Special Publication 800-61

Revision 1

National Institute of
Standards and Technology
U.S. Department of Commerce

コンピュータセキュリティ インシデント対応ガイド

米国立標準技術研究所による勧告

Karen Scarfone
Tim Grance
Kelly Masone

この文書は下記団体によって翻訳監修されています。

IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

NRI SECURE TECHNOLOGIES

NIST Special Publication 800-61

Revision 1

コンピュータセキュリティ
インシデント対応ガイド
米国立標準技術研究所による勧告

Karen Scarfone, Tim Grance, Kelly Masone

コンピュータセキュリティ

コンピュータセキュリティ部門
情報技術研究所
米国立標準技術研究所
Gaithersburg, MD 20899-8930

2008**年**3**月**

米国商務省 長官

Carlos M. Gutierrez

米国立標準技術研究所 所長

James M. Turner

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: National Institute of Standards and Technology、以下、NIST と称す）の情報技術ラボラトリ（ITL:Information Technology Laboratory）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る。情報技術ラボラトリは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシーを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動ならびに産業界、政府機関および教育機関との共同活動について報告する。

米国立標準技術研究所 Special Publication 800-61 Revision 1

米国立標準技術研究所 Special Publication 800-61 Rev. 1、147ページ（2008年3月）

本文書中で特定される商業的組織、装置、資料は、実験手順または概念を適切に説明するためのものである。したがって、NIST による推薦または保証を意味するものではなく、これらの組織、資料、または装置が、その目的に関して得られる最善のものであると意味しているわけでもない。

本文書は、原典に沿ってできるだけ忠実に翻訳するよう努めていますが、完全に正確であることを保証するものではありません。翻訳監修主体は本レポートに記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。

謝辞

本書の執筆陣であるKaren Scarfone(NIST)、Tim Grance(NIST)、およびKelly Masone(Booz Allen Hamilton)は、本書の草稿を見直し、技術的内容に関する助言を与えてくれた方々に深く感謝する。とりわけ、US-CERT(United States Computer Emergency Readiness Team)を支援するDon Benack、US-CERTのMike Witt、およびNISTのMurugiah Souppayaに感謝の意を表する。また、Wells FargoのDean Farrington、BB&TのJim Duncan、およびthe University at BuffaloのJeff Murphyをはじめ、本書に対するフィードバックを提供してくれたパブリックコメントレビューアにも深く感謝する。

本書執筆陣は、また、本書の原作に貢献してくれた方々にも感謝の意を表する。とりわけ、本ドキュメントの作成全体にわたって洞察に満ちた鋭い助言を与えてくれたNISTのRick Ayers、Chad Bloomquist、Vincent Hu、Peter Mell、Scott Rose、Murugiah Souppaya、Gary Stoneburner、John Wack、およびBooz Allen Hamilton社のDebra Banning、Pete Coleman、Alexis Feringa、Tracee Glass、Kevin Kuhlkin、Bryan Laird、Chris Manteuffel、Ron Ritchey、Marc Stevensと、本ドキュメントの草稿を作成してくれたRon BanerjeeとGene Schultzに感謝する。さらに、セキュリティの専門家であるTom Baxter (NASA)、Mark Bruhn (インディアナ大学)、Brian Carrier (パデュー大学CERIAS)、Eoghan Casey、Johnny Davis、Jr. (復員軍人省)、Dean Farrington (ウェルズファーゴ銀行)、John Hale (タルサ大学)、Georgia Killcrece (CERT®/CC)、Barbara Laswell (CERT®/CC)、Pascal Meunier (パデュー大学CERIAS)、Todd O'Boyle (MITRE)、Marc Rogers (パデュー大学CERIAS)、Steve Romig (オハイオ州立大学)、Robin Ruefle (CERT®/CC)、Gene Schultz (ローレンスバークレイ国立研究所)、Michael Smith (FedCIRC)、Holt Sorenson、Eugene Spafford (パデュー大学CERIAS)、Ken van WykおよびMark Zajicek (CERT®/CC) 、ならびに財務省の担当官にも、貴重なコメントと提案をいただいたことに感謝したい。

目次

付録

図

表

要旨

近年、コンピュータセキュリティインシデントへの対応は、情報技術（IT: Inforamtion Technology）プログラムの重要な要素になってきた。セキュリティ関連の脅威は、その数や種類が増えただけでなく、損害や破壊の規模も大きくなっている。セキュリティに関連する新しいタイプの事件もたびたび発生している。リスク評価の結果を基に予防的対策を実施することで、事件の数を減らすことは可能だが、すべての事件を予防することはできない。そのため、事件を素早く発見し、損失や破壊を最小限に抑え、悪用された脆弱性に対処し、コンピューティングサービスを復旧するためには、インシデント対応能力が必要である。これを受けて、このドキュメントでは、事件処理、特に事件に関連したデータを分析し、各事件への適切な対応を決定するためのガイドラインを提供する。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、アプリケーションには依存していない。

インシデント対応の効果的な実施は複雑な業務であるため、優れたインシデント対応能力を確立するには、十分な計画とリソースが必要である。また、侵入検知／防止システム（Intrusion Detection and Prevention System: 以下IDPSと称する）などの仕組みを使って継続的に脅威を監視することが必要不可欠である。さらに、事件が、現在および将来にわたってもたらす業務への影響を評価するための、明確な手順を確立することは重要であり、また効果的にデータを収集、分析、報告する方法を構築しておくことも、同様に重要である。ほかの内部グループ（人事部、法務部など）や、外部グループ（ほかのインシデント対応チーム、法執行機関など）との関係を構築して、適切なコミュニケーション手段を確立することも非常に重要である。

このドキュメントは、従来から常設されているインシデント対応チームと、最近組織化されたインシデント対応チームの両方に役立つことを目的としている。また、各組織が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、事件を効率的かつ効果的に処理するのを支援する。具体的には、次の項目について説明する。

+ コンピュータセキュリティインシデント対応能力の組織化
  - インシデント対応ポリシーと手順の確立
  - 外部委託の検討も含めた、インシデント対応チームの編成
  - 他のどのような人々にインシデント対応への参加を要請するか
+ 事件処理(初期の準備フェーズから、事件後に教訓を生かすフェーズまで)
+ 特定の種類の事件処理
  – **サービス不能（DoS : Denial of Service)**—リソースを枯渇させることで、ネットワーク、システム、アプリケーションの正規の使用を妨害または阻害する攻撃。
  – **悪意のコード**—ウイルス、ワーム、トロイの木馬など、ホストに感染する、悪意のコード。
  – **不正アクセス**—許可なくネットワーク、システム、アプリケーション、データ等のリソースに論理的または物理的にアクセスすること。
  – **不適切な使用**—ネットワークまたはコンピュータの利用規定に違反すること。
  – **複合要素**— 1つの事件で2つ以上の事件を包含しているもの。たとえば、悪意のコード

に感染することでホストへの不正アクセスが可能となり、さらにほかのホストへの不正アクセスが可能になってしまうなど。

以降の要件や推奨事項を実施することで、国の諸官庁や機関は、効率的かつ効果的に事件に対応できるようになる。

正式なインシデント対応能力を作成、計画、運用すること。各政府機関は、連邦法により、国土安全保障省のUS-CERT（United States Computer Emergency Readiness Team：米国のコンピュータ緊急対応チーム）に事件を報告するよう義務付けられている。

2002年施行の連邦情報セキュリティマネジメント法（FISMA: Federal Information Security Management Act、以下FISMA と称す）は、政府機関が、インシデント対応能力を確立することを義務づけている。また、政府の各民間機関は、US-CERTとの一次および二次の窓口(POC: Point Of Contact)を指定し、すべての事件を報告し、是正措置と影響を内部的に文書化しなければならない。各機関には、これらの要求を満たす具体的な方法を決める責任がある。

インシデント対応能力を確立するには、次の活動を実施する。

+ インシデント対応ポリシーおよび計画を作成する
+ インシデント対応ポリシーに基づき、事件処理と報告を実施する手順を作成する
+ 事件に関して外部組織と連絡するためのガイドラインを作成する
+ チーム構成と要員配置モデルを選択する
+ インシデント対応チームと、内部グループ(法務部など)や外部グループ(法執行機関)との間で関係を樹立する
+ インシデント対応チームが提供するサービスを決定する
+ インシデント対応チームの要員配置とトレーニングを行う

ネットワーク、システム、アプリケーションのセキュリティを効果的に高めることで、事件の頻度を減らすこと。

通常、問題が発生した後で対処するよりも、問題を予防するほうが低いコストで済み効果も大きい。よって、事件の予防は、インシデント対応能力を補完する重要な事項である。セキュリティコントロールが十分でないと、多数の事件が発生する可能性があるため、対応するためのリソースや能力が不足してしまう。その結果、復旧が遅れたり不完全なものとなり、被害が拡大し、サービスやデータが利用できない期間が長くなってしまう。ネットワーク、システム、アプリケーションのセキュリティを積極的に維持するための、十分なインシデント対応能力とリソースがあれば、事件処理をより効果的に実行でき、インシデント対応チームは深刻な事件の処理に集中することができる。

事件に関してほかの組織とやり取りするためのガイドラインを文書化すること。

事件処理の際、ほかのインシデント対応チーム、法執行機関、マスコミ、ベンダー、外部の被害者など、外部の関係者と連絡を取らなくてはならない場合がある。このような連絡はすみやかに行う必要があることが多いため、適切な情報だけを適当な関係者と共有できるように、あらかじ

め連絡のガイドラインを定めておくべきである。機密情報が不適切に漏れてしまうと、事件そのものよりも大きな破壊や経済的な損失が起こる可能性がある。内外の連絡先と予備連絡先の一覧を作成して保守することで、関係者間で容易かつ迅速に連絡を取ることができるようになる。

事件の検知と分析の重要性を組織全体に徹底すること。

1つの組織でも、毎日何千・何百万という事件の兆候が見られる場合があり、これがログやコンピュータセキュリティソフトウェアにより記録される。データの初期分析を行って、人間が確認すべき事象を選別するには、自動化が必要である。分析処理を自動化する上で、イベント相関処理ソフトウェアとログの一元化が非常に有効である。しかし、この処理の有効性は、処理対象のデータの質に依存する。よって、ログやセキュリティソフトウェアにより適切な情報が収集され、データを定期的にレビューできるように、ログ取得の標準と手順を規定しておくべきである。

事件に優先順位を付けるための、文書化したガイドラインを作成すること。

各事件の処理に優先順位を付けることは、インシデント対応プロセスにおいて、非常に重要な決定事項である。以下の内容に基づき事件に優先順位を付ける。

+ 影響を受けるリソース(たとえば、公開ウェブサーバ、ユーザのワークステーションなど)の重要度

+ 現在または将来的な、技術面での事件の影響(たとえばrootの奪取、データ破壊など)

影響を受けるリソースと、事件による現在および将来的な技術的影響を、合わせて検討することで、事件の業務への影響が決まる。たとえば、ユーザのワークステーションにおけるデータ破壊の場合は、生産性が若干落ちるだけで済むかもしれないが、公開ウェブサーバのroot奪取は、収益、生産性、サービスへのアクセス、評判に大きな損害をもたらし、機密データ(クレジットカード番号、社会保障番号など)が漏れてしまうこともある。

事件処理を行う者は、事件の間は非常に大きなストレスにさらされるため、優先順位付けのプロセスを明確にしておくことが重要である。各組織は、インシデント対応チームがさまざまな状況でどのように行動すべきかを決定し、適切な行動と最大応答時間を規定した、サービス内容合意書(SLA: Service Level Agreement)を作成すべきである。インシデント対応プログラムの一部を外部委託する組織では、この文書が特に有益である。ガイドラインを文書化することが、より迅速で一貫した意思決定を促進する。

事件から得た教訓を生かすこと。

大きな事件を処理した後は、反省会を開催し、事件処理プロセスがどれだけ有効だったかを評価して、現在のセキュリティコントロールと訓練にどのような改善が必要かを明確にする。反省会は、重要度の低い事件に対しても定期的に開催する。反省会から集めた情報を使って、セキュリティの脆弱性、ポリシーと手順の不備を体系的に探す。対処済みの事件について作成された追跡レポートは、証拠として重要なだけでなく、将来事件を処理する際の参考や、インシデント対応チームの新しいメンバーの訓練用としても重要である。発生した各事件の詳細情報が格納された事件データベースも、事件処理担当者にとっては貴重な情報源である。

大規模な事件の際には、状況に応じた判断を心がけること。

大規模な事件の処理は複雑であるため、状況に応じて判断するのは非常に難しい。インシデント対応では、組織内の多数の人間が役割を果たし、さまざまな外部グループと迅速かつ効率的に連

絡を取る必要がある。正しく判断して実行できるように、すべての情報を収集、編成、分析することは簡単なことではない。状況に応じて判断する上で重要なことは、大規模な事件の処理に備えておくことであり、これには以下の項目が含まれる。

+ 組織内(たとえば最高情報責任者(CIO)、情報セキュリティ部門長、ITサポート部門長、業務継続計画部門長など)や組織外(たとえばUS-CERT、インシデント対応組織、ほかの組織の同様の部門)のさまざまな個人やグループについて、業務時間内および業務時間外の連絡手段や通報手段を確立し、文書化や維持、演習を行う。

+ 業務への影響を踏まえ、インシデント対応活動に優先順位を付けるためのガイドラインを計画して文書化する。

+事件処理担当者やほかの関係者から情報を収集し、情報が必要な関係者に適切な情報を配布する責任をもつ、1人以上のインシデント対応リーダーを任命する。

+ 定期的に演習とシミュレーションを行うことで、大規模な事件の処理に関する訓練を行う。大規模な事件はまれにしか発生しないため、インシデント対応チームでは、大規模な事件を効果的に処理するための経験が不足しがちである。

1. はじめに

1.1. 権限

米国国立標準技術研究所（NIST）は、2002年施行のFISMA、公法107-347に基づくその法的責任を果たすために、この文書を作成した。

NISTは、すべての連邦政府機関の運営および資産に適切な情報セキュリティをもたらすために、最低限の要求事項を含んだ標準およびガイドラインを作成する責務があるが、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局による通達（OMB Circular: Office of Management and Budget Circular、以下OMB Circular と称す）A-130、第8b(3)項、『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項に一致しており、これはA-130の付録IV「重要部門の分析」で分析されているとおりである。

このガイドラインは連邦政府機関が使用する目的で作成されている。非政府組織が自由意志で使用することもでき、著作権の制約はない（NISTへの帰属が望ましいが）。

本文書における一切は、商務長官が法的権威に基づき連邦政府に対して義務および拘束力を与えた標準および指針を否定するものではない。また、これらの指針は、商務長官、OMB局長、または他のすべての連邦政府当局者の既存の権威に変更を加えたり、これらに取って代わるものと解釈してはならない。

1.2. 目的および適用範囲

本書は、事件に効果的かつ効率的に対応するための実用的な手引きとなることで、各組織が情報セキュリティインシデントによるリスクを軽減するのに役立てることを意図したものである。本書は、効果的なインシデント対応プログラムの策定に関するガイドラインを含んでいるが、第一の焦点は、あくまでもセキュリティ事故の検知、分析、優先順位付けおよび処理にある。各機関は、固有のセキュリティ要件や業務要件に合うように、推奨されるガイドラインや対処方法を調整することをお勧めする。

1.3. 対象とする読者

このドキュメントは、セキュリティインシデントに備えて対応する責任を持った、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）、システム管理者と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向けに作成されている。

1.4. ドキュメントの構成

本書は、大きく7つのセクションに分かれている。セクション2では、インシデント対応の必要性と、インシデント対応チームの構成の概略を説明し、事件処理に参加する可能性がある、組織内のほかのグループを明らかにする。セクション3では、基本的な事件処理ステップを再確認し、事件処理、特に事件の検知と分析をより効果的に実施するためのアドバイスを提供する。セクション4から8では、サービス不能(DoS)、悪意のコード、不正アクセス、不適切な使用、複合要素の5種類の事件を処理する上での、具体的な推奨内容を説明する。

付録Aは、インシデント対応の推奨事項をまとめたものである。付録Bには、インシデント対応の

シナリオと、インシデント対応の訓練で使用する質問が含まれている。付録Cは、各事件で収集すべきデータフィールドの一覧である。付録Dと付録Eは、それぞれ用語集と頭字語の一覧である。付録Fは出版物の一覧、付録Gはオンラインのツールとリソースの一覧である。これらのリソースは、インシデント対応の計画と実行の際に役立つ。付録Hには、インシデント対応についてよく聞かれる質問を挙げてある。付録Iは、セキュリティインシデントに関連する危機に対処する際に従うべき、主なステップの一覧である。付録Jは、US-CERTが提供する、インシデント報告に関する手引きである。

2. コンピュータセキュリティインシデント対応能力の組織化

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)を組織化するためには、いくつかの大きな判断や行動が必要となる。まず考慮すべき点は、「事件」という用語の範囲が明確になるように、この用語に対し組織固有の定義を与えることである。インシデント対応チームがどのようなサービスを提供するかを決め、それを提供するためにはどのチーム構成やモデルが合っているかを検討し、1つ以上のインシデント対応チームを選択して実際に編成する。インシデント対応を一貫した方法で効果的かつ効率的に実施するためには、チームを編成する際に、インシデント対応ポリシーと計画、および手順を作成することが重要である。ポリシーと計画、および手順には、組織内のほかのチームや、法執行機関、マスコミ、ほかのインシデント対応組織など、外部の関係者との間のやりとりを反映させる。このセクションは、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手引きとなるだけでなく、現在の能力を維持し向上させるためのアドバイスも提供する。

2.1. 事象と事件

「事象」とは、システムまたはネットワークで識別できるあらゆる出来事のことをいう。事象には、ユーザによるファイル共有への接続、サーバへのウェブページ受信要求、ユーザによる電子メール(Eメール)の送信、ファイアウォールによる接続のブロックなどが含まれる。「有害事象」とは、システムクラッシュ、ネットワークパケットの氾濫、システム特権の不正利用、機密データへの不正アクセス、データを破壊する悪意のコードの実行といった、ネガティブな結果を伴う事象である。このガイドでは、コンピュータセキュリティに関する有害事象だけを扱い、自然災害や停電などによる有害事象は対象としない。

「コンピュータセキュリティインシデント（事件）」とは、組織が定めるセキュリティポリシーやコンピュータの利用規定に対する違反行為[1] または差し迫った脅威[2]、あるいは、標準的なセキュリティ活動に対する違反行為または差し迫った脅威を示す。以下にインシデント[3]の例を示す。

+ サービス不能
  - アタッカーが特殊なパケットをウェブサーバに送信し、クラッシュさせる。
  - アタッカーが、外部にある侵入済みの数百ものワークステーションに対し、組織のネットワークに向けて、可能な限り大量のICMP (Internet Control Message Protocol)要求を送信するように指示する。
+ 悪意のコード
  - ワームが、オープンになっているファイル共有を使って、組織内の何百ものワークステーションに急速に感染する。
  - ウイルス対策ソフトウェアベンダーから、新種のウイルスがインターネットで電子メー

1 コンピュータセキュリティポリシーへの違反と利用規定への違反は、同じ方法を使って検出できることが多い。通常、インシデント対応チームは、コンピュータの利用規定への違反を多数処理することが多い。この問題については、セクション7で詳しく説明する。

2 「差し迫ったの脅威」とは、特定の事件が起きようとしているという根拠を、組織が持っているという状況を指す。たとえば、ウイルス対策ソフトウェアの保守を行っている者が、新種のワームがインターネット上で急速に広まっているという警告を、ソフトウェアベンダーから受け取った場合などである。

3 以降では、「事件(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」は同じものを指す。

ルを通じて急速に広まっているという警告を受け取る。このウイルスは、組織内のホストの多くで存在する脆弱性を利用している。過去のウイルス対策事件を踏まえると、この新種のウイルスは、3時間以内にいくつかのホストに感染すると予想される。

+ 不正アクセス
  - アタッカーが、エクスプロイト(exploit)ツールを実行し、サーバのパスワードファイルにアクセスする。
  - 加害者が、システム(およびシステム内の機密情報)への管理者レベルの不正アクセスを取得し、指定した金額を支払わなければ、侵入の詳細をマスコミに公表すると被害者を脅迫する。
+ 不適切な使用
  - 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、ソフトウェアの不正コピーを他人に渡す。
  - だれかがほかの人を電子メールで脅迫する。

2.2. インシデント対応の必要性

インシデント対応が必要になってきた理由は、攻撃により個人データや業務データが頻繁に損なわれるためである。ウイルス、ワーム、トロイの木馬などの悪意のコードによる事件は、世界中の何百万ものシステムとネットワークを麻痺させ、大きな損害を与えた。また、国家保障に対する関心の高まりと、個人情報の流出に対する懸念から、コンピュータベースのアタックによる影響への意識が高まっている。これらの事象(およびその他多数の事象)が引き金となり、コンピュータセキュリティの防御が破られた場合に、迅速かつ効率的に対応するのが日常的になっている。連邦政府、民間部門、学術機関においては、このような脅威に対処するために、コンピュータセキュリティインシデント対応の考え方を広く受け入れて実施するようになった。

インシデント対応能力を持つことのメリットは以下のとおりである。

+ 事件に体系的に対応し、適切な手順がとられる。
+ 担当者が、迅速かつ効率的にセキュリティインシデントから復旧するのを助け、情報の損失や盗難、サービスの中断を最小限に抑える。
+ 事件処理の際に得た情報を使って、将来の事件に備え、システムとデータを強力に防護する。
+ 事件に伴って発生する可能性がある法的な問題を正しく扱う。

業務上の理由でインシデント対応能力を確立する以外に、政府の諸官庁や機関は、情報セキュリティの脅威に対して組織的かつ効果的に防御することを定めた法律、規制、ポリシーに準拠する必要がある。主なものを以下に示す。

+ OMB Circular A-130の付録III[4]では、政府機関が「システムでセキュリティインシデントが起きた場合に、ユーザを支援したり、共通の脆弱性や脅威に関する情報を共有する機能を有すること。また、この機能が、ほかの組織との情報の共有を可能とし...政府機関が司法省の指導に沿って適切な法的行動を起こすことができるようにするための機能であること。」

4 http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

となっている。

+ FISMA[5]は、各機関が「セキュリティインシデントを検知、報告し、インシデントに対応するための手順」を有することを義務付けており、以下の目的で政府情報セキュリティインシデントセンターを開設している。
  - 「機関の情報システムのオペレータに対し、技術支援をタイムリーに提供する…情報セキュリティインシデントの検知と処理に関する指導も含む…
  - 情報セキュリティを脅かす事件に関する情報を収集して分析する…
  - 機関の情報システムのオペレータに対し、現在および将来起こりうる情報セキュリティの脅威や脆弱性について通知する…。」

+ 連邦情報処理基準（FIPS: Federal Information Processing Standards、以下FIPSと称す）200『連邦政府の情報および情報システムの最低セキュリティ要件(Minimum Security Requirements for Federal Information and Information Systems)』[6]は、連邦政府の情報および情報システムの最低セキュリティ要件(インシデント対応も含む)を規定するものである。それらのセキュリティ要件は、NIST SP 800-53『連邦政府情報システムにおける推奨セキュリティ管理策(Recommended Security Controls for Federal Information Systems)』に記載されている。

+ OMB Memorandum M-07-16『個人情報の侵害に対する保護および対応(Safeguarding Against and Responding to the Breach of Personally Identifiable Information)』[7]は、個人情報にかか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する。

2.3. インシデント対応のポリシー、計画および手順の作成

ここでは、インシデント対応に関するポリシーと計画、および手順について説明する。特に、マスコミ、法執行機関、事件報告組織などの外部の関係者とのやりとりについて重点的に説明する。

2.3.1. ポリシーの要素

インシデント対応を左右するポリシーは、組織ごとに非常に違ったものになる。ただし、組織がインシデント対応能力を自前で用意するか外部委託するかにかかわらず、ほとんどのポリシーには、以下のような重要な要素が含まれる。[8]

+ マネジメント層の責任表明
+ ポリシーの目的と目標
+ ポリシーの範囲(だれに、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、それらのインシデントが自組織にもたらす結果。
+ 組織構造と、役割、責任、権限レベルを表す記述。インシデント対応チームが装置を押収または接続を切断したり、疑いのある活動を監視したりする権限と、ある種の事件について報告する義務も含めること。

---

5 http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
6 http://csrc.nist.gov/publications/PubsSPs.html
7 http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
8 付録Gに、インシデント対応ポリシーと手続きフォームの例が掲載されているウェブサイトへのポインターを示す。

+ 事件の優先順位付けまたは重大さの格付け。

+ 実施評価(セクション3.4.2で説明)。

+ 報告フォームとコンタクトフォーム

2.3.2. 計画の要素

組織にとって、インシデントに対応するための正式なアプローチを確立することは、重要である。このアプローチは、的が絞られていて調整がなされたものであるべきである。このような機能を効果的に実施するには、インシデント対応計画の策定が必要になる。インシデント対応計画は、インシデント対応機能を実施するための手引きを提供し、インシデント対応機能を組織全体に適合するための高いレベルのアプローチを提供する。それぞれの組織は、自身のミッション、組織の規模、組織の構造、および組織の機能に見合った独自の要求事項を満たすための、計画を策定しなければならない。この計画では、インシデント対応機能を効果的に維持・熟成させるためのリソースおよびマネジメント層のサポートに関して、明確に記述しなければならない。インシデント対応計画には、以下のものが含まれる。

+ ミッション

+ 戦略および目標

+ 上級管理職による承認

+ インシデント対応への組織的な取り組み

+ インシデント対応チームによる他の職員への連絡方法

+ インシデント対応機能を測定するためのマトリックス

+ インシデント対応機能を熟成させるための手引き

+ インシデント対応計画をどのようにして組織全体に適合させるか

インシデント対応にかかわる組織のミッション、戦略および目標を明確にすることにより、インシデント対応機能の構造を決定しやすくなる。このような構造に関しては、インシデント対応計画の中で論じるべきである。異なる種類のインシデント対応構造に関しては、セクション2.4.1で説明する。

組織が作成し、マネジメント層の承認を得たインシデント対応計画は、実施され定期的（少なくとも年に1回）に見直される。この見直しにより組織は、インシデント対応機能の成熟を確実にし、インシデント対応に関する組織の目標を達成できるようになる。

2.3.3. 手順の要素

各手順は、インシデント対応のポリシーと計画を踏まえること。標準運用手順(SOP: Standard Operating Procedures)は、インシデント対応チームが使用するものであり、特定の技術手順、手法、

チェックリスト、フォームが記述されている。SOPは広範囲かつ詳細なものとし、対応活動には組織の優先順位を反映させるようにする。また、対応が標準化されていることで、誤り(特に事件処理のペースやストレスからくる誤り)を減らすことができる。SOPはテストを行い、正確さと有用性を検証した後、チームの全メンバーに配布する。SOPの利用者にはトレーニングを実施すべきであるが、その際SOPドキュメントを教育ツールとして使用してもよい。我々が提案するSOPの要素をセクション3～8に示す。

2.3.4. 外部の関係者との情報共有

組織は、外部の関係者に事件について連絡しなくてはならない場合がある。少なくとも連邦政府機関は、事件が発生した場合に、US-CERT®に報告しなければならない。また、場合によっては、組織が他の関係者にも連絡することがある （たとえば、CERT® コーディネーションセンター(CERT® /CC)への事件の報告、法執行機関への連絡、マスコミの問い合わせへの対応など）。インシデント処理担当者は、組織のインターネットサービスプロバイダ(ISP)、アタッカーが使用しているISP、脆弱性があるソフトウェアのベンダー、担当者が理解しようとしている異常な活動に詳しいインシデント対応チームなど、その他の関係者と事件について話し合わなくてはならない場合もある。さまざまな理由から、事件の詳細を外部の組織に連絡したい(または連絡しなくてはならない)ことがある。インシデント対応チームは、事件が起きる前に、組織の広報部、法務部、マネジメント層と詳細に話し合い、情報共有に関するポリシーと手順を確立しておく必要がある。そうしないと、事件に関する機密情報が権限のない者に提供され、事件そのものよりも大きな破壊や経済的な損失が起こる可能性がある。チームは、責任の所在の明確化と証拠を残す目的で、外部関係者とのすべての連絡およびやりとりの内容を文書化するべきである。

以降のセクションは、実際の事件の処理に関する、さまざまな種類の外部関係者との連絡についての手引きである。外部の連絡先には、マスコミ、法執行機関、事件報告組織が含まれる。図2-1は、組織が連絡しなくてはならない外部関係者を示す。矢印は、連絡の方向を示す。たとえば、ソフトウェアベンダーには組織の側から連絡する。双方向の矢印は、どちらから連絡してもよいことを示す。

図2-1 事件に関連する外部関係者との連絡

2.3.4.1. マスコミ

マスコミへの対応は、インシデント対応の重要な部分である。インシデント対応チームは、マスコミとのやりとりや情報の公開について、組織のポリシーに合った手順を確立しておく必要があ

る。[9]一本化したマスコミ窓口と1つ以上の予備の窓口を設け、そこを通じて事件について話し合ったほうが有益であることが多い。マスコミに連絡する担当者を設ける際には、以下の点を考慮する(これらの事項は、担当者以外の者がマスコミに連絡する際にも考慮すべき事項である)。

+ 事件に関してマスコミとやり取りするための訓練をする。訓練には以下の内容を盛り込む。
  - 対策の技術的な詳細(ファイアウォールがどのプロトコルを通すかなど)といった機密情報を公開しないことの重要性。このような情報は、アタッカー予備軍に利用される可能性がある。
  - 重要な情報を、きちんと効果的に一般大衆に伝えることの、肯定的な側面。
+ マスコミと話し合う前に、事件に関する問題と機密性について、マスコミの窓口に手短に説明する手順を確立する。
+ 事件処理の訓練の中で、模擬的にインタビューと記者会見を行う。以下に示すのは、マスコミ窓口への質問内容の例である。
  - 攻撃したのはだれか
  - なぜ攻撃が行われたか
  - いつ起きたか
  - どのようにして攻撃されたか
  - この事件の被害範囲はどの程度か
  - この事件は、セキュリティ対策がずさんだったために起きたのか
  - 何が起きたかを調べるために、また、将来における再発を防止するために、どのような手順を踏んでいるのか
  - この事件の影響は
  - なんらかの個人情報が流出したか
  - この事件の経済的な損失はどの程度か

2.3.4.2. 法執行機関

セキュリティ関連の事件が有罪判決に結びつかない理由のひとつは、各組織が法執行機関に適切に連絡しないためである。事件を調査する法執行機関としては、政府の調査機関(連邦捜査局(FBI: Federal Bureau of Investigation)、米国財務省検察局(U.S. Secret Service)など)、地区検察局、各州の法執行機関、地方(郡)の法施行機関など、いくつかのレベルがある。また、各機関には監察総監室(OIG: Office of Inspector General)があり、自らの機関内の違法を調査している。インシデント対応チームは、事件が発生する前に、さまざまな法執行機関の担当者と面識を持ち、事件を報告する条件、その方法、どのような証拠を収集するか、それをどのように収集するかについて話し合っておくべきである。

9 たとえば、マスコミとの事件に関する話し合いのすべてに、広報部と法務部のメンバーが参加するといったことを手順化する。

法執行機関に連絡する際には、法の定めと組織の手順にのっとって、指定の担当者を通じて連絡すること。多くの組織では、法執行機関の一次窓口として、インシデント対応チームのだれか一人を指名することを好む。窓口となった者は、関連するすべての法執行機関の報告手順に精通し、どの機関に連絡すればよいかをすぐに助言できるようにしておく必要がある。一般に、複数の機関に連絡すべきではない。もし複数の機関に連絡すると、管轄区域上の衝突が発生する可能性がある。そこで、管轄区域上の問題にはどのようなものがあるかを理解しておく必要がある(地勢的な配置を例にすると、ある州を本拠地とする組織が、別の州にサーバを持っており、さらに別の州にいるアタッカーが、また別の州にあるシステムを遠隔操作してそのサーバを攻撃したような場合)。

2.3.4.3. インシデント報告組織

FISMAによれば、政府機関は事件をUS-CERT [10]に報告するよう義務付けられている。US-CERTは、省庁横断的なインシデント対応の権限を持っており、政府民間機関の事件処理作業を支援する。US-CERTは、各機関の既存の対応チームを置き換えるものではないが、事件を扱う活動の中心となることで、政府民間機関の作業を支援する。US-CERTは、すべての機関から提供された情報を分析し、攻撃の傾向や前兆を探す。傾向や前兆は、1つの組織のデータをレビューするよりも、多数の組織のデータをレビューしたほうが見つけやすい。

政府の各機関は、US-CERTとの一次窓口と二次窓口を指定し、すべての事件を報告し、是正措置と影響を内部的に文書化しなければならない。各機関には、これらの要求を満たす具体的な方法を決定する責任があるため、誰がどのように事件を報告するかを決めたポリシーを作成する。US-CERTへの事件の報告は、オンラインでできるようになっている [11] US-CERTへの事件の報告に関する情報（報告の要件、事件の種類、および報告期限など）は、本書の付録Jに記載している。また、これらの情報は、US-CERTのウェブサイトでも公開している。[12] 報告義務の例としては、システムのroot奪取により不正アクセスが行われた場合(検知後1時間以内)や、取り扱いに注意を要さないシステムがウイルスに感染した場合(検知後24時間以内)がある。すべての政府機関は、インシデント対応手順を確実にUS-CERTの報告義務に準拠させ、それらの手順を守ること。これは、政府機関で単に義務付けられているというだけでなく、各機関にとっても有益である。なぜなら、各機関から有益なデータが収集できれば、US-CERTは各機関に対してより有益な情報を提供できるためである。

すべての組織において、事件が発生した場合には、US-CERTに報告することを奨励する。組織内に連絡すべきCSIRTが存在しない場合は、以下のような組織に連絡することができる。

+ IAIP(**Information Analysis Infrastructure Protection：情報分析インフラ防護**) [13] ーIAIPはDHS (Department of Homeland Security：国土安全保障省)の一部であるため、米国の重要なインフラストラクチャに対する脅威に関心を持っている。IAIPへの事件の報告は、NICC(National Infrastructure Coordinating Center)への電話連絡または電子メールを介して行うことができる。[14]

+ **CERT®/CC (CERT® Coordination Center：CERT®コーディネーションセンター)** [15]
CERT®/CCは以前はCERTと呼ばれており、カーネギーメロン大学内にある。この民間団体は、インターネット関係のコンピュータセキュリティインシデントに関心を持っている。

10 http://www.us-cert.gov/
11 https://forms.us-cert.gov/report/index.php
12 http://www.us-cert.gov/federal/reportingRequirements.html
13 以前は国家インフラ保護センター(NIPC: National Infrastructure Protection Center)と呼ばれていた。
14 NICCへの連絡先は以下の通りである。E-mail address：nicc@dhs.gov　Tel：202-282-9201
15 http://www.cert.org

CERT®/CCは、オンラインで事件を報告するための事件報告システムを提供している。[16]

+ **ISAC (Information Sharing and Analysis Centers：情報共有分析センター)** [17] 1998年の大統領令(PDD) 63により、情報共有分析センターと呼ばれる業界固有の民間部門のグループの設立が奨励された。ISACの目的は、コンピュータセキュリティ関連の重要な情報をメンバー間で共有することである。電力、金融サービス、情報技術、電気通信といった産業部門において、多数のISACが設立された。

組織は、事件の報告に加えて、是正措置を内部的に文書化しなければならない。文書化に関する追加情報は、NIST SP 800-53 Revision 2のセクション3.5に記載されている。

2.3.4.4. その他の外部関係者

前述のように組織は、事件について、他のいくつかのグループと協議を行いたいと思うことがある。それらのグループには以下の者が含まれる。

+ **組織が加入するISP** ネットワークベースのDoS攻撃の場合には、攻撃をブロックしたり、送信元を追跡したりする際に、加入しているISPの助けが必要になる場合がある。

+ **攻撃元アドレスの所有者** アタッカーが外部組織のIPアドレス空間から攻撃している場合は、事件処理担当者はその組織の指定されたセキュリティ窓口に連絡し、活動について警告したり、証拠を収集するよう依頼する。そのアドレス空間の所有者がアタッカーであったり、アタッカーと関係があったりする場合もあるため、処理担当者は、その外部組織となじみがない場合には注意すること。

+ **ソフトウェアベンダー** 状況によっては、事件処理担当者は疑いのある活動について、ソフトウェアベンダーと話をすることになる。その中で、特定のログエントリーの重要性や、特定の侵入検知シグネチャで既知の誤検知がないかを質問する。その際、事件に関する情報はできるだけ公開しないようにする。ソフトウェアの未知の脆弱性によりサーバに侵入された場合などは、多くの情報を提供しなくてはならないこともある。事件処理担当者は、新しい脆弱性に対するパッチや修正プログラムが入手できるかどうかについてベンダに質問する場合もある。

+ **他のインシデント対応チーム** FIRST (Forum of Incident Response and Security Teams) [18] およびGFIRST(Government Forum of Incident Response and Security Teams) [19]のようなグループは、インシデント対応チーム間での情報共有を振興している。組織が直面している異常な事件が、他のチームによってすでに処理されている事件と類似のものである可能性もある。情報を共有することで、関係する全チームがより効果的かつ効率的に事件処理を行えるようになる。正式なグループに参加する以外にも、事件関連のメーリングリストに参加し、事件に関する機密でない情報を匿名で提供して、意見を求める方法もある。[20]

+ **影響を受ける外部関係者** 事件は外部の関係者に直接影響を与える場合がある。たとえば、外部の組織から連絡が入り、自組織のユーザがその組織を攻撃しているというクレームを受けることもある。セクション7では、このトピックについて詳しく説明する。外部の関係者が影響を受けるその他のケースは、アタッカーが、クレジットカード情報といった、

16 https://irf.cc.cert.org
17 ISACの沿革に関する情報は https://www.it-isac.org/index.php にある。
18 http://www.first.org
19 GFIRSTは政府の諸官庁および機関である。(http://www.us-cert.gov/federal/gfirst.html)
20 一般的なメーリングリストの例を付録Gに示す。

その関係者の機密情報にアクセスした場合である。管轄区域によっては、事件で影響を受けるすべての関係者に通知するよう義務付けられている。状況はどうであれ、マスコミやその他の外部組織が連絡するよりも前に、影響を受ける外部関係者に連絡するのが望ましい。処理担当者は、必要な情報だけを提供するように注意すること。影響を受ける関係者が、公開すべきでない内部調査の詳細を要求する場合もある。

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information(個人情報の侵害に対する保護および対応)は、政府機関が、PII(personally identifiable information：個人情報)の侵害に関する通知の方針を策定し、実施することを求めている。[21] 事件処理担当者には、自組織のPII侵害通知方針に精通していること、また、PII侵害が発生したと疑われる場合に自組織が行うインシデント対応が、他の組織とどのように違うかを理解することが求められる (たとえば、より多くの関係者に通知する、または、より短い時間枠で通知を行うなど)。PII侵害通知方針に関する具体的な奨励事項は、OMB Memorandum M-07-16に記載されている。

インシデント対応チームは、どのような種類の外部組織に連絡し、どの情報を提供するかについて、広報部や法務部と話し合うことを強くお勧めする。この手順を文書化しておき、インシデント対応チームの全メンバーがこれに従うこと。

2.4. インシデント対応チームの構成

インシデント対応チームは、組織に関する事件が起きたことを発見した人または疑いを持った人が、だれでも連絡できるようになっておく必要がある。事件の大きさや要員の対応可能状況に応じて、1人以上のチームメンバーがその事件を扱う。事件処理担当者は、事件データを分析し、事件の影響を判断し、組織への影響に歯止めをかけ、適切な活動を行い、サービスを正常な状態に復旧する。インシデント対応チームには2、3人しかメンバーがいないこともあるが、チームの成功は、組織全体の参加と協力に大きく左右される。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各モデルについて議論し、適切なモデルを選択するための手引きを提供する。

2.4.1. チームのモデル

インシデント対応チームの構成モデルは、以下の3つに分類される。

+ **中央のインシデント対応チーム** ひとつのインシデント対応チームが組織全体の事件を処理する。このモデルは、小規模な組織、またはコンピューティングリソースの地理的分散が最小限に留まっている大組織に対して有効である。

+ **分散した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、各チームは組織の特定の論理的または物理的な域内で発生した事件を処理する責任を持つ。このモデルは、大規模な組織(たとえば部局ごとに1チームずつ)や、重要なコンピューティングリソースが離れた場所にある場合(たとえば、地区ごとに1チームずつ、または重要な設備ごとに1チームずつ)に有効である。しかし、インシデント対応プロセスを組織全体で一貫させ、チーム間で情報を共有するためには、各チームは同じ中央の部門に所属すべきである。複数のチームが同じ事件の一部を調査していたり、同様の事件を処理したりする可能性があることから、これは特に重要である。チーム間の密なやりとりや一貫した対応により、事件処理がより効果的かつ効率的になる。

+ **調整チーム** あるインシデント対応チームが、他のチームに対して、そのチームに対する権

21 このMemorandumは、http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.から入手できる。

限を持つことなく指導や助言を与える。たとえば、政府省庁のインシデント対応チームが各機関のインシデント対応チームを支援する場合がある。このモデルは、CSIRTのためのCSIRTと考えることができる。このドキュメントの焦点は、中央および分散したCSIRTであるため、調整チームモデルについては詳しく扱わない。[22]

インシデント対応チームには、以下の3つの要員配置モデルが考えられる。

+ **職員による対応** 組織がインシデント対応作業をすべて実施し、契約業者の技術面および管理面のサポートは限定的なものにとどめる。

+ **部分的外部委託** 事件対応インシデント対応作業の一部を外部委託する。セクション2.4.2では、外部委託の際に考慮すべき主な要因を説明する。インシデント対応業務は、組織と1つ以上の外部委託先とでさまざまな方法で分担できるが、以下に示すいくつかの分担方法が一般的になっている。

  - 最も一般的なやり方は、侵入検知センサー、ファイアウォール、その他のセキュリティ装置の24時間365日の監視を、MSSP(Managed Security Services Provider:オフサイトの管理セキュリティサービスプロバイダ)に外部委託する方法である。MSSPは疑いのある活動を見つけて分析し、検出された各事件を組織のインシデント対応チームに報告する。MSSPの従業員は複数の顧客に関する活動を同時に監視できるため、このモデルは、内部の事故対応チームと比較してコストとスキルの両面で優れた24時間365日の監視と対応を提供することが可能である。

  - 組織のなかには、基本的なインシデント対応作業を内部で行い、重大かつ広範な事件が発生した場合のみ、契約業者に事件処理の支援を求める組織もある。契約業者が提供するサービスで最も多いのは、コンピュータフォレンジック、詳細な事件の分析、事件の封じ込めと根絶、脆弱性の軽減である。

+ **完全な外部委託** 組織は完全に事件対応インシデント対応作業のすべてを外部委託する。委託先としては、オンサイトの契約業者であることが多い。このモデルは、組織がフルタイムでのオンサイトのインシデント対応チームを必要としているものの、その能力を持った職員が十分に確保できない場合に採用されることが多い。

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成モデルと要員配置モデルを選択する際には、以下の要因を考慮すること。

+ **24時間365日対応の必要性** 大規模な組織や、重要なインフラストラクチャをサポートしている小規模な組織では、インシデント対応要員が24時間365日対応できる必要がある。通常これは、事件処理担当者に電話やポケットベルで常時連絡可能なことを意味するが、同時にいつでもオンサイトでの対応が必要であるということも意味する。事件が長引けば、それだけ被害や損害が大きくなる可能性があるため、即時対応が最も優れている。スプーフィングされたパケットをルーターの複数のホップを超えて送信元まで追跡するような場合など、ほかの機関や組織と共同で作業しているときには、すぐに連絡が取れることが必要になることが多い。事件の調査、封じ込め、緩和のために迅速に対応する事件対応チームは、組織にとってまさに役立つ存在である。

---

22 調整チームモデルの情報と、その他のチームモデルに関する詳しい手引きは、CERT®/CCのドキュメント『*Organizational Models for Computer Security Incident Response Teams (CSIRTs)*』で提供されている。このドキュメントは http://www.cert.org/archive/pdf/03hb001.pdf から入手可能である。

+ **常勤のチームメンバーと非常勤のチームメンバー** 予算、要員が限られ、インシデント対応の必要性も薄い組織では、インシデント対応チームのメンバーが非常勤の場合がある。この場合のインシデント対応チームは、自主消防隊のようなものである。緊急事態が起きると、すぐにチームのメンバーとそれを支援できる者に連絡が行く。ITヘルプデスクのような従来のグループが事件報告の最初の窓口となってもよい。ヘルプデスクのメンバーを訓練して、初動調査とデータ収集を行い、重大な事件が起きたと思われる場合には、インシデント対応チームに連絡する。チームメンバーが非常勤である組織では、メンバーのインシデント対応能力と知識を確実に維持するよう努める必要がある。

+ **職員のモラル**、インシデント対応業務は非常にストレスのたまる業務であり、ほとんどのチームのメンバーに課せられる呼び出し待機義務もまたそうである。この両方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、過剰なストレスにさらされやすい。多くの組織では、特に24時間サポートに参加してくれる、意思が強く、役に立ち、経験があり、適切な能力を持った人間を見つけようと努力している。

+ **コスト** 特に職員が、24時間365日オンサイトで対応する必要がある場合、コストは大きな要因である。組織はインシデント対応に特有のコストを予算に組み入れ損ねていることがある。たとえば、ほとんどの組織は、訓練やスキルの維持に十分な資金を割り当てていない。インシデント対応チームは、ITの非常に多くの局面を取り扱うため、メンバーにはほとんどのIT要員よりも非常に幅広い知識が必要になる。また、コンピュータフォレンジックソフトウェアなど、事件に対応するツールの使い方も理解しなくてはならない。組織は、チームが実践的な経験を習得し、遂行能力を向上させるよう、定期的にチームが演習するための資金も提供すべきである。見過ごされがちなその他のコストとしては、チームの作業領域と通信装置の物理的なセキュリティのためのコストがある。

+ **要員の専門知識** 事件処理では、いくつもの技術領域における専門的な知識と経験が必要である。必要な知識の幅と深さは、組織のリスクの大きさに応じて変わる。外部委託先が、侵入検知、脆弱性、エクスプロイト、セキュリティのその他の面に関して、組織の職員よりも深い知識を持っていることがある。また、セキュリティサービスプロバイダは、複数の顧客の事象を相関させて、個々の顧客よりも早く新しい脅威を発見することができる。しかし、組織の技術スタッフのメンバーは、外部委託先よりも組織の環境について深い知識を持っていることが多く、組織固有の動作に絡んだ誤検知や、ターゲットの重要度を判断するのに有利である。セクション2.4.3では、推奨するチームメンバーの技能について補足説明する。

+ **組織上の構成** 組織内に独立して機能する複数の部門がある場合、それぞれの部門にインシデント対応チームがあったほうが、より効果的な事故対応が可能である。主組織が中央のインシデント対応部門を持ち、チームにまたがった標準的なプラクティスや連絡の促進を行ってもよい。

外部委託を検討する際には、以下の点を念頭に置くこと。[23]

+ **現在および将来の業務品質** 外部委託先の作業の品質は、非常に重要な検討項目である。現在の業務の品質だけでなく、外部委託先の将来的な業務の品質を確保しようとする努力も

23 NIST SP 800-35『IT セキュリティサービスガイド(*Guide to Information Technology Security Services)*』では、セキュリティサービスを受ける際の手引きが提供されている。このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.html で入手可能である。もうひとつの優れたリソースはCERT®/CC発行の『*Outsourcing Managed Security Services*』で、http://www.cert.org/archive/pdf/omss.pdf から入手可能である。

考慮すべきである。たとえば、人の入れ替わりや強度の疲労を極力減らし、新しい従業員に対して充実したトレーニングプログラムを提供するといったことである。組織は、外部委託先の業務の品質をどのようにして監査あるいは客観的に評価するかについても考慮する必要がある。

+ **責任の分割** 組織は、環境の運用面での判断(たとえば、ウェブサーバの切断など)を外部委託先に行わせたくないのが普通である。そこで、どの時点で外部委託先がインシデント対応を組織に引き継ぐかを決めることが重要である。業務の一部を外部委託するモデルの中には、事件データと事件にさらに対処するにあたっての推奨事項を外部委託先が組織の内部チームに提供することによって、この問題に対処するものもある。この場合、内部チームが運用面の最終的な判断を下すことになる。

+ **契約業者に対する機密情報の公開** この問題は、インシデント対応の責任を分割して、機密情報へのアクセスを制限することで、歯止めをかけることができる。たとえば、契約業者は、どのユーザIDが事件で使われたかはわかるが、そのユーザIDに関連付けられている人間まではわからないとする。この場合契約業者は、海賊版のソフトウェアをダウンロードするのにユーザID 123456 が使われたことを確認し報告することができても、123456 が誰なのかは知らない。最終的には組織内の信用の置ける人間が調査を引き継ぐことになる。

+ **組織固有の知識の欠如** 事件を正確に分析して優先順位を付けるためには、組織の環境を詳しく知っていることが必要となる。組織は、外部委託先に対し、組織が憂慮する事件とはどのような事件か、どのリソースが最も重要か、さまざまな状況下でどのレベルの対応が必要かについて、定期的に更新したドキュメントを提供すべきである。組織はまた、ITインフラストラクチャ、ネットワーク構成、システムに対する、すべての変更と更新も報告すべきである。そうしないと、契約業者は、各事件をどのように処理すべきかについて、推測に頼らざるを得なくなり、必然的に事件の処理を誤る結果となり、両者がいらだちを感じることになる。インシデント対応を外部委託しない場合でも、チーム間の連絡がうまくいっていなかったり、単に必要な情報を収集していない場合には、組織固有の知識の欠如は問題となる。

+ **相関関係の不足** 複数の情報源からの相関関係は非常に重要である。たとえば、侵入検知システムがウェブサーバに対する攻撃をログに記録したものの、外部委託先がそのログにアクセスできないと、攻撃が成功したのかどうかを判断できない。この場合外部委託先の作業効率を上げるためには、重要なシステムやセキュリティ装置のログに対する管理者レベルのリモートアクセス権限が必要になる。ただし、これにより管理コストが増えることと、追加のアクセスエントリーポイントを設けることになるために機密情報が不正に公開される危険が増すことに留意すること。

+ **複数の場所での事件の処理** 効果的にインシデント対応作業を行うには、担当者が組織の設備にいなければならない場合が多い。外部委託先がオフサイトにいる場合、外部委託先がどこにいるか、どれだけ早くインシデント対応チームを現場に配備できるか、それにはどれだけのコストがかかるかを考慮すべきである。オンサイト作業の際には、外部委託先が作業を許可されていない設備や区域がある点にも注意すること。

+ **インシデント対応の技能を内部で維持する** インシデント対応を完全に外部委託する組織では、基本的なインシデント対応スキルを内部で保持するように努力すべきである。外部委託先が対応できない状況も起きる可能性がある(たとえば、新種のワームが数千もの組織を同時に攻撃した場合や、自然災害、国内の航空便でストライキが起きた場合など)。組織は、外部委託先が行動できない場合に備え、自らが事件を処理する準備をしておくべきである。また、組織の技術スタッフは、外部委託先が提供する推奨事項の重要性、技術

的な意味および影響を、理解できるレベルであることが求められる。

2.4.3. インシデント対応要員

組織がどのインシデント対応モデルを選ぶにせよ、職員の一人がインシデント対応の責任を持つことになる[24]。インシデント対応のすべてを外部委託するモデルでは、この責任者が外部委託先の作業を監督し評価する責任を負う。その他すべてのモデルでは、チームマネージャと、チームマネージャが不在の場合に権限を引き継ぐ代理のチームマネージャを任命することで、一般にこの責任が達成される。チームマネージャは、上位マネジメント層やほかのチームや組織などとの調整役となったり、危機を打開し、チームに必要な要員・リソース・技能を確保するなど、一般にさまざまな作業をこなす。チームマネージャはまた、技術にも熟達しており、優れたコミュニケーション能力を持ち、特に幅広い対象とのコミュニケーションにたけている必要がある。最後に、チームマネージャは、たとえ高度の緊張が要求される状況であっても、ほかのグループと前向きな作業関係を維持することができなくてはならない。

チームマネージャとチームマネージャ代理に加え、技術リーダーを任命するチームもある。技術リーダーは、非常に高い技術的な技能とインシデント対応経験を持ち、インシデント対応チーム全体の技術的な作業品質を監督して、その品質に最終的な責任を持つ。ここで、技術リーダーと事件リーダーを混同しないように注意すること。大規模なチームでは、特定の事件を処理するための一次窓口として、事件リーダーを任命することが多い。インシデント対応チームの規模と事件の大きさによっては、データ分析や証拠の収集といった実際の事件処理を、事件リーダーが行わないこともある。代わりに事件リーダーは、処理担当者の作業を調整し、処理担当者からの情報を収集し、事件に関する最新情報をほかのグループに提供する。また、事件が長引いた場合に、チームのための食事や宿泊場所を手配するなど、チームの要求が満たされるようにする。

インシデント対応チームのメンバーは、優れた技術的な能力を持っている必要がある。この能力は、チームの成功にとって不可欠である。チームのメンバーが組織全体から高いレベルの技術的な尊敬を集めていなければ、だれも助けを求めてこなくなるからである。アドバイザリを発行するなどの業務で技術的な間違いがあると、チームの信用に傷が付くことになる。また、技術的な判断が甘いと、事件が悪い方向に進んでしまうこともある。技術面での不可欠な技能には、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、侵入検知が含まれる。チームの各メンバーには、優れた問題解決能力が求められる。それには、運用停止に対処するなど、実際のトラブルシューティング経験を積むことである。(実質的な面や財政的な面を考慮すると)すべてのメンバーが技術的なエキスパートになる必要はないが、主要な技術分野(特定のオペレーティングシステム、ウェブサーバ、電子メールサーバなど)ごとに少なくとも１人の者が、高度に熟達した技術者であるべきである。

メンバーに対し学習し成長する機会を与えることで、メンバーが消耗してしまわないようにすることが大切である。以下に、技術を習得し維持していくための方法を提案する。

+ 技術領域やセキュリティ上の訓練だけでなく、技術的要素が少ないトピック(インシデント対応の法的な側面など)についても、習熟度を維持、向上、発展させるために十分な予算を組むこと。常勤の各メンバーについては少なくとも年に2回、非常勤のメンバーについては少なくとも年に1回、技術カンファレンスに参加させること。

+ 技術面でのより深い知識を得る助けとなるような図書、雑誌、その他の技術資料を利用できるようにすること。

---

24 一人目が対応できない場合に備え、インシデント対応を監督するための交代要員として、少なくとももう一人の者を任命すべきである。

- チームのメンバーにほかの作業をする機会を与えること。たとえば教育資料の作成、セキュリティ意識向上ワークショップの開催、システム管理者の事件検知に役立つソフトウェアツールの開発、研究などが考えられる。
- メンバーをインシデント対応チームの内外で配置転換することを検討すること。
- 十分な人員を配置し、チームのメンバーが連続した休暇を取れるようにする。
- 年長の技術要員が、経験の少ない要員が事件処理を学ぶのを補佐できるような、社内指導教育プログラムを作成する。
- チームのメンバーとほかの者(たとえばネットワーク管理者)を一時的に職務交換して、新しい技術的な技能を習得させる。
- 予算が許せば、必要な領域に関する深い技術的な知識を持った外部の専門家(例えば契約業者)を時々参加させる。
- 事件処理シナリオを作成し、自分たちならどのように処理するかを、チームのメンバーに議論させる。シナリオディスカッションで使用する数種のシナリオと質問リストを、付録Bに示す。
- シミュレーションによる事件処理訓練を実施する。訓練を行うことで、事件処理担当者の遂行能力が向上するだけでなく、ポリシー、手順、コミュニケーションに関する問題も見つかるため、特に重要である。

インシデント対応チームのメンバーは、技術ノウハウだけでなくほかのスキルも身につけるべきである。インシデント対応を成功させる上では協力と協調が必要であるため、チームワークスキルは根本的に重要である。また、チームの全メンバーが、優れたコミュニケーション能力を身につけるのが望ましい。チームは、被害者、マネージャ、システム管理者、人事部、広報部、法務部など、さまざまな人間と対話するため、会話能力は特に重要である。また、チームメンバーがアドバイザリや手順を書く場合には、文章記述能力も重要である。チームのメンバー全員が高い会話能力や文章記述能力を身につける必要はないが、各チームの少なくとも2、3人はこれらの能力を身につけ、上級管理職、ユーザ、一般大衆に対し説明できるようにしておく必要がある。

2.4.4. 組織内の依存関係

事件処理に参加してもらう必要がある組織内のほかのグループを見つけておき、実際に必要になる前に協力を要請しておくことが重要である。どんなインシデント対応チームも、以下に示すような部門の専門知識、判断、能力に頼ることになるからである。

- **マネジメント層** マネジメント層は、インシデント対応の中で常に中心的な役割を持つ。最も根本的な意味で、マネジメント層がインシデント対応ポリシー、予算、要員配置を確立する。最終的に、マネジメント層は、さまざまな利害関係者間でインシデント対応の調整を行い、損害を最小限に抑え、議会、OMB、会計検査院(GAO: General Accounting Office)、その他関係者に報告する責任を負う。マネジメント層のサポートがなければ、インシデント対応チームは成功するとは考えられない。
- **情報セキュリティ部門** 情報セキュリティチームのメンバーは、事件の発生またはその予兆に最初に気づくことが多く、事件の初期分析を行うことがある。さらに、情報セキュリティ要員は、事件処理の他の段階、たとえば事件を封じ込めるためのネットワークセキュリティコントロール(たとえばファイアウォールのルールセットなど)の変更などにおいて必

要になる場合がある。

+ **通信部門** いくつかの事件は、安全でないモデムへのダイヤルなど、電話回線への不正アクセスが関係する。構内交換機(PBX)への侵入は、他のシステムへの侵入に関係することが多い。通信部門のメンバーは、現在の能力や、通信キャリアと協調して作業する際の窓口と手順を認識している。

+ **ITサポート部門** IT技術の専門家(たとえばシステム管理者、ネットワーク管理者、ソフトウェア開発者)は、事件が発生した際に事件処理を支援するための必要な技術スキルを持っているだけでなく、自分達が毎日扱っている技術を最もよく理解しているのが普通である。攻撃されたシステムをネットワークから切り離すべきかといった判断を行う際に、この理解が役立つ。

+ **法務部門** プライバシーの権利を含め、法律や国の指導に準拠することを確実にするために、法律の専門家がインシデント対応ポリシーや計画、および手順をレビューすべきである。さらに、証拠収集、容疑者の告訴、訴訟を含め、事件に法的な派生問題があると信ずるに足る理由がある場合には、法律顧問や法務部の指導を求めるべきである。

+ **広報部およびマスコミとの窓口** 事件の性質や影響によっては、マスコミや一般大衆に知らせる必要がある場合がある(当然ながら、セキュリティ面や法執行機関の利害による制約の範囲内で)。この問題については、セクション2.3.2で詳しく説明する。

+ **人事部** ある職員が事件の明確なターゲットになっている場合や、事件を起こしていると疑われる場合には、懲戒手続きや職員カウンセリングなどの面で、人事部門が関わってくることがある。

+ **業務継続計画部門** コンピュータセキュリティインシデントは、組織のビジネスの勢いを弱めるものであり、脆弱性と内在リスクレベルのバロメーターとなる。業務継続計画の専門家は、ビジネス影響評価、リスク評価、業務継続計画の微調整ができるよう、事件とその影響について知らされているべきである。業務継続性計画担当者は、厳しい状況で業務の中断を最小化するための幅広いノウハウを持っているため、ある種の事件(サービス不能(DoS)など)への対応を計画する際に有用である。組織は、業務継続プロセスが、インシデント対応ポリシーや手順と同期するようにしなければならない。

+ **物理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インシデントのなかには、物理的なセキュリティ侵害によって発生するものもあれば、論理的および物理的に調整された攻撃に関連するものもある。組織に対する脅威では、論理的なリソースと物理的なリソースのどちらがターゲットになっているかわからない場合もある。また、インシデント対応チームは、事件処理の際に設備にアクセスできる必要がある。たとえば、侵入を受けたワークステーションを鍵のかかった部屋から取り出す場合である。そのため、物理セキュリティ、設備管理、インシデント対応チームが密接に連係することが重要である。

2.5. インシデント対応チームのサービス

インシデント対応チームの主な業務はインシデント対応を行うことであるが、インシデント対応だけを行うというのは非常にまれである。以下に、インシデント対応チームが提供する補足的なサービスの例を示す。[25]

25 CERT®/CCは、チームが提供する可能性があるサービスのより詳しい一覧を http://www.cert.org/csirts/services.html で提供している。

+ **アドバイザリの配布** オペレーティングシステムやアプリケーションの新しい脆弱性を説明したアドバイザリを発行したり、脆弱性に対処するための情報を提供したりする。[26] 脆弱性と事件は直結するため、このような情報をすぐに公開することは、優先順位の高い作業である。現在起きている事件に関する情報を配布することも、他の者が同様な事件の兆候を見つける上で有益である。作業が重複し、矛盾した情報が広まるのを防ぐため、コンピュータセキュリティアドバイザリの配布は、組織内の1つのチームだけが行うことをお勧めする。NVD(National Vulnerability Database)は、新しい脆弱性が追加された場合に、電子メール、XMLファイル、およびRSSデータフィードにより情報を提供する。[27]

+ **脆弱性評価** ネットワーク、システム、アプリケーションのセキュリティ関連の脆弱性を調査し、どのようにして悪用されうるのか、どのようなリスクがあるかを判断し、リスクを軽減する方法を助言する[28]。この責務を拡大して、チームが監査や侵入テストも行うようにし、事前の連絡なくサイトを訪問して、その場で評価を実施してもよい。事件処理担当者は、あらゆる種類の事件を日常的に見ており、脆弱性とそれがどのように悪用されるかについて、直接得た知識を持っているため、脆弱性評価を行うのには適任である。しかし、事件処理担当者の時間がいつ空くかは予測できないため、組織は通常、脆弱性評価の主な責任をほかのチームに割り当て、事件処理担当者は補助的なリソースとして活用することが多い。

+ **侵入検知** 組織内の他の者に十分な時間、リソース、専門的な技術がないという理由から、インシデント対応チームが侵入検知の責任を負う場合もある。[29] インシデント対応チームは、侵入検知を通じて得た知識に基づいて事件をより迅速かつ正確に分析することが求められるため、このような作業を行うことは、インシデント対応チームのためにもなる。しかし、理想的には、侵入検知の第一の責任は他のチームに割り当て、インシデント対応チームのメンバーは、余裕がある場合に侵入検知に参加するようにすべきである。

+ **教育と意識向上** 教育と意識向上は、リソースを倍増させる手段となる。事件の検知、報告、対応について、ユーザや技術スタッフの理解が深まるほど、インシデント対応チームの労力は少なくて済む。この情報は、ワークショップ、セミナー、ウェブサイト、広報、ポスター、モニター上のステッカーなど、さまざまな手段を通じて伝えることができる。

+ **技術動向の監視** チームが技術動向を監視する役割を果たしてもよい。つまり、情報セキュリティの脅威について、最新動向を観察するということである。例としては、セキュリティ関連のメーリングリストを監視したり、侵入検知データを分析してワームの活動の活発化を見つけたり、だれでも入手可能な新しいルートキット[30] を調査するなどがあげられる。次に、見つけた動向に基づいてセキュリティ管理策を改善する方法を助言する。チームが技術動向観察も行うことで、新しいタイプの事件を処理する体制も整うことになる。

+ **パッチ管理** インシデント対応チームにパッチ管理(パッチの入手、テスト、組織全体の該当

---

26 アドバイザリを書く際には、セキュリティ問題に対していかなる個人や組織も責めないように注意すること。アドバイザリの正確さに関してチームや組織はいっさいの責任を持たない、などの免責事項をアドバイザリ入れるべきかどうかについては、法律アドバイザーに相談すること。これは、請負業者やベンダーにアドバイザリを渡す場合、または職員以外で組織のコンピューティングリソースを使用する者にアドバイザリを渡す場合には、特に重要である。

27 http://nvd.nist.gov/

28 NIST SP 800-115『*Technical Guide to Information Security Testing*』は、脆弱性評価と侵入テストを実施する際の手引きである。このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.html で入手可能である。

29 NIST SP 800-94『*Guide to Intrusion Detection and Prevention Systems (IDPS)*』では、IDPS技術の特性に関する記述と、それらの技術の設計、実施、設定、安全化、監視およびメンテナンスに関する奨励事項を提供している。このドキュメントは、//csrc.nist.gov/publications/PubsSPs.html で入手可能である。

30 ルートキットは、アタッカーがホストに対するルートレベルのアクセスを得た後に使用するツールを集めたものである。ルートキットはホスト上でのアタッカーの活動を隠蔽し、アタッカーが隠された手段を使ってホストにルートレベルのアクセスをし続けられるようにする。

する管理者やユーザへの配布)の責任を持たせるのは、一般に勧められない。[31]パッチ管理は時間がかかり骨の折れる作業であり、事件処理において遅らせることができないプロセスでもある。実際にパッチ管理サービスは、大規模な事件の封じ込め、根絶およびシステムの復旧を行う際に、最も必要なサービスとなることが多い。パッチ管理スタッフとインシデント対応チームとの間で効果的なコミュニケーションチャンネルがあれば、パッチ管理プログラムの成功に寄与するところも大きくなるだろう。

2.6. 推奨事項

このセクションで説明した、コンピュータセキュリティインシデント処理能力を編成するための主な推奨事項を、以下に要約する。

+ **正式なインシデント対応能力を確立する** 組織は、コンピュータセキュリティの防御が破られた場合に迅速かつ効果的に対応できるよう、準備しておく必要がある。FISMAでは、政府機関がインシデント対応能力を確立することを義務付けている。

+ **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である。その中では、どの事象を事件と判断するかを定義し、インシデント対応の組織構造を確立し、役割と責任を定義し、事件報告の要件を明確にする。

+ **インシデント対応ポリシーをもとに、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、インシデント対応ポリシーにもとづきインシデント対応機能を実施するための、手引きを提供する。インシデント対応計画では、短期および長期の目標を設定し、計画を評価するためのマトリックスとともに明記する。また、事件処理担当者に対するトレーニングの頻度や、事件処理担当者に要求される事項も記載する。

+ **インシデント対応手順を作成する** インシデント対応手順は、インシデント対応の詳細なステップを示すものである。この手順は、インシデント対応プロセスのすべてのフェーズを対象とする。インシデント対応手順は、インシデント対応ポリシーおよび計画にもとづくものとする。

+ **事件関連の情報共有に関するポリシーと手順を確立する** 組織は、マスコミ、法執行機関、インシデント対応組織といった、外部の関係者に事件の詳細について連絡しようと考える(またはそうしなくてはならない)場合がある。インシデント対応チームは、組織の広報部のスタッフ、法律アドバイザー、マネジメント層とこの要件について詳細に話し合い、情報共有に関するポリシーと手順を確立しておく必要がある。マスコミ等の外部関係者とやりとりする際には、組織の現行のポリシーに従う。

+ **適切な事件報告組織に、事件についての関係情報を提供する** 政府民間機関は、事件をUS-CERTに報告するよう義務付けられており、その他の組織は、US-CERTおよび／または他の事件報告組織に報告する。事件報告組織は、報告されたデータを使って、報告元の団体に対して新しい脅威や事件の動向に関する情報を提供するため、この報告は有益である。

+ **インシデント対応チームモデルを選ぶ際には、関係する要因を検討すること** とりうるチーム構成モデルと要員配置モデルのそれぞれの長所と短所について、組織の要件や利用で

31 パッチ管理など脆弱性軽減の詳細については、NIST SP 800-40『パッチ及び脆弱性管理プログラムの策定（Creating a Patch and Vulnerability Management Program）』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照。

きるリソースに照らし、慎重に検討すること。

+ **インシデント対応チームには適切なスキルをもった人間を選ぶこと** チームの信頼と熟達度は、メンバーの技術的なスキルによるところが大きい。技術的な判断が甘いと、チームの信用に傷が付き、事件が悪い方向に進んでしまうことがある。技術面での不可欠な技能には、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、侵入検知が含まれる。事件処理を効果的に行うためには、チームワークとコミュニケーション能力も必要である。

+ **事件処理に参加してもらう必要がある、組織内のほかのグループを明確にする** どのインシデント対応チームも、ほかのチームのノウハウ、判断、能力に頼ることになる。これには、マネジメント層、情報セキュリティ部門、ITサポート部門、法務部、広報部、設備管理部門が含まれる。

+ **チームが提供するサービスを決める** チームの主な業務はインシデント対応であるが、ほとんどのチームはその他の職務も行う。例としては、セキュリティアドバイザリの配布、脆弱性評価の実施、セキュリティに関するユーザ教育、侵入検知センサーの監視などがある。

3. 事件処理

インシデント対応プロセスには、初期の準備段階から事後分析まで、いくつかのフェーズがある。最初のフェーズでは、インシデント対応チームを確立して訓練し、必要なツールやリソースを取得する。準備の間は、リスク評価の結果に基づき、いくつかの管理策を選択して実施し、発生する事件の数を制限するよう努める。しかし、管理策を実施しても残存リスクがあるのは避けられず、絶対確実な管理策というものも存在しない。よって、セキュリティ違反を検知して、事件が起きた場合に組織に警告することが必要である。事件の重大性を踏まえ、事件を封じ込めて最終的に復旧することで、影響を軽減するように行動することができる。事件を適切に処理した後で報告書を作成し、事件の原因や被害と、将来事件を防止するために行うべき対策を詳細に記述する。インシデント対応プロセスの主なフェーズには、準備、検知と分析、封じ込め/根絶/復旧、事件後の対応がある。このセクションでは、これらについて詳しく説明する。図3-1は、インシデント対応のライフサイクルを図示したものである。

図3-1 インシデント対応ライフサイクル

3.1. 準備

インシデント対応方法論では、一般的に準備の重要性が強調される。この準備には、事件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、アプリケーションを十分に安全な状態に保つことで、事件を予防することが含まれる。一般的にインシデント対応チームは事件防止の責任を負わないが、事件防止は非常に重要なことであるため、現在ではインシデント対応プログラムの基本的な要素となっている。システムを安全にするための奨励事項を作成する上で、インシデント対応チームのノウハウは貴重である。このセクションは、事件の処理に備え、事件を予防するための基本的な手引を提供する。

3.1.1. 事件処理に備える

表3-1に、事件処理の際に役立つツールやリソースを挙げる。事件分析に役立つ具体的なツールに関する情報や、インシデント対応に関する有用な情報が掲載されているウェブサイトの一覧については、付録Gを参照のこと。セクション3.2では、IDPSやログの一元管理などの仕組みを使った、事件の検知に関する情報を提供する。

表3-1 事件処理のためのツールとリソース

入手	ツール/リソース
	事件処理担当者への連絡と設備
	連絡先情報 チームのメンバー、法執行機関、ほかのインシデント対応チームなど、組織内外の関係者(一次窓口と二次窓口)の連絡先。電話番号、電子メールアドレス、公開鍵(下記の暗号化ソフトウェアに応じたもの)、連絡先の身元を確認するための手順などが考えられる。
	呼び出し情報 エスカレーション情報を含む、組織内のほかのチームの呼び出し情報(エスカレーションの詳細は3.2.6を参照)。
	事件報告手段 電話番号、電子メールアドレス、疑いのある事件を報告するのに使用するオンラインフォームなど。少なくとも1つの手段では、匿名で事件を報告できるようになっているのが望ましい。
	ポケットベルまたは携帯電話 勤務時間外のサポートや、オンサイトでの連絡のためにチームのメンバーが持つ。
	暗号化ソフトウェア チームのメンバー間、組織内、外部の関係者との間での連絡で使用する。ソフトウェアは、FIPS 140-2で検証済みの暗号化アルゴリズムを使用していること[32] 。
	作戦本部室 中心となって組織内外の連絡・調整を行う。常設の作戦本部室が不要な場合は、必要時に作戦本部室を確保する手順を策定しておくこと。
	安全な保管手段 証拠物や機密物を安全に保管するための手段。
	事件分析ハードウェアとソフトウェア
	コンピュータフォレンジックワークステーション[33] とバックアップ装置 ディスクイメージの作成、ログファイルの保存、その他事件データの保管用。
	ラップトップコンピュータ データの分析、パケットのスニッフィング、報告書の作成などで使用する、簡単に持ち運びができるコンピュータ。
	予備のワークステーション、サーバ、ネットワーク機器 バックアップの復旧、悪意のコードの試用など、さまざまな用途で使用する。追加機材のための予算が確保できない場合は、現在実験室にある機材を利用するか、オペレーティングシステム(OS)をエミュレートするソフトウェアを使って、仮想的な実験室を作ることもできる。
	未使用媒体 フロッピーディスク、CD-R、DVD-Rなど。
	簡単に持ち運びができるプリンター 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物を印刷する際に使用する。
	パケットスニッファとプロトコルアナライザ 事件の証拠が含まれている可能性があるネットワークパケットを捕捉して分析する。
	コンピュータフォレンジックソフトウェア ディスクイメージを分析して、事件の証拠を探す。
	フロッピーとCD 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。
	証拠収集アクセサリ 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、証拠・記録の保管フォーム、証拠保管バッグとタグ、証拠テープなど。

32 FIPS 140-2『Security Requirements for Cryptographic Modules』は、http://csrc.nist.gov/publications/PubsSPs.html から入手可能である。

33 コンピュータフォレンジックワークステーションは、事件処理担当者によるデータの取得と分析を支援するように設計されている。一般にこのワークステーションは、証拠記憶装置として使用するリムーバブルハードディスクを装備している。

事件分析リソース	
	ポートリスト 一般に使用されるポートとトロイの木馬のポート
	マニュアル 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マニュアル。
	ネットワーク図と重要な資産の一覧 これらの図や一覧にはウェブサーバ、電子メールサーバ、FTPサーバなどが含まれる。
	基準 予想されるネットワークの活動、システムの活動、アプリケーションの活動の基準。
	暗号化ハッシュ 事件の分析、検証、根絶を迅速に行うための、重要なファイルのハッシュ。[34]
事件鎮静化ソフトウェア	
	媒体 OSのブートディスクやCD-ROM、OSの媒体、アプリケーションの媒体など。
	セキュリティパッチ OSやアプリケーションのベンダーから入手。
	バックアップイメージ OS、アプリケーションおよびデータのバックアップイメージ(予備の媒体に記録されている)。

多くのインシデント対応チームでは、ジャンプキットと呼ばれる持ち運び可能なバッグまたはケースを用意している。このジャンプキットには、オフサイトの調査で事件処理担当者が必要とする機材が多く入っている。ジャンプキットはいつでも使用できるようになっており、重大な事件が起きると、事件処理担当者はジャンプキットを抱えて出発する。ジャンプキットに入れておくものは、表3-1とほぼ同じものである。たとえばジャンプキットには、必要なソフトウェア(パケットスニッファ、コンピュータフォレンジックソフトウェアなど)をインストールしたラップトップが含まれている。その他の重要な機材としては、バックアップ装置、未使用の媒体、基本的なネットワーク装置とケーブル、オペレーティングシステムとアプリケーションの媒体やパッチなどがある。ジャンプキットを準備する目的は、迅速な対応を可能にするためであることから、ジャンプキットの中の機材を一時的にほかで使用するというのは避けるべきである。また、ジャンプキットを常に最新の状態に保つことも重要である(たとえば、ラップトップにセキュリティパッチをインストールしたり、オペレーティングシステム媒体を更新するなど)。ジャンプキットを作成して維持するためのコストと、事件をより迅速かつ効果的に封じ込めることによる救済メリットについて比較考慮することをお勧めする。

3.1.2. 事件の予防

事件の数を妥当な数に抑えることは、組織のビジネスプロセスを保護する上で非常に重要である。セキュリティコントロールが十分でないと、大量の事件が起こり、インシデント対応チームの手に負えなくなってしまう可能性がある。これにより、事件の対応が遅れたり、不完全になり、ビジネスインパクトが拡大する結果となる(被害が拡大し、サービスやデータが利用できない期間が長くなる)。組織のセキュリティ体制を改善して事件を予防するための確実なアプローチは、システムとアプリケーションのリスク評価を定期的に行うことである。評価を行うことで、脅威と脆弱性の組み合わせがもたらすリスクが、どのようなリスクであるかを判断することができる。[35]。各リスクには優先順位を付け、リスク全体のレベルが妥当な範囲になるまで、各リスクを軽減、転換、受け入れられるようにする。信頼できる同様の組織のコントロール方針を取り入れるか、

34 NSRL (National Software Reference Library)プロジェクトは、オペレーティングシステム、アプリケーション、グラフィックイメージファイルを含むさまざまなファイルのハッシュの記録を保有している。http://www.nsrl.nist.gov からハッシュをダウンロードすることができる。

35 リスク管理のため手引きとしては、NIST SP 800-30『IT システムのためのリスクマネジメントガイド(Risk Management Guide for Information Technology Systems)』がある。このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.html で入手可能である。

最低でもそれを調査することで、ほかで有効だったものは自らの組織でも有効だという、ある程度の確信が得られる。

定期的にリスク評価を実施することのもうひとつの利点は、重要なリソースを明確にすることにより、そのリソースの監視と対応活動に注力できるようになるという点である[36]。だからといって、あまり重要でないリソースのセキュリティを無視してかまわないというわけではない。なぜならば組織のセキュリティレベルは、対象リソース内の最も弱い部分と同じレベルになってしまうからである。リスク評価がどれだけ有効であっても、それはあくまで現在のリスクを反映しているに過ぎないという点に注意すること。新しい脅威と脆弱性は常に生まれている。コンピュータセキュリティは、不断の努力なくしては効果がない、継続したプロセスである。

ネットワーク、システム、アプリケーションのセキュリティを高めるための特定の助言を提供することは、このドキュメントの範囲外である。一般にインシデント対応チームはリソースのセキュリティを高める責任を負わないが、十分なセキュリティ訓練の必要性を説くことはできる。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固有の手引きについては、すでにほかのドキュメントで優れた助言が提供されている[37]。したがって本文書では、ネットワーク、システム、アプリケーションのセキュリティを高めるために推奨される主な活動の一部を、簡単に説明する。

+ **パッチ管理** 事件の大部分は、システムやアプリケーションが持つ比較的少数の脆弱性を悪用したものであることは、多数の情報セキュリティの専門家が同意するところである[38]。大規模な組織は、パッチ管理プログラムを実施して、システム管理者によるパッチの識別、取得、テスト、配布を支援するべきである。

+ **ホストのセキュリティ** すべてのホストは、適切に堅牢性を高めるべきである。各ホストに対して適切にパッチが適用されるようにするだけでなく、最低限のサービスが適切なユーザとホストだけに提供されるようにホストが設定されるべきである。これが「最低限の特権」の原則である。安全でないデフォルト設定(デフォルトのパスワード、安全でない共有など)は変更すべきである。セキュリティ対策が実施されたリソースにユーザがアクセスしようとした場合には、警告バナーが表示されるようにする。ホストは監査が実施できるようにし、重要なセキュリティ関連のイベントについてはログを取得する。多くの組織では、管理者がホストのセキュリティ対策を首尾一貫して効果的に実施できるよう、オペレーティングシステムとアプリケーションの設定ガイドを用意している。[39]

+ **ネットワークセキュリティ** ネットワークの境界では、明示的に許可されていないすべての活動を拒否するように設定する。組織が適切に機能するために必要な活動だけが許可されるべきである。これには、モデム、VPN (virtual private network)、ほかの組織への専用線接続といったすべての接続ポイントのセキュリティを高めることが含まれる。

+ **悪意のコードの予防** ウイルス、ワーム、トロイの木馬などの悪意のコードを検知して阻止するソフトウェアを、組織全体に配布する。悪意のコードの予防策は、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

---

36 重要なリソースの明確化に関する情報が、FIPS199『連邦政府の情報および情報システムに対するセキュリティ分類規格 (Standards for Security Categorization of Federal Information and Information Systems) 』にある。このドキュメントは http://csrc.nist.gov/publications/PubsSPs.html で入手可能である。

37 http://csrc.nist.gov/publications/PubsSPs.html には、コンピュータセキュリティに関するNIST Special Publication へのリンクがあり、その中にオペレーティングシステムやアプリケーションのセキュリティ基準に関するドキュメントが含まれている。

38 『The SANS Top 20 Security Risks list』には最も一般的に悪用される脆弱性の一覧が掲載されている。このドキュメントは、http://www.sans.org/top20で入手可能である。

39 NISTは、セキュリティチェックリストのレポジトリを運営している。このレポジトリは、http://checklists.nist.gov/ で入手可能である。

レベル(電子メールサーバ、ウェブプロキシーなど)、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クライアント)で配備する。セクション5では、悪意のコードの予防についてさらに詳しく説明する。

+ **ユーザの意識向上とトレーニング** 組織は、ユーザに対して、ネットワーク、システム、アプリケーションの適正な利用に関するポリシーや手順について知らせるべきである。また、過去の事件の教訓もユーザ間で共有できるようにして、自分たちの行動が組織にどのような影響を与えるかを認識させるべきである。事件に関するユーザの意識が向上することで、特に悪意のコードに関係する事件や、利用ポリシー違反に関係する事件の頻度が減る。情報技術(IT)スタッフは、ネットワーク、システム、アプリケーションを組織のセキュリティ標準に従って維持できるように訓練されているべきである。

3.2. 検知と分析

図3-2 インシデント対応のライフサイクル(検知と分析)

3.2.1. 事件の分類

事件の発生の仕方は数え切れないほどあるため、各事件を処理するための順を追った指示を含んだ包括的な手続きを作成することは現実的ではない。組織ができることは、あらゆる種類の事件に対処するための一般的な準備を行い、共通の種類の事件に対処するための特定の準備をすることである。以下に示す事件の分類は、すべてを網羅したものではなく、事件の明白な分類を提供することを意図したものでもない。むしろ、事件の主な分類に基づいて事件を処理するための、手引きとなるものである[40]。

+ **サービス不能**—リソースを枯渇させることで、ネットワーク、システム、アプリケーションの正規の使用を妨害または阻害する攻撃。
+ **悪意のコード**—ウイルス、ワーム、トロイの木馬など、ホストに感染する、悪意のコード。
+ **不正アクセス**—許可なくネットワーク、システム、アプリケーション、データ等のリソースに論理的または物理的にアクセスすること。
+ **不適切な使用**—ネットワークまたはコンピュータの利用規定に違反すること[41]。

---

40 このドキュメントの分類は、新しい分類学を形成しようというものではないが、議論の元としては役に立つだろう。付録Jでは、インシデント報告分類のリストを掲載している。このリストは、連邦政府機関が、事件をUS-CERTに報告する際に利用する。

41 妥当な利用ポリシーには、ユーザが組織のコンピューティングリソースを使ってやっていいことと悪いことを明記する。多くのポリシーでは、ユーザが行ってはならない具体的な行動(たとえば、ポルノ画像にアクセスするなど)を挙げるだけではなく、ユーザがコンピューターリソースを通じた違法な活動(盗まれたクレジットカードを使ってオンラインで商品を購入するなど)に参加してはならないことも明記している。

+ **複合要素**—1つの事件で2つ以上の事件を包含しているもの。

事件によっては、複数の分類に当てはまるものがある。このような事件は、以下に示すように、転送機構によって分類すべきである[42]。

+ バックドアを作成するウイルスは、不正アクセス事件ではなく、悪意のコードの事件として処理する。なぜなら、悪意のコードが唯一利用された転送メカニズムだからである。

+ ウイルスがバックドアを作成し、それが不正アクセスを得るために利用された場合は、複合要素として処理する。なぜなら、2つの転送メカニズムが利用されたからである。

このセクションでは、あらゆる種類の事件を処理するための、推奨される方法に重点を置く。セクション4から8では、事件の分類に応じた、より具体的なアドバイスを提供する。

3.2.2. 事件の兆候

多くの組織にとって、インシデント対応プロセスの最も難しい部分は、事件を正確に検知して評価することである。つまり、事件が起きたのかどうかを判断し、もしそうであれば、問題の種類、範囲、規模を判断することである。以下の3つの要因の組み合わせが、このことを難しくしている。

+ 事件はさまざまな方法で検知され、検知された情報の詳細レベルや正確さもそれぞれに異なる。自動的な検知機能には、ネットワーク型あるいはホスト型のIDPS、ウイルス対策ソフトウェア、ログアナライザが含まれる。事件は、ユーザによる問題報告など、人間が見つける場合もある。事件によっては、容易に検知できる明白な兆候があることもあれば、自動化しないと検知がほぼ不可能なものもある。

+ 事件の可能性がある兆候の量が、一般的に多い。たとえば、ある組織が一日に何千、何百万という侵入検知センサーの警報を受け取ることも珍しくはない[43]。

+ 事件関連のデータを正しく効率的に分析するためには、深く専門的な技術上の知識と、幅広い経験が必要である。ほとんどの組織では、このレベルの知識を持つ職員が数名いたとしても、別の業務に割り当てられている可能性が高い。

事件の兆しは、兆候と前兆のどちらかに分類される。「前兆」は、事件が将来起こるかもしれないというサインである。「兆候」とは、事件がすでに起きたか、または現在起こっている可能性を示すサインである。あまりにも多くの兆候があるため、ここですべてを挙げることはできないが、以下にいくつかの例を示す。

+ FTPサーバに対しバッファーオーバーフロー攻撃が仕掛けられたことを検知したネットワーク侵入検知センサーが、警報を発する。

+ ホストがワームに感染したことを検知したウイルス対策ソフトウェアが、警報を発する。

+ ウェブサーバがクラッシュする。

+ インターネット上のホストへのアクセスが遅いという、ユーザからの苦情を受ける。

---

42 このドキュメントでは、事件を転送メカニズムによって分類しているため、「PIIインシデント」などの分類は存在しない。したがってPII(個人情報)の侵害も、転送メカニズム(悪意のコードによるPIIへの不正アクセス、アタッカーによるPII記録媒体への物理的アクセスなど)によって分類される。

43 たとえば、1台のウェブサーバに対してウェブ脆弱性スキャンを一度行っただけで、ネットワークベースのIDPSと、ウェブサーバのホストベースのIDPS製品の両方で、数百もの警報が生成される場合がある。アタッカーがそのようなスキャンを10台のウェブサーバに対して行うと、何千というIDPS警報が生成されることになる。

- システム管理者が、異常な文字が使われたファイル名を発見する。
- ユーザがヘルプデスクを呼び出し、脅迫的な電子メールメッセージがあったことを報告する。
- ホストのログに、監査設定の変更が記録される。
- アプリケーションが、見慣れないリモートシステムからの、複数回のログインの試みの失敗をログに記録する。
- 電子メール管理者が、怪しい内容の大量のバウンスメールを見つける。
- ネットワーク管理者が、典型的なトラフィックフローからの異常な逸脱に気づく。

事件の検知を受身の行動だと考えるべきではない。なぜならば事件の検知を試みることで、事件に先行する活動を検出する場合もあるからである。たとえば、ネットワークIDPSセンサーが、あるホスト群での異常なポートスキャン活動を記録し、その直後に同じホスト群の中の1台のホストに対してDoS攻撃が開始される場合もある。このスキャン活動に関する侵入検知警報は、その後のDoS事件の「前兆」だったのである。その他の前兆の例としては、以下のものがある。

- ウェブサーバが、ウェブ脆弱性スキャナの使用を示すエントリーをログに記録する。
- 組織のメールサーバの脆弱性をターゲットにした、新しいエクスプロイトの告知。
- 政治的ハッカーグループが、組織を攻撃するという声明を出して脅迫する。

すべての攻撃が前兆により検知される訳ではない。前兆がまったくない攻撃もあれば、組織が検出できない前兆をもつ攻撃もある。前兆を検知したら、自動または手動で組織のセキュリティ体制を変更し、ターゲットを攻撃から守ることで、事件を予防する機会が与えられることもある[44]。最も深刻なケースでは、組織が、リスクを素早く軽減するために、事件がすでに発生しているかのように行動することが考えられる。前兆を検知した場合、組織は、少なくとも特定の活動(たいていは、特定のホストへの接続や特定のタイプのネットワークトラフィック)をより詳しく監視することはできる。

3.2.3. 前兆と兆候のソース

前兆と兆候は、さまざまなソースを使って見つけることができる。最も一般的なのは、コンピュータセキュリティソフトウェアの警報、ログ、公に入手できる情報、人間である。表3-2に、各分類に対する前兆と兆候の一般的なソースを示す。

44 自動的なセキュリティ体制の変更の例としては、侵入防止ソフトウェアがある。これは、異常な偵察活動を検知し、以降の関連する活動をブロックする。手動のセキュリティ変更の例としては、管理者が新しいファイアウォール規則を作成し、特定のホストへの接続をブロックする方法がある。

表3-2 前兆と兆候の一般的なソース

前兆または兆候のソース	説明
コンピュータセキュリティソフトウェアの警報	
ネットワーク型IDPS、ホスト型IDPS、ワイヤレスIDPS、ネットワーク行動分析用IDPS	IDPS製品は疑いのある事象を見つけ、それに関する関連データを記録するように設計されている。記録されるデータは、攻撃を検出した日付と時刻、攻撃の種類、送信元と宛先のIPアドレス、ユーザ名(該当かつ判明する場合)などである。ほとんどのIDPS製品は、攻撃シグネチャを使って悪意のある活動を発見する。最新の攻撃を検知できるように、シグネチャは最新に保つ必要がある。IDPSは、誤検知を起こす場合がある。誤検知とは、実際に悪意のある活動がないにもかかわらず、警報を発してしまうことである。分析者は、記録されたサポートデータを詳しくレビューするか、関連データをほかのソースから入手して、IDPSの警報を手動で検証する必要がある。これらの4つのIDPSは、それぞれに異なるデータ収集機能、ロギング機能、侵入検知機能、および侵入防止機能を備えている。[45] ほとんどの環境においては、複数の種類のIDPSを導入すべきである。
ウイルス対策ソフトウェアおよびスパムメール対策ソフトウェア	ウイルス対策ソフトウェアおよびスパイウェア駆除ソフトは、さまざまな形式の悪意のコードを検出し、それらのコードがホストに感染するのを防止する。悪意のコードを検出すると、ウイルス対策ソフトウェアまたはスパイウェア駆除ソフトは、警報を発する。現在のウイルス対策製品およびスパイウェア駆除製品は、シグネチャを最新にしておけば、非常に効果的に悪意のコードを検知、根絶、隔離する。このアップデート作業は、大規模な組織では手に負えなくなってしまうこともある。ひとつの対処方法としては、各ホストが更新をプルするように設定されるのを期待するのではなく、中央のウイルス対策ソフトウェアがシグネチャの更新を各ホストにプッシュするようにすることである。ウイルス対策製品によって検知内容が違うため、複数のベンダーの製品を使用して網羅性と正確性を高めている組織もある。ウイルス対策ソフトウェアは、ネットワーク境界(ファイアウォール、電子メールサーバなど)と、ホストレベル(ワークステーション、ファイルサーバ、クライアントソフトウェアなど)の、少なくとも2つのレベルに配備するべきである。スパイウェア駆除ソフトは、ウイルス対策ソフトウェアが堅牢なスパイウェア検知機能を備えていない場合に、使用する。スパイウェア駆除ソフトを使用する場合は、ウイルス対策ソフトウェアを使用する場合と同レベルの配備を行うこと。 スパイウェア駆除ソフトは、スパムを検出し、スパムがユーザのメールボックスに届かないようにする。スパムには、マルウェアやフィッシング攻撃などの、悪意を持つコンテンツが含まれている場合がある。よって、スパイウェア駆除ソフトによる警告は、攻撃が試みられたことを示す場合がある。
ファイル完全性チェックソフトウェア	事件により重要なファイルが改ざんされることがあるが、ファイル完全性チェックソフトウェアは、そのような改ざんを検知することができる。このソフトウェアは、ハッシュアルゴリズムを用いて指定された各ファイルのチェックサムを計算する。ファイルが改ざんされた後でチェックサムを再計算すると、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きわめて高い。チェックサムを定期的に再計算し、以前の値と比較することで、ファイルの改ざんが検知できる。
サードパーティーの監視サービス	サードパーティーに費用を払って、ウェブサーバ、DNS (Domain Name System)サーバ、FTPサーバなどの、だれでもアクセスできるサービスの監視を依頼する組織もある。サードパーティーは、各サービスに *x* 分ごとに自動的にアクセスする。サービスにアクセスできない場合、電話、ポケットベル、電子メールなど、組織が指定した方法で警告する。監視サービスによっては、ウェブページなど、特定のリソースの改ざんを検知して警報を発することも可能である。監視サービスは主に運用面の観点から有効だが、DoS攻撃やサーバ侵入の兆候も提供することができる。

45 NIST SP 800-94『*Guide to Intrusion Detection and Prevention Systems (IDPS)*』では、IDPS技術の特性に関する記述と、それらの技術の設計、実施、設定、安全化、監視およびメンテナンスに関する奨励事項を提供している。このドキュメントは、//csrc.nist.gov/publications/PubsSPs.html で入手可能である。

ログ	
オペレーティングシステム、サービス、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、アプリケーションのログ(特に監査関連のデータ)は、事件が発生した場合に大きな価値があることが多い。ログからは、アタッカーがどのアカウントにアクセスしたか、どのような活動を行ったかなど、豊富な情報が得られる。また、ログは、イベント情報の集約にも寄与する。これによりユーザは、一つのイベントでスキャンされたホストの総数を割り出すことができる。残念なことに多くの事件では、ログに証拠が残っていないことが多い。その理由としては、ホスト上でログの取得が無効になっている、または設定が正しくないなどがあげられる。事件を効果的に処理するためには、全システムでの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する。すべてのシステムで監査を有効にし、監査イベント、特に管理レベルでの活動をログに取得する。また、すべてのシステムを定期的にチェックし、ログ取得が適正に機能していること、およびログ取得の標準に準拠していることを確認する。ログは適切に循環、保存すること。ログファイルを保存する際には、ファイルの完全性のチェックを行い、ログが不正にアクセスされて改ざんされていないことを確認する。ログは、複数イベントの相互的な関連づけを可能にし、イベント分析を助成する。イベント情報によっては、事件と判断され、警告が生成されることもある。ログの一元管理を行うソフトウェアには、syslog、security event and information software、ホスト型IDPSなどがあり、種類は豊富である。[46]セクション3.2.4では、ログの一元化を行うことの価値について説明する。
ネットワーク機器のログ	ファイアウォールやルーター等のネットワーク機器のログは、一般には前兆または兆候の一次ソースとしては用いられない。通常、これらの機器は、ブロックした接続の試みをログに記録するように設定されているが、その活動の特性については、ほとんど情報を得ることができない。それでも、傾向(特定のポートへのアクセス試みの回数が大幅に増加したなど)を見て、ほかの機器で検知された事象と相関させることで有効に利用できる。
公に入手できる情報	
新しい脆弱性とエクスプロイトに関する情報	新しい脆弱性とエクスプロイトの情報を絶えずチェックすることで、いくつかの事件の発生を予防することができる。また、このような活動は、新しい攻撃の検知と分析にも役立つ。NVD(National Vulnerability Database)は、脆弱性に関する情報を含むデータベースである。[47] US-CERT [48]、CERT®/CC、IAIP、エネルギー省のCIAC (Computer Incident Advisory Capability [49]といったいくつかの組織から、ブリーフィング、ウェブの投稿、メーリングリストを通じて、定期的に脅威の最新情報が提供されている。
ほかの組織での事件に関する情報	ほかの組織で起きた事件に関する報告は、豊富な情報を提供してくれる。インシデント対応チームやセキュリティの専門家が、自分たちが遭遇した偵察や攻撃に関する情報を共有できるようなウェブページやメーリングリストがある。さらに、ほかの多くの組織からのログや侵入検知警報を収集、整理、分析している組織もある[50] 。
人	
組織内の人間	組織内のユーザ、システム管理者、ネットワーク管理者、セキュリティスタッフ、その他の人間が、事件の兆候を報告する場合がある。このような報告は、すべて確認することが重要である。一般にユーザは、事件が起きているかどうかを判断するだけの知識を持っていない。また、最高の訓練を受けた技術の専門家であっても、間違いを起こすことがある。そのような情報を提供した人間に、情報の正確さについてどの程度の確信があるかを聞くのもひとつの方法である。この評価と提供された情報を合わせて記録しておくと、特に矛盾するデータが見つかった場合などには、事件の分析において非常に役に立つ。

46 NIST SP 800-92『コンピュータセキュリティログ管理ガイド(*Guide to Computer Security Log Management)*』では、ログ管理の課題に対応するための、奨励事項を提供している。このドキュメントは、//csrc.nist.gov/publications/PubsSPs.html で入手可能である。

47 http://nvd.nist.gov/

48 http://www.us-cert.gov/cas/signup.html

49 http://www.ciac.org/ciac

50 Internet Storm Center (http://isc.incidents.org)は、事件の動向に関する無料の情報ソースである。

他の組織の人間	ほかの組織の人間から事件の報告を受けるということはほとんどないが、あった場合にはかなり重く受け止めるべきである。よくある例としては、特定の組織のシステムに重大な脆弱性を見つけたハッカーが、その問題について当該組織に直接連絡してくるか、公衆に発表することがある。ほかの可能性としては、外部組織から連絡が入り、自組織内のだれかがその組織を攻撃していると言われることもある。外部ユーザがその他の兆候(書き換えられたウェブページや、サービスが利用できないなど)を報告してくる場合もある。ほかのインシデント対応チームから事件の報告を受ける場合もある。外部の関係者が兆候を報告するための手段を設け、訓練を受けたスタッフがこの手段を注意して監視することが大切である。単に電話番号と電子メールアドレスを準備し、メッセージをヘルプデスクに転送するようにするだけで済むこともある。

3.2.4. 事件の分析

すべての前兆または兆候が正確であることが保障されていれば、事件の検知と分析は簡単であるが、不幸なことに実際にはそうではない。たとえば、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は、正しくないことがある。侵入検知システムが、多数の誤検知(誤った兆候)を生成するのは、よく知られている。これらは、事件の検知と分析を難しくしているものの例である。このため組織は、各兆候を評価して、正しい情報であるかどうかを判断する必要がある。さらに悪いことに、人間または自動化されたソースから得られる兆候の合計は、一日に数千から数百万にもなる。ごく少数の本当に起きたセキュリティインシデントを、すべての兆候の中から見つけ出すことは、気が遠くなる作業である。

たとえ兆候が正しいとしても、必ずしも事件が起きたとは限らないのだ。ウェブサーバのクラッシュや、重要なファイルの改ざんは、セキュリティインシデント以外でも、人為的ミスなど、いくつもの理由で発生する可能性がある。とはいえ兆候があった場合には、事件が起きたことを疑い、相応に行動するのが妥当である。一般に、事件処理担当者は、事件が起きていないと判断できるまでは、起きていると仮定すべきである。特定の事象が実際に事件であるかどうかを決定するのは、判断の問題となることもある。場合によっては、ほかの技術者や情報セキュリティ担当者と協力して判断することが必要な場合もある。多くの場合組織は、その状況がセキュリティに関係があるかどうかにかかわらず、同じように対処することが求められる。たとえば、12時間ごとにインターネットに接続できなくなり、だれも原因がわからない場合、スタッフは問題の早期解決に向けて、(セキュリティ関連の事件に使用するのと)同じリソースを使用して問題を診断するだろう。

明らかに書き換えられたウェブページなど、検知が簡単な事件もある。しかし、多くの事件は、そのように明確な症状に結びつかない。1つのシステムコンフィグレーションファイルの1つの変化といった小さな兆候が、事件が起きたという唯一の兆候であることもある。事件処理において最も難しい作業が、事件の検知であるかも知れない。事件処理担当者には、不明確で、矛盾する、不完全な症状を分析して、何が起きたかを判断する責任がある。検知をある程度簡単にする技術的な解決法はあるものの、最善の対策は、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のできる、十分な経験を持った熟練したスタッフメンバーからなるチームを編成することである。十分に訓練された能力のあるスタッフなしでは、事件検知と分析は効率が悪いものとなり、手痛い間違いを犯すことになる。

インシデント対応チームは、各事件の分析と検証を行うために素早く作業し、各ステップを文書化する。事件が起きたとチームが確信した場合には、チームは迅速に初動分析を行い、影響のあるネットワーク、システム、アプリケーションなどの事件の範囲、事件の犯人や原因、どうやって事件が起きたか(どのツールや攻撃方法が使用されたか、どの脆弱性が悪用されたか)を特定する。初動分析を通じて、事件の封じ込めや、事件の影響のより詳しい分析など、以降の行動に優先度を付けるのに十分な情報を得ることができる。疑わしい場合には、事件処理担当者は、さらなる

分析で問題がないとわかるまでは、最悪の事態を想定[51]すべきである 。

最初の分析と検証は、難しい作業である。以下に示すのは、事件の分析をより簡単かつ効果的に行うための推奨事項である。

+ **ネットワークとシステムのプロファイル** プロファイリングとは、変更が簡単に見つかるよう、予想される活動の特性を測定することである。プロファイリングの例としては、ファイル完全性チェックソフトウェアをホスト上で実行して重要なファイルのチェックサムを計算したり、ネットワークの帯域使用率やホストのリソース使用率を監視して、さまざまな日のさまざまな時間の平均とピーク使用率レベルを求めるといったことがある。プロファイリングプロセスが自動化されれば、活動の変化を素早く検知して管理者に報告することができるが、実際には、プロファイリング技術を使って正確に事件を検知するのは難しい。組織は、いくつかある検知や分析技術の一つとしてプロファイリングを利用するべきである。

+ **正常動作の理解** 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、アプリケーションを調査し、正常な動作がどのようなものかを確実に理解して、異常時の動作をより簡単に見分けられるようにする。環境全体にわたってすべての動作に関する包括的な知識を得ることができる事件処理担当者はいないが、事件処理担当者はどの専門家がギャップを埋めることができるかについて知っておくべきである。

  この知識を得るためのひとつの方法は、ログエントリーとセキュリティ警報のレビューである。フィルタリングによってログが適当なサイズになっていないと、これはうんざりするような作業になる。処理担当者がログや警報に慣れてくると、説明がつかないエントリーに焦点を当てることができるようになる。このようなエントリーは、ほかのエントリーに比べて、より調査が必要となるものであり、また、より興味深いものである。ログを頻繁にレビューすることで、分析者は常に新しい知識を身につけ、ある時間にわたる傾向や変化に気づくことができる。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る。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、事件を処理する準備にもなる。事件の処理では、これらのスキルが必要になる。

+ **一元化されたログ取得とログ保管ポリシーの作成** 事件に関する情報は、ファイアウォール、ルーター、IDPS、およびアプリケーションログなど、いくつもの場所に記録される。そこで、一元的なログサーバを設置して、組織内のログを生成する各装置が、ログエントリーのコピーをそのサーバに送るように設定する。[52] こうすることで、関係するすべてのログエントリーが集まるため、事件処理担当者にとっては便利である。この統合により、ログの安全な格納場所も提供され、アタッカーが侵入したホスト上でロギングを無効にしたり、ログを改ざんしたりした場合の影響を減らすことができる。さらに、ログデータをどれだけ長く保持するかを規定したログ保管ポリシーの作成と実施は、分析の際に非常に役立つ。なぜなら、古いログエントリーから偵察活動が判明したり、以前と同様の攻撃があったことがわかる場合があるためである。ログを保管するもうひとつの理由は、事件が数日、数週間、数ヶ月間後にならないと発見されない可能性があるためである。ログデータを保管する期間は、組織のデータ保管ポリシーや、データの量など、いくつかの要因に依存する。

---

51 組織によっては、別のインシデント対応モデルを採用しているところもある。そのモデルでは、組織内のほかの者(システム管理者、ネットワーク管理者、または、セキュリティ管理者など)が、事件が本物だと確認するまでは、事件への対応をインシデント対応チームに依頼しない。どちらのモデルも有効であり、組織は、スタッフのリソースやスキルに応じて適切なモデルを選べばよい。

52 NIST SP 800-92『コンピュータセキュリティログ管理ガイド(Guide to Computer Security Log Management)』では、ログ管理の課題に対応するための、奨励事項を提供している。このドキュメントは、//csrc.nist.gov/publications/PubsSPs.html で入手可能である。

一般に、ログデータは少なくとも数週間、できれば数ヶ月間保管すべきである。

+ **イベント相関処理の実施** 事件の証拠は、いくつものログで捕捉される可能性がある。各ログは、事件に関する異なる種類のデータを含む可能性がある。たとえば、ファイアウォールのログが使用されたソースIPアドレスを含み、アプリケーションのログがユーザ名を含むといった具合である。ネットワーク侵入検知センサーは、特定のホストが攻撃されたことを検知できるが、攻撃が成功したかどうかまではわからない可能性がある。分析者はホストのログを調査して、この情報を判断する必要がある。複数の兆候のソースの間でイベントの相関処理を行うことは、ある事件が発生したかどうかを検証する上でも、各データを素早く整理する上でも、非常に有益なことである。イベントの相関処理では、ネットワーク、ホスト、サービス、アプリケーション、セキュリティ装置からのデータを一箇所に集めることになるため、一元化したログを使用することで、イベントの相関処理が簡単に素早く行えるようになる。

+ **すべてのホストの時刻を同期させておく** NTP (Network Time Protocol)のようなプロトコルは、ホスト間でクロックを同期させるために使用される[53]。イベントを報告する機器の時刻の設定が合っていないと、イベントの相関処理が難しくなるため、時刻を合わせることはインシデント対応にとっては重要なことである。証拠の観点からは、ログのタイムスタンプに矛盾がないことが非常に望ましい。たとえば、12:07:01、12:10:35、11:07:06 に攻撃が起きたことを示す3つのログがあるよりも、ある攻撃が 12:07:01 a.m.に起きたことを示す3つのログがあったほうがよい。

+ **情報の知識ベースの維持と利用** 知識ベースには、処理担当者が分析の際に素早く参照する必要がある情報を格納しておく。知識ベースは複雑な構造にすることもできるが、単純なアプローチが有効である。テキストドキュメント、スプレッドシート等、比較的単純なデータベースが、チームのメンバー間でデータを共有するのに効果的かつ柔軟な仕組みを提供する。付録Gには、プロトコル分析(広く使われているポート番号など)に役立つドキュメントへのポインターを掲載している。知識ベースには、以下のような情報も格納する。

  - 悪意のコードとデマ情報へのリンク。一般的に、最も包括的で最新の情報源は、主要なウイルス対策ソフトウェアベンダーである。

  - スパム送信のブラックリストに載っているドメイン一覧へのリンク

  - 侵入検知警報、オペレーティングシステムのログエントリー、アプリケーションのエラーコードなどが示す、前兆や兆候の重要性と正当性の説明。

+ **インターネットのサーチエンジンを使った調査** GoogleやYahooなどの総合的なサーチエンジンは、異常な活動、特にスキャニングなどについての情報を探すのに便利である。たとえば、分析者がTCP (Transmission Control Protocol)ポート22912をターゲットにした、異常なスキャンを見つけたとする。そこで、「TCP」、「ポート」、「22912」などの用語で検索すると、いくつかヒットするものがあり、その中に同様の活動のログが含まれていたり、ポート番号の重要性についての説明が含まれている場合もある。インシデント対応や侵入検知に関する公開メーリングリストのほとんどは、ウェブベースのアーカイブを持っているため、インターネットサーチエンジンはリストのアーカイブも検索する。処理担当者は、アクセス可能な個人のメーリングリストやフォーラムを検索したり、他のCSIRTに連絡して、そのような活動を見たことがないかどうか尋ねることもできる。

+ **パケットスニッファを使った補足データの収集** いくつかの兆候では、処理担当者が何が起

53 NTPの詳細は、http://www.ntp.org を参照のこと。

きているのかを理解するのに十分な詳細が記録されないことがある。事件がネットワーク上で起きている場合に必要なデータを収集する最も早い方法は、パケットスニッファを使ってネットワークトラフィックを捕捉することである。特定の条件に一致したトラフィックを記録するようにスニッファを設定すれば、データを扱いやすい量に抑えることができ、かつ、うっかりほかの情報を捕捉することも少なくなる。組織によってはプライバシーの面から、事件処理担当者がスニッファを使う前に、許可を申請して取得しなくてはならないこともある。スニッファは、ネットワークベースの攻撃に関し、最も純粋で完全なデータを提供してくれる。事件によっては、スニッファを使わなければ解決が非常に難しいものがある。

+ **データのフィルタリングの検討** 多くの組織では、すべての兆候をレビュー･分析する時間はない。大量のデータを目の前にすれば圧倒されてしまうのが人間であり、多くの場合、単にデータを無視してしまう。事件の有効な検知を促進するため、このような反応を克服し、少なくとも最も疑わしい活動は調査するようにする必要がある。有効な戦略のひとつは、兆候をフィルタリングして、兆候の分類のうちあまり重要でないものは分析者に見せないことである。もうひとつの戦略は、兆候をフィルタリングして、最も重要な兆候の分類だけを分析者に見せることである。ただし、新しい悪意のある活動が選択した兆候の分類になるとは限らないため、このアプローチは危険である。しかし、このアプローチも、兆候をまったくレビューしないよりはましである。

+ **経験を最優先する** 活動の意図を判断することは困難な場合が多い。たとえば、処理担当者がDNSサーバに関する異常な活動(攻撃ではなく、異常なトラフィックパターンとポート番号)を見つけたとする。これは、DNSサーバに攻撃をしかけるための偵察なのか？または、DNSサーバを仲介装置として使って他のサーバを攻撃しようとしているのか？あるいは、ロードバランサーが生成した良性のトラフィックなのか？このデータについては考えられる説明がいくつかあり、処理担当者にとっては十分に詳細な情報がないために、どの説明が正しいかを最終的に判断できない。疑わしい活動の意図を判断する最良の方法は、できるだけ多くの事件処理経験を積むことである。経験のある処理担当者であれば、データをレビューすることにより、事件の重大さをすぐに直感できる。

+ **経験が少ないスタッフのための診断マトリックスの作成** このようなマトリックスは、ヘルプデスクのスタッフ、システム管理者など、自分で兆候や前兆を分析する人に最も役立つ。また、新しい侵入検知分析者や、インシデント対応チームのメンバーにも役立つ。表3-3は、診断マトリックス例の抜粋であり、症状を左側に、事件のカテゴリを上に並べてある。マトリックス内のボックスは、一般的にどの兆候が各事件のカテゴリと関連するかと、その兆候とカテゴリとの関連の強さを示す。強さは、参考になるのであれば、「はい」「いいえ」で表現しても、割合で表現してもよい。このマトリックスは、兆候を見て考えられる原因を特定することができない、経験が少ないスタッフメンバーに対する手引きとなる。このマトリックスは、トレーニングツールとしても利用できる。マトリックスの各エントリーの根拠や、それぞれの種類の事件の確認方法など、補足説明文を追加すると、このマトリックスはより有用なものになる。

表3-3 診断マトリックス例の抜粋

症状	サービス不能	悪意のコード	不正アクセス	不適切な使用
ファイル、重要、アクセスの試み	低	中	高	低
ファイル、不適切な内容	低	中	低	高
ホストクラッシュ	中	中	中	低
ポートスキャン、受信、異常	高	低	中	低
ポートスキャン、送信、異常	低	高	中	低
使用、帯域、高	高	中	低	中
使用、電子メール、高	中	高	中	中

+ **他からの支援を求める** 場合によって、チームが事件の完全な原因と性質を判断できないことがある。チームに、事件を封じ込めて根絶するだけの十分な情報がない場合は、内部リソース(情報セキュリティスタッフ)や外部リソース(US-CERT、ほかのCSIRT、インシデント対応ノウハウを持った契約業者)に事件の分析、封じ込め、根絶の支援を依頼することになる。事件を完全に封じ込め、悪用された脆弱性を修正し、同様の事件が起こらないようにするためには、各事件の原因を正確に判断することが重要である。

3.2.5. 事件の文書化

事件が起きている、または起きたことが疑われる場合は、すぐに事件に関するすべての事実を記録し始めることが大切である[54]。このための記録媒体としては、日誌が最も単純であるが[55]、PDA、ラップトップコンピュータ、オーディオレコーダ、デジタルカメラもこの目的で活用できる[56]。システムイベント、電話の会話、発見したファイルの改ざんを文書化することは、より効率的で、より体系的で、間違いの少ない問題処理につながる。事件が検出された時点から最終的に解決された時点までのすべてのステップは、文書化して、タイムスタンプを記録する。事件に関するすべてのドキュメントには日付を記入し、事件処理担当者がサインをする。こういった情報は、告訴することになった場合に、法廷で証拠として使用することもできる。処理担当者は、最低でも2名のチームになって作業を行うようにする(一人がイベントを記録し、もうひとりが技術的な作業を行う)。セクション3.3.2では、証拠についてさらに詳しく説明する。

インシデント対応チームは、事件の状態と、関連するほかの情報の記録を保持する[57]。このような目的でアプリケーションやデータベースを使用することは、事件をタイムリーに処理して解決するためにも、必要となる[58]。たとえば、ある事件処理担当者が、前の日に別の担当者が対処した事

54 事件処理担当者は、事件に関する事実だけを記録し、個人的な意見や結論は記述しない。主観的な内容は、証拠として記録するのではなく、事件報告書に記載する。

55 日誌を使用する場合は、バインド(ひもなどで綴じること)し、インクを使ってページ番号を記入し、ページが抜き取られたりしないように、完全な状態で保つことが望ましい。

56 機器を使用する前に、その機器を使用して収集した証拠の適正性を検討すること。たとえば、証拠資料になりうるデバイスは、それ自体を他の証拠を記録するために使用してはならない。

57 付録Cに、事件を報告する際に収集する、推奨されるデータフィールドの一覧を示す。また、CERT®/CCのドキュメント『State of the Practice of Computer Security Incident Response Teams (CSIRTs)』には、事件報告フォームの例がいくつか掲載されている。このドキュメントは、http://www.cert.org/archive/pdf/03tr001.pdf から入手可能である。

58 パデュー大学が開発したCenter for Education and Research in Information Assurance and Security (CERIAS) Incident Response Database (CIRDB)は、事件関連のデータを記録し、事件を追跡するための仕組みである。CIRDBは、https://cirdb.cerias.purdue.edu/ から入手できる。

件に関係する緊急の呼び出しを受けたが、その担当者はちょうど休暇に出かけたということもありうる。処理担当者は、以下の情報が格納されている事件データベースにアクセスすることで、素早くその事件について知ることができる。

+ 事件の現在の状態
+ 事件の概要
+ この事件に対して、事件処理担当者がとった行動の内容
+ ほかの関連者(システム所有者、システム管理者など)の連絡先情報
+ 事件調査の際収集した証拠の一覧
+ 事件処理担当者からのコメント
+ 次にとるべきステップ(たとえば、システム管理者によるアプリケーションへのパッチの適用を待つなど)[59]

事件に関するデータには機密情報が含まれていることが多いので、インシデント対応チームは事件に関連するデータの保護に注意を払うべきである。たとえば、悪用された脆弱性に関するデータ、最近のセキュリティ違反、不適切な活動を行った可能性があるユーザなどである。機密情報が不当に漏れてしまうリスクを減らすため、事件データへのアクセスは、適切に制限すること。たとえば、権限を持った者だけが事件データベースにアクセスできるようにする。事件に関連する電子メール、事件報告書などのドキュメントは暗号化し、送信者と送信者の意図した受信者だけが読めるようにする。[60]

3.2.6. 事件の優先順位付け

事件処理の優先順位付けは、事件処理プロセス中で、おそらくもっとも重要な判断ポイントである。リソースに制限があるという理由で、起きた順に事件を処理するということは、やめるべきである。代わりに、2つの要因に基づいて、処理に優先順位を付ける。

+ **事件による、現在および将来起こりうる技術的な影響** 事件処理担当者は、事件による現在の技術的な悪影響(たとえばデータへの不正なユーザレベルアクセス)だけでなく、事件をすぐに封じ込めない場合の、将来予想される技術的な影響(たとえばroot奪取など)も考慮すべきである。たとえば、ワークステーションに感染して広まるワームは、現在は影響が少ないかもしれないが、数時間以内には、ワームのトラフィックにより、主なネットワークが停止してしまうかもしれない。
+ **影響を受けたリソースの重要度** 事件により影響を受けるリソース(たとえばファイアウォール、ウェブサーバ、インターネット接続、ユーザワークステーション、アプリケーションなど)の、組織に対する重要度はさまざまである。リソースの重要度は、主にそのデータやサービス、ユーザ、信頼関係、ほかのリソースとの相互依存関係、可視性(たとえば、公開ウェブサーバと内部の部門ウェブサーバ)によって決まる。多くの組織は、業務継続

59 Trans-European Research and Education Networking Association (TERENA)が作成したRFC 3067, TERENA's Incident Object Description and Exchange Format Requirements (http://www.ietf.org/rfc/rfc3067.txt)は、各事件でどのような情報を収集すべきかの助言を与えてくれる。IETF Extended Incident Handling (inch)ワーキンググループ (http://www.cert.org/ietf/inch/inch.html)により、TERENA の作業を拡張するRFCである、RFC 5070, Incident Object Description Exchange Format (http://www.ietf.org/rfc/rfc5070.txt).が作成された。

60 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(Guide to Integrating Forensic Techniques Into Incident Response)』では、コンピュータフォレンジック機能の確立に関する詳細(方針および手順の策定を含む)を提供している。

計画またはサービス内容合意書(SLA)を通じてリソースの重要度を決めており、それらの中に各主要リソースを復旧するための最大時間を明記している。可能であれば、インシデント対応チームは、リソースの重要度に関する既存の有効なデータを入手して利用するべきである[61]。

影響を受けるリソースと、事件による現在および将来的な技術的影響を合わせて検討することで、事件のビジネスインパクトが決まる。たとえば、ユーザのワークステーションでのroot奪取の場合は、生産性が若干落ちるだけで済むかもしれないが、公開ウェブサーバのユーザレベルの不正アクセスの場合は、収益、生産性、サービスへのアクセス、評判に大きな損害をもたらし、機密データ(クレジットカード番号、社会保障番号など)が漏れてしまうこともある。チームは、事件によるビジネスインパクトの推定に基づいて、各事件への対応に優先順位をつける。たとえば、セキュリティに関連しない不適切な使用については、ビジネスインパクトが比較的低いことから、一般に他の種類の事件ほど迅速な対応を必要としない(セクション7は、このような事件に優先順位を付けるための手引きである)。

組織は、発生した事件がおよぼす自組織への影響を、定量化するのに最も適しているといえる。なぜなら組織は、自身の状況を最も良く理解しているためである。よってUS-CERTに事件を報告する組織は、個々の事件に対して、重大さ(severity rate)を設定すべきである。この重大さは、政府機関、連邦政府および国の重要インフラに対する影響を示すものである。[62] 組織による重要インフラへの影響の格付けは、US-CERTの事件処理を支援する。これによりUS-CERTは、重要インフラを脅かす(または影響を与える)事件を効果的に処理することができる。組織は、事件の重大さを特定するための準備として、表3-4 [63] を参照して、事件による2つの影響 (現在の影響および将来的な影響)の格付けを行う。

表3-4 影響の格付けの定義

値	格付け	定義
0.00	まったくない(None)	一つの政府機関、複数の政府機関、または重要インフラに対して、何の影響もない。
0.10	最低限(Minimal)	一つの政府機関に対して、ごくわずかな影響がある。
0.25	低位(Low)	一つの政府機関に対して、適度の影響がある。
0.50	中位(Medium)	一つの政府機関に対して深刻な影響をおよぼす、または、複数の政府機関や重要インフラに対して、ごくわずかな影響をおよぼす。
0.75	高位(High)	複数の政府機関または重要インフラに対して、適度の影響をおよぼす。
1.00	重大(Critical)	複数の政府機関または重要インフラに対して、深刻な影響をおよぼす。

61 業務継続性計画の基本的な概念は、ビジネスインパクト分析(BIA)であり、特定の事象の影響を決定することを意味する。組織のBIA情報を直接事件の優先順位付けに適用してもかまわない。

62 本セクションの「重大さ(severity rate)」の設定に関する情報(表3-4、3-5、3-6の内容を含む)、および「重大さ」を算出するための公式は、US-CERTが提供するものである。

63 本テーブルにおける「適度」は、「妥当な制限内である、または平均である、永久に機能不能となる程深刻ではない」ことを意味し、「深刻」は「重大であり、非常に危険または有害である」ことを意味する。

影響の格付けに続いて組織は、表3-5を参照して、事件に巻き込まれたシステムの重要度(criticality)を特定する。

表3-5 システムの重要度の格付けの定義

値	格付け	定義
0.10	最低限(Minimal)	任務上極めて重要なシステムではないシステム(従業員のワークステーションなど)またはインフラ。
0.25	低位(Low)	一つの政府機関の任務を支援するシステム(DNSサーバ、ドメインコントローラなど)ではあるが、任務上極めて重要なシステムではない。
0.50	中位(Medium)	一つの政府機関にとって、任務上極めて重要なシステム(給与システムなど)。
0.75	高位(High)	複数の政府機関または重要インフラの一部を支援するシステム(ルートDNSサーバなど)。
1.00	重大(Critical)	複数の政府機関または重要インフラにとって、任務上極めて重要なシステム。

全体的な重大さを算出するためには、以下の公式を使用する。

全体的な重大さ(または影響スコア) = Round ((現在の影響の格付け * 2.5) + (将来的な影響の格付け * 2.5) + (システムの重要度の格付け * 5))

算出結果と表3-6を照らし合わせることで、全体的な重大さの格付けが決定する。

表3-6 事件の重大さ(severity rate)の格付け

スコア	格付け
00.00 – 00.99	なし(None)
01.00 – 02.49	最低限(Minimal)
02.50 – 03.74	低位(Low)
03.75 – 04.99	中位(Medium)
05.00 – 07.49	高位(High)
07.50 – 10.00	重大(Critical)

各組織は、表3-7に示すマトリックス例のような形式で、優先順位付けのガイドラインを文書化すべきである。列見出しは、リソースの重要度を示し、行見出しは、技術的な影響の分類を示す。マトリックス内の値は、インシデント対応チームがその事件への対応を開始するまでの最大時間を示す。これは、インシデント対応に対するSLAとみなすことができる。一般に、SLAは事件を解決するまでの最大時間を指定するものではない。事件を処理するのに必要な時間はさまざまで

あり、たいていの場合、インシデント対応チームがコントロールできる類のものではないためである。マトリックスは、各組織のニーズと、リソースの重要度を決めるためのアプローチに基づいて、カスタマイズすることができる。たとえば、いくつかの重要度の分類があってもかまわない。被害のないウイルス感染などの小さな事件は、インシデント対応チームではなく、現場のITスタッフが処理することが最善の場合もある。また、マトリックスは、標準の勤務日に起きた事件に対するものと、休日に起きた事件に対するものの2つを作成するのが望ましい。

表3-7 インシデント対応SLAマトリックス例

現在の影響または将来予想される影響	事件により現在影響を受けている、または将来影響を受ける可能性が高いリソースの重要度		
	高い(インターネット接続、公開ウェブサーバ、ファイアウォール、顧客データなど)	中(システム管理者のワークステーション、ファイルサーバ、プリントサーバ、XYZアプリケーションデータ)	低い(ユーザのワークステーション)
ルートレベルアクセス	15分	30分	1時間
データの不正な変更	15分	30分	2時間
機密データへの不正アクセス	15分	1時間	1時間
不正なユーザレベルアクセス	30分	2時間	4時間
サービス利用不可	30分	2時間	4時間
嫌がらせ[64]	30分	ローカルITスタッフ	ローカルITスタッフ

事件が複数のリソース(システム、アプリケーション、データなど)に影響する場合には、1つの事件に対して2つ以上のマトリックスエントリーを適用してかまわない。事件処理担当者は、該当するすべてのマトリックスエントリーを特定し、最も急を要する行動から着手してもよい。たとえば、悪意のコードにより、重要度の高いリソースへの不正なユーザレベルのアクセス(30分以内に対応)と重要度の低いリソースへの侵入(1時間以内に対応)が可能となった場合、事件処理担当者はまず重要度が高いリソースの問題に対処し、次に重要度の低いリソースに対処することになる。場合によっては事件処理担当者が、重要度の低いリソースに対する調査を、指定されている最大開始時間(この例では1時間)よりも早く開始したいと思うかもしれない。その調査から他のリソースの事件を処理する際に役立つ情報が得られると確信できる場合には、なおさらである。

マトリックスのアプローチは、インシデント対応チームがさまざまな状況下でどのように対処すべきかについて、組織が注意深く考えることを促す。マトリックスは、事件処理の判断を行うためのフレームワークを提供することにより、事件処理担当者の時間を節約する。事件の間、処理担当者は、非常に大きなストレスにさらされ、意思決定が難しい場合がある。事件処理担当者には、特に予期しない状況や異常な状況が発生した場合に、各自の判断に基づいて、あえてマトリックスに従わないといった自由裁量が求められる。。

各組織は、チームが指定された時間内に事件に応答しない場合に備え、エスカレーションプロセ

64 この分類は、ユーザにいやがらせをする以外の悪影響がない事件を指す。例としては、ユーザの画面に一時間に一度メッセージを表示するだけの悪意のコードへの感染などがある。

スを確立しておく。これはさまざまな理由により発生する。たとえば、携帯電話やポケットベルが故障した場合や、個人的な緊急の案件が発生した場合、事件処理担当者が夜中の呼び出しに答えた後にまた眠ってしまった場合などである。エスカレーションプロセスでは、どのくらいの時間応答を待つか、応答がなかった場合に何をすべきかを明記する。一般に、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ある。短時間(おそらく15分程度)待った後、インシデント対応チームのマネージャなど、事件をより高いレベルにエスカレーションさせる。その人物から一定の時間内に応答がない場合は、事件をより高いレベルのマネジメント層にエスカレーションさせる。誰かが応答するまでこのプロセスを繰り返す。

3.2.7. 事件の通知

事件を分析して優先順位を付けた後には、インシデント対応チームは組織内の適切な人間や、場合によっては他の組織に通知する必要がある[65]。事件をタイムリーに報告および通知することにより、すべての関係者が自らの役割を果たすことができるようになる。今日の情報セキュリティの脅威の影響の大きさと複雑さを考えると、共同で事件に対応するのが最も有効なアプローチである。インシデント対応ポリシーには、事件報告に関する項目を記載する。少なくとも、何を誰にいつ(最初の通知、定期的な最新状況の報告など)報告するかが含まれていなくてはならない。厳密な報告要件は機関によって様々であるが、一般に以下の関係者への通知が必要である。

+ CIO
+ 情報セキュリティ部門長
+ 各地区の情報セキュリティ担当
+ 組織内のほかのインシデント対応チーム
+ システムオーナー
+ 人事部門(電子メールによる嫌がらせなど、職員が関係する場合)
+ 広報部(公共性がある事件の場合)
+ 法務部(法的問題が想定される事件の場合)
+ US-CERT (連邦政府機関または連邦政府機関の業務を代行するシステムは、報告が義務付けられている)

US-CERTへの報告に関する要件は、事件の分類によって異なる。たとえば、悪意のコード関連の事件(分類3)は、事件検出後24時間以内に、不正アクセス関連の事件(分類1)は、事件検出後1時間以内に、US-CERTに報告しなければならない。事件の分類および報告要件は、付録Jに掲載している。

事件の処理の間、チームは特定の関係者に現在の事件の状態を頻繁に通知しなくてはならない場合がある。悪意のコードによる大規模な感染などのいくつかのケースでは、チームは組織全体に最新情報を連絡しなくてはならない。チームはさまざまな連絡手段(たとえば、本人が直接伝える、または紙に書いて渡すなど)を計画して準備しておき、特定の事件に適した手段を選ぶこと。たとえば、電子メールサーバが悪意のコードによって圧倒されている場合、電子メールで事件の最新情報を送るのは控えた方がよい。考えられる連絡手段としては、以下のものがある。

---

65 外部関係者への連絡については、セクション2.3.2で詳細に示す。

+ 電子メール
+ ウェブサイト(イントラネットベース)
+ 電話
+ 口頭(日次の状況説明)
+ ボイスメールの挨拶メッセージ(たとえば、事件の最新情報のための専用のボイスメールを設定し、挨拶メッセージを事件の最新情報を反映したものに更新する)
+ 紙(掲示板やドアにビラを貼る、すべての入り口でビラを手渡しするなど)

3.3. 封じ込め、根絶、復旧

図3-3 インシデント対応のライフサイクル(封じ込め、根絶、復旧)

3.3.1. 封じ込め戦略の選択

事件を検知･分析した後には、事件が広がってリソースを食いつぶしたり、被害が増加する前に、封じ込めることが大切である。ほとんどの事件では封じ込めが必要になるため、各事件の処理中の早い段階で検討することが重要である。封じ込めで最も重要なのが、意思決定である(たとえば、システムのシャットダウン、有線/無線ネットワークからの切断、モデムケーブルの切断、特定の機能の無効化など)。事件を封じ込めるための戦略と手順があらかじめ決まっていれば、このような意思決定はかなり容易になる。組織は、事件を処理する際の許容可能なリスクを定義し、相応の戦略を策定しておくべきである。

封じ込めの戦略は、事件の種類によってさまざまである。たとえば、電子メールを媒介としたウイルスへの感染に対する全体的な戦略は、ネットワークベースの分散サービス不能攻撃に対する戦略とはまったく異なる。このドキュメントのセクション4から8では、さまざまな種類の事件を封じ込めるための、具体的な手引きを提供する。事件の封じ込めに関しては、主な事件の種類ごとに個別の戦略を作成することが奨励される。組織は、迅速で効果的な意思決定ができるように、基準を明確に文書化しておくべきである。適切な戦略を決定するための基準には、次のものが含まれる。

+ リソースに対する潜在的な損害およびリソースの盗難の可能性
+ 証拠保全の必要性
+ サービスの可用性(ネットワーク接続、外部関係者へのサービス提供)
+ 戦略を実施するのに必要な時間とリソース
+ 戦略の有効性(事件の部分的な封じ込めや、完全な封じ込めなど)

+ 対策の期間(たとえば、4時間以内に中止する緊急回避策、2週間以内に中止する一時回避策、恒久策など)

特定の状況において、組織が、封じ込めを遅らせて、アタッカーの活動を監視する場合もある。通常これは、さらなる証拠を集めるために行う。インシデント対応チームは、封じ込めを遅らせることが現実的であるかどうかについて、法務部と話し合うべきである。システムに侵入されたことがわかっていて放置した場合、アタッカーが侵入したシステムを使って他のシステムを攻撃した事に対して組織が責任を負う事になる場合がある。また、アタッカーが不正アクセスをエスカレートさせたり、短時間の間にほかのシステムに侵入したりする場合があるため、封じ込めを遅らせることは危険である。したがってこのような戦略は、アタッカーの行動を逐一監視し、瞬時にアタッカーを切断できる高度な経験を積んだインシデント対応チームだけが試みるべきである。ただしその場合でも、封じ込めを遅らせる事は通常、それにより生じる高いリスクには見合わないことに留意すること。

封じ込めに関連するもうひとつの潜在的な問題は、ある種の攻撃では、封じ込めを行うことで別の被害が生じる場合がある点である。たとえば、侵入されたホストが、ほかのホストに対して定期的にpingを実行するような悪意のあるプロセスを実行しているとする。事件処理担当者が事件を封じ込めるために侵入されたホストをネットワークから切断した場合、その後のpingは失敗する。この失敗の結果、悪意のあるプロセスがホストのハードディスク上の全データを(エラーログなどで)上書きするかもしれない。処理担当者は、ホストをネットワークから切断したからといって、ホストへのさらなる被害を防止できると考えてはならない。

3.3.2. 証拠の収集と処理

事件の際に証拠を収集する第一の目的は事件を解決することであるが、それらの証拠が法的な処置のために必要になる場合がある。[66] そこで重要なのは、侵入されたシステムに関する情報を含むすべての証拠をどのようにして保全したかを明確に文書化することである[67]。事前に法務部のスタッフや適切な法執行機関と話し合い、法廷で証拠として認められるように、適用される法律や規制を満たす手順を作成しておき、この手順に従って証拠を収集する[68]。また、証拠はいつでも説明できるようになっていなくてはならない。証拠を人から人に渡す際には、証拠・記録の保管フォームにその旨を記載し、各関係者がサインする。組織は、すべての証拠に対する詳細なログを保管する。それらには以下のものが含まれる。

+ 識別情報(たとえば場所、シリアル番号、型番号、ホスト名、MAC (Media Access Control)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・処理した者の名前、役職、電話番号
+ 証拠処理の日付と時刻(タイムゾーンを含む)
+ 証拠の保管場所

---

66 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(Guide to Integrating Forensic Techniques into Incident Response)』では、コンピュータフォレンジック機能の確立に関する詳細(方針および手順の策定を含む)を提供している。NIST SP 800-86は主に、PCを対象としたフォレンジック技術に焦点をあてているが、このドキュメントの内容の多くは他のシステムにも適用することができる。このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.htmlで入手できる。

67 証拠の収集と処理は、通常すべての事件については実施しない。たとえば、悪意のコードの事件の多くは、証拠を収集するに値しない。多くの組織では、ほとんどの事件の分析に、コンピュータフォレンジックを必要としない。

68 司法省(DOJ)のCCIPS (Computer Crime and Intellectual Property Section)による『Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations』は、証拠収集時の法的な手引きとして利用できる。このドキュメントは、http://www.cybercrime.gov/s&smanual2002.htmで入手可能である。もうひとつの便利なドキュメントが『Best Practices for Seizing Electronic Evidence』である。これは、米国財務省検察局 http://www.secretservice.gov/electronic_evidence.shtmlから入手できる。

コンピューティングリソースからの証拠収集には、いくつかの課題がある。一般に、事件発生が疑われる場合にはすぐに対象のシステムから証拠を収集するのが望ましい。多くの事件では、事象の動的な連鎖が起こる。問題とそのソースを特定するためには、システムのスナップショットが有効であり、これは、この段階で行うことができる他のほとんどの作業よりも優れている。調査中に事件処理担当者、システム管理者、その他の者が不注意によってシステムの状態を変えてしまうこともあるため、証拠の観点からはそのようなことが起きる前に、システムのスナップショットを取得するほうがより確実である。ユーザとシステム管理者は、証拠を保全するためにとるべきステップについて知らされるべきである。セクション3.3.2.1と3.3.2.2では、標準のコンピュータ(PC、サーバ、ネットワークデバイスなど)から収集した証拠と、モバイルデバイス(スマートフォン、PDA)から収集した証拠を保全するための情報を提供している。

3.3.2.1. 標準コンピュータを対象にしたフォレンジック

影響を受けたホストからファイルをコピーする前に、ファイルシステムやイメージバックアップには記録されない一時的な情報を収集するのが望ましいことが多い。この情報には、現在のネットワーク接続、プロセス、ログインセッション、オープンされているファイル、ネットワークインタフェースの設定、メモリーの内容などが含まれる。このデータに、アタッカーの身元や使用された攻撃方法の手がかりが含まれていることがある。ローカルクロックが実際の時刻とどれだけずれているかについても記録しておくと便利である。一方で、動作中のシステムから情報を取得することによるリスクについても留意すべきである。ホスト上で実行されたいかなるアクションによっても、ある程度マシンの状態が変わってしまう。また、アタッカーがシステムに侵入している最中に処理担当者の行動に気づくと、大変な結果になる可能性がある。

高度な訓練を積んだ注意深い事件処理担当者であれば、不用意に証拠を変えることなく、動的な証拠を取得するために必要な最低限のコマンドだけを実行することができる。深く考えずに選択されたコマンドを1つ実行しただけで、取り返しがつかないほど証拠が破壊されてしまうことがある。たとえば、単にディレクトリの内容を表示しただけでも、表示される各ファイルの最終アクセス時刻が変更されてしまう。さらに、情報を隠蔽したりさらなる被害を加えたりする目的で、コマンドが改変されていたり置き換えられている(トロイの木馬やルートキットなど)可能性があるため、侵入されたホストからのコマンドの実行は危険である。事件処理担当者は、侵入されたホストのコマンドを使用せずにすべての必要なコマンドが実行できるよう、信頼できるコマンドやすべての依存ファイルが入った、ライトプロテクトされたフロッピーあるいはCDを使用するべきである。また、「ライトブロッカー(write blocker)」プログラムを使って、ホストがハードディスクに書き込むのを防ぐこともできる。

一時的なデータを取得した後時間をおかずに、コンピュータフォレンジックのトレーニングを受けた事件処理担当者が、中身の入っていないライトプロテクトされたメディアかライトワンスメディアに完全なディスクイメージを作成する。ディスクイメージには、削除されたファイルやファイルフラグメントを含め、すべてのデータが保存される。証拠が告訴または内部の懲戒処分で必要になる可能性がある場合には、処理担当者は少なくとも2つの完全なイメージを作成し、適切にラベルをつけ、片方を証拠として使用するために安全に保管する(ディスクイメージだけはなく、すべての証拠にタグをつけて安全な場所に保管する)。場合によっては、処理担当者がオリジナルのディスクを証拠として確保することがある。その場合、システム復旧の一部として、2つめのイメージを別のディスクにリストアしてもよい。

コンピュータフォレンジックを実施するにあたっては、標準的なファイルシステムのバックアップよりも、ディスクイメージを取得するほうがより多くのデータが記録されるため優位である。イメージの取得が望ましい他の理由としては、オリジナルのリソース上で分析を行うよりも、イメージ上で分析したほうがはるかに安全なことが挙げられる。分析により、オリジナルデータを誤って変えてしまったり、破壊してしまうことがあるからである。。システムを動かし続けるこ

とのリスクよりも、システムを停止することによるビジネスインパクトのほうが大きい場合には、ディスクイメージを取得できない場合もある。しかしながら多くの事件の処理では、特に告訴には結びつかないような事件の処理では、標準的なファイルシステムのバックアップによって既存のファイルの情報を取得できるので、事が足りる場合もある。アタッカーを告訴するかどうかによらず、調査を継続する間イメージまたはバックアップを使ってターゲットをリストアすることができるため、ディスクイメージの取得とファイルシステムのバックアップはどちらも有効である。

コンピュータフォレンジックソフトウェアは、ディスクイメージを取得するためだけでなく、分析プロセスの多くを自動化するのに便利である。たとえば、以下のことが可能である。

+ ファイルフラグメント、隠れたファイルやディレクトリ、削除されたファイルやディレクトリを、あらゆる場所(たとえば、使用中の領域、空き領域、スラック領域)から見つけて復旧する
+ ファイルの拡張子(.doc、.jpg、.mp3など)に頼るのではなく、ファイル構造、ヘッダー、その他の特性を調査することによって、各ファイルに含まれているデータの種類を特定する
+ すべてのグラフィックファイルの内容を表示する
+ 複雑な検索の実行
+ 取得したドライブのディレクトリ構造をグラフィカルに表示する
+ レポートの生成

証拠収集の際には、たとえばアタッカーが使用したIPアドレスが含まれているファイアウォールのログなど、ほかのリソースの補足的なログファイルのコピーを取得するのが賢明である。ログは、ハードディスクやその他のメディアの取得と同様に、中身の入っていないライトプロテクトされたメディアか、またはライトワンスのメディアにコピーする。コピーの片方を証拠として保管し、もう片方を詳しい分析のためにほかのシステムにリストアする。通常処理担当者の多くは、ログファイルやデジタルの証拠物に対するメッセージダイジェストを作成する。これは、ファイルのチェックサムを生成することを意味する。ファイルを変更した後でチェックサムを再計算すると、チェックサムが同じになる可能性はきわめて低い。メッセージダイジェストは、FIPS 140-2 および FIPS 180-2 で検証済みのメッセージダイジェストアルゴリズムを使用したソフトウェアを使用して生成するべきである[69] (メッセージダイジェストは、コンピュータフォレンジックの他の用途にも便利である。たとえば、メディアを取得する際に、オリジナルとコピーの各メディアのチェックサムを計算しておき、イメージ作成の際に一貫性が維持されていることを確認するなど)。ログを取得する各ホストのローカルクロックの時刻と、実際の時刻とのずれがあれば、事件処理担当者はそれを記録する。

事件分析を支援するため、適切に記録されなかった事件の様子を再現したいと考える場合がある。たとえば、ユーザが悪意のあるウェブサイトを閲覧し、ワークステーションが破壊されたとする。この場合、ワークステーションには記録が残らない。そこで別のワークステーションを用意し、パケットスニッファとホストベースのセキュリティソフトウェアを使って活動を記録・分析しながら、同じウェブサイトにアクセスすることで、何が起きたかを判断することができる。このような攻撃を再現する場合には、不注意で他の事件を起こさないよう、十分に注意すること。

---

69 FIPS 180-2のタイトルは、『Secure Hash Standard』である。FIPS 140-2とFIPS 180-2で検証済みの一般的なメッセージダイジェストアルゴリズムとしては、Secure Hash Algorithm (SHA-1)がある。FIPS 140-2の検証については、http://csrc.nist.gov/groups/STM/cmvp/を、FIPS 180-2標準については http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf を参照のこと。

事件の再現が行われる他の例として、内部のユーザが不適切なファイルをダウンロードしていることが疑われる場合がある。ユーザがどのFTPサーバにアクセスしたかをファイアウォールが記録している場合、同じFTPサーバにアクセスして、どんな内容を含んでいるか、ユーザのワークステーションのファイル名がFTPサーバのファイル名と同じかどうかを確認する場合がある。ただし、その外部サービスが誰でも利用できる場合(匿名ログオンを許しているFTPサーバなど)にだけアクセスを検討すること。ネットワークトラフィックを監視して、ユーザがどのFTPアカウントとパスワードを使ったかを確認することもできるが、他人がその情報を再利用してFTPサーバにアクセスすることは、一般的に許されない。

3.3.2.2. モバイルデバイスを対象にしたフォレンジック

スマートフォンやPDAは、電子メールやウェブサイトへのアクセス、およびドキュメントの閲覧など、コンピュータ関連のさまざまな用途に利用されている。これにより組織が、事件に巻き込まれたモバイルデバイスに対して、フォレンジックを行う必要性が高まっている。モバイルデバイスからデータを抽出するための専用のフォレンジックツールや手順も存在する。このようなツールや手順の詳細は、本ドキュメントの範囲外であるため、ここでは扱わない。携帯電話を対象にしたフォレンジックの詳細は、NIST SP 800-101『Guidelines on Cell Phone Forensics』を参照のこと。[70]

3.3.3. アタッカーの特定

事件処理の際、システムオーナーなどは通常、アタッカーを特定したいと考える。特にアタッカーを告訴しようと考えている場合なら、この情報は重要かもしれないが、事件処理担当者は、あくまで封じ込め、根絶、復旧に重点を置くべきである。アタッカーの特定は時間がかかる割には効果がないプロセスであり、ビジネスインパクトを最小限にするというチームの第一目標が果たせなくなる可能性がある。以下では、アタッカーを特定するために最も一般的に行われる活動について説明する。

+ **アタッカーのIPアドレスの確認**　新任の事件処理担当者は、アタッカーのIPアドレスを重視することが多い。ping、traceroute あるいは他の接続確認のための手段を使って、アドレスが偽装されていないことを確認しようと試みる場合がある。しかし、そのアドレスのホストがリクエストに応答することがわかるのがせいぜいで、役には立たない。応答しないからといって、アドレスが本物でないとは限らない。例えば、ホストが ping や traceroute を無視するように設定されていることもありうる。アタッカーが動的な割り当てを受けたアドレス(たとえばダイヤルアップモデムのプールから)は、すでに別のだれかに再割り当てされているかもしれない。もっと大切なことは、IPアドレスが本物でチームがそのアドレスに ping すると、組織が活動を検知したことがアタッカーに知られてしまうかもしれないということである。事件を完全に封じ込める前にそのようなことになると、攻撃の証拠が入ったハードディスクを消去するなど、アタッカーはさらなる被害を及ぼす可能性がある。アドレスの検証などの活動を行う場合には、別の組織(たとえばISP)のIPアドレスを入手し、実際の活動元がアタッカーにわからないようにするべきである。

+ **アタッカーのシステムをスキャン**　事件処理担当者によっては、ping や traceroute を使って攻撃元のIPアドレスを確認するだけでなく、ポートスキャナ、脆弱性スキャナなどのツールを使って、アタッカーに関するさらなる情報の収集を試みる者もいる。たとえばスキャンにより、トロイの木馬がシステム上で受信待ちになっているのがわかれば、攻撃されたホストに侵入されたことがわかる。スキャンが組織のポリシーに違反したり、法律違反と

70 このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.html で入手できる。

なることもあるため、スキャンを実施する前に、この問題について法務部の担当者と話し合うこと。

+ **サーチエンジンを使ったアタッカーの調査** ほとんどの攻撃において事件処理担当者は、ソースIPアドレス、電子メールアドレス、IRCのニックネームなど、アタッカーの特定につながる情報をいくつかは得ることができる。このデータを使ってインターネットで検索を行うことで、アタッカーに関するさらなる情報が得られる場合がある。たとえば、同様のアタックに関するメーリングリストのメッセージや、アタッカーのウェブサイトが見つかることがある。一般にこのような調査は、事件を完全に封じ込める前に行う必要はない。

+ **事件データベースの利用** いくつかのグループが、さまざまな組織から収集した侵入検知システムのログデータやファイアウォールのログデータを整理して、事件データベースに保存している。いくつかのデータベースでは、特定のIPアドレスに関連する記録を検索できるようになっている。事件処理担当者は、このデータベースを使って、他の組織が同じソースからの疑わしい活動を報告していないかどうかを調べることができる。また、関連する活動がないか、組織自身の事件追跡システムやデータベースをチェックするのもよい。

+ **可能性のあるアタッカーの通信チャネルの監視** アタッカーを特定するために事件処理担当者が使うもうひとつの方法としては、アタッカーが使う可能性がある通信チャネルを監視する方法がある。たとえばIRCは、多くのBotが利用する主な通信手段であり、アタッカーが特定のIRCチャネルに集まって、自分が書き換えたウェブサイトについて自慢したり、情報を共有したりする場合もあるため、監視の対象となりうる。しかし、そのようにして得た情報は、事実としてではなく、より詳しく調査して確認する手がかりとして扱うべきである。

3.3.4. 根絶と復旧

事件を封じ込めたら、事件の要素を削除するための根絶を行わなくてはならない場合がある。これには、悪意のコードの削除や、破られたユーザアカウントを無効にするといったことが含まれる[71]。事件によっては、根絶が必要でない場合や復旧作業中に根絶を実施する場合がある。復旧では、管理者がシステムを通常の運用状態に戻し、(該当する場合には)同様の事件が起きないようシステムを強化する。復旧で行う作業には、クリーンなバックアップからのシステムのリストア、ゼロからのシステム再構築、侵害されたファイルのクリーンなファイルへの置き換え、パッチのインストール、パスワードの変更、ネットワーク境界のセキュリティ強化(ファイアウォールルール、境界ルーターのアクセスコントロールリスト)などがある。また、復旧作業の一環として、システムのロギングやネットワーク監視のレベルを上げることが望ましいことが多い。一度リソースへの攻撃が成功すると、再度攻撃されたり、組織の別のリソースが同様の手口で攻撃されることが多い。システムを復旧してセキュリティを高めるための多くの有用な情報が、インターネット上で入手することができる[72]。たとえば、NIST Checklist Programでは、さまざまなオペレーティングシステムやアプリケーションのセキュリティを高めるための、設定に関するチェックリストを提供している。[73]根絶と復旧活動は一般にオペレーティングシステムやアプリケーションに固有のものであるため、詳細な助言や手引きはこのドキュメントの範囲外である。

---

71 セクション4から8に、事件を分類ごとに根絶するための情報を示す。

72 http://csrc.nist.gov/publications/PubsSPs.html には、コンピュータセキュリティに関するNIST Special Publication へのリンクがある。CERT®/CCからも、システムのセキュリティを高め、事件から復旧するために有用なドキュメントが、http://www.cert.org/ で提供されている。

73 http://checklists.nist.gov/

3.4. 事件後の対応

図3-4 インシデント対応ライフサイクル(事件後の対応)

3.4.1. 教訓

インシデント対応の最も大切な部分のひとつであり、最も省略されがちなのが、学習と改善である。各インシデント対応チームは新しい脅威に対して進化し、技術を向上させ、教訓を学ぶべきである。これは多くの組織が認めているところであるが、大きな事件の後に(小さな事件については定期的に)、すべての関係者が参加して「反省会」を開催することは、セキュリティ対策とセキュリティ処理プロセス自体を改善するのに非常に有効である[74]。このミーティングで、何が起きたか、対策として何をしたか、それがどの程度有効だったかをレビューすることで、事件を締めくくる機会が得られる。このミーティングは事件が集結してから数日以内に実施すべきである。反省会で答えるべき質問には、以下のものがある。

+ 正確に何がいつ起きたか。
+ スタッフとマネジメント層がどの程度うまく事件に対処したか。文書化された手順に従ったか。それは適切だったか。
+ すぐに必要になった情報は何か。
+ 復旧を妨げたかもしれないステップや行動があったか。
+ 次に同様の事件が起きた場合、スタッフやマネジメント層は、どのような違った行動をとるか。
+ どのような是正措置があれば、将来にわたって同じ様な事件が起きるのを防げるか。
+ 将来事件を検出、分析、軽減するために、どのようなツールやリソースが追加で必要となるか。

小規模な事件では、限定的な事後分析でよいが、攻撃方法が新しく、広く関心や興味が持たれる事件はその限りではない。重大な攻撃が起きた後は、情報共有の仕組みとして、チームや組織の境界を越えた事後ミーティングを行うことに価値がある。このようなミーティングを開催する上での主な留意点は、適任者が参加することである。分析する事件にかかわった人を招くのももちろん重要だが、将来協力を得やすくするためにだれを招くべきかを検討するのも賢明である。

ミーティングの成功の可否は、議題にも左右される。ミーティングの前に参加者から期待と要望(話し合うトピックの提案も含む)を募ると、参加者の要望が満たされる可能性が高くなる。また、

74 一度の反省会で複数の事件を議題にしてよい。

ミーティングの前か開始時に打ち合わせのルールを確立しておくと、混乱や口論が少なくて済む。グループ討議を円滑化できるよう、1人かそれ以上の司会者に参加してもらうと、非常に有益な結果が得られる。最後に、議論で合意のあった主なポイントやアクションアイテムを記録し、ミーティングに参加できなかった関係者に配布することも大切である。

反省会には他にもメリットがある。反省会からの報告は、より多くの経験を持ったチームメンバーが事件にどのように対応するかを示すものであり、チームの新しいメンバーを教育するための優れた題材となる。インシデント対応ポリシーや手順を更新することも、教訓を生かすプロセスでは大切な部分である。事件の処理方法を事後分析することで、欠けているステップや手順の間違いがわかることも多く、変化のための刺激が与えられる。情報技術は日々変化し、要員も変わっていくため、インシデント対応チームは事件を処理するためのすべての関連ドキュメントと手順を、指定された周期でレビューすべきである。

もうひとつ重要な事後活動としては、各事件に対する追跡レポートの作成がある。これは、将来の利用を目的としたきわめて価値のある資料である。まず、レポートには、同様の事件の処理に役立つ参考資料を記載する。法的な観点から見て、イベントの正式な記録(システムのログデータなどのタイムスタンプを含んだ情報を含む)を作成することは、事件による金銭的な損害(ソフトウェアやファイルの消失、ハードウェアの損害、要員のコスト(復旧サービスを含む))の合計を見積もるのと同様に重要である。この見積は、その後の米国検事総長事務局などの機関による告訴のための基礎となる。追跡レポートは、記録保管ポリシーで決められた期間保管する[75] 。

3.4.2. 収集された事件データの利用

教訓を得るための活動を通じて、各事件に関する客観的なデータと主観的なデータを得ることができる。何年にもわたって収集された事件データは、いくつかの面で役立つ。特に、作業に要した合計時間と費用は、インシデント対応チームの追加投資を正当化するために利用できる。事件の性質を調査することで、体系的なセキュリティの弱点や脅威、事件の動向の変化がわかることもある。このデータをリスク評価プロセスに還元することで、最終的に追加のコントロールの選択と実施に結びつくこともある。もうひとつのデータの有効な利用方法は、インシデント対応チームの成功を評価することである。事件データが適切に収集･保管されていれば、インシデント対応チームの成功(あるいは少なくとも活動)の尺度がいくつか得られる。さらに、事件情報の報告を義務付けられている組織(たとえば連邦機関)では、その要求を満たすために必要なデータの収集が求められる。

単に入手できるからという理由でデータを収集するのではなく、訴訟で利用できるデータの収集に重点を置くべきである。たとえば、週毎に前兆となるポートスキャンの数を数え、その年の最後に集計した結果、ポートスキャンが8%増えたことがわかったとしても、その作業にかなりの時間をかけた割にはたいして役に立たない。絶対数は有益でない。必要なのは、それが組織のビジネスプロセスに対してどの程度脅威となるかを理解することである。各組織は、報告義務と、そのデータから期待される投資収益(たとえば、そのデータを使って新しい脅威を特定し、関連する脆弱性が悪用される前に、それらの脆弱性を軽減できるなど)を基にして、どの事件データを収集するかを決定すること。事件関連のデータに対する評価基準としては、以下のものが考えられる。

75 General Records Schedule (GRS) 24『Information Technology Operations and Management Records』によれば、「コンピュータセキュリティインシデントの処理、報告および追跡に関する記録」は、「必要なすべての追跡活動が完了してから3年後」に破棄することとなっている。GRS 24は、米国国立公文書館 (http://www.archives.gov/records_management/records_schedules.html) から入手できる。

+ **処理した事件の数**[76] より多くの事件を処理することが必ずしもよいことではない。たとえば、処理した事件数が減ったのは、インシデント対応チームの怠慢ではなく、ネットワークやホストのセキュリティコントロールが向上したためかもしれない。処理した事件の数は、インシデント対応チームが実行しなくてはならない相対的な作業量の基準であり、チームの質を測るものではない(ただし、作業の質を特定するための評価にもとづき、事件の件数がカウントされている場合を除く)。事件の分類(不正アクセスなど)ごとに個別に事件の数を集計すると、より効果的である。サブカテゴリを使えば、より効果的な情報が得られる。たとえば、内部の者による不正アクセスの数が増えた場合には、要員の身元調査に関するポリシーの強化およびコンピューティングリソースの誤使用に関するポリシーの強化、ならびに内部ネットワークのセキュリティコントロールの強化(たとえば、侵入検知ソフトウェアを、より多くの内部ネットワークやホストに配備する)が必要になる。

+ **事件ごとの時間** 各事件について、以下のようないくつかの方法により時間を測定することができる。

  - その事件に費やした労力の合計
  - 事件の開始から解決までに経過した時間
  - 事件処理プロセスの各ステージ(封じ込めや復旧など)の経過時間
  - 最初に報告を受けてから、インシデント対応チームが対応するまでにどれだけ時間がかかったか
  - 事件をマネジメント層(および必要な場合にはUS-CERTなどの外部組織)に報告するまでに、どれだけ時間がかかったか

+ **各事件の客観的な評価** 組織は、解決した事件への対応を分析して、対応がどれだけ有効だったかを判断することができる。以下に事件の客観的な評価を行う例を示す。

  - ログ、フォーム、レポート、および事件に関するそのほかのドキュメントをレビューし、確立されたインシデント対応ポリシーや手順に準拠しているかどうか確認する。
  - 事件がどの程度効果的に記録されているかを判断するために、事件のどの前兆や兆候が記録されているかを確認する。
  - 事件を検知する前にダメージを受けているか否かを判断する。
  - 事件の実際の原因が見つかったか否かを判断する。
  - 事件による金銭的な損害の見積額を計算する[77] 。
  - どのような対策をしていれば事件を予防できたかを確認する。

+ **各事件の主観的な評価** インシデント対応チームの各メンバーは、チームのほかのメンバーやチーム全体の評価に加えて、自分の業務を評価するよう要求される場合がある。もうひ

76 処理した事件の数といった基準は、複数の組織間で比較しても、一般には意味がない。というのは、各組織で主な用語を違う意味で定義しているためである。たとえば、ほとんどの組織では、「事件」という用語を独自のポリシーや業務の点から定義している。ポートスキャンの数といった、より具体的な基準も、組織間の比較はほとんど意味がない。たとえば、異なるセキュリティシステム(ネットワーク侵入検知センサーなど)が、特定の活動がポートスキャンであるか否かを判断する際に、同じ条件を使うということは考えられない。

77 事件のコストの見積に関する情報が、Incident Cost and Analysis Modeling Projects (ICAMP)のウェブサイト http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml にある。

とつの貴重な情報源は、攻撃されたリソースのオーナーである。事件が効果的に処理されたとオーナーが考えているのか、また結果が満足できるものであったかをオーナーに確認することも必要である。

これらの基準を使ってチームの成果を評価するほかに、組織のインシデント対応プログラムを定期的に監査するのも有効である。監査により、修正すべき問題点や不備が見つかる。インシデント対応の監査では、該当する規制、ポリシー、一般に広く受け入れられている慣行に照らし合わせて、最低でも以下の項目を評価すること。

+ インシデント対応のポリシー、計画、および手順
+ ツールとリソース
+ チームモデルと構成
+ 事件処理トレーニングと教育
+ 事件のドキュメントとレポート
+ このセクションの初めに述べた成功の評価基準

3.4.3. 証拠の保管

各組織は、事件の証拠をどれだけの期間保管するかについてのポリシーを確立すること。ほとんどの組織では、事件が終結してから数ヶ月または数年間、すべての証拠を保管するようにしている。ポリシーを策定する際には、以下の要因を考慮すること。

+ **告訴** アタッカーを告訴する可能性がある場合は、すべての法的行動が完了するまで、証拠を保管しておく必要がある。場合によっては、何年もかかることがある。さらに、現在重要でないように見える証拠も、将来重要になってくる可能性もある。たとえば、アタッカーが1度の攻撃で得たデータを使って、後からより大規模な攻撃を実行できる場合は、最初の攻撃の証拠が、2番目の攻撃がどのようにして行われたかを説明するための鍵となる場合がある。

+ **データの保管** ほとんどの組織にはデータ保管ポリシーがあり、ある種のデータをどれだけ長く保管するかが規定されている。たとえば、電子メールメッセージの最長保管期間を180日としている組織もある。1つのディスクイメージに何千もの電子メールが含まれている場合は、それがどうしても必要でない限り、180日を超えてイメージを保管したいとは思わないだろう。セクション3.4.2で説明したように、General Records Schedule (GRS) 24では、事件処理記録は、3年間保管することが規定されている。

+ **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(ハードディスク、侵入されたシステム)は、ディスクイメージを格納するのに使ったハードディスクやその他の機器同様に、個別ではほとんどの組織にとって高価なものではない。しかし、そのような装置を何十個も何年にもわって保管するとなると、かなりのコストになる可能性がある。また、保管したハードウェア(ハードディスクなど)や媒体(バックアップテープなど)を扱うことができる、動作可能なコンピュータも保管する必要がある。

3.5. 事件処理のチェックリスト

表3-8のチェックリストは、事件の最初の処理で実施する主なステップを示すものである。各項目は、事件の検知と分析だけに対応する。これらのステップを実施した後、事件処理担当者は、事件の種類ごとに作られたチェックリストを使用する。セクション4から8には、事件の5つの分類ご

との処理のチェックリストが含まれている。表3-9に、どの分類にも合致しない事件を処理するための、一般的なチェックリストを示す。

実際に実施するステップは、処理する事件の種類と各事件の性質により異なる場合がある点に注意すること。たとえば、処理担当者が、兆候の分析(表3-8のステップ1.1)により何が起きたかが正確にわかっている場合は、ステップ1.2や1.3を実行して活動を詳しく調査する必要はない。このチェックリストは、処理担当者が実施すべき主なステップを示している。これらのステップの順序は、厳密な順序を示すものではなく、必ずしもこの順番に沿って作業をする必要はない。

表3-8 最初の事件処理のチェックリスト

	活動	完了
	検知と分析	
1.	事件が起き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	調査を実施する(サーチエンジン、知識ベースなど)。	
1.4	事件が起きたと思われる場合には、すぐに調査の記録と証拠の収集を開始する。	
2.	セクション3.2.1で説明した分類を使用して、事件を分類する(サービス不能、悪意のコード、不正アクセス、不適切な使用、複合要素)	
3.	適切な事件分類チェックリストに従う。事件がどのカテゴリにも一致しない場合は、一般のチェックリストに従う。	

表3-9 分類できない事件を処理するための汎用チェックリスト

	活動	完了
	検知と分析	
1.	ビジネスインパクトに基づき、事件の処理に優先順位を付ける。	
1.1	どのリソースが影響をうけたかを確認し、将来どのリソースが影響を受けるかを予測する。	
1.2	事件の現在および将来的な技術的影響を見積もる。	
1.3	技術的な影響と影響を受けるリソースに基づき、優先順位マトリックスで適切なセル(1つまたは複数)を見つける。	
2.	適切な内部の人間または外部組織に事件について報告する。	
	封じ込め、根絶、復旧	
3.	証拠を取得、保全、確保、記録する。	
4.	事件を封じ込める。	
5.	事件を根絶する。	
5.1	悪用されたすべての脆弱性を見つけて修正する。	
5.2	悪意のコード、不適切なデータ、その他の構成要素を削除する。	

6.	事件から復旧する。	
6.1	影響を受けたシステムを運用可能な状態に戻す。	
6.2	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。	
6.3	必要なら、将来の関連する活動を見つけるため、追加の監視を実施する。	
事後活動		
7.	追跡レポートを作成する。	
8.	反省会を開催する。	

3.6. 推奨事項

このセクションで説明した、事件の処理に関する主な推奨事項を、以下に要約する。

- **事件処理で利用できそうなツールとリソースを入手する** さまざまなツールやリソースが利用できる状態になっていれば、チームはより効率的に事件を処理できる。例としては、連絡先一覧、暗号化ソフトウェア、ネットワーク図、バックアップ装置、コンピュータフォレンジックソフトウェア、ポートリスト、セキュリティパッチなどがある。

- **ネットワーク、システム、アプリケーションを十分に安全な状態に保つことで、事件の発生を予防する** 事件の予防は組織にとって有益なだけでなく、インシデント対応チームの作業負荷も減らすことができる。定期的にリスクを評価し、見つかったリスクを許容できるレベルまで軽減することが、事件を減らす上で有効である。ユーザ、ITスタッフ、マネジメント層のセキュリティポリシーや手順に対する自覚も非常に大切である。

- **いくつもの種類のセキュリティソフトウェアが生成した警報を使って、前兆や兆候を見つける** IDPS、ウイルス対策ソフトウェア、スパイウェア駆除ソフト、ファイル完全性チェックソフトウェアは、事件の兆候を見つける上で有用である。各ソフトウェアは、ほかのソフトウェアが検知できない事件を検知することもある。よって、複数の種類のコンピュータセキュリティソフトウェアを利用することを強くお勧めする。サードパーティーの監視サービスも有用である。

- **外部の者が事件を報告する仕組みを確立する** 外部の者が組織に事件を報告したい場合がある。たとえば、組織のユーザのひとりが彼らを攻撃していると思われるような場合である。組織は電話番号と電子メールアドレスを公開して、それを使って外部の者がそのような事件を報告できるようにすべきである。

- **全システムにログと監査の基準レベルを義務付け、重要なシステムではより高い基準レベルを義務付ける** オペレーティングシステム、サービス、アプリケーションのログは、事件の分析の際に役立つことが多い(監査が有効になっている場合は、なおさらである)。ログは、アタッカーがどのアカウントにアクセスしたか、どのような活動を行ったか、などの情報を提供する。

- **ネットワークとシステムのプロファイル** プロファイリングでは、期待される活動レベルの特性を測定することで、あるパターンの変更をより簡単に見つけることができる。プロファイリングプロセスを自動化すれば、期待される活動レベルからのずれを素早く検出して管理者に報告することができ、事件や運用上の問題の早期検出につながる。

- **ネットワーク、システム、アプリケーションの正常な動作を理解する** チームのメンバーが

正常な動作とはどのようなものなのかを理解すれば、異常な動作もより簡単に認識することができる。この知識を得るには、ログエントリーやセキュリティ警報をレビューするのが一番である。これにより処理担当者は、典型的なデータに慣れると同時に、異常なエントリーの調査を通じて、より詳しい知識を得ることができる。

+ **一元化されたログ取得とログ保管ポリシーの作成** 事件に関する情報は、さまざまな場所で記録される可能性がある。そこで、一元的なログサーバを設置して、組織内のログを生成する各装置が、ログエントリーのコピーをそのサーバに送るように設定する。こうすることで、関係するすべてのログエントリーが集まるため、事件処理担当者にとっては便利である。また、各ホストでログに変更が加えられても、すでに一元的なサーバに送られたデータには影響しない。以前のログエントリーが、前回の同様な活動や関連する活動を示す場合もあるため、ログ保管ポリシーは大切である。

+ **イベント相関処理の実施** 事件の兆候は、いくつものログで捕捉される可能性がある。複数のソースのイベントを相関させることは、事件に関して入手できるすべての情報を収集し、事件が発生したかどうかを検証する上で、とても重要である。ログを一元化することで、相関処理を簡単かつ素早く行うことができるようになる。

+ **すべてのホストの時刻を同期させておく** イベントを報告する機器の時刻の設定が合っていないと、イベント相関処理が困難になる。時刻にずれがあると、証拠の観点からも問題が起こる。

+ **情報の知識ベースの維持と利用** 処理担当者は、事件分析の際、情報を素早く参照する必要がある。一元化された知識ベースは、一貫した、保守可能な情報源となる。知識ベースには、よく使われるポート番号やマルウェア情報へのリンクなどの一般的な情報と、以前の事件の前兆や兆候などのデータを格納する。

+ **経験が少ないスタッフのための診断マトリックスの作成** ヘルプデスクのスタッフ、システム管理者、インシデント対応チームの新しいメンバーは、どの種類の事件が起きているかを判断する際、助けが必要である。事件の分類と各分類に関連する症状を一覧にした診断マトリックスがあると、どの種類の事件が起きているか、どのように事件を確認するかに関する手引きとなる。

+ **事件が起きた疑いがある場合には、すぐに全情報の記録を開始する** 事件が検出された時点から、最終的に解決された時点までのすべてのステップを文書化し、タイムスタンプを記録する。こういった情報は、告訴することになった場合に、法廷で証拠として使用することができる。実行したステップを記録することで、より効率的で体系的な、誤りのない問題処理が可能になる。

+ **事件データの保護** 事件データには、脆弱性、セキュリティ違反、不適切な活動を行った可能性があるユーザ等の機密情報が含まれていることが多い。事件処理チームは、事件データへのアクセスが、論理的かつ物理的に適切に制限されるようにするべきである。

+ **影響のあるリソースの重要性や事件の技術的な影響に基づき、ビジネスインパクトごとに事件に優先順位を付ける** リソースに制限があるという理由で、起きた順に事件を処理することは、やめるべきである。代わりに、事件の現在および将来のビジネスインパクトを基に、チームがどれだけ迅速に事件に対応しなくてはならないか、どのような行動をとるべきかについて、文書化したガイドラインを作成する。このガイドラインがあれば、事件処理担当者の時間が節約でき、行った処置について、マネジメント層とシステムオーナーに対する説明ができる。各組織は、チームが指定された時間内に事件に対応しない場合に備え、エスカレーションプロセスを確立しておく。

+ **組織のインシデント対応ポリシーの中に、事件報告に関する項目を盛り込む** どの事件をいつだれに報告しなくてはならないかについて、明記する。一般に通知すべき関係者としては、最高情報責任者(CIO)、情報セキュリティ部門長、各地区の情報セキュリティ管理者、組織内のほかのインシデント対応チーム、システムオーナーがある。

+ **事件を封じ込めるための戦略と手順の確立** ビジネスへのインパクトを制限するために、事件を素早く効果的に封じ込めることは重要である。組織は、事件を封じ込める際の許容可能なリスクを定義し、相応の戦略と手順を作成しておくこと。封じ込めの戦略は、事件の種類によってさまざまである。

+ **証拠収集と処理のための、確立された手順に従うこと** あらゆる証拠を保全する方法について、明確に文書化すること。証拠は、いつでも説明できるようになっていなくてはならない。法務部のスタッフや法執行機関と会って事件処理について話し合い、その内容に基づいて手順を作成する。

+ **揮発性データを証拠としてシステムから取得する** この作業にはネットワーク接続の一覧、プロセス、ログインセッション、オープンされたファイル、ネットワークインタフェース設定、メモリーの内容が含まれる。信頼できる媒体から注意して選んだコマンドを実行することで、システムの証拠を破壊することなく、必要な情報を収集できる。

+ **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って、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、中身の入っていないライトプロテクトされたメディアか、ライトワンスメディアに作成する。調査および証拠としての目的からは、このプロセスのほうが、ファイルシステムのバックアップよりも優れている。イメージ取得が望ましいほかの理由としては、オリジナルのシステム上で分析を行うよりも、イメージ上で分析したほうがより安全なことが挙げられる。分析により、オリジナルを誤って変えてしまうことがあるからである。

+ **大きな事件の後には反省会を開催する** 反省会は、セキュリティ対策と事件処理プロセス自体を改善する上で、非常に有用である。

4. サービス不能事件の処理

4.1. 事件の定義と例

「サービス不能」(DoS)は、中央処理装置(CPU)、メモリー、帯域、ディスク領域などのリソースを枯渇させることで、ネットワーク、システム、アプリケーションの正規の使用を妨害または阻害する活動である。DoS攻撃の例としては、次のようなものがある。

+ 異常に大量のトラフィックを生成し、利用できるネットワーク帯域をすべて使い切る。
+ 異常なTCP/IPパケットをサーバに送り、オペレーティングシステムをクラッシュさせる。
+ アプリケーションに不正な要求を送り、クラッシュさせる。
+ プロセッサを大量に使用する要求を送り、サーバの処理リソースを完全に使い切る(たとえば、サーバが各応答を暗号化しなくてはならないような要求)[78]
+ サーバに対して多数のログインセッションを確立し、ほかのユーザがログインセッションを開始できないようにする。
+ ワイヤレスネットワークが使用する周波にて放送を行うことで、そのネットワークを使用できなくする。
+ 大きなファイルを多数作成し、利用可能なすべてのディスク領域を消費する。

ほとんどの組織では、広い帯域のネットワークを使用しているため、単一の攻撃マシンではネットワークのDoSにならない。しかし現在では、アタッカーが「分散型サービス不能」(DDoS)攻撃を行うようになった。[79]これは、多数のコンピュータ間の攻撃を連係させるものである 。アタッカーが十分な数のホストを使用した場合、生成されるネットワークトラフィックによって、ターゲットとなるホストのみならず、あらゆる組織の利用可能帯域を使い果たすことが可能になる。DDoS攻撃は次第に大きな脅威になってきており、攻撃によってコンピュータやネットワークサービスが利用できなくなった場合、大きな混乱と経済的損失がもたらされる。いかなる組織もDDoS攻撃から完全に自身を守ることはできないが、セクション4.2.2の手引きを実施すれば、このような攻撃の脅威を軽減することはできる。

DDoS攻撃には、一般に、「エージェント」と「ハンドラ」の2種類の要素が使われる。「エージェント」は、侵入したホスト上で動作し、実際の攻撃を実行する。「ハンドラ」は、エージェントを制御するプログラムで、いつ、何を、どうやって攻撃するかを指示する 。[80] エージェントは、次第にBotと呼ばれるようになり、Botを実行するホストのセットは、botnetと呼ばれるようになった。ハンドラプログラムは、場合によっては使用されないこともある。そのようなケースでは、アタッカーがIRCチャネルなどの別の手段を用いてBotと通信するか、Botにあらかじめ攻撃命令を仕込んでおく。アタッカーは、DDoS攻撃を実行する際に、何千ものBotから成る大規模のBotnetを使用することが多い。図4-1は、DDoS攻撃の3つのステップを示している。まず、アタッカーはホストに侵入し、Bot(エージェント)を設置する。次にアタッカーはハンドラを使用して、何を、

78 この方法で悪用されるサービスの例としては、DNSSEC (DNS Security Extension)やsoBGP (Secure Origin Border Gateway Protocol)がある。

79 分散型サービス不能攻撃に関する詳細は、Dave Dittrich's Web page on DDoS attacks and tools (http://staff.washington.edu/dittrich/misc/ddos)を参照するか、Los Angelesのカリフォルニア大学のJelena Mirkovic, Janice Martin, Peter Reiherの著書「A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms (http://lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf)」を読むことをお勧めする。

80 エージェントは「スレーブ」または「デーモン」と呼ばれ、ハンドラは「マスター」と呼ばれることもある。

いつどうやって攻撃するかをBotに指示する。最後にBotは指示に従ってターゲットとなる被害者を攻撃する。

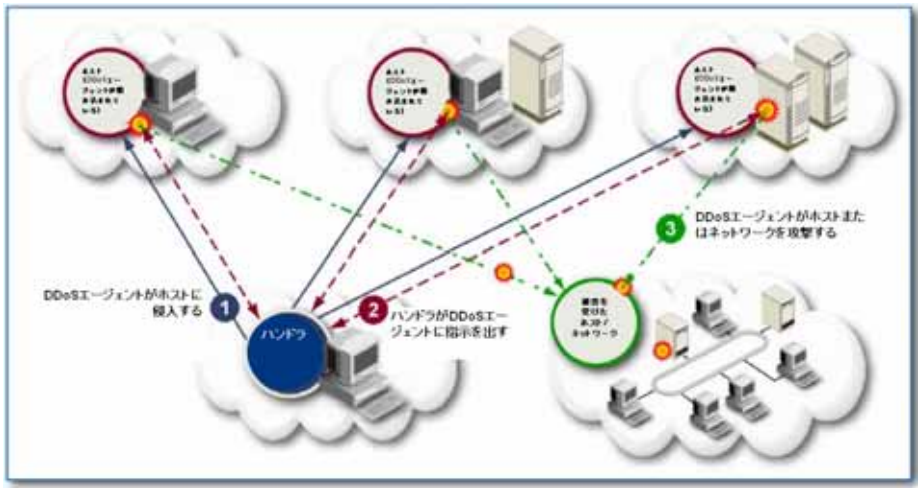

図4-1 分散型のサービス不能

DDoS攻撃には、リフレクタ攻撃、アンプ攻撃、floodの3つの種類がある。以下に、これらのDoS攻撃に関する詳細を示す。

4.1.1. リフレクタ攻撃

「リフレクタ攻撃」では、あるホストが、偽装された送信元アドレスを使って多数の要求を中間ホストのサービスに送信する[81](ここで使用されるサービスは、送信元アドレスがうまく偽装できるUDP (User Datagram Protocol)ベースのサービスであることが多い。アタッカーが偽装された送信元アドレスをよく使うのは、実際の攻撃元を隠すためである)。この中間ホストは各要求に対して応答を生成し、偽装されたアドレスに対して応答を送る。この中間ホストは知らずに攻撃を行うことから、「リフレクタ」と呼ばれる。リフレクタアタックでは、偽装されたアドレスを持つホスト、リフレクタ自身、またはその両方でDoSが行われる。一般に利用されるリフレクタサービスには、echo (ポート7)、chargen (ポート9)、DNS (ポート53)、SNMP (Simple Network Management Protocol) (ポート161)、ISAKMP (Internet Security Association and Key Management Protocol) (ポート500)などがある。

場合によっては、2つのリフレクタを使って自己完結型のDoSが構成される場合もある。アタッカーは、特定のリフレクタに対する要求を、ほかのリフレクタに割り当てられたアドレスを送信元と仕立てて行うことができる。これにより、最初のリフレクタが応答を生成すると、この応答は第2のリフレクタに送られる。リフレクタの組み合わせを適当に選ぶと、2つのリフレクタ間でループが起きる。最も初期のリフレクタ攻撃は、echoとchargenサービスのループで構成されていたが、現在の攻撃は、リフレクタサービスのさまざまな組み合わせで構成される。ほとんどのリフレクタ攻撃は、ネットワーク型およびホスト型のファイアウォールのルールセットを使って、宛先ポートと送信元ポートの疑わしい組み合わせを拒否するように設定することで防ぐことができる。

81 詳細は、Vern Paxsonによる『An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks』(http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html) を参照。

図4-2の左上の図に、通常のDNSの問い合わせと応答のネットワークトラフィックパターンを示す。DNSクライアントは、UDPポート1792からサーバのDNSポート53に対して問い合わせを送る。DNSサーバは、UDPパケットをクライアントのUDPポート1792に送ることで、問い合わせに応答する。右側の図は、左上の図と同じDNSサーバを使ったリフレクタ攻撃を示したものである[82]。はじめに、アタッカーがDNSサーバにパケットを送信する。このパケットは、アタッカーによって偽装された送信元アドレス(この例ではj.k.l.m)とポート7(通常はリフレクタサービスであるechoに割り当てられているポート)を使用するように設定されている。DNSサーバがパケットを受信すると、応答を生成して、偽装されたアドレスj.k.l.m(被害者)に送信する。ここで、被害者がechoサービスを提供している場合、受信したデータに対する反射パケットが生成され、DNSサーバに送り返される。DNSサーバが犠牲者から送られたパケットに応答することにより、DNSサーバと被害者の間にループができることになる。

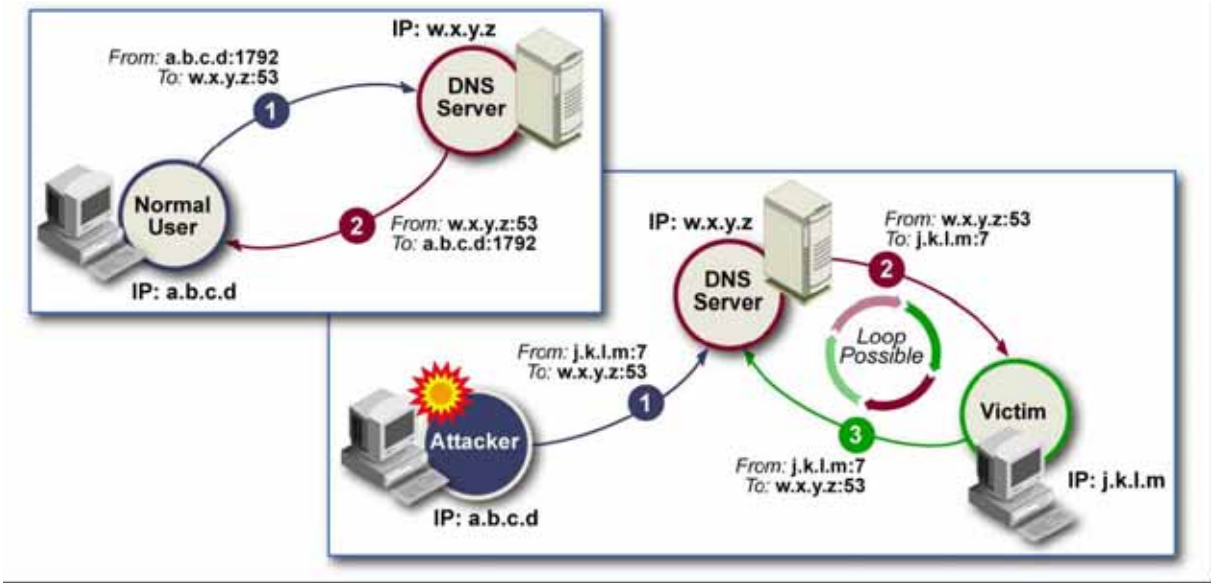

図4-2 DNSサーバを使ったリフレクタ攻撃

4.1.2. アンプ(amplifier)攻撃

リフレクタ攻撃と同様に、アンプ攻撃も偽装された送信元アドレスを使用して中間ホストに要求を送る。ただし、アンプ攻撃では1台の中間ホストを使うのではない。その最終目標は、複数の中間ホストから成るネットワークを利用することである。そのためには、予想されるブロードキャストアドレスにICMPまたはUDPの要求を送り、多数のホストがブロードキャストを受信してそれに応答するのを期待する[83]。アタッカーの要求は偽装した送信元アドレスを使用しているため、応答はすべて偽装されたアドレスに送られ、そのホストまたはそのホストのネットワークにDoS攻撃が行われる。ほとんどの環境では、境界ルーターがディレクティッドブロードキャスト(directed broadcast)を転送しないように設定することで、アンプ攻撃をブロックしているが、まだ許可しているものもある。

DNS recursion攻撃は、アンプ攻撃の一例である。DNSサーバが再帰を許す場合、サーバは、権限

82 このドキュメントでは、アタッカーによる悪意のある活動を、図中の星形のマークで示す。
83 アンプ攻撃でよく使用される要求はICMPメッセージであるが、前述のリフレクタサービスのようにUDPも使用される。一方、TCPは使用できない。ブロードキャストはコネクションレスであるが、TCPはコネクション指向のプロトコルであるため、TCPにはブロードキャストという概念が存在しないのである。

を持たないドメイン名に対するリクエストを処理し、委譲情報(delegation information)を要求側に返してしまう。非再帰的(non-recursive)なDNSサーバは、ローカルに持っている情報のみを返す。DNS recursionでは、アタッカーが、数何千もの偽装要求を、再帰を許すDNSサーバに対して行う。これらの要求はサーバによって処理され、結果は偽装されたIP(被害者のアドレス)に送信される。このような攻撃が行われた場合、偽装されたIPアドレスにギガバイトのDNS応答が転送され、被害者のホストが圧倒されてしまう。[84]

4.1.3. Flood攻撃

Flood攻撃は、多くの不完全な接続要求を開始することによって、リソースを利用できなくするDDoS攻撃である。この種の攻撃は、システムの容量を逼迫し、新しい接続を確立できないようにする。Flood攻撃は、さまざまな手法を使って実施される。Flood攻撃がDdoS攻撃につながることも多い。このような例としては、ピアツーピア攻撃があげられる。ピアツーピア攻撃では、アタッカーが、特定のピアツーピアネットワークからファイル共有ハブを取り外して、トラフィックを被害者のウェブサイトにリダイレクトするように設定する。その後何千台ものコンピュータが、偽装されたファイル共有ハブ(コンピュータからはファイル共有ハブに見えるもの)に接続しようとすると、被害者のウェブサーバのリソースは食いつぶされ、接続は失敗に終わる。

Flood攻撃の別の例としては、synflood 攻撃がある。synfloodは、アタッカーが短時間のうちに多数のTCPコネクションを開始し(SYNパケットを送る)、各コネクションを完全に確立するのに必要なTCPのスリーウェイハンドシェイクを完了しない場合に発生する。かつては、多くのオペレーティングシステムにおいて、サービスごとに同時に保留状態にすることができるコネクションの数がごく少数に限られていた。アタッカーが特定のサービスポートに対して100個のTCPコネクションを開始し、いずれのコネクションも完了しなかった場合、古いコネクションがタイムアウトし始めるまで(通常1コネクションにつき約1分間)は、ほかのコネクションを受け付けるためのリソースがOSには残っていない。これは、ターゲットとなるサービスに対して一時的なDoSとなる。アタッカーがSYNパケットを送信し続ければ、DoSは継続される。現在のオペレーティングシステムやファイアウォールの多くは、synfloodに対する防御が可能なため、synfloodはあまり大きな脅威ではなくなっている。それでも、アタッカーが短時間のうちに何千というTCPコネクションを開始すると、synfloodが起こる可能性がある。DDoSツールによりこの種の攻撃が可能になっている。

図4-3に、正常なTCPコネクションと意図的なsynfloodの違いを示す。図の左側は、TCPのスリーウェイハンドシェイクを示し、SYN、SYN/ACK、ACKパケットで構成される。ホストは、ACKを受信するまではコネクションが完全に確立されたとはみなさない。図の右側は、synfloodを示す。アタッカーは、サーバとの間でいくつものTCPスリーウェイハンドシェイクを開始するが、コネクションは確立されない。この例ではアタッカーがコネクション要求の送信元を偽装しているため、サーバは偽装されたホストにパケットを送信し、ハンドシェイクを試みる。ところが存在しないホストのIPアドレスが送信元となっているために、サーバはハンドシェイクに対する応答を受信することができず、効果的にDoSが起きることになる。

84 US-CERT発行の"The Continuing Denial of Service Threat Posed by DNS Recursion"では、DNS recursion攻撃の概要を詳細に記述し、これらの攻撃からシステムを保護するための方法を紹介している。このドキュメントは、http://www.us-cert.gov/reading_room/DNS-recursion033006.pdfから入手できる。DNSセキュリティに関する詳細は、NIST SP 800-81『Secure Domain Name System (DNS) Deployment Guide』(http://csrc.nist.gov/publications/PubsSPs.html)に記載されている。

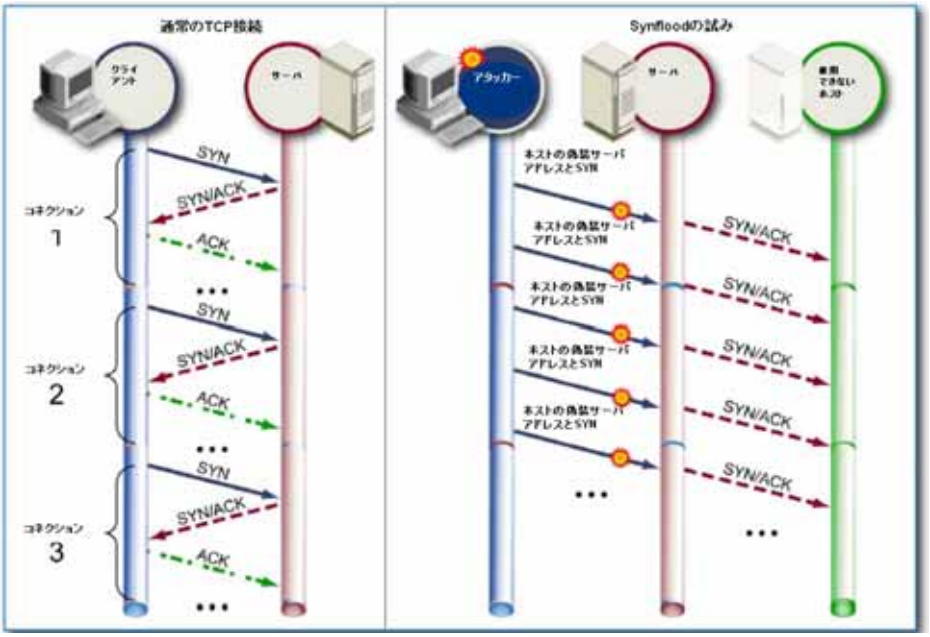

図4-3 synflood攻撃

4.2. 準備

このセクションでは、DoS事件の処理に備え、DoS事件を予防するための手引きを示す。

4.2.1. 事件処理の準備

セクション3.1.1と3.2.3で説明した一般的な手引きに加え、DoS事件の処理に備える際には以下に示すいくつかの内容を実行する。

+ 組織のISPや二次プロバイダと話し、ネットワーク型のDoS攻撃の処理において、どのような支援が得られるのかを確認する。これには、フィルタリングや、トラフィックの制限(特定の送信元IPアドレスのブロックや、着信ICMPトラフィックに最大限度を設けるなど)、DoSトラフィックのログの提供、攻撃元の逆探知などが含まれる[85]。ISPや二次プロバイダの支援を要請する際に従うべき手順については、明確に定義すること。これには、24時間365日の一次および二次窓口、複数の連絡チャネル、ISPが組織からの要求を認証する方法などが含まれる。

+ 多数の組織に影響を与える広範なDoS攻撃に対し、(自組織や他組織が)連係対応に参加することが可能かどうかを調査することも検討する。たとえば、中央のインシデント対応団体(たとえば、US-CERT、CERT®/CCなど)と攻撃に関する情報をすみやかに交換すれば、その団体が連係対応を計画し、影響を受けた組織がそれを実施するといったことも可能となる。これにより組織は、事件をより迅速かつ効果的に封じ込めることができる。

+ IDPSを配備して、DoSトラフィックを検知するように設定する。たとえば、ネットワーク侵入検知ソフトウェアは、一般にさまざまな種類のDoS攻撃用のシグネチャを持っている。

85 多くのISPでは、裁判所の命令がないかぎり、攻撃を受けた組織に対して攻撃のログを提供することはない。

ネットワーク行動分析ソフトウェアは、Dos攻撃による異常なトラフィックフローを特定することができる。ワイヤレスIDPSは、ワイヤレス型のDos攻撃を検知できる。攻撃によってはISPのリソースが逼迫し、組織の境界ルーターにすら届かない可能性もあるため、侵入検知についてはISPと話し合うべきである。ISPによってはトラフィック監視を実行し、ISPのネットワーク上での主要なDoS攻撃の発生を検知できる場合がある。

+ ネットワーク帯域使用率と重要なホストのリソース使用率の基準を確立するために、継続的にリソースの監視を行う。また、基準からの大きなずれがあれば、ログに記録したり警報を発したりするようにする。

+ さまざまなISP間とさまざまな物理的位置の間での遅延時間の統計を提供しているウェブサイトを探す。これはよく「インターネットヘルスモニター(*Internet health monitoring*)」と呼ばれる[86]。ネットワーク型のDoSが起きたら、このウェブサイトを使って、同様の攻撃がほかの組織でも起きていないかを調べることができる(たとえば、ワームによって地域的な分断が起きてないかなど)。

+ ネットワークの管理者と会って、ネットワーク型のDoSやDDoS攻撃の分析と封じ込めを行う際に、どのような支援が得られるかを話し合っておく。たとえば、管理者は攻撃の最中にログの取得を調整できるかもしれない(たとえば、特定の種類の活動についてより詳しい情報を収集するなど)。管理者はまた、ログのコピーの取得など、証拠の保護でも役立ってくれる可能性がある。

+ 事件の最中に組織のインターネット接続や内部のネットワーク接続が失われた場合に備え、DoS攻撃の処理で役立ちそうなコンピュータベースの情報のローカルなコピー(電子的なコピーや紙のコピー)を保管する。

4.2.2. 事件の予防

セクション3.1.2には、事件の予防に関するガイドラインやリソースへのポインターが含まれている。以下の項目は、DoS事件を予防するための、その他の助言である。

+ ネットワーク境界で、明示的に許可されていないすべての送受信トラフィックを拒否するように設定する[87]。これには、次のものが含まれる。

  - echoやchargenなどのサービスの利用をブロックする。これらは、もはや正当な目的を持たず、DoS攻撃でよく利用されるサービスとなっている。

  – 出口フィルタと入口フィルタを実行し、明らかに偽装されたパケットをブロックする[88]。

  – 割り当てられていないIPアドレス範囲(bogonリストと呼ばれる)からのトラフィックをブロックする[89]。IPアドレスを偽装する攻撃ツールは、インターネットでの利用がまだ割り当てられていないアドレスを使用することがある。

---

86 インターネットヘルスモニターのウェブサイトの例としては、Internet Health Report (http://www.internetpulse.net)がある。

87 DDos攻撃のブロックに関する優れた情報源が、『Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks』(入手先はhttp://www.cisco.com/warp/public/707/newsflash.html) である。

88 「入口フィルタ」とは、不正なIPアドレスからの受信パケット(予約された送信元アドレスを持つパケットなど)をブロックする処理である。これに対し「出口フィルタ」は、不正なIPアドレスからの送信パケット(たとえば、内部ネットワークの送信元アドレスを持ったパケットが、誤って組織から出てインターネットに入り込んだ場合)をブロックする。詳細は、RFC (Request for Comment) 2267『Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing』(http://www.ietf.org/rfc/rfc2267.txt)を参照。

89 http://www.cymru.com/Documents/bogon-list.html

  - トラフィックを正しくブロックするために、ファイアウォールのルールとルーターのアクセスコントロールリストを記述して順に並べる[90]。
  - ディレクティッドブロードキャストを転送しないよう境界ルーターを設定する。
  - 送受信するICMPトラフィックを、必要な種類とコードだけに制限する。
  - よく利用されるIRC、ピアツーピアサービス、インスタントメッセージのポートに対する、外向きの接続をブロックする(これらのサービスの利用が許可されていない場合)。

+ ICMPなどの特定のプロトコルに対して帯域制限を実施し、帯域全体の指定された割合しか消費しないようにする。帯域制限は、組織のネットワーク境界(たとえば境界ルーター、ファイアウォールなど)および組織のISPで実施可能である。
+ インターネットにアクセスできるホストでは、不要なサービスをすべて無効にし、DoS攻撃で使われる可能性があるサービスの利用を制限する(たとえば、DNSサーバを、再帰を許可しないように設定する)。
+ 主要な機能に冗長性を持たせる(複数のISP、ファイアウォール、ウェブサーバ)
+ ネットワークとシステムを、最高の能力に近いところで動作させない。さもないと、小規模なDoS攻撃でも残っているリソースが食いつぶされることになる。

4.3. 検知と分析

DoS攻撃は、以下の表に示すような、特定の前兆や兆候を通じて検知することができる。表4-1の「サービス不能の前兆」では、考えられるDoS攻撃の前兆の一覧を挙げ、そのような活動がなぜ行われるかを説明し、関連する事件の発生を予防するために推奨される対応を説明する。表4-2「サービス不能の兆候」には、ネットワーク型のDoS、オペレーティングシステムに対するDoS、アプリケーションに対するDoSなどの悪意のある活動と、それらの活動の兆候の一覧を示す。組織は、これらの表を手軽にカスタマイズして、環境特有の前兆や兆候を追加してかまわない。それがより効率的で効果的な事件処理プロセスを促進する。

表4-1 サービス不能の前兆

前兆	対応
DoS攻撃の前には、どの攻撃が有効かを判断するための、偵察活動が行われることが多い。これは通常、実際の攻撃で使用されるトラフィックの少量のものである。	DoS攻撃の準備と思われる異常な活動を検知した場合は、セキュリティ設定を素早く変更することで攻撃をブロックできる可能性がある。たとえば、ファイアウォールのルールセットを変更して、特定のプロトコルが使われるのをブロックしたり、脆弱なホストを保護するなどが考えられる。
新しくリリースされるDoSツールが、組織に対して重大な脅威をもたらす可能性がある。	新しいツールを調査し、可能ならセキュリティコントロールを変更して、そのツールが組織に対しては有効でなくなるようにする。

90 たとえば、最初の規則で公開DNSサーバに問い合わせが到達するのを許可し、DNSサーバが問い合わせに対してUDPポート53を使って応答するのを許可する。2番目の規則は、UDPポート7のechoサービスの利用を禁止する。頭のよいアタッカーは、送信元ポートが53、宛先ポートが7のUDPパケットを送ることで、DNSサーバをリフレクタとして使用するかもしれない。ルールセットは順番に評価されるため、このトラフィックは最初の規則に一致し、許可されることになる。

表4-2 サービス不能の兆候

悪意のある活動	予想される兆候
特定のホストに対するネットワーク型のDoS	・システムが利用できないというユーザからの報告を受ける ・不明なコネクションロス ・ネットワーク侵入検知の警報 ・ホストの侵入検知の警報(ホストが過負荷になるまでの間) ・ネットワーク帯域使用率の増加 ・単一のホストに対する大量のコネクション ・非対称のネットワークトラフィックパターン(ホストには大量のトラフィックが送られるものの、ホストからはほとんどトラフィックが出てこない) ・ファイアウォールとルーターのログエントリーに異常が見られる ・送信元アドレスが異常なパケット
ネットワークに対するネットワーク型のDoS	・システムとネットワークが利用できないというユーザからの報告を受ける ・不明なコネクションロス ・ネットワーク侵入検知の警報 ・ネットワーク帯域使用率の増加 ・非対称のネットワークトラフィックパターン(ネットワークに入っていくトラフィックは大量だが、ほとんどネットワークからトラフィックが出てこない ・ファイアウォールとルーターのログエントリーに異常が見られる ・送信元アドレスが異常なパケット ・存在しない宛先アドレスを持ったパケット
特定のホストのオペレーティングシステムに対するDoS	・システムとアプリケーションが利用できないというユーザからの報告を受ける ・ネットワークとホストの侵入検知の警報 ・オペレーティングシステムのログエントリーに異常が見られる ・送信元アドレスが異常なパケット
特定のホスト上のアプリケーションに対するDoS	・アプリケーションが利用できないというユーザからの報告を受ける ・ネットワークとホストの侵入検知の警報 ・アプリケーションのログエントリーに異常が見られる ・送信元アドレスが異常なパケット

これらの表は事件の分析の際に役立つかもしれないが、重要な要素である悪意のない活動に関係する兆候が欠けている。悪意のない事象と悪意のある事象は似た症状を示すことがあり、このことが、事件が発生したかどうかを(分析者が)すぐに判断するのを難しくしている。兆候の表を拡張して悪意のない活動を追加することで、行われている活動に悪意がないか悪意があるかを区別しやすくなる。たとえば、インターネット接続が失われた場合、症状の多く(すべてではないが)がネ

ットワークベースのDDoSと似たものになる可能性がある。悪意のない活動情報を表に追加する際には、悪意のない活動がどのように悪意のある活動と区別されるかも合わせて記述すること。

DoS攻撃は、事件分析において、以下に示すようなさらなる困難をもたらす。

+ DoS攻撃では、コネクションレスプロトコル(UDPやICMP)を使用するか、コネクション型のプロトコルを、完全にコネクションを確立しない状態で使用する(TCP SYNパケットを送信して、synflood攻撃を起こすなど)。そのため、アタッカーは比較的容易に送信元のIPアドレスを偽装でき、攻撃元の追跡を困難にすることができる。ISPなら活動の追跡を支援できるかもしれないが、自分でログをレビューして、関係していると思われる以前の偵察活動を探した方が効果的であることが多い。偵察活動では、アタッカーが偵察の結果を受信したいと考えることから、偽装したアドレスを使用しないことが多く、アタッカーの居場所が示される可能性がある。

+ DDoS攻撃では、1台(あるいはまったくハンドラを使用しない)のハンドラで制御される数千のワークステーションを使用することが多い。通常、これらのワークステーションには、Botが設置されている。これは「ゾンビ」と呼ばれるもので、コントローラによってアクティブ化され、他のシステムへの攻撃を開始する。被害を受けるサイトにはハンドラのIPはわからず、仮にわかったとしても、単にアタッカーが侵入した別のホストである可能性が高い。

+ ネットワーク型のDos攻撃は、IDPSセンサーで高い精度で検知するのは難しい。たとえば、synfloodの警報は、ネットワークIDPS製品上で最も一般的に発生する誤検知の一つである。アタッカーが素早いSYNスキャンを実施している間に、各ポートにたった1つの要求が送られただけでも、多くのIDPS製品がそれをsynfloodとして報告してしまう。また、サーバがクラッシュした場合、そのサーバに再接続しようとするホストはSYNパケットを送り続けることがある。場合によっては、正規のコネクションが短時間に多数確立されたことが原因で(たとえばウェブページの多数の要素を取得するなど)、synflood警報が作動することもある。

+ システムが停止した場合、DoS攻撃が原因だと誰も気づかないことがある。たとえば、あるWebサーバが、オペレーティングシステムが不安定なためにたびたびクラッシュし、機能の復旧にはリブートが必要だとする。仮にアタッカーが特別に作成したパケットをウェブサーバに送り、それが原因でサーバがクラッシュしたとしても、システム管理者がオペレーティングシステムが不安定なためにクラッシュしたと思いこみ、攻撃されたことに気づかない可能性がある。

4.4. 封じ込め、根絶、復旧

セクション3.3で説明した一般的な手引きに加え、このセクションでは、DoS事件の封じ込めと証拠の収集・処理を行うための、具体的な推奨事項を説明する。

4.4.1. 封じ込め戦略の選択

DoS事件の封じ込めは、通常はDoSを停止することである。これは簡単なこともあるが、多くの場合そうではない。まず最初に思いつくのが、活動元からのすべてのトラフィックをブロックすることである。しかし前述のように、この種の攻撃では送信元アドレスが偽装されているか、数千の侵入されたホストが使用されることが多く、どちらにしても、送信元IPアドレスに基づく効果的なフィルタリングを実施するのは難しいか不可能である。仮に使われている送信元アドレスをブロックできても、アタッカーは単にほかのIPアドレスに移ればいいだけである。DoSを封じ込めるための、考えられるその他の対策には以下のものがある。

+ **悪用されている脆弱性または弱点を修正する** たとえば、パケットフィルタがUDPポート7(echo)を使用したパケットをブロックしていないことと、公的にアクセス可能なホストで誤ってechoが動作していることが原因で攻撃が起きた場合、フィルタルールを変更してechoポート宛のパケットブロックし、ホストの構成を変更してechoサービスを提供しないようにする。もしパッチが適用されていないオペレーティングシステムが、特別に作成されたパケットによるDoSを受けやすい場合は、オペレーティングシステムにパッチを適用する。ホストを強化する際は、DoSを止めるためにホストを一時的にネットワークから切り離さなくてはならない場合もある。

+ **攻撃の特徴を踏まえたフィルタリングの実施** たとえば、攻撃がICMP echo要求を使用している場合は、境界のセキュリティを変更して、この要求がネットワークに入ってくるのを一時的にブロックすることができる。しかしながら、この方法は常に現実的というわけではない。仮にアタッカーがSYNフラッドをウェブサーバのHTTP (HyperText Transfer Protocol)ポートに送っていて、事件処理担当者がそのポート宛のSYNパケットをブロックするようにフィルタを設定すると、それ自体がユーザに対するDoSとなってしまう。さらに、DoS攻撃ツールは非常に多くの方法を取ることが可能であるため、ある攻撃がブロックされても、アタッカーは簡単に別の方法に切り替えることができる。もうひとつの戦略が帯域制限である。特定のプロトコルを使ったパケットや特定のホスト宛のパケットを、毎秒一定数しか許可しないようにする。フィルタリング手法は事件の封じ込めには有効なこともあるが、さらなる問題を招く場合がある。たとえば、新しい規則をルーターやファイアウォールに追加すると、装置の性能に大きな悪影響を与え、ネットワークのスローダウンや、DoSが起きることすらある。組織は、フィルタリングをどこで実施すべきか(境界ルーターやファイアウォールなど)を慎重に検討し、長期間にわたる攻撃へのフィルタリングを容易にするために、ネットワーク機器をアップグレードすることも覚悟しておくべきである。

+ **ISPにフィルタリングの実施を依頼する** 外部ホストからのネットワーク型のDoSにより、組織のインターネットルーターがパケットであふれてしまうことがある。この活動をブロックするためには、ISPに依頼してフィルタリングを実施してもらわなければならない。

+ **ターゲットの再配置** 特定のホストがターゲットになっていて、ほかの封じ込め戦略の効果がない場合、そのホストをほかのIPアドレスに移動するのもよい。アタッカーは移動したターゲットを見つけて再度攻撃してくる可能性もあるため、これは、「不知によるセキュリティ(security through obscurity)」と考えられる。ターゲットとなったサービスを、同じ脆弱性を持たないほかのホストに移動することもできる。

+ **アタッカーを攻撃する** たとえば、攻撃しているDDoSエージェントをリモートから停止させるためのプログラムを使用したり、ネットワークやサーバの設定を変更して、送信元に攻撃トラフィックを跳ね返すといったことも可能である。しかし、送信元アドレスが偽装されている場合や、送信元アドレスが正規のものであって、かつ共有されている場合(たとえばプロキシ型ファイアウォールなど)、この手法は関係のない人まで攻撃してしまう。事件処理担当者は、この手の「ハックバック」手法を使用すべきでない。

セクション3で述べたように、推奨される行動があらかじめ決まっていれば、DoS事件封じ込めの意思決定プロセスが簡単になる。そのためには、考えられる対策をいつ実施するかに関して、マトリックスやその他の文書化されたガイドラインを作成する。封じ込め戦略にはいくつかの対策を順に記述する。たとえば次のようになる。

1. 攻撃の特徴を踏まえたフィルタリングの実施
2. 悪用されている脆弱性または弱点の修正

3. ISPにフィルタリングの実施を依頼する

4. ターゲットの再配置

4.4.2. 証拠の収集と処理

DoS攻撃の証拠収集は、以下のさまざまな理由から、困難で時間がかかることが多い。

+ **観測されるトラフィックからの攻撃元の特定** 送信元IPアドレスは偽装されていることが多い。DDoS攻撃では数千のホストが使用され、そのそれぞれが複数の偽装されたアドレスを使用している可能性がある。仮にホストが実際のアドレスを使用しているとしても、これらはあくまで攻撃のトラフィックを生成している中間的な箱であり、攻撃全体を指揮しているシステムではない。

+ **複数のISPにまたがった攻撃の逆探知** 事件処理担当者は、攻撃元を逆探知するために(技術的かつ論理的に可能だということが前提ではあるが)、複数のISPに順に連絡をとらなければならない場合がある。ISPによっては、召喚状なしには協力できない場合があり、召喚状の取得には時間がかかる。また、すでに終わった攻撃を逆探知することは、現在進行中の攻撃を逆探知することよりも、はるかに難しい。各ISPからの協力を取り付けるのに要する時間を考えると、逆探知できるようになるまでには攻撃が止まっている可能性が高い。

+ **大量のログエントリーをレビューする** ほとんどのDoS攻撃はリソースを逼迫させることで起きるため、その結果として異常に大量のログエントリーが生成される可能性がある。ログ取得標準や実施によっては、ログは上書きされ、証拠が残らない可能性がある。また、すべてのログエントリーをレビューし、関係する情報を抽出するのは、非常に時間がかかる。

4.5. サービス不能事件の処理のためのチェックリスト

表4-3のチェックリストは、DoS事件の処理で実行する主なステップを示したものである。このチェックリストは、表3-8の最初の事件処理チェックリストの続きである。各ステップの正確な順番は、各事件の性質や、組織が進行中のDoS攻撃を止めるために選んだ戦略によって変わってくる点に注意すること。

表4-3 サービス不能攻撃による事件の処理のチェックリスト

	活動	完了
	検知と分析	
1.	ビジネスインパクトに基づき、事件の処理に優先順位を付ける。	
1.1	どのリソースが影響をうけたかを確認し、将来どのリソースが影響を受けるかを予測する。	
1.2	事件の現在および将来的な技術的影響を見積もる。	
1.3	技術的な影響と影響を受けるリソースに基づき、優先順位マトリックスで適切なセル(1つまたは複数)を見つける。	
2.	適切な内部の人間または外部組織に事件について報告する。	
	封じ込め、根絶、復旧	
3.	証拠を取得、保全、確保、記録する。	

4.	事件の封じ込め - DoSを止める(まだ実行していない場合)	
4.1	悪用されたすべての脆弱性を見つけて修正する。	
4.2	まだ封じ込められない場合は、可能なら攻撃の特徴を基にフィルタリングを実施する。	
4.3	まだ封じ込められない場合は、攻撃をフィルタリングするようISPに支援を求める	
4.4	まだ封じ込められない場合は、ターゲットを再配置する。	
5.	事件を根絶する。ステップ4.1を実施しなかった場合は、悪用されたすべての脆弱性を見つけて修正する。	
6.	事件から復旧する。	
6.1	影響を受けたシステムを運用可能な状態に戻す。	
6.2	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。	
6.3	必要かつ可能なら、将来の関連する活動を見つけるため、追加の監視を実施する。	
事後活動		
7.	追跡レポートを作成する。	
8.	反省会を開催する。	

4.6. 推奨事項

このセクションで説明した、DoS事件の処理に関する主な推奨事項を、以下に要約する。

+ **ファイアウォールルールセットを設定して、リフレクタ攻撃を予防する** ほとんどのリフレクタ攻撃は、ネットワーク型およびホスト型のファイアウォールのルールセット使って、宛先ポートと送信元ポートの疑わしい組み合わせを拒否するように設定することで防ぐことができる。

+ **境界ルーターを設定してアンプ攻撃を防ぐ** 境界ルーターでディレクティッドブロードキャストを転送しないように設定することで、アンプ攻撃を防ぐことができる。

+ **組織のインターネットサービスプロバイダ(ISP)や二次プロバイダから、ネットワークベースのDoS攻撃の処理において、どういった支援が得られるのかを確認する** ISPは特定の種類のトラフィックをフィルタリングしたり、制限できることが多く、DoS攻撃を弱めたり停止したりできる場合がある。また、ISPがDoSトラフィックのログを提供したり、攻撃元の追跡を支援してくれる場合もある。事前にISPに確認して、このような支援を要請する際の手順を確立しておくこと。

+ **セキュリティソフトウェアを設定し、DoS攻撃を検知する** IDPSは、多くの種類のDoS活動を検知できる。ネットワークやシステム活動の基準を確立し、基準からの大きなずれを監視することも、攻撃を検知する上で役立つ。

+ **ネットワーク境界で、明示的に許可されていないすべての送受信トラフィックを拒否するように設定する** 外部との間で出入りするトラフィックの種類を制限することで、アタッカーがDoS攻撃で使用する可能性のある手段を制限できる。

+ **いくつかの対策を順に並べた封じ込め戦略を作成する** 推奨される対策を事前に規定して

おけば、DoS事件を封じ込めるための意思決定プロセスが容易になる。考えられる各対策の有効性は事件によって変わるため、いくつかの対策を選び、どの順番で対策を実施するかを決定する。

5. 悪意のコードによる事件の処理

5.1. 事件の定義と例

「悪意のコード」とは、別のプログラムにこっそりと埋め込まれたプログラムで、データを破壊したり、破壊的なプログラムや侵入目的のプログラムを実行したり、被害者のデータ、アプリケーション、またはオペレーションシステムのセキュリティや機密性、完全性、可用性などを侵害したりすることを目的としている。一般に悪意のコードは、システムのユーザに気づかれないように、これらの不正活動を実施するように設計されている。NIST SP 800-83『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(Guide to Malware and Incident Prevention and Handling)』に記載されているように、 悪意のコードによる攻撃は、ウイルス、トロイの木馬、ワーム、モバイルコード、混合物をはじめ、複数の種類に分類することができる。[91] マルウェアには、バックドア、ルートキット、キーストロークロガー、およびスパイウェアの普及に利用される追跡クッキーなども含まれる。

5.1.1. ウイルス

「ウイルス」は、自己複製、つまり自分自身を複製するように設計されており、自身の複製をほかのファイル、プログラム、コンピュータにばらまく。ウイルスは、自分自身をホストプログラムに埋め込み、そのプログラムがユーザの操作(ファイルのオープン、プログラムの実行、添付ファイルのクリックなど)によって実行されると増殖する。ウイルスの目的はさまざまである。ウイルスには、いらいらさせることが目的のものもあれば、破壊を目的にしているものもある。また、ジョークのように見せかけて、ひそかに破壊を実行するものもある。ウイルスの主な分類としては、コンパイル型ウイルス(オペレーションシステムによって実行されるもの)とインタプリタ型ウイルス(アプリケーションによって実行されるもの)がある。

コンパイル型ウイルスは、一般に、以下の3つの種類に分類される。

+ **ファイル感染型ウイルス** 「ファイル感染型ウイルス」は、ワードプロセッサ、スプレッドシートアプリケーション、コンピュータゲームなどの実行プログラムに自分自身を埋め込む。プログラムに感染すると、システム上のほかのプログラムに感染したり、感染したプログラムを共有して使用するほかのシステムに感染して増殖する。システムのメモリー内に潜み、新しいプログラムが実行されると、そのプログラムに感染するようになっているウイルスもある。ファイル感染の別の手段としては、ファイルを実効するプログラムを変更するのではなく、コンピュータがファイルを開く方法を変更するというものがある。このケースでは、、まずウイルスが実行され、次にプログラムが起動される。JerusalemとCascadeは、最も有名なファイル感染型ウイルスである[92]。

+ **ブートセクタウイルス** 「ブートセクタウイルス」は、ハードディスクのマスターブートレコード(MBR)か、フロッピーディスクなどのリムーバブル媒体のブートセクタに感染する。ブートセクタは、ドライブやディスクの先頭の部分であり、ディスクの構造に関する情報が格納されている。また、このセクタには、ブートプログラム(ホスト起動時にオペレーティングシステムをブートするために実行されるプログラム)も格納されている。一方、ハード

91 NIST SP 800-83では、マルウェア事件に対する組織の予防対策を改良するための奨励事項を提供している。また、マルウェア事件(特に広範囲に及ぶもの)への対応能力を高めるための奨励事項も提供している。このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.html から入手できる。

92 ウイルスに関する詳しい情報は、ほとんどのウイルス対策ソフトウェアベンダーのウェブサイトで得ることができる。ウイルス対策ソフトウェアベンダーとしては、Sophos 社(http://www.sophos.com/security/)、Symantec 社(http://www.symantec.com/business/security_response/threatexplorer/threats.jsp)、Trend Micro 社(http://www.trendmicro.com/vinfo/virusencyclo)などがある。

ディスクのMBRには、BIOS (Basic Input/Output System)が格納されており、この領域は、ブートプログラムをロードできるディスク上の唯一の領域である。フロッピーディスク等のリムーバブル媒体では、ブート可能でなくてもシステムに感染する。コンピュータのブート時に感染したディスクがドライブに入っていれば、ウイルスが実行される可能性がある。ブートセクタウイルスは隠すのが簡単で、成功する確率が高く、完全にコンピュータが動作できなくなるまで危害を与えることもできる。ブートセクタウイルスの感染による症状としては、ブート中にエラーメッセージが表示されたり、ブートできなかったりということが挙げられる。Form、Michelangelo、Stonedがブートセクタウイルスの例である。

+ **複合感染型ウイルス** －複合感染型ウイルスは、複数の感染手段を利用するもので、通常はファイルとブートセクタの両方に感染する。したがって、複合感染型ウイルスはファイル感染型ウイルスとブートセクタウイルスの特徴を併せ持っている。複合感染型ウイルスの例としてはFlipやInvaderがある。

OSによって実行されるコンパイル型ウイルスとは異なり、インタプリタ型ウイルスは特定のアプリケーションやサービスだけが実行できるソースコードで構成されている。インタプリタ型ウイルスはほかの種類のウイルスよりも作成や変更がずっと簡単であるため、きわめて一般的になってきている。以下に、インタプリタ型の主な2つの種類を示す。

+ **マクロウイルス** マクロウイルスは、最も流行し繁栄しているウイルスである。「マクロウイルス」は、自身をワードプロセッサのファイルやスプレッドシートのファイルに埋め込む。その名が示すとおり、マクロウイルスはアプリケーションのマクロプログラミング言語を使用して動作・繁殖する。Microsoft Officeのような、多くの一般的なソフトウェアパッケージでは、複雑な作業や繰り返し作業を自動化するために、製品内でマクロプログラミング言語を使用している。アタッカーは、マクロプログラミング言語の機能を利用し、悪意のコードを配布する。マクロ機能を持ったアプリケーションのドキュメントは、ユーザ間で共有されることが多いため、マクロウイルスが急速に広まる傾向にある。さらに、マクロウイルスの感染は、プログラムがファイルを作成したり開いたりする際に使用するテンプレートにまで及ぶ。その結果、感染したテンプレートを使って作成または開いたすべてのドキュメントが、マクロウイルスに感染してしまう。Concept、Marker、Melissaウイルスが、有名なマクロウイルスの例である。

+ **スクリプトウイルス** スクリプトウイルスはマクロウイルスにたいへんよく似ている。主な違いは、マクロウイルスがワードプロセッサなどの特定のアプリケーションが解釈する言語で記述されるのに対して、スクリプトウイルスはOSにより実行されるサービスが解釈する言語で記述される点である。よく知られているスクリプティングウイルスは、FirstとLove Stagesである。

5.1.2. ワーム

「ワーム」完全に自己完結した自己複製型のプログラムであり、ホストプログラムがなくても標的に感染する。ワームはまた自己増殖の能力も備えている。ワームは、ウイルスと違って完全に機能するコピーを作成でき、ユーザの介入なしに自身を実行する。ワームは、Windowsのセキュリティ保護されていない共有など、既知の脆弱性や構成上の弱点を利用する。ワームの中にはシステムリソースやネットワークリソースの浪費を主な目的とするものもあるが、その多くはバックドアをインストールし、分散型サービス不能（DDoS）攻撃をほかのホストに対して実行したり、そのほかの悪質な処理を実行したりすることによって、システムにダメージを与える。以下に、ワームの主な2つの種類を示す。

+ **ネットワークサービスワーム** ネットワークサービスワームは、OSやアプリケーションに関連したネットワークサービス内の脆弱性を悪用することによって拡散する。システムに感染

したワームは、通常そのシステムを利用してほかのシステムをスキャンし、標的となるサービスが実行されているかどうかを調べる。そして、それらのシステムへの感染も試みる。ネットワークサービスワームはまったく人の関与なしに実行されるため、通常、ほかの形態のマルウェアよりも急速に拡大する。ワームが急速に広まり、それらが新しい標的を探すために集中的にスキャンを実行する結果、感染したシステムだけでなく、ネットワークや（ネットワーク侵入検知センサーなどの）セキュリティシステムの処理能力が飽和することがしばしばある。ネットワークサービスワームの例として、SasserやWittyがある。

+ **大量メールワーム** 大量メールワームは電子メールによって媒介されるウイルスに似ているが、既存のファイルに感染するのではなく自己完結型である点が主な相違である。大量メールワームがいったんシステムに感染すると、通常、そのシステムで電子メールアドレスを検索し、システムの電子メールクライアントか、ワーム自身に組み込まれた自己完結型のメール送信プログラムを使用して、それらのアドレスに自分自身のコピーを送信する。大量メールワームは通常、自分自身の単一のコピーを複数の受信者に同時に送信する。大量の電子メールによって電子メールサーバとネットワークが飽和するだけでなく、大量メールワームに感染したシステムではパフォーマンス上の深刻な問題がしばしば生じる。大量メールワームの例として、Beagle、Mydoom、Netskyなどがある。

5.1.3. トロイの木馬

ギリシャ神話の木馬にちなんで名付けられたトロイの木馬は、見かけ上は良性のプログラムを装いながら、実際には悪意の目的を潜ませた非複製型プログラムである。トロイの木馬には、既存のファイル（システムやアプリケーションの実行可能ファイルなど）を悪意のあるものに置き換えるものや、既存のファイルを上書きせずに別のアプリケーションをシステムに追加するものがある。トロイの木馬は、便利な機能を実行しているように見えるため、検知が難しいことが多い。トロイの木馬は、以下の3つの型に分類することができる。

+ 元のプログラムの機能を引き続き実行しつつ、そのプログラムとは別に無関係な悪意のある活動を実行する。

+ 元のプログラムの機能を引き続き実行するが、そのプログラムの機能を悪意のある活動を実行するよう変更したり(例 パスワードを収集するログインプログラムのトロイの木馬版)、そのほかの悪意のある活動を隠蔽したりする(例 ほかの悪意のあるプロセスを表示しない、プロセス列挙プログラムのトロイの木馬版)。

+ 元のプログラムの機能を完全に置き換えて、悪意のある機能を実行する。たとえば、ゲームと称し、実際には実行されるとすべてのシステムファイルを単に削除するだけのファイルがある。

トロイの木馬を用いてスパイウェアプログラムを配布する手口はますます一般化してきている。スパイウェアは、P2Pファイル交換ソフトにバンドルされていることが多い。害のないプログラムであると想定してインストールすると、スパイウェアプログラムが密かにインストールされてしまう。また、トロイの木馬はしばしばほかの種類の攻撃ツールをシステムに送り込む。これらのツールによって、攻撃者は感染したシステムに不正にアクセスしたり、システムを利用したりすることができるようになる。これらのツールは、トロイの木馬にバンドルされていたり、トロイの木馬がシステムに組み込まれて実行された後にダウンロードされたりする。

5.1.4. 悪意のあるモバイルコード

「モバイルコード」は、通常はユーザによる明示的な指示なしにローカルシステムで実行されることを目的として、リモートシステムから送信されるソフトウェアである[93]。モバイルコードはWebブラウザや電子メールクライアントなど、多種多様なオペレーティングシステムやアプリケーションで使用できるプログラムを作成するための一般的な手段となっている。モバイルコードは通常は害がないが、攻撃者は、悪意のあるモバイルコードがシステムを攻撃するための効果的な手段であり、ウイルスやワーム、トロイの木馬などをユーザのワークステーションに送信するための格好のメカニズムであることに気づいている。悪意のあるモバイルコードは、ファイルに感染したり自分自身を伝染させようとしたりしない点が、ウイルスやワームと大きく異なる。特定の脆弱性を悪用するのではなく、モバイルコードに許可されているデフォルトの権限を利用してシステムに影響を及ぼすことが多い。モバイルコードを作成するためのポピュラーな言語には、Java、ActiveX、JavaScript、およびVBScriptなどがある。

5.1.5. 混合攻撃

「混合攻撃」は、複数の方法を使用して広まる悪意のコードである。有名なNimda「ワーム」は、実際には混合攻撃の例である[94]。Nimdaは、4つの拡散方法を使用している。

+ **電子メール**　脆弱性のあるホストで、ユーザが感染した電子メール添付ファイルを開くと、HTMLベースの電子メールを表示するために使用しているWebブラウザの脆弱性がNimdaによって悪用される。Nimdaはホストに感染したあとホスト上で電子メールアドレスを検索し、自分自身のコピーをそれらのアドレスに送信する。

+ **Windowsの共有**　Nimdaは、セキュリティ保護がされていないWindowsファイル共有を使用しているホストをスキャンし、NetBIOSを転送メカニズムとして利用し、感染したファイルをそのホストに転送する。感染したファイルをユーザが実行すると、そのホストでNimdaがアクティブになる。

+ **Webサーバ**　NimdaはWebサーバをスキャンし、Microsoftインターネットインフォメーションサービス（IIS）に存在する既知の脆弱性を探し出す。脆弱性のあるサーバであることがわかると、自分自身のコピーをそのサーバに転送し、サーバとそのファイルに感染しようとする。

+ **Webクライアント**　脆弱性のあるWebクライアントから、すでにNimdaに感染したWebサーバにアクセスすると、クライアントのワークステーションが感染する。

これらの方法を使用するほかにも、混合攻撃は、インスタントメッセージやピアツーピアのファイル共有といったほかのサービスを通じて広まる。Nimdaをはじめ、ほとんどの混合攻撃は、ワームと呼ばれる傾向がある。これは、それらの混合攻撃が、ワームと同じ特性をいくつか有するためである。実際にNimdaは、ウイルス、ワーム、モバイルコードの特性を備えている。

5.1.6. 追跡クッキー

クッキーは、特定のWebサイトの使用に関する情報を保持した小さなデータファイルである。[95] セッションクッキーは、1回のWebサイトセッションに対してのみ有効な一時的なクッキーである。

---

93 NIST SP 800-28 Version 2『Guidelines on Active Content and Mobile Code』には、モバイルコードの詳細な説明がある。このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.html で入手できる。

94 Nimdaワームに関するCERT®/CC アドバイザリは、http://www.cert.org/advisories/CA-2001-26.html で入手できる。

95 クッキーにはデータが平文のテキストで格納されることが多い。そのため、第三者がクッキーに不正にアクセスし、クッキーに格納されているデータを利用したり改ざんしたりすることも可能である。一部のWebサイトでは、暗号化されたクッキーを作成し、データを不正なアクセスから守っている。

永続クッキーはコンピュータ上に無期限に格納される。これは以後アクセスしてくるユーザをそのサイトで識別できるようにすることを目的としている。永続クッキーの意図されている用途は、単一のWebサイトに対するユーザ固有の設定を記録しておき、将来ユーザがサイトにアクセスした時にサイトの外観や動作を自動的にカスタマイズできるようにすることである。このようにすることで、Webサイトは永続クッキーを利用して自身のサービスをより効果的にユーザに提供できるようになる。

残念ながら、永続クッキーはスパイウェアとして濫用される可能性もある。ユーザによる認知や同意がないまま、疑わしい理由でユーザのWeb閲覧活動を追跡するおそれがある。たとえば、市場調査会社が多数のWebサイト上に広告を掲載し、ユーザのマシン上でクッキーを1つ使用して、それらすべてのWebサイトにおけるユーザの活動を追跡し、ユーザの振る舞いに関する詳細なプロファイルを作成することが可能である。このように使われるクッキーは追跡クッキーと呼ばれている。追跡クッキーによって収集された情報は別の業者に売り渡され、広告や他のコンテンツをユーザに向けて送付するのに使われることが多い。ほとんどのスパイウェア検出／駆除ユーティリティは、特にシステム上の追跡クッキーを見つけようとする。

5.1.7. 攻撃ツール

マルウェア感染やほかのシステム侵害の一部として、さまざまな種類の攻撃ツールがシステムに送り込まれることがある。これらのツールはマルウェアの一種であり、攻撃者はこれらを利用して、感染したシステムやそのデータへの不正アクセスや不正利用を行ったり、さらなる攻撃を仕掛けたりすることができる。攻撃ツールが別のマルウェアによって転送される場合は、（トロイの木馬などの中で）マルウェアそのものの一部として送り込まれるか、マルウェアに感染した後に送り込まれることがある。たとえば、ワームによって、ワームに感染したシステムから特定の悪意のあるWebサイトにアクセスし、そのサイトからツールをダウンロードし、システムにインストールするように仕向けられる場合がある。以下に、攻撃ツールの例を示す。:

+ **バックドア**は、特定のTCP（伝送制御プロトコル）またはUDP（ユーザデータグラムプロトコル）ポートでコマンドを傍受する、悪意のあるプログラムを表す一般用語である。バックドアのほとんどはクライアントコンポーネントとサーバコンポーネントで構成される。クライアントは侵入者のリモートコンピュータに存在し、サーバは感染したシステムに存在する。クライアントとサーバ間の接続が確立されると、遠隔地にいる侵入者が感染対象コンピュータをある程度制御できるようになる。少なくともほとんどのバックドアでは、攻撃者が一連の特定の操作をシステム上で実行することが可能である。たとえば、ファイルの転送やパスワードの取得、任意のコマンドの実行などが可能となる。バックドアのなかにはBot機能を持つものや、遠隔のアタッカーが必要に応じて感染したシステムにアクセスすることを可能にするものもある。

+ **キーストロークロガー**は、キーロガーとも呼ばれ、キーボードの使用を監視して記録する[96]。キーストロークロガーは、システムに入力された情報を記録する。たとえば、電子メールの

96 キーストロークロガーによっては、画面キャプチャなど、ほかのデータ記録機能も持つものがある。

内容、ローカルまたはリモートのシステムやアプリケーションのユーザ名とパスワード、金融情報（クレジットカード番号、社会保障番号、暗証番号（PIN）など）が記録される可能性がある。キーストロークロガーには、攻撃者にシステムからのデータの取得を要求するものや、電子メールやファイル転送などの手段を通じて別のシステムにデータを能動的に転送するものがある。

+ **ルートキット**は、システムにインストールされ、システムの標準機能を悪意を持って密かに改ざんするファイルの集まりである。UNIXやLinuxなどのオペレーティングシステムでは、ルートキットによって（システムバイナリを含む）数十から数百ものファイルが変更または置き換えられてしまう。一方、Windowsなどのオペレーティングシステムでは、ファイルを変更または置き換えるものや、メモリ内にのみ常駐してOSの組み込みシステムコールの使用を変更するものがある。ルートキットは、数多くの変更をシステムに加えることによって、ルートキット自身の存在や、ルートキットによってシステムに加えられた変更そのものの証拠を隠すため、ルートキットがシステムに存在することや、ルートキットがどのような変更を行ったのかについて判断することはたいへん難しい。たとえば、ルートキットは、自分自身のファイルに関するディレクトリやプロセスのエントリーを一覧表示に表示されないようにすることがある。ルートキットはバックドアやキーストロークロガーなどのほかの種類の攻撃ツールをシステムにインストールする目的で用いられることが多い。

+ **ウェブブラウザのプラグイン**は、特定の種類のコンテンツをWebブラウザを通じて表示または実行するための手段を提供する。攻撃者は、スパイウェアとして機能する悪意のプラグインを作成することがある。ブラウザにインストールされたこれらのプラグインは、ブラウザのあらゆる使用状況（ユーザがどのWebサイトやWebページにアクセスしたのかなど）を監視して、外部の第三者に報告することができる。プラグインはWebブラウザの起動時に自動的にロードされるため、システム上のWeb活動を容易に監視できる手段となる。悪意のWebブラウザプラグインの中にはスパイウェアダイヤラとなっているものがある。これらはモデム回線を利用して、ユーザの許可や認知がないまま電話番号にダイヤルする。ダイヤラの多くは分単位で高額な課金を行う電話番号に電話をかけるように設定されているが、救急サービス（米国911番）などに迷惑電話をかけるものもある。[97]

+ **電子メールジェネレータ**は、電子メール生成プログラムをシステムに送り込むことができる。電子メール生成プログラムを使用すると、ユーザの許可や認知なしに大量の電子メールを作成してほかのシステムに送信することができる。攻撃者は、マルウェアやスパイウェア、スパム、あるいは他のユーザが望んでいないコンテンツを、事前に定義されたリストの電子メールアドレスに送信するように、電子メールジェネレータを設定することが多い。

5.1.8. マルウェア以外の脅威

この項では、マルウェアに分類されない脅威のうち、マルウェアに関連付けられることが多い2つの形態(フィッシング詐欺と偽ウイルス)について簡単に説明する。フィッシング詐欺と偽ウイルスは、双方ともソーシャルエンジニアリングに依存する。ソーシャルエンジニアリングとは、

97 ダイヤラーのなかには、トロイの木馬などWebブラウザプラグイン以外の形態のものもある。

人をだまして機密情報を開示させる、あるいは、良性であるように見えるが実際は悪意のあるファイルをダウンロードして実行するというような特定の動作を実行させようとする攻撃者が使う一般用語である。フィッシングと偽ウイルスは、一般にはマルウェアの一形態とはみなされていないが、マルウェアと関連して議論されることが多いため、完全を期すためにこの項で簡単に説明する。

フィッシングは、個人をだまして機密性の高い個人情報を開示させるために用いられるコンピュータベースの詐欺手法である。[98] フィッシング攻撃を仕掛ける場合、攻撃者は、あたかもオンライン企業やクレジットカード会社、金融機関などの有名な組織のものであるかのように見えるWebサイトや電子メールを作成する。[99] このような詐欺を目的とした電子メールやWebサイトは、ユーザをだまして個人情報（通常は金融情報）を開示させることを意図としている。たとえば、フィッシング攻撃者は、オンラインバンキングサイトのユーザ名とパスワードや、銀行の口座番号を探す場合がある。

フィッシング攻撃は、犯罪者が身元情報の窃盗や詐欺などの広範な違法行為を働く際の助けとなっている。また、マルウェアや攻撃ツールをユーザのシステムにインストールするのにも利用される可能性がある。マルウェアをインストールするフィッシング攻撃では、Webサイト上に虚偽のバナー広告やポップアップウィンドウを表示するのが常套手段である。偽の広告やポップアップウィンドウをクリックしたユーザのシステムには、ユーザが気づかないうちにキーストロークロガーがインストールされてしまうことがある。フィッシング攻撃者はこれらのツールを利用することにより、1つのWebサイトについてだけでなく、ユーザが訪問する任意かつすべてのWebサイトについてユーザの個人情報やパスワードを記録することができる。

偽ウイルスは、その名が示すとおり、偽のウイルス警告である。通常、偽ウイルスでは、「壊滅的なものであり、コンピュータリソースを感染から適切に保護するために迅速な措置が必要だ」といった説明が表示される。ユーザ間で電子メールを通じて送信されるウイルス警告の大多数は、実際は偽ものである。ユーザは、そのような警告を配布することによってほかのユーザを助けることになると信じているため、偽ウイルスはユーザ間で何か月あるいは何年にもわたって転送されることが多い。偽ウイルスは通常は損害を与えることはないが、中には悪意のあるものもあり、OSの設定を変更したりファイルを削除したりするようユーザに指示を出すものもある。その結果、セキュリティ上または運用上の問題を引き起こす可能性がある。偽ウイルスの受信者の多くは、新しい脅威について技術サポートのスタッフに連絡して警告したり、ガイダンスを求めたりするため、偽ウイルスが組織にとって時間を浪費する存在となる可能性もある。

5.2. 準備

このセクションでは、悪意のコードによる事件の処理に備えそれを予防するための手引きを示す。

5.2.1. 事件処理の準備

セクション3.1.1と3.2.3で説明した一般的な手引きに加え、悪意のコードによる事件の処理に備える際には、以下に示す内容も実行する。

+ **悪意のコードの問題について、ユーザに自覚させる** この情報には、悪意のコードが増殖するのに使用する手段と、感染の症状の基本的なレビューを盛り込む。定期的にユーザ教育

98 最近のフィッシング攻撃の例を含むフィッシングの詳細に関しては、Anti-Phishing Working Group Web site (http://www.antiphishing.org/)を参照のこと。別の良いリソースとしては、FTC(Federal Trade Commission)発行の『How Not to Get Hooked by a “Phishing” Scam』 (http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm)がある。

99 フィッシング攻撃は従来からのコンピュータに制限されるものではなく、携帯電話やPDA端末などのコンピューティング機器も標的にされることがある。

セッションを開催することは、悪意のコードがもたらすリスクについて、ユーザに自覚させるのに役立つ。また、感染したら何をすべきかについての手引き(たとえば、ワークステーションをネットワークから切断する、ヘルプデスクに電話するなど)も説明する。常時適切に対処しないと、小さな事件でも悪い結果になる場合があるためである。

+ **ウイルス対策ソフトウェアベンダーの広報を読む** ウイルス対策ソフトウェアベンダーのメーリングリストに加入して、新しい悪意のコードの脅威に関する情報をタイムリーに入手する。

+ **重要なホストには、ホスト型の侵入検知システムを配備する** ホスト型のIDPSは、設定の変更や、システムの実行ファイルの改ざんなど、悪意のコードの事件を検知することができる。ファイル完全性チェッカーは、システムの感染した要素を見つけるのに便利である。

+ **マルウェアインシデント分析リソースを収集する** 事件が発生する前に、適切な分析リソースを入手する。事件の特定と確認を補助するための、ポートリスト、オペレーティングシステム関連文書、アプリケーション関連文書、重要な資産のネットワーク図とリスト、および想定されるネットワーク活動、システム活動、およびアプリケーション活動のベースラインを用意する。

+ **マルウェアインシデント軽減ソフトを入手する** 回復作業を補助するために、適切なインシデント軽減ソフトを入手する。 組織は、オペレーティングシステムの起動ディスクやCD、オペレーティングシステムのベンダーとアプリケーションのベンダーからのセキュリティパッチ、およびディスクイメージングソフトウェアとクリーンバックアップを備えるべきである。

組織のなかには、トロイの木馬のポートとしてよく利用されるポートへの接続をブロックするように、ネットワーク境界の設定しているところもある。これは、トロイの木馬のクライアントがサーバコンポーネントに通信するのを阻止するために行われる。しかし、このアプローチは一般に有効でない。既知のトロイの木馬は、数百もの異なるポート番号を使用し、多くのトロイの木馬は、使用するポートを自由に設定できるようになっている。さらに正当なサービスと同じポート番号を使用するトロイの木馬もあるため、ポート番号で通信をブロックするわけにはいかない。ポートのブロックを誤って実施しているために、正常なコネクションまでブロックしてしまう組織もある[100]。個々のトロイの木馬のポートに対して個別にフィルタリング規則を作成すると、フィルタリング装置に対する要求も増えることになる。デフォルトですべてのトラフィックを拒否し、許可されたコネクションだけを許可するほうが、特定のトロイの木馬のポートをブロックしようとするよりも、より効果的である。一般に、特定のトロイの木馬のポートをブロックするのは、組織が、そのトロイの木馬にひどく感染した場合だけにすべきである。

5.2.2. 事件の予防

セクション3.1.2は、事件の発生を予防するための、一般的なガイドラインとリソースである。以下のパラグラフでは、悪意のコードの事件を予防するための具体的な助言を提供する。

+ **ウイルス対策ソフトウェアの利用** 悪意のコードと戦い、被害を食い止めるためには、ウイルス対策ソフトウェアは必需品である。このソフトウェアは、組織全体のすべてのホストで動作させ、新しい脅威を阻止するよう、最新のウイルスシグネチャを使って最新状態に

100 ポートが27374になっていれば、それが送信元ポートでも宛先ポートでも、すべてのコネクションをブロックするように誤ってフィルタリング装置が設定されていることがある。27374はSubSevenで使用されるが、オペレーティングシステムが正当なクライアントポートとしてこれを使用することもある。

保つべきである[101]。ウイルス対策ソフトウェアは、電子メール、ファイル転送、インスタントメッセージソフトウェアなど、悪意のコードを運ぶアプリケーションに対しても使用することをお勧めする。各ファイルをダウンロード、オープン、実行する際にリアルタイムでスキャンするのと同様に、システムのスキャンを定期的に行うように設定する。また、感染したファイルからウイルスを除去および隔離するように設定する[102]。ウイルス対策製品によっては、ウイルス、ワーム、トロイの木馬を見つけるだけでなく、悪意のある内容がないか、HTML (HyperText Markup Language)、ActiveX、JavaScript等のモバイルコードの中を調べるようになっている。

+ **スパイウェアの設置の防止** Webブラウザの中には、Webブラウザプラグインなどのソフトウェアのインストールについて、ユーザに承諾を求めるように設定できるものがある。すべてのWebサイトについて、クライアントへのソフトウェアのインストールを防止することが可能なブラウザもある。これらの設定は特に、Webブラウザへのスパイウェアのインストールを防ぐのに役立つ。スパイウェアの脅威を軽減するために組織は、スパイウェア検出／駆除ユーティリティか、スパイウェアの脅威を認識する機能を備えたウイルス対策ソフトウェアのいずれかを使用するようにする。ウイルス対策ソフトウェアは、要件を満たすソフトウェアが利用可能なすべてのシステムで使用するべきである。

+ **疑いのあるファイルのブロック** 悪意のコードに関係するファイル拡張子(.pif、.vbsなど)や、疑いのあるファイル拡張子(.txt.vbs、.htm.exeなど)持った添付ファイルをブロックするように、電子メールサーバやクライアントを設定する。こうすることで未知の脅威を阻止することができるが、正規の活動を誤ってブロックしてしまうこともある。組織によっては、受信者が添付ファイルを実行する前に、ファイルを保存して名前を変更しなければならないように、疑わしい電子メールの添付ファイルのファイル拡張子を変更している。環境によっては、このような措置が機能とセキュリティの良好な妥協策となる。

+ **スパムのフィルタリング** スパムはフィッシングやスパイウェアの送付に使用されることが多く、ほかの種類のマルウェアが含まれていることもある。電子メールサーバや電子メールクライアント、あるいはネットワークベースのアプライアンスでスパムフィルタリングソフトウェアを使用することにより、ユーザに到達するスパムの量を大幅に減らすことができ、ひいてはスパムによって引き起こされるマルウェアインシデントの相応の削減につながる。

+ **ファイル転送機能を持った不必要なプログラムの使用を制限する** 例としては、ピアツーピアでファイルや音楽を共有するプログラム、インスタントメッセージソフトウェア、IRCクライアントとサーバが含まれる。これらのプログラムは、悪意のコードをユーザ間で広めるのに頻繁に利用される。

+ **電子メールの添付ファイルの安全な扱い方について、ユーザを教育する** ウイルス対策ソフトウェアは、各添付ファイルを開く前にスキャンするように設定する。ユーザは、疑わしい添付ファイルや出所が不明な添付ファイルは開かないようにする。また、送信者を知っているからといって、添付ファイルが感染していないと思ってはならない。たとえば、送信者が、自身のシステムが悪意のコードに感染していて、そのコードがシステム上のファイルから電子メールアドレスを抽出し、コードの複製をこれらのアドレスに送りつけていることに気づかない場合がある。この場合、受信者にとっては、電子メールが信頼の置け

101 シグネチャの最新版を自動的にダウンロードしてインストールするようにウイルス対策ソフトウェアを設定することを好む組織もあれば、気づかずにシステムの機能を損なうことがないよう、ユーザにシグネチャの最新版の利用を許可する前に、テストすることを好む組織もある。どちらのアプローチにも利点と欠点があり、どちらかが明らかに優れているということはない。

102 ファイルからウイルスを除去できなかった場合は、事件処理と証拠の観点から、ファイルを削除するよりも隔離するほうが望ましい。

る人から届いたように見えるが、メールの送信者はメールが送られたことすら気づかないといったことになる。ユーザには、開いてはいけないファイルの種類(たとえば*.bat*、*.com*、*.exe*、*.pif*、*.vbs*など)についても教育する。ユーザがよい習慣を身につけることで、悪意のコードの事件の数や深刻性は減るが、それでも組織は、ユーザのミスによってシステムが感染する可能性を考慮しなければならない。

+ **開かれているWindowsの共有を解除する** いくつかのワームは、Windowsを実行しているホストの安全でない共有を通じて広まる。組織内の1台のホストがワームに感染すると、安全でない共有を通じて、組織内のほかの何百・何千というホストに瞬く間に広まる可能性がある。ホストの開かれている共有を定期的にスキャンし、共有のセキュリティを適切に高めるよう、システムオーナーに指示するべきである。また、ネットワーク境界を設定し、NetBIOSポートを使用したトラフィックが組織のネットワークに出入りできないようにする。この作業により、開かれた共有を通じて、外部のホストから直接内部のホストに感染するのを防ぐだけでなく、内部のワーム感染がほかの組織に広まるのも防ぐことができる。

+ **ウェブブラウザを安全に使用して、モバイルコードを制限する** 署名されていないActiveXやその他のモバイルコードの転送メカニズムが、ローカルシステムに知らないうちにダウンロードされて実行されないように、すべてのウェブブラウザのセキュリティを設定する。さまざまな場所(内部サーバ、外部サーバ)でどの種類のモバイルコードを使用してよいかを規定した、インターネットセキュリティポリシーを策定することを検討すべきである。Webコンテンツフィルタリングソフトウェアを導入してWeb関連のネットワーク活動を監視し、信頼できない場所から送信された特定の種類のモバイルコードをブロックすることもできる。

+ **電子メールのオープンリレーを防止する** 大量メール送信ワームの中には、組織のメールサーバをオープンリレーとして使用しようとするものがある。オープンリレーとは、電子メールの送信者も受信者も対象組織に所属していないことを意味する。オープンリレーを許可する電子メールサーバは、大量メール送信ワームに伝染のための容易な手段を提供する可能性がある。組織は、オープンリレーを防ぎ、電子メールサーバをリレーとして使用しようとするすべての試みを記録するように、電子メールサーバを設定することを検討すべきである。[103]

+ **電子メールクライアントをより安全に動作するように設定する** 組織全体の電子メールクライアントを、うっかりと感染してしまうような操作を防ぐように設定する。たとえば、添付ファイルを自動的に開いたり、実行しないようにする。

5.3. 検知と分析

マルウェアは数分のうちに感染が組織全体に広がるおそれがあるため、マルウェアインシデントの検知と確認を迅速に行うよう努めるべきである。早期に検知することにより、感染するシステムの数を最小限に留めることができ、復旧に要する作業と組織が被る損害の量も少なくなる。重大なマルウェアインシデントの場合、組織への攻撃の速度があまりに速いため、対応する時間がまったく取れないこともあるが、ほとんどのインシデントは、より緩やかに発生・進行する。

悪意のコードの事件はいろいろな形で起きる可能性があるため、さまざまな前兆や兆候を通じて検知できる。表5-1の「悪意のコードの前兆」では、考えられる悪意のコードの前兆の一覧を挙げ、そのような活動がなぜ行われるかを説明し、事件の発生を予防するために推奨される対応を説明

103 オープンリレーリレーと、電子メールのセキュリティの他の側面の詳細については、NIST SP 800-45『Guidelines on Electronic Mail Security』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照。

する。表5-2「悪意のコードの兆候」では、ウイルス、ワーム、トロイの木馬の感染など、悪意のコードの活動と、各活動の考えられる兆候を挙げる。混合攻撃は、ウイルス、ワーム、モバイルコードの手法など、使われている個別の方法に応じて検知されるため、ここには挙げていない。組織は、これらの表を手軽にカスタマイズして、環境特有の前兆や兆候を追加してかまわない。それがより効率的で効果的な事件処理プロセスを促進する。

表5-1 悪意のコードの前兆

前兆	対応
組織が使用しているソフトウェアをターゲットとした、新種の悪意のコードについての警報	新種のウイルスを調査し、本物かデマかを判断する。これは、ウイルス対策ソフトウェアベンダーのウェブサイトやウイルスデマ情報のウェブサイトでわかる。悪意のコードが本物だと確認されたら、その新種の悪意のコードに対するウイルスシグネチャを使って、ウイルス対策ソフトウェアを更新する。ウイルスシグネチャがまだ入手できず、脅威が甚大で差し迫っている場合は、電子メールサーバやクライアントで新しい悪意のコードの特徴に一致する電子メールをブロックするなど、ほかの手段を使ったブロックが必要になる可能性がある。組織は、新種のウイルスについて、ウイルス対策ソフトウェアベンダーに連絡してもよい。
ウイルス対策ソフトウェアが、新しく受信した感染ファイルを検知し、ウイルス除去や隔離に成功した。	悪意のコードがどうやってシステムに入ってきたか、どんな脆弱性や弱点を悪用しようとしていたかを調べる。悪意のコードがほかのユーザやホストに重大なリスクを生じさせかねなかった場合は、悪意のコードがシステムに到達するのに使用した弱点と、ターゲットホストに感染するのに使われた弱点を修正する。

前兆を検知することにより、組織はセキュリティ体制を変更し、前兆のすぐあとに発生するインシデントに対応するための警戒態勢を敷くことで、インシデントを防止する機会を得る。最も深刻なケースで、組織が重大なインシデントに巻き込まれることがほぼ確実であるような場合、組織はインシデントがすでに発生しているものと仮定して行動することを決定し、インシデント対応機能を発動することもできる。とはいえ、ほとんどではないものの、多くのマルウェアインシデントは明確な前兆がなく、また、前兆はインシデント発生の直前に現れることが多い。したがって、組織はそのような事前の警告に依存するべきではない。

表5-2 悪意のコードの兆候

悪意のある活動	予想される兆候
電子メールで広まるウイルスがホストに感染した	・ファイルが感染したことを検知したウイルス対策ソフトウェアが警報を発する ・送受信する電子メールの数が突然増加した ・ワードプロセッサのドキュメントやスプレッドシート等のテンプレートへの変更 ・削除または破壊されたファイルや、アクセスできないファイルがある ・画面に奇妙なメッセージやグラフィックスなど、異常なものが表示される ・プログラムの起動が遅い、動作が遅い、まったく起動しない ・システムが不安定、クラッシュする ・ウイルスがrootレベルにアクセスする場合は、表6-3の「不正アクセスの兆候」の、「ホストのroot奪取」に対する兆候を参照

脆弱なサービスを通じて広まるワームにホストが感染する	・ファイルが感染したことを検知したウイルス対策ソフトウェアが警報を発する ・脆弱なサービス(たとえば、開かれているWindowsの共有や、HTTPなど) をねらったポートスキャンやコネクションの失敗 ・ネットワーク使用率の増加 ・プログラムの起動が遅い、動作が遅い、まったく起動しない ・システムが不安定、クラッシュする ・ワームがrootレベルにアクセスする場合は、表6-3の「不正アクセスの兆候」の、「ホストのroot奪取」に対する兆候を参照
トロイの木馬がインストールされホストで実行されている	・トロイの木馬バージョンのファイルを検知したウイルス対策ソフトウェアが警報を発する ・トロイの木馬のクライアントサーバ通信を検知したネットワーク侵入検知装置が警報を発する ・トロイの木馬のクライアントサーバ通信に関する兆候が、ファイアウォールとルーターのログに記録される ・ホストと不明なリモートシステム間のネットワーク通信 ・異常かつ予期しないポートのオープン ・不明なプロセスの動作 ・ホストによる大量のネットワークトラフィックの生成。特に外部ホストに向けたもの ・プログラムの起動が遅い、動作が遅い、まったく起動しない ・システムが不安定、クラッシュする ・トロイの木馬がrootレベルにアクセスする場合は、表6-3の「不正アクセスの兆候」の「ホストのroot奪取」に対する兆候を参照
ウェブサイト上で悪意のあるモバイルコードを使用して、ホストをウイルス、ワーム、トロイの木馬に感染させる	・関係する悪意のコードの種類に対する、上記の兆候 ・何かの許可を要求する、予期しないダイアログボックスが表示される ・グラフィックスの異常。たとえば、メッセージボックスのオーバーラップやオーバーレイなど
ウェブサイト上の悪意のコードがホストの脆弱性を悪用する	・何かの許可を要求する、予期しないダイアログボックスが表示される ・グラフィックスの異常。たとえば、メッセージボックスのオーバーラップやオーバーレイなど ・送受信する電子メールの数が突然増加した ・ホストと不明なリモートシステム間のネットワーク通信 ・モバイルコードがrootレベルにアクセスする場合は、表6-3の「不正アクセスの兆候」の、「ホストのroot奪取」に対する兆候を参照
ユーザがウイルスデマ情報を受信	・メッセージの送信元が権威あるコンピュータセキュリティグループでなく、政府機関や政府の要人である。 ・外部の情報源へのリンクがない ・口調や用語が、パニックや切迫感を呼び起こそうとしている

	・特定のファイルを削除し、メッセージをほかの人に転送するようせき立てている

これらの兆候のほとんどはマルウェア以外が原因で発生する可能性がある。たとえば、Webサーバのクラッシュは、マルウェア以外による攻撃、OSの欠陥や停電などが原因で起こる可能性がある。電子メールの返送は、システムハードウェアの障害や電子メールサーバの設定の誤りが原因で起こる可能性もあれば、スパム送信業者によるなりすましの可能性もある。こうした複雑な要素はマルウェアインシデントの検知と確認の難しさを示すものであり、何が起きたのかを判断するために速やかな分析を行うことのできる、十分な訓練を受けた、技術的な知識を有するインシデント対応担当者を確保する必要があることを示している。

悪意のコードは、ほかのシステムに広まる傾向があるため、事件に適切に優先順位を付けることが重要である。ほとんどの場合、事件の基本的な分析を通じてどの悪意のコードが使用されたかがわかる。このため、事件による影響を予測することは、比較的容易である。事件処理担当者は、事件の際、感染したすべてのシステムを把握することはできないかもしれないが、ほとんどの場合、事件が数台のシステムにしか影響しないのか、組織全体の何千というサーバやワークステーションに影響するのかは判断できる。組織では、マルウェアに関係する各種の状況に対する適切な対応レベルを明確にするための一連の基準を確立するべきである。この基準には次のような考慮事項を盛り込む。

- マルウェアがどのような手段で環境に侵入し、どのような感染メカニズムを使用するか
- どのような種類のマルウェアか（ウイルス、ワーム、トロイの木馬など）
- マルウェアによってどのような種類の攻撃ツールがシステムに置かれたか
- マルウェアが影響を与えているネットワークおよびシステム、およびどのように影響を与えているか
- インシデントを封じ込めなかった場合に、今後数分、数時間、および数日のうちにインシデントの影響がどの程度増大するか

5.4. 封じ込め、根絶、復旧

セクション3.3で説明した一般的な手引きに加え、このセクションでは、悪意のコードによる事件の封じ込めと証拠の収集・処理を行うための、具体的な推奨事項を説明する。

5.4.1. 封じ込め戦略の選択

悪意のコードはひそかに活動し、ほかのシステムに急速に増殖する可能性があるため、感染が拡大してより大きな被害を与える前に、事件を早期に封じ込める必要がある。感染したシステムが重要でない場合は、すぐにネットワークから切り離すことを強くお勧めする。一方、感染したシステムが重要な機能を実行している場合は、サービスが利用できないことによる組織への損害が、すぐにシステムを切り離さないことによるセキュリティ上のリスクを上回る場合にだけ、ネットワークに接続したままにしておく。悪意のコードによる事件を封じ込める際に実行する必要があ

るその他の行動としては、次のものがある。

+ **セクション5.2.2に挙げた行動** ホストの1台が感染すると、ほかのシステムも感染する可能性が非常に高いため、封じ込めプロセスには、悪意のコードがほかのシステムに広がるのを防ぐことが含まれる。

+ **ほかに感染したホストを見つけて隔離する** ウイルス対策ソフトウェアの警報メッセージはよい情報源であるが、ウイルス対策ソフトウェアですべての感染が検知できるわけではない。事件処理担当者は、以下に示すような別の手段を使って感染の兆候を探さなくてはならいこともある。

  - ポートスキャンを行って、既知のトロイの木馬やバックドアポートを待ち受けているホストを検知する。

  - 特定の悪意のコードに対処するためにリリースされている、ウイルス対策のスキャンツールとクリーンアップツールを使用する。

  - 電子メールサーバのログ、ファイアウォールのログ、悪意のコードが通過した可能性があるシステムのログ、および各ホストのログをレビューする。

  - 感染に関係のある活動を見つけるよう、ネットワークおよびホストの侵入検知ソフトウェアを設定する。

  - システム上で動作しているプロセスを監査して、すべて正当なものであることを確認する。

+ **不明な悪意のコードをウイルス対策ソフトウェアベンダーに送る** 時折、ウイルス対策ソフトウェアで断定的に判別できない悪意のコードが環境に入ってくることがある。ベンダーからの、最新のアンチウイルスシグネチャがないと、システムから悪意のコードを根絶し、さらなる感染を予防するのは、困難または不可能である。事件処理担当者は、不明な悪意のコードのコピーをウイルス対策ソフトウェアベンダーに送るための手順に精通している必要がある。

+ **電子メールをブロックするよう電子メールサーバとクライアントを設定する** 多くの電子メールプログラムは、特定のタイトル、添付ファイル名、悪意のコードに対応するその他の条件で電子メールをブロックするよう、手動で設定できる。これは絶対確実というわけでも、効率的な対策というわけでもないが、差し迫った脅威が存在し、アンチウイルスシグネチャがまだ入手できない場合には、最良の選択肢となりうる。

+ **特定のホストのブロック** たとえば、もし悪意のコードが外向きの電子メールやコネクションを生成しようとする場合、事件処理担当者は、感染したシステムが接続しようとするIPアドレスやサービスへのアクセスをブロックすることも検討すべきである。また、組織内の感染したホストが感染を広めようとしている場合は、感染したホストの物理的位置を見つけてウイルスなどを除去するまでの間、事態を掌握するために、そのホストのIPアドレスからのネットワークトラフィックをブロックしてもよい。

+ **電子メールサーバのシャットダウン** 重大な悪意のコードの事件のほとんどでは、内部のホストが数百から数千も感染していると、電子メールで広まろうとするウイルスのせいで、電子メールサーバが完全に過負荷に陥る場合がある。電子メールを介したウイルスの拡散を止めるためには、電子メールサーバをシャットダウンしなくてはならない場合もある。場合によっては、シャットダウンが必要な不明な電子メールサーバ(たとえば、気づかずに電子メールサーバを動作させているファイルサーバなど)が見つかることもある。

+ **インターネットからのネットワークの隔離** 深刻なワームの蔓延が起きると、ネットワークがワームのトラフィックであふれかえる場合がある。また時折、インターネット全体でワームがあまりにも大量のトラフィックを生成し、ネットワーク境界が完全に過負荷に陥ることもある。特に、ワームのトラフィックのせいで組織のインターネットアクセスが基本的に役に立たない場合は、組織をインターネットから切断することをお勧めする。この行動は外部のワームから組織のシステムが攻撃されるのを防ぐ。もし組織のシステムがすでに感染している場合は、この行動により、内部のシステムがほかのシステムを攻撃し、トラフィックの輻輳を増やすのを防ぐことにもなる。

+ **ユーザの参加を要請する** ユーザには、システムが感染したことを識別する方法と、感染した場合の措置について説明した作業指示を与えることができる。措置としては、たとえばヘルプデスクに電話で連絡する、ネットワークへのシステムの接続を解除する、システムの電源を切る、などが考えられる。ユーザの関与は封じ込めに大いに役立つ可能性があるが、マルウェアインシデントの封じ込めを主にこの手段に頼ることは避けるべきである。

+ **サービスの無効化** インシデントは、サービスの喪失を通じて迅速かつ効果的に封じ込めることができる。たとえば、マルウェアに悪用されているサービスを停止したり、ネットワーク周辺部で特定のサービスを遮断したり、サービスの一部（大規模なメーリングリストなど）を無効にしたりする。組織が利用しているサービスを無効にすると、組織の機能に明らかにマイナスの影響が出る。また、サービスを無効にすると、そのサービスに依存しているほかのサービスを誤って停止させてしまうこともある。重要なサービスについては、インシデント対応担当者が封じ込めに関する決定を下す際に考慮できるように、それらの依存関係の一覧を維持するべきである。マルウェアによる影響を最も受けやすいサービスは、電子メールである。

+ **接続の無効化** ネットワーク接続を一時的に制限することによるインシデントの封じ込めは、大きな効果を発揮することがある。組織のネットワークは、接続の喪失による封じ込めを容易に実施できるように、そして機能不全がより少なく済むように、設計し実装することができる。たとえば、組織によってはサーバとワークステーションを別々のサブネットに配置しているところがある。マルウェアの封じ込めに関係するもう1つのネットワークデザイン戦略は、感染したシステムに独立の仮想ローカルエリアネットワーク（VLAN）を使用する方法である。

コンピューティングは日々変化しているため、感染したホストと脆弱なホストを捜すのは非常に複雑な作業である。すべてのホストの電源が入っており、常にネットワークに接続されている場合は、悪意のコードの一掃は比較的容易である。しかし実際の状況では、ホストは感染しているが電源がオフになっていたり、ほかのネットワークに移動されていたり、システムのオーナーが外出している間起動したままになっているかもしれない。オーナーが休暇中の間停止されていた脆弱なホストは、再度電源を入れたとたんに感染する可能性がある。脆弱なホストと感染したホストの特定は、単にユーザの偶発的な行動の結果に頼るべきではない。しかし、特に多数のモバイルユーザと在宅勤務者がいる場合には、感染したマシンを手動で突き止めるための要員も時間もない組織が多い。方法を自動化したとしても、複数のオペレーティングシステムをブートできるホストや、仮想オペレーティングシステムソフトウェアを使用しているホストもあり、すべてのホストを見つけるのには適していない場合がある。組織は、悪意のコードによる大規模な事件が起きる前に、事件の効果的な封じ込め戦略の一環として、複数の特定戦略を用いることを、慎重に検討すべきである。

5.4.2. 証拠の収集と処理

悪意のコードは感染したユーザにより自動的に送信されたか、誤って送信されたものであるため、

悪意のコードについての証拠を収集することはたしかに可能だが、無駄に終わることが多い。このため、悪意のコードの犯人を見つけることはきわめて難しく時間もかかる。感染しているホストを識別する手法の分類として、フォレンジック識別、動的識別、および手動識別がある。

+ **フォレンジックによる識別** フォレンジックによる識別は、最近の感染の証拠を探し出すことによって、感染したシステムを識別する手法である。証拠は、非常に新しい場合（数分前）やそれほど新しくない場合（数時間前や数日前）があるが、情報が古いほどその情報が正確である可能性も低くなる。証拠の情報源として最も明らかなものは、マルウェアの活動を識別することを目的とした情報源である。たとえば、ウイルス対策ソフトウェア、スパイウェア検出／駆除ユーティリティ、コンテンツフィルタリング（スパム対策など）、ホストベースの侵入防止ソフトウェアなどである。フォレンジックデータを使用して感染しているホストを識別する方法は、ほかの方法よりも優れている場合がある。なぜなら、データがすでに収集されており、関係するデータをデータセット全体から抽出するだけで済むからである。

+ **動的識別** 動的識別の手法は、現在どのホストが感染しているのかを識別するのに使用する。感染が確認されたら速やかになんらかの動的なアプローチを使用し、ホストを対象とした封じ込めと根絶の措置を講じることができる。たとえば、駆除ユーティリティを実行する、パッチやウイルス対策の更新を配備する、感染しているシステムのためのVLANにホストを移動する、などを実行できる。動的なアプローチは組み合わせて利用することが最善である。なぜなら、個々のアプローチは特定のホストにおける特定種類の感染の検索にのみ役立つからである。

+ **手動識別** 手動識別は3つの手段のうち最も労力を要する方法だが、感染しているホストを確実に識別するために必要な措置となる場合が多い。ユーザまたはITスタッフは、マルウェアや感染の兆候に関する情報のほか、ウイルス対策ソフトウェア、OSやアプリケーションのパッチ、あるいはスキャンツールを駆使して、感染を特定する。組織では、重大なマルウェアインシデントの発生時に支援を担当するスタッフを事前に任命しておき、必要なマニュアルを提供して、考えられる支援作業について定期的にトレーニングするべきである。

5.4.3. 根絶と復旧

ウイルス対策ソフトウェアとスパイウェア駆除ソフトは悪意のコードの感染を効果的に見つけて削除する。しかし、感染したファイルのなかにはウイルスを除去することができないものもある。(ファイルは、クリーンなバックアップコピーを使って削除・置き換え可能である。アプリケーションの場合は、感染したアプリケーションを再インストールする。)悪意のコードによりアタッカーがrootレベルでアクセス可能だった場合は、アタッカーがほかにどんな行動をしたか判断できない可能性がある[104]。そのような場合、システムは以前の感染していないバックアップからリストアするか、一から再構築する。システムの損害の程度や、システムへの不正なアクセスの程度がはっきりしない場合は、システムの再構築を検討すべきである。[105] その後システムの安全を強化し、システムが同じ悪意のコードに二度と感染しないようにする。

5.5. 悪意のコードによる事件の処理のためのチェックリスト

表5-3のチェックリストは、悪意のコードによる事件の処理で実施する主なステップを示すものである。このチェックリストは、表3-8の最初の事件処理チェックリストの続きである。各ステップの正確な順番は、各事件の性質や、組織が事件を封じ込めるために選んだ戦略によって変わってくる点に注意すること。

104 セクション6では、root奪取の処理と復旧の手引きについて説明する。

105 マルウェアインシデント発生後のシステムの復旧に関する詳細は、NIST SP 800-83 『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(Guide to Malware Incident Prevention and Handling)』を参照のこと。

表5-3 悪意のコードによる事件の処理のチェックリスト

	活動	完了
	検知と分析	
1.	ビジネスインパクトに基づき事件の処理に優先順位を付ける。	
1.1	どのリソースが影響を受けたかを確認し、将来どのリソースが影響を受けるかを予測する。	
1.2	事件の現在および将来的な技術的影響を見積もる。	
1.3	技術的な影響と影響を受けるリソースに基づき、優先順位マトリックスで適切なセル(1つまたは複数)を見つける。	
2.	適切な内部の人間または外部組織に事件について報告する。	
	封じ込め、根絶、復旧	
3.	事件を封じ込める。	
3.1	感染したシステムを判別する。	
3.2	感染したシステムをネットワークから切断する。	
3.3	悪意のコードに利用された脆弱性を修正する。	
3.4	必要なら、悪意のコードの転送メカニズムをブロックする。	
4.	事件を根絶する。	
4.1	感染したファイルのウイルスを除去、隔離、削除、置換する。	
4.2	組織内のほかのホストについて、悪用された脆弱性を修正する。	
5.	事件から復旧する。	
5.1	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。	
5.2	必要なら、将来の関連する活動を見つけるため、追加の監視を実施する。	
	事後活動	
6.	追跡レポートを作成する。	
7.	反省会を開催する。	

5.6. 推奨事項

このセクションで説明した、悪意のコードによる事件の処理に関する主な推奨事項を、以下に要約する。

+ **悪意のコードの問題について、ユーザに自覚させる** ユーザは、悪意のコードが増殖するために使用する手法や感染の症状について精通すること。定期的にユーザ教育セッションを開催することは、悪意のコードがもたらすリスクについて、ユーザに自覚させるのに役立つ。電子メールの添付ファイルの安全な取り扱い方法を教育することで、感染の発生を減らすことができる。

+ **ウイルス対策ソフトウェアベンダーの広報を読む** 新種の悪意のコードの脅威に関する公

開情報は、事件処理担当者に対してタイムリーな情報となる。

+ **重要なホストには、ホスト型のIDPS(ファイル完全性チェッカーを含む)を配備する** ホスト型のIDPS、特にファイル完全性チェッカーは、設定の変更や、システムの実行ファイルの改ざんなど、悪意のコードの事件を検知することができる。

+ **ウイルス対策ソフトウェアを使用し、最新のウイルスシグネチャを使って最新に保つ** ウイルス対策ソフトウェアは、悪意のコードを転送する可能性があるすべてのホストとアプリケーションに配備する。ウイルス対策ソフトウェアは、悪意のコードの感染を検知、除去、隔離するように設定する。すべてのウイルス対策ソフトウェアは、新しい脅威も検知できるよう、最新のウイルスシグネチャを使って最新に保つようにする。

+ **疑いのあるファイルをブロックするようにソフトウェアを設定する** 悪意がある可能性が非常に高いファイルは、外部から入ってくるのをブロックすべきである。これには、たいてい悪意のコードに関連するファイル拡張子や、ファイルの拡張子の疑わしい組み合わせのファイルが含まれる。

+ **開かれているWindowsの共有を解除する** 多くのワームは、Windowsを実行しているホストの安全でない共有を通じて広まる。1台でも感染すると、安全でない共有を通じて、数百から数千ものホストに瞬く間に感染する可能性がある。

+ **悪意のコードによる事件は、できるだけ早く封じ込める** 悪意のコードはひそかに活動し、ほかのシステムに急速に増殖する可能性があるため、感染が拡大してより大きな被害を与える前に、事件を早期に封じ込める必要がある。感染したシステムは、すぐにネットワークから切断すべきである。電子メールを媒介とした悪意のコードによる事件を掌握するため、電子メールサーバレベルでブロックするか、または、一時的に電子メールサービスを中断しなくてはならない場合もある。

6. 不正アクセス事件の処理

6.1. 事件の定義と例

「不正アクセス」事件は、ユーザがアクセスを許されていないリソースへのアクセスを得ることによって起こる。不正なアクセスを得る方法としては、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の悪用や、ユーザ名とパスワードの入手、ソーシャルエンジニアリングなどがある。アタッカーは1つの脆弱性を通じて限られたアクセスを取得し、そのアクセスを使ってほかの脆弱性を攻撃し、最終的により高いレベルのアクセスを取得する。不正アクセスの例としては、次のものがある。

+ 電子メールサーバのリモートroot権限を奪取する
+ ウェブサーバの書き換え
+ パスワードの予測とクラッキング
+ 給与支払い記録や医療情報、およびクレジットカード番号といった機密データを、許可なく参照またはコピーする
+ ユーザ名やパスワードをキャプチャするため、ワークステーションでパケットスニッファを実行
+ 匿名FTPサーバのパーミッションエラーを使って、海賊版のソフトウェアや音楽ファイルを配布
+ 安全でないモデムにダイヤルし、内部ネットワークにアクセス
+ 幹部のふりをしてヘルプデスクに電話し、幹部の電子メールパスワードをリセットして、新しいパスワードを知る
+ ログイン中のまま放置されているワークステーションを許可なく使う

6.2. 準備

このセクションでは、不正アクセス事件の処理に備え、事件を予防するための手引きを示す。

6.2.1. 事件処理の準備

セクション3.1.1と3.2.3で説明した一般的な手引きに加え、不正アクセス事件の処理に備える際には以下に示すようなその他の内容も実行する。

+ 不正アクセスを得ようとする試みを検知して警告するように、ネットワーク型およびホスト型のIDPS(ファイル完全性チェッカーやログモニターなど)を設定する。
+ 一元化したログサーバを使用し、組織全体のホストからの関連情報を単一の安全な場所に保管する。
+ パスワード漏洩などの場合に、アプリケーション、システム、管理ドメイン、又は組織の全ユーザがパスワードを変更しなくてはならなくなった場合の手順を確立する。この手順は組織のパスワードポリシーに準拠すること。
+ 不正アクセス事件についてシステム管理者と話し合い、事件処理プロセスにおける彼らの役割を理解させる。

6.2.2. 事件の予防

セクション3.1.2で説明した、事件の予防に関する一般的な手引きを適用すれば、不正アクセス事件の数は確実に減る。強固で何層にも重ねた防御戦略を採用し、許可のないユーザと不正に利用しようとしているリソースの間に何層にもセキュリティレイヤーを設けるのが、事件を減らすために推奨される方法である。表6-1に、階層化した防御戦略を支えるステップを示す。[106]

表6-1 不正アクセス事件を予防するための活動

分類	具体的な活動
ネットワークセキュリティ	• ネットワーク境界で、明示的に許可されていないすべての受信トラフィックを拒否するように設定する。 • モデムやVPNを含むすべてのリモートアクセス手段のセキュリティを適切に高める。モデムが安全でないと、内部のシステムやネットワークへの不正アクセスを簡単に許してしまう。セキュリティが適切でないモデムを見つけるには、ウォーダイヤリングが最も効率がよい方法である[107]。リモートアクセスのセキュリティを高める際には、クライアントの信用性を慎重に検討する。クライアントが組織の管理対象外である場合は、できるだけ少ないリソースへのアクセスを提供し、その行動をしっかりと監視すること。 • 公にアクセス可能なサービスは、安全な非武装地帯(DMZ)ネットワークセグメントに置く。こうすることで、外部ホストはDMZのホストだけにコネクションを確立でき、内部セグメントのホストにはコネクションを確立できないように、ネットワーク境界を設定することができる。 • 内部ネットワークのすべてのホストでプライベートIPアドレスを使用する。これにより、アタッカーによる内部ホストへの直接の接続確立が非常に制限される。
ホストのセキュリティ	• 定期的に脆弱性評価を行い、重大なリスクを見つけて、リスクを許容できるレベルまで軽減する。 • ホストの不必要なサービスをすべて無効にする。重要なサービスは分離し、別のホストで実行する。これによりアタッカーが重要なサービスが動作しているホストに侵入しても、すぐにアクセスできるのは1つのサービスだけであり、他のサービスに影響が及ばなくなる。 • サービスは最低限の権限で動作させ、エクスプロイトに成功した場合の影響を少なくする。 • ホスト型のファイアウォールソフトウェア／パーソナルファイアウォールソフトウェアを使用して、各ホストが攻撃にさらされないようにする。 • ホストのアイドル画面を自動的にロックし、オフィスを離れる場合にはログアウトするようにユーザを指導することで、ログイン中のシステムに対する不正な物理的アクセスを制限する。 • パスワードファイル、機密データベース、公開ウェブページなどの重要なリソースに対するパーミッションの設定を定期的に検証する。パーミッションの変更を定期的に報告できるよう、このプロセスは簡単に自動化することができる。
認証と承認	• パスワードポリシーを作成する。その中で、複雑で予測しにくいパスワードを使用することを義務付け、パスワードの共有を禁止し、異なるシステム(特に外部のホストやアプリケーション)では別のパスワードを使用するように指示する。

106 ワイヤレスセキュリティに関する奨励事項は、NIST SP 800-97 『無線ロバストセキュリティネットワークの確立 (Establishing Wireless Robust Security Networks)』とWireless Network Security for IEEE 802.11a/b/g and Bluetoothを参照のこと。これらのドキュメントは、http://csrc.nist.gov/publications/PubsSPs.htmlから入手可能である。NIST SP 800-97は、IEEE 802.11i および NIST SP 800-48 Revision 1 (DRAFT)に対するガイドでもある。

107 ウォーダイヤリングは、ある範囲の電話番号にダイヤルして、待ち受けているモデムを見つけ、モデムが接続されているホストへのアクセスを試みるプロセスである。モデムの普及率はピーク時に比べて大幅に減少しているが、現在でも特定の機能を果たすために、モデムを使用している組織は多い。

	・特に重要なリソースに対しては、十分強力な認証を使用する。 ・ソフトウェアの評価や開発を行う際に職員と契約業者が従うべき、認証と承認の標準を作成する。たとえば、パスワードを転送または保管する場合は、FIPS 140-2で検証済みのアルゴリズムを使用して強力に暗号化する。 ・ユーザアカウントの作成と取り消しのための手順を確立する。これには、新しいアカウント要求に対する承認プロセスと、不要になったアカウントを定期的に無効または削除するプロセスも含む。
物理的なセキュリティ	・重要なリソースへのアクセスを制限する、物理的なセキュリティ対策を実施する。

6.3. 検知と分析

不正アクセス事件はさまざまな形で起こるため、事件を検知するための前兆や兆候は、数十種類に及ぶ。表6-2の「不正アクセスの前兆」では、考えられる不正アクセス攻撃の前兆の一覧を挙げ、そのような活動がなぜ行われるかを説明し、その後の事件の発生を予防するために推奨される対応を説明する。表6-3「不正アクセスの兆候」では、root奪取、データの改ざん、不正なアカウントの利用といった、悪意のある活動の一覧を示す。各活動に対し、その活動の考えられる兆候も挙げる。組織は、これらの表を手軽にカスタマイズして、環境特有の前兆や兆候を追加してかまわない。それがより効率的で効果的な事件処理プロセスを促進する。

表6-2 不正アクセスの前兆

前兆	対応
不正アクセス事件の前には、ホストとサービスをマッピングさせ、脆弱性を見つけるための偵察活動が行われることが多い。活動にはポートスキャン、ホストスキャン、脆弱性スキャン、ping、 traceroute、DNSゾーン転送、OSフィンガープリンティング、バナー取得などが含まれる。このような活動はまずIDPSで検知され、次にログ分析で発見される。	事件処理担当者は、偵察パターンのはっきりした変化を探すこと。たとえば、突然特定のポート番号やホストに対する偵察が激しくなったなど。この活動により悪用される可能性がある脆弱性を見つけた場合、組織には脆弱性に対処して将来の攻撃をブロックするだけの時間が与えられる(たとえば、ホストへのパッチ適用、使用していないサービスの停止、ファイアウォールルールの変更など)。
不正なアクセスを取得するための新しいエクスプロイトが公にリリースされ、それが組織に対して大きな脅威になる。	新しいエクスプロイトを調査し、可能な場合はセキュリティコントロールを変更して、そのエクスプロイトが組織に及ぼす可能性がある影響を最小限にする。
ソーシャルエンジニアリングを受けた可能性があるとのユーザからの報告。ソーシャルエンジニアリングとは、アタッカーがユーザから巧みにパスワードなどの機密情報を聞き出したり、プログラムや添付ファイルをダウンロードまたは実行させようとする行為である。	インシデント対応チームは、ユーザへの広報を行い、ソーシャルエンジニアリングへの対処法について指導する。また、アタッカーがどのリリースに興味を持っているかを特定し、対応するログベースの前兆を探す。ソーシャルエンジニアリングは偵察活動の単なる一部に過ぎないためである。
人間またはシステムが物理的なアクセスの試みの失敗に気づく(たとえば、部外者が鍵のかかった配線室のドアを開けようとする、だれかが現在使用されていないIDバッジを使用するなど)。	可能なら、警備員がその者を引き留める。また、その者の活動の目的を特定し、現在の物理的セキュリティコントロールおよびコンピュータのセキュリティコントロールが、そのような脅威をブロックするのに十分強力であるかどうかを確認する(物理的なアクセスに失敗したアタッカーが、代わりにリモートコンピューティングベースの攻撃を仕掛けてくる可能性がある)。必要なら、物理的セキュリティコントロールおよびコンピュータのセキュリティコントロールを強化する。

表6-3 不正アクセスの兆候

悪意のある活動	予想される兆候
ホストのroot奪取	・不正なセキュリティ関連のツールやエクスプロイトの存在 ・ホストへまたはホストからの異常なトラフィック(アタッカーがそのホストを使用してほかのシステムを攻撃する可能性がある)が見つかる ・システム設定の変更。以下のもの含まれる。 ◦ プロセス/サービスの変更や追加 ◦ 予期しない開かれたポート ◦ システム状態の変更(再起動、シャットダウン) ◦ ログや監査ポリシーおよび監査データへの変更 ◦ ネットワークインタフェースカードがプロミスキャスモードに設定されている(パケットスニッフィング) ◦ 新しい管理レベルのユーザアカウントまたはグループ ・重要なファイル(実行可能プログラム、OSカーネル、システムライブラリ、設定ファイルおよびデータファイルなど)の内容、タイムスタンプ、特権が変更される ・アカウントが不正に使用されている(たとえば、だれも使っていないアカウントの利用、複数の場所からのアカウントの同時使用、特定のユーザからの予期しないコマンド、多数のロックアウトされたアカウント) ・期待されるリソース使用率に大きな変化(たとえばCPU、ネットワーク活動、全ログ、ファイルシステムなど)が見られる ・システムが利用できないというユーザからの報告を受ける ・侵入を検知したネットワークとホストの侵入検知装置が警報を発する ・異常な名前の新しいファイルやディレクトリ(たとえばバイナリ文字、先頭にスペースがある、先頭にドットがあるなど)が見つかる ・オペレーティングシステムやアプリケーションのログにきわめて異常なメッセージが記録される ・ホストに侵入したとのアタッカーからの連絡を受ける
データの不正改ざん(たとえば、ウェブサーバの書き換え、FTP warezサーバ[108])など)	・侵入を検知したネットワークとホストの侵入検知装置が警報を発する ・リソース使用率が増加する ・データ変更に関するユーザの報告を受ける(たとえば書き換えられたウェブページなど) ・重要なファイル(ウェブページなど)が変更される ・異常な名前の新しいファイルやディレクトリ(たとえばバイナリ文字、先頭にスペースがある、先頭にドットがあるなど)が見つかる

108 「warezサーバ」とは、違法なファイルを配布するために使用されるファイルサーバである。元々「warez」とは海賊版のソフトウェアを指すが、現在では、著作権のある音楽や動画のコピーなど、その他の違法なファイルも含まれるようになった。アタッカーは、FTPサーバをwarezファイルの配布に利用するために、サーバの脆弱性を突いて不正アクセスを行う。

	・期待されるリソース使用率に大きな変化(たとえばCPU、ネットワーク活動、全ログ、ファイルシステムなど)が見られる
標準ユーザアカウントの不正使用	・重要なファイル(パスワードファイルなど)がアクセスされる ・アカウントが不明に使用されている(たとえば、だれも使っていないアカウントの利用、複数の場所からのアカウントの同時使用、特定のユーザからの予期しないコマンド、多数のロックアウトされたアカウント) ・ウェブプロキシのログに、ハッカーツールのダウンロードに関する兆候が記録される
物理的な侵入者	・ネットワークやシステムが利用できないというユーザからの報告を受ける ・システム状態が変更される(再起動、シャットダウン) ・ハードウェアが完全にまたは部分的に喪失する(システムが開けられ、特定の部品が取り出された) ・不正な新しいハードウェア(たとえばアタッカーがネットワークにパケットスニッフィング用のラップトップを接続したり、ホストにモデムを接続した)が見つかる
不正なデータアクセス(たとえば、顧客情報データベース、パスワードファイルなど)	・FTP、HTTP等のプロトコルを使ったデータへのアクセスの試みを検知した侵入検知装置が警報を発する ・ホストが重要なファイルに対するアクセスの試みを記録する

不正アクセス事件は、いくつものステップで起きる傾向があるという点で、ほかのタイプの事件とは違う。一般にアタッカーは、ホストの特定、オペレーティングシステムの特定、各ホストが実行しているサービスやアプリケーションの特定等、ネットワークをマッピングするための複数の偵察活動を行い、リモートから悪用できそうな脆弱性を発見する。偵察は非常にありふれたものになってきたため、時間とリソースの制限から無視されることも多い。しかし、少なくとも最低限の偵察活動のレビューを実施し、自分たちが現在直面しているリスクの感覚を得るのが大切である。

偵察ステップが終わると、アタッカーはシステムへの不正アクセスを得るための活動を開始する。第一ステップで特権アクセスが得られる脆弱性も多いが、ユーザレベルのアクセスしか得られない脆弱性もある。最終的に、ほとんどのアタッカーはシステムの管理者レベルでのアクセスを得ようとする。そのため、まず特権アクセスが得られる脆弱性を探す。そのような脆弱性が見つからなかったり、悪用に成功しなかった場合は、アタッカーはユーザレベルのアクセスを許す脆弱性を探し、アクセスレベルを高めるためにさらなる攻撃を実行する。このプロセスにはかなりの時間がかかる可能性があるため、途中のステップで、つまりあるアクセスは得たもののさらなるアクセスを追求中に攻撃が検知される場合もある。インシデント対応チームは、完全な管理者権限のアクセスが取得される前に検知、確認、阻止するよう努力しなければならない。アタッカーは、管理者レベルのアクセスを得ると、ルートキットをインストールして、バックドアを仕掛け、将来リモートから管理者の権限でシステムにアクセスできるようにする可能性が高い。

不正アクセス事件では、悪意のない活動と悪意のある活動を見分けるのが難しい場合がある。システムのシャットダウン、監査設定の変更、実行可能ファイルの変更などは、攻撃ではなく、日

常的なシステム管理でも行われる可能性がある。活動元を特定するための鍵が、組織の変更管理プロセスである。オペレーティングシステムのアップグレードなど、システムの保守が予定されている場合は、この情報を、前兆と兆候を監視し分析するスタッフ(外部委託先や請負作業者を含む)に提供する。疑いのある兆候が検知されたら、分析者はすぐにそれが計画された保守活動によるものであるかどうかを確認する。変更管理プロセスに必要な情報が正しく捕捉されていないと、事件処理担当者はシステム管理者に連絡して、その活動を行ったかどうか確認しなくてはならない。システム管理者に連絡がつく頃には、悪意のある行動は完全なroot奪取にエスカレートする可能性がある。

事件に優先順位を付ける際には、現在および将来予想される事件の影響を判断しなければならないが、不正アクセスではこの判断がが非常に難しい。アタッカーはみなユーザレベルのアクセス権を管理者レベルのアクセスにエスカレートさせようと考えるため、現在起きている事件も最終的にrootレベルアクセスになる可能性がある。現在の事件の影響の特定には、大規模な分析が必要となる場合があるが、事件の優先順位付けは、そのような分析が完了する前に行わなければならない場合がある。従って不正アクセス事件の場合、何もしなければ影響はますます大きくなるという前提で、現在の影響の見積りに基づいて優先順位を付けるのが最善である。次に、許可なくアクセスされたリソースの重要度ごとに、それぞれの影響の分類に応じて対応期限を割り当てる。

6.4. 封じ込め、根絶、復旧

セクション3.3で説明した一般的な手引きに加え、このセクションでは、不正アクセス事件の封じ込めと証拠の収集・処理を行うための、具体的な推奨事項を説明する。

6.4.1. 封じ込め戦略の選択

不正アクセス事件を封じ込めようとする場合、応答時間がきわめて重要である。何が起きたかを正確に決定するには、広範な分析が必要かもしれないが、積極的な攻撃の場合は、事態は急速に変化する。ほとんどの場合、初期分析を行って事件に優先順位を付け、初期の封じ込め策を実施してから、さらなる分析を行って封じ込め策が十分かどうかを判断することが推奨される。たとえば、アタッカーが特定のシステムのパスワードファイルをコピーしたかどうかはすぐにはわからない場合がある。パスワードがこのシステムに固有のものだと仮定すると、事件処理担当者がパスワードファイルが漏洩されたかどうかを確認するまでシステムをネットワークから切断することで、アタッカーがこれらのパスワードを使用するのを防ぐことができる。しかし、ほとんどの環境では、パスワードはシステムに固有のものではない。システムとユーザの間には、妙な信頼関係があり、ユーザは多くのシステムに対して、同じ、または類似したパスワードを使用することが多い。このため盗まれたパスワードは、盗んだシステムとは別のシステムへのアクセスにも使われることが多い。事件は、数分以内に単一のホストから数十ものホストに広まるのである。

事件処理担当者は、封じ込め戦略を選ぶ際、紙一重の判断を迫られることもある。事件処理担当者が最悪の事態を想定した場合、すべてのネットワークとシステムを停止することになるかもしれないからである。事件処理担当者は、稼働環境全体を何日間にもわたって停止させるのではなく、リスクを実際的なレベルまで軽減することに重点を置いた、より穏当な対策を考えるべきである(もちろん、悪意のある活動の程度が非常に大きく、完全な停止に値するのなら別である)。不正アクセス事件の初期および最終的な封じ込めでは、以下の行動の適切な組み合わせが効果的である。

+ **影響のあるシステムを隔離する** これが不正アクセス事件を封じ込めるための最も簡単な方法である。影響を受けたシステムをネットワークから切断する。これにより、影響を受けたシステムは、それ以上の侵入を受けなくなる。しかし、影響を受けたシステムをすべて特定するのは難しい。アタッカーは、侵入した1台のシステムを、内部のほかのシステムに対する攻撃元として使用することが多い。処理担当者は、ほかのシステムの攻撃成功

の兆候を調べ、それらの要素も同様に封じ込めなくてはならない。多数のシステムを確認しなくてはならない場合は、バックドアのポートスキャンなど、自動化された方法を使用することもできる。

+ **影響を受けたサービスを無効にする**　アタッカーが特定のサービスを使用して不正アクセスを得ている場合、一次的または恒久的なサービスの無効化も事件の封じ込めのひとつである。たとえば、アタッカーがFTPの脆弱性を悪用しており、不正アクセスがFTPのデータファイルに限られる場合は、一時的にFTPサービスを止めれば事件を封じ込めることができる。サーバがFTPを実行している場合は、永久にFTPを無効にする。

+ **アタッカーの侵入ルートを除去する**　可能なら、許可されたユーザへのサービスの中断を最小化しつつ、次のターゲットになりそうな近くのリソースにアタッカーがアクセスできないようにする。例としては、特定のネットワークセグメントに対する受信方向のコネクションを一時的にブロックしたり、リモートアクセスサーバを切断したりすることが挙げられる。

+ **攻撃で使用された可能性があるユーザアカウントを無効にする**　1台のシステムから入手したアカウントとパスワードが、ほかのシステムでも使える可能性があるため、そのアカウントは組織全体で無効にしなくてはならない。また、アタッカーが作成した可能性がある新しいユーザアカウントも探す。各アカウントは、アタッカーが何を実行したかを処理担当者が確認するまでは、単にパスワードを変更するのではなく、無効にすべきである。

+ **物理的なセキュリティ対策の強化**　不正アクセス事件が物理セキュリティ違反にかかわる場合は、さらなる封じ込め戦略も実行する。たとえば、部外者がサーバルームにアクセスしたことが疑われる場合は、サーバルームのセキュリティを強化するだけでなく、警備員か法執行機関が設備を捜索して、侵入者がもうそこにいないことを確認すべきである。その他のセキュリティ変更も有効である。一度アタッカーがセキュリティを破ることができたということは、再び破られる可能性があるということである。

6.4.2. 証拠の収集と処理

システムへの不正なアクセスがあったと疑われる場合、処理担当者はシステムの完全なバックアップイメージを作成する。ホストとアプリケーションのログ、侵入検知警報、ファイアウォールのログなど、関連するほかのデータからも、不正アクセスの相関的な証拠が得られる可能性がある。事件の最中に物理的なセキュリティ違反が起きた場合は、物理的なセキュリティシステムのログ、監視カメラのテープ、目撃者の証言などからも追加の証拠が得られる場合がある。不正アクセス事件は、ほかの事件よりも告訴に結びつく可能性が高いため、確立された証拠収集および処理手順に従い、法執行機関に参加してもらう価値があるような状況であれば、法執行機関に連絡する。

6.4.3. 根絶と復旧

不正アクセスに成功したアタッカーはルートキットをインストールすることが多い。これは、システムのバイナリなどのファイルを改ざんまたは置き換えるものである。ルートキットは実行形跡の多くを隠し、何が変わったかを見つけにくいようにしている[109]。よって、アタッカーがシステムへのrootアクセスを取得したと思われる場合は、処理担当者はOSを信用してはならない。一般に最良の対策は、正しいことがわかっているバックアップからシステムをリストアするか、オペレーティングシステムとアプリケーションを一から再インストールし、システムを適切に強化

109 chkrootkit (http://www.chkrootkit.org/)のようなツールは、ルートキットがシステムにインストールされているかどうかを判断するのに便利である。

することである。システム及び被害を受けたシステムと信頼関係にあったすべてのシステムで、すべてのパスワードを変更することが強く推奨される。複数の脆弱性が悪用されるような不正アクセス事件もあるため、処理担当者は利用されたすべての脆弱性を見つけ、各脆弱性を修正または緩和するための戦略を決定することが大切である。存在するほかの脆弱性に対処しておかないと、アタッカーは今度はそれを利用する可能性がある。

アタッカーが管理者レベルよりも低いレベルのアクセスだけを取得した場合は、根絶と復旧作業は、アタッカーが取得したアクセスの程度に応じたものにする。アクセスを取得するのに利用された脆弱性には適切に対処する。弱点を体系的に見つけて対処するための追加の作業も当然実行する。たとえば、アタッカーが弱いパスワードを推測することでユーザレベルのアクセスを得た場合は、そのアカウントのパスワードをより強力なパスワードに変えるだけでなく、システム管理者やシステムオーナーは、より強力なパスワードの要件を強制することを検討すべきである。システムが組織のパスワードポリシーに準拠している場合は、組織のパスワードポリシーを見直すことも検討すべきである。

6.5. 不正アクセス事件を処理するためのチェックリスト

表6-4のチェックリストは、不正アクセス事件の処理で実施する主なステップを示すものである。このチェックリストは、表3-8の最初の事件処理チェックリストの続きである。各ステップの正確な順番は、各事件の性質や、組織が事件を封じ込めるために選んだ戦略によって変わってくる点に注意すること。

表6-4 不正アクセスによる事件の処理のチェックリスト

	活動	完了
	検知と分析	
1.	ビジネスインパクトに基づき、事件の処理に優先順位を付ける。	
1.1	どのリソースが影響を受けたかを確認し、将来どのリソースが影響を受けるかを予測する。	
1.2	事件の現在の技術的影響を見積もる。	
1.3	技術的な影響と影響を受けるリソースに基づき、優先順位マトリックスで適切なセル(1つまたは複数)を見つける。	
2.	適切な内部の人間または外部組織に事件について報告する。	
	封じ込め、根絶、復旧	
3.	事件の初期封じ込めを実施する。	
4.	証拠を取得、保全、確保、記録する。	
5.	事件の初期封じ込めを確認する。	
5.1	事件を詳しく分析し、封じ込めが十分かどうかを判断する(ほかのシステムでの侵入の兆候の確認も含む)。	
5.2	必要ならさらなる封じ込め対策を実施する。	
6.	事件を根絶する。	
6.1	悪用されたすべての脆弱性を見つけて修正する。	
6.2	事件の構成要素をシステムから取り除く。	

7.	事件から復旧する。	
7.1	影響を受けたシステムを運用可能な状態に戻す。	
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	必要なら、将来の関連する活動を見つけるため、追加の監視を実施する。	
事後活動		
8.	追跡レポートを作成する。	
9.	反省会を開催する。	

6.6. 推奨事項

このセクションで説明した、不正アクセス事件の処理に関する主な推奨事項を、以下に要約する。

+ **侵入検知ソフトウェアを設定して、不正なアクセスを取得しようという試みに対して警報を発生する** ネットワーク型およびホスト型の侵入検知ソフトウェア(ファイル完全性チェックソフトウェアを含む)は、不正なアクセスを取得しようとする試みを検知するのに有用である。各ソフトウェアは、ほかのソフトウェアが検知できない事件を検知することもある。よって、複数の種類のコンピュータセキュリティソフトウェアを利用することを強くお勧めする。

+ **すべてのホストに対して、ログの一元化のための設定を行う** 組織全体のすべてのホストからのデータが一元化された安全な場所に格納されていれば、事件はより簡単に検知できる。

+ **全ユーザにパスワードを変更させるための手順を確立する** パスワード漏洩により、アプリケーション、システム、管理ドメイン(または、おそらく組織全体)の全ユーザがパスワードを変更しなくてはならなくなる場合がある。

+ **ネットワーク境界で、明示的に許可されていないすべての受信トラフィックを拒否するように設定する** 入力トラフィックの種類を制限することで、アタッカーはより少ないターゲットにしか到達できなくなり、かつ、ターゲットに到達するために指定されたプロトコルしか使用できなくなる。これにより不正アクセス事件の数が減少する。

+ **モデムや仮想プライベートネットワーク(VPN)を含むすべてのリモートアクセス手段のセキュリティを高める** モデムが安全でないと、内部のシステムやネットワークへの不正アクセスを簡単に許してしまう。リモートアクセスクライアントは、組織の管理外であることが多いため、リソースへのアクセスを許すとリスクが増える。

+ **公にアクセスできるサービスは、安全な非武装地帯(DMZ)ネットワークセグメントに置く** これにより外部のホストはDMZセグメント上のホストにしかコネクションを開始できなくなり、内部ネットワークセグメントにはコネクションを開始できなくなる。これにより不正アクセス事件の数が減少する。

+ **ホスト上で不必要なサービスはすべて無効にし、重要なサービスは分離する** 動作しているあらゆるサービスが、侵入の機会を与える可能性がある。重要なサービスを分離することは大切である。なぜなら、重要なサービスが動作しているホストにアタッカーが侵入しても、すぐにアクセスできるのは、その1つのサービスだけであり、他のサービスに影響が及ばないからである。

+ **ホストベースのファイアウォールソフトウェアまたはパーソナルファイアウォールを使用して、各ホストが攻撃にさらされないようにする** 各ホストにホスト型のファイアウォールまたはパーソナルファイアウォールを配備し、明示的に許可されていないすべての活動を拒否するように設定することで、不正アクセス事件の可能性をさらに減らすことができる。

+ **パスワードポリシーの作成と実施** パスワードポリシーでは複雑で予測の難しいパスワードの使用を義務付け、重要なリソースにアクセスするための認証方法が十分強力であることを確認する。弱いパスワードやデフォルトのパスワードは予想またはクラックされる可能性が高く、不正アクセスにつながる。

+ **変更管理情報をインシデント対応チームに提供する** システムのシャットダウン、監査設定の変更、実行可能ファイルの変更などは、攻撃ではなく、日常的なシステム管理でも行われる可能性がある。このような兆候が検知された場合、チームは変更管理情報を使用して、兆候が許可された活動によるものかどうかを確認できるようにしておく必要がある。

+ **リスク軽減とサービス維持のバランスを考えた封じ込め戦略を選択する** 事件処理担当者は、影響を受けていないサービスを維持しつつ、リスクを業務上支障の少ないレベルまで軽減することに重点を置くような、穏当な封じ込め対策を検討すること。

+ **rootが奪取されたと思われるシステムはリストアまたは再インストールする** root奪取の影響は、完全に確認するのが難しいことが多い。rootが奪取されたと思われる場合は、システムを正しいことがわかっているバックアップからリストアするか、オペレーティングシステムとアプリケーションを再インストールする。また、その後事件が二度と起こらないように、システムを適切に強化する。

7. 不適切な使用による事件の処理

7.1. 事件の定義と例

「不適切な使用」の事件は、ユーザが適切なコンピュータの利用方針に違反した行動を取った場合に起きる。このような事件はセキュリティに関係しないこともあるが、その処理はセキュリティ関連の事件の処理と非常によく似ている。よって、インシデント対応チームが不適切な使用に関する多くの事件を処理するのが一般的になってきている。チームが処理する事件には、ユーザが以下のようなことをした場合が含まれる。

+ パスワードクラッキングツールやポルノ画像のダウンロード
+ 個人のビジネスを売り込むためのスパムの送信
+ 同僚をいやがらせる電子メールメッセージの送信
+ 組織のコンピュータ上に不正なウェブサイトを構築
+ 海賊版のファイルを取得または配布するための、ファイルまたは音楽共有サービスの利用
+ 組織内から外部への機密情報の送信

ある種の不適切な使用の事件では、外部の団体がターゲットになっており、より処理が難しいこともある。もちろんこれは責任問題に発展する。この問題が特に興味深い問題となっている理由としては、組織が実際の攻撃元ではない場合であっても、外部の団体から見ると、組織が彼らを攻撃しているように見えるという点である。処理担当者は迅速に活動を調べ、証拠を収集し、その活動が組織のネットワークまたはシステムから発生したものかどうかを確認すること。外部団体から指摘される不適切な使用の事件の例としては、次のものがある。

+ 内部のユーザが、ほかの組織の公開ウェブサイトを書き換えた。
+ 内部のユーザが、盗まれたクレジットカード番号を使ってオンラインの小売業者から品物を購入した。
+ サードパーティーがスパム電子メールを送っているが、そのメールの送信元アドレスが偽装されており、当組織に属するように見えるアドレスが使用された
+ サードパーティーが、ある組織に対してDoSを実行したが、その際、当組織に属するアドレスを送信元IPアドレスとして偽装したパケットが使用された。

7.2. 準備

このセクションでは、不適切な使用の事件の処理に備え、事件を予防するための手引きを示す。

7.2.1. 事件処理の準備

セクション3.1.1と3.2.3で説明した一般的な手引きに加え、不適切な使用による事件の処理に備える際には、以下に示すようなその他の内容も実行する。

+ 組織の人事部門と法務部門の担当者に会い、不適切な使用の事件の処理について話し合う。ユーザの活動の監視とログ取得は、組織のポリシーに準拠すること。また、インシデント対応チームは、直接職員に関係する事件処理の複雑さを理解する必要がある。たとえば、最初の兆候からはある職員がポルノ画像をダウンロードしているように見えても、さらに

分析すると、別のだれかがその職員のアカウントを使用しているということもある。インシデント対応手順には、慎重さと機密保持を盛り込む必要がある。

+ 物理セキュリティチームのメンバーに会って、内部ユーザとの交渉について話し合う。事件処理担当者は、自身の安全も考えなくてはならない。たとえば、ユーザが精神的に不安定だったり、非合法の活動をおこしていながら認めようとしなかったりする場合がある。そういったユーザと面談しようとしたり、ユーザのワークステーションを取得しようとすると、事件処理担当者に危険が生じる可能性がある。インシデント対応チームは、物理セキュリティチーム(および必要に応じて人事部門などのほかの部門)の助けを得て、そのような状況を扱うための手順を確立する。

+ 特に外部の団体をターゲットとした事件の責任問題について、広報部や法務部と話し合う。事件処理担当者は、攻撃されたと主張している団体と事件についていつ話し合い、どんな情報を公開すべきかについて理解することがきわめて重要である。

+ 以下のような特定の活動を検知するように、ネットワーク型のIDPS、電子メールコンテンツフィルタリングソフトウェア、および／または他のセキュリティ管理策を設定する。

  - ピアツーピアのファイル共有サービスや音楽共有サービスといった、不正なサービスの利用

  – スパム(たとえば、電子メールを中継しようとするなど)

  – 疑わしい単語(たとえば「機密」、性的にあからさまな用語など)をファイル名に使用した、すべてのファイル活動(たとえば電子メールの添付ファイル、FTPの転送、ウェブ要求)

  - 外部への偵察活動や攻撃

- FTPコマンド、ウェブ要求、電子メールヘッダーなど、ユーザの活動をログに保存する。これは、プロキシやアプリケーションのログ、またはネットワーク型のIDPSセンサーで実行できる。目的は、電子メールの本文や添付ファイルなどのデリケートな内容を保存することなく、そのような活動について基本的な情報をログに記録することである。プライバシーの問題と、調査や証拠目的で収集する情報の価値とのバランスを取る必要がある。

7.2.2. 事件の予防

一般的に、不適切な使用の事件の予防には、適切な行動に関するユーザの認識を高めるめること、ユーザに利用規定を読んで署名するように促すこと、彼らの行動が定期的に監視されていることを知らせること以外にできることはない。しかし、以下で推奨する活動は、特定の種類の不適切な使用の事件を減らすのに役立つ場合がある。

+ ピアツーピアのファイル共有や音楽共有サービスなど、組織のポリシーに違反するサービスの利用を防ぐよう、ファイアウォールや他のセキュリティ管理策を設定する。しかし、このようなサービスでは世界中で数百万のワークステーションが使用され、さまざまなポートが使われる可能性があるため、このトラフィックをブロックするのが適切でない場合がある。

+ 許可されていないメールの中継ができないよう、電子メールサーバを設定する。メールの

中継は、スパムの送信によく使われる方法である[110]。

+ すべての電子メールサーバにスパムフィルタリングソフトを実装する。これは、外部から送られてくるスパムの多くをブロックできるだけでなく、内部のユーザがスパムを送るのも防止できる。

+ URL (Uniform Resource Locator)フィルタリングを実装し、不適切なウェブサイトへのアクセスを防止する。これは、ユーザに使用を強制する場合にだけ有効である。これは、URLフィルタリングソフトウェアが動作するウェブプロキシサーバを設置し、すべての外向きのウェブ要求をプロキシサーバが行うように設定することで実施できる。ユーザが外部のウェブサイトにアクセスするには、プロキシサーバのどれかを通過しなければならない。

+ SSH(Secure Shell)、HTTPS (HTTP Secure)、IPsec (IP Security Protocol)といった、暗号化されたプロトコルを使った外向きのコネクションの制限を検討する。不必要な暗号化されたコネクションを使えば、ユーザはセキュリティコントロールが監視できない行動が取れるようになる。たとえば、ユーザは外部のサーバに対してSSH (Secure Shell)コネクションを確立し、違法なファイルをダウンロードすることができる。コネクションは暗号化されているため、ネットワークセキュリティコントロールはその活動の性質を判断できない。トラフィックを制限するために考えられる手段としては、ファイアウォールのルールセットやURLフィルタリング（たとえば、公開HTTPSプロキシサーバへのアクセスをブロックするなど)がある。

7.3. 検知と分析

不適切な使用の事件は、ユーザの画面で不適切な内容を見たとか、脅迫的な電子メールを受け取ったという、ユーザからの報告で検知されることがよくある。通常は、不適切な使用の前兆はない[111]。表7-1の「不適切な使用の兆候」では、許可されていないサービスの利用や不適切な内容へのアクセスといった行動と、それぞれの活動に対する考えられる兆候を挙げている。組織はこの表を手軽にカスタマイズして、環境特有の前兆や兆候を追加してかまわない。それがより効率的で効果的な事件処理プロセスを促進する。

110 Mail Abuse Prevention System (MAPS)のウェブサイト(http://www.mail-abuse.com/an_sec3rdparty.html)には、さまざまな電子メールプログラムが悪用されメールが中継されることを防ぐための、アドバイスが掲載されている。

111 例外としては、内部のユーザが外部のネットワークやホストを攻撃する前に偵察活動を行う場合がある。この場合、DoSまたは不正アクセス事件と同じ前兆がある。

表7-1 不適切な使用の兆候

不適切な行動	予想される兆候
不適切なサービスの利用(ウェブサーバ、ファイル共有、音楽共有など)	・ネットワーク侵入検知ソフトウェアやネットワーク行動分析ソフトウェアが警報を発する ・ホストが異常なトラフィックを送受信する ・ホストで新しいプロセス/ソフトウェアがインストールされ動作している ・異常な名前(たとえば「warez」サーバ式名前)を持つ新しいファイルやディレクトリが見つかる ・リソース使用率が増加する(CPU、ファイル記憶装置、ネットワーク活動など) ・ユーザからの報告を受ける ・アプリケーションのログエントリー(ウェブプロキシー、FTPサーバ、電子メールサーバなど)に異常が見つかる
不適切な内容へのアクセス(ポルノ画像のダウンロード、スパムの送信など)	・ネットワーク侵入検知が警報を発する ・ユーザからの報告を受ける ・アプリケーションのログエントリー(ウェブプロキシー、FTPサーバ、電子メールサーバなど) に異常が見つかる ・ワークステーション、サーバ、リムーバブル媒体上に不適切なファイルが存在する
外部の団体への攻撃	・ネットワーク侵入検知が警報を発する ・外部の団体からの報告を受ける ・ネットワーク、ホスト、アプリケーションのログエントリーに異常が見つかる[112]

インシデント対応チームは、明らかな事件とはみなされない不適切な使用の報告に対する支援対応について、慎重に行うべきである。たとえば、マネージャが、職員がコンピュータで長時間を浪費しているように見えるが、その職員が何をしているのかわからないと報告することがある。インシデント対応チームは、その職員のインターネットの利用を監視し、ハードディスクのファイルを分析するように頼まれることもある。しかし、しかるべきマネジメント層と人事担当者が書面で許可するまでは、そのような要望を支援すべきではない。

不適切な使用の事件を分析するのはたいてい簡単であるが、外部の団体から報告された事件は例外である。そのような事件を分析するための鍵は、組織が本当にその攻撃の元になっているのか、それとも偽装によってそのように見えるだけなのかを判断することである。ロギングが適切に行われており、優れたセキュリティコントロールがあれば、これは非常に簡単に判断できるはずである。たとえば、あらゆる外向きの通信がファイアウォールを通過するとして、ファイアウォールがすべてのコネクションおよびコネクションの試みをログに保存するように設定されていれば、すべての外向きの攻撃が記録されるはずである。組織の境界のセキュリティが弱いと、攻撃が組

112 前兆の例としては、送信元アドレスがねつ造されたバウンスメールに関する、電子メールサーバのログエントリーや、対応するSYNがないTCP RSTパケットに関するファイアウォールのログエントリー(すなわち、偽装されたパケットのbackscatter)がある。

織からのものなのかどうかを判断するのが難しくなる。なぜならばファイアウォールを迂回する別のルートを、アタッカーが利用することも可能であるからである。

事件の分析を複雑にしているもうひとつの要因が、現在あるデータをレビューしても、事件を起こしている人物を特定できない場合である。活動が続くようであれば、コンピューティングリソースや物理的なリソースの監視を強めることで、個人を特定しやすくなる。より困難な選択肢としては、疑いのある加害者の使用特性と目的のプロファイルを作成し、人事部門と連係して、プロファイルを膨らますという手法が挙げられる。この手法は、特定の場合にだけ有効である。予防のための監視は、だれが事件を起こしているかを特定するための、推奨される手段となる。これはまた、その行動が単発的なものであるか、意図的なものではないか、行動パターンの一部なのかを判断するのにも役立つ。

不適切な使用の事件は、一般に簡単に優先順位を付けることができる。犯罪が絡んでおらず、組織の評判に大きな傷が付かない限り、これらの事件をほかの事件と同じ緊急度で処理する必要はない。表7-2に不適切な使用の事件に対するマトリックス例を示す。セクション3.2.6で示したマトリックスとは構成が違っているが、どちらのマトリックスも事件のビジネスインパクトに基づいて対応に優先順位を付けている。表7-2では、(1)活動が犯罪かどうか、(2)組織の評判にどの程度傷がつくか、の2つの要因によってビジネスインパクトを定義している。犯罪活動の場合には、証拠収集の理由から、より素早い対応が必要となる。組織の評判に大きな傷が付くような事件は、少し、あるいはまったく傷が付かないような事件よりも、一般的に迅速に処理すべきである。

表7-2 不適切な使用の事件に対するサービスレベル合意の例

事件の現在の影響または将来予想される影響	事件の特性	
	犯罪活動	非犯罪活動
組織の評判に大きく傷が付く	15分以内に初期対応を開始 1時間以内に広報部、人事部、法務部、法執行機関に連絡	1時間以内に初期対応を開始 2時間以内に広報部、人事部に連絡
組織の評判に多少の傷が付く	2時間以内に初期対応を開始 4時間以内に人事部、法務部、法執行機関に連絡	4時間以内に初期対応を開始 8時間以内に人事部に連絡
組織の評判に傷が付かない	4時間以内に初期対応を開始 8時間以内に人事部、法務部、法執行機関に連絡	1日以内に初期対応を開始 2日以内に人事部に連絡

不適切な使用の事件に優先順位を付けるにあたっては、注意すべき点がが1つある。それは、不適切な使用の事件のうち、相当な数の事件が、ホストのroot奪取や悪意のコードの感染など、以前の事件に引き続いて起こる活動であるということである。セクション8では、2つ以上の事件を包含する事件の優先順位付けについて説明する。

7.4. 封じ込め、根絶、復旧

不適切な使用の事件では、好ましくないファイルを削除したり、許可されていないソフトウェアをアンインストールする以外は、一般に封じ込め、根絶、復旧活動は必要ない[113]。証拠収集は、

113 ユーザがほかの組織を攻撃している場合は例外である。この事件はできるだけ早く封じ込め、ほかのシステムへのさらなる被害を防ぎ、潜在的な責任を限定する。もうひとつの例外としては、インシデント対応チームが外部の組織に対して、その組織のホストに違法なファイルがあることを通知する場合がある。

不適切な使用の事件の多くにおいて重要である。証拠は個人を訴追したり懲戒処分にしたりする場合に必要であり、また、組織が活動の防止、検知、阻止に最善を尽くしたことを示すことで責任を限定するためにも必要である。内部のユーザは多数の設備に物理的にアクセスできることから、証拠の保管は特に重要である。証拠の改ざんや破壊に備え、組織の物理的なセキュリティスタッフとの連係が必要になる場合がある。

7.5. 不適切な使用の事件を処理するためのチェックリスト

表7-3のチェックリストは、不適切な使用の事件の処理で実施する主なステップを示すものである。このチェックリストは、表3-8の最初の事件処理チェックリストの続きである。各ステップの順序は、個々の事件の特性に応じて変わってくる点に注意すること。

表7-3 不適切な使用による事件の処理のチェックリスト

	活動	完了
	検知と分析	
1.	ビジネスインパクトに基づき事件の処理に優先順位を付ける。	
1.1	活動が犯罪的な性質のものであるか判断する。	
1.2	組織の評判にどれだけ傷が付くかを予測する。	
1.3	犯罪性と評判へのダメージに基づき、優先順位マトリックスで適切なセル(1つまたは複数)を見つける。	
2.	適切な内部の人間または外部組織に事件について報告する。	
	封じ込め、根絶、復旧	
3.	証拠を取得、保全、確保、記録する。	
4.	必要なら、事件の封じ込めと根絶を行う(不適切なファイルの削除など)	
	事後活動	
5.	追跡レポートを作成する。	
6.	反省会を開催する。	

7.6. 推奨事項

このセクションで説明した、不適切な使用の事件の処理に関する主な推奨事項を、以下に要約する。

+ **不適切な使用の事件の処理について、組織の人事部および法務部と話し合う** ユーザの活動を監視してログに記録するプロセスは、組織のポリシーと該当するすべての法律に準拠していなくてはならない。職員に直接かかわる事件処理手順には、慎重さと機密保持を盛り込むこと。

+ **責任問題について組織の法務部と話し合う** 不適切な使用の事件では、特に外部の団体がターゲットになっている場合に、責任問題が発生する可能性がある。事件処理担当者は、攻撃されたと主張している団体と事件についていつ話し合い、どんな情報を公開すべきかについて理解すること。

+ **特定の種類の不適切な使用を検知するように侵入検知ソフトウェアを設定する** 侵入検知ソフトウェアには、許可されていないサービスの利用、外向きの偵察活動や攻撃、不適切な電子メールの中継(スパムの送信)など、特定の不適切な使用の事件を検知するための機能が組み込まれている。

+ **ユーザの活動に関する基本的な情報をログに記録する** ユーザの活動に関する基本的な情報(たとえばFTPコマンド、ウェブ要求、電子メールヘッダーなど)は、調査および証拠として価値がある。

+ **すべての電子メールサーバを、不正なメール中継で利用できないように設定する** メールの中継は、スパムを送信するために使用されることが多い。

+ **すべての電子メールサーバでスパムフィルタリングを実行する** スパムフィルタリングソフトウェアは、外部から組織に送られたスパムと、内部のユーザが送ったスパムの両方について、その多くをブロックできる。

+ **URLフィルタリングソフトウェアを実行する** URLフィルタリングソフトウェアは、多くの不適切なウェブサイトへのアクセスを防ぐ。ユーザにはこのソフトウェアの使用を義務付ける必要がある。通常は、トラフィックがURLフィルタリングを実施しているサーバを通過しないと、外部のウェブサーバにアクセスできないように設定する。

8. 複合要素の事件の処理

8.1. 事件の定義と例

「複合要素の事件」とは、1つの事件で2つ以上の事件を包含しているものである。図8-1は、複合要素の事件に至るステップの例を示す。

1. 電子メールを通じて広まった悪意のコードが、内部のワークステーションに侵入する。
2. アタッカー(悪意のコードを送った者であるとは限らない)が感染したワークステーションを使って、ほかのワークステーションやサーバに侵入する。
3. アタッカー(ステップ1と2に関係した者であるとは限らない)が、侵入したホストのひとつを使用して、別の組織に対してDDoS攻撃を行う。

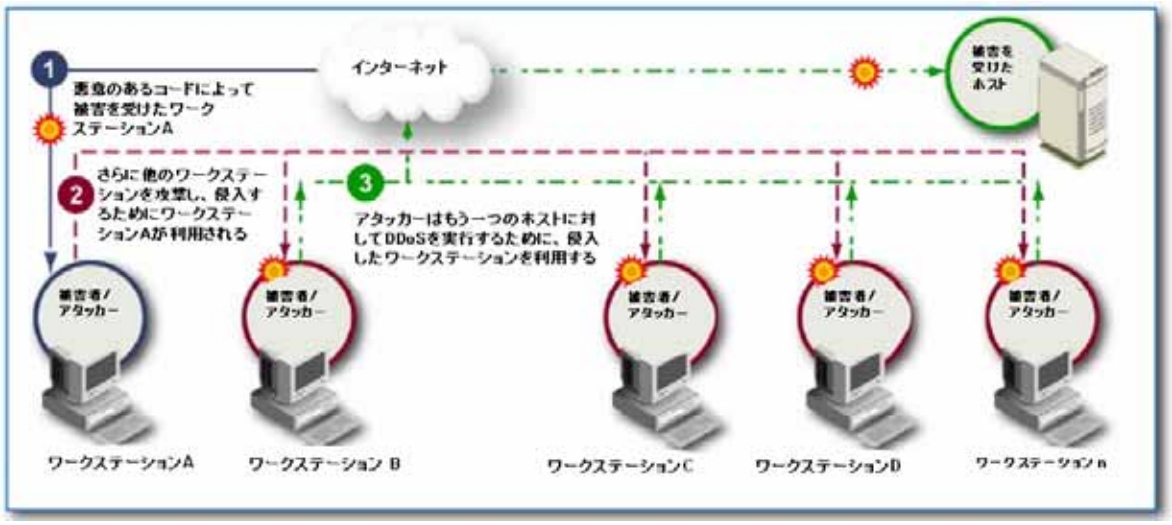

図8-1 複合要素の事件の例

この複合要素の事件は、悪意のコードの事件、いくつかの不正アクセス事件、DoS事件で構成される。DoS攻撃のターゲットからの苦情で組織が事件に気づく場合、不適切な使用の事件も起きている。例が示すように、複合要素の事件はいくつもの事件に関係し、さまざまな加害者によって実行される。そのため事件分析プロセスが複雑化している。

8.2. 準備、検知、分析

複合要素事件は、分析が難しいことが多い。事件処理担当者は、事件の一部についてだけは知っているかもしれないが、事件がいくつもの段階からなっているとは気づかない場合がある。また、仮に複数の事件に気づいていたとしても、それらが関係しているとはわからない場合もある。さらに分析を複雑にしているのは、事件の各ステージが数週間または数ヶ月間にわたって発生することがある点である。組織に優秀なログ取得プロセスとログアーカイブプロセスがないと、事件の以前のステージの証拠は消えてしまう。データがあったとしても、全データの中でどの兆候が関係しているのかを判断するのは、分析者にとって難題である。

複数の要素の事件を処理するための主な準備は、これまでに説明した各分類の事件のものと同じである。ほかの有用な活動としては、訓練の中で、複数の要素の事件に関するシナリオをレビューするというものがある。一元化したログと相関処理ソフトウェアの利用は、事件を効率よく分析するための手段としてこれまでも推奨してきたが、複合要素の事件の分析では前兆や兆候のソ

ースがいくつもあることが多いことから、これが非常に有効となる。すべての前兆や兆候に同じ観点からアクセスできれば、事件処理担当者は、複数の要素を持った事件をより早く診断できる。

8.3. 封じ込め、根絶、復旧

事件処理担当者は、事件のすべての要素をいち早く特定することに執着すべきではない。検知されるあらゆる事件が複数の要素の事件である可能性があるが、ある事件に1つの要素しかないと断定できるようになるには、長い時間がかかる場合がある。その間、最初の事件の封じ込めは完了しないままである。よって一般的には、最初の事件を封じ込めてからほかの要素の兆候を探すのがよい。経験のある処理担当者は、ほかの要素があるかどうかについて、経験に基づいて推測することがきる。多くの場合、不正アクセス事件には複数の要素がある可能性が高く、その他の種類の事件については複数の要素がある可能性は低いと考えてかまわない。

組織には、すべての要素を同時に処理するだけのリソースがないことが多いため、処理担当者は事件の複数の要素に気づいたら、各要素の処理に個別に優先順位を付けるべきである。すべての事件分類を扱った優先順位付けのガイドラインが作成されている場合は、処理担当者はそれぞれの要素に対する指定された対応期限を探し、最も緊急のものから処理することができる。ほかに考慮が必要な要因としては、各要素がどれだけ新しいかということがある。たとえば、現在起きているDoS攻撃は、6週間前に起きた悪意のコードの感染よりも、通常はより迅速に対処すべきである。さらに、ある1つの要素によってアタッカーがターゲットに到達するためのパスが作られた場合、処理担当者はその1つの要素を封じ込めることで、事件全体を封じ込めることができる(緊急ではないものの、ほかの要素も処理する必要がある点に注意すること)。ただし、アタッカーがすでにターゲットへの別のパスを作成または発見している可能性がある点に注意すること。

8.4. 複合要素の事件を処理するためのチェックリスト

表8-1のチェックリストは、複合要素の事件の処理で実施する主なステップを示すものである。このチェックリストは、表3-8の最初の事件処理チェックリストの続きである。各ステップの順番は、各事件の性質や、組織が事件を封じ込めるために選んだ戦略によって変わってくる点に注意すること。

表8-1 複合要素事件の処理のチェックリスト

	活動	完了
	検知と分析	
1.	ビジネスインパクトに基づき、事件の処理に優先順位を付ける。	
1.1	該当する事件分類のチェックリストのステップ1の指示に従う。	
1.2	事件の各要素について、適切な方針を決定する。	
2.	適切な内部の人間または外部組織に事件について報告する。	
	封じ込め、根絶、復旧	
3.	ステップ1の結果に基づき、各要素について、封じ込め、根絶、復旧のステップに従う。	
	事後活動	
4.	追跡レポートを作成する。	
5.	反省会を開催する。	

8.5. 推奨事項

このセクションで説明した、複合要素の事件の処理に関する主な推奨事項を、以下に要約する。

+ **一元化したログとイベント相関処理ソフトウェアを使用する** すべての前兆や兆候にある一つの観点からアクセスできれば、事件処理担当者は、複数の要素を持った事件をより早く見つけることができる。

+ **最初の事件を封じ込めてから、事件のほかの要素の兆候を探す** ある事件に1つの要素しかないと断定できるようになるには、長い時間がかかる場合がある。その間、最初の事件の封じ込めは完了しないままである。よって一般的には、まず最初の事件を封じ込めるのがよい。

+ **事件の各要素の処理に個別に優先順位を付ける** たいていの場合、組織のリソースは限られており、事件のすべての要素を同時に処理することはできない。各要素に対する対応ガイドラインと、各要素がどれだけ新しいかを踏まえた上で、各要素に優先順位を付けるべきである。

付録 A　推奨事項

付録Aには、このドキュメントのセクション2から8で説明した主な推奨事項を挙げる。推奨事項の最初のグループは、インシデント対応能力の編成に該当する。残りはインシデント対応ライフサイクルの各フェーズ(準備、検知と分析、封じ込め、根絶、復旧、事後活動)ごとにグループ化されている。各グループには、そのインシデント対応フェーズに対する一般的な推奨事項と、そのフェーズでの事件の特定のカテゴリ(たとえばサービス不能(DoSなど))に対する推奨事項が含まれている。

A.1　コンピュータセキュリティインシデント対応能力の組織化

+ **正式なインシデント対応能力を確立する 組織は、**コンピュータセキュリティの防御が破られた場合に迅速かつ効果的に対応できるよう、準備しておく必要がある。FISMAでは、政府機関がインシデント対応能力を確立することを義務付けている。

A.1.1　インシデント対応ポリシー、計画、および手順の作成

+ **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である。その中では、どの事象を事件と判断するかを定義し、インシデント対応の組織構造を確立し、役割と責任を定義し、事件報告の要件を明確にする。

+ **インシデント対応ポリシーをもとに、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、インシデント対応ポリシーにもとづきインシデント対応機能を実施するための、手引きを提供する。インシデント対応計画では、短期および長期の目標を設定し、計画を評価するためのマトリックスとともに明記する。また、事件処理担当者に対するトレーニングの頻度や、事件処理担当者に要求される事項も記載する。

+ **インシデント対応手順を作成する**　インシデント対応手順は、インシデント対応の詳細なステップを示すものである。この手順は、インシデント対応プロセスのすべてのフェーズを対象とする。インシデント対応手順は、インシデント対応ポリシーおよび計画にもとづくものとする。

+ **事件関連の情報共有に関するポリシーと手順を確立する**　組織は、マスコミ、法執行機関、インシデント対応組織といった、外部の関係者に事件の詳細について連絡しようと考える(またはそうしなくてはならない)場合がある。インシデント対応チームは、組織の広報部のスタッフ、法律アドバイザー、マネジメント層とこの要件について詳細に話し合い、情報共有に関するポリシーと手順を確立しておく必要がある。マスコミ等の外部関係者とやりとりする際には、組織の現行のポリシーに従う。

+ **適切な事件報告組織に、事件についての関係情報を提供する**　政府民間機関は、事件をUS-CERTに報告するよう義務付けられており、その他の組織は、US-CERTおよび／または他の事件報告組織に報告する。事件報告組織は、報告されたデータを使って、報告元の団体に対して新しい脅威や事件の動向に関する情報を提供するため、この報告は有益である。

A.1.2 インシデント対応チームの構成とサービス

+ **インシデント対応チームモデルを選ぶ際には、関係する要因を検討すること** とりうるチーム構成モデルと要員配置モデルのそれぞれの長所と短所について、組織の要件や利用できるリソースに照らし、慎重に検討すること。

+ **インシデント対応チームには適切なスキルをもった人間を選ぶこと** チームの信頼と熟達度は、メンバーの技術的なスキルによるところが大きい。技術的な判断が甘いと、チームの信用に傷が付き、事件が悪い方向に進んでしまうことがある。技術面での不可欠な技能には、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、侵入検知が含まれる。事件処理を効果的に行うためには、チームワークとコミュニケーション能力も必要である。

+ **事件処理に参加してもらう必要がある、組織内のほかのグループを明確にする** どのインシデント対応チームも、ほかのチームのノウハウ、判断、能力に頼ることになる。これには、マネジメント層、情報セキュリティ部門、ITサポート部門、法務部、広報部、設備管理部門が含まれる。

+ **チームが提供するサービスを決める** チームの主な業務はインシデント対応であるが、ほとんどのチームはその他の職務も行う。例としては、セキュリティアドバイザリの配布、脆弱性評価の実施、セキュリティに関するユーザ教育、侵入検知センサーの監視などがある。

A.2 準備

+ **事件処理で利用できそうなツールとリソースを入手する** さまざまなツールやリソースが利用できる状態になっていれば、チームはより効率的に事件を処理できる。例としては、連絡先一覧、暗号化ソフトウェア、ネットワーク図、バックアップ装置、コンピュータフォレンジックソフトウェア、ポートリスト、セキュリティパッチなどがある。

+ **ネットワーク、システム、アプリケーションを十分に安全な状態に保つことで、事件の発生を予防する** 事件の予防は組織にとって有益なだけでなく、インシデント対応チームの作業負荷も減らすことができる。定期的にリスクを評価し、見つかったリスクを許容できるレベルまで軽減することが、事件を減らす上で有効である。ユーザ、ITスタッフ、マネジメント層のセキュリティポリシーや手順に対する自覚も非常に大切である。

A.2.1 サービス不能事件

+ **ファイアウォールルールセットを設定して、リフレクタ攻撃を予防する** ほとんどのリフレクタ攻撃は、ネットワーク型およびホスト型のファイアウォールのルールセット使って、宛先ポートと送信元ポートの疑わしい組み合わせを拒否するように設定することで防ぐことができる。

+ **境界ルーターを設定してアンプ攻撃を防ぐ** 境界ルーターでディレクティッドブロードキャストを転送しないように設定することで、アンプ攻撃を防ぐことができる。

+ **組織のインターネットサービスプロバイダ(ISP)や二次プロバイダから、ネットワークベースのDoS攻撃の処理において、どういった支援が得られるのかを確認する** ISPは特定の種類のトラフィックをフィルタリングしたり、制限できることが多く、DoS攻撃を弱めたり停止したりできる場合がある。また、ISPがDoSトラフィックのログを提供したり、攻撃元の追跡を支援してくれる場合もある。事前にISPに確認して、このような支援を要請する

際の手順を確立しておくこと。

+ **セキュリティソフトウェアを設定し、DoS攻撃を検知する** IDPSは、多くの種類のDoS活動を検知できる。ネットワークやシステム活動の基準を確立し、基準からの大きなずれを監視することも、攻撃を検知する上で役立つ。

+ **ネットワーク境界で、明示的に許可されていないすべての送受信トラフィックを拒否するように設定する** 外部との間で出入りするトラフィックの種類を制限することで、アタッカーがDoS攻撃で使用する可能性のある手段を制限できる。

A.2.2 悪意のコードの事件

+ **悪意のコードの問題について、ユーザに自覚させる** ユーザは、悪意のコードが増殖するために使用する手法や感染の症状について精通すること。定期的にユーザ教育セッションを開催することは、悪意のコードがもたらすリスクについて、ユーザに自覚させるのに役立つ。電子メールの添付ファイルの安全な取り扱い方法を教育することで、感染の発生を減らすことができる。

+ **ウイルス対策ソフトウェアベンダーの広報を読む** 新種の悪意のコードの脅威に関する公開情報は、事件処理担当者に対してタイムリーな情報となる。

+ **重要なホストには、ホスト型のIDPS(ファイル完全性チェッカーを含む)を配備する** ホスト型のIDPS、特にファイル完全性チェッカーは、設定の変更や、システムの実行ファイルの改ざんなど、悪意のコードの事件を検知することができる。

+ **ウイルス対策ソフトウェアを使用し、最新のウイルスシグネチャを使って最新に保つ** ウイルス対策ソフトウェアは、悪意のコードを転送する可能性があるすべてのホストとアプリケーションに配備する。ウイルス対策ソフトウェアは、悪意のコードの感染を検知、除去、隔離するように設定する。すべてのウイルス対策ソフトウェアは、新しい脅威も検知できるよう、最新のウイルスシグネチャを使って最新に保つようにする。

+ **疑いのあるファイルをブロックするようにソフトウェアを設定する** 悪意がある可能性が非常に高いファイルは、外部から入ってくるのをブロックすべきである。これには、たいてい悪意のコードに関連するファイル拡張子や、ファイルの拡張子の疑わしい組み合わせのファイルが含まれる。

+ **開かれているWindowsの共有を解除する** 多くのワームは、Windowsを実行しているホストの安全でない共有を通じて広まる。1台でも感染すると、安全でない共有を通じて、数百から数千ものホストに瞬く間に感染する可能性がある。

A.2.3 不正アクセス事件

+ **侵入検知ソフトウェアを設定して、不正なアクセスを取得しようという試みに対して警報を発生する** ネットワーク型およびホスト型の侵入検知ソフトウェア(ファイル完全性チェックソフトウェアを含む)は、不正なアクセスを取得しようとする試みを検知するのに有用である。各ソフトウェアは、ほかのソフトウェアが検知できない事件を検知することもある。よって、複数の種類のコンピュータセキュリティソフトウェアを利用することを強くお勧めする。

+ **すべてのホストに対して、ログの一元化のための設定を行う** 組織全体のすべてのホストからのデータが一元化された安全な場所に格納されていれば、事件はより簡単に検知できる。

+ **全ユーザにパスワードを変更させるための手順を確立する** パスワード漏洩により、アプリケーション、システム、管理ドメイン(または、おそらく組織全体)の全ユーザがパスワードを変更しなくてはならなくなる場合がある。

+ **ネットワーク境界で、明示的に許可されていないすべての受信トラフィックを拒否するように設定する** 入力トラフィックの種類を制限することで、アタッカーはより少ないターゲットにしか到達できなくなり、かつ、ターゲットに到達するために指定されたプロトコルしか使用できなくなる。これにより不正アクセス事件の数が減少する。

+ **モデムや仮想プライベートネットワーク(VPN)を含むすべてのリモートアクセス手段のセキュリティを高める** モデムが安全でないと、内部のシステムやネットワークへの不正アクセスを簡単に許してしまう。リモートアクセスクライアントは、組織の管理外であることが多いため、リソースへのアクセスを許すとリスクが増える。

+ **公にアクセスできるサービスは、安全な非武装地帯(DMZ)ネットワークセグメントに置く** これにより外部のホストはDMZセグメント上のホストにしかコネクションを開始できなくなり、内部ネットワークセグメントにはコネクションを開始できなくなる。これにより不正アクセス事件の数が減少する。

+ **ホスト上で不必要なサービスはすべて無効にし、重要なサービスは分離する** 動作しているあらゆるサービスが、侵入の機会を与える可能性がある。重要なサービスを分離することは大切である。なぜなら、重要なサービスが動作しているホストにアタッカーが侵入しても、すぐにアクセスできるのは、その1つのサービスだけであり、他のサービスに影響が及ばないからである。

+ **ホストベースのファイアウォールソフトウェアまたはパーソナルファイアウォールを使用して、各ホストが攻撃にさらされないようにする** 各ホストにホスト型のファイアウォールまたはパーソナルファイアウォールを配備し、明示的に許可されていないすべての活動を拒否するように設定することで、不正アクセス事件の可能性をさらに減らすことができる。

+ **パスワードポリシーの作成と実施** パスワードポリシーでは複雑で予測の難しいパスワードの使用を義務付け、重要なリソースにアクセスするための認証方法が十分強力であることを確認する。弱いパスワードやデフォルトのパスワードは予想またはクラックされる可能性が高く、不正アクセスにつながる。

A.2.4 不適切な使用の事件

+ **不適切な使用の事件の処理について、組織の人事部および法務部と話し合う** ユーザの活動を監視してログに記録するプロセスは、組織のポリシーと該当するすべての法律に準拠していなくてはならない。職員に直接かかわる事件処理手順には、慎重さと機密保持を盛り込むこと。

+ **責任問題について組織の法務部と話し合う** 不適切な使用の事件では、特に外部の団体がターゲットになっている場合に、責任問題が発生する可能性がある。事件処理担当者は、攻撃されたと主張している団体と事件についていつ話し合い、どんな情報を公開すべきかについて理解すること。

+ **特定の種類の不適切な使用を検知するように侵入検知ソフトウェアを設定する** 侵入検知ソフトウェアには、許可されていないサービスの利用、外向きの偵察活動や攻撃、不適切な電子メールの中継(スパムの送信)など、特定の不適切な使用の事件を検知するための機

能が組み込まれている。

+ **ユーザの活動に関する基本的な情報をログに記録する** ユーザの活動に関する基本的な情報(たとえばFTPコマンド、ウェブ要求、電子メールヘッダーなど)は、調査および証拠として価値がある。

+ **すべての電子メールサーバを、不正なメール中継で利用できないように設定する** メールの中継は、スパムを送信するために使用されることが多い。

+ **すべての電子メールサーバでスパムフィルタリングを実行する** スパムフィルタリングソフトウェアは、外部から組織に送られたスパムと、内部のユーザが送ったスパムの両方について、その多くをブロックできる。

+ **URLフィルタリングソフトウェアを実行する** URLフィルタリングソフトウェアは、多くの不適切なウェブサイトへのアクセスを防ぐ。ユーザにはこのソフトウェアの使用を義務付ける必要がある。通常は、トラフィックがURLフィルタリングを実施しているサーバを通過しないと、外部のウェブサーバにアクセスできないように設定する。

A.2.5 複合要素の事件

+ **一元化したログとイベント相関処理ソフトウェアを使用する** すべての前兆や兆候にある一つの観点からアクセスできれば、事件処理担当者は、複数の要素を持った事件をより早く見つけることができる。

A.3 検知と分析

+ **いくつもの種類のセキュリティソフトウェアが生成した警報を使って、前兆や兆候を見つける** IDPS、ウイルス対策ソフトウェア、スパイウェア駆除ソフト、ファイル完全性チェックソフトウェアは、事件の兆候を見つける上で有用である。各ソフトウェアは、ほかのソフトウェアが検知できない事件を検知することもある。よって、複数の種類のコンピュータセキュリティソフトウェアを利用することを強くお勧めする。サードパーティーの監視サービスも有用である。

+ **外部の者が事件を報告する仕組みを確立する** 外部の者が組織に事件を報告したい場合がある。たとえば、組織のユーザのひとりが彼らを攻撃していると思われるような場合である。組織は電話番号と電子メールアドレスを公開して、それを使って外部の者がそのような事件を報告できるようにすべきである。

+ **全システムにログと監査の基準レベルを義務付け、重要なシステムではより高い基準レベルを義務付ける** オペレーティングシステム、サービス、アプリケーションのログは、事件の分析の際に役立つことが多い(監査が有効になっている場合は、なおさらである)。ログは、アタッカーがどのアカウントにアクセスしたか、どのような活動を行ったか、などの情報を提供する。

+ **ネットワークとシステムのプロファイル** プロファイリングでは、期待される活動レベルの特性を測定することで、あるパターンの変更をより簡単に見つけることができる。プロファイリングプロセスを自動化すれば、期待される活動レベルからのずれを素早く検出して管理者に報告することができ、事件や運用上の問題の早期検出につながる。

+ **ネットワーク、システム、アプリケーションの正常な動作を理解する** チームのメンバーが正常な動作とはどのようなものなのかを理解すれば、異常な動作もより簡単に認識するこ

とができる。この知識を得るには、ログエントリーやセキュリティ警報をレビューするのが一番である。これにより処理担当者は、典型的なデータに慣れると同時に、異常なエントリーの調査を通じて、より詳しい知識を得ることができる。

+ **一元化されたログ取得とログ保管ポリシーの作成** 事件に関する情報は、さまざまな場所で記録される可能性がある。そこで、一元的なログサーバを設置して、組織内のログを生成する各装置が、ログエントリーのコピーをそのサーバに送るように設定する。こうすることで、関係するすべてのログエントリーが集まるため、事件処理担当者にとっては便利である。また、各ホストでログに変更が加えられても、すでに一元的なサーバに送られたデータには影響しない。以前のログエントリーが、前回の同様な活動や関連する活動を示す場合もあるため、ログ保管ポリシーは大切である。

+ **イベント相関処理の実施** 事件の兆候は、いくつものログで捕捉される可能性がある。複数のソースのイベントを相関させることは、事件に関して入手できるすべての情報を収集し、事件が発生したかどうかを検証する上で、とても重要である。ログを一元化することで、相関処理を簡単かつ素早く行うことができるようになる。

+ **すべてのホストの時刻を同期させておく** イベントを報告する機器の時刻の設定が合っていないと、イベント相関処理が困難になる。時刻にずれがあると、証拠の観点からも問題が起こる。

+ **情報の知識ベースの維持と利用** 処理担当者は、事件分析の際、情報を素早く参照する必要がある。一元化された知識ベースは、一貫した、保守可能な情報源となる。知識ベースには、よく使われるポート番号やマルウェア情報へのリンクなどの一般的な情報と、以前の事件の前兆や兆候などのデータを格納する。

+ **経験が少ないスタッフのための診断マトリックスの作成** ヘルプデスクのスタッフ、システム管理者、インシデント対応チームの新しいメンバーは、どの種類の事件が起きているかを判断する際、助けが必要である。事件の分類と各分類に関連する症状を一覧にした診断マトリックスがあると、どの種類の事件が起きているか、どのように事件を確認するかに関する手引きとなる。

+ **事件が起きた疑いがある場合には、すぐに全情報の記録を開始する** 事件が検出された時点から、最終的に解決された時点までのすべてのステップを文書化し、タイムスタンプを記録する。こういった情報は、告訴することになった場合に、法廷で証拠として使用することができる。実行したステップを記録することで、より効率的で体系的な、誤りのない問題処理が可能になる。

+ **事件データの保護** 事件データには、脆弱性、セキュリティ違反、不適切な活動を行った可能性があるユーザ等の機密情報が含まれていることが多い。 事件処理チームは、事件データへのアクセスが論理的かつ物理的に適切に制限されるようにするべきである。

+ **影響のあるリソースの重要性や事件の技術的な影響に基づき、ビジネスインパクトごとに事件に優先順位を付ける** リソースに制限があるという理由で、起きた順に事件を処理することは、やめるべきである。代わりに、事件の現在および将来のビジネスインパクトを基に、チームがどれだけ迅速に事件に対応しなくてはならないか、どのような行動をとるべきかについて、文書化したガイドラインを作成する。このガイドラインがあれば、事件処理担当者の時間が節約でき、行った処置について、マネジメント層とシステムオーナーに対する説明ができる。各組織は、チームが指定された時間内に事件に対応しない場合に備え、エスカレーションプロセスを確立しておく。

+ **組織のインシデント対応ポリシーの中に、事件報告に関する項目を盛り込む** どの事件をいつだれに報告しなくてはならないかについて、明記する。一般に通知すべき関係者としては、最高情報責任者(CIO)、情報セキュリティ部門長、各地区の情報セキュリティ管理者、組織内のほかのインシデント対応チーム、システムオーナーがある。

A.4 封じ込め、根絶、復旧

+ **事件を封じ込めるための戦略と手順の確立** ビジネスへのインパクトを制限するために、事件を素早く効果的に封じ込めることは重要である。組織は、事件を封じ込める際の許容可能なリスクを定義し、相応の戦略と手順を作成しておくこと。封じ込めの戦略は、事件の種類によってさまざまである。

+ **証拠収集と処理のための、確立された手順に従うこと** あらゆる証拠を保全する方法について、明確に文書化すること。証拠は、いつでも説明できるようになっていなくてはならない。法務部のスタッフや法執行機関と会って事件処理について話し合い、その内容に基づいて手順を作成する。

+ **揮発性データを証拠としてシステムから取得する** この作業にはネットワーク接続の一覧、プロセス、ログインセッション、オープンされたファイル、ネットワークインタフェース設定、メモリーの内容が含まれる。信頼できる媒体から注意して選んだコマンドを実行することで、システムの証拠を破壊することなく、必要な情報を収集できる。

+ **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って、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、中身の入っていないライトプロテクトされたメディアか、ライトワンスメディアに作成する。調査および証拠としての目的からは、このプロセスのほうが、ファイルシステムのバックアップよりも優れている。イメージ取得が望ましいほかの理由としては、オリジナルのシステム上で分析を行うよりも、イメージ上で分析したほうがより安全なことが挙げられる。分析により、オリジナルを誤って変えてしまうことがあるからである。

A.4.1 サービス不能事件

+ **いくつかの対策を順に並べた封じ込め戦略を作成する** 推奨される対策を事前に規定しておけば、DoS事件を封じ込めるための意思決定プロセスが容易になる。考えられる各対策の有効性は事件によって変わるため、いくつかの対策を選び、どの順番で対策を実施するかを決定する。

A.4.2 悪意のコードの事件

+ **悪意のコードによる事件は、できるだけ早く封じ込める** 悪意のコードはひそかに活動し、ほかのシステムに急速に増殖する可能性があるため、感染が拡大してより大きな被害を与える前に、事件を早期に封じ込める必要がある。感染したシステムは、すぐにネットワークから切断すべきである。電子メールを媒介とした悪意のコードによる事件を掌握するため、電子メールサーバレベルでブロックするか、または、一時的に電子メールサービスを中断しなくてはならない場合もある。

A.4.3 不正アクセス事件

+ **変更管理情報をインシデント対応チームに提供する** システムのシャットダウン、監査設定

の変更、実行可能ファイルの変更などは、攻撃ではなく、日常的なシステム管理でも行われる可能性がある。このような兆候が検知された場合、チームは変更管理情報を使用して、兆候が許可された活動によるものかどうかを確認できるようにしておく必要がある。

+ **リスク軽減とサービス維持のバランスを考えた封じ込め戦略を選択する** 事件処理担当者は、影響を受けていないサービスを維持しつつ、リスクを業務上支障の少ないレベルまで軽減することに重点を置くような、穏当な封じ込め対策を検討すること。

+ **rootが奪取されたと思われるシステムはリストアまたは再インストールする** root奪取の影響は、完全に確認するのが難しいことが多い。rootが奪取されたと思われる場合は、システムを正しいことがわかっているバックアップからリストアするか、オペレーティングシステムとアプリケーションを再インストールする。また、その後事件が二度と起こらないように、システムを適切に強化する。

A.4.4 複合要素の事件

+ **最初の事件を封じ込めてから、事件のほかの要素の兆候を探す** ある事件に1つの要素しかないと断定できるようになるには、長い時間がかかる場合がある。その間、最初の事件の封じ込めは完了しないままである。よって一般的には、まず最初の事件を封じ込めるのがよい。

A.5 事後活動

+ **大きな事件の後には反省会を開催する** 反省会は、セキュリティ対策と事件処理プロセス自体を改善する上で、非常に有用である。

A.5.1 不正アクセス事件

+ **事件の各要素の処理に個別に優先順位を付ける** たいていの場合、組織のリソースは限られており、事件のすべての要素を同時に処理することはできない。各要素に対する対応ガイドラインと、各要素がどれだけ新しいかを踏まえた上で、各要素に優先順位を付けるべきである。

付録 B　事件処理のシナリオ

インシデントへの対応のシナリオを含んだ訓練は、インシデントに対応するための技能を身に付け、インシデントへの対応プロセスに関する潜在的な課題を明らかにできる、安価で効果的な手段となる。これらの訓練では、インシデントへの対応に参加する各人員に対し、簡単なシナリオと一連の関連する質問の一覧を提示する。次に、個々の質問についてグループで討議し、最も可能性の高い回答を決定する。訓練の目的は、シナリオの内容が現実に発生した場合に対応担当者が実際に行うと考えられる作業を明らかにし、それらの対応作業をポリシー、手続き、および一般に推奨される実践事項と比較して、相違や不足を特定することにある。たとえば、ある質問への回答から、インシデント対応チームが特定のソフトウェアを持っていないことや、組織内の別のチームが就業時間外のサポートを提供していないことが理由で、対応が遅れるということがわかる場合がある。

次の質問は、ほとんどすべてのシナリオに該当する。各質問には、このドキュメントの関連セクションへの参照が挙げてある。質問とシナリオの後に、それぞれ追加で事件固有の質問が記載されている。これらの質問やシナリオを、各組織のインシデント対応訓練に合わせて使用することを強くお勧めする。[114]

B.1　シナリオの質問

準備:

1. あなたの組織では、この活動を事件とみなしますか? もしそうなら、この活動は、組織のどのポリシーに違反していますか? (セクション2.1)
2. この種のインシデントの発生を防止し、その影響を限定するために、どのような措置を講じていますか？(セクション3.1.2)

検知と分析:

1. あなたの組織では、インシデントのどんな前兆（あれば）を検知しますか？前兆があった場合、あなたの組織はインシデントが起きる前に行動を起こそうとしますか？ (セクション3.2.2、3.2.3)
2. あなたの組織では、インシデントのどんな兆候を検知しますか？どの兆候があったらインシデントが起きた可能性があると考えますか？ (セクション3.2.2、3.2.3)
3. インシデント対応チームは、どうやってこのインシデントを分析し検証しますか？ (セクション3.2.4)
4. チームはこのインシデントを、組織内のだれに／どのグループに報告しますか？ (セクション3.2.7)
5. 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の対応に優先順位をつけますか？ (セクション3.2.6)

114 訓練に関する詳細は、NIST SP 800-84『IT計画およびIT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(*Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities)*』を参照のこと。このドキュメントは、http://csrc.nist.gov/publications/PubsSPs.html で入手可能である。

封じ込め、根絶、復旧:

1. このインシデントを封じ込めるために、あなたの組織はどんな方策を採用しますか？この方策がほかよりも望ましいのはなぜですか？ (セクション3.3.1)
2. インシデントを封じ込めないと、何が起きる可能性がありますか？ (セクション3.3.1)
3. あなたの組織では、どんな証拠ソース(あれば)を取得しますか? 証拠はどのようにして取得しますか? どこに保管しますか? どれだけの期間保管しますか? (セクション3.2.5、3.3.2、3.4.3)

事後活動:

1. このインシデントに関する反省会にはだれが参加しますか？ (セクション3.4.1)
2. 将来同様のインシデントの発生を防ぐには何ができますか？ (セクション3.1.2)
3. 同様のインシデントの検知を向上させるためには何ができますか？ (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、インシデント対応チームのメンバーが何人参加しますか？ (セクション2.4.3)
2. インシデント対応チーム以外で、組織内のどのグループがこのインシデントの処理に関連しますか？(セクション2.4.4)
3. チームからどの外部関係者にこのインシデントを報告しますか？いつ報告しますか？報告はどのように行いますか？ (セクション2.3.2)
4. 外部関係者への連絡事項には、ほかに何がありますか？ (セクション2.3.2)
5. このインシデントへの対応にあたって、どのツールやリソースを使用しますか？ (セクション3.1.1)
6. インシデントが別の日の別の時間（就業時間内と就業時間外）に起きていたら、対応方法にどのような面で違いが生じていましたか？ (セクション2.4.2)
7. インシデントが物理的に別の場所（オンサイトとオフサイト）で起きていたら、対応方法にどのような面で違いが生じていましたか？ (セクション2.4.2)

B.2 シナリオ

シナリオ1: DNS (Domain Name System)サーバのサービス不能

土曜の午後、外部のユーザが組織の公開ウェブサイトに徐々にアクセスできなくなった。1時間のうちに事態は悪化し、最終的には、組織の公開ウェブサーバにほとんどアクセスできなくなった。その間、組織のネットワーク部門のメンバーが、インターネットの境界ルーターにより自動生成された警報に対応したところ、組織の公開DNS(Domain Name System)サーバの両方が異常に大量のUDP (User Datagram Protocol)パケットを送受信しており、それらのパケットによって、組織のインターネットの帯域の多くが占有されていることがわかった。トラフィックを分析したところ、DNSサーバが、同一のIP (Internet Protocol)アドレスから大量の要求を受信していることがわかった。またネットワーク管理者は、そのアドレスからのすべてのDNS要求の送信元ポートが、UDP 7ま

たはUDP 19になっているのに気づいた。この分析を行っている間に、組織のネットワーク侵入検知センサーが、echoとchargenサービスに関連する疑わしい活動を記録した。

以下に、このシナリオに対する追加の質問を示す。

1. すべてのパケットで使われている外部IPアドレスに関して、だれに連絡すべきですか?
2. 最初の封じ込め対策を実施したところ、ネットワーク管理者が、内部の9台のホストでもDNSサーバに対して同じ異常な要求を送信しているのを発見したとします。これにより、事件の処理にどのような影響がありますか?
3. 9台の内部ホストのうち2台が、システムオーナーに連絡がつく前にネットワークから切断されたとします。どうやってシステムオーナーを特定しますか?

シナリオ2: 内部で生成されたスパム

木曜の朝、組織の苦情受付用電子メールアカウントが、「おたくの組織からスパムが届いた」というある人からの苦情メッセージを受け取った。このメッセージには、一攫千金の話を売り込むスパムのコピー(と完全な電子メールアドレス)が含まれていた。そこで、苦情受付用アカウントを監視しているセキュリティ管理者が電子メールを確認したところ、ヘッダーが、そのスパムが組織のメールサーバを使って送られたものであることを示していることに気づいた。セキュリティ管理者は、その電子メールと作業内容に関する簡単なメモを、インシデント対応チームのアドレスに転送した。その後インシデント対応チームのメンバーが作業内容を分析し、スパムのヘッダーが本物で、組織のメールサーバから送信されたものであると確信した。

以下に、このシナリオに対する追加の質問を示す。

1. インシデント対応チームは、どのようにしてスパムの送信元を確認しますか?
2. スパムに対する苦情にどのように対応しますか?

シナリオ3: ワームとDDoSエージェントへの感染

火曜の朝、新しいワームがインターネット上に放たれた。このワームは、2週間前に公にアナウンスされたMicrosoft Windowsの脆弱性を悪用しており、パッチは脆弱性の発表と同時にリリースされた。このワームは、(1) 感染したホスト上で見つけたすべてのアドレスに対して自分自身を電子メールで送る(2) 開かれているWindows共有があるホストを探して、自身を送信する、という2つの方法を使って増殖する。このワームは、メールで送るコピーごとに異なる添付ファイル名を生成するようになっている。各添付ファイルのファイル名はランダムに生成され、拡張子は10以上あるうちのどれかが使用される。メールのタイトルと本文は、それぞれ100以上の中から選択されるようになっている。ワームがホストに感染すると、管理者権限を取得し、分散型サービス不能(DDoS)のエージェントをさまざまなIPアドレスからFTP (File Transfer Protocol)を使ってダウンロードしようとする(エージェントを提供しているIPアドレスの数は不明である)。ウイルス対策ソフトウェアベンダーは、このワームに対する警告をすぐに発したが、ベンダーがシグネチャをリリースする前に、ワームは急速に広まった。ワームが広まり始めてから3時間後にはアンチウイルスシグネチャが入手可能になったが、組織はすでに大規模な感染による被害を受けていた。

以下に、このシナリオに対する追加の質問を示す。

1. インシデント対応チームは、どうやって感染したすべてのホストを見つけますか?
2. 組織は、アンチウイルスシグネチャがリリースされる前にワームが組織に入って来るのをどのようにして防ぎますか?
3. 組織は、アンチウイルスシグネチャがリリースされる前に感染したホストがワームを広めるのをどのようにして防ぎますか?
4. すべての脆弱なマシンに対してパッチを適用しようと考えますか。もしそうなら、どのようにして行いますか?
5. DDoSエージェントを受信した感染ホストが、次の朝ほかの組織のウェブサイトを攻撃するように設定されているとしたら、この事件の処理はどのように変わりますか?
6. 感染した1つまたは複数のホストに社員に関する個人情報が含まれていたとしたら、この事件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事件の状態について逐次情報を提供しますか? ワームのせいで電子メールサービスが過負荷または使用できなくなったらどうしますか?
8. 現在ネットワークに接続されていないホスト(たとえば、スタッフが休暇中だったり、職員が離れた場所におり、しばしばダイヤルインする場合など)に対処するために、どんな追加対策(あれば)を行いますか?

シナリオ4: 盗まれたクレジットカード番号の使用

月曜の朝、組織の法務部がFBI (Federal Bureau of Investigation)から電話を受けた。その内容は、組織のネットワークの中から、だれかが疑わしい活動を行っているというものだった。その日遅く、この活動について話し合うため、FBIのエージェント、マネジメント層のメンバー、法務部がミーティングを開いた。FBIは、いくつかの盗まれたクレジットカード番号を使ったオンライン購入活動を調査しており、先週の取引のうち30を超える取引について、組織のIPアドレスのひとつが使用されたことをつきとめた。エージェントは組織の支援を要請し、これを受けてマネージャは、インシデント対応チームに必要な証拠を取得するよう要請した。この件は秘密にしておくことがきわめて重要である。

以下に、このシナリオに対する追加の質問を示す。

1. インシデント対応チームは、どのようなソースから証拠を収集しますか?
2. 提示されたIPアドレスを現在どのホストが使用しているかを、どうやって特定しますか? 提示されたIPアドレスを1週間前にどのホストが使用していたかを、どうやって実証しますか?
3. 調査を秘密にするために何をしますか?
4. そのホストにルートキットがインストールされていて不正な取引が行われていることを発見したとしたら、この事件の処理はどのように変わりますか?

シナリオ5: 侵入されたデータベースサーバ

火曜の夜、データベース管理者が、実稼働しているデータベースサーバの何台かで、稼働時間外の保守を行った。管理者は、サーバの1つで、見慣れない異常なディレクトリ名がいくつかあるのに気づいた。ディレクトリー覧を確認してファイルのいくつかを見たところ、サーバが攻撃を受けたと結論付け、インシデント対応チームに支援を要請してきた。チームの調査で、アタッカーは6週間前にrootアクセスの取得に成功していることがわかった。

以下に、このシナリオに対する追加の質問を示す。

1. いつ侵入が起きたかを、どのソースを使って判断しますか?
2. データベースサーバでパケットスニッファが動作しており、ネットワークからパスワードをキャプチャしているのを発見した場合、この事件の処理はどのように変わりますか?
3. 取り扱いに注意が必要な顧客情報を含んだデータベースを毎晩コピーし、電子メールで外部のアドレスに送るようなプロセスがサーバで動作しているのを発見した場合、事件の処理はどのように変わりますか?
4. そのサーバにルートキットがインストールされていていることを発見したとしたら、この事件の処理はどのように変わりますか?

シナリオ6: ウイルスデマ情報

水曜の午後、凶悪な新種のウイルスについてあるユーザが電子メールを転送してきた。このユーザは、ほかの組織にいる友人からメールを受け取ったとのことだった。メールによれば、新種のウイルスはウイルス対策ソフトウェアで検知できず、ユーザはハードディスクから3つのウイルスファイルを探して削除するようにとのことだった。そこで、ヘルプデスクの職員がメッセージを調査し、デマメールだと判断し、ユーザに電子メールで返信した。

その間、別のユーザが同じウイルス警告メールをほかの外部関係者から受け取り、組織内外に転送した。木曜の午後までに、ヘルプデスクは、3つある「ウイルスファイル」をハードディスクから削除したという人からの電話をいくつも受けた。これらのファイルは実際には正当なファイルであり、いくつかのアプリケーションが使用していた。ヘルプデスクのリーダーは、インシデント対応チームの支援を要請した。

以下に、このシナリオに対する追加の質問を示す。

1. 先を見越して、3つのファイルがなくなっているホストを特定しますか? もしそうなら、どのようにして行いますか? 特定しないなら、それにはどんな悪影響がありますか?

シナリオ7: FTPサーバ上の不正なデータ

ネットワーク管理者は、週次利用レポートの作成中に、組織の非武装地帯(DMZ)セグメントの業務時間外の帯域使用率が、通常より非常に高いことに気づいた。管理者は、ネットワーク監視ソフトウェアの設定を変更することで、DMZの帯域使用率についてより詳細な統計を収集した。次の日、管理者は、いつもと違って活動のかなりの部分が組織のFTPサーバに関係していることを発見した。ネットワーク管理者は、ちょうど休暇を終えたばかりのFTPサーバの管理者に、活動の増加について連絡した。FTPサーバの管理者は、サーバが不正なデータを保有しているのをす

ぐに見つけた。どうやら海賊版のソフトウェア、音楽、動画らしかった。管理者はインシデント対応チームにこの活動について連絡してきた。

以下に、このシナリオに対する追加の質問を示す。

1. 違法なデータをFTPサーバにアップロードした個人をすべて特定しようと考えますか? もしそうなら、どのようにして行いますか?
2. サーバ上の不正なデータが違法だということを確認しようと考えますか? もしそうなら、どのようにして行いますか?

シナリオ8: 外部へのDDoS攻撃

日曜の夜、組織のネットワーク侵入検知センサーの1つが、大量のICMP (Internet Control Message Protocol) pingを使った外部への疑わしいDDoS活動について警報を発した。侵入分析担当者が警報を確認したところ、警報が正しいということは確認できなかったが、既知のどの誤検知にも一致しなかった。分析者はインシデント対応チームに連絡し、活動を詳しく調査するよう依頼してきた。DDoS活動では偽装された送信元IPアドレスが使用されるため、活動の元が組織内のどのホストであるかを特定するのに非常に多くの時間と労力を要した。その間もDDoS活動は続いた。調査の結果、5台のサーバがDDoSトラフィックを生成しているらしいことがわかった。そこで、これら5台のサーバを分析したところ、それぞれDDoSルートキットの兆候が見られた。また、サーバのうちの3台は、ほかの内部ホストを攻撃するのに使用され、1台は、同様に外部ホストを攻撃するのに使用されていた。

以下に、このシナリオに対する追加の質問を示す。

1. 組織内のどのホストがトラフィックを生成しているか、どうやって特定しますか? インシデント対応チーム以外のどのチームが、事件処理を支援できますか?
2. DDoS攻撃のターゲットになっているIPアドレスの所有者に連絡しますか? もしそうなら、だれがどのように連絡しますか?
3. 最初の侵入が、1台のサーバのモデムを通じて行われたことがわかった場合、どのようにしてこの活動を詳しく調査しますか?

シナリオ9: 給与支払い記録への不正アクセス

水曜の夕方、組織の物理セキュリティチームが、給与支払い管理者から、見知らぬ人が自分のオフィスから出て行こうとするところを見たという電話を受けた。その人物は廊下を逃げていき、建物の出口に通じる階段に消えたとのことだった。管理者は自分のワークステーションをロックしないまま数分間席を外していた。給与支払いプログラムは、席を立った時の状態のまま、ログイン中の状態でメインメニュー上にあったが、管理者はマウスが動かされたらしいことに気づいた。インシデント対応チームは事件に関する証拠を収集し、何が実行されたか(たとえば、給与支払いデータへのアクセスや改ざん、取り扱いに注意を要する個人情報へのアクセス、トロイの木馬の設置など)を確認するよう依頼された。

以下に、このシナリオに対する追加の質問を示す。

1. 何が実行されたかをどうやって確認しますか?

2. 給与支払い管理者が、自分のオフィスから出て行った人間が、以前給与支払い部門の職員だったことに気づいたとしたら、事件の処理はどのように変わりますか?
3. 物理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の手法を使って建物や給与支払い部門への物理アクセスを得たことを突き止めた場合、事件の処理はどのように変わりますか?
4. その人物が現在の職員だと信ずるに足る理由を得た場合、事件の処理はどのように変わりますか?
5. 先週のリモートアクセスログから、給与支払い管理者のユーザIDを使った、異常に大量のログイン失敗が見つかった場合、事件の処理はどのように変わりますか?
6. そのコンピュータに2週間前にキーロガーがインストールされたことを発見したとしたら、この事件の処理はどのように変わりますか?

シナリオ10: ハッキングツールのダウンロード

金曜の午後、ネットワーク侵入検知センサーが疑わしいFTP活動を記録した。内容は、内部ユーザが外部FTPサーバからファイルをダウンロードしたとのことだった。侵入分析者が警報を確認したところ、警報は誤検知だとわかった(たしかに、その警報は攻撃が起きたことを示していたが、センサーによるサポートデータには攻撃の兆候がなかった)。しかしこのデータはほかの関心を引き起こした。というのは、ユーザが、スペースやピリオドの繰り返しや、通常のFTPディレクトリ名では使われない文字が含まれた、怪しいディレクトリ構造から実行ファイルをダウンロードしていることがわかったためである。侵入分析者がインターネットのサーチエンジンを使ってこの実行ファイル名の詳しい情報を調査した結果、そのいくつかがハッキングツールの名前と一致した。分析者は事件対応チームに連絡し、詳しい分析と、この活動をどう処理すべきかの判断を依頼してきた。

以下に、このシナリオに対する追加の質問を示す。

1. ユーザが何のファイルをダウンロードしたかをどうやって確認しますか?
2. ダウンロードされたファイルがハッキングツールであることを、どうやって確認しますか?
3. ツールをダウンロードした疑いのあるユーザが、組織の情報セキュリティチームのメンバーだった場合、事件の処理はどのように変わりますか?
4. ツールをダウンロードした疑いのあるユーザが、インシデント対応チームのメンバーだった場合、事件の処理はどのように変わりますか?
5. ツールをダウンロードした疑いのあるユーザが、以前請け負い業者であり、契約が更改されなかったことがちょうどわかったとした場合、事件の処理はどのように変わりますか?

シナリオ11: 消えたホスト

木曜の午後、ネットワーク侵入検知センサーが、内部ホストをターゲットにした脆弱性スキャン活動を記録した。これは、内部のIPアドレスを使って生成されたものであった。侵入検知分析者は、許可を受け予定された脆弱性スキャン活動の連絡を受けていなかったため、この活動をイン

シデント対応チームに報告した。チームが分析を開始すると、この行動が止まり、そのIPアドレスを使用しているホストは見つからなくなった。

以下に、このシナリオに対する追加の質問を示す。

1. 脆弱性をスキャンしていたホストの身元に関する情報は、どのデータソースになら含まれている可能性がありますか?
2. だれが脆弱性スキャンを行っていたかをどうやって見つけますか?
3. ダウンロードされたファイルがハッキングツールであることを、どうやって確認しますか?
4. 脆弱性スキャンが、組織の最も重要なホストに向けられたものだとした場合、事件の処理はどのように変わりますか?
5. 脆弱性スキャンが、外部のホストに向けられたものだとした場合、事件の処理はどのように変わりますか?
6. 脆弱性スキャンが行われる30分前に、だれかが施設に押し入ったのを物理セキュリティスタッフが発見した場合、事件の処理はどのように変わりますか?

シナリオ12: 在宅勤務の侵害

土曜の夜、ネットワーク侵入検知ソフトウェアが、内部のIPアドレスからのプローブとスキャンを記録した。数台のサーバ上のホスト侵入検知ソフトウェアも、プローブとスキャンを記録した。侵入検知分析者は、内部のIPアドレスが組織のVPNサーバのものであることを突き止め、インシデント対応チームに連絡した。チームは侵入検知ソフトウェア、ファイアウォール、VPNサーバのログを調べ、活動を生成している外部のIPアドレス、そのセッションで認証されたユーザID、そのユーザに関連付けられたユーザの名前を特定した。

以下に、このシナリオに対する追加の質問を示す。

1. チームの次のステップはどのようなものにすべきですか(たとえば、ユーザの家に電話する、ユーザIDを無効にする、VPNセッションを切断するなど)? どうして最初にそのステップを実行するのですか? 次に実行すべきステップは何ですか?
2. 特定されたユーザのパーソナルコンピューターが、家族がダウンロードしたゲームの中に入っていたトロイの木馬に感染しているとします。これは、チームの事件の分析にどのように影響しますか? これは、証拠収集と処理にどのように影響しますか?
3. たしかにその外部IPアドレスは特定されたユーザが使っているが、そのIPアドレスはNAT (Network Address Translation)を実行しているファイアウォール装置のもので、その後ろには8台のホストがある場合、事件処理はどのように変わりますか?
4. ユーザのパーソナルコンピューターによる事件を根絶するため、チームは何をすべきですか?
5. ユーザがウイルス対策ソフトウェアをインストールしたところ、トロイの木馬がインストールされていて、さらにキーストロークロガーが含まれていることがわかったとします。これにより、事件の処理にどのような影響がありますか? ユーザがシステム管理者だった場合、事件の処理にどのような影響がありますか? ユーザが組織の高官だった場合、事件

の処理にどのような影響がありますか?

6. その外部IPアドレスが特定されたユーザによって使用されていなかった場合、事件の処理はどのように変わりますか?
7. チームがそのホストを分析する前に、影響を受けたホストのオペレーティングシステムをユーザが再インストールしてしまった場合、事件の処理はどのように変わりますか?
8. 組織が保有する個人情報を、そのユーザが自身のPCに保存していた場合、事件の処理はどのように変わりますか?

シナリオ13: テロリストの脅威

木曜の午後、組織の物理セキュリティチームにマネージャから電話があり、彼女の部下が、テロリストグループと一緒にいるという人物から電話を受けたと報告してきた。電話の相手は組織を脅迫し、来週攻撃すると言ってきたが、攻撃の種類や、組織の何が(たとえば設備、人、コンピューティングリソースなど)ターゲットとなるかは言わなかった。調査を行った結果、この脅迫をまじめに受け取るべきだと考えた物理セキュリティチームは、情報セキュリティチームやインシデント対応チームを含む適切な内部チームに連絡を取り、脅威について伝えてきた。

以下に、このシナリオに対する追加の質問を示す。

1. 脅迫の連絡に対して、インシデント対応チームは独自に何をすべきですか(あれば)?
2. 物理セキュリティコントロールが高められると、事件に対するチームの対応にどのような影響がありますか?

シナリオ14: フレームとポートスキャニング

シナリオ13の脅迫を受けた後の火曜の午後に、侵入検知分析者が、遠隔施設にあるいくつかのサーバに向けられた、異常なスキャニング活動の検知を示す、いくつかの警報を受けた。分析者はインシデント対応チームに電話し、活動の調査と評価を支援するよう依頼した。インシデント対応チームのだれかが要望に応える前に、チームはその遠隔施設が火事になっているのを知った。現時点では鎮火している間に設備が避難させられたということ以外、詳細はわからない。

以下に、このシナリオに対する追加の質問を示す。

1. インシデント対応チームは何から取りかかるべきですか?
2. 侵入検知分析者が電話をかけ直してきて、その後1台のサーバに対する攻撃を示す警報があったことを報告してきた場合、事件の処理はどのように変わりますか?
3. 火事の結果遠隔施設へのネットワーク接続が失われた場合、事件の処理はどのように変わりますか?
4. 火事の結果スキャンの明白なターゲットが壊れた場合、事件の処理はどのように変わりますか?
5. インシデント対応チームがいる施設で火事が起きた場合、事件の処理はどのように変わりますか?

6. インシデント対応チームとターゲットになったシステムが同じ施設にあり、そこで火事が起きた場合、事件の処理はどのように変わりますか?

シナリオ15: ピアツーピアのファイル共有

組織のポリシーでは、ピアツーピアのファイル共有サービスの利用は禁止されている。たとえば、ワークステーション型のファイル共有を通じて、インターネット上で音楽ファイルが転送できるようなサービスがこれに該当する。組織のネットワーク侵入検知センサーでは、人気のあるピアツーピアのファイル共有サービスの利用を検出できるシグネチャが有効になっている。月曜の夕方、侵入検知分析者が、3時間前からいくつかのファイル共有警報が起きており、同じ内部IPアドレスに関係しているのに気づいた。

1. この事件の処理に優先順位を付ける際には、どんな要素を使用しますか(たとえば、共有されているファイルの明らかな内容など)?
2. プライバシー上のどのような問題がこの事件の処理に影響を与えますか?
3. ピアツーピアのファイル共有を行っているコンピュータ上に、取り扱いに注意を要する個人情報が保存されていた場合、事件の処理はどのように変わりますか?

シナリオ16: 不明なワイヤレスアクセスポイント

月曜の朝、組織のヘルプデスクはビルの同じフロアの3人のユーザから電話を受けた。それによると、ワイヤレスアクセスで問題が起きているとのことだった。問題解決の支援を求められたネットワーク管理者が、ワイヤレスアクセス可能なラップトップをユーザのフロアに持って行った。自分のワイヤレスネットワークの設定を見たところ、新しいアクセスポイントが表示されているのに気づいた。彼はチームメートと共にチェックを行い、このアクセスポイントは彼のチームが設置したものではなく、許可なく開設された不正なアクセスポイントの可能性が非常に高いと判断した。

1. この事件を処理する際の最初の大きなステップは何ですか(たとえば、不正なアクセスポイントを物理的に探す、そのアクセスポイントに論理的にアタッチするなど)?
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? アクセスポイントを見つける最も目立たない方法は何ですか?
3. もしアクセスポイントが、組織のオフィスで働いている外部の者(たとえば請負作業者)が一時的に設置したものである場合、事件の処理はどのように変わりますか?
4. もし侵入検知分析者が、ワイヤレスユーザがいるフロアに置いてあるワークステーションのいくつかに関する、疑いのある活動の兆候を報告してきた場合、事件の処理はどのように変わりますか?
5. チームがアクセスポイントを物理的に見つけようとしている間に、アクセスポイントが取り外された場合、事件の処理はどのように変わりますか?

付録 C　事件に関係するデータフィールド

各組織は、それぞれの事件で収集すべき標準のデータフィールドを規定すべきである。この作業により、より効果的で一貫した事件処理が可能となるだけでなく、該当する事件報告義務を果たすのにも役立つ。また、事件を報告する際に収集する基本的なフィールド群(事件報告者の名前、電話番号、場所など)と、事件処理担当者が対応中に収集すべきフィールド群も指定すべきである。この2つのフィールド群が、セクション3.2.5で説明した事件報告データベースの基礎となる。以下に示す一覧は、事件に対してどんな情報を収集すべきかに関する提案であり、包括的なものではない。組織は、インシデント対応チームのモデルと構成、および「事件」という用語の定義といったいくつもの要因を踏まえて、組織ごとに固有のフィールド一覧を作成すること。

C.1　基本的なデータフィールド

+ 事件報告者の連絡先情報
  - 名前
  - 組織ユニット(機関、部門、部、チーム)
  - 電子メールアドレス
  - 電話番号
  - 場所(住所、オフィスの部屋番号など)
+ 事件の詳細
  - 事件を発見した日付と時刻(タイムゾーンを含む)
  - 事件が発生した日付と時刻(タイムゾーンを含む)
  - 事件の種類(サービス不能、悪意のコード、不正アクセス、不適切な使用など)
  - 事件の物理的な位置(市、州など)
  - 事件の現在の状態(攻撃が継続中など)
  - 事件のソースや原因(わかる場合)。ホスト名とIPアドレスを含む。
  - 事件の説明(どうやって検知したか、何が起きたかなど)
  - オペレーションシステムの種類、オペレーションシステムのバージョンおよびパッチレベル
  - ウイルス対策ソフトウェアがインストールされ、有効かつ最新になっているか(はい／いいえ)
  - 影響を受けたリソースの説明(ネットワーク、ホスト、アプリケーション、データなど)。システムのホスト名とIPアドレス、および機能を含む。
  - 事件を緩和するための要素
  - 事件の技術的な影響の見積(データ消去、システムクラッシュ、アプリケーション利用不可など)。(セクション2.3.6を参照して、事件の重大さの格付けと影響の格付けを行うこと)

- 実施した対応活動(ホストの停止、ホストのネットワークからの切断など)
- 連絡するほかの組織(ソフトウェアベンダーなど)
- 事件の最中に侵害された個人情報(あれば)の種類

+ 一般的なコメント

C.2 事件処理担当者のデータフィールド

+ インシデント対応の現在のステータス
+ 事件の概要
+ 事件処理活動
  - すべての処理担当による活動の記録
  - 関連する全団体の連絡先情報
  - 収集した証拠の一覧
+ 事件処理担当者のコメント
+ 事件の原因(アプリケーションの設定ミス、ホストのパッチ未適用など)
+ 事件のコスト[115]
+ 事件のビジネスインパクト[116]

115 セクション3.4.2に事件のコストの計算方法に関する情報が記載されている。
116 事件のビジネスインパクトは、事件の影響の説明(たとえば、経理部が2日間業務を遂行できないなど)でもよいし、損害に基づく影響の分類(たとえば「影響大」の事件は$100,000を超える損害など)でもよい。

付録 D　用語集

『コンピュータセキュリティインシデント処理ガイド』で使われている主な用語を以下に定義する。

エージェント: 分散型サービス不能(DDoS)攻撃で使用されるプログラムで、ハンドラの指示に従ってホストに悪意のコードを送信する。

ベースライニング: リソースを監視して典型的な利用パターンを確定し、大きなずれを検知できるようにすること。

混合攻撃: 複数の手法を使用して広まる、悪意のコード。

ブートセクタウイルス: システムのブートセクタに潜み、マスターブートレコードに感染するウイルス。

ボット: 「エージェント」を参照。

コンピュータフォレンジック: データの完全性を維持しながら、調査目的でコンピュータ関連のデータを収集、保管、分析すること。

コンピュータセキュリティインシデント: 「事件」を参照。

コンピュータセキュリティインシデント対応チーム(CSIRT): コンピュータセキュリティ関連の事件への対応を支援する目的で発足させた機能。コンピュータインシデント対応チーム(CIRT)、CIRC(コンピュータインシデント対応センター、コンピュータインシデント対応機能)とも呼ばれる。

サービス不能(DoS): リソースを枯渇させることで、ネットワーク、システム、アプリケーションの正規の使用を妨害または阻害する攻撃。

分散型サービス不能(DDoS): 多数のホストを使用して攻撃を実行するDoSの手法。

出口フィルタ: 送信元アドレスが内部ネットワークのものになっているなど、明らかに間違っているIP (Internet Protocol)アドレスを使用している送信方向のパケットをブロックするプロセス。

事象: ネットワークまたはシステム内の目に見える出来事。

誤検知: 悪意のある活動が起きていないのに、起きていると間違って出してしまった警報。

ファイル感染型ウイルス: 自身をワードプロセッサやスプレッドシートアプリケーション、ゲームなどのプログラムファイルに埋め込むウイルス。

ファイル完全性チェッカー: ファイルのメッセージダイジェストを生成、保存、比較して、ファイルの変更を検知するソフトウェア。

フォレンジック: 「コンピュータフォレンジック」を参照。

ハンドラ: DDoS攻撃で使用されるプログラムの種類で、ネットワーク全体に配布されたエージェントを制御するためのもの。あるいは、事件処理業務において、 事件処理対応者のことをいう。

不適切な使用: ネットワークやコンピュータの利用規定に違反すること。

事件: コンピュータセキュリティポリシー、利用規定、標準コンピュータセキュリティ活動などの違反または差し迫った違反。

事件処理: セキュリティポリシーおよび推奨される活動の違反を軽減すること。

インシデント対応: 「事件処理」を参照。

兆候: 事件がすでに起きたか、または現在起こっている可能性を示すサイン。

入口フィルタ: 予約された送信元アドレスなど、明らかに間違っているIPアドレスを使用している受信方向のパケットをブロックするプロセス。

IDPS: コンピュータシステムまたはネットワーク上の疑わしい活動の監視プロセスを自動化し、事件の兆候を分析して、検出された事件の防止を試みるソフトウェア。

マクロウイルス: 自身をドキュメントに埋め込むウイルスで、ドキュメントのアプリケーションのマクロプログラミング機能を使用して動作・繁殖する。

悪意のコード: ウイルス、ワーム、トロイの木馬など、ホストに感染するコード型のエンティティ。

悪意のあるモバイルコード: リモートシステムからローカルシステムに転送され、ユーザの明示的な指示なしにローカルシステム上で実行されるソフトウェア

メッセージダイジェスト: 一般に、ファイルに対して生成されるチェックサムで、ファイルの変更を検知するために使用する。メッセージダイジェストアルゴリズムの例としては、SHA-1 (Secure Hash Algorithm-1)がある。

複合要素の事件: 1つの事件で2つ以上の事件を包含しているもの。

パケットスニッファ: ネットワークトラフィックを観察して記録するソフトウェア。

パッチ管理: パッチを入手、テストし、組織全体の該当する管理者やユーザに配布するプロセス。

ポートスキャニング: プログラムを使って、システムのどのポートが開いているか(システムがこれらのポートを経由した接続を許しているか)をリモートから調べること。

前兆: アタッカーが事件を起こす準備をしていることを示すサイン。

プロファイリング: 変更がより簡単に見つかるよう、予想される活動の特性を測定すること。

リスク: 1つ以上の不利な事象が起きる見込み。

ルートキット: アタッカーがホストへのルートレベルのアクセスを得た後に使用するツール群。ホスト上でのアタッカーの活動を隠し、アタッカーが隠された手段を使ってホストにルートレベルのアクセスをし続けられるようにする。

スキャニング: その後の攻撃で使用する情報を得るために、ほかのシステムにパケットや要求を送ること。

シグネチャ: ある攻撃に関係する、認識可能で特徴的なパターン。ウイルス中のバイナリ文字列や、システムへの不正アクセスを得るために使用する特定のキーストロークなどがある。

ソーシャルエンジニアリング: だれかをだまして、システムやネットワークを攻撃するために使

用する情報(パスワードなど)を聞き出そうとすること。

脅威: 不利な事象を起こす可能性がある元凶。

トロイの木馬: 自己複製不可能なプログラムで、便利な目的を持っているように見えて、実は別の悪意のある目的を持ったもの。

不正アクセス: 許可なくネットワーク、システム、アプリケーション、データ等のリソースに論理的または物理的にアクセスすること。

被害者: 攻撃されるマシン。

ウイルス: 自己複製するプログラムで、ほかのプログラムやファイルを変更することで動作・拡散するもの。

ウイルスデマ情報: 存在しないウイルスに関する緊急警告メッセージ。

脆弱性: 悪用や誤用の対象となるシステム、アプリケーション、ネットワークの弱点。

ワーム: 自己複製し、自己増殖する、自己完結型のプログラムで、ネットワークの仕組みを利用して広まっていく。

付録 E　頭字語

『コンピュータセキュリティインシデント処理ガイド』で使われている主な頭字語を以下に定義する。

BIA　Business Impact Analysis (**ビジネスインパクト分析**)

BIOS　Basic Input/Output System (**基本入出力システム**)

CCIPS　Computer Crime and Intellectual Property Section

CERIAS Center for Education and Research in Information Assurance and Security

CERT®/CC CERT® Coordination Center (**コーディネーションセンター**)

CIAC　Computer Incident Advisory Capability

CIO　Chief Information Officer (**最高情報責任者**)

CIRC　Computer Incident Response Center (**コンピュータインシデント対応センター**), Computer Incident Response Capability (**コンピュータインシデント対応機能**)

CIRDB　CERIAS Incident Response Database

CIRT　Computer Incident Response Team (**コンピュータインシデント対応チーム**)

CPU　Central Processing Unit (**中央処理装置**)

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

DHS　Department of Homeland Security (**国土安全保障省**)

DMZ　Demilitarized Zone (**非武装地帯**)

DNS　Domain Name System (**ドメイン名システム**)

DNSSEC DNS Security Extension (DNS**セキュリティ拡張**)

DOJ　Department of Justice (**司法省**)

DoS　Denial of Service (**サービス不能**)

e-mail　Electronic Mail (**電子メール**)

FAQ Frequently Asked Questions (**よく聞かれる質問**)

FBI Federal Bureau of Investigation (**連邦捜査局**)

FIPS Federal Information Processing Standards (**連邦政府情報処理規格**)

FIRST Forum of Incident Response and Security Teams

FISMA Federal Information Security Management Act (**連邦情報セキュリティ管理法**)

FTC Federal Trade Commission

FTP File Transfer Protocol (**ファイル転送プロトコル**)

GAO General Accounting Office (**会計検査院**)

GFIRST Government Forum of Incident Response and Security Teams

GRS General Records Schedule

HTML HyperText Markup Language

HTTP HyperText Transfer Protocol

HTTPS HyperText Transfer Protocol Secure

IAIP Information Analysis Infrastructure Protection (**情報分析インフラ保護**)

IANA Internet Assigned Numbers Authority

ICAMP Incident Cost and Analysis Modeling Project

ICMP Internet Control Message Protocol

IDPS Intrusion Detection and Prevention System (**侵入検知／防止システム**)

IETF Internet Engineering Task Force

IIS Internet Information Services

IP Internet Protocol

IPsec IP Security Protocol

IR Interagency Report

IRC Internet Relay Chat

ISAC Information Sharing and Analysis Center (**情報共有分析センター**)

ISAKMP Internet Security Association and Key Management Protocol

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

MAC Media Access Control

MAPS Mail Abuse Prevention System

MBR Master Boot Record (**マスターブートレコード**)

MSSP Managed Security Services Provider

NAT Network Address Translation

NICC National Infrastructure Coordinating Center

NIJ National Institute of Justice (**国立司法研究所**)

NIPC National Infrastructure Protection Center (**国家インフラ保護センター**)

NIST National Institute of Standards and Technology (**米国立標準技術研究所**)

NSRL National Software Reference Library

NTP Network Time Protocol

NVD National Vulnerability Database

OIG Office of Inspector General (**監察総監室**)

OMB Office of Management and Budget (**行政管理予算局**)

OS Operating System (**オペレーティングシステム**)

PBX Private Branch Exchange (**構内交換機**)

PDA Personal Digital Assistant

PDD Presidential Decision Directive (**大統領令**)

PII Personally Identifiable Information

PIN Personally Identifiable Number

POC Point of Contact

RFC Request for Comment

SHA Secure Hash Algorithm

SLA Service Level Agreement (**サービスレベル合意**)

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

soBGP Secure Origin Border Gateway Protocol

SOP Standard Operating Procedure

SP Special Publication

SSH Secure Shell

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TERENA Trans-European Research and Education Networking Association

UDP User Datagram Protocol

URL Uniform Resource Locator

US-CERT United States Computer Emergency Readiness Team

VPN Virtual Private Network

付録 F　印刷されたリソース

Bejtlich, Richard.　The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley, 2004.

Carrier, Brian.　File System Forensic Analysis.　Addison-Wesley, 2005.

Casey, Eoghan.　*Digital Evidence and Computer Crime*, Second Edition.　Academic Press, 2004.

Davis, Chris, et al.　Hacking Exposed Computer Forensics.　McGraw-Hill, 2004.

Hoglund, Greg and Butler, Jamie.　Rootkits.　Addison-Wesley, 2005.

James, Lance.　Phishing Exposed.　Syngress, 2005.

Jaquith, Andrew.　Security Metrics: Replacing Fear, Uncertainty, and Doubt.　Addison-Wesley, 2007.

Jones, Keith, et al.　Real Digital Forensics: Computer Security and Incident Response. Addison-Wesley, 2005.

Lucas, Julie and Moeller, Brian.　The Effective Incident Response Team.　Addison-Wesley, 2003.

Mirkovic, Jelena et al.　Internet Denial of Service: Attack and Defense Mechanisms.　Prentice Hall, 2004.

Nazario, Jose.　Defense and Detection Strategies Against Internet Worms.　Artech House, 2003.

Northcutt, Stephen, et al.　*Inside Network Perimeter Security, Second Edition.　Sams, 2005.*

Prosise, Chris, et al.　Incident Response and Computer Forensics, Second Edition.　McGraw-Hill Osborne Media, 2003.

Schweitzer, Douglas.　*Incident Response: Computer Forensics Toolkit.*　John Wiley and Sons, 2003.

van Wyk, Kenneth and Forno, Richard, *Incident Response*, O'Reilly and Associates, 2001.

Skoudis, Ed and Zeltser, Lenny.　Malware: Fighting Malicious Code.　Prentice Hall, 2005.

Szor, Peter.　The Art of Computer Virus Research and Defense.　Symantec Press, 2005.

Vacca, John R.　Computer Forensics: Computer Crime Scene Investigation.　Charles River Media, 2005.

付録 G　オンラインのツールとリソース

以下に、インシデント対応能力を確立して維持するのに役立つ、オンラインのツールとリソースの例を示す。

インシデント対応組織

組織	URL
AusCERT - Australian Computer Emergency Response Team	http://www.auscert.org.au
CCIPS - Computer Crime and Intellectual Property Section, **米国司法省**	http://www.cybercrime.gov
CERT®/CC - CERT® Coordination Center,**カーネギーメロン大学**	http://www.cert.org
CERT®/CC Incident Reporting System	https://irf.cc.cert.org
CIAC - Computer Incident Advisory Capability, **米国エネルギー省**	http://www.ciac.org/ciac
FIRST - Forum of Incident Response and Security Teams	http://www.first.org/
GFIRST - Government Forum of Incident Response and Security Teams	http://www.us-cert.gov/federal/gfirst.html
HTCIA - High Technology Crime Investigation Association	http://www.htcia.org
IETF Extended Incident Handling (inch) Working Group	http://www.cert.org/ietf/inch/inch.html
InfraGard	http://www.infragard.net
ISC - Internet Storm Center	http://isc.incidents.org
US-CERT - United States Computer Emergency Response Team	http://www.us-cert.gov
US-CERT Incident Reporting System	https://forms.us-cert.gov/report/

インシデント対応関連のメーリングリスト

メーリングリスト名	アーカイブの場所
Bugtraq	http://www.securityfocus.com/archive/1
Focus on IDS	http://www.securityfocus.com/archive/96
Forensics	http://www.securityfocus.com/archive/104
Incidents	http://www.securityfocus.com/archive/75
LogAnalysis	http://www.loganalysis.org/pipermail/loganalysis/
National Cyber Alert System	http://www.us-cert.gov/cas/
Technical Cyber Security Alerts	http://www.us-cert.gov/cas/techalerts/
Cyber Security Alerts	http://www.us-cert.gov/cas/alerts/

Cyber Security Bulletins	http://www.us-cert.gov/cas/bulletins/
Cyber Security Tips	http://www.us-cert.gov/cas/tips/
Current Activity	http://www.us-cert.gov/current/

技術リソースサイト

リソース名	URL
CERIAS (Center for Education and Research in Information Assurance and Security) Intrusion Detection Pages	http://www.cerias.purdue.edu/about/history/coast/archive/data/category_index.php
CHIHT (Clearing House for Incident Handling Tools)	http://chiht.dfn-cert.de
CSIRT Development, CERT®/CC	http://www.cert.org/csirts
CSRC - Computer Security Resource Center, NIST	http://csrc.nist.gov
Incident Handling Links and Documents	http://www.honeypots.net/incidents/links
Intrusion Detection Links and Documents	http://www.honeypots.net/ids/links
NIJ (National Institute of Justice) Electronic Crime Program	http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/welcome.htm
NIST Internet Time Service	http://tf.nist.gov/service/its.htm
SANS Institute Reading Room	http://www.sans.org/reading_room/
SecurityFocus	http://www.securityfocus.com
The Electronic Evidence Information Center	http://www.e-evidence.info

脆弱性とエクスプロイトの情報リソース

リソース名	URL
CERT®/CC Advisories	http://www.cert.org/advisories
CERT®/CC Incident Notes	http://www.cert.org/incident_notes
CERT®/CC Vulnerability Notes Database	http://www.kb.cert.org/vuls
CIAC Bulletins	http://www.ciac.org/ciac/bulletins.html
Common Vulnerabilities and Exposures (CVE)	http://cve.mitre.org/
National Vulnerability Database (NVD)	http://nvd.nist.gov/
Open Vulnerability Assessment Language (OVAL)	http://oval.mitre.org/

Packet Storm	http://www.packetstormsecurity.com
SANS Top 20 Security Risks List	http://www.sans.org/top20
SecurityFocus Vulnerabilities Database	http://www.securityfocus.com/bid

NIST　Special Publication

リソース名	URL
NIST Interagency Report (IR) 7100 - PDA Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf
NIST IR 7250 - Cell Phone Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/nistir-7250.pdf
NIST SP 800-28 Version 2 - Guidelines on Active Content and Mobile Code	http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-30 - Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
NIST SP 800-40 Version 2 - Creating a Patch and Vulnerability Management Program	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
NIST SP 800-41 - Guidelines on Firewalls and Firewall Policy	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
NIST SP 800-44 Version 2 - Guidelines on Securing Public Web Servers	http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
NIST SP 800-45 Version 2 - Guidelines on Electronic Mail Security	http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf
NIST SP 800-48 Revision 1 (Draft) - Wireless Network Security for IEEE 802.11a/b/g and Bluetooth	http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-53 Revision 2 - Recommended Security Controls for Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
NIST SP 800-72 - Guidelines on PDA Forensics	http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf
NIST SP 800-81 - Secure Domain Name System (DNS) Deployment Guide	http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf
NIST SP 800-83 - Guide to Malware Incident Prevention and Handling	http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
NIST SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
NIST SP 800-92 - Guide to Computer Security Log Management	http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
NIST SP 800-94 - Guide to Intrusion Detection and	http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Prevention Systems (IDPS)	
NIST SP 800-97 - Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
NIST SP 800-101 - Guidelines on Cell Phone Forensics	http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
NIST SP 800-115 (Draft) - Technical Guide to Information Security Testing	http://csrc.nist.gov/publications/PubsSPs.html

その他の技術的なリソースドキュメント

リソース名	URL
CIO Cyberthreat Response and Reporting Guidelines	http://www.cio.com/research/security/incident_response.pdf
Computer Security Incident Response Planning	http://documents.iss.net/whitepapers/csirplanning.pdf
Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)	http://www.cert.org/csirts/csirt_faq.html
Denial of Service Attacks	http://www.cert.org/tech_tips/denial_of_service.html
Electronic Crime Scene Investigation: A Guide for First Responders	http://www.ncjrs.gov/pdffiles1/nij/187736.pdf
Handbook for Computer Security Incident Response Teams (CSIRTs)	http://www.cert.org/archive/pdf/csirt-handbook.pdf
How to Design a Useful Incident Response Policy	http://www.securityfocus.com/infocus/1467
Incident Management Capability Metrics, Version 1.0	http://www.cert.org/archive/pdf/07tr008.pdf
Incident Response: Managing Security at Microsoft	http://www.microsoft.com/downloads/details.aspx?familyid=36e889be-4fb0-447a-943a-7484cba0e7c1&displaylang=en
Incident Response Tools for Unix, Part One: System Tools	http://www.securityfocus.com/infocus/1679
Incident Response Tools for Unix, Part Two: File-System Tools	http://www.securityfocus.com/infocus/1738
Managing the Threat of Denial-of-Service Attacks	http://www.cert.org/archive/pdf/Managing_DoS.pdf
OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information	http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
Responding to Intrusions	http://www.sei.cmu.edu/pub/documents/sims/pdf/sim006.pdf
RFC 2350: Expectations for Computer Security Incident Response	http://www.ietf.org/rfc/rfc2350.txt
RFC 3067: TERENA's Incident Object Description and Exchange Format Requirements	http://www.ietf.org/rfc/rfc3067.txt
RFC 3227: Guidelines for Evidence Collection and Archiving	http://www.ietf.org/rfc/rfc3227.txt

RFC 4732: Internet Denial-of-Service Considerations	http://www.ietf.org/rfc/rfc4732.txt
RFC 5070: The Incident Object Description Exchange Format	http://www.ietf.org/rfc/rfc5070.txt
Sample Incident Handling Forms, SANS Institute	http://www.sans.org/incidentforms
Staffing Your CSIRT—What Basic Skills Are Needed?	http://www.cert.org/csirts/csirt-staffing.html
State of the Practice of Computer Security Incident Response Teams	http://www.cert.org/archive/pdf/03tr001.pdf
A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms	http://lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

知識ベースリソース

リソース名	URL
IANA Protocol Numbers and Assignment Services	http://www.iana.org/protocols/
Domain Name System Parameters	http://www.iana.org/assignments/dns-parameters
ICMP Type Numbers	http://www.iana.org/assignments/icmp-parameters
Internet Multicast Addresses	http://www.iana.org/assignments/multicast-addresses
Internet Protocol V4 Address Space	http://www.iana.org/assignments/ipv4-address-space
IP Protocol Numbers	http://www.iana.org/assignments/protocol-numbers
IP Version Numbers	http://www.iana.org/assignments/version-numbers
Port Numbers	http://www.iana.org/assignments/port-numbers
Syslog Parameters	http://www.iana.org/assignments/syslog-parameters
TCP Header Flags	http://www.iana.org/assignments/tcp-header-flags
TCP Option Numbers	http://www.iana.org/assignments/tcp-parameters
IETF RFCs for Common Protocols (DNS, FTP, HTTP and SMTP)	http://www.ietf.org/rfc.html
RFC 959: File Transfer Protocol (FTP)	http://www.ietf.org/rfc/rfc0959.txt
RFC 1034:Domain Names—Concepts and Facilities	http://www.ietf.org/rfc/rfc1034.txt
RFC 1035: Domain Names—Implementation and Specification	http://www.ietf.org/rfc/rfc1035.txt
RFC 2065: Domain Name System Security Extensions	http://www.ietf.org/rfc/rfc2065.txt
RFC 2228: FTP Security Extensions	http://www.ietf.org/rfc/rfc2228.txt
RFC 2616: Hypertext Transfer Protocol—HTTP/1.1	http://www.ietf.org/rfc/rfc2616.txt
RFC 2617: HTTP Authentication: Basic and Digest Access Authentication	http://www.ietf.org/rfc/rfc2617.txt

RFC 2821: Simple Mail Transfer Protocol	http://www.ietf.org/rfc/rfc2821.txt
RFC 2822: Internet Message Format	http://www.ietf.org/rfc/rfc2822.txt
RFC 2965: HTTP State Management Mechanism	http://www.ietf.org/rfc/rfc2965.txt
Ports-Official and Unofficial Port Assignments	http://ports.tantalo.net/
TCP Ports List	http://www.gasmi.net/docs/tcp.html

付録 H　よく聞かれる質問

ユーザ、システム管理者、情報セキュリティスタッフメンバー、組織内のその他の人は、インシデント対応について疑問があるかもしれない。以下に示すのは、インシデント対応についてよく聞かれる質問(FAQ)である。このFAQをカスタマイズして、各ユーザコミュニティが入手できるようにすることをお勧めする。

1. **事件とは何ですか?**

   一般に事件とは、コンピュータセキュリティポリシー、利用規定、標準コンピュータセキュリティ活動などの違反を指す。事件の例としては、以下のものがある。

   + 公開ウェブサーバに対する分散型サービス不能攻撃
   + 1つのネットワーク上の数百ものワークステーションに感染し、効果的にネットワークを停止させるワーム
   + 電子メールサーバに対してリモートから管理者レベルのアクセスを得るアタッカー
   + パスワードクラッキングツールをダウンロードするユーザ
   + ほかの組織の公開ウェブサイトを書き換えるユーザ

2. **事件処理とは何ですか?**

   事件処理は、事件を検知・分析し、その影響を限定するプロセスである。たとえば、アタッカーがインターネット経由でシステムに侵入した場合、事件処理プロセスがセキュリティ違反を検知する。次に事件処理担当者がデータを分析し、攻撃がどれだけ深刻かを判断する。事件には優先順位が付けられる。事件処理担当者は、事件の進行を止め、影響を受けたシステムができるだけ早く通常の運用に戻るよう行動する。

3. **インシデント対応とは何ですか?**

   「事件処理」と「インシデント対応」は、このドキュメントでは同じ意味で使用する。[117]

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(コンピュータセキュリティインシデント対応チーム[CSIRT]とも呼ぶ)は、組織の一部または全体にインシデント対応サービスを提供する責任を負う。このチームは、事件と思われる情報を受け取り、それを調査し、事件による被害を最小化するべく行動する。組織によっては、インシデント対応チームが正式で専任になっているところもある。それ以外の組織では、必要に応じてほかの業務から集めた人間がインシデント対応チームのメンバーとなる。インシデント対応チームを持たず、インシデント対応業務を外部委託している組織もある。

---

117 「事件処理」と「インシデント対応」の定義は一般には異なる。たとえば、CERT®/CCでは、「事件処理」を事件の検知、報告、分析、対処全体のプロセスを表し、「インシデント対応」は、特に事件の封じ込め、復旧、他者への通知を表す。詳細は、http://www.cert.org/csirts/csirt_faq.html を参照。

5. インシデント対応チームはどんなサービスを提供しますか?

インシデント対応チームが提供するサービスは、組織によって大きく異なる。一般にチームは、事件処理を行う以外に、新しい脅威に関するアドバイザリを配布したり、ユーザや技術スタッフを教育し、事件予防と処理の中で、自分達がどんな役割を持っているのかを自覚させる。また多くのチームでは、侵入検知システムの監視や管理の責任も果たす。監査や侵入テストなど、その他のサービスを実施するチームをある。

6. 事件はだれに報告すべきですか?

各組織は、内部的に事件を報告するための、明確な連絡先(POC)を確立しなくてはならない。すべての事件を直接インシデント対応チームに報告するようにインシデント対応機能を構成している組織もあれば、情報技術(IT)ヘルプデスクなど、既存のサポート構造を最初の連絡先としている組織もある。ほかのインシデント対応チームなど、外部の団体がいくつかの事件を報告してくる点も認識すべきである。政府民間機関は、事件をUS-CERT(United States Computer Emergency Readiness Team)に報告するよう、法律で義務付けられている。

7. 事件はどうやって報告するのですか?

ほとんどの組織には、事件を報告するための方法が複数ある。活動を報告する者のスキル、事件の緊急性、事件の機密性などはさまざまであるため、いろいろな報告方法が望まれる。緊急事態を報告するためには、電話番号かポケットベルの番号がわかっていなくてはならない。正式でない事件報告なら電子メールアドレスを知らせればよいが、正式な事件報告にはウェブベースのフォームが便利である。チームに機密情報を送る場合には、安全な場所にあるマシンにFAXを送るか、チームが公開している公開鍵を使ってデータを暗号化する。

8. 事件を報告する際にはどんなデータを提供すればよいのですか?

情報は厳密なほどよい。たとえば、ワークステーションが悪意のコードに感染したと思われる場合、事件報告には次のデータを含めるべきである。

+ ユーザの名前、ユーザID、連絡先(電話番号、電子メールアドレス)
+ 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、IPアドレス
+ 事件が起きた日付と時刻
+ 何が起きたか順を追った説明。感染を見つけた後でワークステーションに何をしたかも含む。説明は詳しく記述し、悪意のコードが表示したメッセージや、ウイルス対策ソフトウェアの警報のメッセージは、正確な綴りを記述すること。

9. インシデント対応チームはどのくらい早く事件報告に対応しますか?

対応までの時間はさまざまな要素に依存する。要素としては、事件の種類、影響のあるリソースやデータの重要度、事件の重大性、影響のあるリソースに対する既存のサービスレベル合意(SLA)、時刻や曜日、チームが別の事件を処理中かどうかなどがある。一般に最も優先順位が高いのは、組織やほかの組織に大きな被害を及ぼしそうな事件の処理である。

10. 事件にかかわる人間は、法執行機関にいつ連絡すべきですか?

法執行機関への連絡は、インシデント対応チームのメンバー、最高情報責任者(CIO)、その他の任命された職員が行う。ユーザ、システム管理者、システムオーナー、その他の関係者は連絡すべきでない。インシデント対応チームは、確立されたポリシーや手順に従い、適切な時期に法執行機関に連絡する。

11. システムが攻撃されたことを見つけたら、何をすべきですか?

すぐにシステムの利用をやめ、インシデント対応チームに連絡する。事件の報告者が、事件の初期処理を支援することになる場合もある。たとえば、攻撃されたシステムからネットワークケーブルを抜いたり、事件処理担当者が到着するまでの間システム上の証拠を守るため、システムを物理的に監視するといったことである。

12. スパムを受け取ったらどうすればいいですか?

組織がスパム報告用に指定したアドレスに電子メールを転送する。スパムに関してまとめた統計は、アンチスパム対策の必要性を正当化する際に利用できる。この統計は、コンピュータセキュリティインシデントの動向を調査している事件報告組織にも送られる。スパムを受信した人は、メーリングリストからの削除を依頼することを含め、決してスパムメッセージに返信すべきではない。返信すると、この電子メールアドレスが有効で現に使われていることを送信者に証明することになる。

13. 友達から新種のウイルスについて警告を受け取りましたが、どうすればいいですか?

ウイルスデマ情報のウェブサイトでその新種のウイルスが本物かデマかを確認する。電子メールで配布される多くのウイルス警告はデマであり、その中の指示に従うと、システムが壊れてしまう可能性がある。ウイルス対策ソフトウェアベンダーのウェブサイトはウイルスデマ情報を提供していることが多い。それでもまだウイルス警告の信ぴょう性が疑わしい場合は、ヘルプデスクに連絡してさらなる支援を求める。

14. 事件に関してマスコミから連絡を受けたらどうすべきでしょうか?

インシデント対応に参加した人間は、事件と外部関係者に関しての組織のポリシーに従って、マスコミの質問に答えてかまわない。事件を議論する上で組織を代表する資格がない人は、組織の広報部を紹介する以外は、事件に関してコメントすべきでない。そうすることで広報部は、正確で一貫した情報をマスコミおよび一般大衆に提供できる。

付録 I　危機処理のステップ

以下に、技術の専門家が重大な事件が発生したことを確信したものの、組織に利用できるインシデント対応能力がない場合に実施すべき主なステップを示す。この付録は、現在危機に直面していて、このドキュメント全体を読む時間がないという人にとって、基本的な参考資料となる。

1. **すべてを記録に残すこと** これには、実行するあらゆる行動、あらゆる証拠、ユーザ、システムオーナー、事件に関係するその他の人とのあらゆる会話を含む。

2. **支援してくれる同僚を捜す** 二人以上で協力すれば、事件処理ははるかに容易になる。たとえば、ひとりが行動している間、もう一人はそれを記録する。

3. **証拠を分析して事件が起きたことを確認する** 必要に応じてさらに調査(インターネットサーチエンジン、ソフトウェアマニュアルなど)し、証拠をよく理解する。組織内の技術専門家に連絡し、助けを求める。

4. **事件が起きたと思われる場合には、組織内の適切な人に通知する** これには最高情報責任者(CIO)、情報セキュリティ部門長、ローカルセキュリティマネージャが含まれる。事件の詳細をだれかと話す場合は慎重に行う。その事件により個人情報が流出したと思われる場合は、組織のデータ侵害ポリシーが規定する関係者に、その旨を通知する。知る必要がある人にしか話さないようにし、十分安全な通信手段を使用する(アタッカーが電子メールサービスを侵害した場合、事件に関する電子メールは送らないこと)。

5. US-CERT(政府の諸官庁と機関の場合)および／または他の外部組織に事件を通知する。まずは、誤って機密情報を公開しないように、事件に関して広報部、法務部、および／またはマネジメント層と話し合う。その後、US-CERTおよび／または他の外部組織に事件を報告し、事件対応の支援を要請する。

6. **進行中の事件を止める** そのための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ある。サービス不能(DoS)攻撃などでは、ファイアウォールやルーターの設定を変更して、事件の一部になっているネットワークトラフィックを止めなくてはならない場合もある。

7. **事件の証拠を保管する** 影響を受けたシステムのバックアップを作成する(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)。また、事件に関連する証拠が入ったログファイルをコピーする。

8. **事件のすべての影響を一掃する** これには、悪意のコードの感染ファイル、不適切なデータ(海賊版ソフトウェアなど)、トロイの木馬のファイル、事件がもたらしたシステムへの変更に対する作業が含まれる。システムが完全に侵害された場合は、一から再構築するか、正しいことがわかっているバックアップからリストアする。

9. **悪用されたすべての脆弱性を見つけて修正する** 事件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することで起きた可能性が高い。そのような脆弱性を見つけて取り除くか軽減し、再発しないようにすることが重要である。

10. **運用が通常に戻ったことを確認する** 事件により影響を受けたデータ、アプリケーション、その他のサービスが通常の運用に戻ったことを確認する。

11. **最終レポートの作成** このレポートには、事件処理プロセスを詳述する。また、何が起きたかを要約し、もし正式なインシデント対応能力があれば、どれだけ早く状況を処理し、リスクを軽減し、被害を制限できたかも記載する。

付録 J　連邦政府機関による事件報告の分類

政府民間機関は、事件をUS-CERTに報告するよう義務付けられており、その他の組織は、US-CERTおよび／または他の事件報告組織に報告する。事件報告組織は、報告されたデータを使って、報告元の団体に対して新しい脅威や事件の動向に関する情報を提供するため、この報告は有益である。

FISMAを支援するために、連邦政府機関はすべてのコンピュータセキュリティインシデントをUS-CERTに報告することが義務付けられている。組織は、US-CERTのCONOPS(Concept of Operations)に従って事件の分類を行い、CONOPSが規定する報告期限内に事件を報告する。事件に対するこれらの分類および記述は、CONOPSの開発中に、interagency body(省庁間で構成される団体)によって策定され合意されたものである。OMBは2007年5月、政府機関がUS-CERTに事件を報告する際に、それらの事件分類と報告期間に従うことを義務付けるメモランダム(memorandum)を公表した。[118]、以下の表は、2008年1月時点の、US-CERTの事件分類と報告期間を示すものである。

表J-1 US-CERTが規定する事件分類と報告期間

分類	名前	説明	報告期限
CAT0	実習／ネットワーク防御テスト	この分類は、内部／外部ネットワーネットワークの防御やレスポンスに関する(州の、連邦政府の、国の、国際的な)実習、および承認された活動テストを行う際に使用される。	この分類は、各政府機関が内部の実習のために使用するものである。したがって報告期限の指定はない。
CAT1	不正アクセス	許可なく連邦政府のネットワーク、システム、アプリケーション、データ等のリソースに論理的または物理的にアクセスすること。	事件の発生または発見から1時間以内。
CAT2	*サービス不能(DOS)	リソースを枯渇させることで、ネットワーク、システム、アプリケーションの正規の使用を妨害または阻害する攻撃。これには、この攻撃の被害者や参加者による活動が含まれる。	攻撃が続行中で、政府機関がその攻撃を軽減できない場合、事件の発生または発見から2時間以内。
CAT3	*悪意のコード	ウイルス、ワーム、トロイの木馬など、ホストに感染する、悪意のコード。ウイルス対策ソフトウェアによって隔離された悪意のロジックに関しては、報告する義務はない。	その日の内。ただし、それらのコードによる感染が政府機関全体に及ぶ場合は、事件の発生または発見から1時間以内。
CAT4	*不適切な使用	ネットワークまたはコンピュータの利用規定に違反すること。	週に一度。
CAT5	スキャン／プローブ／アクセスの試み	後に利用することを目的として、連邦政府機関のコンピュータ、開いているポート、プロトコル、サービス、またはそれらの組み合わせへのアクセスまたは識別を試みること。この活動がセキュリテ	月に一度。ただし、システムの分類が可能な場合は、事件の発見から1時間以内。

118 事件分類と報告期限に関する情報は、http://www.us-cert.gov/を参照のこと。.また、The OMB memorandum, M-07-16に関しては、http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdfを参照のこと。

		ィ侵害やサービス不能に直接結びつくわけではない。	
CAT6	調査	未確認の事件。悪質な活動または異常な活動である可能性があり、報告者によって、さらなるレビューが必要であると判断されるもの。	この分類は、現在調査中の事件を、他の事件と区別するためのものである。したがって報告期限の指定はない。

*事件の分類にかかわらず、個人情報の侵害が発生した場合は、発見から1時間以内に、US-CERTに報告すべきである。

本書記載の複合要素の事件に関しては、侵害に利用される手段をもとに分類を行う。たとえば、悪意のコードがルートレベルの不正アクセスを提供するとする。この場合事件は、悪意のコードによる事件として分類されるべきである。