2020.01.06

情報セキュリティニュース ＜2019 No.3＞

CSIRT の構築とその運用

【要旨】
■2019 年もサイバー攻撃は国内外問わず多数発生、直接 PC やサーバを攻撃するだけでなくスマートフォンやタブレット、IoT デバイスを介するなど、攻撃手法も多様化しており、対策には専門的な知見を有した組織（CSIRT）を設置しておくことが必要である。
■CSIRT は事故対応のみを行う組織ではなく、平常時においてインシデントを発生させないような活動も担うものと理解すべきである。
■サイバーセキュリティリスクは多くのリスクと接点がある。CSIRT は、経営や緊急対策本部とのコミュニケーションを図るなど、組織的な連携が望まれる。

１．サイバー攻撃による被害とインシデント対応体制の必要性

サイバー攻撃等の被害は国内外問わず多数発生しており、PCやサーバへの標的型攻撃や不正アクセス、WEBサイトやアプリケーションへの攻撃だけでなく、スマートフォンやタブレット、IoTデバイスを介するなど、攻撃手法も多様化している。闇市場（ダークウェブ[1]）では、各種サイトのログインIDとパスワードのセット、メールアドレス、サイバー攻撃に用いるウイルスやフィッシング詐欺キットだけでなく、サイバー攻撃の請負までも「商品」として売買されており（CaaS<Cyberattack-as-a-Service>）、2019年はランサムウェア[2]やフィッシング[3]による被害が多数見られた。ビジネスを行う上でITの利用・活用が必須となる中、多様化・高度化するサイバー攻撃を完全に防ぎきることは困難となっており、万が一攻撃にあった際の対応に右往左往しないためには、予め専門的な知見を有した組織を設置しておくことが必要である。この専門性を有した組織として、CSIRT（シーサート）への注目が高まっている。

２．CSIRTとは

CSIRTとは、“Computer Security Incident Response Team”の略称であり、その名が示す通り、コンピューターセキュリティに関する初動対応などを担うチームとして組織されるものである。また、インシデント発生時以外の平時にもリサーチなどの活動も行う。

---

[1] 通常使用する検索エンジンでは見つけられず、また、通常使用するブラウザではアクセスできない匿名性の高いウェブサイト。元々は米国海軍によって開発されたもので、匿名性を確保することで情報通信の秘匿性を確保するという目的だったが、違法な商品の取引や犯罪を助長する情報の温床になっている。
[2] マルウェアの一種で、電子メールなどを通じて侵入した PC をロックして使用不能にしたり、PC 内のファイルを暗号化により参照・使用不能にしたりした後で、元に戻すことと引き換えに「身代金（Ransom）」を要求する不正プログラム。ランサムウェアによって暗号化されてしまうと、攻撃者にしか解除できない。
[3] 金融機関や大手通販などの正規の Web サイトを装った偽サイトを設け、そこに電子メールなどで誘導することで、ID、パスワード、暗証番号やクレジットカード番号などを詐取する攻撃。

表1　CSIRTが担う役務の例

カテゴリ	概要
インシデント事後対応	インシデントの被害範囲を限定することを目的とした、インシデントやインシデントに関連する事象への対応を行う
インシデント事前対応	インシデントの発生抑制を目的とした、インシデントやセキュリティイベントの検知や、発生の可能性を減少させる
セキュリティ品質向上	社内セキュリティの品質を向上させる →間接的にインシデントの発生抑制をする

3．CSIRT構築と運営のポイント

（1）守るべき対象と脅威の把握

CSIRTの構築にあたっては、以下の表2記載事項の検討が必要になるが、この検討に際しては、『経営層、システム管理者、ネットワーク管理者、全社員、顧客、その他関係組織が期待すること』を十分に考慮しながら検討が望まれる。

表2　CSIRTの構築にあたって確認・検討すべき事項の例

①守るべき対象の把握	社内システム・ネットワークにおいて重要なシステムはどれか？ 運用の主管はどこか？　など
②脅威の把握	過去に発生した重大なインシデントは？ 再発傾向にあるインシデントは？　など
③リスクの分析	現状のインシデントレスポンス体制は？ 情報セキュリティ関連ルールの浸透は？　など

（2）CSIRTの業務範囲

（1）で把握した「守るべき対象」に対して事故対応のみを行う組織ではなく、平常時におけるインシデントを発生させないための活動も担うことが重要である。CSIRTの具体的な役割は、組織の規模・特性などにより異なるが、少なくとも、以下表3内「必須」の2点は必要である。

表3　CSIRTの業務範囲の例

必須	・インシデントの発生・再発を予防するための活動を行う ・適切なレスポンスと有効な対策を実施することにより、インシデントの被害を抑制し損害を最小限にする
外部の専門事業者活用を含めて適宜検討	・インシデント関連情報、脆弱性情報、攻撃予兆情報の収集、分析 ・自社内インフラや自社内システムの安全性確保 ・自社開発製品のセキュリティ品質の確保 ・自社が開発した顧客向けシステムのサービスの維持

（3）経営層から人員の任命と体制構築を指示

経営層はサイバー攻撃を「経営リスク」として認識し、CSIRTが役務を遂行するための適切な予算・権限を付与する。CSIRTとIT部門では求められるスキルは異なり、メンバーの任命には留意が必要となる。

表4　CSIRTおよびIT部門に求められるスキル

	CSIRT	IT部門
ヒューマンスキル	・各部署及び外部との折衝能力および調整能力	・チーム活動に必要な連携能力
テクニカルスキル	・セキュリティの概念 ・攻撃及び防御手法 ・ネットワーク・サーバ関連知識	・開発手法及び言語 ・ネットワーク設計・設定知識
知識	・最新のインシデント動向 ・組織内の事業に影響を与えるポイント	・組織内ネットワーク及びシステムの構成 ・最新の製品知識

4．経営等とのコミュニケーション

企業を取り巻くリスクの中でも、とりわけサイバーセキュリティリスクは多くのリスクと接点がある。サイバー攻撃にあった結果、情報の窃取・改ざんなどデータへの被害・影響だけでなく、施設やインフラの物理的破壊・乗っ取りも起こりうる。その影響は自社にとどまらず取引先やユーザにまで広がることもあり、事態の収束対応に不手際があった場合には、取引先やユーザから業務遅延や情報漏えいによる損害賠償請求を受けたり、役員の善管注意義務違反を申し立てる株主代表訴訟が提起されるなど、経営の責任が問われる事態に発展することも考えられる。

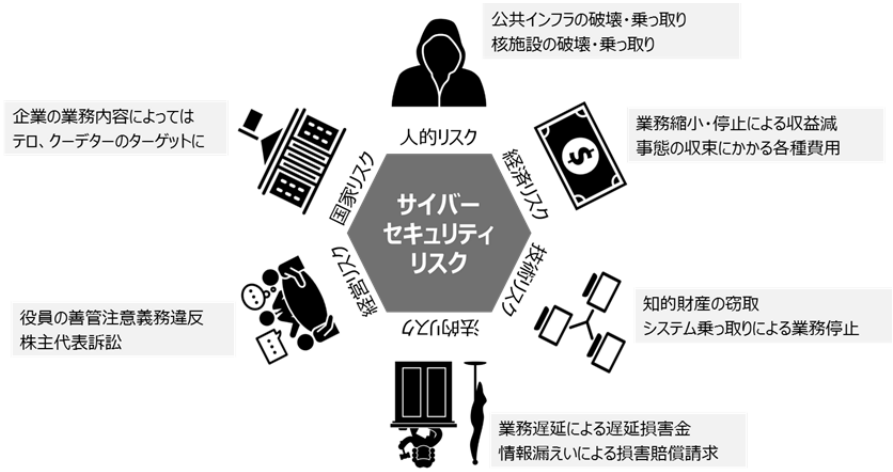

図1　サイバーセキュリティリスクと他のリスクとの関連性

全社的な対応が必要なインシデントが発生した場合、影響範囲や被害を把握し、被害拡大を防止するなどの適切な対応方針を立案するには、各部門で発生した事象を緊急対策本部などが取りまとめ、全社で一元的に管理することが望ましい。

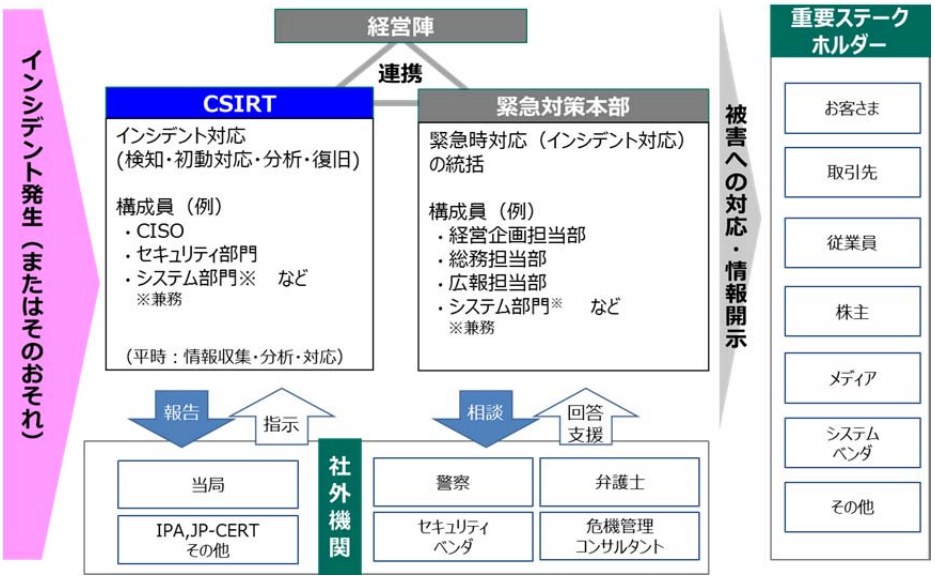

図2　企業におけるインシデント対応の全体像の例

サイバーインシデント発生時は、事態の収束に向けて高度な専門技術が必要であり、その専門性を持つCSIRTには、日常から情報システム部門が担っている業務や、情報システム部門が扱っているデータの重要性を把握することはもちろん、経営層の意思決定に基づいた全社的な対応を行う組織の一員として、どのように他の関係者や被害者等と向き合うのか、どのような順序で情報システムやデータを復旧させることが望ましいのか、リスクを総合的に判断しながら対応方針を立案することが求められる。ただし、一朝一夕で出来ることではないため、CSIRTと経営・社内関係部署・外部

の専門機関とのホットラインを構築しつつ、自社でできることを整理し、難しいことは外部へのアウトソースも視野に入れながら、少人数の体制であっても「まずはできることからはじめてみる」ことが望ましい。

サイバー攻撃への対策におわりはなく、「経営リスク」に対して、しなやかに対応する力（レジリエンス）をつけていくことが望まれる。

ＭＳ＆ＡＤインターリスク総研㈱　リスクマネジメント第四部
上席コンサルタント　　大和田　勝