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

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、ユーザー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**パケットスニファー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イ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ー

■ 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NIST SP 800-84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、NIST SP 800-30, 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、FIPS 199「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、NIST SP 800-137 「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、NIST SP 800-117 Revision 1, 「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」Version 1.2 (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。

■ ユーザー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・手順をユーザーに周知すべきです。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ーと共有し、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
認可されたユーザー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、ユーザー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、またはユーザー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NIST SP 800-83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、ウイルス対策ソフト、ログアナライザなどがあります。インシデントは、ユーザー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

■ アンチウイ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、各カテゴリの前兆と兆候の一般的なソースを示します。

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、ユーザー名（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）。

ソース	説　明
ウイルス対策およびアンチスパムソフトウェア	ウイルス対策ソフトは、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。現在のウイルス対策製品は、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、ユーザー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

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

Source ソース	Description 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

Source ソース	Description 説　明
組織内の人々	ユーザー、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。外部ユーザーは、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、サーバーが利用できないという苦情など、ユーザー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せん。さらに悪いことに、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。サーバー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ーを調査することは、インシデントを処理する準備にもなる。インシデントの処理では、これらのスキルが必要になる。（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、あるいは数ヶ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、NIST SP 800-92「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ー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ーなどです。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 NIST SP 800-86「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、RFC 3067、TERENA's Incident Object Description and Exchange Format Requirements (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。IETF Extended Incident Handling (inch) Working Group (http://www.cert.org/ietf/inch/inch.html)は、TERENAの作業を拡張したRFC 5070, Incident Object Description Exchange Format (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 サーバーに対するDDoS攻撃は、サーバーにアクセスしようとするユーザーの機能を一時的に低下させる可能性があり、公開 Web サーバー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ー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ー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、カテゴリは相互に排他的ではなく、組織は複数のカテゴリ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	**Definition 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の例を示しています。

表 3-4 復旧作業カテゴリ

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。ユーザー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、NIST SP 800-86『Guide to Integrating Forensic Techniques into Incident Response』を参照してください。

※1 NIST SP 800-86「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ーア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、回復には数ヶ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。GRS 24 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、すべての証拠を数ヶ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	**check**
	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。	

	行 動	check
	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、ウイ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、組織のユーザー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ー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。