

2. [サーバを追加]をクリックします。

[サーバ登録]が表示されます。

3. サーバの設定情報を入力します。

サーバ情報

登録するレプリカサーバの[サーバ名]と[IPアドレス]を入力します。

フィルタリングサービス設定

フィルタリングサービスが監視するリクエストのポート番号と、処理可能な最大プロセス数を入力します。[プライマリサーバと同じ設定を使用する]チェックボックスをオンにすると、プライマリサーバの設定を使用します。

注意:
- 「HTTP」の設定項目は、ICAP版では「ICAP」として表示されます。
- ICAP版の場合、「HTTPS」と「FTP over HTTP」の設定項目は表示されません。
- スタンドアロン版で透過プロキシが有効になっている場合、「FTP over HTTP」の設定項目は表示されません。
- プロセス数を上限値 (9999) に設定した場合、メモリ消費量が増大します。十分なリソースを確保してから適宜設定値を調整してください。

規制画面表示設定

規制画面のアドレスバーに表示されるドメイン名を設定します。空欄にした場合はIPアドレスが表示されます。
[フィルタリングサービス設定]の[プライマリサーバと同じ設定を使用する]チェックボックスをオンにすると、プライマリサーバと同じ設定が使用されます。

注意: この設定項目は、ICAP版の場合のみ表示されます。

ウィルスチェック連携設定

ウィルスチェック連携機能を使用する場合は、[有効]チェックボックスをオンにします。
[連携先ホスト]にIPアドレスまたはホスト名、ICAPポート番号、接続パスを指定します。
[プロトコル中の連携手順]の[Preview/Continue有効]チェックボックスをオンにすると、Preview/Continueが有効になり、連携先ホストの応答時間の待機状態を短縮できます。
[ログ出力設定]でログに追加するICAPヘッダを指定します。

注意:
- [連携先ホスト]の変更後は、フィルタリングサービスを再起動してください。
- ICAP版の場合、この設定項目は表示されません。

---

4. 画面右上の[保存]ボタンをクリックします。

確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

「登録が完了しました」と表示されます。
以上で、レプリカサーバの登録は完了です。

6. 画面右上の[前画面へ戻る]ボタンをクリックします。

[サーバ設定]が表示されます。
サーバ情報に、登録したサーバの名前と設定が表示されます。

注意: 登録後に、登録したレプリカサーバの管理サービス、拡張Webサービス、フィルタリングサービスを再起動してください。

2-4. サーバの設定を変更する

プライマリサーバおよびレプリカサーバの設定を変更する場合、次の手順で設定してください。

1. [サーバ管理]-[サーバ設定]をクリックします。

   [サーバ設定]が表示されます。

2. 設定を変更したいサーバの右にある[選択]ボタンをクリックします。

   選択したサーバの設定情報が表示されます。

3. サーバの設定情報を変更します。

   サーバ情報

   管理画面で表示される「サーバ名」を入力します。

   管理画面設定(プライマリサーバのみ)

   ブラウザから管理画面にアクセスするときのポート番号を入力します。

注意:
- 管理画面のポート番号は、LogLyzer との通信にも使用しています。ポート番号を変更した場合は、LogLyzer側での設定も変更してください。
- 設定変更を反映するには、プライマリサーバおよびレプリカサーバの拡張 Web サービスを再起動する必要があります。Windows 版の場合は、コントロールパネルから拡張Webサービス(ISWMWebService)をいったん停止し、起動してください。
  Linux版の場合は、次のコマンドを実行して拡張Webサービスを再起動してください。
  停止:<インストールディレクトリ>/bin/amsweb stop
  起動:<インストールディレクトリ>/bin/amsweb start

フィルタリングサービス設定

フィルタリングサービスが監視するリクエストのポート番号と処理可能な最大プロセス数を入力します。[プライマリサーバと同じ設定を使用する]チェックボックスをオンにすると、プライマリサーバの設定を使用します。

注意:
- 「HTTP」の設定項目は、ICAP版では「ICAP」として表示されます。
- ICAP版の場合、「HTTPS」と「FTP over HTTP」の設定項目は表示されません。
- スタンドアロン版で透過プロキシが有効になっている場合、「FTP over HTTP」の設定項目は表示されません。

プロセス使用率が、プロセス数警告設定で指定された値を超えた際には警告メールが送信されます。メール通知機能の設定については、「6. メール通知設定」(98ページ)を参照してください。

フィルタリングサービス共通設定(プライマリサーバのみ)

リクエストモード(スタンドアロン版のみ)	追加ヘッダの動作を次の中から選択します。 • 上位プロキシがある時、転送 • 転送しない • 転送する • 認証のみ転送 • 追加ヘッダのみ転送
転送バッファサイズ※(スタンドアロン版のみ)	転送バッファサイズを指定します。
POST転送バッファサイズ(スタンドアロン版のみ)	POST転送バッファサイズを指定します。[転送バッファサイズと同じ値を使用する]を選択すると、[転送バッファサイズ]と同じ設定が使用されます。
タイムアウト値※(ICAP版のみ)	リクエストのタイムアウト値を指定します。 ICAPクライアントからリクエストを受信するタイムアウト値を1ミリ秒～9,999,999ミリ秒の範囲で指定します。
サーバ接続タイムアウト値※(スタンドアロン版のみ)	Webサーバとの通信がタイムアウトになる時間を1ミリ秒～9,999,999ミリ秒で設定します。
サーバ転送Nagleアルゴリズム(スタンドアロン版のみ)	サーバ転送Nagleアルゴリズムを無効にする場合はチェックボックスをオンにします。 連続する小さいパケットの送信を遅延するNagleアルゴリズムが無効化され、逐次送信されます。

クライアント接続タイムアウト値※(スタンドアロン版のみ)	クライアントとの通信がタイムアウトになる時間を1ミリ秒～9,999,999ミリ秒で設定します。
クライアント転送Nagleアルゴリズム(スタンドアロン版のみ)	クライアント転送Nagleアルゴリズムを無効にする場合はチェックボックスをオンにします。 連続する小さいパケットの送信を遅延するNagleアルゴリズムが無効化され、逐次送信されます。
HTTPS通信タイムアウト値※(スタンドアロン版のみ)	HTTPS 通信時に Web サーバとの通信がタイムアウトになる時間をミリ秒で設定します。
最大ヒープサイズ※	Java ヒープ領域サイズの最大値を 16M バイトから指定します。 サーバに搭載されているメモリサイズ以上の数値は設定しないでください。
ヘルスチェック間隔※	サーバが正常に稼動しているかを監視する間隔を設定してください。
Keep-Alive設定(スタンドアロン版のみ)	Keep-Aliveの設定を次の中から選択します。 • 無効: クライアント-プロキシ間、プロキシ-上位サーバ間とも、毎回接続し直します。 • 全て有効: クライアント-プロキシ間、プロキシ-上位サーバ間とも、持続接続します。 • クライアントとの接続のみ有効: クライアント-プロキシ間だけ持続接続し、プロキシ-上位サーバ間は毎回接続し直します。
HTTPバージョン設定(スタンドアロン版のみ)	HTTPのバージョンを選択します。 • HTTP/1.1対応: 受信したHTTPバージョンをそのまま転送します。 • HTTP/1.0のみ使用: 受信したHTTPバージョンをHTTP/1.0に変更して転送します。
プロトコル利用制御※(スタンドアロン版のみ)	HTTP/2、WebSocket、QUICK を使用した通信を制御する場合は、チェックボックスをオンにします。
透過プロキシ※(スタンドアロン版のみ)	クライアントのブラウザにプロキシを設定せずにプロキシを使用させたい場合は、チェックボックスをオンにします。

HTTPメソッド転送許可設定	転送を許可するHTTPメソッドを選択します。 [全選択] ボタンをクリックすると、すべてのメソッドをオンにします。[全解除] ボタンをクリックすると、すべてのメソッドをオフにします。
ロードバランサ補助設定	ロードバランサを使用して負荷分散を行っている環境では、チェックボックスをオンにしてください。 ユーザから受けたフィルタリング規制一時解除、HTTPSデコード警告解除、サーバー証明書警告解除の通知が全サーバで共有されるようになります。

注意:
- ※印の項目を変更した場合、変更を反映するため、登録済みの全サーバの管理サービスとフィルタリングサービスを再起動してください。
- 透過プロキシを使用する場合は、設定に加えて Linux カーネルのルーティング機能、または、ネットワーク外部機器やソフトウェアを用いたパケット制御により、クライアントからの通信をプロキシへ転送する必要があります。
  ※Windows Serverのルーティング機能では、透過プロキシ向けのパケット制御は行えません。
  ※ISWM単体で透過プロキシを実現することはできません。

規制画面表示設定(ICAP版のみ)

規制画面のアドレスバーに表示されるドメイン名を設定します。空欄にした場合はIPアドレスが表示されます。
[フィルタリングサービス設定]の[プライマリサーバと同じ設定を使用する]チェックボックスをオンにすると、プライマリサーバと同じ設定が使用されます。

注意: ICAPクライアントをインストールしたサーバ上(SquidやBlueCoat)で名前解決できるようにする必要があります。

Webコンテンツキャッシュ設定

Webコンテンツキャッシュ設定を使用する場合は、[有効]チェックボックスをオンにします。Webコンテンツキャッシュ設定では以下を指定します。

キャッシュモード※	キャッシュモードを以下の中から選択します。 • メモリとディスク: キャッシュにメモリとディスクを使用します。 • メモリのみ: キャッシュにメモリを使用します。 • ディスクのみ: キャッシュにディスクを使用します。
使用メモリ設定※	使用メモリを指定します。

最大使用ディスク設定※	使用できるディスク容量を設定します。
メモリキャッシュ対象コンテンツサイズ	メモリへの Web コンテンツキャッシュを許容する最小サイズと最大サイズをバイト単位で設定します。ここで設定した値の範囲から外れるコンテンツは、メモリにキャッシュされません。
ディスクキャッシュ対象コンテンツサイズ	ディスクに Web コンテンツキャッシュを許容する最小サイズと最大サイズをバイト単位で設定します。ここで設定した値の範囲から外れるコンテンツは、ディスクにキャッシュされません。
キャッシュ無効設定	キャッシュしないコンテンツを指定します。 • 拡張子: キャッシュしないコンテンツの拡張子を指定します。 • コンテンツタイプ: キャッシュしないコンテンツタイプを指定します。 • User-Agent: キャッシュしないUser-Agentを指定します。 • 宛先ホスト: キャッシュしない宛先ホストを指定します。 • パラメータ付URL パラメータ付きURLに対するレスポンスについてWebコンテンツキャッシュへ保管しない場合は、チェックボックスをオンにします。
サーバー時応答キャッシュ時間	オリジンサーバが一時的なステータスを返却してきた場合の応答を Web コンテンツキャッシュに一時保管する最大時間を秒単位で設定します。

注意:
- ※印の項目を変更した場合、変更を反映するため、登録済みの全サーバの管理サービスとフィルタリングサービスを再起動してください。
- 対象となる通信はHTTPのみです。HTTPSなど、他の通信ではキャッシュされません。
- ICAP版の場合、この設定項目は表示されません。

ウィルスチェック連携設定

ウィルスチェック連携機能を使用する場合は、[有効]チェックボックスをオンにします。

[連携先ホスト]にIPアドレスまたはホスト名、ICAPポート番号、接続パスを指定します。

[プロトコル中の連携手順]の[Preview/Continue有効]チェックボックスをオンにすると、Preview/Continueが有効になり、連携先ホストの応答時間の待機状態を短縮できます。

[クライアントへの転送設定]で、[解凍した転送データを再圧縮する]チェックボックス

をオンにすると、ICAPサーバへの転送の際に解凍したデータを再圧縮します。
[ログ出力設定]でログに追加するICAPヘッダを指定します。
[連携除外設定]で以下を指定します。

Content-Length	ウィルスチェック連携を除外するHTTPレスポンスのContent-Lengthの値をKバイト単位で設定します。ここで設定した値を超える場合に連携から除外されます。
拡張子	ウィルスチェック連携を行わない拡張子を設定します。設定した値がリクエスト URL のファイル拡張子と完全に一致した場合に連携から除外されます。
コンテンツタイプ	ウィルスチェック連携を行わないコンテンツタイプを設定します。設定した値がHTTPレスポンスのContent-Typeと部分一致した場合に連携から除外されます。

注意:
- [連携先ホスト]の変更後は、フィルタリングサービスを再起動してください。
- レプリカサーバの場合、[連携除外設定] の設定項目は表示されません。プライマリーサーバと同じ設定が適用されます。
- HTTPSサイトにおいてウィルスチェック連携機能を使用するには、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]より、HTTPSデコード機能を有効にし、「HTTPSデコードによる暗号解除後のデータをウイルスチェックの対象とする」チェックボックスをオンにして下さい。
- ICAP版の場合、この設定項目は表示されません。

4. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

5. [OK]ボタンをクリックします。

以上で、サーバの設定変更は完了です。

注意: [フィルタリングサービス設定]で[ポート]を変更した場合、変更を反映するため、登録済みの全サーバの管理サービスを再起動してください。

2-5. レプリカサーバを削除する

レプリカサーバの設定を削除する場合、次の手順で削除してください。

1. [サーバ管理]-[サーバ設定]をクリックします。

   [サーバ設定]が表示されます。

2. 設定を削除したいレプリカサーバの右にある[選択]ボタンをクリックします。

   選択したサーバの設定情報が表示されます。

3. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

以上で、レプリカサーバの削除は完了です。

2-6. サーバの設定を同期させる

ISWM に登録されているサーバは、管理画面で設定を変更したときに自動的に一括同期されます。何らかの問題で同期に失敗しているサーバがある場合、[サーバ設定]-[サーバ情報]でサーバ名が赤く表示されます。
設定の復旧に失敗している場合には青く表示されます。
設定の反映に失敗している場合には橙で表示されます。
このような場合、次の手順で同期に失敗しているサーバとの同期を実行してください。

注意: 管理画面で設定を変更し、今すぐにレプリカサーバに反映したいとき、[設定情報管理]-[保存/復旧/同期]-[レプリカサーバ同期]で、[今すぐ同期を実行]ボタンをクリックしてください。
なお、管理画面で設定を変更したとき、プライマリサーバへの反映、レプリカサーバへの反映は自動的に行います。管理画面で設定を変更したとき、自動的にプライマリサーバとレプリカサーバが同期しないように設定したい場合は、[設定情報管理]-[保存/復旧/同
期]-[レプリカサーバ同期]で、[設定変更時に自動で同期を行う]チェックボックスをオフにしてください。

1. [サーバ管理]-[サーバ設定]をクリックします。

   [サーバ設定]が表示されます。
   サーバ名が赤く表示されているサーバが同期に失敗しているサーバです。

サーバ名が青く表示されているサーバが復旧に失敗しているサーバです。
サーバ名が橙で表示されているサーバが反映に失敗しているサーバです。

2. [修復]ボタンをクリックします。

プライマリサーバの設定が、登録されているレプリカサーバに反映されます。
すべてのサーバが正常に同期されている場合、[修復]ボタンは表示されません。

3. [再表示]ボタンをクリックします。

3. データベースのダウンロード

3-1. ダウンロードの設定

ISWMは、URLデータベースをダウンロードして更新することで、精度の高いフィルタリングとセキュリティを実現します。URLデータベースを含むネットスター社のURLデータベースは、定期的に更新されます。ISWMをインストールしたサーバへの、URLデータベースの定期的なダウンロードにより、常に最新のURLデータベースを使用できます。
デフォルトでは1時間に1回、最新版のURLデータベースの有無を確認します。
インストール直後やサーバの設定変更後などに、手動でダウンロードする場合は、「3-2. データベースをダウンロードする」(55ページ)を参照してください。

注意: データベースファイルの破損によりURLデータベースのロードに失敗した場合、自動的にバックアップされた以前のデータベースファイルを読み込んで、URLデータベースを復旧します。
メール通知機能(サービス異常発生通知)が有効な場合、リカバリ結果はメールで通知されます。URLデータベースのロード失敗をメールで通知された場合、[サーバ管理]-[データベース設定]で、データベースのバージョン情報を確認してください。
メール通知機能の設定については、「6. メール通知設定」(98ページ)を参照してください。

1. [サーバ管理]-[データベース設定]をクリックします。

   [データベース設定]が表示されます。

2. 設定を変更したいサーバの右にある[選択]ボタンをクリックします。

   [データベース設定編集]が表示されます。

   注意: ダウンロード情報は、サーバごとに設定します。

3. 選択したサーバで次の項目を入力します。

ライセンス設定

ライセンスキー	使用許諾契約書に記載されたライセンスキーを入力します。
企業･団体名	会社名または団体名を入力します。(全角32文字、半角64文字以内)
メールアドレス	管理者のメールアドレスを入力します。 ここで入力されたメールアドレスには、ダウンロード用サーバの変更など、データベースについてのご案内をお送りします。

上位プロキシサーバ設定

インターネットへの接続に上位のプロキシサーバを利用している場合、[使用する]チェックボックスをオンにし、IPアドレス/ホスト名やポート番号、認証用のアカウント、パスワードを入力してください。

[プライマリサーバと同じ設定を使用する]チェックボックスをオンにすると、プライマリサーバの設定を使用します。

注意: IPv6アドレス登録時は[ ]で囲んでください。なお、IPv6アドレスは省略形式で登録されます。

ダウンロード設定

ダウンロード先URL	特に必要がない限り、変更する必要はありません。 初期設定では、「https://iswm.netstar-inc.com/db90」に設定されています。
ダウンロード時間自動設定	チェックボックスをオンにすると 1 時間ごとに、オフにした場合は1日1回、自動的にダウンロードを試みます
リトライ回数	データベースのダウンロードに失敗したときにリトライする回数を2回～5回の中から選択します。
リトライ間隔	リトライする間隔を30分、40分、50分、60分の中から選択します。
ダウンロード開始時間	データベースのダウンロードを実行する時間を0時～23時の中から選択します。

ダウンロード

[データベース更新]ボタンをクリックすると、データベースを更新します。

注意:
- ダウンロード時間自動設定が有効になっている場合、リトライ回数、リトライ間隔、ダウンロード開始時間は設定できません。
- デフォルトでは1時間ごとにURLデータベースをダウンロードします。また、データベースのダウンロードが失敗したときには、エラーメッセージが表示されます。

4. 画面右上の[保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

5. [OK]ボタンをクリックします。

以上で、ダウンロードの設定は完了です。

注意: ダウンロード中は、「～のデータベースダウンロード処理中です。」が表示されます。「～のデータベースダウンロード処理が完了しました。」が表示されればダウンロード完了です。
ライセンス切れ、誤りがあった場合は、「ライセンス期限切れ、またはライセンス誤設定により～にサンプルデータベースがダウンロードされました。」が表示されます。

3-2. データベースをダウンロードする

インストール直後やサーバのメンテナンス時などは、手動で URL データベースを更新してください。

■ すべてのサーバでダウンロードする

登録されているサーバすべてにデータベースをダウンロードする場合は、次の手順でダウンロードしてください。

1. [サーバ管理]-[データベース設定]をクリックします。

[データベース設定]が表示されます。

2. [データベース更新]ボタンをクリックします。

   確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

以上で、ダウンロードは完了です。

■ サーバを選択してダウンロードする

選択したサーバにだけ、データベースをダウンロードする場合は、次の手順でダウンロードしてください。

注意: プライマリサーバとの同期に失敗した場合など、個別のレプリカサーバにデータベースをダウンロードしたい場合にだけ使用してください。

1. [サーバ管理]-[データベース設定]をクリックします。

   [データベース設定]が表示されます。

2. ダウンロードを実行したいサーバの右にある[選択]ボタンをクリックします。

   [データベース設定編集]が表示されます。

3. [ダウンロード]-[データベース更新]ボタンをクリックします。

   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

以上で、ダウンロードは完了です。

4. 信頼済み証明書設定

ISWMでは、HTTPSデコードを有効にしている場合の接続先サーバやLDAPS接続先サーバなど、SSLサーバの証明書を検証するための認証局証明書を信頼済み証明書として保持しています。

システムが保持している認証局証明書に加え、ユーザ独自の認証局証明書を登録することにより、特定のサーバに対する証明書の検証が行えるようになります。

注意:
- システムが保持している認証局証明書については、管理画面での表示 / 追加 / 削除が行えません。
- ICAP 版で認証局証明書の追加や削除を行った場合、フィルタリングサービスの再起動が必要となります。
  詳細については、「1-1. サーバの設定と登録」(40ページ)を参照してください。

■ 証明書を追加する

認証局証明書の登録方法について説明します。

1. [サーバ管理]-[信頼済み証明書設定]をクリックします。

   [信頼済み証明書設定]が表示されます。

2. [証明書設定]-[認証局証明書]の[参照]ボタンをクリックし、証明書を選択します。

   登録できる証明書のファイル形式はDERまたはPEM形式です。

3. [証明書設定]-[識別名]に証明書の名前を入力します。

   注意: caから始まる識別名や、既に登録済みの識別名は使用できません。

4. [登録]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

   証明書が追加登録されます。

■ 証明書を削除する

登録した認証局証明書の削除方法について説明します。

1. [サーバ管理]-[信頼済み証明書設定]をクリックします。

   [信頼済み証明書設定]が表示されます。

2. 信頼済み証明書一覧から、削除する証明書のチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
   タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

3. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

   証明書が削除されます。

● 信頼済み証明書一覧の操作方法

信頼済み証明書一覧の操作方法について説明します。

1. [表示件数]により、1画面に表示する証明書の件数を変更できます。

   件数は15件、100件、500件から選択できます。

2. タイトル行をクリックすることで、証明書一覧の並び替えができます。

   ソート項目は、[識別名]、[証明書名]、[発行者名]、[有効期間開始日]、[有効期間終了日]のタイトル行から選択できます。
   選択されたソート項目は、△(昇順)で表示されます。

3. 画面に表示する証明書一覧のページを変更できます。

	クリックすると、先頭のページが表示されます。
	クリックすると、前のページが表示されます。
	現在表示中のページ番号が表示されます。 表示したいページを直接指定することもできます。
	クリックすると、次のページが表示されます。
	クリックすると、最終のページが表示されます。

4. [削除]ボタンをクリックすると、証明書一覧から、チェックボックスをオンにした証明書を削除します。

5. ユーザ認証/LDAPの設定

ここでは、フィルタリング対象となるユーザの認証方法、LDAP 連携、LDAP 同期設定について説明します。
ISWMではフィルタリングルールをグループやユーザごとに適用する場合、登録されているユーザの認証が必要です。

注意: ユーザ認証を無効に設定した場合、すべてのユーザにルートグループのフィルタリングルールが設定され、グループ別にフィルタリングルールを設定することはできません。

5-1. ユーザ認証の種類

設定できるユーザ認証方法には以下の種類があります。

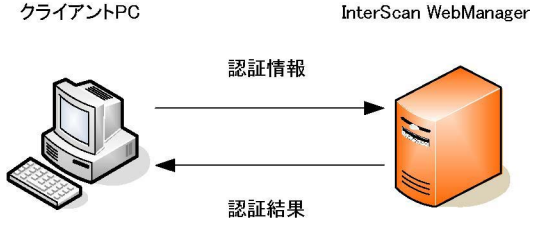
- IP アドレス認証
- BASIC 認証 (ローカル)
- BASIC 認証 (LDAP 連携)
- NTLM 認証 (スタンドアロン版のみ)
- Kerberos 認証 (スタンドアロン版のみ)

■ IPアドレス認証

ユーザ/グループ管理で設定されたIPアドレスによる認証をします。
ISWMでは、ユーザ認証を有効にした場合、IPアドレス認証は必ず有効になります。IPアドレスとアカウント認証を併用することで強固なセキュリティを実現します。

■ BASIC認証(ローカル)

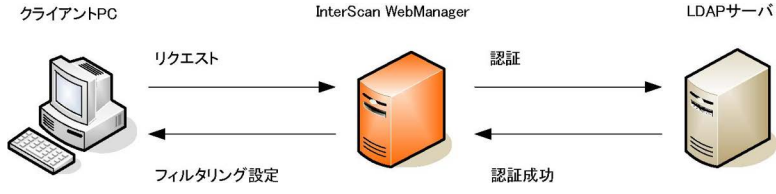
クライアントPCで入力したログイン情報をISWMでBASIC認証します。



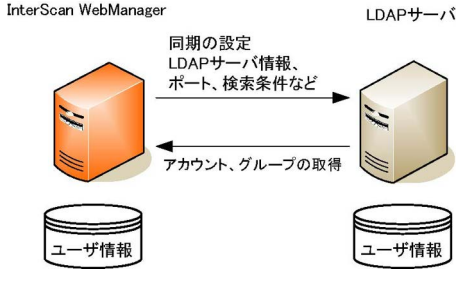
BASIC認証(ローカル)の設定方法については、「5-2. BASIC認証(ローカル)を設定する」(63ページ)を参照してください。

■ BASIC認証(LDAP連携)

LDAPサーバと連携したBASIC認証をします。LDAP連携を選択した場合、LDAP連携設定とLDAP同期設定を行ってください。
LDAPサーバとの同期設定を行った後は、ISWMはユーザ情報(アカウント)を確認後、LDAPサーバに問い合わせ、LDAPサーバの認証結果を利用してユーザ認証します。



LDAPサーバのユーザ情報を認証に利用する場合、LDAPサーバの情報をISWMのユーザ情報として取得できます。
LDAPサーバとの同期を実行すると、LDAPサーバの保持しているユーザ情報(アカウント)と、グループ情報がISWMに作成され、LDAPサーバによる認証が可能となります。



LDAPサーバのユーザ情報を利用してBASIC認証を行う場合、認証方式を[BASIC認証]-[LDAP連携を行う]に設定し、続けてLDAPサーバとの連携、同期の設定をしてください。
設定方法については、以下を参照してください。

BASIC認証(LDAP連携)の設定	「5-3. BASIC認証(LDAP連携)を設定する」(64ページ)
連携するLDAPサーバの登録	「5-7. LDAPサーバの登録と管理」(73ページ)
LDAP連携設定	「5-10. LDAPサーバとの連携を設定する」(79ページ)
LDAP同期設定	「5-11. LDAPサーバと同期する」(84ページ)

■ NTLM認証(スタンドアロン版のみ)

Microsoft社のActive Directoryと連携し、NTLM認証を使用したWindowsクライアントからのシングルサインオンを実現します。
Active DirectoryでWindowsのユーザ認証をしている環境において、対応ブラウザを使用してインターネットで Web ページを閲覧する場合、あらためてユーザ名とパスワードを入力することなく、ISWMでユーザ認証ができます。
Active Directoryのユーザ情報を利用してNTLM認証を行う場合、認証方式を[NTLM認証]に設定し、続けてActive DirectoryサーバとのLDAP連携、同期の設定をしてください。
設定方法については、以下を参照してください。

NTLM認証の設定	「5-4. NTLM認証を設定する」(65ページ)
連携するLDAPサーバの登録	「5-7. LDAPサーバの登録と管理」(73ページ)
LDAP連携設定	「5-10. LDAPサーバとの連携を設定する」(79ページ)
LDAP同期設定	「5-11. LDAPサーバと同期する」(84ページ)

■ Kerberos認証(スタンドアロン版のみ)

Microsoft社のActive Directoryと連携し、Kerberos認証を使用したWindowsクライアントからのシングルサインオンを実現します。
Active DirectoryでWindowsのユーザ認証をしている環境において、対応ブラウザを使用してインターネットで Web ページを閲覧する場合、あらためてユーザ名とパスワードを入力することなく、ISWMでユーザ認証ができます。
Active Directoryのユーザ情報を利用してKerberos認証を行う場合、認証方式に[Kerberos認証]を選択し、続けてActive DirectoryサーバとのLDAP連携、同期の設定をしてください。
設定方法については、以下を参照してください。

Kerberos認証の設定	「5-5. Kerberos認証を設定する」(69ページ)
連携するLDAPサーバの登録	「5-7. LDAPサーバの登録と管理」(73ページ)
LDAP連携設定	「5-10. LDAPサーバとの連携を設定する」(79ページ)
LDAP同期設定	「5-11. LDAPサーバと同期する」(84ページ)

5-2. BASIC 認証 (ローカル) を設定する

クライアントPCで入力したログイン情報をISWMでBASIC認証をする場合は、次の手順で設定してください。

注意: ここではスタンドアロン版の画面を使用しています。ICAP版では表示される項目が異なります。

1. [サーバ管理]-[認証設定]をクリックします。

   [認証設定]が表示されます。

2. [ユーザ認証]-[有効]チェックボックスをオンにします。

3. [認証方式]-[アカウント認証を行う]チェックボックスをオンにします。

   注意: ユーザ認証をする場合、IPアドレス認証は必ず有効になります。

4. [認証方式]-[BASIC認証]をクリックし、[ローカルでの認証を行う]をクリックします。

   注意:
   - IPアドレスの識別に接続元IPのみを利用する場合、[クライアントIP識別設定]-[HTTP リクエストヘッダを参照してクライアントの IP アドレスを識別する] チェックボックスをオフにしてください。
   - 登録されていないユーザの認証を有効にする場合、[未登録ユーザ設定]-[有効] チェックボックスをオンにしてください。
   - 第1階層に登録されているグループ単位でアカウントを管理する場合は、[第一階層グループ毎にアカウントの管理をする]チェックボックスをオンにしてください。
   - 第 1 階層グループごとのアカウント管理を有効にした場合、認証ダイアログで「第一階層グループ名」+「¥」+「アカウント名」を入力してください。このとき、第2階層～第10階層のグループ名を入力しても認証されません。
     例:「sales¥yamada」

5. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

6. [OK]ボタンをクリックします。

以上で、BASIC認証(ローカル)の設定は完了です。

5-3. BASIC 認証 (LDAP 連携) を設定する

LDAPサーバと連携したBASIC認証は、次の手順で設定します。

注意:
- ここではスタンドアロン版の画面を使用しています。ICAP 版では表示される項目が異なります。
- 設定完了後は、必ず LDAP サーバとの同期を行ってください。LDAP サーバと定期的に自動同期を設定することもできます(自動連携)。
- LDAP連携を設定すると、アカウントやパスワードの認証はLDAPサーバで実行されます。ISWMではパスワードなどの情報を持たないため、アカウントの登録/削除、パスワードの変更はできません。IP アドレスをユーザ名として登録したユーザは、登録/削除できます。

1. [サーバ管理]-[認証設定]をクリックします。

[認証設定]が表示されます。

2. [ユーザ認証]-[有効]チェックボックスをオンにします。

3. [認証方式]-[アカウント認証を行う]チェックボックスをオンにします。

注意: ユーザ認証をする場合、IPアドレス認証は必ず有効になります。

4. [認証方式]の[BASIC認証]をクリックし、[LDAP連携を行う]をクリックします。

注意:
- IPアドレスの識別に接続元IPのみを利用する場合、[クライアントIP識別設定]-[HTTP リクエストヘッダを参照してクライアントの IP アドレスを識別する] チェックボックスをオフにしてください。
- 登録されていないユーザの認証を有効にする場合、[未登録ユーザ設定]-[有効] チェックボックスをオンにしてください。

5. [LDAPグループ特定方式]を選択してクリックします。

[認証設定]-[LDAPグループ特定方式]

ユーザのDNからグループ階層を特定する	指定した組織単位 (OU) 以下の構造を ISWM のグループ構成にインポートして、組織単位でフィルタリング設定を行います。

グループ毎にユーザ抽出条件を指定する	ISWMのグループごとにLDAPサーバから取り込むユーザの条件を設定できます。Active Directory のセキュリティグループなど、組織単位とは異なるグループ単位でフィルタリング設定を行います。複数グループの抽出条件に一致する場合、設定した優先順位に従って ISWM のグループに取り込みます。 セキュリティグループの中にグループが存在する場合など、抽出したグループの階層検索を有効にする際には、[セキュリティグループの階層検索を有効にする] チェックボックスをオンにします。

注意: セキュリティグループの階層検索では、1 階層分のグループが対象となります。

6. [LDAP認証キャッシュ]で、LDAP認証情報キャッシュする時間を入力します。

初期値は60分です。
[クリア]ボタンをクリックすると、現在キャッシュされているLDAP認証情報をクリアできます。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

「更新が完了しました。」と表示されます。

以上で、BASIC認証(LDAP連携)の設定は完了です。
続けてLDAPサーバの設定をしてください。詳細は、「5-7. LDAPサーバの登録と管理」(73ページ)を参照してください。

5-4. NTLM 認証を設定する

注意: NTLM認証は、スタンドアロン版だけが設定できます。ICAP版では設定項目が表示されません。

■ NTLM認証時の注意

- NTLM 認証機能を利用する場合、Active Directory サーバと ISWM を LDAP 連携する必要があります。
- NTLM 認証時は、ブラウザ側でシングルログインに対応しているのでアカウントやパスワードは、クライアント側で Windows にログインしたユーザ ID とパスワードで自動認証されます。
  自動認証に失敗した場合は、認証ダイアログが表示されるのでアカウントおよびパスワードを入力して認証してください。
- LDAP サーバにログインしたアカウントがある場合は、ISWM で該当するアカウント、またはグループのフィルタリング設定が適用されます。
- NTLM 認証時は、LDAP 連携のため検索条件で、アカウントを「sAMAccountName」に設定してください。検索条件でアカウントを「cn」に設定している場合、正しくアカウントが検索されません。
- ISWM とクライアント PC の間に、他のプロキシ (下位プロキシ) を使用することはできません。クライアント PC と ISWM が直接通信できる環境が必要です。
- ISWM とインターネットの間にプロキシサーバ (上位プロキシ) がある場合、上位プロキシでの認証は利用できません。
- NTLM 認証を設定した場合、ISWM に対して BASIC 認証 (ローカルでの認証) よりもサーバに負荷がかかります。NTLM 認証で運用を開始する前に十分に稼動検証をしてください。負荷が大きい場合は、ユーザごとにサーバを分散して運用するようにしてください。
- ISWM の BASIC 認証では、登録されたユーザアカウントに対して認証を行う場合、大文字小文字の識別がされます。Windows 上でユーザアカウントを登録する場合には、大文字と小文字を混在できますが、Windows の仕様上、ログインするときには、大文字と小文字は区別しません。
  NTLM 認証 (シングルサインオン) を利用する場合とそれ以外の場合で注意が必要です。NTLM では、Active Directory 内ですべてのユーザ名を大文字で管理しています。同様に、ISWM でもユーザアカウントは大文字に変換して管理しています。
- 同じドメインの LDAP サーバを複数登録する場合は、各サーバの NetBIOS ドメイン名を、必ず、Active Directory で設定した名称に統一してください。
- 異なるドメインやサブドメインの LDAP サーバを複数登録する場合は、フォレストの構成にするか、またはドメイン間の信頼関係を結んでください。

NTLM認証をする場合は、次の手順で設定してください。

1. [サーバ管理]-[認証設定]をクリックします。
   [認証設定]が表示されます。
2. [ユーザ認証]の[有効]チェックボックスをオンにします。

3. [認証方式]の[アカウント認証を行う]チェックボックスをオンにします。

注意: ユーザ認証をする場合、IPアドレス認証は必ず有効になります。

4. [認証方式]の[NTLM認証]をクリックします。

注意:
- IPアドレスの識別に接続元IPのみを利用する場合、[クライアントIP識別設定]-[HTTP リクエストヘッダを参照してクライアントの IP アドレスを識別する] チェックボックスをオフにしてください。
- 登録されていないユーザの認証を有効にする場合、[未登録ユーザ設定]-[有効] チェックボックスをオンにしてください。

5. [LDAPグループ特定方式]を選択してクリックします。

[認証設定]-[LDAPグループ特定方式]

ユーザのDNからグループ階層を特定する	指定した組織単位 (OU) 以下の構造を ISWM のグループ構成にインポートして、組織単位にフィルタリング設定を行います。
グループ毎にユーザ抽出条件を指定する	ISWMのグループごとにLDAPサーバから取り込むユーザの条件を設定できます。Active Directory のセキュリティグループなど、組織単位とは異なるグループ単位でフィルタリング設定を行います。複数グループの抽出条件に一致する場合、設定した優先順位に従って ISWM のグループに取り込みます。

6. [LDAP認証キャッシュ]で、LDAP認証情報キャッシュする時間を入力します。

初期値は60分です。
[クリア]ボタンをクリックすると、現在キャッシュされているLDAP認証情報をクリアできます。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

以上で、NTLM認証の設定は完了です。

続けて連携するLDAPサーバを登録してください。詳細は、「5-7. LDAPサーバの登録と管理」(73ページ)を参照してください。

5-5. Kerberos 認証を設定する

注意: Kerberos認証は、スタンドアロン版だけが設定できます。ICAP版では設定項目が表示されません。

■ Kerberos認証時の注意

- Kerberos 認証機能を利用する場合、Active Directory サーバと ISWM を LDAP 連携する必要があります。
- Kerberos 認証時は、シングルサインオンによるログインに対応しているので、クライアント側の Windows ログインにより自動認証されます。
  自動認証に失敗し、認証ダイアログが表示される場合にはアカウントおよびパスワードを入力して認証してください。
- LDAP サーバにログインしたアカウントがある場合は、ISWM で該当するアカウント、またはグループのフィルタリング設定が適用されます。
- Kerberos 認証時は、LDAP 連携のため検索条件で、アカウントを「sAMAccountName」に設定してください。検索条件でアカウントを「cn」に設定している場合、正しくアカウントが検索されない場合があります。
- ISWM とクライアント PC の間に、他のプロキシ (下位プロキシ) を使用することはできません。クライアント PC と ISWM が直接通信できる環境が必要です。
- ISWM とインターネットの間にプロキシサーバ (上位プロキシ) がある場合、上位プロキシでの認証は利用できません。
- Kerberos 認証を設定した場合、ISWM に対して BASIC 認証 (ローカルでの認証) よりもサーバに負荷がかかります。Kerberos 認証で運用を開始する前に十分に稼動検証をしてください。負荷が大きい場合は、ユーザごとにサーバを分散して運用するようにしてください。
- ISWM の BASIC 認証では、登録されたユーザアカウントに対して認証を行う場合、大文字小文字の識別がされます。Windows 上でユーザアカウントを登録する場合には、大文字と小文字を混在できますが、Windows の仕様上、ログインするときには、大文字と小文字は区別しません。Kerberos 認証 (シングルサインオン) を利用する場合とそれ以外の場合で注意が必要です。Kerberos 認証では、ActiveDirectory 内ですべてのユーザ名は大文字小文字を区別していません。同様に、ISWM でもユーザアカウントは大文字小文字を区別していません。
- 同じドメインの LDAP サーバを複数登録する場合は、各サーバのドメイン名を、必ず Active Directory で設定した名称に統一してください。
- Kerberos 認証ではブラウザから送信されてくるチケットを認証する際にチケットの使用可能期間を確認します。クライアント PC、Active Directory のサーバ、プライマリサーバおよびレプリカサーバの時刻が異なる場合は認証が正しく行われない場合があります。各 PC およびサーバで時刻の同期を行ってください。

- クライアント側のブラウザの設定で Kerberos 認証が使用できるように設定してください。Windows の場合は、インターネットオプションで統合 Windows 認証を有効にし、認証プロバイダの URL をローカルイントラネットゾーンに追加してください。また、プロキシ設定は必ずサービスプリンシパル名に設定した ISWM のホスト名（FQDN）で入力してください。IP アドレスで入力した場合は、Kerberos 認証が正しく行われません。
- 管理画面の「ドメイン名」は必ず FQDN で入力してください。短縮名だけを設定すると、Kerberos 認証が正しく行われません。

Kerberos認証をする場合は、次の手順で設定してください。

1. [サーバ管理]-[認証設定]をクリックします。
   [認証設定]が表示されます。
2. [ユーザ認証]の[有効]チェックボックスをオンにします。
3. [認証方式]の[アカウント認証を行う]チェックボックスをオンにします。

   注意: ユーザ認証をする場合、IPアドレス認証は必ず有効になります。

4. [認証方式]の[Kerberos認証]をクリックします。

   注意:
   - IPアドレスの識別に接続元IPのみを利用する場合、[クライアントIP識別設定]-[HTTP リクエストヘッダを参照してクライアントの IP アドレスを識別する] チェックボックスをオフにしてください。
   - 登録されていないユーザの認証を有効にする場合、[未登録ユーザ設定]-[有効] チェックボックスをオンにしてください。

5. [LDAPグループ特定方式]を選択してクリックします。

[認証設定]-[LDAPグループ特定方式]

ユーザのDNからグループ階層を特定する	指定した組織単位 (OU) 以下の構造を ISWM のグループ構成にインポートして、組織単位にフィルタリング設定を行います。
グループ毎にユーザ抽出条件を指定する	ISWMのグループごとにLDAPサーバから取り込むユーザの条件を設定できます。Active Directory のセキュリティグループなど、組織単位とは異なるグループ単位でフィルタリング設定を行います。複数グループの抽出条件に一致する場合、設定した優先順位に従って ISWM のグループに取り込みます。

6. [LDAP認証キャッシュ]で、情報キャッシュする時間を入力します。

   初期値は60分です。
   [クリア]ボタンをクリックすると、現在キャッシュされているLDAP認証情報をクリアできます。

7. [Kerberos認証設定]で、Kerberos認証に関する設定を行います。

   詳細は、「K. Kerberos認証使用時の設定例」(499ページ)を参照してください。

8. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

9. [OK]ボタンをクリックします。

以上で、Kerberos認証の設定は完了です。
続けて連携するLDAPサーバを登録してください。詳細は、「5-7. LDAPサーバの登録と管理」(73ページ)を参照してください。

5-6. リクエスト別認証を設定する

リクエスト別認証設定とは、ユーザが設定した「User-Agent名」または「宛先ホスト名」に合致した場合に、ルートグループのユーザとして認証し、フィルタリングを行う機能です。
Windows Update時やブラウザ以外のアプリケーションからの通信では認証処理が原因で通信に失敗することがあります。その場合は、ルートグループのユーザとして認証させることで認証処理が省略され、正常に通信ができるようになります。

注意: ルートグループのユーザが正常に通信ができるように適切なルールをルートグループ側で設定してください。

■ リクエスト別認証を設定する

次の手順で設定します。

1. [サーバ管理]-[認証設定]をクリックします。

   [認証設定]が表示されます。

2. [リクエスト別認証設定]の[User-Agent認証]に、ルートグループのユーザとして認証したいUser-Agent名を設定します。

注意:
- User-Agent名は改行区切りで複数入力できます。
- 設定した文字列が HTTP リクエストの User-Agent ヘッダに含まれる場合は、必ずルートグループのユーザとして認証し、フィルタリングを行います。

3. [リクエスト別認証設定]の[宛先ホスト認証]に、ルートグループのユーザとして認証したい宛先ホスト名を設定します。

注意:
- 宛先ホスト名は改行区切りで複数入力できます。ワイルドカードとして「*」を使用する場合、「*」は「.」を含む1文字以上の文字列として使用してください。例えば「*netstar.jp」と設定した場合は「www.netstar.jp」および「game.netstar.jp」の両方が対象になります。また「www.netstar*」と設定した場合は「www.netstar.jp」および「www.netstar-inc.com」の両方が対象になります。
- 設定した宛先ホスト名と合致した場合は、必ずルートグループのユーザとして認証し、フィルタリングを行います。

4. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

5. [OK]ボタンをクリックします。

以上で、リクエスト別認証の設定は完了です。

5-7. LDAP サーバの登録と管理

ISWMは、複数のLDAPサーバを登録して連携できます。
ここでは、LDAPサーバの登録、管理について説明します。

■ LDAPサーバを登録する

LDAPサーバは、BASIC認証(LDAP連携)、NTLM認証またはKerberos認証設定後、次の手順で登録します。

1. [サーバ管理]-[LDAPサーバ設定]をクリックします。

[LDAPサーバ設定]が表示されます。

注意: [サーバ管理]-[LDAPサーバ設定]は、[サーバ管理]-[認証設定]-[認証方式]で[BASIC認証]-[LDAP連携を行う]または[NTLM認証]または[Kerberos認証]を設定した場合だけ、設定可能になります。認証設定方法については、「5-3. BASIC認証(LDAP連携)を設定する」(64ページ)または「5-4. NTLM認証を設定する」(65ページ)または「5-5. Kerberos認証を設定する」(69ページ)を参照してください。

---

2. [LDAPサーバ設定]タブの[サーバを登録]をクリックします。

[LDAPサーバ登録]が表示されます。

3. LDAPサーバの情報を入力します。

WindowsのActive Directoryと連携する場合、「認証設定」画面で設定した「LDAPグループ特定方式」によって、[検索ベース]、[管理者アカウント]、[検索フィルタ]の設定が異なります。「5-12. Active Directory連携時のLDAPサーバ設定」(89ページ)の設定例を参照して設定してください。

サーバ情報

ドメイン名 または NetBIOSドメイン名	• ドメイン名(BASIC認証時-LDAP連携/Kerberos認証時) 連携するLDAPサーバのドメイン名を入力します。 新しいドメインを登録する場合、[新規登録]をクリックし、ドメイン名(FQDN形式を推奨)を半角英数字で入力します。大文字、小文字は区別されるため、文字列は正確に指定してください。 登録済みドメイン名から選択する場合、[登録済み]をクリックし、プルダウンメニューからドメイン名を選択します。 • NetBIOSドメイン名(NTLM認証時) Active Directoryで設定したNetBIOSドメイン名を入力します。 新しいNetBIOSドメインを登録する場合、[新規登録]をクリックし、NetBIOSドメイン名を15文字以内の半角英数字、大文字で入力します。 登録済みドメイン名から選択する場合、[登録済み]をクリックし、プルダウンメニューからドメイン名を選択します。
IPアドレス/ホスト名	LDAPサーバのIPアドレスまたはホスト名を入力します。
ポート	LDAPサーバの接続ポート番号を入力します。 ポート番号は1～65535の間で設定してください。 初期値は389です。
接続方法	使用するプロトコルをLDAP/LDAPSから選択します。 LDAPSの標準ポート番号は636ですが、接続方法を切り替えた場合でも上記[ポート]で指定された値は自動的に変更されません。
検索ベース	LDAPのBASE情報をDNで入力します。
管理者アカウント	LDAPサーバのアカウントをDNで入力します。
パスワード	LDAPサーバにアクセスするときのパスワードを入力します。
パスワード(確認)	パスワードの確認入力をします。
Active Directoryオプション	[NetBIOS ドメイン名] に入力したドメインを、ドメインツリーの親ドメインとして検索対象に含めるか、フォレストの信頼関係として検索対象に含めるかを選択します。
検索フィルタ	[アカウント]にユーザアカウントの検索条件とスキーマをそれぞれ設定します。 [グループ]にグループの検索条件とスキーマをそれぞれ設定します。

アカウント追加属性	LDAPサーバに登録してあるメールアドレス、コメントを取り込むかどうかを設定します。コメントとするスキーマは自由に入力できます。

注意:
- [認証設定]画面のLDAPグループ特定方式で[グループ毎にユーザ抽出条件を指定する]を選択している場合、検索条件はアカウントだけが表示されます。
- LDAPサーバから取り込もうとしているユーザアカウントのDNを構成するスキーマの値には、「"」(ダブルクォート)または「\」(バックスラッシュ)は使用できません。
- LDAP 連携時、ユーザの抽出条件設定によっては同一名称のユーザアカウントが複数抽出されてしまう場合があります。ユーザアカウント名とするスキーマには、そのスキーマの値が必ず一意になるものを選択してください。
- ユーザの抽出条件の設定によっては、すでにISWMに登録されているユーザアカウント(例: root、guest)と重複するユーザアカウントが抽出されてしまうと、不具合を起こす場合があります。ユーザアカウント名にするスキーマには、そのスキーマの値が既存のユーザアカウント名(例: root、guest)と重複しない値を選択してください。
- 検索条件のスキーマリストに、任意のスキーマ(属性)名を利用できます。
  スキーマを追加するには、<インストールディレクトリ>/conf/proxy.inf を編集し、SCHEMA_LIST キーにカンマ区切りでスキーマを追加してください。

```
[LDAP]
SCHEMA_LIST=ou,cn,name,dc,sn,givenName,uid,o,sAMAccountName,mail,user
PrincipalName
```

4. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [前画面へ戻る]ボタンをクリックすると、LDAPサーバを登録しないで[LDAPサーバ設定]に戻ります。

5. [OK]ボタンをクリックします。

「登録が完了しました。」と表示されます。

■ LDAPサーバを変更、削除する

LDAPサーバの変更、削除は、以下の手順で行います。

1. [サーバ管理]-[LDAPサーバ設定]をクリックします。

   [LDAPサーバ設定]が表示されます。

   注意: [サーバ管理]-[LDAPサーバ設定]は、[サーバ管理]-[認証設定]-[認証方式]で[BASIC認証]-[LDAP連携を行う]または[NTLM認証]または[Kerberos認証]を設定した場合だけ、設定可能になります。認証設定方法については、「5-3. BASIC認証(LDAP連携)を設定する」(64ページ)または「5-4. NTLM認証を設定する」(65ページ)または「5-5. Kerberos認証を設定する」(69ページ)を参照してください。

2. [LDAPサーバ設定]タブの[LDAPサーバ情報]で、変更または削除するLDAPサーバの[選択]ボタンをクリックします。

   [LDAPサーバ編集]が表示されます。

3. LDAPサーバを削除する場合は[削除]ボタンを、サーバ情報を変更する場合は必要項目を変更して[保存]ボタンをクリックします。

   設定項目の説明と変更方法については、「5-7. LDAPサーバの登録と管理」(73ページ)を参照してください。
   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

5-8. LDAP サーバの冗長構成への対応について

複数のLDAPサーバを登録した場合、連携しているLDAPサーバが一部停止してもアカウント認証を継続することができます。
プライマリサーバの管理サービスが定期的にLDAPサーバの状態を監視し、LDAPサーバが停止していて応答がない場合に自動的に切り離すための条件を設定したり、接続が可能になったLDAPサーバを再接続するための条件を設定することで、認証処理の待ち状態を制御することができます。
LDAPサーバの自動切り離し・再接続の条件を設定するための操作については、「5-10. LDAPサーバとの連携を設定する」(79ページ)を参照してください。
接続可能となったLDAPサーバを管理画面から手動で再接続する場合の操作については、「5-9. LDAPサーバの連携優先順位を変更する」(77ページ)を参照してください。

5-9. LDAP サーバの連携優先順位を変更する

BASIC認証(LDAP連携)、NTLM認証またはKerberos認証設定後、登録したLDAPサーバの連携優先順位を変更します。

1. [サーバ管理]-[LDAPサーバ設定]をクリックします。

[LDAPサーバ設定]が表示されます。登録したLDAPサーバが、連携優先順位の昇順に表示されます。

注意: [サーバ管理]-[LDAPサーバ設定]は、[サーバ管理]-[認証設定]-[認証方式]で[BASIC認証]-[LDAP連携を行う]または[NTLM認証]または[Kerberos認証]を設定した場合だけ、設定可能になります。認証設定方法については、「5-3. BASIC認証(LDAP連携)を設定する」(64ページ)または「5-4. NTLM認証を設定する」(65ページ)または「5-5. Kerberos認証を設定する」(69ページ)を参照してください。

---

2. [LDAPサーバ情報]タブの[LDAPサーバ情報]でLDAPサーバの連携優先順位を変更します。

[LDAPサーバ情報]に表示されている各行をドラッグアンドドロップすることによって優先順位を変更することができます。変更のイメージを以下に示します。

<同一ドメイン名(または同一NetBIOSドメイン名)内のサーバの優先順位の変更>

「IPアドレス/ホスト名」の部分をドラッグアンドドロップすることで、同一ドメイン名(または同一NetBIOSドメイン名)の範囲でサーバの優先順位を変更することができます。この場合、異なるドメインの優先順位は変更できません。

<ドメイン名(またはNetBIOSドメイン名)単位での優先順位の変更>

「ドメイン名」(またはNetBIOSドメイン名)の部分をドラッグアンドドロップすることで、ドメイン単位で優先順位を変更することができます。この場合、ドメイン内のサーバの優先順位は変更できません。

3. [有効]ボタンまたは[無効]ボタンをクリックして、LDAPサーバの状態を切り替えます。

メンテナンス等でLDAPサーバを停止する場合、連携対象外にすることで、一時的に切り離すことができます。[有効]ボタンをクリックすると、連携対象になります。[無効]ボタンをクリックすると連携対象外になります。

注意: 接続が不可能になったLDAPサーバの自動切り離しが行われた場合、「接続状態」の[再接続]ボタンが有効になります。[再接続]ボタンをクリックすると切り離したLDAPサーバに再接続を試行します。LDAPサーバの自動切り離し・再接続の条件を設定するための操作については、「5-10. LDAP サーバとの連携を設定する」(79ページ)を参照してください。

4. [連携情報更新]の[更新]ボタンをクリックして、グループの同期を行います。

5. [OK]ボタンをクリックします。

以上で、LDAPサーバの連携優先順位の変更は完了です。

■ 連携優先順位に基づいて各LDAPサーバへ分散させる場合

複数のLDAPサーバが登録されていて、連携優先順位に基づいて接続先を各LDAPサーバに分散したい場合には、次の手順で設定します。

1. [サーバ管理]-[認証設定]をクリックします。

   ［認証設定］が表示されます。

2. [LDAP接続先分散]のチェックボックスをオンにします。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

以上で、連携優先順位に基づいて接続先を各LDAPサーバに分散する設定は完了です。

5-10. LDAP サーバとの連携を設定する

LDAP サーバの連携優先順位を変更後、変更した優先順位に従って、自動連携の設定や自動切り離し・自動再接続に関する条件を設定します。

1. [サーバ管理]-[LDAPサーバ設定]をクリックします。

   [LDAPサーバ設定]が表示されます。

> **注意:** [サーバ管理]-[LDAPサーバ設定]は、[サーバ管理]-[認証設定]-[認証方式]で[BASIC認証]-[LDAP連携を行う]または[NTLM認証]または[Kerberos認証]を設定した場合だけ、設定可能になります。認証設定方法については、「5-3. BASIC認証(LDAP連携)を設定する」(64ページ)または「5-4. NTLM認証を設定する」(65ページ)または「5-5. Kerberos認証を設定する」(69ページ)を参照してください。

2. [LDAPサーバ設定]タブで、LDAPサーバとの連携に関する以下の情報を設定します。

[LDAPサーバ情報]

ドメイン名 または NetBIOSドメイン名	• ドメイン名(BASIC認証時-LDAP連携/Kerberos認証時) 連携するLDAPサーバのドメイン名を入力します。 半角英数字と「_」、「-」が使用できます(大文字と小文字が区別されます)。 • NetBIOSドメイン名(NTLM認証時) Active Directoryで設定したNetBIOSドメイン名を15文字以内で入力します。 半角英数大文字と「_」、「-」が使用できます(小文字入力時は登録時自動的に大文字に変更されます)。
IPアドレス/ホスト名	LDAPサーバのIPアドレス/ホスト名が表示されます。変更する場合は、[選択]ボタンをクリックします。
検索ベース	LDAPサーバに設定してある検索ベースが表示されます。変更する場合は、[選択]ボタンをクリックします。

3. LDAPサーバと自動連携する場合のタイミングについて設定します。

[自動連携]-[自動連携設定]

自動更新	LDAPサーバのグループ構造を定期的にインポートするかどうかを選択します。自動連携設定については、「LDAPサーバとの自動連携設定」(82ページ)を参照してください。
更新時刻	LDAPサーバのグループ構造をインポートする時刻を設定します。 最大で1日3回インポートする時刻を指定できます。

注意:
- すぐにLDAPサーバのグループ構造をインポートする場合は、[連携情報更新]-[連携情報更新]の[更新]ボタンをクリックしてください。
- [認証設定]画面のLDAPグループ特定方式で[グループ毎にユーザ抽出条件を設定する]を選択している場合、自動連携設定、連携情報更新は表示されません。また、自動連携設定が有効に設定されていても、動作しません。

4. LDAPサーバの自動切り離し・自動再接続に関する条件を設定します。

プライマリサーバの管理サービスが定期的にLDAPサーバの状態を監視して、LDAPサーバが停止していて応答がない場合に自動的に切り離したり、再接続したりする条件を設定します。

自動管理	プライマリサーバの管理サービスが連携するLDAPサーバの状態監視により、サーバの自動切り離し・自動再接続を行う場合に[有効]チェックボックスをオンにします。
自動切り離し条件	接続が不可能になったLDAPサーバの自動切り離しを行う監視失敗回数のしきい値を、1～100000回の範囲で設定します。
自動再接続条件	接続が可能になったLDAPサーバの自動再接続を行う監視成功回数のしきい値を、1～100000回の範囲で設定します。

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

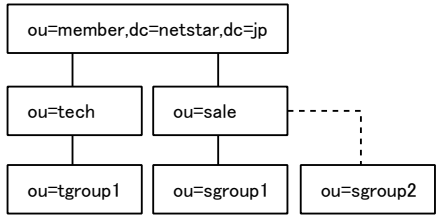
6. [OK]ボタンをクリックします。

以上で、LDAPサーバとの連携設定は完了です。

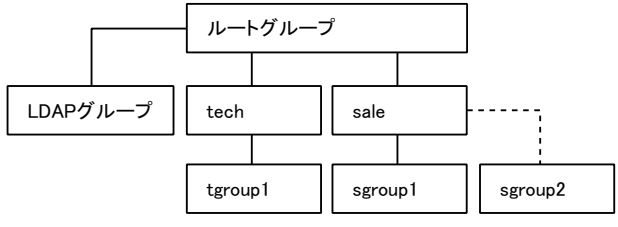
■ LDAPサーバとの自動連携設定

LDAP サーバとの自動連携機能を使用することで、LDAP サーバに登録されたグループおよびユーザに対して、適切なフィルタリングの設定を自動で適用します。
LDAPサーバとの自動連携を設定すると、LDAPサーバの組織構成をインポートし、ISWMで利用するグループを自動構築します。

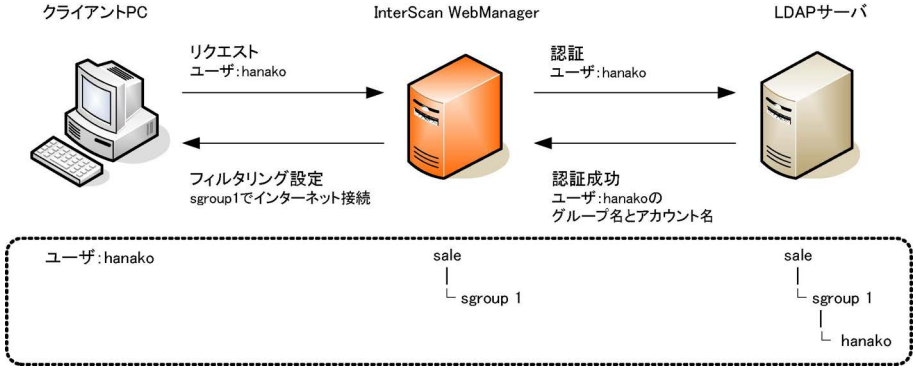
LDAP 側での組織構成



ISWM で自動構築されるグループ



このとき ISWM 側でユーザ情報は作成されません。空のグループだけが作成されます。このグループに対して適宜フィルタリングの設定を適用します。フィルタリングの設定については、「第4章 フィルタリング設定について」(158ページ)を参照してください。
LDAP連携を設定している場合、ISWMにインターネットの接続要求があると、まずLDAPサーバで認証をします。LDAP サーバに登録されているユーザの場合は、アカウント名とグループ名がISWMに通知されます。



ユーザhanakoはISWMに登録されていませんが、sgroup1グループのユーザとしてフィルタリングをします。
ISWM は、受け取ったアカウント名が登録されていれば、そのアカウントのフィルタリングルールを参照します。アカウント名が登録されていない場合は、受け取ったグループ名のフィルタリングルールを参照します。グループも登録されていない場合は、認証エラーまたは未登録ユーザとしてフィルタリングをします。
LDAPサーバで新たにグループが追加された場合は、次回の自動更新時にISWMに追加されます。追加されたグループのフィルタリングルールは、上位グループの設定がコピーされます。
第一階層のグループが追加された場合は、ルートグループのフィルタリングルールがコピーされます。

注意:
- [認証設定]画面のLDAPグループ特定方式で[グループ毎にユーザ抽出条件を設定する]を選択している場合、自動連携設定は使用できません。
- LDAPサーバとの自動連携では、グループ単位でフィルタリングルールを設定します。アカウント単位では設定できません。ユーザにフィルタリングルールを設定したい場合や、グループ管理者を設定したい場合は、LDAPサーバとの同期を実行し、アカウント情報をISWMにインポートしてください。インポート後にユーザなどの設定ができるようになります。
- インポートしたアカウントを、別の任意のグループに移動することもできます。アカウントを移動した場合は、移動後のグループのフィルタリングルールが適用されます。

5-11. LDAP サーバと同期する

BASIC認証(LDAP連携)、NTLM認証またはKerberos認証設定後、登録したLDAPサーバをISWMと同期させます。LDAPサーバとの同期設定は、[認証設定]画面で選択したLDAPグループ特定方式の設定により異なります。

■ ユーザのDNからグループ階層を特定する場合

[認証設定]画面で[LDAPグループ特定方式]に[ユーザのDNからグループ階層を特定する]を選択した場合、次の手順でLDAPサーバとの同期設定をします。

注意: LDAPサーバと自動連携する場合、同期設定をしなくても運用できます。この場合には、グループ情報だけを自動連携で同期してください。

1. [グループ/ユーザ管理]-[LDAPユーザ同期]をクリックします。

   [LDAPユーザ同期]が表示されます。

   注意: [グループ/ユーザ管理]-[LDAPユーザ同期]は、[サーバ管理]-[認証設定]-[認証方式]で[BASIC認証]-[LDAP連携を行う]または[NTLM認証]または[Kerberos認証]を設定した場合だけ、設定可能になります。認証設定方法については、「5-3. BASIC認証(LDAP連携)を設定する」(64ページ)または「5-4. NTLM認証を設定する」(65ページ)または「5-5. Kerberos認証を設定する」(69ページ)を参照してください。

2. [ユーザ情報同期]-[未登録アカウント一覧]で、LDAPサーバと同期するアカウント、グループのチェックボックスをオンにして[登録]ボタンをクリックします。

   [登録]ボタンをクリックすると、選択したアカウント情報およびグループ構造が、ISWMにインポートされます。
   [全登録]ボタンをクリックすると、[未登録アカウント一覧]のすべてのアカウント情報およびグループ構造が、ISWMにインポートされます。

   注意: LDAP連携を設定すると、アカウントやパスワードの認証はLDAPサーバで実行されます。ISWM ではパスワードなどの情報を持たないため、アカウントの登録/削除、パスワードの変更はできません。IPアドレスをユーザ名として登録したユーザは、登録/削除できます。

LDAPサーバから削除されたアカウントやグループは、[削除候補アカウント一覧]に表示されます。
ISWMのグループ/ユーザ情報からも削除する場合、削除するアカウント、グループを選択して[削除]ボタンをクリックしてください。
[全削除]ボタンをクリックすると、一覧に表示されているアカウント、グループをすべて削除します。

以上で、LDAPサーバ同期の設定は完了です。
LDAPサーバでの認証に失敗したアカウントは、[認証設定]-[未登録ユーザ設定]の設定によって、適用されるフィルタリングルールが異なります。

設定	適用されるフィルタリングルール
未登録ユーザ設定が有効に設定されている場合	未登録ユーザのフィルタリング設定が適用されます。
未登録ユーザ設定が無効に設定されている場合	ISWMでの認証は無効になり、エラー画面が表示されます。

■ グループごとにユーザ抽出条件を指定する場合

[サーバ管理]-[認証設定]-[LDAPグループ特定方式]で[グループ毎にユーザ抽出条件を指定する]を選択した場合のLDAPサーバとの同期設定について説明します。

● グループにユーザを取り込む条件を設定する

グループごとにユーザを取り込む条件、および、同一ユーザが複数のグループに所属する場合に取り込むグループの優先順位を設定します。

注意: ユーザを取り込む条件およびグループ登録の優先順位はシステム管理者(ADMINグループに所属するユーザ)のみ設定できます。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。

   [グループ管理]が表示されます。

2. グループ一覧から、抽出条件を設定するグループ名をクリックします。

   設定画面にグループの設定内容が表示されます。グループ一覧で下の階層を開くには、グループ名の[+]をクリックします。

3. [LDAP設定]タブをクリックします。

4. [編集]ボタンをクリックします。

   [LDAP設定編集]が表示されます。

5. [アカウント抽出条件を設定する]チェックボックスをオンにします。

   注意: [アカウント抽出条件を設定する]チェックボックスをオンにしたグループに対してのみ、ユーザの取り込みを行います。該当するグループがない場合、「LDAP」グループとして取り込みを行います。

6. グループに取り込むアカウントの条件と、優先順位を設定します。

   「グループごとにユーザ抽出条件を指定する場合」(85ページ)を参照して、属性名と属性値を設定してください。
   また、[↑]、[↓]ボタンをクリックすると、取り込む優先順位が高い順にグループを並び替えできます。

   注意:
   - Active Directory のセキュリティグループからアカウントを抽出する場合、属性名は「memberOf」に設定してください。
   - アカウント抽出条件と優先順位は LDAP サーバと同期するときにも変更できます。
   - グループを新規登録する場合、登録するグループは「/ 新規登録グループ /」として表示されます。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   LDAPグループ特定条件の設定が有効になります。

以上で、LDAPサーバからユーザを抽出して、ISWMのグループに取り込む条件の設定が完了しました。続いて、LDAPサーバと同期して、ユーザをISWMのグループに取り込みます。

● LDAP サーバと同期してユーザ情報を取り込む

LDAPサーバとの連携設定、グループユーザを取り込む条件の設定が完了したら、LDAPサーバと同期してユーザ情報をISWMに取り込みます。

注意:
- [サーバ管理]-[認証設定]-[LDAPグループ特定方式]で[グループ毎にユーザ抽出条件を指定する]を選択した場合、LDAPサーバとの自動連携はできません。
  LDAPサーバでアカウントの変更が発生した場合には、[LDAPユーザ同期]画面で再度ユーザ情報を取り込んでください。
- 認証に成功していて、ISWM に取り込まれていないユーザは、LDAP グループのフィルタリング設定が適用されます。

1. [グループ/ユーザ管理]-[LDAPユーザ同期]をクリックします。

[LDAPユーザ同期]画面が表示されます。

2. [ユーザ情報同期]でLDAPサーバから取り込むアカウントと、アカウントが取り込まれるISWMのグループを確認します。

[グループ特定条件]でグループ名をクリックすると、抽出条件を変更できます。変更後、[保存]ボタンをクリックすると、変更した条件でアカウント情報が抽出されます。

グループ特定条件を一括してインポートする場合は、一括処理の[参照] ボタンをクリックしてファイルを選択します。

次に[ファイル文字コード]プルダウンメニューから、ファイル文字コード(UTF-8、Shift_JIS、EUC_JP)を選択して[実行]ボタンをクリックしてください。

処理結果の画面が、別ウィンドウで表示されます。

[閉じる]ボタンをクリックすると、処理結果の画面が閉じます。

注意:
- インポートする場合は、既存の内容が削除されます。
- インポートを行った場合は、[保存] ボタンをクリックしなくとも内容が保存されます。

3. [ユーザ情報同期]-[未登録アカウント一覧]でLDAPサーバと同期するアカウント、グループを選択して[登録]ボタンをクリックします。

[登録]ボタンをクリックすると、選択したアカウント情報が、設定したグループに取り込まれます。
[全登録]ボタンをクリックすると、すべてのアカウント情報が、設定したグループに取り

込まれます。

注意: LDAP連携を設定すると、アカウントやパスワードの認証はLDAPサーバで実行されます。ISWM ではパスワードなどの情報を持たないため、アカウントの登録/削除、パスワードの変更はできません。IP アドレスをユーザ名として登録したユーザは、登録/削除できます。

LDAPサーバから削除されたアカウントやグループは、[削除候補アカウント一覧]に表示されます。
ISWMのグループ/ユーザ情報からも削除する場合、削除するアカウント、グループを選択して[削除]ボタンをクリックしてください。
[全削除]ボタンをクリックすると、一覧に表示されているアカウント、グループをすべて削除します。

以上で、LDAPサーバの同期設定は完了です。
未登録アカウントは、設定したアカウント抽出条件に一致するグループの有無によって、適用されるフィルタリングルールが異なります。

設定	適用されるフィルタリングルール
一致するグループがある場合	抽出条件に一致するグループのフィルタリング設定が適用されます。 一致するグループが複数ある場合、優先順位の高いグループの設定が適用されます。
一致するグループがない場合	LDAPグループのフィルタリング設定が適用されます。

5-12. Active Directory 連携時の LDAP サーバ設定

ユーザ認証方式としてNTLM認証またはKerberos認証を選択した場合、LDAP グループ特定方式によって「検索ベース」、「管理アカウント」、「検索条件」の設定が異なります。
それぞれの特定方式にあわせて設定してください。

■ ユーザのDNからグループ階層を特定する場合

WindowsのAcitvie Directoryと連携する場合、[サーバ管理]-[LDAPサーバ設定]-[サーバを登録]で、Active Directoryの設定にあわせてISWMの「検索ベース」と「管理者アカウント」を設定してください。

Active Directory での設定例

ドメインの名前空間	tsr_test.netstar.jp
すべてのユーザが所属するルートグループ	root_group
管理者アカウント	yamada

管理者アカウントは、usersディレクトリの「Domain Users」に所属するメンバーです。

ISWM での設定例

検索ベース	ou=root_group,dc=tsr_test,dc=netstar,dc=jp
管理者アカウント	cn=yamada,cn=users,dc=tsr_test,dc=netstar,dc=jp

スキーマの設定例

スキーマを設定することで、無効になっているコンピュータ名やユーザを取り込まないように設定できます。次の設定例を参考に、ご利用の環境にあわせてスキーマを設定してください。

Active Directory のログイン名を取得する検索文字列の場合

アカウント	(&(objectClass=user)(sAMAccountName=*))
グループ	(&(objectClass=top)(ou=*))

Active Directory でパスワードロックされたユーザは取得しない場合

アカウント	(&(&(objectClass=user)(!(lockoutTime>=1)))(sAMAccountName=*))
グループ	(&(objectClass=top)(ou=*))

Active Directory で「無効」になっているユーザ以外を検索する検索文字列の場合

アカウント	(&(&(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))(sAMAccountName=*))
グループ	(&(objectClass=top)(ou=*))

OU 配下にユーザとコンピュータが存在していた場合、ユーザのみ抽出する場合

アカウント	(&(&(objectClass=user)(!(objectClass=computer)))(sAMAccountName=*))
グループ	(&(objectClass=top)(ou=*))

指定したセキュリティグループに属するユーザを検索する文字列の場合

例) ベースで指定した配下に存在するユーザで、セキュリティグループ「test1」または「test2」に所属しているユーザ

アカウント	(&(|(&(objectClass=user)(memberOf=CN=test1,OU=OU1,OU=OU_MT,DC=supportech,DC=netstar-inc,DC=com))(&(objectClass=user)(memberOf=CN=test2,OU=OU1,OU=OU_MT,DC=supportech,DC=netstar-inc,DC=com)))(sAMAccountName=*))
グループ	(&(objectClass=top)(ou=*))

注意: ユーザアカウントのDNを構成するスキーマの値には「"」(ダブルクォート)または「\」(バックスラッシュ)は使用できません。ただしエスケープコードとして記述した場合は使用できます。

■ グループごとにユーザ抽出条件を指定する場合

WindowsのActive Directoryと連携する場合、[サーバ管理]-[LDAPサーバ設定]-[サーバを登録]で、Active Directoryの設定にあわせてISWMの「検索ベース」と「管理者アカウント」を設定してください。

Active Directory での設定例

ドメインの名前空間	tsr_test.netstar.jp
すべてのユーザが所属するルートグループ	root_group
管理者アカウント	yamada

管理者アカウントは、usersディレクトリの「Domain Users」に所属するメンバーです。

ISWM での設定例

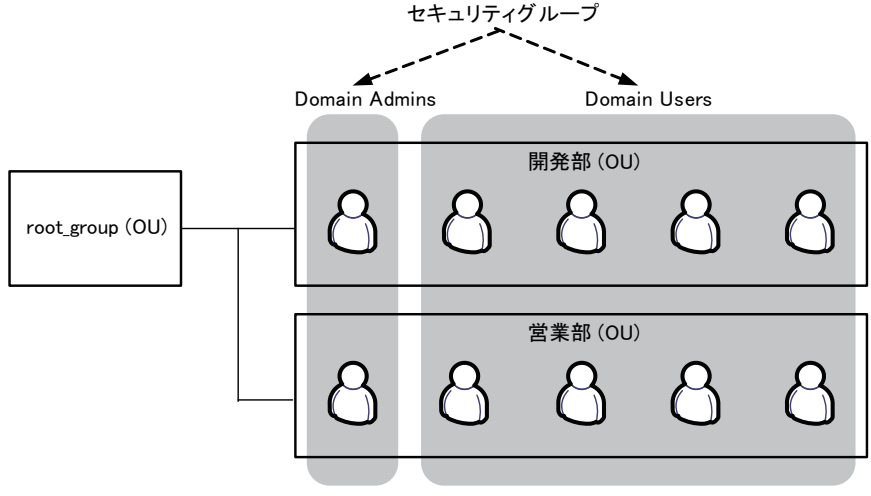
検索ベース	ou=root_group,dc=tsr_test,dc=netstar,dc=jp
管理者アカウント	cn=yamada,cn=users,dc=tsr_test,dc=netstar,dc=jp
アカウント	(&(objectClass=user)(sAMAccountName=*))

ユーザ抽出条件の設定例

次の設定例を参考に、ご利用の環境にあわせてユーザ抽出条件を設定してください。

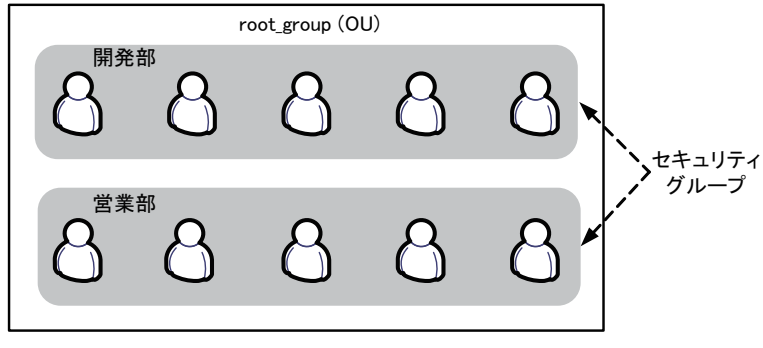
注意:
- 設定例ではルートグループ (root_group) にセキュリティグループを作成していますが、セキュリティグループは任意の場所に作成できます。
- 属性名が「memberOf」の場合には、セキュリティグループをインポートします。属性名を変更することにより、セキュリティグループ以外の情報でもインポートできます。たとえば、属性名を「cn」、属性値を「yamada」に設定すると、「yamada」だけをインポートします。ただし、検索範囲がユーザのプロパティの内部となるため、「ou」や「営業部」などを指定してもインポートできません。
- 部署の構造を Active Directory で「組織単位 (OU)」として登録し、プロジェクトごとにセキュリティグループを作成する管理方法などもあります。
- Active Directory 側で、ユーザの所属するセキュリティグループを「プライマリグループ」に設定すると、「memberOf」属性が削除されるため[グループ毎にユーザ抽出条件を指定する]でユーザの所属するグループが抽出できなくなります。

Active Directory 側で、部署の構造を組織単位 (OU) で登録し、部署ごとの管理者 (アドミニストレータ) をセキュリティグループ「Domain Admins」として設定している場合



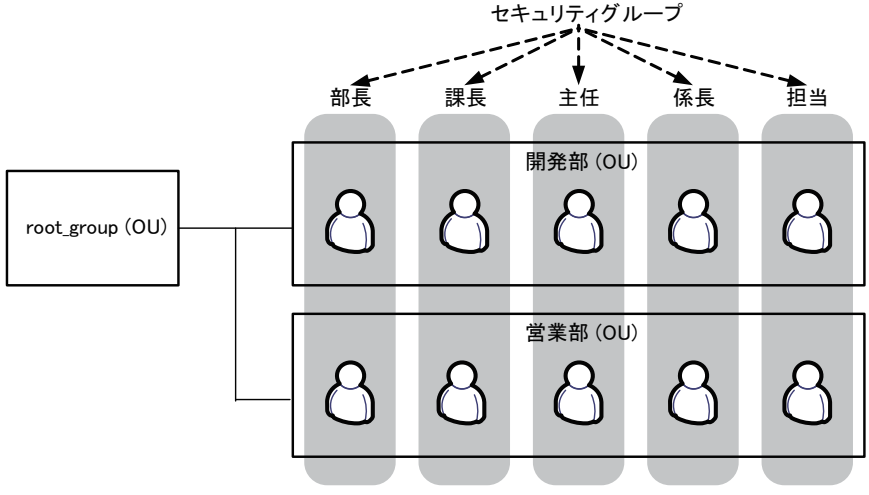
セキュリティグループ	属性値
Domain Admins	cn=Domain Admins,ou=root_group,dc=tsr_test,dc=netstar,dc=jp

部署ごとにセキュリティグループを設定している場合



部署名 (セキュリティグループ)	属性値
開発部(dev_user)	cn=dev_user,ou=root_group,dc=tsr_test,dc=netstar,dc=jp
営業部(sales_user)	cn=sales_user,ou=root_group,dc=tsr_test,dc=netstar,dc=jp

役職ごとにセキュリティグループを設定している場合



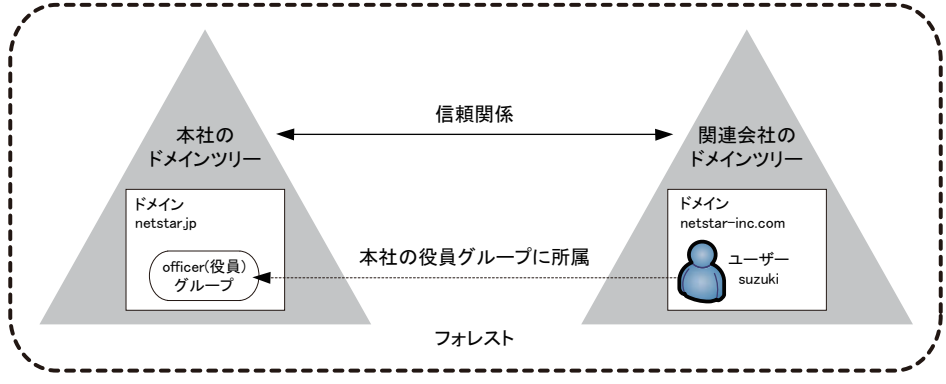
役職名 (セキュリティグループ)	属性値
部長(division_head)	cn=division_head,ou=root_group,dc=tsr_test,dc=netstar,dc=jp
課長(section_head)	cn=section_head,ou=root_group,dc=tsr_test,dc=netstar,dc=jp
係長(assistant_manager)	cn=assistant_manager,ou=root_group,dc=tsr_test,dc=netstar,dc=jp
主任(senior_staff)	cn=senior_staff,ou=root_group,dc=tsr_test,dc=netstar,dc=jp
社員(staff)	cn=staff,ou=root_group,dc=tsr_test,dc=netstar,dc=jp

注意: 複数のセキュリティグループに登録している場合は優先度を設定できます。

■ フォレスト内でセキュリティグループとユーザが別のドメインに所属している場合

フォレスト内でセキュリティグループとユーザがそれぞれ別のドメインに所属している場合でも、信頼関係で結ばれたドメイン間であれば、ISWM のグループにセキュリティグループを割り当てて、ユーザを抽出できるようになります。
[サーバ管理]-[LDAPサーバ設定]-[LDAPサーバ登録]で、「Active Directoryオプション」の[このドメインをフォレストの信頼関係として検索対象に含める] チェックボックスをオンにしてください。

関連会社のユーザが、本社の役員セキュリティグループに所属している場合



次の設定例を参考に、ご利用の環境にあわせてユーザ抽出条件を設定してください。

Active Directory での設定例（セキュリティグループの所属するドメイン）

セキュリティグループが所属するドメインの名前空間	tsr_test.netstar.jp
セキュリティグループが所属するルートグループ	root_group
セキュリティグループの名前	officer（役員）

Active Directory での設定例（ユーザの所属するドメイン）

ユーザが所属するドメインの名前空間	kr_test.netstar-inc.com
ユーザが所属するルートグループ	root_group
ユーザの名前	suzuki

ISWM での LDAP サーバ設定例（セキュリティグループが所属するドメイン）

検索ベース	dc=tsr_test,dc=netstar,dc=jp

注意: 検索ベースは ForeignSecurityPrincipals が存在する階層よりも上の階層を指定する必要があるため、必ずドメインのトップで指定してください。

ISWM での LDAP サーバ設定例（ユーザが所属するドメイン）

検索ベース	ou=root_group,dc=kr_test,dc=netstar-inc,dc=com

ISWM でのグループのアカウント抽出条件の設定例

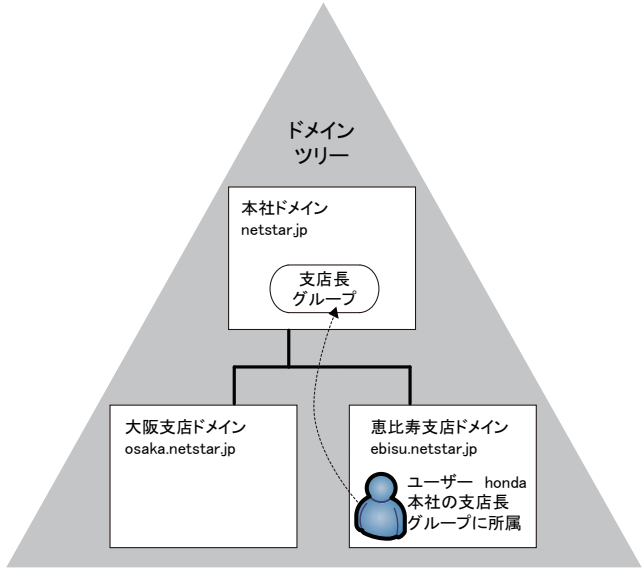
属性名	属性値
memberOf	cn=officer,ou=root_group,dc=tsr_test,dc=netstar,dc=jp

■ ドメインツリーでセキュリティグループとユーザが別のドメインに所属している場合

ドメインツリー内でセキュリティグループとユーザがそれぞれ別のドメインに所属している場合でも、ISWM のグループにセキュリティグループを割り当てて、ユーザを抽出できるようになります。

[サーバ管理]-[LDAPサーバ設定]-[LDAPサーバ登録]で、「Active Directoryオプション」の[このドメインをドメインツリーの親ドメインとして検索対象に含める]チェックボックスをオンにしてください。

支店ドメインのユーザが、本社の支店長セキュリティグループに所属している場合



次の設定例を参考に、ご利用の環境にあわせてユーザ抽出条件を設定してください。

Active Directory での設定例（セキュリティグループの所属するドメイン）

セキュリティグループが所属するドメインの名前空間	tsr_test.netstar.jp
セキュリティグループが所属するルートグループ	root_group
セキュリティグループの名前	manager（支店長）

Active Directory での設定例（ユーザの所属するドメイン）

ユーザが所属するドメインの名前空間	kr_test.netstar-inc.com
ユーザが所属するルートグループ	root_group
ユーザの名前	honda

ISWM での LDAP サーバ設定例（セキュリティグループが所属するドメイン）

検索ベース	dc=tsr_test,dc=netstar,dc=jp

注意: 検索ベースは ForeignSecurityPrincipals が存在する階層よりも上の階層を指定する必要があるため、必ずドメインのトップで指定してください。

ISWM での LDAP サーバ設定例（ユーザが所属するドメイン）

検索ベース	ou=root_group,dc=kr_test,dc=netstar-inc,dc=com

ISWM でのグループのアカウント抽出条件の設定例

属性名	属性値
memberOf	cn=manager,ou=root_group,dc=tsr_test,dc=netstar,dc=jp

6. メール通知設定

6-1. メール通知の設定をする

ISWMではライセンスの期限切れなどの通知メールを、あらかじめ登録したメールアドレスに送信できます。
また、プライマリサーバとレプリカサーバの通信障害やフィルタリングサービスの起動/停止の失敗など、サービスに異常が発生した場合、サービス異常発生の通知メールを送信できます。
メール通知は、次の手順で設定します。

1. [サーバ管理]-[メール通知設定]をクリックします。

   [メール通知設定]が表示されます。

2. [メール通知機能]で[有効]チェックボックスをオンにします。

3. メール送信の設定をします。

   メール送信の際に必要なSMTPサーバ情報を入力します。暗号化を利用する場合は、[暗号化方式]の[SSL方式]または[TLS方式]を選択します。メール送信に認証がある場合、[認証]で[使用する]チェックボックスをオンにし、アカウントやパスワードなどの認証情報も入力します。

4. [メール通知詳細]で、送信するメールのチェックボックスをオンにします。

メールの種類

ライセンス期限切れ事前通知	ISWMのライセンスキーが180日以内に期限切れになる場合、以下の日程で通知メールを送信します。 180、90、60、30、21、14、7、3、2、1日前
サービス異常発生通知	次のような異常発生を検知した場合、通知メールを送信します。 • プライマリサーバとレプリカサーバの通信に失敗 • フィルタリングサービスの起動、停止処理に失敗 • URLデータベースのロードに失敗
サービス警告発生通知	次のような警告発生を検知した場合、通知メールを送信します。 • ISWMをインストールしたディスクの空き容量が所定のしきい値(10、5、3、2、1%)を下回った場合 • LDAPサーバの自動切り離しが行われた場合 • プロセス使用率が指定されたしきい値を超えた場合

サービス情報通知	LDAP サーバの自動接続が行われた場合、通知メールを送信します。
設定変更通知	管理画面で ISWM の設定が変更された場合、通知メールを送信します。

5. 選択した通知メールを送信する宛先と件名を入力します。

   宛先を複数登録する場合は「,」(半角カンマ)で区切ってメールアドレスを入力してください。

6. 画面右上の[保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

以上で、メール通知設定は完了です。
メールの誤配信を防止するため、次の「6-2. 通知メールをテスト送信する」(99 ページ)でテストメールを送信してください。

注意: POP before SMTPには対応していません。

6-2. 通知メールをテスト送信する

1. [サーバ管理]-[メール通知設定]をクリックします。

   [メール通知設定]が表示されます。

2. [テスト送信]の[送信]ボタンをクリックします。

   確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

以上で、テストメールの送信は完了です。
宛先に正しく送信されているか確認してください。

7. 上位プロキシ設定

ここでは、上位プロキシ設定について説明します。

注意: 上位プロキシの設定は、システム管理者のみ行うことができます。

7-1. 上位プロキシの設定をグループ別に有効にする

グループごとに、個別に異なる上位プロキシを使用するように設定します。
上位プロキシの設定をグループ別に有効にする手順を以下に説明します。

1. [サーバ管理]-[上位プロキシ設定]をクリックします。

   [上位プロキシ設定]が表示されます。

2. [グループ別のプロキシ設定を有効にする]チェックボックスをオンにします。

3. [保存]ボタンをクリックします。

   [グループ/ユーザ管理]-[グループ管理]-[ネットワーク設定]で設定した、上位プロキシ設定の内容が表示されます。グループごとに、以下のいずれかが表示されます。
   - システム共通の設定を使用する
   - 上位グループと同じ設定を使用する
   - 上位プロキシを使用しない

   [ネットワーク設定]で[グループで個別に設定を行う]を選択した場合は、[プロトコル]、[ホスト]、[ポート]が表示されます。

   注意: グループごとに上位プロキシを設定する方法については、「3-4. グループにネットワーク設定をする」(135ページ)を参照してください。

7-2. 上位プロキシの条件を設定する

リクエスト元(IPアドレス/グループ名)や、アクセス先(宛先ホスト/宛先IPアドレス/カテゴリ)ごとに個別に異なる上位プロキシを使用するように設定します。
上位プロキシの条件を設定するための手順を以下に説明します。

1. [サーバ管理]-[上位プロキシ設定]をクリックします。

   [上位プロキシ設定]が表示されます。

2. [上位プロキシ条件設定]の[追加]ボタンをクリックします。

条件を設定する画面が表示されます。条件を設定する画面は以下の3つのタブで構成されています。

- [条件]タブ
- [プロキシ]タブ
- [設定先]タブ

3. [条件]タブで[種類]と[値]を入力します。

種類には、[宛先ホスト]、[宛先IPアドレス]、[リクエスト元IP]、[リクエストグループ]および[カテゴリ]があります。条件を複数設定する場合は[条件の追加]をクリックします。

注意:
- [条件]タブで何も設定しなかった場合は、[条件]欄に「すべて」と表示され、すべてのリクエストに設定したプロキシが適用されます。
- [宛先ホスト]の設定では、ラジオボタンでいずれかを選択します。
  ホスト名によるリクエストを対象とする
  ホスト名によるリクエストとIPアドレスによるリクエストの逆引き結果ホスト名を対象とする

  ドメイン名の逆引きリクエストはISWMおよびDNSサーバの負荷上昇の原因になる場合がありますのでご注意ください。
- [宛先IPアドレス]の設定では、ラジオボタンでいずれかを選択します。
  IPアドレスによるリクエストを対象とする
  IPアドレスによるリクエストとホスト名によるリクエストの正引き結果IPアドレスを対象とする

4. [プロキシ]タブで、上位プロキシの使用可否を設定します。

使用しない	インターネットへの接続において上位プロキシサーバを利用しない場合は、このラジオボタンをオンにします。
単一サーバのみ使用	インターネットへの接続において単一の上位プロキシサーバを利用する場合は、このラジオボタンをオンにします。続けて、プライマリの[ホスト]と[ポート]を入力します。[ホスト]と[ポート]は両方入力してください。 すべてのプロトコル(HTTP/HTTPS/FTP over HTTP)に同じプロキシサーバを使用する場合は、[すべてのプロトコルで同じプロキシサーバを使用する]チェックボックスをオンにして[ホスト]と[ポート]を入力します。

ホットスタンバイ	インターネットへの接続において複数の上位プロキシサーバをホットスタンバイで利用する場合は、このラジオボタンをオンにします。続けて、プライマリおよびセカンダリの[ホスト]と[ポート]を入力します。[ホスト]と[ポート]は両方入力してください。 すべてのプロトコル(HTTP/HTTPS/FTP over HTTP)に同じプロキシサーバを使用する場合は、[すべてのプロトコルで同じプロキシサーバを使用する]チェックボックスをオンにして[ホスト]と[ポート]を入力します。

注意: 上位プロキシサーバには、障害時のネットワーク切断を回避するために、プライマリとセカンダリの2台の上位プロキシサーバを指定してホットスタンバイ構成にすることができます。これにより、プライマリに接続できなかった場合、それ以降、セカンダリを使用するようになります。セカンダリを使用していてプライマリに接続できた場合は、それ以降、プライマリを使用するようになります。

5. [設定先]タブで、設定対象のサーバを選択します。

すべてのサーバに対して共通で設定する場合は、「全てのサーバ」を選択します。個別に設定する場合は、「プライマリサーバ」または「レプリカサーバ」を選択します。省略はできません。

6. [保存]ボタンをクリックします。

設定した条件が表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7-3. 上位プロキシの条件設定を変更する

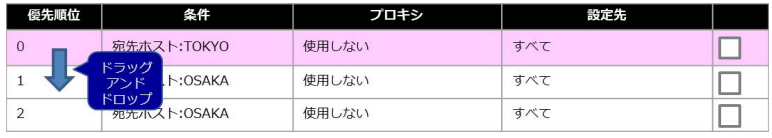
設定済みの上位プロキシの条件を変更するための手順を以下に説明します。

1. [サーバ管理]-[上位プロキシ設定]をクリックします。

[上位プロキシ設定]が表示されます。[上位プロキシ条件設定]には設定済みの条件が一覧表示されます。

注意:

- 上位プロキシ条件を複数設定した場合、優先順位をドラッグアンドドロップすることで条件の優先順位を変更できます。ただし、設定変更中はドラッグができません。変更のイメージを以下に示します。



- 設定した条件をすべて削除する場合は、[全選択]ボタンをクリックしてから[削除]ボタンをクリックします。

2. 条件の中から変更したい表内のセルを直接クリックします。

クリックしたセルに対応したタブが表示されます。例えば、[プロキシ]欄のセルをクリックすると[プロキシ]タブが表示されます。

3. 設定内容を変更します。

4. [保存]ボタンをクリックします。

変更した条件が表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. 一般設定

ここでは、[サーバ管理]-[一般設定]で設定できる内容について説明します。

注意: 一般設定は、システム管理者のみ行うことができます。

8-1. セーフサーチロック

セーフサーチとは、検索サイト各社が提供している、検索結果から成人向けの内容を除外するサービスです。常にセーフサーチを有効にする機能をセーフサーチロックといいます。

注意:
- 本機能はスタンドアロン版のみ対応しています。
- Google、Yahoo! JAPAN、Bing、YouTubeに対応しています。検索サイトによっては、「https://」で始まるURLでサービスを提供しています。そのようなサイトではHTTPS規制設定のサーバデコード方式が無効になっていると、セーフサーチロックが正常に動作しません。HTTPS検索サイトでセーフサーチロックを有効にする場合は、HTTPS規制設定のサーバデコード方式を有効にしてください。

セーフサーチを有効にする手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。
   [一般設定]が表示されます。
2. [セーフサーチロック]の[有効]チェックボックスをオンにします。
3. [保存]ボタンをクリックします。

8-2. アクセス制御設定

リクエスト先のポート番号ごとに、アクセスを許可または禁止することができます。また、リクエスト元(クライアント側)の特定のIPアドレスをアクセス禁止にすることができます。
この機能を利用するための手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。
   [一般設定]が表示されます。

2. [アクセス制御設定]で以下を設定します。

HTTP接続禁止ポート番号	HTTPプロトコルにおいて接続を禁止するポート番号を設定します。何も設定しない場合はすべてのポート番号を許可します。 ポート番号はカンマ区切りで複数設定することができます。 初期値では25番、110番ポートが設定されています。
HTTPS接続許可ポート番号	HTTPS プロトコルにおいて接続を許可するポート番号を設定します。何も設定しない場合はすべてのポート番号を拒否します。 ポート番号はカンマ区切りで複数設定することができます。 初期値では443番ポートが設定されています。
フィルタリングサービスクライアントIPアドレス制限	コントロールサーバ、プロキシに接続できるクライアントのIPアドレスを設定します。何も設定しない場合はすべてのIPアドレスを許可します。 IPアドレスは改行区切りで複数設定することができます。また、[IPアドレス]-[IPアドレス]の形式で範囲指定することもできます。 例:192.168.100.10-192.198.100.20

3. [保存]ボタンをクリックします。

8-3. フィルタリングバイパス設定

フィルタリングバイパス設定とは、ユーザが設定した「User-Agent名」または「宛先ホスト名」に合致した場合に、フィルタリング処理の対象外とする機能です。
例えば、通常のプロキシ動作では対応できない特殊な通信を行うWebサーバやクライアント間の通信（独自拡張を行ったHTTP等やISWMが対応していないHTTP通信等）で接続に失敗する場合は、フィルタリングの対象外とすることで接続できるようになる可能性があります。

注意:
- 本機能はスタンドアロン版のみ対応しています。
- 認証処理やフィルタリング処理などによって正常に接続できないプログラムや接続先があった場合の回避策として使用してください。ただし一切フィルタリングしないため、セキュリティ上の問題が発生する可能性があります。設定には十分注意してください。
- 認証処理だけを回避する場合は、[サーバ設定]-[リクエスト別認証設定] を使用してください。
- 特定のURL についてフィルタリング処理を回避する場合は、[個別アクセス管理]-[例外URL 設定]から対象のルールを選択し、任意のURL を[許可カテゴリ]として例外URL に追加してください。

設定の手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。

[一般設定]が表示されます。

2. [フィルタリングバイパス設定]で迂回対象の条件（User-Agentおよび宛先ホスト）を設定します。

User-Agent	ここで設定したUser-Agentを含むリクエストのアカウント認証およびフィルタリング処理がバイパスされます。User-Agentは改行区切りで複数設定することができます。ワイルドカードとして「*」を使用する場合、「*」は「.」を含む1文字以上の文字列として使用してください。
宛先ホスト	ここで設定した宛先ホストが一致する接続先へのリクエストのアカウント認証およびフィルタリング処理がバイパスされます。宛先ホストは改行区切りで複数設定することができます。ワイルドカードとして「*」を使用する場合、「*」は「.」を含む1文字以上の文字列として使用してください。

3. [保存]ボタンをクリックします。

注意:
- 迂回対象となったリクエストに対するアクセスログは出力されません。システムログへの出力についてはリクエスト単位ではなく接続全体が終了した際に、クライアントIP、相手先ホスト名、上りと下りの総転送量のみ出力されます。バイパス通信中に複数のリクエストが送受信された場合でも同様です。
- 迂回対象となったリクエストに対するプロキシ通信のタイムアウト処理は実施されません。
- FTP over HTTPリクエストによる通信は迂回対象とすることができません。
- フィルタリングバイパスの設定条件に一致した場合でも、Proxy-Authorizationヘッダおよび Proxy-Connectionヘッダの削除、上位プロキシ設定(グループ別のプロキシ設定は除く)は動作します。

8-4. 保存 / 復旧設定

[設定情報管理]-[保存/復旧/同期]で保存するファイルの最大保存件数を設定する手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。

   [一般設定]が表示されます。

2. [保存復旧設定]の[最大保存件数]に、保存するファイルの上限数を設定します。

3. [保存]ボタンをクリックします。

注意:
- 設定ファイル(proxy.inf)から設定する場合は、[MANAGEMENT_CFG]セクションの「MAX_BACKUPS」キーに、保存するファイルの上限数を設定します。
- 初期設定では「5」件が設定されています。

8-5. 通知設定

あらかじめ設定したディスク残量の値に達したときに、管理サービスからメールで警告通知を行うことができます。
警告通知を行う場合のディスク残量の値(割合)を設定する手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。

[一般設定]が表示されます。

2. [通知設定]の[ディスク残量警告設定]に、警告通知を行うディスク残量の割合を%単位で設定します。

注意:
- ディスク残量が 10% になったタイミングで警告通知を行う場合は「10」と設定します。
- ディスク残量の割合はカンマ区切りで複数指定できます(例:10,5,3,2,1)。
- ディスク残量の割合は1～99 の範囲で設定してください。
- 本設定を有効にするには[サーバ管理]-[メール通知設定]で[サービス警告発生通知]チェックボックスをオンにする必要があります。

3. [保存]ボタンをクリックします。

注意:
- 設定ファイル (proxy.inf) から設定する場合は、[SERVICE_OBSERVE] セクションの「CAPACITY_WARN_THRESHOLD」キーに、警告通知を行うディスク残量の割合を%単位で設定します。
- 初期設定では「10,5,3,2,1」が設定されています。この場合、ディスク残量が、それぞれ10%、5%、3%、2%、1%になったタイミングで管理サービスから警告通知を行われます。

8-6. 例外 URL 自動登録設定

対象ディレクトリに例外 URL が記載されたファイルがある場合、自動でインポートする機能です。
例外URL自動登録設定を有効にする手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。

   [一般設定]が表示されます。

2. [例外URL自動登録設定]の[有効]チェックボックスをオンにします。

3. [保存]ボタンをクリックします。

注意:
- 例外URL自動登録の対象となるファイルは例外URL情報ファイルとなります。ファイル名は任意で構いません。
- 例外 URL 情報ファイルについては、「例外 URL 情報ファイルのフォーマット」(402ページ)を参照してください。
- 例外 URL 自動登録の対象となるファイルは次のディレクトリに配置する必要があります。
  <インストールディレクトリ>/var/auto_import_exurl
- 処理されたファイルは次のディレクトリへ移動されます。
  <インストールディレクトリ>/var/exurl_import

8-7. 例外 URL 自動削除設定

例外URLを定期的にチェックし、削除対象の例外URLがある場合は自動で削除する機能です。
例外URL自動削除設定を有効にする手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。

   [一般設定]が表示されます。

2. [例外URL自動削除設定]の[有効]チェックボックスをオンにします。

3. [保存]ボタンをクリックします。

8-8. ARMS (Automatic registration service for Malware Site) 設定

ARMS (Automatic registration service for Malware Site) とは、標的型攻撃対策製品と連携し、脅威情報を自動的に登録する機能です。
ARMS設定を有効にする手順を以下に説明します。

1. [サーバ管理]-[一般設定]をクリックします。

   [一般設定]が表示されます。

2. [ARMS取り込み設定]の[有効]チェックボックスをオンにします。

3. ARMSの設定をします。

取り込み間隔	分単位で取り込みの間隔を指定します。
取り込みURL	取り込みの対象とするファイルが公開されている URL を指定します。 対象とするファイルは改行区切りの URL のリストとなります。 テキストファイルの先頭行および末尾行は、ヘッダーおよびフッターとみなすため、登録の対象としません。
差分取り込み	前回取得したテキストファイルと比較を行い、前回含まれていなかったURLのみを登録します。
登録URL有効期間	登録URLの有効期間を指定しないときは[有効期間を設定しない]を選択します。 有効期間を指定するときは、[有効期間を設定する] を選択し、期間を指定します。

4. [保存]ボタンをクリックします。

注意: ▪ この機能は、プライマリサーバの管理サービスでのみ動作します。

グループとユーザの管理

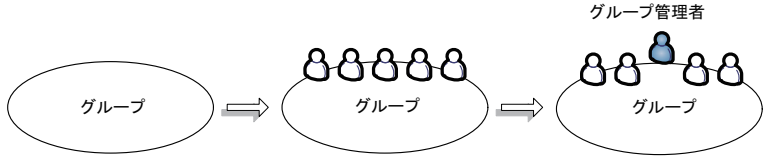
1. グループとユーザについて

ここでは、ユーザとグループについて、設定前に知っておいていただきたい内容について説明します。

1-1. グループとユーザ

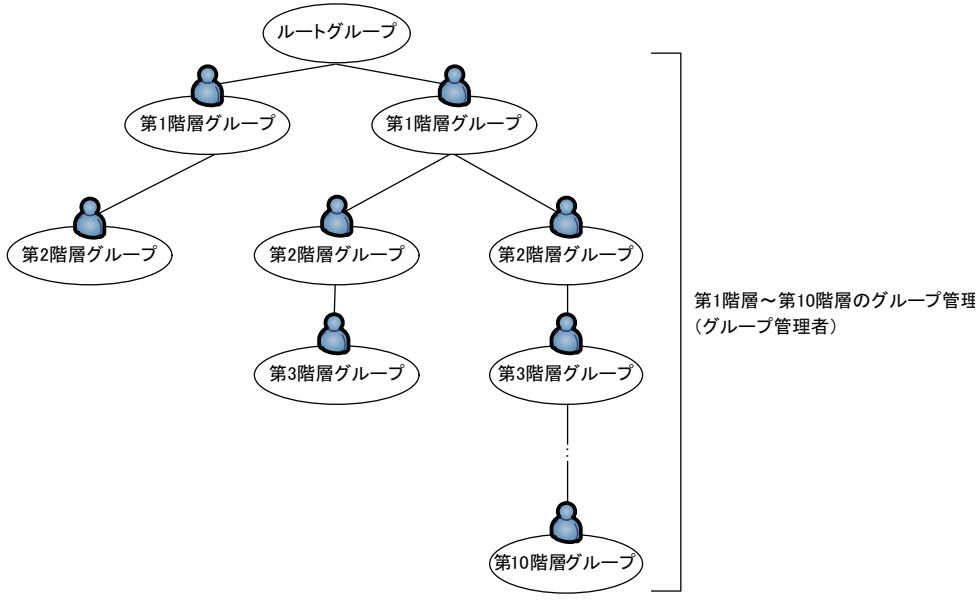
ISWMでは、ユーザをグループ単位で管理できます。1つのグループは1人または複数のユーザで構成されます。
グループには管理者(グループ管理者)を登録できます。グループ管理者は、グループ内のユーザの管理やグループのフィルタリング設定を作成できます。

ユーザとグループの作成



ISWM では、「ルートグループ」を頂点とするツリー構造でグループを管理します。ルートグループの直下を「第1階層グループ」として、「第10階層グループ」まで作成できます。
グループには、ユーザとグループ管理者を登録できます。第1階層のグループ管理者と、第2階層～第10階層のグループ管理者では、使用できる機能が異なります。

グループのツリー構造



注意: ルートグループには、ユーザとグループ管理者を登録できません。

1-2. グループについて

ISWMのグループはルートグループの下で管理されます。

ルートグループ	すべてのグループのフィルタリングルールのベースとなる設定が登録されています。 ルートグループは、グループ名を変更できません。また、ルートグループには、ユーザを登録できません。

初期設定ではルートグループの直下に第1階層グループとして、次の3つのグループが登録されています。

ADMINグループ	ISWMの管理者が所属するグループです。 初期状態では、「root」アカウントが登録されています。 ADMINグループの下位には、グループを登録できません。
GROUPグループ	グループ作成用のサンプルです。 初期状態では、「guest」アカウントが登録されています。
LDAPグループ	LDAPサーバと連携して、ユーザを管理するときに使用します。 管理画面で設定した条件で LDAP サーバを検索し、検索結果のルートに存在するユーザを格納します。 LDAP との連携については、「5. ユーザ認証 /LDAP の設定」(60 ページ)を参照してください。

注意: ADMIN グループ、GROUP グループ、LDAP グループは、任意の名前に変更できますが、ADMIN グループ、LDAP グループを削除することはできません。

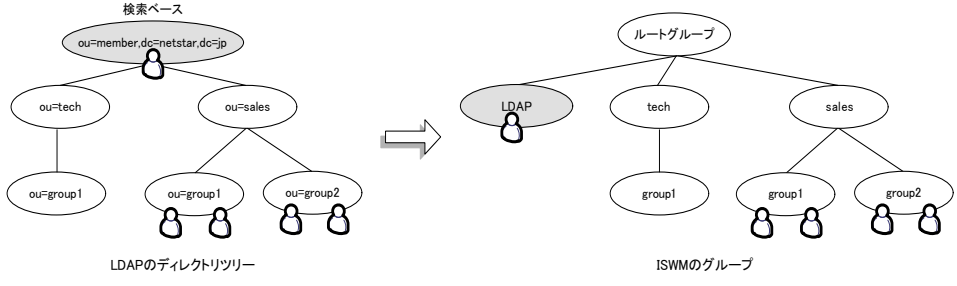
■ LDAP との連携

[サーバ管理]-[認証設定]で、LDAP連携を有効にしている場合、LDAPグループ特定方式の設定により、2種類の登録方法があります。

ユーザの DN からグループ階層を特定する

LDAP グループ特定方式で[ユーザのDNからグループ階層を特定する]を選択した場合、検索ベースの直下に存在するユーザが「LDAP」グループに登録されます。
検索ベースの直下に存在するグループは第1階層グループとして登録されます。

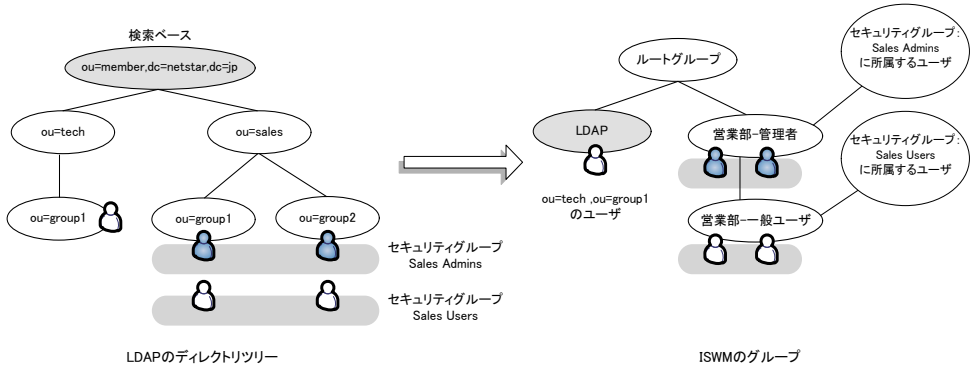
LDAP との連携（ユーザの DN からグループ階層を特定する）



グループ毎にユーザ抽出条件を指定する

LDAPグループ特定方式で[グループ毎にユーザ抽出条件を指定する]を選択した場合、検索に該当するユーザはグループごとに指定した抽出条件に一致するグループに登録されます。複数グループの抽出条件に一致する場合、設定した優先順位によってグループが決定されます。すべてのグループの抽出条件に一致しないユーザは、LDAPグループに登録されます。

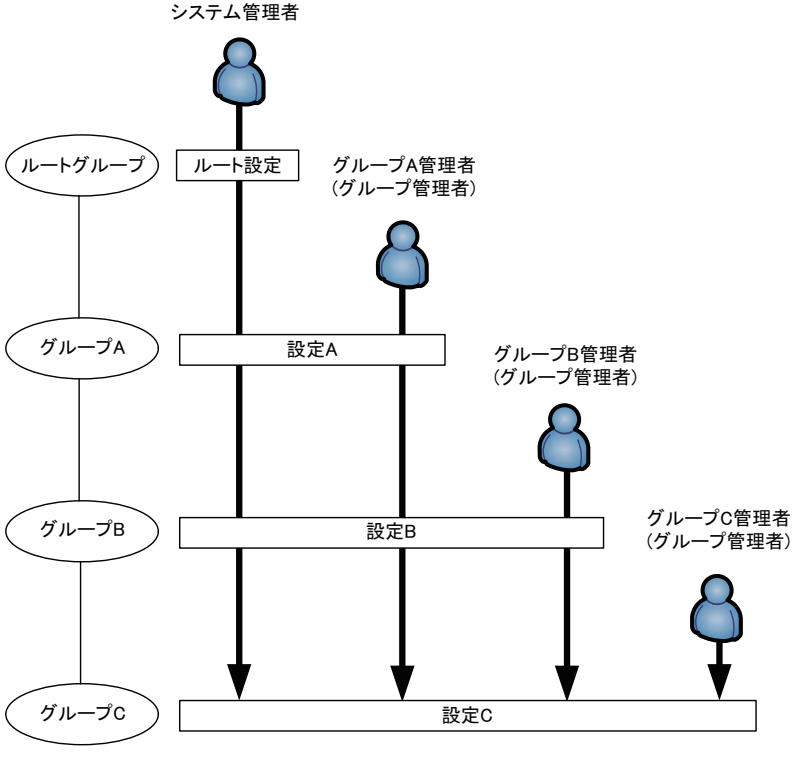
LDAP との連携（グループ毎にユーザ抽出条件を指定する）



1-3. グループとフィルタリング設定

グループごとに異なるフィルタリング設定を適用できます。
システム管理者はすべてのグループのフィルタリング設定を管理できます。グループ管理者は、所属グループと下位グループのフィルタリング設定を管理できます。

グループごとにフィルタリング設定を管理する



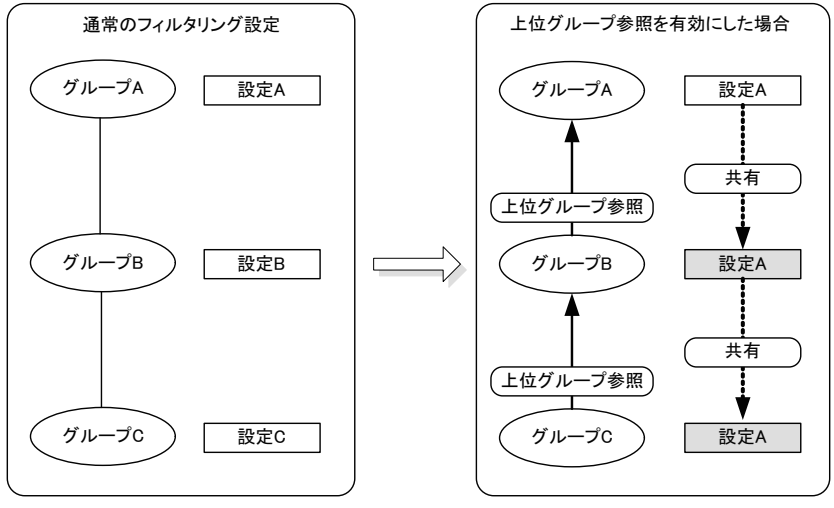
注意:
- グループごとにフィルタリング設定を適用する場合、[サーバ管理]-[認証設定] でユーザ認証を有効にしてください。「5. ユーザ認証/LDAPの設定」(60ページ)を参照してください。
- グループごとにフィルタリング設定を適用しない場合、ルートグループのフィルタリング設定が適用されます。

■ フィルタリング機能の参照

上位グループと下位グループの間で、フィルタリング設定を参照できます。
フィルタリング設定の参照方法の詳細については、「1-5. フィルタリング設定の参照」(170 ページ)を参照してください。
ここでは、「上位グループ参照」と「下位グループ強制参照」の2種類について説明します。

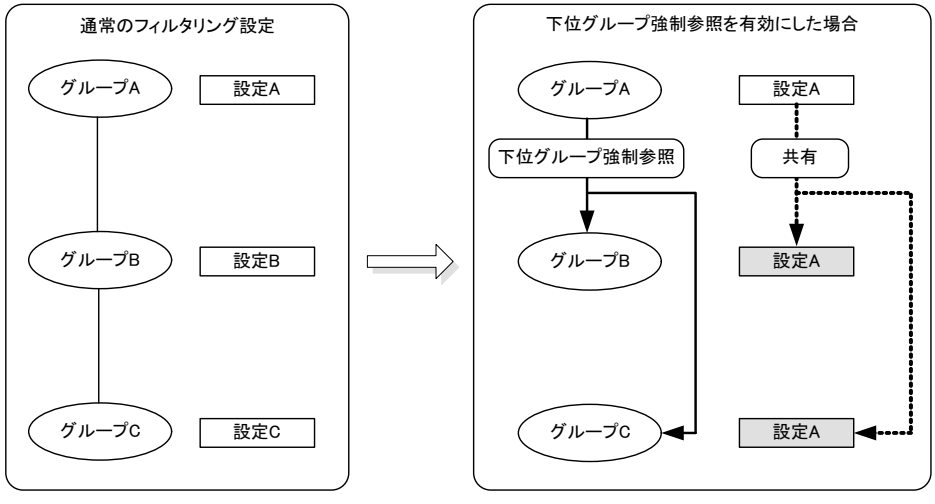
下位グループが、上位グループのフィルタリング設定を参照する(上位グループ参照)

下位グループは、参照先の上位グループからフィルタリング設定を共有できます。
上位グループ参照はグループを登録するときに設定できます。グループの登録後は[グループ/ユーザ管理]-[グループ管理]で設定します。



上位グループが、下位グループにフィルタリング設定を参照させる(下位グループ強制参照)

上位グループは、自分のグループのフィルタリング設定を下位グループに強制的に適用させます。このとき下位グループではフィルタリング設定を変更できません。また、ユーザも設定できません。下位グループ強制参照は、[グループ/ユーザ管理]-[グループ管理]で設定します。



注意: 上位グループのカテゴリルールをカテゴリ設定制限基準ルールとして、下位グループで設定できる規制内容を制限することも可能です。
詳細については、「1-5. フィルタリング設定の参照」(170 ページ)を参照してください。

1-4. ユーザについて

ISWMには、次の9種類のアカウント種別があります。アカウント種別によって、管理画面にログインした後に表示される項目が異なります。

アカウント種別	説明
システム管理者	システムの管理者です。 管理画面上ですべての設定が可能です。
システム管理者(制限付き)	制限付きのシステムの管理者です。 グループ/ユーザ管理、共通アクセス管理、個別アクセス管理、規制解除申請管理の設定が可能です。 サーバ管理、設定情報管理、ログ管理の設定情報の閲覧のみが可能です。
システム管理者 (例外URL設定のみ)	例外URL設定のみのシステムの管理者です。 すべてのグループの例外URLの設定のみが可能です。 ユーザ自身のパスワード、メールアドレスの変更ができます。
システム管理者(閲覧のみ)	閲覧のみのシステムの管理者です。 管理画面上ですべての設定情報の閲覧のみが可能です。
グループ管理者	グループの管理者です。 所属グループと下位グループのグループ/ユーザ管理、個別アクセス管理、規制解除申請管理の設定が可能です。 第一階層のグループ管理者だけがアクセスログの閲覧が可能です。
グループ管理者(制限付き)	制限付きのグループの管理者です。 所属グループと下位グループのグループ/ユーザ管理、個別アクセス管理、規制解除申請管理の設定が可能です。
グループ管理者(閲覧のみ)	閲覧のみのグループの管理者です。 所属グループと下位グループのグループ/ユーザ管理、個別アクセス管理、規制解除申請管理、設定情報管理、ログ管理の設定情報の閲覧のみが可能です。
グループ管理者 (例外URL設定のみ)	例外URL設定のみのグループの管理者です。 所属グループと下位グループの例外 URL の設定のみが可能です。 ユーザ自身のパスワード、メールアドレスの変更ができます。
一般ユーザ	各グループに所属する一般ユーザです。 ユーザ自身のパスワード、メールアドレスの変更ができます。

注意:
- グループ管理者は、アカウントで登録します。グループ管理者を IP アドレスで登録することはできません。
- LDAP 連携が有効な場合、管理画面でアカウントのパスワードを変更することはできません。このとき、一般ユーザではメールアドレスの変更だけが可能です。
- 第一階層のグループ管理者(制限付き)およびグループ管理者(閲覧のみ)で管理画面にアクセスした場合、自分の所属するグループのアクセスログの閲覧は可能です。ただしローテート済みのログの削除はできません。グループ管理者(制限なし)だけがログを削除できます。

■ 特殊なユーザ

次の特殊なユーザが存在します。ユーザを特殊なユーザとして登録することはできません。

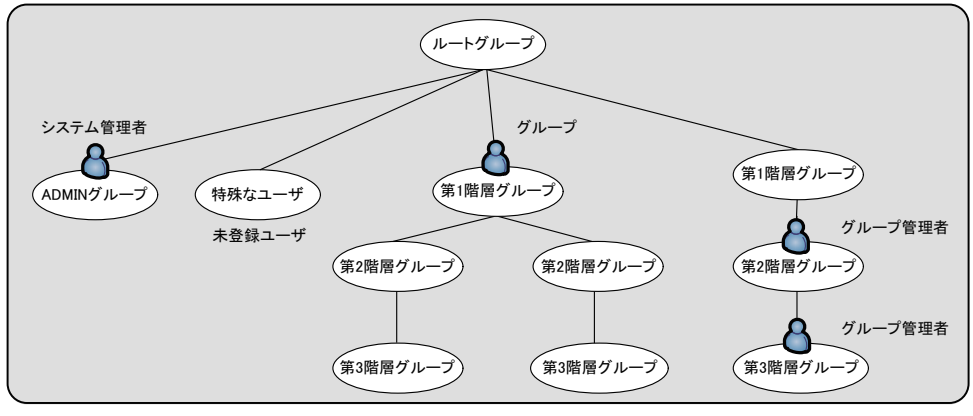
未登録ユーザ	[サーバ管理]-[認証設定]で、ユーザ認証が有効なときに認証できなかったユーザです。 未登録ユーザは「未登録ユーザ」グループに所属します。未登録ユーザとして、アカウントや IP アドレスを登録することはできません。

注意:
- 未登録ユーザは[グループ/ユーザ管理]には表示されません。
- 未登録ユーザへのフィルタリングを有効にするためには、[サーバ管理]-[認証設定]で[未登録ユーザ設定]を有効にしてください。「5. ユーザ認証/LDAPの設定」(60ページ)を参照してください。

■ 管理者の管理権限について

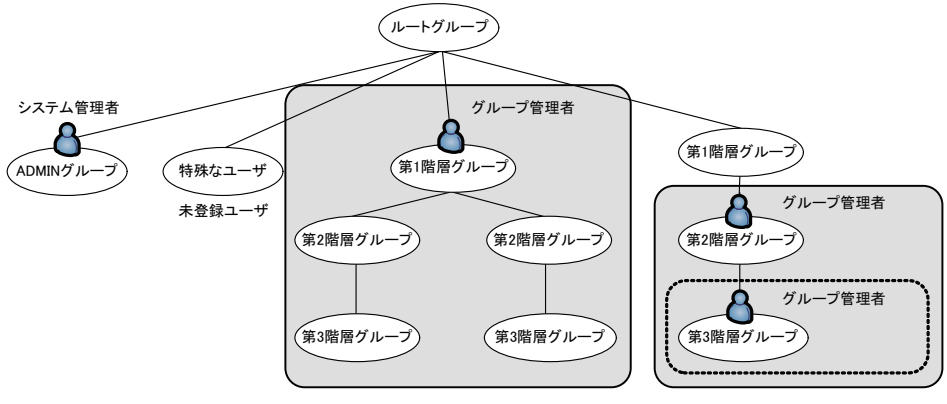
システム管理者は、ルートグループ、特殊なグループを含めて、すべてのグループを管理できます。

システム管理者の管理範囲



グループ管理者は、所属するグループと下位のグループを管理できます。

グループ管理者の管理範囲



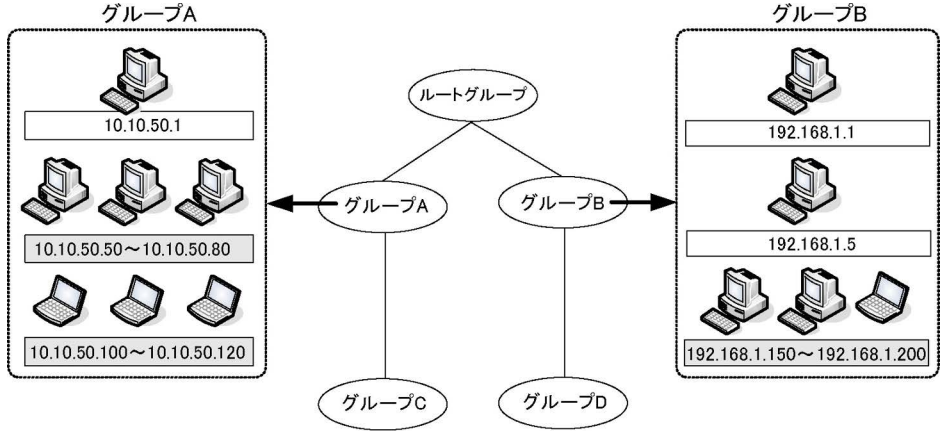
注意: システム管理者、グループ管理者は、アカウントで登録します。IP アドレスでは登録できません。

1-5. IP アドレスでユーザを管理する

ISWMでは、IPアドレスとアカウントの2種類でユーザを管理できます。
ここでは、ユーザをIPアドレスで管理する場合について説明します。ユーザをアカウントで管理する場合は、「1-6. アカウントでユーザを管理する」(124ページ)を参照してください。

■ IP アドレス管理の特長

IPアドレスでユーザを管理すると、端末を使用するユーザに関係なく、端末のIPアドレス単位で管理できます。単一のIPアドレスまたはIPアドレスを範囲指定して登録できます。IPアドレスを範囲指定して登録した場合、指定した範囲内のIPアドレスを一括して管理できます。



注意:
- ユーザを認証する場合には、[サーバ管理]-[認証設定] でユーザ認証を有効にしてください。
- システム管理者は、IPアドレスの登録および管理が可能です。
- グループ管理者は、IPアドレスでのユーザ登録はできません。
  所属するグループと下位グループのIPアドレス一覧をCSVファイルに出力する機能だけが使用できます。

■ グループ単位のフィルタリング設定の適用

IPアドレスでユーザを認証して、IPアドレスが登録されているグループのフィルタリング設定を適用できます。認証できないIPアドレスからのリクエストは、認証エラーになります。

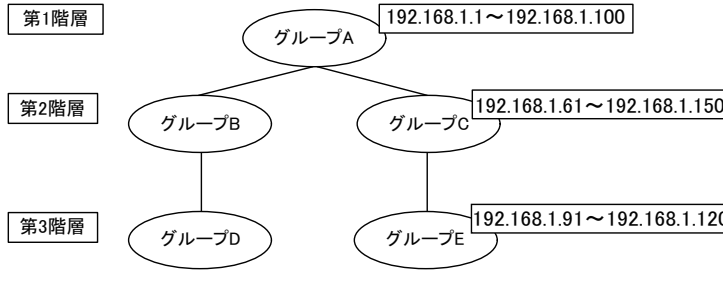
注意: IP アドレス認証とアカウント認証を併用しているときは、IP アドレスでの認証が優先されます。IPアドレスでの認証に失敗すると、アカウント認証のダイアログが表示されます。

■ 重複する IP アドレス設定

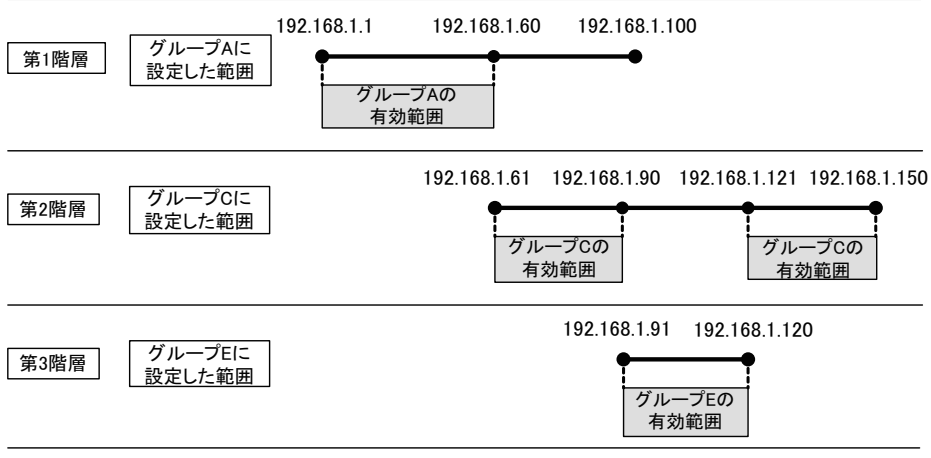
階層が異なるグループ同士では、IPアドレスを重複して設定できます。IPアドレスが重複する範囲では、下位のグループの設定から順番に有効になります。

注意:
- 同じ階層では、IPアドレスを重複して設定できません。
- 実際に有効になる IP アドレスの範囲は、[グループ / ユーザ管理]-[IP アドレス有効範囲]で確認できます。

例として、グループA、グループC、グループEにIPアドレスを設定した場合について説明します。



IPアドレスの重複する範囲では、下位のグループの設定から有効になるため、グループA、グループC、グループEで実際に有効になる範囲は、次の図のようになります。



■ IP アドレスの一括登録、削除

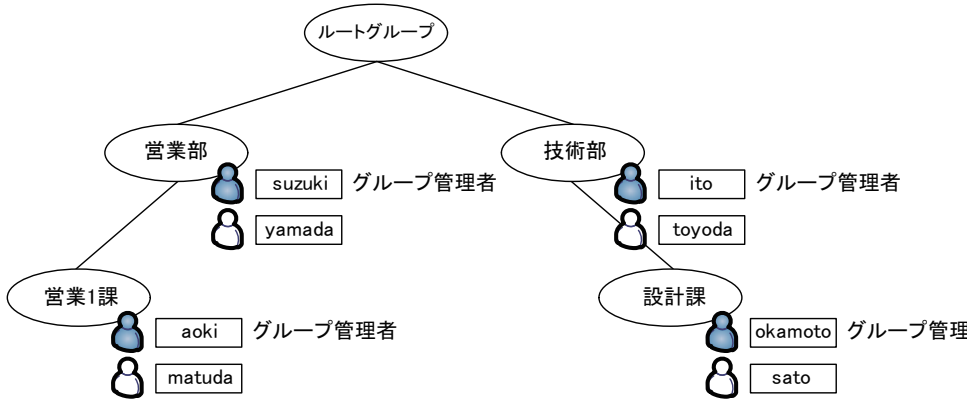
CSVファイルを使用して、IPアドレスを一括して登録、削除できます。
詳細については、「5. ユーザ、グループ情報の一括登録、削除」(152ページ)を参照してください。

1-6. アカウントでユーザを管理する

ISWMでは、IPアドレスとアカウントの2種類でユーザを管理できます。
ここでは、ユーザをアカウントで管理する場合について説明します。ユーザをIPアドレスで管理する場合は、「1-5. IPアドレスでユーザを管理する」(121ページ)を参照してください。

■ アカウント管理の特長

アカウントでユーザを管理すると、端末に関係なく、使用者単位で管理できます。また、グループ管理者を登録できます。



■ グループ単位のフィルタリング設定の適用

アカウントでユーザを認証して、アカウントが所属するグループのフィルタリング設定を適用できます。未登録ユーザを有効にしていた場合、ISWM に登録されていないアカウントからのリクエストは、未登録ユーザのフィルタリング設定が適用されます。

注意:

- アカウントでユーザを認証する場合には、[サーバ管理]-[認証設定] でユーザ認証を有効にしてください。また、[アカウント認証を行う]チェックボックスをオンにしてください。
- [サーバ管理]-[認証設定] で「未登録ユーザ設定」が無効の場合、認証できないアカウントからのリクエストには認証エラー画面が表示されます。
- IP アドレスとアカウントの両方が登録されているユーザの場合、ユーザ認証時にはIPアドレスが優先して使用されます。IPアドレスでユーザを認証する場合、認証画面を表示しないで認証するため、アカウントとパスワードを入力する必要はありません。

■ アカウントの管理方法

アカウントの管理方法には、次の2種類の方法があります。

ISWM のローカルアカウント

ISWMで、アカウントを管理します。

LDAP サーバと連携したアカウント

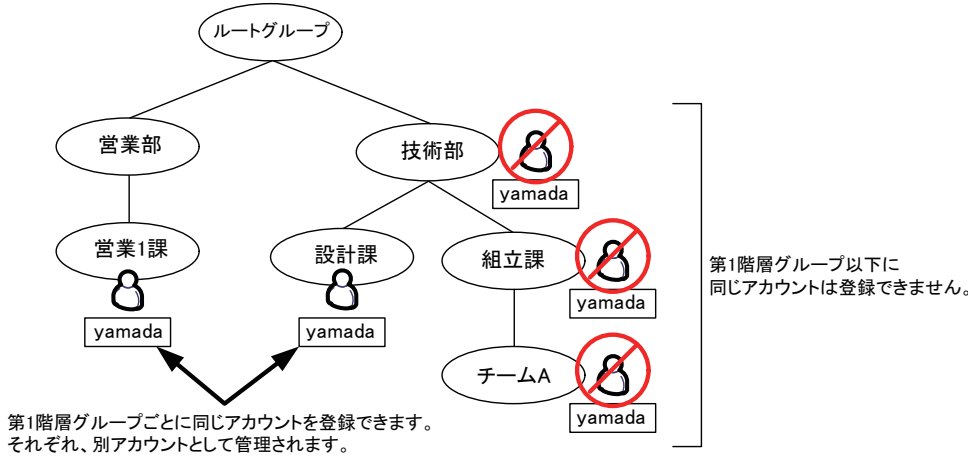
LDAPサーバに登録されたユーザ情報を取得します。アカウントは、LDAPサーバと同期して管理されます。
LDAPとの連携については、「5. ユーザ認証/LDAPの設定」(60ページ)を参照してください。

■ 同一アカウントの登録

[サーバ管理]-[認証設定]で、次の設定の場合、第1階層グループごとに同じアカウントを登録できます。

ユーザ認証	[有効]がオン
認証方式	[BASIC認証]-[ローカルでの認証を行う]を選択
アカウント管理	[第一階層グループ毎にアカウントの管理をする]がオン

次の図では、営業部と技術部が第 1 階層グループとして登録されています。営業部の下位に所属する営業 1 課と、技術部の下位に所属する設計課には、それぞれアカウント「yamada」が登録できます。
営業1課と設計課の「yamada」は別のアカウントとして管理されます。



注意: [サーバ管理]-[認証設定]で、[第一階層グループ毎にアカウントの管理をする]チェックボックスをオンにした場合、アカウント名は次の形式で入力してください。
「第 1 階層グループ名」+「¥」または「\」(バックスラッシュ)+「アカウント名」
上の図の場合、「営業部 ¥yamada」または「技術部 ¥yamada」と入力します。
グループ名およびアカウント名では、大文字と小文字が区別されます。ただし、NTLM 認証時および Kerberos 認証時には大文字と小文字は区別されません。

■ アカウントの一括登録、削除

CSVファイルを使用して、アカウントを一括して登録、削除できます。
詳細については、「5. ユーザ、グループ情報の一括登録、削除」(152ページ)を参照してください。

2. [グループ/ユーザ管理]画面でできること

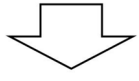
[グループ/ユーザ管理]画面では、次の機能が使用できます。

2-1. グループ、ユーザの登録、管理

グループは[グループ管理]、ユーザは[ユーザ管理]でそれぞれ、登録、管理します。
設定の流れは次のようになります。

1. グループの登録、管理

グループを登録します。登録したグループは、名前の変更、削除が可能です。
グループの登録、管理→「3. グループの登録と管理」(133ページ)



2. ユーザの登録、管理

グループにユーザを登録します。また、登録したユーザの変更や移動、削除などが可能です。
ユーザはIPアドレス、アカウントの2種類で管理できます。
ユーザの登録、管理→「4. ユーザの登録と管理」(139ページ)

注意: LDAP サーバと連携している場合、アカウントの登録 / 変更 / 削除はできません。また、グループ名の変更もできません。

2-2. グループ、ユーザ情報を一括登録、削除する

[ユーザ一括処理]では、CSV形式のファイルを読み込んで、グループ、ユーザ情報を一括して登録、削除できます。
詳細については、「5. ユーザ、グループ情報の一括登録、削除」(152ページ)を参照してください。

2-3. 登録した IP アドレスとグループの一覧を確認する

[IPアドレス有効範囲]では、登録したIPアドレスとグループの一覧を確認できます。
詳細については、「6. IPアドレス設定一覧の確認」(156ページ)を参照してください。

2-4. LDAP サーバと同期する

[LDAPユーザ同期]では、登録したLDAPサーバをISWMと同期することができます。
詳細については、「7. LDAP同期の設定」(157ページ)を参照してください。

2-5. [グループ管理] 画面の構成

[グループ/ユーザ管理]-[グループ管理]をクリックすると、[グループ管理]画面が表示されます。
[グループ管理]画面は、以下の要素で構成されます。

■ グループ一覧

登録されているグループをツリー表示します。現在選択しているグループは、背景が水色で表示されます。
[+] が表示されているグループは、下位にグループが登録されています。[+] をクリックするとツリーが展開され、下位のグループを表示します。
[-]をクリックすると、ツリーを閉じます。
[すべて開く]をクリックすると、登録されているすべての全グループが展開されて表示されます。
[すべて閉じる]をクリックすると、ルートグループのみ表示されます。

注意: システム管理者の場合、すべてのグループが表示されます。
グループ管理者の場合、所属するグループおよび下位グループが表示されます。

■ 設定画面

選択したグループに対する設定画面が表示されます。設定画面は以下の4つのタブで構成されています。

- [グループ情報] タブ
- [ルール設定] タブ
- [LDAP 設定] タブ
- [ネットワーク設定] タブ
- [ヘッダ編集設定] タブ

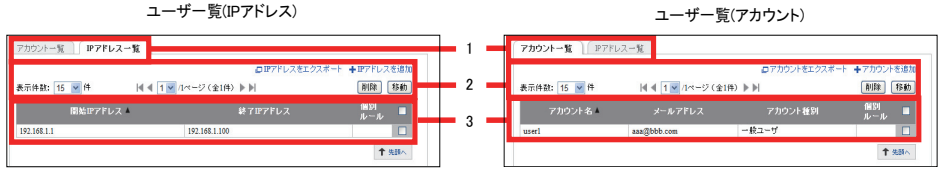
各タブでの操作の詳細については、「3. グループの登録と管理」(133ページ)を参照してください。
グループを新規に登録する場合は、[グループを追加]をクリックします。グループの登録に関する操作の詳細については、「3-1. グループを登録する」(133ページ)を参照してください。

2-6. [ユーザ管理] 画面の構成

[グループ/ユーザ管理]-[ユーザ管理]をクリックすると、[ユーザ管理]画面が表示されます。
[アカウントを検索]をクリックすると、登録したアカウントを、アカウント名またはコメントの部分一致で検索することができます。また、検索結果はCSVファイルに出力可能です。
アカウントの検索に関する操作の詳細については、「4-4. アカウントを検索する」(143 ページ)を参照してください。

■ユーザー覧

IPアドレス、アカウント別にユーザを一覧表示します。[IPアドレス一覧]タブまたは[アカウント一覧]タブをクリックして、表示方法を切り替えます。



1. ユーザー一覧の表示をIPアドレス、アカウント別に切り替えます。

[IPアドレス一覧]タブ	IPアドレス一覧に表示を切り替えます。
[アカウント一覧]タブ	アカウント一覧に表示を切り替えます。

2. IPアドレス/アカウントの新規登録や、選択したIPアドレス、アカウントを管理します。

[IPアドレスをエクスポート]/[アカウントをエクスポート]	グループ内のIPアドレス/アカウント一覧をCSV形式のファイルに出力します。
[IPアドレスを追加]/[アカウントを追加]	IPアドレス/アカウントを新規登録します。
表示件数	1ページに表示するIPアドレス/アカウントの件数を選択します。
	クリックすると、先頭のページが表示されます。
	クリックすると、前のページが表示されます。
	現在表示中のページ番号が表示されます。 表示したいページを直接指定することもできます。
	クリックすると、次のページが表示されます。
	クリックすると、最終のページが表示されます。
[削除]ボタン	ユーザー一覧で、チェックボックスをオンにしたIPアドレス/アカウントを削除します。
[移動]ボタン	ユーザー一覧で、チェックボックスをオンにしたIPアドレス/アカウントを他のグループに移動します。

注意:
- LDAP連携が有効な場合、アカウント一覧では[移動]ボタンおよび[アカウントをエクスポート]だけが表示されます。
- IPアドレス一覧では、アカウント種別によって表示されるボタンが異なります。システム管理者ではすべてのボタンが表示されます。グループ管理者では、[IPアドレスをエクスポート]だけが表示されます。
- ルートグループには、[アカウントをエクスポート]、[IP アドレスをエクスポート]が表示されます。

3. グループ一覧で選択したグループに所属するユーザのIPアドレス/アカウント一覧を表示します。

IPアドレス/アカウントは、[表示件数]で設定した件数が表示されます。

開始IPアドレス([IPアドレス一覧]タブの場合)	IPアドレスが範囲で登録されている場合、範囲の開始IPアドレスが表示されます。
終了IPアドレス([IPアドレス一覧]タブの場合)	IPアドレスが範囲で登録されている場合、範囲の終了IPアドレスが表示されます。
アカウント名([アカウント一覧]タブの場合)	登録されているアカウント名が表示されます。
アカウント種別([アカウント一覧]タブの場合)	アカウントに対する種別(以下のいずれか)が表示されます。 • システム管理者 • システム管理者(制限付き) • システム管理者(閲覧のみ) • システム管理者(例外URL設定のみ) • グループ管理者 • グループ管理者(制限付き) • グループ管理者(閲覧のみ) • グループ管理者(例外URL設定のみ) • 一般ユーザ
個別ルール	クリックすると、選択したユーザに適用するルールを確認、編集することができます。適用ルールは以下のとおりです。 • カテゴリ/スケジュール • ブラウザ規制 • 検索キーワード規制 • 書き込みキーワード規制 • 規制オプション

IPアドレス/アカウント表示右側のチェックボックスは、ユーザのグループを移動するときと、ユーザを削除するときに使用します。グループ移動、削除対象とするIPアドレスまたは

アカウントのチェックボックスをオンにして、[移動]ボタンまたは[削除]ボタンをクリックします。

3. グループの登録と管理

グループの登録と管理方法について説明します。
ユーザの登録と管理については、「4. ユーザの登録と管理」(139ページ)を参照してください。
[グループ管理]画面の名称については、「2-5. [グループ管理]画面の構成」(128ページ)を参照してください。

3-1. グループを登録する

グループの登録方法について説明します。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。

   [グループ管理]が表示されます。

2. グループ一覧から、登録したいグループの上位グループ名をクリックします。

   設定画面にグループの設定内容が表示されます。

3. [グループを追加]をクリックします。

   [グループ登録]が表示されます。

4. 登録するグループの内容を設定します。

グループ名(必須項目)	登録するグループ名を半角64文字以内で入力します。
コメント	グループに対するコメントを半角100文字以内で入力できます。
ルール設定	以下のいずれかを選択します。 • 親グループの適用ルールを参照する 親グループ(上位グループ)の設定ルールをすべて参照する新しいグループを作成します。作成した子グループ(下位グループ)でルールの変更・追加を行う場合は、新たにルールを追加する必要があります。 • 親グループの適用ルールをコピーする 親グループ(上位グループ)のスケジュール設定、例外URL設定などのルールをコピーしたグループを作成します。作成した子グループ(下位グループ)でコピーしたルールの変更・追加ができます。

注意:
- LDAP 連携が有効なときに、[LDAP グループ特定方式] に [ユーザの DN からグループ階層を特定する]を選択していると、グループ名は変更できません。
- グループ名、コメントには、次の文字を使用できません。
  タブ記号、半角記号(¥ / : ; ? < > | ")、全角記号(¥ ／ ： ； ？ ＜ ＞ ｜ ”)

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

[グループ管理]に「登録が完了しました。」と表示されます。

7. [ルール設定]タブ、[LDAP設定]タブ、[ネットワーク設定]タブをクリックして設定します。

詳細については、次の表を参照してください。

[ルール設定]タブ	「3-2. グループにフィルタリングルールを適用する」(134ページ)
[LDAP設定]タブ	「3-3. グループにLDAP設定をする」(135ページ)
[ネットワーク設定]タブ	「3-4. グループにネットワーク設定をする」(135ページ)

注意:
- 次の条件を満たす場合、[LDAP設定]タブが表示されます。
  - ADMIN グループ所属のユーザでログインしている。
  - [サーバ管理]-[認証設定] で、「認証方式」に BASIC 認証 (LDAP 連携)、NTLM 認証または Kerberos 認証設定後、[LDAP グループ特定方式] に [グループ毎にユーザ抽出条件を指定する] を選択している。
- ICAP版、グループ管理者の場合、[ネットワーク設定]タブは表示されません。

3-2. グループにフィルタリングルールを適用する

グループにフィルタリングルールを適用するには、あらかじめ[個別アクセス管理]でフィルタリングルールを設定する必要があります。
設定したフィルタリングルールをグループに適用します。
フィルタリングルールを設定する方法については、「5. 個別アクセスの設定」(214ページ)を参照してください。
フィルタリングルールをグループに適用する設定方法については、「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

3-3. グループに LDAP 設定をする

グループにLDAPに関する設定をします。[サーバ管理]-[認証設定]-[LDAPグループ特定方式]で[グループ毎にユーザ抽出条件を指定する]を選択した場合のLDAPサーバとの同期設定について、グループごとにユーザを取り込む条件、および、同一ユーザが複数のグループに所属する場合に取り込むグループの優先順位を設定できます。
詳細については、「グループにユーザを取り込む条件を設定する」(85 ページ)を参照してください。

3-4. グループにネットワーク設定をする

グループにネットワークに関する設定をします。グループごとに上位プロキシの設定、HTTPSデコードの設定ができます。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。

   [グループ管理]が表示されます。

2. グループ一覧から、ネットワーク設定をするグループ名をクリックします。

   設定画面にグループの設定内容が表示されます。

3. [ネットワーク設定]タブをクリックします。

4. [編集]ボタンをクリックします。

   [ネットワーク設定編集]が表示されます。

5. 上位プロキシ設定、HTTPSデコード設定をします。

上位プロキシ設定	上位プロキシの設定を選択します。 • システム共通の設定を使用する: システム共通の上位プロキシの設定を使用します。 • 上位グループと同じ設定を使用する: 上位グループの上位プロキシの設定を使用します。 • 上位プロキシを使用しない: 上位プロキシの設定を使用しない場合、IPアドレス/ドメイン、ポート番号を入力する必要はありません。 • グループで個別に設定を行う: グループごとに上位プロキシを設定します。 IPアドレス/ドメイン、ポート番号を入力してください。 [すべてのプロトコルに同じプロキシサーバを使用する]チェックボックスをオンにすると、すべてのプロトコルに同じプロキシサーバを使用します。
HTTPSデコード設定	[HTTPS 通信をデコードする] チェックボックスをオンにすると、HTTPSデコード設定が有効になります。

注意:
- 「上位プロキシ設定」は、[サーバ管理]-[上位プロキシ設定]で[グループ別のプロキシ設定を有効にする]チェックボックスをオンにした場合に表示されます。
- 「HTTPSデコード設定」の[HTTPS通信をデコードする]チェックボックスは、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]の[設定単位]でグループ毎を選択したときに表示されます。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存] ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず [保存] ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

「更新が完了しました。」と表示されます。

3-5. グループにヘッダ編集を設定する

グループごとにヘッダ編集の設定が行えます。
ヘッダ編集の設定方法については「ヘッダ編集の設定」(182ページ)を参照してください。

3-6. グループ情報を変更する

グループの設定(グループ名、コメント)を変更する方法について説明します。

注意: LDAP サーバとの連携が有効で、ユーザの DN からグループ階層を特定する場合、グループ名は変更できません。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。

   [グループ管理]が表示されます。

2. グループ一覧から、グループの設定を変更するグループ名をクリックします。

   設定画面に設定内容が表示されます。

3. [グループ情報]タブをクリックします。

4. [編集]ボタンをクリックします。

   [グループ情報編集]が表示されます。

5. グループ名、コメントを変更します。

   設定項目については、「3-1. グループを登録する」(133ページ)を参照してください。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存] ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず [保存] ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   「更新が完了しました。」と表示されます。

3-7. グループを削除する

グループを削除する方法について説明します。

注意: [ログ管理]-[ログ設定]でログファイルの出力単位を「第一階層グループ毎」に設定している場合、第1階層グループを削除すると、削除したグループのログファイルは管理画面に表示されません。
削除するグループのログファイルが必要な場合には、必ずログファイルを保存してから、第1階層グループを削除してください。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。
   [グループ管理]が表示されます。
2. グループ一覧から、削除するグループ名をクリックします。
   設定画面にグループの設定内容が表示されます。
3. [グループ情報]タブをクリックします。
4. [削除]ボタンをクリックします。
   確認のダイアログが表示されます。
5. [OK]ボタンをクリックします。
   「削除が完了しました。」と表示されます。

注意: 下位グループが存在する場合、削除の確認ダイアログで [OK] ボタンをクリックすると、下位グループも同時に削除されることを注意するダイアログが表示されます。

4. ユーザの登録と管理

ユーザの登録と管理方法について説明します。ユーザはIPアドレスとアカウントの2種類で登録、管理できます。詳細については、次の表を参照してください。
グループとユーザの詳細については、「1. グループとユーザについて」(111ページ)を参照してください。
[ユーザ管理]画面の名称については、「2-5. [グループ管理]画面の構成」(128ページ)、または「2-6. [ユーザ管理]画面の構成」(129ページ)を参照してください。

	IP アドレス	アカウント
ユーザを登録する	「4-2. IP アドレスを登録する」(140ページ)	「4-3. アカウントを登録する」(141ページ)
アカウントを検索する	—	「4-4. アカウントを検索する」(143ページ)
ユーザにフィルタリングルールを適用する	「4-5. IPアドレス/アカウントのユーザにフィルタリングルールを適用する」(145ページ)	
ユーザ情報を変更する	「4-6. IP アドレス / アカウントを変更する」(145 ページ)	
ユーザのグループを移動する	「4-7. IPアドレス/アカウントを他のグループに移動する」(147ページ)	
ユーザを削除する	「4-8. IP アドレス / アカウントを削除する」(148 ページ)	
グループ内のユーザー覧をファイルに出力する	「4-9. IPアドレス/アカウント一覧をファイルに出力する」(149ページ)	

4-1. IPアドレスの管理とアカウント種別

IPアドレスの管理はシステム管理者、グループ管理者で使用できる機能が異なります。

	システム管理者	グループ管理者
IPアドレスの登録	○	―
グループを移動する	○	―
IPアドレスの削除、全削除	○	―
IPアドレス一覧の出力	○	○ ※

○:使用できます。　　―:使用できません。
※所属するグループおよび下位グループのCSV出力が可能です。

4-2. IP アドレスを登録する

グループにIPアドレスを登録します。IPアドレスは単一、または範囲指定して登録できます。

注意:　IP アドレスを登録できるのは、システム管理者だけです。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。
   [ユーザ管理]が表示されます。
2. グループ一覧から、IPアドレスを登録するグループ名をクリックします。
   ユーザ一覧が表示されます。
3. [IPアドレス一覧]タブをクリックします。
4. [IPアドレスを追加]をクリックします。
   [IPアドレス登録]が表示されます。

5. 登録するIPアドレスを入力します。

選択中のユーザ **選択中のグループ**	選択中のユーザ名とグループ名が表示されます。
開始IPアドレス(必須項目)	登録するIPアドレスを入力します。 IP アドレスを範囲で登録する場合、範囲の開始とする IP アドレスを入力します。
終了IPアドレス	IP アドレスを範囲指定する場合、範囲の終了とする IP アドレスを入力します。 単一の IP アドレスを登録する場合、入力する必要はありません。

注意: IPアドレスを範囲で登録する場合、IPアドレスが「開始IPアドレス」<「終了IPアドレス」となるように入力してください。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されます。

注意: 選択したグループに初めて IP アドレスを登録した場合、ユーザ一覧に操作ボタンが追加されます。

4-3. アカウントを登録する

グループにアカウントを登録します。アカウント種別も設定できます。

注意: LDAP連携が有効な場合、アカウントの移動だけが可能です。アカウントの登録および削除はできません。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

[ユーザ管理]が表示されます。

2. グループ一覧から、アカウントを登録するグループをクリックします。

ユーザ一覧が表示されます。

3. [アカウント一覧]タブをクリックします。

4. [アカウントを追加]をクリックします。

[アカウント登録]が表示されます。

5. 登録するアカウントの情報を入力します。

選択中のユーザ **選択中のグループ**	アカウントを登録するユーザ名とグループ名が表示されます。
アカウント名(必須項目)	登録するアカウント名を半角20文字以内で入力します。
パスワード(必須項目)	パスワードを半角20文字以内で入力します。
パスワード(確認)(必須項目)	確認のため、再度パスワードを入力します。
メールアドレス	登録するアカウントのメールアドレスを半角 128 文字以内で入力します。
コメント	登録するアカウントに対するコメントを半角 100 文字以内で入力します。
アカウント種別	登録するアカウントの種別を選択します。アカウント種別は以下のいずれかを選択できます。 • システム管理者 • システム管理者(制限付き) • システム管理者(閲覧のみ) • システム管理者(例外URL設定のみ) • グループ管理者 • グループ管理者(制限付き) • グループ管理者(閲覧のみ) • グループ管理者(例外URL設定のみ) • 一般ユーザ アカウントについては、「ログインするアカウントについて」(33ページ)を参照してください。

注意:
- アカウント名、パスワード、メールアドレスには、半角英数字および次の記号を使用できます。
  また、アカウント名には半角スペースも使用できます。
  ! # $ % & ' ( ) = ` ~ { + } _ - ^ @ [ ] . * / < > |
- コメントには、次の文字を使用できません。
  タブ記号、半角記号(¥ / : ; ? < > | ")、全角記号(¥ ／ : ; ? ＜ ＞ ｜ ”)

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

「登録が完了しました。」と表示されます。

注意: 選択したグループに初めてアカウントを登録した場合、ユーザ一覧に操作ボタンが追加されます。

4-4. アカウントを検索する

登録したアカウントを部分一致で検索できます。検索結果をクリックすると、アカウント情報を表示します。また、検索結果はCSVファイルに出力可能です。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

[ユーザ管理]が表示されます。

2. 検索対象にするグループをクリックします。

すべてのグループを検索対象にする場合、ルートグループのチェックボックスをオンにします。

3. [アカウントを検索]をクリックします。

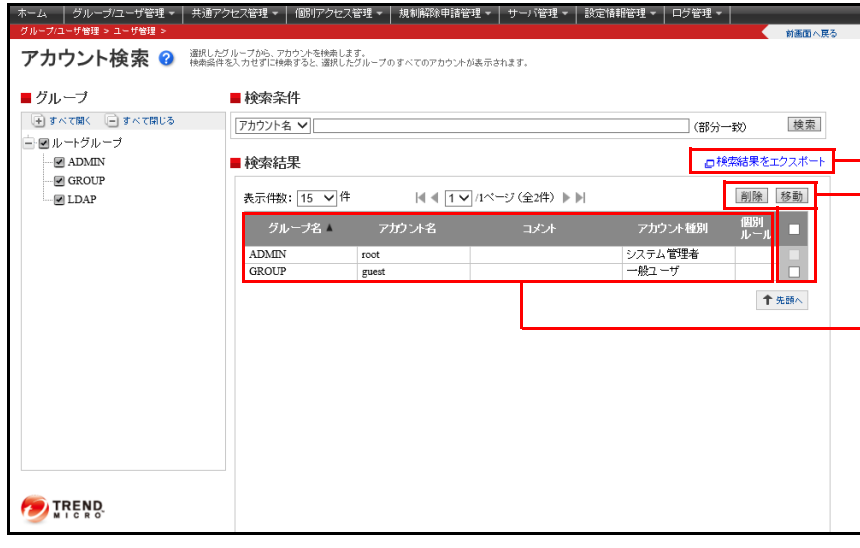
[アカウント検索]が表示されます。

4. 検索条件を入力します。

[アカウント名]か[コメント]を選択してから、テキストボックスに検索用ワードを入力します。

5. [検索]ボタンをクリックします。

検索結果が表示されます。



a. [検索結果をエクスポート]をクリックすると、[ユーザ情報エクスポート]画面が別ウィンドウで表示されます。ファイル文字コードとパスワードを出力するかどうかを選択して、[エクスポート]ボタンをクリックすると、検索結果をCSVファイルに出力できます。ファイル文字コードは、[UTF-8]、[Shift_JIS]、[EUC_JP]から選択できます。

操作方法および出力したCSVファイルのフォーマットについては、「4-9. IPアドレス/アカウント一覧をファイルに出力する」(149ページ)を参照してください。

b. 検索結果のチェックボックスをオンにして[削除]ボタンをクリックすると、選択されたアカウントが削除されます。

また、検索結果のチェックボックスをオンにして[移動]ボタンをクリックすると、[ユーザ移動]画面が別ウィンドウで表示されます。[ユーザ移動]画面の操作方法については、「4-7. IPアドレス/アカウントを他のグループに移動する」(147ページ)を参照してください。

c. 検索結果の各項目は、次のとおりです。

グループ名	所属するグループを表示します。
アカウント名	アカウント名を表示します。
コメント	[アカウント登録]で設定したコメントを表示します。
アカウント種別	[アカウント登録]で選択したアカウント種別を表示します。
個別ルール	クリックすると、選択したユーザに適用するルールを確認、編集することができます。

注意: アカウント名をクリックすると、クリックしたアカウントの詳細情報が表示されて、情報を変更することができます。この画面の操作方法については、「4-6. IP アドレス / アカウントを変更する」(145 ページ)を参照してください。

4-5. IP アドレス / アカウントのユーザにフィルタリングルールを適用する

ユーザにフィルタリングルールを適用するには、あらかじめ[個別アクセス管理]でフィルタリングルールを設定する必要があります。
設定したフィルタリングルールをユーザに適用します。
フィルタリングルールを設定する方法については、「5. 個別アクセスの設定」(214ページ)を参照してください。
フィルタリングルールをユーザに適用する設定方法については、「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

4-6. IP アドレス / アカウントを変更する

IPアドレス/アカウントを変更する方法について説明します。

注意: IP アドレスを変更できるのは、システム管理者だけです。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

   [ユーザ管理]が表示されます。

2. グループ一覧から、変更するIPアドレス/アカウントが登録されているグループ名をクリックします。

   ユーザ一覧が表示されます。

3. [IPアドレス一覧]タブまたは[アカウント一覧]タブをクリックして、ユーザ一覧の表示を切り替えます。

4. ユーザ一覧から、設定を変更するIPアドレス/アカウントをクリックします。

   [IPアドレス詳細]または[アカウント詳細]が表示されます。

5. [編集]ボタンをクリックします。

   [IPアドレス情報]タブの[編集]ボタンをクリックした場合は、[IPアドレス情報編集]が表示されます。
   [アカウント情報]タブの[編集]ボタンをクリックした場合は、[アカウント情報編集]が表示されます。

   注意: [削除] ボタンをクリックすると、現在表示されている IP アドレスまたはアカウントが削除されます。

6. IPアドレス/アカウントの設定を変更します。

   IPアドレスの設定項目については、「4-2. IPアドレスを登録する」(140ページ)を参照してください。
   アカウントの設定項目については、「4-3. アカウントを登録する」(141ページ)を参照してください。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存] ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず [保存] ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   「更新が完了しました。」と表示されます。

4-7. IP アドレス / アカウントを他のグループに移動する

ユーザ一覧で、チェックボックスをオンにしたIPアドレス/アカウントを別のグループに移動する方法について説明します。

注意: IP アドレスのグループ移動ができるのは、システム管理者だけです。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

   [ユーザ管理]が表示されます。

2. グループ一覧から、移動するIPアドレス/アカウントが登録されているグループ名をクリックします。

   ユーザ一覧が表示されます。

3. [IPアドレス一覧]タブまたは[アカウント一覧]タブをクリックして、ユーザ一覧の表示を切り替えます。

4. ユーザ一覧から、グループを移動するIPアドレス/アカウントのチェックボックスをオンにします。

   注意: 1 回の操作で移動可能な IP アドレス / アカウントは、[表示件数] で設定した件数までです。設定した表示件数を超えて移動する場合は、ページを切り替えて1ページごとに移動してください。

5. ユーザ一覧の[移動]ボタンをクリックします。

   [ユーザ移動]画面が別ウィンドウで表示されます。

6. [ユーザ移動]画面で、移動先のグループをクリックします。

   確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

   「移動が完了しました。」と表示されます。

4-8. IP アドレス / アカウントを削除する

IPアドレス/アカウントを削除する方法について説明します。

注意: IP アドレスを削除できるのは、システム管理者だけです。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

   [ユーザ管理]が表示されます。

2. グループ一覧から、削除するIPアドレス/アカウントが登録されているグループ名をクリックします。

   ユーザ一覧が表示されます。

3. [IPアドレス一覧]タブまたは[アカウント一覧]タブをクリックして、ユーザ一覧の表示を切り替えます。

4. ユーザ一覧から、削除するIPアドレス/アカウントのチェックボックスをオンにします。

   注意: 1 回の操作で削除可能な IP アドレス / アカウントは、[表示件数] で設定した件数までです。設定した表示件数を超えて削除する場合は、ページを切り替えて1ページごとに削除してください。

5. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   「削除が完了しました。」と表示されます。

4-9. IP アドレス / アカウント一覧をファイルに出力する

グループ内のIPアドレス/アカウント一覧をCSV形式のファイルに出力する方法について説明します。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

   [ユーザ管理]が表示されます。

2. グループ一覧から、IPアドレス/アカウント一覧をファイルに出力するグループ名をクリックします。

   ユーザ一覧が表示されます。

   注意: システム管理者の場合、ルートグループを選択すると、[IP アドレス一覧] タブには [IP アドレスをエクスポート]、[アカウント一覧] タブには [アカウントをエクスポート] が表示されます。ルートグループでは、登録されているすべての IP アドレス / アカウント一覧を出力できます。

3. [IPアドレス一覧]タブまたは[アカウント一覧]タブをクリックして、ユーザ一覧の表示を切り替えます。

4. IPアドレス一覧をファイルに出力する場合、[IPアドレス一覧]タブの[IPアドレスをエクスポート]をクリックします。

   アカウント一覧をファイルに出力する場合、[アカウント一覧]タブの[アカウントをエクスポート]をクリックします。
   [ユーザ情報エクスポート]画面が別ウィンドウで表示されます。
   ファイル出力をキャンセルする場合は、[ユーザ情報エクスポート]画面の[閉じる]ボタンをクリックします。

   注意: 各 IP アドレス / アカウントのチェックボックスのオン / オフにかかわらず、登録されているすべての IP アドレス / アカウントが、CSV 形式で出力されます。

5. 出力するファイルのエンコード形式を選択します。

   プルダウンメニューから、「UTF-8」、「Shift_JIS」、「EUC_JP」の3種類が選択できます。

6. アカウント一覧をファイルに出力する場合、パスワードを出力するかどうかを選択します。

   パスワードを出力する場合、[パスワードを出力する]チェックボックスをオンにします。
   パスワードを出力しない場合、[パスワードを出力する]チェックボックスをオフにします。

7. [エクスポート]ボタンをクリックします。

   指定した形式でエンコードされたIPアドレス/アカウントの一覧をダウンロードできます。
   ダウンロード方法については、ブラウザのヘルプを参照してください。

8. [閉じる]ボタンをクリックします。

   [ユーザ情報エクスポート]画面が閉じます。

■ ファイルのフォーマット

IP アドレスの場合

初期状態では、ファイル名は「ipList.csv」となります。ファイル名は、ダウンロードするときに変更できます。ファイルのフォーマットは次のとおりです。

```
1 行目:  グループ名,開始IPアドレス,終了IPアドレス,個別ルール
2 行目:  ″第1 階層－グループA″,″192.168.1.1″,″192.168.1.50″,″個別ルール″
3 行目:  ″第1 階層－グループA″,″192.168.1.51″,″192.168.1.60″
```

注意: グループの階層は、「¥」または「\」(バックスラッシュ) で表示されます。

1行目はフィールドのヘッダが格納されます。2行目以降にグループ内のIPアドレス一覧が格納されます。
ダウンロードしたファイルは、一括登録、削除するときにも使用できます。
一括登録、削除については、「5. ユーザ、グループ情報の一括登録、削除」(152ページ)を参照してください。

アカウントの場合

初期状態では、ファイル名は「accountList.csv」となります。ファイル名は、ダウンロードするときに変更できます。ファイルのフォーマットは次のとおりです。

```
1 行目:  アカウント名, パスワード, グループ名, メールアドレス, アカウント種別, コメント, 個別ルール
2 行目:  "user01","Member#01"," 第1 階層ーグループA","user01@netstar.jp","0","コメント"
3 行目:  "user02","Member#02"," 第1 階層ーグループA","user02@netstar.jp","1","コメント","個別ルール"
```

注意:

- アカウント種別には、次の値が格納されます。
  - 一般ユーザの場合には「0」
  - グループ管理者(閲覧のみ)の場合には「1」
  - グループ管理者(制限付き)の場合には「2」
  - グループ管理者の場合には「3」
  - システム管理者(閲覧のみ)の場合には「4」
  - システム管理者(制限付き)の場合には「5」
  - システム管理者の場合には「6」
  - グループ管理者(例外URL設定のみ)の場合には「7」
  - システム管理者(例外URL設定のみ)の場合には「8」
- グループの階層は、「¥」または「\」(バックスラッシュ)で表示されます。

1 行目はフィールドのヘッダが格納されます。2 行目以降にグループ内のアカウント一覧が格納されます。
ダウンロードしたファイルは、一括登録、削除するときにも使用できます。
一括登録、削除については、「5. ユーザ、グループ情報の一括登録、削除」(152ページ)を参照してください。

5. ユーザ、グループ情報の一括登録、削除

CSV形式のファイルを読み込んで、グループ/ユーザ情報を一括して登録、削除できます。
読み込むCSVファイルのフォーマットについては、「5-1. ファイルのフォーマット」(153ページ)を参照してください。

注意:
- システム管理者は、すべてのグループに対して一括登録、削除できます。
- グループ管理者は、所属するグループおよび下位グループに対して一括登録、削除できます。

1. [グループ/ユーザ管理]-[ユーザ一括処理]をクリックします。

   [ユーザ一括処理]が表示されます。

2. 追加するデータの種別(アカウント、IPアドレス)、読み込むCSVファイルのファイル名、CSVファイルのエンコードを設定します。

   ユーザ一覧から出力したIPアドレス、アカウント一覧のCSVファイルも使用できます。
   手順については、「4-9. IPアドレス/アカウント一覧をファイルに出力する」(149ページ)を参照してください。

データ種別選択	アカウント、IPアドレスのどちらを登録するかを選択します。 この項目は、システム管理者だけが選択可能です。 グループ管理者の場合には、設定項目が表示されません。グループ管理者では、アカウントだけ登録、削除できます。
ファイルエンコード選択	読み込むCSVファイルのエンコード形式を選択します。 UTF-8、Shift_JIS、EUC_JPから選択できます。
CSVファイル選択	読む込むCSVファイルのパスとファイル名を入力します。 [参照]ボタンをクリックすると、[アップロードするファイルの選択]画面が別ウィンドウで表示されます。一覧からファイルを選択して、[開く]ボタンをクリックすると、選択したファイルのパスとファイル名が設定されます。

3. [登録]ボタンまたは[削除]ボタンをクリックします。

   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

処理結果の画面が、別ウィンドウで表示されます。
[閉じる]ボタンをクリックすると、処理結果の画面が閉じます。

5-1. ファイルのフォーマット

一括登録、削除に使用する、CSVファイルのフォーマットについて説明します。
文字コードは、UTF-8、Shift_JIS、EUC_JPが使用できます。

■ IP アドレス形式の場合

- フォーマット

グループ名	開始 IP アドレス	終了 IP アドレス	個別ルール

- 入力例

" グループ A¥ グループ B",	"192.168.1.151",	"192.168.1.200",	" ルール個別適用 "

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、「第1階層¥第2階層¥第3階層」のように、第1階層から「¥」または「\」(バックスラッシュ) で区切って入力します。
開始IPアドレス	登録するIPアドレスを入力します。 IPアドレスを範囲指定する場合、範囲の開始とするIPアドレスを入力します。
終了IPアドレス	IPアドレスを範囲指定する場合、範囲の終了とするIPアドレスを入力します。 単一のIPアドレスを指定する場合、入力する必要はありません。
個別ルール	アカウントに個別ルールが適用されている場合、"ルール個別適用" と出力されます。値の設定はできません。

■ アカウント形式の場合

- フォーマット

アカウント名	パスワード	グループ名	メールアドレス	アカウント種別	コメント	個別ルール

- 入力例

"user01",	"password",	"グループA¥グループB",	"user01@netstar.jp",	"1",	"任意のコメント",	"ルール個別適用"

フィールド名	設定内容
アカウント名	アカウント名を入力します。
パスワード	パスワードを入力します。
グループ名	グループ名を入力します。 上位グループが存在する場合、「第1階層¥第2階層¥第3階層」のように、第1階層から「¥」または「\」(バックスラッシュ) で区切って入力します。
メールアドレス	メールアドレスを入力します。
アカウント種別	0:一般ユーザ 1:グループ管理者(閲覧のみ) 2:グループ管理者(制限付き) 3:グループ管理者 4:システム管理者(閲覧のみ) 5:システム管理者(制限付き) 6:システム管理者 7:グループ管理者(例外URL設定のみ) 8:システム管理者(例外URL設定のみ)
コメント	任意のコメントを指定できます。 コメントが不要な場合、入力する必要はありません。
個別ルール	アカウントに個別ルールが適用されている場合、" ルール個別適用 " と出力されます。値の設定はできません。

■ 注意事項

CSVファイルを作成、編集するときには、次のことに注意してください。

- ファイルの 1 行目にはフィールド名を入力したヘッダが必要です。
- すべてのフィールドを"」で囲んでください。また、フィールドの区切り文字は「,」(半角カンマ) を使用してください。
- 一括登録するユーザの所属するグループが ISWM に登録されていない場合、自動的にグループが作成されます。
- IP アドレスの範囲が不正な場合、エラーが発生します。
- 一括登録する場合、登録済みの IP アドレス、アカウントが含まれていると、エラーが発生します。
  管理画面から操作した場合、システムログの ctrl.log ファイルが出力されます。詳しくは、「ログファイルの内容」(369 ページ)を参照してください。また、コマンドラインインタフェースを使用した場合、amserror.log ファイルが出力されます。詳しくは、「A-2. amserror.log について」(385 ページ)を参照してください。
- 重複した IP アドレスの設定については、「重複する IP アドレス設定」(122 ページ)を参照してください。
- IP アドレスを範囲で登録する場合、IP アドレスが「開始 IP アドレス」<「終了 IP アドレス」となるように入力してください。

6. IPアドレス設定一覧の確認

「IPアドレス有効範囲」では、各グループに登録したIPアドレスの設定を確認できます。階層が異なるグループ同士でIPアドレスの設定範囲が重複する場合、システムで有効な範囲が表示されます。詳細については、「重複するIPアドレス設定」(122ページ)を参照してください。

注意: システム管理者は、すべてのグループの設定を確認できます。
グループ管理者は、所属するグループおよび下位グループの設定を確認できます。

1. [グループ/ユーザ管理]-[IPアドレス有効範囲]をクリックします。

[IPアドレス有効範囲]が表示されます。

a. IPアドレス一覧を並び替えます。

[IPアドレス]ボタン	クリックすると、IPアドレスの昇順に表を並び替えます。
[グループ]ボタン	クリックすると、グループの昇順に表を並び替えます。

b. [IPアドレス有効範囲]画面には、[表示件数]で設定した件数が表示されます。設定した表示件数を超えてIPアドレスが登録されている場合は、ページを切り替えて表示してください。

	クリックすると、先頭のページが表示されます。
	クリックすると、前のページが表示されます。
	現在表示中のページ番号が表示されます。 表示したいページを直接指定することもできます。
	クリックすると、次のページが表示されます。
	クリックすると、最終のページが表示されます。

7. LDAP同期の設定

[LDAPユーザ同期]では、BASIC認証(LDAP連携)、NTLM認証またはKerberos認証設定後、登録したLDAPサーバをISWMと同期することができます。
詳細については、「5-11. LDAPサーバと同期する」(84ページ)を参照してください。

フィルタリングの設定

1. フィルタリング設定について

ISWMは、クライアントPCからのリクエストを受信すると、フィルタリング設定で設定した規制内容に従って、リクエスト先のURLの参照を許可または規制します。

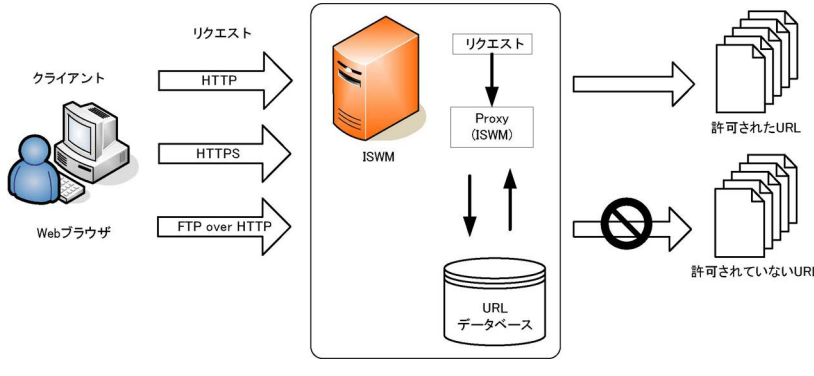
注意: フィルタリング可能なリクエスト種別は、HTTP、HTTPS、FTP over HTTP(ブラウザを使用したFTP)の3種類です。

1-1. フィルタリングの流れ

スタンドアロン版、ICAP版を使用した場合のフィルタリングの流れについて説明します。

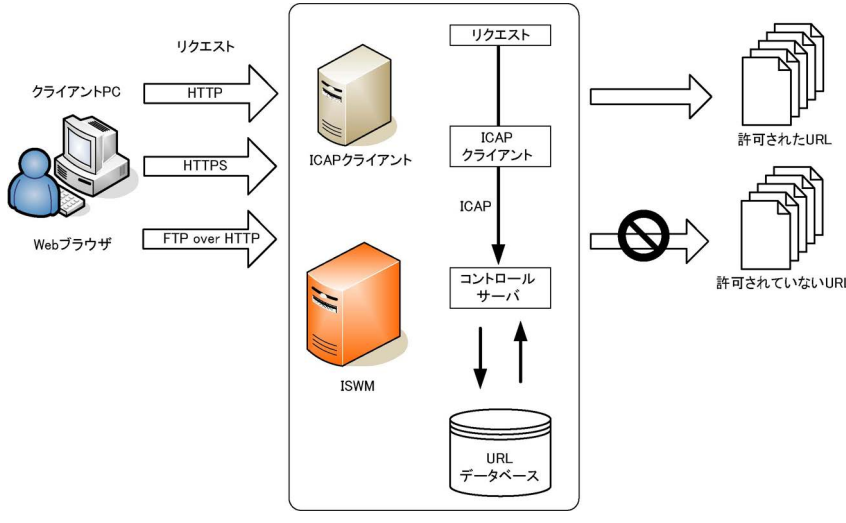
■ スタンドアロン版の場合

ISWMをインストールしたサーバがプロキシサーバとして動作します。
クライアントPCからのリクエストは、ISWMに送信され、フィルタリング設定に従って、リクエスト先のURLの参照を許可または規制します。



■ ICAP 版の場合

クライアントPCからのリクエストは、ICAPクライアントに送信されます。ICAPクライアントとISWMの間では、ICAPを使用して通信します。ISWMは、フィルタリング設定に従って、ICAPクライアントから受信したリクエスト先のURLの参照を許可または規制します。



1-2. フィルタリング機能の概要

クライアントPCからのリクエストをフィルタリングするためには、フィルタリング設定をする必要があります。ここでは、ISWMのフィルタリング設定について説明します。

■ フィルタリング設定の構成

フィルタリング設定は、[共通アクセス管理]および[個別アクセス管理]で行います。
[共通アクセス管理]では、すべてのグループ/ユーザに適用するフィルタリング設定をします。
[個別アクセス管理]では、グループ/ユーザに適用するフィルタリングルールを設定します。
[個別アクセス管理]で設定したフィルタリングルールを、[グループ/ユーザ管理]でグループ/ユーザに適用します。
設定の流れについては、「1-6. フィルタリング設定の流れ」(175ページ)を参照してください。

● 共通アクセス管理の場合

共通アクセス管理でのフィルタリング設定には、次の設定内容があります。

HTTPS 規制
クライアントPCからHTTPSサイトのURLにリクエストした場合にディレクトリ単位で規制する設定ができます。

高度分類クラウド
データベースでカテゴリ分類できなかったURLや例外URLに対して、未分類だったURLをクラウドで分類するための設定をします。

ブラウザ規制
特定のブラウザを使用したアクセスを規制するか、許可するかを設定します。
規制または許可の対象とするブラウザを設定できます。

検索キーワード規制
検索サイトなどで、指定したキーワードを使用した検索を規制するかどうかを設定します。
規制対象とする検索キーワードを設定できます。

書き込みキーワード規制
掲示板などで、指定したキーワードを使用した書き込み(POST リクエスト)を規制するかどうか設定します。
規制対象とする書き込みキーワードを設定できます。

規制画面
規制を実施したときにユーザへ通知する規制画面を設定します。

カテゴリ名
ユーザ設定サブカテゴリ名を設定できます。

規制オプション
POSTリクエストを規制する場合の書き込み許容サイズを設定します。

ヘッダ編集
特定のサイトに対して、クライアントからのリクエストヘッダに追加するヘッダの内容を設定します。

● 個別アクセス管理の場合

個別アクセス管理でのフィルタリング設定には、次の設定内容があります。

カテゴリルール

不法、アダルト、ショッピングなど、複数のカテゴリに分類されたWebサイトへの規制を設定します。また、サブカテゴリが存在するカテゴリでは、サブカテゴリ単位に規制内容を設定できます。

カテゴリ別のフィルタリング対象URLは、ネットスター社のURLデータベースから取得します。

URLデータベースは定期的に更新され、常に最新のURLデータベースを使用できます。

スケジュール

フィルタリング対象のグループやユーザに対して、適用するカテゴリルールと、ルールを適用する時間帯を設定します。

スケジュールには、デフォルトで適用される基本設定と、曜日、時間帯ごとに設定できる時間帯設定、祝日や特定の日付に適用される祝日設定の3種類があります。

注意: 祝日設定に割り当てる祝日や特定の日付は、設定ファイル(cal.inf)で設定します。詳しくは、「B. 設定ファイル」(440ページ)を参照してください。

例外 URL

カテゴリルールの例外として、アクセスを規制するURLを設定します。

また、規制対象のURLを「許可」または「閲覧のみ許可」に設定できます。「許可」に設定すると、規制対象URLでも自由にアクセスできるようになります。「閲覧のみ許可」に設定すると、規制対象URLでも閲覧のみできるようになります。

例外 URL スケジュール

フィルタリング対象のグループに対して、適用する例外URLルールと、ルールを適用する時間帯を設定します。

例外URLスケジュールには、デフォルトで適用される基本設定と、曜日、時間帯ごとに設定できる時間帯設定があります。

例外サービス

カテゴリルールの例外として、アクセスを許可するサービスを設定します。

規制対象のサービスを「許可」または「閲覧のみ許可」に設定できます。「許可」に設定すると、規制対象URLでも自由にアクセスできるようになります。「閲覧のみ許可」に設定すると、規制対象URLでも閲覧のアクセスを許可します。

優先カテゴリ

クライアントPCからリクエストしたURLが複数のカテゴリに該当する場合の優先カテゴリを設定します。

ブラウザ規制

特定のブラウザを使用したアクセスを規制するか、許可するかを設定します。

規制または許可の対象とするブラウザを設定できます。

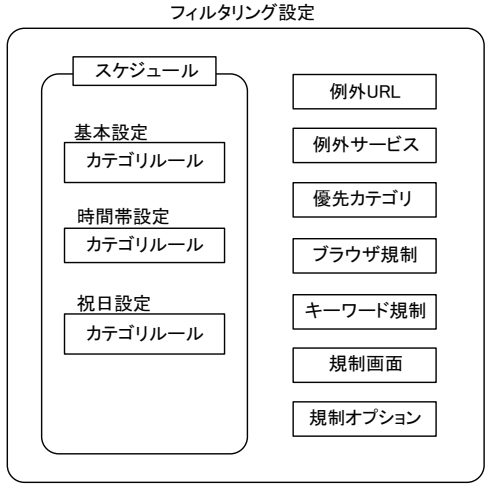
検索キーワード規制
検索サイトなどで、指定したキーワードを使用した検索を規制するよう設定している場合に、規制対象とする検索キーワードを設定します。

書き込みキーワード規制
掲示板などで、指定したキーワードを使用した書き込み(POSTリクエスト)を規制するよう設定している場合に、規制対象とする書き込みキーワードを設定します。

規制画面
規制を実施したときにユーザへ通知する規制画面を設定します。

規制オプション
IPアドレスを使用したURLの規制、規制を一時解除する場合の解除時間やパスワードなどを設定します。
また、POSTリクエストを規制する場合の書き込み許容サイズを設定できます。

これらのフィルタリング設定は、次の図のようになります。



■ フィルタリング設定対象

フィルタリング設定対象は、以下のとおりです。
[共通アクセス管理]で設定したフィルタリング設定は、すべてのグループ/ユーザに適用します。
[個別アクセス管理]で設定したフィルタリングルールは、グループ/ユーザに適用します。
「フィルタリング設定例」(166ページ)を参照してください。

● 共通アクセス管理の場合

共通アクセス管理でのフィルタリングの設定対象は、すべてのグループ/ユーザです。

● 個別アクセス管理の場合

個別アクセス管理でのフィルタリングの設定対象は以下のとおりです。グループ管理者は、所属グループおよび下位グループのフィルタリングを設定できます。

- グループ単位
- グループ内の特定ユーザ

注意:
- グループ単位、グループ内の特定ユーザに対してフィルタリング設定を適用する場合、[サーバ管理]-[認証設定]でユーザ認証を有効にしてください。「5. ユーザ認証/LDAPの設定」(60ページ)を参照してください。[サーバ管理]を操作できるのは、システム管理者だけです。
- [サーバ管理]-[認証設定]で「未登録ユーザ設定」が有効な場合、認証できないユーザに対して「未登録ユーザ」グループのフィルタリング設定が適用されます。なお、[サーバ管理]を操作できるのは、システム管理者だけです。
- ユーザ認証が有効でない場合、すべてのユーザにルートグループのフィルタリング設定が適用されます。

■ カテゴリルールの設定

カテゴリルールの設定、規制内容などについて説明します。
設定については、「5-1. カテゴリルールの設定」(214ページ)を参照してください。

カテゴリ、サブカテゴリ単位で規制が可能

不法、アダルト、ショッピングなど、複数のカテゴリに分類されたWebサイトへの規制を設定します。また、サブカテゴリの存在するカテゴリでは、サブカテゴリ単位に規制内容を設定できます。

カテゴリルールは、グループごとに複数登録できます。下位グループでは、上位グループのルールをベースとして使用できます。

注意: カテゴリごとに規制画面に表示するメッセージを設定できます。
設定については、「5-10. 規制画面の設定」(296ページ)を参照してください。

規制レベル

規制レベルには、「動作の規制レベル」と「一時解除方法の規制レベル」があります。

動作の規制レベル	動作		一時解除方法の規制レベル	一時解除方法		説明
ゆるい		許可	なし	なし		自由にアクセスを許可します。
↓		書き込み規制	ゆるい		一時解除可能(パスワードなし)	規制画面を表示しますが、一定時間だけ掲示板などへの書き込みができます。閲覧は可能です。
			↓		一時解除可能(パスワードあり)	掲示板などへの書き込みするためのパスワード(一時解除パスワード)を設定して、書き込みを制限できます。閲覧は可能です。
			厳しい		一時解除不可	掲示板などへの書き込みを禁止します。閲覧は可能です。
厳しい		規制	ゆるい		一時解除可能(パスワードなし)	規制画面を表示しますが、一定時間だけ閲覧ができます。
			↓		一時解除可能(パスワードあり)	閲覧するためのパスワード(一時解除パスワード)を設定して、アクセスを制限できます。
			厳しい		一時解除不可	アクセスを規制して、規制画面を表示します。

■ フィルタリング実行スケジュールの設定

グループごとに作成したカテゴリルールを適用するスケジュールには、次の3種類の設定があります。

詳細については、「1-3. スケジュール種別」(167ページ)を参照してください。

基本設定	デフォルトで適用するカテゴリルールを設定します。
時間帯設定	指定した曜日、時間帯に適用するカテゴリルールを設定します。
祝日設定	指定した日付に適用するカテゴリルールを設定します。

■ 指定した URL をフィルタリング対象に登録可能

URLデータベースに含まれないURLを「例外URL」として、フィルタリング対象に登録できます。URL(HTTP、HTTPS、FTP)のほかにも、指定した文字列が含まれる場合などを設定できます。
設定については、「5-3. 例外URLの設定」(230ページ)を参照してください。

■ 規制対象の URL を「許可」または「閲覧のみ許可」に設定可能

例外URLの[許可カテゴリ]-[許可カテゴリ]にURLを登録すると、フィルタリング用データベースで「規制」として登録されているURLに自由にアクセスできるようになります。
例外URLの[許可カテゴリ]-[閲覧のみ許可]にURLを登録すると、フィルタリング用データベースで「規制」として登録されているURLを閲覧できるようになります。ただし、書き込みはできません。
設定については、「5-3. 例外URLの設定」(230ページ)を参照してください。

■ 規制対象の URL でもサービスで「許可」に設定可能

例外サービスの[動作設定]で[許可]にすると、フィルタリング用データベースで「規制」として登録されているURLのサービスでも自由にアクセスできるようになります。また、[閲覧のみ許可]にすることで、フィルタリング用データベースで「規制」として登録されている URL のサービスへの閲覧のアクセスを許可します。
設定については、「3-5. 例外サービスの設定」(184ページ)を参照してください。

■ グループとフィルタリング設定

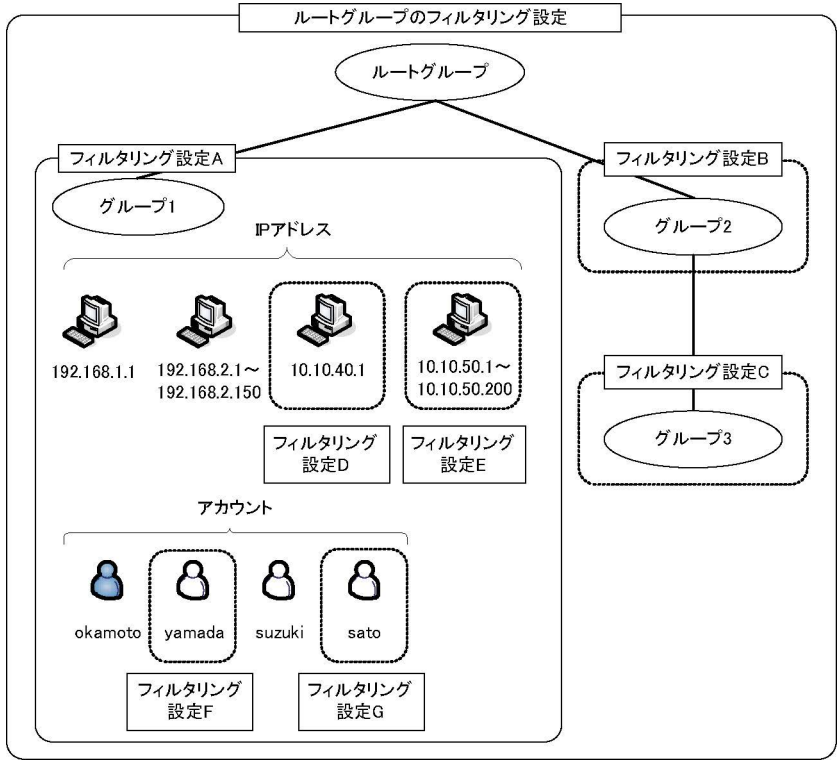
上位グループと下位グループの間で、フィルタリング設定を参照できます。
多くのグループで構成される場合でも、上位グループのフィルタリング設定を下位グループで参照することで、上位グループから一元管理できます。
詳細については、「1-5. フィルタリング設定の参照」(170ページ)を参照してください。

■ グループ内の特定ユーザへのフィルタリング設定

グループ内のアカウントまたはIPアドレスを、グループに適用するフィルタリング設定とは異なるフィルタリング設定を適用できます。「フィルタリング設定例」(166ページ)を参照してください。
グループ内の特定ユーザにフィルタリング設定するには、[グループ/ユーザ管理]-[ユーザ管理]で設定します。
詳細については、「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

注意: 例外URLなど、[グループ/ユーザ管理]-[ユーザ管理]で設定できない項目については、ユーザが所属するグループに設定されたフィルタリング設定が適用されます。

■ フィルタリング設定例



上の図のグループとフィルタリング設定の対応は次のようになります。

設定名	適用グループ / ユーザ	設定
ルートグループのフィルタリング設定	全ユーザ (ユーザ認証が無効の場合)	[グループ/ユーザ管理]-[グループ管理]
フィルタリング設定 A	グループ1	
フィルタリング設定 B	グループ2	
フィルタリング設定 C	グループ3	

設定名	適用グループ / ユーザ	設定
フィルタリング設定 D	IPアドレス「10.10.40.1」の端末	[グループ/ユーザ管理]-[ユーザ管理]
フィルタリング設定 E	IPアドレス「10.10.50.1~10.10.50.200」の端末	
フィルタリング設定 F	アカウント「yamada」	
フィルタリング設定 G	アカウント「sato」	

1-3. スケジュール種別

■ スケジュール設定の構成

スケジュール設定には、基本設定、時間帯別設定、祝日設定の3種類があります。

基本設定

グループの基本カテゴリルールを設定します。基本設定は、時間帯別設定または祝日設定と重複しない期間に適用されます。新規グループを登録した場合、初期状態では上位グループの基本設定が登録されます。

基本設定は、すべての曜日に 24 時間設定されます。特定の曜日または時間帯に別のカテゴリルールを適用する場合には、時間帯設定を使用します。

設定については、「5-2. スケジュールの設定」(222ページ)を参照してください。

時間帯別設定

特定の曜日、時間帯に適用するカテゴリルールを設定します。

月曜から金曜の就業時間中と就業時間外、土日の設定など、適用するカテゴリルールを詳細に設定できます。

設定については、「5-2. スケジュールの設定」(222ページ)を参照してください。

祝日設定

指定した日付に、指定した曜日のスケジュールを適用します。祝日など、日付は固定で、曜日が不定な場合などに使用します。

たとえば、年末年始や創立記念日などの特別な休日を「日曜日」に設定すると、日曜日のスケジュールを適用します。また、日曜日や祝日に特別営業する日を「月曜日」に設定すると、月曜日のスケジュールを適用します。

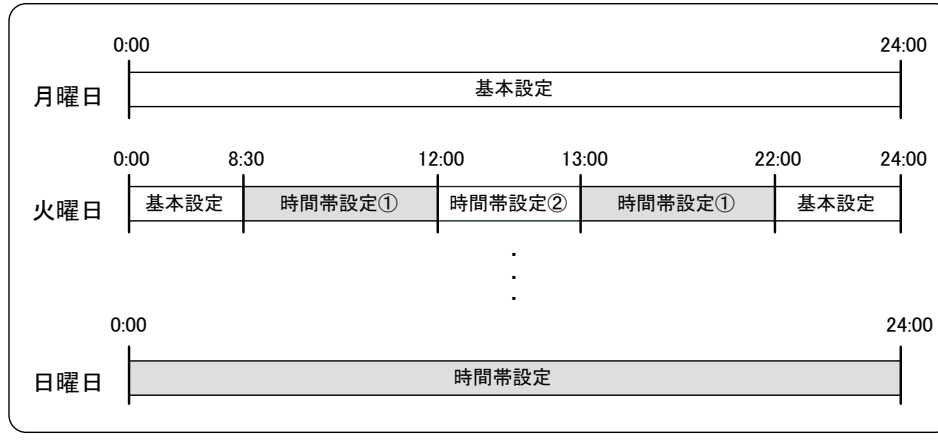
祝日設定は、設定ファイル(cal.inf)を編集して設定します。詳細については、「B. 設定ファイル」(440ページ)を参照してください。cal.infの初期状態では、国民の祝日が日曜日として設定されています。

例:

勤務時間内(時間帯設定①)には、旅行やスポーツなどの業務に関係ないカテゴリを、閲覧禁止に設定します。

また、勤務時間外(時間帯設定②と基本設定)には、業務に関係ないカテゴリを、閲覧許可に設定します。

基本設定と時間帯設定 (スケジュール設定で設定)



例:

年末年始の休暇が1月1日から1月3日までの場合、祝日設定で「日曜」に設定すると、日曜日のスケジュールを適用します。

祝日設定(cal.infで設定)

1-4. パス内 URL 規制機能

翻訳サイトや検索サイトなどで、リクエスト先のURLに別のURLを含む形式のリクエストに対してフィルタリング設定を適用できます。また、掲示板などで使用される、パラメータ内にURLを含む形式のリクエストに対してもフィルタリング設定を適用できます。

注意: リクエスト内に含まれるURLはHTTPまたはHTTPSプロトコルのみ対応しています。

■ 規制可能なリクエスト形式

パス内URL規制機能は、以下の3種類のリクエスト形式に対応しています。

リクエストされた URL の先頭以降に「http://」または「https://」が含まれるリクエスト

「http://」または「https://」以降の部分をURLとしてフィルタリング設定を適用します。
以下のURLでは、「http://game.netstar.jp/」をURLとしてフィルタリング設定を適用します。
http://archive.netstar.jp/web/20061016/http://game.netstar.jp/

CGI など、パラメータ内に URL が含まれるリクエスト

リクエストされたURLで、「?」以降の部分がパラメータを意味します。パラメータは「パラメータ=設定値」の形式となります。1つのURLに複数のパラメータが存在する場合、パラメータ間は「&」で区切られます。
登録されたパラメータが含まれる URL がリクエストされると、パラメータから文字列を抽出してフィルタリング設定を適用します。
以下のリクエストでは、「url=game.netstar.jp/English/」、「lang=ja」、「code=UTF-8」の3つのパラメータが含まれています。この場合、リクエストから「game.netstar.jp/English/」を抽出して、フィルタリング設定を適用します。
http://honyaku.netstar.jp/honyaku.cgi?url=game.netstar.jp/English/index.html&lang=ja&code=UTF-8

注意: パラメータ内でプロトコル部分が省略された形でURLが含まれている場合、HTTPプロトコルのURLとしてフィルタリング設定を適用します。

「nph-proxy.cgi」または「nph-proxy.pl」の文字列が含まれるリクエスト

URLのパス部に「nph-proxy.cgi」または「nph-proxy.pl」の文字列が含まれている場合は、nph-proxyを利用していると判断し、URLを抽出してフィルタリング設定を適用します。
以下のURLでは、[スキーム]と[ドメイン]と[パス]が結合されてパス内URLとして抽出されます。
http://[元URLのドメイン:元URLのポート]/[元URLのパス先頭]/nph-proxy.cgi/[文字列]/[スキーム]/[ドメイン]/[パス]

注意: [文字列] は nph-proxy ごとの設定で不特定の文字列のため無視されます。「nph-proxy.cgi（またはnph-proxy.pl」から[スキーム]までのパス部を[文字列]として扱います。

1-5. フィルタリング設定の参照

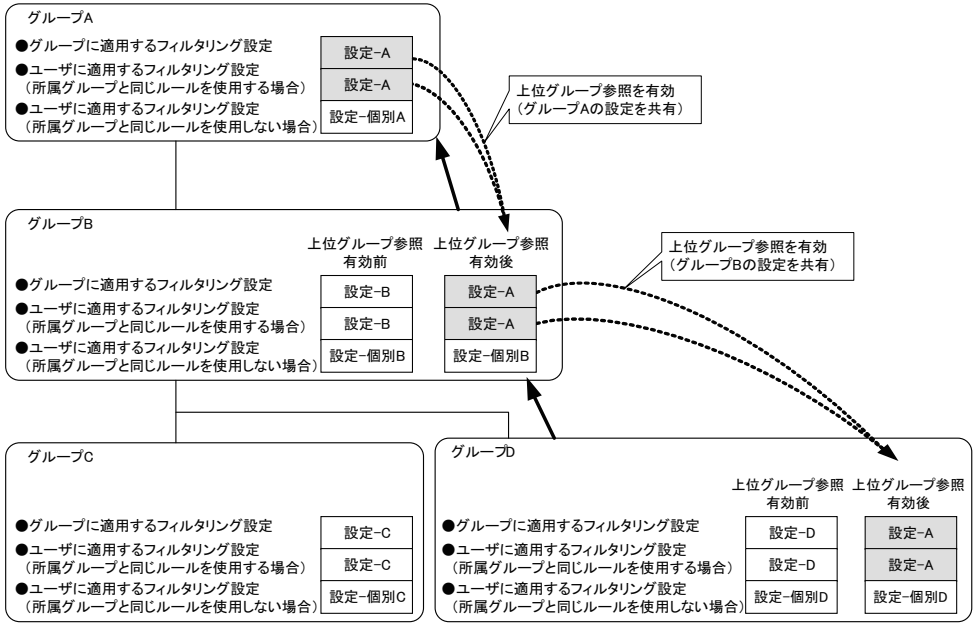
上位グループで作成したフィルタリング設定を、下位グループから参照できます。
また、上位グループのフィルタリング設定を下位グループに強制的に参照させることが可能です。

■ 上位グループ参照

上位グループ参照を有効にすると、上位グループで作成したフィルタリング設定を参照できます。
上位グループ参照を有効にしたグループでは、ユーザのフィルタリング設定だけが可能です。

グループに適用するフィルタリング設定	上位グループの設定を参照します。
ユーザに適用するフィルタリング設定（所属グループと同じルールを使用する場合）	上位グループの設定を参照します。
ユーザに適用するフィルタリング設定（所属グループと同じルールを使用しない場合）	上位グループの設定を参照しません。

上位グループ参照は、[グループ/ユーザ管理]-[グループ管理]で設定できます。
上位グループ参照を無効にする場合、参照している上位グループのフィルタリング設定がコピーされます。
次の図では、グループB、グループDで上位グループ参照を有効にしています。
グループBの上位グループ参照の有効、無効を切り替えると、グループDで参照している設定は、グループBの最新の設定に変更されます。

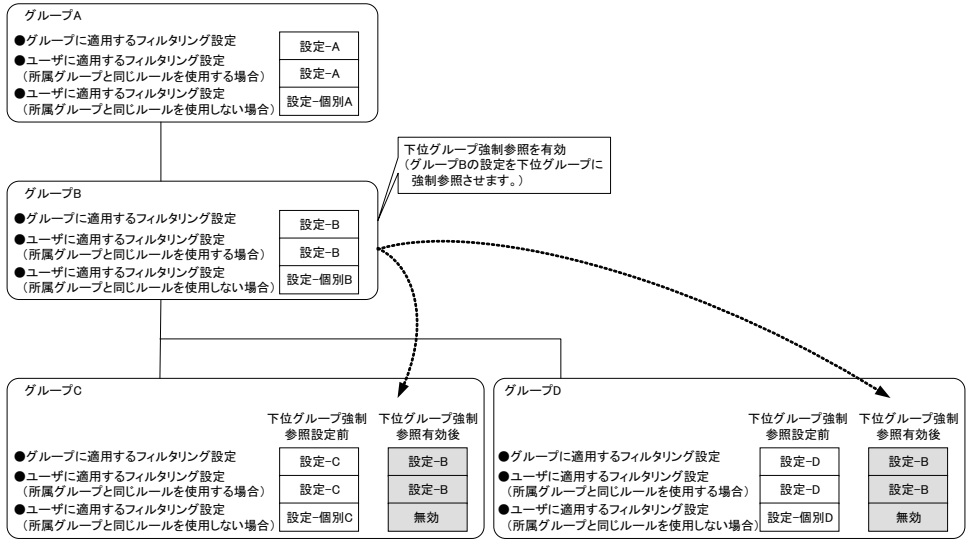


■ 下位グループ強制参照

下位グループ強制参照を有効にすると、下位グループに、フィルタリング設定を強制的に参照させることが可能です。
参照させる設定は、自グループのすべてのフィルタリング設定です。下位グループでは、適用されるフィルタリング設定の確認だけが可能です。
下位グループ強制参照は、[グループ/ユーザ管理]-[グループ管理]で設定できます。

注意:
- 下位グループ強制参照を有効にすると、下位グループではフィルタリングの設定ができません。
  また、下位グループのユーザに適用するフィルタリング設定(所属グループと同じルールを使用しない場合)も無効になります。
- 下位グループ強制参照を無効にした場合、下位グループでは、参照しているフィルタリング設定の内容が設定されます。下位グループのユーザに適用するフィルタリング設定(所属グループと同じルールを使用しない場合)は、もう一度設定する必要があります。

次の図では、グループBで下位グループ強制参照を有効にしています。
グループC、グループDのフィルタリング設定(グループ、ユーザ)は無効になり、グループBのフィルタリング設定を参照します。
グループBで、下位グループ強制参照を無効にすると、グループC、グループDは参照しているグループBの内容が設定されます。

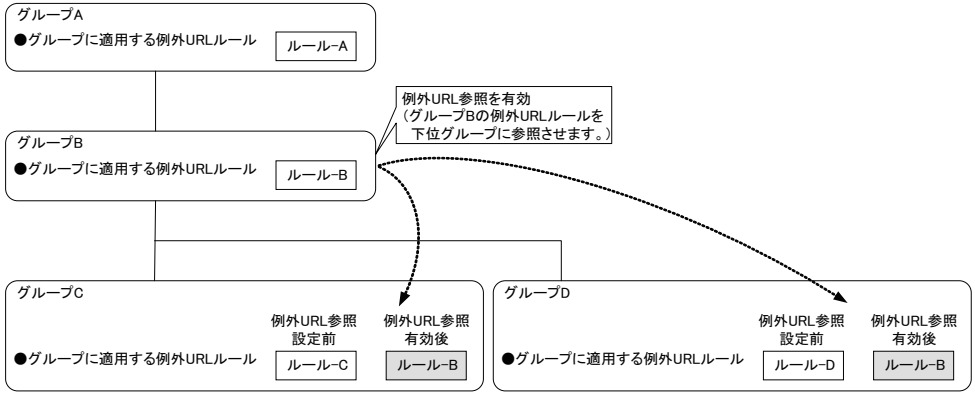


■ 例外 URL 参照

例外URL参照を有効にすると、下位グループに、例外URLルールを参照させることが可能です。
例外URLは下位グループに適用されますが、下位グループ側でも個別ルールを適用できます。
例外URL参照は、[グループ/ユーザ管理]-[グループ管理]で設定できます。

注意:
- ユーザに例外URLルールの適用はできません。
- 例外 URL 参照を無効にした場合、下位グループでは、参照している例外 URL ルールが適用されます。

次の図では、グループBで例外URL参照を有効にしています。
グループC、グループDの例外URLルール(ルールCおよびルールD)が有効で、かつ上位のグループBの例外URLルールも参照します。
参照している上位の例外URLルールと各グループで設定した例外URLルールは別ルールとして各グループに適用されます。そのため、グループ B で例外 URL 参照を無効にした場合でも、各グループの例外URLルール(ルールCおよびルールD)には影響を与えません。



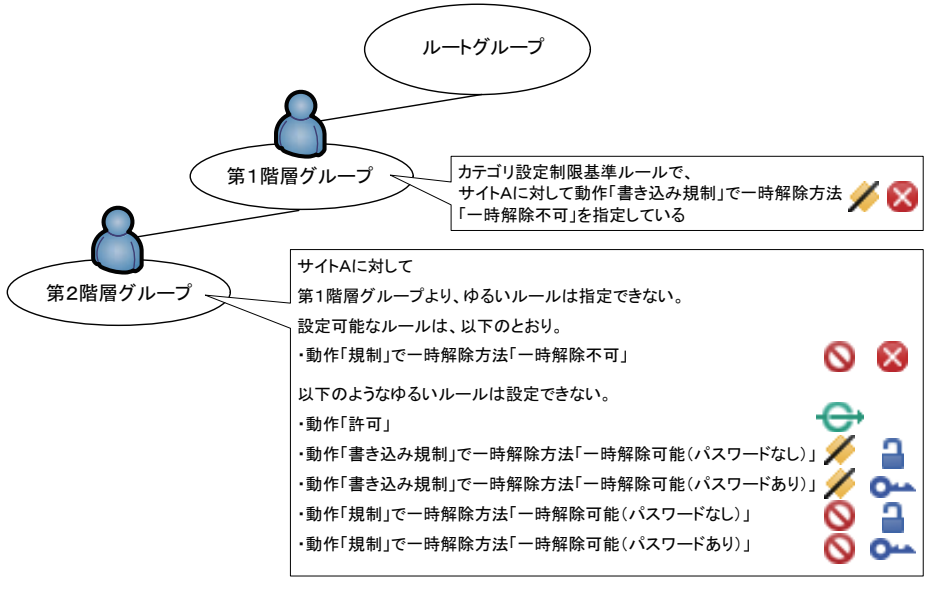
■ カテゴリ設定制限

カテゴリ設定制限を有効にすると、下位グループのカテゴリ関連ルールに設定制限を設けることが可能です。
特定のカテゴリルールを、カテゴリ設定制限基準ルールに設定できます。カテゴリ設定制限基準ルールを設定すると、下位グループではカテゴリ設定制限基準ルールの規制内容がベースとなり、規制をゆるめることができません。
上位グループのルールをカテゴリ設定制限基準ルールとして設定すると、下位グループのカテゴリルールが、上位グループよりもゆるい規制内容になってしまうことや、設定漏れを防ぎます。

注意:
- カテゴリ設定制限基準ルールは、1グループで1ルールだけ設定できます。
- カテゴリ設定制限基準ルールを設定した場合、下位グループでは、カテゴリ設定制限基準ルールおよび下位グループのカテゴリルールだけをベースにできます。
  たとえば、ルートグループでカテゴリ設定制限基準ルールを設定すると、すべてのグループにカテゴリ設定制限が有効になります。
- 他のグループのルールをスケジュールで使用しているときにカテゴリ設定制限基準ルールを適用すると、下位グループは指定したカテゴリ設定制限基準ルールに置き換わります。

次の図のように、上位グループのあるカテゴリに対して動作「書き込み規制」で一時解除方法「一時解除不可」をカテゴリ設定制限基準ルールに設定すると、下位グループでは、以下のようなゆるいルールは設定できません。

- 動作「許可」
- 動作「書き込み規制」で一時解除方法「一時解除可能(パスワードなし)」
- 動作「書き込み規制」で一時解除方法「一時解除可能(パスワードあり)」
- 動作「規制」で一時解除方法「一時解除可能(パスワードなし)」
- 動作「規制」で一時解除方法「一時解除可能(パスワードあり)」



注意: 動作「書き込み規制」で一時解除方法「一時解除不可」は、動作「規制」で一時解除方法「一時解除可能(パスワードなし)」または「一時解除可能(パスワードあり)」より厳しい規制レベルと判断されます。
動作の規制レベルでは「書き込み規制」は「規制」よりゆるいが、一時解除方法の規制レベルでは「一時解除不可」が「一時解除可能(パスワードなし)」または「一時解除可能(パスワードあり)」より厳しく、一時解除方法の規制レベルが優先されるからです。

1-6. フィルタリング設定の流れ

フィルタリング設定には、グループに適用する設定とユーザに適用する設定の2種類があります。それぞれの設定の流れについて説明します。

■ グループのフィルタリング設定

グループごとのフィルタリング設定の流れは次のようになります。

注意: ユーザ認証が有効になっていない場合には、ルートグループのフィルタリング設定が適用されます。

1. 共通アクセスの設定

すべてのグループに適用するフィルタリング設定をします。
共通アクセスの設定→「4. 共通アクセスの設定」(187ページ)

a. HTTPS規制の設定

クライアントPCからHTTPSサイトのURLにリクエストした場合にディレクトリ単位で規制する設定をします。
HTTPS規制の設定→「4-1. HTTPS規制の設定」(187ページ)

b. 高度分類クラウドの設定

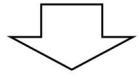
データベースでカテゴリ分類できなかったURLや例外URLに対して未分類だったURLに対して、クラウドで分類するための設定をします。
高度分類クラウドの設定→「4-2. 高度分類クラウドの設定」(194ページ)

c. その他のルールの設定

クライアントPCのWebブラウザの規制、規制するキーワード、規制を実施したときにユーザへ通知する規制画面などを設定します。
ブラウザ規制の設定→「4-3. ブラウザ規制の設定」(196ページ)
検索キーワード規制の設定→「4-4. 検索キーワード規制の設定」(201ページ)
書き込みキーワード規制の設定→「4-5. 書き込みキーワード規制の設定」(204ページ)
規制画面の設定→「4-6. 規制画面の設定」(207ページ)
規制オプションの設定→「4-8. 規制オプションの設定」(211ページ)
ヘッダ編集の設定→「4-9. ヘッダ編集の設定」(212ページ)

d. カテゴリ名の設定

ユーザ設定サブカテゴリ名を設定します。
カテゴリ名の設定→「4-7. カテゴリ名の設定」(211ページ)



2. 個別アクセスの設定

グループに適用するフィルタリングルールを設定します。
個別アクセスの設定→「5. 個別アクセスの設定」(214ページ)

a. カテゴリルールの設定

グループに適用するカテゴリルールを設定します。
カテゴリ別に規制内容を選択して、カテゴリルールを設定します。
カテゴリの設定→「5-1. カテゴリルールの設定」(214ページ)

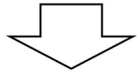
b. スケジュールの設定

グループに適用するスケジュールを設定します。
フィルタリング対象のグループに対して、適用するカテゴリ/例外URLルールと、ルールを適用する時間帯を設定します。
スケジュールの設定→「5-2. スケジュールの設定」(222ページ)
例外URLスケジュールの設定→「5-4. 例外URLスケジュールの設定」(247ページ)

c. その他のルールの設定

カテゴリルールの例外としてアクセスを規制するURL、利用を制限するサービス、クライアントPCからリクエストしたURLが複数のカテゴリに該当する場合の優先カテゴリ、クライアントPCのWebブラウザの規制、規制するキーワード、規制を実施したときにユーザへ通知する規制画面などを設定します。
例外URLの設定→「5-3. 例外URLの設定」(230ページ)
例外サービスの設定→「5-5. 例外サービスの設定」(255ページ)
優先カテゴリの設定→「5-6. 優先カテゴリの設定」(264ページ)
ブラウザ規制の設定→「5-7. ブラウザ規制の設定」(271ページ)
検索キーワード規制の設定→「5-8. 検索キーワード規制の設定」(280ページ)
書き込みキーワード規制の設定→「5-9. 書き込みキーワード規制の設定」(288ページ)
規制画面の設定→「5-10. 規制画面の設定」(296ページ)

規制オプションの設定→「5-11. 規制オプションの設定」(302ページ)



3. フィルタリングルールをグループに適用

設定したフィルタリングルールを、グループに適用します。

フィルタリングルールをグループに適用→「6-1. フィルタリングルールをグループに適用」(310ページ)

■ ユーザのフィルタリング設定

ユーザへのフィルタリング設定の流れは次のようになります。

1. 共通アクセスの設定

すべてのユーザに適用するフィルタリング設定をします。
共通アクセスの設定→「4. 共通アクセスの設定」(187ページ)

a. HTTPS規制の設定

クライアントPCからHTTPSサイトのURLにリクエストした場合にディレクトリ単位で規制する設定をします。
HTTPS規制の設定→「4-1. HTTPS規制の設定」(187ページ)

b. 高度分類クラウドの設定

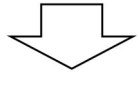
データベースでカテゴリ分類できなかったURLや例外URLに対して未分類だったURLに対して、クラウドで分類するための設定をします。
高度分類クラウドの設定→「4-2. 高度分類クラウドの設定」(194ページ)

c. その他のルールの設定

クライアントPCのWebブラウザの規制、規制するキーワード、規制を実施したときにユーザへ通知する規制画面などを設定します。
ブラウザ規制の設定→「4-3. ブラウザ規制の設定」(196ページ)
検索キーワード規制の設定→「4-4. 検索キーワード規制の設定」(201ページ)
書き込みキーワード規制の設定→「4-5. 書き込みキーワード規制の設定」(204ページ)
規制画面の設定→「4-6. 規制画面の設定」(207ページ)
規制オプションの設定→「4-8. 規制オプションの設定」(211ページ)
ヘッダ編集の設定→「4-9. ヘッダ編集の設定」(212ページ)

d. カテゴリ名の設定

ユーザ設定サブカテゴリ名を設定します。
カテゴリ名の設定→「4-7. カテゴリ名の設定」(211ページ)



2. 個別アクセスの設定

ユーザに適用するフィルタリングルールを設定します。
個別アクセスの設定→「5. 個別アクセスの設定」(214ページ)

a. カテゴリルールの設定

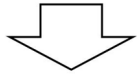
ユーザに適用するカテゴリルールを設定します。
カテゴリ別に規制内容を選択して、カテゴリルールを設定します。
カテゴリの設定→「5-1. カテゴリルールの設定」(214ページ)

b. スケジュールの設定

ユーザに適用するスケジュールを設定します
フィルタリング対象のユーザに対して、適用するカテゴリルールと、ルールを適用する時間帯を設定します。
スケジュールの設定→「5-2. スケジュールの設定」(222ページ)

c. その他のルールの設定

クライアントPCのWebブラウザの規制、規制するキーワード、規制を実施したときにユーザへ通知する規制画面などを設定します。
ブラウザ規制の設定→「5-7. ブラウザ規制の設定」(271ページ)
検索キーワード規制の設定→「5-8. 検索キーワード規制の設定」(280ページ)
書き込みキーワード規制の設定→「5-9. 書き込みキーワード規制の設定」(288ページ)
規制オプションの設定→「5-11. 規制オプションの設定」(302ページ)



3. フィルタリングルールをユーザに適用

設定したフィルタリングルールを、ユーザに適用します。
フィルタリングルールをユーザに適用→「6-2. フィルタリングルールをユーザに適用」(323ページ)

2. [共通アクセス管理]画面でできること

[共通アクセス管理]画面では、すべてのグループ/ユーザに適用するフィルタリング設定をします。
[共通アクセス管理]画面のサブメニューで設定する内容について説明します。
設定の詳細については、次の表を参照してください。

設定	参照先	適用範囲
HTTPS 規制設定	「4-1. HTTPS規制の設定」(187ページ)	すべてのグループ/ユーザ
高度分類クラウド設定	「4-2. 高度分類クラウドの設定」(194ページ)	
ブラウザ規制設定	「4-3. ブラウザ規制の設定」(196ページ)	
検索キーワード規制設定	「4-4. 検索キーワード規制の設定」(201ページ)	
書き込みキーワード規制設定	「4-5. 書き込みキーワード規制の設定」(204ページ)	
規制画面設定	「4-6. 規制画面の設定」(207ページ)	
カテゴリ名設定	「4-7. カテゴリ名の設定」(211ページ)	
規制オプション設定	「4-8. 規制オプションの設定」(211ページ)	
ヘッダ編集設定	「4-9. ヘッダ編集の設定」(212ページ)	

2-1. HTTPS規制の設定

HTTPS規制設定では、HTTPSプロトコルの詳細なディレクトリ単位でのフィルタリングの有効/無効を設定します。
HTTPS規制設定では、ISWMでHTTPS通信をデコードするサーバデコード方式が使用されます。

2-2. 高度分類クラウドの設定

データベースでカテゴリ分類できなかったURLをクラウドで分類するための設定です。
クラウドにより付与されたカテゴリはフィルタリングの対象となります。
ここで設定した内容は、すべてのグループ/ユーザーに適用されます。

注意: 高度分類クラウドは、ライセンスキーによる認証を行うため、ライセンスの有効期限が切れていると使用できません。

2-3. ブラウザ規制の設定

特定のブラウザを使用したアクセスを規制するか、許可するかを設定します。
規制または許可の対象とするブラウザを設定できます。
ここで設定した内容は、すべてのグループ/ユーザに適用されます。
[共通アクセス管理]-[ブラウザ規制設定]の設定が、[個別アクセス管理]-[ブラウザ規制設定]の設定よりも優先されます。

2-4. 検索キーワード規制の設定

検索サイトなどで、指定したキーワードを使用した検索を規制するかどうかを設定します。
規制対象とする検索キーワードを設定できます。
ここで設定した内容は、すべてのグループ/ユーザに適用されます。

2-5. 書き込みキーワード規制の設定

掲示板などで、指定したキーワードを使用した書き込み(POSTリクエスト)を規制するかどうかを設定します。
規制対象とする書き込みキーワードを設定できます。
ここで設定した内容は、すべてのグループ/ユーザに適用されます。

2-6. 規制画面の設定

規制画面に表示するファイルやURL、またはメッセージを設定します。
また、規制画面に表示するドメイン名を設定します。
規制画面とは、クライアントPCからリクエストしたURLの表示を、ISWMが規制したことを、ユーザに通知する画面です。

2-7. カテゴリ名の設定

カテゴリルールの「ユーザ設定カテゴリ」のサブカテゴリ名を設定します。
ここで設定したサブカテゴリ名は、カテゴリルールの設定時に全グループに共通して適用されます。

2-8. 規制オプションの設定

POSTリクエストを規制する場合の書き込み許容サイズを設定します。

規制オプション設定では、システム一括でサイズを設定するか、ルール毎にサイズを設定するかを選択できます。
[システム一括でサイズを設定する]を選択した場合は、すべてのグループ/ユーザに適用する、書き込み許容サイズを設定します。
[ルール毎にサイズを設定する]を選択した場合は、[個別アクセス管理]-[規制オプション設定]で個別に書き込み許容サイズを設定します。
また、複数のカテゴリに個別に書き込み許容サイズが設定された場合、判定する際の優先動作を[カテゴリ順で判定する] 、または [許容サイズのもっとも大きな値でのみ判定する] のどちらかに設定することができます。

2-9. ヘッダ編集の設定

サーバ送信時に追加するリクエストヘッダを設定します。
指定のドメインを対象として、クライアントブラウザからのリクエストヘッダに指定のヘッダを追加してサーバに送信します。

3. [個別アクセス管理]画面でできること

[個別アクセス管理]画面では、グループ/ユーザに適用するフィルタリングルールを設定します。
[個別アクセス管理]画面のサブメニューで設定する内容について説明します。
設定の詳細については、次の表を参照してください。

設定	参照先	適用範囲
カテゴリ設定	「5-1. カテゴリルールの設定」(214ページ)	グループ/ユーザ
スケジュール設定	「5-2. スケジュールの設定」(222ページ)	グループ/ユーザ
例外 URL 設定	「5-3. 例外URLの設定」(230ページ)	グループ
例外 URL スケジュール設定	「5-4. 例外URLスケジュールの設定」(247ページ)	グループ
例外サービス設定	「5-5. 例外サービスの設定」(255ページ)	グループ
優先カテゴリ設定	「5-6. 優先カテゴリの設定」(264ページ)	グループ
ブラウザ規制設定	「5-7. ブラウザ規制の設定」(271ページ)	グループ/ユーザ
検索キーワード規制設定	「5-8. 検索キーワード規制の設定」(280ページ)	グループ/ユーザ
書き込みキーワード規制設定	「5-9. 書き込みキーワード規制の設定」(288ページ)	グループ/ユーザ
規制画面設定	「5-10. 規制画面の設定」(296ページ)	グループ
規制オプション設定	「5-11. 規制オプションの設定」(302ページ)	グループ/ユーザ

3-1. カテゴリルールの設定

グループ/ユーザに適用するカテゴリルールを設定します。
不法、アダルト、ショッピングなど、複数のカテゴリに分類されたWebサイトへの規制を設定できます。

3-2. スケジュールの設定

グループ/ユーザに適用するスケジュールルールを設定します。

フィルタリング対象のグループやユーザに対して、適用するカテゴリルールと、ルールを適用する時間帯を設定できます。

3-3. 例外 URL の設定

グループに適用する例外URLルールを設定します。
カテゴリルールの例外として、アクセスを規制するURLを設定します。
また、規制対象のURLを「許可」または「閲覧のみ許可」に設定できます。
「許可」に設定すると、規制対象URLでも自由にアクセスできるようになります。「閲覧のみ許可」に設定すると、規制対象URLでも閲覧のみできるようになります。

3-4. 例外 URL スケジュールの設定

グループに適用する例外URLスケジュールルールを設定します。
カテゴリルールの例外として設定した例外 URL ルールについて、適用する時間帯を設定できます。

3-5. 例外サービスの設定

グループに適用する例外サービスルールを設定します。
カテゴリルールの例外として、アクセスを許可するサービスを設定します。
「許可」に設定すると、規制対象URLでも自由にアクセスできるようになります。「閲覧のみ許可」に設定すると、規制対象URLへの閲覧のアクセスを許可します。

3-6. 優先カテゴリの設定

グループに適用する優先カテゴリルールを設定します。
クライアントPCからリクエストしたURLが複数のカテゴリに該当する場合に優先するカテゴリを設定できます。

3-7. ブラウザ規制の設定

グループ/ユーザに適用するブラウザ規制ルールを設定します。
特定のブラウザを使用したアクセスを規制するか、許可するかを設定できます。
規制または許可の対象とするブラウザを設定します。
[共通アクセス管理]-[ブラウザ規制設定]の設定が、[個別アクセス管理]-[ブラウザ規制設定]の設定よりも優先されます。

3-8. 検索キーワード規制の設定

グループ/ユーザに適用する書き込みキーワード規制ルールを設定します。
規制対象とする書き込みキーワードを設定できます。
[共通アクセス管理]-[検索キーワード規制設定]の設定と合わせて規制されます。

3-9. 書き込みキーワード規制の設定

グループ/ユーザに適用する書き込みキーワード規制ルールを設定します。
規制対象とする書き込みキーワードを設定できます。
[共通アクセス管理]-[書き込みキーワード規制設定]の設定と合わせて規制されます。

3-10. 規制画面の設定

グループに適用する規制画面ルールを設定します。
規制画面に表示する画像、規制メッセージを設定できます。
規制画面とは、クライアントPCからリクエストしたURLの表示を、ISWMが規制したことを、ユーザに通知する画面です。

3-11. 規制オプションの設定

グループに適用する規制オプションルールを設定します。
IPアドレスを使用したURLの規制、規制を一時解除する場合の解除時間やパスワードなどを設定できます。
また、POSTリクエストを規制する場合の書き込み許容サイズを設定できます。
なお、書き込み許容サイズは、[共通アクセス管理]-[規制オプション設定]で[ルール毎にサイズを設定する]を選択した場合に設定できます。

4. 共通アクセスの設定

4-1. HTTPS規制の設定

HTTPS 規制を有効にすると、クライアント PC から HTTPS サイトの URL をリクエストした場合、ホスト名以降のディレクトリやファイル名まで含めた、きめ細かなフィルタリングが可能になります。
HTTPS 規制にはサーバデコード方式を使用しています。

注意: HTTPS規制を設定できるのは、システム管理者のみです。

ここではスタンドアロン版での HTTPS 規制の設定について説明します。

ICAP 版での HTTPS 規制の設定については、「■ ICAP 版での HTTPS 規制の設定」(193 ページ)を参照してください。

■ サーバデコード方式で規制する場合

ISWM で HTTPS 通信をデコードすることで、HTTPS リクエストをディレクトリ単位で規制します。

注意:
- サーバデコード方式を利用した HTTPS を使用した場合、クライアント側のブラウザで警告画面が表示されることがあります。詳細については、「G. 証明書のインストール」(489ページ)を参照してください。

1. [共通アクセス管理]-[HTTPS規制設定]をクリックします。

   [HTTPS規制設定]が表示されます。

2. 認証局を設定します。

   認証局証明書をダウンロードする場合は、[認証局証明書のダウンロード]のリンクをクリックし、ダウンロード先を指定して保存します。
   認証局を設定、または変更する場合は、[認証局変更]の[参照]ボタンをクリックし、認証局証明書のファイルを指定します。[PKCS#12パスワード]に暗証鍵を入力します。

3. 認証コードを入力します。

[サーバデコード方式]

認証コード	サーバデコード方式を使用するための認証コードを入力します。 認証コードについてはご購入先の販売店または弊社ホームページよりお問い合わせください。

4. [登録]ボタンをクリックします。

確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

認証コードが登録され、[サーバデコード方式]の設定内容が表示されます。

6. HTTPSリクエストをディレクトリ単位で規制するための設定を行います。

[サーバデコード方式]

HTTPS デコード		サーバデコード方式で規制を有効にする場合に、チェックボックスをオンにします。 HTTPS通信で使用する暗号を一時的に解読して、フィルタリングおよびアクセス履歴を保存します。 チェックボックスをオンにすると、[設定単位]と[警告画面設定]が設定可能になります。
設定単位	システム一括	すべてのグループ/ユーザでHTTPSデコード機能を有効にします。
	グループ毎	[グループ/ユーザ管理]-[グループ管理]-[ネットワーク設定]で、個別にHTTPSデコード機能の有効/無効を選択できます。
警告画面設定		HTTPSデコード処理実行前に、警告画面を表示させる場合に、チェックボックスをオンにします。
		[警告画面の再表示間隔]のプルダウンメニューから、警告画面が表示される間隔(1時間、3時間、6時間、12時間、24時間)を設定します。
対象ホスト設定		HTTPSデコードの対象とするホストを設定する場合に使用します。[HTTPSデコード対象ホスト設定]で設定したホストを対象とする場合は、[対象ホストをHTTPSデコード対象にする]ラジオボタンを選択します。 設定したホストを対象外にする場合は、[対象ホスト以外をHTTPSデコード対象にする]ラジオボタンを選択します。 [対象ホスト一覧へ]をクリックすると、[HTTPSデコード対象ホスト]が表示されます。
除外カテゴリ設定		HTTPSデコードの対象外とするカテゴリを設定する場合に使用します。 [除外カテゴリ設定へ]をクリックすると、[HTTPSデコード除外カテゴリ設定]が表示されます。
POST ログ出力設定		HTTPSデコード時にPOSTログを出力するカテゴリ/サブカテゴリを設定する場合に使用します。 [POSTログ出力設定へ]をクリックすると、[HTTPSデコードPOSTログ出力設定]が表示されます。 POSTログ出力設定がオフの場合は、[ログ管理]-[ログ設定]のリンクが表示されます。

パス部ログ出力設定	HTTPSデコード時にアクセスログに出力されるURLからパス部を除いた状態で出力するカテゴリ/サブカテゴリを設定する場合に使用します。 [パス部ログ出力設定へ]をクリックすると、[HTTPSデコードパス部ログ出力設定]が表示されます。

注意: [警告画面設定]をチェックした場合の警告画面は「2-3. 警告画面」(379ページ)を参照してください。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

8. [OK]ボタンをクリックします。

以上で、サーバデコード方式で規制する場合の設定は完了です。
対象ホストの設定を行う場合は、「HTTPS デコード対象ホストを設定する場合」(190 ページ)を参照してください。
HTTPS デコード対象外のカテゴリを設定する場合は、「HTTPS デコード除外カテゴリを設定する場合」(192 ページ)を参照してください。
POST ログ出力の設定を行う場合は、「HTTPS デコード POST ログ出力を設定する場合」(192 ページ)を参照してください。
パス部のログ出力を行う場合は、「HTTPS デコードパス部のログ出力を設定する場合」(193 ページ)を参照してください。

■ HTTPS デコード対象ホストを設定する場合

[サーバデコード方式]有効時にデコードを行うホストを設定したい場合は、対象ホストに登録してください。
HTTPSデコード対象ホストを設定する場合は、[対象ホスト設定]-[対象ホスト一覧へ]をクリックします。
[HTTPデコード対象ホスト設定]が表示されます。

[HTTPS デコード対象ホスト設定]画面ではHTTPS デコードの対象/ 対象外とするホストリストを登録できます。
ホストリストに対してHTTPS デコードの対象とするか、逆にHTTPS デコードの対象外とするかは[対象ホスト設定]で設定を行ってください。
ここでは、HTTPS デコードの対象外とするホストの設定を行う場合として説明します。

- 一括処理

  ホストリストを一括してインポートまたはエクスポートできます。
  エクスポートする場合は以下の手順で行います。

  (1) [HTTPS デコード対象をエクスポートする] ラジオボタンを選択します。

  (2) [ファイル文字コード] プルダウンメニューから、ファイルエンコードを選択します。

  ファイルエンコードは [UTF-8]、[Shift_JIS]、[EUC_JP] から選択できます。

  (3) [実行] ボタンをクリックします。

  インポートする場合は以下の手順で行います。

  (1) [HTTPS デコード対象をインポートする] ラジオボタンを選択します。

  (2) [ファイル文字コード] プルダウンメニューから、ファイルエンコードを選択します。

  ファイルエンコードは [UTF-8]、[Shift_JIS]、[EUC_JP] から選択できます。

  (3) [ファイル名] の [参照] ボタンをクリックして、インポートするファイルを選択します。

  (4) [実行] ボタンをクリックします。

注意: インポートする場合、既存のリストは破棄されます。

- HTTPS デコード対象ホスト設定

  HTTPSデコードの対象外とするホストを設定する場合は、[IPアドレス/ホスト名]フィールドに、ホスト名または、IPアドレスを入力します。ワイルドカード(*)を入力可能です。
  [登録]ボタンをクリックすると、[HTTPSデコード対象ホスト一覧]に登録されます。
  [キャンセル]ボタンをクリックすると、入力されたIPアドレス/ホスト名は無効になります。

- HTTPS デコード対象ホスト一覧

  すでに設定された対象ホストの一覧が表示されます。[IPアドレス/ホスト名]のタイトル行をクリックすると、IPアドレス/ホスト名順に並び変わります。[登録]のタイトル行をクリックすると、登録した順に並び替わります。
  すでに設定された対象ホストを変更する場合は、対象となるホストの[選択]ボタンをクリックします。[HTTPSデコード対象ホスト設定]-[IPアドレス/ホスト名]フィールドに設定内容が表示されるので、変更した後に[更新]ボタンをクリックします。
  登録されているホストのチェックボックスをオンにして、[削除]ボタンをクリックすると、対象となるホストが一覧から削除されます。
  [前画面へ戻る]ボタンをクリックすると[HTTPS規制設定]に戻ります。

■ HTTPS デコード除外カテゴリを設定する場合

[サーバデコード方式]有効時にデコードから除外するカテゴリを設定したい場合は、除外カテゴリに登録してください。
HTTPSデコード除外カテゴリを設定する場合は、[除外カテゴリ設定]-[除外カテゴリ設定へ]をクリックします。
[HTTPデコード除外カテゴリ設定]が表示されます。

HTTPSデコード時に除外するカテゴリ/サブカテゴリを設定する場合は、除外したいカテゴリ/サブカテゴリのチェックボックスをオンにします。
[保存]ボタンをクリックすると、設定内容が保存されます。
[前画面へ戻る]ボタンをクリックすると[HTTPS規制設定]に戻ります。

■ HTTPS デコード POST ログ出力を設定する場合

[サーバデコード方式]有効時にPOSTログを出力するカテゴリ/サブカテゴリを設定したい場合は、POSTログを出力したいカテゴリ/サブカテゴリを選択してください。
HTTPSデコードPOSTログ出力を設定する場合は、[POSTログ出力設定]-[POSTログ出力設定へ]をクリックします。
[HTTPSデコードPOSTログ出力設定]が表示されます。
HTTPSデコード時にPOSTログを出力するカテゴリ/サブカテゴリを設定する場合は、POSTログを出力したいカテゴリ/サブカテゴリのチェックボックスをオンにします。
[保存]ボタンをクリックすると、設定内容が保存されます。
[前画面へ戻る]ボタンをクリックすると[HTTPS規制設定]に戻ります。

■ HTTPS デコードパス部のログ出力を設定する場合

[サーバデコード方式]有効時に、デコードしたURLからパス部分を、カテゴリ/サブカテゴリごとに、アクセスログに出力しないように設定できます。初期状態ではすべてのカテゴリ/サブカテゴリで、デコードしたURLすべてがアクセスログに出力されます。
HTTPSデコードパス部ログ出力を設定する場合は、[パス部ログ出力設定]-[パス部ログ出力設定へ]をクリックします。
[HTTPSデコードパス部ログ出力設定]が表示されます。HTTPSデコード時にパス部を出力しないカテゴリ/サブカテゴリのチェックボックスをオフにします。
[保存]ボタンをクリックすると、設定内容が保存されます。
[前画面へ戻る]ボタンをクリックすると[HTTPS規制設定]に戻ります。

■ ICAP 版での HTTPS 規制の設定

ICAPクライアントでHTTPS通信をデコードすることで、HTTPSリクエストをディレクトリ単位で規制します。
ICAP クライアントの設定方法については、「ICAPクライアントの設定」(14ページ)を参照してください。
ICAP版でのHTTPS規制の設定では、規制画面を表示する際に用いられる認証局の設定が行えます。
認証局証明書の設定は以下の手順で行います。

1. [共通アクセス管理]-[HTTPS規制設定]をクリックします。

   [HTTPS規制設定]が表示されます。

2. 認証局を設定します。

   認証局証明書をダウンロードする場合は、[認証局証明書のダウンロード]のリンクをクリックし、ダウンロード先を指定して保存します。
   認証局を設定、または変更する場合は、[認証局変更]の[参照]ボタンをクリックし、認証局証明書のファイルを指定します。[PKCS#12パスワード]に暗証鍵を入力します。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

以上で、ICAP版での認証局の設定は完了です。

POSTログ出力の設定を行う場合は、「HTTPSデコードPOSTログ出力を設定する場合」(192ページ)を参照してください。

パス部のログ出力を行う場合は、「HTTPSデコードパス部のログ出力を設定する場合」(193ページ)を参照してください。

以上で、HTTPS規制の設定は完了です。

4-2. 高度分類クラウドの設定

データベースでカテゴリ分類できなかった URL に対して、クラウドで分類するための設定です。

1. [共通アクセス管理]-[高度分類クラウド設定]をクリックします。

   [高度分類クラウド設定]が表示されます。

2. 認証コードを入力します。

認証コード	高度分類クラウドを使用するための認証コードを入力します。 認証コードについてはご購入先の販売店または弊社ホームページよりお問い合わせください。

3. [登録] ボタンをクリックします。

   確認のダイアログが表示されます。

4. [OK] ボタンをクリックします。

   認証コードが登録され、[高度分類クラウド] の設定内容が表示されます。

5. 高度分類クラウドを利用するための設定を行います。

高度分類クラウド設定		[有効] チェックボックスをオンにすると、高度分類クラウド設定が有効になり、処理が行われます。
判定動作[*1]	高度分類クラウドで判定した結果を規制の判定に利用する際の動作を設定します。	
	カテゴリ規制	高度分類クラウドで判定されたカテゴリを、ローカルデータベースで判定されたカテゴリ同様に規制対象とします。 高度分類クラウドとの通信が失敗した場合を未分類のままとし、規制内容は未分類の設定に従います。
	カテゴリ規制 (通信失敗時は規制)	高度分類クラウドで判定されたカテゴリについて、ローカルデータベースで判定されたカテゴリ同様に規制対象とします。高度分類クラウドとの通信が失敗した場合は未分類とせず、閲覧を規制します。
	カテゴリ規制無し (ログ出力のみ)	ログへのカテゴリの反映のみ実施し、高度分類クラウドで判定されたカテゴリは規制判定には使用しません。 カテゴリが付与された場合でも、そのカテゴリルールの設定によらず未分類のルールによって規制判定が行われます。 また、高度分類クラウドで付与されたカテゴリをログで確認するためには、ログ出力の「登録カテゴリ」の出力を有効にしてください。
判定対象 URL[*2]	クラウドに送信する URL の削除処理を設定します。	
	オリジナル URL	入力URL をそのまま送信します。
	パラメータ部を削除した URL	入力URL からパラメータ部を削除して送信します。
	パス部以降を削除した URL	入力URL からパラメータ部とパス部を削除します。
判定除外ホスト		除外するホスト名を入力します。 ・ ホスト名は改行区切りで複数指定できます。 ・ ワイルドカードとして「*」が使用できます。「*」は「.」を含む1文字以上の文字列として使用してください。

IP アドレス除外	チェックボックスをオンにすると、接続先URL が IP アドレスの場合、判定から除外することができます。[プライベートIP のみ除外] チェックボックスをオンにすると、プライベートIP アドレスの場合のみ判定から除外されます。
ログ出力設定	チェックボックスをオンにすると、有効になります。 ・[クラウドで付与したカテゴリを区別可能にする] ・[クラウドで判定したURL をシステムログに残す]

*1 本機能で付与されたカテゴリは優先カテゴリの対象とはなりません。また、カテゴリ毎の一時解除が有効な場合は、データベースや例外URL で付与されたカテゴリか、クラウドで付与されたカテゴリかに係わらず、同じカテゴリとして一時解除することができます。

*2 URL の一部削除を行う場合、情報の送信はされなくなりますが、削除することでカテゴリが変わる場合があります。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

注意:
- 高度分類クラウドは、ライセンスキーによる認証を行うため、デフォルトサーバのライセンスの有効期限が切れていると使用できません。ライセンスキーが切れている場合は、[サーバ管理]-[データベース設定] でデフォルトサーバのライセンスキーを設定してください。
- データベース設定で上位プロキシサーバを使用している場合、クラウドへの通信も同じプロキシサーバを使用します。
- 本機能により付与されたカテゴリは、カテゴリ毎のデコード除外の対象にはなりません。

4-3. ブラウザ規制の設定

■ ブラウザ規制を設定する

特定のブラウザを使用したアクセスを規制するか、許可するかを設定します。

1. [共通アクセス管理]-[ブラウザ規制設定]をクリックします。

[ブラウザ規制設定]が表示されます。

2. ブラウザ規制を設定します。

ブラウザ規制設定を使用しない	ブラウザ規制設定を使用するかどうか、登録したブラウザを使用したアクセスの規制/許可を選択します。 詳しくは、「ブラウザを設定する」(197ページ)を参照してください。
登録ブラウザを規制する	
登録ブラウザを許可する	
登録ブラウザ	アクセスを規制または許可するブラウザを登録します。 詳しくは、「ブラウザを設定する」(197ページ)を参照してください。

注意:
- [共通アクセス管理]-[ブラウザ規制設定]の設定は、すべてのグループ/ユーザに適用されます。
  [共通アクセス管理]-[ブラウザ規制設定]の設定が、[個別アクセス管理]-[ブラウザ規制設定]の設定よりも優先されます。
- 「登録ブラウザを許可する」を選択した場合に、登録ブラウザが何も登録されていないときは、すべてのアクセスが規制されます。

■ ブラウザを設定する

指定したブラウザからのアクセスだけを規制したり、許可したりできます。
ブラウザからのアクセスを規制、または許可する動作については、ラジオボタンから選択します。指定するブラウザは、[登録ブラウザ] で登録します。

注意: [共通アクセス管理]-[ブラウザ規制設定]で規制したブラウザを、[個別アクセス管理]-[ブラウザ規制設定]で許可に設定することはできません。
たとえば、[共通アクセス管理]-[ブラウザ規制設定]で登録ブラウザを「MSIE」、「登録ブラウザを許可する」に設定すると、すべてのグループ/ユーザでUser-Agentに「MSIE」を含まないブラウザを使用したアクセスが規制されます。[個別アクセス管理]-[ブラウザ規制設定]では、登録ブラウザを「MSIE 8」のように設定することで、[共通アクセス管理]-[ブラウザ規制設定]よりも規制を強めることができます。

● ブラウザを登録する

1. 「登録ブラウザ」からのアクセスの規制/許可を設定します。

ブラウザ規制設定を使用しない	ブラウザを規制しません。すべてのブラウザからのアクセスを許可します。
登録ブラウザを規制する	登録ブラウザからのアクセスを規制します。

登録ブラウザを許可する	登録ブラウザからのアクセスだけを許可し、他のすべてのブラウザからのアクセスを規制します。

2. User-Agentヘッダが存在しないブラウザも登録ブラウザに含める場合は、[User-Agentヘッダが存在しない場合も登録ブラウザに含める]チェックボックスをオンにします。

3. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

設定した内容が保存されます。

5. [登録ブラウザ]-[ブラウザを追加]をクリックします。

[ブラウザ登録]画面が別ウィンドウで表示されます。

6. ブラウザ情報を入力します。

[User-Agent]には、ブラウザのUser-Agentを入力します。
[サンプル]のプルダウンメニューからブラウザ名を選択すると、[User-Agent]に代表的なブラウザのUser-Agentが自動的に入力されます。
User-Agentの指定は、部分一致が可能です。
部分一致を利用して、次のようにUser-Agentを設定できます。

Web ブラウザ	User-Agent に含まれる文字列
Internet Explorer 7.0	MSIE 7.0
Internet Explorer 8.0	MSIE 8.0
Internet Explorer 9.0	MSIE 9.0
Internet Explorer 10.0	MSIE 10.0
Internet Explorer 11.0	Trident/7.0
Microsoft Edge	Edge/
Firefox	Firefox/
Google Chrome	Chrome/

注意:
- 指定した文字列が User-Agent と部分一致で合致した場合に規制が有効になります。
  大文字、小文字は区別されるため、文字列は正確に指定してください。
- ワイルドカード(*)を入力可能です。
- [User-Agent]を空欄で設定した場合、User-Agent のヘッダの値が空白のみ、または空文字の場合に規制が有効になります。

[コメント]には、User-Agentに対するコメントを入力します。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

入力したブラウザ情報が登録されます。

9. [閉じる]ボタンをクリックします。

[ブラウザ登録]画面が閉じます。

● 登録ブラウザの設定を変更する

1. [登録ブラウザ]から、変更するブラウザ情報をクリックします。

[ブラウザ編集]画面が別ウィンドウで表示されます。

2. ブラウザ情報を変更します。

3. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

ブラウザ情報が変更されます。

5. [閉じる]ボタンをクリックします。

[ブラウザ編集]画面が閉じます。

● ブラウザ情報を削除する

1. [登録ブラウザ]から、削除するブラウザ情報のチェックボックスをオンにします。

タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

2. [削除]ボタンをクリックします。

確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

ブラウザ情報が削除されます。

4-4. 検索キーワード規制の設定

■ 検索キーワード規制を設定する

検索サイトなどで、指定したキーワードを使用した検索を規制するかどうかを設定します。

1. [共通アクセス管理]-[検索キーワード規制設定]をクリックします。

   [検索キーワード規制設定]が表示されます。

2. 検索キーワード規制を設定します。

検索キーワード規制を使用する	検索キーワード規制を使用するかどうかを設定します。 詳しくは、「検索キーワードを設定する」(201ページ)を参照してください。
登録キーワード	規制対象とする検索キーワードを登録します。 詳しくは、「検索キーワードを設定する」(201ページ)を参照してください。

注意: [共通アクセス管理]-[検索キーワード規制設定]の設定は、すべてのグループ/ユーザに適用されます。

■ 検索キーワードを設定する

検索サイトなどで、指定したキーワードを使用した検索を規制するかどうかを設定します。規制対象とする検索キーワードを設定できます。
キーワードを使用した検索を規制するかどうかの動作については、[検索キーワード規制を使用する]チェックボックスで設定します。規制対象とする検索キーワードは、[登録キーワード]で登録します。

注意:
- 規制されたキーワードを管理者が規制解除申請で承認すると、[登録キーワード] に登録したキーワードが削除されます。
  規制解除申請については、「3-3. 規制解除申請を承認、拒否する」(344ページ)を参照してください。
- [共通アクセス管理]-[検索キーワード規制設定]で規制した検索キーワードは、[個別アクセス管理]-[検索キーワード規制設定]にも反映されます。
  たとえば、[共通アクセス管理]-[検索キーワード規制設定]で登録検索キーワードを「オークション」に設定すると、すべてのグループ/ユーザで「オークション」を使用した検索が規制されます。[個別アクセス管理]-[検索キーワード規制設定]では、[共通アクセス管理]-[検索キーワード規制設定]で設定していない検索キーワードを設定することで、[共通アクセス管理]-[検索キーワード規制設定]よりも規制を強めることができます。

● 検索キーワードを登録する

1. 検索キーワード規制を使用するかどうかを設定します。

キーワードを使用した検索を規制する場合は、[検索キーワード規制を使用する]チェックボックスをオンにします。

2. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

3. [OK]ボタンをクリックします。

設定した内容が保存されます。

4. [登録キーワード]-[キーワードを追加]をクリックします。

[キーワード登録]画面が別ウィンドウで表示されます。

5. 検索キーワードを入力します。

検索キーワードを最大20文字で設定します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   入力した検索キーワード情報が登録されます。

● 登録検索キーワードの設定を変更する

1. [登録キーワード]から、変更する検索キーワード情報をクリックします。

   [キーワード編集]画面が別ウィンドウで表示されます。

2. 検索キーワード情報を変更します。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

   検索キーワード情報が変更されます。

● 検索キーワード情報を削除する

1. [登録キーワード]から、削除する検索キーワード情報のチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。

2. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

   検索キーワード情報が削除されます。

4-5. 書き込みキーワード規制の設定

■ 書き込みキーワード規制を設定する

掲示板などで、指定したキーワードを使用した書き込み (POST リクエスト) を規制するかどうかを設定します。

1. [共通アクセス管理]-[書き込みキーワード規制設定]をクリックします。

   [書き込みキーワード規制設定]が表示されます。

2. 書き込みキーワード規制を設定します。

書き込みキーワード規制を使用する	書き込みキーワード規制を使用するかどうかを設定します。 詳しくは、「書き込みキーワードを設定する」(291ページ)を参照してください。
登録キーワード	規制対象とする書き込みキーワードを登録します。 詳しくは、「書き込みキーワードを設定する」(291ページ)を参照してください。

注意: [共通アクセス管理]-[書き込みキーワード規制設定]の設定は、すべてのグループ/ユーザに適用されます。

■ 書き込みキーワードを設定する

掲示板などで、指定したキーワードを使用した書き込み(POSTリクエスト)を規制するかどうかを設定します。規制対象とする書き込みキーワードを設定できます。
キーワードを使用した書き込みを規制するかどうかの動作については、[書き込みキーワード規制を使用する]チェックボックスで設定します。規制対象とする書き込みキーワードは、[登録キーワード]で登録します。

注意:
- 規制されたキーワードを管理者が規制解除申請で承認すると、[登録キーワード] に登録したキーワードが削除されます。
  規制解除申請については、「3-3. 規制解除申請を承認、拒否する」(344 ページ)を参照してください。
- [共通アクセス管理]-[書き込みキーワード規制設定]で規制した書き込みキーワードは、[個別アクセス管理]-[書き込みキーワード規制設定]にも反映されます。
  たとえば、[共通アクセス管理]-[書き込みキーワード規制設定]で登録書き込みキーワードを「オークション」に設定すると、すべてのグループ/ユーザで「オークション」を使用した書き込みが規制されます。[個別アクセス管理]-[書き込みキーワード規制設定]では、[共通アクセス管理]-[書き込みキーワード規制設定]で設定していない書き込みキーワードを設定することで、[共通アクセス管理]-[書き込みキーワード規制設定]よりも規制を強めることができます。

● 書き込みキーワードを登録する

1. 書き込みキーワード規制を使用するかどうかを設定します。
   キーワードを使用した書き込みを規制する場合は、[書き込みキーワード規制を使用する]チェックボックスをオンにします。

2. [保存]ボタンをクリックします。
   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

3. [OK]ボタンをクリックします。
   設定した内容が保存されます。

4. [登録キーワード]-[キーワードを追加]をクリックします。
   [キーワード登録]画面が別ウィンドウで表示されます。

5. 書き込みキーワードを入力します。
   書き込みキーワードを最大20文字で設定します。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

入力した書き込みキーワード情報が登録されます。

● 登録書き込みキーワードの設定を変更する

1. [登録キーワード]から、変更する書き込みキーワード情報をクリックします。

[キーワード編集]画面が別ウィンドウで表示されます。

2. 書き込みキーワード情報を変更します。

3. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

書き込みキーワード情報が変更されます。

● 書き込みキーワード情報を削除する

1. [登録キーワード]から、削除する書き込みキーワード情報のチェックボックスをオンにします。

タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

2. [削除]ボタンをクリックします。

確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

   書き込みキーワード情報が削除されます。

4-6. 規制画面の設定

■ 規制画面形式を設定する

ユーザがリクエストしたURLへの接続に対してISWMが規制を実施したことをユーザへ通知する、規制画面の内容を設定します。

1. [共通アクセス管理]-[規制画面設定]をクリックします。

   [規制画面設定]が表示されます。

2. [規制画面形式]から規制画面の形式をクリックして選択します。

   注意: ここではスタンドアロン版の画面を使用しています。ICAP版では表示される項目が異なります。

3. 選択した形式で表示するファイルやURL、またはメッセージを入力します。

   規制画面の形式については、「規制画面について」(209ページ)を参照してください。

4. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

5. [OK]ボタンをクリックします。

以上で、規制画面形式の設定は完了です。

■ 規制画面表示サービスを設定する

規制画面のアドレスバーに表示されるドメイン名を設定します。

注意: ICAP版の場合は、[ポート]、[プロセス数]を設定してください。

- ポート
  規制画面を表示するコントロールサーバの、ポート番号を指定します。
- プロセス数
  規制画面を表示するコントロールサーバが同時に処理できる、プロセス数を指定します。

1. [共通アクセス管理]-[規制画面設定]をクリックします。

   [規制画面設定]が表示されます。

2. [規制画面表示サービス設定]-[規制画面ドメイン名]にドメイン名を入力し、[保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意:
   - [規制画面ドメイン名] は、ISWM をインストールしたサーバ上で名前解決できる必要があります。また、localhostなど自身を表す名前は使用できません。
   - ICAP版の場合は、[プロセス数]が表示されます。
   - 設定変更を反映するには、プライマリサーバおよびレプリカサーバの拡張 Web サービスを再起動する必要があります。Windows 版の場合は、コントロールパネルから拡張Webサービス(ISWMWebService)をいったん停止し、起動してください。Linux版の場合は、次のコマンドを実行して拡張Webサービスを再起動してください。
     停止:<インストールディレクトリ>/bin/amsweb stop
     起動:<インストールディレクトリ>/bin/amsweb start

3. [OK]ボタンをクリックします。

以上で、規制画面表示サービスの設定は完了です。

■ 規制画面について

クライアント PC から、フィルタリング対象の URL にアクセスした場合、ISWM はクライアント PC に規制画面を表示します。規制画面とは、対象 URL の表示に規制を実施したことを通知する画面です。
規制画面の形式には「ファイル」、「URL」、「メッセージ」の 3 種類があります。

注意:
- 規制解除申請機能を使用する場合、[規制画面形式] で [ファイル] を選択してください。「URL」および「メッセージ」を選択した場合、規制画面に規制解除申請画面へのリンクが表示されません。
  規制解除申請機能については、「2. 規制解除申請の設定」(337 ページ) を参照してください。
- ICAP版の[規制画面形式]で[ファイル]または[メッセージ]を選択する場合、コントロールサーバまたはICAP クライアントの規制画面表示用 Web サーバの「ポート番号」と「同時に処理可能なプロセス数」をそれぞれ、[ポート]と[プロセス数]に設定してください。
- ICAP 版では、ブラウザのプロキシ除外に、ISWM のアドレスが登録されている場合は表示されません。
- 「規制画面ドメイン名」は、ISWM をインストールしたサーバ上で名前解決できる必要があります。また、localhostなど自身を表す名前は使用できません。

● ファイル

任意の HTML ファイルを規制画面に表示します。
デフォルトでは、「nfblock.htm」に設定されています。HTML ファイルは以下のフォルダ / ディレクトリに格納してください。

Windows の場合

<インストールフォルダ>¥conf¥block

Linux の場合

<インストールディレクトリ>/conf/block

注意: ICAP版の場合は、[ポート]と[プロセス数]を設定してください。
- ポート
  規制画面を表示するコントロールサーバの、ポート番号を指定します。
- プロセス数
  規制画面を表示するコントロールサーバが同時に処理できる、プロセス数を指定します。

● URL

ネットワーク上の任意のページを規制画面として使用します。
デフォルトでは「http://iswm.netstar-inc.com/」に設定されています。社内および社外の URL を指定できます。

注意: HTTPS プロトコルの場合、ドメインより下位のフォルダは指定できません。また、指定しても無視されます。

● メッセージ

任意のメッセージと、規制したカテゴリの情報を文字列 (テキストデータ) として表示します。

注意:
- [個別アクセス管理]-[規制画面設定]で規制メッセージを設定した場合は、[個別アクセス管理]-[規制画面設定]で設定した規制メッセージが表示されます。[共通アクセス管理]-[規制画面設定]で設定した規制メッセージは表示されません。
  詳しくは、「5-10. 規制画面の設定」(296ページ) を参照してください。
- ICAP版の場合は、[ポート]と[プロセス数]を設定してください。
  - ポート
    規制画面を表示するコントロールサーバのポート番号を指定します。
  - プロセス数
    規制画面を表示するコントロールサーバが同時に処理できるプロセス数を指定します。

● 規制画面ドメイン名

規制画面のアドレスバーにドメイン名を表示します。
ドメイン名を空欄にすると、IP アドレスが表示されます。

注意: [規制画面ドメイン名]は、ISWMをインストールしたサーバ上で名前解決できる必要があります。また、localhostなど自身を表す名前は使用できません。

4-7. カテゴリ名の設定

ユーザ設定カテゴリは最大で 99 個のサブカテゴリを設定することができ、それぞれ任意に名前を付けることができます。ここでは、サブカテゴリの名前の変更方法について説明します。ユーザ設定カテゴリについては、「5-1. カテゴリルールの設定」(214 ページ)を参照してください。

1. [共通アクセス管理]-[カテゴリ名設定]をクリックします。

   [カテゴリ名設定]が表示されます。

2. [表示設定]の[サブカテゴリ数]に設定したいカテゴリ数を入力し、[保存]をクリックします。

   設定した数のカテゴリ名入力欄が表示されます。

3. [ユーザ設定サブカテゴリ名]でサブカテゴリ名を変更する「ユーザ設定」に新しいサブカテゴリ名を入力します。

4. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

以上で、サブカテゴリ名の設定は完了です。
設定したカテゴリ名はカテゴリルールのユーザ設定カテゴリに、サブカテゴリ名として反映されます。

4-8. 規制オプションの設定

ISWM では、インターネット上の掲示板などへの書き込みを規制 (POST リクエストの規制) できます。
設定したサイズを超える書き込みが規制対象となります。

1. [共通アクセス管理]-[規制オプション設定]をクリックします。

   [規制オプション設定]が表示されます。

2. 規制オプションの内容を設定します。

[書き込み許容サイズ]

システム一括でサイズを設定する	すべてのグループ/ユーザに適用する、書き込み許容サイズを設定する場合に選択します。 書き込み許容サイズ(byte単位)を設定してください。 設定したサイズを超える書き込みが規制対象となります。
ルール毎にサイズを設定する	ルールごとに書き込み許容サイズを設定する場合に選択します。 [個別アクセス管理]-[規制オプション設定]で個別に書き込み許容サイズを設定してください。 設定したサイズを超える書き込みが規制対象となります。 また、複数のカテゴリに個別に書き込み許容サイズが設定された場合、判定する際の優先動作を [カテゴリ順で判定する] 、または [許容サイズの最も大きな値でのみ判定する] のどちらかに設定することができます。 また、[カテゴリ順で判定する]を選んだ場合は、ユーザ設定カテゴリについても[ユーザ設定カテゴリは許容サイズの最も大きな値のみで判定する]を選択することができます。

3. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

以上で、規制オプションの設定は完了です。

4-9. ヘッダ編集の設定

クライアントブラウザからのリクエストヘッダに追加するヘッダを設定できます。

1. [共通アクセス管理]-[ヘッダ編集設定]をクリックします。

[ヘッダ編集設定]が表示されます。

2. ［設定を追加]をクリックします。

新規に項目が追加されて表示されます。

3. 追加するヘッダの設定を行います。

ヘッダ編集	[有効]チェックボックスをオンにすると、対象項目のヘッダ編集機能が有効になります。
対象ドメイン	ヘッダ編集を適用するドメインを指定します。 リクエスト先ホストが設定された値と後方一致する場合に設定が適用されます。 複数のドメインに対して適用させる場合は改行区切りで入力します。
ヘッダ	リクエストヘッダに追加するヘッダを[ヘッダ名]と[ヘッダ値]で指定します。 [項目を追加]をクリックすると、複数のヘッダを追加することができます。

4. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

項目を削除する場合は [削除] チェックボックスをオンにして、保存ボタンをクリックします。

以上で、ヘッダ編集の設定は完了です。

5. 個別アクセスの設定

5-1. カテゴリルールの設定

■ カテゴリルールを設定する

ここでは、カテゴリルールの設定方法について説明します。

1. [個別アクセス管理]-[カテゴリ設定]をクリックします。

[カテゴリ設定]が表示されます。

2. グループ一覧から、カテゴリルールを設定するグループをクリックします。

[所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

[ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

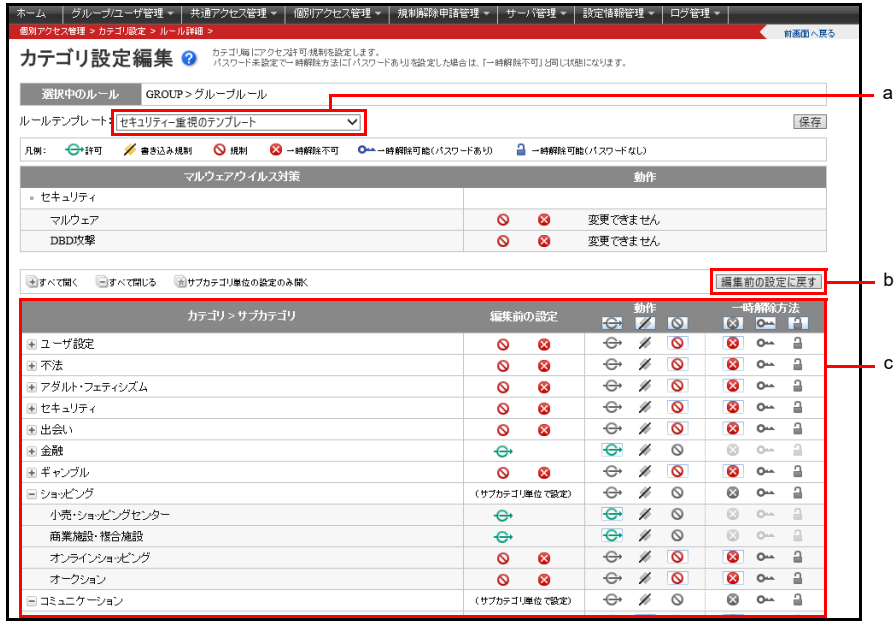
6. [OK]ボタンをクリックします。

   ルールが登録され、[ルール詳細]が表示されます。

7. [カテゴリ設定]タブの[編集]ボタンをクリックします。

   [カテゴリ設定編集]が表示されます。

8. 規制内容を設定します。



a. **ルールテンプレート**	登録するルールのベースとするルールを選択します。
b.**[編集前の設定に戻す] ボタン**	編集前の規制内容に戻します。
c. **規制内容**	カテゴリ別の規制内容を設定します。 設定方法については、「カテゴリごとに規制内容を設定する」(218ページ)を参照してください。

9. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

10. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

● 規制内容について

規制内容には、「動作の規制レベル」と「一時解除方法の規制レベル」があります。

動作の規制レベル	動作		一時解除方法の規制レベル	一時解除方法		説明
ゆるい		許可	なし	なし		自由にアクセスを許可します。
↓		書き込み規制	ゆるい		一時解除可能(パスワードなし)	規制画面を表示しますが、一定時間だけ掲示板などへの書き込みができます。閲覧は可能です。
			↓		一時解除可能(パスワードあり)	掲示板などへの書き込みするためのパスワード(一時解除パスワード)を設定して、書き込みを制限できます。閲覧は可能です。
					一時解除不可	掲示板などへの書き込みを禁止します。閲覧は可能です。
			厳しい			
厳しい		規制	ゆるい		一時解除可能(パスワードなし)	規制画面を表示しますが、一定時間だけ閲覧ができます。
			↓		一時解除可能(パスワードあり)	閲覧するためのパスワード(一時解除パスワード)を設定して、アクセスを制限できます。
					一時解除不可	アクセスを規制して、規制画面を表示します。
			厳しい			

注意:
- 一時解除パスワードおよび閲覧可能な時間(一時解除時間)は、[個別アクセス管理]-[規制オプション設定]で設定します。
  規制オプションについては、「5-11. 規制オプションの設定」(302ページ)を参照してください。
- 一時解除は、[共通アクセス管理]-[規制画面設定]の[規制画面形式]で、ファイルを指定した場合にだけ、有効になります。
- 書き込み規制の対象となる URL は、HTTP プロトコルまたは、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]有効時のHTTPSプロトコルでPOST、PUTメソッドを使用しているURLになります。

● カテゴリごとに規制内容を設定する

カテゴリは、メインカテゴリとサブカテゴリから構成されます。
サブカテゴリごとに規制内容を設定する場合には、カテゴリ名の左にある[+]をクリックします。[-]をクリックすると、サブカテゴリの表示を隠します。
編集前の設定の列には、ルールを読み込んだ時点の設定が表示されます。
タイトル行にある規制内容アイコンをクリックすると、すべてのカテゴリの規制内容を一括して変更できます。

注意:
- サブカテゴリ単位で個別に規制内容を設定した場合、メインカテゴリには規制内容が表示されません。設定した規制内容を確認するには、サブカテゴリを表示して確認してください。
- 上位グループで、カテゴリ設定制限基準ルールが設定されている場合には、カテゴリ設定制限基準ルールの規制内容よりもゆるい規制内容は設定できません。

● ユーザ設定カテゴリの運用方法

ユーザ設定カテゴリに例外URLとして、任意のURLを登録することで、URLデータベースに登録されていないURLに、規制内容を設定できます。
ユーザ設定カテゴリに規制内容を設定すると、ユーザ設定カテゴリに登録したURLに、設定した規制内容が適用されます。サブカテゴリの名称は、[共通アクセス管理]-[カテゴリ名設定]で変更できます。
用途や種類に応じて最大99種類のカテゴリに、任意のURLを登録して規制内容を設定できます。
URLは、例外URLとして登録します。
登録方法については、「5-3. 例外URLの設定」(230ページ)を参照してください。

● 未分類 (その他全て) カテゴリ

カテゴリに分類されていないURLは、「未分類(その他全て)」カテゴリの規制内容が適用されます。

注意:
- 「未分類 (その他全て)」カテゴリでアクセスが規制された場合、規制画面では「未分類」カテゴリと表示されます。
- パラメータにURLを含むリクエストの場合、パラメータのURLにも「未分類(その他全て)」カテゴリの規制内容が適用されます。パラメータにURLを含むリクエストについては、「1-4. パス内URL規制機能」(169ページ)を参照してください。

■ カテゴリルールを変更する

登録したカテゴリルールを変更する方法について説明します。

1. [個別アクセス管理]-[カテゴリ設定]をクリックします。

   [カテゴリ設定]が表示されます。

2. グループ一覧から、カテゴリルールを変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、変更するカテゴリルールをクリックします。

   [ルール詳細]が表示されます。

4. [カテゴリ設定]タブをクリックします。

5. [編集]ボタンをクリックします。

   [カテゴリ設定編集]が表示されます。

6. 規制内容を変更します。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ カテゴリルールのルール情報を変更する

登録したカテゴリルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[カテゴリ設定]をクリックします。
   [カテゴリ設定]が表示されます。
2. グループ一覧から、カテゴリルールのルール情報を変更するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、ルール情報を変更するカテゴリルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [編集]ボタンをクリックします。
   [ルール情報編集]が表示されます。
6. ルール情報を変更します。
7. [保存]ボタンをクリックします。
   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。
   変更した内容が保存され、[ルール詳細]に戻ります。

■ カテゴリルールを複製する

登録したカテゴリルールを複製する方法について説明します。

1. [個別アクセス管理]-[カテゴリ設定]をクリックします。
   [カテゴリ設定]が表示されます。
2. グループ一覧から、カテゴリルールを複製するグループをクリックします。
   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製するカテゴリルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、[ルール詳細]が表示されます。

8. [カテゴリ設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[カテゴリ設定] タブ	「5-1. カテゴリルールの設定」(214ページ)

■ カテゴリルールを削除する

登録したカテゴリルールを削除する方法について説明します。

1. [個別アクセス管理]-[カテゴリ設定]をクリックします。

   [カテゴリ設定]が表示されます。

2. グループ一覧から、カテゴリルールを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、削除するカテゴリルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [削除]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

カテゴリルールが削除され、[カテゴリ設定]に戻ります。選択しているグループ内のカテゴリルールがすべて削除されると、「カテゴリルールが存在しません。」と表示されます。

5-2. スケジュールの設定

[個別アクセス管理]-[カテゴリ設定]で登録したカテゴリルールを適用する曜日、時間帯を設定して、スケジュールを作成します。

■ スケジュールルールを設定する

まず、スケジュールルールを登録します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

[スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールを設定するグループをクリックします。

[所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

[ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されて、ルールが登録されます。

7. [スケジュール設定]タブの[編集]ボタンをクリックして、スケジュールを設定します。

[スケジュール設定編集]が表示されます。

注意: [個別アクセス管理]-[カテゴリ設定]で登録したカテゴリルールを適用する曜日、時間帯を設定して、スケジュールを作成します。
ここでは例として、「土休日」ルールを土日終日、「時間外」ルールを月～金の深夜に適用します。それ以外の時間帯は、上位グループであるルートグループの基本設定に適用された、カテゴリルールが、適用されたままとなります。

8. [時間帯別のカテゴリ設定]-[時間帯を追加]をクリックします。

[時間帯別のカテゴリ設定]に[1]の時間帯設定が追加されます。

9. [時間帯別のカテゴリ設定]の[1]で、時間帯設定を設定します。

適用する曜日、時間帯、ルールを設定します。

曜日	特定の曜日に時間帯設定を適用する場合は、[指定する]チェックボックスをオンにして、設定したい曜日をチェックします。[指定する]チェックボックスをオフにすると、すべての曜日に時間帯設定が適用されます。
時間	時間帯設定を適用する時間を設定します。
カテゴリ設定	時間帯設定として適用するカテゴリルールを所有しているグループとルール名を選択します。 [確認]ボタンをクリックすると、[カテゴリ設定]画面が別ウィンドウで表示されます。選択したカテゴリルールの規制内容を確認できます。

注意:
- 時間帯設定は0:00～24:00 までの範囲で設定できます。24:00 以降の設定は2 つの設定に分けてください。
- 複数の時間帯設定を登録する場合、時間が重なる設定は登録できません。

10. 他の時間帯設定を適用するカテゴリルールを設定する場合には、[時間帯を追加]をクリックします。

[時間帯別のカテゴリ設定]に[2]の時間帯設定が追加されます。

11. [時間帯別のカテゴリ設定]の[2]で、時間帯設定を設定します。

適用する曜日、時間帯、ルールを設定します。

12. さらに他の時間帯設定を作成する場合には、手順10、11 を繰り返します。

13. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

14. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

■ スケジュールの基本設定を変更する

基本設定を変更する方法について説明します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

[スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールの基本設定を変更するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、スケジュールの基本設定を変更するルールをクリックします。

[ルール詳細]が表示されます。

4. [スケジュール設定]タブをクリックします。

5. [編集]ボタンをクリックします。

   [スケジュール設定編集]が表示されます。
   [スケジュール設定編集]では、スケジュールの基本設定の変更と時間帯設定の登録が可能です。
   時間帯設定の登録方法については、「スケジュールの時間帯設定を登録する」(225ページ)を参照してください。

6. [基本のカテゴリ設定]で、スケジュールの基本設定を設定します。

所有グループ	基本設定として適用するカテゴリルールを所有しているグループを選択します。
ルール名	基本設定として適用するカテゴリルールを所有しているグループのルール名を選択します。 [確認]ボタンをクリックすると、[カテゴリ設定]画面が別ウィンドウで表示されます。選択したカテゴリルールの規制内容を確認できます。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   設定した内容が保存され、[ルール詳細]に戻ります。
   引き続き時間帯設定を登録する場合には、「スケジュールの時間帯設定を登録する」(225ページ)の手順4に進みます。

■ スケジュールの時間帯設定を登録する

新しい時間帯設定を登録する方法について説明します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

   [スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールの時間帯設定を登録するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、スケジュールの時間帯設定を登録するルールをクリックします。

   [ルール詳細]が表示されます。

4. [スケジュール設定]タブをクリックします。

5. [編集]ボタンをクリックします。

   [スケジュール設定編集]が表示されます。

6. [時間帯別のカテゴリ設定]-[時間帯を追加]をクリックします。

   [時間帯別のカテゴリ設定]に[1]の時間帯設定が追加されます。

7. [時間帯別のカテゴリ設定]の[1]で、時間帯設定を設定します。

   適用する曜日、時間帯、ルールを設定します。

曜日	特定の曜日に時間帯設定を適用する場合は、[指定する]チェックボックスをオンにして、設定したい曜日をチェックします。[指定する]チェックボックスをオフにすると、すべての曜日に時間帯設定が適用されます。
時間	時間帯設定を適用する時間を設定します。
カテゴリ設定	時間帯設定として適用するカテゴリルールを所有しているグループとルール名を選択します。 [確認]ボタンをクリックすると、[カテゴリ設定]画面が別ウィンドウで表示されます。選択したカテゴリルールの規制内容を確認できます。

注意:
- 時間帯設定は0:00～24:00までの範囲で設定できます。24:00以降の設定は2つの設定に分けてください。
- 複数の時間帯設定を登録する場合、時間が重なる設定は登録できません。

8. 時間帯設定を複数作成する場合には、手順6、7を繰り返します。

9. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

10. [OK]ボタンをクリックします。

    設定した内容が保存され、[ルール詳細]に戻ります。

■ スケジュールの時間帯設定を変更、削除する

時間帯設定を変更、削除する方法について説明します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

   [スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールの時間帯設定を変更、削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、スケジュールの時間帯設定を変更、削除するルールをクリックします。

   [ルール詳細]が表示されます。

4. [スケジュール設定]タブをクリックします。

5. [編集]ボタンをクリックします。

   [スケジュール設定編集]が表示されます。

6. [時間帯別のカテゴリ設定]で、変更する場合は時間帯設定を変更し、削除する場合は[削除]チェックボックスをオンにします。

   複数の時間帯設定を変更し、複数の[削除]チェックボックスをオンにした場合、同時に複数の時間帯設定を変更、削除できます。
   設定項目については、「スケジュールの時間帯設定を登録する」(225ページ)を参照してください。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更または削除した内容が保存され、[ルール詳細]に戻ります。

■ スケジュールルールのルール情報を変更する

登録したスケジュールルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

   [スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールルールのルール情報を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ルール情報を変更するスケジュールルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [編集]ボタンをクリックします。

   [ルール情報編集]が表示されます。

6. ルール情報を変更します。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ スケジュールルールを複製する

登録したスケジュールルールを複製する方法について説明します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

   [スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールルールを複製するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製するスケジュールルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、[ルール詳細]が表示されます。

8. [スケジュール設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[スケジュール設定] タブ	「スケジュールの基本設定を変更する」(224ページ)
	「スケジュールの時間帯設定を登録する」(225ページ)

■ スケジュールルールを削除する

登録したスケジュールルールを削除する方法について説明します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

   [スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールルールを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、削除するスケジュールルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [削除]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

スケジュールルールが削除され、[スケジュール設定]に戻ります。選択しているグループ内のスケジュールルールがすべて削除されると、「スケジュールルールが存在しません。」と表示されます。

5-3. 例外 URL の設定

■ 例外 URL ルールを登録する

例外URLルールを登録します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。

[例外URL設定]が表示されます。

2. グループ一覧から、例外URLを設定するグループをクリックします。

[所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

[ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

   [ルール詳細]が表示されます。

8. [例外URL設定]タブ、[一括処理]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[例外 URL 設定] タブ	「例外URLを設定する」(231ページ)
[一括処理] タブ	「例外URLを一括処理する」(244ページ)

■ 例外 URL を設定する

指定したURLを例外URLとして登録できます。例外URLに登録すると、以下の機能を使用できます。

- URL データベースに登録されていない URL を個別にカテゴリ登録できます。
- URL データベースに登録されているカテゴリとは異なるカテゴリとして、URL を登録できます。
- 「許可カテゴリ」に URL を登録すると、URL データベースで規制対象の URL でも、自由にアクセスできるようになります。
- 「閲覧のみ許可」に URL を登録すると、URL データベースで規制対象の URL でも、閲覧できるようになります。ただし、書き込みはできません。
- 登録する URL に有効期間を設定することができます。有効期間外の URL はフィルタリングの対象となりません。

注意:
- 例外URLはグループごとに設定できます。
- グループと同じ例外URLルールを下位グループに使用させることができます。「フィルタリングルールをグループに一括適用する」(311ページ)を参照してください。

例外URLの設定方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。
   [例外URL設定]が表示されます。
2. グループ一覧から、例外URLを設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、例外URLを設定するルールをクリックします。
   [ルール詳細]が表示されます。
4. [例外URL設定]タブをクリックします。
5. 例外URLを設定します。
   登録されている例外URLの一覧が表示されます。例外URL一覧は、[絞り込み条件]プルダウンメニューにより、「すべて」、「有効期間内」、「有効期間外」を表示することができます。
   また、例外URLの登録、変更、削除ができます。手順については、次の表を参照してください。

例外 URL を登録する	「例外URLを登録する」(232ページ)
例外 URL 一覧の操作	「例外URL一覧の操作方法」(241ページ)
例外 URL を変更する	「例外URLを変更する」(242ページ)
例外 URL を削除する	「例外URLを削除する」(243ページ)

6. [一括処理]タブをクリックします。
7. 例外URLを一括処理します。
   手順については、「例外URLを一括処理する」(244ページ)を参照してください。

■ 例外 URL を登録する

例外URLの登録方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。
   [例外URL設定]が表示されます。

2. グループ一覧から、例外URLを登録するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外URLを登録するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外URL設定]タブをクリックします。

5. [例外URLを追加]をクリックします。

   [例外URL登録]が表示されます。

6. 例外URLを設定します。

   [登録形式]

   [登録形式]プルダウンメニューより、「通常URL」、「IPアドレスレンジ指定URL」、「ワイルドカード指定URL」、「ホスト名/IPアドレス」を選択します。

   [URL]

   [URL]プルダウンメニューより、プロトコルを選択し、例外URLを登録します。
   次の5種類のプロトコルに対応しています。
   入力規則については、「URLの設定」(236ページ)を参照してください。

http://	HTTPを使用するURLを入力します。
https://	HTTPSを使用するURLを入力します。
ftp://	FTP over HTTPを使用するURLを入力します。
utext://	規制する文字列を設定する場合に使用します。 入力した文字列が含まれるURLを規制します。
ufile://	末尾から一致するURLを設定する場合に使用します。

注意:
- ドメイン部に「.」を、パス部に「/」を含んだワイルドカード (*) を使用する場合は、[ワイルドカード「*」の検索対象を拡張する] チェックボックスをオンにしてください。
- 「utext」は下記のようなパス部の文字列「CGI」などを規制することを想定しています。
  www.netstar.jp:443/testfolder/CGI/program.html
- 「ufile」は「?」以降のリクエストパラメータ部を除いてファイル部の末尾から一致になります(「*/abc.cgi?aaa=bbb」の場合は「*/abc.cgi」の末尾から一致)。
- [登録形式]で[ホスト名/IPアドレス]を選択している場合、この項目は表示されません。
- 入力した文字列の先頭および末尾のスペースは自動的に取り除かれます。

[ホスト名 /IP アドレス]

特定のサイト全体を例外として登録する場合、該当するIPアドレス名、またはホスト名を登録します。この指定の場合、ドメイン部のみを対象に後方一致で判定します。プロトコル、ポート番号、およびパスは判定に含まれません。

注意: [登録形式]で[ホスト名/IPアドレス]以外を選択している場合、この項目は表示されません。

[カテゴリ]

「>」の左側のプルダウンメニューを、[メインカテゴリ]プルダウンメニューと呼びます。
「>」の右側のプルダウンメニューを、[サブカテゴリ]プルダウンメニューと呼びます。

- [メインカテゴリ] プルダウンメニュー
  指定する URL へのアクセスを許可する場合は、[許可カテゴリ]を選択します。
  指定する URL へのアクセスを規制する場合は、[規制カテゴリ]を選択します。
  カテゴリごとにアクセスを規制する場合は、規制する URL のカテゴリを選択します。
- [サブカテゴリ] プルダウンメニュー
  [メインカテゴリ] プルダウンメニューで選択したカテゴリ内容から、サブカテゴリを選択します。
  「許可カテゴリ」のサブカテゴリには、[許可カテゴリ]と[閲覧のみ許可]があります。
  [閲覧のみ許可]に登録された URL は、URL データベースで「規制」に登録されていても閲覧できるようになります。ただし、書き込みはできません。
  「規制カテゴリ」のサブカテゴリには、「規制カテゴリ優先」と「許可カテゴリ優先」があります。「規制カテゴリ優先」を選択すると、規制カテゴリに登録された URL を優先して規制します。[許可カテゴリ優先]を選択すると、許可カテゴリに登録された URL を優先してアクセスを許可します。

注意: ユーザ設定カテゴリのサブカテゴリの名称は、[共通アクセス管理]-[カテゴリ名設定]で変更できます。

[有効期間]

例外URLの有効期間を設定します。
有効期間を設定しない場合は、[有効期間を設定しない]ラジオボタンをオンにしてください。
有効期間を設定する場合は、[有効期間を設定する]ラジオボタンをオンにし、開始日、終了日をYYYYMMDDで指定してください(YYYY:西暦、MM:月、DD:日)。
開始日、終了日の右側にある  をクリックして表示されるカレンダーから、開始日、終了日を指定することもできます。

注意:
- 上位グループでカテゴリ設定制限が有効な場合、サブカテゴリの「許可カテゴリ」および「閲覧のみ許可」にURLを登録できません。
- サブカテゴリの「許可カテゴリ」および「閲覧のみ許可」を選択した場合には、URLの入力が必要です。
- サブカテゴリの「許可カテゴリ」および「閲覧のみ許可」を選択した場合には、utext、ufileプロトコルを登録できません。
- サブカテゴリの「閲覧のみ許可」には、HTTP プロトコルと HTTPS プロトコルだけ登録できます。
- URL が空白の場合には、選択したプロトコルを使用するすべての URL が例外URLと認識され、フィルタリングが実行されます。たとえば「http://」を選択してURLが空白の場合、「http://」で始まるすべてのURLが例外URLと認識されます。
- 終了日に過去日付は設定できません。

[コメント]

登録する例外URLについてのコメントを設定します。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意:
- プロトコル部分だけを選択して、URL が空白の場合には、選択されたプロトコルの規制を確認するダイアログが表示されます。
- 入力URLと登録形式、URLが同一の有効期間外のURLがすでにある場合、上書き確認ダイアログが表示されます。
  [OK]ボタンをクリックした場合、URLの有効期間が更新されます。

8. [OK]ボタンをクリックします。

入力したURLが登録され、[ルール詳細]に戻ります。

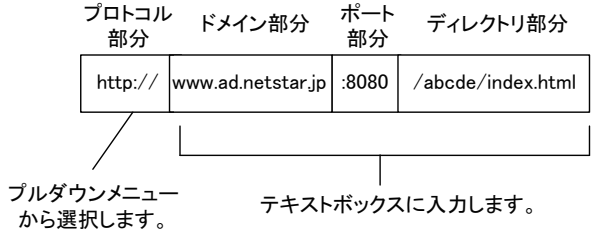
注意:
- 例外URLは例外URLルールごとに設定できます。
- グループと同じ例外URLルールを下位グループに使用させることができます。「フィルタリングルールをグループに一括適用する」(311ページ)を参照してください。

● URL の設定

例外URL登録時におけるURLの設定について説明します。

[通常URLの場合]

- HTTP、HTTPS、FTP プロトコルの場合



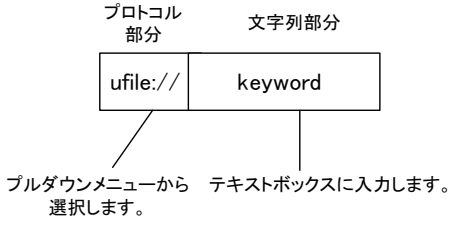
プロトコル部分	プルダウンメニューから選択します。
ドメイン部分	最大半角128文字まで入力できます。 • 大文字で入力した場合、小文字に変換されます。 • 先頭に半角スペース、「.」を入力した場合、削除して登録されます。 • 「/」または「:」で始まっている場合、エラーが発生します。 • 末尾が「.」の場合、エラーが発生します。
ポート部分	ポート番号を1～65535の範囲で指定できます。 • 「:」を複数入力した場合、エラーが発生します。 • 半角数字以外の文字、または範囲外の数値を入力した場合、エラーが発生します。

ディレクトリ部分	最大半角256文字まで入力できます。ディレクトリ部分を入力しないで登録した場合、「/」が追加されます。 HTTPSプロトコルの場合、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]の設定が有効な場合のみ、ディレクトリ部分を登録できます。どちらも無効の場合はディレクトリ部分を入力すると、登録できません。

注意:
- ドメイン部分、ポート部分、ディレクトリ部分を入力しない場合、選択したプロトコルを使用するすべてのURLが例外URLと認識され、フィルタリングが実行されます。
- ドメイン部分、ポート部分、ディレクトリ部分に全角文字を入力した場合、エラーが発生します。

例:
「netstar.jp」と指定した場合、次のURLはすべて規制対象になります。
www.netstar.jp
www2.netstar.jp
netstar.jp/abcd/
www.netstar.jp/abcd/efg/

- UTEXT、UFILE プロトコルの場合



プロトコル部分	プルダウンメニューから選択します。 • utext://(文字列規制) リクエスト URL のパスに、文字列部分に設定した文字列が存在する場合にアクセスを規制します。 • ufile://(ファイル名規制) リクエスト URL のパスの末尾に、文字列部分に設定した文字列が存在する場合にアクセスを規制します。
文字列部分	最大半角256文字まで入力できます。 • 全角文字を入力した場合、エラーが発生します。 • 半角スペース、「"」、「*」を入力した場合、エラーが発生します。

注意: 文字列部分が入力されていない場合には、エラーが発生します。

例 1:

「utext://」プロトコルで文字列部分を「chat」と指定した場合、次のURLには「chat」が含まれているため、すべて規制対象になります。

chat.netstar.jp
www.netstar.jp/chatroom
www.netstar.jp/user/chat1.html

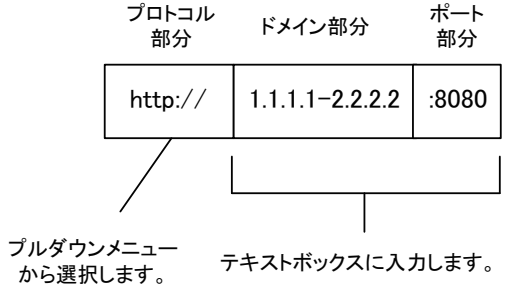
例 2:

「ufile://」プロトコルで文字列部分を「cgi」と指定した場合、次のURLの末尾は「cgi」のため、すべて規制対象になります。

www.netstar.jp/board.cgi
www.netstar.jp/cgi-bin/board.cgi

[IP アドレスレンジ指定 URL の場合]

- HTTP、HTTPS、FTP プロトコルの場合

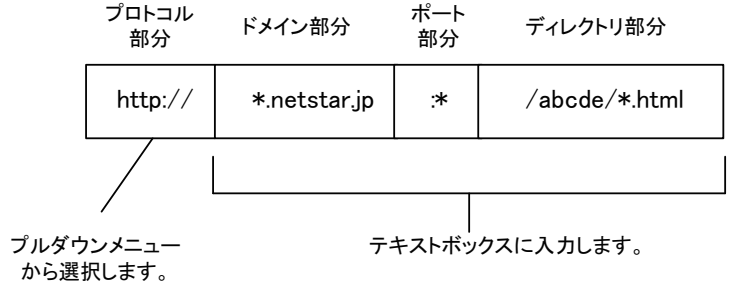


プロトコル部分	プルダウンメニューから選択します。
ドメイン部分	IPアドレスを範囲で指定できます。IPv6アドレスでも指定できます。
ポート部分	ポート番号を空、または1～65535の範囲で指定できます。 半角数字以外の文字、または範囲外の数値を入力した場合、エラーが発生します。 ポート番号を指定した場合は、入力したIPアドレスの範囲すべてに影響します。 ポート番号を指定しない場合は、すべてのポートで有効になります。

注意:
- ドメイン部分をIPv6アドレスで指定する場合、「I-2. 例外URLの設定」(495ページ)を参照してください。
- ドメイン部分、ポート部分に全角文字を入力した場合、エラーが発生します。
- UTEXT、UFILEプロトコルは使用できません。
- 登録形式に「IP アドレスレンジ指定 URL」を指定した場合、ディレクトリ部分を入力できません。

[ワイルドカード使用 URL の場合]

- HTTP、HTTPS、FTP プロトコルの場合



プロトコル部分	プルダウンメニューから選択します。
ドメイン部分	最大半角128文字まで入力できます。 • 大文字で入力した場合、小文字に変換されます。 • 先頭に半角スペース、「.」を入力した場合、削除して登録されます。 • 「/」または「:」で始まっている場合、エラーが発生します。 • 末尾が「.」の場合、エラーが発生します。 • ワイルドカード (*) を入力可能です。
ポート部分	ポート番号を1～65535の範囲で指定できます。 • 「:」を複数入力した場合、エラーが発生します。 • 半角数字以外の文字、または範囲外の数値を入力した場合、エラーが発生します。 • ワイルドカード (*) を入力可能です。

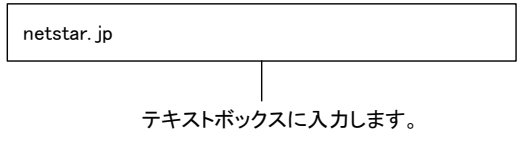
ディレクトリ部分	最大半角256文字まで入力できます。ディレクトリ部分を入力しないで登録した場合、「/」が追加されます。 HTTPSプロトコルの場合、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]の設定が有効な場合のみ、ディレクトリ部分を登録できます。どちらも無効の場合はディレクトリ部分を入力すると、登録できません。 ワイルドカード(*)を入力可能です。

注意:
- ドメイン部分、ポート部分に全角文字を入力した場合、エラーが発生します。
- UTEXT、UFILEプロトコルは使用できません。
- ワイルドカード(*)は1文字以上の文字列として使用できます。
- ワイルドカード(*)は「.」や「/」をまたいで判定することはできません。
- [ワイルドカード「*」の検索対象を拡張する]チェックボックスをオンにした場合は、「.」や「/」をまたいで判定することができます。

● ホスト名 /IP アドレスの設定

例外URL登録時におけるホスト名/IPアドレスの設定について説明します。
ホスト名/IPアドレスで例外URLを指定する場合、ドメイン部のみを対象に後方一致で判定します。プロトコル、ポート番号、およびパスは判定に含まれません。

文字列 (ホスト名/IPアドレス) 部分



文字列部分	最大半角128文字まで入力できます。 • 大文字で入力した場合、小文字に変換されます。 • 先頭に半角スペース、「.」を入力した場合、削除して登録されます。 • 「/」または「:」で始まっている場合、エラーが発生します。 • 末尾に半角スペース、「.」を入力した場合、削除して登録されます。 • 「:」で終わっている場合、エラーが発生します。 • 文字列中に半角スペース、「/」、「:」が入力されている場合、エラーが発生します。

注意:
- ドメインをIPv6アドレスで指定する場合、「例外URLの設定」(184ページ)を参照してください。
- プロトコルやポート番号は使用できません。
- 文字列部分が入力されていない場合には、エラーが発生します。

例

「netstar.jp」と指定した場合、次のURLはすべて規制対象になります。
www.netstar.jp
www2.netstar.jp

● 例外 URL 一覧の操作方法

例外URL一覧の操作方法について説明します。

1. 例外URL一覧に表示する対象を設定します。[絞り込み条件]プルダウンメニューより、「すべて」、「有効期間内」、「有効期間外」を選択できます。

有効期間外の例外URLは[状態]に「×」が表示されます。

2. 1画面に表示する例外URLの表示件数を変更できます。

3. 現在の例外URL一覧を、タイトル行をクリックして並び替えができます。

ソート項目は、[登録]、[カテゴリ]、[URL]、[状態]のタイトル行から選択できます。
選択されたソート項目は、△(昇順)で表示されます。

4. 画面に表示する例外URL一覧のページを変更できます。

	クリックすると、先頭のページが表示されます。
	クリックすると、前のページが表示されます。
	現在表示中のページ番号が表示されます。 表示したいページを直接指定することもできます。
	クリックすると、次のページが表示されます。
	クリックすると、最終のページが表示されます。

5. [削除]ボタンをクリックすると、例外URL一覧から、チェックボックスをオンにしたURLを削除します。

   「例外URLを削除する」(243ページ)を参照してください。

6. 例外URL一覧から、例外URLをクリックすると、例外URLの設定を変更できます。

   次の「例外URLを変更する」(242ページ)を参照してください。

■ 例外 URL を変更する

登録した例外URLの変更方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。

   [例外URL設定]が表示されます。

2. グループ一覧から、例外URLを変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外URLを変更するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外URL設定]タブをクリックします。

5. 例外URL一覧から、変更する例外URLをクリックします。

   [例外URL編集]が表示されます。

6. 例外URLの設定を変更します。

   例外URLの設定項目については、「例外URLを登録する」(232ページ)を参照してください。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ 例外 URL を削除する

登録した例外URLの削除方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。

   [例外URL設定]が表示されます。

2. グループ一覧から、例外URLを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外URLを削除するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外URL設定]タブをクリックします。

5. 例外URL一覧から、削除する例外URLのチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
   タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

6. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

   例外URLが削除されます。

■ 例外 URL を一括処理する

例外URLを一括で処理する方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。
   [例外URL設定]が表示されます。
2. グループ一覧から、例外URLを設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、例外URLを設定するルールをクリックします。
   [ルール詳細]が表示されます。
4. [一括処理]タブをクリックします。
5. 例外URLを一括処理するための設定をします。

例外 URL をエクスポートする	[例外URLをエクスポートする]ラジオボタンをオンにし、[実行]ボタンをクリックすると、登録されている例外URLを指定されたファイルにCSV形式でエクスポート(出力)します。 [ファイル文字コード]プルダウンメニューから、ファイルエンコード(UTF-8、Shift-JIS、EUC_JP)を選択します。
例外 URL をインポートする	[例外URLをインポートする]ラジオボタンをオンにし、[実行]ボタンをクリックすると、指定されたファイルに記述されている例外URLをインポートします。フォーマットについては、「A-7. amsurl[例外URL]」(400ページ)を参照してください。 [ファイル文字コード]プルダウンメニューから、ファイルエンコード(UTF-8、Shift-JIS、EUC_JP)を選択します。 [参照]ボタンをクリックして、インポートするファイルを選択します。 [登録方式]プルダウンメニューから、インポート方法(追加、置換)を選択します。 「追加」を選択すると、指定されたファイルに記述されている例外URLを追加登録します。「置換」を選択すると、対象のグループに登録されている例外URLをすべて削除し、ファイルに記述されている例外URLを一括登録します。

注意: エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

6. [実行]ボタンをクリックします。

注意: インポート、エクスポートとも選択されている例外URLルールのみが一括処理の対象となります。

■ 例外 URL ルールのルール情報を変更する

登録した例外URLルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。
   [例外URL設定]が表示されます。
2. グループ一覧から、例外URLルールのルール情報を変更するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、ルール情報を変更する例外URLルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [編集]ボタンをクリックします。
   [ルール情報編集]が表示されます。
6. ルール情報を変更します。
7. [保存]ボタンをクリックします。
   確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。
   変更した内容が保存され、[ルール詳細]に戻ります。

■ 例外 URL ルールを複製する

登録した例外URLルールを複製する方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。
   [例外URL設定]が表示されます。
2. グループ一覧から、例外URLルールを複製するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、複製する例外URLルールをクリックします。
   [ルール詳細]が表示されます。
4. [このルールを複製]をクリックします。
   [ルール情報複製]が表示されます。
5. ルール情報を変更します。
6. [保存]ボタンをクリックします。
   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。
   ルールが複製され、[ルール詳細]が表示されます。
8. [例外URL設定]タブ、[一括処理]タブをクリックして設定します。
   詳細については、次の表を参照してください。

[例外 URL 設定] タブ	「例外URLを設定する」(231ページ)
[一括処理] タブ	「例外URLを一括処理する」(244ページ)

■ 例外 URL ルールを削除する

登録した例外URLルールを削除する方法について説明します。

1. [個別アクセス管理]-[例外URL設定]をクリックします。
   [例外URL設定]が表示されます。
2. グループ一覧から、例外URLルールを削除するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、削除する例外URLルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [削除]ボタンをクリックします。
   確認のダイアログが表示されます。
6. [OK]ボタンをクリックします。
   例外URLルールが削除され、[例外URL設定]に戻ります。選択しているグループ内の例外URLルールがすべて削除されると、「例外URLルールが存在しません。」と表示されます。

5-4. 例外 URL スケジュールの設定

[個別アクセス管理]-[例外URL設定]で登録した例外URLルールを適用する曜日、時間帯を設定して、スケジュールを作成します。

注意: 上位グループから「例外 URL 参照」が設定されているグループでは、例外 URL スケジュールを設定できません。

■ 例外 URL スケジュールルールを登録する

例外URLスケジュールルールを登録します。

1. [個別アクセス管理]-[例外URLスケジュール設定]をクリックします。
   [例外URLスケジュール設定]が表示されます。

2. グループ一覧から、例外URLスケジュールを設定するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

   [ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

   [ルール詳細]が表示されます。

8. [例外URLスケジュール設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[例外 URL スケジュール設定] タブ	「例外URLスケジュールの基本設定を変更する」(249ページ)
	「例外URLスケジュールの時間帯設定を登録する」(250ページ)

■ 例外 URL スケジュールの基本設定を変更する

基本設定を変更する方法について説明します。

1. [個別アクセス管理]-[例外URLスケジュール設定]をクリックします。

   [例外URLスケジュール設定]が表示されます。

2. グループ一覧から、例外URLスケジュールの基本設定を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外URLスケジュールの基本設定を変更するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外URLスケジュール設定]タブをクリックします。

5. [編集]ボタンをクリックします。

   [例外URLスケジュール設定編集]が表示されます。
   [例外URLスケジュール設定編集]では、例外URLスケジュールの基本設定の変更と時間帯設定の登録が可能です。
   時間帯設定の登録方法については、「例外URLスケジュールの時間帯設定を登録する」(250ページ)を参照してください。

6. [基本の例外URL設定]-[ルール一覧]で、所有グループを選択します。

   基本設定として適用する例外URLルールを所有しているグループを選択します。
   選択したグループが所有する例外URLルールが[ルール一覧]に表示されます。

7. [基本の例外URL設定]-[ルール一覧]で、適用する例外URLルールの[→]ボタンをクリックします。

   [基本の例外URL設定]-[適用ルール]に例外URLルールが追加されます。

注意:
- 例外URLルールは最大10件まで適用できます。
- 適用ルールから外したい場合は、[🗑]ボタンをクリックします。

8. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

9. [OK]ボタンをクリックします。

   設定した内容が保存され、[ルール詳細]に戻ります。
   引き続き時間帯設定を登録する場合には、「例外URLスケジュールの時間帯設定を登録する」(250ページ)の手順6に進みます。

■ 例外 URL スケジュールの時間帯設定を登録する

新しい時間帯設定を登録する方法について説明します。

1. [個別アクセス管理]-[例外URLスケジュール設定]をクリックします。

   [例外URLスケジュール設定]が表示されます。

2. グループ一覧から、例外URLスケジュールの時間帯設定を登録するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外URLスケジュールの時間帯設定を登録するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外URLスケジュール設定]タブをクリックします。

5. [編集]ボタンをクリックします。

   [例外URLスケジュール設定編集]が表示されます。

6. [時間帯別の例外URL設定]-[時間帯を追加]をクリックします。

   [時間帯別の例外URL設定]に[1]の時間帯設定が追加されます。

7. [時間帯別の例外URL設定]の[1]で、時間帯設定を設定します。

適用する曜日、時間帯、ルールを設定します。

曜日	特定の曜日に時間帯設定を適用する場合は、[指定する]チェックボックスをオンにして、設定したい曜日をチェックします。[指定する]チェックボックスをオフにすると、すべての曜日に時間帯設定が適用されます。
時間	時間帯設定を適用する時間を設定します。
ルール設定	[ルール一覧]の[所有グループ]で、時間帯設定として適用する例外URLルールを所有しているグループを選択します。 [ルール一覧]に表示された例外URLルールの[ ]ボタンをクリックすると、[適用ルール]に例外URLルールが追加されます。 [適用ルール]から例外URLルールを除外したい場合は、[ ]ボタンをクリックします。

注意:
- 時間帯設定は0:00～24:00までの範囲で設定できます。24:00以降の設定は2つの設定に分けてください。
- 複数の時間帯設定を登録する場合、時間が重なる設定は登録できません。
- 例外URLルールは最大10件まで適用できます。

8. 時間帯設定を複数作成する場合には、手順6、7を繰り返します。

9. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

10. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

■ 例外 URL スケジュールの時間帯設定を変更、削除する

時間帯設定を変更、削除する方法について説明します。

1. [個別アクセス管理]-[例外URLスケジュール設定]をクリックします。
   [例外URLスケジュール設定]が表示されます。

2. グループ一覧から、例外URLスケジュールの時間帯設定を変更、削除するグループをクリックします。
   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外URLスケジュールの時間帯設定を変更、削除するルールをクリックします。
   [ルール詳細]が表示されます。

4. [例外URLスケジュール設定]タブをクリックします。

5. [編集]ボタンをクリックします。
   [例外URLスケジュール設定編集]が表示されます。

6. [時間帯別の例外URL設定]で、変更する場合は時間帯設定を変更し、削除する場合は[削除]チェックボックスをオンにします。
   複数の時間帯設定を変更し、複数の[削除]チェックボックスをオンにした場合、同時に複数の時間帯設定を変更、削除できます。
   設定項目については、「例外URLスケジュールの時間帯設定を登録する」(250ページ)を参照してください。

7. [保存]ボタンをクリックします。
   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。
   変更または削除した内容が保存され、[ルール詳細]に戻ります。

■ 例外 URL スケジュールルールのルール情報を変更する

登録した例外URLスケジュールルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[例外URLスケジュール設定]をクリックします。

   [例外URLスケジュール設定]が表示されます。

2. グループ一覧から、例外URLスケジュールルールのルール情報を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ルール情報を変更する例外URLスケジュールルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [編集]ボタンをクリックします。

   [ルール情報編集]が表示されます。

6. ルール情報を変更します。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ 例外 URL スケジュールルールを複製する

登録した例外URLスケジュールルールを複製する方法について説明します。

1. [個別アクセス管理]-[例外URLスケジュール設定]をクリックします。

   [例外URLスケジュール設定]が表示されます。

2. グループ一覧から、例外URLスケジュールルールを複製するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製する例外URLスケジュールルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、[ルール詳細]が表示されます。

8. [例外URLスケジュール設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[例外 URL スケジュール設定] タブ	「例外URLスケジュールの基本設定を変更する」(249ページ)
	「例外URLスケジュールの時間帯設定を登録する」(250ページ)

■ 例外 URL スケジュールルールを削除する

登録した例外URLスケジュールルールを削除する方法について説明します。

1. [個別アクセス管理]-[例外URLスケジュール設定]をクリックします。

   [例外URLスケジュール設定]が表示されます。

2. グループ一覧から、例外URLスケジュールルールを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、削除する例外URLスケジュールルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   例外URLスケジュールルールが削除され、[例外URLスケジュール設定]に戻ります。選択しているグループ内の例外URLスケジュールルールがすべて削除されると、「所有ルール一覧]に「1件もありません。」と表示されます。

5-5. 例外サービスの設定

■ 例外サービスルールを登録する

例外サービスルールを登録します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。

   [例外サービス設定]が表示されます。

2. グループ一覧から、例外サービスを設定するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

   [ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

   [ルール詳細]が表示されます。

8. [例外サービス設定]タブをクリックして設定します。

   詳細については、「例外サービスを設定する」(256ページ)を参照してください。

■ 例外サービスを設定する

指定したサービスを例外サービスとして登録できます。例外サービスに登録すると、以下の機能を使用できます。

- サービスを「許可」に設定すると、URL データベースで規制対象の URL でも、自由にアクセスできるようになります。
- サービスを「閲覧のみ許可」に設定すると、URL データベースで規制対象の URL でも、閲覧のアクセスを許可します。
- 登録するサービスに有効期間を設定することができます。有効期間外のサービスは例外の対象となりません。

例外サービスの設定方法について説明します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。

   [例外サービス設定]が表示されます。

2. グループ一覧から、例外サービスを設定するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外URLを設定するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外サービス設定]タブをクリックします。

5. 例外サービスを設定します。

   登録されている例外サービスの一覧が表示されます。
   例外サービスの登録、変更、削除ができます。手順については、次の表を参照してください。

例外サービスを登録する	「例外サービスを登録する」(257ページ)
例外サービス一覧の操作	「例外サービス一覧の操作方法」(259ページ)
例外サービスを変更する	「例外サービスを変更する」(260ページ)
例外サービスを削除する	「例外サービスを削除する」(261ページ)

■ 例外サービスを登録する

例外サービスの登録方法について説明します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。

   [例外サービス設定]が表示されます。

2. グループ一覧から、例外サービスを登録するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外サービスを登録するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外サービス設定]タブをクリックします。

5. [例外サービス設定を追加]をクリックします。

   [例外サービス登録]が表示されます。

6. [サービス一覧]で登録するサービスの[ ]ボタンをクリックします。

   [選択済みサービス]にサービスが追加されます。

注意:
- サービスを検索する場合は、[サービス名]に名前を入力して[検索]ボタンをクリックします。
- [サービスカテゴリ名]プルダウンメニューでカテゴリを選択し、サービスを絞り込むことができます。
- 選択済みサービスから外したい場合は、[ ]ボタンをクリックします。

7. [動作設定]で例外サービスを設定します。

[動作]

例外サービスの動作を以下の中から設定します。
許可:
サービスへのすべてのアクセスを許可します。
閲覧のみ許可:
サービスへの閲覧のアクセスを許可します。

[有効期間]

例外サービスの有効期間を設定します。
有効期間を設定しない場合は、[有効期間を設定しない]ラジオボタンをオンにします。
有効期間を設定する場合は、[有効期間を設定する]ラジオボタンをオンにし、開始日、終了日をYYYYMMDDで指定します(YYYY:西暦、MM:月、DD:日)。
開始日、終了日の右側にある  をクリックして表示されるカレンダーから、開始日、終了日を指定することもできます。

8. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [選択済みサービス]が空欄の場合、エラーが表示されます。

9. [OK]ボタンをクリックします。

入力したサービスが登録され、[ルール詳細]に戻ります。

■ 例外サービス一覧の操作方法

例外サービス一覧の操作方法について説明します。

1. 1画面に表示する例外サービスの表示件数を変更できます。

2. 現在の例外サービス一覧を、タイトル行をクリックして並び替えができます。

   ソート項目は、[登録]、[動作]、[サービス名]、[サービスカテゴリ名]、[登録日]、[コメント]、[状態]のタイトル行から選択できます。
   選択されたソート項目は、△(昇順)で表示されます。

3. 画面に表示する例外サービス一覧のページを変更できます。

	クリックすると、先頭のページが表示されます。
	クリックすると、前のページが表示されます。
	現在表示中のページ番号が表示されます。 表示したいページを直接指定することもできます。
	クリックすると、次のページが表示されます。
	クリックすると、最終のページが表示されます。

4. [削除]ボタンをクリックすると、例外サービス一覧から、チェックボックスをオンにした

サービスを削除します。

「例外サービスを削除する」(261ページ)を参照してください。

5. 例外サービス一覧から、例外サービスをクリックすると、例外サービスの設定を変更できます。

   次の「例外サービスを変更する」(260ページ)を参照してください。

■ 例外サービスを変更する

登録した例外サービスの変更方法について説明します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。

   [例外サービス設定]が表示されます。

2. グループ一覧から、例外サービスを変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外サービスを変更するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外サービス設定]タブをクリックします。

5. 例外サービス一覧から、変更する例外サービスをクリックします。

   [例外サービス編集]が表示されます。

6. 例外サービスの設定を変更します。

   例外サービスの設定項目については、「例外サービスを登録する」(257ページ)を参照してください。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ 例外サービスを削除する

登録した例外サービスの削除方法について説明します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。

   [例外サービス設定]が表示されます。

2. グループ一覧から、例外サービスを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外サービスを削除するルールをクリックします。

   [ルール詳細]が表示されます。

4. [例外サービス設定]タブをクリックします。

5. 例外サービス一覧から、削除する例外サービスのチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
   タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

6. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

   例外サービスが削除されます。

■ 例外サービスルールのルール情報を変更する

登録した例外サービスルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。
   [例外サービス設定]が表示されます。
2. グループ一覧から、例外サービスを変更するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、例外サービスを変更するルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [編集]ボタンをクリックします。
   [ルール情報編集]が表示されます。
6. ルール情報を変更します。
7. [保存]ボタンをクリックします。
   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。
   変更した内容が保存され、[ルール詳細]に戻ります。

■ 例外サービスルールを複製する

登録した例外サービスルールを複製する方法について説明します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。
   [例外サービス設定]が表示されます。
2. グループ一覧から、例外サービスを複製するグループをクリックします。
   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外サービスを複製するルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、複製したルールの[ルール詳細]が表示されます。

■ 例外サービスルールを削除する

登録した例外サービスルールを削除する方法について説明します。

1. [個別アクセス管理]-[例外サービス設定]をクリックします。

   [例外サービス設定]が表示されます。

2. グループ一覧から、例外サービスを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、例外サービスを削除するルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

例外サービスルールが削除され、[例外サービス設定]に戻ります。選択しているグループ内の例外サービスルールがすべて削除されると、「例外サービスルールが存在しません。」と表示されます。

5-6. 優先カテゴリの設定

クライアントPCからリクエストしたURLが複数のカテゴリに該当する場合の優先カテゴリを設定します。

■ 優先カテゴリルールを登録する

優先カテゴリルールを登録します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

[優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリを設定するグループをクリックします。

[所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

[ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

   [ルール詳細]が表示されます。

8. [優先カテゴリ設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[優先カテゴリ設定] タブ	「優先カテゴリを設定する」(265ページ)

■ 優先カテゴリを設定する

優先カテゴリの設定方法について説明します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

   [優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリを設定するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、優先カテゴリを設定するルールをクリックします。

   [ルール詳細]が表示されます。

4. [優先カテゴリ設定]タブをクリックします。

5. 優先カテゴリを設定します。

登録されている優先カテゴリの一覧が表示されます。
また、優先カテゴリの登録、変更、削除ができます。手順については、次の表を参照してください。

優先カテゴリを登録する	「優先カテゴリを登録する」(266ページ)
優先カテゴリを変更する	「優先カテゴリを変更する」(267ページ)
優先カテゴリを削除する	「優先カテゴリを削除する」(268ページ)

■ 優先カテゴリを登録する

優先カテゴリの登録方法について説明します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

[優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリを登録するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、優先カテゴリを登録するルールをクリックします。

[ルール詳細]が表示されます。

4. [優先カテゴリ設定]タブをクリックします。

5. [優先カテゴリ設定を追加]をクリックします。

[優先カテゴリ設定登録]が表示されます。

6. 優先カテゴリを設定します。

[カテゴリ 1]

「>」の左側のプルダウンメニューを、[メインカテゴリ]プルダウンメニューと呼びます。
「>」の右側のプルダウンメニューを、[サブカテゴリ]プルダウンメニューと呼びます。

- [メインカテゴリ] プルダウンメニュー
  優先するメインカテゴリカテゴリを選択します。
- [サブカテゴリ] プルダウンメニュー
  [メインカテゴリ] プルダウンメニューで選択したカテゴリ内容から、サブカテゴリを選択します。

[カテゴリ 2]

以下すべてのカテゴリを選択する	[以下すべてのカテゴリを選択する]ラジオボタンをオンにすると、表示されているすべてのカテゴリを選択します。
カテゴリを 1 つ選択する	[カテゴリを1つ選択する]ラジオボタンをオンにすると、1つのカテゴリを選択します。 「>」の左側のプルダウンメニューを、[メインカテゴリ]プルダウンメニューと呼びます。 「>」の右側のプルダウンメニューを、[サブカテゴリ]プルダウンメニューと呼びます。 • [メインカテゴリ] プルダウンメニュー 優先するメインカテゴリカテゴリを選択します。 • [サブカテゴリ] プルダウンメニュー [メインカテゴリ] プルダウンメニューで選択したカテゴリ内容から、サブカテゴリを選択します。

[動作]

規制内容を設定します。

[動作]プルダウンメニューより、「許可」、「書き込み規制」、「規制」を選択します。

[動作]プルダウンメニューで「書き込み規制」、「規制」を選択した場合、[一時解除方法]プルダウンメニューより、「不可」、「可能(パスワードあり)」、「可能(パスワードなし)」を選択します。

規制内容については、「規制内容について」(217ページ)を参照してください。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

8. [OK]ボタンをクリックします。

入力した優先カテゴリが登録され、[ルール詳細]に戻ります。

■優先カテゴリを変更する

登録した優先カテゴリの変更方法について説明します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

[優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリを変更するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、優先カテゴリを変更するルールをクリックします。

   [ルール詳細]が表示されます。

4. [優先カテゴリ設定]タブをクリックします。

5. 優先カテゴリ一覧から、変更する優先カテゴリをクリックします。

   [優先カテゴリ設定編集]が表示されます。

6. 優先カテゴリの設定を変更します。

   優先カテゴリの設定項目については、「優先カテゴリを登録する」(266ページ)を参照してください。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ 優先カテゴリを削除する

登録した優先カテゴリの削除方法について説明します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

   [優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、優先カテゴリを削除するルールをクリックします。

   [ルール詳細]が表示されます。

4. [優先カテゴリ設定]タブをクリックします。

5. 優先カテゴリ一覧から、削除する優先カテゴリのチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
   タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

6. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

   優先カテゴリが削除されます。

■ 優先カテゴリルールのルール情報を変更する

登録した優先カテゴリルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

   [優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリルールのルール情報を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ルール情報を変更する優先カテゴリルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [編集]ボタンをクリックします。

   [ルール情報編集]が表示されます。

6. ルール情報を変更します。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ 優先カテゴリルールを複製する

登録した優先カテゴリルールを複製する方法について説明します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

   [優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリルールを複製するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製する優先カテゴリルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、[ルール詳細]が表示されます。

8. [優先カテゴリ設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[優先カテゴリ設定] タブ	「優先カテゴリを設定する」(265ページ)

■ 優先カテゴリルールを削除する

登録した優先カテゴリルールを削除する方法について説明します。

1. [個別アクセス管理]-[優先カテゴリ設定]をクリックします。

   [優先カテゴリ設定]が表示されます。

2. グループ一覧から、優先カテゴリルールを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、削除する優先カテゴリルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   優先カテゴリルールが削除され、[優先カテゴリ設定]に戻ります。選択しているグループ内の優先カテゴリルールがすべて削除されると、「優先カテゴリルールが存在しません。」と表示されます。

5-7. ブラウザ規制の設定

■ ブラウザ規制ルールを登録する

ブラウザ規制ルールを登録します。

1. [個別アクセス管理]-[ブラウザ規制設定]をクリックします。

   [ブラウザ規制設定]が表示されます。

2. グループ一覧から、ブラウザ規制を設定するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

   [ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

[ルール詳細]が表示されます。

8. [ブラウザ規制設定]タブをクリックして設定します。

詳細については、次の表を参照してください。

[ブラウザ規制設定] タブ	「ブラウザ規制を設定する」(273ページ)

■ ブラウザ規制を設定する

特定のブラウザを使用したアクセスを規制するか、許可するかを設定します。

1. [個別アクセス管理]-[ブラウザ規制設定]をクリックします。

   [ブラウザ規制設定]が表示されます。

2. グループ一覧から、ブラウザ規制を設定するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ブラウザ規制を設定するルールをクリックします。

   [ルール詳細]が表示されます。

4. [ブラウザ規制設定]タブをクリックします。

5. ブラウザ規制を設定します。

共通アクセス設定を確認	[共通アクセス設定を確認]をクリックすると、[共通アクセス管理ブラウザ規制設定]画面が別ウィンドウで表示されます。 [共通アクセス管理]-[ブラウザ規制設定]の設定内容を確認できます。 [共通アクセス管理]-[ブラウザ規制設定]の設定が、[個別アクセス管理]-[ブラウザ規制設定]の設定よりも優先されます。
[編集] ボタン	[編集]ボタンをクリックして表示される[ブラウザ規制設定編集]で、登録したブラウザを使用したアクセスの規制/許可を選択します。 詳しくは、「ブラウザを設定する」(274ページ)を参照してください。
登録ブラウザ	アクセスを規制または許可するブラウザを登録します。 詳しくは、「ブラウザを設定する」(274ページ)参照してください。

■ ブラウザを設定する

指定したブラウザからのアクセスだけを規制したり、許可したりできます。
ブラウザからのアクセスを規制、または許可する動作については、[編集]ボタンをクリックして表示される[ブラウザ規制設定編集]で設定します。指定するブラウザは、[登録ブラウザ]で登録します。

注意:

- 共通ルールで規制したブラウザを、個別ルールで許可に設定することはできません。
- 共通ルールで登録ブラウザを「MSIE」、「登録ブラウザを許可する」に設定すると、すべてのグループ/ユーザでUser-Agentに「MSIE」を含まないブラウザを使用したアクセスが規制されます。この状態で個別ルールに登録ブラウザを「MSIE 8」のように設定することで、共通ルールよりも規制を強めることができます。
- 「登録ブラウザを許可する」を選択した場合に、登録ブラウザが何も登録されていないときは、すべてのアクセスが規制されます。
- 共通ルールでブラウザ規制を設定した場合、[ログ管理]-[ログ設定]でログの出力単位が「第一階層グループ毎」に設定されていても、常に共通ルールのログとしてブラウザ規制のログを出力します。そのため、システム管理者以外では閲覧できません。共通ルールで規制にしたブラウザ規制のログを参照する場合、次の手順を実行してください。

  管理画面を使用する場合

  (1) システム管理者で管理画面にログインします。
  (2) [ログ管理]-[アクセスログ]をクリックします。
  [アクセスログ]が表示されます。
  (3) [出力単位]で「システム一括」を選択して、[選択]ボタンをクリックします。

  コマンドラインインタフェースを使用する場合

  -acオプションを指定して、amslogコマンドを実行してください。
  詳細については、「A-15. amslog[ログファイルのアーカイブ]」(421ページ)を参照してください。

● ブラウザを登録する

1. [編集]ボタンをクリックします。

[ブラウザ規制設定編集]が表示されます。

2. 「登録ブラウザ」からのアクセスの規制/許可を設定します。

登録ブラウザを規制する	登録ブラウザからのアクセスを規制します。
登録ブラウザを許可する	登録ブラウザからのアクセスだけを許可し、他のすべてのブラウザからのアクセスを規制します。

3. User-Agentヘッダが存在しないブラウザも登録ブラウザに含める場合は、[User-Agentヘッダが存在しない場合も登録ブラウザに含める]チェックボックスをオンにします。

4. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

5. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

6. [登録ブラウザ]-[ブラウザを追加]をクリックします。

[ブラウザ登録]画面が別ウィンドウで表示されます。

7. ブラウザ情報を入力します。

[User-Agent]には、ブラウザのUser-Agentを入力します。
[サンプル]のプルダウンメニューからブラウザ名を選択すると、[User-Agent]に代表的なブラウザのUser-Agentが自動的に入力されます。
User-Agentの指定は、部分一致が可能です。
部分一致を利用して、次のようにUser-Agentを設定できます。

Web ブラウザ	User-Agent に含まれる文字列
Internet Explorer 7.0	MSIE 7.0
Internet Explorer 8.0	MSIE 8.0
Internet Explorer 9.0	MSIE 9.0
Internet Explorer 10.0	MSIE 10.0
Internet Explorer 11.0	Trident/7.0
Microsoft Edge	Edge/
Firefox	Firefox/
Google Chrome	Chrome/

注意:
- 指定した文字列が User-Agent と部分一致で合致した場合に規制が有効になります。
  大文字、小文字は区別されるため、文字列は正確に指定してください。
- ワイルドカード(*)を入力可能です。
- [User-Agent]を空欄で設定した場合、User-Agent のヘッダの値が空白のみ、または空文字の場合に規制が有効になります。

[コメント]には、User-Agentに対するコメントを入力します。

8. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

9. [OK]ボタンをクリックします。

入力したブラウザ情報が登録されます。

● 登録ブラウザの設定を変更する

1. [登録ブラウザ]から、変更するブラウザ情報をクリックします。

   [ブラウザ編集]画面が別ウィンドウで表示されます。

2. ブラウザ情報を変更します。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

   ブラウザ情報が変更されます。

● ブラウザ情報を削除する

1. [登録ブラウザ]から、削除するブラウザ情報のチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
   タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

2. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

   ブラウザ情報が削除されます。

■ ブラウザ規制ルールのルール情報を変更する

登録したブラウザ規制ルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[ブラウザ規制設定]をクリックします。

   [ブラウザ規制設定]が表示されます。

2. グループ一覧から、ブラウザ規制ルールのルール情報を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ルール情報を変更するブラウザ規制ルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [編集]ボタンをクリックします。

   [ルール情報編集]が表示されます。

6. ルール情報を変更します。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ ブラウザ規制ルールを複製する

登録したブラウザ規制ルールを複製する方法について説明します。

1. [個別アクセス管理]-[ブラウザ規制設定]をクリックします。

   [ブラウザ規制設定]が表示されます。

2. グループ一覧から、ブラウザ規制ルールを複製するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製するブラウザ規制ルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、[ルール詳細]が表示されます。

8. [ブラウザ規制設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[ブラウザ規制設定] タブ	「ブラウザ規制を設定する」(273ページ)

■ ブラウザ規制ルールを削除する

登録したブラウザ規制ルールを削除する方法について説明します。

1. [個別アクセス管理]-[ブラウザ規制設定]をクリックします。
   [ブラウザ規制設定]が表示されます。
2. グループ一覧から、ブラウザ規制ルールを削除するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、削除するブラウザ規制ルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [削除]ボタンをクリックします。
   確認のダイアログが表示されます。
6. [OK]ボタンをクリックします。
   ブラウザ規制ルールが削除され、[ブラウザ規制設定]に戻ります。選択しているグループ内のブラウザ規制ルールがすべて削除されると、「ブラウザ規制ルールが存在しません。」と表示されます。

5-8. 検索キーワード規制の設定

■ 検索キーワード規制ルールを登録する

検索キーワード規制ルールを登録します。

1. [個別アクセス管理]-[検索キーワード規制設定]をクリックします。
   [検索キーワード規制設定]が表示されます。
2. グループ一覧から、検索キーワード規制を設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. [所有ルール一覧]-[ルールを追加]をクリックします。
   [ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

[ルール詳細]が表示されます。

8. [検索キーワード規制設定]タブをクリックして設定します。

詳細については、次の表を参照してください。

[検索キーワード規制設定] タブ	「検索キーワードを設定する」(283ページ)

■ 検索キーワード規制を設定する

規制対象とする検索キーワードを設定します。

1. [個別アクセス管理]-[検索キーワード規制設定]をクリックします。
   [検索キーワード規制設定]が表示されます。
2. グループ一覧から、検索キーワード規制を設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、検索キーワード規制を設定するルールをクリックします。
   [ルール詳細]が表示されます。
4. [検索キーワード規制設定]タブをクリックします。
5. 検索キーワード規制を設定します。

共通アクセス設定を確認	[共通アクセス設定を確認]をクリックすると、[共通アクセス管理検索キーワード規制設定]画面が別ウィンドウで表示されます。 [共通アクセス管理]-[検索キーワード規制設定]の設定内容を確認できます。 [共通アクセス管理]-[検索キーワード規制設定]の設定と合わせて規制されます。
登録キーワード	規制対象とする検索キーワードを登録します。 詳しくは、「検索キーワードを設定する」(283ページ)参照してください。

■ 検索キーワードを設定する

規制対象とする検索キーワードを設定できます。
規制対象とする検索キーワードは、[登録キーワード]で登録します。

注意:

- 規制されたキーワードを管理者が規制解除申請で承認すると、[登録キーワード] に登録したキーワードが削除されます。
  規制解除申請については、「3-3. 規制解除申請を承認、拒否する」(344ページ)を参照してください。
- 共通ルールで規制した検索キーワードは、個別ルールで許可に設定することはできません。
  たとえば、共通ルールで登録検索キーワードを「オークション」に設定すると、すべてのグループ/ユーザで「オークション」を使用した検索が規制されます。個別ルールでは、共通ルールで設定していない検索キーワードを設定することで、共通ルールよりも規制を強めることができます。
- 共通ルールで検索キーワード規制を設定した場合、[ログ管理]-[ログ設定] でログの出力単位が「第一階層グループ毎」に設定されていても、常に共通ルールのログとして検索キーワード規制のログを出力します。そのため、システム管理者以外では閲覧できません。
  共通ルールで規制にした検索キーワード規制のログを参照する場合、次の手順を実行してください。

  管理画面を使用する場合

  (1) システム管理者で管理画面にログインします。
  (2) [ログ管理]-[アクセスログ]をクリックします。
  [アクセスログ]が表示されます。
  (3) [出力単位]で「システム一括」を選択して、[選択]ボタンをクリックします。

  コマンドラインインタフェースを使用する場合

  -acオプションを指定して、amslogコマンドを実行してください。
  詳細については、「A-15. amslog[ログファイルのアーカイブ]」(421ページ)を参照してください。

● 検索キーワードを登録する

1. [登録キーワード]-[キーワードを追加]をクリックします。

   [キーワード登録]画面が別ウィンドウで表示されます。

2. 検索キーワードを入力します。

   検索キーワードを最大20文字で設定します。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

   入力した検索キーワード情報が登録されます。

● 登録検索キーワードの設定を変更する

1. [登録キーワード]から、変更する検索キーワード情報をクリックします。

   [キーワード編集]画面が別ウィンドウで表示されます。

2. 検索キーワード情報を変更します。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

   検索キーワード情報が変更されます。

● 検索キーワード情報を削除する

1. [登録キーワード]から、削除する検索キーワード情報のチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。

2. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

   検索キーワード情報が削除されます。

■ 検索キーワード規制ルールのルール情報を変更する

登録した検索キーワード規制ルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[検索キーワード規制設定]をクリックします。

   [検索キーワード規制設定]が表示されます。

2. グループ一覧から、検索キーワード規制ルールのルール情報を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ルール情報を変更する検索キーワード規制ルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [編集]ボタンをクリックします。

   [ルール情報編集]が表示されます。

6. ルール情報を変更します。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

変更した内容が保存され、[ルール詳細]に戻ります。

■ 検索キーワード規制ルールを複製する

登録した検索キーワード規制ルールを複製する方法について説明します。

1. [個別アクセス管理]-[検索キーワード規制設定]をクリックします。

   [検索キーワード規制設定]が表示されます。

2. グループ一覧から、検索キーワード規制ルールを複製するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製する検索キーワード規制ルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、[ルール詳細]が表示されます。

8. [検索キーワード規制設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[検索キーワード規制設定]タブ	「検索キーワード規制を設定する」(282ページ)

■ 検索キーワード規制ルールを削除する

登録した検索キーワード規制ルールを削除する方法について説明します。

1. [個別アクセス管理]-[検索キーワード規制設定]をクリックします。
   [検索キーワード規制設定]が表示されます。
2. グループ一覧から、検索キーワード規制ルールを削除するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、削除する検索キーワード規制ルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [削除]ボタンをクリックします。
   確認のダイアログが表示されます。
6. [OK]ボタンをクリックします。
   検索キーワード規制ルールが削除され、[検索キーワード規制設定]に戻ります。選択しているグループ内の検索キーワード規制ルールがすべて削除されると、「検索キーワード規制ルールが存在しません。」と表示されます。

5-9. 書き込みキーワード規制の設定

■ 書き込みキーワード規制ルールを登録する

書き込みキーワード規制ルールを登録します。

1. [個別アクセス管理]-[書き込みキーワード規制設定]をクリックします。
   [書き込みキーワード規制設定]が表示されます。
2. グループ一覧から、書き込みキーワード規制を設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. [所有ルール一覧]-[ルールを追加]をクリックします。
   [ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

[ルール詳細]が表示されます。

8. [書き込みキーワード規制設定]タブをクリックして設定します。

詳細については、次の表を参照してください。

[書き込みキーワード規制設定] タブ	「書き込みキーワード規制を設定する」(290ページ)

■ 書き込みキーワード規制を設定する

規制対象とする書き込みキーワードを設定します。

1. [個別アクセス管理]-[書き込みキーワード規制設定]をクリックします。
   [書き込みキーワード規制設定]が表示されます。
2. グループ一覧から、書き込みキーワード規制を設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、書き込みキーワード規制を設定するルールをクリックします。
   [ルール詳細]が表示されます。
4. [書き込みキーワード規制設定]タブをクリックします。
5. 書き込みキーワード規制を設定します。

共通アクセス設定を確認	[共通アクセス設定を確認]をクリックすると、[共通アクセス管理書き込みキーワード規制設定]画面が別ウィンドウで表示されます。 [共通アクセス管理]-[書き込みキーワード規制設定]の設定内容を確認できます。 [共通アクセス管理]-[書き込みキーワード規制設定]の設定と合わせて規制されます。
登録キーワード	規制対象とする書き込みキーワードを登録します。 詳しくは、「書き込みキーワードを設定する」(291ページ)を参照してください。

■ 書き込みキーワードを設定する

規制対象とする書き込みキーワードを設定できます。
規制対象とする書き込みキーワードは、[登録キーワード]で登録します。

注意:
- 規制されたキーワードを管理者が規制解除申請で承認すると、[登録キーワード] に登録したキーワードが削除されます。
  規制解除申請については、「3-3. 規制解除申請を承認、拒否する」(344ページ)を参照してください。
- 共通ルールで規制した書き込みキーワードは、個別ルールで許可に設定することはできません。
  たとえば、共通ルールで登録書き込みキーワードを「オークション」に設定すると、すべてのグループ/ユーザで「オークション」を使用した書き込みが規制されます。個別ルールでは、共通ルールで設定していない書き込みキーワードを設定することで、共通ルールよりも規制を強めることができます。
- 共通ルールで書き込みキーワード規制を設定した場合、[ログ管理]-[ログ設定] でログの出力単位が「第一階層グループ毎」に設定されていても、常に共通ルールのログとして書き込みキーワード規制のログを出力します。そのため、システム管理者以外では閲覧できません。
  共通ルールで規制にした書き込みキーワード規制のログを参照する場合、次の手順を実行してください。

  管理画面を使用する場合

  (1) システム管理者で管理画面にログインします。
  (2) [ログ管理]-[アクセスログ]をクリックします。
  [アクセスログ]が表示されます。
  (3) [出力単位]で「システム一括」を選択して、[選択]ボタンをクリックします。

  コマンドラインインタフェースを使用する場合

  -acオプションを指定して、amslogコマンドを実行してください。
  詳細については、「A-15. amslog[ログファイルのアーカイブ]」(421ページ)を参照してください。

● 書き込みキーワードを登録する

1. [登録キーワード]-[キーワードを追加]をクリックします。

   [キーワード登録]画面が別ウィンドウで表示されます。

2. 書き込みキーワードを入力します。

   書き込みキーワードを最大20文字で設定します。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

   入力した書き込みキーワード情報が登録されます。

● 登録書き込みキーワードの設定を変更する

1. [登録キーワード]から、変更する書き込みキーワード情報をクリックします。

   [キーワード編集]画面が別ウィンドウで表示されます。

2. 書き込みキーワード情報を変更します。

3. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

   書き込みキーワード情報が変更されます。

● 書き込みキーワード情報を削除する

1. [登録キーワード]から、削除する書き込みキーワード情報のチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
   タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

2. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

   書き込みキーワード情報が削除されます。

■ 書き込みキーワード規制ルールのルール情報を変更する

登録した書き込みキーワード規制ルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[書き込みキーワード規制設定]をクリックします。

   [書き込みキーワード規制設定]が表示されます。

2. グループ一覧から、書き込みキーワード規制ルールのルール情報を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ルール情報を変更する書き込みキーワード規制ルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [編集]ボタンをクリックします。

   [ルール情報編集]が表示されます。

6. ルール情報を変更します。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

変更した内容が保存され、[ルール詳細]に戻ります。

■ 書き込みキーワード規制ルールを複製する

登録した書き込みキーワード規制ルールを複製する方法について説明します。

1. [個別アクセス管理]-[書き込みキーワード規制設定]をクリックします。

[書き込みキーワード規制設定]が表示されます。

2. グループ一覧から、書き込みキーワード規制ルールを複製するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製する書き込みキーワード規制ルールをクリックします。

[ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

[ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

ルールが複製され、[ルール詳細]が表示されます。

8. [書き込みキーワード規制設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[書き込みキーワード規制設定]タブ	「書き込みキーワード規制を設定する」(290ページ)

■ 書き込みキーワード規制ルールを削除する

登録した書き込みキーワード規制ルールを削除する方法について説明します。

1. [個別アクセス管理]-[書き込みキーワード規制設定]をクリックします。

   [書き込みキーワード規制設定]が表示されます。

2. グループ一覧から、書き込みキーワード規制ルールを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、削除する書き込みキーワード規制ルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   書き込みキーワード規制ルールが削除され、[書き込みキーワード規制設定]に戻ります。選択しているグループ内の書き込みキーワード規制ルールがすべて削除されると、「書き込みキーワード規制ルールが存在しません。」と表示されます。

5-10. 規制画面の設定

■ 規制画面ルールを登録する

規制画面ルールを登録します。

1. [個別アクセス管理]-[規制画面設定]をクリックします。

[規制画面設定]が表示されます。

2. グループ一覧から、規制画面を設定するグループをクリックします。

[所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

[ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

[ルール詳細]が表示されます。

8. [規制画面設定]タブをクリックして設定します。

詳細については、次の表を参照してください。

[規制画面設定] タブ	「規制画面を設定する」(297ページ)

■ 規制画面を設定する

規制画面に表示する画像、規制メッセージを設定します。

注意:
- 規制画面に表示する画像は、[共通アクセス管理]-[規制画面設定] の [規制画面形式] で、[ファイル]が設定されているときに有効になります。
- 規制メッセージは、[共通アクセス管理]-[規制画面設定]の[規制画面形式]で、[ファイル]または[メッセージ]が設定されているときに有効になります。
- [個別アクセス管理]-[規制画面設定]で規制メッセージを設定した場合は、[個別アクセス管理]-[規制画面設定]で設定した規制メッセージが表示されます。[共通アクセス管理]-[規制画面設定]で設定した規制メッセージは表示されません。

1. [個別アクセス管理]-[規制画面設定]をクリックします。

[規制画面設定]が表示されます。

2. グループ一覧から、規制画面を設定するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、規制画面を設定するルールをクリックします。

[ルール詳細]が表示されます。

4. [規制画面設定]タブをクリックします。

5. [編集]ボタンをクリックします。

[規制画面設定編集]が表示されます。

6. 規制画面に表示する画像、規制メッセージを設定します。

画像設定	規制画面に表示する画像を選択します。 新たに画像をアップロードして使用する場合、[新たに画像をアップロードして使用する]ラジオボタンをオンにし、画像ファイルのパスとファイル名を入力します。 [参照]ボタンをクリックすると、[アップロードするファイルの選択]画面が別ウィンドウで表示されます。一覧からファイルを選択して、[開く]ボタンをクリックすると、選択したファイルのパスとファイル名が設定されます。 アップロードできる画像の形式はGIF、サイズは幅250ピクセル×高さ100ピクセルです。
メッセージ設定(カテゴリ共通)	カテゴリ共通の規制メッセージを設定します。 設定しない場合は、デフォルトのメッセージを使用します。 規制メッセージは、全角文字、半角英数字、半角記号を使用して、最大半角128文字まで入力できます。
メッセージ設定(カテゴリ共通リクエスト種別ごと)	閲覧リクエスト時規制と書き込みリクエスト時規制で、異なるカテゴリ共通メッセージを設定できます。 設定しない場合は、カテゴリ共通メッセージを使用します。 規制メッセージは、全角文字、半角英数字、半角記号を使用して、最大半角128文字まで入力できます。
メッセージ設定(カテゴリ単位)	カテゴリ別の規制メッセージを設定します。 [サブカテゴリ単位で設定]チェックボックスをオンにすると、サブカテゴリ別の規制メッセージを設定できます。 規制メッセージは、全角文字、半角英数字、半角記号を使用して、最大半角128文字まで入力できます。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

■ 規制画面ルールを変更する

登録した規制メッセージを変更する方法について説明します。

1. [個別アクセス管理]-[規制画面設定]をクリックします。

   [規制画面設定]が表示されます。

2. グループ一覧から、規制画面を変更するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、規制画面を変更するルールをクリックします。

   [ルール詳細]が表示されます。

4. [規制画面設定]タブをクリックします。

5. [編集]ボタンをクリックします。

   [規制画面設定編集]が表示されます。

6. 規制画面の設定を変更します。

7. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

   変更した内容が保存され、[ルール詳細]に戻ります。

■ 規制画面ルールのルール情報を変更する

登録した規制画面ルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[規制画面設定]をクリックします。
   [規制画面設定]が表示されます。
2. グループ一覧から、規制画面ルールのルール情報を変更するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、ルール情報を変更する規制画面ルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [編集]ボタンをクリックします。
   [ルール情報編集]が表示されます。
6. ルール情報を変更します。
7. [保存]ボタンをクリックします。
   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。
   変更した内容が保存され、[ルール詳細]に戻ります。

■ 規制画面ルールを複製する

登録した規制画面ルールを複製する方法について説明します。

1. [個別アクセス管理]-[規制画面設定]をクリックします。
   [規制画面設定]が表示されます。
2. グループ一覧から、規制画面ルールを複製するグループをクリックします。
   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製する規制画面ルールをクリックします。

   [ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

   [ルール情報複製]が表示されます。

5. ルール情報を変更します。

6. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

   ルールが複製され、[ルール詳細]が表示されます。

8. [規制画面設定]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[規制画面設定] タブ	「規制画面を設定する」(297ページ)

■ 規制画面ルールを削除する

登録した規制画面ルールを削除する方法について説明します。

1. [個別アクセス管理]-[規制画面設定]をクリックします。
   [規制画面設定]が表示されます。
2. グループ一覧から、規制画面ルールを削除するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、削除する規制画面ルールをクリックします。
   [ルール詳細]が表示されます。
4. [ルール情報]タブをクリックします。
5. [削除]ボタンをクリックします。
   確認のダイアログが表示されます。
6. [OK]ボタンをクリックします。
   規制画面ルールが削除され、[規制画面設定]に戻ります。選択しているグループ内の規制画面ルールがすべて削除されると、「規制画面ルールが存在しません。」と表示されます。

5-11. 規制オプションの設定

■ 規制オプションルールを登録する

規制オプションルールを登録します。

1. [個別アクセス管理]-[規制オプション設定]をクリックします。
   [規制オプション設定]が表示されます。
2. グループ一覧から、規制オプションを設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. [所有ルール一覧]-[ルールを追加]をクリックします。
   [ルール情報登録]が表示されます。

4. ルール名を入力します。

所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名 (必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   「保存が完了しました。」と表示されて、ルールが登録されます。

7. 登録したルールをクリックします。

   [ルール詳細]が表示されます。

8. [規制/一時解除設定]タブ、[書き込み許容サイズ]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[規制 / 一時解除設定] タブ	「規制/一時解除を設定する」(304ページ)
[書き込み許容サイズ] タブ	「書き込み許容サイズを設定する」(306ページ)

■ 規制 / 一時解除を設定する

規制/一時解除の設定方法について説明します。

注意: 一時解除は、[共通アクセス管理]-[規制画面設定]の[規制画面形式]で、ファイルを指定しているときにだけ、有効になります。

1. [個別アクセス管理]-[規制オプション設定]をクリックします。
   [規制オプション設定]が表示されます。
2. グループ一覧から、規制オプションを設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、規制オプションを設定するルールをクリックします。
   [ルール詳細]が表示されます。
4. [規制/一時解除設定]タブをクリックします。
5. [編集]ボタンをクリックします。
   [規制/一時解除設定編集]が表示されます。
6. 規制/一時解除を設定します。

[動作設定]

IP アドレス規制	規制する動作のチェックボックスをオンにします。 • [IP アドレスのリクエストを規制する]: IP アドレスを使用した URL(http://192.168.1.1/ など) を規制します。 一時解除方法については、[一時解除方法] プルダウンメニューより、「不可」、「可能(パスワードあり)」、「可能(パスワードなし)」を選択できます。 • [プライベートアドレス以外を対象とする]: プライベートアドレス以外の IP アドレスを規制します。 • [HTTPS のみ対象とする]: HTTPS 通信の場合のみ、IP アドレスを規制します。

一括書き込み規制	[すべての書き込みリクエストを規制する]チェックボックスをオンにすると、未分類を除くカテゴリに該当したすべての書き込みリクエストを規制します。 一時解除方法については、[一時解除方法]プルダウンメニューより、「不可」、「可能(パスワードあり)」、「可能(パスワードなし)」を選択できます。
一括一時解除	[カテゴリによって規制されたすべてのリクエストを一時的に解除可能とする]チェックボックスをオンにすると、カテゴリ設定によって規制されているすべてのリクエストを一時解除します。 一時解除方法については、[一時解除方法]プルダウンメニューより、「可能(パスワードあり)」、「可能(パスワードなし)」を選択できます。
マルチパートリクエスト規制	[マルチパート形式のリクエストを規制する]チェックボックスをオンにすると、マルチパート形式のPOSTリクエストを規制します。データのアップロードが可能な掲示板や、Webメールサービスでの添付ファイル付きメールの送信など、テキストとバイナリデータを同時に送信する書き込み(POSTリクエスト)を規制できます。

[一時解除設定]

解除時間	一時解除する時間(1秒～86,400秒)を設定します。
パスワード	一時解除に使用するパスワードを最大半角20文字で設定します。

注意:
- パスワードには、半角英数字および次の記号を使用できます。
  ! # $ % & ' ( ) = ` ~ { + } _ - ^ @ [ ] . * / < > |
- パスワード未設定で一時解除方法に「一時解除可能(パスワードあり)」を設定した場合は、「一時解除不可」と同じ状態になります。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

■ 書き込み許容サイズを設定する

書き込み許容サイズの設定方法について説明します。

注意: 書き込み許容サイズは、[共通アクセス管理]-[規制オプション設定]で[ルール毎にサイズを設定する]を選択した場合に設定できます。

1. [個別アクセス管理]-[規制オプション設定]をクリックします。
   [規制オプション設定]が表示されます。
2. グループ一覧から、規制オプションを設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. 所有ルール一覧から、規制オプションを設定するルールをクリックします。
   [ルール詳細]が表示されます。
4. [書き込み許容サイズ]タブをクリックします。
5. [編集]ボタンをクリックします。
   [書き込み許容サイズ設定編集]が表示されます。
6. 書き込み許容サイズを設定します。

全てのカテゴリに同じサイズを設定する	設定した値を書き込み許容サイズとして、全カテゴリに適用する場合に選択します。 書き込み許容サイズ(byte単位)を設定してください。 設定したサイズを超える書き込みが規制対象となります。 「0byte」に設定した場合には、すべての書き込みが規制対象となります。
カテゴリ単位でサイズを設定する	設定した値を書き込み許容サイズとして、カテゴリごとに適用する場合に選択します。 書き込み許容サイズ(byte単位)を設定してください。 [サブカテゴリ単位で設定]チェックボックスをオンにすると、サブカテゴリごとに書き込み許容サイズを設定できます。 設定したサイズを超える書き込みが規制対象となります。 「0byte」に設定した場合には、すべての書き込みが規制対象となります。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

● カテゴリごとの規制内容と規制オプションの組み合わせ

カテゴリルールでは、カテゴリごとに規制内容が設定されています。
カテゴリごとの規制内容と、規制オプションの一括書き込み規制、一括一時解除を組み合わせて設定する場合、規制オプションの一括書き込み規制、一括一時解除→カテゴリごとの規制内容の順番で適用されます。

■ 規制オプションルールのルール情報を変更する

登録した規制オプションルールのルール情報を変更する方法について説明します。

1. [個別アクセス管理]-[規制オプション設定]をクリックします。

[規制オプション設定]が表示されます。

2. グループ一覧から、規制オプションルールのルール情報を変更するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、ルール情報を変更する規制オプションルールをクリックします。

[ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [編集]ボタンをクリックします。

[ルール情報編集]が表示されます。

6. ルール情報を変更します。

7. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

変更した内容が保存され、[ルール詳細]に戻ります。

■ 規制オプションルールを複製する

登録した規制オプションルールを複製する方法について説明します。

1. [個別アクセス管理]-[規制オプション設定]をクリックします。

[規制オプション設定]が表示されます。

2. グループ一覧から、規制オプションルールを複製するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、複製する規制オプションルールをクリックします。

[ルール詳細]が表示されます。

4. [このルールを複製]をクリックします。

[ルール情報複製]が表示されます。

5. [ルール情報を変更します。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

7. [OK]ボタンをクリックします。

ルールが複製され、[ルール詳細]が表示されます。

8. [規制/一時解除設定]タブ、[書き込み許容サイズ]タブをクリックして設定します。

   詳細については、次の表を参照してください。

[規制 / 一時解除設定] タブ	「規制/一時解除を設定する」(304ページ)
[書き込み許容サイズ] タブ	「書き込み許容サイズを設定する」(306ページ)

■ 規制オプションルールを削除する

登録した規制オプションルールを削除する方法について説明します。

1. [個別アクセス管理]-[規制オプション設定]をクリックします。

   [規制オプション設定]が表示されます。

2. グループ一覧から、規制オプションルールを削除するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. 所有ルール一覧から、削除する規制オプションルールをクリックします。

   [ルール詳細]が表示されます。

4. [ルール情報]タブをクリックします。

5. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

   規制オプションルールが削除され、[規制オプション設定]に戻ります。選択しているグループ内の規制オプションルールがすべて削除されると、「規制オプションルールが存在しません。」と表示されます。

6. フィルタリングルールをグループ/ユーザに適用

6-1. フィルタリングルールをグループに適用

ここでは、設定したフィルタリングルールをグループに適用する方法について説明します。

注意: グループにフィルタリングルールを適用するには、あらかじめ[個別アクセス管理]でフィルタリングルールを設定する必要があります。
フィルタリングルールの設定方法については、「5. 個別アクセスの設定」(214ページ)を参照してください。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。
   [グループ管理]が表示されます。
2. グループ一覧から、フィルタリングルールを適用するグループ名をクリックします。
   設定画面にグループの設定内容が表示されます。
3. [ルール設定]タブをクリックします。
   フィルタリングルールを適用します。

以降の操作方法については、次の表を参照してください。

適用するフィルタリングルール	参照先
フィルタリングルール(一括適用)	「フィルタリングルールをグループに一括適用する」(311ページ)
カテゴリルール	「カテゴリルールをグループに適用する」(312ページ)
スケジュールルール	「スケジュールルールをグループに適用する」(313ページ)
例外 URL ルール	「例外URLルールをグループに適用する」(314ページ)
例外 URL スケジュールルール	「例外URLルールをグループに適用する」(314ページ)
例外サービスルール	「例外サービスルールをグループに適用する」(316ページ)
優先カテゴリルール	「優先カテゴリルールをグループに適用する」(317ページ)
ブラウザ規制ルール	「ブラウザ規制ルールをグループに適用する」(318ページ)

適用するフィルタリングルール	参照先
検索キーワード規制ルール	「検索キーワード規制ルールをグループに適用する」(319ページ)
書き込みキーワード規制ルール	「書き込みキーワード規制ルールをグループに適用する」(320ページ)
規制画面ルール	「規制画面ルールをグループに適用する」(321ページ)
規制オプションルール	「規制オプションルールをグループに適用する」(322ページ)

■ フィルタリングルールをグループに一括適用する

フィルタリングルールをグループに一括適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [ルール設定]タブの[編集]ボタンをクリックします。

   [ルール設定編集]が表示されます。

2. 一括設定の適用範囲を指定します。

   フィルタリングルールの一括設定には、次の4種類があります。
   詳細は、「1-5. フィルタリング設定の参照」(170ページ)を参照してください。

   上位グループ参照
   チェックボックスをオンにすると、グループのフィルタリング設定は、「上位グループのフィルタリング設定」を参照します。ただし、上位グループで「カテゴリ設定制限」が有効な場合は設定できません。上位グループ参照を有効にしたグループではユーザのフィルタリング設定だけが可能です。

   下位グループ強制参照
   チェックボックスをオンにすると、自グループのフィルタリング設定を下位グループに対して強制的に参照させます。「下位グループ強制参照を有効にしたグループ」の下位に属するすべてのグループおよびユーザは、フィルタリングの設定ができません。グループに適用されるフィルタリング設定の確認だけが可能です。

   例外 URL 参照
   チェックボックスをオンにすると、下位グループに、例外URLルールを参照させることが可能です。

カテゴリ設定制限

チェックボックスをオンにすると、下位グループのカテゴリ関連ルールに設定制限を設けることができます。この場合、特定のカテゴリルールを、基準となるカテゴリ設定制限基準ルールに設定することができます。カテゴリ設定制限基準ルールを選択して[確認]ボタンをクリックすると、カテゴリ設定の詳細が別ウィンドウで表示されます。

注意:
- カテゴリ設定制限基準ルールを設定すると、下位グループではカテゴリ設定制限基準ルールの規制内容がベースとなり、規制をゆるめることができません。また、例外URLの「許可カテゴリ」も設定できません。
- 選択したグループにカテゴリルールが登録されていない場合は、カテゴリ設定制限基準ルールは設定できません。

3. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

■ カテゴリルールをグループに適用する

カテゴリルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[カテゴリ/スケジュール設定]をクリックします。

[カテゴリ/スケジュール設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

[適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

個別にカテゴリルールを適用する	個別にカテゴリルールを適用する場合に選択します。 選択すると、カテゴリルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したカテゴリルールの詳細が画面の下部に表示されます。 カテゴリの設定内容の詳細については、「5-1. カテゴリルールの設定」(214ページ)を参照してください。
個別にスケジュールルールを適用する	個別にスケジュールルールを適用する場合に選択します。 「スケジュールルールをグループに適用する」(313ページ)

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ スケジュールルールをグループに適用する

スケジュールルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[カテゴリ/スケジュール設定]をクリックします。

   [カテゴリ/スケジュール設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

個別にカテゴリルールを適用する	個別にカテゴリルールを適用する場合に選択します。 「カテゴリルールをグループに適用する」(312ページ)
個別にスケジュールルールを適用する	個別にスケジュールルールを適用する場合に選択します。 選択すると、スケジュールルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したスケジュールルールの詳細が画面の下部に表示されます。 スケジュールの設定内容の詳細については、「5-2. スケジュールの設定」(222ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 例外 URL ルールをグループに適用する

例外URLルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[例外URL設定]をクリックします。

   [例外URL設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

> **注意:** 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. [所有グループ]から、例外URLルールを所有するグループを選択します。

   選択されたグループで所有しているルールが一覧表示されます。

> **注意:** ルールをクリックすると、ルールの設定内容が画面の下部に表示されます。設定内容の詳細については「5-3. 例外URLの設定」(230ページ)を参照してください。

4. [ルール一覧]の中から、適用するルールの  ボタンをクリックして選択します。

   選択されたルールが、画面右側の[適用ルール]に追加表示されます。

   注意:
   - [適用ルール]に表示されるルールで、上位グループから「例外URL参照」が設定されているルールは灰色で表示されます。削除/変更はできません。
   - 適用ルールから外したい場合は、  ボタンをクリックします。
   - 適用可能なルールの数は最大10件です。

5. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

■ 例外 URL スケジュールルールをグループに適用する

例外URLスケジュールルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[例外URL/スケジュール設定]をクリックします。

   [例外URL/スケジュール設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

   注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

個別に例外 URL ルールを適用する	個別に例外URLルールを適用する場合に選択します。 「例外URLルールをグループに適用する」(314ページ)
個別にスケジュールルールを適用する	個別に例外URLスケジュールルールを適用する場合に選択します。 選択すると、例外URLスケジュールルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択した例外URLスケジュールルールの詳細が画面の下部に表示されます。 例外URLスケジュールの設定内容の詳細については、「5-4. 例外URLスケジュールの設定」(247ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 例外サービスルールをグループに適用する

例外サービスルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[例外サービス設定]をクリックします。

   [例外サービス設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

> **注意:** 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. [個別にルールを適用する]ラジオボタンを選択します。

4. [所属グループ]プルダウンメニューでグループを選択します。

5. [ルール名]プルダウンメニューで適用するルールを選択します。

6. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

■ 優先カテゴリルールをグループに適用する

優先カテゴリルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[優先カテゴリ設定]をクリックします。

   [優先カテゴリ設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

   注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

優先カテゴリを設定しない	優先カテゴリを設定しない場合に選択します。選択した場合、優先カテゴリルールは適用されません。
個別にルールを適用する	個別に優先カテゴリルールを適用する場合に選択します。選択すると、優先カテゴリルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択した優先カテゴリルールの詳細が画面の下部に表示されます。優先カテゴリの設定内容の詳細については、「5-6. 優先カテゴリの設定」(264ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ ブラウザ規制ルールをグループに適用する

ブラウザ規制ルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[ブラウザ規制設定]をクリックします。

   [ブラウザ規制設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

> **注意:** 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

ブラウザ規制を使用しない	ブラウザを規制しない場合に選択します。この場合、すべてのブラウザからのアクセスを許可します。
個別にルールを適用する	個別にブラウザ規制ルールを適用する場合に選択します。選択すると、ブラウザ規制ルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したブラウザ規制ルールの詳細が画面の下部に表示されます。ブラウザ規制の設定内容の詳細については「5-7. ブラウザ規制の設定」(271ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 検索キーワード規制ルールをグループに適用する

検索キーワード規制ルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[検索キーワード規制設定]をクリックします。

   [検索キーワード規制設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

検索キーワード規制を使用しない	検索キーワードを規制しない場合に選択します。この場合、検索サイトなどにおいて、任意の用語での検索を許可します。
個別にルールを適用する	個別に検索キーワード規制ルールを適用する場合に選択します。 選択すると、検索キーワード規制ルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択した検索キーワード規制ルールの詳細が画面の下部に表示されます。検索キーワード規制の設定内容の詳細については、「5-8. 検索キーワード規制の設定」(280ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 書き込みキーワード規制ルールをグループに適用する

書き込みキーワード規制ルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[書き込みキーワード規制設定]をクリックします。

   [書き込みキーワード規制設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

> **注意:** 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

書き込みキーワード規制を使用しない	書き込みキーワードを規制しない場合に選択します。
個別にルールを適用する	個別に書き込みキーワード規制ルールを適用する場合に選択します。 選択すると、書き込みキーワード規制ルールを所有しているグループ名とルールを選択することができます。 [確認]ボタンをクリックすると、選択した書き込みキーワード規制ルールの詳細が画面の下部に表示されます。 書き込みキーワード規制の設定内容の詳細については、「5-9. 書き込みキーワード規制の設定」(288ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 規制画面ルールをグループに適用する

規制画面ルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[規制画面設定]をクリックします。

   [規制画面設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

所有グループ **ルール名**	規制画面ルールを所有しているグループ名とルールを選択します。[確認]ボタンをクリックすると、選択した規制画面ルールの詳細が画面の下部に表示されます。 規制画面の設定内容の詳細については、「5-10. 規制画面の設定」(296ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 規制オプションルールをグループに適用する

規制オプションルールをグループに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-1. フィルタリングルールをグループに適用」(310ページ)を参照してください。

1. [適用ルール]-[規制オプション設定]をクリックします。

   [規制オプション設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

   注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

   規制オプションルールを所有しているグループ名とルールを選択することができます。
   [確認]ボタンをクリックすると、選択した規制オプションルールの詳細が画面の下部に表示されます。規制オプションの設定内容の詳細については、「5-11. 規制オプションの設定」(302ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

6-2. フィルタリングルールをユーザに適用

ここでは、設定したフィルタリングルールをユーザに適用する方法について説明します。

注意: ユーザにフィルタリングルールを適用するには、あらかじめ[個別アクセス管理]でフィルタリングルールを設定する必要があります。
フィルタリングルールの設定方法については、「5. 個別アクセスの設定」(214ページ)を参照してください。

1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

   [ユーザ管理]が表示されます。

2. グループ一覧から、フィルタリングルールを適用するユーザが登録されているグループ名をクリックします。

   ユーザ一覧が表示されます。

3. [IPアドレス一覧]タブまたは[アカウント一覧]タブをクリックして、ユーザ一覧の表示を切り替えます。

4. ユーザ一覧から、フィルタリングルールを適用するIPアドレス/アカウントをクリックします。

   [IPアドレス詳細]または[アカウント詳細]が表示されます。

5. [ルール設定]タブをクリックします。

   フィルタリングルールを適用します。

以降の操作方法については、次の表を参照してください。

適用するフィルタリングルール	参照先
カテゴリルール	「カテゴリルールをユーザに適用する」(324ページ)
スケジュールルール	「スケジュールルールをユーザに適用する」(325ページ)
ブラウザ規制ルール	「ブラウザ規制ルールをユーザに適用する」(326ページ)
検索キーワード規制ルール	「検索キーワード規制ルールをユーザに適用する」(327ページ)
書き込みキーワード規制ルール	「書き込みキーワード規制ルールをユーザに適用する」(328ページ)

適用するフィルタリングルール	参照先
規制オプションルール	「規制オプションルールをユーザに適用する」(329ページ)

■ カテゴリルールをユーザに適用する

カテゴリルールをユーザに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

1. [適用ルール]-[カテゴリ/スケジュール設定]をクリックします。

   [カテゴリ/スケジュール設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

   注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

所属グループと同じルールを使用する	所属しているグループと同じルールを適用する場合に選択します。
個別にカテゴリルールを適用する	個別にカテゴリルールを適用する場合に選択します。 選択すると、カテゴリルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したカテゴリルールの詳細が画面の下部に表示されます。 カテゴリの設定内容の詳細については、「5-1. カテゴリルールの設定」(214ページ)を参照してください。
個別にスケジュールルールを適用する	個別にスケジュールルールを適用する場合に選択します。 「スケジュールルールをユーザに適用する」(325ページ)

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ スケジュールルールをユーザに適用する

スケジュールルールをユーザに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

1. [適用ルール]-[カテゴリ/スケジュール設定]をクリックします。

   [カテゴリ/スケジュール設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

所属グループと同じルールを使用する	所属しているグループと同じルールを適用する場合に選択します。
個別にカテゴリルールを適用する	個別にカテゴリルールを適用する場合に選択します。 「カテゴリルールをユーザに適用する」(324ページ)
個別にスケジュールルールを適用する	個別にスケジュールルールを適用する場合に選択します。 選択すると、スケジュールルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したスケジュールルールの詳細が画面の下部に表示されます。 スケジュールの設定内容の詳細については、「5-2. スケジュールの設定」(222ページ)参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ ブラウザ規制ルールをユーザに適用する

ブラウザ規制ルールをユーザに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

1. [適用ルール]-[ブラウザ規制設定]をクリックします。

   [ブラウザ規制設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

所属グループと同じルールを使用する	所属しているグループと同じルールを適用する場合に選択します。 カッコの中には、以下のどちらかが表示されます。 • グループ名 > ルール名 • ブラウザ規制を使用していません
ブラウザ規制を使用しない	ブラウザを規制しない場合に選択します。この場合、すべてのブラウザからのアクセスを許可します。
個別にルールを適用する	個別にブラウザ規制ルールを適用する場合に選択します。選択すると、ブラウザ規制ルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したブラウザ規制ルールの詳細が画面の下部に表示されます。ブラウザ規制の設定内容の詳細については、「5-7. ブラウザ規制の設定」(271ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 検索キーワード規制ルールをユーザに適用する

検索キーワード規制ルールをユーザに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

1. [適用ルール]-[検索キーワード規制設定]をクリックします。

   [検索キーワード規制設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

所属グループと同じルールを使用する	所属しているグループと同じルールを適用する場合に選択します。 カッコの中には、以下のどちらかが表示されます。 • グループ名 > ルール名 • 検索キーワード規制を使用していません
検索キーワード規制を使用しない	検索キーワードを規制しない場合に選択します。この場合、検索サイトなどにおいて、任意の用語での検索を許可します。
個別にルールを適用する	個別に検索キーワード規制ルールを適用する場合に選択します。 選択すると、検索キーワード規制ルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択した検索キーワード規制ルールの詳細が画面の下部に表示されます。検索キーワード規制の設定内容の詳細については、「5-8. 検索キーワード規制の設定」(280ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 書き込みキーワード規制ルールをユーザに適用する

書き込みキーワード規制ルールをユーザに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

1. [適用ルール]-[書き込みキーワード規制設定]をクリックします。

   [書き込みキーワード規制設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

> **注意:** 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

所属グループと同じルールを使用する	所属しているグループと同じルールを適用する場合に選択します。 カッコの中には、以下のどちらかが表示されます。 • グループ名 > ルール名 • 書き込みキーワード規制を使用していません
書き込みキーワード規制を使用しない	書き込みキーワードを規制しない場合に選択します。
個別にルールを適用する	個別に書き込みキーワード規制ルールを適用する場合に選択します。 選択すると、書き込みキーワード規制ルールを所有しているグループ名とルールを選択することができます。 [確認]ボタンをクリックすると、選択した書き込みキーワード規制ルールの詳細が画面の下部に表示されます。 書き込みキーワード規制の設定内容の詳細については、「5-9. 書き込みキーワード規制の設定」(288ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

■ 規制オプションルールをユーザに適用する

規制オプションルールをユーザに適用します。
ここでは、[ルール設定]タブが表示されている前提で説明します。
[ルール設定]タブの表示方法については「6-2. フィルタリングルールをユーザに適用」(323ページ)を参照してください。

1. [適用ルール]-[規制オプション設定]をクリックします。

   [規制オプション設定]が表示されます。

2. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

   注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

3. 適用ルールを選択します。

所属グループと同じルールを使用する	所属しているグループと同じルールを適用する場合に選択します。
個別にルールを適用する	個別に規制オプションルールを適用する場合に選択します。選択すると、規制オプションルールを所有しているグループ名とルールを選択することができます。 [確認]ボタンをクリックすると、選択した規制オプションルールの詳細が画面の下部に表示されます。規制オプションの設定内容の詳細については、「5-11. 規制オプションの設定」(302ページ)を参照してください。

4. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

5. [OK]ボタンをクリックします。

簡易設定

1. [簡易設定]画面でできること

簡易設定は、1台のサーバでISWMのフィルタリングサービスを運用する場合に、運用に必要な最小限の設定、およびフィルタリングルール適用を一括して設定する方法です。

注意: 複数のサーバで負荷分散して運用する場合や、ユーザをグループに分けて個々にフィルタリングルールを適用するといった設定はできません。複数のサーバで負荷を分散してISWMを運用する場合は、[サーバ管理]画面で各種の設定をしてください。

1-1. 簡易設定の設定内容

簡易設定では、グループ/ユーザ別にフィルタリングルールを適用することができません。
簡易設定で設定できる内容は以下のとおりです。

選択できるユーザ認証方式	フィルタリングルール設定	
	選択できる適用方法	スケジュール設定
ユーザ認証なし	全ユーザ一括適用	設定できません

ユーザ認証方式の設定については、「5. ユーザ認証/LDAPの設定」(60ページ)を参照してください。

1-2. フィルタリングルールの適用

簡易設定で選択できるフィルタリングルールは、ルートグループに登録されているフィルタリングルールだけです。
適用するフィルタリングルールを変更したい場合は、グループ/ユーザ別に次のようにフィルタリングルールを変更してください。

グループに適用するフィルタリングルールを変更する場合

[グループ/ユーザ管理]-[グループ管理]の[ルール設定]タブ-[適用ルール]で、グループに適用するフィルタリングルールを変更してください。

ユーザに適用するフィルタリングルールを変更する場合

- ユーザを IP アドレスで管理している場合
  [グループ/ユーザ管理]-[ユーザ管理]の[IPアドレス一覧]タブでユーザをクリックして表示される[IPアドレス詳細]の[ルール設定]タブ-[適用ルール]で、ユーザに適用するフィルタリングルールを変更してください。

- ユーザをアカウントで管理している場合
  [グループ/ユーザ管理]-[ユーザ管理]の[アカウント一覧]タブでユーザをクリックして表示される[アカウント詳細]の[ルール設定]タブ-[適用ルール]で、ユーザに適用するフィルタリングルールを変更してください。

フィルタリングルールの適用については「6. フィルタリングルールをグループ / ユーザに適用」(310ページ)を参照してください。

2. 簡易設定でシステムとフィルタリングルールを設定する

システムの簡易設定は、以下の手順で設定してください。

1. [ホーム]画面で[簡易設定]をクリックします。

   [簡易設定]が表示されます。

2. [ライセンス設定]、[フィルタリングサービス設定]、[データベース設定]で、URLデータベースのダウンロードに必要な情報を入力します。

   [ライセンス設定]では、URLデータベースのダウンロードに必要なライセンスキーなどを設定します。

ライセンスキー	ライセンス証書に記載されたライセンスキーを入力します。
企業・団体名	会社名または団体名を入力します。 (全角32文字、半角64文字以内)
メールアドレス	管理者のメールアドレスを入力します。 ここで入力されたメールアドレスには、ダウンロード用サーバの変更など、データベースについてのご案内をお送りします。

[フィルタリングサービス設定]、[データベース設定]は、必要に応じて設定します。

フィルタリングサービス設定	フィルタリングサービスに使用するポート番号を変更する場合、[設定を変更する]チェックボックスをオンにします。
データベース設定	URLデータベースダウンロード用の上位プロキシサーバ設定です。 インターネットへの接続に上位のプロキシサーバを利用している場合、[データベースダウンロード時に上位プロキシサーバを使用する]チェックボックスをオンにし、上位プロキシサーバの情報を入力します。

注意:
- [フィルタリングサービス設定]の「HTTP」の設定項目は、ICAP版では「ICAP」として表示されます。
- ICAP版の場合、[フィルタリングサービス設定]の「HTTPS」と「FTP over HTTP」の設定項目は表示されません。
- スタンドアロン版で透過プロキシが有効になっている場合、「FTP over HTTP」の設定項目は表示されません。

3. [カテゴリ設定]で、[設定を変更する]チェックボックスをオンにして、ルートグループに適用するカテゴリルールを選択します。

ルートグループに登録されているカテゴリルールから選択します。ルートグループには、システムで「DEFAULT RULE」、「セキュリティー重視」、「小学校」、「中学校」、「高校」、「大学」、「企業・官公庁(基本的な設定)」、「企業・官公庁(業務効率化重視)」のルールが登録されています。
[確認]ボタンをクリックすると、[カテゴリ設定]画面が別ウィンドウで表示されます。
[カテゴリ設定]で選択したカテゴリルールの規制内容を確認できます。

動作の規制レベル	動作		一時解除方法の規制レベル	一時解除方法		説明
ゆるい		許可	なし	なし		自由にアクセスを許可します。
↓		書き込み規制	ゆるい ↓ 厳しい		一時解除可能(パスワードなし)	規制画面を表示しますが、一定時間だけ掲示板などへの書き込みができます。閲覧は可能です。
					一時解除可能(パスワードあり)	掲示板などへの書き込みするためのパスワード(一時解除パスワード)を設定して、書き込みを制限できます。閲覧は可能です。
					一時解除不可	掲示板などへの書き込みを禁止します。閲覧は可能です。
厳しい		規制	ゆるい ↓ 厳しい		一時解除可能(パスワードなし)	規制画面を表示しますが、一定時間だけ閲覧ができます。
					一時解除可能(パスワードあり)	閲覧するためのパスワード(一時解除パスワード)を設定して、アクセスを制限できます。
					一時解除不可	アクセスを規制して、規制画面を表示します。

[カテゴリ設定]画面を閉じるには、[閉じる]ボタンをクリックします。

4. [保存]をクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

5. [OK]ボタンをクリックします。

ライセンス設定、フィルタリングサービス設定、データベース設定と、適用するカテゴリルールを設定し、URLデータベースのダウンロードを開始します。

以上で、簡易設定は完了です。
ダウンロード先 URL の変更や、ダウンロードの詳細を設定する場合、「3. データベースのダウンロード」(53ページ)を参照してください。

注意: フィルタリングサービス設定を変更した場合、フィルタリングサービスの再起動が必要です。
詳細については、「2. サーバの設定と登録」(42ページ)を参照してください。

規制解除申請の設定と管理

1. [規制解除申請管理]画面でできること

規制解除申請の設定と管理ができます。

1-1. 規制解除申請の設定

[規制解除申請管理]-[規制解除申請設定]では、規制対象のURLにアクセスしたときに表示される規制画面から、ユーザが規制解除を申請するための設定を行います。

1-2. 規制解除申請の管理

[規制解除申請管理]-[規制解除申請一覧]では、ユーザから送信された規制解除申請を管理します。
管理者は、ユーザからの規制解除申請を、処理済・未処理別に確認できます。
管理者は、未処理の申請内容を確認して、承認または拒否できます。承認結果は、ユーザに通知メールを送信することもできます。
また、処理済の規制解除申請の一覧を確認して、不要な履歴を削除できます。

注意: 規制解除申請機能を使用するためには、[規制解除申請管理]-[規制解除申請設定]で、規制解除申請機能の[ユーザからの規制解除申請を受け付ける]チェックボックスをオンにしてください。
設定については、「2. 規制解除申請の設定」(337ページ)を参照してください。

---

2. 規制解除申請の設定

規制解除申請機能を使用すると、規制されたURLにアクセスしたとき、ブラウザから規制解除を申請できます。ユーザから送信された規制解除申請は申請履歴として保存され、管理画面で処理が可能です。また、メール通知設定が有効な場合、申請が送信されたときにシステム管理者や設定した通知先にメールを送信したり、規制解除申請の処理結果をメール通知できます。
ここでは、規制解除申請機能の設定について説明します。規制解除申請画面の操作については、「1-1. 規制解除申請の設定」(336ページ)を、規制解除申請の処理については、「3. 規制解除申請の管理」(341ページ)を参照してください。

注意:
- 規制解除申請機能を利用する場合、[共通アクセス管理]-[規制画面設定]で規制画面形式を「ファイル」に設定してください。詳しくは、「規制画面形式を設定する」(207ページ)を参照してください。
- ISWMでのユーザ認証が「有効」に設定されていない場合、規制解除申請機能は利用できません。

1. [規制解除申請管理]-[規制解除申請設定]をクリックします。

   [規制解除申請設定]が表示されます。

2. [規制解除申請機能]の[ユーザからの規制解除申請を受け付ける]チェックボックスをオンにします。

   [申請取得間隔]と[申請通知]の設定が可能になります。

   注意: メールによる規制解除の申請通知をする場合、[申請通知]-[通知先]でメールの送付先を設定してください。また、[サーバ管理]-[メール通知設定]でメール送信に必要な設定をしてください。詳しくは、「6. メール通知設定」(98 ページ)を参照してください。

3. [申請取得間隔]を設定します。

   レプリカサーバの管理サービスから規制解除申請ファイルを回収する間隔を、1～100,000の範囲で秒単位で設定します。初期値は60秒です。

4. [申請通知]を設定します。

申請通知	件名		申請メールの件名を入力します。 初期状態では、「規制解除申請通知」と入力されています。
	通知先	システム管理者	[システム管理者へ通知する] チェックボックスをオンにすると、ADMINグループに所属するユーザ(アカウント)に申請メールを送信します。
		グループ管理者	グループ管理者に対する通知方法を設定します。 • 通知しない グループ管理者には通知しません。 • 第一階層グループの管理者へ通知 規制解除申請を行ったユーザが所属するグループの第一階層グループのグループ管理者にだけ通知します。 • 所属グループの管理者へ通知 規制解除申請を行ったユーザが所属するグループのグループ管理者にだけ通知します。 • 所属グループと全ての上位グループの管理者へ通知 規制解除申請を行ったユーザが所属するグループ、およびその上位の階層に登録されているすべてのグループ管理者に通知します。
		その他の通知先	システム管理者、グループ管理者以外に通知したい場合、通知するメールアドレスを入力します。複数の通知先を設定する場合、メールアドレスを「,」(半角カンマ)で区切ってください。
結果通知	申請の承認 / 拒否結果を申請者へ通知する		チェックボックスをオンにすると、規制解除申請の承認、拒否結果を申請者に対してメール送信できます。また、結果通知の件名も入力できます。 初期状態では、「規制解除申請結果通知」と入力されています。

注意:
- ユーザが申請した規制解除申請の内容は、ログファイルに記録されます。ログファイルの内容は、[ログ管理]-[アクセスログ]で確認できます。詳しくは、「第8章 ログの設定と管理」(357ページ)を参照してください。
  規制解除申請のログファイルは、「ISWM_offer_yyyymmdd_***.log」というファイル名で保存されます。
- IP アドレスのユーザには申請通知メールを送信できません。IP アドレスで登録されているユーザに申請通知メールを送信する場合、[その他の通知先]にメールアドレスを入力してください。また、IP アドレスのユーザからの規制解除申請に対しては、結果通知メールを送信できません。
- メールアドレスが登録されていないアカウントには通知できません。
- LDAP 連携を使用している場合、アカウントが同期されていないユーザからの申請内容には、アカウント名が記録されません。

5. 申請結果を通知する場合は、結果通知の[申請の承認/拒否結果を申請者へ通知する]チェックボックスをオンにします。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

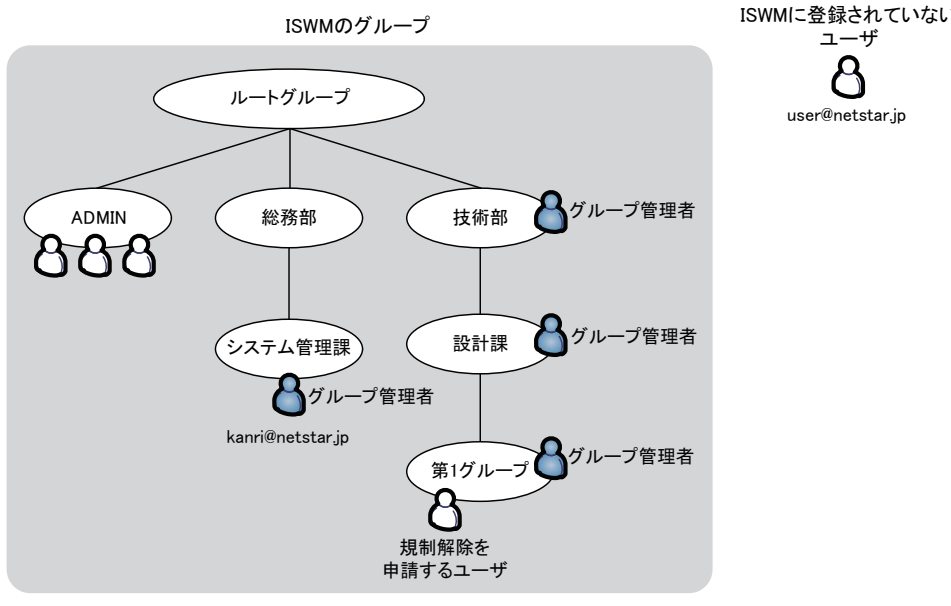
7. [OK]ボタンをクリックします。

以上で、規制解除申請の設定は完了です。

2-1. 申請メール通知先の設定

申請メール通知先の設定と通知先について、次の「申請メール通知先の設定例」の図を例として説明します。ここでは、第 1 グループのユーザが規制解除を申請したときの申請メール通知先について示します。

申請メール通知先の設定例



[システム管理者] の設定

[システム管理者へ通知する] チェックボックスをオンにすると、ADMIN グループのすべてのアカウントにメールで通知します。

[グループ管理者] の設定

[第一階層グループの管理者へ通知] を選択した場合

技術部グループのグループ管理者にだけ、メールで通知します。

[所属グループの管理者へ通知] を選択した場合

第1グループのグループ管理者にだけ、メールで通知します。

[所属グループと全ての上位グループの管理者へ通知] を選択した場合

技術部グループ、設計課グループ、第1グループのグループ管理者にメールで通知します。

[その他の通知先] の設定

システム管理課グループのグループ管理者のメールアドレス「kanri@netstar.jp」、および ISWMに登録されていないメールアドレス「user@netstar.jp」を指定した場合、両方にメールで通知します。

3. 規制解除申請の管理

ユーザが規制されたURLに対する規制解除を申請すると、規制解除申請が申請履歴として保存されます。[規制解除申請管理]-[規制解除申請一覧]では、ユーザから送信された規制解除申請を「未処理」、「処理済」の分類で管理できます。
管理者は未処理の規制解除申請について、管理画面上で承認または拒否できます。このとき、承認結果をユーザにメールで通知することも可能です。また、処理済の規制解除申請について、不要な申請履歴を削除できます。承認した規制解除申請は、次のように処理されます。

URL で規制された場合
「許可カテゴリ」または「閲覧のみ許可」として例外URLに登録できます。

キーワードで規制された場合
対象のキーワードを規制キーワードから削除できます。

3-1. 規制解除申請のメール通知の条件

規制解除申請の結果をメール通知する場合、次の条件をすべて満たす必要があります。

申請者のアカウントにメールアドレスが登録されている

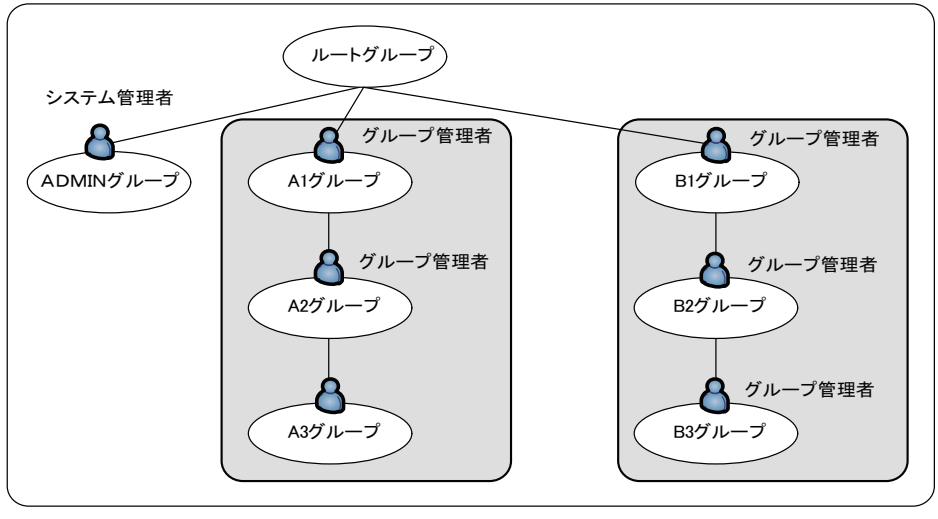
[サーバ管理]-[メール通知設定] の [メール通知設定] で、メール通知機能が有効に設定されている
設定については、「6. メール通知設定」(98ページ)を参照してください。

[規制解除申請管理]-[規制解除申請設定] で、メール通知の結果通知が設定されている
設定については、「2. 規制解除申請の設定」(337ページ)を参照してください。

3-2. 規制解除申請の管理とアカウント種別

システム管理者は、すべての規制解除申請の閲覧および承認、拒否ができます。グループ管理者では、所属グループと下位グループの規制解除申請の閲覧および承認、拒否ができます。

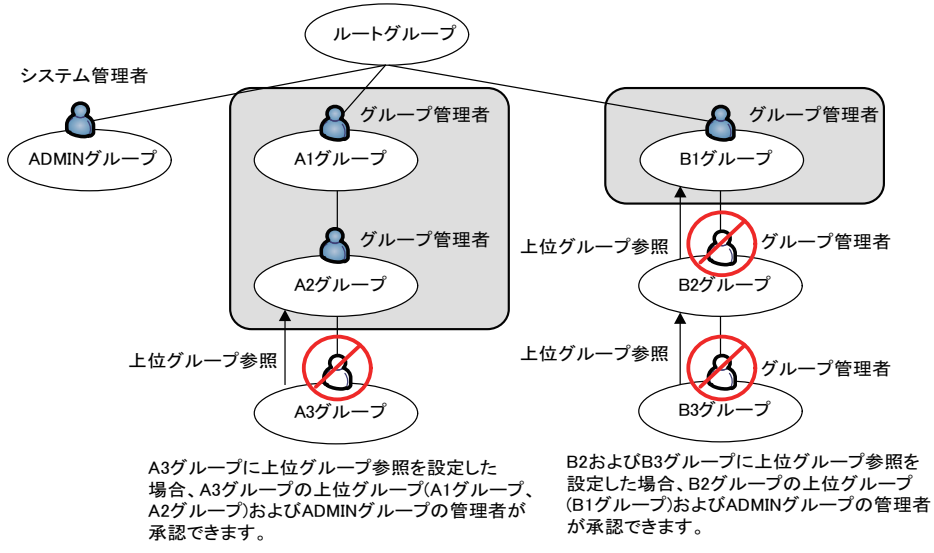
承認範囲



所属グループのフィルタリング設定で「上位グループ参照」を設定した場合

規制解除申請の閲覧と拒否はできますが、承認はできません。
参照している上位グループより上位の管理者だけが承認できます。

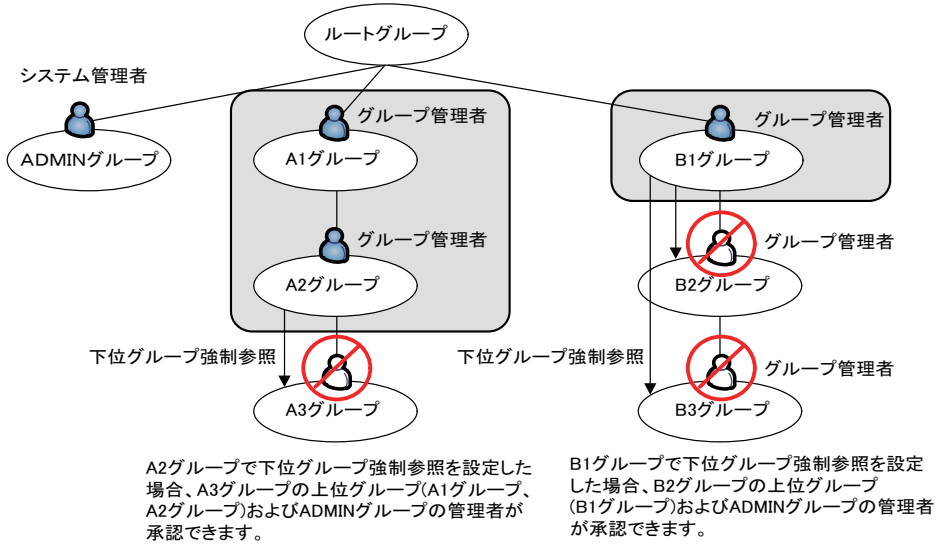
承認範囲



所属グループより上位グループのフィルタリング設定で「下位グループ強制参照」を設定した場合

規制解除申請の閲覧と拒否はできますが、承認はできません。
下位グループ強制参照を設定したグループより上位の管理者だけが承認できます。

承認範囲



3-3. 規制解除申請を承認、拒否する

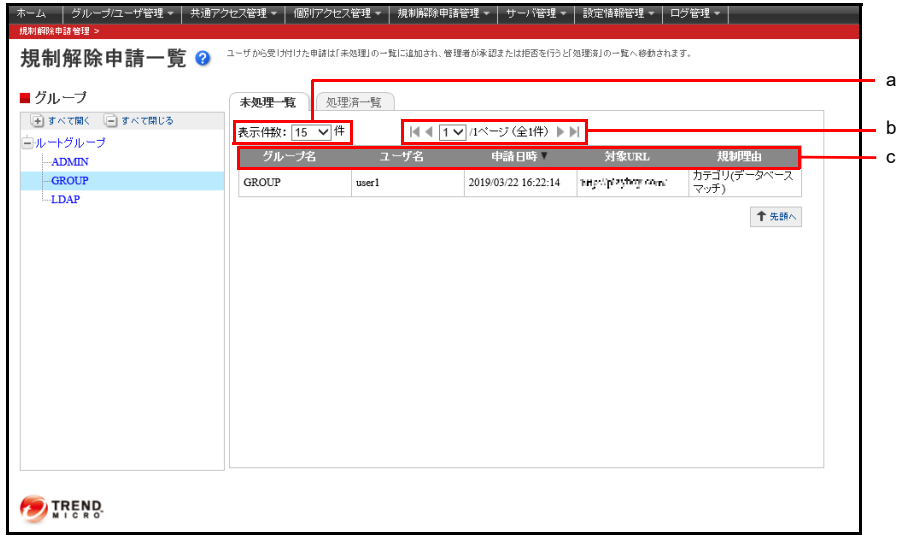
ユーザからの規制解除申請を承認、拒否します。

注意: 規制解除申請一覧に表示されるグループ名 / ユーザ名は、申請時の名称になります。申請後にグループ名/ユーザ名を変更した場合は、変更前の名称が表示されます。

1. [規制解除申請管理]-[規制解除申請一覧]をクリックします。
[規制解除申請一覧]が表示されます。

注意: システム管理者の場合、すべてのグループが表示されます。
グループ管理者の場合、所属するグループおよび下位のグループだけが表示されます。

2. 画面左側のグループ一覧から、規制解除申請を承認、拒否するグループをクリックします。[未処理一覧]タブに未処理の規制解除申請が表示されます。



a. 1画面に表示する規制解除申請の表示件数を変更できます。

b. 画面に表示する規制解除申請一覧のページを変更できます。

	クリックすると、先頭のページが表示されます。
	クリックすると、前のページが表示されます。
	現在表示中のページ番号が表示されます。 表示したいページを直接指定することもできます。
	クリックすると、次のページが表示されます。
	クリックすると、最終のページが表示されます。

c. 現在の規制解除申請一覧を、タイトル行をクリックして並び替えができます。

ソート項目は、[グループ名]、[ユーザ名]、[申請日時]、[対象URL]、[規制理由]のタイトル行から選択できます。
選択されたソート項目は、△(昇順)で表示されます。

3. 承認、拒否する規制解除申請をクリックします。

   [規制解除申請詳細]が表示されます。

4. [規制解除申請詳細]で、申請内容を確認後、[承認する]または[拒否する]を選択して、[確定]ボタンをクリックします。

   規制解除申請の結果が登録されます。メール通知が設定されている場合、ユーザに通知メールを送信します。

   - URL で規制された場合

承認 / 拒否理由		申請者へのコメントを入力します。
例外 URL	登録先ルール	ルールを所有しているグループ名とルール名を「>」でつなげて表示されます。
	カテゴリ	例外URLのカテゴリを[許可カテゴリ]と[閲覧のみ許可]から選択します。
	URL	規制を解除するための例外URLを設定します。 規制解除申請では登録形式は「通常 URL」として登録されます。
	有効期間	規制解除する有効期間を設定します。[有効期間を設定しない]と[有効期間を設定する]から選択します。 [有効期間を設定する]をオンにした場合は、開始日と終了日をYYYYMMDD形式で指定します。 (YYYY:西暦、MM:月、DD:日)

注意:
- URLで規制された場合は、「許可カテゴリ」または「閲覧のみ許可」として例外URLに登録できます。
  例外URLについては、「5-3. 例外URLの設定」(230ページ)を参照してください。
- 承認ができない(閲覧と拒否だけできる)ユーザの場合は、[例外URL]の項目は画面に表示されません。

- キーワードで規制された場合

承認 / 拒否理由		申請者へのコメントを入力します。
規制キーワード	対象ルール	ルールを所有しているグループ名とルール名を「>」でつなげて表示されます。
	削除キーワード	規制を解除するために削除するキーワードが表示されます。

注意:
- キーワードで規制された場合は、対象となるキーワードを削除できます。
  すべてのグループ / ユーザに適用するフィルタリング設定からキーワードを削除する場合は、「4-4. 検索キーワード規制の設定」(201ページ)、「4-5. 書き込みキーワード規制の設定」(204ページ)を参照してください。
  各グループ / ユーザに適用するフィルタリングルールからキーワードを削除する場合は、「5-8. 検索キーワード規制の設定」(280 ページ)、「5-9. 書き込みキーワード規制の設定」(288ページ)を参照してください。
- 承認ができない(閲覧と拒否だけできる)ユーザの場合は、[規制キーワード]の項目は画面に表示されません。

以上で、規制解除申請の承認、拒否は終了です。

3-4. 規制解除申請の承認、拒否結果を閲覧する

規制解除申請の結果を閲覧します。

1. [規制解除申請管理]-[規制解除申請一覧]をクリックします。

   [規制解除申請一覧]が表示されます。

2. 画面左側のグループ一覧から、規制解除申請の結果を閲覧するグループをクリックします。

   [未処理一覧]タブに未処理の規制解除申請が表示されます。

3. [処理済一覧]タブをクリックします。

   [処理済一覧]タブに規制解除申請の結果が表示されます。

4. 規制解除申請をクリックします。

   [規制解除申請結果]が表示され、規制解除申請の結果を閲覧できます。
   閲覧が終了したら、[前画面へ戻る]ボタンをクリックして、[規制解除申請一覧]に戻ります。

以上で、規制解除申請の承認、拒否結果の閲覧は終了です。

3-5. 規制解除申請を削除する

[処理済一覧]タブから規制解除申請の結果を削除します。

1. [規制解除申請管理]-[規制解除申請一覧]をクリックします。

   [規制解除申請一覧]が表示されます。

2. 画面左側のグループ一覧から、規制解除申請を削除するグループをクリックします。

   [未処理一覧]タブに未処理の規制解除申請が表示されます。

3. [処理済一覧]タブをクリックします。

   規制解除申請の結果が表示されます。

4. 削除する規制解除申請結果のチェックボックスをオンにします。

   タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
   タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになり

ます。

5. [削除]ボタンをクリックします。

   確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。
   「削除が完了しました。」と表示され、選択した規制解除申請結果が削除されます。

注意:
- URL で規制された規制解除申請を承認した場合、規制解除申請の履歴を削除しても「許可カテゴリ」または「閲覧のみ許可」として登録した例外URLは削除されません。承認したURLを再度規制したい場合は、例外URLを削除してください。
  例外URLの削除については、「例外URLを削除する」(243ページ)を参照してください。
- キーワードで規制された規制解除申請を承認した場合、規制解除申請の履歴を削除してもキーワードは削除されたままになります。承認したキーワードを再度規制したい場合は、規制キーワードを再登録してください。
  すべてのグループ/ユーザに適用するフィルタリング設定にキーワードを登録する場合は、「4-4. 検索キーワード規制の設定」(201ページ)、「4-5. 書き込みキーワード規制の設定」(204ページ)をしてください。
  各グループ/ユーザに適用するフィルタリングルールにキーワードを登録する場合は、「5-8. 検索キーワード規制の設定」(280ページ)、「5-9. 書き込みキーワード規制の設定」(288ページ)を参照してください。

以上で、規制解除申請の削除は終了です。

設定情報の管理

1. [設定情報管理]画面でできること

システム設定(proxy.inf)の情報一覧の確認、設定の保存/復旧/同期ができます。

1-1. 設定情報の確認

システム設定(proxy.inf)の情報一覧を確認できます。
→「2. 設定情報の確認」(353ページ)

1-2. 設定の保存 / 復旧 / 同期

管理画面で設定した内容の保存、および保存した設定の復旧ができます。
万一の際のバックアップに設定を保存しておくことをお勧めします。設定は最大で5つまで保存できるので、試験運用時の設定の保存/復旧にも利用できます。
また、設定をレプリカサーバに同期できます。
→「3. 設定の保存/復旧/同期」(354ページ)

2. 設定情報の確認

ISWMでは、システム設定(proxy.inf)の情報一覧を確認できます。

1. [設定情報管理]-[設定情報一覧]をクリックします。

   [設定情報一覧]が表示されます。

2. [設定情報一覧]で、システム設定(proxy.inf)の情報一覧を確認します。

   システム設定(proxy.inf)の詳細については、「B-3. proxy.inf」(442ページ)を参照してください。

3. 設定の保存/復旧/同期

ISWM は、グループ情報やフィルタリングルール、スケジュールなどの設定をバックアップとして保存しておくことで、万一の障害時の復旧作業時に、迅速なシステム復旧を可能にします。
また、設定をレプリカサーバに同期できます。

注意: インストール終了後に、初期状態を「yyyymmdd_default」として自動的に保存します。何らかの障害でデータが破損した場合、このデータを指定して復旧することで、初期状態に戻すことができます。

3-1. 設定を保存する

ISWM では、グループ情報やフィルタリングルール、スケジュールなどの設定をファイルに保存できます。
また、設定をローカルにダウンロードできます。ローカルにダウンロードした設定は、アップロードして保存することもできます。

1. [設定情報管理]-[保存/復旧/同期]をクリックします。

   [保存/復旧/同期]が表示されます。

2. 現在の状態を保存する場合、[保存/復旧]-[現在の状態を保存する]をクリックします。

   ローカルにある設定をアップロードして保存する場合、[保存/復旧]-[アップロードして保存する]をクリックします。

3. 現在の状態を保存する場合、[保存/復旧]-[現在の状態を保存する]-[ファイル名]欄に保存するファイル名を入力し、[保存]ボタンをクリックします。

   ローカルにある設定をアップロードして保存する場合、[保存/復旧]-[アップロードして保存する]-[ファイル名]欄にアップロードする設定ファイル名を入力し、[保存]ボタンをクリックします。[参照]ボタンをクリックすると、[アップロードするファイルの選択]画面が別ウィンドウで表示されます。一覧からファイルを選択して、[開く]ボタンをクリックすると、選択したファイルのパスとファイル名が設定されます。
   確認のダイアログが表示されます。

4. [OK]ボタンをクリックします。

   保存したファイルが一覧表示されます。

   注意:
   - 設定は最大で5件まで保存できます。
   - 設定は、[保存/復旧]に表示される一覧のファイル名をクリックして、ローカルにダウンロードできます。
   - 不要になった設定は、[保存/復旧]に表示される一覧から選択して、[削除]ボタンをクリックして削除できます。

以上で、設定の保存は完了です。

3-2. 設定を復旧する

ISWMでは、保存した設定からサーバの設定を復旧できます。

注意: 復旧時は、プライマリサーバと同期してレプリカサーバも復旧します。また、復旧に失敗した場合は、サーバ設定画面にメッセージが表示されます。

1. [設定情報管理]-[保存/復旧/同期]をクリックします。

   [保存/復旧/同期]が表示されます。

2. 復旧に使用する設定の右にあるラジオボタンをクリックして選択し、[復旧]ボタンをクリックします。

   確認のダイアログが表示されます。

3. [OK]ボタンをクリックします。

   [保存/復旧/同期]に、「復旧が完了しました。サーバの再起動を行ってください。」と表示されます。

4. サーバを再起動します。

   注意: 設定の復旧完了後は、すべてのサーバを再起動してください。

以上で、設定の復旧は完了です。

3-3. 設定を同期する

ISWMでは、設定をレプリカサーバに同期できます。また、設定を変更したときに自動的にレプリカサーバと同期するように設定できます。

1. [設定情報管理]-[保存/復旧/同期]をクリックします。

   [保存/復旧/同期]が表示されます。

2. [今すぐ同期を実行]ボタンをクリックします。

   確認のダイアログが表示されます。

   注意: 管理画面で設定を変更したとき、自動的にプライマリサーバとレプリカサーバが同期しないように設定したい場合は、[設定変更時に自動で同期を行う]チェックボックスをオフにしてください。

3. [OK]ボタンをクリックします。

   設定がレプリカサーバに反映されます。

以上で、設定の同期は完了です。

ログの設定と管理

1. [ログ管理]画面でできること

[ログ管理]では、ユーザのアクセスログとシステムログを管理します。また、Syslog転送機能の設定が行えます。

1-1. ログファイルの取得/出力先設定

[ログ管理]-[ログ設定]では、各種のログファイルの取得方法や出力する項目などの設定ができます。

1-2. Syslog 転送の設定

[ログ管理]-[Syslog転送設定]では、ログ転送機能を設定します。
ログ転送機能によってISWMのアクセスログをネットワーク上のSyslogサーバに転送できます。
Syslog転送設定は、システム管理者だけが使用できます。

1-3. アクセスログの管理

[ログ管理]-[アクセスログ]では、ユーザのアクセスログを管理します。
アクセスログには、アクセスしたユーザ(アカウント/IPアドレス)および閲覧したURLなどが記録されます。アクセスログを調査して、不正なアクセスを確認したり、ユーザがアクセスするWebサイトの傾向を分析できます。
アクセスログ管理機能は、システム管理者と第一階層のグループ管理者が使用できます。第二階層以下のグループ管理者は使用できません。

注意:
- 第一階層のグループ管理者が、アクセスログ管理機能を使用するためには、[ログ管理]-[ログ設定]で、アクセスログの出力単位を「第一階層グループ毎」に設定してください。ログの出力単位が「システム一括」の場合、メインメニューの[ログ管理]が表示されません。
  設定については、「2. ログファイルの設定」(359ページ)を参照してください。
- アクセスログの調査、分析には、アクセスログ分析ツール「LogLyzer」を使用できます。

1-4. システムログの管理

[ログ管理]-[システムログ]では、システムログを管理します。
システムログには、いつ、どのプロセスで、どんな操作を行ったかが記録されます。
システムログを調査して、システムの操作履歴を確認できます。
システムログ管理機能は、システム管理者だけが使用できます。

2. ログファイルの設定

2-1. ログファイルの出力設定

LogLyzerとの連携により、ISWMの各種のログ(リクエストログ、POSTログ)を出力して分析することができます。ここでは、ISWMで収集するログファイルの出力設定をします。

1. [ログ管理]-[ログ設定]をクリックします。

   [ログ設定]が表示されます。

2. 次の項目を設定します。

共通設定

ファイル名	作成するログファイル名を入力します。拡張子を含めて、128文字以内で指定します。 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。 ログファイル名にディレクトリを指定した場合、指定ディレクトリにログファイルが保存されます。
ローテート種別	サイズや時期などにより、ログを更新するタイミングを設定します。 指定したタイミングで、それまでのログファイルを別ファイルとして保存し、新しいログファイルにログの記録を開始します。 タイミングは[サイズ]または時期([毎日]、[毎週]、[毎月])から選択します。 ローテート種別で[サイズ]を選択した場合、ローテートするファイルサイズを入力します。MB単位で指定します。 ローテート種別で[毎日]、[毎週]、[毎月]を選択した場合は、ファイルサイズが2Gバイトを超えたときにも自動でローテートするかどうかを指定できます。[ファイルサイズが2Gバイトを超えたときにローテートする]チェックボックスをオンにすると、ローテートします。 ※リクエストログおよびPOSTログは、ローテートのタイミングを「毎日」に設定した場合は毎日午前0時、「毎週」に設定した場合は日曜日の午前0時、「毎月」に設定した場合は毎月1日の午前0時に、ローテートを実施します。 再起動などによってローテートのタイミング時に ISWM のサービスが停止していた場合、実施されません。

自動削除	チェックボックスをオンにすると [保持ファイル数] で指定したファイル数を超えた時点で、自動的にログファイルを削除します。
保持ファイル数	ログファイルとして保持するファイルの最大数を指定します。

アクセスログ出力設定

ファイル出力単位	アクセスログを出力する単位を選択します。 • システム一括 • 第一階層グループ毎

リクエストログ出力設定

出力形式	アクセスログの出力形式を選択します。 • 出力しない: クライアントからのリクエストを出力しません。 • TEXTのみ出力する: TEXT、HTML、CSS、XMLファイルなどに対してのリクエストを出力します。 • 全てのファイルを出力する: 画像ファイルなども含め、すべてのファイルに対するクライアントからのリクエストを出力します。

出力項目	アクセスログとして出力する項目を選択します(複数選択可)。 • グループ名: ユーザ認証によって特定されたグループ名を出力します。 グループ名が特定されなかった場合は出力されません。 • アカウント名: ユーザ認証によって特定されたアカウント名を出力します。 アカウント名が特定されなかった場合は出力されません。 • ブラウザバージョン: クライアントから送信されたブラウザ情報(User-Agent)を出力します。 • WWWサーバIP: アクセスしたWebサーバのドメイン名をIPアドレスに変換して出力します。 • 応答コード: アクセスしたURLからの応答コードを出力します。 • 送信データサイズ: 送信データサイズを出力します。 • 受信データサイズ: 受信データサイズを出力します。 • ファイルタイプ: アクセスしたURLで特定されたファイルタイプを出力します。ファイルタイプが特定されなかった場合は出力されません。 • コンテンツタイプ: HTTPヘッダのContent-Typeから取得したMIMEタイプを出力します。 • 登録カテゴリ: 登録カテゴリを出力します。 • HTTPバージョン: リクエストされたHTTPバージョンを出力します。 • リクエストメソッド: リクエストされたメソッド名を出力します。 • リンク元サイト: リンク元サイトを出力します。

出力条件	アクセスログとして出力する条件を選択します(複数選択可)。 • Proxied: 上位へ転送したリクエスト(規制対象として登録されていないか、許可カテゴリに含まれているデータ) • Confirm: 規制されたリクエスト(一時解除可能) • Blocked: 規制されたリクエスト(ポリシーで許可されていないか、IP規制、データベース更新中の場合) • Allowed: 許可されたリクエスト(規制カテゴリに登録されているがポリシーで許可されたデータ) • Release: 一時解除されたリクエスト(ポリシーで許可されていないが一時解除機能によって転送したデータ) • CfmPost: 書き込み規制されたリクエスト(一時解除可能) • BlkPost: 書き込み規制されたリクエスト

注意: ICAP版では、出力項目の[WWWサーバIP]、[応答コード]、[転送時間]、[受信データサイズ]、[コンテンツタイプ]は表示されません。

POSTログ出力設定

掲示板などに書き込みした内容や送信したファイルなどをPOSTログに保存するときの最小サイズと最大サイズをバイト単位で入力します。
一回の書き込みや送信につき、先頭から指定した最大バイト数をPOSTログに保存します。指定した最大サイズを超えた部分の内容は保存されません。指定した最小バイト数未満の内容は通信ヘッダなども含めて保存されません。
最大バイト数はデフォルトでは0に設定されているので、書き込み内容や送信ファイルなどは保存されません。

注意: POST ログは全角文字をエンコードした状態で保存します。そのためテキストエディタなどでは、書き込み内容が正常に表示されないことがあります。
このような場合には、LogLyzer などの全角文字をデコードして表示するツールを使用すると、書き込み内容が正常に表示できます。

通信シーケンスログ出力設定

[出力設定]の[出力する]チェックボックスをオンにすると、詳細なアクセス状況を記録することができます。

注意:
- ICAP版では通信仕様上、CONNECTによるトンネリング通信、FTP通信、名前解決など、ICAPクライアントがICAPサーバを経由せずに行う通信に関してのログは出力されません。
- ICAP版で通信シーケンスログを利用する場合にクライアントからの接続数が増加するため、設定ファイル (proxy.inf) の [CONTROL_CFG] セクションに「ICAP_MAXCONNECTIONS=」を追加し、値として [CONTROL_CFG] セクションの「SERVER_PROCESS」と同じ数値を追加してください。

3. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

4. [OK]ボタンをクリックします。

以上で、ログファイルの出力設定は完了です。

3. Syslog転送の設定

[ログ管理]-[Syslog転送設定]では、アクセスログの転送設定が行えます。

注意: システム管理者だけがSyslog転送を設定できます。

3-1. Syslog転送を設定する

1. 転送機能を有効にします。

   Syslog転送機能を使用する場合は、[有効]チェックボックスをオンにします。

2. 転送先サーバを設定します。

   [Syslogサーバ]にIPアドレスまたはホスト名、ポート番号を指定します。

3. 転送時のプロトコルを指定します。

   [通信プロトコル]でログ転送時のプロトコルを指定します。
   指定できる転送プロトコルは「UDP」、「TCP」、「TLS」の3種類です。

   注意: TLS以外の通信プロトコルではログが暗号化されないため、データを傍受される危険性があります。[上記注意事項に同意し、通信プロトコルを変更する]チェックボックスをオンにすることで、TLS以外の通信プロトコルが選択できます。

4. ログのフォーマットを指定します。

   [フォーマット]にログのフォーマットを指定します。
   ログのフォーマットは「IETF」、「BSD」の2種類から選択できます。

5. ファシリティを指定します。

   [機能区分]にSyslogのファシリティを指定します。

6. プライオリティを指定します。

   [重大度]にSyslogのプライオリティを指定します。

7. 設定を保存します。

   画面右上の[保存]ボタンをクリックします。

確認のダイアログが表示されます。

注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

8. [OK]ボタンをクリックします。

以上で、Syslog転送の設定は完了です。

4. アクセスログの管理

[ログ管理]-[アクセスログ]では、システム全体または第1階層グループごとにアクセスログを管理します。システム管理者はシステム全体、第一階層のグループ管理者は管理するグループと下位グループのアクセスログを管理できます。
アクセスログには、現在記録中のログファイルとローテート済みのログファイルがあります。現在記録中のログファイルは閲覧が、ローテート済みのログファイルはダウンロード、または削除が可能です。
ローテートについては、「2. ログファイルの設定」(359ページ)を参照してください。

注意:
- 第二階層以下のグループ管理者の場合、メインメニューの[ログ管理]は表示されません。
- 第一階層のグループ管理者が[ログ管理]-[アクセスログ]を使用する場合、[ログ管理]-[ログ設定]で、アクセスログの出力単位を「第一階層グループ毎」に設定してください。「システム一括」に設定している場合、メインメニューの[ログ管理]が表示されません。
  設定については、「2. ログファイルの設定」(359ページ)を参照してください。
- 出力中のログを強制的にローテートしたい場合、「amslog」コマンドを使用してください。
  「A-15. amslog[ログファイルのアーカイブ]」(421ページ)を参照してください。

4-1. 現在のアクセスログを閲覧する

現在記録中のアクセスログの内容を最新行から最大1000行分まで閲覧できます。

1. [ログ管理]-[アクセスログ]をクリックします。

   システム管理者の場合、[アクセスログ]に[出力単位]が表示されます。
   グループ管理者の場合、所属グループの[アクセスログ]に[現在のログ]および[ローテート済みのログ]が表示されます。手順3に進んでください。

2. [出力単位]で、アクセスログ出力単位を選択して、[選択]ボタンをクリックします。

   [現在のログ]および[ローテート済みのログ]が表示されます。

3. [現在のログ]および[ローテート済みのログ]で、アクセスログの一覧を確認します。

   現在のログファイル一覧、ローテート済みのログファイル一覧を、タイトル行をクリックしてそれぞれ昇順に並び替えることができます。ソート項目は、[ログファイル名]、[サーバ名]、[サイズ[Mbyte]]、[更新日時]のタイトル行から選択できます。

選択されたソート項目は、△(昇順)で表示されます。

注意: ローテート済みのログは、[ログ管理]-[ログ設定]-[共通設定]-[自動削除]で指定されたファイル数を超えると、自動的に削除されます。

4. [現在のログ]で、閲覧するログファイル名をクリックします。

   [ログ閲覧]画面が別ウィンドウで表示されます。
   アクセスログの出力項目については、「2. ログファイルの設定」(359ページ)を参照してください。

出力単位	アクセスログ出力単位を表示します。
サーバ名	アクセスログ出力対象のサーバ名を表示します。
ファイル名	表示中のアクセスログファイル名を表示します。

5. 表示する行数を選択し、[表示]ボタンをクリックします。

   行数はログの末尾から[100行]、[500行]、[1000行]を選択できます。表示されるログは末尾の行ほど、新しいログになります。

6. [閉じる]ボタンをクリックします。

   [ログ閲覧]画面を閉じ、[アクセスログ]のアクセスログの一覧に戻ります。

4-2. ローテート済みアクセスログをダウンロード、削除する

ローテート済みアクセスログは、CSVファイルでダウンロードできます。また、不要なローテート済みアクセスログを削除できます。

1. [ログ管理]-[アクセスログ]をクリックします。

   システム管理者の場合、[アクセスログ]に[出力単位]が表示されます。
   グループ管理者の場合、所属グループの[アクセスログ]に[現在のログ]および[ローテート済みのログ]が表示されます。手順3に進んでください。

2. [出力単位]で、アクセスログ出力単位を選択して、[選択]ボタンをクリックします。

   [現在のログ]および[ローテート済みのログ]が表示されます。

3. [現在のログ]および[ローテート済みのログ]で、アクセスログの一覧を確認します。

現在のログファイル一覧、ローテート済みのログファイル一覧を、タイトル行をクリックしてそれぞれ昇順に並び替えることができます。ソート項目は、[ログファイル名]、[サーバ名]、[サイズ[Mbyte]]、[更新日時]のタイトル行から選択できます。
選択されたソート項目は、△(昇順)で表示されます。

注意: ローテート済みのログは、[ログ管理]-[ログ設定]-[共通設定]-[自動削除]で指定されたファイル数を超えると、自動的に削除されます。

4. [ローテート済みのログ]で、ダウンロードまたは削除するアクセスログのチェックボックスをオンにします。

タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

5. [ダウンロード]ボタンまたは[削除]ボタンをクリックします。

確認のダイアログが表示されます。

注意: アクセスログをダウンロードする場合、1 ファイルずつダウンロードしてください。複数のアクセスログを一度にダウンロードすることはできません。

6. [OK]ボタンをクリックします。

[ダウンロード]ボタンをクリックした場合、選択したアクセスログがダウンロードされます。
[削除]ボタンをクリックした場合、選択したアクセスログが削除されます。

5. システムログの管理

[ログ管理]-[システムログ]では、システム全体でシステムログを管理します。
システム管理者だけがシステムログを管理できます。
システムログには、現在記録中のログファイルとローテート済みのログファイルがあります。現在記録中のログファイルは閲覧が、ローテート済みのログファイルはダウンロード、または削除が可能です。ローテートについては、「2. ログファイルの設定」(359ページ)を参照してください。

5-1. システムログの一覧を表示する

現在ログ記録中のシステムログファイルとローテート済みシステムログファイルを一覧表示します。
ログファイルの閲覧、管理方法については、「5-2. 現在のシステムログを閲覧する」(371ページ)または「5-3. ローテート済みシステムログをダウンロード、削除する」(372 ページ)を参照してください。

1. [ログ管理]-[システムログ]をクリックします。

   [システムログ]に[現在のログ]および[ローテート済みのログ]が表示されます。

2. [現在のログ]および[ローテート済みのログ]で、システムログの一覧を確認します。

   現在のログファイル一覧、ローテート済みのログファイル一覧を、タイトル行をクリックしてそれぞれ昇順に並び替えることができます。ソート項目は、[ログファイル名]、[サーバ名]、[サイズ[Mbyte]]、[更新日時]のタイトル行から選択できます。
   選択されたソート項目は、△(昇順)で表示されます。

■ ログファイルの内容

システムログのファイル名は、以下のルールで設定されます。
現在のシステムログファイル:
<ログファイル名>_xxx.aaa
ローテート済みのシステムログファイル:
<ログファイル名>_xxx_yyyymmdd_nnn.aaa

ログファイル名	[ログ管理]-[ログ設定]-[共通設定]-[ファイル名]で設定したファイル名が表示されます。

ログの種類 (xxx)	ログファイルの種類が表示されます。 • サービスログ(service) サービスの起動、稼動状況、システムエラーなどが記録されます。 • 管理ログ(adm) 管理サービス(稼動状況、データベースのダウンロードなど)の状況などが記録されます。 • コントロールログ(ctrl) 管理画面への処理内容が記録されます。 • LogLyzerログ(loglyzersys) LogLyzerからのログ取り込み状況が記録されます。 • プロキシサーバログ(proxy) プロキシサーバの稼動状況などが記録されます。 • 注意ログ(notice) 認証に失敗した理由などが記録されます。 • フィルタリングサーバログ(filtering) フィルタリングサーバの稼動状況などが記録されます。 • キャッシュサーバ初期化ログ(cacheini) キャッシュサーバ初期化の内容などが記録されます。 • キャッシュサーバログ(laptor) キャッシュサーバの内容などが記録されます。 • アクセスログ(http) HTTP、HTTPS、FTP over HTTPのプロキシの内容が記録されます。 • POSTログ(post) 掲示板などに書き込みした内容が記録されます。 • 通信シーケンスログ(sequence) 詳細なアクセス状況が記録されます。 • 規制解除申請ログ(offer) ユーザから送信された規制解除申請の内容が記録されます。 • マッチングログ(matching) URLデータベース処理に関するシステムログが記録されます。 • ICAP連携ログ(icap) ICAP連携の処理内容が記録されます。 • 集計ログ(geo) 集計サービスの状況などが記録されます。
日付 (yyyymmdd)	ローテートした日付が表示されます。
連番 (nnn)	同一日付でローテートされた場合のための連番(001～999)が表示されます。

拡張子 (aaa)	拡張子が表示されます。

ログファイル名を「iswm.log」に指定した場合、ローテート済みシステムログは、以下のようなファイル名で保存されます。

- iswm_service_20201001_001.log
- iswm_adm_20201001_001.log
- iswm_ctrl_20201001_001.log
- iswm_loglyzersys_20201001_001.log
- iswm_proxy_20201001_001.log
- iswm_notice_20201001_001.log
- iswm_filtering_20201001_001.log
- iswm_laptor_20201001_001.log
- iswm_http_20201001_001.log
- iswm_post_20201001_001.log
- iswm_offer_20201001_001.log
- iswm_matching_20201001_001.log
- iswm_icap_20201001_001.log
- iswm_sequence_20201001_001.log
- iswm_geo_20201001_001.log

注意:
- 注意ログ (notice) は、スタンドアロン版だけに出力されます。ICAP 版では出力されません。
- ローテート済みシステムログは、ローテート後、[ログ管理]-[ログ設定]-[共通設定]-[自動削除]で指定されたファイル数を超えると、自動的に削除されます。
- キャッシュサーバ初期化ログ (cacheini) は、サイズや時期などによるローテート、およびamslogコマンドによるローテートの対象外になります。

5-2. 現在のシステムログを閲覧する

記録中のシステムログは、ファイルをクリックして最近のログを1000行まで閲覧できます。

1. [ログ管理]-[システムログ]をクリックします。
   [システムログ]に[現在のログ]および[ローテート済みのログ]が表示されます。
2. [現在のログ]に表示されているログファイルから閲覧したいログファイルをクリックし

ます。

[ログ閲覧]画面が別ウィンドウで表示されます。

3. 表示する行数を選択し、[表示]ボタンをクリックします。

行数はログの末尾から[100行]、[500行]、[1000行]を選択できます。表示されるログは末尾の行ほど、新しいログになります。

4. [閉じる]ボタンをクリックします。

[ログ閲覧]画面が閉じます。

5-3. ローテート済みシステムログをダウンロード、削除する

ローテート済みシステムログファイルは、ダウンロードしてエディタなどで閲覧します。また、不要なローテート済みシステムログを削除できます。

注意: ローテート済みのログは、[ログ管理]-[ログ設定]-[共通設定]-[自動削除]で指定されたファイル数を超えると、自動的に削除されます。なお、ローテート済みのログは閲覧できません。

1. [ログ管理]-[システムログ]をクリックします。

[システムログ]に[現在のログ]および[ローテート済みのログ]が表示されます。

2. [ローテート済みのログ]で、ダウンロードまたは削除するシステムログのチェックボックスをオンにします。

タイトル行のチェックボックスをオンにすると、すべてのチェックボックスがオンになります。
タイトル行のチェックボックスをオフにすると、すべてのチェックボックスがオフになります。

3. [ダウンロード]ボタンまたは[削除]ボタンをクリックします。

確認のダイアログが表示されます。

注意: システムログをダウンロードする場合、1 ファイルずつダウンロードしてください。
複数のシステムログを一度にダウンロードすることはできません。

4. [OK]ボタンをクリックします。

   [ダウンロード]ボタンをクリックした場合、選択したシステムログがダウンロードされます。
   [削除]ボタンをクリックした場合、選択したシステムログが削除されます。

クライアントPCの設定

1. クライアントPCの設定

ISWMでフィルタリングを実行するとき、クライアントPCのWebブラウザでプロキシサーバの設定が必要な場合があります。使用するWebブラウザのプロキシサーバの設定で、プロキシサーバのIPアドレス/ドメイン、ポート番号を設定します。

1-1. スタンドアロン版の場合

ISWMがプロキシサーバとして動作して、フィルタリングを実行します。クライアントPCのWebブラウザでは、次のようにプロキシサーバを設定します。

プロキシサーバのIPアドレス	ISWMのIPアドレス
プロキシサーバのポート番号	ISWMで、フィルタリングに使用するポート番号(HTTP、HTTPS、FTP over HTTP)

注意:
- スタンドアロン版では、URL が相対パス形式となったリクエストラインには対応していません。
- ISWM の IP アドレス、フィルタリングに使用するポート番号は、[サーバ管理]-[サーバ設定]の[サーバ情報]で確認できます。

1-2. ICAP版の場合

クライアントPCからの通信は、ICAPクライアント経由でISWMに送信されます。クライアントPCのWebブラウザでは、次のようにプロキシサーバを設定します。

プロキシサーバのIPアドレス	ICAPクライアントのIPアドレス
プロキシサーバのポート番号	ICAP クライアントのポート番号 (HTTP、HTTPS、FTP over HTTP)

注意: ICAPクライアントが透過プロキシとして動作している場合、クライアントPCでプロキシサーバを設定する必要はありません。

2. Webフィルタリング

クライアントPCからリクエスト(HTTP/HTTPS/FTP over HTTP)が送信されると、ISWMでは登録したフィルタリング設定を使用して、フィルタリングを実行します。
[サーバ管理]-[認証設定]の設定によって、グループ、ユーザに適用されるフィルタリング設定が異なります。
認証設定については、「5. ユーザ認証/LDAPの設定」(60ページ)を参照してください。

ユーザ認証が有効な場合

グループごとに設定したフィルタリング設定が適用されます。グループ内のユーザにフィルタリングルールを設定している場合には、ユーザのフィルタリング設定が適用されます。

注意:

- BASIC 認証を使用している場合には、ブラウザ起動時に認証ダイアログが表示されます。ISWMに登録されているアカウント、パスワードを入力して、[OK]ボタンをクリックすると、認証が行われます。認証できない場合には、次のように処理されます。
  - [未登録ユーザ設定] が有効の場合、「未登録ユーザ」グループのフィルタリング設定が適用されます。
  - [未登録ユーザ設定] が無効の場合、認証エラー画面が表示されます。
- [LDAP グループ特定方式] の設定が [グループ毎にユーザ抽出条件を指定する] の場合、LDAPサーバの認証に成功していて、ISWMにユーザ情報が取り込まれていないユーザには、LDAPグループのフィルタリング設定が適用されます。
- 第1階層グループごとにアカウントを管理する場合、アカウント名は次の形式で入力してください。
  「第1階層グループ名」+「¥」または「\」(バックスラッシュ)+「アカウント名」
  例:sales¥yamada
  グループ名およびアカウント名では、大文字と小文字が区別されます。ただし、NTLM認証時およびKerberos認証時には大文字と小文字は区別されません。

ユーザ認証が無効の場合

ルートグループのフィルタリング設定が適用されます。

2-1. 規制画面

カテゴリルールで、「規制」を設定したカテゴリのURLをリクエストすると、規制画面が表示されます。
規制画面の表示方法は、「ファイル」、「URL」、「メッセージ」の3種類があります。「4-6. 規制画面の設定」(207ページ)を参照してください。

注意: Microsoft Edge、Firefox、Chromeをご使用の場合、クライアントがHTTPS規制サイトにアクセスしようとした場合、そのリクエストは規制画面にリダイレクトされます。このとき、ブラウザの証明書警告画面が表示されますので、証明書のインストールを行ってください。手順は、「G. 証明書のインストール」(489ページ)を参照してください。

■ 規制画面 (ファイル) の場合

任意の HTML ファイルを規制画面に表示します。初期状態では「nfblock.htm」が設定されています。
HTMLファイルは次の場所に格納してください。

Windows の場合

＜インストールフォルダ＞¥conf¥block

Linux の場合

＜インストールディレクトリ＞/conf/block

サーバ名	規制応答を行ったサーバのサーバ名が表示されます。
応答時間	規制応答を行った時刻が表示されます。
規制画面に表示する画像	初期状態では、ISWMのロゴ画像が表示されます。 [個別アクセス管理]-[規制画面設定]の規制画面ルールをクリックして表示される[ルール詳細]の[規制画面設定]タブ-[画像設定]で画像が設定されている場合、画像設定で設定した画像が表示されます。 規制画面に表示する画像は、[共通アクセス管理]-[規制画面設定]の[規制画面形式]で、ファイルを指定した場合にだけ、有効になります。

規制メッセージ	初期状態では、「このウェブサイトは現在管理者によって規制されています。」と表示されます。 [個別アクセス管理]-[規制画面設定]の規制画面ルールをクリックして表示される[ルール詳細]の[規制画面設定]タブ-[メッセージ設定 (カテゴリ共通)] で規制メッセージが設定されている場合、メッセージ設定 (共通) で設定した規制メッセージが表示されます。また、[個別アクセス管理]-[規制画面設定]の規制画面ルールをクリックして表示される[ルール詳細]の[規制画面設定]タブ-[メッセージ設定(カテゴリ単位)]で規制メッセージが設定されている場合、メッセージ設定 (カテゴリ単位) で設定した規制メッセージが1行目に表示されます。 規制メッセージは、[共通アクセス管理]-[規制画面設定]の[規制画面形式] で、ファイルまたはメッセージを指定した場合にだけ、有効になります。 メッセージ設定(カテゴリ単位)のメッセージ、メッセージ設定(共通)のメッセージの一方が未設定の場合には、設定されているメッセージだけが表示されます。
リクエストURL	クライアントPCからリクエストされたURLが表示されます。
規制したURLのカテゴリ	リクエストされた URL のメインカテゴリ、サブカテゴリが表示されます。
規制解除申請画面へのリンク	[規制解除申請管理]-[規制解除申請設定]で規制解除申請機能が有効な場合に表示されます。 クリックすると、規制解除申請画面が別ウィンドウで表示されます。 申請理由を入力して、[規制解除申請]ボタンをクリックすると、リクエストした URL と申請理由がログファイルとして保存されます。また、申請メール通知設定が設定されていると、設定した通知先に申請内容をメールで送信できます。 規制解除申請機能については、「2. 規制解除申請の設定」(337 ページ)を参照してください。
認証局証明書のダウンロード	証明書ファイルのダウンロードボタンが表示されます。

■ 規制画面 (URL) の場合

ネットワーク上の任意のWebページを規制画面として使用します。
社内および社外のURLを指定できます。初期状態では、「http://iswm.netstar-inc.com/」が設定されています。

■ 規制画面 (メッセージ) の場合

任意のメッセージと規制したカテゴリの情報を文字列(テキストデータ)として表示します。

サーバ名	規制応答を行ったサーバのサーバ名が表示されます。
応答時間	規制応答を行った時刻が表示されます。
規制メッセージ	[共通アクセス管理]-[規制画面設定]で設定したメッセージが表示されます。 [個別アクセス管理]-[規制画面設定]の規制画面ルールをクリックして表示される[ルール詳細]の[規制画面設定]タブ-[メッセージ設定(カテゴリ共通)]で規制メッセージ(上の画面では「グループA用の規制メッセージ」)が設定されている場合、[共通アクセス管理]-[規制画面設定]で設定したメッセージを置き換えて表示します。 [個別アクセス管理]-[規制画面設定]の規制画面ルールをクリックして表示される[ルール詳細]の[規制画面設定]タブ-[メッセージ設定(カテゴリ単位)]で規制メッセージが設定されている場合、カテゴリ別規制メッセージ(上の画面では『「ニュース」カテゴリのURLに対する規制メッセージです。』)が1行目に表示されます。
リクエストURL	クライアントPCからリクエストされたURLが表示されます。
規制したURLのカテゴリ	リクエストされたURLのメインカテゴリ、サブカテゴリが表示されます。
認証局証明書のダウンロード	証明書ファイルへのリンクが表示されます。

2-2. 一時解除

カテゴリルールで、「一時解除」を設定したカテゴリのURLをリクエストすると、規制画面に一時解除パスワードの入力部分が表示されます。
一時解除パスワードを入力すると、一時解除時間で設定した時間だけ、リクエストしたURLにアクセスできます。

1. [パスワード] テキストボックスに、一時解除パスワードを入力します。

2. [一時解除]ボタンをクリックします。

一時解除時間で設定した時間だけ、リクエストした URL にアクセスできます。

注意:
- 一時解除は[共通アクセス管理]-[規制画面設定]の[規制画面形式]で、ファイルを指定したときにだけ、有効になります。
- カテゴリごとに一時解除を有効にするには、[個別アクセス管理]-[カテゴリ設定] でカテゴリルールを設定します。
  「カテゴリルールを設定する」(214ページ)を参照してください。
  グループ / ユーザに対して、カテゴリルールを適用する場合、「カテゴリルールをグループに適用する」(312 ページ)または「カテゴリルールをユーザに適用する」(324 ページ)を参照してください。
- 優先カテゴリに一時解除を有効にするには、[個別アクセス管理]-[優先カテゴリ設定]で優先カテゴリルールを設定します。
  「5-6. 優先カテゴリの設定」(264ページ)を参照してください。
  グループに対して、優先カテゴリルールを適用する場合、「優先カテゴリルールをグループに適用する」(317ページ)を参照してください。
- 一時解除パスワード、一時解除時間を設定するには、[個別アクセス管理]-[規制オプション設定]で規制オプションルールを設定します。
  「5-11. 規制オプションの設定」(302ページ)を参照してください。
  グループ/ユーザに対して、規制オプションルールを適用する場合、「規制オプションルールをグループに適用する」(322ページ)または「規制オプションルールをユーザに適用する」(329ページ)を参照してください。
- 一時解除パスワードを設定していない場合は、テキストボックスは表示されません。

2-3. 警告画面

■ HTTPS デコード警告画面

[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]-[警告画面設定]で、[HTTPSデコード処理の実行前に、ユーザへ警告画面を表示する] チェックボックスをオンにすると、HTTPS デコード実行前にユーザへの警告画面が表示されます。警告画面で[同意して続行]ボタンをクリックすると、HTTPSサイトを閲覧できます。

■ 証明書警告画面

上位サーバの証明書が、信頼できる認証局によって署名されていない場合に表示されます。
HTTPSサイトを閲覧する場合は、危険性を理解した上で、証明書警告画面の[続行(非推奨)]ボタンをクリックしてください。

注意: [共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]-[HTTPSデコード]有効時のみ表示されます。

2-4. その他の規制

カテゴリごとの規制、一時解除以外に、ISWMで規制できる内容について説明します。

■ 書き込み規制

カテゴリルールで、「書き込み規制」を設定したカテゴリの URL をリクエストすると、掲示板やチャット、フォームを使用したデータ送信など、Webを経由したデータの書き込みを規制できます。

注意:
- 書き込み規制の対象となる URL は、HTTP プロトコルまたは、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]有効時のHTTPSプロトコルでPOST、PUTメソッドを使用しているURLになります。
- 書き込み規制が設定されている場合の書き込み許容サイズは、以下で設定します。
  - システム一括でサイズを設定する場合
    [共通アクセス管理]-[規制オプション設定] で設定します。
    「4-8. 規制オプションの設定」(211 ページ)を参照してください。
  - ルール毎にサイズを設定する場合
    [個別アクセス管理]-[規制オプション設定] で設定します。
    「5-11. 規制オプションの設定」(302 ページ)を参照してください。

■ ブラウザ規制

リクエストを要求した Web ブラウザ、Web ブラウザのバージョンで、アクセスを規制できます。
Webブラウザの判定は、リクエストヘッダの「User-Agent」フィールドで行います。

■ 規制対象の URL を「許可」または「閲覧のみ許可」に設定する

例外URLの[許可カテゴリ]-[許可カテゴリ]にURLを登録すると、フィルタリング用データベースで規制対象のURLでも自由にアクセスできるようになります。
例外URLの[許可カテゴリ]-[閲覧のみ許可]にURLを登録すると、フィルタリング用データベースで規制対象の URL でも閲覧できるようになります。ただし、掲示板、チャットなどの書き込みやフォーム送信は規制されます。

■ 対象の URL を「規制」に設定する

例外URLの[規制カテゴリ]-[規制カテゴリ優先]にURLを登録すると、対象のURLが必ず規制されます。
例外URLの[規制カテゴリ]-[許可カテゴリ優先]にURLを登録すると、対象のURLが規制されますが、[許可カテゴリ]-[許可カテゴリ]または[許可カテゴリ]-[閲覧のみ許可]に同じURLが登録されている場合は許可カテゴリの設定が優先されます。

■ サービスを「許可」または「閲覧のみ許可」に設定する

例外サービスでサービスを「許可」で登録すると、フィルタリング用データベースで規制対象のURLでも自由にアクセスできるようになります。
例外サービスで「閲覧のみ許可」で登録すると、フィルタリング用データベースで規制対象のURLでも閲覧のアクセスを許可します。

3. パスワードの変更

一般ユーザ、システム管理者者(例外URL設定のみ)、グループ管理者(例外URL設定のみ)は、管理画面にログインして、登録したアカウントのパスワード、メールアドレスを変更できます。

注意:
- システム管理者、システム管理者(制限付き)、システム管理者(閲覧のみ)、グループ管理者、グループ管理者(制限付き)、グループ管理者(閲覧のみ)は、[グループ/ユーザ管理]-[ユーザ管理]で、パスワード、メールアドレスを変更してください。
「4-6. IPアドレス/アカウントを変更する」(145ページ)を参照してください。
- LDAP 連携時、管理画面ではメールアドレスだけ変更できます。パスワードは LDAP サーバで変更してください。

1. ブラウザで管理画面にアクセスします。

プライマリサーバの IP アドレスが 192.168.1.1、ポートが 2319 の場合
http://192.168.1.1:2319/index.html と入力します。
ログイン画面が表示されます。

注意: ポート番号を変更している場合、設定にあわせてURLのポート番号部分(2319)を変更してください。

2. アカウントとパスワードを入力し、[ログイン]ボタンをクリックします。

変更するユーザのアカウントとパスワードを使用します。
ログインすると、[アカウント情報編集] が表示されます。

注意: 第 1 階層グループごとにアカウントを管理する場合、アカウント名は次の形式で入力してください。
「第1階層グループ名」+「¥」または「\」(バックスラッシュ)+「アカウント名」
例:sales¥yamada
グループ名およびアカウント名では、大文字と小文字が区別されます。

3. パスワード、メールアドレスを変更します。

アカウント名	ログインしたユーザのアカウント名が表示されます。
パスワード	現在のパスワードが「●」で表示されます。 パスワードを変更する場合には、新しいパスワードを入力します。
パスワード(確認)	[パスワード]に入力したパスワードを再度入力します。
メールアドレス	任意でメールアドレスを入力します。

4. [保存]ボタンをクリックします。

   更新を確認するダイアログが表示されます。

5. [OK]ボタンをクリックします。

以上で、パスワード、メールアドレスの変更は完了です。

付録

A. コマンドラインインタフェース

A-1. コマンドの使用方法

管理画面の各種設定をコマンドラインから実行できます。
コマンドは、次のディレクトリで実行してください。
＜インストールディレクトリ＞/bin/

注意:
- Linux 環境では、root またはインストール時に指定した ISWM 実行ユーザで実行してください。
- コマンドを使ったエクスポートおよびインポートは同一バージョン間で行ってください。異なるバージョン間で行った場合、正常にインポートできない場合があります。

■グループ記述ファイル

以下のコマンドでは、実行時の対象となるグループを事前に「グループ記述ファイル」として作成します。

- amsaccount
- amsip
- amsurl
- amscaterule
- amsschedule
- amslog
- amscatemsg
- amscatepostsize

グループ記述ファイルは、以下のような書式で、テキストファイルとして作成してください。

1行につき、1つのグループを記述します。

```
総務部
営業本部￥第 1 営業グループ
大学院￥網星研究室
```

注意:
- 上位グループが存在する場合、第 1 階層から「¥」または「\」(バックスラッシュ) で区切って入力します。
- グループ記述ファイルでは、グループ名を「"」(ダブルクオーテーション) で囲む必要はありません。

A-2. amserror.logについて

amserror.logには、コマンド実行時のエラーが記録されます。
以下のように、出力日時とエラーメッセージを、コマンドを実行したフォルダに出力します。
2010-04-02 20:29:36,234 Failed to store configuration file.

A-3. コマンド一覧

ISWMでは、次のコマンドを実行できます。

コマンド	オプション	実行される内容	プライマリサーバ	レプリカサーバ	参照ページ
amsaccount	-add	アカウントの管理	○	×	「A-4. amsaccount[アカウントの管理]」(388ページ)
	-del		○	×	
	-mod		○	×	
	-export		○	×	
	-search		○	×	
amsip	-add	IPアドレスユーザの管理	○	×	「A-5. amsip[IPアドレスユーザの管理]」(392ページ)
	-del		○	×	
	-mod		○	×	
	-export		○	×	

コマンド	オプション	実行される内容	プライマリサーバ	レプリカサーバ	参照ページ
amsgroup	-add	グループ管理	○	×	「A-6. amsgroup[グループ管理]」(395ページ)
	-massadd		○	×	
	-del		○	×	
	-mod		○	×	
	-export		○	×	
amsurl	-export	例外URL設定	○	×	「A-7. amsurl[例外URL]」(400ページ)
	-import		○	×	
	-add		○	×	
	-clear		○	×	
amscaterule	-create	カテゴリルール管理	○	×	「A-8. amscaterule[カテゴリルール管理]」(403ページ)
	-mod		○	×	
	-del		○	×	
	-export		○	×	
amsschedule	-add	スケジュール管理	○	×	「A-9. amsschedule[スケジュール管理]」(408ページ)
	-del		○	×	
	-mod		○	×	
	-export		○	×	
amsdatabase	-download	URLデータベースの管理	○	×	「A-10. amsdatabase[URLデータベース管理]」(412ページ)
	-info		○	×	
	-status		○	×	
amshttpsdectgt	-import	HTTPSデコード対象ホスト管理	○	×	「A-11. amshttpsdectgt[HTTPSデコード対象ホスト管理]」(414ページ)
	-export		○	×	
amsldapgroup	-import	LDAPグループ情報管理	○	×	「A-12. amsldapgroup[LDAPグループ情報管理]」(416ページ)

コマンド	オプション	実行される内容	プライマリサーバ	レプリカサーバ	参照ページ
amsdata	-save	設定の保存/復旧/同期	○	×	「A-13. amsdata[設定の保存 / 復旧 / 同期]」(417ページ)
	-restore		○	×	
	-list		○	×	
	-del		○	×	
	-synchronize		○	×	
	-reflection		○	×	
	-retry		○	×	
	-sys		○	×	
	-reload		○	×	
amsserver	-	サーバ情報の表示	○	×	「A-14. amsserver[サーバ情報表示]」(420ページ)
amslog	-rotation	ログファイルのアーカイブ作成	○	○	「A-15. amslog[ログファイルのアーカイブ]」(421ページ)
	-list		○	×	
	-level		○	○	
amscatemsg	-mod	カテゴリ別メッセージの変更/出力	○	×	「A-16. amscatemsg[カテゴリ別規制メッセージ管理]」(424ページ)
	-export		○	×	
amscontrol	-start	フィルタリングサービスの起動と停止	○	○	「A-17. amscontrol[フィルタリングサービスの起動 / 停止]」(426ページ)
	-stop		○	○	
	-restart		○	○	
amsadminstat	-status	レプリカサーバの状態管理	×	○	「A-18. amsadminstat[レプリカサーバの状態管理]」(427ページ)
	-reset		×	○	

コマンド	オプション	実行される内容	プライマリサーバ	レプリカサーバ	参照ページ
amscatepostsize	-mod	カテゴリ別書き込み規制サイズの変更/出力	○	×	「A-19. amscatepostsize[カテゴリ別書き込み規制サイズ]」(430ページ)
	-export		○	×	
amsgruleflg	-mod	ルール適用(グループ)管理の変更/出力	○	×	「A-20. amsgruleflg[ルール適用(グループ)管理]」(432ページ)
	-export		○	×	
amsuruleflg	-mod	ルール適用(ユーザ)管理の変更/出力	○	×	「A-21. amsuruleflg[ルール適用(ユーザ)管理]」(435ページ)
	-export		○	×	
amstune	--status	サーバのチューニング	○	○	「A-22. amstune[サーバのチューニング]」(437ページ)
	--level		○	○	
amsversion	-	バージョン情報の表示	○	○	「A-23. amsversion[バージョン情報表示]」(439ページ)

○:使用できます。　×:使用できません。

注意: <インストールディレクトリ>/bin に格納している次のファイルは、直接実行しないでください。
amsproxyexe:フィルタリングサービス拡張起動シェル
amsadminexe:管理サービス拡張起動シェル
amsproxysd:フィルタリングサービス管理用起動シェル
amsfilteringexe: 管理サービス拡張起動シェル
amscollectorexe: 集計サービス拡張起動シェル

A-4. amsaccount[アカウントの管理]

amsaccountは、アカウントの追加/削除/設定変更/ファイル出力/検索を行うコマンドです。
追加/削除/設定変更について、対象とするユーザはユーザ情報が記述されたファイル(CSV形式)を参照します。

ファイルのフォーマットについては、「ユーザ情報ファイルのフォーマット」(390ページ)を参照してください。

注意: -encoding オプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ アカウントの追加 [-add]

```
amsaccount -add ファイル名 -encoding [EUC|SJIS|UTF8]
```

-add オプションを使用すると、指定されたファイルに記述されているユーザを一括で追加します。

注意: グループが存在しない場合、ファイルに記述されたグループを新規作成します。
第2階層～第10階層のグループの場合には、上位グループも同時に作成されます。

■ アカウントの削除 [-del]

```
amsaccount -del ファイル名 -encoding [EUC|SJIS|UTF8]
```

-delオプションを使用すると、指定されたファイルに記述されているユーザを一括で削除します。

■ アカウントの設定変更 [-mod]

```
amsaccount -mod ファイル名 -encoding [EUC|SJIS|UTF8]
```

-mod オプションを使用すると、指定されたファイルに記述されているユーザの設定を一括で変更します。

注意: アカウント認証が有効で、さらに LDAP 連携時はパスワード変更することができません。ただし、rootユーザの場合は、パスワードを変更できます。

■ ユーザ情報の出力 [-export]

```
amsaccount -export ファイル名 [-g グループ記述ファイル名 ] -encoding [EUC|SJIS|UTF8] [-p [ON|OFF]]
```

-exportオプションを使用すると、登録されているユーザ一覧を指定されたファイルにCSV形式で出力します。

注意:
- -g オプションを追加してグループ記述ファイルを指定すると、グループ記述ファイルに記述されたグループだけをエクスポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。
- -p オプションを指定した場合は、エクスポート時にパスワードを出力するかどうかを指定します。
  パスワードを出力する場合は「ON」、パスワードを出力しない場合は「OFF」を指定します。
  -pオプションを指定しない場合は、エクスポート時にパスワードを出力します。

■ アカウントの検索 [-search]

```
amsaccount -search アカウント名 [-delay [-multiple 遅延時間倍率 ] ]
```

-searchオプションを使用すると、登録されているユーザを検索して画面に出力します。
指定したアカウント名に部分一致したユーザについて、グループ名と併せて出力されます。

注意:
- -delayオプションを追加すると、検索時に処理を遅延させます。
- -delay オプションに加えて -multiple オプションを指定すると、通常の遅延時間を乗算させた時間で遅延処理を行います。

■ ユーザ情報ファイルのフォーマット

amsaccountコマンドで入出力するユーザ情報ファイルは、次のフィールドで構成されます。

- フォーマット

アカウント名	パスワード	グループ名	メールアドレス	アカウント種別	コメント	個別ルール

- 出力例

"user1",	"password1",	"ネットスター¥営業",	"user1@netstr-inc.com",	"1",	"コメント",	"ルール個別適用"

フィールド名	設定内容
アカウント名	アカウント名を入力します。

フィールド名	設定内容
パスワード	パスワードを入力します。
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3 階層」のように、「¥」または「\」(バックスラッシュ) で区切って入力します。
メールアドレス	メールアドレスを入力します。 メールアドレスを指定しない場合、省略できます。
アカウント種別	0:一般ユーザ 1:グループ管理者(閲覧のみ) 2:グループ管理者(制限付き) 3:グループ管理者 4:システム管理者(閲覧のみ) 5:システム管理者(制限付き) 6:システム管理者 7:グループ管理者(例外URL設定のみ) 8:システム管理者(例外URL設定のみ)
コメント	コメントを入力します。
個別ルール	アカウントに個別ルールが適用されている場合、" ルール個別適用"と出力されます。値の設定はできません。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- フィールドは「"データ"」のように「"」(ダブルクオーテーション)で囲み、フィールド同士は「,」(半角カンマ)で区切ります。
- データのないフィールドは空になりますが、フィールドは省略しないでください。フィールドを省略すると、正しく読み込むことができなくなります。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

読み込んだファイルに処理できない行が存在した場合、処理できなかった行の内容がログファイルに出力されます。また、プライマリサーバとレプリカサーバの通信エラーや、その他のエラーについてもログファイルに出力されます。ログファイルについては、「A-2. amserror.logについて」(385ページ)を参照してください。

■ 終了コード

amsaccountコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-5. amsip[IPアドレスユーザの管理]

amsipは、IPアドレスユーザの追加、削除、変更、出力をするコマンドです。
対象とするユーザは、IPアドレスユーザ情報が記述されたファイル(CSV形式)を参照します。
ファイルのフォーマットについては、「IPアドレスユーザ情報ファイルのフォーマット」(394ページ)を参照してください。

注意: -encodingオプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ IP アドレスユーザの追加 [-add]

```
amsip -add ファイル名 -encoding EUC|SJIS|UTF8
```

指定したファイルに記述されているIPアドレスユーザを一括で追加します。
所属するグループが存在しない場合には、上位グループを含めて新規に作成します。新規作成されるグループの設定は、管理画面から新規作成された場合と同じになります。

■ IP アドレスユーザの削除 [-del]

```
amsip -del ファイル名 -encoding EUC|SJIS|UTF8
```

指定したファイルに記述されているIPアドレスユーザを一括で削除します。
グループ名とユーザ名の組でユーザを特定し、両方が一致した場合だけ削除します。

■ IP アドレスユーザの変更 [-mod]

```
amsip -mod ファイル名 -encoding EUC|SJIS|UTF8
```

指定したファイルに記述されているIPアドレスユーザの設定を一括で変更します。
グループ名と開始IPアドレスでユーザを特定し、両方が一致した場合だけ変更します。

■ IP アドレスユーザの出力 [-export]

```
amsip -export ファイル名 [-g グループ記述ファイル名 ] -encoding EUC|SJIS|UTF8
```

登録されているIPアドレスユーザ情報をファイルに出力します。

注意:
- -g オプションを追加してグループ記述ファイルを指定すると、グループ記述ファイルに記述されたグループだけをエクスポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

■ IP アドレスユーザ情報ファイルのフォーマット

amsipコマンドで入出力するIPアドレスユーザ情報ファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	開始IPアドレス	終了IPアドレス	個別ルール

- 出力例

"ネットスター¥営業",	"192.168.1.10",	"192.168.1.25",	"ルール個別適用"

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3 階層」のように、「¥」または「\」(バックスラッシュ) で区切って入力します。
開始IPアドレス	IPアドレスを範囲指定する場合、開始とするIPアドレスを入力します。
終了IPアドレス	IPアドレスを範囲指定する場合、終了とするIPアドレスを入力します。 単一のIPアドレスを指定する場合、入力する必要はありません。
個別ルール	アカウントに個別ルールが適用されている場合、" ルール個別適用"と出力されます。値の設定はできません。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- フィールドは"データ"のように"(ダブルクオーテーション)で囲み、フィールド同士は,(半角カンマ)で区切ります。
- データのないフィールドは空になりますが、フィールドは省略しないでください。フィールドを省略すると、正しく読み込むことができなくなります。
- IPアドレスを範囲指定する場合には、「終了IPアドレス」よりも「開始IPアドレス」の値の方が小さくなるように設定してください。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

追加・削除・変更でフォーマットが違うなど、処理できない行が記述されていた場合には、それらをログファイルに出力します(行エラー)。正常な行については処理が行われます。
プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsipコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-6. amsgroup[グループ管理]

amsgroupは、グループの追加、削除、変更、出力をするコマンドです。
対象とするユーザは、ユーザ情報が記述されたファイル(CSV形式)を参照します。
ファイルのフォーマットについては、「スケジュール情報ファイルのフォーマット」(409ページ)を参照してください。

注意: -encodingオプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ グループの追加 [-add]

```
amsgroup -add ファイル名 -encoding [EUC|SJIS|UTF8]
```

指定されたファイルに記述されているグループを追加します。
上位グループが存在しない場合には作成されます。その場合の上位グループの設定は、管理画面から新規にグループを作成された場合と同じです。

■ グループの追加（大量データ登録）[-massadd]

```
amsgroup -massadd ファイル名 -encoding [EUC|SJIS|UTF8]
```

機能は-addオプションと同様です。大量のデータを登録する場合に指定します。

注意: 他のユーザが管理画面またはコマンドラインインタフェースを使用している状態では使用しないでください。競合により設定ファイルが破損する可能性があります。

■ グループの削除 [-del]

```
amsgroup -del ファイル名 -encoding [EUC|SJIS|UTF8]
```

指定されたファイルに記述されているグループ名のグループを削除します。
削除されたグループにユーザ、ルール、スケジュールが存在する場合には、同時に削除されます。
また、下位グループが存在する場合にも同様に削除されます。

■ グループの変更 [-mod]

```
amsgroup -mod ファイル名 -encoding [EUC|SJIS|UTF8]
```

指定したファイルに記述されているグループの設定を一括で変更します。
グループが存在しない場合にはエラーとなります。

■ グループの出力 [-export]

```
amsgroup -export ファイル名 -encoding [EUC|SJIS|UTF8]
```

-exportオプションを使用すると、指定されたファイルに登録済みのグループをエクスポートします。

■ グループ情報ファイルのフォーマット

amsgroupコマンドで読み込むファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	コメント	グループID	上位グループ参照フラグ	下位グループ強制適用フラグ	カテゴリ設定制限基準カテゴリルール名
例外URL適用フラグ	HTTPSデコードフラグ	上位プロキシ使用フラグ	上位HTTPプロキシ	上位HTTPSプロキシ	上位FTPoverHTTPプロキシ

- 出力例

"ネットスター¥開発",	"コメント",	"グループID",	"0",	"0",	"ネットスター¥開発¥ルール1",
"0",	"0",	"0",	"",	"",	""

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
コメント	グループコメントを入力します。 グループコメントが不要な場合、省略できます。
グループID	グループのエクスポート時にグループIDが出力されます。 グループ ID は閲覧のみ可能です。追加および変更はできません。
上位グループ参照フラグ	0:参照しない　1:参照する
下位グループ強制適用フラグ	0:適用しない　1:適用
カテゴリ設定制限基準カテゴリルール名	"グループ1¥グループ2¥ルール1"のように"¥"で区切ってルールおよび所属グループまで階層的に指定します。
例外URL適用フラグ	0:下位へ適用しない　1:下位へ適用
HTTPSデコードフラグ	0:無効　1:有効
上位プロキシ使用フラグ	0:システム設定に従う 1:上位グループの設定に従う 2:グループ設定の上位プロキシを使用
上位HTTPプロキシ	IPアドレスにはIPv6が指定できます。

フィールド名	設定内容
上位HTTPSプロキシ	IPアドレスにはIPv6が指定できます。
上位FTPoverHTTPプロキシ	IPアドレスにはIPv6が指定できます。

注意:
- ファイルの1行目にはフィールド名を入力したヘッダが必要です。
- フィールドは「"データ"」のように「"」(ダブルクオーテーション)で囲み、フィールド同士は「,」(半角カンマ)で区切ります。
- データのないフィールドは空になりますが、フィールドは省略しないでください。フィールドを省略すると、正しく読み込むことができなくなります。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ グループ名の指定

ISWM 管理画面上の表記	コマンドラインでの指定
ルートグループ	"ルートグループ"
未登録ユーザ	"未登録ユーザ"
ADMIN	"ADMIN"
LDAP	"LDAP"
ユーザ作成のグループ	例: "ネットスター¥開発¥PC"

■ エラー処理

amsgroup コマンドは、追加および削除時に処理できない行があった場合、行エラーとしてログファイルに出力します。
プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsgroupコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0

終了タイプ	終了コード (Windows)	終了コード (Linux)
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-7. amsurl[例外URL]

amsurlは、例外URLの入出力や登録/一括削除を行うコマンドです。
例外URLは、例外URL情報が記述されたファイル(CSV形式)を参照します。
ファイルのフォーマットについては、「例外URL情報ファイルのフォーマット」(402ページ)を参照してください。

注意: -encoding オプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ 例外 URL のエクスポート [-export]

```
amsurl -export ファイル名 [-g グループ記述ファイル名 ] -encoding EUC|SJIS|UTF8
```

-exportオプションを使用すると、登録されている例外URLを指定されたファイルにCSV形式でエクスポート(出力)します。

注意:
- -g オプションを追加してグループ記述ファイルを指定すると、例外 URL ファイルに記述されたグループの例外URLだけをエクスポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384　ページ)を参照してください。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

■ 例外 URL のインポート [-import]

```
amsurl -import ファイル名 [-g グループ記述ファイル名 | -all] -encoding EUC|SJIS|UTF8
```

-import オプションを使用すると、指定されたファイルに記述されている例外 URL をインポートします。

注意:
- 実行時には-gオプションまたは-allオプションのどちらかを必ず指定してください。
- -g オプションが指定されている場合には、そのグループ記述ファイルを読み込み、該当するグループの例外URLだけをインポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384　ページ)を参照してください。
- -allオプションが指定された場合には、すべてのグループを対象として例外URLをインポートします。

■ 例外 URL の登録 [-add]

```
amsurl -add ファイル名 [-g グループ記述ファイル名 | -all] -encoding EUC|SJIS|UTF8
```

-addオプションを使用すると、指定されたファイルに記述されている例外URLを登録します。

注意:
- 実行時には-gオプションまたは-allオプションのどちらかを必ず指定してください。
- -g オプションが指定されている場合には、グループ記述ファイルのグループであり、かつファイルに記述されたグループに例外URLを登録します。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- -all オプションが指定された場合には、ファイルに記載されたグループを対象として例外URLを登録します。
- 対象グループのフィルタリング設定が [上位グループ参照] である場合や、上位のグループで[下位グループ強制参照]が適用されている場合には登録されません。

■ 例外 URL の一括削除 [-clear]

```
amsurl -clear ファイル名 [-g グループ記述ファイル名 | -all] -encoding EUC|SJIS|UTF8
```

-clearオプションを使用すると、指定されたファイルに記述されている例外URLルールに登録された例外URLデータを一括削除します。

注意:
- 実行時には-gオプションまたは-allオプションのどちらかを必ず指定してください。
- -g オプションが指定されている場合には、グループ記述ファイルのグループであり、かつファイルに記述されたグループ/ルールの例外URLを全て削除します。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- -all オプションが指定された場合には、ファイルに記載されたグループ / ルールの例外URLを全て削除します。
- 対象グループのフィルタリング設定が [上位グループ参照] である場合や、上位のグループで[下位グループ強制参照]が適用されている場合には削除されません。

■ 例外 URL 情報ファイルのフォーマット

amsurlコマンドで読み込むファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	ルール名	メインカテゴリ名	サブカテゴリ名	例外URL	登録形式	有効期間(開始)	有効期間(終了)	コメント

- 出力形式

"ネットスター¥開発",	"例外ルール1",	"スポーツ",	"レジャー",	"http://sports.netstar.jp",	"0",	"20100801",	"20110731"	"コメント"

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
ルール名	例外URLルール名を入力します。
メインカテゴリ名	メインカテゴリ名を入力します。
サブカテゴリ名	サブカテゴリ名を入力します。
例外URL	例外URLを入力します。
登録形式	登録形式を入力します。 0:通常URL 1:IPアドレスレンジ指定URL 2:ワイルドカード指定URL 3:拡張ワイルドカード指定URL 4:ホスト名/IPアドレス
有効期間(開始)	YYYYMMDD形式で有効期間を設定します。 (YYYY:西暦、MM:月、DD:日)
有効期間(終了)	YYYYMMDD形式で有効期間を設定します。 (YYYY:西暦、MM:月、DD:日)
コメント	コメントを入力します。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- フィールド同士は「,」(半角カンマ)で区切ります。
- データのないフィールドは空になりますが、フィールドは省略しないでください。フィールドを省略すると、正しく読み込むことができなくなります。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

amsurl コマンドは、追加および削除時に処理できない行があった場合、行エラーとしてログファイルに出力します。
プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsurlコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-8. amscaterule[カテゴリルール管理]

amscaterule は、カテゴリルール追加、削除、変更、出力をするコマンドです。
対象とするルールは、ルール情報が記述されたファイル(CSV形式)を参照します。
ファイルのフォーマットについては、「カテゴリルールファイルのフォーマット」(405ページ)を参照してください。

注意: -encoding オプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ ルールの追加 [-create]

```
amscaterule -create ファイル名 [-allow] -encoding EUC|SJIS|UTF8
```

指定されたファイルに記述されたルールを追加します。
すべてのカテゴリが「規制」で、カテゴリ設定制限が「設定しない」に設定されたルールが新たに作成されます。-allowオプションを指定すると、すべてのカテゴリを「許可」にします。
-createオプションを指定した場合、グループ名とルール名を記述したファイルを指定します。

■ ルールの変更 [-mod]

```
amscaterule -mod ファイル名 -encoding EUC|SJIS|UTF8
```

指定されたファイルに記述されたルールの規制方法とカテゴリ設定制限を変更します。
グループ名、ルール名、メインカテゴリ名、サブカテゴリ名で特定される規制方法とカテゴリ設定制限を変更します。グループ内にすでにカテゴリ設定制限基準ルールがある場合は、カテゴリ設定制限は変更できません。

■ ルールの削除 [-del]

```
amscaterule -del ファイル名 -encoding EUC|SJIS|UTF8
```

指定されたファイルに記述されたルールを削除します。
ただし、他のグループで使用されているルールを削除することはできません。

■ ルールのエクスポート [-export]

```
amscaterule -export ファイル名 [-g グループ記述ファイル名 ] -encoding EUC|SJIS|UTF8
```

登録されているルールをファイルに出力します。

注意:
- -g オプションを追加してカテゴリルールファイルを指定すると、該当するグループのカテゴリルールだけをエクスポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。
- -gオプションがない場合、ルートグループ以下のすべてのルールが出力されます。

■ カテゴリルールファイルのフォーマット

amscaterule コマンドで読み込むファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	ルール名	メインカテゴリ名	サブカテゴリ名	規制内容

- 出力形式

"ネットスター¥開発",	"就業時間中",	"不法",	"違法と思われる行為",	"1"

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
ルール名	ルール名を入力します。
メインカテゴリ名	メインカテゴリ名を入力します。
サブカテゴリ名	サブカテゴリ名を入力します。「未分類(その他全て)」カテゴリの場合は、サブカテゴリ名は必要ありません。
規制内容	0:許可 11:規制 12:書き込み規制 21:規制＋一時許可/パスワードあり 22:書き込み規制＋一時許可/パスワードあり 31:規制＋一時許可/パスワードなし 32:書き込み規制＋一時許可/パスワードなし

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- フィールドは「"データ"」のように「"」(ダブルクオーテーション)で囲み、フィールド同士は「,」(半角カンマ)で区切ります。
- データのないフィールドは空になりますが、フィールドは省略しないでください。フィールドを省略すると、正しく読み込むことができなくなります。
- [共通アクセス管理]-[カテゴリ名設定]の[ユーザ設定サブカテゴリ名]で、「ユーザ設定」の名称を変更した場合、変更後の名称で登録する必要があります。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

新しいカテゴリルールを作成する場合、以下の手順で作成してください。

1. amscaterule -create で、指定したグループにカテゴリルールを追加します。
2. amscaterule -exportで、作成したカテゴリルールをファイルに出力します。
3. 出力したファイルを適宜修正します。
4. amscaterule -modで、カテゴリルールを変更します。

■ カテゴリルールの作成例

「ネットスター¥開発」グループに、新規ルール「就業時間中」を作成します。

1. 新規ルール追加用のルール情報ファイルを作成します。

   1 行目にフィールド名、2 行目にグループ、新規ルール名を入力します。

   ```
   グループ名 , ルール名 , メインカテゴリ名 , サブカテゴリ名 , 規制内容
   " ネットスター¥ 開発 "," 就業時間中 ",,,
   ```

2. 「amscaterule -create」を実行し、新規ルールを作成します。

   手順 1 で作成した新規ルール追加用のルール情報ファイル (addrule-group.txt) を指定します。

   ```
   amscaterule -create C:¥ISWM¥addrule-group.txt -encoding SJIS
   ```

   注意:
   - amscaterule -create で追加したルールの規制方法は、すべて 1(規制) に設定されます。
   - -allowオプションを使用した場合、規制方法はすべて0(許可)に設定されます。

3. 「amscaterule-export」を実行し、作成したカテゴリルールをファイルに出力します。

ここでは、「C:¥ISWM¥rule-dev.txt」に出力します。
「test-group.txt」はグループ記述ファイルです。

```
amscaterule -export C:¥ISWM¥rule-dev.txt -g C:¥ISWM¥test-group.txt -encoding SJIS
```

「rule-dev.txt」には、指定したグループに登録された、すべてのカテゴリルールが出力されます。

```
グループ名 , ルール名 , メインカテゴリ名 , サブカテゴリ名 , 規制内容
" ネットスター¥ 開発 "," 就業時間中 "," ユーザ設定 "," ユーザ設定１ ","1"
" ネットスター¥ 開発 "," 就業時間中 "," ユーザ設定 "," ユーザ設定２ ","1"
" ネットスター¥ 開発 "," 就業時間中 "," ユーザ設定 "," ユーザ設定３ ","1"
" ネットスター¥ 開発 "," 就業時間中 "," ユーザ設定 "," ユーザ設定４ ","1"
" ネットスター¥ 開発 "," 就業時間中 "," ユーザ設定 "," ユーザ設定５ ","1"
" ネットスター¥ 開発 "," 就業時間中 "," 不法 "," 違法と思われる行為 ","1"
・・・
```

4. 出力したファイルをテキストエディタなどで修正します。

カテゴリごとに規制方法を修正します。

5. 「amscaterule-mod」を実行し、カテゴリルールを変更します。

手順 4 で修正したファイルを指定して、カテゴリルールを変更します。

```
amscaterule -mod C:¥ISWM¥rule-dev.txt -encoding SJIS
```

■ エラー処理

amscaterule コマンドは、追加および削除時に処理できない行があった場合、行エラーとしてログファイルに出力します。
プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amscaterule コマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-9. amsschedule[スケジュール管理]

amsscheduleは、カテゴリルールのスケジュールの追加、削除、出力をするコマンドです。
対象とするスケジュールは、スケジュール情報が記述されたファイル(CSV形式)を参照します。
ファイルのフォーマットについては、「スケジュール情報ファイルのフォーマット」(409ページ)を参照してください。

注意: -encoding オプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ スケジュールの追加 [-add]

```
amsschedule -add ファイル名 -encoding EUC|SJIS|UTF8
```

指定されたCSVファイルに記述されたスケジュールを追加します。
同一スケジュール内に、指定された時間帯がすでに登録されていた場合にはエラーになります。

■ スケジュールの削除 [-del]

```
amsschedule -del ファイル名 -encoding EUC|SJIS|UTF8
```

指定されたCSVファイルに記述されたスケジュールを削除します。

■ スケジュールの変更 [-mod]

```
amsschedule -mod ファイル名 -encoding EUC|SJIS|UTF8
```

指定されたCSVファイルに記述されたスケジュールを変更します。
スケジュールのエクスポート[-export]で出力したCSVファイルを適宜修正して、スケジュールの変更[-mod]を実行してください。

注意:
- CSV ファイルには、同一スケジュール内に指定したい時間帯をすべて登録してください。登録されていない時間帯には、スケジュールの基本設定が適用されます。
- スケジュールの基本設定がファイルに設定されていない場合はエラーになります。

■ スケジュールのエクスポート [-export]

```
amsschedule -export ファイル名 [-g グループ記述ファイル名 ] -encoding EUC|SJIS|UTF8
```

指定されたファイルに設定済みのスケジュールを保存します。

注意:
- -g オプションを追加してスケジュールファイルを指定すると、該当するグループのスケジュールだけをエクスポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- エクスポートしたときに同じ名前のファイルが存在する場合、内容が上書きされます。

■ スケジュール情報ファイルのフォーマット

amsscheduleコマンドで読み込むファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	スケジュール名	ルール所有グループ	ルール名	基本設定スケジュール指定	曜日	開始時刻	終了時刻

- 出力形式

"ネットスター¥開発",	"会社",	"ネットスター¥開発",	"勤務時間外1",	"0",	"MON/TUE/WED/THU/FRI",	"18:00",	"24:00"

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
スケジュール名	スケジュール名を入力します。
ルール所有グループ	ルールが登録されているグループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
ルール名	ルール名を入力します。
基本設定スケジュール指定	基本設定スケジュールに指定する、指定しないを設定します。 基本設定スケジュールに指定した場合、「曜日」、「開始時間」、「終了時間」を設定する必要はありません。 0:基本設定スケジュールに指定しない 1:基本設定スケジュール設定に指定する
曜日	ルールを適用する曜日を設定します。 「SUN/MON/TUE/WED/THU/FRI/SAT」 適用する曜日を「/」で区切って指定します。 曜日を指定しない場合、省略できます。
開始時間	適用を開始する時間を24時間表記(08:30)で入力します。 10分単位で入力します。 適用時間の範囲を指定しない場合、省略できます。
終了時間	適用を終了する時間を24時間表記(22:00)で入力します。 10分単位で入力します。 適用時間の範囲を指定しない場合、省略できます。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- フィールドは「"データ"」のように「"」(ダブルクオーテーション)で囲み、フィールド同士は「,」(半角カンマ)で区切ります。
- データのないフィールドは空になりますが、フィールドは省略しないでください。フィールドを省略すると、正しく読み込むことができなくなります。
- 「開始時間」と「終了時間」は、開始時間の方が終了時間よりも早い時間に設定してください。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ スケジュール情報ファイル設定例

「ネットスター¥開発」グループに、次のスケジュール情報を追加する設定例を示します。

1. スケジュール「開発部用」に時間帯設定を追加します。

次の 4 種類の時間帯設定を追加します。

- 月～金の8:30～12:00
  「就業時間中」(「ネットスター¥開発」グループに登録されているルール)
- 月～金の12:00～13:00
  「休憩中」(「ネットスター」グループに登録されているルール)
- 月～金の13:00～17:30
  「就業時間中」(「ネットスター¥開発」グループに登録されているルール)
- 土、日の0:00～24:00
  「休日」(「ネットスター¥開発」グループに登録されているルール)

2. スケジュール「管理者用」を追加します。

```
グループ名 , スケジュール名 , ルール所有グループ , ルール名 , 基本設定スケジュール指定 , 曜日 , 開始時間 , 終了時間
" ネットスター¥ 開発 "," 開発部用 "," ネットスター\ 開発 "," 就業時間中 ","0","MON/TUE/WED/THU/FRI","08:30","12:00"
" ネットスター¥ 開発 "," 開発部用 "," ネットスター","," 休憩中 ","0","MON/TUE/WED/THU/FRI","12:00","13:00"
" ネットスター¥ 開発 "," 開発部用 "," ネットスター\ 開発 "," 就業時間中 ","0","MON/TUE/WED/THU/FRI","13:00","17:30"
" ネットスター¥ 開発 "," 開発部用 "," ネットスター\ 開発 "," 休日 ","0","SUN/SAT","00:00","24:00"
" ネットスター¥ 開発 "," 管理者用 "," ネットスター","," 管理者 ","1",,,
```

■ エラー処理

amsscheduleコマンドは、追加および削除時に処理できない行があった場合、行エラーとしてログファイルに出力します。
プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsscheduleコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-10. amsdatabase[URLデータベース管理]

amsdatabaseは、URLデータベースを管理するコマンドです。

■ URL データベースのダウンロード [-download]

```
amsdatabase -download -all|-target [ サーバ番号 ]
```

URLデータベースをダウンロードします。
-targetが指定されている場合には、そのサーバのみでダウンロードを実行します。-targetが指定されていない場合には、すべてのサーバでダウンロードが実行されます。

■ URL データベース情報の表示 [-info]

```
amsdatabase -info -all|-target [ サーバ番号 ]
```

URLデータベースの情報を表示します。
-targetが指定されている場合には、指定したサーバの情報のみを表示します。-targetが指定されていない場合には、すべてのサーバの情報を表示します。
サーバ名は、管理画面で設定された名称で表示されます。また、サーバ番号として( )内に内部的に割り振られたユニークなサーバ番号を表示します。プライマリサーバは常に0(ゼロ)で表示されます。

表示項目	説明
License key	ライセンスキー
Number of user	利用可能なユーザ数
Expiration date	ライセンスキーの有効期限
Update date	更新日
Database date	URLデータベース更新日付
Database version	URLデータベースバージョン

表示例)

```
レプリカサーバ３　（３）
License key       xxxxxxxx
Number of user    100
Expiration date   2009/10/31
Update date       2008/2/1
Database date     2008/2/1
Database version  061910
```

■ ダウンロード状況表示 [-status]

```
amsdatabase -status -all|-target [ サーバ番号 ]
```

URLデータベースのダウンロード状況を表示します。
-targetが指定されている場合には、そのサーバの情報のみを表示します。-targetが指定されていない場合には、すべてのサーバの情報を表示します。

注意: サーバ番号は、amsserverコマンドで確認できます。

表示例)

```
プライマリサーバ  (0)   Downloading
レプリカサーバ１  (1)   ----
レプリカサーバ２  (2)   ----
```

■ エラー処理

プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsdatabaseコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-11. amshttpsdectgt[HTTPSデコード対象ホスト管理]

amshttpsdectgtは、HTTPSデコード対象ホスト一覧の入出力をするコマンドです。
ホスト一覧は、ホスト情報が記述されたファイル(CSV形式)を参照します。
ファイルのフォーマットについては、「HTTPSデコード対象ホスト情報ファイルのフォーマット」(415ページ)を参照してください。

注意: -encoding オプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ HTTPS デコード対象ホスト一覧のエクスポート [-export]

```
amshttpsdectgt -export ファイル名 -encoding EUC|SJIS|UTF8
```

-exportオプションを使用すると、登録されているHTTPSデコード対象ホストを指定されたファイルにCSV形式でエクスポート(出力)します。

注意: エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

■ HTTPS デコード対象ホスト一覧のインポート [-import]

```
amshttpsdectgt -import ファイル名 -encoding EUC|SJIS|UTF8
```

-import オプションを使用すると、指定されたファイルに記述されている HTTPS デコード対象ホストをインポートします。

注意: 既存のHTTPSデコード対象ホストは削除されます。

■ HTTPS デコード対象ホスト情報ファイルのフォーマット

amshttpsdectgtコマンドで読み込むファイルは、次のフィールドで構成されます。

- フォーマット

```
ホスト名
```

- 出力形式

```
"www.update.microsoft.com"
```

フィールド名	設定内容
ホスト名	HTTPSデコード対象ホスト名を入力します。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

amshttpsdectgtコマンドは、追加および削除時に処理できない行があった場合、行エラーとしてログファイルに出力します。
プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amshttpsdectgtコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-12. amsldapgroup[LDAPグループ情報管理]

amsldapgroupは、LDAPグループ情報の入力を行うコマンドです。
LDAPグループ情報は、LDAPグループ情報が記述されたファイル(CSV形式)を参照します。
ファイルのフォーマットについては、「LDAPグループ情報ファイルのフォーマット」(416ページ)を参照してください。

注意: -encoding オプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。

■ LDAP グループ情報のインポート [-import]

```
amsldapgroup -import ファイル名 -encoding EUC|SJIS|UTF8
```

-importオプションを使用すると、指定されたファイルに記述されているLDAPグループ情報をインポートします。

注意: 既存のLDAPグループ情報は削除されます。

■ LDAP グループ情報ファイルのフォーマット

amsldapgroupコマンドで読み込むファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	属性名	属性値

- 出力形式

"GROUP1\SEC1"	"memberOf"	"CN=GroupA,DC=example,DC=com"

フィールド名	設定内容
グループ名	ユーザを取り込むグループ名を入力します。 上位グループが存在する場合、第1階層から「グループ1¥グループ2」のように、「¥」または「\」(バックスラッシュ) で区切って入力します。
属性名	抽出条件の属性名を入力します。
属性値	抽出条件の属性値を入力します。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- ファイルの上部に書かれているほど優先順位が高くなります。
- フィールドは「" データ "」のように「"」(ダブルクオーテーション) で囲み、フィールド同士は「,」(半角カンマ)で区切ります。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

amsldapgroup コマンドは、追加および削除時に処理できない行があった場合、行エラーとしてログファイルに出力します。
プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsldapgroupコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-13. amsdata[設定の保存/復旧/同期]

amsdataは、ISWMサーバの設定の保存、復旧、同期をするコマンドです。

■ 設定の保存 [-save]

```
amsdata -save ファイル名
```

グループ情報やフィルタリングルール、スケジュールなどの設定をファイルに保存します。

拡張子は自動的に付加され、システムで規定されたディレクトリに保存されます。

注意:
- 保存できるファイル数は最大で5つです。6つ以上の設定を保存することはできません。すでに5つの設定が保存されている場合は、不要な設定を削除した後で保存してください。また、同名のファイルを上書き保存することはできません。
- 設定の保存中は、管理画面およびコマンドラインからの操作は一切できません。

■ 設定の復旧 [-restore]

```
amsdata -restore ファイル名
```

ファイル名で指定された、あらかじめ保存されている設定情報により復旧します。

注意:
- 設定の復旧中は、管理画面およびコマンドラインからの操作は一切できません。
- コマンド実行後、プライマリサーバおよびレプリカサーバの管理サービス、拡張Webサービス、フィルタリングサービスを再起動してください。

■ 設定の一覧表示 [-list]

```
amsdata -list
```

保存したファイルの一覧を表示します。
表示例)

```
$ amsdata -list
20080410_default
data_060623
$
```

■ 設定の削除 [-del]

```
amsdata -del ファイル名
```

指定した設定を削除します。

■ 設定の同期 [-synchronize]

```
amsdata -synchronize [-target サーバ番号 ]
```

現在のプライマリサーバの設定を保存し、レプリカサーバに対して同期処理をします。
-targetが指定されている場合には、そのサーバに対してだけ同期を実行します。-targetが指定され

ていない場合は、すべてのサーバに対して同期を実行します。

注意:
- サーバ番号としてプライマリサーバ番号にあたる 0(ゼロ) を指定することはできません。
- 設定の同期中は、管理画面およびコマンドラインからの操作は一切できません。
- コマンド実行後、プライマリサーバおよびレプリカサーバの管理サービス、拡張Webサービス、フィルタリングサービスを再起動してください。

■ 設定の反映 [-reflection]

```
amsdata -reflection
```

管理するすべてのサーバのフィルタリングサービスに対して、現在の設定内容を反映します。
処理中は、管理画面およびコマンドラインからの操作は一切できません。

■ コマンドの再送 [-retry]

```
amsdata -retry
```

管理画面やコマンドラインからレプリカサーバの設定変更に失敗した場合、それ以降の設定変更をせず、設定内容を保存しています。
このコマンドを実行すると、保存されているコマンドを問題のあるレプリカサーバに再送し、同期を再試行します。

■ 設定ファイルの同期 [-sys]

```
amsdata -sys [-target サーバ番号 ]
```

proxy.infファイル、system.infファイルを同期します。
-targetが指定されている場合には、そのサーバに対してのみ同期を実行し、-targetが指定されていない場合には、すべてのサーバに対して同期を実行します。

注意: コマンド実行後、プライマリサーバおよびレプリカサーバの管理サービス、拡張 Webサービス、フィルタリングサービスを再起動してください。

■ 設定の再読み込み [-reload]

```
amsdata -reload
```

グループ情報やフィルタリングルール、スケジュール、proxy.infファイル、system.infファイルなどの設定を読み込み、再設定します。

このコマンドを実行すると、プライマリサーバおよびすべてのレプリカサーバで設定の再読み込みを実行します。

注意:
- proxy.inf ファイル、system.inf ファイルで、サービス起動時に読み込む項目は、コマンド実行時には反映されません。
- プライマリサーバとレプリカサーバ間の同期は行いません。

■ エラー処理

プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsdataコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-14. amsserver[サーバ情報表示]

amsserverは、サーバ情報を表示するコマンドです。

表示項目	説明
サーバ番号	プライマリサーバ、レプリカサーバに割り振られたユニークなサーバ番号を表示します。プライマリサーバは常に 0(ゼロ) で表示されます。
サーバ名	管理画面で設定されたサーバ名を表示します。プライマリサーバの場合、サーバ名の末尾に(Master)と表示されます。
ビルド番号	ISWMのビルド番号を表示します。
IPアドレス	サーバのIPアドレスを表示します。
同期状態	プライマリサーバと同期中: synchronized プライマリサーバとの同期に失敗: failed

表示項目	説明
フィルタリングサーバの動作状態	動作中:running 起動中:starting 再起動中:restarting 停止中:stopping 停止:stop

表示例)

```
0 プライマリサーバ (Master) build1601 192.168.60.1 ---- running
1 レプリカサーバ１ 192.168.60.2 failed starting
2 レプリカサーバ２ 192.168.60.3 failed running
3 レプリカサーバ３ 192.168.60.4 failed running
4 レプリカサーバ３ 192.168.60.5 failed stop
```

■ エラー処理

プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsserverコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-15. amslog[ログファイルのアーカイブ]

amslogは、ログファイルの設定をするコマンドです。

注意: amslog コマンドはレプリカサーバでも実行できます。ただし、-list オプションはプライマリサーバのみ実行可能です。

■ ログファイルのローテーション [-rotation]

```
amslog -rotation
```

ログのローテーションを強制的に実行します。この場合、ログのローテーションは、コマンドを実行したサーバだけを対象とします。

■ ログファイルの一覧表示 [-list]

```
amslog -list [-target サーバ番号 ] [-sys] [-ac [ グループ記述ファイル名 -encoding EUC|SJIS|UTF8]]
```

ローテーションされたログファイルの一覧を表示します。
オプションの組み合わせにより、表示されるログファイルの種類が異なります。
表示例)

```
プライマリサーバ , httpXXX.log, XX Mbyte, 2008/01/17
サーバ１ ,httpXXX.log, XX Mbyte, 2008/01/17
サーバ２ , httpXXX.log,XX Mbyte, 2008/01/17
```

注意: -listオプションはプライマリサーバだけが実行できます。

- -target オプションを指定した場合
  実行例
  - amslog -list -target 0

  指定したサーバ番号のサーバに保存されているローテーション済みログファイルを表示します。
  サーバ番号は「amsserver」コマンドで確認できます。
- -sys オプションを指定した場合
  実行例
  - amslog -list -sys
  - amslog -list -target 0 -sys

  システムログ一覧を表示します。
- -ac オプションを指定した場合
  実行例
  - amslog -list -ac
  - amslog -list -target 0 -ac
  - amslog -list -target 0 -ac C:¥ISWM¥group.txt -encoding SJIS

  アクセスログ一覧を表示します。第1階層グループを指定して一覧を表示したい場合、-acオプションの後にグループ記述ファイルおよび文字コードを指定します。
  -acオプションの後にグループ記述ファイル名の指定がない場合、"システム一括"のログファ

イル一覧が表示されます。

注意:
- -encoding オプションはファイルの文字コードを指定します。エンコード形式の指定が間違っていると正しくファイルを読み込むことができませんので、注意してください。文字コードは、EUC、Shift-JIS、UTF-8から選択します。
- "システム一括"とは、ログ出力単位が"システム一括"またはユーザ認証をしない場合に出力されるログファイルです。

- -sys オプション、-ac オプションの両方を指定した場合、または両方指定しない場合
  実行例
  - amslog -list
  - amslog -list -sys -ac
  - amslog -list -target 0 -sys -ac
  - amslog -list -target 0 -sys -ac C:¥ISWM¥group.txt -encoding SJIS

システムログ、アクセスログの両方を一覧表示します。

■ ログの出力レベルの変更 [-level]

```
amslog -level [FATAL|ERROR|WARN|INFO|DEBUG] -process [FILTERING]
```

ログの出力レベルを変更します。レベル指定またはプロセス指定がない場合はエラーとして処理を中断します。
ログの出力レベルの変更は、コマンドを実行したサーバだけを対象とします。

-processオプションを指定した場合は、指定したプロセスの出力レベルのみ変更されます。
「FILTERING」を指定した場合、ログの出力レベルが変更されるログファイルは proxy.log と filtering.logとなります。

注意: コマンドの実行によって、プライマリサーバやレプリカサーバで動作している対象プロセスのログの出力レベルが変更されますが、再起動した時点で変更前の設定に戻ります。

■ エラー処理

プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amslogコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-16. amscatemsg[カテゴリ別規制メッセージ管理]

amscatemsgはカテゴリ別の規制メッセージを変更/出力するコマンドです。
対象とするメッセージは、グループ名、メインカテゴリ名、規制メッセージが記述されたファイル(CSVファイル形式)を参照します。
ファイルのフォーマットについては、「カテゴリ別規制メッセージファイルのフォーマット」(425 ページ)を参照してください。

■ カテゴリ別規制メッセージの設定変更 [-mod]

```
amscatemsg -mod ファイル名 -encoding EUC|SJIS|UTF8
```

-mod オプションを使用すると、指定されたファイルに記述されているカテゴリ別規制メッセージを一括で変更します。

■ カテゴリ別規制メッセージの出力 [-export]

```
amscatemsg -export ファイル名 [-g グループ記述ファイル名 ] -encoding EUC|SJIS|UTF8
```

-exportオプションを使用すると、登録されているカテゴリ別規制メッセージを指定されたファイルにCSV形式で出力します。

注意:
- -g オプションを追加してグループ記述ファイルを指定すると、グループ記述ファイルに記述されたグループのカテゴリ別規制メッセージだけをエクスポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

■ カテゴリ別規制メッセージファイルのフォーマット

amscatemsgコマンドで入出力するカテゴリ別規制メッセージファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	ルール名	メインカテゴリ名	サブカテゴリ名	規制メッセージ

- 出力形式

"ネットスター¥開発",	"規制画面ルール1",	"アダルト",	"アダルト検索・リンク集",	"閲覧できません"

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
ルール名	規制画面のルール名を入力します。
メインカテゴリ名	メインカテゴリ名を入力します。
サブカテゴリ名	サブカテゴリ名を入力します。
規制メッセージ	規制メッセージを入力します。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

読み込んだファイルに処理できない行が存在した場合、処理できなかった行の内容がログファイルに出力されます。また、プライマリサーバやレプリカサーバの通信エラーや、その他のエラーについてもログファイルに出力されます。ログファイルについては、「A-2. amserror.logについて」(385ページ)を参照してください。

■ 終了コード

amscatemsgコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-17. amscontrol[フィルタリングサービスの起動/停止]

amscontrolは、フィルタリングサービスの起動、停止、再起動を実行するコマンドです。
-targetオプションを指定した場合、サーバ番号で指定されたISWMのフィルタリングサービスを起動します。対象を指定しなかった場合は、コマンドを実行しているサーバのフィルタリングサービスを起動します。
-allオプションを指定した場合、すべてのISWMサーバのフィルタリングサービスを起動します。

注意: amscontrolコマンドはレプリカサーバでも実行できます。ただし、-targetオプションはプライマリサーバのみ実行できます。

■ フィルタリングサービスの起動 [-start]

```
amscontrol -start -all | -target [ サーバ番号 ]
```

フィルタリングサービスを起動します。

■ フィルタリングサービスの停止 [-stop]

```
amscontrol -stop -all | -target [ サーバ番号 ]
```

フィルタリングサービスを停止します。

■ フィルタリングサービスの再起動 [-restart]

```
amscontrol -restart -all | -target [ サーバ番号 ]
```

フィルタリングサービスを再起動します。

■ エラー処理

プライマリサーバとレプリカサーバの通信エラーや､その他のエラーが起きた場合は､amserror.logに出力します。

■ 終了コード

amscontrolコマンドは終了時に､次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-18. amsadminstat[レプリカサーバの状態管理]

amsadminstatは､レプリカサーバの状態表示､初期化をするコマンドです。

■ レプリカサーバの状態表示 [-status]

```
amsadminstat -status
```

コマンドを実行したレプリカサーバが特定のプライマリサーバと連携されているかを表示します。
このコマンドはレプリカサーバの管理サービス上でのみ実行可能です。

表示項目	説明
サーバ番号	レプリカサーバに割り振られたユニークなサーバ番号を表示します。 プライマリサーバと連携されていない場合は-1と表示されます。
プライマリサーバのIPアドレス	連携しているプライマリサーバのIPアドレスが表示されます。 プライマリサーバと連携が行われていない場合はunknownと表示されます。

表示項目	説明
プライマリサーバとの連携状態	standalone: 新規インストールされた後、プライマリサーバの管理サービスから登録されていない状態 updated: アップデートインストールされた後、プライマリサーバの管理サービスから登録されていない状態 managed: プライマリサーバの管理サービスに登録されて連携している状態

表示例1)

```
-1, unknown, standalone
```

表示例2)

```
3, 192.168.60.188, managed
```

■ プライマリサーバとの連携を初期化 [-reset]

```
amsadminstat -reset
```

プライマリサーバとの連携を初期化します。
プライマリサーバとの連携を初期化したレプリカサーバは、amsadminstat -status コマンドを実行して表示されるプライマリサーバとの連携状態が「managed」から「standalone」へ変わります。
プライマリサーバとの連携中は、他のプライマリサーバからのリクエストを無視します。連携が解除されると、新しいプライマリサーバとの連携のためリクエストを待ちます。

注意:
- このコマンドはプライマリサーバとの連携状態が「managed」である場合のみ実行可能です。
- プライマリサーバとの連携を初期化して、サービスの状態が「managed」から「standalone」になった場合、レプリカサーバ側で「managed」の状態にすることはできません。
  もう一度プライマリサーバで管理対象のレプリカサーバを追加してください。

■ エラー処理

プライマリサーバとレプリカサーバの通信エラーや、その他のエラーが起きた場合は、amserror.logに出力します。

■ 終了コード

amsadminstatコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-19. amscatepostsize[カテゴリ別書き込み規制サイズ]

amscatepostsizeはカテゴリ別書き込み規制サイズ(グループ用)を変更/出力するコマンドです。
書き込み規制サイズの設定は、グループ名、メインカテゴリ名、サブカテゴリ名、規制サイズが記述されたファイル(CSVファイル形式)を参照します。
ファイルのフォーマットについては、「カテゴリ別規制サイズ設定ファイルのフォーマット」(431 ページ)を参照してください。

■ カテゴリ別書き込み規制サイズの設定変更 [-mod]

```
amscatepostsize -mod ファイル名 -encoding EUC|SJIS|UTF8
```

-mod オプションを使用すると、指定されたファイルに記述されているカテゴリ別書き込み規制サイズを一括で変更します。

■ カテゴリ別書き込み規制サイズの出力 [-export]

```
amscatepostsize -export ファイル名 [-g グループ記述ファイル名 ] -encoding EUC|SJIS|UTF8
```

-export オプションを使用すると、登録されているカテゴリ別書き込み規制サイズを指定されたファイルにCSV形式で出力します。

注意:
- -g オプションを追加してグループ記述ファイルを指定すると、グループ記述ファイルに記述されたグループのカテゴリ別書き込み規制サイズだけをエクスポートします。
- グループ記述ファイルについては、「グループ記述ファイル」(384 ページ)を参照してください。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

■ カテゴリ別規制サイズ設定ファイルのフォーマット

amscatepostsize コマンドで入出力するカテゴリ別書き込み規制サイズの設定ファイルは、次のフィールドで構成されます。

- フォーマット

グループ名	ルール名	メインカテゴリ名	サブカテゴリ名	書き込み規制サイズ

- 出力形式

"ネットスター¥開発",	"規制オプションルール1",	"金融",	"投資商品の購入",	"100"

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
ルール名	ルール名を入力します。
メインカテゴリ名	メインカテゴリ名を入力します。
サブカテゴリ名	サブカテゴリ名を入力します。「未分類(その他全て)」カテゴリの場合は、サブカテゴリ名は必要ありません。
書き込み規制サイズ	書き込み規制サイズを入力します。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

読み込んだファイルに処理できない行が存在した場合、処理できなかった行の内容がログファイルに出力されます。また、プライマリサーバやレプリカサーバの通信エラーや、その他のエラーについてもログファイルに出力されます。ログファイルについては、「A-2. amserror.logについて」(385ページ)を参照してください。

■ 終了コード

amscatepostsizeコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-20. amsgruleflg[ルール適用（グループ）管理]

グループに対して指定されたファイルに記述されているルール適用を管理します。

■ グループに対するルールの変更 [-mod]

```
amsgruleflg -mod ファイル名 -encoding EUC|SJIS|UTF8
```

グループに対して指定されたファイルに記述されているルール適用を設定します。

■ グループに対するルールの出力 [-export]

```
amsgruleflg -export ファイル名 [-g グループ記述ファイル ] -encoding EUC|SJIS|UTF8
```

設定されているグループのルール適用情報をファイルに出力します。

注意:
- -g オプションが指定されている場合には、そのファイルを読み込み該当するグループの情報だけをエクスポートします。
- -g オプションが指定されていない、または -g オプションの後ろにファイル名が指定されていない場合には、すべてのグループの情報をエクスポートします。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

■ グループに対するルールのフォーマット

amsgruleflgコマンドで管理するルールは、次のフィールドで構成されます。

- フォーマット

グループ名	カテゴリルール所有グループ名	カテゴリルール名	スケジュール所有グループ名	スケジュール名	規制画面ルール所有グループ名
規制画面ルール名	規制オプションルール所有グループ名	規制オプションルール名	例外URLルール所有グループ名	例外URLルール名	

- 出力例

"ネットスター¥開発",	"カテゴリルール所有グループ名",	"カテゴリルール1",	"スケジュール所有グループ名",	"スケジュール1",	"規制画面ルール所有グループ名",
"規制画面ルール1",	"規制オプションルール所有グループ名",	"規制オプションルール1",	"例外URLルール所有グループ名",	"例外URLルール1"	

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
カテゴリルール所有グループ名	カテゴリルールを所有するグループ名を入力します。
カテゴリルール名	カテゴリルール名を入力します。
スケジュール所有グループ名	スケジュールルールを所有するグループ名を入力します。
スケジュール名	スケジュール名を入力します。
規制画面ルール所有グループ名	規制画面ルールを所有するグループ名を入力します。
規制画面ルール名	規制画面ルール名を入力します。
規制オプションルール所有グループ名	規制オプションルールを所有するグループ名を入力します。
規制オプションルール名	規制オプションルール名を入力します。
例外URLルール所有グループ名	例外URLルールを所有するグループ名を入力します。
例外URLルール名	例外 URL ルール名を入力します。最大 10 ルール設定が可能です。複数の例外 URL ルールを設定する場合は、グループ名とルール名を繰り返し設定します。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- カテゴリとスケジュールはどちらか片方が設定可能、両方ルール名が設定されていた場合はカテゴリが設定されます。
- ルール名を設定する場合は必ずルールを所有するグループ名を設定してください。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

読み込んだファイルに処理できない行が存在した場合、処理できなかった行の内容がログファイルに出力されます。また、プライマリサーバやレプリカサーバの通信エラーや、その他のエラーについてもログファイルに出力されます。ログファイルについては、「A-2. amserror.logについて」(385ページ)を参照してください。

■ 終了コード

amsgruleflgコマンド終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-21. amsuruleflg[ルール適用（ユーザ）管理]

ユーザに対して指定されたファイルに記述されているルール適用を管理します。

■ ユーザに対するルールの変更 [-mod]

```
amsuruleflg -mod ファイル名 -encoding EUC|SJIS|UTF8
```

ユーザに対して指定されたファイルに記述されているルール適用を設定します。

■ ユーザに対するルールの出力 [-export]

```
amsuruleflg -export ファイル名 [-g グループ記述ファイル ] -encoding EUC|SJIS|UTF8
```

設定されているユーザのルール適用情報をファイルに出力します。

注意:
- -gオプションが指定されている場合には、そのファイルを読み込み該当するグループの情報だけをエクスポートします。
- -g オプションが指定されていない、または -g オプションの後ろにファイル名が指定されていない場合には、すべてのグループの情報をエクスポートします。
- エクスポート時に同じ名前のファイルが存在する場合は、内容が上書きされます。

■ ユーザに対するルールのフォーマット

amsuruleflgコマンドで管理するルールは、次のフィールドで構成されます。

- フォーマット

グループ名	アカウント名	開始IPアドレス	終了IPアドレス	カテゴリルール所有グループ名
カテゴリルール名	スケジュール所有グループ名	スケジュール名	規制オプションルール所有グループ名	規制オプションルール名

- 出力例

"ネットスター¥開発",	"user1",	"192.168.10.10",	"192.168.10.12",	"カテゴリルール所有グループ名",
"カテゴリルール1",	"スケジュール所有グループ名",	"スケジュールルール1",	"規制オプションルール所有グループ名",	"規制オプションルール1"

フィールド名	設定内容
グループ名	グループ名を入力します。 上位グループが存在する場合、第1階層から「第1階層¥第2階層¥第3階層」のように、「¥」または「\」(バックスラッシュ)で区切って入力します。
アカウント名	アカウント名を入力します。
開始IPアドレス	開始IPアドレスを入力します。
終了IPアドレス	終了IPアドレスを入力します。
カテゴリルール所有グループ名	カテゴリルールを所有するグループ名を入力します。
カテゴリルール名	カテゴリルール名を入力します。
スケジュール所有グループ名	スケジュールルールを所有するグループ名を入力します。
スケジュール名	スケジュール名を入力します。
規制オプションルール所有グループ名	規制オプションルールを所有するグループ名を入力します。
規制オプションルール名	規制オプションルール名を入力します。

注意:
- ファイルの1行目には各項目の名称を入力したヘッダが必要です。
- アカウント名と開始 IP アドレスの両方が設定されている場合はアカウント名として処理されます。
- カテゴリとスケジュールはどちらか片方が設定可能、両方ルール名が設定されていた場合はカテゴリを設定します。
- 単独のIPアドレスの場合には、開始IPアドレスだけで、終了IPアドレスの指定はありません。
- ルール名を設定する場合は必ずルールを所有するグループ名を設定します。
- 不正なフォーマットのファイルを用いた場合、誤った内容が登録されることがあります。

■ エラー処理

読み込んだファイルに処理できない行が存在した場合、処理できなかった行の内容がログファイルに出力されます。また、プライマリサーバやレプリカサーバの通信エラーや、その他のエラーについてもログファイルに出力されます。ログファイルについては、「A-2. amserror.logについて」(385ページ)を参照してください。

■ 終了コード

amsuruleflgコマンド終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
行エラー	-1	255
内部エラー	-2	254
受付拒否	-9	247

A-22. amstune[サーバのチューニング]

amstuneは、サーバのチューニングを行うコマンドです。

■ サーバのパラメータ表示 [--status または -s]

```
amstune --status
```

実行したOSに設定がない場合には、パラメータ値は空白で表示されます。

※OSによって設定するパラメータが異なります。

カラム	説明
パラメータ名	OSのパラメータ名
パラメータ値	OSのパラメータ値(範囲指定の場合にはスペースで区切る)

Windows 版の出力例

```
MaxUserPort=5000
TcpTimedWaitDelay=64
```

Linux 版の出力例

```
ip_local_port_range=1024 49000
tcp_fin_timeout=50
tcp_tw_reuse=1
```

■ 最適化設定 [--level または -l]

```
amstune --level original|medium|high|extra
```

サーバのチューニングを行います。チューニングレベルを選択します。
original : 初回起動時のパラメータ値に戻します
medium : 緩やかなパフォーマンス向上を想定したパラメータチューニングを実施します
high : 高性能なパフォーマンスを想定したパラメータチューニングを実施します
extra : さらに高性能なパフォーマンスを想定したパラメータチューニングを実施します
(Linux版のみ対応します)

《オプション設定時の各パラメータの値》

		original	medium	high	extra
Windows	MaxUserPort	OS の デフォルト値	35000	65534	-
	TcpTimedWaitDelay		100	30	-
Linux	ip_local_port_range	OS の デフォルト値	16384-61000	1025-65535	1025-65535
	tcp_fin_timeout		45	30	30
	tcp_tw_reuse		-	-	1

※「original」を指定した場合は、OS再起動後に設定が反映されます。

■ エラー処理

amstuneコマンドは、エラー種別に対応したメッセージをログファイルに出力します。

■ 終了コード

amstuneコマンドは終了時に、次の終了コードを出力します。

終了タイプ	終了コード (Windows)	終了コード (Linux)
正常終了	0	0
内部エラー	1	1

A-23. amsversion[バージョン情報表示]

amsversionは、バージョン情報を表示するコマンドです。

表示項目	説明
ビルド番号	ISWMのビルド番号を表示します。
リビジョン番号	ISWMのリビジョン番号を表示します。

B. 設定ファイル

ほとんどの設定値は管理画面から設定できますが、一部特殊な設定については、設定ファイルを直接編集して変更する必要があります。
設定ファイルは、テキストファイルとなっており、UTF-8コードに対応したエディタ(Windowsのメモ帳など)で編集することができます。

B-1. 設定ファイル編集時の注意

- 管理画面を終了させてください。
- ISWM サービスを停止してください。ISWM サービスの停止方法については、「6. ISWM の起動と停止」(28 ページ)を参照してください。
- 英数字と記号が使用できます。また、一部日本語が使用できる箇所があります。改行やタブ記号などの特殊記号は使用できません。

B-2. 設定ファイルの種類と格納先

ISWMの設定ファイルには、以下のファイルがあります。

■ proxy.inf

システム情報を定義するUTF-8形式のテキストファイルです。
以下のフォルダ/ディレクトリに保存されます。

Windows の場合

<インストールフォルダ>¥conf¥

Linux の場合

<インストールディレクトリ>/conf/

注意: proxy.infを変更した場合は、amsdata-sysコマンドを実行して変更を反映してください。コマンドの実行後、プライマリサーバおよびレプリカサーバの管理サービス、拡張Webサービス、フィルタリングサービスを再起動してください。

■cal.inf

指定した日付に、そのグループが設定している曜日のルールを適用する設定を保持するファイルです。
以下のフォルダ/ディレクトリに保存されます。

Windows の場合

<インストールフォルダ>¥conf¥

Linux の場合

<インストールディレクトリ>/conf/

注意: cal.infを変更した場合は、amscontrol -restartコマンドを実行して、フィルタリングサービスを再起動してください。
レプリカサーバを運用している環境でcal.infを変更した場合は、amsdata -synchronizeコマンドを実行してレプリカサーバとの同期を実行してください。同期終了後、amscontrol -restart -allコマンドを実行して、すべてのレプリカサーバのフィルタリングサービスを再起動してください。

B-3. proxy.inf

proxy.infの設定項目について説明します。キーの「=(数値)」は初期値を表します。

■[SYSTEM_GLOBAL]

MASTER_ADMIN_HOST=127.0.0.1	• プライマリサーバの管理サービスが起動している IP/ ホスト名。管理画面またはコマンドラインからリクエストを送信する接続先として指定する。 • レプリカサーバに通知するプライマリサーバの IP アドレス名。IPアドレスを変更した場合は、すでに追加済みのレプリカサーバと通信できなくなります。この値には必ず有効なIPアドレスを入力すること。
WWW_ADMIN_PORT=2319	管理画面の待ち受けポート番号。
MAX_DATA_SYNC_THREAD=10	プライマリサーバの管理サービスからレプリカサーバの管理サービスへのデータ同期を実行する最大スレッド数。 この値が実際のレプリカサーバの数よりも少ない場合は、すべてのサーバの同期が完了するまでにタイムラグが発生する。逆に多く設定すると使用メモリを圧迫する可能性がある。 管理画面では設定不可。
DATA_SYNC_TIMEOUT=30000	プライマリサーバの管理サービスからレプリカサーバの管理サービスへのデータ同期実行時のSocketタイムアウト設定。 単位はミリ秒で設定する。管理画面では設定不可。
MAX_JVHEAP=256	プロキシまたはコントロールサーバが使用するJava最大ヒープメモリサイズ。16Mバイトから設定可能。
EFFECTIVE_USER=iswm	ファイルのオーナー、実行ユーザを設定する (Windows 版では初期値が空欄)。
EFFECTIVE_GROUP=iswm	ファイルのグループ、実行グループを設定する (Windows 版では初期値が空欄)。
CACHE_PORT=5963	NsLaptor 通信用ポート番号。各プロセスはこのポート番号を用いてNsLaptorへの接続を行う。

■[CONNECTION_CFG]

BUFF=2048 (スタンドアロン版)	スタンドアロン版のみの設定項目。 Webサーバとの通信時、一度に取得するデータの最大サイズを設定する。 1024バイト～65535バイトまで設定可能。 大きいサイズを設定した場合、大きいサイズのファイルをリクエストしたときに、データが細かく切れずに受信できる。ただし、1コネクションでデータ受信するメモリの使用量が増加する。 小さいサイズを設定した場合、大きいサイズのファイルをリクエストしたときに、データを細かく切って受信する。ただし、1コネクションでデータ受信するメモリの使用量を減らすことができる。
BACKLOG=128	受信ポートの受信待ち行列最大数。 管理画面では設定不可。
CONNECT_KEEPALIVE=ALL (スタンドアロン版)	スタンドアロン版のみの設定項目。 持続接続要求に対して以下の3つの値を設定する。 不正な値の場合はALLとして動作する。 ALL: クライアント - プロキシ間、プロキシ - 上位サーバ間とも持続接続する。 CLIENT: クライアント - プロキシ間のみ持続接続を行い、上位サーバに対しては毎回新しい接続を行う。 NONE: クライアント - プロキシ間、プロキシ - 上位サーバ間とも持続接続を行わない。
SERVER_TIMEOUT=60000 (スタンドアロン版)	スタンドアロン版のみの設定項目。 proxyにおける上位サーバ(上位プロキシサーバまたはWWWサーバ)との接続保持時間。 1ミリ秒～9,999,999ミリ秒まで設定可能。 持続接続時に上位サーバからの read 待ち時間を制限することによって、持続接続の終了が通知されていないにもかかわらず、データの転送が行われていない際に通信を切断できる。 サーバによってはConnection:closeを明示的に返さないままデータの転送を終える場合があるので、ここで設定されている値を超える時間の間通信がない場合は、proxyが接続を切断できる。 パフォーマンスチューニングの際に編集する。

CLIENT_TIMEOUT=60000 **(スタンドアロン版)**	スタンドアロン版のみの設定項目。 proxyにおけるクライアント(Webブラウザ)との接続保持時間。 1ミリ秒～9,999,999ミリ秒まで設定可能。 持続接続時にクライアントからのread待ち時間を制限することによって、持続接続の終了が通知されていないにもかかわらず、データの転送が行われていない際に通信を切断できる。 クライアントからのリクエスト受信を待機しているにもかかわらず、データの転送が行われない場合があるので、ここで設定されている値を超える時間の間通信が行われない場合、proxyが接続を切断できる。 パフォーマンスチューニングの際に編集する。

REQUESTMODE=1	リクエスト先(Webサーバ、上位プロキシ、ICAPクライアント)へのリクエストヘッダ情報の送信有無を設定する。 HTTPS デコード中のヘッダ追加については本設定では動作せず、別途DECODE_ADD_HEADERで設定する。 0:上位プロキシが存在する場合は転送する。 1:常に転送しない。 2:常に転送する。 3:認証情報のみ転送する。 4:追加ヘッダ情報のみ転送する。 5:転送しない。Allow:204の場合は何も変更しない。(ICAP版のみ設定可能) • REQUESTMODE=0 の場合 (上位プロキシ指定あり) Proxy-Authorization ヘッダは上位に転送する。 以下のヘッダも追加される。 Remote-Host: X-Forwarded-For: Forwarded: Proxy-Agent: Via: 上位プロキシが指定されていない場合と ICAP 版では REQUESTMODE=1 と同様。 • REQUESTMODE=1 の場合 Proxy-Authorization ヘッダは上位に転送しない。 他のヘッダも追加しない。 • REQUESTMODE=2 の場合 Proxy-Authorization ヘッダは上位に転送する。 以下のヘッダも追加される。 Remote-Host: X-Forwarded-For: Forwarded: Proxy-Agent:Via: • REQUESTMODE=3 の場合 Proxy-Authorization ヘッダは上位に転送する。 他のヘッダは追加しない。 • REQUESTMODE=4 の場合 Proxy-Authorization ヘッダは上位に転送しない。 以下のヘッダが追加される。 Remote-Host: X-Forwarded-For: Forwarded: Proxy-Agent:Via: • REQUESTMODE=5 の場合 Proxy-Authorization ヘッダは上位に転送しない。 以下のヘッダも存在した場合は削除し転送しない。 Remote-Host: X-Forwarded-For: Forwarded: Proxy-Agent:Via: ICAP クライアントが Allow 204 を指定している場合で、規制対象でないときは 204 応答を行う。その場合 REQUESTMODE によるヘッダ削除は事実上無効となる。

TRANSFER_VERSION=1 (スタンドアロン版)	スタンドアロン版のみの設定項目。 リクエスト / レスポンス転送時に使用する、HTTP バージョンを設定する。 0: 受信した HTTP バージョンを、常に HTTP/1.0 に変更して転送する。 1:受信したHTTPバージョンをそのまま転送する。
POST_KEEPALIVE= FALSE（スタンドアロン版）	スタンドアロン版のみの設定項目。 POSTリクエストの持続接続を実施するか否かのフラグ。 TRUE:持続する FALSE:持続しない
TRANSPARENT_PROXY_ ENABLE＝FALSE （スタンドアロン版）	スタンドアロン版のみの設定項目。 スタンドアロン版で透過プロキシ動作を実施するかを設定する。 TRUE:透過プロキシ動作を実施する FALSE:透過プロキシ動作を実施しない
DATATUNNEL_TIMEOUT =90000(スタンドアロン版)	スタンドアロン版のみの設定項目。 HTTPSプロキシへのCONNECT後のトンネリング通信時のタイムアウト値をミリ秒単位で設定する。 0の場合はタイムアウトしない。
ALLOW_GROUP_PROXY =FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 グループごとに上位プロキシ設定の許可を設定するフラグ。 TRUE:グループごとに上位プロキシ設定を許可し、設定されたプロキシを使用する。 FALSE:グループごとの上位プロキシ設定を禁止し、設定されたプロキシは使用しない。
DNSRESOLVEWARN_TIM EOUT=15000 (スタンドアロン版)	スタンドアロン版のみの設定項目。 ホスト名正引き時の警告ログ用タイムアウト値をミリ秒単位で設定する。 ホスト名の正引きの経過時間がこの設定値を超えた場合に警告ログを出力する。0の場合は出力しない。
SERVERCONNECTWARN _TIMEOUT=15000 (スタンドアロン版)	スタンドアロン版のみの設定項目。 上位サーバへ接続する際の警告ログ出力用タイムアウト値をミリ秒単位で設定する。 上位サーバへ接続する際の経過時間がこの設定値を超えた場合に警告ログを出力する。0の場合は出力しない。

BUFF_POST=8192 （スタンドアロン版）	スタンドアロン版のみの設定項目。 上位サーバへ POST/PUT 転送を行う際の POST 転送バッファサイズを設定する。 上りの転送時に使用され、下りの転送時は通常と同様に BUFF 値が使用される。 0が指定された場合はBUFFの値と同じ数値を使用する。
SERVER_TCPNODELAY=TRUE （スタンドアロン版）	スタンドアロン版のみの設定項目。 上位側とのTCP接続のTCPNODELAYを設定する。 TRUE: 連続する小さいパケットの送信を遅延するNagleアルゴリズムが無効化され、逐次送信する。 FALSE: Nagleアルゴリズムが有効化され、遅延送信する。
CLIENT_TCPNODELAY=TRUE （スタンドアロン版）	スタンドアロン版のみの設定項目。 下位側とのTCP接続のTCPNODELAYを設定する。 TRUE: 連続する小さいパケットの送信を遅延するNagleアルゴリズムが無効化され、逐次送信する。 FALSE: Nagleアルゴリズムが有効化され、遅延送信する。
KEEPALIVE_TIMEOUT_MODE=ADJUST （スタンドアロン版）	スタンドアロン版のみの設定項目。 上位からの応答にKeep-Aliveヘッダが存在し、Timeout値が指定されている場合の動作を設定する。 IGNORE: Keep-Alive ヘッダは修正せずに、後続のリクエストの受信タイムアウトにCLIENT_TIMEOUTを使用する。 DELETE: Keep-Alive ヘッダを削除し、後続のリクエストの受信タイムアウトにCLIENT_TIMEOUTを使用する。 ACCEPT: Keep-Alive ヘッダは修正せずに、後続のリクエストの受信タイムアウトをヘッダに指定されていた値を使用する。 FORCE: Keep-Aliveヘッダを修正し設定された固定値をTimeoutに記述する。後続のリクエストの受信タイムアウトも設定された固定値(FORCE_KEEPALIVE_TIMEOUT)を使用する。 ADJUST: 通常時は IGNORE で動作する。デコード時と上位サーバでSPNEGOの場合、ACCEPTで動作する。
FORCE_KEEPALIVE_TIMEOUT=5 （スタンドアロン版）	スタンドアロン版のみの設定項目。 KEEPALIVE_TIMEOUT_MODEがFORCEの場合のTimeout値を秒単位で設定する。 上位からの応答にKeep-Aliveヘッダが含まれており、Timeout値が設定されていた場合、その値をこの設定値に補正する。
SNI_CAPABLE_UA=TLS/SSL Client （スタンドアロン版）	スタンドアロン版のみの設定項目。 HTTPS透過プロキシにおいて、疑似CONNECT処理時にSNIエクステンションが取得できた場合の疑似User-Agentを設定する。

UNSUPPORTED_SNI_UA=Unsupported SNI Client（スタンドアロン版）	スタンドアロン版のみの設定項目。 HTTPS透過プロキシにおいて、疑似CONNECT処理時にSNIエクステンションが取得できない場合の疑似User-Agentを設定する。
UNKNOWN_PROTOCOL_UA=Unknown Protocol Client（スタンドアロン版）	スタンドアロン版のみの設定項目。 HTTPS 透過プロキシにおいて、疑似 CONNECT 処理時の判別不能なプロトコルの場合の疑似User-Agentを設定する。
DISABLE_OTHER_PROTOCOLS=FALSE（スタンドアロン版）	スタンドアロン版のみの設定項目。 HTTP/2およびQUICの利用を抑制する。 TRUE の場合、平文の HTTP/1.1 のサーバからのレスポンス HTTP ヘッダに含まれる Alternate-Protocol ヘッダ、Alt-Svc ヘッダ Upgrade ヘッダを削除する。
DECODE_ADD_HEADER=FALSE（スタンドアロン版）	スタンドアロン版のみの設定項目。 HTTPS デコードされている場合に追加のリクエストヘッダを転送するかどうかを設定する。 TRUE:転送する。 FALSE:転送しない。

■[LOG_CFG]

LOG_FILE=iswm.log	出力するログファイルの名称を設定する。 ”ファイル名.拡張子”で設定する。128文字まで設定可能。 (例)”netstar.log” と設定した場合、以下のようなファイル名でログファイルが出力される。 ”netstar_proxy.log” ”netstar_adm.log” ”netstar_http.log” ”netstar_post.log” ファイル名だけを設定した場合、<インストールディレクトリ>¥logs以下にログファイルが出力される。 絶対パス＋ファイル名を設定した場合、指定した絶対パスにログファイルが出力される。ただしネットワークパスは指定できない。
LOG_OUTPUT_UNIT=SYSTEM	ログの出力単位。 SYSTEM:システム一括 GROUP:第1階層グループ毎

LOG_MAX=10	ログのローテーションをファイルサイズで行う場合、そのサイズを指定。 1Mバイト～2048Mバイトまで指定可能。
LOG_TYPE=1	アクセスログで出力するログの種類を設定する。 0:出力しない。 1:[MIME-TYPE] でTEXT形式と判断されたファイルへのリクエスト, 判断できないリクエスト(ディレクトリ、ドメイン等)を出力。 2:すべてのリクエストを出力。
LOG_HNCONV=FALSE	アクセスログに、クライアントのIPアドレスをホスト名として出力するか設定する。 TRUE:出力する。 FALSE:出力しない。
LOG_AUTO_EXPIRE=FALSE	ログファイル自動削除機能の有効/無効の識別子 TRUE:自動削除機能を有効にする。 FALSE:自動削除機能を無効にする。
LOG_DURATION=5	1以上の値を設定する。 ローテートログファイルは保存日数ではなくファイルの数でカウントする。自動削除が有効な場合には、この日付の古いものから順に、この指定数分以外のファイルの削除を行う。
LOG_OUTSTATUS=1,1,1,1,1,1,1	ログファイルへ出力する各ステータスについて、それぞれ(Proxied,Confirm,Blocked,Allowed,Release,CfmPost,BlkPost)に0または1を設定する。 0:出力しない 1:出力する ステータス数に誤りがある場合、項目自体が空の場合、記述形式が異なる場合(文字列指定など)の不正な値の場合は、すべて1に設定される。

【スタンドアロン版】 LOG_OUT_COLUMNS= group,user,error_code, req_data_transfer_size, mime_type 【ICAP版】 LOG_OUT_COLUMNS= group,user,mime_type	アクセスログに出力する内容を設定する。出力したい項目を「,」(半角カンマ) 区切りで複数指定可能。空の場合はすべての項目を出力する。 all(すべて):共通 group(グループ名):共通 user(アカウント名):共通 user-agent(ブラウザバージョン):共通 destination-ip(WWWサーバIP):ICAP版では非表示 error_code(エラーコード):ICAP版では非表示 req_data_transfer_size(リクエスト転送データサイズ):共通 res_data_transfer_size(レスポンス転送データサイズ):ICAP 版では非表示 mime_type(ファイルタイプ):共通 content_type(HTTPヘッダから取得したMIMEタイプ):ICAP版では非表示 category(ロングストマッチしたカテゴリ):共通 method(HTTPメソッド名):共通 http_version(HTTPバージョン):共通 referer(リンク元サイト):共通 記述例: group,user,user-agent,destination-ip,mime_type ※空の場合、または不正な文字列が指定された場合は、何も出力されない。
TRACE_POST_REQ_SIZE =0	POSTのBody部分をpostログに記述するサイズを指定(バイト単位)する。 0の場合には、書き込まれない。
LOG_ROTATE=1	ログのローテーションタイミングを設定する。 0:proxy.infのLOG_MAXで設定したサイズを超えるとき、ローテーション。 1:日付が変わるごとに、ローテーション。 2:週が変わるごとに、ローテーション(日曜日)。 3:月が変わるごとに、ローテーション。
LOG_CTG_HTTPS_POST =ALL	HTTPSデコード時にPOSTログを出力するカテゴリ/サブカテゴリを設定する。 POSTログを出力したいカテゴリ/サブカテゴリのIDを「,」(半角カンマ)区切りで複数指定可能。 ALLの場合はすべてのカテゴリ/サブカテゴリを出力する。

LOG_MAX_LIMIT=TRUE	ログのファイルサイズが2Gバイトを超えたときにも自動ローテーションするかを設定する。 TRUE:実施する。 FALSE:実施しない。
LOG_CTG_HTTPS_URL_OUTPUT=ALL	HTTPS デコード時にアクセスログに出力される URL にパス部を出力するカテゴリ/サブカテゴリを設定する。 パス部を出力したいカテゴリ/サブカテゴリのIDを「,」(半角カンマ)区切りで複数指定可能。 ALLの場合はすべてのカテゴリ/サブカテゴリを出力する。
LOG_TYPE_CONTENTTYPE=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 LOG_TYPE の判定時に [MIME-TYPE] とレスポンスヘッダの Content-Typeを判定対象とするかを設定する。 TRUE: レスポンスヘッダの Content-Type を判定対象とする。 FALSE:レスポンスヘッダのContent-Typeを判定対象としない。
TRACE_POST_REQ_MINSIZE=1	POST ログを出力する場合の HTTP ボディサイズの下限を設定する。 この値を下回る場合、POST ログは出力されない。 単位はバイトで設定する。
LOG_SEQUENCE=FALSE	通信シーケンスログの出力の有無を設定する。

■[BLOCK_CFG]

BLOCK_URL=http://iswm.netstar-inc.com/	規制後の転送先Webサーバを設定する。 391バイトまで設定可能。
BLOCK_FILE=nfblock.htm	規制後、ブラウザに表示するHTMLファイルのフォーマットファイルを設定する。 <インストールディレクトリ>/conf/block以下のパスを記述。 128文字まで設定可能。絶対パスで記述する。 <インストールディレクトリ>/conf/block以下と異なるパスに配置した場合は表示できない。
BLOCK_MSG=This Page Access Denied.	規制後にブラウザへ表示するメッセージを設定する。 128文字まで設定可能。

BLOCK_MODE=2	クライアントが規制サイトへアクセスした場合の動作を選択する。 1:proxy.infのBLOCK_URLで指定したWebサーバへ転送する。 2:proxy.infのBLOCK_FILEで指定したHTMLファイルを元に規制画面をブラウザに表示する。 3:proxy.infのBLOCK_MSGで指定したメッセージをブラウザに表示する。
ENABLE_CATEGORY_OVERRIDE=FALSE	一時許可の動作切り替えフラグ。管理画面からの編集は不可。 TRUE:カテゴリごとの一時許可を実施する。 FALSE:一時解除を実行すると、一時許可中は他の一時許可指定のカテゴリも閲覧可能となる。
ENABLE_OFFER_URL=FALSE	規制解除申請機能の有効/無効を設定する。 有効にすると、規制画面(ファイル)に規制解除申請画面へのリンクが表示される。 TRUE:規制解除申請機能を有効にする。 FALSE:規制解除申請機能を無効にする。
OFFER_MAILTO=(デフォルト値:なし)	ENABLE_OFFER_URLがTRUEのときに使用する、申請メールの通知先を設定する。 通知するメールアドレスを半角128文字以内で入力する。 複数のメールアドレスを「,」(半角カンマ)で区切って設定できる。
OFFER_SYSTEM_ADMIN=FALSE	システム管理者(ADMINグループ所属ユーザ)への申請メール通知を設定する。 TRUE:システム管理者にメールで通知する。 FALSE:システム管理者にメールで通知しない。
OFFER_GROUP_ADMIN=1	グループ管理者への申請メール通知を設定する。 1:グループ管理者にメール通知しない。 2: 申請したユーザが所属するグループ階層の第1階層グループ管理者にメール通知する。 3:申請したユーザが所属するグループのグループ管理者にメール通知する。 4:申請したユーザが所属するグループ階層より上位階層のグループ管理者にメール通知する。

BLOCK_ALL_POST=TRUE	書き込み規制の対象とするURLを設定する。 proxy.infにBLOCK_ALL_POSTが存在しない場合、FALSEとして動作する。 TRUE:すべてのリクエストURLに対して書き込み規制を有効にする。 FALSE:URLデータベースに登録されているURLに対してのみ、書き込み規制を有効にする。
OFFER_COLLECT_INTERVAL=60	プライマリサーバの管理サービスが、レプリカサーバの管理サービスから規制解除申請ファイルを回収する間隔を指定する。 単位は秒で設定する。 1秒～100,000秒まで設定可能
HTTPS_DECODE=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 HTTPSデコードの使用を設定する。 TRUE: HTTPSデコードを行う。 FALSE: HTTPSデコードを行わない。
HTTPS_DECODE_TYPE=0 (スタンドアロン版)	スタンドアロン版のみの設定項目。 HTTPSデコードの単位を設定する。 0:システム一括で設定する。 1:グループ毎に設定する。
HTTPS_DECODE_WARN=TRUE (スタンドアロン版)	スタンドアロン版のみの設定項目。 HTTPSデコード警告画面の表示を設定する。 TRUE:表示する。 FALSE:表示しない。
HTTPS_DECODE_WARN_INTER VAL=6 (スタンドアロン版)	スタンドアロン版のみの設定項目。 HTTPS デコード警告画面を表示する時間間隔を、時間単位で設定する。
HTTPS_DECODE_LIST_MATCH=DENY (スタンドアロン版)	スタンドアロン版のみの設定項目。 HttpsDecodeListファイルに定義されているホスト名に対するデコード動作を設定する。 ALLOW:ファイルに定義されているホストのデコードのみ許可する。 DENY:リストに定義されているホストのみデコードの対象から除外する。
PRIORITYCATEGORY_INCLUDE_CASCADE=FALSE	カスケードマッチによって付与されたカテゴリを優先カテゴリの対象にするかを設定する。 TRUE:対象にする。 FALSE:対象にしない。

PRIORITYCATEGORY_ INCLUDE_USRDB=FALSE	例外URLによって付与されたカテゴリを優先カテゴリの対象にするかを設定する。 TRUE:対象にする。 FALSE:対象にしない。
BLOCK_TUNNEL_PROTOCOL=1 （スタンドアロン版）	スタンドアロン版のみの設定項目。 CONNECT のトンネリング通信の開始時にプロトコルチェックを実施するかを設定する。なお、不明プロトコルの場合は接続は切断される。 0: 実施しない。 1: 実施する。 2: 実施する。(SSLv3を遮断する) 3: 実施する。(SSLv3とTLS1.0も遮断する)
BLOCK_INVALID_SNI=TRUE （スタンドアロン版）	スタンドアロン版のみの設定項目。 CONNECTリクエストのホスト名とSNIのホスト名の正常性チェックを実施するかを設定する。不一致の場合は接続は切断される。 FALSE: 実施しない。 TRUE: 実施する。
HTTPS_DECODE_ EXCLUDE_CTG=(デフォルト値:なし) （スタンドアロン版）	スタンドアロン版のみの設定項目。 HTTPSデコード機能にて、デコードから除外するカテゴリIDの一覧を設定する。 "," 区切りで小カテゴリの ID（XXYY）を列挙する。「ALL」を設定すると、全カテゴリのIDを列挙する。
BLOCK_CHUNKED_POST=2	Transfer-Encoding: chunked の POST/PUT のリクエストの動作を設定する。 0: 転送しない。(下位互換動作) 1: 無条件で上位に転送する。(規制処理対象外となる) 2: 書き込み規制が設定されている場合はサイズによらず規制対象とする。それ以外の場合は転送する。 3: 書き込み規制の設定値を超えるまでは転送し、設定サイズを超えた時点で規制対象とする。
RELEASE_FORWARDING_ENABLE=FALSE	ロードバランサによる負荷分散を行っている環境において、フィルタリング規制一時解除、HTTPSデコード警告解除、サーバー証明書警告解除を実施したサーバ以外に回送するかを設定する。 TRUE: 解除を実施したサーバ以外に回送する。 FALSE: 解除を実施したサーバ以外に回送しない。

RELEASE_FORWARDING_TIMEOUT=30000	ロードバランサによる負荷分散を行っている環境において、フィルタリング規制一時解除、HTTPSデコード警告解除、サーバー証明書警告解除を実施したサーバ以外に回送する際の通信タイムアウト。 単位はミリ秒で設定する。管理画面では設定不可。

■[MANAGEMENT_CFG]

MAX_GUSER=99999	1つのグループに登録できるユーザの最大数を設定する。 管理画面では設定不可。 設定できる上限値は 99999。上限値を超える値が記述されていた場合、上限値99999として設定される。
MAX_GGROUP=100	1つのグループの配下に作成できるグループの上限値を設定する。 設定できる上限値は999。上限値を超える値が記述されていた場合、上限値999として設定される。
MAX_GRULE=256	1つのグループで作成できるルールの上限値を設定する。 設定できる上限値は999。上限値を超える値が記述されていた場合、上限値999として設定される。
MAX_R_EXURL=10	1 つのグループに関連付けられる例外 URL ルールの上限値を設定する。 設定できる上限値は99。上限値を超える値が記述されていた場合、上限値99として設定される。
MAX_BACKUPS=5	設定の保存/復旧で指定できる保存ファイル数の上限値。
DEFAULT_REF_PARENT_POLICY=FALSE	新規グループを作成するとき、デフォルトで上位グループ参照機能を有効にするか設定する。 TRUE: 上位グループ参照機能を有効にする。 FALSE: 上位グループ参照機能を無効にする。
CONFIG_AUTO_SYNC=TRUE	設定を変更したときに自動的にレプリカサーバと同期するかどうかを設定する。 TRUE:自動で同期する。 FALSE:自動で同期しない。
MAX_EXURL_REG=10000	システム全体で登録可能な例外URLの上限値を設定する。 上限値を100000とし、これを超える値が設定された場合は上限値10000が使われる。

MAX_USER_CTG＝10	ユーザ設定サブカテゴリの表示の上限値。 10～99まで設定可能。
COUNTRY_ACCESS_ ALERT_CTG＝SECURITY	国・地域のアクセス表示のうち警告表示に分類するカテゴリ ID の一覧。 ”,” 区切りで小カテゴリの ID（XXYY）か SECURITY を列挙する。 ALL：全カテゴリ ID の列挙と等価 SECURITY:マルウェア/ウイルス対策カテゴリIDの列挙と等価

■[PROXY_PORT]

HTTP=8080,450 (スタンドアロン版)	スタンドアロン版のみの設定項目。 プロキシで使用するポート番号とプロセス数を設定する。 ポート番号,プロセス数と設定する。(例:8080,450) ポート番号は、1～65535まで設定可能。 プロセス数は、1～9999まで設定可能。
HTTPS=8443,450 (スタンドアロン版)	スタンドアロン版のみの設定項目。 プロキシで使用するポート番号とプロセス数を設定する。 ポート番号,プロセス数と設定する。(例:8443,450) ポート番号は、1～65535まで設定可能。 プロセス数は、1～9999まで設定可能。
FTP_OVER_HTTP=8021, 100 (スタンドアロン版)	スタンドアロン版のみの設定項目。 プロキシで使用するポート番号とプロセス数を設定する。 ポート番号,プロセス数と設定する。(例:8021,100) ポート番号は、1～65535まで設定可能。 プロセス数は、1～9999まで設定可能。
TRANSPARENT_HTTPS= 8443,450 （スタンドアロン版）	スタンドアロン版のみの設定項目。 HTTPS透過プロキシポートとプロセス数を設定する。 ポート番号,プロセス数と設定する。(例:8443,450) ポート番号は、1～65535まで設定可能。 プロセス数は、1～9999まで設定可能。

■[SYSTEM_UPDATE]

ID=(デフォルト値:なし)	DBダウンロードサーバへ送信する、ライセンスキーを設定する。 0文字～16文字まで設定可能。

NAME=(デフォルト値:なし)	DB ダウンロードサーバへ送信する、ユーザ名 (企業, 団体名) を設定する。 0文字～64文字まで設定可能。
DBSERVER=iswm.netstar-inc.com	DBダウンロード先のURLを設定する。 0文字～128文字まで設定可能。
PLURAL_DOWNLOAD=TRUE	DBダウンロードを一日複数回行うかどうかのフラグ。 TRUE に設定されている場合、DB の自動ダウンロードは system.inf の [SYSTEM_UPDATE] セクションの PLURAL_TIME の値から1時間ごとに実行される。 下記TIME項目の値は使用されない。
TIME=-1:-1	DB自動ダウンロードの開始時間を設定。 1時間毎で設定する。 5:00 ～ 6:00 の間に DB 自動ダウンロードを行いたい場合、”5:00” とする。 ”-1:-1”を設定した場合、”規定時間”とみなし、2:00に設定する。 DB自動ダウンロードは、設定時間から1時間の間で行われる。
MAILADDRESS=(デフォルト値:なし)	DBダウンロードサーバへ送信する、メールアドレスを設定する。 0文字～128文字まで設定可能。
DBUPSERVER=:80	DBダウンロードで上位プロキシを経由したい場合、そのプロキシのIPアドレスとポート番号をIPアドレス:ポート番号で設定する。 (例:192.168.50.60:8080) 指定がない場合は、”:80”と指定する。 ポート番号は、1～65535まで設定可能。
DB_RETRY_TIME=2	DBダウンロードができなかった場合のリトライの回数。 2,3,4,5から選択。
DB_RETRY_INTERVAL=40	DBダウンロードのリトライを行う場合の間隔(単位は分)を指定。 30,40,50,60から選択。
DB_ALIAS=db90	データベースダウンロード用エイリアス
REQUEST_PROTOCOL=https://	DBサーバとエージェント間通信プロトコル http://、https://から選択。

■[SYSTEM_AUTHENTICATION]

AUTHENTICATION=FALSE	URLチェックを行う際、認証処理を行う/行わないの設定。 TRUE: 認証を行う。 FALSE: 認証を行わない。 初期認証の有無についてはREQUIRE_FIRST_AUTHキーに従う。
REQUIRE_FIRST_AUTH=TRUE	初期認証要求の有無。AUTHENTICATIONキーがTRUEの場合のみ有効。 TRUE: リクエストを受けた時点で、認証を行う。 FALSE: リクエストされた URL が規制対象の場合のみ認証を行う。
GR_AUTHENTICATION=FALSE	グループ認証を行うフラグ。管理画面へのログオン形式をグループ認証とする場合のみ有効。 TRUE: グループ認証を行う。 FALSE: グループ認証を行わない。
ACCOUNT_AUTHENTICATION=TRUE	ユーザ認証でアカウント認証を有効にするか設定する。 TRUE: アカウント認証を有効にする。 FALSE: アカウント認証を無効にする。この場合、IP アドレス認証だけが有効になる。
DEFAULT_GROUP_ON=FALSE	連携プロキシが認証したユーザ(IPアドレス)がコントロールサーバのユーザ情報に存在しない場合、”未登録ユーザ”グループのポリシーを用いるか設定する。 TRUE: 使用する。存在しないユーザはすべて”未登録ユーザ”のポリシーに従う。 FALSE: 使用しない。存在しないユーザはすべて規制する。 proxy.infのAUTHENTICATIONに”TRUE”が設定されている必要がある。
ALLOWEMPTYPASSWD=FALSE	認証情報でパスワードが空の場合のLDAP認証処理を設定する。 TRUE: LDAP認証処理を許可する。 FALSE: 認証エラーにする。 TRUEの場合は、LDAP連携しないときであってもパスワードが空を許可する。
IGNORE_IP_HEADER=FALSE	リクエストヘッダに入っているX-Forwarded-Forの値をIPアドレス認証に使うか設定する。 TRUE の場合は X-Forwarded-For の値を無視し、常に接続元 IP アドレスで認証を行う。

■[ACCESS_CTRL]

CFG_ACCESS_IPADDRESS=ALL	システム管理者、グループ管理者が管理画面にログインするときに使用するコンピュータの、IPアドレスを指定する。 IPアドレスは範囲指定できる。設定がない場合、すべてのIPアドレスが許可される。 ALL:すべて許可 [IPアドレス]-[IPアドレス]:範囲指定 複数指定の場合、半角カンマで区切る。
HTTP_DENY_PORT=25 110	HTTPプロトコルでリクエスト先のポート番号で利用できない値を指定する。何も設定していない場合、すべてのポート番号を許可する。 proxy.infにHTTP_DENY_PORTが存在しない場合、25番、110番ポートが設定される。
CLIENT_ACCESS_IPADDRESS=ALL	コントロールサーバ、プロキシに接続できるクライアントのIPアドレス(範囲指定)。設定がなかった場合、すべて許可。 ALL:すべて許可 [IPアドレス]-[IPアドレス]:範囲指定 複数指定の場合、半角カンマで区切る。
WRITING_ALLOW_SIZE=0	リクエストのContent-Lengthの値で、書き込み規制対象のリクエストとして処理するか、判断する。 値が”0”の場合:すべてのPOSTリクエストを規制する。 値が”1”以上の場合:POSTリクエストのContent-Lengthの値が設定した値を超えた場合は、書き込み規制対象にする。単位はバイト。
HTTPS_ACCESS_PORT=443	クライアントが送信してくる HTTPS サイトのポート番号でリクエストを許可する設定。 値が”ALL”の場合: すべてのポート番号を許可する。 値が数値の場合:指定したポート番号を許可する。複数のポート番号を設定する場合、ポート番号を半角スペースで区切る。 ALLと数値が混在する場合: ALLが有効になる。 何も設定していない場合:すべて拒否する。
AUTHORIZED_USER_AGENT=Windows-Update-Agent, Microsoft BITS, EndPointModule, Windows Installer, Microsoft-CryptoAPI, CATsecurity	設定した文字列がHTTP リクエストのUser-Agent ヘッダに含まれる場合は、必ずルートグループのユーザとして認証し、フィルタリングを行う。 AUA_SEPARATORで設定した文字を区切り文字として複数のUser-Agentを設定可能。
AUA_SEPARATOR=,	AUTHORIZED_USER_AGENTの区切り文字。

ALLOW_GROUP_POST=FALSE	POSTリクエストの書き込みサイズを、グループごとに指定することを許可するかを設定する。 TRUE:POSTリクエストの書き込みサイズを、グループごとに指定することを許可する。 FALSE:POST リクエストの書き込みサイズを、グループごとに指定することを許可しない。
AUTHORIZED_HOST=windowsupdate.com,*.windowsupdate.com,windowsupdate.microsoft.com,*.windowsupdate.microsoft.com,update.microsoft.com,*.update.microsoft.com,mp.microsoft.com,*.mp.microsoft.com,download.microsoft.com,*.ws.microsoft.com,ntservicepack.microsoft.com,wustat.windows.com	設定してある場合、リクエスト先ホストと一致する場合は必ずルートグループとしてフィルタリングを行う。 AH_SEPARATORを区切り文字として複数設定可能。ワイルドカード(*)を使用可能。
AH_SEPARATOR=,	AUTHORIZED_HOSTの区切り文字。
BROWSER_ON=FALSE	ブラウザ規制フラグ。 TRUE:ブラウザ規制を使用する。 FALSE:ブラウザ規制を使用しない。
BROWSER_MATCH_ALLOW=TRUE	ブラウザ規制の許可/規制フラグ。 TRUE:ブラウザ(リスト)に合致したブラウザ情報を送信したユーザのみ許可する。 FALSE:ブラウザ(リスト)に合致したブラウザ情報を送信したユーザのみ規制する。
POST_KEYWORD_ON=FALSE	書き込みキーワード規制フラグ。 TRUE:書き込みキーワード規制を使用する。 FALSE:書き込みキーワード規制を使用しない。
SEARCH_KEYWORD_ON=FALSE	検索キーワード規制フラグ。 TRUE:検索キーワード規制を使用する。 FALSE:検索キーワード規制を使用しない。

SAFE_SEARCH_APPLY_ON=FALSE	セーフサーチロック機能の有効/無効フラグ。 TRUE:リクエストを編集し、検索エンジンのセーフサーチロック機能を自動的に有効にする。 FALSE:リクエストを編集せず、検索エンジンのセーフサーチロック機能の制御を行わない。 ICAP版でREQUESTMODE=5の場合には、動作しない。
BROWSER_NO_HEADER=NO_MATCH	ブラウザ規制の際にUser-Agentヘッダが存在しない場合の挙動を設定する。 NO_MATCH: ブラウザ(リスト)に合致していないとみなす。 MATCH: ブラウザ(リスト)に合致したとみなす。
ALLOW_POST_SIZE_ORDER＝DEFAULT	複数のカテゴリに設定された書き込み許容サイズから判定する場合の動作を設定する。 DEFAULT:カテゴリ順で判定する。 GREATER:最も大きな許容サイズの値で判定する。 ONLY_USER_CTG_GREATER:ユーザ設定カテゴリが付与された場合はユーザ設定カテゴリのうち最も大きな許容サイズの値で判定する。 ユーザ設定カテゴリが付与されない場合はカテゴリ順で判定する。
COUNTRY_BLOCKING_ON＝FALSE	国・地域のアクセス規制の有無を設定する。 TRUE:国・地域のアクセス規制を実施する。 FALSE:国・地域のアクセス規制を実施しない。
BLOCK_COUNTRY＝ （デフォルト値:なし）	アクセス規制を行う国・地域を設定する。半角カンマを区切り文字として複数設定可能。
IWCC_ON＝FALSE	高度分類クラウドの使用を設定する。 TRUE:高度分類クラウドを使用する。 FALSE:高度分類クラウドを使用しない。
IWCC_URL_REQ＝ALL	高度分類クラウドへのリクエストに含める URL の形態を設定する。 ALL:入力されたURL DEL_PARAM:パラメータ部を削除したURL HOST:ホスト部までのURL

IWCC_MODE＝FILTERING	高度分類クラウドへのリクエスト解決後の動作モードを設定する。 LOG:ログへの付与のみの監査モード FILTERING:付与されたカテゴリでフィルタリングを実施､付与が失敗した場合などは未分類のまま動作する。 NOFAILSAFE:付与されたカテゴリでフィルタリングを実施､付与が失敗した場合は規制として動作する。
IWCC_DENY_HOST＝（デフォルト値:なし）	高度分類クラウドへのリクエスト除外とするホストまたは IP アドレスを設定する。 半角カンマを区切り文字として複数設定可能。
IWCC_DENY_IP＝ALL	高度分類クラウドへのIPアドレスURLのリクエスト除外方法を設定する。 NONE:除外無し ALL:すべてのIPへのアクセスを除外 PRIVATE:プライベートIPへのアクセスだけを除外
IWCC_RESCATE_LOG＝TRUE	高度分類クラウドで付与されたカテゴリのログ時のプレフィックス付与要否を設定する。 TRUE:プレフィックスを付与する。 FALSE:プレフィックスを付与しない。
IWCC_REQ_LOG＝FALSE	高度分類クラウドへリクエストしたURLのログ出力有無を設定する。 TRUE:リクエストURLをログへ出力する。 FALSE:リクエストURLをログへ出力しない。

■[PROXY_AUTHENTICATION]

ACCOUNT=(デフォルト値:なし)	DBダウンロードを行う際､上位プロキシが存在する場合､送信するアカウント情報を設定する。 1文字～32文字まで設定可能。
PASSWORD=(デフォルト値:なし)	DBダウンロードを行う際､上位プロキシが存在する場合､送信するパスワード情報｡暗号化された値のため編集できない。

■[SERVICE_OBSERVE]

INTERVAL=60	プライマリサーバの管理サービスがフィルタリングサービスの状態(起動中/停止中/再起動中)の確認を行う時間間隔。 1秒～100000秒まで設定可能。
ADMIN_INTERVAL=30	プライマリサーバの管理サービスがレプリカサーバの管理サービスの状態(起動中/データ保存中/復旧中)の確認を行う時間間隔。 1秒～100000秒まで設定可能。
OBSERVE_RETRY=3	プライマリサーバの管理サービスが、フィルタリングサービスの状態を確認するときのリトライ回数。
ADMIN_OBSERVE_RETRY=3	プライマリサーバの管理サービスが、レプリカサーバの管理サービスの状態を確認するときのリトライ回数。
CAPACITY_CHECK_INTERVAL=300	プライマリサーバの管理サービスがディスク空き容量の監視を行う時間間隔。 1秒～100000秒まで設定可能。
CAPACITY_WARN_THRESHOLD=10,5,3,2,1	プライマリサーバの管理サービスがディスク空き容量の警告を行うしきい値。 1%～99%まで設定可能。「,」(半角カンマ)区切りで複数指定可能。
PROCESS_CHECK_INTERVAL=60	管理サービスがプロセス数の監視を行う時間間隔。 1秒～100000秒まで設定可能。
PROCESS_WARN_THRESHOLD=80	管理サービスがプロセス数の警告を行うしきい値。 0%～99%まで設定可能。
LDAP_CHECK_ON=TRUE	プライマリサーバの管理サービスが連携するLDAPサーバの状態監視を実施するかどうかを設定する。 TRUE:監視する。 FALSE:監視しない。
LDAP_CHECK_INTERVAL=10	プライマリサーバの管理サービスが連携するLDAPサーバの状態監視を行う時間間隔を、1～100000秒の範囲で設定する。
LDAP_MANAGEMENT_ON=FALSE	プライマリサーバの管理サービスが連携するLDAPサーバの状態監視により、サーバの自動切り離し/自動再接続の管理を行うかを設定する。 TRUE:自動管理する。 FALSE:自動管理しない。
LDAP_DETACH_THRESHOLD=3	LDAPサーバの自動切り離しを行う監視失敗回数のしきい値を、1～100000回の範囲で設定する。

LDAP_ATTACH_ THRESHOLD=3	LDAPサーバの自動再接続を行う監視成功回数のしきい値を、1～100000回の範囲で設定する。
EXURL_AUTO_IMPORT_ ON=FALSE	例外URLの自動登録機能を実施するかを設定する。 TRUE:実施する。 FALSE: 実施しない。
EXURL_AUTO_DEL_ON= FALSE	例外URLの自動削除機能を実施するかを設定する。 TRUE:実施する。 FALSE: 実施しない。
ARMS_EXURL_ DURATION=30	ARMS連携で例外URLを登録する場合の登録時点からの有効期間を日単位で設定する。 0を設定すると無期限になる。
ARMS_FETCH_ON＝ FALSE	ARMS連携フェッチ機能を有効にする。 TRUE:有効にする。 FALSE: 無効にする。
ARMS_FETCH_ PROTOCOL＝https://	ARMS連携フェッチ時のプロトコルを設定する。 http://、https://から選択。
ARMS_FETCH_HOST＝ （デフォルト値:なし）	ARMS連携フェッチ時の取得先ホスト名を設定する。
ARMS_FETCH_PORT＝ 443	ARMS連携フェッチ時の取得先ポート番号を設定する。
ARMS_FETCH_PATH＝ （デフォルト値:なし）	ARMS連携フェッチ時の取得先のパスを設定する。
ARMS_FETCH_INTERVAL ＝10	ARMS連携フェッチ機能のフェッチ間隔を設定する。 単位は分で本設定の間隔でフェッチを行う。 サービス起動後、本設定経過以降に、取得が繰り返される。 10～1440の範囲で設定する。
ARMS_FETCH_HISTORY_ FILE＝var/ arms_fetch_history.txt	ARMS 連携フェッチ機能の前回フェッチ時の取得 URL を保存するテンポラリファイルを指定する。 相対パスで指定されている場合は、インストールディレクトリを基準とする。
ARMS_FETCH_HISTORY_ ON＝TRUE	ARMS連携フェッチ機能の差分取り込み処理を行うかを設定する。 TRUE:差分取り込みを実施する。 FALSE:差分取り込みを実施しない。

LOG_ANALYZE＝FALSE	Geoスコープ機能のログ集計処理を行うかを設定する。 TRUE:ログ集計を実施する。 FALSE:ログ集計を実施しない。
LOG_ANALYZE_DB_LIST＝(デフォルト値:なし)	集計データベースサービスのIPアドレスとポートの一覧。 半角カンマを区切り文字として複数設定可能。 空の場合はIP アドレスをMASTER_ADMIN_HOST とし、ポートから取得する。
LOG_ANALYZE_AGENT_PORT＝41210	アクセスログエージェントの待ち受けポート。
LOG_ANALYZE_DB_PORT＝41209	集計データベースサービスの待ち受けポート。
LOG_ANALYZE_DB_TARGET_AGENT＝(デフォルト値:なし)	集計データベースサービスの管理するアクセスログエージェントのIPアドレスとポートの一覧。 半角カンマを区切り文字として複数設定可能。 空の場合はレプリカ一覧から取得する。
SYSLOG_TRANSFER=FALSE	アクセスログのSyslog転送を実施するかを設定する。 TRUE: Syslog転送を実施する。 FALSE: Syslog転送を実施しない。
SYSLOG_TRANSFER_HOST=(デフォルト値:なし)	Syslog転送時の宛先ホスト。
SYSLOG_TRANSFER_PORT=6514	Syslog転送時の宛先ポート。
SYSLOG_TRANSFER_PROTOCOL=TLS	Syslog転送時の転送プロトコル。以下の値のいずれかを指定する。 UDP、TCP、TLS
SYSLOG_TRANSFER_FACILITY=USER	転送するログの機能区分(ファシリティ)。以下の値のいずれかを指定する。 KERN、USER、MAIL、DAEMON、AUTH、SYSLOG、LPR、NEWS、UUCP、CRON、AUTHPRIV、FTP、NTP、AUDIT、ALERT、CLOCK、LOCAL0、LOCAL1、LOCAL2、LOCAL3、LOCAL4、LOCAL5、LOCAL6、LOCAL7
SYSLOG_TRANSFER_SEVERITY=INFORMATIONAL	転送するログの重大度(プライオリティ)。以下の値のいずれかを指定する。 EMERGENCY、ALERT、CRITICAL、ERROR、WARNING、NOTICE、INFORMATIONAL、DEBUG

SYSLOG_TRANSFER_MESSAGE_FORMAT=IETF	転送するログのSyslogフォーマット。 BSD:RFC3164形式。 IETF:RFC5424形式。
SYSLOG_TRANSFER_TCP_SOCKET_TIMEOUT=500	TCP/TLS接続時のタイムアウト時間をミリ秒単位で設定する。
SYSLOG_TRANSFER_RETRY_INTERVAL=60	接続失敗した場合に再接続するまでの間隔を秒単位で指定する。
SYSLOG_TRANSFER_UDP_INTERVAL=1	UDPでログ転送を行う場合の転送間隔をミリ秒単位で設定する。 0ミリ秒を設定した場合は間隔なしで転送する。

■[LDAP]

USELDAP=FALSE	LDAP(認証サーバ) からユーザ情報を取得、認証処理の設定を行う。 TRUE:LDAP(認証サーバ)との連携を取る。 FALSE:LDAP(認証サーバ)との連携を取らない。
SCHEMA_LIST=ou,cn,name,dc,sn,givenName,uid,o,sAMAccountName,mail,user PrincipalName	LDAP同期設定のATTRIBUTE、およびGR_ATTRIBUTEに選択するリスト。
AUTO_SYNC=FALSE	LDAP自動連携処理を有効にするかの設定を行う。 TRUE:LDAP自動連携処理を有効にする。 FALSE:LDAP自動連携処理を無効にする。
AUTO_SYNC_INTERVAL=2	指定した時刻に、LDAP自動連携処理を実行する。 時刻:0～23 時刻は半角カンマ区切りで3つまで設定できる。 (例:AUTO_SYNC_INTERVAL=2,15,19)
ENABLE_NTLM_AUTH=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 NTLM認証の有効、無効を設定する。 TRUE:NTLM認証を有効にする。 FALSE:NTLM認証を無効にする。

AUTHENTICATE_CACHE_TIME=60	ユーザが LDAP サーバの認証に成功したときの情報を、認証情報としてキャッシュする時間を設定する。 -1～10080分(=1週間)まで設定可能。 設定可能範囲外の値を設定した場合、デフォルト値 (60 分) が設定される。 0:認証情報をキャッシュしない。 -1:フィルタリングサービスを再起動するまで、認証情報をキャッシュし続ける。ただしキャッシュが2000に達した場合は、古いキャッシュから順にメモリ上から削除される。メモリの使用量を抑制したい場合、-1の設定は推奨されない。 1～10080:指定した時間(分)、認証情報をキャッシュする。
USE_ATTR_GR_CTG=FALSE	LDAPグループ特定方式を設定する。 TRUE:グループ毎にユーザ抽出条件を指定する。 FALSE:ユーザのDNからグループ階層を特定する。
NTLM_AUTH_ALL_CACHE=TRUE (スタンドアロン版)	スタンドアロン版のみの設定項目。 NTLM認証時のキャッシュ方式を設定する。 TRUE:v6方式(IPアドレスとUserAgent)。 FALSE:未登録ユーザおよび認証失敗時のユーザをキャッシュ対象としない。
NTLM_LOG_IP_AC_NAME=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 NTLM 認証の IP 認証時にアカウント名をログ出力するか設定する。 TRUE:アカウント名へ変換して出力する。 FALSE:アカウント名へ変換しないで出力する。
LDAP_LOCAL_MIX_AUTH=FALSE	LDAP 連携アカウントとローカルのアカウントのユーザの認証および取り込み方式を設定する。 TRUE:LDAP サーバのユーザとローカルユーザのユーザ名が重ならないユーザの場合、共存を可能とする。 FALSE:v7方式(LDAP連携時にすべてのユーザ情報を上書きする)。 ※NTLM認証時またはKerberos認証時にActive Directory側に同名ユーザが存在しない場合は認証エラーとなります。

USER_IMPORT_MODE=LOCAL	LDAPとローカルのアカウントを共存させる場合（LDAP_LOCAL_MIX_AUTHがTRUEの場合）、LDAP同期設定時に重複したユーザ名のどちらを優先するかを設定する。 LOCAL:LDAP 同期設定時にローカルに作成されたアカウントを優先する。 LDAP:LDAP 同期設定時に LDAP サーバ側のアカウントを優先する。
NTLM_CACHE_UA=TRUE (スタンドアロン版)	スタンドアロン版のみの設定項目。 NTLM認証時の認証キャッシュにUserAgentを追加するか設定する。 TRUE:UserAgentを追加する。 FALSE:UserAgentを追加しない。
ENABLE_KERBEROS_AUTH=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 Kerberos認証を有効にする設定。 TRUE:Kerberos認証を有効にする。 FALSE:Kerberos認証を無効にする。
ENABLE_KERBEROS_USE_COMMON_SPN=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 Kerberos 認証ですべてのサーバで使用するサーバ自身の認証のための共通のサービスプリンシパル名を使用するかを設定する。 TRUE:すべてのサーバで使用する。 FALSE:サーバごとにFQDNから構成する。
ENABLE_KERBEROS_COMMON_SPN=(デフォルト値:なし) (スタンドアロン版)	スタンドアロン版のみの設定項目。 Kerberos 認証ですべてのサーバで使用するサーバ自身の認証のための共通のサービスプリンシパル名を設定する。
LDAP_SERVER_TIMEOUT=30000	LDAP通信の接続タイムアウト値をミリ秒単位で設定する。 0の場合はシステムによるタイムアウトを使用する。
LDAP_RESPONSEWARN_TIMEOUT=15000	LDAP 通信のレスポンスが応答されたが、一定時間を超えていた場合に警告ログを出す場合のタイムアウト値をミリ秒単位で設定する。 0の場合は出力しない。
KERBEROS_REALM_NAME=(デフォルト値:なし) (スタンドアロン版)	スタンドアロン版のみの設定項目。 Kerberos 認証ですべてのサーバで使用する Kerberos レルム名を設定する。

DOMAIN_SHUFFLE_ON=FALSE	認証時にLDAPサーバリストをドメインごとにシャッフルするかを設定する。 TRUE の場合、LDAP サーバのリストをシャッフルして、並び替えたリストを元に認証を行う。
SEARCH_NESTED_GROUP=FALSE	グループ問い合わせの比較対象にユーザの所属グループまで対象とするかどうかを設定する。 TRUE:対象とする。 FALSE:対象としない。

■[CONTROL_CFG]

PORT=1344 (ICAP版)	ICAP版のみの設定項目。 ICAPクライアントが接続するコントロールサーバのポート番号。 1～65535まで設定可能。
SERVER_TIMEOUT=300000 (ICAP版)	ICAP版のみの設定項目。 コントロールサーバと ICAP クライアント間の通信タイムアウト値を設定。 1ミリ秒～9,999,999ミリ秒まで設定可能。
SERVER_PROCESS=150 (ICAP版)	ICAP版のみの設定項目。 ICAPクライアントが接続するコントロールサーバのポート番号で初期稼動させるプロセス数を設定する。 1～9999まで設定可能。 ただし、ICAP版で通信シーケンスログを使用する場合は、設定をICAPクライアントが許容する同時接続可能数と同程度の数を設定する。
BLOCK_FILE_PORT=21128 (ICAP版)	ICAP版のみの設定項目。 規制画面出力用コントロールサーバのポート番号。 1～65535まで設定可能。
BLOCK_FILE_PROCESS=50 (ICAP版)	ICAP版のみの設定項目。 proxy.infのBLOCK_FILE_PORTで設定したポート番号で稼動するプロセスの最大数。 1～9999まで設定可能。

【スタンドアロン版】 PROXY_BLOCK_FILE_ SERVER=(デフォルト値: なし) 【ICAP版】 ICAP_BLOCK_FILE_ SERVER=(デフォルト値: なし)	規制画面をリダイレクトさせるドメイン名またはホスト名。 リクエストが規制された場合に、ブラウザに表示される規制画面URLのドメイン名またはホスト名を指定する。 ドメイン名またはホスト名は、プロキシサーバ上でICAPサーバのアドレスとして名前解決できる必要がある。また、ブラウザが動作しているクライアントでプロキシの除外対象とならないドメイン名またはホスト名を指定する必要がある(例:localhostや127.0.0.1)。
IPV6_INNER_IP=::1	内部的にローカルIPアドレスとして使用するIPv6アドレスを設定する。
IPV6_OUTER_IP=::1 (スタンドアロン版)	スタンドアロン版のみの設定項目。 外部へ接続する場合にローカルIPアドレスとして使用するIPv6アドレスを設定する。
ICAP_RESPMOD_ ENABLE=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携を実施するか設定する。 TRUE:実施する。 FALSE:実施しない。
ICAP_RESPMOD_HOST= (デフォルト値:なし) (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携先のホスト名を設定する。設定されたホストのICAPサーバに対して接続を行う。
ICAP_RESPMOD_PATH= (デフォルト値:なし) (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携時のリクエストラインに指定するサービスパスを設定する。
ICAP_RESPMOD_PORT= 1344 (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携先のポート番号を設定する。 ポート番号は、1～65536まで設定可能。
ICAP_RESPMOD_ PREVIEW=TRUE (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携時にプレビュー方式を使用するかを設定する。 TRUE:使用する。 FALSE:使用しない。

ICAP_RESPMOD_LOG_HEADER=X-Virus-ID, X-Infection-Found, X-Violations-Found, X-Response-Info, X-Response-Desc (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携ログに追加出力するICAPヘッダを入力する。 「,」(半角カンマ)区切りで複数指定可能。記載した順に値を取得し、出力される。 ヘッダが存在しない場合は「-」が出力される。
ICAP_RESPMOD_LOG_SERVER_ID=(デフォルト値:なし) (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携ログに出力するサーバ識別子を設定する。 空の場合は何も出力されない。
ICAP_RESPMOD_DENY_SIZE=0 (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携を除外するHTTPレスポンスのContent-Lengthの値を設定する。 この設定値を超える場合は、連携から除外される。単位はKバイト。 値が"0"以下の場合:値による除外は行わない。 Content-Lengthが存在しないレスポンスの場合、動作はICAP_RESPMOD_DENY_UNKNOWN_SIZEに従い、除外対象にはならない。
ICAP_RESPMOD_DENY_EXTENSION=(デフォルト値:なし) (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携を行わない拡張子を設定する。 「,」(半角カンマ)区切りで、複数指定可能。 設定した値がリクエスト URL のファイル拡張子と完全一致した場合に、連携から除外される。大文字と小文字は区別されない。
ICAP_RESPMOD_DENY_CONTENT_TYPE=video/, audio/ (スタンドアロン版)	スタンドアロン版のみの設定項目。 ウィルスチェック連携を行わないContent-Typeを設定する。 「,」(半角カンマ)区切りで、複数指定可能。 設定した値が HTTP レスポンスの Content-Type と部分一致した場合に、連携から除外される。大文字と小文字は区別されない。
ICAP_RESPMOD_DENY_PERMIT_CATEGORY=FALSE (スタンドアロン版)	スタンドアロン版のみの設定項目。 「許可カテゴリ」に登録されたURLをウィルスチェック連携の対象にするかどうか設定する。 TRUE:例外URLの[許可カテゴリ]-[許可カテゴリ]または[許可カテゴリ]-[閲覧のみ許可]と一致した場合に、連携から除外される。 FALSE:上記のカテゴリと一致しても連携を実施する。

ICAP_CLIENT_TYPE=DEFAULT (ICAP版)	ICAP版のみの設定項目。 連携するICAPクライアントを設定する。 DEFAULT:一般的なICAPクライアントと連携する。 BLUECOAT:BlueCoatと連携する。 SQUID:Squidと連携する。
WEBCONTENTS_CACHE_ENABLE=FALSE （スタンドアロン版）	スタンドアロン版のみの設定項目。 Webコンテンツキャッシュ機能を使用するかを設定する。 TRUE:使用する。 FALSE:使用しない。
WEBCONTENTS_CACHE_MODE=BOTH （スタンドアロン版）	スタンドアロン版のみの設定項目。 Webコンテンツキャッシュのキャッシュ先を設定する。 BOTH:メモリとディスクにキャッシュする。 ONMEMORY:メモリにキャッシュする。 STORAGE:ディスクにキャッシュする。
WEBCONTENTS_CACHE_ONMEMORY_SIZE=64 （スタンドアロン版）	スタンドアロン版のみの設定項目。 Webコンテンツキャッシュが確保して使用するメモリサイズをMバイト単位で設定する。
WEBCONTENTS_CACHE_STORAGE_SIZE=1024 （スタンドアロン版）	スタンドアロン版のみの設定項目。 Webコンテンツキャッシュが確保して使用するディスクサイズをMバイト単位で設定する。
WEBCONTENTS_CACHE_STORAGE_PATH=var/storage_cache （スタンドアロン版）	スタンドアロン版のみの設定項目。 Webコンテンツキャッシュのディスクキャッシュを配置するディレクトリのパスを設定する。
WEBCONTENTS_CACHE_PORT=41211 （スタンドアロン版）	スタンドアロン版のみの設定項目。 Webコンテンツキャッシュ制御を待ち受けるポート番号を1～65535の間で設定する。
WEBCONTENTS_CACHE_PROCESS=16 （スタンドアロン版）	スタンドアロン版のみの設定項目。 Web コンテンツキャッシュ制御を待ち受けるプロセス数を設定する。
WEBCONTENTS_CACHE_STORAGE_PERMIT_MINSIZE=1024 （スタンドアロン版）	スタンドアロン版のみの設定項目。 ディスクへのWebコンテンツキャッシュを許容する最小サイズをバイト単位で設定する。

WEBCONTENTS_CACHE_STORAGE_PERMIT_MAXSIZE=16777216 （スタンドアロン版）	スタンドアロン版のみの設定項目。 ディスクへのWebコンテンツキャッシュを許容する最大サイズをバイト単位で設定する。
WEBCONTENTS_CACHE_ONMEMORY_PERMIT_MINSIZE=1024 （スタンドアロン版）	スタンドアロン版のみの設定項目。 メモリへのWebコンテンツキャッシュを許容する最小サイズをバイト単位で設定する。
WEBCONTENTS_CACHE_ONMEMORY_PERMIT_MAXSIZE=524288 （スタンドアロン版）	スタンドアロン版のみの設定項目。 メモリへのWebコンテンツキャッシュを許容する最大サイズをバイト単位で設定する。
WEBCONTENTS_CACHE_DENY_CONTENT_TYPE=(デフォルト値:なし) （スタンドアロン版）	スタンドアロン版のみの設定項目。 設定した文字列が、レスポンスのコンテンツタイプヘッダの値と完全一致する場合、Webコンテンツキャッシュへの保管を無効化する。 以下のWEBCONTENTS_CACHE_DCT_SEPARATORを区切り文字として複数設定できる。 文字列は完全一致で、ワイルドカード"*"が使用可能。 "*"は一文字以上の文字列と一致する。 "*"は"."を含むすべての文字と一致する。
WEBCONTENTS_CACHE_DCT_SEPARATOR=, （スタンドアロン版）	スタンドアロン版のみの設定項目。 WEBCONTENTS_CACHE_DENY_CONTENT_TYPE の区切り文字。
WEBCONTENTS_CACHE_DENY_EXTENSION=(デフォルト値:なし) （スタンドアロン版）	スタンドアロン版のみの設定項目。 設定した文字列が、リクエスト先 URL の拡張子と完全一致する場合はWebコンテンツキャッシュへの保管を無効化する。 以下のWEBCONTENTS_CACHE_DE_SEPARATORを区切り文字として複数設定できる。
WEBCONTENTS_CACHE_DE_SEPARATOR=, （スタンドアロン版）	スタンドアロン版のみの設定項目。 WEBCONTENTS_CACHE_DENY_EXTENSIONの区切り文字。
WEBCONTENTS_CACHE_DENY_HOST=(デフォルト値:なし) （スタンドアロン版）	スタンドアロン版のみの設定項目。 設定した文字列が、リクエスト先ホストと完全一致する場合はWebコンテンツキャッシュへの保管を無効化する。 以下のWEBCONTENTS_CACHE_DH_SEPARATORを区切り文字として複数設定できる。 文字列は完全一致で、ワイルドカード"*"が使用可能。

WEBCONTENTS_CACHE_DH_SEPARATOR=, （スタンドアロン版）	スタンドアロン版のみの設定項目。 WEBCONTENTS_CACHE_DENY_HOSTの区切り文字。
WEBCONTENTS_CACHE_DENY_USER_AGENT= (デフォルト値:なし) （スタンドアロン版）	スタンドアロン版のみの設定項目。 設定した文字列が、リクエストの User-Agent ヘッダの値と部分一致する場合、Webコンテンツキャッシュへの保管を無効化する。 以下のWEBCONTENTS_CACHE_DUA_SEPARATORを区切り文字として複数設定できる。
WEBCONTENTS_CACHE_DUA_SEPARATOR=, （スタンドアロン版）	スタンドアロン版のみの設定項目。 WEBCONTENTS_CACHE_DENY_USER_AGENTの区切り文字。
WEBCONTENTS_CACHE_DENY_URLPARAM=TRUE （スタンドアロン版）	スタンドアロン版のみの設定項目。 パラメータ付きURLに対するレスポンスについてWebコンテンツキャッシュへの保管を無効化するかを設定する。 TRUE:無効化する。 FALSE:無効化しない。
WEBCONTENTS_CACHE_TEMPORARY_TIME=10 （スタンドアロン版）	スタンドアロン版のみの設定項目。 オリジンサーバが一時的なステータスを返却してきた場合の応答をWebコンテンツキャッシュに一時保管する最大時間を秒単位で設定する。
ICAP_RESPMOD_REENCODE=FALSE （スタンドアロン版）	スタンドアロン版のみの設定項目。 ウィルスチェック連携時の解凍されたレスポンスボディの再圧縮要否を設定する。 TRUE:再圧縮する。 FALSE:再圧縮しない。
ICAP_RESPMOD_KEEPALIVE_TIMEOUT=55000 （スタンドアロン版）	スタンドアロン版のみの設定項目。 ウィルスチェック連携でICAPサーバとの間のKeep-Aliveのタイムアウト時間をミリ秒単位で指定する。 前回の利用からこの時間を経過しているコネクションを再利用する際に再接続を実施する。 -1の場合は本機能は動作しない。
ICAP_RESPMOD_HTTPS_DECODE_ENABLE=FALSE （スタンドアロン版）	スタンドアロン版のみの設定項目。 ウィルスチェック連携の際にHTTPSデコードされたコンテンツを対象とするかを設定する。 TRUE: 対象とする。 FALSE: 対象としない。

B-4. cal.inf

ポリシー適用日付と曜日を以下の書式で記述します。

yyyymmdd,XXX

yyyymmdd	ポリシーを適用したい日付を年月日で登録する。
xxx	短縮形で曜日を指定する。 SUN:日曜日　MON:月曜日　TUE:火曜日　WED:水曜日　THU:木曜日　FRI:金曜日　SAT:土曜日

記述例) 2011/1/1,SUN 2011/5/5,SUN

C. ICAP クライアントでの NTLM 認証

ICAP クライアントが Active Directory にて NTLM 認証をするシングルサインオン環境においてISWMが、ICAPクライアントからユーザを取得し、グループ判別することで、ISWMの認証を必要とせず、シングルサインオンで利用できます。
ICAPクライアントに連携しているコントロールサーバは、ICAPプロトコルのリクエストヘッダ(X-Authenticated-User)に含まれる情報を元に、ユーザのグループ割り当てをします。
コントロールサーバは、ICAPクライアントが連携しているActive DirectoryをLDAPサーバとして指定することにより、アカウントの所属グループを検索します。

1. 設定ファイル proxy.inf の [CONTROL_CFG] セクションに「ICAP_AUTHENTICATION=TRUE」を追加します。ICAP クライアントとして Squid を使用する場合、設定ファイル proxy.inf の [CONTROL_CFG] セクションに、「ICAP_AUTHENTICATION=TRUE」を追加し、さらに ICAP_CLIENT_TYPE キーに「SQUID」を設定します。

ファイルの保存場所

Linux 版＜インストールディレクトリ >/conf/proxy.inf
「ICAP_AUTHENTICATION=TRUE」の追加と「ICAP_CLIENT_TYPE=SQUID」の設定により、ICAP リクエストに含まれる「X-Authenticated-User」の値を認証ユーザとして扱う設定に変更されます。

注意:
- 初期設定では、ICAP_AUTHENTICATION キーは、proxy.inf ファイルに記載されていません。また、ICAP_CLIENT_TYPE キーには「DEFAULT」が設定されています。
- proxy.infファイルにICAP_AUTHENTICATIONキーがない場合やICAP_AUTHENTICATION=FALSE の場合は、ICAP リクエストに含まれる「X-Authenticated-User」の値を認証ユーザとしない設定となります。
- ICAPクライアントとしてSquidを使用する場合、ICAP_CLIENT_TYPEキーの設定が「SQUID」以外の場合は、ICAP リクエストに含まれる「X-Authenticated-User」の値の取得に失敗し、認証エラーとなります。

2. 管理画面から[サーバ管理]-[認証設定]を開き、[LDAP連携を行う]をクリックして[保存]ボタンをクリックします。

3. 管理画面から[サーバ管理]-[LDAPサーバ設定]を開き、ICAPクライアントで指定しているActive Directoryを指定します。

4. [LDAPユーザ同期へ]をクリックして認証するアカウントの選択、またはLDAP自動連携機能を設定します。

これで、初期設定(FALSE)の「ICAPリクエストに含まれる[X-Authenticated-User]の値を参照せず、ISWMの認証を行う」設定が、「ICAPリクエストに含まれる[X-Authenticated-User]の値を認証ユーザとして扱う」設定に変更されます。

注意:
- ICAP_AUTHENTICATION、ICAP_CLIENT_TYPEの記述自体がない場合、初期設定として動作します。
- ユーザ名は、ICAP クライアントから大文字で送信されるため、log に記録されるユーザ名も大文字となります。

D. 利用するポート

ISWM は、管理画面サービスやプライマリサーバ、レプリカサーバとの同期などのサービスを提供するために、以下のポートを使用しています。
プライマリサーバとレプリカサーバの同期がうまくできない場合、端末側でファイアウォール(Windowsファイアウォールなど)を設定している場合はオフにするか、例外登録してください。
管理画面用ポートは、管理画面の[サーバ管理]-[サーバ設定]の[管理画面設定]で設定できます。

注意: proxy.inf でポート番号を変更した場合は、amsdata -sys コマンドを実行して変更を反映してください。
コマンドの実行後、プライマリサーバおよびレプリカサーバの管理サービス、拡張Webサービス、フィルタリングサービスを再起動してください。

ポート名	設定箇所	ポート番号
管理サービス用ポート	proxy.infにキーを追加することで変更できます。※4	41212
データ同期用ポート		41213
フィルタリングサービス制御用ポート		41214 41215
フィルタリングサービス内部処理用ポート		41216
キャッシュデータ制御用ポート	[SYSTEM_GLOBAL] CACHE_PORT	5963
管理画面用ポート※1	[SYSTEM_GLOBAL] WWW_ADMIN_PORT	2319
HTTPポート(スタンドアロン版)※2	[PROXY_PORT] HTTP	8080
HTTPSポート(スタンドアロン版)※2	[PROXY_PORT] HTTPS	8443
FTP OVER HTTPポート(スタンドアロン版)※2	[PROXY_PORT] FTP_OVER_HTTP	8021
HTTPS透過プロキシポート	[PROXY_PORT] TRANSPARENT_HTTPS	8443
ICAPポート※2	[CONTROL_CFG] PORT	1344

ポート名	設定箇所	ポート番号
Webコンテンツキャッシュ制御待受ポート	[CONTROL_CFG] WEBCONTENTS_CACHE_PORT	41211
HTTP規制画面出力用ポート(ICAP版)※3	[CONTROL_CFG] BLOCK_FILE_PORT	21128
HTTPS規制画面出力用ポート(ICAP版)	system.infにキーを追加することで変更できます。※5	443
アクセスログエージェントポート	[SERVICE_OBSERVE] LOG_ANALYZE_AGENT_PORT	41210
集計データベースサービスポート	[SERVICE_OBSERVE] LOG_ANALYZE_DB_PORT	41209
管理画面停止用ポート	• Windows の場合 ＜インストールフォルダ＞¥lib¥server.xml.template ＜インストールフォルダ＞¥tomcat¥conf¥server.xml • Linux の場合 ＜インストールディレクトリ＞/lib/server.xml.template ＜インストールディレクトリ＞/tomcat/conf/server.xml	8005

※1　管理画面の[サーバ管理]-[サーバ設定]の[管理画面設定]でも設定できます。
※2　管理画面の[サーバ管理]-[サーバ設定]の[フィルタリングサービス設定]でも設定できます。
※3　管理画面の[共通アクセス管理]-[規制画面設定]の[規制画面表示サービス設定]でも設定できます。
※4　管理サービス用ポートは、proxy.infの[SYSTEM_GLOBAL]セクションに「ADMIN_PORT=41212」を追加すると変更できます。
この場合、データ同期用ポートはADMIN_PORTの設定値に+1した値、フィルタリングサービス制御用ポートは ADMIN_PORT の設定値に +2、+3 した値になります。フィルタリングサービス内部処理用ポートはADMIN_PORTの設定値に+4した値になります。
※5　system.infの[BLOCK_CFG]セクションに「BLOCK_HTTPS_PORT=443」を追加すると変更できます。

E. HTTPS プロトコルで管理画面を使用する

HTTPSプロトコルで管理画面を使用する場合の設定方法について説明します。

注意:
- レプリカサーバを使用している場合、レプリカサーバでも同様の設定を行ってください。
- 管理画面のポート番号は、LogLyzer　との通信にも使用しています。ポート番号を変更した場合は、LogLyzer側での設定も変更してください。

1. keytool コマンドを実行し、証明書を発行します。

「-keystore」の後に証明書を保存するファイル名を記述します。

- Windowsでの実行例
  ＜インストールフォルダ＞¥jre¥bin¥keytool -genkey -alias tomcat -keyalg RSA -keystore ＜インストールフォルダ＞¥tomcat¥.keystore
- Linuxでの実行例
  ＜インストールディレクトリ＞/jre/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore ＜インストールディレクトリ＞/tomcat/.keystore

注意:
- keytool コマンドは改行せず、1 行で入力してください。
- ここで作成される証明書は正規の証明書ではありません。そのため、ブラウザ上の証明書の情報では「信頼されていません」と表示されますが、動作には問題ありません。
- keytool コマンドの詳細については、下記の URL を参照してください。
  - Windows の場合
    https://docs.oracle.com/javase/jp/7/technotes/tools/windows/keytool.html
  - Linux の場合
    https://docs.oracle.com/javase/jp/7/technotes/tools/solaris/keytool.html

2. 証明書に必要な項目を設定します。

- キーストアのパスワード(例:password)
- 姓名(例:Your Name)
- 組織単位名(例:Develop)
- 組織名(例:NetSTAR)
- 都市名または地域名(例:Shibuya)
- 都道府県名(例:Tokyo)
- この単位に該当する2文字の国番号(例:JP)

設定が完了すると、手順 1 で「-keystore」の後に指定したファイル名で証明書が作成されます。

- Windowsでの実行例
  <インストールフォルダ>¥tomcat¥.keystore
- Linuxでの実行例
  <インストールディレクトリ>/tomcat/.keystore

3. 拡張Webサービスのテンプレート設定ファイルをテキストエディタなどで開きます。

拡張 Web サービスのテンプレート設定ファイルは次のフォルダ / ディレクトリに格納されています。念のため、変更前にバックアップを取ることをお勧めします。

- Windowsの場合
  <インストールフォルダ>¥lib¥server.xml.template.https
- Linuxの場合
  <インストールディレクトリ>/lib/server.xml.template.https

4. テンプレート設定ファイルを変更します。

次の項目を変更します。

- 手順1で作成した証明書ファイルのパスを指定する。
  - Windows での設定例
    keystoreFile="<インストールフォルダ>¥tomcat¥.keystore"
  - Linux での設定例
    keystoreFile="<インストールディレクトリ>/tomcat/.keystore"
- 手順2で作成した証明書のパスワードを設定する。
  - 設定例
    keystorePass="password"

5. テンプレート設定ファイル(「server.xml.template.https」)を「server.xml.template」として上書きします。

   念のため、上書きする前にオリジナルの「server.xml.template」のバックアップを取ることをお勧めします。

6. 設定ファイル(proxy.inf)を変更します。

   - [CONNECTION_CFG]セクションに「USE_WWW_CONNECT_SSL=TRUE」を追加します。
   - [SYSTEM_GLOBAL]セクションに「WWW_ADMIN_HTTPS_PORT」を追加し、HTTPSプロトコルで使用するポート番号を指定します。
     ポート番号を指定しない場合、デフォルト値として2443が設定されます。
     WWW_ADMIN_HTTPS_PORT=2443(設定例)
   - スタンドアロン版およびICAP版で、フィルタリングサーバ経由で接続する場合は[ACCESS_CTRL]セクションの「HTTPS_ACCESS_PORT」に、HTTPSプロトコルで使用するポート番号を追加します。ポート番号は半角スペースで区切ってください。
     HTTPS_ACCESS_PORT=443 2443(設定例)
   - ICAP版の場合は、SquidおよびICAP側でHTTPSプロトコルに使用するポート番号を開放してください。

7. 「amsdata -sys」コマンドを実行し、設定ファイル(proxy.inf)の変更内容を反映します。

8. プライマリサーバのフィルタリングサービスと拡張Webサービスを再起動します。

   - レプリカサーバを使用している場合、全レプリカサーバのフィルタリングサービスを再起動してください。
     プライマリサーバ、全レプリカサーバのフィルタリングサービスは、管理画面の[サーバ管
     理]-[サーバ設定]で再起動できます。
   - 拡張Webサービスは、「amsweb restart」コマンドで再起動してください。

9. HTTPSプロトコルで管理画面にアクセスします。

プライマリサーバの IP アドレスが 192.168.1.1、HTTPS プロトコルで使用するポート番号を 2443 に設定した場合、次の URL で管理画面にアクセスします。
https://192.168.1.1:2443/index.html

注意:
- HTTP プロトコルでは管理画面に接続できません。
- HTTPS プロトコルで管理画面に接続するように設定している場合、設定ファイルを残してアンインストールしても、管理画面用の設定箇所は削除されます。
  必要に応じて、以下の 2 つのファイルをバックアップしておき、再インストール後に手動で復元してください。
  - Windows の場合
    <インストールフォルダ>¥tomcat¥.keystore
    <インストールフォルダ>¥lib¥server.xml.template
  - Linux の場合
    <インストールディレクトリ>/tomcat/.keystore
    <インストールディレクトリ>/lib/server.xml.template

F. バージョンアップインストールについて

ISWMをインストールする環境に、旧バージョンのISWM(Service Pack含む)がインストールされている場合、バージョンアップインストールが実行されます。

注意:
- バージョンアップインストールは、ISWM 8.0 以降がインストールされている環境の場合に行うことができます。
- インストール先に旧バージョンの設定ファイルが存在するディレクトリを指定した場合は、バージョンアップインストールが実行されます。

F-1. バージョンアップ時の注意事項

- ISWM 8.0 以降がすでにインストールされている場合、設定ファイル、ログファイル、ダウンロードしたデータベースファイルがすべて引き継がれます。

注意: ISWM 8.0以降からISWM 9.1にバージョンアップした場合、データベースファイルは引き継がれますが、管理画面ではバージョンや日付がすべて「0」で表示されます。

- ログファイルのバックアップ時に、ログファイルが大量に保存されている場合、保存されている容量に応じたハードディスクの空き容量が必要になります。ログファイルが大量に保存されている場合には、バージョンアップを行う前に、ログを別のディレクトリに移動してください。
- ISWM 9.1SP1 以前と ISWM 9.1SP2 以降では、キャッシュサーバログのフォーマットが異なり、旧バージョンのログに追記で保存することはできません。このため、バージョンアップインストール時に、ISWM 9.1SP1 以前のキャッシュサーバログファイル(cache)のバックアップを行います。

F-2. 保存された設定ファイルを使って、ISWM 9.1をインストールする

旧バージョンの設定ファイルを残して、ISWM がアンインストールされている環境の場合、設定ファイルをコンバートしてISWM 9.1をインストールできます。

注意: コンバートに失敗すると、ログに出力します。エラーの内容はインストールディレクトリのupdate.logに保存されます。

■ 設定が引き継がれる内容

旧バージョンの次の設定が引き継がれます。

- 設定ファイル
  インストール前の設定ファイルを＜インストールディレクトリ＞/backup/conf_v**_＜コンバートした時刻＞ディレクトリにバックアップします。** には 80、85 などのバージョン数が入ります。
  なお、インストール直後の proxy.inf のバックアップとして、同じディレクトリに「proxy.inf.default」を保存します。
- ログファイル
  - ISWM 9.1SP2以降の場合
    インストール前のログファイルをそのまま使用します。
  - ISWM 8.0～9.1SP1の場合
    インストール前のキャッシュサーバログファイル（cache）を<インストールディレクトリ>/backup/logs_v**_<コンバートした時刻>ディレクトリにバックアップします。**には85、90などのバージョン数が入ります。
- データベースファイル
  インストール前のデータベースファイルをそのまま使用します。

F-3. レプリカサーバのバージョンアップインストールについて

プライマリサーバと複数のレプリカサーバで運用している場合は、それぞれのサーバでバージョンアップ作業を行う必要があります。
バージョンアップ作業前に管理画面でレプリカサーバを削除する必要はありません。

注意: 異なるバージョンまたはビルド番号のプライマリサーバおよびレプリカサーバが混在していると、同期に失敗する場合があります。
プライマリサーバとすべてのレプリカサーバが同一バージョンかつ同一ビルド番号になるまでは、管理画面での設定変更をしないでください。

プライマリサーバとレプリカサーバの構成でのバージョンアップは次の手順で行います。

■ プライマリサーバのサービスを停止させてから順次バージョンアップさせる場合

プライマリサーバのサービスを停止させた後にバージョンアップ作業を行うことで、異なるビルド番号のサーバ間で、設定が同期されないようにします。

1. プライマリサーバの全サービスを停止させます。
   サービスの起動 / 停止手順については、「ISWM の起動と停止」(28 ページ)を参照してください。
2. すべてのレプリカサーバについて、バージョンアップと全サービスの起動を行います。
3. プライマリサーバをバージョンアップします。
4. プライマリサーバの全サービスを起動させます。
5. すべてのサーバのデータベースを更新します。
   [サーバ管理]-[データベース設定] より、[データベース更新] ボタンをクリックします。

注意: データベースのダウンロードが完了するまでは、フィルタリング機能が有効となりません。

■ できる限りサービスを停止せずにバージョンアップさせる場合

管理画面での操作を一切行わないことで、異なるビルド番号のサーバ間で、設定が同期されないようにしながらバージョンアップ作業を行います。

1. 管理画面からログアウトします。
2. すべてのレプリカサーバについて、バージョンアップと全サービスの起動を行います。

   サービスの起動 / 停止手順については、「ISWM の起動と停止」(28 ページ)を参照してください。
3. コマンド実行により、すべてのレプリカサーバのデータベースを更新します。

   プライマリサーバ上で amsdatabase コマンドを実行することにより、レプリカサーバのデータベースを更新します。

   ```
   amsdatabase -download -target [サーバ番号]
   ```

   [サーバ番号] は、amsserver コマンドを実行して表示される情報の一番左に表示される番号です。

   amsserver表示例)

   ```
   0 プライマリサーバ(Master) build1601 192.168.60.1 ---- running
   1 レプリカサーバ１ 192.168.60.2 failed starting
   2 レプリカサーバ２ 192.168.60.3 failed running
   3 レプリカサーバ３ 192.168.60.4 failed stop
   ```

   amsdatabase コマンドについては、「amsdatabase[URL データベース管理]」(412 ページ)を参照してください。

   amsserver コマンドについては、「amsserver[サーバ情報表示]」(420 ページ)を参照してください。
4. プライマリサーバをバージョンアップします。
5. プライマリサーバの全サービスを起動させます。
6. コマンド実行により、プライマリサーバのデータベースを更新します。

   プライマリサーバ上で amsdatabase コマンドを実行します。

   ```
   amsdatabase -download -target 0
   ```

F-4. 設定の保存/復旧を使ったバージョンアップ

ISWM 8.5以降では、異なるOS間での設定の保存/復旧をサポートしています。
そのため、次の手順を実行することで異なるOS間でバージョンアップができます。

1. 旧 OS で ISWM 9.1 にバージョンアップします。
2. 設定の保存を実行して、ファイルに保存します。
3. 新OSにISWM 9.1をインストールします。
4. 設定の復旧を実行して、手順2で保存したファイルを指定します。

F-5. ISWM 9.1を使ったプログラム更新

ISWM 9.1では、同一バージョンからのアップデートインストールをサポートしています。そのため、プログラムを更新する場合はISWM 9.1がインストールされている状態でISWM 9.1をインストールしてください。

注意: 本機能により、設定ファイル、ログファイル、データベースファイル、バックアップファイルを除いたファイルおよびフォルダは、フォルダごと削除された後に再構成されます。そのため、上記以外のフォルダを保持したい場合は、バックアップを取る必要があります。

G. 証明書のインストール

[共通アクセス管理]-[HTTPS規制設定]で、[サーバデコード方式]-[HTTPSデコード]のチェックボックスをオンにした場合や、HTTPSサイトに対する規制画面を表示する場合は、ブラウザの証明書警告画面が表示されますので、Microsoft Edge、Firefox、Chromeに、本製品の管理画面からダウンロードした証明書をインストールしてください。

注意: 証明書のインストールは、クライアント側で使用しているすべてのブラウザで実施してください。

証明書のインストール方法について説明します。

G-1. Microsoft Edgeに証明書をインストールする

Microsoft Edgeに証明書をインストールする方法を説明します。

注意: 以下の手順は、Microsoft Edgeバージョン98を例として説明します。

1. 任意のディレクトリに証明書ファイル ([共通アクセス管理]-[HTTPS 規制設定] の [認証局設定]-[認証局証明書] からダウンロード) を格納します。

   規制画面からダウンロードすることもできます。

2. Microsoft Edgeを起動して、画面右上の[設定など]をクリックし、[設定]を選択します。

   [設定] 画面が表示されます。

3. 画面左上の[設定 メニュー]をクリックし、[プライバシー、検索、サービス]を選択します。

4. [セキュリティ]-[証明書の管理]の右側のアイコンをクリックします。

   [証明書] 画面が表示されます。

5. [信頼されたルート証明機関]タブをクリックします。

   [信頼されたルート証明機関] タブが表示されます。

6. [インポート]ボタンをクリックします。

   [証明書のインポートウィザード] 画面が起動します。

7. [次へ]ボタンをクリックします。

   [インポートする証明書ファイル] 画面が表示されます。

8. [参照]ボタンをクリックして手順1で格納した証明書を選択し、[次へ]ボタンをクリックします。

   [証明書ストア] 画面が表示されます。

9. [証明書をすべて次のストアに配置する]ラジオボタンがオンで、[証明書ストア]フィールドに「信頼されたルート証明機関」が表示されていることを確認し、[次へ]ボタンをクリックします。

   [証明書のインポート　ウィザードの完了] 画面が表示されます。

10. [完了]ボタンをクリックします。

    [セキュリティ警告] 画面が表示されます。

11. [はい]ボタンをクリックし、インポート完了ダイアログで[OK]ボタンをクリックします。

    [証明書] 画面に戻ります。

12. 「InterScanWebManager Service CA」が追加されていることを確認して、[閉じる]ボタンをクリックします。

以上で、Microsoft Edgeへの証明書インストールは完了です。

G-2. FireFoxに証明書をインストールする

FireFoxに証明書をインストールする方法を説明します。

注意: 以下の手順はFireFox 97を例として説明します。

1. 任意のディレクトリに証明書ファイル ([共通アクセス管理]-[HTTPS 規制設定] の [認証局設定]-[認証局証明書] からダウンロード) を格納します。

   規制画面からダウンロードすることもできます。

2. FireFoxを起動して、メニューバーの[ツール]から[設定]を選択します。

   画面右上の [メニュー] アイコン をクリックし、[設定] を選択しても表示できます。
   [設定] タブが表示されます。

3. [プライバシーとセキュリティ]の項目より、[証明書]の[証明書を表示]ボタンをクリックし

ます。

[証明書マネージャ] 画面が表示されます。

4. [認証局証明書]タブの[インポート]ボタンをクリックします。

5. 手順1で格納した証明書を選択して、[開く]ボタンをクリックします。

   [証明書のインポート] ダイアログが表示されます。

6. [この認証局によるウェブサイトの識別を信頼する]チェックボックスをオンにして、[OK]ボタンをクリックします。

7. [OK]ボタンをクリックし、[証明書マネージャ]画面を閉じます。

8. 再度[証明書を表示]ボタンをクリックします。

9. 証明書名と発行者名に「Trend Micro Inc.」が表示されていることを確認して、[OK]ボタンをクリックします。

以上で、FireFoxへの証明書インストールは完了です。

G-3. Chromeに証明書をインストールする

Chromeは、Microsoft Edgeにインストールした証明書を参照します。

H. HTTPS デコード機能を有効にしたときの注意事項

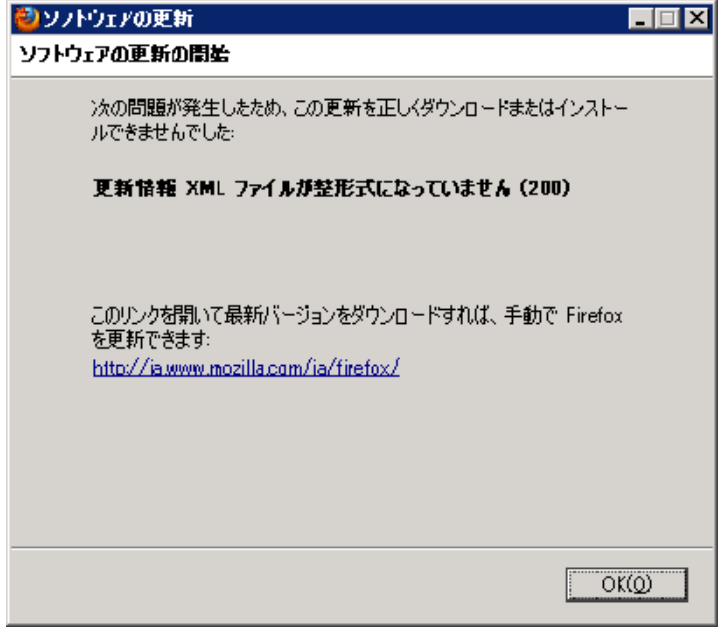
[共通アクセス管理]-[HTTPS 規制設定]で、[サーバデコード方式]-[HTTPS デコード]を有効にした場合、使用するブラウザによって表示されるエラーメッセージと、これらのエラーを回避する方法について説明します。

H-1. Firefox をブラウザに使用している場合

Firefox をブラウザに使用している場合、自動更新を含むソフトウェアやアドオンを更新するときに、エラーが発生します。

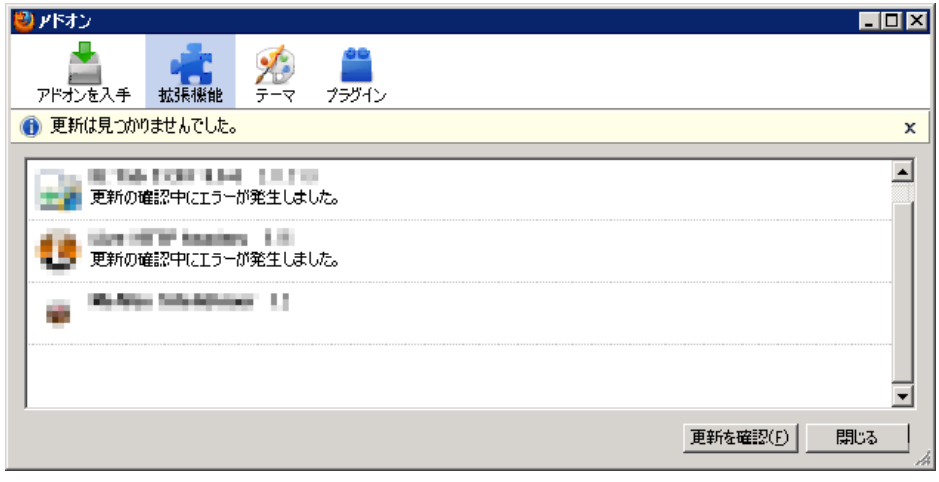
■ソフトウェアの更新確認 (自動更新含む) 時のエラー

[ヘルプ]→[ソフトウェアの更新を確認]を実行するとエラーが発生し、次のメッセージが表示されます。さらに、Firefox 自身の自動更新機能も使用できなくなります。



■アドオンの更新時のエラー

[ツール]→[アドオン]を実行すると、エラーが発生します。さらに、Firefox 自身の自動更新機能も使用できなくなります。



■回避方法

[共通アクセス管理]-[HTTPS 規制設定] で、[サーバデコード方式]-[除外ホスト設定] から「aus2.mozilla.org」と「versioncheck.addons.mozilla.org」を[登録]してください。

注意: アドオンの種類によっては、上記の設定だけでは回避できません。

H-2. クライアント証明書を必要とするサイトへのアクセスについて

クライアント証明書を必要とするサイトへアクセスする場合、HTTPS 通信時にエラーが発生します。
このような場合は、該当サイトを除外ホストに設定してください。

I. IPv6 アドレスの対応

ISWMでは、次の設定がIPv4アドレスまたはIPv6アドレスに対応しています。

- ユーザ (クライアント PC) の設定
- 例外 URL の設定
- HTTPS デコード対象ホストの設定
- フィルタリングサービスの上位プロキシサーバの設定
- データベースダウンロードの上位プロキシサーバの設定

IPv6アドレスに関連する機能は、次のとおりです。

I-1. ユーザ(クライアントPC)の設定

■ユーザの登録・変更

ユーザをIPアドレスで登録・変更する場合、IPv4アドレスとIPv6アドレスで設定できます。
ユーザの登録・変更方法の詳細については、「4-2. IPアドレスを登録する」(140ページ)または、「4-6. IPアドレス/アカウントを変更する」(145ページ)を参照してください。

■IP アドレスユーザの一括操作

IPアドレスユーザを、一括登録画面から登録/削除する場合、またはamsipコマンドを使用して、追加/削除/変更する場合、指定するCSVファイルにIPv6アドレスを記述することができます。
ユーザの一括登録/削除方法の詳細については、「5. ユーザ、グループ情報の一括登録、削除」(152ページ)または、「A-5. amsip[IPアドレスユーザの管理]」(392ページ)を参照してください。

注意:
- IPv6アドレスは、フル形式または省略形式で設定できます。
- IPv6アドレスをフル形式で入力した場合、省略形式として登録されます。
  IPv6 アドレス「2001:0db8:0000:0000:0000:0000:0002:0000」を登録する場合、以下のどちらかの形式で登録できます。
  フル形式:2001:0db8:0000:0000:0000:0000:0002:0000
  省略形式:2001:db8::2:0
  フル形式とは、IPv6 アドレスを省略せずに 128 ビットで記述することを意味しています。

I-2. 例外URLの設定

■例外 URL の登録・変更

例外URLをIPアドレスで登録・変更する場合、IPv4アドレスとIPv6アドレスで設定できます。
例外URLの登録・変更方法の詳細については、「例外URLを設定する」(231ページ)または、「例外URLを変更する」(242ページ)を参照してください。

■例外 URL の一括操作

例外URLを、一括処理画面からインポートする場合または、amsurlコマンドを使用して、インポートする場合、指定するCSVファイルにIPv6アドレスを記述することができます。
例外URLの一括処理方法の詳細については、「例外URLを一括処理する」(244ページ)または、「A-7. amsurl[例外URL]」(400ページ)を参照してください。

注意:

- 通常URLで登録する場合
  - URL 中の IPv6 アドレスは "[" "]" で囲む必要があります。
  - IPv6 アドレスは、フル形式または省略形式で設定できます。
  - IPv6 アドレスをフル形式で入力した場合、省略形式として登録されます。
- IPアドレスレンジ指定URLで登録する場合
  - URL 中の IPv6 アドレスは "[" "]" で囲む必要があります。
  - IPv6 アドレスは、フル形式または省略形式で設定できます。
  - IPv6 アドレスをフル形式で入力した場合、省略形式として登録されます。
    例外 URL に「http://[2001:0db8:0000:0000:0000:0000:0002:0000]」を登録する場合、以下のどちらかの形式で登録できます。
    フル形式:http://[2001:0db8:0000:0000:0000:0000:0002:0000]
    省略形式:http://[2001:db8::2:0]
- ワイルドカードを使ってURLで登録する場合
  - URL 中の IPv6 アドレスは "[" "]" で囲む必要があります。
  - ドメイン部分にワイルドカード (*) を使用する場合は、フル形式でのみ設定できます。
  - ドメイン部分にワイルドカード (*) を使用しない場合は、フル形式または省略形式で設定できます。
    例外 URL にワイルドカード (*) を使って「http://[2001:0000:0000:0012:0000:0060:0007:8000]」を登録する場合
    登録可:http://[2001:0000:0000:0012:*:006*:0007:8*]
    登録不可:http://[2001::12:*:6*:7:8*]

I-3. HTTPSデコード対象ホストの設定

HTTPSデコード対象ホストをIPアドレスで登録・変更する場合、IPv4アドレスとIPv6アドレスで設定できます。
HTTPS デコード対象ホストの登録・変更方法の詳細については、「HTTPS デコード対象ホストを設定する場合」(190ページ)を参照してください。

I-4. フィルタリングサービスの上位プロキシサーバの設定

フィルタリングサービスの上位プロキシサーバをIPアドレスで登録・変更する場合、IPv4アドレスとIPv6アドレスで設定できます。
フィルタリングサービスの上位プロキシサーバの登録・変更方法の詳細については、「2-3. 新規レプリカサーバを登録する」(43ページ)または、「2-4. サーバの設定を変更する」(45ページ)を参照してください。

I-5. データベースダウンロードの上位プロキシサーバの設定

データベースダウンロードの上位プロキシサーバをIPアドレスで設定する場合、IPv4アドレスとIPv6アドレスで設定できます。
データベースダウンロードの上位プロキシサーバの設定方法の詳細については、「3-1. ダウンロードの設定」(53ページ)を参照してください。

J. SNMP エージェント機能

SNMPプロトコル(バージョン:SNMPv2c)に対応した監視サーバ(SNMPマネージャ)が動作している環境では、SNMPエージェント機能を使用できます。
SNMPエージェント機能を使用することで、監視サーバ(SNMPマネージャ)がISWMの稼動状態を定期的に監視してアラートを発生させたり、レポートを作成することができます。

注意:
- SNMPの通信はUDPを使用します。
- オブジェクト情報を変更するSetRequest、自動的に状態(変更)を通知するTrapには対応していません。
- ISWM 側に SNMP を受け付ける監視サーバ(SNMP マネージャ)を制限する機能はありません。OS の機能やファイアウォールを使って、接続する監視サーバ(SNMP マネージャ)を制限してください。

SNMPエージェント機能を使用するための手順は以下のとおりです。
(1)SNMPエージェントを有効にする
(2)管理サービスを再起動する
(3)SNMPマネージャで監視する
以下に、詳細を説明します。

J-1. SNMPエージェントを有効にする

下記の SNMP エージェントに関する設定ファイルをテキストエディタ等で直接編集し、SNMP エージェントを有効にします。併せて、コミュニティ名とポート番号を設定します。
設定ファイルの保存場所:＜インストールディレクトリ＞/conf/sys/snmp-config.xml

<snmp-config enabled="false">	true: SNMPエージェントを有効にする false: SNMPエージェントを無効にする 初期値は「false」です。
<version>v2c</version>	「v2c」固定です。
<community>public</community>	任意のコミュニティ名を、半角英数字および記号(- _ . , : ; ( ) { } [ ])を使用した64文字以内の文字列で設定します。 初期値は「public」です。
<port>10161</port>	使用するポート番号を設定します(1～65535)。 初期値は「10161」です。

<interval>60000</interval>	状態監視を行う間隔をミリ秒単位で設定します(1以上の値)。 初期値は「60000」(1分間に1回)です。

J-2. 管理サービスを再起動する

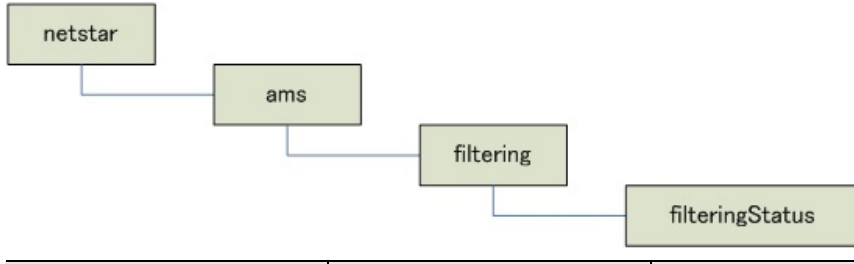
SNMPの設定ファイル(snmp-config.xml)は、管理サービスの起動時に読み込まれます。設定変更後に必ず管理サービスを再起動してください。
管理サービスの再起動については、「6. ISWMの起動と停止」(28ページ)を参照してください。

注意: 設定ファイルの読み込みに失敗した場合や、ポートが開けなかった場合、SNMP エージェント機能は無効になりますが、その他の管理サービスの機能は正常に動作します。

J-3. SNMPマネージャで監視する

SNMPエージェントは定期的にISWMの稼動状態を確認します。監視サーバ(SNMPマネージャ)からSNMPのリクエスト(GetRequest)を受け取ると、次のようなMIBのオブジェクトツリーの値として稼動状態を返します。

オブジェクトツリー



OID	シンボル	状態 (INTEGER)
1.3.6.1.4.1.43320.1.1.1.0	filteringStatus	0:停止中 1:稼動中

稼動状態を受け取った監視サーバ(SNMP マネージャ)側で、適宜、アラートやレポートの設定を行ってください。
ISWMのMIBファイルは次の場所にあります。必要に応じて監視サーバ(SNMPマネージャ)にコピーして使用してください。
MIBファイルの保存場所:<インストールディレクトリ>/conf/ISWM.mib

K. Kerberos 認証使用時の設定例

Kerberos認証を使用する場合の管理画面の設定例と、Active Directoryおよびクライアント側の設定例について説明します。
ここでは下記の環境でActive Directoryが動作している場合を例に説明します。
ドメイン名：meguro.netstar.jp
プライマリサーバのホスト名：sanma1.meguro.netstar.jp

K-1. Kerberosレルム名の設定

[サーバ管理]-[認証設定]の[Kerberos認証設定]でKerberosレルム名を設定します。
下記のようにドメイン名を英大文字で入力します。省略はできません。

```
MEGURO.NETSTAR.JP
```

K-2. サービスプリンシパル名の設定

[サーバ管理]-[認証設定]の[Kerberos認証設定]でサービスプリンシパル名を設定します。

■プライマリサーバおよびレプリカサーバを同一のホスト名で運用する場合

ロードバランサー等を使用してプライマリサーバおよびレプリカサーバをすべて同一の仮想ホスト名で運用する場合は、共通のサービスプリンシパル名を設定します。
[Kerberos認証設定]の[サービスプリンシパル名]で「全体で共通の設定を使用する」をチェックして、「HTTP/ホスト名（FQDN）」または「host/ホスト名（FQDN）」の形式で設定します。

（設定例）

```
HTTP/sanma1.meguro.netstar.jp
```

■プライマリサーバおよびレプリカサーバを異なるホスト名で運用する場合

プライマリサーバおよびレプリカサーバをすべて異なるホスト名やIPで運用する場合は、サーバごとに異なるサービスプリンシパル名を設定します。
下記のようなプライマリサーバおよびレプリカサーバの場合に構成されるサービスサービスプリンシパル名を示します。

（設定例）

```
プライマリサーバ：sanma1.meguro.netstar.jp
サービスプリンシパル名：HTTP/sanma1.meguro.netstar.jp
                        または
                        host/sanma1.meguro.netstar.jp
レプリカサーバ：sanma2.meguro.netstar.jp
サービスプリンシパル名：HTTP/sanma2.meguro.netstar.jp
                        または
                        host/sanma2.meguro.netstar.jp
```

使用するプライマリサーバおよびレプリカサーバごとに、サービスプリンシパル名を設定したキーテーブルファイルをそれぞれ作成します。キーテーブルファイルの作成方法については、「K-3. キーテーブルファイルの作成」(500ページ)を参照してください。
作成後、[Kerberos 認証設定] の [サービスプリンシパル名] で「システムの FQDN を構成する」をチェックして、キーテーブルファイルを登録します。

K-3. キーテーブルファイルの作成

Active Directoryが動作しているサーバにログインして次の作業を行います。
ここではプライマリサーバ（sanma1）の場合を例に説明します。

1. Active Directory に認証用のユーザを作成します。

```
ユーザ名：sanma1user
所属するグループ：OU=sample,DC=meguro,DC=netstar,DC=jp:
パスワード：「パスワードを無期限にする」をチェック
```

2. コマンドプロンプトを管理者として実行します。

3. ダミーのユーザが正しく作成されていることを確認します。

```
setspn -l sanma1user
```

（実行例）

```
次の項目に登録されている
CN=sanma1user,OU=sample,DC=meguro,DC=netstar,DC=jp:
```

4. キーテーブルファイルを作成します。

下記の例では「c:¥」にキーテーブルファイル「sanma1.keytab」が作成されます。

```
ktpass -out c:¥sanma1.keytab -princ HTTP/sanma1.meguro.netstar.jp@MEGURO.NETSTAR.JP +rndPass
-mapuser sanma1user -crypto all -kvno 0 -ptype KRB5_NT_PRINCIPAL
```

※ 上記の例では複数行で記載していますが、1 行で入力する必要があります

（実行例）

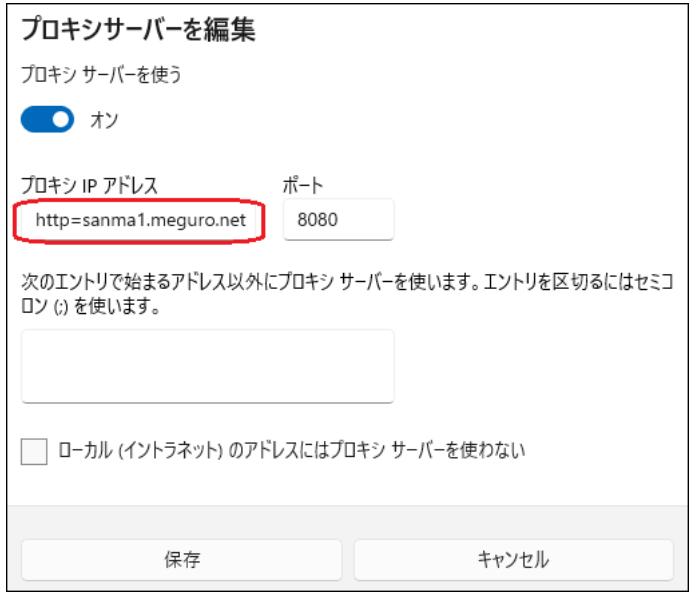
```
Targeting domain controller: adserver1.meguro.netstar.jp
Using legacy password setting method
Successfully mapped HTTP/sanma1.meguro.netstar.jp to sanma1user.
Key created.
Key created.
Key created.
Key created.
Key created.
Output keytab to c:¥sanma1.keytab:
Keytab version: 0x502
keysize 74 HTTP/sanma1.meguro.netstar.jp@MEGURO.NETSTAR.JP ptype 1 (KRB5_NT_PRINCIPAL)
vno 0 etype 0x1 (DES-CBC-CRC) keylength 8 (0x4a9d5104295eb9da)
keysize 74 HTTP/sanma1.meguro.netstar.jp@MEGURO.NETSTAR.JP ptype 1 (KRB5_NT_PRINCIPAL)
vno 0 etype 0x3 (DES-CBC-MD5) keylength 8 (0x4a9d5104295eb9da)
keysize 82 HTTP/sanma1.meguro.netstar.jp@MEGURO.NETSTAR.JP ptype 1 (KRB5_NT_PRINCIPAL)
vno 0 etype 0x17 (RC4-HMAC) keylength 16 (0x2f4500c644c5d37e248e77a0f50f4b41)
keysize 98 HTTP/sanma1.meguro.netstar.jp@MEGURO.NETSTAR.JP ptype 1 (KRB5_NT_PRINCIPAL)
vno 0 etype 0x12 (AES256-SHA1) keylength 32(0x8484e5220031cb50bcbb02d328c3b3a95b728f8945
b1bc963544fcb9ec1c8df8)
keysize 82 HTTP/sanma1.meguro.netstar.jp@MEGURO.NETSTAR.JP ptype 1 (KRB5_NT_PRINCIPAL)
vno 0 etype 0x11 (AES128-SHA1) keylength 16 (0xe3bc6b1a0f105e2128ebd8bb33b5b64c)
```

注意: キーテーブルファイル作成後、[Kerberos 認証設定]の[サービスプリンシパル名]で「システムのFQDN を構成する」をチェックして、キーテーブルファイルを登録します。

K-4. クライアントPCの設定

クライアントPCでのプロキシ設定は、必ずサービスプリンシパル名に設定したホスト名（FQDN）で入力してください。

IPアドレスで入力した場合は、Kerberos認証が正しく行われません。



注意: Kerberos認証ではブラウザから送信されてくるチケットを認証する際にチケットの使用可能期間の確認を行います。クライアントPC、Active Directoryのサーバ、プライマリサーバおよびレプリカサーバの時刻が異なる場合は認証が正しく行われない場合があります。各PCおよびサーバで時刻の同期を行ってください。

K-5. LDAPサーバ設定

管理画面の[サーバ管理]-[LDAPサーバ設定]-[LDAPサーバ情報]の「ドメイン名」は必ずFQDNで入力してください(設定例:meguro.netstar.jp)。

短縮名(meguro)だけを設定すると、Kerberos認証に失敗します。

L. サポートサービス

L-1. サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「スタンダードサポートサービスメニュー」をご覧ください。
サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。サポートセンターの連絡先は、「スタンダードサポート サービスメニュー」に記載されています。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。
サポート契約の有効期限は、ユーザ登録完了から1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意: サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

L-2. 製品Q&A のご案内

トレンドマイクロのWeb サイトでは、製品Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品Q&A には、次のURLからアクセスできます。
https://success.trendmicro.com/jp/technical-support
製品Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme などに記載されていない情報が必要な場合に、製品Q&A を利用してください。
トレンドマイクロでは製品Q&A の内容を常に更新し、新しい情報を追加しています。

M. EU 一般データ保護規則（GDPR）に関する取り組みについて

本製品は、お客さまに関する情報をトレンドマイクロ株式会社および本製品のエンジンおよびデータベースの提供元であるアルプスシステムインテグレーション株式会社に送信する場合があります。
お客さまに関する情報送信についての詳細ならびに送信停止の具体的な方法を、下記のトレンドマイクロのWebサイトにて公開しております。
https://success.trendmicro.com/jp/solution/1120024

索 引

L

N

P

R

S

U

W

あ

か

さ

た

は

ま

や

ら