

セキュリティ運用支援サービス CEC SOC

CEC SOC概要

高度なオペレーターおよびアナリストで構成された、SOC(Security Operation Center)が監視や分析等を行うセキュリティ運用支援サービス。

24時間365日でお客さまのセキュリティ運用を支援します。

マルチベンダー対応

影響範囲の最小化
恒久対処の支援

ニーズに寄り添った
臨機応変な運用変更

CECSOCの特長

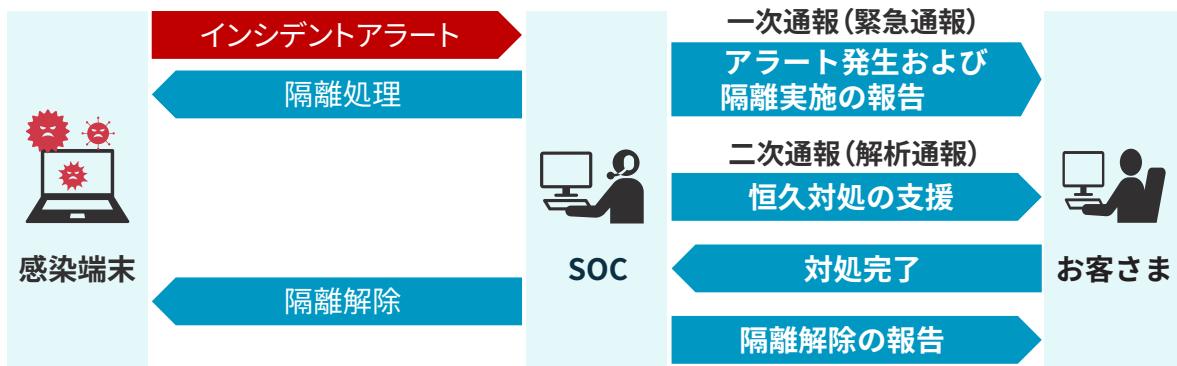


1. 迅速な報告と影響範囲の最小化

- ・検知から一次報告まで30分以内に実施(目標値)
- ・感染と判断した端末を即座にネットワークから隔離し、感染の拡大を防止

2. 同一現象の発生を防止する恒久的な対策の支援

- ・必要に応じて周辺機器のログを調査し、原因究明の上、恒久的な対策を支援
- ・月に一回お客様環境で生じた脅威に関するレポートを作成



CEC SOCの5つの強み

1. 豊富な実績

豊富なSOC実績に支えられた運用サービスを低価格に提供

2. MDR*では実現できない相関分析

ネットワーク機器から社外環境まで、ユーザー環境を6つのゾーンに分けて、相関分析を実施

3. マルチベンダー対応

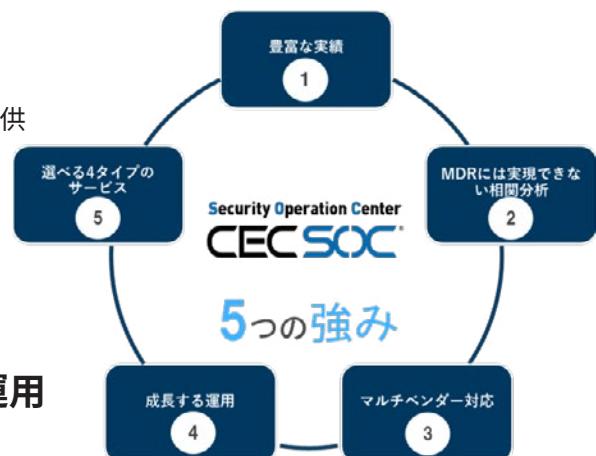
EDR*製品等、市場の需要に合わせ、さまざまなメーカーのセキュリティ製品に対応

4. ニーズに寄り添い臨機応変に成長する運用

セキュリティ運用の開始後も、お客様の細かな仕様に即した柔軟な運用変更が可能

5. 選べる4タイプのサービス

お客様のご要望やご予算に合わせた4タイプのサービスを用意



*MDR : Managed Detection and Response
EDR : Endpoint Detection and Response

※本リーフレットに記載の「CEC SOC」は、株式会社シーイーシーが提供するセキュリティサービスです。

導入効果

Case1 24時間365日の運用・監視によりセキュリティ運用を強化

- 課題：インシデント発生時の影響範囲調査に苦労している
効果：UTM*製品やActive Directoryサーバー等の周辺機器のログを含めて総合的な解析と影響範囲の明確化を実現
- 課題：セキュリティ製品のアラートにどう対応すればよいか分からず
効果：セキュリティ専門技術者により「何が起きているのか」「何をすべきか」を分かりやすくご報告
- 課題：SOCサービス導入後に業務内容が変わり運用を見直したい
効果：より精度の高い監視・分析の実現のために運用計画書の改版を作成

*UTM: Unified Threat Management

Case2 お客様のCSIRT*活動の成長を促進

- 課題：自社でCSIRTを立ち上げたが安定したレベルの運用に苦労している
効果：相談窓口がネットワーク構成やセキュリティ対策等のアドバイス、および技術支援（ソリューション提案を含む）を実施し、CSIRTの成長に貢献
- 課題：CSIRTが成長したことにより運用サービス内容を見直したい
効果：用意された4タイプの運用サービスより、CSIRTの成熟度に沿って不足部分を補う契約へ変更

*CSIRT: Computer Security Incident Response Team

CSIRT成熟度に合わせて選べる4タイプの運用サービス



ユーザーCSIRT

CEC SOC[®]

株式会社 日立システムズエンジニアリングサービス

お問い合わせは

本社：〒220-8132 横浜市西区みなとみらい2-2-1

横浜ランドマークタワー32階

www.hitachi-systems-es.co.jp



*本カタログに記載されている会社名、製品名は、それぞれの会社の登録商標または商標です。

*本カタログに記載されている内容、仕様については、予告なく変更する場合があります。

*本製品を輸出する場合には、外国為替および外国貿易法ならびに、米国の輸出管理関連法規などの規制を御確認の上、

必要な手続きをお取りください。なお、ご不明な場合は、当社営業にお問い合わせください。