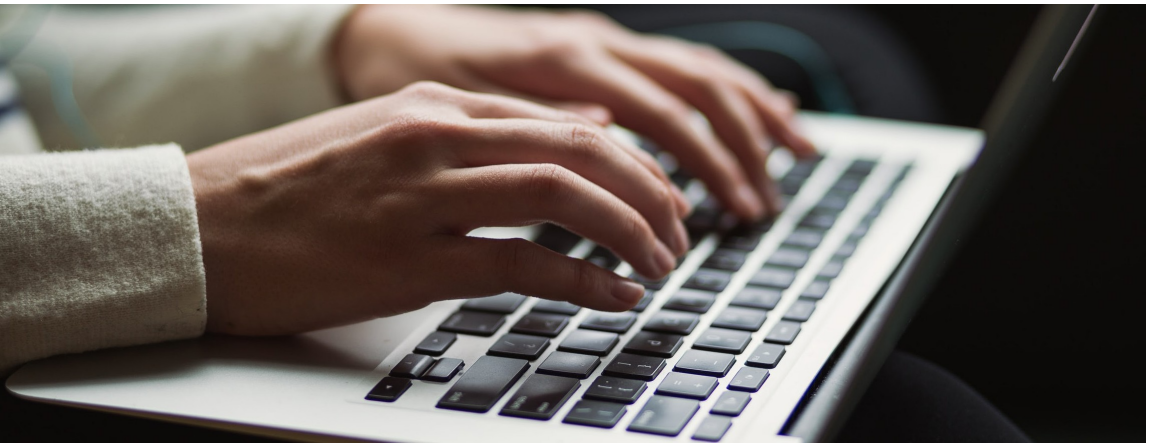
ソリューションブリーフ

Secureworks

# 事前準備と レジリエンスを備えた インシデント対応の変革



サイバーレジリエンシーとは、NIST によると「サイバーリソースの使用、またはサイバーリソースによって有効化されるシステムの悪条件、ストレス、攻撃または侵害を特定、耐久、回復、適応する能力」と定義されています[1]。セキュリティ対策はもちろんのこと、検出だけでなくより効果的な対応と回復のために組織全体の対応能力を向上させる戦略に移行することが重要です。

## 新たなビジネスの現実

今日のサイバーセキュリティのリーダーは、サイバーセキュリティとリスクの軽減と、事業運営と変革のバランスを取る必要があります。 新しいテクノロジーの採用が加速した結果、IT エコシステムはますます複雑になり、攻撃対象領域は急速に拡大しています。業界全体のスタッフとスキル不足、急速に進化する攻撃者が複合し、サイバーセキュリティの専門家の 76% が、脅威の検出と対応が 2 年前よりも困難であると指摘しています[2]。

この新しいビジネス環境では、侵害やデータ侵害が不可避であることを認識することが、堅牢な対応プログラムを構築し、サイバーレジリエンスを実現するための基本的な前提となります。

### チャレンジ

今日の変化のペースと広がりはかつてないものです。組織が直面するサイバーリスクは、採用している事業運営や変革を可能にする技術が、攻撃者の注目をますます集めているため、増大しています。

### ソリューション

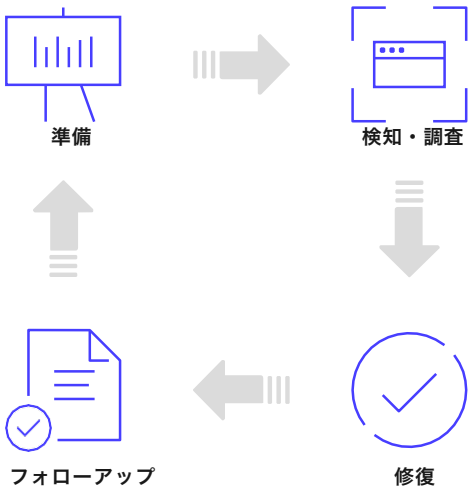
セキュアワークスのインシデント管理リテーナーは、組織がインシデント対応方法の見直しを支援するように設計されており、サイバー防御態勢を強化するための包括的でレジリエンスを重視したアプローチを可能にするだけでなく、サイバーセキュリティによる緊急時にもサポートを提供します。

[1] https://csrc.nist.gov/glossary/term/cyber_resiliency

[2] ESG Master Survey Results, The Threat Detection and Response Landscape, April 2019

セキュアワークスのインシデント対応ライフサイクル (図 1) は、インシデント対応プログラムを構築するためのフレームワークを提供します。これは、事後対応型と従来型の対応能力を、事前対応型で適応性のあるアプローチと組み合わせることの重要性を示しています。準備とインシデント後のフォローアップ活動は、サイバーセキュリティリスクを効果的に管理し、重大なサイバーインシデントの発生時や発生後の混乱やビジネスへの影響を最終的に軽減する上で、極めて重要な役割を果たします。

### 図 1: セキュアワークスのインシデント対応ライフサイクル




## 成熟したインシデント対応

インシデントへの事前対応と準備は、組織のサイバーセキュリティプログラムの重要な構成要素であり、インシデントへの備えはセキュリティ支出への最大の推進力のひとつになりつつあります[3]。しかし、最近の ESG 調査よると、組織のインシデントへの備えは、思っているよりも成熟していないことが示唆されています[4]。

この調査によると、回答者の 92% が、インシデントを迅速に検出して対応する能力について「とてもよい」または「よい」と回答していますが、インシデント対応計画を実施していると答えたのは 68% に過ぎず、その計画を定期的に実行している人はまだ少数です[4]。備えは行われているものの、その体制とレジリエンスの構築には最適でない場合が多く、インシデントに対する備えをさらに調査してみると、推進する主な要因のひとつとして、規制コンプライアンスが挙げられており[4]、戦術的な活動に向かう傾向があることがわかります。

組織は、計画的で組織的なアプローチを確保しながら、備えへの対処の頻度を増やし、さらに深堀りすることで、プログラムを成熟させ、インシデント対応からより多くの価値を生み出すことができます。

[3] ESG Research Report: Cybersecurity Services: omnipresent and heavily invested in, Dec. 2019

[4] ESG Master Survey Results, Incident Readiness Trends, Aug. 2020

## セキュアワークスができること

セキュアワークスのインシデント対応は、14 年以上にわたり、サイバーセキュリティの緊急事態に対応し、お客様の備えと対応のご支援をしてきました。そして当社のインシデント対応チームは、世界中で何千ものお客様のサポートをしてきました。当社のコンサルタントは、20 年にわたる企業の運用セキュリティに関する専門知識、4,000 社以上のお客様の可視性、そして 20 年分の攻撃データを利用し、Counter Threat Unit™ (CTU™) のリサーチャーと脅威ハンターが作成、分析、検証を行っています。

## セキュアワークスのインシデント管理リテーナー

セキュアワークスのインシデント管理リテーナーは、包括的でレジリエンスを重視したアプローチを可能にするように設計されており、サイバー防御力を強化し、サイバーセキュリティの緊急事態が発生した場合にサポートします。セキュアワークスは、お客様のビジネス目標に合わせた階層型リテーナーモデルを提供し、高度なプログラム管理機能により、効果的な事前対応型のアプローチを達成し、導くための専門知識を提供します。

### コンサルティングサービス

インシデント管理リテーナーは、さまざまなインシデント対応およびサイバーセキュリティコンサルティングサービスをご提供します。 当社のコンサルタントは、リスクと影響を最小限に抑えるための主要なサイバーセキュリティプラクティスに関する長年の経験と深い理解を有しております。この専門知識は、数千件にも及ぶサポートから得られた総合的な知識、最新の脅威インテリジェンス、独自のサイバーセキュリティ分析、脅威情報に基づいた方法論によって強化されています。 戦略的・技術的サービスとアドバイザリによって、インシデント対応プログラムとお客様のサイバー防衛能力の構築を支援するための要素をご提供します。

#### インシデント対応計画

インシデント対応およびセキュリティアドバイザリサービスチームの専門家がご提供します。

現状を把握し、対応計画やプログラムを設計

IR 計画、ポリシー、手順の策定

修復と是正の優先順位付け

目標状態の達成に向けたサイバーセキュリティロードマップの定義

- インシデント対応計画の構築とレビュー
- セキュアワークス独自の情報セキュリティ評価 (ISA) フレームワークに基づくセキュリティ管理アセスメント



Secureworks

### ワークショップ・演習

インシデント対応コンサルタントと脅威リサーチャーがご提供します。

脅威とベストプラクティスについて学ぶ

基本的なプロセスでチームをトレーニングする

過去のインシデントから学んだ教訓を確認する

脅威に基づいたシナリオとシミュレーションによる練習

- First Responder ワークショップ
- Lessons Learned ワークショップ
- 机上訓練
- 各種ハンズオンワークショップ

### テストと検証サービス

Adversarial Security Testing チームと CTU Special Ops、IR チームがご提供します。

システム、アプリケーション、人およびチームのテスト

既存の攻撃者の存在を特定

ギャップや弱点を修復

- 脅威ハンティング
- ペネトレーションテスト
- アプリケーションセキュリティテスト
- Red Team テスト

### プログラム管理機能

エンタープライズサービスには、プログラムの進歩とガバナンスを確実に導くための支援を目的とした高度な機能が含まれています。 これには、サイバーセキュリティ緊急事態の発生前、発生中、発生後に、あらゆるレベルで組織横断的な参加を計画し、進捗を追跡し、レビューするための事前のワークショップや、セキュアワークスのインシデント対応の専門家との定期的なミーティングが含まれています。

セキュアワークスは年次 IMR プラニングワークショップを通じて、組織の目的とサイバーセキュリティ戦略を事前に理解し、効果的かつ効率的な対応の準備を支援します。

- 緊急インシデント対応ファンダメンタルズでは、インシデントの処理とエスカレーション・プロセスをレビューし、セキュアワークスのインシデント対応チームがお客様の既存の計画とプロセスを理解し、適時かつ効率的な対応を妨げる可能性のある領域を事前に特定します。
- コンサルティングサービスプランニングでは、組織の目的とサイバーセキュリティ戦略について議論する機会を設け、事前の計画と、セキュアワークスのコンサルティングサービスを活用するためのロードマップを共同で策定します。



Secureworks

四半期ごとのサービスレビューでは、セキュアワークスのインシデント対応の専門家と定期的にやり取りして、結果を確認し、推奨事項を提供し、コンサルティングサービスのロードマップを調整します。エンタープライズサービスには、セキュアワークスのシニアメンバーが提供する年次エグゼクティブ向け報告会が含まれています。この報告会はエグゼクティブを対象に、サイバーリスクに関する洞察、進捗状況、最新情報をお伝えいたします。

**緊急インシデント対応**

サイバーセキュリティの緊急事態が発生した場合、インシデント管理リテーナーは、待機中のグローバルインシデント対応者からのタイムリーなサポートを確保し、さまざまなサイバー脅威シナリオを支援します。セキュアワークスの緊急インシデント対応は小規模な1台のコンピューターシステムの懸念から、事業運営を大幅に混乱または妨害する大規模な企業全体の危機的状況まで、さまざまな種類のインシデントをサポートします。

当社のアプローチは、協調的でインタラクティブなものです。当社はお客様のチームと協力して状況を評価、理解し、対処することで、お客様が適切な行動を取り、サイバーセキュリティ緊急事態の期間とビジネスへの影響を最小限に抑えることができるようにします。当社のチームは、デジタル・フォレンジック調査、マルウェア分析、脅威インテリジェンス分析の機能に加え、脅威の迅速な調査、分析、修復に必要なガイダンスと支援を提供します。

セキュアワークスのインシデント対応は、組織に機能横断的なインシデント支援を提供することで、すべてのインシデント対応のステークホルダーが調整を行い、すべての関係者を相互に定義された対応目標へ導くように設計されています。

緊急インシデント対応のご相談は
**044-380-2888**
**（24 時間 365 日受付）**
までご連絡ください。

サービスの詳細につきましては、
**03-6893-2317**
までご相談ください。
**secureworks.jp**

**セキュアワークスについて**

Secureworks® (NASDAQ: SCWX) は、サイバーセキュリティにおける世界的な先進企業です。当社ソリューションをご活用いただくことにより、お客様やパートナーは攻撃者よりも常に先手を打ち、マーケットに迅速に対応し、ビジネスニーズを満たすことができます。クラウドネイティブの SaaS セキュリティプラットフォームとインテリジェンス主導のセキュリティソリューションの独自の組み合わせにより、20 年以上の脅威インテリジェンスと分析から得た深く広い知見を提供しております。このように、長年にわたるサイバー攻撃の最前線で蓄積した実戦経験に基づく知見を提供するセキュリティプラットフォームは、唯一無二のセキュアワークスだけです。

www.secureworks.jp