トピックス

CSIRT運営に求められるセキュリティオペレーションとは

組織内CSIRT（Computer Security Incident Response Team：シーサートと読む）を構築・運営する企業が増えている。インシデントの予防や緊急対応を担うCSIRTの運営を成功させるには、その活動の1つであるセキュリティオペレーションが欠かせない。本稿では、CSIRT運営におけるセキュリティオペレーションについて解説する。

NRIセキュアテクノロジーズ MSS（Managed Security Services）事業本部 MSS事業推進部
上級ITセキュリティコンサルタント
平舘（ひらだて） 一哉（かずや）
専門はサイバー攻撃対策ソリューション

必須機能になりつつある組織内CSIRT

標的型攻撃や内部不正による情報漏えいなど、サイバーセキュリティインシデント（事件）の被害が後を絶たない。攻撃を防御するためのシステム対策（例えばファイアウォールやウイルスチェックなど）を適切に行っていたとしても、被害に遭う事例が数多く出ている。

こうした状況を踏まえ、「攻撃を抑止・防御する観点からのシステム対策」は当然のこととして、いったん狙われてしまえば攻撃の手から逃れられないことを前提とし、「攻撃を早期に検知して対応し、インシデントの被害を最小化するための態勢面での整備」を進めることが急務となっている。

CSIRTは、インシデントの予防や緊急対応を担う専門の組織である。NRIセキュアテクノロジーズが発表した『企業における情報セキュリティ実態調査2014』では、CSIRTまたは類似の機能を持つ企業の割合が4割を超える結果となっている。

セキュリティオペレーションの重要性

サイバーセキュリティインシデントに関して注意喚起などを行う団体、JPCERT/コーディネーションセンターが発行した『コンピューターセキュリティインシデント対応チーム（CSIRT）のためのハンドブック』によれば、CSIRTが提供する機能は大きく3つに分かれる。①攻撃に備えた計画立案を行う「事前対応」、②実際のインシデント発生時に対応する「事後対応」、③セキュリティ教育や監査などを定期的に行う「セキュリティ品質管理」である。

このうち「事後対応」は日々のCSIRT運営の中心的な活動である。侵入検知システムからのアラートに対応する「セキュリティモニタリング」、ソフトウェアのぜい弱性に対して、その影響の有無を確認して対応策を適用する「ぜい弱性ハンドリング」、アンチウイルスソフトをすり抜けたマルウェアなどを調査する「アーティファクトハンドリング」が含まれる。これらは一般にセキュリティオペレーションと呼ばれており、CSIRT運営の

成功の鍵を握っている。

セキュリティオペレーションの課題

筆者のCSIRTやセキュリティオペレーションに関する提案・支援経験を通じて、CSIRT運営におけるセキュリティオペレーションには、共通した課題があると考えている。

(1) グレーイベントの取り扱い

NRIセキュアテクノロジーズが発表した『サイバーセキュリティ：傾向分析レポート2014』によれば、侵入検知システムを含むセキュリティ機器が自動分析して出力する高リスクアラートのうち、55%は攻撃とも誤検知とも判定できないグレーイベントであった。CSIRT担当者はグレーイベントについて、被攻撃端末の構成情報や、攻撃の痕跡が残された可能性のある周辺機器のログなどをあらためて調査し、本当に攻撃が成功していたのか総合的に判断して対応する必要がある。しかしログの取得レベルが不十分だったり、データ一覧であるインベントリーの管理が徹底されておらず、構成情報を把握するのに手間を要したり、グレーイベントを十分に調査できない場合も多い。セキュリティモニタリング用途に着目したログの取得・管理やインベントリー管理の整備が急務である。

(2) マルチセキュリティベンダー

同じシステムに配備したセキュリティ機器の運用ベンダーが複数に分かれている場合は少なくない。セキュリティモニタリングにおいては、CSIRT担当者は、各々の運用者から報告される分析情報を取りまとめて整合性を取ることが難しい。また、それぞれの機器のベンダーによって、攻撃と判定するレベルが異なるケースもあり、その相違をCSIRT担当者のスキルで総合的に判断する必要がある。ぜい弱性ハンドリングにおいては、ぜい弱性情報の収集方法や、緊急対応の要否判断が難しいだけでなく、ぜい弱性への対応をどこに依頼するべきかという判断の難しさが加わる。効率的なCSIRT運営のために運用ベンダーを一元化していくことも一案である。

(3) 検知の仕組みの不足

インターネットとの境界を防御する視点で、入口・出口対策を行うのは一般的となった。だが、攻撃者がいったん内部に侵入してしまえば、その後の攻撃活動を把握することは難しい。それを把握するためには、組織内部に網を張り巡らす発想で、内部の認証サーバーやファイルサーバー、端末、部門間のルーター、ファイアウオールなどを継続的にモニタリングする必要がある。侵入されたとしても被害を最小限に食い止めたり、セキュリティ事故後の被害範囲の特定や原因を調査したりする検知・分析基盤を整えておくことが今後必要となろう。

再考が求められるセキュリティオペレーション

企業におけるCSIRTの取り組みは始まったばかりであり、セキュリティオペレーションも既存の枠組みを流用する形で活動を始めている企業が多い。前述の課題を踏まえてセキュリティオペレーションを再考することで、品質・効率性が向上し、サイバー攻撃への態勢向上に寄与することになろう。 ■