Web公開 抜粋版

KnowBe4
Human error. Conquered.

不審メールの報告と分析を効率化
PhishERご紹介

～メールの脅威を迅速に特定し、素早く対応～

株式会社電通国際情報サービス
金融ソリューション事業部
戦略アライアンス部

KnowBe4
Human error. Conquered.

Web公開 抜粋版

1 **最初に**

2 **背景**

3 **PhishERとは（本編の一部）**

4 こんなお客様にお勧めです（本抜粋版には含まれません）

5 ISIDの取り組み（本抜粋版には含まれません）

本資料は、全体30ページのうち、
抜粋版となります

1 ｜ 最初に

PhishERとは

◉ トレーニングプラットフォーム“KMSAT”のオプション機能

教育・訓練・分析 → 不審メール報告 → 不審メールのトリアージ → 脅威メールの検疫、隔離

KMSAT

Kevin Mitnick Security Awareness Training

KnowBe4 Phish Alert

Phish Alertボタン（無償）

PhishER

G2 Leader FALL 2022

最上位評価を獲得したSOAR（※）プラットフォーム

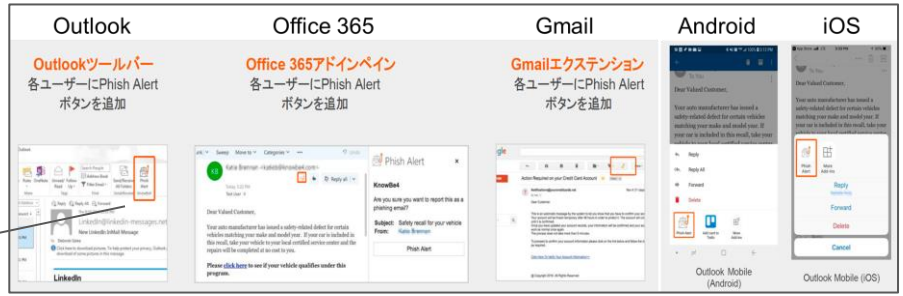
メールの脅威を迅速に特定し、素早く対応

※SOARとはSecurity Orchestration, Automation and Responseの略。セキュリティ運用業務の効率化や自動化を実現するための技術、あるいはソリューション
PhishERは2022年秋G2 Gridレポート「SOARプラットフォーム部門」において6四半期連続でNo.1の評価を獲得
https://prtimes.jp/main/html/rd/p/000000120.000053624.html

1 ｜ 最初に

Phish Alertボタンとは

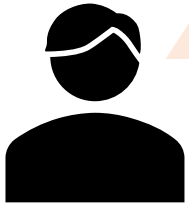
- 不審メール報告を簡単に行える無償のボタン



- 導入メリット

- ボタン一つで**簡単報告**。報告の為の操作（転送や本文作成など）余計な操作をする必要が無く、誤ってURLをクリックしてしまう**リスクの低下**
- 普段から報告を意識する事により不審メールを報告する**文化の醸成**に繋がる

一般ユーザー



- 技術的な対策を潜り抜けた攻撃型メールの**検出・分析・対策**につなげられる
- 特定の個人・部署宛の攻撃メールが増えている場合は、注意喚起などの対策実施。
- 報告メールが増えることで、**攻撃の傾向を掴む**ことができる。

情報セキュリティ管理者／推進チーム

2 | 背景

不審メールの発見から対処までを迅速にすることが求められている

- メールを使った攻撃を防ぐことができない
  - システム面/従業員の不審メールの耐性向上にも限界が

- 不審メールの発見から対処までを迅速に
  - 気付いた誰かが報告し、ただちにそのメールを回収、分析できればSOCで発見できなかった攻撃メールの気付きや、インシデントを未然に防ぐことが可能

2 | 背景

自社で仕組みを作る事の難しさ

- 人材確保の難しさ（エキスパート）
- CSIRTなどの組織化
- 不審メールの報告と分析フローの確立
  - 誤報の見極め（従業員数に比例して不審メール報告件数も増える）

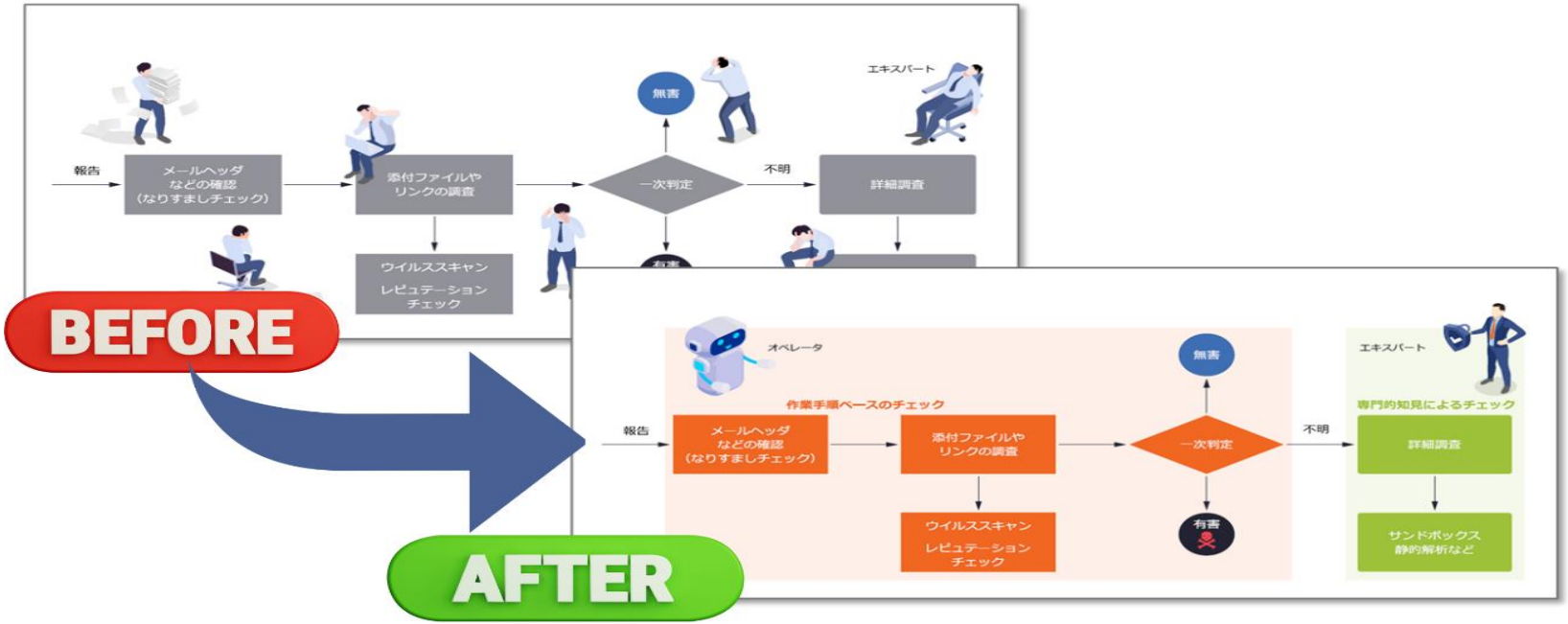
エキスパート

高いスキルを持った要員（エキスパート）が効率的に分析できる仕組みが必要

3 ｜ PhishERとは

PhishERのアプローチ

- 機械的に行える作業と高度なスキルが必要な作業を整理
- 一連の作業を安全に効率的に行える環境をクラウドで提供

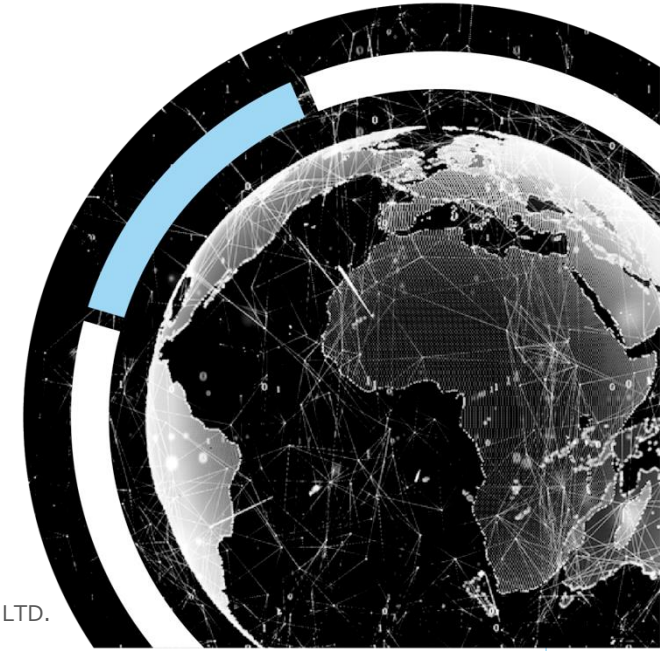


Web公開 抜粋版

KnowBe4
Human error. Conquered.

THANK YOU

更に詳細な資料送付や
デモや個別説明もさせて頂きます



iSiD

株式会社 電通国際情報サービス

金融ソリューション事業部　戦略アライアンス部
g-security@group.isid.co.jp
☎ 03-6713-7030
https://security.isid.co.jp/

OptimizingYourSecurity