2. コンピュータセキュリティのインシデント対応力の組織化

効果的なコンピュータ・セキュリティ・インシデント対応能力（CSIRC）を組織化するには、いくつかの主要な決定と行動が必要です。最初の検討事項の一つは、「インシデント」という用語の範囲が明確になるように、組織固有の定義を作成することです。組織は、インシデント対応チームが提供すべきサービスを決定し、それらのサービスを提供できるチーム構造とモデルを検討し、1つまたは複数のインシデント対応チームを選択して実施すべきです。インシデント対応の計画、方針、手順の作成は、インシデント対応が効果的、効率的、一貫性を持って行われ、チームが必要なことを行う権限を与えられるように、チームを設立するための重要な部分です。計画、方針、手順は、組織内の他のチームや、法執行機関、メディア、その他のインシデント対応組織などの外部関係者とのチームの相互作用を反映したものでなければなりません。このセクションでは、インシデント対応能力を確立しようとしている組織に役立つはずのガイドラインだけでなく、既存の能力の維持と強化に関するアドバイスも提供している。

2.1 イベントとインシデント

イベントとは、システムやネットワークで発生する観察可能な事象のことです。イベントには、ユーザーがファイル共有に接続した場合、サーバーがウェブページの要求を受信した場合、ユーザーが電子メールを送信した場合、ファイアウォールが接続の試みをブロックした場合などがあります。有害なイベントとは、システムのクラッシュ、パケットの洪水、システム特権の不正使用、機密データへの不正アクセス、データを破壊するマルウェアの実行など、負の結果をもたらすイベントのことです。このガイドでは、自然災害や停電などによって引き起こされたイベントではなく、コンピュータセキュリティに関連した有害なイベントのみを扱います。

コンピュータセキュリティインシデントとは、コンピュータセキュリティポリシー、許容される使用ポリシー、または標準的なセキュリティプラクティスに対する違反または違反の差し迫った脅威※1のことです。インシデント※2 の例

■ 攻撃者がボットネットに命令して、大量の接続要求をウェブサーバに送信し、クラッシュさせる。
■ ユーザが騙されて電子メールで送られてくる「四半期報告書」を開くと、実際にはマルウェアであり、ツールを実行することでコンピュータが感染し、外部ホストとの接続が確立されてしまう。
■ 攻撃者が機密データを入手し、組織が指定された金額を支払わなければ詳細が公開されると脅す。
■ ユーザーが、ピアツーピアのファイル共有サービスを通じて、機密情報を提供したり、他人に公開したりする。

※1「違反の差し迫った脅威」とは、組織が特定のインシデントが発生しようとしていると信じる事実上の根拠を持っている状況を指す。例えば、ウイルス対策ソフトウェアのメンテナが、インターネット上で急速に広がっている新しいマルウェアの警告をソフトウェアベンダから通知を受け取ることがあります。

※2 本書の残りの部分では、「インシデント」と「コンピュータセキュリティインシデント」という用語は互換性があります。

2.2 インシデント対応の必要性

攻撃は個人データやビジネスデータを侵害することが多く、セキュリティ侵害が発生した際には、迅速かつ効果的に対応することが重要です。コンピュータセキュリティのインシデント対応という概念が広く受け入れられ、実施されるようになってきました。インシデント対応能力を持つことの利点の 1 つは、適切なアクションが取られるように、インシデントへの体系的な対応（すなわち、一貫したインシデント対応方法論に従うこと）をサポートすることです。インシデント対応は、担当者がインシデントによって引き起こされる情報の損失や盗難、サービスの中断を最小限に抑えるのに役立ちます。インシデント対応のもう一つの利点は、インシデント対応中に得られた情報を使用して、将来のインシデントへの対応に備え、システムやデータの保護を強化することができることです。また、インシデント対応能力は、インシデント中に発生する可能性のある法的問題に適切に対処するのにも役立ちます。

インシデント対応能力を確立するビジネス上の理由に加えて、連邦省庁は、情報セキュリティの脅威に対する協調的で効果的な防御を指示する法律、規制、および政策を遵守しなければならない。

これらの中でも特に重要なものは以下の通りです。

■ 2000 年に発表された OMB の通達 Circular No.A-130, Appendix III,3 は、連邦政府機関に対し、「システムにセキュリティインシデントが発生した場合にユーザーにヘルプを提供し、共通の脆弱性や脅威に関する情報を共有する能力があることを確保する」よう指示しています。この能力は、他の組織と情報を共有し、司法省のガイダンスに沿って、適切な法的措置を追求する際に機関を支援すべきです。
■ FISMA（2002 年制定）4 は、「セキュリティインシデントの検出、報告、および対応のための手順」を持つことを機関に要求し、連邦情報セキュリティインシデントセンターを集中的に設置することを目的としています。以下はその一部です。

- 機関の情報システムの運用者にタイムリーな技術支援を提供する...情報セキュリティインシデントの検出と処理に関するガイダンスを含む...
- 情報セキュリティを脅かすインシデントに関する情報を集計し、分析する。
- 現在および潜在的な情報セキュリティの脅威と脆弱性について、機関の情報システムのオペレータに情報を提供する ...."

■ 連邦情報処理標準（FIPS）200、Minimum Security Requirements for Federal Information and Information Systems5、2006年3月、インシデント対応を含む連邦情報および情報システムの最低セキュリティ要件を規定しています。具体的な要件は、NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizationsに定義されています。

■ OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information6, May 2007, この資料は、個人情報に関わるセキュリティインシデントの報告に関するガイダンスを提供しています。

2.3 インシデント対応方針・計画・手順の作成

ここでは、インシデント対応に関する方針、計画、手順について、外部とのやりとりに重点を置いて説明します。

2.3.1 ポリシーの要素

インシデント対応を管理するポリシーは、組織ごとに非常に個性があります。しかし、ほとんどのポリシーには、同じ重要な要素が含まれています。

■ 経営陣のコミットメント（責任を伴う公約）の表明
■ 方針の目的と目的
■ 方針の範囲（誰に、何に、どのような状況で適用されるか）
■ コンピュータセキュリティインシデントの定義と関連用語
■ 組織構造と役割、責任、および権限のレベルの定義（機器を没収または切断し、不審な活動を監視するためのインシデント対応チームの権限、特定のタイプのインシデントを報告するための要件、外部とのコミュニケー ションおよび情報共有のための要件とガイドライン（誰と、いつ、どのようなチャネルで何を共有できるかなど）、およびインシデント管理プロセスのハンドオフとエスカレーションポイントを含むべきです。
■ インシデントの優先順位付けまたは重大性の評価 ■ パフォーマンス指標（第3.4.2項で議論）
■ 報告書と連絡帳票

2.3.2 計画の要素

組織は、インシデント対応能力を実装するための行程表となるインシデント対応計画を含め、インシデントに対応するための正式な、焦点を絞った、調整されたアプローチを持つべきです。各組織は、組織の使命、規模、構造、および機能に関連する独自の要件を満たす計画を必要とします。計画には、必要なリソースと管理サポートが記載されているべきです。

インシデント対応計画には、以下の要素が含まれるべきである。

■ 任　務
■ 戦略と目標
■ インシデント対応の組織的アプローチ ■ インシデント対応チームが他の組織や他の組織とどのようにコミュニケーションをとるか
■ インシデント対応能力とその有効性を測定するための尺度（基準）
■ インシデント対応力を成熟させるための行程表
■ プログラムが組織全体にどのように適合しているか。

組織の任務、戦略、インシデント対応の目標は、インシデント対応能力の構造を決定するのに役立ちます。インシデント対応プログラムの構造もまた、計画の中で議論されるべきです。セクション2.4.1では、構造の種類について議論します。

組織が計画を策定し、経営陣の承認を得たら、組織は計画を実施し、能力を成熟させ、インシデント対応の目標を達成するためのロードマップに沿っていることを確認するために、少なくとも年1回は計画を見直すべきです。

2.3.3 手順の要素

手順は、インシデント対応方針と計画に基づくべきです。標準作業手順書（SOP）は、インシデント対応チームが使用する特定の技術的なプロセス、技術、チェックリスト、およびフォームを定義したものです。SOP は、組織の優先順位が対応業務に反映されるように、合理的に包括的で詳細なものでなければなりません。さらに、標準化された対応に従うことで、特にストレスの多いインシデント対応状況に起因する可能性のあるエラーを最小化すべきです。SOP は、その正確性と有用性を検証するためにテストされ、その後、す

べてのチームメンバーに配布されるべきです。SOP 文書は、教育ツールとして使用することができます。提案された SOP の要素は、第 3 章で紹介されています。

2.3.4 外部との情報共有

組織は、インシデントに関して外部の関係者とコミュニケーションを取る必要があることが多く、法執行機関への連絡、メディアからの問い合わせ、外部の専門知識の取得など、適切な場合にはいつでもそうすべきです。他の例としては、インターネットサービスプロバイダ（ISP）、脆弱性のあるソフトウェアのベンダ、または他のインシデント対応チームなど、他の関係者とインシデントついて話し合うことが挙げられます。また、組織は、インシデントの検出と分析を改善するために、関連するインシデント指標情報を仲間と積極的に共有してもよいでしょう。インシデント対応チームは、インシデントが発生する前に、組織の広報部、法務部、および経営陣と情報共有について話し合って、情報共有に関する方針と手順を確立するべきです。そうしないと、インシデントに関する機密情報が無許可の関係者に提供され、さらなる混乱と経済的損失につながる可能性があります。チームは、責任と証拠のために、外部の当事者とのすべての接触とコミュニケーションを文書化しなければなりません。

以下のセクションでは、図 2-1 に示すように、いくつかのタイプの外部当事者との通信に関するガイドラインを示します。

 図21

二重頭の矢印は、いずれかの当事者がコミュニケーションを開始できることを示しています。外部当事者との通信に関する追加情報についてはセクション4を、インシデント対応アウトソース業者が関与するコミュニケーションについてはセクション2.4を参照してください。

2.3.4.1 メディア

インシデントハンドリングチームは、メディアとの相互作用および情報開示に関する組織の方針に準拠したメディアコミュニケーション手順を確立すべきです。※ 7

※ 7 例えば、ある組織は、広報室や法務部のメンバーに、マスコミとのすべてのインシデントの議論に参加してほしいと思うかもしれません。

例えば、ある組織は、広報室や法務部のメンバーに、マスコミとのすべてのインシデントの議論に参加してほしいと思うかもしれません。メディアとインシデントについて議論するためには、組織は多くの場合、単一の連絡先（POC）と少なくとも1つの予備連絡先を指定することが有益であると考えます。これらの指定された連絡先を準備するためには、以下の行動が推奨され、また、メディアと連絡を取り合う可能性のある他の人の準備についても考慮すべきです。

■ インシデントに関するメディアとの対話に関する研修を実施ます。そしてこれには、他の攻撃者を支援する可能性のある対策の技術的詳細などの機密情報を明かさないことの重要性や、重要な情報を十分かつ効果的に公衆に伝えることの肯定的な側面が含まれるべきです。

■ 特定のインシデントについてメディアと議論する前に、メディア関係者に問題点やセンシティブ情報について説明する手順を確立します。

■ メディアとのコミュニケーションが一貫して最新のものとなるように、インシデントの現在の状況についての声明を維持します。

■ メディアからの問い合わせに対応するための一般的な手順を全職員に周知します。

■ インシデント対応演習の際には、模擬取材や記者会見を行います。

以下は、報道関係者への問い合わせの質問例です。

— 誰に攻撃されましたか？なぜ攻撃されたのですか？

— いつ起きたのですか？どのようにして発生しましたか？セキュリティ対策が不十分なために発生したのですか?

— このインシデントはどの程度広がっていますか？何が起こったかを特定し、将来の発生を防ぐために、どのような手順を踏んでいますか?

— このインシデントの影響は？個人を特定できる情報（PII）が流出しましたか？このインシデントの推定コストは？

2.3.4.2 法の執行

セキュリティ関連のインシデントの多くが有罪判決に至らない理由の一つは、一部の組織が法執行機関に適切に連絡していないことにあります。インシデントの調査には、いくつかのレベルの法執行機関が利用可能です。例えば、米国内では、連邦捜査機関（連邦捜査局（FBI）や米国シークレットサービスなど）、地方検事局、州法執行機関、地方（郡など）法執行機関などがあります。米国以外の国の法執行機関も関与する可能性があります。例えば、米国外からの攻撃や、米国外に向けられた攻撃の場合などです。さらに、各機関には、各機関内の法律違反を調査するための監察総監部（OIG）があります。インシデント対応チームは、インシデントが発生する前に、様々な法執行機関の代表者と懇意になり、インシデントが彼らに報告されるべき条件、報告がどのように行われるべきか、どのような証拠が収集されるべきか、どのように収集されるべきかを話し合うべきです。

法執行機関は、法律および組織の手順の要件と一致する方法で、指定された個人を通じて連絡を取るべきです。多くの組織は、法執行機関との主要なPOCとして、1人のインシデント対応チームメンバーを任命することが多いです。この人物は、すべての関連する法執行機関の報告手順に精通しており、もしあれば、どの機関に連絡すべきかをアドバイザリできるように十分な準備をしておくべきです。組織は通常、複数の機関に連絡すべきではないことに注意してください。インシデント対応チームは、潜在的な管轄権の問題が何であるかを理解しておくべきです。（例：物理的な場所-ある州に拠点を置く組織が、第2の州にあるサーバーを第3の州のシステムから攻撃され、第4の州の攻撃者によってリモートで使用されている場合）。

2.3.4.3 インシデント報告組織

FISMA は、連邦政府機関が米国コンピュータ緊急事態対応チーム（US-CERT）8 にインシデントを報告することを要求していますが、これは政府全体のインシデント対応組織であり、連邦文民機関のインシデント対応を支援するものです。US-CERTは、既存の機関対応チームに取って代わるものではなく、むしろ、インシデントに対処するための中心的な役割を果たすことで、連邦文民機関の努力を補強します。これらは、単一

の組織のデータを検討する場合よりも、多くの組織からのデータを検討する場合の方が識別しやすいでしょう。

各機関は、US-CERTの一次および二次POCを指定し、その機関のインシデント対応方針に沿ってすべてのインシデントを報告しなければなりません。組織は、誰がインシデントを報告するために指定されているか、およびインシデントがどのように報告され るべきかを明記した方針を作成すべきです。US-CERTにインシデントを報告するための要件、カテゴリー、および時間枠は、US-CERTのウェブサイトに掲載されています。すべての連邦機関は、そのインシデント対応手順が US-CERT の報告要件に準拠していること、およびその手順が適切に守られていることを確認しなければなりません。

すべての組織は、適切な CSIRT にインシデントを報告することが推奨されます。組織に連絡先のある CSIRT がない場合は、情報共有・分析センター（ISAC）などの他の組織にインシデントを報告することができます。これらの業界に特化した民間セクターのグループの機能の1つは、メンバー間でコンピュータセキュリティ関連の重要な情報を共有することです。ISACは、通信、電気部門、金融サービス、情報技術、研究・教育などの産業部門向けにいくつか結成されています。

2.3.4.4 その他の社外サードパーティ団体（サードパーティー）

組織は、以下に列挙されているグループを含む他のグループとインシデントについて話し合うことを希望する場合があります。これらの外部関係者に連絡を取る場合、組織は、US-CERTまたはそのISACを通じて、関係を仲介する「信頼できる紹介者」として活動することを希望する場合があります。他の組織も同様の問題を経験している可能性が高く、信頼された紹介者は、そのようなパターンが特定され、考慮に入れることができます。

■ 組織の ISP
組織は、主要なネットワークベースの攻撃をブロックしたり、その発生源を追跡したりする際に、その ISP からの支援を必要とする場合があります。

■ 攻撃アドレスの所有者
攻撃が外部組織のIPアドレス空間から発生している場合、インシデントハンドラーは、組織の指定されたセキュリ ティコンタクトに話をして、その活動に注意を喚起したり、証拠を収集するように依頼したりすることをお勧めします。US-CERT または ISACとの調整ようなコミュニケーションをすることを強く推奨します。

■ ソフトウェアベンダ
インシデント・ハンドラーは、疑わしい活動についてソフトウェア・ベンダーと話をしたいと思う可能性があります。このコンタクトには、インシデントに関する最小限の情報を明らかにする必要がある場合には、特定のログエントリの重要性に関する質問や、特定の侵入検知シグネチャに対する既知の偽陽性に関する質問が含まれる可能性があります。場合によっては、より多くの情報を提供する必要があるかもしれません。例えば、サーバが未知のソフトウェアの脆弱性によって侵害されたと思われる場合などです。また、ソフトウェアベンダは、組織が現在の脅威環境を理解するのに役立つように、既知の脅威（例：新たな攻撃）に関する情報を提供する場合もあります。

■ 他のインシデント対応チーム
情報を積極的に共有することで、より効果的かつ効率的なインシデント対応を促進することができます（例：事前警告の提供、準備態勢の強化、状況認識の向上）。FIRST（Forum of Incident Response and Security Teams）、GFIRST（Government Forum of Incident Response and Security Teams）、APWG（Anti-

Phishing Working Group）などのグループは、インシデント対応チームではないが、インシデント対応チーム間の情報共有を推進しています。

■ 影響を受ける外部関係者
インシデントは、外部の関係者に直接影響を与えることがあります。例えば、外部の組織が組織に連絡を取り、組織のユーザーの1人が攻撃を受けていると主張することがあります。外部関係者が影響を受けるもう一つの方法は、攻撃者がクレジットカード情報など、外部関係者に関する機密情報にアクセスできるようになった場合です。いくつかの管轄区域では、組織は、そのようなインシデントによって影響を受けるすべての当事者に通知することが要求されています。状況にかかわらず、組織は、メディアやその他の外部組織がインシデントを通知する前に、影響を受ける外部関係者にインシデントを通知することが望ましいです。影響を受ける関係者は、公開されるべきではない内部調査の詳細を要求することがあります。

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)は、連邦政府機関が個人を特定できる情報（PII）の侵害通知ポリシーを策定し、実施することを要求しています。インシデント・ハンドラーは、PII 違反が発生したと疑われる場合、追加の当事者に通知したり、より短い時間枠内で当事者に通知したりするなど、インシデントハンドリングの行動がどのように異なるべきかを理解すべきです。PII侵害通知ポリシーに関する具体的な推奨事項は、OMB Memorandum M-07-16に記載されています。また、National Conference of State Legislaturesには、州のセキュリティ侵害通知法のリストが掲載されています。

2.4 インシデント対応チームの構成

組織が関与するインシデントが発生したことを発見したり、その疑いがある場合には、インシデント対応チームを利用できるようにしなければなりません。その後、インシデントの大きさと人員の空き状況に応じて、1人以上のチームメンバーがインシデントを処理します。インシデント・ハンドラーは、インシデント・データを分析し、インシデントの影響を判断し、被害を限定し、通常のサービスを回復するために適切に行動します。インシデント対応チームの成功は、組織全体の個人の参加と協力にかかっています。このセクションでは、そのような個人を特定し、インシデント対応チームのモデルについて議論し、適切なモデルを選択するためのアドバイスを提供します。

2.4.1 チームモデル

インシデント対応チームの構成には、以下のようなものがあります。

■ 中央インシデント対応チーム
単一のインシデント対応チームが、組織全体のインシデントを処理します。このモデルは、小規模な組織や、コンピューティングリソースの点で地理的な多様性が少ない組織に有効です。

■ 分散型インシデント対応チーム
組織には複数のインシデント対応チームがあり、それぞれが組織の特定の論理的または物理的セグメントを担当します。このモデルは、大規模な組織（例：1部門につき1チーム）や、離れた場所に主要なコンピューティングリソースを持つ組織（例：地理的な地域につき1チーム、主要な施設につき1チーム）に有効です。しかし、インシデント対応プロセスが組織全体で一貫しており、情報がチーム間で共有されるように、チームは単一の調整された組織の一部でなければなりません。複数のチームが同じインシデントの構成要素を見たり、類似のインシデントを扱う可能性があるため、これは特に重要です。

■ 調整チーム
インシデント対応チームは、他のチームに対する権限を持たずに、他のチームにアドバイスを提供します。このモデルは、CSIRT のための CSIRT と考えることができます。本文書では、中央および分散型 CSIRT に焦点を当てているので、調整チームモデルについては、本文書では詳細には触れていません。

インシデント対応チームは、3つのスタッフ配置モデルのいずれかを使用することもできます。

■ 従業員
組織がインシデント対応業務のすべてを行い、限られた技術的および管理的なサポートを請負業者から受けます。

■ 部分的な外部委託
組織は、インシデント対応業務の一部を外部に委託しています。アウトソーシングを検討する際に考慮すべき主な要因については2.4.2項で論じています。インシデント対応業務は、組織と外部委託先の間で様々な方法で分担することができますが、いくつかの取り決めがあることが一般的です。 – 最も一般的なのは、侵入検知センサー、ファイアウォール、およびその他のセキュリティデバイスの監視を、組織がオフサイトのマネージドセキュリティサービスプロバイダ（MSSP）に24時間、週7日（24時間/週7日）委託することです。 – 組織によっては、基本的なインシデント対応業務を社内で行い、特に深刻なインシデントや広範囲に及ぶインシデントの場合は、請負業者に対応を依頼する場合もあります。

■ 完全な委託
組織は、インシデント対応業務を完全に外部に委託します。このモデルは、組織がフルタイムのインシデント対応チームを必要としていますが、十分な資格を持った従業員がいない場合に使用される可能性が高いです。

2.4.2 チームモデルの選択

インシデント対応チームの適切な構造と人員配置モデルを選択する際には、以下の要素を考慮する必要があります。

■ 24時間365日対応の必要性
ほとんどの組織では、インシデント対応スタッフが24時間365日利用可能であることを必要としています。これは通常、インシデント対応担当者が電話で連絡できることを意味しますが、オンサイトでの対応が必要な場合もあります。インシデントが長引けば長引くほど、損害や損失の可能性が高まるため、インシデント対応にはリアルタイムで使用可能であることが最適です。他の組織と連携して攻撃の発生源を追跡するなど、他の組織と連携する際にもリアルタイムでの連絡が必要になることがよくあります。

■ フルタイムのチームメンバーとパートタイムのチームメンバー
資金、人員、またはインシデント対応のニーズが限られている組織では、パートタイムのインシデント対応チームメンバーしかいない場合があり、より仮想的なインシデント対応チームとして役割を果たしています。この場合、インシデント対応チームは、ボランティアの消防署と考えることができます。緊急事態が発生した場合には、チームのメンバーに迅速に連絡が入り、支援できる人が支援を行うことになります。ITヘルプデスクのような既存のグループは、インシデント報告のための最初のPOCとして機能することができます。ヘルプデスクのメンバーは、初期調査とデータ収集を行い、重大なインシデントが発生したと思われる場合には、インシデント対応チームに警告を出すように訓練することができます。

■ 従業員の士気
インシデント対応の仕事は、ほとんどのチームメンバーのオンコール※の責任と同様に、非常にストレスの多い仕事です。この組み合わせにより、インシデント対応チームのメンバーは過度のストレスを感じやすくなります。また、多くの組織では、特に24時間体制でのサポートに参加してくれる、意欲的で、利用可能で、経験豊富で、適切なスキルを持った人材を見つけるのに苦労することになります。役割を分離し、特にチームメンバーが担当する管理業務の量を減らすことは、士気を大幅に向上させることができます。
（訳者注※：呼ばれたらすぐ対応すること）

■ コスト
コストは、特に従業員が年中無休で24時間体制で現場にいなければならない場合には、大きな要因となります。組織は、トレーニングやスキル維持のための十分な資金など、インシデント対応に特化したコストを予算に含めていないことがあります。インシデント対応チームは、IT の多くの側面を扱うため、そのメンバーは、ほとんどの IT スタッフよりもはるかに幅広い知識を必要とします。また、デジタル・フォレンジック・ソフトウェアなどのインシデント対応ツールの使い方も理解していなければなりません。その他、見落とされる可能性のあるコストとしては、チームの作業エリアの物理的なセキュリティや通信メカニズムなどがあります。

■ スタッフの専門知識
インシデント対応には、いくつかの技術分野における専門的な知識と経験が必要です。外部委託企業は、侵入検知、フォレンジック、脆弱性、エクスプロイト、その他のセキュリティの側面について、組織の従業員よりも深い知識を持っている可能性があります。また、MSSP※は、顧客間のイベントを相関させることができるため、個々の顧客よりも迅速に新たな脅威を特定することができるかもしれません。しかし、組織内の技術スタッフは、通常、外部委託企業よりも組織の環境についての知識が豊富であるため、組織固有の行動やターゲットの重要性に関連した誤検知を特定する上で有益である可能性があります。2.4.3 節には、推奨されるチームメンバーのスキルに関する追加情報が記載されています。アウトソーシングを検討する際には、これらの問題を念頭に置いておくべきです。
（訳者注※：マネージドセキュリティサービスプロバイダ）

■ 現在の仕事の質と将来の仕事の質
現在の仕事の質（幅と深さ）だけでなく、今後の仕事の質を確保するための取り組み（離職率や燃え尽きの防止、新人教育の充実など）を考えるべきです。委託先の仕事の質を客観的に評価するためにはどうすればよいかを考えるべきです。

■ 責任の分担
組織はしばしば、環境の運用上の決定権をアウトソーサーに与えたがらないことがあります（例：ウェブサーバーの切断）。このような決定事項に対して適切なアクションを文書化することが重要です。例えば、ある部分的にアウトソースされたモデルでは、外部委託企業がインシデントデータを組織の内部チームに提供し、さらにインシデントを処理するための推奨事項を提供することで、この問題に対処します。最終的には社内チームが運用上の意思決定を行い、外部委託企業は必要に応じてサポートを継続します。

■ 外部委託企業への機密情報の提供
インシデント対応の責任を分担し、機密情報へのアクセスを制限することで、これを制限することができます。例えば、請負業者は、インシデントで使用されたユーザーID（例：ID 123456）を把握しても、そのユーザーIDに関連する人物がわからない場合があります。その場合、従業員が調査を引き継ぐことができます。機密保持契約（NDA）は、機密情報の開示を保護するための1つの可能なオプションです。

■ 組織固有の知識の不足
インシデントの正確な分析と優先順位付けは、組織の環境に関する特定の知識に依存します。組織は、どの

ようなインシデントが懸念されているか、どのリソースが重要であるか、および様々な状況下での対応レベルはどのようなものであるべきかを定義した、定期的に更新された文書を外部委託企業に提供すべきです。また、組織は、ITインフラ、ネットワーク構成、およびシステムに加えられた全ての変更と更新を報告しなければなりません。そうしないと、請負業者は、各インシデントがどのように処理されるべきか、最善の推測をしなければならず、必然的に誤ったインシデントや双方のフラストレーションにつながってしまいます。また、チーム間のコミュニケーションが希薄であったり、組織が必要な情報を収集していない場合、インシデント対応を外部に委託していない場合には、組織固有の知識の欠如が問題となることもあります。

■ 相関性の欠如

複数のデータソース間の相関関係は非常に重要です。侵入検知システムがウェブサーバへの攻撃未遂を記録していても、外部委託企業がサーバのログにアクセスできない場合、攻撃が成功したかどうかを判断できない可能性があります。効率的な運用を行うためには、外部委託企業は、重要なシステムやセキュリティ機器のログに対して、安全なチャネルを介してリモートで管理者権限を要求することになります。これにより、管理コストが増加し、追加のアクセスエントリーポイントが導入され、機密情報が不正に開示されるリスクが高まります。

■ 複数の場所でのインシデントへの対応

効果的なインシデント対応作業のためには、組織の施設に物理的に常駐する必要があります。外部委託企業が離れた場所にある場合は、外部委託企業がどこにあるか、どの施設でもインシデント対応チームをどのくらいの速さで配置できるか、およびそのためのコストはいくらかを検討してください。施設やエリアによっては、外部委託企業に仕事をさせてはいけないところもあるかもしれませんので、現地視察を検討してみてはいかがでしょうか。

■ インシデント対応のスキルを社内で維持

インシデント対応を完全に外部委託している組織は、インシデント対応の基本的なスキルを社内で維持するように努めるべきです。外部委託企業が利用できない状況が発生する可能性があるので、組織は独自のインシデントハンドリングを行う準備をしておくべきです。また、組織の技術スタッフは、外部委託企業の提案の意義、技術的な意味合い、影響力を理解していなければなりません。

2.4.3 インシデント対応要員

インシデント対応の責任者は、1人の従業員と 1人以上の指定された補欠の従業員でなければなりません。完全に外部委託されたモデルでは、この人は外部委託企業の仕事を監督し、評価します。他のすべてのモデルは一般に、チームマネージャーとチームマネージャーの不在時に権限を持つ1人以上の代理がいます。マネジャーは一般に、上層部管理および他のチーム、組織との連絡係としての機能を含むいろいろな業務を行い、危機の状態を和らげ、そしてチームが必要な人員、資源および技術を持っていることを保障します。マネジャーは技術的に熟達し、優秀なコミュニケーション能力、特に聴衆の範囲※に伝達する能力を有するべきです。マネージャーは、インシデント対応活動が適切に行われるように最終的に責任を負います。
（訳者注※：おそらく関係者一般）

チームマネージャーと副責任者に加えて、一部のチームには、テクニカルリード（技術的なスキルとインシデント対応の経験を持ち、チームの技術的な作業の品質を監督し、最終的な責任を負う人）がいます。テクニカルリードのポジションは、インシデントリードのポジションと混同してはなりません。大規模なチームでは、特定のインシデントを処理するための主要なPOCとしてインシデントリードを割り当てることがよくあり、インシデントリードはインシデントの処理について責任を負います。インシデント対応チームの規模やインシデントの大きさにもよりますが、インシデントリードは実際にインシデントを処理することはあり

ませんが、むしろハンドラーの活動を調整し、ハンドラーから情報を収集し、他のグループにインシデントの最新情報を提供し、チームのニーズが満たされていることを確認します。

インシデント対応チームのメンバーは、システム管理、ネットワーク管理、プログラミング、技術サポート、または侵入検知などの優れた技術スキルを持っていなければなりません。すべてのチームメンバーは、優れた問題解決能力と批判的思考能力を持っていなければなりません。すべてのチームメンバーが技術の専門家である必要はありませんが、実際的な検討や資金面での考慮が大きく影響しています。また、ネットワーク侵入検知、マルウェア解析、フォレンジックなど、特定の技術分野に特化したチームメンバーがいると効果的です。さらに、通常はチームの一員ではない技術的な専門家を一時的に呼び寄せるのも有効な場合が多いです。

学習と成長の機会を提供することで、スタッフの燃え尽きを防ぐことが重要です。スキルの構築と維持のための提案は以下の通りです。

■ 技術的な分野やセキュリティ分野、およびインシデント対応の法的側面などの技術的でないトピックに ついて、能力を維持、強化、拡大するための十分な予算を確保します。これには、スタッフを会議に派遣し、会議への参加を奨励するか、そうでなければ インセンティブを与えること、より深い技術的理解を促進する技術資料の利用可能性を確保する こと、資金が許す限り、必要とされる分野で深い技術的知識を持つ外部の専門家（例：請負業者）を 時折呼び寄せることなどが含まれるべきです。

■ 教材の作成、セキュリティ意識向上ワークショップの実施、調査の実施など、チームメンバーに他の業務を行う機会を与えます。

■ インシデント対応チームのスタッフのローテーションを検討し、一時的に他のスタッフ（ネットワーク管理者など）と交替して新たな技術力を身につける交流会に参加させます。

■ チームメンバーが休みなく仕事ができるように十分な人員を確保します（休暇など）。

■ 上級技術スタッフが経験の浅いスタッフがインシデント対応を学べるように、組織内教育プログラムを作成します。

■ インシデントハンドリングのシナリオを作成し、チームメンバーにどのように対処するかを議論させます。付録Aには、シナリオのセットと、シナリオの議論中に使用する質問のリストが含まれています。

インシデント対応チームのメンバーは、技術的な専門知識に加えて、他のスキルを持つべきです。チームワークのスキルは、インシデント対応を成功させるためには協力と調整が必要であるため、根本的に重要です。また、すべてのチームメンバーは、優れたコミュニケーションスキルを持つべきです。チームは様々な人々と交流するので、スピーキングスキルは重要であり、チームメンバーがアドバイザリや手順書を作成する際には、ライティングスキルもまた重要です。チーム内のすべての人が強力なライティングスキルとスピーキングスキルを持つ必要はありませんが、チームが他の人の前で自分自身をうまく表現できるように、すべてのチーム内の少なくとも数人がこれらのスキルを持っている必要があります。

2.4.4 組織内の依存関係

インシデント対応に参加する可能性がある組織内の他のグループを特定し、必要とされる前に協力を募ることができるようにすることが重要です。全てのインシデント対応チームは、以下のような他のグループの専門知識、判断、能力に依存しています。

■ マネジメント層 マネジメント層は、インシデント対応の方針、予算、および人員配置を確立します。最終的に、マネジメント層は、様々な利害関係者間でインシデント対応を調整し、被害を最小限に抑え、議会、OMB、一般会計事務所（GAO）、およびその他の関係者に報告する責任を負っています。

■ 情報セキュリティ部門
インシデント処理の特定の段階（予防、封じ込め、根絶、回復）では、例えば、ネットワークセキュリティ制御（ファイアウォールのルールセットなど）を変更するために、情報セキュリティ部門のメンバーが必要になる場合があります。

■ ITサポート
IT 技術の専門家（システム管理者やネットワーク管理者など）は、支援に必要なスキルを持っているだけでなく、通常、日常的に管理している技術を最もよく理解しています。これにより、攻撃を受けたシステムを切断するかどうかなど、影響を受けたシステムに対して適切なアクションを取ることを確実にすることができます。

■ 法務部門
法律の専門家は、インシデント対応計画、方針、手順を見直し、プライバシーの権利を含む法律や連邦政府のガイダンスに準拠していることを確認すべきです。さらに、インシデントが証拠収集、容疑者の起訴、訴訟を含む法的な影響を及ぼす可能性がある場合、または情報共有のための責任制限を含む覚書（MOU）またはその他の拘束力のある合意が必要な場合には、法務最高責任者または法務部の指導を求めるべきです。

■ 広報・メディア対応
インシデントの性質や影響に応じて、メディア、ひいては一般市民に情報を提供する必要がある場合があります。

■ 人事部
従業員がインシデントを起こした疑いがある場合には、人事部が関与することがあります。

■ 事業継続計画部門
組織は、インシデント対応の方針や手順と事業継続プロセスが同期していることを確認すべきです。コンピュータ・セキュリティのインシデントは、組織のビジネスの回復力を弱体化させます。事業継続計画の専門家は、インシデントとその影響を認識し、ビジネスへの影響評価、リスク評価、事業継続計画を調整できるようにすべきです。さらに、事業継続計画の専門家は、厳しい状況下での業務中断を最小限に抑えるための幅広い専門知識を持っているため、サービス拒否（DoS）状況のような特定の状況への対応を計画する上で貴重な存在となるかもしれません。

■ 物理的なセキュリティと設備管理部門
コンピュータセキュリティのインシデントの中には、物理的セキュリティの侵害によって発生したり、論理的・物理的な攻撃が協調して行われたりするものがあります。また、インシデント対応チームは、インシデント対応中に、鍵のかかったオフィスから妥協したワークステーションを取得するなど、施設や設備へのアクセスが必要になる場合があります。

2.5 インシデント対応チームサービス

インシデント・レスポンス・チームの主な焦点はインシデント・レスポンスの実行ですが、インシデント・レスポンス**のみ**を実行するチームはほとんどありません。以下は、チームが提供する他のサービスの例です。

■ 侵入検知
インシデント・レスポンス・チームは、第一に侵入検知の責任を負うことが多いです。侵入検知技術に関する知識に基づいて、より迅速かつ正確にインシデントを分析できる体制を整えておくことができるということは、インシデント対応チームの持つ一般的なメリットです。※
※ IDPS 技術の詳細については、NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS) を参照してください。これは http://csrc.nist.gov/publications/PubsSPs.html#800-94 で入手可能です。

■ アドバイザリの配布
チームは、新たな脆弱性や脅威について、組織内でアドバイザリを発行することができます※1。情報発信には、必要に応じて自動化された方法を用いるべきです。例えば、米国脆弱性データベース（NVD）では、新たな脆弱性が追加された際に、XML や RSS フィードで情報を提供しています※2。アドバイザリは、攻撃者がソーシャルエンジニアリングで利用する可能性の高い、注目度の高い社会的・政治的イベント（例：有名人の結婚式）など、新たな脅威が出現した場合に最も必要とされることが多いです。重複した作業や矛盾した情報を避けるために、組織内の1つのグループのみがコンピュータセキュリティアドバイザリを配布すべきです。

※1 チームは、セキュリティ上の問題について、いかなる個人や組織を非難することのないように、アドバイザリを言葉で表現すべきです。チームは、アドバイザリの正確性に関してチームと組織は一切の責任を負わないことを明記した免責事項をアドバイザリに記載する必要があるかどうかについて、法務アドバイザーに相談すべきです。これは、組織のコンピューティングリソースの利用者である請負業者、ベンダー、その他の非雇用者にアドバイザリが送信される場合に最も適切です。

※2 http://nvd.nist.gov/

■ 教育と意識向上
教育と啓発は、リソースを倍増させるものであり、ユーザや技術スタッフがインシデントの検出、報告、および対応に関す る知識があればあるほど、インシデント対応チームの負担を軽減することができます。この情報は、ワークショップ、ウェブサイト、ニュースレター、ポスター、モニターやラップトップに貼るステッカーなど、さまざまな方法で伝えることができます。

■ 情報共有
インシデント対応チームは、ISACや地域パートナーシップなどの情報共有グループに参加していることが多いです。したがって、インシデント対応チームは、インシデントに関連する情報を集約し、その情報を他の組織と効果的に共有したり、関連する情報が企業内で共有されるようにしたりするなど、組織のインシデント情報共有の取り組みを管理することが多いです。

2.6 推奨事項

このセクションでは、コンピュータ・セキュリティのインシデント対応能力を組織化するための主な推奨事項を以下にまとめています。

■ 正式なインシデント対応能力を確立する。
コンピュータ・セキュリティの防御が破られた場合、組織は迅速かつ効果的に対応できるように準備しておく必要があります。FISMA では、連邦政府機関がインシデント対応能力を確立することを要求しています。

■ インシデント対応ポリシーを作成する。
インシデント対応ポリシーは、インシデント対応プログラムの基礎となるものです。インシデント対応ポリシーは、インシデント対応プログラムの基礎となるもので、どのような事象がインシデントとみなされるか

を定義し、インシデント対応のための組織構造を確立し、役割と責任を定義し、インシデントを報告するための要件などを列挙しています。

■ インシデント対応方針に基づいてインシデント対応計画を作成する。
インシデント対応計画は、組織の方針に基づいてインシデント対応プログラムを実施するためのロードマップを提供します。この計画は、プログラムを測定するための指標を含め、プログラムの短期目標と長期目標の両方を示します。また、インシデント対応計画は、インシデント・ハンドラーがどのくらいの頻度で訓練されるべきか、およびインシデント・ハンドラーの要件を示す必要があります。

■ インシデント対応手順書を作成する。
インシデント対応手順書は、インシデントに対応するための詳細な手順を提供します。この手順は、インシデント対応プロセスのすべての段階をカバーしなければなりません。手順は、インシデント対応の方針と計画に基づいているべきです。

■ インシデント関連の情報共有に関する方針と手順を確立する。
組織は、メディア、法執行機関、インシデント報告機関などの外部関係者に、適切なインシデントの詳細を伝えるべきです。インシデント対応チームは、組織の広報室、法務部、および経営陣と協議し、情報共有に関する方針と手順を確立します。チームは、メディアやその他の外部関係者との対話に関する既存の組織の方針を遵守すべきです。

■ インシデントに関する関連情報を適切な組織に提供する。
連邦民間機関は、US-CERT にインシデントを報告することが義務付けられています。その他の組織は、US-CERT および／またはその組織の ISAC に連絡することができます。US-CERT および ISAC は、報告されたデータを使用して、新たな脅威およびインシデントの傾向に関する情報を報告者に提供するため、報告は有益です。

■ インシデント対応チームモデルを選択する際には、関連する要因を考慮 組織は、組織のニーズと利用可能なリソースの文脈で、それぞれの可能性のあるチーム構造モデルと人員配置モデルの長所と短所を慎重に秤量する必要があります。

■ インシデント対応チームにふさわしいスキルを持った人材を選定 インシデント対応チームの信頼性と習熟度は、メンバーの技術力と批判的思考力に大きく依存します。重要な技術的スキルには、システム管理、ネットワーク管理、プログラミング、技術サポート、侵入検知などがあります。効果的なインシデント対応には、チームワークとコミュニケーション能力も必要である。すべてのチームメンバーに必要なトレーニングを提供しなければなりません。

■ インシデント対応に必要で参加する可能性のある組織内の他のグループの特定 すべてのインシデント対応チームは、経営陣、情報保証、ITサポート、法務、広報、施設管理など、他のチームの専門知識、判断力、能力に依存しています。

■ チームが提供すべきサービスを決定 チームの主な焦点はインシデント対応ですが、ほとんどのチームはそれ以外の機能を提供します。例えば、侵入検知センサーの監視、セキュリティ・アドバイザリの配布、セキュリティに関するユーザーへの教育などが挙げられます。