

SaaS 型セキュリティ Box

Cloud Edge あんしんプラス

ユーザーズガイド

Version 1.24

日本事務器株式会社

改版履歴

Version	日付	変更内容
1.24	2022/08/12	ポリシー アプリケーション制御機能修正 (5.6SP1)
1.23	2020/01/20	CloudEdge100 G2 接続図追加。
1.22	2019/03/06	CloudEdge50,SB 接続図修正。
1.21	2018/11/07	注意制限事項追記。
1.20	2018/08/05	Ver5.2 対応 HTTPS 通信、ビジネスメール詐欺等強化設定反映。
1.12	2017/10/20	Ver5.0SP1 対応。制限事項、URL フィルタ無効設定、その他修正。
1.11	2017/07/12	メールセキュリティ対策 SMTPS/POP3S/IMAPS 追加。
1.10	2017/04/21	Ver5.0 対応。
1.00	2015/11/20	新規作成。

目次

1. はじめにお読みください	6
1.1. 導入条件	6
1.2. 注意制限事項	8
1.3. CLOUD EDGE あんしんプラスとは	9
1.4. サービス提供概要	10
①セキュリティ機能	10
②管理機能	11
③サポート	11
2. 導入手順	12
2.1. CLOUD EDGE の設置	12
Cloud Edge50 および SB 接続方法	12
Cloud Edge100 接続方法	13
Cloud Edge100 G2 接続方法	14
機器ランプ状態	15
2.2. 管理コンソール(CLOUD CONSOLE)へログイン	16
①ログインパスワードの設定	16
②ログイン	17
3. 管理コンソール(CLOUD CONSOLE)	19
3.1. ログイン後の画面概要	19
4. ダッシュボード	20
4.1. セキュリティステータスのウィジェット	21
4.2. セキュリティステータスのウィジェットのログ閲覧方法	22
①WRS ログ確認	22
②ウイルスログ確認	23
③IPS ログ確認	24
④C&C サーバ確認	25
5. ゲートウェイ	26
6. ポリシー	29
6.1. ポリシールール	29
①設定反映について	29
②初期ポリシールール	30
③ポリシールール設定制限事項	30
6.2. ポリシー設定例	35

ケース①URL フィルタ設定	35
ケース②URL フィルタを無効にする	37
ケース③ファイアウォールルール追加<サービス一覧にある場合>	38
ケース④ファイアウォールルール追加<サービス一覧にない場合>	39
ケース⑤ファイアウォールルール新規追加<Active Directory 認証用>	41
ケース⑥アプリケーション制御	44
ケース⑦複数 Cloud Edge に異なるポリシーを適用	46
ケース⑧IP アドレス(送信元)毎に異なる Firewall Policy を適用	50
6.3. インタフェースオブジェクト	54
6.4. アイデンティティオブジェクト	54
①IP アドレス/FQDN	54
②MAC アドレス	55
③ジオロケーション	55
6.5. 他のオブジェクト	56
①サービス	56
②スケジュール	58
6.6. コンテンツタイプオブジェクト	59
①アプリケーショングループ	59
②URL カテゴリグループ	60
6.7. 許可/ブロックリスト	61
6.8. セキュリティプロファイル	62
①IPS(侵入防御)	63
②不正プログラム対策	64
③メールセキュリティ対策	65
④Web レピュテーション	69
⑤HTTPS 復号	70
⑥DoS 対策	72
⑦エンドポイント識別	73
6.9. ユーザ通知	74
7. 分析とレポート	75
7.1. ログ分析	75
①アプリケーション帯域幅	76
②ポリシー施工	77
③インターネットアクセス	78
④インターネットセキュリティ	79
7.2. お気に入りログ	80
7.3. レポート	81
8. 管理	83

8.1. 管理項目	83
8.2. 監査ログ	84
8.3. 証明書管理	85
①HTTPS 復号証明書の再生成.....	85
②Cloud Edge 証明書のインストール	86
③HTTPS サイトのブラウザ表示.....	88

1. はじめにお読みください

本ユーザーズガイドは、Cloud Edge あんしんプラス(以下「本サービス」と称す)」の個別設定について記載いたします。詳細な設定内容については別途管理コンソールのオンラインヘルプをご確認ください。

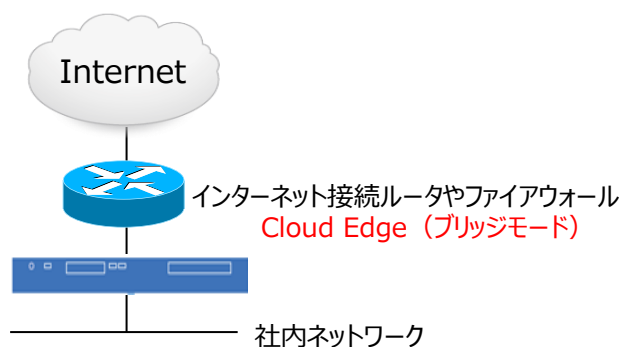
1.1. 導入条件

(1) 本サービスで利用するセキュリティ Box(以下 Cloud Edge と称す。)はインターネットへの接続が必要です。運用には ポート TCP80(HTTP)、443(HTTPS)、UDP53(DNS)、123(NTP)を使用します。

(2) IPv6 は一部セキュリティ機能が対応しています。(Web レピュテーションや IPS、不正プログラム対策等) 詳細はヘルプをご確認ください。

Cloud Edge 自体のネットワーク設定は IPv6 に対応していません。

(3) ブリッジモード(L2 モード)の場合、Cloud Edge はインターネット接続ルータやファイアウォールの社内側へ設置します。



(4) ブリッジモード(L2 モード)の場合、リモートアクセスやサイト間 VPN 機能は利用できません。

(5) ポリシー設定について

初期設定でセキュリティ機能は全て有効になっており、一般的に利用されるアプリケーションポートが許可された状態になっているため、カスタマイズを行わなくても設置するだけですぐに保護が有効になります。URL フィルタやアプリケーション制御、アプリケーションポートの解放が必要な場合、利用環境に合わせたカスタム設定を行っていただくために、本ユーザーズガイドやヘルプを参考にしてください。

(6)Cloud Edge BOX 通信先一覧

接続先	ポート	接続先 URL
アプライアンス管理サーバ	443	https://prod-devmgmt01.cloudedge.trendmicro.com
ログサービス	443	https://prodlogrecv.cloudedge.trendmicro.com
クラウド検索サービス	80	http://proxy-ce-jp.iws.trendmicro.com
クラウドメール検索サービス (CMS、CEMS)	443	https://*.cms.trendmirco.com
		https://prodcems.cloudedge.trendmicro.com
スマートスキャンサービス	443	https://ce55.icrc.trendmicro.com
Web レピュテーションサービス	80	http://ce5-0sp1-en.url.trendmicro.com
	443	https://ce5-0sp1-en.url.trendmicro.com
アップデートサービス	443	https://*.activeupdate.trendmicro.com
Firmware アップデートサーバ	443	https://rel-s3-skynetmsp-firmware-an.s3.amazonaws.com
インターネットアクセス確認	80	http(s)://www.trendmicro.com
		http(s)://www.apple.com
	443	http(s)://www.amazon.com
		http(s)://www.google.com
Geo IP サービス	443	https://rel-s3-skynetmsp-geolocation-an.s3.amazonaws.com
デバイス検出サービス	443	https://rel-s3-skylake-iot-an.s3.amazonaws.com
Cloud Edge Cloud Console	443	https://console.cloudedge.trendmicro.com

1.2. 注意制限事項

(1) 管理者への通知機能

管理者への通知機能は以下になります。

- ・ゲートウェイステータスの変更(オフライン、オンライン復帰)
- ・メールセキュリティステータスの変更(クラウドスキャンが行えずローカルスキャンに切り替わった場合)
- ・C&C コールバック(C&C 通信をブロックした回数が閾値を超えた場合)

(2) Web サイト(HTTPS) やメール(IMAPS、POPS、SMTPS) の保護された通信を Cloud Edge で検査する場合

HTTPS 復号機能を有効にする必要があります。

また HTTPS 復号機能を有効にした場合、Cloud Edge の自己署名ルート CA 証明書をお使いのブラウザやメールクライアントにインストールする必要があります。

HTTPS 複合を有効にするには 6.5⑤HTTPS 複合を参照ください。

メール(IMAPS、POPS、SMTPS)を検査するには 6.5③詳細設定を参照ください。

CA 証明書については 8.3 証明書管理を参照ください。

(3) クラウドサンドボックスオプションご利用の場合

仮想アナライザの有効化を「オン」に設定してください。

管理コンソールより

ポリシー>セキュリティプロファイル>初期設定のプロファイル(利用しているプロファイル)

>メールセキュリティ対策タブ

仮想アナライザの有効化をオンにし、設定を保存後「すべて配信」で反映します。

【補足】

Cloud Edge バージョン 5.2 以降(2018 年 8 月 5 日配信)では

HTTPS 復号機能を有効にしていなくても、URL のホスト名でカテゴリが判定できる通信に関しては、URL フィルタ、Web レピュテーションで不正な HTTPS サイトをブロックすることが可能になります。

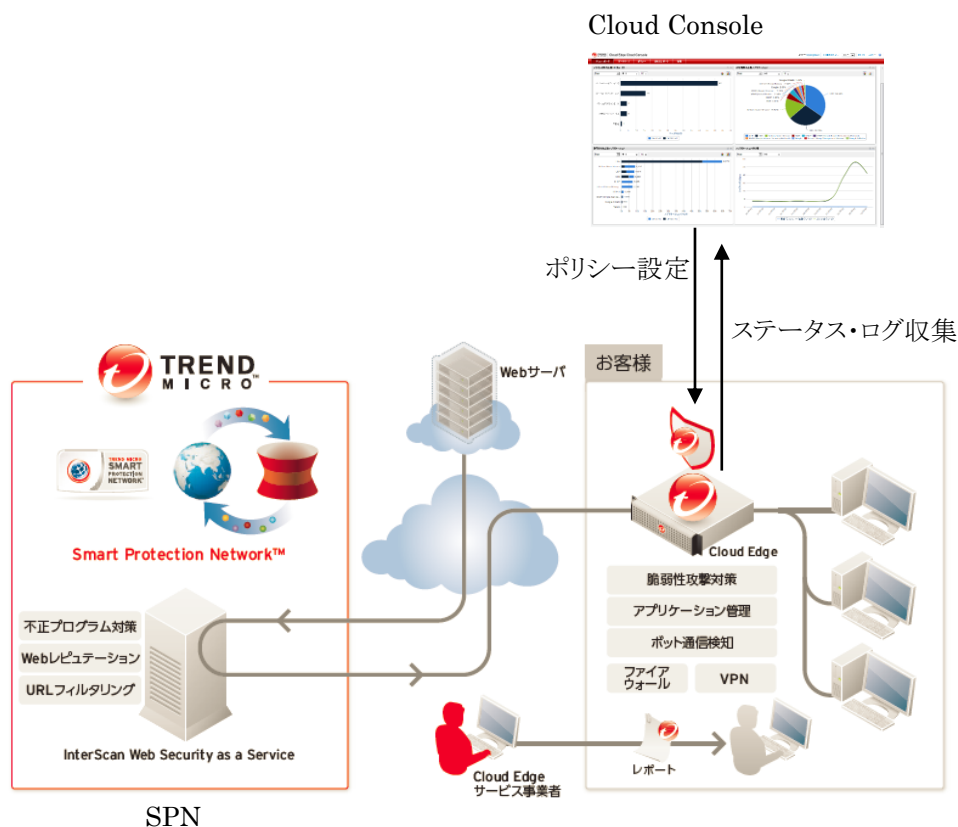
※HTTPS 復号を利用する場合に比べ機能は劣りますが、HTTPS 通信に対する強化が行われています。

1.3. Cloud Edge あんしんプラスとは

本サービスは、「Trend Micro Cloud Edge」をベースとした SaaS 型サービスです。『脆弱性をついた攻撃』や『遠隔操作』『情報漏えい』等、新しい課題に対応できるソリューションです。

インターネット接続ルータの直下に設置し入口、出口対策として機能します。

「サービスイメージ」



Cloud Edge には IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS のみ設定されており、ポリシー設定やログ確認は全てクラウド上の Cloud Console にて行います。

1.4. サービス提供概要

①セキュリティ機能

(1) 不正プログラム対策

オンプレミスでのエンジン検索とクラウドデータを利用した検索を使い分け、高い検出力を維持しながら高いスループットを実現。

(2) Web レピュテーション (WRS)

SPN (16 億 URL) を利用して接続 URL をリアルタイムに評価し不正サイトをブロック。

(3) URL フィルタ

約 80 のカテゴリで制御。

ブラックリスト/ホワイトリストの設定も可能。

(4) ボット通信検知と防御

SPN と NCIE エンジン (ネットワーク通信検査エンジン※ローカル) による C&C 通信防御。

(5) 不正侵入防御 (IPS)

DPI (Deep Packet Inspection) エンジンと 6500 を超えるルールによる脆弱性対策。

対応 OS

Windows、WindowsMobile、Linux、FreeBSD、Symbian、Solais、MacOS、Android、iOS

(6) アプリケーション制御

日本独自のアプリケーションを含む 1,000 以上のアプリケーションをサポート。一部アプリケーションでは機能単位での制御も可能。

ex.) Facebook の投稿のみブロックや Dropbox のファイルアップロードをブロックなど

(7) ファイアウォール

攻撃のみをブロックし、適切なアプリケーショントラフィックだけを通過させる次世代のファイアウォール機能を提供します。

(8) メールセキュリティ

ERS (Email Reputation Service) とオンプレミスのエンジンを利用し、不正プログラム付きメール、スパムメールをブロックまたはタグ付け。コンテンツフィルタリングにより不適切なメールを検知。

対応プロトコル: SMTP(S)、POP3(S)、IMAP(S)

②管理機能

管理コンソール (Cloud Edge Cloud Console)

全ての管理はクラウド上の管理コンソールから一元的に行なうことができ、管理面での負荷を低減する事ができます。また、Cloud Edge とクラウド上の管理コンソール間の通信は暗号化によりセキュアに保たれます。

③サポート

(1) ヘルプデスク

本サービスに関するお問い合わせを電話または e メールにて対応します。

サポート受付内容

- ・設置に関するお問い合わせ
- ・管理コンソールの操作方法に関するお問い合わせ
- ・C&C 接続検知など

(2) ハードウェア保守

ハードウェア故障と判断された場合、先出 SEND BACK にてハードウェアを提供します。

(3) 監視サービス

お客様サイトでの運用状況を監視し、以下のインシデント発生時には、状況の連絡および対処方法についてお客様を支援します。

- ・ハードウェア死活監視
- ・リソース監視 (CPU、メモリ、ディスク)
- ・ボットネット接続検知 (C&C サーバ接続)

(4) ファームウェアアップデート

ファームウェアバージョンアップおよび Hotfix がリリースされた場合にリモートで Cloud Edge のファームウェアアップデート作業を行います。

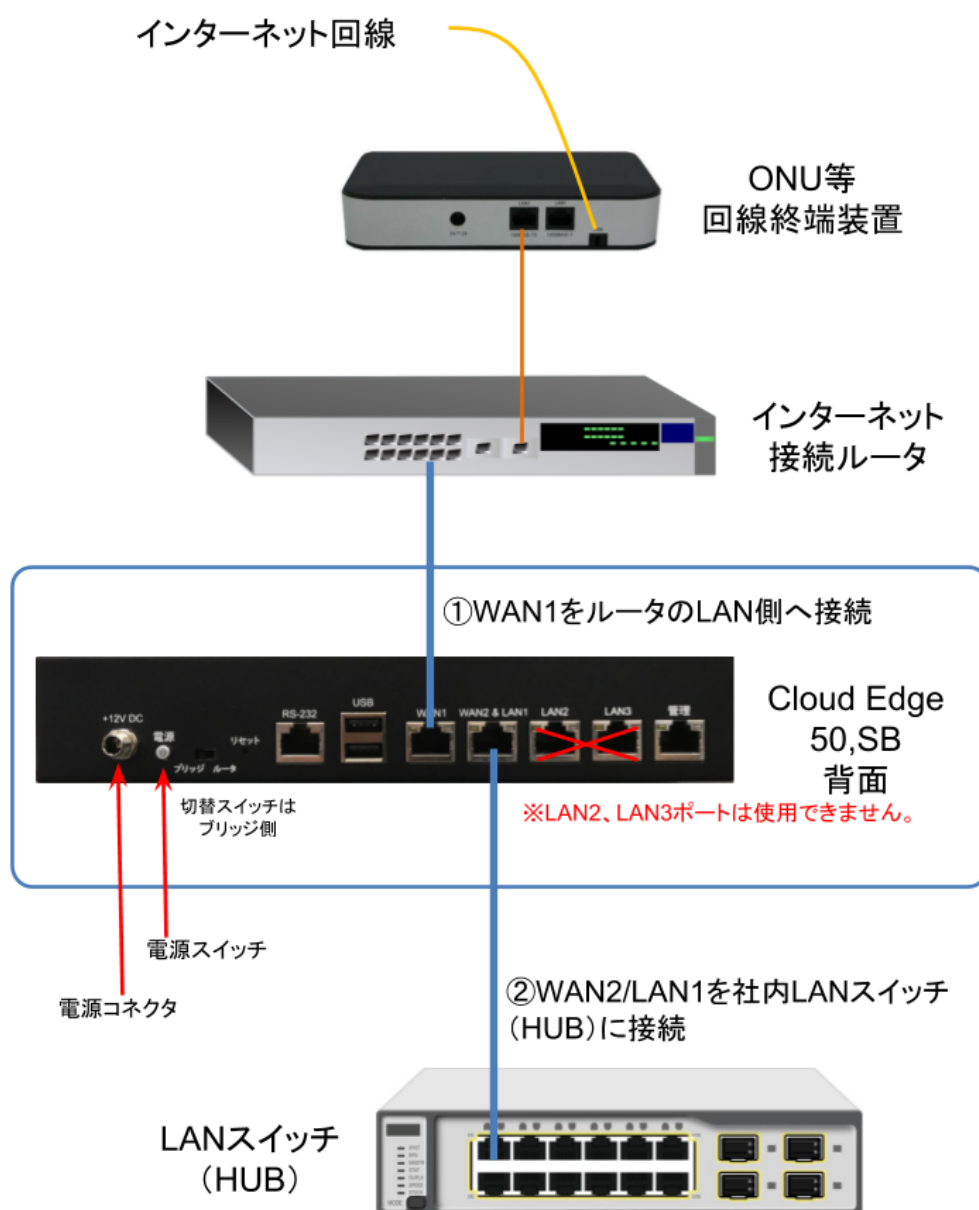
2. 導入手順

サービス利用開始について説明いたします。

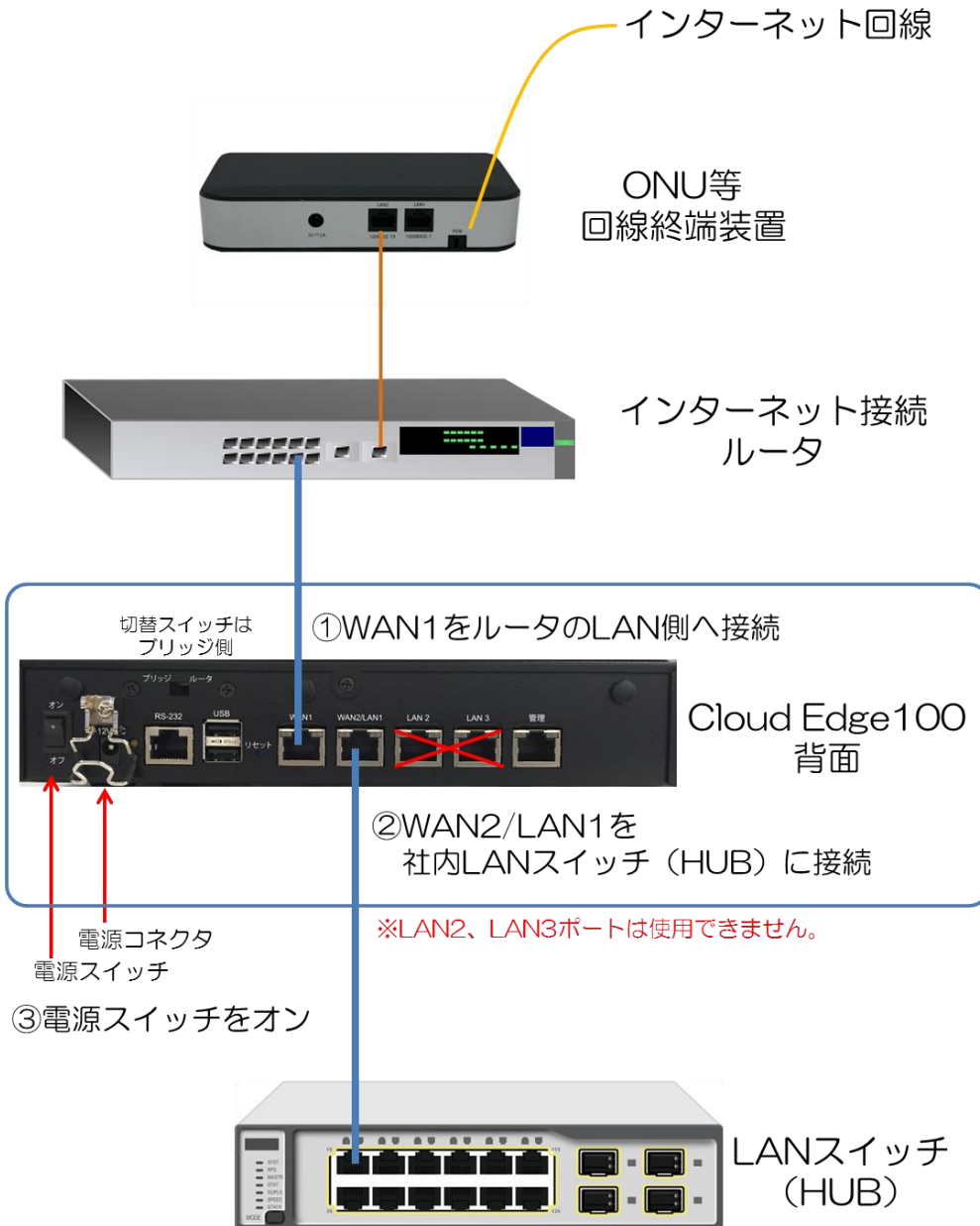
2.1. Cloud Edge の設置

■ Cloud Edge をネットワークに接続します。

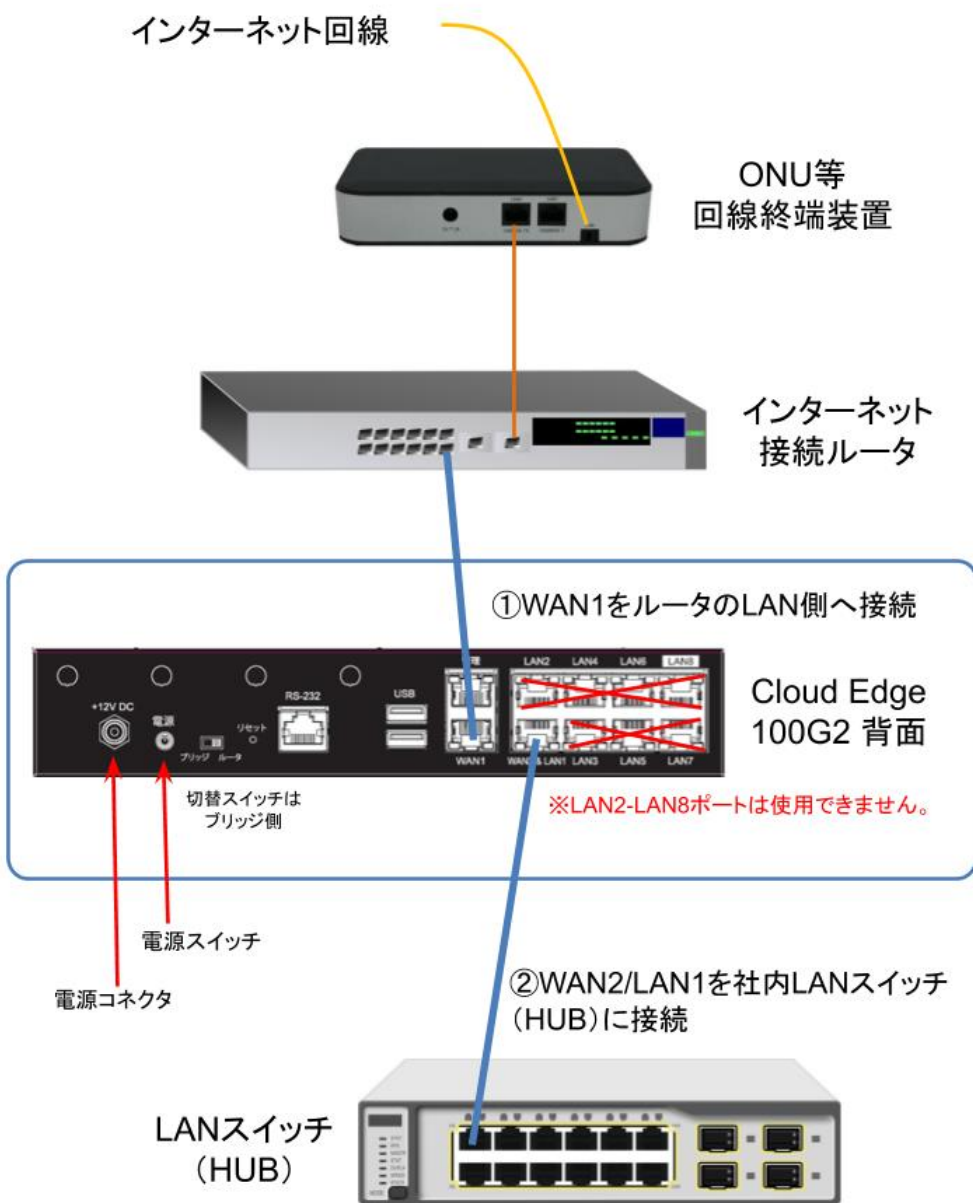
Cloud Edge50 および SB 接続方法



Cloud Edge100 接続方法

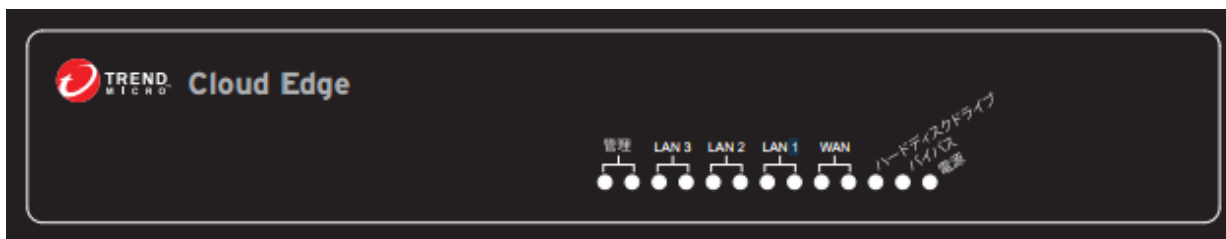


Cloud Edge100 G2 接続方法



機器ランプ状態

■前面



○正常時

- ・電源点灯
- ・WAN1: 左点灯 / 右点滅 (通信データありの時)
- ・WAN2/LAN1: 左点灯 / 右点滅 (通信データありの時)
- ・ストレージ: 点滅 (起動時や通信データありの時)
 - WAN1 および WAN2/LAN1 の左側ランプ
 - 100Mbps リンク時: オレンジ
 - 1000Mbps リンク時: グリーン

×不具合時

正常時のランプが点灯していない。

バイパスランプが付いている。(故障時)

設置完了後、正常稼働確認のためサポートセンターへご連絡ください。

2.2. 管理コンソール(Cloud Console)へログイン

本サービス契約、または評価版のお申込み完了後、新規のお客様のみアカウント登録完了メールがお客様へ送付されます。

件名:[通知] あんしんプラス アカウント登録完了のお知らせ

管理コンソールに接続するためには、アカウント登録完了メールに記載されているログイン ID と設定したパスワードが必要になります。

※すでにあんしんプラスシリーズをご利用のお客様に登録完了メールは届きません。ご利用中のあんしんプラスと同じ管理コンソールよりログインしてください。

アカウント登録完了メール

このメールには重要な情報が記載されています。大切に保管してください。

また、このメッセージは登録システムによって自動的に作成されたメールです。

本メールに対するメッセージの返信は受け付けておりませんので、あらかじめご了承ください。

=====

プラス株式会社 様

アカウントの登録が完了しました。すぐにサービスをご利用できます。

【ログイン ID】

pfs1-zzz00001

【パスワード】

はじめに次の URL をクリックし、パスワード発行の手続きを行ってください。

<https://Forgetpwd.trendmicro.com/ForgetPassword/ResetPassword?T=29560842&v=883c2474-6bb5-485c-a3f1-3c79000>

※この URL は 7 日間のみ有効です。

サービスを利用するには、下記の URL からログインしてください。

* ログイン URL:<https://clp.trendmicro.com/Dashboard?T=295608453>

※上記 URL はサンプルです。お客様へ送信されたアカウント登録完了メールに記載されている URL からログインしてください。

①ログインパスワードの設定

まず初めに管理コンソールへログインするためのパスワードを設定します。

「はじめに次の URL をクリックし、パスワード発行の手続きを行ってください。」の URL をクリックするとパスワードのリセット画面が表示されます。パスワードを入力後「送信」をクリックしてください。

パスワードのリセット

ログインIDを確認して新しいパスワードを入力してください。

ログインID: pfsi-zzz00001

新しいパスワード:

パスワード確認:

送信

以上でパスワードの設定は完了です。

「送信」をクリックすると管理コンソールへのログイン画面を表示します。

また、アカウント登録完了メールのログイン URL から管理コンソールへのログイン画面を開けます。

②ログイン

アカウント登録完了メールに記載されているアカウント及び最初に設定したパスワードを入力してログインをクリックしてください。

登録情報を入力してください

アカウント:

パスワード:

[パスワードのリセット \(パスワードをお忘れの場合\)](#)

アカウント名を記憶する

ログイン

アカウントをまだ取得していない場合 [今すぐ登録](#)

(1) プライバシーポリシーの確認画面が表示されます。

個人情報の取り扱いに同意した上で先に進んでください。

※最初のログイン時のみ表示されます。

プライバシーポリシー

(1) 氏名、会社名、住所、電話番号、メールアドレス等、お客様が本サービスを利用する際に提供される個人情報
(2) 購入製品、ユーザ登録日、契約の更新状況、対応の振込に關連して開示

2. 当社は、コンピュータまたはインターネットに關連するセキュリティ対策製品
(1) サポートサービスの提供
(2) 契約の更新案内
(3) 当社の製品およびサービスに關する案内
(4) 当社の製品およびサービスに關連する他社製品の案内
(5) セキュリティに關する情報の提供
(6) アンケート調査ならびにキャンペーン、セミナーおよびイベントに關する案内
(7) 当社の製品またはサービスの開発を目的とした分析および調査ならびに

3. 当社は、前項の各行為を実施するにあたり、秘密保持契約を締結する

4. お客様は、当社に対し、自己に關する客観的な事実に基づく個人情報に關

OK

(2)ご契約中のサービス内容が表示されます。

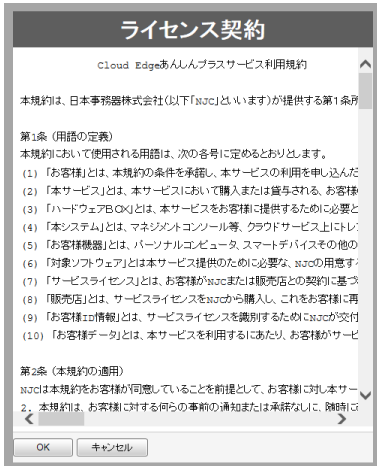
先に進む場合は、Cloud Edge あんしんプラスの「コンソールを開く」をクリックします。

※「キーを入力」は本サービスで使用しません

(3)ライセンス契約の確認画面が表示されます。

利用規約に同意した上で先に進んでください。

※最初のログイン時のみ表示されます。



(4)ログインに成功すると管理コンソールのダッシュボードが開き、セキュリティステータスやトラフィックステータスを確認する画面が表示されます。



3. 管理コンソール (Cloud Console)

管理コンソールについて説明いたします。

3.1. ログイン後の画面概要

ダッシュボード:

1 つまたは複数の Cloud Edge におけるネットワーク活動を表示します。ウィジェットに情報がグラフの形式で視覚的に示され、脅威の追跡情報を確認したり、集約されたログ統計と関連付けて確認したりできます。

ゲートウェイ:

Cloud Edge のハードウェア情報などを確認することができます。

ポリシー:

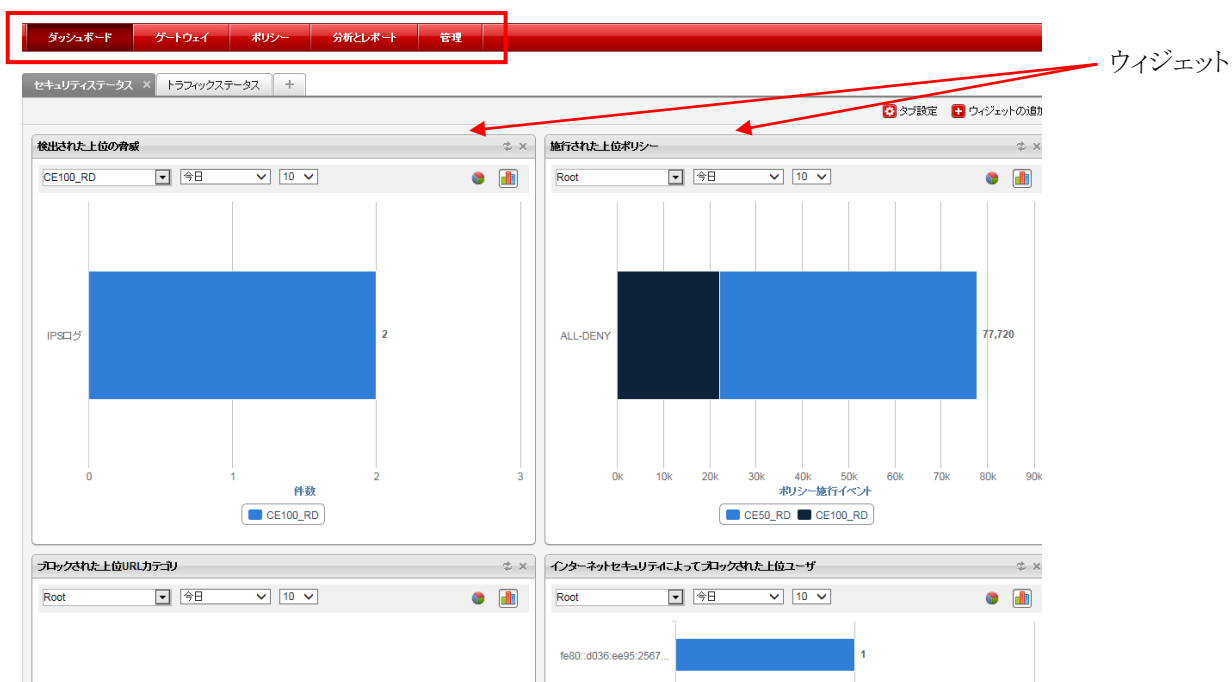
Cloud Edge を通過するトラフィックを制御するポリシールールを管理します。

分析とレポート:

アプリケーションの帯域幅の消費、ネットワークトラフィックへのポリシーの適用、アクセスされた Web サイトやドメイン、検索エンジンの有効性を確認および分析します。

管理:

HTTPS 復号証明書を利用する場合に使用します。※証明書管理以外は設定変更されないようお願いします。

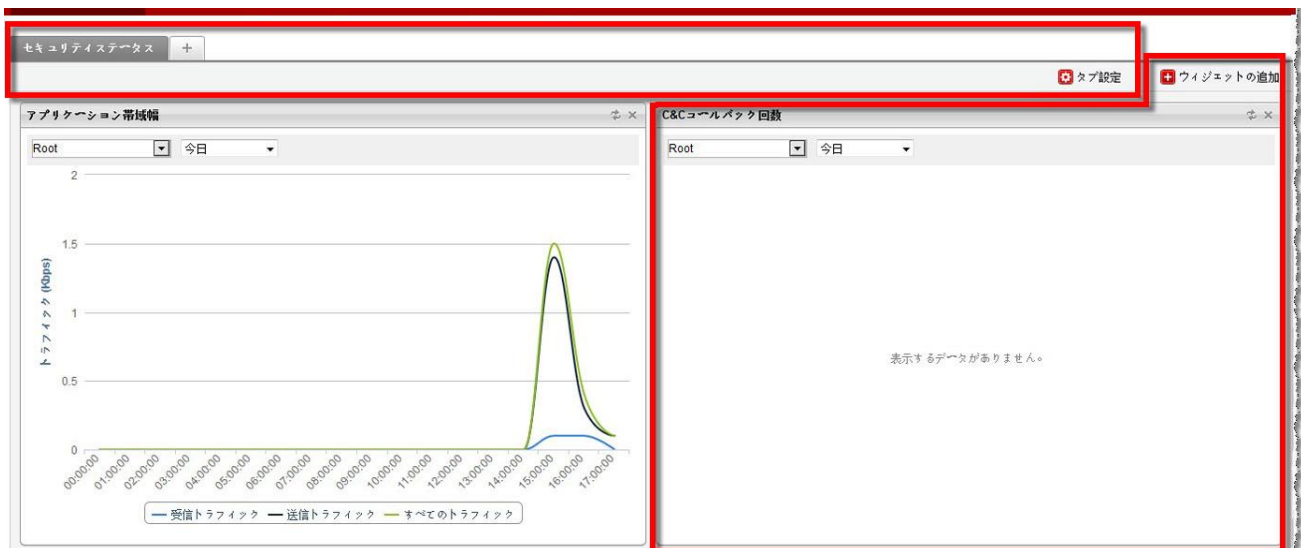


4. ダッシュボード

ダッシュボードについて説明いたします。

1 つまたは複数の Cloud Edge におけるネットワーク活動を表示します。ウィジェットに情報がグラフの形式で視覚的に示され、脅威の追跡情報を確認したり、集約されたログ統計と関連付けて確認したりできます。

ダッシュボードは次のユーザインタフェース要素で構成されます。



・タブ

タブはダッシュボードを管理するための単位であり、1 つのタブに複数のウィジェットを配置することができます。それぞれのタブの中に複数のウィジェットをまとめることができます。タブやウィジェットを追加または変更することで、必要に応じてダッシュボードをカスタマイズできます。ダッシュボードでサポートされるタブの数は 10 個までです。各タブには、最大 10 個のウィジェットを含めることができます。

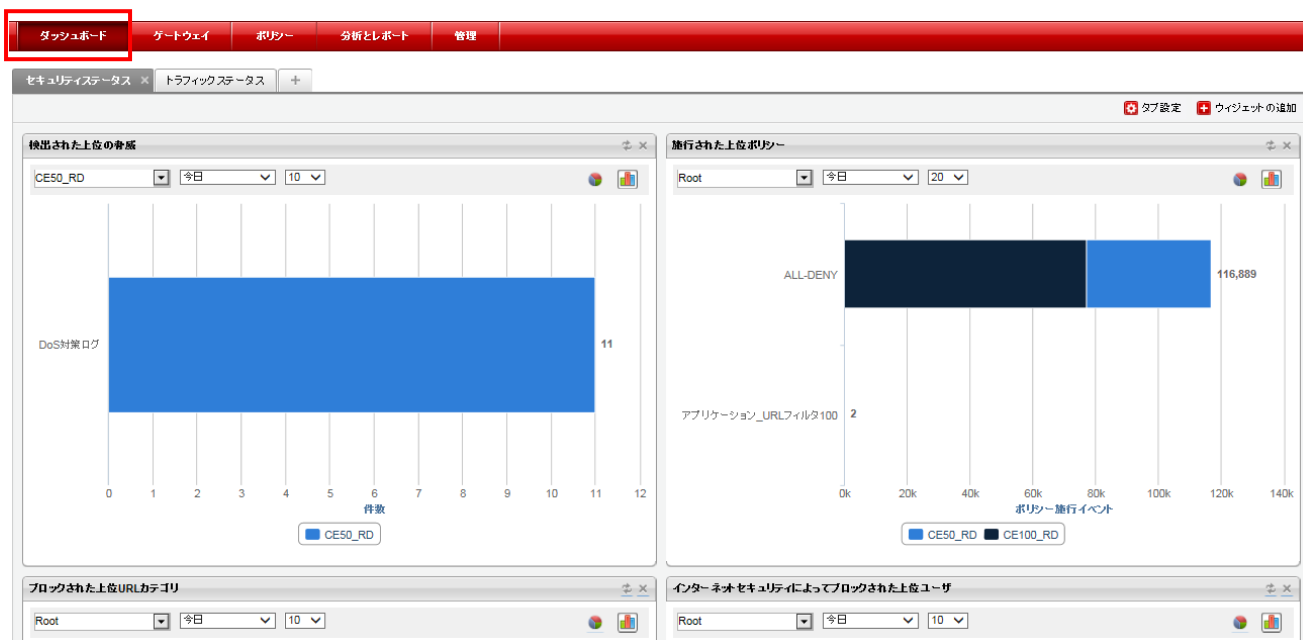
・ウィジェット

ウィジェットはダッシュボードのコアコンポーネントです。ウィジェットでは、情報がグラフの形式で視覚的に示され、脅威の追跡情報を確認したり、1 つまたは複数の Cloud Edge から集約したログ統計と関連付けて確認したりできます。ウィジェットでの情報の表示方法は、ダッシュボードのウィジェットフレームワークで選択できます。ウィジェットでデータポイントをクリックした後、フィルタを選択してそのフィルタに関連する活動を調べたり、[ログの表示] をクリックしてそのログカテゴリに関連する活動を調べたりできます。

4.1. セキュリティステータスのウィジェット

セキュリティステータスカテゴリのウィジェットでは、選択した期間（現在の時刻まで）に検出された脅威がファイアウォール、ウイルス、WRS、URL フィルタ、スパムメール、およびブラックリストに追加する URL ごとに分類されて表示されます。セキュリティステータスカテゴリのウィジェットを次に示します。

※セキュリティステータスはブロックした件数を表示します。



C&C コールバック回数

検出された上位の脅威*

ブロックされた上位アプリケーション

実行された上位ポリシー*

ブロックされた上位 URL カテゴリ*

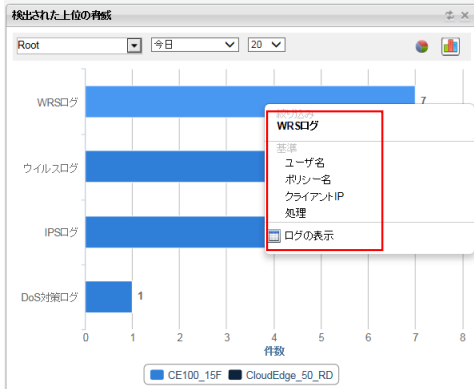
インターネットセキュリティによってブロックされた上位ユーザ*

* 初期設定で表示されるウィジェット

4.2. セキュリティステータスのウィジェットのログ閲覧方法

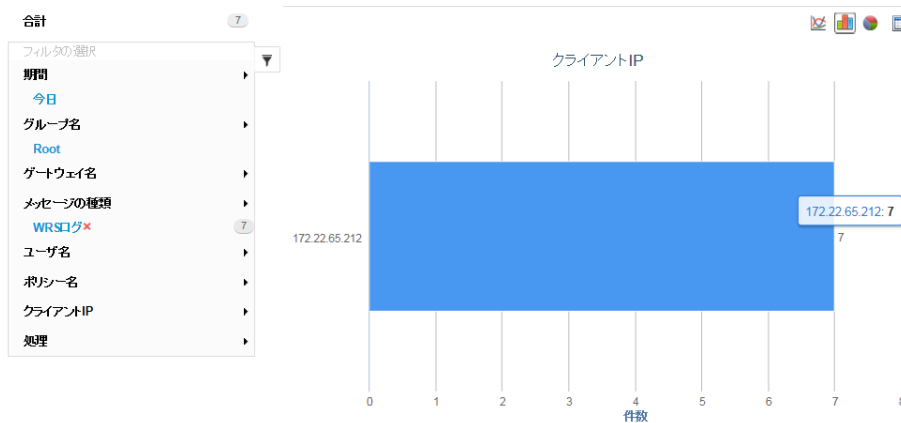
①WRS ログ確認

WRS ログのグラフをクリックし、クライアント IP を選択します。「ログの表示」でいきなりログ表示でも可能です。



WRS でブロックされたクライアント IP を表示します。

グラフをクリックしログの表示を選択します。



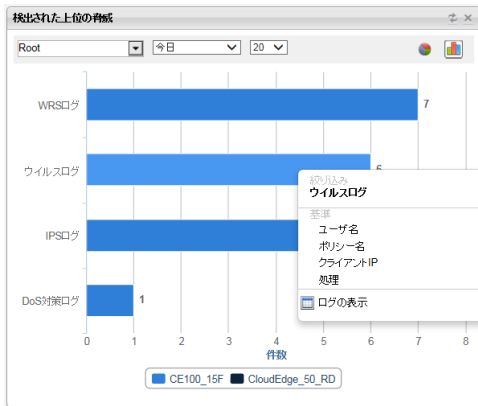
対象のクライアントで検出したログを表示します。

左側メニューより期間指定やクライアント IP からの検索もできます。

時間	メッセージの種類	ユーザ名	URL	クライアントIP	サ-
2015-09-30 15:49:25 JST+0900	WRSログ	172.22.65.212	http://www.eicar....	172.22.65.212	18%
2015-09-30 15:49:23 JST+0900	WRSログ	172.22.65.212	http://www.eicar....	172.22.65.212	18%
2015-09-30 15:49:20 JST+0900	WRSログ	172.22.65.212	http://www.eicar....	172.22.65.212	18%
2015-09-30 15:49:17 JST+0900	WRSログ	172.22.65.212	http://www.eicar....	172.22.65.212	18%
2015-09-30 15:48:58 JST+0900	WRSログ	172.22.65.212	http://www.eicar....	172.22.65.212	18%

②ウイルスログ確認

ウイルスログのグラフをクリックし、ログの表示を選択します。



検出したログを表示します。

左側メニューより期間指定やクライアント IP からの検索もできます。

合計 6

フィルタの選択

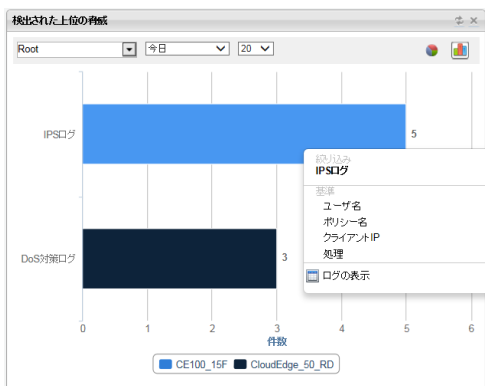
- 期間
 - 今日
- グループ名
 - Root
- ゲートウェイ名
- メッセージの種類
 - ウイルスログ*
- ユーザ名
- ポリシー名
- クライアントIP
- 不正プログラム名
- 処理

CSV形式にエクスポート 列の選択

時間	メッセージの種類	ユーザ名	URL	クライアントIP	サーバIP	不正プログラム名
2015-09-30 15:50:51 JST+0900	ウイルスログ	172.22.65.212	http://www.e...	172.22.65.212	188...	Eicar_test_file
2015-09-30 15:50:45 JST+0900	ウイルスログ	172.22.65.212	http://www.e...	172.22.65.212	188...	Eicar_test_file
2015-09-30 15:50:41 JST+0900	ウイルスログ	172.22.65.212	http://www.e...	172.22.65.212	188...	Eicar_test_file
2015-09-30 15:50:37 JST+0900	ウイルスログ	172.22.65.212	http://www.e...	172.22.65.212	188...	Eicar_test_file
2015-09-30 15:50:23 JST+0900	ウイルスログ	172.22.65.212	http://www.e...	172.22.65.212	188...	Eicar_test_file
2015-09-30 15:50:22 JST+0900	ウイルスログ	172.22.65.212	http://www.e...	172.22.65.212	188...	Eicar_test_file

③IPS ログ確認

IPS ログのグラフをクリックし、ログの表示を選択します。



検出したログを表示します。

左側メニューより期間指定やクライアント IP からの検索もできます。

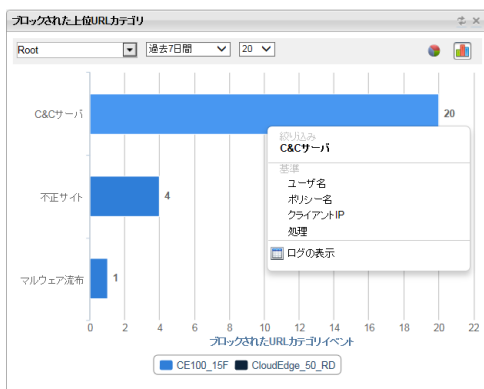
ブロックした IPS ルールも表示されます。

メッセージの種類	ユーザー名	URL	クライアントIP	サーバIP	不正プログラム名	IPSルール
IPSログ	172.2...	http://gendai.i...	172.22.65.212	210.1...	--	EXPLOIT Microsoft Windows Kodak Image Viewer Code Execution (CVE-2007-2217) -1
IPSログ	172.2...	http://gendai.i...	172.22.65.212	210.1...	--	EXPLOIT Microsoft Windows Kodak Image Viewer Code Execution (CVE-2007-2217) -1
IPSログ	172.2...	http://manga...	172.22.65.212	203.1...	--	EXPLOIT Microsoft Windows Kodak Image Viewer Code Execution (CVE-2007-2217) -2
IPSログ	172.2...	http://gendai.i...	172.22.65.212	210.1...	--	EXPLOIT Microsoft Windows Kodak Image Viewer Code Execution (CVE-2007-2217) -1
IPSログ	172.2...	http://gendai.i...	172.22.65.212	210.1...	--	EXPLOIT Microsoft Windows Kodak Image Viewer Code Execution (CVE-2007-2217) -1
IPSログ	172.2...	clients6.googl...	172.22.65.212	216.5...	--	WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)
IPSログ	172.2...	clients6.googl...	172.22.65.212	173.1...	--	WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)

IPS ルールにより脆弱性を悪用するような通信と認識された場合は Cloud Edge によってブロックします。

④C&C サーバ確認

C&C サーバのグラフをクリックし、ログの表示を選択します。



検出したログを表示します。

左側メニューより期間指定やクライアント IP からの検索も可能です。

時間	メッセージの種類	ユーザ名	URL	クライアントIP	サーバIP	ドメイン	プロトコル処理	URLカテゴリ	アプリID	処理	ポリシー名
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...
20...	URLフィルタログ	172.2...	http://103.19...	172.22.65.212	103.1...	10...	-	C&Cサーバ	HTTP	ブロック	アプリ...

5. ゲートウェイ

ゲートウェイについて説明いたします。

Cloud Edge の状態やステータスを確認することができます。



ゲートウェイ名をクリックすると「一般」タブにてインターフェースや IP アドレス、バージョン情報などを表示します。



「ステータス」タブ。ハードウェアのリソースおよび温度情報を表示します。

- CPU 使用率
- メモリ使用率
- HDD の使用率
- 筐体温度 (CPU の温度)

※Cloud Edge のハードウェアがオフライン状態でも、過去七日間のステータスを確認することができます。

※オフライン期間のデータは表示されません。



「ログ/イベント」タブ。システムイベントやネットワークイベントを確認することができます。

The screenshot shows the 'ログ/イベント' (Log/Event) tab. It displays a table of system events with filters for 'システムイベント' (System Event) and '過去7日間' (Last 7 days). The table has columns for '日付時刻' (Date/Time), 'クライアントIP' (Client IP), 'サブカテゴリ' (Sub-category), 'イベント' (Event), and 'メッセージ' (Message).

日付時刻	クライアントIP	サブカテゴリ	イベント	メッセージ
2019-12-25 04:27:52 +0900		Service	dpid	サービスが開始しました。
2019-12-25		Service	dpid	サービスが停止しました。

「ツール」タブ。Ping、Traceroute、ARP を実行、表示できます。

ダッシュボード ゲートウェイ ポリシー 分析とレポート 管理

ゲートウェイ > CloudEdge50

ゲートウェイ情報

ネットワーク ▾

- インタフェース
- 管理アクセス
- DHCP
- ルーティングテーブル

帯域幅制御

エンドユーザ管理 ▾

- 一般設定

アップデート

ネットワークアクセスコントロール ▾

- VBSSエンドポイント保護

ゲートウェイ情報

一般 ステータス ログイベント ツール

次のツールを使用して、ネットワーク接続の問題に関するトラブルシューティングを行います。

Ping Traceroute ARP

ドメイン/IP

ドメインまたはIPの入力

Pingを送信するネットワークインタフェースを選択します バイト数 件数

すべて 56 4

Ping

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=32.3 ms

6. ポリシー

ポリシーについて説明します。

6.1. ポリシールール

アプリケーション/URL フィルタ、サービス(アプリケーションで利用されるポート)に関する設定を行えます。初期設定にてセキュリティ機能が有効化されており、インターネットで一般的に利用されるサービスの通信が許可されています。また、フィッシングサイトや C&C サーバなど不正なサイトはブロックする URL フィルタが設定されています。これらは必要に応じて設定変更することができます。

セキュリティポリシーは、汎用的なものから限定的なものまで、必要に応じてさまざまなレベルで設定できます。ポリシールールは受信トラフィックに対して順番に照合され、トラフィックに一致する最初のルールが適用されるため、限定的なルールから汎用的なルールの順に照合する必要があります。たとえば、単一のアプリケーション向けのルールは、トラフィックに関する他の設定がすべて同じ場合に適用するすべてのアプリケーション向けのルールよりも先に照合する必要があります。

①設定反映について

設定を変更した場合は「すべて配信」をクリックしてください。設定が Cloud Edge に反映されます。



設定配信に成功すると緑色のレが表示されます。※配信に失敗した場合は再度「すべて配信」を実行してください。



②初期ポリシールール

4 つのルールが初期設定で割り当てられています。ルールは上から順に照合され ALL-DENY の上位ルールに該当しない通信は ALL-DENY で全てブロックされます。

※ファイアウォール機能を使わない場合は Firewall Policy (許可) と ALL-DENY (ブロック) は無効で出荷されます。

- (1) アプリケーション_URL フィルタ (ブロック※不正サイト)
- (2) Firewall Policy (許可※一般的によく使われているポート)
- (3) ALL-DENY (ブロック)

- (4) 初期設定のポリシールール (許可)

※「初期設定のポリシールール」全て許可ルールは変更、削除できません。

ポリシールールの管理									
追加 編集 削除 移動 その他 フィルタの適用 <input type="text" value="検索"/>									
ポリシー名	ゲートウェイ...	インタフェース...	IDオブジェクト	サービス	コンテンツタイプ	スケジュール	処理	セキュリティプロファイル	
		FRM → TO	SRC → DST						
ポリシールール									
<input type="checkbox"/>	<input checked="" type="checkbox"/> アプリケ...	すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	SVC す...	APP すべて URL Others,M...	常時	<input checked="" type="radio"/> ブロック	
<input type="checkbox"/>	<input checked="" type="checkbox"/> Firewall P...	すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	SVC D...	APP すべて URL すべて	常時	<input checked="" type="radio"/> 許可	
<input type="checkbox"/>	<input checked="" type="checkbox"/> ALL-DENY	すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	SVC す...	APP すべて URL すべて	常時	<input checked="" type="radio"/> ブロック	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 初期設定...	すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	<input checked="" type="radio"/> すべて ↳ <input checked="" type="radio"/> すべて	SVC す...	APP すべて URL すべて	常時	<input checked="" type="radio"/> 許可	

③ポリシールール設定制限事項

ポリシールール追加・編集画面の「インタフェースオブジェクト」および「セキュリティプロファイル」の設定は利用できません。

優先順位1 ポリシー名:アプリケーション_URL フィルタ 【ブロック】

アプリケーション制御や URL フィルタを設定変更する場合はルール名「アプリケーション_URL フィルタ」を編集します。

選択したものが、ブロックされます。

アプリケーション:ブロックなし

URL カテゴリ:インターネットセキュリティ(不正サイトやフィッシング、C&C 等)をブロック

サービス:全て選択

アプリケーション/URLカテゴリ:

すべて
 アプリケーション/URLカテゴリを指定する

新しいアプリケーショングループの追加

- アプリケーショングループ
- ▲ アプリケーション
 - ▶ ERP
 - ▶ WAP
 - ▶ Webサイト
 - ▶ Webメール
 - ▶ アプリケーションサービス
 - ▶ インスタントメッセージング
 - ▶ ウィルス対策
 - ▶ オーディオビデオ

新しいURLカテゴリグループの追加

- URLカテゴリグループ
- ▲ URLカテゴリ (17)
 - ▶ アダルト
 - ▶ インターネットセキュリティ (17)
 - ▶ コミュニケーションと検索
 - ▶ ネットワーク帯域幅
 - ▶ ビジネス
 - ▶ ライフスタイル
 - ▶ 一般

サービス:

すべて
 サービスを指定する

■インターネットセキュリティ詳細

- ▲ インターネットセキュリティ (17)
 - C&Cサーバ
 - Cookies
 - Made for AdSense
 - Web広告
 - アドウェア
 - ジョークプログラム
 - スパイウェア
 - スпамメール
 - ダイアラー
 - ハッキング
 - パスワード解読
 - フィッシング
 - プロキシ回避
 - マルウェア流布
 - リモートアクセスプログラム
 - 不正サイト
 - 不正ドメイン
 - 新しいドメイン
 - 潜在的に不正なソフトウェア

優先順位2 ルール名: Firewall Policy 【許可】

ファイアウォール(HTTPS などのプロトコル許可/ブロック)に相当する設定は「Firewall Policy」を編集します。

選択したものが許可されます。



許可されるサービス初期設定

導入時は以下許可サービス一覧のサービスが許可されています。

必要ないサービスは「選択済み」より「次の中から選択」へ移動することで通信をブロックすることができます。

また、「次の中から選択」より「選択済み」へ移動することで通信を許可することができます。

「次の中から選択」一覧にないサービスは「新しいサービスオブジェクトの追加」をクリックするとカスタムサービスを追加できます。

◆許可サービス一覧

※黄色のサービスは Cloud Edge 運用に必須のため Firewall Policy の「選択済み」から「次の中から選択」に変更しないでください。

	アクション	IP アドレス	IP アドレス	プロトコル	サービス
1	許可	all	all	TCP	http(80)
2	許可	all	all	TCP	https(443)
3	許可	all	all	UDP	dns(53)
4	許可	all	all	UDP	ntp(123)
5	許可	all	all	TCP	ftp(21)

6	許可	all	all	TCP	pop3(110)
7	許可	all	all	TCP	smtp(25)
8	許可	all	all	TCP	imaps(993)
9	許可	all	all	TCP	imap4(143)
10	許可	all	all	TCP	pop3s(995)
11	許可	all	all	TCP	smtps(465)
12	許可	all	all	TCP	smtp-auth(587)
13	許可	all	all	TCP	ping
14	許可	all	all	TCP	SS あんしんプラス(4120,4122)
15	許可	all	all	UDP	snmp(161)
16	許可	all	all	UDP	snmp-trap(162)
17	許可	all	all	UDP	syslog(514)
18	許可	all	all	TCP	SSH(22)
19	許可	all	all	TCP	telnet(23)
20	許可	all	all	TCP	Remote Desktop(3389)
21	許可	all	all	TCP	LDAP(389)
22	許可	all	all	UDP	RADIUS(1812)
23	許可	all	all	UDP	tftp(69)
24	許可	all	all	IGMP	マルチキャスト
25	許可	all	all	UDP	DHCP(67,68)
26	許可	all	all	UDP	LLMNR(5355)
27	許可	all	all	TCP	SMB_CIFS(137,139,445)
28	許可	all	all	UDP	SMB_CIFS(137,138,445)
29	許可	all	all	UDP	SSDP(1900)
30	許可	all	all	TCP	IPSec(ESP)
31	許可	all	all	UDP	IPSec(500,4500)
32	許可	all	all	TCP	VNC(5800,5900)

優先順位3 ルール名:All-DENY

全てをブロックするルールです。

優先順位4 ルール名:初期設定のポリシールール

初期値で用意されている全てを許可するルールです。Cloud Edge の上位にファイアウォールが設置されており Cloud Edge でファイアウォールルールを使わない場合は、(2)Firewall Policy(許可) (3)ALL-DENY(ブロック)を無効にすることによりファイアウォール機能をオフにすることができます。

追加		編集		削除		移動		その他		フィルタの適用		検索	
ポリシー名	ゲートウェイグループ	送信元	送信先	トラフィックタイプ	スケジュール	処理							
ポリシールール													
		アプリケーション_URLフィルタ	すべて	すべて	すべて	常時	ブロック						
		Firewall Policy	すべて	すべて	すべて	常時	許可						
		ALL-DENY	すべて	すべて	すべて	常時	ブロック						
		初期設定のポリシールール	すべて	すべて	すべて	常時	許可						

6.2. ポリシー設定例

導入時のポリシー設定をカスタマイズする場合の設定手順をケースごとに記載します。

ケース①URL フィルタ設定

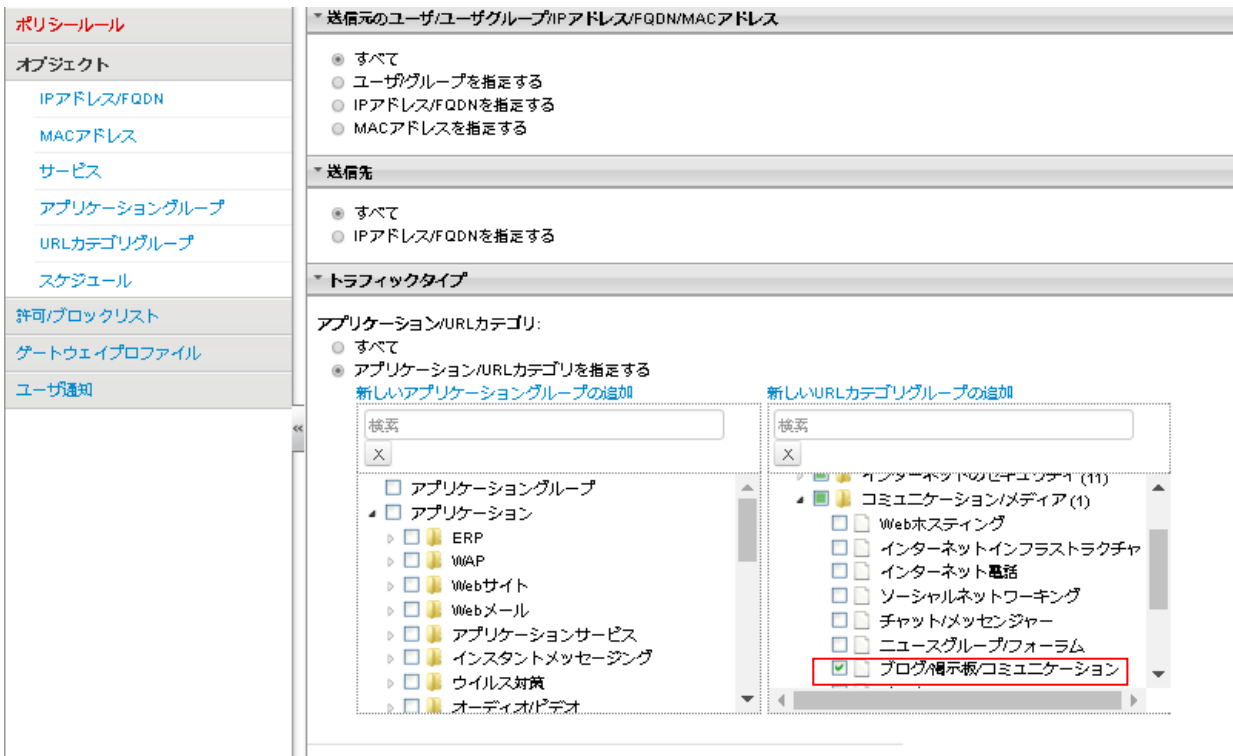
ブログ関連サイトの閲覧を規制する場合

ポリシー＞ポリシールール＞ポリシールールの管理よりアプリケーション_URL フィルタをクリックします。



URL カテゴリよりコミュニケーション/メディアを展開し、ブログ/掲示板/コミュニケーションにチェックを入れます。

設定後、保存をクリックしてください。



設定変更後は「すべて配信」をクリックすることで Cloud Edge に設定が反映されます。



ブログサイトを閲覧すると規制したカテゴリでブロックされます。

Trend Micro Cloud Edgeセキュリティイベント

URLブロック

URLフィルタセキュリティでこのURLカテゴリを制限しているため、Cloud EdgeによってこのWebサイトへのアクセスがブロックされました。

イベントの詳細

URL: [official.ameba.jp/]

カテゴリ: [ブログ/掲示板/コミュニケーション]

このブロックがエラーだと考えられる場合は、IT担当者に連絡して問題を解決してください。

Trend Micro Cloud Edge

ケース②URL フィルタを無効にする

クライアントや他のファイアウォール UTM などで URL フィルタをすでに使用しており、Cloud Edge の URL フィルタを無効に設定する場合。

ポリシー > ポリシールール > ポリシールールの管理よりアプリケーション_URL フィルタをクリックします。

The screenshot shows the 'Policy Rules Management' interface. The left sidebar has 'ポリシールール' (Policy Rules) highlighted with a red box and an arrow. The main table lists several policy rules. The 'アプリケーション_URLフィルタ' (Application URL Filter) rule is highlighted with a red box. Below the table, there are two search windows for '新しいアプリケーショングループの追加' (Add New Application Group) and '新しいURLカテゴリグループの追加' (Add New URL Category Group). The 'URLカテゴリ' (URL Category) window is highlighted with a red box, showing a list of categories including 'インターネットのセキュリティ' (Internet Security) and 'コミュニケーション/メディア' (Communication/Media).

ポリシー名	ゲートウェイグループ	送信元	送信先	トラフィックタイプ	スケジュール	処理
アプリケーション_URLフィルタ	すべて	すべて	すべて	APP URL SVC	常時	ブロック
Firewall Policy	すべて	すべて	すべて	APP URL SVC	常時	許可
ALL-DENY	すべて	すべて	すべて	APP URL SVC	常時	ブロック
初期設定のポリシールール	すべて	すべて	すべて	APP URL SVC	常時	許可

URL カテゴリよりインターネットのセキュリティとコミュニケーション/メディアを展開し、チェックを全て外します。設定後、保存をクリックしてください。

※URL フィルタカテゴリより C&C サーバは廃止されました。C&C 通信は Web レピュテーション機能でブロックします。

The screenshot shows the '新しいURLカテゴリグループの追加' (Add New URL Category Group) dialog box. The 'URLカテゴリ' (URL Category) section is expanded, and the 'インターネットのセキュリティ' (Internet Security) and 'コミュニケーション/メディア' (Communication/Media) categories are highlighted with a red box. The 'サービス' (Service) section is also visible, with 'すべて' (All) selected.

設定変更後は「すべて配信」をクリックすることで Cloud Edge に設定が反映されます。

ケース③ファイアウォールルール追加<サービス一覧にある場合>

SecureFTP を許可する場合

ポリシー>ポリシールール>ポリシールールの管理より Firewall Policy をクリックします。



SFTP を選択済みへ移動し保存をクリックします。



設定変更後は「すべて配信」をクリックすることで Cloud Edge に設定が反映されます。

ケース④ファイアウォールルール追加<サービス一覧にない場合>

TCP8080 ポートなどウェルノウンポート以外のサービスを業務で利用しておりサービス許可に追加する場合
 ポリシー>ポリシールール>ポリシールールの管理より Firewall Policy をクリックします。



「新しいサービスオブジェクトの追加」をクリックします。



サービスに追加するポート番号を入力して保存します。
 (オブジェクトの編集についてはオブジェクトを参照してください。)

名前:任意

プロトコル:TCP or UDP or ICMP

ポート:ポート番号

※単一ポート(8080)、複数ポート(8080,8081)、ポート範囲(8080-8090)またはこれらの組み合わせを指定できます。

設定変更後は「すべて配信」をクリックすることで Cloud Edge に設定が反映されます。

ポリシー名	ゲートウェイグループ	送信元	送信先	トラフィックタイプ	スケジュール	処理
アプリケーション_URLフィルタ	すべて	すべて	すべて	APP URL SVC	常時	ブロック
Firewall Policy	すべて	すべて	すべて	APP URL SVC	常時	許可
ALL-DENY	すべて	すべて	すべて	APP URL SVC	常時	ブロック
初期設定のポリシールール	すべて	すべて	すべて	APP URL SVC	常時	許可

ケース⑤ファイアウォールルール新規追加<Active Directory 認証用>

対向先に VPN 拠店があり Active Directory 認証を許可する場合

Active Directory 認証で利用される RPC 動的ポートは許可するポート範囲が広いいため既存のルールに許可ルールを追加すると全ての宛先(インターネット向き)に対して許可されてしまいます。そのため許可する宛先(Active Directory サーバ)を指定したポリシーを新たに作成することを推奨します。

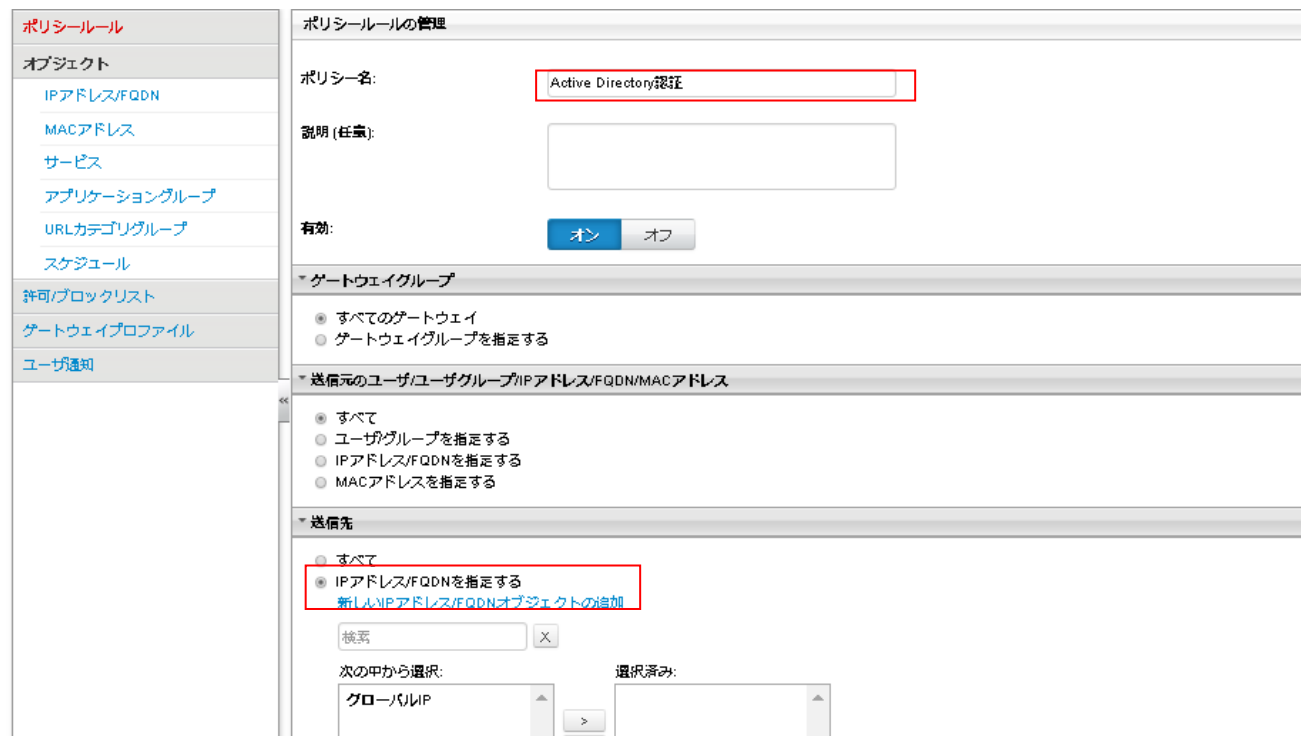
新規ポリシーの作成手順

ポリシー > ポリシールール > ポリシールールの管理より追加をクリックします。



ポリシー名: (任意)を入力します。

送信先の「IP アドレス/FQDN を指定する」を選択し、「新しい IP アドレス/FQDN オブジェクトの追加」をクリックします。



アドレスオブジェクトに追加する IP アドレスを入力して保存します。
(オブジェクトの編集についてはオブジェクトを参照してください。)

名前: 任意

プロトコル: IPv4

IP アドレス: 本ケースの場合 Active Directory サーバの IP アドレス



※IP アドレスまたは CIDR を指定します。複数のアドレスはカンマで区切ります。

例 192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24

送信先に作成したアドレスオブジェクトが選択されます。



以下のサービスを選択済へ移動します。

Kerberos

Kerberos_UDP

LDAP_UDP

RPC エンドポイント マッパー

RPC 動的ポート TCP

RPC 動的ポート UDP

処理は「許可」を選択し、保存をクリックしてください。

▼ **トラフィックタイプ**

アプリケーション/URLカテゴリ:

- すべて
- アプリケーション/URLカテゴリを指定する

サービス:

- すべて
- サービスを指定する

新しいサービスオブジェクトの追加

X

次の中から選択:

CorpCL

>
>>
<<
<

選択済み:

- Kerberos
- Kerberos_UDP
- LDAP_UDP
- RPC エンドポイント マッ
- パー
- RPC 動的ポートTCP

▼ **スケジュール**

新しいスケジュールオブジェクトの追加

▼ **処理**

- 許可
- ブロック
- 検索除外

保存
キャンセル

送信先 AD サーバの許可ポリシールールが追加されました。

ポリシーールの管理							
 追加 編集 削除 移動 其他 フィルタの適用 検索 							
ポリシー名	ゲートウェイグループ	送信元	送信先	トラフィックタイプ	スケジュール	処理	
<input checked="" type="checkbox"/> ActiveDirectory認証	すべて	すべて	ADサーバ	APP URL SVC	常時	許可	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> アプリケーション_URLフィルタ	すべて	すべて	すべて	APP URL SVC	常時	ブロック	<input type="checkbox"/>
<input checked="" type="checkbox"/> Firewall Policy	すべて	すべて	すべて	APP URL SVC	常時	許可	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> ALL-DENY	すべて	すべて	すべて	APP URL SVC	常時	ブロック	<input type="checkbox"/>
<input checked="" type="checkbox"/> 初期設定のポリシールール	すべて	すべて	すべて	APP URL SVC	常時	許可	<input checked="" type="checkbox"/>

設定変更後は「すべて配信」をクリックすることで Cloud Edge に設定が反映されます。

ケース⑥アプリケーション制御

【注意】

アプリケーション制御は一般的なインターネットサービスで利用されるアプリケーションの利用を制限することができます。
 ※CloudEdge5.6SP1 よりアプリケーションごとの設定のみ可能となり、アプリケーション機能ごとの設定は廃止されました。

例えばSNSの閲覧はできるが、投稿はさせない。ストレージサービスのDropboxでアップロードはできるが、ファイルダウンロードはさせない。のような細かな制限はできません。

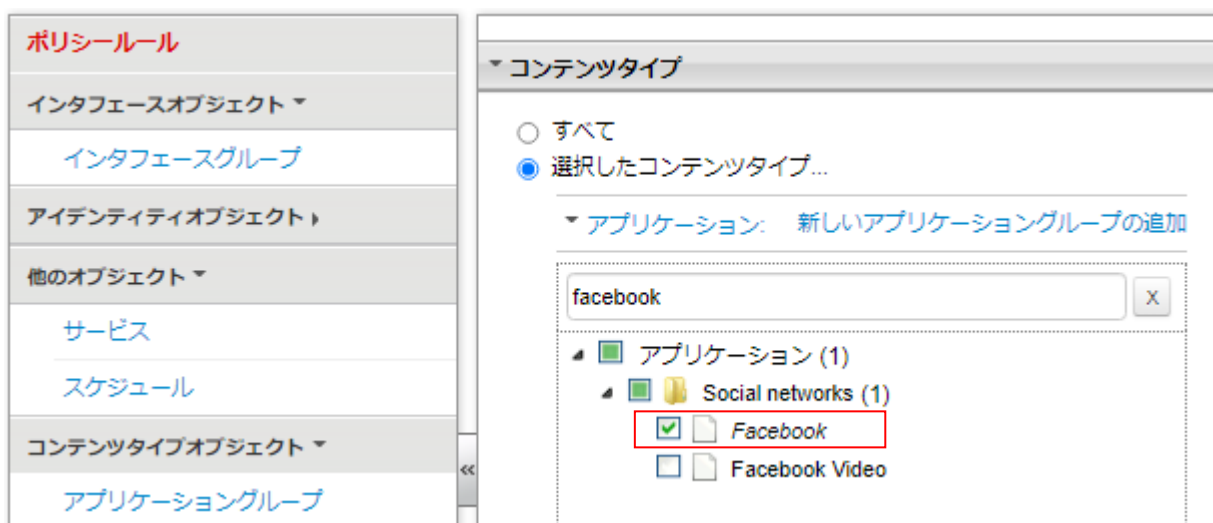
FacebookとTwitterをブロックする場合の例

ポリシー>ポリシールール>ポリシールールの管理よりアプリケーション_URLフィルタをクリックします。

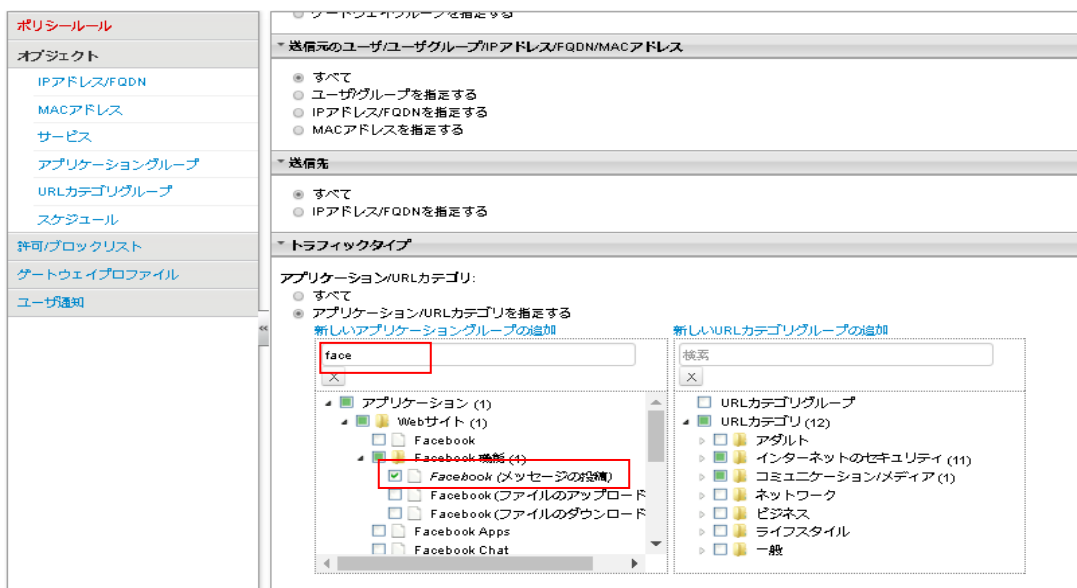


コンテンツタイプ アプリケーションより Facebook にチェックを入れます。

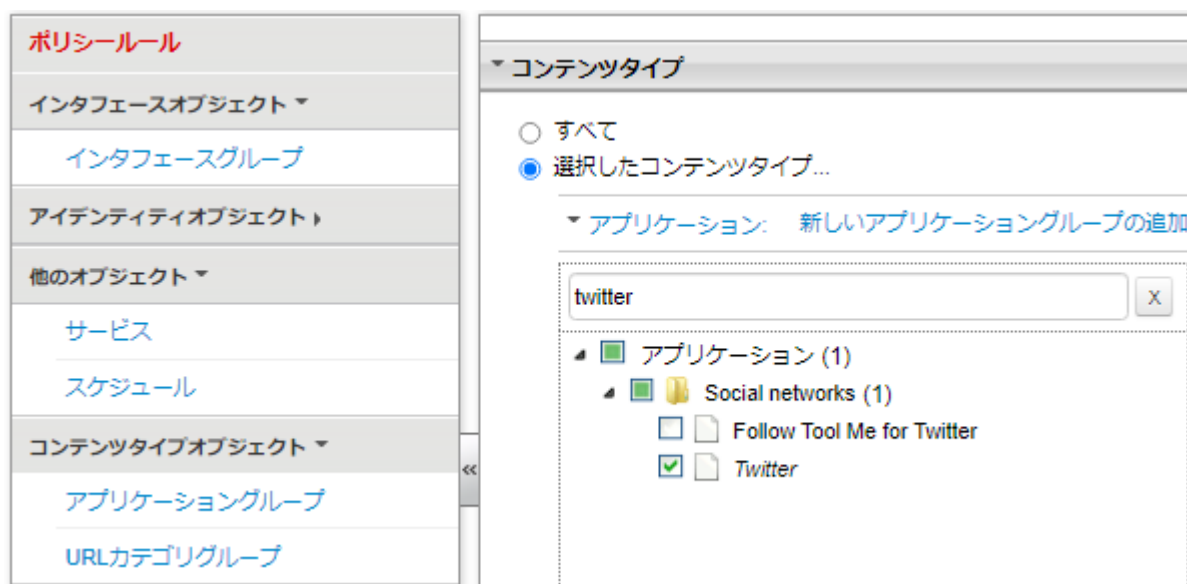
アプリケーション一覧から選択すると探し出すことが困難なため検索欄にアプリケーション名を入力することで表示項目を絞れます。



【注意】CloudEdge5.6SP1 以前は下記のようなアプリケーションの機能(例 Facebook メッセージの投稿のみ)をブロックすることができましたが、現在は不可となっております。



同様に Twitter にチェックを入れ保存をクリックします。



設定変更後は「すべて配信」をクリックすることで Cloud Edge に設定が反映されます。

Facebook、Twitter の利用がブロックされます。

※アプリケーション制御でブロックした場合、ブロック画面は表示されない場合があります。

ケース⑦複数 Cloud Edge に異なるポリシーを適用

本社:Cloud Edge100、拠点:Cloud Edge50 などを導入し本社と拠点で異なるポリシーを設定する場合

ゲートウェイに 2 台の Cloud Edge が登録されている状態です。

グループ/ゲートウェイ名	ステータス	前回のポリシー配信
Root (2)		
CE100_RD	オンライン	2015-11-11 14:07:50
CE50_RD	オンライン	2015-11-11 11:55:44

ポリシールールの複製を作成します。

ポリシー > ポリシールール > ポリシールールの管理より

アプリケーション_URL フィルタと Firewall Policy にチェックを入れ「その他」をクリックし複製を選択します。

アプリケーション_URL フィルタと Firewall Policy の複製が作成されます。

複製されたポリシーを拠点:Cloud Edge50 用として設定してみます。

複製されたポリシー Firewall Policy (1) をクリックしてください。

ポリシー名	ゲートウェイグループ	送信元	送信先	トラフィックタイプ	スケジュール	処理
Firewall Policy(1)	すべて	すべて	すべて	APP URL SVC	常時	許可
アプリケーション_URLフィルタ(1)	すべて	すべて	すべて	APP URL SVC	常時	ブロック
アプリケーション_URLフィルタ	すべて	すべて	すべて	APP URL SVC	常時	ブロック
Firewall Policy	すべて	すべて	すべて	APP URL SVC	常時	許可
ALL-DENY	すべて	すべて	すべて	APP URL SVC	常時	ブロック
初期設定のポリシールール	すべて	すべて	すべて	APP URL SVC	常時	許可

ポリシー編集画面が表示されますのでポリシー名(任意)を変更します。例) Firewall Policy 拠点
ゲートウェイグループの「ゲートウェイグループを指定する」を選択し Cloud Edge50 のみ選択します。
保存をクリックしてください。

ポリシールール管理

ポリシー名: Firewall_Policy 拠点

説明 (任意): 【注意】http、https、dnsサービスは運用に必須のため「選択済み」より「次の中から選択」に変更しないでください。

有効: オン

ゲートウェイグループ

すべてのゲートウェイ
 ゲートウェイグループを指定する

- Root
 - CE100_RD
 - CE50_RD

ポリシー名: Firewall Policy 拠点のゲートウェイグループが Cloud Edge50 に変更されました。

同様に複製されたポリシー アプリケーション_URL フィルタ(1)をクリックしてポリシー名、ゲートウェイグループを変更後、保存します。 例) アプリケーション_URL フィルタ拠点

ポリシールール管理

ポリシー名: アプリケーション_URLフィルタ拠点

説明 (任意):

有効: オン

ゲートウェイグループ

すべてのゲートウェイ
 ゲートウェイグループを指定する

- Root
 - CE100_RD
 - CE50_RD

「Firewall Policy 拠点」よりも「アプリケーション_URLフィルタ拠点」を優先的に処理させる必要があるため、アプリケーション_URL フィルタ拠点ポリシーにチェックを入れ Firewall Policy 拠点の上へ移動します。



拠点用 Cloud Edge のポリシーが作成できました。本社用 Cloud Edge ポリシーを編集します。



拠点用ポリシーと同様にポリシー名とゲートウェイグループを編集してください。

本社用 Cloud Edge のポリシー編集が完了したら「すべて配信」して変更を適用します。

これで本社、拠点それぞれのゲートウェイグループとポリシーが作成できました。

ポリシーールールの管理

	ポリシー名	ゲートウェイグループ	送信元	送信先	トラフィックタイプ	スケジュール	処理
ポリシーールール							
<input type="checkbox"/>	アプリケーション_URLフィルタ拠点	CE50_RD	すべて	すべて	APP URL SVC	常時	ブロック
<input type="checkbox"/>	Firewall_Policy 拠点	CE50_RD	すべて	すべて	APP URL SVC	常時	許可
<input type="checkbox"/>	アプリケーション_URLフィルタ本社	CE100_RD	すべて	すべて	APP URL SVC	常時	ブロック
<input type="checkbox"/>	Firewall Policy本社	CE100_RD	すべて	すべて	APP URL SVC	常時	許可
<input type="checkbox"/>	ALL-DENY	すべて	すべて	すべて	APP URL SVC	常時	ブロック
<input type="checkbox"/>	初期設定のポリシーールール	すべて	すべて	すべて	APP URL SVC	常時	許可

ケース⑧IP アドレス(送信元) 毎に異なる Firewall Policy を適用

192.168.1.0/24、192.168.2.0/24(本社) → Firewall Policy を使用

192.168.10/24(営業所) → このサブネット用に Firewall Policy2 を作成する場合

ポリシールールの複製を作成します。

ポリシー > ポリシールール > ポリシールールの管理より

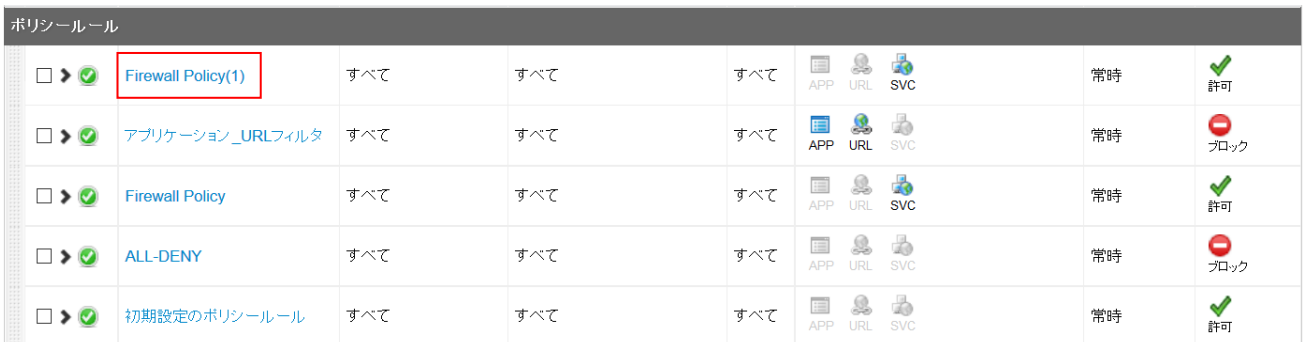
Firewall Policy にチェックを入れ「その他」をクリックし複製を選択します。



Firewall Policy の複製が作成されます。

複製されたポリシーを Firewall Policy2(192.168.10/24) 用として設定してみます。

複製されたポリシー Firewall Policy (1) をクリックしてください。

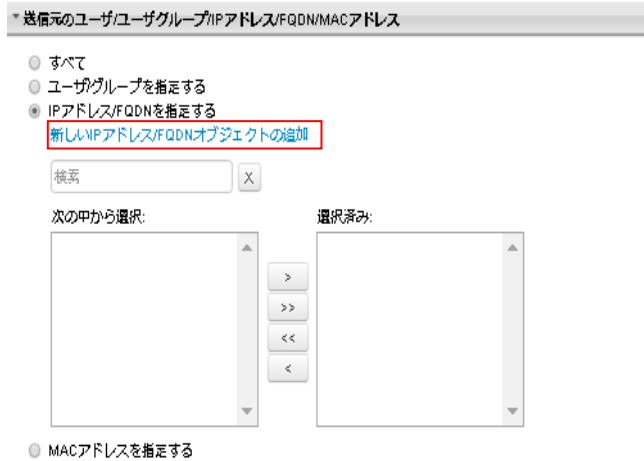


ポリシー編集画面が表示されますのでポリシー名(任意)を変更します。例) Firewall Policy2



Firewall Policy2 の送信元 IP アドレスを変更します。

「IP アドレス/FQDN を指定する」を選択し、新しい IP アドレスオブジェクトの追加をクリックします。



アドレスオブジェクトに追加する IP アドレスを入力して保存します。
(オブジェクトの編集についてはオブジェクトを参照してください。)

名前: 任意

プロトコル: IPv4

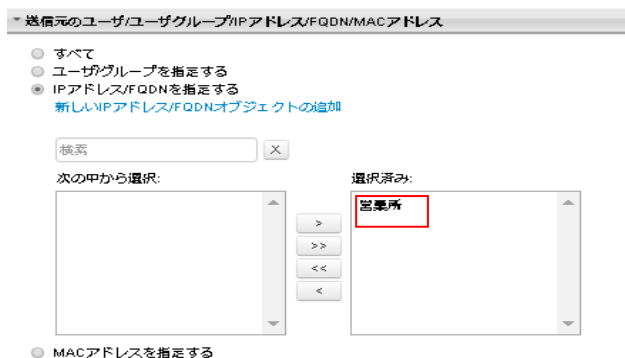
IP アドレス: 本ケースの場合 192.168.10.0/24



※IP アドレスまたは CIDR を指定します。複数のアドレスはカンマで区切ります。

例 192.168.0.1,10.0.0.1-10.0.0.4,10.0.0.8/24

送信元に作成したアドレスオブジェクトが選択されます。



必要に応じて許可するサービスを編集してください。

▼ **トラフィックタイプ**

アプリケーション/URLカテゴリ:

- すべて
- アプリケーション/URLカテゴリを指定する

サービス:

- すべて
 - サービスを指定する
- [新しいサービスオブジェクトの追加](#)

<p>次の中から選択:</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <ul style="list-style-type: none"> Kerberos_UDP LDAP_UDP RPC エンドポイント マッパー RPC 動的ポートTCP RPC 動的ポートUDP 3PC </div>	> >> << <	<p>選択済み:</p> <div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <ul style="list-style-type: none"> DHCP DNS FTP HTTP HTTPS IGMP </div>
---	--------------------	--

▼ **スケジュール**

[新しいスケジュールオブジェクトの追加](#)

常時 ▼

▼ **処理**

- 許可
- ブロック

処理は「許可」を選択し、保存をクリックしてください。

Firewall Policy2 が作成されました。

ポリシーールの管理				
+ 追加 ✎ 編集 🗑 削除 📁 移動 ⚙ その他				
	ポリシー名	ゲートウェイグループ	送信元	送信先
ポリシーール				
<input type="checkbox"/> ➔ <input checked="" type="checkbox"/>	Firewall Policy2	すべて	営業所	すべて
<input type="checkbox"/> ➔ <input checked="" type="checkbox"/>	アプリケーション_URLフィルタ	すべて	すべて	すべて
<input type="checkbox"/> ➔ <input checked="" type="checkbox"/>	Firewall Policy	すべて	すべて	すべて
<input type="checkbox"/> ➔ <input checked="" type="checkbox"/>	ALL-DENY	すべて	すべて	すべて
<input type="checkbox"/> ➔ <input checked="" type="checkbox"/>	初期設定のポリシーール	すべて	すべて	すべて

「Firewall Policy2」よりも「アプリケーション_URL フィルタ」を優先的に処理させる必要があるため、アプリケーション_URL フィルタポリシーにチェックを入れ Firewall Policy2 の上へ移動します。



営業所ポリシー同様に本社用ポリシーを設定し、許可するサービスを編集します。



これで本社、営業所それぞれの Firewall Policy が作成できました。

ポリシー編集が完了したら「すべて配信」をクリックして変更を適用します。



6.3. インタフェースオブジェクト

日本では利用できません。

6.4. アイデンティティオブジェクト

ポリシールール作成時に使用できる、IP アドレス/FQDN、MAC アドレス、およびジオロケーションのアイデンティティオブジェクトを設定できます (IP アドレス/FQDN の場合、他のさまざまな用途にも使用できます)。

①IP アドレス/FQDN

特定の送信元アドレス/FQDN または送信先アドレス/FQDN に対するセキュリティポリシーを設定するには、IP アドレスと IP アドレス範囲および FQDN を定義します。追加/削除/複製することができ、編集する場合は名前をクリックします。
※ポリシーで選択されているオブジェクトは削除できません。

アドレスオブジェクトに追加する IP アドレスを入力して保存します。

名前: 任意

プロトコル: IPv4

IP アドレス: 例) 192.168.10.0/24



この IP アドレスオブジェクトはポリシーの送信元や送信先として指定することができます。



<input type="checkbox"/>	名前	プロトコル	IPアドレス
<input type="checkbox"/>	営業所	IPv4	19.168.10.0/24
<input type="checkbox"/>	本社	IPv4	192.168.1.0/24, 192.168.2.0/24

オブジェクト編集後は「すべて配信」をクリックして設定を適用します。

②MAC アドレス

Cloud Edge は、接続するすべてのエンドポイントから MAC アドレスを収集し、収集したアドレス情報を Cloud Edge Cloud Console に送信します。Cloud Edge Cloud Console は受け取った情報に基づいて MAC アドレスオブジェクトを自動生成します。

特定の送信元アドレスに対するセキュリティポリシーを設定するには、MAC アドレスを定義するか、または収集された既存の MAC アドレスオブジェクトを編集します。

ポリシールール	MACアドレス
オブジェクト	追加 削除
IPアドレス	<input type="checkbox"/> MACアドレス <input type="checkbox"/> IPアドレス <input type="checkbox"/> 説明 <input type="checkbox"/> ユーザー名 <input type="checkbox"/> ゲートウェイ
MACアドレス	<input type="checkbox"/> 00-15-5D-41-0B-CA 172.
サービス	<input type="checkbox"/> 00-50-56-9D-41-05 172.
アプリケーショングループ	<input type="checkbox"/> 00-50-56-9F-51-97 172.
URLカテゴリグループ	<input type="checkbox"/> 00-50-56-A6-42-65 172.

オブジェクト編集後は「すべて配信」をクリックして設定を適用します。

③ジオロケーション

現在は利用できません。

CE 5.5SP2(5.5.3046)より予定。

6.5. 他のオブジェクト

ポリシールールを作成するときを使用できるサービスオブジェクトやスケジュールオブジェクトなど、他のオブジェクトを設定できます。

① サービス

Cloud Edge では、事前に定義された 100 種類以上のサービス (DNS、FTP、HTTP、POP3、SMTP、SSL、および TELNET) を利用できます。必要に応じて、カスタマイズされたサービスを定義することもできます。

特定のアプリケーションのセキュリティポリシーを定義する際、1 つ以上のサービスを選択して、アプリケーションで使用可能なポート番号を制限できます。追加/削除/複製することができ、編集する場合は名前をクリックします。※ポリシーで選択されているオブジェクトは削除できません。

名前	プロトコル	ポート
<input type="checkbox"/> DHCP	UDP	67,68
<input type="checkbox"/> IMAPS	TCP	993
<input type="checkbox"/> Kerberos_UDP	UDP	88
<input type="checkbox"/> LDAP_UDP	UDP	389
<input type="checkbox"/> LLMNR	UDP	5535
<input type="checkbox"/> POP3S	TCP	995
<input type="checkbox"/> RPC エンドポイント マッパー	TCP	135

追加するサービスオブジェクトを入力して保存します。

名前: 任意

プロトコル: TCP/UDP/ICMP

ポート: 例) 8080,8081

サービスオブジェクトの追加/編集

名前: 勤怠WEBサイト

プロトコル: TCP

ポート: 8080,8081

説明:

保存 キャンセル

オブジェクト編集後は「すべて配信」をクリックして設定を適用します。

このサービスオブジェクトはポリシーのサービスとして指定することができます。

▼トラフィックタイプ

アプリケーション/URLカテゴリ:

すべて
 アプリケーション/URLカテゴリを指定する

サービス:

すべて
 サービスを指定する

[新しいサービスオブジェクトの追加](#)

次の中から選択:

- VRRP
- WESP
- WSN
- XNET
- XTP
- 勤怠WEBサイト**

選択済み:

- SSH
- SSあんしんプラス
- SYSLOG
- TELNET
- TFTP
- WS-EML

▼スケジューリング

[新しい...](#)
 常時

名前: 勤怠WEBサイト

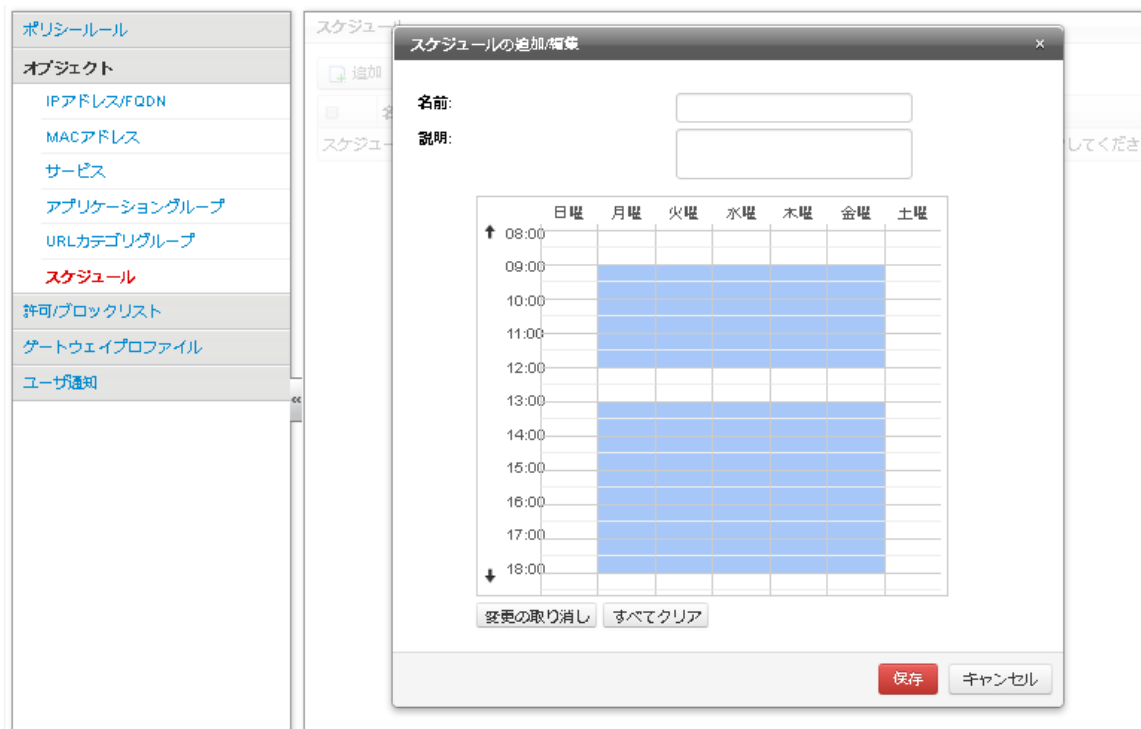
説明:
 ポート: 8080,8081
 プロトコル: TCP

②スケジュール

初期設定では、各セキュリティポリシーはすべての日付と時間に適用されます。セキュリティポリシーを特定の時間に制限するには、スケジュールを定義してから適切なポリシーに適用します。日付や時間の範囲を 1 つのスケジュールオブジェクトで複数指定することができます。

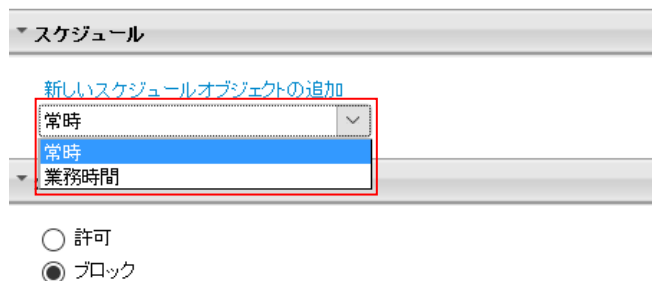
名前:任意

スケジュール指定する時間帯をマウスで選び保存します。



オブジェクト編集後は「すべて配信」をクリックして設定を適用します。

作成したスケジュールオブジェクトはポリシーのスケジュールとして指定することができます。



6.6. コンテンツタイプオブジェクト

ポリシー規則の作成時に使用できるアプリケーショングループや URL カテゴリグループなどのコンテンツタイプオブジェクトを設定できます。

①アプリケーショングループ

アプリケーションをブロックするポリシーを個別にいくつも作成しなくて済むように、アプリケーションをグループ化して 1 つのポリシーでブロックできます。追加／削除／複製することができ、編集する場合は名前をクリックします。※ポリシーで選択されているオブジェクトは削除できません。

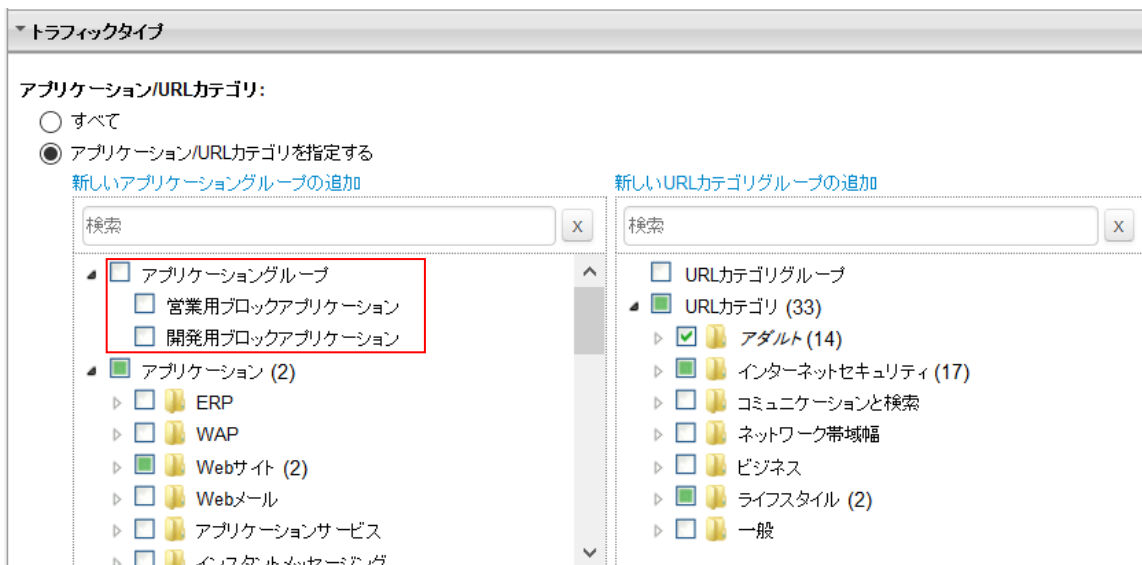
名前:任意

グループ化するアプリケーションを選択して保存します。



オブジェクト編集後は「すべて配信」をクリックして設定を適用します。

作成したアプリケーショングループはポリシーのアプリケーショングループとして指定することができます。

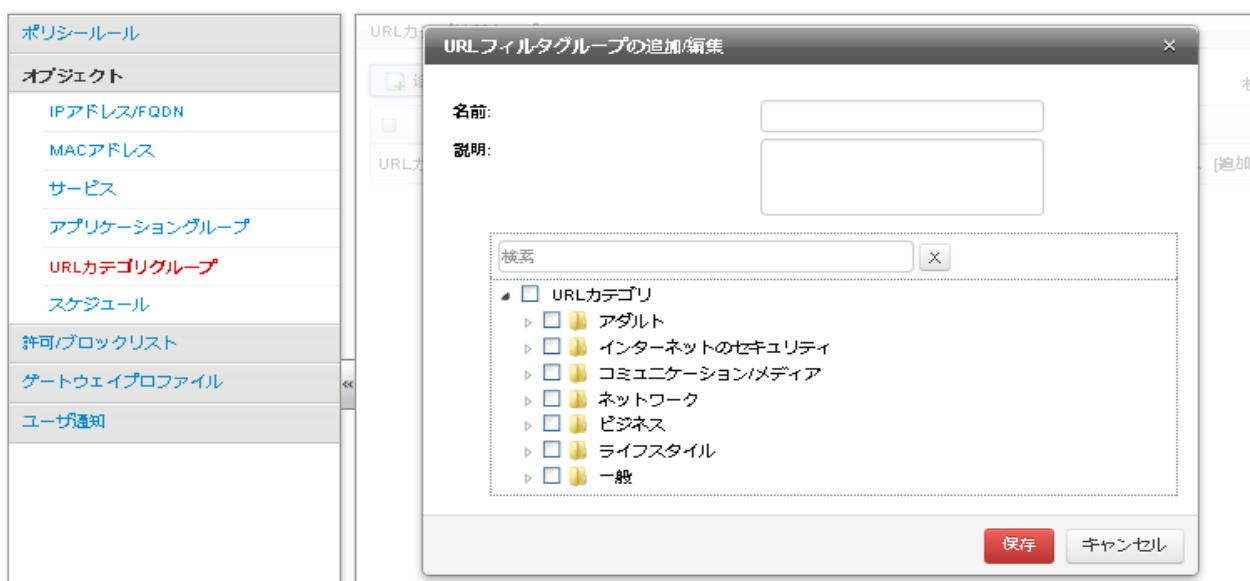


②URL カテゴリグループ

URL カテゴリをブロックするポリシーを個別にいくつも作成しなくて済むように、URL カテゴリをグループ化して1つのポリシーでブロックできます。追加／削除／複製することができ、編集する場合は名前をクリックします。※ポリシーで選択されているオブジェクトは削除できません。

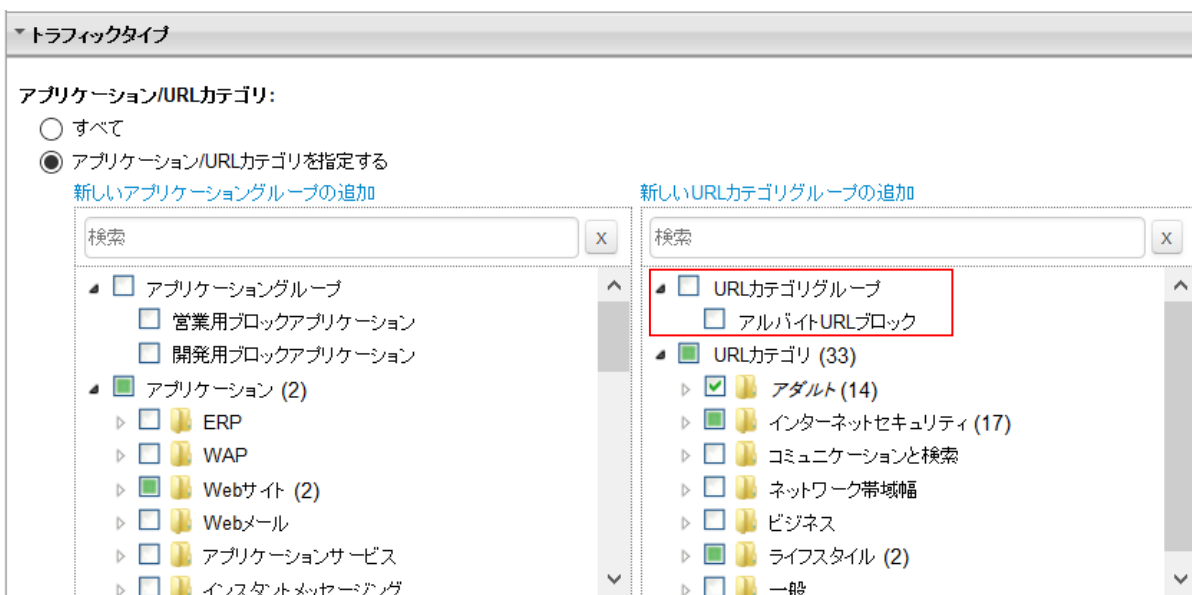
名前:任意

グループ化する URL カテゴリを選択して保存します。



オブジェクト編集後は「すべて配信」をクリックして設定を適用します。

作成した URL カテゴリグループはポリシーの URL カテゴリグループとして指定することができます。



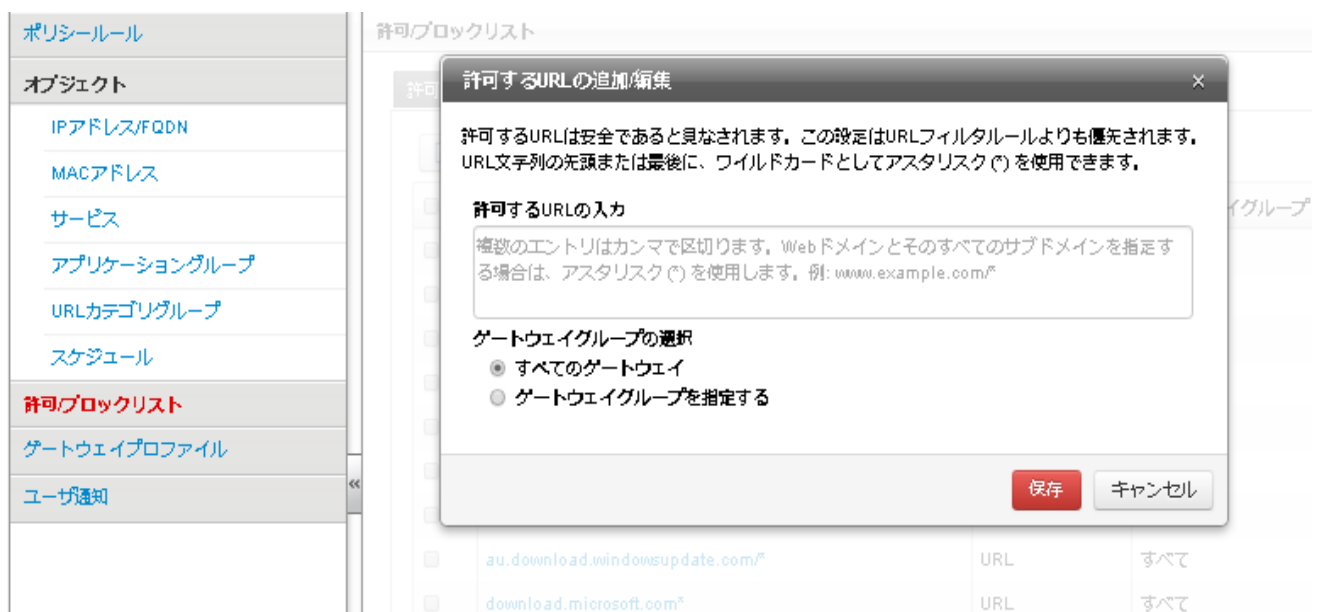
6.7. 許可/ブロックリスト

許可（除外）リストとブロックリストの設定は、URL フィルタ、Web レピュテーション、および高度な脅威保護で定義されている設定よりも優先されます。URL または FQDN/IPv4 アドレスをリストに追加するときは、次の点に留意してください。ワイルドカードとしてアスタリスク (*) を使用できます。ワイルドカードは、URL 文字列の先頭または末尾でのみ使用できます。

※URL の許可は、URL のブロックよりも優先されます。

※初期に設定されている許可する URL は削除しないでください。Cloud Edge の運用や WindowsUpdateなどが行えなくなります。

追加／削除／複製することができ、編集する場合は名前をクリックします。



URL を入力後、保存をしてください。

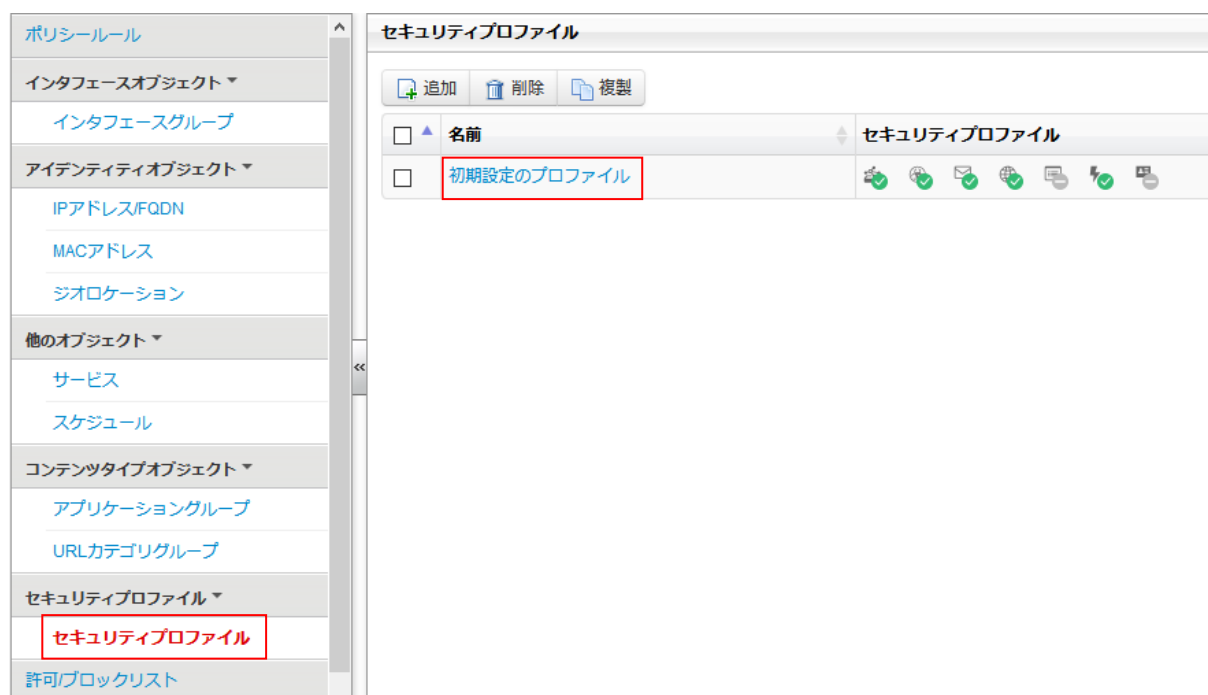
編集後は「すべて配信」をクリックして設定を適用します。

6.8. セキュリティプロファイル

IPS、不正プログラム対策、スパムメール対策、Web レピュテーション、HTTPS 複合、DoS 対策、エンドポイントの識別の設定を行うことができます。初期設定では HTTPS 複合とエンドポイントの識別以外の機能が有効に設定されています。

ポリシー>セキュリティプロファイルより「初期設定のプロファイル」をクリックすると編集できます。

※セキュリティプロファイルは複数作成することができますが Cloud Edge1 台に対して 1 つのセキュリティプロファイルのみ指定することができます。



セキュリティプロファイルの指定

ゲートウェイ>変更するセキュリティプロファイルを選択して



選択後は「すべて配信」をクリックして設定を適用します。

①IPS(侵入防御)

初期設定で有効に設定されています。

ネットワーク侵入防止機能は Cloud Edge の基本機能の 1 つです。侵入防止システム (IPS) は、脅威、セキュリティホール、バックドアプログラムなど、さまざまな攻撃を識別してデバイスへの侵入を防止します。IPS をファイアウォールのセキュリティポリシーと併用することで、ファイアウォールのルールポリシーで許可されたトラフィックをさらに調べて脅威が含まれていないことを確認できるため、セキュリティを強化することができます。

ゲートウェイプロファイルの追加/編集

プロファイル名: 初期設定のプロファイル

説明 (任意): すべてのゲートウェイ用の初期設定プロファイル

IPS 不正プログラム対策 メールセキュリティ対策 Webレピュテーション HTTPS復号 DoS対策 エンドポイントの識別

有効: オン オフ

処理

IPSセキュリティルールの処理: ブロック 監視

詳細設定

有効: オン オフ

設定変更した場合は保存をしてください。

「すべて配信」をクリックして設定を適用します。

②不正プログラム対策

初期設定で有効に設定されています。

不正プログラム対策プロファイルでは、新たに出現するセキュリティ上の脅威に対する保護を提供できます。このプロファイルは、不正プログラムやネットワークに対するその他の脅威から保護するためにすべてのポリシーで使用できます。不正プログラム対策を有効にすると、ネットワーク接続の検索が実行されて不正プログラムがブロックされます。

許可するファイル拡張子： 検索を実行せずに許可されます。

ブロックするファイル拡張子： 検索を実行せずにブロックされます。

タグの追加： メール添付ファイルに不正なコンテンツが含まれていた場合に件名に追加するタグ設定を行います。

The screenshot displays the '不正プログラム対策' (Malware Protection) configuration page. On the left, a sidebar lists navigation options such as 'ポリシールール' (Policy Rules), 'オブジェクト' (Objects), 'IPアドレス/FQDN', 'MACアドレス', 'サービス', 'アプリケーショングループ', 'URLカテゴリグループ', 'スケジュール', '許可/ブロックリスト', 'ゲートウェイプロファイル', and 'ユーザ通知'. The main content area has a top navigation bar with tabs for 'IPS', '不正プログラム対策' (highlighted), 'メールセキュリティ対策', 'Webレピュテーション', 'HTTPS優待', 'DoS対策', and 'エンドポイントの識別'. Below the tabs, there are '有効:' (On/Off) toggle buttons and a checked option for 'クラウド検索を有効にする' (Enable cloud search). The 'ファイル拡張子' (File Extensions) section includes instructions on how to enter file extensions (e.g., PNG, GIF, MP3) and notes that file types are not considered. It features two text input fields: '許可するファイル拡張子:' (Allowed file extensions) containing 'png.gif.jpg.mp3.mp4.avi.mov.wmv' and 'ブロックするファイル拡張子:' (Blocked file extensions). A search dropdown menu is open, showing categories like 'その他' (Others), 'アーカイブ' (Archives), 'イメージ' (Images), 'オーディオビデオ' (Audio/Video), 'ドキュメント' (Documents), and '実行ファイル' (Executable files). A note at the bottom states that specified file types will be excluded from search when downloaded via HTTP.

設定変更した場合は保存をしてください。

「すべて配信」をクリックして設定を適用します。

③メールセキュリティ対策

不正プログラム対策

メールに含まれる不正プログラムを検出します。

ポリシールール	IPS	不正プログラム対策	メールセキュリティ対策	Webレピュテーション	HTTPS復号	DoS対策	エンドポイントの識別
オブジェクト							
IPアドレスFQDN							
MACアドレス							
サービス							
アプリケーショングループ							
URLカテゴリグループ							
スケジュール							
許可/ブロックリスト							
ゲートウェイプロファイル							
ユーザ通知							
	有効:	<input checked="" type="radio"/> オン <input type="radio"/> オフ					
		不正プログラム対策					
	有効:	<input checked="" type="radio"/> オン <input type="radio"/> オフ ⓘ					
	仮想アナライザの有効化:	<input type="radio"/> オン <input checked="" type="radio"/> オフ ⓘ					
	処理:	<input type="radio"/> ブロック <input checked="" type="radio"/> タグの追加 ⓘ					
	件名タグ:	<input type="text" value="[ウイルス駆除済み]"/>					
	本文タグ:	<input type="text" value="[本文タグ] フィールドが空の場合、メッセージ本文にタグは挿入されません。"/>					

クラウドベースの仮想アナライザに不審な添付ファイルを送信してサンドボックス分析を実施し、添付ファイルに不正プログラムが含まれていないかを確認します。※(オプション)

ポリシールール	IPS	不正プログラム対策	メールセキュリティ対策	Webレピュテーション	HTTPS復号	DoS対策	エンドポイントの識別
オブジェクト							
IPアドレスFQDN							
MACアドレス							
サービス							
アプリケーショングループ							
URLカテゴリグループ							
スケジュール							
許可/ブロックリスト							
ゲートウェイプロファイル							
ユーザ通知							
	有効:	<input checked="" type="radio"/> オン <input type="radio"/> オフ					
		不正プログラム対策					
	有効:	<input checked="" type="radio"/> オン <input type="radio"/> オフ ⓘ					
	仮想アナライザの有効化:	<input type="radio"/> オン <input checked="" type="radio"/> オフ ⓘ					
	処理:	<input type="radio"/> ブロック <input checked="" type="radio"/> タグの追加 ⓘ					
	件名タグ:	<input type="text" value="[ウイルス駆除済み]"/>					
	本文タグ:	<input type="text" value="[本文タグ] フィールドが空の場合、メッセージ本文にタグは挿入されません。"/>					

- 不正プログラムを含むメールをブロックするか、件名および本文にタグを追加するか設定します。(初期設定はタグ)

ポリシールール	IPS	不正プログラム対策	メールセキュリティ対策	Webレピュテーション	HTTPS復号	DoS対策	エンドポイントの識別
オブジェクト							
IPアドレスFQDN							
MACアドレス							
サービス							
アプリケーショングループ							
URLカテゴリグループ							
スケジュール							
許可/ブロックリスト							
ゲートウェイプロファイル							
ユーザ通知							
	有効:	<input checked="" type="radio"/> オン <input type="radio"/> オフ					
		不正プログラム対策					
	有効:	<input checked="" type="radio"/> オン <input type="radio"/> オフ ⓘ					
	仮想アナライザの有効化:	<input type="radio"/> オン <input checked="" type="radio"/> オフ ⓘ					
	処理:	<input checked="" type="radio"/> ブロック <input type="radio"/> タグの追加 ⓘ					
	件名タグ:	<input type="text" value="[ウイルス駆除済み]"/>					
	本文タグ:	<input type="text" value="[本文タグ] フィールドが空の場合、メッセージ本文にタグは挿入されません。"/>					

機械学習型検索に不審な添付ファイルを送信して、添付ファイルに不正プログラムが含まれていないかを確認し監視ブロック・タグを追加するかの処理を選択します。

スパムメール対策

Email Reputation Services (ERS) が使用されます。ERS は Smart Protection Network のコンポーネントで、動的レピュテーションデータベースに加え、世界最大の最も信頼されているレピュテーションデータベースの 1 つを使用して、受信メールメッセージの IP アドレスを検証して新しいスパムおよびフィッシングの送信元を特定し、ゾンビやボットネットからのメールを阻止します。

スパムメールをブロックするか、件名および本文にタグを追加するかを選択します。

コンテンツフィルタ

コンテンツフィルタを以下のように設定します。

- コンテンツをメッセージサイズでフィルタリングする。
- メッセージのヘッダ、本文、添付ファイル名をキーワードまたはパターンを使用してフィルタリングする。
- メッセージの本文・添付ファイルをマイナンバーでフィルタリングする。

コンテンツを含むメールにタグ付けするか、完全にブロックするかを設定します。(初期設定はタグ)

設定変更した場合は保存をしてください。

「すべて配信」をクリックして設定を適用します。

除外リスト

ファイルタイプによる許可/ブロック、メール送信者の許可/ブロックを設定できます。

ファイルタイプ **メール送信者**

許可するファイルタイプ - 不正プログラム対策で使用

検索 X

- ▷ その他
- ▷ アーカイブ
- ▷ イメージ (3)
- ▷ オーディオ/ビデオ (3)
- ▷ ドキュメント
- ▷ 実行ファイル

選択したタイプの添付ファイルは、不正プログラム対策の検索が除外されます。

ブロックするファイルタイプ - 不正プログラム対策で使用

検索 X

- ▷ その他
- ▷ アーカイブ
- ▷ イメージ
- ▷ オーディオ/ビデオ
- ▷ ドキュメント
- ▷ 実行ファイル

選択したタイプの添付ファイルは、不正プログラム対策の検索時に削除されます。

ファイルタイプ **メール送信者**

許可する送信者 - スпамメールフィルタ/コンテンツフィルタ/仮想アナライザ/機械学習型検索で使用

許可する送信者のメールアドレスを入力してクリックします

追加

削除

指定した送信者からのメッセージをスパムメールフィルタ/コンテンツフィルタおよび仮想アナライザ/機械学習型検索分析の対象から除外します。不正プログラムの検索は実行されます。

ブロックする送信者 - すべてのメールフィルタで使用

ブロックする送信者のメールアドレスを入力してクリックし

追加

削除

指定した送信者からのメールメッセージをすべてブロックします。

詳細設定

SMTPTS/POP3S/IMAPS の検索を行う場合に「オン」に設定します。

※セキュアプロトコルのため検索を行うためには Cloud Edge の SSL 証明書を生成し、クライアントにインストールする必要があります。SSL 証明書については 8. 管理の証明書管理の手順を確認ください。

▼ 詳細設定

SMTPT	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
POP3S	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
IMAPS	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ

カスタムSSLポートに複数のポートを指定する場合、カンマで区切って入力してください。

SMTPTS	<input type="checkbox"/> オン <input checked="" type="checkbox"/> オフ
POP3S	<input type="checkbox"/> オン <input checked="" type="checkbox"/> オフ
IMAPS	<input type="checkbox"/> オン <input checked="" type="checkbox"/> オフ

SSL証明書: 証明書はセキュアなメール検索に使用されます。SSL証明書を管理するには、[\[管理\]→\[証明書管理\]](#)の順に選択します。

④ Web レピュテーション

初期設定で有効に設定されています。

Web レピュテーションサービス (WRS) では、ユーザがアクセスしようとする URL を調べ、潜在的に危険な Web サイト、特に既知のフィッシングサイトまたはファームサイトでないかを確認します。WRS を採用した Cloud Edge では、感染の拡大を防止、または初期段階で抑えることで、リアルタイムの保護を提供してシステム検索リソースを節約し、ネットワーク帯域幅の消費を削減します。Web レピュテーションテクノロジーは、新たに出現する Web の脅威からエンドユーザを保護します。Web レピュテーション検索は、WRS サーバから URL カテゴリ情報を取得するため、Cloud Edge そのものは URL データベースを保持しません。

URL ブロックのセキュリティレベルを設定できます。(初期設定は低)

The screenshot shows the configuration page for Web Reputation. On the left is a navigation menu with items like 'ポリシールール', 'オブジェクト', '許可/ブロックリスト', 'ゲートウェイプロフィール', and 'ユーザ通知'. The main area has several tabs: 'IPS', '不正プログラム対策', 'メールセキュリティ対策', 'Webレピュテーション', 'HTTPS復号', 'DoS対策', and 'エンドポイントの識別'. The 'Webレピュテーション' tab is active. Below the tabs, there is a '有効' (Enabled) toggle set to 'オン' (On). A section titled 'セキュリティレベル' (Security Level) has three radio buttons: '高' (High), '中' (Medium), and '低' (Low). The '低' (Low) option is selected. Below this, there is a section for '不正なコンテンツを含むサイト' (Sites containing malicious content) with two buttons: 'ブロック' (Block) and '監視' (Monitor). The 'ブロック' button is selected.

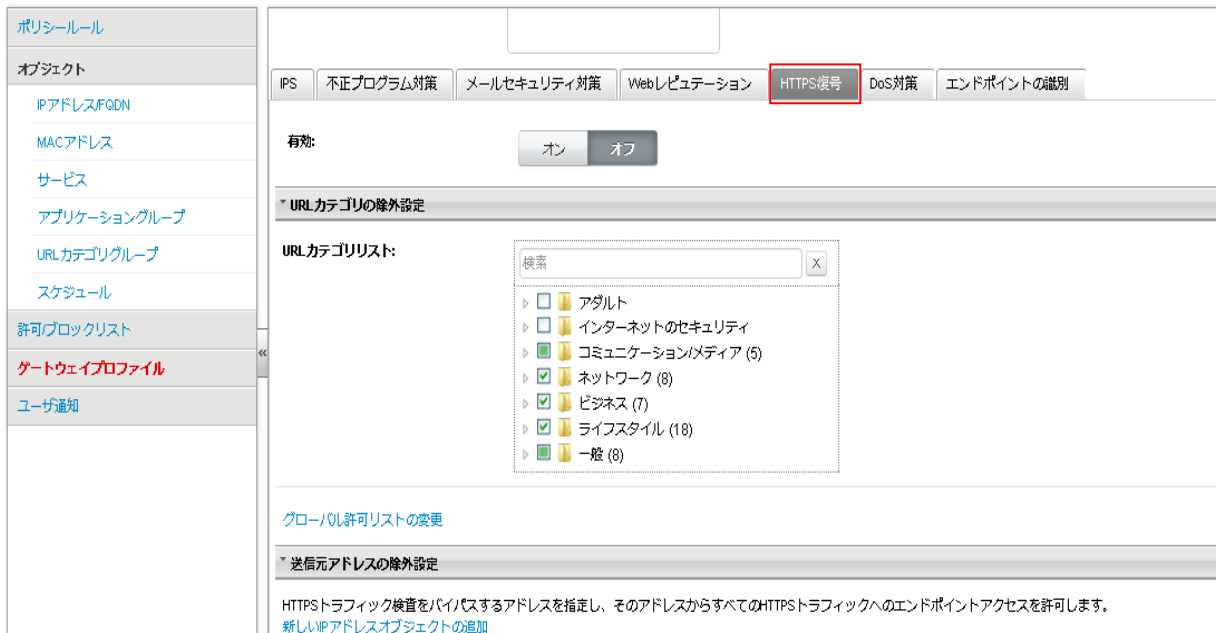
設定変更した場合は保存をしてください。

「すべて配信」をクリックして設定を適用します。

⑤HTTPS 復号

初期設定で無効に設定されています。

HTTPS 復号プロファイルを設定します。このプロファイルで、HTTPS トラフィックを識別したり、特定の URL カテゴリを HTTPS 検査から除外したりできます。



不正な HTTPS サイトに対するセキュリティを強化するには HTTPS 復号機能の利用を推奨いたします。

※ただし複合には負荷がかかるため通信が遅くなる可能性があります。

※HTTPS 復号を有効にした場合、Cloud Edge の証明書はブラウザに信用されていないため、(例えば google サイトなどを開いた場合)信頼されないサイトと警告が出てしまいます。これを解除するためには 8. 管理の証明書管理の手順を確認いただき、クライアントに Cloud Edge の証明書をインストールしてください。

複合を有効にした場合、カスタム HTTPS ポートは、カンマで区切って 5 つまで入力できます。

初期設定のポートは 443 と 8443 です。このリストのポートを送信先とする HTTPS トラフィックは、復号化され検索されません。



【重要】

メールセキュリティ対策プロファイルでセキュアなメール（SMTPS、POP3S、IMAPS）を有効にした場合、有効にしたセキュアなメールプロトコルで使用されるポートをHTTPSポートリストに入力すると、HTTPS 検査で問題が発生する可能性があるため追加できません。たとえば、メールセキュリティ対策プロファイルで SMTPS を有効にし、初期設定の SMTPS ポート（465）を使用する場合、HTTPS ポートリストにポート 465 を入力することはできません。

設定変更した場合は保存をしてください。

「すべて配信」をクリックして設定を適用します。

⑥DoS 対策

初期設定で有効に設定されています。

サービス拒否攻撃や分散サービス拒否 (DDoS) 攻撃は、インターネットに接続されたホストへのサービスを一時的または無期限に妨害または遮断することを目的とした、ユーザがコンピュータやネットワークのリソースを利用できない状態にする攻撃です。

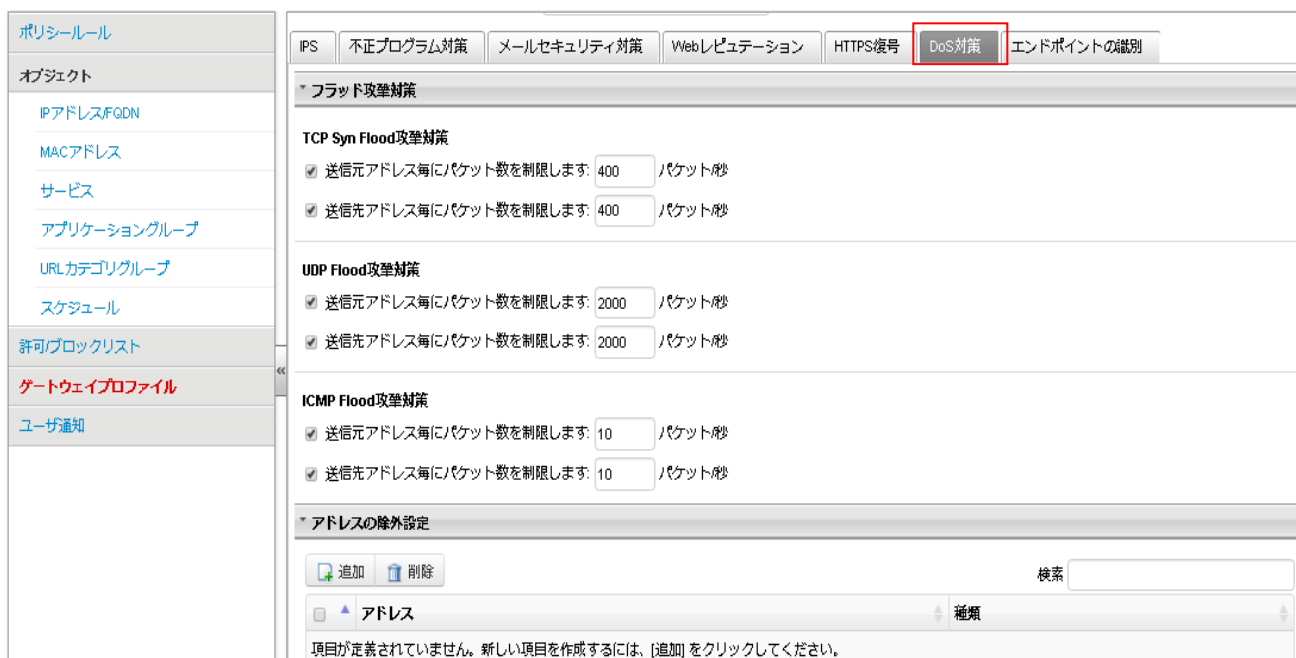
しきい値を作成して Cloud Edge を通過する 1 秒あたりのパケット数を制限できます。

TCP SYN

UDP

ICMP

アドレスの除外設定を行えます。



ポリシールール

オブジェクト

- IPアドレスFQDN
- MACアドレス
- サービス
- アプリケーショングループ
- URLカテゴリグループ
- スケジュール

許可ブロックリスト

ゲートウェイプロフィール

ユーザ通知

IPS 不正プログラム対策 メールセキュリティ対策 Webレピュテーション HTTPS復号 **DoS対策** エンドポイントの識別

フラッド攻撃対策

TCP Syn Flood攻撃対策

- 送信元アドレス毎にパケット数を制限します: 400 パケット/秒
- 送信先アドレス毎にパケット数を制限します: 400 パケット/秒

UDP Flood攻撃対策

- 送信元アドレス毎にパケット数を制限します: 2000 パケット/秒
- 送信先アドレス毎にパケット数を制限します: 2000 パケット/秒

ICMP Flood攻撃対策

- 送信元アドレス毎にパケット数を制限します: 10 パケット/秒
- 送信先アドレス毎にパケット数を制限します: 10 パケット/秒

アドレスの除外設定

追加 削除 検索

アドレス	種類
項目が定義されていません。新しい項目を作成するには、[追加] をクリックしてください。	

設定変更した場合は保存をしてください。

「すべて配信」をクリックして設定を適用します。

⑦エンドポイント識別

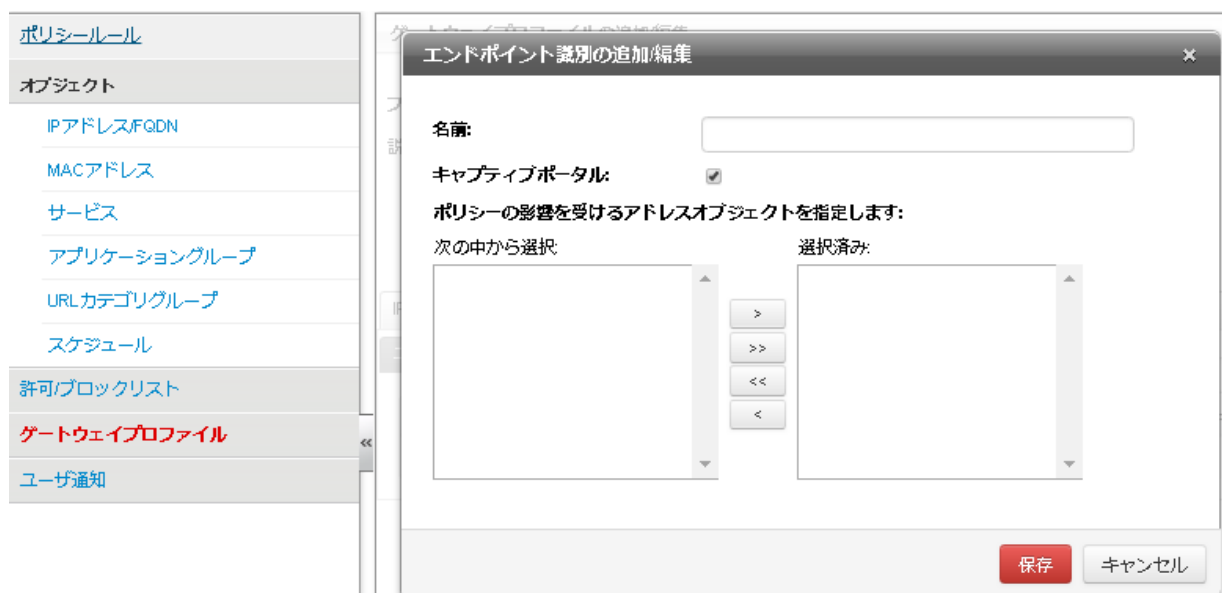
エンドポイント識別では、どのIPアドレスがどのユーザに割り当てられているかを識別します。これにより、ポリシーマッチング用のIPアドレスとユーザのマッピングキャッシュを使用してユーザの識別方法を構築できます。

初期設定では、エンドポイント識別でIPアドレスを自動的に識別することはできません。エンドポイント識別を実行するには、どのアドレスオブジェクトを使用するかを定義する必要があります。選択されたアドレスオブジェクトで定義されている範囲にない送信元IPアドレスについては、エンドポイント識別は実行できません。

IPアドレスまたはIPアドレス範囲ごとに、特定の認証方法を使用するように設定します。

・キャプティブポータルを使用すると、Cloud EdgeでユーザとIPアドレスを関連付けることができない場合にキャプティブポータルで処理を引き継ぎ、Webフォームでユーザを認証できます。

※キャプティブポータルとはWebフォームでユーザを認証する機能。



設定変更した場合は保存をしてください。

「すべて配信」をクリックして設定を適用します。

6.9. ユーザ通知

違反の通知で使用される HTML メッセージを編集およびプレビューします。

ポリシールール	エンドユーザへの通知のカスタマイズ
オブジェクト	通知イベント
IPアドレス/FQDN	IPS違反
MACアドレス	URLフィルタ違反
サービス	WRS違反
アプリケーショングループ	アプリケーション制御違反
URLカテゴリグループ	クラウドのセキュリティイベント
スケジュール	サーバ証明書エラー
許可ブロックリスト	ファイル拡張子違反
ゲートウェイプロファイル	ブロックURL違反
ユーザ通知	ランサムウェア違反
	不正プログラム対策違反

例)IPS 違反

文字やレイアウトを編集できます。

The screenshot shows a window titled "ユーザ通知の編集" (User Notification Edit). The main content area displays a preview of an HTML message. The message content is as follows:

Trend Micro Cloud Edgeセキュリティイベント

侵入防止システム

このWebサイトは有害な活動をホスティングしている可能性があるため、Cloud Edgeによってアクセスがブロックされました。

イベントの詳細

URL: [%U]

攻撃ID: [%V]

このブロックがエラーだと考えられる場合は、IT担当者に連絡して問題を解決してください。

At the bottom right of the window, there are two buttons: "保存" (Save) and "キャンセル" (Cancel).

7. 分析とレポート

分析とレポートについて説明します。

7.1. ログ分析

ログを分析するには、選択したゲートウェイまたはゲートウェイグループから未加工のログのクエリを実行し、選択したフィルタ（ゲートウェイ名、クライアント IP、URL カテゴリ）でグループ化して、さらに詳しく調査するために CSV ファイルにエクスポートします。ログの保存期間は 180 日間です。

ログは次のカテゴリに分類されます。

- アプリケーション帯域幅
- ポリシー施行
- インターネットアクセス
- インターネットセキュリティ



ダッシュボード	ゲートウェイ	ポリシー	分析とレポート	管理
ログ分析				
ログ分析				
アプリケーション帯域幅				
ネットワーク上の IP アドレス、ユーザ、アプリケーションによる帯域幅の消費を確認および分析します。ログを確認した後、アップストリームとダウンストリームの割り当て帯域幅を調整して通信を制御したり、不要なトラフィックをブロックしたり、重要なトラフィックやサービスに適切な帯域幅を割り当てたりできます。				
ポリシー施行				
ポリシーによるネットワークトラフィックの制御方法を確認および分析します。ログを確認した後、ポリシールールを調整して特定のトラフィックを許可またはフィルタしたり、設定が適切でないポリシーのトラブルシューティングを行ったりできます。				
インターネットアクセス				
特定のユーザがアクセスした Web サイトやドメインを確認および分析します。ログを確認した後、特定の種類のトラフィックをフィルタするカスタム URL カテゴリを追加したり、必要に応じてそれらのカテゴリの特定の URL を個別に承認またはブロックしたりできます。				
インターネットセキュリティ				
検索エンジンで不正プログラムやネットワークの脅威などからユーザを保護する方法を確認および分析します。ログを確認した後、セキュリティ機能を有効または無効にしたり、処理、スケジュール、ユーザポリシーを調整してネットワークの保護を強化したりできます。				

①アプリケーション帯域幅

それぞれのログの表示で次のいずれかのフィルタを利用できます。

ゲートウェイ名

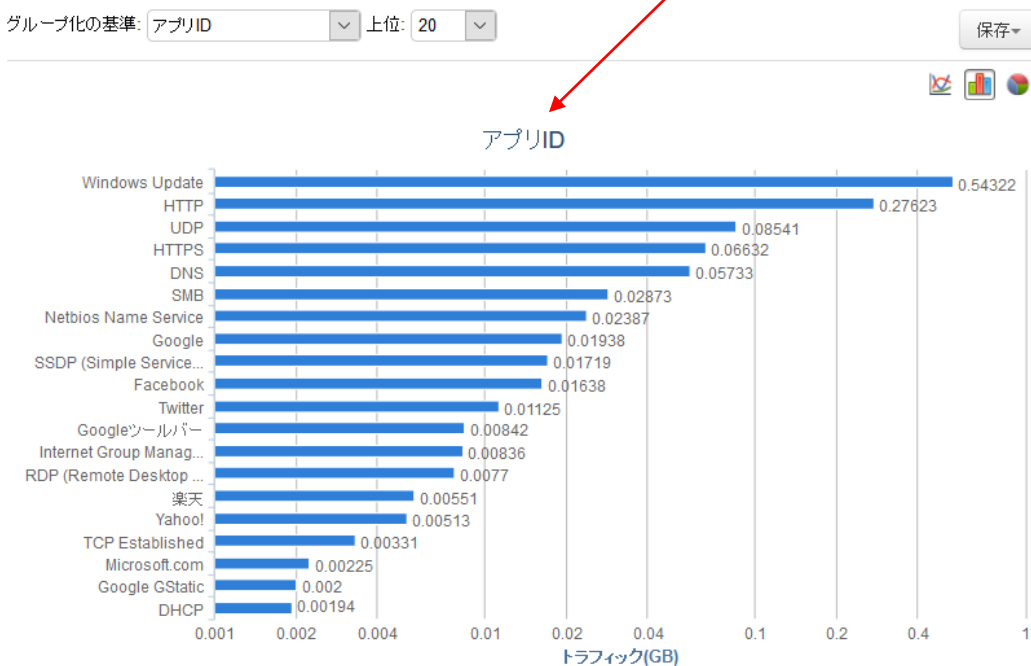
ユーザ名

クライアント IP

アプリ ID



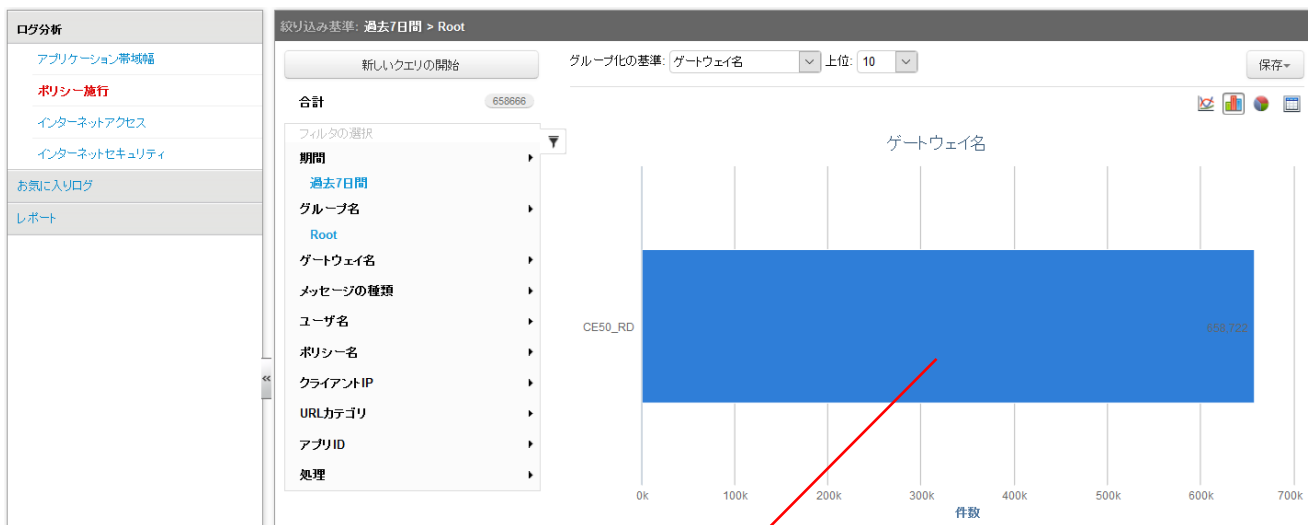
アプリ ID でフィルタした場合。



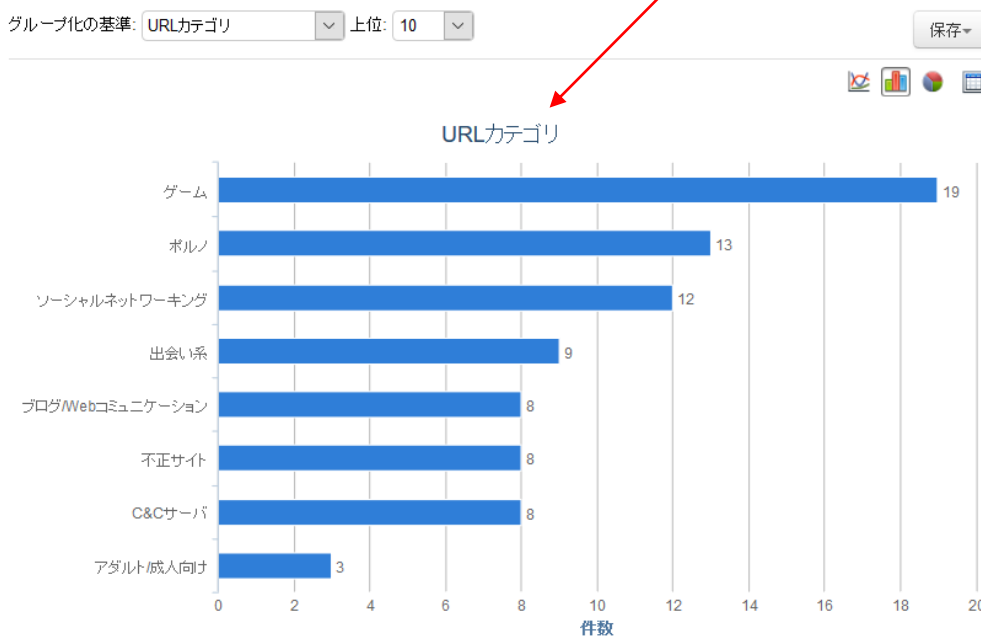
②ポリシー施工

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- ゲートウェイ名
- メッセージの種類
- ユーザ名
- ポリシー名
- クライアント IP
- URL カテゴリ
- アプリ ID
- 処理



URL カテゴリでフィルタした場合。



③インターネットアクセス

それぞれのログの表示で次のいずれかのフィルタを利用できます。

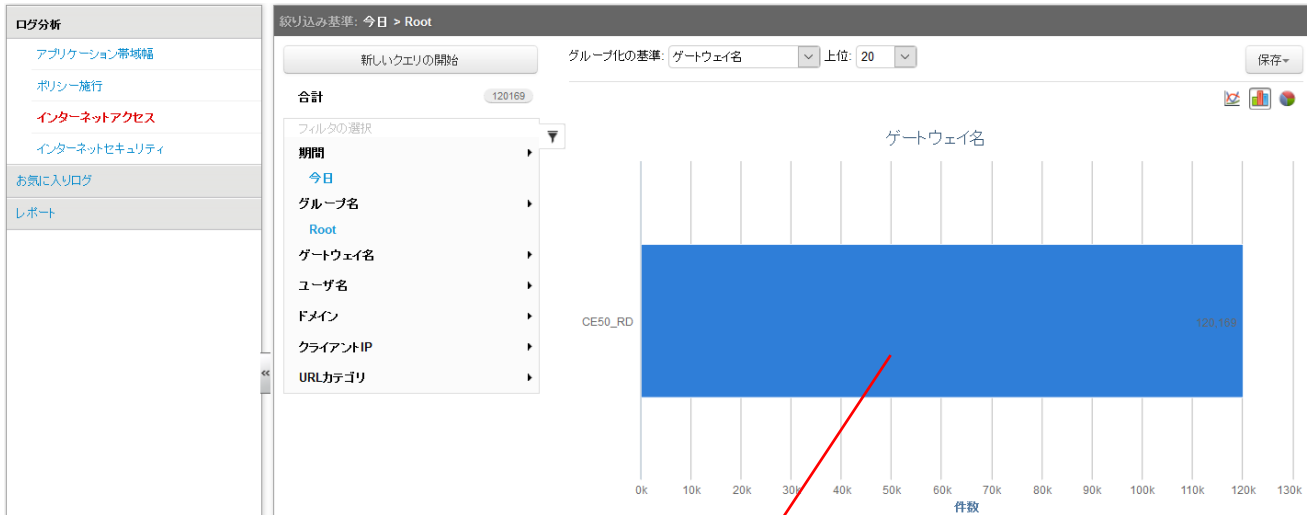
ゲートウェイ名

ユーザ名

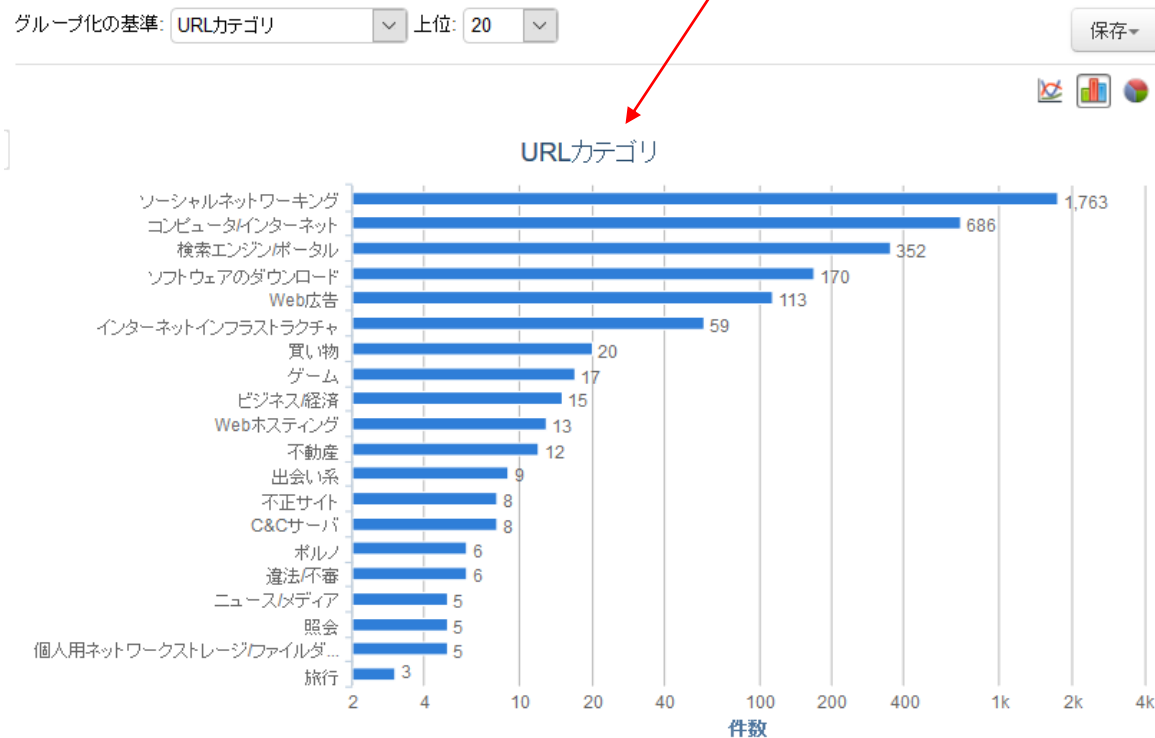
ドメイン

クライアント IP

URL カテゴリ



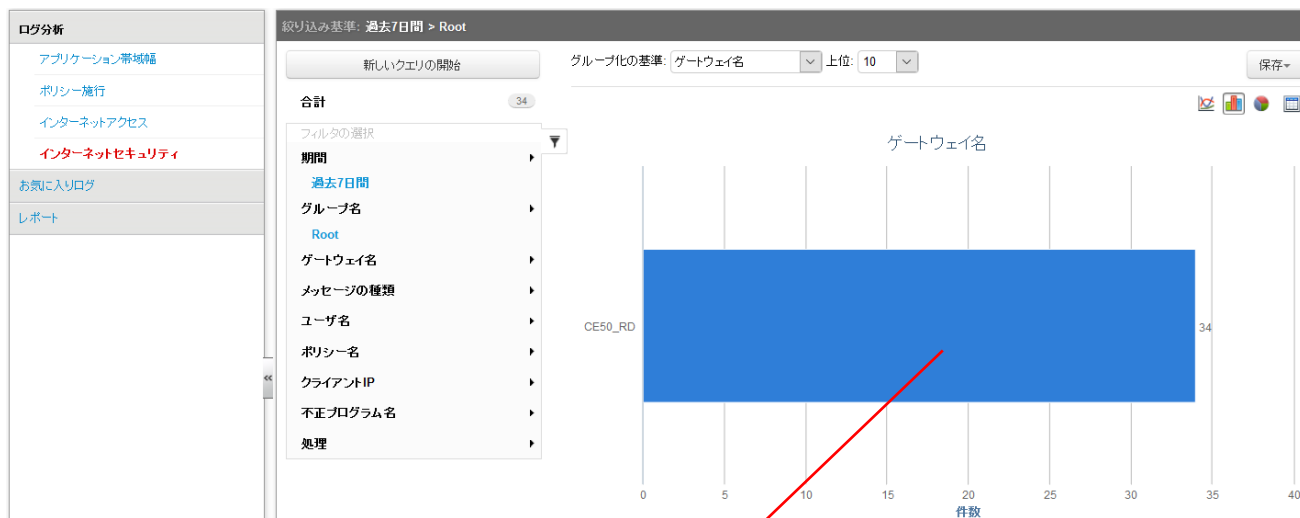
URL カテゴリでフィルタした場合。



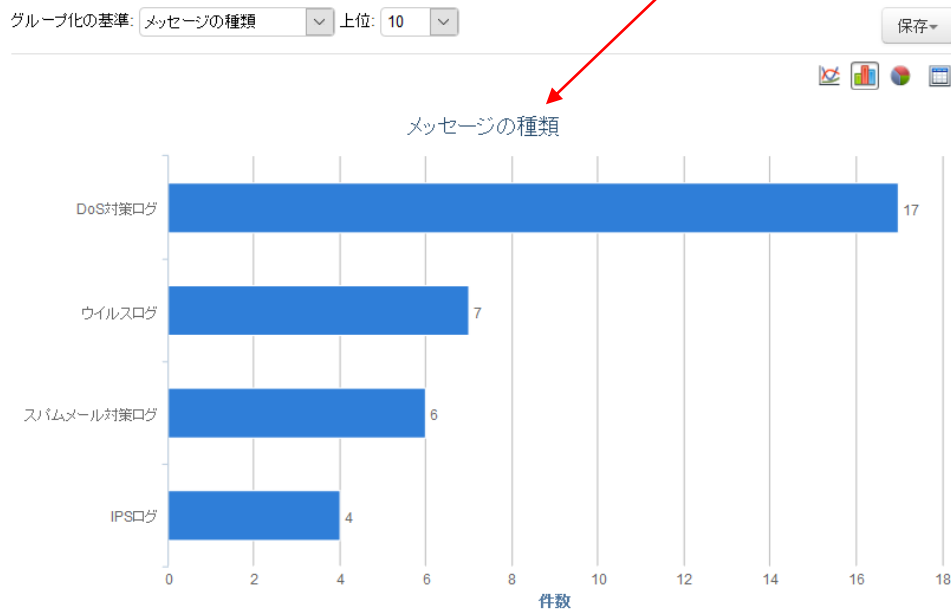
④インターネットセキュリティ

それぞれのログの表示で次のいずれかのフィルタを利用できます。

- ゲートウェイ名
- メッセージの種類
- ユーザ名
- ポリシー名
- クライアント IP
- 不正プログラム名
- 処理

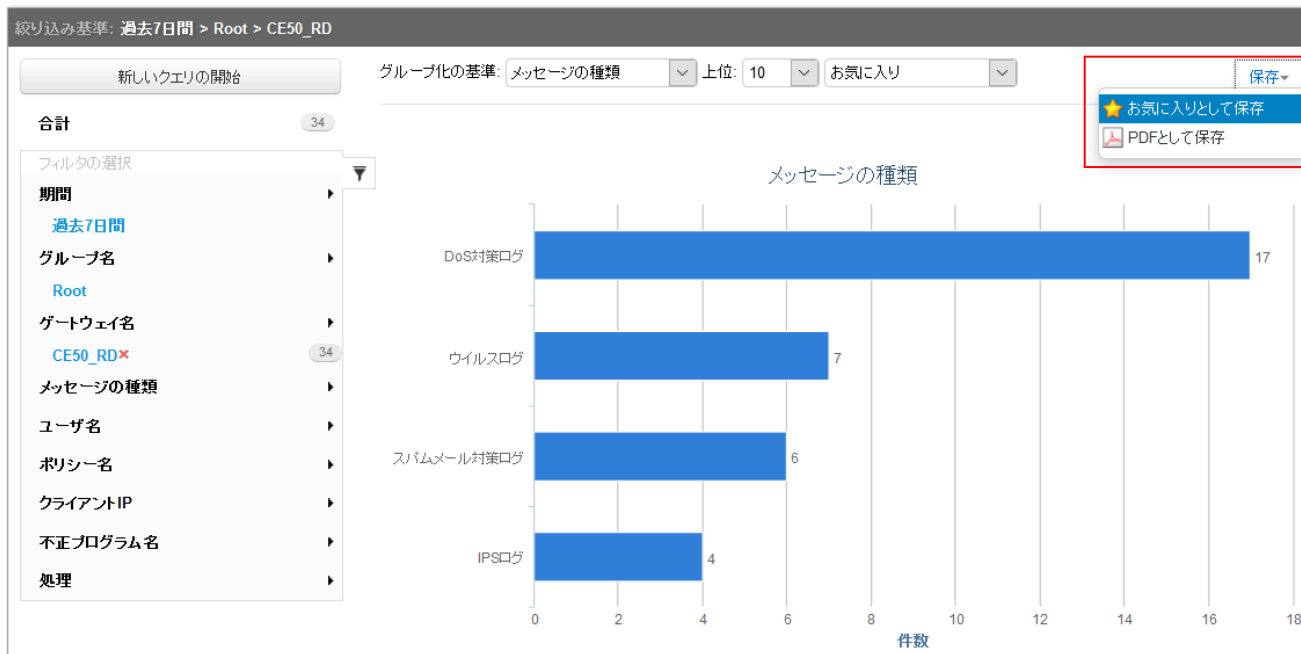


メッセージの種類でフィルタした場合。



7.2. お気に入りログ

ログを分析した後、ログクエリフィルタをお気に入りログとして保存しておけば、そのデータに後ですばやくアクセスできます。



保存されたお気に入りログより名前をクリックすると保存されたフィルタで表示します。

ログ分析		お気に入りログ			
アプリケーション帯域幅 ポリシー施行 インターネットアクセス インターネットセキュリティ		<input type="checkbox"/> 名前 <input type="checkbox"/> 不正検出ログ			
お気に入りログ レポート		<input type="checkbox"/> 説明 インターネットセキュリティ			
		<input type="checkbox"/> 種類 インターネットセキュリティ			
		<input type="checkbox"/> フィルタ 上位: 10 期間: 過去7日間 ゲートウェイ名: CE50_RD ゲートウェイグループ: Root			

7.3. レポート

Cloud Edge Cloud Console では、検出されたウイルスや不正コード、ブロックされたファイル、およびアクセスされた URL に関するレポートを生成できます。ゲートウェイプログラムイベントに関するこの情報を使用して、設定を最適化したり、セキュリティポリシーを微調整したりできます。追加／削除／複製することができ、編集する場合は名前をクリックします。

Cloud Edge Cloud Console では、次の 5 つのカテゴリのレポートを使用できます。

帯域幅

ポリシー施行

インターネットアクセス

インターネットセキュリティ

カスタムレポート

レポートは、必要なときにほぼリアルタイムに手動で生成することも、1 回のみ、毎日、毎週、または毎月といったスケジュールに従って生成するようにもできます。レポートの内容は、登録されているゲートウェイからアップロードされたログデータに基づきます。生成されたレポートに表示されるデータの範囲と量は、レポートで定義されたパラメータによって決まります。

ログ分析	レポート情報
アプリケーション帯域幅	レポート名: <input type="text"/>
ポリシー施行	説明: <input type="text"/>
インターネットアクセス	有効: <input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
インターネットセキュリティ	
お気に入りログ	レポート設定
レポート	バックアップスケジュール: <input type="text" value="オンデマンド"/>
	レポート期間: <input checked="" type="radio"/> 過去7日間 <input type="radio"/> 任意の時間範囲
	保存されているレポート: 新しい「N」個のレポートを保持する <input type="text" value="10"/>
	レポート通知の送信
	有効: <input type="checkbox"/> オン <input checked="" type="checkbox"/> オフ
	ゲートウェイグループ
	<input checked="" type="radio"/> すべて <input type="radio"/> ゲートウェイグループの指定
	レポートの基準
	<input checked="" type="radio"/> すべてのユーザ <input type="radio"/> 特定のユーザ/グループ <input type="radio"/> 特定のIPアドレス/IP範囲

1. レポートの情報を設定します。

レポート名

説明

有効/無効

2. レポートテンプレートの設定を指定します。

バックアップスケジュール: レポートの実行スケジュールを選択します。(オンデマンド、1回、毎日、毎週、毎月)

レポート期間: 時間範囲を選択します。(過去1時間、過去 12 時間、過去 24 時間、今日、過去 7 日間、過去 30 日間)

保存されているレポート: レポートにイベントを上位何件まで表示するかを選択します。(1,5,10,20,30,……90,99)

3. 必要に応じて、[レポート通知の送信] を有効にします。

メールの受信者: 複数のアドレスはカンマで区切ります。

メールの件名: メールの件名を指定します。

メッセージ: HTML 形式のメールメッセージの本文を指定します。

レポートを添付する: メールメッセージに PDF ファイルまたは CSV ファイルを添付する場合に選択します。

4. レポートに含めるゲートウェイまたはゲートウェイグループを選択します。

5. すべてのユーザ、選択したユーザおよびグループ、または IP アドレスおよび IP アドレス範囲のいずれかをレポートに含めるかを選択します。

6. 個々のレポートの種類とオプションを定義します。

7. 必要に応じて、[カスタムレポート] を有効にします。

お気に入りログを保存すると、そのログの情報に後でアクセスするためのレポートテンプレートとしてカスタムレポートが自動的に生成されます。

「お気に入りログ」を参照してください。

設定変更した場合は保存をしてください。

8. 管理

管理について説明します。

8.1. 管理項目

以下の項目を閲覧、設定可能です。※予約アップデートとメンテナンス項目は設定変更しないようお願いします。

ライセンスを管理する

ユーザとアカウント

ユーザ認証

監査ログ

管理者アラート

予約アップデート

メンテナンス

証明書管理

ダッシュボード	ゲートウェイ	ポリシー	分析とレポート	管理
<div style="display: flex;"> <div style="width: 25%; border-right: 1px solid #ccc; padding-right: 5px;"> <p>ライセンス</p> <p>ユーザとアカウント</p> <p style="padding-left: 20px;">アカウント管理</p> <p>ユーザ認証</p> <p style="padding-left: 20px;">ユーザIDの同期</p> <p style="padding-left: 20px;">ホスト対象のユーザとグループ</p> <p style="padding-left: 20px;">キャプティブポータル</p> <p style="padding-left: 20px;">VPNポータル</p> <p>監査ログ</p> <p>予約アップデート</p> <p>メンテナンス</p> <p>証明書管理</p> </div> <div style="width: 75%; padding-left: 5px;"> <p>ライセンス情報</p> <p>Cloud Edgeは、次世代のオンプレミスファイアウォールの利点とSecurity as a Serviceの利便性を兼ね備えた、マネージドサービスプロバイダ向けの製品です。Cloud Edge On-Premisesアプライアンスを顧客のオフィスに配置し、直観的なCloud ConsoleやRemote Managerを使用して、ユーザアクセスとセキュリティポリシーを一元的に管理できます。Cloud Edgeではユーザやポートを識別してアプリケーションを高度な処理能力をもって制御することで、ネットワーク侵害や業務の中断から顧客を保護します。また、VPNもサポートしており、モバイルデバイス、企業サイト、遠隔地の従業員による接続も保護します。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>ライセンスのステータス: 🚨 有効期限が切れています (猶予期間中)。 15 日後に切れます。</p> </div> <p>製品/サービス: Cloud Edge 100</p> <p>会社:</p> <p>バージョン/エディション:</p> <p>アクティベーションコード:</p> <p>有効期限:</p> </div> </div>				

8.2. 監査ログ

監査ログには、ユーザが Cloud Edge Cloud Console に対して実行した設定変更に関する情報が記録されます。

- ライセンス
- ユーザとアカウント
 - アカウント管理
- ユーザ認証
 - ユーザIDの同期
 - ホスト対象のユーザとグループ
 - キャプティブポータル
 - VPNポータル
- 監査ログ**
- 予約アップデート
- メンテナンス
- 証明書管理

監査ログ

期間の指定: 過去30日間

アカウントの選択:

次の中から選択:

SYS_ACCOUNT

>

>>

<<

<

選択済み:

10 レコードの表示 エクスポート クエリ

日時	ユーザ名	ホスト	処理	結果
2015-11-24 09:02:04			ログイン	成功
2015-11-23 23:57:33			ログイン	成功
2015-11-23 23:36:20			レポートテンプレートレポートの削除	成功
2015-11-23 23:30:49			お気に入りログ不正検出ログの追加	成功
2015-11-23 21:54:09			ポリシー配信の開始	成功
2015-11-23 21:54:07			ゲートウェイCE50_RDのゲートウェイプロファイルを default profileに変更	成功

8.3. 証明書管理

Cloud Edge Cloud Console の HTTPS セキュリティ証明書をエクスポートまたは再生成します。

証明書をエクスポートするには、[エクスポート] をクリックしてから、証明書をローカルコンピュータに保存します。

※再作成した場合には、ローカルコンピュータへの証明書の再保存が必要になります。

①HTTPS 復号証明書の再生成

SSL 複合証明書より「再生成」をクリックし Cloud Edge.crt ファイルを保存します。

ライセンス	SSL 復号証明書
ユーザとアカウント	 この証明書は、SMTPS、POP3S、IMAPS、およびHTTPSで使用されるSSL復号に使用されます。ただし、初期設定の証明書にインターネット上の既知の(信頼できる)CAによる署名がありません。ユーザがHTTPS Webサイトにアクセスするたびに、ブラウザに証明書の警告が表示されます。この警告が表示されないようにするには、この証明書をエクスポートしてブラウザにインストールします。
アカウント管理	発行先 CloudEdge
ユーザ権限	発行元 CloudEdge
ユーザIDの同期	有効期限 2044-01-10 08:52:04 JST+0900
ホスト対象のユーザとグループ	エクスポート 再生成
キャプティブポータル	証明書
VPNポータル	PEMエンコード形式のX509証明書ファイル(.crtまたは.pem)を選択してください。インポート処理により、選択した証明書がSSL復号用の信頼された証明書のリストに追加されます。
監査ログ	公開証明書: <input type="text"/> 参照
管理者アラート	秘密鍵: <input type="text"/> 参照
予約アップデート	PEMエンコード形式のX509証明書には秘密鍵ファイルが必要です。
メンテナンス	パスフレーズ(任意): <input type="text"/>
証明書管理	保存 キャンセル

※サードパーティの CA 証明書をインポートする場合は証明書より公開証明書と秘密鍵をインポートします。

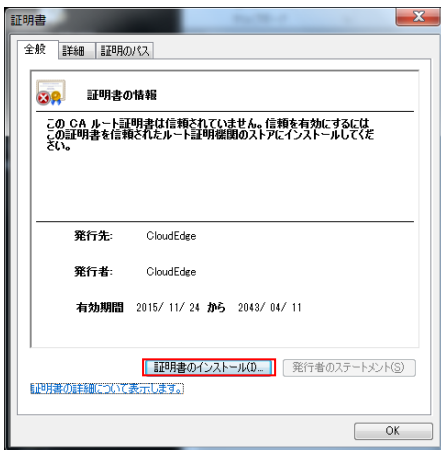
②Cloud Edge 証明書のインストール

HTTPS 復号化機能を有効にした Cloud Edge 経由でインターネット接続を行う全てのコンピュータに Cloud Edge.crt ファイルをインストールします。

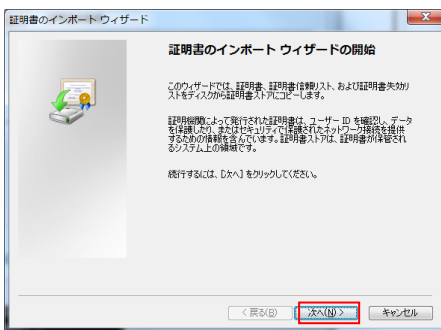
※各ブラウザやメーラーにインストールする必要があります。

Internet Explore の場合

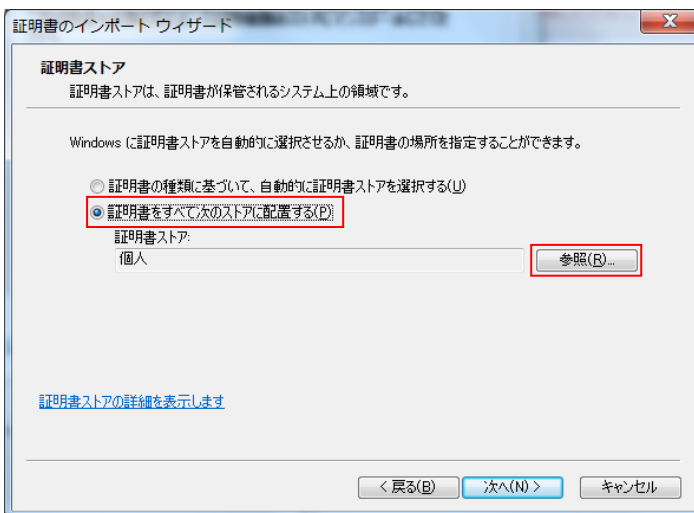
Cloud Edge.crt ファイルをコンピュータで実行し、証明書インストールをクリックします。



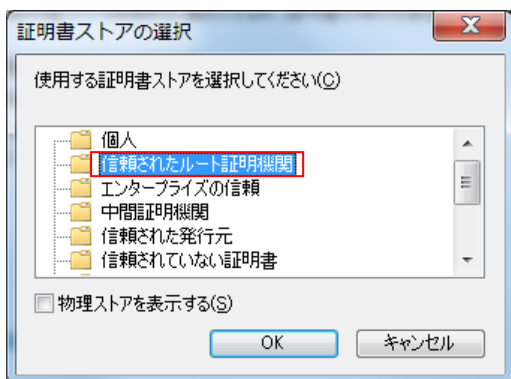
インストールウィザードが開始されますので「次へ」をクリックします。



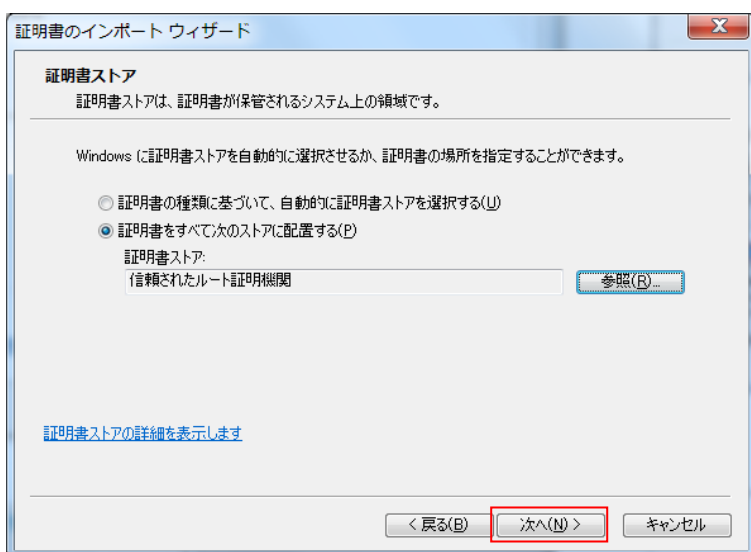
「証明書をすべて次のストアに配置する」を選択し参照をクリックします。



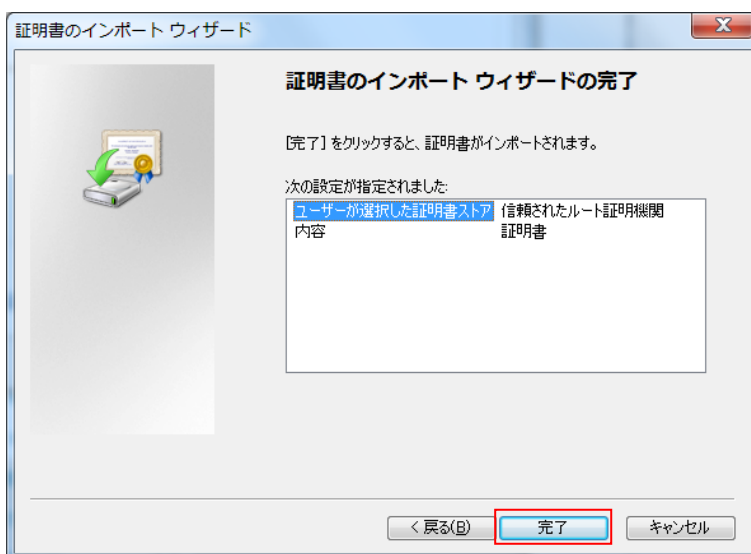
証明書ストアの選択にて「信頼されたルート証明機関」を選択し OK をクリックしてください。



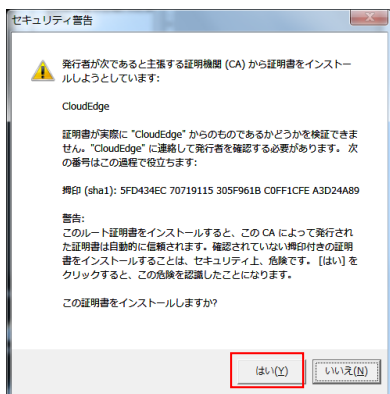
「次へ」をクリックします。



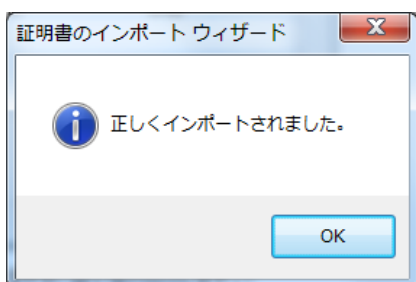
完了をクリックして証明書インポートウィザードを完了します。



セキュリティ警告が表示されますが、はいをクリックします。



OK をクリックして終了します。これでコンピュータに Cloud Edge の証明書が保存されました。



③HTTPS サイトのブラウザ表示

証明書をインストールするとセキュリティ警告が表示されず正しく表示されます。



SaaS 型セキュリティ Box

Cloud Edge あんしんプラス

ユーザーズガイド Version1.24

発行日 : 2022 年 8 月 12 日

発行元 : 日本事務器株式会社