GUARDIANWALL
Inbound Security for Microsoft 365
製品紹介資料

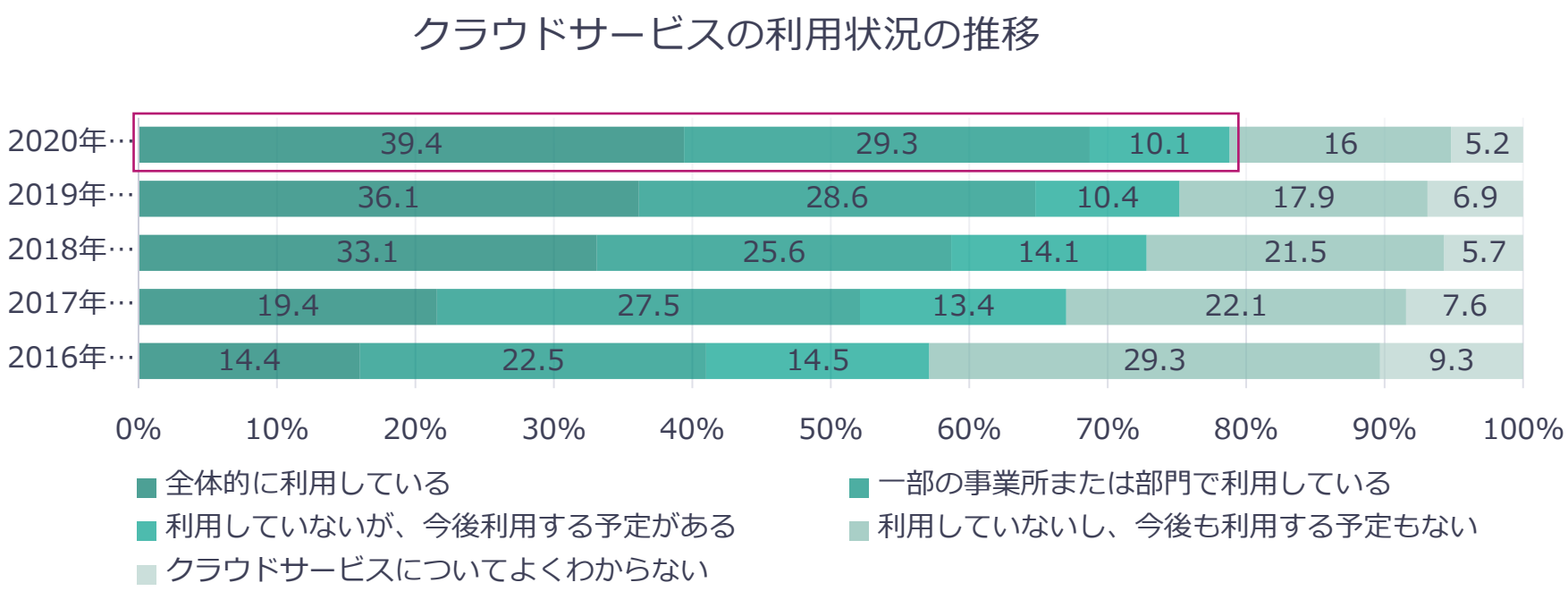
2024/04/18

Canon
キヤノンマーケティングジャパン株式会社

目次

市場背景

- 市場全体でオンプレミスシステムからクラウドサービスへの移行が加速しています
- 特にメール環境は、昨今のテレワーク需要の拡大に伴い、どのような環境からでもアクセスできるMicrosoft 365やGoogle Workspaceなどのサービス利用が急激に増えています



総務省「令和3年版 情報通信白書」を元に作成　https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/html/nd242140.html

市場背景

- セキュリティ脅威の侵入経路としてメールが利用されることは一般的に知られていますが、昨今では従来の仕組みのアンチウイルス・アンチスパムでは検知できない様々な手法が広まっています
- これらの脅威はMicrosoft 365の標準のセキュリティでは防御しきれない場合も多く、年間で約2570万件超の脅威のすり抜けが確認されています

ビジネスメール詐欺 (BEC)

①Microsoft 365偽ログイン画面に誘導しID/PWDを窃取する
②メールを盗み見し、通常業務そっくりの振込依頼を送付し、現金を引き出す

送金

ランサムウェア

①関係者を装うメールでクリックを誘う
②不正なファイルやURLを使いランサムウェアでPC内のファイルを暗号化する

身代金

標的型サイバー攻撃

①関係者を装うメールでクリックを誘う
②開封後、ボットを侵入させ、次回以降の司令を出す

情報窃取

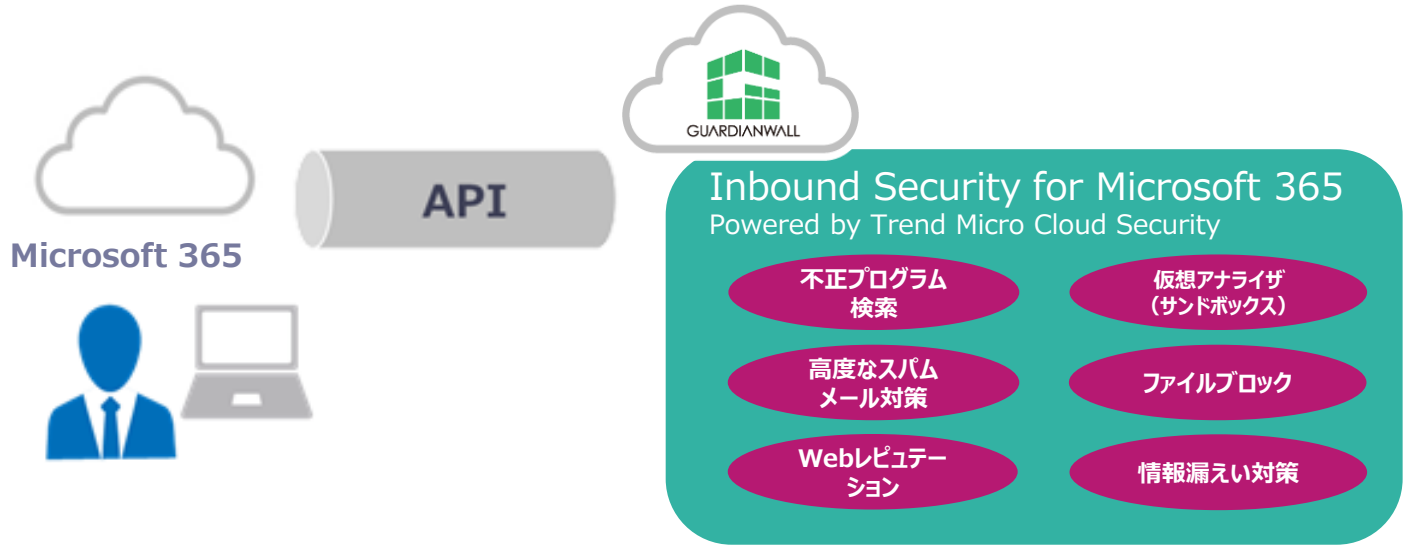
約2570万件
のすり抜け！

※2021年で、Microsoft 365をすり抜けてTrend Micro Cloud App Securityで検知された高度な脅威

出典：m449-2021年年間セキュリティラウンドアップ.pdf

Inbound Security for Microsoft 365とは

- トレンドマイクロ株式会社のクラウドアプリケーション向けセキュリティサービス「Trend Micro Cloud App Security」を活用した、外部からのセキュリティ脅威を防ぐサービスです
- メールだけでなくストレージも保護が可能で、オンラインストレージへ危険なファイルをアップロードしたとしても隔離や削除などの保護対策を実施し、感染の拡大を防ぎます
- Inbound Security for Microsoft 365は以下のサービスに対応しています
  Exchange Online/SharePoint Online/OneDrive for Business
  Box/Dropbox/Google Workspace(Google ドライブ/Gmail)/Microsoft Teams



Inbound Security for Microsoft 365とは

- Inbound Security for Microsoft 365は、以下のようなことにお困りのお客様にお勧めです

- Microsoft 365の標準のセキュリティ機能に不足、不安を感じている
- なるべく手間なくセキュリティを強化したい
- BEC（ビジネスメール詐欺）対策を行いたい
- サンドボックス機能を利用したい
- パスワード付きファイルは受け取りたくない（PPAP対策）
- メールサービスだけではなく、ストレージサービスにもセキュリティ対策を行いたい

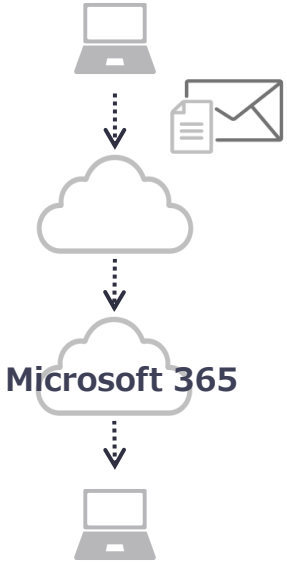
ユーザー規模や業種に関わりなく、どのお客様にもご利用いただけます

ポイント

1. 導入が容易
2. 運用が容易
3. 高度なセキュリティ対策を実現

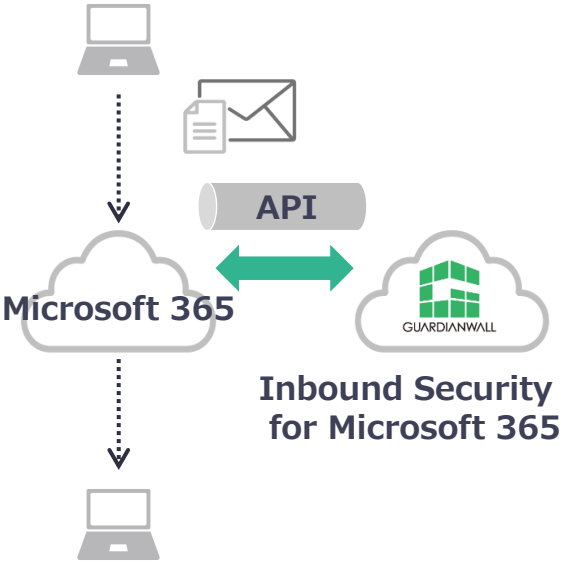
1.導入が容易

- Inbound Security for Microsoft 365はクラウド上に構築されており、Microsoft 365とAPIでやり取りを行うことにより動作します
- メール通信の経路を変えるなどの既存の環境を変更する必要がないため、管理者および利用者に負担なく、簡単に導入することが可能です



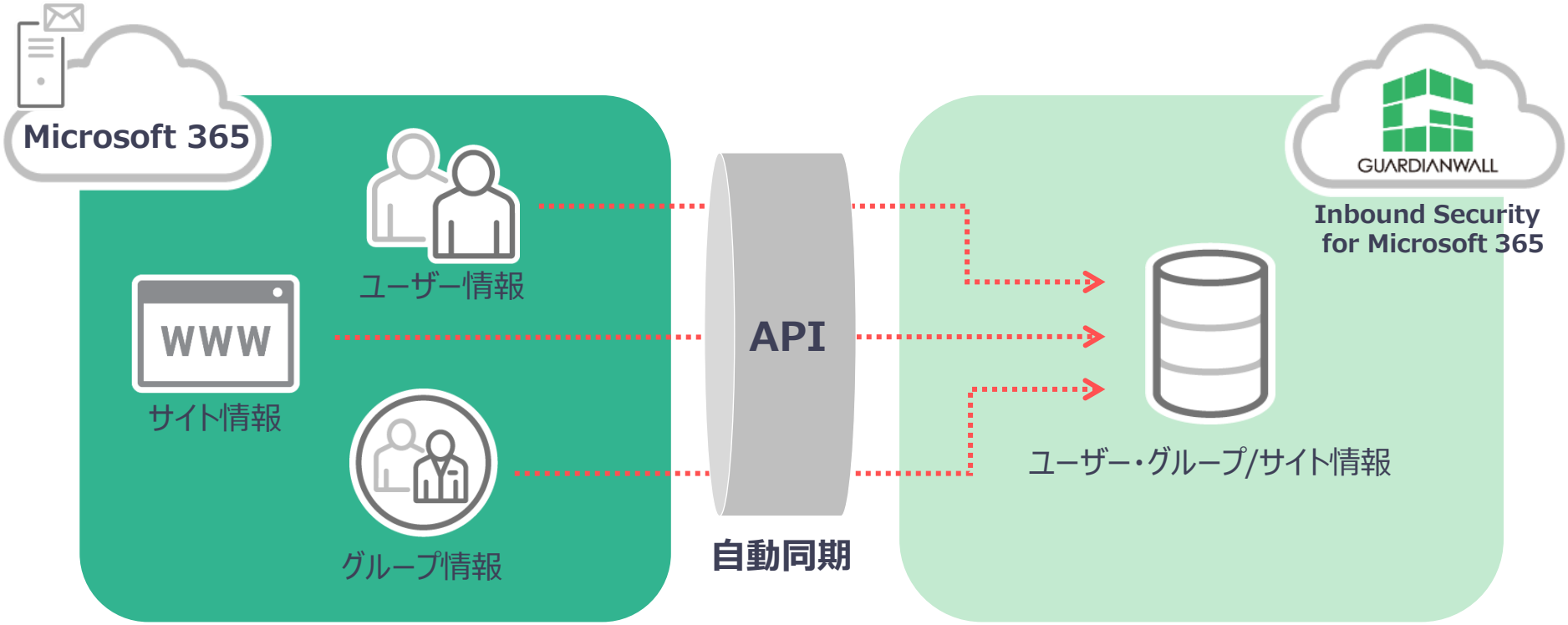
ゲートウェイ型 VS API型

必要あり	MX書き換え,SPF追記など	必要なし
メール配送停止の可能性あり	万一の障害発生時	メール配送停止なし
×	社内メールのスキャン	○
×	SharePointやOneDriveへの対応	○



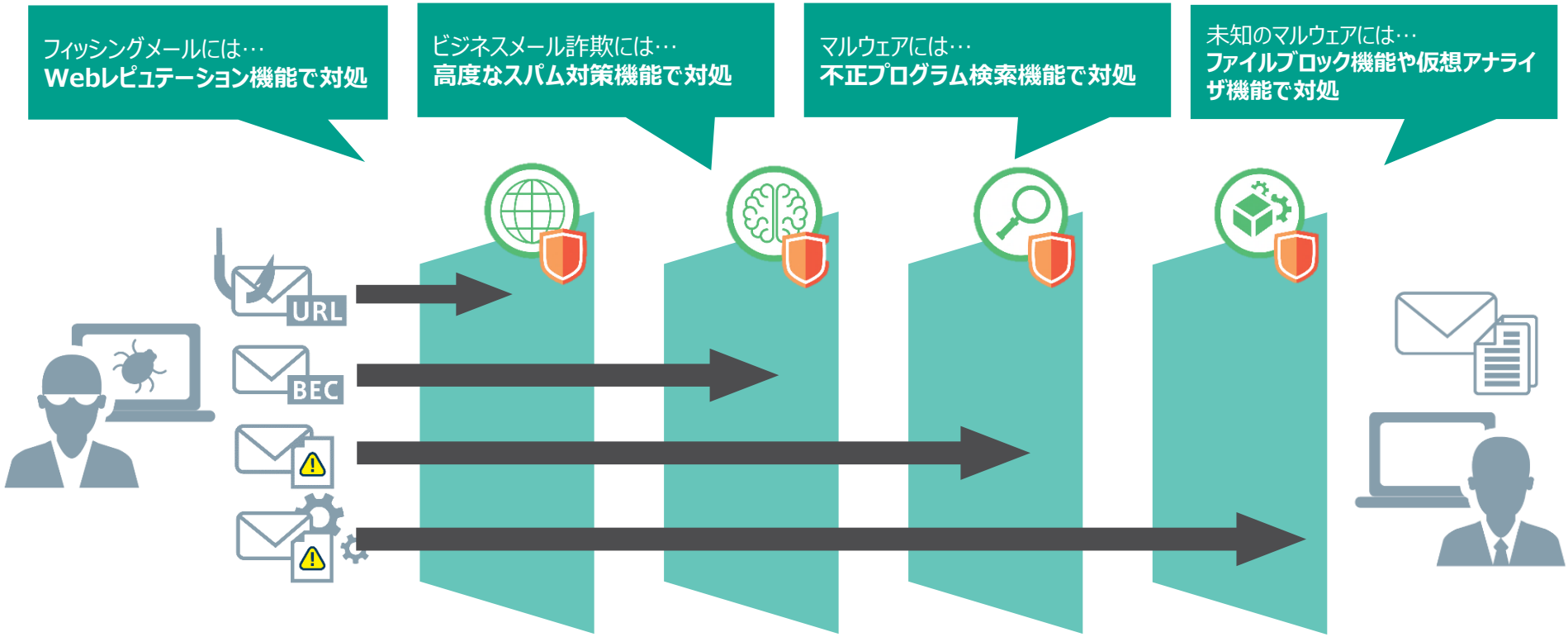
2.運用が容易

- API連携により、Microsoft 365のユーザーおよびグループ情報を自動で取得することで、システム管理者の日々の運用負担を軽減します
- セキュリティを有効にする対象(ユーザーやグループ)を絞ることで、例えば"特定部門のみテスト導入する"などのスモールスタートを行うことも可能です



3.高度なセキュリティ対策を実現

- 攻撃者は攻撃を実施する際に、様々な手法で攻撃メールを送付します。今日のセキュリティ対策には多様な攻撃手法に応じた多層防御が必要です
- Inbound Security for Microsoft 365では様々な機能で攻撃メールから利用者を多角的に防御します



各種機能の紹介

1. 高度なスパムメール対策機能
2. 不正プログラム検索機能
3. ファイルブロック機能
4. Webレピュテーション機能
5. 情報漏えい対策機能
6. 仮想アナライザ機能

1.高度なスパムメール対策機能

【機能概要】
高度なスパムメール対策機能は、メール本文の検査を行い、ビジネスメール詐欺 (BEC)・ランサムウェア・フィッシング・およびその他のスパムメールを検出します　スパムメールを検出した際に、件名にタグを挿入する・迷惑メールフォルダに移動する・隔離するなど運用に合わせて処理を任意に選択することが可能です

【効果・メリット】
この機能により、大量のスパムメールによる業務効率の低下や、ビジネスメール詐欺の被害にあう可能性を低減します

ピックアップ機能
【表示名のなりすましの検出】
メールアドレスの表示名の部分を社内に実在する人間のものに偽装して送付されるメールに対して、
Inbound Security for Microsoft 365では社内のメールアドレス情報との突合せを実施し検疫、組織内で使用している表示名に類似しているものが外部から送信された場合に既定の処理を実行します
メールのなりすまし攻撃に対して効果を発揮します

2.不正プログラム検索機能

【機能概要】
不正プログラム検索機能は、メールに添付されるファイルやオンラインストレージにアップロードされるファイルの検査を行い、マルウェアが含まれていた場合にそれらを駆除、またはメールやファイルを隔離します
パターンファイルによる検索やヒューリスティック分析などの従来の技術に加え、機械学習型検索を併せて利用することで未知の脅威に対しても素早く対応することが可能です

【効果・メリット】
この機能により、マルウェアの侵入および感染による被害を未然に防ぎます

ピックアップ機能
【ZIP暗号化されたファイルの検疫機能】
通常、ZIP暗号化されたファイルは中身を確認することができないため検査を実施できませんが、
Inbound Security for Microsoft 365ではZIP暗号化されたファイルを当該メールの本文にパスワードが記載されている場合に限り、復号化して中身を検疫することが可能です 当該機能は不正プログラム検索機能を有効にすることでデフォルトで使用可能です
Emotetなどの、ウイルスをZIP暗号化して検疫をすり抜けようとするパターンの脅威に効果を発揮します

【アクティブコンテンツのサニタイジング機能】
Microsoft Officeファイルのマクロなどを除去して配送することが可能です(Exchange Onlineのみ)
マクロを悪用してウイルスをダウンロードさせるパターンの脅威に効果を発揮します

3.ファイルブロック機能

【機能概要】

ファイルブロック機能は、特定のファイルタイプを指定し、当該拡張子のファイルが添付されているメールの受信やオンラインストレージへのアップロードをブロックします

【効果・メリット】

この機能により、マルウェアの侵入および感染による被害を未然に防ぎます

ピックアップ機能

【テキストファイル置換】

ファイルブロック機能では既定したファイルタイプに合致するファイルを削除し、代替のテキストファイルに置き換える処理を実施することが可能です

PPAP対策などでZIPファイルの受け取りをすべて拒否したいが、本文は確認できるようにしたいなどの運用を検討している場合に効果を発揮します

4.Webレピュテーション機能

【機能概要】
Webレピュテーション機能は、メール本文や添付ファイル内に含まれるURLの検査を行い、不審なURLが含まれていた場合メールを削除、または隔離を実施します
クラウド上に存在する世界中の脅威情報を集約するデータベースを参照することで不審URLを判定します

【効果・メリット】
この機能により、URLのクリックで感染する標的型メール等への対策を強化することができます

ピックアップ機能
【Time-of-Clickプロテクション機能】
受信メールメッセージに含まれるURLをあらかじめInbound Security for Microsoft 365が指定するURLに書き換えておくことで、ユーザにより当該URLがクリックされたタイミングでその時点で最新のデータベースを参照、問題があればアクセスをブロックします
事後的に脅威が発覚した場合など、ゼロデイ攻撃に効果を発揮します

5.情報漏えい対策機能

【機能概要】

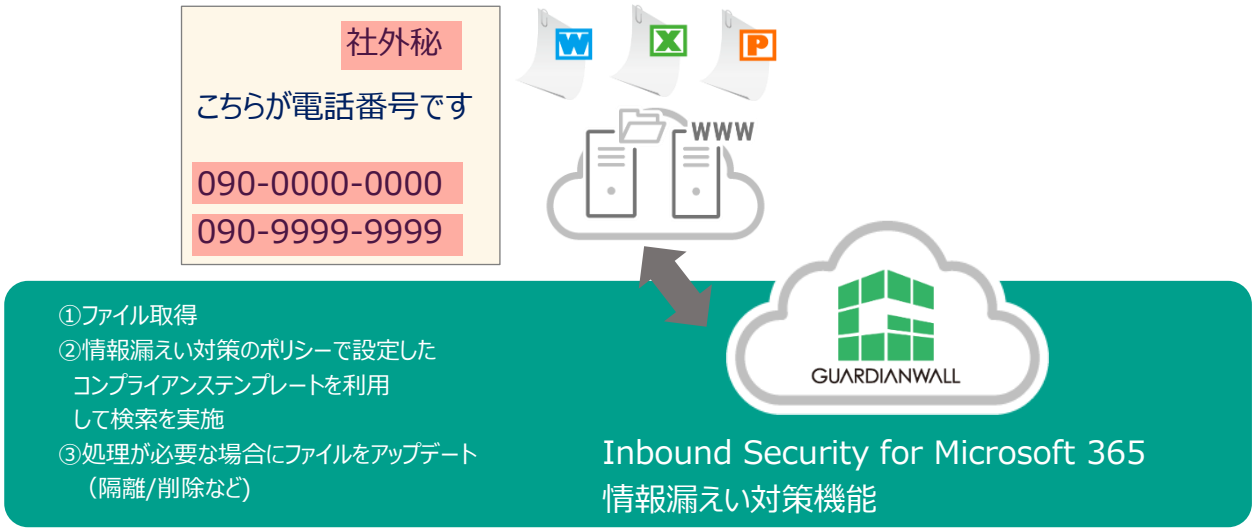
情報漏えい対策機能は、ファイル内の文章の検査を行い、あらかじめ規定した条件に一致したファイルのオンラインストレージへのアップロードなどをブロックすることができます

200以上の事前定義済みのコンプライアンステンプレートが用意されており、クレジットカード番号/個人情報/マイナンバーなどの検出を行うことが可能です

【効果・メリット】

この機能により、機密情報の漏えい等を未然に防ぎます

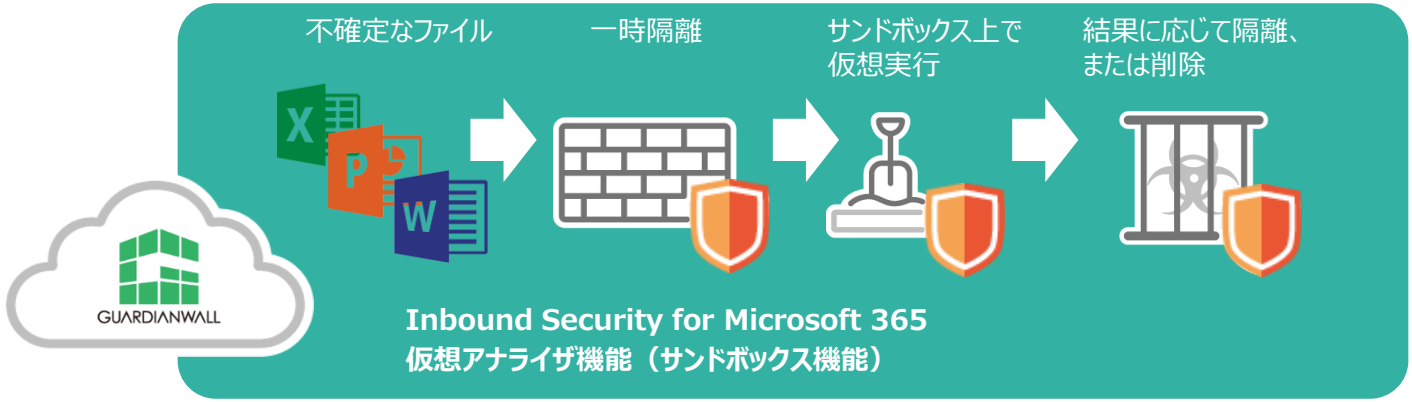
※メールに添付されたファイルにも検査は実施可能ですが、送信をブロックすることはできません



6.仮想アナライザ機能

【機能概要】
仮想アナライザ機能（サンドボックス機能）は、仮想OS上でファイルを実行させることにより挙動を確認する技術です
この技術を用いて検体解析することにより、未知のウイルスを検出することができます
加えて、Inbound Security for Microsoft 365ではフィッシングサイトへの対策強化として、画像解析とAIによるスキャン、動的なURL検索という2つの機能を実装しています

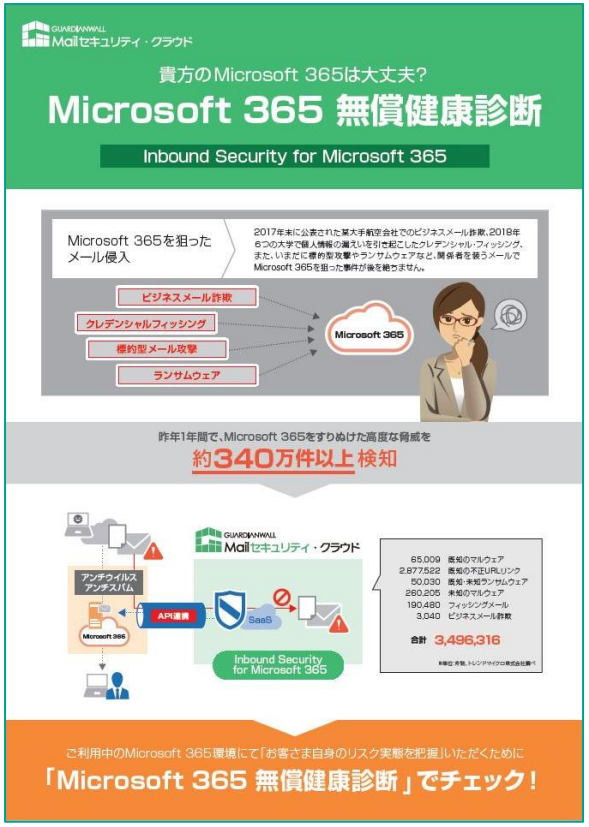
【効果・メリット】
この機能により、より強固に未知の脅威やフィッシングサイトに対応します

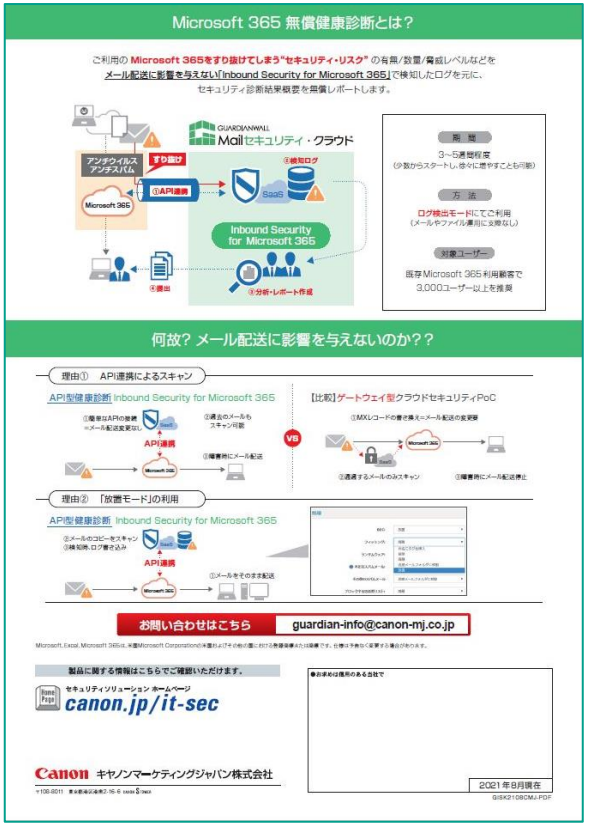


ピックアップ機能
【動的なURL検索】
フィッシングサイトのURLなどは日々新しいものに更新されており、脅威データベースへの登録が間に合わないケースがあります
Inbound Security for Microsoft 365では、DB検索の他、URLをリアルタイムにクロールしWebサイトに不正なパターンが含まれていないかなどを検疫します
最新の不正サイトを用いたゼロデイ攻撃や、速いスピードで亜種を展開するマルウェアなどに対して効果を発揮します

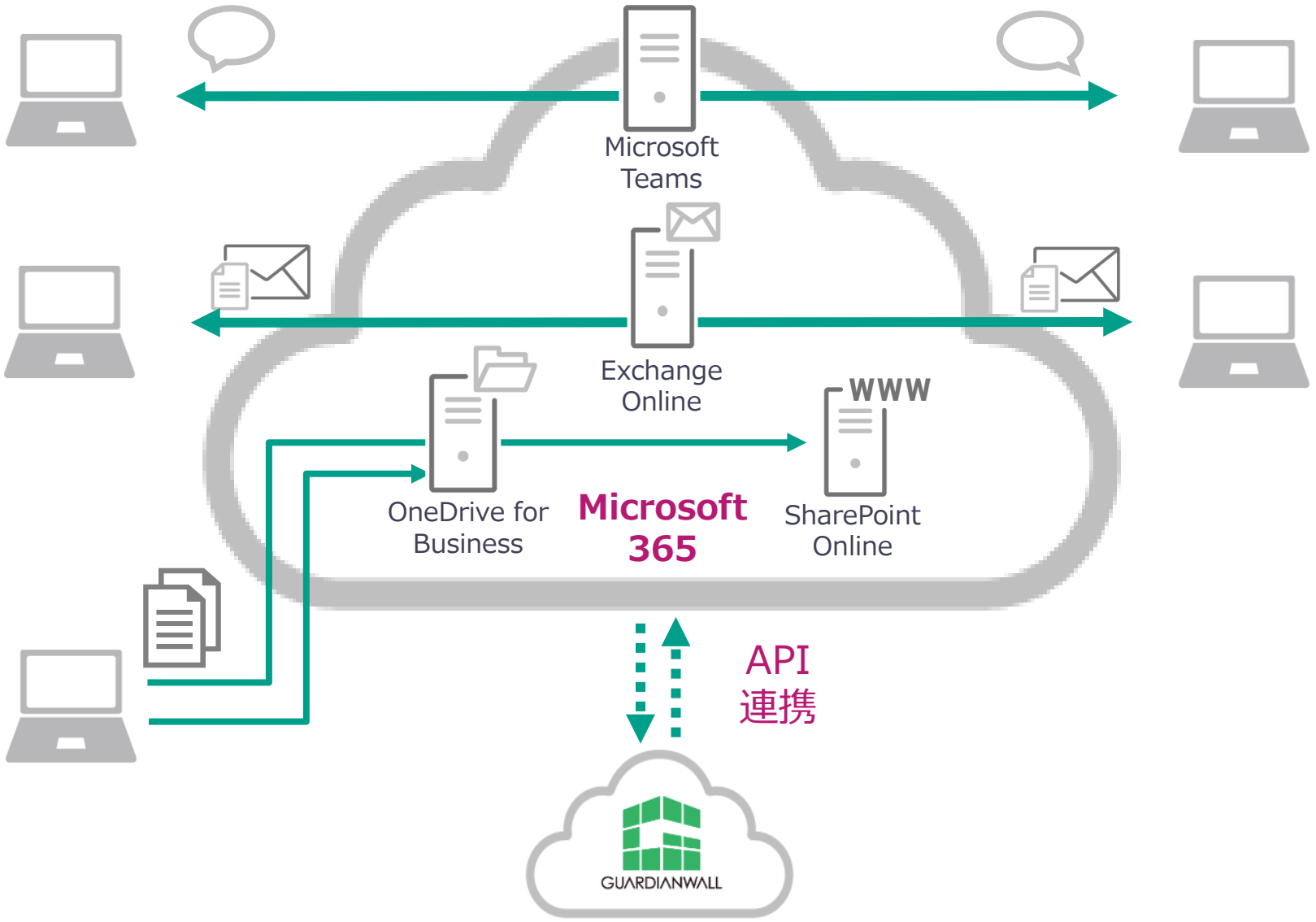
無償健康診断

- 評価版ライセンスを適用、ご利用いただくことでご利用中の脅威の検知状況を可視化し、レポートで提出させていただきます
- 詳しくは以下のチラシをご参照ください





構成イメージ（Microsoft 365の場合）



Inbound Security for Microsoft 365

サービス開始までの流れ

Step1

申込書記入

「Inbound Security for Microsoft 365申込書」に記入し、ご送付ください

5営業日以内に「登録完了通知」が送信されます

Step2

初期設定

「スタートアップガイド」を参照し、初期設定を実施してください

Step3

ご利用開始

「セキュリティ設定設計補助資料」を参照し、必要に応じて設定をチューニングしてください

※“無償健康診断”実施時も同様の流れとなります。

サービス詳細

お申し込みからご利用開始まで	約1週間（要件により異なります）
最低契約ライセンス数	5ライセンス
追加購入時の最低契約ライセンス数	5ライセンス
ライセンスの課金対象	ユーザー数
最低利用期間	1年間
契約開始日	サービス利用開始日の月初1日

※契約期間中の追加ライセンス数が5に満たない場合は、追加費用は発生しません
※複数のクラウドアプリケーションでご利用される場合のライセンスの課金対象は本サービスをご利用いただいているユーザーの総数になります
※加入後、1 年未満で解約される場合は、1 年に満たない期間分の費用を申し受けます
※月額費用の日割り換算はいたしません。月中でのご利用開始の場合も1か月分の月額費用を申し受けます

他GUARDIANWALL製品との組み合わせ

- Inbound Security for Microsoft 365と他のGUARDIANWALL Mailセキュリティ・クラウドの製品群を組み合わせて利用することももちろん可能です
- GUARDIANWALL Mailセキュリティ・クラウドを併用することで
  Inbound Security for Microsoft 365では対処できない送信メールに関する
  フィルタリングを強固に実施することができます

対策	必要な機能概要	Microsoft 365 E1プラン	IS365	GUARDIANWALL Mailセキュリティ・クラウド	IS365とGWMSCを組み合わせて利用すると…
受信メール対策	アンチウイルスやアンチスパムなど	△	○	△	◎
	サンドボックスや添付ファイルURL無害化など	×	○	△	◯
送信メール対策	DLP,ZIP暗号化,上司承認など	△	×	○	◯
その他	ファイルブロック,ポリシー設定など	×	○	○	◎
アーカイブ	アーカイブ実施およびアーカイブ内容の検索など	△	×	○	◯

導入環境

Inbound Security for Microsoft 365が対応するクラウドアプリケーションは以下の通りです

対象アプリケーション	説明
Microsoft 365 ビジネスプラン (ビジネス、エンタープライズ両プランが含まれています)	• Exchange Online • SharePoint Online • OneDrive for Business • Microsoft Teams 以下のプランもサポート対象となります • Microsoft 365 教育機関向けプラン • Microsoft 365 非営利団体向けプラン
各種ストレージサービス	• Box ビジネスプラン：ビジネス、エンタープライズ両プランが含まれます • Dropbox ビジネスプラン
その他サービス	• Google Workspaceプラン：本プランで提供されるGoogle ドライブ、Gmailが対象となります

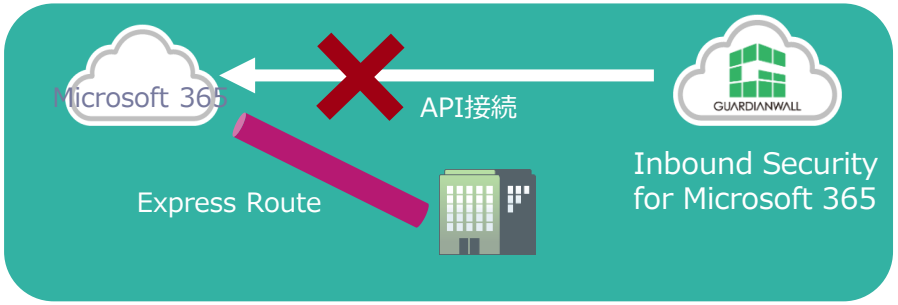
管理コンソールの利用環境は以下の通りです

利用環境	説明
Webブラウザ (Inbound Security for Microsoft 365の管理コンソールアクセス用)	Inbound Security for Microsoft 365では、次のWebブラウザの最新バージョンがサポートされます • Google Chrome • Mozilla Firefox • Microsoft Edge

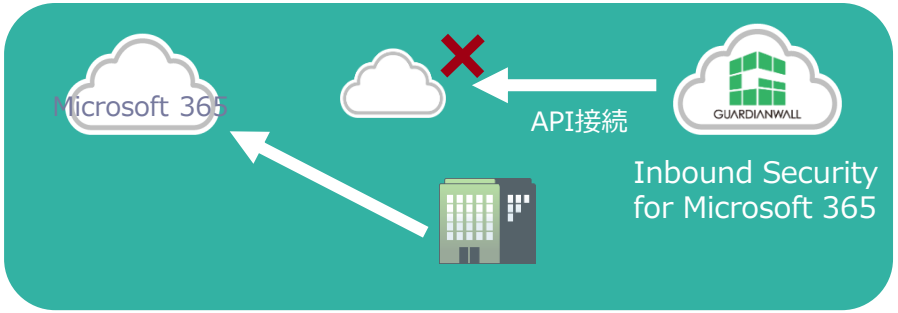
※最新のシステム要件はトレンドマイクロ株式会社の製品ホームページをご確認ください
https://www.trendmicro.com/ja_jp/business/products/user-protection/sps/email-and-collaboration/cloud-app-security.html

ご利用時の注意点

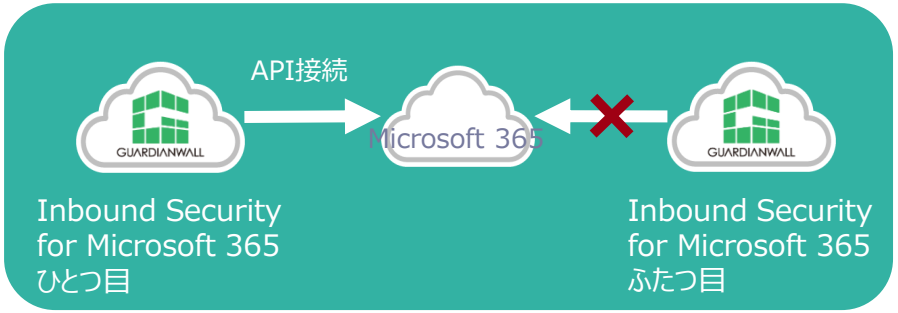
- Microsoft 365への接続にExpress Routeなどの
  専用線サービスをご利用されている場合、
  インターネットを介したAPI接続ができないため、
  本サービスをご利用いただけません



- サードパーティ製のサービスや製品にて
  Microsoft 365への接続にIPアドレス制限
  などをかけている場合、API接続ができないため、
  本サービスをご利用いただくことができない
  場合がございます 詳細はお問い合わせください



- Inbound Security for Microsoft 365は
  Microsoft 365のテナントに対して一対一で紐づきます
  複数Inbound Security for Microsoft 365を
  同一のMicrosoft365テナントに紐づけて
  利用することはできません



製品に関するお問い合わせ

GUARDIANWALLシリーズ
「Inbound Security for Microsoft 365」に関するお問合せは、
以下のあて先へ

キヤノンマーケティングジャパン株式会社

セキュリティソリューション企画本部

guardian-info@canon-mj.co.jp

Appendix:脅威検出時の処理

- Inbound Security for Microsoft 365の各種セキュリティ機能で検出されたメールやファイルに対して、下記の処理を行うことができます
  実施可能な処理はセキュリティ機能によって異なります
- 不正プログラム対策の処理に関しては、「トレンドマイクロの推奨処理」設定により自動的に判断して処理を行うことも可能です　検出された場合はログが記録されます

検索方法	メールサービス	クラウドアプリケーション
放置	変更処理を実施しない	変更処理を実施しない
隔離	ユーザがメールを閲覧できないよう 隠しフォルダへ移動	ファイルをテキストファイルで置換
削除	メールメッセージ全体を削除	ファイルをテキストファイルで置換
テキスト/ファイルで置換	添付ファイルをテキストファイルで置換	なし
件名にタグを挿入	件名の前に任意のキーワードを追加	なし
迷惑メールフォルダに移動	迷惑メールフォルダに移動	なし

※1つのメール/ファイルに対して、複数の機能で検知があった場合は以下の順で処理が実施されます。
削除 > 隔離 > 迷惑メールフォルダに移動 > テキスト/ファイルで置換 > 件名にタグを挿入 > 放置