

# MANAGED PHISHING DETECTION AND RESPONSE(PDR)

By Cofense Phishing Defense Center(PDC)。



## お客様が抱える課題

Cofense は十分に把握しています。フィッシングの 96% がメールを通じて仕掛けられている中、フィッシング対策がビジネスにおける極めて重要な問題となっています。さらに、一般的なセキュリティオペレーションセンター(SOC)アナリストはセキュリティアラートの山に埋もれて、調査できているのはその約 50% に過ぎません。組織はフィッシング攻撃を数時間や数日間ではなく数分間で阻止できるようにするため、脅威をすばやく検知して自動的に隔離できるソリューションを必要としています。



## Cofense が提案するソリューション

Cofense では、Cofense Phishing Defense Center(PDC)のセキュリティ専門家によるユニークな Managed Phishing Detection and Response(PDR)サービスを提供しています。Managed PDR サービスは、内部の専門知識やリソースが不足している組織にとってフィッシング攻撃を効果的に防御し、修復するにあたって最適なサービスです。Cofense PDC の専門家は、わずか 8 分間でお客様のネットワークへの攻撃を検知して阻止することができます。また、Managed PDR の顧客は、2,500 万人ものグローバルユーザーから得られるインテリジェンスを享受することができ、それによって、まだ報告すらされていないネットワーク内のフィッシング攻撃を特定し、削除することが可能となっています。



Cofense PDR プラットフォームは、組織が持っている最強の防御手段-つまり人-を活用できるよう後押しして、Cofense の自動対応およびインテリジェンス技術の駆使と並行して、市場でもっとも総合的なフィッシング対応と検知を成し遂げます。

## COFENSE MANAGED PDR とは:



### 忠実度の高い脅威インテリジェンス

40 名を超えるセキュリティアナリストから構成されるグローバルネットワークにアクセスし、人間(アナリスト)が精査した最新のフィッシング脅威インテリジェンスを活用して、お客様の環境内に潜む脅威を迅速に特定し根絶します。これにはゼロデイフィッシング攻撃に対する防御、毎年300万通以上の不審なメールや30万件以上のPDCアナリスト調査案件から得られるインテリジェンス、99.999%の分類精度などが盛り込まれています。



### 脅威の修復

数日間や数週間ではなく数分間でフィッシング攻撃を特定し、攻撃が成功する前に環境内から速やかに脅威を取り除きます。実際、Cofense PDC の迅速な検知から分析、対応および修復にかかる時間の平均値は約60分であり、一部のフィッシング攻撃に関してはわずか8分間で阻止されました。



### 脅威ハンティング

Cofense のセキュリティアナリストが脅威インテリジェンスを掘り下げて活用し、お客様の環境内に潜むアクティブなフィッシング脅威や脅威の痕跡を能動的に調査し、特定します。

---

## COFENSE MANAGED PDR サービスが選ばれる理由

Cofense PDC アナリストは、他組織で毎週見受けられる数百万通のメールから24時間365日体制で収集される脅威インテリジェンスを活用し、アクティブな脅威の検知と対応に要する平均時間を大幅に短縮しています。Managed PDR の顧客は、2,500万人規模の強みを持つCofense のフィッシング対策ネットワークの一部となって、そこに貢献しそこから恩恵を受け、「ネットワーク効果」とでも呼ぶべき状態に組み込まれます。ある脅威が報告されると、すべての顧客が恩恵を受ける仕組みです。

## COFENSE MANAGED PDR の利点:

- Cofense の専有技術を用いて、お客様の組織を標的にしたリアルタイムフィッシングキャンペーンの報告および対応を強化
- お客様の従業員から報告されたすべての不審なメールを調査
- 不審なメールを報告するすべての Managed PDR の顧客によって発展を続けるネットワークを活用
- お客様の SOC 部門に対してフィッシングの専門知識を補充
- アクティブな攻撃の検知と対応に要する時間を大幅に短縮
- お客様の SOC と一体化して効率的かつ効果的な対応を追究
- フィッシングメールの分析に基づいた、すぐにアクションを取ることのできるインテリジェンスを提供

Cofense Managed PDR をご利用いただくと、PDC アナリストが悪意のあるメールを特定した場合、即座にお客様に通知が届きます。また、脅威に関するコンテキストや修復に関する推奨事項を記載した詳細なエスカレーションレポートもお届けします。第 1 段階および第 2 段階のセキュリティ侵害インジケータ (IOC) はすべて、API を介して入手可能であり、迅速な対応のさらなる改善や攻撃者によって組織が被る影響のさらなる軽減を図れます。

Cofense の目標は、すべての企業をフィッシングの脅威から自己防衛できる組織にすることです。そして、Cofense のグローバルネットワークと Managed PDR サービスの強みを活かすことにより、その実現は、はるかに容易になりました。

**COFENSE MANAGED PDR サービスについての詳細は、次のサイトをご覧ください:** [cofense.com/phishing-defense-services/](https://cofense.com/phishing-defense-services/)

### Cofense について

Cofense® はフィッシング検知対応ソリューションを提供する先進企業です。Cofense の Phishing Detection and Response (PDR) プラットフォームは企業組織向けに設計されており、フィッシングの疑いのあるメールを積極的に報告する 2,500 万人超の人々が作り出すグローバルネットワークの活用と高度な自動化技術とを組み合わせ、フィッシング攻撃をより迅速に阻止し、セキュリティ侵害に対して常に先回りします。Cofense のソリューションを一式そろえて導入していただくことで、組織は従業員に対してフィッシングメールを特定して報告する方法を教育し、自社の環境内でフィッシングメールを検知し脅威修復に向けて迅速に対応することが可能となります。Cofense のソリューションは主要な TIP、SIEM、SOAR の大半とシームレスに統合でき、既存のセキュリティエコシステムと容易に連携を取ることができます。防衛、エネルギー、金融サービス、医療、製造業など幅広い業界にわたる Global 1,000 企業を顧客に持ち、Cofense はセキュリティ向上、インシデントレスポンスの支援、セキュリティ侵害のリスク軽減を実現する方法を会得しています。詳細につきましては、[www.cofense.com](https://www.cofense.com) をご覧いただくか、Twitter および LinkedIn をフォローしてください。



[cofense.com/contact](https://cofense.com/contact)

703.652.0717

1602 Village Market Blvd, SE #400  
Leesburg, VA 20175