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

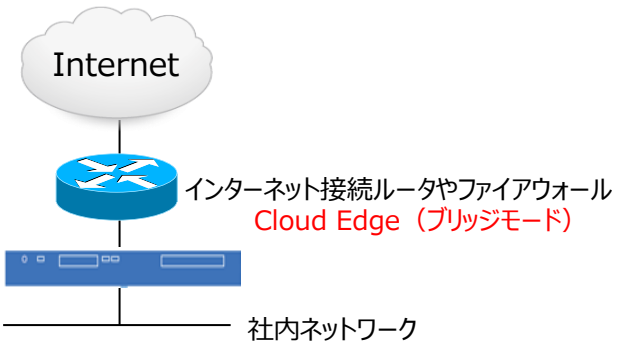
本ユーザーズガイドは、Cloud Edge あんしんプラス（以下「本サービス」と称す）」の個別設定について記載いたします。
詳細な設定内容については別途管理コンソールのオンラインヘルプをご確認ください。

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	80 443	http(s)://www.trendmicro.com
		http(s)://www.apple.com
		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

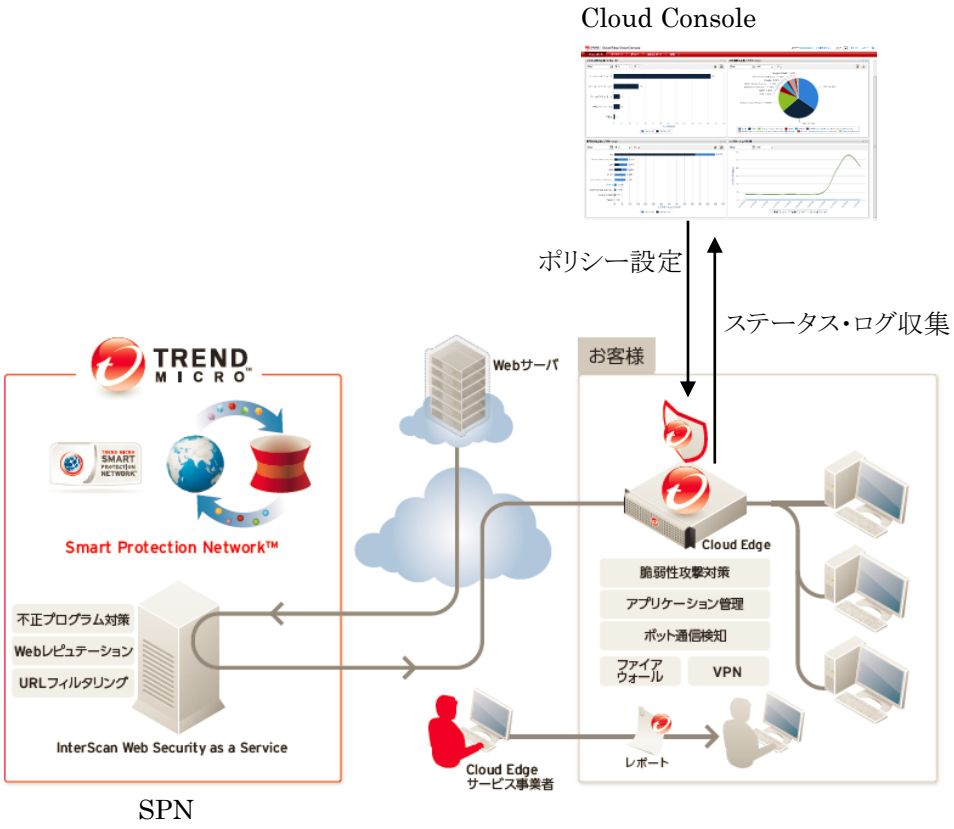
HTTPS 復号機能を有効にしていなくとも、URL のホスト名でカテゴリが判定できる通信に関しては、URL フィルタ、Web レピュテーションで不正な HTTPS サイトをブロックすることが可能になります。

※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、先出センドバック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。

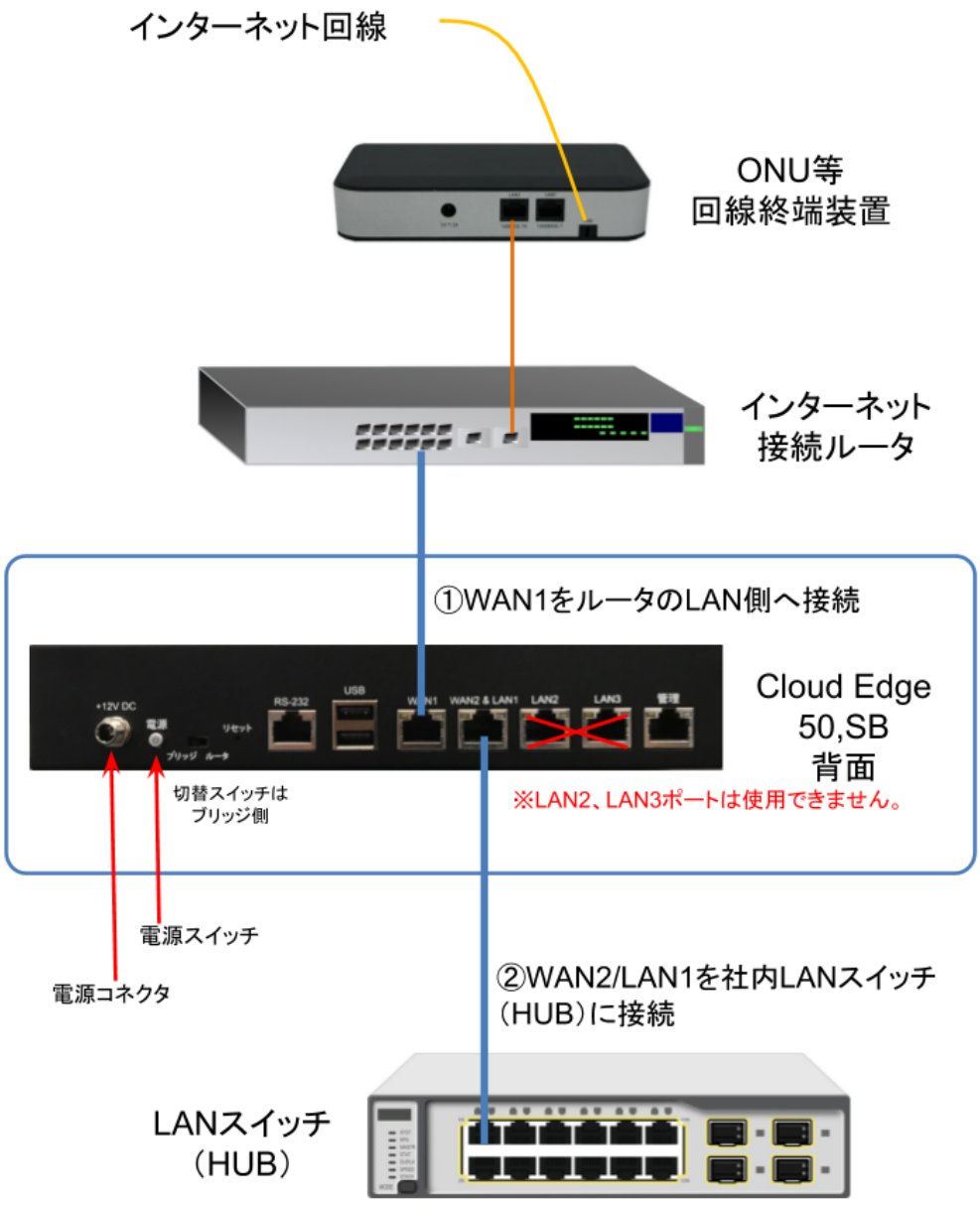
2. 導入手順

サービス利用開始について説明いたします。

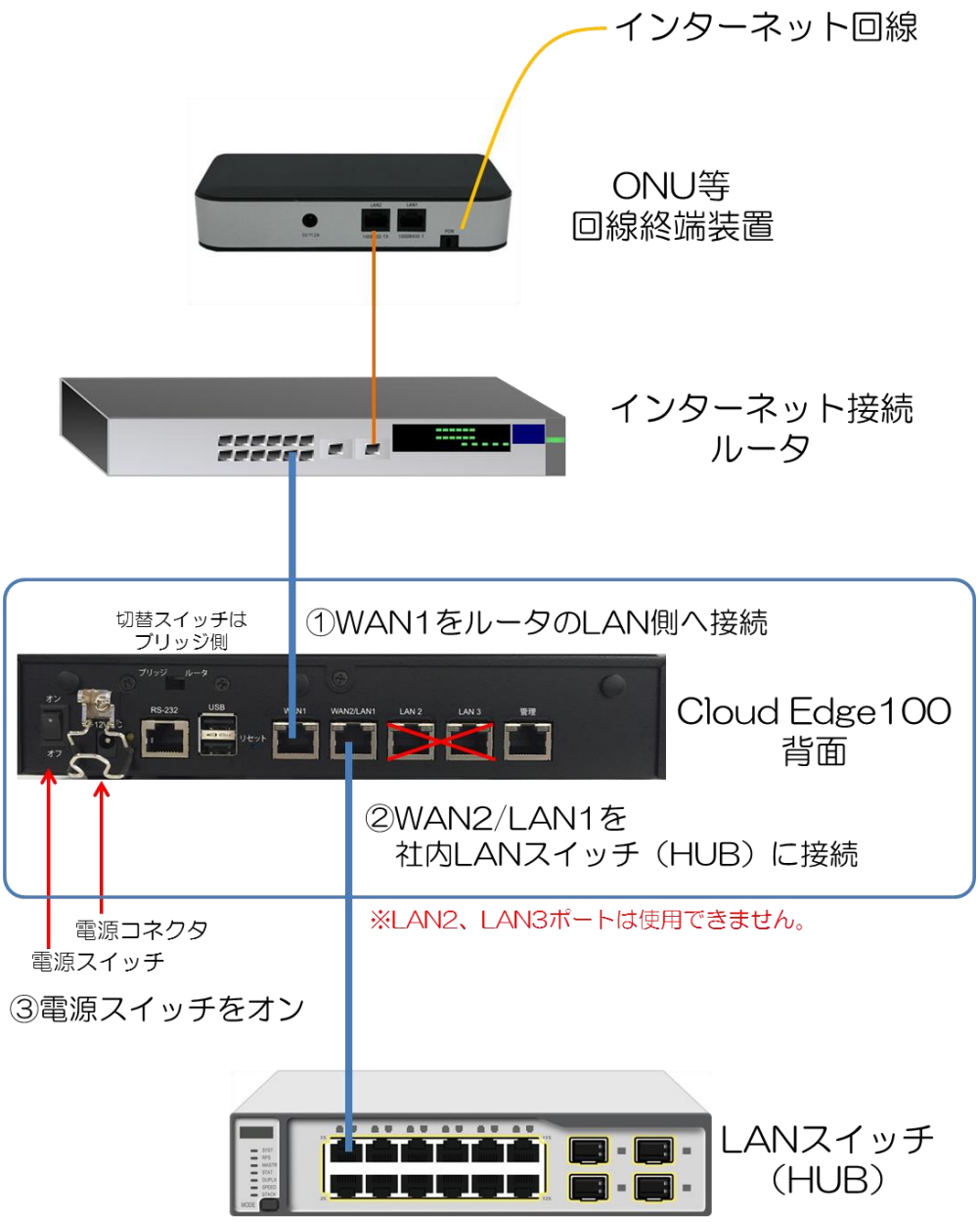
2.1. Cloud Edge の設置

■Cloud Edge をネットワークに接続します。

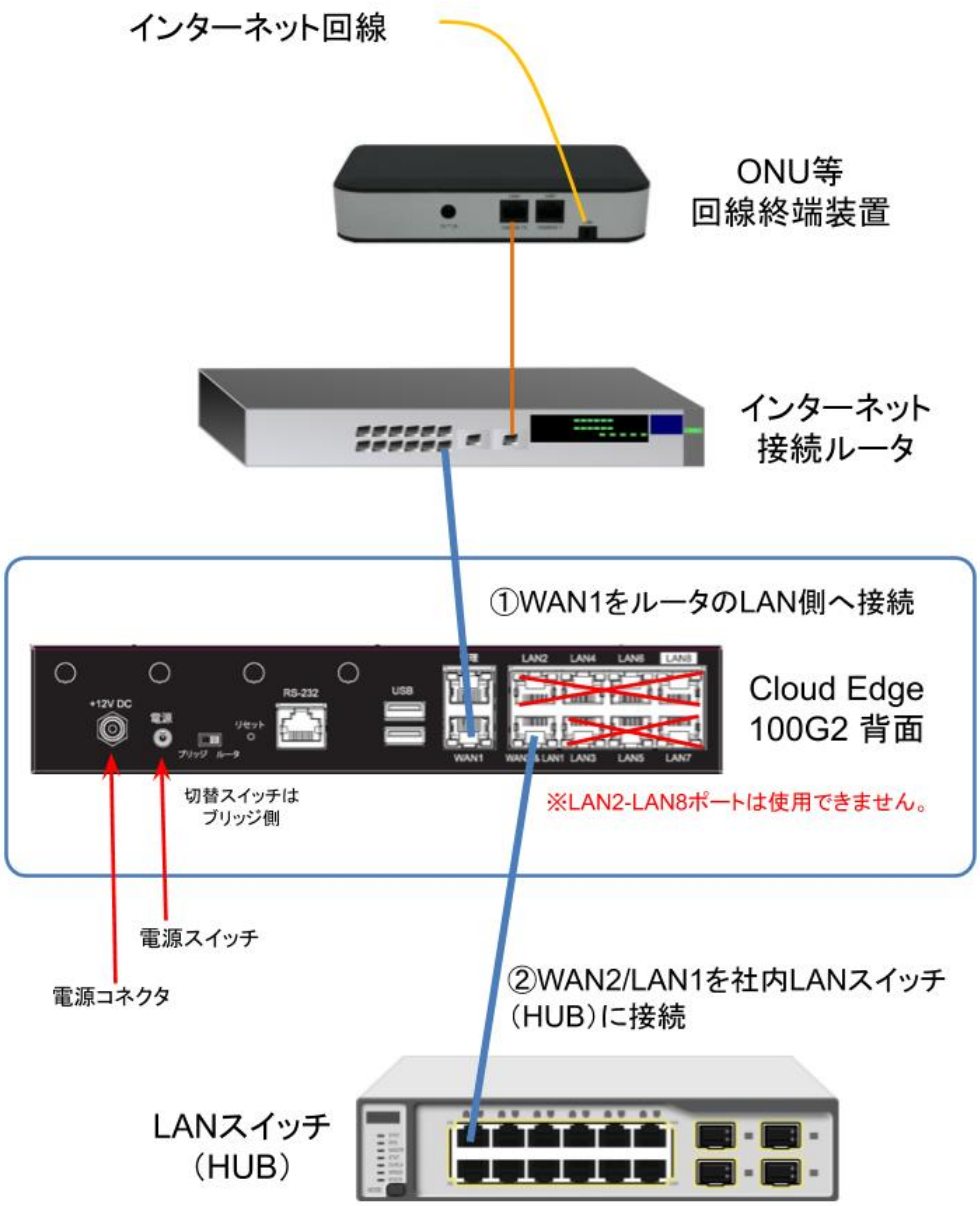
Cloud Edge50 および SB 接続方法



Cloud Edge100 接続方法

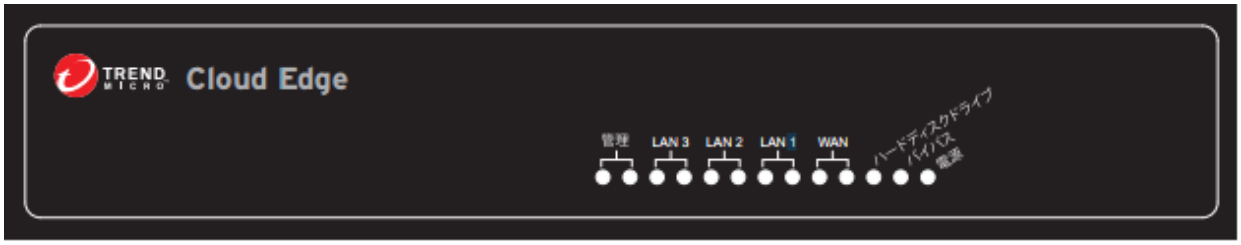


Cloud Edge100 G2 接続方法



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】
pfsl-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。

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 からも管理コンソールへのログイン画面を開けます。

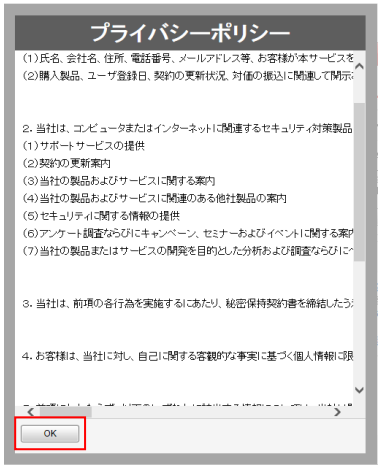
②ログイン

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。

(1)プライバシーポリシーの確認画面が表示されます。

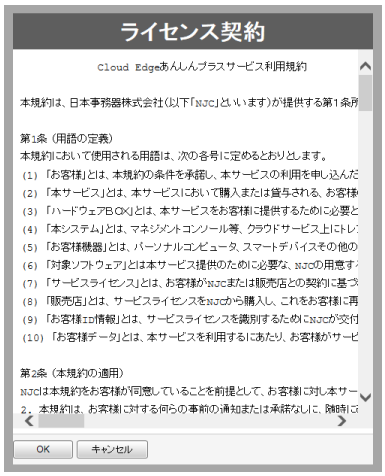
個人情報の取り扱いに同意した上で先に進んでください。

※最初のログイン時のみ表示されます。



(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:

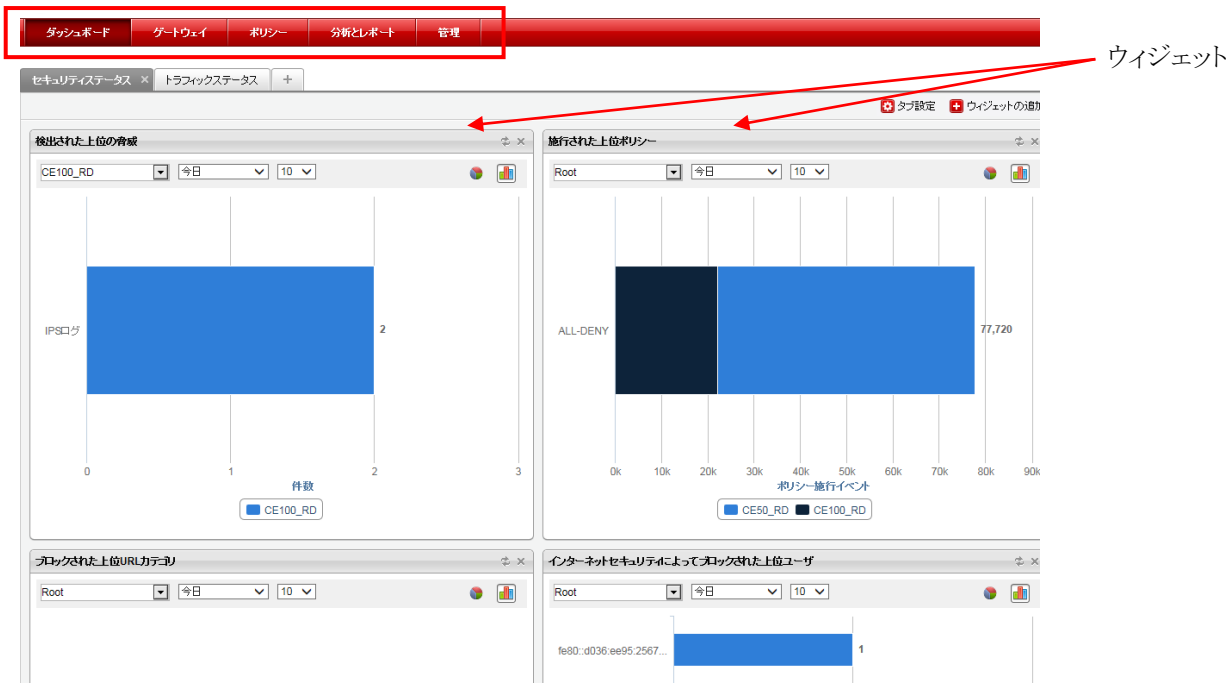
Cloud Edge を通過するトラフィックを制御するポリシールールを管理します。

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:

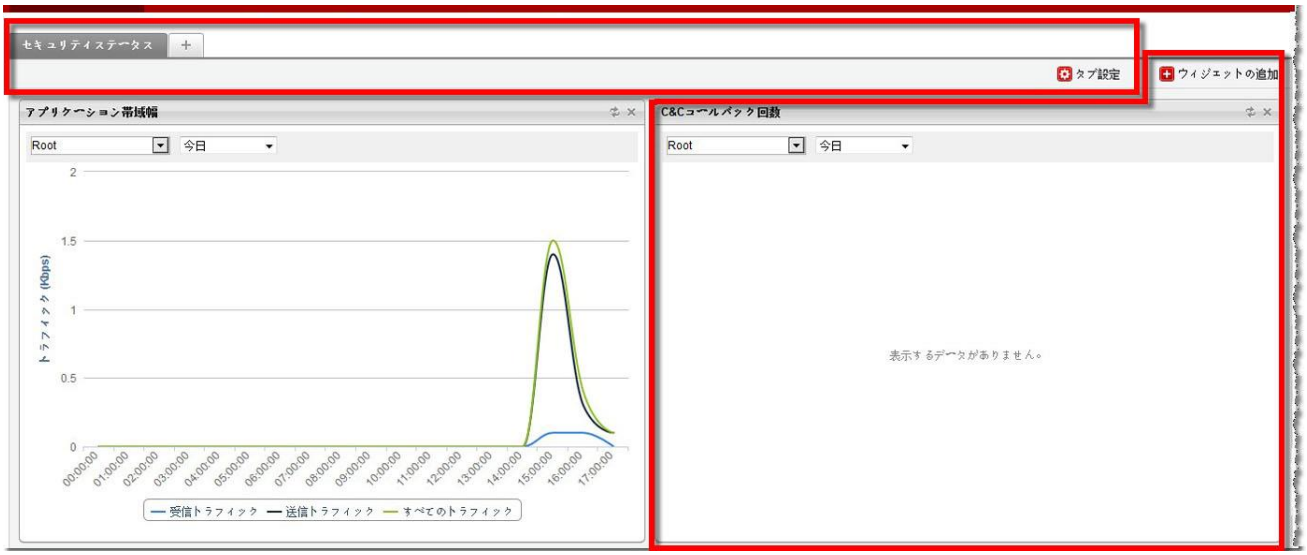
HTTPS 復号証明書を利用する場合に使用します。※証明書管理以外は設定変更されないようお願いします。



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。



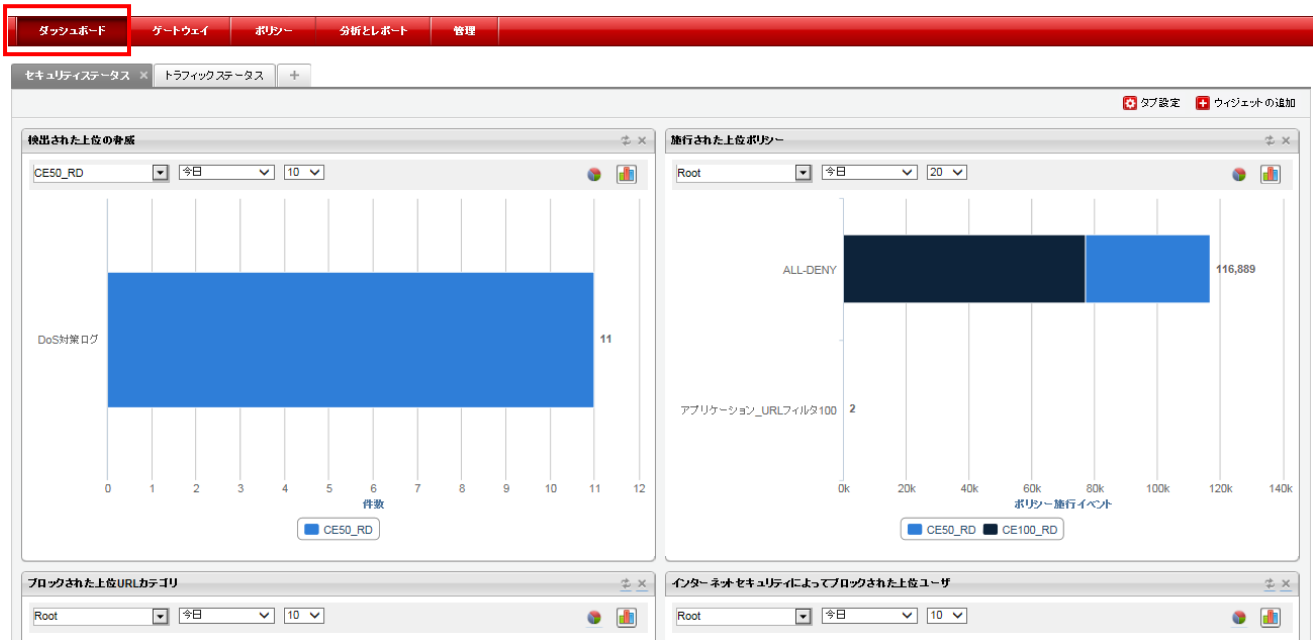
・タブ
タブはダッシュボードを管理するための単位であり、1 つのタブに複数のウィジェットを配置することができます。それぞれのタブの中に複数のウィジェットをまとめることができます。タブやウィジェットを追加または変更することで、必要に応じてダッシュボードをカスタマイズできます。ダッシュボードでサポートされるタブの数は 10 個までです。各タブには、最大 10 個のウィジェットを含めることができます。

・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

施行された上位ポリシー*

ブロックされた上位 URL カテゴリ*

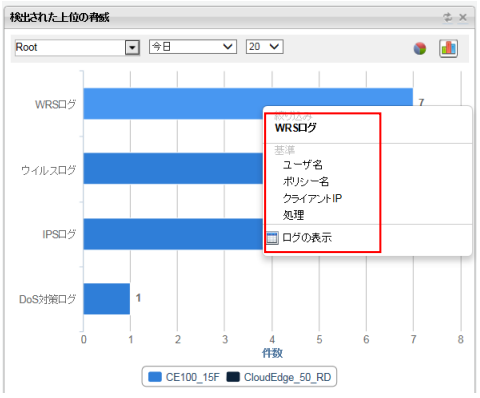
インターネットセキュリティによってブロックされた上位ユーザ*

* 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

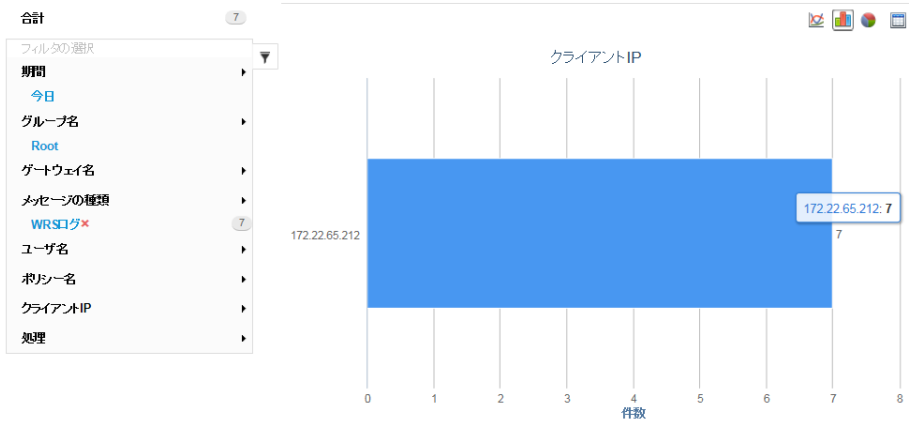
①WRS ログ確認

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。

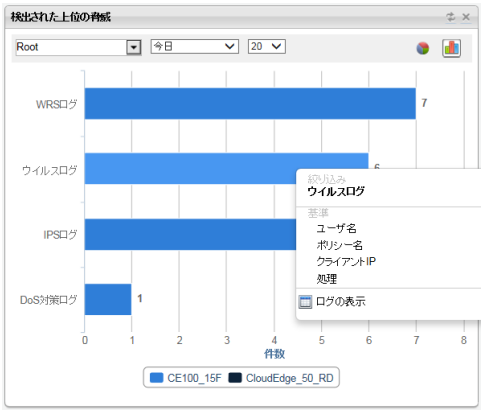


対象のクライアントで検出したログを表示します。

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。

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。



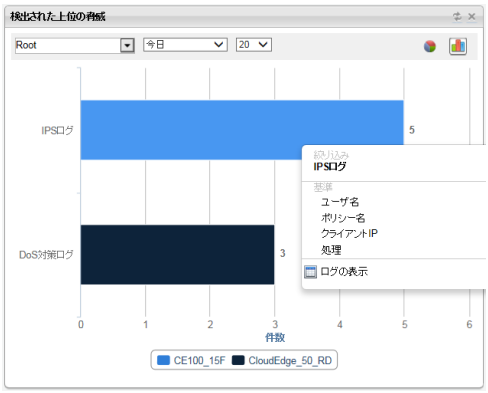
検出したログを表示します。

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。

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。

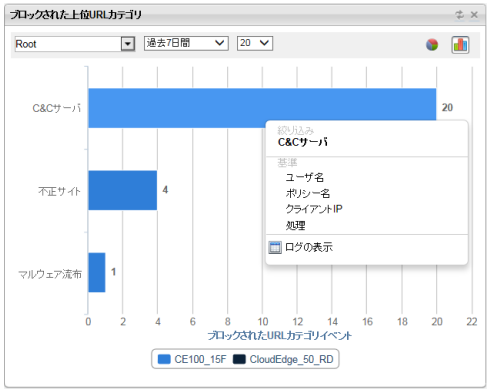
ブロックした IPS ルールも表示されます。

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...
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。

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

6. ポリシー

ポリシーについて説明します。

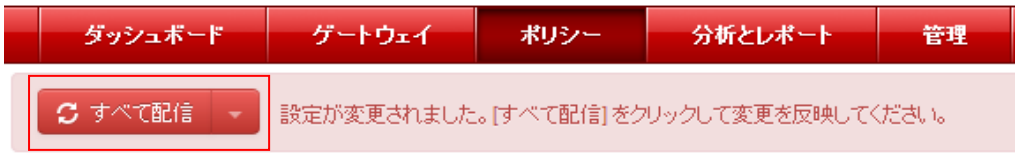
6.1. ポリシールール

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。

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】

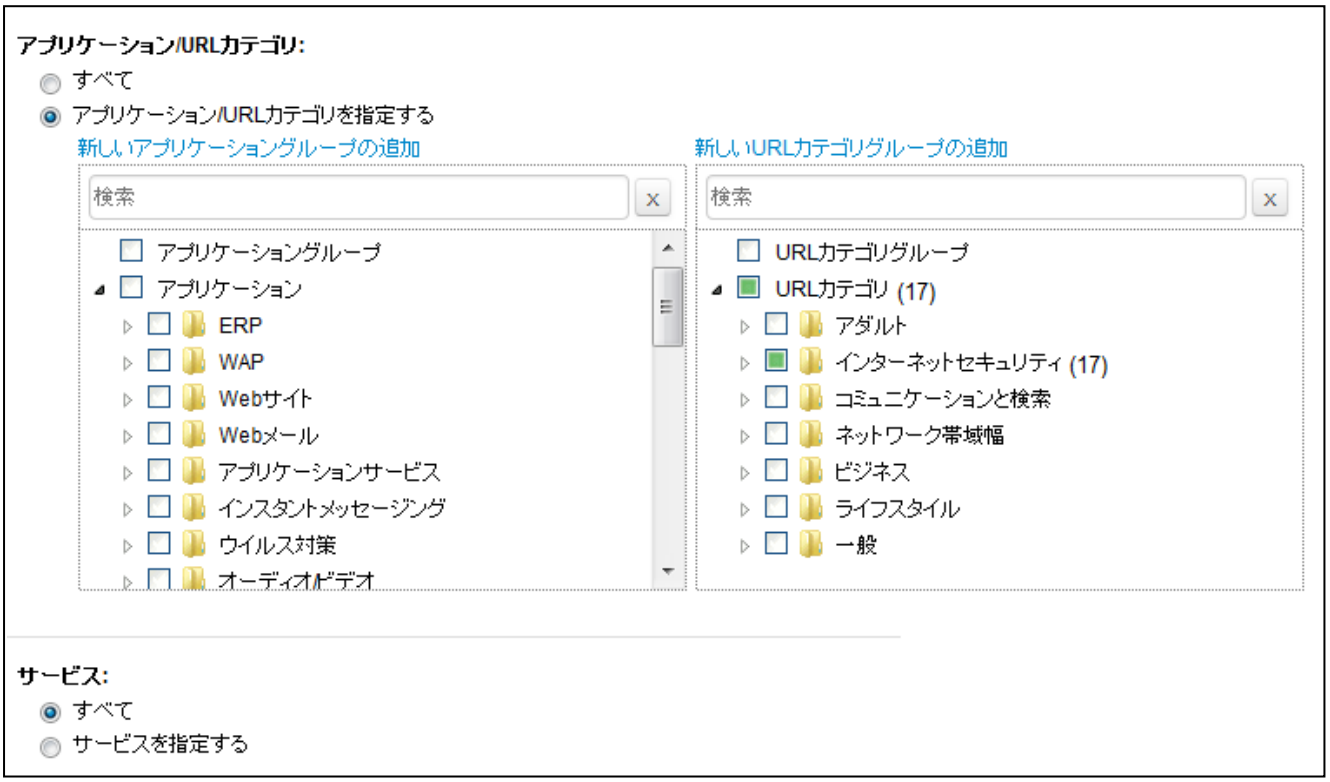
アプリケーション制御や URL フィルタを設定変更する場合はルール名「アプリケーション_URL フィルタ」を編集します。

選択したものが、ブロックされます。

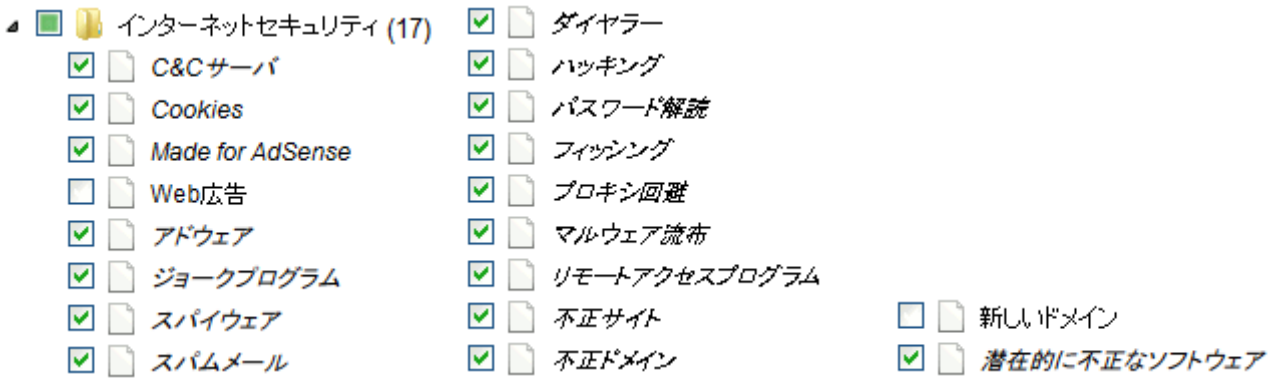
アプリケーション：ブロックなし

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



■インターネットセキュリティ詳細



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。

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。

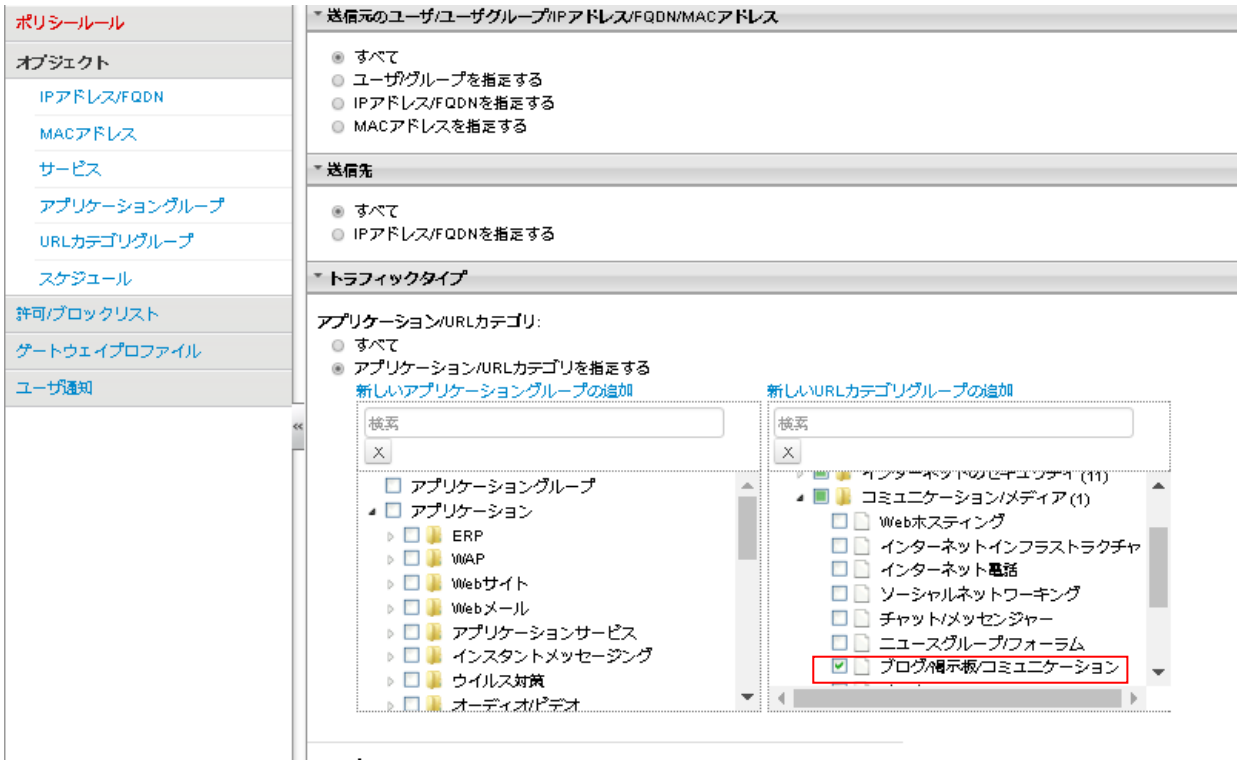
ケース①URL フィルタ設定

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。

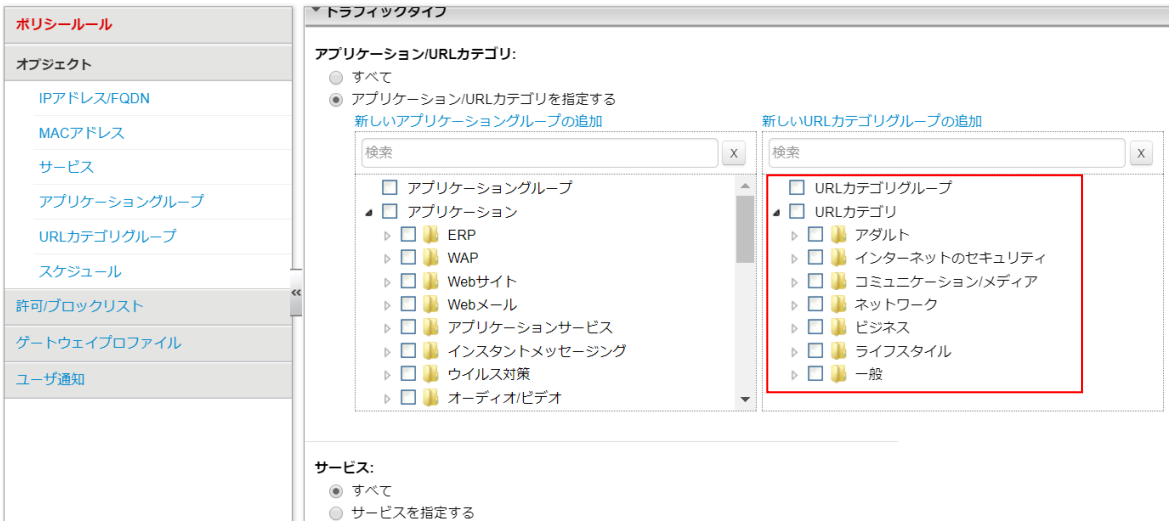
ケース②URL フィルタを無効にする

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。

URL カテゴリよりインターネットセ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。



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。

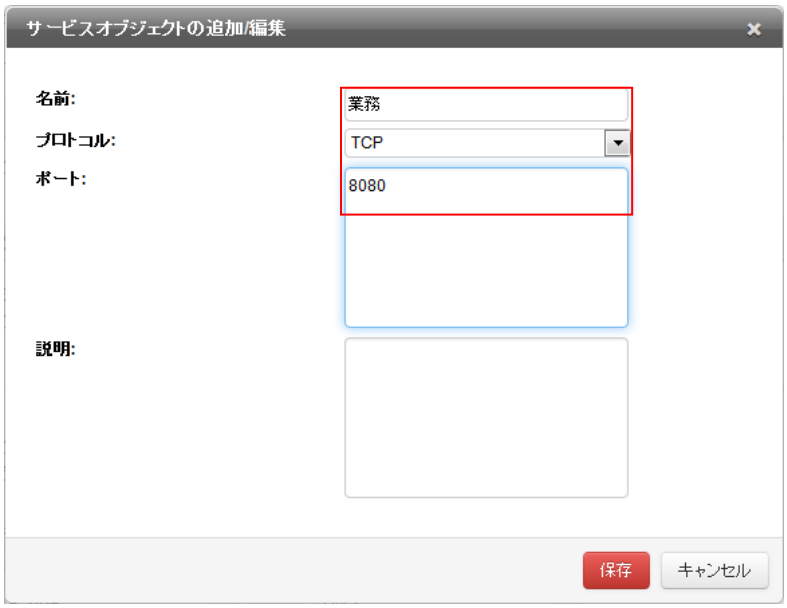
サービスに追加するポート番号を入力して保存します。

(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。

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 拠点があり Active Directory 認証を許可する場合

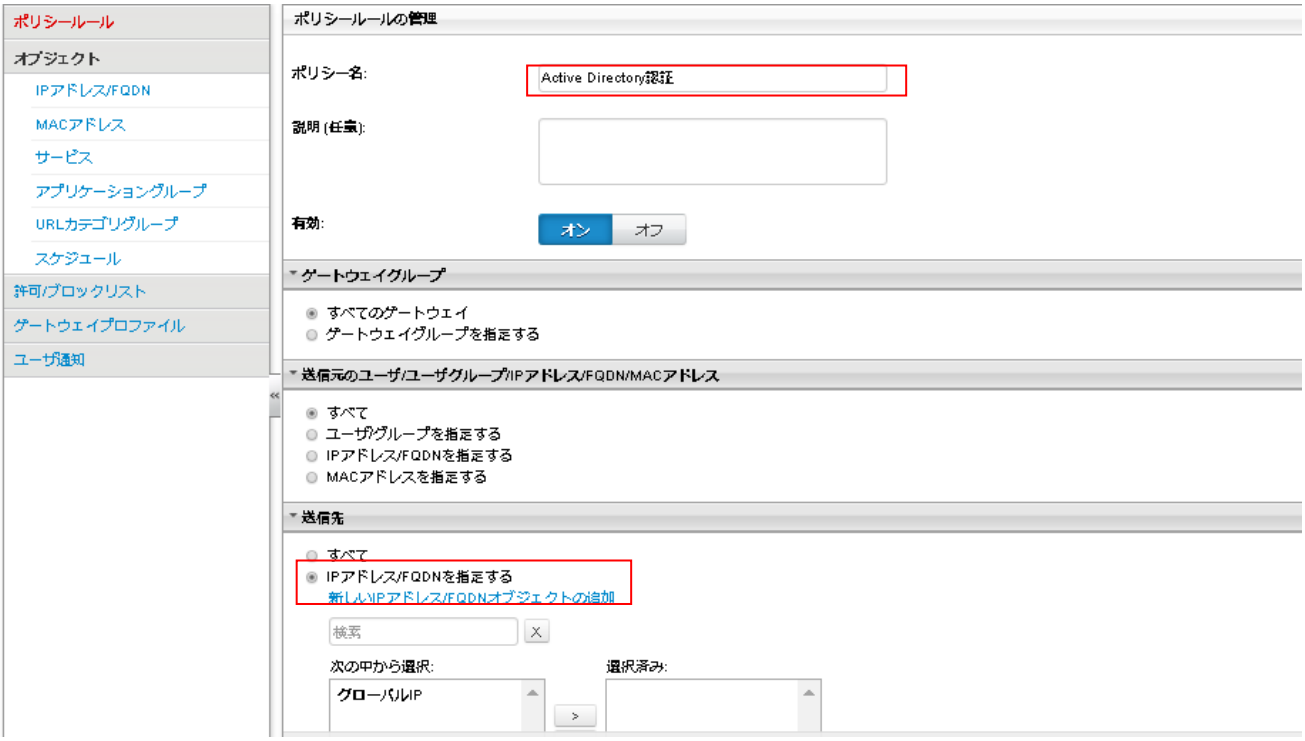
Active Directory 認証で利用される RPC 動的ポートは許可するポート範囲が広いため既存のルールに許可ルールを追加すると全ての宛先（インターネット向き）に対して許可されてしまいます。そのため許可する宛先（Active Directory サーバ）を指定したポリシーを新たに作成することを推奨します。

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

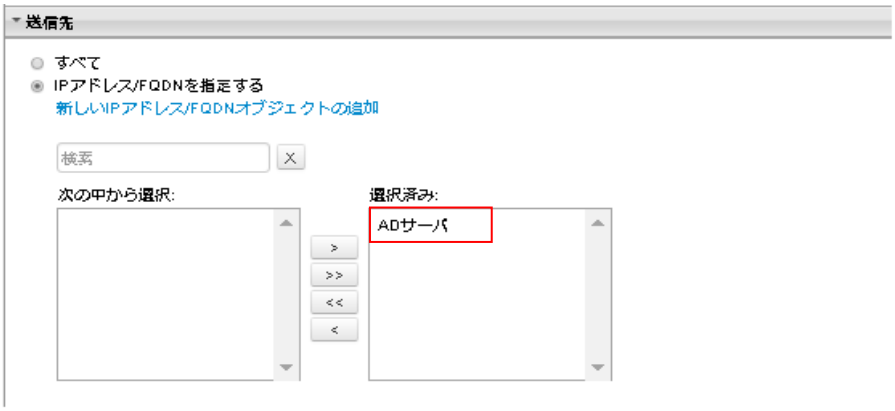
プロトコル：IPv4

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 を措定します。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

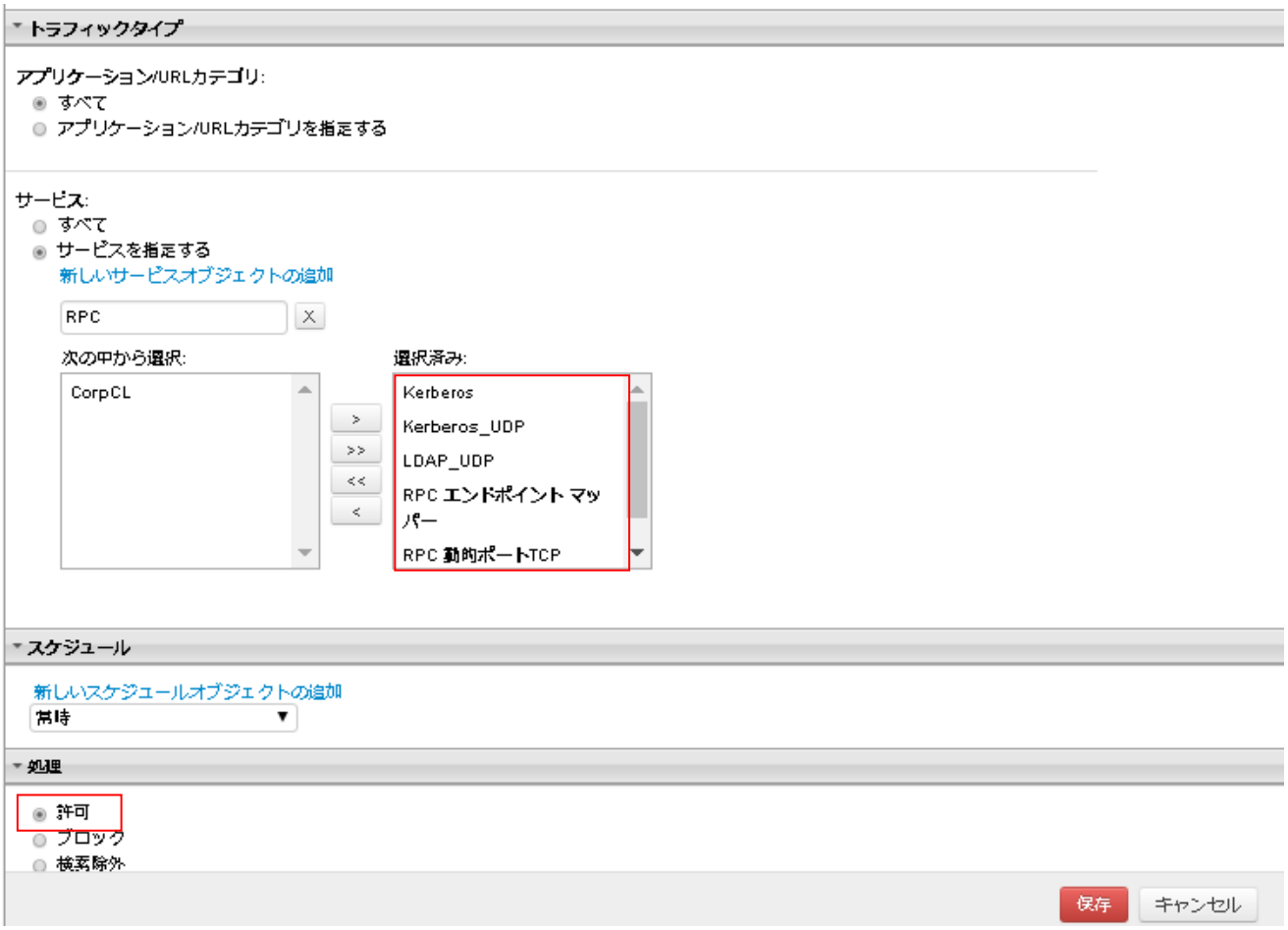
LDAP_UDP

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。



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。

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。

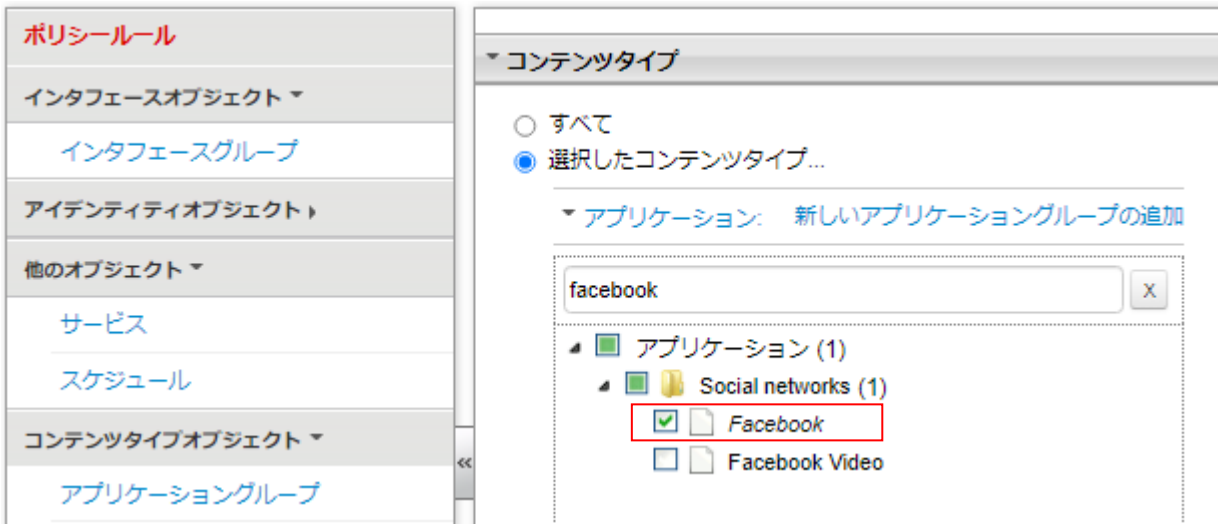
例えばSNSの閲覧はできるが、投稿はさせない。ストレージサービスのDropboxでアップロードはできるが、ファイルダウンロードはさせない。のような細かな制限はできません。

Facebookと Twitterをブロックする場合の例

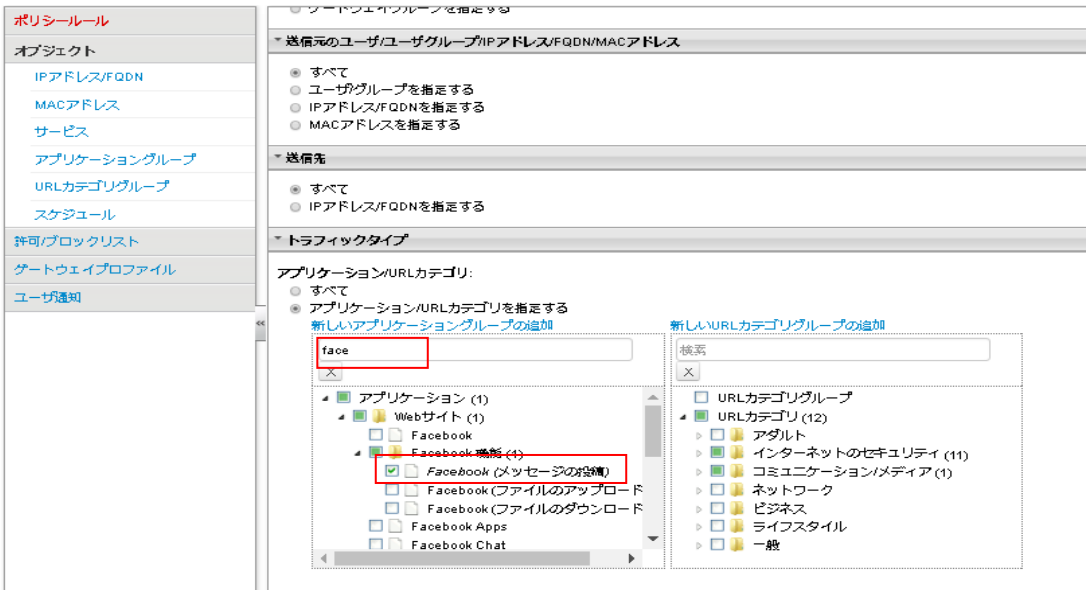
ポリシー＞ポリシールール＞ポリシールールの管理よりアプリケーション_URLフィルタをクリックします。

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。

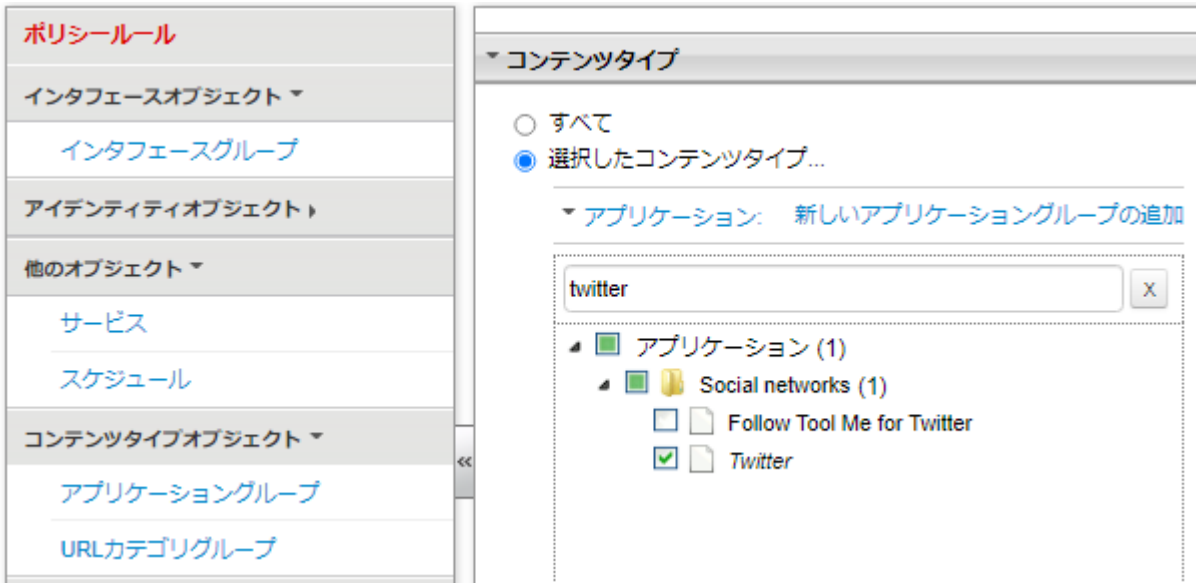
アプリケーション一覧から選択すると探し出すことが困難なため検索欄にアプリケーション名を入力することで表示項目を絞れます。



【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。

ポリシールールの複製を作成します。

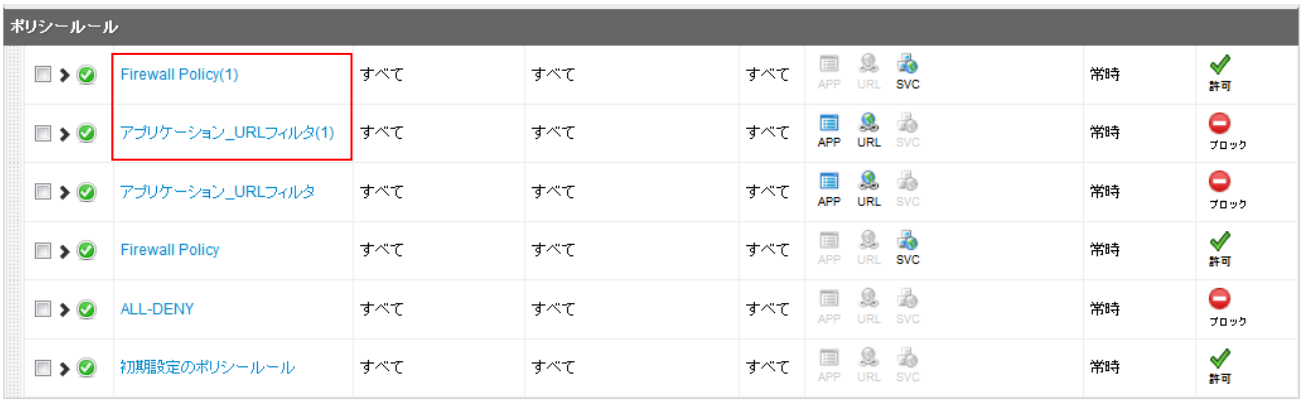
ポリシー＞ポリシールール＞ポリシールールの管理より

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。

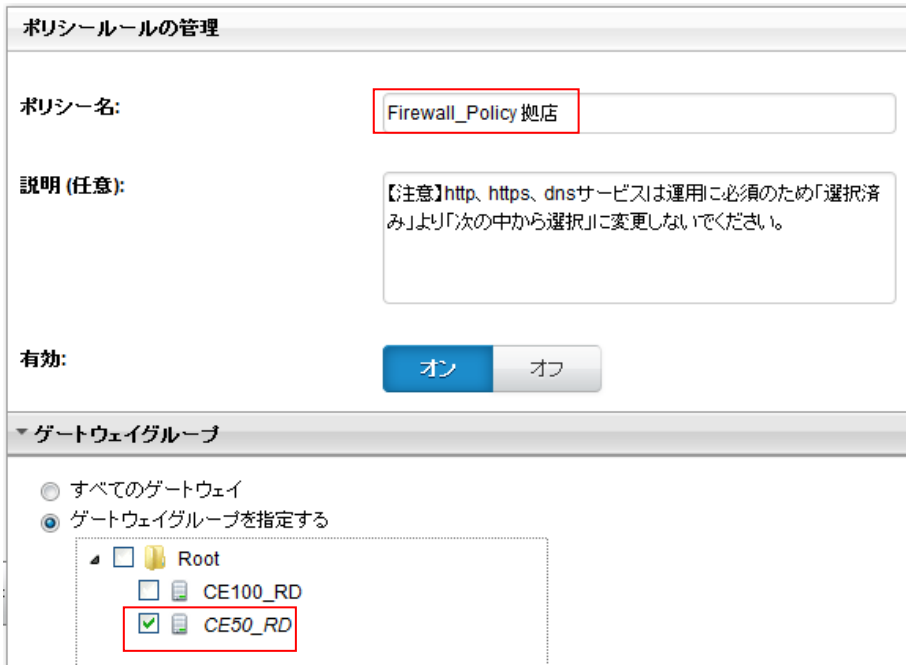
複製されたポリシー　Firewall Policy（1）　をクリックしてください。



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

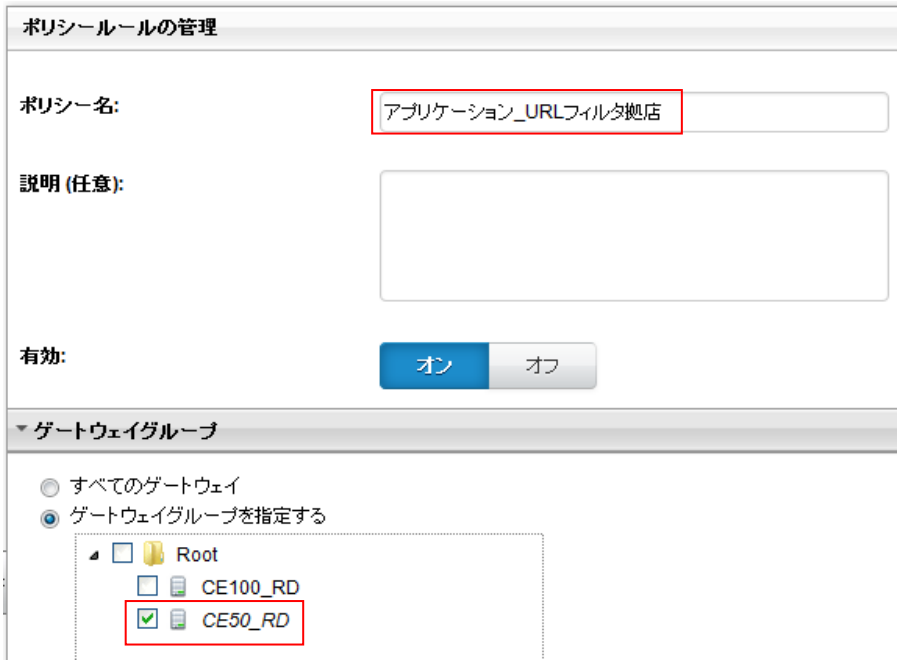
ゲートウェイグループの「ゲートウェイグループを指定する」を選択し Cloud Edge50 のみ選択します。

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



「Firewall Policy 拠店」よりも「アプリケーション_URL フィルタ拠店」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 フィルタ拠店ポリシーにチェックを入れ Firewall Policy 拠店の上へ移動します。

拠店用 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。

拠店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。

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。

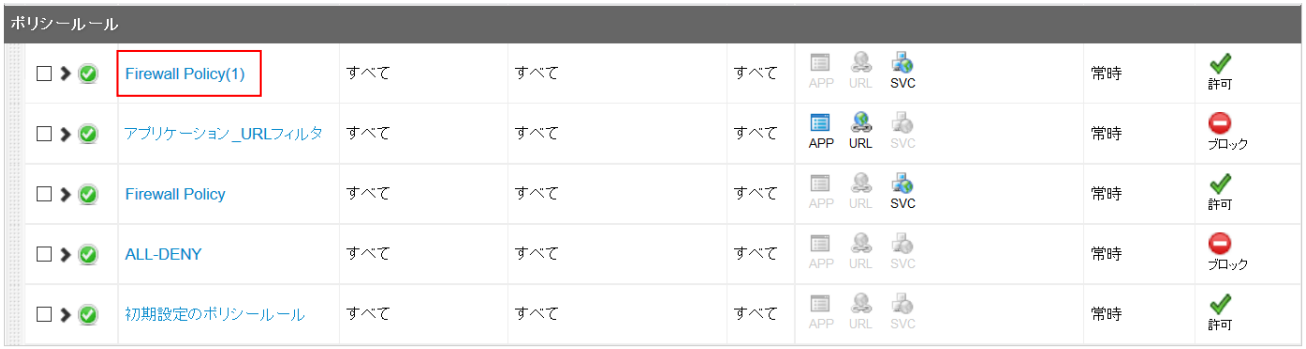
ポリシー＞ポリシールール＞ポリシールールの管理より

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。

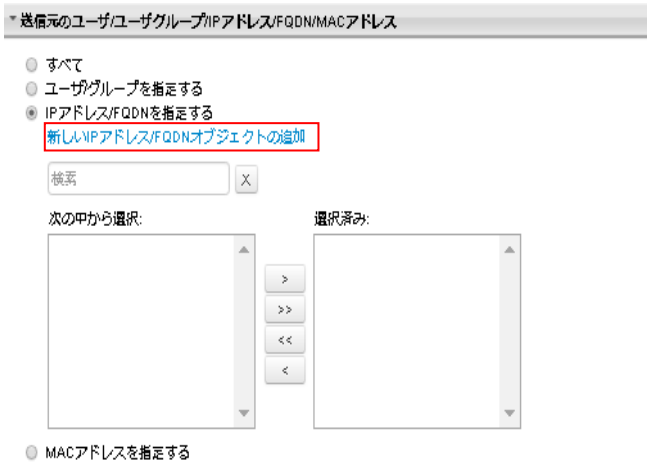
複製されたポリシー　Firewall Policy(1)　をクリックしてください。



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

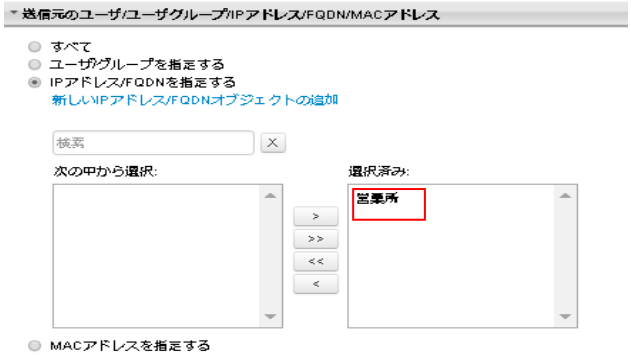
プロトコル：IPv4

IP アドレス：本ケースの場合 192.168.10.0/24

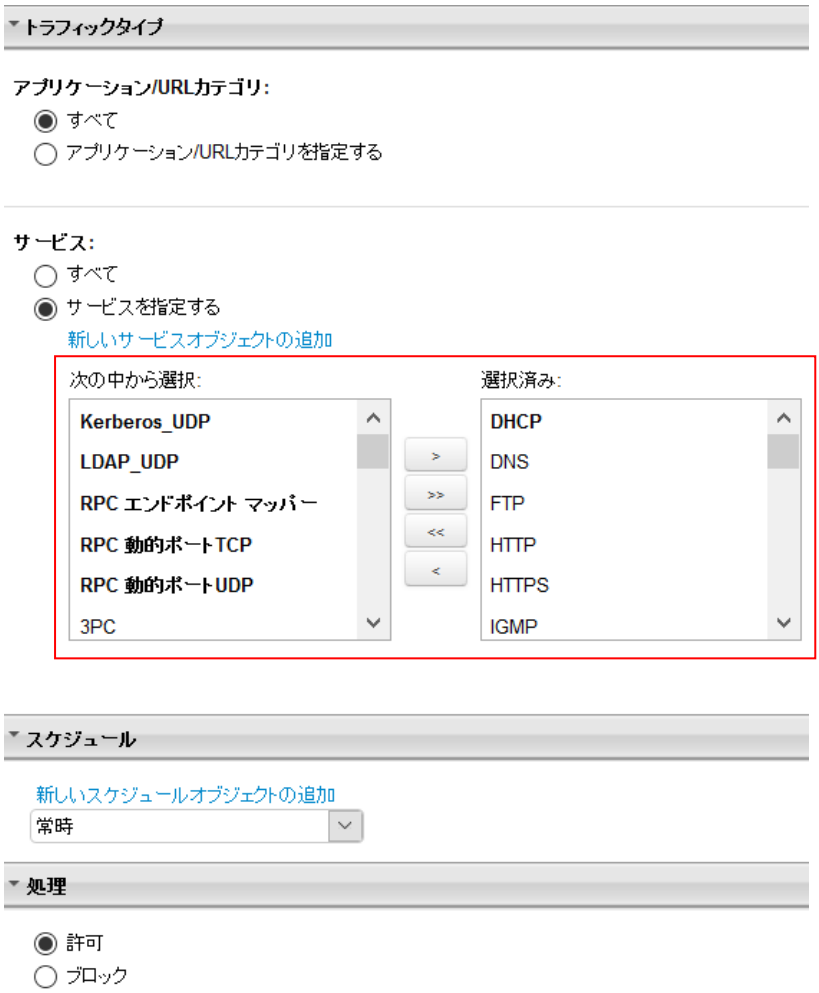
※IP アドレスまたは CIDR を指定します。複数のアドレスはカンマで区切ります。

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。



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。

「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

ポリシールールの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。

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。

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に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。

追加するサービスオブジェクトを入力して保存します。

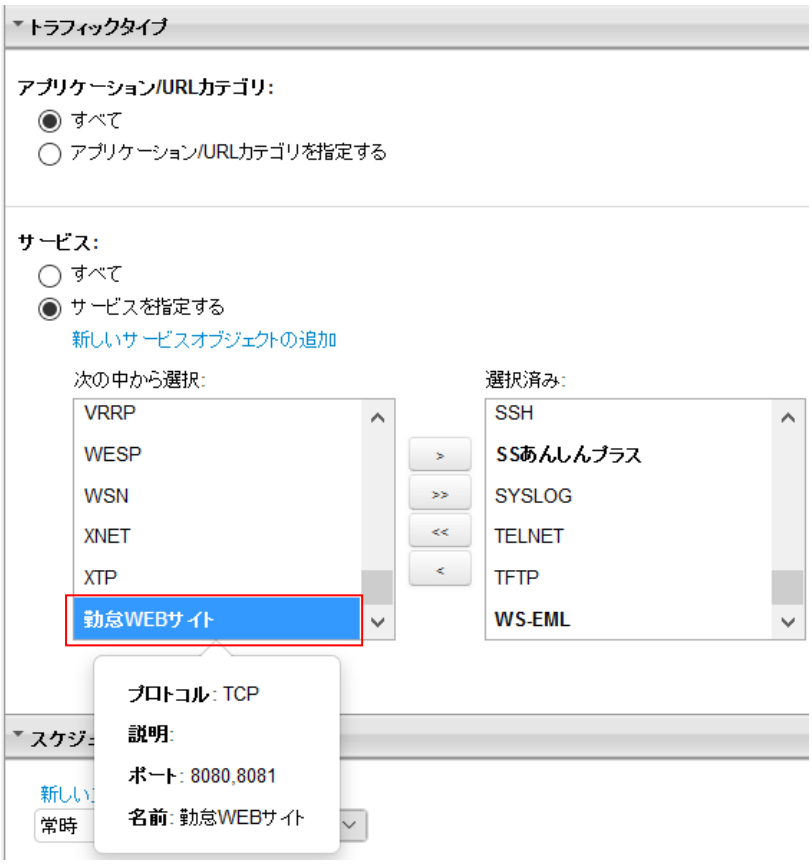
名前：任意

プロトコル：TCP/UDP/ICMP

ポート：例）8080,8081

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。

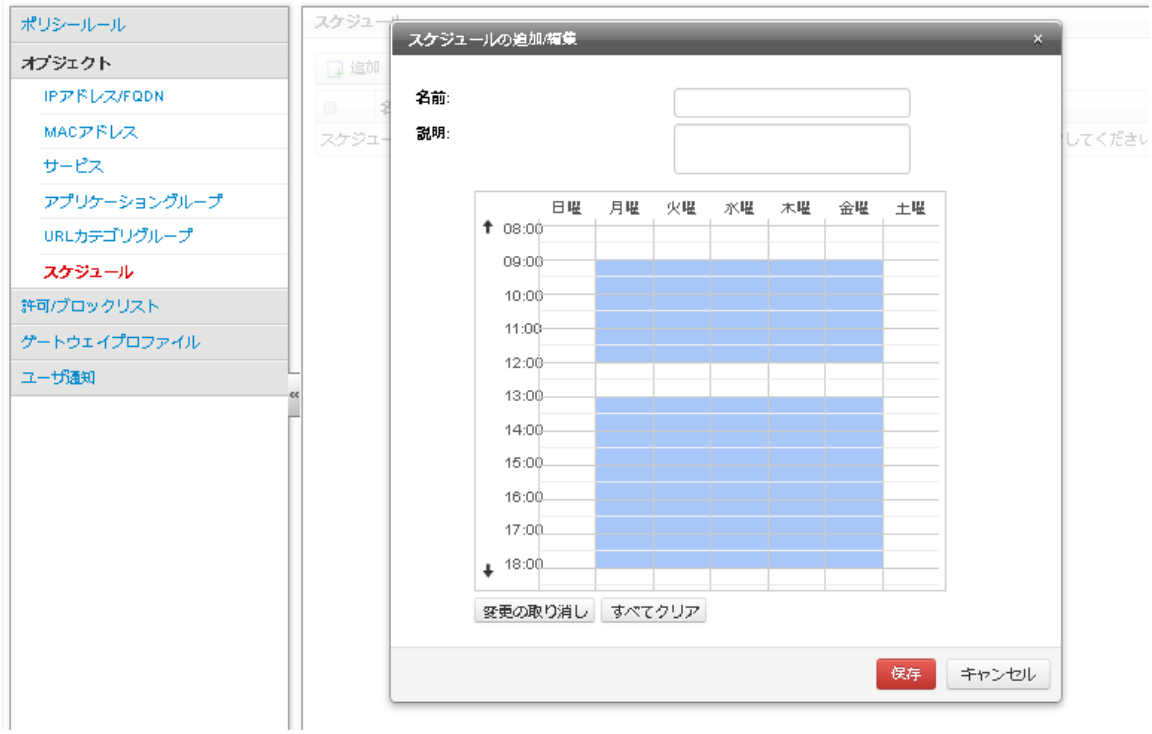


②スケジュール

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。

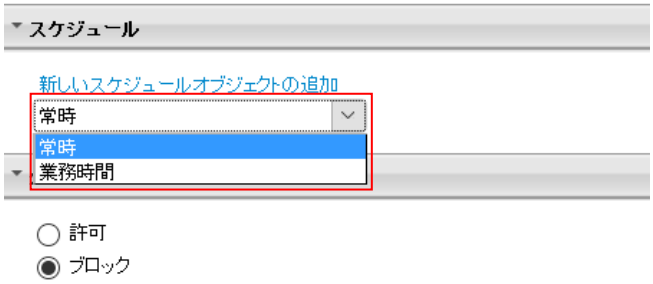
名前:任意

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

ポリシールール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。

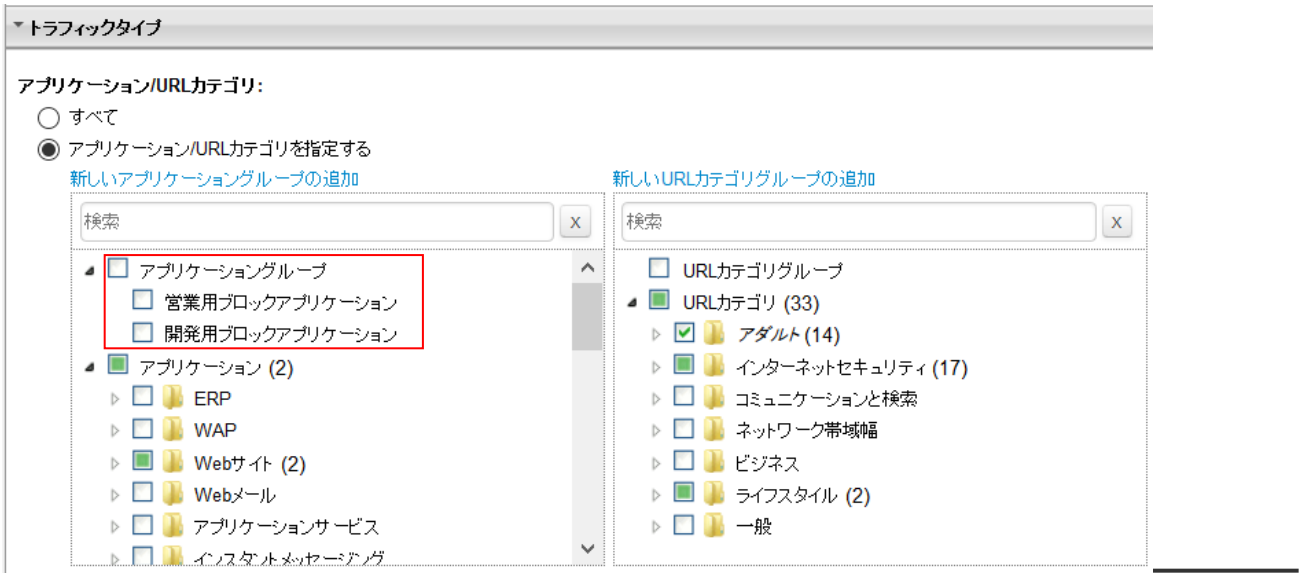
①アプリケーショングループ

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。

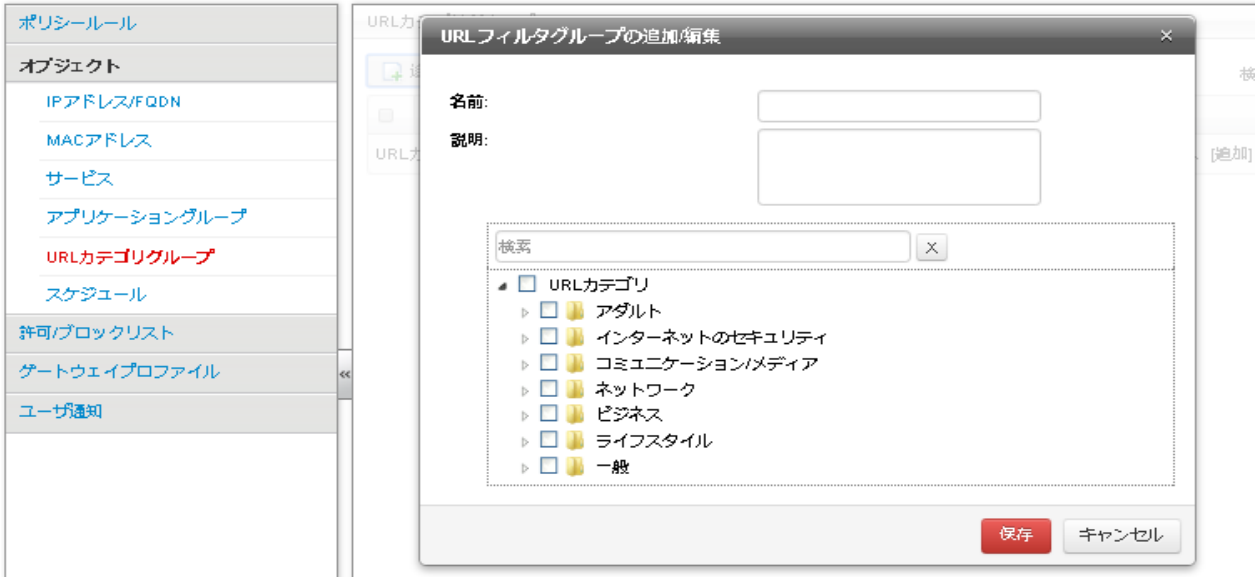
作成したアプリケーショングループはポリシーのアプリケーショングループとして指定することができます。



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。

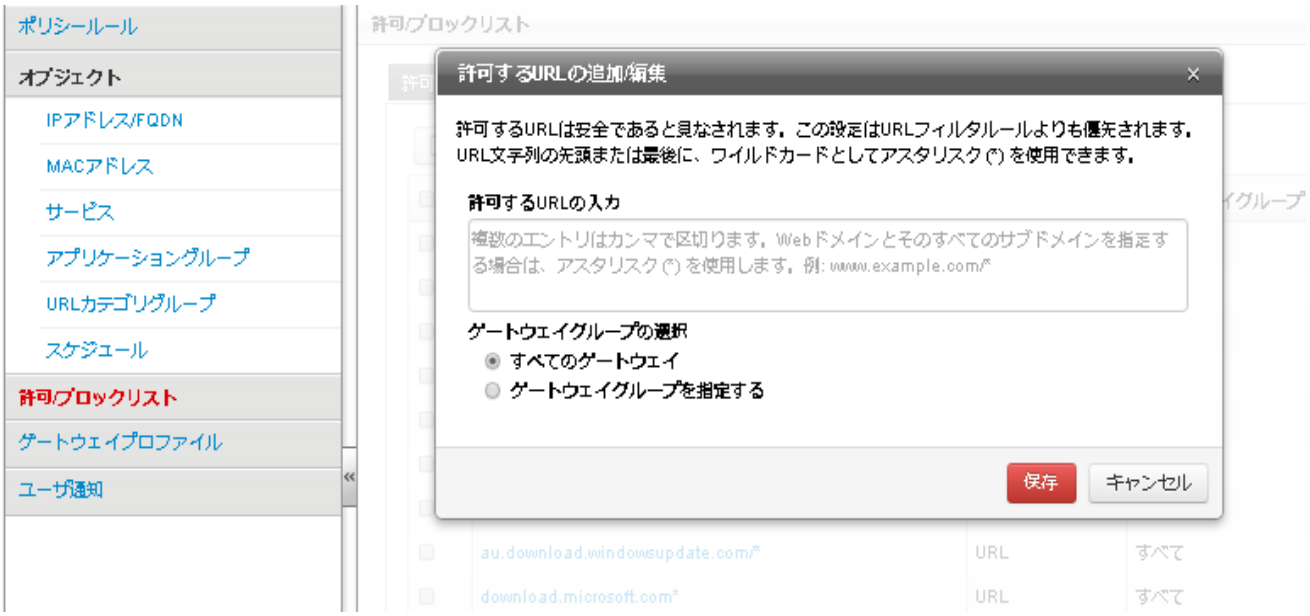
6.7. 許可/ブロックリスト

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。



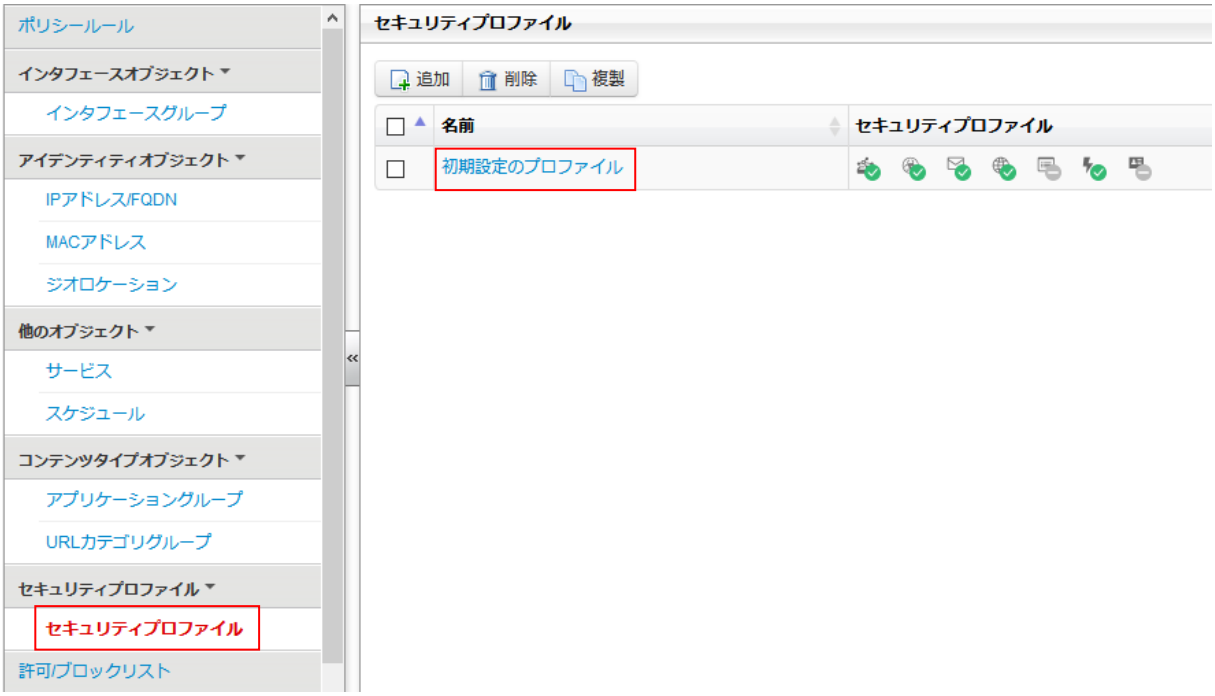
URL を入力後、保存をしてください。

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「初期設定のプロフィル」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。

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： メールの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。

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。

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)

・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)

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。

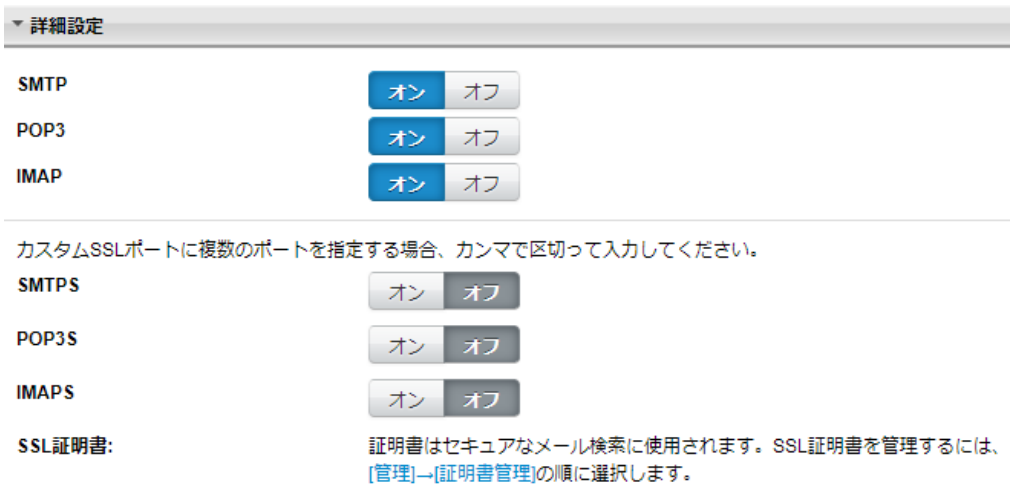
除外リスト

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。

詳細設定

SMTPS/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。

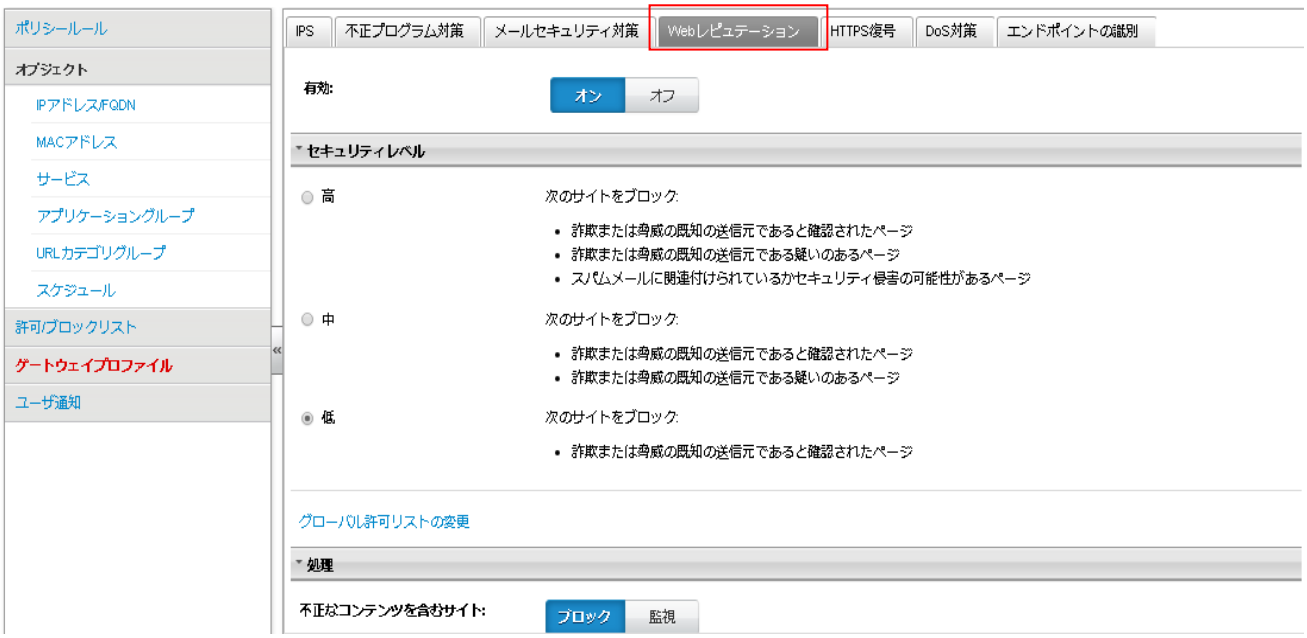


④Web レピュテーション

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ミング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）



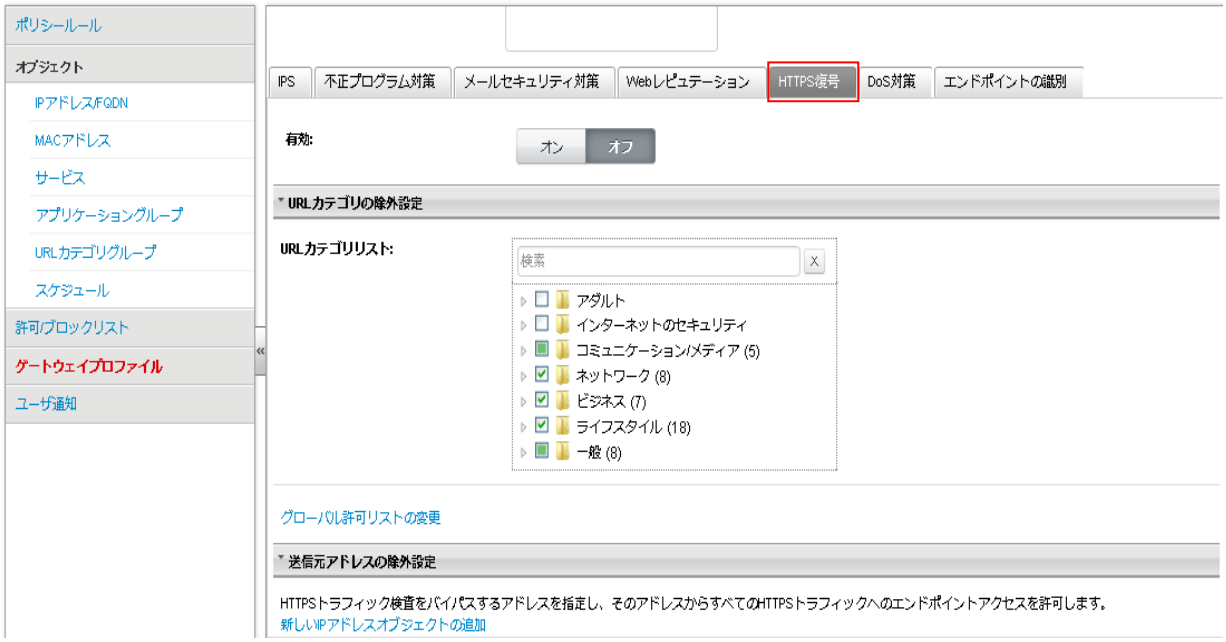
設定変更した場合は保存をしてください。

「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す。

【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。

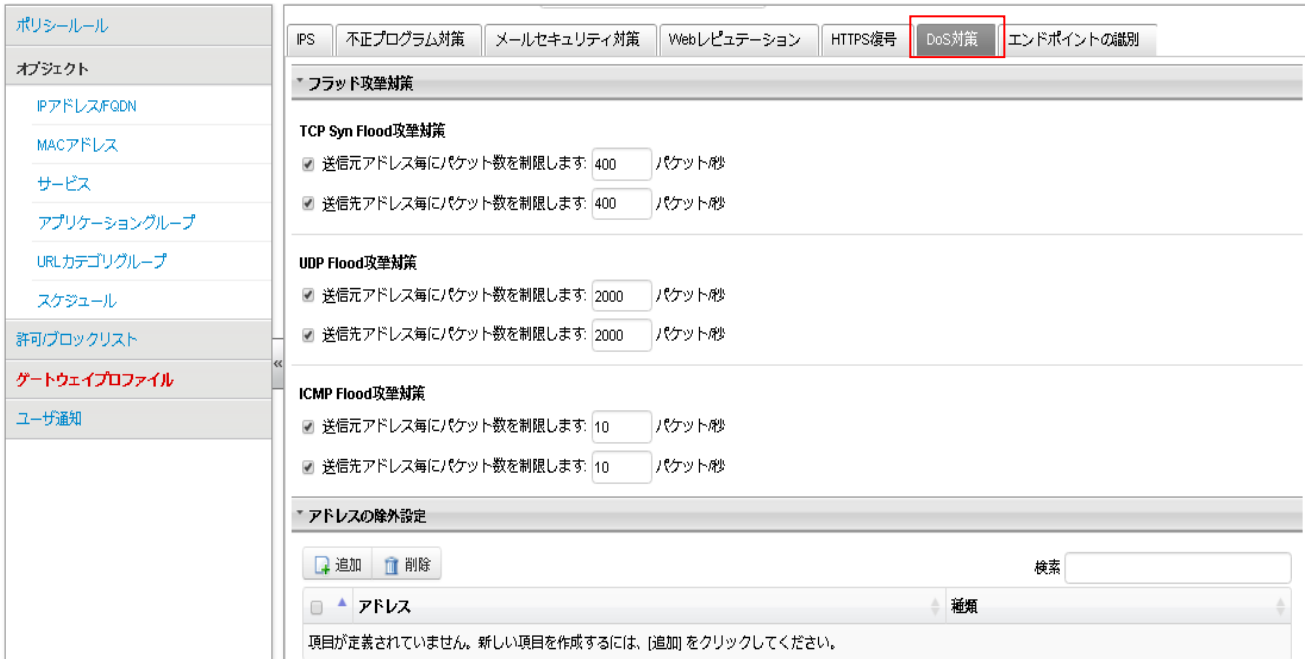
「すべて配信」をクリックして設定を適用します。

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。



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。

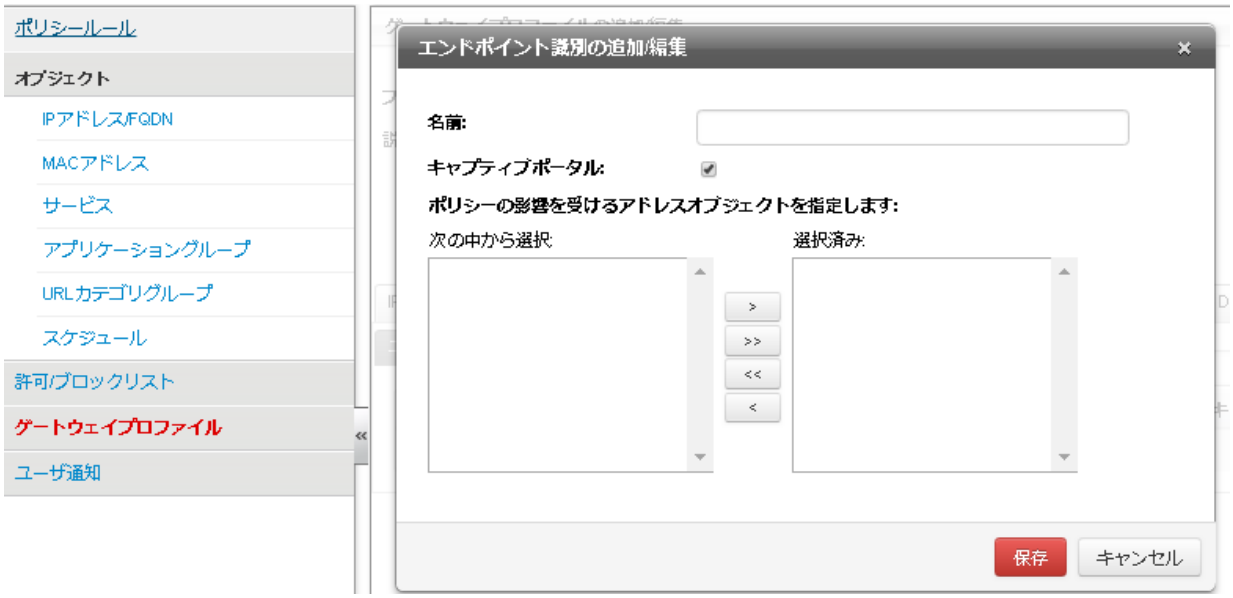
⑦エンドポイント識別

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。



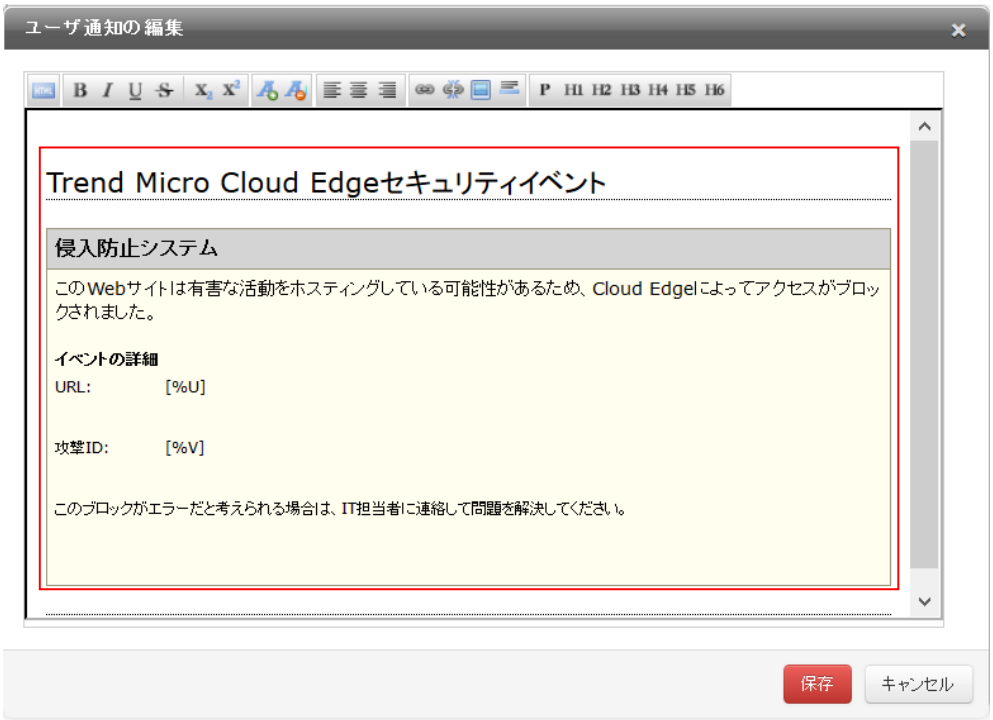
設定変更した場合は保存をしてください。
「すべて配信」をクリックして設定を適用します。

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。

例）IPS 違反

文字やレイアウトを編集できます。



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

①アプリケーション帯域幅

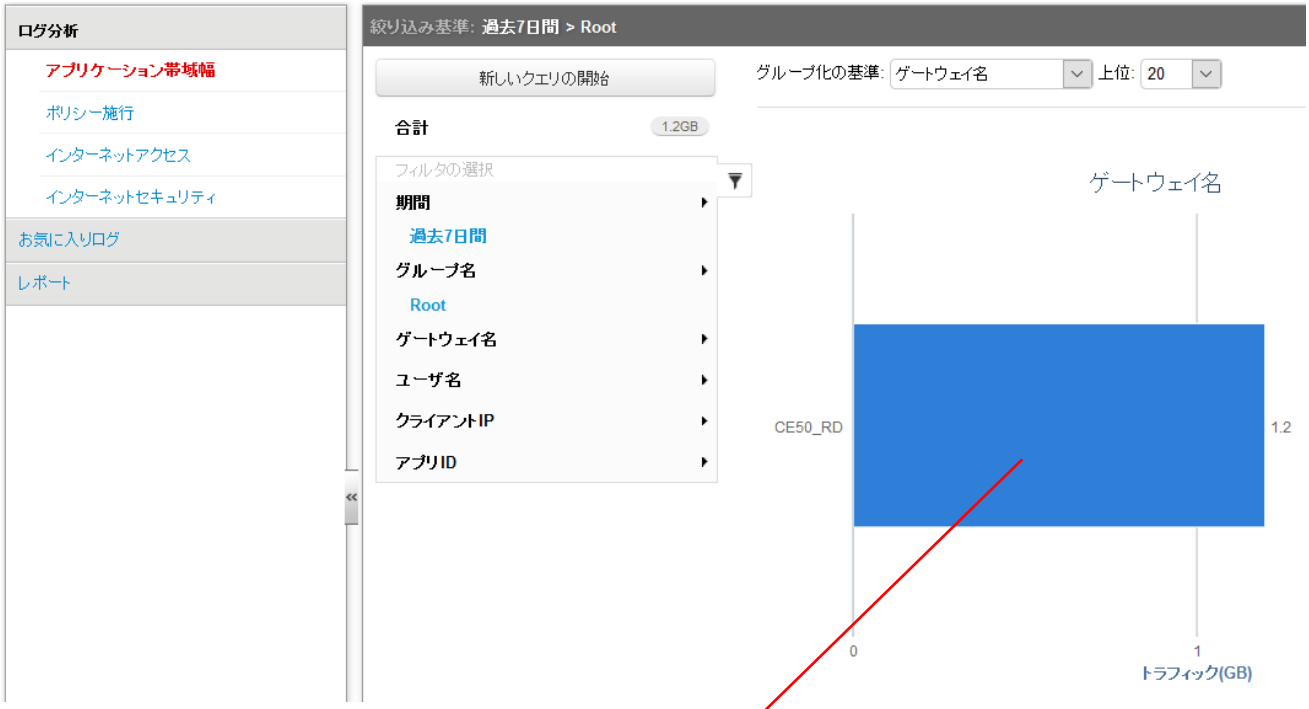
それぞれのログの表示で次のいずれかのフィルタを利用できます。

ゲートウェイ名

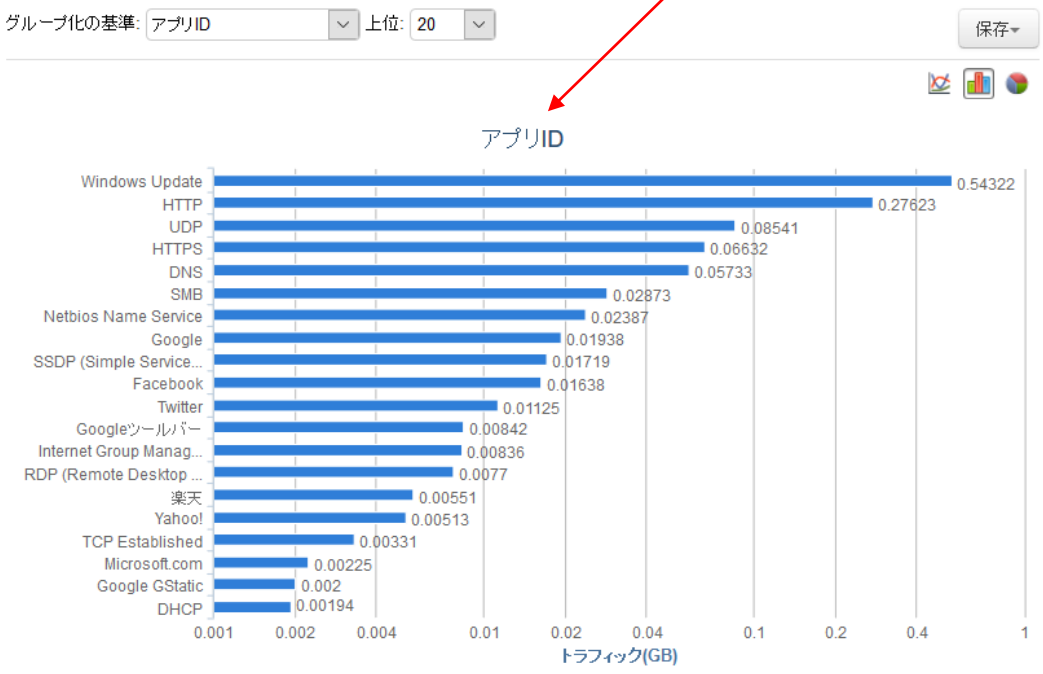
ユーザ名

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

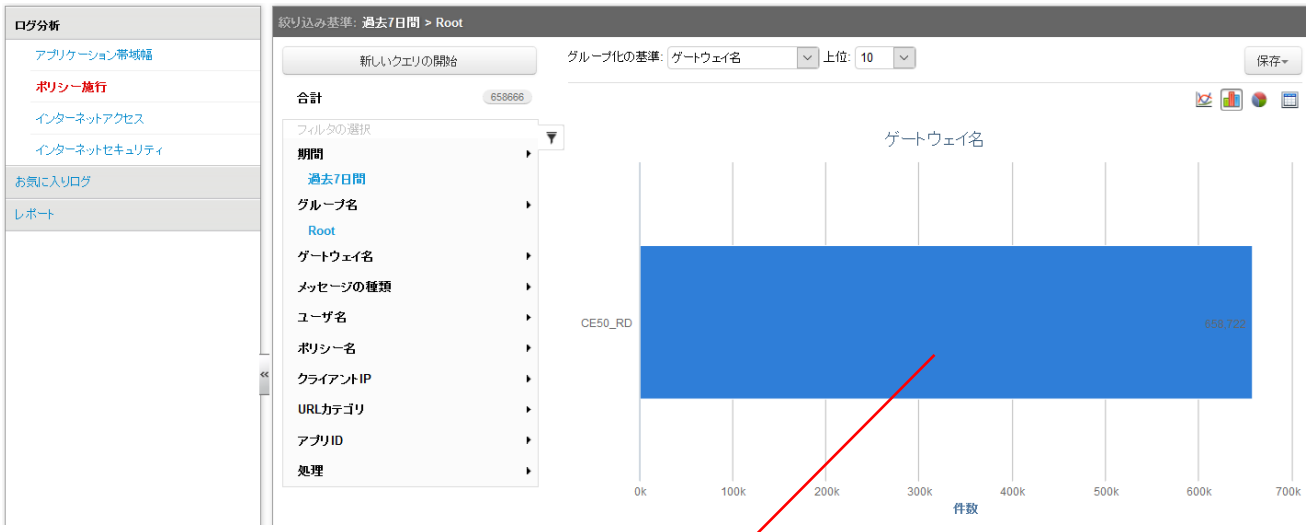
ポリシー名

クライアント IP

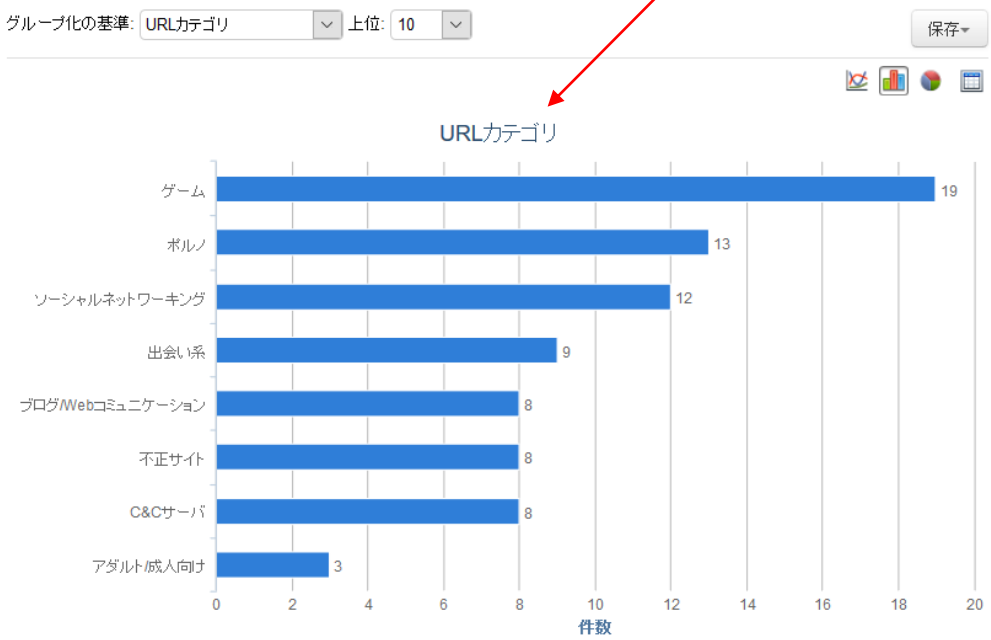
URL カテゴリ

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。

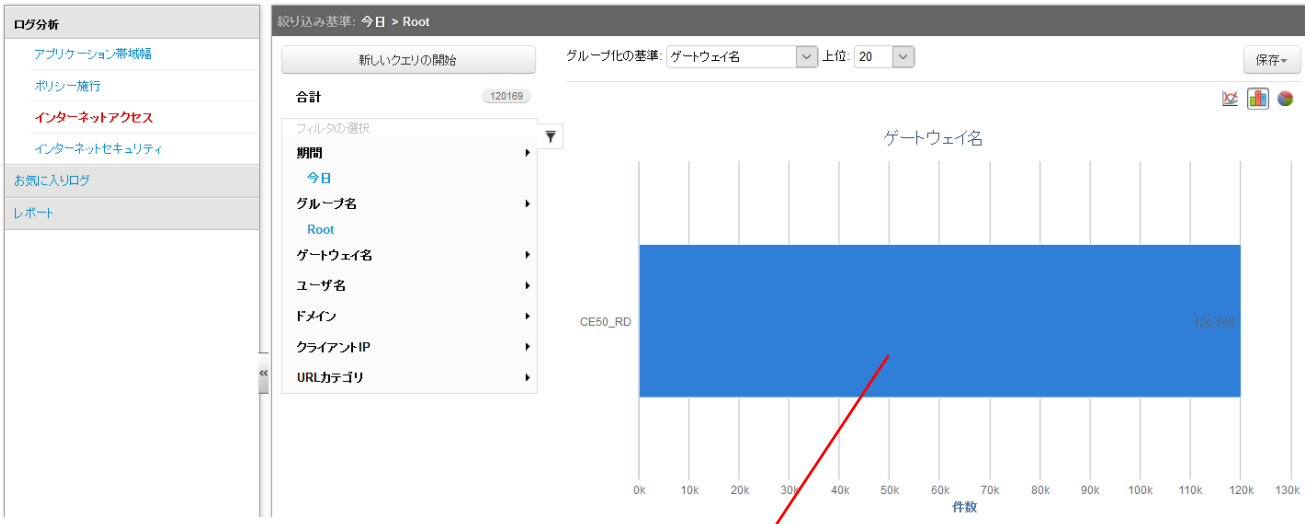
ゲートウェイ名

ユーザ名

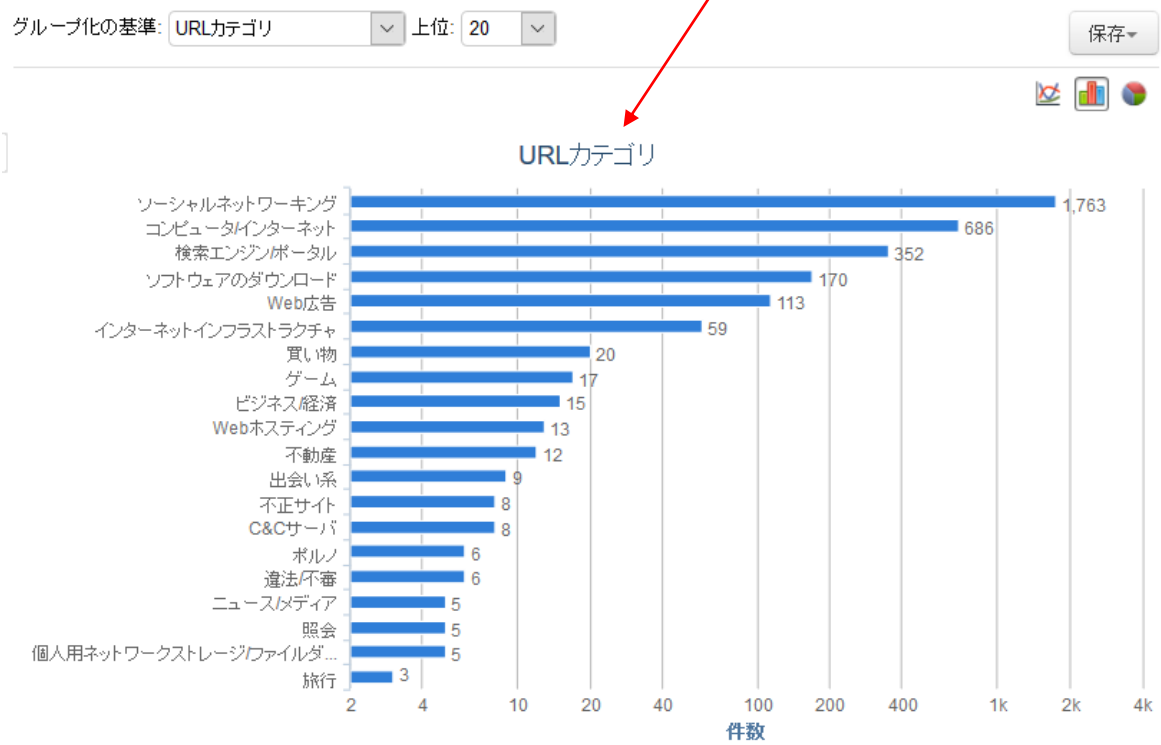
ドメイン

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

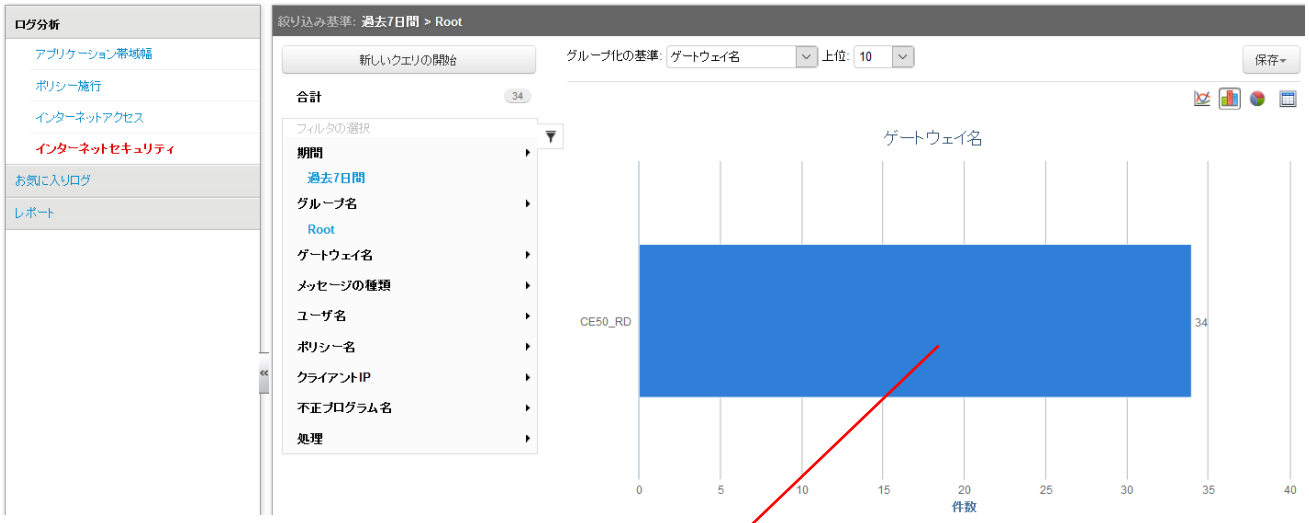
ユーザ名

ポリシー名

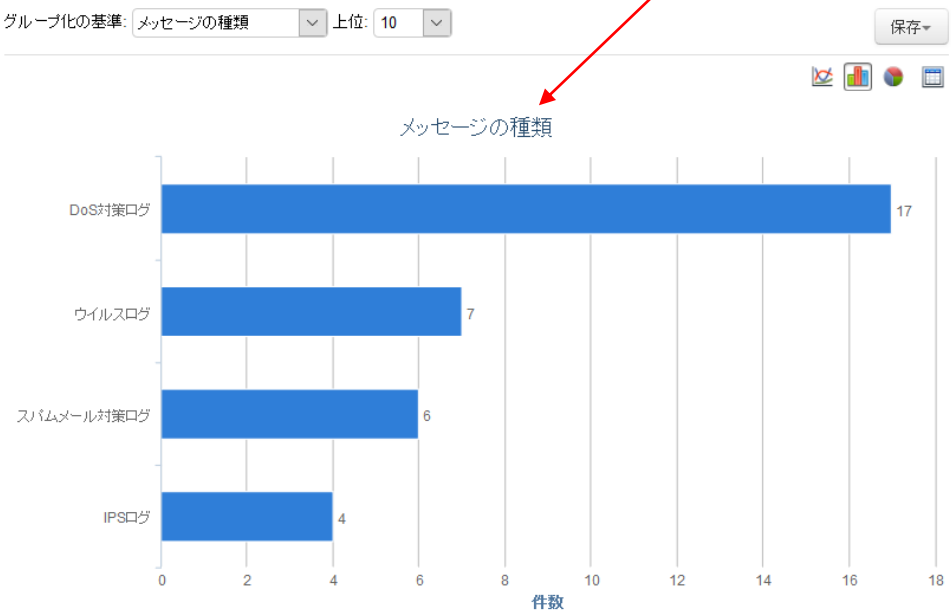
クライアント IP

不正プログラム名

処理

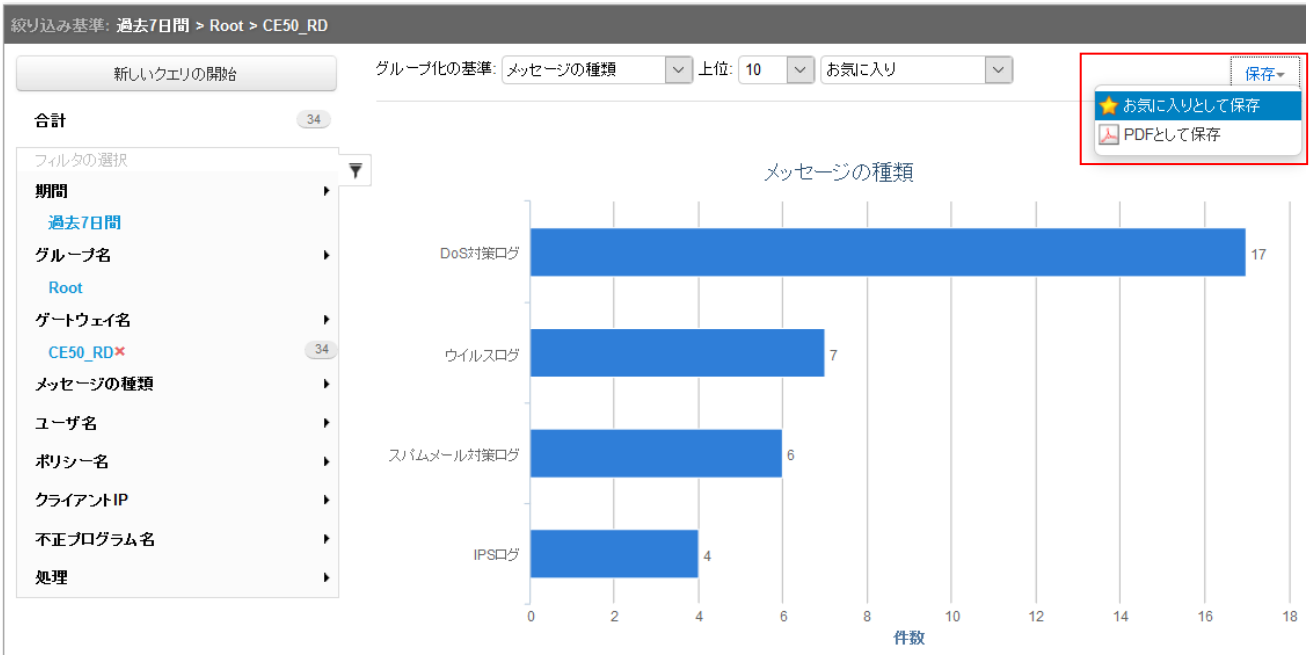


メッセージの種類でフィルタした場合。



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。

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。

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。

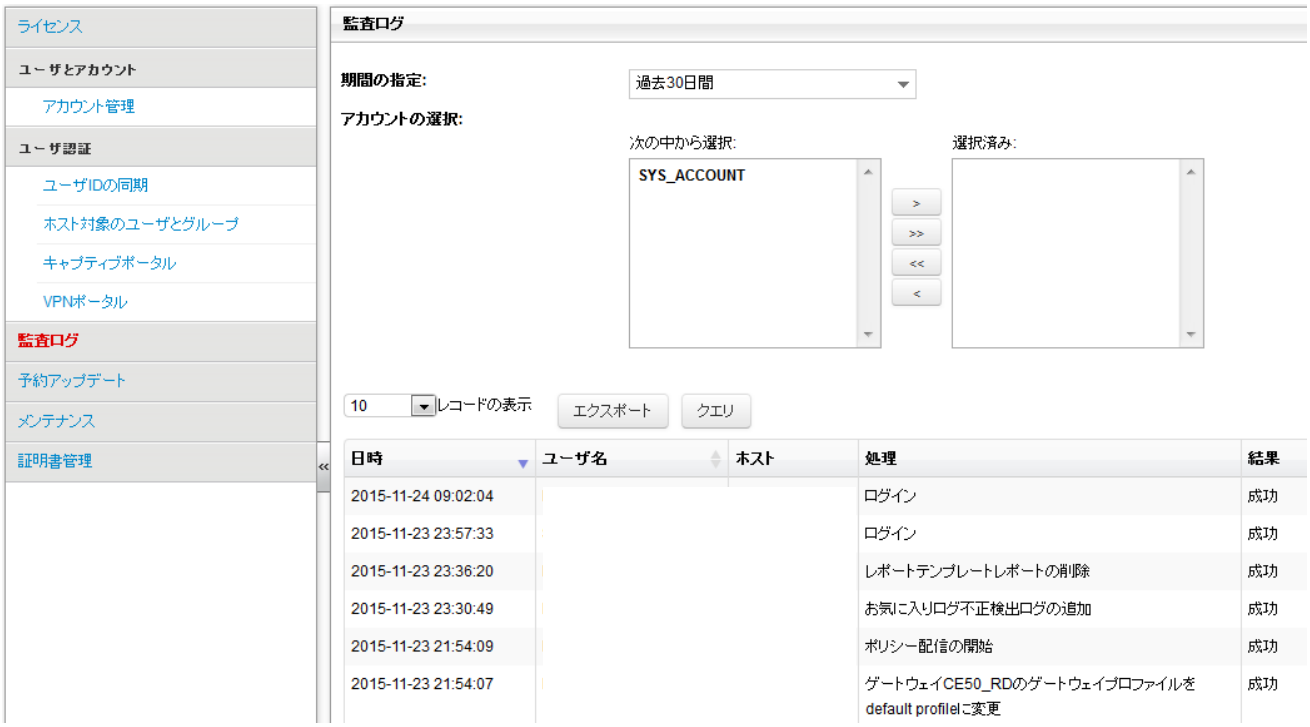
8.1. 管理項目

以下の項目を閲覧、設定可能できます。※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

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。



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。

※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。

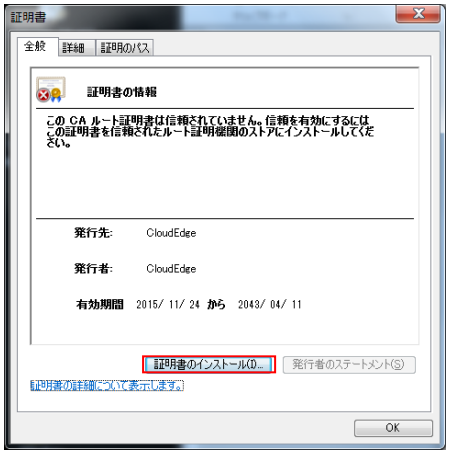
②Cloud Edge 証明書のインストール

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。

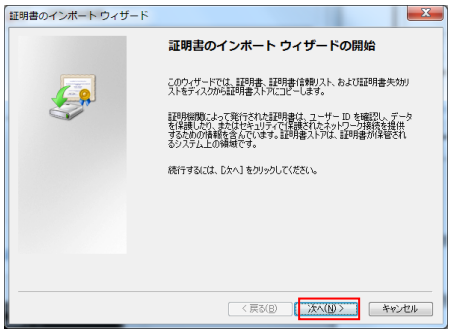
※各ブラウザやメーラーにインストールする必要があります。

Internet Explore の場合

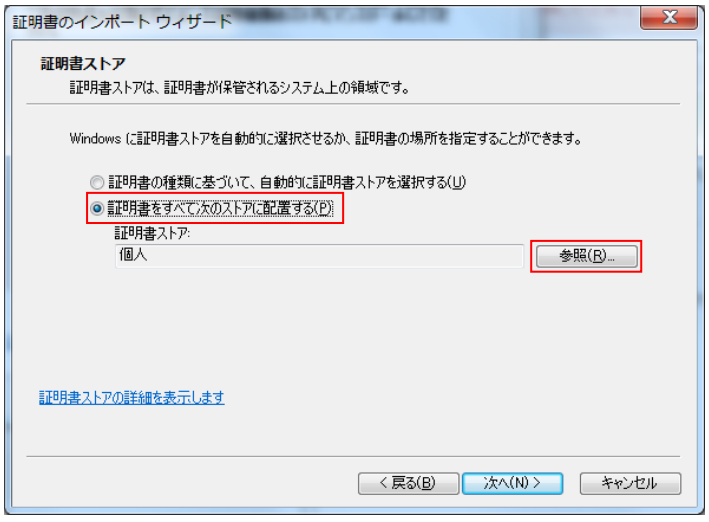
Cloud Edge.crt ファイルをコンピュータで実行し、証明書インストールをクリックします。



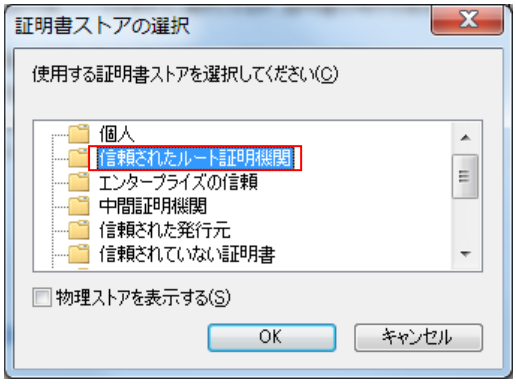
インストールウイザードが開始されますので「次へ」をクリックします。



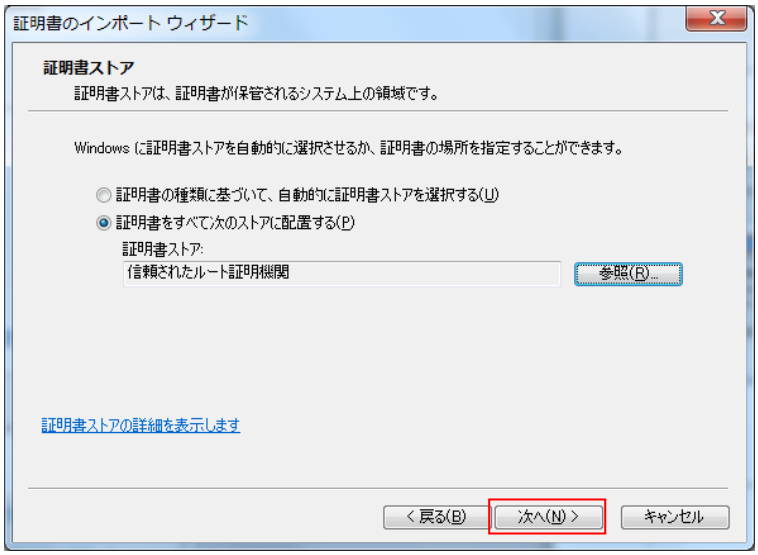
「証明書をすべて次のストアに配置する」を選択し参照をクリックします。



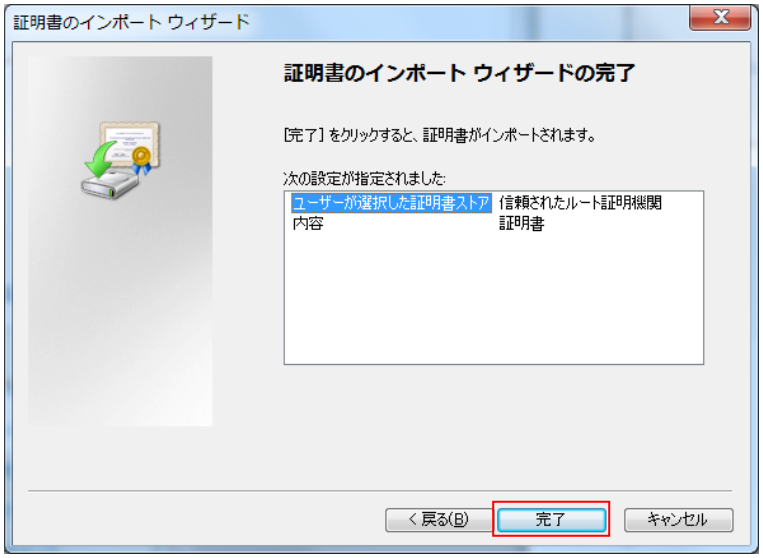
証明書ストアの選択にて「信頼されたルート証明機関」を選択し OK をクリックしてください。



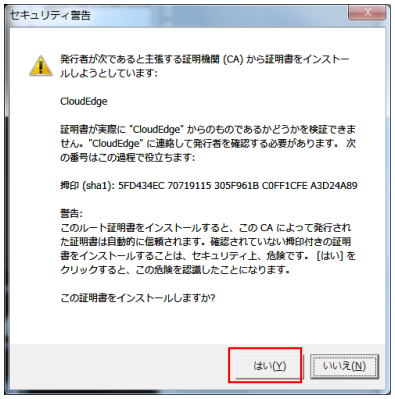
「次へ」をクリックします。



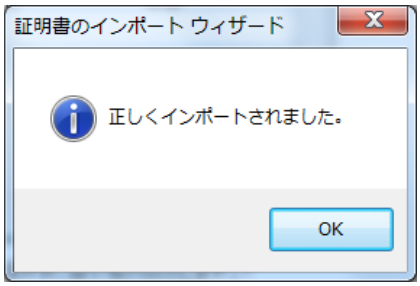
完了をクリックして証明書インポートウィザードを完了します。



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