Trend Micro InterScan WebManager™

クイックスタートガイド

TREND MICRO™

Securing Your Connected World

■ 著作権

■ マニュアルの構成

● クイックスタートガイド (本書)

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

管理者ガイドでは、Trend Micro InterScan WebManager で設定できるさまざまなフィルタリング機能の設定について詳しく説明しています。
また、Linux 版のシステム構築・設定、LDAP 認証サーバとの連携方法など大規模なシステムでの運用方法についても説明しています。
Trend Micro InterScan WebManager の運用形態に応じて、必要項目を参照してください。

■ マニュアルに掲載している画面

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

目次

ご使用になる前に

1. ISWMの概要

1-1. 製品構成

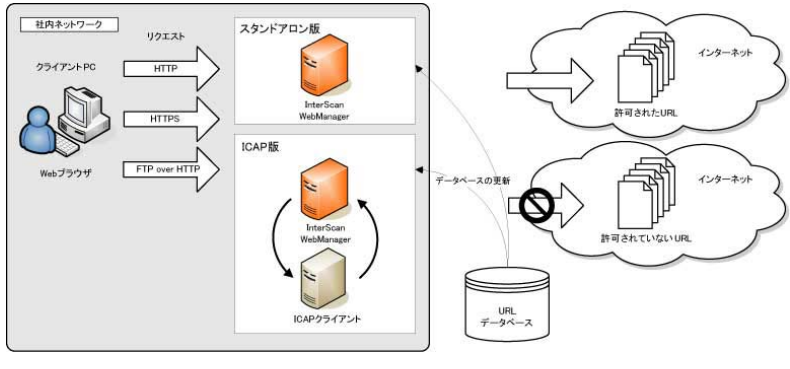
Trend Micro InterScan WebManager(以下、ISWM)は、プロキシやコントロールサーバの種類に応じて、以下の2種類の製品を用意しています。

製品名称	対応 OS	
	Windows	Linux
ISWM 9.1 スタンドアロン	○	○
ISWM 9.1 for ICAP	―	○

○:サポート　　―:未サポート

1-2. フィルタリングサービス

ISWMは、イントラネット内のクライアントPCと外部のWebとのフィルタリング機能を提供するサーバソフトウェアです。企業や学校などのイントラネットから有害サイトや業務に関係のないサイトへのアクセスを制限できます。URLのフィルタリングに使用するデータベースは、データセンターから差分を毎日ダウンロードして、最新の状態に保たれます。データベースの更新中もフィルタリングサービスを継続します。



フィルタリングサービスを利用するクライアントPCは、ブラウザでプロキシの設定を変更する必要があります。

ISWM	登録プロキシサーバ
ISWM 9.1 スタンドアロン	ISWM
ISWM 9.1 for ICAP	ICAPクライアント(BlueCoat、Squid、BIG-IP)

注意:
- ISWM 9.1 スタンドアロンでは、ファイアウォールやICAPクライアントとしてISWMの上位に他のプロキシサーバが存在する場合、そのサーバをプロキシに指定して中継することができます。その際、Keep-Alive(持続接続)に対応していないプロキシサーバであっても中継が可能です。
- ISWM 9.1 for ICAPはICAPクライアントとICAP(Internet Content Adaptation Protocol)にて連携します。ICAPクライアントは、ICAP 1.0以上をサポートしている必要があります。

■ 対応プロトコル

ISWMは、以下のプロトコルのリクエストを管理します。

HTTP(HyperText Transfer Protocol) : 一般的なWebページのプロトコル
HTTPS : SSL(Secure Socket Layer)で保護されたHTTP
FTP over HTTP : HTTP上のFTP(File Transfer Protocol)によるファイル転送

2. ISWMの特長

2-1. さまざまな環境に導入できる柔軟な製品構成

インストール可能なサーバOSとしてWindows、およびLinuxに対応します。
また、プロキシとして、ICAPで通信可能なICAPクライアントをご利用の環境にも対応します。
詳しくは、製品付属のReadmeおよび「1-1. 製品構成」(1ページ)を参照してください。

2-2. カテゴリ分類による高精度なURLデータベース

独自のノウハウにより、ニュース、スポーツなどのさまざまなカテゴリに URL を分類しました。フィルタリング設定時には、カテゴリごとに規制内容を設定するため、アクセスを規制したい分野を簡単に設定できます。カテゴリ分類は随時更新されているため、不適切なWebサイトを的確に規制できます。また、カテゴリに分類されないURLに対する規制内容と組み合わせることにより、すべてのURLに対してフィルタリングを適用できます。

2-3. 規制レベル

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

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

2-4. グループや曜日ごとに設定できるフィルタリング機能

カテゴリルールは、部門や職種など任意に作成したグループごとに、個別に設定することができます。
また、就業時間中、土日など時間帯ごとにカテゴリルールを設定して、使い分けることもできます。
複数のカテゴリルールを運用する場合に便利な「カテゴリ設定制限基準ルール」、「上位グループ参照」、「下位グループ強制参照」などの機能があります。

2-5. システムの運用を支援する簡易設定機能

フィルタリングサービスの開始に必要な最小限の設定を一括して実行できる、簡易設定機能が用意されています。簡易設定では以下の設定を一括で実行し、すぐに運用を開始できます。

- ライセンスキーの登録
- データベースのダウンロード
- カテゴリルールの選択(全ユーザ一括)

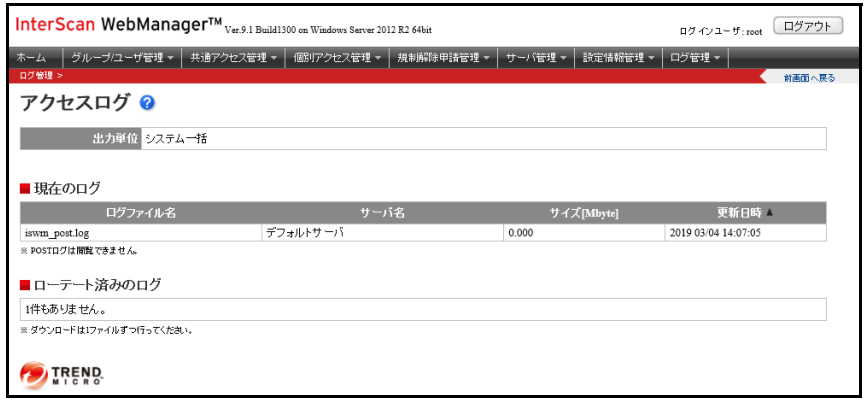
注意:
- ご利用になるネットワーク環境によっては、フィルタリングするプロトコルのポート番号、上位プロキシサーバも登録します。
- 簡易設定ではフィルタリングサービスを利用するすべてのユーザに一括して同一の、カテゴリルールを設定します。
  ユーザ別、グループ別に設定する場合は、「第5章 グループとユーザの登録」(49ページ)、「第6章 フィルタリングの設定」(71ページ)を参照してください。

2-6. システムの運用・管理を支援する機能

管理画面で利用できる便利な機能の一部を紹介します。

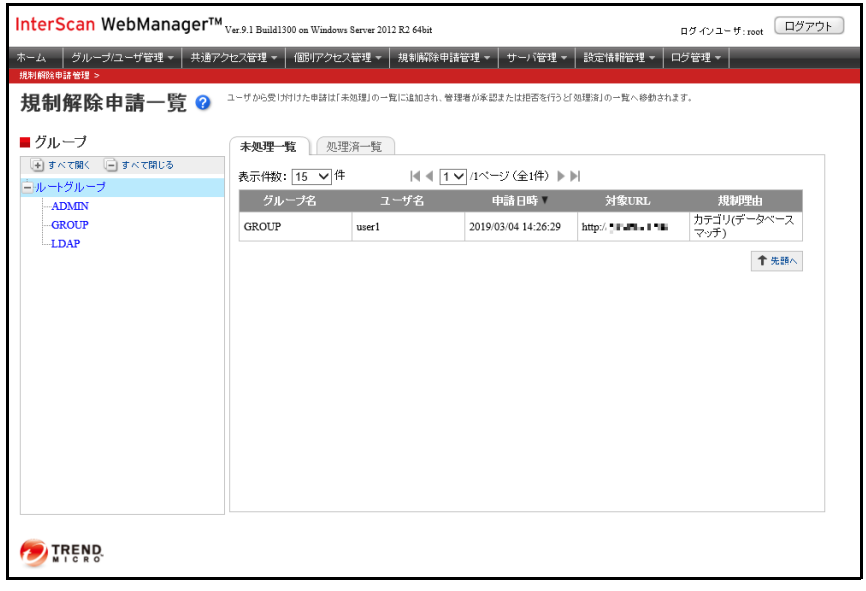
■ アクセスログの一覧表示機能

指定した範囲のアクセスログを管理画面上から確認する機能です。
サーバからログファイルをダウンロードしなくても、管理画面上で任意のアクセスログを表示できます。



■ 規制解除申請の管理機能

ユーザから送信された規制解除申請を未処理、処理済別に一覧表示します。規制解除申請の履歴を一元管理できます。また、未処理の規制解除申請に対して、管理画面で承認または拒否できます。
処理結果をユーザにメール通知することも可能です。



3. ライセンスについて

3-1. ライセンスの有効期限とユーザ数

ご購入いただいたISWMに同梱されているライセンス証書には、URLデータベースをダウンロード可能な期間(ライセンスの有効期限)と、利用可能なユーザ数としてクライアントライセンス数が記載されています。ライセンスの有効期限を過ぎると、URL データベースが消去され、サンプルのデータベースに切り替わります。
また、利用できるユーザ数は、ライセンス証書に記載されたユーザ数が上限となります。
有効期限は、管理画面の [サーバ管理]-[データベース設定] で確認できます。詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

3-2. 契約の更新

ご購入の製品は、契約期限となる前に契約更新をしていただくことで、引き続きご利用いただけます。
契約の更新については、製品をご購入いただいた販売代理店または弊社営業までお問い合わせください。
契約の期間が終了すると、データベースのダウンロードができなくなり、root ユーザ以外は管理画面にアクセスできなくなります。

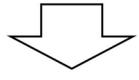
注意: 契約期間終了後にライセンスキーを更新する場合はrootユーザで管理画面にログインしてください。

4. システム運用までの流れ

ISWMの運用を開始するまでの流れを、1台のWindowsサーバで運用する場合を例に説明します。Linux サーバで ICAP 版をお使いになる場合や、複数のサーバで負荷分散して運用する場合は、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

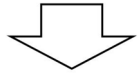
1. ISWMのインストール

フィルタリングサーバとして運用するサーバに、ISWMをインストールします。
詳しくは、「第2章 インストールと使用の準備」(11ページ)を参照してください。



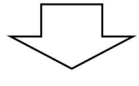
2. サーバの設定

フィルタリングサーバとして運用するために必要な各種の設定をします。
1台のサーバで基本的なフィルタリング機能だけで運用する場合は、簡易設定機能(「2-5. システムの運用を支援する簡易設定機能」(5ページ)参照)でライセンス認証やデータベースのダウンロードなど必要最小限の設定をして運用を開始できます。
詳しくは、「第4章 サーバの設定」(40ページ)を参照してください。



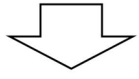
3. クライアントPCの設定

フィルタリングサービスを利用するクライアントPCの設定をします。
詳しくは、「4. クライアントPCの設定」(48ページ)を参照してください。



4. グループとユーザの登録

フィルタリングサービスを利用するユーザを、部門など任意の単位でグループ化します。ISWMは、作成したグループ/ユーザごとに、フィルタリングルールを適用できます。
すべてのユーザに同一のフィルタリングルールを適用して運用する場合、グループを作成する必要はありません。簡易設定機能(「2-5. システムの運用を支援する簡易設定機能」(5ページ)参照)をご利用ください。
詳しくは、「第5章 グループとユーザの登録」(49ページ)を参照してください。



5. フィルタリングの設定

共通アクセス管理で、すべてのグループ/ユーザに適用するフィルタリング設定をします。
個別アクセス管理で、グループ/ユーザに適用するフィルタリングルールを設定します。
詳しくは、「第6章 フィルタリングの設定」(71ページ)を参照してください。

注意: HTTPS 規制をサーバデコード方式で使用する場合、認証コードが必要になります。詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

インストールと使用の準備

1. ISWM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。
ここでは、ISWMを1台のWindowsサーバで運用する場合を例に説明します。LinuxサーバでICAP版をお使いになる場合や、複数のサーバで負荷分散して運用する場合は、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

注意:
- インストール作業前に、すべてのアプリケーションを終了してください。
- すでに旧バージョンの ISWM をお使いの場合、設定を引き継いでバージョンアップインストールします。
  アップデートインストール可能な ISWM のバージョンについては、製品付属のReadmeをご参照ください。
  万が一の場合に備えて、以下のフォルダにある設定ファイルをバックアップしてください。
  ＜インストールフォルダ＞¥conf
  バージョンアップインストールについては、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

---

1. インストールを実行するコンピュータに、管理者権限を持つログインユーザでログインします。

2. インストールメディアを挿入し、セットアッププログラム「setup.exe」を実行します。

セットアッププログラムは、<インストールメディア>¥program¥windows¥にあります。インストール開始画面が表示されます。

3. [次へ]ボタンをクリックします。

使用許諾契約画面が表示されます。

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

使用許諾契約の内容に同意いただけない場合は、[使用許諾契約の条項に同意しない]をクリックしてインストールを中止してください。

5. インストールするフォルダを確認して[次へ]ボタンをクリックします。

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

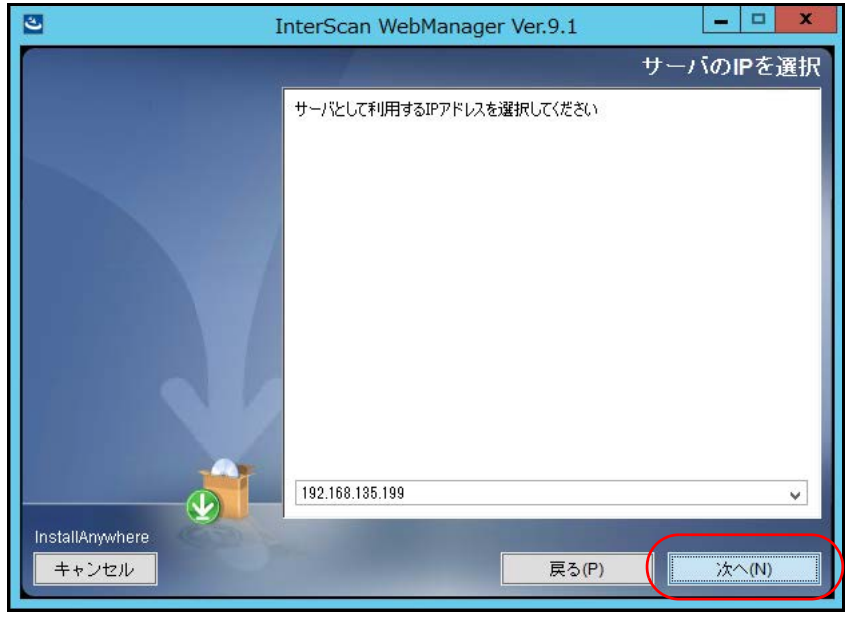
注意:
- 旧バージョンの ISWM の設定ファイルを引き継ぎたい場合は、旧バージョンがインストールされていたフォルダにインストールしてください。
- フォルダ名は半角英数字、'_' 、'-' のみを使用してください。また、フォルダ名全体の長さが128文字を超えないようにしてください。

6. インストールタイプで[プライマリサーバ]が選択されていることを確認し、[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。

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: サーバのIPアドレスが複数設定されている場合、ISWMとして利用するIPアドレスを選択してください。初期値で使用する場合、そのまま次の手順へ進んでください。

8. [インストール]ボタンをクリックします。

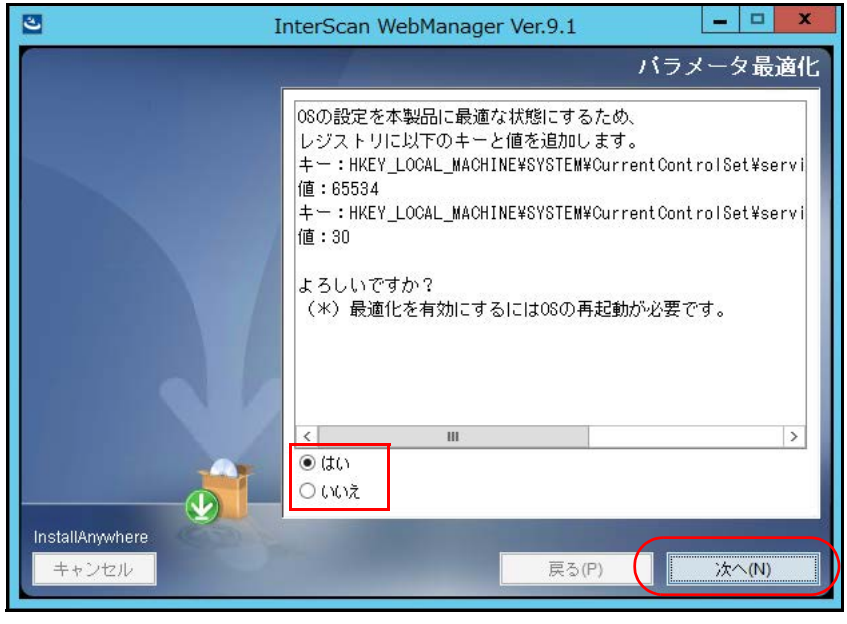
インストールが始まります。
インストールが完了するとインストール完了の画面が表示されます。

9. [次へ]ボタンをクリックします。

OSパラメータの最適化を確認する画面が表示されます。

10. [はい]をクリックして選択し、[次へ]ボタンをクリックします。

設定が完了すると、メッセージが表示されます。



11. [次へ]ボタンをクリックします。

再起動を促すメッセージが表示されます。

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

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

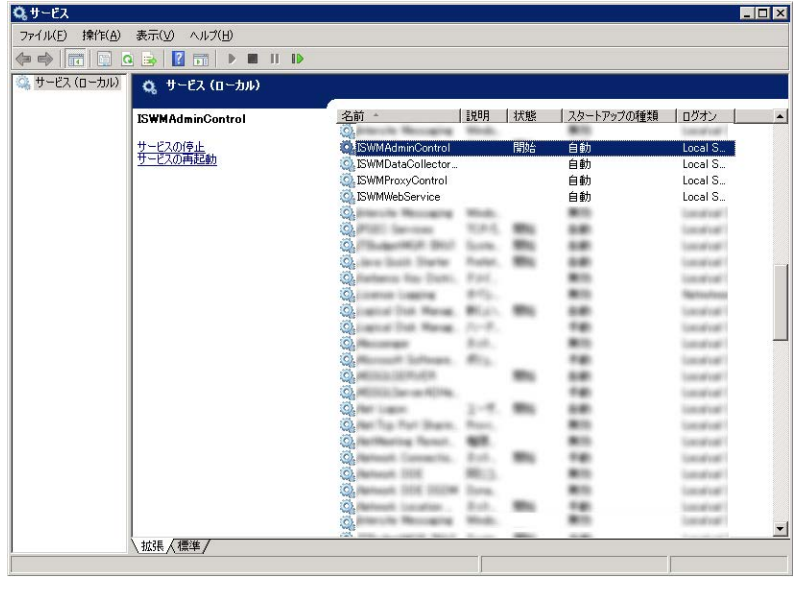
注意： OSパラメータの最適化を実行しなかった場合、コマンドラインからサーバのチューニングを実行できます。詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

以上で、ISWMのインストールは完了です。

2. ISWMの起動と停止

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

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



ISWMには、4つのサービスがあります。

ISWMAdminControl	: 管理サービス
ISWMWebService	: 拡張Webサービス
ISWMProxyControl	: フィルタリングサービス
ISWMDataCollectorControl	: 集計サービス

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

3. ISWMのアンインストール

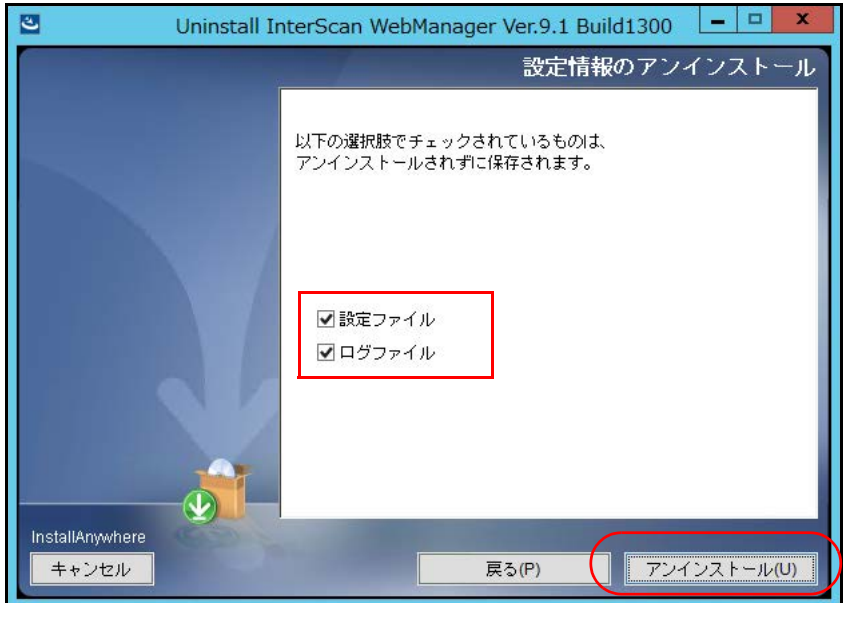
ISWMは、次の手順でアンインストールしてください。

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、[プログラムと機能]をダブルクリックします。
3. ISWMを選択して[変更と削除]ボタンをクリックします。

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

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

   アンインストールが完了するとアンインストール完了画面が表示されます。



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

6. [完了]ボタンをクリックします。

以上で、ISWMのアンインストールは完了です。

管理画面の操作

1. 管理画面へのログイン/ログアウト

ISWM は、プライマリサーバの管理画面で設定します。管理画面には、プライマリサーバ、レプリカサーバ以外の端末からネットワーク経由でアクセスできます。

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

1-1. 管理画面へのログイン

管理画面へのログインは次の手順で行います。

1. ブラウザで管理画面にアクセスします。

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

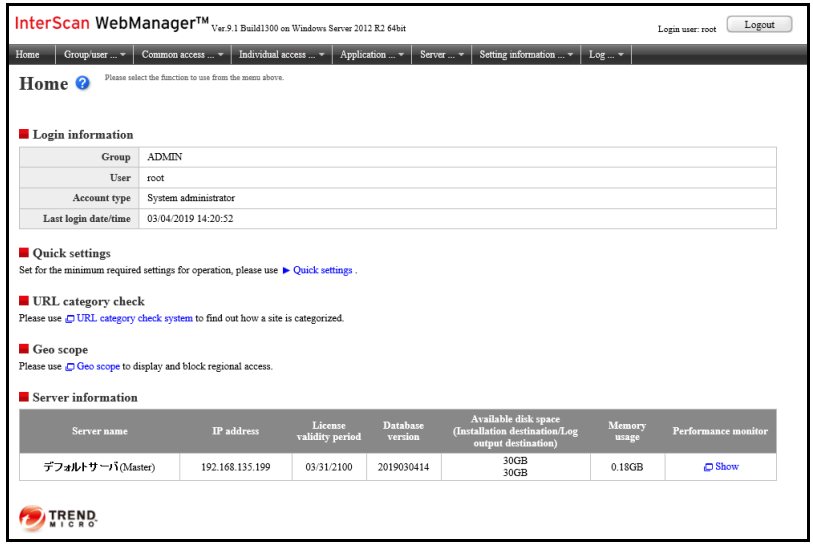
注意: Windows 版の場合、[スタート] ボタン→ [すべてのプログラム] → [InterScanWebManager]→[InterScanWebManager]をクリックするとログイン画面を表示できます。

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。
- 言語で [English] を選択した場合は、画面の項目が英語で表示されます。日本語で作成したグループ名やカテゴリ名は、日本語のままで表示されます。



- ログイン後は、ブラウザなどの [戻る] ボタンなどで、ページを切り替えないでください。また、管理画面を終了させるときは、必ず画面右上の[ログアウト]でログアウトしてから[閉じる]ボタンなどでブラウザを終了させてください。ログアウトしないでブラウザを終了した場合、ログインしたままの状態になります。

■ ログインするアカウントについて

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

アカウント種別	説明
システム管理者	システムの管理者です。 管理画面上ですべての設定が可能です。

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

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

1-2. 管理画面からのログアウト

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

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

1. 画面右上にある[ログアウト]をクリックします。

   確認のダイアログが表示されます。

2. [OK]ボタンをクリックします。

2. [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。

2-1. [ホーム]画面

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

■ ログイン情報

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

■ 簡易設定

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

■ URLカテゴリ確認

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

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

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

■ Geo スコープ

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

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

■ 地域別規制

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

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

4. 未分類のみをブロックする場合は、[未分類のみ対象] を [ON] にします。

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

■ サーバ情報

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

■ メインメニュー

7つのカテゴリに分類された設定項目を表示します。

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

[グループ/ユーザ管理]画面	「2-2. [グループ/ユーザ管理]画面でできること」(28ページ)
[共通アクセス管理]画面	「2-3. [共通アクセス管理]画面でできること」(29ページ)
[個別アクセス管理]画面	「2-4. [個別アクセス管理]画面でできること」(32ページ)
[規制解除申請管理]画面	「2-5. [規制解除申請管理]画面でできること」(35ページ)
[サーバ管理]画面	「2-6. [サーバ管理]画面でできること」(36ページ)
[設定情報管理]画面	「2-7. [設定情報管理]画面でできること」(38ページ)
[ログ管理]画面	「2-8. [ログ管理]画面でできること」(39ページ)

2-2. [グループ/ユーザ管理]画面でできること

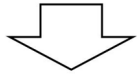
[グループ/ユーザ管理]画面では、次の機能が使用できます。
設定方法や内容については、「第5章 グループとユーザの登録」(49ページ)を参照してください。

■ グループ、ユーザの登録、管理

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

1. グループの登録、管理

グループを登録します。登録したグループは、名前の変更、削除が可能です。



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。

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

[ユーザ一括処理]では、CSV形式のファイルを読み込んで、グループ、ユーザ情報を一括して登録、削除できます。

■ 登録したIPアドレスとグループの一覧を確認する

[IPアドレス有効範囲]では、登録したIPアドレスとグループの一覧を確認できます。

■ LDAPサーバと同期する

[LDAPユーザ同期]では、登録したLDAPサーバをISWMと同期することができます。

2-3. [共通アクセス管理]画面でできること

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

設定	参照先	適用範囲
HTTPS規制設定	『Trend Micro InterScan WebManager v9.1 管理者ガイド』	すべてのグループ/ユーザ
高度分類クラウドの設定		
ブラウザ規制設定		
検索キーワード規制設定		
書き込みキーワード規制設定		
規制画面設定		
カテゴリ名設定		
規制オプション設定		
ヘッダ編集設定		

■ HTTPS規制の設定

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

注意: ICAP版では、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]は表示されません。

■ 高度分類クラウドの設定

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

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

■ ブラウザ規制の設定

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

■ 検索キーワード規制の設定

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

■ 書き込みキーワード規制の設定

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

■ 規制画面の設定

規制画面に表示するファイルやURL、またはメッセージを設定します。
また、規制画面に表示するドメイン名を設定します。
規制画面とは、クライアントPCからリクエストしたURLの表示を、ISWMが規制したことを、ユーザに通知する画面です。

■ カテゴリ名の設定

カテゴリルールの「ユーザ設定カテゴリ」のサブカテゴリ名を設定します。
ここで設定したサブカテゴリ名は、カテゴリルールの設定時に全グループに共通して適用されます。

■ 規制オプションの設定

POSTリクエストを規制する場合の書き込み許容サイズを設定します。
規制オプション設定では、システム一括でサイズを設定するか、ルール毎にサイズを設定するかを選択できます。
[システム一括でサイズを設定する]を選択した場合は、すべてのグループ/ユーザに適用する、書き込み許容サイズを設定します。
[ルール毎にサイズを設定する]を選択した場合は、[個別アクセス管理]-[規制オプション設定]で個別に書き込み許容サイズを設定します。
また、複数のカテゴリに個別に書き込み許容サイズが設定された場合、判定する際の優先動作を[カテゴリ順で判定する] 、または [許容サイズのもっとも大きな値でのみ判定する] のどちらかに設定することができます。

■ ヘッダ編集の設定

サーバ送信時に追加するリクエストヘッダを設定します。
指定のドメインを対象として、クライアントブラウザからのリクエストヘッダに指定のヘッダを追加してサーバに送信します。

2-4. [個別アクセス管理]画面でできること

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

設定	参照先	適用範囲
カテゴリ設定	「3-1. カテゴリルールを設定する」(80ページ)	グループ/ユーザ
スケジュール設定	「3-2. スケジュールを設定する」(85ページ)	グループ/ユーザ
例外URL設定	『Trend Micro InterScan WebManager v9.1 管理者ガイド』	グループ
例外URLスケジュール設定		グループ
例外サービス設定		グループ
優先カテゴリ設定		グループ
ブラウザ規制設定		グループ/ユーザ
検索キーワード規制設定		グループ/ユーザ
書き込みキーワード規制設定		グループ/ユーザ
規制画面設定		グループ
規制オプション設定		グループ/ユーザ

■ カテゴリルールの設定

グループ/ユーザに適用するカテゴリルールを設定します。
不法、アダルト、ショッピングなど、複数のカテゴリに分類されたWebサイトへの規制を設定できます。

■ スケジュールの設定

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

■ 例外URLの設定

グループに適用する例外URLルールを設定します。
カテゴリルールの例外として、アクセスを規制するURLを設定します。
また、規制対象のURLを「許可」または「閲覧のみ許可」に設定できます。

■ 例外URLスケジュールの設定

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

■ 例外サービスの設定

グループに適用する例外サービスルールを設定します。
カテゴリルールの例外として、アクセスを管理するサービスを設定します。
また、規制対象のサービスを「許可」または「閲覧のみ許可」に設定できます。

■ 優先カテゴリの設定

グループに適用する優先カテゴリルールを設定します。
クライアントPCからリクエストしたURLが複数のカテゴリに該当する場合に優先するカテゴリを設定できます。

■ ブラウザ規制の設定

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

■ 検索キーワード規制の設定

グループ/ユーザに適用する検索キーワード規制ルールを設定します。
規制対象とする検索キーワードを設定できます。
[共通アクセス管理]-[検索キーワード規制設定]の設定と合わせて規制されます。

■ 書き込みキーワード規制の設定

グループ/ユーザに適用する書き込みキーワード規制ルールを設定します。

規制対象とする書き込みキーワードを設定できます。
[共通アクセス管理]-[書き込みキーワード規制設定]の設定と合わせて規制されます。

■ 規制画面の設定

グループに適用する規制画面ルールを設定します。
規制画面に表示する画像、規制メッセージを設定できます。
規制画面とは、クライアントPCからリクエストしたURLの表示を、ISWMが規制したことを、ユーザに通知する画面です。

■ 規制オプションの設定

グループに適用する規制オプションルールを設定します。
IPアドレスを使用したURLの規制、規制を一時解除する場合の解除時間やパスワードなどを設定できます。
また、POSTリクエストを規制する場合の書き込み許容サイズを設定できます。
なお、書き込み許容サイズは、[共通アクセス管理]-[規制オプション設定]で[ルール毎にサイズを設定する]を選択した場合に設定できます。

2-5. [規制解除申請管理]画面でできること

規制解除申請の設定と管理ができます。
詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

■ 規制解除申請の設定

[規制解除申請管理]-[規制解除申請設定]では、規制対象のURLにアクセスしたときに表示される規制画面から、ユーザが規制解除を申請するための設定を行います。

■ 規制解除申請の管理

[規制解除申請管理]-[規制解除申請一覧]では、ユーザから送信された規制解除申請を管理します。
管理者は、ユーザからの規制解除申請を、処理済・未処理別に確認できます。
管理者は、未処理の申請内容を確認して、承認または拒否できます。承認結果は、ユーザに通知メールを送信することもできます。
また、処理済の規制解除申請の一覧を確認して、不要な履歴を削除できます。

注意: 規制解除申請機能を使用するためには、[規制解除申請管理]-[規制解除申請設定]で、規制解除申請機能の[ユーザからの規制解除申請を受け付ける]チェックボックスをオンにしてください。
設定については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

2-6. [サーバ管理]画面でできること

レプリカサーバの登録やISWMの設定変更などのほかに、ユーザ認証方法やメール通知設定など、サーバ共通の設定ができます。
設定方法や内容については、「第4章 サーバの設定」(40ページ)を参照してください。

■ サーバの設定と登録

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

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

■ データベースのダウンロード

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

■ 信頼済み証明書設定

SSLサーバの証明書を検証するために使用する認証局証明書の管理が行えます。

■ ユーザ認証/LDAPの設定

フィルタリングサービスをグループごとにする場合のユーザ認証の方法を設定します。LDAP連携やLDAP同期も設定できます。

■ メール通知設定

管理者宛てに、ISWMのライセンス期限切れの事前通知やサーバの動作状況をメールで通知できます。

■ 上位プロキシ設定

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

■ 一般設定

管理画面の[サーバ管理]-[一般設定]で、以下の設定を行うことができます。

・セーフサーチロック

・アクセス制御設定

・フィルタリングバイパス設定

・保存/復旧設定

・通知設定

・例外URL自動登録設定

・例外URL自動削除設定

・ARMS(Automatic registration service for Malware Site)設定

2-7. [設定情報管理]画面でできること

システム設定(proxy.inf)の情報一覧の確認、設定の保存/復旧/同期ができます。
詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

■ 設定情報の確認

システム設定(proxy.inf)の情報一覧を確認できます。

■ 設定の保存/復旧/同期

管理画面で設定した内容の保存、および保存した設定の復旧ができます。
万一の際のバックアップに設定を保存しておくことをお勧めします。設定は最大で5つまで保存できるので、試験運用時の設定の保存/復旧にも利用できます。
また、設定をレプリカサーバに同期できます。

2-8. [ログ管理]画面でできること

[ログ管理]では、ユーザのアクセスログとシステムログを管理します。また、Syslog転送機能の設定が行えます。
詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

■ ログファイルの取得/出力先設定

[ログ管理]-[ログ設定]では、各種のログファイルの取得方法や出力する項目などの設定ができます。

■ アクセスログの管理

[ログ管理]-[アクセスログ]では、ユーザのアクセスログを管理します。
アクセスログには、アクセスしたユーザ(アカウント/IPアドレス)および閲覧したURLなどが記録されます。アクセスログを調査して、不正なアクセスを確認したり、ユーザがアクセスするWebサイトの傾向を分析できます。
アクセスログ管理機能は、システム管理者と第一階層のグループ管理者が使用できます。第二階層以下のグループ管理者は使用できません。

注意:
- 第一階層のグループ管理者が、アクセスログ管理機能を使用するためには、[ログ管理]-[ログ設定]で、アクセスログの出力単位を「第一階層グループ毎」に設定してください。ログの出力単位が「システム一括」の場合、メインメニューの[ログ管理]が表示されません。
  設定については『Trend Micro InterScan WebManager v9.1 管理者ガイド』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。

■ システムログの管理

[ログ管理]-[システムログ]では、システムログを管理します。
システムログには、いつ、どのプロセスで、どんな操作を行ったかが記録されます。
システムログを調査して、システムの操作履歴を確認できます。
システムログ管理機能は、システム管理者だけが使用できます。

サーバの設定

1. 簡易設定の概要

簡易設定は、1台のサーバでISWMのフィルタリングサービスを運用する場合に、運用に必要な最小限の設定、およびフィルタリングルール適用を一括して設定する方法です。

注意: 次の環境で運用する場合には、簡易設定を使用できません。

- 負荷分散のため、複数のサーバで運用する場合
  →[サーバ管理]画面で設定します。
- ユーザやグループ単位にフィルタリングルールを適用する場合
  →[グループ/ユーザ管理]画面および[個別アクセス管理]画面で設定します。

1-1. 簡易設定の設定内容

簡易設定では、グループ/ユーザ別にフィルタリングルールを適用することができません。
簡易設定で設定できる内容は以下のとおりです。

選択できるユーザ認証方式	フィルタリングルール設定	
	選択できる適用方法	スケジュール設定
ユーザ認証なし	全ユーザ一括適用	設定できません

それぞれの項目の詳細設定については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

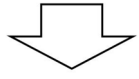
1-2. 選択できるカテゴリルール

簡易設定では、ルートグループに登録されているカテゴリルールから、適用するカテゴリルールを選択し、全ユーザに一括して適用します。
「第6章 フィルタリングの設定」(71ページ)を参照してください。

1-3. 簡易設定での運用の流れ

1. 簡易設定をする

ISWMの運用に必要な最小限の設定をします。
設定は、[ホーム]画面の[簡易設定]-[簡易設定]から行います。
詳しくは、「2. 簡易設定」(42ページ)を参照してください。



2. クライアントPCの設定をする

フィルタリングサービスを利用するクライアントPCの設定をします。
詳しくは、「4. クライアントPCの設定」(48ページ)を参照してください。

2. 簡易設定

簡易設定は、以下の手順で設定してください。

1. [ホーム]画面で[簡易設定]をクリックします。
   [簡易設定]が表示されます。

2. [ライセンス設定]、[フィルタリングサービス設定]、[データベース設定]で、URLデータベースのダウンロードに必要な情報を入力します。

[ライセンス設定]では、URLデータベースのダウンロードに必要なライセンスキーなどを設定します。

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

[フィルタリングサービス設定]、[データベース設定]は、必要に応じて設定します。

フィルタリングサービス設定	フィルタリングサービスに使用するポート番号を変更する場合、[設定を変更する]チェックボックスをオンにします。
データベース設定	URLデータベースダウンロード用の上位プロキシサーバ設定です。 インターネットへの接続に上位のプロキシサーバを利用している場合、[データベースダウンロード時に上位プロキシサーバを使用する]チェックボックスをオンにし、上位プロキシサーバの情報を入力します。

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

3. [カテゴリ設定]で、[設定を変更する]チェックボックスをオンにして、ルートグループに適用するカテゴリルールを選択します。

ルートグループに登録されているカテゴリルールから選択します。ルートグループには、システムで「DEFAULT RULE」、「セキュリティー重視」、「小学校」、「中学校」、「高校」、「大学」、「企業・官公庁(基本的な設定)」、「企業・官公庁(業務効率化重視)」のルールが登録されています。

[確認]ボタンをクリックすると、[カテゴリ設定]画面が別ウィンドウで表示されます。[カテゴリ設定]で選択したカテゴリルールの規制内容を確認できます。
「3. カテゴリルールの確認」(46ページ)を参照してください。

注意: 選択可能なカテゴリルールは、ルートグループに登録されているルールだけです。

4. [保存]をクリックします。

確認のダイアログが表示されます。

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

5. [OK]ボタンをクリックします。

ライセンス設定、フィルタリングサービス設定、データベース設定と、適用するカテゴリルールを設定し、URLデータベースのダウンロードを開始します。

以上で、簡易設定は完了です。

注意: フィルタリングサービス設定を変更した場合、フィルタリングサービスの再起動が必要です。詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。また、使用可能なポート番号については、ネットワーク管理者または管理部門にご確認ください。

3. カテゴリルールの確認

ここでは、[簡易設定]画面で設定した、カテゴリルールの内容について説明します。
ISWMは、WebサイトのURLをカテゴリ別に分類し、カテゴリごとに規制内容を設定しています。
[簡易設定]画面の[カテゴリ設定]の[確認]ボタンをクリックすると、以下の画面で、カテゴリごとに設定されている規制内容を確認できます。
カテゴリには、ジャンルごとにURLが分類されたカテゴリと、ユーザが任意に登録・設定できるユーザ設定カテゴリがあります。
ユーザ設定カテゴリの設定については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

注意: Webサイトの分類は、URLデータベースを提供するネットスター社により管理されています。

3-1. 規制内容について

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

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

注意: 「書き込み規制」はPOSTまたはPUTリクエストに対応しています。

4. クライアントPCの設定

ISWMでフィルタリングを実行するとき、クライアントPCのWebブラウザでプロキシサーバの設定が必要な場合があります。使用するWebブラウザのプロキシサーバの設定で、プロキシサーバのIPアドレス/ドメイン、ポート番号を設定します。

4-1. スタンドアロン 版の場合

ISWMがプロキシサーバとして動作して、フィルタリングを実行します。クライアントPCのWebブラウザでは、次のようにプロキシサーバを設定します。

プロキシサーバのIPアドレス	ISWMのIPアドレス
プロキシサーバのポート番号	ISWMで、フィルタリングに使用するポート番号(HTTP、HTTPS、FTP over HTTP)

注意:
- スタンドアロン版では、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、[サーバ管理]-[サーバ設定]の[サーバ情報]で確認できます。

グループとユーザの登録

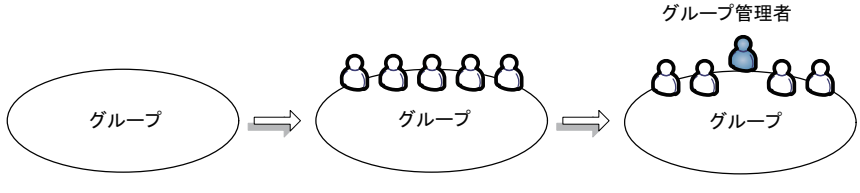
1. グループ管理の概要

ユーザごとに、フィルタリングルールを使い分けたい場合は、適用したいフィルタリングルールごとにグループを作成し、ユーザをグループに登録します。
ここでは、グループの概要とグループの作成方法について説明します。

1-1. グループとユーザ

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

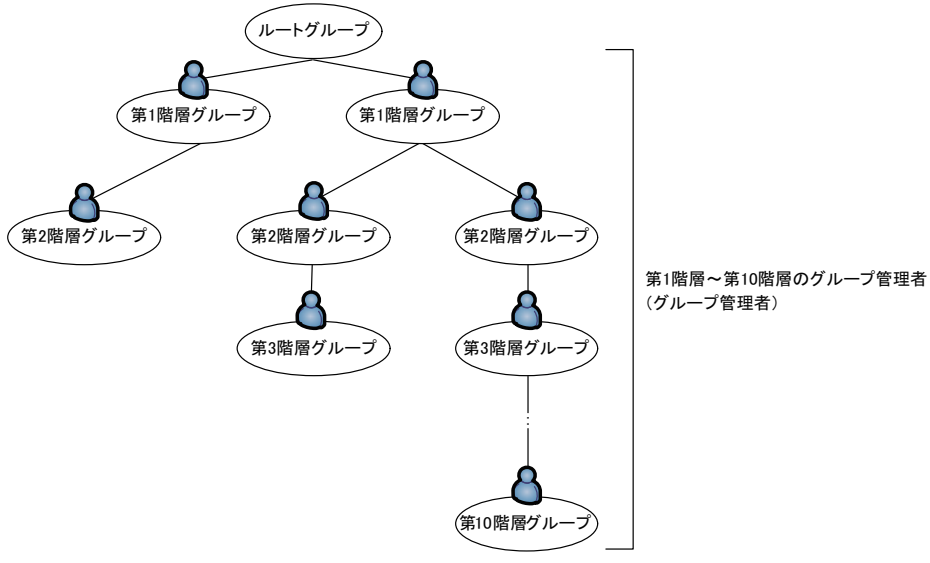
ユーザとグループの作成



1-2. グループの階層

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

グループのツリー構造



注意: ルートグループには、ユーザとグループ管理者を登録できません。

1-3. 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。
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。

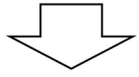
ルートグループ	すべてのグループのフィルタリングルールのベースとなる設定が登録されています。 ルートグループは、グループ名を変更できません。また、ルートグループには、ユーザを登録できません。
ADMINグループ	ISWMの管理者が所属するグループです。 初期状態では、「root」アカウントが登録されています。 ADMINグループの下位には、グループを登録できません。
GROUPグループ	グループ作成用のサンプルです。 初期状態では、「guest」アカウントが登録されています。
LDAPグループ	LDAPサーバと連携して、ユーザを管理するときに使用します。 管理画面で設定した条件でLDAPサーバを検索し、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、「2. ユーザ認証を設定する」(53ページ)を参照してください。

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

1-4. グループとユーザ登録の流れ

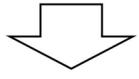
1. ユーザ認証を設定する

登録するユーザの認証方法を設定します。
本書では、BASIC認証(ローカル)の場合を例に説明します。LDAPサーバと連携したユーザ認証をする場合は、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。



2. グループを登録する

ユーザを登録するためのグループを登録します。
詳しくは、「3. グループを登録する」(57ページ)を参照してください。



3. グループにユーザを登録する

登録したグループにユーザを登録します。ユーザは、IPアドレスまたはアカウント情報で登録できます。
詳しくは、「4. グループにユーザを追加する」(61ページ)を参照してください。

本書で説明するグループ/ユーザの登録方法以外に、CSV形式のファイルを読み込んで、グループ/ユーザ情報を一括登録する方法もあります。詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

2. ユーザ認証を設定する

グループ単位でフィルタリングルールを適用するには、ユーザ認証を有効にする必要があります。
ユーザ認証が無効の場合、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適用されます。

注意: 簡易設定を実行した場合や、[サーバ管理]-[認証設定]で[認証設定]-[ユーザ認証]-[有効]をオフにした場合、すべてのユーザに対するユーザ認証が、無効になります。

2-1. ユーザ認証の種類

設定できるユーザ認証方法には以下の種類があります。

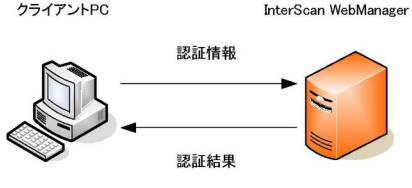
- IP アドレス認証
- BASIC 認証 (ローカル)
- BASIC 認証 (LDAP 連携)
- NTLM 認証 (スタンドアロン版のみ)
- Kerberos 認証 (スタンドアロン版のみ)

■ IPアドレス認証

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

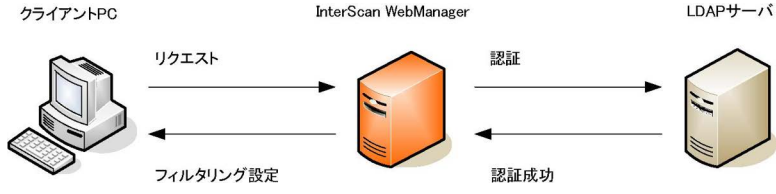
■ BASIC認証(ローカル)

クライアントPCで入力したログイン情報をISWMでBASIC認証します。

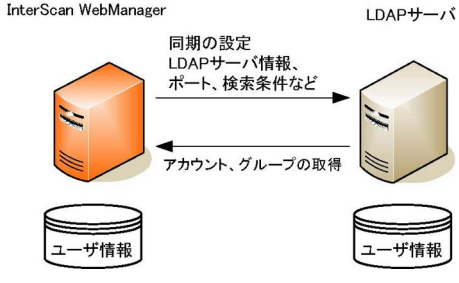


■ BASIC認証(LDAP連携)

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。



■ NTLM認証(スタンドアロン版のみ)

Microsoft社のActive Directoryと連携し、NTLM認証を使用したWindowsクライアントからのシングルサインオンを実現します。
Active DirectoryでWindowsのユーザ認証をしている環境において、対応ブラウザを使用してインターネットでWebページを閲覧する場合、あらためてユーザ名とパスワードを入力することなく、ISWMでユーザ認証ができます。

■ Kerberos認証(スタンドアロン版のみ)

Microsoft社のActive Directoryと連携し、Kerberos認証を使用したWindowsクライアントからのシングルサインオンを実現します。
Active DirectoryでWindowsのユーザ認証をしている環境において、対応ブラウザを使用してインターネットでWebページを閲覧する場合、あらためてユーザ名とパスワードを入力することなく、ISWMでユーザ認証ができます。

2-2. BASIC認証(ローカル)を設定する

ここでは、クライアントPCで入力したログイン情報をISWMでユーザ認証をする、BASIC認証(ローカル)の設定方法を説明します。

1. [サーバ管理]-[認証設定]をクリックします。

   [認証設定]が表示されます。

2. [ユーザ認証]-[有効]チェックボックスをオンにします。

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

   注意: ユーザ認証をする場合、IPアドレス認証は必ず有効になります。

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

5. [保存]ボタンをクリックします。

   確認のダイアログが表示されます。

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

6. [OK]ボタンをクリックします。

以上で、BASIC認証(ローカル)の設定は完了です。

3. 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。
ここでは、ルートグループの直下にある第1階層に、グループを追加します。

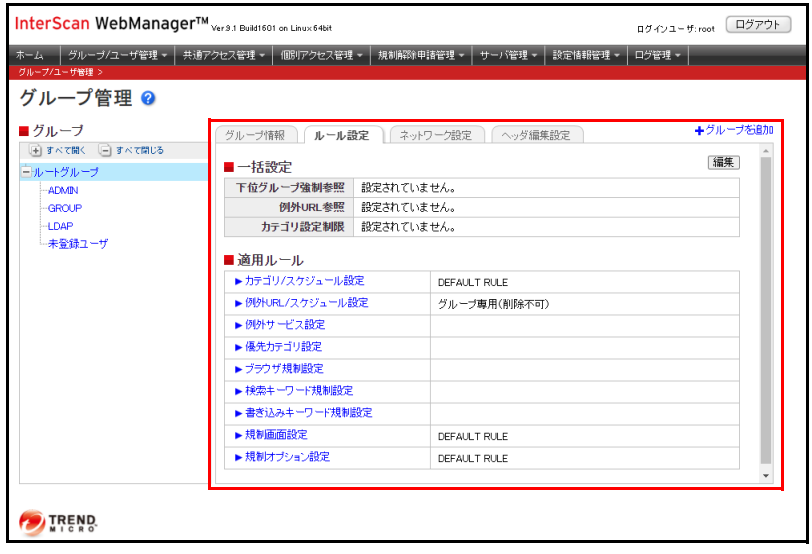
1. [グループ/ユーザ管理]-[グループ管理]をクリックします。

   [グループ管理]が表示されます。

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

   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。
   選択したグループ名の背景が水色表示されます。

設定画面にグループの設定内容が表示されます。



3. [グループを追加]をクリックします。

[グループ登録]が表示されます。

4. グループ名とコメントを入力します。

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

注意: グループ名、コメントには、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | "),全角記号(¥ ／ ： ； ？ ＜ ＞ ｜ ”)

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

[グループ管理]に「登録が完了しました。」と表示されます。

以上で、グループ登録は完了です。
[グループ名]/[コメント]を変更する場合、[グループ情報]タブの[編集]ボタンをクリックして表示される[グループ情報編集]で変更後、[保存]ボタンをクリックします。
グループを削除する場合、[グループ情報]タブで[削除]ボタンをクリックします。

4. グループにユーザを追加する

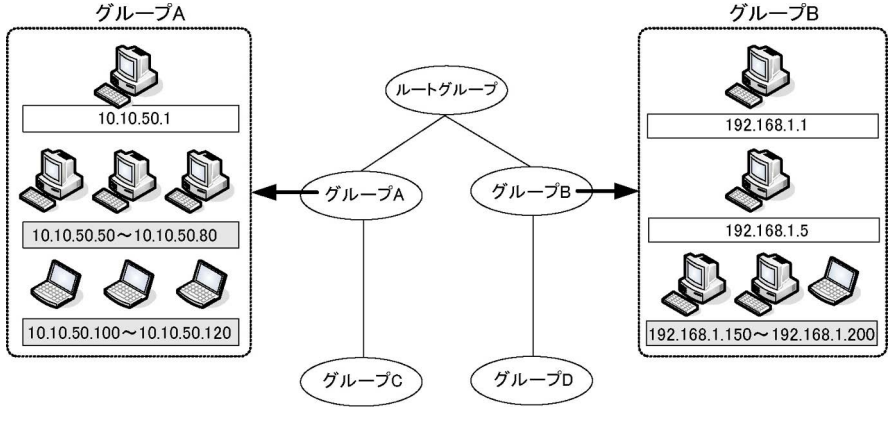
4-1. ユーザの登録方法

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。

注意: アカウントで管理されたユーザは、Web アクセス時にブラウザ上でアカウントとパスワードを入力する必要があります。ユーザごとに適した方法で登録してください。ユーザ管理の詳細については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

■ IPアドレス管理の特長

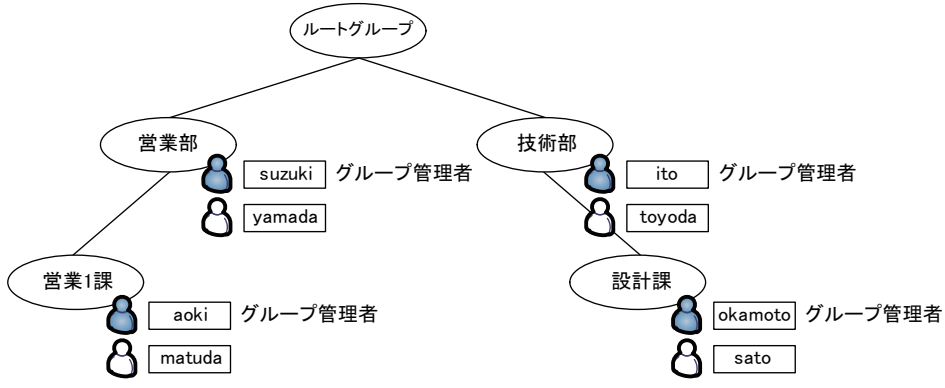
IPアドレスでユーザを管理すると、端末を使用するユーザに関係なく、端末のIPアドレス単位で管理できます。単一のIPアドレスまたはIPアドレスを範囲指定して登録できます。IPアドレスを範囲指定して登録した場合、指定した範囲内のIPアドレスを一括して管理できます。



注意:
- システム管理者だけが、IPアドレスを登録、管理できます。
- グループ管理者は、IPアドレスでのユーザ登録はできません。
  所属するグループと下位グループのIPアドレス一覧をCSVファイルに出力する機能だけが使用できます。

■ アカウント管理の特長

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



4-2. IP アドレスを登録する

端末のIPアドレスを使用して、ユーザ登録する方法について説明します。
IPアドレスは個別、または範囲で登録できます。

注意: IPアドレスを登録できるのは、システム管理者だけです。

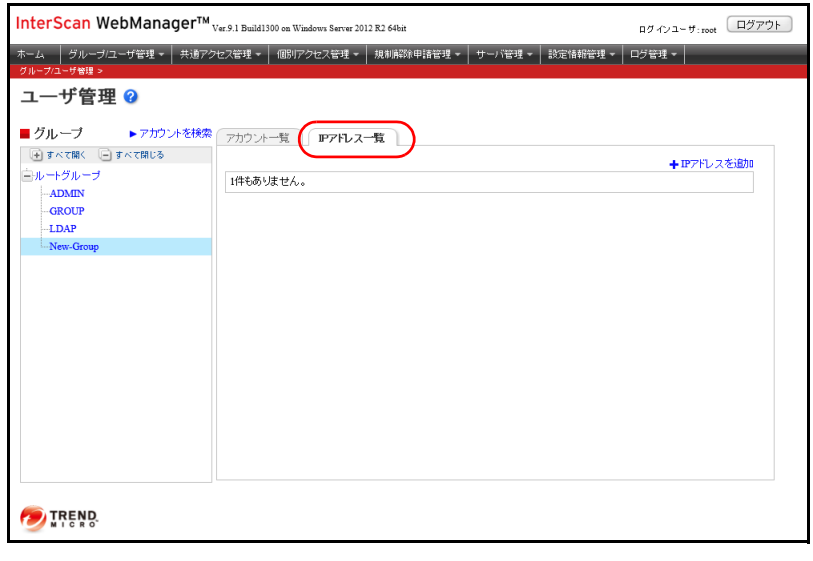
1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。

   [ユーザ管理]が表示されます。

2. グループ一覧から、IPアドレスを登録するグループ名をクリックします。

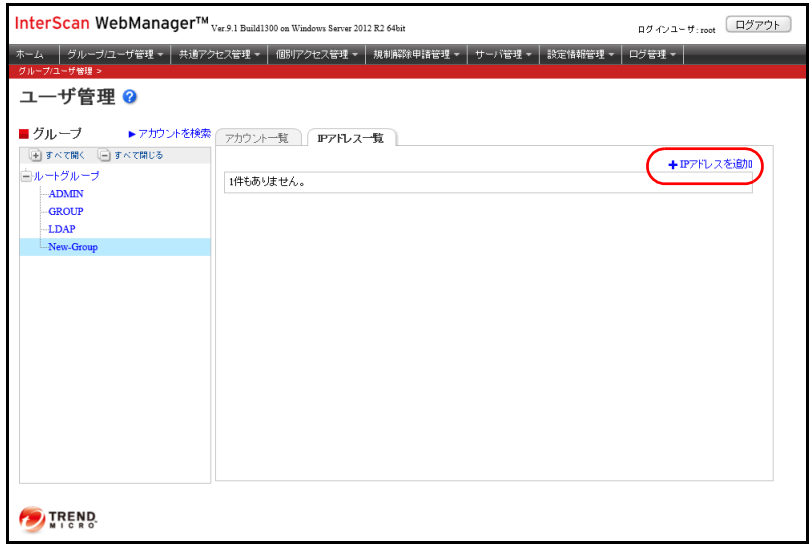
ユーザ一覧が表示されます。

3. [IPアドレス一覧]タブをクリックします。

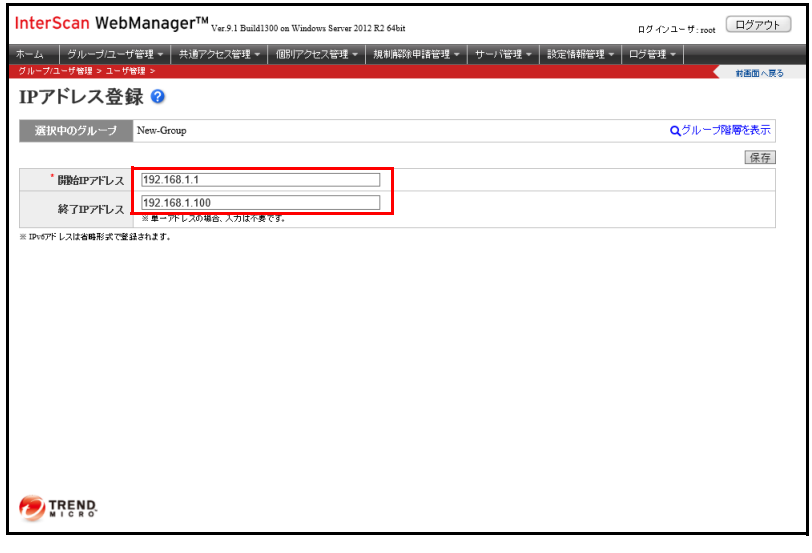


4. [IPアドレスを追加]をクリックします。

[IPアドレス登録]が表示されます。



5. 登録するIPアドレスを入力します。



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

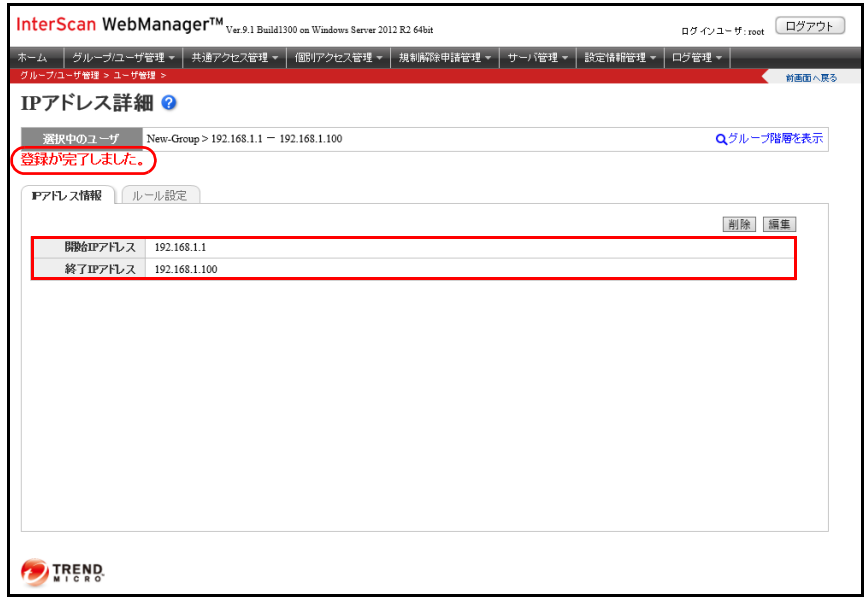
注意: IPアドレスを範囲で登録する場合、IPアドレスが「開始IPアドレス」<「終了IPアドレス」となるように入力してください。

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されます。



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

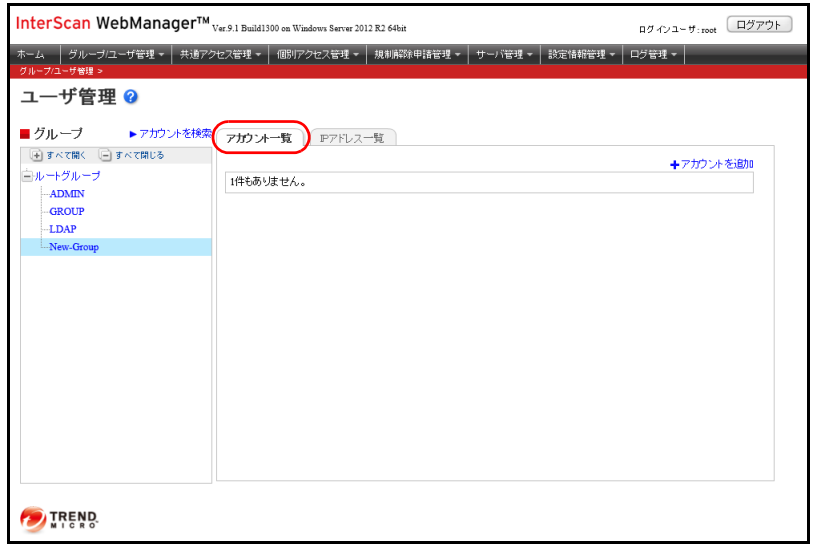
以上で、グループへのIPアドレスの登録は完了です。

4-3. アカウントを登録する

ユーザのアカウントをユーザ名として使用して、ユーザ登録する方法について説明します。

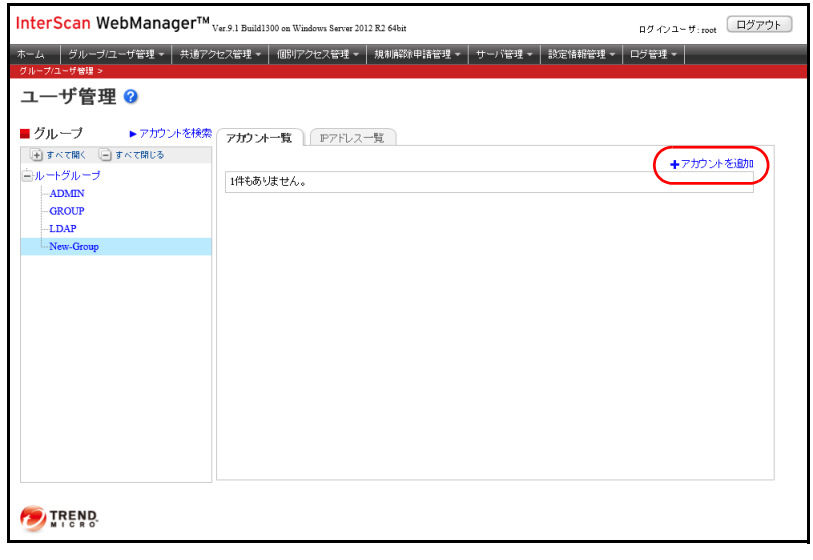
1. [グループ/ユーザ管理]-[ユーザ管理]をクリックします。
   [ユーザ管理]が表示されます。
2. グループ一覧から、アカウントを登録するグループをクリックします。
   ユーザ一覧が表示されます。

3. [アカウント一覧]タブをクリックします。

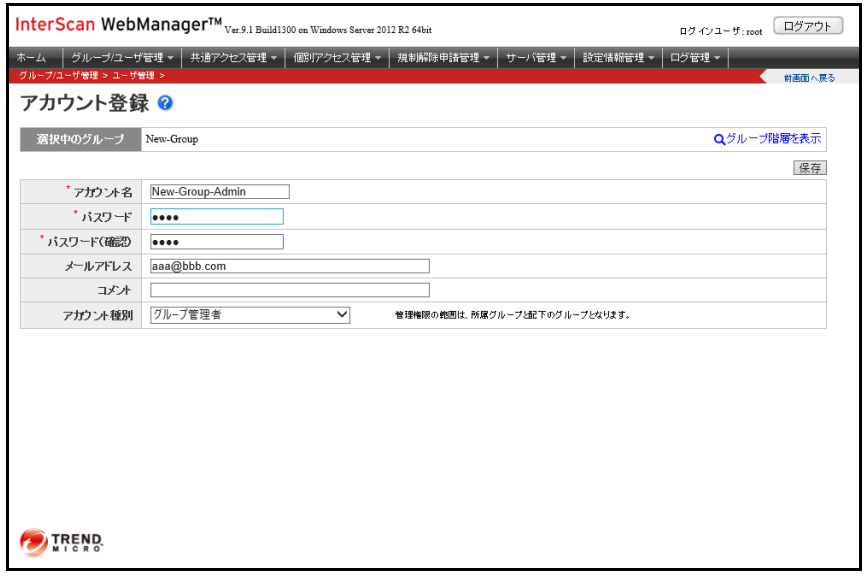


4. [アカウントを追加]をクリックします。

[アカウント登録]が表示されます。



5. 登録するアカウントの情報を入力します。



選択中のユーザ **選択中のグループ**	アカウントを登録するユーザ名とグループ名が表示されます。
アカウント名(必須項目)	登録するアカウント名を半角20文字以内で入力します。
パスワード(必須項目)	パスワードを半角20文字以内で入力します。
パスワード(確認)(必須項目)	確認のため、再度パスワードを入力します。
メールアドレス	登録するアカウントのメールアドレスを半角 128 文字以内で入力します。
コメント	登録するアカウントに対するコメントを半角 100 文字以内で入力します。

アカウント種別	登録するアカウントの種別を選択します。アカウント種別は以下のいずれかを選択できます。 • システム管理者 • システム管理者(制限付き) • システム管理者(閲覧のみ) • システム管理者(例外 URL 設定のみ) • グループ管理者 • グループ管理者(制限付き) • グループ管理者(閲覧のみ) • グループ管理者(例外 URL 設定のみ) • 一般ユーザ アカウントについては、「ログインするアカウントについて」(20ページ)を参照してください。

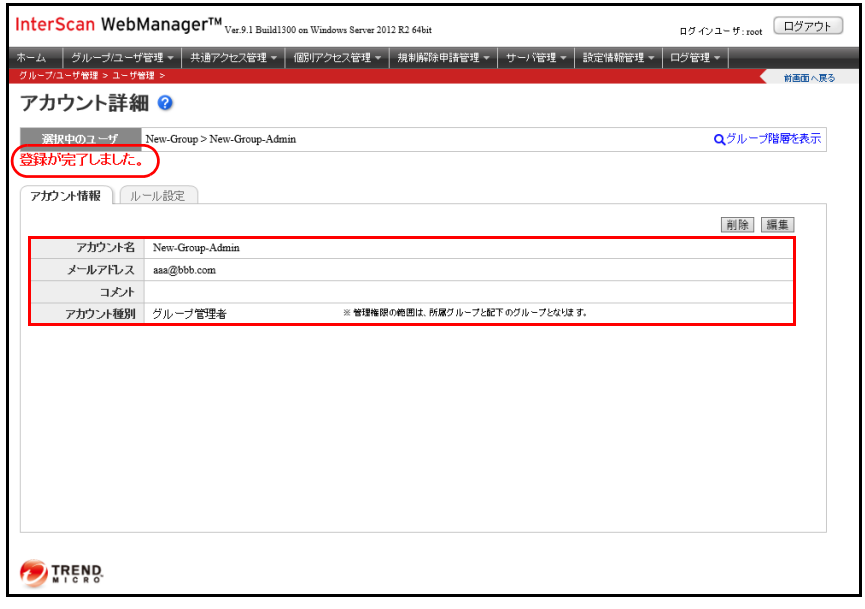
注意:
- アカウント名、パスワード、メールアドレスには、半角英数字および次の記号を使用できます。
  また、アカウント名には半角スペースも使用できます。
  ! # $ % & ' ( ) = ` ~ { + } _ - ^ @ [ ] . * / < > |
- コメントには、次の文字を使用できません。
  タブ記号、半角記号(¥ / : ; ? < > | "),全角記号 (¥ ／ ： ； ？ ＜ ＞ ｜ ”)

6. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

7. [OK]ボタンをクリックします。

「登録が完了しました。」と表示されます。



注意: 選択したグループに初めてアカウントを登録した場合、ユーザー一覧に操作ボタンが追加されます。

以上で、グループへのアカウントの登録は完了です。

フィルタリングの設定

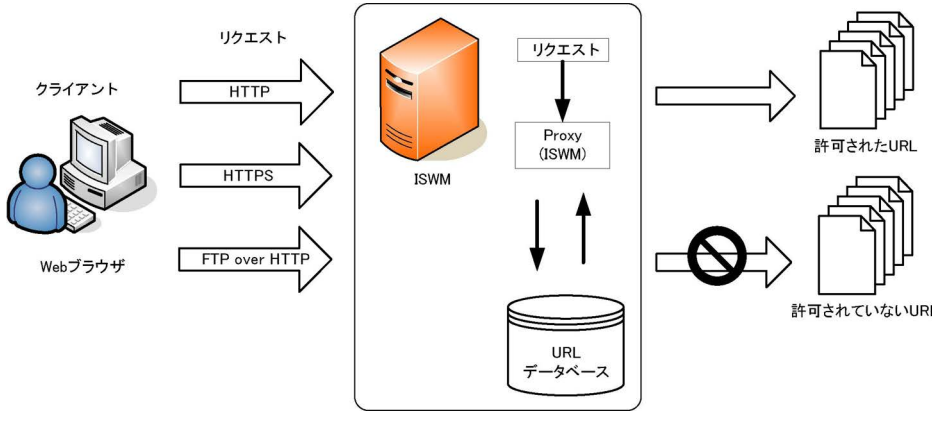
1. フィルタリングの概要

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

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

1-1. ISWM を使用したフィルタリング

Windows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。



1-2. フィルタリング設定の流れ

フィルタリング設定は、[共通アクセス管理]および[個別アクセス管理]で行います。
[共通アクセス管理]では、すべてのグループ/ユーザに適用するフィルタリング設定をします。
[個別アクセス管理]では、グループ/ユーザに適用するフィルタリングルールを設定します。
[個別アクセス管理]で設定したフィルタリングルールを、[グループ/ユーザ管理]でグループ/ユーザに適用します。

フィルタリングルールは、グループに適用する設定とユーザに適用する設定の2種類があります。
ここでは、フィルタリングルールをグループに適用する流れについて説明します。

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

1. 共通アクセスの設定

すべてのグループに適用するフィルタリング設定をします。
詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

a. HTTPS規制の設定

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

b. その他のルールの設定

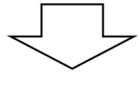
その他のルールには、次の種類があります。

- 高度分類クラウドの設定
- ブラウザ規制の設定
- 検索キーワード規制の設定
- 書き込みキーワード規制の設定
- 規制画面の設定
- 規制オプションの設定
- ヘッダ編集の設定

クライアントPCのWebブラウザの規制、規制するキーワード、規制を実施したときにユーザへ通知する規制画面などを設定します。

c. カテゴリ名の設定

ユーザ設定サブカテゴリ名を設定します。



2. 個別アクセスを設定する

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。
詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

a. カテゴリルールの設定

グループに適用するカテゴリルールを設定します。
カテゴリ別に規制内容を選択して、カテゴリルールを設定します。
詳しくは、「3-1. カテゴリルールを設定する」(80ページ)を参照してください。

b. スケジュールの設定

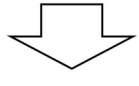
グループに適用するスケジュールを設定します。
フィルタリング対象のグループに対して、適用するカテゴリ/例外URLルールと、ルールを適用する時間帯を設定します。
詳しくは、「3-2. スケジュールを設定する」(85ページ)を参照してください。

c. その他のルールの設定

その他のルールには、次の種類があります。

- 例外 URL の設定
- 例外サービスの設定
- 優先カテゴリの設定
- ブラウザ規制の設定
- 検索キーワード規制の設定
- 書き込みキーワード規制の設定
- 規制画面の設定
- 規制オプションの設定

カテゴリルールの例外として、アクセスを規制するURL、使用を制限するサービス、クライアントPCからリクエストしたURLが複数のカテゴリに該当する場合の優先カテゴリ、クライアントPCのWebブラウザの規制、規制するキーワード、規制を実施したときにユーザへ通知する規制画面などを設定します。



3. フィルタリングルールをグループに適用

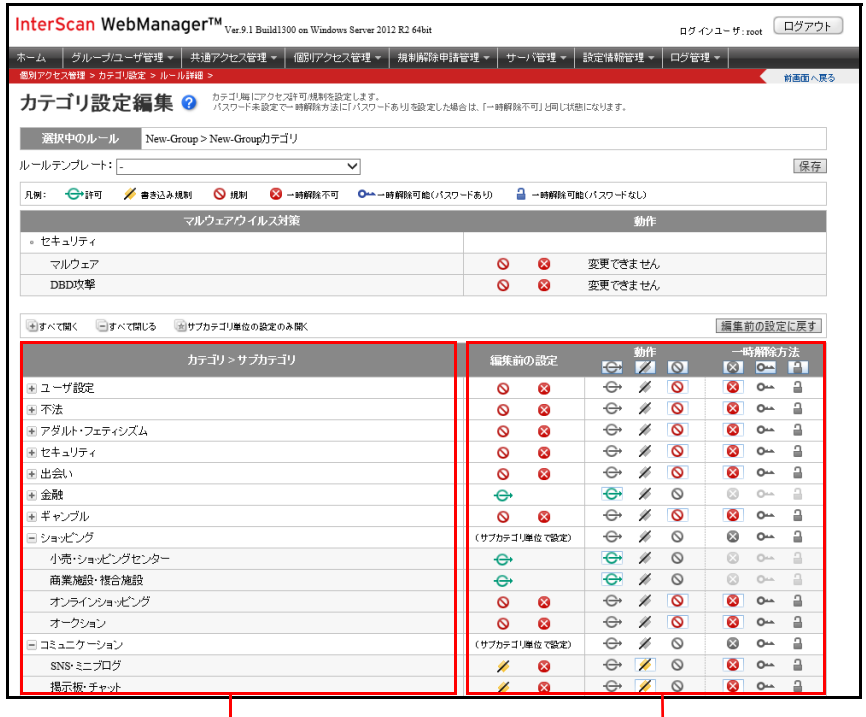
設定したフィルタリングルールを、グループに適用します。
詳しくは、「4. フィルタリングルールをグループに適用する」(93ページ)を参照してください。

1-3. カテゴリルール

不法、アダルト、ショッピングなど、複数のカテゴリに分類されたカテゴリルールを設定します。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設定できます。

■ カテゴリについて

カテゴリ別のフィルタリング対象URLは、ネットスター社のURLデータベースから取得します。URLデータベースは定期的に更新され、常に最新のURLデータベースを使用できます。
ISWMではインストール時に「DEFAULT RULE」、「セキュリティー重視」、「小学校」、「中学校」、「高校」、「大学」、「企業・官公庁(基本的な設定)」、「企業・官公庁(業務効率化重視)」のルールが登録されています。これらを元にルールをカスタマイズしたり、管理者がルールを追加登録することができます。



■ 規制内容について

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

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

注意:
- 一時解除パスワードおよび閲覧可能な時間(一時解除時間)は、[個別アクセス管理]-[規制オプション設定]で設定します。
  規制オプションについては、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。
- 一時解除は、[共通アクセス管理]-[規制画面設定]の[規制画面形式]で、ファイルを指定した場合にだけ、有効になります。
- 書き込み規制の対象となるURLは、HTTPプロトコルまたは、[共通アクセス管理]-[HTTPS規制設定]-[サーバデコード方式]有効時のHTTPSプロトコルでPOST、PUTメソッドを使用しているURLになります。

2. 共通アクセスを設定する

すべてのグループ/ユーザに適用するフィルタリング設定をします。
共通アクセス管理でのフィルタリング設定には、次の設定内容があります。

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

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

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

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

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

規制画面
規制を実施したときにユーザへ通知する規制画面を設定します。

カテゴリ名
ユーザ設定サブカテゴリ名を設定できます。

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

ヘッダ編集
サーバ送信時に追加するリクエストヘッダを設定します。

設定方法については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

3. 個別アクセスを設定する

グループ/ユーザに適用するフィルタリングルールを設定します。
個別アクセス管理でのフィルタリング設定には、次の設定内容があります。

カテゴリルール

不法、アダルト、ショッピングなど、複数のカテゴリに分類されたWebサイトへの規制を設定します。また、サブカテゴリが存在するカテゴリでは、サブカテゴリ単位に規制内容を設定できます。
カテゴリ別のフィルタリング対象URLは、ネットスター社のURLデータベースから取得します。
URLデータベースは定期的に更新され、常に最新のURLデータベースを使用できます。

スケジュール

フィルタリング対象のグループやユーザに対して、適用するカテゴリルールと、ルールを適用する時間帯を設定します。
スケジュールには、デフォルトで適用される基本設定と、曜日、時間帯ごとに設定できる時間帯設定、祝日や特定の日付に適用される祝日設定の3種類があります。

注意: 祝日設定に割り当てる祝日や特定の日付は、設定ファイル(cal.inf)で設定します。詳しくは、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

例外URL

カテゴリルールの例外として、アクセスを規制するURLを設定します。
また、規制対象のURLを「許可」または「閲覧のみ許可」に設定できます。「許可」に設定すると、規制対象URLでも自由にアクセスできるようになります。「閲覧のみ許可」に設定すると、規制対象URLでも閲覧のみできるようになります。

例外URLスケジュール

フィルタリング対象のグループに対して、適用する例外URLルールと、ルールを適用する時間帯を設定します。
例外URLスケジュールには、デフォルトで適用される基本設定と、曜日、時間帯ごとに設定できる時間帯設定、祝日や特定の日付に適用される祝日設定の3種類があります。

例外サービス

カテゴリルールの例外として、アクセスを管理するサービスを設定します。
また、規制対象のサービスを「許可」または「閲覧のみ許可」に設定できます。「許可」に設定すると、規制対象URLでも自由にアクセスできるようになります。「閲覧のみ許可」に設定すると、規制対象URLでも閲覧のアクセスを許可します。

優先カテゴリ

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

設定します。

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

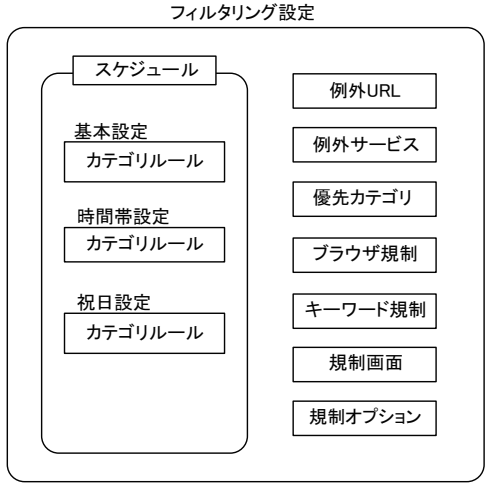
検索キーワード規制
検索サイトなどで、指定したキーワードを使用した検索を規制するよう設定している場合に、規制対象とする検索キーワードを設定します。

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

規制画面
規制を実施したときにユーザへ通知する規制画面を設定します。

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

これらのフィルタリング設定は、次の図のようになります。

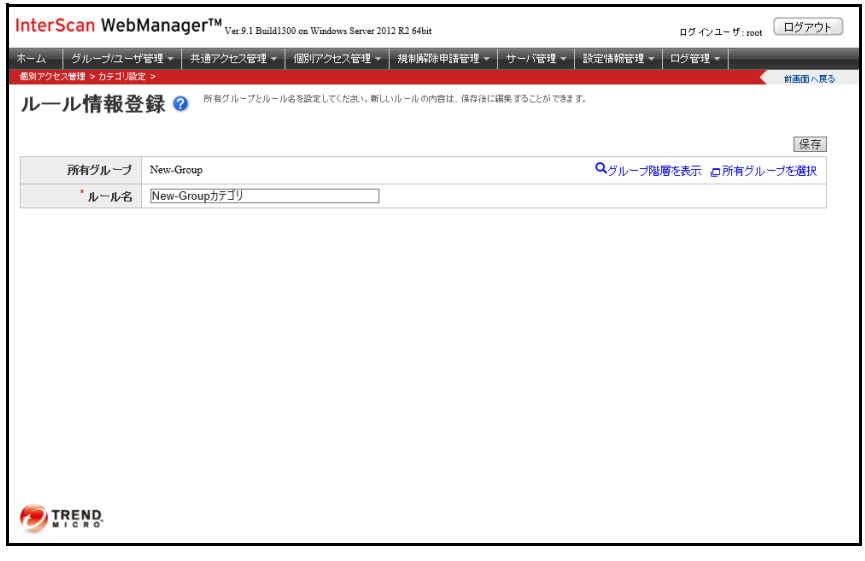


本書では、カテゴリルールとスケジュールの設定方法について説明します。その他の設定方法については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

3-1. カテゴリルールを設定する

ここでは、カテゴリルールの設定方法について説明します。

1. [個別アクセス管理]-[カテゴリ設定]をクリックします。
   [カテゴリ設定]が表示されます。
2. グループ一覧から、カテゴリルールを設定するグループをクリックします。
   [所有ルール一覧]が表示されます。
3. [所有ルール一覧]-[ルールを追加]をクリックします。
   [ルール情報登録]が表示されます。
4. ルール名を入力します。



所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。

所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名(必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

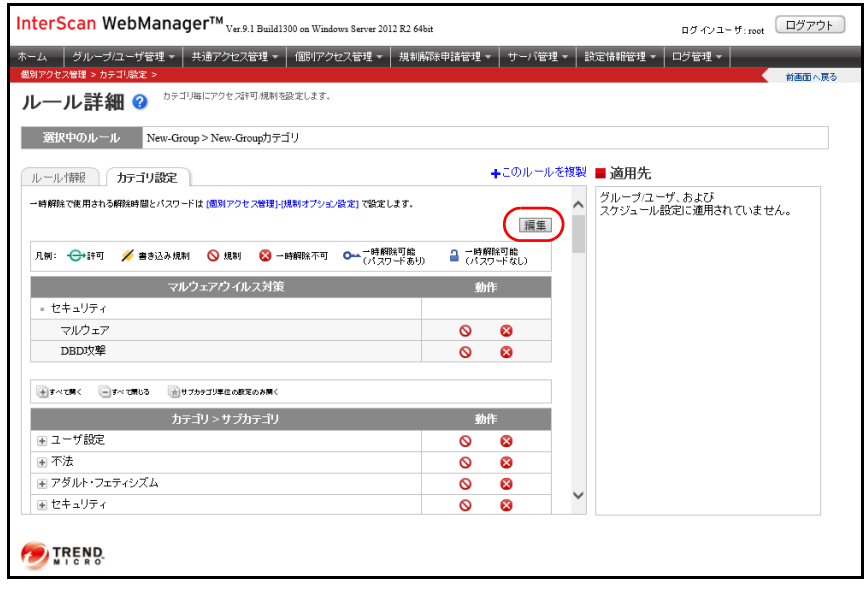
確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

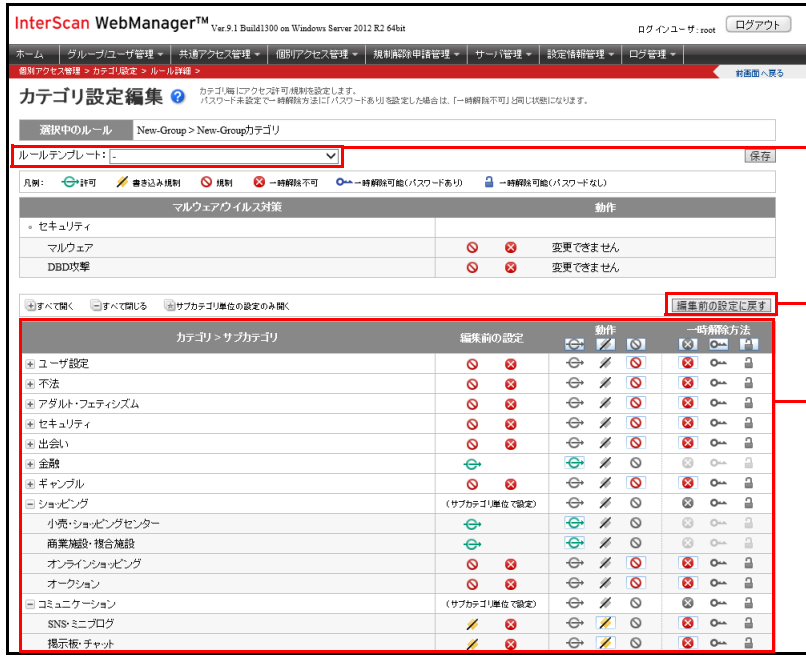
ルールが登録され、[ルール詳細]が表示されます。

7. [カテゴリ設定]タブの[編集]ボタンをクリックします。

[カテゴリ設定編集]が表示されます。



8. 規制内容を設定します。



a.**ルールテンプレート**	登録するルールのベースとするルールを選択します。
b.**[編集前の設定に戻す]ボタン**	編集前の規制内容に戻します。
c.**規制内容**	カテゴリ別の規制内容を設定します。 設定方法については、「カテゴリごとに規制内容を設定する」(83ページ)を参照してください。

9. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

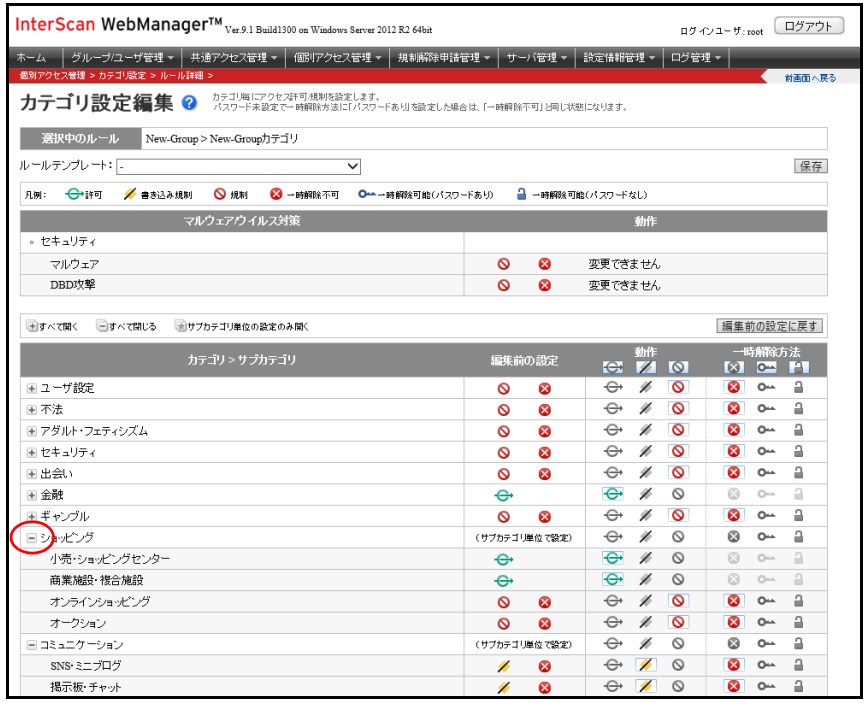
注意: [保存]ボタンをクリックしないと、変更した内容は保存されません。設定を変更する場合は、必ず[保存]ボタンをクリックしてください。

10. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

■ カテゴリごとに規制内容を設定する

カテゴリは、メインカテゴリとサブカテゴリから構成されます。
サブカテゴリごとに規制内容を設定する場合には、カテゴリ名の左にある[+]をクリックします。[-]をクリックすると、サブカテゴリの表示を隠します。



編集前の設定の列には、ルールを読み込んだ時点の設定が表示されます。
タイトル行にある規制内容アイコンをクリックすると、すべてのカテゴリの規制内容を一括して変更できます。

注意:
- サブカテゴリ単位で個別に規制内容を設定した場合、メインカテゴリには規制内容が表示されません。設定した規制内容を確認するには、サブカテゴリを表示して確認してください。
- 上位グループで、カテゴリ設定制限基準ルールが設定されている場合には、カテゴリ設定制限基準ルールの規制内容よりもゆるい規制内容は設定できません。

3-2. スケジュールを設定する

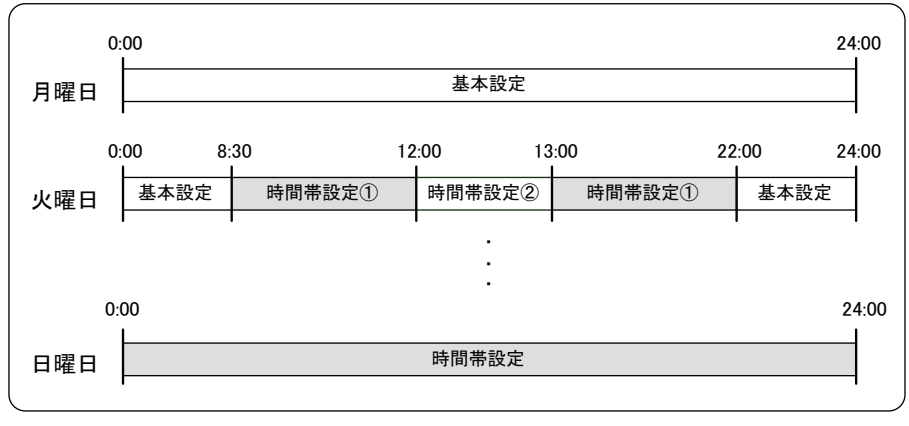
ここでは、スケジュールの設定方法について説明します。

■ スケジュール

フィルタリング対象のグループやユーザに対して、適用するカテゴリルールと、ルールを適用する時間帯を設定します。また、グループに対して、適用する例外URLルールと、ルールを適用する時間帯を設定します。
スケジュールには、デフォルトで適用される基本設定と、曜日、時間帯ごとに設定できる時間帯設定、祝日や特定の日付に適用される祝日設定の3種類があります。
新規グループ登録時点では、上位グループ(第1階層に登録した場合、ルートグループ)の基本設定が、全時間帯に適用されます。
時間帯設定により、月曜から金曜の就業時間中と就業時間外、土日の設定など、適用するカテゴリルールを詳細に設定できます。

例:
勤務時間内(時間帯設定①)には、旅行やスポーツなどの業務に関係ないカテゴリを、閲覧禁止に設定します。
また、勤務時間外(時間帯設定②と基本設定)には、業務に関係ないカテゴリを、閲覧許可に設定します。

基本設定と時間帯設定（スケジュール設定で設定）



ここでは、「第5章 グループとユーザの登録」(49ページ)で追加したグループに、時間帯設定を適用する手順を説明します。例外URL ルールの時間帯設定については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

■ スケジュールを設定する

まず、スケジュールルールを登録します。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

   [スケジュール設定]が表示されます。

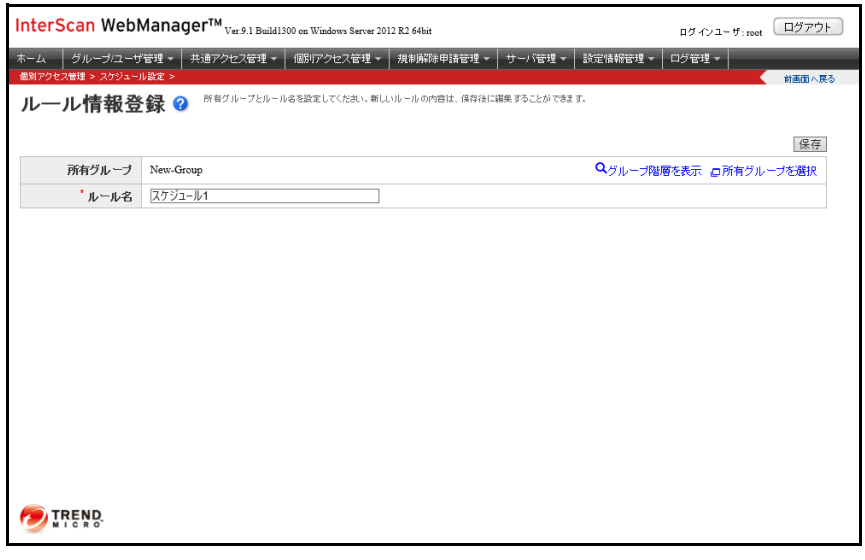
2. グループ一覧から、スケジュールを設定するグループをクリックします。

   [所有ルール一覧]が表示されます。

3. [所有ルール一覧]-[ルールを追加]をクリックします。

   [ルール情報登録]が表示されます。

4. ルール名を入力します。



所有グループ	ルールを所有しているグループ名が表示されます。
グループ階層を表示	[グループ階層を表示]をクリックすると、グループの階層がツールチップで表示されます。
所有グループを選択	[所有グループを選択]をクリックすると、[所有グループ選択]画面が別ウィンドウで表示されます。 ルールを所有するグループを変更する場合、グループを選択します。 ルールを所有するグループを変更しない場合、[閉じる]ボタンをクリックします。
ルール名(必須項目)	登録するルール名を入力します(最大半角20文字以内)。

注意: ルール名には、次の文字を使用できません。
タブ記号、半角記号(¥ / : ; ? < > | ")

5. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

6. [OK]ボタンをクリックします。

「保存が完了しました。」と表示されて、ルールが登録されます。

7. [スケジュール設定]タブの[編集]ボタンをクリックして、スケジュールを設定します。

[スケジュール設定編集]が表示されます。

注意: [個別アクセス管理]-[カテゴリ設定]で登録したカテゴリルールを適用する曜日、時間帯を設定して、スケジュールを作成します。

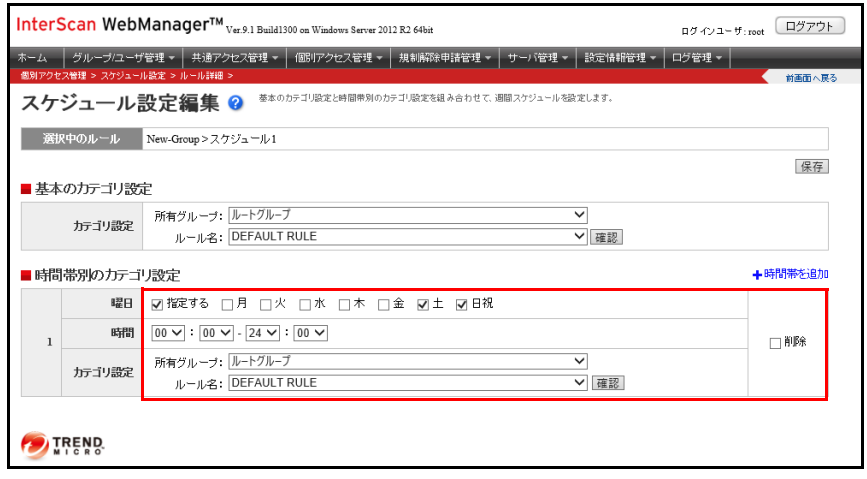
ここでは例として、「土休日」ルールを土日終日、「時間外」ルールを月～金の深夜に適用します。それ以外の時間帯は、上位グループであるルートグループの基本設定に適用された、カテゴリルールが、適用されたままとなります。

8. [時間帯別のカテゴリ設定]-[時間帯を追加]をクリックします。

[時間帯別のカテゴリ設定]に[1]の時間帯設定が追加されます。

9. [時間帯別のカテゴリ設定]の[1]で、時間帯設定を設定します。

適用する曜日、時間帯、ルールを設定します。



曜日	特定の曜日に時間帯設定を適用する場合は、[指定する]チェックボックスをオンにして、設定したい曜日をチェックします。[指定する]チェックボックスをオフにすると、すべての曜日に時間帯設定が適用されます。
時間	時間帯設定を適用する時間を設定します。
カテゴリ設定	時間帯設定として適用するカテゴリルールを所有しているグループとルール名を選択します。 [確認]ボタンをクリックすると、[カテゴリ設定]画面が別ウィンドウで表示されます。選択したカテゴリルールの規制内容を確認できます。

注意：
- 時間帯設定は0:00～24:00までの範囲で設定できます。24:00以降の設定は2つの設定に分けてください。
- 複数の時間帯設定を登録する場合、時間が重なる設定は登録できません。

ここでは例として、曜日ルールを設定します。
土曜と日曜に適用するルールとして、[指定する]チェックボックスをオンにした後、[土]チェックボックスと[日祝]チェックボックスをオンにして、[カテゴリ設定]から、適用するカテゴリルールを選択します。

10. 他の時間帯設定を適用するカテゴリルールを設定する場合には、[時間帯を追加]をクリックします。

[時間帯別のカテゴリ設定]に[2]の時間帯設定が追加されます。

11. [時間帯別のカテゴリ設定]の[2]で、時間帯設定を設定します。

適用する曜日、時間帯、ルールを設定します。

ここでは例として、月～金曜日の深夜のルールを設定します。
[指定する]チェックボックスをオンにした後、[月]チェックボックス～[金]チェックボックスをオンにして、[時間]を22:00～24:00に設定し、[カテゴリ設定]から、適用するカテゴリルールを選択します。

12. さらに他の時間帯設定を作成する場合には、手順10、11を繰り返します。

13. [保存]ボタンをクリックします。

確認のダイアログが表示されます。

14. [OK]ボタンをクリックします。

設定した内容が保存され、[ルール詳細]に戻ります。

■ スケジュールを確認する

スケジュール設定によって時間帯別にグループに適用する、カテゴリルールを確認できます。

1. [個別アクセス管理]-[スケジュール設定]をクリックします。

[スケジュール設定]が表示されます。

2. グループ一覧から、スケジュールの時間帯設定を確認するグループをクリックします。

[所有ルール一覧]が表示されます。

3. 所有ルール一覧から、スケジュールの時間帯設定を確認するルールをクリックします。

[ルール詳細]が表示されます。

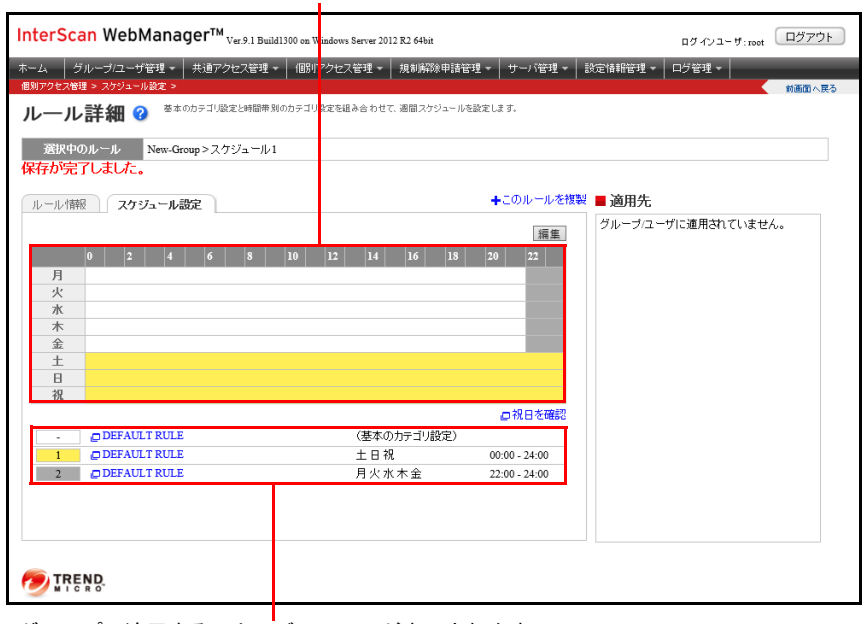
4. [スケジュール設定]タブをクリックします。

グループに適用するカテゴリルールの、時間帯別適用状況が表示されます。

5. グループに適用するスケジュール情報を確認します。

時間帯またはルールをクリックすると、[カテゴリ設定]画面が表示されます。
[カテゴリ設定]画面では、カテゴリルールの規制内容を確認できます。カテゴリルールの確認方法については、「3. カテゴリルールの確認」(46ページ)を参照してください。

曜日、時間帯別の適用スケジュールが表示されます。



グループに適用する、カテゴリルールが表示されます。

スケジュールの基本設定の変更、時間帯設定の変更/削除、祝日設定については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

4. フィルタリングルールをグループに適用する

設定したフィルタリングルールを、グループに適用します。
ここでは、設定したカテゴリルール、スケジュールルールをグループに適用する方法について説明します。

注意: グループにフィルタリングルールを適用するには、あらかじめ[個別アクセス管理]でフィルタリングルールを設定する必要があります。
カテゴリルールの設定方法については、「3-1. カテゴリルールを設定する」(80 ページ)を参照してください。
スケジュールルールの設定方法については、「3-2. スケジュールを設定する」(85ページ)を参照してください。
その他のフィルタリングルールの設定方法については、『Trend Micro InterScan WebManager v9.1 管理者ガイド』を参照してください。

4-1. カテゴリルールをグループに適用する

カテゴリルールルールをグループに適用します。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。
   [グループ管理]が表示されます。
2. グループ一覧から、フィルタリングルールを適用するグループ名をクリックします。
   設定画面にグループの設定内容が表示されます。
3. [ルール設定]タブをクリックします。
4. [適用ルール]-[カテゴリ/スケジュール設定]をクリックします。
   [カテゴリ/スケジュール設定]が表示されます。
5. [ルール選択]ボタンをクリックします。
   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

6. 適用ルールを選択します。

個別にカテゴリルールを適用する	個別にカテゴリルールを適用する場合に選択します。 選択すると、カテゴリルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したカテゴリルールの詳細が画面の下部に表示されます。 カテゴリの設定内容の詳細については、「3-1. カテゴリルールを設定する」(80ページ)を参照してください。
個別にスケジュールルールを適用する	個別にスケジュールルールを適用する場合に選択します。 「4-2. スケジュールルールをグループに適用する」(94ページ)

7. [適用]ボタンをクリックします。

   確認のダイアログが表示されます。

8. [OK]ボタンをクリックします。

4-2. スケジュールルールをグループに適用する

スケジュールルールをグループに適用します。

1. [グループ/ユーザ管理]-[グループ管理]をクリックします。

   [グループ管理]が表示されます。

2. グループ一覧から、フィルタリングルールを適用するグループ名をクリックします。

   設定画面にグループの設定内容が表示されます。

3. [ルール設定]タブをクリックします。

4. [適用ルール]-[カテゴリ/スケジュール設定]をクリックします。

   [カテゴリ/スケジュール設定]が表示されます。

5. [ルール選択]ボタンをクリックします。

   [適用ルール選択]が表示されます。

注意: 選択されたグループに「下位グループ強制参照」または「上位グループ参照」が設定されている場合は、適用ルールを変更できません。

6. 適用ルールを選択します。

個別にカテゴリルールを適用する	個別にカテゴリルールを適用する場合に選択します。 「4-1. カテゴリルールをグループに適用する」(93ページ)
個別にスケジュールルールを適用する	個別にスケジュールルールを適用する場合に選択します。 選択すると、スケジュールルールを所有しているグループ名とルールを選択することができます。[確認]ボタンをクリックすると、選択したスケジュールルールの詳細が画面の下部に表示されます。 スケジュールの設定内容の詳細については、「3-2. スケジュールを設定する」(85ページ)を参照してください。

7. [適用]ボタンをクリックします。

確認のダイアログが表示されます。

8. [OK]ボタンをクリックします。

サポートサービス

1. サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「スタンダードサポートサービスメニュー」をご覧ください。
サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。サポートセンターの連絡先は、「スタンダードサポート サービスメニュー」に記載されています。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。
サポート契約の有効期限は、ユーザ登録完了から1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意: サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

2. 製品 Q&A のご案内

トレンドマイクロのWeb サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次のURLからアクセスできます。
https://success.trendmicro.com/jp/technical-support
製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme などに記載されていない情報が必要な場合に、製品 Q&A を利用してください。
トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。