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

Special Publication 800-83
後援：米国国土安全保障省

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

米国国立標準技術研究所による推奨

Peter Mell
Karen Kent
Joseph Nusbaum

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 800-83

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

米国国立標準技術研究所による推奨

Peter Mell
Karen Kent
Joseph Nusbaum

コンピュータセキュリティ

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

2005 **年** 11 **月**

米国商務省 長官

Carlos M. Gutierrez

技術管理局 技術担当商務次官

Michelle O'Neill

米国国立標準技術研究所 所長

William A. Jeffrey

コンピュータシステムの技術に関する報告書

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と国家安全保障関連を除く情報のプライバシ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 Publication 800 シリーズでは、コンピュータ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、普及活動と、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。

米国国立標準技術研究所、Special Publication 800-83
米国国立標準技術研究所、Special Publication 800-83、101 ページ（2005 年 11 月）

この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。

謝辞

本書執筆者である Peter Mell (NIST)、Karen Kent および Joseph Nusbaum (ともに Booz Allen Hamilton) は、本書草稿のレビューと技術内容に助言を与えてくれた同僚に感謝の意を表したい。とりわけ、本書の作成全体にわたって、鋭く洞察に満ちた助言を与えてくれた Tim Grance、Murugiah Souppaya (NIST)、Gagliano、Thomas Goff、および Pius Uzamere (3 人ともに Booz Allen Hamilton) に感謝したい。また、セキュリティの専門家である Mike Danseglio (Microsoft)、Kurt Dillard (Microsoft)、Michael Gerdes (Getronics RedSiren Security Solutions)、Peter Szor (Symantec)、Miles Tracy (連邦準備制度)、および Lenny Zeltser (Gemini Systems LLC) と、特に有益な意見や提案を提供してくれた会計検査院の代表者の方々にも、感謝の意を表したい。

米国国立標準技術研究所は、NIST Special Publication 800-83 に対する国土安全保障省の後援と支援に対しても深く感謝する。

商標について

目次

付録

図

表

本文書の概要

悪意のコード (malicious code) または悪意のソフトウェア (malicious software) とも呼ばれるマルウェア (malware) は、被害者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、可用性を損なったり、被害者を困らせたり混乱させたりする目的で、通常は気づかれないようにシステムに挿入されるプログラムのことである。マルウェアは多くのシステムにとってきわめて重大な外的脅威となっている。広範囲にわたって損害や混乱を引き起こし、多くの組織で大規模な復旧作業を強いられている。また、ユーザのプライバシを侵害するスパイウェアも、組織における大きな懸念となっている。プライバシを侵害するマルウェアは長年にわたり悪用されてきているが、スパイウェアが数多くのシステムに侵入して個人の活動を監視し金融詐欺を働くようになるのに従って、近年、さらに広い範囲で蔓延するようになってきている。組織は、マルウェアに関係するいくつかの似たような形態の脅威にも直面している。そのような形態の中で一般的になった脅威の 1 つにフィッシングがある。フィッシングは、コンピュータを巧みに利用して個人をだまし、秘密情報を開示させる。もう 1 つの一般的な脅威としてウイルスの偽情報がある。ウイルス偽情報は、新しいマルウェアの脅威に関する虚偽の警告である。

本文書では、組織がマルウェアインシデント防止対策を強化するための推奨事項を提示する。また、組織が持つインシデント対応能力を強化するために様々な推奨事項も提示し、特に広範囲に蔓延するマルウェアインシデントへの、これまで以上の備えを整えられるようにする。ここでの推奨事項は、ウイルス、ワーム、トロイの木馬、悪意のモバイルコード、混合攻撃、スパイウェア追跡クッキー、および攻撃者用ツール (バックドアやルートキットなど) を含む、いくつかの主要な形態のマルウェアに対処するものである。推奨の対象として、ネットワークサービス (電子メール、Web 閲覧、ファイル共有など) やリムーバブルメディアなど、各種の伝送メカニズムを取り扱う。

以下の推奨事項を実施することで、連邦政府の各省庁や機関においてマルウェアインシデントに対し、より効率的で効果的な対処活動が促進される。

組織はマルウェアインシデント防止対策を立て、実施すること。

組織は、現在および近い将来において利用される可能性が最も高い攻撃の媒介要素に応じて、マルウェアインシデント防止対策を立て、実施するべきである。防止のための手法の有効性は環境に左右される場合がある。たとえば、管理された環境においては有効な手法は、管理されていない環境においては効果がない場合がある。このため、組織では各自の環境やシステムに最も適した防止手段を選択する。マルウェアインシデント防止対策には、ポリシーについて考慮すべき事項、ユーザや IT スタッフを対象とする意識向上プログラム、および、脆弱性と脅威の軽減のための活動を盛り込む。

組織のポリシーがマルウェアインシデント防止に寄与することを確かなものにすること。

組織のポリシーステートメントが、ユーザや IT スタッフの意識向上、脆弱性の軽減、セキュリティツールの導入と設定といった、マルウェア防止を強化するための活動の基礎として使われるべきである。組織のポリシーにおいてマルウェア防止について考慮しなければならない事項を明確に規定していなければ、マルウェア防止活動を、一貫性を保ちながら効果的に実施することは難しい。マルウェア防止関連のポリシーは、柔軟に実施できるように、また頻繁に更新する必要がないように、可能な限り汎用性を持たせるべきであるが、ポリシーの意図と範囲が十分明確になる程度に具体的なものである必要もある。マルウェア防止に関連するポリシーには、遠隔地にいる作業者－組織によって管理されているシステムを使用している従業員と、組織の管理外のシステム (請負業者のコンピュータ、職員の私有コンピュータ、ビジネスパートナーのコンピュータ、携帯機器など) を使用している従業員の両方に関連する規程が含まれているべきである。

組織は意識向上プログラムにマルウェアインシデントの防止と対応に関する項目を組み入れるべきである。

組織は、マルウェアインシデント防止に関するユーザへのガイダンスを盛り込んだ意識向上プログラムを実施するべきである。マルウェアの拡散のしかた、マルウェアがもたらすリスク、すべてのインシデントを技術的に防止するのは不可能であること、および、インシデント防止におけるユーザの重要性を、すべてのユーザに意識させなければならない。また、意識向上プログラムを通じて、マルウェアインシデント対応に適用されるポリシーや手続き、たとえば、コンピュータでのマルウェアの検出方法、感染の疑いがある場合の報告方法、インシデント対応担当者の助けとなるようにユーザがとるべき措置などをユーザに認識させる必要もある。さらに、マルウェアインシデント防止に関与する IT スタッフを対象に、意識向上のための活動を実施して、具体的な作業に関するトレーニングを提供するべきである。

組織はマルウェアインシデント防止を助ける脆弱性軽減能力をつけるべきである。

組織は、マルウェアに悪用される可能性のある、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軽減するためのポリシー、プロセス、および手続きを文書化するべきである。脆弱性を軽減する方法は通常複数存在するため、パッチ管理、セキュリティ設定に関するガイドやチェックリストの適用、ホストのさらなるセキュリティ強化対策といったさまざまな手法を適切に組み合わせて、各種の脆弱性に対する効果的な技法がすぐに利用できるようにしておくべきである。

組織はマルウェアインシデントの封じ込めを助ける脅威軽減能力を持つべきである。

組織は、マルウェアがターゲットに対して影響を与える前にマルウェアを検出して阻止できるように、脅威を軽減するための作業を実施するべきである。脅威を軽減するための技術的な管理策として最も一般的に利用されているのが、ウイルス対策ソフトウェアである。NIST は、要件を満たすウイルス対策ソフトウェアを利用することが可能なすべてのシステムに、ウイルス対策ソフトウェアを導入することを強く推奨する。スパイウェアの脅威を軽減するため、スパイウェアの脅威を認識する能力を備えたウイルス対策ソフトウェアか、スパイウェアの検出と駆除を行う専用のユーティリティを、要件を満たすソフトウェアを利用することが可能なすべてのシステムで利用するべきである。そのほか、マルウェアの脅威の軽減に役立つ技術的な管理策として、侵入防止システム、ファイアウォール、ルータ、特定のアプリケーション構成設定などがある。NIST Special Publication 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）*』では、「System and Information Integrity（システムと情報の完全性）」というセキュリティ管理策群の中で、ワークステーション、サーバ、携帯コンピューティング機器、ファイアウォール、電子メールサーバ、リモートアクセスサーバといった各種のホストにおいて、マルウェアやスパイウェアに対する保護メカニズムを備えることを推奨している。

組織はマルウェアインシデント対応のための堅牢なインシデント対応手続きに関する能力をつけるべきである。

NIST Special Publication 800-61『*コンピュータセキュリティインシデント対応ガイド（Computer Security Incident Handling Guide）*』で定義されているように、インシデント対応手続きには、「準備」、「検知と分析」、「封じ込め／根絶／復旧」、「インシデント発生後の活動」の、4 つの主要なフェーズがある。マルウェアインシデント対応に関してフェーズおよびサブフェーズごとの主な推奨事項を以下に示す。

- **準備。**マルウェアインシデントに確実に効果的に対処できるように準備する。以下の措置を推奨する。

- マルウェア専用のインシデント対応ポリシーおよび手続きを作成する。
- マルウェアに関するトレーニングや訓練を定期的に実施する。
- 組織のマルウェアインシデント対応を調整する責任を負う数人の個人または少人数のチームを事前に編成する。
- 有害事象発生時に、インシデント対応担当者、技術スタッフ、管理者層、およびユーザの間で調整作業を維持できるように、いくつかの意思伝達メカニズムを設ける。

■ **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拡大す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えるよう努めるべきである。早期の検知は、感染するシステムの数を最小限に食い止めるのに役立つ。その結果、復旧作業が少なく済み、組織が被る損害の量も減る。以下の措置を推奨する。

- 技術的な管理策（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、侵入検知システムなど）により生成される、マルウェアに関する注意や警告を監視し、発生する可能性のあるマルウェアインシデントを識別する。組織がこのような監視を行うことによって、セキュリティの状態を変更することによりマルウェアインシデントを防止する機会が得られる。
- ユーザの報告、IT スタッフの報告、技術的な管理策などの主要な情報源から得られる、マルウェアインシデントに関するデータをレビューし、マルウェアに関連する活動を識別する。
- マルウェアの識別、現在実行中のプロセスの列挙やその他の分析処理を実行するための最新のツール類を収めた信頼のおけるツールキットを、リムーバブルメディア上に構築する。
- マルウェアに関連する各種のインシデントに対する適切な対処レベルを明確にする、一連の優先順位付けの条件を設ける。

■ **封じ込め。** マルウェアインシデントの封じ込めは、主に「マルウェアの拡散の阻止」と「システム障害の拡大阻止」の 2 つの要素により構成される。封じ込め措置は、ほとんどすべてのマルウェアインシデントに対して必要である。インシデントに対応する際には、早期の段階でどのような封じ込め手段を利用すべきかを組織で決めることが重要になる。封じ込めに関する決定は、組織が受容し得るリスクの程度を反映したものになるが、そうした決定を下す際の方針や手続きを設けておくべきである。この封じ込めの方針は、インシデント対応担当者が具体的な状況に応じて適切な組み合わせの封じ込め手段を選択できるようなものでなければならない。封じ込めに関して、誰が重要な決定を下す権限を持つのか、また、各種の措置がどのような状況のもとで適切であるのかを、組織のポリシーの中で明確化するべきである。封じ込めに関する具体的な推奨事項を以下に示す。

- 感染を識別する方法と、システムが感染した場合にとるべき措置を示した手順をユーザに提供しておくと役立つ可能性がある。ただし、マルウェアインシデントの封じ込めを主にユーザに頼ることは避けるべきである。
- 最新のウイルス対策ソフトウェアでマルウェアを識別し封じ込めることができない場合に備え、ほかのセキュリティツールを使用して封じ込めることができるよう準備しておく。また、未知のマルウェアのコピーをセキュリティソフトウェアのベンダに送付して分析してもらう体制を整えておく。また、新しい脅威への対処についてのガイダンスが必要となる場合に、インシデント対応の専門組織やウイルス対策ベンダなどの、信頼のおける第三者と連絡を取るようにすべきである。
- インシデントを封じ込めるため、マルウェアが使用している電子メールなどのサービスを停止または遮断できるよう準備しておき、そのような措置を講じた場合に生じる影響を理解し

ておく。また、別の組織がマルウェアインシデント対応のためにその組織のサービスを無効にする場合に生じる問題にも対応できるよう準備しておくべきである。

– マルウェアインシデントを封じ込めるために、たとえば、インターネットへのアクセスを中断する、システムをネットワークから物理的に切り離すなど、ネットワーク接続に一時的に制限をかけられるようにしておくべきであるが、このような制限によって組織の機能が受ける可能性がある影響について認識しておく必要がある。

多数のマルウェアインシデント、特に拡散するタイプのマルウェアインシデントを封じ込めるうえで、もう 1 つ重要な作業として、マルウェアに感染したホストの識別がある。感染したホストの識別は、コンピューティングの動的な性質（リモートアクセスやモバイルユーザなど）のために複雑になる場合が多い。規模の大きなマルウェアインシデントが発生する前に、ホストの識別に関する問題について慎重に検討しておく。そうすることによって、感染したホストを識別するための複数の方策を封じ込め作業の一部として利用できるようになる。識別に関して十分広範囲なアプローチを選択し、大規模なマルウェア問題の発生時に、選択したそれぞれのアプローチを効果的に実施するための手続きと技術的な能力を整備しておく。

■ **根絶。**根絶の主な目標は、マルウェアに感染したシステムからマルウェアを駆除することである。広範な根絶作業が潜在的に必要となるため、さまざまな状況に応じて各種の根絶手法を組み合わせて使用できるようにしておく。また、根絶と復旧の作業で予想し得る事態を想定した意識向上活動を実施することを検討するべきである。このような活動は、大規模なマルウェアインシデントが発生した際に生じる可能性のあるストレスを低減するのに役立つ。

■ **復旧。**マルウェアインシデントからの復旧には、感染したシステムの機能やデータの回復と、封じ込めのための一時的対策の解除の、2 つの側面がある。起こり得る最悪のシナリオについて慎重に考慮し、被害を受けたシステムを一から構築し直すのか、それとも既知の正常なバックアップから再構築するのかを含む復旧方法を決定する。封じ込めのための一時的対策（サービスや接続の中断など）を解除すべきタイミングは、発生したマルウェアインシデントが大規模な場合には、判断が難しいことが多い。インシデント対応チームでは、感染したシステムや感染する可能性のあるシステムの推定数が十分少なくなり、以降のインシデントによる影響がほとんどないと判断されるまで、封じ込めのための対策を維持するよう努めるべきである。ただし、サービスや接続の回復に伴うリスクについてはインシデント対応チームが評価すべきだとしても、最終的には管理職層が、インシデント対応チームの勧告や、封じ込めのための対策を維持することによる事業への影響に基づいて、実施すべき措置を決定する責任を負う。

■ **インシデント発生後の活動。**マルウェアインシデント対応はきわめて負担の大きい作業になる可能性があるため、大規模なマルウェアインシデントが発生したあとに得られた教訓について、しっかりとした評価を行い、同様のインシデントの再発を防ぐことが特に重要である。そのようなマルウェアインシデントへの対処から得られた教訓を把握することにより、組織はインシデント対応能力とマルウェアに対する防御を改善することができる。たとえば、セキュリティポリシーやソフトウェアの設定、マルウェア検出／防止ソフトウェアの導入に対する必要な変更点が明確になる。

現在および近未来における脅威を対象とする、マルウェアインシデントの防止・対応能力を確立する。

新しいマルウェアの脅威は絶え間なく発生するため、現在と近未来の両方の脅威に対応し、長期的将来の脅威にも対応できるように変更・追加を行うことのできる、十分な堅牢性と柔軟性を備えた、マルウェアインシデントの防止・対処能力を確立すべきである。マルウェアとマルウェア防御策は、それぞれの改善に呼応して進化を続けている。このため組織は、最新の脅威のタイプと、それ

それのタイプの脅威に対抗するために利用できるセキュリティ管理策について、最新の情報を入手すべきである。新しい分類の脅威がますます深刻なものになるのに応じて、組織は脅威の軽減に適切な管理策を計画して実施する必要がある。すべての組織において、新しく出現する脅威と保護に必要な能力を認識することが、マルウェアインシデント防止に向けた活動に組み込まれるべきである。

1. 序論

1.1 作成機関

本文書は、Federal Information Security Management Act of 2002（2002 年施行の連邦情報セキュリティマネジメント法、以下、FISMA と称す）、公法 107-347 に基づくその法的責任を推進するために、米国国立標準技術研究所（National Institute of Standards and Technology、以下、NIST と称す）により作成された。

NIST は、すべての政府機関システムに十分な情報セキュリティを提供するための標準とガイドライン（最小限の要件を含む）を作成する責任を負うが、このような標準およびガイドラインは国家安全保障に関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（Office of Management and Budget、以下 OMB と称す）の通達（Circular）A-130 の第 8b（3）項『政府機関の情報システムの保護（Securing Agency Information Systems）』の要件と一致しており、これは A-130 の付録 IV「重要部門の分析（Analysis of Key Sections）」で分析されているとおりである。補足情報は、A-130 の付録 III に記載されている。

このガイドラインは、連邦政府機関による使用を目的として用意されたが、非政府組織が自己責任において使用することもできる。その場合は出自を明らかにすることが望ましいが、著作権の制約はない。

本文書におけるいっさいは、商務長官が法的権威に基づき連邦政府機関に対して義務付け、拘束力を有する標準およびガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威を変更したり、これらに取って代わったりするものと解釈してはならない。

1.2 目的と範囲

本文書の目的は、マルウェアがもたらす脅威についての組織の理解を促し、マルウェアインシデントに伴うリスクの緩和に寄与することにある。本文書では、マルウェアの主要な分類について背景となる情報を提供しているほか、マルウェアインシデントの防止と、マルウェアインシデントへの効果的かつ効率的な対処に関する、現実的かつ実用的な指針も提供している。

1.3 対象とする読者

本文書は、コンピュータセキュリティのスタッフ、プログラム管理者、技術サポートのスタッフおよび管理者、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、ネットワーク管理者など、マルウェアインシデントの防止、マルウェアインシデントに対する準備、およびマルウェアインシデントへの対応を担当する人々を対象として作成されている。また、一部の内容は、マルウェアの脅威についてより深く理解しようと努め、インシデント防止とインシデント対応のための効果的な措置を必要としているエンドユーザも対象としている。

1.4 構成

本文書の残りは 4 つの主要セクションに分かれている。セクション 2 では、各種のマルウェアの分類を定義、説明し、比較する。セクション 3 では、何層かの管理策を通じてマルウェアインシデントを防止するための推奨事項について説明する。セクション 4 では、マルウェアインシデント対応プロセスについて、管理された環境と管理されていない環境における、検知、封じ込め、根絶、および復旧の実践的な方針を中心に解説する。セクション 5 では、将来予想されるマルウェアの開発や傾向について触れる。

巻末にはいくつかの付録と参考資料を記載している。付録 A では、本文書全体を通じて説明している、インシデント防止と封じ込めの技術についてまとめている。また、それらの技術がさまざまな環境や状況においてどのような効果があるのかについても、一般的なガイダンスを提供している。付録 B には、簡単なマルウェア対応シナリオを用意している。これらは対応チームにおける議論や訓練のひな形として利用できる。付録 C および D には、それぞれ用語集と略語の一覧を掲載している。付録 E には参考書籍および雑誌の一覧を、付録 F にはオンラインの資料を記載している。読者はこれらの資料を活用することで、マルウェアや、マルウェアインシデント防止、マルウェアインシデント対応について、より深く理解することができる。付録 G には索引を設けている。

2. マルウェアの分類

*悪意のコード*または*悪意のソフトウェア*とも呼ばれる*マルウェア*[1]は、被害者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、可用性を損なう目的や、被害者を困らせたり混乱させたりする目的で、通常は気づかれないようにシステムに挿入されるプログラムのことである。ウイルスやワームなどのマルウェアはこのようなきわめて悪質な機能を、少なくとも最初のうちはユーザに気づかれないように実行する目的で作られている。1980 年代から、マルウェアはしばしば個人や組織に迷惑や不便をかけてきたが、こんにちではほとんどのシステムにとって、広範囲にわたって損害や混乱を引き起こすきわめて重大な外的脅威であり、ほとんどの組織において大規模な復旧作業を強いられている。また、ユーザのプライバシ侵害を目的とする*スパイウェア*も、組織における大きな懸念事項になっている。プライバシを侵害するマルウェアは長年にわたり悪用されてきているが、2003 年から 2004 年にかけては、数多くのシステムに侵入して個人の活動を監視し金融詐欺を働くスパイウェアが流行し、さらに広い範囲にわたって悪用されるようになった。

このセクションでは以降のセクションにおける説明の基礎として、マルウェアの各種の分類の概要を示す。マルウェアには、ウイルス、ワーム、トロイの木馬、悪意のモバイルコードや、これらを組み合わせた混合攻撃がある[2]。マルウェアにはまた、バックドア、ルートキット、キーストロークロガーなどの攻撃ツールや、スパイウェアとしての追跡クッキーも含まれる。各分類における議論では、マルウェアが通常どのような方法でシステムに入り込み感染し伝染するのか、一般的な意味でどのような動作をするのか、どのような目的を持っているのか、そして、システムにどのような影響を与えるのかについて、それぞれ説明する。また、このセクションでは、マルウェアではないものの、しばしばマルウェアと関連して議論されるいくつかの脅威についても簡単に説明する。さらに、マルウェアの歴史にも簡単に触れ、過去と現在におけるマルウェアの分類ごとの相対的な重要度を示す。最後に、マルウェアのカテゴリを比較して、類似点や相違点を明らかにする。

2.1 ウイルス

*ウイルス*は、自己複製、つまり、自分自身のコピーを作成し、そのコピーをほかのファイルやプログラム、またはコンピュータに配布するように設計されている。ウイルスはそれぞれ感染のメカニズムを持っている。たとえば、ワードプロセッサファイルに悪意のマクロコードを挿入するなどして、自分自身をホストプログラムやデータファイルに忍び込ませることができる。ウイルスの*ペイロード*には、ウイルスの目的に応じたコードが含まれている。ペイロードは、比較的害のないもの（人に迷惑をかける、個人的な意見を表明するなど）から、きわめて有害なもの（個人情報を他人に転送する、システムを消去するなど）まで多様である。また、ウイルスの多くは*トリガ*を持っている。トリガとは、ペイロードの実行を引き起こす条件のことで、通常はユーザの操作（ファイルを開く、プログラムを実行する、電子メールの添付ファイルをクリックするなど）が伴う。2 種類の主なウイルスとして、オペレーティングシステム（OS）によって実行される*コンパイル型ウイルス*と、アプリケーションによって実行される*インタプリタ型ウイルス*がある。このセクションでは両方の種類のウイルスについて説明するほか、ウイルスが検出を免れるために利用している各種の難読化技法についても説明する。

2.1.1 コンパイル型ウイルス

*コンパイル型ウイルス*は、コンパイラプログラムにより、そのソースコードが OS で直接実行できる形式に変換されたウイルスである。コンパイル型ウイルスは通常次の 3 つに分類される。

---

[1] malware という言葉は、malicious software の短縮形である。

[2] セキュリティコミュニティの中では、マルウェアの各分類の厳密な違いについてコンセンサスが形成されているわけではない。この文書で提示している定義は、マルウェアの各分類について一般に受け入れられている特徴に基づいたものである。

- **ファイル感染型。***ファイル感染型ウイルス*は、自分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、コンピュータゲームなどの実行可能プログラムに添付する。プログラムに感染したウイルスは、システム上のほかのプログラムに伝染するだけでなく、感染した共有プログラムを使用するほかのシステムにも伝染する。ファイル感染型ウイルスとして最もよく知られた 2 つのウイルスに、Jerusalem と Cascade がある[3]。

- **ブートセクタ感染型。***ブートセクタウイルス*は、ハードディスクドライブのマスタブートレコード（MBR）や、ハードディスクドライブまたはリムーバブルメディア（フロッピーディスクなど）のブートセクタに感染する。ブートセクタとはドライブやディスクの先頭の領域で、ドライブやディスクの構造に関する情報が格納される場所である。ブートセクタには、ホストの起動時に OS をブートするために実行されるブートプログラムが収められている。ハードディスクドライブの MBR は、コンピュータの BIOS（基本入出力システム）がブートプログラムをロードすることができるディスク上のユニークな場所である。フロッピーディスクなどのリムーバブルメディアは、ブート可能でなくてもシステムを感染させることができる。感染したディスクがコンピュータのブート時に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ぺいが容易であり、成功の確率が高く、コンピュータを完全に運用不能にするほどの害を及ぼすおそれがある。コンピュータがブートセクタウイルスに感染した場合の兆候は、ブート中にエラーメッセージが表示されたり、ブートができなくなったりするというものである。ブートセクタウイルスの例としては、Form、Michelangelo、Stoned などがある。

- **複合感染型。***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。

コンパイル型ウイルスは、ファイルへの感染に加えて感染対象システムのメモリに常駐することが可能であり、そのため、新しいプログラムが実行されるたびにプログラムがウイルスに感染する。コンパイル型ウイルスの中で、ブートセクタウイルスは*メモリ常駐型*である可能性が最も高い。メモリ常駐型のウイルスは長期間にわたってメモリ内にとどまるため、非メモリ常駐型のウイルスと比べて、感染するファイルの数が多くなり、通常のシステム運用が妨害される頻度が高い。

2.1.2 インタプリタ型ウイルス

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。それほど技能のない攻撃者でも、インタプリタ型ウイルスを入手し、ソースコードを手直しして、他者に配布することが可能である。1 つのインタプリタ型ウイルスにはしばしば数十の派生版が存在し、それらのほとんどはオリジナルに些細な変更を加えただけのものである。インタプリタ型ウイルスには、主にマクロウイルスとスクリプトウイルスの 2 種類がある。

*マクロウイルス*は、最も流行していて成功率の高いウイルスの一種である。これらのウイルスは自分自身をワードプロセッサファイルやスプレッドシートなどのアプリケーション文書に添付し、対象アプリケーションのマクロプログラミング言語を利用して実行や伝染を行う。Microsoft Office をはじめとする数多くの著名なソフトウェアパッケージでは、複雑で反復的な作業を自動化するためにマクロプログラミングの機能が利用されているが、マクロウイルスでもこれらの機能が利用される。ユーザ

[3] これらの事例のほか、このセクション全体にわたって引用しているそのほかの事例の詳細については、付録 F の「技術資料サイト」の項に記載されているウイルス情報 Web サイトを参照。このセクションに記載されているコンパイル型ウイルスの事例は、そのほとんどが 1990 年代初期からのものであり、それらは当時最も一般的な形式のマルウェアであった。

はマクロ機能を有するアプリケーションにより作成された文書を共有することが多いため、これらのウイルスは急速に蔓延する傾向が強い。また、マクロウイルスの感染が発生すると、ファイルを作成したり開いたりするためにプログラムで使用されているテンプレートにウイルスが感染する。いったんテンプレートがウイルスに感染すると、そのテンプレートを使用して作成されたり開かれたりする文書もすべて感染することになる。よく知られたマクロウイルスの例としては、Concept、Marker、Melissa などのウイルスがある。

*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。たとえば、一部の Microsoft Windows システムに搭載されている Windows スクリプトホスト機能は、VBScript で記述されたスクリプトを実行することができる。よく知られたスクリプトウイルスの例としては、First や Love Stages がある。

2.1.3 ウイルスの難読化技法

ウイルスのほとんどは 1 つ以上の*難読化技法*を用いて作成されている。これは、ウイルス自身が検出されにくくなるようにするウイルス作成手法である。ウイルスの検出が困難になれば、広範囲に拡散する可能性が高くなる。よく使用されている難読化技法を以下に示す[4]。

- **自己暗号化と自己復号。**ウイルスの中には、自分のウイルスコード本体を暗号化および復号することによって、自分自身を直接的な検査から隠ぺいするものがある。暗号化を利用するウイルスは、暗号化を幾層にもわたって利用したり、ランダムな暗号化キーを使用したりすることがある。この結果、基礎となるコードが同じであっても、実際の個々のウイルスの見かけはそれぞれ異なる。

- **ポリモーフィズム。**ポリモーフィズムは、特に堅牢性の高い自己暗号化形式である。ポリモーフィックウイルスは、一般にデフォルトの暗号化設定にいくつかの変更を加えるほか、復号コードも変更する。ポリモーフィックウイルスでは、基礎のウイルスコードの内容は変更されず、暗号化によって外見だけが変更される。

- **メタモーフィズム。**メタモーフィズムは、ウイルス自身の内容を隠すのではなく変更を加えるという考えに基づいている。ウイルスはいくつかの方法で変更を加えることができる。たとえば、不要なコードの並びをソースコードに追加したり、ソースコードの断片の順序を変更したりといった方法である。そのあと、変更を加えたコードを再コンパイルすることによって、オリジナルとは外見がまったく異なるウイルス実行ファイルが作成される。

- **ステルス型。**ステルス型ウイルスは、各種の技法を用いて感染の特徴を隠ぺいする。たとえば、ステルス型ウイルスの多くは OS ファイルの一覧表示機能を操作して、報告されるファイルのサイズがオリジナルファイルのサイズとなるようにし、感染したそれぞれのファイルに付加されたウイルスのサイズが含まれないようにする。

- **武装。**武装の目的は、ウイルス対策ソフトウェアや専門家が逆アセンブルやトレースなどの手段を通じてウイルスの機能を分析することができないように、ウイルスを作成することである。

- **トンネリング。**トンネリングを利用したウイルスは、自分自身を OS の低レベル部分に忍び込ませ、低レベルの OS 呼び出しを横取りできるようにする。自分自身をウイルス対策ソフト

[4] ウイルスの難読化技法の一覧については、『*The Art of Computer Virus Research and Defense (コンピュータウイルスの研究と防御の技術)*』(Peter Szor 著、Addison-Wesley、2005 年) を参照。

ウェアよりも下位に配置することで、ウイルスはウイルス対策ソフトウェアから検出されないように OS を操ろうとする。

ベンダ各社のウイルス対策ソフトウェア製品は、難読化技法がどのように組み合わせて使用されていてもそれらを無効化することを試みるように設計されている。難読化技法のうち、自己暗号化、ポリモーフィズム、ステルス型といった、比較的古いものについては、通常はウイルス対策ソフトウェアによって効果的に処理される。しかし、メタモーフィズムなど比較的新しく複雑なものは、今もなお出現しているため、ウイルス対策ソフトウェアでも対応がかなり難しくなる可能性がある。

2.2 ワーム

*ワーム*は、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。ウイルスとは異なり、ユーザが関与しなくても自分自身の機能の完全なコピーを作成して実行することができる。ワームはウイルスと比べて短期間のうちにより多くのシステムに感染する潜在能力を持っていることから、攻撃者の間で一般的になりつつある。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（「2.7.1」の項を参照）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。ワームは主に、ネットワークサービスワームと大量メールワームの 2 つに分類される。

*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。ひとたびワームがシステムに感染すると、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*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。

2.3 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[5]。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。トロイの木馬は以下の 3 つの特徴のいずれかに合致する傾向がある。

[5] トロイの木馬を *trojan* と呼ぶこともある。

- 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。たとえば、アプリケーションのパスワードを収集するゲームなどがある。
- 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。

トロイの木馬は検知が困難な場合がある。多くはシステム上で自己の存在を隠し、元のプログラムの機能を正常に実行するよう特別に作られているため、ユーザやシステム管理者が気づかないことがある。新しいトロイの木馬の多くでは、検知を避けるためにウイルスで使用されている手法と同じ難読化技法もいくつか使われている。

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ウェアなどのソフトウェア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。セクション2.7では、トロイの木馬を通じて送り込まれることが多い、悪意のあるツールについていくつか説明している。

トロイの木馬はシステムで技術上の深刻な問題を引き起こす可能性がある。たとえば、トロイの木馬によって正規のシステム実行可能ファイルが置き換えられ、その結果、特定の機能が誤って実行されたり、特定の機能が完全に失われたりすることがある。特に、スパイウェア関連のトロイの木馬は、意図的にシステムに侵入し、多数の変更をシステムに加え、自分自身を削除した場合に、状況によってはシステムが全く機能しなくなるような深刻なダメージが引き起こされるような手法で導入させることによって、多数のシステムに壊滅的な被害を与えてきている。また、トロイの木馬やトロイの木馬によってインストールされるツールがリソースを大量に消費し、感染したシステムにおいて顕著なパフォーマンスの低下を引き起こす可能性がある。よく知られているトロイの木馬として、SubSeven、Back Orifice、Optix Pro などがある。

2.4 悪意のモバイルコード

*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[6]。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。悪意のモバ

[6] モバイルコードの詳細については、NIST Special Publication (SP) 800-28『*Guidelines on Active Content and Mobile Code*』を参照。この文書は Computer Security Resource Center (CSRC) の Web サイト (http://csrc.nist.gov/publications/nistpubs/) で入手できる。

イルコードでよく使われる言語には、Java、ActiveX、JavaScript、VBScript などがある。Nimda は、悪意のモバイルコードの中でも最もよく知られたものの 1 つであり、JavaScript を使って書かれていた。セクション2.5において、Nimda に関する補足情報を提供している。

2.5 混合攻撃

*混合攻撃*は、複数の感染手段や伝送手段を利用するマルウェアの一種である。よく知られた Nimda「ワーム」は実際は混合攻撃の一例であり[7]、以下の 4 つの配布手段が用いられていた。

- **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 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でスキャンし、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。

混合攻撃は、上記の配布手段を利用することに加え、インスタントメッセージや P2P ファイル交換ソフトウェアなどのサービスを介して拡散する可能性がある。Nimda と同様の混合攻撃事例の多くが、誤ってワームと呼ばれることがある。これは、ワームの特徴の一部を備えているためである。しかし実際には、Nimda はウイルス、ワーム、そして悪意のモバイルコードの特徴を兼ね備えている。混合攻撃の別の例として、Bugbear がある。Bugbear は、大量メールワームとネットワークサービスワームの両方の機能を備えていた。混合攻撃は、単独の手段しか持たないマルウェアよりも複雑であるため、作成することはかなり難しい。

混合攻撃は、複数の手段を必ずしも同時に実行する必要はなく、複数の感染を順番に実行することもできる。この方法は、とりわけトロイの木馬をシステムに送り込んでインストールするための手段として流行してきている。たとえば、システムへの侵入に成功したウイルス、ワーム、または悪意のモバイルコードが、トロイの木馬のコピーをインストールして実行することができる。以後、トロイの木馬が、スパイウェアをシステムにインストールするなど、さらに悪意のある行為を実行できる。

2.6 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[8]。*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。*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

---

7 Nimda の詳細については、『*CERT®/CC 報告 CA-2001-26 Nimda ワーム (CERT®/CC Advisory CA-2001-26 Nimda Worm)*』(http://www.cert.org/advisories/CA-2001-26.html で入手可能) を参照。

8 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。

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。

ユーザの個人情報を捉えて送り届ける別の方法として、Web バグを使用したものがある。*Web バグ*は、Web ページや電子メールの HTML（ハイパーテキストマークアップ言語）コンテンツの中で参照される、Web サイト上のごく小さな画像である。この画像は、HTML コンテンツを閲覧しているユーザに関する情報を収集すること以外の目的は持っていない。Web バグは通常、1 ピクセル分しかないため、ユーザには通常見えない。追跡クッキーと同様に、Web バグも市場調査会社に利用されることが多い。Web バグはユーザの IP（インターネットプロトコル）アドレスや Web ブラウザの種類などの情報を収集したり、さらに追跡クッキーにアクセスしたりすることができる。このような操作ができるため、Web バグをスパイウェアとして利用し、ユーザの個人的なプロファイルを作成することが可能である。

2.7 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。「2.7.1」～「2.7.6」の各項では、いくつかのよく知られている攻撃ツールについて説明する。

2.7.1 バックドア

*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。また、以下のような特殊な機能を持つバックドアもある。

+ **ゾンビ。***ゾンビ*はしばしば*ボット*と呼ばれ[9]、ほかのシステムを攻撃させるためにシステムにインストールされるプログラムである。最も一般的なゾンビの種類としては DDoS *エージェント*がある。攻撃者は一度に多数のエージェントにリモートコマンドを発行して、標的に対して組織的な攻撃を実行することができる。よく知られた DDoS エージェントに、Trinoo や Tribe Flood Network がある。

+ **リモート管理ツール。**名前が示すとおり、*リモート管理ツール* (RAT) は、インストール先のシステムに対して、遠隔地にいる攻撃者が必要に応じてアクセスできるようにする。ほとんどの RAT はシステムの機能やデータへのフルアクセスを許可する。このため、システムの画面に表示されるすべての内容を監視したり、システムに接続されている Web カメラやマイク、スピーカなどのデバイスを遠隔から制御したりすることができる。よく知られている RAT に、SubSeven、Back Orifice、NetBus などがある。

2.7.2 キーストロークロガー

*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[10]。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。キーストロークロガーの例としては、KeySnatch、Spyster、KeyLogger Pro などがある。

2.7.3 ルートキット

*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。ルートキットの例としては、LRK5、Knark、Adore、Hacker Defender などがある。

2.7.4 Web ブラウザプラグイン

*Web ブラウザプラグイン*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

---

[9] ゾンビはボットと呼ばれることが多いが、用語としての「ボット」は、実際には任意の機能を自動的に実行するプログラムを意味する一般用語である。したがって、ボットは害のない場合とある場合の両方の可能性があり、複数の種類のマルウェアを技術的にボットと呼ぶことができる。同じ種類のボットを実行しているコンピュータのグループのことを*ボットネット*と呼ぶ。

[10] 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。

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[11]。

2.7.5 電子メールジェネレータ

マルウェアは*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。

2.7.6 攻撃ツールキット

攻撃者の多くは、システムを探ったり攻撃したりすることが可能な、複数の異なる種類のユーティリティやスクリプトを収めたツールキットを使用する。マルウェアやそのほかの手段によって、ひとたび、システムのセキュリティが侵害されると、攻撃者はツールキットをダウンロードしてそのシステムにインストールする。すると、ツールキットは、ツールキットがインストールされたシステムのセキュリティをさらに侵害したり、ほかのシステムを攻撃したりするために使用される。攻撃ツールキットに見られる典型的なプログラムの種類には以下のものがある。

- **パケットスニファ。***パケットスニファ*は、有線または無線のネットワーク上でネットワークトラフィックを監視し、パケットを捕捉するように設計されている。一般に、パケットスニファはすべてのパケットを捕捉するように設定したり、特定の性質（特定の TCP ポート、特定の送信元 IP アドレス、特定の送信先 IP アドレスなど）を持つパケットだけを捕捉するように設定したりすることができる。パケットスニファのほとんどは*プロトコルアナライザ*でもある。つまり、個々のパケットに基づいてストリームを再構築し、数百または数千にのぼる任意の異なるプロトコルを使用している通信を解読することができる。

- **ポートスキャナ。***ポートスキャナ*は、システム上のどのポートが開いているのか（つまり、システムがそのポートを経由した通信を許可しているかどうか）を遠隔から調べようとするプログラムである。攻撃者はポートスキャナを利用することで、潜在的な標的を識別することができる。

- **脆弱性スキャナ。***脆弱性スキャナ*は、ローカルシステムまたはリモートシステムの脆弱性を探し出すプログラムである。攻撃者は脆弱性スキャナを利用して、首尾よく悪用できそうなホストを見つけることができる。

- **パスワードクラッカ。**OS やアプリケーションのパスワードを割り出す（クラッキングする）ことのできる、さまざまなユーティリティが出まわっている。ほとんどのクラッキングユーティリティは、パスワードの推測を試みることができるほか、可能性のあるすべてのパスワードを総当たり的に試みることもできる。符号化または暗号化されたパスワードに対して総当たりによる攻撃を行うのに要する時間は、使用されている暗号化手法のタイプや、パスワードそのものの工夫の度合いによって大幅に異なる。

- **リモートログインプログラム。**攻撃ツールキットには、ほかのシステムへのリモートログインに使用できる SSH や telnet などのプログラムが含まれていることが多い。攻撃者はこれら

[11] ダイヤラの中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。

のプログラムを、セキュリティ侵害されたシステムの制御やシステム間でのデータ転送といった多様な目的に使用することができる。

+ **攻撃ツール。**攻撃ツールキットには、ローカルシステムまたはリモートシステムに対して攻撃を仕掛けることのできる各種のユーティリティやスクリプトが収められていることが多い。攻撃には、システムのセキュリティ侵害やサービス運用妨害など、さまざま目的を持つものがある。

攻撃ツールキットに含まれるプログラムの多くは、善意と悪意の両方の目的に使用できるものである。たとえば、パケットスニファとプロトコルアナライザは、ネットワーク管理者がネットワーク通信の問題を解決する際に使用することが多いが、攻撃者がほかの通信を傍受するのにも使用できる。セキュリティ管理者は、システムにおけるユーザのパスワードの強度をテストするためにパスワードクラッカを使用することがある。攻撃ツールキットに含まれていることが多い一部の種類のプログラムは、特定のオペレーティングシステムに診断ユーティリティや管理ユーティリティとして組み込まれている。したがって、これらの種類のプログラムが 1 つでもシステムに存在するからといって、必ずしも悪意のある問題が発生したことを示すわけではない。

2.8 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 つの形態について簡単に説明する。最初に、フィッシングの手法について説明する。フィッシングは、ユーザをだまして金融情報やそのほかの機密データを開示させるために使用される。フィッシング攻撃では、マルウェアやそのほかの攻撃ツールがシステムに送り込まれることが非常に多い。もう 1 つの脅威として、偽ウイルス情報がある。これらは、新たなマルウェアの脅威に関する虚偽の警告である。フィッシングと偽ウイルスはどちらも*ソーシャルエンジニアリング*に完全に依存している。ソーシャルエンジニアリングとは、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。

2.8.1 フィッシング

*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[12]。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[13]。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

---

12 最近のフィッシング攻撃の事例など、フィッシングの詳細については、フィッシング対策作業部会の Web サイト（http://www.antiphishing.org/）を参照。また、米国連邦取引委員会（FTC）より発行されている『*How Not to Get Hooked by a "Phishing" Scam*（*「フィッシング」詐欺にだまされない方法*）』も参考となる。この文書は http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm で入手できる。

13 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。

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。

2.8.2 偽ウイルス

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。よく知られた偽ウイルスに Good Times がある。

2.9 マルウェアの歴史

さまざまな種類のマルウェアについて、それらの相対的な重要度を把握するため、マルウェアに関する歴史について知っておくと役に立つ[14]。

コンピュータウイルスの概念は、実はコンピューティングの初期の時代に形成されていた。史上最も古いウイルスは害のないいたずらで、1980 年代初期までは悪意のあるウイルスが公の場で問題にされることはなかった。最初に作成されたワームは 1970 年代後期のもので、これも害はなく、システムの保守を目的とするものであった。1980 年代後期まではマルウェアが一般的になることはなく、そのあいだ、最も一般的だったのはコンパイル型ウイルスであり、特にブートセクタウイルスが流行していた。当時、ウイルスの作者は、自分のウイルスが検出を免れることができるようにいくつかの難読化技法も開発していた。1988 年、悪名高い Morris ワームが登場し、ネットワークに接続された数千ものコンピュータを混乱に陥れた。トロイの木馬が登場し始めたのは 1980 年代中頃である。

1990 年代初期のあいだは、マルウェアの状況は概ね変わらず、依然としてコンパイル型ウイルスが悪意のコードの形態として流行していた。しかし、1990 年代後半になって、コンピューティングにおけるいくつかの重要な変化に伴い、マルウェアに新たな機会が与えられた。まず、パーソナルコンピュータの台数が大幅に増加した。加えて、電子メールクライアントの使用や、マクロ言語を備えたワードプロセッサやスプレッドシートなどのソフトウェアの使用が拡大した。それに応じて、ウイルスの作者はインタプリタ型ウイルスの開発を始め、電子メールを通じてそれらを拡散させるようになった。また、同様の機能を持った自己完結型のワームの開発も始めた。インタプリタ型ウイルスは、一般にコンパイル型ウイルスと比べて作成や変更がしやすいという利点があったため、それほど技能のないプログラマでもウイルスを作成することができた。2 つのインタプリタ型マルウェア攻撃である Melissa ウイルス（1999 年）と LoveLetter ワーム（2000 年）はそれぞれ、数百万台ものシステムに

---

[14] この項で説明している内容は、『*Threat Assessment of Malicious Code and Human Threats（悪意のあるコードと人的脅威の脅威アセスメント）*』（Lawrence E. Bassham、W. Timothy Polk（いずれも NIST）共著、http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html）、『*A Short History of Computer Viruses and Attacks（コンピュータウイルスと攻撃の簡単な歴史）*』（Brian Krebs（Washington Post）著、http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26?start=15&per=18）、および『*Computer Virus Timeline（コンピュータウイルス年表）*』（Infoplease 著、http://www.infoplease.com/ipa/A0872842.html）を参考としている。

影響を及ぼした。トロイの木馬と RAT を組み合わせた BackOrifice などもまた、1990 年代後半に流行した。

2000 年以降は、ワームがマルウェアの形態として広まっている。ワームのほうがウイルスよりもはるかに急速に拡散するため、ウイルスの作者はウイルスよりもワームを好むことが多い。ウイルスの中でもブートセクタウイルスは相対的に一般的ではなくなった。その主な原因はフロッピーディスクの使用が減ったことである[15]。これに対して、マクロウイルスは最も一般的なウイルスのタイプとなっている。2001 年には、初めての大規模な混合攻撃である Nimda が登場し、大規模な混乱を引き起こした。Nimda はウイルス、ワーム、そして悪意のモバイルコードの特徴を兼ね備えたものであった。最近では、Web ブラウザや HTML ベースの電子メールが普及したことにより、悪意のモバイルコードによる攻撃がますます一般化してきている。しかし、悪意のモバイルコードは、まだワームほどには広まっていない。別の傾向として、ワーム、トロイの木馬、悪意のモバイルコードなどのマルウェアによって、ルートキット、キーストロークロガー、バックドアなどの攻撃ツールが感染したシステムに送り込まれる事例が増えている。

2.10 まとめ

マルウェアは、ほとんどのシステムにとって最も重大な外的脅威となっており、損害を引き起こし、ほとんどの組織において広範囲にわたる復旧作業が必要となる。マルウェアは主に以下のように分類される。

- **ウイルス。** ウイルスは、自分自身をホストプログラムやデータファイルに忍び込ませることによって、自己複製する。ウイルスはユーザの操作（ファイルを開く、プログラムを実行するなど）を通じて起動されることが多い。ウイルスはさらに以下の 2 つに分類される。
  - **コンパイル型ウイルス。** コンパイル型ウイルスはオペレーティングシステムによって実行される。コンパイル型ウイルスの種類には、自分自身を実行可能プログラムに添付するファイル感染型ウイルス、ハードディスクドライブのマスタブートレコードやリムーバブルメディアのブートセクタに感染するブートセクタウイルス、および、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合わせ持つ複合感染型ウイルスがある。
  - **インタプリタ型ウイルス。** インタプリタ型ウイルスはアプリケーションによって実行される。さらにこの分類の中で、マクロウイルスとスクリプトウイルスがある。前者は、アプリケーションのマクロプログラミング言語の機能を利用してアプリケーションの文書や文書テンプレートに感染する。後者は、OS のサービスによって処理されるスクリプト言語が認識するスクリプトに感染する。
- **ワーム。** ワームは自己複製および自己完結型のプログラムで、通常はユーザの関与なしに自分自身を実行する。ワームはさらに以下の 2 つに分類される。
  - **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、ネットワークサービス内の脆弱性を利用してほかのシステムに伝染し感染する。
  - **大量メールワーム。** 大量メールワームは電子メール添付ウイルスに似ているが、既存のファイルに感染することはなく、自己完結型である。

[15] ブートセクタウイルスは 1990 年代初期に最も流行していた。当時は、ファイルの格納やシステム間でのファイルの転送の手段としてフロッピーディスクが最も一般的であった。電子メールやファイル交換ソフトウェアといった、より高速なファイル転送手段が普及するにつれて、攻撃者はそれらの手段を利用して、より急速に拡散する別の種類のマルウェアを開発し始めるようになった。しかし、ブートセクタウイルスも依然として発生しており、ブート時にシステムに存在する CD や DVD そのほかのリムーバブルメディアを通じてそれらのウイルスがシステムに感染する可能性がある。

- **トロイの木馬。**トロイの木馬は、見かけ上は良性を装いながら、実際には悪意のある目的を潜ませている、自己完結および非複製型のプログラムである。トロイの木馬は、既存のファイルを悪意のあるものに置き換えるか、悪意のある新しいファイルをシステムに追加する。しばしば、別の攻撃ツールをシステムに送り込む。

- **悪意のモバイルコード。**悪意のモバイルコードは、悪意のある目的のもとに、通常はユーザによる明示的な指示なしに、リモートシステムからローカルシステムに送信され、ローカルシステム上で実行されるソフトウェアである。悪意のモバイルコードでよく使われる言語には、Java、ActiveX、JavaScript、VBScript などがある。

- **混合攻撃。**混合攻撃は複数の感染手段や伝送手段を利用したものである。たとえば、ウイルスとワームの伝染手段を組み合わせた混合攻撃が可能である。

- **追跡クッキー。**追跡クッキーは多数の Web サイトからアクセスされる永続クッキーであり、第三者がこれを利用してユーザの振る舞いのプロファイルを作成できる。追跡クッキーは Web バグと組み合わせて用いられることが多い。Web バグは、Web ページや電子メールの HTML コンテンツの中で参照される、Web サイト上のごく小さな画像である。この画像の唯一の目的は、コンテンツを閲覧しているユーザに関する情報を収集することである。

- **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。これらのツールを利用することにより、攻撃者は感染したシステムやそのデータへの不正アクセスやその不正利用、あるいは、さらなる攻撃の実行が可能になる。よく知られた攻撃ツールとして以下のものがある。

  – **バックドア。**バックドアは、特定の TCP または UDP ポートでコマンドを傍受する、悪意のプログラムである。ほとんどのバックドアでは、攻撃者はパスワードの取得や、任意のコマンドの実行などの一連の特定の操作をシステム上で実行することが可能になる。バックドアの種類として、ゾンビ（ボットとも呼ばれる）とリモート管理ツールがある。ゾンビは、あるシステムにインストールされることによってほかのシステムを攻撃する。リモート管理ツールは、ツールがインストールされたシステムにおいて、遠隔地にいる攻撃者が必要に応じてシステムの機能やデータにアクセスできるようになる。

  – **キーストロークロガー。**キーストロークロガーはキーボードの使用を監視し記録する。キーストロークロガーには、攻撃者がシステムからデータを取得する必要があるものや、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。**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。通常、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を隠す。このため、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加えたのかについて判断することはたいへん難しい。

  – **Web ブラウザプラグイン。**Web ブラウザプラグインは、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。攻撃者はしばしば、スパイウェアとして機能しブラウザのあらゆる使用を監視する悪意のプラグインを作成する。

  – **電子メールジェネレータ。**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、マルウェアやスパイウェア、スパムなどの電子メールを大量に作成してほかのシステムに送信できる。

– **攻撃ツールキット。**攻撃者の多くは、複数の異なる種類のユーティリティやスクリプトを収めたツールキットを使用する。これらを使用するとシステムの探査や攻撃を行うことができる。このようなツールには、パケットスニファ、ポートスキャナ、脆弱性スキャナ、パスワードクラッカ、リモートログインプログラム、攻撃用プログラムおよびスクリプトなどがある。

マルウェアに加えて、マルウェアに関連付けられることが多いマルウェア以外の一般的な脅威もいくつか存在する。フィッシングは、コンピュータベースの手法を用いてユーザをだまし、金融情報やほかの機密性の高い情報を開示させる。フィッシング攻撃では、マルウェアや攻撃ツールがシステムに送り込まれることが多い。他の悪意のあるコンテンツの脅威として、新たなマルウェアの脅威に関する虚偽の警告を発する偽ウイルスがある。

表 2-1 は、ウイルス、ワーム、トロイの木馬、悪意のモバイルコード、追跡クッキー、および攻撃ツールについて、主な特徴をもとに比較したものである。混合攻撃については、ほかに分類されたマルウェアの機能が組み合わされている場合があるため、これらの分類を用いて具体的な特徴を定義することはできない。

表 2-1 マルウェアの分類別の違い

特徴	ウイルス	ワーム	トロイの木馬	悪意のモバイルコード	追跡クッキー	攻撃ツール
自己完結型か？	×	○	○	×	○	○
自己複製型か？	○	○	×	×	×	×
どのような伝染手段をとるか？	ユーザの操作	自己伝染	該当せず	該当せず	該当せず	該当せず

3. マルウェアインシデントの防止

このセクションでは、組織内でのマルウェアインシデント防止のための推奨事項を提示する。防止のための 4 つの主な要素として、ポリシー、意識向上、脆弱性の軽減、そして脅威の軽減がある。ポリシーにおいてマルウェア防止を確実にうたうことは、予防的な管理策を実施するための基礎となる。人的ミスを通じて発生するインシデントの数を減らすためには、すべてのユーザを対象としたマルウェアに関する一般的な意識向上プログラムだけでなく、マルウェア防止関連の活動に直接関与する IT スタッフのために詳細な意識向上トレーニングを確立し維持することがきわめて重要である。脆弱性の軽減に向けた努力を惜しまなければ、潜在的な攻撃経路や手段のいくつかを取り除くことができる。ウイルス対策ソフトウェアやファイアウォールなどの脅威軽減の手法やツールを組み合わせて実装すれば、脅威によるシステムやネットワークへの攻撃を阻止できる。3.1 項から 3.4 項では、これらの領域について詳しく説明し、マルウェアに対する効果的な多重防御を組織が備えるためには、推奨事項の各分類に記載されたガイダンスを実施する必要があることを示す。

マルウェア防止のアプローチを策定する際には、現在および近い将来に使用される可能性が最も高い攻撃の経路や手段に注意する。また、システムがどの程度適切に管理されているのかを考慮する（たとえば、管理された環境、管理されていない環境など）。これは各種の予防的アプローチの実効性に大きく関係する。さらに、ウイルス対策ソフトウェアの配置やパッチ管理プログラムといった既存機能を、マルウェア防止の取組みに組み入れるべきである。しかし、マルウェアインシデントの防止にどれだけの労力を注いだとしても、インシデントは発生する（未知の種類の脅威や、人的エラーなど）という意識を持つことが必要である。この理由から、セクション 4 で説明するように、マルウェアインシデントへのしっかりとした対応能力を組織で整え、マルウェアが引き起こす可能性のある損害を限定し、データやサービスを効率よく復元できるようにしておく必要がある。

3.1 ポリシー

組織は、自身のポリシーにおいてマルウェアインシデントの防止を確実にうたうべきである。これらのポリシーステートメントを、ユーザや IT スタッフの意識向上、脆弱性の軽減、脅威の軽減（それぞれ 3.2 項から 3.4 項を参照）など、マルウェア防止のほかの取組みの基礎とする。マルウェア防止に関する考慮事項をポリシーの中で明確に示していなければ、マルウェア防止の活動を組織全体で一貫して効果的に実施することは難しい。マルウェア防止に関連したポリシーはできるだけ汎用性のあるものにする。そうすることで、ポリシーの実施の自由度が高まり、ポリシーを頻繁に更新する必要性を軽減できる。ただし、ポリシーの意図と範囲が十分明確になる程度に具体化することも必要である。組織によってはマルウェアポリシーを独立して設けている場合もあるが、マルウェア防止の考慮事項の多くは利用規定ポリシーなどのほかのポリシーに含まれている。そのため、独立のマルウェアポリシーがほかのポリシーの内容と一部重複することがある[16]。マルウェア防止に関するポリシーには、遠隔地にいる作業者－組織によって管理されているシステムを使用している作業者と、組織の管理外のシステム（請負業者のコンピュータ、職員の自宅のコンピュータ、提携企業のコンピュータ、携帯機器など）を使用している作業者に関する規程が含まれているべきである。

[16] たとえば、利用規定ポリシーの多くでは、組織のコンピューティングリソースを組織の支援にのみ利用すべきであることが明記されている。コンピューティングリソースの個人的な利用はマルウェアインシデントの一般的な発生源である。しかし、組織ではほかにもいくつかの理由でコンピューティングリソースの個人的な利用を許可しない場合がある。したがって、このポリシー考慮事項についてはマルウェアポリシーよりも組織の利用規定ポリシーで対応したほうが適切である。

マルウェア防止に関連したポリシーの考慮事項には、次のようなものがある[17]。

- 組織外から持ち込まれるメディアを使用する前にスキャンしてマルウェアの有無を確かめる。
- 電子メールの添付ファイル（.zip ファイルなどの圧縮ファイルを含む）を、必ずローカルのドライブまたはメディアに保存し、開く前にスキャンする。
- 特定の種類のファイル（.exe ファイルなど）について、電子メールによる送受信を禁止する。また、マルウェアの脅威への緊急の対処として、それ以外の特定の種類のファイルを一定期間ブロックする。
- マルウェアの転送に利用されることが多いユーザアプリケーションなどの不要なソフトウェア（たとえば、外部インスタントメッセージの個人的な利用、デスクトップ検索エンジン、P2P ファイル交換ソフトウェアサービス）、必要のないサービス、組織が提供するサービスと重複するサービス（電子メールなど）であり、かつマルウェアによって悪用されうる脆弱性を持つサービスについて、それらの利用を制限または禁止する。
- ユーザによる管理者レベル特権の使用を制限する。この措置は、ユーザを通じてシステムに持ち込まれたマルウェアによって利用される特権を制限するのに役立つ。
- OS やアプリケーションのアップグレードおよびパッチに関して、システムを最新に保つ。
- リムーバブルメディア（フロッピーディスク、CD（コンパクトディスク）、USB（ユニバーサルシリアルバス）フラッシュドライブなど）の使用を制限する。特に、誰でもアクセスできるキオスクのような感染の危険性の高いシステムに対してこの制限を強化する。
- 各種のシステム（ファイルサーバ、電子メールサーバ、プロキシサーバ、ワークステーション、PDA など）、およびアプリケーション（電子メールクライアント、Web ブラウザなど）において必要となる予防ソフトウェア（ウイルス対策ソフトウェア、スパイ検出／駆除ユーティリティなど）のタイプを指定し、それらのソフトウェアの構成と保守に必要な高次の要求事項（ソフトウェアの更新頻度、システムスキャンの範囲および頻度など）を列挙する。
- インターネットを含むほかのネットワークへのアクセスについて、組織で承認しセキュリティ保護を施したメカニズムを通じてのみ、アクセスを許可する。
- ファイアウォールの構成変更は、必ず正式な手続きを経て承認されるようにする。
- 各種の送信元（内部 Web サーバ、別組織の Web サーバなど）から使用してもよいモバイルコードの種類を指定する。
- モバイルデバイスの使用を、信頼のおけるネットワークに限定する。

3.2 意識向上

効果的な意識向上プログラムは、組織の IT システムや情報を利用する際の適切な行動規程を説明している。したがって、意識向上プログラムには、マルウェアインシデントの頻度や深刻さの低減に役立つ、マルウェアインシデントの防止に関するユーザガイダンスが含まれるべきである。組織内部のすべてのユーザに、マルウェアの侵入、感染、および拡散の方法や、マルウェアがもたらすリスク、あるいは、技術的管理策ではすべてのインシデントは防げないこと、および、インシデントを防ぐうえでユーザが重要な役割を果たすことを意識させるべきである。また意識向上活動においては、たとえば、在宅勤務者や出張中の職員が、ホテルや喫茶店などの外部の環境にて遭遇する、

[17] これらの考慮事項はすべてマルウェアインシデントの防止促進を目的としているが、その多くはインシデントの検出や封じ込めにも役立つ可能性がある。

さまざまな環境の特徴についても考慮する。加えて、組織の意識向上プログラムでは、3.1 項で説明した、組織のポリシーや手続きに記載されているマルウェアインシデント防止に関する考慮事項、およびマルウェアインシデントを回避するために一般に推奨されている実践事項をカバーするべきである。実践事項の例として次のものがある。

- 未知または既知の送信者から送られた、疑わしい電子メールや添付ファイルを開かない。
- Web ブラウザで疑わしいポップアップウィンドウをクリックしない。
- 悪意のあるコンテンツが含まれている可能性が少しでもありそうな Web サイトにアクセスしない。
- マルウェアに関連付けられている可能性が高いファイル拡張子（*.bat*、*.com*、*.exe*、*.pif*、*.vbs* など）のファイルを開かない。
- 各種のセキュリティ管理メカニズム（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、パーソナルファイアウォールなど）を無効にしない。
- 管理者レベルのアカウントを通常のシステム運用に使用しない。
- 信頼のおけないソースからアプリケーションをダウンロードしたり実行したりしない。

また、セクション 4 で説明するように、マルウェアインシデント対応に適用するポリシーや手続き、たとえば、システムが感染したかどうかを識別する方法や、感染の疑いを報告する方法、インシデント対応を支援するためにユーザが行う必要のありそうな措置（ウイルス対策ソフトウェアの更新、システムスキャンによるマルウェアの有無の確認）などをユーザに認識させる。また、ユーザは、重大なマルウェアインシデントに関する全ての通知の正当性を確認するために、それらの通知がどのようにして伝達され与えられるのかについて知らされていなければならない。さらに、インシデントを封じ込めるために一時的に環境に加えられる可能性のある変更、たとえば、感染したシステムをネットワークから切断することや、特定の種類の電子メール添付ファイルをブロックすることなどについてもユーザに認識させるべきである。

意識向上活動の一環として、組織は、犯罪者がユーザをだまして情報を開示させる手口についてユーザを教育するべきである。また、2.8.1項で説明したフィッシング攻撃を回避するための推奨事項をユーザに提供すべきである。そのような推奨事項の例として次のものがある。

- 金融情報や個人情報を求める電子メールには絶対に返信しない。そのような情報について組織から電子メールでたずねることはしない。電子メールは許可を得ていない第三者によって監視されやすいからである。代わりに、正規の電話番号を通じて電話で問い合わせるか、組織の既知の Web サイトアドレスを Web ブラウザに入力する。電子メールに記載されている連絡先情報は使用しない。
- 電子メールへの返信や、要求していないのに表示されるポップアップウィンドウに対して、パスワードや暗証番号などのアクセスコードを入力しない。そのような情報は組織の正規の Web サイトにのみ入力する。
- 疑わしい電子メール添付ファイルは、たとえ既知の送信者からのものであっても開かない。予期していない添付ファイルを受信した場合は、送信者に連絡して（電子メール以外の電話などの手段が望ましい）、添付ファイルが正規のものであることを確認する。
- 疑わしい電子メールや要求していない電子メールには、いっさい返信しない。電子メールアドレスを、悪意を持つ第三者のメーリングリストから削除するよう要求することは、その電子メール

アドレスの存在と実際に利用しているという確証を第三者に与えてしまい、さらなる攻撃の試みを招くおそれがある。

ユーザの意識向上プログラムは、マルウェアインシデントの頻度や深刻さの軽減に役立つが、その効果は、脆弱性や脅威の軽減（それぞれ 3.3 項と 3.4 項を参照）のための技術的な管理策による効果と比べると小さいのが普通である。したがってマルウェアインシデント防止のための主要な手段として、ユーザの意識向上に頼るべきではない。意識向上プログラムは、あくまでもインシデントに対抗する追加的な保護を提供するために技術的管理策を補うものであるべきである。

ユーザのための意識向上プログラムはまた、マルウェアインシデント防止に関与する IT スタッフ（セキュリティ管理者、システム管理者、ネットワーク管理者など）にとっても意識向上活動の基礎として役立つ。すべての IT スタッフメンバは、マルウェア防止に関するなんらかの基本的なレベルの意識を持つべきであり、各個人は、それぞれの責任範囲に関わるマルウェア防止関連作業についてトレーニングを受けるべきである。また継続的な活動として、一部の IT スタッフメンバ（セキュリティチームやインシデント対応チームのメンバが最もあてはまる）は、新たなマルウェア脅威に関する速報の受信とレビュー、組織への想定リスクの評価、しかるべき IT スタッフメンバに対する新たな脅威の通知を行うことにより、感染を防止できるようにするべきである。マルウェアインシデント対応に関連した IT スタッフの意識向上活動については、セクション 4 で説明する。

3.3 脆弱性の軽減

セクション 2 で述べたように、マルウェアは、オペレーティングシステム、サービス、およびアプリケーションの脆弱性を悪用することによってシステムを攻撃することが多い。したがって、脆弱性の軽減はマルウェアインシデントを防止するうえで非常に重要である。結論として、新たな脆弱性が発表されてから間もなく、あるいは、脆弱性が公に認知される前にマルウェアがリリースされる場合は特に、脆弱性の軽減が非常に重要である。脆弱性は通常、パッチの適用によるソフトウェアの更新やソフトウェアの再構成（脆弱性のあるサービスの無効化など）といった、1 つ以上の手段によって軽減することができる。

絶え間なく発見される新たな脆弱性への対処を含め、脆弱性の軽減には困難が伴うため、組織は、脆弱性を軽減するためのポリシー、プロセス、および手続きを文書化し、軽減作業を支援するための脆弱性管理プログラムの策定を検討するべきである[18]。また、自組織の脆弱性を絶えず評価し、脆弱性軽減作業の優先順位が適切に設定されるようにするべきである。新たな脆弱性や影響範囲が広い新種のマルウェアの脅威に関する情報は、インシデント対応チーム・組織（U.S. Computer Emergency Readiness Team（US-CERT）など）が発行する勧告、ベンダのセキュリティ速報、ウイルス対策ソフトウェアベンダからのマルウェアに関する勧告などの複数の情報源を通じて収集するべきである[19]。さらに、新たな脆弱性や脅威に関する情報を評価し、適切な軽減手段を決定して、情報を該当する当事者に配布するためのメカニズムを確立する。軽減作業の進捗を追跡するための手段も用意しておく。

単独の措置では、ほとんどの脆弱性について十分な軽減が行えないことから、脆弱性軽減には多重防御の原則を用いてアプローチするべきである。3.3.1 項から 3.3.3 項では、脆弱性軽減技法の 3

[18] 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。

[19] 2005 年 10 月に MITRE Corporation が発表した同社の Common Malware Enumeration（CME）プロジェクトでは、新種の重大なマルウェアの脅威を個々に識別するための標準の識別子が確立されている。ウイルス対策ベンダ各社では同一のマルウェアに対して異なる名称を付けることが多い。そのため、ベンダ速報を購読していたり、複数のウイルス対策製品から警告を受け取ったりしていると、混乱する可能性がある。CME プロジェクトの目的は、すべてのウイルス対策製品で使用可能な標準の識別子を提供することにある。CME の詳細については、http://cme.mitre.org/を参照。

つの一般的なタイプである、パッチ管理、最小権限、およびその他のホスト強化措置について説明する[20]。組織は脆弱性の軽減に加えて、マルウェアが脆弱性を悪用する機会を阻止することにフォーカスした、脅威の軽減措置も実施するべきである。ウイルス対策ソフトウェアなどのセキュリティツールは、マルウェアが標的に到達する前にそれを検出し阻止することができる。脅威の軽減は、ユーザをだまして悪意のあるファイルを実行させるような、脆弱性を利用しないマルウェアに対して特に重要である。また、影響範囲が広い新種の脅威による攻撃がすぐに実行される可能性が高く、組織に脆弱性軽減のための適切な選択肢がないような状況においても、脅威の軽減はきわめて重要である。たとえば、新たな脆弱性に対応したパッチが入手できない場合が考えられる。3.4 項では、脅威の軽減に役立つセキュリティツールを中心に説明する。

3.3.1 パッチ管理

システムへのパッチの適用は、オペレーティングシステムやアプリケーションに存在する既知の脆弱性を軽減するためのごく一般的な手段である。パッチ管理にはいくつかの手順が伴う。たとえば、そのパッチの重要性の評価、パッチを適用した場合と適用しない場合の影響の評価、各パッチの十分なテスト、管理された方法によるパッチの適用、パッチの評価と決定のプロセスの文書化などである。マルウェアに悪用される可能性が高い新しい重大な脆弱性が発表されてから、その脆弱性を標的としたマルウェアが実際にリリースされるまでの時間が、月単位から週単位または日単位へと短縮されてきているため、インシデントの防止に十分な速さでパッチを配備することが、ますます困難になってきている。新しいパッチを十分にテストするためには数週間ほどかかることが多いため、パッチを組織全体に即座に配備することが不可能であったり、賢明な策ではないことも多い。場合によっては、パッチ以外の脆弱性軽減技法や脅威軽減措置を用いたほうが安全である。また、パッチの十分なテストが完了し適用可能であると判断された場合であっても、組織内の脆弱性のあるすべてのマシン、特にリモートシステム（在宅勤務者など）にパッチを確実に適用することが困難であることも多い。とはいえ、パッチの適用はマルウェアインシデントのリスクを低減する最も効果的な手段の 1 つであり、システムへのパッチの適用が間に合わなかったためにマルウェアの成功を許した事例は多い。セクション 4 でも述べるが、パッチ管理はインシデントへの対応においても重要な技法である。

3.3.2 最小権限

最小権限の原則とは、最低限の権限のみを該当するユーザ、プロセス、およびホストに付与するようホストを設定することである。マルウェアは、脆弱性を首尾よく悪用するために管理者権限を必要とするものが多いため、最小権限はマルウェアインシデントの防止に役立つ可能性がある。インシデントが実際に発生しても、最小権限を事前に適用しておくことで、マルウェアに起因する損害を最小限に抑えられる可能性がある。通常、最小権限は組織のサーバやネットワークデバイスで採用されるが、ユーザから管理者権限を削除することを目的として、ユーザのデスクトップやラップトップで採用されることもある。最小権限の実装とサポートには多大なリソースが必要になる可能性がある。たとえば、ユーザは管理者特権がないと OS やアプリケーションの更新をインストールできないことがある。最小権限は、管理されていない環境よりも管理された環境の中で適用されることのほうが多い。

3.3.3 そのほかのホスト強化措置

ホストに対して継続的にパッチを適切に適用し、最小権限の原則に可能な限り従うことに加えて、組織はマルウェアインシデントの可能性をさらに減らすことが可能なそのほかのホスト強化措置を実装することを検討するべきである。そのような措置の例として次のものがある。

---

[20] 脆弱性の軽減に役立つ可能性のある手順がほかにも多数存在する。ここに示す技法は、ほとんどすべてのシステムのセキュリティ保護に適用できるが、マルウェアに対する保護の場合に特に有用である。

- 脆弱性を含む可能性のある不必要なサービス（特にネットワークサービス）を無効にするか、または削除する。
- セキュリティ保護されていないファイル共有をなくす。ファイル共有はワームの感染メカニズムとしてよく使われる。
- OS やアプリケーションのデフォルトのユーザ名とパスワードを削除または変更する。マルウェアはこれらを利用してシステムへのアクセス権を不正に取得する可能性がある。
- ネットワークサービスへのアクセスを許可する前に必ず認証を行う。
- バイナリやスクリプトの自動実行を無効にする。

OS やアプリケーションの設定ガイドやチェックリストを活用して、管理者がホストのセキュリティを一貫性をもって効果的に保護できるようにする[21]。通常、設定ガイドやチェックリストには、デフォルトのセキュリティレベルを強化するための推奨設定が記載されているほか、システムのセキュリティを保護するための具体的な手順が記載されていることもある。また、軽減されていない脆弱性を明確化するために脆弱性の評価を定期的に実施し、それらの脆弱性に対応するための計画を立てる[22]。システムに存在する既知のすべての脆弱性についてすでに対応済みである場合でも、脆弱性の評価を定期的に実施することが依然として重要である。これは、通常のシステム保守活動において誤って脆弱性軽減措置を排除してしまう可能性があるためである。たとえば、パッチをインストールしたために、誤って別のパッチが削除されてしまったり、セキュリティ設定が安全でないデフォルト設定に変更されてしまったりする可能性がある。

3.4 脅威の軽減

3.3 項で触れたように、脆弱性を軽減するための作業に加えて、マルウェアが標的に影響を及ぼす前にマルウェアを検出し阻止できるように、脅威を軽減するための作業を実施する。この項では、マルウェアの脅威を軽減することのできるいくつかの種類のセキュリティツール（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、侵入防止システム（IPS）、およびファイアウォールとルータ）について説明する。また、これらの各分類について、ツールが持つ標準的な機能、ツールが対応するマルウェアの種類や攻撃の経路と手段の種類、およびマルウェアの検出と阻止のためにツールで使用されている手法を説明する。ツールの実装、構成、管理に際しての推奨事項とガイドラインについても触れるほか、ツールの欠点や各ツールがほかのツールを補完する方法についても説明する。さらに、脅威の軽減に役立つ可能性のあるクライアントとサーバのアプリケーション設定についても述べる。

3.4.1 ウイルス対策ソフトウェア

ウイルス対策ソフトウェアは、マルウェアの脅威を軽減するために最もよく使用されている技術的な管理策である。マルウェアの標的となることが多いオペレーティングシステムやアプリケーションにとって、ウイルス対策ソフトウェアがインシデント防止のための必需品となっている。ウイルス対策ソフトウェアには数多くのブランドが存在するが、そのほとんどは、次の推奨機能を通じて同様の保護を提供する。

- 起動ファイルやブートレコードなどの重要なシステムコンポーネントをスキャンする。

---

21 http://csrc.nist.gov/pcig/cig.html では、NIST から発行されている、各種のオペレーティングシステムやアプリケーションのチェックリストと実装ガイドを入手できる。また、NIST SP 800-70『*IT 製品のためのセキュリティ設定チェックリストプログラム（Security Configuration Checklists Program for IT Products）*』（http://csrc.nist.gov/checklists/）も参照。

22 脆弱性評価の詳細については、NIST SP 800-42『*ネットワークセキュリティテストにおけるガイドライン（Guideline on Network Security Testing）*』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照。

- システムでの活動をリアルタイムに監視して疑わしい活動がないか確認する。たとえば、電子メールの送受信のたびにすべての電子メールの添付ファイルをスキャンし、既知のウイルスがないか調べるのが一般的である。ウイルス対策ソフトウェアは、ユーザがファイルをダウンロードするとき、開くとき、または実行するときに、リアルタイムスキャンを自動的に実施するように設定すべきである。このようなスキャンのことを*アクセス時スキャン*と呼ぶ。

- 電子メールクライアント、Web ブラウザ、ファイル転送プログラム、インスタントメッセージソフトウェアといった、一般的なアプリケーションの動作を監視する。ウイルス対策ソフトウェアでは、システムへの感染やほかのシステムへのマルウェアの拡散に使用される可能性が最も高いアプリケーションが関与する活動を監視する。

- ファイルをスキャンし、既知のウイルスがないかを調べる。ファイルシステムの感染を特定できるように、すべてのハードディスクドライブを定期的にスキャンするよう、また任意で、ほかのストレージメディアについても同様にスキャンするようにウイルス対策ソフトウェアを設定する。また、ユーザが必要に応じて手動でスキャンを起動できるようにもしておく。このようなスキャンのことを*要求時スキャン*と呼ぶ。

- 一般的な種類のマルウェアである、ウイルス、ワーム、トロイの木馬、悪意のモバイルコード、混合攻撃だけでなく、キーストロークロガーやバックドアなどの攻撃ツールについても特定する[23]。ほとんどのウイルス対策製品では、スパイウェア検出の機能も強化されてきている。3.4.2 項で説明するように、スパイウェア検出／駆除ユーティリティを使用して、堅牢なスパイウェア対処機能をまだ備えていないウイルス対策製品を補完することができる。

- ファイルの感染除去（ファイルの内部からマルウェアを駆除すること）および、ファイルの隔離（あとで感染除去や検査ができるように、マルウェアが含まれているファイルを隔離した場所に格納しておくこと）を行う。マルウェアが駆除されて元のファイルが復元されるという理由により、通常は、ファイルの隔離よりもファイルの感染除去のほうが好ましい。しかし、感染したファイルの多くは感染除去できない。したがって、ウイルス対策ソフトウェアは、感染したファイルの感染除去を試み、感染除去できないファイルについては隔離するか削除するように設定すべきである。

3.4.1.1 項から 3.4.1.3 項では、ウイルス対策ソフトウェアの検出精度、配備、および管理に関する補足情報と推奨事項を説明する。また、ウイルス対策ソフトウェアの欠点についても触れる。

3.4.1.1 ウイルス対策ソフトウェアの検出精度

ウイルス対策ソフトウェア製品は主として、既知のマルウェアが持つ一定の特徴を探し出すことによってマルウェアを検出する。このような一定の特徴のことを*シグネチャ*と呼ぶ。シグネチャは既知のマルウェアを識別するのにたいへん効果があり、既知のマルウェアの新たな派生版（オリジナルにわずかな変更が加えられたマクロウイルスなど）を識別するのにも適切な手段となることが多い。通常、大手のウイルス対策ベンダ各社は、新種の重要な脅威に対するシグネチャを数時間以内に

[23] あらゆる種類のマルウェアや攻撃ツールの中で、ルートキットは従来から最も検出が困難なマルウェアである。これは、OS をカーネルレベルで変更することが多く、ウイルス対策ソフトウェアに見つからないようにしているためである。Windows システムでは、Microsoft が Windows 対応の「マルウェアの削除ツール」と呼ばれる無償のユーティリティを提供している。このユーティリティは、特定の一般的なマルウェアの脅威（主に一般的なワームやルートキット）がないかを検査し、それらの駆除を試みる。このツールは Automatic Updates または Microsoft Update を通じて自動的にシステムにインストールできる。あるいは、Microsoft の Web サイト（http://www.microsoft.com/japan/security/malwareremove/default.mspx）から直接ダウンロードまたは実行できる。このツールは少数の一般的な脅威だけを検出するように作成されているため、ウイルス対策ソフトウェアを補完するものであり、代替となるものではない。このツールの詳細については、Microsoft Knowledge Base（MSKB）の記事 890830（http://support.microsoft.com/?id=890830）を参照。

公開している。脅威を分析し、シグネチャを作成してテストし、文書と一緒に配布しなければならないことを考えると、ベンダ各社による対応には目を見張るものがある。

シグネチャは既知の脅威がベースとなっているため、まったく新種のマルウェアを識別するには効果がない。このようなマルウェアに対応するため、ウイルス対策ベンダ各社はヒューリスティック（発見的）技法を製品に組み込んでいる。これらの技法は、ファイルの持つ数多くの特徴を調べることによって未知のマルウェアを識別するように設計されている。一般に用いられているヒューリスティック技法としては、たとえば、ファイルに疑わしいコードシーケンスがないかを検索し、ファイルの動作をシミュレートして異常な活動を探し出す技法がある（つまり、ファイルを仮想マシンの中で実行し、その動作を監視する）。残念ながら、ヒューリスティック技法では害のないコンテンツが誤って悪意のあるものと分類されてしまうことがある。このことを*フォールスポジティブ*と呼ぶ。フォールスポジティブはユーザやサポートスタッフにかなりの不便をかける可能性があるため、ほとんどのウイルス対策製品ではヒューリスティック技法の使用が、デフォルトとして「中」または「低」のレベルに設定されている。この設定によってフォールスポジティブの数は減少するが、ウイルス対策ソフトウェアによる新たなマルウェア脅威の検出の失敗、すなわち*フォールスネガティブ*が増えてしまう。どのようなレベルのヒューリスティック技法を用いたとしても、ウイルス対策ソフトウェアでは新たなマルウェア脅威の検出について高い精度を達成することはできない。しかし、シグネチャが十分最新であれば、既知の脅威の識別に優れた能力を発揮する。したがって、マルウェアの検出精度を向上させるために、ウイルス対策ソフトウェアのシグネチャやソフトウェア更新を最新に保つ必要がある。

3.4.1.2 ウイルス対策ソフトウェアの配置と管理

ウイルス対策ソフトウェアはマルウェアインシデントを防止するうえでたいへん重要であるため、NIST では各組織に対し、要求を満たすウイルス対策ソフトウェアが利用可能なすべてのシステムに、ウイルス対策ソフトウェアを導入することを強く推奨している[24]。ウイルス対策ソフトウェアは、OS のインストール後に可能な限り早くインストールした後、最新のシグネチャとウイルス対策ソフトウェアパッチを使用して更新するべきである（ウイルス対策ソフトウェア自身の既知の脆弱性をすべて取り除くため）。次に、感染の有無を確認するためにウイルス対策ソフトウェアによるシステムの完全スキャンを実行する。システムのセキュリティを支援するために、ウイルス対策ソフトウェアは、マルウェアを検出し阻止する効果が継続するように、適切に設定・維持されなければならない。

管理された環境では、ウイルス対策管理者によって定期的に管理・監視される、集中管理されたウイルス対策ソフトウェアを使用するべきである。ウイルス対策管理者は通常、組織全体におけるウイルス対策シグネチャとソフトウェア更新の入手、テスト、承認、配信に関する責任を負う。一般に、ユーザに対しては、ウイルス対策ソフトウェアを各自のシステムで無効にしたり削除したりできないようにし、重要な設定も変更できないようにする。ウイルス対策管理者は、システムで最新のウイルス対策ソフトウェアが使用されており、そのソフトウェアが正しく設定されていることを定期的に確認する。この情報は集中管理されたウイルス対策管理ソフトウェアを通じて入手可能であることが多い。この情報はまた、スキャンや、ネットワークログイン時に実行されるシステム検査、そのほかの方法を通じて収集することができる。これらすべての推奨事項を実施することは、組織が強固で一貫性のあるウイルス対策を組織全体に導入する際の、強力なサポートとなる。

管理されていない環境、特に、ユーザが各自のシステムを完全に制御できるような環境では、ウイルス対策ソフトウェアが一貫性のない状態で導入・管理される可能性が高い。管理されていない環境を持つ組織は、管理された環境に移行することを検討するべきである。管理されていない環境では、組織は特に意識向上活動に重点を置く必要がある。組織は、ローカルシステム管理者およびユーザに対してシグネチャ更新を求める通知の定期的な送信、ソフトウェアを最新に保つことの重要性に関する知識を増やすための意識向上活動の実施、システムを更新するための手順を追った説明書の配布、新種の重大な脅威が発生しウイルス対策シグネチャの更新が必要になった場合のローカルシステム管理者およびユーザへの通知を実施するべきである。また、組織は、ローカルシステム管理者およびユーザに対して、ウイルス対策シグネチャとソフトウェアの更新を自動的に頻繁に（少なくとも毎日）確認し、速やかに更新のダウンロードとインストールが実施されるように各自のウイルス対策ソフトウェアを設定することを奨励するべきである。

集中管理されたウイルス対策を導入している組織では、対策の実施において、十分な冗長性と容量を持たせることで、通常時のニーズとピーク時のニーズに確実に対応できるようにすべきである。

---

[24] 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）*』では、「システムおよび情報の完全性（SI）（System and Information Integrity）」というセキュリティ管理策群の中で、ウイルス対策ソフトウェアのための具体的な推奨事項について説明している。管理策「#SI-3、悪意のあるコードからの保護（Malicious Code Protection）」では、「情報システムは、悪意のあるコードからの保護機能（自動更新機能を含む）を実装する」ことを推奨している。また、以下のような補足的なガイダンスが述べられている。「組織は、情報システムの重要な入口と出口（ファイアウォール、電子メールサーバ、リモートアクセスサーバなど）および、ネットワーク上のワークステーション、サーバ、またはモバイルコンピューティング機器において、対ウイルス保護メカニズムを導入する。組織は、悪意のあるコード（ウイルス、ワーム、トロイの木馬など）を検出し根絶するための対ウイルス保護メカニズムを使用する。悪意のあるコードは、(i) 電子メール、電子メール添付ファイル、インターネットアクセス、リムーバブルメディア（フロッピーディスクやコンパクトディスクなど）、またはそのほかの一般的な手段を通じて、あるいは、(ii) 情報システムの脆弱性を悪用することによって送り込まれる。対ウイルス保護メカニズム（最新のウイルス定義を含む）の新しいリリースが利用可能になった場合は常に、組織の構成管理ポリシーおよび手続きに沿って、それらを更新する。複数のベンダのウイルス対策ソフトウェア製品を使用することについて検討する。たとえば、境界機器とサーバ、ワークステーションとで、異なるベンダを使う」。NIST SP 800-53 は http://csrc.nist.gov/publications/nistpubs/index.html で入手できる。

たとえば、ウイルス対策クライアントソフトウェアの管理とクライアントへの更新の配布のために複数のウイルス対策サーバを用意することができる。現実的に可能であれば、互いに関連しない複数の OS プラットフォームを、ウイルス対策サーバ用として利用するのも良い。こうすることで、いくつかのウイルス対策サーバに対する単一の攻撃が、すべてのウイルス対策サーバに影響を及ぼす可能性を低減できる。また、ウイルス対策サーバ用の OS プラットフォームとして、組織内の大部分のサーバやワークステーションとは異なるものを使用することも検討するべきである。1 つの脆弱性のために、組織内の大部分のサーバやワークステーション、そしてウイルス対策サーバまでもが影響を受けた場合、短時間の攻撃でほとんどのホストが感染し、ウイルス対策サーバが利用できなくなるおそれがある。

マルウェア防止を改善するために考えられる別の措置として、電子メールサーバなどの重要なシステムに複数のウイルス対策製品を使用する方法がある。たとえば、あるウイルス対策ベンダで別のベンダよりも数時間早く新しいシグネチャが入手できる場合がある。あるいは、組織において特定のシグネチャ更新に関する運用上の問題が存在する場合がある。別の可能性として、ウイルス対策製品そのものに、悪用され得る脆弱性が含まれている場合がある。そのような場合でも代わりの製品が利用できれば、主として利用している製品の問題が解決するまで保護を提供することができる。単一のシステムで複数のウイルス対策製品を同時に実行すると、製品間で競合を起こす可能性が高いため、複数の製品を同時に使用する場合は別々のシステムにインストールするべきである。たとえば、境界に設置された電子メールサーバと内部の電子メールサーバとで、使用するウイルス対策製品を使い分ける。このようにすれば、新たな脅威をより効果的に検出できるようになるが、管理作業やトレーニングの量を増やす必要が生じるとともに、ハードウェアやソフトウェアに追加費用が生じる。

3.4.1.3 ウイルス対策ソフトウェアの欠点

ウイルス対策ソフトウェアはマルウェアインシデント防止のための必需品となっているが、ウイルス対策ソフトウェアであらゆるマルウェアインシデントを阻止することは不可能である。このセクションですでに説明したように、ウイルス対策ソフトウェアは未知の脅威を阻止することは不得意である。新たな脅威が認識されれば、数時間以内に新しいシグネチャが入手できるかもしれないが、シグネチャの入手、テスト、および導入には時間がかかる。時折、シグネチャが原因となって、ウイルス対策ソフトウェアや OS がクラッシュしたり、システムやアプリケーションと別の競合を生じたりすることがあるため、テストは重要である。最善の場合であっても新たな脅威が認識されてから新しいシグネチャの導入が開始されるまで、少なくとも数時間はかかるため、新たなマルウェアの脅威にシステムが感染する機会がかなり残ることになる。シグネチャの導入にも相当の時間がかかることもある。ウイルス対策サーバやネットワークは、組織のすべてのマシンを一度に更新することができない可能性がある。また、ネットワークに接続していないシステムが更新されず、感染してしまう可能性もある（リムーバブルメディア上のマルウェアなどに）。

ウイルス対策ソフトウェアのもう 1 つの課題は、マルウェアが、各種のネットワークプロトコルやサービス（電子メール、ファイル転送、P2P ファイル交換ソフトウェア、Web ブラウズ、チャットセッション、インスタントメッセージなど）、あるいはリムーバブルメディア（CD、フロッピーディスク、フラッシュドライブなど）を含む多数の手段により拡散できることにある。組織は、ホストベースとネットワークベースの両方のウイルス対策スキャン（つまり、ファイアウォールと電子メールサーバからのスキャン）を使用するべきであり、それにより、ファイアウォールやファイアウォールの内側にあるホストを通じて（たとえば、感染したリムーバブルメディアをワークステーションに挿入するなどによって）組織に侵入しようとする脅威に対処できるようになる。しかし、現在のウイルス対策ソフトウェア製品でも、組織内部のすべてのシステムについて、すべての可能な伝送メカニズムを監視する能力を備えていない場合がある。たとえば、新しい種類のアプリケーション、サービス、またはネットワークプロトコルが関与する活動をウイルス対策ソフトウェアが分析できない場合がある。組織の管理外のシステ

ムによって組織のネットワークが使用されることについても注意を払う必要がある。たとえば、職員が自宅のコンピュータからダイヤルインや仮想プライベートネットワーク（VPN）を通じて接続する場合や、提携企業が各組織のシステムから接続する場合などが考えられる。これらの外部システムがマルウェアに感染し、組織のネットワークを利用してマルウェアの拡散を試みる可能性がある。

3.4.2 スパイウェア検出／駆除ユーティリティ

スパイウェア検出／駆除ユーティリティは、システム上の多数の種類のスパイウェアを識別して、スパイウェアファイルを隔離または削除するものである。多数の種類のマルウェアの識別を試みるウイルス対策ソフトウェアとは異なり、スパイウェア検出／駆除ユーティリティはマルウェア形式とマルウェア以外の形式の両方のスパイウェアに対応するように特化している。現在、スパイウェア検出／駆除ユーティリティは一部のウイルス対策プログラムよりも堅牢なスパイウェア処理機能を提供している。スパイウェアインシデントの防止が重要なのは、単にスパイウェアがユーザのプライバシを侵害するからだけではなく、システムの機能上の問題を頻繁に引き起こすからである。たとえば、パフォーマンスを低下させたりアプリケーションの動作を不安定にさせたりする[25]。スパイウェア検出／駆除ユーティリティによっては、悪意の Web ブラウザプラグインなど、特定の形式のマルウェアへの対応に特化しているものもあるが、ほとんどのユーティリティは、次に示すような、より広範囲にわたる同様の推奨機能を提供する。

- スパイウェアをシステムに送り込むのに使用される可能性が最も高い、Web ブラウザや電子メールクライアントなどのアプリケーションの動作を監視する。
- ファイル、メモリ、および構成ファイルを定期的にスキャンし、既知のスパイウェアがないか調べる。
- 悪意のモバイルコード、トロイの木馬、追跡クッキーといった、複数種類のスパイウェアを識別する。
- スパイウェアファイルを隔離または削除する（ほとんどのスパイウェアファイルは自己完結型であるため、通常は感染除去は該当しない）。
- ネットワークドライバと Windows シェルの設定を監視する。
- 起動時に自動的にロードされるプロセスやプログラムを監視する。
- ポップアップ広告、追跡クッキー、ブラウザプラグインのインストール、ブラウザハイジャックといった、スパイウェアの複数のインストール手段を防止する。

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。

---

[25] NIST SP 800-53 の管理策#SI-8『スパムおよびスパイウェアからの保護（Spam and Spyware Protection）』では、「情報システムは、スパムおよびスパイウェアからの保護を導入する」ことを推奨している。SI-8 の補足ガイダンスではさらに次を推奨している。「組織では、情報システムの重要な入口（ファイアウォール、電子メールサーバ、リモートアクセスサーバなど）において、および、ネットワーク上のワークステーション、サーバ、またはモバイルコンピューティング機器において、スパムとスパイウェアに対する保護メカニズムを導入する。組織は、電子メール、電子メール添付ファイル、インターネットアクセス、リムーバブルメディア（たとえば、フロッピーディスクやコンパクトディスク）、そのほかの一般的な手段により送り込まれる一方的なメッセージおよびスパイウェア／アドウェアを検出し、適切に対処するために、スパムおよびスパイウェア保護メカニズムを使用する。たとえば、周辺部の機器やサーバと、ワークステーションとで、使用するベンダ製品を使い分けるなど、複数のベンダのスパムおよびスパイウェア対策ソフトの使用を検討する。」NIST SP 800-53 はhttp://csrc.nist.gov/publications/nistpubs/index.htmlで入手できる。

通常、スパイウェア検出／駆除ユーティリティではスパイウェアのシグネチャが利用される。これはウイルス対策ソフトウェアで使用されるものと同様のものである。これらのツールは、既知の脅威とその派生版を認識するのに有効である。しかし、未知の脅威の検出能力についてはまちまちである。スパイウェア検出／駆除ユーティリティはシグネチャに依存しているため、スパイウェアの検出能力が向上するように、最新のシグネチャとソフトウェア更新によってソフトウェアを最新に保つべきである。また、ほかの種類のマルウェアの脅威を検出可能なウイルス対策ソフトウェアなどの管理策によって、スパイウェア検出／駆除ユーティリティを補完するべきである。さらに、スパイウェア脅威の検出能力を向上させるために、複数のスパイウェア検出／駆除ユーティリティを使用することも検討するべきである。

スパイウェア検出／駆除ユーティリティが、集中的な管理と監視の機能を提供するようになったのはごく最近のことである。ユーティリティによっては、更新の確認とダウンロードを自動的に行う機能すら提供せず、ユーザが手動でユーティリティを開いて自分で確認を実行しなければならないものもある。スパイウェア検出／駆除ユーティリティを組織全体で導入することを検討している場合は、ユーティリティの配布、構成、管理方法と、スパイウェアインシデントを識別するためにそれらのユーティリティの活動をどのように監視するのかについて決定するべきである。ウイルス対策ソフトウェアとスパイウェア検出／駆除ユーティリティとは類似した特徴が数多くあるため、通常はどちらの種類の製品に対しても同じ考慮事項を適用するようにする。

3.4.3 侵入防止システム

ネットワークベース侵入防止システム (IPS) は、パケットの傍受とネットワークトラフィックの分析を実施して、疑わしい活動を識別し阻止する[26]。ネットワークベース IPS は通常は*インライン*で配置される。つまり、ソフトウェアはネットワークファイアウォールのように動作する。IPS は、パケットを受信して分析し、それらを許可すべきかどうかを判断して、受け入れ可能なパケットの通過を許可する。ネットワークベース IPS のアーキテクチャにより、攻撃が標的に到達する前にネットワーク上のいくつかの攻撃を検出できる。ほとんどのネットワークベース IPS では、攻撃シグネチャと、ネットワークプロトコルおよびアプリケーションプロトコルの分析を組み合わせて用いる。つまり、よく攻撃の対象となるアプリケーション (電子メールサーバや Web ブラウザなど) のネットワーク活動を想定される動作と比較して、悪意のある活動の可能性を識別する。

ネットワークベース IPS 製品は、マルウェアのほかに多数の種類の悪意のある活動を検出するのに使用されるが、一般的にデフォルトで検出できるマルウェアは、最近の重大なワームなど少数のマルウェアのみである。しかし、一部の IPS 製品は高度なカスタマイズが可能で、数多くの新種の重大なマルウェアに対応した攻撃シグネチャを、管理者がわずかな時間で作成して導入できるようになっている。このような作業には、シグネチャの記述が不適切な場合に、害のない活動が誤ってブロックされるフォールスポジティブが生じるリスクが伴うが、カスタムシグネチャを作成することによって、ウイルス対策シグネチャが入手できるようになる数時間前に新種のマルウェアによる脅威をブロックすることが可能になる。ネットワークベースの IPS 製品は、ネットワークサービスワームや、容易に認識できる特徴 (件名や添付ファイル名など) を持った電子メール媒介ワームおよびウイルスなど、特定の既知の脅威を阻止するのに効果がある。しかし、悪意のモバイルコードやトロイの木馬を阻止する能力は、通常は備えていない。ネットワークベースの IPS 製品によっては、アプリケーションプロトコルを分析することでいくつかの未知の脅威を検出し阻止できるものもある。

[26] 侵入防止システムは侵入検知システム (IDS) に似ているが、IPS が悪意のある活動の阻止を試みることができるのに対して、IDS はそれができない。この項では、IDS ではなく IPS を使用したマルウェアインシデントの阻止または封じ込めについて説明する。セクション 4 では、IPS と IDS の両方の技術を使用してマルウェアインシデントを検知する方法について説明する。

ネットワークベース IPS の特別な形式として、*DDoS 攻撃軽減ソフトウェア*と呼ばれるものがある。このソフトウェアは、異常なネットワークトラフィックフローを識別することによって攻撃の阻止を試みる。これらの製品は主に組織に対する DDoS 攻撃の阻止を目的としたものだが、ワーム活動やそのほかの形態のマルウェアの識別だけでなく、バックドアや電子メールジェネレータといった攻撃ツールの使用も識別できる。通常、DDoS 攻撃軽減ソフトウェアは、ホスト同士がどのプロトコルを使用して互いに通信をしているのかに関する情報を含む通常のネットワークトラフィックパターンと標準時およびピーク時の活動量を監視し、基準を確立する。さらに、ネットワーク活動を監視して基準からの大幅な逸脱を識別する。マルウェアによって特に大量のネットワークトラフィックが発生した場合や、ふだん見られないようなネットワークプロトコルやアプリケーションプロトコルがマルウェアで使用された場合、DDoS 攻撃軽減ソフトウェアはそれらの活動を検知してブロックできなければならない。一部のマルウェアインシデントを制限する別の方法は、特定のホストやサービスが使用できる帯域幅の最大量を制限するようにネットワーク機器を設定することである。また、一部の種類のネットワーク監視ソフトウェアは、想定されるネットワーク活動からの大幅な逸脱を検知し報告することができるが、このようなソフトウェアは、検知した活動をマルウェア関連のものであるとして分類したり、ブロックしたりすることは、通常はできない。

ホストベース IPS 製品は、その原理と用途においてネットワークベース IPS と同様であるが、ホストベース IPS 製品は単一のホストの特性とそのホストの内部で発生するイベントを監視するという点が異なる。ホストベース IPS の監視対象となる活動には、ネットワークトラフィック、システムログ、実行中のプロセス、ファイルに対するアクセスおよび変更、システムやアプリケーションの構成の変更などがある。ホストベース IPS 製品は、攻撃シグネチャと想定される挙動または典型的な挙動に関する知識の組み合わせを用いて、システムに対する既知あるいは未知の攻撃を識別する場合が多い。たとえば、ファイルへの変更操作を監視するホストベースの IPS 製品は、ファイルへ感染しようとするウイルスの検出や、ファイルを置き換えようとするトロイの木馬の検出に効果がある場合があるだけでなく、マルウェアによって送り付けられることが多いルートキットなどの攻撃ツールの使用を検出するのにも効果的である。ホストベースの IPS 製品がホストのネットワークトラフィックを監視する場合には、ネットワークベース IPS 製品と同様の検知機能が提供される。

ウイルス対策ソフトウェアやスパイウェア検出／駆除ユーティリティと同様に、ネットワークベース IPS 製品およびホストベース IPS 製品でもフォールスポジティブやフォールスネガティブが発生する。通常、IPS 製品は精度を向上させるためのチューニング機能を備えているが、チューニングの効果には製品や環境によって大きな差がある。フォールスポジティブが生じると害のない活動がブロックされる可能性があるため、その影響について組織で検討し、フォールスポジティブが生じる可能性がほとんどないシグネチャや異常条件定義に一致する場合にだけ活動をブロックするように IPS を設定することを検討するべきである。ほとんどの IPS 製品では、ブロック機能をシグネチャごとあるいは異常条件定義ごとに有効または無効にすることができる。一部の組織では、すべてのブロック機能をデフォルトで無効にし、ワームなどの新種の重大な脅威に直面したときだけ有効にしている。

マルウェアの防止に関しては、ホストベース IPS ソフトウェアによって、未知の脅威の検出･阻止能力を向上させることができる場合がある。検知の精度を高めるようにホストベース IPS ソフトウェアをチューニングすることができれば、ウイルス対策ソフトウェアやそのほかの技術的な管理策では認識することができない未知の脅威を阻止するのに役立つ可能性がある。IPS ソフトウェアは特に、ウイルス対策ソフトウェアが監視していない DNS（ドメインネームシステム）のようなネットワークサービスを利用する脅威を識別するのに役立つ場合がある。

ネットワークサービスワームなど、大量のトラフィックを発生させるマルウェアの脅威に対しては、ネットワークベース IPS 製品をネットワーク境界に設置することによって、マルウェアが組織のネットワークに加える負荷を大幅に減らすことができる。ウイルス対策ソフトウェアと IPS ソフトウェアを組み合わせて使用すれば、マルウェアインシデント全体の防止率を向上させることができるだけでなく、

マルウェア処理の負荷を 2 種類の技術的な管理策群に分割するのにも役立てることができる。重大なマルウェアインシデントが発生した場合、ウイルス対策ソフトウェアだけではマルウェアイベントの数によって過負荷になる可能性があるが、複数種類の管理策の間で処理を共有することで、マルウェアの処理に起因する処理速度の低下を抑えることができる。

3.4.4 ファイアウォールとルータ

ファイアウォールやルータなどのネットワーク機器のほか、ホストベースのファイアウォールソフトウェアは、ネットワークトラフィックを調べ、ルールセットに基づいてトラフィックを許可または拒否する。ルータは通常、アクセス制御リスト (ACL) と呼ばれる簡単なルールセットを使用する。ACL はネットワークトラフィックの最も基本的な特性のみを扱うのに対して、ファイアウォールはより強固な機能を提供する。ファイアウォールには、ネットワークファイアウォールとホストベースファイアウォールの 2 種類がある。*ネットワークファイアウォール*は、ネットワーク間に設置される機器で、一方のネットワークから他方のネットワークへ転送されるトラフィックの種類を制限する。*ホストベースファイアウォール*は、単一のホストにおいて実行されるソフトウェアの一種で、当該ホストのみに関する内向きおよび外向きのネットワーク活動を制限することができる。どちらの種類のファイアウォールもマルウェアインシデントの防止に役立つ。3.4.4.1 項および 3.4.4.2 項は、ネットワークファイアウォールとホストベースファイアウォールについてそれぞれ説明する。また、3.4.4.3 項ではルータについて簡単に説明する。

3.4.4.1 ネットワークファイアウォール

組織では通常、外的脅威からの保護を実現するために 1 つ以上のネットワークファイアウォールをネットワーク境界で使用している。ネットワークファイアウォールは、ネットワークトラフィックをルールセットと比較することによって動作する。各ルールは通常、ネットワークまたはアプリケーションのプロトコルと、通信の発信元および送信先を指定する。たとえば、あるルールは外部ホストから組織の電子メールサーバへの電子メールの到達を許可する。この場合、特定のサービスやサービスポート番号を標的としたネットワークサービスワームを阻止する効果的な手段として、ネットワークファイアウォールの利用が考えられる(特に、サービスやポートが組織で広く使用されていない場合に効果的である。)ネットワークファイアウォールは内向きのトラフィックと外向きのトラフィックの両方を制限することができるため、組織の内部で感染した特定のワームが、外部のシステムに拡散するのを阻止するのにも利用できる。

マルウェアインシデントを防止するため、組織は*デフォルトで拒否*のルールセットを実装するべきである。つまり、明示的に許可されていないすべての内向きおよび外向きのトラフィックがファイアウォールによって拒否されるようにする。このようなルールセットを設けておけば、マルウェアは、組織にとって不要とみなされるサービスを利用して拡散することができなくなる[27]。ワームの拡散を減らすため、外部のシステム (在宅勤務者の自宅のシステムやビジネスパートナーのシステムなど) から組織のネットワークに送信することができるトラフィックの種類に厳密な制限を設けることが特に重要である。また、組織のネットワークファイアウォールで出口フィルタおよび入口フィルタが必ず実行されるようにするべきである。*入口フィルタ*は、不正な IP アドレスを送信元とするパケット (たとえば、予約済みまたは未割り当ての送信元アドレスを持つパケット) など、ネットワーク内に入るべきでないパケットの通過をブロックする処理である。*出口フィルタ*は、不正な IP アドレスを送信元とするパ

[27] サービスによってはその使用をファイアウォールのルールセットを通じて簡単にブロックできないものがある。たとえば、一部の P2P ファイル交換ソフトウェアサービスやインスタントメッセージサービスは、HTTP や SMTP (Simple Mail Transfer Protocol) などのほかのサービスに割り当てられているポート番号を使用できる。そのようなサービスの使用を、ポート番号のブロックにより防止しようとすると、正規のサービスがブロックされてしまう可能性がある。このような場合は、インスタントメッセージサーバなど、サービスの一部のホストとなっている特定の IP アドレスへのアクセスをブロックする必要があるかもしれない。また、この節で後述するように、アプリケーションプロキシは、想定されているサービスとは別のサービスが使用されているような何らかの状況を特定することができる。

ケット（たとえば、ネットワーク内部のアドレスを送信元アドレスに持ち、誤って組織を出てインターネットに入り込もうとしているパケット）など、ネットワークの外に出るべきでないパケットの通過をブロックする[28]。ワームは、拡散を試みる際に IP アドレスを無作為に生成することが多いため、不正な IP アドレスを持つパケットをブロックすれば、組織の内部ネットワークに侵入するワームの数が減ると考えられる。組織はネットワークファイアウォールのルールセットを定期的に見直すことにより、個々のルールの有効性を確認するとともに、現時点ではルールセットによって許可されているが、今後許可すべきでない全ての活動を特定するべきである。

ファイアウォールソフトウェア自体は、ネットワーク通信の中に含まれている攻撃を探し出すことはしないが、攻撃を探し出すことができる追加のソフトウェアを実行することがしばしばある。たとえば、ファイアウォールの多くは侵入防止ソフトウェアやウイルス対策ソフトウェアを実行して、電子メールや Web トラフィックといった特定の種類の通信に含まれている攻撃を探し出す。ファイアウォールの中にはプロキシとして機能するものがある。*プロキシ*はクライアントからの要求を受け取り、クライアントに代わって要求を望ましい送信先に送信する。プロキシを使用すると、接続の試みが成功するたびに実際には 2 つの別々の接続が生成される。1 つはクライアントとファイアウォールを結ぶ接続で、もう 1 つはファイアウォールと実際の送信先との接続である。プロキシによっては、HTTP（Hypertext Transfer Protocol）などのアプリケーションプロトコルの基本的な分析や検証を行い、なんらかのマルウェアが含まれている可能性があるために無効と判断されるクライアント要求を拒否できるものがある。このようなプロキシはアプリケーション層ファイアウォールとしても知られている。

ネットワークファイアウォールは一般的に*ネットワークアドレス変換*（NAT）の実行にも利用される。NAT は、あるネットワークのアドレスを別のネットワークのアドレスにマッピングする処理のことである。NAT は、最も多くの場合、内部ネットワークのプライベートアドレスを、インターネットに接続しているネットワークの 1 つ以上のパブリックアドレスにマッピングする。ホストにプライベートアドレスが使用されていて、それらが NAT を通じてパブリックアドレスにマッピングされている場合、インターネットを横断してプライベートアドレスの経路制御を行うことができないため、外部ホストは内部ホストに対して直接接続を開始することができない。これは、インターネットベースのホスト上のネットワークサービスワームが組織内部のホストにアクセスするのを防ぐのに役立つ可能性がある。

ネットワークサービスを標的とした新種の重大なマルウェアの脅威が切迫している場合、特に、ウイルス対策ソフトウェアや侵入防止ソフトウェアによる標的となっているサービスの監視が行われていない場合には、インシデント防止のためにネットワークファイアウォールに頼る必要がある場合がある。最悪の状況に備えるため、組織は、ネットワークサービスを利用したマルウェアインシデントを防止するためにファイアウォールのルールを速やかに追加または変更できるように準備しておくべきである。ファイアウォールのルールはまた、特定の IP アドレスに依存するマルウェア（たとえば、10 個の外部ホストのうちのいずれか一つからトロイの木馬をダウンロードするワームなど）の阻止に役立つことがある。それらの外部ホストの IP アドレスに関わるすべての活動をブロックするルールを追加することにより、トロイの木馬が組織に入り込むのを防ぐことができる。

3.4.4.2 ホストベースファイアウォール

ホストベースファイアウォールは、個々のホストの内向きおよび外向きのネットワーク活動を制限することができる。それによって、ホストのマルウェアへの感染と、感染したホストからほかのホストへのマルウェアの拡散を阻止することができる。通常、サーバ用のホストベースファイアウォールでは、ネットワークファイアウォールと同様のルールセットが使用される。デスクトップ用またはラップトップ

---

[28] 詳細については、IETF（Internet Engineering Task Force）の 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。未割り当ての IP アドレス範囲の詳細については、http://www.cymru.com/Documents/bogon-list.html を参照。

用のホストベースファイアウォールでも同様のルールセットを使用するものがあるが、ほとんどはアプリケーションリストに基づいて活動を許可または拒否する。リストにないアプリケーションが関与する活動は、自動的に拒否されるか、あるいは、活動に関する決定を下すよう求めるプロンプトに対するユーザの応答に基づいて許可または拒否される。マルウェアインシデントを防止するために、ホストベースファイアウォールのルールセットを、内向きのトラフィックをデフォルトで拒否するように設定するべきである。外向きのトラフィックに対しても、実用上問題がなければデフォルトで拒否をするルールセットを使用すべきであるが、そのようなルールセットを使用した場合、システムの利便性やユーザの満足度に著しい悪影響を及ぼす可能性がある。

ルールに基づくネットワーク活動の制限に加えて、多くのワークステーション用ホストベースファイアウォールには、ウイルス対策ソフトウェアや侵入防止ソフトウェアの機能の他、Web ブラウザのポップアップウィンドウの抑止、モバイルコードの制限、クッキーのブロック、あるいは、Web ページや電子メールに潜むプライバシ侵害の問題の特定といった機能が組み込まれている。これらの機能を統合したホストベースファイアウォールは、ほとんどの種類のマルウェアインシデントを防止するだけでなく、マルウェア感染の拡大の阻止にも大きな効果がある。たとえば、ウイルス対策機能を備えたホストベースファイアウォールは、受信および送信される電子メールに大量メール送信ウイルスやワームの兆候がないかを監視し、そのような活動を検知した場合には電子メールサービスを一時的に停止することができる。そのため、数種類のマルウェア防止機能を備えたワークステーション用ホストベースファイアウォールは、適切な設定がなされ、最新のシグネチャとソフトウェア更新によって常に最新の状態が保たれている限り、一般的に、マルウェアの脅威を軽減するためのホストベースの最適な技術的管理策を単独で提供する。ネットワークに接続しているが、ネットワークファイアウォールやそのほかのネットワークベースのセキュリティ管理策によって保護されていないシステムにとっては、ホストベースファイアウォールが特に重要となる。インターネットから直接アクセスすることが可能なシステムについては、ネットワークサービスワームやそのほかの脅威がそれらのシステムに接続して攻撃するのを防ぐために、可能な限りホストベースのファイアウォールによって保護されるべきである

3.4.4.3 ルータ

ファイアウォールが一般的に、サービスとホストの IP アドレスの組み合わせに基づいて内向きおよび外向きのネットワーク活動を制限するのに対し、ルータは通常、より範囲が広く粒度が粗いルールによって設定される。通常は、組織のネットワークがインターネットに接続する場所で 1 つ以上のルータを使用する。これらのルータは、*インターネット境界ルータ*と呼ばれる。ルータは通常、組織の主たるファイアウォールの手前に配置され、入口フィルタや出口フィルタのような、ネットワーク活動に関するいくつかの基本的な検査を実施する。これらの検査は、一部のインターネットベースのワームが組織のファイアウォールに到達するのを阻止するのに役立つ場合がある。ファイアウォールでもそのようなワームをブロックすべきであるが、インターネット境界ルータにその役割を持たせることによって、ファイアウォールの負担を多少軽くすることができる。

重大なワームインシデントが発生した場合、ファイアウォールが過負荷にならないように、組織のインターネット境界ルータの一部を再設定して、着信するワーム活動をブロックする必要がある場合がある。内部ネットワークのルータを再設定して、特定のサービスの活動がネットワーク間を行き来しないようにブロックすることもできる。こうすることで、特定のネットワークで感染したホストからマルウェアがほかのネットワークに拡散するのを防ぐことができる。組織は、ワーム感染の封じ込めを支援するために、ルータの ACL を必要なときに速やかに変更できるよう準備しておくべきである。

3.4.5 アプリケーション設定

マルウェアの多くは、電子メールクライアントや Web ブラウザ、ワードプロセッサなどの一般的なアプリケーションが提供する機能を利用する。デフォルトでは、アプリケーションはセキュリティよりも機能を優先して設定されることが多い。従って、マルウェアがアプリケーションを攻撃する際の経路と手段を限定するために、アプリケーションの特徴と機能のうち不要なもの、特にマルウェアによって一般的に悪用される機能を無効にすることを検討するべきである。また、マルウェアの典型的な伝染手段となっているアプリケーション（Web ブラウザ、電子メールクライアントおよびサーバなど）を特定し、それらのアプリケーションを、悪意があると考えられるコンテンツをフィルタリングし、悪意があると考えられるほかの活動を停止するように設定することを検討するべきである。マルウェアインシデントを防止するうえで考慮すべきアプリケーション設定には次のものがある。

- **疑わしい電子メールの添付ファイルをブロックする。多くの**組織ではインシデントを防止するために、疑わしい電子メールの添付ファイルを特定し、電子メールから添付ファイルを削除するか、電子メールそのものをブロックするように、電子メールサーバを設定している（電子メールクライアントも同様に設定していることが多い）。たとえば、多くの組織では、マルウェアに関連付けられることが多いファイル拡張子（.pif、.vbs など）や疑わしいファイル拡張子の組み合わせ（.txt.vbs、.htm.exe など）を持つ添付ファイルをブロックしている。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（Web バグがスパムの中に埋め込まれていることが多い）、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処理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。

- **Web サイトのコンテンツのフィルタリング。**通常、Web コンテンツフィルタ処理ソフトウェアは、仕事場にふさわしくない情報へのアクセスを防ぐものと考えられているが、フィッシング Web サイトや、敵意がある（つまり、訪問者にマルウェアを配布しようとする）と考えられる他のサイトの一覧が含まれている場合もある。Web コンテンツフィルタリングソフトウェアは、望ましくないファイルの種類を（ファイル拡張子などにより）ブロックすることもできる。

- **モバイルコードの実行を制限する。**Web ブラウザや電子メールクライアントなどのアプリケーションは、要求された形式のモバイルコード（JavaScript、ActiveX、Java など）だけを許可し、特定の場所（たとえば、内部の Web サイトのみ）から送信されたモバイルコードだけを実行するように設定することができる。これは、一部の悪意のモバイルコードを阻止するのに効果があるが、害のない Web サイトの機能に影響を与える場合もある。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。

- **Web ブラウザのクッキーを制限する。**ほとんどの Web ブラウザは、クッキーを許可するか拒否するかの判断をクッキーごとにユーザに促すか、あるいは、セッションクッキーを自動的に許可または拒否するが、個々の永続クッキーを許可するか、あるいは、自動的に拒否するかの判断をユーザに促すように設定することができる[29]。また、ほとんどの Web ブラウザは、ユーザがア

[29] クッキーオプションの設定や、ユーザがアクセスする Web サイトによっては、クッキーを許可するかどうかをユーザにたずねたり、特定の種類のクッキーを自動的に拒否したりすることが、ユーザにとって非常に不便な場合がある。

クセスした Web サイトに対してのみ設定されたクッキー（ファーストパーティクッキーと呼ばれる）を許可し、広告業者や他の組織の Web サイトに対して設定されたクッキー（サードパーティクッキーと呼ばれる）を許可しないように設定することもできる。ファーストパーティクッキーを許可し、サードパーティクッキーをブロックすることは、システムに置かれる追跡クッキーの数を減らすのに大いに役立つ可能性がある。

- **Web ブラウザのポップアップウィンドウをブロックする。**ポップアップウィンドウの中には、見かけは正規のシステムメッセージボックスや Web サイトであるが、実際にはユーザをだまして偽のサイト(フィッシングに使用されるサイトなど)に誘導したり、ユーザにシステムへの変更を許可するように仕向けるなど、悪意ある行為を働くこともものがある。ほとんどの Web ブラウザはポップアップウィンドウをブロックできるが、サードパーティ製のポップアップブロッカーを追加することによりポップアップウィンドウをブロックすることができるものもある。

- **Web ブラウザへのソフトウェアのインストールを防ぐ。**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。全ての 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。

- **電子メールの画像の自動読み込みを防ぐ。**ほとんどの電子メールクライアントは、電子メールに含まれている画像を自動的に読み込まないように設定することができる。これは、電子メールを利用した Web バグを阻止するのに特に役立つ。この構成設定により、読み込まれなかった Web バグの輪郭線が電子メールの中で小さなボックスとして表示されるため、ユーザが画像の読み込みを選択しない限りユーザの活動が追跡されることはない。

- **ファイルの関連付けを変更する。**オペレーティングシステムの多くは、たとえば.txt ファイルはテキストエディタで開くなど、どの種類のファイルがどの特定のプログラムに関連付けられるのかを指定するためのメカニズムを備えている。ユーザがファイルを開こうとすると、通常はオペレーティングシステムによってデフォルトのファイルの関連付けが調べられ、指定のアプリケーションが実行される。この仕組みはユーザにとっては便利だが、マルウェアにとっても好都合である。たとえば、ユーザがだまされて電子メールの添付ファイルを開くように仕向けられると、結果的に添付ファイルがオペレーティングシステムによって自動的に実行されることになる。多くの組織では、マルウェアに利用されることが最も多いファイルの種類（.pif、.vbs など）について、システムでのファイルの関連付けを変更し、ユーザがファイルを開こうとしたときに自動的にファイルが実行されないようにしている。

- **マクロの使用を制限する。**ワードプロセッサやスプレッドシートなどのアプリケーションにはマクロ言語が組み込まれていることが多いが、マクロウイルスはこれを利用する。マクロ機能を備えた最も一般的なアプリケーションは、信頼のおける場所からのマクロだけを許可したり、マクロを実行しようとするたびに許可または拒否の判断をユーザに求めたりする、マクロのセキュリティ機能を提供する。

- **電子メールのオープンリレーを防ぐ。**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[30]。

以上のようなアプリケーション設定はマルウェアインシデントの発生頻度を減らすのに効果があるが、適切な設定の選択は難しいことが多い。ほとんどの場合、より安全に動作するようにアプリケーションを設定すると、機能が縮小されてしまう。たとえば、Web ブラウザで Java のサポートを無効にすると、組織の Java ベースの Web アプリケーションが実行できなくなってしまう。したがって、個々の設定がもたらす影響を慎重に考慮し、セキュリティが改善されることのメリットと機能が失われることのデメリットとを比較する必要がある。また、使用されているクライアントアプリケーションの多様性にも注意を払う必要がある。たとえば、クライアントシステムにはさまざまなバージョンの複数の Web ブラウザや電子メールクライアントがインストールされている可能性があり、それらはそれぞれ異なる機能と可能な構成設定を有すると考えられる。組織が、標準の電子メールクライアントと比べて、機能が限定された、セキュリティ設定オプションがほとんどない、Web ベースの電子メールクライアント提供することも考えられる。

ほとんどの組織では、サーバでのアプリケーション設定の実装と管理は比較的容易であるが、クライアントで同様の事を行うのは、はるかに困難である。高度に管理された環境であれば、通常、すべてのクライアントについてアプリケーション設定を集中的に制御することは可能だが、それ以外のほとんどの環境では現実的ではない。組織が自ら選択した設定を新しいシステムに実装することは可能かもしれないが、それらの設定が変更されないことを保証したり、セキュリティや機能のニーズの変更に対応して必要に応じて設定を自動的に更新することはできない。どのようにすればアプリケーションのクライアント設定を効果的に実装、管理、確認できるかを、組織で検討するべきである。管理されていない環境では、意識向上活動やユーザの自発的な参加に頼らざるを得ない場合もある。管理された環境では、選択したアプリケーション構成設定に対して必要な例外事項が発生した場合の、それらの承認、実装、維持、および定期的な検証の方法について検討するべきである。

クライアントアプリケーションの構成設定を変更することによって得られる利点の多くは、ホストベースファイアウォールを使用することによっても実現可能である。3.4.4.2項で説明しているように、ホストベースファイアウォールの多くは、ウイルス対策ソフトウェアによるアプリケーションの内容監視や、Web ブラウザのポップアップウィンドウの抑制、モバイルコードの実行制限、クッキーのブロックを行うことができる。また、ホストベースファイアウォールの多くはスパムのフィルタリングと Web コンテンツのフィルタリングを行うことができる。しかし、ホストベースファイアウォールはすべてのアプリケーション設定に対応しているわけではない。そのため、ホストベースファイアウォールと、クライアントの適切なアプリケーション設定とを併用するのが最も効果的である。

アプリケーションの構成設定を速やかに変更することができれば、新種の重大な脅威を阻止するうえでたいへん有益となる可能性がある。たとえば、電子メールをベースとする新たな脅威が発生し、ウイルス対策ソフトウェアや侵入防止ソフトウェアではまだ検出することができない場合、組織は、新たな脅威の特徴に一致するすべての電子メールを削除するように、電子メールサーバおよびクライアントの設定を再構成することができる。組織は、マルウェアによる緊急事態が発生した場合のこれらの設定の実装方法を事前に検討し、適切な手続きを確立し管理するべきである。

3.5 まとめ

組織は、現在および近い将来において利用される可能性が最も高いと考えられる攻撃の経路と手段に基づいて、マルウェアによるインシデントを防止するための手法を計画し、実施するべきである。組織は、自組織の環境やシステムに最も適した予防的手段を選択するべきである。たとえば、管理

[30] オープンリレーと、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。

された環境では有効な手法が、管理されていない環境では効果を発揮しない場合がある。マルウェアによるインシデントを防止するための効果的な手法には、ポリシーに関する考慮、ユーザや IT スタッフを対象とする意識向上プログラム、および、脆弱性と脅威を軽減するための作業が組み込まれているべきである。

さらなるインシデント防止の取組みの基礎として、組織のポリシーが確実にマルウェアインシデントの防止に寄与するものとすること。マルウェア防止に関連した一般的なポリシーに関する考慮事項は、次の 3 つの一般的なカテゴリに分けられる。

- システム利用上の許容範囲の指定
- 脆弱性の軽減
- 脅威の軽減

マルウェア防止に関連したポリシーは、組織が管理するシステムと組織の管理外のシステムの両方を使用する、遠隔地にいる作業者に関する考慮事項に言及したものとするべきである。

組織は、マルウェアインシデントの防止に関するユーザへのガイダンスを含む意識向上プログラムを実施するべきである。すべてのユーザは、マルウェアの拡散のしかた、マルウェアがもたらすリスク、技術的管理策によってすべてのインシデントを防ぐことは不可能であること、および、インシデントを防ぐうえでのユーザの重要性についての意識を持つようになるべきである。組織はまた、意識向上プログラムを通じて、感染の疑いがある場合の報告方法やインシデント対応担当者を支援する上でユーザが行う必要があることなど、マルウェアインシデント対応に適用されるポリシーや手続きをユーザに認識させるべきである。さらに、マルウェアインシデントの防止に関わる IT スタッフを対象に、意識向上のための活動を実施し、具体的な作業に関するトレーニングを提供する。

組織は、OS やアプリケーションの脆弱性がマルウェアに悪用されないように、脆弱性を軽減するためのポリシー、プロセス、および手続きの文書化を完了しておくべきである。通常、脆弱性は 1 つ以上の手段によって軽減できるため、パッチ管理や最小特権の原則などの脆弱性軽減手法を組み合わせて利用するべきである。パッチ管理は複雑なプロセスであり、脆弱性を軽減するうえで非常に効果的であるが、新たな脆弱性が発表されてから数日以内に新たなマルウェアの脅威が発生するような状況においては、実用的でない可能性がある。最小特権の原則をシステムに適用することにより、管理者レベルの特権の悪用が必要なマルウェアの侵入を阻止することができ、また、一部のマルウェアによって引き起こされる可能性のある損害を少なくすることができる。潜在的な脆弱性をさらに減らすために、追加的なホスト強化策として、セキュリティ保護されていないファイル共有の排除や、不要なサービスの無効化あるいは除去などの実施を検討すべきである。

組織は、脆弱性の軽減に加えて、マルウェアが標的に影響を与える前にマルウェアの検出･阻止を行うために、脅威を軽減するための作業を実施するべきである。特に、次にあげる技術的な管理策が脅威の軽減に役立つ。

- ウイルス対策ソフトウェアは、マルウェアの脅威を軽減するために最もよく使用されている技術的な管理策であり、マルウェアインシデント防止に必要なものとなっている。スパイウェア検出／駆除ユーティリティは、マルウェアおよびマルウェア以外の形態のスパイウェアの軽減に特化したものである。ウイルス対策ソフトウェアとスパイウェア検出／駆除ユーティリティはともに、シグネチャに依存しており、検出の精度を向上するために最新の状態に保つ必要がある。
- ネットワークベース IPS は、限定的なマルウェア検出機能をデフォルトで提供するが、通常、ワームなどの既知の特定の脅威を阻止するためにカスタマイズすることができる。ホストベース IPS は、マルウェアに関連したさまざまな既知および未知の脅威を阻止することができる。

- ファイアウォールは、ネットワークサービスに対する攻撃を防止することができる。ホストベースファイアウォールもまた、アプリケーションの内容を監視する機能と、マルウェアインシデントによってアプリケーションの脆弱性が悪用されたりアプリケーションの機能が利用されたりするのを防ぐための機能を提供する。ルータは、特定のワームによる脅威をブロックするのに役立つ可能性がある。
- アプリケーション設定についても、機能を犠牲にしてセキュリティを強化するように構成することができる。

4. マルウェアインシデントへの対応

NIST SP 800-61『*コンピュータセキュリティインシデント対応ガイド (Computer Security Incident Handling)*』で定義されているように、インシデント対応プロセスには「準備」、「検知と分析」、「封じ込め/根絶/復旧」、「インシデント発生後の活動」の、4 つの主要なフェーズがある。図 4-1 はこのインシデント対応のライフサイクルを示したものである。このセクションでは、SP 800-61 の考え方に基づき、マルウェアインシデント[31]への対応についてさらに詳しく説明する。

マルウェアインシデント対応の最初のフェーズは、インシデント対応チームのためにマルウェア専用のインシデント対応手続きとトレーニングプログラムを策定するといった、準備活動の実施に関わる。セクション 3 で説明したように、準備フェーズはまた、マルウェアインシデントの数を削減するためにポリシー、意識向上活動、脆弱性軽減、およびセキュリティツールの使用を伴う。これらの措置を講じたとしても、リスクが残ることは避けられず、完璧な解決策は存在しない。したがって、インシデントが発生した場合に常に組織に対して警告が発せられるように、マルウェアの感染を検知することが必要である。マルウェアインシデントでは迅速な検知が特に重要である。なぜなら、マルウェアインシデントがほかの種類のインシデントよりも短時間で多数のユーザやシステムに影響を及ぼす可能性が高く、検知が早ければそれだけ感染するシステムの数を減らせるからである。

図 4-1. インシデント対応のライフサイクル

各インシデントについて、組織はその深刻度に応じて適切な行動をとり、インシデントの封じ込め、感染の根絶、およびインシデントからの最終的な復旧を行うことにより、インシデントの影響を軽減する。感染が広範囲に拡大し、組織のシステムの大部分が同時に感染している可能性がある場合には、このような措置がきわめて困難になることがある。インシデントへの対応が完了した後に、インシデントの原因とコストの詳細を記載するとともに、将来のインシデントを防止し、必ず発生するインシデントに対応する上でより効果的な準備を行うために組織が実行すべき手順を詳述 したレポートを発行するべきである。

基本的なインシデント対応プロセスはマルウェアインシデントの種類を問わず同じであるが、広範囲な感染の場合は、標準的なインシデント対応プロセスが具体的に対応していない多くの課題がみえてくる。このセクションでは、広範囲に感染するマルウェアインシデントへの対応にフォーカスするが、そこで提供されるガイダンスは、より深刻度の低いマルウェアインシデントへの対応にも役立つはずである。

4.1 準備

組織がしっかりとしたインシデント対応能力を備えることは、マルウェアインシデント対応準備の基礎的な要素である。そのような能力がなければ、規模がきわめて小さい組織でない限り、広範囲に

[31] インシデント対応能力を確立する方法の詳細については、NIST SP 800-61『コンピュータセキュリティインシデント対応ガイド (*Computer Security Incident Handling Guide*)』(http://csrc.nist.gov/publications/nistpubs/index.html) を参照。

感染したマルウェアを効果的に封じ込めて根絶することはきわめて困難になる可能性がある。マルウェアへの対応のニーズが特に高い組織では、一般的なインシデント対応チームのほかに、専門のマルウェアインシデント対応チームを設けているところもある。マルウェアインシデントは短時間のうちに組織全体に大規模なマイナスの影響を及ぼす可能性があるため、組織は、マルウェアインシデントへの対応に関与する可能性のあるすべての個人とチームの役割と責任を規定したマルウェア専用のインシデント対応ポリシーと手続きを策定して備えるべきである。マルウェアをテーマとしたトレーニングや訓練の定期的な実施は、人々に自らの役割と責任を確実に意識させ、マルウェアに関するポリシーや手続きが正確かつ網羅的であることを保証するうえで、大いに役立つ可能性がある。広範囲への感染に対応するための予行演習は、準備作業として特に役立つ可能性がある。なぜなら、そのようなインシデントは、ほとんどの組織では発生する頻度は比較的低いが、最も大きな影響を与えるからである。

また、これ以外にも、マルウェアインシデントへの効果的な対応に必要な能力を有していることを確実にするための準備をしておくべきである。4.1.1 項から 4.1.3 項では、インシデント対応チームにおけるマルウェア関連技能の構築と維持、組織全体における連絡と調整の促進、必要なツールやリソースの獲得を含む、いくつかの推奨される準備項目について説明する。

4.1.1 マルウェア関連技能の開発と維持

インシデント対応チームの標準的な技能に加えて、マルウェアインシデント対応担当者にとって以下の分野の知識が役立つ場合がある。

- **マルウェア感染の手口。** マルウェアインシデント対応担当者は全員、マルウェアの主要な分類ごとに、それぞれがシステムにどのように感染し、どのように拡散するのかを十分に理解しておく必要がある。
- **マルウェア検知ツール。** 3.4 項で説明したように、マルウェアは、ウイルス対策ソフトウェア、ネットワークベースおよびホストベースの侵入防止ソフトウェア、スパイウェア検出／駆除ユーティリティとそのほかの各種ツールによって検知することができる。組織のマルウェア検知ツールの実装と設定に詳しいインシデント対応担当者であれば、参考データの分析と脅威の特徴の識別をより適切に行うことができるであろう。対応担当者は全員、少なくとも組織のウイルス対策ソフトウェアについて熟知している必要がある。
- **コンピュータフォレンジック。** 組織は、少なくとも数人の、コンピュータフォレンジックのツールと技法に精通したインシデント対応担当者を確保するべきである。この専門技術は、ルートキットがインストールされた疑いがある場合など、特に困難なマルウェアの状況を調査する際に必要となる[32]。
- **IT に関する幅広い理解。** IT に関する幅広い知識があれば、対応担当者はマルウェアの脅威の組織全体に対する潜在的な大きさと影響の可能性を評価し、その封じ込め、根絶、および復旧のための有効な推奨措置を提示することができる。
- **プログラミング。** 一般的なスクリプト言語やマクロ言語でのプログラミング技能を有するチームメンバを確保したり、組織内のプログラミング専門技術を持つほかの人員をあてにしたりすることにより、チームが新型のインタプリタ型ウイルスやワームの振る舞いと潜在的な影響を短時間で理解するのに役立つ可能性がある。

[32] コンピュータフォレンジックの詳細については、NIST SP 800-86（草稿版）『*Guide to Applying Forensic Techniques to Incident Response*』（http://csrc.nist.gov/publications/nistpubs/）を参照。

組織は、マルウェア関連のトレーニングや訓練（4.1 項を参照）を実施することに加え、技能を構築し維持するためのほかの手段も検討するべきである。考えられる手段の 1 つは、インシデント対応担当者に、一時的にウイルス対策技術者あるいは管理者の仕事を担当させることで、新しい技術的なスキルを習得させ、ウイルス対策スタッフの手続きや実務をより深く知る機会を与えることである。また、インシデント対応担当者に一時的に脆弱性管理チームの仕事を担当させることで、脆弱なシステムの検出方法やパッチの適用方法についての知識を増やすことができる。このような現場に触れることにより、対応担当者が封じ込めや根絶に関するより適切な意思決定を行うのに役立つ可能性がある。

4.1.2 連絡と調整の促進

マルウェアインシデントへの対応、特に広域感染インシデントへの対応に際して最も一般的な問題の 1 つは、不十分な連絡と調整である。ユーザを含め、インシデントに関与する人はだれでも、状況の把握や理解が限定されるために意図せずともさらなる問題を引き起こす可能性がある。組織は、連絡と調整を改善するために、組織としてのマルウェアインシデント対応を調整する責任を担う、数人の個人または少人数のチームを事前に任命しておくべきである。調整担当者の主な目標は、状況を常に把握することであり、そのために、関係するあらゆる情報を収集し、組織にとって最善の決定を下し、関係する情報や決定を組織内のすべての関係者に適切なタイミングで伝える。マルウェアインシデントの場合、関係者にはエンドユーザが含まれることが多い。エンドユーザに対しては、システムへの感染を防ぐ方法、感染の兆候を知る方法、システムが感染したと思われる場合の対応方法が指示される場合がある。また、調整担当者は、封じ込め、根絶、復旧の各作業を支援するすべてのスタッフに技術的なガイダンスや指示を与えるとともに、管理層に対して、インシデントへの対応状況と、インシデントによる現在のおよび将来想定される影響について最新の情報を定期的に提供する必要がある。

広域感染マルウェアインシデントは、電子メールサービス、内部 Web サイト、Voice over IP やその他の形態の通信を阻害することが多いため、ネガティブな事象が発生している間もインシデント対応担当者、技術スタッフ、管理層およびユーザの間で良好な連絡と調整を維持できるように、複数の連絡の仕組みを確立しておくべきである。考えられる連絡手段としては、電話、携帯電話、ポケベル、電子メール、ファックス、書面がある。状況がよい場合であっても、連絡する相手によって異なる連絡手段を用いるのが効果的な場合が多い。たとえば、ユーザへは電子メールで連絡し、主要な技術担当者間のやり取りには標準の電話会議用の電話番号を使用する。管理層に対する最新情報の提供は、直接行う場合、電話会議で行う場合、あるいは、インシデントの状況やそのほかの有益な情報が定期的に更新される音声メールボックスを通じて行う場合がある。4.3.1 項では、音声メールメッセージの同報送信や、人の行き来が多いオフィスエリアでのサインの掲示を含む、ユーザと連絡をとるための他の手段について説明する。

組織はまた、マルウェア警告の真偽に関する質問への回答を行うための連絡拠点を確立しておくべきである。多くの組織では IT ヘルプデスクを一次的な連絡拠点として利用し、ヘルプデスク担当者が真のマルウェア脅威や偽のウイルス情報に関する情報源にアクセスできるようにすることで、担当者が警告の真偽を速やかに判断し、ユーザに何をするべきかに関するガイダンスを提供できるようにしている[33]。組織は、マルウェア警告の真偽を確かめずに警告をほかのユーザに転送することがないよう、ユーザに注意を促すべきである。

---

[33] ウイルス警告の真偽の判断に役立つ可能性のある情報源としては、Computer Incident Advisory Capability（CIAC、http://ciac.llnl.gov/ciac/）、Computer Virus Myths のサイト（http://www.vmyths.com/）、大手ウイルス対策ソフトウェア業者の Web サイトなどがある。

4.1.3 ツールやリソースの確保

組織は、マルウェアインシデント対応を支援するために必要なツール（ハードウェアとソフトウェア）およびリソースを確保することも必要である。ツールの例としてはパケットスニファやプロトコルアナライザがある。3.4 項では、インシデント対応担当者が使用できるようにしておくべきそのほかのツールとして、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、ホストベース IPS ソフトウェアなどについて説明している。インシデント対応チームは、マルウェアによってシステムにどのような変更がなされたのかをより的確に判断するために既知の正常なオペレーティングシステムとアプリケーションファイルのハッシュセットを構築してもよい[34]。リソースの例としては、連絡先一覧、呼び出し情報、よく使用されるポート番号、既知の重要な資産などがある。表 4-1 に、マルウェアインシデント対応担当者のための主要なツールやリソースのチェックリストを示す[35]。

表 4-1. マルウェアインシデント対応担当者のためのツールとリソース

入手済	ツール／リソース
	マルウェアインシデント対応担当者のための連絡手段と設備
	連絡先情報。チームメンバや、ウイルス対策ベンダ、他のインシデント対応チームなど有益な情報を持っている可能性のある組織内外の関係者（主たる連絡先と予備の連絡先）の電話番号や電子メールアドレスなど。
	呼び出し情報。エスカレーション先など、組織内のほかのチームに関する情報。
	ポケ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が携帯する。
	代替インターネットアクセス手段。深刻なマルウェアインシデントのためにインターネットへのアクセスができなくなったときに、新たな脅威に関する情報の検索、パッチや更新のダウンロード、およびインターネット上のほかのリソースへのアクセスに使用する。
	作戦本部室。中心となって連絡・調整するために使用する。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続きを策定しておくべきである。
	マルウェアインシデント分析ハードウェアとソフトウェア
	ラップトップコンピュータ。データの分析やパケットのスニッフィングなどを行うための簡単に持ち運びができるワークステーションとして。
	予備のワークステーション、サーバ、ネットワーク機器。マルウェアを隔離された環境で試験するのに使用される。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使用するか、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や CD など、マルウェアのサンプルやそのほかのファイルを必要に応じて格納および移送する場合に使用する。
	パケットスニファとプロトコルアナライザ。マルウェア活動が含まれている可能性のあるネットワークトラフィックを捕捉し分析する。
	信頼のおける最新バージョンの OS の、実行可能ファイルと分析ユーティリティ。フロッピーディスクや CD などに格納しておき、マルウェア感染を示す兆候についてシステムを調べるために使用される。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、システム管理ツール、フォレンジックユーティリティなど。
	マルウェアインシデント分析リソース
	ポートリスト。よく使用されるポートや、トロイの木馬やバックドアに利用される既知のポートなど。
	文書。OS、アプリケーション、プロトコル、ウイルス対策シグネチャ、侵入検知シグネチャなどに関する。
	ネットワーク図と、重要資産一覧。Web サーバ、電子メールサーバ、FTP サーバなど。

[34] NIST の National Software Reference Library（NSRL）は、多数のオペレーティングシステムやアプリケーションのファイルのハッシュを保有している。対応担当者はファイルのハッシュを定期的に作成することもできる。対応担当者は、可能な場合は常に NSRL のプロジェクトが作成したものなどの標準のハッシュセットを利用し、主に組織固有のファイルについてカスタムのハッシュセットを作成するようにするべきである。連邦政府機関では、検証済みの暗号化モジュールに含まれている、FIPS 承認済の暗号化アルゴリズムを使用しなければならないため、対応担当者は可能な場合は常に MD5 ではなく SHA-1 を使ってファイルのハッシュを生成するべきである。

[35] そのほかのリソースについては付録 F を参照。

入手済	ツール／リソース
	基準。想定されるネットワーク、システム、およびアプリケーションの活動の基準。
	マルウェアインシデント軽減ソフトウェア
	媒体。OS のブートディスクおよび CD、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から入手したもの。
	ディスクイメージングソフトウェアとバックアップイメージ。バックアップイメージは、予備の媒体に格納された OS、アプリケーション、およびデータ。

4.2 検知

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。

マルウェアは多くの形態をとり、多くの手段を通じて拡散する可能性があるため、マルウェアインシデントの兆候にはさまざまなものが考えられ、それらの兆候が記録あるいは観測される可能性がある組織内の場所は数多く考えられる。特にマルウェアの脅威が新しい未知のものである場合には、インシデントの原因がマルウェアであることを確認するために、広範な技術知識と経験が要求される大量の分析が必要となる場合がある。インシデント対応担当者は、マルウェアインシデントの検知と確認が完了した後に、インシデントの対応に適切な優先順位を割り当てられるように、問題の種類、範囲、および程度をできるだけ速やかに判断するべきである。4.2.1 項から 4.2.3 項では、マルウェアインシデントの兆候の理解、インシデントの特徴の識別、インシデントの範囲の決定、および対応作業の優先順位付けに関するガイダンスを提供する。

4.2.1 マルウェアインシデントの兆候について

マルウェアインシデントのサインは前兆と兆候の 2 つに分類される。*「前兆」*は、将来マルウェアによる攻撃が発生する可能性を示すサインである。*「兆候」*は、マルウェアインシデントがすでに発生したか、あるいは、現在発生している最中である可能性を示すサインである。

マルウェアの前兆は、そのほとんどが以下のいずれかの形式をとる。

+ **マルウェアに関するアドバイザリ。**ウイルス対策ベンダおよびそのほかのセキュリティ関連組織は、新種の重大なマルウェアの脅威に関するアドバイザリを配布および公開している。インシデント対応担当者はマルウェアアドバイザリのメーリングリストに加入し、数時間後または数日以内に組織に影響を及ぼす可能性のある脅威について、事前に警告を受け取れるようにしておくべきである。また、インシデント対応担当者は、一般的なセキュリティメーリングリストから、あるいはすでにマルウェアによる影響を受けたほかの組織の担当者から、新たなマルウェアの報告を受けることもある。さらに、ウイルス対策ベンダなどのほかの情報源から公に情報を入手する前に、信頼できる情報をサービスの加入者に提供することを目的として、発生しつつあるマルウェアの脅威の識別と分析を行う有料の早期警戒サービスを利用することもできる。
+ **セキュリティツールの警告。**ウイルス対策ソフトウェアや IPS などのツールは、マルウェアの検知、隔離、駆除、あるいはシステムへの感染防止を行うことができる。このような活動により、セキュリティツールから警告が発せられるが、それらの警告は引き続いて発生するイ

ンシデントのサインである可能性がある。たとえば、ある手段を通じてマルウェアがシステムへの侵入を試みたものの失敗し（その結果警告が生成される）、そのあとに同じ種類のマルウェアが、監視されていない攻撃の経路と手段（セキュリティ保護されていないモデムなど）を通じて組織に侵入したり、適切なセキュリティ保護がなされていないシステムにアクセスしたりして、インシデントを引き起こす可能性がある。

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。

インシデントは明確な前兆がないままに発生することが多いが、マルウェアインシデントが進行中であることを示す兆候は数多く存在する場合が多い。兆候の例として次のものがある。

+ Web サーバがクラッシュする。
+ ユーザから、インターネット上のホストへのアクセスが遅い、システムリソースが使い果たされる、ディスクへのアクセスが遅い、システムの起動が遅いという苦情が寄せられる。
+ ウイルス対策ソフトウェアにより、ホストがワームに感染していることが検知され、警告が発せられる。
+ システム管理者が、通常使用されない文字のファイル名を発見する。
+ 監査の設定に変更があったことがホストのログに記録される。
+ ユーザが Web ブラウザを実行しようとするたびに、ユーザのラップトップコンピュータが自動的に再起動する。
+ 疑わしい内容の電子メールが大量に送り返されているのを、電子メール管理者が発見する。
+ ウイルス対策ソフトウェアやパーソナルファイアウォールなどのセキュリティ管理策が、多数のホストで無効にされている。
+ ネットワークトラフィックフローが通常から異常に逸脱しているのをネットワーク管理者が発見する。

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。対応担当者は、数多くのさまざまな情報源からの考えられる兆候をレビューし、それらの情報源のデータを相関づけることにより、マルウェアに関係する活動を識別することに熟練している必要がある。兆候の主な情報源は以下のように、いくつかカテゴリに大きく分類できる。

- **ユーザ。**ユーザはマルウェア関連の兆候をヘルプデスクやそのほかの技術サポートスタッフに報告することが多い。たとえば、ユーザが自身のワークステーションでウイルス対策の警告を目にしたり、運用の障害に遭遇したり、異常な動作に気づいたりすることがある。また、ユーザが感染の原因となり、本来すべきではない、なんらかの操作を誤って実行してしまったあとに、そのことをヘルプデスクに知らせることもある。
- **IT スタッフ。**一般に、システム管理者、ネットワーク管理者、セキュリティ管理者やそのほかの IT スタッフのメンバは、通常の活動に精通しており、期待される動作から大幅に逸脱した動作が観測された場合には、そのことに気付く。
- **セキュリティツール。**ウイルス対策ソフトウェアや IPS などの一部のセキュリティツールには、マルウェアの明確な兆候を記録するものがある。また、ネットワーク監視ソフトウェアなどのツールには、期待される動作からの逸脱を、マルウェア関連として特別に識別することなく、単に報告するものもある。セキュリティツールにより生成される警告やそのほかの情報をマルウェアの検知に役立てるには、それらを頻繁にあるいは継続して監視する必要がある。

マルウェアが示す特徴は多種多様であるため、兆候の包括的な一覧を作成することは現実的ではない。しかし、表 4-2 に、各種のマルウェアと攻撃ツールに起因するマルウェアインシデントの最も可能性のある兆候の一覧を示す。この表は、起こりうるマルウェアインシデントを各個人がより迅速に識別し分類するのに役に立つかもしれない。表 4-2 には、マルウェアが管理者レベルのアクセスに成功した場合のインシデントの兆候は示していない。マルウェアがシステムに管理者レベルでアクセスできた場合、マルウェアは実質的にシステム上で可能なすべての操作を実行できる可能性がある。したがって、そのようなインシデントの兆候はほとんど際限がない。

表 4-2. マルウェアと考えられる兆候

兆候	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア[36]	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
セキュリティツール											
ウイルス対策ソフトウェアの警告	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
スパイウェア検出／駆除ユーティリティの警告					✓	✓				✓	
ネットワークベース侵入防止システムの警告			✓	✓			✓				
ホストベースの侵入検知による、ファイル変更の警告					✓				✓		
ファイアウォールおよびルータのログエントリ			✓				✓				
ホストにおいて観測された活動											
システムを起動できない	✓								✓		
システムの起動中にエラーメッセージが表示される	✓								✓		
システムが不安定になりクラッシュする		✓	✓		✓		✓		✓		

[36] この分類にはボットおよびリモート管理ツールが含まれる。

兆候	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア[36]	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
プログラムの起動や実行が遅い、あるいはプログラムがまったく動作しない	✓	✓	✓		✓				✓	✓	
システムの起動時に未知のプロセスが実行される					✓		✓	✓			✓
通常は使われないポートおよび予期しないポートが開く							✓				
送受信される電子メールの数が急増する		✓		✓					✓		
ワードプロセッサの文書やスプレッドシートなどのテンプレートに変更が加えられる		✓									
Web ブラウザの設定が変更される (ホームページの変更や新しいツールバーの追加など)						✓				✓	
ファイルが削除されたり、破損したり、アクセス不能になったりする	✓	✓			✓				✓		
奇妙なメッセージや画像、重なり合ったメッセージボックスなど、見慣れない項目が画面に表示される		✓				✓			✓		✓
予期しないダイアログボックスが表示され、なんらかの操作の許可を要求される						✓				✓	
ネットワークにおいて観測された活動											
ネットワークの使用が大幅に増加する			✓	✓			✓				✓
脆弱性のあるサービス (開いている Windows 共有や HTTP など) を標的としたポートスキャン、不成功に終わった接続の試み			✓				✓				
ホストと未知のリモートシステムとのあいだのネットワーク接続			✓		✓	✓	✓	✓	✓	✓	✓

4.2.2 マルウェアインシデントの特徴の識別

完全に信頼のおける兆候は存在しない。ウイルス対策ソフトウェアでさえ、害のない活動を悪意のある活動と誤認することがある。そのため、インシデント対応担当者はマルウェアインシデントが疑われる兆候をすべて分析し、マルウェアが原因であること確認する必要がある。組織全体にわたる大規模な感染のような事例であれば、インシデントの兆候は明白なので確認が不要な場合がある。兆候の分析と確認を行う目的は、(インシデント処理担当者が)インシデントの原因がマルウェアであることの確証を可能な限り得て、原因となっているマルウェアの脅威の種類 (ワームやトロイの木馬など) について基本的な理解を持つことにある。インシデントの原因が容易に確定できない場合は、マルウェアが原因であると仮定して対応し、あとでマルウェアが関係していないと分かった時点で対応を変更するほうが良い場合が多い。マルウェアの決定的な証拠が見つかるまで待っていると、対応作業に深刻なマイナスの影響が生じ、組織が被る損害が著しく大きくなるおそれがある。

分析と確認のプロセスの一環として、インシデント対応担当者は通常、検知の源を調べることによってマルウェア活動の特徴を識別する。活動の特徴を理解することは、インシデント対応作業に適切な優先順位を割り振り、効果的な封じ込め、根絶、および復旧の活動を計画するのにたいへん役立つ。インシデント対応担当者は、事前にセキュリティ管理者と共同で、マルウェア情報の検知に

役立てることのできるデータ源を識別しておき、どのような種類の情報が各データ源に記録される可能性があるのかについて理解しておくようにする。また、ウイルス対策ソフトウェアなどの明らかなデータ源に加えて、次のような二次的な情報源についても把握し利用するべきである。

- ファイアウォールおよびルータのログファイル。ブロックされた接続の試みを示すことがある。
- 電子メールサーバおよびネットワークベース IPS センサのログファイル。電子メールのヘッダや添付ファイル名が記録されることがある。
- パケットスニファ、ネットワークベース IPS センサ、およびネットワークフォレンジック分析ツールのパケット捕捉ファイル。マルウェアに関係するネットワークトラフィックが記録されることがある。

検知源のデータを調べ、マルウェアの特徴をいくつか識別できたら、インシデント対応担当者はそれらの特徴をウイルス対策ベンダのマルウェアデータベースで検索し、原因として最も可能性の高いマルウェアを識別する。マルウェアが公になってからしばらく時間が経っている場合、ウイルス対策ベンダ各社が、そのマルウェアに関して次のような情報を大量に得ている可能性が高い。

- マルウェアの分類（ウイルス、ワーム、トロイの木馬など）
- 攻撃されるサービスとポート
- 悪用される脆弱性
- 電子メールの件名、添付ファイル名、添付ファイルのサイズ、本文の内容
- 影響を受ける可能性のあるオペレーティングシステム、機器、アプリケーションなどのバージョン
- マルウェアがシステムに感染する手口（脆弱性、設定の誤りなど）
- 感染したシステムにマルウェアが及ぼす影響（影響を受けるファイルの名前と場所、改ざんされる構成設定、設けられるバックドアポートなど）
- マルウェアの伝染の手口と封じ込めの方法
- マルウェアをシステムから駆除する方法

残念ながら、脅威の相対的な重要度によっては、最新の脅威が数時間または数日のあいだマルウェアデータベースに登録されていないことがある。したがって、インシデント対応担当者は対応作業を速やかに開始できるように、ほかの情報源も検討しなければならないことがある。たとえば、公共のセキュリティメーリングリストを利用することが考えられる。このようなメーリングリストには、マルウェアインシデントの体験談が記載されていることがある。しかし、そのような報告は不完全あるいは不正確なことが多いため、そのような情報源から得られる情報はすべて有効性を確認するべきである。マルウェアの特徴に関する情報が得られる可能性のある別の貴重な情報源は、ほかの組織の担当者である。新種の重大な脅威が世界中で比較的ゆっくりと蔓延しつつある場合、ほかの組織ですでに感染を受け、脅威に関するデータを収集している可能性がある。たとえば、電子メール添付ウイルスの拡散がアメリカ合衆国の東部時間の平日午前 6 時に始まった場合に、東部にある組織のほうが西部にある組織よりも先にウイルスの影響を受けることが考えられる。同様の問題に直面しているほかの組織の担当者と、良好な関係を確立し維持することは、すべての関係者にとってメリットとなる可能性がある。

インシデント対応担当者は、感染した通常のシステムまたはマルウェアテストシステムにおいてマルウェアの振る舞いを調べることもできる。たとえば、感染したシステムからマルウェアのサンプルを入手し、隔離したテストシステムに置くことができる。あるいは、感染したシステムや、感染したシステムのディスクイメージを、隔離したテスト環境に設置することもできる。テスト環境には、マルウェアに関する情報を収集するためのツール一式を組み込む。たとえば、ネットワーク活動を記録するパケットスニファや、テストシステムのファイルの変更を検出するファイル完全性チェッカなどを組み込む。マルウェアテストシステムやマルウェアテスト環境は、さらなる損害を誤って組織に与える危険を冒さずに現在のマルウェアの脅威を分析するのに役立つだけでなく、マルウェアインシデント対応についてスタッフをトレーニングするのにも有用である。

システムでのマルウェアの動作の分析に役立つように、分析担当者は、信頼のおけるツールキットをリムーバブルメディア上に構築するとよい[37]。ツールキットには、マルウェアを識別するための最新のツール（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など）を含めるほか、現在実行中のプロセスの一覧表示やネットワーク接続の表示などを行うツールなど、役立つ可能性のあるユーティリティを含めておく。ツールキットの媒体はマルウェアによる改ざんや感染を防ぐために保護を施す。たとえば、フロッピーディスクを書き込み禁止にしたり、CD のセッションをファイナライズして CD にそれ以上データを書き込めないようにする。このような信頼のおけるツールキットを使用するのは、システム上のマルウェアによって、ウイルス対策ソフトウェアなど、システム自身のセキュリティツールの機能が無効にされたり改ざんされたりして、悪意のある活動が報告されない可能性があるためである。保護が施された検証済みのツールキットからツールを実行することにより、インシデント対応担当者はシステム上での活動をより正確に把握することができる。

4.2.3 インシデントへの対応の優先順位付け

マルウェアインシデントの確認が済んだら、次の作業は、対応の優先順位付けである。ワームなど特定の形態のマルウェアは、非常に急速に広まる傾向があり、数分または数時間のうちに大きな影響を及ぼしかねない。そのため、そのようなマルウェアへは高い優先順位の対応が必要となることが多い。トロイの木馬などそのほかの形態のマルウェアは、単独のシステムに影響を及ぼす傾向があり、そのようなインシデントへの対応は、対象システムが提供するデータやサービスの価値に基づいて決定する。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

[37] 信頼のおけるツールキットを作成する際の選択肢の 1 つは、既存の LiveCD の使用がある。LiveCD は、起動可能なオペレーティングシステムを収めた CD である。LiveCD を使用してシステムを起動することにより、分析担当者はシステム自身のオペレーティングシステムを起動せずにシステムの内容を調べることができる。LiveCD には、各種オペレーティングシステムの多数のバージョンに対応したものが存在する。

4.3 封じ込め

マルウェアの封じ込めには、マルウェアの拡散の阻止と、システムのさらなる被害の防止という、2 つの主要な要素がある。封じ込めの措置は、ほとんどすべてのマルウェアインシデントに対して必要である。インシデントに対応する際には、早期の段階でどのような封じ込め手段を最初に利用すべきかを組織で決めることが重要になる。隔離されたインシデントや、感染しない形態のマルウェアによるインシデントの封じ込めは一般に単純であり、感染したシステムのネットワーク接続を解除したり、システムを停止するなどの措置となる。より広範囲にわたるマルウェアインシデントの場合、組織はほとんどのシステムに対して可能な限り迅速にインシデントを封じ込める方策を採用すべきである。そうすることで、感染するマシンの数を限定し、発生する損害を減らし、すべてのデータとサービスを完全に復旧するのに要する時間を短縮できる。

マルウェアインシデントの封じ込めにあたっては、マルウェアの拡散を阻止することが必ずしもシステムへのさらなる損害をすべて防ぐとは限らない点を理解することが重要である。組織で拡散を阻止したあとでも、システム上のマルウェアが引き続きデータやアプリケーション、OS ファイルなどに感染したり、それらのファイルを削除したりすることがある。また、ネットワーク接続が失われたり、そのほかの封じ込め措置が実行されたりした時点で、さらに損害を引き起こすように作成されているマルウェアもある。たとえば、感染したシステムにおいて、別のシステムに定期的に接触する悪意のあるプロセスが実行されることがある。感染したシステムのネットワーク接続を解除したためにその接続が失われると、マルウェアによってホストのハードディスクドライブ上のデータがすべて上書きされてしまうことがある。このような理由から、対応担当者は、ホストのネットワーク接続を解除したからといってホストへのさらなる損害を防げたとみなしてはならず、多くの場合、さらなる損害を防ぐためにできるだけ速やかに根絶作業を始めるべきである。

封じ込めに関する決定は、組織が受容し得るリスクの程度を反映したものになるが、組織はそうした決定を下す際の方針や手続きを設けておくべきである。たとえば、重要な機能を実行しているシステムが感染した場合、システムの隔離や停止を行わないことによって生じるセキュリティリスクよりも、それらの機能が利用できなくなることから生じるうる損害のほうが大きいと判断される場合、ネットワークへのシステムの接続を解除したり、システムを停止したりしないことを組織で決定することが考えられる。この封じ込めの方針は、インシデント対応担当者が具体的な状況の特徴に応じて適切な組み合わせの封じ込め手段を選択できるようにするものとする。

封じ込め手段は以下の 4 つの基本分類に分けることができる。つまり、「ユーザの関与に頼る方法」、「自動検知の実行」、「サービスの一時停止」、および「特定の種類のネットワーク接続のブロック」である。4.3.1 項から 4.3.4 項では、これらの分類について詳しく説明する。

4.3.1 ユーザの関与による封じ込め

ユーザの関与は、特に大規模なインシデントにおいては、封じ込め作業における有効な要素となる可能性がある。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。また、マルウェアの根絶についての説明を作業指示に盛り込むことも考えられる。たとえば、ウイルス対策シグネチャを更新してシステムスキャンを実施したり、専用のマルウェア根絶ユーティリティを入手して実行したりすることなどが考えられる。このような措置をユーザに実施してもらうことは、管理されていない環境など、完全に自動化された封じ込め対策（4.3.2 項から 4.3.4 項の説明を参照）が可能でない状況において特に役立つ。

4.1.2 項で説明したように、有益な情報を適切なタイミングで効果的にユーザに伝達することは困難である。電子メールは通常、最も効率的な伝達のメカニズムだが、重大なインシデントの発生時には使用できない可能性がある。また、ユーザが手遅れになるまで電子メールを読まないおそれもある。したがって、組織はユーザに情報を伝達するための代替メカニズムを複数用意しておくべきである。たとえば、組織内のすべての音声メールボックスにメッセージを送信したり、作業現場に掲示板を掲げたり、建物や事務所の入口で作業指示を手渡したりすることなどが考えられる。ログイン時にシステムメッセージを表示することは多少は効果があるかもしれないが、ユーザは 1 回のログインで数日から数週間のあいだログアウトしないことが多い。また、ユーザの多くはそのようなメッセージを無視する傾向が強い。多数のユーザがさまざまな場所（自宅の事務所や小規模の支店など）にいる組織では、そのようなユーザが確実に網羅されるような伝達メカニズムを用意する。もう 1 つ考慮すべき重要な事項は、クリーンアップユーティリティなどのソフトウェア、あるいはパッチや最新のウイルス対策シグネチャなどのソフトウェア更新を、ユーザに提供しなければならない場合があることである。組織では、封じ込めを支援することが期待されるユーザに対して、ソフトウェアユーティリティや更新を送り届けるための複数の手段を明らかにして実装するべきである。

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。封じ込めのガイダンスをどのように伝えたとしても、ユーザ全員がその指示を受け取り、自分が関係するかもしれないと認識するという可能性は少ない。また、封じ込めの指示を受け取ったユーザの中には、理解不足や、指示に従う際の単純なミス、あるいは、システム固有の特徴のためにそのシステムにとって誤った指示となってしまうことなどが原因で、指示に正しく従うことができない人がいる可能性もある。さらに、通常の業務の遂行に専念していて、マルウェアが各自のシステムに与えうる影響について無関心のユーザがいる可能性もある。とはいえ、組織のシステムの相当な数が関係する大規模なインシデントの場合には、ユーザが封じ込めに関与することによって、インシデントへの対応に当たるインシデント対応担当者や技術サポートスタッフの負担を大幅に軽減することができる。

4.3.2　自動検知による封じ込め

マルウェアインシデントの多くは、主に 3.4 項で説明した自動化技術を利用した感染の防止と検知によって封じ込めることができる。これらの技術には、ウイルス対策ソフトウェア、電子メールフィルタ処理、侵入防止ソフトウェアなどがある。ホスト上のウイルス対策ソフトウェアは、感染を検知して駆除できるため、封じ込めの支援に優先的に利用されることの多い自動検知の手段である。新種のマルウェアの脅威を認識または阻止できなかった検知ツールは一般的に、あとになって同じマルウェアの特徴を認識して拡散を阻止するように更新または設定しなおすことができる。残念ながら、重大なインシデントの発生時にそのような措置を適切なタイミングで実施するのは難しい場合がある。たとえば、大量のマルウェア活動によってすでに深刻な被害を受けているネットワークやシステム（ウイルス対策サーバなど）を使用してソフトウェア更新を配布することは、現実的ではない可能性がある。特に、組織内の多数または大半のホストにできるだけ速やかに更新を配布する必要がある場合にはなおさらである。この種の問題は、ソフトウェア更新用のネットワーク帯域幅を予約しておき、自動検知技術用の堅牢な分散アーキテクチャを構築することによって、多少は軽減することができる。しかし、マルウェアの脅威の中には、ネットワークの大半の通信を一時的に機能停止に陥れるほど深刻なものがある。そのうえ、たとえ更新を配布できたとしても、すべてのシステムを即座に更新することは通常は不可能である。たとえば、ウイルス対策ソフトウェアが有効になっていないシステムや、正しく設定されていないシステムが存在する可能性がある。特に、この最後の問題は管理されていない環境の特徴の 1 つである。管理されていない環境では、ユーザが自身のシステムを制御している度合いが大きい傾向がある。しかし、マルウェアによってはウイルス対策ソフトウェアやそのほかのセキュリティ管理策を無効にするものがあり、管理された環境であっても、システムの大部分を自動的に更新することが不可能な場合がある。

広範囲にわたるインシデントでは、更新済みのウイルス対策ソフトウェアでマルウェアを識別できない場合や、最新のシグネチャがまだ完全には行き渡っていない場合、組織はウイルス対策シグネチャによる封じ込めを効果的に実施できるようになるまでのあいだ、ほかのセキュリティツールを使用してマルウェアを封じ込められるように備えておくべきである[38]。最新のシグネチャを入手したら、配備の前に少なくとも最小限のテストを行い、更新そのものが組織にマイナスの影響を及ぼさないことを確認するのが賢明である。複数のセキュリティツールを使用して自動の検知および封じ込めの活動を行うもう 1 つ理由として、負荷の分散がある。大量の感染が発生した場合、マルウェアインシデントの作業負荷の処理をすべてウイルス対策ソフトウェアに任せることは非現実的である。マルウェアの検知とブロックを行うための数段構えの防御体制を組織で採用することにより、作業負荷を複数のコンポーネントに分散することができる。また、複数の種類の自動検知機器を用意することのメリットは、それぞれの機器が効果を発揮する検出機能が、状況に応じて異なる点にある。ウイルス対策ソフトウェア以外の自動検知手段の例として次のものがある。

+ **電子メールのフィルタ処理。**電子メールサーバおよびクライアントに加え、スパム対策ソフトウェアは、既知の不正な件名や送信者、メッセージテキスト、添付ファイルの名前や種類など、一定の特徴を持つ電子メールや電子メール添付ファイルをブロックするように設定できる[39]。ただし、マルウェアが利用する特徴はますます広範囲にわたっている。たとえば、正規の電子メールでも使用されている可能性のある、数百もの異なる件名を使用するウイルスも存在する。ウイルスによっては、無作為の件名や添付ファイル名を生成するものや、既存の害のない電子メールに対して返信を生成するものさえ存在する。このようなウイルスに対しては電子メールのフィルタ処理手段が役に立たないことがある。また、ほとんどの悪意のある添付ファイルには、疑わしいファイル拡張子が付いている（特に、*.bat*、*.cmd*、*.exe*、*.pif*、*.scr* など）。しかし、かつては害のなかった*.zip* などの拡張子が悪意のある添付ファイルに使用されることが流行してきている。

+ **ネットワークベース IPS ソフトウェア。**ほとんどの IPS 製品は、その防止機能を特定のシグネチャに対して有効にすることができる。ネットワークベース IPS 機器をインラインにした場合、つまり、ネットワークのアクティブな一部とし、マルウェア用のシグネチャを持たせると、マルウェアを識別して、マルウェアが標的に到達するのを阻止することができる。IPS 機器で防止機能を有効にしない場合は、深刻なインシデントが発生した際に、1 台以上の IPS センサを再設定または再配備して、活動を阻止できるように IPS を有効にするのが賢明である可能性がある。IPS 技術は、送受信両方向の感染の試みを阻止できなければならない。もちろん、マルウェアの封じ込めにおける IPS の価値は、マルウェアを識別するためのシグネチャの入手が可能かどうか、およびその正確性によって決まる。いくつかの IPS 製品では、マルウェアの既知の特徴の一部に基づいて管理者がカスタムのシグネチャを作成したり、既存のシグネチャをカスタマイズしたりできる。たとえば、管理者は IPS を利用して、電子メールにおける既知の不正な添付ファイル名や件名を指定したり、既知の不正な送信先ポート番号を指定したりできる。多くの場合、IPS の管理者は、ウイルス対策ベンダからシグネチャを入手できる何時間も前に、独自の正確なシグネチャを用意することができる。また、IPS シグネチャはネットワークベース IPS センサにのみ効果があるが、ウイルス対策シグネチャは一般にすべてのワークステーションとサーバに効果がある。そのため、一般に新しい

[38] インシデント対処担当者はまた、未知のマルウェアのコピーをウイルス対策ベンダやそのほかのセキュリティソフトウェアベンダに送付して分析してもらうための組織のポリシーや手続きにも精通している必要がある。このような措置によって、新たな脅威にベンダがより迅速に対処できるようになる。また、必要に応じ、組織のポリシーの許す範囲で、インシデント対処組織やウイルス対策ベンダなどの信頼のおける第三者と連絡を取り、新たな脅威への対応に関するガイダンスを受けるようにする。

[39] 一般に、組織全体にわたって特定の電子メールや電子メール添付ファイルをブロックするように電子メールクライアントを設定することは、高度に管理された環境においてのみ実現可能である。

ウイルス対策シグネチャに比べ、新しい IPS シグネチャを速やかに配備するほうがリスクが少ない。

+ **ホストベース IPS ソフトウェア。**ホストベース IPS 製品の中には、特定の実行可能ファイルの実行を制限できるものがある。このような製品では、管理者が、実行されるべきでないファイルの名前を指定できる。新たな脅威に対応したウイルス対策シグネチャをまだ入手できない場合、その脅威の一部となっているファイルの実行をブロックするようにホストベース IPS ソフトウェアを設定できる場合がある。

4.3.3 サービスの無効化による封じ込め

マルウェアインシデントによっては、もっと徹底的な、機能停止を伴う可能性のある封じ込め措置を必要とするものがある。たとえば、インシデントに起因するネットワークトラフィックやアプリケーションの活動（電子メールやファイル転送など）の量があまりにも多くなり、多数のアプリケーションが事実上使用不能になることがある。そのようなインシデントは、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。また、サービスが感染経路となったり、感染したホストからデータを転送する経路となったりすることもある。いずれの場合も、影響を受けているサービスを停止することが、ほかのすべてのサービスを停止することなく感染を封じ込める最善の手段になると考えられる。通常、この措置はアプリケーションレベルで実行されるか（サーバ上のサービスを無効にするなど）、ネットワークレベルで実行される（サービスに対応する IP アドレスまたはポートを遮断するようにファイアウォールを設定するなど）。目標は、最小限の機能を無効にしながら、インシデントを効果的に封じ込めることである。ネットワークサービスの無効化を支援するために、組織は使用しているサービスの一覧と、各サービスで使用されている TCP ポートおよび UDP ポート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。電子メールサーバは、電子メールを介して拡散しようとするウイルスやワームによって完全に飽和状態になる可能性がある。電子メールサーバを停止して電子メール添付マルウェアの拡散を食い止めることで、たいていの場合、一部のマルウェアインシデントを迅速に封じ込めることができる。しかし、組織には、ファイルサーバで誤って電子メールサーバが実行されているなど、停止する必要があるものの、その存在が知られていない電子メールサーバもある。そのような場合、封じ込めが遅れる可能性がある。状況がそれほど深刻でなければ、電子メールサービスの一部を無効にすることで、すべての電子メールサービスを停止することなく封じ込めを効果的に行える場合がある。たとえば、投稿無制限のメーリングリストを一時的に無効にすることによって、マルウェアの拡散と電子メールサーバの負荷が大幅に減少することがある。

サービスの無効化は、技術的な観点から見れば一般に単純なプロセスだが、それがもたらす結果を理解することは難しい場合が多い。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。たとえば、電子メールサービスを無効にした結果、電子メールを通じて情報を複製しているディレクトリサービスに支障が生じる可能性がある。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。また、同様の機能を持つ代替のサービスを提供すると役立つ可能性がある。たとえば、高度に管理された環境では、ある電子メールクライアントの脆弱性が新種のウイルスによって悪用されようとしている場合に、ユーザに対してその電子メールクライアントの利用を一時的に中止して、代わりに脆弱性のない Web ベースの電子メールクライアントを利用してもらうようにすることができる。このような措置は、電子メールへのアクセスを

ユーザに提供しつつ、インシデントを封じ込めるのに役立つ。同じ方策を、Web ブラウザやそのほかの一般的なクライアントアプリケーションの脆弱性を悪用するインシデントの場合にも適用できる。

また、別の組織がマルウェアインシデントに対応するためにその組織のサービスを無効にすることがあるが、それによって生じる問題についても対応できるよう準備しておくべきである。たとえば、組織内のチームが一時的に別の組織のための作業を行う場合に、チームメンバの電子メールが別の組織の電子メールシステムのアカウントに転送されるようにアカウントを設定している場合がある。この場合、他方の組織で電子メールサービスが無効にされると、転送された電子メールが送り返され、再度転送され、再び送り返される、という具合にメールループに陥ることになる。このような状況になると、少数のユーザアカウントが原因で電子メールサービスの著しいパフォーマンス低下が生じるおそれがある。

4.3.4 接続の無効化による封じ込め

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。たとえば、感染したシステムが、ルートキットをダウンロードするために複数の外部システムのいずれか 1 つに接続しようとしている場合、対応担当者は外部システムの IP アドレスへのアクセスをすべて遮断することを検討してみる。同様に、組織内部の感染したシステムがマルウェアの拡散を試みている場合には、状況をコントロールして、感染したホストを物理的に特定してマルウェアを駆除するあいだ、そのシステムの IP アドレスからのネットワークトラフィックを遮断できる。また、特定の IP アドレスのネットワークアクセスを遮断する方法に代わり、感染したシステムをネットワークから切り離すという方法もある。これは、ネットワーク機器を設定しなおしてネットワークアクセスを拒否するか、ネットワークケーブルを物理的に取り外すか、または着脱可能なネットワークインタフェースカードを感染したシステムから取り外すことで実現できる。

最も徹底的な封じ込め措置は、感染していないシステムに必要なネットワーク接続を意図的に遮断することである。その場合、リモートのダイアルアップユーザや VPN ユーザなどのシステムのグループがネットワークにアクセスできなくなることがある。最悪の場合には、マルウェアの拡散を阻止し、システムへの損害を食い止め、脆弱性軽減のための機会を得るために、主ネットワークからサブネットを隔離したり、組織全体をインターネットから切り離したりすることさえ必要になる場合もある。接続の広範な喪失によって封じ込めを実施することが、組織にとって受け入れられる可能性が最も高いのは、マルウェアの活動のためにすでに深刻なネットワークの機能不全が発生している場合や、感染したシステムからほかの組織に対する攻撃が仕掛けられている場合などである。接続の大規模な喪失は、常に組織上の多くの機能に影響を与える。そのため、通常はできるだけ早く接続を回復する必要がある。

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。ワークステーションを標的としたマルウェアインシデントが発生しても、感染したワークステーションのサブネットを主ネットワークから隔離することで、サーバのサブネットでは引き続き、外部の顧客や感染していないワークステーションのサブネットに機能を提供できる。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。このデザインでは、ホストがネットワークに接続しようとすると、ホストのセキュリティ状況が確認される。この確認は、ホストのさまざまな特性(OS のパッチの適用状況やウイルス対策の更新状況）を監視するエージェントを各ホストに配置して実現することが多い。ホストからネットワークへの接続が試みられると、ルータなどのネットワーク機器によって、ホストのエージェントからの情報が要求される。ホストが要求に応答しない場合や、ホストが安全ではないことが応答で示された場合には、ネットワーク機器によってホストが別の VLAN 上に配置される。同じ技法を、組織の通常のネットワ

ーク上にすでに存在するホストに対しても使用できる。これにより、感染したホストを自動的に別の VLAN に移動することが可能になる[40]。

感染したホストのために独立の VLAN を用意することは、ウイルス対策シグネチャの更新や、OS およびアプリケーションのパッチをホストに提供する一方で、ホストによる実行が可能な操作を厳しく制限するのに役立つ。独立の VLAN がなければ、感染したホストのネットワークアクセスを完全に取り除かなければならない可能性がある。その場合、マルウェアを封じ込めて根絶し、脆弱性を軽減するために、更新を各ホストに手動で転送して適用しなければならない。独立した VLAN を効果的に利用するための別の方法として、すべてのホストを VLAN 内の特定のネットワークセグメントに配置し、その後各ホストがクリーンな状態になり、パッチが適用されたと判断された時点で、ホストを実稼動のネットワークに移動するという方法がある。この方法は状況によっては効果を発揮する可能性がある。VLAN を使用する場合の欠点の 1 つは、感染したホストからのトラフィックが引き続き実運用のトラフィックと同じ機器を通じて搬送される点である。VLAN は、論理的な分離は実現するが、物理的な分離は実現しない。その結果、マルウェアの活動と、システムの更新、およびシステムへのパッチ適用によって、大量のトラフィックが VLAN 上に生じ、ネットワーク機器のすべてのユーザに運用上の問題を引き起こす可能性がある。

4.3.5 封じ込めに関する推奨事項

封じ込めは、すでに説明した 4 つの分類（ユーザ、自動検知、サービスの喪失、接続の喪失）における数多くの手段を通じて実施できる。あらゆる状況に対して適切または効果があるような、単一のマルウェア封じ込めの方策や個別の手段は存在しない。そのため、インシデント対応担当者は、現在のインシデントを封じ込める効果がある一方で、システムへの損害を限定し、封じ込め手段がほかのシステムに及ぼす可能性のある影響が少なくなるような、封じ込め手段の組み合わせを選択するべきである。たとえば、すべてのネットワークアクセスを停止することは、マルウェアの拡散を阻止するのにはたいへん効果的かもしれないが、システム上の感染によるファイルの破壊を引き続き許してしまい、組織の重要な機能の多くが停止してしまうことにもなる。

ほとんどの組織では、最も徹底的な封じ込めの方法が許されるのは短時間のあいだだけである。したがって、封じ込めの際に適切な決定が下されるように、封じ込めに関してだれが重要な決定を下す権限を持つのか、および、各種の措置（たとえば、インターネットから組織を切り離すなど）がどのような状況のもとで適切なのかを、ポリシーの中で明確にするべきである。

4.3.6 感染したホストの識別

マルウェアに感染したホストを識別することは、すべてのマルウェアインシデントにおいて行うことであり、広範囲にわたるインシデントの場合には特に重要である。感染したホストを識別すれば、適切な封じ込め、根絶、および復旧の措置を講じることができる。残念ながら、感染したホストの識別はコンピューティングの動的な性質のために複雑になる場合が多い。たとえば、ユーザはシステムを停止したり、ネットワーク接続を解除したり、さまざまな場所に移動したりするため、どのホストが現在感染しているのかを識別することがきわめて困難になる。また、ホストによっては複数の OS を起動できるものや、仮想のオペレーティングシステムソフトウェアを使用できるものがある。そのような場合、ある OS においてシステムが感染していても、システムが現在別の OS を使用していると感染を検知できないことがある。

[40] Microsoft は、このためのプラットフォームとして NAP（Network Access Protection）と呼ばれるプラットフォームを開発した。NAP の詳細については http://www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx を参照。

また、感染したホストの正確な識別がほかの要因によっても複雑化する可能性がある。たとえば、脆弱性が軽減されていないシステムでは、駆除と再感染が何度も発生することがある。マルウェアの中には、ほかのマルウェアの痕跡の一部または全部を実際に削除するものがある。そのような場合、感染が部分的に、または完全に削除され、検出されないままになってしまう可能性がある。大規模なインシデントに巻き込まれたすべてのホストを識別することは、感染しているシステムの数が非常に多くなるため特に難しくなる場合が多い。加えて、感染しているホストに関するデータが、ウイルス対策ソフトウェアや IDS、ユーザレポートなどの、複数の情報源から得られる可能性があり、それらを整理して最新に保つのはたいへん難しくなる。

すべての識別を自動的な手段を通じて実行できれば理想的だが、さまざまな理由のため（4.3.6.1 項から 4.3.6.2 項を参照）、通常は不可能である。ほとんどの組織では、インシデントの発生時に、感染したシステムの識別と報告をユーザに要請したり、個々のシステムを技術スタッフに個別に検査させたりするなど、手作業による識別手段を通じて包括的に識別を行うことは、現実的ではない。組織では、規模の大きなマルウェアインシデントが発生する前に、ホストの識別に関する問題について慎重に検討しておくべきである。そうすることによって、識別のための複数の方策を有効な封じ込め方策の実装の一環として利用できるようになる。また、組織はどのような種類の識別情報が必要となる可能性があり、どのデータ源にそれらの情報が記録されている可能性があるかを判断するべきである。たとえば、リモートでの措置にはホストの現在の IP アドレスが必要になるのが普通である。もちろん、ローカルでの措置の場合はホストの物理的な場所が必要になる。ある情報を利用してほかの情報を調べることができる場合が多い。たとえば、IP アドレスを MAC（媒体アクセス制御）アドレスにマッピングし、さらにその MAC アドレスを、特定のオフィスグループにサービスを提供しているスイッチにマッピングできる場合がある。ネットワークログイン時にマッピングを記録するなどの手段で、IP アドレスをシステムの所有者やユーザにマッピングできれば、その所有者やユーザに連絡してホストの場所を教えてもらうことができる。

感染しているホストの物理的な場所を特定する難しさは、いくつかの要因に左右される。管理された環境では、物事の遂行方法が標準化されているため、ホストの場所を特定することは比較的容易なことが多い。たとえば、システム名にユーザの ID やオフィス番号、あるいはシステムのシリアル番号（ユーザ ID に結び付けられる可能性がある）が含まれていることがある。また、資産目録管理ツールに、ホストの特性に関する最新の情報が含まれていることもある。それ以外の環境、特にユーザがシステムを完全に自分の管理下においていて、ネットワークの管理が一元化されていないような環境では、マシンから場所をたどることが難しい場合がある。たとえば、管理者は 10.3.1.70 というアドレスのシステムが感染したとみられることはわかるものの、そのマシンがどこにあり、だれが使用しているのかはまったくわからないことがある。管理者は、感染しているシステムをネットワーク機器を通じて突き止めなければならないことがある。たとえば、スイッチポートマッパは、スイッチをポーリングして特定の IP アドレスを調べ、その IP アドレスに関連付けられているスイッチポート番号とホスト名を識別できる。感染しているシステムが複数のスイッチを隔てた場所にあると、1 台のマシンを突き止めるのに数時間を要することがある。感染しているシステムがスイッチを直接経由していない場合でも、管理者は各種の配線設備やネットワーク機器を通じて接続を手動で追跡しなければならないことがある。あるいは、感染したと考えられるシステムのネットワークケーブルを取り外すか、スイッチポートを停止して、ユーザが通信不全を報告してくるまで待つという手段もある。この方法の場合、感染していない少数のシステムの接続が意図せずに失われるおそれがある。しかし、識別および封じ込めのための最終手段として慎重に実行すればきわめて有効になりうる。

組織によっては、まず相応の努力を払って感染しているホストを識別し、それらのホストを対象に封じ込め、根絶、および復旧の作業を実施したあと、まだ未感染として確認されておらず、適切なセキュリティ保護が施されていないホストがネットワークに接続しないような措置を講じている。このような措置を講じる際は、あらかじめ十分な検討を行い、インシデント対応担当者に対して、特定の状

況下でホストを締め出す権限を事前に書面で与えておく。一般に、締め出しの措置は、MAC アドレスや静的 IP アドレスなど、特定のホストの特徴に基づいて決められるが、システムが単独のユーザに対応する場合にはユーザ ID に基づいて実行することもできる。別の可能性として、ネットワークログインスクリプトを使用して感染しているホストへのアクセスを識別して拒否する方法もある。しかし、感染しているシステムが起動直後、ユーザ認証の前にマルウェアの拡散を始めた場合、この方法は効果がないことがある。4.3.4 項で説明したように、感染したホストや未確認のホスト用に独立の VLAN を用意することは、感染を検出するメカニズムが信頼のおけるものである限り、システムを締め出すためのよい手段となる。締め出し措置は極端な状況の場合にのみ必要となると考えられるが、組織では必要に応じて締め出しを即座に行えるように、どのようにすれば個々のホストやユーザを締め出せるのかを事前に検討しておく。

4.3.6.1 項から 4.3.6.3 項では、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、および手動識別について説明する。

4.3.6.1 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処理（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。セキュリティアプリケーションのログには疑わしい活動の詳細な記録が含まれていることがある。それらの記録は、セキュリティ侵害の発生または阻止を示すこともある。セキュリティアプリケーションが管理された状態で組織に配備されていれば、個々のホストと中央のアプリケーションログの両方でログを参照できる可能性がある。

必要な情報が通常の証拠の情報源に含まれていない場合には、次のような二次的な情報源に注目しなければならない場合がある。

- **ネットワーク機器のログ。**接続活動を記録するファイアウォールやルータ、そのほかのフィルタ処理機器、あるいはネットワーク監視ツールは、特定のマルウェアの特徴を示すネットワーク接続活動（特定のポート番号の組み合わせや、見慣れないプロトコルなど）を識別するのに役立つことがある。
- **シンクホールルータ。**「*シンクホールルータ*」は、未知の経路（未使用のサブネット上の送信先 IP アドレスなど）を持つトラフィックをすべて受信する組織内部のルータである。このようなトラフィックは伝染を試みるマルウェアに起因する場合がある。したがって、シンクホールルータによって観測されるトラフィックの中にいつもと異なる変化が見つかれば、新たなマルウェアの脅威を示している可能性がある。未知の経路を持つネットワークトラフィックをすべて捕捉できるシンクホールルータを設置すると、ほかのシステムへの感染を試みている組織内の感染しているシステムを識別するのに有効な場合がある。通常、シンクホールルータは、受信トラフィックに関する情報をログサーバと IDS に送信するように設定される。また、パケットスニファも疑わしい活動の記録に使用されることがある。
- **アプリケーションサーバのログ。**電子メールや HTTP など、マルウェアの感染メカニズムとして利用されることが多いアプリケーションのログには、どのホストが感染したかを示す情報が記録されることがある。1 つの電子メールメッセージに関する情報が、送信端末から受信端末まで、複数の場所に記録されることがある。たとえば、送信者のシステムや、メッセージを処理する個々の電子メールサーバ、受信者のシステムのほか、ウイルス対策サーバ、スパムフィルタ処理サーバ、コンテンツフィルタ処理サーバなどに、情報が記録されること

がある。同様に、Web ブラウザを実行しているホストで、悪意のある Web 活動に関する情報が豊富に得られる可能性がある。たとえば、お気に入り Web サイトの一覧、アクセスした Web サイトの履歴、アクセスした日付と時刻、キャッシュされた Web データファイル、クッキー（作成日と有効期限を含む）などの情報が得られる。DNS サーバのログも情報源として役に立つ。DNS サーバのログには、感染しているホストから悪意のある外部サイトの IP アドレスを取得しようとした兆候が示されることがある。感染しているホストは、これらのサイトにデータを転送しようとしたり、あるいは単にやり取りをしようとしたりする。

+ **ネットワークフォレンジックツール。**ネットワークフォレンジック分析ツールやパケットスニファなど、パケットを捕捉し記録するソフトウェアプログラムには、マルウェアの活動について特に詳細な情報が記録されることがある。ただし、これらのツールはネットワーク活動のほとんどまたはすべての情報を大量に記録するため、必要な情報だけを抽出するのにかなり時間を要する場合がある。感染しているホストを識別するための、より効率的な手段が利用できる場合が多い。

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。しかし、データソースによってはデータの抽出に相当の時間を要する場合がある。また、イベント情報はすぐに陳腐化するので、それが原因で、感染していないホストが不必要な封じ込めの対象となったり、感染しているホストが封じ込め措置を回避したりするおそれがある。正確かつ包括的で、適度に新しいフォレンジックデータの情報源が利用できれば、感染しているホストを識別するのに最も有効な手段になると考えられる。

4.3.6.2 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。動的識別は次に示すようないくつかの方法を通じて実行できる。

+ **ログインスクリプト。**ネットワークログインスクリプトは一般に変更を加えることで、特定のホストの特性を調べてマルウェアの兆候がないかを確認できる。ログインスクリプトを通じてホストを識別する場合の不利な点は、感染しているホストが感染から数日、数週間、あるいは数か月を経過しないと、いったんネットワークを離れて再接続を試みることをしない場合がある点である。

+ **ネットワークベース IPS または IDS のカスタムシグネチャ。**感染しているホストを識別するための IPS または IDS のカスタムシグネチャを作成するのは、有効な手法となる場合が多い。組織によっては、強力なシグネチャ作成機能を備えた IPS または IDS センサをそれぞれ独立に設置しているところがある。これらのセンサはマルウェア感染の識別専用として使用できる。これにより、高品質な情報源が提供されると同時に、ほかのセンサがマルウェアの警告によって過負荷になるのを防ぐことができる。

+ **パケットスニファ。**特定のマルウェアの脅威の特徴に一致するネットワークトラフィックだけを探し出すように、パケットスニファを設定すると、感染しているホストの識別に有効な場合がある。パケットスニファは特に、マルウェアから生成されるネットワークトラフィックのほとんど、あるいは全部が同じネットワーク機器または少数の機器を経由しようとする場合に役立つ。

- **脆弱性評価ソフトウェア。**ホストの脆弱性を識別するように作成されているソフトウェアプログラムの多くは、既知の特定のマルウェアの脅威も検出できる。ただし、脆弱性評価ソフトウェアは、通常は新たな脅威に感染したホストの識別には役立たない。また、脆弱性評価ツールの多くは、ホストベースファイアウォールを使用しているホスト上に存在する脆弱性を検出できない場合がある。
- **ホストスキャン。**特定のマルウェアの脅威が原因となり、特定のポートを傍受するバックドアが、感染したホストで実行された場合、そのポートに対してホストスキャン を実行すると、感染しているホストの検索に有効な場合がある。
- **そのほかのスキャン。**ホストスキャン以外の種類のスキャンも、特定の特徴を持ったホストの検索に役立つことがある。たとえば、特定の構成設定や特定のサイズのシステムファイルなど、感染を示す特徴をスキャンできる。

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。たとえば、パーソナルファイアウォールを実行しているホストでは、ホストスキャンによる感染の識別が成功しないことがある。これは、ファイアウォールによってスキャンがブロックされるためである。しかし、パケットスニファやログインスクリプトならば、そのようなホストでも感染を識別できる可能性がある。動的なアプローチの組み合わせは非常に正確な結果を示せるが、感染の状態は絶えず変化し、データは一定の期間にわたって収集されるため、動的なアプローチは繰り返し実行する必要がある。

4.3.6.3 手動識別

感染しているホストを識別するもう 1 つの手段は、手動によるアプローチである。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。感染に起因するトラフィックによってネットワークが完全に飽和している場合、動的な方法による識別が不可能になることがある。マルウェアのネットワークトラフィックによって、なりすましのアドレスが使用され、大量の活動が生じると、有効なエントリが莫大な量のデータに埋もれてしまい、フォレンジックによる識別が事実上不可能になることがある。また、多くの管理されていない環境で見られるように、ユーザが自分のシステムを管理下においている場合には、システムごとに特徴がまったく異なる可能性があるため、自動識別手段の結果がきわめて不完全で不正確になることがある。こうした状況では、主として手動による方法が最善の選択肢となる可能性がある。

手動による方法を実施するにはいくつかの可能な手法が存在する。その 1 つは、ユーザ各自が感染を識別するように要請する方法である。そのためには、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に関する情報をユーザに提供する必要がある。これらの情報は CD やそのほかの媒体に収めて配布しなければならない場合がある。同様の手動による手法として、すべてのシステム、または感染の疑いがあるシステムを、現場の IT スタッフ（ふだんマルウェアインシデントへの対応に参加しない個人も含む）に検査してもらう方法がある。場合によっては、IT スタッフのいないリモートオフィスで、非 IT スタッフがこの作業を行わなければならないこともある。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。

4.3.6.4 識別に関する推奨事項

動的な方法による識別は通常、結果が最も正確であるが、感染を識別する最速の手段でない場合が多い。組織内のすべてのホストをスキャンするのに相当な時間を要することがある。また、接続が解除されたシステムや電源が落とされたシステムは識別されないため、スキャンを繰り返し行う

必要が生じる。フォレンジックデータが新しいものであれば、その情報が包括的でないにしても、すぐに利用できる情報の適切な情報源となる。一般に、手動による方法は、組織全体を対象とした包括的な識別の手段としては実際的ではないが、ほかの手段が利用できない場合には必要な識別手段となり、ほかの手段では不十分な場合にその不足分を補うことができる。多くの場合、複数の方法を同時に、または順番に実施することによって、最善の結果を最も効果的に得ることができる。

組織では、各自の環境で可能な方法について前もって慎重に検討し、十分な数の識別の方法を選択し、選択したそれぞれの方法を重大なマルウェアインシデントの発生時に効果的に実施するための手続きと技能を開発する。また、識別作業の支援が可能な個人またはグループも明らかにしておく。たとえば、識別作業を行う可能性のある対象者としては、セキュリティ管理者（ウイルス対策ソフトウェア、IPS、ファイアウォール、脆弱性評価、スキャン）、システム管理者（DNS、電子メール、Web サーバ）、ネットワーク管理者（パケットスニファ、ルータ）、デスクトップ管理者（Windows のレジストリまたはファイルのスキャン、ログオンスクリプトの変更）などが考えられる。識別に関与する可能性のあるすべての人員に対し、各自の役割と必要な作業の実施方法を確実に理解してもらうようにする。

4.4 根絶

根絶の主な目標は、感染しているシステムからマルウェアを駆除することであるが、根絶作業にはそれ以上の作業を伴うのが普通である。システムの脆弱性やそのほかのセキュリティ上の弱点（セキュリティ保護されていないファイル共有など）のために感染を許した場合、根絶作業には、他のマルウェアや元の脅威の派生版による再感染あるいは感染を防止するために、原因となった弱点を除去または軽減する作業が含まれる。4.3.6 項で述べたように、根絶作業は封じ込めの作業に統合される場合が多い。たとえば組織では、感染しているホストの識別に始まり、パッチの適用による脆弱性の解消、感染を駆除するウイルス対策ソフトウェアの実行までを行うユー ティリティを実行できる。封じ込めの作業によって根絶作業の選択肢が限定されることが多い。たとえば、感染しているシステムを主ネットワークから切り離すことによってインシデントを封じ込めた場合は、リモートから更新できるように独立の VLAN にシステムを接続するか、またはシステムへのパッチの適用とシステムの再構成を手動で行う。ホストを主ネットワークから切り離しているため、ユーザが各自のシステムをフルに使用できる状態を取り戻せるように、インシデント対応チームはホストに対して可能な限り速やかに根絶作業を実施する必要に迫られる。

状況に応じて、さまざまな組み合わせの根絶手法が必要になる。最も一般的な根絶ツールは、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、およびパッチ管理ソフトウェアである。自動の根絶手段（ウイルス対策スキャンをリモートで起動するなど）は、手動の根絶手段（感染しているシステムの設置場所を直接訪問して駆除ソフトウェアを CD から実行するなど）よりもずっと効率がよい。ただし、どのような状況でも自動の根絶手段が最適であるとは限らない。たとえば、感染しているホストが、ほかのシステムに重大な損害を与えようとしていたり、帯域幅を大幅に専有しようとしていたりした場合は、おそらくネットワークから隔離したままにしておき、手動の作業を通じて処理するべきである。また、4.3.1 項で説明したように、状況によってはユーザに対し、封じ込めと根絶の活動に参加してもらう必要が生じる。作業指示とソフトウェア更新をユーザに与えればよい場合もあるが、支援を必要とするユーザがいる場合もある。いつでも利用が可能な公式または非公式のヘルプデスク区域を主要な施設に設けるのも有効である。影響を受けているユーザを IT スタッフに一人ひとり見つけ出させて作業に割り込ませるよりも効率的で便利ある。重大なマルウェアインシデントの発生時には、追加 IT スタッフメンバをほかの職務から一時的に解放して、根絶作業の支援に当たらせることができる。IT スタッフがいない場所の場合、自分たちでシステムの面倒を見られるように、基本的な根絶作業を実施できるように数人を訓練しておくと有益である。組織では、必要な場合にいくつかの異なる種類の根絶作業を同時に実施できるようしておくべきである。

マルウェアインシデントによっては、根絶作業の一環として、感染したホストの再構築が必要になる場合がある。再構築には、OS やアプリケーションの再インストールとセキュリティ保護、および既知の正常なバックアップからのデータの復元が含まれる。通常、ホストの再構築にはほかの根絶作業よりも多大なリソースが必要となるため、それ以外の根絶措置またはそれらの組み合わせでは不十分な場合に限り、再構築を実施する。たとえば、スパイウェアの種類によってはホストからの駆除がきわめて困難なものがあり、たとえ駆除できたとしても、ホストを起動できない水準まで OS が損傷を受けている場合がある。また、感染したホストにおいて行われた活動が不明な場合にも、再構築が最善の選択肢となることが多い。ホストが複数のマルウェアに感染した場合、感染の期間が長期間にわたるか不明な場合、あるいは、バックドアやルートキットなど、損害を与えるほかの攻撃ツールがインストールされている場合には、マルウェアの感染以外に悪質な行為がホストに対してなされている可能性がある。そのような場合には、ホストを再構築することが、その完全性を取り戻すための最も信頼性の高い手段となる。組織では、マルウェアインシデントの発生時に必要に応じて速やかにホストを再構築できるようしておくべきである。

根絶作業は厄介な作業になるおそれがある。その理由は、作業の対象となるシステムの数が多数に及び、重大なインシデントの発生時にはさらなる感染および再感染が数日、数週間、あるいは数か月にわたって発生する傾向があるためである[41]。インシデント対応担当者は、感染が残っているホストを識別し、根絶の成功率を評価するために、識別活動を定期的に実施するべきである。感染したホストの数が減少すれば、インシデント対応チームの作業が前進していることを示すことになり、チームは残りのホストに対応するための最適な戦略を選択し、十分な時間とリソースを割り振る作業がしやすくなる。感染しているホストの数が当初の数から大幅に減少すると、インシデントの解決を宣言する誘惑にかられる可能性がある。しかし、組織では、感染や脆弱性が疑われるマシンの数を十分低いレベルにまで減らすよう努めるべきである。つまり、それらすべてのマシンを一度にネットワークに接続した際に脆弱なマシンがすべて感染したとしても、感染全体の影響が最小限にとどまるようにする。

組織全体の人員（特にユーザや管理職層）が、根絶作業に要する時間について現実的な予想を立てるようにあらかじめ準備しておかなかった場合、広範囲なマルウェア感染の根絶作業はさらに重圧が高くなるおそれがある。作業の対象となるシステムの数が非常に多く、システムはますます動的になっているため、多くの組織では根絶作業を感染しているシステムの大半で実施し終わるまでに、優に数日から 1 週間が経過する可能性がある。そして、事実上すべてのシステムからマルウェアの脅威を根絶するまでに数週間から数か月かかる可能性がある。根絶と復旧の作業（4.5 項を参照）に対する期待が妥当なものとなるように意識向上活動を実施すれば、重大なマルウェアインシデントによって生じる可能性のあるストレスを低減できる。

ルートキットの多くは、システムやシステムの最も重要なファイルに何百もの変更を加えるため、ルートキットをシステムから完全に根絶し、根絶したことを検証するには、かなりの時間とリソースが必要となる場合が多い。通常、ルートキットがインストールされたシステムやその疑いが強いシステムは、すべて再構築するべきである。このようなシステムは、オペレーティングシステムやアプリケーションを再インストールして再構成するか、または既知の正常なバックアップからシステムを復元することによって、再構築する。一般に、次のインシデントの特徴を 1 つでも示したシステムはすべて、通常の根絶作業を実施するのではなく再構築を積極的に検討すべきである。

---

[41] 根絶作業にもかかわらず、特定の種類のマルウェアがいつまでも組織の内部に存続することがある。たとえば、マルウェアがシステムのバックアップに格納され、バックアップの復元によってマルウェアも復元されることがある。また、マルウェアがリムーバブルメディアに感染し、その後その媒体が長期間使用されないこともある。最初の感染から何年も経ったあとに、リムーバブルメディアにアクセスしたことが原因で、マルウェアがホストへの感染を試みる可能性がある。このような脅威は内部のネットワーク上に存在するため、通常はネットワーク周辺部の防御（ファイアウォールなど）は効果がない。

- 1 人以上の攻撃者が、システム管理者レベルのアクセス権を獲得した。
- バックドア、またはワームにより作成された保護されていない共有、あるいはそのほかの手段を通じて、システム管理者レベルの不正なアクセスがだれにでも可能であった。
- システムファイルが、トロイの木馬、バックドア、ルートキット、攻撃ツール、またはそのほかの手段によって置き換えられた。
- 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、またはそのほかのプログラムや手法によってマルウェアを根絶したあとも、システムが不安定であったり正常に機能しなかったりする。これは、マルウェアがまだ完全には根絶されていないか、あるいは、システムやアプリケーションにとって重要なファイルまたは設定が損傷を受けたことを示す。

マルウェアインシデントが上記のいずれの特徴も示さなければ、通常は、システムを再構築せずに、システムからマルウェアを根絶すれば十分である。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。

4.5 復旧

マルウェアインシデントからの復旧には、感染したシステムの機能やデータの回復と、一時的な封じ込め措置の解除という 2 つの側面がある。システムの損傷が限定的なマルウェアインシデント（たとえば、少数のデータファイルが改ざんされただけで、ウイルス対策ソフトウェアで完全に駆除された感染など）ではほとんどの場合、システムを復旧するための追加的な作業は必要ない。4.4 項で説明したように、それよりもはるかに損傷が大きく、無数のシステムファイルやデータファイルを破壊したり、ハードディスクドライブを完全に消去したりするようなマルウェアインシデント（トロイの木馬、ルートキット、バックドアなど）の場合には、まずシステムを再構築するか、既知の正常なバックアップからシステムを復元したあと、マルウェアの脅威に対する脆弱性をなくすようにシステムのセキュリティを確保するのが最善な場合が多い。組織では、新種のマルウェアの脅威によって組織の大部分のワークステーションのハードディスクドライブが完全に消去される事態など、起こり得る最悪のシナリオを慎重に検討し、そのような場合にシステムを復旧する方法を決めておくべきである。復旧方法を決める際には、だれが復旧作業を実施するのかを明らかにし、必要となる作業時間や暦上の経過時間を見積もって、復旧作業の優先順位をどのように決定するのかを決める。

サービス（電子メールなど）や接続（インターネットアクセス、在宅勤務者用の VPN など）の中断などの一時的な封じ込め措置をいつ解除すべきかは、重大なマルウェアインシデントの発生時においては、判断が難しい場合が多い。たとえば、マルウェアの感染拡大を阻止するために電子メールサービスを停止し、そのあいだ、脆弱なシステムにパッチを適用し、感染したシステムでマルウェアの封じ込め、根絶、復旧の各措置を個別に実施することを考える。脆弱なシステムをすべて探し出してパッチを適用し、感染したすべてのシステムで駆除を行うには、数日から数週間かかることがある。しかし、そのような長い期間、電子メールを中断し続けることはできない。電子メールサービスが回復すると、ほぼ確実に、ある時点で、感染したシステムから再びマルウェアの拡散が始まる。しかし、ほとんどすべてのシステムでパッチの適用および駆除作業が完了していれば、マルウェアによる新たな感染の影響は最小限に抑えられるはずである。インシデント対応チームでは、パッチが適用されていないシステムや感染したシステムの推定数が十分に少なくなり、以降のインシデントによる影響がほとんどないと判断されるまで、封じ込め措置を維持するよう努めるべきである。また、インシデント対応担当者は、インシデントの封じ込めを十分に維持しつつ、組織の通常の機能への影響が少なく済むような、代替の封じ込め措置も検討するべきである。ただし、サービスの回復に伴うリスクについてはインシデント対応チームが評価すべきであっても、最終的には管理職層が、インシデント対応チームの勧告や、封じ込め措置を維持することによる事業への影響に対する認識に基づいて、必要な措置を決定する責任を負うべきである。

4.6 反省会

重大なマルウェアインシデントが発生すると、対応を担当する主たる担当者は、数日から数週間にわたって集中して作業に当たるのが普通である。主要な対応作業が終局に近づくにつれて、主たる担当者は通常、肉体的にも精神的にも疲労が蓄積しており、インシデント対応の期間中に中断されていたほかの作業の実施も遅れている。その結果、重大なマルウェアインシデントへの対応に関する反省会が、大幅に遅れたり、完全に省略されたりすることがある。しかし、重大なマルウェアインシデントへの対応はきわめて負担の大きい作業になる可能性があるため、重大なマルウェアインシデントに対してしっかりとした反省会を組織で実施することが特に重要である。対応担当者やそのほかの主たる担当者に対して、ほかの作業分を取り返すための若干の日数を与えることは妥当であるが、インシデントの体験がまだ全員の中にはっきりと残っているうちに、レビュー会議やそのほかの取組みを迅速に行うべきである。マルウェアインシデントにおける反省会のプロセスは、ほかの種類のインシデントの場合とまったく変わらない。マルウェアインシデントに関する反省会活動の成果として、次のような例が考えられる。

+ **セキュリティポリシーの変更。** 同様のインシデントを防止するために、セキュリティポリシーを変更することが考えられる。たとえば、*.scr* という拡張子で終わる電子メール添付ファイルが使用されていたために広範囲にわたる感染が発生した場合は、*.scr* ファイルを電子メールで送受信することを禁止するようポリシーを変更することが望ましいと考えられる。
+ **意識向上プログラムの変更。** 感染の数を減らしたり、ユーザによるインシデント報告や自分のシステムのインシデントに対応する作業支援の活動を改善したりするために、ユーザのセキュリティ意識向上トレーニングを変更することが考えられる。
+ **ソフトウェアの再構成。** セキュリティポリシーの変更に対応するために、あるいは、既存のポリシーを順守するために、OS やアプリケーションの設定に変更を加える必要が考えられる。
+ **マルウェア検出ソフトウェアの導入。** ウイルス対策ソフトウェアやそのほかのマルウェア検出ツールによる保護がなされていなかった伝送メカニズムを通じてシステムが感染した場合は、インシデントの経験を通じて、追加のソフトウェアの購入と導入が十分に正当化されることが考えられる。
+ **マルウェア検出ソフトウェアの再構成。** 次のようなさまざまな方法で検出ソフトウェアを再構成する必要が考えられる。
  - ソフトウェアとシグネチャの更新頻度を増やす。
  - 検出の精度を改善する（フォールスポジティブを減らす、フォールスネガティブを減らすなど）。
  - 監視の範囲を広げる（監視する感染メカニズムを増やす、監視するファイルまたはファイルシステムを増やすなど）。
  - マルウェアの検出に対応して自動的に実行される措置を変更する。
  - シグネチャ更新の配布効率を改善する。

4.7 まとめ

組織は、マルウェアインシデントに対処するための堅牢なインシデント対処プロセス能力を持つべきである。NIST SP 800-61 で定義されているように、インシデント対応プロセスには「準備」、「検知と分析」、「封じ込め/根絶/復旧」、「インシデント発生後の活動」の、4 つの主要なフェーズがある。

以下は、マルウェアインシデントへの対応における主な推奨事項を、インシデント対応のフェーズ順にまとめたものである。

+ **準備。**マルウェアインシデントへの効果的な対応に必要な能力を確保するための準備をしておくべきである。以下の措置を推奨する。
  - マルウェア専用のインシデント対応ポリシーと手続きを策定して備える。これらのポリシーや手続きでは、マルウェアインシデント対応に関与する可能性のあるすべての個人とチームの役割と責任を定める。
  - マルウェアに関するトレーニングや訓練を定期的に実施する 。
  - マルウェアインシデント対応担当者のためのマルウェア関連技能を開発し維持する。たとえば、マルウェア感染の手口やマルウェア検出ツールについて理解してもらう。
  - 連絡と調整を円滑化するために、マルウェアインシデントに対する組織としての対応を調整する役目を担う、数人の個人または少人数のチームを事前に編成しておく。
  - 有害事象発生時に、インシデント対処担当者、技術スタッフ、管理職層、およびユーザの間で調整作業を維持できるように、いくつかの意思伝達メカニズムを設ける。
  - マルウェア警告の真偽に関する質問への回答を行う連絡拠点を確立しておく。
  - マルウェアインシデント対応を支援するために必要なハードウェアおよびソフトウェアツールを入手する。
+ **検知と分析。**マルウェアはものの数分のうちに感染が組織全体に拡大するおそれがあるので、マルウェアインシデントの検知と確認を迅速に行えるように努めるべきである。 早期の検知は、感染するシステムの数を最小限に食い止めるのに役立つ。その結果、復旧作業が少なく済み、組織が被る損害の量も減る。 検知と分析については以下の措置を推奨する。
  - マルウェアに関するアドバイザリやセキュリティツール (ウイルス対策ソフトウェアや IPS など) の警告を監視し、マルウェアインシデントの前兆を検出する。それによって、組織はセキュリティ体制を変更してマルウェアインシデントを防止する機会を得る。
  - ユーザの報告、IT スタッフの報告、セキュリティツール (ウイルス対策ソフトウェアや IDS など) といった、マルウェアインシデントの兆候を示す主要な情報源から得られるデータを検討し、それらの情報源のデータを照合して、マルウェア関連の活動を識別する。完全に信頼のおける兆候は存在しないため、マルウェアインシデントと疑わしき兆候をすべて分析し、マルウェアが個々のインシデントの原因であることを確認する。必要に応じて二次的なデータ源を利用して、活動を照合したり、より詳細な情報を収集したりする。
  - マルウェアの識別や現在実行中のプロセスの列挙およびそのほかの分析処理を実行する、最新のツール類を収めた信頼のおけるツールキットを、リムーバブルメディア上に構築する。
  - マルウェアに関連する各種のインシデントに対して適切な対応レベルを明確にする、一連の優先順位の条件を設ける。
+ **封じ込め。**封じ込めには、マルウェアの拡散の阻止と、システムのさらなる被害の防止という、2 つの主要な要素がある。封じ込めの措置は、ほとんどすべてのマルウェアインシデントに対して必要である。インシデントに対応する際には、早期の段階でどのような封じ込め

手段を最初に利用すべきかを組織で決めることが重要になる。封じ込めに関する決定は、組織が受容し得るリスクの程度を反映したものになるが、組織はそうした決定を下す際の方針や手続きを設けておくべきである。この封じ込めの方針は、インシデント対応担当者が具体的な状況の特徴に応じて適切な組み合わせの封じ込め手段を選択できるようにするものとする。封じ込めの際に適切な決定が下されるように、封じ込めに関してだれが重要な決定を下す権限を持つのか、および、各種の措置がどのような状況のもとで適切なのかを、ポリシーの中で明確にするべきである。封じ込め手段は以下の 4 つの基本分類に分けることができる。

- **ユーザの関与。**感染を識別する方法と、システムが感染した場合の措置を示した手順を、ユーザに提供しておくと役立つ可能性がある。ただし、マルウェアインシデントの封じ込めを主にユーザに頼ることは避ける。
- **検知の自動化。**ウイルス対策ソフトウェア、電子メールフィルタ処理、侵入防止ソフトウェアなどの自動化技術は、マルウェアインシデントを封じ込めることができる場合が多い。広範囲にわたるインシデントにおいて、最新のウイルス対策ソフトウェアでマルウェアを識別できない場合に備え、ほかのセキュリティツールを使用して封じ込めることができるよう準備しておく。
- **サービスの無効化。**インシデントを封じ込めるため、マルウェアが使用しているサービスを停止または遮断できるよう準備しておき、そうした措置によって生じる結果を理解しておく。また、別の組織がマルウェアインシデントに対応するためにその組織のサービスを無効にすることがあるが、それによって生じる問題についても対応できるよう準備しておくべきである。
- **接続の無効化。**マルウェアインシデントを封じ込めるため、ネットワーク接続に追加の制限をかけられるようにしておく。こうした制限によって組織の機能が受ける可能性のある影響について認識しておく。

インシデント対応担当者は、未知のマルウェアのコピーをウイルス対策ベンダやそのほかのセキュリティソフトウェアベンダに送付して分析してもらうための手続きに精通している必要がある。また、必要に応じ、インシデント対応組織やウイルス対策ベンダなどの信頼のおける第三者と連絡を取り、新たな脅威への対応におけるガイダンスを受けるようにする。

多数のマルウェアインシデント、特に拡散するタイプのマルウェアインシデントを封じ込めるうえで、もう 1 つ重要な作業として、マルウェアに感染したホストの識別がある。このプロセスはコンピューティングの動的な性質のために複雑になる場合が多い。規模の大きなマルウェアインシデントが発生する前に、ホストの識別に関する問題について慎重に検討しておく。そうすることによって、感染したホストを識別するための複数の方策を効果的な封じ込め作業の一部として利用できるようになる。そして、識別に関して十分広範囲なアプローチを選択し、選択したそれぞれのアプローチを大規模なマルウェア問題の発生時に効果的に実施するための手続きと技術的な能力を整備しておく。

+ **根絶。**根絶の主な目標は、マルウェアに感染したシステムからマルウェアを駆除することである。作業の対象となるシステムの数が非常に多く、システムはますます動的になっているため、多くの組織では根絶作業を感染しているシステムの大半で実施し終わるまでに、優に数日から 1 週間が経過する可能性がある。そして、事実上すべてのシステムからマルウェアの脅威を根絶するまでに数週間から数か月かかる可能性がある。組織では、さまざまな状況に応じて各種の根絶手法を組み合わせて同時に使用できるようにしておくべきである。また、根絶と復旧の作業で予想し得る事態を想定した意識向上活動を検討する。こうした活動は、重大なマルウェアインシデントによって生じる可能性のあるストレスを低減するのに役立つ。マルウェアインシデントが原因で管理者レベルの不正なアクセスやシステムフ

ァイルの変更が発生した場合に備えて、影響を受けた個々のシステムのオペレーティングシステムやアプリケーションを再インストールして再構成するか、または既知の正常なバックアップからシステムを復元することによって、再構築できるようにしておくべきである。

+ **復旧。**マルウェアインシデントからの復旧には、感染したシステムの機能やデータの回復と、一時的な封じ込め措置の解除という 2 つの側面がある。起こりうる最悪のシナリオを慎重に検討し、復旧の実施方法を決定するべきである。封じ込めのための一時的対策（サービスや接続の中断など）を解除すべきタイミングは、発生したマルウェアインシデントが大規模な場合には、判断が難しいことが多い。インシデント対応チームでは、感染したシステムや感染する脆弱性を持つシステムの推定数が十分少なくなり、以降のインシデントによる影響がほとんどないと判断されるまで、封じ込めのための対策を維持するよう努めるべきである。ただし、サービスまたは接続の回復に伴うリスクについてはインシデント対応チームが評価すべきであっても、最終的には管理職層が、インシデント対応チームの勧告や、封じ込め措置を維持することによる事業への影響に対する認識に基づいて、必要な措置を決定する責任を負うべきである。

+ **インシデント発生後の活動。**マルウェアインシデントへの対応はきわめて負担の大きい作業になる可能性があるため、重大なマルウェアインシデントに対してしっかりとした反省会活動を組織で実施することが特に重要である。マルウェアインシデントへの対応から得られた教訓を把握することは、組織のインシデント対応能力とマルウェアに対する防御力を向上させるのに役立つ。たとえば、セキュリティポリシー、ソフトウェアの設定、マルウェア検出／防止ソフトウェアの導入に対して、必要となる変更を明らかにできるようになる。

（本ページは意図的に白紙のままとする）

5. マルウェアの今後

組織でマルウェアの防止とマルウェアインシデント対応能力の計画を立てる際には、マルウェアの今後について考慮するべきである。新しいマルウェアの脅威は絶え間なく発生するため、短期的な未来の脅威に対応し、長期的な脅威にも対応するように変更や構築を行うことのできる、十分な堅牢性と柔軟性を備えた、マルウェアの防止および対応の能力を確立すべきである。マルウェアも、マルウェアに対抗する防御策も、一方が他方に応じて改められるかたちで進化を続けている。現時点では、ほとんどの組織において、マルウェアを作る側もマルウェアを阻止する側も明らかに優勢であるとはいえない。

マルウェアの脅威の今後については不明だが、マルウェアの歴史に基づいていくつかの合理的な予想を立てることは可能である（マルウェアの歴史については2.9項を参照のこと）。ウイルス対策ベンダのマルウェアデータベースには、毎週数十の新種の脅威が登録されているが、このことは新たな脅威の発生頻度が増え続けていることを示している。その原因としては、まず既存の脅威の派生版を容易に作成できることがある。たとえば、広範囲に広まった新種のワームは、数十の派生版が数日のうちに登場することが多い。また、最近では脅威が悪意のモバイルコードに移っていることも、新たな脅威の頻度が増えている理由である。悪意のモバイルコードは一部の古い形態のマルウェア（ウイルスなど）と比べて作成や変更が比較的容易である。攻撃者が特別な技能を身に付けなくても既存のマルウェアを新たな派生版に作り変えることができる限り、新たな脅威の頻度は増え続けると予想される。

予想される別の動向として、ごく短時間のうちに重大な損害を引き起こす脅威の数が増えることが考えられる。2004 年に登場したネットワークサービスワームの Witty は、ハードディスクドライブ上のデータを破壊するように設計されていた。Cooperative Association for Internet Data Analysis（CAIDA）の分析によれば、このワームはインターネット上で広がり始めた時点から 1 時間足らずで、攻撃可能な標的のほとんどに感染することに成功した[42]。Witty ワームにはもう 1 つ特筆すべき面がある。それは、このワームが登場したのが、悪用された脆弱性の公表から 1 日後であったことである。このため、マルウェアが登場する前にシステムへのパッチの適用やそのほかの軽減活動を組織で実施する時間はほとんどなかった。攻撃者はしばしば、標的となる脆弱性が公表される前であっても脆弱性を悪用するマルウェアを登場させることがある。そのような脅威のことを*ゼロデイ攻撃*と呼ぶ。Witty ワーム並みのスピードと破壊力を持ち、広く実装されているアプリケーションや OS を標的としたゼロデイ攻撃は、数分のうちに無数のシステムに深刻な損害を与える可能性がある。そのようなワームが登場することは確実にあり得ることである。組織ではこのことを考慮し、組織の運営に及ぼす可能性のある影響と最善の対応方法を検討すべきである。また、既知および未知の両方の脅威を検知して阻止することのできるセキュリティ管理策の組み合わせを導入することを検討するべきである。一般に、悪質または危険な振る舞いを単に検出するのでなく、阻止するのに有効なセキュリティ管理策に、特に重点を置くようにするべきである。

もう 1 つ、マルウェアの重要な動向として、マルウェアやそのほかの悪意のあるコンテンツを利用して詐欺を働く事例が増えていることがあげられる。これらの事例は、スパイウェアやフィッシング攻撃など、プライバシを侵害する手口を利用し、ユーザをだまして個人情報を開示させることに成功しており、なりすまし犯罪や金融詐欺の事件の増加を招いている。現時点では、これらの脅威を阻止するための技術的なセキュリティ管理策はまだ十分に確立されてはいないが、保護機能の向上の

[42] この分析については、「The Spread of the Witty Worm」（http://www.caida.org/analysis/security/witty/）を参照。CAIDA では Slammer ワームについても分析を公開している（「The Spread of the Sapphire/Slammer Worm」、http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html）。この分析によれば、Slammer ワームは脆弱性を持っていた標的ホストのほとんどに 10 分以内に感染していた最近の調査では、Witty や Slammer に類似のワームは、数分ではなく数秒のうちに広範囲に拡散できることが指摘されている。詳細については、「The Top Speed of Flash Worms」（http://www.caida.org/outreach/papers/2004/topspeedworms/topspeed-worm04.pdf）を参照。

要望が高まるにつれて、現在よりもずっと堅牢なスパイウェア検出／駆除ユーティリティが開発され、同様の機能がウイルス対策ソフトウェアにも追加されるものと考えられる。導入される技術的な管理策の質が向上し、ユーザが攻撃者の手口について理解を深めるにつれて、攻撃者は、より工夫を凝らした革新的な手段を利用して自動検出を避け、ユーザの信頼を悪用することになるだろう。

攻撃者はまた、PDA や携帯電話など、従来とは異なるプラットフォームを攻撃するあるいは、PDA や携帯電話などをマルウェアの運搬手段として利用するウイルスやワームを作り始めている。ワイヤレスコンピューティングを駆使したモバイル技術の利用が増え続けるにつれて、それらの技術を利用したマルウェアインシデントの発生頻度と深刻度が高まる可能性が非常に大きい。これは、最新の脅威の種類と、それぞれの脅威の種類から保護するために利用できるセキュリティ管理策に関する情報を組織が常に把握している必要があることを強調するものである。新しい分類の脅威がますます深刻になるにつれて、組織は、それらの脅威を軽減するために適切なセキュリティ管理策を計画して実施すべきである。

付録A—封じ込め技術の概要

本文書では、マルウェアインシデントの封じ込めに役立つ各種の技術について説明している。これらの技術のほとんどはインシデントの防止、検知、および根絶に役立つが、この項では主に封じ込めについて説明する。その理由は、封じ込めがマルウェアインシデントへの対応において最も複雑なフェーズだからである。また、一般に、マルウェアインシデントへの対応において、封じ込めのフェーズに関連する技術はほかのどのフェーズの技術よりも多い。この付録では、それぞれの技術を利用してマルウェアインシデントを封じ込める方法の概要を説明する。そして、具体的な状況に応じて最も適した技術を識別するためのツールを紹介する。これらは効果的な封じ込め方策を策定する際の土台となる。

マルウェアインシデントへの対応の方策を策定するにあたっては、マルウェアインシデントの封じ込めに使用できる可能性のあるすべての技術を検討するべきである。表 A-1 では、特によく利用されている技術の一覧を示し、マルウェアおよび攻撃ツールの主要な各分類に対するそれぞれの技術の有効性について全般的なガイダンスを提供する。この表では便宜上、環境を 2 つに分類（管理された環境と管理されていない環境）し、脅威を 2 つに分類（単純な脅威と複雑な脅威）している。これらの分類の意味を次に示す。

+ **管理された環境。** 管理された環境では、1 つ以上の中心的なグループが、組織全域の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およびアプリケーションの設定に対して、大幅な管理権限を持っている。このため、システムの初期導入時や、以降のサポートおよび保守の際に、より優れたセキュリティ管理策を実装することが可能であり、一貫したセキュリティ体制を組織全体にわたって維持できる。この項のガイダンスでは、管理された環境においては、ほとんどのシステムがマルウェアの防止と対応のために推奨されている措置を実施しているものと仮定している。たとえば、すべてのホストにウイルス対策ソフトウェアをインストールして最新の状態に保つ、ファイアウォールでデフォルトで拒否のポリシーを使用する、オペレーティングシステムとアプリケーションにパッチを適用するなどの措置を実施しているものと仮定している。

+ **管理されていない環境。** 管理されていない環境では、システム所有者やユーザが各自のシステムの管理を大幅に任されており、通常は管理者権限を持っている。これらのシステムは当初、組織の標準構成を使用している可能性もあるが、所有者やユーザが構成を変更した可能性があり、結果としてセキュリティが低下しているおそれがある。この項のガイダンスでは、管理されていない環境において、マルウェアの防止と対応のために推奨されている措置を実施しているシステムは一部であり、ほとんどのシステムでは措置の一部を実施しているものと仮定している。

+ **単純な脅威。** 単純な脅威とは、識別できる特徴が少ないマルウェアの脅威のことである。たとえば、1 つの固定の件名と、3 つのうちいずれかの添付ファイル名を使用する大量メールワームは、単純な脅威とみなされる。また、固定のポート番号を 1 つ使用し、1 つの特定の IP アドレスとのみ通信するバックドアも、単純な脅威と考えられる。

+ **複雑な脅威。** 単純な脅威とは異なり、複雑な脅威では、識別できる数百あるいは数千の特徴のいずれかが使用される。複雑な脅威の中には特徴を無作為に生成するものさえある。一例として、任意の 50 個の件名と任意の 50 個のファイル名のいずれかを使用し、無作為な送信者アドレス、電子メール本文、および添付ファイルサイズを使用する、大量メールワームがある。別の例では、大規模なリスト内の任意の IP アドレスから

ペイロードをダウンロードする悪意のモバイルコードがある。利用される大規模なリストは悪意のモバイルコードの事例ごとに異なる。複雑な脅威は単純な脅威よりも封じ込めが難しい場合が多い。

表 A-1 に示す標準のガイダンスは、管理された環境における単純な脅威への対応を対象とする。

表 A-1. 防止および封じ込め技術の典型的な有効性

技術	単純な脅威、管理された環境	管理されていない環境との主な違い	複雑な脅威の場合との主な違い
セキュリティツール			
ネットワークベースのウイルス対策ソフトウェア	• 監視されているネットワークポイント（インターネットファイアウォールなど）の通過を試みるすべての種類の既知のマルウェアの阻止にたいへん有効である。一部の未知のマルウェアの阻止にも有効である。	• なし。	• なし。
ホストベースのウイルス対策ソフトウェア	• ホスト（ワークステーション、サーバなど）への感染を試みる既知のマルウェアの阻止にたいへん有効である。一部の未知のマルウェアの阻止にも有効である。	• ホストによっては、旧式のソフトウェアを使用しているものや誤ったソフトウェアの設定を行っているもの、ソフトウェアが無効になっているものやソフトウェアがインストールされていないものもあるため、有効性が低い。	• なし。
スパイウェア検出／駆除ユーティリティの警告（通常はホストベース）	• ホスト（ワークステーション、サーバなど）への感染を試みる既知のスパイウェアの阻止にたいへん有効である。一部の未知のスパイウェアの阻止にも有効である。	• ホストによっては、旧式のソフトウェアを使用しているものや誤ったソフトウェアの設定を行っているもの、ソフトウェアが無効になっているものやソフトウェアがインストールされていないものもあるため、有効性が低い。	• なし。
ネットワークベースの侵入防止システム	• 監視されているネットワークポイント（インターネットファイアウォールなど）の通過を試みる主要な既知のワームの阻止に有効である。場合によっては、未知のワームの阻止にも有効である。 • バックドア使用の識別と阻止に多少有効である。	• なし。	• 検出精度が低いため、一般に有効性は低い。 • 脅威の特徴が無作為の場合は、一般に有効性はまったくない。

技術	単純な脅威、管理された環境	管理されていない環境との主な違い	複雑な脅威の場合との主な違い
ホストベースの侵入防止システム	• ホスト（ワークステーション、サーバなど）への感染を試みる既知および未知のマルウェアの阻止に多少有効である。 • 重要なシステムファイルの改ざんを試みるマルウェアの識別に有効である。	• ホストによっては、旧式のソフトウェアを使用しているものや誤ったソフトウェアの設定を行っているもの、ソフトウェアが無効になっているものやソフトウェアがインストールされていないものもあるため、有効性が低い。さらに、ソフトウェアが適切にチューニングされている可能性が低く、そのために検出精度が低下する。	• 検出精度が低いため、一般に有効性は低い。
ネットワークベースのスパムフィルタ処理	• 組織の電子メールサービスを利用する既知の電子メールベースのマルウェアの阻止にたいへん有効である。一部の未知のマルウェアの阻止にも有効である。	• なし。	• 検出精度が低いため、一般に有効性は低い。 • 脅威の特徴が無作為の場合は、一般に有効性はまったくない。
ホストベースのスパムフィルタ処理	• 組織の電子メールサービスを利用する既知の電子メールベースのマルウェアの阻止にたいへん有効である。一部の未知のマルウェアの阻止にも有効である。	• ホストによっては、旧式のソフトウェアを使用しているものや誤ったソフトウェアの設定を行っているもの、ソフトウェアが無効になっているものやソフトウェアがインストールされていないものもあるため、有効性が低い。	• 検出精度が低いため、一般に有効性は低い。 • 脅威の特徴が無作為の場合は、一般に有効性はまったくない。
ネットワークベースの Web コンテンツフィルタ処理	• 既知の Web ベースのマルウェアの阻止に有効である。	• なし。	• 検出精度が低いため、一般に有効性は低い。
ホストベースの Web コンテンツフィルタ処理	• 既知の Web ベースのマルウェアの阻止に有効である。	• ホストによっては、旧式のソフトウェアを使用しているものや誤ったソフトウェアの設定を行っているもの、ソフトウェアが無効になっているものやソフトウェアがインストールされていないものもあるため、有効性が低い。	• 検出精度が低いため、一般に有効性は低い。
ネットワーク構成の変更			
ネットワークベースのファイアウォール	• ファイアウォールのポリシーによって許可されていないネットワークサービスを利用するインターネットベースのワームが、ネットワークに進入したりネットワークから進出したりするのを防ぐのにたいへん有効である。 • 外部のサービス（インスタントメッセージなど）やホスト（Web サイトなど）へのアクセスを遮断し、マルウェアの感染メカニズムとして利用されるのを防ぐ	• なし。	• 多数の IP アドレスへのアクセス、または多数の IP アドレスからのアクセスの遮断を試みる場合には、有効性が低いことがある。

技術	単純な脅威、管理された環境	管理されていない環境との主な違い	複雑な脅威の場合との主な違い
	のに有効である。 • 不正なホスト（大量メールワームに感染したワークステーションなど）により生成される電子メールが組織のネットワークから送出されるのを防ぐのに有効である。 • マルウェア（バックドア、悪意のモバイルコード、キーストロークロガー、悪意のブラウザプラグインなど）による、攻撃用 IP アドレスへのアクセス、または攻撃用 IP アドレスからのアクセスを遮断するのに有効である。		
ホストベースのファイアウォール[43]	• ネットワークサービスワームがホスト（ワークステーション、サーバなど）に感染するのを防ぐのにたいへん有効である。 • 感染したホスト（バックドア、キーストロークロガー、Web ブラウザ活動、電子メールジェネレータなど）により生成される発信活動がホストから送出されるのを防ぐのに有効である。	• ホストによっては、旧式のソフトウェアを使用しているものや誤ったソフトウェアの設定を行っているもの、ソフトウェアが無効になっているものやソフトウェアがインストールされていないものもあるため、有効性が低い。	• なし。
インターネット境界ルータ	• 周辺部のセキュリティポリシーによって許可されていないネットワークサービスを使用するインターネットベースのワームが、組織のネットワークに進入するのを防ぐのにたいへん有効である。 • マルウェア（バックドア、悪意のモバイルコード、キーストロークロガー、悪意のブラウザプラグインなど）による、攻撃用 IP アドレスへのアクセス、または攻撃用 IP アドレスからのアクセスを遮断するのに有効である。	• なし。	• 多数の IP アドレスへのアクセス、または多数の IP アドレスからのアクセスの遮断を試みる場合には、有効性が低いことがある。

[43] この項目はホストベースのファイアウォール製品のファイアウォール機能だけを対象としており、製品が持っている可能性のあるそのほかの機能（ウイルス対策ソフトウェア、ホストベースの侵入防止、スパムフィルタ処理、Web コンテンツフィルタ処理など）は対象としていない。

技術	単純な脅威、管理された環境	管理されていない環境との主な違い	複雑な脅威の場合との主な違い
内部ルータ	• ファイアウォールのポリシーによって許可されていないネットワークサービスを利用するワームが、組織のネットワークおよびサブネットに進入したり、そこから進出したりするのを防ぐのにたいへん有効である。 • マルウェア（バックドア、悪意のモバイルコード、キーストロークロガー、悪意のブラウザプラグインなど）による、攻撃用 IP アドレスへのアクセス、または攻撃用 IP アドレスからのアクセスを遮断するのに有効である。 • 感染したホスト上の電子メールジェネレータから生成される送信電子メール活動を遮断するのにいくらか有効である。	• なし。	• 多数の IP アドレスへのアクセス、または多数の IP アドレスからのアクセスの遮断を試みる場合には、有効性が低いことがある。
ホスト構成の変更			
ホストの強化（パッチ適用を含む）	• 脆弱性やセキュリティ保護されていない設定を悪用するマルウェアの感染拡大を阻止するのに有効である。	• パッチの適用や強化が迅速にまたは適切に実施されないホストが多いため、有効性が低い。	• なし。
電子メールサーバの設定（電子メール添付ファイルのブロックなど）	• 組織の電子メールサービスを利用する電子メールベースのマルウェアの阻止にたいへん有効である。	• なし。	• 検出精度が低いため、一般に有効性は低い。 • 脅威の特徴が無作為の場合は、一般に有効性はまったくない。
組織のサーバ上で運用されているほかのサービスの設定	• ネットワークサービスワームの阻止に、いくらか有効であるか、たいへん有効である。	• なし。	• 検出精度が低いため、一般に有効性は低い。 • 脅威の特徴が無作為の場合は、一般に有効性はまったくない。
アプリケーションクライアントの設定（電子メールクライアントや Web ブラウザでのモバイルコードの実行制限、ワードプロセッサでのマクロの使用制限など）	• 一部の特定のマルウェアの阻止に有効である。	• ユーザが設定を行うための操作を実行する必要があるため（手動による設定の変更、配布されたツールやスクリプトの実行など）、有効性は限られる。	• なし。

表 A-2 および表 A-3 は表 A-1 の情報をまとめたもので、管理された環境における単純な脅威の場合 (表 A-2) と複雑な脅威の場合 (表 A-3) の各技術の有効性を示している。これらの表では、それぞれの技術が各種のマルウェアや攻撃ツールに対して通常どの程度有効であるのかについて、別々に格付けしている。格付けは、高 (脅威の分類に対する有効性が高い) 、中 (中程度の有効性がある) 、低 (有効性が低い) としている。通常、中または低の有効性の格付けは、対象の技術が特定の事例に対しては有効であるものの、それ以外の事例に対してはほとんどまたはまったく有効でないことを意味している。空欄は、対象の技術が通常は対象の脅威に適用されないことを示している。表 A-4 および表 A-5 は、管理されていない環境における単純な脅威の場合 (表 A-4) と複雑な脅威の場合 (表 A-5) の各技術の有効性を評価したものである。

表 A-2. 管理された環境における単純な脅威に対する典型的な有効性

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア[44]	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
セキュリティツール											
ネットワークベースのウイルス対策ソフトウェア	高	高	高	高	高	高	高	高	高	高	高
ホストベースのウイルス対策ソフトウェア	高	高	高	高	高	高	高	高	高	高	高
スパイウェア検出／駆除ユーティリティ					高	高				高	
ネットワークベースの侵入防止システム			中	中			低				
ホストベースの侵入防止システム			低		中	低	低	低	中	低	低
ネットワークベースのスパムフィルタ処理				高	低	中					高
ホストベースのスパムフィルタ処理				高	低	中					高
ネットワークベースの Web コンテンツフィルタ処理					低	中				中	
ホストベースの Web コンテンツフィルタ処理					低	中				中	
ネットワーク構成の変更											
ネットワークベースのファイアウォール			高	中		中	中	中		中	中

[44] この分類にはボットとリモート管理ツールが含まれる。

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア[44]	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
ホストベースのファイアウォール			高			中	中	中		中	中
インターネット境界ルータ			高			中	中	中		中	
内部ルータ			高			中	中	中		中	低
ホスト構成の変更											
ホストの強化（パッチ適用を含む）	低	低	中	中	中	中					
電子メールサーバの設定（電子メール添付ファイルのブロックなど）	低	低		高	中	中					高
組織のサーバ上で運用されているほかのサービスの設定			低～高								
アプリケーションクライアントの設定（電子メールクライアントや Web ブラウザでのモバイルコードの実行制限、ワードプロセッサでのマクロの使用制限など）		中	中			中				中	

表 A-3. 管理された環境における複雑な脅威に対する典型的な有効性

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
セキュリティツール											
ネットワークベースのウイルス対策ソフトウェア	高	高	高	高	高	高	高	高	高	高	高
ホストベースのウイルス対策ソフトウェア	高	高	高	高	高	高	高	高	高	高	高
スパイウェア検出／駆除ユーティリティ					高	高				高	
ネットワークベースの侵入防止システム			低	低			低				
ホストベースの侵入防止システム			低		低	低	低	低	低	低	低
ネットワークベースのスパムフィルタ処理				低～中	低	低					低～中
ホストベースのスパムフィルタ処理				低～中	低	低					低～中
ネットワークベースの Web コンテンツフィルタ処理					低	低				低	
ホストベースの Web コンテンツフィルタ処理					低	低				低	
ネットワーク構成の変更											
ネットワークベースのファイアウォール			高	中		中	低～中	低～中		低～中	低～中
ホストベースのファイアウォール			高			中	中	中		中	中
インターネット境界ルータ			高			中	低～中	低～中		低～中	
内部ルータ			高			中	低～中	低～中		低～中	低
ホスト構成の変更											

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
ホストの強化（パッチ適用を含む）	低	低	中	中	中	中					
電子メールサーバの設定（電子メール添付ファイルのブロックなど）	低	低		低～中	低	低					低～中
組織のサーバ上で運用されているほかのサービスの設定			低～中								
アプリケーションクライアントの設定（電子メールクライアントや Web ブラウザでのモバイルコードの実行制限、ワードプロセッサでのマクロの使用制限など）		中	中			中				中	

表 A-4. 管理されていない環境における単純な脅威に対する典型的な有効性

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
セキュリティツール											
ネットワークベースのウイルス対策ソフトウェア	高	高	高	高	高	高	高	高	高	高	高
ホストベースのウイルス対策ソフトウェア	中	中	中	中	中	中	中	中	中	中	中
スパイウェア検出／駆除ユーティリティ					中	中				中	
ネットワークベースの侵入防止システム			中	中			低				
ホストベースの侵入防止システム			低		低	低	低	低	低	低	低
ネットワークベースのスパムフィルタ処理				高	低	中					高
ホストベースのスパムフィルタ処理				中	低	中					中
ネットワークベースの Web コンテンツフィルタ処理					低	中				中	
ホストベースの Web コンテンツフィルタ処理					低	中				中	
ネットワーク構成の変更											
ネットワークベースのファイアウォール			高	中		中	中	中		中	中
ホストベースのファイアウォール			中			中	中	中		中	中
インターネット境界ルータ			高			中	中	中		中	
内部ルータ			高			中	中	中		中	低
ホスト構成の変更											
ホストの強化（パッチ適用を含む）	低	低	低～中	低～中	低～中	低～中					
電子メールサーバの設定（電子メール添付ファイルのブロックなど）	低	低		高	中	中					高

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
組織のサーバ上で運用されているほかのサービスの設定			低～高								
アプリケーションクライアントの設定（電子メールクライアントや Web ブラウザでのモバイルコードの実行制限、ワードプロセッサでのマクロの使用制限など）		低	低			低				低	

表 A-5. 管理されていない環境における複雑な脅威に対する典型的な有効性

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
セキュリティツール											
ネットワークベースのウイルス対策ソフトウェア	高	高	高	高	高	高	高	高	高	高	高
ホストベースのウイルス対策ソフトウェア	中	中	中	中	中	中	中	中	中	中	中
スパイウェア検出／駆除ユーティリティ					中	中				中	
ネットワークベースの侵入防止システム			低	低			低				
ホストベースの侵入防止システム			低		低	低	低	低	低	低	低
ネットワークベースのスパムフィルタ処理				低～中	低	低					低～中
ホストベースのスパムフィルタ処理				低～中	低	低					低～中
ネットワークベースの Web コンテンツフィルタ処理					低	低				低	
ホストベースの Web コンテンツフィルタ処理					低	低				低	
ネットワーク構成の変更											
ネットワークベースのファイアウォール			高	中		中	低～中	低～中		低～中	低～中
ホストベースのファイアウォール			中			中	中	中		中	中
インターネット境界ルータ			高			中	低～中	低～中		低～中	
内部ルータ			高			中	低～中	低～中		低～中	低
ホスト構成の変更											

技術	マルウェアの種類						攻撃ツールの種類				
	複合感染型ウイルス	マクロウイルス	ネットワークサービスワーム	大量メールワーム	トロイの木馬	悪意のモバイルコード	バックドア	キーストロークロガー	ルートキット	悪意のブラウザプラグイン	電子メールジェネレータ
ホストの強化（パッチ適用を含む）	低	低	低～中	低～中	低～中	低～中					
電子メールサーバの設定（電子メール添付ファイルのブロックなど）	低	低		低～中	低	低					低～中
組織のサーバ上で運用されているほかのサービスの設定			低～中								
アプリケーションクライアントの設定（電子メールクライアントや Web ブラウザでのモバイルコードの実行制限、ワードプロセッサでのマクロの使用制限など）		低	低			低				低	

マルウェアインシデントを封じ込めるための方策の策定にあたっては、深刻なインシデントが発生した際にインシデント対応担当者が封じ込めの方策を速やかに選択し実施しやすくするためのツールを開発することを組織で検討するべきである。たとえば、新種のネットワークサービスワームが組織を攻撃し、組織のホストベースのファイアウォールソフトウェアに存在する脆弱性を利用している疑いがあることが明らかになったとする。また、このワームは比較的単純な特徴を持っており、組織ではホストのオペレーティングシステムとアプリケーションを高いレベルで集中管理しているとする。この場合組織の封じ込めの方策は、表 A-2 に基づくことになる。考えられる 1 つの方策は、たとえば、まず有効性が高いすべての技術の管理者に対して、最も適切な順序で連絡を取ることである。この事例では、次のような順序が考えられる。

1. ネットワークベースおよびホストベースのウイルス対策ソフトウェア[45]
   + ワームを検出して阻止する

[45] ネットワークウイルス対策ソフトウェアによって監視および分析されているアプリケーションプロトコルをホストベースファイアウォールで使用していない場合、この事例ではネットワークウイルス対策ソフトウェアは有効でない可能性がある。

- 感染したシステムの識別と駆除を行う

2. ホストベースのファイアウォール
   - ワーム活動のホストへの進入またはホストからの進出を遮断する
   - ホストベースのファイアウォールソフトウェア自身の設定を変更して、ワームによる悪用を防ぐ
   - ホストベースのファイアウォールソフトウェアを更新することで悪用されないようにする
3. ネットワークファイアウォール
   - ネットワークやサブネットへのワームの進入またはそこからの進出を検知して阻止する
4. インターネット境界ルータおよび内部ルータ
   - ネットワークファイアウォールが処理しきれないほどのトラフィック量がある場合や、特定のサブネットで保護を強化する必要がある場合は、ネットワークやサブネットへのワームの進入またはそこからの進出するのを検知して阻止する

インシデント対応担当者はまた、自己の裁量でほかの技術（ネットワークベースおよびホストベースの侵入防止システムなど）の管理者と連絡を取り、各管理者がワームを阻止するように各自のシステムを設定できるかどうかを判断することもできる。

管理されていない環境では、ホストベースのファイアウォールが集中管理されている可能性は低い。したがって、インシデント対応担当者は、ホストベースのファイアウォールが封じ込めに寄与するように更新、再設定、あるいは変更されていることに期待はできない。そのため、インシデント対応担当者はネットワークファイアウォールやルータなど、ネットワークベースの封じ込め管理策への依存度をずっと高める必要があり、ホストレベルではインシデントへの対応を実施できないと考えられる。

付録B—マルウェアインシデントへの対応のシナリオ

マルウェア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、マルウェア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、マルウェアインシデントへの対応に参加する各人員に対し、簡単なマルウェア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。

B.1 項に示した質問はほとんどすべてのマルウェアシナリオに当てはまる。これらの質問のあとに、いくつかの具体的なシナリオを示す。それぞれのシナリオのあとにそのシナリオに固有の追加質問を続ける。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。

B.1 シナリオの質問

準備／防止：

1. この種のマルウェア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？

検知と分析：

1. あなたの組織では、マルウェア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？

2. あなたの組織では、マルウェア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マルウェアインシデントが起きた可能性があると考えますか？

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？

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？

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？

封じ込め、根絶、および復旧：

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？

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？

インシデント発生後の活動：

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？

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？

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？

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が何人参加しますか？

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？

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？

4. 外部関係者への連絡事項には、ほかに何がありますか？

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？

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？

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？

B.2 シナリオ

シナリオ 1：ワームおよび DDoS エージェントの感染

ある火曜日の朝、新種のワームがインターネット上に登場した。ワームは Microsoft Windows の脆弱性を悪用したものである。この脆弱性は 2 週間前に公表されたもので、その時点でパッチが公開されていた。ワームは 2 つの方法を通じて拡散している。1 つは、感染したホスト上で見つかったすべてのアドレスにワーム自身を電子メールで送信する方法である。もう 1 つは、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方法である。このワームは、電子メールで送信す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作られている。各添付ファイルのファイル名は無作為に生成され、数十あるファイル拡張子のいずれかが使われる。また、電子メールの件名と本文は、それぞれ 100 を超える中から選択されるようになっている。ワームはホストに感染すると、管理者権限を取得し、FTP を使用してさまざまな IP アドレスから分散型サービス運用妨害（DDoS）エージェントをダウンロードしようとする。（エージェントを供給している IP アドレスの数は不明である）。ウイルス対策ベンダ各社は、このワームに関する警告を速やかに発したが、ベンダからシグネチャが公開される前に、ワームが非常に急速に拡散している。ワームが拡散を始めてから 3 時間後、ウイルス対策シグネチャが入手できるようになったが、組織はすでに広範囲な感染に見舞われていた。

このシナリオに対する追加の質問を次に示す。

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. ウイルス対策シグネチャが公開される前に、ワームが組織に侵入するのを、組織はどのようにして防ぎますか？

3. ウイルス対策シグネチャが公開される前に、感染したホストからワームが拡散するのを、組織はどのようにして防ぎますか？

4. 脆弱性のあるすべてのマシンに対してパッチの適用を試みますか？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、翌朝にほかの組織の Web サイトを攻撃するように設定されているとしたら、このインシデントへの対応はどのように変わりますか？

6. インシデント対応チームから組織のユーザに対して、どのようにしてインシデントの状態について逐次情報を提供しますか？ワームが原因で電子メールサービスが過負荷状態になったり使用不能になったりした場合はどうしますか？

7. 現在ネットワークに接続されていないホスト（休暇中のスタッフや、サイトの外にいて時折ダイヤルインする職員など）に対応するために、どんな追加対策(あれば)を行いますか？

シナリオ 2：外部への DDoS 攻撃

ある日曜日の夜、組織のネットワーク侵入検出センサの 1 つで、大量の ICMP（Internet Control Message Protocol）ping を伴う外部への DDoS 活動の疑いが警告された。侵入分析担当者が警報を確認したところ、警報が正しいことを確定できなかったが、既知のどのフォールスポジティブにも合致しなかった。分析担当者は、活動を詳しく調査できるようにインシデント対応チームに連絡を取った。DDoS 活動ではなりすましの送信元 IP アドレスが使用されるため、組織内部のどのホスト（1 つまたは複数）がその活動を生成しているのかを特定するのにかなりの時間と労力を要した。そのあいだ、DDoS 活動は続く。調査の結果、7 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。サーバの初期分析を行ったところ、それぞれのサーバで DDoS ルートキットの兆候が見られた。

このシナリオに対する追加の質問を次に示す。

1. チームは、組織内のどのホストがトラフィックを生成しているのかをどのようにして特定しますか？ほかのどのチームがインシデント対応チームを支援できる可能性がありますか？

2. トラフィックを生成しているサーバを識別したあと、チームはサーバがマルウェアに感染しているかどうかをどのようにして判断しますか？

シナリオ 3：給与記録への不正なアクセス

ある水曜日の夕方、見知らぬ人物が事務所から立ち去るのを見かけた給与管理者が、組織の物理セキュリティチームに電話で連絡した。給与管理者は、その人物が廊下を駆け抜け、建物の出口に通じる階段室に入るのを見たという。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、数分のあいだ無人にしていた。給与管理プログラムは、管理者が席を離れたときと同じログインしたままの状態でメインメニュー画面が表示されていたが、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、インシデントに関連する証拠を収集し、どのような行為が行われたか（給与データへのアクセスまたはそのデータの改ざん、トロイの木馬の設置など）を調べるよう依頼された。

このシナリオに対する追加の質問を次に示す。

1. どのような行為が行われ、どのようなマルウェア（あれば）がインストールされたのかを、チームでどのように調べますか？

2. 侵入者がいたことが判明していることから、このインシデントへの対応は、ほかのマルウェア関連のインシデントの場合と比べてどのように変わりますか？

シナリオ 4：在宅勤務システムの侵害

ある土曜日の夜、ネットワーク侵入検出ソフトウェアが、内部の IP アドレスから発信されたいくつか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出ソフトウェアも、いくつかのプローブとスキャンを記録した。侵入検知分析担当者は、内部の IP アドレスが組織の仮想プライベートネットワーク（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 サーバの各ログを調べ、その活動を生成している外部の IP アドレス、該当セッションに対して認証されたユーザ ID、およびそのユーザ ID に関連付けられているユーザの名前を特定した。

このシナリオに対する追加の質問を次に示す。

1. 特定されたユーザのパーソナルコンピュータが、その家族によってダウンロードされたゲームに含まれていたトロイの木馬に感染しているとします。それはインシデントへの対応にどのような影響を与えますか？

2. 特定されたユーザのパーソナルコンピュータがネットワークサービスワームに感染しているとします。それはインシデントへの対応にどのような影響を与えますか？

シナリオ 5：アプリケーションのクラッシュ

ある月曜日の朝、組織のヘルプデスクが 3 人のユーザから電話を受けた。いずれも、スプレッドシートアプリケーションが使用中に何度もクラッシュする問題が生じているということだった。その日のうちに、ほかのユーザからも同様の問題が電話で報告された。ユーザのほとんどは同じチームまたは関連するチームに所属している。

1. どのような種類のマルウェアがスプレッドシートアプリケーションのクラッシュの原因として考えられますか？マルウェア以外の原因として最も可能性が高いのは何ですか？

2. クラッシュの原因がマルウェアであるかどうかを判断するためには、どのような手順を実施したらよいですか？

シナリオ 6：悪意のモバイルコード

ある金曜の午後、数人のユーザからヘルプデスクに連絡があり、奇妙なポップアップウィンドウやツールバーが Web ブラウザに表示されるという報告があった。ユーザの状況説明はどれも似かよっていることから、ヘルプデスクエージェントは、ユーザのシステムが同じものの影響を受けており、Web ベースの悪意のモバイルコードが原因として最も可能性が高いと確信した。

1. インシデント対応チームは、どの脆弱性または構成設定が悪意のモバイルコードによるシステムへの感染を許したのかをどうやって調べますか？

2. インシデント対応チームは、どの Web サイト（1 つまたは複数）からユーザのシステムに悪意のモバイルコードが送信されたのかをどうやって調べますか？

シナリオ 7：混合型マルウェア攻撃

組織で新しいインスタントメッセージプラットフォームを採用してから間もなく、その利用者が広範囲にわたるマルウェアの攻撃を受けた。このマルウェアは、インスタントメッセージを通じて自身を伝染させるものである。セキュリティ管理者からの初期の報告では、攻撃はワームによるものとみられた。しかし、以降の報告で、Web サーバと Web クライアントも攻撃に関与していることが示された。いずれも同じメッセージをユーザに表示することから、インスタントメッセージと Web ベースの攻撃がワームに関連しているものとみられる。

1. このマルウェアは混合攻撃を行うものである可能性が最も高いことから、その対応はワームの場合とどのように変わりますか？
2. 組織は、どの攻撃媒介要素に対して最初に封じ込め措置の重点を置きますか？また、それはなぜですか？

（本ページは意図的に白紙のままとする）

付録C—用語集

『*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*』で使用している用語について、その一部の定義を以下に示す。

ウイルス対策ソフトウェア（Antivirus Software）：コンピュータやネットワークを監視し、主要な種類のマルウェアをすべて識別して、マルウェアインシデントの防止や封じ込めを行うプログラム。

バックドア（Backdoor）：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、悪意のプログラム。

混合攻撃（Blended Attack）：複数の感染手段や伝送手段を利用するマルウェアの一種。

ブートセクタウイルス（Boot Sector Virus）：ハードディスクドライブのマスタブートレコード（MBR）や、ハードディスクドライブまたはリムーバブルメディア（フロッピーディスクなど）のブートセクタに感染するウイルス。

コンパイル型ウイルス（Compiled Virus）：コンパイラプログラムにより、そのソースコードがオペレーティングシステムで直接実行できる形式に変換されたウイルス。

クッキー（Cookie）：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。

デフォルトで拒否（Deny by Default）：明示的に許可されていない着信および発信のトラフィック（マルウェアの拡散に使用される可能性のある不要なサービスなど）をすべて拒否する、ファイアウォールやルータの設定。

感染除去（Disinfecting）：ファイルの内部からマルウェアを取り除くこと。

出口フィルタ（Egress Filtering）：ネットワークから出るべきでない発信パケットをブロックすること。

フォールスネガティブ（False Negative）：特定の脅威の検出を目的とするセキュリティツールがその脅威の検出に失敗する事例。

フォールスポジティブ（False Positive）：セキュリティツールが害のないコンテンツを誤って悪意のあるものとして分類してしまう事例。

ファイル感染ウイルス（File Infector Virus）：自分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、コンピュータゲームなどの実行可能プログラムに添付するウイルス。

ホストベースの侵入防止システム（Host-Based Intrusion Prevention System）：単一のホストの特徴と、そのホストの内部で発生しているイベントを監視し、疑わしい活動を識別して阻止するプログラム。

兆候（Indication）：マルウェアインシデントがすでに発生したか、発生中である可能性を示すサイン。

入口フィルタ（Ingress Filtering）：ネットワークに進入すべきでない着信パケットをブロックすること。

インタプリタ型ウイルス（Interpreted Virus）：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たウイルス。

キーストロークロガー（Keystroke Logger）：キーボードの使用を監視し記録する仕組み。

マクロウイルス（Macro Virus）：自分自身をワードプロセッサファイルやスプレッドシートなどのアプリケーション文書に添付し、対象アプリケーションのマクロプログラミング言語を利用して実行や伝染を行うウイルス。

悪意のコード（Malicious Code）：「マルウェア」を参照。

マルウェア（Malware）：被害者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、または可用性を損なう目的で、あるいは被害者を困らせたり混乱させたりする目的で、通常は気づかれないようにシステムに挿入されるプログラム。

大量メールワーム（Mass Mailing Worm）：感染したシステムで電子メールアドレスを特定し（感染システムを検索することが多い）、それらのアドレスに自分自身のコピーを送信することによって拡散するワーム。送信には、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が使用される。

メモリ常駐型（Memory Resident）：感染したシステムのメモリ内に長期間にわたってとどまるウイルス。

モバイルコード（Mobile Code）：ローカルシステムでの実行を目的として、通常はユーザによる明示的な指示なしにリモートシステムから送信されるソフトウェア。

複合感染型ウイルス（Multipartite Virus）：複数の感染手段を利用するウイルス。通常はファイルとブートセクタの両方に感染する。

ネットワークサービスワーム（Network Service Worm）：オペレーティングシステムやアプリケーションに関連したネットワークサービスの中にある脆弱性を利用することによって拡散するワーム。

ネットワークベースの侵入防止システム（Network-Based Intrusion Prevention System）：パケットの傍受とネットワークトラフィックの分析を実行して、疑わしい活動を識別し阻止するプログラム。

難読化技法（Obfuscation Technique）：ウイルス自身が検出されにくくなるようにウイルスを作成する手段。

アクセス時スキャン（On-Access Scanning）：ファイルをダウンロードするとき、開くとき、または実行するときに、リアルタイムスキャンを実行してマルウェアがないかを調べるようにセキュリティツールを設定すること。

要求時スキャン（On-Demand Scanning）：ユーザが必要に応じてセキュリティツールを起動し、コンピュータ上でマルウェアをスキャンできるようにすること。

ペイロード（Payload）：ウイルス本体のうち、ウイルスの目的に応じたコードが含まれている部分。ペイロードは、比較的良性のもの（人に迷惑をかける、個人的な意見を表明するなど）から、きわめて悪性のもの（個人情報を他人に転送する、システムを消去するなど）まで多様である。

永続クッキー（Persistent Cookie）：Web サイトが以降のアクセス時にユーザを識別できるように、コンピュータ上に無期限に格納されるクッキー。

フィッシング（Phishing）：コンピュータを利用した詐欺手段を通じて個人をだまし、機密情報や個人情報を入手すること。

前兆（Precursor）：将来マルウェアによる攻撃が発生する可能性を示すサイン。

プロキシ（Proxy）：クライアントからの要求を受け取り、クライアントに代わって要求を必要な送信先に送信するプログラム。

隔離（Quarantining）：あとで感染除去や検査ができるように、マルウェアが含まれているファイルを隔離した場所に格納しておくこと。

リモート管理ツール（Remote Administration Tool）：リモートの攻撃者が必要に応じてシステムにアクセスできるように、当該システムにインストールされたプログラム。

ルートキット（Rootkit）：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。

セッションクッキー（Session Cookie）：単一の 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。

シグネチャ（Signature）：既知のマルウェアの特徴を集めたもの。既知のマルウェアや、その新種の派生版の一部を識別するのに使用できる。

スパイウェア（Spyware）：ユーザのプライバシ侵害を目的とするマルウェア。

スパイウェア検出／駆除ユーティリティ（Spyware Detection and Removal Utility）：コンピュータを監視し、スパイウェアの識別と、スパイウェアインシデントの防止や封じ込めを行うプログラム。

追跡クッキー（Tracking Cookie）：ユーザのコンピュータ上に置かれ、さまざまな Web サイトにおけるユーザの活動を追跡し、ユーザの振る舞いの詳細なプロファイルを作成するクッキー。

トリガ（Trigger）：ペイロードが実行される契機となる条件。通常はユーザの操作（ファイルを開く、プログラムを実行する、電子メールの添付ファイルをクリックするなど）によって生じる。

トロイの木馬（Trojan Horse）：見かけ上は害がないように装いながら、実際には悪意のある目的を持った非複製型プログラム。

ウイルス（Virus）：マルウェアの形態の 1 つ。自己複製、つまり、自分自身のコピーを作成し、それらをほかのファイルやプログラム、またはコンピュータに配布するように作成されたもの。

Web ブラウザプラグイン（Web Browser Plug-In）：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メカニズム。

Web バグ（Web Bug）：Web ページや電子メールの HTML（ハイパーテキストマークアップ言語）コンテンツの中で参照される、Web サイト上のごく小さなグラフィック。このグラフィックの目的は、コンテンツを閲覧しているユーザに関する情報を収集することである。

ワーム（Worm）：完全な自己完結性と自己伝染力を備えた自己複製プログラム。

ゾンビ（Zombie）：あるシステムにインストールされることによってほかのシステムを攻撃するプログラム。

（本ページは意図的に白紙のままとする）

付録D—略語

『*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*』で使用している略語について、その一部の定義を以下に示す。

ACL	Access Control List (**アクセス制御リスト**)
APWG	Anti-Phishing Working Group
ASC	Anti-Spyware Coalition
AVIEN	Anti-Virus Information Exchange Network
BIOS	Basic Input/Output System (**基本入出力システム**)
CAIDA	Cooperative Association for Internet Data Analysis
CARO	Computer Antivirus Research Organization
CD	Compact Disc (**コンパクトディスク**)
CIAC	Computer Incident Advisory Capability
CME	Common Malware Enumeration
CSRC	Computer Security Resource Center
DDoS	Distributed Denial of Service (**分散型サービス運用妨害**)
DNS	Domain Name System (**ドメインネームシステム**)
DShield	Distributed Intrusion Detection System
DVD	Digital Video Disc (**デジタルビデオディスク**)
EICAR	European Institute for Computer Antivirus Research
FAQ	Frequently Asked Questions (**よく寄せられる質問**)
FISMA	Federal Information Security Management Act (**連邦情報セキュリティマネジメント法**)
FTC	Federal Trade Commission (**連邦取引委員会**)
FTP	File Transfer Protocol (**ファイル転送プロトコル**)
HTML	Hypertext Markup Language (**ハイパーテキストマークアップ言語**)
HTTP	Hypertext Transfer Protocol (**ハイパーテキスト転送プロトコル**)
ICMP	Internet Control Message Protocol (**インターネット制御通知プロトコル**)
ID	Identification (**識別子**)
IDS	Intrusion Detection System (**侵入検知システム**)
IETF	Internet Engineering Task Force
IIS	Internet Information Services (**インターネットインフォメーションサービス**)
IP	Internet Protocol (**インターネットプロトコル**)
IPS	Intrusion Prevention System (**侵入防止システム**)
ISC	Internet Storm Center
IT	Information Technology (**情報技術**)
ITL	Information Technology Laboratory (**情報技術ラボラトリ**)
MAC	Media Access Control (**媒体アクセス制御**)
MBR	Master Boot Record (**マスタブートレコード**)
NAP	Network Access Protection
NAT	Network Address Translation (**ネットワークアドレス変換**)

NIST	National Institute of Standards and Technology (**米国国立標準技術研究所**)
NSRL	National Software Reference Library
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**)
PDA	Personal Digital Assistant
PIN	Personal Identification Number (**暗証番号**)
RAT	Remote Administration Tool (**リモート管理ツール**)
RFC	Request for Comment
SI	System and Information Integrity (**システムおよび情報の完全性**)
SMTP	Simple Mail Transfer Protocol (**簡易メール転送プロトコル**)
SP	Special Publication (**特別刊行物**)
TCP	Transmission Control Protocol (**伝送制御プロトコル**)
UDP	User Datagram Protocol (**ユーザデータグラムプロトコル**)
USB	Universal Serial Bus (**ユニバーサルシリアルバス**)
US-CERT	United States Computer Emergency Readiness Team
VBScript	Visual Basic Script (Visual Basic **スクリプト**)
VLAN	Virtual Local Area Network (**仮想ローカルエリアネットワーク**)
VPN	Virtual Private Network (**仮想プライベートネットワーク**)

付録E—印刷資料

Erbschloe, Michael.*Trojans, Worms, and Spyware:A Computer Security Professional's Guide to Malicious Code*.Butterworth-Heinemann, 2004.

Feinstein, Ken. *How to Do Everything to Fight Spam, Viruses, Pop-Ups, and Spyware*.McGraw-Hill Osborne Media, 2004.

Grimes, Roger.*Malicious Mobile Code:Virus Protection for Windows*.O'Reilly, 2001.

McClure, Stuart, et al.*Hacking Exposed:Network Security Secrets & Solutions, Fifth Edition*.McGraw-Hill Osborne Media, 2005.

Nazario, Jose.*Defense and Detection Strategies Against Internet Worms*.Artech House Publishers, 2003.

Prosise, Chris, et al.*Incident Response and Computer Forensics, Second Edition*.McGraw-Hill Osborne Media, 2003.

Schweitzer, Douglas.*Securing the Network from Malicious Code:A Complete Guide to Defending Against Viruses, Worms, and Trojans*.Wiley, 2002.

Skoudis, Ed, and Lenny Zeltser.*Malware:Fighting Malicious Code*.Prentice Hall PTR, 2003.

Szor, Peter.*The Art of Computer Virus Research and Defense*.Addison-Wesley, 2005.

Tittel, Ed. *PC Magazine Fighting Spyware, Viruses, and Malwar*e. John Wiley & Sons, 2004.

Virus Bulletin (**雑誌**).Virus Bulletin Ltd.

（本ページは意図的に白紙のままとする）

付録F—オンライン資料

マルウェアの理解、マルウェアインシデントの防止、およびマルウェアインシデントへの対応に役立つオンライン資料の例を以下に示す。

組織

組織	URL
Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
Anti-Spyware Coalition (ASC)	http://www.antispywarecoalition.org/
Anti-Virus Information Exchange Network (AVIEN)	http://www.avien.org/
Common Malware Enumeration (CME)	http://cme.mitre.org/
Computer Antivirus Research Organization (CARO)	http://www.caro.org/
Computer Incident Advisory Capability (CIAC)	http://www.ciac.org/ciac/
Cooperative Association for Internet Data Analysis (CAIDA)	http://www.caida.org/
Distributed Intrusion Detection System (DShield)	http://dshield.org/
European Institute for Computer Antivirus Research (EICAR)	http://www.eicar.org/
Internet Storm Center (ISC)	http://isc.incidents.org/
SANS Institute	http://www.sans.org/
United States Computer Emergency Readiness Team (US-CERT)	http://www.us-cert.gov/
Virus Bulletin	http://www.virusbtn.com/
Viruslist.com	http://www.viruslist.com/en/
WildList Organization International	http://www.wildlist.org/

技術資料サイト

資料名	URL
C|Net Download.com–Spyware Center	http://www.download.com/Spyware-Center/2001-2023_4-0.html?tag=dir
Computer Associates Virus Information Center	http://www3.ca.com/securityadvisor/virusinfo/default.aspx
CSRC–Practices & Checklist/Implementation Guides	http://csrc.nist.gov/pcig/cig.html
F-Secure Security Information Center	http://www.f-secure.com/virus-info/
McAfee AVERT Virus Information Library	http://vil.nai.com/vil/default.asp
SANS Malware FAQ	http://www.sans.org/resources/malwarefaq/
SecurityFocus Virus	http://www.securityfocus.com/virus/
Sophos Virus Analyses	http://www.sophos.com/virusinfo/analyses/
Spywaredata.com	http://www.spywaredata.com/
Symantec Security Response–Search and Latest Virus Threats Page	http://securityresponse.symantec.com/avcenter/vinfodb.html
Trend Micro Virus Encyclopedia Search	http://www.trendmicro.com/vinfo/virusencyclo/
Unassigned IP Address Ranges	http://www.cymru.com/Documents/bogon-list.html
Vmyths.com–Truth About Computer Virus Myths & Hoaxes	http://www.vmyths.com/

メーリングリストと通知サービス

メーリングリスト／通知サービス名	URL
Focus-Virus	http://www.securityfocus.com/archive/100/
F-Secure Radar	http://www.f-secure.com/products/radar/
Incidents	http://www.securityfocus.com/archive/75/
McAfee AVERT Alerts	http://vil.nai.com/vil/content/alert.htm
Sophos Email Notification	http://www.sophos.com/virusinfo/notifications/
Symantec Security Response–Alerting Offerings	http://securityresponse.symantec.com/avcenter/alerting_offerings.html
Trend Micro Newsletters	http://www.trendmicro.com/subscriptions/default.asp

そのほかの技術資料文書

資料名	URL
CAIDA, *The Spread of the Sapphire/Slammer Worm*	http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html
CAIDA, *The Spread of the Witty Worm*	http://www.caida.org/analysis/security/witty/
CAIDA, *The Top Speed of Flash Worms*	http://www.caida.org/outreach/papers/2004/topspeedworms/topspeed-worm04.pdf
CARO, CARO Virus Naming Convention	http://www.caro.org/tiki-index.php?page=CaroNamingScheme
FTC, *How Not to Get Hooked by a "Phishing" Scam*	http://ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
IETF, RFC 2267, *Network Ingress Filtering:Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*	http://www.ietf.org/rfc/rfc2267.txt
Infoplease, Computer Virus Timeline	http://www.infoplease.com/ipa/A0872842.html
Microsoft, *The Antivirus Defense-in-Depth Guide*	http://www.microsoft.com/technet/security/topics/serversecurity/avdind_0.mspx
NIST, SP 800-28, *Guidelines on Active Content and Mobile Code*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, SP 800-31, *Intrusion Detection Systems*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, SP 800-40, *Creating a Patch and Vulnerability Management Program*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, SP 800-42, *Guideline on Network Security Testing*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, SP 800-45, *Guidelines on Electronic Mail Security*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, SP 800-53, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, SP 800-61, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, SP 800-70, *Security Configuration Checklists Program for IT Products*	http://csrc.nist.gov/checklists/
NIST, SP 800-86 (草稿版) , *Guide to Applying Forensic Techniques to Incident Response*	http://csrc.nist.gov/publications/nistpubs/index.html
NIST, *Threat Assessment of Malicious Code and Human Threats*	http://csrc.nist.gov/publications/nistir/threats/threats.html
Washington Post, *A Short History of Computer Viruses and Attacks*	http://www.washingtonpost.com/ac2/wp-dyn/A50636-2002Jun26?start=15&per=18

付録G—索引