NIST800-61　Rev.2

コンピュータセキュリティ

ハンドリングガイド

２０１２年８月

コンピュータシステム技術に関するレポート

米国国立標準技術研究所（NIST）の情報技術研究所（ITL）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献しています。ITL は、情報技術の発展と生産的な利用を促進するために、試験、試験方法、参照データ、概念実証の実施、技術分析を開発しています。ITL の責任には、連邦政府の情報システムにおける国家安全保障関連情報以外の情報のセキュリティとプライバシーを費用対効果の高い形で確保するための管理、管理、技術、物理的な基準とガイドラインの策定が含まれています。NIST800 シリーズでは、情報システムセキュリティに関する ITL の研究、ガイドライン、アウトリーチの取り組み、産業界、政府、学術機関との連携活動について報告しています。

権　限

本書は、連邦情報セキュリティ管理法（FISMA）公法（P.L.）107-347 に基づく NIST の法的責任を強化するために、NIST が作成したものです。NIST は、連邦政府の情報システムに対する最低限の要件を含む情報セキュリティの標準とガイドラインを策定する責任があるが、このような標準とガイドラインは、国家安全保障システムに対して政策権限を行使する連邦政府の適切な職員の明示的な承認なしには、国家安全保障システムに適用されてはなりません。本ガイドラインは、管理予算局(OMB)の CircularA-130,Section8b(3)「機関情報システムの保護」の要求事項と一致しており、CircularA130,AppendixIV:AnalysisofKeySections で分析されています。補足情報は、CircularA-130,AppendixIII,SecurityofFederalAutomatedInformationResources に記載されています。本書のいかなる内容も、法令上の権限の下で商務省長官が連邦機関に対して強制的かつ拘束力のある基準およびガイドラインを作成したことに反するものであってはなりません。また、これらのガイドラインは、商務長官、OMB長官、またはその他の連邦政府職員の既存の権限を変更したり、それに取って代わるものとして解釈されるべきではありません。この出版物は、非政府組織が任意で使用することができ、米国では著作権の対象とはなりません。しかし、帰属表示は、NIST によって認識されます

1. 序　章

1.1 権　限

国立標準技術研究所（NIST）は、2002 年の連邦情報セキュリティ管理法（FISMA）（公法 107-347）に基づく法的責任を推進するために、この文書を作成しました。NIST は、すべての機関の業務と資産に適切な情報セキュリティを提供するために、最低限の要件を含む標準とガイドラインを策定する責任がありますが、このような標準とガイドラインは、国家安全保障システムには適用されないものとします。本ガイドラインは、管理予算局（OMB）通達 CircularA-130 の第 8b(3)項「省庁情報システムのセキュリティ確保」の要求事項と一致しており、A-130 の付録 IV:重要な項の分析で分析されています。補足情報は、A-130「付録 III」に記載されています。本ガイドラインは、連邦政府機関が使用するために作成されたものです。非政府組織が任意で使用することができ、著作権の対象とはなりませんが、帰属表示が望まれます。また、これらのガイドラインは、商務省長官、OMB長官、またはその他の連邦職員の既存の権限を変更したり、それに取って代わるものとして解釈されるべきではありません。

1.2 目的と範囲

本書は、インシデントへの効果的かつ効率的な対応に関する実践的なガイドラインを提供することで、コンピュータセキュリティインシデントによるリスクを軽減するための組織を支援することを目的としています。本書には、効果的なインシデント対応プログラムの確立に関するガイドラインが含まれていますが、本書の主な焦点は、インシデントの検出、分析、優先順位付け、および対応です。組織は、推奨されるガイドラインとソリューションを、特定のセキュリティとミッションの要件を満たすように調整することが推奨されます。

1.3 対象者

この文書は、コンピュータセキュリティインシデント対応チーム（CSIRT)、システムおよびネットワーク管理者、セキュリティスタッフ、技術サポートスタッフ、最高情報セキュリティ責任者（CISO)、最高情報責任者（CIO)、コンピュータセキュリティプログラムマネージャー、その他セキュリティインシデントへの準備や対応に責任を持つ人々のために作成されました。

1.4 文章構成

本書の残りの部分は、以下のセクションと付録で構成されています。

- セクション 2 では、インシデント対応の必要性について議論し、可能なインシデント対応チームの構造を概説し、インシデントハンドリングに参加する可能性のある組織内の他のグループを強調しています。
- セクション 3 では、基本的なインシデント対応のステップをレビューし、インシデント対応をより効果的に行うためのアドバイス、特にインシデントの検出と分析を提供しています。
- セクション 4 では、インシデント対応の調整と情報共有の必要性を検討しています。
- 付録 A には、インシデント対応の卓上ディスカッションで使用するためのインシデント対応シナリオと質問が含まれています。
- 付録 B は、各インシデントについて収集すべきデータフィールドのリストを提供しています。
- 付録 C と D には、それぞれ用語集と頭字語のリストが含まれています。
- 付録 E は、インシデント対応の計画と実行に有用なリソースを特定しています。
- 付録 F では、インシデント対応に関するよくある質問を取り上げています。
- 付録 G には、コンピュータ・セキュリティ・インシデント関連の危機に対処する際に従うべき主な手順が記載されています。
- 付録 H には、前回の改訂以降の重要な変更点をリストアップした変更ログが含まれています。

抄　録

コンピュータセキュリティのインシデント対応は、情報技術（IT）プログラムの重要な要素となっています。インシデント対応を効果的に行うことは複雑な作業であるため、成功するインシデント対応能力を確立するには、相当な計画とリソースが必要となります。本書は、コンピュータ・セキュリティ・インシデント対応能力を確立し、インシデントを効率的かつ効果的に処理するために、組織を支援するものです。本書は、特にインシデント関連データを分析し、各インシデントへの適切な対応を決定するためのインシデント対応のガイドラインを提供します。このガイドラインは、特定のハードウェアプラットフォーム、オペレーティングシステム、プロトコル、またはアプリケーションに依存せずに使用することができます。

キーワード

コンピュータセキュリティ

インシデントインシデントハンドリング

インシデント対応

情報セキュリティ

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、ユーザがファイル共有に接続した場合、サーバがウェブページの要求を受信した場合、ユーザ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、ウィ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ー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りません。

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 CircularNo.A-130,AppendixIII,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 Systems、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。
- OMBMemorandumM-07-16,Safeguarding Against and Responding to the Breach of Personally Identifiable Information 6,May2007,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す。

■ 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ー、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 のように、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ています。

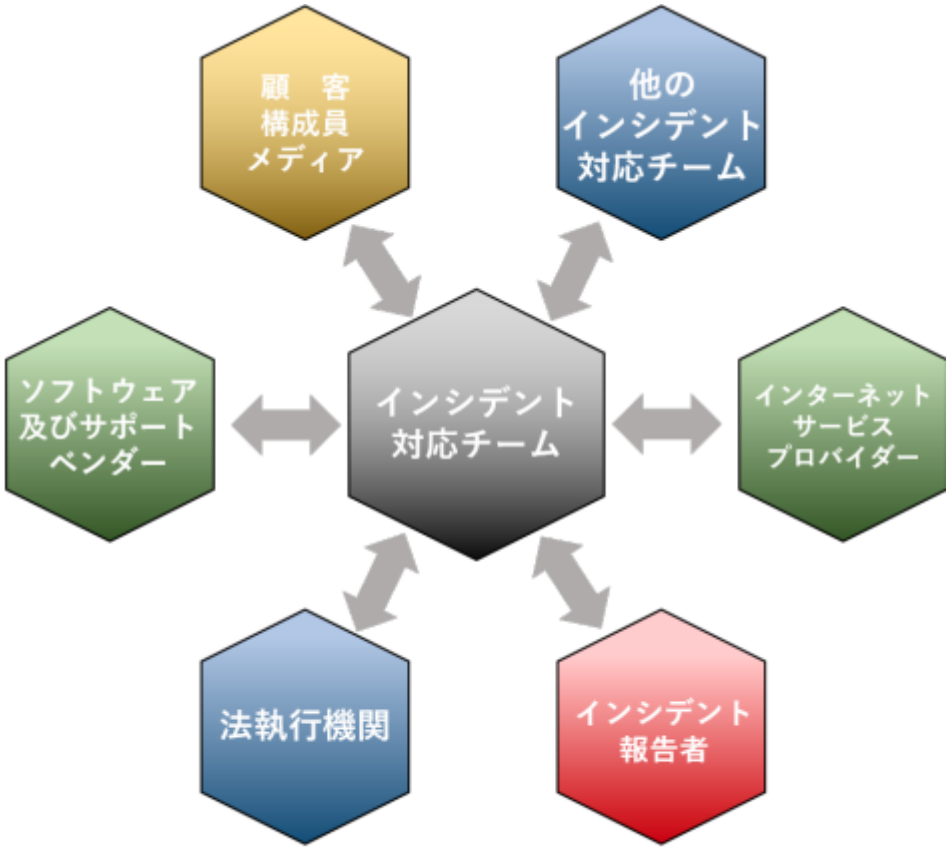

図2-1 外部との連絡

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します。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。

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）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ー**

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ーは、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（ForumofIncidentResponseandSecurityTeams）、GFIRST（GovernmentForumofIncidentResponseandSecurityTeams）、APWG（Anti-PhishingWorkingGroup）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、OMBMemorandumM-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 ID（例：ID123456）を把握しても、そのユーザ 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。マネージャーは一般に、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。マネー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、NISTSP800-94,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、USCERT 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する。**

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する。**

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を特定する。**

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する。**

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への教育などが挙げられます

3.インシデントのハンドリング

インシデント対応プロセスにはいくつかの段階があります。最初の段階では、インシデント対応チームの設立と訓練、必要なツールとリソースの獲得が含まれます。準備期間中、組織は、また、リスク評価の結果に基づいて一連の管理策を選択して実施することで、発生するインシデントの数を制限しようします。しかし対策を実施した後も、残留リスクは確実に存在します。そのため、インシデントが発生した際に組織に注意を喚起するためには、セキュリティ侵害を検知することが必要です。インシデントの深刻度に応じて、組織は、インシデントを抑制し、最終的にインシデントから回復することで、インシデントの影響を軽減することができます。このフェーズでは、マルウェアインシデントを根絶している間に、追加のホストがマルウェアに感染していないかどうかを確認するなど、検出と分析に活動が戻ることがよくあります。インシデントが適切に処理された後、組織は、インシデントの原因とコスト、および将来のインシデントを防止するために組織が取るべき手順を詳細に記載した報告書を発行します。このセクションでは、インシデント対応プロセスの主要なフェーズである、準備、検出と分析、封じ込め、根絶と回復、およびインシデント後の活動について詳細に説明します。図 3-1 は、インシデント対応のライフサイクルを示しています。

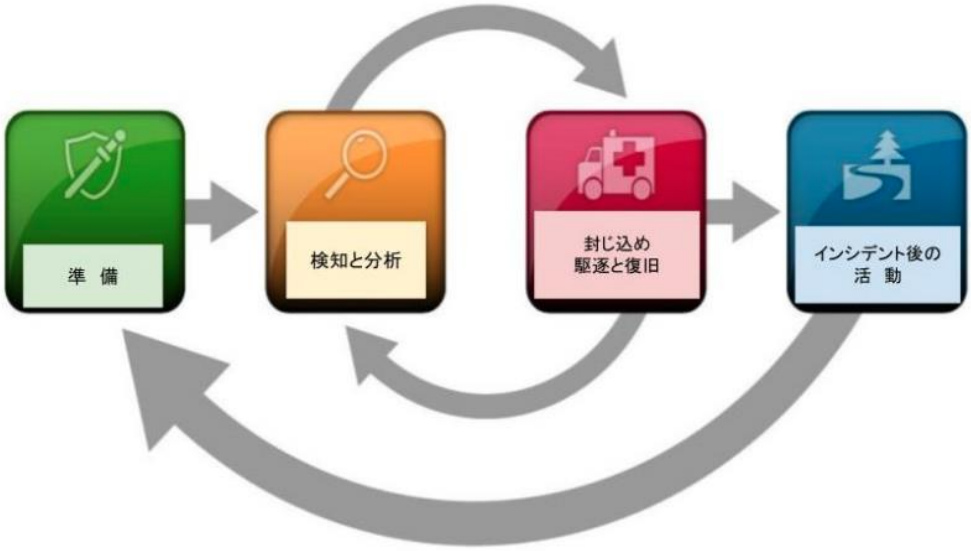

図 3-1 インシデント対応のライフサイクル

3.1 準備

インシデント対応の方法論は、一般的に準備を重視しています。すなわち、組織がインシデントに対応できるようにインシデント対応能力を確立するだけでなく、システム、ネットワーク、およびアプリケーションの安全性を十分に確保することでインシデントを防止するのです。インシデント対応チームは、通常、インシデント予防の責任者ではありませんが、インシデント対応プログラム

を成功させるための基本的な役割を担っています。このセクションでは、インシデントへの対応準備とインシデントの予防に関する基本的なアドバイスを提供します。

3.1.1 インシデントハンドリングの準備

以下のリストは、インシデントハンドリング中に価値があると思われる利用可能なツールとリソースの例を提供しています。これらのリストは、組織のインシデントハンドラーがどのようなツールやリソースを必要としているかを議論するための出発点となることを意図しています。例えば、スマートフォンは、回復力のある緊急通信と調整メカニズムを持つための一つの方法です。組織は、1 つのメカニズムが故障した場合に備えて、複数の（別々の、異なる）通信および調整メカニズムを持つべきです。

インシデントハンドラーの通信と設備について

- チームメンバー、および法執行機関やその他のインシデント対応チームなど、組織内外のその他の人（プライマリーコンタクトおよびバックアップコンタクト）の連絡先情報(電話番号、電子メールアドレス、公開暗号化キー（以下に説明する暗号化ソフトウェアに準拠)、および連絡先の身元を確認するための指示などが含まれます。）
- エスカレーション情報を含む組織内の他チームのオンコール情報
- 電話番号、電子メールアドレス、オンラインフォーム、ユーザが疑わしいインシデントを報告するために使用できる安全なインスタントメッセージングシステムなどのインシデント報告メカニズム。
- インシデント情報やステータスなどを追跡するための、問題追跡システム
- 時間外のサポートや現場でのコミュニケーションのために、チームメンバーが携帯するスマートフォン
- 暗号化ソフトウェアは、チームメンバー間、組織内、および外部の関係者との通信に使用されるもので、連邦政府機関の場合、ソフトウェアは FIPS140-2 認証済みの暗号化アルゴリズムを使用する必要があります。
- 連絡調整のための作戦室。常設の作戦室が必要ない場合や現実的でない場合は、チームは必要に応じて一時的な戦闘室を調達するための手順を作成すべきです。
- 証拠品などの機密性の高いものを確保するための安全な保管手段

インシデント分析のハードウェアとソフトウェア

- ディスクイメージを作成し、ログファイルを保存し、その他の関連するインシデントデータを保存するためのデジタル・フォレンジック・ワークステーション※１および/またはバックアップ装置※１デジタル・フォレンジック・ワークステーションは、インシデントハンドラーがデータを取得して分析するのを支援するために特別に設計されています。これらのワークステーションには、通常、証拠保管に使用できるリムーバブルハードドライブのセットが含まれています。
- データ分析、パケットの盗聴、レポート作成などの活動に使用するノートパソコン
- ワークステーション、サーバ、ネットワーク機器、または仮想化されたものをスペアとして、バックアップの復元やマルウェアの試用など、様々な目的で使用できます。
- 空のリムーバブルディスク
- ネットワークに接続されていないシステムからログファイルなどの証拠品のコピーを印刷するための携帯型プリンタ
- ネットワークトラフィックをキャプチャして分析するためのパケットスニファとプロトコルアナライザ
- ディスクイメージを解析するデジタルフォレンジックソフトウェア
- 信頼のおけるバージョンのプログラムを入れておき、システムから証拠を集める際に使用するリムーバブルメディア
- 証拠収集アクセサリー：法的行動の可能性に備えて証拠を残しておくための、堅表紙のノート、デジタルカメラ、オーディオレコーダー、書類・証拠の受け渡し記録フォーム、証拠保管バッグとタグ、証拠テープなど。

インシデント分析リソース

- 一般に使用されるポートとトロイの木馬のポートのポートリスト
- OS、アプリケーション、プロトコル、侵入検知とアンチウィルスシグネチャなどのドキュメント
- ネットワーク図と重要な資産の一覧例）データベースサーバ
- 期待されるネットワーク、システム、アプリケーションの活動の現在の基準
- インシデントの分析、検証、および撲滅を迅速に行うための重要ファイルの暗号化ハッシュ

インシデント軽減ソフトウェア

■ 復元やリカバリーのためのクリーンな OS やアプリケーションのインストールイメージへのアクセス

多くのインシデント対応チームは、調査中に必要となる可能性のある資材が入った携帯用ケースであるジャンプキットを作成しています。ジャンプキットは、いつでも持ち運べるようにしておく必要があります。ジャンプキットには、上記の箇条書きのリストに記載されているものと同じものが多く含まれています。例えば、各ジャンプキットには通常、適切なソフトウェア（例：パケットスニッファー、デジタルフォレンジック）を搭載したノートパソコンが含まれています。その他の重要な材料には、バックアップデバイス、ブランクメディア、および基本的なネットワーク機器とケーブルが含まれています。ジャンプキットを持つ目的は、迅速な対応を容易にすることですので、チームはジャンプキットからのアイテムの借用を避けるべきです。

各インシデント担当者は、少なくとも 2 台のコンピューティングデバイス（ノートパソコンなど）にアクセスできるようにしておくべきです。1 台は、ジャンプキットからのものなど、パケットスニッフィング、マルウェア解析、およびそれらを実行するノートパソコンを汚染する危険性のあるその他のすべてのアクションを実行するために使用してください。このノートパソコンは、別のインシデントに使用する前に、スクラブし、すべてのソフトウェアを再インストールする必要があります。このノートパソコンは特別な目的のため、標準的なエンタープライズツールや設定以外のソフトウェアを使用する可能性が高いことに注意してください。調査用ノートパソコンに加えて、各インシデントハンドラーは、報告書を書いたり、電子メールを読んだり、実地でのインシデント分析とは無関係の他の業務を行ったりするために、標準的なノートパソコン、スマートフォン、または他のコンピューティングデバイスを持っているべきです。

模擬インシデントを含む演習も、インシデントハンドリングのためのスタッフの準備に非常に有用です。演習※の詳細については NISTSP800-84 を、演習シナリオのサンプルについては付録 A を参照してください。

※ IT 計画および IT 対応能力のためのテスト、トレーニング、演習プログラムのガイド
http://csrc.nist.gov/publications/PubsSPs.html#800-84

3.1.2 インシデントの予防

組織のビジネスプロセスを保護するためには、インシデントの数を適度に少なくすることが非常に重要です。セキュリティ管理が不十分な場合、インシデントが大量に発生し、インシデント対応チームを圧倒する可能性があります。その結果、対応に時間がかかったり、不完全なものになったりして、ビジネスへの悪影響が大きくなる可能性があります（例：被害の拡大、サービスの長期化、データの利用不能など)。

ネットワーク、システム、およびアプリケーションのセキュリティ確保に関する具体的なアドバイスを提供することは、この文書の範囲外です。インシデント対応チームは、一般的にリソースの安全確保には責任を負いませんが、健全なセキュリティ対策の提唱者となり得ます。インシデント対応チームは、組織が他の方法では気付かない問題を特定できる可能性があります。インシデント対応チームは、ギャップを特定することで、リスク評価と訓練において重要な役割を果たすことができます。他の文書では、一般的なセキュリティの概念や、オペレーティングシステムやアプリケーションに特化したガイドラインについてのアドバイスがすでに提供されています※。しかし、以下に、ネットワーク、システム、およびアプリケーションのセキュリティを確保するために推奨されている主な実践方法の概要について簡単に説明します。

※http://csrc.nist.gov/publications/PubsSPs.html は、コンピュータセキュリティに関する NIST の特別出版物へのリンクを提供しています。

■　リスク評価

システムとアプリケーションの定期的なリスク評価は、脅威と脆弱性の組み合わせによってどのようなリスクが引き起こされているかを判断するべきです※１。これには、組織固有の脅威を含め、適用可能な脅威を理解することが含まれます。それぞれのリスクには優先順位をつけ、リスクの全体的な合理的なレベルに達するまで、リスクを軽減、移転、受容することができます。定期的にリスクアセスメントを実施するもう一つの利点は、重要な資源が特定され、スタッフはそれらの資源に対する監視と対応活動に重点を置くことができるという点です※２。

※１　リスク評価に関するガイドラインは、NISTSP800-30,リスクアセスメントの実施の手引き http://csrc.nist.gov/publications/PubsSPs.html#800-30-Rev1 に掲載されています。

※2 クリティカルなリソースの特定に関する情報は、FIPS199「連邦情報および情報システムのセキュリティ分類基準」(http://csrc.nist.gov/publications/PubsFIPS.html) で議論されています。

■ ホストセキュリティすべてのホストは、標準的な設定を用いて適切にセキュリティを強化する必要があります。各ホストのパッチを適切に適用することに加えて、権限のあるタスクを実行するために必要な権限のみをユーザに付与するという原則に従うように設定されている必要があります。監査を有効にし、セキュリティ関連の重要なイベントをログに記録しなければなりません。ホストとその設定のセキュリティを継続的に監視する必要があります※3。多くの組織は、一貫して効果的にホストのセキュリティを確保するために、Security Content Automation Protocol(SCAP)※4で表現されたオペレーティングシステムとアプリケーションの設定チェックリストを使用しています※5。

※3 継続的監視の詳細については、NISTSP800-137「連邦政府の情報システムと組織のための情報セキュリティの継続的な監視」(http://csrc.nist.gov/publications/PubsSPs.html#800-137)を参照してください。
※4 SCAP の詳細については、NISTSP800-117Revision1,「セキュリティ・コンテンツ・オートメーション・プロトコル(SCAP)の採用と使用の手引き」
Version1.2(http://csrc.nist.gov/publications/PubsSPs.html#800-117)を参照してください。
※5 NIST はセキュリティチェックリストのリポジトリを http://checklists.nist.gov/で公開しています。

■ ネットワークセキュリティネットワークの境界は、明示的に許可されていないすべてのアクティビティを拒否するように設定する必要があります。これには、仮想プライベートネットワーク(VPN)や他の組織への専用接続など、すべての接続ポイントのセキュリティを確保することが含まれます。

■ マルウェアの予防マルウェアを検出して停止させるためのソフトウェアは、組織全体に配備されている必要があります。マルウェア対策は、ホストレベル（サーバやワークステーションのオペレーティングシステムなど)、アプリケーションサーバレベル（電子メールサーバ、ウェブプロキシなど)、アプリケーションクライアントレベル（電子メールクライアント、インスタントメッセージングクライアントなど）で展開する必要があります。

■ ユーザの意識向上とトレーニングネットワーク、システムおよびアプリケーションの適切な使用に関するポリシー・手順をユーザに周知すべきです。また、過去のインシデントから得られた適用可能な教訓をユーザと共有し、自分たちの行動が組織にどのような影響を与えるかを確認できるようにする必要があります。インシデントに関するユーザの意識を向上させることで、インシデントの頻度を減らすことができます。IT スタッフは、組織のセキュリティ基準に従ってネットワーク、システム、およびアプリケーションを維持できるように訓練を受けるべきです。

3.2 検出と分析

3.2.1 攻撃手法

インシデントは無数の方法で発生する可能性があるため、すべてのインシデントに対処するためのひとつひとつの手順書を作成することは不可能です。組織は、一般的にどのようなインシデントにも対応できるように準備しておくべきですが、一般的な攻撃手法を使用するインシデントに対応できるように準備することに重点を置くべきです。異なるタイプのインシデントには、異なる対応戦略が必要です。以下に挙げた攻撃手法は、インシデントの決定的な分類を提供することを意図したものではありません。むしろ、これらは単に一般的な攻撃方法を列挙したものであり、より具体的な対処方法を定義するための基礎として利用することができます。

■ 外部／リムーバブルメディアリムーバブルメディアや周辺機器（例えば、感染した USB フラッシュドライブからシステムに拡散する悪意のあるコードなど）から実行される攻撃。

■ 消耗システム、ネットワーク、またはサービスを危殆化、劣化、または破壊するために、ブルートフォースの手法を用いた攻撃(例:サービスやアプリケーションへのアクセスを妨害または拒否することを目的とした DDoS、パスワード、CAPTCHAS、デジタル署名などの認証メカニズムに対するブルートフォース攻撃)。

■ ウェブ Web サイトや Web ベースのアプリケーションから実行される攻撃。例えば、資格情報を盗むために使用されるクロスサイトスクリプティング攻撃や、ブラウザの脆弱性を突いてマルウェアをインストールするサイトへのリダイレクトなどが挙げられます。

■ E メールメールメッセージや添付ファイルを介して実行される攻撃。例えば、添付文書を装ったエクスプロイトコードや、メールメッセージの本文にある悪意のあるウェブサイトへのリンクなどが挙げられます。

■ なりすまし善良なものを悪意のあるものに置き換える攻撃。例えば、なりすまし、中間者攻撃、不正な無線アクセスポイント、SQL インジェクション攻撃などは、すべてなりすましを伴います。

■ 不適切な使用認可されたユーザによる組織の許容される利用ポリシーの違反に起因するすべてのインシデント（上記のカテゴリーを除く）。例えば、ユーザがファイル共有ソフトウェアをインストールして機密データの損失を招いた場合、またはユーザがシステム上で違法行為を行った場合。

■ 機器の紛失または盗難ノートパソコン、スマートフォン、認証トークンなど、組織が使用しているコンピューティングデバイスやメディアの紛失や盗難。

■ その他上のどのカテゴリーにも当てはまらない攻撃。このセクションでは、あらゆるタイプのインシデントに対処するための推奨される実践方法に焦点を当てています。攻撃手法に基づいた具体的なアドバイスの提供は、この出版物の範囲外です。このようなガイドラインは、マルウェアのインシデント予防と処理に関する NISTSP800-83 のような、他のインシデント処理のトピックを扱う別の出版物で提供されます。

3.2.2 インシデントの兆候

多くの組織にとって、インシデント対応プロセスの中で最も困難な部分は、インシデントの可能性を正確に検出して評価することであり、インシデントが発生したかどうか、発生した場合には問題の種類、程度、および大きさを判断することです。これを困難にしているのは、3 つの要因が重なっているからです。

■ インシデントは、詳細さと正確性が異なるさまざまな方法で検出される可能性があります。自動検出機能には、ネットワークベースおよびホストベースの IDPS、ウィルス対策ソフト、ログアナライザなどがあります。インシデントは、ユーザから報告された問題などの手動の手段

によっても検出されることがあります。インシデントの中には、簡単に検出できる明白な兆候があるものもあれば、ほとんど検出できないものもあります。

■ インシデントの潜在的な兆候の量は一般的に多く、例えば、組織が一日に何千、何百万もの侵入検知センサーのアラートを受信することも珍しくありません。（このようなアラートの分析に関する情報については、セクション 3.2.4 を参照）

■ インシデント関連データを適切かつ効率的に分析するためには、深く専門的な技術知識と豊富な経験が必要です。

インシデントの兆候は、「前兆」と「兆候」という 2 つのカテゴリーのどちらかに分類されます。兆候とは、インシデントが発生した可能性がある、または現在発生している可能性があることを示すサインです。
ほとんどの攻撃は、ターゲットから見れば、識別可能な前兆や検出可能な前兆を持っていません。前兆が検出された場合、組織は、攻撃からターゲットを救うためにセキュリティ姿勢を変更することで、インシデントを防止する機会があるかもしれません。最低限、組織はターゲットが関与する活動をより綿密に監視することができます。前兆の例としては、以下のようなものがあります。

■ 脆弱性スキャナの使用状況を示すウェブサーバのログエントリ
■ 組織のメールサーバの脆弱性を標的とした新たなエクスプロイトの発表
■ 組織を攻撃すると表明した集団からの脅迫

前兆は比較的まれですが、兆候はとてもありふれています。兆候の種類が多すぎてリストアップしきれませんが、以下にいくつかの例を挙げます。

■ ネットワーク侵入検知センサーによるデータベースサーバに対してバッファオーバーフロー発生の警告
■ アンチウィルスソフトによるホストのマルウェア感染検出の警告
■ システム管理者によるファイル名に異常な文字が含まれていることへの警告
■ ホストのログに、監査設定の変更が記録される。
■ アプリケーションによる見慣れないリモートシステムからの複数ログイン失敗をログに記録される。
■ 電子メール管理者が、不審な内容の電子メールが大量の配信エラー（バウンスメール）を見つける。

■ ネットワーク管理者が、典型的なネットワークトラフィックフローからの異常な逸脱に気づく。

3.2.3 前兆と兆候のソース

前兆と兆候は、多くの異なるソースを使用して特定されますが、最も一般的なものは、コンピュータセキュリティソフトウェアの警告、ログ、公開されている情報及び人です。表 3-2 に、各カテゴリーの前兆と兆候の一般的なソースと説明を示します。

アラート

ソース	説　明
侵入検知・防止システム（IDPS）	IDPS 製品は不審なイベントを識別し、攻撃が検出された日時、攻撃の種類、送信元と送信先の IP アドレス、ユーザ名（該当する場合は既知のもの）など、不審なイベントに関する関連データを記録します。ほとんどの IDPS 製品では、攻撃シグネチャを使用して悪意のある活動を識別しています。最新の攻撃を検出できるように、シグネチャを常に最新の状態に保つ必要があります。IDPS ソフトウェアは、悪意のある活動が発生していることを示す偽のポジティブアラートを生成しますが、実際には何も発生していないことがしばしばあります。アナリストは、記録されたサポートデータを精査するか、他のソースから関連データを入手して IDPS アラートを手動で検証する必要があります。
シーム(SIEM)	セキュリティ情報・イベント管理（SIEM）製品は IDPS 製品と似ていますが、ログデータの分析に基づいてアラートを生成します（後述）。
ウィルス対策およびアンチスパムソフトウェア	ウィルス対策ソフトは、様々な形態のマルウェアを検出し、アラートを生成し、マルウェアがホストに感染するのを防ぎます。現在のウィルス対策製品は、マルウェアのシグネチャが最新の状態に保たれていれば、多くのマルウェアのインスタンスを停止させる効果があります。スパム対策ソフトは、スパムを検出し、ユーザのメールボックスに届かないようにします。スパムにはマルウェアやフィッシング攻撃、その他の悪質なコンテンツが含まれている可能性があるため、スパム対策ソフトからの警告は攻撃の企図を示している可能性があります。
ファイル完全性チェックソフトウェア	ファイル完全性チェックソフトウェアは、インシデント時に重要なファイルに加えられた変更を検出することができます。ハッシュアルゴリズムを使用して、指定された各ファイルの暗号チェックサムを取得します。ファイルが変更され、チェックサムが再計算された場合、新しいチェックサムが古いチェックサムと一致しない可能性が非常に高くなります。定期的にチェックサムを再計算し、以前の値と比較することで、ファイルの変更を検出することができます。
サードパーティによるモニタリングサービス	サードパーティは、サブスクリプションベースの様々な無料モニタリングサービスを提供しています。例えば、IP アドレスやドメイン名などが他の組織が関与する現在のインシデント活動に関連している時に、組織に通知する不正検知サービスがあります。似たような情報を持つ無料のリアルタイムブラックリストもあります。サードパーティ監視サービスのもう一つの例として、CSIRC の通知リストがあります。これらのリストは、他のインシデント対応チームのみが利用できることが多いです。

ロ　グ

ソース	説　明
OS,サービス 及び アプリケーションの ロ　グ	オペレーティングシステム、サービス、およびアプリケーションからのログ（特に監査関連データ）は、インシデントが発生した際に、どのアカウントにアクセスしたか、どのようなアクションが実行されたかを記録するなど、非常に価値のあるものであることが多いです。組織は、すべてのシステムでログ取得の基準レベルが必要で、重要なシステムではより高い基準レベルにします。ログは、イベント情報を関連付けて分析に使用することができます。イベント情報に応じて、インシデントを示すアラートを生成することができます。3.2.4 節では、集中ログの価値について述べています。
ネットワーク デバイスのログ	ファイアウォールやルータなどのネットワークデバイスからのログは、通常、前兆や兆候の主要なソースではありません。これらのデバイスは通常、ブロックされた接続試行をログに記録するように設定されていますが、アクティビティの性質に関する情報はほとんど得られません。しかし、ネットワークの傾向を特定したり、他のデバイスで検出されたイベントを関連付けたりする上では貴重な情報となります。
ネットワーク フロー	ネットワークフローとは、ホスト間で発生する特定の通信セッションのことです。ルータやその他のネットワーク機器は、ネットワークフロー情報を提供することができ、マルウェアやデータの流出、その他の悪意のある行為によって引き起こされる異常なネットワークアクティビティを見つけるために使用することができます。フローデータのフォーマットには、NetFlow、sFlow、IPFIX など多くの標準があります。

公に入手可能な情報

ソース	説　明
新しい脆弱性や エクスプロイト に関する情報	新しい脆弱性とその悪用を常に把握しておくことは、いくつかのインシデントの発生を防ぎ、新たな攻撃の検出と分析に役立てることができます。US-CERT33 や CERT®/CC などの組織は、ブリーフィング、ウェブ投稿、およびメーリングリストを通じて、脅威の更新情報を定期的に提供しています。

人

ソース	説　明
組織内の人々	ユーザ、システム管理者、ネットワーク管理者、セキュリティ担当者、および組織内のその他の者が、インシデントの兆候を報告することがあります。そのような報告をすべて検証することが重要です。情報を提供した人に、その情報の正確さにどの程度の自信があるかを尋ねるのも一つの方法です。この推定値を提供された情報と一緒に記録しておくと、インシデント分析の際に、特に矛盾するデータが発見された場合に、かなり役立ちます。
組織外の人々	外部から発生したインシデントの報告は、真摯に受け止めるべきです。例えば、組織のシステムが攻撃されていると主張する者から組織に連絡が来るかもしれません。外部ユーザは、改ざんされたウェブページや利用できないサービスなど、他の兆候を報告することもあります。他のインシデント対応チームもインシデントを報告することがあります。外部の関係者が兆候を報告するための仕組みを用意し、訓練を受けたスタッフがそれらの仕組みを注意深く監視することが重要です。これは、ヘルプデスクにメッセージを転送するように設定された電話番号と電子メールアドレスを設定するのと同じくらい簡単なことかもしれません。

3.2.4 インシデント分析

すべての前兆や兆候が正確であることが保証されていれば、インシデントの検出や分析は簡単です。しかし、残念ながらそうではありません。例えば、サーバが利用できないという苦情など、ユーザが提供した兆候が正しくないことがよくあります。侵入検知システムは、誤ったポジティブ、つまり不正確な兆候を生成することがあります。これらの例は、インシデントの検出と分析を困難にしていることを示しています。理想的には、それぞれの指標は、その正確性を判断するために評価されなければなりまセンサーらに悪いことに、兆候の総数は1日に何千、何百万ということもあります。すべての兆候の中から実際に発生したセキュリティインシデントを見つけるのは、大変な作業になります。

また、兆候が正確であったとしても、必ずしもインシデントが発生したとは限りません。サーバのクラッシュや重要なファイルの変更など、いくつかの兆候の中には、人為的なミスなど、セキュリティインシデント以外のいくつかの理由で発生する可能性があります。しかし、兆候が発生していれば、インシデントが発生しているかもしれないと疑い、それに応じて行動することは理にかなっています。特定の事象が実際にインシデントであるかどうかの判断は、時に判断の問題となります。判断を下すために、他の技術担当者や情報セキュリティ担当者と協力することが必要な場合もあります。多くの場合、状況がセキュリティ関連であるかどうかに関係なく、同じ方法で処理され

るべきです。例えば、ある組織でインターネット接続が 12 時間ごとに失われ、誰も原因がわからない場合、スタッフは同じように迅速に問題を解決したいと考え、原因に関係なく同じリソースを使って問題を診断することになるでしょう。

インシデントの中には、明らかに改ざんされたウェブページなど、検出しやすいものもあります。しかし、多くのインシデントは、そのような明確な症状とは関連していません。システム構成ファイルの変更のような小さな兆候だけが、インシデントが発生したことを示す唯一の兆候かもしれません。インシデントハンドリングでは、検出が最も困難な作業かもしれません。インシデントハンドラーは、何が起こったのかを判断するために、曖昧で、矛盾した、不完全な症状を分析する責任があります。検出を容易にする技術的な解決策は存在しますが、最良の解決策は、前兆や兆候を効果的かつ効率的に分析し、適切な行動をとることができる、経験豊富で熟練したスタッフのチームを構築することです。十分な訓練を受けた有能なスタッフがいなければ、インシデントの検出と分析は非効率的に行われ、コストのかかるミスを犯すことになります。

インシデント対応チームは、事前に定義されたプロセスに従って、各インシデントの分析と検証を迅速に行い、各ステップを文書化する必要があります。インシデントが発生したとチームが判断した場合、チームは迅速に初期分析を行い、どのネットワーク、システム、またはアプリケーションが影響を受けるのかなど、インシデントの範囲を決定する必要があります。インシデントが発生したのは誰なのか、何が原因なのか、インシデントがどのように発生しているのか（どのようなツールや攻撃方法が使用されているのか、どのような脆弱性が悪用されているのかなど）。初期分析は、インシデントの封じ込めやより深いインシデントの影響分析など、チームがその後の活動に優先順位をつけるのに十分な情報を提供しなければなりません。

初期分析と検証を行うことは困難です。以下は、インシデント分析をより簡単で効果的なものにするための推奨事項です。

■ 正常な動作を理解する

インシデント対応チームのメンバーは、ネットワーク、システム、およびアプリケーションを研究し、異常な動作をより簡単に認識できるように、その正常な動作を理解する必要があります。インシデントハンドラーは、環境全体のすべての行動について包括的な知識を持っているわけではありませんが、どの専門家がそのギャップを埋めることができるかを知っておく必要があります。この知識を得るための一つの方法は、ログエントリとセキュリティアラートを確

認することです。これは、ログを適切なサイズに凝縮するためのフィルタリングが使用されていない場合、退屈な作業になるかもしれません。ハンドラーがログやアラートに慣れてくると、原因不明のエントリに焦点を当てることができるようになり、通常は調査することがより重要になります。頻繁にログのレビューを行うことで、知識を新鮮なものに保つことができ、分析者は時間の経過とともに傾向や変化に気づくことができるようになります。また、レビューにより、各ソースの信頼度の指標も得ることができます。

（以下は rev.1日本語オリジナル）

ログをレビューし、興味のあるエントリを調査することは、インシデントを処理する準備にもなります。インシデントの処理では、これらのスキルが必要になります。（引用ここまで）

■ ログ保持ポリシーの作成

インシデントに関する情報は、ファイアウォール、IDPS、アプリケーションログなど、いくつかの場所に記録される可能性があります。ログデータの保持期間を指定したログ保持ポリシーを実装すると、古いログエントリには、偵察活動や以前に同様の攻撃が行われたことが示されている可能性があるため、分析に非常に役立つ可能性があります。ログを保持するもう一つの理由は、数日後、数週間後、あるいは数か月後にならないとインシデントが発見されない可能性があることです。ログデータの保持期間は、組織のデータ保持ポリシーやデータ量など、いくつかの要因に依存します。ログに関する追加の推奨事項については、NISTSP800-92「Guide to Computer Security Log Management」を参照してください。

■ イベント相関処理の実施

インシデントの証拠は、異なるタイプのデータを含む複数のログに記録されることがあります。ファイアウォールログには使用されたソース IP アドレスが記録され、アプリケーションログにはユーザ名が記録されることがあります。ネットワーク IDPS は、特定のホストに対して攻撃が開始されたことを検出することができますが、攻撃の成否はわかりません。アナリストは、その情報を判断するためにホストのログを調べる必要があるかもしれません。複数の兆候ソース間のイベントを相関させることは、特定のインシデントが発生したかどうかを検証する上で非常に重要です。

■ すべてのホストのクロックを同期

NTP（Network Time Protocol）などのプロトコルは、ホスト間のクロックを同期させます。イベントを報告するデバイスのクロック設定が一貫していない場合、イベントの相関関係はよ

り複雑になります。例えば、攻撃が 12:07:01、12:10:35、11:07:06 に発生したことを示すログよりも、証拠という観点から、攻撃が 12:07:01 に発生したことを示す 3 つのログを持つ（一貫したタイムスタンプがある）方が望ましいです。

■ 情報のナレッジベースの維持・使用

ナレッジベースには、ハンドラーがインシデント分析時に素早く参照するために必要な情報が含まれている必要があります。複雑な構造のナレッジベースを構築することも可能ですが、シンプルなアプローチが効果的です。テキスト文書、スプレッドシート、比較的シンプルなデータベースは、チームメンバー間でデータを共有するために効果的かつ柔軟性があり、検索可能なメカニズムを提供します。また、ナレッジベースには、IDPS アラート、オペレーティングシステムのログエントリ、アプリケーションのエラーコードなどの前兆や兆候の重要性や妥当性の説明など、さまざまな情報が含まれていることが望ましいです。

■ イベントの相関関係処理の実施

インターネット検索エンジンは、アナリストが、異常なアクティビティに関する情報を見つけるのに役立ちます。例えば、TCP ポート 22912 をターゲットにした異常な接続の試みをアナリストが目にすることがあります。「TCP」、「port」、および「22912」という用語で検索すると、類似のアクティビティのログや、ポート番号の重要性についての説明を含むいくつかのヒットが返ってくることがあります。これらの検索を行うことによる組織へのリスクを最小限に抑えるために、調査には別のワークステーションを使用すべきであることに注意してください。

■ パケットスニファを実行して追加データを収集

インジケータは、ハンドラーが何が起こっているのかを理解するのに十分な詳細を記録していないことがあります。インシデントがネットワーク上で発生している場合、必要なデータを収集する最速の方法は、パケットスニッファーにネットワークトラフィックをキャプチャさせることかもしれません。指定された基準に一致するトラフィックを記録するようにスニッファーを設定することで、データ量を管理可能な状態に保ち、他の情報を不用意に取得することを最小限に抑えることができます。プライバシーの問題があるため、組織によっては、パケットスニッファーを使用する前にインシデントハンドラーに要求して許可を得ることが必要とする場合があります。

■ データのフィルタリングすべての兆候を確認して分析するには、シンプルに十分な時間はありません。最低限、最も疑わしい活動を調査する必要があります。効果的な戦略の 1 つは、取るに足らない兆候のカテゴリーをフィルタリングすることです。もう一つのフィルタリング戦略は、最も重要度の高い兆候のカテゴリーのみを表示することです。しかしこの方法では、新たな悪意のある活動が、選択した兆候カテゴリーのいずれかも該当しない可能性があるため、大きなリスクを伴います。

■ 他社の支援を求める時として、チームはインシデントの完全な原因と性質を判断できないことがあります。チームがインシデントを封じ込め、根絶するための十分な情報が不足している場合は、内部のリソース（情報セキュリティスタッフなど）や外部のリソース（US-CERT、他の CSIRT、インシデント対応の専門知識を持つ請負業者など）に相談する必要があります。各インシデントの原因を正確に判断して、インシデントを完全に封じ込め、悪用された脆弱性を緩和して、同様のインシデントが発生しないようにすることが重要です。

3.2.5 インシデントの文書

インシデントが発生したと疑われるインシデント対応チームは、直ちにインシデントに関するすべての事実を記録しなければなりません※１。ログブックはそのための効果的でシンプルな媒体※２ですが、ノートパソコン、オーディオレコーダー、デジタルカメラもこの目的を果たすことができます※３。システムイベント、会話、および観察されたファイルの変更を文書化することは、より効率的かつ体系的で、エラーの発生しにくい問題処理につながります。インシデントが検出されてから最終的な解決に至るまでのすべてのステップは、文書化され、タイムスタンプが付けられていなければなりません。またそれらの全ての文書には、日付が付けられ、インシデントハンドラーによって署名されなければなりません。このような性質の情報は、法的起訴が追求された場合、法廷で証拠として使用することもできます。可能な限り、ハンドラーは少なくとも 2人のチームで作業すべきです。一人がイベントを記録し、記録する一方で、もう一人が技術的な作業を行うことができます。セクション 3.3.3.2 には、証拠についてのより詳しい情報が示されています※４。

インシデント対応チームは、その他の関連情報とともに、インシデントの状況に関する記録を保持すべきです※５。問題追跡システムなどのアプリケーションやデータベースを使用することは、インシデントが適時に処理され、解決するのに役立ちます。問題追跡システムには、以下の情報が含まれているべきです。

■　インシデントの現在の状態（新規、進行中、調査のために転送された、解決されたなど）。

■　インシデントの概要

■　インシデントに関連する兆候

■　このインシデントに関連するその他のインシデント

■　このインシデントに関して、すべてのインシデントハンドラーがとった行動

■　書類・証拠受け渡し記録（該当する場合

■　インシデントに関連した影響評価

■　他の関係者の連絡先情報（システム所有者、システム管理者など

■　インシデント調査で集めた証拠の一覧表

■　インシデントハンドラーからのコメント

■　次の措置（例：ホストの再構築、アプリケーションのアップグレード）※６

インシデント対応チームは、インシデントデータを保護し、インシデントデータへのアクセスを制限する必要があります。例えば、悪用された脆弱性に関するデータ、最近のセキュリティ侵害、不適切な行為を行った可能性のあるユーザなどです。例えば、インシデントデータベースへのアクセスは、権限のある担当者のみが行うべきです。インシデント通信（電子メールなど）や文書は、権限を与えられた人員のみが読めるように、暗号化するか、その他の方法で保護されるべきです。

※１　インシデントハンドラーは、個人的な意見や結論ではなく、インシデントに関する事実のみを記録すべきです。主観的な材料は、証拠として記録されないように、インシデント報告書で提示されるべきです。

※２　ログブックを使用する場合は、製本し、インシデント担当者がページ番号を付け、ペン書きし、そのままにしておくことが望ましい（ページを切り取らないこと）。

※３　装置を使用する前に、装置で収集した証拠の許容性を検討してください。例えば、証拠となる可能性のある機器は、それ自体が他の証拠を記録するために使用すべきではありません。

※４　NISTSP800-86「インシデント対応にフォレンジック技術を統合するためのガイド」では、ポリシーと手順の策定を含むフォレンジック能力の確立に関する詳細な情報を提供しています。

※５　付録Ｂには、インシデントが報告される際に収集すべきデータ要素の推奨リストが記載されています。また、CERT®/CC文書「コンピュータ・セキュリティ・インシデント対応チーム（CSIRTs）の実践状況」には、いくつかのインシデント報告書式のサンプルが記載されています。この文書は、http://www.cert.org/archive/pdf/03tr001.pdf で入手可能です。

※6 Trans-European Research and Education Networking Association(TERENA)は、RFC3067、TERENA'sIncidentObjectDescriptionandExchangeFormatRequirements(http://www.ietf.org/rfc/rfc3067.txt)を開発しました。この文書は、各インシデントに対してどのような情報を収集すべきかについての推奨事項を提供しています。IETFExtendedIncidentHandling(inch)WorkingGroup(http://www.cert.org/ietf/inch/inch.html)は、TERENA の作業を拡張したRFC5070,IncidentObjectDescriptionExchangeFormat(http://www.ietf.org/rfc/rfc5070.txt)を作成しました。

3.2.6 インシデントの優先順位付け

インシデントの処理に優先順位をつけることは、おそらくインシデントハンドリングプロセスの中で最も重要な決定ポイントです。インシデントは、リソースの制限の結果、先着順で処理されるべきではありません。その代わり、以下のような関連する要因に基づいて優先的に処理を行うべきです。

■ インシデントの機能的影響

IT システムを標的としたインシデントは、通常、それらのシステムが提供するビジネス機能に影響を与え、その結果、それらのシステムのユーザに何らかのネガティブな影響を与えます。インシデントハンドラーは、インシデントが影響を受けるシステムの既存の機能にどのような影響を与えるかを考慮する必要があります。インシデントハンドラーは、インシデントの現在の機能的な影響だけでなく、インシデントがすぐに収束しない場合には、インシデントの将来的な機能的な影響も考慮する必要があります。

■ インシデントによる情報への影響

インシデントは、組織の情報の機密性、完全性、および可用性に影響を与える可能性があります。例えば、悪意のあるエージェントが機密情報を流出させることがあります。インシデント担当者は、この情報流出が組織の全体的なミッションにどのような影響を与えるかを考慮する必要があります。機密情報の流出につながるインシデントは、データのいずれかがパートナー組織に関係している場合、他の組織にも影響を及ぼす可能性があります。

■ インシデントからの復旧性

インシデントの規模と影響を受けるリソースの種類によって、インシデントからの復旧に費やさなければならない時間とリソースの量が決まります。インシデントからの復旧が不可能な場合もあり（例えば、機密情報の機密性が損なわれた場合など）、将来的に同様のインシデントが発生しないようにするための努力をしない限り、インシデント処理サイクルの長期化に限られたリソースを費やすことは意味がありません。他のケースでは、インシデントを処理するために、組織が利用できるリソースをはるかに上回るリソースを必要とする場合もあります。インシデント担当者は、インシデントから実際に回復するために必要な努力を検討し、回復努力が生み出す価値やインシデント処理に関連する要件と比較して慎重に検討すべきです。

組織のシステムへの機能的な影響と組織の情報への影響を組み合わせることで、インシデントのビジネスへの影響を決定します。-例えば、公開 Web サーバに対する DDoS 攻撃は、サーバにアクセスしようとするユーザの機能を一時的に低下させる可能性があり、公開 Web サーバへの不正なルートレベルのアクセスは、個人を特定できる情報（PII）を流出させる結果となり、組織の評判に長期的な影響を与える可能性があります。

インシデントからの復旧性は、インシデントに対処する際にチームが取り得る対応を決定します。機能的な影響が大きく、復旧にかかる労力が少ないインシデントは、チームが即座に対応するための理想的な候補となります。しかし、インシデントの中には、スムーズな回復経路を持たないものもあり、より戦略的レベルの対応が必要な場合もあります。-例えば、攻撃者がギガバイトの機密データを流出させて公開するようなインシデントが発生した場合、データはすでに公開されているため、簡単に復旧することはできません。この場合、チームは、データ流出インシデントへの対応の責任の一部をより戦略的レベルのチームに移すことができます。チームは、インシデントによって引き起こされたビジネスへの影響の推定値と、インシデントからの復旧に必要な推定努力に基づいて、各インシデントへの対応に優先順位をつけるべきです。

組織は、状況を認識しているため、自らのインシデントの影響を最もよく定量化することができます。表 3-2 は、組織が自社のインシデントの評価に使用することができる機能的影響のカテゴリーの例を示しています。インシデントを評価することは、限られたリソースに優先順位をつけるのに役立ちます。

表３－２機能的影響カテゴリー

カテゴリー	定　義
な　し	すべての利用者、サービス等組織の能力に影響を与えない
低	最小限の影響;組織はまだすべてのユーザにすべての重要なサービスを提供することができますが、効率性を失っています
中	組織はシステムユーザに重要なサービスを提供する能力を失っている
高	組織が利用者に重要なサービスを提供できなくなっている

表 3-3 は、インシデント中に発生した情報漏洩の程度を表す情報影響カテゴリーの例を示しています。この表では、「なし」の値を除いて、カテゴリーは相互に排他的ではなく、組織は複数のカテゴリーを選択することができます。

表３－３情報的影響カテゴリー

カテゴリー	定　義
な し	情報が流出、変更、削除されていないか、または他の方法で危険にさらされていない。
プライバシー侵害	納税者、従業員、受益者等の機密性の高い個人情報（PII）へのアクセスや流出
専有情報の流出	保護された重要インフラ情報(PCII)などの未分類の専有情報へのアクセスまたは流出
完全流出	機密情報や専有情報が変更または削除された

表 3-4 は、インシデントからの復旧に必要なリソースのレベルと種類を反映した復旧作業カテゴリーの例を示しています。

表 3-4 復旧作業カテゴリー

カテゴリー	定　義
通　常	復旧までの時間は、既存のリソースで予測可能
補　完	リソースを追加することで回復までの時間が予測可能
拡　張	回復までの時間が予測できないため、追加のリソースと外部からの支援が必要
回復不可能	・インシデントからの復旧が不可能（例：機密データが流出して公開された）。 ・調査の開始

また、組織は、チームが指定された時間内にインシデントに対応しない場合のために、エスカレーションプロセスを確立すべきです。これは様々な理由で起こりえます。例えば、携帯電話が故障したり、個人的な緊急事態が発生した場合などである。エスカレーションプロセスでは、回答が得られるまでの時間と、回答が得られなかった場合の対処法を説明する必要があります。一般的に、最初のステップは、同じ携帯電話番号にかけ直すなど、最初の連絡を繰り返すことです。短い時間

（おそらく 15 分）待った後、通報者は、インシデント対応チームのマネージャーなど、より高いレベルにインシデントをエスカレーションする必要があります。その担当者が一定時間内に応答しない場合は、インシデントをより高いレベルの管理者に再度エスカレーションする必要があります。誰かが応答するまで、このプロセスを繰り返すべきです。

3.2.7 インシデントの通知

インシデントが分析され、優先順位が付けられたとき、インシデント対応チームは、関与する必要のあるすべての人がそれぞれの役割を果たすように、適切な個人に通知する必要があります。インシデント対応方針には、最低でも、誰に何を、どのようなタイミングで報告しなければならないか（最初の通知、定期的な状況の更新など）、インシデント報告に関する規定が含まれているべきです。正確な報告要件は組織によって異なりますが、一般的に通知される当事者は以下の通りです。

- CIO
- 情報セキュリティ責任者
- 地域情報セキュリティ担当者
- 組織内の他のインシデント対応チーム
- 外部のインシデント対応チーム（必要に応じて
- システムの所有者
- 人事（メールでのハラスメントなど、従業員が関わる案件の場合
- 広報（宣伝の可能性があるインシデントの場合
- 法務部（法的に影響を及ぼす可能性のあるインシデントの場合
- US-CERT（連邦政府に代わって運営される連邦政府機関およびシステムに必要
- 法執行機関（適切な場合

インシデント処理中、チームは特定の関係者、場合によっては組織全体にも状況報告を行う必要があるかもしれません。チームは、帯域外の方法（対面、紙など）を含むいくつかのコミュニケーション方法を計画し、準備し、特定のインシデントに適した方法を選択する必要があります。考えられるコミュニケーション方法としては、以下のようなものがあります。

- 電子メール
- ウェブサイト（内部・外部、ポータル
- 電話

■ 対面での説明会（毎日のブリーフィングなど
■ 音声メールボックスのグリーティング（例：インシデント更新用に別の音声メールボックスを設定し、グリーティングメッセージを更新して現在のインシデントの状況を反映させる。ヘルプデスクの音声メールグリーティングを使用する
■ 紙媒体（掲示板やドアへの掲示、玄関先での配布など）

3.3 封じ込め・根絶・復旧

3.3.1 封じ込め戦略の選択

インシデントがリソースを圧倒したり、被害が拡大したりする前に、封じ込めが重要です。ほとんどのインシデントでは封じ込めが必要であるため、各インシデントへの対応の初期段階では、封じ込めは重要な検討事項です。封じ込めを行うことで、個別に対応した修復戦略を策定する時間を確保することができます。封じ込めの本質的な部分は、意思決定(システムをシャットダウンする、ネットワークから切断する、特定の機能を無効にするなど)です。インシデントを封じ込めるための事前の戦略と手順があれば、そのような決定ははるかに容易になります。組織は、インシデントに対処する際の許容可能なリスクを定義し、それに応じて戦略を策定すべきです。

封じ込め戦略は、インシデントの種類によって異なります。例えば、電子メールを媒介とするマルウェア感染を封じ込める戦略は、ネットワークベースの DDoS 攻撃とは大きく異なります。組織は、主要なインシデントの種類ごとに個別の封じ込め戦略を作成し、意思決定を容易にするために基準を明確に文書化する必要があります。適切な戦略を決定するための基準には、以下のようなものがあります。

■ 資源への被害・盗難の可能性
■ 証拠保全の必要性
■ サービスの可用性（ネットワーク接続性、外部に提供されるサービスなど
■ 戦略を実行するために必要な時間とリソース
■ 戦略の有効性（例：部分的封じ込め、完全封じ込め
■ 解決策の期間（例：緊急回避策は 4 時間以内に削除する、一時的な回避策は 2 週間以内に削除する、恒久的な解決策）

場合によっては、攻撃者の活動を監視できるように、攻撃者をサンドボックス（封じ込めの一形態）にリダイレクトして、通常は追加の証拠を収集する組織もあります。インシデント対応チーム

は、この戦略が実行可能かどうかを判断するために、法務部門と話し合うべきです。サンドボックス以外の攻撃者の活動を監視する方法は、使用すべきではありません。システムが侵害されたことを知っている組織が、侵害の継続を許した場合、攻撃者が侵害されたシステムを使って他のシステムを攻撃した場合、組織は責任を負うことになるかもしれません。攻撃者が不正アクセスをエスカレートさせたり、他のシステムを侵害したりする可能性があるため、封じ込め戦略の遅延は危険です。

封じ込めに関するもう一つの潜在的な問題は、一部の攻撃が封じ込められた場合に追加の損害を引き起こす可能性があることです。例えば、侵害されたホストが悪意のあるプロセスを実行して、他のホストに定期的に ping を打つことがあります。インシデントハンドラーが侵害されたホストをネットワークから切断することでインシデントを封じ込めようとすると、その後の ping は失敗します。失敗の結果、悪意のあるプロセスがホストのハードドライブ上のすべてのデータを上書きしたり、暗号化したりする可能性があります。ハンドラーは、ホストがネットワークから切断されたからといって、ホストへのさらなる被害が防止されたと思い込んではいけません。

3.3.2 証拠の収集と処理

インシデント中に証拠を収集する主な理由は、インシデントを解決することですが、法的手続きのために必要な場合もあります※１。そのような場合には、漏洩したシステムを含むすべての証拠がどのように保存されたかを明確に文書化することが重要です※２。証拠は、あらゆる証拠が法廷で認められるように、法務担当者や適切な法執行機関との以前の話し合いで策定された、適用されるすべての法規制を満たす手順にしたがって収集されるべきです※３。さらに、証拠は常に説明されるべきである。証拠が人から人へ移されるときはいつでも、書類・証拠受け渡し記録は移された内容を詳述し、各当事者の署名を含めるべきです。以下を含むすべての証拠について、詳細な記録を残すべきです。

- 識別情報（例：場所、シリアル番号、モデル番号、ホスト名、メディアアクセス制御（MAC）アドレス、コンピュータの IP アドレスなど
- 調査中に証拠を収集した、または取り扱った各個人の氏名、肩書き、電話番号
- 証拠処理の各発生日時（時間帯を含む
- 証拠が保管されていた場所

コンピューティングリソースから証拠を収集することには、いくつかの課題があります。一般的には、インシデントが発生した可能性があると疑われたらすぐに、対象となるシステムから証拠を取

得することが望ましいです。多くのインシデントは、動的なイベントの連鎖を引き起こします。初期のシステムスナップショットは、問題とその原因を特定する上で、この段階で実行できる他のほとんどのアクションよりも効果があるかもしれません。証拠の観点からは、インシデントハンドラーやシステム管理者などが調査中に不注意でマシンの状態を変更してしまった後に行うよりも、そのままの状態でシステムのスナップショットを取得する方がはるかに良いでしょう。ユーザとシステム管理者は、証拠を保存するために取るべき手順を認識しておく必要があります。証拠保全に関する追加情報については、NISTSP800-86『Guide to Integrating Forensic Techniques into Incident Response』を参照してください。

※1 NISTSP800-86「インシデント対応へのフォレンジック技法の統合に関するガイド」は、フォレンジック能力の確立に関する詳細な情報を提供しています。PC のフォレンジック技術に焦点を当てていますが、資料の多くは他のシステムにも適用可能です。この文書は http://csrc.nist.gov/publications/PubsSPs.html#800-86 でご覧いただけます。

※2 証拠の収集と処理は、通常、発生したすべてのインシデントに対して行われるわけではありません（例えば、ほとんどのマルウェアのインシデントでは、証拠を収集する必要はありません）。多くの組織では、ほとんどのインシデントに対してデジタルフォレンジックは必要ありません。

※3 司法省コンピュータ犯罪・知的財産課（CCIPS）の「犯罪捜査におけるコンピュータの捜索・押収と電子証拠の入手」は、証拠収集に関する法的ガイダンスを提供しています。この文書は http://www.cybercrime.gov/ssmanual/index.html で入手可能です。

3.3.3 攻撃ホストの特定

インシデント処理の間、システム所有者やその他の人は、攻撃している（単数あるいは複数の）ホストを特定したい、または特定する必要があることがあります。この情報は重要な場合もありますが、インシデント処理担当者は一般的に、封じ込め、根絶、回復に集中すべきです。攻撃してくるホストを特定することは、時間のかかる無駄なプロセスであり、チームの主要な目標であるビジネスへの影響を最小化することを妨げる可能性があります。以下の項目では、攻撃ホストの特定のために最も一般的に行われる活動について説明します。

■ 攻撃ホストの IP アドレスを検証する

新しいインシデントハンドラーは、攻撃ホストの IP アドレスに焦点を当てることが多いです。ハンドラーは、そのアドレスへの接続性を検証することで、そのアドレスが偽装されていないことを検証しようとするかもしれません。しかし、これは単にそのアドレスのホストがリクエストに応答するかしないかを示しているだけです。応答しないということは、そのアドレスが実在しないということを意味するわけではありません。また、攻撃者が既に他の誰かに再割り当てされたダイナミックアドレスを受信している可能性もあります。

■ 検索エンジンを使って攻撃するホストを調査する

検索エンジンを利用した攻撃ホストの調査攻撃の発信元と思われる IP アドレスを使ってインターネット検索を行うと、攻撃に関するより多くの情報（例えば、類似の攻撃に関するメーリングリストのメッセージなど）が得られる可能性があります。

■ インシデントデータベースの利用

インシデントデータベースの利用。複数のグループが、さまざまな組織からインシデントデータを収集し、整備しています。この情報共有は、トラッカーやリアルタイムのブラックリストなど、さまざまな形で行われます。また、組織は、独自のナレッジベースや問題追跡システムをチェックして、関連する活動を確認することもできます。

■ 攻撃者の可能性のある通信チャネルの監視インシデントハンドラーは、攻撃するホストが使用する可能性のある通信チャネルを監視することができます。例えば、多くのボットは IRC を主な通信手段として使用しています。また、攻撃者は特定の IRC チャンネルに集まって、自分たちの危殆化した状況を自慢したり、情報を共有したりすることもあります。しかし、インシデントハンドラーは、そのような情報を入手しても、事実としてではなく、潜在的な手がかりとしてのみ扱うべきです。

3.3.4 根絶と回復

インシデントが収束した後、マルウェアの削除や破られたユーザカウントの無効化など、インシデントの構成要素を排除するために根絶が必要になる場合がありますが、悪用されたすべての脆弱性を特定して緩和することもできます。根絶の際には、組織内の影響を受けるすべてのホストを特定

し、それらを修復できるようにすることが重要です。インシデントによっては、根絶が必要ない場合もあれば、回復の最中に実行される場合もあります。

回復では、管理者はシステムを正常な動作に戻し、システムが正常に機能していることを確認し、（該当する場合には）脆弱性を修正して同様のインシデントを防止します。回復には、クリーンなバックアップからのシステムの復元、ゼロからのシステムの再構築、感染したファイルのクリーンなバージョンへの置き換え、パッチのインストール、パスワードの変更、ネットワークの境界セキュリティの強化（例：ファイアウォールのルールセット、境界ルータのアクセス制御リスト）などのアクションが含まれる場合があります。より高度なレベルのシステムロギングやネットワーク監視は、回復プロセスの一部であることが多いです。一度攻撃に成功すると、リソースが再び攻撃されたり、組織内の他のリソースが同様の方法で攻撃されたりすることがよくあります。

根絶と回復は、修復手順に優先順位が付けられるように、段階的なアプローチで行う必要があります。大規模なインシデントの場合、回復には数か月かかることもあります。初期の段階では、将来のインシデントを防ぐために、比較的迅速（数日から数週間）に価値の高い変更を行い、全体的なセキュリティを向上させることを目的とすべきです。後の段階では、長期的な変更（インフラの変更など）と、企業のセキュリティを可能な限り維持するための継続的な作業に焦点を当てるべきです。

根絶と回復のためのアクションは、一般的に OS やアプリケーション固有のものであるため、それらに関する詳細な推奨事項やアドバイスは、本書の範疇外です。

3.4 インシデント後の活動

3.4.1 教訓

インシデント対応の最も重要な部分の 1 つは、最も省略されがちな「学習と改善」でもあります。各インシデント対応チームは、新しい脅威、改善された技術、および学んだ教訓を反映させるために進化しなければなりません。重大なインシデントの後や、リソースが許す限り定期的に小さなインシデントの後に、すべての関係者との「学んだ教訓」会議を開催することは、セキュリティ対策とインシデント処理プロセス自体を改善する上でとても有効です。また複数のインシデントを 1 回の教訓会議でカバーすることができます。この会議では、何が発生したのか、何が介入のために行われたのか、介入がどの程度うまくいったのかを見直すことで、インシデントに関してクローズす

る機会を提供します。会議は、インシデント終了後数日以内に開催されるべきです。会議で回答すべき質問には、以下のようなものがあります。

- 正確に何が、どのようなタイミングで起こったのか ？
- スタッフと管理者は、インシデントに対処する上でどの程度うまくいったか ?文書化された手順は守られていたか ?それらは適切だったか ？
- どのような情報がもっと早く必要だったか ？
- 復旧を阻害するような措置や行動が取られていなかったか ？
- 次回同様のインシデントが発生した場合スタッフと管理者は何か違ったことをするだろうか ？
- 他の組織との情報共有はどのように改善されたか ？
- どのような是正措置を取れば、将来、同様のインシデントを防ぐことができるか ？
- 同様のインシデントを検出するために、将来的にどのような前兆や兆候に注意すべきか ？
- 将来のインシデントを検出、分析、および軽減するために、どのような追加ツールまたはリソースが必要か ？

小規模なインシデントでは、広く懸念され関心を集めている新しい攻撃方法によって実行されたインシデントを除けば、インシデント後の分析は限定的になります。深刻な攻撃が発生した後は、通常、情報共有のためのメカニズムを提供するために、チームや組織の境界を越えて事後分析会議を開催する価値があります。このような会議を開催する際に最も重要なことは、適切な人材を確保することです。分析対象となるインシデントに関わった人を招くことが重要であるだけでなく、今後の協力関係を円滑にするためにも、誰を招くべきかを考えておくことが賢明です。

このような会議が成功するかどうかは、議題にもよります。会議の前に参加者から期待やニーズについての意見を収集しておくことで、参加者のニーズが満たされる可能性が高まります。さらに、会議の開始前または開始中に会議規則を確立することで、混乱や不和を最小限に抑えることができます。グループのファシリテーションに習熟したモデレーターを 1人または複数人配置することで、高い効果を得ることができます。最後に、合意の主なポイントと行動項目を文書化し、会議に出席できなかった当事者に伝えることも重要です。

教訓を学んだ会議は他の利点を提供します。これらの会議からの報告は、経験豊富なチームメンバーがどのようにインシデントに対応しているかを示すことで、新しいチームメンバーをトレーニン

グするための良い材料となります。インシデント対応の方針と手順を更新することも、教訓を得たプロセスの重要な部分です。インシデントが処理された方法の事後分析を行うと、多くの場合、手順に欠けていたステップや不正確さが明らかになり、変更のきっかけとなります。情報技術の性質の変化や人員の変化のため、インシデント対応チームは、指定された間隔で、インシデントを処理するためのすべての関連文書と手順を見直すべきです。

もう一つの重要なインシデント後の活動は、各インシデントのフォローアップ報告書を作成することです。報告書は、類似のインシデントへの対応を支援するための参考資料となります。イベントの正式な時系列（システムからのログデータなどのタイムスタンプ付き情報を含む）を作成することは、インシデントが引き起こした損害額の推定金額を作成することと同様に、法的な理由から重要です。この推定値は、米国司法長官室のような組織によるその後の起訴活動の基礎となる可能性があります。フォローアップ報告書は、記録保持方針に規定されているように、一定期間保存されるべきです※１。

※１ 一般記録スケジュール（GRS）24「情報技術の運用管理記録」では、"コンピュータセキュリティインシデントの処理、報告、およびフォローアップ記録"は、"必要なすべてのフォローアップ措置が完了してから 3 年後に破棄されるべきである"と規定されています。GRS24 は、国立公文書館記録局（http://www.archives.gov/records-mgmt/grs/grs24.html）から入手可能です。

3.4.2 収集したインシデントデータの利用

学んだ教訓は、各インシデントに関する客観的なデータと主観的なデータのセットを作成すべきです。時間の経過とともに、収集されたインシデントデータは、いくつかの点で有用なものとなるはずです。データ、特に関与した総時間とコストは、インシデント対応チームの追加資金を正当化するために使用できます。インシデントの特性を調査することで、システム的なセキュリティの弱点や脅威、インシデントの傾向の変化を示すことができます。このデータは、リスク評価プロセスに戻され、最終的には追加の対策の選択と実施につながります。データのもう一つの有効な利用法は、インシデント対応チームの成功度を測定することです。インシデントデータが適切に収集され、保存されていれば、インシデント対応チームの成功（または少なくとも活動）のいくつかの尺度が得られるはずです。また、インシデントデータを収集して、インシデント対応能力の変更がチームのパフォーマンスに対応する変化をもたらすかどうかを判断することもできます（例：効率性の向上、コストの削減）。さらに、インシデント情報の報告を要求される組織は、要求事項を満た

すために必要なデータを収集する必要があります。他の組織とのインシデントデータの共有に関する追加情報については、セクション 4 を参照してください。

組織は、単にデータが入手可能だからといってデータを収集するのではなく、実行可能なデータを収集することに焦点を当てるべきです。例えば、毎週発生する前兆となるポートスキャンの数を数え、年末にポートスキャンが 8%増加したことを示すチャートを作成することは、あまり参考にならず、非常に時間のかかることになります。絶対的な数字だけでは、組織のビジネスプロセスに対する脅威をどのように表しているかを理解することが重要です。組織は、報告要件とデータから期待される投資収益率（例えば、新しい脅威を特定し、それらが悪用される前に関連する脆弱性を緩和すること）に基づいて、どのようなインシデントデータを収集するかを決定する必要があります。インシデント関連データの測定基準としては、以下のようなものが考えられます。

■ 対応したインシデントの数※ 1

例えば、対応したインシデント数は、インシデント対応チームの過失ではなく、ネットワークやホストのセキュリティ管理が改善されたために減少する場合があります。処理されたインシデント数は、インシデント対応チームが実行しなければならなかった作業の相対的な量を測るものであって、チームの品質を測るものではないと考えるのが最善です。各インシデントカテゴリーごとに別々のインシデントカウントを作成する方がより効果的です。また、より多くの情報を提供するためにサブカテゴリーを使用することもできます。例えば、インサイダーによって実行されるインシデントの数が増加していることから、人員の身元調査やコンピューティングリソースの不正使用に関するポリシーの規定を強化したり、内部ネットワークのセキュリティ管理を強化したりすることができます（例えば、より多くの内部ネットワークやホストに侵入検知ソフトウェアを配備するなど)。

※ 1 扱われたインシデントの数などの指標は、一般的に、複数の組織を比較する際には価値がありません。例えば、ほとんどの組織では、「インシデント」を独自のポリシーと実践の観点から定義しており、ある組織では単一のインシデントと見なしていたものが、他の組織では複数のインシデントと見なしている場合があります。また、ポートスキャンの数など、より具体的な指標も、組織の比較においてはほとんど価値がありません。例えば、ネットワーク侵入検知センサーなどの異なるセキュリティシステムが、ポートスキャンとしての活動をラベル付けする際に、すべて同じ基準を使用する可能性は非常に低いと考えられます。

■ インシデントあたりの時間

各インシデントについて、時間はいくつかの方法で測定することができます。

- インシデントの作業に費やされた労働力の総量
- インシデントの開始からインシデントの発見、最初の影響評価、およびインシデント処理プロセスの各段階（封じ込め、回復など）までの経過時間
- インシデント対応チームがインシデントの初動報告に対応するまでに要した時間
- 管理者への報告、および必要に応じて適切な外部団体（US-CERT など）への報告にどのくらいの期間を要したか。

■ 各インシデントの客観的な評価

- 解決したインシデントへの対応を分析することで、それがどれだけ効果的であったかを判断することができます。以下は、インシデントの客観的な評価を行う例です。
- 確立されたインシデント対応方針および手順に準拠しているかどうか、ログ、記録用紙、報告書、およびその他のインシデント文書をレビューする。
- インシデントのどの前兆と兆候が記録されたかを特定し、インシデントがどれだけ効果的に記録され、特定されたかを判断する。
- インシデントが発覚する前に被害が発生したかどうかの判断
- インシデントの実際の原因が特定されたかどうかを判断し、攻撃の方向性、悪用された脆弱性、標的または被害を受けたシステム、ネットワーク、およびアプリケーションの特徴を特定する。
- インシデントが以前のインシデントの再発であるかどうかの判断
- インシデントによる推定金銭的損害の計算（インシデントによって悪影響を受けた情報や重要なビジネスプロセスなど）
- 最初の影響評価と最終的な影響評価との差の測定（3.2.6 項参照
- どのような対策があれば、インシデントを防ぐことができたかを特定すること。

■ 各インシデントの主観的評価

インシデント対応チームのメンバーは、自分のパフォーマンスだけでなく、他のチームメンバーやチーム全体のパフォーマンスの評価を求められることがあります。もう一つの貴重な情報源は、攻撃を受けたリソースの所有者であり、その所有者がインシデントが効率的に処理されたと考えているかどうか、またその結果が満足のいくものであったかどうかを判断するためです。

チームの成功を測定するためにこれらの測定基準を使用するだけでなく、組織は定期的にインシデント対応プログラムを監査することも有用であると考えられます。監査は、問題や欠陥を特定し、それを修正することができます。最低限、インシデント対応監査では、以下の項目を適用される規則、方針、および一般に認められた慣行に照らして評価する必要があります。

■ インシデント対応の方針、計画、および手順
■ ツールとリソース
■ チームモデルと構造
■ インシデントハンドラーの訓練と教育
■ インシデント文書と報告書
■ このセクションで先に説明した成功の尺度

3.4.3 証拠の保持

組織は、インシデントからの証拠をどのくらいの期間保持すべきかについての方針を確立すべきです。ほとんどの組織は、インシデントが終了した後、すべての証拠を数か月または数年の間保持することを選択しています。方針を作成する際には、以下の要因を考慮すべきです。

■ 起　訴

攻撃者が起訴される可能性がある場合、すべての法的措置が完了するまで証拠を保持する必要がある場合があります。場合によっては、数年かかることもあります。さらに、今は取るに足らないと思われる証拠が、将来的にはより重要になる可能性があります。例えば、攻撃者が 1 回の攻撃で収集した情報を使って、後になってより深刻な攻撃を行うことができた場合、最初の攻撃の証拠が、2 回目の攻撃がどのようにして行われたかを説明する鍵となる可能性があります。

■ データの保持

ほとんどの組織は、特定の種類のデータをどのくらいの期間保存するかを規定したデータ保持ポリシーがあります。例えば、ある組織では、電子メールのメッセージは 180日間しか保持しないように規定しているかもしれません。ディスクイメージに数千通の電子メールが含まれている場合、組織は絶対に必要な場合を除き、そのイメージを 180日間以上保持することを望ま

ないかもしれません。セクション 3.4.2 で議論されているように、一般記録スケジュール (GRS)24 では、インシデント処理記録は 3 年間保存されるべきであると規定されています。

■ コスト

証拠として保管されるオリジナルのハードウェア（例えば、ハードドライブ、漏洩したシステム)、及びディスクイメージを保持するために使用されるハードドライブやリムーバブルメディアは、一般的に個々に安価ではありますが、組織がこのようなコンポーネントを何年にもわたって多数保管している場合、そのコストは多額になる可能性があります。また組織は、保存されたハードウェアやメディアを使用できるコンピュータを保持しておく必要があります。

3.5 インシデントハンドリングチェックリスト

表 3-5 のチェックリストには、インシデントの処理において実行すべき主なステップが記載されています。実際に実行されるステップは、インシデントの種類や個々のインシデントの性質に基づいて異なる場合があることに注意してください。例えば、ハンドラーが兆候の分析に基づいて何が起こったかを正確に知っている場合（ステップ 1.1)、活動をさらに調査するためにステップ 1.2 または 1.3 を実行する必要はないかもしれません。このチェックリストは、ハンドラーが実行すべき主なステップについてのガイドラインを提供するものであり、常に従わなければならないステップの正確な順序を指示するものではありません。

図 3-5 インシデントハンドリングチェックリスト

	行　動	チェック
検知と分析		
1．インシデントが発生したかどうかを判断する		
1.1	前兆と兆候を分析する	
1.2	関連する情報を探す	
1.3	調査の実施（検索エンジン、ナレッジデータベースなど）	
1.4	ハンドラーは、インシデントが発生したと確信したらすぐに調査の文書化と証拠の収集を開始	
2.　関連する要因（機能的影響、情報的影響、復旧努力など）に基づいて、インシデントへの対応に優先順位をつける。		
3.　社内の適切な担当者および外部組織に報告する。		
封じ込め、根絶、復旧		
4.　証拠の取得、保存、確保、文書化		
5.　インシデントの封じ込め		
6.　インシデントの根絶		
6.1	悪用されたすべての脆弱性を特定し、軽減する	
6.2	マルウェアや不適切な素材などを除去する	
6.3	より多くの影響を受けるホストが発見された場合(新しいマルウェア感染など)、検出と分析のステップ(1.1,1.2)を繰り返して、他の影響を受けるすべてのホストを特定し、(5)のインシデントを封じ込め、(6)のインシデントを根絶してください。	
7.　インシデントからの復旧		
7.1	影響を受けたシステムを動作可能な状態に戻す	
7.2	影響を受けたシステムが正常に機能していることを確認する	
7.3	必要に応じて、将来の関連活動を探すために追加のモニタリングを実施する。	
インシデント後の活動		
8.　フォローアップレポートの作成		
9.　教訓会議の開催（重大インシデントの場合は必須、それ以外の場合は任意）		

3.6 推奨事項

このセクションでは、インシデントの処理に関する重要な推奨事項を以下にまとめています。

■　インシデント処理中に価値がありそうなツールやリソースを入手する。チームは、さまざまなツールやリソースがすでに利用可能であれば、インシデントの処理をより効率的に行うことができます。例としては、連絡先リスト、暗号化ソフトウェア、ネットワーク図、バックアップデバイス、デジタルフォレンジックソフトウェア、ポートリストなどが挙げられます。

■ ネットワーク、システム、およびアプリケーションの安全性を十分に確保することで、インシデントの発生を防止する。インシデントを防止することは、組織にとって有益なことであり、インシデント対応チームの作業負荷を軽減することにもつながります。定期的なリスク評価を実施し、特定されたリスクを許容可能なレベルまで低減することは、インシデントの数を減らす上で効果的です。また、ユーザ、IT スタッフ、管理者によるセキュリティポリシーと手順の認識も非常に重要です。

■ 複数のタイプのセキュリティソフトウェアによって生成されたアラートを使用し、前兆や兆候を特定する。インシデントの兆候を検出するためには、侵入検知および防止システム、ウィルス対策ソフトウェア、およびファイルの整合性をチェックするソフトウェアが有効です。各タイプのソフトウェアは、他のタイプのソフトウェアでは検出できないインシデントを検出できる可能性があるため、複数のタイプのコンピュータ・セキュリティ・ソフトウェアの使用を強く推奨します。また、第三者による監視サービスも有効です。

■ 外部からインシデントを報告するための仕組みを確立する。外部の関係者は、組織にインシデントを報告したいと思うかもしれません。例えば、組織のユーザの一人が組織を攻撃していると考えているかもしれません。組織は、外部の者がそのようなインシデントを報告するために使用できる電話番号と電子メールアドレスを公表すべきです。

■ すべてのシステムで基準レベルのログ収集と監査を行い、すべての重要なシステムではより高い基準レベルを要求する。OS、サービス、およびアプリケーションからのログは、特に監査が有効になっている場合には、インシデント分析の間に価値を提供することがよくあります。ログは、どのアカウントにアクセスしたか、どのようなアクションが実行されたかなどの情報を提供することができます。

■ ネットワークとシステムのプロファイリングプロファイリングは、予想されるアクティビティレベルの特性を測定することで、パターンの変化をより簡単に特定できるようにします。プロファイリング・プロセスが自動化されていれば、予想されるアクティビティレベルからの逸脱を迅速に検出して管理者に報告することができ、インシデントや運用上の問題をより迅速に検出することができます。

■ ネットワーク、システム、およびアプリケーションの正常な動作を理解する。正常な動作を理解しているチームメンバーは、異常な動作をより簡単に認識することができます。この知識は、ログエントリやセキュリティアラートを確認することで得られます。この知識は、ログエントリやセキュリティアラートを確認することで得られます。ハンドラーは、典型的なデータに精通し、異常なエントリを調査してより多くの知識を得ることができます。

■ ログ保持ポリシーを作成する。インシデントに関する情報は、いくつかの場所に記録される可能性があります。ログデータをどのくらいの期間維持するかを指定するログ保持ポリシーを作成して実装すると、古いログエントリには、偵察活動や類似の攻撃の以前のインスタンスが示されている可能性があるため、分析に非常に役立つ場合があります。

■ イベントの相関関係を実行する。インシデントの証拠が複数のログに記録されている場合があります。複数のソース間でイベントを相関させることは、インシデントのために利用可能なすべての情報を収集し、インシデントが発生したかどうかを検証する上で非常に重要です。

■ すべてのホストクロックを同期させる。イベントを報告するデバイスのクロック設定が一貫していない場合、イベントの相関関係はより複雑になります。クロックの不一致は、証拠の観点からも問題を引き起こす可能性があります。

■ 情報のナレッジデータベースを維持し、使用する。ハンドラーは、インシデント分析中に情報を素早く参照する必要があります。一元化されたナレッジデータベースは、一貫性があり、維持可能な情報源を提供します。ナレッジデータベースには、過去のインシデントの前兆や兆候に関するデータなどの一般的な情報が含まれている必要があります。

■ チームがインシデントが発生したと疑ったら、すぐにすべての情報の記録を開始する。インシデントが検出されてから最終的に解決するまでのすべてのステップを文書化し、タイムスタンプを付けます。このような性質の情報は、法的訴追が行われた場合、法廷での証拠となることがあります。また、実行された手順を記録することで、より効率的で体系的で、エラーが発生しにくい問題処理につながります。

■ インシデントデータを保護する。インシデントデータには、脆弱性、セキュリティ侵害、不適切な行為を行った可能性のあるユーザなどの機密情報が含まれていることがよくあります。チ

ームは、インシデントデータへのアクセスが、論理的にも物理的にも適切に制限されていることを確認する必要があります。

■ 関連する要因に基づいて、インシデントの処理に優先順位をつける。リソースの制限があるため、インシデントは、先着順で処理すべきではありません。その代わりに、組織は、インシデントの機能的および情報への影響、インシデントからの回復可能性などの関連要因に基づいて、チームがインシデントにどの程度迅速に対応しなければならないか、どのようなアクションを実行すべきかを概説する文書化されたガイドラインを確立する必要があります。これにより、インシデント担当者の時間を節約し、管理者やシステム所有者に自分たちの行動を正当化する根拠を提供することができます。また、組織は、チームが指定された時間内にインシデントに対応しない場合のために、エスカレーションプロセスを確立するべきです。

■ 組織のインシデント対応方針にインシデント報告に関する規定を含める。組織は、どのインシデントを報告しなければならないか、いつ報告しなければならないか、誰に報告しなければならないかを明記しなければなりません。最も一般的に通知される関係者は、CIO、情報セキュリティ責任者、地域の情報セキュリティ担当者、組織内の他のインシデント対応チーム、およびシステム所有者です。

■ インシデントを封じ込めるための戦略と手順を確立する。インシデントを迅速かつ効果的に封じ込め、ビジネスへの影響を最小限に抑えることが重要です。組織は、インシデントを封じ込めるための許容可能なリスクを定義し、それに応じた戦略と手順を策定する必要があります。封じ込め戦略は、インシデントの種類に応じて異なるべきです。

■ 証拠の収集と処理のために確立された手順に従う。チームは、すべての証拠がどのように保存されたかを明確に文書化すべきです。証拠には常に詳細な記述・説明が添付されるべきです。チームは、法務スタッフや法執行機関と会合を持ち、証拠の取り扱いについて話し合い、それに基づいた手順を策定するべきです。

■ システムから揮発性のあるデータを証拠として収集する。これには、ネットワーク接続、プロセス、ログインセッション、開いているファイル、ネットワークインターフェースの構成、およびメモリの内容のリストが含まれます。信頼できるメディアから慎重に選択したコマンドを実行することで、システムの証拠を損なうことなく必要な情報を収集することができます。

■ ファイルシステムのバックアップではなく、完全なフォレンジックディスクイメージを使用してシステムのスナップショットを取得する。ディスクイメージは、サニタイズされた書き込み保護可能なメディアまたは書き込み可能なメディアで作成する必要があります。このプロセスは、調査や証拠保全の目的では、ファイルシステムのバックアップよりも優れています。また、元のシステムを分析するよりも、イメージを分析した方が、元のシステムを不注意で変更してしまう可能性があるため、イメージを分析する方がはるかに安全であるという点でも、イメージ分析は価値があります。

■ 重大なインシデントの後に教訓会議を開催する。教訓会議は、セキュリティ対策やインシデント対応プロセスそのものの改善に非常に役立ちます。

4. 連携と情報共有

現代の脅威や攻撃の性質から、インシデント対応中に組織が協力して取り組むことが、これまで以上に重要になってきています。組織は、インシデント対応活動の一部を適切なパートナーと効果的に調整するようにしなければなりません。インシデント対応における連携の最も重要な側面は情報共有であり、異なる組織が脅威、攻撃、および脆弱性の情報を相互に共有することで、各組織の知識が他の組織に利益をもたらすようにします。インシデント情報の共有は、同じ脅威や攻撃が複数の組織に同時に影響を与えることが多いため、相互に利益をもたらすことが多いです。

セクション 2 で述べたように、パートナー組織と情報を調整して共有することで、IT インシデントに効果的に対応する組織の能力を強化することができます。例えば、組織がネットワーク上で不審と思われる行動を特定し、そのイベントに関する情報を信頼できるパートナーに送信した場合、そのネットワーク内の他の誰かがすでに同様の行動を見ている可能性があり、シグネチャ、検索すべき他の指標、または是正措置の提案など、不審な行動に関する追加の詳細情報を提供して対応することができます。信頼できるパートナーとの連携により、組織は孤立して活動するよりも迅速かつ効率的にインシデントに対応することができます。

標準的なインシデント対応技術の効率性の向上だけが、組織間の連携と情報共有の唯一のインセンティブではありません。情報共有のもう一つのインセンティブは、特にその組織が中小規模の場合、単一の組織では利用できないかもしれない技術を使ってインシデントに対応できることです。例えば、小規模な組織がネットワーク上で特に複雑なマルウェアのインスタンスを特定した場合、マルウェアを完全に分析してシステムへの影響を判断するための社内リソースを持っていない可能性があります。この場合、組織は信頼できる情報共有ネットワークを活用して、マルウェアの分析を実行するのに十分な技術力を持つサードパーティのリソースに、このマルウェアの分析を効果的に外注することができるかもしれません。

このセクションでは、連携と情報共有に焦点を当てます。セクション 4.1 では、インシデント対応の連携の概要を示し、組織のインシデント対応プロセスを補完するための組織横断的な調整の必要性に焦点を当てています。第 4.2 節では、組織間で情報を共有するための技術について議論し、セクション 4.3 では、どのような情報を他の組織と共有するか、あるいは共有しないかをどのように制限するかを検討しています。

4.1 連　携

セクション 2.3.4 で議論されているように、組織は、インシデント対応活動を実施する過程で、いくつかのタイプの外部組織と相互作用する必要があるかもしれません。これらの組織の例としては、他のインシデント対応チーム、法執行機関、インターネットサービスプロバイダ、構成員及び顧客が挙げられます。組織の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、これらの関係者とのインシデント連携を計画し、すべての関係者がそれぞれの役割を理解し、効果的なコミュニケーションラインを確立する必要があります。図 4-1 は、インシデント対応のライフサイクルの各段階で連携を行っている組織の例を示しており、連携がライフサイクル全体を通して価値あるものであることを強調しています。

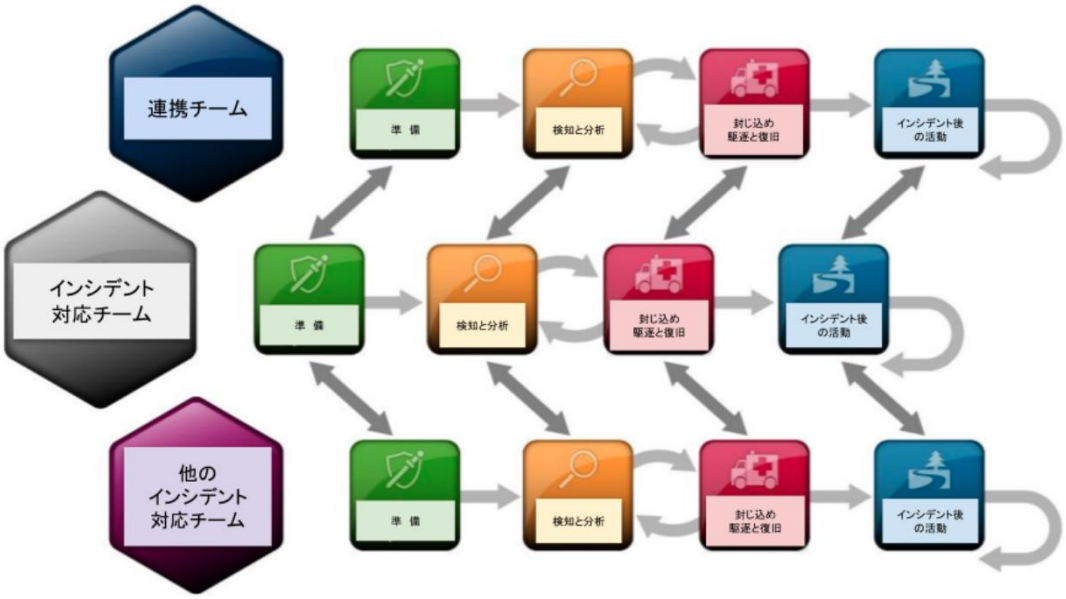

図 4-1 インシデント対応における連携

4.1.1 連携の関係

組織内のインシデント対応チームは、調整する組織の種類に応じて、さまざまなタイプの調整に参加することができます。例えば、インシデント対応の技術的詳細を担当するチームメンバーは、複数の組織にまたがる攻撃を緩和するための戦略を共有するために、パートナー組織の運用上の同種の部署と調整することができます。あるいは、同じインシデントの間に、インシデント対応チームマネージャーは、必要な報告要件を満たすために ISAC と調整し、インシデントへの対応を成功させるためのアドバイスや追加のリソースを求めることができます。表 4-1 は、外部組織との連携時に存在する可能性のある連携関係の例をいくつか示しています。

表 4-1　連　携

カテゴリー	定　義	情報共有
チームと チーム	チームとチームの関係は、異なる組織の技術的なインシデント対応者が、インシデント処理のライフサイクルのどの段階でも仲間と協力しているときにはいつでも存在する。このタイプの関係に参加している組織は、通常、互いに権限を持たない仲間であり、情報を共有し、リソースをプールし、知識を再利用して両チームに共通する問題を解決することを選択している。	チームとチームの関係で最も頻繁に共有される情報は、戦術的かつ技術的なもの（例えば、危殆化の技術的指標、提案された是正措置）であるが、準備段階の一部として実施される場合には、他の種類の情報（計画、手順、教訓）を含む場合もある。
チームと 連携チーム	チームと連携チームの関係は、組織的なインシデント対応チームと、USCERT や ISAC のような連携されたインシデント対応と管理のための中心的なポイントとして機能する別の組織との間に存在する。このタイプの関係には、連携機関がメンバー組織からある程度の報告を要求することと、連携チームが参加メンバー組織にタイムリーで有用な情報を発信することを期待することが含まれる。	チームと連携チームは、戦術的、技術的な情報だけでなく、脅威、脆弱性、および連携チームの活動対象となるコミュニティへのリスクに関する情報を頻繁に共有する。また、連携チームは、リソースと注意をどこに集中させるかを決定するために、インシデントに関する具体的な影響情報を必要とすることもある。
連携チームと 連携チーム	US-CERT や ISAC などの複数の連携チーム間の関係は、複数のコミュニティに影響を及ぼす可能性のある横断的なインシデントに関連する情報を共有するために存在する。連携チームは、それぞれの地域社会のメンバー組織を代表して行動し、コミュニティ間の対応を支援するために、横断的なインシデントの性質と範囲、および再利用可能な緩和戦略に関する情報を共有している。	連携チームが相手チームと共有する情報の種類は、「定常状態」の活動中には定期的なサマリーで構成されることが多く、その間には、戦術的、技術的な詳細、対応計画、および連携されたインシデント対応活動中の影響やリスク評価に関する情報の交換が行われる。

組織は、連携に必要な人間関係を構築することが難しいと感じるかもしれません。コミュニティの構築は、組織が属する業界や、組織が活動している地理的な地域から始めるのが適しています。組織のインシデント対応チームは、自分の属する業界や地域内の他のチームと（チーム間のレベルで）関係を築こうとしたり、すでに情報共有を促進している業界内の確立された組織に参加したりすることができます。関係性を構築するためのもう一つの考慮点は、関係性には強制的なものと自発的なものがあるということです。例えば、チーム間の関係は通常任意のものであるのに対し、チーム間の関係は強制的なものであることが多いです。組織が自発的な関係を追求するのは、相互の自己利益を満たすためです。強制的な関係は、通常、業界内の規制機関または別の組織または事業体等によって定義されます。

4.1.2 協定と報告要件

外部組織と情報を共有しようとする組織は、連携作業を開始する前に、法務部に相談すべきです。議論が行われる前に、制定する必要がある契約やその他の合意があるかもしれません。例としては、組織の最も機密性の高い情報の機密性を保護するための守秘義務契約（NDA）があります。また、組織は、インシデント情報を ISAC と共有したり、より高いレベルの CIRT にインシデントを報告したりするなど、報告に関する既存の要件も考慮すべきです。

4.2 情報共有のテクニック

情報共有は、組織間の連携を可能にするための重要な要素です。たとえ小規模な組織であっても、多くのインシデントに効果的に対処するためには、仲間やパートナーとインシデント情報を共有する必要があります。組織は、インシデントが完全に解決するまで待ってから他の人とインシデントの詳細を共有するのではなく、インシデント対応のライフサイクル全体を通してそのような情報共有を行うべきです。セクション 4.3 では、組織が他の人と共有することを望む場合と望まない場合があるインシデント情報のタイプについて論じています。

このセクションでは、情報共有のためのテクニックに焦点を当てます。セクション 4.2.1 ではアドホックな方法に、セクション 4.2.2 では部分的に自動化された方法に注目します。最後に、セクション 4.2.3 では、情報共有に関連するセキュリティ上の考慮事項について論じます。

4.2.1 アドホック※

ほとんどのインシデント情報の共有は、従来、電子メール、インスタントメッセージングクライアント、電話などのアドホックな方法で行われてきました。アドホックな情報共有メカニズムは、通常、パートナー組織のインシデント対応チームの従業員との個々の従業員のつながりに依存しています。従業員は、これらのつながりを利用して仲間と情報を手動で共有し、インシデントに対応するための戦略を構築するために仲間と連携します。組織の規模にもよりますが、このようなアドホックな手法は、パートナー組織と情報を共有するための最も費用対効果の高い方法かもしれません。しかし、アドホックな情報共有は非公式なものであるため、情報共有プロセスが常に機能することを保証できません。例えば、特にコネのある従業員がインシデント対応チームを辞めた場合、そのチームは一時的に、外部組織との効果的な連携のために頼りにしていた情報共有チャネルの大半を失う可能性があります。

また、アドホックな情報共有方法は、どのような情報が伝達され、どのように伝達されるかという点で、標準化されていないことがほとんどです。標準化されていないため、手動での介入が必要となり、部分的に自動化された方法よりも処理にリソースがかかる傾向があります。可能な限り、組織は、パートナー組織との正式な合意や、情報共有の部分的な自動化に役立つ技術的なメカニズムを通じて、情報共有戦略を正式なものにすることを試みるべきです。

※「特定の目的の」「その場限りの」という意味のラテン語

4.2.2 部分的な自動化

組織は、組織間の連携を効率的かつ費用対効果の高いものにするために、情報共有プロセスを可能な限り自動化することを試みるべきです。実際には、すべてのインシデント情報の共有を完全に自動化することは不可能であり、また、セキュリティと信頼性の観点からも望ましいことではありません。組織は、自動化された情報共有と、情報の流れを管理するための人間中心のプロセスとのバランスを取ることを試みるべきです。

自動化された情報共有ソリューションを設計する際には、組織はまず、パートナーとどのようなタイプの情報をやり取りするかを検討する必要があります。組織は、共有したいすべての組織や事業体等間の関係を列挙した正式なデータ辞書を構築したいと思うかもしれません。組織が共有する情報の種類を理解したら、この情報を取り込むための形式的で機械処理可能なモデルを構築する必要

があります。可能な限り、組織は共有する必要のある情報を表現するために、既存のデータ交換標準を使用すべきです※。組織は、データ交換モデルを決定する際、パートナー組織と協力して、選択した標準がパートナー組織のインシデント対応システムと互換性があることを確認すべきです。既存のデータ交換モデルを選択する場合、組織は、インシデント対応領域の異なる側面をモデル化した複数のモデルを選択し、モジュール方式でこれらのモデルを活用し、ライフサイクルの特定の意思決定ポイントで必要な情報のみを通信することを好むかもしれません。付録 E は、インシデント対応ドメインに適用可能なデータ交換モデルを定義する既存の標準の非網羅的リストです。

インシデント情報を共有するためのデータ交換モデルを選択することに加えて、組織は、パートナー組織と協力して、情報交換が自動化された方法で行われるための技術的な転送メカニズムに合意しなければなりません。これらのトランスポートメカニズムには、少なくとも、情報を交換するためのトランスポートプロトコル、情報リソースと通信するためのアーキテクチャモデル、および特定の組織で情報リソースにアクセスするための適用可能なポートとドメイン名が含まれます。例えば、パートナー組織のグループは、各組織の DMZ 内の特定のドメイン名のポート 4590 のハイパーテキスト転送プロトコルセキュア（HTTPS）を介して IODEF/Real-Time Inter-Network Defense （RID）データを交換するために、REST（Representational State Transfer） アーキテクチャを使用してインシデント情報を交換することを決定することができます。

※National Technology Transfer and Advancement Act (NTTAA)によると、「すべての連邦政府機関および省庁は、自主的なコンセンサス基準機関によって開発または採択された技術基準を使用しなければならない」とされています。詳細は http://standards.gov/nttaa.cfm を参照のこと。

4.2.3 セキュリティに関する考慮事項

インシデント対応チームが情報共有を計画する際にセキュリティ上の考慮事項がいくつかあります。一つは、インシデント情報のどの部分を誰が見ることができるかを指定できることです（例えば、機密情報の保護)。また、インシデント情報から前兆、兆候、およびその他の技術情報の情報を乱すことなく、センシティブなデータの断片を除去するために、データのサニタイズまたはスクラビングを行うことも必要かもしれません。また、インシデント対応チームは、他の組織がチームと共有した情報を保護するために必要な措置が取られていることを確認する必要があります。

また、データ共有に関して考慮すべき多くの法的問題もあります。追加情報については、セクション 4.1.2 を参照のこと。

4.3 粒度の高い情報の共有

組織は、情報共有の利点と機密情報を共有することの欠点のバランスをとる必要があり、理想的には、必要な情報を共有し、必要な情報のみを適切な関係者と共有する必要があります。組織は、インシデント情報を、ビジネスに影響を与える情報と技術的な情報の 2 つのタイプで構成されていると考えることができます。ビジネスに影響を与える情報は、セクション 4.1.1 で定義されているように、チームと連携チームの関係の中で共有されることが多いですが、技術的な情報は、3 つのタイプの連携関係の中で共有されることが多いです。このセクションでは、両方のタイプの情報について説明し、詳細な情報共有を実行するための推奨事項を提供します。

4.3.1 ビジネスへの影響情報

ビジネスへの影響情報には、ミッションへの影響、財務上の影響などの観点から、インシデントが組織にどのような影響を与えているかが含まれます。このような情報は、少なくとも概要レベルでは、インシデントによって引き起こされた損害の推定値を伝えるために、より高いレベルの連携対応チームに報告されることが多いです。連携対応チームは、報告組織に提供すべき支援の程度に関する意思決定を行うために、この影響情報を必要とする場合があります。また、連携チームは、特定のインシデントが自分たちが代表するコミュニティの他の組織にどのような影響を与えるかを決定するために、この情報を使用することもあります。

連携チームは、メンバー組織に対し、ある程度のビジネスへの影響情報の報告を要求することがあります。例えば、連携チームは、第 3.2.6 項で定義されたカテゴリーを使用して、影響情報を報告することをメンバー組織に要求することができます。この場合、ある組織は、仮想的なインシデントについて、機能的影響は「中程度」、情報的影響は「なし」、回復可能時間の延長が必要であると報告することになります。この高レベルの情報は、メンバー組織がインシデントから回復するために、ある程度のレベルの追加リソースを必要とすることを連携チームに警告します。連携チームは、その後、メンバー組織との追加コミュニケーションを追求し、インシデントについて提供された技術情報に基づいて、どの程度のリソースが必要か、また、リソースの種類を決定することができます。

ビジネスへの影響情報は、インシデントが発生した組織の使命を確実にすることに何らかの関心を持つ組織に報告するためにのみ有用です。多くの場合、インシデント対応チームは、明確な価値提案や正式な報告要件がない限り、外部組織とのビジネスインパクト情報の共有を避けるべきです。同業者やパートナー組織と情報を共有する場合、インシデント対応チームは、セクション 4.3.2 で概説されているように、技術的な情報の交換に焦点を当てるべきです。

4.3.2 技術情報

組織内でのインシデントの発生を示す技術的な兆候には、さまざまな種類があります。これらの兆候は、攻撃するホストのホスト名や IP アドレス、マルウェアのサンプル、類似のインシデントの前兆や兆候、インシデントで悪用された脆弱性の種類など、インシデントに関連するさまざまな技術情報に由来しています。セクション 3.2.2 では、進行中のインシデントを特定するために、組織がこれらの兆候をどのように収集し、活用すべきかの概要を説明しています。さらに、セクション 3.2.3 では、インシデント兆候データの一般的な情報源のリストを提供します。

組織は、独自の内部兆候を収集することで価値を得ますが、パートナー組織から受け取った兆候を分析したり、外部の分析・利用のために内部兆候を共有したりすることで、さらなる価値を得ることができます。組織が見ていないインシデントに関連する外部兆候データを受け取った場合、その兆候データを使用して、インシデントが発生し始めた時点でそのインシデントを特定することができます。同様に、組織は、特定の兆候データを取得するための内部リソースが不足しているために気づかなかった進行中のインシデントを検出するために、外部兆候データを使用することができます。組織は、内部兆候データを外部組織と共有することでも利益を得られます。例えば、組織が経験しているインシデントに関連する技術情報を共有した場合、パートナー組織は、そのインシデントに対処するための改善策を提案して対応することができます。

組織は、このような情報を可能な限り共有すべきです。しかし、組織が悪用された脆弱性の詳細を明らかにしたくない理由には、セキュリティ上の理由と責任上の理由があるかもしれません。攻撃の一般的な特徴や攻撃するホストの身元などの外部指標は、通常、他の人と共有しても安全です。組織は、どのような種類の技術情報を様々な関係者と共有すべきか、あるいは共有すべきでないかを検討し、適切な情報を可能な限り他の組織と共有するように努めなければなりません。

技術的兆候データは、組織が実際のインシデントを特定できる場合に役立ちます。しかし、外部ソースから受け取ったすべての兆候データが、それを受け取った組織に関係するわけではありません。場合によっては、この外部データは、受信した組織のネットワーク内で誤検知を発生させ、存在しない問題にリソースが費やされる可能性があります。

インシデント情報の共有に参加している組織は、共有コミュニティから技術的兆候情報を取得し、その情報を企業全体に、できれば自動化された方法で発信することに長けたスタッフを持つべきです。また、組織は、実際のインシデントを意味すると比較的高いレベルで確信できる兆候のみを共有するように努めるべきです。

4.4 推奨事項

本セクションでは、インシデントへの対応に関する主な推奨事項を以下にまとめています。

■ インシデントが発生する前に、外部関係者とのインシデント連携を計画する。
外部関係者の例としては、他のインシデント対応チーム、法執行機関、インターネットサービスプロバイダ、および構成員や顧客が挙げられます。この計画は、すべての関係者がそれぞれの役割を理解し、効果的なコミュニケーションラインが確立されていることを確認するのに役立ちます。

■ 連携作業を開始する前に、法務部に相談する。
協議を行う前に、契約やその他の合意が必要な場合がある可能性があります。

■ インシデント対応のライフサイクル全体を通して、インシデント情報の共有を行う。
情報共有は、組織間の連携を可能にするための重要な要素です。組織は、インシデントが完全に解決するのを待たずに、他の連携チームとインシデントの詳細を共有すべきです。

■ 情報共有プロセスを可能な限り自動化させる。
これにより、組織横断的な連携が、効率的かつ費用対効果の高いものになります。組織は、自動化された情報共有と、情報の流れを管理するための人間中心のプロセスとのバランスを図るべきです。

■ 情報共有の利点と、機密情報を共有することの欠点とのバランスをとる。

理想的には、組織は必要な情報を適切な関係者と共有し、必要な情報のみを共有すべきです。ビジネスに影響を与える情報は、チームと連携チームの関係で共有されることが多いですが、技術的な情報は、あらゆる種類の連携関係の中で共有されることが多いです。同業者やパートナー組織と情報を共有する場合、インシデント対応チームは技術情報の交換に重点を置くべきです。

■ 適切なインシデント情報を可能な限り他の組織と共有する。

組織は、どのタイプの技術情報を様々な関係者と共有すべきか、あるいは共有すべきでないかを検討すべきです。例えば、攻撃の一般的な特徴や攻撃するホストの身元などの外部指標は、通常、他の人と共有しても安全ですが、組織が悪用された脆弱性の詳細を明らかにしたくない理由として、セキュリティ上の理由と責任上の理由の両方があるかもしれません。

4.付　録

付録 A インシデントハンドリングのシナリオ

インシデントハンドリングシナリオは、そのスキルの構築とプロセスの潜在的な問題点を特定するための軽易で効果的な方法を提供します。インシデントハンドリングチームまたはチームメンバーには、シナリオと関連する質問のリストが提示されます。その後、チームはそれぞれの質問について議論し、最も可能性の高い回答を決定します。ゴールは、チームが実際に何をするかを判断し、それをポリシー、手順、および一般的に推奨されている慣行と比較して、矛盾や欠陥を特定することです。例えば、ある質問への回答は、チームにソフトウェアがないために回答が遅れることや、他のチームが時間外のサポートを提供していないために回答が遅れることを示しているかもしれません。

以下の質問は、ほぼすべてのシナリオに当てはまります。各質問の後には、文書の関連するセクションを参照してください。質問の後にはシナリオがあり、それぞれの質問の後には追加のインシデント固有の質問が続きます。組織において、これらの質問とシナリオを、独自のインシデントハンドリング演習で使用するよう強く推奨します※。

※演習の詳細については、http://csrc.nist.gov/publications/PubsSPs.html#800-84 にある NISTSP800-84,GuidetoTest,Training,andExerciseProgramsforITPlansandCapabilities を参照してください。

A.1　シナリオの質問

準　備

1. 組織はこの活動をインシデントと考えますか ?その場合、この活動は組織のどの方針に違反していますか ?(セクション 2.1)
2. このタイプのインシデントの発生を防止するため、またはその影響を制限するために、どのような対策が講じられていますか ?(セクション 3.1.2)

検知と分析

1. インシデントの前兆があるとすれば、組織はどのようなものを検知する可能性はありますか?前兆があれば、組織はインシデントが発生する前に行動を起こせますか?(セクション 3.2.2.2,3.2.3)
2. どのような兆候があれば、組織はインシデントを検知できますか ?どのような兆候があれば、インシデントが発生したかもしれないと誰かに思わせることができますか ?(セクション 3.2.2.2、3.2.3)
3. この特定のインシデントを検出するために、どのような追加ツールが必要になるかもしれませんか?(セクション 3.2.3)
4. インシデント対応チームは、どのようにしてこのインシデントを分析し、検証しますか ?どのような人員が分析及び検証プロセスに関与しますか ?(セクション 3.2.4)
5. チームは、組織内のどのような人々やグループにインシデントを報告しますか ?(セクション 3.2.7)
6. チームはどのようにしてこのインシデントの処理に優先順位をつけますか ?(セクション 3.2.6)

封じ込め、根絶、回復

1. このインシデントを封じ込めるために、組織はどのような戦略をとるべきですか ?この戦略が他の戦略よりも望ましい理由は何ですか ?(セクション 3.3.1)
2. インシデントが封じ込められなかった場合、何が起こりえますか ?(セクション 3.3.1)
3. この特定のインシデントに対応するために、どのような追加ツールが必要になるかもしれなませんか ?(セクション 3.3.1、3.3.4)
4. 封じ込め、根絶、回復のプロセスにはどのような人員が関与しますか ?(セクション 3.3.1、3.3.4)
5. 組織は、もしあるならば、どのような証拠の情報源を取得すべきですか ?どのようにして証拠を取得しますか ?どこに保管しますか ?どのくらいの期間保管されるべきですか ?(セクション 3.2.5、3.3.2、3.4.3)

インシデント後の活動

1. このインシデントに関する教訓を学ぶ会議には誰が出席しますか ?(セクション 3.4.1)
2. 今後同様のインシデントが発生しないようにするために、何ができますか ?(セクション 3.1.2)

3. 同様のインシデントの検出を改善するために何ができますか ?(セクション 3.1.2)

一般的な質問

1. このインシデントの対応には、何人のインシデントハンドリングチームメンバーが参加しますか ?(セクション 2.4.3)
2. インシデント対応チーム以外に、組織内のどのようなグループがこのインシデントの対処に関与しますか ?(セクション 2.4.4)
3. チームはどの外部関係者にインシデントを報告しますか?各報告はいつ行われますか?各報告はどのように行われますか ?どのような情報を報告するか、あるいは報告しないか、その理由は ?(セクション 2.3.2)
4. その他、外部とのコミュニケーションはどのような場合に発生しますか ?(セクション 2.3.2)
5. このインシデントに対処するために、チームはどのようなツールやリソースを使用しますか ?(セクション 3.1.1)
6. もしインシデントが別の日と時間に発生していたら、処理のどのような側面が違っていたでしょうか(時間内と時間外) ?(セクション 2.4.2)
7. インシデントが異なる物理的な場所で発生していたら、処理のどのような側面が違っていたでしょうか（オンサイトとオフサイト） ?(セクション 2.4.2)

A.2 シナリオ

シナリオ１：ドメインネームシステム(DNS)サーバの DoS(サービス拒否)

土曜日の午後、外部のユーザが組織の公開ウェブサイトにアクセスする際に問題が発生します。その後 1 時間ほどで問題は悪化し、ほぼすべてのアクセスが失敗するまでになりました。一方、組織のネットワーキング担当者の一人がインターネットとの境界ルータからの警告に応答し、組織のインターネット帯域幅が、組織のパブリック DNS サーバとの間のユーザ・データグラム・プロトコル(UDP)パケットの異常に大量のパケットによって消費されていると判断しました。トラフィックを分析すると、DNS サーバは 1 つの外部 IP アドレスから大量のリクエストを受信していることがわかります。また、そのアドレスからの DNS リクエストはすべて同じソースポートから来ています。このシナリオに関する追加の質問は以下の通りです。

1. 問題の外部 IP アドレスに関して、組織は誰に連絡すべきか?

2. 初期の封じ込め対策を実施した後、ネットワーク管理者が、9 台の内部ホストが DNS サーバに同じ異常な要求を試みていることを検出したとします。
3. 9 台の内部ホストのうち 2 台が、システムの所有者が特定される前にネットワークから切断されたとします。システム所有者はどのようにして特定されますか?

シナリオ 2：ワームと分散型サービス拒否（DDoS）エージェントの侵入

火曜日の朝、新しいワームがリリースされます。このワームはリムーバブルメディアを介して拡散し、自分自身をコピーして Windows の共有を開くことができます。ワームがホストに感染すると、DDoS エージェントをインストールします。ワームが拡散し始めてから数時間後のウィルス対策シグネチャが利用可能になる前に、組織はすでに広範囲の感染を起こしています。

このシナリオに関する追加の質問は以下の通りです。

1. インシデント対応チームは、感染したすべてのホストをどのようにして特定しますか?
2. ウィルス対策シグネチャがリリースされる前に、組織はどのようにしてワームが組織内に侵入するのを防止しようとしますか?
3. ウィルス対策のシグネチャがリリースされる前に、感染したホストによるワームの拡散をどのようにして防ぐことができますか?
4. 組織はすべての脆弱性のあるマシンにパッチを当てることを試みますか?その場合、どのようにしてパッチを適用しますか?
5. DDoS エージェントを受け取った感染ホストが、翌朝に別の組織のウェブサイトを攻撃するように設定されていた場合、このインシデントの処理はどのように変わりますか?
6. 感染したホストの 1 台以上に、組織の従業員に関する機密性の高い個人情報が含まれていた場合、このインシデントの処理はどのように変わりますか?
7. インシデント対応チームは、どのようにして組織のユーザにインシデントの状況を通知しますか?
8. 現在ネットワークに接続されていないホスト(例:休暇中のスタッフ、たまに接続するオフサイトの従業員)に対して、チームはどのような追加対策を行いますか?

シナリオ 3：ドキュメントの盗難

月曜日の朝、組織の法務部門は、組織のシステムに関わる不審な活動について、連邦捜査局(FBI)から電話を受けました。その日の後半、FBI 捜査官が経営陣と法務部のメンバーと面会し、その活動について話し合うことになります。FBI は、機密性の高い政府文書の公開に関わる活動を調査し

ており、その文書の一部は組織のものであると報告されていました。捜査官は組織の支援を求め、経営陣はこれらの文書が正当なものであるかどうか、どのようにして漏洩した可能性があるかを判断するために必要な証拠を入手するために、インシデント対応チームの支援を求めています。
このシナリオに関する追加の質問は以下の通りです。

1. インシデント対応チームは、どのような情報源から証拠を収集する可能性がありますか ？
2. 調査の秘密を守るために、チームは何をしますか ？
3. チームが漏洩の原因となった内部ホストを特定した場合、このインシデントの処理はどのように変わるでしょうか?
4. チームが漏洩の原因となった内部ホストにインストールされたルートキットを発見した場合、このインシデントの処理はどのように変わりますか?

シナリオ 4 :データベースサーバの危殆化

火曜日の夜、データベース管理者は、いくつかの本番用データベースサーバのメンテナンスを時間外に行いました。管理者は、サーバの 1 つに見慣れない珍しいディレクトリ名があることに気付きました。ディレクトリのリストを確認し、いくつかのファイルを閲覧した後、管理者はサーバが攻撃されたと結論付け、インシデント対応チームに支援を要請しました。チームの調査では、攻撃者が 6 週間前にサーバへのルートアクセスに成功したことが判明しました。
このシナリオに関する追加の質問は以下の通りです。

1. チームはどのような情報源を使用して、侵害がいつ発生したかを判断することができますか?データベースサーバがパケットスニッファーを実行し、ネットワークからパスワードを取得していたことをチームが発見した場合、このインシデントの処理はどのように変わるでしょうか?
2. サーバが毎晩、機密性の高い顧客情報(個人を特定できる情報を含む)を含むデータベースをコピーして外部アドレスに転送するプロセスを実行していたことをチームが発見した場合、このインシデントの処理はどのように変わるでしょうか?
3. チームがサーバ上にルートキットを発見した場合、このインシデントの処理はどのように変わりますか?

シナリオ５：不明な流出

日曜日の夜、組織のネットワーク侵入検知センサーの１つが、大規模なファイル転送を含む異常なアウトバウンドネットワークアクティビティを警告しました。侵入アナリストがアラートを確認すると、何千もの.RAR ファイルが内部ホストから外部ホストにコピーされており、外部ホストは別の国に位置していることがわかりました。アナリストは、インシデント対応チームに連絡して、その活動をさらに調査できるようにします。.RAR ファイルの内容は暗号化されているため、チームは.RAR ファイルが何を保持しているかを見ることができません。.RAR ファイルを含む内部ホストを分析すると、ボットのインストールの兆候が見られます。

このシナリオに関する追加の質問は以下の通りです。

1. .RAR ファイルの内部にある可能性の高いものをチームはどのように判断するのでしょうか ?他のどのチームがインシデント対応チームを支援しますか ？
2. インシデント対応チームが、最初の侵害が内部ホストのワイヤレスネットワークカードを介して行われたと判断した場合、チームはこの活動をどのようにしてさらに調査しますか?
3. インシデント対応チームが、内部ホストが企業内の他のホストからの機密ファイルのステージングに使用されていると判断した場合、チームはどのようにしてこの活動をさらに調査しますか?

シナリオア６：給与記録への不正アクセス

水曜日の夕方、組織のフィジカルセキュリティチームは、給与計算の管理者から「見知らぬ人物がオフィスを出て廊下を駆け下り、ビルから出ていくのを見た」と電話を受けました。その管理者は、数分間だけ自分のワークステーションの鍵を開けたまま放置していました。給与計算プログラムは放置したままログインし、メインメニューに表示されていましたが、管理者はマウスが移動したように見えることに気付きました。インシデント対応チームは、インシデントに関連する証拠を取得し、どのような行動が行われたかを判断するように求められています。

このシナリオに関する追加の質問は以下の通りです。

1. どのようにして、どのようなアクションが実行されたかを判断するのでしょうか?
2. 給与管理者が、退社した人物を元給与計算部門の従業員と認識していた場合、このインシデントの処理はどのように違っていたのでしょうか ？
3. その人物が現役の従業員であると信じるに足る理由があった場合、このインシデントの処理はどのように異なるでしょうか ？

4. フィジカルセキュリティチームが、その人物がソーシャルエンジニアリング技術を使って建物に物理的にアクセスしたと判断した場合、このインシデントの処理はどのように異なるでしょうか?
5. 前週のログに、給与管理者のユーザ ID を使用したリモートログインの試みに異常に多くの失敗があった場合、このインシデントの処理はどのように異なるのでしょうか?
6. 2 週間前に、インシデント対応チームがコンピュータにキーストロークロガーがインストールされていたことを発見した場合、このインシデントの処理はどのように異なるでしょうか ?

シナリオ 7 ：消えるホスト

木曜日の午後、ネットワーク侵入検知センサーが、内部 IP アドレスによって生成された内部ホストに向けられた脆弱性スキャン活動を記録します。侵入検知アナリストは、許可され、かつスケジュールされた脆弱性スキャンがないことを知っているため、その活動をインシデント対応チームに報告します。チームが分析を開始すると、アクティビティが停止しており、その IP アドレスを使用しているホストが存在しなくなっていることがわかります。

このシナリオに関する追加の質問は以下の通りです。

1. どのようなデータソースが脆弱性スキャンホストの身元に関する情報を含んでいる可能性がありますか?
2. チームは、どのようにして脆弱性スキャンを実行していた人を特定するのでしょうか ?
3. 脆弱性スキャンが組織の最も重要なホストに向けられていた場合、このインシデントの処理はどのように異なるでしょうか?
4. 脆弱性スキャンが外部ホストに向けられていた場合、このインシデントの取り扱いはどのように異なるでしょうか?
5. 内部 IP アドレスが組織の無線ゲストネットワークに関連付けられていた場合、このインシデントの処理はどのように異なるでしょうか?
6. フィジカルセキュリティスタッフが、脆弱性スキャンが発生する 30 分前に誰かが施設に侵入したことを発見した場合、このインシデントの処理はどのように異なるでしょうか?

シナリオ８：在宅勤務の妥協点

土曜日の夜、ネットワーク侵入検知ソフトウェアは、ウォッチリストの IP アドレスから発信されたインバウンド接続を記録します。侵入検知アナリストは、その接続が組織の VPN サーバに行われていると判断し、インシデント対応チームに連絡します。チームは、侵入検知、ファイアウォール、および VPN サーバのログを確認し、セッションで認証されたユーザ ID と、そのユーザ ID に関連付けられたユーザ名を特定します。

このシナリオに関する追加の質問は以下の通りです。

1. チームの次のステップは何ですか?なぜこのステップを最初に実行する必要があるのでしょうか?次に実行すべきステップは何ですか?
2. 外部 IP アドレスがオープンプロキシに属していた場合、このインシデントの処理はどのように異なるでしょうか?
3. ユーザが知らないうちに、その ID が複数の外部 IP アドレスから VPN 接続を開始するために使用されていた場合、このインシデントの処理はどのように異なるでしょうか?
4. 特定されたユーザのコンピュータが、家族のメンバーによってダウンロードされたトロイの木馬を含むゲームによって危険にさらされていたとします。これは、証拠の収集と処理にどのような影響を与えますか ?ユーザのコンピュータからインシデントを根絶するという点で、チームは何をすべきでしょうか?
5. ユーザがウィルス対策ソフトをインストールし、トロイの木馬にキーストロークロガーが含まれていたと判断したとします。このことは、インシデントの処理にどのような影響を与えますか?ユーザがシステム管理者であった場合、このことはインシデントの処理にどのような影響を与えますか?ユーザが組織内の高位幹部であった場合、このことはインシデントの処理にどのような影響を与えるでしょうか?

シナリオ９：匿名の脅威

木曜日の午後、組織のフィジカルセキュリティチームは、IT マネージャーから「従業員 2 名が組織のシステムに対する匿名の脅迫を受けた」との報告を受けました。調査に基づき、フィジカルセキュリティチームは、脅威を真剣に受け止めるべきだと考え、インシデント対応チームを含む適切な内部チームに脅威を通知します。

このシナリオに関する追加の質問は以下の通りです。

1. インシデント対応チームは、脅威の通知に対応して、何かあるとすれば、どのように異なる行動をとるべきでしょうか ？

2. フィジカルセキュリティ管理の強化は、インシデント対応チームの対応にどのような影響を与える可能性がありますか ？

シナリオ１０：ピアツーピアによるファイル共有

この組織では、ピアツーピアのファイル共有サービスの使用を禁止しています。この組織のネットワーク侵入検知センサーは、複数の一般的なピアツーピアファイル共有サービスの使用を検知できるシグネチャを有効にしています。月曜日の夕方、侵入検知アナリストは、過去 3 時間の間に複数のファイル共有アラートが発生し、すべて同じ内部 IP アドレスが関係していることに気付きました。

1. このインシデントの処理に優先順位をつけるには、どのような要因を使用すべきでしょうか(共有されているファイルの内容など)。
2. どのようなプライバシーへの配慮が、このインシデントの処理に影響を与える可能性がありますか?
3. ピアツーピアのファイル共有を実行するコンピュータにも機密性の高い個人情報が含まれている場合、このインシデントの処理はどのように異なるでしょうか?

シナリオ１１：不明な無線アクセスポイント

月曜日の朝、組織のヘルプデスクは、ビルの同じフロアにいる 3人のユーザから、無線アクセスに問題があるとの電話を受けました。問題解決の支援を依頼されたネットワーク管理者は、無線アクセスが可能なノートパソコンをユーザのフロアに持ってきました。無線ネットワークの設定を見ていると、新しいアクセスポイントが利用可能であることに気付きます。チームメイトに確認したところ、このアクセスポイントは自分のチームでは配備されていないため、許可なく設置された不正なアクセスポイントである可能性が高いと判断しました。

1. このインシデントに対処するための最初の主要なステップは何でしょうか（不正アクセスポイントを物理的に見つける、アクセスポイントに論理的に接続するなど） ？
2. アクセスポイントを見つける最も早い方法は何ですか?アクセスポイントの場所を特定する最も内密な方法は何ですか?
3. アクセスポイントが外部の関係者（契約者など）によって一時的に組織のオフィスに配置されていた場合、このインシデントの処理はどのように異なるでしょうか？

4. 侵入検知アナリストが、ビルの同じフロアにあるいくつかのワークステーションに関係する不審な活動の兆候を報告した場合、このインシデントの処理はどのように異なるでしょうか?
5. チームがまだ物理的にアクセスポイントの位置を特定しようとしている間に、アクセスポイントが取り外されていた場合、このインシデントの処理はどのように異なるでしょうか?

付録Ｂ　インシデント関連データ要素

組織は、各インシデントについて収集すべきインシデント関連のデータ要素の標準的なセットを特定すべきです。この取り組みは、より効果的で一貫性のあるインシデント処理を促進するだけでなく、適用されるインシデント報告の要件を満たすために組織を支援することにもなります。組織は、インシデントが報告されたときに収集される基本的な要素（例えば、インシデント報告者の名前、電話番号、および場所）のセットと、インシデント対応者が対応中に収集する追加の要素のセットを指定すべきです。2 つの要素のセットは、前にセクション 3.2.5 で議論したインシデント報告データベースの基礎となります。以下のリストは、インシデントに対して収集すべき情報の提案であり、包括的なものではありません。各組織は、そのインシデント対応チームのモデルと構造、および"インシデント"という用語の定義を含むいくつかの要因に基づいて、独自のデータ要素リストを作成するべきです。

B.1 基本データ要素

■ インシデントレポーター・ハンドラーの連絡先

- 名　前
- 役　割
- 組織単位（例：代理店、部署、部署、チーム）と所属
- メールアドレス
- 電話番号
- 所在地（住所、事務所の部屋番号など）

■ インシデントの詳細

- 状態変化の日付/タイムスタンプ（タイムゾーンを含む）

  インシデントが開始されたとき、インシデントが発見/検出されたとき、インシデントが報告されたとき、インシデントが解決/終了したとき、など
- インシデントの物理的な場所（例：市、州）
- インシデントの現在の状況（進行中の攻撃など）
- ホスト名と IP アドレスを含む、インシデントの発生源/原因(既知の場合)
- インシデントの説明（例‥どのようにして検出されたか、何が起こったか）

- システムのホスト名、IP アドレス、機能を含む、影響を受けるリソース（ネットワーク、ホスト、アプリケーション、データなど）の説明
- 既知の場合は、インシデントのカテゴリー、インシデントに関連する攻撃のベクトル、およびインシデントに関連する指標（トラフィックパターン、レジストリキーなど–優先順位付けの要因（機能的な影響、情報への影響、復旧可能性など）
- 緩和要因（例：機密データを含む盗まれたノートパソコンが完全なディスク暗号化を使用していたなど）
- 実行されたレスポンスアクション（例：ホストのシャットオフ、ネットワークからのホストの切断）
- 連絡を取った他の組織（例：ソフトウェアベンダー）

■ 総　評

B.2 インシデントハンドラーのデータ要素

■ インシデント対応の現状

■ インシデントの概要

■ インシデント対応アクション

- すべてのハンドラーが実行したアクションのログ
- 関係者の連絡先
- 集められた証拠の一覧

■ インシデントハンドラーのコメント

■ インシデントの原因（アプリケーションの設定ミス、パッチが適用されていないホストなど）

■ インシデントの費用

■ インシデントのビジネスへの影響※

※インシデントのビジネスへの影響は、インシデントの影響の説明（例えば、会計部門が 2日間タスクを実行できないなど）か、コストに基づく影響のカテゴリー（例えば、「重大な」インシデントは 10 万ドル以上のコストがかかるなど）のいずれかである可能性があります。

付録 C用語集

本資料で使用されている用語は以下の通りです。

バーゼルニング

リソースを監視して典型的な利用パターンを判断し、重大な逸脱を検出できるようにすること。

コンピュータセキュリティインシデント

「インシデント」を参照

コンピュータセキュリティインシデントレスポンスチーム（CSIRT）

コンピュータセキュリティ関連のインシデントへの対応を支援する目的で設置された機能。コンピュータインシデントレスポンスチーム（CIRT）または CIRC（コンピュータインシデントレスポンスセンター、コンピュータインシデント対応能力）とも呼ばれる。

イベント

ネットワークまたはシステムで観察可能なあらゆる出来事

偽陽性

悪意のあるアクティビティが発生していることを誤って示すアラート

インシデント

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慣行に対する違反による差し迫った脅威。

インシデントハンドリング

セキュリティポリシーおよび推奨されるプラクティスの違反を緩和すること。インシデント対応「インシデントハンドリング」参照

インジケータ（兆候）

インシデントが発生した可能性がある、または現在発生している可能性があることを示す兆候。

侵入検知および侵入防止システム

コンピュータシステムまたはネットワークで発生しているイベントを監視し、インシデントの可能性のある兆候を分析し、検出されたインシデントを停止させようとするプロセスを自動化するソフトウェア。

マルウェア

ウィルス、ワーム、トロイの木馬、またはその他のコードベースの悪意のある存在で、ホストに感染することに成功したもの。

前　兆

攻撃者がインシデントを引き起こす準備をしている可能性のある兆候。

プロファイリング

予想される活動の特性を測定して、活動の変化をより容易に特定できるようにすること。

シグネチャ

ウィルスのバイナリ文字列や、システムへの不正アクセスに使用される特定のキーストロークなど、攻撃に関連した認識可能で識別可能なパターン。

ソーシャルエンジニアリング

システムやネットワークを攻撃するために使用できる情報（パスワードなど）を明らかにしようと誰かを騙そうとする試み。

脅　威

不利な事象の潜在的な発生源。

脆弱性

システム、アプリケーション、またはネットワークの弱点で、悪用されたり悪用されたりする可能性があるもの。

付録 D 頭字語（略語）集

この文書で使用されているいくつかの略語は、以下に定義されています。

CCIPS

Computer Crime and Intellectual Property Section

コンピュータ犯罪・知的財産部門

CERIAS

Center for Education and Research in Information Assurance and Security

情報セキュリティ教育研究センター

CERT®/CC

CERT® Coordination Center

CERT®コーディネーションセンター

CIO

Chief Information Officer

最高情報責任者

CIRC

Computer Incident Response Capability

コンピュータインシデント対応能力

CIRC

Computer Incident Response Center

コンピュータインシデント対応センター

CIRT

Computer Incident Response Team

コンピュータインシデント対応チーム

CISO

Chief Information Security Officer

最高情報セキュリティ責任者

CSIRC

Computer Security Incident Response Capability

コンピュータセキュリティインシデント対応能力

CSIRT

Computer Security Incident Response Team

コンピュータセキュリティインシデント対応チーム

DDoS

Distributed Denial of Service

分散型サービス拒否攻撃

DHS

Department of Homeland Security

米国国土安全保障省

DNS

Domain Name System

ドメインネームシステム

DDoS

DoS Denial of Service

サービス拒否攻撃

FAQ

Frequently Asked Questions

よくある質問

FBI

Federal Bureau of Investigation

連邦捜査局

FIPS

Federal Information Processing Standards

連邦情報処理規格

FIRST

Forum of Incident Response and Security Teams

インシデントレスポンス・セキュリティチームフォーラム※

FISMA

Federal Information Security Management Act

連邦情報セキュリティマネジメント法

GAO

General Accountability Office

米国会計検査院

GFIRST

Government Forum of Incident Response and Security Teams

インシデントレスポンス・セキュリティチーム政府フォーラム※

GRS

General Records Schedule

米国記録スケジュール←要修正

HTTP

Hyper Text Transfer Protocol

ハイパーテキストトランスファープロトコル

IANA

Internet Assigned Numbers Authority

インターネット割当番号公社

IDPS

Intrusion Detection and Prevention System

侵入検知・防止システム

IETF

Internet Engineering Task Force

インターネット技術特別調査委員会

IP

Internet Protocol

インターネットプロトコル

IR

Interagency Report

内部機関報告書

IRC

Internet Relay Chat

インターネットリレーチャット

ISAC

Information Sharing and Analysis Center

セキュリティ情報共有組織

ISP

Internet Service Provider

インターネットサービスプロバイダ

IT

Information Technology

情報技術

ITL

Information Technology Laboratory

情報技術研究所

MAC

Media Access Control

媒体アクセス制御

MOU

Memorandum of Understanding

基本合意書、了解覚書

MSSP

Managed Security Services Provider

マネージドセキュリティサービスプロバイダ

NAT

Network Address Translation

ネットワークアドレス変換

NDA

Non-Disclosure Agreement

秘密保持契約、秘密保持契約書

NIST

National Institute of Standards and Technology

米国国立標準技術研究所

NSRL

National Software Reference Library

ナショナルソフトウェアリファレンスライブラリ

NIST のプロジェクトで、法執行機関やコンピュータ・フォレンジック調査に関与する他の組織が使用する既知のソフトウェア、ファイルプロファイル、ファイル署名のリポジトリを維持・提供している。

NTP

Network Time Protocol

ネットワークタイムプロトコル

NVD

National Vulnerability Database

脆弱性情報データベース

OIG

Office of Inspector General

監察総監室（OIG）は、全米の事業所における監査・調査・評価を通して、事業とマネジメントの問題点を長官及び議会の両方に対して報告し、改善を勧告している。

OMB

Office of Management and Budget

米国行政管理予算局

OS

Operating System

オペレーティングシステム

PII

Personally Identifiable Information

個人情報、個人を特定できる情報

PIN

Personal Identification Number

個人識別番号

※和名不明

付録 E 情報源

以下のリストは、インシデント対応能力の確立と維持に役立つ情報源の一例です。

（訳者注：２０１２年８月現在の情報）

インシデント対応組織

組 織	URL
Anti-PhishingWorkingGroup(APWG) フィッシング対策実務者グループ	http://www.antiphishing.org/
ComputerCrimeandIntellectualPropertySection(CCIPS),U.S. DepartmentofJustice 米国司法省コンピュータ犯罪および知的財産担当課	http://www.cybercrime.gov/
CERT®CoordinationCenter,CarnegieMellonUniversity(CERT®/CC) カーネギーメロン大学 CERT®コーディネーションセンター	http://www.cert.org/
EuropeanNetworkandInformationSecurityAgency(ENISA) 欧州ネットワーク・情報セキュリティ機関	http://www.enisa.europa.eu/activities/cert
ForumofIncidentResponseandSecurityTeams(FIRST) インシデントレスポンス・セキュリティチームフォーラム※	http://www.first.org/
GovernmentForumofIncidentResponseandSecurityTeams(GFIRST) インシデントレスポンス・セキュリティチーム政府フォーラム※	http://www.us-cert.gov/federal/gfirst.html
HighTechnologyCrimeInvestigationAssociation(HTCIA) ハイテクノロジー犯罪捜査協会※	http://www.htcia.org/
InfraGard インフラガード	http://www.infragard.net/
InternetStormCenter(ISC)※	http://isc.sans.edu/
NationalCouncilofISACs※	http://www.isaccouncil.org/
UnitedStatesComputerEmergencyResponseTeam(US-CERT) 米コンピュータ緊急事態対策チーム	http://www.us-cert.gov/

※和名不明記入のあるものは訳者によるもの。

NIST 出版物

出版物名	URL
NISTSP800-53Revision3, 連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策	http://csrc.nist.gov/publications/PubsSPs.html#800-53
NISTSP800-83, マルウェアによるインシデントの防止と対応のためのガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-83
NISTSP800-84, IT 計画および IT 対応能力のためのテスト、トレーニング、演習プログラムのガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-84
NISTSP800-86, 媒体のサニタイズに関するガイドライン	http://csrc.nist.gov/publications/PubsSPs.html#800-86
NISTSP800-92, コンピュータセキュリティログ管理ガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-92
NISTSP800-94, 侵入検知および侵入防止システム（IDPS）に関するガイド	http://csrc.nist.gov/publications/PubsSPs.html#800-94
NISTSP800-115, 情報セキュリティのテスト・評価のための技術的ガイド※	http://csrc.nist.gov/publications/PubsSPs.html#800-115
NISTSP800-128, 情報システムにおけるセキュリティを焦点とした設定・管理ガイド※	http://csrc.nist.gov/publications/PubsSPs.html#800-128

※訳者によるもの。他は IPA による。

インシデントハンドリングに適用されるデータ交換仕様

題 名	説 明	追加情報
AI	AssetIdentification 資産の特定※	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7693
ARF	AssetResultsFormat 資産結果のフォーマット※	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7694
CAPEC	CommonAttackPatternEnumerationandClassification 共通攻撃パターン一覧	http://capec.mitre.org/
CCE	CommonConfigurationEnumeration 共通セキュリティ設定一覧	http://capec.mitre.org/
CEE	CommonEventExpression 共通イベント記述	http://cee.mitre.org/
CPE	CommonPlatformEnumeration 共通プラットフォーム一覧	http://cpe.mitre.org/
CVE	CommonVulnerabilitiesandExposures 共通脆弱性識別子	http://cve.mitre.org/
CVSS	CommonVulnerabilityScoringSystem 共通脆弱性評価システム	http://www.first.org/cvss/cvss-guide
CWE	CommonWeaknessEnumeration 共通脆弱性タイプ一覧	http://cwe.mitre.org/
CybOX	CyberObservableeXpression サイバー攻撃観測記述形式	http://cybox.mitre.org/
MAEC	MalwareAttributeEnumerationandCharacterization マルウェア特徴属性一覧	http://maec.mitre.org/
OCIL	OpenChecklistInteractiveLanguage 対話型チェックリスト記述言語	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7692
OVAL	OpenVulnerabilityAssessmentLanguage セキュリティ検査言語	http://oval.mitre.org/
RFC4765	ntrusionDetectionMessageExchangeFormat(IDMEF) 侵入検知メッセージ交換フォーマット	http://www.ietf.org/rfc/rfc4765.txt
RFC5070	ncidentObjectDescriptionExchangeFormat(IODEF) インシデントオブジェクト記述法と交換フォーマット	http://www.ietf.org/rfc/rfc5070.txt

RFC5901	ExtensionstotheIODEFforReportingPhishing フィッシング報告用の IODEF文書クラス拡張	http://www.ietf.org/rfc/rfc5901.txt
RFC5941	SharingTransactionFraudData 取引詐欺のデータの共有	http://www.ietf.org/rfc/rfc5941.txt
RFC6545	Real-timeInter-networkDefense(RID)	http://www.ietf.org/rfc/rfc6545.txt
RFC6546	TransportofReal-timeInter-network Defense(RID)MessagesoverHTTP/TLS リアルタイムのネットワーク間防衛の交通 HTTP/TLS 経由（RID）のメッセージ	http://www.ietf.org/rfc/rfc6546.txt
SCAP	SecurityContentAutomationProtocol セキュリティ設定共通化手順	http://csrc.nist.gov/publications/PubsSPs.html#SP-800126-Rev.%202
XCCDF	ExtensibleConfigurationChecklistDescriptionFormat セキュリティ設定チェックリスト記述形式	http://csrc.nist.gov/publications/PubsNISTIRs.html#NISTIR-7275-r4

付録Ｆ　よくある質問

組織内のユーザ、システム管理者、情報セキュリティ担当者などから、インシデント対応に関する質問を受けることがあります。以下は、よくある質問（FAQ）です。組織は、この FAQ をカスタマイズしてユーザコミュニティで利用できるようにすることをお勧めします。

1.インシデントとは何ですか ？

一般的に、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、または標準的なコンピュータセキュリティ慣行の違反のことです。インシデントの例としては、以下のようなものがあります。

■ 攻撃者がボットネットに命じて、組織の Web サーバに大量の接続要求を送信し、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。

■ 加害者が機密データへの不正アクセスを取得し、組織が指定された金額を支払わない場合は、詳細を報道機関に公開すると脅迫する。

■ ユーザが、ピアツーピアのファイル共有サービスを通じて、ソフトウェアの違法コピーを他人に提供する。

2. インシデントハンドリングとは ？

インシデントハンドリングとは、インシデントを検知・分析し、インシデントの影響を限定するプロセスのことです。例えば、攻撃者がインターネットを介してシステムに侵入した場合、インシデントハンドリングプロセスはセキュリティ侵害を検知する必要があります。その後、インシデントハンドラーはデータを分析し、攻撃がどの程度深刻なものかを判断します。インシデントハンドラーは、インシデントに優先順位をつけ、インシデントの進行を食い止め、影響を受けたシステムが一刻も早く通常の動作に戻るように行動します。

3. インシデント対応とは何ですか ？

「インシデントハンドリング」と「インシデントレスポンス」という用語は、本書では同義語となります※。

※「インシデントハンドリング」と「インシデントレスポンス」の定義は、大きく異なる。例えば、CERT®/CC は、「インシデントハンドリング」を、インシデントの検出、報告、分析、および対応の全体的なプロセスを指すために使用しているのに対し、「インシデントレスポンス」は、具体的にインシデントの封じ込め、回復、および他者への通知を指しています。詳細については、http://www.cert.org/csirts/csirt_faq.html を参照してください。

4. インシデント対応チームとは何ですか ？

インシデント対応チーム（Computer Security Incident Response Team[CSIRT]とも呼ばれる）は、組織の一部または全部にインシデント対応サービスを提供する役割を担っています。チームは、起こりうるインシデントに関する情報を受け取り、それを調査し、インシデントによる被害を最小限に抑えるための対策を講じます。

5. インシデント対応チームはどのようなサービスを提供しているのですか ？

インシデント対応チームが提供する特定のサービスは、組織によって大きく異なります。ほとんどのチームは、インシデント対応を行うことに加えて、侵入検知システムの監視と管理の責任を負います。また、チームは、新しい脅威に関するアドバイスを配布したり、インシデントの予防と処理における役割についてユーザや IT スタッフを教育したりすることもあります。

6. インシデントは誰に報告すべきですか ？

組織は、内部的にインシデントを報告するための明確な接点（POC）を確立すべきです。組織によっては、すべてのインシデントがインシデント対応チームに直接報告されるように、インシデント対応能力を構築する場合もあれば、IT ヘルプデスクなどの既存のサポート体制を初期の POC に使用する場合もあります。組織は、他のインシデント対応チームなどの外部関係者が、一部のインシデントを報告することを認識すべきです。連邦政府機関は、法律に基づき、すべてのインシデントを米国コンピュータ緊急事態対応チーム（USCERT）に報告することを義務付けられています。すべての組織は、適切なコンピュータ・セキュリティ・インシデント対応チーム（CSIRT）にインシデントを報告することが推奨されています。組織に連絡先となる 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。

7. インシデントはどのように報告されますか ？

ほとんどの組織では、インシデントを報告するための複数の方法があります。活動を報告する人のスキル、インシデントの緊急性、およびインシデントの感度の違いにより、適切な報告方法が

変わる場合があります。緊急事態を報告するための電話番号を設けるべきです。電子メールアドレスは、非公式のインシデント報告に使用される可能性ありますが、正式なインシデント報告にはウェブベースのフォームが適切な場合があります機密情報は、チームが公開した公開鍵を使用して資料を暗号化することで、チームに提供することができます。

8. インシデントを報告する際には、どのような情報を提供すべきでしょうか ？

情報は正確であればあるほど良いです。例えば、ワークステーションがマルウェアに感染しているように見える場合、インシデントレポートには、以下のデータをできるだけ多く含める必要があります。

■ ユーザの名前、ユーザ ID、および連絡先情報（電話番号、電子メールアドレスなど

■ ワークステーションの場所、モデル番号、シリアル番号、ホスト名、および IP アドレス

■ インシデントが発生した日時

■ 感染が発見された後にワークステーションに何が行われたかなど、何が起こったのかを段階的に説明します。この説明は、マルウェアやウィルス対策ソフトの警告などのメッセージの正確な文言を含めて詳細に行う必要があります。

9. インシデント対応チームは、インシデント報告にどのくらいの早さで対応しますか ？

応答時間は、インシデントの種類、影響を受けるリソースとデータの重要度、インシデントの深刻度、影響を受けるリソースに対する既存のサービスレベル契約（SLA)、時間と曜日、チームが処理している他のインシデントなど、いくつかの要因に依存します。一般的に、組織または他の組織に最も大きな被害をもたらす可能性の高いインシデントを処理することが最優先されます。

10. インシデントに関与している人は、いつ法執行機関に連絡すべきですか ？

法執行機関との連絡は、インシデント対応チームのメンバー、最高情報責任者（CIO)、またはその他の指定された関係者によって開始されるべきであり、ユーザ、システム管理者、システム所有者、およびその他の関係者は、連絡を開始すべきではありません。

11. システムが攻撃されていることを知った人はどうすればいいですか ？

直ちにシステムの使用を停止し、インシデント対応チームに連絡しなければなりません。また、発見した人物は、インシデントの初期処理を支援する必要があるかもしれません。例えば、イン

シデントハンドラーが到着するまでの間、システム上の証拠を保護するためにシステムを物理的に監視するなどです。

12. インシデントに関してメディアから連絡を受けた人は、何をすべきですか ？

ある人物は、インシデントと外部関係者に関する組織の方針に従って、メディアの質問に答えることができます。また、その人が組織を代表してインシデントを語る資格がない場合には、その人はインシデントに関するコメントをしてはならず、通報者を組織の広報室に紹介する以外は、インシデントに関するコメントをしてはなりません。これにより、広報室はメディアや一般市民に正確で一貫性のある情報を提供することができます。

付録 G 危機対応のステップ

これは技術専門家が重大なインシデントが発生し、組織にインシデント対応能力がないと考えた場合に実行すべき主な手順のリストです。これは危機に直面したときに、この文書全体を読み通す時間がない人のために何をすべきかの基本的な参考資料としての役割を果たします。

1. すべてを文書化する。

この取り組みには、実行されたすべてのアクション、すべての証拠の断片、ユーザ、システム所有者、およびインシデントに関するその他の人とのすべての会話が含まれます。

2. 援助してくれる同僚を見つける。

例えば、一人が行動を行い、もう一人がそれを文書化するなどです。

3. 証拠を分析して、インシデントが発生したことを確認する。

必要に応じて、証拠をよりよく理解するために追加の調査(インターネットの検索エンジン、ソフトウェアの文書など)を行います。組織内の他の技術専門家に連絡を取り、追加の支援を求めます。

4. 組織内の適切な担当者に通知する。

これには最高情報責任者（CIO)、情報セキュリティ責任者、現地のセキュリティ管理者が含まれるべきです。インシデントの詳細を他の人に話す場合は慎重に行い、知る必要のある人だけに伝え、合理的に安全なコミュニケーションメカニズムを使用します(攻撃者が電子メールサービスに侵入した場合は、インシデントに関する電子メールを送信しないこと)。

5. US-CERT および/またはその他の外部組織に通知し、インシデントへの対応を支援してもらう。

6. インシデントがまだ進行中の場合はインシデントを停止する。

最も一般的な方法は、影響を受けたシステムをネットワークから切断することです。場合によっては、サービス拒否（DoS）攻撃など、インシデントの一部であるネットワークトラフィックを停止するために、ファイアウォールおよびルーターの構成を変更する必要があります。

7. インシデントの証拠を保存する。

影響を受けたシステムのバックアップ（ファイルシステムのバックアップではなく、ディスクイメージのバックアップが望ましい）を作成します。インシデントに関連する証拠を含むログファイルのコピーを作成します。

8. インシデントのすべての影響を一掃する。

この作業には、マルウェア感染、不適切な素材（海賊版ソフトウェアなど)、トロイの木馬ファイル、およびインシデントによってシステムに加えられたその他の変更が含まれます。システムが完全に侵害されている場合は、ゼロからシステムを再構築するか、既知の良好なバックアップから復元します。

9. 悪用されたすべての脆弱性を特定し緩和する。

インシデントは、オペレーティングシステムやアプリケーションの脆弱性を利用して発生した可能性があります。そのような脆弱性を特定し、インシデントが再発しないように排除するか、または緩和することが重要です。

10. 操作が正常に復旧したことを確認する。

インシデントの影響を受けたデータ、アプリケーション、およびその他のサービスが通常の運用に戻ったことを確認してください。

11. 最終報告書を作成する。

この報告書には、インシデント処理プロセスの詳細を記載する必要があります。また、何が起こったのか、正式なインシデント対応能力があれば、どのように状況を処理し、リスクを軽減し、被害をより迅速に限定できたのかについての要約を提供する必要があります。