SERVICE LINE UP

Cyber Defense Center

インシデントの監視や対応をお客様に代わってSOC・CSIRTが代行します。
サイバー攻撃に迅速かつ適切に対応し、事業のサイバーレジリエンスを高めます。

サイバー攻撃の兆候を早期に発見する（SOC）

巧妙化するサイバー攻撃には、検知・分析の専門家「SOC」で対抗を

SOC*はセキュリティアラートの監視・分析、インシデントの発見を行う組織です。
被害拡大前に異常を検知できるため、多くの企業で導入が進められています。

＊Security Operation Center

「Cyber Defense Center」で解決！

- ログを解析できる専門的な人材がいない
- インシデントの原因を早期に特定したい
- デバイスの増加やリモートワークの影響で監視工数がかかる

Service Menu アラート監視　アラート分析

- セキュリティアナリストを擁するSOCがアラート監視・分析を代行
- サイバー攻撃の予兆や発生を早期に発見・通知

Step 01 ログを収集


リアルタイム監視

Step 02 インシデント分析

分析基盤SIEM*／
セキュリティアナリスト

Step 03 レポーティング

インシデントの報告

＊SIEM（Security Information and Event Management）：ログの収集・分析、インシデントの検知を行うソリューション

ウイルス感染や情報漏えい等のインシデント対応を行う（CSIRT）

被害を最小化し、迅速に復旧するインシデント対応の要「CSIRT」

CSIRT*はインシデントの影響調査や原因の究明、対策を行う組織です。
サイバー攻撃を全て防ぐのは困難なため、侵入を前提に被害最小化を図る体制が求められています。

＊Computer Security Incident Response Team

「Cyber Defense Center」で解決！

- インシデント発生時に適切に対応できるか不安
- セキュリティ人材が不足している
- インシデントの発生自体を抑制したい

Service Menu インシデント対応

- インシデントの分析や対応をCSIRTが代行
- 再発防止まで支援することで、インシデントの発生そのものを抑制

Step 01 インシデント分析
攻撃元／攻撃先、攻撃手法、
影響範囲等の特定

Step 02 インシデント対応
オンサイト／リモート
システムやネットワーク
への対策

Step 03 レポーティング
インシデントの原因や
対応結果の報告

Step 04 再発防止策の検討
暫定対策や恒久的な
再発防止策の検討