報道関係者各位
（参考資料）

2021 年 8 月 2 日
株式会社インターネットイニシアティブ

# IIJ、SOCサービスの機能を拡充し「EDR運用オプション」を提供開始

*-- EDR製品の導入から運用、インシデント一次対応までを提供し、お客様の負担を軽減 --*

当社は、セキュリティオペレーションセンター（SOC）でお客様システムのセキュリティログを監視し、インシデント対応を行う「IIJ C-SOC サービス」において、米 CrowdStrike 社の EDR（※）製品「CrowdStrike Falcon®」の導入から運用までを提供する「EDR 運用オプション」を本日より提供開始いたします。本オプションでは、EDR ツールを利用して PC などのユーザ端末の動作を常時監視し、ログの収集、調査・分析、インシデントの一次対応までを、IIJ の専任セキュリティアナリストがお客様に代わって行います。本オプションを導入することにより、お客様は EDR 運用にかかる作業負担を軽減でき、インシデント発生時の迅速な検知と対応が可能になります。

※EDR（Endpoint Detection and Response）：PC などのユーザ端末（エンドポイント）で起きている挙動（ファイルやプロセスの動き、レジストリ変更など）を自動的に収集した上で、さらに攻撃プロセスを関連付けて調査の迅速化や正確性の向上、拡散範囲の特定などを実現する製品です。

## 背景

企業においてテレワークやクラウドサービス利用が増えていることを背景に、社内ネットワークを経由せずに社外から直接クラウドサービスにアクセスするユーザ端末（エンドポイント）をターゲットにした攻撃が増えており、企業にとってエンドポイントセキュリティの強化が課題になっています。

EDR は、マルウェア感染後の異常動作や、ウイルス対策ソフトでは検出しにくいファイルレス攻撃などエンドポイントでしか特定できない不正な挙動を検知できるほか、プロセスの強制停止、端末の論理隔離などの制御機能を備えており、多くの企業で導入が進んでいます。しかしながら、EDR で発生したアラートをもとに状況を把握し原因追求や脅威への対処を行うには、高度なスキルと 24 時間 365 日インシデントに対応できる体制整備が必要であるため、有効活用できていないケースが多くなっています。そのような導入・運用にかかる課題を解決すべく、このたび、IIJ C-SOC サービスの EDR 運用オプションを提供することとしました。EDR 製品は、世界での導入実績が豊富で評価も高い CrowdStrike を採用し、今後、対応製品を順次追加していく予定です。

* CrowdStrike 社は、クラウド型 EDR 市場において「リーダー」に格付けされており、IDC による 2020 年クラウド型エンドポイントセキュリティ市場調査（Worldwide Corporate Endpoint Security Market Shares, 2020）で 1 位を獲得しています。

## 「IIJ C-SOC サービス EDR 運用オプション」の概要と特徴

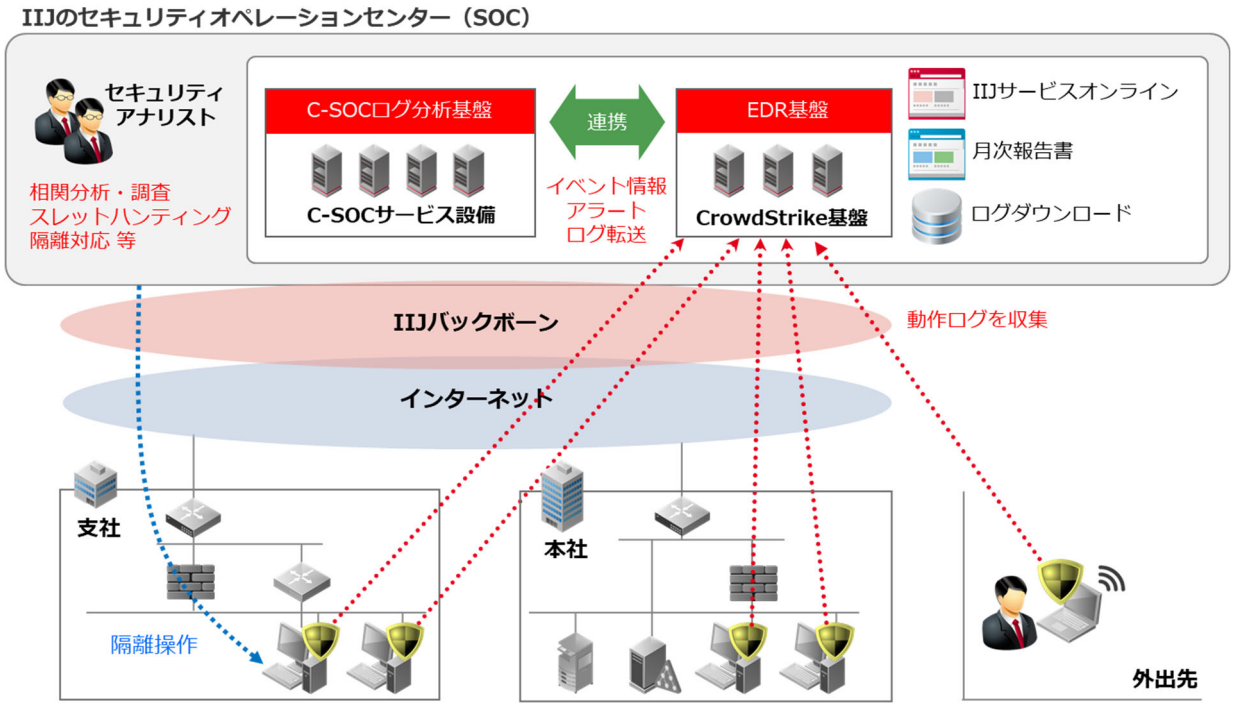
IIJ SOC の専任セキュリティアナリストが、CrowdStrike Falcon®の導入から、運用、インシデント一次対応までをお客様に代わって行います。また IIJ 独自の情報分析基盤（※）と連携することで精度の高いインシデント検知を行います。

※情報分析基盤では、ISP として保持するバックボーントラフィックや DNS 情報、お客様に提供しているセキュリティサービスから得た膨大なログやイベント情報を集約し、ビッグデータ解析を経て、最新の脅威動向に対応し得るセキュリティ情報を生成しています。

・ EDR 製品の高度な運用を提供
お客様側では、監視対象となるクライアント機器にエージェントをインストールしていただきます。IIJ のセキュリティアナリストは、監視対象機器から収集した動作ログをもとに、悪性ファイルのダウンロード、起動、動作等ネットワーク上では発見できない不正な挙動の検知、分析、一次対処を 24 時間 365 日の体制で行います。CrowdStrike の基盤と IIJ のサービス基盤を連携させ、EDR 以外の別製品との相関分析や、スレットハンティング等の調査を行うことで、精度の高いセキュリティ運用を実施します

・　お客様側でのインシデント一次対応が不要
　インシデント発生時には、お客様との事前の取り決めに従い、IIJ のセキュリティアナリストがユーザ端末を論理的に隔離するなど能動的な対応を行い、お客様への影響を最小化します。また、IIJ C-SOC サービスプレミアムと本オプションを組み合わせることで、インシデントハンドリングに必要な技術的な作業をすべて IIJ の SOC で担います。大規模な運用体制を維持しなくても一次対応が可能となり、お客様は再発防止策などの対応に注力いただけます。

イメージ図




参考価格（1,000 人規模で利用する場合）
- 初期費用　2,500,000 円
- 月額費用　1,500,000 円（ライセンス費用を含みます）

➢　IIJ C-SOC サービスの詳細については、以下サイトをご覧ください。
　https://www.iij.ad.jp/biz/c-soc/

IIJ では今後とも、「安全をあたりまえに」をコンセプトとするセキュリティ事業ブランド「wizSafe（ウィズセーフ）」の下に、インターネットを誰もが安心して安全に使える社会インフラへと発展させるべく、活動してまいります。

■　エンドースメント
CrowdStrike のアジア太平洋および日本のチャネルアンドアライアンスのヴァイスプレジデントであるジェフ・スウェイン（Geoff Swaine）は次のように述べています。
「IIJ C-SOC サービスと CrowdStrike の組み合わせは、日本の企業がサイバー脅威に対する防衛力を向上させるのに非常に役立ちます。強力なサイバーセキュリティ体制を構築することは、企業にとって、増大するサーバー攻撃のリスクから守り続けるために不可欠なのです。」

報道関係お問い合わせ先
株式会社インターネットイニシアティブ　広報部　荒井、増田
TEL：03-5205-6310　FAX：03-5205-6377
E-mail：press@iij.ad.jp URL：https://www.iij.ad.jp/