JEITA

IS－15－技標－２

平成26年度情報セキュリティ調査報告書

－新たな脅威に対する組織の対応体制に関する調査－

平成２７年３月

一般社団法人 電子情報技術産業協会
情報セキュリティ調査専門委員会

はじめに

本報告書は、情報セキュリティ調査専門委員会が、近年のセキュリティインシデントに関する脅威の動向を踏まえ、新たな脅威に対するインシデントレスポンス体制の機能と形態を調査し、組織の特性に応じた効果的なインシデントハンドリングの対応体制および求められる製品・サービスについて提言するものである。

近年、情報セキュリティに関わるインシデントについては、大規模な情報流出事件、大手企業や官公庁に対する標的型攻撃、制御システムに対する攻撃等、高度化・グローバル化が進み、セキュリティインシデントが発生した場合、一つの部門だけで対応するには困難な状況にある。

セキュリティインシデントに、組織的かつ的確に対応するために必要となる組織が CSIRT (Computer Security Incident Response Team) である。国内の CSIRT 間連携を実現する場として、日本シーサート協議会が設立されているが、参加チーム数は、設立時(2007年)の 6 チームから 71 チーム (2015 年 2 月 15 日現在) にまで増加しており、インシデントハンドリングの体制整備を進めている組織が増加していることが窺える。

CSIRT については、決まった形が無く、個々の組織の特性に応じて体制を整備していく必要があるため、その必要性を認識しながらも設立に至っていない組織も多い。そのような組織の助けとなるよう、先進的な取り組みを行っている CSIRT や有識者に対するヒアリング、ユーザ企業への訪問調査および Web アンケート調査を実施し、組織特性に応じたインシデントハンドリング体制のあるべき姿について検討を行った。合わせて、CSIRT 構築・運用に際しての課題を洗い出し、求められている製品・サービスのニーズについても検討を行った。

今年度の調査・分析にあたり、ヒアリング・視察にご協力いただいた企業・有識者の方々、そして本委員会の関係者の皆様に対し、深く感謝の意を表すとともに、本報告書が関係の方々に活用され、今後のビジネス拡大の一助となれば幸いである。

2015 年 3 月

情報セキュリティ調査専門委員会
委員長　白石節男

情報セキュリティ調査専門委員会名簿

（敬称略・順不同）

委員長	白石節男	富士通（株）
副委員長	坂上　勉	三菱電機（株）
委員	福島孝文	東芝テック（株）
〃	水島九十九	日本電気（株）
〃	對馬孝高	（株）日立製作所
〃	武本　敏	（株）日立製作所
〃	池田政弘	富士ゼロックス（株）
〃	増田佳弘	富士ゼロックス（株）
〃	池田恵一	富士通（株）
〃	濱田　剛	三菱電機インフォメーションテクノロジー（株）
〃	平木博史	（株）リコー
〃	佐藤　淳	（株）リコー
オブザーバ	川口修司	（株）三菱総合研究所
〃	江連三香	（株）三菱総合研究所
〃	阪口瀬理奈	（株）三菱総合研究所
事務局	稲垣　宏	（一社）電子情報技術産業協会
	内田光則	（一社）電子情報技術産業協会

目次

第1章　社会環境の変化

本章では、日々変化し続けている社会環境に関して、特に情報セキュリティ面から見た環境の変化について紹介する。

1.1 情報セキュリティを取り巻く社会環境の変化

インターネットがグローバル社会における社会経済活動に不可欠の基盤となり、近年のICTの発達により、ますます電子化された情報が膨大に増え続けている。企業で扱う情報機器だけでも、PC、サーバ、大容量記憶媒体など多岐に渡り、大量の情報を簡単に扱えるようになった。また、サイバー犯罪の増加、コンピュータウイルスのまん延、重要インフラにおけるシステム障害など情報漏えいに関するリスクは高まり続けており、新たな脅威やリスクも顕在化してきている。

また、インシデント発生時の影響も大きくなり、企業や組織における情報セキュリティ対策は、ますます重要かつ多様化してきている。サイバー攻撃においては、一度標的にされてしまうと、防御が非常に難しいという現実もある。そのため企業においては、ステークホルダーに対して説明責任を果たすために十分な対策を講じておくことが大変重要になってきている。

このような情報セキュリティを取り巻く社会環境変化における顕著なトピックを、以下に概観する。

1.1.1 サイバー攻撃の高度化・多様化

近年、サイバー攻撃が高度化し極めて大きな脅威となってきている。特にその目的は、情報システム端末に不正プログラムを感染させるためではなく、外部からシステム内部への侵入による情報窃取や破壊等を行うことに変化してきている。標的型攻撃はプロの犯罪者による窃盗行為であり、金銭や金銭につながる情報の詐取に移行しているのである。

かつては、Web改ざんにより自己顕示につながるメッセージが表示される攻撃や、データベースが改ざんされ､データを誤表示させるなどしてWebサイトが使用できなくなる攻撃が散見された。政府や民間企業の信用失墜を目的とした改ざんが行われ、マスコミに大きく報道されることで、サイバー攻撃者は自己顕示欲を満足させ愉快犯的な攻撃を行っていたのである。

従来の標的型攻撃は見た目で判別可能なものも多かったが、最近では手口の高度化・巧妙化が進んでいる。よく閲覧するウェブサイトを改ざんしたり、また広く利用されているソフトウェアの正規サイトを改ざんし、ソフトウェアの更新を行ったPC端末に不正プログラムを感染させる。また、業務に関連するメールを数回やりとりし、相手を信用させた後に不正プログラムを添付したメールを送付して感染させることもある。脆弱性を狙った攻撃によってネットワークに侵入し､組織が所有する情報が攻撃者によって内容確認され、

個人情報や企業秘密などの情報を盗むことが目的となっている。また、長期間ネットワーク内に侵入し、次の攻撃の為の踏み台として利用する場合もある。

また、Web 改ざんはサイト運営自体を侵害するためではなく、ウイルス拡散サイトへの誘導を行う為とその目的が変わってきた。そのため、Web 改ざんに気づかないユーザーが、ウイルス拡散サイトで次々に感染被害に遭い、深刻な被害に直面することになる。

現在では特定の組織を狙って作り込まれた標的型攻撃が多く、サイバー攻撃の対象が不特定多数から政府機関や特定の企業へ移り変わってきている。サイバー攻撃の目的の変化が、攻撃対象を変化させ、それによって侵入、攻撃方法も変化している。メール、Web、SNS などの侵入手段の多様化、様々な脆弱性を利用した攻撃、それらを組み合わせた複雑な攻撃が新しいサイバー攻撃なのである。

2020 年に東京オリンピック・パラリンピックが開催される。テロ行為は社会に驚愕や恐怖感を与えようとする政治的動機に由来するものであり、テロリストにとっては世界中の観衆を引き付けるオリンピックは格好の攻撃対象となる。サイバー攻撃によって国家インフラや国家機密が危険にさらされる大きなリスクが問題視されている。サイバー攻撃による会場の停電、交通機関システムへの妨害や関連サイトの改ざんなどが懸念されている。

1.1.2 新たな技術革新によるリスク懸念

ICT の技術革新により、クラウドコンピューティング技術、IPv6 等の新たなインターネット技術、情報家電、携帯端末、電子タグの普及など新しい ICT を活用した製品やサービスが生みだされている。

特に、IoT（Internet of Things）といわれるセンサーネットワークの進化により、ヒト同士ならず、ヒトとモノ、モノ同士が、時間や距離を超えて常時ネットワークで繋がるサイバー空間が急速に拡大している。一般には「モノのインターネット」と言われるが、モノがインターネットプロトコルでネットワークされた状態である。従来はヒトの操作によってインターネットに情報発信されていたのに対して、IoT はモノが自らインターネットに情報発信する点が異なる。

今後は、センサーだけではなく収集されるデータも急速に増大していく。インターネットに接続するさまざまなデバイスの数は 2015 年中に 250 億個に達すると予測されている。データ量は 100 倍とか 1,000 倍などといった規模に膨らみ、更なる大規模化が予想されている。それに伴い、増大する IoT 専用のデータ格納クラウドなどの周辺サービスも拡大することが予想されている。

IoT に関する取り組みは始まったばかりである。また、IoT は、収集可能なデータの種類や量を爆発的に増やせることから、ビッグデータ活用の実用性や実現性を一気に高め、ビッグデータ活用に更なるイノベーション機会を提供することになる。これまで多くの試行錯誤により効果が検証され経験と勘に支えられてきた分野、たとえば農業においてもその経験や勘を見える化し、データ活用する研究が進んでいる。

自動車産業においては、様々なセンサーからの情報を解析し、自動車のディスプレイで表示する技術や自動運転についての研究が進んでいる。米国電気電子学会（IEEE）は、「2025 年までには、走行中の車の 60%がインターネット接続される。」と予測している。

また、住宅（スマートハウス）においては、通信機能がついた電力計「スマートメーター」を各家庭に設置することが推進されている。これにより、単に電力使用量の把握が自動化され、料金メニューを多様化できるだけではなく、周辺のさまざまな機器と連携した新たなサービスが期待できる。サーモスタットやドアロックなど、いわゆるスマートホーム・デバイスの数も今年は 2500 万になると見られる。

しかしながら、IoT は消費者に巨大な便益を与える一方で、データ収集や活用が進むにつれセキュリティリスクが増大する。プライバシー侵害と情報セキュリティへの大きな脅威となる。IoT デバイスは、たとえばヘルス、医療関連分野で普及し始めているが、膨大な個人情報を収集し転送することになる。このような機微情報は極めてプライバシー性の高いもので、その処理には潜在的に非常に大きなリスクを伴うのである。

1.1.3 IT システム・サービスの重要性

近年、モバイルブロードバンドの拡大、スマートフォンやタブレット端末等のスマートデバイスの普及、SNS の急速な利用拡大により、社会生活は ICT に支えられているといっても過言ではない状況である。

スマートフォンは、小型で高い利便性を備えており、高機能で操作性が高いため利用者が急速に拡大している。更に GPS 位置情報等を取得し、利用するアプリケーションが多数存在することから、従来以上に利用者の個人情報等が集約され易くなっている。

その一方で、多くの利用者は大きなリスクはないと認識しており、パソコン利用者と比較しても情報セキュリティに対する意識が低い。更には全世界的にも利用者が多く、セキュリティ対策ソフトの技術が発展途上であり、ハッカーなどマルウェア開発者にとってはローコストでハイリターンな攻撃対象となっている。

あらゆる社会インフラは IT によって支えられており、その社会基盤は IT の上に成り立っている。通信や金融などのライフラインの制御システム、私たちの命を守る医療システムなど重要な社会インフラを支えるシステム等はサービス提供中に決して停止してはならない。24 時間 365 日の中で絶え間なく運用されなければならないのである。

近年では、制御システムにも情報系システム等の技術が採用されて、また情報系システムと相互接続されるケースが増加しているため、情報セキュリティ上のリスクが高まっている。特に重要な社会インフラの制御システムにおける情報セキュリティは、社会生活の安全・安心に直結するものである。

発電所や工場プラントなどの制御システムが停止すると、設備のサービス停止に伴い、社会生活が麻痺し、立ち行かなくなることを意味する。更に、設備や装置の暴走や損壊につながる可能性もあり、障害が発生した場合には即、大事故につながる可能性もある。

政府においても、電子政府の推進等が行われており、行政サービスにおいても ICT に支えられているのである。政府共通プラットフォームや社会保障・税番号制度（マイナンバー制度）が推進されるなど、今後も一層行政の電子化は進展することとなり、情報セキュリティの確保が不可欠になっている。マイナンバー制度は、各個人の所得水準や年金・医療などの受給実態を正確に把握し、効率的な社会保障給付を実現することが目的である。仮に個人番号が漏えいし不正使用されると、医療データや財産などの個人のプライバシーや権利利益の侵害になるため、マイナンバー対する安全管理措置が極めて重要になる。

1.1.4 内部不正による情報流出

企業・組織の知的財産は最も価値の高い資産の一つであり、市場競争力の源泉となる。また多くの企業は、自社が保有する顧客情報やビジネスに関する大量の企業情報を保管している。それらは、その企業にとって重要であるだけでなく、個人的な利益を求める者にとって大きな価値となる。

これまでも従業員や委託先社員等の内部者の不正行為による情報窃取等の被害が数多く起こっていたが、最近になって企業や組織の内部関係者の不正行為により不正競争防止法で逮捕される情報漏えい事件が多数発生している。個人情報や企業機密などの情報漏えいによる損害賠償など、事業の根幹を揺るがしかねないような事件、事故が目立ってきている。情報漏えいは、コスト面だけでなく社会的な信頼失墜など、企業に与える影響は計り知れない。

2014 年、マスメディアで大きく報じられた通信教育大手での個人情報漏えい事件は、関連会社の元従業員、つまり内部関係者の犯行によるものであった。内部犯行による情報漏えいは、一度発生すれば多数の重要なデータが流出し、企業の経営責任に直結する問題となる。この事件では、顧客データベースの管理を委託されていた外部業者の派遣社員が、約１年間に渡って顧客情報を外に持ち出して名簿業者に販売していた。「国内で過去最大規模の個人情報流出事件」と呼ばれ、内部犯行による情報漏えいの危険性を如実に示したものとなった。

内部犯行による持ち出し対象は、顧客の個人情報だけではなく、財務情報やノウハウ、設計などに関わる技術情報など、企業の競争力に直結する情報が、退職者によって外部に持ち出された事件も多い。内部関係者は外部の攻撃者とは異なり、データにアクセスできる正当なアクセス権限を持っている。意図的に不正をしたとしても、技術的な対策だけでは防止が非常に難しい。

1.1.5 グローバル化の進展

グローバルな経済活動やインターネットを経由して国境を越えたサービスの提供が行われ、国境を超えて流通する情報が増大している。各企業は、他国の企業との間で情報共有し、いかにタイムリーに相互に国境を越えてデータ情報を流通させるかが競争力を高めるキーポイントとなっている。

また、クラウドサービス等による国境を超えた情報の流通が極めて容易になってきている。情報が国境を越えて自由に流通することにより、グローバルな観点での利便性等が向上し、更にはグローバルな観点での各国間制度の相互の調和が重要となってきている。特にデータプライバシー保護や情報セキュリティに関する各国間の法制度等の相違が、情報が国境を越えて自由に流通する際の課題として顕在化している。情報共有や情報移転を可能にするためには、情報セキュリティ制度や個人情報保護やプライバシーに関する国際的に調和のとれた信頼性のある制度を整備することが求められている。

また開放的で相互運用可能であり、安全で信頼性の高いサイバー空間の必要性が議論されている。インターネットがグローバル経済成長の牽引力であることが確認され、経済やネットワークの保護、インターネットの自由等の領域について優先すべき政策課題となっている。クラウドコンピューティング等の新たなサービスによるイノベーション・成長機会の認識、知的財産侵害への対応等における国際協力の推進など安全なインターネット利用環境が整備できるかが大きな課題となっている。

日本のグローバル企業においても、サイバー攻撃の高度化・多様化に伴うサイバー空間における脅威が高まる中、官民連携によるサイバー空間の監視や秩序維持に努めることが重要になってきている。サイバーテロやハクティビズム（政治的ハッカー活動）、その他のサイバー攻撃が今後も更に激化すると見込まれている。サイバー攻撃を受けるのは日常的であると考えて、各企業において技術的対策や人的対策を講じることが求められている。

第2章　脅威やインシデントハンドリング体制に関する動向

企業・団体などの IT への依存度が高まっている。それに伴ってセキュリティ上のリスクも高まっている。ここでは、最近の IT に対するセキュリティ脅威の状況を概観し、セキュリティインシデントが発生した場合の対応体制の動向について紹介する。

2.1 最近の脅威の動向

2.1.1 情報セキュリティ脅威の動向

2014 年度に発生した主な情報セキュリティ上の事案としては、

- 某通信教育会社における個人情報漏えい事件
- 某映画会社からの大量情報漏えい
- OpenSSL や GNU bash など広く使用されている S/W の脆弱性発覚
- インターネットバンキングにおける不正送金
- アカウントリスト・パスワードリスト攻撃による被害
- ビル管理システムなど制御システムへの攻撃増加
- 標的型攻撃の高度化

などがあげられる。具体的な攻撃事例としては以下のようなものがある。

表 2-1　2014 年度に発生した情報セキュリティ脅威の事例

攻撃対象	発覚時期	脅威の概要
通信教育会社	2014 年 7 月	通信教育会社の顧客 DB を管理する子会社の委託先の派遣社員が、私物のスマートフォンを使って顧客 DB から顧客情報の一部を持ち出し名簿業者に売却。
映画会社	2014 年 11 月	映画会社が製作した映画をめぐり、映画の舞台となった国から映画の公開中止を求められる中、同映画会社がハッカー集団から攻撃を受け、社内の電子メールや複数の未公開の映画、脚本などが漏えい。
銀行	2014 年 6 月	銀行の偽サイトが開設され、同銀行の預金者がそのサイトにアクセスすると、契約者に配布されている乱数表の数字を全て入力するよう要求される。偽サイトの開設者は入力された乱数表の値を使って、正規サイトにログインし預金を不正送金する。
クレジットカード会社	2014 年 4 月	OpenSSL の Heartbleed 脆弱性を悪用されたことにより、同社 Web サービスから個人情報が流出した恐れがあることを公表。
研究所	2014 年 10 月	GNU bash の Shellshock 脆弱性を悪用した海外からの攻撃により侵入を受けたことを確認し、一部サービスを停止。
SNS サービスなど	2014 年 6 月	パスワードリスト攻撃などにより、SNS サービスのアカウントを乗っ取り、サービス上での友人などに Web マネー等の購入とそのプリペイド番号の送信を依頼することにより、その Web マネーを搾取する。
標的型攻撃	2014 年 5 月	2013 年に国内組織の問い合わせ窓口を標的にした「やり取り型」攻撃が複数組織に対して同時並行的に行われていたことを J-CSIP[1]が確認し報告。攻撃先担当者の返信を見ながら攻撃手法を変化させるなどより巧妙化。

特徴としては、

- 被害範囲や被害金額が大規模
- 対策が広範囲に必要となる
- 金銭や価値のある情報の窃取を目的とする悪意を持った巧妙な攻撃の増加

という点があげられ、大企業のみならず一般企業や個人にまで攻撃範囲が拡大してきていることがわかる。ウイルス対策ソフトの導入や適時の修正パッチ適用などの一般的な対策だけではなく、被害が出ている攻撃についての情報収集・情報交換などが必要になっていると考えられる。

[1] J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan。サイバー情報共有イニシアティブ
https://www.ipa.go.jp/security/J-CSIP/

2.1.2 重要インフラ脅威の動向

2014 年に日本政府の情報セキュリティ政策会議が決定した「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」では、重要インフラとして、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の 13 分野が示されている。電力分野におけるスマートグリッドの構築など重要インフラのネットワーク化が進みつつあり、重要インフラへの攻撃の可能性は高まっている。McAfee が 2013 年に公表した「In the Dard 重要産業が直面するサイバー攻撃」によると、重要インフラに対する攻撃としては、大規模 DoS 攻撃によるサービスの停止、ネットワーク攻撃またはネットワーク攻撃を仕掛けるとの脅しによる恐喝、システム破壊を目的とするマルウェアなどがある。重要インフラに対する攻撃のもう一つの特徴としては、攻撃が他国政府から行われたと考える IT 管理者が約 60%と高いレベルを示すことである。McAfee の同レポートによると攻撃元として懸念されている国としては、中国、ロシア、米国、北朝鮮などが上げられている。

日本国内では重工、重電など重要インフラを担う企業に対する標的型攻撃の深刻な被害が 2011 年に表面化したことを受けて、情報処理推進機構が重要インフラを担う企業を中心に、サイバー攻撃に対する情報共有と早期対応の場として「サイバー情報共有イニシアティブ(J-CSIP : Initiative for Cyber Security Information sharing Partnership of Japan)」を 2011 年に発足させている。J-CSIP では会員企業から攻撃事例の情報提供を受けて、会員企業に情報共有を行っている。2014 年度の状況としては 2014 年 4 月から 12 月の間に J-CSIP に情報提供された標的型攻撃は 426 件となっており、既に 2013 年度(2013 年 4 月～2014 年 3 月)の合計件数 233 の 2 倍近くに達している。

表 2-2　重要インフラに対する標的型攻撃の状況

	4月～6月	7月～9月	10月～12月	1月～3月	合計
2013年度	64	61	51	57	233
2014年度	226	79	121		426

また、複数の組織を対象とした「やり取り型」標的型攻撃が 2014 年 8 月から 10 月にかけて発生しているが、攻撃対象の担当者の反応を見ながら攻撃手口を変更したり、無害なメールで攻撃対象の担当者を信用させようとしたりするなど、巧妙かつ執拗さを増しており注意が必要である。

2.1.3 制御システム脅威の動向

制御システムといえば以前はオフライン、もしくはクローズドなネットワークに接続された制御専用 OS で動作するシステムであったが、近年はコストダウンのために Linux や Windows などの汎用 OS を活用し、M2M や IoT という言葉に代表される様にネットワー

クに接続されてリモート監視や保守を受けるシステムとなってきている。また、一般的な情報システムと異なり、可用性を最も重視するため、ウイルス対策ソフトの導入や OS の更新が行えないことも珍しくない。そのため、近年サイバー攻撃の対象となる事例も増加している。

表 2-3　制御システムへの脅威事例

米国 1997 年	**米国の重要インフラに直接的な被害を与えた最初の事例** 10 代の若者がダイアルアップモデムを使って、マサチューセッツ州ウォーセスター空港の設備にサービスを提供していた通信事業者 NYNEX のデジタル・ループ・キャリア・システムを停止させ、空港の管制塔、セキュリティ、消防署、気象サービスおよび空港を利用する航空会社の電話サービスを利用不能にした。さらに、管制塔に設置してある滑走路のライトを制御する送信機をシャットダウンしたため、6 時間にわたって同設備を使えなくなった。
豪州 2000 年	**SCADA システムへの攻撃の事例** オーストラリアの SCADA ソフトウェアを開発する企業の元従業員が、上下水処理場の運営会社の職に応募したものの不採用とされたことに恨みを抱き、2 ヶ月の間 46 回にわたって同社の下水処理の制御システムに侵入し、下水排水施設のデータを書き換えたりオペレーションを妨害し、結果として 264,000 ガロンもの未処理の下水を河川や公園に放出した。
米国 2005 年	**ウイルス感染により制御システムが停止する事例** 米国のダイムラー・クライスラー(現ダイムラー)の 13 の自動車工場が単純なインターネットワームにより操業停止となった。情報ネットワークと制御ネットワークの間にはファイアウォールが設置されていたにもかかわらず、Zotob ワームが制御システム内に入り込み、プラント中に広がった(外部から持ち込まれ、制御システムに接続されたノート PC 経由の可能性も指摘されている)。自動車生産は 50 分間停止する状態となったほか、部品サプライヤへの感染も疑われて部品供給の懸念も生じ、およそ 1,400 万ドルの損害をもたらした。
米国 2009 年	**BA システムへのハッキングの事例** テキサス州ダラスの病院に勤務する契約警備員が、病院の HVAC(Heating, Ventilation, and Air Conditioning)システムや顧客情報のコンピュータに侵入し、独立記念日に大規模な DDoS 攻撃を仕掛けることを計画。病院内の PC にマルウェアをインストールする様子を動画で公開するなどしていたことから、SCADA セキュリティの専門家に FBI 及びテキサス州検察局に通報されて発覚し、逮捕された。
日本 2014 年	**ビル管理システムを狙ったポート探索の事例** 警察庁は警察庁の定点観測システムにて 3 月中旬以降 BACnet で使用されているポートに対する探索と思われるアクセスを検知していると発表。関連システムの管理者にシステムの不用意なインターネットへの公開などに注意するよう呼びかけた。

2.1.4 内部犯行

2014 年 7 月に発覚した某通信教育会社の顧客情報漏えい事件は、漏えいした情報が大規模(最大 2070 万件)であったこと、情報へのアクセス権がある内部犯による情報漏えいで

あったこと、その内部犯が通信教育会社の「子会社の委託先の派遣社員」であり重要な情報へのアクセスが許されていたことへの驚きがあったこと、などで企業や組織で情報管理を担当する関係者に、内部者による不正行為のリスクをあらためて認識させる事態となった。シマンテックの「インターネットセキュリティ脅威レポート(ISTR) 第 19 号」によると、2013 年の個人情報漏えい件数に占める原因の割合では内部犯行はハッカーによる攻撃についで 2 位となっているが、一回の漏えい事件での平均漏えい件数でみると 1 位となっており、内部犯行が大規模漏えいにつながりやすいことを示している。

2.2 インシデントハンドリング体制の動向

2.2.1 CSIRT の定義

組織において IT 依存度が高まっている上、セキュリティ上の脅威が巧妙かつ執拗になってきている昨今、コンピュータ・セキュリティに関するインシデントの発生を完全に防ぐことはほぼ不可能な状況になっている。コンピュータ・セキュリティに関するインシデントが発生したとき、組織として的確に対応するためには高い専門性を持つ機能が必要であり、そのための組織が CSIRT である。本報告書では CSIRT を「組織内におけるコンピュータ・セキュリティに関するインシデントハンドリングと、その準備としてのインシデント・脆弱性情報の収集及び、インシデントの発生を予防するための活動を行う機能」と定義する。CSIRT の各局面における機能とその局面で連携すべき他の組織についてまとめると、以下のようになる。

表 2-4 CSIRT の機能

側面	機能	連携組織
組織内部向け	■平常時	
	・ユーザのセキュリティ意識啓発 ・インシデントの早期検知	・組織内ユーザ部署 ・セキュリティベンダ
	■インシデント発生時	
	・インシデント発生情報報告窓口 ・インシデント対応(攻撃経路・影響範囲の分析、復旧作業)、または対応支援 ・経営層との連携 ・部署間調整	・組織内ユーザ部署 ・経営層 ・セキュリティベンダ
組織外部向け	■平常時	
	インシデント動向、攻撃予兆情報、脆弱性等の情報収集	政府機関、IPA、JPCERT/CC、セキュリティベンダ、他組織 CSIRT
	■インシデント発生時	
	インシデント対応機関との連携	政府機関、IPA、JPCERT/CC、セキュリティベンダ、社内(広報)等

コンピュータ・セキュリティに関するインシデントとしては、組織内で利用している情報システムに対するインシデントと、自社製品に関するインシデントの二種類がある。特に後者に対応する機能を PSIRT(Product Security Incident Response Team)と呼んで区別する場合があるが、両者をまとめて CSRIT と呼ぶ場合もある。本報告書では、CSIRT は、PSIRT を包含するより広範囲なインシデント対応を行う機能として捉えるものとする。

CSIRT の要員は専任の場合もあれば、他の部署との兼務、あるいはシステム部門内のバーチャル組織となっている場合もある。

2.2.2 全体動向

国内では組織内 CSIRT 同士の情報共有、緊密な連携体制の実現と共通の問題を解決する場として、2007 年に日本シーサート協議会が発足し活動している。日本シーサート協議会の CSIRT 加盟数は 2013・2014 年に大幅に増加しており、国内企業のコンピュータ・セキュリティに対する危機意識の高まりの表れと見ることができる。日本政府においても 2013 年 4 月までに全省庁に CSIRT が設置されている。また、CSIRT の必要性が認知されるにしたがって、セキュリティベンダなどによる CSIRT 構築・運用支援サービスが登場してきている。

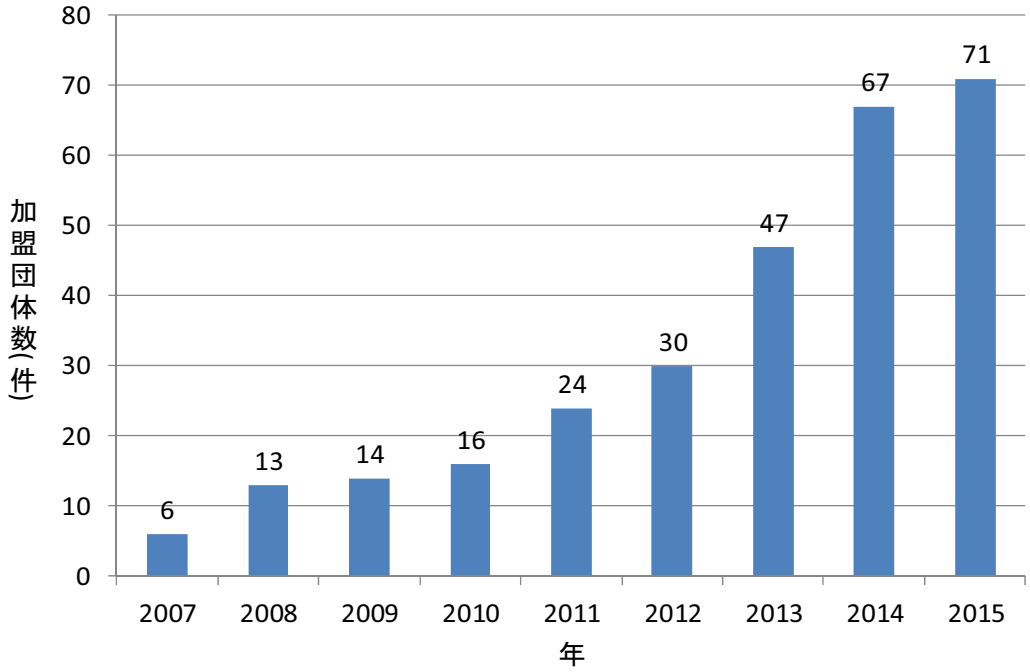

図 2-1 日本シーサート協議会加盟団体数の変化(2015 年 2 月 15 日時点)

第3章　企業のインシデントハンドリング体制の先進事例

第 2 章では CSIRT の必要性とその機能、また、組織の業務形態などによって CSIRT 構築体制が異なることを述べた。

企業で取り扱っている情報資産やインシデントへの対応方針は、それぞれの業界や事業内容によって大きく異なっている。インシデントハンドリング体制として CSIRT を組織に組み込む形態としては、部署毎に専任の CSIRT 要員をもつ「専門組織型」、専任ではないが必要時に CSIRT 活動を担う「兼務（仮想組織）型」、CSIRT 運用は個人にまかされており個人が各部署に働きかける「個人運用型」があるが、企業の文化や業態によって異なる。ここでは、セキュリティインシデントに対して先進的に取り組みを行っている企業について紹介する。

3.1 建設業

3.1.1 リスクへの対応や考え方

建設業では、数千人を越える作業員と 1,000 以上の拠点（作業所、営業所）を保有して事業が運営されている企業もある。昨今は拠点も世界各国に拡がっておりインターネットやモバイル端末の利用も盛んである。

作業所は建設案件によって数年ごとに設置と撤去が繰り返されており、通常の事務所の様に固定されていない。各拠点で作業員は顧客情報（個人情報）だけでなく、設計図、工程表、作業指示書などの情報を共有することで働いている。また、政府関連施設やプラントなどの建設案件に携わっている場合には、何処にどの様な建設をするかという情報も機密情報扱いにする必要がある。また、作業所で従事する作業員は電子情報だけでなく、現場では紙などの物理媒体に記載された情報を利用しており、総合的な管理体制が必要となってくる。

建設業では､設計図等の機密情報が漏えいすることが最も重大なリスクとなる｡その他、情報が利用できなくなり作業が止まること、情報の改ざんで誤った作業が行われるなどがあるが、これらは機密情報の流出に比べてリスクは低くなる。この為、セキュリティ要素の機密性を重視して対策をおこなっている。紙媒体の情報は施錠管理などにより比較的保護し易い。しかし、電子情報のインシデントは、ごく短時間に大量の情報が影響を受け被害が急速に拡大するので、初動対応が重要である。しかし、情報システムの対策だけでは限界があり、インシデント発生時（有事）の初動を効果的に実施する為には、ルールと体制の整備、そして教育などの人的対策が必要となってくる。また、インシデント発生時に受けるリスクは事故媒体（紙や電子情報など）と情報内容（設計情報、契約情報など）によって対応部門が異なる事が多いので、全社的なルールと、全社的なインシデント対応体制を構築する必要がある。

3.1.2 事例（大成建設株式会社）

建設業界の先進的な事例として大成建設のインシデント対応体制がある。大成建設では情報セキュリティポリシーを施行し、社内の正式文書を「紙」から「電子」に変更して管理規定を全面改定した。その後、電子情報セキュリティ・インシデントによる被害の予防対策と緊急時対応体制を強化するため、組織内 CSIRT　Taisei-SIRT（Taisei- Security Incident Response Team）を 2013 年に設置した[2]。

大成建設の情報システムは、社長室配下にある情報企画部とグループ会社の大成情報システムとが一体となって運用管理を行っている。Taisei-SIRT は、この両組織から役職と適正により、組織横断的にリーダークラスの要員によって構成されている仮想組織である。

Taisei-SIRT は、ダメージコントロールの視点からの活動を実施している。インシデントの発生を前提として、たとえ攻撃されたとしても、被害をできるだけ小さく抑えるように活動する。Taisei-SIRT は、平時には、社外組織からのリスク情報の収集、社内ルール改善、セキュリティ啓発などの危機管理（インシデントマネジメント）をする。そして、重大インシデント発生時（有事）には、全社的なリスク対応組織との連携で、迅速な緊急対応を図っている。

このように、既存の全社リスク管理体制と CSIRT とをうまく融合させ、インシデントに関する迅速な情報共有と対応につなげ、そして、インシデントを一刻でも早く発見し、そのビジネスインパクトを判断し、会社全体としての判断を迅速に下せる体制が必要である。

3.2 金融業

3.2.1 リスクへの対応や考え方

金融機関では管理すべきリスクの種類は、信用リスク、市場リスク、流動性リスク（資金調達リスク）、オペレーショナルリスク、決済に関するリスクなどがある[3]。サイバーセキュリティリスクはこれらのリスクに影響しており、多くのリスク対応部署に係わることになる。また、部署によって考え方が異なり、全体の考え方でない場合がある。

金融機関は政府（金融庁）から可用性 100%であることが求められているため、機密性よりも可用性や完全性が非常に重要となる。さらに、金融機関はシステムが大きく、また重要性も高いためサイバーセキュリティへのリソース投入は比較的大きいといえる。また、金融機関は資金を持っているからという理由で狙われることが多い。この為金融機関を狙った攻撃（フィッシング、不正送金マルウェア、DDoS 攻撃など）が増加しているが、金

[2]「電子情報セキュリティ対応体制の強化、Taisei-SIRT を設置」
http://www.taisei.co.jp/about_us/release/2013/1353286819127.html
[3] 三井フィナンシャルグループ ディスクロージャー誌　リスク管理への取り組み
http://www.smfg.co.jp/investor/financial/disclosure/h2607_c_disc_pdf/h2607c_12.pdf

融機関からの大規模情報漏えいは発生していない。

犯罪者は金融機関の持つ資金を狙い、フィッシング等の攻撃を仕掛けてくる。金融機関ではコストを掛けて Web アプリケーションなどのメンテナンスを迅速に行っているので脆弱性を狙った攻撃で被害を受けることは少ない。この為、不正送金マルウェアや DDoS 攻撃が多い。これらは国内外の金融機関でも同様である。

インシデント対応組織は、多くのやるべき事が存在しているので、専門組織として構築されることが多いが、その組織体制は金融機関により大きく異なっており、一概に同じ体制をとっているとは言えない。しかし、金融機関の業務は情報システムに大きく依存しており、業務リスクとシステムリスクとの関連性が非常に強いため、経営トップがサイバーセキュリティ問題への認知度が高いことと、金融監督当局の権限の強さからか他の分野に比べてシステムリスクに対する取り組みの感度が高い。

金融機関では、当局の位置付けが重要である。日本でも金融庁の権限が大きい。米国では、金融規制は必達になるため管理・監査項目への対応が大変である。金融業界は、規制は望ましくないと考えているため、事故に繋がらないよう、業界主導・自主的に活発に活動している。

3.2.2 事例（みずほフィナンシャルグループ）

金融業界の先進的な事例としてみずほフィナンシャルグループのインシデント対応体制がある。みずほフィナンシャルグループでは 2012 年にサイバー攻撃を専門的に対応するための部署として、サイバーセキュリティチーム Mizuho-CIRT(Mizuho Cyber Incident Response Team)を IT・システム部門内に設置した[4]。

Mizuho-CIRT の主な活動は、インターネットバンキングへの攻撃対応（フィッシング、Banking Trojan）、イントラ標的型攻撃への対応、Web システム全体の脆弱性対応などを実施している。特にフィッシング対策に関しては利用者にも大きな影響を与えること、フィッシングサイトでマルウェア感染することがあるで、フィッシングの観点からも Mizuho-CIRT の活動が注目されている。

Mizuho-CIRT では、フィッシングサイトの発生を早期に検知するために様々な情報提供先から情報を入手して、フィッシングサイトの分析を実施する。そしてフィッシングサイトの発生を検知した場合には、フィッシングサイトによる被害極小化のために、サイトの停止、利用者への注意喚起、アンチウィルスでのブロックなどを行う。この被害極小化では様々な部署と外部機関とのやり取りが発生するのでこの対応も Mizuho-CIRT が実施する。

---

[4] フィッシング対策協議会セミナー資料「フィッシング対策と CSIRT について」
https://www.antiphishing.jp/news/pdf/apcseminar2012mizuho.pdf

Mizuho-CIRT の重要な役割は、サイバーセキュリティに対する「専門窓口」である。これにより、次のようなことが実現できる。

(1)自社内の情報集約

・インシデント情報を集約、何が起きているのか正確に認識する。

・必要な権限者、部署への情報展開。

(2)対外窓口

・フィッシング対策協議会、JPCERT/CC、警察、他行・他企業、等と連携する。

・自社からの情報発信窓口。

(3)事象の分析

・顧客感染型の出現等攻撃は高度化しており、それに応じた知識とノウハウを持った専門家。

Mizuho-CIRT はこの様に専門組織として活動を行っている。

3.3 重要インフラ

2014 年に政府から発行された情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」において、重要インフラは、従来の 10 分野に新たに 3 分野が加えられ、13 分野になった。

基本的に重要インフラは可用性 100%と、安全・安心の確保が望まれている。
情報セキュリティに関しては IT 推進部門がインシデント対応も担っており、CSIRT のような専門的な組織よりも個人運用に近い形になっている場合が多かった。しかし、各組織も全社的なインシデントへの対応体制を構築することを目指している。また、重要インフラで利用されるシステムは、各分野においても、事業内容や事業環境によってそれぞれ異なったシステム構築しており、一律なリスク対応をすることができない。このため、各事業者はセキュリティインシデントが発生することを前提として体制を構築している。

3.3.1 リスクへの対応と考え方

重要インフラ事業の中心となる制御システムは、情報システムと直接には接続していないクローズド環境であることから情報セキュリティインシデントに対する脅威は少ないと考えられている。制御システムに使用している機器（PC 等）に、脆弱性パッチなどをあてると、かえってシステムの挙動がおかしくなり稼働できない可能性があるため、即座にはパッチをあてない判断をすることもある。

但し、制御システムの構成機器とは USB メモリなどでデータを交換することもあるため、現在で考え得るセキュリティ対策（USB メモリのウィルススキャン等）を施すなどしている。

内部犯行への対策については、手順のマニュアル化と安全教育を実施し対応している組

織がほとんどである。

完全に閉ざされたシステムであれば良いが、一箇所でもオープンな環境に接続されてしまうとそこが大きな脆弱な箇所となるので、システムのセキュリティ状態の見える化と管理が必要といえる。サイバー攻撃、内部犯行などの意図的要因、ハードウェア／ソフトウェア障害やオペレーションミスなどの非意図的要因、災害や疾病、他分野からの波及等が脅威になることは認識している。

3.4 企業リスクに応じた取り組み

それぞれの企業の置かれた環境や事業内容は異なっている。事業によって顧客情報（個人情報）、設計情報などの機密情報の漏えいを最大のリスクにするのか、システムの可用性低下が最大のリスクなのかにより対策の方針やセキュリティ意識が大きく異なっていることが、今回実施したアンケート（付録）[5]の結果から読みとれる。

保有された個人情報などの機密情報が多い企業と少ない企業、そして可用性を最大限に要求される重要なシステムの有無によって分類すると企業の考え方が見えてくる。（表3-1）

5　株式会社三菱総合研究所「新たな脅威に対する組織の対応体制に関する調査」2015 年

表 3-1 重要なシステムの有無と保有する個人情報量による企業の特徴

		重要なシステムの有無	
		あり	なし
保有する電子化された個人情報の量	多い	【セグメントA】 ・金融・保険、情報通信、流通・EC 等 ・企業規模は大きい（予算、従業員数共に） ・IT 投資、セキュリティ投資、CIO 設置率も高い ・全体的にリスク意識は高く、特に情報漏えいを重要視 ・より高度なツールを導入し、改善要求がある ・チームは経営直下の場合もあり、様々な機能を持つ 特に経営や社外への報告機能 ・セキュリティインシデントへの課題意識は強い	【セグメントC】 ・製造、大手小売、医療・福祉 等 ・企業規模は比較的大き目 ・IT 投資に対してセキュリティ投資が小さい傾向 ・一番の脅威は内部要因によるシステム障害 ・情報漏えい対策ツールの導入率が比較的低い ・ツールは最低限の機能しか求めていない ・情シス内の専門チーム。機能は限定的で、社内調整がメイン ・セキュリティインシデントへの課題意識は高くない
	少ない	【セグメントB】 ・製造、電気・ガス・水道等、卸売等 ・企業規模は比較的大き目 ・CIO 設置率は高い ・セキュリティ意識は比較的低い ・ツールへの満足度は低い ・セキュリティインシデントへの課題意識は強くない	【セグメントD】 ・製造、中小小売、サービス 等 ・企業規模が小さい（予算、従業員数共に） ・IT やセキュリティ投資が小さい ・チームは組織構造がフラットなため、経営直下の割合が高く、かつサービス停止権限もつ ・平常時も緊急時も機能は少ない ・セキュリティ課題意識はあまりない

【セグメントA】個人情報多い　×重要なシステムあり（例；金融、建設、情報通信、流通・EC 等）
【セグメントB】個人情報 少ない×重要なシステムあり（例；電気・ガス、製造、卸売等）
【セグメントC】個人情報多い　×重要なシステムなし（例；医療、大手小売等）
【セグメントD】個人情報 少ない×重要なシステムなし（例；サービス、中小小売等）

情報漏えいの観点からはセグメントAとCに同様のリスクがあるが、セグメントCのセキュリティ意識が低いことがわかる。セグメントDについては企業規模が小さく、予算も少なくセキュリティ対策にまで対応できていないことがわかる。

重要なシステムを保有しているという企業（セグメント A、B）は、安定してシステムを動作させることを最重要とすることが求められており、比較的システムへの投資が多く行われている。

特に、重要なシステムを保有しており個人情報が多い企業（セグメントA）は、システムで取り扱っているデータ自身に価値があるため情報漏えいは、直接的に事業リスクに結びつく。このためセキュリティインシデント対策も積極的に進められている。重要なシステムを保有しており個人情報が少ない企業（セグメントB）は、システムで取り扱っているデータには直截な価値はなくシステムが提供する動作が価値を作り出していると言える。

従って、システムを安定して動作させるコストはかけるがデータを保護するセキュリティにはあまり投資しないと言える。

重要なシステムがないという企業（セグメント C、D）は、システムは業務効率化のために利用しているのであり、セキュリティ投資は最低限しかかけられないで業務効率を中心に考えていると思われる。

重要なシステムがないが個人情報を多く持つ企業は、システムへのセキュリティ投資コストとインシデント発生時の対応コストの投資対効果を常に考えており、インシデント発生時に損害賠償をすれば良いという考え方もある。重要なシステムがなく個人情報も少ない企業は事業規模も小さく、従業員も少ないことが多い。このため、インシデント体制の構築のみならず、セキュリティ対策すらできない企業もある。

これらの企業状況を分析するとそれぞれのセグメント毎の要求は表 3-2 のように考えることができる。

表 3-2　企業のセグメント別にみるセキュリティ対策

		重要なシステムの有無	
		あり	なし
保有する電子化された個人情報の量	多い	【セグメント A】 ・セキュリティ予算は大きく、現在様々なセキュリティソリューションやツールを導入している ・今後より高度な機能や最新のツールを望んでいると考えられる。	【セグメント C】 ・個人情報を多く持つ、規模の大きな企業が多いが、重要システムを保有していないため、セキュリティ意識が不十分と考えられる。 ・今後、サイバー攻撃リスクが上がるに伴い、セキュリティソリューションやツールを導入する可能性がある。
	少ない	【セグメント B】 ・重要システムを保有しているため、必要最低限のセキュリティは実施していると考えられる。 ・ツールへの要望等は具体的にはあがってこない。	【セグメント D】 ・小規模な企業が多く、セキュリティを導入することが容易でない ・高度なセキュリティソリューション・ツールの導入によりも最低限の機能を備えた、簡便なツールが求められると考えられる。

ビッグデータを活用する社会では、情報システムで個人情報やプライバシー情報を含んだパーソナルデータを活用するシーンが増大する。このためデータの適切な保護が必要となってくる。セグメント C,D にみられる「重要なシステムがない企業」はパーソナルデータを活用するには脆弱な状態であるといえる。これらの企業においても、今後のビジネス展開を考えるとパーソナルデータの活用が不可欠と考えられるため、低コストで利便性の高いセキュリティ対策ソリューションのニーズが高まると考えられる。

第4章　インシデントハンドリングに関連する製品やソリューションの動向

サイバー攻撃や情報漏えいなどの情報セキュリティに関わるインシデントが発生した際の被害を最小化するためには、インシデントの発生を前提とした十分な備えと、インシデントが発生した際の迅速な対応を可能にするインシデント対応の環境と体制の整備が必要となる。

近年、インシデントハンドリングの活動を支援するためのさまざまな製品やソリューションが提供されているが、それらの導入・利用に当たっては、各企業の事業内容に応じた情報セキュリティ上の脅威、リスク、コスト効果等を総合的に判断した上で進めてゆく必要がある。

本章では、インシデントハンドリングに関連する製品やソリューションについて、今回実施したアンケート調査の結果（付録）と、さまざまな業種の企業へのヒアリング結果を踏まえて概観する。

4.1 製品やソリューションの動向

アンケート調査の結果、情報セキュリティ関連の製品やソリューションの導入状況・意向に関しては、「ログ管理・分析」、「システム可視化・イベント管理」、「セキュリティ監査・審査」、「クライアント端末監視・管理」、「ポリシー管理・設定管理・動作監視制御」など、おもに事業継続や内部統制などを目的とした製品・ソリューションを導入している企業は全体の約 50%前後であるものの、「インシデントハンドリング」、「統合ネットワーク監視・遮断」、「個人情報漏えい対応」、「フォレンジック」、「脆弱性診断」、などのインシデントハンドリング関連の製品・ソリューションを導入している企業は全体の約 30%前後に過ぎないことがわかった。

現在、インシデントハンドリングに関連する製品やサービス/ソリューションには、さまざまなものが提供されており、各企業が事業継続を図る上での情報セキュリティ上の脅威、リスクとその受容可能レベル、期待されるコスト効果等に応じて、さまざまな商品・サービス/ソリューションの導入/利用を選択できるようになっている。表 4-1-1 に、インシデントハンドリング関連製品やサービス/ソリューションをまとめる。

表 4-1-1 インシデンハンドリング関連製品/ソリューション

	対応フェーズ	活動	製品	サービス/ソリューション
事前対応	準備	脆弱性情報入手		脆弱性情報提供サービス
		脆弱性検査	ネットワーク脆弱性検査ツール Web アプリケーション脆弱性検査ツール	プラットフォーム診断 Web アプリケーション診断
		サイバー演習	IT セキュリティ予防接種ツール	インシデント対応訓練 IT セキュリティ予防接種
	検知、分析	侵入検知/監視	侵入検知システム (IDS/IPS/WAF) 改ざん検知システム 脅威分析システム（ふるまい検知システム）	MSS（マネージド・セキュリティ・サービス）
		ログ管理/分析	統合ログ管理システム SIEM	SIEM 運用 セキュリティ・インテリジェンス
事後対応	封じ込め、根絶、復旧	インシデント管理	インシデント管理システム	インシデント対応
		フォレンジック	データ保全ツール 分析ツール	フォレンジック解析
	発生後対応	証拠保管	データ保全ツール	フォレンジック解析

4.2 製品ソリューションの適用例

ここでは、4.1 章で述べたインシデントハンドリング関連の製品、サービス/ソリューションの中から主要なものの適用例について述べる。

4.2.1 脆弱性検査

インターネット上に公開された Web サイトに対して脆弱性検査を実施し、発見された脆弱性を除去することは、不正侵入のリスクを軽減させるのに有効である。Web サイトの脆弱性を検査するツールには、Web アプリケーションとしての実装上の脆弱性を検査する「Web アプリケーション脆弱性検査ツール」と、ネットワーク設定や OS/ミドルウエアに内在する脆弱性を検査する「ネットワーク脆弱性検査ツール」があり、これらのツールを併用して検査を実施することが望ましい。（表 4-2-1 に各ツールによる検査内容を示す。）

これらのツールのうち、特に、ネットワーク脆弱性検査ツールに関しては、攻撃者が脆弱性のある Web サイトを探索するためにも利用していることから、攻撃対象となるリスクを回避するためにも、有効である。

表 4-2-1 脆弱性検査ツールでの検査内容

検査ツール	検査内容
Web アプリケーション脆弱性検査ツール	• OWASP トップ 10[6]、SANS トップ 25[7]等の Web アプリケーション脆弱性の検査
ネットワーク脆弱性検査ツール	• 不要オープンポートの有無 • 未適用パッチの有無 • 侵入コード（Exploits）への耐性 • 権限昇格の脆弱性有無 • バックドアの有無

一方、上記のような脆弱性検査ツールを購入して自社で検査を実施することが、スキル要員の不足やコスト効果の点で困難な場合がある。このため、脆弱性検査を実施するサービス（プラットフォーム診断サービス、Web アプリケーション診断サービスなど）が、セキュリティ専門ベンダから提供されている。なお、脆弱性検査サービスでは、ネットワークを経由してセキュリティ専門ベンダからリモートで実施する検査と、検査担当者が依頼者側に訪問して実施するオンサイト検査が提供されるのが一般的である。

なお、新たな脆弱性が発見された際、脆弱性検査ツールを用いていつでも自社で検査できる体制と、セキュリティ専門ベンダによる攻撃者視点での検査の両方を実施することにより、高い即応性と精度の検査が可能となる。

4.2.2 モニタリング/検知

攻撃の発生を検知し、攻撃を遮断するためには、IDS、IPS、WAF などの侵入検知システム（センサーアプライアンス）を導入することが有効である。今回のヒアリング調査の中でも、システムへの不正侵入や改ざん、情報漏えいなどのインシデント発生後の原因調査や証拠保全などの事後対策よりも、インシデントの発生に至らないよう、入口での侵入抑止のためにモニタリング/検知環境を充実させたいという意見が多く聞かれた。また、アンケート調査の結果でも「統合ネットワーク監視・遮断」導入済み企業が約 40%と比較的高い割合となっており、モニタリング/検知に関心が高いことがわかる。しかしながら、その一方で、侵入検知システムを導入することで、脆弱性検査やパッチ適用が不要になると誤解してしまっているケースもあることが懸念される。

一方、このような侵入検知システムの導入に際しては、システムが検出するアラート情報を分析し、関係者に警告を通知するための運用体制（SOC：セキュリティオペレーションセンター）の構築が伴う。このため、専門的なスキルを備えた人材がいない企業の場合は、コスト/効果の点から、セキュリティ専門ベンダが提供している 24 時間 365 日体制のマネージドセキュリティサービス（MSS）を利用することが多い。

---

[6] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[7] http://www.sans.org/top25-software-errors/

なお、監視対象とするサイトが、さまざまなデータセンターに分散して存在している場合、それぞれのデータセンターに侵入検知システムを導入する必要が生じてしまうことから、このことが障壁となり導入が進まないケースもある。

さらに、昨今、コスト最適化のため、パブリッククラウド上への既存システムの移行や新規システムの構築を進める企業が増えている。しかしながら、パブリッククラウドが運用されているデータセンター内に侵入検知のためのアプライアンス機器を設置することは難しい。このため、ソフトウエア型や SaaS 型の侵入検知システムも提供されているが、導入企業での運用・監視を前提としたものが主流であり、セキュリティ専門ベンダによる常時監視サービスの提供が少ないのが現状である。

4.2.3 ログ管理/分析

各種ネットワーク機器やセキュリティ関連システム、OS、アプリケーションなどのさまざまな情報源からのログ情報を収集し、時系列的な相関関係を把握できるようにしておくことは、内部統制、および、インシデント発生時の原因究明、証拠保全、説明責任の確保といった点で重要となる。今回のアンケート調査の結果からも、「ログ管理・分析」の製品・サービスを導入済みと回答した企業が約 60%近くを占めていることから、各企業とも関心が高い内容であることが分かった。

近年、さまざまな形式のログを収集・分析可能とする「セキュリティ情報およびイベント管理システム（SIEM: Security Information and Event Management）」、および、SIEM の構築と運用を支援するサービスが提供されており、SIEM の導入により、表 4-2-2 に示すような多様な生成元からのログデータの時系列的な相関関係を迅速に把握し、インシデント発生の原因究明やインシデント発生の兆候分析を迅速に実施することができる。

しかしながら、単にログ情報を収集するだけでは SIEM の構築を進めることは難しく、守るべき情報や攻撃シナリオに基づいて十分なログ設計を行った上で導入する必要がある。特に、今回、先進的なインシデントマネジメント体制を備えている企業へのヒアリング調査でも、同様の示唆を得ることができた。

また、重要インフラなど、大規模な制御系システムにおける統合ログ管理システムの導入に関しては、制御系システムの多くがカスタマイズされた環境であることから、商用システムとの互換性を図ることが課題であることが、ヒアリング調査の結果からわかった。

さらに、収集されたログ情報をリアルタイムで分析し、その結果を可視化する「セキュリティ・インテリジェンス」と呼ばれる製品やサービスも、近年、提供されるようになってきている。

表 4-2-2 統合ログ管理システムの情報源

分類	ログ情報
ネットワーク機器、セキュリティ関連システム	下記システムのログ ・アンチウィルス ・侵入検知・防御システム ・Web プロキシ ・脆弱性管理ソフトウエア ・認証サーバ ・ルータ ・ファイアウォール ・ネットワーク検疫サーバ
オペレーティングシステム	・システムイベント ・監査記録
アプリケーション	・クライアントとサーバ間で交換されたメッセージ ・認証履歴、アカウント変更履歴等 ・トランザクションの統計情報

4.2.4 デジタル・フォレンジック（コンピュータ・フォレンジック）

不正侵入や内部不正による情報漏えい等が発生した場合、法的紛争や訴訟に備えて、データの保全、調査・分析を行うとともに、改ざん、毀損等について分析・情報収集等を行う必要が生じる。これらの一連の調査手法と技術は、「デジタル・フォレンジック」、または「コンピュータ・フォレンジック」と呼ばれる。[8]

インシデント発生時の初動対応におけるデータ保全を支援する製品として、HDD 複製機器（デュプリケータ）、保全用ソフトウエアなどがあるが、一般に、これらの製品を用いて確実にデータ保全を実施するためには高度な専門スキルが要求される。このため、情報漏えい等の事故が発生した際には、セキュリティ専門ベンダが提供するデジタル・フォレンジックサービスを利用するのが一般的であるが、事故が発生してから NDA や業務委託契約の締結を開始すると時間がかかってしまい、本来の事故対応が遅れてしまうといった課題があることが、ヒアリング調査の結果からわかった。

4.2.5 教育/人材育成

インシデントが発生した際の、封じ込め、根絶、復旧を的確に行えるようにするため、インシデント対応訓練を実施することが有効である。今回のアンケート調査の結果からは「緊急対応訓練支援」については、実施済み、もしくは実施を計画している企業は全体の約 30%程度ではあるものの、ヒアリング調査を実施した重要インフラを持つ企業の場合では、システムベンダ等を含め、より広範な関係者を含めた訓練の実施が重要であるという意見が聞かれた。

一方、セキュリティ人材の不足から、インシデントハンドリングを担当するメンバのス

[8] デジタル・フォレンジック研究会　https://digitalforensic.jp/home/what-df

キル開発も重要とされてきている。インシデントハンドリングに関する教育コースとしては、TERENA[9]（欧州研究教育ネットワーク協会）が開発した TRANSITS[10]がある。TRANSITS には、TRANSITS-I（入門編）と TRANSITS-II（応用編）があり、現在、日本シーサート協議会が日本語による TRANSITS-I の研修会を定期的に（年 1 回）に開催している。

また、アンケート調査の結果、「教育・トレーニング、意識向上のための啓発」についてのニーズも比較的高いことがわかった（導入済、導入検討中を含めて約 50%）。このニーズに応えるサービスのひとつに、近年、大きな脅威となっている標的型攻撃メール（APT 攻撃）に関して、従業員を対象に疑似的な標的型攻撃メールを送信し、添付文書や本文中のリンクの開封率を計測する訓練サービス（IT セキュリティ予防接種）が、セキュリティベンダから提供されている。

4.2.6 脅威情報/脆弱性情報の共有

迅速なインシデント対応を実現するためには、脅威情報や脆弱性情報を早期に入手し、早期に攻撃の兆候を察知できるようにすることが重要となる。現在、脅威情報や脆弱性情報を、メール配信、フィード配信、Web 上で閲覧可能にするサービスが、JPCERT/CC、US-CERT 等から提供されている。

また、脅威情報を共有するコミュニティとして、重要インフラ事業者を対象にしたサイバー情報共有イニシアティブ（J-CSIP）や、金融機関を対象にした FS-ISAC[11]（米国）、金融 ISAC（日本）[12]などの取り組みもある。

---

9 TERENA: Trans-European Research and Education Networking Association
10 https://www.terena.org/activities/transits/
11 FS-ISAC（Financial Services Information Sharing and Analysis Center）
https://www.fsisac.com/
12 http://www.f-isac.jp/

第5章　インシデント対応に関する課題

本章では、会員企業を取り巻くインシデント対応に関する現状と課題について、また企業内インシデント対応組織である CSIRT 構築・運用に際しての課題について検討した。

5.1 会員企業を取り巻くインシデント対応の現状

企業で扱う情報機器は、PC、サーバ、ネットワーク、大容量記憶媒体など多岐に渡り、大量の情報を簡単に扱えるようになったが、一方でサイバー犯罪は増加し、コンピュータウイルスの蔓延や標的型攻撃などの新しい脅威やリスクも顕在化してきている。スマートハウスやヘルスケア、医療関連分野で具体化してきている IoT（Internet of Things）などの技術革新による新たなプライバシーに関するリスクがある。また、内部犯行による情報漏えいはサイバー攻撃についで 2 番目の件数となっており、2014 年に発生した大規模な顧客情報の漏えいは個人情報保護法の改正内容にも影響[13]するほど問題になった。インシデント発生時の影響も大きくなり、企業や組織における情報セキュリティ対策は、ますます重要かつ多様化してきている。

2013 年度と 2014 年度のサイバー攻撃の事例を紹介したが様々な業種で多くの被害が発生している。サイバー攻撃などのインシデントが発生すると企業はインシデントの把握と分析、被害抑制のための方策の決定、被害の把握、マスコミ対応、顧客への謝罪や補償などさまざまな対応を実施することになる。インシデントレスポンスでは社外に対しても適切なメッセージを迅速に発信することが求められるなど、迅速な対応が被害を低く押さえることになる。ところが、インシデント発生時の対応の多くはセキュリティ技術者ではないシステム管理者が実施しており、システム管理者が経験則からインシデントを判断すると、「障害」を念頭に置いた切り分け調査を行うためにサイバー攻撃か障害かの一次判断が遅れる場合が多い。

組織としてコンピュータ・セキュリティに関するインシデントが発生したとき、的確に対応するための部署である CSIRT が 2013 年、2014 年に大幅に増加しており、日本シーサート協議会の加盟数は 2013 年の 47 団体から 2015 年 2 月の 71 団体となっている。また、本委員会で実施したアンケートでは 5 割ほどの企業がインシデントに対応する組織を持っていると回答している。それ以外の企業のほとんどで、情報システム部門がインシデントに対応する、としておりインシデントに対する対応を想定しているようであるが、個人情報の保有状況や重要システムの業務との関わり具合により、インシデントレスポンスの重要性の認識には差がある。緊急対処時の体制が確立した理由として、実際のセキュリティ事故発生事例を挙げる組織が多く、報道などで対外的な信用の損失が伴って初めて予

[13] http://www.cas.go.jp/jp/houan/150310/siryou1.pdf
「個人情報データベース等提供罪の新設」等

算が割かれる状況がみられる。

多くの場合、インシデント対応の活動は経営層直轄の強い権限や組織横断力を行使するのが難しいようである。ただし、重大なインシデントで報道される規模の事象となれば社長直轄や、経営層やリスク管理部門が参加することになる。

アンケート調査を実施した結果から、セキュリティ関連の製品・サービスの導入に関しては、「ログ管理・分析」、「セキュリティ監査・審査」、「システム可視化・イベント管理」、「クライアント端末監視・管理」、「ポリシー管理・設定管理・動作監視制御」など、おもに事業継続やインシデント発生時の対応を図ることを想定した製品・ソリューションを導入済みの企業は比較的多いものの、インシデント発生前の、予防や検知を支援する製品・ソリューションを導入済みの企業は、まだそれほど多くなかった。

また、重要インフラを担う企業を中心に 2011 年に発足した「サイバー情報共有イニシアティブ（J-CSIP）」では 2014 年度の状況としては 2014 年 4 月から 12 月の間に J-CSIP に情報提供された標的型攻撃は 426 件となっており、既に 2013 年度(2013 年 4 月～2014 年 3 月)の合計件数 233 の 2 倍近くに達している。一般企業においても、工場の製造装置や計測機器、業務用の様々に機器が制御システムとして通常の情報機器とは異なる管理の中で新たな脅威があることが把握されてきている。

CSIRT を構築・運用している先進企業では、インシデント対応の活動は全社的な対応が必要となることがあるため、経営層と日常的なコミュニケーションを行う、問題意識の共有を図る、など、経営層の認知とサポートを得るための活動を行っている。ネットワークやセキュリティの監視を継続的に行い、インシデント発生の調査分析を行うなど非常に専門性の高い技術者が必要であるが、外部のサービスを活用し各組織の状況に合わせて機能をインプリメントして実現している。専門人材は常に必要とされているが、求めて得られる状況ではなく各企業の状況に合わせ育成を図っている。類似した課題を他の組織がどのように解決したのか、事例を共有し効果的な活動としている。

5.2 インシデント対応の課題

インシデント対応を企業・組織が行うための課題をあげる。

昨今の脅威である標的型攻撃は公開される前の脆弱性を悪用した攻撃も散見され、また大規模な攻撃とはならないので、報道などで攻撃が表面化せず、その様な攻撃パターンが存在することが知られにくく、従来の様に製品ベンダやセキュリティベンダからの情報だけでは充分な対処を行うことが困難なことが課題として挙げられる。また、多くが海外からの攻撃であり、他国での被害発生状況の早期入手が必要なことも多い。業界・分野の他組織と情報を共有し、更には海外組織との情報共有のための、FIRST(Forum of Incident Response and Security Teams)等のグローバルなコュミニティとの連携や新たなコミュニティの形成が必要だと考えられる。

インシデント発生による企業が受ける損害が時として非常に甚大であることは述べてき

たが、インシデント自体を全く防ぐことは現実的ではなく、インシデントの被害をいかに少なく抑えるかが重要である。そのための課題が、インシデントに対応する初動の迅速化と復旧の早期化である。

現在の様に日常的に脆弱性が見つかり対応を迫られ、また自社の Web ページが改変されるなど様々なサイバー攻撃が存在する中で、迅速な対応を行うための組織が CSIRT である。CSIRT のあり方は多種多様で、ガイドはあるが決まった形が無く、個々の組織の特性に応じて体制を整備していく必要がある。CSIRT の運営のためにはネットワークやセキュリティの監視を行うなど専門的な活動が必要であり、何よりインシデントの影響度を見極め、どのような対応を取るのか判断する、または経営が判断できる情報の提供を行う能力を自社内に持つ必要があり、人材不足が課題である。

多くの情報機器や様々なソフトウェアを利用している環境で、脆弱性情報を得て素早く対応するためには保有する IT システムの構成管理が課題となる。

前節の繰り返しになるが、インシデントの緊急対処時の体制が確立した理由として、実際のセキュリティ事故発生事例を挙げる組織が多く、報道などで対外的な信用の損失が伴って初めて予算が割かれる状況がみられる。インシデント対応はその内容によっては様々な部署と連携して素早く全社的な対応をとる必要がある。また、重大事象では社長など経営トップがマスコミ対応する必要があるなど経営上重要な扱いが必要とされるが事故が発生するまでその認識が得られないなど、CSIRT の認知度の向上が課題である。

第6章　提言

本章では、インシデント対応体制を構築しようとしている組織、およびそれらの組織を支援するビジネスへの提言を記す。

6.1 新たな脅威に対する組織の対応体制の在り方

CSIRT の主要な役割として、インシデントが発生した際にその被害を最小に留める為の事後対応と、インシデントを未然に防ぐ為の事前対応（情報収集と脆弱性への対処など）が挙げられる。

サイバーセキュリティの脅威としては、従来は不特定多数に対するコンピュータウイルスやワームによる無差別的な被害を生じさせるものが主流であった。このような脅威では被害が大規模となる場合があるが、その攻撃手段は均一なものであり対処が比較的容易である。また、被害が大規模ゆえにその様な脅威が存在することが広く知られる事となる。

しかし、昨今は特定少数を対象とした標的型攻撃が頻発しており、巧妙かつ高度な攻撃手法がとられるようになっている。従来の攻撃では公知となった脆弱性を悪用するものが大多数であったが、標的型攻撃においては公開される前の脆弱性を悪用した 0-day 攻撃も散見される。これらの新たな脅威では特定の組織のみを標的としており、無差別・大規模な攻撃とはならないので、報道などで攻撃が表面化せず、その様な攻撃パターンが存在することが知られにくい。脆弱性情報の入手経路として、従来の製品ベンダやセキュリティベンダからの情報だけを活用するのでは充分な対処を行うことが困難となりつつある。

標的型攻撃の様な高度な攻撃では、ある組織が攻撃された後に当該組織と同じ業界・分野の他組織に対して引き続き同様の攻撃がなされる事例が見られる。この様な状況下、同様の脅威を未然に防ぐことができるよう、同業他社などとの情報共有の推進やコミュニティの形成により高度な攻撃への早期対応を図ることが有効である。

情報共有の枠組みの一例として、サイバー情報共有イニシアティブ（J-CSIP）がある。この様な既存の情報共有の枠組みは政府が主導した特定業種・大規模企業向けのものが主であるが、サイバー攻撃が日常的に発生している現在、業界・分野内での情報共有の更なる推進、中小企業向けの情報提供の枠組み構築、新たな視点でのコミュニティ形成、国際的な情報共有の推進など、更なる情報共有の深化が必要と考えられる。

新たな脅威に対する組織の対応体制としては、事後対応に備えることはもちろん、事前対応に向けた活動も重要となる。脅威に関する情報収集や組織外との情報共有を行い、他組織での被害事例を把握することで同様の脅威への対処に役立つ。その為には、入手した情報を CSIRT が適切に解釈、補足した上で自組織内への注意喚起と必要な対策を展開する機能を担うことが一層重要となる。CSIRT はサイバーセキュリティ情報のハブとなり、必要な組織に対して迅速に情報を伝達できる機能・体制を整備することが必要である。

6.2 導入・強化のシナリオ

これまでに示した通り、CSIRT のあるべき姿は一律ではなく、組織によって異なる。CSIRT の目的や組織の背景などを踏まえ、各組織の実態に即した CSIRT を構成する必要がある。ここでは自組織のインシデントへの対応を目的とする組織内 CSIRT について記す。

CSIRT の一義的な役割として、インシデント発生時に迅速に対応し、被害を極小化することが挙げられる。この為、CSIRT の導入を進める際には、まずは適切なインシデント対応を実践できる体制を構築することとなる。

CSIRT とは必ずしも実体のある、専任の要員を抱えた組織体として形作られる必要はなく、インシデント対応の機能を提供できるならば兼任者からなるバーチャルな組織でも構わない。インシデント発生時のハンドリング体制（誰がどのような情報をエスカレーションし、誰が判断を下すのか、等のルールの明確化）を整備し、インシデント発生時に迅速かつ適切な判断を行い、被害を最少化できる体制の確立が第一段階となる。

ハンドリング体制を検討する際には、組織の現状を踏まえ、既存のインシデント対応体制があればそれを活用して整備すべきである。当初からあまりに理想論に走った体制を目指すと実効性を伴わない場合が多く、理想像を見据えた上で着実な体制整備を進めることが望ましい。

インシデントに速やかに対応するには、できるだけ早くインシデントが発生したことを検知する必要があり、その為には IT システムの状況を常時把握できる必要がある。迅速にインシデントを検出するためには、適切な内容の監視やログ取得及び分析・評価を適時に実施できるよう、監視と分析を自動化する事が望ましい。インシデントの早期検出により、早期に事後対応を開始でき、事態収拾の期間短縮にもつながる。また、ログ取得は起きてしまったインシデントへの対応の為だけではなく、その様なログを取得していることを組織内に周知することにより、内部犯行の抑止にもつながる。

IT システムのログを適切に取得していない、あるいは取得していたとしても監視・分析等を実施していない場合には、情報漏えい等の事件が発生したとしても組織内ではインシデントを検出することが困難となるし、対策していたとしても検出漏れのおそれは残る。外部からの通報で初めてインシデントを認知する状況も考えられ、その様な場合に備えて、セキュリティインシデントのおそれがある事象が報告された場合の連絡ルート、部門間の連携等について事前に検討しておくことは重要である。

CSIRT を構築・運用する際に多くの組織で課題となるのが技術的知識や人材の不足である。攻撃者側は営利目的の為グローバルに連携しており、高度かつ巧妙な攻撃の脅威が増大し続けている。加えて、IoT といった新たなネットワーク接続デバイスが増え、攻撃の形態およびリスクもこれまで以上に増えている。刻々と状況が変わるセキュリティ事情に追随していくのは容易ではない。この問題は簡単には解決できるものではなく、セキュリ

ティベンダ等の外部専門サービスの活用も含めて検討が必要であろう。

しかし、技術的知識あるいは人材の不足はサービス活用により補えるが、インシデント対応には組織としての判断が必要となる場面が生じる。例えば、情報漏えい事故が発生し事業に大きな影響を与え得る場合には、経営層の判断が必須であろう。技術的な対応はアウトソースできても、判断を下すのは組織内の適切な管理者が行わねばならない。サービスを活用する場合には、どこまでをサービス提供事業者に任せ、どこからは事業判断として自組織で決断する必要があるか事前に検討し、判断基準を整備しておくことが望ましい。

ハンドリング体制を確立した後は、インシデントを未然に防ぐ為の事前対応の整備を進めることが望ましい。ベンダ等からの脆弱性情報収集やインシデント事例収集と分析、脆弱性への対応を行い、インシデント発生に備える。更に一歩進んで、外部組織の CSIRT と連携し、インシデントの早期検知やノウハウの共有を進めることも考えられる。日本国内での CSIRT 間連携の為のコミュニティとして、NCA（日本シーサート協議会）や国際的な連携の場としては FIRST がある。必要に応じて、その様なコミュニティへの参画も検討されたい。

脆弱性が公表され、その対応を行おうとした際に、構成管理が課題となる場合がある。組織が保有する IT システムでどの様なソフトウェアのどのバージョン、リビジョンが利用されているか、パッチの適用状況はどうか、といった情報が適切に管理されていないと、対策要否の確認や対策実施に時間を要してしまい、場合によっては対処漏れが生じうる。IT システムでの構成管理、変更管理の欠如が、適切な事前対応を行う際の妨げとなる場合があるので注意が必要である。なお、IT システムを構成するすべてのソフトウェアにおいて脆弱性を内包するリスクを抱えている。構成管理を行う際には有償の商用ソフトウェアだけでなく、無償で利用できる為に管理が漏れがちとなるオープンソースソフトウェア（OSS）についても忘れずに管理いただきたい。

CSIRT を構築する上で重要な要素が、経営層の認知とサポートである。多くの組織において、インシデント対応体制の必要性は認識されつつも予算の確保が困難であるとの現状がある。特に、事故を経験していない組織の場合には顕著である。CSIRT が有効に機能する為には、CSIRT 要員のモチベーションを維持・向上させること、CSIRT 活動によるインセンティブが得られることが必要である。インシデントが発生していない状態では CSIRT 活動をアピールすることが中々難しく、CSIRT 活動が単なる「コスト」として見られてしまうおそれが有る。経営層に対するコミュニケーションを密にし、問題意識を共有することと、CSIRT の日々の活動を見える化し、経営層・組織内での認知度を向上させることも検討いただきたい。

6.3 関連ビジネスへの提言

多くの組織ではセキュリティインシデントへの対応経験はあまり無く、CSIRT を構築しようとしても何を決めれば良いか判断が付かない。この様な場合には CSIRT の構築を支

援するコンサルティングへのニーズがあると想定されるが、一方コスト面での制約も有り、支援の一環として経営層への理解を深める働きかけも要望されている。

また、インシデントに対応できるセキュリティ技術者が人的リソース、技術的知識の両面で不足している場合が往々にして見られ、インシデント対応体制を補完する専門サービスが望まれている。例えば、監視やログ分析は、製品を導入しても組織内に対応できる要員が不足していては有効活用できないので、むしろサービスとして提供して、セキュリティインシデントを早期に検出できる体制を実現できる方がユーザとしては受け入れやすい。同様に、インシデント発生時のフォレンジック分析についてもツールの提供より分析サービス提供の方が望まれるだろう。ユーザ側で技術的知識などの理由から対応が困難な作業については、サービスとして提供されると受け入れられる余地があると思われる。

また、前節で記したとおり、構成管理の不備により脆弱性対策が遅れてしまう場合が見られる。組織内の IT システムの構成管理・変更管理を支援するツールやサービスも、IT システムを安全な状態に保つ為に有効であろう。加えて、組織が保有するソフトウェアの脆弱性や修正パッチの情報を自動的に収集できれば、事前対応の精度向上、対策までの期間短縮に役立つ。その様なツールやサービスのニーズも有ると想定される。

一方、これまでクローズドな環境において利用されていた制御系などの製品分野においても、オープンネットワークに接続される場合が増えつつある。このような製品においては、セキュリティに対してあまり意識がされていない場合も見られ、リスクが高いと想定される。システムベンダ、セキュリティベンダともに、その様な製品分野においてもセキュリティを向上できるよう検討いただきたい。

おわりに

本報告書では、新たな脅威に対するインシデントハンドリング体制の機能と形態を調査し、組織の特性に応じた効果的な組織の対応体制について提言を行った。

業界や組織の特性ごとに求められるインシデントハンドリング体制は異なるものの、ヒアリングやアンケートの調査結果から、インシデントハンドリング体制の構築・運用にあたっては、経営層のコミットメントが鍵となることが明らかとなった。経営層に CSIRT を認知させ、活動状況を見える化し、情報を共有することで、予算の確保、モチベーションの維持などにつながっていると考えられる。また、CSIRT 構築・運用にあたっては、技術的知識や人材不足が課題として上げられている。ベンダには、運用まで一体となったサービスの提供が求められている。

今後ますます高度化していくことが想定される情報セキュリティの脅威への対策として、CSRIT が有効に機能するため、また、合わせて情報セキュリティ産業発展のために本書が活用されることを期待する。

平成26年度情報セキュリティ調査報告書
－新たな脅威に対する組織の対応体制に関する調査－

発　行　日　　平成27年３月
編集・発行　　一般社団法人　電子情報技術産業協会
　　インダストリ・システム部
　　情報システムグループ
　　〒100-0004　東京都千代田区大手町1-1-3
　　大手センタービル
　　TEL　(03)5218-1057
印　　刷　　三 協 印 刷 株 式 会 社