GUARDIANWALL
Inbound Security for Mail Gateway
製品紹介資料

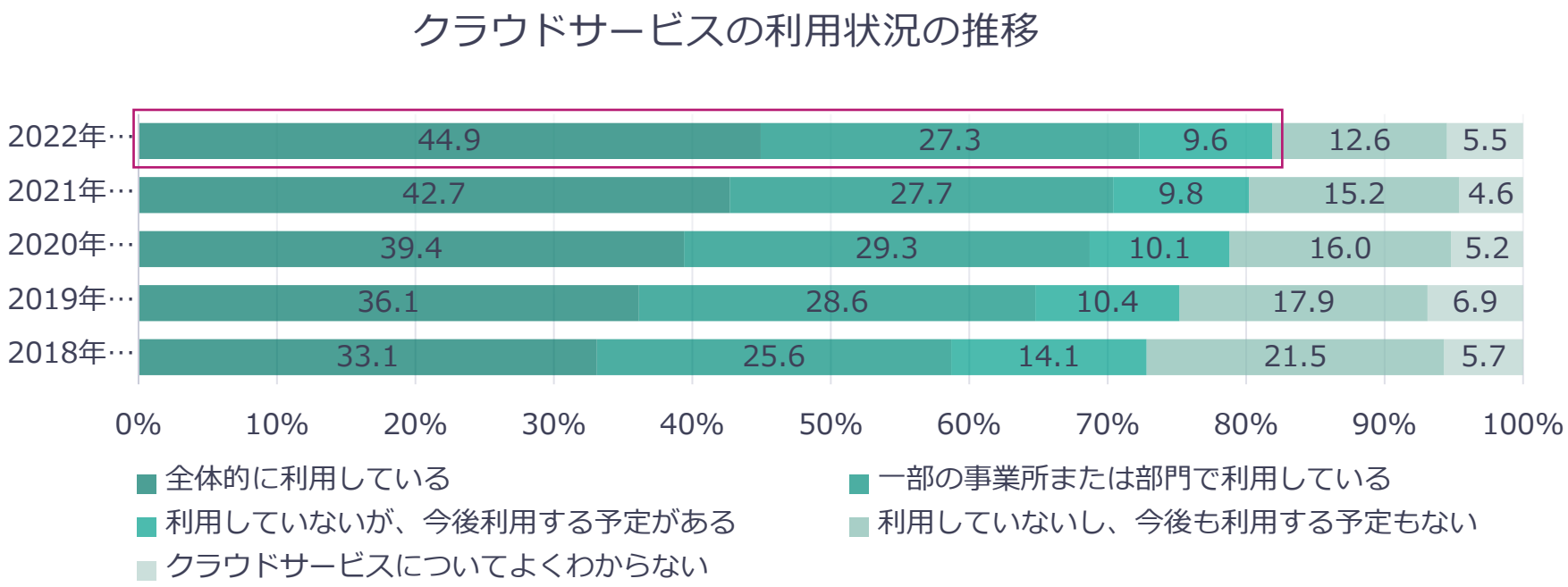
2023/11/30

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

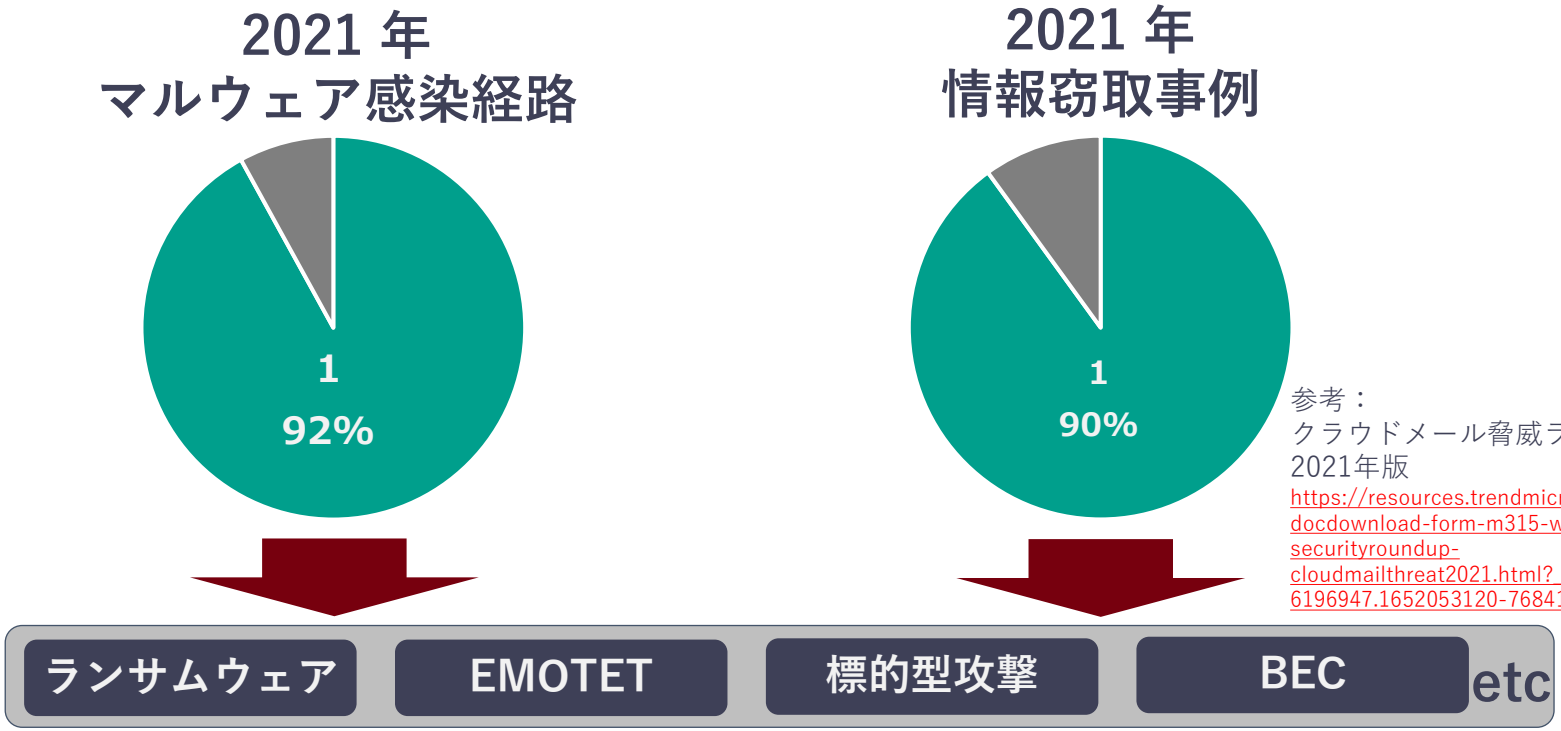
- 市場全体でオンプレミスシステムからクラウドサービスへの移行が加速しています
- 特にメール環境は、昨今のテレワーク需要の拡大に伴い、どのような環境からでもアクセスできるMicrosoft 365やGoogle Workspaceなどのサービス利用が急激に増えています



出典：「令和５年版情報通信白書」（総務省） https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00250

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
- メールからのマルウェア感染は、脅威感染経路の9割を占めております



参考：
クラウドメール脅威ラウンドアップ
2021年版
https://resources.trendmicro.com/jp-docdownload-form-m315-web-bysector-securityroundup-cloudmailthreat2021.html?_ga=2.254585167.696196947.1652053120-768413694.1651052489

Inbound Security for Mail Gateway(ISMG)とは

- トレンドマイクロ株式会社のメールセキュリティサービス「Trend Micro Email 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
- クラウドサービスのため、オンプレミスサーバーでのサービスに比べ管理コストが削減でき、脅威対策を常に最新状態に保てるメリットがございます

1

常に最新状態

Inbound Security for Mail Gatewayは弊社がもつ高度なコアテクノロジーを採用し常に最新の状態を維持し　クラウドサンドボックスや機械学習をはじめとした高度な機能を多層にてご提供します。

2

管理コストの削減

Inbound Security for Mail Gatewayは弊社により運営される電子メールセキュリティのため、サーバーやセキュリティ製品を所有する必要がなく、オンプレミスと比べ初期投資やインフラ維持コストの削減に貢献します。

3

利用開始が簡単

お客さまは、自社ドメインを設定、MXレコードを変更するだけでご利用いただけます。

※お客さまのご利用中のメールアドレスを全て設定する必要はありません。
※※

4

帯域の有効利用

Inbound Security for Mail Gateway はお客さまへ届くべきではないメールがフィルタされるので、クリーンなメールがお客さまシステムへ配送されます。故に、社内ネットワークに流れるデータを適正化し、関連するリソースを軽減します。

※お客さま環境あるいは、ポリシーによりその他の設定変更を要する場合があります。
※※お客さまの選択により、エンドユーザーのメールアドレスをInbound Security for Mail Gatewayシステムへ登録しての運用も可能です。

Inbound Security for Mail Gatewayとは

- Inbound Security for Mail Gatewayは、以下のようなことにお困りのお客さまにお勧めです

- メールセキュリティ環境に不足、不安を感じている
- 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）
- メールサーバーダウン時のバックアップでのメール保持や転送を行いたい
- クラウドサービスでオンプレミスメール環境の対策を行いたい

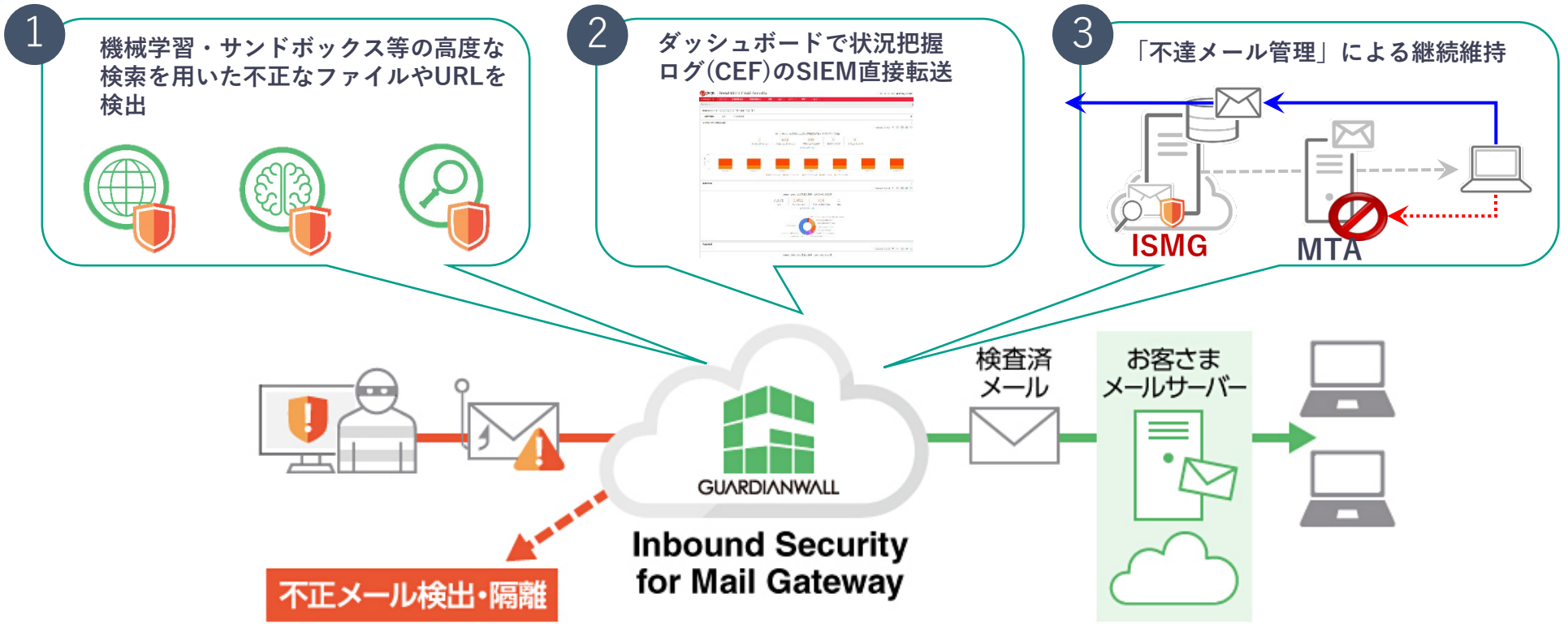
ユーザー規模やクラウド、オンプレミスサーバーに関わりなく、
どのお客さまにもご利用いただけます

ポイント

1. 統合的なメールセキュリティ環境を提供
2. 高度なセキュリティ対策を実現
3. システム管理者の負荷軽減

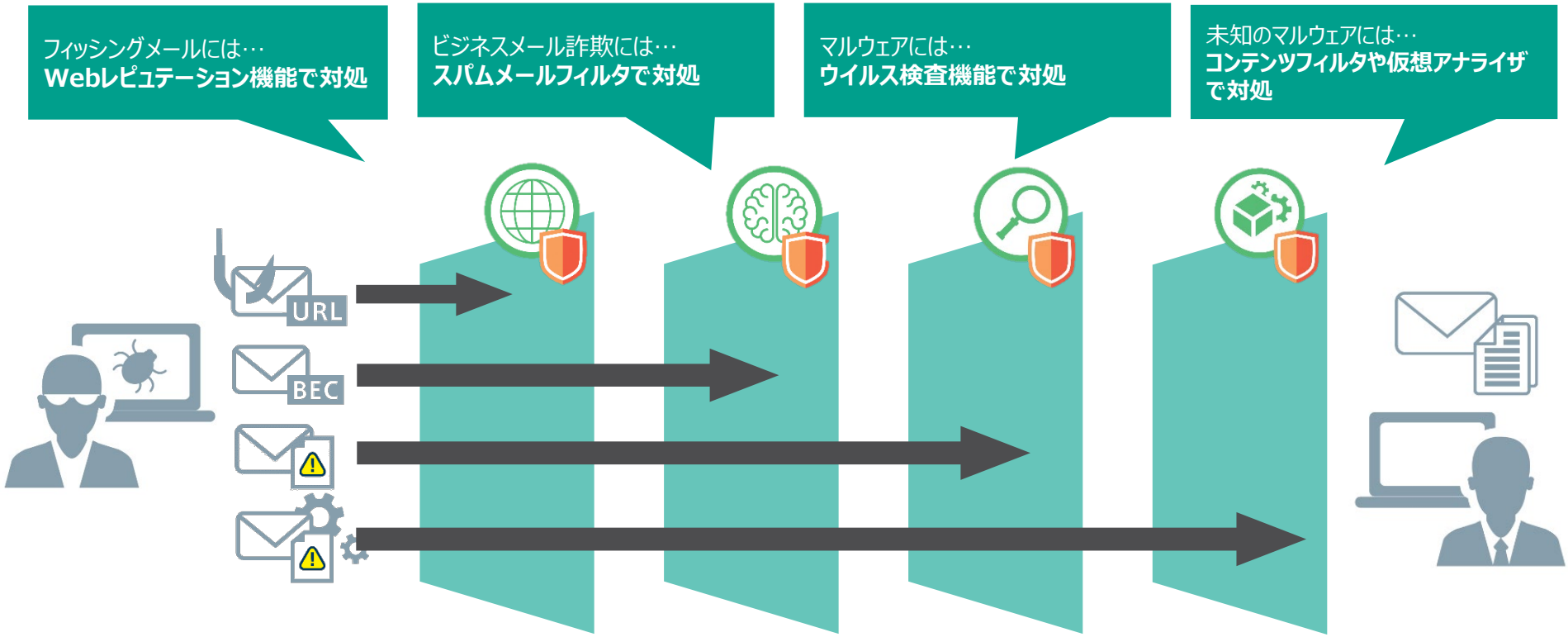
1.統合的なメールセキュリティ環境を提供

- Inbound Security for Mail Gatewayは脅威検査だけでなく、MTAダウン時のメール継続維持や検出状況等をわかりやすく管理できるダッシュボード機能を提供しております



2.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 Mail Gateway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



3.システム管理者の負荷軽減

- Inbound Security for Mail Gatewayでは脅威検出されたメールを、システム管理者による管理と合わせて受信者による管理も可能となっており、低脅威度のメールは受信者により復元、削除をさせ、高脅威度のメールはシステム管理者で管理といった負荷分散による軽減が可能です。

- また、メールサーバー側で障害等により受信が不可となった際にも、最大で10日間メールを保持することができ、メールサーバー側復旧までの間メールロストを避けることが可能です。

各種機能の紹介

1. スパムメールフィルタ
2. ウイルス検索機能
3. コンテンツフィルタ機能
4. 送受信フィルタ機能
5. ドメインベース認証機能
6. 仮想アナライザ機能
7. Webレピュテーション機能

1.スパムメールフィルタ機能

【機能概要】
スパムメールフィルタ機能は、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 Mail Gatewayでは登録したメールアドレス情報との突合せを実施し検疫、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.ウイルス検索機能

【機能概要】
ウイルス検索機能は、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 Mail GatewayではZIP暗号化されたファイルを事前設定したパスワード、もしくはメール受信後に猶予時間を設けてパスワードメールの受信を待ちパスワード解析を行うことが可能です
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
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.コンテンツフィルタ機能

【機能概要】

コンテンツフィルタ機能は、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をブロックします
ファイル拡張子の他にもメールサイズや件名やメール本文、受信者数などでも同様にブロック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

【テキストファイル置換】
ファイルブロック機能では指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.送受信フィルタ機能

【機能概要】
送受信フィルタ機能は、メール受信の際、送信者のメールアドレスを用いて検査前にフィルタをかけることができます
送信者アドレスはエンベロープアドレスに加え、ヘッダアドレスも検査対象とすることができます
また、Inbound Security for Mail Gateway ではメールアドレス、ドメイン以外にも送信元IPアドレスでも同様にホワイトリスト、ブラックリスト登録が可能です

【効果・メリット】
この機能により、信頼性のある送信元と、危険性や受信自体をブロックしたメールを強制的にブロックでき受信するメールの適正化が可能です
承認済み送信者に登録された送信者は、IPレピュテーション、スパムメール、フィッシング、BEC攻撃、ソーシャルエンジニアリング攻撃、Webレピュテーション、グレーメールメッセージフィルタの対象から除外されます。

5.ドメインベース認証機能

【機能概要】
ドメインベース認証機能は、SPFチェックやDKIM認証、DMARCといった認証方法を使用したなりすましを防止する機能です
DKIM、DMARC以外にも、送信者のドメインと送信元IPアドレスを事前に登録しておくことで、
そのドメインとIPアドレスの組み合わせ以外からのなりすましを防ぐ機能もございます

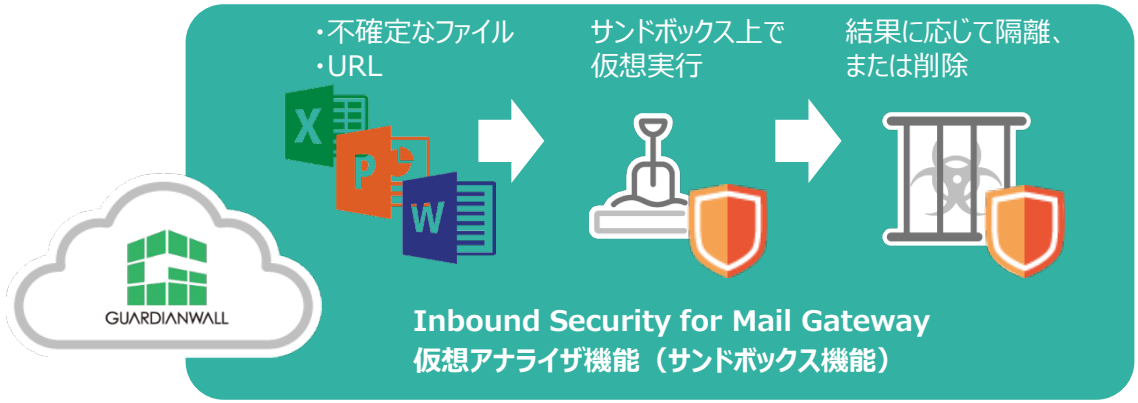
本機能を利用することで、メールの送信元信頼性を確認した上での受信が可能になり、メール環境へ入るメールの健全性が向上します

【効果・メリット】
ビジネスメール詐欺（BEC）におけるニセ請求書や不正な添付ファイルや フィッシングメールでも「関係者になりすまし」た送信者を装うことで、攻撃につなげます。Inbound Security for Mail Gatewayでは、DMARCなどの 送信者ドメイン認証をはじめ、メールヘッダーの精査などを通してなりすましメールを検出することが可能です

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

【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 Mail Gateway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

7.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 Mail Gatewayが指定するURLに書き換えておくことで、ユーザーにより当該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

サービス開始までの流れ

Step1

申込書記入

「Inbound Security for Mail Gateway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

「ユーザー運用ガイド」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

ご評価時も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	10ユーザー
追加購入時の最低契約ライセンス数	10ユーザー
ライセンスの課金対象	メールアカウント数※
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

※メールBOXを持たないメーリングリストのアカウントは課金対象から除外していただいて構いません

導入環境

Inbound Security for Mail Gateway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 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
Google Workspace	• Google Workspaceプラン：本プランで提供されるGmailが対象となります
その他サービス	• 上記サービス以外のSMTP接続が可能なローカル、クラウドベースMTA

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 Mail Gatewayの管理コンソールアクセス用)	Inbound Security for Mail Gateway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 67.0以上 • Mozilla Firefox60.0以上 • Microsoft Edge 91

※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/email-security.html#

ご利用時の注意点

- サービスの仕様により、Mailセキュリティ・クラウドの送信系サービス（MailFilter on Cloud/MailConvert on Cloud/ MailArchive on Cloud 送信）と併用する場合は本サービスの送信保護機能はご利用いただけません。

- 本サービスでは、最大 150 MB のサイズのメールを送受信できます。
  メール送受信サイズを超過した場合、差出人へエラーメール（バウンスメール）を送信します。
  一般に電子メールでは添付ファイルは半角英数字に変換されて送信されます。
  変換方式の 1 つである BASE64 にて変換された場合、添付ファイルのサイズが 1.3 ～ 1.4 倍になりますので
  ご注意ください。

- DoS攻撃やサービス悪用等へのリスク低減のため、下記の通りメール流量制限を設けております。
  ※制限に抵触した場合、一定時間当該IPアドレスやメールアドレスとの通信をブロックします。
  - 送信方向制限
    接続元IPアドレス：5分間に1000通のメールを送信
    送信者メールアドレス(エンベロープ送信者)：10分間に500通のメールを送信
  - 受信方向制限
    接続元IPアドレス：1分間に3600通のメールを受信
    送信者メールアドレス(エンベロープ送信者)：1分間に200通のメールを送信

製品に関するお問い合わせ

GUARDIANWALLシリーズ
「Inbound Security for Mail Gateway」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