CRESCO

AI × SOC により、すべての企業に24時間365日の安心を

CRESCO Managed Security Services



目 次

近年の情報セキュリティ脅威の動向 02 - 05

- 脅威動向と構造変化 03
- 経営への損失インパクト 04
- 現状の課題（監視の空白領域） 05

サービス概要 06 -12

- CRESCO Managed Security Services とは？ 07
- CRESCO Managed Security Services で実現できること 08
- 導入しやすいサービス設計 09
- CRESCO Managed Security Services の全体像 10
- 基本サービス・オプションサービス 11
- 導入プロセス 12

近年の情報セキュリティ脅威の動向

脅威動向と構造変化

企業を対象としたサイバー攻撃は「件数の増加」ではなく、**「構造的変化」** が始まっており、従来の対策だけでは対応しきれない場面が増えています。

- AIを駆使した攻撃者がリアルタイムフィッシングやランサムウェアを自動化・高度化
  （**フロンティアAI時代の構造変化**）
- 証券会社を装ったフィッシングによる不正インターネット取引の被害額は **約7,400億円** に達した
- ネットバンキング不正送金の発生件数は **4,677件**、被害額は **年間102億円越** で過去最高を記録
- 2025年のランサムウェア被害は **226件** と高水準で継続
  大企業も被害を受けており業種・規模を問わず標的に

参考：警察庁サイバー脅威レポート最新版｜昨年を総括、過去最悪の被害額が並んだ1年間
サイバー空間をめぐる脅威の情勢等

攻撃手法は「防御対策よりも速いペースで変化している」と指摘されており、より 継続的な監視と対応が求められる状況 になっています

経営への損失インパクト

CRESCO

サイバーインシデントは事業継続にも影響を及ぼし、対応しない場合の損失は財務・信頼・規制の複数の影響が重なる可能性があります。

財務損失

不正送金・補償費用・復旧費用が直接発生。金融機関は顧客資産を預かるため、インシデント発生と同時に損害が確定する可能性があります。被害額はネットバンキング不正送金だけで **年間102億円超**（業界全体）に上ります。

事業停止リスク

コアバンキング停止による **取引遅延・顧客苦情・評判悪化。復旧に数日～数週間 を要するケースも存在**し、顧客離れや株価下落につながります。

規制・法的リスク

金融庁サイバーセキュリティガイドライン(2025年10月改訂) では、経営陣の**善管注意義務違反による損害賠償責任**が明示され、組織としての管理体制強化が求められています。

参考：
金融分野におけるサイバーセキュリティ対策について

サイバーセキュリティは「IT部門の問題」ではなく、
経営層を含めた全社的な取り組みが重要視されています

現状の課題（監視の空白領域）

CRESCO

複数の調査・監査結果から、セキュリティ対策の導入は進展している一方で、運用・監視との間にギャップが存在し、アラートが十分に活用されないままインシデント検知が遅延するリスクがあります。

空白① 夜間・休日　⚠ **インシデントの発見が遅れる可能性**

攻撃者は人員が手薄な時間帯を狙う。
24時間365日の監視体制を自社で維持するには、高い人件費と専門人材の確保が必要となる。

空白② ログはあるが分析されていない　⚠ **脅威が埋もれたまま見逃してしまう可能性**

ログやアラートは生成されているものの、分析体制や運用プロセスが不足している場合、十分に活用されないケースがある。
結果として、重要なアラートが対応されないまま見過ごされる可能性がある。

空白③ セキュリティ専門人材の不足　⚠ **育成コスト増大・慢性的な人材不足リスク**

IPA「情報セキュリティ白書2025」でもセキュリティ人材不足が深刻な課題として指摘されており、金融機関でも例外ではない。

参考：プレス発表「情報セキュリティ白書2025」PDF版の公開

対策導入だけでは不十分であり、
運用・監視まで含めて初めてセキュリティは機能します

サービス概要

CRESCO Managed Security Services とは？

CRESCO Managed Security Servicesは、豊富な経験と広範な知識を有するセキュリティアナリストが、24時間365日体制でお客様環境のセキュリティ監視・分析・対応支援を行うマネージドセキュリティサービスです。

Microsoft SentinelとAI分析を活用したSOC監視を中核に、初動対応支援、デジタルフォレンジック、セキュリティコンサルティングなどを提供し、お客様のセキュリティ運用を包括的に支援します。

お客様の課題や運用体制に応じてサービスを柔軟に組み合わせることで、スモールスタートから段階的な拡張まで対応可能です。

このような課題はありませんか？

- **導入済みのセキュリティ製品やログを有効活用したい**
- **ガイドラインや規制への対応を強化したい**
- **24時間365日の監視体制を実現したい**
- **セキュリティ対策を包括的に強化したい**

CRESCO Managed Security Services で実現できること



SIEMとAI分析の活用による高度なセキュリティ監視

Microsoft SentinelとAI分析を活用し、大量のセキュリティイベントから重要な脅威をリアルタイムに検知します。自動トリアージにより誤検知を抑制し、運用負荷を軽減しながら重要なインシデントを効率的に抽出します。



業界特有の脅威に対応するセキュリティ運用

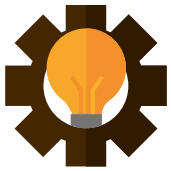
金融業界をはじめとする業界特有の脅威への対応実績を活かし、各業界のリスクや攻撃傾向に応じた検知ルールを継続的に見直し・改善します。また、金融庁ガイドラインなどの規制対応に必要となる各種レポートや報告資料の作成も支援するなど、セキュリティ運用をトータルでサポートします。



24時間365日のSOC運用体制

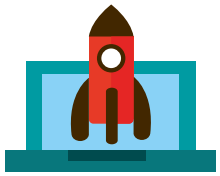
グローバルSOC体制により、24時間365日の有人監視を実現します。夜間・休日を含めた継続的な監視により対応の空白時間を低減し、脅威の早期発見から初動対応までを迅速に支援します。

導入しやすいサービス設計



既存環境を活用したスムーズな導入

導入済みのファイアウォール、EDR、クラウドサービスのログを活用し、新たな投資を抑えながら導入できます。



最短1か月で監視体制を構築

既存環境との連携により短期間で導入でき、早期にセキュリティ監視を開始できます。



スモールスタートに対応

PoCや一部システムから導入し、お客様の運用状況や予算に応じて段階的に対象範囲を拡大できます。

CRESCO Managed Security Services の全体像

お客様環境の各種ログをMicrosoft Sentinelに集約し、AI分析とセキュリティアナリストによる24時間365日の監視を実施します。脅威の検知・通知を起点に、初動対応・原因調査・再発防止まで、ワンストップでご支援します。

お客様環境 (各種システム・サービス)

- ファイアウォール (FW)
- EDR／端末
- サーバ・オンプレ機器
- クラウドサービス
- ネットワーク機器
- 業務システム・アプリ

ログ
アラート

CRESCO Managed Security Services（SOC）

データ基盤

- Microsoft Sentinel
- AI分析

監視・分析

24

セキュリティアナリストが
24時間365日体制で監視・分析

1 収集・正規化 → 2 AI分析 → 3 脅威検知 → 4 トリアージ（重要度判定） → 5 アラート通知

お客様への提供

- アラート通知
- 対応状況の共有
- ポータル
- 月次レポート
- 定例ミーティング

24時間365日の継続監視と支援により、お客様のセキュリティをトータルでサポート

基本サービス・オプションサービス

CRESCO

基本サービス

SOC（24時間365日監視）

ログ監視・AIログ分析・インシデント検出と通知を提供。日本語・英語・ベトナム語によるサポートに対応します。
お客様向けポータルを標準提供し、検知状況や対応履歴、月次レポートをいつでも確認できます。

オプション **EDR（端末監視）**	エンドポイントの挙動を継続的に監視し、マルウェア感染や不審な操作、内部不正の兆候を早期に検知します。**SOC監視と連携**することで、端末レベルの脅威発見から調査・対応までを迅速に実施し、被害拡大の抑制を支援します。
オプション **インシデント初動対応**	セキュリティインシデント発生時に、状況把握から封じ込め、影響範囲の確認、関係者への報告までを迅速に支援します。**豊富な対応経験を持つアナリストが初動対応をサポート**することで、お客様の負荷軽減と事業影響の最小化に貢献します。 ※オンサイト対応は一部地域で未対応となります。
オプション **デジタルフォレンジック**	インシデント発生後に侵入経路や原因、影響範囲を詳細に調査します。ログや端末情報などの証跡を分析し、**再発防止に向けた課題を整理**するとともに、関係者向け報告や原因分析に必要な**報告書作成を支援**します。
※2027年度リリース予定 **オプション** **プライベートSOC**	**お客様専用のSOC環境を構築**し、監視ルールや運用フローを個別要件に合わせて設計・運用します。高いセキュリティ要件や独自の運用ポリシーにも柔軟に対応し、きめ細かな監視サービスを提供します。
その他 **セキュリティコンサルティング**	セキュリティ戦略の策定からリスクアセスメント、ルール整備、教育・訓練まで幅広く支援します。各種ガイドラインや業界規制への対応もサポートし、**組織全体のセキュリティ成熟度向上**に向けて継続的に伴走します。

※この他に、PoCやサイバー攻撃可視化サービスなどもご用意しておりますので、まずはお問合せください。
※Microsoft Sentinel以外にも、Sumo LogicなどのSIEM製品に対応した「MSS for SIEM」を提供しています。

導入プロセス

ご契約から**最短1か月で運用開始**できる、シンプルで確実な導入プロセスを提供します。

所要期間：約1週間

STEP 1
ヒアリング

- セキュリティリスクの整理・監視対象システム/範囲の特定
- 収集ログのヒアリング
- お客様環境の把握と要件確認シートの作成

所要期間：約2週間

STEP 2
要件定義・設計・準備

- 標準ルール・監視ルール・アラート通知ルールの設定
- カスタムルールの追加（企業独自ルール・過去インシデント対応ルール）
- ログ収集設定・運用テスト

所要期間：約1週間

STEP 3
稼働支援

- 運用テスト完了・関係者向け運用トレーニング実施
- お客様向けポータルのご提供

本番稼働

STEP 4
運用開始

- 24時間365日体制での監視・エスカレーション
- 月次レポート・セキュリティレポート発行
- 検知ルールの継続チューニング・脅威情報の随時反映

もっと詳しく聞きたい方は、
お気軽にご相談ください。

お問い合わせフォームはこちら

https://wakuwaku.cresco.co.jp/contact

人が想い描く未来、その先へ CRESCO





本書に含まれる情報は、貴社内部でのご検討、評価の目的のために提供されるものです。貴社内でのご使用、複製、開示は、この目的のために必要最小限の範囲でお願いします。貴社との間で正式な契約が成立した場合には、その規定に従ってこれをお取り扱いいただくものとします。なお、貴社にて既に知得されている情報については、これらの制限は及びません。

※本資料に記載されている会社名、商品名は各社の商標または登録商標です。

お問い合わせ

株式会社クレスコ

〒108-6026 東京都港区港南2-15-1
品川インターシティA棟26階

https://wakuwaku.cresco.co.jp/contact