

**セキュリティおまかせプラン
EMOTET対策推奨設定
Cloud Edge編
(Ver 1.0)**

2022年 3月
西日本電信電話株式会社

1.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情報をお送りしております。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。

<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=xxxxxx>

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いたします。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。

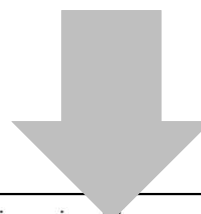
【本メールに関するお問い合わせ】
セキュリティおまかせプラン開通事務局
TEL：0120-xxx-xxxx（9:00-17:00 平日 ※年末年始を除く）

【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



1.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。ログインできると、「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、Cloud Edgeの「コンソールを開く」を選択します。

登録済みの製品/サービス ヘルプ

製品/サービス

+キーの入力

| サービスプラン名 | 製品/サービス | シート/ユニット | ライセンス種別 | 開始日 | 有効期限 | アクション |
|--------------------|-------------------------|----------|---------|------------|------|----------|
| 【NFR】CloudEdge 50 | Cloud Edge 50 | 10 シート | 製品版 | 2021/10/28 | 自動更新 | コンソールを開く |
| 【NFR】エンドポイントセキュリティ | ウイルスバスター ビジネスセキュリティサービス | 10 シート | 製品版 | 2020/12/03 | 自動更新 | コンソールを開く |

①「コンソールを開く」を選択します。

有効期限内 間もなく期限切れ 有効期限切れ

②ダッシュボードが表示されます。ログインは以上で完了です。

Cloud Edge Cloud Console

ダッシュボード ゲートウェイ ポリシー 更新とレポート 管理

セキュリティステータス トラフィックステータス デバイスマップとセキュリティ +

実行された上位ポリシー

Root 過去7日間 20

160-11 URLフィルタリング 39

ポリシー実行イベント

ブロックされた上位URLカテゴリ

Root 過去7日間 10

Web広告

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

Root 過去1時間 10

APT (総的サイバー攻撃) イベント

Root 過去7日間

2.「不正プログラム対策」内の「スマートスキャン」「機械学習型検索」の有効手順（1/2）

不正プログラム対策の機械学習型検索の有効する手順を記載します。
「ポリシー > セキュリティプロファイル > 【50-1】初期設定のプロファイル > 不正プログラム対策」の順に移動します。

①「ポリシー」を選択します。

②「セキュリティプロファイル」を選択します。

③「【50-1】初期設定のプロファイル」を選択します。

④「不正プログラム対策」を選択します。

The screenshot shows the TREND Cloud Edge Cloud Console interface. The navigation menu at the top includes 'ダッシュボード', 'ゲートウェイ', 'ポリシー', '分析とレポート', and '管理'. The 'ポリシー' menu is selected. The main content area shows a list of security profiles under 'セキュリティプロファイル'. The profile '[50-1] 初期設定のプロファイル' is selected. The configuration page for this profile is shown, with the '不正プログラム対策' option selected under the 'IPS' section. The '有効にする' (Enable) section has the 'オン' (On) radio button selected. The 'ファイル拡張子' (File Extensions) section shows a list of allowed file extensions: png, gif, jpg, mp3, mp4, avi, mov, wmv.

2.「不正プログラム対策」内の「スマートスキャン」「機械学習型検索」の有効手順（2/2）

「スマートスキャンを有効にする」にチェックを入れます。
「機械学習型検索を有効にする」にチェックを入れます。

The screenshot shows the Trend Micro Cloud Edge Cloud Console interface. The main navigation bar includes 'ダッシュボード', 'ゲートウェイ', 'ポリシー', '分析とレポート', and '管理'. The left sidebar lists various policy objects, with 'セキュリティプロファイル' (Security Profiles) selected. The main content area is titled 'セキュリティプロファイルの追加/編集' (Add/Edit Security Profile) and shows the configuration for a profile named '【50-1】初期設定のプロファイル'. The '不正プログラム対策' (Malware Protection) tab is active, and the 'オン' (On) toggle is selected. Two checkboxes are checked and highlighted with a blue callout box: 'スマートスキャンを有効にする' (Enable Smart Scan) and '機械学習型検索を有効にする' (Enable Machine Learning Search). Below this, the 'ファイル拡張子' (File Extensions) section is visible, with a text input field containing 'png,gif,jpg,mp3,mp4,avi,mov,wmv'. A note at the bottom states: '指定した拡張子のファイルがHTTPでダウンロードされた場合、不正プログラム対策での検索が除外されます。' (When files with the specified extension are downloaded via HTTP, they are excluded from malware protection search.)

3.「メールセキュリティ対策」「不正プログラム対策」内の「機械学習型検索」の有効手順（1/2）

メールセキュリティ対策の機械学習型検索を有効化する手順を記載します。

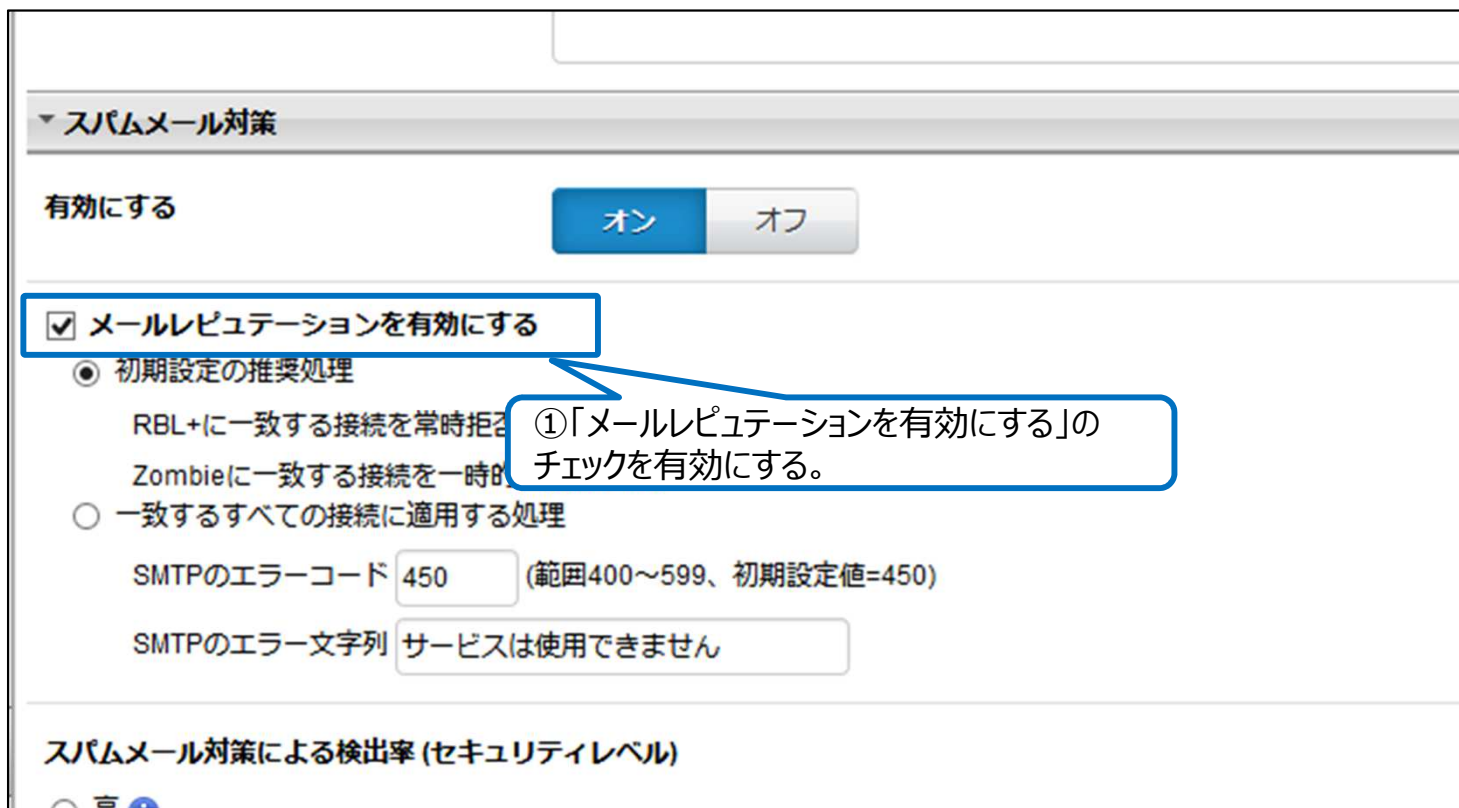
メールセキュリティ対策タブを選択します。

不正プログラム対策の「機械学習型検索を有効化」をオンにします。処理は「タグの追加」を選択します。

The screenshot displays a web interface with several tabs at the top: IPS, 不正プログラム対策, メールセキュリティ対策 (highlighted), 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. Below the tabs, there are two main sections for configuration. The first section, under '不正プログラム対策', has a '有効にする' (Enable) toggle set to 'オン' (On). A callout bubble points to the 'メールセキュリティ対策' tab with the text '①「メールセキュリティ対策」タブを選択します。'. The second section, under '機械学習型検索の有効化:', has a '有効にする' toggle set to 'オン'. A callout bubble points to this toggle with the text '②オンにします。'. Below the toggle, there are '処理:' (Action) options: 'ブロック', 'タグの追加' (highlighted), and an information icon. A callout bubble points to 'タグの追加' with the text '③「タグの追加」を選択します。'. Underneath, there are input fields for '件名タグ:' (Subject Tag) containing '[ウイルス駆除済み]' and '本文タグ:' (Body Tag) containing a placeholder message: '[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。'

3. 「メールセキュリティ対策」「不正プログラム対策」内の「機械学習型検索」の有効手順（2/2）

続いて、「スパムメール対策」の「メールレピュテーションを有効にする」のチェックを有効にします。右下の「保存」ボタンを選択します。



▼ スпамメール対策

有効にする オン オフ

メールレピュテーションを有効にする

初期設定の推奨処理

RBL+に一致する接続を常時拒否

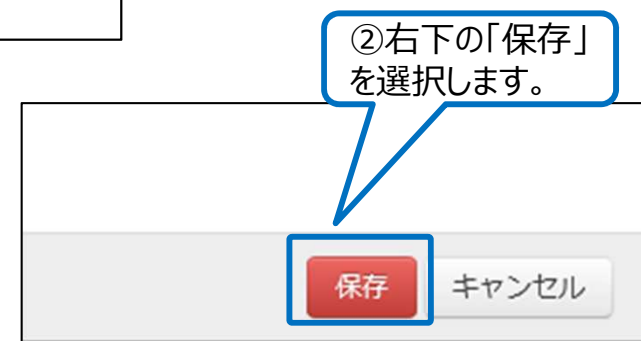
Zombieに一致する接続を一時的に拒否

一致するすべての接続に適用する処理

SMTPのエラーコード (範囲400~599、初期設定値=450)

SMTPのエラー文字列

スパムメール対策による検出率 (セキュリティレベル)



②右下の「保存」を選択します。

4.Cloud Edge本体への設定反映

Cloud Edge本体に設定を反映させるために「すべて配信」を選択します。
ゲートウェイ配信ステータスが「成功」になることを確認します。

The screenshot shows the Cloud Edge Cloud Console interface. At the top, there is a navigation bar with tabs for 'ダッシュボード', 'ゲートウェイ', 'ポリシー', '分析とレポート', and '管理'. Below this, a notification bar indicates that settings have been changed and that the 'すべて配信' button should be clicked to reflect the changes. A callout box points to the 'すべて配信' button with the instruction: ①「すべて配信」を選択します。

The main content area shows a list of objects under 'ポリシールール'. A dialog box titled 'ゲートウェイ配信ステータス' (Gateway Distribution Status) is open, showing the distribution status for 'CloudEdge_02'. The status is initially '配信中: 1' (Distribution in progress: 1). A blue arrow points to the right, where the status has changed to '成功: 1' (Success: 1). A callout box points to this status with the instruction: ②「成功」を確認します。

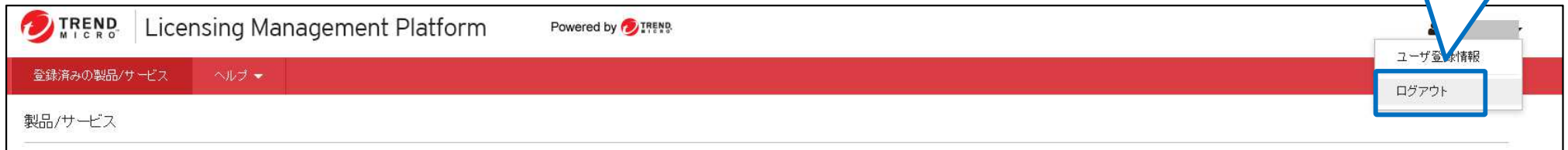
| 名前 | ステータス |
|--------|--------|
| 【50-1】 | 配信中: 1 |
| 初期設定 | 成功: 1 |

5.Cloud Edgeからログオフ

Cloud Edgeの右上の「ログオフ」を選択します。
Licensing Management Platformの「ログアウト」を選択します。



②「ログアウト」を選択します。



以上で設定は完了です。

6.その他留意事項

その他留意事項として、以下の点にご留意ください。

- 被害に遭わない心がけとして、以下2点についてもご留意ください。
 - 不審なメールや添付ファイルを開かないこと
 - Officeのマクロ機能を「無効」にしておくこと
- 下記のサイトもご参考いただき、必要な対策を実施ください。
JPCERT/CCマルウェアEmotetへの対応FAQ
<https://blogs.jpCERT.or.jp/ja/2019/12/emotetfaq.html>
- 以下の推奨設定につきましては、デフォルト値（施工時）有効済の設定となります。
 - 「メールセキュリティ対策」内の「不正プログラム対策」を有効にする
 - 「メールセキュリティ対策」内の「スパムメール対策」を有効にする
 - 「Webレピュテーション」を有効にする
- 以下の推奨設定につきましては、別途クラウドサンドボックスオプションの契約が必要となります。
 - 「メールセキュリティ対策」「不正プログラム対策」内の「仮想アナライザの有効化」をオンにする