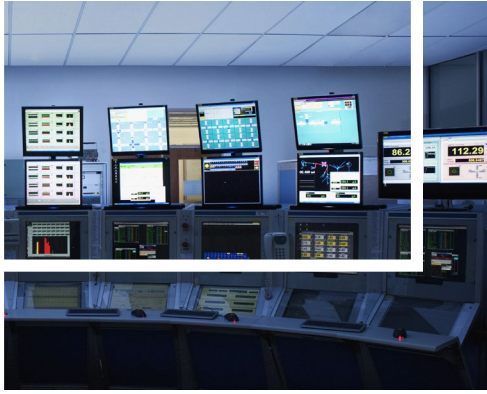
CSIRTを進化させる次の一手
「サイバーセキュリティ資産管理」による CSIRTパフォーマンスの最大化



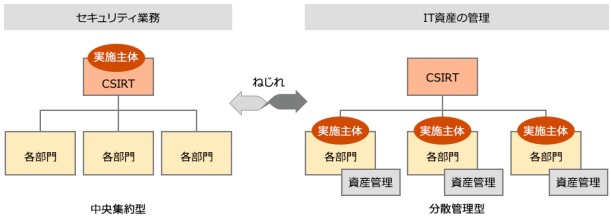
PwCコンサルティング合同会社　ディレクター　辻 大輔
PwCコンサルティング合同会社　マネージャー　渕 遼亮

1.はじめに - あらためて問う、資産管理の重要性

企業における情報セキュリティマネジメントでは、CSIRT（Computer Security Incident Response Team）をはじめとする専門組織の設置を通じてセキュリティ機能が「集約」され、インシデントレスポンス態勢の高度化を実現しているケースが多く見られます。一方、この機能集約という業務面の整備のみが先行し、その機能の遂行に求められる保護すべきIT資産の管理は、依然として各組織に「分散」されている場合も少なくありません。

このねじれた構造がセキュリティマネジメントにおける業務負担やコストの上昇、また活動自体の効率性や敏捷性に課題を生じさせています。

図表 1：セキュリティ機能と資産管理のねじれ



サイバー攻撃が高度化し、ビジネスの急速なデジタル化によって保護対象が増加・多様化する現在そして未来においては、CSIRTはこれまでよりもクイックに業務サイクルを回し、組織の安全性を担保し続ける必要があります。こうした取り組みを実現するためには、IT資産の管理情報を一元的に集約すると共に、セキュリティ機能と資産管理の主体のねじれを解消してCSIRT活動のパフォーマンスを最大化する「サイバーセキュリティ資産管理」（CSAM：Cyber Security Asset Management）が必須基盤と考えます。今回は資産管理の現状と課題をあらためて見つめ直し、サイバーセキュリティ資産管理がなぜ必要なのかを考察します。

2. 現状の課題 - CSIRT活動を阻害する分散化された資産管理

セキュリティ機能と資産管理のねじれ構造は、CSIRTが保護すべき資産の詳細を把握していないこと、また必要な情報にアクセスするまでに時間と労力を要していることを示しています。これは企業や組織に、次のような課題を生じさせます。

セキュリティリスクの放置

CSIRTが各組織・各資産の抱えている脆弱性やセキュリティリスクを把握できていないために必要な対策を講じられず、セキュリティリスクが放置される危険があります。

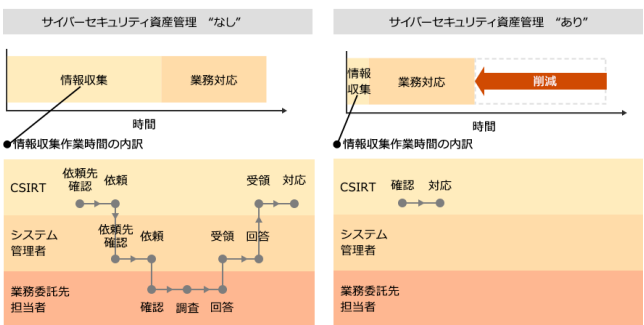
また、各組織に委ねられた資産管理の品質にCSIRT活動が依存するため、管理漏れが生じた場合、CSIRTはセキュリティ機能を全く提供することができません。

セキュリティ業務効率の悪化

CSIRTが各組織の資産管理情報にすぐにアクセスできないことで、CSIRT活動に必要な情報の入手に時間を要し、また関係者を幾重にも巻き込むなど、業務効率を悪化させる可能性があります。

例えば、インシデント対応時に、対処法の判断に必要な情報が手元で管理できていない場合、担当者へのヒアリングや実機へのログインを伴う調査が必要となり、インシデントへの対処・封じ込めに時間を要します。サイバーセキュリティ資産管理を導入し必要な情報を恒常的に管理することで、情報収集における時間が大幅に削減し、迅速な対処・封じ込めを実現することができます（図表2）。

図表 2：サイバーセキュリティ資産管理の有無で変わるインシデント対応方法（イメージ）



3.「サイバーセキュリティ資産管理」の導入に向けて

ではここからは、CSIRT活動に必要となる情報を即時的かつ漏れなく収集・管理するサイバーセキュリティ資産管理をいかに実現するかを考えます。CSIRT活動に必要な情報は多岐に渡るため、情報収集・管理の設計に不備があると、期待する効果が得られないだけでなくサイバーセキュリティ資産管理自体の負荷が高まる恐れがあります。

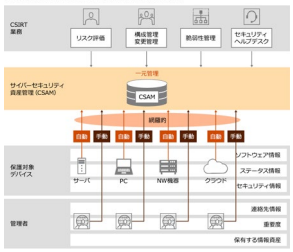
まず設計で重要なことは、目的を達成するために必要な、管理すべき情報を定義することです。この際、業務単位で、その開始から終了までに必要な情報を詳細に洗い出し、システムの重要性や費用対効果を考慮の上、サイバーセキュリティ資産管理においてどの粒度まで情報を管理するかを決定します。

例えばインシデント対応業務では、部門からの相談・報告、トリアージ、対処・封じ込めといった各工程で異なる情報を取り扱います。どのような情報を管理するべきかについては、システムごとの重要性や特性に鑑み、どの工程まで業務効率を改善するべきかを検討することで導くことができます（図表3）。

図表 3：インシデント対応における情報の整理

工程	必要な情報	情報管理の方針		
		公開系システム	社内システム（要塞）	社内システム（一般）
連絡・報告	・連絡先 ・担当者 ・アプリメモ ・ホスト名	○（手動）	○（手動）	○（手動）
トリアージ	・システムの重要性 ・保有する情報の機微性 ・業務用途	○（手動）	○（手動）	○（手動）
対処・封じ込め	・OS・ソフトウェア情報 ・平時の起動プロセス ・平時のオープンポート番号 ・AV/パターンファイルのバージョン	●（自動）	●（自動）	×
サービス停止判断	・判断者 ・停止条件 ・停止時の連絡先 ・停止に影響を与える業務	○（手動）	○（手動）	○（手動）

図表 4：サイバーセキュリティ資産管理における情報の収集・管理方法



また、必要な情報の収集方法を検討することも重要です（図表4）。

サイバーセキュリティ資産管理で管理する情報は、「静的な情報」と「動的な情報」に分類されます。「静的な情報」とは、システムの運用時にほぼ変更がない情報（各種連絡先や属性など）を指し、各部門へのヒアリングや棚卸によって収集可能です。

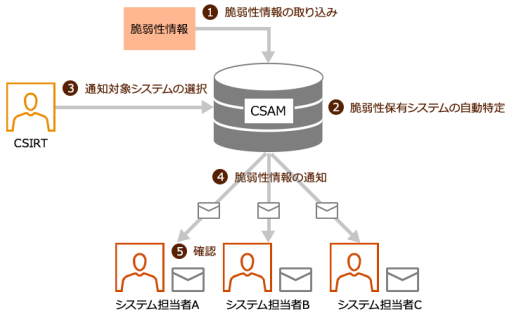
一方、「動的な情報」とは、システムの運用時に頻繁に更新される情報（バージョン情報やオープンポート、起動プロセスなどのステータス情報）を指します。これらの情報は、陳腐化することのないよう、情報収集を自動化することが望まれます。

そのほか、サイバーセキュリティ資産管理自体のアクセス管理といったセキュリティに係る事項や、収集した情報を業務に還元する活用方法の検討も欠かせません。

4. サイバーセキュリティ資産管理で向上するCSIRTパフォーマンス

サイバーセキュリティ資産管理を活用することで、CSIRT活動の飛躍的な向上が期待できます。単純なケースでは、ソフトウェアの利用有無やバージョン情報が一元管理できると、セキュリティ製品（IPS／IDS、WAF、AVなど）やSOC（Security Operation Center）による検知イベントへの影響の有無や、新たに公開された脆弱性情報に対する影響を、短時間で正確に把握できます。さらに、脆弱性の自動特定から通知、対応管理までのプロセスをサイバーセキュリティ資産管理で実現すると、インシデントの発生防止にも大きく寄与することができるでしょう（図表5）。

図表 5：サイバーセキュリティ資産管理を活用した脆弱性管理



多くの企業では、セキュリティ監査の名目で年次で担当者に膨大な設問が投げかけられることに「業務負荷が高い」といった不満の声が挙がっています。この課題も、サイバーセキュリティ資産管理によって各システムから収集した情報を活用し、設問数を削減することで軽減・解消が可能です。さらに、サイバーセキュリティ資産管理で収集したシステムの設定や環境値と期待値との比較を自動化することで、セキュリティ監査の自動化だけでなく、新たに構築されるシステムに対しても、そのセキュリティ対策状況を評価することができるようになります。

これまでの資産管理の域を超えて情報システムをセキュリティ目線で一元管理し、業務を最適化する。そうすることで、保護対象のシステムが増加・多様化しても持続可能なセキュリティ態勢が構築でき、CSIRTの体制整備のみならず、さらなる機能活性化への礎となることでしょう。

お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com