



# MICROSOFT OFFICE 365 のセキュリティと コンプライアンス にかかるコスト

# 目次

<b>エグゼクティブ サマリー</b> .....	<b>3</b>
<b>OFFICE 365でメールセキュリティが重要な理由</b> .....	<b>3</b>
フィッシング詐欺 .....	3
マルウェア .....	4
ビジネスメール詐欺 .....	4
標的型攻撃 .....	4
見えないものには対処できない .....	4
サイロ化されたセキュリティに持続性はない .....	4
データ損失防止には正確性と柔軟性が不可欠 .....	5
eディスカバリに対応したアーカイブとコンプライアンス .....	5
<b>バンドルセキュリティの見えないコスト</b> .....	<b>5</b>
セキュリティチーム .....	6
IT部門 .....	7
稼働時間/サービスの可用性 .....	7
メッセージの追跡、配信不能レポート (NDR) .....	7
メールとマシンのクリーンアップにかかる時間 .....	7
コンプライアンス担当者 .....	8
アーカイブ .....	8
情報の保護 .....	8
<b>PROOFPOINTのメリット</b> .....	<b>9</b>
高度な技術でOffice 365の保護を強化 .....	10
高度脅威に対する有効性 .....	10
なりすましメールの阻止 .....	10
優先度の低い受信ボックス .....	10
詳細なフォレンジックと脅威インテリジェンス .....	10
自動取得でクリーンアップコストを削減 .....	10
セキュリティエコシステムとの統合 .....	10
フォレンジック収集と侵害検証 .....	11
メールのデータ損失防止 .....	11
メールの継続性 .....	11
コンプライアンス アーカイブ .....	11
カスタマーサポート .....	11
ProofpointでOffice 365のセキュリティを強化 .....	11

# エグゼクティブ サマリー

会社でMicrosoft Office 365への移行が決まりました。クラウドコラボレーション機能のメリットは理解できますが、Office 365に移行した場合、セキュリティ、コンプライアンス、eディスカバリ<sup>\*</sup>にどのような影響があるのでしょうか。

プライバシー、コンプライアンス、データ保存の要件を満たすように高度脅威対策、データ保護、オンラインアーカイブを設計するのは簡単ではありません。特に、Office 365ではさらに難しくなります。Microsoftのライセンスの一部として提供されているのに、サードパーティのメールセキュリティやアーカイブに追加の費用がかかるのはなぜでしょうか。メールセキュリティやコンプライアンスソリューションに差があるのはなぜでしょう。

これらの質問に答えるのは簡単ではありません。Microsoftのセキュリティでは問題が発生し、予想以上にコストがかかる場合もあります。高度脅威、メールセキュリティ、コンプライアンスアーカイブのすべてのソリューションが同じ機能を搭載しているわけではありません。

キャンプ用テントと家の違いと同じです。突然雨が降っても、ぬれずに済むことに変わりはありません。しかし、テントでは暴風雨に耐えられません。

同様に、高度なメールセキュリティソリューションは、現在の変化の激しいサイバー環境でも優れたセキュリティとコンプライアンス対策を提供することができます。

## OFFICE 365でメールセキュリティが重要な理由

標的型攻撃の91%はメールから始まっています<sup>1</sup>。

フィッシング詐欺やマルウェア攻撃では、メールを使って人的要因を悪用し、認証情報やデータを盗み出しています。

## フィッシング詐欺

脅威と認識されてから20年以上経過した現在、フィッシング詐欺は洗練された技術を駆使して、認証情報、金銭、機密情報を盗み出しています。最近のフィッシング詐欺は多層的で、検出を回避する技術を利用しています。無差別な攻撃だけでなく、特定の標的に限定した攻撃も発生しています。マルウェアを使用しない攻撃も発生しています。サイバー犯罪者は、スパムフィルターなどのセキュリティ対策を回避するため、正規のサービスを利用してフィッシング詐欺メールを送信しています。

攻撃の手口に関係なく、フィッシング攻撃は成功を収めています。

『Verizon 2016 Data Breach Investigations Report』によると、フィッシング詐欺メールを開いたユーザー数は昨年の23%から30%に増加しています<sup>2</sup>。また、SANS Instituteによると、95%のネットワーク攻撃がスパイフィッシングに起因しています<sup>3</sup>。

<sup>\*</sup> 国内未対応のため、弊社営業担当までお問い合わせください。

## 主な成功事例

「Proofpointは、大規模な攻撃からOffice 365のメールを保護してくれました。」

—CISO、Global 500のメーカー

「ProofpointでOffice 365メールを保護することで、被害を受けたシステムを短時間で復旧でき、コストも節約できました。」

—CSO、Fortune 500の金融機関

「カスタマーサービスとサポートが優れています。この製品は非常にうまく動作し、この1年間フィッシング詐欺は発生していません」

—Kenneth Brown、CIO、Whitworth University

「Office 365のままでは大量のフィッシング詐欺メールがシステムに侵入してきました。エンドユーザーにトレーニングを行い、クリックして認証情報を入力しないように伝えたにも関わらず、多くのユーザーが被害を受けました。Proofpointでこの問題が解決されました。今では、このような被害が発生していたことなど想像もできません」

— ネットワーク管理者、私立大学

## マルウェア

最近の攻撃者は、自動化ツールを利用して、公開されているソーシャルメディアのプロファイルから標的にに関する情報を収集しています。これは、勤務先、関心、趣味、婚姻状況、職歴などの情報が攻撃者に筒抜けになっていることを意味します。攻撃者は、これらの情報を利用し、メールに含まれている悪意のあるURLや添付ファイルをクリックさせ、システムへの侵入を試みます。

## ビジネスメール詐欺

この他にも、新たな重大な脅威として、ビジネスメール詐欺（BEC）が急増しています。BEC攻撃は、上司や役員を装うメールで詐欺を行う攻撃です。たとえば、CEOから会計担当者への送金を指示するメールが届き、指示どおり行くと、犯罪者に金銭が送金されるというものです。BECは不正送金だけでなく、個人を特定できる情報や給与明細などを送信するように指示する場合があります。

この脅威は、収益に大きな影響を及ぼす可能性があります。2016年のIBMの報告書によると、データ漏洩1件あたりのコストの総額は平均400万ドルで、2013年の平均値よりも29%増加しています<sup>4</sup>。

Office 365に移行にした場合、どのような影響があるのでしょうか。Office 365で中心となる機能はMicrosoft Exchange Onlineのメールです。セキュリティ、コンプライアンス、アーカイブ機能も搭載されていますが、エンタープライズクラスの組織の要件を満たすものではありません。

メールの保護対策が不十分でデータ侵害が発生すれば、ブランドが傷つき、信用を失い、収益が減少することになりますこのため、Office 365メールの保護強化が重要な課題となります。

## 標的型攻撃

攻撃経路として最も利用されるのがメールです。サイバー犯罪者は、他のコミュニケーションツールよりもメールの使用頻度が高いことを知っています。

攻撃者は、金銭や機密情報にアクセス権のある人事、IT、財務部門の担当者を狙います。ソーシャルエンジニアリングを駆使して感染ファイルを開かせたり、不正なサイトを閲覧させ、認証情報や財務情報を盗み出そうとします。マルウェアや盗み出した認証情報を利用してシステムへの侵入に成功すると、さらに社内ネットワークを経由して機密情報や価値のある情報を盗み出します。メールゲートウェイを保護することは重要なビジネス課題です。

## 見えないものには対処できない

脅威の痕跡（IoC）を検知するには、適切な情報が必要です。詳細なレポートを提供するメールゲートウェイがあれば、大量の情報の中から見つけ出さなければなりません。

メールゲートウェイで脅威をブロックすることには2つの重要な利点があります。まず、ネットワークに到達した後、攻撃の最終段階だけでなく、攻撃全体について理解することができます。次に、ゲートウェイで脅威を検知することで、攻撃を未然に防ぐことができます。

## サイロ化されたセキュリティに持続性はない

脅威の状況は常に変化しています。ハッカーは複数の経路から攻撃を仕掛けてきます。強固なセキュリティ対策を行うには、十分に調整された防御体制が不可欠です。Office 365の保護は最優先の課題です。しかし、効果的なソリューションを実現するには、セキュリティエコシステムの残りの部分との統合が不可欠です。ファイアウォールからセキュリティ管理プラットフォームまでを統合することで、優先度の高い脅威から先に対応し、攻撃を封じ込めることができます。

サイバー犯罪者は、他のコミュニケーションツールよりもメールの使用頻度が高いことを知っています

# データ損失防止には正確性と柔軟性が不可欠

Office 365の主な機能の1つはデータ損失防止（DLP）です。効果的なDLPを実施するには、正確性と柔軟性が不可欠です。不正確なソリューションでは、誤検知が大量に発生し、最悪の場合、データを失う可能性があります。また、組織ごとにDLPの要件が異なりますビジネス要件に合ったDLPシステムを構築するには、独自の分類と柔軟なポリシーが必要になります。オンプレミスとOffice 365の両方でデータを保持している場合、複数のポリシーを設定できたとしても、効果的な情報保護を行うことはできません。

## eディスカバリに対応したアーカイブとコンプライアンス\*

不正なコンテンツを排除することは重要ですが、ビジネス関連のコンテンツは、法規制に従い、合法的な方法で保管しなければなりません。コスト効率に優れ、保護要件を満たした方法でeディスカバリに対応しなければなりません。

コンプライアンスとeディスカバリの規則を遵守するには、保護されていないデータをOffice 365エコシステムに格納するだけでは不十分です。メール、ソーシャルメディア、エンタープライズコラボレーション（YammerやSlackなど）、ユーザーのラップトップに保存されたデータも対象になります。低コストのアーカイブが最善の解決策とは限りません。長期的に見れば、問題発生時の制裁金や訴訟準備金が高くなり、かえってコストが高くなる可能性もあります。

## バンドルセキュリティの見えないコスト

バンドルされたソリューションには見えないコストが隠れています。Office 365がセキュリティ要件を満たしていない場合、結果的に多くの時間と費用を費やし、情報と信頼を失う可能性があります。バンドルされたソリューションを使用しても、結果的に専用のセキュリティレイヤーが必要になります。この見えないコストについて考えてみましょう。

\* 国内未対応のため、弊社営業担当までお問い合わせください。



## セキュリティチーム

セキュリティ対策は労力を要する作業です。脅威の高度化でさらに厳しい状況になっています。コンプライアンス規制でセキュリティが重要な経営課題として扱われるようになりましたが、問題はそれだけではありません。自社を狙う攻撃を把握するために可視化を行う必要があります。このような情報がなければ、セキュリティ問題を組織レベルで解決することはできません。その結果、大量の時間を費やす結果になります。

Ponemon Instituteの調査によると、データ侵害が原因で倒産した企業も少なくありません<sup>6</sup>。このコストは、失った情報資産の種類や回数によって大きく異なります。次のことを考えてみてください。

- 防止できた侵害による生産性の低下
- 脅威の調査、優先順位付け、封じ込めに費やす時間（多くの企業は、攻撃されたユーザー1人あたり2~16時間）
- 不正な添付ファイルやURLを含むメールの駆除に要する時間
- このようなメールを長期的に受信した場合に直面するリスク
- 脅威を阻止し、組織を保護するために施行したセキュリティ対策の非効率性で失った時間（1アラートの対応にかかった日数）
- 可視化が制限されている場合、環境に対する脅威の把握に要した時間
- Office 365メールの停止中に個人メールに切り替えた場合のセキュリティへの影響（組織や主要アナリストが挙げる最大の懸念事項の1つがOffice 365のダウンタイムです<sup>6</sup>）

**組織レベルでの問題  
解決に必要な可視性  
と情報がなければ、  
大量の時間を費やす  
ことになります。**



## IT部門

IT管理者は、停電やサポートのコストを考慮する必要があります。

### 稼働時間/サービスの可用性

Forrester Researchは、Office 365メールの最大の課題の1つとして、可用性を指摘しています<sup>7</sup>。最近の業界の試算によると、停電の総コストは1分あたり5,600ドル、1時間あたり30万ドル以上になります<sup>8</sup>。Office 365のセキュリティを強化し、これらのコストを最小限に抑えるために、次のことを確認してください。

- メールに対する依存度メールの停止で顧客や見込み顧客からのメールが失われた場合の影響
- Office 365のメールの送受信が中断した場合に問題の認識にかかる時間
- サービス復旧時の期待値を設定するために、タイムリーなデータと十分な可視性を維持しているか
- ユーザーが個人メールで作業を継続する場合に伴うセキュリティとコンプライアンスのリスク

### メッセージの追跡、配信不能レポート（NDR）

IT部門のメール担当者やセキュリティ担当者の元には、毎日のようにメールの状況を確認する問い合わせが届いています。この問題に対処するプロセスについて、次のことを調べてみましょう。

- 問題のサポートに費やすことができる時間
- メッセージログのインデックス化の頻度ログの保存期間
- 検索クエリの結果が数分または数時間以内に返ってくるかどうか
- 古いログと新しいログで検索時間が異なるかどうか
- ログをすばやく見つけるために必要な検索条件があるかどうか、検索結果に不足がないかどうか
- より詳細な情報が必要な場合の連絡方法
- 追跡するメッセージの量と時間に対する誤検知の影響

### メールとマシンのクリーンアップにかかる時間

IT担当者は、メール関連のセキュリティイベントが発生してシステムが侵害された場合、感染したコンピュータを復旧するのに数時間から数日を費やしています。さらに、ユーザーがコンテンツに再度アクセスしたり、別のユーザーに転送しないように、これらのメールを削除しなければなりません。このプロセスはITとユーザーの生産性に影響を及ぼします。次のことを確認してください。

- 不要なイメージングを行ったり、やむを得ず再イメージングを行ったマシンの数
- 感染を封じ込めるツールとマシンの優先順位を判断するツールがあるかどうか
- メッセージのクリーンアップに費やす時間

「Proofpointは、大規模な攻撃からOffice 365のメールを保護してくれました。」

—CISO、Global 500のメーカー

# コンプライアンス担当者

コンプライアンス対応は重要な仕事です。コンプライアンスに違反した場合、費用がかかり、収益を損なう可能性があります。

## アーカイブ\*

データセンターレベルでは、Office 365はEUのデータ保護法、HIPAA（Health Insurance Portability and Accountability Act）、ISO 27001などの主要な規制に対応しています。しかし、Office 365には、メールデータをアーカイブして管理し、訴訟や監査時に容易にアクセスできるようにするという点では重大な欠陥があります。法的効力のある記録保持やワークフローがなければ、時間とリソースを無駄にし、訴訟費用が増す可能性があります。

英国の金融サービス法は、加盟国に6年間記録を保持するように義務付けています。金融取引業規制機構（FINRA）、証券取引委員会（SEC）、カナダの投資産業規制機関（IIROC）が制定した金融サービス規制に従い、通信の選択と検証を管理するモジュールが必要になります。

米国とカナダの投資家を保護することを目的としたFINRA（米国）、SEC（米国）、IIROC（カナダ）の規制に違反した場合の制裁金は、数百万ドルに及ぶ可能性があります<sup>9</sup>。追加のコストとして、セキュリティ対策、監査、潜在的な信用被害対策の費用がかかる可能性があります。

Office 365の機能を評価する場合には、次の点を検討する必要があります。

- Office 365を使用した場合、訴訟の際に、特定の個人が行ったすべての通信およびトランザクションの記録（ソーシャルメディアや共同作業プラットフォームを含む）を提供できるかどうか。複数の訴訟が同時に発生した場合の対応はどうか。
- 訴訟が発生した場合、コンテンツを法的に保持する方法
- IT部門がeディスカバリとデータのエクスポートにかかる時間。検索時間。Microsoftがこの機能に対するSLA（Service Level Agreement）を提供しているかどうか。検索処理の実行場所
- エクスポートするデータセットを決めた後に、指定されたFTPサイトにファイルを自動的にアップロードできるかどうか。または、ワークフローのこの部分を手動で終了する時間を設定する必要があるかどうか。データ検証チームへのデータ送信が遅れた場合の結果。
- 組織が生成したコンプライアンスコンテンツを収集して維持できるかどうか。ソーシャルメディアプラットフォームに存在するデータ。
- コンテンツの監督と監視が可能かどうか（規制によっては、コンテンツの監視とサンプリングが必要になります）。最新の技術を使用しているかどうか。基本的なキーワード一致にのみ依存しているかどうか。

## 情報の保護

すべての業種の違反統計に注意を払う価値があります。どの企業も常にデータを失うリスクを抱えています。内部の関係者がデータを故意に露出し、外部の攻撃者が盗み出す可能性もあります。また、従業員が誤って会社の重要な資産を公開してしまう可能性もあります。米国政府では、2014年だけで61,000件のセキュリティ侵害が発生しています<sup>10</sup>。Identity Theft Resource Centerによると、過去2年間で医療機関の91%がセキュリティ侵害を経験しています<sup>11</sup>。

金融詐欺に発展するビジネスメール詐欺（BEC）の例を見ると、法務部門の担当者を騙して機密情報を送信させたり、人事部門の担当者を騙して年度末の税務書類を送付させた事例が確認されています<sup>12</sup>。

データ侵害訴訟の懸念が高まり、セキュリティは重要な経営問題となっています。この点を踏まえて、Office 365のセキュリティを見直す必要があります。機密データ（複数のファイルタイプを含む）の検出能力、すべての侵入経路での問題解決能力、ポリシーの適用と問題報告の能力を見直す必要があります。

感染メールを管理するワークフローで送信メールにポリシーを適用することは、コンプライアンスだけでなく、セキュリティの重要なレイヤーとしても機能します。

\* 国内未対応のため、弊社営業担当までお問い合わせください。



次の点を確認しましょう。

- 機密情報が含まれている可能性のあるファイルの種類を検出できるかどうか
- ポリシーアラートを引き起こしたコンテンツをすばやく特定できるかどうか
- 問題を修復するインシデント対応のワークフローがあるか
- 自動応答により、メール、ファイル共有、Microsoft SharePointサイトなど、複数の経路に関する問題を修復できるかどうか。それぞれの経路からの攻撃を減らすために別個のDLPソリューションが必要かどうか。これらのポリシーを同期し、一貫性を報告する方法。
- 機密データの検出時に暗号化を行う方法。間違った受信者へのメッセージを取り消す精度。暗号化されたメールの中で、モバイルデバイスで閲覧されるメールの割合。受信者への影響。

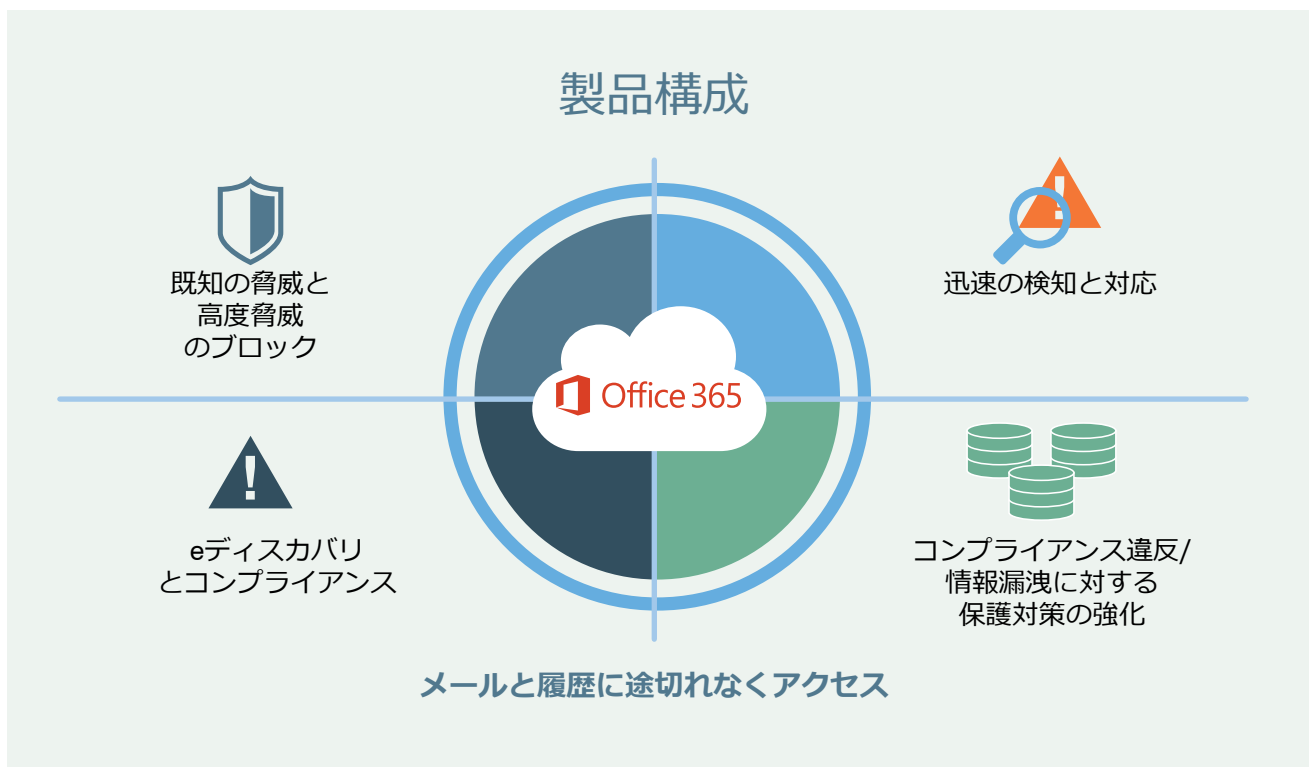
## PROOFPOINTのメリット

現在の複雑で、変化の激しい脅威と法規制に対応するには、新しい保護アプローチが必要です。メールに関しては、URLのレピュテーションチェックや古いメッセージトレース機能だけでは不十分です。これらの技術だけでは、脅威を可視化し、インテリジェンスを提供することはできません。また、侵害の検証や封じ込めにも役に立ちません。

高度な保護対策、迅速な可視化と対応は不可欠な要素です。Proofpointのメールセキュリティ技術は、Office 365のネイティブ機能をはるかに上回り、多層的で堅牢な保護機能を提供します。カスタマーサポートも充実しています。Proofpointにより、次のことが可能になります。

- 既知の脅威と高度脅威を阻止する
- 脅威を迅速に可視化し、対応する
- データ保護の強化により、貴重な情報を保護し、コンプライアンスを維持する
- コンプライアンスとeディスカバリ<sup>\*</sup>を遵守する
- フォレンジックでメールのアーカイブと履歴に常にアクセスできる<sup>\*</sup>

\* 国内未対応のため、弊社営業担当までお問い合わせください。



# 高度な技術でOFFICE 365の保護を強化

Proofpointを利用すると、Office 365に装備された保護機能を強化できます。

## 高度脅威に対する有効性

現在の巧妙化した攻撃に対応するには、専用のセキュリティ層が必要です。Proofpointは、静的技術と動的技術を組み合わせ、巧妙な高度脅威を検知します。サンドボックスで新しい攻撃ツール、手口、標的を検出します。メールに含まれるURLや添付ファイルを解析し、金融機関を狙うトロイの木馬、認証情報を狙うフィッシング詐欺、特定の企業を狙う標的型攻撃から組織を保護します。

また、独自の予測分析により、メールのトラフィックパターンに基づいて不審なURLを事前に特定し、サンドボックスで分析します。これにより、以前は検知できなかった悪意のあるURLからの攻撃リスクを最小限に抑えます。

## なりすましメールの阻止

ポリシー、認証、分類、高度なDLPを含む包括的なソリューションにより、可視化と施行を強化します。これにより、高度なりすましやBEC攻撃による被害を大幅に抑制します。独自の機械学習、通信傾向のベースライン機能、不正なメッセージ属性の分析機能、全体的な検出と可視化を行うポリシーが搭載されています。

## 優先度の低い受信ボックス

個人の傾向を学習し、グレイメールを正確に分類します。重要なビジネスメールをブロックすることなく、優先度の低いメッセージを適切に処理します。ユーザーダイジェストによる可視化で、優先度の低い受信トレイに分類されたメールをすばやく確認できます。要件が変わると、ダイジェストから設定をすぐに更新します。

## 詳細なフォレンジックと脅威インテリジェンス

攻撃者の特性、攻撃で使用されているツールと技術、狙われている対象をすぐに確認できます。組織を狙った攻撃の全体像を理解できます。

## 自動取得でクリーンアップコストを削減

自動またはオンデマンドで、ユーザーがアクセスできない隔離領域にメールを移動します。この機能は、Office 365 Exchange OnlineとExchangeの両方のメールボックスで機能します。

## セキュリティエコシステムとの統合

複数のセキュリティベンダーから構成される大規模なエコシステムと緊密に連携し、Office 365に被害をもたらす脅威を迅速に阻止します。

- Palo Alto Networksとの統合（脅威インテリジェンスの強化）
- SplunkなどのSIEMツールとの統合（脅威インテリジェンスと検出）。リアルタイムストリーミングにより、メールとネットワークイベントを関連付け、脅威を迅速に検出して対応することができます。
- 迅速な保護。既存の施行ツールを利用し、ネットワークレベルでメールの脅威に対応し、脅威の検出と保護のギャップを埋めることができます。次のものを阻止します。
  - システム間での感染拡大
  - マルウェアからの制御信号
  - 外部サイトへの機密データの送信

Proofpointは、既存のツールと連携して脅威を自動的に封じ込め、検出から保護までの時間を短縮します。

### 対応デバイス

- Cisco ASA
- Palo Alto Networks
- Check Point

- Cisco IOS
- Juniper SRX (JUNOS)
- Fortinet FortiGate
- Blue Coat

- Microsoft Exchange/ Office 365
- OpenDNS
- CyberArk
- Imperva

## フォレンジック収集と侵害検証

すべての攻撃が成功するわけではありません。したがって、対応の優先順位を考慮する必要があります。エンドポイントから脅威の痕跡（IoC）を自動的に収集することで、エンドポイントのスナップショットとサンドボックスのバージョンと比較し、感染の検証と脅威の分析を行うことができます。また、ターゲットマシンで過去の感染の証拠を確認し、他のマシンでオンデマンドスキャンを実行し、IoCを確認することもできます。データ収集を自動化することで、レスポンスの品質が向上します。

「ProofpointでOffice 365メールを保護することで、被害を受けたシステムを短時間で復旧でき、コストも節約できました。」

—CSO、Fortune 500の金融機関

## メールのデータ損失防止

DLPプロジェクトは失敗する傾向があります。一貫したポリシーとインシデント対応キューを使用して、最も関心のあるチャンネルに重点的に対応することで、成功確率が劇的に高まります。弊社のソリューションは、Office 365 ファイルだけでなく、複数のコンテンツタイプに対応しています。コンプライアンス違反に関する詳細な情報も提供します。組織の要件と優先度に応じてポリシーを調整できます。堅牢なインシデント対応ワークフローにより、インシデント発生時に迅速な対応を行うことができます。

## メールの継続性\*

Office 365のメールが停止した場合でも、ユーザーは生産性を維持できます。この常時稼働ポリシーにより、ユーザーはITからの対応を待つことなくメールの送受信を継続し、重要なビジネスコミュニケーションを維持できます。エンドユーザーは、OutlookまたはWebポータル経由でカレンダーや連絡先を含むすべてのデータにアクセスできます。過去30日間のメールがエンドユーザーの受信トレイに保存されます。すべてのメールは、ヘッダーを変えずにメールサーバーに復元されます。アーカイブとフォレンジックで問題が起きることはありません。

## コンプライアンス アーカイブ\*\*\*

殆どの組織は、Exchange Online、OneDrive for Business、Skype for Businessなど、Office 365のコンテンツを保存することが義務付けられています。Microsoftが提供するアーカイブ機能は、eディスカバリやコンプライアンスではなく、ストレージ管理を重視するものです。

弊社のソリューションは、Microsoft Office 365のアーカイブを上回る機能を提供します。不変のアーカイブストレージと500種類以上の添付ファイルのインデックス（Microsoft以外のファイルフォーマットを含む）を維持し、Slack、Bloomberg、ソーシャルメディアプラットフォームなど、様々なソースからコンテンツを収集して保存します。強力なeディスカバリワークフローと検索性能により、フォレンジックをより迅速かつ簡単に行うことができます。弊社独自のDouble-Blind Key Encryptionアーキテクチャにより、クラウドベースのストレージに保存されているデータの暗号化キーを完全に制御できます。

## カスタマーサポート

セキュリティ専門企業として業界最高のカスタマーサポートを提供し、顧客満足度評価で95%の評価を得ています。包括的なサポートオプションにより、セキュリティ、継続性、コンプライアンスの管理と拡張を容易に行うことができます。

## PROOFPOINTでOFFICE 365のセキュリティを強化

Office 365のセキュリティを強化することは非常に重要です。脅威の高度化が進み、その数も急増しています。このような攻撃やコンプライアンスリスクからユーザー、データ、ブランドを保護しなければなりません。

弊社のセキュリティソリューションは、Microsoftネイティブの保護機能を上回る機能を提供します。業界最高のセキュリティ、コンプライアンス、メール継続性をクラウドベースのOffice 365に提供します。Proofpointを使用すると、ユーザーの接続性と保護状態を犠牲にすることなく、Office 365の持つメリット（自由度、柔軟性、コスト効率）を最大限利用することができます。

詳しくは、[www.proofpoint.co.jp/solutions/threat-protection-compliance-office-365](http://www.proofpoint.co.jp/solutions/threat-protection-compliance-office-365)をご覧ください。

\* 日本未発表です。詳細は弊社営業担当までお問い合わせください。

\*\* 国内未対応のため、弊社営業担当までお問い合わせください。

- <sup>1</sup> Kim Zetter (Wired). "[Hacker Lexicon: What Are Phishing and Spear Phishing?](#)" (ハッカーの用語: フィッシングとスパイフィッシングの違い) 2015年4月
- <sup>2</sup> Verizon. "[2016 Data Breach Investigations Report.](#)" (2016年度データ漏洩/侵害調査報告書) 2016年4月
- <sup>3</sup> Neal Weinberg (Network World). "[How to blunt spear phishing attacks.](#)" (スパイフィッシング攻撃の撃退方法) 2013年3月
- <sup>4</sup> IBM "[IBM & Ponemon Institute Study: Data Breach Costs Rising, Now \\$4 million per Incident](#)" (IBMとPonemon Instituteの調査報告: データ侵害のコストが増大、インシデント1件あたりの被害は400万ドルに)
- <sup>5</sup> Ponemon Institute and IBM. "[2016 Ponemon Cost of Data Breach Study: Global Analysis](#)" (2016年データ漏えいコストに関する調査報告書: 世界分析) 2016年6月
- <sup>6</sup> Proofpoint. "[Is Microsoft Office 365 Secure?](#)" (Microsoft Office 365は安全か) 2016年
- <sup>7</sup> Proofpoint. "[Six Key Capabilities for Securing Office 365 Email.](#)" (Office 365メールを保護する6つの機能) 2016年5月
- <sup>8</sup> Andrew Lerner (Gartner). "[The Cost of Downtime.](#)" (ダウンタイムのコスト) 2014年7月
- <sup>9</sup> Financial Industry Regulatory Authority (FINRA). "[FINRA Fines Scottrade \\$2.6 Million for Significant Failures in Required Electronic Records and Email Retention.](#)" (FINRAが電子記録およびメールの保存義務違反でScottradeに260万ドルの制裁金を科す) 2015年11月
- <sup>10</sup> Ian Bremmer (Time). "[These 5 Facts Explain the Threat of Cyber Warfare.](#)" (サイバー戦争の脅威を表す5つの事実) 2015年6月
- <sup>11</sup> [Identity Theft Resource Center.](#)
- <sup>12</sup> FBI. "[FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals.](#)" (FBI、企業の財務担当者を狙う詐欺の増加を警告) 2016年3月

## PROOFPOINTについて

Proofpoint, Inc. (NASDAQ:PFPT) は、高度な脅威やコンプライアンス違反のリスクからビジネスを保護する次世代のサイバーセキュリティ企業です。Proofpointは、メール、モバイルアプリ、ソーシャルメディア経由で自社のユーザーを狙う高度な標的型攻撃を阻止し、社内の機密情報を保護できるようにサイバーセキュリティの担当者をサポートします。また、問題が発生した場合に迅速に対応できるように、適切な情報とツールを提供します。Proofpointのソリューションは、Fortune 100企業の半数以上を含む様々な規模の企業で採用されています。モバイル、ソーシャルを利用した現在のIT環境に対応し、クラウドとビッグデータを駆使した分析で高度な脅威を阻止しています。

©Proofpoint, Inc. Proofpointは、Proofpoint, Incまたは米国またはその他の国の関係会社における商標です。その他の登録商標及び商標はそれぞれその所有者に帰属します。