報道関係者各位

# 8 万人対象のフィッシング演習、
# エフセキュアがリサーチ結果を発表

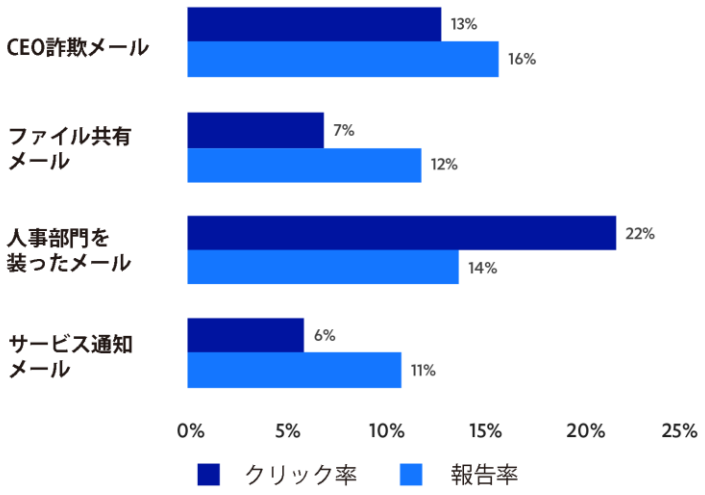
**～ エンジニア層も一般社員と同程度またはそれ以上にフィッシングの罠に陥りやすいことが判明 ～**

2022 年 1 月 31 日
エフセキュア株式会社

先進的サイバー・セキュリティ・テクノロジーのプロバイダである F-Secure (本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、エフセキュア) は、同社が 8 万人以上を対象に実施したフィッシングメール演習に関するリサーチの結果を発表しました。リサーチによると、人事部門を装ったメールや、請求書作成についてのメールが最も多くクリックされていること、そしてエンジニア層も他の一般社員と同程度またはそれ以上にフィッシングの罠に陥りやすいことが判明しました。

『To Click or Not to Click』(クリックすべきか、しないべきか) と名付けられたこのリサーチには、異なる業界の 4 つの企業の 82,402 人が参加し、攻撃に使用されやすい 4 種類のフィッシング手法を模した電子メールに対して、どのように反応するかを検証しました。

今回の調査で最も高い割合でクリックされたのは休暇取得に関する人事部門からの通知を模したメールであり、メール受信者のうち 22%がメール中のリンクをクリックしていました。2 番目に多くクリックされていたのは、メール受信者に請求書の作成を依頼するメール (本レポートでは「CEO Fraud: CEO 詐欺」と呼んでいます) で、受信者のうち 16%がクリックしていました。続いてドキュメント共有を模したメール (7%)、オンラインサービスからのサービス通知を装ったメール (6%) となっていました。



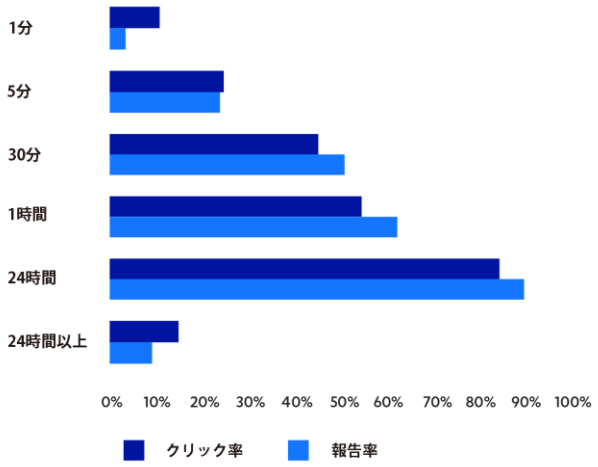

**(図 1: メールタイプ別のクリック率／報告率)**

エフセキュアでサービスデリバリーマネージャーを務め、本レポートの主執筆者である Matthew Connor (マシュー・コナー) は、このリサーチにおいて最も注目すべき発見は、テクニカル部門に所属する従業員が、それ以外の部門の社員と同等またはそれ以上にフィッシングの被害に遭いやすいということだと語っています。
「技術者は企業のインフラへのアクセス権限を持っているため、攻撃者がより積極的に狙っている可能性があり、そのため、彼らがフィッシングに対する標準的あるいは高度な警戒心を持ち合わせているかが試されることとなります。今回の調査終了後に実施したアンケートによると、こうしたテクニカル部門の社員はそれ以外の部署の人々よりも過去のフィッシングの試みをしっかり認識していることがわかりました。従って、これからも不審なメールをフィッシングとして認識し続けることができるかが防御のための重要な課題となります。しかし、たとえ高い認識レベルも持っていたとしても、彼らのフィッシングメールのクリック率がその他の社員と同程度またはそれ以上であるという事実は、フィッシング対策において大きな脅威となるものでしょう。」

調査対象となった企業のうち 2 社で、IT／DevOps 部門の社員がフィッシング演習メールをクリックした割合は、どちらもその企業の他部門と同等かそれ以上となっていました。1 社では企業全体でのクリック率が 25%だったのに対して DevOps 部門が 26%、IT 部門が 24%と、ほぼ同程度でした。また、もう 1 社では企業全体では 11%でしたが、DevOps 部門が 30%、IT 部門が 21%と、非常に高いクリック率でした。

また、これらのテクニカル部門は他部署と比較し、フィッシングの疑いがあるメールの報告についても大きなアドバンテージを持っているとは言えないこともわかりました。1 社では、IT 部門と DevOps 部門の不審メール報告能力は、9 部門中でそれぞれ 3 位と 6 位でした。もう 1 社では、16 部門中で DevOps が 11 位、IT は 15 位でした。

本レポートでは、迅速かつシンプルな不審メール報告プロセスの価値も強調されていました。フィッシング演習メールが受信ボックスに届いてから最初の 1 分間で、「不審である」と報告した社員の実に 3 倍以上もの社員がメール中のリンクをクリックしていました。この数字は、5 分前後で横ばいとなり、その後も同じ傾向が続いています。




**(図 2: メール配信後の経過時間別のクリック率／報告率)**

また、時間の経過とともに不審メール報告も増加していく一方で、企業ごとに異なるプロセスが重要な役割を果たしました。不審メールにフラグを立てるためのボタンを全社員のメールクライアントに搭載している企業においては、受信者の 47%が調査期間中にそのボタンを使用しました。他の 2 つの企業での参加者は、フィッシング演習メールを「不審である」と報告したのはわずか 13%と 12%となっていました (もう 1 社は不審メール報告に関するデータを提供していませんでした)。

エフセキュアのコンサルティング部門である F-Secure Consulting でディレクターを務める Riaan Naude (リアン・ナウデ) によると、今回の調査で明らかになった不審メールの報告率とクリック率のパターンは、今後企業がフィッシングへの対策を立てるうえで非常に実践的な機会を提供することができたと語っています。
「今回のリサーチでは、セキュリティ部門と他部門が協力し、企業のフィッシングへの耐性を向上させるためのスターティングポイントとして、迅速かつシンプルに不審メールを報告できるプロセスの必要性を明確に指摘しています。このプロセスを適切に行うことで、攻撃を早期に発見し、防御できることを意味しているのです。」

フィッシングやその他のセキュリティ上の課題への対応をサポートするエフセキュアのソリューションの詳細については、以下のページをご覧ください。
https://www.f-secure.com/jp-ja/business

『To Click or Not to Click: 8 万人を対象としたフィッシング演習から学んだこと』ダウンロードページ:
https://www.f-secure.com/content/dam/press/ja/media-library/reports/2022201_F-Secure_Phishing_Study_Report_JP.pdf
ブログ掲載ページ:
https://blog.f-secure.com/ja/insight-from-a-large-scale-phishing-study/

エフセキュアプレスページ:
https://www.f-secure.com/jp-ja/press

## エフセキュアについて

エフセキュアほど現実世界のサイバー脅威についての知見を持つ企業は市場に存在しません。数百名にのぼる業界で最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的なセキュリティ対策に関する AI テクノロジー、そして「検知と対応」。これらの橋渡しをするのがエフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200 社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。
エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は https://www.f-secure.com/en/welcome (英語) および https://www.f-secure.com/ja_JP/ (日本語) をご覧ください。また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。

---

※　以下、メディア関係者限定の特記情報です。個人の SNS 等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】

エフセキュア株式会社
広報部　　秦　和哉
TEL：03-4578-7745 (直通)
japan-pr@f-secure.com