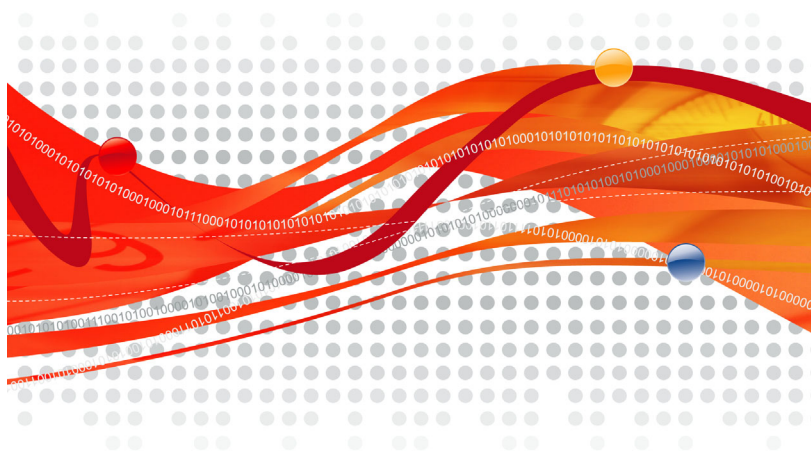


Trend Micro InterScan WebManager™



管理者ガイド

安心を、ひとつ上のステージへ。



本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、GateLock、VSAPI、eDoctor、eManager、Trend Micro Policy Server、トレンドマイクロ・プレミアム・サポート・プログラム、Certified Rescue Partner、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、RBL+、PhishChecker、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWallEnforcer、Trend Flex Security、EPS、Trend Micro EPSは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2001-2008 Trend Micro Incorporated. All rights reserved.

P/N: ISWMFF-AE0300 (2008/3)

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、Solaris 版、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。

目次

マニュアルの構成	3
第 1 章 インストールと使用の準備	13
1. システム運用までの流れ	13
1-1. 基本的な運用	14
2. インストールの流れ	16
2-1.Windows サーバへインストールする	16
2-2.Solaris/Linux サーバへのインストール (ICAP クライアントを利用する場合)	17
2-3.Solaris/Linux サーバへのインストール (Squid を利用する場合)	18
2-4. 複数 サーバでの負荷分散運用	19
3. Windows へのインストール	20
4. Solaris/Linux へのインストール (スタンドアロン版、ICAP 版)	23
5. Solaris/Linux へのインストール (Squid 版)	27
6. ICAP クライアントの設定	35
6-1. NetCache との連携	35
6-2. BlueCoat との連携	41
7. Squid の設定	50
7-1. Squid の設定	50
8. サービスの起動と停止	51
8-1. Windows の場合	51
8-2. Solaris/Linux の場合	52
9. アンインストール	53
9-1. Windows の場合	53
9-2. Solaris/Linux の場合	54

10. 管理画面へのログイン / ログアウト	56
10-1. 管理画面へのログイン	56
10-2. 管理画面からのログアウト	59
11. [ホーム] 画面の各部名称	60
11-1. [ホーム] 画面	60

第 2 章 システムの設定と管理 65

1. [システム管理] 画面でできること	65
2. サーバの設定と登録	68
2-1. サーバ情報を確認する	68
2-2. サーバの起動と停止	69
2-3. 新規スレーブサーバを登録する	70
2-4. サーバの設定を変更する	72
2-5. スレーブサーバを削除する	76
2-6. サーバの設定を同期させる	77
3. データベース / モジュールのダウンロード	78
3-1. ダウンロードの設定	78
3-2. データベース / モジュールをダウンロードする	81
4. 管理画面 / 規制画面の表示設定	83
4-1. 管理画面情報を設定する	83
4-2. 規制画面形式を設定する	84
5. ログファイルの設定	89
5-1. ログファイルの出力設定	89
5-2. システムログの一覧を表示する	93
5-3. 現在のシステムログを閲覧する	96
5-4. ローテート済みシステムログをダウンロード、削除する	97
6. システム設定の保存、復旧	99

6-1. システム設定を保存する	99
6-2. システム設定を復旧する	100
7. メール通知設定	102
7-1. メール通知の設定をする	102
7-2. 通知メールをテスト送信する	104
8. ユーザ認証の設定	105
8-1. ユーザ認証の種類	105
8-2. Basic 認証 (ローカル) を設定する	108
8-3. Basic 認証 (LDAP 連携) を設定する	109
8-4. NTLM 認証を設定する	112
8-5. LDAP サーバの登録と管理	114
8-6. LDAP サーバとの連携を設定する	120
8-7. LDAP サーバと同期する	124
8-8. Active Directory 連携時の LDAP サーバ設定	132
9. フィルタリングルール共通設定	137
9-1. 書き込み規制を設定する	137
9-2. HTTPS 規制を設定する	138
9-3. 規制解除申請を設定する	140
9-4. ユーザ設定カテゴリのサブカテゴリ名を設定する	144

第 3 章 ユーザとグループの管理..... 147

1. グループとユーザについて	147
1-1. グループとユーザ	147
1-2. グループについて	149
1-3. グループとフィルタリング設定	151
1-4. ユーザについて	153
1-5. IP アドレスでユーザを管理する	156

1-6. アカウントでユーザを管理する	159
2. [グループ/ユーザ管理] 画面でできること	162
2-1. [グループ/ユーザ選択] 画面の構成	163
3. グループの登録と管理	166
3-1. グループを登録する	166
3-2. グループの設定を変更、削除する	170
4. ユーザの登録と管理	172
4-1. IP アドレスを登録する	173
4-2. アカウントを登録する	176
4-3. アカウントを検索する	180
4-4. IP アドレス / アカウントを変更する	182
4-5. IP アドレス / アカウントのグループを移動する	184
4-6. IP アドレス / アカウントを削除する	187
4-7. IP アドレス / アカント一覧をファイルに出力する	190
5. ユーザ、グループ情報の一括登録、削除	193
5-1. ファイルのフォーマット	195
6. IP アドレス設定一覧の確認	198

第 4 章 フィルタリングの設定 201

1. フィルタリング設定について	201
1-1. フィルタリングの流れ	201
1-2. フィルタリング機能の概要	204
1-3. フィルタリング設定の参照	211
1-4. スケジュール種別	214
1-5. フィルタリング設定の流れ	216
2. [フィルタリング設定] 画面でできること	219
2-1. グループに適用するフィルタリング設定を作成する	219

2-2. 例外ユーザの登録とフィルタリング設定	222
2-3. 上位グループ参照と下位グループ指定	224
3. カテゴリ別フィルタリングルールの設定	226
3-1. カテゴリ別ルールを登録する	226
3-2. カテゴリ別ルールを変更、削除する	231
4. スケジュールの設定	233
4-1. スケジュール一覧を表示する	233
4-2. スケジュールの基本設定を変更する	235
4-3. スケジュールの時間帯設定を登録する	238
4-4. スケジュールの時間帯設定を変更、削除する	241
4-5. 例外ユーザ用スケジュールを登録する	244
4-6. 例外ユーザ用スケジュールを変更する	246
4-7. 例外ユーザ用スケジュールを削除する	248
5. 例外 URL の設定	250
5-1. 例外 URL を登録する	252
5-2. 例外 URL を変更する	258
5-3. 例外 URL を削除する	260
6. クライアント規制設定	262
6-1. クライアント規制を設定する	262
6-2. ブラウザ規制を設定する	264
7. 規制オプションの設定	270
7-1. オーバーライドの詳細設定	273
7-2. 書き込み規制の詳細設定	274
8. カテゴリ別規制メッセージの設定	277
9. フィルタリング設定の確認	279
10. 例外ユーザのフィルタリング設定	284
10-1. 例外ユーザのフィルタリング設定の流れ	284

10-2. 例外ユーザに登録する	285
10-3. 例外ユーザの登録を解除する	290
11. パス内 URL 規制機能	292
12. URL メモリキャッシュ機能	293
第 5 章 簡易設定	295
1. [簡易設定] 画面でできること	295
1-1. 簡易設定と詳細設定の設定内容	295
1-2. フィルタリングルールの適用	296
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	297
第 6 章 アクセス マネジメント ビューの操作	301
1. Access Management View でできること	301
2. フィルタリング設定の情報漏えいリスクを確認する	304
2-1. 情報漏えいリスクの判定結果を確認する	306
2-2. 情報漏えいリスクの判定方法	311
3. 情報漏えいリスクの確認対象を設定する	314
第 7 章 アクセスログの管理	317
1. [アクセス管理] 画面でできること	317
2. アクセスログの管理	318
2-1. 現在のアクセスログを閲覧する	318
2-2. ローテート済みアクセスログをダウンロード、削除する	321
第 8 章 クライアント PC の設定	323
1. クライアント PC の設定	323
2. Web フィルタリング	325

2-1. 規制画面	326
2-2. オーバーライド	330
2-3. その他の規制	332
3. パスワードの変更	333
4.SSL Access Controller の設定	336
4-1.ISWM との連携設定	337
4-2.SSL Access Controller のインストール	339
4-3.SSL Access Controller のアンインストール	343
 付録.....	 345
A. コマンドラインインタフェース	345
A-1. コマンドの使用方法	345
A-2. amSError.log について	346
A-3. コマンド一覧	347
A-4. amSuser [アカウントの管理]	350
A-5. amSip [IP アドレスユーザの管理]	353
A-6. amSexuser [例外ユーザの管理]	356
A-7. amSgroup [グループ管理]	359
A-8. amSurl [例外 URL]	363
A-9. amSrule [フィルタリングルール管理]	366
A-10. amSSchedule [スケジュール管理]	371
A-11. amSdatabase [URL データベース管理]	376
A-12. amSdata [設定の保存 / 復旧 / 同期]	378
A-13. amSServer [サーバ情報表示]	382
A-14. amSlog [ログファイルのアーカイブ]	384
A-15.amScatMsg [カテゴリ別規制メッセージ管理]	387
A-16. amScontrol [フィルタリングサービスの起動 / 停止]	389

A-17. amsadminstat [スレーブサーバの状態管理]	391
A-18. amsversion [バージョン情報表示]	392
B. 設定ファイル	393
B-1. proxy.inf	395
B-2. cal.inf	410
B-3. sacproxy.ini	410
C. ICAP クライアントでの NTLM 認証	411
D. 利用するポート	413
E. HTTPS プロトコルで管理画面を使用する	415
F. Squid 版で設定を変更する場合の注意事項	419
G. バージョンアップインストールについて	421

インストールと使用の準備

1. システム運用までの流れ

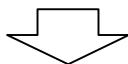
Trend Micro InterScan WebManager (以下、ISWM) の基本的なフィルタリングサービスを利用するには、次の手順に従って製品をインストール、設定してください。

注意： 設定変更の際、マスタサーバとスレーブ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。
複数のスレーブサーバを登録して運用する場合は、スレーブサーバを登録する前に、マスタ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を設定を完了してください。

1-1. 基本的な運用

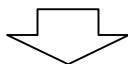
1. ISWM のインストール

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」(13 ページ)



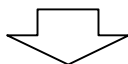
2. 連携する Squid または ICAP の設定 (Squid 版、ICAP 版のみ)

ISWM と連携して動作する Squid または ICAP 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。
Squid 版の場合→「7. Squid の設定」(50 ページ)
ICAP 版の場合→「6-1. NetCache との連携」(35 ページ)または「6-2. BlueCoat との連携」(41 ページ)



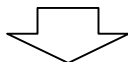
3. URL データベースのダウンロード

管理画面にログインし、URL 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 →「10. 管理画面へのログイン / ログアウト」(56 ページ)
URL データベースのダウンロード →「3. データベース / モジュールのダウンロード」(78 ページ)



4. スレーブサーバの登録 (複数台で運用する場合のみ)

管理画面にログインし、マスタサーバに、連携するスレーブサーバを登録します。
管理画面へのログイン →「10. 管理画面へのログイン / ログアウト」(56 ページ)
スレーブサーバの登録 →「2-3. 新規スレーブサーバを登録する」(70 ページ)

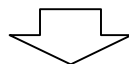


5. システムの設定

ISWM をインストールしたマスタ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。

システムの設定 →「第 2 章 システムの設定と管理」(65 ページ)



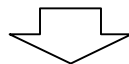
6. グループ / ユーザの登録

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。

ユーザとグループの管理 →「第 3 章 ユーザとグループの管理」(147 ページ)

ユーザ認証の設定 →「8. ユーザ認証の設定」(105 ページ)



7. フィルタリングルールの設定

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」(201 ページ)

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

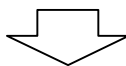
ISWM はご利用になるネットワーク環境や、サーバ OS によってインストール手順が異なります。ISWM 5.0 からバージョンアップする場合、421 ページの「G. バージョンアップインストールについて」を参照してください。

2-1. Windows サーバへインストールする

1. マスタサーバに 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マスタサーバに、ISWM をインストールします。

詳しくは、20 ページの「3. Windows へのインストール」を参照してください。



2. スレーブサーバに ISWM をインストールする (複数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。

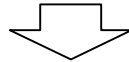
スレーブサーバへインストールする場合はインストール画面でインストールタイプをスレーブサーバに設定し、インストール完了後に管理画面でマスタサーバに登録してください。

2-2. Solaris/Linux サーバへのインストール (ICAP クライアントを利用する場合)

1. マスタサーバに ISWM をインストールする

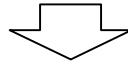
ISWM のシステム設定やグループ / ユーザの管理、フィルタリングの設定をするマスタサーバに、ISWM をインストールします。

詳しくは、23 ページの「4. Solaris/Linux へのインストール (スタンドアロン版、ICAP 版)」を参照してください。



2. ICAP クライアント (BlueCoat、NetCache) の設定をする

35 ページの「6. ICAP クライアントの設定」を参照して ICAP クライアントの設定をしてください。



2. スレーブサーバに ISWM をインストールする (複数で運用する場合のみ)

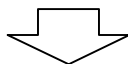
複数のサーバでフィルタリングサービスの負荷を分散して運用する場合は、負荷分散用のサーバにも ISWM をインストールします。

スレーブ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スレーブサーバに設定し、インストール完了後に管理画面でマスタサーバに登録してください。

2-3. Solaris/Linux サーバへのインストール (Squid を利用する場合)

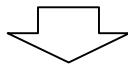
1. マスタサーバに ISWM をインストールする

Squid を利用している Solaris サーバ、または Linux サーバに ISWM をインストールします。
詳しくは、27 ページの「5. Solaris/Linux へのインストール (Squid 版)」を参照してください。



2. Squid の設定をする

50 ページの「7. Squid の設定」を参照して Squid の設定をしてください。



2. スレーブサーバに ISWM をインストールする (複数で運用する場合のみ)

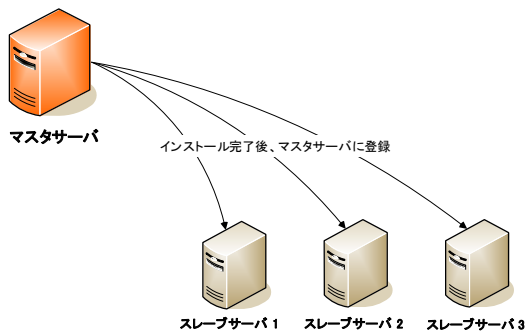
複数のサーバでフィルタリングサービスの負荷を分散して運用する場合は、負荷分散用のサーバにも ISWM をインストールします。

スレーブ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スレーブサーバに設定し、インストール完了後に管理画面でマスタサーバに登録してください。

2-4. 複数 サーバでの負荷分散運用

ISWM では複数のサーバを 1 台のマスタサーバで管理します。マスタサーバとしてインストールするか、スレーブ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、スレーブサーバは、マスタサーバと関連付けられていません。マスタサーバの設定完了後に、必ず ISWM の管理画面からスレーブサーバの登録をしてください。

サーバ構成例



-
- 注意：**
- マスタサーバとすべてのスレーブサーバは、同一の OS で運用してください。
 - インストール完了後は、サーバ種別（マスタサーバ、スレーブサーバ）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、サーバタイプをマスタサーバとしてインストールしたサーバで提供されます。スレーブ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 ISWM 5.0 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おくことをおすすめします。
＜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、421ページの「G. バージョンアップインストールについて」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 CD-ROM を CD-ROM ドライブに挿入し、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、<CD-ROM ドライブ>¥program¥windows¥ にあります。
インストール開始画面が表示されます。

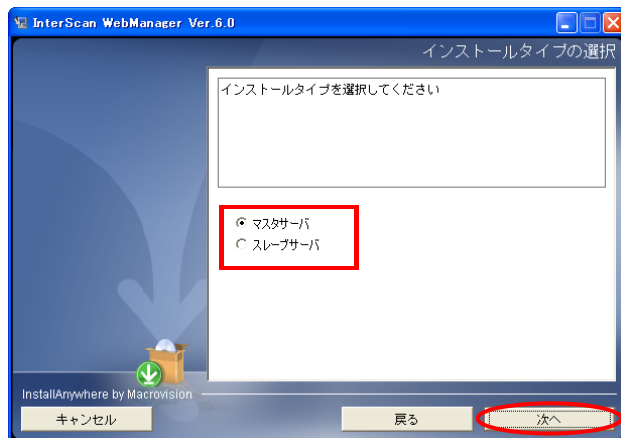
3. [次へ] ボタンをクリックします。
使用許諾契約画面が表示されます。
4. [使用許諾契約の条項に同意する] をクリックして選択し、[次へ] ボタンをクリックします。
使用許諾契約の内容に同意いただけない場合は、[使用許諾契約の条項に同意しない] をクリックしてインストールを中止してください。

5. インストールするフォルダを確認して [次へ] 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。

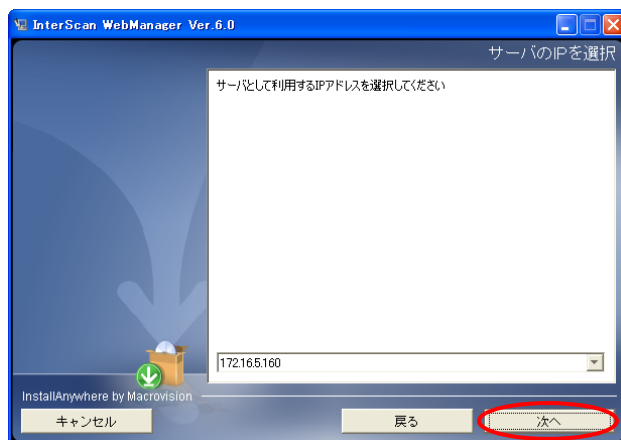
注意： 旧バージョンの ISWM の設定ファイルを引き継ぎたい場合は、旧バージョンがインストールされていたフォルダにインストールしてください。

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。マスタサーバ、スレーブサーバについては、16 ページの「2. インストールの流れ」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： ▪スレーブサーバの場合、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再起動を促すメッセージが表示されます。

9. [完了] ボタンをクリックして Windows を再起動します。

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。

以上で、ISWM のインストールは完了です。

4. Solaris/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。

Solaris または 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 35 ページの「6. ICAP クライアントの設定」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 ISWM 5.0 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おくことをおすすめします。

<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、421 ページの「G. バージョンアップインストールについて」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 CD-ROM 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。

- ・ Solaris <CD-ROM ドライブ>/program/solaris/
- ・ Linux <CD-ROM ドライブ>/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。

- Solaris /opt/iswm
- Linux /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

3- Squid

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マスタサーバとして動作させるか、スレーブサーバとして動作させるかを決定します。「1」(マスタサーバ) または「2」(スレーブサーバ) を入力して <Enter> を押してください。

```
Please select server type
-> 1- Master Server
    2- Slave 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。マスタサーバ、スレーブサーバについては 16 ページの「2. インストールの流れ」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 Master
-> 1- 192.168.11.108
ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

注意：

- ・スレーブサーバの場合、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、ISWM サービスの起動を促す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.** <Enter> を押してインストーラを終了します。

以上で、ISWM のインストールは完了です。

5. Solaris/Linux へのインストール (Squid 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。

Solaris サーバまたは Linux サーバへ ISWM (Squid 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。

インストールが完了したら、続けて 50 ページの「7. Squid の設定」を参照して、連携する Squid 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 ISWM 5.0 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おくことをおすすめします。

＜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、421 ページの「G. バージョンアップインストールについて」を参照してください。

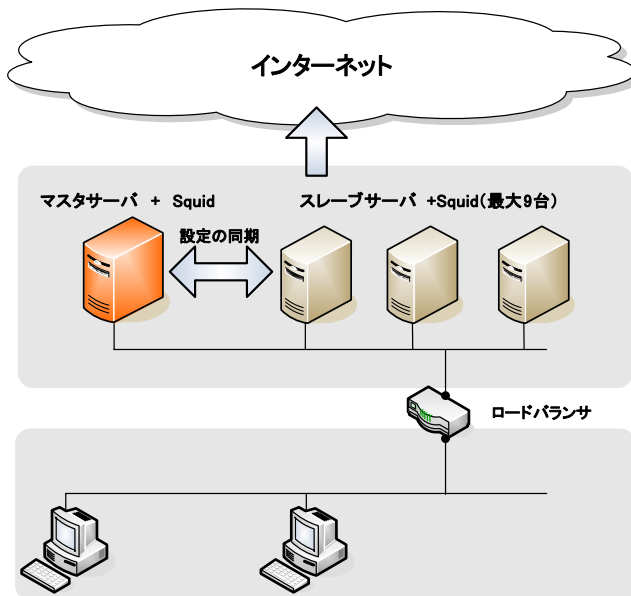
- ISWM を実行する環境には、日本語環境が必要です。日本語表示可能なコンソール、またはウィンドウシステムを使用してください。
-

Squid のインストールタイプとして、リダイレクタプログラムとコントロールサーバプログラムを別々のサーバで運用するオフボックスインストールと、同一のサーバで運用するオンボックスインストールがあります。

■ オンボックスインストールのシステム構成

ISWM のリダイレクトプログラム、コントロールサーバプログラムを Squid と同じサーバにインストールする方法です。この場合、インストールタイプの選択手順では、「All」を選択してください。

オンボックスインストールのシステム構成例

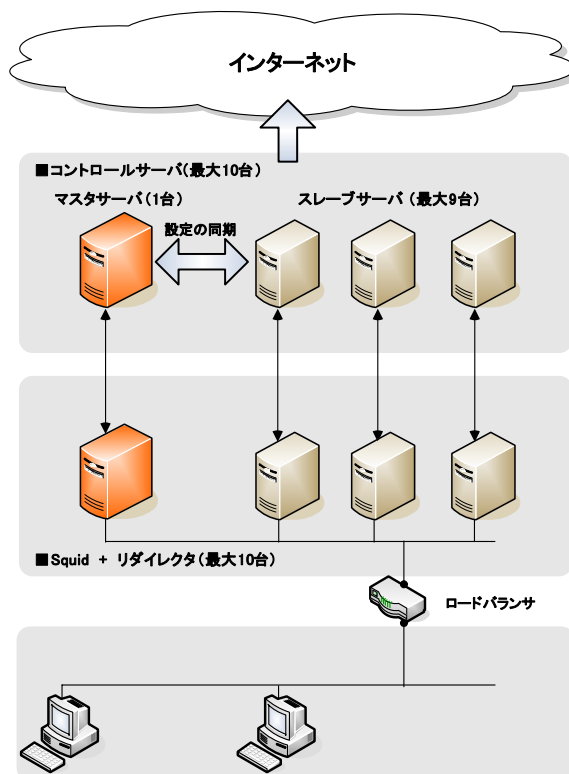


■ オフボックスインストールのシステム構成

ISWM のリダイレクタプログラムを Squid と同じサーバにインストールし、コントロールサーバプログラムを別のサーバにインストールする方法です。

この場合、インストールタイプの選択手順では、「Redirector」または「Control Server」を選択してください。

オフボックスインストールのシステム構成例



注意： オフボックスインストール時に、リダイレクタプログラムとコントロールサーバプログラムを Solaris と Linux などのように別々の OS にインストールして運用することはできません。必ず同一のバージョン、サービスパックの OS で運用してください。

ISWM を新規にインストールする場合、次の手順でインストールしてください。

1. インストール CD-ROM 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。

- Solaris <CD-ROM ドライブ>/program/solaris/
- Linux <CD-ROM ドライブ>/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。

- Solaris /opt/iswm
- Linux /usr/local/iswm

5. 「3」を入力して <Enter> を押します。

Please Choose the Install Set to be installed by this installer.

1- Standalone

2- ICAP

-> 3- Squid

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:

6. インストールタイプを選択して <Enter> を押します。

Please select Installation type

-> 1- Redirector

2- Control Server

3- ALL

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:

Redirector	オフボックスインストール時に、リダイレクタプログラムをインストールするときに選択します。
Control Server	オフボックスインストール時に、コントロールサーバプログラムをインストールするときに選択します。
All	オンボックスインストール時に選択します。

7. 次のメッセージが表示された場合は、Squid の設定ファイル「squid.conf」を絶対パスで指定し、<Enter> を押します。

このメッセージは、手順 6 でインストールタイプとして「Redirector」または「All」を選択した場合に表示されます。squid.conf が初期値の /usr/local/squid/etc/ にある場合、そのまま <Enter> を押してください。

```
Please input the path of squid.conf
path of squid.conf (DEFAULT: /usr/local/squid/etc/squid.conf)
:
```

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。
9. ISWM の設定に必要な IP アドレスを設定して <Enter> を押します。

```
Please select the IP address which it utilizes as the control server
-> 1- 192.168.11.108
ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

設定方法は、手順 6 で選択したインストールタイプによって異なります。

Redirector	コントロールサーバプログラムの稼動するサーバの IP アドレスを入力します。
Control Server または ALL	リダイレクトプログラムが接続可能な NIC (Network Interface Card) を一覧から選択します。

10. 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。

手順 6 でインストールタイプに Redirector を選択した場合、手順 15 に進んでください。

11. 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マスタサーバとして動作させるか、スレーブサーバとして動作させるかを決定します。「1」（マスタサーバ）または「2」（スレーブサーバ）を入力して<Enter> を押してください。

```
Please select server type
-> 1- Master Server
    2- Slave 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。マスタサーバ、スレーブサーバについては 16 ページの「2. インストールの流れ」を参照してください。

12. ISWM 実行ユーザを自動設定するかを選択し、<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:
```

13. 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:
```

14. ISWM を自動起動するかを選択して <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 reisters
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。

15. 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、再起動を促す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。

16. <Enter> を押してインストーラを終了します。

以上で、ISWM のインストールは完了です。

続けて 50 ページの「7. Squid の設定」を参照して、連携する Squid を設定してください。

6. ICAP クライアントの設定

ISWM 6.0 for ICAP をご利用になる場合、ICAP クライアントである NetCache または BlueCoat 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。

6-1. NetCache との連携

ICAP クライアントとして NetCache を利用する場合、ICAP サービスファームの登録と Access Control Lists の設定をしてください。

注意： ISWM を NetCache と連携させて動作させるために NetCache 側で必要な設定をします。
詳しくは NetCache 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と ICAP 設定画面の表示

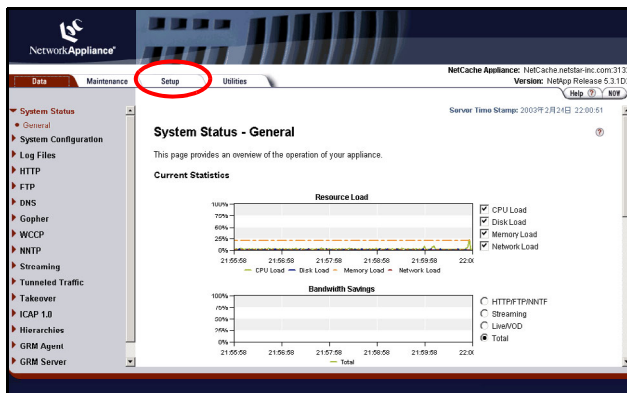
次の手順で NetCache 管理画面にログインして ICAP 設定画面を表示してください。
ここでは、リリース 5.3.1D2 の場合を例に説明します。

1. ブラウザから `http://<netcache-server>:<netcache-adminport>/` にアクセスします。
 - `<netcache-server>` : NetCache 稼動サーバ名 /IP アドレス
 - `<netcache-adminport>` : NetCache 管理画面用ポート番号 (初期設定では 3132)

WWW 認証ダイアログが表示されます。

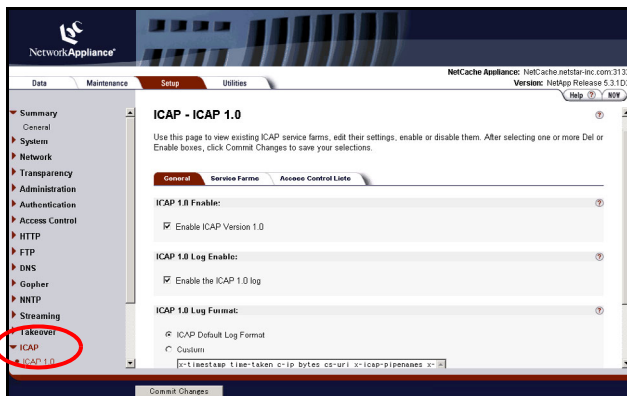
2. NetCache 管理者アカウント、パスワードを入力して [OK] ボタンをクリックします。
NetCache 管理画面が表示されます。

3. 画面上の [Setup] タブをクリックします。



4. 画面左側メニューから [ICAP] をクリックし、表示されたメニューから [ICAP 1.0] をクリックします。

ICAP 設定画面が表示されます。



注意： NetCache の ICAP プロトコル用の設定画面は [General]、[Service Farms] および [Access Control Lists] の 3 つのタブに分けられています。

続けて ICAP サービスファームを登録します。

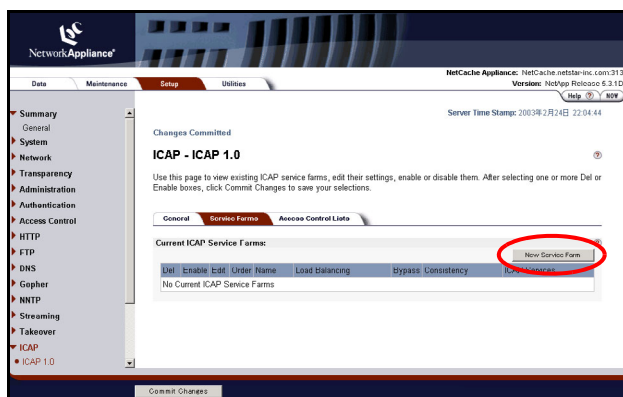
■ ICAP サービスファームの登録

1. ICAP 設定画面から [Service Farms] タブをクリックします。

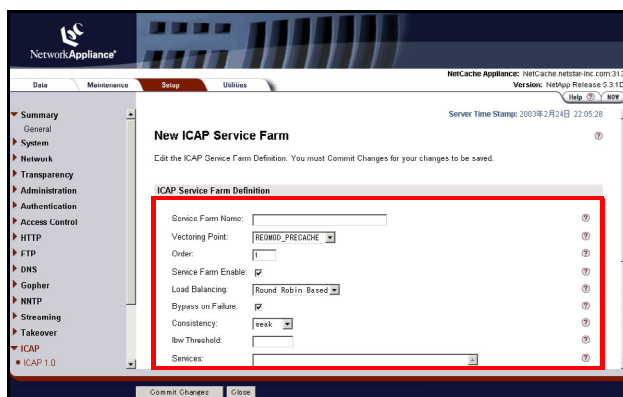
ICAP Service Farms 画面が表示されます。

2. [New Service Farm] ボタンをクリックします。

ICAP サービスファーム登録画面が表示されます。

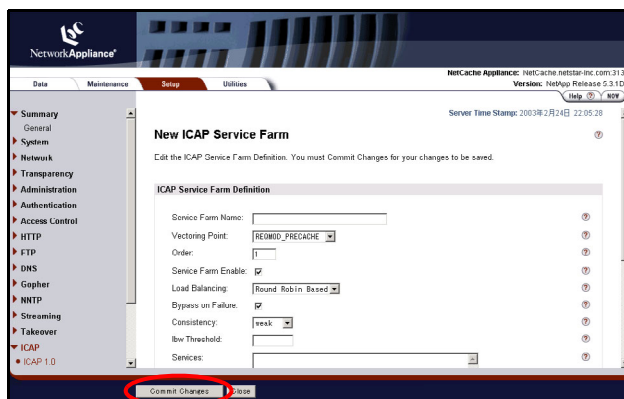


3. ICAP サービスファーム登録画面で、次の項目を設定します。



Service Farm Name	ISWM
Vectoring Point	REQMOD_PRECACHE
Order	1
Service Farm Enable	有効 (チェックボックスをオンにする)
Load Balancing	● ISWM が 1 台の場合 [IP Based] ● ISWM が複数の環境でオーバーライド機能を使用する場合 [IP Based] ● それ以外の場合 [Round Robin Based]
Bypass on Failure	無効 (チェックボックスをオフにする)
Consistency	Weak
Lbw Threshold	空欄にする
Services	環境にあわせて IP アドレス、ホスト名、ICAP ポート番号を指定する 記入例) icap://<ISWM-Server>:<ICAP-Port>/iswm on < ISWM-Server> :ISWM の導入コンピュータの IP アドレス / ホスト名 <ICAP-Port> :LISTEN している ICAP ポート番号 (初期設定は 1344) ※ ICAP サーバを複数構築、または複数のポート番号で LISTEN している場合、[Services] に複数行記述できます。

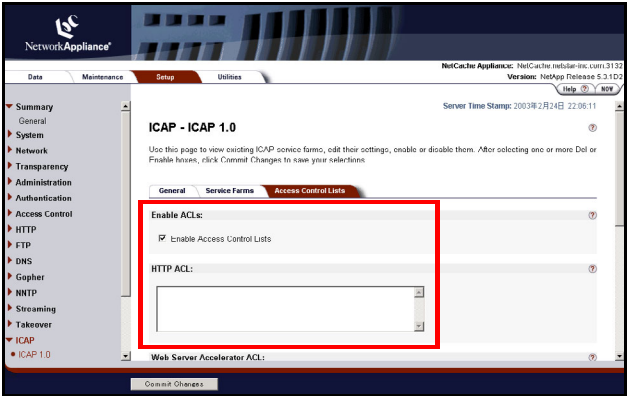
4. 画面下の [Commit Changes] ボタンをクリックして、新規サービスファームを登録します。



続けて Access Control Lists の設定をします。

■ Access Control Lists の設定

1. ICAP 設定画面から [Access Control Lists] タブをクリックします。
Access Control Lists 画面が表示されます。
2. 次の項目を設定します。



Enable ACLs	[Enable Access Control Lists] チェックボックスをオンにする
HTTP ACL	icap(ISWM) any
HTTP-Based Tunneling ACL	icap(ISWM) any
FTP ACL	icap(ISWM) any

3. 画面下の [Commit Changes] ボタンをクリックします。
設定が更新されます。

以上で、ISWM と NetCache の ICAP 連携の設定は完了です。

6-2. 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設定をしてください。

注意： BlueCoat サーバは、SGOS 2.1.06 以上をお使いください。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 2.1.09 の場合を例に説明します。

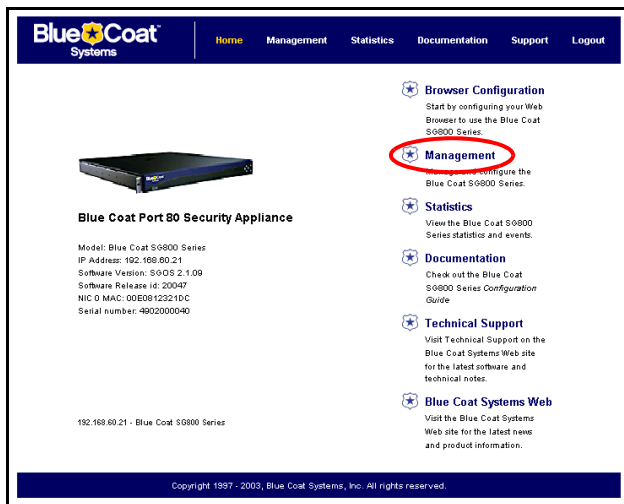
1. ブラウザから `http://<bluecoat-server>:<bluecoat-adminport>/` にアクセスします。

- `<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 8081)

BlueCoat 管理画面が表示されます。

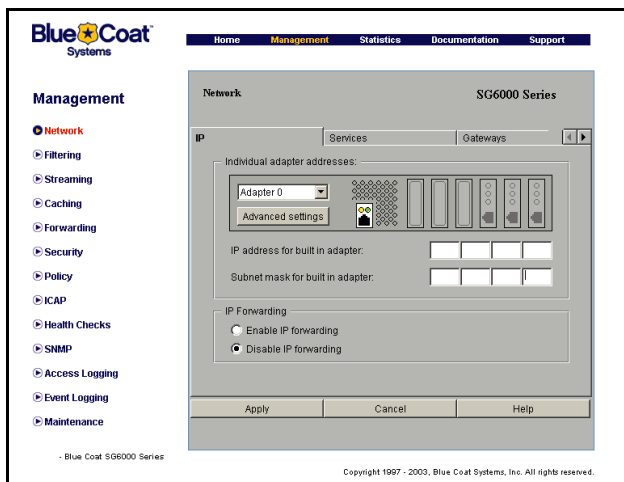
2. [Management] をクリックします。

WWW 認証ダイアログが表示されます。



3. 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。

Management 初期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

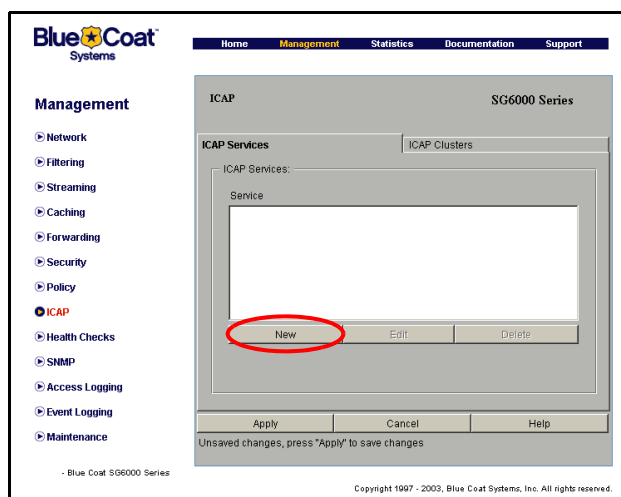
ISWM との連携のために ICAP サービスの登録、ポリシーの設定を行います。ICAP サービスを登録するには、次の手順に従ってください。

1. 画面左のメニューの [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. [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。

Edit ICAP Service ICAP_filtering

ICAP version: 1.0

Service URL:

Maximum number of connections: 5

Connection timeout (seconds): 70

Patience page delay (seconds): 10 ☐ enabled

ICAP v1.0 Options

Method supported: ☒ response modification ☐ request modification

Preview size (bytes): 0 ☒ enabled

Send: ☐ Client address ☐ Server address

ICAP server tag:

Sense settings Get settings from ICAP server

Health Check Options

Register Register the service for health checks

Health check Perform a health check on this service

OK Cancel

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) <code>icap://<ISWM-Server>:<ICAP-Port>/</code> < ISWM-Server> :ISWM for ICAP 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 ※ ICAP サーバを複数構築、または複数のポート番号で LISTEN している場合には、[Services] に複数行記述できます。
Maximum number of connections	75 (初期設定を使用)
Connection timeout(seconds)	75 (初期設定を使用)
Method supported	request modification
Health Checks Options	ICAP サーバを複数構築している場合には、BlueCoat の Health Checks 機能を使用することを推奨します。

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。

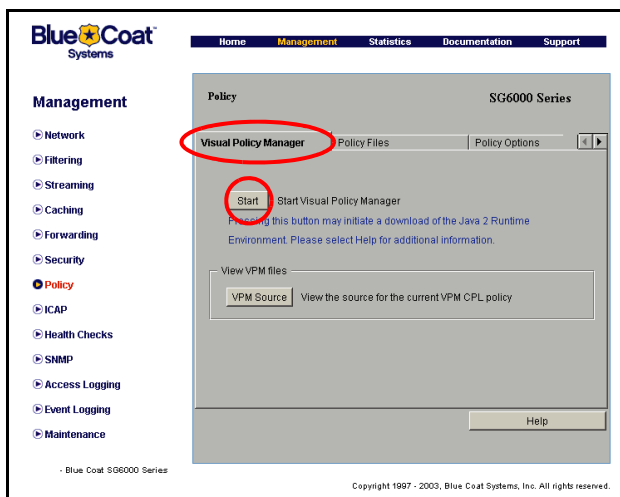
7. [Apply] ボタンをクリックして BlueCoat に設定を反映します。

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。

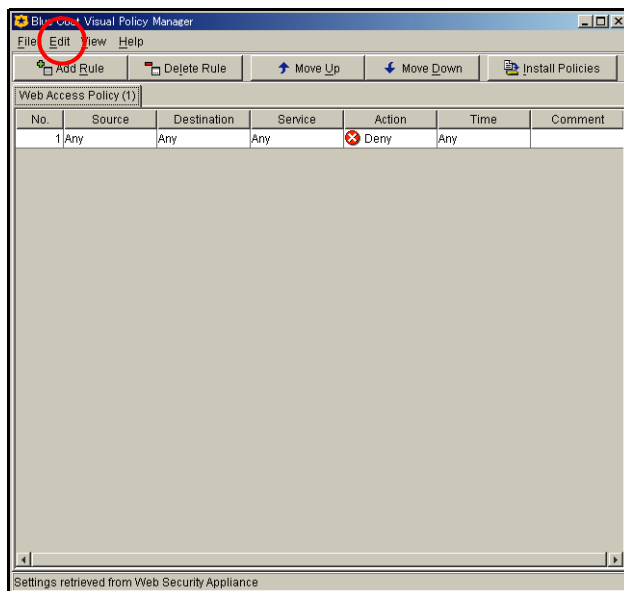
■ ポリシーの設定

1. 画面左のメニューより [Policy] 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、[Start] ボタンをクリックします。
Visual Policy Manager 画面が表示されます。



注意： Visual Policy Manager は署名付きアプレットで実行されるため、証明書の確認ダイアログが表示されます。証明書を信頼する場合には、[このセッションで許可する]、[常に許可する] を選択し Visual Policy Manager を開始します。

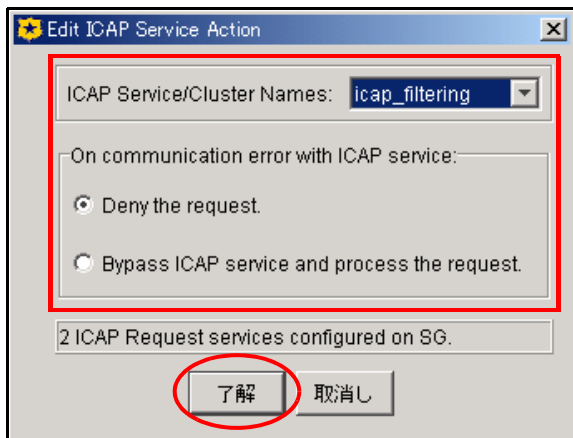
3. メニューバーの [Edit] をクリックし、表示されるプルダウンメニューから [Add Web Access Policy] をクリックします。



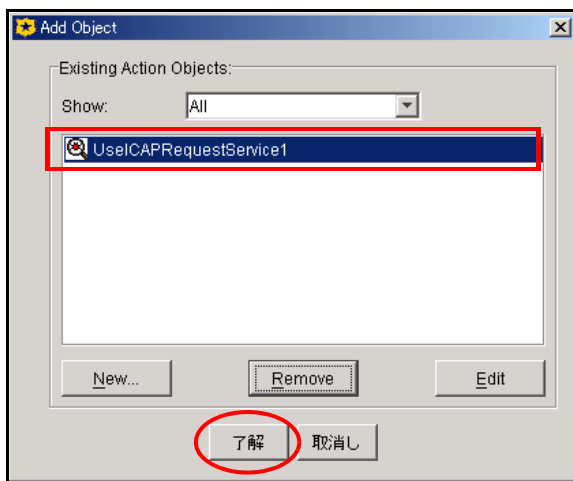
4. ポリシー名を入力し、[了解] ボタンをクリックします。
ポリシーが追加されます。
5. 追加されたポリシーの [Action] のセルを右クリックし、[Set] をクリックします。
[Add Object] ダイアログが表示されます。
6. [New...] ボタンをクリックし、[Use ICAP Request Service...] をクリックします。
[ADD ICAP Service Action] ダイアログボックスが表示されます。

7. 次の項目を設定し、[了解] ボタンをクリックします。

- ICAP Service/Cluster Names : 登録した ICAP サービスを選択
 - On communication error with ICAP service : [Deny the request] を選択
- [Action] 一覧に ICAP サービスが追加されます。



8. [Add Object] に追加された ICAP サービスを選択し、[了解] 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 Policies] 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。

7. Squid の設定

ISWM 6.0 for Squid をご利用の場合、Squid と連携するために次の設定をしてください。

7-1. Squid の設定

ISWM と連携させる Squid の設定を必要に応じて調整してください。

ISWMは、リダイレクトプログラムインストール時に、Squidの設定ファイル「squid.conf」に次のISWM用設定を追加します。

```
redirect_program <インストールディレクトリ>/bin/amsrdr start  
redirect_children 5
```

クライアントの多い環境では、「squid.conf」を編集してリダイレクトプログラムの起動数を増やすなどの調整をしてください。リダイレクトプログラムの最大起動数は「redirect_children」で定義されます。初期値は「5」です。

■ リダイレクトプログラムの起動について

リダイレクトプログラムは、Squid を起動または再起動することで自動的に起動します。

ただし、リダイレクトプログラムを起動する前に、必ずコントロールサーバプログラムを起動してください。リダイレクトプログラムを先に起動すると、一時的にフィルタリングが正常に動作しない状態になります。

コントロールサーバプログラムの各サービスの起動方法については、51ページの「8. サービスの起動と停止」を参照してください。

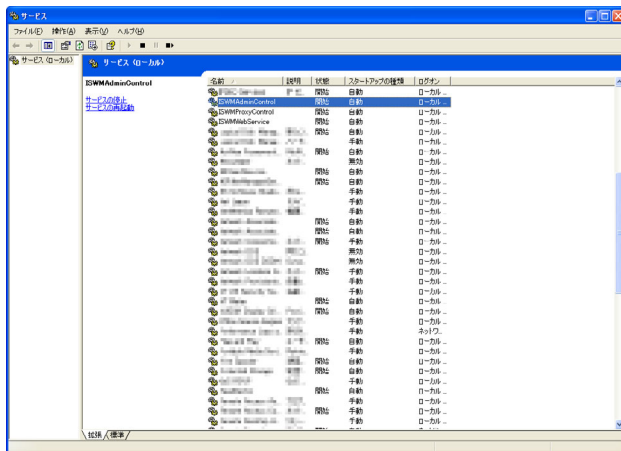
8. サービスの起動と停止

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。

8-1. 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、3 つのサービスがあります。

- ISWMAAdminControl : 管理サービス
- ISWMWebService : 拡張 Web サービス
- ISWMPProxyControl : フィルタリングサービス

8-2. Solaris/Linux の場合

Solaris 版と 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

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。

▪ Squid 版の場合、Squid を起動または再起動すると、自動的にリダイレクトプログラムが起動します。フィルタリングサービスが停止し、Squid およびリダイレクトプログラムだけが起動している状態では、フィルタリングが正常に動作しません。この場合、proxy.inf の [CONTROL_CFG] セクションにある「CONNECT_RETRY」の値により動作が異なります。「0」の場合は、すべてのリクエストに対して規制メッセージを表示し、正の値の場合は、すべてのリクエストを許可します。

9. アンインストール

9-1. 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。

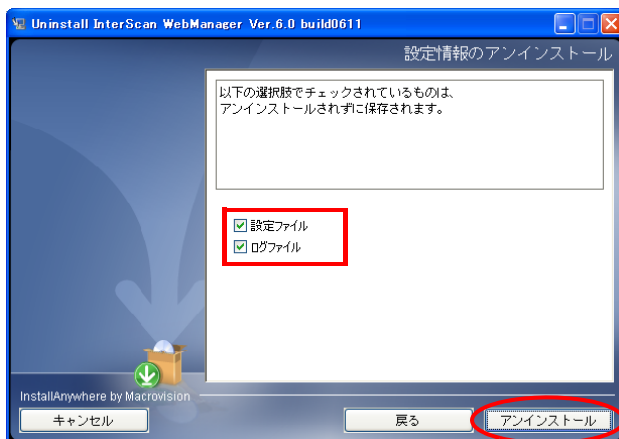
アンインストールの確認画面が表示されます。

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。
-

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。

9-2. Solaris/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

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。

- Solaris /opt/iswm
- Linux /usr/local/iswm

注意： Squid 版の場合、必ず Squid を再起動してください。

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。

10. 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、ブラウザからマスタ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。
 - Internet Explorer の [インターネットオプション] → [プライバシー] で「高」以上に設定するとCookieが使用できなくなります。また、[インターネットオプション] → [セキュリティ] で「高」以上に設定すると、管理画面にログインできなくなります。
-

10-1. 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。

マスタサーバの 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] → [InterScan WebManager]→[InterScan WebManager] 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、設定にあわせてポート番号 (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。
 - ・ログイン後は、ブラウザなどの [戻る] ボタンなどで、ページを切り替えしないでください。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] ボタン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。アカウントの種類には、マスタ管理者、グループ管理者、サブグループ管理者、エンドユーザがあります。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。

アカウントの種類	説明
マスタ管理者	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。
グループ管理者	第1階層のグループ管理者です。 第1階層以下に所属するグループ/ユーザ管理、フィルタリング設定、例外ユーザ設定、アクセス管理の設定ができます。
サブグループ管理者	第2階層以下のグループ管理者です。 第2階層以下に所属するグループ/ユーザ管理、フィルタリング設定、例外ユーザ設定の設定ができます。
エンドユーザ	各グループに所属するエンドユーザです。 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。

エンド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。メールアドレスの変更のみ可能になります。パスワードはLDAPサーバで変更してください。

10-2. 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]ボタン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]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。



2. [OK] ボタンをクリックします。

11. [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。

11-1. [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」と「メニューガイド」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情報とユーザ情報を確認できます。

■ メニューガイド

目的別に各設定項目へのリンクがあります。重要な設定項目や、よく設定を変更/確認する項目は、メインメニューを開かなくても、メニューガイドからワンクリックでアクセスできます。

簡易設定

簡易設定へのリンクがあります。

[簡易設定へ] 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、1 台のフィルタリングサーバで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。

詳細設定

ISWM の各種設定画面へのリンクボタンがあります。

各リンクボタンをクリックすると、通常の運用でよく利用する設定項目や画面を表示します。

サーバの状態やユーザ認証設定、グループ / ユーザ、フィルタリングの設定をする場合にご利用ください。

■ メインメニュー

4 つのカテゴリに分類された設定項目を表示します。

メインメニュー

サブメニュー



各メイン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。

[システム管理] 画面	「第 2 章 システムの設定と管理」	65 ページ
[グループ / ユーザ管理] 画面	「第 3 章 ユーザとグループの管理」	147 ページ
[フィルタリング設定] 画面	「第 4 章 フィルタリングの設定」	201 ページ
[アクセス管理] 画面	「第 7 章 アクセスログの管理」	317 ページ

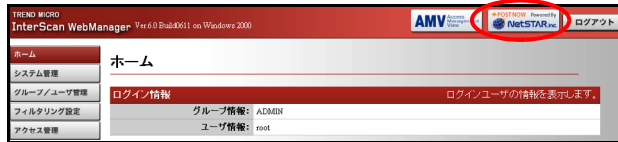
各画面では、設定可能な項目がサブメニューとして表示されます。

[システム設定] 画面の [サーバ設定] を表示しています



■ ネットスターリンクサービス

管理画面の右上にある  をクリックすると「ネットスターリンク」サービスに接続します。



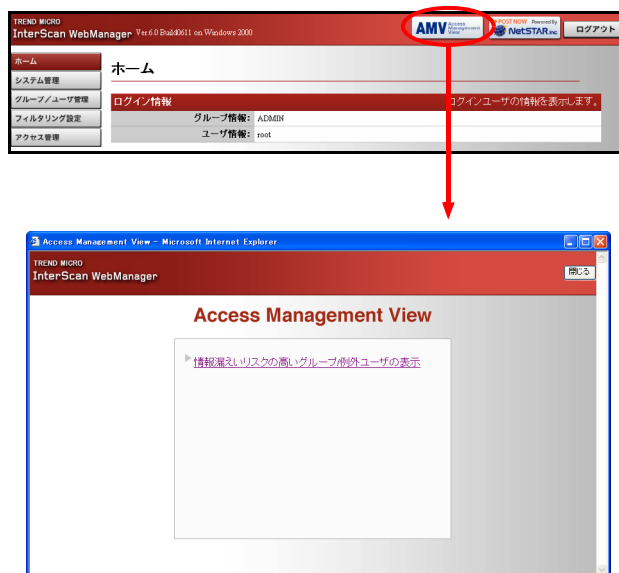
ネットスターリンクサービスでは、次のサービスを提供しています。

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： ライセンスキー、企業・団体名、メールアドレスなどのユーザ情報が入力されていない場合、ネットスターリンクサービスに接続することはできません。
[システム管理] → [ダウンロード設定] の [■ダウンロード情報] で、各サーバの [選択] ボタンをクリックして表示される [ダウンロード詳細情報] で設定してください。

■ アクセス マネジメント ビュー

管理画面の右上にある **AMV** Access Management View (以降「アクセス マネジメント ビューへのリンク」と記載) をクリックすると、[Access Management View] 画面が別ウィンドウで表示されます。設定方法や内容については 301 ページの「第 6 章 アクセス マネジメント ビューの操作」を参照してください。



注意： 閲覧権限のないユーザの管理画面には表示されません。アクセス マネジメント ビューで情報漏えいリスクを確認できるのは、[AMV 閲覧権限] をオンにしたアカウントのユーザだけです。

■ ヘルプ

管理画面の右上に [ヘルプ] が表示されている場合、クリックすると、『Trend Micro InterScan WebManager 管理者ガイド』(本書) の該当ページが表示されます。



MEMO

システムの設定と管理

1. [システム管理] 画面でできること

スレーブサーバの登録や Trend Micro InterScan WebManager (以下、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、システム共通の設定ができます。

■ サーバの設定とスレーブサーバの新規登録

スレーブ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、再起動もできます。

スレーブサーバは、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。

→「2. サーバの設定と登録」(68 ページ)

■ スレーブサーバとの同期

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。また、システム設定の復旧に失敗している場合には青く表示されます。

この場合、同期に失敗しているサーバと通信し、同期を試みることができます。



同期に失敗
しているサーバ

→「2. サーバの設定と登録」(68 ページ)

■ URL データベース / モジュールのダウンロード

フィルタリング用 URL 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、URL 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 / モジュールのダウンロード」(78 ページ)

■ 管理画面 / 規制画面の表示設定

管理画面を表示する際のポート番号を設定します。また、規制画面として表示する URL やファイルを設定できます。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。

→「4. 管理画面 / 規制画面の表示設定」(83 ページ)

■ ログファイルの取得 / 出力先設定

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。

→「5. ログファイルの設定」(89 ページ)

■ サーバ設定の保存と復旧

管理画面で設定した内容の保存、および保存したシステム設定の復旧ができます。

万一の際のバックアップにシステム設定を保存しておくことをおすすめします。また、システム設定は最大で 5 つまで保存できるので、試験運用時のシステム設定の保存 / 復旧にも利用できます。

→「6. システム設定の保存、復旧」(99 ページ)

■ 異常時 / モジュールのアップデート時のメール通知設定

管理者あてに、ISWM のライセンス期限切れの事前通知や、最新モジュールの配布状況、サーバの動作状況をメールで通知できます。

→「7. メール通知設定」(102 ページ)

■ ユーザ認証の設定

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同期もここで設定します。

→「8. ユーザ認証の設定」(105 ページ)

■ フィルタリングルール共通の設定

POST リクエストを規制するデータサイズを設定します。設定したデータサイズは、すべてのフィルタリングルールに適用されます。

また、規制対象の URL にアクセスした時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が可能です。

→「9. フィルタリングルール共通設定」(137 ページ)

注意： Squid 版では、書き込み規制の設定 (POST リクエストを規制するデータサイズの設定) が表示されません。

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マスタサーバ、およびスレーブサーバの状態や設定を確認できます。

1. [システム管理] → [サーバ設定] をクリックします。

[サーバ情報] が表示されます。



サーバ情報

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。また、青く表示されているサーバは、システム設定の復旧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マスタサーバやスレーブ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。[サーバ情報]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： Squid 版の場合、フィルタリングサービスが停止し、Squid およびリダイレクトプログラムだけが起動している状態では、フィルタリングが正常に動作しません。
このとき、proxy.inf の [CONTROL_CFG] セクションにある「CONNECT_RETRY」の値が「0」の場合、すべてのリクエストに対して規制メッセージを表示します。正の値の場合は、すべてのリクエストが許可されます。

1. [システム管理] → [サーバ設定] をクリックします。
[サーバ情報] 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、停止の中から変更したい状態をクリックします。



2-3. 新規スレーブサーバを登録する

ISWM は、最大 9 台までのスレーブサーバを管理できます。サーバにスレーブ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：**
- ・[■サーバ情報] 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、規制画面が正しく表示されません。マスタサーバおよび全スレーブサーバの IP アドレスを例外 URL の [許可カテゴリ] に登録してください。
また、ラウンドロビンによる負荷分散を行っている環境でオーバーライドを設定した場合、正常に動作しません。

1. [システム管理] → [サーバ設定] をクリックします。
[サーバ情報] が表示されます。
2. [■サーバ登録] - [新規サーバ登録] をクリックします。
[サーバ設定] が表示されます。
3. サーバの設定情報を入力します。

サーバ設定

サーバ名: スレーブサーバ: slave1
IPアドレス: 172.16.5.213

フィルタリングサービス設定

設定参照: ☐ 有効にMasterの設定を参照します。

HTTP	ポート: 8080	プロキシ数: 100
HTTPS	ポート: 8443	プロキシ数: 75
FTP OVER HTTP	ポート: 8021	プロキシ数: 75

上位プロキシサーバ設定

設定参照: ☐ 有効にMasterの設定を参照します。
☐ 有効にProxyの設定を参照します。

HTTP	IPアドレス:	上位ポート: 80
HTTPS	IPアドレス:	上位ポート: 80
FTP OVER HTTP	IPアドレス:	上位ポート: 80

※ 登録完了後に拡張Webサービス、フィルタリングサービス、管理サービスの再起動が必要になります。

■サーバ情報

登録するスレーブサーバの [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。[設定参照]-[有効] チェックボックスをオンにすると、マスタサーバの設定を参照します。

注意： ・「HTTP」の設定項目は、Squid 版では「リダイレクタ」、ICAP 版では「ICAP」として表示されます。

・Squid 版、ICAP 版の場合、「HTTPS」と「FTP OVER HTTP」の設定項目は表示されません。

■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 / ドメイン、ポート番号を入力してください。[設定参照]-[有効] チェックボックスをオンにすると、マスタサーバの設定を参照します。

注意： Squid 版、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 [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。
「登録が完了しました」と表示されます。以上でスレーブサーバの登録は完了です。
6. 画面右上の [戻る] ボタンをクリックします。
[サーバ情報] 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、登録したスレーブ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。また、Squid 版の場合には、Squid も再起動してください。

2-4. サーバの設定を変更する

マスタサーバおよびスレーブ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。

注意： Squid 版でサーバの設定を変更する場合は、419 ページの「F. Squid 版で設定を変更する場合の注意事項」を参照してください。

1. [システム管理] → [サーバ設定] をクリックします。
[サーバ情報] 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。

サーバ設定

サーバの設定をします。

サーバ名: デフォルトサーバ
IPアドレス: 172.16.3.100

■ フィルタリングサービス設定

フィルタリングサービスの設定をします。

サービス	ポート	プロセス数
HTTP	8080	150
HTTPS	8443	75
FTP OVER HTTP	8021	75

■ フィルタリングサービス共通設定

フィルタリングサービスの共通設定をします。

リクエストモード: 転送しにくい ☒ ※ 追加ヘッダの無い転送モード。

転送バッファサイズ: 2048 byte

サーバ接続タイムアウト値: 15000 ms

クライアント接続タイムアウト値: 15000 ms

最大ヒープサイズ: 640 Mbyte

サードスレッド間隔: 60

Keep-Alive設定: 全て有効

HTTPバージョン設定: ☐ HTTP/1.1 優先 ☒ HTTP/1.0のみ使用

HTTPリクエスト転送許可設定:

☒ GET	☒ DELETE	☐ MOVE
☐ COPY	☐ LOCK	☐ UNLOCK
☐ PROPPATCH	☐ LOCK	☐ UNLOCK

※ 選択されたメソッドの転送を許可します。

■ 上位プロキシサーバ設定

上位プロキシサーバの設定をします。

上位プロキシサーバ使用設定: ☐ 使用する

サービス	IPアドレス	上位ポート
HTTP		80
HTTPS		443
FTP OVER HTTP		21

※ 項目「ポート」変更時に設定変更を反映するには、管理している全てのサーバで、管理サービスの再起動が必要になります。
※ 設定変更を反映するには、管理している全てのサーバでフィルタリングサービスの再起動が必要になります。

■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。

■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。[設定参照]-[有効] チェックボックスをオンにすると、マスタサーバと同じ設定が有効になります。

注意：

- ・「HTTP」の設定項目は、Squid 版では「リダイレクタ」、ICAP 版では「ICAP」として表示されます。
- ・Squid 版、ICAP 版の場合、「HTTPS」と「FTP OVER HTTP」の設定項目は表示されません。

■フィルタリングサービス共通設定（マスタサーバのみ）

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。
タイムアウト値 (Squid 版、ICAP 版のみ)	リクエストのタイムアウト値を指定します。 • Squid 版の場合： クライアントから規制画面表示用 Web サーバへのリクエストのタイムアウト値を 1 ミリ秒 ～ 9,999,999 ミリ秒の範囲で指定します。短い場合、規制画面が表示されない場合があります。 • ICAP 版の場合： 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。
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。

最大ヒープサイズ	Java ヒープ領域サイズの最大値を 64MB ～ 2048MB の範囲内で指定します。 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。
サービス確認間隔	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。
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。

注意： Squid 版、ICAP 版の場合、[HTTP バージョン設定] は表示されません。

■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 アドレスやポート番号を入力してください。

[設定参照] - [有効] チェックボックスをオンにすると、マスタサーバの設定を参照します。

注意： Squid 版、ICAP 版の場合、この設定項目は表示されません。

4. [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。

注意： [更新] 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 [更新] 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。また、Squid 版の場合には、Squid も再起動してください。

2-5. スレーブサーバを削除する

スレーブ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. [システム管理] → [サーバ設定] をクリックします。
[サーバ情報] が表示されます。
2. 設定を削除したいスレーブサーバの右にある [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、スレーブ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、[サーバ情報]-[■サーバ情報]でサーバ名が赤く表示されます。

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。

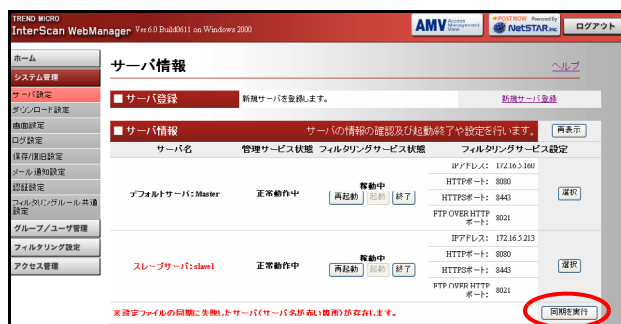
1. [システム管理]→[サーバ設定]をクリックします。

[サーバ情報]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。

2. [同期を実行]ボタンをクリックします。

マスタサーバの設定が、登録されているスレーブ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、[同期を実行]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 / モジュールのダウンロード

3-1. ダウンロードの設定

ISWMは、URLデータベースやモジュール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フィルタリング用データベースは、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 データベースやモジュール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、次の間隔で最新版の有無を確認します。

- ・ URL データベース : 1日に1回 (午前2時)
- ・ モジュール : 1日に1回 (午前3時)

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、81 ページの「3-2. データベース / モジュールをダウンロードする」を参照してください。

1. [システム管理]→[ダウンロード設定]をクリックします。

[ダウンロード情報]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。

[ダウンロード設定]が表示されます。

The screenshot shows the 'ダウンロード情報' (Download Information) page in the Trend Micro InterScan WebManager interface. The page has a sidebar on the left with navigation links like 'ホーム', 'システム管理', 'サーバ設定', 'ダウンロード設定', etc. The main content area is titled 'ダウンロード' (Download) and contains a section for 'ダウンロード情報' (Download Information). This section includes a table with columns for 'サーバ名' (Server Name), 'データベース情報' (Database Information), and 'モジュール情報' (Module Information). The table lists two servers: 'デフォルトサーバ' and 'スレーブサーバ: slave1'. For each server, it shows version numbers, build numbers, and update dates. In the rightmost column of the table, there are '選択' (Select) buttons for each server, which are circled in red in the image. Above the table, there are tabs for 'データベースダウンロード' (Database Download) and 'モジュールダウンロード' (Module Download), and a '更新' (Update) button.

サーバ名	データベース情報	モジュール情報	操作
デフォルトサーバ	バージョン: 2007012027 DBビルド: 2007012027 更新日: 2008/03/01	Build番号: 0611 更新日: 2008/03/01	ユーザ数: 2000 有効期限: 2008/03/01 [選択]
スレーブサーバ: slave1	バージョン: 2007012027 DBビルド: 2007012027 更新日: 2008/03/01	Build番号: 0611 更新日: 2008/03/01	ユーザ数: 2000 有効期限: 2008/03/01 [選択]

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。

The screenshot shows the 'ダウンロード設定' (Download Settings) page in the InterScan WebManager interface. The page has a sidebar on the left with navigation links like 'ホーム', 'システム管理', 'サーバ設定', 'ダウンロード設定', etc. The main content area is titled 'ダウンロード設定' and contains three sections:

- ダウンロード詳細情報** (Download Detailed Information): Includes fields for 'サーバ名' (Server Name), 'ライセンスキー' (License Key), '企業・団体名' (Company/Institution Name), and '連絡先 e-mail' (Contact Email).
- 上位プロキシサーバ設定** (Proxy Server Settings): Includes a checkbox for '上位プロキシサーバ使用設定' (Proxy Server Usage Setting), and fields for 'IPアドレス' (IP Address), 'ポート' (Port), 'アカウント' (Account), 'パスワード' (Password), and 'パスワード(確認)' (Password Confirmation).
- ダウンロード共通設定** (Download Common Settings): Includes fields for 'ダウンロード先URL' (Download URL), 'ダウンロード時間自動設定' (Automatic Download Time Setting), 'リトライ回数' (Retry Count), 'リトライ間隔' (Retry Interval), 'データベースダウンロード間隔' (Database Download Interval), and 'モジュール自動アップデート' (Module Automatic Update).

Red brackets on the right side of the screenshot point to these sections with labels: 'ダウンロード詳細情報', '上位プロキシサーバ設定', and 'ダウンロード共通設定'.

■ ダウンロード詳細情報

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。
企業名・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)
連絡先 e-mail	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。

■ダウンロード共通設定

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、「 http://iswm.netstar-inc.com/db60 」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日8回、3時間ごとに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。
データベース 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。
モジュール 自動アップデート (スタンドアロン版、 ICAP 版のみ)	チェックボックスをオンにするとモジュールの自動アップデートをします。 モジュールのアップデートは1日に1回チェックされ、アップデートがあった場合、自動的に最新版モジュールのダウンロードとアップデートが実行されます。

- 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、データベースダウンロード開始時間は設定できません。
 - ・Squid 版の場合、モジュールの自動アップデートができません。手動でアップデートをしてください。
 - ・モジュールは、URL データベースをダウンロードする時に最新版があるかチェックされます。最新版のモジュールがある場合、URL データベースのダウンロードが完了してから1時間後にモジュールのダウンロードが開始されます。デフォルトでは午前2時にURLデータベースをダウンロードします。また、モジュール、データベースのダウンロードが失敗した時には、エラーメッセージが表示されます。

4. 画面右上の [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。

- 注意：** [更新] 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 [更新] 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。

3-2. データベース / モジュール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、手で URL データベースやモジュール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またはモジュール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. [システム管理] → [ダウンロード設定] をクリックします。
[ダウンロード情報] が表示されます。
2. [データベースダウンロード] または [モジュールダウンロード] の [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。

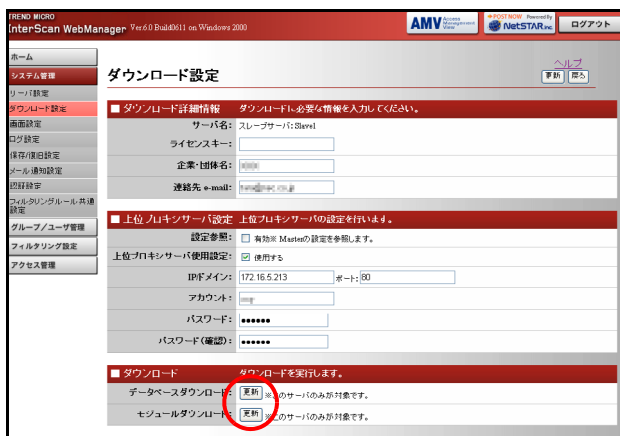
■ サーバを選択してダウンロードする

選択したサーバにだけ、データベースまたはモジュール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： マスタサーバとの同期に失敗した場合など、個別のスレーブサーバにデータベース、モジュールをダウンロードしたい場合にだけ使用してください。

1. [システム管理]→[ダウンロード設定]をクリックします。
[ダウンロード情報]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。
[ダウンロード設定]が表示されます。
3. [■ダウンロード]-[データベースダウンロード]または[モジュールダウンロード]の[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. 管理画面 / 規制画面の表示設定

4-1. 管理画面情報を設定する

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設定します。

- 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。
 - Squid 版で設定を変更する場合は、419 ページの「F. Squid 版で設定を変更する場合の注意事項」を参照してください。

- [システム管理] → [画面設定] をクリックします。
[画面設定] が表示されます。
- [■管理画面情報] - [ポート] にポート番号を入力し、[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。



- 注意：** 設定変更を反映するには、マスタサーバおよびスレーブサーバの拡張 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。
- Solaris 版、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

- [OK] ボタンをクリックします。
- 以上で、管理画面情報の設定は完了です。

4-2. 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 が規制をかけたことをユーザに通知する、規制画面の内容を設定します。

1. [システム管理] → [画面設定] をクリックします。
[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。Squid 版、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 URL やファイル、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、85 ページの「規制画面について」を参照してください。
4. [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。

注意： [更新] 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 [更新] 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

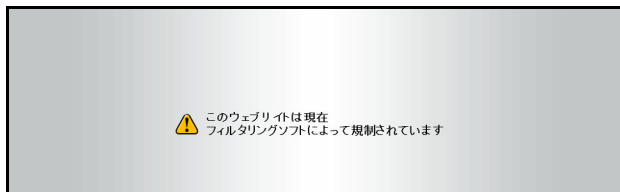
クライアント PC から、フィルタリング対象の URL にアクセスした場合、ISWM はクライアント PC に規制画面を表示します。規制画面とは、対象 URL の表示に規制をかけたことを通知する画面です。規制画面の形式には「URL」、「ファイル」、「メッセージ」の 3 種類があります。

-
- 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、140 ページの「9-3. 規制解除申請を設定する」を参照してください。
 - Squid 版、または 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 [受信プロセス数] に設定してください。
 - Squid 版の場合、規制対象で https プロトコルを使用した URL の閲覧を試みたときは、リクエストした URL、規制理由 (カテゴリ) ともに表示されません。
-

● 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：・Squid 版の場合、URL を規制画面形式として指定すると、ネットワーク上にある、https プロトコルを使用したページを、規制画面として使用します。デフォルトでは「<https://iswm.netstar-inc.com/>」に設定されています。

規制画面には、社内および社外の URL を指定できます。

それぞれの以下のように動作します。

規制対象で http プロトコルを使用した URL の閲覧を試みた場合→

<http://iswm.netstar-inc.com/>

規制対象で https プロトコルを使用した URL の閲覧を試みた場合→

<https://iswm.netstar-inc.com/>

規制対象で https プロトコルを使用した URL にアクセスしたときに、ネットワーク上の任意の http プロトコルのページに切り替えることはできません。

・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。

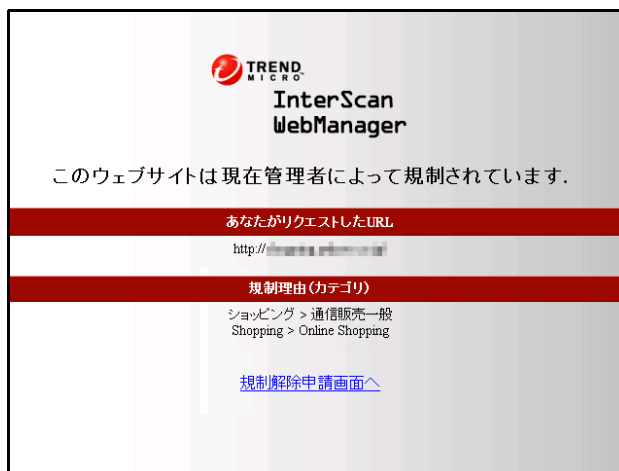
● ファイル

任意の HTML ファイルを規制画面として表示します。

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に格納してください。

Windows の場合 <インストールディレクトリ> ¥conf¥block

Solaris/Linux の場合 <インストールディレクトリ> /conf/block



注意： ・Squid 版、ICAP 版の場合は、[ポート] と [受信プロセス数] 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。

- ・受信プロセス数

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。

- ・規制解除申請機能を使用する場合、規制解除申請画面のファイル名は「nfdr_offer.htm」となります。HTML ファイルのカスタマイズは可能ですが、ファイル名は変更できません。

規制解除申請機能については、140 ページの「9-3. 規制解除申請を設定する」を参照してください。

● 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：**
- ・グループごと、またはカテゴリごとの規制メッセージを設定した場合は、グループまたはカテゴリのメッセージが表示されます。[画面設定]で設定したメッセージは表示されません。
詳しくは、277 ページの「8. カテゴリ別規制メッセージの設定」を参照してください。
 - ・Squid 版、ICAP 版の場合は、[ポート]と[受信プロセス数]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。
 - ・受信プロセス数
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。
-

5. ログファイルの設定

5-1. 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（アクセスログ、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. [システム管理]→[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]、[毎日]、[毎週]、[毎月]から選択します。 ※アクセスログおよび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。
ローテーションサイズ	ローテート種別で「サイズ」を選択した場合に、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。 ※ローテート種別に「毎日」、「毎週」、「毎月」のいずれかを選択した場合は、無効になります。
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

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
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。 • 転送データサイズ: アクセスした URL から取得したデータの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。 • 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。 ※ Squid 版では、[ブラウザバージョン]、[HTTP バージョン]、[応答コード]、[転送データサイズ] は表示されません。 ※ ICAP版では、[応答コード]、[転送データサイズ] は表示されません。

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) • Blocked: 転送しなかったリクエスト(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: 監視したデータ(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: 解放したデータ(ポリシーで許可されていないがオーバーライド機能によって転送したデータ) • BlkPost: 書き込み規制によって規制されたデータ

■ POST ログ出力設定

掲示板などに書き込みした内容を POST ログに保存する時の最大サイズを、バイト単位で入力します。

一回の書き込みにつき、先頭から指定したバイト数を POST ログに保存します。指定したサイズを超えた部分の内容は保存されません。

デフォルトでは 0 に設定されているので、書き込み内容は保存されません。

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。
• Squid 版では、[POST ログ出力設定] は表示されません。

3. [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。

注意： [更新] 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 [更新] 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。

5-2. 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、「5-3. 現在のシステムログを閲覧する」(96 ページ)または「5-4. ローテート済みシステムログをダウンロード、削除する」(97 ページ)を参照してください。

1. [システム管理]→[ログ設定]をクリックします。
[ログ設定]が表示されます。
2. [■システムログ一覧]-[システムログ一覧へ]をクリックします。
[システムログファイル一覧]が表示されます。

ログ設定

■ 共通設定 ログの共通設定を行います。

ファイル名: iswm.log

ローテート種別: ☒ サイズ ☐ 日 ☐ 曜日 ☐ 毎月

ローテーションサイズ: 10 Mbyte

自動削除: ☒ 有効

保持ファイル数: 5 ファイル

※ 自動削除が有効な時、日付の異なる指定数分のログを削除して、制限します。
※ 共通設定の変更が反映するまで、管理している全てのサーバで拡張性サービス、ファイルジョーニングサービス、管理サービスの再起動が必要になります。

■ アクセスログ出力設定 アクセスログの出力設定を行います。

出力単位: システム一括

出力形式: TEXTのみ出力する

出力項目: ☒ グループ名 ☒ アカウント名 ☒ ブラウザバージョン ☒ WWWサーバIP ☒ 応答コード ☒ 転送データサイズ ☒ ファイルタイプ ☐ HTTPバージョン ☐ リクエストメソッド

出力条件: ☒ 転送されたデータ ☒ Downloadされたデータ ☒ Allowed: カスタマイズルールで許可されたデータ ☒ Release: オーバーライド機能によって転送されたデータ ☒ HTTP: 書き込み機能によって転送されたデータ

■ POSTログ出力設定 POSTログの出力設定を行います。

POSTデータ出力サイズ: 0 Mbyte

■ システムログ一覧 システムログ一覧を表示します。

システムログ一覧へ

3. [システムログファイル一覧] で、システムログの一覧を確認します。

現在のログ

ログファイル名	サーバ名	サイズ (Mbyte)	更新日時
www_access.log	デフォルトサーバ	0.001	2007/12/28 09:53
www_error.log	デフォルトサーバ	0.006	2007/12/28 09:53
www_logjammya.log	デフォルトサーバ	0.000	2007/12/28 09:54
www_err.log	デフォルトサーバ	0.016	2007/12/28 10:51

ローテート済みのログ

ログファイル名	サーバ名	サイズ (Mbyte)	更新日時
www_access_20071227_001.log	デフォルトサーバ	0.001	2007/12/27 13:21
www_error_20071227_001.log	デフォルトサーバ	0.003	2007/12/27 14:36
www_err_20071227_001.log	デフォルトサーバ	0.002	2007/12/27 14:36
www_logjammya_20071227_001.log	デフォルトサーバ	0.002	2007/12/27 14:36

※ダウンロードは1ファイルずつ行ってください。

ダウンロード 削除

記録中のログファイル

ローテート済みのログファイル

ログファイルのソート

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、ソート用ボタンで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、[ログファイル名順]、[サーバ名順]、[サイズ (Mbyte) 順]、[更新日時順] ボタンから選択できます。

選択されたソート項目 (ボタン) は、白文字で表示されます。

■ 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	[■ 共通設定] - [ログファイル名] 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。 • システムログ (sys) ISWM 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。 • 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。 • 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。 • 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。 • LogLyzer ログ (loglyzersys) LogLyzer からのログ取り込み状況が記録されます。 • リダイレクタログ (amsrdr) リダイレクタとコントロールサーバ間のアクセス状況が記録されます (Squid 版のみ)。
日付 (yyymmdd)	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_sys_20080401_001.log
- iswm_adm_20080401_001.log
- iswm_ctrl_20080401_001.log
- iswm_http_20080401_001.log
- iswm_offer_20080401_001.log
- iswm_post_20080401_001.log
- iswm_loglyzersys_20080401_001.log
- iswm_amsrdr_20080401_001.log

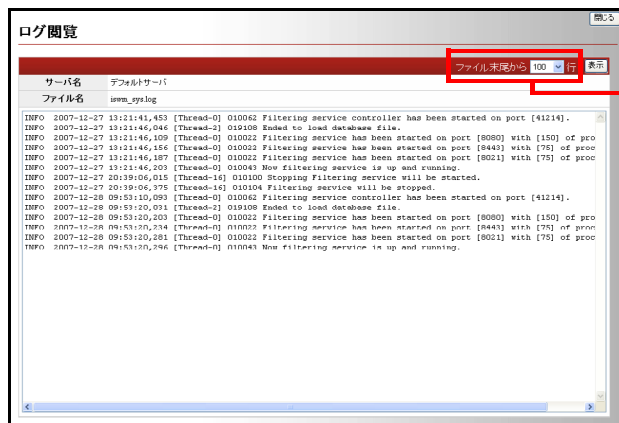
注意： ローテート済みシステムログは、ローテート後、[システム管理]→[ログ設定]-[■共通設定]-[自動削除]で指定されたファイル数を超えると、自動的に削除されます。

5-3. 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. [システム管理]→[ログ設定]をクリックします。
[ログ設定]が表示されます。
2. [■システムログ一覧]-[システムログ一覧へ]をクリックします。
[システムログファイル一覧]が表示されます。

3. [■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。



表示行数変更用
プルダウンメニュー

4. 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。
5. [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。

5-4. ローター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： ローター済みログは、[システム管理]→[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、ローテート済みログは閲覧できません。

1. [システム管理] → [ログ設定] をクリックします。
[ログ設定] が表示されます。

2. [■システムログ一覧] - [システムログ一覧へ] をクリックします。

[システムログファイル一覧] が表示されます

3. [■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。

[全選択] ボタンをクリックすると、すべてのチェックボックスをオンにします。[全解除] ボタンをクリックすると、すべてのチェックボックスをオフにします。



4. [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。

5. [OK] 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。

6. システム設定の保存、復旧

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システム情報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。

注意： インストール終了後に、初期状態を「yyyyymmdd_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。

6-1. システム設定を保存する

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システム情報をファイルに保存できます。

1. [システム管理] → [保存 / 復旧設定] をクリックします。
[保存 / 復旧設定] が表示されます。
2. 保存するファイル名を [■保存設定]-[保存ファイル名] 欄に入力し、[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。



3. [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：

- ・システム設定は最大で 5 件まで保存できます。
- ・不要になったシステム設定は、[■ 復旧設定] 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、システム設定の保存は完了です。

6-2. システム設定を復旧する

ISWM では、保存したシステム設定からサーバの設定を復旧できます。

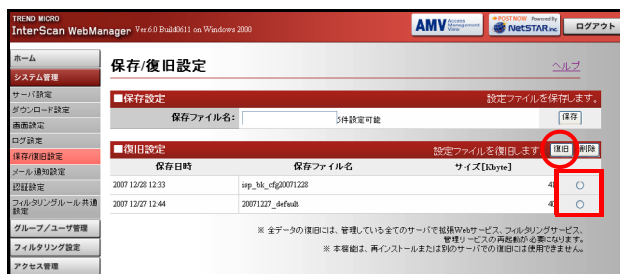
注意： 復旧時は、マスタサーバと同期してスレーブサーバも復旧します。また、復旧に失敗した場合は、サーバ情報画面にメッセージが表示されます。

1. [システム管理] → [保存 / 復旧設定] をクリックします。

[保存 / 復旧設定] が表示されます。

2. 復旧に使用するシステム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。
[■保存設定] 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、システム設定の復旧は完了です。

7. メール通知設定

7-1. メール通知の設定をする

ISWM ではライセンスの期限切れや最新モジュールのアップデート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、マスタサーバとスレーブ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. [システム管理] → [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。

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
最新モジュール情報通知	ダウンロードサーバに最新のモジュールがあるかを毎日 1 回チェックし、最新モジュールがあった場合、通知メールを送信します。
サービス異常発生通知	管理サービスが、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。 • マスタサーバとスレーブ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
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 [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。

注意： [更新] 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 [更新] 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「7-2. 通知メールをテスト送信する」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。

7-2. 通知メールをテスト送信する

1. [システム管理] → [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。

The screenshot shows the 'メール通知設定' (Email Notification Settings) page in the Trend Micro InterScan WebManager. The left sidebar contains a navigation menu with options like 'ホーム', 'システム管理', 'ポリシー設定', 'ログ検索', 'メール通知設定' (highlighted), 'アカウント管理', 'グループ/ユーザ管理', 'ファイルアップロード設定', and 'アクセス管理'. The main content area is titled 'メール通知設定' and includes a 'テスト送信' (Test Send) button, which is circled in red. Below this, there are fields for 'SMTPサーバ' (SMTP Server), 'ポート' (Port), '認証' (Authentication), 'アカウント' (Account), 'パスワード' (Password), and '通知メール発出人' (Notification Email Sender). A section titled 'メール通知詳細' (Email Notification Details) contains several checkboxes for enabling specific notifications: 'ライセンス期限切れ事前通知' (License expiration notice), '最新スケジュール情報通知' (Latest schedule information), 'サービス異常発生通知' (Service abnormality notification), and '設定変更通知' (Setting change notification). Each checkbox has a corresponding '宛先' (Recipient) field.

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。

8. ユーザ認証の設定

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。

8-1. ユーザ認証の種類

設定できるユーザ認証方法には、「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) の 4 種類があります。

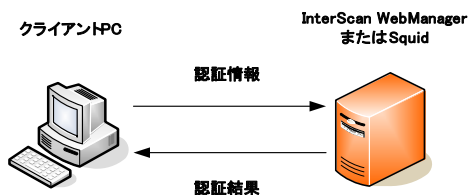
■ IP アドレス認証

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 へのログイン情報を ISWM で Basic 認証します。

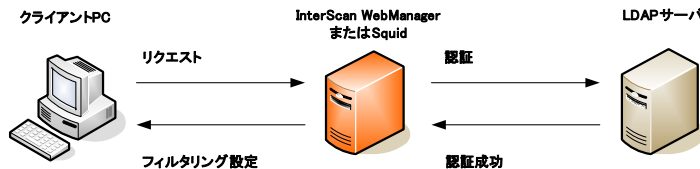


Basic 認証 (ローカル) の設定方法については、108 ページの「8-2. Basic 認証 (ローカル) を設定する」を参照してください。

■ Basic 認証 (LDAP 連携)

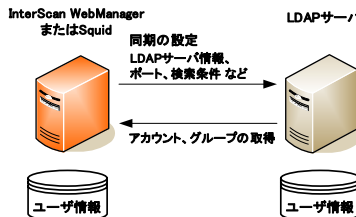
LDAP サーバと連携した Basic 認証をします。LDAP 連携を選択した場合、LDAP 連携設定と LDAP 同期設定を行ってください。

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	「8-3. Basic 認証 (LDAP 連携) を設定する」	109 ページ
連携する LDAP サーバの登録	「8-5. LDAP サーバの登録と管理」	114 ページ
LDAP 連携設定	「8-6. LDAP サーバとの連携を設定する」	120 ページ
LDAP 同期設定	「8-7. LDAP サーバと同期する」	124 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で Internet Explorer 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。

認証ディレクトリサーバ	Windows 2000 Server、または Windows Server 2003 (R2 含む) の Active Directory ドメインコントローラ
対応 OS (クライアント)	Windows 2000 Professional/Server (SP4 推奨) Windows XP Professional (SP2 含む) Windows Vista Business Windows Vista Ultimate
対応 Web ブラウザ	Internet Explorer 5.5/6.0/7.0 ※NTLM認証に対応していないブラウザからのWeb閲覧はできません。

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。

連携する LDAP サーバの登録	「8-5. LDAP サーバの登録と管理」	114 ページ
LDAP 連携設定	「8-6. LDAP サーバとの連携を設定する」	120 ページ
LDAP 同期設定	「8-7. LDAP サーバと同期する」	124 ページ

8-2. Basic 認証 (ローカル) を設定する

クライアント PC のローカルアカウントで 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。Squid 版、ICAP 版では表示される項目が異なります。

1. [システム管理] → [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クリックしてオンにします。



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

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。
- ・Squid 版の場合、[アカウント認証を行う] チェックボックスは表示されません。
[ユーザ認証] - [有効] チェックボックスをオンにすると、IP アドレス認証とアカウント認証の両方が有効になります。

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：

- ・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クリックして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 階層および第 3 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. [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。

注意： [更新] 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 [更新] 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。

8-3. 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。Squid 版、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. [システム管理] → [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クリックしてオンにします。



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

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： 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クリックして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。

[■ 認定設定] - [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。

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. [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。

注意： [更新] 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 [更新] 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。

8-4. 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。Squid 版、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 もしくは ISWM が接続されたプロキシサーバと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 に対して基本認証 (NTLM 認証なし) 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 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、ログインする時には、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。

NTLM 認証をする場合は、次の手順で設定してください。

1. [システム管理] → [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クリックしてオンにします。



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クリックしてオンにします。

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。
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. [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。

注意： [更新] 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 [更新] 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。

8-5. 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) または NTLM 認証設定後、次の手順で登録します。

1. [システム管理] → [認証設定] で、[LDAP サーバ情報へ] ボタンをクリックします。

[LDAP サーバ情報] が表示されます。



注意： [LDAP サーバ情報へ] ボタンは、[システム管理] → [認証設定] - [認証方式] で [Basic 認証] - [LDAP 連携を行う] または [NTLM 認証] を設定した場合だけ、表示されます。認証設定方法については、「8-3. Basic 認証 (LDAP 連携) を設定する」(109 ページ) または 「8-4. NTLM 認証を設定する」(112 ページ) を参照してください。

2. [新規サーバ登録] 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]、[検索条件] の設定が異なります。「8-8. Active Directory 連携時の LDAP サーバ設定」(132 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

NetBIOS ドメイン名 (NTLM 認証設定時のみ)	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	LDAP サーバの IP アドレスまたはドメイン名を入力します。
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。
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行います。

注意： [システム管理] → [認証設定] - [認証方式] で [BASIC 認証] を設定した場合、NetBIOS ドメイン名は表示されません。

[■ LDAP 連携設定] - [検索条件]

アカウント	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	グループの検索条件とスキーマをそれぞれ設定します。

-
- 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、既にスタティック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。
 <インストールディレクトリ>/conf/proxy.inf で、次の設定をしてください。
 [LDAP]
 SCHEMA_LIST=ou,cn,name,dc,sn,givenName,uid,o,sAMAccountName
-

- 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。

注意： [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 サーバ情報] 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. [システム管理] → [認証設定] で、[LDAP サーバ情報へ] ボタンをクリックします。

[LDAP サーバ情報] が表示されます。

注意： [LDAP サーバ情報へ] ボタンは、[システム管理] → [認証設定] - [認証方式] で [Basic 認証] - [LDAP 連携を行う] または [NTLM 認証] を設定した場合だけ、表示されます。

認証設定方法については、「8-3. Basic 認証 (LDAP 連携) を設定する」(109 ページ) または「8-4. NTLM 認証を設定する」(112 ページ) を参照してください。

2. [■ 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。

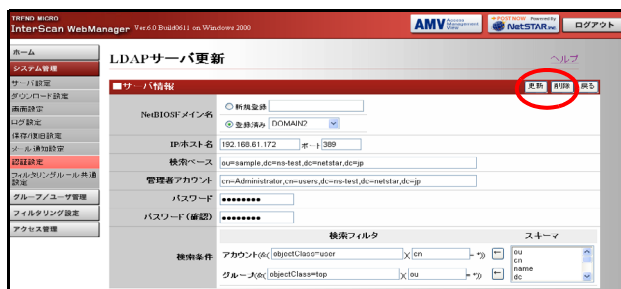
[LDAP サーバ更新] が表示されます。



注意： [システム管理] → [認証設定] - [認証方式] で [BASIC 認証] を設定した場合、NetBIOS ドメイン名は表示されません。

- LDAP サーバを削除する場合は [削除] を、サーバ情報を変更する場合は必要項目を変更して [更新] 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、114 ページの「8-5. LDAP サーバの登録と管理」を参照してください。



確認のダイアログが表示されます。

- [OK] ボタンをクリックします。

8-6. LDAP サーバとの連携を設定する

Basic 認証 (LDAP 連携) または NTLM 認証設定後、登録した LDAP サーバの連携優先順位を設定し、連携を実行します。設定した優先順位にしたがって、同期設定、アカウントの認証、自動連携を行います。

1. [システム管理] → [認証設定] で、[LDAP サーバ情報へ] ボタンをクリックします。

[LDAP サーバ情報] 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： [LDAP サーバ情報へ] ボタンは、[システム管理] → [認証設定] - [認証方式] で [Basic 認証] - [LDAP 連携を行う] または [NTLM 認証] を設定した場合だけ、表示されます。

認証設定方法については、「8-3. Basic 認証 (LDAP 連携) を設定する」(109 ページ) または「8-4. NTLM 認証を設定する」(112 ページ)を参照してください。

2. LDAP サーバの NetBIOS ドメイン、連携優先順位を設定します。

[■ LDAP サーバ情報]

NetBIOS ドメイン名 (NTLM 認証設定時のみ)	Active Directory で設定した NetBIOS ドメイン名を入力します。 15字以内。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。) [デフォルトドメイン]をクリックして選択状態にすると、デフォルトで使用する NetBIOS ドメインに設定されます。
IP / ホスト名	LDAP サーバの IP / ホスト名が表示されます。
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。
優先順位	連携優先順位を変更するLDAPサーバの[優先順位]欄をクリックして選択すると、[↑]、[↓] ボタンで連携優先順位を変更できます。

注意： [システム管理] → [認証設定] - [認証方式] で [BASIC 認証] を設定した場合、NetBIOS ドメイン名は表示されません。

3. LDAP サーバとの連携を設定します。

[■ LDAP 連携設定] - [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、122 ページの「LDAP サーバとの自動連携設定」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 連携設定] の [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。

注意： [更新] 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 [更新] 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。

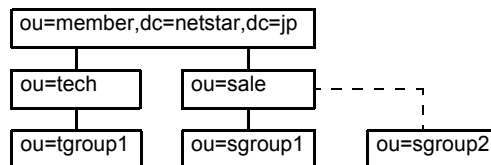
以上で、LDAP サーバとの連携設定は完了です。

■ LDAP サーバとの自動連携設定

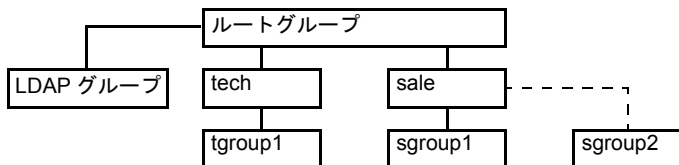
LDAP サーバとの自動連携機能を使用することで、LDAP サーバに登録されたグループおよびユーザーに対して、適切なフィルタリングの設定を自動で適用します。

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

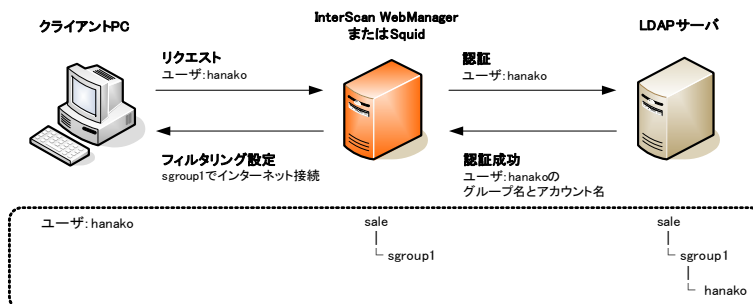


ISWM で自動構築されるグループ



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、201 ページの「第 4 章 フィルタリングの設定」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。例外ユーザ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。インポート後に例外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。

8-7. LDAP サーバと同期する

Basic 認証 (LDAP 連携) または NTLM 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. [システム管理] → [認証設定] で、[LDAP 同期設定へ] ボタンをクリックします。

[LDAP 同期設定] が表示されます。



注意： [LDAP 同期設定へ] ボタンは、[システム管理] → [認証設定] - [認証方式] で [Basic 認証] - [LDAP 連携を行う] または [NTLM 認証] を設定した場合だけ、表示されます。

認証設定方法については、「8-3. Basic 認証 (LDAP 連携) を設定する」(109 ページ) または「8-4. NTLM 認証を設定する」(112 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。

LDAP同期設定

■ユーザ情報同期

現在LDAPサーバに登録されているフィルタリングサーバに未登録のアカウントです。
 「登録/全登録」を行うと選択されているアカウント情報がフィルタリングサーバに登録されます。

全12ページ

[全登録] [登録] [削除]

未登録アカウント一覧:

LDAPサーバ名	グループ	アカウント	登録
192.168.61.172	研究室	user01	☐
	研究室	user02	☐
	研究室	user03	☐
	研究室	user04	☐
	LDAP	user05	☐
	LDAP	user06	☐
	LDAP	user07	☐
	営業部	user08	☐
	営業部・販売課	user09	☐
	営業部・販売課	user10	☐
	開発部	user11	☐
	開発部	user12	☐
	開発部	user13	☐
	開発部・品質管理課	user14	☐
	開発部・品質管理課	user15	☐
	開発部・設計1課	user16	☐
	開発部・設計1課	user17	☐
	開発部・設計1課	user18	☐
	開発部・設計1課	user19	☐
	開発部・設計2課	user20	☐

削除済みアカウント一覧:

グループ	アカウント	削除
GROUP	group	☐

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、[削除済みアカウント一覧] 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] 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

[システム管理] → [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/ユーザ選択] をクリックします。

[グループ/ユーザ選択] 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。

[■ LDAP グループ特定条件] 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. [アカウント取り込み対象とする] - [有効] チェックボックスをクリックしてオンにします。



注意： [アカウント取り込み対象とする] を有効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。

4. 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。

126 ページの「グループごとにユーザ抽出条件を指定する場合」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ることができます。

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。

5. [■グループ更新] の [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。

新規グループを登録する場合は、[登録] ボタンをクリックします。

注意： [更新] 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 [更新] 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。

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：

- [システム管理] → [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 同期設定] 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. [システム管理] → [認証設定] で、[LDAP 同期設定へ] ボタンをクリックします。
[LDAP 同期設定] 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、[更新] 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。



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。

■ユーザ情報同期

現在LDAPサーバに登録されていてフィルタリングサーバに未登録のアカウントです。
「登録/全登録」を行うと選択されているアカウント情報がフィルタリングサーバに登録されます。

全2ページ(21件) 前へ 1 2 次へ

[全登録] 全ての未登録アカウントを登録します **[登録]** 選択された未登録アカウントを登録します

LDAPサーバ名	グループ	アカウント	☐	☐
192.168.61.172	LDAP	user01	☐	
	LDAP	user02	☐	
	ns-test_admins	user03	☐	
	ns-test_admins	user04	☐	
192.168.61.155	LDAP	user05	☐	
	LDAP	user06	☐	
	LDAP	user07	☐	
	LDAP	user08	☐	
	LDAP	user09	☐	
	LDAP	user10	☐	
	LDAP	user11	☐	
	LDAP	user12	☐	
	LDAP	user13	☐	
	LDAP	user14	☐	
	LDAP	user15	☐	
	LDAP	user16	☐	
	test_test_admins	user17	☐	
	test_test_admins	user18	☐	
	test_test_admins	user19	☐	
	test_test_admins	user20	☐	

未登録アカウント一覧:

現在フィルタリングサーバにあってLDAPサーバに存在しないアカウントです。
「削除/全削除」を行うと選択されているアカウントがフィルタリングサーバから削除されます。

全1ページ(1件)

[全削除] 全ての削除済みアカウントを削除します **[削除]** 選択された削除済みアカウントを削除します

GROUP	アカウント	☐
GROUP	guest	☐

削除済みアカウント一覧:

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、[削除済みアカウント一覧]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。

8-8. 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 Active Directory と連携する場合、[システム管理]→[認証設定]→[LDAP サーバ情報]→[LDAP サーバ登録]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、[システム管理] → [認証設定] → [LDAP サーバ情報] → [LDAP サーバ登録] 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

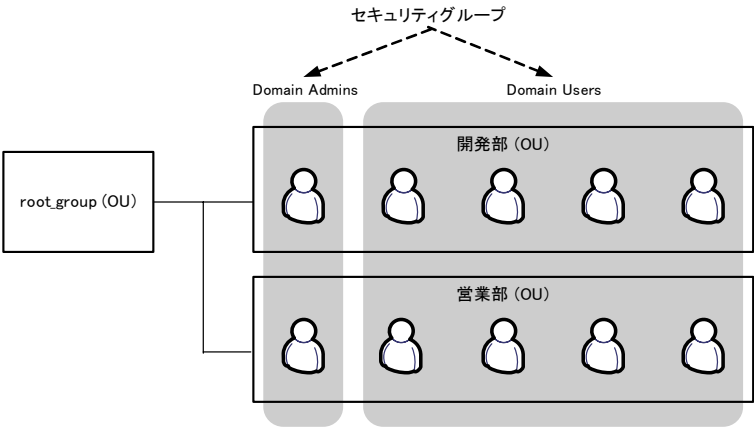
検索ベース	ou=root_group,dc=tsr_test,dc=netstar,dc=jp
管理者アカウント	cn=yamada,cn=users,dc=tsr_test,dc=netstar,dc=jp
アカウント	(&(objectClass=user)(sAMAccountName=*))

● 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。

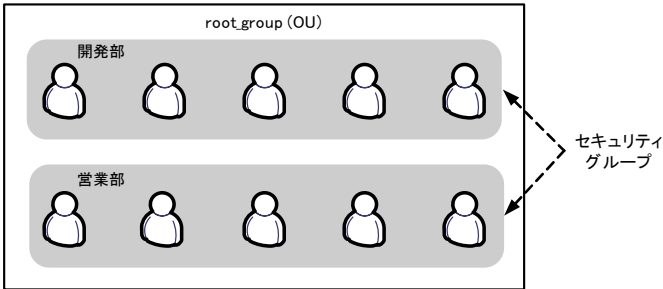
-
- 注意：**
- 設定例ではルートグループ (root_group) にセキュリティグループを作成していますが、セキュリティグループは任意の場所に作成できます。
 - 属性名が「memberOf」の場合には、セキュリティグループをインポートします。属性名を変更することにより、セキュリティグループ以外の情報でもインポートできます。例えば、属性名を「cn」、属性値を「yamada」に設定すると、「yamada」だけをインポートします。ただし、検索範囲がユーザのプロパティの内部となるため、「ou」や「営業部」などを指定してもインポートできません。
 - 部署の構造を Active Directory 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



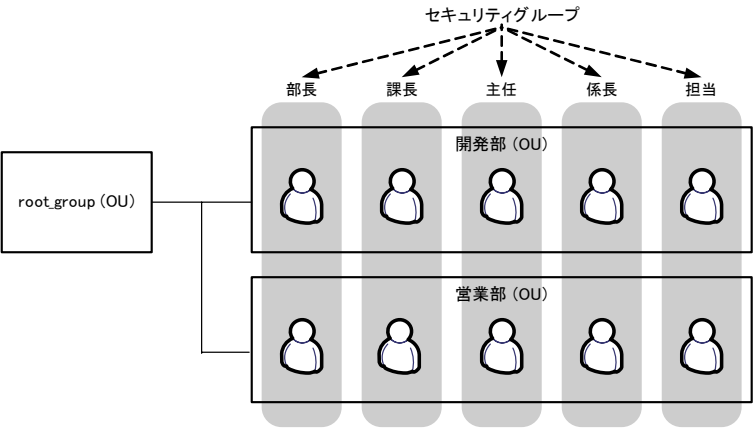
セキュリティグループ	属性値
Domain Admins	cn=Domain Admins,ou=root_group,dc=tsr_test,dc=netstar,dc=jp

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。

9. フィルタリングルール共通設定

フィルタリングルール共通設定画面では、フィルタリングルールに共通で適用される以下の設定をします。

- ・ 書き込み規制
- ・ HTTPS 規制
- ・ 規制解除申請
- ・ ユーザ設定カテゴリ

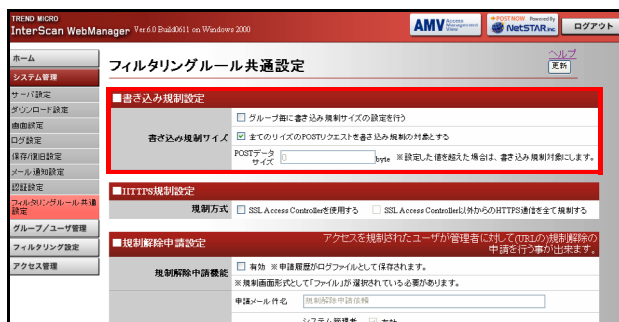
9-1. 書き込み規制を設定する

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。以下の3つの規制方法があります。

- ・ グループごとに指定したサイズを超える書き込みを規制する
- ・ すべての書き込みを規制する
- ・ 指定したサイズを超える書き込みを規制する

注意： Squid 版では POST リクエストの設定ができないため、[■書き込み規制設定] が表示されません。

1. [システム管理] → [フィルタリングルール共通設定] をクリックします。
[フィルタリングルール共通設定] が表示されます。
2. 書き込み規制の内容を設定します。



[■書き込み規制設定] - [書き込み規制サイズ]

グループ毎に書き込み規制サイズの設定を行う	グループごとに書き込み規制サイズを設定し、設定したサイズを超える書き込み (POST リクエスト) を、規制の対象とする場合に、チェックボックスをオンにします。グループごとの書き込み規制は、[グループ設定] - [規制オプション設定] - [書き込み規制] で設定します。詳しくは、270 ページの「7. 規制オプションの設定」を参照してください。
全てのサイズの POST リクエストを書き込み規制の対象とする	すべての書き込み (POST リクエスト) を規制する場合に、チェックボックスをオンにします。
POST データサイズ	指定したサイズ (byte 単位) を超える POST リクエストを規制する場合に入力します。

3. [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、書き込み規制 の設定は完了です。

9-2. HTTPS 規制を設定する

SSL Access Controller による規制の有効 / 無効を設定します。SSL Access Controller とは、HTTPS プロトコルのフィルタリングを実行するためにクライアント PC にインストールする、Internet Explorer 専用のアドオンプログラムです。インストール方法等については、336 ページの「4. SSL Access Controller の設定」を参照してください。

HTTPS 規制を有効にすると、SSL Access Controller をインストールしたクライアント 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。

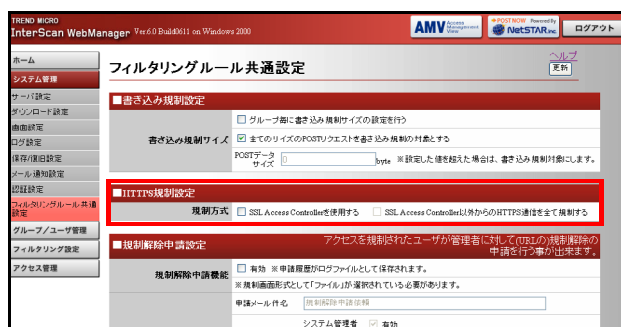
-
- 注意：**
- HTTPS 規制はスタンドアロン版、ICAP 版でご利用いただけます。Squid 版では [■ HTTPS 規制設定] は表示されません。
 - SSL Access Controller がインストールされていないクライアント PC では、HTTPS サイトをドメイン単位でしか規制できません。
 - SSL Access Controller による HTTPS 規制は、書き込み規制には適用されません。
-

1. [システム管理] → [フィルタリングルール共通設定] をクリックします。
[フィルタリングルール共通設定] が表示されます。

2. [■ HTTPS 規制設定] - [規制方式] で HTTPS 規制の設定をします。

規制を有効にする場合は、[SSL Access Controllerを使用する]チェックボックスをオンにしてください。[SSL Access Controller 以外からの HTTPS 通信をすべて規制する]チェックボックスも自動的にオンになります。必要に応じてオフにしてください。

[■ HTTPS 規制設定] の設定と、SSL Access Controller インストール有無によって、実際にクライアント PC に適用される HTTPS 通信規制については、337 ページの「4-1. ISWM との連携設定」を参照してください。



3. [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、HTTPS 規制の設定は完了です。

9-3. 規制解除申請を設定する

規制された URL にアクセスしたとき、Web ブラウザから規制解除を申請できます。規制解除申請はログファイルとして保存されます。また、メール通知設定が有効な場合、システム管理者や設定した通知先にメールを送信できます。

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、85ページの「規制画面について」を参照してください。

- 注意：**
- Squid 版の場合、https プロトコルの URL では規制解除申請機能を使用できません。
 - 規制解除申請機能を利用する場合、[システム管理] - [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、84 ページの「4-2. 規制画面形式を設定する」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. [システム管理] → [フィルタリングルール共通設定] をクリックします。
[フィルタリングルール共通設定] が表示されます。
2. [■規制解除申請設定] - [規制解除申請機能] の [有効] チェックボックスをクリックしてオンにします。

申請メール通知設定が設定可能になります。申請内容をメールで通知する場合、手順 3 に進み申請メール通知設定を設定します。申請内容をメールで通知しない場合、手順 4 に進みます。



注意： メールによる規制解除の申請通知をする場合、[申請メール通知先] でメールの送付先を設定してください。また、[システム管理] - [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、102ページの「7. メール通知設定」を参照してください。

3. 申請メールの件名、通知先を設定します。

[■ 規制解除申請設定] - [申請メール通知設定]

申請メール件名		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。
申請メール通知先	システム管理者	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。 - グループ管理者に対する通知なし 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のみに通知 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。 - 所属グループ管理者のみに通知 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。 - 全てのグループ管理者に通知 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。

-
- 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、[アクセス管理]-[アクセスログ管理]で確認できます。詳しくは、317 ページの「第 7 章 アクセスログの管理」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。
 - ・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。
-

4. [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。

-
- 注意：** [更新] 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 [更新] ボタンをクリックしてください。
-

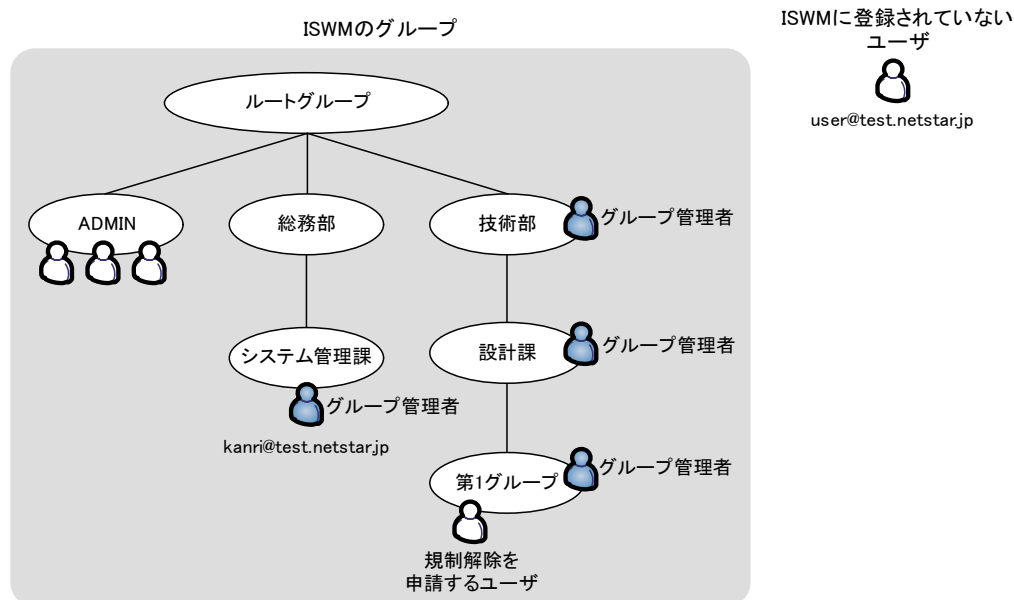
5. [OK] ボタンをクリックします。

以上で、規制解除申請の設定は完了です。

■ 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グループのユーザー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

[有効] 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のみに通知] 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。

・ [所属グループ管理者のみに通知] 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。

・ [全てのグループ管理者に通知] 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@test.netstar.jp」、および ISWM に登録されていないメールアドレス「user@test.netstar.jp」を指定した場合、両方にメールで通知します。

9-4. ユーザ設定カテゴリのサブカテゴリ名を設定する

ユーザ設定カテゴリは 10 個のサブカテゴリで構成され、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、226 ページの「3. カテゴリ別フィルタリングルールを設定」を参照してください。

1. [システム管理] → [フィルタリングルール共通設定] をクリックします。

[フィルタリングルール共通設定] が表示されます。

2. [■カテゴリ設定] 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。

The screenshot shows the 'Filtering Rule Common Settings' page in the Trend Micro InterScan WebManager. The 'Category Settings' section is highlighted with a red box. It contains a table with 10 rows, each representing a user setting category (ユーザ設定1 to ユーザ設定10). The table has two columns: 'Category Name' and 'Subcategory Name'. The 'Subcategory Name' column is currently empty for all rows, indicating where the administrator can enter new subcategory names.

ユーザ設定1	ユーザ設定2	ユーザ設定3	ユーザ設定4	ユーザ設定5	ユーザ設定6	ユーザ設定7	ユーザ設定8	ユーザ設定9	ユーザ設定10

3. [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、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別ルール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。

MEMO

ユーザとグループの管理

1. グループとユーザについて

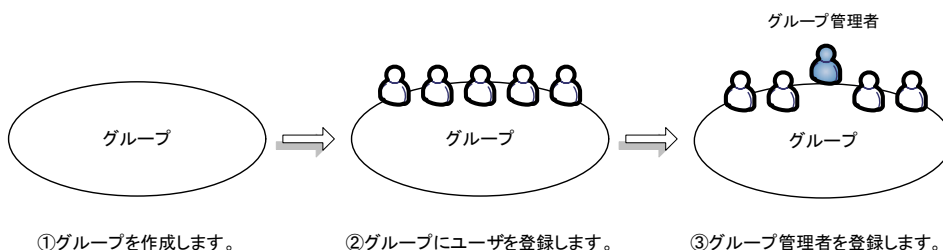
ここでは、ユーザとグループについて、設定前に知っておいていただきたい内容について説明します。

1-1. グループとユーザ

Trend Micro InterScan WebManager（以下、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

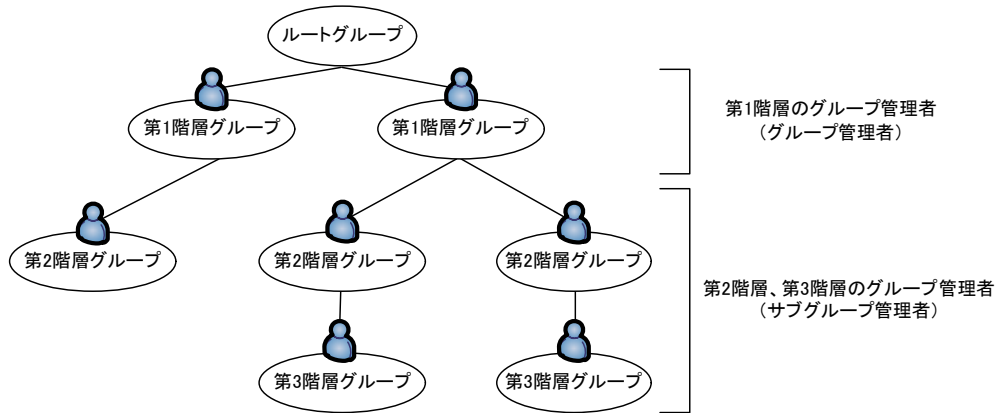


ISWM では、「ルートグループ」を頂点とするツリー構造でグループを管理します。ルートグループの直下を「第1階層グループ」として、「第3階層グループ」まで作成できます。

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3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。

本書では、第2階層、第3階層のグループ管理者を、「サブグループ管理者」と呼びます。

グループ管理者とサブグループ管理者



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、105 ページの「8. ユーザ認証の設定」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、グループを削除することはできません。

■ LDAP との連携

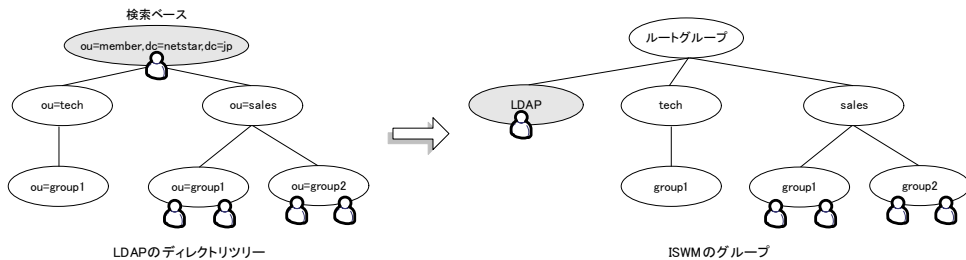
[システム管理] → [認証設定] で、LDAP 連携を有効にしている場合、LDAP グループ特定方式の設定により、2 種類の登録方法があります。

● 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、検索結果のルートに存在するユーザが「LDAP」グループに登録されます。

検索結果のルート階層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)

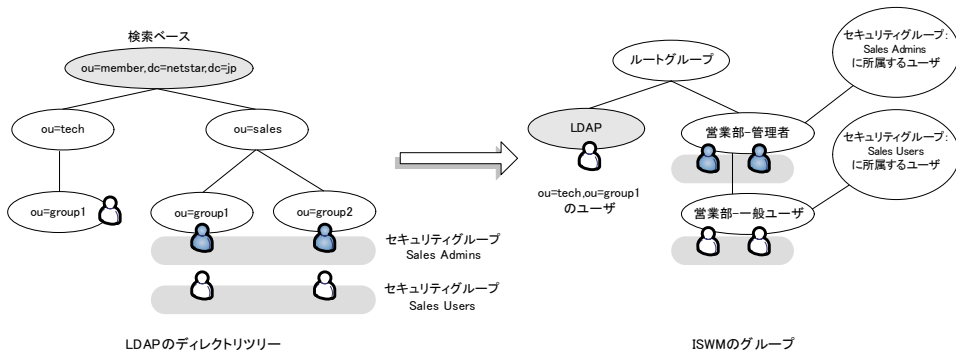


● グループ毎にユーザ抽出条件を指定する

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)

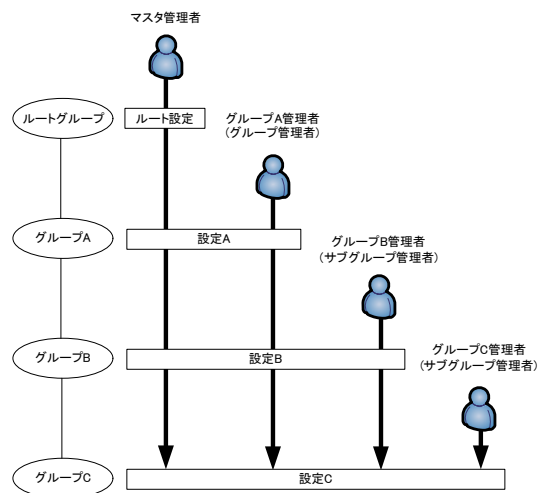


1-3. グループとフィルタリング設定

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。

マスタ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。グループ管理者およびサブグループ管理者は、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、[システム管理]→[認証設定]でユーザ認証を有効にしてください。105ページの「8. ユーザ認証の設定」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

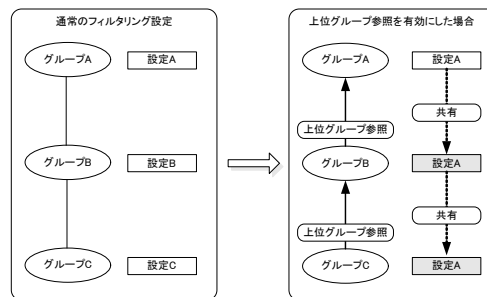
上位グループと下位グループの間で、フィルタリング設定を参照できます。

フィルタリング設定の参照方法には、次の2種類があります。詳細については、211 ページの「1-3. フィルタリング設定の参照」を参照してください。

・ 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）

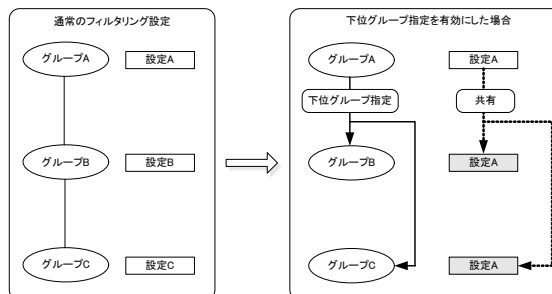
下位グループは、参照先の上位グループからフィルタリング設定を共有できます。

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 [フィルタリング設定] 画面で設定します。



・ 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（下位グループ指定）

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共有させます。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、例外ユーザも設定できません。下位グループ指定は、[フィルタリング設定] 画面で設定します。



注意： 上位グループのフィルタリングルールを最低基準として、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、204 ページの「1-2. フィルタリング機能の概要」を参照してください。

1-4. ユーザについて

ISWMには、次の4種類のユーザ種別があります。ユーザ種別によって、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。

マスタ管理者	ISWMの管理者です。マスタ管理者は、ADMIN グループに所属します。 マスタ管理者は、管理画面のすべての設定が可能です。
グループ管理者	第1階層のグループ管理者です。 管理画面では、所属グループと下位グループのグループ管理、ユーザ管理、フィルタリング設定、アクセスログの管理が可能です。
サブグループ管理者	第2階層、第3階層のグループ管理者です。 管理画面では、所属グループと下位グループのグループ管理、ユーザ管理、フィルタリング設定が可能です。
エンドユーザ	各グループに所属するユーザです。 管理画面では、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：**
- グループ管理者またはサブグループ管理者は、アカウントで登録します。グループ管理者またはサブグループ管理者を IP アドレスで登録することはできません。
 - アカウントで登録したユーザは、[AMV 閲覧権限] をオンにすることで、アクセス マネジメント ビューを使用して、情報漏えいリスクを確認できます。IPアドレスで登録したユーザは、アクセス マネジメント ビューを使用できません。
 - 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、エンドユーザではメールアドレスの変更だけが可能です。

■ 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	[システム管理]→[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。

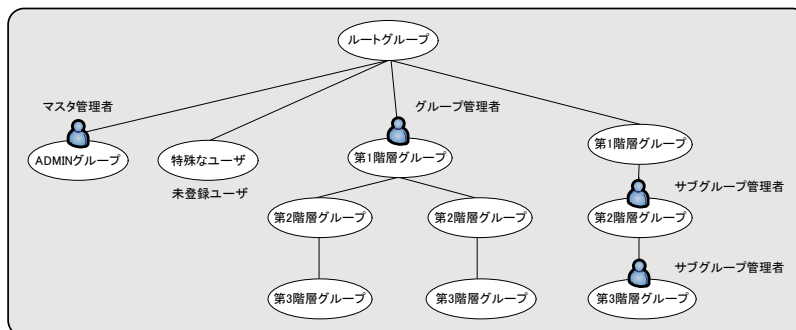
注意：・未登録ユーザは [グループ/ユーザ管理] には表示されません。[フィルタリング設定]→[グループ設定] では、「未登録ユーザ」グループのフィルタリング設定を管理できます。

・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、[システム管理]→[認証設定]で [未登録ユーザ設定] を有効にしてください。105 ページの「8. ユーザ認証の設定」を参照してください。

■ 管理者の管理権限について

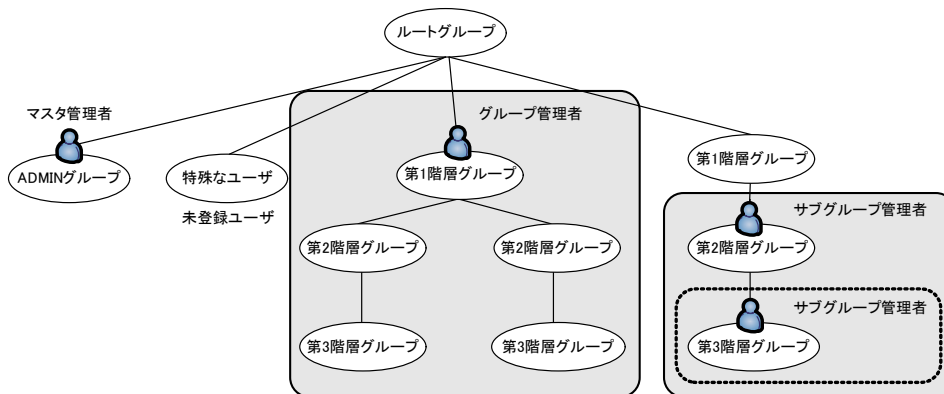
マスタ管理者は、ルートグループ、特殊なグループを含めて、すべてのグループを管理できます。

マスタ管理者の管理範囲



グループ管理者、サブグループ管理者は、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、サブグループ管理者の管理範囲



注意： マスタ管理者、グループ管理者、サブグループ管理者は、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。

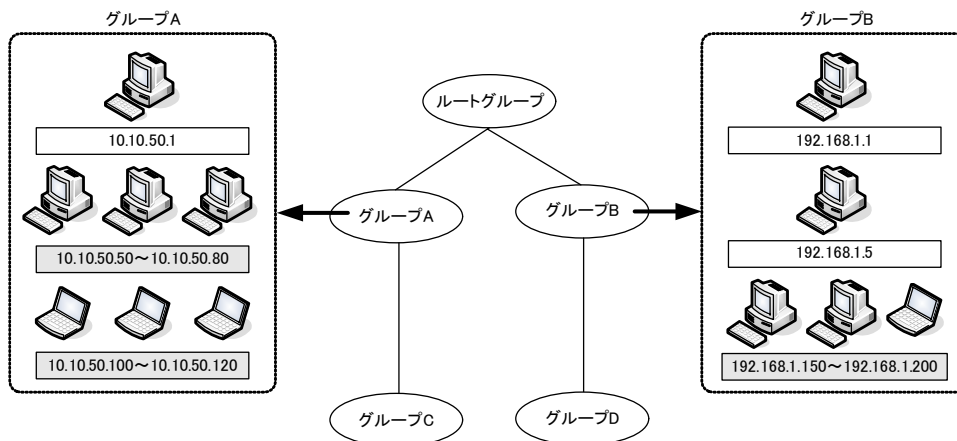
1-5. IP アドレスでユーザを管理する

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、159 ページの「1-6. アカウントでユーザを管理する」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、[システム管理]→[認証設定]でユーザ認証を有効にしてください。
 - ・マスタ管理者は、IP アドレスの登録および管理が可能です。
 - ・グループ管理者およびサブグループ管理者は、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。

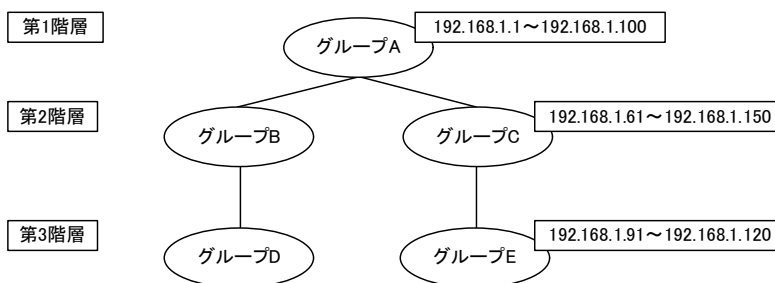
■ 重複する IP アドレス設定

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。

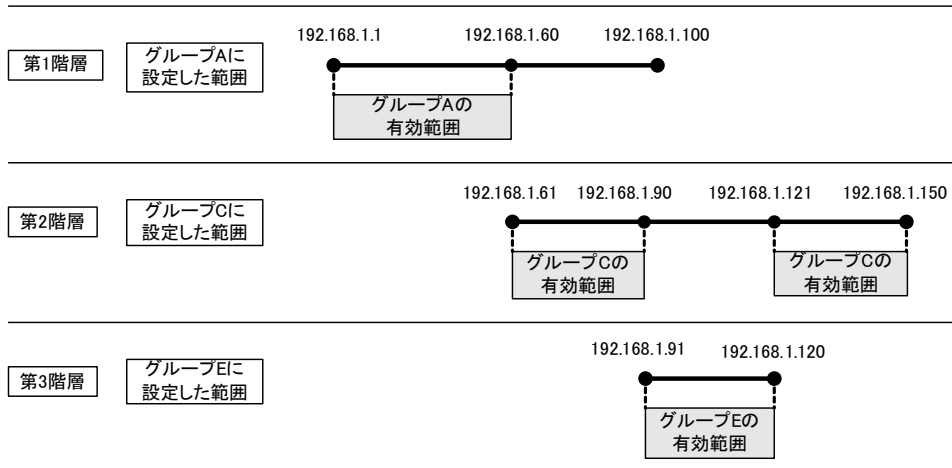
注意：

- ・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、[システム管理] → [IP アドレス一覧] 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。

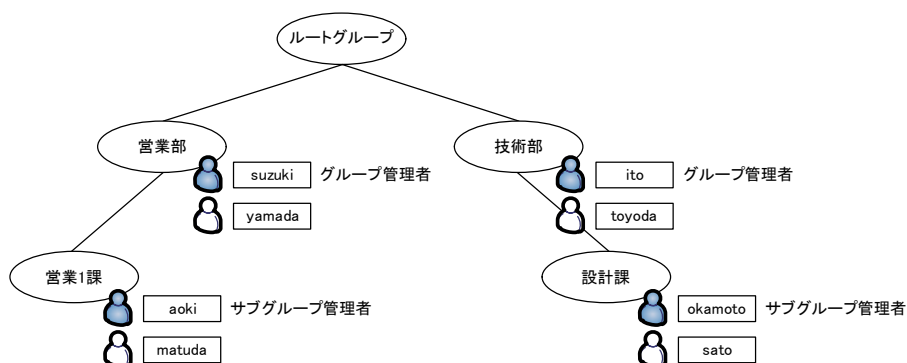
詳細については、193 ページの「5. ユーザ、グループ情報の一括登録、削除」を参照してください。

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、156 ページの「1-5. IP アドレスでユーザを管理する」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、サブ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、認証でき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、[システム管理]→[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。
 - ・[システム管理]→[認証設定] で「未登録ユーザ」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。

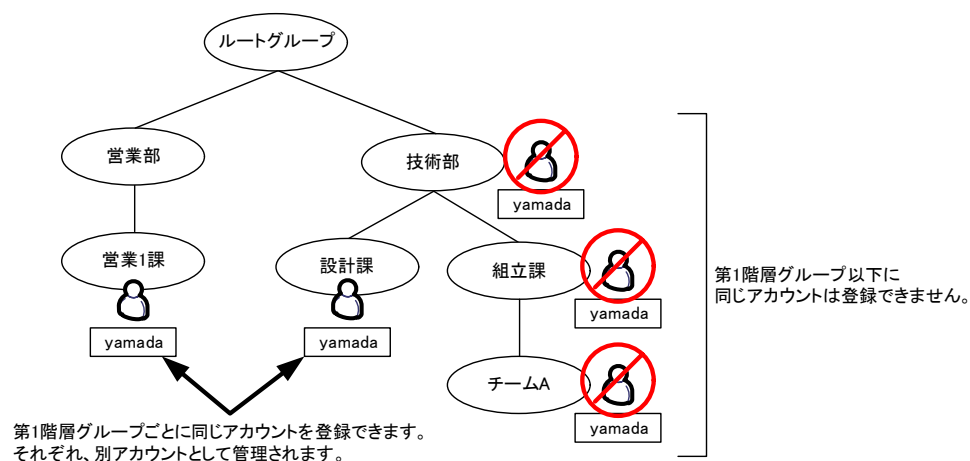
LDAP との連携については、105 ページの「8. ユーザ認証の設定」を参照してください。

■ 同一アカウントの登録

[システム管理] → [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 1 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： [システム管理] → [認証設定] で、[第 1 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、193 ページの「5. ユーザ、グループ情報の一括登録、削除」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。

■ グループ、ユーザの登録、管理

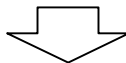
グループ、ユーザは、[グループ/ユーザ選択] で登録、管理します。

グループ、ユーザの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」(166 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」(172 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。

■ グループ、ユーザ情報を一括登録、削除する

[一括登録/削除] 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、193 ページの「5. ユーザ、グループ情報の一括登録、削除」を参照してください。

■ 登録した IP アドレスとグループの一覧を確認する

[IP アドレス一覧] 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、198 ページの「6. IP アドレス設定一覧の確認」を参照してください。

2-1. [グループ / ユーザ選択] 画面の構成

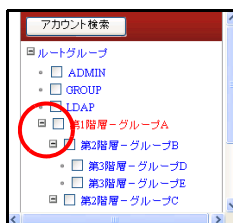
[グループ / ユーザ選択] 画面は、次の3つの要素で構成されます。



■ 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、赤文字で表示されます。[+] 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。

グループ名左側にあるチェックボックスは、アカウントを検索するときに使用します。詳しくは 180 ページの「4-3. アカウントを検索する」を参照してください。

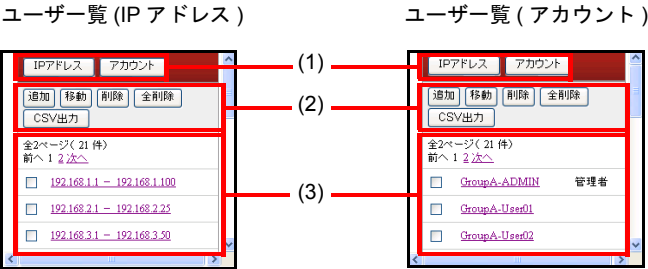


注意： マスタ管理者の場合、すべてのグループが表示されます。

グループ管理者およびサブ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。

■ ユーザー一覧

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] ボタンまたは[アカウント] ボタンをクリックして、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] ボタン	IP アドレス一覧に表示を切り替えます。
[アカウント] ボタン	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。

[追加] ボタン	IP アドレス / アカウントを新規登録します。
[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 / アカウントのグループを移動します。
[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。
[全削除] ボタン	グループ内の IP アドレス / アカウントをすべて削除します。
[CSV 出力] ボタン	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。

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[CSV 出力] ボタンだけが表示されます。

・IP アドレス一覧では、管理者によって表示されるボタンが異なります。マスタ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、サブグループ管理者では、[CSV 出力] ボタンだけが表示されます。

・ルートグループには、[CSV 出力] ボタンだけが表示されます。

- (3) グループ一覧から選択したグループの 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、1 画面に最大 20 件まで表示できます。20 件以上登録されている場合には、1 ページに 20 件ずつ分割して表示されます。

前へ	クリックすると、前のページに戻ります。
ページ数	クリックすると、クリックしたページ番号の IP アドレス一覧を表示します。
次へ	クリックすると、次のページに進みます。

IP アドレス / アカウント表示左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。

■ 設定画面

選択したグループ、ユーザに対する設定画面を表示します。

注意： [更新] 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 [更新] ボタンをクリックしてください。

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、172 ページの「4. ユーザの登録と管理」を参照してください。

[グループ/ユーザ選択] 画面の名称については、163 ページの「2-1. [グループ/ユーザ選択] 画面の構成」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/ユーザ選択] をクリックします。

[グループ/ユーザ選択] 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。

ここでは、第 1 階層にグループを追加するため、[ルートグループ] をクリックしています。



設定画面に [■グループ更新] が表示されます。



3. [■グループ更新] - [グループ登録へ] をクリックします。

[■グループ登録] が表示されます。

■ グループ更新	
グループ情報を更新/削除します。 更新	
グループ名	ルートグループ
グループコメント	
グループ登録へ	グループ登録へ

注意： 次の条件を満たす場合、[■グループ更新] または [■グループ登録] の下に [■LDAP グループ特定条件] 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。
- ・[システム管理] - [認証設定] で、「認証方式」に BASIC 認証 (LDAP 連携) または NTLM 認証を選択し、[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。

[■LDAP グループ特定条件] の設定については、126 ページの「グループごとにユーザ抽出条件を指定する場合」を参照してください。

4. 登録するグループの内容を設定します。

■ グループ登録	
グループを登録します。 登録	
グループ名	
グループコメント	
フィルタリング設定	☐ 上位グループ参照で登録する
	☐ 例外URLを上位グループからコピーする ※最低基準設定が有効な場合「許可カテゴリ」のURLはコピー対象外です
	☐ カテゴリ別規制メッセージを上位グループからコピーする

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。
グループコメント	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。

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、グループコメントには、次の文字を使用できません。

¥ / : ; ? < > | "

[フィルタリング設定]

上位グループのフィルタリング設定を参照するときや、例外 URL 設定またはカテゴリ別規制メッセージを上位グループからコピーする場合に設定します。

上位グループ参照で登録する	オンにすると、上位グループ参照を有効にします。上位グループ参照については、次の項目を参照してください。 「1-3. フィルタリング設定の参照」(211 ページ) 「2-3. 上位グループ参照と下位グループ指定」(224 ページ)
例外 URL を上位グループからコピーする	[上位グループ参照で登録する] がオフのときに設定できます。 オンにすると、上位グループの例外 URL 設定をコピーします。 例外 URL については、250 ページの「5. 例外 URL の設定」を参照してください。
カテゴリ別規制メッセージを上位グループからコピーする	[上位グループ参照で登録する] がオフのときに設定できます。 オンにすると、上位グループのカテゴリ別規制メッセージをコピーします。 カテゴリ別規制メッセージについては、277 ページの「8. カテゴリ別規制メッセージの設定」を参照してください。

注意：・例外 URL、カテゴリ別メッセージのコピーは、グループを登録するときだけに設定できます。

・上位グループで最低基準ルールが設定されている場合、[上位グループで参照する] は表示されません。また、上位グループから例外 URL をコピーしても、「許可カテゴリ」に登録された例外 URL はコピーされません。

・グループを登録した後に上位グループ参照を変更する場合、[フィルタリング設定] → [グループ設定] で設定してください。

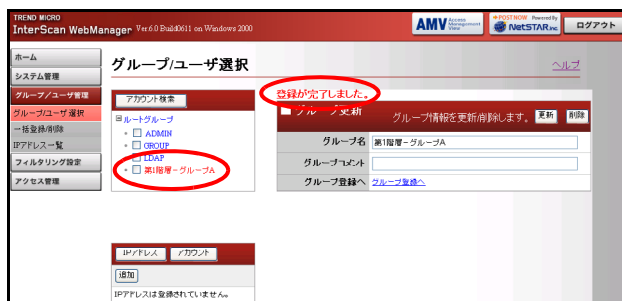
5. [■グループ登録] の [登録] ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK] ボタンをクリックします。

[■グループ更新] に「登録が完了しました。」と表示されます。

グループ一覧にグループが追加されます。また、登録したグループの情報が [■グループ更新] に表示されます。

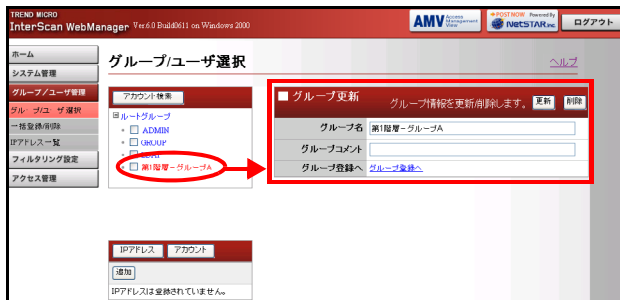


3-2. グループの設定を変更、削除する

グループの設定（グループ名、グループコメント）を変更する方法と、グループを削除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。
 - ・[システム管理]→[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/ユーザ選択]をクリックします。
[グループ/ユーザ選択]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、削除するグループ名をクリックします。
設定画面に[■グループ更新]が表示されます。



注意： 次の条件を満たす場合、[■グループ更新] または [■グループ登録] の下に [■LDAP グループ特定条件] 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。
 - ・[システム管理] - [認証設定] で、「認証方式」に BASIC 認証 (LDAP 連携) または NTLM 認証を選択し、[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。
- [■ LDAP グループ特定条件] の設定については、126 ページの「グループごとにユーザ抽出条件を指定する場合」を参照してください。
-

3. グループの設定を変更する場合、グループ名、グループコメントを変更します。
設定項目については、166 ページの「3-1. グループを登録する」を参照してください。
4. [更新] 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： [更新] 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 [更新] 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。
グループの設定を変更した場合、「更新が完了しました。」と表示されます。
グループを削除した場合、「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、147ページの「1. グループとユーザについて」を参照してください。

[グループ/ユーザ選択] 画面の名称については、163ページの「2-1. [グループ/ユーザ選択] 画面の構成」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	173 ページ	176 ページ
アカウントを検索する	—	180 ページ
ユーザ情報を変更する	182 ページ	
ユーザのグループを移動する	184 ページ	
ユーザを削除する	187 ページ	
グループ内のユーザー一覧をファイルに出力する	190 ページ	

■ IP アドレスの管理で利用できる機能

IPアドレスの管理はマスタ管理者、グループ管理者、サブグループ管理者で利用できる機能が異なります。

	マスタ管理者	グループ管理者	サブグループ管理者
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。

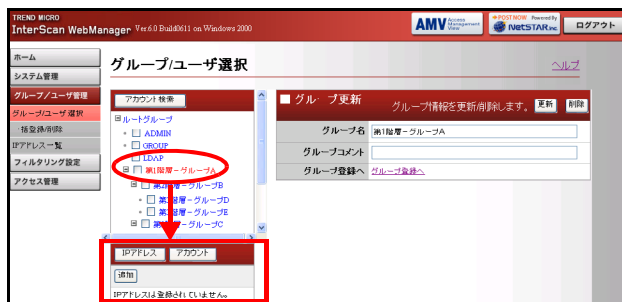
※所属するグループおよび下位グループの CSV 出力が可能です。

4-1. IP アドレスを登録する

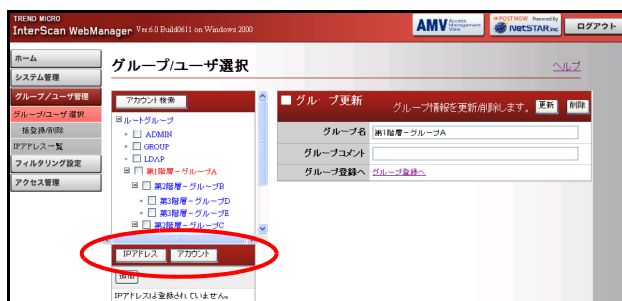
グループに IP アドレスを登録します。IP アドレスは単一、または範囲指定して登録できます。

注意： IP アドレスを登録できるのは、マスタ管理者だけです。

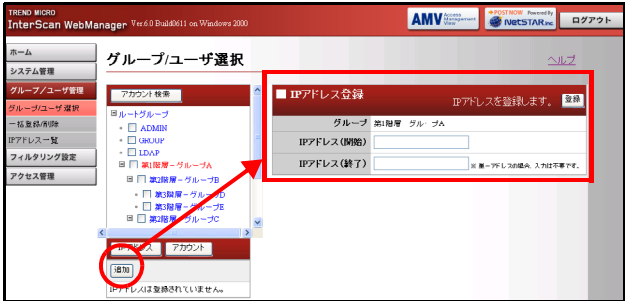
1. [グループ/ユーザ管理] → [グループ/ユーザ選択] をクリックします。
[グループ/ユーザ選択] が表示されます。
2. グループ一覧から、IP アドレスを登録するグループ名をクリックします。
ユーザー一覧が表示されます。



3. [IP アドレス] ボタンをクリックします。



4. IP アドレスの登録を開始します。ユーザー一覧の [追加] ボタンをクリックします。
- 設定画面に [■ 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。

■ IPアドレス登録

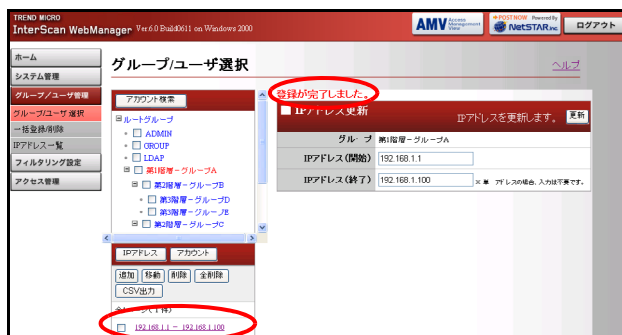
IPアドレスを登録します。 登録

グループ	第1階層-グループA
IPアドレス(開始)	
IPアドレス(終了)	※ 単一アドレスの場合、入力不要です。

グループ	IP アドレスを登録するグループ名が表示されます。
IP アドレス (開始) (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。
IP アドレス (終了)	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「IP アドレス (開始)」 < 「IP アドレス (終了)」となるように入力してください。

6. [■ IP アドレス登録] の [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。
7. [OK] ボタンをクリックします。
[■ IP アドレス更新] に「登録が完了しました。」と表示されます。
ユーザー一覧に IP アドレスが追加されます。また、登録した IP アドレスの情報が [■ IP アドレス更新] に表示されます。



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、ユーザー一覧に操作ボタンが追加されます。

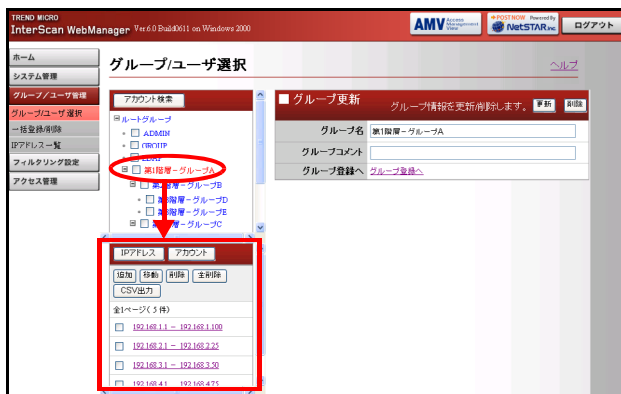
4-2. アカウントを登録する

グループにアカウントを登録します。グループ管理者、サブグループ管理者の設定やアクセス マネジメント ビューの閲覧許可も設定できます。

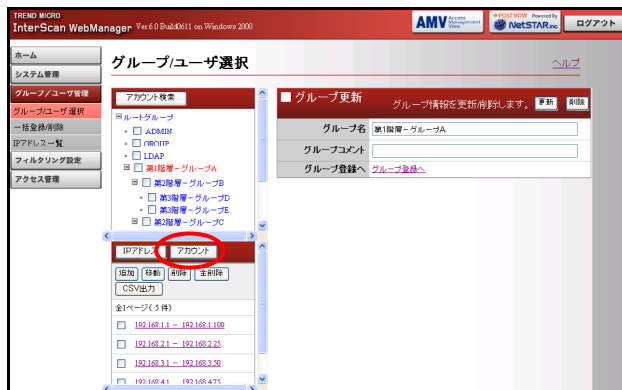
注意： LDAP 連携が有効な場合、アカウントの移動だけが可能です。アカウントの登録および削除はできません。

1. [グループ/ユーザ管理] → [グループ/ユーザ選択] をクリックします。
[グループ/ユーザ選択] 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。
ユーザー一覧が表示されます。



3. [アカウント] ボタンをクリックします。



4. ユーザー一覧の [追加] ボタンをクリックします。
設定画面に [■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。

■ アカウント登録

アカウントを登録します。

グループ	第1階層-グループA
アカウント	
パスワード	
パスワード(確認)	
メールアドレス	
グループ管理者	☐
AMV閲覧権限	☐ ※ Access Management Viewの閲覧を許可します

グループ	アカウントを登録するグループ名が表示されます。
アカウント (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。
グループ管理者	チェックボックスをオンにすると、登録するアカウントをグループ管理者、またはサブグループ管理者に設定します。
AMV 閲覧権限	チェックボックスをオンにすると、アクセス マネジメントビューの閲覧を許可します。 アクセス マネジメント ビューについては、301 ページの「第 6 章 アクセス マネジメント ビューの操作」を参照してください。

注意：・アカウント、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、アカウントには半角スペースも使用できます。
!#\$%&'()*=~{+}_-^@[].*/<>|

・[AMV 閲覧権限] がオフの場合、登録したアカウントで管理画面にログインしても、 (アクセス マネジメント ビューへのリンク)は表示されません。

6. [■アカウント登録] の [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。

7. [OK] ボタンをクリックします。

[■アカウント更新] に「登録が完了しました。」と表示されます。

ユーザー一覧にアカウントが追加されます。また、登録したアカウントの情報が [■アカウント更新] に表示されます。



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、ユーザー一覧に操作ボタンが追加されます。

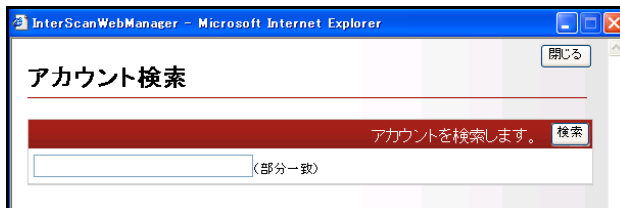
4-3. アカウントを検索する

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] → [グループ/ユーザ選択] をクリックします。
[グループ/ユーザ選択] が表示されます。
2. 検索対象にするグループのチェックボックスをオンにします。
すべてのグループを検索対象にする場合、チェックボックスはすべてオフにします。
3. グループ一覧の [アカウント検索] ボタンをクリックします。



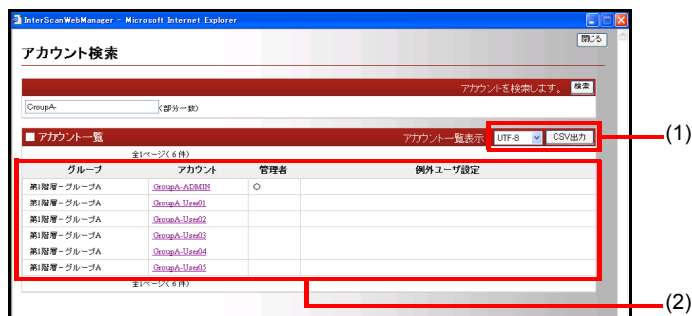
[アカウント検索] 画面が別ウィンドウで表示されます。



4. 検索条件を入力します。
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。



- (1) 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情報が管理画面に表示されます。アカウント一覧の各項目は、次のとおりです。

グループ	所属するグループを表示します。
アカウント	アカウント名を表示します。 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情報が管理画面に表示されます。
管理者	グループ管理者の場合、「○」が表示されます。
例外ユーザ設定	例外ユーザの場合、「○」が表示されます。

注意： アカウント名をクリックすると、検索結果の画面が自動的に閉じ、ユーザーに検索結果が表示されます。また、設定画面にアカウント情報が表示されます。

- (2) エンコードを選択して、[CSV 出力] 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。エンコードは、[UTF-8]、[Shift_JIS]、[EUC_JP] から選択できます。出力した CSV ファイルのフォーマットについては、190 ページの「4-7. IP アドレス / アカウント一覧をファイルに出力する」を参照してください。

6. [アカウント検索] 画面の [閉じる] ボタンをクリックします。

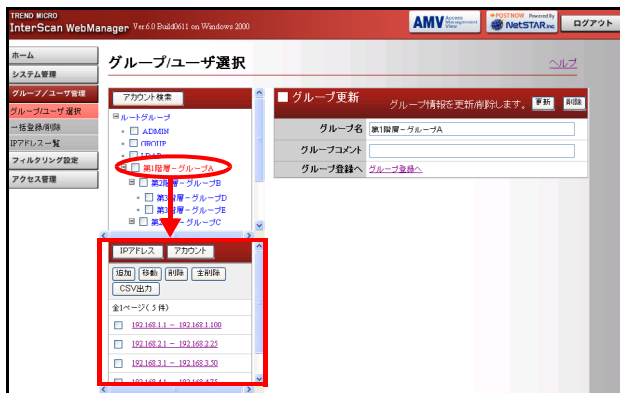
[アカウント検索] 画面が閉じます。

4-4. 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、マスタ管理者だけです。

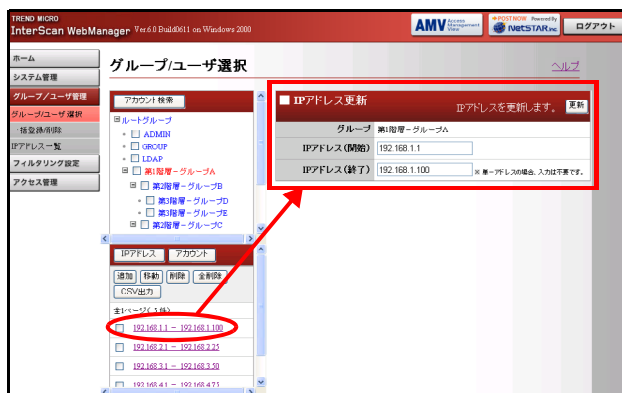
1. [グループ / ユーザ管理] → [グループ / ユーザ選択] をクリックします。
[グループ / ユーザ選択] が表示されます。
2. グループ一覧から、変更する IP アドレス / アカウントが登録されているグループ名をクリックします。
ユーザー一覧が表示されます。



3. [IP アドレス] ボタンまたは [アカウント] ボタンをクリックして、ユーザー一覧の表示を切り替えます。

4. ユーザー一覧から、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。

設定画面に [■ IP アドレス更新] / [■ アカウント更新] が表示されます。
ユーザー一覧の操作方法については、164 ページの「ユーザー一覧」を参照してください。



5. 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、173 ページの「4-1. IP アドレスを登録する」を参照してください。

アカウントの設定項目については、176 ページの「4-2. アカウントを登録する」を参照してください。

6. [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。

注意： [更新] 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 [更新] 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。

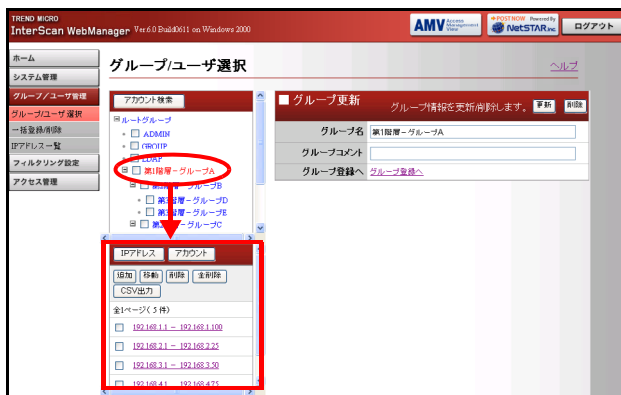
4-5. IP アドレス / アカウントのグループを移動する

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、マスタ管理者だけです。

1. [グループ/ユーザ管理] → [グループ/ユーザ選択] をクリックします。
[グループ/ユーザ選択] 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。

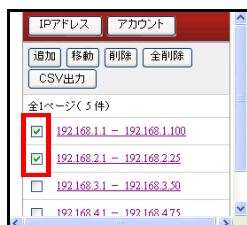
ユーザー一覧が表示されます。



3. [IP アドレス] ボタンまたは [アカウント] ボタンをクリックして、ユーザー一覧の表示を切り替えます。

4. ユーザー一覧から、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。

ユーザー一覧の操作方法については、164 ページの「ユーザー一覧」を参照してください。

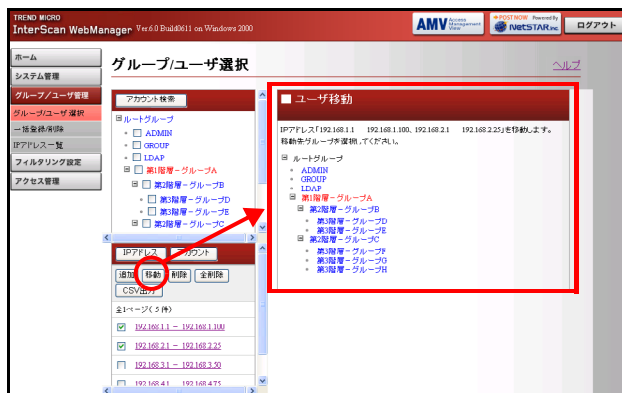


注意： 1 回の操作で移動可能な IP アドレス / アカウントは、1 ページ内の最大 20 件までです。
複数ページの IP アドレス / アカウントを移動する場合には、1 ページごとに移動してください。

5. ユーザー一覧の [移動] ボタンをクリックします。

設定画面に [■ユーザ移動] が表示されます。

[■ユーザ移動] のツリーの操作方法は、グループ一覧と同様です。



6. [■ユーザ移動] 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。

4-6. 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は、次の 2 種類があります。

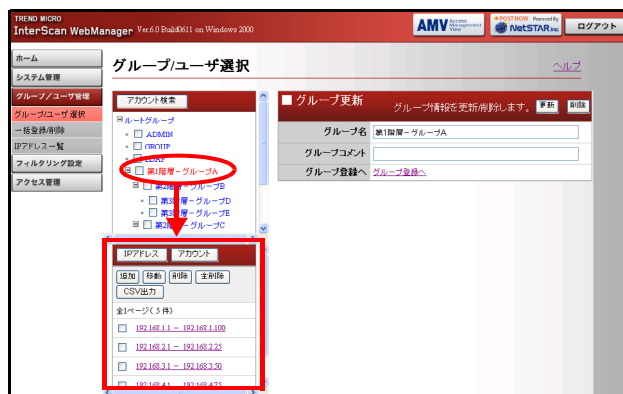
- ・ グループ内の指定した IP アドレス / アカウントを削除する。
- ・ グループ内の IP アドレス / アカウントをすべて削除する。

注意： IP アドレスを削除できるのは、マスタ管理者だけです。

■ グループ内の指定した IP アドレス / アカウントを削除する

1. [グループ/ユーザ管理] → [グループ/ユーザ選択] をクリックします。
[グループ/ユーザ選択] 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。

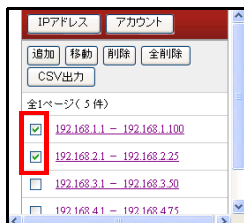
ユーザー一覧が表示されます。



3. [IP アドレス] ボタンまたは [アカウント] ボタンをクリックして、ユーザー一覧の表示を切り替えます。

4. ユーザー一覧から、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。

ユーザー一覧の操作方法については、164 ページの「ユーザー一覧」を参照してください。



注意： 1 回の操作で削除可能な IP アドレス / アカウントは、1 ページ内の最大 20 件までです。
複数ページの IP アドレス / アカウントを削除する場合には、1 ページごとに削除してください。

5. ユーザー一覧の [削除] ボタンをクリックします。

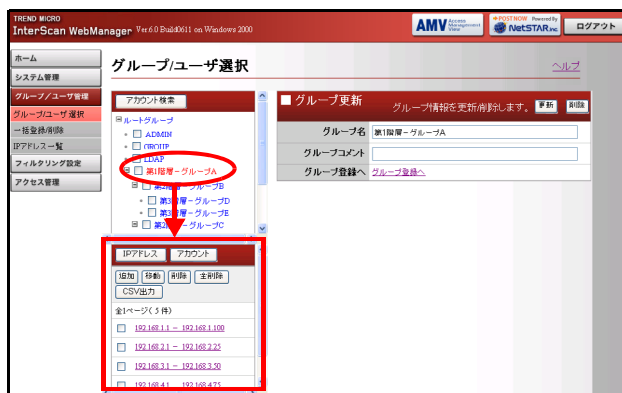
確認のダイアログが表示されます。

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。

■ グループ内の IP アドレス / アカウントをすべて削除する

1. [グループ/ユーザ管理] → [グループ/ユーザ選択] をクリックします。
[グループ/ユーザ選択] 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。
ユーザー一覧が表示されます。



3. [IP アドレス] ボタンまたは [アカウント] ボタンをクリックして、ユーザー一覧の表示を切り替えます。
4. ユーザー一覧の [全削除] 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。

4-7. 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] → [グループ/ユーザ選択] をクリックします。
[グループ/ユーザ選択] 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： マスタ管理者の場合、ルートグループを選択すると、ユーザー一覧にファイルのエンコード選択と [CSV 出力] ボタンが表示されます。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。

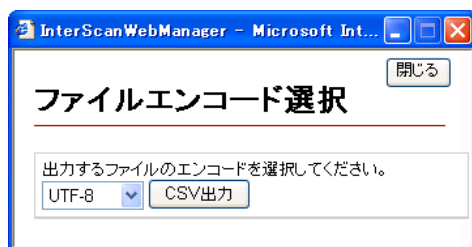
3. [IP アドレス] ボタンまたは [アカウント] ボタンをクリックして、ユーザー一覧の表示を切り替えます。

4. ユーザー一覧の [CSV 出力] ボタンをクリックします。



[ファイルエンコード選択] 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、[ファイルエンコード選択] 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. [CSV 出力] 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。

7. [閉じる] ボタンをクリックします。

[ファイルエンコード選択] 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, IP アドレス (開始), IP アドレス (終了), 例外ユーザ設定
2 行目：	"第 1 階層-グループ A","192.168.1.1","192.168.1.50","例外ユーザ"
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、193 ページの「5. ユーザ、グループ情報の一括登録、削除」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, 管理者フラグ, AMV 閲覧権限, 例外ユーザ設定
2 行目：	"user01","Member#01","第 1 階層-グループ A","user01@netstar.jp","1","1",
3 行目：	"user02","Member#02","第 1 階層-グループ A","user02@netstar.jp","0","0","例外ユーザ"

注意： ・管理者フラグには、グループまたはサブグループ管理者の場合には「1」、エンドユーザの場合には「0」が格納されます。

・AMV 閲覧権限には、閲覧を許可されている場合には「1」、許可されていない場合には「0」が格納されます。

・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、IP アドレス / アカウントを一括登録、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、193 ページの「5. ユーザ、グループ情報の一括登録、削除」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、195 ページの「5-1. ファイルのフォーマット」を参照してください。

注意： マスタ管理者は、すべてのグループに対して一括登録、削除できます。
グループ管理者およびサブグループ管理者は、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] → [一括登録 / 削除] をクリックします。
[一括登録 / 削除] 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。

ユーザー一覧から出力した 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、190 ページの「4-7. IP アドレス / アカウント一覧をファイルに出力する」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、マスタ管理者だけが選択可能です。 グループ管理者、サブ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、サブグループ管理者では、アカウントだけ登録できます。
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、[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	IP アドレス (開始)	IP アドレス (終了)

・入力例

"グループ A¥グループ B",	"192.168.1.151",	"192.168.1.200"

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。
IP アドレス (開始)	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。
IP アドレス (終了)	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。

■ 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	管理者フラグ	AMV 閲覧権限

・入力例

"user01",	"password",	"グループ A¥グループ B",	"user01@netstar.jp",	"1",	"1"

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。
管理者フラグ	0: エンドユーザの場合 1: グループ管理者の場合
AMV 閲覧権限	0:AMV 閲覧権限なし 1:AMV 閲覧権限あり

■ 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。また、amserror.log ファイルが出力されます。詳しくは、346 ページの「A-2. amserror.log について」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、157 ページの「重複する IP アドレス設定」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「IP アドレス（開始）」<「IP アドレス（終了）」となるように入力してください。

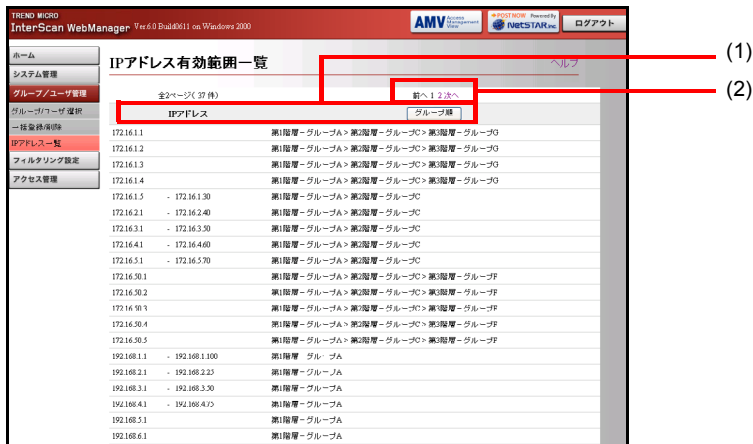
6. IP アドレス設定一覧の確認

「IP アドレス一覧」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、157 ページの「重複する IP アドレス設定」を参照してください。

注意： マスタ管理者は、すべてのグループの設定を確認できます。
グループ管理者およびサブグループ管理者は、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 アドレス一覧] をクリックします。

[IP アドレス有効範囲一覧] が表示されます。



(1) 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。
[グループ順] 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。

- (2) [IP アドレス有効範囲一覧] 画面には、1 画面最大 20 件まで表示できます。IP アドレスが 20 件以上登録されている場合には、1 ページに 20 件ずつ分割して表示されます。

前へ	クリックすると、前のページに戻ります。
ページ数	クリックすると、クリックしたページ番号の IP アドレス一覧を表示します。
次へ	クリックすると、次のページに進みます。

MEMO

フィルタリングの設定

1. フィルタリング設定について

Trend Micro InterScan WebManager (以下、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。

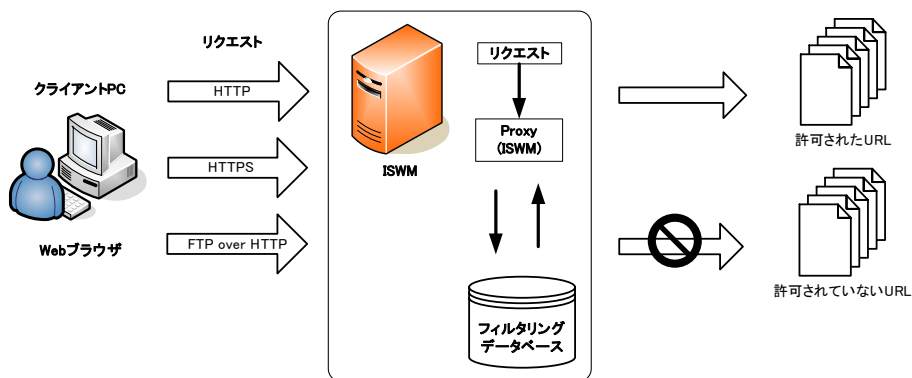
注意： フィルタリング可能なリクエスト種別は、HTTP、HTTPS、FTP over HTTP (Web ブラウザを使用した FTP) の 3 種類です。

1-1. フィルタリングの流れ

スタンドアロン版、ICAP 版、Squid 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。

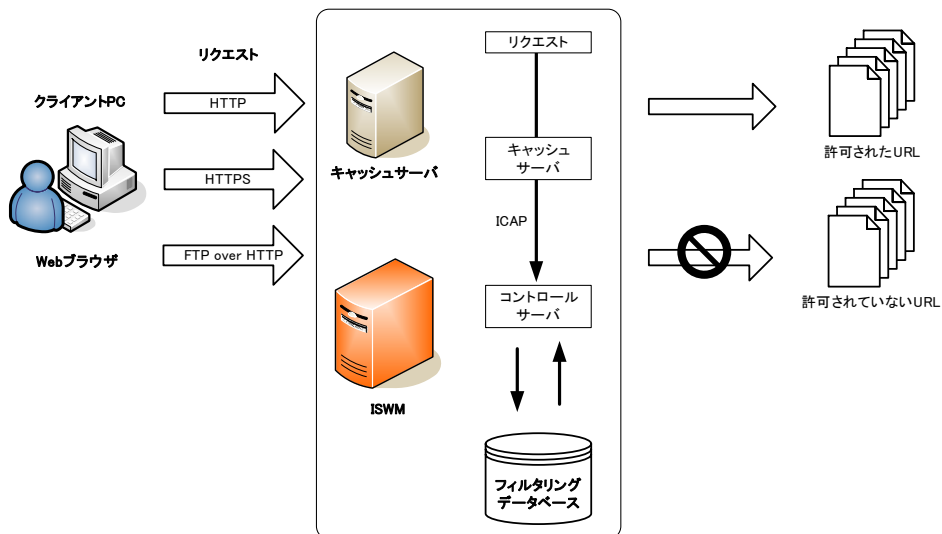
■ スタンドアロン版の場合

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。



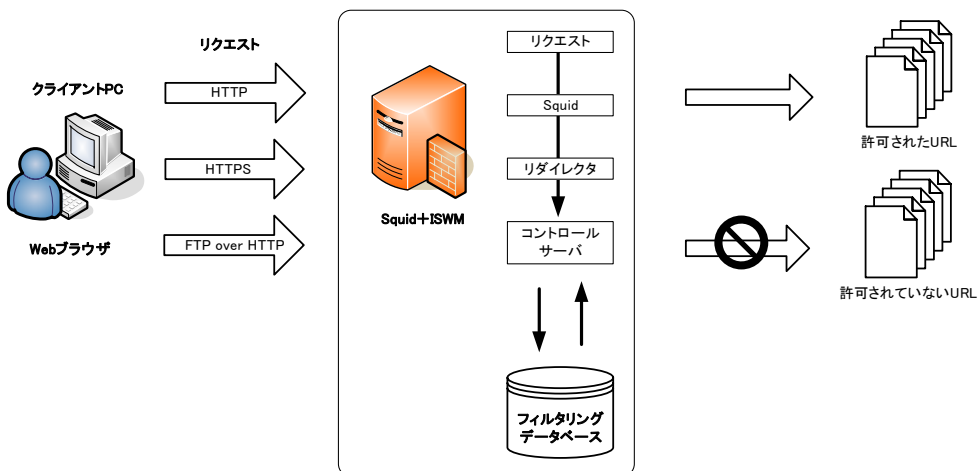
■ ICAP 版の場合

クライアントPCからのリクエストは、キャッシュサーバに送信されます。キャッシュサーバと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、キャッシュサーバ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。



■ Squid 版の場合

クライアントPCからのリクエストは、Squidに送信されます。Squidに送信されたリクエストは、ISWMのリダイレクタプログラムを使用して、ISWM コントロールサーバプログラムに送信されます。ISWMは、フィルタリング設定に従って、Squidからリダイレクタ経由で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作成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には、次の3種類の設定内容があります。

設定の流れについては、216 ページの「1-5. フィルタリング設定の流れ」を参照してください。

- **カテゴリ別ルール**

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、ネットスター社のフィルタリング用データベースから取得します。フィルタリング用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**

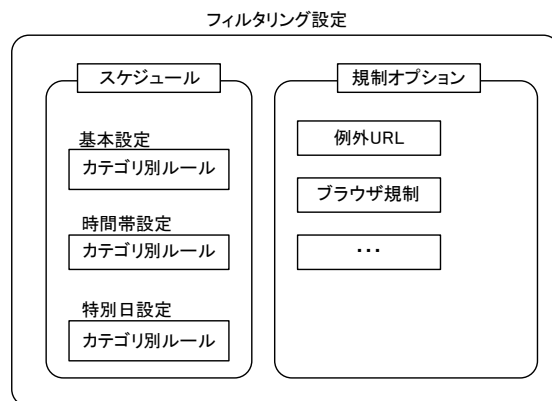
フィルタリング対象のグループや個別ユーザに対して、適用するカテゴリ別ルールと、ルールを適用する時間帯を設定します。

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特定日設定の3種類があります。

注意： 特別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、393 ページの「B. 設定ファイル」を参照してください。

▪ その他の規制オプション

カテゴリ別ルールの特例として、アクセスを規制する URL や、クライアント PC の Web ブラウザの規制などを設定できます。



■ フィルタリング設定対象

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。207 ページの「フィルタリング設定例」を参照してください。

- ユーザ全体
- 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、[システム設定]→[認証設定]でユーザ認証を有効にしてください。105 ページの「8. ユーザ認証の設定」を参照してください。

▪ [システム設定]→[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。

▪ 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。

■ 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「例外ユーザ」に登録すると、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。207 ページの「フィルタリング設定例」を参照してください。

例外ユーザの登録およびフィルタリング設定は、[フィルタリング設定]→[例外ユーザ設定] で設定します。284 ページの「10. 例外ユーザのフィルタリング設定」を参照してください。

注意： 例外 URL など、[例外ユーザ設定] 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。

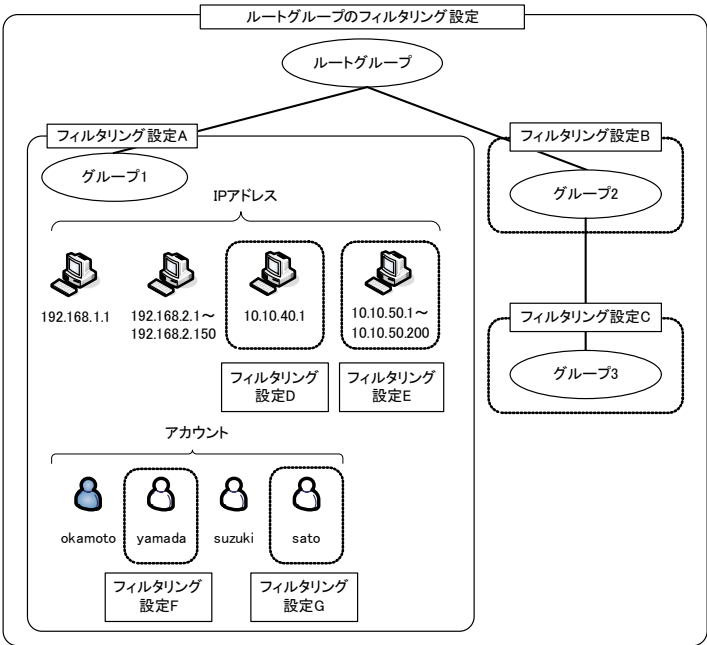
■ グループとフィルタリング設定

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と、上位グループから一元管理できます。

詳細については、211 ページの「1-3. フィルタリング設定の参照」を参照してください。

■ 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)	[フィルタリング設定] → [グループ設定]
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	[フィルタリング設定] → [例外ユーザ設定]
フィルタリング設定 D	IP アドレス「10.10.40.1」の端末	
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」	

■ フィルタリングルールの設定

フィルタリングルールの設定、規制内容などについて説明します。
設定については、226 ページの「3. カテゴリ別フィルタリングルールの設定」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。
カテゴリ別ルールは、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、277 ページの「8. カテゴリ別規制メッセージの設定」を参照してください。

- ・ **4 種類の規制レベル**

アクセス制御には、次の 4 種類の規制レベルがあります。

ゆるい ↓ 厳しい		許可	自由にアクセスを許可します。
		オーバーライド	規制画面を表示しますが、一定時間だけ閲覧ができます。閲覧するためのパスワード (オーバーライドパスワード) を設定して、アクセスを制限することも可能です。
		書き込み規制	掲示板などへの書き込みを禁止します。閲覧は可能です。
		規制	アクセスを規制して、規制画面を表示します。

最低基準ルールの設定

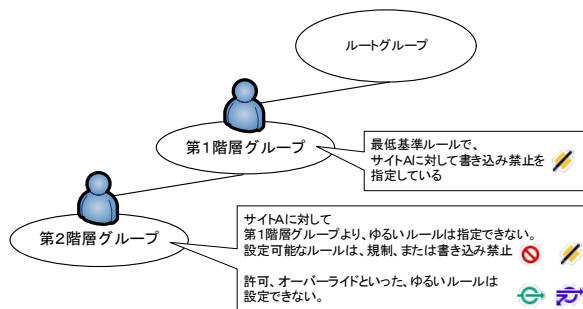
特定のフィルタリングルールを、最低基準ルールに設定できます。最低基準ルールを設定すると、下位グループでは最低基準ルールの規制内容がベースとなり、規制をゆるめることができません。

上位グループのルールを最低基準ルールとして設定すると、下位グループのフィルタリングルールが、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： 最低基準ルールは、1 グループで 1 ルールだけ設定できます。

- 最低基準ルールを設定した場合、下位グループでは、最低基準ルールを設定したグループおよび下位グループのフィルタリングルールだけをベースにできます。たとえば、ルートグループで最低基準ルールを設定すると、すべてのグループに最低基準ルールが有効になります。
- 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最低基準ルールを適用すると、下位グループは指定した最低基準ルールに置き換わります。

次の図のように、上位グループで、あるカテゴリに「書き込み規制」を設定した最低基準ルールを設定すると、下位グループの「書き込み規制」が設定されたカテゴリでは、「許可」、「オーバーライド」を設定できません。



■ 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フィルタリング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、214 ページの「1-4. スケジュール種別」を参照してください。

基本設定	デフォルトで適用するフィルタリングルールを設定します。
時間帯設定	指定した曜日、時間帯に適用するフィルタリングルールを設定します。
特定日設定	指定した日付に適用するフィルタリング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

フィルタリング用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。

また、登録した例外 URL をネットスター社の登録リストサーバに送信できます。登録リストサーバに送信された例外 URL は、個別に内容を確認して、フィルタリング用データベースに反映されることがあります。

設定については、250 ページの「5. 例外 URL の設定」を参照してください。

■ 規制対象の URL を閲覧のみ許可に設定可能

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、250 ページの「5. 例外 URL の設定」を参照してください。

1-3. 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

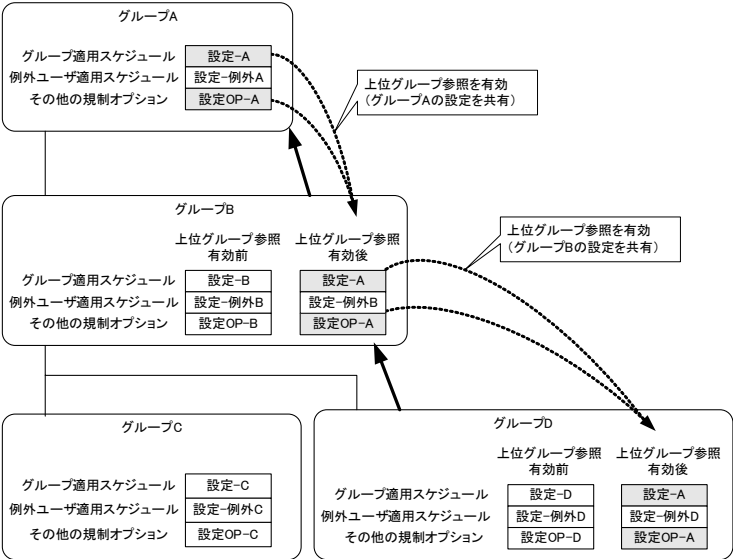
上位グループ参照を有効にすると、上位グループで作成したフィルタリング設定を参照できます。
参照する設定は、グループ適用スケジュールと、その他の規制オプションになります。
上位グループ参照を有効にしたグループでは、例外ユーザの指定、設定だけが可能です。

グループ適用スケジュール	上位グループの設定を参照します。
例外ユーザ適用スケジュール	上位グループの設定を参照しません。
その他の規制オプション ・例外 URL 設定 ・クライアント規制 ・規制オプション ・カテゴリ別規制メッセージ	上位グループの設定を参照します。

上位グループ参照は、グループを登録するときと、[グループ設定]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をコピーできます。上位グループのフィルタリング設定をコピーしない場合には、上位グループ参照を有効にする前のフィルタリング設定に戻ります。

	参照している設定を コピーする	参照している設定を コピーしない
グループ適用スケジュール	上位グループの設定	上位グループ参照を有効にする 前の設定
その他の規制オプション ・例外 URL 設定 ・クライアント規制 ・規制オプション ・カテゴリ別規制メッセージ		

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。



■ 下位グループ指定

下位グループ指定を有効にすると、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、上位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。

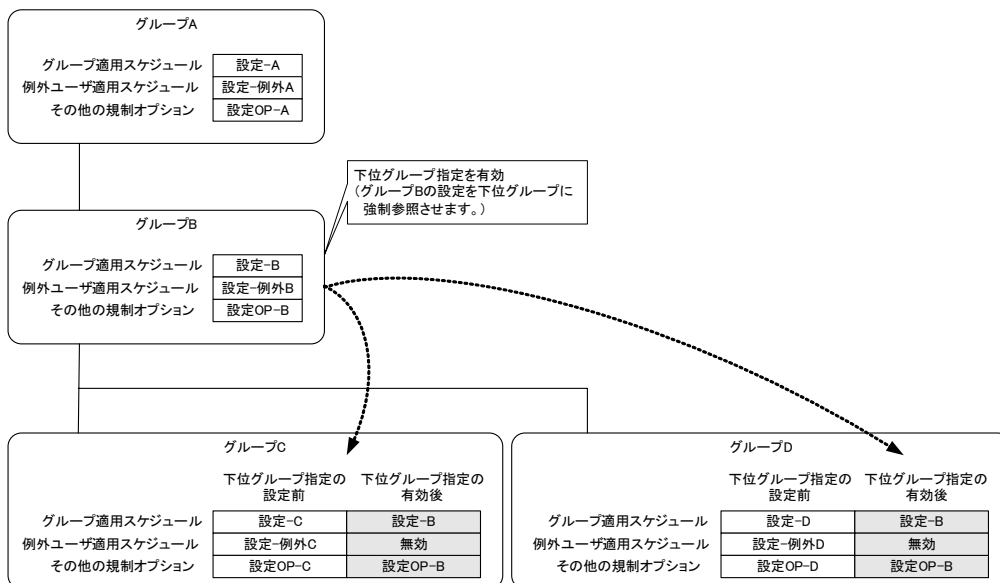
下位グループ指定は、[グループ設定]で設定できます。

- 注意：**
- 下位グループ指定を有効にすると、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、下位グループの例外ユーザの設定も無効になります。
 - 下位グループ指定を無効にした場合、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。下位グループの例外ユーザの設定は、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で下位グループ指定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、例外ユーザ）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、下位グループ指定を無効にすると、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。



1-4. スケジュール種別

■ スケジュール設定の種類

スケジュールには、グループ適用スケジュールと例外ユーザ用スケジュールの2種類があります。

- **グループ適用スケジュール**

グループに適用するスケジュールです。

- **例外ユーザ用スケジュール**

例外ユーザに適用するスケジュールです。

例外ユーザには、個別に例外ユーザ用スケジュールを設定できます。

グループ適用スケジュール、例外ユーザ用スケジュールは、[グループ設定]で設定します。例外ユーザの場合には、[グループ設定]で例外ユーザ用スケジュールを設定して、[例外ユーザ設定]で、ユーザごとにスケジュールを割り当てます。

■ スケジュール設定の構成

スケジュール設定（グループ適用スケジュール、例外ユーザ用スケジュール）には、基本設定、時間帯別設定、特別日設定の3種類があります。

- **基本設定**

グループの基本フィルタリングルールを設定します。基本設定は、時間帯別設定または特別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。

設定については、233 ページの「4. スケジュールの設定」を参照してください。

- **時間帯別設定**

特定の曜日、時間帯に適用するフィルタリング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、適用するフィルタリングルールを詳細に設定できます。

設定については、233 ページの「4. スケジュールの設定」を参照してください。

・ 特別日設定

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。

特別日設定は、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、393 ページの「B. 設定ファイル」を参照してください。cal.inf の初期状態では、2008 年から 2012 年までの国民の祝日が日曜日として設定されています。

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フィルタリングルールを適用する場合には、時間帯設定を使用します。

- 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 (フィルタリング設定で設定)



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

特別日設定(cal.infで設定)



1-5. 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例外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

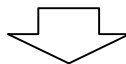
グループごとのフィルタリング設定の流れは次のようになります。

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. グループの選択

フィルタリングを設定するグループを選択します。

グループの選択 →「[グループ設定] の操作方法」(219 ページ)



2. フィルタリングルールを設定

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。

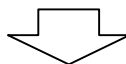
カテゴリ別に規制内容を選択して、フィルタリングルールを設定します。また、規制 URL にアクセスしたときに表示されるメッセージをカテゴリ別に設定することも可能です。

フィルタリングルールを設定

→「3. カテゴリ別フィルタリングルールを設定」(226 ページ)

規制メッセージの設定

→「8. カテゴリ別規制メッセージの設定」(277 ページ)

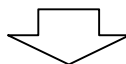


3. スケジュールの設定

グループに適用する基本フィルタリングルールを設定します。また、指定した曜日、時間帯に異なるフィルタリングルールを適用することも可能です。

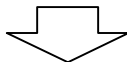
スケジュールの設定

→「4. スケジュールの設定」(233 ページ)



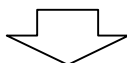
4. 例外 URL の設定

指定した URL をカテゴリごとに例外 URL に登録してフィルタリングします。
例外 URL の設定 →「5. 例外 URL の設定」(250 ページ)



5. クライアント規制設定

特定のブラウザを規制する設定を行います。
クライアント規制設定 →「6. クライアント規制設定」(262 ページ)



6. その他の規制の設定

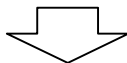
IP アドレスリクエスト拒否などのオプション設定を行います。
その他の規制の設定 →「7. 規制オプションの設定」(270 ページ)

■ 例外ユーザのフィルタリング設定

例外ユーザのフィルタリング設定の流れは次のようになります。

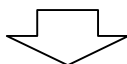
1. グループのフィルタリング設定

例外ユーザに設定するユーザが所属するグループのフィルタリング設定を行います。
例外 URL 設定、カテゴリ別規制メッセージなどはグループの設定が適用されます。



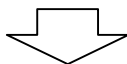
2. フィルタリングルールを設定

例外ユーザに適用するフィルタリングルールを設定します。
カテゴリ別に規制内容を選択して、フィルタリングルールを設定します。
フィルタリングルールの設定 →「3. カテゴリ別フィルタリングルールの設定」(226 ページ)



3. スケジュールの設定

例外ユーザに適用する基本フィルタリングルールを設定します。また、指定した曜日、時間帯に異なるフィルタリングルールを適用することも可能です。
スケジュールの設定 →「4. スケジュールの設定」(233 ページ)



4. 例外ユーザの登録、設定

グループに登録された IP アドレス、またはアカウントを例外ユーザに登録します。
また、スケジュール以外の例外ユーザ用フィルタリング設定を行います。
例外ユーザの登録、設定 →「10. 例外ユーザのフィルタリング設定」(284 ページ)

2. [フィルタリング設定] 画面でできること

[フィルタリング設定] 画面は、[グループ設定]、[例外ユーザ設定] の2種類のサブメニューがあります。それぞれのサブメニューで設定する内容について説明します。

また、上位グループと下位グループ間でのフィルタリング設定の参照について説明します。

フィルタリング設定の詳細については、次の表を参照してください。

カテゴリ別ルール設定	「3. カテゴリ別フィルタリングルールの設定」	226 ページ
スケジュール設定	「4. スケジュールの設定」	233 ページ
例外 URL 設定	「5. 例外 URL の設定」	250 ページ
クライアント規制設定	「6. クライアント規制設定」	262 ページ
規制オプション設定	「7. 規制オプションの設定」	270 ページ
カテゴリ別規制メッセージ設定	「8. カテゴリ別規制メッセージの設定」	277 ページ

2-1. グループに適用するフィルタリング設定を作成する

[グループ設定] では、グループに適用するフィルタリング設定を作成します。また、グループに適用するフィルタリング設定を確認できます。

■ [グループ設定] の操作方法

1. [フィルタリング設定] → [グループ設定] をクリックします。

[グループ設定] が表示されます。

2. 画面左側のグループ一覧から、フィルタリング設定を作成するグループをクリックします。

[■フィルタリング設定] が表示されます。



注意： グループ一覧が表示される画面では、画面を切り替えても同じグループが選択されます。

[フィルタリング設定] → [グループ設定]

[フィルタリング設定] → [例外ユーザ設定]

[グループ / ユーザ管理] → [グループ / ユーザ選択]

3. [■フィルタリング設定] のリンクをクリックして、フィルタリング設定を作成します。

詳細については、次の表を参照してください。

上位グループ参照	「1-3. フィルタリング設定の参照」	211 ページ
下位グループ指定		213 ページ
カテゴリ別ルール設定	「3. カテゴリ別フィルタリングルールの設定」	226 ページ
スケジュール設定	「4. スケジュールの設定」	233 ページ
例外 URL 設定	「5. 例外 URL の設定」	250 ページ
クライアント規制設定	「6. クライアント規制設定」	262 ページ
規制オプション設定	「7. 規制オプションの設定」	270 ページ
カテゴリ別 規制メッセージ設定	「8. カテゴリ別規制メッセージの設定」	277 ページ

-
- 注意：**
- 例外ユーザに適用するカテゴリ別フィルタリングルールは、[カテゴリ別ルール設定] で作成します。
また、例外ユーザ用のスケジュールは、[スケジュール設定] で作成します。
 - スケジュール、クライアント規制、規制オプションは、グループ登録時に上位グループの設定をコピーします。
例外URLおよびカテゴリ別規制メッセージは、グループ登録時に上位グループの設定をコピーできます。
 - 上位グループのフィルタリング設定で最低基準ルールが設定されている場合、グループ登録時に例外 URL をコピーしても「許可カテゴリ」に登録された URL はコピーされません。
-

2-2. 例外ユーザの登録とフィルタリング設定

[例外ユーザ設定] では、ユーザを例外ユーザに登録、解除します。また、例外ユーザのスケジュール、規制オプション、クライアント規制を設定します。

■ [例外ユーザ設定] の操作方法

1. [フィルタリング設定] → [例外ユーザ設定] をクリックします。
[例外ユーザ設定] が表示されます。
2. 画面左側のグループ一覧から、設定するグループ名をクリックします。
グループ一覧の下に、ユーザー一覧が表示されます。



注意： グループ一覧が表示される画面では、画面を切り替えても同じグループが選択されます。

[フィルタリング設定] → [グループ設定]

[フィルタリング設定] → [例外ユーザ設定]

[グループ/ユーザ管理] → [グループ/ユーザ選択]

3. ユーザー一覧から、例外ユーザに設定するアカウント名または IP アドレスをクリックします。

画面右側に、[■例外ユーザ情報]、[■スケジュール] が表示されます。

[アカウント] ボタンまたは [IP アドレス] ボタンをクリックすると、ユーザー一覧の表示を切り替えてできます。



4. 例外ユーザのフィルタリング設定を作成します。

例外ユーザ用に設定できるフィルタリング設定には、次の項目があります。設定方法については、284 ページの「10. 例外ユーザのフィルタリング設定」を参照してください。

スケジュール設定	グループ適用スケジュールとは別に、例外ユーザに適用するスケジュールを設定できます。
規制オプション設定	規制メッセージやオーバーライド設定、IP アドレスを使用したリクエストへの拒否などの規制を設定できます。
クライアント規制設定	特定のブラウザを使用したアクセスを許可または規制できます。

注意：

- 例外ユーザ用のカテゴリ別ルール、スケジュールは、[グループ設定] で作成します。
- [例外ユーザ設定] にない設定は、所属するグループと同じ設定が適用されます。

2-3. 上位グループ参照と下位グループ指定

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。詳細については、211ページの「1-3. フィルタリング設定の参照」を参照してください。

フィルタリング設定の参照設定には、次の2種類があります。

- **上位グループ参照**

上位グループ参照を有効にすると、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。上位グループ参照を有効にしたグループでは次の設定だけが可能です。

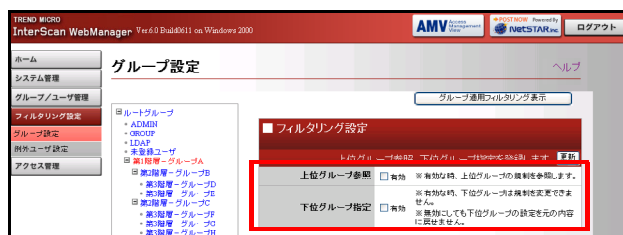
- 例外ユーザの登録、解除
- 例外ユーザのフィルタリングルール設定
- 例外ユーザのスケジュール設定

- **下位グループ指定**

下位グループ指定を有効にすると、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。「下位グループ指定を有効にしたグループ」の下位グループでは、グループおよび例外ユーザの設定はできません。下位グループでは、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。

-
- 注意：**
- 上位グループ参照の設定が適用される項目は、設定画面へのリンクが表示されません。
 - 上位グループで、最低基準ルールが登録されている場合には、上位グループ参照は表示されません。
 - 下位グループで、上位グループ参照が有効なときに、上位グループで最低基準ルールが登録された場合、上位グループ参照が解除されます。このとき、下位グループに上位グループの設定をコピーできます。
上位グループの設定をコピーしなかった場合には、上位グループ参照を有効にする前の設定に戻ります。
-

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、参照設定を行うグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] で、参照設定の有効 / 無効を設定します。
[上位グループ参照] / [下位グループ指定] の [有効] チェックボックスをオン/オフすると、設定の有効 / 無効を切り替えられます。



4. [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。

注意： [更新] 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 [更新] 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。
「更新しました。」と表示されます。

注意：

- ・上位グループ参照を無効にする場合には、参照している設定のコピーを確認するダイアログが表示されます。
- ・下位グループ指定の有効 / 無効を切り替える場合には、下位グループ指定の設定変更を確認するダイアログが表示されます。

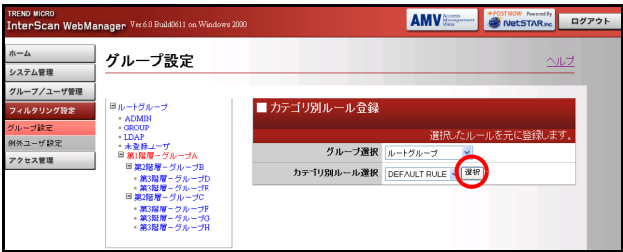
3. カテゴリ別フィルタリングルールの設定

ここでは、カテゴリ別フィルタリングルールの登録、変更、削除方法について説明します。

3-1. カテゴリ別ルールを登録する

新しいカテゴリ別フィルタリングルールを登録します。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、カテゴリ別ルールを登録するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [カテゴリ別ルール登録] をクリックします。
[■カテゴリ別ルール登録] が表示されます。
4. 登録するルールのベースとするグループ、ルールを選択して、[選択] ボタンをクリックします。
選択したルールの設定内容が表示されます。

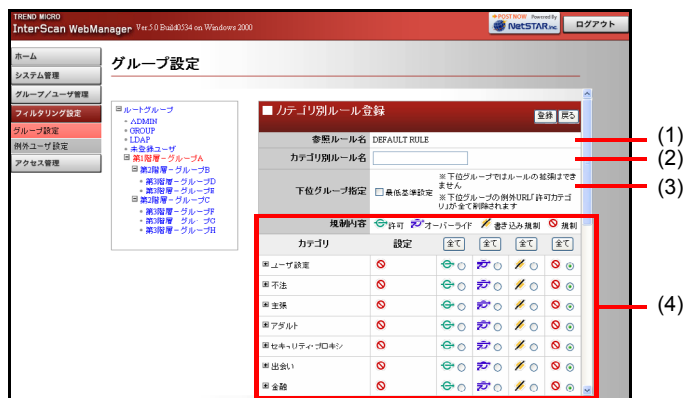


グループ選択	登録するルールのベースとするルールが登録されているグループを選択します。現在のグループおよび上位グループから選択できます。
カテゴリ別ルール選択	[グループ選択] で選択したグループに登録されている、フィルタリングルールの一覧が表示されます。 最低基準ルールは、青色で表示されます。

注意： 上位グループで、最低基準ルールが登録されている場合、[グループ選択] には、最低基準設定が登録されているグループと下位グループが表示されます。

5. 登録するルールの名前や、規制内容を設定します。

[戻る] ボタンをクリックすると、グループ選択、カテゴリ別ルール選択に戻ります。



(1)参照ルール名	手順4の[カテゴリ別ルール選択] で選択したルール名が表示されます。
(2)カテゴリ別ルール名 (必須項目)	登録するルール名(最大半角 20 文字)を入力します。
(3)下位グループ指定	[最低基準設定] チェックボックス オンにすると、設定した規制内容を最低基準ルールに設定します。下位グループでは、最低基準ルールの規制内容よりもゆるめることはできません。また、例外 URL の「許可カテゴリ」に URL を登録できません。 詳細については、208 ページの「フィルタリングルールの設定」を参照してください。
(4)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、229 ページの「カテゴリごとに規制内容を設定する」を参照してください。

注意： カテゴリ別ルール名には全角文字、半角英数字、半角記号が使用できます。ただし、以下の半角記号とタブは使用できません。

": ; ? | < > ¥ /

6. [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。

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。

8. 選択しているグループに複数のルールを登録する場合には、[戻る] ボタンをクリックします。

グループ選択、カテゴリ別ルール選択に戻ります。

別のグループにルールを登録する場合には、ルールを登録するグループをグループ一覧から選択します。

■ 規制内容について

規制内容には、以下の 4 種類のレベルがあります。

ゆるい ↓ 厳しい		許可	自由にアクセスを許可します。
		オーバーライド	規制画面を表示しますが、一定時間だけ閲覧ができます。閲覧するためのパスワード (オーバーライドパスワード) を設定して、アクセスを制限することも可能です。
		書き込み規制	掲示板などへの書き込みを禁止します。閲覧は可能です。
		規制	アクセスを規制して、規制画面を表示します。

- 注意：**
- ・オーバーライドパスワードおよび閲覧可能な時間 (オーバーライドタイマー) は、[規制オプション設定] で設定します。270 ページの「7. 規制オプションの設定」を参照してください。
 - ・オーバーライドは、[システム管理] → [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 プロトコルで POST、PUT メソッドを使用している URL になります。https (CONNECT メソッド) や Java を使用した入力ページは、書き込み規制の対象にできません。
 - ・Squid 版の場合、https の Web サイトにはオーバーライドを適用できません。

■ 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。

カテゴリ	サブカテゴリ	設定	全て	全て	全て	全て
同ユーザー設定		⊘	🔒	🔒	🔒	🔒
	ユーザー設定1	⊘	🔒	🔒	🔒	🔒
	ユーザー設定2	⊘	🔒	🔒	🔒	🔒
	ユーザー設定3	⊘	🔒	🔒	🔒	🔒
	ユーザー設定4	⊘	🔒	🔒	🔒	🔒
	ユーザー設定5	⊘	🔒	🔒	🔒	🔒

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。

規制内容アイコンの上にある[全て]ボタ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。

ルールを読み込んだ時点の設定を表示します。

すべてのカテゴリの規制内容を一括して変更できます。

カテゴリ	サブカテゴリ	設定	全て	全て	全て	全て
同ユーザー設定		⊘	🔒	🔒	🔒	🔒
	ユーザー設定1	🔒	🔒	🔒	🔒	🔒
	ユーザー設定2	🔒	🔒	🔒	🔒	🔒
	ユーザー設定3	⊘	🔒	🔒	🔒	🔒
	ユーザー設定4	🔒	🔒	🔒	🔒	🔒
	ユーザー設定5	🔒	🔒	🔒	🔒	🔒

- 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、最低基準ルールが設定されている場合には、最低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、フィルタリング用データベースに登録されていない URL に、規制内容（許可、オーバーライド、書き込み規制、規制）を設定できます。

ユーザ設定カテゴリをカテゴリ別ルールとして登録し、規制内容を設定すると、ユーザ設定カテゴリのサブ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、[システム管理] - [フィルタリングルール共通設定] で変更できます。

用途や種類に応じて最大 10 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 250 ページの「5. 例外 URL の設定」を参照してください。

カテゴリ	サブカテゴリ	設定	全て	全て	全て	全て
ユーザ設定						
	内部統制関連					
	個人情報保護関連					
	ユーザ設定3					
	ユーザ設定4					
	ユーザ設定5					

3-2. カテゴリ別ルールを変更、削除する

登録したカテゴリ別ルールを変更、削除する方法について説明します。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、カテゴリ別ルールを変更、削除するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [カテゴリ別ルール変更・削除] をクリックします。
[■カテゴリ別ルール変更・削除] が表示されます。
4. 変更、削除するルールを選択して、[選択] ボタンをクリックします。
[カテゴリ別ルール選択] には、選択したグループに登録されているルールが表示されます。



[■カテゴリ別ルール変更] に、選択したルールの設定内容が表示されます。



5. 設定を変更する場合、カテゴリ別ルール名、下位グループ指定、規制内容を変更します。
6. [更新] 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： [更新] 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 [更新] 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。

- **設定を変更した場合**

「更新が完了しました。」と表示されます。別のルールを変更する場合には、[戻る] ボタンをクリックして、[■カテゴリ別ルール変更・削除] に戻ります。

- **設定を削除した場合**

「削除が完了しました。」と表示され、[■カテゴリ別ルール変更・削除] に戻ります。選択しているグループ内のルールがすべて削除されると、「カテゴリ別ルールが存在しません。」と表示されます。

4. スケジュールの設定

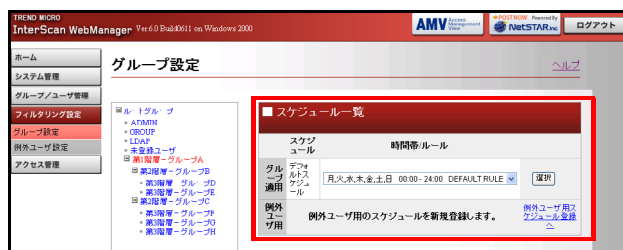
「カテゴリ別ルール設定」で登録したフィルタリングルールを適用する曜日、時間帯を設定して、スケジュールを作成します。

「スケジュール設定」では、グループに適用するスケジュールと、例外ユーザ用のスケジュールの両方を設定できます。

4-1. スケジュール一覧を表示する

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、スケジュール一覧を表示するグループをクリックします。
[■ フィルタリング設定] が表示されます。
3. [■ フィルタリング設定] - [スケジュール設定へ] をクリックします。
[■ スケジュール一覧] が表示されます。
4. スケジュール一覧を確認します。

初期状態では、上位グループのグループ適用スケジュールが設定されます。



- ・ グループ適用スケジュールを確認する

[グループ適用スケジュール] のプルダウンメニューから、登録済みのスケジュールを確認できます。

- ・ 例外ユーザ用スケジュールを確認する

例外ユーザ用スケジュールは複数設定できます。設定ごとにプルダウンメニューが作成されます。

5. スケジュールを設定します。

グループ適用スケジュール、例外ユーザ用スケジュールの設定については、次の表を参照してください。

[グループ適用スケジュール]

スケジュールの基本設定を変更する	235 ページ
スケジュールの時間帯設定を登録する	238 ページ
スケジュールの時間帯設定を変更、削除する	241 ページ

注意： スケジュール種別については、214 ページの「1-4. スケジュール種別」を参照してください。

[例外ユーザ用スケジュール]

例外ユーザ用スケジュールを登録する	244 ページ
例外ユーザ用スケジュールを変更する	246 ページ
例外ユーザ用スケジュールを削除する	248 ページ

注意： 例外ユーザのフィルタリングルールは、「カテゴリ別ルール設定」で登録します。
226 ページの「3. カテゴリ別フィルタリングルールの設定」を参照してください。

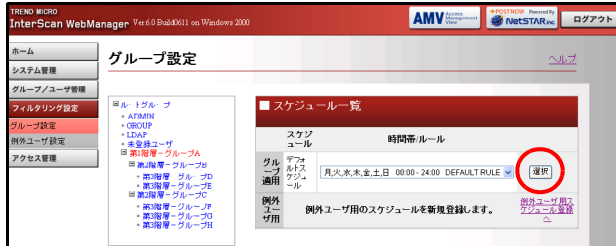
4-2. スケジュールの基本設定を変更する

初期状態では、上位グループの基本設定が登録されています。基本設定を変更する方法について説明します。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [スケジュール設定へ] をクリックします。
[■スケジュール一覧] が表示されます。

4. グループ適用スケジュールの [選択] ボタンをクリックします。

[■スケジュール変更] が表示されます。



[■スケジュール変更] 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、238 ページの「4-3. スケジュールの時間帯設定を登録する」を参照してください。

5. スケジュールの基本設定を設定します。



スケジュール名 (必須項目)	基本設定のスケジュール名 (最大半角 32 文字) を入力します。
基本ルール グループ > カテゴリ別ルール	基本設定として適用するフィルタリングルールが登録されているグループとルール名を選択します。 [表示] ボタンをクリックすると、[カテゴリ別フィルタリングルール] 画面が別ウィンドウで表示されます。選択したフィルタリングルールの規制内容を確認できます。

注意： スケジュール名には全角英数字、全角記号、半角英数字と半角記号「-」および「_」が使用できます。

6. [基本設定]の[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。

- 注意：**
- ・[更新]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[更新]ボタンをクリックしてください。
 - ・[基本設定]の[更新]ボタンをクリックしても、時間帯設定の内容は更新されません。



7. [OK]ボタンをクリックします。

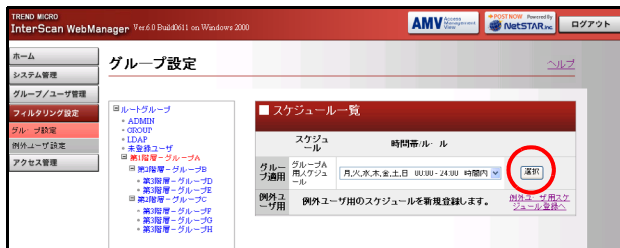
「更新が完了しました。」と表示されます。[戻る]ボタンをクリックすると、[■スケジュール一覧]に戻ります。

引き続き時間帯設定を登録する場合には、238 ページの「4-3. スケジュールの時間帯設定を登録する」の手順5に進みます。

4-3. スケジュールの時間帯設定を登録する

初期状態では、上位グループの時間帯設定が登録されています。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. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [スケジュール設定へ] をクリックします。
[■スケジュール一覧] が表示されます。
4. グループ適用スケジュールの [選択] ボタンをクリックします。
[■スケジュール変更] が表示されます。



5. [■スケジュール変更] - [新規時間帯] 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	オンにした曜日に時間帯設定を適用します。 [全選択] ボタンをクリックすると、すべての曜日をオンにします。 [全解除] ボタンをクリックすると、すべての曜日をオフにします。
時間	時間帯設定を適用する時間を設定します。
グループ>カテゴリ別ルール	時間帯設定として適用するフィルタリングルールが登録されているグループとルール名を選択します。 [表示] ボタンをクリックすると、[カテゴリ別フィルタリングルール情報] 画面が別ウィンドウで表示されます。選択したフィルタリング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。

6. [新規時間帯] の [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。



注意： [新規時間帯] の [登録] ボタンをクリックしても、基本設定の内容は更新されません。

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。登録した時間帯設定は、[設定済時間帯] に追加されます。時間帯設定を複数作成する場合には、手順 5～手順 7 を繰り返します。
[戻る] ボタンをクリックすると、[■スケジュール一覧] に戻ります。



4-4. 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. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [スケジュール設定へ] をクリックします。
[■スケジュール一覧] が表示されます。
4. グループ適用スケジュールの [選択] ボタンをクリックします。
[■スケジュール変更] が表示されます。



5. [■スケジュール変更] - [設定済時間帯] から、変更または削除する設定のチェックボックスをオンにします。

設定が 1 画面に収まらない場合、右側にスクロールバーが表示されます

複数の時間帯設定をオンにした場合、同時に複数の時間帯設定を変更（削除）できます。



チェックボックスをオンにした
時間帯設定を変更または削除対
象にします。

6. 設定を変更する場合、チェックボックスをオンにした時間帯設定を変更します。

設定項目については、238 ページの「4-3. スケジュールの時間帯設定を登録する」を参照してくだ
さい。

7. [設定済時間帯] の [更新] 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：**
- ・[更新] 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 [更新] ボタンをクリックしてください。
 - ・[設定済時間帯] の [更新] ボタンをクリックしても、基本設定の内容は更新されません。



8. [OK] ボタンをクリックします。

設定を変更した場合には、「更新が完了しました。」と表示されます。
設定を削除した場合には、「削除が完了しました。」と表示されます。

9. [戻る] ボタンをクリックします。

[■スケジュール一覧] に戻ります。

4-5. 例外ユーザ用スケジュールを登録する

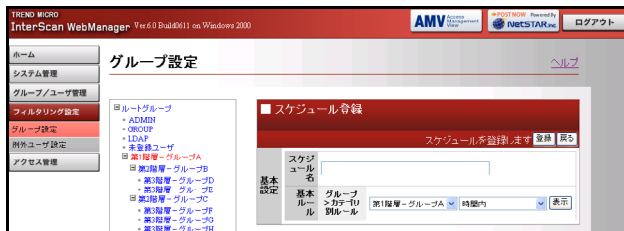
例外ユーザ用のスケジュールを登録する方法について説明します。例外ユーザ用スケジュールとして、複数のスケジュールを登録できます。

注意： 例外ユーザのフィルタリング設定は、[例外ユーザ設定] で作成します。284 ページの「10. 例外ユーザのフィルタリング設定」を参照してください。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、例外ユーザ用スケジュールを登録するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [スケジュール設定へ] をクリックします。
[■スケジュール一覧] が表示されます。
4. [■スケジュール一覧] - [例外ユーザ用スケジュール登録へ] をクリックします。



[■スケジュール登録] が表示されます。



5. 例外ユーザ用スケジュールの基本設定を設定します。

グループ適用スケジュールと同様に、スケジュール名と適用するルールを選択します。
235 ページの「4-2. スケジュールの基本設定を変更する」を参照してください。

6. [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。

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。

基本設定を登録すると、時間帯設定の登録が可能になります。時間帯設定の登録方法は、グループ適用スケジュールと同様です。238 ページの「4-3. スケジュールの時間帯設定を登録する」を参照してください。

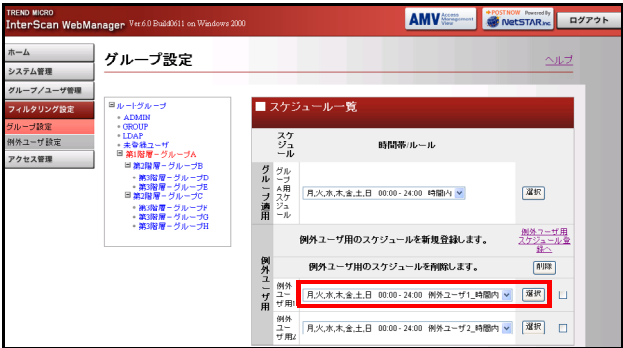
[戻る] ボタンをクリックすると、[■スケジュール一覧] に戻ります。



4-6. 例外ユーザ用スケジュールを変更する

例外ユーザ用スケジュールの設定を変更する方法について説明します。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、例外ユーザ用スケジュールを変更するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [スケジュール設定へ] をクリックします。
[■スケジュール一覧] が表示されます。
4. [■スケジュール一覧] で、変更する例外ユーザ用スケジュールの [選択] ボタンをクリックします。
[■スケジュール変更] が表示されます。



5. スケジュールを変更します。

スケジュールの変更方法は、グループ適用スケジュールと同様です。手順については、次の表を参照してください。

基本設定を変更する	「4-2. スケジュールの基本設定を変更する」	235 ページ
時間帯別設定を変更、 削除する	「4-4. スケジュールの時間帯設定を変更、削除する」	241 ページ

注意： 次の操作は、1つの操作ごとに [登録] ボタン / [変更] ボタン / [削除] ボタンをクリックしてください。

- 基本設定の変更
- 新規時間帯設定の登録
- 時間帯設定の変更、削除



基本設定を更新します。

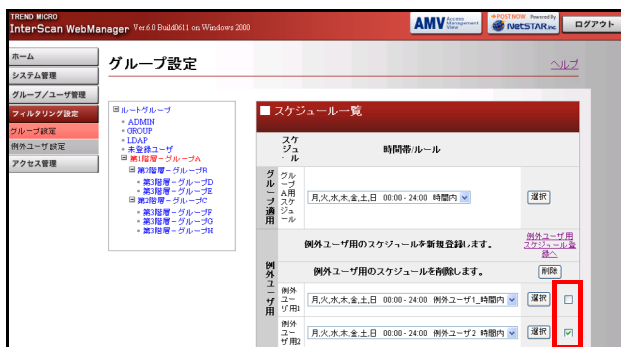
時間帯設定を新規登録します。

時間帯設定を更新または削除します。

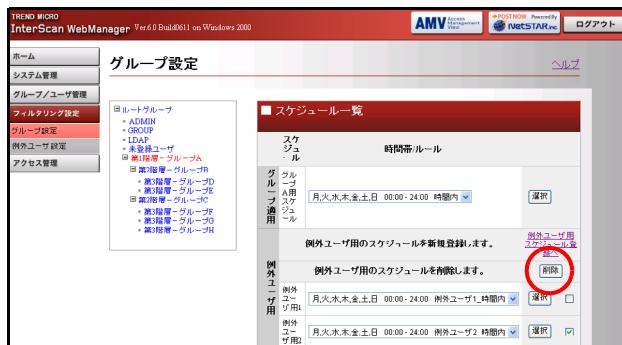
4-7. 例外ユーザ用スケジュールを削除する

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、例外ユーザ用スケジュールを削除するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [スケジュール設定へ] をクリックします。
[■スケジュール一覧] が表示されます。
4. [■スケジュール一覧] で、削除する例外ユーザ用スケジュールのチェックボックスをオンにします。

複数の例外ユーザ用スケジュールをオンにした場合、同時に削除できます。



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。」と表示されます。

5. 例外 URL の設定

グループごとに指定した 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。

- ・フィルタリング用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。このとき、ネットスター社のフィルタリング候補 URL リストサーバに送信することも可能です。送信した URL は、ネットスター社によって定期的にチェックされ、フィルタリング対象として適切であればデータベースに反映されます。
- ・フィルタリング用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。
- ・「閲覧のみ許可」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、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。

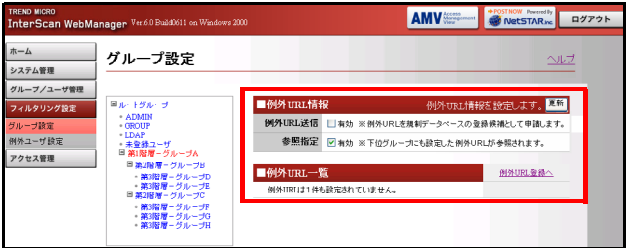
注意：・例外 URL はグループごとに設定できます。登録数に上限はありません。
ただし、登録数が 10,000 件を超える場合、サーバの性能により動作が遅くなる可能性があります。

・新規グループを登録するときに、上位グループの例外 URL 設定をコピーできます。
166 ページの「3-1. グループを登録する」を参照してください。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。

3. [■フィルタリング設定] - [例外 URL 設定へ] をクリックします。

[■例外 URL 情報]、[■例外 URL 一覧] が表示されます。



[■例外 URL 情報]

例外 URL 送信	[有効] チェックボックスをオンにすると、例外URLを登録するときに候補リストサーバに送信できます。 候補リストサーバに送信されたURLは、ネットスター社で定期的にチェックされ、必要と認められれば、フィルタリング用データベースの適切なカテゴリに登録されます。フィルタリング用データベースが常に最新の情報に最適化されるため、URLデータベースの定期的なダウンロードにより、最適なフィルタリングが可能になります。
参照指定	[有効] チェックボックスをオンにすると、現在の例外URL情報を下位グループにも参照させることができます。

注意： 例外 URL 送信が有効な場合、例外 URL の登録時に候補リストサーバに送信するか確認するダイアログが表示されます。

[■例外 URL 一覧]

登録されている例外 URL の一覧が表示されます。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	「5-1. 例外 URL を登録する」	252 ページ
例外 URL 一覧の操作	「例外 URL 一覧の操作方法」	257 ページ
例外 URL を変更する	「5-2. 例外 URL を変更する」	258 ページ
例外 URL を削除する	「5-3. 例外 URL を削除する」	260 ページ

4. [■例外 URL 情報] の設定を変更した場合には、[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。

注意： [更新] 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 [更新] ボタンをクリックしてください。

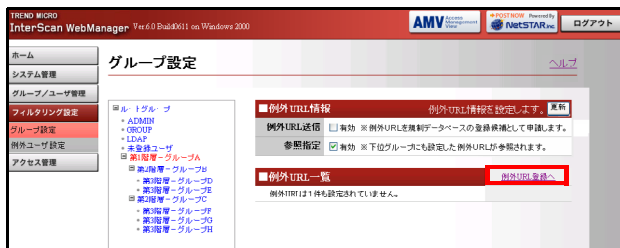
5. [OK] ボタンをクリックします。

「更新が完了しました。」と表示されます。

5-1. 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. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [例外 URL 設定へ] をクリックします。
[■例外 URL 情報]、[■例外 URL 一覧] が表示されます。
4. [■例外 URL 一覧] - [例外 URL 登録へ] をクリックします。
[■例外 URL 情報] が表示されます。



5. 例外 URL を設定します。

[戻る] ボタンをクリックすると、[■例外 URL 一覧] に戻ります。

■例外URL情報

例外URLを登録します。登録 戻る

カテゴリ

許可カテゴリ

サブカテゴリ

許可カテゴリ

URL

http://

[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には、「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には、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

[カテゴリ] で選択したメインカテゴリから、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、フィルタリング用データベースで「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。

注意： ユーザ設定カテゴリのサブカテゴリの名称は、[システム管理] - [フィルタリングルール共通設定] で変更できます。

[URL]

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、255 ページの「URL の設定」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：**
- 1つのグループで、登録済みの URL を重複して登録することはできません。
 - 上位グループで最低基準設定が有効な場合、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」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。
-

6. [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。

-
- 注意：**
- 例外 URL 送信が有効な場合、例外 URL の登録時に候補リストサーバに送信するか確認するダイアログが表示されます。
 - 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。
-

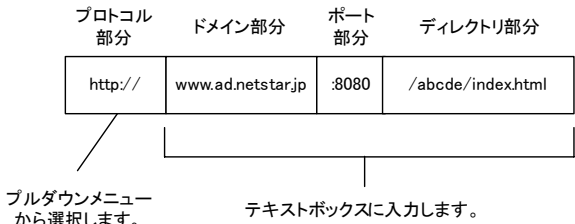
7. [OK] ボタンをクリックします。

[■例外 URL 一覧] に戻り、「登録が完了しました。」と表示されます。
一覧に登録した URL が追加されます。

■ URL の設定

例外 URL 登録時の設定について説明します。

・ HTTP、HTTPS、FTP プロトコルの場合



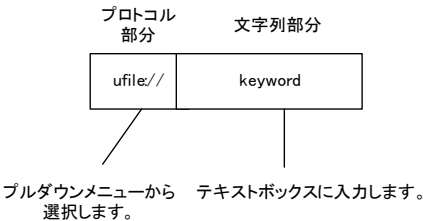
プロトコル部分	プルダウンメニューから選択します。
ドメイン部分	最大半角 128 文字まで入力できます。 • 大文字で入力した場合、小文字に変換されます。 • 先頭に半角スペース、「.」を入力した場合、削除して登録されます。 • 「/」または「:」で始まっている場合、エラーが発生します。 • 末尾が「.」の場合、エラーが発生します。
ポート部分	ポート番号を 1 ～ 65535 の範囲で指定できます。 • 「:」を複数入力した場合、エラーが発生します。 • 半角数字以外の文字、または範囲外の数値を入力した場合、エラーが発生します。
ディレクトリ部分	最大半角 256 文字まで入力できます。デ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、[システム管理] → [フィルタリングルール共通設定] - [■ HTTPS 規制設定] で、[SSL Access Controller を使用する] チェックボックスをオンにしたときだけ、ディレクトリ部分を入力できます。[SSL Access Controller を使用する] チェックボックスがオフのときにディレクトリ部分を入力すると、エラーが発生します。 SSL Access Controller については、336 ページの「4. SSL Access Controller の設定」を参照してください。

- 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	ブ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

■ 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) 現在の登録件数と表示しているページ数が表示されます。20 件を超える場合には、1 画面 20 件ずつ複数ページに分けて表示されます。
- (2) クリックしたボタンの項目の昇順に例外 URL 一覧をソートします。ソートに使用している項目名は白文字で表示されます。
- (3) 例外 URL の登録件数が、複数ページ存在するときに使用します。

前へ	リンクをクリックすると、現在のページから、1 ページ前に戻ります。 現在のページが 1 ページの場合には、リンクが表示されません。
ページ番号	リンクをクリックしたページ番号を表示します。
次へ	リンクをクリックすると、現在のページから、1 ページ次に進みます。 現在のページが最終ページの場合には、リンクが表示されません。

(4) [削除] ボタン

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。
260 ページの「5-3. 例外 URL を削除する」を参照してください。

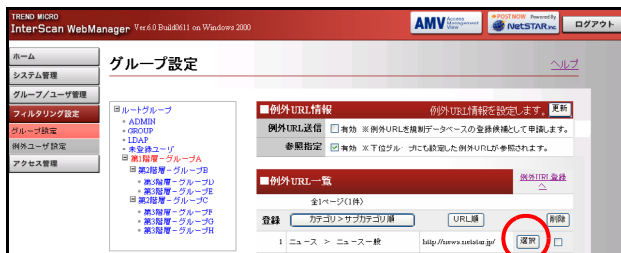
(5) [選択] ボタン

クリックすると、例外 URL の設定を変更できます。
次の「5-2. 例外 URL を変更する」を参照してください。

5-2. 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. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [例外 URL 設定へ] をクリックします。
[■例外 URL 情報]、[■例外 URL 一覧] が表示されます。
4. [■例外 URL 一覧] から変更する URL を選択して、[選択] ボタンをクリックします。
[■例外 URL 情報] が表示されます。



5. 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、252 ページの「5-1. 例外 URL を登録する」を参照してください。
[戻る] ボタンをクリックすると、[■例外 URL 一覧] に戻ります。

6. [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。



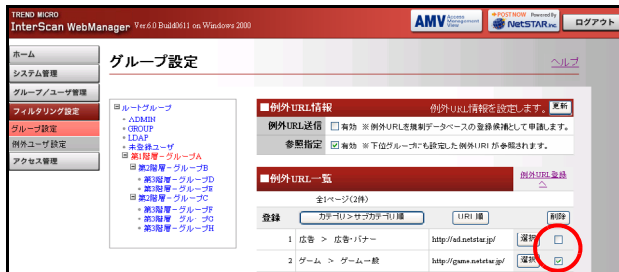
注意： [更新] ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず [更新] ボタンをクリックしてください。

7. [OK] ボタンをクリックします。
[■例外 URL 一覧] に戻り、「更新が完了しました。」と表示されます。

5-3. 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. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [例外 URL 設定へ] をクリックします。
[■例外 URL 情報]、[■例外 URL 一覧] が表示されます。
4. [■例外 URL 一覧] で、削除する URL のチェックボックスをオンにします。
複数の URL をオンにした場合、同時に削除できます。



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。

■例外URL情報		例外URL情報を設定します。 更新	
例外URL送信	☐ 有効 ※ 例外URLを規制データベースの登録候補として申請します。		
参照指定	☒ 有効 ※ 下位グループにも設定した例外URLが参照されます。		
■例外URL一覧		例外URL登録 △	
全1ページ(2件)			
登録	カテゴリ>サブカテゴリ順	URL順	削除
1	広告 > 広告・バナー	http://ad.netstar.jp/	選択 ☐
2	ゲーム > ゲーム一般	http://game.netstar.jp/	選択 ☒

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。

6. クライアント規制設定

6-1. クライアント規制を設定する

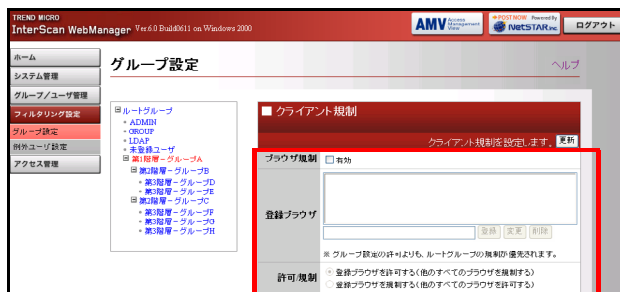
特定のブラウザを使用したアクセスを許可するか、規制するかを設定します。

注意： • Squid 版ではクライアント規制を設定できないため、[■フィルタリング設定] にクライアント規制が表示されません。

• 初期状態では、上位グループの設定が登録されています。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、クライアント規制を設定するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [クライアント規制設定へ] をクリックします。
[■クライアント規制] が表示されます。

4. クライアント規制を設定します。



ブラウザ規制	[有効] チェックボックスをオンにすると、[登録ブラウザ] でアクセスしたクライアントのリクエストを [許可 / 規制] の設定内容で、許可または規制します。
登録ブラウザ	アクセスを許可または規制するブラウザを登録します。ブラウザ規制が有効な場合にだけ、設定できます。 詳しくは、264 ページの「6-2. ブラウザ規制を設定する」を参照してください。
許可 / 規制	[登録ブラウザ] に登録したブラウザを使用したアクセスの許可 / 規制を選択します。 ブラウザ規制が有効な場合にだけ、設定できます。

注意： ルートグループでブラウザ規制を設定した場合、すべての下位グループ、例外ユーザに対してブラウザ規制が適用されます。

5. [■クライアント規制] の [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。



注意： [更新] 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 [更新] 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。

「更新が完了しました。」と表示されます。

6-2. ブラウザ規制を設定する

「ブラウザ規制」の[有効]チェックボックスをオンにすると、指定したブラウザからのアクセスだけを許可したり、規制できます。

指定するブラウザは、[登録ブラウザ]で登録します。ブラウザからのアクセスを許可、または規制する動作については、[許可/規制]で設定します。

-
- 注意：**
- ・ルートグループで規制したブラウザを、下位グループで許可に設定することはできません。
たとえば、ルートグループで登録ブラウザを「MSIE」、「登録ブラウザを許可する」に設定すると、すべてのグループで User-Agent が「MSIE」以外のブラウザを使用したアクセスが規制されます。下位グループでは、登録ブラウザを「MSIE 6」のように設定することで、上位グループよりも規制を強めることができます。
 - ・ルートグループでブラウザ規制を設定した場合、[システム管理]→[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、常にルートグループ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、マスタ管理者以外では閲覧できません。
ルートグループ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) マスタ管理者で管理画面にログインします。
- (2)[アクセス管理]→[アクセスログ管理]をクリックします。
[アクセスログ管理]が表示されます。
- (3)[アクセスログ出力単位]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、384 ページの「A-14. amslog [ログファイルのアーカイブ]」を参照してください。

■ ブラウザ規制を登録する

1. [ブラウザ規制]-[有効] チェックボックスをオンにします。
[登録ブラウザ]、[許可/規制] が設定可能になります。

クライアント規制

クライアント規制を設定します。更新

ブラウザ規制

☒ 有効

登録ブラウザ

登録変更削除

※ グループ設定の許可よりも、ルートグループの規制が優先されます。

許可/規制

☒ 登録ブラウザを許可する(他のすべてのブラウザを規制する)

☐ 登録ブラウザを規制する(他のすべてのブラウザを許可する)

2. [登録ブラウザ] のテキストボックスに、ブラウザ情報を入力します。
Web ブラウザの User-Agent を入力します。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 5.0	MSIE 5
Internet Explorer 5.5	MSIE 5.5
Internet Explorer 6.0	MSIE 6
Internet Explorer 7.0	MSIE 7
Netscape 6.0	Netscape6
Netscape 7.0	Netscape/7
Firefox	Firefox
Netscape、Firefox、Mozilla 共通	Gecko
Opera ※	Opera

※ Opera では、User-Agent に「Compatible; MSIE 5.5」や、「Compatible; MSIE 6.0」が含まれる場合があります。

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。

3. [登録] 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。

4. [許可 / 規制] で、「登録ブラウザ」からのアクセスの許可 / 規制を設定します。

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。
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。

5. [■クライアント規制] の [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。

注意： [更新] 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 [更新] 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。

「更新が完了しました。」と表示されます。

■ 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。
クリックしたブラウザ情報がテキストボックスに表示されます。

■ クライアント規制

クライアント規制を設定します。 [更新](#)

ブラウザ規制 ☒ 有効

登録ブラウザ

- MSIE 5
- MSIE 5.5**
- Netscape6
- Netscape/7
- Firefox

MSIE 5.5 [登録](#) [変更](#) [削除](#)

※ グループ設定の許可よりも、ルートグループの規制が優先されます。

許可/規制

- ☒ 登録ブラウザを許可する(他のすべてのブラウザを規制する)
- ☐ 登録ブラウザを規制する(他のすべてのブラウザを許可する)

2. ブラウザ情報を変更します。
3. [変更] ボタンをクリックします。
ブラウザ情報が変更されます。

■ クライアント規制

クライアント規制を設定します。 [更新](#)

ブラウザ規制 ☒ 有効

登録ブラウザ

- MSIE 5
- MSIE 6**
- Netscape6
- Netscape/7
- Firefox

[登録](#) [変更](#) [削除](#)

※ グループ設定の許可よりも、ルートグループの規制が優先されます。

許可/規制

- ☒ 登録ブラウザを許可する(他のすべてのブラウザを規制する)
- ☐ 登録ブラウザを規制する(他のすべてのブラウザを許可する)

注意： [登録] ボタンをクリックした場合、新規項目として追加されます。

4. [■クライアント規制] の [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。

注意： [更新] 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 [更新] 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。

「更新が完了しました。」と表示されます。

■ 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をクリックします。

2. [削除] ボタンをクリックします。

ブラウザ情報が削除されます。

3. [■クライアント規制] の [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。

注意： [更新] 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 [更新] 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。

「更新が完了しました。」と表示されます。

7. 規制オプションの設定

[規制オプション設定] では、規制する検索ワードや書き込みワードの指定、またはIPアドレスを使用した URL の規制など、詳細なフィルタリング機能を設定します。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] 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。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [規制オプション設定へ] をクリックします。
[■規制オプション設定] が表示されます。
4. 規制オプションを設定します。



設定については、以下の項目を参照してください。

規制メッセージ	グループごとの規制メッセージを最大半角 128 文字で入力します。規制メッセージには、全角文字、半角英数字、半角記号を使用できます。
オーバーライドパスワード	オーバーライドに関連する項目を設定します。 273 ページの「7-1. オーバーライドの詳細設定」を参照してください。
オーバーライドタイマー	
オーバーライド	
IP アドレスリクエスト拒否	[有効] チェックボックスをオンにすると、IP アドレスを使用した URL (http://192.168.1.1/ など) を規制できます。
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します。 272 ページの「規制キーワードの設定」を参照してください。
規制検索キーワード	
書き込み規制	書き込み規制に関連する項目を設定します。 274 ページの「7-2. 書き込み規制の詳細設定」を参照してください。
書き込み規制サイズ	
マルチパートリクエスト規制	
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) を規制します。 272 ページの「規制キーワードの設定」を参照してください。
規制書き込みキーワード	

注意： ・Squid 版では、次の設定項目は表示されません。

書き込み規制サイズ/マルチパートリクエスト規制/書き込みキーワード規制/
規制書き込みキーワード

- ・規制メッセージは [システム管理] → [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。
- ・書き込み規制サイズは [システム管理] → [フィルタリングルール共通設定] の
[■書き込み規制設定] で、[グループ毎に書き込み規制サイズの設定を行う] が
設定されているときに表示されます。
- ・ルートグループで設定した規制検索キーワード、規制書き込みキーワードは、す
べてのグループに適用されます。

5. [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。

注意： [更新] 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 [更新] 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。

「更新が完了しました。」と表示されます。

■ 規制キーワードの設定

規制検索キーワード、規制書き込みキーワードの設定について説明します。

1. [検索キーワード規制] または [書き込みキーワード規制] の [有効] チェックボックスをオンにします。

規制検索キーワード、規制書き込みキーワードが設定可能になります。

2. [規制検索キーワード] または [規制書き込みキーワード] を設定します。

キーワードを最大 20 文字で設定します。テキストボックスにキーワードを入力し、[追加] ボタンをクリックします。

登録したキーワードを変更、削除する場合、キーワードをクリックして、[変更] または [削除] ボタンをクリックします。



注意： ルートグループで設定した規制検索キーワード、規制書き込みキーワードは、すべてのグループに適用されます。

3. [■規制オプション] の [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。

注意： [更新] 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 [更新] 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。

「更新が完了しました。」と表示されます。

7-1. オーバーライドの詳細設定

オーバーライドに関連した、[規制オプション設定] の項目について説明します。

注意： オーバーライドは [システム管理]→[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。

- ・ **オーバーライドパスワード**

オーバーライド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。

!#\$%&'()= `~{+}_-^@[].*/<>|

・オーバーライドパスワードが未設定の場合、パスワードなしでオーバーライドを解除できます。

- ・ **オーバーライドタイマー**

オーバーライドを解除する時間 (1 秒～ 3,600 秒) を設定します。

- ・ **オーバーライド**

[有効] チェックボックスをオンにすると、カテゴリ別ルールで「規制」に設定されているカテゴリに対して、オーバーライドを適用します。

[規制オプション設定] の「書き込み規制」と同時に設定した場合、書き込み規制→オーバーライドの順番に適用されます。詳しくは、275 ページの「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」を参照してください。

7-2. 書き込み規制の詳細設定

書き込み規制に関連した、[規制オプション設定] の項目について説明します。

- **書き込み規制**

[有効] チェックボックスをオンにすると、すべての URL に書き込み規制を適用します。

[規制オプション設定] の「オーバーライド」と同時に設定した場合、書き込み規制→オーバーライドの順番に適用されます。詳しくは、275 ページの「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」を参照してください。

- **書き込み規制サイズ**

[システム管理] → [フィルタリングルール共通設定] の [■書き込み規制設定] で、[グループ毎に書き込み規制サイズの設定を行う] が設定されているときに表示されます。

[全てのサイズの POST リクエストを書き込み規制の対象とする] チェックボックスをオンにすると、グループで発生したすべての書き込み (POST リクエスト) を規制の対象にします。POST データサイズを指定した場合、指定したサイズを超える書き込み (POST リクエスト) を規制の対象にします。

- **マルチパートリクエスト規制**

[有効] 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。

■ 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

各グループに適用されたカテゴリ別フィルタリングルールでは、カテゴリごとに規制内容（許可、オーバーライド、書き込み規制、規制）が設定されています。

カテゴリごとの規制内容と、規制オプションのオーバーライド、書き込み規制を組み合わせで設定する場合、以下の4種類の組み合わせがあります。

- ・ 規制オプションのオーバーライド、書き込み規制の両方が無効
- ・ 規制オプションのオーバーライドだけが有効
- ・ 規制オプションの書き込み規制だけが有効
- ・ 規制オプションのオーバーライド、書き込み規制の両方が有効

ここでは、上記の組み合わせに設定した場合の規制ルールについて説明します。

(1) 規制オプションのオーバーライド、書き込み規制の両方が無効

規制オプションのオーバーライド、書き込み規制の両方が無効のため、カテゴリごとの規制ルールが適用されます。

	カテゴリごとの規制ルール			
	許可	オーバーライド	書き込み規制	規制
Web ページの閲覧	○	△	○	×
Web ページへの書き込み	○	△	×	×

○:許可 △:オーバーライド ×:規制

(2) 規制オプションのオーバーライドだけが有効

カテゴリごとの規制ルールで、規制対象の操作に対してオーバーライドが適用されます。以下の表では、色の付いている部分の操作に対してオーバーライドが適用されます。

	カテゴリごとの規制ルール			
	許可	オーバーライド	書き込み規制	規制
Web ページの閲覧	○	△	○	△
Web ページへの書き込み	○	△	△	△

○:許可 △:オーバーライド ×:規制

(3) 規制オプションの書き込み規制だけが有効

すべてのルールに対して書き込みが規制されます。

以下の表では、色の付いている部分の操作に対して書き込み規制が適用されます。

	カテゴリごとの規制ルール			
	許可	オーバー ライド	書き込み規制	規制
Web ページの閲覧	○	△	○	×
Web ページへの書き込み	×	×	×	×

○:許可 △:オーバーライド ×:規制

(4) 規制オプションのオーバーライド、書き込み規制の両方が有効

規制オプションのオーバーライド、書き込み規制の両方が有効な場合、すべてのルールに対して書き込みが規制された後、規制となっているルールにオーバーライドが適用されます。

書き込みをした場合（掲示板で[投稿]ボタンをクリックするなど）、規制画面が表示されます。規制画面でオーバーライドパスワードを入力すると、オーバーライドタイマーで設定した時間の間だけ、書き込みできるようになります。

以下の表で色の付いている部分にオーバーライドが適用されます。

	カテゴリごとの規制ルール			
	許可	オーバー ライド	書き込み規制	規制
Web ページの閲覧	○	△	○	△
Web ページへの書き込み	△	△	△	△

○:許可 △:オーバーライド ×:規制

注意： 規制画面が表示される前に入力した内容は、オーバーライド実行時にクリアされます。オーバーライド実行後、再度入力する必要があります。

8. カテゴリ別規制メッセージの設定

カテゴリごとの規制画面に表示するメッセージを設定できます。

注意：・サブカテゴリ単位での規制メッセージは設定できません。

- ・[■規制オプション設定] でグループへの規制メッセージを設定している場合には、グループへの規制メッセージとカテゴリ別規制メッセージの両方が表示されます。

カテゴリ別規制メッセージは、グループを登録するときに、上位グループの設定をコピーできます。166 ページの「3-1. グループを登録する」を参照してください。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、カテゴリ別規制メッセージを設定するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] - [カテゴリ別規制メッセージを設定へ] をクリックします。
[■カテゴリ別規制メッセージ設定] が表示されます。
4. カテゴリ別規制メッセージを設定します。

カテゴリ別規制メッセージは、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。



5. [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。

注意： [更新] 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 [更新] ボタンをクリックしてください。

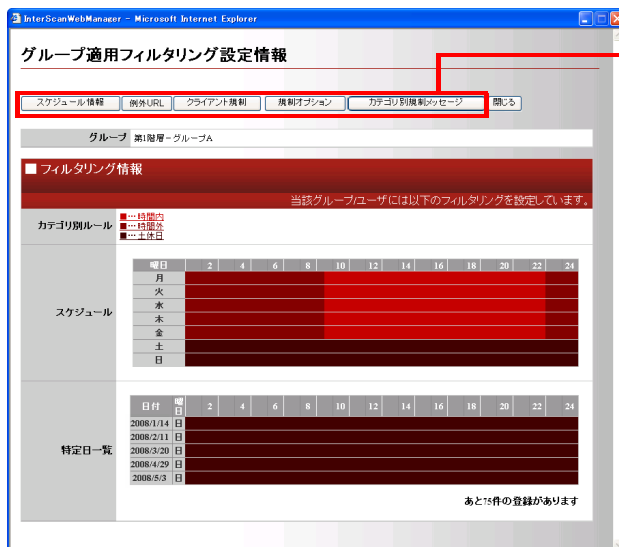
6. [OK] ボタンをクリックします。

「更新が完了しました。」と表示されます。

9. フィルタリング設定の確認

グループに適用するフィルタリング設定を確認できます。

1. [フィルタリング設定] → [グループ設定] をクリックします。
[グループ設定] が表示されます。
2. グループ一覧から、フィルタリング設定を確認するグループをクリックします。
[■フィルタリング設定] が表示されます。
3. [■フィルタリング設定] で [グループ適用フィルタリング表示] ボタンをクリックします。
[グループ適用フィルタリング設定情報] 画面が、別ウィンドウで表示されます。
4. グループに適用するフィルタリング設定を確認します。



クリックすると、表示を切り替えることができます。

初期状態では、[スケジュール情報] ボタンをクリックした状態で表示されます。
画面上のボタンをクリックして、表示を切り替えます。表示できる情報については、次の表を参照してください。

スケジュール情報	281 ページ
例外 URL	282 ページ
クライアント規制	282 ページ
規制オプション	283 ページ
カテゴリ別規制メッセージ	283 ページ

注意： Squid 版では、[クライアント規制] ボタンは表示されません。

- 5.** [閉じる] ボタンをクリックします。
[グループ適用フィルタリング設定情報] 画面が閉じます。

■ スケジュール情報

グループに適用されているフィルタリングスケジュールおよびフィルタリングルールを表示します。
[カテゴリ別ルール] のルール名、[スケジュール] および [特別日一覧] の時間帯をクリックすると、
[カテゴリ別フィルタリングルール情報] が表示されます。[戻る] ボタンをクリックすると、[スケジュール情報] に戻ります。

スケジュール情報 | 例外URL | クライアント規制 | 複製オプション | カテゴリ別規制メッセージ | 閉じる

グループ 第1層-グループA

■ フィルタリング情報

当該グループ/ユーザには以下のフィルタリングを設定しています。

カテゴリ別ルール

- ...時間帯
- ...時間帯
- ...土休日

スケジュール

曜日	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
月																								
火																								
水																								
木																								
金																								
土																								
日																								

特別日一覧

日付	曜日	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2008/1/14																									
2008/2/11																									
2008/3/20																									
2008/4/29																									
2008/5/3																									

あと75件の登録があります

注意： [カテゴリ別フィルタリングルール情報] で [閉じる] ボタンをクリックすると、[グループ適用フィルタリング設定情報] 画面が閉じます。

■ 例外 URL

例外 URL の一覧を表示します。

[カテゴリ > サブカテゴリ]、[URL 順] ボタンをクリックすると、並び順を変更できます。



注意： ・上位グループで設定した例外 URL は、青色の文字で表示されます。

- ・「閲覧のみ許可」に登録した URL は、「許可カテゴリ > 閲覧のみ許可」として表示されます。

■ クライアント規制

クライアント規制の設定内容を表示します。



注意： ルートグループのブラウザ規制は、すべてのユーザに対して有効になります。ルートグループのブラウザ規制は、[共通設定] として表示されます。

■ 規制オプション

規制オプションの設定内容を表示します。

スケジュール情報		例外URL	クライアント規制	規制オプション	カテゴリ別規制メッセージ	閉じる
グループ 第1階層-グループA						
■ 規制オプション 規制オプションが設定されています。						
規制メッセージ		グループA用の規制メッセージ				
オーバーライドパスワード	オーバーライドにパスワードを設定しております。					
オーバーライドタイマー	オーバーライドは120秒間可能です。					
オーバーライド	規制対象カテゴリでオーバーライドが可能となっています。					
IPアドレスリクエスト拒否	IPアドレスでリクエストを送信することはできません。					
検索キーワード規制		検索キーワード規制が設定されています。				
規制検索キーワード	グループ設定	通信販売 オークション				
書き込み規制		書き込み規制が設定されています。				
マルチパートリクエスト規制	マルチパートリクエスト規制が設定されています。					
書き込みキーワード規制	書き込みキーワード規制が設定されています。					
規制書き込みキーワード	グループ設定	出会い 薬物				

注意： ルートグループで設定した、検索キーワード規制および書き込みキーワード規制は、すべてのユーザに対して有効となります。ルートグループの検索キーワード規制および書き込みキーワード規制は、[共通設定] として表示されます。

■ カテゴリ別規制メッセージ

カテゴリ別規制メッセージの設定内容を表示します。

スケジュール情報		例外URL	クライアント規制	規制オプション	カテゴリ別規制メッセージ	閉じる
グループ 第1階層-グループA						
■ カテゴリ別規制メッセージ カテゴリ別規制メッセージが設定されています。						
カテゴリ名		カテゴリ別規制メッセージ				
ユーザ設定	「ユーザ設定」カテゴリのURLに対する規制メッセージ					
不法	「不法」カテゴリのURLに対する規制メッセージ					
主張	「主張」カテゴリのURLに対する規制メッセージ					
アダルト	「アダルト」カテゴリのURLに対する規制メッセージ					
セキュリティ・プロキシ	「セキュリティ・プロキシ」カテゴリのURLに対する規制メッセージ					
出会い	「出会い」カテゴリのURLに対する規制メッセージ					
金融	「金融」カテゴリのURLに対する規制メッセージ					
ギャンブル	「ギャンブル」カテゴリのURLに対する規制メッセージ					
ゲーム	「ゲーム」カテゴリのURLに対する規制メッセージ					
ショッピング	「ショッピング」カテゴリのURLに対する規制メッセージ					
コミュニケーション	「コミュニケーション」カテゴリのURLに対する規制メッセージ					

10. 例外ユーザのフィルタリング設定

指定したアカウントまたは IP アドレスを例外ユーザに登録すると、グループに適用されるフィルタリング設定とは別のフィルタリング設定を適用できます。

[例外ユーザ設定] では例外ユーザの登録および解除や、例外ユーザ用フィルタリング設定を行います。

10-1. 例外ユーザのフィルタリング設定の流れ

例外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。

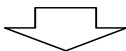
1. グループのフィルタリング設定

例外ユーザに設定するユーザが所属するグループの、フィルタリング設定を行います。
例外 URL 設定、カテゴリ別規制メッセージなどは、グループの設定が適用されます。



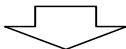
2. フィルタリングルールを設定

例外ユーザに適用するフィルタリングルールを設定します。
カテゴリ別に規制内容を選択して、フィルタリングルールを設定します。
フィルタリングルールを設定 →「3. カテゴリ別フィルタリングルールを設定」(226 ページ)



3. スケジュールの設定

例外ユーザに適用する基本フィルタリングルールを設定します。また、指定した曜日、時間帯に異なるフィルタリングルールを適用することも可能です。
スケジュールの設定 →「4. スケジュールの設定」(233 ページ)
例外ユーザ用スケジュールの登録 →「4-5. 例外ユーザ用スケジュールを登録する」(244 ページ)



4. 例外ユーザの登録、設定

グループに登録された IP アドレス、またはアカウントを例外ユーザに登録します。
また、スケジュール以外の例外ユーザ用フィルタリング設定を行います。
例外ユーザの登録、設定 →「10-2. 例外ユーザに登録する」(285 ページ)

10-2. 例外ユーザに登録する

指定したアカウントまたはIPアドレスを、例外ユーザに登録します。

1. [フィルタリング設定] → [例外ユーザ設定] をクリックします。
[例外ユーザ設定] が表示されます。

注意： グループ一覧が表示される画面では、画面を切り替えても同じグループが選択されます。

[フィルタリング設定] → [グループ設定]

[フィルタリング設定] → [例外ユーザ設定]

[グループ / ユーザ管理] → [グループ / ユーザ選択]

2. ユーザー一覧から、例外ユーザに登録するアカウントまたはIPアドレスをクリックします。
[■例外ユーザ情報]、[■スケジュール] が表示されます。



3. 例外ユーザ用のフィルタリング設定を作成します。

[■例外ユーザ情報]

グループ名	選択しているユーザのグループを表示します。
アカウント名 (IP アドレス)	選択しているアカウント名または IP アドレスを表示します。

[■スケジュール]

ボタンをクリックすると、表示を切り替えできます。各項目での設定方法については、次の表を参照してください。

スケジュール選択	287 ページ
規制オプション変更	288 ページ
クライアント規制変更	289 ページ

注意： Squid 版では、[クライアント規制変更] ボタンは表示されません。

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。

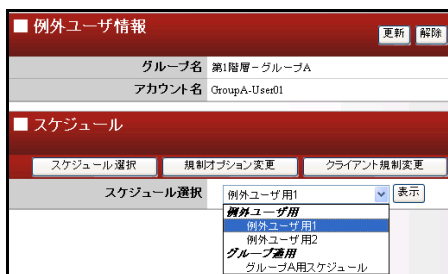
「登録が完了しました。」と表示され、ユーザー一覧に「例外ユーザ」の表示が追加されます。



■ スケジュール選択

例外ユーザ用のスケジュールを選択します。

[グループ設定] で作成した、グループ適用スケジュール、例外ユーザ用スケジュールから選択できます。



注意： 例外ユーザ用のカテゴリ別ルール、スケジュールについては、[グループ設定] で登録してください。

カテゴリ別ルールの設定方法については、226 ページの「3. カテゴリ別フィルタリングルールの設定」を参照してください。

スケジュールの設定方法については、233 ページの「4. スケジュールの設定」を参照してください。

■ 規制オプション変更

例外ユーザ用の規制オプションを設定します。
初期状態では、[グループ設定]の規制オプション設定の設定内容が表示されます。
設定項目については、270 ページの「7. 規制オプションの設定」を参照してください。

■ 例外ユーザ情報

更新

解除

グループ名

第1階層-グループA

アカウント名

GroupA-User01

■ 規制オプション

スケジュール選択

規制オプション変更

クライアント規制変更

規制メッセージ

オーバーライド
パスワード

オーバーライドタイマー

120

秒 ※デフォルト値は120秒です。

オーバーライド

☐有効 ※規制対象カテゴリでオーバーライドが可能です。

IPアドレスリクエスト拒否

☐有効

検索キーワード
規制

☐有効

規制検索キー
ワード

追加

変更

削除

書き込み規制

☐有効

マルチパートリク
エスト規制

☐有効

書き込みキー
ワード規制

☐有効

規制書き込みキ
ワード

追加

変更

削除

■ クライアント規制変更

例外ユーザ用のクライアント規制を変更します。

初期状態では、[グループ設定] のクライアント規制の設定内容が表示されます。

設定項目については、262 ページの「6. クライアント規制設定」を参照してください。

注意： Squid 版では、[クライアント規制変更] ボタンが表示されません。

■ 例外ユーザ情報 更新 解除

グループ名 第1階層-グループA
アカウント名 GroupA-User01

■ クライアント規制

スケジュール選択 規制オプション変更 クライアント規制変更

ブラウザ規制 ☒ 有効

登録ブラウザ

- MSIE 5
- MSIE 6
- Netscape6
- Netscape/7
- Firefox

登録 変更 削除

許可/規制

☒ 登録ブラウザを許可する
☐ 登録ブラウザを規制する

10-3. 例外ユーザの登録を解除する

例外ユーザの登録を解除する方法について説明します。

1. [フィルタリング設定] → [例外ユーザ設定] をクリックします。
[例外ユーザ設定] が表示されます。
2. ユーザー一覧から、例外ユーザの登録を解除するアカウントまたは IP アドレスをクリックします。
[■例外ユーザ情報]、[■スケジュール] が表示されます。



3. [解除] 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。

「解除が完了しました。」と表示され、ユーザー一覧から「例外ユーザ」の表示が削除されます。



11. パス内 URL 規制機能

翻訳サイトや検索サイトなどで別の 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 2 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。

12. URL メモリキャッシュ機能

ISWMでは、リクエストされたURLが次の条件のいずれかを満たす場合、メモリにキャッシュします。

- リクエストされた URL がフィルタリング用データベースに登録されていない。
- リクエストされた URL が例外 URL の「許可カテゴリ > 許可カテゴリ」に登録されている。

キャッシュされた URL がリクエストされた場合、フィルタリング用データベースを検索することなく、許可の URL として処理されます。

-
- 注意：**
- キャッシュサイズの最大まで URL がキャッシュされた場合、参照された時間が最も古いキャッシュから順にクリアされます。
 - キャッシュデータはフィルタリング用データベース更新時、フィルタリングサービス再起動時、および `amsdata -reload` コマンド実行時などにクリアされます。
 - 例外 URL を更新 (登録、削除) すると、キャッシュデータはクリアされます。
-

MEMO

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 Trend Micro InterScan WebManager (以下、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システム設定、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、[システム設定] 画面で各種の設定をしてください。

1-1. 簡易設定と詳細設定の設定内容

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。簡易設定と詳細設定で設定できる内容の違いは以下のとおりです。

システム 設定方法	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
簡易設定	ユーザ認証無し	全ユーザー一括適用	設定できません
詳細設定	アカウント / IP アドレス認証 LDAP 認証 NTLM 認証 (スタンドアロン版のみ)	全ユーザー一括適用 グループ別適用 ユーザ別適用	曜日、時間帯、特定日ごとに設定可能

ユーザ認証方式の設定については、105 ページの「8. ユーザ認証の設定」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、[フィルタリング設定]→[グループ設定]の[■フィルタリング設定]-[カテゴリ別ルール登録]または[カテゴリ別ルール変更・削除]でフィルタリングルールを登録、または変更してください。

フィルタリングルールの登録・変更については 226 ページの「3. カテゴリ別フィルタリングルールの設定」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 [簡易設定へ] ボタンをクリックします。
[簡易設定] が表示されます。
2. [■ 基本設定] で URL データベース、モジュールのダウンロードに必要な情報を入力します。

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。
企業名・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)
連絡先 e-mail	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情報、上位プロキシサーバ設定は、必要に応じて設定します。

フィルタリングサービス情報	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、 [変更する] チェックボックスをオンにします。
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、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情報] の「HTTP」の設定項目は、Squid 版では「リダイレクタ」、ICAP 版では「ICAP」として表示されます。

・Squid 版、ICAP 版の場合、[フィルタリングサービス情報] の「HTTPS」と「FTP OVER HTTP」の設定項目は表示されません。

3. [■カテゴリ別ルール選択] で、ルートグループに適用するカテゴリ別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別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」、「小学校」、「中学校」、「高校」、「大学」、「企業」、「官公庁」の7つのルールが登録されています。

The screenshot shows the 'Easy Settings' (簡易設定) page in the Trend Micro InterScan WebManager. The left sidebar contains navigation links: Home, System Management, Server Settings, Proxy Port Settings, Logging Settings, Proxy/Cache Settings, Authentication Settings, Proxy/Cache Rule Group Management, Filtering Service Settings, and Access Management. The main content area is titled 'Easy Settings' and includes a 'Basic Settings' (基本設定) section with fields for License Key, Company/Institution Name, and Contact Email. Below this is the 'Filtering Service Information' (フィルタリングサービス情報) section, which includes checkboxes for enabling services and fields for their respective ports. The 'Category Rule Selection' (カテゴリ別ルール選択) section is highlighted with a red box, showing the 'DEFAULT RULE' selected. The page also includes a 'Help' (ヘルプ) link and a 'Logout' (ログアウト) button.

[表示] ボタンをクリックすると、[カテゴリ別フィルタリングルール情報] 画面が別ウィンドウで表示されます。[■カテゴリ別ルール選択] で選択したカテゴリ別ルールの規制内容 (許可 / オーバーライド / 書き込み規制 / 規制) を確認できます。

ゆるい  厳しい		許可	自由にアクセスを許可します。
		オーバーライド	規制画面を表示しますが、一定時間だけ閲覧ができます。閲覧するためのパスワード (オーバーライドパスワード) を設定して、アクセスを制限することも可能です。
		書き込み規制	掲示板などへの書き込みを禁止します。閲覧は可能です。
		規制	アクセスを規制して、規制画面を表示します。

[カテゴリ別フィルタリングルール情報] 画面を閉じるには、[閉じる] ボタンをクリックします。

4. [設定] 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： [設定] 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 [設定] 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。

基本設定と、適用するカテゴリ別ルールを設定し、URL データベース、モジュール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、78 ページの「3. データベース / モジュールのダウンロード」を参照してください。

注意： フィルタリングサービス情報を変更した場合、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、68 ページの「2. サーバの設定と登録」を参照してください。

MEMO

アクセス マネジメント ビューの操作

1. Access Management View でできること

アクセス マネジメント ビューは、管理画面右上にある  をクリックすると表示されます。

注意： 閲覧権限がないアカウントの場合、アクセス マネジメント ビューへのリンクは表示されません。
アクセス マネジメント ビューの閲覧権限は、[グループ/ユーザ管理]→[グループ/ユーザ選択]で設定します。
159 ページの「1-6. アカウントでユーザを管理する」を参照してください。

アクセス マネジメント ビューでは、次の機能を使用できます。

■ フィルタリング設定の情報漏えいリスク確認

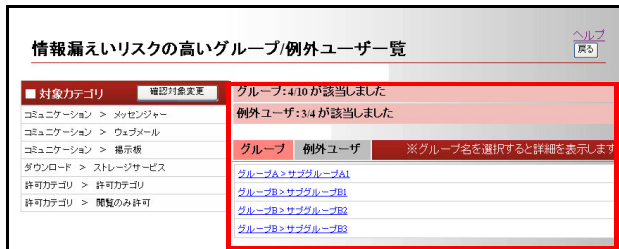
グループや例外ユーザに適用するフィルタリング設定の情報漏えいリスクを分析し、高リスクと判定されたフィルタリング設定を一覧表示します。

→「2. フィルタリング設定の情報漏えいリスクを確認する」(304 ページ)

システムを運用する前やフィルタリング設定を変更したときに、フィルタリング設定に情報漏えいの危険性が残されていないことを確認できます。

注意： 情報漏えいリスクの確認対象は、カテゴリ別ルールの子カテゴリ単位および例外 URL の許可カテゴリ (許可カテゴリ、閲覧のみ許可) から選択できます。

詳しくは、314 ページの「3. 情報漏えいリスクの確認対象を設定する」を参照してください。



情報漏えいリスクが高い
フィルタリング設定を
グループ、例外ユーザー別に
一覧表示します。

一覧表示されたフィルタリング設定をクリックすることにより、情報漏えいリスクが高いカテゴリ別ルールと例外 URL を、確認対象の子カテゴリごとに確認できます。

→「3. 情報漏えいリスクの確認対象を設定する」(314 ページ)

■ 情報漏えいリスクの詳細確認 (カテゴリ別ルール)

情報漏えいリスクの確認対象に設定したサブカテゴリごとの判定結果と、カテゴリ別ルールの総合判定を確認できます。

情報漏えいリスクの高いグループ/例外ユーザ詳細確認

グループ グループA > サブグループA1

■ ルール		■ 例外URL	
ルール名	結果	例外URL	件数
営業部	×	許可カテゴリ > 許可カテゴリ	22 件
開発部	○	許可カテゴリ > 閲覧のみ許可	2 件

カテゴリ	ルール名と規制オプション				結果
	営業部	書き込み規制サイズ	書き込み規制	オーバーライド	
コミュニケーション > メッセージャー	+				×
コミュニケーション > ウェブメール	+				×
コミュニケーション > 掲示板	+				○
ダウンロード > ストレージサービス	+				○

0バイトより大きい書き込みは情報漏えいリスクが低いとみなします。

カテゴリ別ルールの
情報漏えいリスク判定
結果を表示します。

選択したルールの
サブカテゴリごとに
情報漏えいリスク判定
結果を表示します。

■ 情報漏えいリスクの詳細確認 (例外 URL)

情報漏えいリスクの確認対象に設定したサブカテゴリに登録された例外 URL の件数と一覧を確認できます。

情報漏えいリスクの高いグループ/例外ユーザ詳細確認

グループ ADMIN

■ ルール		■ 例外URL	
ルール名	結果	例外URL	件数
営業部	×	許可カテゴリ > 許可カテゴリ	22 件
開発部	○	許可カテゴリ > 閲覧のみ許可	2 件

例外URL (許可カテゴリ: 閲覧・書き込みが可能になります。)

※ 青色文字表示は上位グループで登録されている例外URLです。

全2ページ (22件) 前へ 12 次へ

http://dummy.net/star.jp/
http://dummy1.net/star.jp/
http://dummy10.net/star.jp/
http://dummy11.net/star.jp/
http://dummy12.net/star.jp/

登録された例外 URL を、
件数順に表示します。
情報漏えいリスクが高い
カテゴリは赤色、リスクが
低いカテゴリは黒色で、
件数を表示します。

選択した例外 URL の
カテゴリに登録された
URL 一覧を表示します。

2. フィルタリング設定の情報漏えいリスクを確認する

グループ、例外ユーザに適用するフィルタリング設定の情報漏えいリスクを確認する手順について説明します。

注意： 情報漏えいリスクの確認対象は、カテゴリ別ルールの子カテゴリ単位および例外URLの許可カテゴリ（許可カテゴリ、閲覧のみ許可）です。

初期設定ではシステムで確認を推奨する子カテゴリが設定されていますが、自由に変更できます。情報漏えいリスクの確認対象の設定方法については、314ページの「3. 情報漏えいリスクの確認対象を設定する」を参照してください。

1. 管理画面右上の、 をクリックします。

[Access Management View] 画面が別ウィンドウで表示されます。

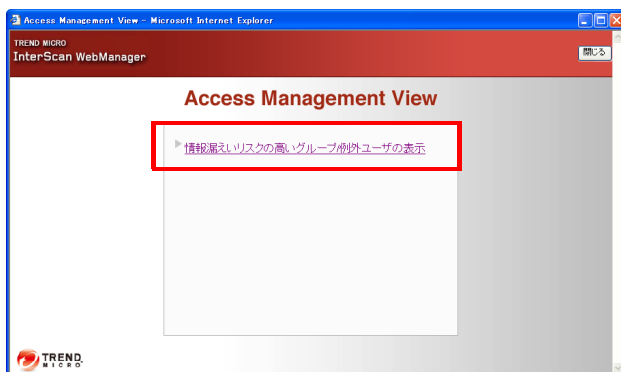
注意： 閲覧権限がないアカウントの場合、アクセス マネジメント ビューへのリンクは表示されません。

アクセス マネジメント ビューの閲覧権限は、[グループ/ユーザ管理]→[グループ/ユーザ選択]で設定します。

159 ページの「1-6. アカウントでユーザを管理する」を参照してください。

2. [情報漏えいリスクの高いグループ/例外ユーザの表示] をクリックします。

[情報漏えいリスクの高いグループ/例外ユーザー一覧] 画面が表示されます。



3. 情報漏えいリスクが高いグループ、例外ユーザのフィルタリング設定を確認します。

[グループ] または [例外ユーザ] をクリックすると、情報漏えいリスクの高いグループ、例外ユーザの表示を切り替えることができます。

一覧表示されたグループ、例外ユーザをクリックすると、情報漏えいリスクを確認する項目ごとの詳細情報が表示されます。306 ページの「2-1. 情報漏えいリスクの判定結果を確認する」を参照してください。

情報漏えいリスクの高いグループ/例外ユーザー一覧

ヘルプ

情報漏えいリスクの高いグループ、例外ユーザの数が表示されます。

クリックすると、グループ一覧/例外ユーザー一覧を切り替えることができます。

■対象カテゴリ	情報漏えいリスクを確認するサブカテゴリ名を「カテゴリ>サブカテゴリ」の形式で一覧表示します。
グループ	クリックすると、情報漏えいリスクの高いグループを「上位グループ>グループ」の形式で一覧表示します。 グループ名をクリックすると、詳細情報を表示します。
例外ユーザー	クリックすると、情報漏えいリスクの高い例外ユーザを「所属するグループ>ユーザ」の形式で一覧表示します。 クリックすると、詳細情報を表示します。

注意： 情報漏えいリスクが高いフィルタリング設定、例外ユーザが存在しない場合、「情報漏えいリスクの高いグループ/例外ユーザは存在しませんでした」と表示されます。

4. [閉じる] ボタンをクリックします。

[Access Management View] 画面が閉じます。

[戻る] ボタンをクリックすると、アクセス マネジメント ビューのトップ画面に戻ります。

以上で、情報漏えいリスクが高いフィルタリング設定の確認は完了です。

必要に応じて情報漏えいリスクが高いと判定されたフィルタリング設定を修正してください。

情報漏えいリスクの判定条件については、311ページの「2-2. 情報漏えいリスクの判定方法」を参照してください。

情報漏えいリスクを確認する対象カテゴリを変更する場合、314 ページの「3. 情報漏えいリスクの確認対象を設定する」を参照してください。

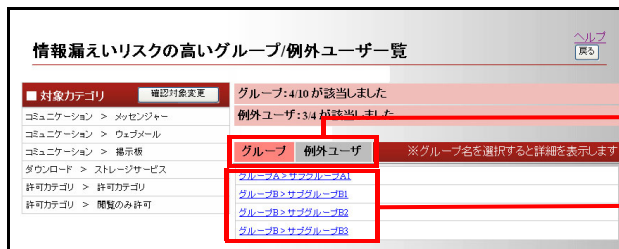
2-1. 情報漏えいリスクの判定結果を確認する

[情報漏えいリスクの高いグループ/例外ユーザー一覧]で、グループ名または例外ユーザ名をクリックすると、情報漏えいリスクの確認対象に設定した、カテゴリ別ルールおよび例外 URL のサブカテゴリごとの詳細情報を確認できます。

[情報漏えいリスクの高いグループ/例外ユーザ詳細確認]画面の見かたと、情報漏えいリスクの判定方法について説明します。

1. [情報漏えいリスクの高いグループ/例外ユーザー一覧]で、情報漏えいリスクの判定結果を確認するグループ、または例外ユーザをクリックします。

[グループ]、[例外ユーザ]をクリックするとグループ一覧、例外ユーザー一覧を切り替えできます。



クリックすると、グループ一覧/例外ユーザー一覧を切り替えできます。

情報漏えいリスクの判定結果を確認するグループ、例外ユーザをクリックします。

[情報漏えいリスクの高いグループ/例外ユーザ詳細確認]が表示されます。

クリックしたグループ、例外ユーザのカテゴリ別ルールの情報漏えいリスク判定結果と、登録された例外 URL (許可カテゴリ、閲覧のみ許可) の件数が表示されます。例外 URL の件数は、情報漏えいリスクが高いカテゴリでは赤色、リスクが低いカテゴリでは黒色で、表示されます。



クリックしたグループ、例外ユーザが表示されます。

2. 情報漏えいリスクの判定結果を確認するカテゴリ別ルール名、または例外 URL のカテゴリをクリックします。

情報漏えいリスクの判定結果の詳細が表示されます。

情報漏えいリスクの高いグループ/例外ユーザ詳細確認			
グループ グループA>サブグループA1			
ルール		例外URL	
ルール名	結果	例外URL	件数
営業部	×	許可カテゴリ > 許可カテゴリ	22 件
開発部	○	許可カテゴリ > 開発のみ許可	2 件

カテゴリごとの判定結果を確認できます。

登録されている URL 一覧を確認できます。

■ルール

グループ、例外ユーザに適用するカテゴリ別ルールを表示します。ルール名をクリックすると、詳細情報が表示されます。

画面については、308 ページの「情報漏えいリスクの詳細情報 (カテゴリ別ルール)」を参照してください。

ルール名	選択したグループ、例外ユーザのスケジュールに設定されているカテゴリ別ルールが、一覧表示されます。
結果	カテゴリ別ルールの情報漏えいリスク判定結果が表示されます。 ○: 情報漏えいリスクが低い。 ×: 情報漏えいリスクが高い。

注意： 確認対象に設定したカテゴリに、情報漏えいリスクが高い項目が 1 件以上存在する場合、「情報漏えいリスクが高い」と判定されます。
詳細については、311 ページの「2-2. 情報漏えいリスクの判定方法」を参照してください。

■例外 URL

例外 URL の許可カテゴリ (許可カテゴリ、閲覧のみ許可) に登録されている URL の件数を表示します。カテゴリ名をクリックすると、登録されている URL の一覧が表示されます。
画面については、310 ページの「情報漏えいリスクの詳細情報 (例外 URL)」を参照してください。

例外 URL	例外 URL のカテゴリが「カテゴリ名 > サブカテゴリ名」形式で表示されます。
件数	登録された例外 URL が、件数順にカテゴリ別で表示されます。 情報漏えいリスクが高いカテゴリでは赤色、リスクが低いカテゴリでは黒色で、件数が表示されます。

3. [戻る] ボタンをクリックします。

[情報漏えいリスクの高いグループ / 例外ユーザー一覧] に戻ります。

以上で、情報漏えいリスクが高いフィルタリング設定の詳細の確認は完了です。

■ 情報漏えいリスクの詳細情報 (カテゴリ別ルール)

[■ルール] に表示されているカテゴリ別ルール名をクリックすると、情報漏えいリスク確認対象のカテゴリごとに判定結果が表示されます。

情報漏えいリスクの高いグループ/例外ユーザ詳細確認

グループ: グループA > サブグループA1

■ ルール		■ 例外 URL	
ルール名	結果	例外 URL	件数
営業部	×	許可カテゴリ > 許可カテゴリ	22 件
情報部	○	許可カテゴリ > 閲覧のみ許可	2 件

カテゴリ	ルール名と規制オプション				結果
	営業部	書き込み規制サイズ	書き込み規制	オーバーライド	
コミュニケーション > メッセージャー	×				×
コミュニケーション > ウェブメール	×				×
コミュニケーション > 掲示板	×	1024 バイト	無効	無効	×
ダウンロード > ストレージサービス	○				○

0 バイトより大きい書き込みは情報漏えいのリスクが高くなります。

クリックしたカテゴリ別
ルールの規制内容が表示
されます。

情報漏えいリスク確認対象
のカテゴリごとに
判定結果が表示されます。

・ [カテゴリ]

情報漏えいリスクの確認対象に設定したカテゴリが表示されます。

確認対象の設定については、314 ページの「3. 情報漏えいリスクの確認対象を設定する」を参照してください。

・ [ルール名と規制オプション]

情報漏えいリスクの確認対象カテゴリについて、カテゴリ別ルールの規制内容と規制オプションの設定、情報漏えいリスク判定結果が表示されます。

判定結果については、311 ページの「2-2. 情報漏えいリスクの判定方法」を参照してください。

カテゴリ別ルール名と規制内容	選択した カテゴリ別ルール名と情報漏えいリスク確認対象カテゴリの規制内容が表示されます。
書き込み規制サイズ	書き込み規制サイズが表示されます。グループごと、またはすべてのグループに共通の設定となります。
書き込み規制	フィルタリング設定の規制オプションの書き込み規制の設定が表示されます。
オーバーライド	フィルタリング設定の規制オプションのオーバーライドの設定が表示されます。
結果	カテゴリ別ルールの情報漏えいリスク判定結果が表示されます。 ○:情報漏えいリスクが低い。 ×:情報漏えいリスクが高い。

注意： ・ Squid 版の場合、[書き込み規制サイズ] は表示されません。

- ・ 書き込み規制サイズの設定については、次の項目を参照してください。
→システム全体で設定する場合：「9. フィルタリングルール共通設定」(137ページ)
→グループごとに設定する場合：「7. 規制オプションの設定」(270 ページ)

■ 情報漏えいリスクの詳細情報 (例外 URL)

[■ 例外 URL] に表示されているカテゴリをクリックすると、登録されている URL 一覧が表示されます。



例外 URL は 1 画面に最大 20 件まで表示されます。20 件以上登録されている場合、20 件ずつ複数ページに分割して表示されます。

前へ	クリックすると、前のページに戻ります。
ページ数	クリックすると、クリックしたページ番号の例外 URL 一覧を表示します。
次へ	クリックすると、次のページに進みます。

注意：

- 例外 URL が登録されていない場合、一覧表示はできません。
- 例外 URL の参照指定が有効な場合、上位グループで登録した例外 URL は青字で表示されます。

2-2. 情報漏えいリスクの判定方法

情報漏えいリスクは、確認対象の設定に従って、次の順番に判定されます。

- (1) 規制オプションのオーバーライド
- (2) 例外 URL の登録
- (3) カテゴリ別ルールの規制内容

(1)～(3)までのすべての項目がチェックされた結果、問題がないと判定された場合、グループまたは例外ユーザの「情報漏えいリスクが低い」と判定されます。

(1) 規制オプションのオーバーライド

規制オプションのオーバーライドが有効な場合、「情報漏えいリスクが高い」と判定されます。

(2) 例外 URL の登録

次の条件を満たす場合、「情報漏えいリスクが高い」と判定されます。

許可カテゴリ > 許可カテゴリ	1 件以上 URL が登録されている。
許可カテゴリ > 閲覧のみ許可	規制オプションのオーバーライドが有効で、かつ 1 件以上 URL が登録されている。

(3) カテゴリ別ルールの規制内容

カテゴリ別ルールでは、確認対象に設定したカテゴリごとに情報漏えいリスクを判定します。すべてのカテゴリで「○ (情報漏えいリスクが低い)」と判定されると、カテゴリ別ルールの判定結果が「○ (情報漏えいリスクが低い)」となります。

詳細については、次の「カテゴリ別ルール規制内容の情報漏えいリスク判定方法」を参照してください。

情報漏えいリスクの高いグループ/例外ユーザ詳細確認

グループ グループA>サブグループA1

■ ルール

ルール名	結果
書き込み	×
閲覧	○

■ 例外URL

例外URL	件数
許可カテゴリ > 許可カテゴリ	22 件
許可カテゴリ > 閲覧のみ許可	2 件

カテゴリ	ルール名と規制オプション				結果
	開発部	書き込み規制サイズ	書き込み規制	オーバーライド	
コミュニケーション > メッセージャー	×				○
コミュニケーション > ウェブメール	×				○
コミュニケーション > 掲示板	×	1024 バイト	無効	無効	○
ダウンロード > ストレージサービス	×				○

すべての確認対象カテゴリが「○」の場合、カテゴリ別ルールの結果が「○」になります。

0 バイトより大きい書き込みは情報漏えいリスクが高いとみなします。

注意：

- 確認対象に設定されていないカテゴリについては判定されません。
- 確認対象で書き込み許容サイズが設定されていない場合、書き込み規制サイズは判定されません。

■ カテゴリ別ルール規制内容の情報漏えいリスク判定方法

カテゴリごとの情報漏えいリスク判定方法について説明します。
カテゴリの規制内容により、判定方法が異なります。

- 規制内容が「許可」、または「オーバーライド」の場合

(1) 規制オプションの書き込み規制

規制オプションの書き込み規制が無効な場合、「情報漏えいリスクが高い」と判定されません。

(2) 書き込み規制サイズ

[情報漏えい確認対象設定] で設定した「書き込み許容サイズ」と値を比較して、書き込み許容サイズよりも値が大きい場合、「情報漏えいリスクが高い」と判定されます。

書き込み許容サイズよりも値が小さい (書き込み許容サイズ $\geq$ 書き込み規制サイズ)	情報漏えいリスクが低い。
書き込み許容サイズよりも値が大きい (書き込み許容サイズ $<$ 書き込み規制サイズ)	情報漏えいリスクが高い。

注意：・Squid 版の場合、書き込み規制サイズは判定されません。

- ・書き込み規制サイズはシステム共通、またはグループごとに設定できます。すべてのサイズのPOSTリクエストを書き込み規制の対象に設定している場合、書き込み規制サイズは 0 バイトになります。
- ・書き込み許容サイズの設定については、314 ページの「3. 情報漏えいリスクの確認対象を設定する」を参照してください。

・規制内容が「書き込み規制」の場合

許可、またはオーバーライドの「(2) 書き込み規制サイズ」と同じ方法で判定します。

3. 情報漏えいリスクの確認対象を設定する

情報漏えいリスクを確認するカテゴリや、書き込みを許可するサイズを設定します。設定した項目について、情報漏えいリスクが判定されます。情報漏えいリスクの確認対象は、マスタ管理者だけが変更できます。

1. 管理画面右上の、 をクリックします。

[Access Management View] 画面が別ウィンドウで表示されます。

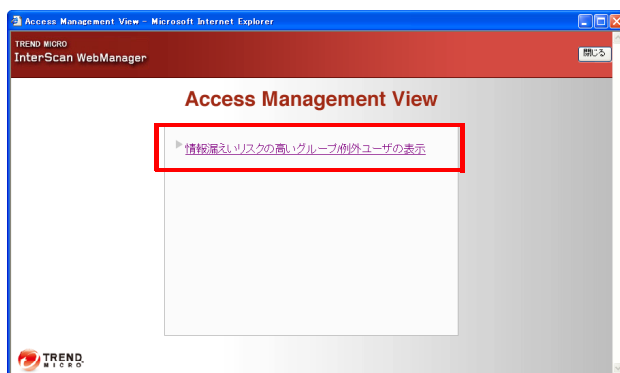
注意： 閲覧権限がないアカウントの場合、アクセス マネジメント ビューへのリンクは表示されません。

アクセス マネジメント ビューの閲覧権限は、[グループ/ユーザ管理]→[グループ/ユーザ選択] で設定します。

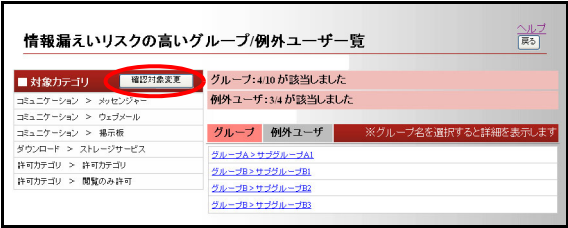
159 ページの「1-6. アカウントでユーザを管理する」を参照してください。

2. [情報漏えいリスクの高いグループ / 例外ユーザの表示] をクリックします。

[情報漏えいリスクの高いグループ / 例外ユーザー一覧] 画面が表示されます。



3. [確認対象変更] をクリックします。
- [情報漏えい確認対象設定] が表示されます。



4. 情報漏えいリスクを確認するカテゴリを設定します。
- 情報漏えいリスクを確認するカテゴリ名、および例外 URL の登録カテゴリ名の、チェックボックスをオンにします。
- 確認対象として推奨するカテゴリは、青字で表示されます。



情報漏えいリスク確認対象に推奨するカテゴリは青字で表示されます。

[カテゴリ順] ボタン	カテゴリ別ルール名の項目順に並べ替えます。
[設定順] ボタン	チェックボックスがオンのカテゴリ→チェックボックスがオフのカテゴリの順に並び替えます。

5. 「**■書き込み許容サイズ**」で、書き込みを許可するサイズを設定します。

チェックボックスをオンにして、書き込みを許容するサイズの上限をバイト単位で入力します。
「書き込み許容サイズ<書き込み規制サイズ」となる場合、情報漏えいのリスクが高いと判定されます。

情報漏えい確認対象設定

戻る 更新

※カテゴリ、例外URL、書き込み許可サイズを確認するか設定します。
※ 確認対象外として掲載するカテゴリを赤字で表示して取ります。

■ カテゴリ

カテゴリ検索

設定欄

コミュニケーション > マネジメント	☒
コミュニケーション > マネジメント	☒
コミュニケーション > ウェブメール	☒
コミュニケーション > メールマガジン・ML	☐
コミュニケーション > 掲示板	☒
コミュニケーション > IT書示版	☐
コミュニケーション > SNS・ブログ	☐
ダウンロード > ダウンロード	☐
ダウンロード > プログラムダウンロード	☐
ダウンロード > ストレージサービス	☒
ダウンロード > 動画配信	☐
検索 > 転載・転載	☐
検索 > キャリアアップ	☐

■ 例外URL

許可カテゴリ > 許可カテゴリ	☒
許可カテゴリ > 閲覧のみ許可	☒

■ 書き込み許可サイズ

0	10万以下

※書き込み許可サイズは書き込み容量の制限、リスクが高くなります。

注意： 書き込み規制サイズの設定については、次の項目を参照してください。

- システム全体で設定する場合：「9. フィルタリングルール共通設定」(137 ページ)
- グループごとに設定する場合：「7. 規制オプションの設定」(270 ページ)

6. 「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。

注意： [更新] 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 [更新] 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。

「更新しました。」と表示されます。

8. 「戻る」ボタンをクリックします。

[情報漏えいリスクの高いグループ / 例外ユーザー一覧] 画面に戻ります。
[閉じる] ボタンをクリックすると、[Access Management View] 画面が閉じます。

以上で、情報漏えいリスクの確認対象の設定は完了です。

アクセスログの管理

1. [アクセス管理] 画面でできること

[アクセス管理] → [アクセスログ管理] 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、マスタ管理者とグループ管理者が使用できます。サブグループ管理者は使用できません。

-
- 注意：**
- ・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、[システム管理] → [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 [アクセス管理] が表示されません。
設定については、89 ページの「5. ログファイルの設定」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。
-

2. アクセスログの管理

[アクセスログ管理] 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。マスタ管理者はシステム全体、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。

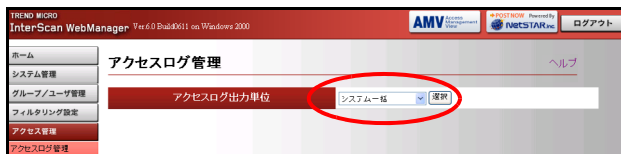
アクセスログには、現在記録中のログファイルとローテート済みのログファイルがあります。現在記録中のログファイルは閲覧が、ローテート済みのログファイルはダウンロード、または削除が可能です。ローテートについては、89 ページの「5. ログファイルの設定」を参照してください。

-
- 注意：**
- ・サブグループ管理者の場合、メインメニューの [アクセス管理] は表示されません。
 - ・グループ管理者が [アクセスログ管理] を使用する場合、[システム管理] → [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 [アクセス管理] が表示されません。設定については、89 ページの「5. ログファイルの設定」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。384 ページの「A-14. amslog [ログファイルのアーカイブ]」を参照してください。
-

2-1. 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. [アクセス管理] → [アクセスログ管理] をクリックします。
マスタ管理者の場合、[アクセスログ管理] が表示されます。
グループ管理者の場合、所属グループの [アクセスログファイル一覧] が表示されます。手順 3 に進んでください。
2. [アクセスログ管理] 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。



[アクセスログファイル一覧] が表示されます。

3. [アクセスログファイル一覧] 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、ソート用ボタンで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、[ログファイル名順]、[サーバ名順]、[サイズ (Mbyte) 順]、[更新日時順] ボタンから選択できます。

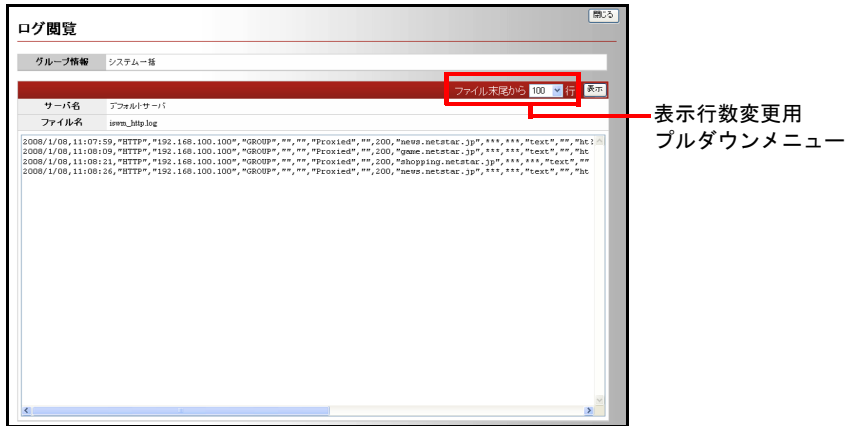
選択されたソート項目 (ボタン) は、白文字で表示されます。

注意： ローテート済みのログは、[システム管理]→[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、89 ページの「5. ログファイルの設定」を参照してください。



グループ情報	アクセスログ出力対象のグループ名を表示します。
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、[アクセスログファイル一覧] に戻ります。

2-2. ロータート済みアクセスログをダウンロード、削除する

ロータ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、不要なロータート済みアクセスログを削除できます。

1. [アクセス管理]→[アクセスログ管理]をクリックします。
マスタ管理者の場合、[アクセスログ管理]が表示されます。
グループ管理者の場合、所属グループの[アクセスログファイル一覧]が表示されます。手順3に進んでください。
2. [アクセスログ管理]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。
[アクセスログファイル一覧]が表示されます。
3. [アクセスログファイル一覧]で、アクセスログの一覧を確認します。



ソート用ボタン

現在のログファイル一覧、ロータート済みのログファイル一覧を、ソート用ボタンで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、[ログファイル名順]、[サーバ名順]、[サイズ (Mbyte) 順]、[更新日時順] ボタンから選択できます。

選択されたソート項目 (ボタン) は、白文字で表示されます。

注意： ロータート済みのログは、[システム管理]→[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。

[全選択] ボタンをクリックすると、すべてのチェックボックスをオンにします。[全解除] ボタンをクリックすると、すべてのチェックボックスをオフにします。



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] 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。

クライアント PC の設定

1. クライアント PC の設定

Trend Micro InterScan WebManager (以下、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。

■ 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、透過プロキシのように 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、[システム管理] → [サーバ設定] の [■サーバ情報] で確認できます。

■ 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。

■ Squid 版の場合

クライアント PC からの通信は、Squid サーバにインストールしたリダイレクタプログラム経由で 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	Squid サーバの IP アドレス
プロキシサーバのポート番号	Squid サーバのポート番号 (HTTP、HTTPS、FTP over HTTP)

注意：

- ・Squid サーバのポート番号は、Squid.conf で設定したポート番号を使用します。
- ・Squid が透過プロキシとして動作している場合には、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。

[システム管理]→[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。

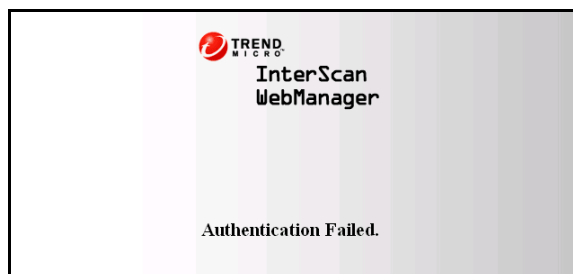
認証設定については、105 ページの「8. ユーザ認証の設定」を参照してください。

■ 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。グループ内に例外ユーザを登録している場合には、例外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の管理をする場合、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

ルートグループの設定が適用されます。

2-1. 規制画面

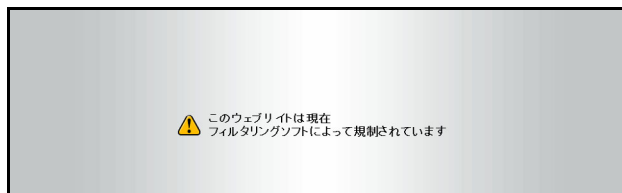
カテゴリ別フィルタリングルールで、「規制」を設定したカテゴリの URL をリクエストすると、規制画面が表示されます。

規制画面の表示方法は、URL/ ファイル/ メッセージの 3 種類があります。83 ページの「4. 管理画面 / 規制画面の表示設定」を参照してください。

■ 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。

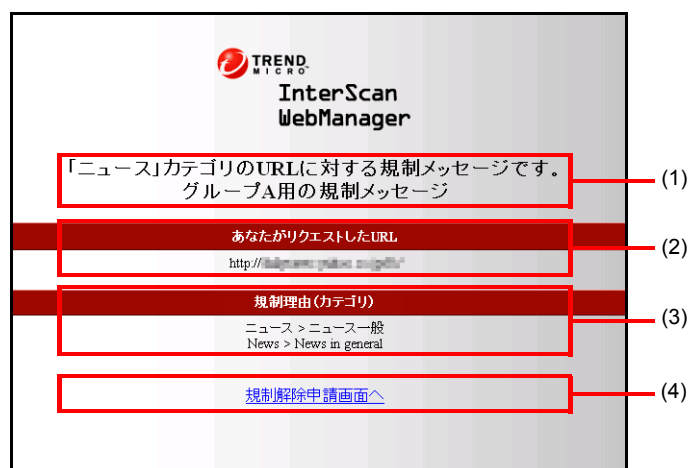
社内および社外の URL を指定できます。初期状態では、「<http://iswm.netstar-inc.com/>」が設定されています。



■ 規制画面（ファイル）の場合

任意の HTML ファイルを規制画面として表示します。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 <インストールディレクトリ> %conf%\block
Solaris/Linux の場合 <インストールディレクトリ> /conf/block



(1) 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。[フィルタリング設定] の規制オプションで規制メッセージが設定されている場合、規制オプションで設定したメッセージ（上の画面では「グループ A 用の規制メッセージ」）が表示されます。また、[フィルタリング設定] のカテゴリ別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。

注意：

- ・規制メッセージは、[システム管理] → [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。
- ・カテゴリ別規制メッセージ、規制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。

(2) 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。

(3) 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。

(4) 規制解除申請画面へのリンク

[システム管理] → [フィルタリングルール共通設定] で規制解除申請機能が有効な場合に表示されます。

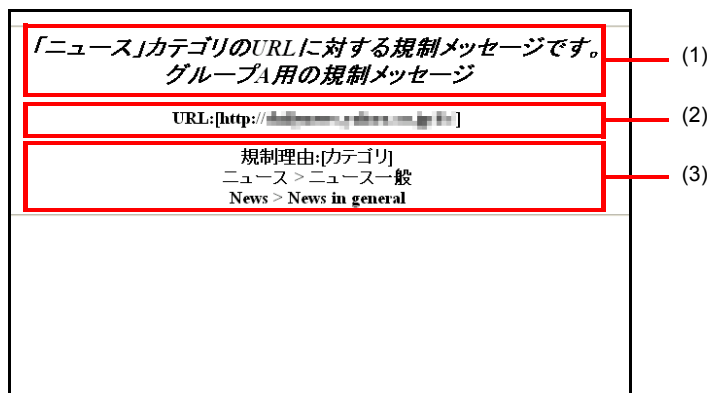
クリックすると、規制解除申請画面が別ウィンドウで表示されます。

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、140 ページの「9-3. 規制解除申請を設定する」を参照してください。

■ 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。



(1) 規制メッセージ

[システム管理] → [画面設定] で設定したメッセージが表示されます。

[フィルタリング設定] の規制オプションで規制メッセージ（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、[システム管理] → [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。

[フィルタリング設定] のカテゴリ別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。

(2) 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。

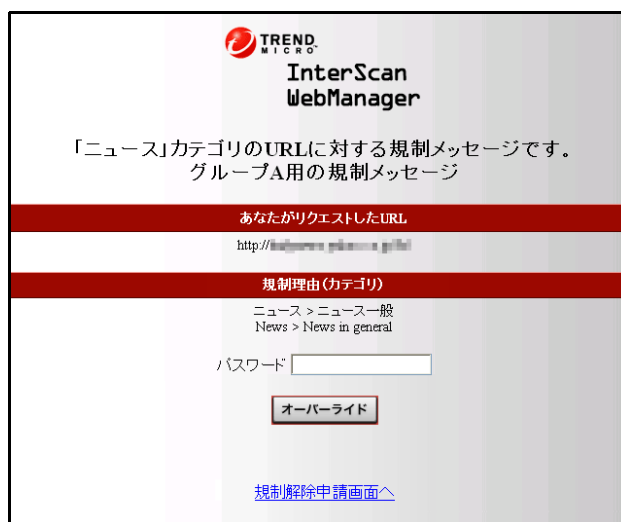
(3) 規制した URL のカテゴリ

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。

2-2. オーバーライド

カテゴリ別フィルタリングルールで、「オーバーライド」を設定したカテゴリの URL をリクエストすると、規制画面にオーバーライドパスワードの入力部分が表示されます。オーバーライドパスワードを入力すると、オーバーライドタイマー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：**
- ・オーバーライドは [システム管理]→[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。
 - ・カテゴリごとにオーバーライドを有効にするには、[フィルタリング設定]→[グループ設定] の「カテゴリ別ルール設定」で設定します。
 - ・特定のグループに対して、規制対象のカテゴリにオーバーライドを適用する場合、[フィルタリング設定]→[グループ設定] の [規制オプション設定] で設定します。
 - ・例外ユーザに対して、規制対象のカテゴリにオーバーライドを適用する場合、[フィルタリング設定]→[例外ユーザ設定] の [規制オプション設定] で設定します。
 - ・オーバーライドパスワード、オーバーライドタイマーは、[フィルタリング設定]→[グループ設定]、または [例外ユーザ設定] の [規制オプション設定] で設定します。270 ページの「7. 規制オプションの設定」を参照してください。
 - ・オーバーライド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。
-



1. [パスワード] テキストボックスに、オーバーライドパスワードを入力します。
2. [オーバーライド] ボタンをクリックします。

オーバーライド タイマー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。

2-3. その他の規制

カテゴリごとの規制、オーバーライド以外に、ISWM で規制できる内容について説明します。

■ 書き込み規制

カテゴリ別フィルタリングルールで、「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 プロトコルで POST、PUT メソッドを使用している URL になります。https (CONNECT メソッド) や Java を使用した入力ページは、書き込み規制の対象にできません。
 - 書き込み規制をする POST リクエストのサイズは、[システム管理]→[フィルタリングルール共通設定] で設定します。140 ページの「9-3. 規制解除申請を設定する」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 を閲覧のみ許可する

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。

3. パスワードの変更

エンドユーザは、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：**
- ・マスタ管理者、グループ管理者、サブグループ管理者は、[グループ / ユーザ管理] → [グループ / ユーザ選択] で、パスワード、メールアドレスを変更してください。
182 ページの「4-4. IP アドレス / アカウントを変更する」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。

マスタサーバの IP アドレスが 192.168.1.1、ポートが 2319 の場合

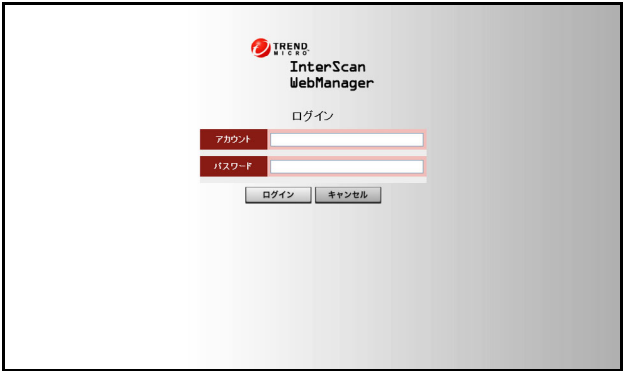
<http://192.168.1.1:2319/index.html> と入力します。

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、設定にあわせてポート番号 (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。

変更するエンド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、[■アカウント更新] 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の管理をする場合、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	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. [更新] 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。
「更新が完了しました。」と表示されます。

4.SSL Access Controller の設定

SSL Access Controller とは、HTTPS プロトコルのフィルタリングを実行するためにクライアント PC にインストールする、Internet Explorer 専用のアドオンプログラムです。

従来は、HTTPS サイト (「https://」で始まる SSL URL) にアクセスする場合、ホスト単位でしか許可・禁止の設定ができませんでした。SSL Access Controller をクライアント側にインストールすることで、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。

通常、クライアント PC から HTTPS サイトの URL をリクエストする場合、ホスト名以外のパスやデータは、すべて暗号化した状態で転送されます。したがって、ISWM はリクエスト URL のホスト名部分しか認識できません。

しかし、SSL Access Controller をインストールした PC では、HTTPS サイトの URL を、完全なパスの状態で、ISWM にリクエストとして送信します。URL 以外のデータは、従来どおり暗号化した状態で転送されます。

SSL Access Controllerを使用しない場合



HTTPSサイトの、ホスト名以外のパスは認識できない。

SSL Access Controllerを使用した場合



HTTPSサイトの完全なパスを認識できる。

また、SSL Access Controller をインストールしていないクライアント PC からの HTTPS 通信を、すべて規制する設定も可能です。HTTPS 通信規制は、管理画面で設定します。

-
- 注意：**
- Squid 版は、SSL Access Controller には対応していません。
 - SSL Access Controller は、Internet Explorer にのみ対応しています。
 - HTTPS プロトコルの書き込み規制には対応していません。
-

■ SSL Access Controller のシステム要件

SSL Access Controller は、以下の環境でお使いください。

OS	Windows XP Professional SP2 (日本語 32bit 版) Windows Vista Ultimate / Business (日本語 32bit 版)
CPU	Intel Pentium / Celeron 系 800MHz 以上
空きメモリ	256MB 以上
対応 Web ブラウザ	Internet Explorer 6.0 SP2 Internet Explorer 7.0

注意： DNS による名前解決ができる環境で使用してください。

4-1. ISWM との連携設定

クライアント PC に SSL Access Controller をインストールする前に、ISWM で必要な設定について説明します。

1. [システム管理] → [フィルタリングルール共通設定] をクリックします。
[フィルタリングルール共通設定] が表示されます。[フィルタリングルール共通設定] については、137 ページの「9. フィルタリングルール共通設定」を参照してください。

2. [■ HTTPS 規制設定] で、[SSL Access Controller を使用する] チェックボックスをオンにします。

[SSL Access Controller 以外からの HTTPS 通信を全て規制する] チェックボックスが、自動的にオンになります。必要に応じて、[SSL Access Controller 以外からの HTTPS 通信を全て規制する] チェックボックスをオフにしてください。

[■ HTTPS 規制設定] の設定と、適用される HTTPS 通信規制は、以下のとおりです。

設定	適用される HTTPS 規制
SSL Access Controller を使用する	SSL Access Controller をインストールしたクライアント PC の HTTPS 通信を、HTTPS サイトのホスト名以降を含む完全パスを指定して規制できます。 SSL Access Controller をインストールしないクライアント PC の HTTPS 通信については、HTTPS サイトのホスト名までを指定した規制が可能です。
SSL Access Controller 以外からの HTTPS 通信を全て規制する	SSL Access Controller をインストールしないクライアント PC からの HTTPS 通信を、すべて規制します。

3. [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。

注意： [更新] 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 [更新] 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。

「更新が完了しました。」と表示されます。

以上で、ISWM との連携設定は完了です。

4-2. SSL Access Controller のインストール

SSL Access Controller は、以下の手順でクライアント PC にインストールしてください。

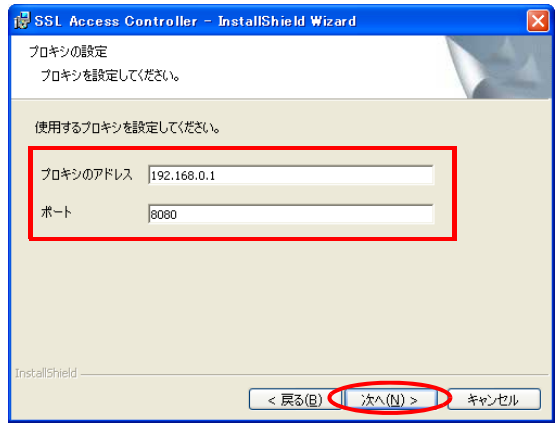
注意： インストール後、OS の再起動が必要です。

- SSL Access Controller をインストールする前に、すべてのアプリケーションを終了してください。
 - SSL Access Controller の「sacproxy.ini」に ISWM の IP アドレスとポート、およびローカルプロキシのポートを設定し、「sac_setup.exe」と同じフォルダに格納してインストールを開始することで、インストール中の入力を省略できます。
「sac_setup.exe」および「sacproxy.ini」は、ISWM の CD-ROM の「program\sac」に格納されています。「sacproxy.ini」については、393 ページの「B. 設定ファイル」を参照してください。
 - ISWM に接続できない環境では、SSL Access Controller をインストールできません。
-

1. インストールを実行するクライアント PC 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. セットアッププログラム「sac_setup.exe」を実行します。
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します] をクリックして選択します。
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ません] をクリックしてインストールを中止してください。
5. [次へ] ボタンをクリックします。
製品使用時の注意事項が表示されます。
6. [はい] をクリックして選択します。
注意事項の内容に同意いただけない場合は、[いいえ] をクリックしてインストールを中止してください。

7. [次へ] ボタンをクリックします。

プロキシの設定画面が表示されます。

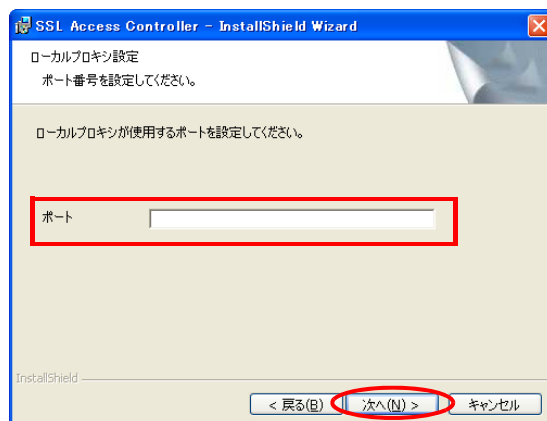


プロキシのアドレス	ISWM のマスタサーバ、スレーブサーバのうち、SSL Access Controller との通信に使用するサーバの IP アドレスを設定します。
ポート	ISWM の HTTP ポート番号を設定します。

注意：「sac_setup.exe」と同じフォルダに「sacproxy.ini」を格納してインストールした場合、「sacproxy.ini」であらかじめ設定した内容が、テキストボックスに表示されます。
[ポート] は、「sacproxy.ini」の初期設定では「8080」です。

8. [プロキシのアドレス]と[ポート]を設定して、[次へ]ボタンをクリックします。

ローカルプロキシ設定画面が表示されます。



注意：「sac_setup.exe」と同じフォルダに「sacproxy.ini」を格納してインストールした場合、「sacproxy.ini」であらかじめ設定した内容が、テキストボックスに表示されます。「sacproxy.ini」で設定していない場合、[ポート]には、「18081」(初期値)が表示されます。

9. Internet Explorer と SSL Access Controller 間の通信に使用するポート番号を設定して、[次へ]ボタンをクリックします。

注意：他のアプリケーションが通信に使用するポートと、重複しないように設定してください。

10. [インストール]ボタンをクリックします。

インストールが開始されます。

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「Program Files¥Trend Micro¥SSL Access Controller」フォルダにインストールされます。

11. [完了]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. [はい] ボタンをクリックします。

Windows が再起動します。

以上で、SSL Access Controller のインストールは完了です。
インストールが完了すると、プロキシサーバの設定が次の設定に変更されます。

サーバの種類	IP アドレス	ポート番号
HTTP	ISWM の IP アドレス	手順 8 で設定した、ISWM の HTTP ポート番号 (初期値 8080)
Secure	127.0.0.1	手順 9 で設定した、ローカルプロキシ設定のポート番号 (初期値 18081)
FTP	ISWM の IP アドレス	手順 8 で設定した、ISWM の HTTP ポート番号 (初期値 8080)

注意：

- ・アンインストールすると、インストール前の設定に戻ります。
- ・自動構成スクリプトを使用している場合、プロキシサーバの設定は変更されません。自動構成スクリプトを変更するか、手動でプロキシサーバを設定してください。
- ・SSL Access Controller をインストールした PC では、[インターネットのプロパティ] の [ローカルエリアネットワークの設定] でプロキシサーバの設定を変更しても、再起動時に元の設定に戻ります。プロキシサーバの設定を変更する場合は、sacproxy.ini の編集が必要になります。

4-3. SSL Access Controller のアンインストール

クライアント PC から SSL Access Controller をアンインストールする手順について説明します。アンインストールには、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。

注意： ・アンインストール後、OS の再起動が必要です。

・SSL Access Controller をアンインストールする前に、すべてのアプリケーションを終了してください。

1. アンインストールを実行するクライアント PC 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→[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. 「SSL Access Controller」を選択して [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. [はい] ボタンをクリックします。
アンインストールが開始されます。
再起動を促すメッセージが表示されます。
5. [はい] ボタンをクリックします。
Windows が再起動します。

以上で、SSL Access Controller のアンインストールは完了です。

アンインストールが完了すると、Internet Explorer のプロキシサーバの設定が SSL Access Controller をインストールする前の設定に戻ります。

注意： 自動構成スクリプトを使用している場合、SSL Access Controller をアンインストールしてもプロキシサーバの設定は変更されません。

MEMO

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： UNIX 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。

■ 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。

- amsuser
- amsip
- amsexuser
- amsurl
- amsrule
- amsschedule
- amslog
- amscatmsg

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。
グループは 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「"」（ダブルクォーテーション）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。

2008-01-23 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	マスタ サーバ	スレーブ サーバ	参照 ページ
amsuser	-add	アカウントの管理	○	×	350 ページ
	-del		○	×	
	-mod		○	×	
	-export		○	×	
amsip	-add	IP アドレスユーザの管理	○	×	353 ページ
	-del		○	×	
	-mod		○	×	
	-export		○	×	
amsexuser	-export	例外ユーザの管理	○	×	356 ページ
	-set		○	×	
	-unset		○	×	
amsgroup	-add	グループ管理	○	×	359 ページ
	-del		○	×	
	-mod		○	×	
	-export		○	×	
amsurl	-export	例外 URL 設定	○	×	363 ページ
	-import		○	×	
amsrule	-create	フィルタリングルール管理	○	×	366 ページ
	-mod		○	×	
	-del		○	×	
	-export		○	×	
	-standard		○	×	

コマンド	オプション	実行される内容	マスタ サーバ	スレーブ サーバ	参照 ページ
amsschedule	-add	スケジュール管理	○	×	371 ページ
	-del		○	×	
	-mod		○	×	
	-export		○	×	
amsdatabase	-download	URL データベースの管理	○	×	376 ページ
	-info		○	×	
	-status		○	×	
amsdata	-save	設定の保存 / 復旧 / 同期	○	×	378 ページ
	-restore		○	×	
	-list		○	×	
	-del		○	×	
	-synchronize		○	×	
	-retry		○	×	
	-sys		○	×	
	-reload		○	×	
amsserver	-	サーバ情報の表示	○	×	382 ページ
amslog	-rotation	ログファイルのアーカイブ作成	○	○	384 ページ
	-list		○	×	
amscatmsg	-mod	カテゴリ別メッセージの変更 / 出力	○	×	387 ページ
	-export		○	×	
amscontrol	-start	フィルタリングサービスの起動と 停止	○	○	389 ページ
	-stop		○	○	
	-restart		○	○	
amsadminstat	-status	スレーブサーバの状態管理	×	○	391 ページ
	-reset		×	○	
amsversion	-	バージョン情報の表示	○	○	392 ページ

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

amsrdr : リダイレクタ起動シェル (Squid 版だけ)

A-4. amsuser [アカウントの管理]

amsuser コマンドは、アカウントの追加 / 削除 / 設定変更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、351ページの「ユーザ情報ファイルのフォーマット」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]

`amsuser -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3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]

`amsuser -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]

`amsuser -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。

■ ユーザ情報の出力 [-export]

```
amsuser -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、登録されているユーザー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、345 ページの「グループ記述ファイル」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。

■ ユーザ情報ファイルのフォーマット

amsuser 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

ユーザ名	パスワード	グループ名	e-mail アドレス	グループ管理者	AMV 閲覧権限

・出力例

"user1",	"password1",	" ネットスター ¥ 営業 ",	"user1@netstr-inc.com",	"1",	"1"

フィールド名	設定内容
ユーザ名	ユーザ名を入力します。
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。
e-mail 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。
グループ管理者	0: エンドユーザの場合 1: グループ管理者の場合
AMV 閲覧権限	0:AMV 閲覧権限なし 1:AMV 閲覧権限あり

-
- 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「'''（ダブルクォーテーション）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。
-

■ 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、マスタサーバとスレーブ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、346 ページの「A-2. amsserror.log について」を参照してください。

■ 終了コード

amsuser 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 (Solaris/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、354ページの「IPアドレスユーザ情報ファイルのフォーマット」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、345 ページの「グループ記述ファイル」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	IP アドレス (開始)	IP アドレス (終了)

・出力例

"ネットスター¥営業",	"192.168.1.10",	"192.168.1.25",

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slash）で区切って入力します。
IP アドレス (開始)	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。
IP アドレス (終了)	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には、入力する必要はありません。

-
- 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「'''（ダブルクォーテーション）で囲み、フィールド同士は「,」（半角カンマ）で区切ります。
 - ・データの無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ません。
 - ・IP アドレスを範囲指定する場合には、「IP アドレス（終了）」よりも「IP アドレス（開始）」の値の方が小さくなるように設定してください。
-

■ 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。マスタサーバとスレーブ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 (Solaris/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. amsexuser [例外ユーザの管理]

amsexuser は、例外ユーザの追加、解除、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、357ページの「例外ユーザ情報ファイルのフォーマット」を参照してください。

-
- 注意：**
- ・管理画面では例外ユーザの「規制メッセージ」と「ブラウザ規制」が設定できますが、amsexuser コマンドでは指定できません。
amsexuser で登録した例外ユーザの場合は常に、規制メッセージなし、ブラウザ規制なしとして登録されます。登録後に管理画面で変更してください。
 - ・-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。
-

■ 例外ユーザ情報の出力 [-export]

`amsexuser -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ユーザ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、グループ記述ファイルに記述されたグループの例外ユーザ情報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、345 ページの「グループ記述ファイル」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。
-

■ 例外ユーザの設定 [-set]

`amsexuser -set ファイル名 [-ip] -encoding EUC|SJIS|UTF 8`

指定されたファイルに記述されているユーザを例外ユーザにします。

-
- 注意：** ユーザ名が IP アドレスで記述されている場合、-ip オプションを指定します。
-

■ 例外ユーザの解除 [-unset]

```
amsexuser -unset ファイル名 [-ip] -encoding EUC|SJIS|UTF8
```

指定されたファイルに記述されているユーザを例外ユーザから除外します。

- 注意：**
- ・ユーザ名が IP アドレスで記述されている場合、**-ip** オプションを指定します。
 - ・グループ名とユーザが完全に一致する場合だけ例外ユーザから除外されます。

■ 例外ユーザ情報ファイルのフォーマット

amsexuser コマンドで入出力する例外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	ユーザ名	終了 IP アドレス	スケジュール名	IP リクエスト 拒否	書込規制	オーバーライド	オーバーライド パスワード	オーバーライド タイマー

・出力例

"LDAP",	"netusr",	,	"daytime",	"0",	"1",	"1",	"pass",	"300"

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。
ユーザ名	ユーザをアカウント名、または IP アドレスで入力します。 ユーザを IP アドレス範囲で指定する場合、開始 IP アドレスを入力します。
終了 IP アドレス	ユーザを IP アドレス範囲で指定する場合に入力します。 ユーザ名をアカウント名、または単一の IP アドレスで指定する場合は入力する必要はありません。
スケジュール名	適用するスケジュール名を入力します。
IP アドレスリクエスト拒否	IP アドレス形式のリクエストの拒否を設定します。 0: 無効 1: 有効

フィールド名	設定内容
書き込み規制 (規制オプション)	有効に設定すると、すべての URL で書き込みが規制されます。 0: 無効 1: 有効
オーバーライド (規制オプション)	有効に設定すると、規制対象カテゴリの URL にオーバーライドが適用されます。 0: 無効 1: 有効
オーバーライドパスワード	オーバーライド解除用のパスワードを指定します。 オーバーライドを使用しない場合、入力する必要はありません。
オーバーライドタイマー	オーバーライドの有効時間を指定します。 オーバーライドを使用しない場合、入力する必要はありません。

- 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「"」（ダブルクォーテーション）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。

■ エラー処理

amsexuser コマンドは、追加および解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。

マスタサーバとスレーブ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

amsexuser コマンドは終了時に、以下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 (Solaris/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-7. 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、360ページの「グループ情報ファイルのフォーマット」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	グループコメント	IP アドレス リクエスト拒否	書き込み規制	上位グループ参照	下位グループ指定	オーバーライド	オーバーライド タイマー
オーバーライド パスワード	例外 URL 送信	例外 URL 参照指定	グループ ID	書き込み規制サイズ	マルチパート リクエスト規制		

・出力例

" ネットスター ¥ 開発 ",	" コメント ",	" 1 ",	" 1 ",	" 1 ",	" 0 ",	" 1 ",	" 300 ",
" password ",	" 0 ",	" 0 ",	" 3 ",	" 50 ",	" 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。
グループコメント	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。
IP アドレスリクエスト拒否	IP アドレス形式のリクエストの拒否を設定します。 0: 無効 1: 有効
書き込み規制 (規制オプション)	有効に設定すると、すべての URL で書き込みが規制されます。 0: 無効 1: 有効
上位グループ参照	0: 無効 1: 有効
下位グループ指定	0: 無効 1: 有効
オーバーライド (規制オプション)	有効に設定すると、規制対象カテゴリの URL にオーバーライドが適用されます。 0: 無効 1: 有効
オーバーライドタイマー	オーバーライドの有効時間を指定します。 オーバーライドを使用しない場合、入力する必要はありません。
オーバーライドパスワード	オーバーライド解除用のパスワードを入力します。 オーバーライドを使用しない場合、入力する必要はありません。

フィールド名	設定内容
例外 URL 送信	0: 無効 1: 有効
例外 URL 参照設定	0: 無効 1: 有効
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。
書き込み規制サイズ	数値を入力すると、入力した数値 (byte 単位) を超える POST リクエストが規制されます。
マルチパートリクエスト規制	0: 無効 1: 有効

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「"」(ダブルクォーテーション) で囲み、フィールド同士は「,」(半角カンマ) で区切ります。
- ・データの無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。

■ 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。

マスターサーバとスレーブサーバの通信エラーや、その他のエラーが起きた場合は、amserver.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 (Solaris/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. amsurl [例外 URL]

amsurl は、例外 URL の入出力をするコマンドです。

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、364 ページの「例外 URL 情報ファイルのフォーマット」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、345 ページの「グループ記述ファイル」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または -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、すべてのデータを入れ替えます。このとき、既に登録されている例外 URL はすべて削除されます。

- 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、345 ページの「グループ記述ファイル」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 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	メインカテゴリ名	サブカテゴリ名	例外 URL

・出力形式

" ネットスター ¥ 開発 ",	" スポーツ ",	" レジャー ",	"http://sports.netstar.jp"

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slash）で区切って入力します。
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。

-
- 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「"」（ダブルクォーテーション）で囲み、フィールド同士は「,」（半角カンマ）で区切ります。
 - ・データの無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。
-

■ 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。

マスタサーバとスレーブ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 (Solaris/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. amsrule [フィルタリングルール管理]

amsrule は、フィルタリングルール追加、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、368ページの「フィルタリングルールファイルのフォーマット」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]

```
amsrule -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、最低基準設定が「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]

```
amsrule -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最低基準設定を変更します。
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最低基準設定を変更します。グループ内に既に最低基準ルールがある場合は、最低基準は変更できません。

■ ルールの削除 [-del]

```
amsrule -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]

```
amsrule -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フィルタリングルールファイルを指定すると、該当するグループのフィルタリング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、345 ページの「グループ記述ファイル」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。
-

■ 最低基準設定の変更 [-standard]

```
amsrule -standard ファイル名 true|false -encoding EUC|SJIS|UTF8
```

指定したファイルの最低基準設定を変更します。

true が指定された場合には、指定されたファイルに記述されたルールを最低基準ルールとし、既に設定されている場合は解除します。**false** が指定された場合には、最低基準ルールを解除します。

■ フィルタリングルールファイルのフォーマット

amsrule 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。
規制内容	0: 許可 1: 規制 2: オーバーライド 3: 書き込み規制

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「"」（ダブルクォーテーション）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ません。
- ・[システム管理] → [フィルタリングルール共通設定] の [■ カテゴリ設定] で、サブカテゴリ「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。

新しいフィルタリング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. amsrule -create で指定したグループにフィルタリングルールを追加します。
2. amsrule -export で作成したフィルタリング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. `amsrule -mod` でフィルタリングルールを変更します。

● フィルタリングルールの作成例

「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. 「amsrule -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。

```
amsrule -create C:¥ISWM¥addrule-group.txt -encoding SJIS
```

注意：

- `amsrule -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. 「amsrule -export」を実行し、作成したフィルタリング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。

```
amsrule -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、すべてのフィルタリング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 , 規制方法
"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. 「amsrule -mod」を実行し、フィルタリングルールを変更します。
手順 3 で修正したファイルを指定して、フィルタリングルールを変更します。

```
amsrule -mod C:\ISWM\rule-dev.txt -encoding SJIS
```

■ エラー処理

amsrule 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。
マスタサーバとスレーブ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

amsrule 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 (Solaris/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. amsschedule [スケジュール管理]

amsschedule は、フィルタリング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、372ページの「スケジュール情報ファイルのフォーマット」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既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登録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、345 ページの「グループ記述ファイル」を参照してください。
 - ・エクスポートした時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	デフォルト 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",	"勤務時間外",	"0",	"MON/TUE/WED",	"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。

フィールド名	設定内容
デフォルトスケジュール指定	デフォルトスケジュールに指定する、指定しないを設定します。 デフォルト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: デフォルトスケジュールに指定しない 1: デフォルト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「"」（ダブルクォーテーション）で囲み、フィールド同士は「,」（半角カンマ）で区切ります。
- ・データの無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。

● 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) グループ適用スケジュール「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) 例外ユーザ用スケジュール「管理者用」を追加します。

注意： グループ適用スケジュールと異なるスケジュール名の設定は、例外ユーザ用スケジュールとして登録されます。

```
グループ名,スケジュール名,ルール所有グループ名,ルール名,デフォルトスケジュール指定,
曜日,開始時刻,終了時刻
"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。

マスタサーバとスレーブ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 (Solaris/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-11. 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 [-target サーバ番号 | -all]

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 [-target サーバ番号 | -all]

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。マスタサーバは常に 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)

```
スレーブサーバ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 [-target サーバ番号 | -all]
```

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)

```
マスタサーバ      (0)  Downloading
スレーブサーバ1    (1)  ----
スレーブサーバ2    (2)  ----
```

■ エラー処理

マスタサーバとスレーブ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 (Solaris/Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-12. 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。

■ システム設定の保存 [-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システム情報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 つ以上のシステム情報を保存することはできません。既に 5 つのシステム情報が保存されている場合は、不要なシステム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。
 - ・システム設定の保存中は、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。
-

■ システム設定の復旧 [-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：**
- ・システム設定の復旧中は、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、マスタサーバおよびスレーブ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。また、Squid 版の場合は、Squid も再起動してください。
-

■ システム設定の一覧表示 [-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
$
```

■ システム設定の削除 [-del]

```
amsdata -del ファイル名
```

指定したシステム情報を削除します。

■ システム設定の同期 [-synchronize]

```
amsdata -synchronize [-target サーバ番号]
```

現在のマスタサーバの設定を保存し、スレーブ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：**
- サーバ番号としてマスタ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。
 - システム設定の同期中は、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、マスタサーバおよびスレーブ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。また、Squid 版の場合は、Squid も再起動してください。
-

■ コマンドの再送 [-retry]

```
amsdata -retry
```

管理画面やコマンドラインからスレーブ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スレーブサーバに再送し、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、マスタサーバおよびスレーブ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。また、Squid 版の場合は、Squid も再起動してください。

■ システム情報の再読み込み [-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 ファイルなどのシステム情報を読み込み、再設定します。

このコマンドを実行すると、マスタサーバおよびすべてのスレーブサーバでシステム情報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。
- ・ マスタサーバとスレーブサーバ間の同期は行いません。

■ エラー処理

マスタサーバとスレーブ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 (Solaris/Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-13. 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	マスタサーバ、スレーブ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。マスタサーバは常に 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。マスタサーバの場合、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	マスタサーバと同期中 :synchronized マスタサーバとの同期に失敗 :failed
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 マスタサーバ (Master) build0611 192.168.60.1 ---- running
1 スレーブサーバ1 192.168.60.2 failed starting
2 スレーブサーバ2 192.168.60.3 failed running
3 スレーブサーバ3 192.168.60.4 failed running
4 スレーブサーバ3 192.168.60.5 failed stop
```

■ エラー処理

マスタサーバとスレーブサーバの通信エラーや、その他のエラーが起きた場合は、amsserror.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 (Solaris/Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-14. 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 コマンドはスレーブサーバでも実行できます。ただし、-list パラメータはマスタ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

```
マスタサーバ, 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 パラメータはマスタサーバだけが実行できます。

- **-target パラメータを指定した場合**

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。

■ エラー処理

マスタサーバとスレーブ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 (Solaris/Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-15. amscatmsg [カテゴリ別規制メッセージ管理]

amscatmsg コマンド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、388ページの「カテゴリ別規制メッセージファイルのフォーマット」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]

```
amscatmsg -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]

```
amscatmsg -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、345 ページの「グループ記述ファイル」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	メインカテゴリ名	規制メッセージ

・出力形式

"ネットスター¥開発",	"アダルト",	"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。
メインカテゴリ名	メイン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。

■ 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、マスタサーバやスレーブ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、346 ページの「A-2. amSError.log について」を参照してください。

■ 終了コード

amsg 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 (Solaris/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-16. amsscontrol [フィルタリングサービスの起動/停止]

amsscontrol 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： amsscontrol コマンドはスレーブサーバでも実行できます。ただし、-target パラメータはマスタ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]

```
amsscontrol -start [-target サーバ番号 | -all]
```

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]

```
amsscontrol -stop [-target サーバ番号 | -all]
```

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]

```
amsscontrol -restart [-target サーバ番号 | -all]
```

フィルタリングサービスを再起動します。

■ エラー処理

マスタサーバとスレーブサーバの通信エラーや、その他のエラーが起きた場合は、amsserror.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 (Solaris/Linux)
正常終了	0	0
内部エラー	-2	254
受付拒否	-9	247

A-17. amsadminstat [スレーブサーバの状態管理]

amsadminstat は、スレーブサーバの状態表示、初期化をするコマンドです。

■ スレーブサーバの状態表示 [-status]

```
amsadminstat -status
```

コマンドを実行したスレーブサーバが特定のマスターサーバと連携されているかを表示します。
このコマンドはスレーブ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	スレーブ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。 マスターサーバと連携されていない場合は -1 と表示されます。
マスターサーバの IP アドレス	連携しているマスターサーバの IP アドレスが表示されます。 マスター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。
マスターサーバとの連携状態	standalone : 新規インストールされた後マスタ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マスタ管理サービスから登録されていない状態 managed : マスタ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
```

■ マスタサーバとの連携を初期化 [-reset]

```
amsadminstat -reset
```

マスタサーバとの連携を初期化します。

マスタサーバとの連携を初期化したスレーブサーバは、amsadminstat -status コマンドを実行して表示されるマスタサーバとの連携状態が「managed」から「standalone」へかわります。

マスタサーバとの連携中は、他のマスタ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、新しいマスタサーバとの連携のためリクエストを待ちます。

注意： ・このコマンドはマスタサーバとの連携状態が「managed」である場合のみ実行可能です。

・マスタ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、スレーブサーバ側で「managed」の状態にすることはできません。

もう一度マスタ管理サービスで管理対象のスレーブサーバを追加してください。

A-18. 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。

■ 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、51 ページの「8. サービスの起動と停止」を参照してください。

■ 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。
以下のディレクトリに保存されます。

Windows の場合	<インストールディレクトリ>%conf%
Solaris/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、マスタサーバおよびスレーブ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。また、Squid版の場合は、Squid も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。以下のディレクトリに保存されます。

Windows の場合	<インストールディレクトリ>%conf%
Solaris/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。

スレーブ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スレーブ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、すべてのスレーブ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。

● sacproxy.ini

SSL Access Controller インストール時に設定が必要な項目の設定値を、あらかじめ指定するためのファイルです。ISWM の CD-ROM の「program\sac」に格納されています。

本ファイルで ISWM の IP アドレスとポート、およびローカルプロキシのポートを設定し、「sac_setup.exe」と同じフォルダに格納してインストールを開始することで、インストール中の入力を省略できます。

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、以下のディレクトリに保存されます。

%Program Files%\Trend Micro\SSL Access Controller

B-1. 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	・ マスタ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。 ・ スレーブサーバに通知するマスタサーバの IP アドレス名。 IP アドレスを変更した場合は、既に追加済みのスレーブ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 =3219	管理画面の待ち受けポート番号。
MAX_DATA_SYNC_THREAD =10	マスタ管理サービスからスレーブ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。 この値が実際のスレーブ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	マスタ管理サービスからスレーブ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=640	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。384MB ～ 2048 MB まで設定可能。ただし、使用する OS によって、設定できる最大値が異なる。
EFFECTIVE_USER=root	ファイルのオーナー、実行ユーザを設定する。
EFFECTIVE_GROUP=root	ファイルのグループ、実行グループを設定する。

■ [CONNECTION_CFG]

BUFF=2048	Web サーバおよび HTTP クライアント (ICAP クライアント) との通信時、1 度取得するデータの最大サイズ。 1024 バイト ~ 65535 バイト まで設定可能。 サイズを増減することにより、以下のメリット、デメリットが発生する。 増加: サイズの大きなファイルをリクエストした場合、データを細かく切らずに受信できる。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。 減少: サイズの大きなファイルをリクエストした場合、データを細かく切って受信する。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。 ただし、データ転送サイズが大きい場合は、処理回数が増加するため、転送時間が増加する。 上限値を超えた場合、または 1024 以下の値が指定されている場合はデフォルト値 (2048) が適用される。
BACKLOG=75	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	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おこない、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	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	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）ヘリクエストヘッダ情報を送信の有無を設定する。 0: 上位プロキシがある時は転送。 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。 • REQUESTMODE=0 の場合（上位サーバ指定あり） Proxy-Authorization ヘッダは上位に転送し、以下のヘッダも追加される。 Remote-Host: X-Forwarded-For: Forwarded: Proxy-Agent: Via: • REQUESTMODE=1 の場合 Proxy-Authorization ヘッダは上位に転送しない。 他のヘッダは追加しない。 • REQUESTMODE=2 の場合 Proxy-Authorization ヘッダは上位に転送する。 以下のヘッダが追加される。 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:

TRANSFER_VERSION=0	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。

■ [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_sys.log" "netstar_adm.log" "netstar_http.log" "netstar_amsrdr.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。 1MB ～ 2048MB 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 アドレスから、ホスト名を出力するかを設定する。 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	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,Blocked,Allowed,Release,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。
LOG_OUT_COLUMNS (スタンドアロン版) =group,user,error_code, data_transfer_size, mime_type (Squid版、ICAP版) =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): Squid版では非表示 destination-ip (WWWサーバIP): 共通 error_code (エラーコード): ICAP版、Squid版では非表示 data_transfer_size (転送データサイズ): ICAP版、Squid版では非表示 mime_type (ファイルタイプ): 共通 method (HTTPメソッド名): 共通 http_version (HTTPバージョン): Squid版では非表示 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。 最大値は「2147483647」。0の場合には、書き込まれない。
LOG_ROTATE=0	ログのローテーションタイミंगを設定する。 0: proxy.infのLOG_MAXで設定したサイズを超える時、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。

■ [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。 Squid 版だけ使用される。391 バイトまで設定可能。
BLOCK_HTTPS_URL =https://iswm.netstar-inc.com	規制後の転送先 SSLWeb サーバを設定する。 Squid 版だけ使用される。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。 スタンドアロン版、ICAP 版の場合 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。 Squid 版の場合 1: リクエストしたサイトが、HTTP または FTP なら、proxy.inf の BLOCK_URL で指定した Web サーバへ転送する。HTTPS なら、proxy.inf の BLOCK_HTTPS_URL で指定した Web サーバへ転送する。 2: proxy.inf の [CONTROL_CFG] BLOCK_FILE_SERVER、BLOCK_FILE_PORT で指定した内部リダイレクト先へ転送する。 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 [CONTROL_CFG] BLOCK_FILE_SERVER、BLOCK_FILE_PORT で指定した内部リダイレクト先へ転送する。 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	オーバーライドの動作切り替えフラグ。管理画面からの編集は不可。TRUE に設定した場合、メモリ使用量が増加するため、十分なヒープの割り当てが必要。 TRUE: カテゴリごとのオーバーライド実施を可能にする。 FALSE: オーバーライドを実行するとオーバーライド中は他のオーバーライド指定のカテゴリも閲覧可能となる (ISWM 3.5 までの動作と同じ)。
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。

BLOCK_HTTPS_PATH=FALSE	ドメイン以下のディレクトリを指定した、パス付き HTTPS サイトへのアクセス規制を設定する。 TRUE: パス付き HTTPS サイトを規制する。 FALSE: パス付き HTTPS サイトを規制しない。
X_NS_HTTPS_URL=0	BLOCK_HTTPS_PATH が TRUE の場合、専用モジュールである SSL Access Controller 以外からのアクセスの規制を設定する。 0: SSL Access Controller 以外からのアクセスを規制しない。 1: SSL Access Controller 以外からのアクセスを規制する。
PROXIED_USER_AGENT=InterScanWebManager,Windows Update,Industry Update Control,Service Pack Setup,EndPointModule,Microsoft WU Client,Microsoft BITS,Windows-Update-Agent,Windows Installer,Microsoft-CryptoAPI	X_NS_HTTPS_URL が 1 の場合、HTTPS 通信のアクセス規制対象から除外する User-Agent を設定する。
PUA_SEPARATOR=,	PROXIED_USER_AGENT の区切り文字。

■ [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_EX_GUSER=30	第 1 階層グループごとに登録できる例外ユーザ数の上限値。
MAX_G_SCHEDULE=20	第 1 階層グループごとに登録できるスケジュール数の上限値。
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。

■ [PROXY_PORT]

HTTP=8080,150	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 :8080,150) 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=8443,75	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 :8443,75) 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=8021,75	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 :8021,75) 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。

■ [UP_SERVER]

HTTP=:80	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) 上位プロキシ指定が無い場合は、":80"と指定する。 ポート番号は、1 ～ 65535 まで設定可能。
HTTPS=:80	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) 上位プロキシ指定が無い場合は、":80"と指定する。 ポート番号は、1 ～ 65535 まで設定可能。
FTP_OVER_HTTP=:80	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) 上位プロキシ指定が無い場合は、":80"と指定する。 ポート番号は、1 ～ 65535 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 =FALSE	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は、1 日 8 回 3 時間ごとに DB を自動ダウンロードする。 ダウンロードは、1:00、4:00、7:00、10:00、13:00、16:00、19:00、22:00 から 1 時間以内に行われる。下記の 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) 指定が無い場合は、":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。
AUTO_PRG_UPDATE =FALSE	プログラムダウンロード処理を自動で行う / 行わないの設定値。 TRUE: 行う FALSE: 行わない
DB_ALIAS=db60	データベースダウンロード用エイリアス

REQUEST_PROTOCOL =http://	DB サーバ～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	第 1 階層グループ毎のアカウント管理を行うフラグ。 TRUE: 第 1 階層グループ毎のアカウント管理を行う。 FALSE: 第 1 階層グループ毎のアカウント管理を行わない。
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 =TRUE (Squid 版、ICAP 版) =FALSE (スタンドアロン版)	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 =TRUE (Squid 版) =FALSE (スタンドアロン版、ICAP 版)	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	マスタ管理者、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： 全ての 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。管理画面での編集は不可。 値が”ALL”の場合： 全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。 proxy.inf に HTTP_ACCESS_PORT が存在しない場合、443 番ポートが設定される。

AUTHORIZED_USER_AGENT =Windows-Update-Agent, Microsoft BITS, EndPointModule, Windows Installer, Microsoft-CryptoAPI	特定の User-Agent を含むリクエストを、特例としてルートグループのユーザでフィルタリングを行う。 Windows Update やアプリケーションの自動アップデートなど、下位グループでのフィルタリングの設定を意図的に無視したい場合に使用する。 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。

■ [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を設定する。 1 文字 ~ 32 文字 まで設定可能。

■ [SERVICE_OBSERVE]

INTERVAL=60	マスタサーバ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	マスタサーバ管理サービスがスレーブサーバ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	マスタサーバ管理サービスが、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	マスタサーバ管理サービスが、スレーブサーバ管理サービスの状態を確認するときのリトライ回数。

■ [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) との連携をとる。 FALSE: LDAP (認証サーバ) との連携をとらない。
SCHEMA_LIST =ou,cn,name,dc,sn, givenName,uid,o, sAMAccountName	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。

■ [CONTROL_CFG]

SERVER = コントロールサーバの IP アドレス (Squid 版) =127.0.0.1 (スタンドアロン版、ICAP 版)	リダイレクタが接続するコントロールサーバの IP アドレス。 Squid 版のみの設定項目。管理画面による編集は不可。
PORT =53556 (Squid 版、スタンドアロン版) =1344 (ICAP 版)	Squid のリダイレクタまたは 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。Squid 版、ICAP 版だけの設定項目。 1 ～ 65535 まで設定可能。
SERVER_TIMEOUT =10000 (Squid 版、スタンドアロン版) =300000 (ICAP 版)	タイムアウトするまでの値を設定。 Squid 版、ICAP 版だけの設定項目。 1 ミリ秒～ 1,000,000 ミリ秒まで設定可能。 Squid 版の場合：Squid が規制画面を表示するときに利用する read timeout 値に利用する。 ICAP 版の場合：コントロールサーバがリダイレクタなどと通信を行う際、用いるタイムアウト値。
SERVER_PROCESS=150	Squid のリダイレクタまたは 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働させるプロセス数を設定する。 Squid 版、ICAP 版だけの設定項目 1 ～ 9999 まで設定可能。
CONNECT_RETRY=10	リダイレクタが、コントロールサーバと通信が確立できなかった際、再接続までに受けたリクエストをスルーする回数。 0 を設定した場合、通信が確立できなかった時、規制する。 1 以上を設定した場合、通信が確立できなかった時、規制しない。 管理画面では設定不可。
BLOCK_FILE_PORT=21128	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	proxy.inf の BLOCK_FILE_PORT で設定したポート番号で稼働するプロセスの最大数。 1 ～ 9999 まで設定可能。

BLOCK_FILE_SERVER = コントロールサーバの IP アドレス (Squid 版) =127.0.0.1 (スタンドアロン版、 ICAP 版)	リダイレクタが、規制サイトからリダイレクト (転送) させる、コン トロールサーバの IP アドレス。Squid 版だけの設定項目。 管理画面では設定不可。

B-2. 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

記述例)
20080101,TUE
20080509,FRI

B-3. sacproxy.ini

ISWM の IP アドレスとポート、およびローカルプロキシのポートを設定します。

Server	RelayHost	ISWM (またはプロキシサーバ) の IP アドレスを指定 する。(例 : 192.168.0.1)
	RelayPort	ISWM (またはプロキシサーバ) のプロキシサービ スのポート番号を指定する。 初期値 : 8080
LocalProxy	LocalPort	ローカルプロキシの待ち受けポート番号を指定す る。 初期値 : 18081

C. ICAP クライアントでの NTLM 認証

NetCache/BlueCoat 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、NetCache/BlueCoat 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。

NetCache/BlueCoat 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) に含まれる情報をもとに、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、NetCache/BlueCoat 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。

ファイルの保存場所

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

ICAP_AUTHENTICATION=TRUE キーを追加することにより、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：

- ・ proxy.inf ファイルに ICAP_AUTHENTICATION キーが無い場合や 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。
- ・ 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。

2. 管理画面から [システム設定]→[認証設定] を開き、[LDAP 認証] をクリックして [更新] ボタンをクリックします。
3. [LDAP 連携設定へ] ボタンをクリックし、NetCache/BlueCoat で指定している Active Directory を指定します。
4. [LDAP 同期設定へ] ボタンをクリックし、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。
5. <インストールディレクトリ>/conf/proxy.inf にて、以下の設定項目の「FALSE」を「TRUE」に変更します。

[CONTROL_CFG]

「ICAP_AUTHENTICATION=FALSE」

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 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、NetCache/BlueCoat 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。
-

6. マスタサーバおよびスレーブサーバのフィルタリングサービスを再起動します。

D. 利用するポート

ISWM は、管理画面サービスやマスタサーバ、スレーブ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。

マスタとスレーブ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。

管理サービス用ポートは、管理画面の [システム管理]→[画面設定] の [■管理画面情報] 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、マスタサーバおよびスレーブ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。また、Squid版の場合は、Squid も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	変更できません※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
管理画面、LogLyzer 用ポート※1	[SYSTEM_GROBAL] 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
ICAP ポート (ICAP 版)※2	[CONTROL_CFG] PORT	1344
リダイレクタポート (Squid 版)※2	[CONTROL_CFG] PORT	53556

ポート名	設定箇所	ポート番号
HTTP 規制画面出力用ポート (ICAP 版 /Squid 版) ※3	[CONTROL_CFG] BLOCK_FILE_PORT	21128
HTTPS 規制画面出力用ポート (Squid 版)	変更できません	443
SSL Access Controller ローカルプロキシの待ち受けポート	sacproxy.ini の [Local Proxy] LocalPort	18081

※1 管理画面の [システム管理] → [画面設定] の [■管理画面情報] でも設定できます。

※2 管理画面の [システム管理] → [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 [システム管理] → [画面設定] の [■規制画面形式] でも設定できます。

※4 管理サービス用ポートは、proxy.inf の [SYSTEM_GROBAL] 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した値になります。

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。

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
```

・ Solaris / 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

<http://java.sun.com/javase/ja/6/docs/ja/technotes/tools/windows/keytool.html>

Solaris / Linux の場合

<http://java.sun.com/javase/ja/6/docs/ja/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)
- ・ 州名または地方名 (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
 <インストールディレクトリ>%tomcat%.keystore
- Solaris/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
 <インストールディレクトリ>%lib%server.xml.template.https
- Solaris/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="<インストールディレクトリ>%tomcat%.keystore"
 - Solaris / 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)

- Squid 版および 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. マスタ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。

- スレーブサーバを使用している場合、全スレーブ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。
マスタサーバ、全スレーブサーバのフィルタリングサービスは、管理画面の [システム管理] → [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。

マスタサーバの 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 プロトコルだけで管理画面を使用する場合、LogLyzer との連携はできません。
 - 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
 - <インストールディレクトリ >%tomcat%.keystore
 - <インストールディレクトリ >%lib%server.xml.template
 - Solaris/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. Squid 版で設定を変更する場合の注意事項

● Squid 版の管理画面で設定を変更する場合

Squid版の管理画面で次の項目を変更した場合は、Squid およびリダイレクタを再起動してください。

- [システム管理] → [サーバ設定] の [■フィルタリングサービス設定]
[リダイレクタ] - [ポート]
- [システム管理] → [画面設定] の [■規制画面形式]
[ポート]
[URL]
[SSL URL]
[ファイル]
[メッセージ]
- [システム管理] → [ログ設定] の [■共通設定]
[ファイル名]
[ローテーションサイズ]

● Squid 版の設定ファイル (proxy.inf) を変更する場合

proxy.inf で次のキーを変更した場合は、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、すべてのコントロール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。また、Squid およびリダイレクタも再起動してください。

[BLOCK_CFG]	BLOCK_URL
	BLOCK_HTTPS_URL
	BLOCK_MODE
[LOG_CFG]	LOG_FILE
	LOG_MAX
[CONTROL_CFG]	SERVER
	PORT
	BLOCK_FILE_PORT
	BLOCK_FILE_SERVER
	CONNECT_RETRY

●オフボックス環境で設定を変更する場合

コントロールサーバとリダイレクタを別サーバで運用するオフボックス環境の場合、管理画面または proxy.inf で、Squid およびリダイレクタの再起動が必要な設定を変更したときには、コントロールサーバの proxy.inf を、「Squid + リダイレクタ」側のサーバに手動でコピーしてください。

proxy.inf は、次の場所に格納されています。

- コントロールサーバ
 <インストールディレクトリ>/conf/
- Squid + リダイレクタ
 <インストールディレクトリ>/conf/

注意： FTP やネットワークの共有フォルダなどを使用して、コントロールサーバから、「Squid + リダイレクタ」側のサーバに proxy.inf をコピーしてください。
また、proxy.inf をコピーした後で、Squid を再起動してください。

G. 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、ISWM 5.0 (Service Pack 含む) がインストールされている場合、ISWM 6.0 にアップデートインストールを行います。

アップデートインストールでは、ISWM 5.0 の設定内容を ISWM 6.0 用にコンバートします。

- アップデートインストール (Windows 版)
- update mode (Solaris/Linux 版)

注意： ▪ ISWM 3.5 以前のバージョン からのアップデートインストールはできません。

- アップデートインストール時、ISWM 5.0 はアンインストールされます。
 - 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フォルダの update.log に保存されます。
-

■ バージョン 5.0 の設定ファイルをコンバートして、バージョン 6.0 をインストールする

ISWM 5.0 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 6.0 をインストールできます。

-
- 注意：** ▪ インストールタイプの選択画面で、ISWM 5.0 の設定ファイルのサーバタイプと異なる設定を選択した場合、警告画面が表示され、インストールできません。
- 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フォルダの update.log に保存されます。
-

● 設定が引き継がれる内容

ISWM 5.0 の次の設定が引き継がれます。

- 設定ファイル
コンバート処理後に ISWM 5.0 の設定ファイルを
<インストールディレクトリ>%backup%conf_v50_<コンバートした時刻> フォルダにバックアップします。
- ユーザ、グループ情報
- カテゴリ別ルール

- 書き込み規制サイズの設定
- スケジュール
- 例外 URL
- カテゴリ別規制メッセージ
- 規制画面の HTML

Service Pack が未適用の状態からアップグレードした場合、規制解除申請機能に対応した HTML ファイルは、
<インストールディレクトリ>\conf\block\offer.htm としてインストールされます。

■ Squid 版のバージョンアップインストールについて

- Squid 版の場合、Squid を停止しないでリダイレクタおよびコントロールサーバを上書きインストールすると、フィルタリングが正常に動作しなくなります。必ず Squid を停止してから、リダイレクタおよびコントロールサーバをインストールしてください。
- リダイレクタだけをバージョンアップした場合、コンバートが行われません。この場合には、コントロールサーバから手動で設定ファイルをコピーしてください。

英数字

あ

アカウントの変更	182	規制画面形式	84
[アクセス管理] 画面	317	規制メッセージ	271、327、329
アクセス マネジメント ビュー	301	クライアント規制	262、289
アクセスログ出力設定	90	グループ	149、151、157
アクセスログの管理	317	[グループ / ユーザ管理] 画面	162
アンインストール	53	グループ管理者	58、148、153
インストール	16、20、23、27	グループ記述ファイル	345
閲覧のみ許可	210、253	グループの一括削除	193
エンドユーザ	58、153	グループの一括登録	193
オーバーライドタイマー	271、330、358、360	グループの削除	170
オーバーライドパスワード	271、330、358、360	グループの設定の変更	170
オフボックスインストール	29	グループの登録	166
オンボックスインストール	28	現在のアクセスログ	318
		現在のシステムログ	96
		検索キーワード規制	271
		コマンドラインインタフェース	345
か			
下位グループの指定	152、213、224		
書き込みキーワード規制	271	さ	
書き込み規制サイズ	361	サーバの同期	65、77、382
書き込み (POST) 規制	137、208、271、332	サービス異常発生通知	103
拡張 Web サービス	51、52、54	最新モジュール情報通知	103
カテゴリ別規制メッセージ	168、277、283	最大ヒープサイズ	74
カテゴリ別ルールの登録	226	最低基準の設定	209、227、367
カテゴリ別ルールの変更、削除	231	サブグループ管理者	58、148、153
[簡易設定] 画面	295	[システム管理] 画面	65
管理画面	59、66、83	システム設定の同期	77
管理画面情報	83、413	システム設定の復旧	100
管理サービス	51、52、54、413	システム設定の保存	99
規制オプション	270、288	システム設定の保存 / 復旧	99、378
規制解除申請画面	87、328	システムログ一覧	93
規制解除申請機能	140	上位グループ参照	152、211
規制画面	66、83、326	上位プロキシサーバの設定	71、74、79

情報漏えいリスク確認対象	314	マルチパートリクエスト規制	271、361
情報漏えいリスクの確認	304	未登録ユーザ	154
情報漏えいリスク判定結果	306	メール通知	102
情報漏えいリスク判定方法	311	モジュールの自動アップデート	80
スケジュール	204、210、214、371	モジュールのダウンロード	66、78
スケジュール一覧	233		
スケジュールの登録	238、244	や	
スケジュールの変更	235、241、246	ユーザー一覧のファイル出力	190
スレーブサーバ	19、391	ユーザ情報の変更	182
スレーブサーバの登録	70	ユーザ認証	66、105
設定変更通知	103	ユーザの一括削除	193
		ユーザの一括登録	193
た		ユーザの移動	184
第一階層グループ毎のアカウント管理	109、161	ユーザの削除	187
データベースダウンロード開始時間	80	ユーザの登録	173、176
データベースのダウンロード	376		
		ら	
は		ライセンス期限切れ事前通知	66、103
バージョンアップインストール	421	リダイレクタ	27、50、203
パス内 URL 規制機能	292	利用するポート	413
パスワードの変更	333	ルートグループ	149
フィルタリングサービス	52、73、389	例外 URL	250、363
[フィルタリング設定] 画面	219	例外 URL の削除	260
フィルタリング設定の確認	279	例外 URL の登録	252
フィルタリング設定の参照	211	例外 URL の変更	258
ブラウザ規制	264、332	例外ユーザ	206、284、356
[ホーム] 画面	60	例外ユーザの登録	222、285
		例外ユーザの登録解除	290
ま		例外ユーザのフィルタリング設定	218、284
マスタ管理者	58、153	例外ユーザ用スケジュールの削除	248
マスタサーバ	19	例外ユーザ用スケジュールの登録	244
		例外ユーザ用スケジュールの変更	246

ローテーションサイズ	90
ローテート済みアクセスログ	321
ログファイル	89
ログファイルの出力設定	89
ログファイルのローテート	95
ローテート種別	90、95