トピックス

CSIRTの次なる一手
―プロアクティブなセキュリティ機能構築の必要性―

大規模組織を中心に構築が進んでいるCSIRTだが、構築したCSIRTが要員不足などの理由で十分に機能していないといった課題が多数存在する。さらには、進化するサイバー攻撃に対し、CSIRTも高度化していかなければならないという課題もある。本稿では、これらの課題解決の考察を述べるとともに、今後CSIRTに必要とされる次の一手を紹介する。

NRIセキュアテクノロジーズ 事業開発部長
関取（せきとり） 嘉浩（よしひろ）
専門は情報セキュリティ関連の事業企画

組織内CSIRT構築の現状

大規模組織を中心に、セキュリティインシデントが発生したときの対応にあたるCSIRT（Computer Security Incident Response Team）と呼ばれる組織・機能の構築が進んでいる。NRIセキュアテクノロジーズが毎年行っている「企業における情報セキュリティ実態調査」の最新版（2015年）によると、「CSIRTを構築済み」「類似機能を情報システム部門で実施」「構築中・検討中」などを合わせて、2013年の調査では28.9%であったものが、48.7%に上っていることからもこの傾向がうかがえる。

CSIRTの構築・運用によって、企業はセキュリティインシデントに対するノウハウを集約し、対応フローやプロセスを明確化・整理した上で、有事の際に組織として迅速に対応することが可能になる。また、CSIRTはインシデント情報や脆弱性情報を他社と共有する際の窓口機能も持つ。このような観点から構築のメリットは大きい。

一方、CSIRTの運用における課題もある。本稿では主要な2つの課題をご紹介し、解決のための考察を述べる。

CSIRT運用における課題

前掲の調査の中で、CSIRTを構築している企業に対し「運営に係る課題として認識していることは？」という設問がある。その回答の上位をみると「要員の不足（45.8%）」「要員のスキル不足（43.8%）」が挙げられており、さらに別の設問の回答としてCSIRT構成要員の83.3%は他業務との兼任という実情がある。これではせっかく構築したCSIRTが期待通りに機能せず、絵に描いた餅で終わってしまう恐れもある。

サイバー攻撃への対応を行うCSIRT要員には、専門的な能力・スキルが不可欠である。企業はCSIRT構築において運営予算も含めたリソースの確保、計画的な要員の育成に中長期的に取り組む必要がある。

また、場合によってはセキュリティ専門会社へのアウトソースも考慮し、まずはCSIRTをスモールスタートするといった方針も考え

られる。これで少なくともインシデント発生時の即応体制としては効果が期待できる。

高度化する攻撃への課題

2つ目の課題としては、悪質・高度化する攻撃への対応である。

CSIRTの通常業務としてはソフトウェアの脆弱性情報や攻撃情報の収集、SOC（Security Operation Center）とのネットワーク監視情報の共有などがある。これらを日々行いながら、ひとたびインシデントが発生した際には集中的に拡散防止、原因究明・根絶、再発防止策を講じるという、どちらかというと受動的（リアクティブ）な活動が主体である。

ところが、実際に対応すべきインシデントの端緒情報は、従業員や顧客・公的機関からの指摘で初めて認識されるケースが多い。こうした状況をみると、現在の受動体質のCSIRTでは、高度化する攻撃への対応が後手に回る危険性がある。そこで、CSIRTの機能をさらに一歩進化させ、能動的（プロアクティブ）な機能も取り入れる必要に迫られている。

プロアクティブな機能を有するCSIRT

プロアクティブな対策の核は2つある。一度起こった事案を徹底分析し、再発防止のスキームの構築を行う「サイバーインテリジェンス機能」と、攻撃に至る前の予兆をいち早く発見する「ハンティング機能」である。

前者のサイバーインテリジェンス機能は、スパイ映画に出てくる諜報機関の機能をイメージする方も多いと思うが、実際はログの解析を含む攻撃情報の詳細を分析・蓄積しておき、同じ兆候が起きたときに実害に至る前に食い止めるという地道な活動である。

次に後者のハンティング機能については、消防と警察を例に挙げて説明したい。現状の受動的CSIRTを、火災発生時に出動する「消防署」にたとえるとすると、能動的CSIRTは、「警察の自動車警ら隊」のような機能である。問題が起こりそうな部分を能動的に見つけ、発生前に適切な措置をとることを目的にする。

この2つの機能を担当する部隊を「ハントチーム」と呼び、欧米のセキュリティ先進大手企業では、CSIRTの一部として編成・運用が始まっている。

カギを握るのは、やはり要員のスキル向上

ハントチームの要員は、前述のCSIRT要員のスキルに加えて、デジタルフォレンジックやペネトレーションテストといった分野の高いレベルのスキルが必要となる。習得にあたっては実践的な専門研修を履修してある程度の能力向上を図った後に、実務経験を積み重ねていくという方法が効率的である。NRIセキュアテクノロジーズでは、すでに日本でもこれら専門スキルが習得できる研修コースを提供しているので活用していただきたい。

要員不足とスキル不足という運用の課題を解決し、さらにハントチーム機能を含めた、プロアクティブなCSIRTの運用実現が日本企業において今後の急務となる。 ■