Abnormal

Abnormal AIが実現する Microsoft 365 メールセキュリティ インフラの強化

2024 年 5 月

目次

Microsoft 365 への移行：
メールセキュリティの新しいアプローチを可能にする

510億ドル

2013年以降、
ビジネスメール詐欺による
損失額。

28%

詐欺攻撃の全体のうち、
社員が原因となる
メールやファイルを
開封してしまう割合。

わずか 2.1%

攻撃が
セキュリティチームに
報告される割合。

70%

Abnormal Securityの
顧客のうち、
セキュアメール
ゲートウェイの
使用をやめた割合。

企業インフラやアプリケーション運用においてクラウドを優先するアプローチが主流となる中、Fortune 500企業の80%を含む100万を超える組織が、メール用途に Microsoft 365 を利用しています。オンプレミスからクラウドベースのメールへ移行したことで、4億人以上ものユーザーの生産性が向上し、より柔軟なビジネス運営が実現しました。

クラウドへの移行は、メールセキュリティへの投資を見直すことができるようになりました。過去のオンプレミスメールサーバーでは、スパムやマルウェアの猛攻を防ぐために、セキュアメールゲートウェイ（SEG）の使用がほぼ必須でした。しかし、Microsoft 365への移行により、Exchange Online Protectionとオプションの Microsoft Defender for Office 365（MDO）アドオンが提供する固有のセキュリティ機能を、単独で、またはサードパーティのセキュアメールゲートウェイと組み合わせて利用できるようになりました。

このアプローチにより、企業は全体として良好なメールセキュリティ体制を確立してきたといえます。しかし、メール脅威の状況は進化を続けており、人間の弱点を狙ったより洗練された攻撃が増えています。セキュリティツールの進化やエンドユーザーの意識向上にもかかわらず、ビジネスメールの流出やその他の巧妙な詐欺的攻撃は依然として増加しており、過去 5 年間で 430 億ドルもの損失が報告されています。

AI ネイティブな保護の必要性

では、セキュリティの責任者は、どうすればコストを増やすことなく、組織をより効果的に保護することができるのでしょうか？メールセキュリティのリスクを最小限に抑えるには、まず Microsoft が提供する既存のメールセキュリティ機能を把握し、従来型のセキュリティツールとの重複部分を理解することが重要です。

より高度な保護と予算の効率化を実現するには、Microsoft の既存機能を補完する形で追加のメール保護ソリューションを導入する必要があります。既存機能を無効化したり、重複したりせず、補強するアプローチが求められるのです。このホワイトペーパーでは、Microsoft が提供する機能をレビューし、メールセキュリティを補完するアプローチのメリットを調査します。

Microsoft 365 における メール保護機能

現在、企業が利用できるコミュニケーションアプリは膨大な数があるにもかかわらず、メールは依然として企業コミュニケーションの基盤となっています。サイバー犯罪者はこれを認識しており、メールを標的とするさまざまな攻撃手法を長年にわたり開発してきました。それに対抗するため、セキュリティ業界は徹底的かつ包括的なセキュリティ機能の基盤を構築してきました。

Microsoft は、これらの機能をビジネス向け M365 に統合しました。この機能をプラットフォーム内で統合することで、Microsoft 365 の初期導入時やセキュリティ防御強化時に、多くの企業がセキュアメールゲートウェイを使用せずに、メールセキュリティを強化できるようになっています。

Microsoft Exchange Online Protection

Exchange Online Protection（EOP）は、すべての Microsoft 365 エンタープライズプランに含まれています。また、中小企業向けには、Exchange Online メールボックスを含むすべての Microsoft 365 Business プランにも含まれています。

EOP は、スパムやマルウェアから組織を保護し、メッセージポリシー違反を防止するソリューションであると Microsoft は説明しています。Microsoft 365 のメールホスティングに EOP を組み合わせることで、以下のようなメールセキュリティ機能が提供されます。

Exchange Online Protection に関する詳細は Microsoft EOP ページをご覧ください。

カテゴリー	機能の説明
保護機能	マルウェア対策、フィッシング対策、スプーフィング対策、 受信/送信スパムポリシー、接続フィルタリング、ブロック/許可リスト、 エッジブロッキングなど
隔離と報告	管理者およびユーザーによるメッセージの報告、隔離機能、 フィッシング報告用アドインなど
メールフロー	転送ルール、許容ドメイン、コネクタ、スキップリストなど
モニタリング	メッセージトレース、メールおよびセキュリティレポート、監査ログなど
サービスレベルアグリーメント（SLA）	既知のウイルスを 100%防御し、スパムを 99%以上防御するなど、 複数の金銭的保証付き SLA を提供

Microsoft Defender for Office 365

Microsoft Defender for Office 365（MDO、旧称Advanced Threat Protection またはATP）は、追加購入可能なアドオンとして、2つのプラン（プラン1とプラン2）で提供されています。また、E5ライセンスには標準で含まれています。

EOPが大量の既知の攻撃を防御する一方で、MDO P1はゼロデイのマルウェア、フィッシング、およびビジネスメール詐欺（BEC）に対する追加の防御機能を提供します。MDO P2はさらに進化し、調査や対応機能、シミュレーションおよびトレーニング機能が追加されます。

MDO を Microsoft 365 のメールホスティング環境に追加することで、以下のような利点が得られます。

カテゴリー	機能の説明
防御と検出	Safe LinksやSafe Attachments、ワークロード保護、クリック時点でのURL保護、高度なフィッシング対策、ユーザーおよびドメインなりすまし対策など
調査	SIEM統合APIによる検出、リアルタイム検出ツール、URLトレーシングを含む。P2にはThreat Explorerやトラッカー、キャンペーンビューなどの追加機能が含まれる
対応	Threat Explorerや侵害されたユーザーに対する自動調査・対応、またはSIEM統合APIによる自動調査を含む

詳しい情報については、
Microsoft Defenderのページを参照してください。

Microsoft 365 を補強して高度なメール攻撃を阻止する

最も危険でコストのかかる攻撃を防ぐ高度なメール保護のニーズに対応するために、Microsoft EOP 及び MDO で既に可能なメールセキュリティ機能を補強するソリューションを選択することで、企業は予算と運用の効率性を向上させることができます。目的は、これらの機能を重複させたり、無効にしたりするのではなく、補強してより強力な保護を提供することです。

適切なアーキテクチャの選択

この目的を達成するには、SMTP セキュリティゲートウェイを再導入するのではなく、M365 と統合可能な API ベースのソリューションを選択することが組織にとって最適です。セキュアメールゲートウェイは Exchange Online Protection の前に配置されるため、EOP の接続フィルタリングや検出機能が無効になります。実際、多くの SEG ベンダーは、機能の互換性を確保するために EOP 機能を無効にすることを推奨します。

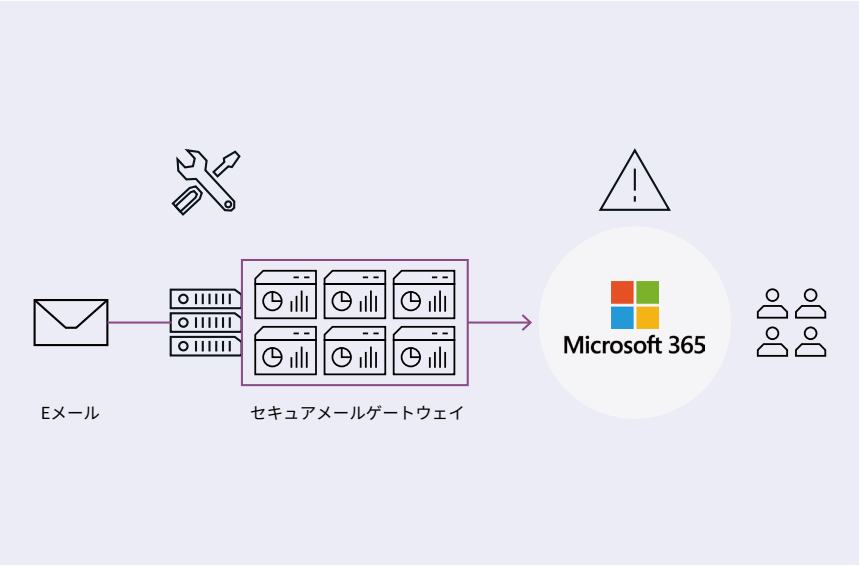

図 1. 組織は M365環境を保護するためにセキュアメールゲートウェイを追加できますが、このアーキテクチャではMicrosoftの機能を無効化する必要があります。

対照的に、API アーキテクチャを採用することで、EOP は設計通りに機能し続けることができます。API 統合により、EOP 本来の機能を低下させたり妨げたりすることなく、高度なメール攻撃の継続的なリスクに対応するための追加の保護レイヤーが提供されます。

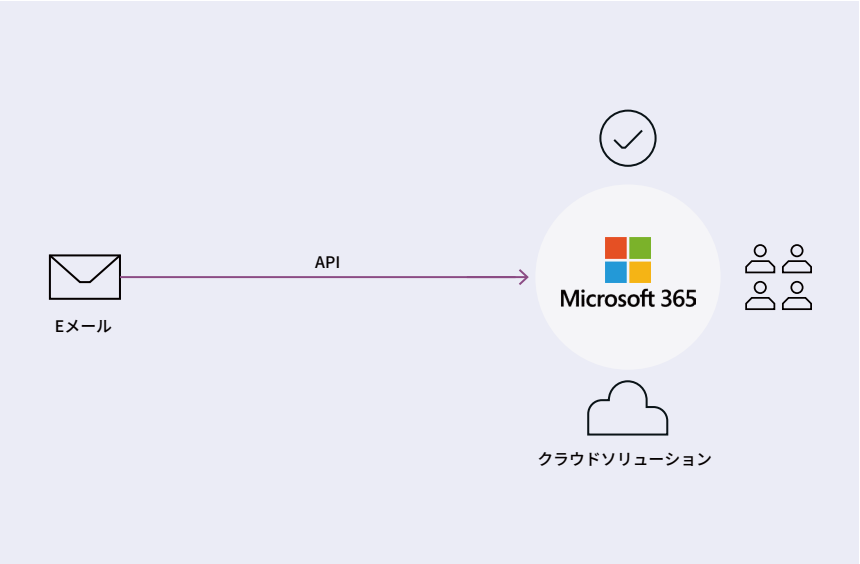

図 2. 組織は代わりにクラウドネイティブなAPIソリューションをM365環境に追加することで、Microsoftが意図した通りに機能できるようになります。

機能の重複を回避する

アーキテクチャのアプローチに加えて、セキュリティ予算の効率を最大化するうえで同様に重要なのは、メール保護要件に対応する際に、Microsoftが既に提供している機能の重複を制限するということです。

以下の表は、一般的なメール保護カテゴリーの一覧を示しており、API または SEG ソリューションが、企業の既存の EOP および MDO 環境と重複するかどうか、またどこで重複するかを特定するのに役立ちます。

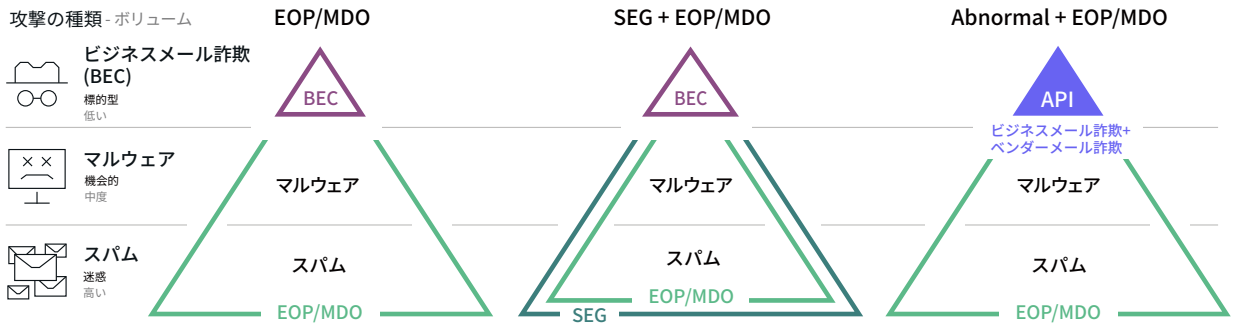

図 3. 組織はM365環境に安全なセキュアメールゲートウェイを追加することで、スパムやマルウェアに対する保護を段階的に強化できます。しかし、標的型攻撃への対応はほとんどされません。そのため、スパムやマルウェア対策にはMicrosoft本来の機能を活用しつつ、少量ながら高度に標的となるソーシャルエンジニアリング攻撃を防ぐソリューションを優先することで、最も高い効果と投資利益率（ROI）を得ることができます。

「私は（企業のメールにおいて）、Abnormal Securityの他にSEGを追加する価値を見出せませんでした。SEGがないことのデメリットは感じておらず、むしろメリットを感じています。そのため、SEGに費やしていた予算をAbnormal Securityに振り向けました。」

カバレッジと投資利益率の最大化

機能カバレッジを広げるために、これまで多くの組織はメールセキュリティスタックに第三のソリューションを追加し、あらゆる種類のメール攻撃に対する包括的な保護を確保してきました。理論上はこのアプローチは機能し、基本的な攻撃から高度な攻撃まで組織や従業員を保護することができます。

しかし、適切なソリューションを選択すれば、セキュアメールゲートウェイを使用せずとも、Microsoftと連携して必要な追加カバレッジを提供することができます。Abnormal Securityと組み合わせることで、Microsoft 365の本来の保護機能が強化され、すべての脅威に対する優れた保護を実現できます。さらに、SEGに関連する財務的および運用上のコストを削減することができます。

Forrester TEIレポートを読む →

多層防御の保護		Microsoft 365 + Abnormal =		多層防御
		脅威インテリジェンス/悪意のある攻撃の保護	行動分析/既知の安全な攻撃の保護	相乗効果
受信メールのセキュリティ対策	スパム グレーメール	脅威インテリジェンス ルールベース	行動分析 行動分析	
マルウェア対策	完全な添付/リンクの保護	脅威インテリジェンス	行動分析	
フィッシング対策	外部フィッシング スピアフィッシング 内部フィッシング	脅威インテリジェンス 脅威インテリジェンス ルールベース	行動分析 行動分析 行動分析	
ソーシャルエンジニアリング対策	BEC+CEO詐欺 BEC+インボイス詐欺	ルールベース いいえ	行動分析 行動分析	
アカウント乗っ取り対策	内部アカウントの乗っ取り ベンダーアカウントの乗っ取り	脅威インテリジェンス いいえ	行動分析 行動分析	
モダンなエンドユーザー体験	ネイティブなアウトルック体験 自動セーフリスティング	はい 脅威インテリジェンス	異常検出 異常検出	
簡素化された可視性と運用	精細な検出と修復	いいえ	異常検出	

Abnormal Human Behavior AI の活用

Abnormal の Human Behavior AI は、組織内の人々とその行動を深く理解します。Abnormal は何千ものデータの側面を分析し標準化することで、各個人の統合されたプロファイルを作成します。また、コミュニケーションパターンを観察することで、非公式な組織内の階層や社内外の関係性を把握し、ビジネスの文脈も理解します。

クラウドネイティブなAPI構造

従来のセキュアメールゲートウェイとは異なり、Abnormal は Microsoft 365 の API に統合され、メールの流れを妨げることなく数分で導入可能です。この API アーキテクチャにより、プラットフォームは M365 だけでなく、EDR や IAM ツールからも何千もの行動シグナルを取り込むことができます。さらに、社内外の通信を可視化することで、関係性や行動パターンの文脈から脅威を特定できます。

ビジネスインサイト

Abnormal は、すべての従業員、アプリケーション、取引先、およびメールテナントに対する可視性を提供するとともに、行動分析に基づく脅威インテリジェンスを提供します。この可視性を活用することで、セキュリティチームは設定のずれ、サードパーティアプリの権限、ユーザー権限の昇格、その他の潜在的なリスクを継続的に監視できます。Abnormal はまた、重大なイベントを明らかにし、セキュリティチームがメールプラットフォームのセキュリティ衛生を向上させるのを支援します。

Human Behavior AI検出エンジン

Abnormal は、個々のイベントや一連のイベントを行動パターンと比較して異常を検出し、従来のゲートウェイでは対処できない脅威のリスクレベルを判断します。特に、アカウント侵害によるソーシャルエンジニアリング攻撃を阻止し、説明可能な AI を活用して、意思決定エンジンの結果がチームにとって理解され、信頼されるようにします。

Abnormal を導入すれば、セキュリティチームはポリシー設定や手動での確認プロセスなしに、従業員をフィッシング攻撃から守ることができます。これにより、企業は市場で最も洗練された先進的なメールセキュリティソリューションを手に入れることができます。

まとめ

高度化するメール脅威からの保護に新たなパラダイムを求める企業にとって、M365 アーキテクチャや既存の EOP、MDO 投資との連携効率を最大化できるソリューションを選ぶことが重要です。そのためには、API ベースのアーキテクチャを採用し、AI を活用してセキュリティカバレッジと投資対効果を最大化するソリューションに目を向けるべきです。

Abnormal Security は、その期待に応える次世代のメールセキュリティを提供します。M365 とシームレスに統合するシンプルなクラウドネイティブ構造と、人間的 AI アプローチを活用することで、包括的なメール保護、検知、対応を実現します。Microsoft との連携により、Abnormal は保護を強化し、冗長なセキュアメールゲートウェイ（SEG）を排除することが可能になります。

Abnormal と Microsoft を組み合わせることで、企業は SEG を完全に廃止でき、実際に 70% の顧客がすでにセキュアメールゲートウェイを使用していません。次々と生まれる攻撃や予算削減の波が押し寄せる現代において、Abnormal Security は人間的行動セキュリティにおける No.1 の AI ネイティブプラットフォームです。

Abnormal

Abnormal Security は、AI を活用したリーディングプラットフォームとして、人間の行動を分析し、洗練された受信攻撃の阻止や、メールや接続されたアプリケーション内のアカウント侵害の検出を実現します。異常検知エンジンは、アイデンティティとコンテキストを活用して人間の行動を理解し、クラウドメールのあらゆるイベントのリスクを分析するとともに、人間の脆弱性を狙った高度なソーシャルエンジニアリング攻撃を検知・阻止します。

Abnormal は、Microsoft 365 や Google Workspace との API 統合により、わずか数分で導入可能であり、即座にプラットフォームの価値を実感できます。さらに、Slack、Workday、ServiceNow、Zoom など、さまざまなクラウドアプリケーションにも追加保護機能を提供します。

Microsoftセキュリティを強化しませんか？

ROIを確認する →

Demo版を試す →