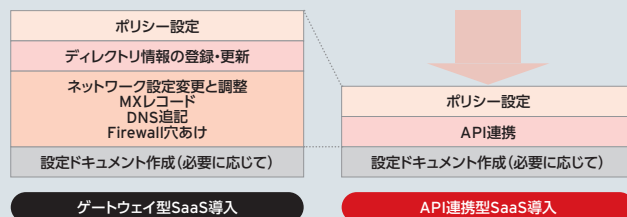


## 導入・管理面のメリット

### 導入期間・コストの抑制

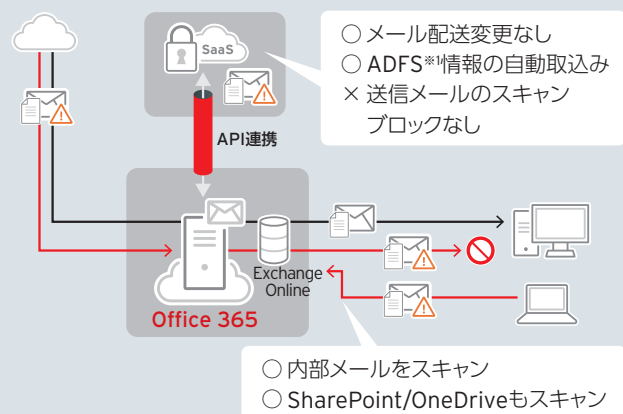


- 面倒なディレクトリ認証もAPI連携で不要
- 「ルール」「処理」「通知」の3つを選ぶだけのかんたん設定
- スキャン対象を絞ってのスタートも可能
- 導入までの期間・コストを抑制

### 「API連携型」と「ゲートウェイ型」の比較

#### API型 Trend Micro Cloud App Security

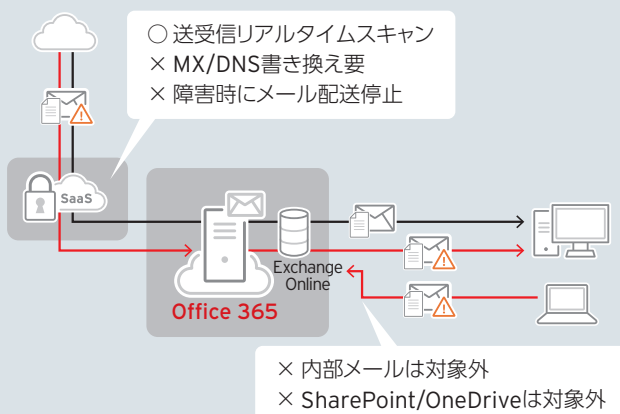
API連携により、メールボックスやクラウドストレージに対してスキャンが実行され、再スキャンができる。



\*1 ADFS: Active Directory Federation Service

#### ゲートウェイ型クラウドセキュリティ

メール送受信の経路でスキャンが実行され、受信後は再スキャンができない。



### マルチクラウド※2に1ライセンスで対応

追加費用なしでメールだけでなく、クラウドストレージサービスも守ることができます。同じユーザであればTrend Micro Cloud App Securityが対応している複数のクラウドアプリケーションを保護しても、追加費用なしの1ライセンスで対応可能です。

※2: マルチクラウドとは、複数のクラウドサービスを組み合わせて使うこと。

※右記標準価格は1年間のスタンダードサポートサービス提供を含む各サービスの1ライセンスあたりの使用許諾料金であり、サービスの継続利用、バージョンアップ、パターンファイルのダウンロード等のサポートサービス継続をご希望の場合は1年ごとに契約の更新が必要です。

※記載内容は予告なく変更される場合があります。

※追加、更新の価格は新規標準価格と同額です。

(注) 契約期間中の追加ライセンス数が5ライセンスに満たない場合、契約の更新時までは追加費用なしで利用可能です。その後更新を迎えた時、または追加利用数が5以上になった時に追加購入ください。なお、更新と同時に購入の際は5ライセンス未満での追加購入が可能です。

### Trend Micro Cloud App Security

#### 標準価格表(消費税別)

価格 ランク	ライセンス数	Cloud App Security
		新規標準価格
A	5 ~ 499	¥ 5,150
B	500 ~ 999	¥ 4,530
C	1,000 ~ 1,999	¥ 4,150
D	2,000 ~ 4,999	¥ 3,670
E	5,000 ~ 9,999	¥ 3,190
F	10,000 ~ 24,999	¥ 2,780
G	25,000 ~	¥ 2,590
新規・更新時最低購入数量		5ライセンス
追加時最低購入数量 (注)		5ライセンス
ライセンス課金対象		アカウント数

体験版など詳しくは ▶ [www.go-tm.jp/tmcas](http://www.go-tm.jp/tmcas)



お問い合わせ先

東京本社  
〒151-0053 東京都渋谷区代々木2-1-1  
新宿メインタワー  
TEL.03-5334-3601 (法人お問い合わせ窓口)  
FAX.03-5334-3639

名古屋営業所  
〒460-0002 愛知県名古屋市中区丸の内3-22-24  
名古屋桜通ビル7F  
TEL.052-955-1221 FAX.052-963-6332

[www.trendmicro.com](http://www.trendmicro.com)

TREND MICRO, Connected Threat Defense, およびXGenはトレンドマイクロ株式会社の登録商標です。本ドキュメントに記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。記載内容は2019年2月現在のものです。内容は予告なく変更になる場合がございます。Copyright©2019 Trend Micro Incorporated. All right reserved.

BR-CAS-005

User Protection



# Trend Micro Cloud App Security™

Office 365、G Suite、Box、Dropboxのセキュリティを強化

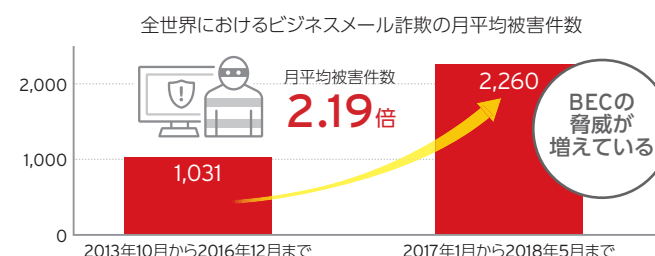


## 知っておきたいクラウドサービスの2つのリスク

メール経由の脅威とクラウドストレージからの情報漏えいリスク

### リスク1

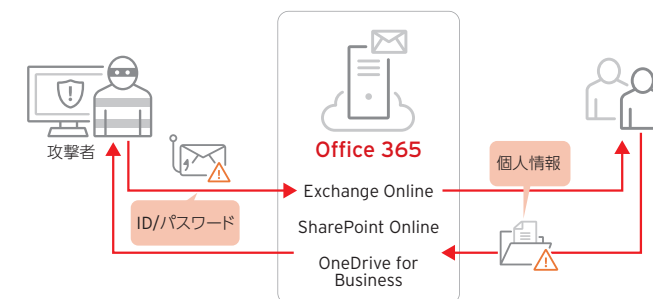
ビジネスメール詐欺 (BEC) の脅威が拡大\*



\*FBIの公表情報をもとにトレンドマイクロが独自に算出  
<https://www.ic3.gov/media/2017/170504.aspx>  
<https://www.ic3.gov/media/2018/180712.aspx>

### リスク2

クラウドストレージからの情報漏えい



詳細は裏面へ ➡

# 多層防御とAIによる機械学習でクラウドアプリケーションのセキュリティを強化

## Office 365<sup>※1</sup>、G Suite<sup>※2</sup>におけるセキュリティ課題

※1 対応アプリケーション: Exchange Online, OneDrive for Business, SharePoint Online  
※2 対応アプリケーション: Gmail, Google ドライブ (Gmailは、2019年4月～6月対応予定)



### 続発するメールインシデント

- ・ビジネスメール詐欺による事業損失
- ・クレデンシャル・フィッシングによる認証情報・個人情報の流出



### クラウドストレージの情報漏えいリスク

- ・OneDrive for Business、Google ドライブからの個人情報漏えいインシデント
- ・個人・機密情報のパブリッククラウドストレージへの保存



### 複雑化する運用管理

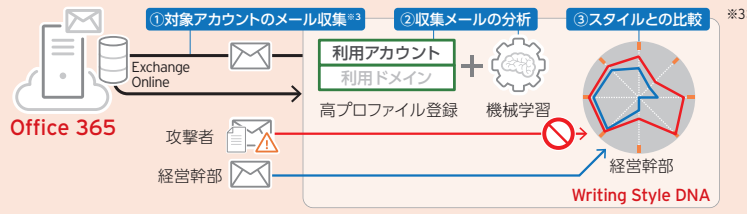
- ・複数システム活用によるMXレコードの引き回し
- ・ディレクトリサービスと別系統のユーザ管理



## 続発するメールインシデントに対する多層防御

### NEW メール本文のスタイル精査 Writing Style DNA™

攻撃者から送られてきたなりすましメールを、あらかじめ収集された対象アカウントのメール文のスタイルと比較。正規のメールか判定します。

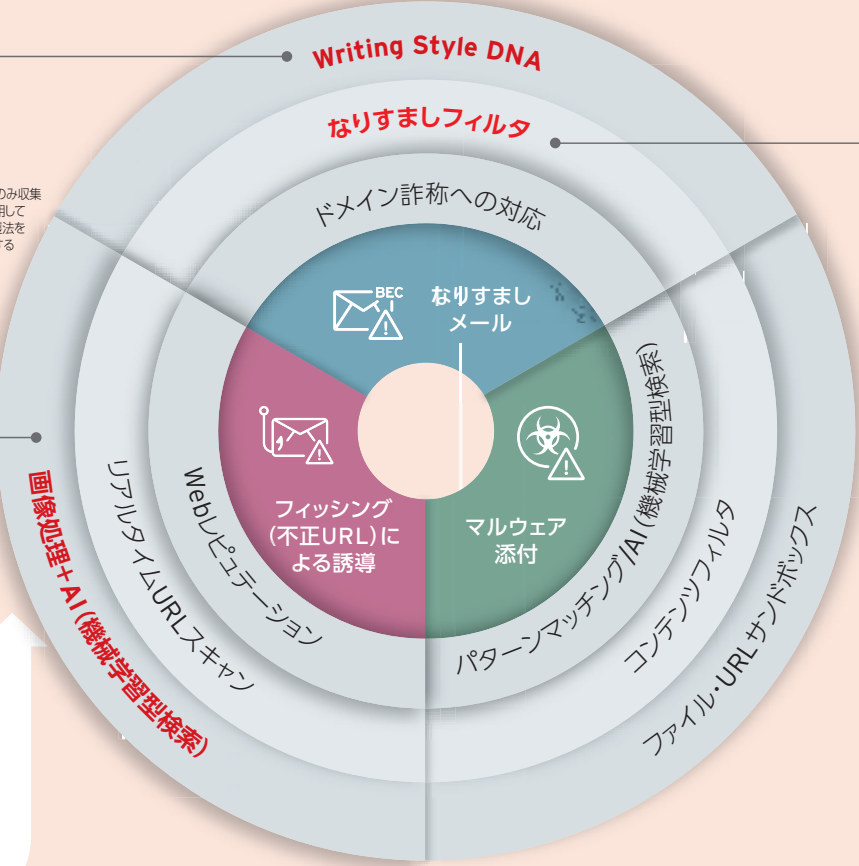
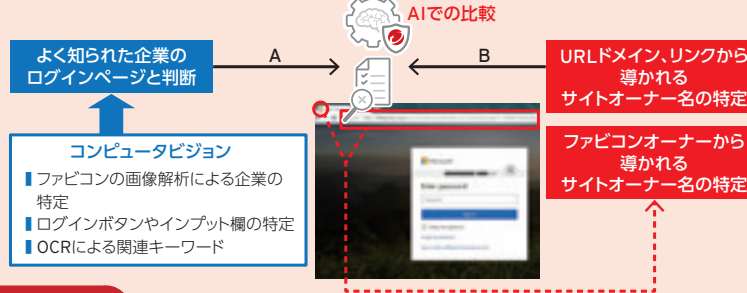


※3: メール内容は分析用としてのみ収集し、暗号化し厳重に管理・運用しております。改正個人情報保護法をはじめとする個人情報に関する法規制を遵守するとともに、各国のセキュリティ規制に準拠するセキュリティ基準を保持しております。加えて、お客さまにとって安心できる、かつ有益なデータ利用を進めてまいります。

偽ログインサイトへの誘導を検知

### 画像処理とAIによる「偽ログイン画面」の検知

コンピュータビジョンによる画像解析結果と、取得したファビコンのオーナー情報をAIで比較。正規サイトか機械的に判断します。



機械学習を併用し「なりすましメール」を検出

### なりすましフィルタ

不正メールがエンベロープやヘッダー・メール本文に残す典型的な痕跡を、SNAP<sup>※5</sup>フィルタで検知することで、体系的になりすましメールを検出します。

※5 SNAP: Social eNginneering Attack Protection

#### Mail Header

Message-Id: <08924520399f2e5d9e07...>  
User-Agent: Workspace Webmail 6.4.1  
Subject: Re: URGENT  
Reply-To: "Wilson Ceo" <emailpresident2@gmail.com>

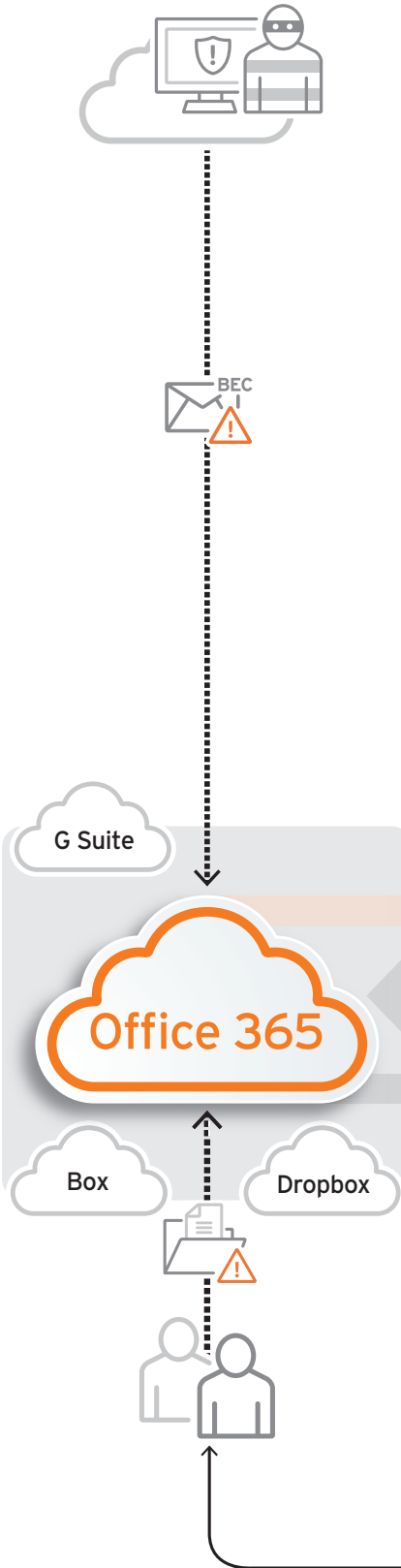
捏造されたFrom: ドメイン  
手入力で追加されたReply-To: ceo@compny.com  
Replyがフリーメール



スパムメール対策	
クレデンシャル・フィッシング対策(偽ログイン画面対策)	
	パターンマッチングファイル検索
	サンドボックス動的解析
	ドキュメント脆弱性検出
	機械学習型検出
	添付ファイルブロックフィルタ
	本文とファイルの不正URLを検索
メール不正プログラム対策	

## Trend Micro Cloud App Security™

## 漏えいを防ぐ仕組み作りでクラウドストレージの安全性を確保

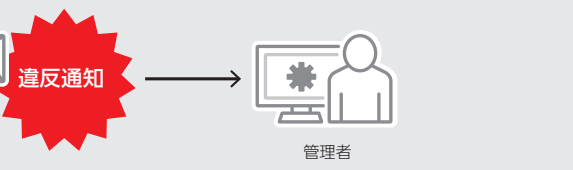


### API連携<sup>※4</sup>

※4: Application Programming Interface

### 外部漏えいにつながるデータを置かない仕組み

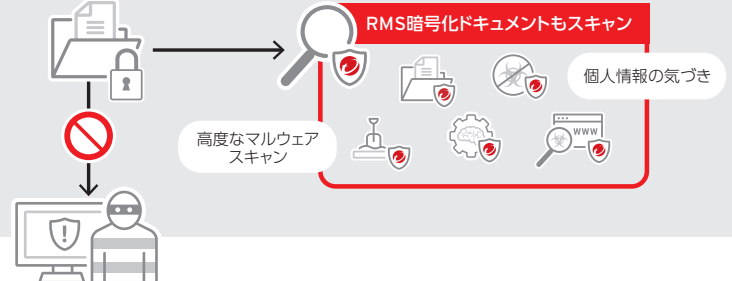
不適切な場所に個人情報やマイナンバーのデータを保管していないことを、情報漏えい対策(DLP)機能により把握、管理できます。攻撃された場合のデータ流出による被害を防ぎます。



### 持ち出されても悪用できないセキュアな仕組み

RMS<sup>※6</sup>で暗号化されたドキュメントもスキャン可能。個人情報が含まれた暗号化ファイルの検出や、持ち出されても利用できない仕組みとの共存が可能です。

※6: Rights Management Service



共有文書不正プログラム対策	パターンマッチングファイル検索
	サンドボックス動的解析
	ドキュメント脆弱性検出
	機械学習型検出
共有文書情報漏えい対策	添付ファイルブロックフィルタ
	ファイル内の不正URLを検索
レポート作成、送信	
Connected Threat Defenseによる不審オブジェクトの受取	

※個人情報保護法(日本語版を含む)漏えいの可能性があるメール添付など、流出を監視します。