セキュリティおまかせプラン
ゲートウェイセキュリティご利用マニュアル
（Ver 1.1）

2019年　8月

西日本電信電話株式会社

改定履歴

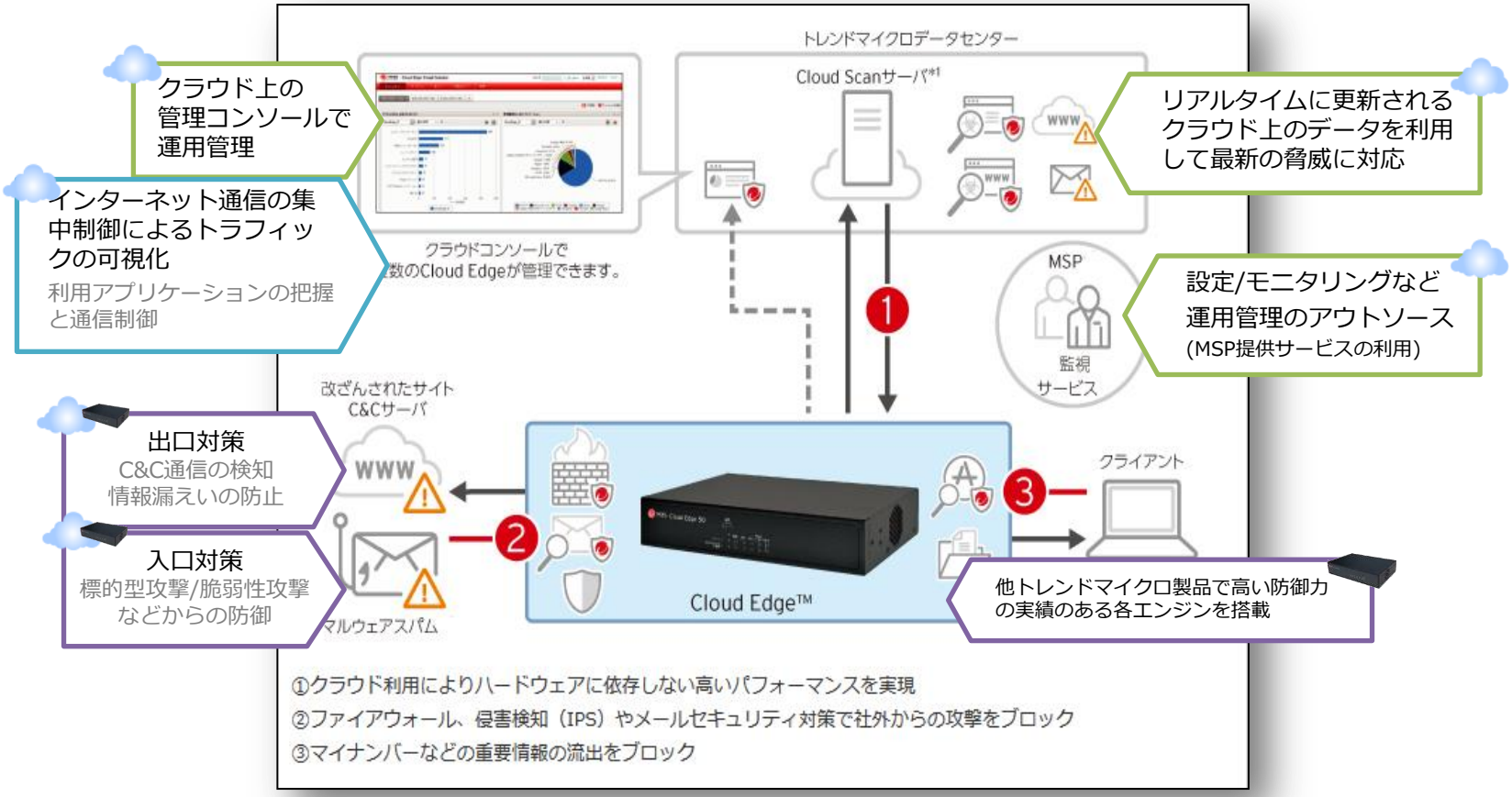
No	Date	主な変更内容	Ver
1	2018/11/15	初版	1.0
2	2019/08/30	メールセキュリティの詳細設定方法（検索対象メールプロトコルの変更）を追加	1.1

目次

1.ゲートウェイセキュリティ概要

ゲートウェイセキュリティ（CloudEdge）は、お客さまのネットワーク境界上に接続するハードウェアと、トレンドマイクロのクラウドサービス上にある「Cloud Scanサーバ」を組み合わせた中小企業向けクラウド型UTMです。
運用管理のための管理コンソールをご利用いただくことで、運用状況の確認や各種設定変更が可能です。

ゲートウェイセキュリティ（CloudEdge）



※1トレンドマイクロが運用管理するWebアクセスセキュリティをクラウド上で提供するクラウド型セキュリティサービス

2.ゲートウェイセキュリティの機能

Cloud Edgeはセキュリティ対策機能の他、運用管理をサポートする機能を多数ご提供いたします。

主なセキュリティ対策機能

機能	説明
アプリケーションコントロール	アプリケーションの利用制限を行う機能。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。
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
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
Webレピュテーション	SPN（16億URL）を利用して接続URLをリアルタイムに評価
不正プログラム対策	アプライアン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
ボット対策	SPNとNCIEエンジン（ネットワーク通信検査エンジン）によるC&C通信防御
URLフィルタリング	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
メールセキュリティ対策	メールレピュテーション(受信メールの送信元IPを検査する機能)とクラウド上のエンジン(ERSとCMSのスキャンサービスを利用)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する。また、コンテンツフィルタリングを利用し、不適切なメールの検知やマイナンバー情報の漏えい対策が可能

運用管理

機能	説明
ポリシー/プロファイル管理	セキュリティ機能をユーザ/アプライアンス単位で設定・管理可能
ダッシュボード	運用に合わせて表示ウィジェットをカスタマイズ可能
ログ分析/レポート	利用頻度の高いログクエリ条件を保存、定期的なレポート出力が可能
管理者アラート	運用状況に関する通知を管理者様メールアドレスに送付

3.管理コンソールへのログイン方法（1/2）

ご登録いただいております「管理者様アドレス」宛に、メールにて、ログインに必要なURL・アカウントID情報をお送りいたします。
まず、パスワード設定用のＵＲＬをクリックいただき、パスワードの設定をお願いいたします。

＜メール例＞

□件名 【セキュリティおまかせプラン】新規アカウント発行のお知らせ
□送信元アドレス no-reply.security-omakase@west.ntt.co.jp
□本文

この度はNTT西日本 セキュリティおまかせプランへのお申込みありがとうございます。

お客様管理ポータルへのログイン用ユーザアカウントを発行致しました。次のURLからログインできます。
https://clp.trendmicro.com/Dashboard?T=fWX6g

アカウントの詳細:
アカウント名: TMF●●●●●●●●●●

ログイン用のパスワードを設定する必要があります。次のURLからパスワードを設定してください。なお、このURLは7日間のみ有効です。
https://●●●●●●●

変更後のパスワードは大切に保管いただきますようお願いします。パスワードを忘れるとお客様管理ポータルにログインできなくなります。

ご不明な点がございましたら、次の連絡先にお問い合わせください。

【本メールに関するお問い合わせ】
セキュリティおまかせプラン開通事務局
TEL：0120-xxx-xxxx（9:00-17:00 平日 ※年末年始を除く）

【サポートに関するお問い合わせ】
セキュリティおまかせサポートセンタ
TEL：0800-xxx-xxxx（9:00-21:00 平日・土日祝 ※年末年始を除く）

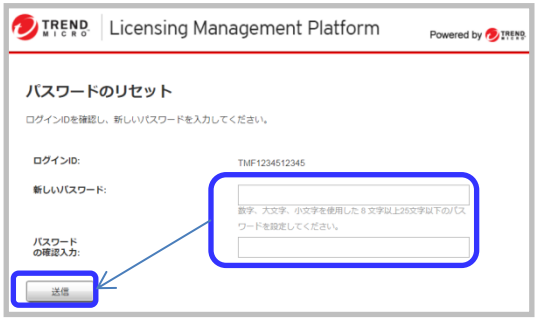
*このメールアドレスは配信専用です。このメッセージに返信しないようお願いいたします。

ログイン用ＵＲＬ

アカウント名

パスワード設定用ＵＲＬ

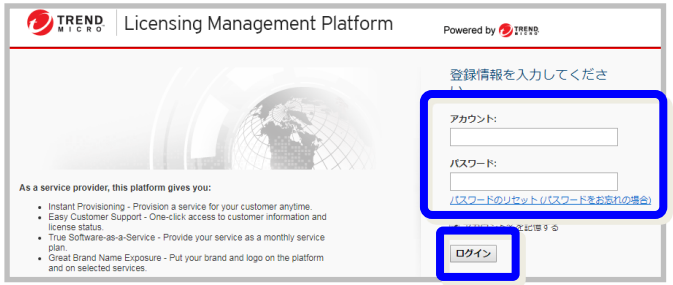
初めにこちらのＵＲＬより、
パスワードの設定をお願いします。



3.管理コンソールへのログイン方法（2/2）

ログインURLをクリックし、アカウント名と設定したパスワードを入力し、ログインボタンを押します。
ログイン頂きますと、「セキュリティおまかせプラン」にてご契約のサービスが表示されますので、CloudEdgeのコンソールを選択し、管理コンソールを立ち上げます。

①ログイン画面へアクセス
https://clp.trendmicro.com/Dashboard?T=fWX6g



②ID/パスワードを入力し、「ログイン」をクリック

③お申込み頂いたサービスが表示されますので、CloudEdge50（または10、100）の「コンソールを開く」をクリックします。

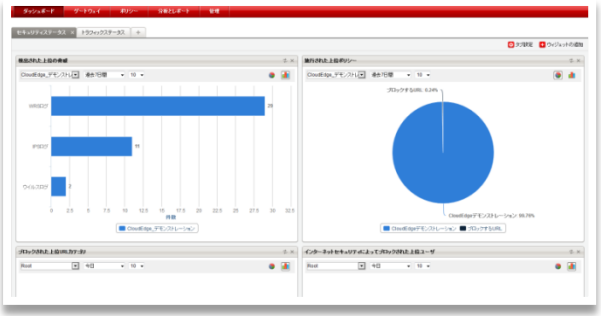
※表記が多少異なる場合がございます。
※初回ログイン時は、トレンドマイクロ株式会社のプライバシーポリシーが表示されますので、ご確認の上、「OK」をクリックいただきますようお願いいたします。

④ゲートウェイ（CloudEdge）の管理コンソールが立ち上がります。ログインは以上で完了です。

4．ダッシュボード画面の見方

Cloud上のWebコンソール（Cloud Console）を利用することで、Cloud Edgeのポリシーの設定や、状況の確認を行うことができます。上部のメインメニューの項目をクリックすることにより、必要な設定箇所に画面を移動することができます。

＜メインメニュー＞



■ダッシュボード

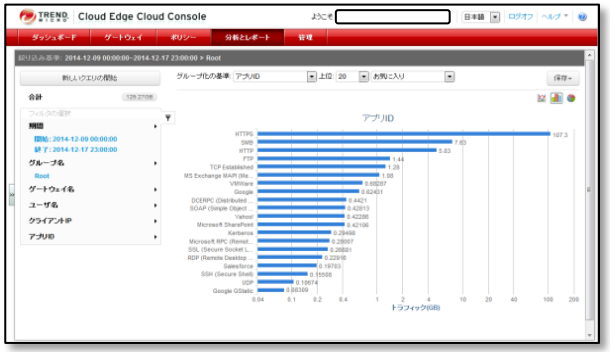
ネットワーク内に設置された1台、または複数のCloud Edgeゲートウェイで発生している活動をウィジェットに表示します。ウィジェットには情報がグラフの形式で視覚的に表示され、脅威の追跡情報を確認したり、蓄積されたログデータと関連付けて確認頂けます。

■ゲートウェイ

現在のステータス、前回のポリシー配信結果や、インタフェースのステータスなどを確認頂けます。

■ポリシー

ゲートウェイ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

高度なログ分析機能とレポート機能が搭載されており、ポリシーの施行状況やインターネットアクセス状況を分析することが可能です。

5－1．設定変更可能な機能一覧

代表的な設定項目の中でご契約者様にて設定変更が可能な項目は以下となります。なお、設定変更を行う際は、事前に次ページの手順でバックアップを取得いただくことをおすすめいたします。また、下記一覧に含まれない設定変更をご希望される場合は、セキュリティおまかせサポートセンタへご連絡頂きますようお願いいたします。

	機能	内容	ご契約者様による設定	ページ番号
①	アプリケーションコントロール	業務上不要なアプリケーション等を指定し、利用を制限します。	○	13p
②	URLフィルタ	業務上不要なURLカテゴリ等を指定し、利用を制限します。	○	14p
③	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ます。	○	15～18p
④	許可・ブロックリスト	個別に許可/ブロックするURLを登録します。	○	19p
⑤	HTTPS復号	HTTPS接続時のスキャンを設定します。有効にする場合、証明書をクライアント端末のブラウザにインストール必要があります。	○	20p
⑥	メールセキュリティ対策			21～24p
	不正プログラム対策	不正プログラムを含むメールを「ブロック」するか「タグ付け」するかを設定します。	○	
	機械学習型検索	高度な分析を使用し、パターンファイルが作られていないような、不正プログラムの亜種の検知を行います。	○	
	スパムメール対策	アンチスパムエンジンによりメールのヘッダ、本文、そのほかの各種情報を判断し、不正なコンテンツでないかをチェックします。	○	
	メールレピュテーション機能	スパムメール対策として使用します。IPアドレスを検証し、スパムおよびフィッシングの送信元を特定し、ブロックします。	○	
	例外リスト	ファイルタイプ、メール送信者などを指定し、メールセキュリティ機能の例外登録を行います。	○	
	詳細設定	検索対象メールプロトコルの変更を行います。	○	
⑦	**管理者アラート**	**ゲートウェイの状態、セキュリティインシデントの状況をサポートセンタで監視するために必要な設定となりますので、ご契約者様による設定変更は不可となっています。※本設定を変更された場合、セキュリティおまかせプランの監視サービスをご利用いただけない場合がございます。**	×	-

5 – 2．バックアップの作成方法

バックアップの実施手順です。
設定変更前にバックアップを作成頂くことで、変更に伴って不具合が発生した場合に、速やかな復旧が可能となります。

①「管理」⇒「メンテナンス」

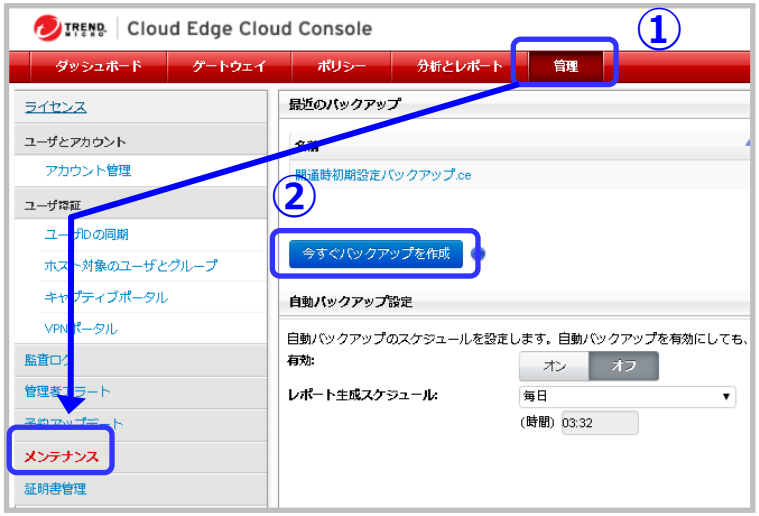
②「今すぐバックアップを作成」をクリック

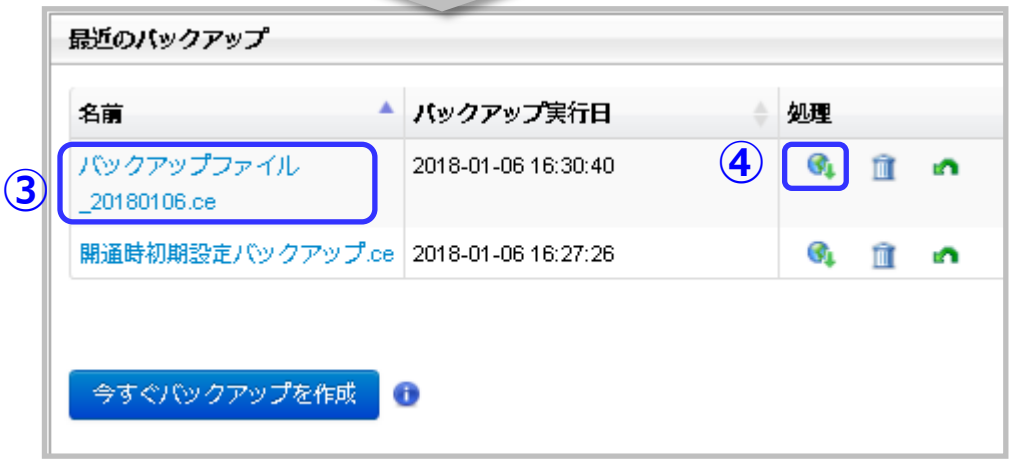
※前回バックアップ時点と差分がない場合は、
バックアップファイルは作成されません。

③バックアップファイルが作成されます。
※最大3世代まで管理コンソール上で保存可能

④ダウンロードする場合は、「処理」のダウンロードボタンを
クリックすると、ceファイルが作成されます。

以上でバックアップは完了です。
次ページにて、復元方法を説明します。

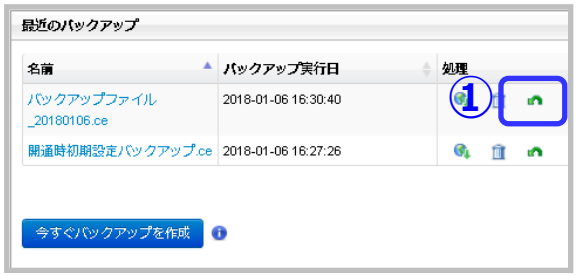




5 – 3．バックアップ復元方法（1/2）

【管理コンソール上のバックアップファイルで復元する場合】

①「管理」⇒「メンテナンス」から
対象のバックアップファイルの「復元」ボタンを
クリックします。



②メッセージが表示されるので、
「OK」をクリックします。

③「正常に復元されました」と表示されることを
確認し、「すべて配信」ボタンをクリックします。

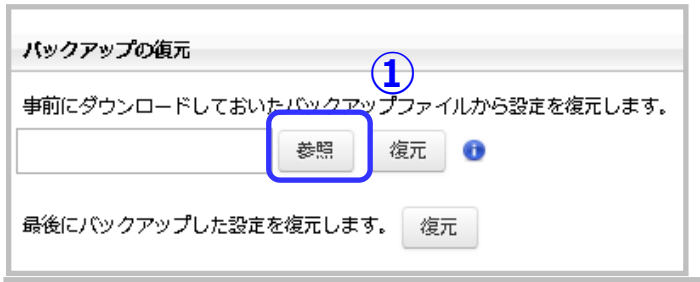
④配信が完了すると、チェックマークが表示されます。

以上で復元は完了です。

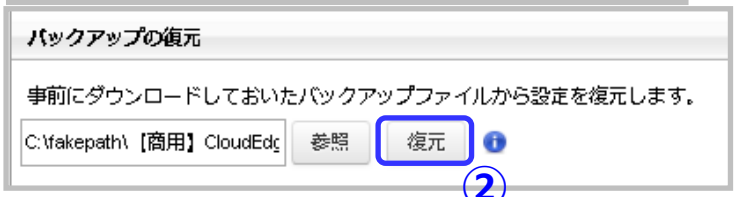
5－3．バックアップ復元方法（2/2）

【ダウンロードしたバックアップファイルで復元する場合】

①「管理」⇒「メンテナンス」から
「バックアップの復元」にて、
「参照」ボタンをクリックします。



②対象のバックアップファイル（ceファイル）を
指定し、「復元」ボタンをクリックします。



③「正常に復元されました」と表示されることを
確認し、「すべて配信」ボタンをクリックします。

④配信が完了すると、チェックマークが表示されます。

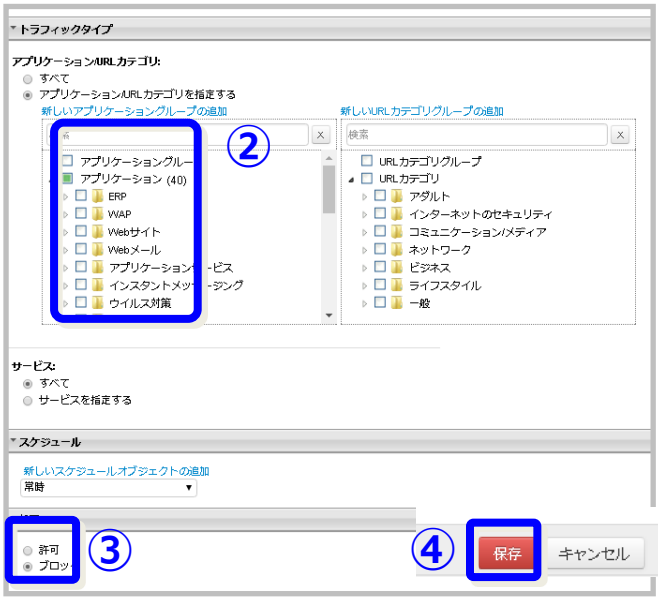
以上で復元は完了です。

6 – 1 .アプリケーションコントロール設定

①「ポリシー」⇒「ポリシールール」にて、
【50-1】アプリケーションコントロールを選択します。
※追加で作成することも可能です。

[参考情報]
・ポリシールールは上から優先的に適用されます。
- 有効になっているポリシー
- 無効になっているポリシー

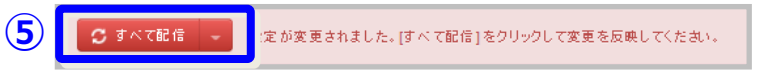
②トラフィックタイプにて、
対象のアプリケーションURLカテゴリを選択します。
※カテゴリをクリックすると、より詳細な項目単位で、
ご指定いただくことが可能です。



③処理にて、「ブロック」または、「許可」を選択します。

④「保存」をクリックします。

⑤「すべて配信」をクリックします。



6 – 2. URLフィルタリング設定

①「ポリシー」⇒「ポリシールール」にて、
【50-1】URLフィルタリングを選択します。
※追加で作成することも可能です。

[参考情報]
・ポリシールールは上から優先的に適用されます。
- 有効になっているポリシー
- 無効になっているポリシー

②トラフィックタイプにて、フィルタリング対象を選択します。
※カテゴリをクリックすると、より詳細な項目単位で、
ご指定いただくことが可能です。

③処理にて、「ブロック」または、「許可」を選択します。

④「保存」をクリックします。

⑤「すべて配信」をクリックします。

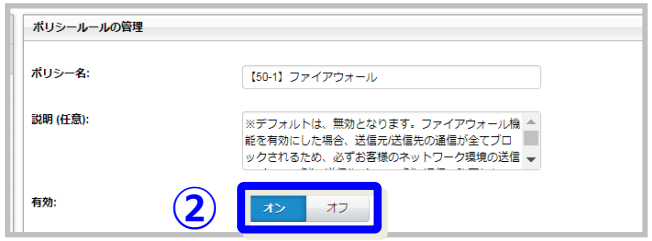
6 – 3.ファイアウォール設定（1/3）

ファイアウォール機能を有効にする場合、送信元/送信先の通信が全てブロックされるため、必ずお客様のネットワーク環境の送信元（ＬＡＮ側）/送信先（ＷＡＮ側）通信で許可したいＩＰアドレス情報を確認した後、個別許可設定を実施ください。

※ここではファイアウォール機能を有効にされる場合を例に手順を記載いたします。

①「ポリシー」⇒「ポリシールール」にて、
【50-1】ファイアウォールを選択します。

②有効にする場合「オン」を選択します。

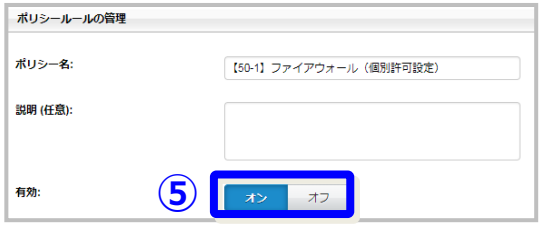


③「保存」します。

6 – 3.ファイアウォール設定（2/3）

④ファイアウォール（個別許可設定）のポリシーを選択します。

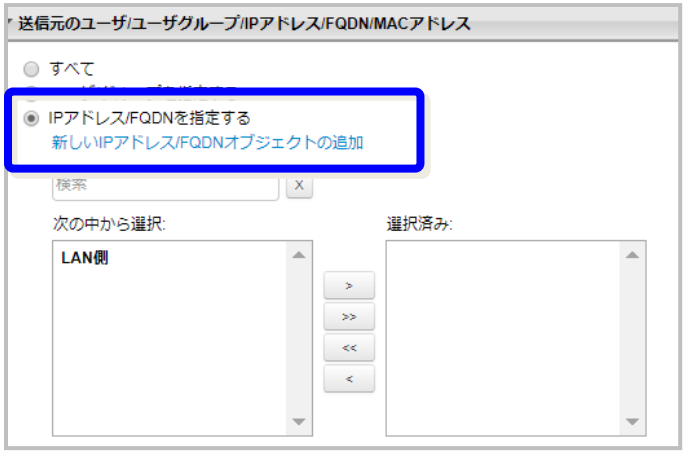
⑤有効を「オン」に切り替えます。



⑥送信元のユーザ/ユーザグループ/IPアドレス/FQDN/MACアドレスの項目内の「IPアドレス/FQDNを指定する」を選択します。

⑦送信元のユーザにて、「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。

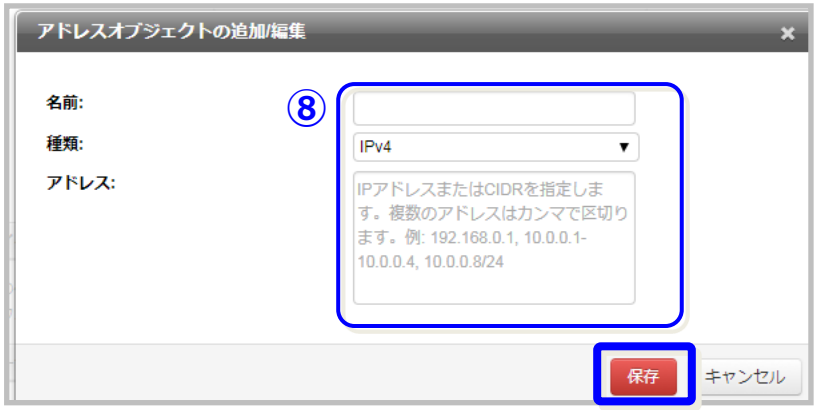
⑥、⑦



6 – 3.ファイアウォール設定（3/3）

⑧名前：任意の名称を指定
　種類：IPv4
　アドレス：対象のアドレスを指定
　　※複数のアドレスはカンマ区切り

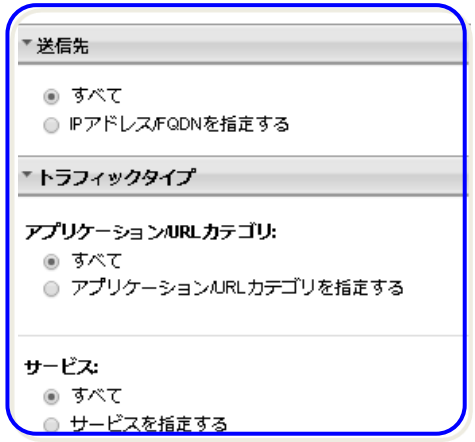
　投入後、「保存」をクリックします。

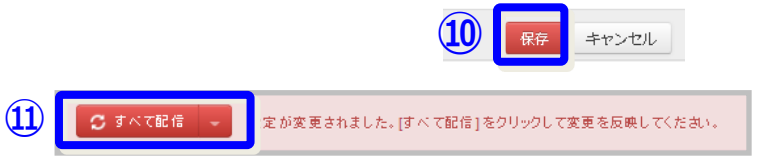


⑨ご利用環境に合わせて、
　送信先アドレス/トラフィックタイプ/サービスを指定します。

⑩「保存」をクリックします。

⑪「すべて配信」をクリックします。





※注意※
ご利用環境がDHCP利用となっている場合、
次ページのDHCP個別許可設定を実施します

＜参考＞ファイアウォール有効時のDHCP許可

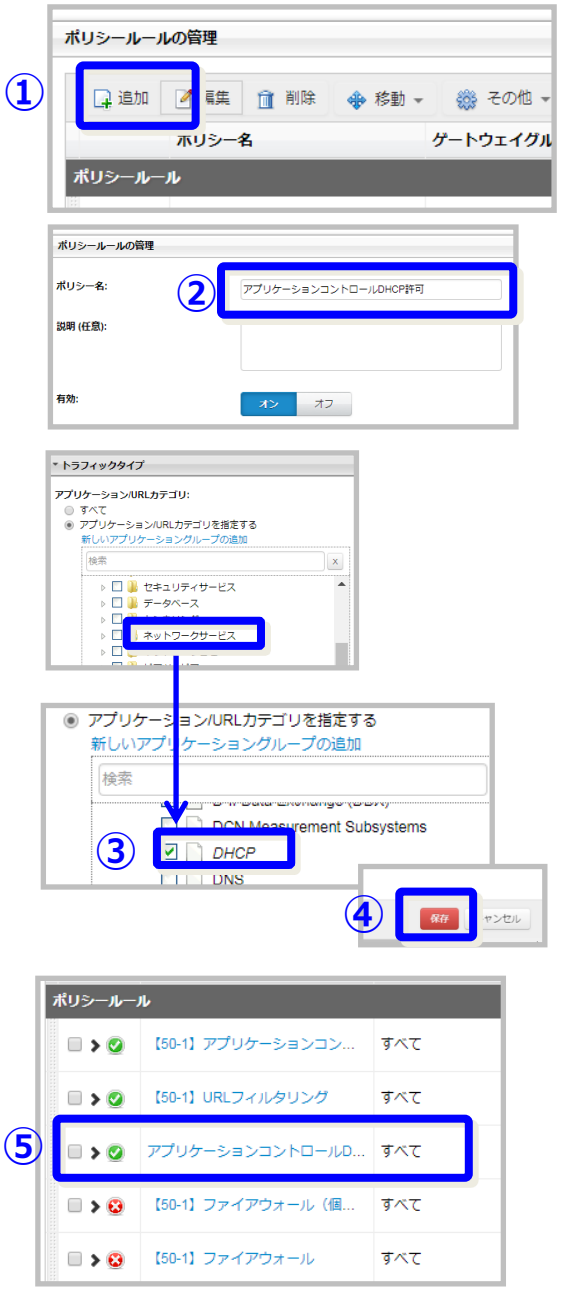
①ポリシールールの管理にて、「追加」をクリックします。

②ポリシー名で「アプリケーションコントロール　DHCP許可」を入力

③トラフィックタイプにて、
「アプリケーション/URLカテゴリを指定する」を選択し、
「ネットワークサービス」内の「DHCP」のみにチェックを入れます。

④保存をクリックします。

⑤ポリシーの適用順位をファイアウォール（個別許可設定）の
上位に配置します。



6 – 4.許可&ブロックリスト設定

①「ポリシー」⇒「許可/ブロックリスト」

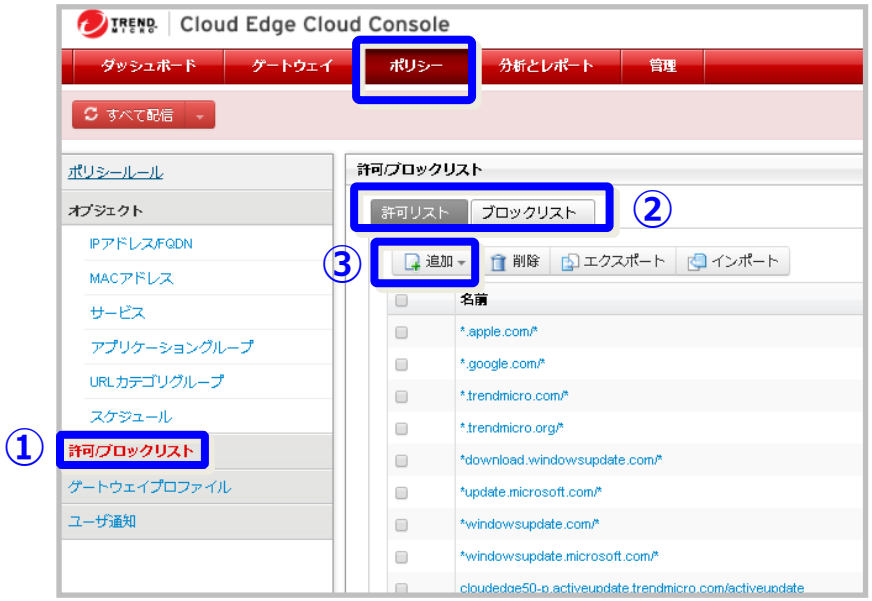
②　「通過」させる場合：許可リスト
「ブロック」させる場合：ブロックリスト　を選択します。

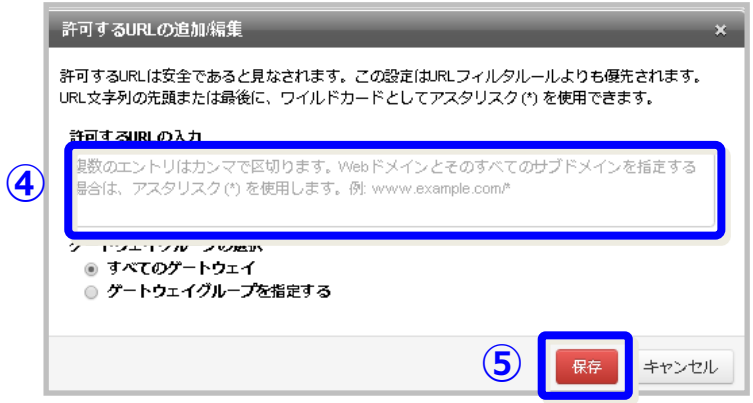
③追加をクリックします。

④ＵＲＬまたはＩＰアドレスを入力します。

⑤「保存」をクリックします。

⑥「すべて配信」をクリックします。





6 – 5 .HTTPS復号設定

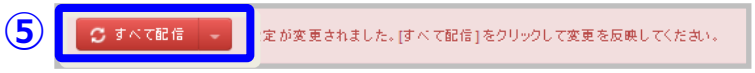
①「ポリシー」⇒「ゲートウェイプロファイル」

②【50-1】初期設定のプロファイルを選択します。

③HTTPS復号を有効にする場合は、
「オン」を選択します。

④「保存」ボタンをクリックします。

⑤「すべて配信」ボタンをクリックします。



管理コンソールにおける設定は以上です。

続いて、クライアント端末へ証明書をインストールします。
25～30pをご確認ください。

6 – 6.メールセキュリティ設定（1/4）

①「ポリシー」⇒「ゲートウェイプロファイル」

②【50-1】初期設定のプロファイルを選択します。

③「メールセキュリティ対策」を選択します。

④不正プログラム対策の有効/無効を選択します。

⑤機械学習型検索の有効/無効を選択します。

6 – 6.メールセキュリティ設定（2/4）

⑥スパムメール対策の有効/無効を選択します。

⑦メールレピュテーションの有効/無効を選択します。

※メールレピュテーションを有効にすると、スパムメールを高い確度で
検知できます。

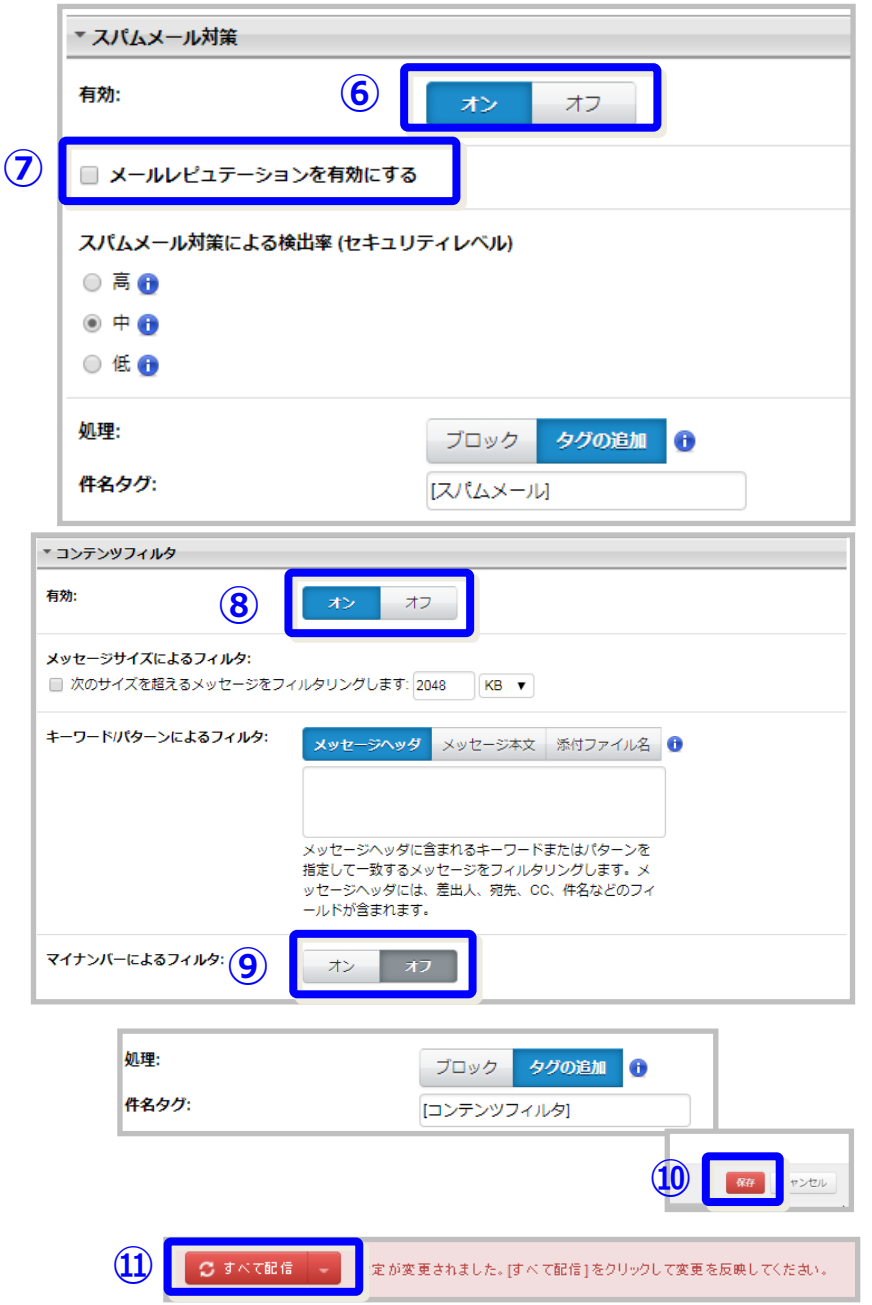
⑧コンテンツフィルタの有効/無効を選択します。

⑨マイナンバーによるフィルタを行う場合、
「オン」を選択します。

※検索対象は本文のみです。（添付ファイルは検索されません）
※処理は初期値「タグの追加」となっております。
送受信をブロックする場合、「ブロックを選択します」

⑩「保存」ボタンをクリックします。

⑪「すべて配信」ボタンをクリックします。



6 – 6.メールセキュリティ設定（3/4）

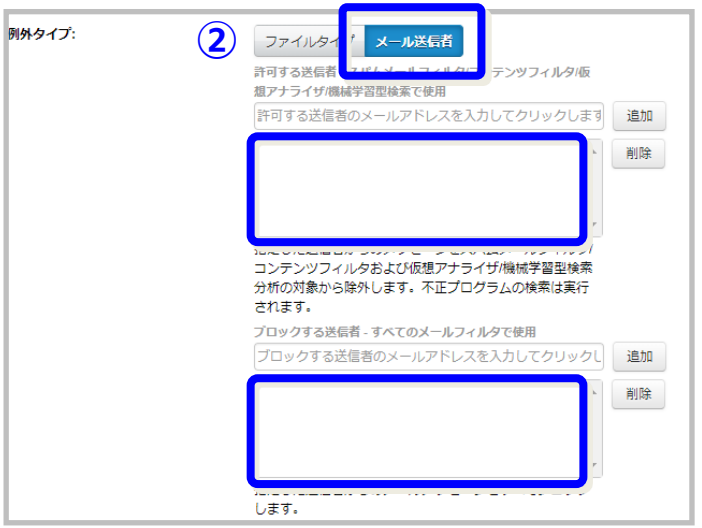
例外登録を行う場合は、下記手順にて実施ください。

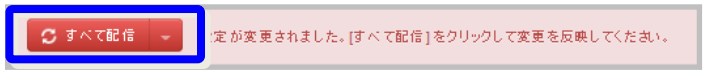
＜ファイルタイプ指定の場合＞
①「ファイルタイプ」を選択し、
　許可するファイルタイプ、ブロックするファイルタイプに
　チェックを入れる。

＜メール送信者を指定する場合＞
②「メール送信者」を選択し、許可する送信者の
　メールアドレスを入力し、「追加」をクリックします。

③「保存」をクリックします。

④「すべて配信」をクリックします。



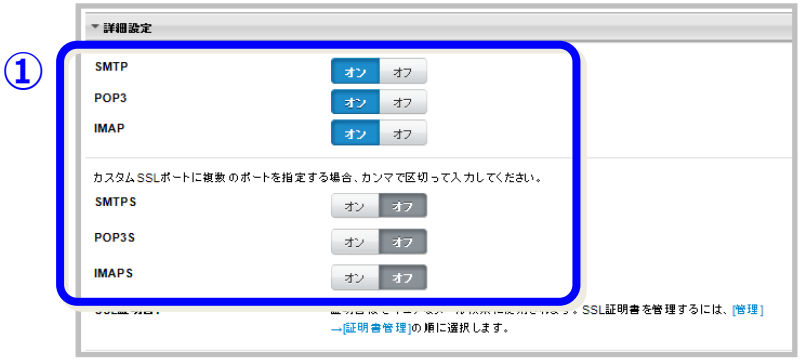


6 – 6 .メールセキュリティ設定（4/4）

メールプロトコルの有効/無効を変更する場合は、下記手順にて実施してください。

※初期値はSMTP,POP3,IMAPが「オン」、SMTPS,POP3S,IMAPSが「オフ」となっております。

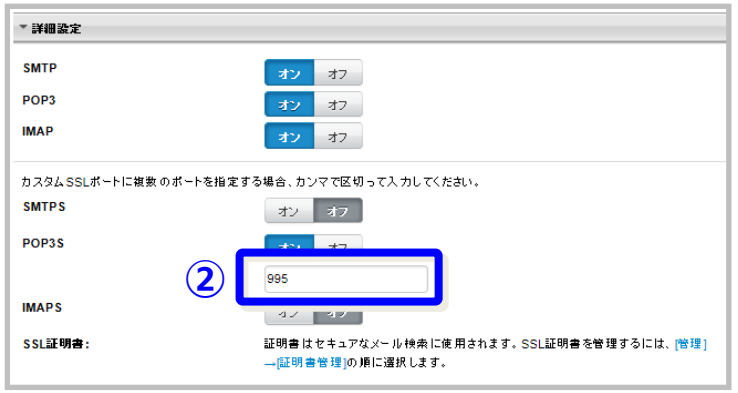
①メールプロトコルで有効にするものを「オン」
　無効にするものを「オフ」に変更します。



②必要に応じて、カスタムSSLポートを指定します。

③「保存」をクリックします。

④「すべて配信」をクリックします。



※SMTPSの復号化によって、外部ネットワークから社内ネットワークのMTAへ
　メールが送信できなくなる場合があります。

続いて、メールソフトへ証明書をインストールします。

6 – 7.証明書ダウンロード

Cloud Edgeでは、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）認証局（CA＝Certification Authority）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、またはSMTPS、POP3S、IMAPSでメールを送受信するたびに、ブラウザまたはメールクライアント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。

①「管理」⇒「証明書管理」をクリックします。

②「エクスポート」をクリックすると、「CloudEdge.crt」というファイルをダウンロードします。
このファイルが証明書です。

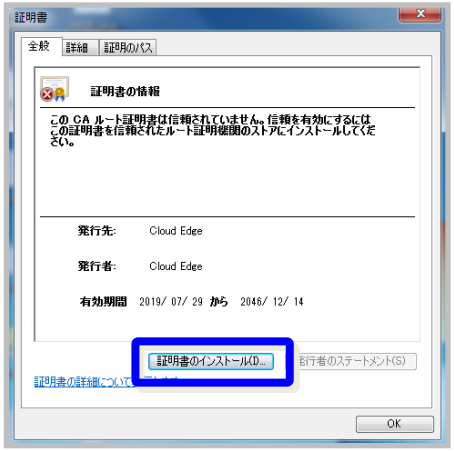
続いて、ダウンロードした証明書をインポートします。

6 – 8.証明書インポート（ 1/5 ）

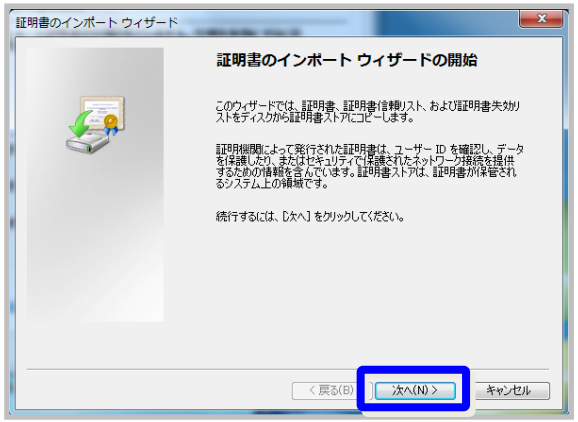
【Windows（Internet Explorer、Outlook、Chromeなど）の場合】

※下記手順はクライアント端末での作業となります。

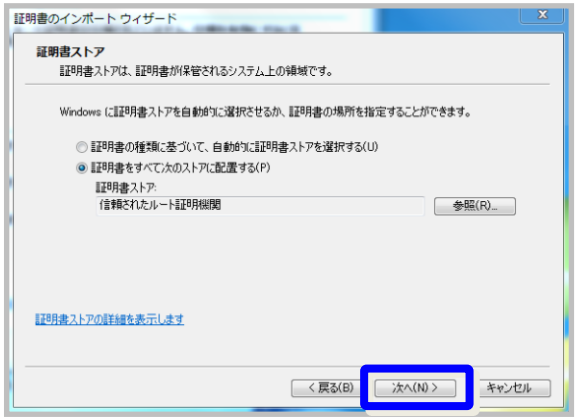
① ダウンロードした「CloudEdge.crt」をダブルクリックします。
「セキュリティの警告」が表示された場合は、「開く」をクリックします。
②「証明書」ダイアログボックスが開くので、「証明書のインストール」をクリックします。



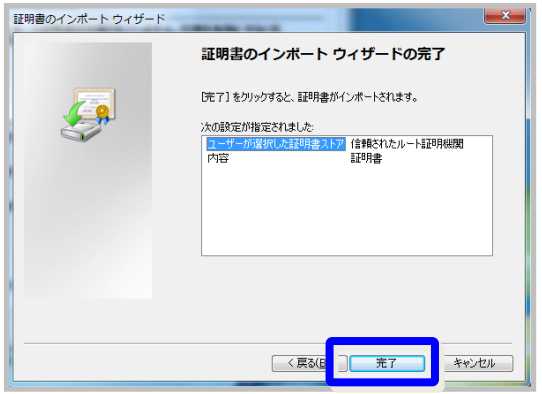
③「証明書のインポートウィザード」が開きます。
「次へ」をクリックします。



④「証明書をすべて次のストアへ配置する」を選び、「参照」をクリックします。「信頼されたルート証明機関」を選択し、「OK」をクリックします。「次へ」をクリックします。



⑤「完了」をクリックして「証明書のインポートウィザード」を閉じます。
「セキュリティの警告」が表示された場合は、「開く」をクリックします。
「正しくインポートされました」と表示されたら、インポートの完了です。

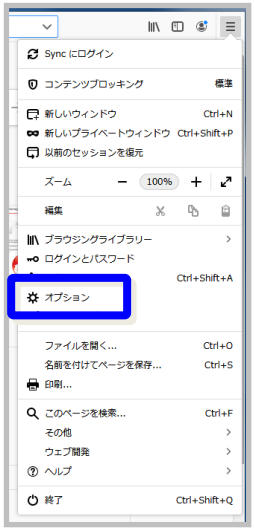


6 – 8.証明書インポート（ 2/5 ）

【Firefoxの場合　1/2】

※下記手順はクライアント端末での作業となります。

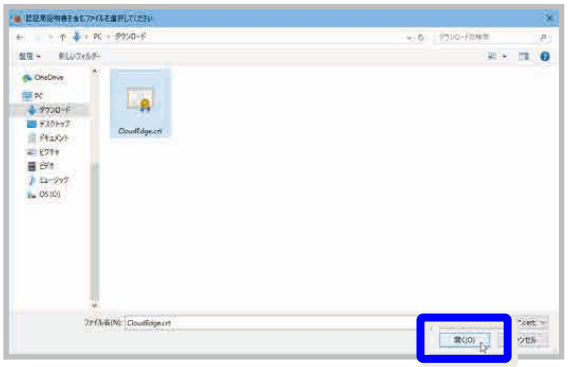
① Firefox を起動し、ツールバーの一番右にあるメニューをクリックして、「オプション」をクリックします。



② 「詳細」→「証明書」の順にクリックし、「証明書を表示」をクリックします。

③ 「認証局証明書」を選択し、「インポート」をクリックします。

④証明書ファイルをクリックして選択し、「開く」をクリックします。

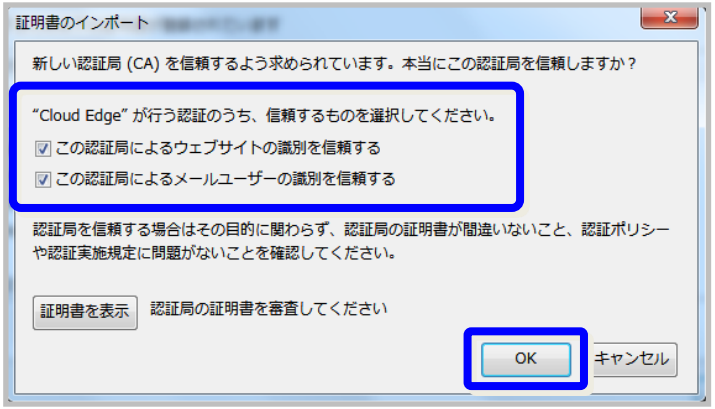


6 – 8.証明書インポート（ 3/5 ）

【Firefoxの場合　2/2】

※下記手順はクライアント端末での作業となります。

⑤「証明書のインポート」ダイアログボックスが開いたら、
チェックボックスすべてにチェックを入れ、「OK」をクリックします。



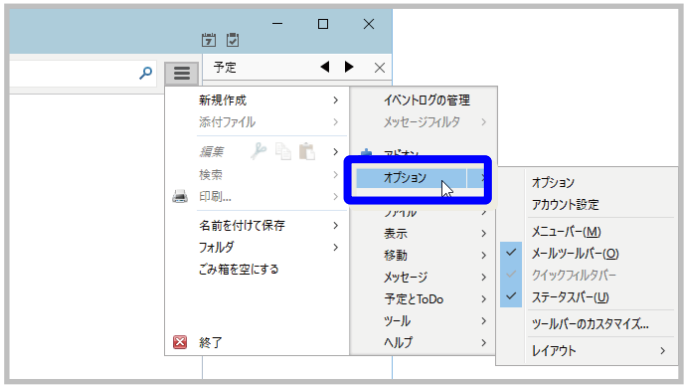
⑥「証明書マネージャー」に戻り、「Trend Micro」の下に
「Cloud Edge｜Software Security Device」という項目が
追加されていれば、インポートの完了です。

6 – 8.証明書インポート（ 4/5 ）

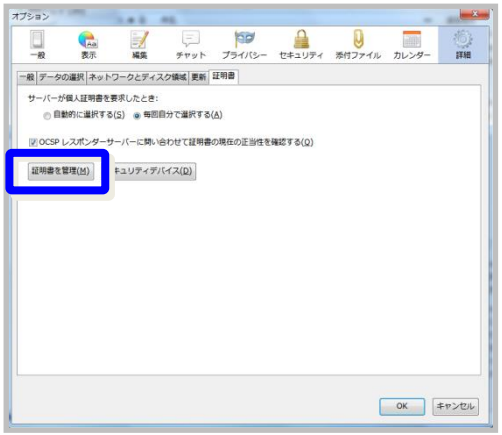
【Thunderbirdの場合　1/2】

※下記手順はクライアント端末での作業となります。

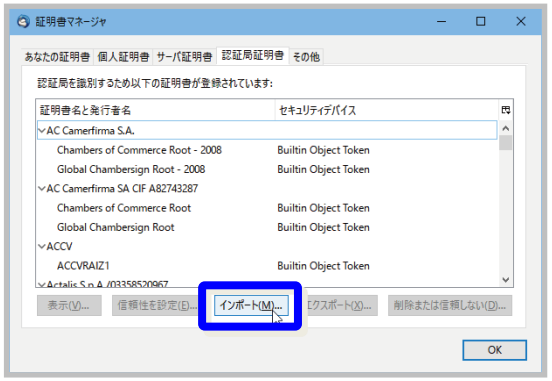
① Thunderbirdを起動し、ツールバーの一番右にあるメニューをクリックして、「オプション」をクリックします。



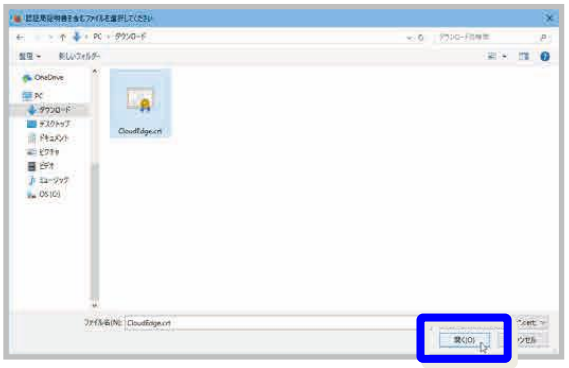
②「詳細」→「証明書」の順にクリックし、「証明書を管理」をクリックします。



③「証明書マネージャ」が開くので、「認証局証明書」が選択されている事を確認し、「 インポート」をクリックします。



④証明書ファイルをクリックして選択し、「開く」をクリックします。

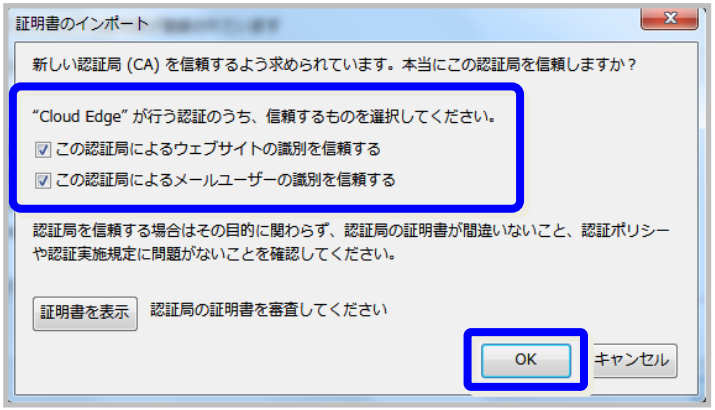


6 – 8.証明書インポート（ 5/5 ）

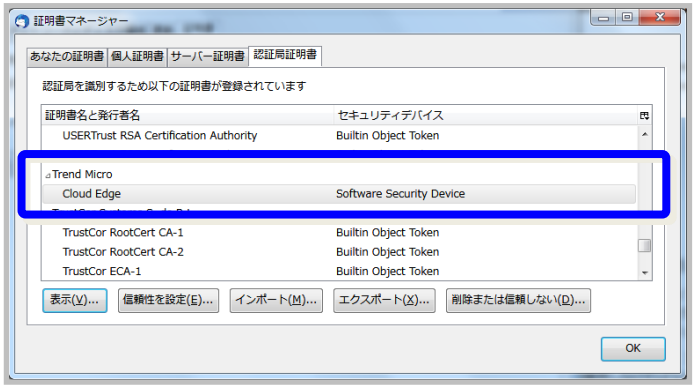
【Thunderbirdの場合　2/2】

※下記手順はクライアント端末での作業となります。

⑤「証明書のインポート」ダイアログボックスが開いたら、
チェックボックスすべてにチェックを入れ、「OK」をクリックします。



⑥「証明書マネージャー」に戻り、「Trend Micro」の下に
「Cloud Edge｜Software Security Device」という項目が
追加されていれば、インポートの完了です。



7.レポート設定（1/2）

Cloud Edge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、アクセスされたURLに関するレポートを生成できます。レポートの情報を活用し、ポリシーの最適化を図ることが可能です。

レポート機能では初期設定として、月次レポートを発行するように登録されております。
ご利用者様の任意の期間でレポートを発行される場合は、以下の手順にて作成可能です。

①「分析とレポート」⇒「レポート」

②「追加」をクリックします。

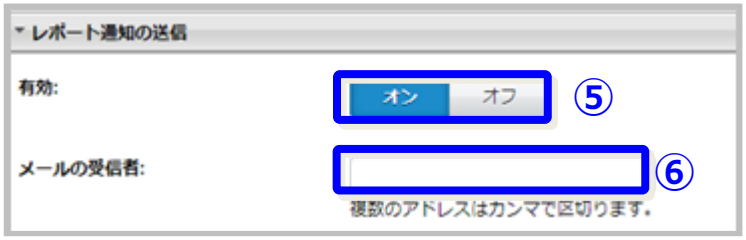
③任意のレポート名を入力します。

④レポート生成スケジュールを設定します。

（例）オンデマンド（非定期）で出力する場合
・生成スケジュール：オンデマンド
・レポート期間　　：任意の時間範囲を指定

7.レポート設定（2/2）

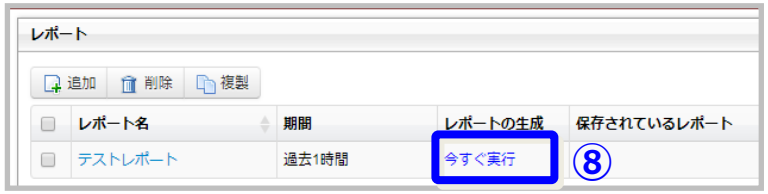
⑤レポートをメール通知する場合は、
有効を「オン」にします。
※直接コンソール上で確認頂くことも可能です。（⑨参照）



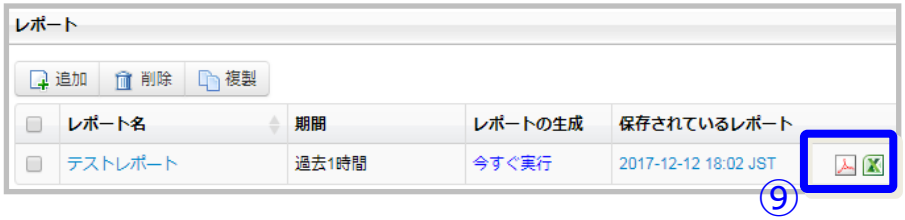
⑥メールの受信者を登録します。

⑦「保存」をクリックします。

⑧レポートの設定完了後、「今すぐ実行」を
クリックします。
※メール通知ONの場合、このタイミングで
メール送信されます。



⑨PDFまたはエクセルのアイコンをクリックすると、
レポートをダウンロード可能です。



8.管理者アラート設定の確認方法

CloudEdgeでは、ゲートウェイステータスが変更された場合や、C & Cコールバック通信を検知した場合、管理者にアラートを通知することが可能です。本機能は、セキュリティサポートセンタにおいて監視を行うために必要な機能となっておりますので、設定変更をご希望される場合は、セキュリティサポートセンタに必ずご連絡をお願いいたします。

【アラート受信者の確認方法】

①「管理」⇒「管理者アラート」をクリックします。

②「アラート受信者」に記載のメールアドレスが、
ご登録されているお客様管理者アドレスになります。

※ご注意ください※

・管理者アラート機能を無効にすると、
セキュリティサポートセンタによる監視が不可となります。
無効にしないようお願いいたします。

・アラート受信者の変更/追加をご希望される場合は、
セキュリティサポートセンタにご連絡いただきますようお願いいたします。

9.ログ分析

「ログ分析」機能では、4つのメニューがあり、各メニューでは、機能毎の検知ログを閲覧およびダウンロードいただくことが可能です。

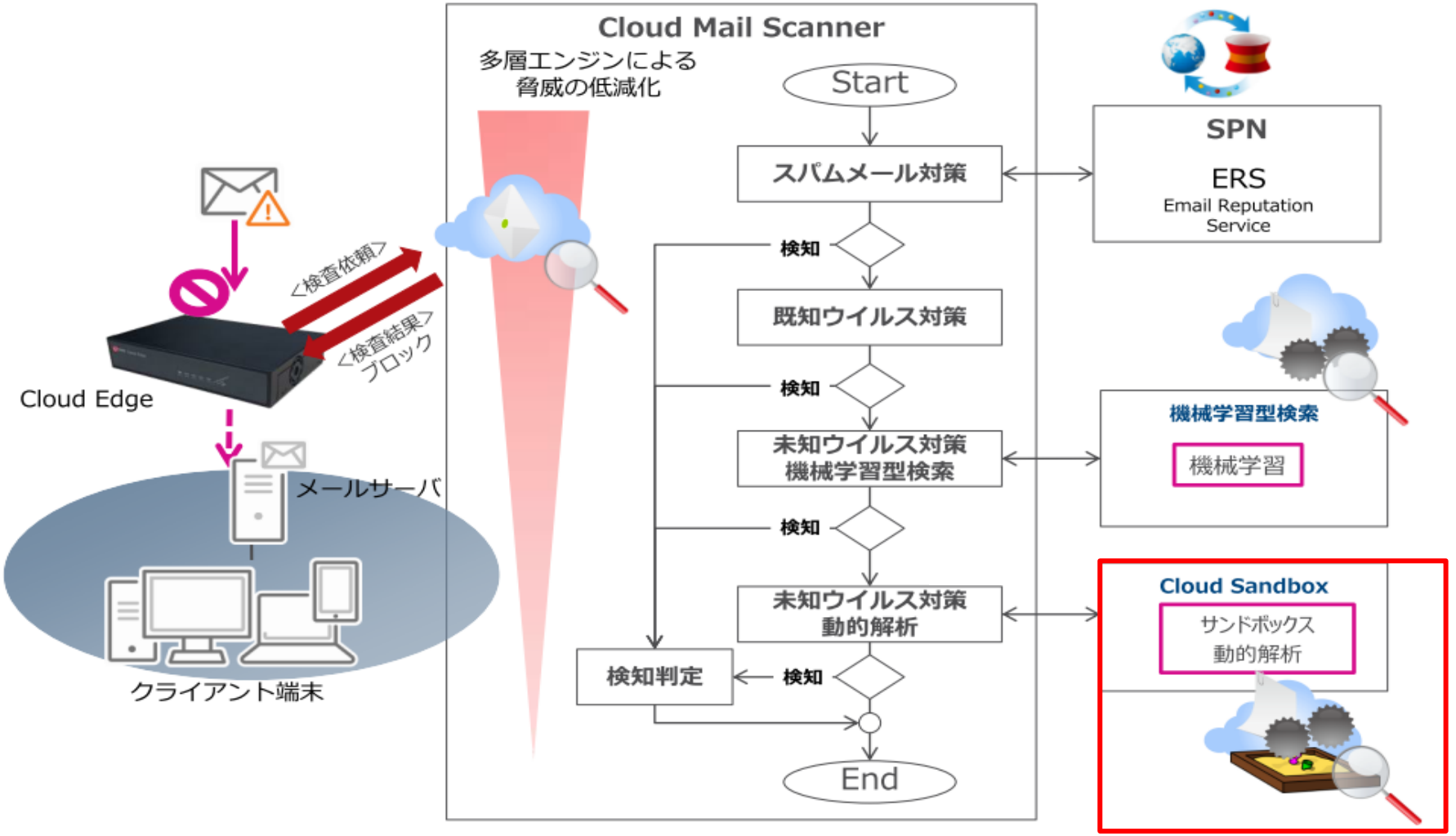
①「分析とレポート」⇒「ログ分析」にて、
確認対象のログを選択します。

ログ種類	内容
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。務上不要なURLカテゴリ等を指定し、利用を制限します。
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。

１０.クラウドサンドボックス機能（1/2）

クラウドサンドボックス機能は、従来のメールセキュリティ検索、機械学習型検索でもメール添付ファイルの不正マルウェアの検知ができなかった場合にクラウド上の仮想アナライザにメールをコピー送付し分析を実施します。

■クラウドサンドボックス機能



１０.クラウドサンドボックス機能（2/2）

各種通知メールは下記のとおりです。

【分析開始時】

差出人：

宛先： XXXXXXXXX@XXXXXX

件名：【不審な添付ファイル】XXXXXXXX

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
Cloud Edgeはこのメールに不審な添付ファイルが含まれている可能性があることを検知しました。
添付ファイルは、詳しい分析のために仮想アナライザに送信されました。
30分以内に不正プログラムが見つかった場合は、メール通知が送信されます。
＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝
ご確認ください。よろしくお願いします。

【分析後】不正を検知しなかった場合

差出人：

宛先： XXXXXXXXX@XXXXXX

件名：【トレンドマイクロ仮想アナライザフィードバック】XXXXXXXX

最近受信したメールメッセージに不審な添付ファイルが含まれていたため、分析のために仮想アナライザに転送されました。
仮想アナライザによる分析の結果、このメールは安全であることが確認されました。

メールメッセージの詳細：

件名： XXXXXXXXXX
送信元： XXXXXXX@XXXXXXXX
宛先： XXXXXXX@XXXXXXXX
添付ファイル： XXXXXXXXX

【分析後】不正を検知した場合

差出人：

宛先： XXXXXXXXX@XXXXXX

件名：【トレンドマイクロ仮想アナライザフィードバック】XXXXXXXX

最近受信したメールメッセージに不審な添付ファイルが含まれていたため、分析のために仮想アナライザに転送されました。
仮想アナライザによる分析の結果、このメールに不正プログラムが含まれていることが確認されました。

メールメッセージの詳細：

件名： XXXXXXXXXX
送信元： XXXXXXX@XXXXXXXX
宛先： XXXXXXX@XXXXXXXX
添付ファイル： XXXXXXXXX

【分析後】分析が完了しなかった場合

差出人：

宛先： XXXXXXXXX@XXXXXX

件名：【トレンドマイクロ仮想アナライザフィードバック】XXXXXXXX

最近受信したメールメッセージに不審な添付ファイルが含まれていたため、分析のために仮想アナライザに転送されました。
仮想アナライザによる分析は保留中であるか、まだ完了していません。

メールメッセージの詳細：

件名： XXXXXXXXXX
送信元： XXXXXXX@XXXXXXXX
宛先： XXXXXXX@XXXXXXXX
添付ファイル： XXXXXXXXX