

# AIベースのフィッシングインシデント対応

メール解析とレスポンスタイムを90%以上短縮



## ワンダッシュボード=迅速かつシンプルな調査・分析・対応

IRONSCALESは、メールサーバーとシームレスに統合し、1つの統合ダッシュボードからユーザーのメールボックスからフィッシングメールを削除することを可能にします。ここでは、セキュリティプロセスの連携・自動化とレスポンスの迅速化という大きなメリットがあります。

## 迅速なレスポンスのための的確なレポーティング

検出されたメールや従業員から報告されたメールは、「IRONSCALES Resolution Center」のオープンインシデント領域に表示されます。SOCチームは、各インシデントに対する迅速な判断を下すために必要な情報をリアルタイムで確認することができます。例えば、当該インシデントに対する報告数、同様なメールを受信しているメールボックス、送信元の全情報、本文の全内容などです。

## IRONSCALES独自のフォレンジック&トリアージ

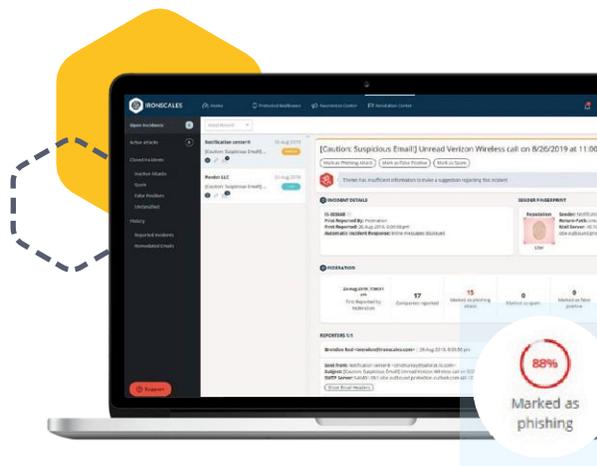
IRONSCALESは、脅威の重大度を自動的に分析・トリアージ(優先順位付け)し、IRONSCALESは、脅威の重大度を自動的に分析・トリアージ(優先順位付け)し、マルチAV/視覚的類似性検知/サンドボックススキャンと連携したIRONSCALES独自のフォレンジック分析を用いて、疑わしいメールの包括的なフィッシングフォレンジック調査を実施します。

## 自動化された不審メールの隔離・削除・修復

リンクや添付ファイルなどの明確な危険の徴候が検出された場合、IRONSCALESのプラットフォームは、すべての影響を受けるメールボックスからこの危険と判定されたメールを自動的に隔離・削除します。同時に、エンドポイントとSIEM(Security Information and Event Management)システムの両方に対して、的確な対策情報を生成します。さらに、IRONSCALESは、マシンラーニングとAIを使って、今、発生している類似のフィッシングメールを検出し、1つに分類・クラスター化し、一括隔離・削除します。これによって、ポリモーフィック攻撃に広範囲に対処することができ、変異型の攻撃が検出されず、未解決のまま放置されることを防ぎます。

**フィッシングの特定、検証、隔離・削除に要する平均時間はなんと3時間を超える！**

フィッシングメール対策はどの組織においても基本的な要件となっています。しかし、この対悪テクノロジーはいくら採用しても、そこには限界があります。多くのセキュリティ担当者が、今、このようなバラバラのシステムやポイントソリューションに苦闘しています。この課題に加えて、セキュリティ担当者は悪意のあるメールがユーザーのメールボックスに届いてから約82秒以内にメッセージを特定して、ユーザーがクリックして開くという最悪の事態になる前に対処することが求められています。考えてみてください。この82秒という短時間の間にセキュリティ担当者はメールの脅威を発見し、対応しなければならないのです。



私の一日は、30分刻みで、1つのインシデントに対処するのに費やされています。次から次へと発生してくるのです。グローバル金融サービス会社、CISO



あるガートナーのお客様は、Outlookにフィッシング報告ボタンをインストールしたところ、SOCに提出されるフィッシングの疑いのあるメッセージの数が800%も増加したそうです。SOCに今必要なことは、フィッシング攻撃の報告と解決を自動化し、すべてのメールボックスで類似した攻撃をいち早く検知し、対処することです。

GARTNER (FIGHTING PHISHING – 2020 FORESIGHT)より

## どこからでもフィッシングメールの脅威に対応

iOSおよびAndroidモバイルアプリと連携して、セキュリティチームはどこからでもフィッシングメールの脅威に対応することができます。外出中にどこからでも迅速な対応が可能になります、キーボード操作は一切不要です。

## 人とマシンの融合による防御

テクノロジーソリューションだけでは、巧妙化するフィッシング攻撃を止めることはできません。人のよる的確なインテリジェントな判断と、AIや機械学習などの最新のテクノロジーによる支援を組み合わせることこそが、抜本的なフィッシング対策を実現するのです。IRONSCALESのオールインワンプラットフォームは、人とマシンの融合から生まれるハイブリッドソリューションを作り出します。人の英知をAIのアルゴリズムにフィードバックすることで、防御レイヤーをさらに強化されていきます。

## 主な機能と特徴

- セキュリティプロセスの連携・自動化とレスポンスの迅速化を実現
- 迅速なレスポンスを可能にする直感的なダッシュボードを提供
- サードパーティのSIEM、SOAR、マルチAV、サンドボックスソリューションと統合が可能
- iOSとAndroidのモバイルアプリで外出先からインシデントを解決
- 従業員は通知ボタンのワンクリックでフィッシングメールの報告が可能  
セキュリティ管理者はワンクリックで全受信者のメールボックスからフィッシングメールを一括削除
- AI/マシンラーニングにより、社内のメール管理者の作業工数と労力を大幅に削減(スクリプトや他のツールは必要なし)

## なぜIRONSCALESなのか？

- 1 まず、第一に、IRONSCALESが選択されるのは、導入の早さと運用の容易さです。そして、BECやアカウント乗っ取りなどの高度な攻撃など、あらゆる種類のメール脅威を阻止する能力において、他に類を見ないサービスを提供していることです。
- 2 IRONSCALESは、メールボックスレベルで、攻撃のターゲットとなる可能性が最も高い部署から導入といったスモールスタートが可能。
- 3 また、IRONSCALESが「メールセキュリティ」と「ユーザーアウェアネス」を組み合わせた包括的なメールセキュリティプラットフォームであることも、IRONSCALESが選択される理由の1つです。

私たちは、自動化されたソリューションを探していました。これまでのソリューションは、まさに手作業そのものでした。

グローバル金融サービス会社、CISO



IRONSCALESをさらに知りたい方は、  
[www.ironcales.jp](http://www.ironcales.jp)をアクセスしてください。

あらゆるタイプのフィッシング攻撃の予見、検知・防御から隔離・削除までの迅速かつシンプルなソリューションを今すぐ手に入れることができます。