# X-SOC FOR CROWDSTRIKE

株式会社クロスポイントソリューション (以下、CP-SOL) は、セキュリティインシデントの検知から対応までを一気通貫で対応する『**X-SOC (クロス ソック) サービス**』を 2021 年 8 月に立ち上げ、その第一弾として CrowdStrike を活用した『**X-SOC for CrowdStrike**』をリリースしました。

駒形 秀雄
セキュリティソリューション事業部長

## はじめに

『**X-SOC (クロス ソック) サービス**』及び『**X-SOC for CrowdStrike**』の特徴やサービスのこだわりポイント、お客様のメリットなどについて、サービス企画からリリースまでに携わった 2 人のマネージャーに伺ってみます。【広報担当】

## X-SOC サービスの立ち上げにあたって

**Q: X-SOC サービス立ち上げのきっかけは何ですか？**
A: 当社の 2021 年度事業計画の目玉として、マネージド・セキュリティ・サービスを事業化することを経営が宣言し、2020 年度 4Q に準備に着手しました。2021 年度 1Q にインキュベーションとして SOC ビジネス準備室を設立し、サービス検討を開始しました。【駒形】

**Q: なぜマネージド・セキュリティ・サービスだったのでしょうか？**
A: CP-SOL はこれまでにインシデントレスポンスサービスを推進させていただいていますが、MSS を提供するに至った契機は、サイバーセキュリティ教育を事業化した子会社「クロスポイントセキュリティジム (以下、CP-SG)」を設立したことが大きいです。
CP-SG が提供するサイバーセキュリティ教育は、サイバーセキュリティ先進国のイスラエルで作られており、イスラエルのレッドチームがサイバー攻撃を仕掛け、受講者がインシデントに対応するといった SOC アナリスト育成の演習メニューを持っています。
お客様向けにご提供するほか、当社の社員を実戦的なセキュリティ人材にするための教育メニューとして活用しています。【駒形】

**Q: サービス名称「X-SOC (クロス ソック)」の由来を教えて下さい。**
A: X(エックス)には、「未知数」・「何が入るか分からない」という意味がありますので、「あらゆるセキュリティ製品の SOC ＝ マルチベンダーSOC」の意味付けをし、X(エックス) を社名の一部にかけて “クロス” と呼ぶこととしました。【駒形】

過検知を限りなく減らして運用に入るとアラートはほぼ出ない。
また、多層防御環境下では EDR のアラートは少ない

**Q: X-SOC サービスのこだわりポイントはありますか？**
A: 既に多くの MSS ベンダーがサービス提供されている中、当社は後発でもあり、マルチベンダーSOC である以外に、大きく 2 つの特徴を入れました。
1 つは、ID 数課金ではなく「対応件数課金」を採用したことです。
例えば、3 万 ID のお客様でも月間の対応件数を 3 件や 5 件などにセットすることで、ID 数課金に比べて安価になり、納得感のある価格をご提示できると考えています。【駒形】

**Q: ID 数に比例して、対応件数が多くなるのではありませんか？**
A: はい、一般的にはそうですが、お客様の事例ではセンサー数が約 13,000 で過検知チューニング後のアラート発生はほぼ 0 件です。
他のお客様のケースでは、クラウドセキュリティ対策の効果が顕著でエンドポイントに情報を取り込む前に相応の対策が効いていることで、約 1 年間でアラートは 5 件に満たないぐらいです。このお客様のセンサー数は約 5,000 です。【駒形】

**Q: もう１つのこだわりポイントは何でしょうか？**
A: 脅威度(Severity)によって対応を変えたい、感染したホストによって対応を変えたいと思われるお客様は多く、サービスで一律のプロセスや判断基準では、様々なお客様の要望をカバーできないことからプロセスのカスタマイズを取り入れています。
例えば、PC と業務サーバーでは、ネットワーク隔離した時の業務インパクトが大きく異なることから、PC の場合は即時隔離、サーバーの場合は調査・分析・報告をしてご判断いただいてからネットワーク隔離というプロセスにされるお客様が多いです。【駒形】

お客様の要望に沿うためにプロセスのカスタマイズに対応

羽山 豪
セキュリティソリューション事業部
SOC サービス推進部 部長

## X-SOC for CrowdStrike について

**Q: X-SOC サービスの第一弾に CrowdStrike を選んだ理由を教えて下さい。**
A: 2 つ理由があります。1 つ目の理由ですが、当社は CrowdStrike を活用したインシデントレスポンスを以前からご提供しており、アラートトリアージなどの過去のナレッジや、サービス仕様書・手順書の一部を活用できることがあります。
2 つ目の理由は、CrowdStrike の SIEM が Splunk ベースであることから、エンドポイントログ分析の際に Splunk の取り扱い経験が活かせることです。当社は Splunk エンジニアを増やしており当社の方向感とも合致しています。【羽山】

**Q: X-SOC for CrowdStrike の特徴、お客様のメリットは何でしょうか？**
A: X-SOC サービスの特徴やメリットと同じです。CrowdStrike の活用という点で例を挙げると、お客様とのインシデント対応状況の共有は CrowdStrike のポータルで行います。特別な仕組みを準備することなくサービスをご提供することでお客様向け価格を低減することに寄与しています。
EDR 製品として CrowdStrike を選ぶメリットは、EDR/NGAV だけでなく、資産管理や脆弱性管理などの機能を装備できることや、他社のセキュリティ製品と連携が可能でセキュリティの高度化が図れることが挙げられます。【羽山】

**Q: 他社のセキュリティ製品と連携が可能とは？**
A:「他社のセキュリティ製品が検知したアラートを元に CrowdStrike で自動ネットワーク隔離する」などが可能です。連携可能なセキュリティ製品のカテゴリーは、NDR・クラウドセキュリティ・CASB・UEBA など幅広く、プロダクトしての拡張性が高いと考えています。
X-SOC サービスとしても、EDR 以外のセキュリティ製品に順次対応し、統合 SOC サービスに拡張していく予定です。【羽山】

CrowdStrike はプロダクトとしての拡張性が高い

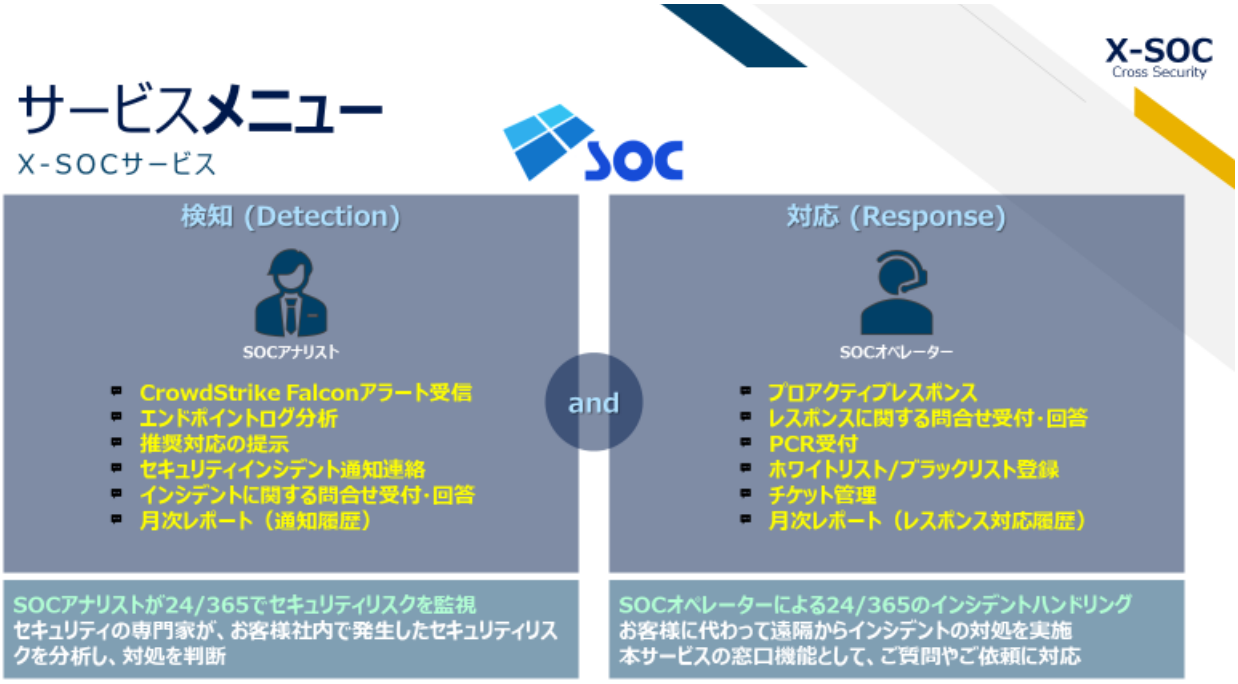
**Q: 他にはありますか？**
A: 当社は CrowdStrike 社の MSSP (Managed Security Service Provider) として特別な契約を締結しており、例えば 1ID からでもライセンスをご提供できます。5ID・10ID など少ない単位でミニマムスタートをしたい場合は、ご相談いただければと思います。
他には、導入が早いことが挙げられます。サービスをカスタマイズ無しでご利用いただく場合は、プロセス変更が不要なため、ライセンスの準備が整い次第すぐにサービスを開始できます。【羽山】

## まとめ

X-SOC サービスは、CP-SOL のインシデントレスポンスサービスの経験に基づいたこだわりが詰まったサービスでした。
X-SOC for CrowdStrike も、製品の利点をそのまま活かした、安価で拡張性の高いサービスだということが分かりました。
『X-SOC for CrowdStrike』にご興味がありましたら、是非営業担当までお問合せ下さい。【広報担当】

## サービスメニュー (CrowdStrike ライセンス)


## サービスメニュー (X-SOC サービス)




**株式会社クロスポイントソリューション**
〒104-0032 東京都中央区八丁堀 3-14-2 東八重洲シティービル