



おまかせクラウドアップセキュリティ

# Box アクティベーション手順

東日本電信電話株式会社

| 年月          | 版     | 変更内容等                        |
|-------------|-------|------------------------------|
| 2021年08月25日 | 第1.0版 | 初版制定                         |
| 2021年09月10日 | 第1.1版 | 情報ラベル、商標についての資料の追加           |
| 2022年04月05日 | 第1.2版 | API連携時にエラーになった場合に再度実行を行う旨を記載 |
| 2022年06月21日 | 第1.3版 | 表紙記載の組織名を変更                  |
| 2022年08月03日 | 第1.4版 | 各種手順に文言追記                    |
| 2022年12月12日 | 第1.5版 | 事前準備完了の文言ページに他手順への誘導文面記載     |
| 2023年02月09日 | 第1.6版 | UI変更に伴い画像差し替え                |
|             |       |                              |
|             |       |                              |

おまかせクラウドアップセキュリティの管理コンソール画面にログインするための準備を行います。  
事前に管理コンソール画面にログインする際のパスワードを設定します。

# 事前準備 (1)

## 1. 事前準備

- ・開通メール「件名：新規アカウント発行のお知らせ」
- ・各クラウドアプリケーションの管理者のメールアドレス及び管理者パスワード

## 2. パスワード設定



2021/01/27 (水) 20:09  
PLX\_account\_support\_MailBox@trendmicro.co.jp  
新規アカウント発行のお知らせ

宛先 [REDACTED]

[REDACTED]

\* \* 様

Licensing Management Platform ログイン用の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=kjfSy>

アカウントの詳細:  
会社名: [REDACTED]  
アカウント名: [REDACTED]

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。

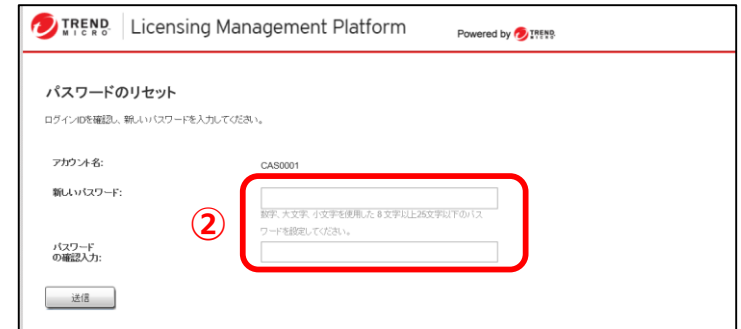
① <https://forgetpwd.trendmicro.com/ForgetPassword/ResetPassword?T=kjfSy&v=8abc15e1-d6e9-4250-8d9d-3c985a6588f7>

ご不明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。

トレンドマイクロ株式会社  
[http://esupport.trendmicro.co.jp/corporate/default.aspx?gnv=sb\\_support&Homeclick=gnv\\_sb\\_support&cm\\_re=Corp--gnv--sb\\_support](http://esupport.trendmicro.co.jp/corporate/default.aspx?gnv=sb_support&Homeclick=gnv_sb_support&cm_re=Corp--gnv--sb_support)  
03-5334-3601

- ① URLを押下します。  
※有効期限は7日間です。

- ②任意のパスワードを設定します。



TREND MICRO Licensing Management Platform Powered by トレンドマイクロ

### パスワードのリセット

ログインの確認し、新しいパスワードを入力してください。

アカウント名: CAS0001

新しいパスワード:  ②  
数字、大文字、小文字を使用した 8 文字以上26文字以下のパスワードを設定してください。

パスワードの確認入力:

送信

事前準備が完了しました。

次に、おまかせクラウドアップセキュリティとお客様でお申し込みいただいたクラウドアプリケーションの紐づけ作業を行います。

※本項目の設定のみではおまかせCASの機能は動作しません。

必ず以下の別紙の設定も実施いただくようお願いいたします。

- ・【ポリシー設定】高度な脅威対策設定手順
- ・【ポリシー設定】情報漏えい対策設定手順

# アクティベーション方法（1）

## 1. コンソール画面ログイン



提供されたアカウントとパスワードを入力して「**ログイン**」を押下します。  
※アカウントは開通メールに記載されております。  
※パスワードはP4にて設定したものになります。



①左図画面が表示された場合のみ、  
「**2要素認証設定を行う**」を押下します。  
※設定方法は「**2要素認証設定マニュアル**」をご参照ください。



②「**OK**」を押下します。

# アクティベーション方法（2）

TREND MICRO Licensing Management Platform Powered by TREND MICRO

最新情報の配信サービス ヘルプ

製品/サービス

+ キーワード

| 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    |
|----------|--------------------|----------|---------|------------|------------|----------|
| CAS      | Cloud App Security | 10シート    | 製品版     | 2023/02/18 | 2025/06/17 | コンソールを開く |

有効期限が: 有効期限切れ: 有効期限切れ:

③「コンソールを開く」を押下します。



ライセンス契約

日本のお客さま

本製品の使用許諾契約の内容につきましては、製品インストールメディア内に格納されている使用許諾契約書をご確認ください。  
格納されている使用許諾契約書と当社Webサイトに掲載している使用許諾契約書に異なる定めのあった場合には、当社Webサイトに掲載されている使用許諾契約書が優先されます。  
また、CD-ROMなどのインストールメディアのない製品やサービスにつきましては、当社Webサイトに掲載している契約書をご確認くださいようお願いいたします。

<http://www.trendmicro.co.jp/support/eula>

For other countries/languages

Please open below link in your browser and read the Trend Micro End User License Agreements.

<https://www.trendmicro.com/eula>

同意する キャンセル

④

④「同意する」を押下します。



TREND MICRO

| 今月の新機能  | 近日公開予定  |
|---|---|
| <p><b>Salesforceに対するセキュリティ対策の公式リリース</b></p> <p>※注意: Salesforceが対応したライセンスは日本ではまだ販売を開始しておりません。</p> <p>Salesforce SandboxとSalesforce本番環境に対する高度な脅威対策が正式に提供されるようになります。Salesforceをご利用のお客さまは、別途ライセンスを購入し、高度な脅威対策や情報漏えい対策ソリューションの検定を完了することによって、すべてのオブジェクトの検定を一歩保護するものと、Salesforce環境を利用して、Chatter、コミュニティ、ケース、および添付ファイルに送信された不正なURLやファイルから環境を保護できるようになります。</p> <p><b>Salesforce向けの高度な脅威対策ポリシーと情報漏えい対策ポリシーにおける権限管理の強化</b></p> <p>Salesforce向けの高度な脅威対策ポリシーと情報漏えい対策ポリシーで現在サポートされている【設定】に加えて、【権限】と【検索】の2つの処理が追加されます。</p> <p><b>Salesforce向けの高度な脅威対策ポリシーにおけるケースと添付ファイルのサポート</b></p> <p>高度な脅威対策機能が強化され、すでにサポートされているChatterとコミュニティに加えて、ケースと添付ファイルの2つのアプリはSalesforce環境の不正なファイルやURLから保護されるようになります。</p> <p><b>高度なフィッシング検出機能を提供するTrend Micro Phish Insightの統合</b></p> <p>※注意: 日本語版ではこの機能は提供しておりません。</p> <p>Trend Micro Phish Insightを統合することで、Phishingなどのソーシャルエンジニアリングには、お客様のセキュリティ意識を高め、向上させることができます。この統合により管理画面に、Cloud App Securityの検出率とTrend Micro Phish Insightの検出率を統合して表示できるようになります。</p> | <p><b>Exchange OnlineおよびGmailのWebドキュメンテーションでのURLのRetro Scanと自動修復</b></p> <p>ユーザのメールのメタデータに含まれる悪意のあるURLを再検索し、Webドキュメンテーションサービスによりアップロードされた最新のパターンファイルを使用して検出された脅威を削除するオプションが提供されます。ユーザのメールのメタデータには、最近になって発見された未検出の悪意のあるURLが含まれている可能性があります。このメタデータを一度検索することで、お役のメールアドレスが攻撃の影響を受けていないかどうかを確認するフォレンジック調査の重要な部分になります。</p> <p><b>Microsoft Teamsにおける手動検索のサポート</b></p> <p>Microsoft Teamsの保護機能が強化され、管理者は、高度な脅威対策および情報漏えい対策でリアルタイム検索に加えて手動検索を実行できるようになります。</p> <p><b>1つのローカルアカウントでの複数のCloud App Securityインスタンスの管理</b></p> <p>管理者は、1つのローカルアカウントを同じサイト内の複数のCloud App Securityインスタンスにバインドすることにより、それぞれの管理アカウントを使用して管理コンソール上でログオフとログオンを繰り返す代わりに、バインドされたインスタンスを切り替えることで1つのローカルアカウントで複数のインスタンスを管理できるようになります。</p> <p><b>表示名の新しい検出</b></p> <p>高度なスパムメール対策フィルタが強化され、管理者は、受信メールの送信者の表示名を検査するかどうかを選択することで、メールのなりすまし攻撃から従業員を保護できるようになります。同時に提供されるローカルアカウントリストに格納するメール送信者を追加することで、表示名のなりすまし攻撃から防御することもできます。</p> |

次回は表示しない 閉じる

⑤

⑤「閉じる」を押下します。

# アクティベーション方法（3）



コンソール画面にログインできていることを確認します。

⑥「運用管理」の中の「サービスアカウント」を押下します。



# API連携 – Box (1) <<CAS側の設定>>



## Boxのサービスアカウントの準備

手順1: Box関連のサービスデータにアクセスするために要求されるAPIに対する権限をCloud App Securityに付与します。 **ここをクリック** ②

手順2: [完了]をクリックします。

完了



①初期ログイン時は左記画面が表示されます。  
表示されない場合には、管理コンソール上部の「運用管理」⇒「サービスアカウント」を選択し押下します。

「追加」⇒「Box」を押下します。

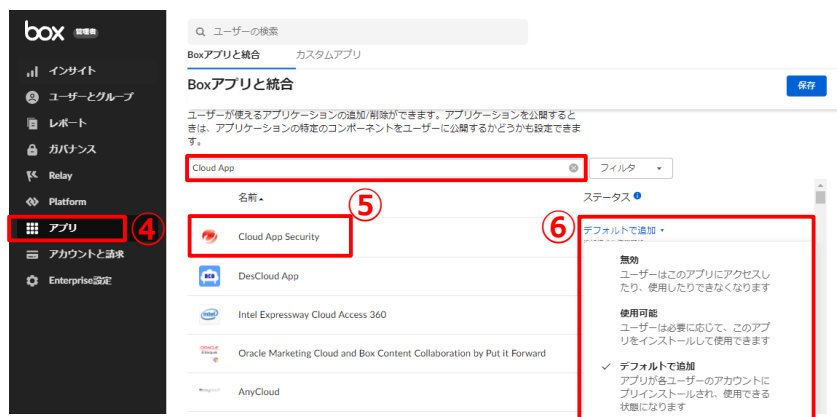
②手順1の「ここをクリック」を押下します。

画面に従い、Boxの管理者のメールアドレス及び管理者パスワードを入力します。

③右図の画面にて「Boxへのアクセス許可」を押下した後、  
②の画面に戻るため「完了」を押下します。

これ以降はBox側の作業に移ります。次頁へ進みます。

※正常に同期が行われずエラーメッセージ等が表示された場合、通信環境の問題やタイムアウトの可能性がありますので右上「×」を押下して一度連携画面を閉じてWebページをリロードし再度お試しください。(2~3回程度で成功することが多いです)



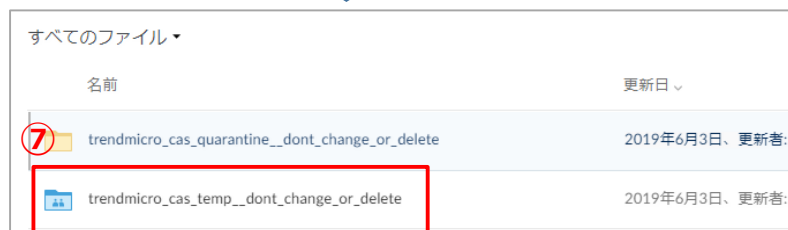
④ <https://app.box.com/master/settings> へアクセスします。管理者のメールアドレス及び管理者パスワードでログイン後、設定から「**アプリ**」タブを開きます。

⑤ アプリタブの画面下部「**アプリケーションの個別管理**」の検索窓で、「**Cloud App Security**」を検索します。

⑥ 項目内プルダウンより「**デフォルトで追加**」を選択します。その後、<https://account.box.com/> にアクセスします。



- 「**Cloud App Security**」を追加している場合のみ保護され、アプリケーションを削除すると保護が解除されます。
- 「**メールと通知**」で通知を無効化していない場合、ファイルが隔離されるたびに、すべての利用者が通知を受信してしまいますのでご注意ください。



⑦ 管理者の「**すべてのファイル**」一覧に作成された「**trendmicro\_cas\_temp\_dont\_change\_or\_delete**」を右クリックし、「**設定**」を開きます。

⑧ 「**メールと通知**」にて、以下2箇所にてチェックを実施します。  
 ・「**このフォルダとすべてのサブフォルダのデフォルト設定を上書きする**」  
 ・「**すべてのコラボレータへのすべてのメール通知を無効化する**」  
 画面上部へスクロールし「**保存**」を押下します。

これで、Boxとの同期設定は完了です。

初期設定時には、Box側の情報を同期する動作が行われます。ライセンス数やファイル容量が多い場合（例：10,000ユーザ以上）には、設定が終了するまでに3～4時間程度かかる場合があります。

## タスクリスト表示

Cloud App Security

タスクリスト (4)

- デレゲート アカウントを準備しました。 × 成功しました 2016/04/11 18:59
- SharePoint Onlineのサイトコレクションおよびサブサイトを更新しました。 × 成功しました 2016/04/11 19:01
- OneDrive for Businessユーザを更新しました。 × 成功しました 2016/04/11 19:01
- ユーザおよびグループを更新しました。 × 成功しました 2016/04/11 18:59

## 通知表示

Cloud App Security

通知 (6)

- Exchange Onlineは保護されています。 × 成功しました 2016/04/11 19:01
- SharePoint Onlineは保護されています。 × 成功しました 2016/04/11 19:01
- OneDrive for Businessは保護されています。 × 成功しました 2016/04/11 19:01
- ローカルログオンアカウントを作成して複数の管理者を管理します。 × オプション
- 高度な脅威対策のポリシーを作成します。 × オプション
- 情報漏えい対策のポリシーを作成します。 × オプション

初期設定が完了すると、上記画面のように対象サービスのタスクが「成功しました」となります。

※「保留」ステータスの場合は、他のアプリケーションの連携は実施できないため、「成功しました」の文言が出るまでお待ちください。



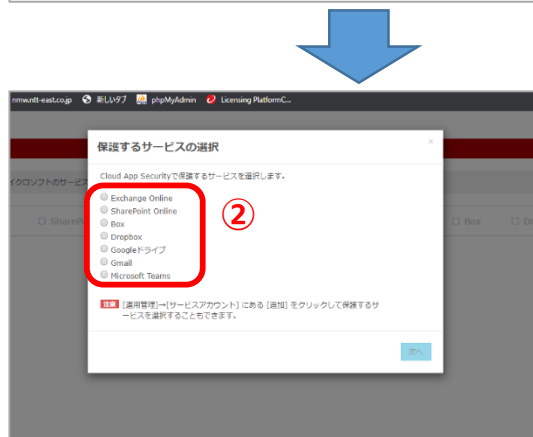
ステータスが「保留」のまま変わらない場合、何かしらの問題が発生している可能性があります。  
一度画面を切り替えて確認します。  
それでも「保留」の場合は時間を置いて、再度アクティベーションを実施します。

# (参考) API連携 – 初期ログイン時の対応 (1)

※初回にコンソール画面よりログインした場合のみ、下記の画面に推移します。



①「コンソールを開く」を押下します。



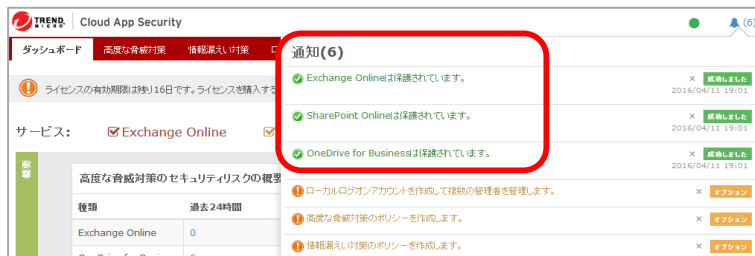
②保護するサービスを選択します。



③選択したサービスの管理者のメールアドレス及び管理者パスワードを入力します。

④「送信」を押下します。

## (参考) API連携 – 初期ログイン時の対応 (2)



「通知」にアクティベートしたサービスが表示されるので、内容を確認します。

- Boxは、Box, Inc.の商標または登録商標です。
- Trend Micro Cloud App Security、Cloud App Securityは、トレンドマイクロ株式会社の登録商標です。