脅威の侵入を防ぐための
効率的なメールセキュリティとは？

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

2023年3月29日

Canon

アジェンダ

- **脅威の侵入はすぐそこに？**
  - 情報セキュリティ10大脅威　2023
  - 外部脅威事例
- **脅威の侵入と防御を考えよう**
  - 外部脅威“対策”の考え方
- **GUARDIANWALL Inbound Security for Microsoft 365のご紹介**
  - 製品の特長
  - 製品デモ　～ZIP暗号化ファイルの隔離～
- **まとめ**

脅威の侵入はすぐそこに？

情報セキュリティ10大脅威 2023

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

- ランクインの顔ぶれは大きく変わらず
- 脅威を認識し、適切な対策をとることが重要
- メールを切り口に考えてみると・・・

外部脅威

内部脅威

出典：情報処理推進機構 「情報セキュリティ10大脅威 2023」より引用
（https://www.ipa.go.jp/security/vuln/10threats2023.html）

情報セキュリティ10大脅威 2023

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）	7位
7位	ビジネスメール詐欺による金銭被害	8位
8位	脆弱性対策情報の公開に伴う悪用増加	6位
9位	不注意による情報漏えい等の被害	10位
10位	犯罪のビジネス化 （アンダーグラウンドサービス）	圏外

■攻撃手口

添付ファイルの悪用

URLリンク詐称

なりすまし

巧妙化・高度化

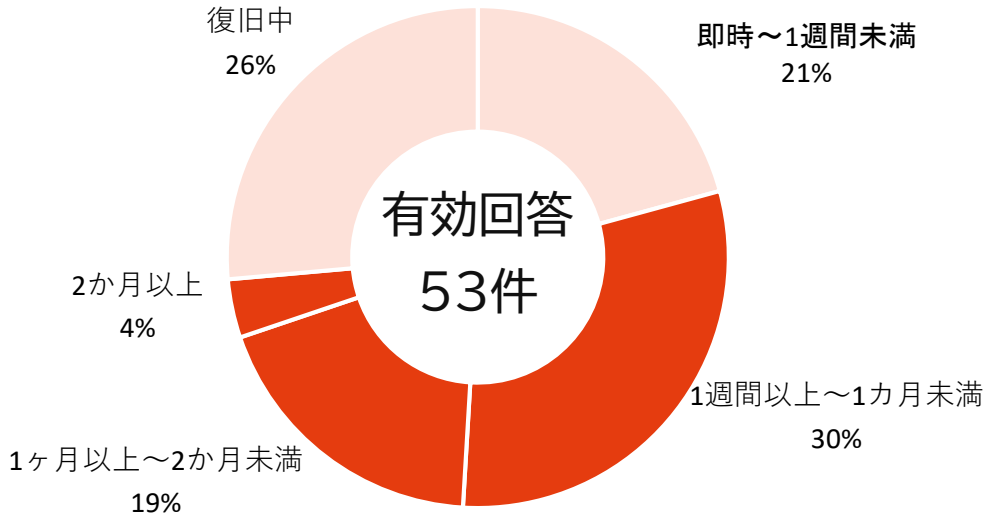
メールからの脅威が引き続き多い

出典：情報処理推進機構 「情報セキュリティ10大脅威 2023」より引用
（https://www.ipa.go.jp/security/vuln/10threats2023.html）

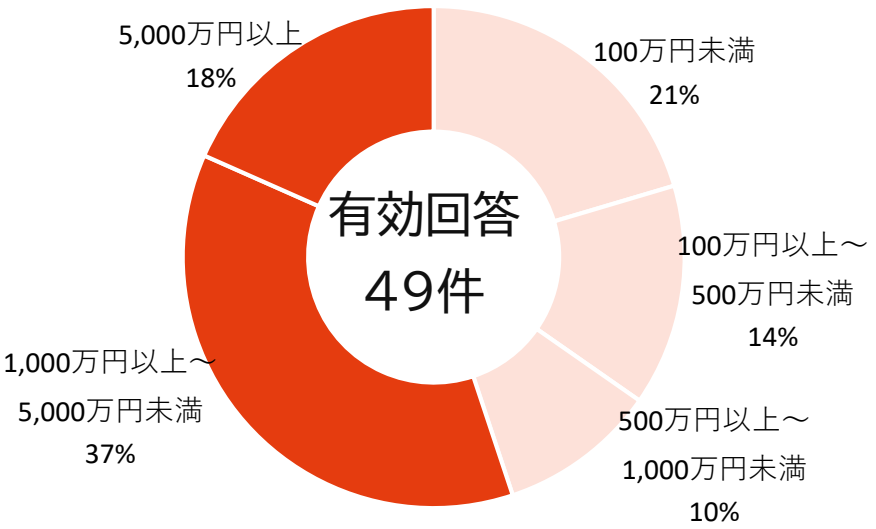
外部脅威事例

■ランサムウェア被害組織が受ける影響

復旧に要した期間



調査・復旧費用の総額



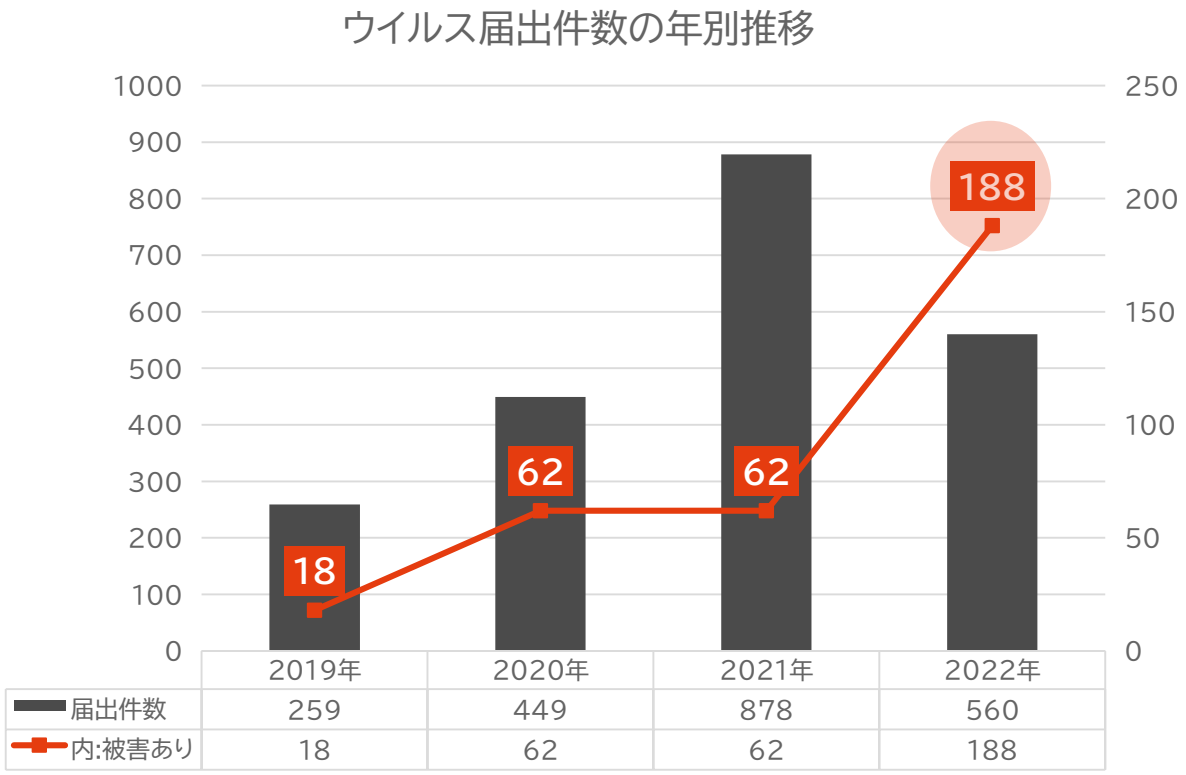
53%が被害から復旧までに1ヶ月以上要した

55%がランサムウェア被害の調査･復旧費用の総額に1,000万円以上要した

出典:警察庁 「令和4年上半期におけるサイバー空間をめぐる脅威の情勢等について」を基に作成
(https://www.npa.go.jp/news/release/2022/20220914001.html)

コンピュータウイルス・不正アクセスの届出状況

■コンピュータウイルス・不正アクセスの届出状況



2022年に被害のあった188件中
Emotet感染が**145件**
ランサムウェア感染が**17件**

Emotetを含め
電子メール
に関連する被害が増大

出典:情報処理推進機構 「コンピュータウイルス・不正アクセスに関する届出」を基に作成
コンピュータウイルス・不正アクセスの届出状況[2022年(1月～12月)]
(https://www.ipa.go.jp/security/outline/todokede-j.html)

Emotetについて

■Emotetの侵入経路としてメールがよく利用されています
侵入を許してしまうと甚大な被害につながりかねません

■Emotetの攻撃手法

メールからの侵入

・なりすまし、偽装
・不正URLからの感染
・Officeファイルに含まれるマクロ
・パスワード付きZIPによる検疫逃れ

PPAPの悪用による被害

探索・情報窃取

・認証情報（ID/パスワード）
・顧客情報・個人情報
・取引内容などの営業機密

■想定される被害

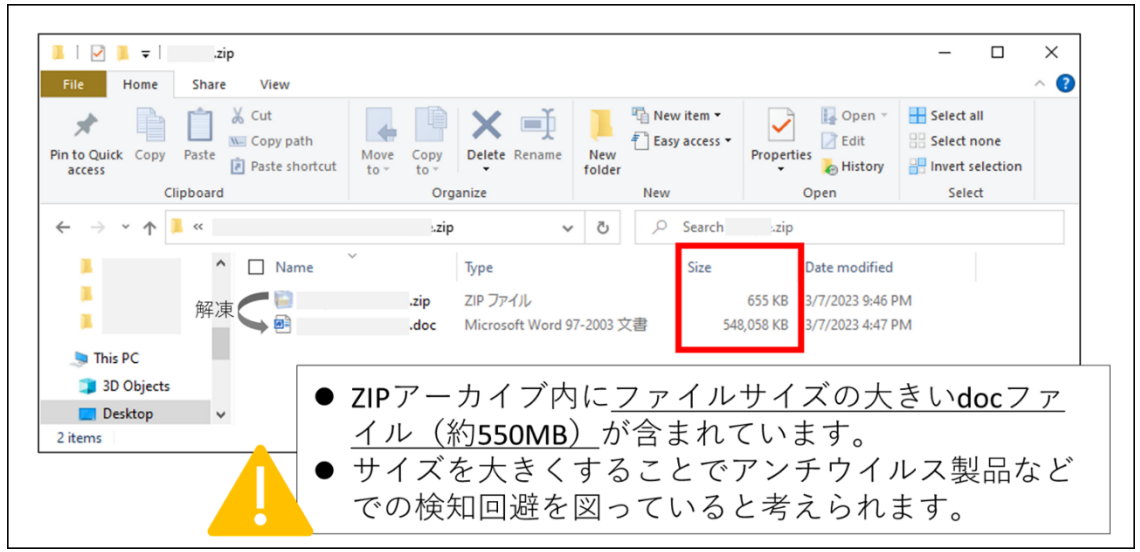
情報漏えい事故
不正アクセス被害
顧客情報・個人情報の漏えい

事業継続が危機に陥る
ランサムウェアによる金銭要求
データ暴露を示唆し脅迫

さらなる攻撃の踏み台に
攻撃メール大量送信
ネットワーク内で感染拡大

最新のEmotet情報

■「高圧縮ファイル爆弾」を利用した攻撃も・・・

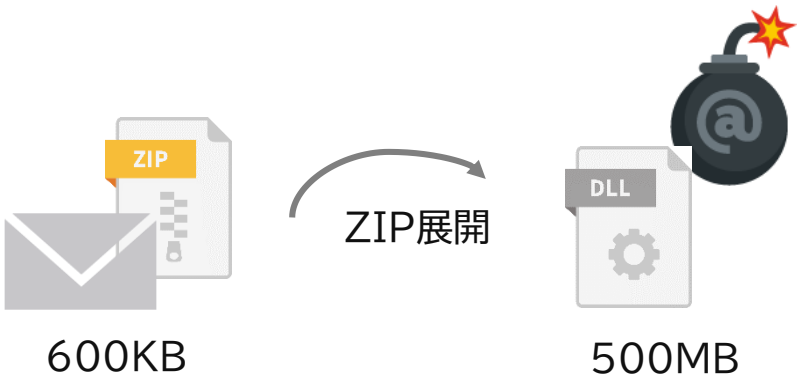


・メールには数百キロバイトのZIPファイルが添付
・展開すると中に約550MB程度のdocファイル
　が含まれている
・docを実行すると、Emotetに感染する恐れ

ウイルス対策ソフトを無効化しすり抜けるためにしばしば
利用されている「ZIP　BOMB」
Emotetの配布手段として確認されています。

高圧縮ファイル爆弾

ZIP BOMB



出典：JPCERTコーディネーションセンター（JPCERT/CC）
マルウェアEmotetの感染再拡大に関する注意喚起
（https://www.jpcert.or.jp/at/2022/at220006.html）

Emotetの影響

■被害者になってしまうと同時に、感染してしまうと拡大の加害者にもなりえます

①ウイルス付き添付ファイル送信　②セキュリティソフトのすり抜け　③組織内情報への侵入　④感染拡大の原因になる

メールを通して侵入してくる外部脅威への対策が必要！

脅威の侵入と防御を考えよう

企業がおこなう外部脅威対策の考え方

A

ポリシー策定

ToDo !

- メール業務の分析
- メール利用規定の策定
- 労務規定への反映
- 有事対応方針の策定

B

利用者教育

ToDo !

- リスク教育
- 利用ガイド
- メールソフトの設定

C

システムでの対策

ToDo !

- ZIP暗号化ファイルの受信拒否
- 不審なURLの検知
- メール無害化
- なりすまし検知

・・・など

システムによる対策

■『社員に対する教育』と『システムによる対策』の双方有効ですが、特に『**システムによる対策**』が重要です

対策例	対策を実現する機能
 パスワード付きZIPを受け取らない	ファイルブロック
 マクロファイルを安全な形で受け取る	不正プログラム検索（サニタイズ）
 なりすまし検知	高度なスパムメール対策
 不審URLが記載されたメールをブロック	Webレピュテーション（不審URL検知）

外部脅威対策のご提案

Inbound Security for Microsoft 365

Inbound Security for Microsoft 365とは

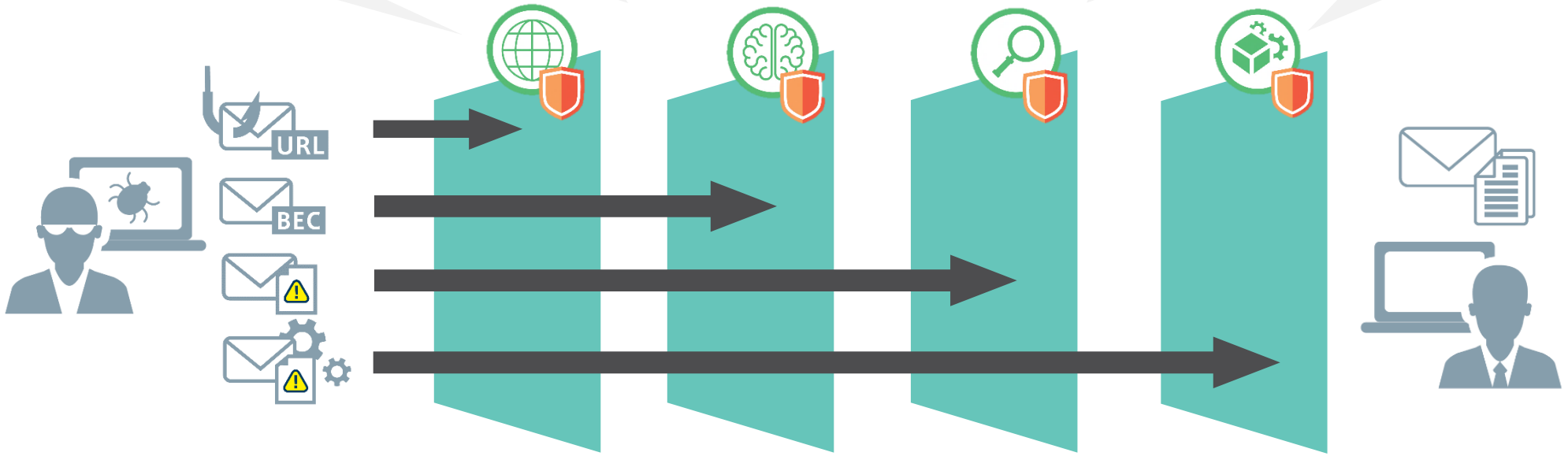
API連携でご利用いただくMicrosoft 365向けセキュリティ対策サービスです

フィッシングメールには…
Webレピュテーション機能で対処

ビジネス詐欺メールには…
高度なスパム対策機能や機械学習機能（なりすまし対策）で対処

マルウェアには…
不正プログラム検索機能で対処

未知のマルウェアには…
ファイルブロック機能や仮想アナライザ機能で対処



不正プログラム検索機能(パスワード解析)

ここがpoint！

注意すべき圧縮ファイルの処理が可能
本文中のパスワードで圧縮ファイルを検査する

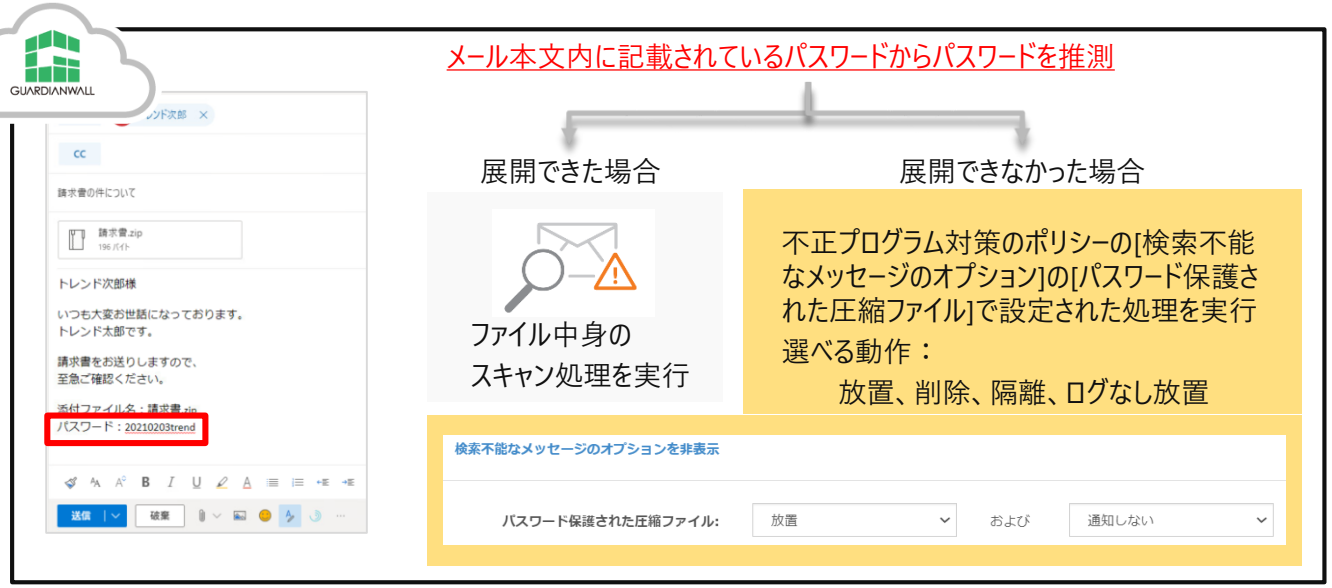
注意すべき圧縮ファイル
- 解凍後のファイル数が最大9999を超えた場合
- 解凍後のファイルサイズが150MBを超えた場合
- 圧縮ファイルが5階層を超える場合

処理方法の設定が可能！

後ほど、デモ

サイバー犯罪者

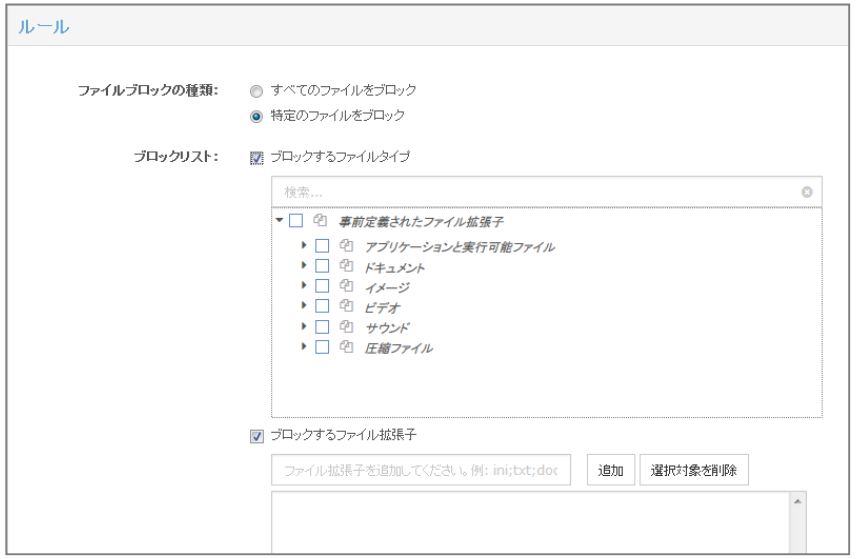
パスワード付き圧縮ファイルを
添付したメールを送信



ファイルブロック機能

ここがpoint！ **パスワード付きZIPを受け取らない**

- 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。
- Emotet対策としてZIPファイルを対象にした場合、受信するメールにZIP形式の添付ファイルがあるとメールを削除、隔離を行うことが可能です



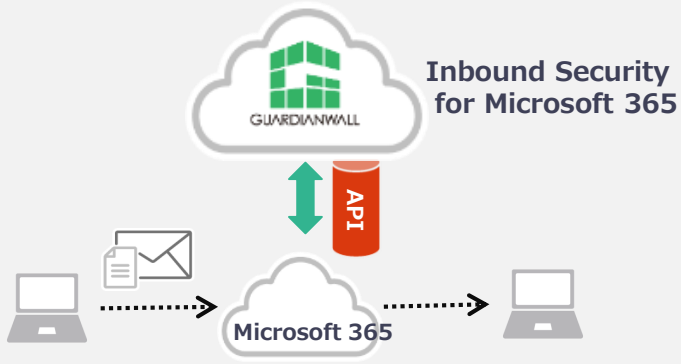
後ほど、デモ

Inbound Security for Microsoft 365の特長

1

API連携

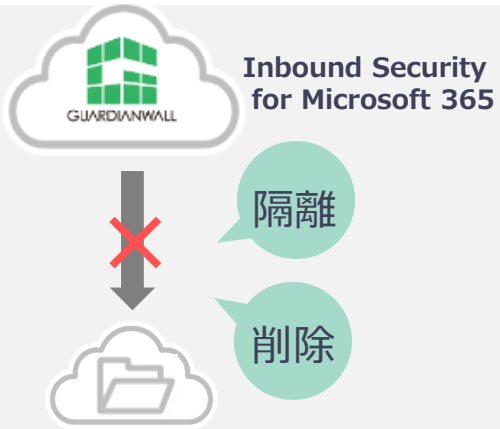
APIでやり取りを行うため、経路変更の
必要がなく、簡単に導入できます



2

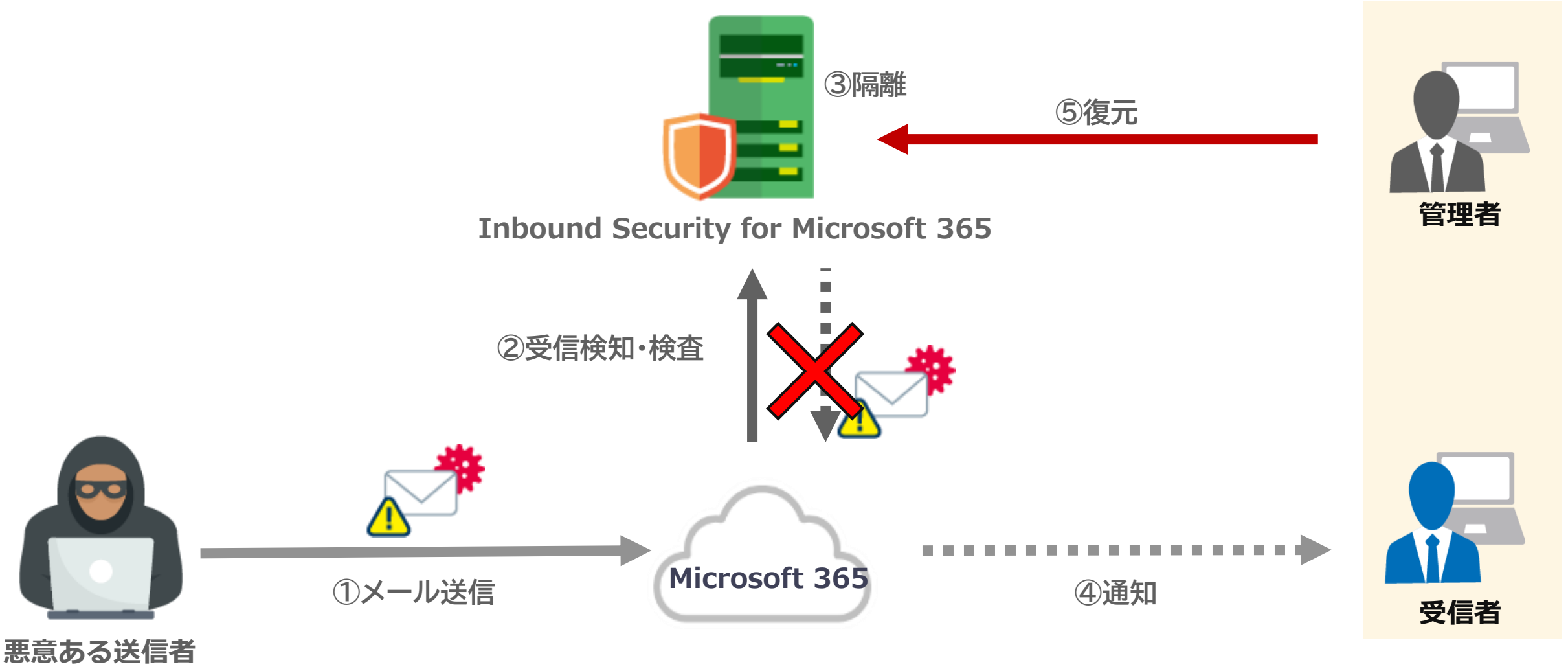
オンライン
ストレージ対応

オンラインストレージへの危険なファイルのアップロードに隔離や
削除などの保護対策を実施し、感染の拡大を防ぎます



ZIPファイルをブロックしてみよう！

デモイメージ


③隔離
⑤復元
管理者
Inbound Security for Microsoft 365
②受信検知・検査
①メール送信
Microsoft 365
④通知
受信者
悪意ある送信者

受信対策デモ

受信対策を実際にご覧ください！

ライセンス体系

月額/ユーザー

¥300

Inbound Security for Microsoft 365

サービス利用料金の特徴

- 初期費用¥0
- 利用料金の月額払い・年一括払いの選択

製品比較

	機能	キヤノンマーケティングジャパン	A社	B社	C社
		IS365	A社製品	B社製品	C社製品
受信メール脅威対策	既知の脅威への対策	○	○	○	○
	未知の脅威への対策	◎	○	△	△ オプション
オンラインストレージ脅威対策	アップロードファイルへの対応	◎	△	○	×
運用管理	管理者の手離れのよさ	○	○	△	△

POINT 01

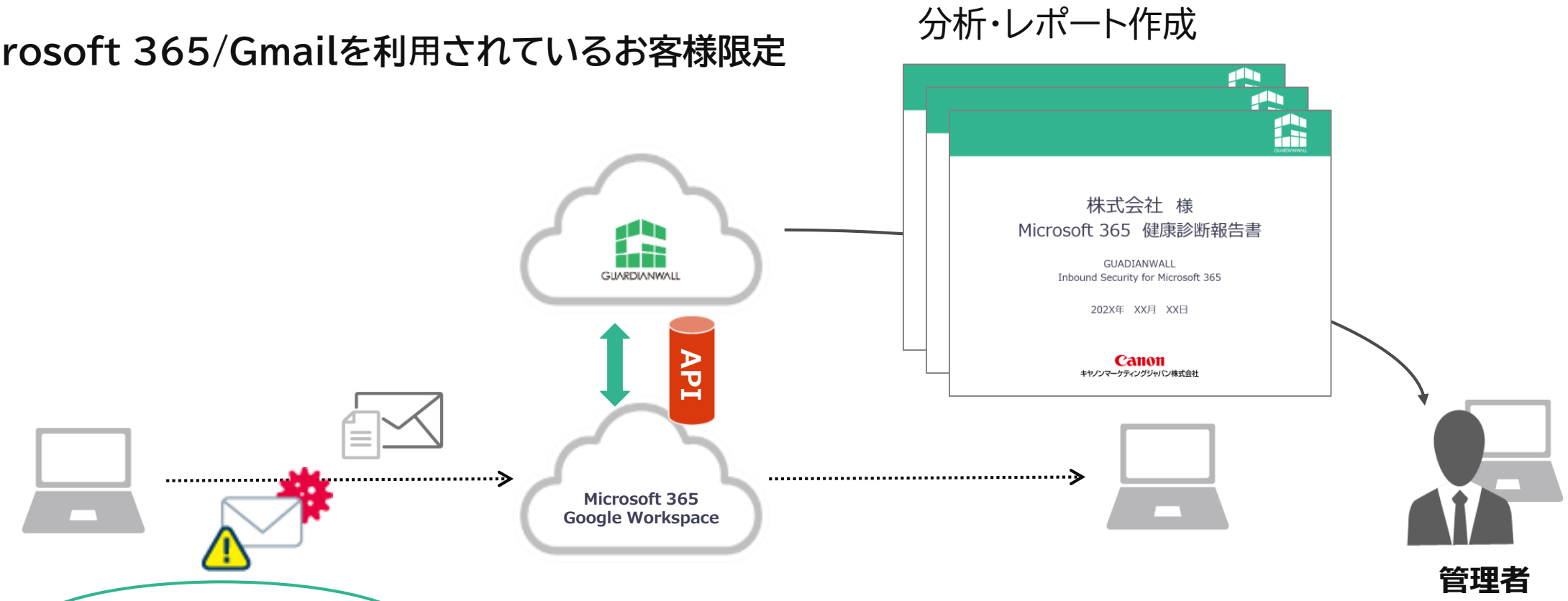
サンドボックス機能など高度な機能も標準搭載！

POINT 02

メールのみならずクラウドストレージにも対応！

無償健康診断のススメ

■Microsoft 365/Gmailを利用されているお客様限定



お申込はこちら

GUARDIANWALL Mailセキュリティ 評価版のお申し込み
https://forum1.canon.jp/public/application/add/1575

まとめ

1.電子メールを入口とした脅威は未だ後を絶たない状況です
　外部脅威の侵入を防ぐ対策が必要です

2.Emotetやランサムウェアなどのマルウェア感染が、時間・コストのビジネスリスクを増大させています

3.攻撃手法は高度化・巧妙化しているため
　リテラシー向上と合わせてシステムによる対策が求められています

4.外部脅威の侵入を防ぐ対策製品として
　Inbound Security for Microsoft 365を是非ご検討ください

ご清聴ありがとうございました

キヤノンマーケティングジャパン株式会社