

法人向けセキュリティサービス

# Cloud App Security

## (利用マニュアル)

第 1.4 版

2021/10/08

◆目次	P1
はじめに（必ずお読みください）	P2
1．開通案内メールの受領&管理コンソールログイン	P3
2．対象のクラウドアプリとの同期化	P4
3．その他設定	P9
＜参考1＞セキュリティポリシーの設定/利用開始(デフォルト設定活用)	
＜参考2＞セキュリティポリシーの設定/利用開始(監視のみ)	

## 1.はじめに(必ずお読みください)

本マニュアルは、法人向けセキュリティサービス利用規約上に規定される機密情報の一部をなすものです。本マニュアルの取り扱いにつきましては、当該規定に従い、十分ご注意下さい。

### 「Cloud App Security」ご利用の流れ

#### ① 開通案内メールの受領&管理コンソールログイン確認

「サービス提供開始のお知らせ」に記載された内容に従い、ログイン ID と初期パスワードの確認後、管理コンソールにログインします。



#### ② 対象のクラウドアプリとの同期化

監視を開始するために、対象クラウドアプリのアカウント情報を Cloud App Security 側に登録し同期します。

※本マニュアルでは「Microsoft Office 365」を例に説明いたします。詳しくは次頁以降をご参考ください。



#### ③ 検索開始

お客さまのご用途に応じ、セキュリティポリシーの設定を行って、脅威の検索を開始してください。

※セキュリティポリシーの設定方法については、オンラインヘルプ(管理コンソール上部の「？」ボタンを押下) および本マニュアル巻末の＜参考 1＞を参照ください。

## 1. 開通案内メールの受領 & 管理コンソールログイン

### ① 開通案内メール受領

サービス開通日に合わせ送信される、以下の開通案内メールをご確認ください。

件名：サービス提供開始のお知らせ - Cloud App Security

FROM：cas-info@sec-business.net

契約回線 ID(N 番)：N○○○○○○○○○○

平素は、NTT コミュニケーションズのサービスをご利用頂きありがとうございます。

お申込みいただきましたサービスがご利用可能となりました。

<登録完了のご案内>

お客さまのアカウント登録が完了致しました。

アカウントの詳細

ログイン ID：XXXXXXXXXX

パスワード：XXXXXXXXXX

以下の URL から管理コンソールにログインできます。

<https://clp.trendmicro.com/Dashboard?T=h0hEU>

<以下省略>

### ② 管理コンソール URL にアクセス

開通案内メールに記載された、管理コンソール URL にアクセスし、同じく開通案内メールに記載されたログイン ID とパスワードでログインを試してください。

(※パスワードはログイン後、変更してください)

## 2. 対象のクラウドアプリとの同期化

### ① Licensing Management Platform へのログイン

開通案内メールに記載された管理コンソール URL にアクセスすると、Licensing Management Platform(以下、LMP)へのログイン画面が表示されます。

ログイン ID とパスワードを入力しログインしてください。

**TREND MICRO Licensing Management Platform** Powered by TREND MICRO

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

アカウントをまだ取得していない場合 [今すぐ登録](#)

As a service provider, this platform gives you:

- Instant Provisioning - Provision a service for your customer anytime.
- Easy Customer Support - One-click access to customer information and license status.
- True Software-as-a-Service - Provide your service as a monthly service plan.
- Great Brand Name Exposure - Put your brand and logo on the platform and on selected services.

### ② Cloud App Security の管理コンソールへの移動

LMP にログインすると、以下の画面が表示されます。この画面からはお客さまの契約状況が確認可能です。

Cloud App Security(以下、CAS)の管理コンソール画面を表示するためには、アクション項目の「コンソールを開く」をクリックしてください。

**TREND MICRO Licensing Management Platform** Powered by TREND MICRO

ようこそ: NTTc [ログアウト](#)

登録済みの製品サービス ユーザ登録情報 サポート情報

登録済みの製品/サービス

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
ライセンス	Cloud App Security	1シート	製品版	2016/08/16	自動更新	<a href="#">コンソールを開く</a>

☒ 有効期限内 
 ☐ 間もなく期限切れ 
 ☒ 有効期限切れ

### ③ 初期設定（クラウドアプリとの同期化）

CAS の管理コンソールの初回ログイン時は以下の画面が表示されます。

※画面を消してしまった場合は、管理コンソールの「運用管理」→「サービスアカウント」→「追加」で行ってください。

#### 保護するサービスの選択

Cloud App Securityで保護するサービスを選択します。

- ☐ Exchange Online
- ☐ SharePoint Online
- ☐ Box
- ☐ Dropbox
- ☐ Googleドライブ
- ☐ Gmail
- ☐ Microsoft Teams

**注意** [運用管理]→[サービスアカウント]にある[追加]をクリックして保護するサービスを選択することもできます。

次へ

「保護するサービスの選択」より対象のクラウドアプリをご選択ください。

※本マニュアルでは「Exchange Online」を例として説明します。

## ④ アカウント情報の登録

表示された手順に従い、選択したクラウドアプリの認証情報（資格情報）を入力します。

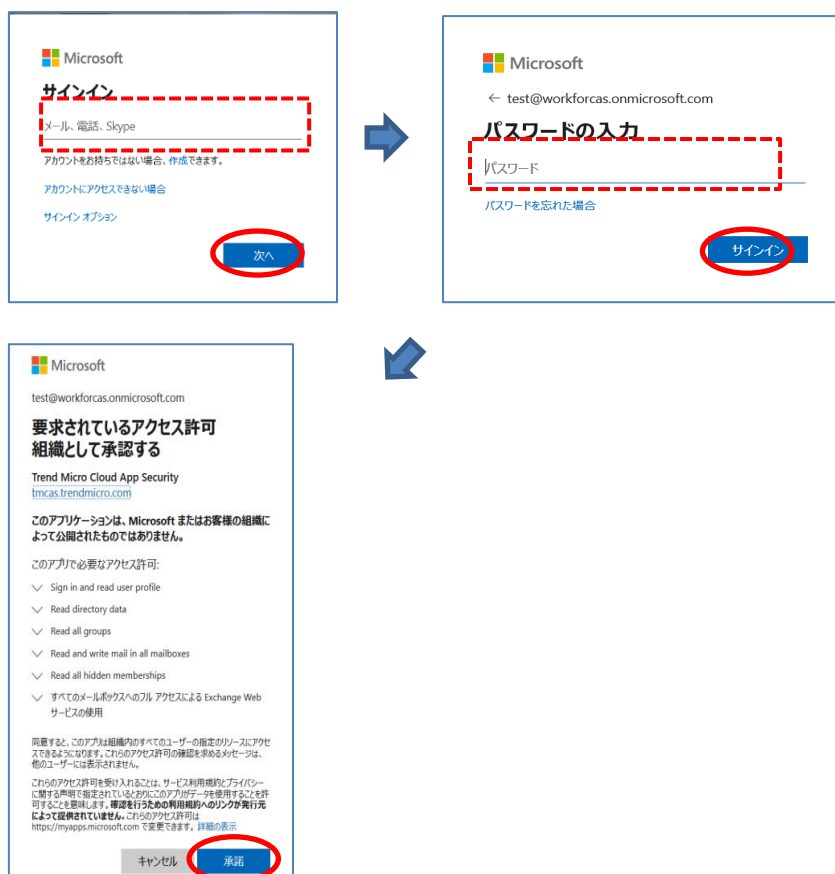
※本マニュアルでは「Microsoft Office 365 (Exchange Online)」を例として説明します。

1. 手順 1. の「ここをクリック」を押下します。

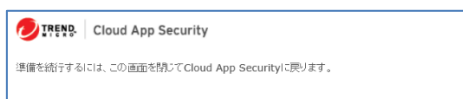


2. 画面に従い、認証情報を入力します。

※Exchange Online の場合、Office365 グローバル管理者のログイン ID/パスワードを入力し、アクセス許可を承認します。



3. 認証に成功するとブラウザの別タブに以下の画面が表示されますので、この画面を閉じて元の画面(1.の画面)に戻ります。

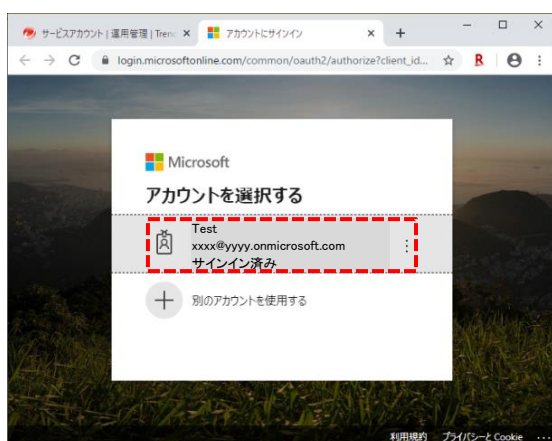


4. 手順 2. の「ここをクリック」を押下します。



5. 画面に従い、再度認証を行います。

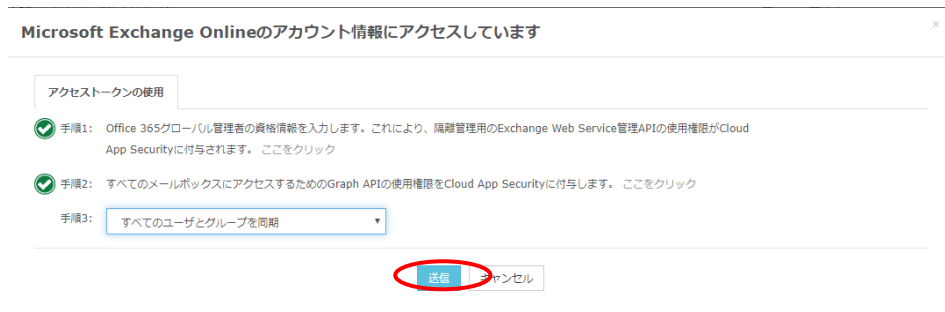
※設定によっては、2.の認証情報を再度入力する場合もあります。





5. 手順 3. で同期対象を指定し、「送信」を押下します。

※保護対象としたいユーザに特別な制約がない限りは、「すべてのユーザとグループを同期」を選択してください。



## ⑤同期化完了

アカウント情報の登録が完了すると、管理コンソール上に「成功しました」の通知が表示されます。(画面情報のベルマークにカーソルをあてると表示されます:「処理中」と表示されている場合は、まだ同期作業中です。そのまましばらくお待ちください。)

※同期済みのクラウドアプリの接続状態も同じ画面で確認できます。



以上で、クラウドアプリとの同期化は完了です。これにより、対象のクラウドアプリと Cloud App Security との間で通信が開始されます。

この後は、用途に合わせ、管理コンソールの「高度な脅威対策」メニューにて各クラウドアプリのセキュリティポリシーを設定し、脅威の検出を開始してください。オンラインヘルプ(管理コンソール上部の「?」ボタンを押下)に詳細がございます(「機能」⇒「高度な脅威対策」⇒「高度な脅威対策ポリシーを追加する」参照)。



なお、本マニュアル巻末でも、＜参考 1＞にてデフォルト設定を活用した、最もシンプルな設定手順を紹介しております。ご活用ください。

### 3. その他設定

#### ※管理コンソールへのログイン

管理コンソールにログインするためには以下の2つの方法があります。

- ・ Licensing Management Platform からのログイン（4 頁参照）
- ・ 管理者アカウントを追加し、CAS 管理コンソール URL からログイン（次頁参照）

Licensing Management Platform からのログインが正常に行われない場合に備え、管理者アカウントを追加しておくことをお勧めします。

#### ■管理者アカウント追加

管理コンソールにアクセスし各種設定変更が可能な、管理者アカウントを複数作成することが可能です。

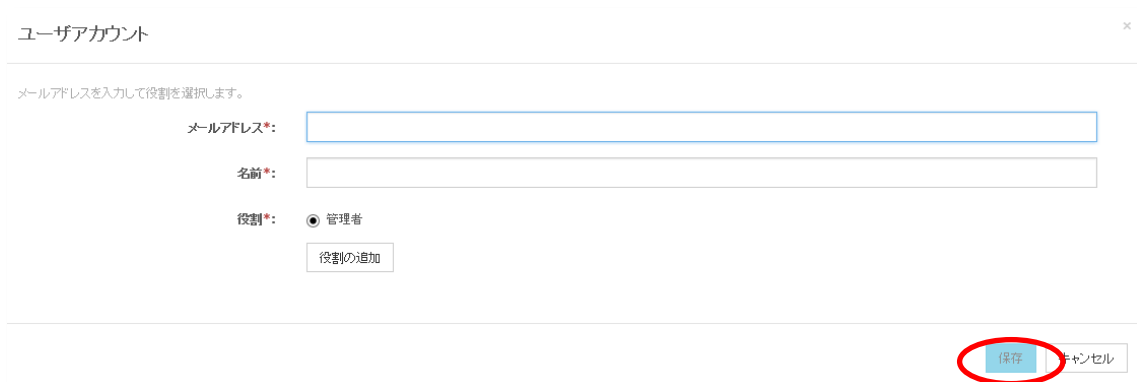
①「運用管理」より「管理者と役割」をクリックしてください。



②左上の「追加」をクリックしてください。



③管理者として追加したい情報（メールアドレス、名前等）を記載し、「保存」をクリックしてください。



ユーザアカウント

メールアドレスを入力して役割を選択します。

メールアドレス\*:

名前\*:

役割\*: ☒ 管理者

④記載したメールアドレス宛に以下のメールが送信されます。

件名：アラート: Trend Micro Cloud App Security アカウントのパスワードをリセットしてください

FROM : Do Not Reply <DoNotReply4@jp.tmcas.trendmicro.com>

〇〇様

Trend Micro Cloud App Security アカウントのパスワードのリセットが必要です。

次の URL をクリックしてパスワードをリセットしてください。

<https://admin.tmcas.trendmicro.co.jp/#!/XXXXXXXXXXXXXXXXXXXXXXXXXXXX>

コンソール URL: <https://admin.tmcas.trendmicro.co.jp>

ユーザ名: XXXXXXXXXX

<以下省略>

⑤メールの文面に従い、URL にアクセスし、パスワードをリセットしてください。  
パスワードリセット後は、上記メールに記載されている  
コンソール URL (<https://admin.tmcas.trendmicro.co.jp>) より、追加した管理者アカウントで  
CAS の管理コンソールにログインすることが可能です。



**Trend Micro Cloud App Security**  
クラウドアプリケーション向けセキュリティ強化ソリューション

48,631,579  
Cloud App Securityにより  
検出された世界中の脅威

1.96 B  
Cloud App Securityにより  
検索された世界中のメールメッ  
セージやファイル

電子メールや共有ファイルの 安全な利用を実現

Trend Micro Cloud App Securityは、保護対象のクラウドアプリケーションを直接統合することにより、ネットワークを追加設定したトラフィックのルーティング経路を変更したりすることなくクラウドアプリケーションの脅威対策とデータ保護を強化します。サンドボックス技術により、ファイルバターンに頼らないOffice文書やPDFドキュメントの不正なふるまいの分析を可能にします。また、情報漏えい対策機能により、機密情報を扱う通信の可視性とコンプライアンスの監査が向上します。

ここをクリックして、サポートされるクラウドアプリケーションについて確認してください。

ユーザー名

パスワード

パスワードをお忘れの場合 [ローカルアカウント](#)

ログイン

Copyright © 2017 Trend Micro Incorporated. All rights reserved.

以上で、管理者アカウント追加は完了です。

## ＜参考 1＞セキュリティポリシーの設定（デフォルト設定活用）

同期完了後、お客さまのご用途に応じ、管理コンソールの「高度な脅威対策」メニューを使用してさらにセキュリティポリシーの設定を行い、脅威の検索を開始させます。

参考として、デフォルト設定を活用した、最もシンプルな設定手順を記載いたします。  
ご活用ください

※本マニュアルでは「Exchange Online」を例として説明します。

### ①デフォルトポリシーの表示

管理コンソールの「高度な脅威対策」のメニューより、設定したいクラウドアプリのデフォルトポリシー（初期設定の～ポリシー）をクリックします。



※「監視のみ」というポリシーも表示されていますが、選択しないでください。

※デフォルトポリシーを残し新たに設定したい場合は、同画面コピー機能を活用ください。

### ②ポリシーの修正

ポリシー画面左側の各観点を押下し、必要な修正を行います。

1. 「一般」では修正はありません。

・コピーしたポリシーを使用する場合は、ここで新たなポリシー名を設定できます。

高度な脅威対策ポリシー | Exchange Online

<b>一般</b> 高度なスパムメール対策 不正プログラム検索 ファイルブロック Webレピュテーション 仮想アナライザ	<input type="checkbox"/> リアルタイム検索を有効にする <input type="checkbox"/> 迷惑メールフォルダを検索しない ポリシー名 * : 初期設定のExchangeポリシー - 高度な脅威対策 概要: このポリシーは別のポリシーが作成されていない場合に対象として使用されます。 優先度: 2
---	---

2. 「高度なスパムメール対策」の「ルール」で以下の修正を行います。

※メールアプリのみの設定です(メニュー自体がない場合は設定不要)

- ・「高度なスパムメール対策を有効にする」にチェックにします。
- ・適用範囲を「すべてのメッセージ」に変更します
- ・検出レベルを「中」に変更します(※)



(※) 「中」が標準的な設定ですが、適切なレベルはお客様により異なります。検出数過多/過検知・誤検知が散見されるようであれば、検出レベルを「低」に戻してご利用ください。

その下、「不正プログラム」「ファイルブロック」では特に変更はしません。

- 「Web レピュテーション」の「ルール」「承認済み/ブロックする URL リスト」で以下の修正を行います。
  - 適用範囲を「すべてのメッセージ」に変更します
  - 「メッセージ添付ファイルに含まれる不審 URL を検索する」をチェック
  - 「承認済み URL リストを有効にする」をチェック（結果「内部ドメインを承認済み URL リストに追加する」が有効になります）

- 「仮想アナライザ」の「ルール」で以下の修正を行います。
  - 「次を分析：」の「URL」をチェック

- すべての修正が済んだら、画面右下の「保存」ボタンを押下して設定を保存します。

## ③ポリシーの適用（脅威検知開始）

設定を保存すると、①の画面に戻るので、保存したポリシーの「オフ」をクリックして「オン」に変更します。



これで、設定した監視ポリシーが有効になり、ポリシーに従った脅威の検出が開始されます。

検出状況は、管理コンソールの「ログ」メニューにて確認下さい。（「ログ」メニューの見方/使い方については、オンラインマニュアルを参照ください。）



## ＜参考2＞セキュリティポリシーの設定（監視のみ）

本格利用前に、事前に検知の程度を確認しておきたいなど、実際の脅威の処理（隔離/削除など）をせずに、検知結果のみを管理コンソールに表示したい場合は、「監視のみ」の設定が便利です。

以下の手順で設定が可能ですので、ご活用ください。

※本マニュアルでは「Exchange Online」を例として説明します。

### ①デフォルトポリシーの表示

管理コンソールの「高度な脅威対策」のメニューより、設定したいクラウドアプリのデフォルトポリシー（初期設定の～ポリシー（監視のみ））をクリックします。

The screenshot shows the Trend Micro Cloud App Security interface. The '高度な脅威対策' (Advanced Threat Protection) tab is selected. Under the 'ポリシー' (Policies) section, the 'Exchange Online' policy is listed. The policy name '初期設定のExchange Onlineポリシー - 高度な脅威対策 (監視のみ)' is highlighted with a red box. The status is 'オフ' (Off). The description indicates it is a monitoring-only policy. The target is 'すべてのユーザ' (All users).

優先度	ポリシー	対象
1	初期設定のExchange Onlineポリシー - 高度な脅威対策 (監視のみ) 初期設定のポリシー: 監視モードで動作して、対象の検索と検出の記録のみを行います。すべての処理は「放置」に設定され変更できません。	すべてのユーザ
2	初期設定のExchangeポリシー - 高度な脅威対策 初期設定のポリシー: 別のポリシーが作成されていない場合に対象として使用されるポリシー	すべてのユーザ

### ②ポリシーの修正

ポリシー画面左側の各観点を押下し、必要な修正を行います。

1. 「一般」では修正はありません。

次の「高度なスパムメール対策」に進んでください。

2. 「高度なスパムメール対策」の「ルール」で以下の修正を行います。

※メールアプリのみの設定です(メニュー自体がない場合は設定不要)

- ・「高度なスパムメール対策を有効にする」にチェックにします。
- ・適用範囲を「すべてのメッセージ」に変更します
- ・検出レベルを「中」に変更します

高度な脅威対策ポリシー | Exchange Online

一般

☒ 高度なスパムメール対策を有効にする

☒ 検出機能向上のため不審メール情報をトレンドマイクロに送信する

Trend Micro Cloud App Securityは、メールメッセージを介して送信されるビジネスメール詐欺 (BEC)、ランサムウェア、高度なフィッシング、および他の頻繁に見られる攻撃を検出するコンテンツ検索機能を提供します。詳細については、[こちら](#)を参照してください。

ルール

適用: 受信メッセージ

検出レベル:

☐ 高: スパムメールの検出率が最も高くなりますが、誤検出の可能性も高くなります

☒ 中: スパムメールの検出率が高く、誤検出の可能性は中程度です

☐ 低: スパムメールとして明白なものが検出され、誤検出の可能性が最も低くなります

3. 「不正プログラム検索」の「処理」で以下の修正を行います。

- ・すべて「通知しない」に変更します。

一般

高度なスパムメール対策 ☒

不正プログラム検索 ☒

ファイルブロック ☒

Webレピュテーション ☒

仮想アナライザ ☒

ルール

処理

処理: 検出された脅威に対するカスタマイズ処理

検出された脅威	検出された脅威に対するカスタマイズ処理	および	通知
ウイルス:	放置	および	通知
ワーム/トロイの木馬:	放置	および	通知
バックdoor:	放置	および	通知
その他の不正コード:	放置	および	通知
スパイウェア/グレーウェア:	放置	および	通知
ランサムウェア:	放置	および	通知
検索不能な圧縮ファイル:	放置	および	通知しない
サイズが150MBを超えるファイル: 添付ファイルが150MBを超えるメール:	放置	および	通知しない

検索不能なメッセージのオプションを表示

その下、「ファイルブロック」では特に変更はしません。

4. 「Web レピュテーション」の「ルール」「承認済み/ブロックする URL リスト」で以下の修正を行います。

- ・適用範囲を「すべてのメッセージ」に変更します
- ・「メッセージ添付ファイルに含まれる不審 URL を検索する」をチェック
- ・「承認済み URL リストを有効にする」をチェック（結果「内部ドメインを承認済み URL リストに追加する」が有効になります）

5. 「仮想アナライザ」の「ルール」「処理」で以下の修正を行います。

- ・「次を分析:」の「URL」をチェック
- ・すべて「通知しない」に変更します。

リスク	リスク高	リスク中	リスク低	未評価	および	通知
通知	通知	通知	通知	通知	通知	通知しない
通知しない	通知しない	通知しない	通知しない	通知しない	通知しない	通知しない

6. すべての修正が済んだら、画面右下の「保存」ボタンを押下して設定を保存します。



### ③ポリシーの適用（監視のみ脅威検知開始）

設定を保存すると、①の画面に戻るので、保存したポリシーの「オフ」をクリックして「オン」に変更します。



これで、設定した監視のみのポリシーが有効になり、ポリシーに従った脅威の検出が開始されます。

検出状況は、管理コンソールの「ログ」メニューにて確認下さい。（「ログ」メニューの見方/使い方については、オンラインマニュアルを参照ください。）