HIGH-MARGIN, LOW-MAINTENANCE EMAIL SECURITY ADD-ON

AIを搭載する先駆的メールセキュリティ Vade for M365のご紹介

Vade Japan株式会社

株式会社グローバル・アドバンス
（DISTRIBUTOR）

vade

アジェンダ

- Vade のご紹介
- メールセキュリティの必要性
- Vade for M365とは

©2022 – Vade

Vade とは

2009 本社：フランス共和国リールにて設立

45% 年平均成長率（2015-2019）

96% 契約更新率：サブスクリプションモデル

200 従業員数

2017 日本市場に参入
日本国内にスレッドセンター設立

Georges Lotigier
CEO

Expert Insights 2021
Best of Phishing Protection

Expert Insights 2021
Best of Post-Delivery Protection

©2022 – Vade

予測的メール防衛のグローバルリーダー

業種問わず導入、国内大手3キャリアのフィルタリングサービスにも採用

©2022 – Vade

メールセキュリティの必要性

サイバー犯罪の90%以上がメールをきっかけにしています

「IPA 情報セキュリティ10大脅威2022」

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等のニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによるスマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
インターネット上のサービスからの個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬIT基盤の障害に伴う業務停止
インターネット上のサービスへの不正ログイン	10	不注意による情報漏えい等の被害

出典：IPA 情報セキュリティ10大脅威2022　https://www.ipa.go.jp/security/vuln/10threats2022.html

- ほとんどは「フィッシングによる個人情報の詐取」で3年連続上位、ついに1位に
  - コロナ禍で自宅でのインターネット利用が増加
  - 実在する公的機関や有名企業を騙ったメールからフィッシングサイトへ誘導し個人情報や認証情報を搾取
- ランサムウェアや標的型攻撃の手口に利用
  - メールの添付ファイルやリンクにウイルスを仕込ませる
  - Emotetの再流行
- ビジネスメール詐欺（BEC）の巧妙化
  - 内容が巧妙化（COVID-19等）し、不自然な点を見つけるのが困難

©2022 – Vade

マルウェアEmotet 2022年3月感染大爆発

取引先、知り合いになりすましたメール起因のマルウェア脅威

610件（2022年2月第一週）　→（7倍）　**4380件**（2022年3月第一週）

- **Emotetに感染すると…**
  - メール関連の情報を窃取（メールアカウント、メール本文、アドレス帳など）
  - 感染の拡大（メールを拡散）
  - 様々なサービスの認証情報窃取（ブラウザ保存のID、パスワードなど）

  - 他マルウェアの感染踏み台
    - データ暗号化によるデータの人質（ランサムウェア）
    - オンラインバンクなどの金銭の窃取
    - 遠隔操作・トロイの木馬（RAT）

    など

©2022 – Vade

マルウェアEmotet の特徴

特徴１．正規メールの返信を装う　　開封率が極めて高い
- **実際のメールアカウントを利用して送られる**
  - 人の警戒心および従来型検知をすり抜ける可能性が極めて高い

- **差出人・件名・本文・ファイル名などに受信者と関係のある文言を使う**
  - 件名に「過去メールを引用」、「汎用的なビジネス文言」、「受信者の名前」など

特徴２．パスワード付 zipファイル　PPAPへの慣れ
- 既存エンドポイントなどのシグネチャソリューションでは対応できない
- EDRなどのソリューションでも発症するまで検知できない可能性あり

特徴３．感染していないのに送信元名に悪用される場合あり

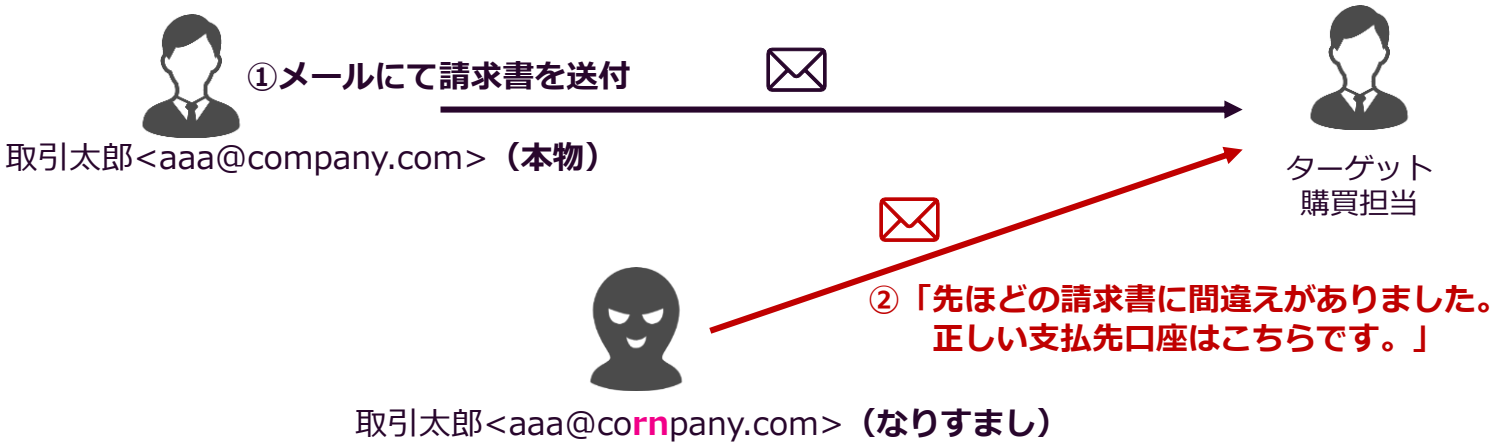
©2022 – Vade

ビジネスメール詐欺（Business Email Compromise: BEC）

取引先や従業員からのメールになりすまして金銭の不正振り込みに誘導、被害金額が極めて大きい

- 人の心理をつくソーシャルエンジニアリングを多用
  - ✓ 送信メールアドレスの乗っ取り、なりすまし
  - ✓ 本文に不自然な日本語が少ない
- 高度な場合は、事前に内容を傍受する仕組みをもつことも…
- スマホのメールアプリは送信メールアドレスが表示されない

**添付ファイル、URL記載が無く、
エンドポイント等で対応ができない**



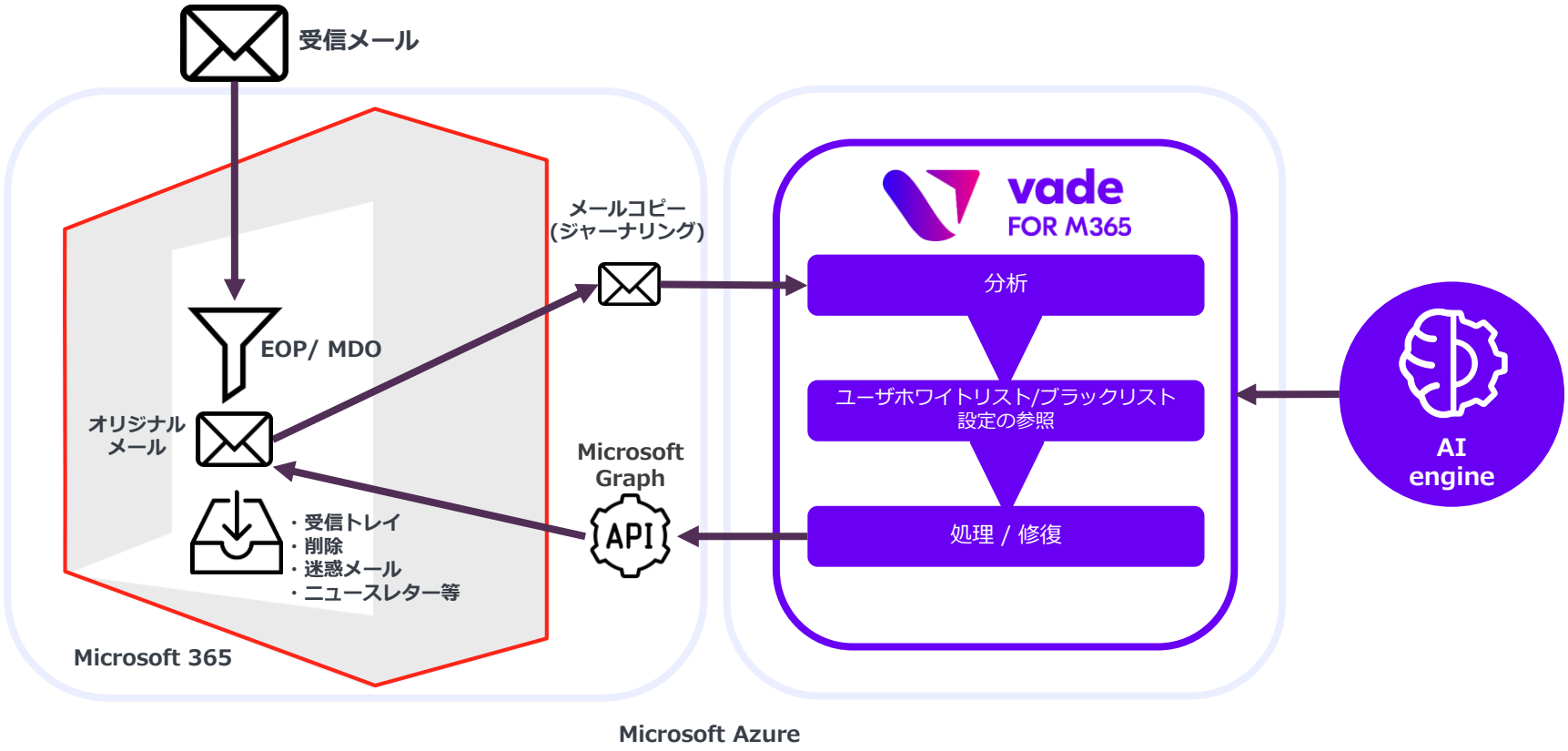
©2022 – Vade

Vade for M365

AIを搭載した予測的メール防衛

vade

Vade for M365｜システム構成



©2022 – Vade

Gartner Market Guide for Email Security 2021

Key Findings

- The adoption of cloud email systems continues to grow, forcing security and risk management leaders to evaluate the native capabilities offered by these providers.
- Solutions that integrate directly into cloud email via an API, rather than as a gateway, ease evaluation and deployment and improve detection accuracy, while still taking advantage of the integration of the bulk of phishing protection with the core platform.
- Vendor consolidation and in[illegible] capabilities (aka extended d[illegible]
- Ransomware, impersonation and account takeover attacks are increasing and causing direct financial loss, as users place too much trust in the identities associated with email inherently vulnerable to deception and social engineering. The evolution in threats has led to increased demand for other techniques and services, such as domain-based message authentication, reporting and conformance (DMARC), cloud access security broker (CASB)/API integrations, continuous awareness and mail-focused security orchestration, automation and response (MSOAR).

ゲートウェイよりも、APIを介してクラウドメールに直接統合するソリューションは、評価と導入を容易にし、検出精度を向上させる。さらにフィッシング対策の大部分をコア・プラットフォームに統合する利点を持っている。

(出典)：https://www.gartner.com/doc/reprints?id=1-27MOD8ND&ct=211011&st=sb

メールセキュリティを変える
Vade for M365の３ポイント

1. 既存メールセキュリティの課題克服

2. 高い検知率

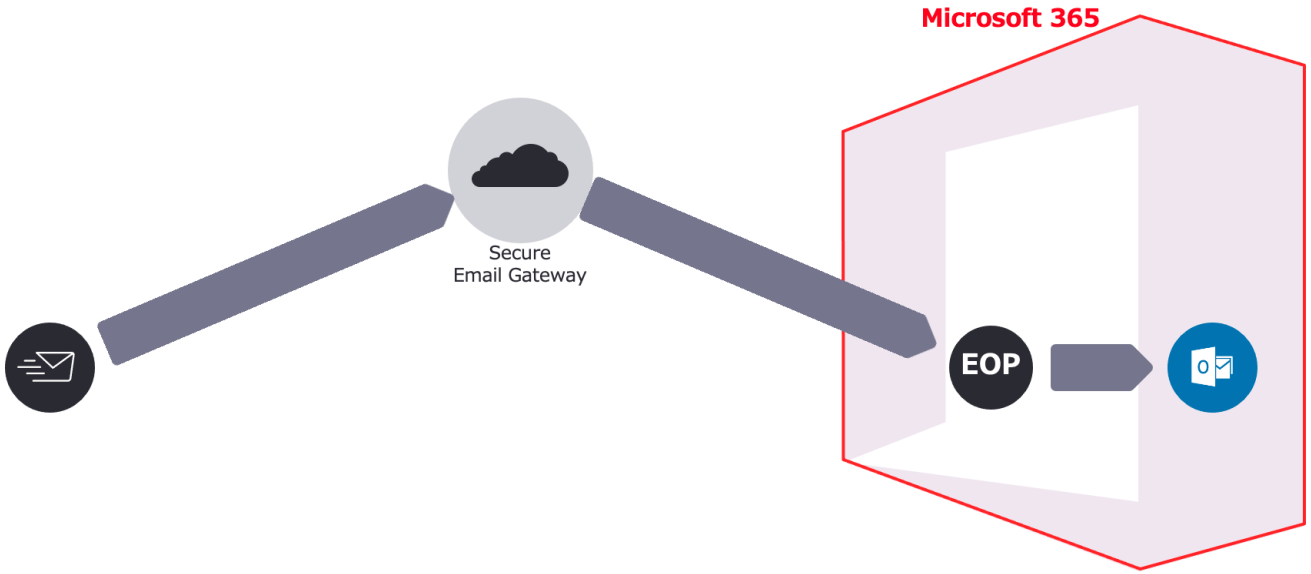
3. シンプルな検証、導入、運用管理

©2022 – Vade

1.既存メールセキュリティの課題克服

ゲートウェイ方式の既存メールセキュリティ

- 10年以上前から導入されている方式
- メールサーバの前段にゲートウェイとして設置され、送受信メールの検知、ブロック等を実施するメールセキュリティの仕組み
- オンプレ型からクラウド型が主流になってきたが、仕組みとしては同一



©2022 – Vade

1.既存メールセキュリティの課題克服

ゲートウェイ方式の課題

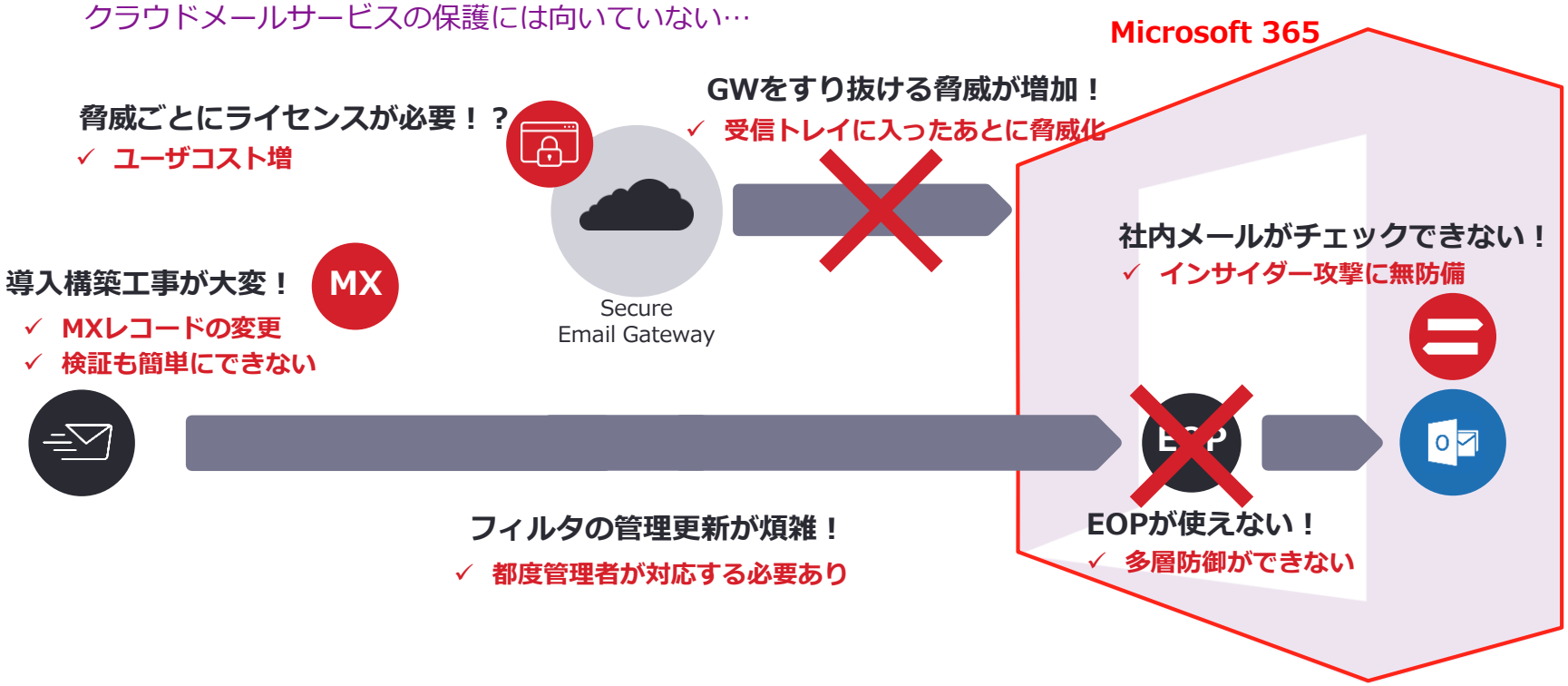
- **導入、構築工事が大変！（MXレコードの変更）**
  - 本番メール環境の設定を変更するため、工事のタイミングがシビア（連休深夜帯など）
  - 工事前後でメールが紛失していないかチェックテスト等、細かい計画が必要
  - 検証を実施するにも同様の工事が必要、簡単に検証できない…
- **社内メールが確認できない！**
  - 脅威メールを社内展開されてしまった際にチェックができない
- **フィルタの管理更新が煩雑！**
  - ブロックしたメールを確認して開放する作業
  - ホワイトリスト、ブラックリスト登録が必要

©2022 – Vade

1.既存メールセキュリティの課題克服

ゲートウェイ方式の課題

オンプレメールサーバ向けの設計で
クラウドメールサービスの保護には向いていない…

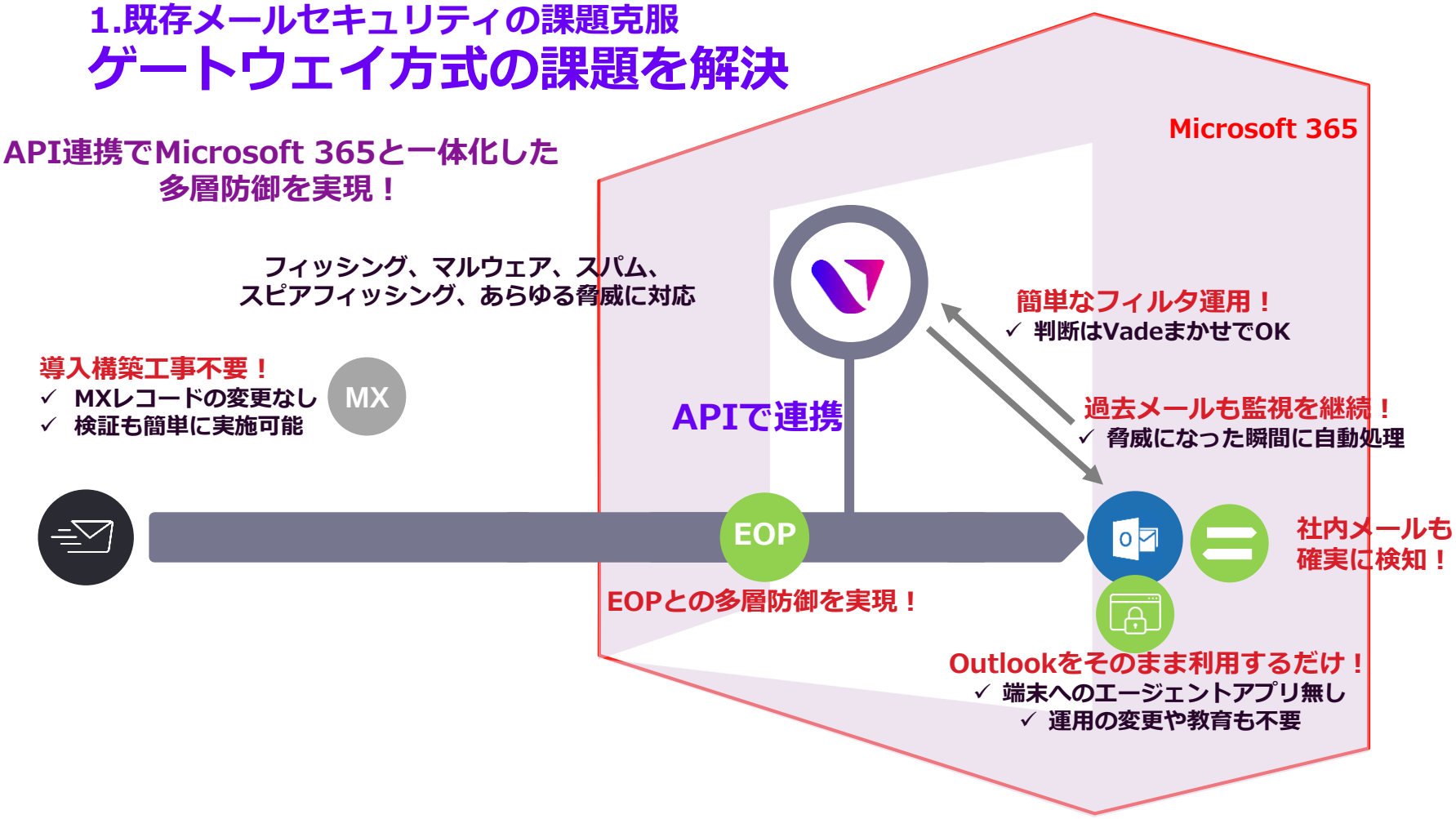


©2022 – Vade

1.既存メールセキュリティの課題克服

ゲートウェイ方式の課題を解決

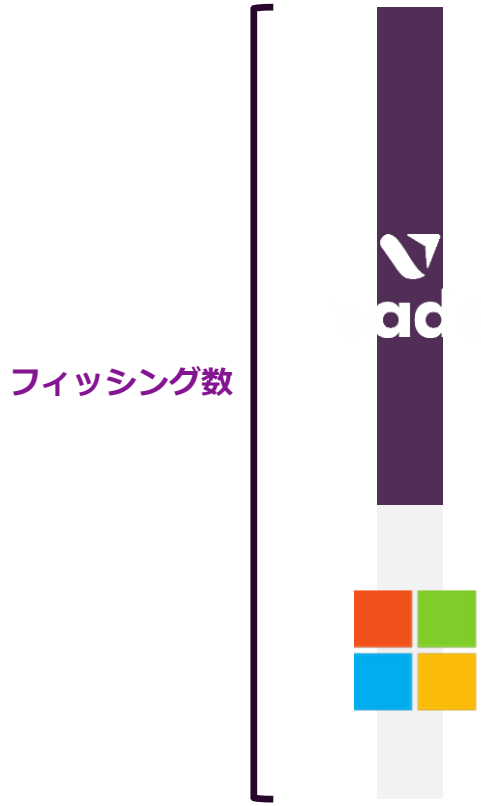
API連携でMicrosoft 365と一体化した多層防御を実現！



©2022 – Vade

2. 高い検知率

未知の脅威に対して確実なセキュリティ検知



63%

EOPをすり抜けた
フィッシングを検知

37%

【測定条件】
メールボックス数：23,000
測定期間：2019年10月18日から2020年1月16日

©2022 – Vade

2. 高い検知率

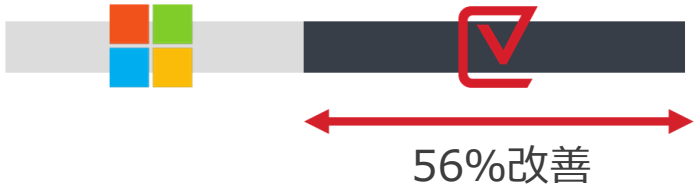
Microsoft EOP・ATPと実現する多層防御の有効性

フィッシング、マルウェアに対して多層防御により検知率を向上させる

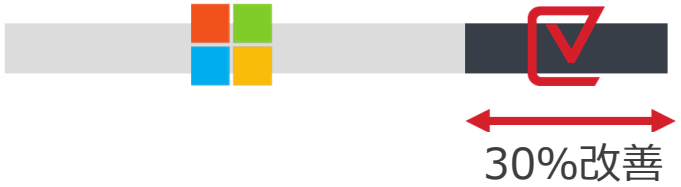
Microsoft EOP に対する**フィッシング**検知

Microsoft ATP に対する**フィッシング**検知

Microsoft EOP に対する**マルウェア**検知



Microsoft ATP に対する**マルウェア**検知

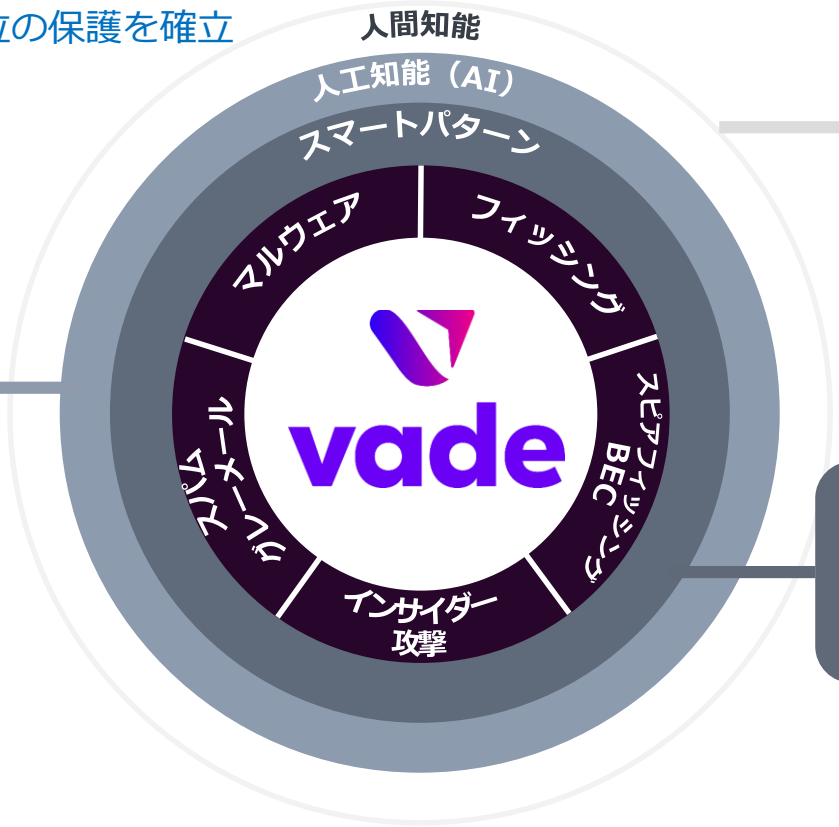


©2022 – Vade

2. 高い検知率

AIと人の連携により標的型攻撃を阻止する

あらゆる脅威に対して全方位の保護を確立



「人工知能（AI）」
- 機械学習
  ：フィッシングページのリアルタイム検出
- 自然言語処理（NLP）
  ：メール内容解析

など

17の特許取得

「人間知能」
- 世界3拠点24時間体制のVadeエンジニアによるタイムリーなフィルタ更新

「スマートパターン」
- 10,000のヒューリスティック（行動）アルゴリズムによる分析
- メールの特徴を捉えて分析
  初めての脅威も確実に検知

©2022 – Vade

3. 簡単な導入、運用管理と安価なライセンス

- ✓ SaaSとしてご提供
- ✓ Microsoftの標準APIを利用、10分以内に導入可能で**SI不要**

- ✓ **数クリックで設定完了**
- ✓ Exchange Onlineとシームレスに接続

- ✓ Outlookをそのまま利用するだけ
- ✓ 従業員への**フィッシング対策トレーニング（自動）**

- ✓ **無償トライアル**の即提供
- ✓ **既存環境へ一切の影響なし**
- ✓ 比較レポートにより追加検知率の簡単把握

- ✓ トライアルから契約へかんたん切換
- ✓ ユーザID単位での価格設定
- ✓ 1ユーザ当たり**月額300円以下**

©2022 – Vade

Vade for M365 価格表

エディション	リファレンス	ユーザー数	月	1年	3年
Email Security Premium	VS-CH-M365/nM	1-250	¥369	¥3,900	¥10,101
		251-1000	¥295	¥3,120	¥8,081
		1001-3000	¥237	¥2,496	¥6,465
		3000-	要相談		

©2022 – Vade

お問い合わせ

ありがとうございました。

お気軽にお問い合わせください。

株式会社グローバル・アドバンス
（DISTRIBUTOR）

03-5543-3682
info@g-advance.co.jp

- 本資料に記載されている会社名、商品、サービス名等は各社の登録商標または商標です。なお、本資料中では、「™」、「®」は明記しておりません。
- 本資料は、出典元が記載されている資料、画像等を除き、Vadeが著作権を有しています。
- 著作権法上認められた「私的利用のための複製」や「引用」などの場合を除き、本資料の全部または一部について、無断で複製・転用等することを禁じます。
- 本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。

vade