

# PROOFPOINT EMAIL FRAUD DEFENSE

## メールは、企業を狙う1番の侵入経路です

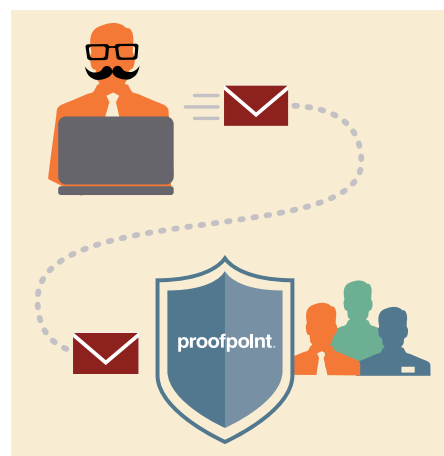
- BEC 詐欺で企業に 53 億ドル以上の被害が 2013 年 1 月以降に出ています。<sup>1</sup>
- 30% の受信者はフィッシングメッセージを開き、12% は添付ファイルをクリックします。<sup>2</sup>
- ドメインなりすましがメール詐欺の大半を占めており、それらはメール認証により防ぐことができたものです。<sup>3</sup>

## 利点

- メール詐欺や、フィッシング攻撃が受信ボックスに届く前に阻止します。
- 完全な可視化により、組織から送信されるメールを制御します。
- 早く確実にメール認証を御社のドメインとゲートウェイに実装します。
- 御社の顧客やパートナーも保護します。

Proofpoint Email Fraud Defense はあなたの従業員、顧客そしてビジネスパートナーすべてを、信頼できるドメインを装ったサイバー犯罪から守ります。シンプルで信頼性の高い電子メール認証により、メール詐欺を受信トレイに届く前に止めることができます。

Email Fraud Defense は、ソーシャルエンジニアリングを利用したビジネスメール詐欺 (BEC) や消費者フィッシングなどの攻撃から組織を守ります。このような攻撃は常に変化しており、インフラストラクチャよりも従業員をターゲットにします。そのため、従来のセキュリティツールではメール詐欺を阻止するのは困難になっています。サイバー犯罪者たちは、同僚やパートナーあるいはベンダーを装って、被害者からお金や貴重な情報を簡単に盗みとります。マルウェアやエクスポイトを使う必要はありません。



Email Fraud Defense は、DMARC (Domain-based Message Authentication, Reporting and Conformance) 認証を使ってそのような攻撃の阻止に役立ちます。業界標準のプロトコルが、送られてきたメールが正規の送信元からのものかを確認します。DMARC 認証がメールを信頼のできるものにします。また、攻撃者が御社の組織の一員になりすまることがないようにします。Email Fraud Defense を使い、他の組織からの電子メールであっても、御社環境へ侵入するなりすましメールの阻止を実現します。

Email Fraud Defense を活用し、すべての種類のメール詐欺を防ぐことが可能となります。また、御社の組織で送受信されるすべてのメールの認証ステータスを完全に可視化することができます。Email Fraud Defense は、不正なメールをブロックし、正規の送信者からのメールを滞りなく配信できるという自信を与えてくれます。

## 御社の従業員、顧客、パートナーを保護しましょう

従業員やパートナーたちは外部のメールサービスプロバイダーを使って、御社を代表してメールを送信しています。犯罪者は信頼されているアイデンティティになりすまし、BEC および認証情報フィッシングを使ってメールの受信者を騙すのです。

<sup>1</sup> FBI、2017 年 5 月 "Business E-Mail Compromise/ E-Mail Account Compromise: the 5 Billion Dollar Scam." (「ビジネスメール詐欺 / メールアカウント詐欺: 50 億ドル規模の詐欺」)。

<sup>2</sup> Verizon、"2016 Data Breach Investigations Report" 2016 年 4 月

<sup>3</sup> Proofpoint "The Human Factor 2017" 2017 年 6 月。

メールエコシステム全体を可視化することが可能です。どのメールが認証されているか、いないか、またその理由についても可視化することが可能です。到達すべき正規のメールが認証されなかった場合、その解決方法を知ることができます。

Email Fraud Defense は、組織で送受信するメールの全てを信頼して承認することができるよう支援します。360 度の可視性により、組織として送信する正規のメールをすべて承認し、詐偽メールは受信ボックスに到達する前に阻止します。

- メール詐偽の攻撃から御社の従業員、顧客そしてパートナーを守ります。
- Eメールコミュニケーションにおける人々の信頼性を維持します。
- 組織で送受信するメールの全てを可視化します。

### 正規のメールをブロックすることなくメール認証を簡素化

従業員、顧客そしてパートナーに送信される正規のメールを特定し認証することで、認証されないメールをすべてブロックすることができます。

しかし、認証の実施は自動化することができません。また、それには深い専門知識が必要になります。そのため DMARC の実施が難しい場合があります。よくある例として、正規のメールがブロックされてしまい、業務を妨げるということがあります。

Email Fraud Defense は、認証をすばやく自信を持って実装するために必要なツールとサービスを提供します。

- 送信された正規のメールの識別を自動化することができます。
- 認証が失敗した場合、それぞれの理由を特定し解決方法を知ることができます。
- 専門家によるガイドとサポートを導入から継続的に受け、ドメインとゲートウェイにメール認証を効率的に実装することができます。

### PROOFPOINT EMAIL PROTECTION への投資の強化により、より高度なセキュリティと柔軟性を実現

従業員に送信されるメールを可視化し管理することでメール詐偽を防ぐことが可能になります。Email Fraud Defense で速やかに、そして安全にメールプロテクションを設定し、組織に届くメールすべての認証を強化することができます。

保護に加え、Proofpoint Email Protection の柔軟性を活用し、正当なメールの認証失敗を受け入れるよう設定することができます。つまり、組織に届くメールすべての認証をよりすばやく実行できるようになります。さらに、Email Fraud Defense と Email Protection の Impostor Classifier ( 詐欺メールの分類 ) を組み合わせることで、あらゆるタイプのメール攻撃から守るための何重ものアプローチが得られます。

- 従業員への BEC およびフィッシングによる攻撃を防ぎましょう。
- 可視化と管理を迅速に行うことで、組織に送信されたメールの全てを信頼して承認することができます。

#### PROOFPOINT について

Proofpoint Inc. (NASDAQ:PFPT) は次世代のサイバーセキュリティ企業です。組織が高度な脅威とコンプライアンスのリスクから今日の業務のあり方を保護できるようサポートしています。Proofpoint は、サイバーセキュリティの専門家たちが、ユーザーをターゲットとする ( 電子メール、モバイルアプリ、ソーシャルメディア経由の ) 高度な攻撃から彼らを保護し、ユーザーが作成する重要な情報を保護し、万が一の場合に素早く対応するために必要な知識とツールをチームで活用するお手伝いをいたします。フォーチュン 100 企業の 50 パーセント以上を含むすべての規模の大手組織は、現在のモバイルおよびソーシャルメディア対応 IT 環境向けに構築されており、クラウドの力とビッグデータを生かした分析プラットフォームを活用して、より高度な脅威に対応できる Proofpoint ソリューションに依存しています。

©Proofpoint, Inc. Proofpoint は、米国およびその他の国々における Proofpoint, Inc. の商標です。本書に記載されたその他すべての商標は、それぞれの所有者に帰属します。