“機能するCSIRT”はこうして創る

成功のカギは適切な運用と IT技術者の“セキュリティー実践力”にあり

日本アイ・ビー・エム株式会社
セキュリティー事業本部
サイバー・セキュリティー・サービス
セキュリティー・サービス担当部長

徳田 敏文
Toshifumi Tokuda

1999年、インターネットセキュリティシステムズに入社。脆弱性検査手法の開発やマネージド・セキュリティー・サービスの立ち上げを事業責任者としてリード。2007年、IBMとの会社統合後は社内のセキュリティー事故対応を担当。現在はお客様向けセキュリティー事故緊急対応サービスの立ち上げに従事している。

日本アイ・ビー・エム株式会社
セキュリティー事業本部
サイバー・セキュリティー・サービス
シニア・マネージング・コンサルタント
セキュリティー・スペシャリスト

小倉 秀敏
Hidetoshi Ogura

1999年、インターネットセキュリティシステムズに入社。製品サポートおよびプリセールスのマネージャー、エバンジェリストとして活動。2007年、IBMとの会社統合後はセキュリティー・サービスのプリセールスとして活動。現在はお客様向けセキュリティー事故緊急対応サービスとCSIRT構築支援、特定分野向けペネトレーション・テストに従事している。

サイバー攻撃や内部不正による度重なる情報漏洩事件を背景に、企業や組織内でセキュリティー・インシデント（重要ソフトウェアの脆弱性問題や情報漏洩事件など）の対応に当たる専門チーム「CSIRT（Computer Security Incident Response Team、シーサート）」を設置する動きが高まっています。しかし、CSIRTをどのように組織し、運営していくのかについては、まだまだ手探りの状態です。

そこで、CSIRTの役割や運営のポイント、さらにはCSIRTに必要とされる人材について、IBMの徳田敏文と小倉秀敏に話を聞きます。2人は、お客様のセキュリティー・インシデント対応やCSIRT作りの支援で多くの経験を積み、今日もその第一線で活躍するスペシャリストです。

CSIRT設置の目的は、被害の最小化

―― ここにきて、なぜCSIRTの必要性が高まっているのでしょうか。

徳田　大きな理由の一つは、企業の情報資産の守り方が変わってきたことです。インターネットが高度に発達した今日、情報資産の所在や、それらを利用するプロセスは一定ではなく、セキュリティー確保の難度が高まっています。それに伴い、セキュリティー・インシデントの発生を阻止する対策のみならず、インシデントが起こることを前提にした対策を整えること――つまり、インシデントへの対応力を強化することが求められ、それがCSIRTに対する期待と必要性の高まりにつながっているのです。

―― インシデントへの対応力強化とは、最終的に何を目的にしているのですか。また、CSIRTが担うべきミッションとは何なのでしょうか。

徳田　CSIRTを置くことの最大の目的は、セキュリティー・インシデント発生時に被害を最小化することです。この大目標の下、情報を収集・分析することでインシデントの全体像や原因について把握し、速やかな復旧・再発防止の措置・対策を策定するのがCSIRTの役割です（**図1**）。インシデント・ハンドリングのプロセスは、「調

査（検知・分析）」「トリアージ（対応の優先順位付け）」「対応（制御・根絶・回復）」の順番で流れます。何らかのセキュリティー・インシデントが起きた際に、そのプロセスを速やかに、かつ適切に回し、被害を可能な限り小さく抑える専門チームがCSIRTです。

―― 企業や組織がセキュリティー・インシデントに対応するためには、国際標準の「ISMS（Information Security Management System：情報セキュリティマネジメントシステム）」に則っていれば十分ということではないのでしょうか。

徳田　ISMSなどの厳格なルールに従うことは大切です。しかし、決められたルールに従っているだけでは、想定外のインシデントには対応できません。

ルールというのは決められた手順書であって、そこに記されているのは、「何をどう守るか」のプロセスや、「想定される事態」に対する対処法です。ところが今日では守る対象が流動的になり、セキュリティー・インシデントがどこでどのようなかたちで発生するかが読めません。つまり、厳格なルールの遵守を徹底させても、想定外のインシデントが起きればそれに対応できないのです。CSIRTはそうしたセキュリティー対策上の問題を抜本的に解決する役割も担っています。

またもう一つ、「ルールがあればセキュリティーが担保できる」という発想の背後には「性善説」の考え方があります。ルールを定めておけば、「社内・組織の誰もがそれを遵守してくれるはず、だからセキュリティーが保証される」と考えるのは危ういですね。

IBMもかつて「性善説」に基づくセキュリティー施策を社内的に展開していました。セキュリティーに関して厳格なルールを敷き、それで安全性が担保されると考えていました。IBMでは2011年にCSIRTを設置した際にセキュリティー・ルールを大幅に緩和するという、これまでとは逆の施策を講じました。不思議なことに、厳格なルールを敷いていたころよりも、セキュリティー上の問題が発生する件数がはるかに少なくなったのです。

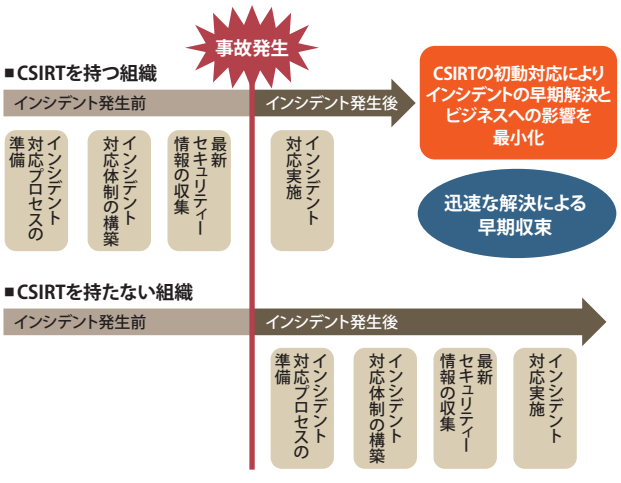

図1. CSIRTの存在意義

―― つまり、セキュリティーに対する考え方を変えることが大切だということですね。

徳田　そう言えます。性善説に基づく考え方は改めるべきですし、重要情報の所在や活用プロセスが常に流動的であることを前提に、有効な対策を打っていかなければなりません。CSIRTを置くことは、そのきっかけを作ることにつながるのです。

CSIRTを設置しても、想定外の事態に見舞われれば迅速な対処は難しいでしょう。しかし、CSIRTの取り組みを推進することで、少なくとも「想定外のことはいつでも起こりうる」という意識が芽生えます。それが結果的に、さまざまなインシデントへの対応力の強化につながっていきます。

大切なのは、「運用」していくこと

―― CSIRTを設置する上で、企業や組織が最も留意すべきはどんな点でしょうか。

小倉　CSIRTの設置自体を目的にしないことです。型どおりのインシデント対応計画書を作りCSIRTのメンバーを選定するだけではインシデント対応の能力は上がりません。言い換えれば、CSIRTの「かたち」だけを整えても、本来の目的を見据えた運用をしなければ、CSIRTが有効に機能することはありません。

―― “有効に機能するCSIRT作り”には、何が必要とされるのですか。

徳田　一つは、演習です。CSIRTのチームがインシデント対応の訓練を繰り返すことで、実際のインシデント発生時にどう対処すべきかを肌感覚で掴むことが可能になります。例えば、「すぐに手を付けなければならないことは何なのか」「それと並行して取り組むべきことは何なのか」「自分たちで対応できる範囲はどこまでで、外部の力をどこでどう活用すべきか」といったことが、訓練を通

じて見えてきます。こうした訓練を怠ると、有事の際にCSIRTのメンバーが集まっても何から着手すべきかの判断が下せず、時間だけがいたずらに過ぎていく事態に陥りかねません。

―― CSIRTの取り組みを進める上で、他に心掛けるべきことはありますか。

小倉　陥りがちな落とし穴は、インシデント対応の計画書を詳細に作り込んでしまうことです。先に徳田が触れたとおり、今日では、想定外のセキュリティー・インシデントが発生することが多く、想定通りのインシデントが起きるほうが稀なのです。ですから、いくら計画を精緻に作っても、その通りには事が進まないのがほとんどです。

例えば、消防士の消火訓練にしても、担当地域のあらゆる家の構造と出火リスクを想定してはいないでしょう。そもそも、あらゆるリスクを想定した消火計画を詳細に立てること自体が不可能ですしナンセンスです。それは、セキュリティー・インシデントも同様で、起こりうるあらゆるインシデントに対して詳細な対応計画を立てることはできません。また逆に、想定リスクを絞り込み詳細な対応計画を立てても、思わぬところから“出火”すれば、計画の大半が役に立たなくなります。したがって、セキュリティー・インシデントの対応計画は、重要なコントロール・ポイントはどこで、ポイントごとにどう対応すればよいのかという大枠を定めるに留めておくことが肝心です。そうすることが、さまざまなインシデントへの柔軟な対応につながります。

求められるセキュリティー人材は経営と技術の“橋渡し役”

―― CSIRTをどのような人材で構成するかも、取り組みの成否を左右するポイントだと思います。CSIRTに求められるのは、どのような人材なのですか。

徳田　先に話したとおり、CSIRTの目標は被害の最小化であり、その被害とは企業が守るべき何かが損なわれたり、盗まれたりすることを意味します。そのため、「自社が守るべきモノは何か」をはっきりと理解している人をCSIRTのメンバーの中に含める必要があります。それは、経営陣である場合もありますし、経営陣に対して適切な情報を提供し成すべきことを提示・提言できる社員である場合もあります。言い換えるならば、「経営と技術との橋渡しができる人」です。CSIRTに関係する組織は、経営層、社内の各部門・各部署、セキュリティー事業者、顧客、マスコミなど多岐にわたりますが、中でも経営陣とCSIRTとの関係は緊密であることが必須です。セキュリティー・インシデントの発生時には高次の経営判断が求められ、そうした判断は、各事業部門・部署のマネージャー・クラスでは下せないからです。その意味でも、CSIRTは、経営陣が自らリーダーシップを握っているか、経営陣からセキュリティー対応に関する実行責任と全権を委譲されているかのいずれかでなければならず、後者の場合、経営と技術との橋渡し役が中核メンバーであることが求められるのです。

―― この他にどんな人材でチームを組むのが適切なのでしょうか。

小倉　企業や組織によって異なりますが、大切なのは問題解決能力の高さをメンバー選びのポイントに置くことです。例えば、「ビジネスの現場で起きているインシデントに対して即座に優先付けができる人」や、「事態の収拾に向けて、外部の関係組織とどう連絡を取り、どんなスキルを持った、どのような人の力を借りるべきかが適切に判断できる人」などで、チームを組むべきでしょう。

―― 先ほど言及された「経営と技術との橋渡し役ができる人」を、もう少し具体的に説明していただけますか。

徳田　端的に言うと、「セキュリティー実践力のあるIT技術者」です。これからのサイバー・セキュリティーを支える人材は、セキュリティー技術レベルにより大きく4つのレイヤーから成ると考えられます（**図2**）。レイヤーの最上位に位置するのが、いわゆる「トップガン」と呼ばれる世界トップレベルのセキュリティー人材で、そのすぐ下位に位置付けられるのが「セキュリティー・エキスパート」です。その下位に、セキュリティー実践力のあるIT技術者、「一般社員」と続きます。

このうち、トップガンやセキュリティー・エキスパートは、基本的にはセキュリティー事業者に所属している方たちなどで、企業が雇用・育成する必要はないと考えます。企業に求められるのは、セキュリティー実践力のあるIT技術者で、その人材がCSIRTでも中心的な役割

を担います。

例えば、経営陣は、メディアで報道されたセキュリティー・インシデントが、「自社にどのような影響を及ぼすのか」「自社でも起こりうるのか」「その発生リスクを最小化するには、何をどうするのが適切か」といったことを即座に知りたいと望みます。そうした経営サイドの要望に対して、経営の視点と、経営陣が理解できる語彙を持って、分かりやすく、かつ、正しく事実を伝え、適切な経営判断を促していくことが、「経営と技術との橋渡し」です。そうした能力を持った人材――つまり、セキュリティー実践力のあるIT技術者が、CSIRTのリーダーシップを執っていくことが理想です。

また、自社内の技術スキルだけでは解決できない課題については、外部のセキュリティー事業者の力を借りることが必要とされます。そうした事業者からの提案内容を理解した上で、事業者に的確・適切な指示を出すこともCSIRTリーダーには求められます。セキュリティー実践力のあるIT技術者ならば、その役割も担えるのです。

CSIRTリーダーの育成を目指して

―― IBMでは、CSIRTリーダー向けの研修を行っていますが、これは、どのような内容のものなのですか。

徳田　この研修は、企業のCSIRT創設支援のカリキュラムです。全体は4日間のプログラムから構成され、「体験」を中心にした実践的な内容になっています（**表1**）。

現在、多くの企業がセキュリティー運用を外部に委託していますが、すべてを委託先に任せていると、運用の中身が見えなくなり、セキュリティー・インシデントに対する当事者意識も自ずと薄れていきます。また、万が一のインシデント発生時に、自ら何も判断できなくなる恐れも強まります。そこで、「インシデント対応の実際」を体験していただくことで、自社・自組織のセキュリティー運用やインシデント対応は「自分たちがリードすべきものであること」を改めて理解いただこうと考えたのです。

研修では、実際に起こったインシデントのログを使いながら、その対応に当たった当事者が講師を務めるため、リアリティーのあるインシデント対応の演習が行えます。演習を通じてインシデント対応に対する当事者意識を強く持っていただき、経営層に対する積極的な施策の提案やセキュリティー事業者の適切な活用を推進していただきたいと考えています。

―― 最後に、今後CSIRTの設置をお考えの方にメッセージをお願いします。

徳田　まず、セキュリティー・インシデントへの対応が自分たちの問題であるとはっきりと意識することが大切です。また、目に見える成果をすぐに求めず、適切なロジックの下で施策の評価を重ねて、理想形に近づけていくスタンスも重要です。繰り返しになりますが、CSIRTの設置は目的ではありません。CSIRTの取り組みを通して、インシデント対応のさまざまな気付きを得ながら、被害の最小化という大目標に向けて努力を続けることが大切です。

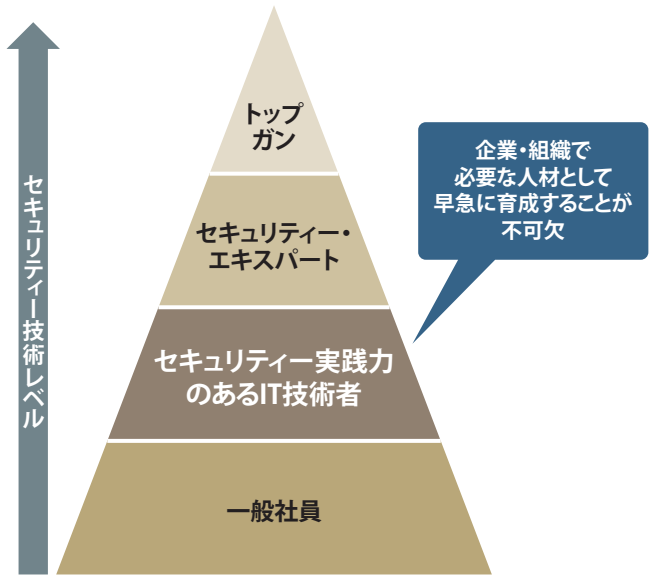

図2. セキュリティー人材

表1. IBMが提供しているCSIRT研修のカリキュラム

1日目	CSIRTの一般的な活動内容を解説。併せて、事例を基にした演習形式でインシデント対応の全体的な流れを体験する。法執行機関の対応について経験者からの講義もある。
2日目	外部からの攻撃をテーマにしたインシデント対応の演習を通じて、標的型サイバー攻撃などで使われる攻撃パターンや分析手法を学習する。実際のログを解析しながらインシデント対応の実務を体験するという実践的なカリキュラムが展開される。
3日目	内部不正をテーマにしたインシデント対応を演習。大規模情報漏洩事件の実例を用いながら、実際にインシデントに対応した技術担当者から、事例解析のかたちで講義を受け、対応の難しさを体験する。内部犯行によるインシデントの体験やマルウェア感染時のフォレンジックツールの使用方法なども学習。
4日目	インシデント発生後の情報収集、外部との連携、公表の適切な方法を学ぶ。また、総合演習として、インシデント対応の全体的な進め方や、記者会見の実施判断をどう下すかなども体験できる。