さらば、燃え尽き症候群
自動化でセキュリティ部門の負担を軽減

企業のセキュリティにおけるウィークポイントは従業員だと言われることがあります。しかし、フィッシングメールの報告が簡単に行えるようになれば、従業員は最初の防衛線となることができます。

疑わしいと報告されるメールの数が増加すれば、セキュリティ部門の仕事も増加します。だからこそ、自動化が重要となるのです。

1,000人規模の組織では、平均して

116 通/月

のメールが報告されています

10,000人規模の組織では、平均して

1,160 通/月

のメールが報告されています

フィッシングと報告されたメールを手動で調査する時間

経験豊富なセキュリティチーム：

15分～1時間

経験の浅い／人員不足のセキュリティチーム：

最大5時間

フィッシング判定の自動化でセキュリティチームの負担を低減

疑わしいと報告されたメールのうち、

99%以上

が自動処理に

1%未満

が手動での判定を必要とした

報告されるフィッシングメールを手作業で判定するために毎月必要な時間

1,000人規模の企業の場合：

29時間から580時間

10,000人規模の企業の場合：

290時間から5,800時間

報告されるフィッシングメールに対して、自動化されたフィッシング分析とトリアージを行った場合の、毎月の手作業での調査時間

1,000人規模の企業の場合：

17分から5.8時間

10,000人規模の企業の場合：

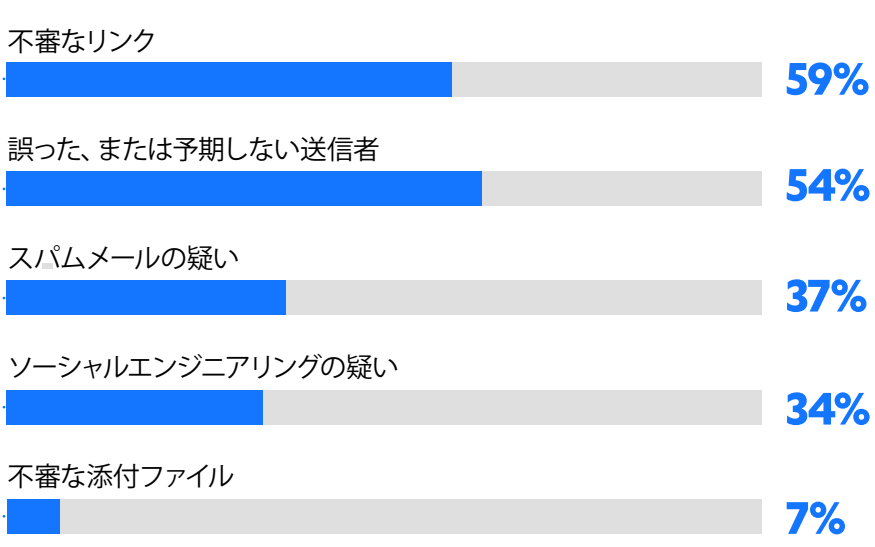
2.9時間から58時間

フィッシングメールの報告の簡易化がもらたす価値

報告されたメールの99%は、自動化によって処理されました。そのうち33%は自動的に「悪意がある」または「疑わしい」と判断されました。

残りの1%のメールは手動による追加分析に付され、そのうち63%が「悪意がある」または「疑わしい」と判断されました。

従業員がメールを報告する理由...

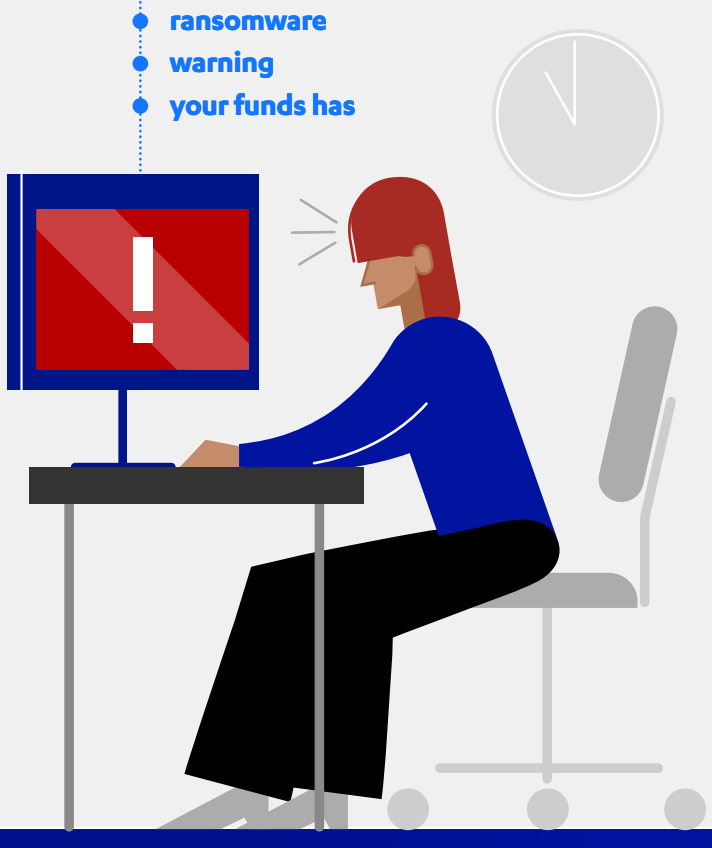


報告されたメールに見られる、疑わしい単語やフレーズのトップ10

	単語／フレーズ	単語／フレーズが含まれる割合	リスクレベル
1.	click here	15	Medium
2.	Login	8	Medium
3.	Payment	8	Low
4.	please click	7	Medium
5.	Password	7	Low
6.	Record	6	Low
7.	please visit	5	Medium
8.	click here to	4	Medium
9.	M&A	3	Medium
10.	Bitcoin	3	Medium

高いリスクを持つ単語／フレーズ

- **dropbox**
- **amount of usd**
- **message is from a trusted**
- **ransomware**
- **warning**
- **your funds has**



F-Secure