IS-09-技標-02

セキュリティ市場・技術調査報告書

平成 21 年 5 月

社団法人 電子情報技術産業協会

はじめに

本調査報告書は、セキュリティ市場・技術調査専門委員会が、「組織内 CSIRT－組織におけるインシデントレスポンスの実態と課題」に関する調査を行い、その在り方や普及のシナリオ、関連ビジネスについて検討、分析した結果を報告するものである。

近年、IT に対する攻撃は経済的利益を目的とした犯行へ、特定の組織・企業を狙う手法に変わりつつあるし、企業からの個人情報の漏えいは、企業の信用並びにそのブランドを一瞬にして失墜させる脅威を我々に与えている。現在、このようなインシデント（事故）への対応は、企業の事業継続に関わる主要課題の一つであると考えられている。

企業の事業継続の一環として、攻撃や情報漏えい等の事故に対応する部門、または部門を横断した対応チームを設け、組織内にインシデント対応機能（CSIRT : Computer Security Incident Response Team）を持つ必要性が高まっている。組織内 CSIRT を設けることにより、従来組織内に点在していたインシデントに関する様々な情報を集約することで、インシデントが発生した際に迅速かつ的確な「組織としての意思決定と対応」を行うことが可能となり、被害の最小化及び同様の問題に対する事前策の検討などの効果を期待できる。

本年度の活動として当委員会は、組織内 CSIRT の必要性やその普及のためのシナリオ、またそこに JEITA 会員企業にとって、どのようなビジネス展開が期待できるかを明らかにすることを目的として調査を行った。調査内容としては、(1) CSIRT に関する国内外の動向調査、(2) CSIRT を有する企業等の事例調査、(3) 企業における CSIRT 構築・関連サービスのニーズ調査を、各企業の CSIRT 担当者や専門家の講演受講、サービス提供企業へのヒアリング、ユーザ企業に対するアンケート調査などを通じて行い、その調査結果を、報告書としてとりまとめた。

本調査報告書の作成にあたり、視察やアンケートにご協力いただいた企業やご講演いただいた学識経験者の方々、そして当専門委員会の関係の皆様に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、今後のセキュリティビジネスの更なる発展に寄与できれば幸いである。

2009 年 3 月

セキュリティ市場・技術調査専門委員会

委員長　伊藤　丘

目　次

1.CSIRT の概要

1.1.最近の脅威の動向

IT に対する脅威は、日々変化している。

近年の IT に対する攻撃について動向を調査してみると、攻撃の動機という観点からは、単なる愉快犯的な行為から、付加価値の高い情報の持ち出しなど、経済的利益を目的とした犯行へ変化しつつあるということがわかる。また、攻撃の規模や手法については、以下のような変化が読み取れ、攻撃の検知が困難になってきている。

① 不特定多数を狙った攻撃から標的型攻撃へ

愉快犯に多い、ネットワークを最大限に利用した不特定多数を狙う大規模な攻撃から、ビジネス文書を悪用するなど特定の組織や個人を狙った攻撃に変化している。このような標的型攻撃としては、以下のような例が報告されている。

- 送信メールや添付ファイルに当該組織の業務に関連することが書かれている。
- 発信者としてCEOなどの名前を騙り、添付ファイル付のメールを送る。
- 内部から送信された電子メールを模倣し、組織内の個人をターゲットとしてメールが送信される。
- メールに添付されて送信されるのは、バックドア、スパイウェアをダウンロードするためのプログラム等である。

また、セキュリティ対策が十分に行われていないクライアント PC を多数乗っ取り、攻撃者の指示により、それらの機器が一斉に同じ対象（標的）に対し通信を行ったり、スパムメールを送信したりするボット攻撃なども、この種の攻撃の主流となっている。

② 攻撃手法の巧妙化、高度化

既存の攻撃手法についても、巧妙化、かつ、高度化している。例えばウィルスについても、以下のように様々な機能拡張が施されている。

- 被攻撃者の脆弱性の有無を判断して、適切な攻撃コードを選択し攻撃する。
- 常駐のウィルス対策ソフトを停止させてから攻撃する。

③ 複数の攻撃手法の組み合わせ

さらに、複数の攻撃手法を組み合わせる、以下のような例も見られる。

- サーバのクラッキングにより、被攻撃者は改ざんされたWeb ページへ誘導され、悪意のあるソフトウェアを強制的にダウンロードさせられる。サーバのクラッキング手法

としては、ARPスプーフィング（ARPの応答を偽装し、本来の通信先とは異なるホストに通信を誘導することにより、情報を不正に取得する）、ウィルスの感染等が報告されている。

・ キーロガーソフトによるID／パスワードの不正取得により、特定個人の情報を取得され、なりすましメールにより悪意のあるソフトウェアが送付される。悪意のあるソフトウェアである添付ファイルを開封させるために、巧妙なソーシャルエンジニアリングが行われる。

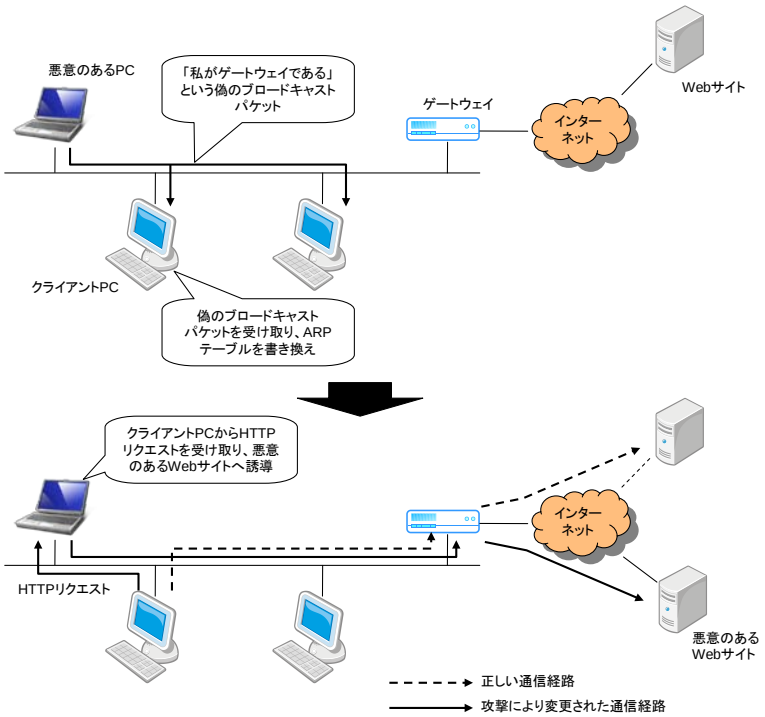

図 1.1-1 ARP スプーフィング

一方で、セキュリティ向上のためのパッチ適用やバージョンアップがシステム利用に影響を及ぼす例も報告されており、事業継続という意味ではこれ自体も脅威となっているという問題もある。従って、システムの可用性をできる限り犠牲にせず、セキュリティを向上する必要性が増している。

昨今の企業活動は IT に依存するところが大きく、上に示したように攻撃手法が巧妙になっていることから、従来の体制ではより確実に守り切ることが困難となってきている。また、攻撃により事故が起こった場合、企業の経営にも影響を与えかねず、事故に対する対応の遅れが被害金額の拡大やブランドイメージの失墜などにも繋がる。そのため、企業としては、このような事故の情報や対応策を内外から速やかに収集し、共有する体制を構築する必要性が増してきている。

1.2.背景と目的、CSIRT の定義、効果

1.2.1.CSIRT設立の背景と目的

(1)CSIRT設立の背景

インシデント（incident）とは、一般に「重大な事故に至る可能性がある出来事」を意味している。またコンピュータセキュリティ（情報セキュリティ）における「インシデント」とは、コンピュータウィルスやサービス運用妨害攻撃、情報漏えいなど、IT システムの正常な運用または利用を阻害して実害を加える事象や、そのような事象に繋がる可能性のある脆弱性の探索などの実害を加えていない事象なども含まれる。

最近では多くの業務が情報システムに依存すると共に、システムが複雑化してきており、インシデントの発見、原因の特定、復旧などに時間が掛かるようになってきた。また、特定の 1 カ所で発生したインシデントでも、その被害や影響は爆発的にシステム全体に拡大する恐れがある。さらに、インシデントを引き起こす攻撃手法も巧妙化・高度化してきており、対応には高い専門性が必要で、単独の部署毎の対応が難しくなってきている[1]。

このようなインシデントに対応し、インシデントの影響の拡大を防ぎ、情報を収集分析して原因や対策を検討して復旧や再発防止を実施する組織が CSIRT である。

従来のセキュリティ対策は、ウィルス対策ソフトの導入や、ファイアウォールや侵入検知システムの設置などのように、インシデントの発生をいかに防ぐかに注力されていた。しかし、①パッチ適用忘れなどの人為的ミス、②未知の脆弱性の悪用、③技術的な対応の限界、④社員等の意識や運用に頼る箇所が存在、などによりインシデントを完全に予防することはできないのも事実である。

インシデント対応には、インシデントの検知及び報告受付、トリアージ、分析、対策策定、調整、対策実施、監督官庁への報告やプレスリリースなどの多くの機能が必要となる。そして、それぞれの機能は有機的に結びつけられなければ迅速にインシデントに対応することはできない。特に、「組織内の情報共有及び連携機能」、「外部組織との信頼構築及び調整機能」は必須である。さらに組織全体として統一性及び一貫性がある体制が必要となる。これらが「CSIRT」の構築が求められてきている背景である[2]。

(2)CSIRTの目的

CSIRT はインシデントに対応することであり、一般的に以下のような目的を持っている。

① 迅速にインシデントによる被害を抑制し、損害を最小限にすること
② 適切なレスポンスと有効な対策を提供すること

---

[1]付録「組織内 CSIRT に関する調査研究報告書」参照
[2]付録「組織内 CSIRT に関する調査研究報告書」図表 1-4 参照

③ 将来発生するインシデントに対する予防をすること

これらの目的は一般的なものである。実際に CSIRT を構築する場合には、それぞれの組織での目的を明確にしておく必要がある。また、どの目的を最優先にするのか優先順位付けをしておくとともに、手順書等を整備することで迅速な対応ができるようになる。

CSIRT の目的は、CSIRT のおかれている組織環境によっても異なる。目的が変わることにより、CSIRT の具体的な実装方法なども変わってくる。

有限責任中間法人JPCERT コーディネーションセンター（JPCERT/CC）の「コンピュータ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」では、CSIRT のタイプ（おかれている組織）とミッション、そして考えられるサービスの目的（CSIRT の目的）の一例が記載されている [3]。これを表 1.2.1-1 に示す。

表 1.2.1-1 のなかで、「組織内 CSIRT」は CSIRT のタイプ＝企業のチーム、に相当する。

表 1.2.1-1 CSIRT タイプ別に考えられる CSRIT の目的

CSIRT のタイプ	ミッションの特徴	考えられるサービスの目的
国際的なコーディネーションセンター	他国の CSIRT と連携することにより、コンピュータセキュリティの脅威に関するグローバルな観点でのナレッジベースを獲得する。	・世界中の他の CSIRT と連携して、コンピュータセキュリティインシデントに対する技術的支援を提供する。 ・インシデントハンドリング活動を通じて、現在または潜在的な侵入脅威に関する技術的詳細を追求して文書化する。 ・侵入脅威の検知、防止、復旧に関する情報を作成して開示する。
国のチーム	コンピュータセキュリティの脅威に関する国の対外連絡窓口を維持し、国内のシステムから行われたセキュリティインシデント及び、国内のシステムを標的としたセキュリティインシデントの数を低減する	・コンピュータセキュリティインシデントに対する技術支援をその国の言語とタイムゾーンで提供する。 ・脆弱性を検知、防止、及び復旧するための技術情報を提供する。 ・国内の法執行機関に対する連絡窓口としての役割を果たす。
ネットワークサービスプロバイダチーム	顧客のネットワーク接続のためのセキュアな環境を提供する。 コンピュータセキュリティインシデントに関して効果的な対応を顧客に提供する。	・コンピュータセキュリティインシデントに対する技術的支援を提供する。 ・ネットワークインフラのセキュリティを確保する。 ・国のチームなどへの連絡窓口としての役割を果たす。
IT ベンダ	製品のセキュリティを向上させる。	・脆弱性に対する技術支援を提供する。 ・CSIRT と協力して、インシデントの原因を分析する。 ・新しいパッチや現在のベストプラクティスに関する注意喚起を作成し、一般に公表する。

[3] JPCERT/CC「コンピュータ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」（http://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf）

企業のチーム	社内の情報インフラのセキュリティを向上させ、攻撃や侵入による損害の脅威を最小限に抑える。	・インシデントハンドリング支援のための総合的拠点を社内のシステム管理者、ネットワーク管理者、及びシステムユーザに提供する。 ・社内のシステムに影響を及ぼすインシデントに対してオンサイトの技術支援を提供し、侵入脅威や攻撃を隔離して復旧する。

出典：JPCERT/CC「コンピュータ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」より

1.2.2.組織内CSIRTの定義

CSIRT の活動は「その組織の範囲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に関する活動とその準備をすること」と定義される。また、活動（サービス）対象が、CSIRT が属する組織の人、システム、ネットワークなど、組織に関わるインシデントに対応する CSIRT は「組織内 CSIRT（あるいは企業内 CSIRT）」と呼ばれる。

この組織内 CSIRT は必ずしも「インシデント対応を専門に行う部署」である必要は無い。必要なのは「インシデント対応を専門に行う機能」である。組織によっては他の関連業務と兼務することによって、組織内に CSIRT の機能のみを構築している場合もある。CISIRT の事前に構築し機能させることで、インシデントの発生の予兆を検知もできるようになり、インシデントの発生を予防することも可能である。

活動内容は組織によって異なるが、一般的に CSIRT の構築するために必要な機能は以下の通りである。

①対応する対象範囲のインフラ等に関する技術情報の収集
- インシデント動向及び対応手法の収集
- セキュリティホール情報の収集
- ソフトウェア及びシステムの脆弱性関連情報の収集
- 収集した情報の必要な部門への流通

②組織内の情報共有と連絡調整（組織内連携）
- 組織内のインシデント報告を集めるために一本化された窓口の提供
- 組織内のインシデントの一元管理と部署間調整
- 発生したインシデントに対応する、あるいはその対応に必要な技術的支援及びノウハウの提供
- インシデント対応に必要な、組織としての意思決定の支援
- 組織内の業務システムのユーザに対するセキュリティ意識の啓発
- CSIRT 構築と円滑な運用のためのアドバイス機能（コンサルティング）

③外部の CSIRT との連携による情報共有と連絡調整（外部連携）
- 外部に起因するインシデントを解決するための、他組織に対する依頼

・ 外部からのインシデント関連情報を受け取る一本化された窓口の提供
・ 外部組織との信頼の構築

CSIRT では、これらの機能をそれぞれの組織のミッションや目的にあわせて具体的に実装していく。CSIRT 機能は手順書等の文書にしておくことが、誤り無く機能を実行するために必要である。また、機能を滞りなく迅速に実行するために自動化できる箇所は極力自動化することが望ましい。

CSIRT を構築するにあたって、活動範囲や提供するサービス等を明確に定義し社内に向けて公表する必要がある。これらの定義より、CSIRT の実装方法も変わってくる。また CSIRT の定義を公表することで、組織内の協力を得ることもでき、活動を円滑に実施することが可能になる。

CSIRT の活動内容を定義する場合には、組織が過去に遭遇したインシデントや、今後発生が予想されるインシデントなどについて可能な限り詳細に分析を行い、内容や優先度を定義していくことが重要である。また、技術の進歩により組織を取り囲む環境などが変化していくので、適宜活動内容を見直し、再定義していく必要がある。

1.2.3.組織内CSIRTの効果

CSIRT を構築することで得られる効果は以下の通りである。

① 情報セキュリティインシデントに関する情報管理の一元化が実現でき、社内のセキュリティ情報の共有化と、セキュリティ対応の指示系統の迅速化が促進できる。
② 外部組織とのインシデント情報を取り扱う窓口が一本化されることで、インシデント関連情報の一元管理ができるようになる。
③ 組織を代表とする窓口が提供されることで、他の外部組織とのリスクコミュニケーションが行い易くなる。これにより、インシデント関連情報の質や量の向上が期待でき、予想外のインシデントにも早期対応ができるようになる。また、機密情報の流通も組織の窓口でコントロールできるので外部に対して「信頼関係」を築くことが可能になる。

このように CSIRT を構築することで、組織（あるいは企業）の活動や事業を安全に提供することができる。さらに、外部に対して信頼ある CSIRT を構築することで、今どのようなインシデントが世の中で起こっていて、その原因や対策といったインシデント対応に必要な情報を常に入手することができるようになる。これら必要な情報を、常に把握しておけば、万が一自社において同じようなインシデントが発生しても速やかに対応することができ、復旧までの様々なコスト（時間、人件費など）を軽減することができる。

さらに、インシデント対応において、それぞれの組織の対策において判断が必要になる

状況で、トラブルシューティングの対応に慣れた CSIRT の専門家によるアドバイスがあれば迅速且つ効果的な動きが取れ、組織の社会に対する信頼も向上させることができる。

1.3.国内外の動向

企業の活動における IT への依存度が高まる中、様々なセキュリティインシデントが発生しており、その対応は企業の事業継続に関わる主要課題の一つであると考えられている。しかし、そのためには幅広い情報収集と高度な分析機能が必要であり、専門チームが必要とされる。

このような組織としては米国でセキュリティインシデントに対応するために専門家の協力とセキュリティインシデントの備えを目的として CERT/CC （Computer Emergency Response Team / Coordination Center）が 1988 年に設立され、現在はインシデントマネジメントに関するベストプラクティス、ツール作成や CSIRT 構築のためのドキュメント公開などの活動をしている。

日本ではJPCERT/CC（Japan Computer Emergency Response Team / Coordination Center）が 1996 年に設立され、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、情報の収集と分析、対応の支援、再発防止対策の検討と助言などを行っている。また、日本の組織に「組織内 CSIRT」 の構築を支援する目的で資料（CSIRTマテリアル [4]や「コンピュータ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」など）を作成、公開している。

また CSIRT の国際的な連合として FIRST（Forum of Incident Response and Security Teams）が 1990 年に組織されている。FIRST は新たに組織された CSIRT に対して、メンバとの交流やアイディアなどを提供することによって、組織の構築をサポートする。また、CSIRT 構築のためのドキュメント、ベストプラクティスの公開（CSIRT Case Classification, CSIRT Setting up Guide）や CSIRT のインシデントマネジメント機能のベンチマーク手法について検討している。

FIRSTには現在 [5]43 カ国 201 の組織が加盟している [6]。日本からは JPCERT/CCが 1998 年に加盟し、現在では警察庁や国の機関、民間企業のCSIRTの 14 組織が参加おり、米国、英国、ドイツに次ぐ組織数となっている。

ヨーロッパにおける CSIRT も多く、各国レベルで独自のフォーラムを組織し、国内の CSIRT の連携を強めている。

日本におけるCSIRTの状況として、2005 年に経済産業省が「情報セキュリティ早期警戒

---

[4] CSIRT マテリアル：http://www.jpcert.or.jp/csirt_material/

[5] 2009 年 2 月 17 日現在

[6] FIRST のウェブサイト：http://first.org/

パートナーシップ」の運用を開始し、2006 年から組織内CSIRTの構築が進んでいる。[7]現在も複数の企業が組織内CSIRT構築に向けた準備を進めている。

日本国内で活動する、有志の民間及び企業内 CSIRT により、2007 年には日本シーサート（CSIRT）協議会が設立され、現在 13 の組織が加盟している。同じような状況や課題を持つ CSIRT 同士による緊密な連携と、インシデント関連情報や脆弱性情報、あるいは関連する攻撃予兆情報などを互いに収集し共有するための場を提供する。

FIRST や日本シーサート協議会に加入していなくても、IT に関わる事業継続という点で様々なセキュリティインシデントに対応するための組織を持っている企業が多数存在することが今回の調査で確認された。 企業経営の IT への依存の高まりとともに今後も組織内 CSIRT の必要性が増してくると考える。

1.4.組織内 CSIRT の事例

1.4.1.事例 1（富士ゼロックス株式会社）

(1)CSIRT構築の経緯

富士ゼロックスでは、情報セキュリティガバナンス強化のための専門組織を、2005 年 7 月に立ち上げた。この専門組織は、当初、個人情報保護法への確実な対応を主目的として立ち上げたが、個人情報のみならず、お客様からお預かりする情報や自社の企業秘密のセキュリティ対応も役割として活動している。この専門組織の中で、重点を置いている活動のひとつが、インシデント管理（CSIRT 機能）である。CSIRT は、軽微なものも含めたインシデントを把握することで、大きな事故予防や、有効性の高い情報セキュリティ管理策の企画に繋がるという考え方に基づき、管理の仕組みを運用している。

(2)組織体系

総務部の中に、全社共通の情報セキュリティ活動に従事する選任組織として編成されている（図 1.4.1-1 参照）。

[7] 付録「組織内 CSIRT に関する調査研究報告書」付録 I の講演録参照

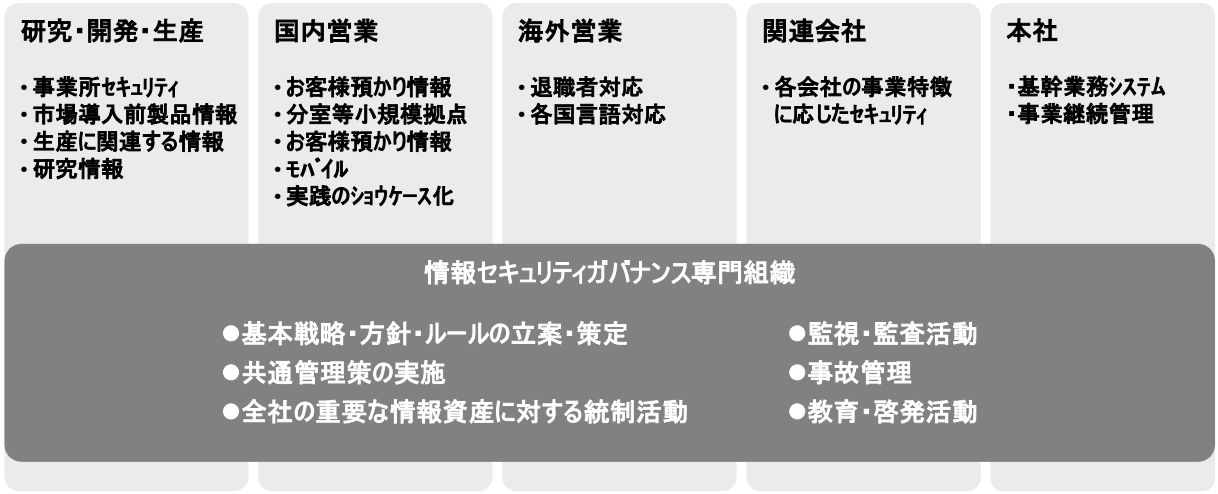

図　1.4.1-1　富士ゼロックスの情報セキュリティガバナンス専門組織（CSIRT）

全社課題と組織毎の個別リスクへの対応とを整合させるため、この組織は部門毎のセキュリティ機能と連携し、全社のセキュリティガバナンスには 2 層構造の体制を適用している。

(3)CSIRTの役割

CSIRT の役割は以下の通りである。

1. 基本戦略・方針・ルールの立案・策定
2. 全社共通の管理策の企画と導入
3. 全社の重要な情報資産に関する統制活動
4. 監視・監査活動
5. 事故（インシデント）管理
6. 教育・啓発活動

事故（インシデント）管理のため、社員が日々アクセスしている社内ポータルにインシデント報告のための手順が掲載されており、事故報告に関して 3 点の基本方針を定めている。

① 事故発生後、2 時間以内の緊急連絡
② 事故報告書の提出
③ 再発防止策実施状況の監査結果提出

情報セキュリティインシデントが報告されると、その処理に際して判断の迅速性と行動の機動性が要求され、内容によっては高度なリスクマネジメントが要求されるため、その活動は情報セキュリティ担当役員の管掌のもとに遂行されている。また、情報通信系のインシデントに関しては、その分析と対処に関して情報通信システム部と連携して活動している。

教育・啓発活動としては、事故報告管理及び事故からの学習に繋がる教材を提供し、全従業員を対象とした情報セキュリティ教育を実施している。例えば、具体的な事故事例を教材に盛り込むことや、事故の再現ビデオを視聴することで、事故の脅威を実感してもらい、事故予防につなげようとしている。

(4)CSIRT構築による効果

情報セキュリティのガバナンスを専任体制化することにより、これまで行き場の無かった問い合わせや相談が現場から多数発生し、潜在していたリスクを顕在化する上で有効に機能している。

また、事故報告の情報を定期的に分析し、情報セキュリティ強化施策の立案に役立てることができるようになった。例えば、事故報告を統合的に分析することで、ある情報システムの利用において､異なる事業部門で類似の事故が起きていることがわかる場合がある。この場合、事故当事者部門での再発防止に加えて、事故原因の分析結果から、情報システムの仕組みの問題というより、根本的な原因に対して手を打つことが可能となった。

(5)今後の課題

重大な事故の発生を防ぐためには、日々の軽微な事故及びその背後にある不安全行動・不安全状態を管理し、異常要素を排除する必要がある。そのために、情報セキュリティ強化施策などの仕組みによる対応を進めると同時に、教育等を通じた社員の意識変革を推進して企業文化として定着させて行くことを今後の長期課題として位置づけている。

1.4.2.事例 2（沖電気工業株式会社）

(1)OKI-CSIRT構築の経緯

世の中でセキュリティ事故が数多く報告されているにもかかわらず、企業グループ内で同種の事故の発生を防止できなかったことに対して、社内規則の整備やセキュリティ技術者がいるだけでは社内のセキュリティガバナンスができないと判断し､2008 年 8 月より情報セキュリティ委員会に OKI-CSIRT が組織された。

OKI-CSIRT により技術面から世の中のセキュリティ事故の状況を把握し、予防策を企業グループ内に展開することで、セキュリティ事故の発生や発生時の被害を最小限に抑えることが期待されている。

(2)組織体系

OKI-CSIRT は独立した組織ではなく、情報セキュリティ委員会の下で技術的サポートを行うために仮想的に作られた組織である。

組織のメンバは、情報システム部門及びコンピュータセキュリティ担当部署の一部メンバが兼任で活動している。

(3)OKI-CSIRTの役割

OKI-CSIRT は、企業グループ内の情報基盤サービス利用者、管理者に対してコンピュータセキュリティに関する相談窓口として位置づけられ、以下についてセキュリティインシデント対応、及び予防活動を行う。

- 不正プログラムによる情報漏えい
- コンピュータウィルス感染
- 企業グループ内情報基盤サービスに対する不正アクセス、不正利用
- 電子情報に係わる企業グループ内規則への違反行為

コンピュータウィルス感染については USB 経由の感染が世の中に増加する中で、製品へのウィルス混入対策の必要性についても経営層が強く認識したことにより、OKI-CSIRT による事業部門の品質管理部門への技術支援体制が整えられた。OKI-CSIRT のサービス概要を以下に示す。

①セキュリティインシデント対応

セキュリティインシデントの報告を受け、関連部門から情報を収集しインシデントの危険度、影響範囲を分析する。分析の結果、必要に応じて社内関連部門への協力を依頼し、インシデントへの対抗手段を決定して対応を関連部門へ指示する。影響を受けたシステムやサービスに対しては、担当部門による復旧を支援する。

②予防活動

外部から最新の脆弱性情報やインシデント情報を収集し、重要な情報や予防措置が必要なインシデント情報を関連部署に提供する。

また、情報基盤サービス提供者に対して脆弱性検査の実施、及び解析に必要なログや記録などの整備状況を調査し、システム管理者に改善を提言する。

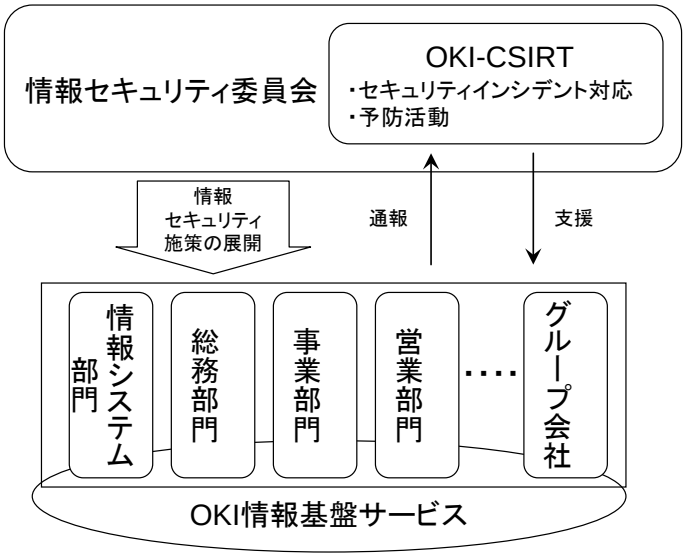

図 1.4.2-1　OKI-CSIRT の役割

(4)OKI-CSIRT構築による効果

これまで部門により個別に収集あるいは認識されていなかったセキュリティ事故情報や脆弱性情報は、OKI-CSIRT にて内外の情報が一元的に収集、ハンドリングされることにより、必要とされる関連部門に提供するルートが確立された。

また、OKI-CSIRT メンバが他社の CSIRT のメンバと交流する機会ができ、技術力の向上に繋がっている。

(5)今後の課題

OKI-CSIRT により、初年度の活動にて、インシデント対応や製品へのコンピュータウィルス感染防止への企業グループ内体制が整えられた。

今後はインシデントの予防活動をより一層充実させていきたい。具体的には、リスクの高い情報に対してこれまでもログの分析は実施しているが、インシデントと結びつく兆候を捉えられるようなノウハウの蓄積を考えている。OKI-CSIRT の予算確保の上でも、経営層に対して OKI-CSIRT がセキュリティ事故発生時のインシデント対応よりも、インシデントの予防をアピールする方が有効と考える。

さらに、OKI-CSIRT にて取得したノウハウを基に、OKI グループのお客様で発生するセキュリティインシデントに対しても技術支援を行える体制を目指していく。

2.企業におけるインシデントレスポンスの現状

2.1.アンケート調査結果（委員会、Web 調査）

本委員会では、本委員会委員企業及び従業員 50 名以上のユーザ企業に対し、企業における事業リスクの観点から見た情報セキュリティ対策の実態把握を目的としたアンケート調査を実施した。予備調査として、企業向けアンケート調査に先駆け、仮説の検証と効果的な質問設計を目的とし、本委員会委員を対象に CSIRT 構築状況に関するアンケート調査を実施した。本調査では、以下の２つのケースを想定した質問によりインシデント対応における体制の整備状況について特徴的な傾向を分析することとした。

- ケース1（情報漏えい）：会社の代表連絡先に社外から「●●BBS（有名掲示板サイト）に貴社の顧客情報らしきものが流出している」という情報提供を受けた。
- ケース2（HPの改ざん）：お客様お問い合わせ窓口で、一般人から「貴社のHPを閲覧したところ、コンピュータウィルスに感染した」、「内容が改ざんされているようだ」という連絡を受けた。

アンケート調査は、企業におけるシステム企画運用管理担当者または自社のITシステム導入を決定または導入検討し推薦する立場の者を対象とし約500社から回答があった。

2.2.回答者の属性

回答企業の業種は多岐に亘り、中でも製造業が最も多く、次いで情報サービス業、小売業、情報以外のサービス業の順であった。また、従業員数は、約 85%が 5,000 人以下であり、中でも 101～300 人と回答した企業が最も多かった。

2.3.企業におけるインシデント対応体制に関する状況

CSIRT を保有しているのは、約 20%の企業で、従業員数が多い企業や、「金融・保険業」「電気通信業」「情報・IT 関連業」「電気・ガス・熱供給・水道業」「教育・学習支援業」等の業種である。これらの企業は、機能としても CSIRT が必要と考えている傾向にある。CSIRT は無くとも、インシデントに対応する組織が定められている企業は、ケース 1 とケース 2 とも 50%前後に達する。

ケース 1 とケース 2 で対応組織があると回答した人はほぼ重複した。逆にどちらのケースにも対応組織が無いと答えている企業は 40%近くあり、これらではインシデントへの対応組織が全く整備されていないと考えられる

対応組織の有無による問題点の認識度の違いとしては、対応組織が定められていない企業の方が、インシデント対応全般において問題意識が強い。対応組織の有無で最も差が出るのは「対応組織の明確化」、「報告先の明確化」「情報共有」、「専門的知識を持った人材」

であり、対応組織が定められていない企業の潜在的なニーズになっていると考えられる。

対応組織がどこになるかに関しては、情報漏えいの場合は「リスク・危機管理に係る専門組織」の割合が高く、一方 HP の改ざんの場合情報セキュリティ組織や情報システム部門の割合が高い。企業によってインシデントやリスクの認識に差があると考えられる。

対応組織の持つ機能としては、インシデントの監視・検知、報告、情報共有などの機能は大半の組織で整備されているが、外部組織との連携や、報告、広報活動についてはカバーしていない組織が多い。

CSIRT を持っている企業ほど CSIRT の必要性について強く認識している。一方で、組織としての CSIRT は整備されてなくても、CSIRT の機能に対する必要性は比較的高く認識されている。

過去に事故を経験している企業では、事故を経験していない企業と比べて CSIRT の構築率が非常に高く、事故をきっかけに CSIRT を整備する企業が多いと考えられる。

CSIRT 構築している企業では各インシデントに対する対応組織構築のメリットとして、「インシデントに対する迅速対応」、「社内のセキュリティ意識の高まり」などが多く挙げられており、対応組織の活動が一定の効果を得ていると言える。一方で、対応組織があるにも関わらず、CSIRT を構築していない企業では、CSIRT を構築している企業に比べて全体的に感じているメリットが少なく、特に「ノウハウの構築」や「セキュリティ統制」の部分で十分なメリット受けていない状況が見受けられる。

CSIRT を持つ企業における CSIRT 構築の成功要因として「組織横断的な組織」、「経営層への説明」、「組織の周知」、「社内における専門家の育成」等が挙げられている。

インシデント対応における問題点としては、CSIRT が無い企業における専門的知識を持った人材不足が挙げられている。また CSIRT が有る企業、無い企業共に、人手不足は問題として捉えられている。

全体として CSIRT が構築されていない中でも CSIRT 構築のニーズを感じている企業では、CSIRT 構築のニーズを感じていない企業に比べて問題意識が高い。ただし、専門的人材の不足、インシデント対応における費用対効果に対しては CSIRT 構築のニーズを感じていない企業においても一定の問題意識が持たれており、これらの問題が一般の企業で CSIRT 構築が進まないボトルネックになっていると考えられる。

CSIRT を持つ企業ではインシデントハンドリングや CSIRT 関連サービスに対する導入検討率が高く、市場として有望であると考えられる。一方で CSIRT が無い企業では全般的に製品・サービスの導入率が低く、特にインシデントレスポンス、アウトソーシング関連製品のニーズは非常に低い。

昨年度に引き続き、シンクライアントの導入検討率が高く、今後も市場の拡大が予想される。フィルタリングツールやデータ暗号化ツールの導入状況は昨年度に比べて成熟期に移行している。一方で、ワンタイムパスワードや情報漏えい対応複写機などのように、大企業における導入検討率が下がっているツールも見受けられる。

2.4.企業におけるインシデント対応体制に関するアンケート調査のまとめ

① インシデント対応組織の位置づけは企業によって異なる

情報漏えいのケース 1 を例に取ると、社内でインシデント対応を行う組織が明確に定められている企業は 54%となっている。また、対応組織がある場合も、リスク・危機管理に係る組織や、情報システム部門、間接部門の内部組織という位置づけの場合が大半となっており、情報セキュリティやインシデント専門の組織を構築している企業は少ない。このように各企業によってインシデント対応組織の位置づけが分散する背景には、インシデントの経験やリスクに対する企業の考え方、既存組織が持っていた役割など様々な要因があると考えられる。

② インシデントへの対応組織が決められている企業でも､実際に効果的なインシデントハンドリングするだけの体制が整備されているとは限らない

全体として対応組織が定められていない企業では、対応組織が定められている企業に比べて、インシデント対応における問題点を強く認識している傾向が見られる。一方で、インシデント対応組織が定められている企業においても､「インシデントの種類によっては対応組織が明確になっていない」､「人手が足りない」､「専門的知識を持った人材がいない」などの問題点が 30%以上の割合で挙げられており、組織が整備されていても、必ずしも十分なインシデント対応を行うための体制が整備されているとは言えない。

③ 事故を経験するなどインシデント対応の必要性を実感している企業ほど、CSIRT 構築が積極的に進められている

本アンケートでは回答企業の約 20%でインシデント対応専門組織 CSIRT が構築されているという回答を得た。過去に事故を経験している企業では、事故を経験していない企業と比べて CSIRT の構築率が非常に高い結果となった。また企業におけるインシデント対応に係る製品・サービスの導入意向を比較しても、CSIRT が無い企業ではどの製品・サービスでも導入意向が低いのに対し、CSIRT が有る企業の導入意向は非常に高く、インシデント対応への関心の大きさを示している。事故などを経験することでインシデント対応の必要性を強く認識している企業から、再発防止策としての実践的な CSIRT の構築が進んでいるという状況が見られる。

④ CSIRT を構築することで、効果的なインシデント対応の実現に加え、従業員の情報セキュリティ意識向上などの間接的な効果も得られている。

CSIRT を構築している企業においてインシデント対応組織があることでのメリットとして「インシデントに対して、迅速にかつ効果的に対応することができる」と並んで、「専門組織を置くことで、社内の情報セキュリティに関する意識が高まる」が多く挙げられている。専門組織を設置することで、従業員に対してインシデント対応に取り組む企業の姿勢

が従業員の中で共有され、意識向上に繋がっていると考えられる。

⑤ CSIRT 構築のカギは経営層の理解と従業員への周知

CSIRT を構築している企業における CSIRT 構築の成功要因として、CSIRT 組織の本質である「関係部署を巻き込んだ組織横断的な組織として設置した」、「グループ会社や子会社を取り込んだグループ横断的組織として設置した」という項目に続き、「設置に際して、経営層の理解を得るために十分な説明を行った」という項目が挙げられており、また「インシデントの窓口として、社員に組織の周知を徹底した」という項目も高い割合となっている。つまり、CSIRT を有効に機能させるためには、経営層を含め全従業員が CSIRT の目的と役割を十分に認識することが重要であると言える。また、このような意識の共有が、CSIRT 構築の間接的な効果、セキュリティ意識の向上にも繋がっていくものと考えられる。

3. インシデントレスポンス関連ビジネスの動向

3.1.インシデントレスポンス関連市場の動向

3.1.1.インシデントレスポンス関連市場の概要

内部統制の強化を背景に、ログの分析、活用に対して課題を持つ企業が増加していると同時に、インシデント発生時の迅速な対応が求められている。しかし、インシデントレスポンス体制を自社に構築するためには、専門家の不足や費用負担などの問題がある。特に専門家の不足は重大であり、インシデントレスポンス関連部門を社内に構築できる企業であっても、専門家不足の課題解決を外部の力に頼る必要がある。そのため、インシデントレスポンス関連のサービスや製品の提供を生業とする事業者が求められ、インシデントレスポンス関連市場が形成されている。CSIRT 普及のためには、このようなインシデントレスポンス関連市場が重要であると考えられるため、本委員会ではこれらの市場動向を調査した。

富士キメラ総研「2007 ネットワークセキュリティビジネス調査」によるとインシデントレスポンス関連市場は、2006 年度実績で 1,344 億円であり、その後も 2007 年から 2009 年にかけて毎年 20%以上の成長が見込まれている。その後、成長率は鈍化するものの 2011 年には、3,671 億円の市場が形成されることが見込まれている。

本調査委員会では、表 3.1-2 に示すサービス・製品をインシデントレスポンス関連サービス・製品とし、その導入状況や導入意向を調査した。さらに、インシデントレスポンス関連ビジネスの現状を調査するために、代表的なインシデントレスポンス関連ビジネス提供者にヒアリングを実施した。

表 3.1.1-1 インシデントレスポンス関連サービス・製品

事前対応
1. ログ管理・分析
2. 脆弱性診断
3. 侵入検知
4. クライアント端末監視・管理
5. セキュリティ監査、審査
6. セキュリティ関連情報の提供
事後対応
7. インシデントハンドリング （インシデントの分析から、実際の対応支援までのハンドリング）
8. 脆弱性ハンドリング （外部から得た脆弱性情報を収集し、該当する社内システムに修正パッチを施すまでの一連の流れのハンドリング）
9. システム復旧
10. 個人情報漏えい対応
11. 損害保険
12. フォレンジックサービス
13. 遺失物回収
14. 広報支援 （事故発生時の対外公表へのサポートなど）

品質管理
15.（インシデント対応に係る）リスク分析
16.（インシデント対応に係る）セキュリティコンサルティング
17. IT-BCP コンサルティング （IT システムの継続性に関するコンサルティング）
18. 緊急対応訓練支援
19. 教育／トレーニング、意識向上のため啓発
20. CSIRT 構築支援
21. CSIRT アウトソーシング

3.1.2. ユーザ企業からみたインシデントレスポンス関連サービス・製品の動向

インシデントレスポンス関連サービス・製品の導入意向を調査した結果を、事前対応、事後対応軸、及び物理媒体対応、電子媒体対応軸でマッピングしたものを図 3.1.2-1 に示す。これによると、主に事前対応に関連するサービス・製品である「ログ管理・分析」、「クライアント端末監視・管理」の 2 つに大きな導入意向が見られる。また、その他のサービス・製品に関してもおおむね 10%から 20%程度の中規模の導入意向が見られる。このことより、インシデントレスポンス関連サービス・製品については、その種類などによらず、広範囲に亘る導入意向があることが確認できた。

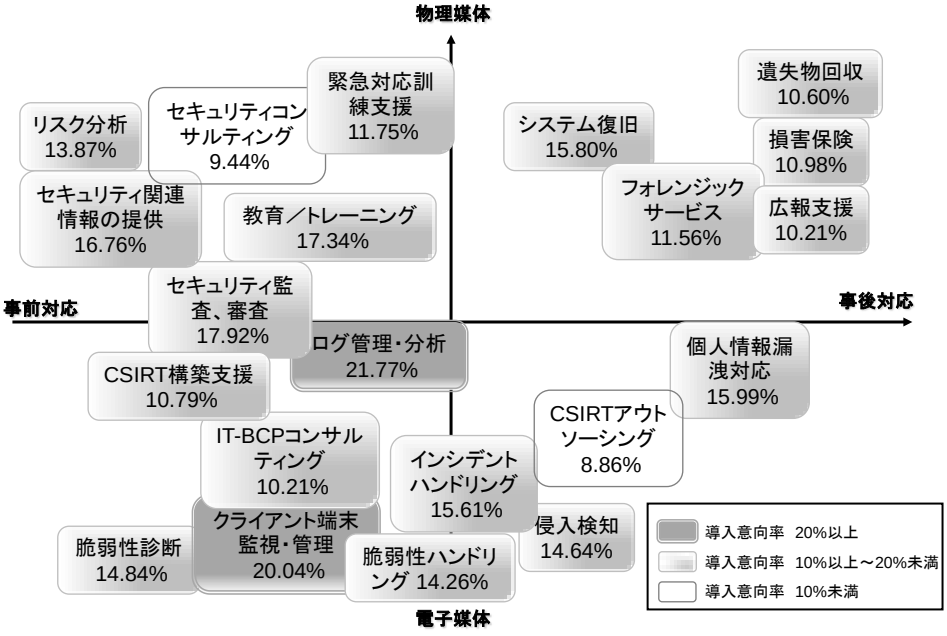

図 3.1.2-1 インシデントレスポンス関連サービス・製品の導入意向

さらに、同アンケートのサービスや製品の現在の導入率と導入意向率との関係を見るために、各サービスや製品を導入率でマッピングしなおしたものを図 3.1.2-2 に示す。本調査によると、侵入検知やクライアント監視やログ管理など事前対応に関連するサービス・製品はすでに導入されており、分析やハンドリングと言った品質管理、事後対応に関連する

サービス･製品は､導入意向があるものの実際に導入されている割合が低いことがわかる。さらに、すでに導入されている攻撃検知やログ管理に関しても、それらの分析を含む「クライアント端末監視・管理」や「ログ管理・分析」が他のものより一段と導入意向が高いことがわかる。これらのことは、事前対応として情報を収集する製品やサービスを導入したものの、収集した情報の分析やハンドリングに対してはこれからサービスや製品を導入する意向であることを示唆している。このことは、今後のサービス・製品展開を考える上で考慮すべき点だと考えられる。

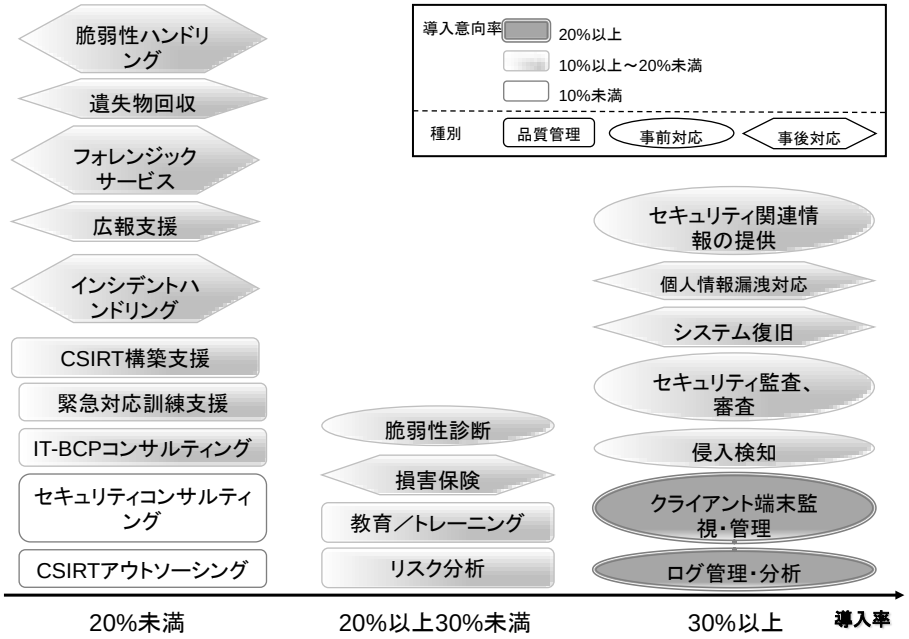

図 3.1.2-2 インシデントレスポンス関連サービス・製品の導入率と導入意向率

3.1.3.サービス提供者から見たインシデントレスポンス関連市場動向

インシデントレスポンス関連市場動向を調査するため、代表的なインシデントレスポンス関連サービスを提供している事業者に対してヒアリングを実施した。代表的なインシデントレスポンス関連サービスの事例では、事故発生時の対応サービスをメニュー化し、サービスする事業者が徐々に見られつつあるが、事故発生時の対応サービスを提供する案件数は増加しているものの、1 件あたりの単価は小さく、他のサービスを導入する足がかりとして利用されることが多い。一方で、事故発生時の対応サービスを明確にサービスメニュー化していない事業者であっても、脆弱性検査ツールや侵入検知ツールの導入や運用の延長として、インシデントレスポンスに関連するサービスを提供していることも多い。このような場合には、上記サービス・製品に加え、プライベート SOC（Security Operation

Center）構築支援や、教育、インシデントレスポンス体制の構築支援などのコンサルタントサービスなど、幅広いインシデントレスポンス関連のサービスが提供されている。

これらの企業を分析すると、インシデントレスポンスに関するノウハウや人材を持った企業が、事故発生時の対応サービスとしてそのノウハウを提供する場合と、フォレンジックツールや、ログ取得ツール、攻撃検知ツールなど、インシデントを発見するための基となる情報を事前に収集するツールに強みを持ち、それらのツールの販売と同時に事故発生時のサービスを実施する場合、さらには、セキュリティ基盤構築に関わるコンサルタントに強みを持つ企業が、事故発生時の対応基盤の構築支援をする場合などに分けられる。

今後の展開としては、各社ともユーザ企業の拡大と、ソリューション展開によるサービスの多様化を課題としている。

3.2.主な関連製品・サービスの内容

「3.1 インシデントレスポンス関連市場の動向」でも述べられている通り、専門家不足などの課題を解決するため、インシデントレスポンス関連の製品・サービスを提供する市場が形成されている。インシデントレスポンス関連で提供されている製品・サービスは、大きく「事前対応型」、「事後対応型」、「品質管理」の 3 つに分類することができる。ここでは、それぞれの代表的な製品・サービスの内容について紹介する。

3.2.1.事前対応型

事前にソフトウェアなどの脆弱性や不正アクセスの兆候を検知し、インシデント発生の抑制を図ることを目的としており、以下のようなサービスが提供されている。

(1)脆弱性診断サービス

脆弱性診断サービスは、診断対象により 2 つに分類できる。サーバやネットワーク機器を対象としたネットワーク診断サービスと Web アプリケーションを対象とした Web アプリケーション診断サービスである。

ネットワーク診断サービスは、診断ツールを用い、サーバやネットワーク機器の OS、アプリケーションなどのセキュリティホールのチェックを行い、問題点の洗い出し、改善策の提案などを行うサービスである。

Web アプリケーション診断サービスは、診断ツールや専門家の手作業での診断により、Web アプリケーションのセキュリティ上の問題点を洗い出し、適切な対策方法の提案・アドバイスなどを行うサービスである。

(2)不正アクセス監視サービス

IDS（Intrusion Detection System）を使用して、ネットワークを流れるパケットやファイ

アウォールのログなどを監視し、不正なアクセスが発生した場合、システム管理者に通知するサービスで、通常、専用の監視センターから 24 時間 365 日の監視が行われる。

(3)情報セキュリティ事件・事故対応シミュレーション

情報漏えい、ウィルス感染などの情報セキュリティ事故を擬似的に発生させ、従業員の対応プロセスを評価するサービスである。また、緊急時の対応訓練なども行い、訓練時に発生した不備に対するアドバイスも行う。

3.2.2.事後対応型

インシデント発生時の被害拡大防止や復旧対応を目的としており、以下のような製品・サービスが提供されている。

(1)インシデントハンドリング

事故発生後の初動対応から、原因分析・調査、復旧作業及び再発防止対策までを支援するサービスである。さらに監督官庁への報告・警察への届け出・マスコミ対応支援まで含めたサービスも提供されている。また、Winny などファイル交換ソフトによる情報流出時に、ファイルの特定、流出の規模・傾向を調査するサービスも提供されている。

(2)フォレンジック

製品として、ネットワークフォレンジック製品とコンピュータフォレンジック製品が提供されている。ネットワークフォレンジック製品は、ネットワーク上の通信を全て記録し、情報セキュリティ事故発生時などに復元・解析することができる製品である。コンピュータフォレンジック製品は、調査対象となるパソコンやサーバのハードディスクについて、解析用の複製を作成し、証拠保全・分析を行う製品である。これらの作業については、専門的な知識が必要となるため、サービスとして提供している事業者も多い。

3.2.3.品質管理

特にインシデントハンドリングや CSIRT 固有のものではなく、従来から提供されているサービスであり、組織のセキュリティレベルを向上させることを目的としている。インシデント対応などで得られた経験を、セキュリティ品質管理プロセスの一環としてサービスにフィードバックすることで、組織の長期的なセキュリティ活動を向上させることができる。

(1)事業継続計画策定支援サービス

大規模災害などの不測の事態が発生した場合でも、事業を継続、もしくは早期に通常の状態に復旧するための計画策定を支援するサービスである。「全社方針・推進体制の確立」「ビジネス影響分析」「事業継続計画策定」「テスト・訓練」「評価・改善」などのステップでサービスを提供する。また、新型インフルエンザ対策コンサルティングサービスを提供する事業者も現れてきている。

4.CSIRT 普及に向けた課題と提言

4.1.CSIRT 普及の課題

本報告書付録の「組織内 CSIRT に関する調査研究報告書」のアンケート調査では、インシデント対応専門組織 CSIRT が構築されているのは回答企業の 2 割となっている。また、情報漏えいのインシデントに対応する組織が明確に定められている企業は 54%あるが、大半がリスク・危機管理に係る組織や情報システム部門、間接部門の内部組織という位置づけでインシデント対応専門の組織を構築している企業は少ない。インシデント対応組織が定められている企業において、「インシデントの種類によっては対応組織が明確になっていない」「人手が足りない」「専門知識を持った人材がいない」などの問題点が 30%以上の割合で挙げられており、組織が整備されていても、十分なインシデント対応を行うための体制が整備されているとは言えない状況と報告されている。

CSIRT が有る組織と無い組織で、過去の情報セキュリティに係る事故の経験を比較すると CSIRT がある組織の事故経験率が圧倒的に高い結果となっている。事故の経験により、インシデント対応の重要性を認識し、再発防止策として実践的な CSIRT 構築がされている状況であるが、事故が発生しないと企業において CSIRT 構築が進まない、普及していかないという課題が見てとれる。

インシデント対応組織の位置づけも、対象とするインシデント、社内体制、構築プロセスなどにより、企業によって様々な状況となっており、他社の構築事例をもとに容易に自社導入が進められるものではない難しさがある。

4.2.CSIRT 普及に向けた提言

現時点では、インシデントレスポンスに課題を抱える企業は多いが、実際に重大事故の直面した経験が無い場合には、インシデント対応としては、既存の組織（情報システム部や総務部等）に委ねてしまうケースが多く、その場合には、効果的なインシデントハンドリングするだけの体制が整備されているとは限らない。また、専門チームとしての組織内 CSIRT を構築する場合でも、対象とするインシデントや取り組み方法に企業間のばらつきが多く、時としては、本来あるべき姿とは異なる運用が為されている場合もあることがわかった。

今回の調査報告書では、組織内 CSIRT のあるべき姿を具体的にまとめることはしていないが、事業継続に悪影響を及ぼすリスクを回避する意味からも、各企業にあっては、組織内 CSIRT を設置し、インシデントが発生した際に迅速かつ的確な「組織としての意思決定と対応」を行い、被害の最小化及び同様の問題に対する事前策の検討などを進めておくべきであろう。また、JEITA に参画されている IT・情報システム支援業務に関わる企業にあっては、組織内 CSIRT 構築のためのサポートビジネスや付随する情報機器やサービスの提供ビジネスを積極的に進めることを期待する。

おわりに

本年度の調査にて、組織におけるインシデントレスポンスの実態と課題について、組織内 CSIRT の動向、事例、ニーズを中心に調査し、組織内 CSIRT が企業にとって必要であり重要であると再確認することができた。また、同時に、組織内 CSIRT 構築を推進して行く上で、JEITA 会員企業にとってどのようなビジネス展開が期待できるかも示すことができたが、このようなビジネス形成により、会員企業のみならず多くの企業において、組織内 CSIRT の構築必要性についての認識が深まり、組織内 CSIRT 構築が更に促進されることを期待する。