ホワイトペーパー

セキュリティオペレーションセンターの効率化によるサイバーセキュリティの強化

組織のニーズに最も適した SOC モデルを見極める。

SOPHOS

エグゼクティブサマリー

サイバーセキュリティ環境は常に変化しており、脅威はますます巧妙化し広範囲に及んでいます。このような環境下において、セキュリティオペレーションセンター (SOC) は、組織がサイバーインシデントを迅速に検知、分析、対応するために不可欠になっています。組織は、自社で SOC を運用するのか、一部業務を外部ベンダーに委託するのか、あるいはすべてをアウトソースするのか、自社にとって最適なモデルを見極める必要があります。その上で、SOC のパフォーマンスを適切な指標で評価し、セキュリティ体制を維持・強化しながら、ビジネス目標との整合性を確保することが求められます。

63% の企業

人材不足やスキル不足のためにランサムウェアの被害を受けた。[1]

現代のサイバーセキュリティ環境における SOC の役割

デジタル化が進む中で、サイバー攻撃の脅威も増加し、サイバー犯罪者や国家支援を受けた脅威アクターによる高度で巧妙な攻撃が常態化しています。最近では、最初に侵入されてからランサムウェア攻撃が展開されるまでの期間が平均でわずか 2 日にまで短縮されており、懸念すべき状況になっています。[2] さらに、サイバーセキュリティ業界は深刻な人材不足に直面しており、自社での SOC の構築、運用、維持が一層困難になっています。

SOC は、セキュリティインシデントの特定、調査、対応を専門に担う組織です。SOC の具体的な役割には、資産管理、変更管理、脆弱性管理、セキュリティイベント管理、インシデント管理のほか、脅威インテリジェンスの活用や、自動化や品質保証などの DevOps 関連活動も含まれます。SOC は組織のあらゆるセキュリティ分野を直接管理するわけではありませんが、セキュリティ問題への対応を調整する重要な役割を担っています。SOC の具体的な使命や目標は、組織のリスク許容度、業界、成熟度、使用しているツールやプロセスなどによって大きく異なる場合があります。

人材不足

サイバーセキュリティ業界は依然として深刻な人材不足に直面しています。

SOC モデルの種類

SOC モデルにはそれぞれ異なる特徴や利点があり、その中から自社に最適なモデルを選択することができます。

自社で運用する SOC モデルは、専任チームが継続的に運用できるだけの十分な資金力を持つ組織が採用することが多くあります。このような自社運用型 SOC でも、侵入テスト、高度な脅威ハンティング、脅威インテリジェンスなどの専門的な機能を外部ベンダーに委託する場合があります。また、大規模な組織や拠点が分散している組織では、複数の SOC を統一された指揮体制のもとで運用する「階層型モデル」が採用されることもあります。

ハイブリッド型 SOC は、社内リソースと外部サービスを組み合わせ、外部ベンダーとの連携を通じて、自社に合わせたセキュリティ体制を構築するモデルとして、近年普及が進んでいます。セキュリティサービスプロバイダーは、一般的に 24 時間 365 日体制の監視とアラートトリアージ、インシデント調査、脅威ハンティング、専門化による支援を担当します。これにより社内チームは、セキュリティアーキテクチャや設計、ポリシーやコンプライアンス管理、リスク軽減、セキュリティ意識向上トレーニング、修復作業を内製化する場合の対応計画の実行などに、リソースを集中できるようになります。この SOC モデルは、柔軟な運用が可能で、特定スキルの不足や予算の制約といった課題にも対応しやすいため、多くの組織にとって非常に魅力的な選択肢となっています。

すべての運用を外部ベンダーにアウトソースする SOC モデルは、サイバーセキュリティの監視および対応業務を、包括的なサードパーティサービスとして提供してもらう形態です。必要な専門知識が社内に不足している組織が、基本的な機能を備えた SOC を迅速に立ち上げたい場合、このモデルを選択し、実績のある MDR プロバイダーに SOC 業務を委任することができます。組織は外部ベンダーの力を活用しながら、自社の既存 IT およびセキュリティテクノロジーと連携させ、環境全体にわたって広範な可視化を実現し、インシデント対応活動を調整できます。

ご存知でしょうか？

ランサムウェア攻撃の 88% は営業時間外に発生しています。[2]

自社に最適な SOC モデルとは？

組織にとって最適な SOC モデルを決定するには、全体的なリスクプロファイルなど、いくつもの要因を考慮しなければなりません。許容できるリスクレベルと、サイバーセキュリティ予算のバランスを慎重に見極める必要があります。検討すべき重要事項を以下に示します。

1. 社内リソースの制約 (専門知識や人員・能力の有無)
2. 自社で運用すべき業務範囲と外部に委託すべき範囲のバランス
3. セキュリティ運用の現在の成熟度
4. 専門スキルを持つ人材の採用、育成、定着に関する課題
5. 新しいテクノロジーを継続的に取り入れ、進化し続ける脅威やアクティブアドバーサリーの手法を未然に防ぐ必要性
6. IT 部門、法務、リスク管理、コンプライアンス、その他の業務部門との部門間連携の重要性

どのモデルを選択するにしても、そのモデルの選択が妥当であり、必要なリソースを長期的に確保するための、根拠ある計画や提案を立てることが重要です。SOC の機能が、あらかじめ定めた設計方針や運用目標に沿っているかどうかを、定期的に評価し見直すことも不可欠です。

多くの組織がサイバーセキュリティ人材の不足に直面しており、24 時間 365 日体制で稼働する SOC を自社のリソースだけで構築・維持するための十分な予算を確保できないケースも少なくありません。また、経験豊富な CISO (最高情報セキュリティ責任者) は、サイバーセキュリティ運用に対する監督と統制を維持することで、組織全体の長期的な持続可能性を確保することの重要性を理解しています。そのため、SOC モデルの検討にあたっては、以下のような点も考慮する必要があります。

ハイブリッド型 SOC モデルの利点

ハイブリッド型 SOC モデルは、自社運用型とアウトソース型の両方の利点を効果的に融合した形態であり、他のモデルにはない独自の強みを備えています。組織は、サードパーティプロバイダーの専門性と効率性を活用しながら、自社のニーズに合わせてセキュリティ運用をカスタマイズし、一定のコントロールを維持することが可能です。

ハイブリッド型 SOC の主な利点の 1 つは、経験豊富なセキュリティ専門家の支援を受け、信頼性の高い脅威インテリジェンスを活用できる点にあります。さらに、スケールメリットも享受できるため、効率的かつ効果的なセキュリティ運用が可能となります。これらの専門家は、多様な脅威に日々対応している大規模な組織に所属しており、サイバーセキュリティ分野の最新動向を常に把握しています。急速に変化する脅威環境に対応しなければならない中で、自社の単独チームだけでは、このように幅広く豊富な経験や知識を得ることは困難です。

さらに、サードパーティプロバイダーと提携することで、社内チームが稼働していない夜間、週末、祝日を含め、24 時間 365 日体制の継続的な監視が可能になります。

ハイブリッド型 SOC は、検知システムの最適化にも役立ち、アラート疲れを大幅に軽減し、インシデント対応の平均時間 (MTTR) を短縮できます。また、専門的な脅威調査に伴う多額のコストを削減できることも、ハイブリッド型 SOC の重要なメリットです。外部パートナーが調査を担うことで、新たな脅威に対する継続的な検知が可能となります。

さらに、社内リソースを重要な IT、テクノロジー、コンプライアンス関連の課題に集中させる一方で、SOC パートナーがセキュリティインシデント対応に専念できる体制を構築することが可能です。このような役割分担により、リソースと専門知識を効率的かつ効果的に配分できます。この体制によって、IT 部門や法務、リスク管理部門なども、それぞれのセキュリティ業務により集中できる環境が整います。

サイバーセキュリティトレーニングには時間とコストがかかりますが、ハイブリッドモデルでは効率化されます。外部プロバイダーのスタッフは、フォレンジック、マルウェア解析、インシデント対応、クラウドセキュリティなど、サイバーセキュリティのあらゆる分野において最新の知識とスキルを備えています。これにより、社内チームはサイバーセキュリティ全般にわたる専門性を維持する負担から解放され、自社のビジネスにとって最も重要な領域にリソースを集中させることができます。

ハイブリッド型 SOC モデルは、組織のリスク許容度に応じて運用を階層化し、対応を柔軟に調整できる点も特長です。これにより、効果的で的確なセキュリティ対策が可能になります。さらに、ハイブリッド型 SOC はコスト削減効果が高く、中小企業だけでなく、一部のセキュリティ機能のアウトソースを検討している大企業にとっても魅力的な選択肢となっています。

SOC 効果の測定

選択した SOC モデルに関わらず、SOC の効果を評価するには、セキュリティ環境や SOC リソースの有効性を反映する指標を活用することが不可欠です。以下に示す指標や関連データを、リアルタイムの件数に加え、週次・月次・四半期単位の統計としてダッシュボードで可視化し、SOC の対応力や調査品質を継続的に監視および評価することが推奨されます。

セキュリティ環境に関する指標は、潜在的な脅威の範囲や量、組織が脆弱なポイント、組織がリスクの影響を受けうる範囲や規模を把握するための洞察を提供します。例えば、受信した疑わしいまたは悪意あるメールの件数、外部システムに対するスキャンや攻撃の試行回数、発生源別のセキュリティインシデント件数などの指標があります。

SOC の有効性を評価する際、指標はリスク削減や法規制遵守などのビジネス成果に結びつく、明確に定められたポリシーやセキュリティ体制の目標に対するパフォーマンスを追跡する必要があります。具体的には、対応のスピードや調査の質、セキュリティスタッフが各活動に費やした時間の内訳、コンプライアンスカテゴリ別のインシデント件数、アタックサーフェスの縮小に関わるエンジニアリング作業量などを追跡します。主要な指標には、調査のトリアージに要する時間、修正対応が行われた調査件数、プロアクティブな脅威ハンティングを起点とした修正件数、そして深刻度別に分類された修正済み脆弱性の件数などが含まれます。

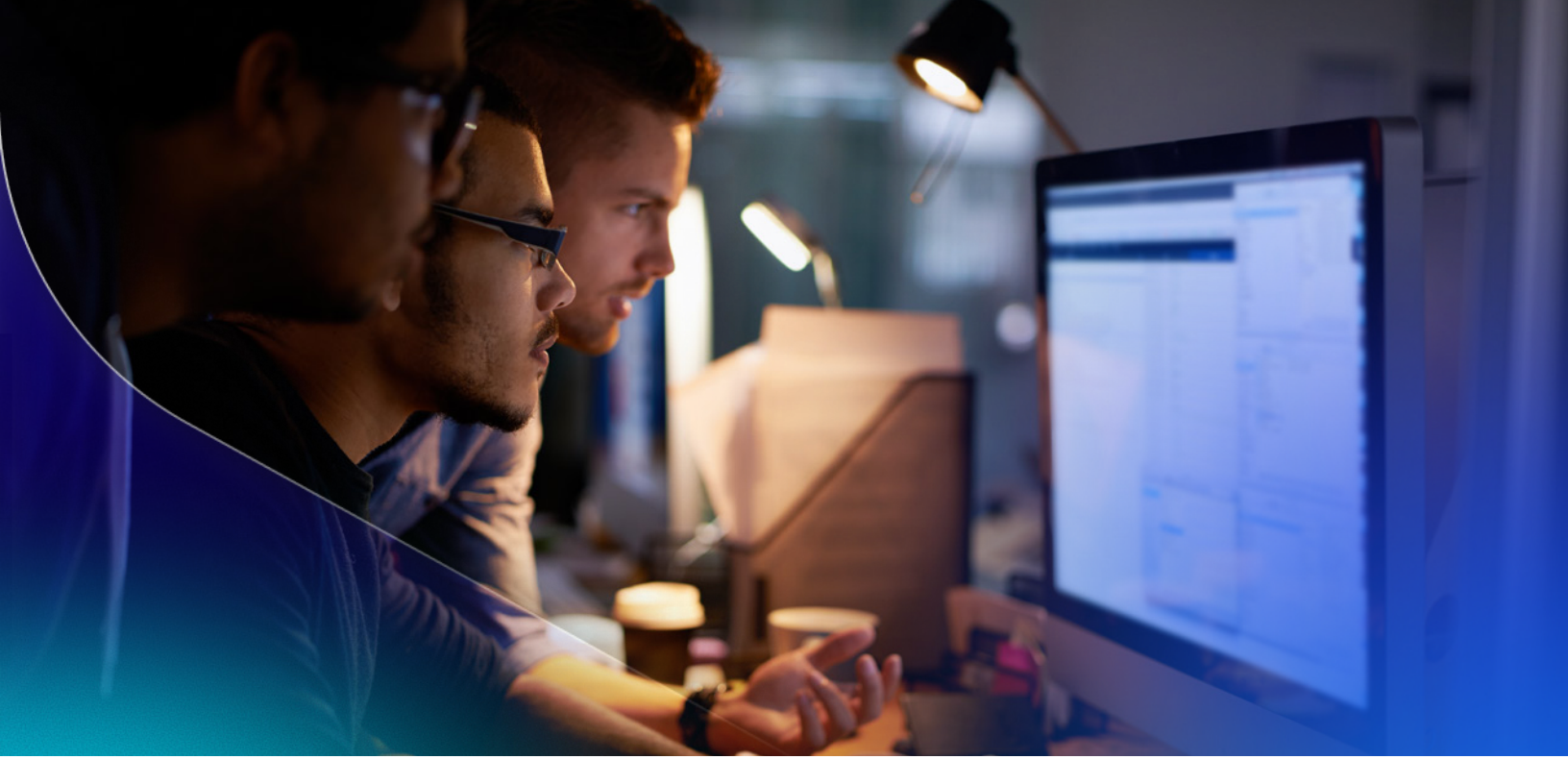
これらの指標を定期的に監視することで、組織は SOC が効率的に運用されているだけでなく、組織全体にわたるセキュリティ体制やビジネス目標にも確実に貢献していることを確認できます。

指標の要件：

- 潜在的な脅威の範囲と量に関する洞察を提供する
- 組織が脆弱なポイントを特定する
- 組織がリスクの影響を受けうる範囲や規模を把握する
- 定められたポリシーやセキュリティ体制の目標に対するパフォーマンスを追跡する

主要な指標：

- 調査のトリアージに要する時間
- 修正対応が行われた調査件数
- プロアクティブな脅威ハンティングを起点とした修正件数
- 深刻度別に分類された修正済み脆弱性の件数



先進的な SOC ソリューションを見つける

企業ごとにセキュリティ成熟度や置かれた状況は異なりますが、絶えず変化する脅威環境に対応するため、サイバーセキュリティに真剣に取り組むすべての組織にとって、高機能な SOC の活用は不可欠です。自社のリソースで SOC を構築する場合でも、外部プロバイダーと連携する場合でも、ハイブリッドモデルを採用する場合でも、適切なパートナーシップを結ぶことで効果的に脅威を防ぎながら、ビジネス目標を達成できます。

多くの企業が人材不足や予算の制約、複雑化するサイバー脅威に対応するため、ハイブリッド型またはフルマネージド SOC を採用しています。これらの SOC モデルは、高い柔軟性と専門的な洞察、そして 24 時間 365 日の監視体制を提供します。信頼できるパートナーによる拡張性のあるセキュリティ運用を実現しつつ、社内チームが戦略的な取り組みに専念できる環境を支援します。

Sophos MDR には、このアプローチが持つあらゆる優れたメリットが凝縮されています。ソフォスは、サイバーセキュリティの成熟度に応じた階層型のサービスを提供しており、組織のニーズに合わせて高度な検知、調査、対応機能を提供します。社内 SOC チームの支援から、全業務を委託されたパートナーとしての運用まで、Sophos MDR は脅威の可視化と対応力を強化し、組織が防御力を高めて最も重要な資産を守るための支援を提供します。

[1] ソフォスランサムウェアの現状レポート 2025 年版
[2] ソフォス、2025 年版アクティブアドバーサリーレポート

SOPHOS

Sophos MDR (Managed Detection and Response) の詳細については、sophos.com/mdr. をご覧ください。

英国およびワールドワイドセールス
Tel：03-3568-7550
Email: sales@sophos.co.jp

オーストラリアおよびニュージーランドセールス
Tel：03-3568-7550
Email: sales@sophos.co.jp

北米セールス
Tel：03-3568-7550
Email: sales@sophos.co.jp

ソフォス株式会社営業部
Tel：03-3568-7550
Email: sales@sophos.co.jp