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

Special Publication 800-86

インシデント対応へのフォレンジック技法の統合に関するガイド

米国国立標準技術研究所による勧告

Karen Kent
Suzanne Chevalier
Tim Grance
Hung Dang

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 800-86

インシデント対応へのフォレンジック技法の統合に関するガイド

米国国立標準技術研究所による勧告

Karen Kent, Suzanne Chevalier,
Tim Grance, Hung Dang

コンピュータ セキュリティ

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

2006 年 8 月

米国商務省　長官

Carlos M. Gutierrez

技術管理局　技術担当商務次官

Robert C. Cresanti

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を施し、国家安全保障にかかわらない情報のプライバシーを確保するための、技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報システムセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動ならびに産業界、政府機関および教育機関との共同活動について報告する。

米国国立標準技術研究所、Special Publication 800-86
米国国立標準技術研究所、Special Publication 800-86, 121 ページ（2006 年 8 月）

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

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

謝辞

本書執筆陣である Karen Kent、Tim Grance（ともに NIST）、Suzanne Chevalier、および Hung Dang（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 Rick Ayers、Wayne Jansen、Peter Mell、Murugiah Souppaya（4 人ともに NIST）、Adam Feldman、Mike Noblett、および Joseph Nusbaum（3 人ともに Booz Allen Hamilton）に感謝したい。また、特に貴重な意見や提案を寄せてくれた、セキュリティの専門家である Susan Ballou（Office of Law Enforcement Standards）、Brian Carrier（Purdue University）、Eoghan Casey（Stroz Friedberg, LLC）、Duane Crider（Microsoft）、Kurt Dillard（Microsoft）、Dean Farrington（Wells Fargo Bank）、Jessica Reust（Stroz Friedberg, LLC）、Marc Rogers（Purdue University）、Miles Tracy（米国連邦準備制度）、および国務省の代表者の方々にも感謝の意を表したい。

商標

目次

付録

図

表

要旨

フォレンジックスサイエンスは、一般に、法律に科学的手法を適用することと定義されている。ディジタルフォレンジックスは、コンピュータ／ネットワークフォレンジックスとも呼ばれ、さまざまな定義がある。一般には、情報の完全性を保護し、データの厳密な保管引渡し管理を維持しながら、データの識別、収集、検査、および分析に科学的手法を適用することとみなされている。データとは、特定の形態で整形されたディジタル情報の個別の断片を指す。各組織がさまざまなソースから得るデータの量は、増加の一途をたどっている。たとえば、標準的なコンピュータシステム、ネットワーク機器、コンピュータ周辺装置、PDA（personal digital assistant：携帯情報端末）、家庭用電子機器、各種のメディアなど、さなざまなソースにデータを格納したり、それらを使用して移動したりできる。

データソースの種類は多いため、ディジタルフォレンジック技法は、犯罪や内部ポリシー違反の調査、コンピュータセキュリティインシデントの再現、運用上の問題のトラブルシューティング、偶発的なシステム損害からの復旧など、さまざまな用途に使用し得る。ディジタルフォレンジックス（以下、*フォレンジックス*と称す）を行う能力は、ほぼすべての組織に必要である。このような能力を持たない組織では、組織のシステムやネットワークのなかでどのような事象（たとえば、保護されている機密データの露出など）が起きたかを特定するのが困難になる。このガイドでは、フォレンジック能力の確立に関する詳細を説明する。これには、ポリシーと手続きの策定が含まれる。中心となる題材は、フォレンジック技法を使ったコンピュータセキュリティインシデント対応の支援であるが、題材の多くはほかの状況にも適用できる。

組織によって従うべき法律や規制が異なるため、この文書を、ディジタルフォレンジック調査を行うための手引きとして使用したり、法的な助言として解釈したり、犯罪活動調査の根拠として使用したりするべきではない[1]。代わりに、各組織は、法律顧問、法執行機関の当局者、および管理職層によって提供される広範囲の指導と併せて、フォレンジック能力を開発するための出発点としてこのガイドを使用するべきである。

ディジタルフォレンジックス実施のプロセスは、次の基本フェーズで構成される。

- **収集**：データの完全性を保護する手続きに従いながら、関連するデータを識別し、ラベル付けし、記録し、ソースの候補から取得する。
- **検査**：データの完全性を保護しながら、収集したデータを自動的手法および手動的手法の組み合わせを使ってフォレンジック的に処理することにより、特に注目に値するデータを見定めて抽出する。
- **分析**：法的に正当と認められる手法および技法を使用して検査結果を分析することにより、収集と検査を行う契機となった疑問を解決するのに役立つ情報を導き出す。
- **報告**：分析結果を報告する。これには、使用された措置の記述、ツールや手続きの選択方法の説明、実行する必要があるそのほかの措置（追加のデータソースのフォレンジック検査、識別された脆弱性の安全対策、既存のセキュリティ管理策の改善など）の特定、フォレンジックプロセスのポリシー、手続き、ツール、およびそのほかの側面の改善に関する推奨事項の提示などが含まれる可能性がある。

[1] 法執行機関に対するコンピュータ／ネットワークフォレンジック要件の詳細については、『*Electronic Crime Scene Investigation: A Guide for First Responders*』および『*Forensic Examination of Digital Evidence: A Guide for Law Enforcement*』を参照すること。これらの文書は、いずれもhttp://www.ncjrs.gov/で各文書のタイトルを検索することによって入手できる。

このガイドでは、フォレンジックプロセスを実行するための一般的な推奨事項を示す。また、4 つの主要なデータソースの分類であるファイル、オペレーティングシステム、ネットワークトラフィック、およびアプリケーションを対象に分析プロセスを使用する方法の詳細についても説明する。このガイドでは、各分類に含まれるデータソースの基本的な構成要素および特性の説明と、各分類に含まれるデータの収集、検査、および分析の技法の説明に重点を置いている。このガイドではまた、事象をよりよく理解するために複数のデータソースを組み合わせて使用する際の推奨事項も示す。

以下の推奨事項を実施することにより、連邦政府の各省庁や機関において、効率的で効果的なディジタルフォレンジック活動が促進されるはずである。

各組織は、法執行機関との連絡、監視の実行、フォレンジックのポリシーと手続きの定期的な見直しの実施など、フォレンジックに関する主要なすべての考慮事項に対応した明確な声明を組織のポリシーに確実に含めるようにすること。

ポリシーは、高次においては、システムやネットワークの監視と調査を、許可された職員が正当な理由に基づき適切な条件の下で行うことを許可するべきである。各組織は、インシデント対応担当者やフォレンジックに関わる役割を持つそのほかの者に対し、独立のフォレンジックポリシーを持つこともできる。このポリシーにおいて、適切な振る舞いに関する、より詳細な規則を提供する。フォレンジックポリシーでは、組織のフォレンジック活動を実行または支援するすべての個人および外部組織の役割と責任を明確に規定するべきである。このポリシーでは、さまざま条件の下で誰がどの内部チームおよび外部組織と連絡を取るのかを明確に示すべきである。

各組織は、組織のポリシーと適用可能なすべての法律および規制に基づいて、フォレンジック作業を実行するための手続きとガイドラインを作成し、管理すること。

想定されるあらゆる状況に合わせて調整された包括的な手続きを作成するのは現実的でないため、ガイドラインでは、フォレンジックの技法を使ってインシデントを調査するための一般的な方法論に重点を置くべきである。ただし、各組織は定型的な作業を実行するための順を追った手続きの作成を検討するべきである。これらのガイドラインと手続きによって、一貫性のある効果的で正確な措置が促進される。このことは、訴訟や内部の懲戒処分につながる可能性があるインシデントでは特に重要である。フォレンジック面から見て適切な方法で証拠を取り扱うことにより、意志決定者は自信を持って必要な措置を取ることができる立場に置かれる。これらのガイドラインと手続きは、訴訟手続きにおける証拠能力の裏付けとなるべきである。これには、証拠の適切な収集と取り扱い、ツールや機器の完全性の保護、保管引渡し管理の維持、および証拠の適切な保管に関する情報が含まれる。電子的なログやそのほかの記録は、改変または操作される可能性があるため、各組織はポリシー、ガイドライン、および手続きによってこのような記録の完全性を立証できるように備えておくべきである。これらのガイドラインと手続きは、定期的に、およびチームのポリシーや手続きに重大な変更が行われたときに、見直しを行うべきである。

各組織は、フォレンジックツールの妥当かつ適切な使用が、組織のポリシーと手続きによって確実に裏付けられるようにすること。

組織のポリシーと手続きでは、さまざまな条件下で実行すべきフォレンジック措置と実行すべきでないフォレンジック措置を明確に説明するとともに、フォレンジックツールによって記録される可能性がある機密情報（パスワード、社会保障番号などの個人データ、電子メールの内容など）の必要な保護策も記載するべきである。法律顧問は、すべてのフォレンジックポリシーと高次の手続きを慎重に精査するべきである。

各組織は、組織の IT 担当者がフォレンジック活動に参加できるように確実に備えができているようにすること。

組織全体の IT 担当者、特にインシデント対応担当者やインシデントに最初に対応するそのほかの者は、フォレンジックスに関する自分の役割と責任を理解し、フォレンジック関連のポリシーと手続きに関するトレーニングや教育を受け、自分が責任を負う技術がインシデントやそのほかの事象に含まれる場合に、ほかの人々と協力し、支援する準備を整えるべきである。また、IT 担当者は、フォレンジックス活動の全般的な備えの一環として（IT 担当者が実行すべき措置とすべきでない措置の判断など）、および、必要に応じて具体的なフォレンジックス状況についても、弁護士と綿密に相談するべきである。さらに、管理職層は、フォレンジック能力の支援、フォレンジックポリシーの審査と承認、および特定のフォレンジック措置（ミッションクリティカルシステムをオフラインにすることなど）の承認を行う責任を負う。

（本ページは意図的に白紙のままとする）

1. はじめに

1.1 作成機関

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

NIST は、すべての連邦政府機関の運営および資産に適切な情報セキュリティをもたらすために、最低限の要求事項を含んだ標準およびガイドラインを作成する責務があるが、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局（OMB; Office of Management and Budget）Circular A-130、第 8b(3)項、『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項に一致しており、これは A-130 の付録 IV「重要部門の分析」で分析されているとおりである。補足情報は、A-130、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が使用する目的で作成されている。非政府組織が自由意志で使用することもでき、著作権の制約はない（翻訳者注:著作権に関するこの記述は、SP800-86 の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する）。

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

このガイドラインは、犯罪活動の調査に関係する法執行機関の職員の義務を示すものではない。

1.2 目的と範囲

この文書は、コンピュータ／ネットワークフォレンジックスを行うための実践的ガイダンスを提供することにより、各組織によるコンピュータセキュリティインシデントの調査や情報技術（IT）の運用上の問題のトラブルシューティングを支援することを目的としている。**このガイドでは、法執行機関の観点ではなく、IT の観点からフォレンジックスを示している**[2]。特に、この文書では効果的なフォレンジックス活動を行うためのプロセスを説明し、ファイル、オペレーティングシステム（OS）、ネットワークトラフィック、アプリケーションなどの、さまざまなデータソースに関する助言を提供する。

この文書は、ディジタルフォレンジック調査を行うための網羅的かつ順を追ったガイドとして使用したり、法律上の助言として解釈したりしてはならない。この文書の目的は、さまざまな技法と、それらの技法を使ってインシデント対応や活動のトラブルシューティングを行う方法の例を読者に伝えることである。読者は、推奨される実践事項を適用する前に、必ずそれぞれの状況に関係する（地域、州、連邦、および国際上の）法律や規制の遵守について管理職層や弁護士に相談することが推奨される。

---

[2] 法執行機関に対するコンピュータ／ネットワークフォレンジック要件の詳細については、『*Electronic Crime Scene Investigation: A Guide for First Responders*』および『*Forensic Examination of Digital Evidence: A Guide for Law Enforcement*』を参照すること。これらの文書は、いずれもhttp://www.ncjrs.gov/で各文書のタイトルを検索することによって入手できる。

1.3 対象とする読者

この文書は、調査、インシデント対応、またはトラブルシューティングのためにフォレンジックスを行う責任を負うインシデント対応チーム、フォレンジックス分析担当者、システム、ネットワーク、セキュリティの各管理者、およびコンピュータセキュリティプログラム管理者のために作成された。このガイドで推奨する実践事項は、電子的な証拠の取り扱いと検査に関連する主な原則を明らかにするように設計されている。電子機器やソフトウェア、およびフォレンジックの手続きやツールは絶えず変化するため、このガイドに示したものよりも新しい情報や詳しい情報については、ほかの資料（このガイドに示した資料を含む）を参照することを読者に期待する。

1.4 文書の構成

この文書は以降、以下の 7 つの主要なセクションに分かれている。

- セクション 2 では、コンピュータ／ネットワークフォレンジックスの必要性を論じ、組織のフォレンジックス能力の確立と組織化に関するガイダンスを示す。
- セクション 3 では、コンピュータ／ネットワークフォレンジックスの実行に関わる基本的な手順である、データの収集、検査、分析、および報告について説明する。
- セクション 4 からセクション 7 では、セクション 3 で説明した枠組みに基づいて、さまざまなデータソースからのデータの収集、検査、および分析の詳細を示す。セクション 4 からセクション 7 で説明するデータソースの分類は、それぞれデータファイル、OS、ネットワークトラフィック、およびアプリケーションである。
- セクション 8 では、分析によって複数のデータソースの事象を相互に関連付ける方法を例証する事例研究を示す。

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 には、この文書で提示した主な推奨事項を示す。
- 付録 B では、フォレンジックスの技法が有効と思われるシナリオを示し、各シナリオに関して読者に一連の質問を行う。
- 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 には印刷資料の一覧を、付録 F にはオンラインのツールや資料を記載している。これらは、フォレンジックス能力の確立やフォレンジックスのツールと技法の理解に役立つと考えられる。
- 付録 G には、この文書の索引を示す。

2. フォレンジックス能力の確立と組織化

データという用語は、特定の形態で整形されたディジタル情報の個別の断片を指す。業務および個人で利用するコンピュータ[3]の増加やネットワークの普及により、増え続けるさまざまなソースのデータを記録して分析することができるツールに対するニーズが高まった。たとえば、標準的なコンピュータシステム（デスクトップ、ラップトップ、サーバなど）、ネットワーク機器（ファイアウォール、ルータなど）、コンピュータ周辺装置（プリンタ）、PDA（携帯情報端末）、CD、DVD、リムーバブルハードディスク、バックアップテープ、フラッシュメモリ、USB メモリなどにデータを格納したり、それらを使用して移動したりできる。多くの家庭用電子機器（携帯電話、テレビゲーム機器、ディジタルオーディオプレーヤ、ディジタルビデオレコーダなど）も、データを保存するために使用できる。このようにデータソースの種類が増え続けていることが、フォレンジックスのツールと技法の開発や改良の加速を促している。この現象のもう 1 つの原因は、このようなツールや技法が、犯罪の調査、コンピュータセキュリティインシデントの再現、運用上の問題のトラブルシューティング、偶発的なシステム損害からの復旧など、さまざまな用途に使用できるという認識にある。

このセクションでは、組織のフォレンジックス能力の組織化に関するいくつかの側面を論じる。最初にフォレンジックスの多種多様な潜在的用途を示し、その後でフォレンジックスプロセスの概要を示す。続いて、フォレンジックスサービスの一般的な提供方法を論じ、フォレンジックス作業の実行に必要な技能の開発と維持に関するガイダンスを示す。このセクションではまた、一部のフォレンジック活動に、法律顧問や物理的セキュリティのスタッフなど、組織全体からさまざまなチームが参加する必要があることを説明する。このセクションの最後では、ポリシー、ガイドライン、および手続きにおいてどのようにフォレンジックスに対応するのか（役割と責任の規定、ツールと技法の適切な使用法に関するガイダンスの提供、情報システムライフサイクルへのフォレンジックスの取り込みなど）について論じる。

このガイドに示す技法とプロセスは、ディジタルフォレンジックスの原則に基づいている。*フォレンジックサイエンス*は、一般に、法律に科学的手法を適用することと定義されている。ディジタルフォレンジックスは、コンピュータ／ネットワークフォレンジックスとも呼ばれ、さまざまな定義がある。一般には、情報の完全性を保護し、データの厳密な保管引渡し管理を維持しながら、データの識別、収集、検査、および分析に科学的手法を適用することとみなされている。**組織によって従うべき法律や規制が異なるため、この文書を、ディジタルフォレンジック調査を行うための手引きとして使用したり、法的な助言として解釈したり、犯罪活動調査の根拠として使用したりするべきではない。代わりに、各組織は、法律顧問、法執行機関の当局者、および管理職層によって提供される広範囲の指導と併せて、フォレンジック能力を開発するための出発点としてこのガイドを使用するべきである。**

2.1 フォレンジックスの必要性

この 10 年間で、コンピュータ関連犯罪の件数が増加したことにより、法執行機関は犯罪に関わる人物、物件、場所、時期、および方法を特定するために、コンピュータベースの証拠を使用するようになり、その支援を目的とする企業や製品の増加にも拍車がかかった。その結果、コンピュータ犯罪の証拠データを法廷に適正に提示することを目的とするコンピュータ／ネットワークフォレンジックスが発達した。フォレンジックツールとフォレンジック技法は、ほとんどの場合、犯罪の調査やコンピュータセキュリティインシデント対応との関連で認識されている。その用途は、疑いのあるシステムを調査し、証拠を収集して保全し、事象を再構成し、事象の現在の状態を見極めることにより、事象に対応することである。しかし、フォレンジックツールやフォレンジック技法は、ほかにも次のような多くの種類の作業に利用することができる。

[3] この文書では、コンピュータという用語を、すべての計算装置、記憶装置、および周辺装置を指すものとして使用している。

- **運用上のトラブルシューティング**。フォレンジックツールとフォレンジック技法の多くは、運用上の問題のトラブルシューティングに適用できる。たとえば、ネットワーク構成に誤りのあるホストの仮想的または物理的な場所の特定、アプリケーションの機能的な問題の解決、ホストの OS やアプリケーションの現在の構成設定の記録と確認などに適用できる。

- **ログの監視**。各種のツールや技法がログの監視に役立つ。たとえば、ログエントリを分析したり、複数のシステムのあいだでログエントリの相互関係を示したりできる。これは、インシデント対応、ポリシー違反の識別、監査、およびそのほかの活動に役立つ可能性がある。

- **データ復旧**。偶発的または故意に削除または変更されたデータを含め、システムから消失したデータを復旧できるツールが数多く揃っている。復旧できるデータの量は、場合によって異なる。

- **データの取得**。一部の組織では、再配備または廃棄するホストからデータを取得するためにフォレンジックスツールを使用する。たとえば、あるユーザが組織を離れたときに、そのユーザのワークステーションからデータを取得し、将来必要になったときに備えて保存することができる。そのあとで、ワークステーションの媒体をサニタイズすることにより、元のユーザのデータをすべて削除できる。

- **注意義務／規制の遵守。**既存の規制や新たに出現する規制により、多くの組織は機密情報を保護し、監査のために一定の記録を保持することが求められる。また、保護されている情報が第三者に暴露された場合、各組織はほかの政府機関や影響を受ける個人に通知するように求められることもある。フォレンジックスは、各組織が注意義務を果たし、そのような要件を遵守するのに役立つ。

フォレンジックプロセスは、状況に関わらず、以下の基本的なフェーズで構成される[4]。

- **収集**。プロセスの最初のフェーズでは、データの完全性を保護するガイドラインと手続きに従いながら、関連するデータを識別し、ラベル付けし、記録し、ソースの候補から取得する。一般に、動的なデータ（現在のネットワーク接続など）や電池式の装置（携帯電話や PDA など）に含まれるデータは消失する可能性があるため、収集は適切なタイミングで行う。

- **検査**。検査では、データの完全性を保護しながら、収集した大量のデータを自動的手法と手動的手法の組み合わせを使ってフォレンジック的に処理することにより、特に注目に値するデータを見定めて抽出する。

- **分析**。プロセスの次のフェーズは、法的に正当と認められる手法および技法を使用して検査結果を分析することにより、収集と検査を行う契機となった疑問を解決するのに役立つ情報を導き出す。

- **報告**。最後のフェーズでは、分析結果を報告する。この報告には、使用された措置の記述、ツールと手続きの選択方法の説明、実行する必要があるそのほかの措置（追加のデータソースのフォレンジック検査、識別された脆弱性の安全対策、既存のセキュリティ管理策の改善など）の特定、フォレンジックプロセスのポリシー、ガイドライン、手続き、ツール、およびそのほかの側面の改善に関する推奨事項の提供などが含まれる可能性がある。報告フェーズをどの程度正式なものとするかは、状況によって大きく異なる。

[4] フォレンジックプロセスには多くのモデルがある。各モデルのフェーズは、正確には少しずつ異なるが、各モデルに反映されている基本原則や全体的な方法論は同じである。モデル間の主な違いは、プロセスの各フェーズの細分化レベルと個々のフェーズで使われる用語にある。このガイドに示すモデルは、各フェーズの簡単なとらえ方を提示する。各組織は、個々のニーズに最も適したフォレンジックモデルを選ぶべきである。

フォレンジックプロセスの詳細については、セクション 3 で説明する。セクション 4 からセクション 7 では、各種のフォレンジックデータの収集、検査、および分析の詳細について説明する。

2.2 フォレンジック要員の配置

コンピュータ／ネットワークフォレンジックスを行う能力は、ほぼすべての組織に必要である。このような能力を持たない組織は、組織のシステムやネットワークのなかでどのような事象（たとえば、保護されている機密データの露出など）が起きたかを特定するのが困難になる。この能力がどの程度必要かは、場合によって異なるが、組織におけるフォレンジックツールやフォレンジック技法の主な利用者は、通常、次の 3 つのグループに分けることができる[5]。

- **調査担当者。**組織内部の調査担当者は、ほとんどの場合、監察総監室（OIG：Office of Inspector General）に所属し、不正行為の疑惑を調査する責任を負う。一部の組織では、犯罪活動に関係している疑いがある事象の調査を OIG が直接引き受ける。通常、OIG はフォレンジックの技法やツールを数多く使用する。組織内部の調査担当者には、ほかに法律顧問や人事部門のメンバーなどが含まれることもある。法執行機関の当局者や犯罪調査を行う可能性がある組織外部の人間は、組織内部の調査担当者のグループに属するとみなされない。
- **IT 担当者**。このグループには、技術サポートスタッフや、システム、ネットワーク、およびセキュリティの各管理者が含まれる。IT 担当者は、日常業務（監視、トラブルシューティング、データ復旧など）のなかで、各自の専門分野固有の少数のフォレンジック技法およびツールを使用する。
- **インシデント対応担当者**。このグループは、不正なデータアクセス、システムの不適切な使用、悪意のあるコードへの感染、サービス運用妨害攻撃など、さまざまなコンピュータセキュリティインシデントに対応する。インシデント対応担当者は、通常、調査のなかで多種多様なフォレンジックの技法およびツールを使用する。

多くの組織は、フォレンジック作業の実行に自組織のスタッフと外部の者を併用する。たとえば、標準的な作業は内部で実行し、特別な支援が必要な場合にだけ外部の者を使用する組織もある。すべてのフォレンジック作業を内部で実行することを望む組織でも、通常は要求水準の高い作業は外注する。たとえば、物理的に破損した媒体を復元するためにデータ復旧会社に送ったり、例外的なソース（携帯電話など）からのデータ収集を法執行機関の専門職員やコンサルタントに任せたりする。このような作業には、通常、ほとんどの組織がその調達や維持に要する高い費用を正当化できないような、専用のソフトウェア、機器、施設、および技術的専門知識が必要である。3.1.2 項で説明するように、各組織は法執行機関の当局者によって行われるべき措置をあらかじめ決めておくべきである。また、訴訟手続きのために専門家の証言が必要な場合、各組織は外部の支援を求めることがある。

フォレンジックスの各側面を内部または外部のだれが取り扱うべきかを決める際には、次の要素に留意するべきである。

- **コスト。**潜在的なコストは数多く存在する。データの収集と検査に使用するソフトウェア、ハードウェア、および機器には、かなりのコスト（購入価格、ソフトウェアの更新とアップグレード、保守など）がかかる可能性があり、これらを改ざんから保護するために追加の物理的セキュリティ手段が必要になることもある。このほかの大きな費用には、スタッフのトレーニングやや作業のコストに関するものがある。専任のフォレンジックスの専門家については、こ

[5] フォレンジック活動を行う個人は、その属するグループに関係なく、フォレンジックの原則と実践事項を理解し、各活動の正しい手続きに従う必要がある。

のコストが特に大きい。一般に、ごくまれにしか必要とされないフォレンジック措置は、外部の者が行う方が費用対効果が高い可能性があるのに対し、頻繁に必要とされる措置は内部で行う方が費用対効果が高い可能性がある。

- **対処時間。**現場に常駐する職員は、現場に常駐していない職員より迅速にコンピュータフォレンジック活動を開始できる可能性がある。物理的な場所が地理的に分散している組織では、遠隔地にある施設の近くにいる非常駐の外注業者の方が組織の本部にいる職員より迅速に対応できる可能性がある。

- **データの機密性。**データの機密性とプライバシの懸念から、外部の者にハードディスクのイメージを取得させたり、データにアクセスできるそのほかの措置を実行させたりすることに前向きでない組織もある。たとえば、インシデントの痕跡を含むシステムに、保健医療情報、財務記録、そのほかの機密データが含まれていることもあり得る。データのプライバシを保護するために、そのシステムを組織の管理下に置くことが望ましい場合もある。一方、チーム内部にプライバシの懸念（たとえば、インシデント対応チームのメンバーがインシデントに関与している疑いなど）がある場合は、独立した第三者がフォレンジック措置を実行するのが望ましい。

フォレンジック作業を実行するインシデント対応担当者は、フォレンジックの原則、ガイドライン、手続き、ツール、技法だけでなく、データを隠蔽したり破壊したりできる反フォレンジックツールや反フォレンジック技法についても、妥当な範囲の総合的な知識をもつ必要がある。また、インシデント対応担当者にとっては、情報セキュリティや特定の技術的事柄（組織内で最もよく使われている OS、ファイルシステム、アプリケーション、ネットワークプロトコルなど）に関する専門知識を持つことも有益である。この種の知識を持つことにより、より迅速かつ効果的なインシデント対応が促進される。インシデント対応担当者は、システムとネットワークを全般的に幅広く理解することも必要である。これにより、特定のフォレンジック活動（たとえば、一般的でないアプリケーションのデータの検査や分析など）を対象とした技術的な専門知識の提供に適したチームや個人をすばやく特定できるようになる。

フォレンジックスを行う各個人は、場合によってはほかの種類の作業も実行する必要がある。たとえば、調査の結果が裁判所で使用される場合、インシデント対応担当者は、証言や、調査結果の裏付けを求められたりすることがある。インシデント対応担当者は、技術サポートスタッフ、システムやネットワークの管理者、およびそのほかの IT 担当者にフォレンジックスのトレーニングコースを提供することもある。たとえば、フォレンジックスのツールと技法の概要、特定のツールの使用に関する助言、新しい種類の攻撃の兆候などがトレーニングの主題として考えられる。インシデント対応担当者は、フォレンジックスツールに関する意見を聞き、既存のフォレンジックス能力の潜在的な不備を明らかにするために、IT 担当者のグループと対話する場を設けるのもよい。

インシデント対応チームでは、チームのいずれかのメンバーが欠けることでチームの機能に重大な影響が出ないように、チームの複数のメンバーが個々の一般的なフォレンジック活動を実行できるべきである。インシデント対応担当者は、フォレンジックツールの使用法やそのほかの技術や手続きについて、相互にトレーニングを行うことができる。実地訓練や、IT とフォレンジックに関する外部のトレーニングコースも、技能の開発と維持に役立つ可能性がある。さらに、チームのメンバーに新しいツールや技術のデモを見学させたり、実験環境でフォレンジックツールや反フォレンジックツールを実際に試したりするのが有益な場合もある。これは、インシデント対応担当者を携帯電話や PDA などの機器のデータの収集、検査、および分析に慣れさせるのに、特に有効である。インシデント対応担当者は、新しいフォレンジックの技術、技法、および手続きの動向を把握している必要がある。

2.3 ほかのチームとの交流

1 人の人間が組織のなかで使われるすべての技術（すべてのソフトウェアを含む）に精通することは、事実上不可能である。したがって、フォレンジック措置を行う個人は、追加的な支援を得るために必要に応じて組織内のほかのチームや個人と接触できるべきである。たとえば、特定のデータベースサーバが関係するインシデントへの対応は、そのデータベースの管理者が、背景となる事情を提供し、技術的な質問に回答し、データベースのマニュアルやそのほかの参考資料を提供する用意ができていれば、より効率的に行える可能性がある。各組織は、組織全体の IT 担当者、特にインシデント対応担当者やインシデントに最初に対応するそのほかの者が、フォレンジックスに関する自分の役割と責任を理解し、フォレンジック関連のポリシー、ガイドライン、および手続きに関するトレーニングや教育を継続的に受け、自分が責任を負う技術がインシデントやそのほかの事象に含まれる場合に、ほかの人と協力し、支援する準備ができているようにするべきである。

IT 担当者やインシデント対応担当者だけでなく、組織内のほかの人間も、主に非技術的な立場でフォレンジック活動に参加することが必要な場合がある。例としては、管理職層、法律顧問、人事担当者、監査員、物理的セキュリティスタッフなどが挙げられる。管理職層は、フォレンジック活動の支援、フォレンジックポリシーの審査と承認、および特定のフォレンジック措置（たとえば、ハードディスクからデータを収集するためにミッションクリティカルシステムを 6 時間オフラインにすることなど）の承認を行う責任を負う。法律顧問は、すべてのフォレンジックポリシーと高次のガイドラインおよび手続きを慎重に精査するべきであり、フォレンジック措置が確実に法律に従って行われるように、必要があれば追加のガイダンスを提供できる。人事部門は、職員との折衝の取り扱いや内部インシデントへの対応を支援できる。監査員は、フォレンジック活動のコストを含む、インシデントの経済的影響の判定を支援できる。物理的セキュリティスタッフは、証拠の取得や証拠の物理的保護を支援できる。これらのチームがフォレンジックプロセスにおいて際立った役割を果たすことはほとんどないが、これらのチームが提供するサービスは有益な場合がある。

チーム内のコミュニケーションを促進するため、各チームは 1 人以上の連絡窓口を指名するべきである。これらの人々は、チームの各メンバーが持つ専門知識を把握し、支援の問い合わせを適切な者に振り向ける。各組織は、適切なチームが必要に応じて参照できる連絡先リストを維持管理するべきである。このリストには、標準の連絡手段（職場の電話）と緊急の連絡手段（携帯電話）の両方を入れるべきである。

2.4 ポリシー

各組織は、法執行機関との連絡、監視の実行、フォレンジックのポリシー、ガイドライン、および手続きの定期的な見直しの実施など、フォレンジックに関する主要なすべての考慮事項に対応した明確な声明を組織のポリシーに確実に含めるようにするべきである。ポリシーは、高次においては、システムおよびネットワークの監視と調査を、許可された職員が正当な理由に基づき適切な条件の下で行うことを許可するべきである。各組織は、インシデント対応担当者やフォレンジックに関わる役割を持つそのほかの者に対して、独立のポリシーを持つこともできる。このポリシーによって、適切な振る舞いに関する、より詳細な規則が提供される。フォレンジックに関わる職員は、このポリシーを熟知し、理解しているべきである。ポリシーは、法律および規制の改定や新しい判決に伴って頻繁に更新しなければならない場合がある。多くの司法管区にまたがる組織の場合は特にそうである。さらに、組織のフォレンジックポリシーは、プライバシに対する適切な配慮に関するポリシーを含む、組織のほかのポリシーと矛盾がないようにするべきである。2.4.1 項から 2.4.3 項では、ポリシーに関連するトピックをさらに詳しく論じる。

2.4.1 役割と責任の規定

フォレンジックポリシーでは、組織のフォレンジック活動を実行または支援するすべての人々の役割と責任を明確に規定するべきである。これには、インシデント対応時に行う活動と日常業務（システム管理やネットワークのトラブルシューティングなど）の活動の両方が含まれるべきである。このポリシーには、フォレンジック活動に参加するすべての内部チーム（たとえば、2.3 項に示したチーム）と、法執行機関、外注業者、インシデント対応組織などの外部組織が含まれるべきである。このポリシーでは、さまざま条件下で誰がどの内部チームおよび外部組織と連絡を取るのかを明確に示すべきである。このポリシーではまた、司法管区の競合（犯罪が、複数の司法管区にまたがって行われた場合に、複数の法執行機関によって調査される可能性があること）について論じ、競合を解決する方法について説明するべきである。2.2 項に示したように、一部の組織には不正行為の疑いを調査する責任を負う監察総監室（OIG）がある。OIG は、司法管区の競合の解決にも適していると考えられる。一部の組織では、犯罪が行われた疑いがある場合に、OIG がその調査を直接引き受ける。

2.4.2 フォレンジックツールの使用に関するガイダンスの提供

インシデント対応担当者、IT 担当者（システムやネットワークの管理者など）、および組織内のほかの職員は、さまざまな理由でフォレンジックツールとフォレンジック技法を使用する。これらの技術には多くの利点があるが、偶然または故意に誤使用され、情報が不正にアクセスされたり、インシデントの証拠を含む情報が改変または破壊されたりする可能性もある。また、状況によっては、特定のフォレンジックツールの使用が正当化されないこともある（たとえば、軽微なインシデントは、何百時間もかけてデータの収集や検査を行う労力に値しない可能性がある）。

ツールが合理的かつ適切に使用されることを保証するには、組織のポリシー、ガイドライン、および手続きによって、さまざまな条件下で実行すべきフォレンジック活動と実行すべきでないフォレンジック活動を明確に説明するべきである。たとえば、ネットワーク管理者は、運用上の問題を解決するためにネットワーク通信を定期的に監視できるべきだが、明示的に許可されない限り、ユーザの電子メールを参照するべきではない。ヘルプデスクエージェントは、アプリケーションの問題を解決するために、あるユーザのワークステーションのネットワーク通信を監視する許可を与えられる一方で、ほかのネットワーク監視は許可されないことが考えられる。個人ユーザは、どのような状況においてもネットワーク監視の実施を禁止されるかもしれない。ポリシー、ガイドライン、および手続きでは、通常の状況（一般的な職務など）と特別な状況（インシデント対応など）の下で、該当する役割ごとに許可および禁止される具体的な活動を明確に規定するべきである。

ポリシー、ガイドライン、および手続きでは、反フォレンジックツールや反フォレンジック技法の使用法も取り扱うべきである。セクション 4 からセクション 7 で説明するように、反フォレンジックソフトウェアの目的は、データを隠蔽または破壊することによって、ほかの人がそのデータにアクセスできないようにすることである。反フォレンジックソフトウェアには、慈善事業に寄付する予定のコンピュータからデータを削除したり、ユーザのプライバシを保護するために Web ブラウザによってキャッシュされたデータを削除したりなど、建設的な用途が数多くある。しかし、フォレンジックツールと同様に、反フォレンジックツールも悪意のある理由で使用される可能性がある。したがって、各組織はこのようなツールの使用を誰にどのような状況で許可するかを規定するべきである。

フォレンジックツールは、機密情報を記録できるため、ポリシー、ガイドライン、および手続きにおいて、情報の必要な保護策も記載するべきである。また、インシデント対応担当者がパスワードや患者の医療情報を見た場合など、機密情報の偶発的な暴露の発生に対応するための要件も必要である。

2.4.3 情報システムライフサイクルにおけるフォレンジックスへの対応

多くのインシデントは、フォレンジックに関する考慮事項が情報システムライフサイクルに組み込まれていれば、より効率的かつ効果的に対応できる。このような考慮事項の例を以下に示す。

- システムの定期的なバックアップを実行し、以前のバックアップを一定期間保持すること。
- ワークステーション、サーバ、およびネットワーク装置の監査を可能にすること。
- 監査記録を集中管理された安全なログサーバに転送すること。
- 監査（認証の試みをすべて記録することを含む）を実行するようにミッションクリティカルアプリケーションを設定すること。
- 共通に配備される OS やアプリケーションのファイルに関してファイルハッシュのデータベースを維持し、特に重要な資産に対してファイル完全性チェックソフトウェアを使用すること。
- ネットワークとシステムの構成の記録（ベースラインなど）を維持すること。
- データ保持ポリシーを確立すること。これらのポリシーは、システムやネットワーク活動の履歴レビューの実施、継続中の訴訟や調査に関連するデータを保全するための要求または要件の遵守、および不要になったデータの破棄を支援する。

これらの考慮事項のほとんどは、組織のポリシーや手続きに含まれる既存の規定を拡張したものであるため、通常は集中管理されたフォレンジックスポリシーではなく、関連する個々の文書のなかで規定される。

2.5 ガイドラインと手続き

2.4 項で述べたように、各組織は組織のポリシー、インシデント対応の要員配置モデル、およびフォレンジック活動の参加者とみなされるそのほかのチームに基づいて、フォレンジック作業を実行するためのガイドラインと手続きを作成し、維持管理するべきである。活動が外部の者によって行われる場合でも、組織内部のスタッフはその外部の者とやり取りし、ある程度は活動に関与する。たとえば、外部の者に支援の必要を伝えたり、システムへの物理的または論理的なアクセスを許可したり、調査担当者が到着するまでインシデントの現場を保全する。内部スタッフは、外部の者と緊密に連携して、組織のポリシー、ガイドライン、および手続きが確実に理解され、遵守されるようにするべきである。

組織のフォレンジックガイドラインでは、想定されるあらゆる状況に合わせて調整された包括的な手続きを作成するのは現実的でないため、フォレンジックの技法を使ってインシデントを調査するための一般的な方法論を記載するべきである。ただし、各組織は、ハードディスクのイメージの取得や、揮発性情報のシステムからの捕捉と記録、物理的な証拠（リムーバブルメディアなど）の保全など、定型的な作業を実行するための手順を作成することも検討するべきである。これらのガイドラインと手順の目標は、一貫性のある効果的で正確なフォレンジック措置を可能にすることである。このことは、訴訟や内部の懲戒処分につながる可能性があるインシデントでは特に重要である。電子的なログやそのほかの記録は、改変または操作される可能性があるため、各組織はポリシー、ガイドライン、および手続きによってこのような記録の完全性を立証できるように備えておくべきである[6]。

[6] コンピュータセキュリティログの完全性を維持する方法の詳細については、NIST SP 800-92（草稿版）『*コンピュータセキュリティログ管理ガイド（Guide to Computer Security Log Management）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

情報のあり方は、すべての情報資産が電子的形態で存在する形に急速に移行しつつある。官民いずれのセクタにおいても、特定の措置や意志決定の実行、特定の情報項目の存在など、電子的記録の真正性、信用性、および信頼性を決定的に証明することがますます重要になっている。業務記録は、通常、業務そのものと同等に扱われてきた。法律やフォレンジックのコミュニティの一部では、電子的記録を簡単に作成、改変、または操作できることに対する懸念が高まっている。また、官民両セクタのコンプライアンスに関わるさまざまな取り組みにおいて、電子的記録の完全性を立証することの重要性がますます高まっている。このような問題は、弁護士および上級 IT 責任者と論じるべき問題であり、この文書の範囲を超えているため注意が必要だが、健全な、文書化された、合理的に説明できるフォレンジック技法とほかの手法（ログの維持と分析など）の組み合わせは、インシデント対応担当者だけでなく、意志決定者にとっても重要な手段である。

フォレンジックのガイドラインと手続きは、組織のポリシーと適用可能なすべての法律に矛盾しないようにするべきである。各組織は、ガイドラインと手続きの作成に、品質保証手段としての技術専門家と法律顧問を含めるべきである。管理職層も、ガイドラインと手続きの作成に関与し、特に、主要な意志決定項目がすべて文書化されていることや、一貫性のある方法で意志決定を行うための適切な方針が規定されていることを確認するべきである。

これらのガイドラインと手続きは、訴訟手続きにおける証拠能力の裏付けとなるべきである。これには、証拠の適切な収集と取り扱い、ツールや機器の完全性の保護、保管引渡し管理の維持、および証拠の安全な保管に関する情報が含まれる[7]。インシデントに対応して行われるすべての事象または措置を記録することは不可能かもしれないが、主な事象と措置の記録を取ることで、見過ごしがなくなり、インシデントへの対応方法をほかの人々に説明しやすくなる。この記録は、事例の管理、報告書の作成、および法廷での証言に役立つ。職員がインシデントに対応した日時（システムの復旧に要した時間を含む）の記録を保持することは、損害のコストを算定するのにも役立つ。また、フォレンジック面から見て適切な方法で証拠を取り扱うことにより、意志決定者は自信を持って必要な措置を取ることができる立場に置かれる。

ガイドラインや手続きを作成したら、それらの正確さが維持されるように管理することも重要である。管理職層は、ガイドラインと手続きを見直す頻度（一般には少なくとも年 1 回）を決めるべきである。チームのポリシー、ガイドライン、および手続きが大幅に変更されたときも、必ず見直しを行うべきである。ガイドラインや手続きが更新された場合は、以前のバージョンを将来の訴訟手続きでの使用に備えて保管しておくべきである。ガイドラインと手続きの見直しには、それらの作成に参加したチームが含まれるべきである。見直しの実施に加えて、各組織は特定のガイドラインや手続きの正確性を確認するのに役立つ訓練を実施することもある。

2.6 推奨事項

フォレンジック能力の確立と組織化に関する主な推奨事項を以下に示す。

- **各組織は、コンピュータ／ネットワークフォレンジックスを行う能力を持つこと。**フォレンジックスは、犯罪や不適切な行為の調査、コンピュータセキュリティインシデントの再構成、運用上の問題のトラブルシューティング、監査記録維持のための注意義務の支援、偶発的なシステム損傷からの復旧など、組織内のさまざまな職務で必要とされている。このような能力を持たない組織は、組織のシステムやネットワークのなかでどのような事象（たとえば、保護さ

[7] この文書では、法執行機関に課されるコンピュータ／ネットワークフォレンジックの要件は説明していない。法執行機関に対するコンピュータ／ネットワークフォレンジックの要件の詳細については、『Electronic Crime Scene Investigation: A Guide for First Responders』および『Forensic Examination of Digital Evidence: A Guide for Law Enforcement』を参照のこと。これらの文書は、いずれもhttp://www.ncjrs.gov/app/topics/topic.aspx?topicid=158で入手できる。

れている機密データの露出など）が起きたかを特定するのが困難になる。また、フォレンジック面から見て適切な方法で証拠を取り扱うことにより、意志決定者は自信を持って必要な措置を取ることができる立場に置かれる。

- **各組織は、フォレンジックスの各側面をどの関係者に対応させるかを決定すること。**ほとんどの組織は、フォレンジック作業の実行に自組織のスタッフと外部の者を併用する。各組織は、技能と能力、コスト、対応時間、およびデータの機密性に基づいて、どの関係者がどの作業に対応するべきかを決めるべきである。

- **インシデント対応チームは、しっかりとしたフォレンジック能力を持つこと。**チームの複数のメンバーが個々の一般的なフォレンジック活動を実行できるべきである。実地訓練や、IT とフォレンジックに関するトレーニングコースは、技能の開発と維持に役立つ可能性がある。新しいツールや技法のデモも同様である。

- **組織内の多くのチームがフォレンジックスに参加すること。**フォレンジック措置を行う各個人は、追加的な支援を得るために必要に応じて組織内のほかのチームや個人と接触できるべきである。フォレンジック活動を支援できるチームの例としては、IT 担当者、管理職層、法律顧問、人事担当者、監査員、物理的セキュリティスタッフなどが挙げられる。これらのチームのメンバーは、フォレンジックスにおける各自の役割と責任を理解し、フォレンジック関連のポリシー、ガイドライン、および手続きに関するトレーニングや教育を受け、フォレンジック措置に関してほかの人への協力と支援を提供できるように備えておくべきである。

- **フォレンジックに関する考慮事項をポリシーのなかで明確に取り扱うこと。**ポリシーは、高次においては、システムやネットワークの監視と調査を、許可された職員が正当な理由に基づき、適切な条件の下で行うことを許可するべきである。各組織は、インシデント対応担当者やフォレンジックに関わる役割を持つそのほかの者に対し、独立のフォレンジックポリシーを持つこともできる。このポリシーによって、適切な振る舞いに関する、より詳細な規則を提供する。フォレンジック活動への支援を求められる可能性がある者は、フォレンジックポリシーを熟知し、理解するべきである。ポリシーに関するそのほかの考慮事項を以下に示す。

  – フォレンジックポリシーでは、組織のフォレンジック活動を実行または支援するすべての人々の役割と責任を明確に規定するべきである。このポリシーでは、関係するすべての内部および外部の者を記載し、さまざま条件下で誰がどの関係者と連絡を取るのかを明確に示すべきである。

  – 組織のポリシー、ガイドライン、および手続きでは、通常の状況と特別な状況の下で実行すべきフォレンジック措置と実行すべきでないフォレンジック措置を明確に説明し、反フォレンジックツールや反フォレンジック技法も取り扱うべきである。ポリシー、ガイドライン、および手続きでは、機密情報の偶発的な暴露への対応も取り扱うべきである。

  – フォレンジックに関する考慮事項を情報システムライフサイクルに組み込めば、多くのインシデントに、より効率的かつ効果的に対応できるようになる可能性がある。この例として、ホストを対象とした監査の実施、システムやネットワーク活動の履歴レビューの実施を支援するデータ保持ポリシーの確立などがある。

- **各組織は、フォレンジック作業を実行するためのガイドラインと手続きを作成し、管理すること。**ガイドラインには、フォレンジック技法を使ってインシデントを調査するための一般的な方法論を記載し、順を追った手続きによる定型作業の実行方法を説明するべきである。これらのガイドラインと手続きは、訴訟手続きにおける証拠能力の裏付けとなるべきである。電子的なログやそのほかの記録は、改変または操作される可能性があるため、各組織はポリシー、ガイドライン、および手続きによってこのような記録の信頼性と完全性を立証できるよう

に備えておくべきである。また、これらのガイドラインと手続きを定期的に見直して、その正確さを維持するべきである。

（本ページは意図的に白紙のままとする）

3. フォレンジックプロセスの実行

フォレンジックスを行う最も一般的な目的は、注目すべき事象に関連する事実を発見して分析することにより、その事象をより深く理解することである。フォレンジックスは、2.1 項で説明したように、訴訟手続きや内部懲戒処分のための証拠の収集、マルウェアインシデントや運用上の特別な問題への対応など、多くの異なる状況で必要とされる可能性がある。フォレンジックスは、そのニーズに関係なく、図 3-1 に示す 4 フェーズのプロセスを使って行われるべきである。これらの各段階の詳細は、フォレンジックスに対する具体的なニーズに応じて異なる。組織のポリシー、ガイドライン、および手続きでは、標準的な手続きとの違いを示すべきである。

この項では、フォレンジックプロセスの基本フェーズである収集、検査、分析、および報告について説明する[8]。「収集」では、特定の事象に関連するデータの識別、ラベル付け、記録、および収集を行い、その完全性を保護する。2 番目のフェーズの「検査」では、収集されたデータの種類に適したフォレンジックツールやフォレンジック技法を実行することにより、データの完全性を保護しながら、収集されたデータから関連する情報を識別し、抽出する。「検査」では、自動化されたツールと手作業のプロセスを組み合わせて使用できる。次のフェーズの「分析」では、検査結果を分析することにより、収集と検査を行う契機となった疑問を解決するのに役立つ情報を導き出す。最後のフェーズでは、分析結果の「報告」を行う。この報告には、実行された措置の説明、実行する必要があるそのほかの措置の特定、フォレンジックプロセスのポリシー、ガイドライン、手続き、ツール、およびそのほかの側面の改善に関する勧告などが含まれる可能性がある。

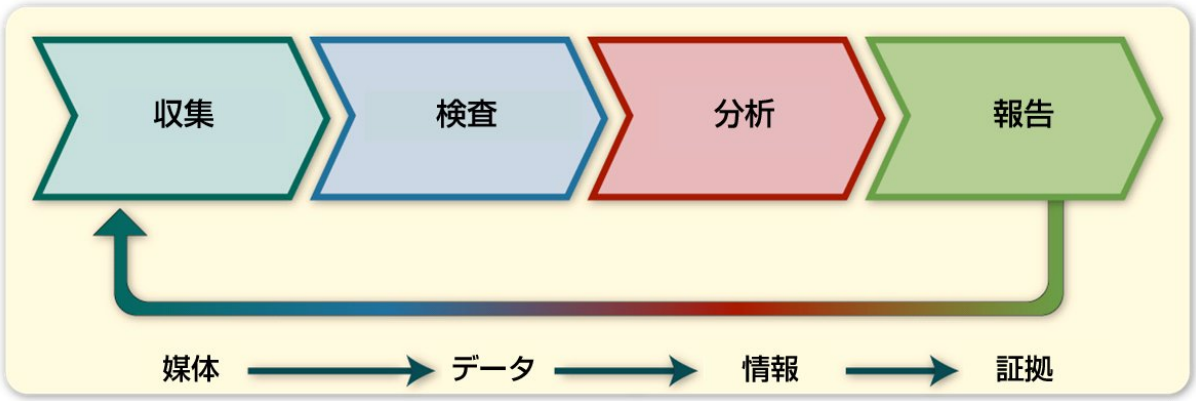

図 3-1. フォレンジックプロセス

図 3-1 の下部に示したように、フォレンジックプロセスでは、証拠が法執行のために必要なのか、組織の内部で使用するために必要なのかに関わらず、媒体を証拠に変換する[9]。具体的には、収集されたデータを検査する時点で最初の変換が行われる。この段階では、媒体からデータを抽出し、それをフォレンジックツールで処理できる形式に変換する[10]。次に、分析によってデータを情報に変換する。最後に、情報から証拠への変換は知識から行動への変換と似ており、分析によって得られた情報を報告フェーズにおいて 1 つ以上の方法で使用する。たとえば、特定の個人を起訴するための

---

8 2.1 項で説明したように、この文書に示すフォレンジックプロセスモデルは、フォレンジックプロセスの各フェーズの簡単なとらえ方を提示する。同じ基本原則や全体的な方法論を反映するフォレンジックプロセスモデルは、ほかにも数多く存在する。フォレンジックモデル間の主な違いは、プロセスの各フェーズの細分化レベルと、個々のフェーズで使われる用語にある。各組織は、個々のニーズに最も適したフォレンジックモデルを選ぶべきである。

9 法律の観点からみると、「*証拠*」という用語は、厳密には裁判官によって法廷への提出が認められた項目のみを指す。しかし、「*証拠*」という用語は一般にはもっと広い意味で使われており、この文書でも、より緩やかな「証拠」の定義を使用している。

10 ここでは、「*媒体*」という語はシステムとネットワークの両方を指す。

証拠として、何らかの行動を阻止または抑制するための実用的な情報として、または特定の事実の新しい手がかりを得るための知見として、情報を使用できる。

3.1 データの収集

フォレンジックプロセスの最初の段階は、データの潜在的なソースを識別し、それらのソースからデータを取得することである。3.1.1 項では、利用可能な各種のデータソースについて説明し、各組織がフォレンジックを目的とするデータの継続的な収集を支援するために取れる措置について論じる。3.1.2 項では、データの収集に関して推奨される手順を説明する。これには、訴訟や内部懲戒の手続きを支援するのに必要な追加的措置も含まれる。3.1.3 項では、インシデント対応に関する考慮事項について論じる。特に、収集されたデータの価値を、収集プロセスが組織に与えるコスト負担や影響に照らして検討することの必要性を強調する。

3.1.1 データソース候補の識別

業務上の用途と個人的な用途の両方で、ディジタル技術の使用範囲がますます広がったことにより、数多くのデータソースが出現した。最も明白かつ一般的なデータソースは、デスクトップコンピュータ、サーバ、ネットワーク記憶装置、およびノート型パソコンである。これらのシステムは、一般に、CD や DVD などの媒体が使用できる内蔵ドライブと、外部のデータ記憶媒体および装置を接続できる数種類のポート（USB：Universal Serial Bus、Firewire、PCMCIA：Personal Computer Memory Card International Association など）を備えている。データソースとなりうる外部記憶形態の例としては、USB ドライブ、メモリカード、フラッシュカード、光ディスク、磁気ディスクなどがある。標準的なコンピュータシステムには、一時的に（システムがシャットダウンまたは再起動されるまでのあいだ）利用できる揮発性のデータも含まれている。コンピュータ関連機器に加えて、多くの種類の携帯ディジタル機器（PDA、携帯電話、ディジタルカメラ、ディジタルレコーダ、ディジタルプレーヤなど）にも、データが含まれている可能性がある。分析担当者は、物理的な場所（オフィスなど）を調査し、データソースの候補を認識できるべきである[11]。

分析担当者は、ほかの場所にあるデータソース候補についても検討するべきである。たとえば、セクション 6 からセクション 7 で説明するように、通常、組織内にはネットワーク活動やアプリケーションの使用に関する情報のソースが数多く存在する。情報は、ほかの組織によっても記録されることがある（インターネットサービスプロバイダ（ISP：Internet service provider）のネットワーク活動のログなど）。分析担当者は、各データソースの所有者と、それがデータの収集に与える影響に留意するべきである。たとえば、ISP の記録のコピーを入手するには、一般に裁判所の命令が必要である。組織の施設内に置かれた外部所有資産（たとえば、職員が個人的に所有するノート型パソコンや請負業者のノート型パソコンなど）に関しては、分析担当者は組織のポリシーだけでなく法的な考慮事項にも留意するべきである。在宅勤務者のホームオフィスに置かれたコンピュータが関与するインシデントなど、組織の管理下にない場所が関与する場合は、状況がもっと複雑になることがある。一次的なデータソースからデータを収集することが事実上不可能な場合もある。したがって、分析担当者は、同じデータの一部または全部が存在する可能性がある代替データソースを把握し、入手できないソースの代わりに使用するべきである。

各組織は、フォレンジックに役立つと考えられるデータを収集するための先を見越した継続的な対応策を講じることができる。たとえば、5.1.1 項で説明するように、ほとんどの OS は、通常の運用の一環として監査を実行し、特定の種類の事象（認証の試みやセキュリティポリシーの変更など）を記録するように設定できる。監査記録からは、事象の発生時間や事象の発生源などの貴重な情報が

[11] フォレンジック措置は、組織内のさまざまな役割を持つ人々によって行われる可能性があるため、この文書では、一般に「分析担当者」という語をフォレンジック措置を行う個人の総称として使用している。

得られる[12]。もう 1 つの有効な措置は、集中管理されたログ機能を実装することである。これは、特定のシステムやアプリケーションが生成したログのコピーが中央の安全なログサーバに転送されることを意味する。集中管理されたログ機能により、無許可のユーザによるログの改ざんや反フォレンジック技法を使った分析の妨害が阻止される[13]。システムの定期的なバックアップを行うことにより、分析担当者は特定時点のシステムの内容を参照できるようになる。さらに、セクション 6 からセクション 7 で説明するように、侵入検知システム、ウイルス対策ソフトウェア、スパイウェア検知／削除ユーティリティなどのセキュリティ監視管理策は、攻撃や侵入が行われた時期と方法を示すログを生成できる。

データ収集に関する先を見越したもう 1 つの対応策は、特定のシステムのキーボードの使用を記録するキーストロークの監視など、ユーザの振る舞いの監視である。この対応策により、活動の貴重な記録が得られる可能性もあるが、組織のポリシーやログインバナーによってこのような監視が行われる可能性があることをユーザに知らせなければ、プライバシの侵害になる可能性もある。ほとんどの組織では、疑いのあるインシデントに関する追加情報を収集する場合を除き、キーストロークの監視などの技法は採用されない。このような監視を行う権限については、法律顧問と話し合い、組織のポリシーで明確に文書化するべきである。

3.1.2 データの取得

分析担当者は、潜在的なデータソースを識別したあと、それらのソースからデータを取得する必要がある。データの取得は、データ取得計画の策定、データの取得、および取得したデータの完全性の検証という、3 つの手順からなるプロセスを使って行われるべきである。以下の項目は、これら 3 つの手順の概要を示す。ただし、手順 2 と 3 の詳細は、取得するデータの種類に応じて異なる。4.2 項、5.2 項、6.3 項、および 7.3 項では、データファイル、OS データ、ネットワークトラフィックデータ、およびアプリケーションデータの取得と完全性の検証について、それぞれ詳しく説明する。

1. **データ取得計画を策定する。**ほどんどの場合、データソースの候補が複数存在するため、計画の策定は最初の重要な手順である。分析担当者は、データを取得する順序を確定し、ソースの優先順位を決める計画を作成するべきである。優先順位付けの重要な要素として、次のようなものがある。

   - **予想価値。**分析担当者は、状況に対する理解や同じような状況での過去の経験に基づいて、個々の潜在的データソースの相対的な予想価値を推定できるべきである。
   - **揮発性。***揮発性データ*とは、稼働中のシステム上に存在し、コンピュータの電源断や時間の経過に伴って消失するデータを指す。揮発性データは、システム上で実行されるほかの操作の結果として消失することもある。多くの場合、揮発性データの取得には、不揮発性データより高い優先順位が与えられるべきである。ただし、不揮発性データも、ある程度動的な場合がある（たとえば、新しい事象が発生するたびに上書きされるログファイルなど）。
   - **必要な労力。**データソースの取得に必要な労力は、データソースの種類によって大きく異なる可能性がある。この労力には、分析担当者や組織内のほかの人（法律顧問を含む）が費やす時間だけでなく、機器やサービスのコスト（外部の専門家など）も含まれる。

---

12 イベントの発生時にシステムの監査が有効でなかった場合、インシデント対応担当者は事象の発見後に監査を有効にして、継続している活動の証拠を記録しようとすることがある。これによってインシデントの証拠が改変されたり、攻撃者がインシデント対応担当者の存在に気づいたりする可能性があるため、監査を有効にした場合の影響を考慮するべきであり、インシデント対応担当者は各自の措置を文書化するべきである。

13 集中管理されたログの詳細については、NIST SP 800-92（草稿版）『*コンピュータセキュリティログ管理ガイド（Guide to Computer Security Log Management）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

たとえば、ネットワークルータからデータを取得するのに必要な労力は、ISP からデータを取得する場合に比べてかなり少ないと考えられる。

個々の潜在的なデータソースについて上記の 3 つの要素を考慮することにより、分析担当者は、データソース取得の優先順位付けに関する意志決定や取得すべきデータソースの判断を十分な情報に基づいて行うことができる。場合によっては、データを取得する対象となるデータソース候補があまりにも多く、そのすべてを取得するのが現実的でないこともある。各組織は、データソース取得の優先順位付けの複雑さを慎重に検討し、分析担当者が優先順位付けを効果的に実行するのに役立つ計画、ガイドライン、および手続きを文書として策定するべきである。

2. **データを取得する。**セキュリティツール、分析ツール、またはそのほかの手段によってデータをまだ取得していない場合、データ取得の一般的なプロセスでは、フォレンジックツールを使った揮発性データの収集、不揮発性データソースの複製による不揮発性データの収集、および元の不揮発性データソースの保全を行う。データの取得は、ローカルに、またはネットワーク経由で行うことができる。一般には、データの取得をローカルで行うほうが、システムやデータをよくコントロールできるため望ましいが、ローカルでのデータ収集がいつも可能だとは限らない（たとえば、システムが施錠された部屋やべつの場所にある場合など）。ネットワーク経由でデータを取得する場合は、収集するデータの種類と収集に投じる労力に関して意志決定を行うべきである。たとえば、異なるネットワーク接続を介して複数のシステムからデータを取得することが必要な場合もあれば、1 つのシステムから 1 つの論理ボリュームをコピーするだけで十分な場合もある。

3. **データの完全性を検証する。**データを取得したあとは、その完全性を検証するべきである。法律上の理由でデータが必要な場合には、データが改ざんされていないことを分析担当者が立証することが特に重要である。データの完全性の検証は、通常、ツールを使って元のデータとコピーされたデータのメッセージダイジェストを算出する作業と、2 つのメッセージダイジェストを比較して両者が同じであることを確認する作業からなる。

分析担当者がデータの収集を始める前に、将来の訴訟や内部懲戒の手続きにおけるデータの使用に対応する方法で証拠の収集と保全を行う必要性に関して、分析担当者または管理職層が（組織のポリシーや法律顧問の助言に従って）意志決定するべきである。必要性がある場合には、手違いや証拠改ざんの疑いが生じないように、明確に規定された保管引渡し管理に従うべきである。これには、証拠を物理的に引き渡されたすべての人の記録を保持すること、証拠を対象にして行われた活動とその時期を文書化すること、使われていない証拠を安全な場所に保管すること、証拠のコピーを作成し、検査や分析を行う際はコピーした証拠だけを使用すること、および元の証拠とコピーされた証拠の完全性を検証することが含まれる。証拠を保全する必要があるかどうか明確でない場合、一般には、特に規定されない限り、証拠は保全するべきである。

さらに、ほかにもいくつかの方策を講じるべきである。プロセス全体を通して、データを収集するために実行されたすべての手順の詳細なログを保持するべきである。これには、プロセスで使用された各ツールの情報も含まれる。文書化することにより、ほかの分析担当者があとで必要に応じてプロセスを繰り返すことができる。また、コンピュータの設定や周辺装置の視覚的な記憶を提供するため、証拠の写真を撮るべきである。さらに、システムに実際に触れる前に、分析担当者はモニタに表示されている画像、文書、実行中のプログラム、そのほかの関連情報のメモに残したり写真に撮ったりするべきである。スクリーンセーバが有効になっている場合は、スクリーンセーバがパスワードで保護されていることがあるので、そのことも文書化するべきである。可能な場合は、現場にいる誰か 1 人を証拠管理者に任命し、収集したすべての項目の写真撮影、文書化、およびラベル付けを行う権限と、行われたすべての措置とその措置を行った人、場所および時間を記録する単独の責

任を与えるべきである。証拠が長期間にわたって訴訟手続きで必要とされない場合もあるため、適切な記録文書を残すことにより、分析担当者はデータ収集のために行われた措置を正確に思い出すことができ、証拠の取り扱いに誤りがあったという主張への反論にも使用できる。

分析担当者による証拠収集を支援するために、フォレンジックワークステーション、バックアップ装置、空き媒体、証拠取り扱い用の支給品（ハードカバーのノート、保管引渡し管理用の記入用紙、証拠保管用のバッグやタグ、証拠テープ、ディジタルカメラ）など、必要なリソースを事前に準備するべきである。場合によっては、無許可での立ち入りや証拠の改ざんを防止するために、現場の物理的な保全を確実に行うようにする必要があるかもしれない。これは、物理的セキュリティスタッフの一員に部屋を警備させるだけで済む場合もある。また、法律上の理由で法執行機関の代表者がデータ収集を担当しなければならない状況もあり得る。これには、ISP の記録の入手や、外部のコンピュータシステムや例外的な装置および媒体からのデータの収集が含まれる（ただし、これらに限定されない）。各組織は、法律顧問の指導に基づいて、法執行機関の当局者がどのような種類のデータを収集するのが最適かを事前に定めておくべきである。

分析担当者は、収集されたデータに対して行われる措置を考慮し、潜在的な影響に備えて計画しておくべきである。場合によっては、法執行機関や検査と分析を行うほかの第三者にデータを引き渡すことがある。その結果、収集したハードウェアが長期間にわたって利用できなくなる可能性もある(第三者による検査と分析のため)。原本媒体を訴訟手続きのために保全しておく必要があれば、その媒体が何年間も利用できなくなることもある。もう 1 つの懸念は、調査に関係ない機密情報（医療記録や財務情報など）が、必要なデータとともに意図せずに確保されてしまう可能性があることである。

3.1.3 インシデント対応に関する考慮事項

インシデント対応中にフォレンジックスを行う場合に考慮すべき重要なことは、インシデントを封じ込める方法と時期である。システムやシステム内のデータの損害の拡大を防いだり、証拠を保全したりするには、関係するシステムを外部の影響から隔離しなければならない場合がある。多くの場合、分析担当者はインシデント対応チームと協力して、封じ込め（ネットワークケーブルの取り外し、電源の遮断、物理的セキュリティ対策の追加、ホストの正常なシャットダウンなど）に関する意志決定を行うべきである。この意志決定は、インシデントの封じ込めに関する既存のポリシーと手続き、およびインシデント対応チームがインシデントに伴うリスクに関して行った評価に基づいて行うべきである。これは、選択した封じ込め戦略またはその組み合わせによって、可能な場合は潜在的な証拠の完全性を維持しながら、リスクを十分に軽減するためである。

各組織は、さまざまな封じ込め戦略が組織の効果的な運営能力に及ぼす影響も事前に考慮するべきである。たとえば、ディスクのイメージやそのほかのデータを取得するために重要なシステムを数時間オフラインにすると、組織の必要な業務を遂行する能力に悪影響が出る可能性がある。停止時間が長引くと、組織にとって大きな財政的損失が発生する可能性がある。したがって、組織の業務の中断を最小限に抑えるように注意するべきである。

インシデントを封じ込めるためによく行われる処置の 1 つは、収集プロセスにおいてコンピュータの周囲を保護し、許可された個人だけに立ち入りを限定することにより、証拠が改ざんされないようにすることである。また、対象コンピュータにアクセスできるユーザは、パスワードや特定のデータのありかを示す情報を提供できる可能性があるため、これらのユーザ全員のリストを文書化するべきである。コンピュータがネットワークに接続されている場合は、コンピュータに接続されているケーブルを取り外すことで、リモートユーザによるコンピュータのデータの変更を防げる。コンピュータに無線ネットワーク接続が使われている場合は、外付けのネットワークアダプタをコンピュータから取り外すか、内蔵のネットワークアダプタを無効にすることで、ネットワーク接続を解除できる。どの方法も

使用できない場合は、コンピュータが使用している無線ネットワークアクセスポイントの電源を遮断することにより、同じ結果が得られるはずである。ただし、この方法の場合、調査対象外のユーザも日常業務を遂行できなくなる可能性がある。また、コンピュータの範囲内に複数のアクセスポイントが存在する可能性もある。一部の無線ネットワークアダプタは、一次アクセスポイントが使用できなくなったときに自動的にほかのアクセスポイントへの接続を試みるため、この方法でインシデントを封じ込めるためには、場合によっては複数のアクセスポイントの接続を解除する必要がある。

3.2 検査

データを収集したあとの次のフェーズは、データの検査である。このフェーズでは、収集したデータから関連する情報を評価して抽出する。このフェーズでは、データ圧縮、暗号化、アクセス制御メカニズムなど、データやコードの判読を困難にする OS やアプリケーションの機能を迂回または緩和しなければならない場合もある。取得したハードディスクドライブには、大量のデータファイルが含まれている可能性がある。ファイル圧縮やアクセス制御によって情報が隠蔽されているものも含め、注目すべきデータを含むデータファイルの識別は困難な作業になる可能性がある。また、注目すべきデータファイルに、フィルタ処理を必要とする無関係な情報が含まれることもある。たとえば、前日のファイアウォールのログに数百万件のレコードが保存されていたとしても、注目すべき事象に関連するレコードはそのうちの 5 件だけかもしれない。

幸い、各種のツールや技法を使って、選別しなければならないデータの量を減らすことができる。テキスト検索やパターン検索を使って、特定の主題や人物に言及している文書を見つけたり、特定の電子メールアドレスに対応する電子メールログエントリを特定したりなど、関連するデータを識別することができる。もう 1 つの有効な技法は、各データファイルの内容の種類（テキスト、グラフィック、音楽、圧縮されたファイルアーカイブなど）を特定できるツールを使用することである。データファイルの種類を知ることで、さらに調査する価値があるファイルを特定したり、検査の対象にならないファイルを除外したりできる。また、既知のファイルに関する情報を格納したデータベースも存在する。これらのデータベースを使って、さらに調査すべきファイルとそうでないファイルを選別することもできる。検査のツールと技法については、4.3 項、5.3 項、6.4 項、および 7.4 項で具体的に説明する。

3.3 分析

関連する情報を抽出したあと、分析担当者はデータから結論を導き出すためにデータの調査と分析を行うべきである[14]。フォレンジックスの基本は、体系的な手法を使って、入手可能なデータに基づいて適切な結論に達するか、または結論をまだ導き出せないと判断することである。分析には、人、場所、項目、および事象を識別することと、結論に達するためにそれらの要素がどのように関連するかを判断することが含まれる。多くの場合、この作業には複数のソースのデータを相互に関連付けることが含まれる。たとえば、ネットワーク侵入検知システム（IDS）のログの特定のイベントが特定のホストに結びついており、そのホストの監査ログのイベントが特定のユーザアカウントに結びつき、そのホストの IDS ログは、そのユーザが行った行為を示していたりする。集中管理されたログ機能やセキュリティ事象管理ソフトウェアなどのツールを使用して、データを自動的に収集して相互に関連付ければ、このプロセスを容易することができる。システムの特性を既知のベースラインと比較することにより、システムに加えられた各種の変更を識別できる。セクション 8 では、この分析プロセスについてさらに詳しく説明する。

3.1.2 項で説明したように、訴訟や内部懲戒処分で証拠が必要とされる場合、分析担当者は分析結果と行われたすべての処置を慎重に文書化するべきである。

---

[14] フォレンジックプロセスの方法論のなかには、検査フェーズのあとに独立した分析フェーズを持つものがある。この文書では、説明を簡潔にするため、分析を検査フェーズの一部として示す。通常、分析担当者はデータを検査し、そのデータの分析を行ったあと、最初の分析結果に基づいて追加の検査と分析を行う。

3.4 報告

最後のフェーズは報告である。報告は、分析フェーズによって得られた情報を準備して提示するプロセスである。報告には、以下を含め、多くの要素が影響する。

- **説明の選択肢。**事象に関する情報が不十分な場合は、発生したことを確定的に説明するまでに至らない可能性がある。事象に関する確定的と思えるような説明が複数ある場合、報告プロセスにおいてそれぞれの説明を十分に検討するべきである。分析担当者は、体系的な手法を使って、提案された各説明の立証または反証を試みるべきである。
- **対象への配慮。**データや情報の提示相手を知ることは、重要である。法執行機関の関与を必要とするインシデントには、収集されたすべての情報のきわめて詳細な報告が必要であり、場合によっては取得したすべての証拠データのコピーも必要である。システム管理者は、ネットワークトラフィックや関連する統計情報を特に細かく確認したいかもしれない。上級管理職層は、発生した事象の概要（たとえば、攻撃の発生方法を簡潔かつ視覚的に示したもの）と、同じようなインシデントを防止するために必要な措置だけを欲しがるかもしれない。
- **実用的な情報。**報告には、データから得られた実用的な情報を特定することも含まれる。分析担当者は、これらの情報から新しい情報のソースを収集できる可能性がある。たとえば、インシデントや犯罪に関する追加的な情報につながるかもしれない接触先のリストをデータから作成できる可能性がある。また、将来の事象を防止できる情報が得られる可能性もある。たとえば、将来の攻撃に使用される可能性があるシステム上のバックドア、犯罪の計画、ある時期に増殖を開始するように設定されたワーム、悪用される可能性がある脆弱性などの情報である。

分析担当者は、報告プロセスの一部として、ポリシーの不備や手続き上の誤りなど、是正する必要がある問題を明らかにするべきである。フォレンジックチームやインシデント対応チームの多くは、大きな事象の発生後に正式なレビューを開催する。このようなレビューでは、ガイドラインや手続きに関して考えられる改善について真剣な検討が行われる傾向があり、通常は各レビューのあとで少なくとも小規模な変更が承認され、実施される。たとえば、共通にみられる問題の 1 つは、多くの組織が、発生する可能性があるインシデントの種類ごとに連絡すべき職員の最新の連絡先リストを維持するのは、リソースに対する負担が大きいと認識していることである。ほかにも、調査時に収集されたギガバイト単位あるいはテラバイト単位のデータをどのように扱うべきか、また、将来の調査に役立つ追加的なデータを記録するためにセキュリティ管理策（監査、ログ、侵入検知など）をどのように変更できるかといった問題が共通にみられる。正式なレビューは、これらのプロセスの改善方法を明らかにするのに役立つ可能性がある。ガイドラインや手続きの変更が実施された場合は、チームのメンバー全員に対して、その変更を通知し、従うべき適切な手続きを頻繁に意識させるべきである。通常、チームには、変更を追跡し、各プロセスと手続きに関する文書の最新版を識別するための正式な仕組みがある。また、多くのチームでは、主な手順をチームに意識させるためのポスターやそのほかの目につきやすい文書を壁やドアに貼り、いつでも全員が作業の適切な実行方法を思い出せるようにしている。

明らかにされた問題の解決に加えて、分析担当者は各自の技能を維持および強化させるために他の処置も講じるべきである。一部のフォレンジック検査担当者は、各自の認証または認定を維持するために、常日頃からコンピュータ記憶媒体、データの種類や形式、およびそのほかの関連する問題に関する最新技術に対応した最新のツールや技法に関して自分自身をリフレッシュする必要がある。求められるかどうかに関係なく、セミナー、実地の職業経験、および学術的ソースを通して技能を定期的にリフレッシュすることは、フォレンジック措置を行う人々が急速に変化する技術や仕事上の責任に確実に追随するための助けになる。フォレンジックチームのメンバー全員が年 1 回の技

能試験に合格することを求める組織もある。ポリシー、ガイドライン、および手続きの定期的な見直しは、組織が技術の動向や法律の改定に確実に追随していくためにも役立つ。

3.5 推奨事項

このセクションに示したフォレンジックプロセスに関する主な推奨事項は、以下のとおりである。

- **各組織は、一貫性のあるプロセスを使ってフォレンジックスを実施すること。**このガイドでは、収集、検査、分析、報告の 4 つのフェーズからなるフォレンジックプロセスを示している。各フェーズの詳細は、フォレンジックスに対するニーズに応じて異なる可能性がある。

- **分析担当者は、データソース候補の範囲を認識すること。**分析担当者は、物理的な場所を調査し、データソースの候補を認識できるべきである。分析担当者は、組織の内部および外部のほかの場所にあるデータソース候補についても検討するべきである。分析担当者は、一次ソースからデータを収集するのが可能でない場合は、代わりのデータソースを使用できるように備えておくべきである。

- **各組織は、先を見越して有用なデータを収集すること。**OS に対する監査の設定、集中管理されたログ機能の実装、システムの定期的なバックアップの実行、およびセキュリティ監視管理策の使用によって、将来のフォレンジック活動に必要なデータのソースを生成することができる。

- **分析担当者は、標準的なプロセスを使ってデータの収集を行うこと。**このプロセスで推奨される手順は、データソースの識別、データ取得計画の策定、データの取得、および取得したデータの完全性の検証である。計画では、データの予想価値、データの揮発性、および必要な労力に基づいてデータを取得する順序を確定し、データソースの優先順位を決めるべきである。データの収集を始める前に、将来の訴訟や内部懲戒の手続きにおけるデータの使用に対応する方法で証拠の収集と保全を行う必要性に関して、分析担当者または管理職層が意志決定するべきである。必要性がある場合には、手違いや証拠改ざんの疑いが生じないように、明確に規定された保管引渡し管理に従うべきである。証拠を保全する必要があるかどうか明確でない場合、一般には、特に規定されない限り、証拠は保全するべきである。

- **分析担当者は、体系的な手法を使ってデータを調査すること。**フォレンジックスの基本は、分析担当者が体系的な手法を使って、入手可能なデータを分析することにより、入手可能なデータに基づいて適切な結論を導き出すか、または結論をまだ導き出せないと判断することである。訴訟や内部懲戒処分で証拠が必要とされる場合、分析担当者は分析結果と行われたすべての処置を慎重に文書化するべきである。

- **分析担当者は、各自のプロセスと実践事項を見直すこと。**現在および最近のフォレンジック措置の見直しは、ポリシーの不備、手続き上の誤り、および是正する必要があるそのほかの問題を識別し、組織が技術の動向や法律の変更に確実に追随していく上で役立つ可能性がある。

4. データファイルのデータの使用

データファイル（*ファイル*ともいう）は、論理的に 1 つのエンティティとしてまとめられ、一意の名前（*ファイル名*など）によって参照される情報の集まりである。ファイルのデータには、文書、画像、ビデオ、アプリケーションなど、数多くの種類がある。コンピュータ媒体のフォレンジック処理が成功するかどうかは、その媒体に存在するファイルを収集、検査、分析する能力に依存している。

このセクションでは、最も一般的な媒体の種類と*ファイルシステム*の概要（ファイルの命名、格納、編成、およびアクセスの方法）を示す。次に、ファイルの収集方法とファイルの完全性を保つ方法について論じる。このセクションでは、ファイルの復旧に関連するさまざまな技術的問題（削除されたファイルからのデータの復旧など）についても論じる。このセクションの最後の部分では、ファイルの検査と分析について説明し、分析担当者を支援するツールと技法に関するガイダンスを提供する[15]。

4.1 ファイルの基本

分析担当者は、ファイルの収集や検査を試みる前に、ファイルとファイルシステムについて妥当な範囲で総合的な理解を有しているべきである。まず、分析担当者はファイルが格納されている可能性のある各種の媒体を認識しているべきである。4.1.1 項では、パソコンやそのほかの種類のディジタル機器で使用される媒体の例をいくつか示す。また、4.1.2 項では、ファイルを整理するためにファイルシステムがどのように使われているのかを説明し、いくつかの一般的なファイルシステムの概要を示す。4.1.3 項では、削除されたファイルのデータがファイルシステム内にどのように残存するかを論じる。

4.1.1 ファイルの格納媒体

コンピュータやそのほかのディジタル機器が広く普及したことにより、ファイルを格納するために使われる媒体の種類も大幅に増加した。従来からあるハードディスクドライブやフロッピーディスクなどの媒体に加えて、家庭用機器（PDA や携帯電話など）や新しい媒体（ディジタルカメラによって普及したフラッシュメモリカードなど）にも、ファイルが格納されることが多くなった。表 4-1 に、コンピュータやディジタル機器でよく使われる媒体の種類を示す。このリストは、現在利用可能な媒体の種類を網羅するものではなく、分析担当者が目にする可能性がある媒体の多様性を示すことを目的としている。

[15] 検査と分析の詳細については、http://www.ncjrs.gov/pdffiles1/nij/199408.pdfにある『*Examination of Digital Evidence: A Guide for Law Enforcement*』を参照のこと。

表 4-1. よく使われる媒体の種類

媒体の種類	読み取り装置	一般的な容量[16]	注釈
主にパソコンで使われるもの			
フロッピーディスク	フロッピーディスクドライブ	1.44 MB（メガバイト）	3.5 インチディスク。使われなくなりつつある。
CD-ROM	CD-ROMドライブ	650 MB～800 MB	追記型（CD-R）ディスクと書き換え可能（CD-RW）ディスクを含む。最もよく使われる媒体。
DVD-ROM	DVD-ROMドライブ	1.67 GB（ギガバイト）～15.9 GB	単層および 2 層の追記型（DVD±R）ディスクと書き換え可能（DVD±RW）ディスクを含む。
ハードディスクドライブ	該当せず	20 GB～400 GB	多くのファイルサーバでは、大容量のドライブが使用される。
Zip ディスク	Zipドライブ	100 MB～750 MB	フロッピーディスクより容量が大きい。
Jaz ディスク	Jazドライブ	1 GB～2 GB	Zip ディスクと似ているが、現在は製造されていない。
バックアップテープ	互換性のあるテープドライブ	80 MB～320 MB	多くは音楽用のカセットテープに似ている。環境条件の影響を受けてやや破損しやすい。
光磁気（MO）ディスク	互換性のある MOドライブ	600 MB～9.1 GB	5.25 インチディスク。バックアップテープより環境条件の影響を受けにくい。
ATA（Advanced Technology Attachment）フラッシュカード	PCMCIA スロット	8 MB～2 GB	PCMCIA フラッシュメモリカード。大きさは 85.6×54×5 mm。
多くの種類のディジタル機器で使われるもの			
USB（フラッシュ）ドライブ	USB インタフェース	16 MB～2 GB	その大きさから「thumb drive（親指ドライブ）」とも呼ばれる。
CompactFlash カード	PCMCIA アダプタまたはメモリカードリーダ	16 MB～6 GB	Type I カードの大きさは 43×36×3.3 mm。Type II カードの大きさは 43×36×5 mm。
Microdrive	PCMCIA アダプタまたはメモリカードリーダ	340 MB～4 GB	インタフェースとフォームファクタは、CompactFlash Type II カードと同じ。
MMC（MultiMediaCard）	PCMCIA アダプタまたはメモリカードリーダ	16 MB～512 MB	大きさは 24×32×1.4 mm。
SD（Secure Digital）カード	PCMCIA アダプタまたはメモリカードリーダ	32 MB～1 GB	SDMI（Secure Digital Music Initiative）の要件に適合する。ファイル内容のデータ暗号化機能が組み込まれている。フォームファクタは、MMC とほぼ同じ。
メモリースティック	PCMCIA アダプタまたはメモリカードリーダ	16 MB～2 GB	メモリースティック（50×21.5×2.8 mm）、メモリースティック Duo（31×20×1.6 mm）、メモリースティック PRO、メモリースティック PRO Duo がある。一部は SDMI の要件に適合し、ファイル内容のデータ暗号化機能が組み込まれている。
SmartMedia カード	PCMCIA アダプタまたはメモリカードリーダ	8 MB～128 MB	大きさは 37×45×0.76 mm。
xD ピクチャーカード	PCMCIA アダプタまたは xD ピクチャーカードリーダ	16 MB～512 MB	現在は富士フィルムとオリンパスのディジタルカメラでのみ使用されている。大きさは 20×25×1.7 mm。

[16] 技術の進歩とコストの減少により、多くの媒体の種類では最大容量がしだいに増加している。

4.1.2 ファイルシステム

通常、媒体にファイルを格納するには、その媒体をパーティションで区切ってフォーマットすることにより、論理ボリュームを作成する必要がある。*パーティション*の作成は、媒体を物理的に独立した単位として機能する部分に論理的に分割する行為である。*論理ボリューム*は、ファイルシステムとしてフォーマットされ、1 つのエンティティとして機能するパーティションまたはパーティションの集まりである。一部の種類の媒体（フロッピーディスクなど）には、1 つのパーティション（したがって、1 つの論理ボリューム）しか入れることができない。論理ボリュームの形式は、選択されたファイルシステムによって決まる。

*ファイルシステム*は、論理ボリューム上のファイルを命名、格納、編成、およびアクセスする方法を規定する。多くの異なるファイルシステムが存在し、それぞれ固有の機能とデータ構造を備えているが、すべてのファイルシステムに共通する特徴もある。1 つは、ディレクトリとファイルという概念を使用してデータの編成と格納が行われる点である。*ディレクトリ*は、ファイルをグループにまとめるために使われる組織的構造である。ディレクトリには、ファイルに加えて、*サブディレクトリ*と呼ぶ他のディレクトリを入れることもできる。もう 1 つは、ファイルシステムでは媒体上のファイルの場所を示すために、なんらかのデータ構造を使う点である。また、ファイルシステムでは、各データファイルは、媒体上の 1 つ以上の*ファイルアロケーションユニット*に書き込まれる。ファイルアロケーションユニットは、FAT(File Allocation Table: ファイルアロケーションテーブル)や NTFS(NT File System: NT ファイルシステム)などのファイルシステムではクラスタと呼ばれ、UNIX や Linux などのシステムではブロックと呼ばれる。

以下に、よく使われるファイルシステムをいくつか示す。

- **FAT12**[17]**。**FAT12 は、フロッピーディスクと 16 MB 未満の FAT ボリュームにのみに使われている。FAT12 では、12 ビットのファイルアロケーションテーブルエントリを使ってファイルシステム内のエントリのアドレスが指定される。

- **FAT16。**MS-DOS、Windows 95／98／NT／2000／XP、Windows Server 2003、および一部の UNIX OS は、FAT16 をネイティブにサポートする。FAT16 は、ディジタルカメラやオーディオプレーヤなどのマルチメディア機器でもよく使われている。FAT16 では、16 ビットのファイルアロケーションテーブルエントリを使ってファイルシステム内のエントリのアドレスが指定される。MS-DOS および Windows 95／98 では、FAT16 ボリュームの最大サイズは 2 GB に制限される。Windows NT 以降の OS では、FAT16 ボリュームの最大サイズは 4 GB に増加している。

- **FAT32**[18]**。**Windows 95 OEM（Original Equipment Manufacturer）Service Release 2（OSR2）、Windows 98／2000／XP、および Windows Server 2003 は、FAT32 をネイティブにサポートしており、一部のマルチメディア機器も同様である。FAT32 では、32 ビットのファイルアロケーションテーブルエントリを使ってファイルシステム内のエントリのアドレスが指定される。FAT32 ボリュームの最大サイズは 2 TB（テラバイト）である。

- **NTFS。**Windows NT／2000／XP および Windows Server 2003 は、NTFS をネイティブにサポートする。NTFS は、*回復可能なファイルシステム*である。つまり、エラーの発生時にファイルシステムの一貫性を自動的に回復できる。また、NTFS はデータの圧縮と暗号化をサポ

[17] FAT12 および FAT16 の詳細については、http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/c13621675.mspxを参照のこと。

[18] FAT32 ファイルシステムの仕様は、FAT32 に関する高度に技術的な詳細情報を提供するもので、http://www.microsoft.com/whdc/system/platform/firmware/fatgen.mspxからダウンロードできる。

ートし、データファイルとディレクトリに対してユーザレベルおよびグループレベルのアクセス許可を設定できる[19]。NTFS ボリュームの最大サイズは 2 TB である。

- **HPFS（High-Performance File System）。**HPFS は、OS/2 でネイティブにサポートされており、Windows NT 3.1、3.5、および 3.51 で読み取りが可能である。HPFS は、FAT のディレクトリ編成を基盤にしており、ディレクトリの自動ソート機能を提供する。また、HPFS では、より小さいアロケーション単位を利用することにより、無駄になるディスク領域を減らしている。HPFS ボリュームの最大サイズは 64 GB である。

- **ext2fs（Second Extended Filesystem）**[20]**。**ext2fs は、Linux でネイティブにサポートされている。ext2fs は、ファイルシステムの一貫性を保証するため、標準の UNIX ファイル形式とファイルシステムチェックをサポートしている。ext2fs ボリュームの最大サイズは 4 TB である。

- **ext3fs（Third Extended Filesystem）。**ext3fs は、Linux でネイティブにサポートされている。ext2fs ファイルシステムをベースとし、大量のデータに対してファイルシステムの一貫性チェックをすばやく実行できるジャーナリング機能を備えている。ext3fs ボリュームの最大サイズは 4 TB である。

- **ReiserFS**[21]**。**ReiserFS は、Linux でサポートされ、Linux のいくつかの代表的なバージョンにおけるデフォルトのファイルシステムである。ジャーナリング機能を備え、ext2fs ファイルシステムや ext3fs ファイルシステムよりもかなり高速に動作する。最大ボリュームサイズは 16 TB である。

- **HFS（Hierarchical File System）**[22]**。**HFS は、Mac OS でネイティブにサポートされている。HFS は、主に Mac OS の古いバージョンで使われているが、新しいバージョンでもまだサポートされている。Mac OS 6 および 7 における HFS ボリュームの最大サイズは、2 GB である。Mac OS 7.5 における HFS ボリュームの最大サイズは、4 GB である。7.5.2 以降の Mac OS では、HFS ボリュームの最大サイズは 2 TB に増加している。

- **HFS+**[23]**。**HFS+は、Mac OS 8.1 以降でネイティブにサポートされ、Mac OS X ではジャーナリングファイルシステムである。HFS の後継であり、長いファイル名のサポートや各国語によるファイル名を可能にする Unicode ファイル名のサポートなど、数多くの機能拡張が行われている。HFS+ボリュームの最大サイズは 2 TB である。

- **UFS（UNIX File System）**[24]**。**UFS は、Solaris、FreeBSD、OpenBSD、Mac OS X など、数種類の UNIX OS でネイティブにサポートされている。しかし、ほとんどの OS は独自の機能を追加しているため、UFS の詳細は実装ごとに異なる。

- **CDFS（Compact Disk File System）。**名前からわかるように、CDFS ファイルシステムは CD で使われている。

- **ISO（International Organization for Standardization）9660 および Joliet。**ISO 9660 ファイルシステムは、CD-ROM でよく使われている。よく使われるもう 1 つの CD-ROM ファイルシステムは、ISO 9660 のバリエーションである Joliet である。ISO 9660 が最大 32 文字までの

---

19 NTFS のそのほかの機能については、http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/c13621675.mspxを参照のこと。

20 ext2fs の詳細については、http://e2fsprogs.sourceforge.net/ext2.htmlを参照のこと。

21 ReiserFS とその後継である Reiser4 の詳細については、http://www.namesys.com/を参照のこと。

22 HFS の概要については、http://developer.apple.com/documentation/mac/Files/Files-17.htmlを参照のこと。

23 HFS+の概要とその実装の技術的詳細については、http://developer.apple.com/technotes/tn/tn1150.htmlを参照のこと。

24 UFS の概要については、http://en.wikipedia.org/wiki/Unix_File_Systemを参照のこと。

ファイル名をサポートするのに対し、Joliet は最大 64 文字までサポートする。Joliet は、Unicode 文字を含むファイル名もサポートする。

- **UDF（Universal Disk Format）。**UDF は、DVD で使われているファイルシステムであり、一部の CD でも使われている。

4.1.3 媒体上のそのほかのデータ

4.1.2 項で説明したように、ファイルシステムの目的は、媒体上にファイルを格納することである。しかし、ファイルシステムには削除されたファイルのデータや既存のファイルの古いバージョンのデータも保持されている。これらのデータには、重要な情報が含まれている可能性がある（4.2 項では、このような種類のデータを収集する技法について論じる）。以下の項目は、これらのデータが各種の媒体にどのように残りうるかを説明したものである。

- **削除されたファイル。**ファイルを削除すると、通常は媒体からファイルは消去されず、そのファイルの場所を指すディレクトリのデータ構造内の情報に削除のマークが付けられる。これは、そのファイルが媒体にまだ格納されているが、OS によって列挙されなくなることを意味する。オペレーティングシステムは、これを空き領域とみなし、削除されたファイルの一部または全体をいつでも上書きできる。

- **スラック領域。**すでに言及したように、ファイルシステムはファイルアロケーションユニットを使ってファイルを格納する。ファイルに必要な領域がファイルアロケーションユニットのサイズより小さい場合でも、ファイルアロケーションユニット全体がそのファイルのために予約される。たとえば、ファイルアロケーションユニットのサイズが 32 KB（キロバイト）で、ファイルがわずか 7 KB だった場合、32 KB 全体がそのファイルに割り当てられるが、使用されるのは 7 KB だけなので、結局 25 KB が未使用領域となる。この未使用領域を*ファイルスラック領域*と呼び、削除されたファイルの一部などの残存データが保持されている可能性がある。

- **空き領域。***空き領域*は、媒体上のどのパーティションにも割り当てられていない領域であり、未割り当てのクラスタ（ブロック）を含んでいる。ここには、ある時点でファイル（およびボリューム全体）が存在し、そのあと削除された可能性がある媒体上の領域が含まれることが多い。空き領域には、データの一部がまだ含まれている可能性がある。

データが隠される可能性があるもう 1 つの形態は、NTFS ボリューム内の代替データストリーム（ADS：Alternate Data Streams、以下 ADS と称す）による方法である。NTFS は、長いあいだ、ファイルやディレクトリに対する複数のデータストリームをサポートしている。NTFS ボリューム内の各ファイルは、ファイルの一次データを格納するために使われる無名ストリームと、必要に応じて補助的な情報（ファイルのプロパティや画像のサムネイルデータなど）を格納するために使用できる 1 つ以上の名前付きストリーム（file.txt:Stream1、file.txt:Stream2 など）で構成される[25]。たとえば、ユーザが Windows Explorer でファイルを右クリックしてファイルのプロパティを表示し、［概要］タブに表示された情報を変更すると、OS はそのファイルの概要情報を名前付きストリームに格納する。

ファイル内のすべてのデータストリームは、そのファイルの属性（タイムスタンプやセキュリティ属性など）を共有する。名前付きストリームはファイルの格納クォータ（制限容量）に影響するが、Windows の標準的なファイルユーティリティ（Explorer など）ではファイルの無名ストリームのサイズだけが報告されるため、名前付きストリームの大部分はユーザから隠蔽されている。この結果、ユーザは Windows の標準的なファイルユーティリティを使ってファイルに ADS があるかどうかをすぐに確認することができない。このため、NTFS ファイルシステム内に隠れデータが含まれている可能性がある。ADS を含むファイルを NTFS 以外のファイルシステムに移動すると、ADS はファイルか

[25] ディレクトリは、無名ストリームを持たないが、名前付きストリームを含むことがある。

ら事実上取り除かれるため、分析担当者が ADS の存在に気づかないと、ADS が失われる可能性がある。ADS を識別するためのソフトウェアやプロセスが公開されている[26]。

4.2 ファイルの収集

データ収集では、分析担当者は関連するファイルやファイルシステムの複数のコピー（通常はマスタコピーと作業用コピー）を作成するべきである[27]。これにより、分析担当者は元のファイルやマスタコピーに影響を与えることなく作業用コピーを使用できる。4.2.1 項では、媒体からファイルや残存ファイルデータをコピーするための主な技法やツールについて説明する。4.2.2 項では、ファイルの完全性を維持することの重要性を論じ、完全性の保護や検証を支援するハードウェアおよびソフトウェアに関するガイダンスを提供する。多くの場合、ファイルだけでなく、ファイルの重要なタイムスタンプ（ファイルの最終更新時間やアクセス時間など）も収集することが重要である。4.2.3 項では、タイムスタンプとその保全方法について説明する。4.2.4 項では、ファイルの収集に関するそのほかの技術的問題（隠しファイルの発見方法や RAID（redundant array of inexpensive disks）実装からのファイルのコピー方法など）を取り扱う。

4.2.1 媒体からのファイルのコピー

媒体からファイルをコピーするときは、次の 2 つの異なる技法を使用できる。

- **論理バックアップ**。*論理バックアップ*は、論理ボリュームのディレクトリとファイルをコピーする。媒体上に存在する可能性があるほかのデータ（削除されたファイルやスラック領域に格納された残存データなど）は捕捉されない。
- **ビットストリームイメージの取得。***ビットストリームイメージの取得*は、*ディスクイメージの取得*ともいい、元の媒体の空き領域やスラック領域も含むビット単位のコピーを生成する。ビットストリームイメージの取得には、論理バックアップより多くの格納領域と実行時間が必要である。

訴訟や内部懲戒処分で証拠が必要とされる場合、分析担当者は元の媒体のビットストリームイメージを取得し、元の媒体にラベル付けし、それを証拠として確実に保管するべきである。元の媒体が改変されないようにするとともに、元の媒体のコピーを必要に応じていつでも再作成できるようにするために、以降の分析はすべてコピー先の媒体を使って行うべきである。イメージのコピーを作成するために行われたすべての手順を文書化するべきである。それにより、どの分析担当者も同じ手続きを使って元の媒体の正確な複製を作成できるようになる。また、書面による記録を適切に行っておけば、収集プロセスで証拠の取り扱いに誤りがなかったことを証明できる。分析担当者は、イメージを記録するために行われた手順とは別に、ハードディスクドライブのモデルとシリアル番号、媒体の格納容量、イメージの取得に使われたソフトウェアやハードウェアに関する情報（名前、バージョン番号、ライセンス情報）などの補足情報を文書化するべきである。これらの措置は、いずれも引き渡し管理を支える。

ビットストリームイメージの取得を行うときは、ディスクーディスクコピーまたはディスクーファイルコピーを実行できる。*ディスクーディスクコピー*は、その名前が示すように、媒体の内容を別の媒体に直接コピーする。*ディスクーファイルコピー*は、媒体の内容を 1 つの論理的なデータファイルにコピーする。ディスクーディスクコピーは、コピー先の媒体をコンピュータに直接接続してその内容をすぐに

---

[26] ADS の詳細については、http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/c13621675.mspx、http://www.infosecwriters.com/texts.php?op=display&id=53、および http://www.heysoft.de/Frames/f_faq_ads_en.htm を参照のこと。

[27] マスタコピーの目的は、1 つ目の作業用コピーが改変やそのほかの理由で使用できなくなった場合に備えて、追加の作業用コピーを作成することである。

参照できるので便利である。ただし、ディスクーディスクコピーでは、元の媒体と同等の媒体がもう 1 つ必要になる[28]。ディスクーファイルコピーでは、データファイルのイメージを簡単に移動してバックアップできる。ただし、分析担当者がイメージファイルの論理的内容を参照するには、イメージを媒体に復元するか、またはビットストリームイメージの論理的内容を表示する機能を持つアプリケーションで開くか読み取る必要がある。その詳細は、OS やフォレンジックスツールによって異なる。4.3 項では、このプロセスについてさらに詳しく説明する。

ビットストリームイメージの取得や論理バックアップを実行できるハードウェアおよびソフトウェアのツールは数多く存在する。ハードウェアツールは、一般に持ち運び可能で、ビット単位でのイメージ取得機能を提供し、イメージを取得する対象となるドライブまたはコンピュータに直接接続でき、ハッシュ機能を内蔵している[29]。ハードウェアツールは、IDE（Integrated Drive Electronics）や SCSI（Small Computer System Interface）などの一般的な種類のコントローラを使用するドライブからデータを取得できる。ソフトウェアソリューションは、一般に、イメージを取得する対象となる媒体が接続されているワークステーション上で実行される起動ディスク、CD、またはインストール済みプログラムで構成される[30]。ソフトウェアソリューションには、ファイルまたはパーティションの論理的なコピーを作成し、ドライブの空き領域や未割り当て領域を無視する可能性があるものと、媒体のビット単位のイメージコピーを作成するものがある。

一部のディスクイメージ取得ツールは、その主要機能に加えて、自動化された監査証跡や保管引渡し管理などのフォレンジック記録機能も実行できる。このようなツールを使用することにより、検査プロセスの一貫性や結果の正確さと再現性を裏付けることができる。入手可能なディスクイメージ取得ツールの数は、ますます増えつつある。このようなツールの増加とツールを検査する標準の欠如に対応して、NIST のコンピュータフォレンジックスツール検査（CFTT：Computer Forensics Tool Testing）プロジェクトが、ツールの結果の有効性を確認するための厳格な検査手続きを策定した。現時点では、CFTT の検査を受けたディスクイメージ取得ツールの数はごくわずかである[31]。

一般に、ビットストリームイメージの取得を行うツールを使って、*稼働中のシステム*（現在使用中のシステム）から物理的な装置全体のビット単位のコピーを取得するべきではない。これは、そのようなシステム上のファイルやメモリは絶え間なく変化しており、それらの有効性を確認できないためである[32]。しかし、稼働中のシステムでも、論理的な領域のビット単位のコピーを作成して、その有効性を確認することは可能である。ただし、論理バックアップの実行する場合でも、稼働中のシステムからファイルをコピーしない方が望ましい。バックアップ中に、ファイルに変更が加わる可能性があり、プロセスによって開かれた状態のファイルは簡単にコピーできない可能性がある。したがって、分析担当者は、どのファイルを取得する必要があるか、コピーをどの程度正確かつ完全なものにする必要があるか、および稼働中のシステムがどの程度重要かに基づいて、稼働中のシステムからファイル

---

28 コピーを実行する前に、コピー先の媒体をフォレンジック的にクリーンにすることにより、媒体上の既存のデータを消去しておくべきである。コピー先の媒体は、コピー元のデータより格納容量が大きいものにするべきである。

29 ハードウェアベースのディスクイメージ取得ツールの例としては、Image MASSter の SOLO Forensics（http://www.ics-iq.com/）や Logicube の Solitaire（http://www.logicube.com/）などがある。そのほかの製品については、付録 F に示した Web サイト（たとえば、TUCOFS：The Ultimate Collection of Forensics Software（http://www.tucofs.com/tucofs/tucofs.asp?mode=filelist&catid=10&oskey=12）など）を参照のこと。**この文書に示すアプリケーション群は、フォレンジックに使用されるアプリケーションの網羅的な一覧ではない。また、この文書で特定の製品を暗に推奨しているわけでもない。**

30 ソフトウェアベースのディスクイメージ取得ツールの例としては、Linux の dd、SafeBack（http://www.forensics-intl.com/safeback.html）、EnCase（http://www.encase.com/）、Norton Ghost（http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=br&pvid=ghost10）、ILook（http://www.ilook-forensics.org/）などがある。そのほかの製品については、付録 F に示した Web サイトを参照のこと。

31 検査結果については、http://www.cftt.nist.gov/disk_imaging.htmを参照のこと。

32 たとえば、システム上で実行されているサービスやプロセスは、誰かが現在そのコンピュータを使用していなくても、システムのハードディスクに書き込みを行う可能性がある。

をコピーすることが現実的かどうかを判定するべきである[33]。たとえば、1 人のユーザのホームディレクトリからファイルを収集するだけのために、何百人ものユーザが使用する重要なサーバを停止させる必要はない。稼働中のシステムの論理バックアップの場合、分析担当者は標準的なシステムバックアップソフトウェアを使用できる。しかし、バックアップを実行した場合、バックアップをローカルとリモートのどちらで行うかによって、システムのパフォーマンスに影響が出たり、ネットワーク帯域幅の大きな割合を占めたりする可能性がある。

各組織は、フォレンジックのためにビットストリームイメージの取得や論理バックアップ（稼働中のシステムからのバックアップを含む）を実行できる状況、およびそれらの作業を実行できる職員を示すポリシー、ガイドライン、および手続きを持つべきである[34]。通常は、システムの分類（影響の高、中、低）と注目すべき事象の性質に基づいてポリシー、ガイドライン、および手続きを確立するのが最も効果的である。特に重要なシステムのために、独立したポリシー声明、ガイドライン、および手続きを作成する組織もある。ポリシー、ガイドライン、および手続きでは、バックアップとイメージに関する意志決定を行う権限を持つ個人またはグループを明示するべきである。これらの人々は、リスクを検討し、健全な意志決定を行う能力を持つべきである。ポリシー、ガイドライン、および手続きでは、システムの種類ごとにどの個人またはグループがバックアップやイメージ取得を実行する権限を持つかについても明示するべきである。業務やシステムに含まれるデータの機密性のため、一部のシステムへのアクセスが制限される場合もある。

4.2.2 データファイルの完全性

バックアップ中やイメージ取得中は、元の媒体の完全性を維持するべきである。分析担当者は、バックアップまたはイメージ取得のプロセスによって元の媒体上のデータが変更されないことを保証するために、媒体のバックアップまたはイメージ取得の実行中にデータ書き込み防止ツールを使用するとよい。*データ書き込み防止ツール*は、コンピュータに接続された記憶媒体へのコンピュータによる書き込みを防止するハードウェアベースまたはソフトウェアベースのツールである。ハードウェア型のデータ書き込み防止ツールは、処理の対象となるコンピュータと記憶媒体に物理的に接続され、その媒体への書き込みを防止する[35]。ソフトウェア型のデータ書き込み防止ツールは、分析担当者のフォレンジックシステムにインストールされる。現在入手できるのは、MS-DOS システム用と Windows システム用のみである。一部の OS（Mac OS X や Linux など）では、二次的なデバイスをマウントせずに起動するように設定できるため、ソフトウェアデータ書き込み防止ツールは必要でない場合がある。だたし、ハードウェアデータ書き込み防止装置を接続することで、完全性が確実に維持されるようになる。MS DOS ベースのソフトウェアデータ書き込み防止ツールは、INT13 および拡張 INT13 によるディスク書き込みをトラップすることにより機能する。Windows ベースのソフトウェア型のデータ書き込み防止ツールは、デバイスに送信された割り込みをフィルタを使って選別することで、記憶媒体への書き込みを防止する[36]。

---

33 分析担当者は、システムから揮発性データを収集する必要性があるかどうかについても検討するべきである。システムが稼働中の場合、システムの揮発性データはより短時間で変わる可能性が高く、その保存がより困難になると考えられる。

34 この推奨事項の目的は、ユーザによる各自のデータおよびローカルワークステーションのバックアップの実行を制限することではなく、ユーザがしかるべき理由もなく他人のシステムやデータのバックアップを収集できないようにすることである。

35 ハードウェア型のデータ書き込み防止ツールの例としては、FastBloc（http://www.guidancesoftware.com/lawenforcement/ef_index.asp）、NoWrite（http://www.mykeytech.com/nowrite.html）、SCSIBlock（http://www.digitalintelligence.com/products/scsiblock/）などがある。そのほかのツールについては、付録 F に示した Web サイトを参照のこと。

36 ソフトウェアデータ書き込み防止ツールの例としては、PDBlock（http://www.digitalintelligence.com/software/disoftware/pdblock/）などがある。そのほかのツールについては、付録 F に示した Web サイトを参照のこと。

一般に、ハードウェア型のデータ書き込み防止ツールを使用する場合は、媒体または媒体を読み取るために使用するデバイスをデータ書き込み防止ツールに直接接続し、そのデータ書き込み防止ツールを、バックアップやイメージ取得を行うために使用するコンピュータまたはデバイスに接続する。ソフトウェア型のデータ書き込み防止ツールを使用する場合は、そのソフトウェアをコンピュータに読み込んでから、媒体または媒体を読み取るために使用するデバイスをそのコンピュータに接続する。データ書き込み防止ツールでは、特定のデバイスに対する書き込み防止を有効にしたり無効にしたりもできる。書き込み防止機能を使用する場合は、接続されているすべてのデバイスに対して機能を有効にすることが重要である[37]。また、データ書き込み防止ツールを定期的にテストして、新しいデバイスに対応するかどうかを確認するべきである。たとえば、新しいデバイスのために準備されていた機能やそれまで未使用だった機能を利用してデバイス固有の機能を実装した場合、最終的にデバイスへの書き込みが行われ、その内容が変更される可能性がある。

バックアップまたはイメージ取得の実行後は、コピー先のデータが元のデータの正確な複製であることを検証することが重要である[38]。データの完全性を検証および確認するためには、コピー先のデータのメッセージダイジェストを算出して使用できる[39]。*メッセージダイジェスト*は、データを一意に識別するハッシュであり、データ内の 1 ビットでも変更すると全く異なるメッセージダイジェストが生成されるという特性を持っている。データのメッセージダイジェストを算出するアルゴリズムは数多く存在するが、最もよく使われているのは、MD5 と SHA-1（Secure Hash Algorithm 1）の 2 つである。これらのアルゴリズムは、入力値として任意の長さのデータを取り、出力値として 128 ビットのメッセージダイジェストを生成する。SHA-1 は、連邦情報処理基準（FIPS：Federal Information Processing Standards）で承認されたアルゴリズムであるが、MD5 はそうでないため、連邦政府機関はメッセージダイジェストとして MD5 ではなく SHA-1 を使用するべきである[40]。

ビットストリームイメージの取得を行う場合は、元の媒体のメッセージダイジェストを算出し、記録してからイメージの取得を行うべきである。イメージを取得したら、コピー先の媒体のメッセージダイジェストを算出し、元のメッセージダイジェストと比較して、データの完全性が維持されていることを検証するべきである。次に、元の媒体のメッセージダイジェストを再び算出し、イメージ取得プロセスによって元の媒体が変更されなかったことを検証し、すべての結果を記録文書化するべきである。このプロセスは、論理バックアップにも使用するべきである。ただし、メッセージダイジェストをデータファイルごとに算出して比較するべきである。ビットストリームイメージの場合も、論理バックアップの場合も、データの完全性を確認するために作成したメッセージダイジェストは、読み取り専用または追記型の媒体に保存するか、印刷したあと、適切な場所に保管するべきである。

4.2.3　ファイルの更新、アクセス、作成の日時

多くの場合、ファイルがいつ作成され、使用され、操作されたかを知ることは重要であり、ほとんどの OS はファイルに関する特定のタイムスタンプを記録している。最もよく使われるタイムスタンプは、次に示す更新、アクセス、作成（MAC：Modification、Access、Creation）日時である。

37　これらは、データ書き込み防止ツールを使用するための一般的なガイドラインにすぎない。分析担当者は、ツールの適切な使用法について、個々のデータ書き込み防止ツール製品の操作手順を参照すること。

38　稼働中のシステムでバックアップを実行する場合、バックアップを開始してからバックアップを完了して検証するまでのあいだに一部のファイルが変わる可能性がある。

39　メッセージダイジェストは、フォレンジック活動中に取得したすべてのデータ（ログファイルや論理バックアップを含む）の完全性を確認するために使用されるべきである。

40　連邦政府機関は、FIPS で承認されたアルゴリズムと FIPS で有効性が確認された暗号モジュールを使用しなければならない。NIST の暗号モジュール検証プログラム（CMVP：Cryptographic Module Validation Program）では、FIPS テストの調整を行っている。CMVP の Web サイトは、http://csrc.nist.gov/cryptval/にある。FIPS 180-2『*Secure Hash Standard*』は、http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdfで入手できる。NIST は、連邦政府の各機関が 2010 年までに SHA-1 から SHA のより強力な形式（SHA-224、SHA-256 など）へ移行するように計画すべきであると発表している。詳細については、2004 年 8 月にhttp://csrc.nist.gov/hash_standards_comments.pdf で公開された NIST のコメント、およびhttp://www.nsrl.nist.gov/collision.htmlを参照のこと。

- **更新日時。**これは、ファイルに書き込みが行われた場合や、ファイルが別のプログラムによって変更が加えられた場合など、ファイルが最後に何らかの方法で変更された日時である。
- **アクセス日時。**これは、ファイルに対するアクセス（表示、オープン、印刷など）が最後に行われた日時である。
- **作成日時。**これは、一般にファイルが作成された日時であるが、ファイルがシステムにコピーされた場合は、ファイルが新しいシステムにコピーされた日時が作成日時となる。更新日時は変更されない。

ファイルシステムの種類によって保存される日時の種類は異なる可能性がある。たとえば、Windows システムでは最終更新日時、最終アクセス日時、および最終作成日時が保持される[41]。UNIX システムでは、最終更新日時、i ノード[42]最終変更日時、および最終アクセス日時が保持される。ただし、一部の UNIX システム（BSD や SunOS の各バージョンを含む）では、実行可能ファイルを実行しても、その最終アクセス日時は更新されない。一部の UNIX システムでは、ファイルのメタデータの最新変更日時が記録される。*メタデータ*は、データに関するデータである。ファイルシステムの場合、メタデータはファイルの内容に関する情報を提供するデータである。

分析担当者が事象を時系列に正確に示す必要がある場合は、ファイルの日時情報を保全するべきである。したがって、分析担当者は、データファイルの収集方法によってはファイルの日時情報を保全できない場合があることに注意するべきである。ビットストリームイメージの取得では、ビット単位のコピーを作成するため、ファイルの日時情報を保全できる。しかし、一部のツールを使って論理バックアップを行った場合は、データファイルをコピーしたときにファイルの作成日時が変更されることがある。このため、ファイルの日時情報が不可欠な場合は、必ずビットストリームイメージを使ってデータを収集するべきである。

分析担当者は、ファイルの日時情報が常に正確であるとは限らないことにも注意するべきである。ファイルの日時情報が正確でない理由には、次のような理由もある。

- コンピュータのクロックによって示される時間が正確でない。たとえば、クロックが信頼できる時間ソースと定期的に同期していない可能性がある。
- 期待される詳細レベルで時間が記録されていない場合がある（秒や分が省略されるなど）。
- 攻撃者が、記録されているファイルの日時情報を改変した可能性がある。

4.2.4 技術的問題

データファイルの収集では、いくつかの技術的な問題が発生することがある。4.2.1 項で述べたように、最も重要な問題は、媒体上の空き領域やスラック領域に存在する削除されたファイルやファイルの残がいの収集である。個人ユーザは、さまざまな技法を使ってこのようなデータの収集を妨害してしまうかもしれない。たとえば、*完全消去*を実行するために利用できるユーティリティが数多く存在する。完全消去とは、媒体（または特定のファイルなど、媒体の一部）をランダムな値または一定の値（たとえば、0 のみ）で上書きすることである。このようなユーティリティは、サービスや信頼性の点で異なるが、そのほとんどはファイルの容易な収集を防止するという点で効果的である（特に完全消去を複数回行った場合）。個人ユーザは、ハードディスクドライブの減磁（*消磁*ともいう）、媒体の物理的な破損や破壊など、物理的な手段を使ってデータの収集を阻止してしまうかもしれない。物理的な技法とソフトウェアベースの技法のどちらであっても、ソフトウェアを使ってすべてのデータ

[41] NTFS ファイルシステムを使用する Windows システムでは、エントリ更新日時も記録される。

[42] *i ノード*は、ファイルに設定されている特権やファイルの所有者など、ファイルの特定の特性に関する一連のデータである。

を復旧することが困難に（場合によっては不可能に）なる可能性がある。このような場合に復旧を試みるには、高度な施設、ハードウェア、技法とともに、高度な専門性を備えたフォレンジック専門家を利用する必要があるが、そのような手段を一般的に利用するには、そのためにかかるコストや労力があまりにも多すぎる[43]。場合によっては、データをまったく復旧できないこともある。

もう 1 つの一般的な問題は、隠しデータの収集である。多くの OS では、ユーザが特定のファイル、ディレクトリ、またはパーティションを隠すものとして目印を付けることができる。「隠す」というのは、それらの要素がデフォルトではディレクトリー覧に表示されなくなるということである[44]。一部のアプリケーションや OS は、ユーザが誤って変更または削除する可能性を減らすため、設定ファイルを隠している。また、一部の OS では、削除されたディレクトリに「隠し」マークが付けられることがある。隠しデータには、豊富な情報が含まれている可能性がある。たとえば、隠しパーティションには、別の OS と多くのデータファイルが格納されているかもしれない[45]。ユーザは、パーティションテーブルに変更を加えて、ディスク管理を妨害し、データ領域が存在することをアプリケーションから認識できないようにすることで、隠しパーティションを作成できる。隠しデータは、NTFS ボリューム上の ADS、媒体上のファイル終端のスラック領域や空き領域、および一部のハードディスクドライブ上のホスト保護領域（HPA：Host Protected Area、ベンダーのみが使用できるようにしたドライブ上の領域）で見つかることもある。多くの収集ツールは、データを隠蔽するこれらの手法の一部またはすべてを認識し、関連するデータを復旧することができる。

発生する可能性があるもう 1 つの問題は、ストライピング（RAID-0、RAID-5 など）を使用する RAID アレイからのデータの収集である[46]。この構成では、ストライピングされたボリュームは、別々のディスクドライブに存在する同一サイズのパーティションで構成される。ボリュームにデータが書き込まれると、ディスクのパフォーマンスを向上させるために、それぞれのパーティションにデータが均等に分配される。この場合、ストライピングされたボリュームの内容を検査するためには、ボリュームのすべてのパーティションが存在する必要があるが、各パーティションは物理的に独立のディスクドライブに存在するため、問題が起きる可能性がある。ストライピングされたボリュームを検査するには、RAID アレイの各ディスクドライブのイメージを取得し、検査システム上で RAID 構成を再作成する必要がある[47]。検査システムの起動には、RAID アレイを認識して使用することができ、RAID アレイへの書き込みを防止するフォレンジック起動ディスクを使用する必要がある。一部のイメージ取得ツールは、ストライピングされたボリュームを取得し、ボリュームの未使用データ領域（空き領域やスラック領域など）を保全することができる[48]。

4.3 データファイルの検査

論理バックアップまたはビットストリームイメージの取得を行ったあとは、データを検証する前に、バックアップまたはイメージを別の媒体に復元する必要がある。これは、分析の実行に使用するフォレンジックツールによって異なる。イメージファイルから直接データを分析できるツールもあるが、最初にバックアップまたはイメージを媒体に復元する必要があるツールもある[49]。イメージファイルと復元

---

43 このような復旧の試みを専門に行う企業として、Data Recovery Services、DriveSavers、Ontrack Data Recovery などがある。

44 UNIX システムでは、先頭に「.」が付いたファイルやディレクトリは「非表示」とみなされ、-a フラグを使わずにファイルを一覧表示した場合は表示されない。

45 隠しパーティションを見つけるために利用できる無償のツールの例としては、DOS に組み込まれている FDISK ユーティリティなどがある。そのほかのツールについては、付録 F に示した Web サイトを参照のこと。

46 RAID の概要については、http://www.adaptec.com/worldwide/product/markeditorial.html?prodkey=quick_explanation_of_raidを参照のこと。

47 RAID-5 では 1 つのディスク上にパリティ情報が格納されるため、それ以外のディスクすべてのイメージを取得することで、RAID-5 ボリュームを検査できる。

48 RAID の詳細については、http://www.anandtech.com/storage/showdoc.html?i=1491を参照のこと。

49 かつて、ツールの機能がもっと限られていた頃は、同じ OS や関連する OS を使ってデータファイルをシステムに復元することが、多くの場合に推奨されていた。現在のツールは進歩し、基盤となる OS に関係なく、多くの種類のデータ

されたイメージのどちらを検査で使用するかに関係なく、検査するデータが変更されないように、また何度検査してもデータから一貫性のある結果が得られるように、データには読み取り専用権限でアクセスするべきである。4.2.2 項で述べたように、このプロセスでは、データ書き込み防止ツールを使って、復元されたイメージに対する書き込みの発生を防止できる。分析担当者は、（必要な場合に）バックアップを復元したあと、収集されたデータの検査を開始し、削除されたファイル、スラック領域や空き領域に含まれるファイルの残がい、および隠しファイルを含むすべてのファイルを特定することにより、関連するファイルおよびデータのアセスメントを行う。分析担当者は、次にファイルの一部またはすべてからデータを抽出する必要があるが、暗号化やパスワード保護などの手段によってその作業が複雑になる可能性がある。この項では、ファイルとデータの検査に関わるプロセスと、検査の効率化に役立つ技法について説明する。

4.3.1 ファイルの特定

検査の最初の手順は、ファイルを特定することである。ディスクイメージには、何ギガバイトものスラック領域や空き領域が捕捉され、そのなかに何千ものファイルやファイルの断片が含まれている可能性がある。未使用領域から手作業でデータを抽出するのは、基盤となるファイルシステムの形式に関する知識を必要とし、時間のかかる困難なプロセスである。幸い、未使用領域からのデータの抽出、抽出されたデータのデータファイルへの保存、さらに削除されたファイルやゴミ箱にあるファイルの復旧といったプロセスを自動化できるツールがいくつか存在する。分析担当者は、16 進エディタや専用のスラック回復ツールを使ってスラック領域の内容を表示することもできる。

4.3.2 データの抽出

検査プロセスの残りでは、ファイルの一部またはすべてからデータを抽出する。ファイルの内容を理解するために、分析担当者はファイルにどのような種類のデータが格納されているかを知る必要がある。ファイル拡張子の本来の目的は、ファイル内容の種類を示すことにある。たとえば、jpg という拡張子はグラフィックファイルを示し、mp3 という拡張子は音楽ファイルを示す。しかし、ユーザは任意の種類のファイルに任意のファイル拡張子を割り当てることができる。たとえば、テキストファイルに **mysong.mp3** という名前を付けたり、ファイル拡張子を省略したりできる。さらに、一部のファイル拡張子は、ほかの OS では隠されたり、サポートされなかったりする可能性がある。したがって、分析担当者はファイル拡張子が正しいと想定するべきではない。

分析担当者は、多くのファイルについて、ファイルのヘッダを確認することにより、格納されているデータの種類をより正確に識別できる。*ファイルヘッダ*には、ファイルに関する識別情報と、（場合によっては）ファイル内容に関する情報を提供するメタデータが含まれている。図 4-1 に示すように、ファイルヘッダにはそのファイルに格納されているデータの種類を示すファイルシグネチャが含まれている[50]。図 4-1 の例では、ファイルヘッダが FF D8 であり、これが JPEG ファイルであることを示している。ファイルヘッダが実際のファイルデータとは別のファイルに格納されている場合もある。ファイル内のデータの種類を識別するもう 1 つの効果的な技法は、ファイル内の ASCII 値の分布をファイル内の合計文字数に対するパーセンテージで示す簡単なヒストグラムである。たとえば、空白文字、「a」、および「e」の個数が特に多い場合は一般にテキストファイルであり、ヒストグラム全体が均一に分布している場合は圧縮ファイルである。そのほかのパターンは、暗号化されたファイルやステガノグラフィによって変更が加えられたファイルを示していると考えられる。

ファイルに対して使用できるように設計されているため、ほとんどの場合、データファイルを特定の OS に復元する必要はなくなった。

50 ファイルヘッダから、ファイルが暗号化されているかどうかがわかる場合もある。攻撃者は、実際のファイル形式を隠すために 16 進エディタを使ってファイルヘッダを変更したあと、ファイルを使用するためにファイルヘッダを元に戻すことができる。場合によっては、ヘッダを変更してもファイルを使用できる可能性もある。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà..JFIF.....
00000010	00	01	00	00	FF	DB	00	43	00	08	06	06	07	06	05	08	....ÿÛ.C.....
00000020	07	07	07	09	09	08	0A	0C	14	0D	0C	0B	0B	0C	19	12	.....
00000030	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	..... $.'
00000040	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",#..(7),01444.'
00000050	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342ÿÛ.C...
00000060	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	32	32	32	32	........2!.!2222

図 4-1. ファイルヘッダの情報

多くの場合、暗号化は分析担当者にとって難問である。ユーザは、個々のファイル、フォルダ、ボリューム、またはパーティションを暗号化することにより、他人が復号鍵やパスフレーズなしでそれらの内容にアクセスできないようにしている可能性がある[51]。暗号化は、OS による場合もあれば、サードパーティ製のプログラムによる場合もある。暗号化されたファイルを識別するのは比較的簡単だが、復号するのは通常それほど簡単ではない。分析担当者は、ファイルヘッダを検査したり、システムにインストールされた暗号化プログラムを特定したり、暗号鍵（ほかの媒体に保存されていることが多い）を見つけたりすることで、暗号化の方法を特定できる可能性がある。暗号化の方法がわかれば、分析担当者はファイルを実際に復号できるかどうかをより適切に判断できる。多くの場合、暗号化の方法が強力で、復号に使われる認証（パスフレーズなど）を入手できないため、ファイルを復号することができない。

分析担当者は、暗号化されたデータの存在を比較的簡単に検出できるが、ステガノグラフィが使用されているかどうかを知るのはもっと難しい。*ステガノグラフィ*（*ステゴ*ともいう）は、データをほかのデータのなかに埋め込むことである。ステガノグラフィの例には、ディジタル透かしや、画像の中に語句や情報を隠すことなどがある。分析担当者がステガノグラフィで埋め込まれたデータを見つけるために使用できる技法として、同じ画像の複数バージョンの検出、グレースケール画像の存在の特定、メタデータやレジストリの検索、ヒストグラムの使用、ハッシュセットを使った既知のステガノグラフィソフトウェアの検索などがある。分析担当者は、ステガノグラフィで埋め込まれたデータが存在することを確信したら、どのソフトウェアによってデータが作成されたかを判定し、ステゴ鍵を発見することによって、または総当たり攻撃と暗号攻撃を使ってパスワードを特定することによって、埋め込まれたデータを抽出できる可能性がある[52]。しかし、このような試みは、特に分析担当者が検査対象の媒体上で既知のステガノグラフィソフトウェアの存在を発見できなかった場合、成功しないことが多く、また多大な時間を要する可能性がある。このほか、ファイルを分析し、そのファイルがステガノグラフィによって変更が加えられた可能性を推定できるソフトウェアプログラムもある。

分析担当者は、ステガノグラフィではなく、パスワードによって保護されたファイルにもアクセスする必要があるかもしれない。パスワードは、そのパスワードによって保護されるファイルと同じシステムに格納されていることが多いが、符号化または暗号化されている。個々のファイルにかけられているパスワードや OS のパスワードのクラッキング（割り出し）ができるさまざまなユーティリティが存在する[53]。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

---

51 一部のオペレーティングシステムではボリュームやパーティションを暗号化できるが、破損やそのほかの機能的問題によってデータのわずか 1 セクタでも破損するとデータをすべて失うことになるため、これは一般的でない。個々のファイルやフォルダの暗号化の方がはるかに一般的であり、多くの新しいオペレーティングシステムでサポートされている。

52 ステガノグラフィについて詳しく論じることは、この文書の範囲を超えている。詳細については、http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htmで入手できる論文『*An Overview of Steganography for the Computer Forensics Examiner*』（Gary Kessler 著）を参照のこと。

53 オープンソースのパスワードクラッキングユーティリティの例として、複数の OS やファイル形式をサポートする John the Ripper などがある。そのほかのパスワードクラッキングユーティリティについては、付録 F に示した Web サイト（たとえば、Computer Forensics Tools（http://www.forensix.org/tools/）や TUCOFS：The Ultimate Collection of Forensic Software（http://www.tucofs.com/tucofs.htm）など）を参照のこと。

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の種類や、パスワードそのもののの工夫の度合いによって大幅に異なる。もう 1 つの手法は、パスワードの迂回である。たとえば、分析担当者はシステムを起動してスクリーンセーバのパスワードを無効にしたり、システムのマザーボードから基本入出力システム（BIOS：Basic Input/Output System）のジャンパを引き抜くか製造者のバックドアパスワードを使用することによって BIOS のパスワードを迂回したりできる[54]。もちろん、パスワードの迂回に伴ってシステムの再起動を行う可能性があるが、それが好ましくない場合もある。もう 1 つの可能性は、管理職および法律上の適切な承認を得たうえで、ネットワークまたはホストベースの管理策（パケットスニファやキーストロークロガーなど）によってパスワードの捕捉を試みることである。ハードディスクドライブに起動パスワードが設定されている場合は、パスワードを推測したり（ベンダーが設定したデフォルトのパスワードなど）、専用のハードウェアやソフトウェアを使ってパスワードを迂回したりできる可能性がある。

4.3.3 フォレンジックツールキットの使用

分析担当者が、データの検査や分析、およびいくつかの収集活動の実行を可能にするさまざまなツールを利用できるようになっているべきである。多くのフォレンジック製品では、分析担当者がファイルやアプリケーションの分析だけでなく、ファイルの収集、ディスクイメージの読み取り、ファイルからのデータの抽出など、広範囲のプロセスを実行できるようになっている。ほとんどの分析製品は、レポートを生成する機能や、分析中に発生したあらゆるエラーをログに記録する機能も備えている。これらの製品は、分析を行う際にきわめて有益だが、データに関する特定の疑問を解決するには、どのプロセスを実行するべきかを理解することが不可欠である。分析担当者は、収集されたデータに関する簡単な疑問にすばやく対応したり、解決したりしなければならない場合がある。このような場合、完全なフォレンジック評価は不要か、または実行できない可能性さえある。フォレンジックツールキットには、さまざまな方法でデータの検査と分析を遂行でき、フロッピーディスク、CD、またはフォレンジックワークステーションからすばやく効率的に起動できるアプリケーションを含めるべきである。以下のプロセスは、分析担当者が各種のツールを使って実行できるようにすべきプロセスの例である。

- **ファイルビューアの使用**。ある種のファイルの内容を表示するのに、本来のソースアプリケーションではなく、ビューアを使用することは、データのスキャンやプレビューを行うための重要な技法であり、分析担当者が表示するファイルの種類ごとにネイティブアプリケーションを使用せずに済むため、効率的である。一般的な種類のファイルを表示するためのさまざまなツールが入手可能であり、グラフィックだけを表示するための専用ツールも存在する。利用可能なファイルビューアが特定のファイル形式をサポートしていない場合、本来のソースアプリケーションを使用するべきである。それもできない場合は、ファイルの形式を調べ、ファイルから手作業でデータを抽出しなければならない可能性がある[55]。

- **ファイルの展開**。圧縮ファイルには、有益な情報やほかの圧縮ファイルが格納されている可能性がある。したがって、分析担当者は圧縮ファイルを見つけて抽出することが重要である。圧縮ファイルの内容を、検索やそのほかの措置の対象に含めるために、ファイルの展開をフォレンジックプロセスの早い段階で行うべきである。ただし、分析担当者は圧縮ファイルに悪意のある内容（たとえば、ファイルが繰り返し（一般に数十～数百回）圧縮された「圧縮爆弾」など）が含まれている可能性があることに留意するべきである。圧縮爆弾により、検査ツールが機能しなくなったり、大量のリソースを消費したりすることがある。また、圧縮爆弾に

[54] 既知の BIOS バックドアパスワードの詳細と例については、論文『*How to Bypass BIOS Passwords*』（http://labmice.techtarget.com/articles/BIOS_hack.htm）を参照のこと。

[55] Wotsit's Format（http://www.wotsit.org/）などの Web サイトには、数百に及ぶファイルの種類のファイル形式情報が掲載されている。

マルウェアやそのほかの悪意のあるペイロードが含まれている場合もある。ファイルを展開する前に圧縮爆弾を検出する決定的な方法はないが、その影響を最小限に抑える方法はある。たとえば、検査システムは、最新のウイルス対策ソフトウェアを使用するべきであり、影響をそのシステムに限定するためにスタンドアロンにするべきである。また、検査システムのイメージを作成し、必要に応じてシステムを復元できるようにしておくべきである。

- **ディレクトリ構造のグラフィック表示。**この実践事項により、分析担当者は、インストールされているソフトウェアの種類や、データを作成したユーザが持っていると思われる技術的能力など、媒体の内容に関する一般的な情報をより簡単かつ迅速に収集できるようになる。ほとんどの製品は、Windows、Linux、および UNIX のディレクトリ構造を表示できるが、一部の製品は Macintosh のディレクトリ構造専用である。

- **既知のファイルの識別。**注目すべきファイルを見つけることの利点は明白だが、重要でないファイル（OS やアプリケーションの問題のない既知のファイルなど）を検討対象から除外することが有益な場合も多い。分析担当者は、有効性が確認されたハッシュセット(NIST の NSRL（National Software Reference Library）プロジェクト[56]が作成したハッシュセットや、個人的に作成して有効性が確認されたハッシュセット[57]など)を既知の害のないファイルや悪意のあるファイルを識別するための基礎として使用するべきである。ハッシュセットは、一般に SHA-1 および MD5 アルゴリズムを使用して既知の各ファイルのメッセージダイジェスト値を確立する。

- **文字列検索とパターン一致検索の実行。**文字列検索は、大量のデータを精査して重要な語句や文字列を見つけるのに役立つ。論理検索、あいまい検索、同義語検索と概念検索、語幹抽出検索、およびそのほかの検索手法を使用できるさまざまな検索ツールが存在する。一般的な検索の例として、1 ファイル内の複数語句の検索、つづりの誤った語句の検索などがある。一般的な状況で使用する検索語の簡潔なセットを作成しておくと、分析担当者が確認すべき情報の量を減らすことができる。文字列検索を実行する際の考慮事項や予想される困難の例を以下に示す。

  – 独自のファイルフォーマットについては、別のツールを使用しないと文字列検索ができない可能性がある。また、圧縮ファイル、暗号化ファイル、パスワードで保護されたファイルについては、文字列検索の前に追加的な前処理が必要である。

  – 外国の文字や Unicode 文字などを含む複数の文字からなるデータセットが使用されていると、文字列検索で問題が発生することがある。言語変換機能を備えることでこれを克服しようとしている検索ツールもある。

  – 予想されるもう 1 つの問題は、検索ツールや検索アルゴリズムに内在する制限である。たとえば、検索する文字列が隣接しない複数のクラスタに分かれて格納されていると、文字列検索で一致しない場合がある。同様に、検索文字列の一部があるクラスタに格納されており、検索文字列の残りの部分がもう 1 つのクラスタに格納されているが、後者が前者のクラスタを含むファイルの一部ではない場合に、誤って一致する検索ツールもある。

- **ファイルのメタデータへのアクセス。**ファイルの*メタデータ*は、ファイルの詳細情報を提供する。たとえば、グラフィックファイルのメタデータを収集すると、そのグラフィックの作成日、著

[56] NSRL のホームページは、http://www.nsrl.nist.gov/にある。

[57] 分析担当者は、定期的にシステムファイルのハッシュを作成することもできる。分析担当者は、事象が発生したときにこれらのハッシュセットを利用し、既知の害のないファイルを検査からすばやく除外できる。分析担当者は、できるだけ標準のハッシュセット（NSRL のプロジェクトで用意されているものなど）を利用し、カスタムのハッシュセットは主に組織固有のファイルに対して作成するようにするべきである。

作権情報、説明、および作成者の身元識別情報が得られる[58]。ディジタルカメラで作成されたグラフィックのメタデータには、画像を撮るために使われたディジタルカメラのメーカーとモデル、および f 値、フラッシュ、絞り設定などが含まれている可能性がある。ワードプロセッサファイルの場合は、メタデータによって作成者、ソフトウェアのライセンスを受けた組織、最後に編集した日時とユーザ、およびユーザ定義のコメントが指定されている可能性がある。ファイルからメタデータを抽出するには、特別なユーティリティを使用する。

4.4 分析

検査が完了したあとの次の段階は、抽出したデータの分析を行うことである。4.3.3 項で述べたように、各種のデータの分析に役立つツールが数多く存在する。分析担当者は、これらのツールを使用したり、データを手作業で確認したりする場合、システム時間とファイル時間を使用する価値を認識するべきである。インシデントがいつ発生したか、ファイルがいつ作成または変更されたか、または電子メールがいつ送信されたかを知ることは、フォレンジック分析にとってきわめて重要な場合がある。たとえば、このような情報を使って活動を時系列に沿って再構成できる。これは、簡単な作業のように思えるかもしれないが、システム間の故意または偶発的な時間設定の矛盾に起因して複雑になることが多い。分析対象データが存在するコンピュータの時刻、日付、および時間帯の設定を知ることは、分析担当者にとって大いに役立つ。セクション 5 では、このことについて詳しく説明する。

通常、組織が正確なタイムスタンプを使ってシステムを管理すれば、分析担当者にとって有益である。NTP（Network Time Protocol）は、NIST またはそのほかの組織によって運用されている原子時計を使ってコンピュータの時間を同期する。同期は、個々のシステムが比較的正確な時間を維持するのに役立つ。

複数のツールを使って検査や分析を行う場合、分析担当者は各ツールがどのようにファイルの更新、アクセス、作成（MAC）日時を抽出し、変更し、表示するかを理解するべきである。たとえば、OS が書き込み可能な状態でファイルシステムをマウントした場合に、ファイルやディレクトリの最終アクセス日時を変更するツールがある。データ書き込み防止ツールを使って、これらのツールが MAC 日時を変更するのを防ぐこともできる。ただし、データ書き込み防止ツールは、これらの時間が媒体上で変更されるのを防ぐことはできても、OS が変更内容をメモリにキャッシュする（つまり、ランダムアクセスメモリ（RAM）に変更内容を格納する）のを防ぐことはできない。その場合、OS は実際の日時ではなくキャッシュされた MAC 日時を報告し、不正確な結果を返す可能性がある。分析担当者は、データファイルやディレクトリの最終アクセス日時を照会する場合、使用するツールによっては照会のたびに時間が変わる可能性があることを認識するべきである。これらの問題があるため、分析担当者は MAC を表示する手法を慎重に選択し、その手法の詳細を記録するべきである。

分析担当者は、事象データに基づいてフォレンジック時系列情報を生成できる特別なツールを使用できる。このようなツールは、通常、一連の事象を表示して分析するためのグラフィックインタフェースを分析担当者に提供する。これらのツールに共通する機能の 1 つは、分析担当者が関連する事象をメタ事象にグループ化するための機能である。これは、分析担当者が事象の「全体像」を把握するのに役立つ。

多くの場合、フォレンジック分析にはファイルのデータだけでなく、そのほかのソースのデータも関係する（OS の状態、ネットワークトラフィック、アプリケーションなど）。セクション 8 では、分析によってファイルのデータとほかのソースのデータを相互に関連付ける方法を例示する。

---

[58] メタデータは、特定の種類のグラフィックファイルにしか含まれていない。たとえば、JPEG 形式のグラフィックには、メタデータが含まれている可能性があるが、ビットマップ形式のグラフィックには含まれていない。

4.5 推奨事項

このセクションに示したデータファイルのデータの使用に関する主な推奨事項は、以下のとおりである。

- **分析担当者は、元のファイルではなく、ファイルのコピーを検査すること。**収集フェーズでは、分析担当者は必要なファイルやファイルシステムの複数のコピー（通常はマスタコピーと作業用コピー）を作成するべきである。これにより、分析担当者は元のファイルやマスタコピーに影響を与えることなくファイルの作業用コピーを使用できる。訴訟や懲戒処分で証拠が必要とされる場合や、ファイル日時情報を保全することが重要な場合は、ビットストリームイメージの取得を行うべきである。

- **分析担当者は、ファイルの完全性を保護し、検証すること。**バックアップ中またはイメージの取得中にデータ書き込み防止ツールを使用することで、コンピュータによる記憶媒体への書き込みが防止される。ファイルのメッセージダイジェストを算出して比較することにより、コピー先のデータの完全性を検証するべきである。バックアップやイメージには、できる限り読み取り専用権限でアクセスするべきである。データ書き込み防止ツールを使って、バックアップファイルやイメージファイル、または復元されたバックアップやイメージへの書き込みを防止することもできる。

- **分析担当者は、ファイル拡張子ではなく、ファイルヘッダを利用してファイル内容の種類を識別すること。**ユーザはファイルに任意のファイル拡張子を割り当てることができるため、分析担当者はファイル拡張子が正しいと想定するべきではない。分析担当者は、多くのファイルについて、ファイルのヘッダを確認することにより、格納されているデータの種類を識別できる。ファイルヘッダに変更を加えて実際のファイル形式を隠すことも可能だが、これはファイル拡張子を変更するのに比べればごくまれである。

- **分析担当者は、データの検査と分析に使用するフォレンジックツールキットを用意すること。**このツールキットには、データのすばやい確認と詳細な分析を実行できるさまざまなツールを含めるべきである。このツールキットでは、アプリケーションをリムーバブルメディア（フロッピーディスク、CD など）やフォレンジックワークステーションから素早く効率的に起動できるようにするべきである。

5. オペレーティングシステムのデータの使用

オペレーティングシステム（OS）は、コンピュータ上で実行され、ほかのプログラムを実行するためのソフトウェアプラットフォームを提供するプログラムである。OS はまた、ユーザが入力したコマンドの処理、ディスプレイへの出力の送信、データの格納や取り出しに必要な記憶装置とのやり取り、およびプリンタやモデムなどの周辺装置の制御を担当する。ワークステーションまたはサーバ用の一般的な OS には、Windows、Linux、UNIX、および Mac OS の各種バージョンなどがある。ネットワーク機器（ルータなど）のなかには、Cisco の IOS（Internetwork Operating System）など、独自の OS を持つものもある。PDA では、専用の OS（PalmOS や Windows CE など）が実行されていることが多い[59]。多くの組み込みシステム（携帯電話、ディジタルカメラ、オーディオプレーヤなど）でも、OS が使われている[60]。このセクションでは、フォレンジックに関係する可能性がある OS の構成要素について論じ、一般的なワークステーション OS やサーバ OS のデータの収集、検査、および分析に関するガイダンスを提供する[61]。

5.1 OS の基本

OS データは、不揮発性の状態と揮発性の状態の両方で存在する。*不揮発性データ*とは、コンピュータの電源を切ったあとも存続するデータ（ハードディスクドライブに格納されたファイルシステムなど）を指す。*揮発性データ*とは、稼働中のシステム上に存在し、コンピュータの電源を切ると消失するデータ（システムの現在のネットワーク接続など）を指す。フォレンジックスの観点からは、多くの種類の不揮発性および揮発性データが注目に値する可能性がある。この項では、これら両方の種類の OS データについて論じる。

5.1.1 不揮発性データ

OS 内部の不揮発性データの主なソースは、ファイルシステムである[62]。ファイルシステムはまた、通常、OS 内部のデータの最も大規模かつ豊かなソースであり、一般的なフォレンジック事象において回復される情報のほとんどを含んでいる。ファイルシステムは、1 つ以上の媒体を使って OS に格納場所を提供する[63]。ファイルシステムには、通常、多くの種類のファイルが格納されている。各ファイルは、状況によっては分析担当者にとって貴重なものである可能性がある。また、4.1.2 項で述べたように、未使用のファイルシステム領域から重要な残存データが回復される可能性もある。以下に、OS のファイルシステム内でよく見つかるデータの種類をいくつか示す。

---

59 PDA のフォレンジックの詳細については、NIST SP 800-72『*Guidelines on PDA Forensics*』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照のこと。

60 これらの種類の機器に含まれている可能性がある情報の種類、およびそれらの情報を収集、検査、分析する手法に関する説明は、この文書の対象外である。現在では多種多様な機器があり、それらの機器に格納されているデータをフォレンジック的に処理するために必要となる知識や機器も多岐にわたることから、ほとんどの組織では、このような機器を確保し、このような機器に含まれるデータの収集、検査、分析に熟練している適切な当事者(たとえば、法執行機関など)に機器を預けるのが最適であると考えることであろう。

61 独自仕様の OS や特殊な OS のデータに固有のガイダンスは、この文書の対象外であるが、このセクションで説明している概念の多くはそれらのデータにも当てはまるはずである。

62 標準的なファイルシステムを使用しない一部の機器（家庭用電子機器など）については、この説明が当てはまらないこともある。

63 場合によっては、ファイルシステムが動的なメモリに「格納」されることがある。*メモリファイルシステム*という用語は、システムのメモリのみに存在するファイルシステムを指す。このようなファイルシステムは、揮発性データとみなされる。起動可能な OS の実装をまるごと含んだファイルシステムが、フラッシュドライブなどのリムーバブルメディア上に存在する場合もある。

- **設定ファイル。**OS は、設定ファイルを使って OS やアプリケーションの設定を保存することがある[64]。たとえば、設定ファイルを使って、システムの起動後に自動的に開始するサービスを列挙したり、ログファイルや一時ファイルの場所を指定したりできる。ユーザが OS やアプリケーションの設定ファイルを個別に持っており、それらのファイルに、ハードウェア関連の設定（画面解像度、プリンタ設定など）やファイルの関連付けなど、ユーザ固有の情報や基本設定が含まれている場合もある。特に注目すべき設定ファイルを以下に示す。
  - **ユーザとグループ。**OS は、ユーザアカウントとグループの記録を保持している。アカウント情報には、所属グループ、アカウント名と説明、アカウントの権限、アカウントのステータス（アクティブ、無効など）、およびアカウントのホームディレクトリへのパスが含まれていることが考えられる。
  - **パスワードファイル。**OS は、データファイルにパスワードのハッシュを格納することがある。OS によっては、各種のパスワードクラッキングユーティリティを使ってパスワードハッシュを平文のパスワードに変換できる。
  - **スケジュール設定されたジョブ。**OS は、特定の時間に自動的に実行されるようにスケジュール設定された作業（ウイルススキャンを毎週実行するなど）のリストを管理している。このリストから収集できる情報には、作業名、作業の実行に使われるプログラム、コマンドラインのスイッチと引数、作業が実行される日時などがある。
- **ログ。**OS のログファイルには、OS の各種イベントに関する情報が格納されるが、アプリケーション固有のイベント情報が保持されることもある。OS によっては、ログがテキストファイル、独自フォーマットのバイナリファイル、またはデータベースに格納される場合がある。複数の独立したファイルにログエントリを書き込む OS もある。OS のログでよく見つかる情報の種類は、次のとおりである。
  - **システムイベント。**システムイベントは、OS の構成要素によって実行された運用上の措置（システムのシャットダウンやサービスの開始など）である。通常は、失敗イベントと最も重要な成功イベントがログに記録されるが、多くの OS ではシステム管理者がログに記録されるイベントの種類を指定できるようになっている。各イベントについて記録される詳細情報も、場合によって大きく異なる。通常、各イベントのタイムスタンプが記録されるが、そのほかの補足情報として、イベントコード、ステータスコード、ユーザ名などがある。
  - **監査記録。**監査記録には、認証の試みの成功と失敗、セキュリティポリシーの変更などのセキュリティ事象情報が含まれる。OS は、通常、システム管理者が監査対象となる事象の種類を指定できるようになっている。一部の OS では、管理者が特定の措置を実行する試みの成功、失敗、またはすべてをログに記録するように設定できる。
  - **アプリケーションイベント。**アプリケーションイベントは、アプリケーションの起動と終了、アプリケーションの障害、アプリケーション設定の大幅な変更など、アプリケーションによって実行された重要な運用上の措置である。セクション 7 では、アプリケーションイベントのログ記録について詳しく説明する。
  - **コマンド履歴。**一部の OS には、各ユーザが実行した OS コマンドの履歴を含む個別の（通常はユーザごとの）ログファイルがある。

---

64 Windows システムでは、多くの構成設定が*レジストリ*と呼ばれる一連の特殊なファイルに格納されている。レジストリの詳細については、Microsoft Knowledge Base の記事 256986『*Description of the Microsoft Windows Registry*』（http://support.microsoft.com/?id=256986）を参照のこと。

  - **最近アクセスしたファイル。**OS は、直前のファイルアクセスやそのほかのファイル使用をログに記録し、最近アクセスしたファイルのリストを作成することがある。

- **アプリケーションファイル**。アプリケーションは、実行可能ファイル、スクリプト、ドキュメント、設定ファイル、ログファイル、履歴ファイル、グラフィック、サウンド、アイコンなど、多くの種類のファイルで構成されている可能性がある。セクション 7 では、アプリケーションファイルについて詳しく説明する。

- **データファイル**。データファイルには、アプリケーション用の情報が格納されている。一般的なデータファイルの例には、テキストファイル、ワードプロセッサの文書、スプレッドシート、データベース、オーディオファイル、グラフィックファイルなどがある。また、ほとんどの OS は、データを印刷するときに、印刷可能な形式のデータを格納した 1 つ以上の一時印刷ファイルを作成する。セクション 4 からセクション 7 では、アプリケーションのデータファイルについて詳しく説明する。

- **スワップファイル**。ほとんどの OS は、アプリケーションがよく使用するデータの一時的な格納場所を提供するため、RAM とともにスワップファイルを使用する。スワップファイルは、本来、RAM とのあいだでデータのページ（セグメント）をスワップ（交換）できるようにすることによって、プログラムが利用できるメモリ量を拡大するものである。スワップファイルには、ユーザ名、パスワードハッシュ、連絡先情報など、OS やアプリケーションの幅広い情報が含まれる可能性がある。5.1.2 項では、メモリの内容についてさらに詳しく説明する。

- **ダンプファイル**。一部の OS には、エラー状態のメモリの内容を自動的に保存することにより、そのあとのトラブルシューティングを支援する機能がある。保存されたメモリ内容を保持するファイルは、ダンプファイルと呼ばれている。

- **ハイバーネーションファイル**。ハイバーネーションファイルは、システム(典型的な例として、ノート型パソコン)の電源を切る前に、メモリや開かれたファイルを記録することによってシステムの現在の状態を保存するために作成される。次回システムの電源を入れたときに、システムの状態が復元される。

- **一時ファイル**。OS、アプリケーション、または OS やアプリケーションの更新およびアップグレードのインストール中は、一時ファイルが作成されることが多い。このようなファイルは、通常はインストール処理の終了時に削除されるが、削除されない場合もある。また、一時ファイルは多くのアプリケーションが実行されているときにも作成される。このようなファイルも、通常はアプリケーションの終了時に削除されるが、やはり削除されない場合がある。一時ファイルには、システム上のほかのファイルのコピー、アプリケーションのデータ、またはそのほかの情報が含まれている可能性がある。

ファイルシステムは、不揮発性データの主なソースであるが、注目すべきもう 1 つのソースとして BIOS がある。BIOS には、接続されている機器（CD-ROM ドライブ、ハードディスクドライブなど）、接続の種類と割込み要求線（IRQ：interrupt request line）の割り当て（シリアル、USB、ネットワークカードなど）、マザーボードの構成要素（プロセッサの種類と速度、キャッシュサイズ、メモリの情報など）、システムのセキュリティ設定、ホットキーなど、多くの種類のハードウェア関連情報が含まれている。BIOS はまた、RAID ドライバと通信し、ドライバが提供する情報を表示する。たとえば、BIOS はハードウェア RAID を 1 つのドライブとみなし、ソフトウェア RAID を複数のドライブとみなす。BIOS では、一般にユーザがパスワードを設定できるようになっている。このパスワードにより、BIOS 設定へのアクセスを制限し、パスワードが入力されなければシステムが起動しないようにできる。BIOS には、システムの日付と時間も保持されている。

5.1.2 揮発性データ

OS は、システムの RAM のなかで実行される。OS が動作しているあいだ、RAM の内容は常に変化している。RAM には、任意の時点で、注目に値すると考えられる多くの種類のデータや情報が含まれている可能性がある。たとえば、RAM には、データファイル、パスワードハッシュ、最近実行したコマンドなど、頻繁にアクセスされるデータや最近アクセスされたデータが含まれていることが多い。また、ファイルシステムと同じように、RAM のスラック領域や空き領域にも次のように残存データが含まれている可能性がある。

- **スラック領域**。メモリのスラック領域は、ファイルのスラック領域よりはるかに不確定である。たとえば、OS は一般に*ページ*や*ブロック*と呼ばれる単位でメモリを管理し、それらを要求するアプリケーションに割り当てる。場合によっては、アプリケーションがメモリ単位をまるごと 1 つ分要求していないくても、1 つのメモリ単位がアプリケーションに割り当てられることがある。このため、アプリケーションに割り当てられたメモリ単位のなかに、そのアプリケーションからは利用できないながらも残存データが存在する可能性がある。一部の OS では、パフォーマンスや効率を考慮して、割り当てるメモリ単位のサイズを変えている。その場合は、メモリのスラック領域が小さくなりやすい。

- **空き領域**。メモリページの割り当てと割り当て解除は、ファイルクラスタとほぼ同じように行われる。割り当てられていないメモリページは、しばしば空きページの共通プールに集められる。このプロセスを*ガベージコレクション*と呼ぶことがある。未割り当てのファイルクラスタと同じように、これらの再利用可能なメモリページに残存データが存在するのは珍しいことではない。

OS のなかに存在する可能性があるそのほかの重要な揮発性データの種類には、次のようなものがある。

- **ネットワーク構成**。ネットワークインタフェースカード（NIC：network interface card）のドライバや構成設定など、ネットワーク機能の要素の多くは、ファイルシステムに保存されるのが一般的だが、ネットワークはその性質上、動的である。たとえば、多くのホストの IP（Internet Protocol）アドレスは別のホストによって動的に割り当てられており、これらの IP アドレスは保存される設定の一部ではない。多くのホストには、有線、無線、仮想プライベートネットワーク（VPN：virtual private network）、モデムなど、複数のネットワークインタフェースが定義されており、現在のネットワーク構成には現在どのインタフェースを使用しているかが示される。ユーザがネットワークインタフェースの構成をデフォルトから変更できる場合もある（IP アドレスを手動で変更するなど）。したがって、分析担当者は、可能な限り保存された構成ではなく、現在のネットワーク構成を使用するべきである。

- **ネットワーク接続**。OS は、ほかのシステムとの接続を円滑に行うための支援を提供する。ほとんどの OS は、現在の着信および発信のネットワーク接続のリストを提供でき、一部の OS は最近の接続のリストも提供できる。着信接続の場合、OS は通常どのリソース（ファイル共有やプリンタなど）が使われているかを示す。ほとんどの OS は、システムが接続を待機しているポートおよび IP アドレスのリストも提供できる。セクション 6 では、ネットワーク接続の重要性について詳しく考察する。

- **実行中のプロセス**。*プロセス*は、コンピュータ上で現在実行されているプログラムである。プロセスには、OS によって提供されるサービスと、管理者やユーザによって実行されるアプリケーションがある。ほとんどの OS には、現在実行中のプロセスのリストを表示する方法が用意されている。このリストを調べることにより、システム上で活動しているサービス（Web サーバなど）や個人ユーザが実行しているプログラム（暗号化ユーティリティ、ワードプロセ

ッサ、電子メールクライアントなど）を特定することができる。セクション 7 で説明するように、プロセスリストから、どのコマンドオプションが使われたかがわかる場合もある。実行中のプロセスの特定は、実行されているべきなのに無効化または削除されているプログラム（ウイルス対策ソフトウェアやファイアウォールなど）を特定する場合にも有効である。

- **開かれているファイル**。OS が開かれているファイルのリストを維持管理していることがある。このリストには、通常、個々のファイルを開いたユーザやプロセスも含まれている。
- **ログインセッション**。OS は、通常、現在ログインしているユーザに関する情報（および各セッションの開始時間と持続時間）、前回成功または失敗したログオン、特権の使用、およびユーザ切り替えを管理している[65]。ただし、ログインセッション情報を利用できるのは、ログオンの試みを監査するようにコンピュータが設定されている場合だけのことがある。ログオンの記録は、ユーザのコンピュータの使用傾向を把握したり、特定の事象が発生したときに特定のユーザアカウントが活動していたかどうかを確認したりするのに役立つことがある。
- **オペレーティングシステム時間**。OS は、現在の時間を管理し、夏時間や時間帯の情報を保存している。これらの情報は、事象を時系列に沿って組み立てたり、異なるシステムどうしの事象を相互に関連付けたりする際に役立つことがある。分析担当者は、OS 固有の設定（時間帯など）があるため、OS が示す時間と BIOS が示す時間が異なる可能性があることを認識しているべきである。

5.2 OS データの収集

5.1 項で説明したように、OS データは不揮発性の状態と揮発性の状態の両方で存在する。ファイルシステムのデータなどの不揮発性 OS データは、論理バックアップやビットストリームイメージの取得を行う際に、セクション 4 で説明した手法を使って収集できる。揮発性 OS データは、コンピュータの電源を切る前に収集するべきである。5.2.1 項および 5.2.2 項では、それぞれ揮発性および不揮発性の OS データの収集に関する推奨事項を示す。5.2.3 項では、データの収集を妨げる可能性がある技術的問題について論じる。

5.2.1 揮発性 OS データの収集

ある事象に関係する揮発性 OS データは、その事象が発生してから今までに再起動やシャットダウンが行われていない稼働中のシステムからのみ収集できる。システム上で実行されるあらゆる操作は、それを開始したのがユーザであるか OS 自体であるかに関わらず、ほぼ間違いなく何らかの方法で揮発性 OS データに変更を加える。このため、分析担当者は、揮発性 OS データを保全するべきかどうかをできるだけ速やかに決定するべきである。理想的には、分析担当者が最善の決定を即座に下せるように、この決定を行うための基準をあらかじめ文書化しておくべきである。システムの電源を切ったりネットワークから切断したりすると、潜在的に重要な情報を収集する機会が失われる可能性があるため、この決定の重要性は、いくら強調してもしすぎることはない。たとえば、ユーザが最近データを保護するために暗号化ツールを実行していた場合、コンピュータの RAM にはパスワードハッシュが含まれている可能性があり、パスワードを割り出すために、それを使用することができる。

一方、実行中のコンピュータから揮発性 OS データを収集することには、固有のリスクがある。たとえば、コンピュータ上のファイルが変更されたり、そのほかの揮発性 OS データが変更されたりする

[65] ユーザ切り替えにより、通常のシステムユーザが特定の作業を行うために、高いシステム特権を持つユーザに切り替わることができる。たとえば、特定のプログラムを実行するのに管理者のアクセス権限が必要な場合がある。通常のユーザが、ユーザ切り替えにより、これらのアクセス許可を取得し、アプリケーションを実行したあと、通常の特権に戻ることができる。

可能性は常に存在する。また、悪意のある者が、誤った情報を返したり、ファイルを削除したり、そのほかの悪意のある操作を実行したりするように設計されたルートキットをインストールしている可能性もある。揮発性データを収集するかどうかを決める際は、そのような収集に伴うリスクと重要な情報を回収できる可能性とを比較検討するべきである。3.2 項で述べたように、証拠が必要とされる可能性がある場合、分析担当者はシステムに触れる前に画面上に表示されている内容をすべて記録文書化するべきである。稼働中のシステムがスリープモードになっている場合や、システムに目に見えるパスワード保護がかかっている場合、分析担当者は、揮発性データの収集を試みられるように、システムをスリープモードから復帰させたり、パスワードを割り出したり、パスワード保護を回避したりすることによって、システムの状態を変更すべきかどうかも決定するべきである。揮発性データの収集に必要な労力を費やす価値がない場合、分析担当者は、5.2.2 項で説明するように、代わりにシャットダウンの実行を決定することもある。

5.2.1.1 項では、揮発性 OS データの収集に備えてフォレンジックツールをどのように編成するかを説明する。次に、5.2.1.2 項では、いくつかの種類のデータについて論じ、それぞれの種類を収集するのに効果的なツールの分類および特定の OS ツールについて述べる。最後に、5.2.1.3 項では、特定の状況で有用である可能性が最も高い揮発性 OS データの種類を識別し、重要性と相対的な揮発性に基づいてデータ収集の優先順位を決めることの必要性について説明する。

5.2.1.1 フォレンジックツールの準備

揮発性 OS データを収集する際は、必要となる可能性があるすべてのフォレンジックツールをフロッピーディスク、CD-ROM、または USB フラッシュドライブに格納し、それらの媒体からツールを実行するべきである。このようにすることで、分析担当者は、システムへの影響を最小限にとどめながら OS データを収集できる。また、システムコマンドがユーザによって悪意のある（ハードディスクをフォーマットしたり、誤った情報を返したりするような）プログラムに置き換えられている可能性があるため、フォレンジックツールのみを使用するべきである。ただし、フォレンジックツールを使用しても、取得したデータが正確であるという保証はない。システムが完全に侵害されている場合は、システムの機能をカーネルレベルで変更するルートキットやそのほかの悪意のあるユーティリティがインストールされている可能性がある。このような場合は、ユーザレベルのツールに誤ったデータが返される可能性がある。

フォレンジックツールのコレクションを作成する際は、静的にリンクされたバイナリファイルを使用するべきである。そのような実行可能ファイルは、参照する関数やライブラリ関数をすべて含んでいるため、別個のダイナミックリンクライブラリ（DLL：dynamic link libraries）やそのほかの補助ファイルを必要としない。これによって、ツールの媒体に適切なバージョンの DLL を格納する必要がなくなり、ツールの信頼性が向上する。分析担当者は、揮発性データを収集する前に、各ツールによってシステムにどのような影響や変更が加わるかを知っておくべきである。ファイルの完全性を検証するために、各ツールのメッセージダイジェストを算出して安全に保管しておくべきである。各フォレンジックツールのライセンス情報とバージョン情報も文書化しておくべきである。また、各フォレンジックツールを実行するために使用した正確なコマンド（コマンドラインの引数とスイッチ）も文書化するべきである。実行されたコマンド、実行日時、および実行時の出力内容を捕捉するために実行できるスクリプトをツールの媒体に格納しておくと、役に立つことがある。

ツールを格納した媒体は、変更されないようにツールを保護するべきである。フロッピーディスクは、ツールに変更が加えられないように書き込み禁止にするべきである。CD-ROM は、書き換え可能 CD ではなく追記型 CD（CD-R）にするべきである。書き換え可能 CD にすると、ユーザのコンピュータ上の CD 書き込みユーティリティによって CD の内容が書き換えられる可能性があるためである。

追記型 CD にツールを書き込んだ場合は、それ以上のデータを書き込めないように、ディスクをファイナライズするべきである[66]。

ツールが格納された媒体は、書き込み禁止にする必要があるため、ツールによって生成された結果をツールの媒体に格納することはできない。分析担当者は、ツールの出力をフロッピーディスクに振り向けることが多いが、コンピュータ機器におけるフロッピーディスクドライブの普及率は低下しつつある。そのため、出力を収集するための別の手法が開発されている。Windows や Linux ベースの環境を格納した特別に用意された CD や USB フラッシュドライブを使用することにより、システムの状態を変更せずに出力を収集し、一般的には別の USB フラッシュドライブ、外付けハードディスクドライブ、そのほかの書き込み可能媒体、またはリモートシステムに出力を振り向けることができる。

5.2.1.2 揮発性 OS データの種類

以下のリストでは、揮発性 OS データの種類をいくつか示し、それぞれの種類のデータを収集するためにフォレンジックツールをどのように使用できるかを説明する[67]。

- **メモリの内容**。RAM の内容をデータファイルにコピーし、そのあとのデータ分析を支援できるユーティリティがいくつか存在する。ほとんどのシステムでは、RAM のコピーを試みるユーティリティを実行したときに RAM が変更されることを避けられない。その代わり、RAM の変更を最小限に抑えるために、フットプリントをできるだけ小さくしてコピーを実行することが目標になる。

- **ネットワーク構成**。ほとんどの OS には、現在のネットワーク構成を表示するユーティリティがある（UNIX システムの **ifconfig** や Windows システムの **ipconfig** など）。ネットワーク構成ユーティリティによって提供される情報には、ホスト名、物理的および論理的なネットワークインタフェース、各インタフェースの構成情報（IP アドレス、媒体アクセス制御（MAC: Media Access Control）アドレス、現在の状態）などがある。

- **ネットワーク接続**。OS は、一般に、現在のネットワーク接続のリストを表示する手段を備えている。Windows ベースのシステムと UNIX ベースのシステムには、通常、**netstat** プログラムが含まれている。このプログラムは、発信元と送信先の IP アドレスおよびポートごとにネットワーク接続のリストを表示し、それぞれのインタフェースのどのポートが開いているかも表示する[68]。各プログラムに対するポートの割り当てを表示できるサードパーティ製のユーティリティが入手できる。ほとんどの OS は、リモートでマウントされたファイルシステムのリ

---

66 CD のファイナライズは、CD 書き込みユーティリティの一般的な機能である。一部の CD 書き込みユーティリティでは、現在のセッションをクローズすることもできる。ただし、セッションの *クローズ*は、現在のセッションでディスクに追加データを書き込まないように CD 書き込みユーティリティに指示する機能であり、別のセッションでディスクに追加データが書き込まれること（一般にマルチセッションディスクと呼ぶ）を防ぐものではない。したがって、分析担当者は、ツールキットの CD を作成するときに、セッションのクローズではなく、ディスクのファイナライズを行うべきである。

67 分析担当者が利用できる何百ものツールを記載した情報源が数多く存在する。付録 F に、コンピュータフォレンジックツールに関してさらに詳細な情報を記載する Web サイトをいくつか示す。OS に付属するツールの場合、分析担当者は、対象システムの OS 上にあるツールではなく、読み取り専用媒体に収録したそれらのツールのコピーを使用するべきである。

68 開いているポートを識別するもう 1 つの方法は、別のシステムからポートスキャンソフトウェアを実行することである。ポートスキャンソフトウェアは、さまざまなポートにネットワークトラフィックを送信し、その応答と応答の有無を分析することにより、どのポートが開いているのかを判定する。ただし、ポートスキャンをブロックするホストベースのファイアウォールなどのセキュリティ管理策のために、ポートスキャンによって生成される結果が不正確な場合がある。また、スキャンによってシステムの状態が変化する場合もある。したがって、ポートスキャンは非公式なデータの取得や、OS にアクセスできない場合の情報収集に最も適している。

ストを表示することもできる。このリストには、ネットワーク接続のリストより詳しい情報が含まれている。6.2.7 項では、ネットワーク接続情報の収集について詳しく説明する[69]。

- **実行中のプロセス**。すべての UNIX ベースのシステムは、現在実行中のプロセスを表示する **ps** コマンドを備えている。Windows には、グラフィカルユーザインタフェース（GUI）ベースのプロセス一覧表示ユーティリティであるタスクマネージャが用意されているが、一般的にはテキストベースの一覧表示機能を持っていることが望ましい。Windows システムでは、サードパーティ製のユーティリティを使用して、実行中のプロセスのテキストによる一覧表示が行える。

- **開かれているファイル**。すべての UNIX ベースのシステムは、開かれているファイルを表示する **lsof** コマンドを備えている。Windows システムでは、サードパーティ製のユーティリティを使用して、開かれているファイルのテキストによる一覧表示が行える。

- **ログインセッション**。一部の OS には、現在ログオンしているユーザの一覧を表示するための組み込みコマンドが用意されている（UNIX システムの **w** コマンドなど）。**w** コマンドは、各ユーザのソースアドレスやユーザがシステムにログオンした日時も表示する。Windows システムでは、サードパーティ製のユーティリティを使用して、システムに現在接続されているユーザを一覧表示できる。

- **オペレーティングシステム時間**。現在のシステム時間、時間帯の情報、および夏時間の設定を取得するためのユーティリティがいくつか存在する。UNIX システムでは、**date** コマンドを使ってこれらの情報を取得できる。Windows システムでは、**date**、**time**、および **nlsinfo** コマンドを組み合わせて、これらの情報を取得できる。

多くの場合、前述のツールに加えて、次のような汎用ツールをフォレンジックツールキットに含めると便利である。

- **OS のコマンドプロンプト**。このユーティリティは、ツールキットに含まれるほかのツールを実行する際に使用する OS のコマンドプロンプトを提供する（Windows システムの **cmd** など）。

- **SHA-1 によるチェックサム**。データファイルの SHA-1 メッセージダイジェストを算出できるユーティリティは、ファイルの有効性を確認するのに役立つ。また、ファイルの有効性確認を支援するためには、標的 OS に関連するシステムデータファイルの SHA-1 メッセージダイジェストのリストをツールキットに含めるのも有効である。この目的に対応する各種 OS 用のユーティリティが入手可能である[70]。

- **ディレクトリー覧。**ファイルシステムをナビゲートしたり、その内容を表示したりするために、ディレクトリの内容を一覧表示するユーティリティを含めるべきである。このようなユーティリティは、ほぼすべての OS に含まれている。たとえば、UNIX システムでは **ls** コマンドが使われ、Windows システムでは **dir** コマンドが使われる。

- **文字列検索**。テキスト文字列検索を実行するためのユーティリティは、注目すべきデータファイルを識別するのに役立つことがある。UNIX システムには、テキスト文字列検索を実行するための **grep** コマンドが用意されており、Windows システムでもサードパーティ製の **grep** ユーティリティを入手できる[71]。

---

69 fport の詳細については、http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htmを参照のこと。

70 チェックサムユーティリティの詳細については、http://lists.thedatalist.com/pages/Checksum_Tools.htmを参照のこと。

71 grep の Windows バージョンの 1 つがhttp://unxutils.sourceforge.net/で入手できる。

- **テキストエディタ**。簡単なテキストエディタは、テキストファイルを表示したり、メモを作成したりするのに役立つことがある。Windows システムの**メモ帳**（**Notepad**）や UNIX システムの **vi** など、数多くのテキストエディタが存在する。

5.2.1.3 データ収集の優先順位付け

ツールキットを使って収集すべき揮発性データの種類は、具体的なニーズによって異なる。たとえば、ネットワーク侵入が疑われる場合は、ネットワーク構成情報、ネットワーク接続、ログインセッション、および実行中のプロセスを収集しておくと、侵入者がどのようにシステムにアクセスできるようになったかを知るのに役立つ可能性がある。調査の対象がなりすましの場合は、RAM の内容、実行中のプロセスのリスト、開いているファイルのリスト、ネットワーク構成情報、ネットワーク接続などから、社会保障番号やクレジットカード番号、データを取得または暗号化するために使われたプログラム、パスワードハッシュ、ネットワーク経由で情報を入手するために使われた可能性がある手法などが明らかになる可能性がある。疑わしい場合は、一般的に、できるだけ多くの揮発性データを収集するのが賢明である。コンピュータの電源を切ると、そのようなデータを収集できるあらゆる機会が失われるからである。収集したどの揮発性データを調査するべきかについては、あとで決めることができる。揮発性データの収集に一貫性を持たせるには、ツールキット CD に自動化スクリプトを収録して使用するとよい。このスクリプトには、収集した情報をローカルの記憶媒体（USB ドライブなど）やネットワーク接続されたドライブに転送する手段を含めることができる。

揮発性データは、時間の経過に伴って変化する傾向があるため、揮発性データを収集する際の順序と時系列が重要である。ネットワーク接続はタイムアウトしたり切断されたりする可能性があり、システムに接続するユーザのリストはその時々で異なる場合があるため、分析担当者はほとんどの場合、最初にネットワーク接続とログインセッションに関する情報を収集するべきである。ネットワーク構成情報など、変化する可能性が少ない揮発性データはあとで収集するべきである。一般に揮発性データを収集する際の推奨される順序は、最優先のものから順に、次のとおりである。

1. ネットワーク接続
2. ログインセッション
3. メモリの内容
4. 実行中のプロセス
5. 開かれているファイル
6. ネットワーク構成
7. オペレーティングシステム時間

5.2.2 不揮発性 OS データの収集

分析担当者は、揮発性 OS データを取得したあと、多くの場合、不揮発性 OS データを収集するべきである。そのためには、分析担当者はまずシステムをシャットダウンすべきかどうかを決定するべきである。システムのシャットダウンにより、ビットストリームイメージの取得や多くの論理バックアップを実行できるかどうかが左右されるだけでなく、保全される OS データの種類が変わる可能性もある。ほとんどのシステムは、次の 2 つの方法でシャットダウンできる。

- **正常な OS シャットダウンの実行。**ほぼすべての OS には、シャットダウンの選択肢が用意されている[72]。これにより、OS はシステムをシャットダウンする前に、開かれているファイルのクローズ、一時ファイルの削除、(場合によっては)スワップファイルの消去などのクリーンアップ活動を実行できる。正常なシャットダウンは、悪意のある項目が削除されるきっかけになることもある。たとえば、メモリに常駐したルートキットが消えたり、トロイの木馬が悪意のある活動の証拠を削除したりする可能性がある。OS は、通常、システムの管理者または現在のユーザ(現在のユーザに十分な権限がある場合)のアカウントからシャットダウンされる。

- **システムの電源断。**コンピュータの背面から電源コードを抜くこと(およびノート型パソコンやそのほかの携帯機器のバッテリを取り外すこと)により、正常なシャットダウンでは変更または削除される可能性があるスワップファイル、一時データファイル、およびそのほかの情報を保護できる[73]。残念ながら一部の OS では、電源が突然失われると、開かれているファイルなどのデータを破損する可能性がある。また、PDA や携帯電話などの家庭用機器では、バッテリ電源を取り外すと、データが失われる可能性がある[74]。

実行中のシステム上で問題なく収集活動を実行できるツールもあるが、シャットダウンしたシステム上で実行するのが最適なツールもある。後者の場合、分析担当者は各 OS の特性を認識し、OS の標準的な動作と、保全する必要があるデータの種類に基づいてシャットダウン方法を選択するべきである[75]。たとえば、DOS システムや Windows 95／98 システムでは電源を突然切断してもデータが破壊されないため、電源の切断によってデータが保護されるはずである。ほかの OS では、電源が失われると、開かれているファイルや、その時点でアクセス中だったファイルなどのデータが破壊される可能性がある。これらの場合は、一般に正常なシャットダウンが最適である。ただし、スワップファイルや一時データファイルが特に重要である場合や、正常なシャットダウンを何らかのきっかけにする可能性があるルートキット、トロイの木馬、またはそのほかの悪意のあるプログラムがシステムに含まれている場合は別である。(必要に応じて)シャットダウンを実行したあと、分析担当者はセクション 4 で説明した手法を使ってシステムの記憶媒体からファイルシステムのデータを取得するべきである。

コンピュータの電源を切ったあと、証拠として必要な場合は、コンピュータに接続されているすべての構成要素、記憶装置、媒体、および周辺機器の目録を作成してラベル付けするべきである。目録には、可能な限り、モデル番号、シリアル番号、および項目の説明を含めるべきである。さらに、各項目がコンピュータの外部または内部にどのように接続しているかに関する情報(ケーブル接続、ジャンパの設定など)を文書化し、その写真を撮るべきである。これは、分析担当者がユーザのコンピュータ設定を再現するのに役立つ。法律に基づいて証拠が押収されることを考慮して、各項目は、帯電防止バンドを使って取り扱い、項目を破損するおそれがある静電気放電から保護し、適切に封印し(たとえば、箱に入れてテープでしっかりとめるなど)、輸送のためにしっかり梱包するべきである。担当者は、機密扱いの媒体を取り扱う際に帯電防止バンドを着用し、帯電防止バッグやそのほかの特殊な梱包材を使って媒体を保護するべきである。

---

72 たとえば、Windows システムの場合、分析担当者は[スタート]メニューの[シャットダウン]機能を使用できる。

73 コンピュータの電源コードは無停電電源装置(UPS:Uninterruptible Power Supply)に接続されている可能性があるため、壁の電源コンセントから電源コードを抜く方法は推奨されない。

74 このような機器の電源は、多くの場合、継続的に維持する必要がある。機器に定常的に電源がない場合は、機器の電源を切っても、通常は、そのメモリはバッテリ電源によって短期間(最長で数週間、最短で数分間)だけ維持される。重要なデータを含む家庭用機器を長期間保管する場合は、機器のメモリを保護するために電源を維持するべきである。

75 ほとんどの場合、分析担当者は画面をみることによってどの種類の OS が使用されているかを判断できる。たとえば、Windows システムには、ほかの OS にはみられないタスクバーやそのほかのグラフィック要素が使われている。

ファイルシステムのデータを収集したあとは、ツールを使ってファイルシステムから特定の種類のデータを取得できる。通常のファイル（データ、アプリケーション、設定ファイルなど）の取得は比較的簡単であり、これについてはセクション 4 で説明した。以下のリストでは、不揮発性 OS データのそのほかの種類をいくつか示し、それぞれをファイルシステムから取得する際に役立つツールの使用方法を説明している[76]。

- **ユーザとグループ**。オペレーティングシステムは、システムへのアクセス許可を持つユーザとグループのリストを維持している。UNIX システムでは、ユーザとグループは**/etc/passwd** と**/etc/groups** にそれぞれ指定されている。また、**groups** コマンドと **users** コマンドを使って、システムにログオンしているユーザとそれらのユーザが所属するグループを特定できる。Windows システムでは、**net user** コマンドと **net group** コマンドを使ってシステム上のユーザとグループを列挙できる。

- **パスワード**。ほとんどの OS は、ユーザのパスワードに対応するパスワードハッシュをディスク上に保持している。Windows システムでは、サードパーティ製のユーティリティを使って SAM（Security Account Manager）データベースからパスワードハッシュをダンプできる。UNIX システムでは、通常、**/etc/passwd** ファイルまたは**/etc/shadow** ファイルにパスワードハッシュが格納されている。4.3.2 項で説明したように、パスワードクラッキングプログラムを使ってパスワードハッシュからパスワードを抽出できる。

- **ネットワーク共有**。システムによっては、ローカルのリソースをネットワーク経由で共有できる場合がある。Windows システムでは、**SrvCheck** ユーティリティを使ってネットワーク共有を一覧表示できる[77]。ほかの OS にも、同じような情報を提供するサードパーティ製のユーティリティがある。

- **ログ**。ログがテキストファイルに格納されていない場合は、ログ抽出ユーティリティを使用しなければならないことがある。たとえば、Windows システム上では、最近の成功および失敗したログオンの試みに関する情報は、バイナリ形式のログに格納されており、専用のユーティリティを使って取得できる。UNIX システムでは、ほとんどのログエントリが syslog によってテキストファイルに格納されるか、または**/var/log** ディレクトリに格納されるため、ログから情報を取得するのに特別なユーティリティは必要ない[78]。**.log** で終わるファイル名を検索することにより、ほとんどのログファイルを探せる。

分析担当者は、場合によっては BIOS からデータ（システムの日付と時間、プロセッサの種類と速度など）を収集しなければならないこともある[79]。BIOS には主にシステムのハードウェア構成に関する情報が含まれているため、BIOS データの収集は、システム管理者が運用上の問題のトラブルシューティングを行う際に必要になる可能性が最も高い。一般的に、BIOS データを必要とする分析担当者は、まず必要な揮発性データとファイルシステムを収集し、次にシステムを再起動して適切なファンクションキー（通常、起動中の初期画面で示される）を押すことにより、BIOS 設定を表示する。BIOS パスワードが設定されている場合は、分析担当者は BIOS 設定に簡単にアクセスできず、デフォルトのパスワードを推測するか、パスワード保護を迂回しなければならない可能性がある。BIOS パスワードを迂回するには、該当するメーカーのバックドアパスワードを知る、パスワードクラッキングツールを使用する、マザーボード上の該当するジャンパを移動する、CMOS

---

76 この項で説明するツールの一部は、稼働中のシステムからデータを収集する場合にも使用できる。

77 SrvCheck は、Windows Server 2003 リソースキットに含まれている。

78 syslog プロトコルの詳細については、RFC 3164、『*The BSD Syslog Protocol*』（http://www.ietf.org/rfc/rfc3164.txt）を参照のこと。

79 大容量ハードディスクの場合、BIOS に示されるハードディスクドライブの情報は正確でない可能性がある。現在の多くのドライブは LBA（Logical Block Addressing）を使用しているため、BIOS には誤ったドライブジオメトリ情報が表示される。分析担当者は、ハードディスクドライブ自体の物理的なラベルを確認することで正しい情報が得られるはずである。

（Complementary Metal Oxide Semiconductor）バッテリを取り外す（可能な場合）など、さまざまな方法がある。さまざまなシステムがあるため、システムをいたずらに傷つけないように、分析担当者はまずマザーボードのマニュアルの説明に従って、分析するシステムの詳しい特徴を調べるべきである[80]。

5.2.3 データ収集に関する技術的問題

技術的な問題によって OS データの収集が妨げられる可能性もある。セクション 4 では、ファイルシステムに関するいくつかの問題について説明した。この項では、収集に関するそのほかの問題を中心に取り上げ、それらの問題を軽減するために取れる措置（ある場合）に関するガイダンスを提供する。この項の目的は、考えられるすべての問題を網羅的に議論することではなく、一般的な問題に関する基本的な情報をいくつか提供することにある。

- **OS へのアクセス。**分析担当者が簡単に OS にアクセスできず、揮発性データの収集が困難なことがある。たとえば、ユーザがパスワードで保護されたスクリーンセーバを実行したり、システムをロックしたりする可能性がある。このような場合、分析担当者はこのような保護を迂回するか、揮発性 OS データにアクセスする別の方法を見つける必要がある[81]。パスワードで保護されたスクリーンセーバがアクティブになっている場合、分析担当者はシステムの再起動によってスクリーンセーバを迂回できるが、それによってすべての揮発性 OS データが失われる。ホストにバイオメトリックベースの認証（指紋リーダやそのほかのアドオン認証サービスなど）が使用されている場合は、それによって揮発性 OS データへのアクセス時に同じような問題が発生する可能性がある。OS によっては、システムを再起動せずにスクリーンセーバのパスワードを割り出せることをうたったサードパーティ製のユーティリティがある。これらのユーティリティは、通常、CD ドライブの自動実行機能を利用しており、バックグラウンドで自動的に起動し、暗号化されたパスワードを突き止め、それを復号しようとする。

- **ログの変更**。ユーザは、ログ機能を無効にしたり、ログの格納場所がほとんど確保されないようにログ設定を変更したり、ログに偽のイベントを大量に書き込んだりすることにより、ログの有用性を低下させようとすることがある。ログ機能の変更による影響を減らす 1 つの方法は、集中管理されたサーバにログエントリがアーカイブされるようにシステムを設定することである。

- **フラッシュメモリを内蔵したハードディスクドライブ**。分析担当者は、ときどきフラッシュメモリを内蔵したハードディスクドライブを目にすることがある。このフラッシュメモリには、ドライブにアクセスするのに必要なパスワードが含まれている可能性がある。このパスワードは、コンピュータからドライブを取り外したあとも必要である。一般に、分析担当者はドライブにアクセスするためにパスワードを発見、推測、または割り出す必要がある。

- **キー割り当ての変更**。一部のコンピュータでは、個々のキーまたはキーストロークの組み合わせに対する機能割り当てを、当初の目的とは異なる機能を実行するように変更できる。たとえば、Ctrl＋Alt＋Del キーに対して、所期の動作であるシステムの再起動ではなく、コンピュータのハードディスクドライブの完全消去を割り当てることもできる。対象コンピュータのキーボードを使用する分析担当者は、予期しない動作を実行するキーストロークを入力する

---

80 BIOS パスワードの迂回方法の詳細については、http://www.freelabs.com/~whitis/security/backdoor.htmlおよび http://labmice.techtarget.com/articles/BIOS_hack.htmを参照のこと。

81 いくつかの Web サイトに、特定のスクリーンセーバを迂回する方法（既知の OS の脆弱性を利用するなど）が示されている。しかし、OS が不明だったり、ユーザがその脆弱性を取り除いていた場合、そのようなスクリーンセーバの迂回方法はほとんど役に立たない。パスワードに関する一般情報は、Microsoft Knowledge Base の記事『Information About Unlocking a Workstation』（http://support.microsoft.com/kb/q281250/）および『Password Information in Windows XP』という記事（http://www.kellys-korner-xp.com/win_xp_passwords.htm）から入手できる。

可能性がある。キー割り当ての変更の問題を回避するための最善策は、キーボードを使わずにコンピュータからデータを収集することである。たとえば、分析担当者はクロスケーブルを使って対象コンピュータにフォレンジックワークステーションを接続し、フォレンジックワークステーションからスクリプトを実行することができる。

5.3 OS データの検査と分析

検査プロセスを支援するために使用できるさまざまなツールや技法がある。収集されたデータファイルの検査に使用できるツールや技法については 4.3 項で説明したが、その多くは収集された OS データにも使用できる。また、セクション 7 で説明するように、ファイル完全性チェックツールやホスト IDS などのセキュリティアプリケーションは、OS に対する悪意のある活動を識別するのに大いに役立つ可能性がある。たとえば、ファイル完全性チェックツールを使って OS ファイルのメッセージダイジェストを算出し、既知のメッセージダイジェストと比較することにより、侵害されたファイルがないかどうかを判定できる。コンピュータに侵入検知ソフトウェアがインストールされている場合は、OS に対して行われた操作を示すログが保存されている可能性がある。

分析担当者が直面するもう 1 つの問題は、構造化されていないデータを格納した大規模なバイナリデータファイルであるスワップファイルや RAM ダンプの検査である。16 進エディタを使って、これらのファイルを開き、その内容を検査することは可能だが、大規模なファイルでは、16 進エディタを使って手作業で理解可能なデータを突き止めようとするプロセスには、多大な時間がかかる可能性がある。フィルタ処理ツールを使えば、電話番号、人名、電子メールアドレス、Web アドレス、およびそのほかの重要な情報を表している可能性があるテキストパターンや数値を特定することにより、スワップファイルや RAM ダンプファイルの検査プロセスを自動化できる。

分析担当者は、システム上で実行されている特定のプログラムに関する追加情報（そのプロセスの目的やメーカーなど）を収集したいことが多い。分析担当者は、システム上で現在実行されているプロセスのリストを取得したあと、プロセス名を検索することによってそのような追加情報を入手できる。しかし、(悪意のある)ユーザは機能を隠すためにプログラムの名前を変更することがある（トロイの木馬に **calculator.exe** という名前を付けるなど）。したがって、プロセス名の検索は、プロセスのファイルのメッセージダイジェストを算出して比較することにより、ファイルの正体を確認したあとで行うべきである。同様の検索をライブラリファイル（Windows システムの DLL など）に対して行うことにより、どのライブラリが読み込まれ、その代表的な目的が何であるかを知ることができる。

5.2 項で説明したように、分析担当者は複数のファイルシステムを含む何種類もの OS データを収集する可能性がある。それぞれの種類のデータを選り分けて関係する情報を探すプロセスは、多大な時間を要する可能性がある。一般に、分析担当者は、まず精査すべき少数のデータソースを特定し、次にその精査に基づいてほかの予想される重要情報のソースを見つけるのが有益である。また、多くの場合、分析担当者はほかの種類のソース（ネットワークトラフィックやアプリケーション）から得たデータを含めることもできる。セクション 8 では、分析によって OS のデータとほかのソースのデータを相互に関連付ける方法を例示する。

5.4 推奨事項

このセクションに示した OS のデータの使用に関する主な推奨事項は、次のとおりである。

- **分析担当者は、揮発性 OS データを保全するために適切な行動を取ること。**揮発性 OS データを保全する必要があるかどうかを判断する基準をあらかじめ文書化しておくことにより、分析担当者ができるだけ速やかに十分な情報に基づいて判断を下せるようにするべきである。揮発性 OS データの収集に必要な労力が正当化されるかどうかを判断するには、そのような収集に伴うリスクと重要な情報を回復できる可能性とを比較検討するべきである。

- **分析担当者は、揮発性 OS データの収集にフォレンジックツールキットを使用すること。**フォレンジックツールを使用することにより、システムへの影響を最小限に抑え、ツールを変更から保護しながら、正確な OS データを収集できる。分析担当者は、データの収集時に各ツールによってシステムにどのような影響や変更が加わるかを知っておくべきである。
- **分析担当者は、システムごとに適切なシャットダウンの方法を選択すること。**特定の OS をシャットダウンする方法に応じて、保全されるデータや失われるデータの種類が異なる可能性がある。分析担当者は、各 OS の標準のシャットダウン動作を認識しておくべきである。

6. ネットワークトラフィックのデータの使用

分析担当者は、ネットワークトラフィックのデータを使って、ネットワークベースの攻撃や不適切なネットワーク使用を再構成して分析したり、さまざまな運用上の問題をトラブルシューティングしたりできる。ネットワークを介して伝送される通信の内容（電子メールメッセージや音声など）は、調査の裏付けとして収集されることもある。*ネットワークトラフィック*という用語は、ホスト間の有線または無線ネットワークを介して伝送されるコンピュータネットワーク通信を指す[82]。このセクションでは、ネットワークトラフィックの概要を示す。これには、ネットワークトラフィックデータの主なソース（侵入検知ソフトウェアやファイアウォールなど）の説明も含まれる。また、これらのソースからデータを収集するための技法を論じ、このようなデータ収集における潜在的な法律上および技術上の問題を指摘する。セクションの残りの部分では、ネットワークトラフィックのデータを検査して分析するための技法やツールを中心に取り上げる。このセクションの冒頭では、TCP/IP（Transmission Control Protocol/Internet Protocol）の概要を示す。このセクションに示すデータ、ツール、および方法論を理解するためには、TCP/IP の基本知識が必要である。

6.1 TCP/IP の基本

TCP/IP は、ネットワーク通信を提供するために全世界で広く使われている。TCP/IP の通信は、互いに連携する 4 つの層で構成されている。ユーザがネットワーク経由でデータを伝送するとき、データは最上層から中間層を経て最下層まで、各層において情報を追加されながら、渡されていく。最下層が、蓄積されたデータを物理ネットワーク経由で送信すると、そのデータは宛先に対して各層を下から順に渡される。基本的には、ある層で作ったデータは、その下の層において、それよりも大きな入れ物に入れられカプセル化される。TCP/IP の 4 つの層を最上層から最下層の順に図 6-1 に示す。

アプリケーション層。この層は、DNS（Domain Name System）、HTTP（Hypertext Transfer Protocol）、SMTP（Simple Mail Transfer Protocol）など、特定のアプリケーションのためのデータを送受信する。
トランスポート層。この層は、ネットワーク間でアプリケーション層のサービスを伝送するためのコネクション指向またはコネクションレスのサービスを提供する。トランスポート層は、任意で通信の信頼性を保証することもできる。TCP（Transmission Control Protocl）および UDP（User Datagram Protocol）は、一般によく使われるトランスポート層のプロトコルである。
IP（Internet Protocol）層（ネットワーク層ともいう）。この層は、ネットワークを経由するパケットの経路を制御する。IP は、TCP/IP における基礎的なネットワーク層プロトコルである。ネットワーク層においてよく使われるほかのプロトコルには、ICMP（Internet Control Message Protocol）と IGMP（Internet Group Management Protocol）がある。
ハードウェア層（データリンク層ともいう）。この層は、物理ネットワークの構成要素の通信を取り扱う。最もよく知られているデータリンク層のプロトコルは Ethernet である。

図 6-1. TCP/IP の各層

TCP/IP の 4 つの層は、互いに連携してホスト間でデータを伝送する。図 6-2 に示すように、各層は前の層をカプセル化する。6.1.1 項から 6.1.4 項では、これらの層についてさらに詳しく説明し、ネット

[82] 組織にとって重要なほぼすべてのネットワークトラフィックには、TCP/IP プロトコルスイートが使用されているため、このセクションでは TCP/IP ベースの通信のみを取り扱う。しかし、このセクションで説明している原則のほとんどは、ほかの種類のネットワークトラフィックにも適用できる。

ワークフォレンジックに最も関係が深い特徴を示す。6.1.5 項では、各層の相互関係について説明する。

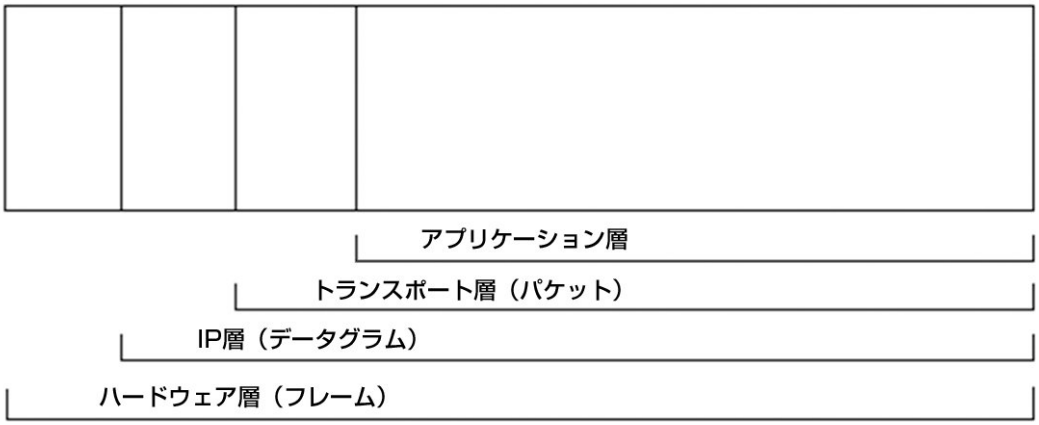

図 6-2. TCP/IP のカプセル化

6.1.1 アプリケーション層

アプリケーション層は、アプリケーションサーバとクライアントとのあいだでデータを伝送することを可能にする。アプリケーション層のプロトコルの例には、HTTP（Hypertext Transfer Protocol）がある。これは、Web サーバと Web ブラウザとのあいだでデータを伝送する。アプリケーション層のほかの一般的なプロトコルには、DNS（Domain Name System）、FTP（File Transfer Protocol）、SMPT（simple Mail Transfer Protocol）、SNMP（Simple Network Management Protocol）などがある。アプリケーション層のよく使われる個別のプロトコルは数百あり、それよりも多くのあまり一般的でないものがある[83]。使われるプロトコルを問わず、アプリケーションデータが生成され、さらなる処理のためにトランスポート層に渡される。セクション 7 では、アプリケーション関連データの収集、検査、および分析を中心に取り上げる。

6.1.2 トランスポート層

トランスポート層は、データをホスト間で伝送できるようにデータをパッケージ化する責任を負う。トランスポート層によってアプリケーションデータがカプセル化された結果として得られる論理単位は「*パケット*」と呼ばれる（接続の最初のネゴシエーション時など、アプリケーションデータなしでパケットが作成される場合もある）。各パケットには、使用されているトランスポートプロトコルの特性を指定するさまざまな「*フィールド*」で構成される「*ヘッダ*」が含まれている。パケットには、アプリケーションデータを保持する「*ペイロード*」が含まれていることがある。

ネットワーク経由で通信するほとんどのアプリケーションは、データを確実に送るためにトランスポート層に依存している。この確実なデータ送信は、一般にトランスポート層のプロトコルである TCP を使って実現される。TCP は、2 つのホスト間の接続を確立し、その接続を介して確実にデータを転送するために最善の努力を行う。TCP の各パケットには、発信元ポートと送信先ポートが含まれている。ポートの 1 つは、一方のシステム上にあるサーバアプリケーションに関連付けられており、もう一方のポートは、他方のシステム上にある対応するクライアントアプリケーションに関連付けられている。クライアントシステムは一般に、アプリケーションで使用するために、利用可能な任意のポート番号を選択するのに対し、サーバシステムは通常、各アプリケーション専用の固定のポート番号を

[83] このため、個々のアプリケーション層プロトコルの詳しい説明はこの文書の範囲を超えている。

持っている。通常、多くのサーバポートは特定のアプリケーションによって使用されるが（ポート 21 は FTP サーバで、ポート 80 は HTTP サーバで使用されるなど）、多くのサーバアプリケーションは任意のポート番号から実行できる。したがって、サーバポート番号だけに基づいて、ネットワークトラフィックに含まれているデータが、そのポート番号に対応するアプリケーションからのデータであると思い込むのは賢明でない。

アプリケーションデータの一部が失われても問題がない場合（ストリーミングオーディオ、ビデオなど）は、UDP（User Datagram Protocol）が一般的に使われる。UDP はコネクションレスであり、あるホストが予備的なネゴシエーションなしで単純に別のホストにデータを送るため、TCP に比べてオーバーヘッドや遅延が少ない。UDP は、データ配信の信頼性を独自に保証するアプリケーション（DNS など）や、ローカルエリアネットワークでの使用に特化したアプリケーション（DHCP（Dynamic Host Configuration Protocol）や SNMP など）でも使用されている。TCP と同じように、UDP の各パケットにも発信元ポートと送信先ポートが含まれている。UDP および TCP のポートはひじょうによく似ているが、互いに異なるものであり、互いを代替することはできない。一部のアプリケーション（DNS など）は、TCP ポートと UDP ポートの両方を使用する。そのようなアプリケーションは、通常、TCP ポートと UDP ポートに同じ番号を使用するが、これは必須ではない。

6.1.3 IP 層

IP 層は、トランスポート層から受け取ったデータのアドレス指定および経路制御を扱う責任を負うため、ネットワーク層と呼ばれることもある。IP ヘッダには、IP Version というフィールドがあるが、これはどのバージョンの IP が使用されているかを示す。一般にこれは IPv4 を示す 4 に設定されているが、IPv6 の使用は増えているので、このフィールドが代わりに 6 に設定されている可能性がある[84]。IP ヘッダのほかの重要なフィールドには、次のようなものがある。

- **発信元および送信先の IP アドレス。**これらは、通信の端点を示すことを目的とした、送信元アドレスと送信先アドレスである[85]。
  IP アドレスの例：10.3.1.70（IPv4）、1000:0:0:2F:8A:400:0427:9BD1（IPv6）。

- **IP プロトコル番号。**これは、IP のペイロードにどのトランスポート層プロトコルが含まれているかを示す[86]。よく使われる IP 番号には、1（ICMP：Internet Control Message Protocol）、6（TCP）、17（UDP）、50（ESP：Encapsulating Security Payload）などがある。

IP 層も、エラー情報およびデータのアドレス指定と経路制御に関係するステータス情報を提供する責任を負う。これは ICMP を使用して行われる。ICMP は、そのエラーメッセージおよびステータスメッセージが送付されたことをまったく保証しないコネクションレスプロトコルである。アプリケーションデータではなく、限定された情報を送信するように設計されているため、ICMP にはポートはない。その代わりに、各 ICMP メッセージの目的を示すメッセージタイプがある[87]。メッセージタイプによっては、メッセージコードがあるものもある。これは、サブタイプであると考えてもよい。たとえば、Destination Unreachable（送信先に到達不能）という ICMP メッセージタイプには、何（ネットワーク、

---

84 ほかのバージョンの IP も可能性としてはあるが、どれも一般的には使われていない。IP Version フィールドの有効な値の正式なリストは、http://www.iana.org/assignments/version-numbers から入手できる。この文書では IPv4 の使用を前提としているが、この文書で説明している技法は IPv6 での使用にも簡単に応用できる（IPv6 に対応する同等のツールが利用可能であることを前提とする）。

85 IP アドレスは、多くの場合、通信の実際の端点を識別するには不正確だったり誤解を招くものであったりする。6.3 項では、この主題についてさらに詳しく説明する。

86 有効な IP プロトコル番号の正式なリストは、http://www.iana.org/assignments/protocol-numbers から入手できる。

87 ICMP の現在有効なタイプのリストは、http://www.iana.org/assignments/icmp-parameters から入手できる。

ホスト、プロトコルなど）が到達不能だったのかを示すメッセージコードの候補がいくつかある。ほとんどの ICMP メッセージは、応答を求めることを目的としていない[88]。

IP アドレスは、間接層を介して使われることが多い。ネットワーク上のリソース(ウェブサーバやメールサーバなど)にアクセスする必要があるユーザは、通常、サーバの IP アドレスではなくサーバの名前（www.nist.gov など）を入力する。この名前は、*ドメイン名*とも呼ばれ、DNS アプリケーション層プロトコルによって IP アドレスに対応付けられる。IP アドレスではなくドメイン名を入力する主な理由は、一般にその方が人間にとって覚えやすいことにある。また、ドメイン名は変わらずに存続し続ける可能性が高いのに対し、ホストの IP アドレスは将来的に変更される可能性がある。ホストをドメイン名で参照すると、それがホストの IP アドレスに対応付けられるため、ホストが現在どのような IP アドレスを使用していても、ユーザはホストに到達できる。

6.1.4 ハードウェア層

ハードウェア層は、その名前が示すとおり、ケーブル、ルータ、スイッチ、NIC などを含む、ネットワークの物理的な構成要素が関係する。ハードウェア層には、各種のハードウェア層プロトコルも含まれ、なかでも Ethernet が最も広く使われている。Ethernet は、MAC アドレスという考え方を利用する。これは、個々の NIC に割り当てられている 6 バイトで構成される一意の固定の値である（例：00-02-B4-DA-92-2C）[89]。個々のフレームには、2 つの MAC アドレスが含まれている。1 つは、当該フレームを転送してきた直前の NIC の MAC アドレスを示し、もう 1 つはフレームの送信先となる次の NIC の MAC アドレスである。フレームが、発信元のホストから送信先のホストに向かう経路上でネットワーク装置（ルータやファイアウォールなど）を経由するたびに、ローカルの発信元と送信先を指すように MAC アドレスが更新される。ハードウェア層の複数の異なる伝送を、単独の IP 層の伝送のなかで互いに結び付けることができる。

各フレームには、MAC アドレスのほかに、フレームのペイロードに含まれているプロトコル（通常は、IP または ARP：Address Resolution Protocol）を示す EtherType 値も含まれている[90]。IP が使用されている場合、それぞれの IP アドレスが特定の MAC アドレスに対応する（複数の IP アドレスが単一の MAC アドレスに対応することが可能なため、MAC アドレスは必ずしも特定の IP アドレスを一意に特定するものではない）。

6.1.5 ネットワークフォレンジックスにおける層の重要性

TCP/IP プロトコルスイートの 4 つの層には、それぞれ重要な情報が含まれている。ハードウェア層は、物理的な構成要素に関する情報を提供し、ほかの層は論理的な側面を記述する。分析担当者は、ネットワーク内の事象に関しては、IP アドレス（IP 層における論理的な識別子）を特定の NIC の MAC アドレス（物理層における物理的な識別子）に対応付けることにより、注目すべきホストを識別できる。IP プロトコル番号（IP 層フィールド）とポート番号（トランスポート層フィールド）の組み合わせによって、どのアプリケーションが使用されていたか、または標的になっていたかを判定できる。これは、アプリケーション層のデータを調べることによって確認できる。

---

88 ICMP は、応答を、特にエラーメッセージに限定するように設計されている。ICMP がこのように設計されていなければ、メッセージの循環が発生する可能性がある。たとえば、ホスト A がホスト B から ICMP エラーメッセージを受け取り、それに対してエラーメッセージで応答し、ホスト B がそのエラーメッセージに対しエラーメッセージで応答したとする。両ホストは、互いにエラーメッセージに対してエラーメッセージを送信し続ける可能性がある。

89 MAC アドレスの先頭の 3 バイトは、NIC のベンダーを示す。マッピングのリストは、http://standards.ieee.org/regauth/oui/oui.txtで入手できる。ただし、MAC アドレスを偽装するようにシステムを設定するさまざまなソフトウェアユーティリティが一般に公開されている。また、メーカーが重複する MAC アドレスを持った NIC を誤って作成したケースもある。

90 0x0800 という EtherType 値は IP を表し、0x0806 は ARP を表す。EtherType 値の詳細については、http://www.iana.org/assignments/ethernet-numbersを参照のこと。

ネットワークフォレンジック分析は、すべての層が対象となる。分析担当者がデータの検査を始めるとき、通常は、限られた情報（ほとんどの場合、注目すべき IP アドレス、および、おそらくプロトコルとポートの情報）しかない。しかし、これだけの情報があれば、一般的なデータソースから詳しい情報を検索するのには十分である。ほとんどの場合、アプリケーション層に、注目すべき実際の活動が含まれている。ほとんどの攻撃はアプリケーション（サービスを含む）の脆弱性を対象としており、ほぼすべての悪用にはアプリケーションの悪用が関与している。活動に関与していた可能性があるホストを特定するためには、分析担当者は、IP アドレスを知る必要がある。これらのホストには、活動の分析に役立つ追加のデータが含まれている可能性もある。注目すべき事象には、一部に例外もあるが（ネットワークの帯域幅を占有するように設計された分散型サービス運用妨害など）、ほとんどの場合、関連するアプリケーションレベルのデータがある。ネットワークフォレンジックスは、アプリケーション層の活動の分析に重要な支援を提供する。

6.2 ネットワークトラフィックのデータソース

各組織には、通常、ネットワークフォレンジックスに役立つ可能性があるネットワークトラフィックに関して、複数種類の情報ソースがある。これらのソースの組み合わせによって、TCP/IP の 4 層すべてから重要なデータが捕捉される。以降の各項では、ネットワークトラフィックデータソースの主な分類（ファイアウォールとルータ、パケットスニファとプロトコルアナライザ、IDS、リモートアクセス、セキュリティ事象管理ソフトウェア、およびネットワークフォレンジック分析ツール）と、そのほかの種類のデータソースに着目する。これらの項では、各ソースの目的、および通常収集されるデータと収集される可能性があるデータの種類について説明する。

6.2.1 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ベースの機器、およびパーソナルファイアウォールなどのホストベースの機器は、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。ファイアウォールとルータは、通常、ほとんどまたはすべての拒否された接続の試みとコネクションレスパケットに関する基本情報をログに記録するように設定されている。なかには、すべてのパケットをログに記録するものもある[91]。ログに記録される情報には、通常、パケットが処理された日付と時刻、発信元と送信先の IP アドレス、トランスポート層プロトコル（TCP、UDP、ICMP など）、およびプロトコルの基本情報（TCP または UDP のポート番号、ICMP のタイプとコードなど）が含まれている。通常、パケットの内容は記録されない。

ネットワークアドレス変換（NAT：network address translation）を行うネットワークベースのファイアウォールとルータには、ネットワークトラフィックに関する貴重な追加データが含まれていることがある。*NAT* とは、あるネットワーク上のアドレスを別のネットワーク上のアドレスにマッピングする処理のことである。これは、ほとんどの場合、内部ネットワークの非公開アドレス[92]をインターネットに接続されているネットワークの 1 つ以上の公開アドレスに対応付けることによって実現される。NAT では、1 つの外部アドレスに対応付けられた複数の内部アドレスを区別するために、内部アドレスごとに異なる発信元ポート番号を対応する外部アドレスに割り当てる。NAT デバイスは、通常、各 NAT アドレスとポートのマッピングを記録する。

ファイアウォールには、プロキシの役割を果たすものもある。*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必要な送信先に送信する。プロキシを使用すると、接続の

---

91 すべてのパケットをログに記録することにより、最近のネットワーク活動に関する情報が、接続や接続の試みに関する情報をログに記録する場合よりも詳しく記録されるが、領域の制約により、短期間しかパケットを保持できない場合もある。また、すべてのパケットを記録するのに必要なオーバーヘッドのためにシステムのパフォーマンスが低下する可能性もある。

92 プライベートアドレスの正式名称は、RFC 1918 アドレスである。RFC 1918、『*Address Allocation for Private Internets*』は、http://www.ietf.org/rfc/rfc1918.txtで入手できる。

試みが成功するたびに実際には 2 つの別々の接続が作成される。1 つはクライアントとプロキシサーバとの接続であり、もう 1 つはプロキシサーバと実際の送信先との接続である。プロキシサーバは、各接続に関する基本情報を記録する可能性がある。多くのプロキシは特定のアプリケーション専用であり、実際に HTTP などのアプリケーションプロトコルの分析や検証を行うものもある。プロキシは、無効だと思われるクライアントの要求を拒否し、それらの要求に関する情報をログに記録する場合もある[93]。

ファイアウォールとルータは、NAT サービスやプロキシサービスを提供するだけでなく、侵入検知や VPN などの機能も実行する場合もある。侵入検知機能と VPN 機能については、6.2.3 項と 6.2.4 項でそれぞれ詳しく論じる。

6.2.2 パケットスニファとプロトコルアナライザ

*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。通常、NIC は明示的にその NIC を送信先とする着信パケットだけを受け付ける。しかし、「*プロミスキャスモード*」に設定されている NIC は、パケットの送信先に関係なく、検知できるすべての着信パケットを受け付ける。一般に、パケットスニファは NIC をプロミスキャスモードに設定することによって機能する。その上で、ユーザ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、特定の発信元 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パケットスニファを設定したりする。パケットスニファは、トラブルシューティングや調査のために特定の種類のトラフィックを捕捉する場合によく使われる。たとえば、IDS の警告によって 2 つのホスト間で異常なネットワーク活動が行われていることが示された場合、パケットスニファを使ってそれらのホスト間で送受信されるすべてのパケットを記録することにより、分析担当者は追加情報を得られる可能性がある。

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でき、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できる[94]。プロトコルアナライザは、通常、稼働中のネットワークのトラフィックだけでなく、以前にパケットスニファによって*キャプチャファイル*に記録されたパケットも処理できる。プロトコルアナライザは、未処理のパケットデータを理解しやすい形式で提示する際にきわめて有用である。プロトコルアナライザについては、6.4 項およびセクション 7 で詳しく論じる。

6.2.3 侵入検知システム

ネットワーク IDS は、疑わしい活動を識別し、関連する情報を記録するために、パケットの傍受とネットワークトラフィックの分析を行う[95]。*ホスト IDS* は、特定のシステムの特性とそのシステムの内部

---

93 一般的なアプリケーションに関してネットワーク周辺部を通過するすべてのネットワークトラフィックを代理で中継するように自組織のネットワークとネットワークセキュリティを設定することにより、個人ユーザがプロキシを迂回しないようにしている組織もある。このような環境では、ネットワークフォレンジックスにとってプロキシサーバのログは特に貴重である。

94 有線ネットワーク用のオープンソースのパケットスニファおよびプロトコルアナライザソフトウェアの例には、Ethereal（http://www.ethereal.com/）、TCPDump（http://www.tcpdump.org/）、WinDump（http://www.winpcap.org/windump/）などがある。Ethereal や Kismet（http://www.kismetwireless.net/）など、無線ネットワーク用のオープンソースソフトウェアも公開されている。そのほかのパケットスニファおよびプロトコルアナライザのソフトウェア製品は、付録 F に示した Talisker Security Wizardry Portal（http://www.networkintrusion.co.uk/protanalyzers.htm）、Softpedia（http://www.softpedia.com/get/Network-Tools/Protocol-Analyzers-Sniffers/）、Packet Storm（http://packetstormsecurity.org/defense/sniff/）、およびそのほかの Web サイトを含め、さまざまな Web サイトに掲載されている。

95 ネットワーク IDS のなかには、管理者が攻撃だけでなく悪用も識別できるようにするものがある。たとえば、管理者は（適切な承認を得た上で）機密に関わるプロジェクトに関連する略語や語句などの注目すべき文字列を使って IDS を

で発生した事象（ネットワークトラフィックを含む）を監視する[96]。特定のネットワークセグメント上のすべてのネットワークトラフィックを監視できるネットワーク IDS センサとは異なり、ホスト IDS ソフトウェアに目的は、そのソフトウェアがインストールされているホストに対するネットワークトラフィックのみを監視することである[97]。IDS ソフトウェアは、通常、疑わしい事象ごとに、ファイアウォールやルータで記録されるのと同じ事象の基本特性（日付と時刻、発信元と送信先の IP アドレス、プロトコル、プロトコルの基本特性など）と、アプリケーション固有の情報（ユーザ名、ファイル名、コマンド、ステータスコードなど）を記録する。IDS ソフトウェアは、活動の考えられる意図を示す情報も記録する。たとえば、攻撃の種類（バッファオーバーフローなど）、標的となった脆弱性、外見上の成功または失敗、攻撃に関する詳細情報の参照先などを記録する[98]。

IDS のなかには、疑わしい活動に関連するパケットを捕捉するように設定できるものがある。これには、IDS が疑わしい活動としてラベル付けするきっかけとなったパケットのみを記録するものから、セッションの残りをすべて記録するものまである。疑わしい活動が検出されたときに、同じセッションのそれまでの活動を保全できるように、すべてのセッションを短期間だけ保存する機能を備えた IDS もある。これらのパケットを捕捉する主な目的は、侵入検知分析担当者が IDS 警告を確認したり、疑わしい活動を調査したりする際に、パケットを精査できるようにすることである。一部の IDS は、*侵入防止*機能も備えており、進行中の攻撃を能動的に阻止しようとする。侵入防止機能が使用されたことは、IDS のログに示されるべきである。

6.2.4 リモートアクセス

*リモートアクセスサーバ*は、VPN ゲートウェイやモデムサーバなど、ネットワーク間の接続を支援する装置である。これには、リモートアクセスサーバ経由で内部システムに接続する外部システムが関係することが多いが、外部システムまたは内部システムに接続する内部システムが含まれることもある。リモートアクセスサーバは、一般に各接続の接続元を記録し、場合によっては各セッションでどのユーザアカウントが認証されたかも示す。リモートアクセスサーバがリモートユーザに IP アドレスを割り当てた場合は、そのこともログに記録される可能性が高い。一部のリモートアクセスサーバは、パケットフィルタリング機能も備えており、通常は 6.2.1 項で説明したファイアウォールやルータと同じようなログ機能を実行する。リモートアクセスサーバは、一般にネットワークレベルで機能するため、多くの異なるアプリケーションの使用に対応している。これらのサーバでは、アプリケーションの機能は認識されないため、通常はアプリケーション固有のデータは記録されない。

各組織は、リモートアクセスサーバに加えて、特定のホストの OS へのリモートアクセスを可能にする特別に設計された複数のアプリケーションを使用することが多い。例としては、セキュアシェル（SSH）、telnet、ターミナルサーバ[99]、リモート制御ソフトウェアなどがある。このようなアプリケーションは、各接続の基本情報（接続元の IP アドレスやユーザアカウントを含む）をログに記録するように設定できることが多い。各組織は一般に、クライアント／サーバアプリケーションなど、リモートから

設定できる。IDS は、ネットワークトラフィックのなかから、それらの文字列のいずれかが使われているファイル転送、電子メール、およびそのほかの形態の通信を検索できる。

96 オープンソースのネットワーク IDS 製品の例には、Bro（http://www.bro-ids.org/）、Snort（http://www.snort.org/）などがある。ネットワーク IDS 製品とホスト IDS 製品の詳細については、Talisker Security Wizardry Portal（http://www.networkintrusion.co.uk/ids.htm）、Honeypots.net（http://www.honeypots.net/ids/products/）、Common Vulnerabilities and Exposures の Web サイト（http://www.cve.mitre.org/compatible/product.html）、および付録 F に示したそのほかの Web サイトを参照のこと。

97 ネットワーク IDS とホスト IDS の詳細については、NIST SP 800-31『*Intrusion Detection Systems*』を参照のこと。この文書は、http://csrc.nist.gov/publications/nistpubs/index.html で入手できる。

98 多くの IDS ベンダーは、それぞれの活動に関する詳細情報を記載したヘルプファイルを提供している。IDS ベンダーは、一般に、CERT®/CC 勧告、CVE（Common Vulnerabilities and Exposures）番号、ソフトウェアベンダーによる脆弱性の公表など、外部の情報源の参照先も提供する。

99 ここでの「*ターミナルサーバ*」は、Microsoft Windows ターミナルサービスや Citrix Metaframe など、オペレーティングシステムやアプリケーションへのグラフィカルリモートアクセスを提供する製品を指す。

アクセスされるアプリケーションも数多く使用する。これらのアプリケーションのなかにも、接続の基本情報をログに記録するものがある。

リモートアクセスに関するログ記録のほとんどは、リモートアクセスサーバやアプリケーションサーバで行われるが、場合によってはクライアントも接続に関する情報をログに記録することがある。

6.2.5 セキュリティ事象管理ソフトウェア

セキュリティ事象管理（SEM：security event management）[100]ソフトウェアは、ネットワークトラフィック関連のセキュリティ事象のさまざまなデータソース（IDS のログ、ファイアウォールのログなど）からセキュリティ事象情報をインポートし、各ソースの事象を相互に関連付ける機能を備えている[101]。一般的な機能として、セキュリティ保護されたチャネルを介してさまざまなデータソースからログのコピーを受信し、ログを標準的な形式に変換し、IP アドレス、タイムスタンプ、およびそのほかの特性を照合することによって関連する事象を識別する。SEM 製品は、一般に、元の事象データを生成しない代わりに、インポートされた事象データに基づいてメタ事象を生成する。多くの SEM 製品は、悪意のある活動（攻撃やウイルス感染など）を識別できるだけでなく、システムとネットワークの悪用や不適切な使用も検出できる。SEM ソフトウェアは、単独のインタフェースを通じて、ネットワークトラフィック情報の多数のソースにアクセスするのに役立つ。

SEM 製品は、OS のログ、ウイルス対策ソフトウェアの警告、物理的なセキュリティ機器のログなど、ほとんどあらゆるセキュリティ事象のデータソースに対応できるため、SEM 製品には事象に関する幅広い情報が取り込まれている可能性がある。しかし、一部のデータフィールドのみが取り込まれるのが一般的である。たとえば、IDS がパケットを記録しても、帯域幅や格納場所の制約から、それらのパケットが SEM に転送されない場合がある。また、ほとんどのデータソースはそれぞれに異なる形式で情報を記録するため、SEM 製品は一般に、各データフィールドを標準的な形式に変換し、一貫した方法でデータをラベル付けすることにより、データを*標準化*する。これは（6.4 項で説明するように）分析には有益であるが、標準化のプロセスによってデータにエラーが入り込んだり、一部のデータが失われたりする可能性がある。幸い、SEM 製品の多くは元のデータソースを改変しないため、分析担当者は元のログのコピーを保持し、データの正確さを検証する必要がある場合はそのコピーを使用するべきである。

6.2.6 ネットワークフォレンジック分析ツール

ネットワークフォレンジック分析ツール（NFAT：network forensic analysis tool）[102]は、通常、パケットスニファ、プロトコルアナライザ、および SEM ソフトウェアを 1 つの製品にまとめたのと同等の機能を提供する。SEM ソフトウェアが既存のデータソース（一般に複数のネットワークトラフィック関連ソースを含む）のあいだの事象の相互関連付けに専念するのに対し、NFAT ソフトウェアでは、ネットワークトラフィックの収集、検査、および分析に重点が置かれている。NFAT ソフトウェアは、ネットワークフォレンジックスをさらに支援する次のような追加機能も備えている。

- 個々のセッション（2 人のユーザ間のインスタントメッセージング（IM：instant messaging）など）から一定期間内のすべてのセッションにいたるまでのさまざまなネットワークトラフィックをツールの内部で再生することにより、事象を再現する。一般的に、再生速度を必要に応じて調整できる。

---

100 SEM ソフトウェアについては、付録 F に示した Web サイト（CVE：Common Vulnerabilities and Exposures の Web サイト（http://www.cve.mitre.org/compatible/product.html）など）を参照のこと。

101 セキュリティ事象管理に対するもう 1 つの一般的な用語は、セキュリティ情報管理（SIM：Security Information Management）である。

102 NFAT ソフトウェアの一覧は、付録 F に示した Talisker Security Wizardry Portal（http://www.networkintrusion.co.uk/fornettools.htm）などの Web サイトから入手できる。

- トラフィックの流れやホスト間の関係を視覚化する。ツールによっては、IP アドレス、ドメイン名、またはそのほかのデータを物理的な場所に結び付け、活動の地理的なマップを作成することもできる。
- 典型的な活動のプロファイルを作成することで、大幅な逸脱を明らかにする。
- アプリケーションの内容からキーワード(「confidential(機密)」、「proprietary(企業秘密)」など)を検索する。

6.2.7 そのほかのソース

ほとんどの組織には、フォレンジックスにある程度役立つ可能性があるネットワークトラフィック情報のソースがほかにも存在する。その例を次に示す。

- **DHCP(Dynamic Host Configuration Protocol)サーバ。**DHCP サービスは、要求に応じてネットワーク上のホストに IP アドレスを割り当てる。ホストのなかには、静的な IP アドレスを持ち、常に同じ IP アドレス割り当てを受けるものもあるが、ほとんどのホストは、通常、動的な割り当てを受ける。これは、ホストがそれぞれの IP アドレス割り当てを定期的に更新する必要があること、および同じホストが同じアドレスを割り当てられる保証はないことを意味する。DHCP サーバには、MAC アドレス、その MAC アドレスに割り当てられた IP アドレス、および割り当てが行われた時間を含む割り当てログが保持されている可能性がある。
- **ネットワーク監視ソフトウェア。**ネットワーク監視ソフトウェアは、ネットワークトラフィックを観察し、その統計情報を収集するように設計されている[103]。たとえば、特定のネットワークセグメントのトラフィックフローに関する概略情報(各種のプロトコルによって通常使用されている帯域幅の量など)を記録することができる。ネットワーク監視ソフトウェアは、各パケットのペイロードのサイズや発信元と送信先の IP アドレスとポートなど、ネットワーク活動に関するより詳しい情報を収集することもある。マネージドスイッチやそのほかのネットワーク機器のなかには、基本的なネットワーク監視機能(帯域幅の使用に関する統計情報の収集機能など)を備えるものがある。
- **インターネットサービスプロバイダの記録。**ISP は、通常業務の一環として、および異常な活動(きわめて大量のトラフィックや、攻撃と考えられる活動など)を調査する際に、ネットワークトラフィック関連のデータを収集することがある。通常の ISP の記録は、数日または数時間程度しか保持されないことが多い。6.3.1 項では、ISP やそのほかの第三者からネットワークトラフィックデータを収集することに関わる法的な考慮事項について論じる。
- **クライアント/サーバアプリケーション。**ネットワーク経由で使用されるクライアント/サーバアプリケーションのなかには、成功または失敗した使用の試みに関する情報を記録するものがある。これらの情報には、クライアントの IP アドレスとポートなど、接続に関連するデータが含まれている可能性がある。記録されるデータフィールドは、(もしあれば)アプリケーションによって大きく異なる。
- **ホストのネットワーク設定とネットワーク接続。**5.1.2 項と 5.2.1 項では、個々のホストから収集できるネットワーク情報の種類(ホストが接続を待機している TCP ポートと UDP ポートを含む)について説明している。

---

[103] オープンソースのネットワーク監視ソフトウェアには、EtherApe(http://etherape.sourceforge.net/)や IPaudit(http://ipaudit.sourceforge.net/)などがある。パケットスニファ、プロトコルアナライザ、および IDS ソフトウェアも、基本的なネットワーク監視機能を実行する場合がある。そのほかの製品名については、付録 F に示した Web サイトを参照のこと。

6.3 ネットワークトラフィックデータの収集

6.2 項で説明したように、各組織は一般に、通常業務中に多くの場所でネットワークトラフィックデータを記録している。各組織は、インシデントを調査したり問題のトラブルシューティングを行ったりするときにも、必要に応じて同じデータ記録の仕組みを使って追加データを収集する。たとえば、ネットワーク管理者やインシデント対応担当者は、ホストが送信した異常なパケットを検査するためにパケットスニファを配備することがある。

ネットワークトラフィックデータは、通常、ログに記録されるか、またはパケットキャプチャファイルに保存される。データの収集は、ほとんどの場合、ログやパケットキャプチャファイルを収集するだけで済むため、簡単である。セクション 4 では、証拠収集の目的に合う形でファイルを収集する方法について説明している。データがファイルに保存されない場合（グラフィカルに表示されるトラフィックフローマップや、コンソール画面にのみ表示されるデータなど）は、画面キャプチャや画面の写真が必要になる可能性がある。ネットワークトラフィックデータの収集は簡単なことが多いが、データの収集を複雑にする可能性がある重要な法的問題および技術的問題がいくつか存在する。

6.3.1 法的な考慮事項

ネットワークトラフィックの収集には、法的な問題が生じる可能性がある。これらの問題の 1 つに、パスワードや電子メールの内容など、プライバシやセキュリティに影響する情報の（意図的または偶発的な）捕捉がある。これによって、収集されたデータを分析しているスタッフのメンバーや、記録システム（IDS センサなど）を管理しているスタッフのメンバーにこれらの情報が暴露される可能性がある。各組織は、機密情報の偶発的な開示への対応に関するポリシーを用意しておくべきである。電子メールやテキスト文書の捕捉に関するもう 1 つの問題は、そのような情報を長期間にわたって保管することが組織のデータ保持ポリシーに違反する可能性があることである。ネットワークの監視に関するポリシーを準備しておき、活動が監視されている可能性があることを示す警告バナーをシステムにおいて表示することも重要である。

ネットワークトラフィックデータの収集は、ほとんどの場合、通常業務の一環として行われるが、トラブルシューティングやインシデント対応の一環として行われることもある。後者の場合、一貫性のあるプロセスに従い、行われたすべての措置を文書化することが重要である。たとえば、特定のユーザによって送受信されたすべてのパケットを記録する場合は、正式な要求と承認のプロセスが問題なく完了したあとで作業を開始するべきである。各組織は、承認なしで実行できる監視の種類とできない監視の種類を明確に説明し、要求と承認のプロセスの詳細を示す手続きを記述または参照するポリシーを設けるべきである。

予想されるもう 1 つの法的な問題は、ログ原本の保護である。6.4 項で説明するように、多くの組織はネットワークトラフィックログのコピーを集中管理された機器に送信するとともに、ネットワークトラフィックを解釈して分析するツールを使用する。ログが証拠として必要とされる場合、コピーや解釈のプロセスの忠実性に疑義が生じた場合に備えて、各組織はログファイルの原本、集中管理されたログファイル、および解釈されたログデータのコピーを収集しておくとよいだろう。6.4 項では、この点について詳しく説明する。

プライバシは、組織にとってより重大な関心事になったため、多くの組織はネットワークフォレンジックデータを含む情報を、ほかの組織と共有することに消極的になった。たとえば、ほとんどの ISP は、自組織のインフィラストラクチャを経由した可能性がある疑わしいネットワーク活動に関する情報を提供するにあたって、裁判所の命令を求めるようになった。これによってプライバシは保護され、ISP の負担と責任は軽減されるが、調査プロセスの進行も遅くなる。これは、組織が、継続中のネットワークベースの攻撃をそのソースまで追跡しようとしているときは特に問題となる（特に、トラフィックが複数の ISP を経由する場合）。

6.3.2 技術的な問題

いくつかの技術的な問題によって、ネットワークトラフィックに関するデータの収集が妨げられることがある。この項では、主な問題のいくつかを説明し、それぞれの問題を軽減するためにできる措置（あれば）に関するガイダンスを提供する。

- **データの格納。**大量のネットワーク活動がある場合、特に有害な事象（攻撃など）の発生中は、短期間に多くの事象がログに記録される。十分な記憶領域が確保されていないと、最近の活動に関する情報が上書きされたり、失われたりする可能性がある。各組織は、通常時およびピーク時のログ使用量を見積もり、何時間分または何日分のデータを保持する価値があるかを判断し、これらの目標に合った十分な記憶領域をシステムやアプリケーションのために確保するべきである[104]。

- **暗号化されたトラフィック。**IPsec（IP Security）、SSH、SSL（Secure Sockets Layer）などのプロトコルを使ってネットワークトラフィックが暗号化されている場合、暗号化されている経路に沿ってネットワークトラフィックを監視している機器は、トラフィックの最も基本的な特性（発信元と送信先の IP アドレスなど）のみを認識する。VPN やそのほかのトンネリング技法が使用されている場合、IP アドレスはトンネル自体のものであり、活動の本当の発信元や送信先ではない可能性がある。復号されたトラフィックに関するデータを収集するには、復号された活動を監視できる場所にデータソースを配置する必要がある。たとえば、IDS センサを VPN ゲートウェイの直前に配置すると、復号された通信に含まれる異常な活動を効率的に識別できる。内部のホストに到達するまでのすべての経路で通信が暗号化されている場合（SSL で暗号化された Web セッションなど）、ネットワークトラフィックを監視している機器は復号されたパケットを見ることができない。各組織は、暗号化する必要がないトラフィックや暗号化すべきでないトラフィックの内容を IDS センサなどのセキュリティ管理策によって監視できるようにするために、トラフィック暗号化技法の適切な使用法を規定するポリシーの確立を検討するべきである。

- **予期しないポートで実行されるサービス。**IDS やプロトコルアナライザなどのアプリケーションは、特定の接続でどのサービスが使用されているかを特定するためにポート番号を利用することが多い。6.1.2 項で説明したように、残念ながらほとんどのサービスは任意のポートで実行できる。予期しないポート番号で実行されるサービスのトラフィックは、適切に捕捉、監視、または分析されない可能性があるため、許可されていないサービスの使用（一般的でないポートでの Web サービスの提供など）が検出されない可能性がある。予期しないポート番号を使用するもう 1 つの動機は、ポート番号に基づいてフィルタ処理を行うネットワーク境界の機器をトラフィックがすり抜けられるようにすることである。予期しないポートの使用を特定する方法は、以下を含め、いくつか存在する。

  – 未知のサーバポートへの接続を検知したら警告するように IDS センサを設定する。

  – プロトコル分析を行うアプリケーションプロキシまたは IDS センサを、予期しないプロトコルを使用する接続（標準の HTTP ポートを使用する FTP トラフィックなど）を見つけたら警告するように設定する。

---

104 各組織は、必要に応じて、コンピュータセキュリティインシデントに関連するログをほかのログより大幅に長い期間にわたって保管するための十分なデータ記憶領域も提供するべきである。たとえば、一般文書保存計画（GRS：General Records Schedule）24、『*Information Technology Operations and Management Records*』は、「コンピュータセキュリティインシデントの対応、報告、および事後措置の記録」を「必要なすべての事後措置が完了してから 3 年後に」破棄するように規定している。GRS 24 は、米国国立公文書館（National Archives and Records Administration、http://www.archives.gov/records-mgmt/ardor/）から入手できる。

  - トラフィックの流れを監視し、新しいトラフィックの流れや異常なトラフィックの流れを特定する。
  - 特定のストリームを別のものとして分析するようにプロトコルアナライザを設定する。

- **代替アクセスポイント。**攻撃者は、主要なアクセスポイント（組織のインターネットゲートウェイなど）を監視しているセキュリティ管理策によって検出されるのを避けるため、代替アクセスポイントからネットワークに入ることが多い。代替アクセスポイントの典型例は、ユーザのワークステーションに接続されたモデムである。攻撃者は、ワークステーションにダイヤルしてアクセスに成功すると、そのワークステーションからほかのホストに対して攻撃を仕掛けることができる。このような場合は、ネットワーク活動がファイアウォール、IDS によって監視されたネットワークセグメント、およびそのほかの一般的なデータ収集ポイントを通過しないため、ネットワーク活動に関する情報がほとんどまたはまったくログに記録されない可能性がある。各組織は一般に、モデムや無線アクセスポイントなどの代替アクセスポイントを制限し、各ポイントをファイアウォール、IDS センサ、およびそのほかの管理策によって監視および規制することにより、この潜在的な問題を解決する。
- **障害の監視。**時折、さまざまな理由（システムの保守、ソフトウェアの障害、攻撃など）でシステムやアプリケーションに障害や機能停止が発生することは、どうしても避けられない。IDS センサなどの監視専用システムの場合は、冗長な装置を使用すること（同じ活動を 2 つのセンサで監視するなど）によって、監視エラーの影響を減らすことができる[105]。もう 1 つの戦略は、ネットワークベースのファイアウォールとホストベースのファイアウォールで接続をログに記録するように設定するなど、複数のレベルで監視を行うことである。

6.4 ネットワークトラフィックデータの検査と分析

注目すべき事象が識別された場合、分析担当者は、何が発生し、組織のシステムやネットワークにどのような影響があったかを判断することを目的として、ネットワークトラフィックデータの評価、抽出、および分析を行う。このプロセスは、1 つのデータソースに関する少数のログエントリを調べ、その事象が誤った警告だったことを確認するだけで簡単に済む場合もあれば、数多くのソース（そのほとんどには関連するデータが含まれていない可能性がある）を 1 つずつ検査して分析し、複数のソースのデータを手作業で相互に関連付けた上で、それらのデータを総合的に分析して事象の予想される意図と重要性を明らかにしなければならないような複雑なものもある。しかし、少数のログエントリを確認するだけの比較的簡単なケースでさえ、驚くほどの労力と時間がかかることがある。

現在のツール（SEM ソフトウェアや NFAT ソフトウェアなど）は、ネットワークトラフィックデータの収集と提示に役立つ可能性があるが、このようなツールは分析機能がやや限られており、十分な訓練を受けた経験豊富な分析担当者でないとうまく使いこなせない。分析担当者は、ツールを理解するだけでなく、ネットワークの動作原理、一般的なネットワークやアプリケーションのプロトコル、ネットワークやアプリケーションのセキュリティ製品、およびネットワークベースの脅威と攻撃手法についても、適度に幅広い知識を持つべきである[106]。分析担当者が、ネットワークアーキテクチャや重要な資産（ファイアウォールや一般に公開されているサーバなど）に使われている IP アドレスなどの組織の環境に関する知識、組織で使用されているアプリケーションや OS をサポートするための情報に関する知識を持っていることも、ひじょうに重要である。分析担当者は、組織全体のシステムやネットワークにおける典型的な使用パターンなど、組織の通常のコンピュータ環境のベースラインを理解していれば、自分の仕事をより簡単かつ迅速に実行できるはずである。分析担当者はまた、ネッ

105 冗長な監視は、ほとんどの組織ではコストがかかるため、特にリスクの高い領域でしか実現できない。

106 分析担当者にとって有益な参考資料には、よく使われるプロトコルとそれらの一般的なポート番号の一覧や、各種の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の標準規格について説明する RFC（Request for Comment）文書などがある。

トワークトラフィックデータソースのそれぞれを確実に理解するとともに、侵入検知シグネチャに関する文書などの補足資料にアクセスできるべきである。分析担当者は、関連するデータをすばやく特定できるように、各データソースの特性と相対的な価値を理解するべきである。

分析プロセスの潜在的な複雑さと、ネットワークトラフィックデータを効果的に分析するのに必要なネットワークや情報セキュリティに関する知識の幅広さを考えると、複雑な状況でデータを分析して結論を導き出すために必要な技法を詳細に説明することは、この文書の範囲を超えている。その代わりに、この項では、検査プロセスと分析プロセスの基本手順に重点を置き、分析担当者が考慮すべき重要な技術的問題を明らかにする。

6.4.1 注目すべき事象を識別する

検査プロセスの最初の手順は、注目すべき事象の識別である。一般に、この識別は次の 2 つの方法のいずれかによって行われる。

- 組織内の誰か（ヘルプデスクエージェント、システム管理者、セキュリティ管理者など）が、セキュリティや運用に関する問題があるという指摘（自動的な警告やユーザの苦情など）を受ける。分析担当者が、該当する活動の調査を依頼される。
- 分析担当者が、通常の業務であるセキュリティ事象データの確認（IDS の監視、ネットワークの監視、ファイアウォールログの確認など）中に、注目すべき事象を識別し、さらに調査すべきであると判断する。

注目すべき事象が識別された場合、分析担当者は、その事象に関する基本情報を調査の基礎として知る必要がある。ほとんどの場合、注目すべき事象は、IDS センサやファイアウォールなどのネットワークトラフィックデータソースを通じて検出されるため、分析担当者はそのデータソースから詳しい情報を入手すれば済む。しかし、ユーザの苦情などの場合は、関連する情報（もしあれば）を含むデータソースや、関与している可能性があるホストまたはネットワークがはっきりしないこともある。したがって、分析担当者は、より一般的な情報（たとえば、4 階のいくつかのシステムが勝手に再起動したという報告）に頼らなければならない可能性がある。事象の情報が具体的（影響を受けたシステムの IP アドレスなど）であればデータの検査も簡単になるが、一般的な情報だけでも、分析担当者が関連するデータソースを見つけるための出発点になる。

6.4.2 データソースを検査する

6.2 項で説明したように、各組織にはネットワークトラフィック関連データのソースが数多く存在する。1 つの注目すべき事象がこれらのデータソースの多くによって指摘される可能性があるが、各ソースを個別に確認するのは非効率的または非現実的である。事象データの最初の検査では、通常、分析担当者は少数の一次データソースを利用する。一次データソースとは、たとえば、すべての IDS センサからの警告を表示する IDS コンソールや、ほかの多くのデータソースを集約してデータを整理する SEM ソフトウェアおよび NFAT ソフトウェアなどである。これは効率的なソリューションであるだけでなく、ほとんどの場合、注目すべき事象はこれらの一次データソースのいずれかの警告によって特定される。

分析担当者は、検査する各データソースについて、その忠実性を考慮するべきである。一般に、分析担当者はほかのソースから標準化（変更）されたデータを受け取るデータソースよりも、元のデータソースを信頼するべきである。また、分析担当者は、解釈に基づくデータ（IDS や SEM の警告など）の妥当性を確認するべきである。悪意のある活動を完全に正確に識別できるツールは存在しない。*フォールスポジティブ*（害のない活動を誤って悪意のあるものとして報告すること）と*フォールス*

ネガティブ(悪意のある活動を誤って害のないものとして分類すること)の両方が発生する[107]。NFAT や IDS などのツールは、接続に含まれるすべてのパケットを処理しない場合、不正確な警告を生成することがある[108]。有効性の確認は、追加データ(未処理のパケットや、ほかのソースによって捕捉された補足情報など)の分析、警告の有効性に関して入手可能な情報(既知のフォールスポジティブに関するベンダーのコメントなど)のレビュー、および問題のツールに関する過去の経験に基づいて行うべきである。多くの場合、経験豊富な分析担当者は、関連データをすばやく検査し、警告がフォールスポジティブであって、それ以上の調査が不要であることを判断できる。

分析担当者は、二次ネットワークトラフィックデータソース(ホストベースのファイアウォールのログ、パケットキャプチャなど)やネットワークトラフィック以外のデータソース(ホスト OS の監査ログ、ウイルス対策ソフトウェアのログなど)も検査しなければならない場合がある。これらの検査を行う最も一般的な理由は次のとおりである。

- **一次ソースにデータがない。**場合によっては、一般的な一次ネットワークトラフィックデータソースに活動の証拠が含まれていないことがある。たとえば、ネットワークセキュリティ機器による監視や管理が行われていない内部ネットワークセグメント上の 2 つのホスト間で攻撃が発生する場合がある。このような場合、分析担当者は、想定されるほかのデータソースを特定し、それらを検査して証拠を見つけるべきである。

- **一次ソースのデータが十分でない、またはデータの有効性が確認されていない。**分析担当者は、一次データソースに十分な情報が含まれていない場合は、二次データソースを検査しなければならない。あるいは、データの有効性を確認しなければならない場合がある。1 つ以上の一次データソースを確認したあと、分析担当者は一次データソースの関連するデータに基づいて、適切な二次データソースを照会するべきである。たとえば、10.20.30.40 という IP アドレスを持つシステムに対して 10.3.0.1 という発信元と思われる IP アドレスから攻撃があったことが IDS の記録からわかった場合は、これらの IP アドレスのいずれかまたは両方を使ってほかのデータソースを照会することにより、この活動に関する追加データが明らかになる可能性がある。分析担当者は、必要に応じて検索範囲を絞るため、タイムスタンプ[109]、プロトコル、ポート番号、およびそのほかの一般的なデータフィールドも使用する。

- **データの最善のソースが別の場所にある。**場合によっては、ネットワークトラフィックデータの最善のソースが、攻撃されたシステム上のホストベースのファイアウォールや IDS のログなど、特定のホスト上に置かれていることがある。これらのデータソースは、ひじょうに役に立つ可能性があるが、攻撃中にそれらのデータが変更または破壊される可能性もある。

追加のデータが必要だが見つからず、疑わしい活動がまだ発生している場合、分析担当者はさらに多くのデータ収集活動を行わなければならない可能性がある。たとえば、分析担当者は、収集情報を増やすためにネットワーク上の適切なポイントでパケットキャプチャを実行してもよい。さらに多くの情報を収集する別の方法には、特定の活動に関してログに記録する情報を増やすようにファイア

---

107 分析担当者の立場からすると、フォールスネガティブの概念は重要である。セキュリティ機器が、観察した攻撃を報告しない場合があることを意味するからである。分析担当者は、セキュリティ機器が、ある活動を悪意のあるものとして報告しなかったからといって、その活動を害のないものとみなすべきでない。

108 すべてのパケットを処理しない理由は、セキュリティ機器の障害(故障、ソフトウェアのバグなど)、セキュリティ機器の過負荷(処理すべきパケットの量が異常に多い場合など)、非同期の経路制御など、いくつか考えられる。非同期の経路制御では、同じ接続の着信パケットと発信パケットが異なる経路を取る。IDS センサなどの機器によってどちらか一方の経路のみが監視されている場合、その機器は接続の一部しか認識できない。

109 4.3.3 項で述べたように、各組織は時刻同期を使ってシステムのクロックの一貫性を維持するべきである。クロックが同期していれば、複数のネットワークトラフィックソース間で事象を相互に関連付けるのは比較的簡単かつ効果的である。事象データのソースが別々の機器にある場合、パケットが使用した経路を確認するのにタイムスタンプが役立つことがある(パケットがネットワークを横断するとき、ある機器から次の機器にパケットが到達するのにいくらかの時間がかかる)。

ウォールやルータを設定したり、該当する活動のパケットを捕捉するように IDS シグネチャを設定したり、特定の活動が発生したときに警告を行うカスタム IDS シグネチャを作成したりする方法などがある。データ収集機能を持つツールに関する追加のガイダンスについては、6.2 項を参照されたい。追加データの収集は、活動が継続中または断続的に続いている場合に役立つ可能性がある。活動が終了していると、追加データを収集する機会はない。

6.4.2.1 データソースの価値

6.2 項で説明したように、各組織には一般にネットワークトラフィックデータのソースが数多く存在する。これらのソースによって収集される情報は多様であるため、分析担当者にとって各ソースの価値は一般的にも特定の場合にも、それぞれに異なる。以下の項目では、ネットワークフォレンジックスにおける最も一般的なデータソースの標準的な価値について説明する。

- **IDS ソフトウェア**。IDS のデータは、疑わしい活動を検査するための出発点になることが多い。IDS は一般に、TCP/IP のすべての層で悪意のあるネットワークトラフィックの識別を試みるだけでなく、事象の有効性を確認する際や、事象をほかのデータソースと相互に関連付ける際に役立つ可能性がある数多くのデータフィールド（および場合によっては未処理のパケット）をログに記録する。しかし、前述のように、IDS ソフトウェアはフォールスポジティブを生成するため、IDS による警告の有効性は確認するべきである。警告の有効性をどの程度確認できるかは、その警告に関連して記録されたデータの量と、警告のきっかけとなったシグネチャの特性や異常検出の方法に関して分析担当者が入手できる情報によって異なる。

- **SEM ソフトウェア**。理想的には、SEM は事象を自動的に複数のデータソース間で関連付け、関連する情報を抽出してそれをユーザに提示できるため、フォレンジックスにとってきわめて有益である。しかし、SEM ソフトウェアはほかの多くのソースからデータを取り込むことによって機能するため、SEM の価値は、どのデータソースからデータが供給されたか、各データソースにどの程度の信頼性があるか、および SEM ソフトウェアがどの程度適切にデータを標準化して事象を関連付けることができるかによって異なる。

- **NFAT ソフトウェア**。NFAT ソフトウェアは、ネットワークトラフィックの分析を支援することを主な目的として設計されているため、注目すべき事象を監視していた場合に価値がある。NFAT ソフトウェアは、通常、トラフィックの再現や視覚化など、分析を支援する機能を備えている。6.2.6 項では、これらの機能について詳しく説明する。

- **ファイアウォール、ルータ、プロキシサーバ、およびリモートアクセスサーバ**。通常、これらのソースのデータは単独ではあまり価値がない。時間の経過を伴うデータを分析することにより、ブロックされた接続の試みの増加など、全体的な傾向がわかることがある。しかし、これらのソースは一般に個々の事象に関する情報をほとんど記録しないため、そのデータからは事象の性質に関する洞察はほとんど得られない。また、毎日数多くの事象がログに記録されるため、その莫大な量のデータに圧倒される可能性がある。これらのデータの主な価値は、ほかのソースで記録される事象を関連付けることにある。たとえば、あるホストが侵害され、ネットワーク IDS センサがその攻撃を検出した場合、攻撃者が使用したと思われる IP アドレスが関係する事象をファイアウォールのログで照会することにより、攻撃がネットワークのどこから入ったかを確認したり、攻撃者が侵害しようとしたほかのホストがわかったりする可能性がある。また、これらの機器によって行われたアドレスのマッピング（NAT など）は、ネットワークフォレンジックスにとっては重要である。攻撃者または攻撃の対象者が使用したと思われる IP アドレスが、実際に数百～数千台のホストによって使われている可能性があるからである。幸い、分析担当者は通常、ログを確認することにより、どの内部アドレスが使われていたかを特定できる。

- **DHCP サーバ。**DHCP サーバは一般に、個々の IP アドレス割り当てとそれに対応する MAC アドレスをタイムスタンプとともにログに記録するように設定できる。これらの情報は、分析担当者が、特定の IP アドレスを使った活動を実行したホストを特定する際に役に立つことがある。しかし、分析担当者は組織の内部ネットワーク上の攻撃者が自分の MAC アドレスや IP アドレスを偽った(*偽装*と呼ばれる操作を行った)可能性があることに留意するべきである。

- **パケットスニファ。**パケットスニファは、すべてのネットワークトラフィックデータソースのなかで、ネットワーク活動に関する情報を最も多く収集できる。しかし、パケットスニファは、害のないデータも大量に(数百万～数千万個のパケットを)捕捉する可能性があり、一般にはどのパケットに悪意のある活動が含まれているかをまったく示さない。ほとんどの場合、パケットスニファは、ほかの機器やソフトウェアが悪意の可能性があるとして識別した事象に関して、より多くのデータを得るために使用するのが最適である。一部の組織は、インシデントの発生時に未処理のネットワークデータを検査や分析で利用できるように、一定期間のパケットをほとんどまたはすべて記録している[110]。パケットスニファのデータは、プロトコルアナライザを使って調べるのが最善である。プロトコルアナライザは、プロトコル標準や一般的な実装の知識に基づいて、分析担当者のためにデータを解釈する。

- **ネットワークの監視。**ネットワーク監視ソフトウェアは、通常のトラフィックの流れからの大幅な逸脱(DDoS 攻撃によって発生するものなど)を識別するのに役立つ。DDoS 攻撃では、数百～数千のシステムが同時に特定のホストやネットワークを攻撃する。ネットワーク監視ソフトウェアは、これらの攻撃がネットワークの帯域幅や可用性に与える影響を文書化できるだけでなく、標的と思われる対象に関する情報も提供する。トラフィックの流れのデータも、ほかのソースによって識別された疑わしい活動を調査する際に役立つ可能性がある。たとえば、過去数日間または数週間以内に特定の通信パターンが発生したかどうかがわかる可能性がある。

- **ISP の記録。**ISP から得られる情報は、主に攻撃の発信元を追跡する際に価値がある(特に、偽装した IP アドレスが攻撃に使われた場合)。6.4.4 項では、この主題についてさらに詳しく論じる。

6.4.2.2 検査と分析のツール

ネットワークフォレンジックスは、何種類ものデータソースに対してさまざまな目的で行えるため、分析担当者は、それぞれが特定の状況に適した複数の異なるツールを日常的に使用する可能性がある。分析担当者は、ネットワークトラフィックデータの検査と分析に対する可能な手法を認識し、あらゆる状況に対して同じツールを適用するのではなく、それぞれのケースで最適なツールを選択するべきである。分析担当者は、ツールの欠点にも留意するべきである。たとえば、特定のプロトコルアナライザが特定のプロトコルを解釈できなかったり、予期しないプロトコルデータ(不正なデータフィールドの値など)を処理できなかったりする可能性がある。同じ不備を持たない代替ツールを利用できるようにしておくと、役に立つことがある。

ツールは、データをフィルタ処理するのに役立つことが多い。たとえば、分析担当者は、検索を絞り込むこむための明確な情報がない状況でデータを検索しなければならない場合がある。このような状況は、分析担当者がセキュリティ事象データのログや警告を定期的または継続的に確認する責任を負っている場合に発生する可能性が高い。ログエントリや警告の数が少ない場合は、データの確認も比較的簡単だが、1 日に数千もの事象が記録される場合もある。手作業によるデータの確認が不可能または非現実的な場合、分析担当者は自動化されたソリューションを使用することによって、事象をフィルタ処理し、重要である可能性が最も高い事象だけが分析担当者に提示されるよう

[110] 多くの NFAT プログラムは、6.2.6 項で説明したように、ほかの機能とともにこの機能を備えている。

にするべきである。確認を効果的に行う技法の 1 つは、ログをデータベースにインポートし、データベースのデータに対してクエリを実行することである。その場合、害のない可能性がきわめて高い活動の種類を除外して残りのデータを確認するか、またはデータを悪意のある可能性が最も高い活動の種類に絞り込む。たとえば、HTTP の活動によってサーバが侵害されたことが最初に疑われる場合は、HTTP の活動以外のすべてを検討対象から除外することからログのフィルタ処理が始まるかもしれない。特定のデータソースを熟知している分析担当者は、一般にそのデータソースに対する盲目的な検索を比較的すばやく実行できるが、よく知らないデータソースでは、特定の種類の活動を検討対象から除外するための基準がほとんどまたはまったくないため、盲目的な検索には多大な時間がかかる可能性がある。

もう 1 つの分析方法は、視覚化ツールを使用することである。視覚化ツールは、セキュリティ事象データをグラフィック形式で提示する。このようなツールは、ネットワークトラフィックの流れを視覚的に表すために最もよく使用され、運用上の問題のトラブルシューティングや悪用の識別を行う際にひじょうに役立つ可能性がある。たとえば、攻撃者は*隠れチャネル*を使用することがある。つまり、秘密裏に情報を伝達するために思いもよらない方法でプロトコルが使用される（たとえば、ネットワークプロトコルのヘッダやアプリケーションのペイロードに特定の値が設定される）ことがある。一般に、隠れチャネルの使用を検出するのは難しいが、有用な方法の 1 つは、予想されるネットワークトラフィックの流れからの逸脱を識別することである。

視覚化ツールは、6.2.6 項で説明したように、NFAT ソフトウェアに含まれていることが多い。視覚化ツールのなかには、トラフィックを再現できるものもある。これらのツールは、タイムスタンプと、連続データフィールドを使って事象の順序を特定し、パケットが組織のネットワークをどのように横断したかをグラフィカルに表示できる。また、一部の視覚化ツールは、ほかの種類のセキュリティ事象データの表示にも使用できる。たとえば、分析担当者は、侵入検知の記録を視覚化ツールにインポートし、発信元や送信先の IP アドレスとポートなど、いくつかの異なる特性に従ってデータを表示できる。さらに、既知の良性な活動の表示を抑制することにより、未知の事象のみを表示することもできる。

視覚化ツールは、特定の種類のデータを分析するのにひじょうに効果的だが、分析担当者はこのようなツールを簡単に習得できないことが多い。通常、ツールにデータをインポートして表示するのは比較的簡単だが、ツールを効率的に使って大規模なデータセットを少数の注目すべき事象に絞り込む方法を習得するには、相当の努力を要する可能性がある。トラフィックの再現は、プロトコルアナライザで行うこともできる。プロトコルアナライザは、一般に視覚化機能を持たないが、個々のパケットをデータストリームに変換し、活動の連続的な前後関係を示すことができる。

6.4.3 結論を導き出す

ネットワークフォレンジックスの最も困難な側面の 1 つは、一般に、利用可能なデータが網羅的でないことである。（ほとんどではないにしろ）多くの場合、一部のネットワークトラフィックデータが記録されず、その結果として失われている。一般に、分析担当者は、分析プロセスを、利用可能なデータと、失われたデータに関する（技術的な知識や知見に基づく）仮定とに基づいて結論を生み出す体系的な手法と考えるべきである。分析担当者は、事象に関して入手可能なすべてのデータを特定して検査するように努めるべきだが、これは、特に冗長なデータソースが数多く存在する場合には、現実的ではないこともある。分析担当者は、事象を再現し、その重大性を理解し、その影響を判定できるだけの十分なデータを最終的に探し出し、その有効性を確認し、分析するべきである。多くの場合、ネットワークトラフィック関連ソース以外のソース（データファイルやホスト OS など）から追加のデータを入手できる。セクション 8 では、分析によってこのようなほかのデータをネットワークトラフィックのデータと相互に関連付けることにより、発生した事象をより正確かつ包括的に理解する方法の例を示す。

一般に、分析担当者は、活動の最も重要な特性を明らかにし、その活動が組織に与えた、または与える可能性があるマイナスの影響を評価することに重点を置くべきである。そのほかの措置（外部攻撃者の身元の特定など）は一般に、多大な時間を要し、達成が難しく、組織が運用上の問題やセキュリティの弱点を是正する助けにはならない。攻撃者の意図を明らかにするのもひじょうに難しい。たとえば、異常な接続の試みは、攻撃者、悪意のあるコード、設定に誤りのあるソフトウェア、誤ったキー入力など、さまざまな要因が考えられる。意図を理解することが重要な場合もあるが、事象のマイナスの影響こそが最大の関心事であるべきである。攻撃者の身元の特定は、特に犯罪活動が行われた場合は、組織にとって重要である可能性があるが、それ以外の場合は、大局的に見て、ほかの重要な目標とのバランスを考慮するべきである。調査の重点は、適切な当事者が最初に決定するべきであり、これらの当事者が攻撃者の身元を特定することが不可欠かどうかを判断する。このような決定に関連するポリシーと手続きを策定するとき、および、特定の状況に関するガイダンスが必要な場合は、法律顧問の助言を求めることが特に重要である。

各組織は、実際の事象の分析だけでなく、誤った警告の原因を理解することにも関心を持つべきである。たとえば、分析担当者は、IDS のフォールスポジティブの根本原因を特定するのに適した立場にいることが多い。分析担当者は、検出の正確さを高めるような変更をセキュリティ事象データソースに対して行うことを推奨するべきである。

6.4.4 攻撃者の特定

ほとんどの攻撃を分析するとき、攻撃者の特定はさしあたっての優先事項ではなく、攻撃を確実に阻止し、システムとデータを復旧することが主な関心事になる。長期にわたるサービス運用妨害攻撃など、攻撃が継続している場合、各組織は攻撃を阻止するために、攻撃者が使用している IP アドレスを特定したがるかもしれない。残念ながら、これは口でいうほど簡単でないことが多い。以下の各項目は、攻撃を行うために使われていると思われる IP アドレスに関わる潜在的な問題について説明する。

- **偽装された IP アドレス。**多くの攻撃には、偽装された IP アドレスが使われる。偽装は、接続を確立する必要がある攻撃で成功させるのはかなり難しいため、接続が不要な場合に最もよく使われる[111]。パケットが偽装される場合、通常、攻撃者は応答に関心がない。ただし、そうでない場合もある。攻撃者は、自身が監視しているサブネットのアドレスを偽装し、そのシステムに応答が送信されたときに、ネットワークから応答を傍受することもできる。偽装が偶然に発生することもある。たとえば、攻撃者がツールの設定を誤り、内部 NAT アドレスを誤って使用した場合などである。攻撃者が特定のアドレスを故意に偽装することもある。たとえば、偽装したアドレスが実際の意図した攻撃標的で、そのとき活動を検出している組織が単に仲介者の役割を果たしている可能性がある。

- **多数の発信者 IP アドレス。**攻撃のなかには、数百～数千の異なる発信者 IP アドレスを使っているようにみえるものがある。この状況が事実を反映している場合もある。たとえば、DDoS 攻撃では、一般に数多くの侵害されたコンピュータを利用して組織的な攻撃が行われる。この状況が架空のものである場合もある。本当の発信者 IP アドレスを攻撃に使用する必要がない場合、攻撃者は多くの異なる偽りの IP アドレスを生成して混乱を増大しようとする。攻撃者が 1 つの本当の IP アドレスと多数の偽りの IP アドレスを使用することもある。その場合、それらの IP アドレスのいずれかを使った攻撃の前後に発生したほかのネットワーク活動を調べることにより、本当の IP アドレスを識別できる可能性がある。一致するアドレスが見つかっても、それが攻撃者のアドレスであるとは限らない。そのときにたまたま組織と通信していた正当な IP アドレスを攻撃者が偶発的にまたは意図的に偽装した可能性もある。

[111] ICMP や UDP などのコネクションレスプロトコルは、最も偽装されやすい。

- **IP アドレスの有効性。**IP アドレスは動的に割り当てられることが多いため、現時点で特定の IP アドレスを持つシステムが攻撃発生時に存在した同じシステムではない可能性がある。また、多くの IP アドレスは、エンドユーザシステムのものではなく、実際の発信者アドレスをそれぞれの IP アドレスに置き換えるネットワークインフラストラクチャ構成要素（NAT を実行するファイアウォールなど）のものである。ユーザのプライバシを守るために、ユーザに代わって活動を行う中間サーバである*アノニマイザ*を使用する攻撃者もいる。

以下に、疑わしいホストの身元の有効性を確認する方法をいくつか示す。

- **IP アドレスの所有者に問い合わせる。**各地のインターネットレジストリ（ARIN：American Registry for Internet Numbers など）[112]は、それぞれの Web サイトで、特定の IP アドレスを所有する（そのアドレスに責任を負う）組織または個人を特定できる WHOIS 検索の仕組みを提供している。この情報は、一部の攻撃を分析するのに役立つことがある。たとえば、疑わしい活動を生成している 3 つの異なる IP アドレスがすべて同じ所有者に登録されていることなどを確認できる。しかし、ほとんどの場合、分析担当者が所有者に直接問い合わせるべきではない。代わりに、所有者に関する情報を分析担当者の組織の管理職層や法律顧問に提供するべきである。管理職層や法律顧問は、該当する組織との接触を始めたり、必要であれば分析担当者にその作業を許可したりできる。このように注意を要するのは、外部組織との情報の共有に関して懸念があるからである。また、IP アドレスの所有者が組織を攻撃している人物である可能性もある。

- **IP アドレスにネットワークトラフィックを送信する。**各組織は、攻撃を行っていると思われる IP アドレスの身元を確認するために、そのアドレスにネットワークトラフィックを送信するべきではない。生成された応答から、攻撃を行っているホストの身元を断定することはできない。さらに、IP アドレスが攻撃者のシステムのものである場合は、攻撃者がトラフィックを検出し、証拠を破壊したり、トラフィックを送信したホストを攻撃したりすることによって対応する可能性もある。IP アドレスが偽装されている場合は、該当するシステムに一方的にネットワークトラフィックを送信すると、不正使用や攻撃として解釈されることもある。いかなる事情があっても、個人が許可なしにほかのシステムにアクセスしようとするべきではない。

- **ISP に支援を求める。**6.3.1 項で述べたように、通常、ISP は疑わしいネットワーク活動に関する情報をほかの組織に提供するにあたって、裁判所の命令を求める。したがって、ISP の支援は、一般に最も深刻なネットワークベースの攻撃を受けた場合だけの選択肢となる。この支援は、IP アドレスの偽装が絡む攻撃に対して特に有効である。ISP には、IP アドレスが偽装されているかどうかに関係なく、継続中の攻撃をその発信元まで追跡する能力がある。

- **IP アドレスの履歴を調査する。**分析担当者は、同じ IP アドレスまたは IP アドレスブロックに関係する過去の疑わしい活動を探すことができる。組織固有のネットワークトラフィックデータアーカイブやインシデント追跡データベースで、過去の活動が見つかることもある。考えられる外部ソースとして、インターネット検索エンジンや IP アドレスによる検索が可能なオンラインインシデントデータベースなどがある[113]。

- **アプリケーションの内容から手がかりを探す。**攻撃に関連するアプリケーションデータパケットに、攻撃者の身元への手がかりが含まれている可能性がある。有益な情報として、IP アドレスのほかに、電子メールアドレス、IRC（Internet relay chat）のニックネームなどがある。

---

112 ARIN の Web サイトはhttp://www.arin.net/にある。そのほかのレジストリは、APNIC：Asia Pacific Network Information Centre（http://www.apnic.net/）、LACNIC：Latin American and Caribbean IP Address Regional Registry（http://lacnic.net/）、および RIPE NCC：Réseaux IP Européens Network Coordination Centre（http://www.ripe.net/）である。

113 一般に公開されているインシデントデータベースの 1 つに、DShield（http://www.dshield.org/）がある。

ほとんどの場合、各組織は攻撃に使われた IP アドレスを積極的に特定する必要はない。

6.5 推奨事項

このセクションに示したネットワークトラフィックデータの使用に関する主な推奨事項は、次のとおりである。

- **各組織は、プライバシと機密情報に関するポリシーを用意すること。**フォレンジックツールやフォレンジック技法を使用すると、分析担当者やフォレンジック活動に関わるそのほかの人々に機密情報が誤って開示される可能性がある。また、フォレンジックツールによって意図せずに捕捉された機密情報を長期間にわたって保管することが、データ保持ポリシーに違反する可能性もある。ポリシーでは、ネットワークの監視についても取り扱い、活動が監視される可能性があることを示す警告バナーをシステムにおいて表示するように求めるべきである。

- **各組織は、ネットワーク活動に関連するログに対して十分な記憶領域を用意すること。**各組織は、通常時およびピーク時のログ使用量を見積もり、組織のポリシーに基づいて何時間分または何日分のデータを保持する価値があるかを判断し、十分な記憶領域をシステムやアプリケーションのために確保するべきである。コンピュータセキュリティインシデントに関連するログは、ほかのログよりはるかに長い期間にわたって保管しなければならない可能性がある。

- **各組織は、情報が収集しやすいようにデータソースを設定すること。**運用上の経験を利用して、組織のフォレンジック分析能力を継続的に向上させるべきである。各組織は、関連する情報の捕捉を最適化するため、データソースの構成設定を定期的に見直し、調整するべきである。

- **分析担当者は、適度に幅広い技術的知識を持つこと。**現在のツールは分析機能がやや限られているため、分析担当者はネットワークの動作原理、一般的なネットワークやアプリケーションのプロトコル、ネットワークやアプリケーションのセキュリティ製品、およびネットワークベースの脅威と攻撃手法について、十分な訓練を受け、経験を積み、豊富な知識を持つべきである。

- **分析担当者は、各データソースの忠実性と価値を考慮すること。**分析担当者は、ほかのソースから標準化されたデータを受け取るデータソースよりも、元のデータソースを信頼するべきである。分析担当者は、データの解釈に基づく異常なデータや予期しないデータ（IDS や SEM の警告など）の有効性を確認するべきである。

- **分析担当者は、一般に事象の特性と影響に重点を置くこと。**攻撃者の身元の特定やほかの同様の措置は、一般に多大な時間を要し、達成が難しく、組織が運用上の問題やセキュリティの弱点を是正する助けにはならない。攻撃者の身元や意図の特定は、特に結果として犯罪調査が行われる場合に重要だが、そのほかの重要な目標（攻撃の阻止、システムやデータの復旧など）とのバランスを考慮するべきである。

（本ページは意図的に白紙のままとする）

7. アプリケーションのデータの使用

電子メール、Web ブラウザ、ワードプロセッサなどのアプリケーションは、コンピュータをユーザにとって有用なものにしている要素である。OS、ファイル、およびネットワークは、すべてアプリケーションをサポートするために必要なものである。OS は、アプリケーションを実行するために必要であり、ネットワークは、アプリケーションデータをシステム間で送信するために必要であり、ファイルは、アプリケーションデータ、構成設定、およびログを保存するために必要である。フォレンジックの観点からは、アプリケーションがファイル、OS、およびネットワークを結び付けている。このセクションでは、アプリケーションのアーキテクチャ(アプリケーションを構成している一般的な構成要素)について説明し、フォレンジックスの対象となる可能性が高いアプリケーションの種類に対する見識を提供する。また、アプリケーションデータの収集、検査、分析に関するガイダンスも提供する。

7.1 アプリケーションの構成要素

すべてのアプリケーションは、実行可能ファイル(および共有コードライブラリなどの関連ファイル)またはスクリプトという形態でコードを含んでいる。多くのアプリケーションは、コードに加えて、構成設定、認証、ログ、データ、補助ファイルなどの構成要素を 1 つ以上持っている。7.1.1 項から 7.1.5 項では、これらの構成要素について詳しく説明し、7.1.6 項ではアプリケーションアーキテクチャの主な種類について論じる。アプリケーションアーキテクチャの種類は、主な構成要素の意図された配置に関連している。

7.1.1 構成設定

ほとんどのアプリケーションでは、ユーザまたは管理者が構成設定を変更することにより、アプリケーションの動作の一部をカスタマイズできるようになっている。フォレンジックスの観点からは、多くの設定項目(背景色の指定など)は問題にならないが、データファイルやログが格納されるホストやディレクトリ、デフォルトのユーザ名など、ひじょうに重要なものもある。構成設定には、一時的なもの(特定のアプリケーションセッション中に動的に設定されるもの)と永続的なものがある。多くのアプリケーションは、すべてのユーザに適用される設定項目を持ち、ユーザ定義の設定項目もサポートしている。構成設定は、以下を含め、いくつかの方法で保存することができる。

- **設定ファイル。**アプリケーションは、テキストファイルまたは独自のバイナリ形式のファイルに設定を保存できる[114]。設定ファイルをアプリケーションと同じホスト上に置く必要があるアプリケーションもあるが、設定ファイルを別のホストに置くことができるアプリケーションもある。たとえば、アプリケーションをワークステーションにインストールし、特定のユーザの設定ファイルをファイルサーバ上のそのユーザのホームディレクトリに保存することもできる。
- **実行時オプション。**一部のアプリケーションは、コマンドラインオプションを使用することにより、実行時に特定の構成設定項目を指定できるようになっている。たとえば、UNIX の電子メールクライアントである **mutt** には、開くメールボックスの場所や設定ファイルの場所を指定するオプションがある。アクティブなセッションで使用されているオプションを識別する方法は、OS やアプリケーションによって異なる。考えられる識別方法としては、アクティブな OS プロセスのリストを確認したり、OS の履歴ファイルを調べたり、アプリケーションのログを確認したりすることなどがある。実行時オプションは、アイコン、スタートアップファイル、バッチファイル、およびそのほかの方法でも指定できる。

[114] たとえば、Windows システムでは、多くの設定項目が Windows レジストリに保存される。Windows レジストリは、本質的には大規模な設定ファイルを集めたものである。

- **ソースコードへの追加。**ソースコードを利用できるようにしているアプリケーション（オープンソースアプリケーションやスクリプトなど）のなかには、ユーザや管理者が指定した構成設定項目をソースコードに事実上直接組み込んでいるものがある。このようなアプリケーションをコンパイル（人間が読めるコードからバイナリの機械可読形式に変換）すると、実際に構成設定項目が実行可能ファイルのなかに取り込まれるため、設定ファイルや実行時オプションで指定する場合に比べて、設定項目へのアクセスがずっと困難になる可能性がある。実行可能ファイル内のテキスト文字列を検索することにより、設定項目を見つけることができる場合もある。

7.1.2 認証

アプリケーションのなかには、アプリケーションを実行しようとしているユーザの身元を確認するものがある。これは、通常、アプリケーションへの不正アクセスを防止するために行われるが、アクセスの問題ではなく、ユーザの身元識別情報に基づいてアプリケーションをカスタマイズできるようにするために行われる場合もある。一般的な認証方法としては、次のようなものがある。

- **外部認証。**アプリケーションは、ディレクトリサーバなどの外部認証サービスを使用することがある。アプリケーションにも認証に関する記録が含まれている可能性があるが、外部認証サービスには、さらに詳細な認証情報が含まれている可能性が高い。
- **独自の認証。**OS ではなくアプリケーションにユーザアカウントとパスワードが含まれるなど、アプリケーションが独自の認証メカニズムを備えている場合がある。
- **パススルー認証。**パススルー認証とは、暗号化されていない OS クレデンシャル（通常はユーザ名とパスワード）を OS からアプリケーションに渡すことを指す。
- **ホスト／ユーザ環境。**管理されている環境（組織内のマネージドワークステーションやマネージドサーバなど）では、一部のアプリケーションが OS によって過去に行われた認証を利用できる可能性がある。たとえば、あるアプリケーションを使用するすべてのホストが同じ Windows ドメインに含まれており、各ユーザがそのドメインによってすでに認証されている場合、そのアプリケーションは OS によって認証された身元識別情報を各ワークステーションの環境から引き出すことができる。その上で、どのユーザにアクセスが許可されたかを追跡し、OS によって認証された身元識別情報と許可されたユーザのリストとを比較することにより、アプリケーションへのアクセスを制限できる。この技法は、ユーザがワークステーション環境で自分の身元識別情報を変更できない場合にのみ有効である。

認証の実装は、環境やアプリケーションによって大きく異なる。このような実装の詳細は、この文書の対象外である。しかし、分析担当者は、ユーザを認証する方法が数多く存在し、そのために、アプリケーションやアプリケーションの実装によってユーザ認証記録のソースが大きく異なる可能性があることを認識するべきである。分析担当者は、（通常は OS によって実施される）アクセス制御を使って特定の種類の情報やアプリケーション機能へのアクセスを制限するアプリケーションがあることも知っておくべきである。この知識は、特定のアプリケーションユーザが実行した操作を知るのに役立つことがある。また、アクセス制御に関する情報（機密に関わる操作の失敗や秘密データへのアクセスの失敗など）を記録するアプリケーションもある。

7.1.3 ログ

一部のアプリケーション（主に、ひじょうに簡単なもの）はログに情報を記録しないが、ほとんどのアプリケーションは何らか形でログへの記録を行っている。アプリケーションは、OS 固有のログ（UNIX システムの syslog、Windows システムのイベントログなど）、テキストファイル、データベース、また

は独自のファイル形式にログエントリを記録する可能性がある。イベントの種類によって記録するログを変えるアプリケーションもある。一般的なログエントリの種類は、次のとおりである。

- **イベント。**イベントログエントリは一般に、実行された操作、各操作が行われた日付と時刻、および各操作の結果を記録する。記録される可能性がある操作の例としては、ほかのシステムへの接続の確立や、管理者レベルのコマンドの発行がある。イベントログエントリには、各操作を実行する際に使われたユーザ名や返されたステータスコード（成功や失敗のステータスだけの場合より詳しい情報が得られる）などの補足情報が含まれることもある。

- **監査。**監査ログエントリは、セキュリティログエントリとも呼ばれ、監査対象の活動（成功および失敗したログオンの試み、セキュリティポリシーの変更、ファイルアクセス、プロセスの実行など）に関する情報を含んでいる[115]。アプリケーションは、OS に組み込まれている監査機能を使用する場合と、監査機能を独自に備えている場合がある。

- **エラー。**一部のアプリケーションは、エラーログを作成する。エラーログには、アプリケーションエラーに関する情報が（通常はタイムスタンプ付きで）記録される。エラーログは、運用上の問題と攻撃のどちらのトラブルシューティングにも役立つ。エラーメッセージは、注目すべきイベントがいつ発生したかを確認する場合や、イベントの特性を特定する場合に役立つことがある。

- **インストール。**アプリケーションは、独立のインストールログファイルを作成することがある。インストールログファイルには、アプリケーションの最初のインストールと以降の更新に関する情報が記録される。インストールログに記録される情報は多種多様だが、インストールの各段階のステータスが含まれることが多い。インストールログから、インストールファイルの提供元、アプリケーションの構成要素が配置された場所、およびアプリケーションの設定にかかわるオプションを示す場合もある。

- **デバッグ。**一部のアプリケーションは、デバッグモードで実行できる。これは、アプリケーションの動作に関して、通常よりもはるかに多くの情報をログに記録することを意味する。デバッグの記録は、ひじょうにわかりにくいものが多く、エラーコードや記録のそのほかの側面を解読できるソフトウェアの作成者にしか意味を成さない場合もある。アプリケーションがデバッグ機能を備えている場合、その機能が有効にされるのは、通常、管理者や開発者が特定の運用上の問題を解決しなければならない場合だけである。

7.1.4 データ

ほぼすべてのアプリケーションは、データの作成、表示、送信、受信、変更、削除、保護、保存など、1 つ以上の方法でデータを処理することを主な目的として設計されている。たとえば、電子メールクライアントでは、ユーザは電子メールメッセージを作成し、それを誰かに送信することができる。また、ほかの誰かから電子メールメッセージを受信し、それを表示したり削除したりできる。アプリケーションのデータは、多くの場合、メモリに一時的に格納され、ファイルに一時的または永続的に格納される。アプリケーションデータを格納するファイルの形式には、汎用的なもの（テキストファイルやビットマップグラフィックなど）と独自仕様のものがある。データは、データベースにも保存される。データベースは、高度に構造化されたファイルとデータ仕様の集合である。一部のアプリケーションは、セッション中に一時ファイルを作成するが、そこにアプリケーションデータが含まれる場合もある。アプリケーションが適切に終了しなかった場合、媒体上に一時ファイルが残ることがある。ほとんどの OS には、一時ファイル用に指定されたディレクトリがあるが、アプリケーションによっては独自の一時ディレクトリを持つものや、データを保存するディレクトリに一時ファイルも格納するものがある。アプリ

[115] ログオンの試みを別の認証ログに記録するアプリケーションもある。認証の詳細については、7.1.2 項を参照のこと。

ケーションにデータファイルのテンプレートやサンプルデータファイル（データベースや文書など）が含まれる場合もある。

7.1.5 補助ファイル

アプリケーションには、多くの場合、文書やグラフィックなど、1 つ以上の種類の補助ファイルが含まれている。補助ファイルは、内容が変化しないことが多いが、だからといってフォレンジックスにとって重要でないとはいえない。補助ファイルの種類には、以下のようなものがある。

- **文書。** これには、管理者マニュアルとユーザマニュアル、ヘルプファイル、ライセンス情報などが含まれる。文書は、分析担当者にとっていろいろな意味で有用である。たとえば、文書では、アプリケーションの機能、アプリケーションの仕組み、アプリケーションの構成要素などが説明されている。文書には、一般に、アプリケーションのベンダーの連絡先情報も記載されている。ベンダーは、質問に回答したり、アプリケーションの理解を助けるそのほかの手段を提供したりできる可能性がある。

- **リンク。** *リンク*は、*ショートカット*とも呼ばれ、ほかの要素（実行可能ファイルなど）を参照するポインタである。リンクは、Windows システムで頻繁に使用される。たとえば、[スタート]メニューに登録されている項目は、実際にはプログラムへのリンクである。リンクのプロパティを調べることにより、分析担当者はそのリンクによってどのようなプログラムが実行され、そのプログラムがどこにあり、どのようなオプションが（あれば）設定されているかを特定できる。

- **グラフィック。** グラフィックファイルには、アプリケーションが使用する独立したグラフィックや、アイコン用のグラフィックが含まれている可能性がある。アプリケーションのグラフィックは、一般に分析担当者にとってあまり重要なものではないが、アイコンのグラフィックは、どの実行可能ファイルが実行されていたかを知るのに重要である可能性がある。

7.1.6 アプリケーションアーキテクチャ

すべてのアプリケーションは、何らかのアーキテクチャを持っている。アーキテクチャとは、アプリケーションの構成要素の論理的な区分と構成要素間で使われる通信メカニズムを指す。ほとんどのアプリケーションは、以下の 3 つの主要なアプリケーションアーキテクチャの分類のいずれかに従って設計されている。

- **ローカル。** ローカルアプリケーションは、アプリケーションの大部分が 1 つのシステムに含まれるように意図されている。コード、構成設定、ログ、および補助ファイルは、ユーザのシステム上に配置される。ローカルアプリケーションが認証を行うことはほとんどない。アプリケーションデータは、ユーザのシステムまたは別のシステム（ファイルサーバなど）に格納され、通常、複数のユーザが同時に変更することはできない。ローカルアプリケーションの例としては、テキストエディタ、グラフィックエディタ、およびそのほかの生産性スイート（ワードプロセッサやスプレッドシートなど）がある。

- **クライアント／サーバ。** クライアント／サーバアプリケーションは、複数のシステム間に分割されるように設計されている。2 層クライアント／サーバアプリケーションは、そのコード、構成設定、および補助ファイルを各ユーザのワークステーションに格納し、そのデータをすべてのユーザがアクセスする 1 つ以上の中央サーバに格納する。ログは、ほとんどの場合、ワークステーションにのみ格納される。3 層クライアント／サーバアプリケーションは、ユーザインタフェースをアプリケーションの残りの部分から分離し、データもほかの構成要素から分離する。標準的な 3 層モデルでは、ユーザインタフェースのコードは（一部の補助ファイルとともに）クライアントワークステーションに置かれ、残りのアプリケーションコードは、アプリケーションサーバに置かれ、データはデータベースサーバに置かれる。Web ベースのアプリ

ケーションの多くは、Web ブラウザ、Web サーバ、アプリケーションサーバ、およびデータベースサーバの 4 層モデルを使用する。各層は隣接する層とだけ通信するため、3 層モデルと 4 層モデルでは、クライアントはデータベースサーバと直接通信しない。一般的なクライアント／サーバアプリケーションの例としては、医療記録システム、電子商取引アプリケーション、および在庫システムがある。

- **ピアツーピア。**ピアツーピアアプリケーションは、個々のクライアントホストが相互に通信し、データを共有するように設計されている。通常、クライアントは最初に、ほかのクライアントに関する情報を提供する集中管理されたサーバと通信する。次に、この情報を使って、集中管理されたサーバを経由する必要がない直接接続を確立する。ピアツーピアアプリケーションの例としては、特定のファイル共有プログラム、チャットプログラム、および IM プログラムがある。ただし、この種のプログラムの一部は、一般にはピアツーピアと呼ばれているが、実際にはクライアントが相互に直接通信せずに集中管理されたサーバと通信するため、クライアント／サーバである。

ほとんどのアプリケーションは、アーキテクチャに関してきわめて柔軟である。たとえば、多くのクライアント／サーバアプリケーションは、1 つのシステムに複数の層をインストールできる。特にアプリケーションのデモやテストの実行時には、すべての層が 1 つのシステムにインストールされる可能性がある。一方、ローカルアプリケーションのなかには、一部の構成要素をローカルシステムに置き、一部をリモートシステムに置くことで、複数のシステムに分割できるものがある。アプリケーションは、さまざまな構成要素のインストール先や、データおよび設定ファイルの格納先を簡単に指定できるようになっていることが多い。多くのアプリケーションには、多種多様な配備方法が存在する可能性がある。

複数のホストにコードを分割するように設計されているアプリケーションは、通常、ホスト間の通信にアプリケーションプロトコルを使用する[116]。電子メールや Web など、広く普及している種類のアプリケーションは、異なる構成要素間の相互運用性を高めるため、既知の標準化されたアプリケーションプロトコルを使用する。たとえば、ほぼすべての電子メールクライアントプログラムは、ほぼすべての電子メールサーバプログラムと互換性があるが、これは各プログラムが同じアプリケーションプロトコル標準に基づいているためである。しかし、標準に基づくプログラムは、特に標準が詳細までを完全に規定していない場合、独自の機能を追加したり、何らかの方法で標準に違反したりすることがある。ほかのアプリケーションとの相互運用性が問題にならず（または望まれておらず）、同じ者がすべてのアプリケーション構成要素を作成している場合は、標準外のプロトコルが使われることが多い。

7.1 項を通して説明してきたように、アプリケーションは連係して動作する構成要素を数多く持っている可能性がある。また、アプリケーションはほかの 1 つ以上のアプリケーションに依存している可能性がある。たとえば、多くの電子商取引アプリケーションのクライアントは、Web ブラウザの内部で動作する。多くのアプリケーションは、印刷や（アプリケーションサーバやそのほかのデバイスの IP アドレスを見つけるための）DNS 検索などの OS サービスも利用している。アプリケーションの複雑さは、電卓のような簡単なユーティリティプログラムから、何千もの構成要素が関係し、何百万人ものユーザをかかえる大規模な商取引アプリケーションまで、さまざまである。

7.2 アプリケーションの種類

アプリケーションは、考えられるほぼすべての目的に対して存在している。フォレンジックの技法はどのアプリケーションにも適用できるが、電子メール、Web 利用、双方向メッセージング、ファイル共

[116] すべてのコードを 1 つのホストに保持するように設計されているアプリケーションは、通常、アプリケーションプロトコルを必要としない。

有、文書の使用、セキュリティアプリケーション、データ隠蔽ツールなど、特定の種類のアプリケーションがフォレンジック分析の対象になる可能性が高い。ほぼすべてのコンピュータには、これらの種類に該当するアプリケーションが少なくともいくつかはインストールされている。以降の各項では、これらの種類のアプリケーションについてそれぞれ詳しく説明する。

7.2.1 電子メール

電子メールは、人々が電子的に通信するための有力な手段になった。個々の電子メールメッセージは、ヘッダと本文で構成される。電子メールの*本文*は、メモや私信など、メッセージの内容そのものである。電子メールの*ヘッダ*には、電子メールに関する各種の情報が含まれている。ほとんどの電子メールクライアントアプリケーションは、デフォルトで各メッセージのヘッダフィールドを一部だけ表示する。たとえば、送信者と受信者の電子メールアドレス、メッセージが送信された日付と時刻、メッセージの件名などである。しかし、通常、ヘッダにはほかにも以下を含むさまざまなフィールドがある[117]。

- メッセージ ID
- メッセージを作成するために使われた電子メールクライアントの種類
- 送信者が指定したメッセージの重要度（低、中、高など）
- 経路制御情報（メッセージの転送中に、メッセージがどの電子メールサーバを通過し、各サーバがいつメッセージを受信したか）
- メッセージのコンテンツタイプ（電子メールの内容が、テキストの本文だけで構成されているのか、添付ファイルや埋め込みグラフィックなども含むのかを示す）

電子メールクライアントアプリケーションは、電子メールの受信、保存、読み取り、作成、および送信を行うために使用される。ほとんどの電子メールクライアントには、電子メールアドレス、名前、電話番号などの連絡先情報を保持できるアドレス帳も用意されている。電子メールの本文、添付ファイル、またはその両方を暗号化するために、暗号化プログラムを電子メールクライアントと組み合わせて使用することがある。

ユーザが電子メールを送信すると、その電子メールは SMTP を使って電子メールクライアントからサーバに転送される。電子メールの送信者と受信者が異なる電子メールサーバを使用している場合、その電子メールは SMTP によってほかの電子メールサーバを経由しながら受信者のサーバに到達するまで転送される。一般に、受信者は別のシステム上の電子メールクライアントを使用し、POP3（Post Office Protocol 3）または IMAP（Internet Message Access Protocol）を使って電子メールを取得する。電子メールクライアントが送信先サーバ上に存在する場合もある（マルチユーザ UNIX システムなど）。送信先サーバは、電子メールの取り込みを可能にする前に、電子メールのチェックを行うことが多い。たとえば、不適切な内容を持つメッセージ（スパムやウイルスなど）のブロックなどを行う。1 つの電子メールメッセージに関する情報は、送信端末から受信端末までの複数の場所に記録される可能性がある。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、情報が記録される可能性がある[118]。

---

117 ほとんどの電子メールクライアントには、電子メールヘッダをすべて表示するのか一部だけ表示するのかを指定する構成設定項目がある。

118 電子メールサービスの詳細については、NIST SP 800-45『電子メールセキュリティガイドライン（*Guidelines on Electronic Mail Security*）』（http://csrc.nist.gov/publications/nistpubs/index.html からダウンロードできる）を参照のこと。

7.2.2 Web 利用

ユーザは Web ブラウザを介して Web サーバにアクセスする。Web サーバには、考えられるほぼすべての種類のデータが含まれている。多くのアプリケーションには Web ベースのインタフェースも用意されており、やはりこれらも Web ブラウザを介してアクセスする。Web ブラウザは、ひじょうに多目的に使用できるため、最もよく使用されるアプリケーションの 1 つである。Web 通信の基本となる標準は HTTP であるが、HTTP にはさまざまな標準形式や独自形式で多くの種類のデータを含めることができる。HTTP は、基本的には Web ブラウザと Web サーバのあいだでデータを転送するための仕組みである[119]。

一般に、Web 利用に関する情報を最も多く含むソースは、Web ブラウザを実行しているホストである。Web ブラウザから取得できる情報として、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（タイムスタンプを含む）、キャッシュされた Web データファイル、Cookie（作成日と有効期限を含む）などがある。Web 利用情報のもう 1 つの有用なソースは、Web サーバである。Web サーバには、通常、受信した要求のログが保存されている。Web サーバが各要求に関してログに記録することが多いデータとしては、タイムスタンプ、IP アドレス、Web ブラウザのバージョン、要求を行ったホストの OS、要求の種類（データの読み取り、データの書き込みなど）、要求されたリソース、ステータスコードなどがある。各要求に対する応答には、要求の成功または失敗を示す 3 桁のステータスコードが含まれている。要求が成功した場合のステータスコードは、どのような操作が行われたかを示し、失敗した場合のステータスコードは、要求が失敗した理由を示す。

Web ブラウザや Web サーバのほかにも、いくつかの種類の機器やソフトウェアによって、関連する情報のログが記録される場合がある。たとえば、Web プロキシサーバやアプリケーションのプロキシ処理を行うファイアウォールは、Web サーバのログと同レベルの詳細な HTTP 活動ログ記録を行うことがある[120]。ルータ、プロキシ処理を行わないファイアウォール、およびそのほかのネットワーク機器は、発信元と送信先の IP アドレスおよびポートなど、HTTP ネットワーク接続の基本的な側面をログに記録することがある。Web コンテンツの監視やフィルタリングのサービスを使用する組織では、それらのサービスのログから（特に、拒否された Web 要求に関する）有用なデータが見つかる可能性がある。

7.2.3 双方向通信

送信者から受信者まで到達するのに通常数分かかる電子メールメッセージとは異なり、双方向通信サービスはリアルタイム（または準リアルタイム）通信を提供する。双方向通信のためによく使われるアプリケーションの種類としては、以下のようなものがある。

- **グループチャット。**グループチャットアプリケーションは、多数のユーザが同時にメッセージを共有できる仮想的な会議空間を提供する。グループチャットアプリケーションは、通常、クライアント／サーバアーキテクチャを使用する。最も人気のあるグループチャットプロトコルである IRC（Internet Relay Chat）は、比較的簡単なテキストベースの通信を使用する標準のプロトコルである[121]。IRC は、ユーザがファイルを送受信するための仕組みも備えている。

---

119 最新の HTTP 標準の詳細については、RFC 2616『*Hypertext Transfer Protocol—HTTP/1.1*』（http://www.ietf.org/rfc/rfc2616.txt）を参照のこと。また、Web サービスの詳細については、NIST SP 800-44『*Guidelines on Securing Public Web Servers*』を参照のこと。この文書は、http://csrc.nist.gov/publications/nistpubs/index.html からダウンロードできる。

120 通常、プロキシは SSL や TLS で保護された HTTP 要求の詳細をログに記録できない。これは、要求とそれに対応する応答が暗号化され、それらの内容が隠蔽された状態でプロキシを通過するためである。

121 IRC の元の標準規格については、RFC 1459、『*Internet Relay Chat Protocol*』（http://www.ietf.org/rfc/rfc1459.txt）を参照のこと。RFC 2810～2813 には、RFC 1459 を補足する追加情報が記載されている。

- **インスタントメッセージングアプリケーション。**IM アプリケーションには、ユーザが相手に直接テキストメッセージやファイルを送信できるピアツーピア型と、集中管理されたサーバを介してメッセージやファイルを受け渡すクライアント／サーバ型がある。IM アプリケーションの構成設定には、ユーザ情報、ユーザの通信相手となるユーザのリスト、ファイル転送情報、およびアーカイブされたメッセージまたはチャットセッションが含まれている可能性がある。インターネットベースの主な IM サービスはいくつかあるが、そのいずれもが独自の通信プロトコルを使用している。いくつかの企業は、組織の内部で動作するエンタープライズ IM 製品も提供している。このような製品は、多くの場合、組織の電子メールサービスにある程度統合されており、認証された電子メールユーザだけが使用できる。

- **オーディオとビデオ**。ネットワークの容量が増加し続けているため、コンピュータネットワーク経由でリアルタイムのビデオやオーディオの通信を行うことが一般的になってきた。VoIP（Voice over IP）などの技術により、ユーザは電話による会話をインターネットなどのネットワーク経由で行えるようになった[122]。オーディオについては、全面的にコンピュータベースのサービスを提供する実装もあるが、中間サーバによってコンピュータネットワークと標準的な電話網とのあいだで通信を変換する部分的なコンピュータベースの実装もある。オーディオ技術の多くは、主にピアツーピアアプリケーションである。ビデオ技術は、テレビ会議を開催したり、2 ユーザ間の「テレビ電話」通信を行ったりするために使用できる。オーディオやビデオの通信によく使われるプロトコルとしては、H.323 や SIP（Session Initiation Protocol）がある[123]。

7.2.4 ファイル共有

ユーザは、さまざまなプログラムを介してファイルを共有できる。前述のように、電子メール、グループチャットプログラム、および IM ソフトウェアは、いずれも特定のファイルを送受信する機能を備えている。しかし、これらのプログラムでは、一般に受信者がファイルを閲覧したり転送するファイルを選択したりすることはできない。このレベルの機能には、本格的なファイル共有のプログラムとプロトコルが必要である。ファイル共有プログラムは、アーキテクチャ別に次のように分類できる。

- **クライアント／サーバ型。**従来からあるファイル共有サービスでは、クライアント／サーバアーキテクチャが使用され、中央のファイルサーバにファイルのリポジトリがある。クライアントがサーバを使用するには、サーバへの接続を開始し、（必要な場合は）サーバに対して認証を行い、（必要な場合は）利用可能なファイルのリストを確認し、サーバとのあいだでファイルを転送する。よく使われるクライアント／サーバ型ファイル共有サービスとして、FTP、NFS（Network File Sharing）、AFP（Apple Filing Protocol）、および SMB（Server Message Block）がある[124]。これらは、入力された認証クレデンシャル（パスワードなど）を含め、転送中のデータの機密性を保護しない標準化されたプロトコルである。SFTP（Secure FTP）や scp（Secure Copy）などのセキュリティ保護された代替プロトコルでは、ネットワーク通信が暗号化される。ほとんどの OS にはファイル共有クライアント（FTP、SMB など）が組み込まれているが、ユーザは同様の機能を備えた各種のサードパーティプログラムをインストールすることもできる。

- **ピアツーピア型。**ほとんどのピアツーピア型ファイル共有サービスは、主に音楽、グラフィック、またはソフトウェアをインターネット経由で交換するために使用される。1 つのサーバにファイルのリポジトリが保持されるクライアント／サーバ型のファイル共有とは異なり、ピアツ

---

122 VoIP の詳細については、NIST SP 800-58『*Security Considerations for Voice Over IP Systems*』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照のこと。

123 SIP の標準規格については、RFC 3261『*SIP: Session Initiation Protocol*』（http://www.ietf.org/rfc/rfc3261.txt）を参照のこと。.

124 SMB の詳細については、http://samba.anu.edu.au/cifs/docs/what-is-smb.html を参照のこと。

ーピア型のファイル共有では、ファイルが多くの異なるホスト上に置かれる分散型である。ピアツーピア型ファイル共有サービスには、通常、クライアント情報（ほかのクライアントがどこにあるか）を提供する中央サーバがあるが、このサーバはファイルやファイル情報の送信には参加しない。ピアツーピア型ファイル共有サービスでは、通常、ユーザ認証が必要ない。ファイルの閲覧や転送は、すべてクライアント（ピア）間で直接行われる。ユーザは、通常、特定のサービスを使用する際のクライアントプログラムを複数のなかから選択できる。ほとんどのサービスでは、各ユーザが各自のシステム上にあるどのファイルを共有するかを制御できるが、暗号化ピアツーピア型と呼ばれるサービスは、各ユーザのハードディスクドライブの暗号化された部分にほかのユーザのファイルを格納し、各自のシステムのその領域に何が保存されるかに関する制御権や情報をユーザに与えないことによって機能する。匿名ピアツーピア型サービスでは、ファイルの本当の発信元や送信先を簡単に特定できないようにするため、要求されたファイルが発信元から送信先に直接送信されず、複数の中間ホストを介して送信される。

7.2.5 文書の使用

多くのユーザは、手紙、報告書、図などの文書作成作業に多くの時間を費やしている。文書には、任意の種類のデータが含まれているため、分析担当者にとって重要である可能性が高い。このような文書を作成、表示、編集するために使われるソフトウェアの種類は、オフィス生産性アプリケーションと呼ばれている。これには、ワードプロセッサ、スプレッドシート、プレゼンテーション、パーソナルデータベースなどのソフトウェアが含まれる。文書には、ユーザやシステムの情報が含まれることが多い。たとえば、文書を作成した人物や文書を直前に編集した人物の名前またはユーザ名、文書を作成するために使ったソフトウェアのライセンス番号やシステムの MAC アドレスなどである[125]。

7.2.6 セキュリティアプリケーション

ホスト上では、多くの場合、電子メールクライアントや Web ブラウザなどのよく使われるアプリケーションを通じて発生する誤用や悪用からホストを保護しようとするセキュリティアプリケーションが 1 つ以上実行されている。よく使われるセキュリティアプリケーションには、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、コンテンツフィルタリング（スパム対策など）、ホストベースの侵入検知ソフトウェアなどがある。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可能性がある。それらの記録から、セキュリティ侵害が発生したかどうかや、セキュリティ侵害が阻止されたかどうかがわかることもある。中央で管理と制御が行われるウイルス対策ソフトウェアなどのセキュリティアプリケーションが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。

7.2.7 データ隠蔽ツール

一部のユーザは、ほかのユーザからデータを隠蔽するツールを使用する。これは、善意の目的（無許可の第三者によるアクセスからデータの機密性と完全性を保護するためなど）で行われる場合と、悪意の目的（不適切な活動の証拠を隠蔽するためなど）で行われる場合がある。データ隠蔽ツールの例としては、ファイル暗号化ユーティリティ、ステガノグラフィツール、システムクリーンアップツールなどがある。システムクリーンアップツールは、特定のアプリケーション（Web ブラウザなど）に関連するデータや一般的な場所（一時ディレクトリなど）にあるデータを削除するための専用ソフトウェアである。データ隠蔽ツールの使用がログに記録されることはほとんどない。分析担当者は、システ

[125] ユーザやシステムの情報を文書内に取り込む可能性があるオフィス生産性アプリケーションの例としては、Microsoft Office がある。この主題の詳細については、Microsoft Knowledge Base の記事 834427（http://support.microsoft.com/default.aspx?scid=kb;en-us;834427）を参照のこと。

ム上にあるこのようなツールを識別し、ツールの影響を認識するために、これらのツールの機能を知っておくべきである。

7.3 アプリケーションデータの収集

7.1 項で説明したように、アプリケーション関連データは、ファイルシステム、揮発性 OS データ、およびネットワークトラフィックのなかに存在する可能性がある。4.2 項、5.2 項、および 6.3 項では、これらの各ソースからのデータ収集に関する具体的な情報を示した。これらのソースに含まれている可能性があるアプリケーションデータの種類は、以下のとおりである。

- **ファイルシステム。**ファイルシステムには、実行可能ファイルやスクリプト、設定ファイル、補助ファイル（文書など）、ログ、データファイルなど、アプリケーションに関連する多くの種類のファイルが含まれている可能性がある。
- **揮発性 OS データ。**揮発性 OS データには、アプリケーションによって使用されるネットワーク接続に関する情報、システム上で実行されているアプリケーションプロセスと各プロセスで使われたコマンドライン引数に関する情報、アプリケーションによって開かれているファイルに関する情報、およびそのほかの関連情報が含まれている可能性がある。
- **ネットワークトラフィック。**最も重要なネットワークトラフィックデータには、リモートアプリケーションへのユーザ接続や、異なるシステム上にあるアプリケーション構成要素どうしの通信が含まれる。そのほかのネットワークトラフィックの記録から追加情報が得られる場合もある。たとえば、アプリケーションからリモート印刷を行うためのネットワーク接続や、アプリケーションクライアントまたはそのほかの構成要素がアプリケーション構成要素のドメイン名を IP アドレスに変換するために行う DNS 検索などがある。

分析担当者は、収集すべきデータを決定する際に、しばしば大きな課題に直面する。多くの場合、分析担当者はまずどのアプリケーションに注目すべきかを決定しなければならない。たとえば、1 つのシステムに複数の 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のは一般的なことである。分析担当者は、あるユーザによる組織の電子メールサービスの使用に関するデータを収集するように求められた場合、そのユーザがそれらのサービスにアクセスするために使用した可能性があるすべての方法に留意する必要がある。たとえば、そのユーザのコンピュータに、電子メールクライアントが 3 種類あり、さらに組織が提供する Web ベースの電子メールクライアントにアクセスするために使用できる Web ブラウザが 2 つあるとする。このユーザのコンピュータに関して、分析担当者はコンピュータからすべてのデータを収集し、どのクライアントが実際に電子メールのために使用されたかを検査プロセスで判定することもできる。ただし、ユーザのコンピュータ以外にも潜在的なデータソースは数多く存在し、それらのソースは使用されたクライアントによって異なる可能性がある。たとえば、Web ベースのクライアントの使用は、Web サーバ、ファイアウォール、IDS、およびコンテンツ監視ソフトウェアのログだけでなく、Web ブラウザの履歴ファイル、Web ブラウザのキャッシュ、Cookie、パーソナルファイアウォールのログにも記録されている可能性がある。状況によっては、必要なデータを収集するために、アプリケーションのすべての構成要素を識別し、（詳しい状況と必要性に基づいて）重要である可能性が最も高い要素を特定し、各構成要素の場所を見つけ、それらの構成要素からデータを収集しなければならない可能性がある。セクション 8 では、アプリケーションの構成要素の識別やデータ収集の優先順位付けの複雑さを説明する例を示す。

7.4 アプリケーションデータの検査と分析

アプリケーションデータの検査と分析は、主にアプリケーションデータの特定部分を調べることによって行われる。アプリケーションデータの特定部分とは、ファイルシステム、揮発性 OS データ、およびネットワークトラフィックであり、それぞれ 4.3 項と 4.4 項、5.3 項、および 6.4 項で説明したツールと

技法を使って調べられる。アプリケーションが特注（ユーザ自身が作成したプログラムなど）であることが検査や分析の妨げになる場合がある。分析担当者が、このようなアプリケーションに関する知識を持っている可能性は少ない。検査について考えられるもう 1 つの問題は、データ暗号化やパスワードなど、アプリケーションベースのセキュリティ管理策を使用することにかかわる。多くのアプリケーションは、このようなセキュリティ管理策を使って、許可されたユーザによる機密データへの不正なアクセスを阻止している。

分析担当者は、複数の異なるアプリケーションデータソースから得られた関連するアプリケーションデータを統合することもある。これは、大部分が手作業によるプロセスである。アプリケーションに関連する事象の詳細な分析や事象の再現には、通常、すべてのソースから得られた情報を理解できる熟練した知識豊富な分析担当者が必要である。このような分析担当者は、個々のアプリケーションデータソースの検査と分析の結果を精査し、情報がどのように互いに当てはまるかを理解することができる。分析担当者の役に立つ可能性があるツールとしては、アプリケーション関連事象を複数のデータソース間で相互に関連付けることができるセキュリティ事象管理ソフトウェア（6.2.5 項で説明）や、特定の種類のログを対象に実行することによって疑わしい活動を識別できるログ分析ソフトウェア（ある種のホストベースの侵入検知ソフトウェアを含む）などがある。セクション 8 では、複数のソースから得たデータを、分析によって相互に関連付けることにより、発生した事象をより正確かつ包括的に把握する方法を示す。

7.5 推奨事項

このセクションに示したアプリケーションのデータの使用に関する主な推奨事項は、次のとおりである。

- **分析担当者は、考えられるすべてのアプリケーションデータソースを考慮すること。**アプリケーションの事象は、多くの異なるデータソースによって記録される可能性がある。また、1 つのシステム上にインストールされた複数のクライアントプログラムや、Web ベースのクライアントインタフェースなど、複数の仕組みを介してアプリケーションが使用される可能性もある。このような状況では、分析担当者はすべてのアプリケーション構成要素を識別し、重要である可能性が最も高い構成要素を決定し、各構成要素の場所を特定し、データを収集するべきである。
- **分析担当者は、さまざまなソースから得られたアプリケーションデータを結び付けること。**分析担当者は、アプリケーション関連事象の詳細な分析や事象の再現を行うために、個々のアプリケーションデータソースの検査と分析の結果を精査し、情報がどのように結び付いているのかを明らかにするべきである。

8. 複数ソースのデータの使用

セクション 4 からセクション 6 では、データファイル、OS、ネットワークトラフィックという 3 種類のデータソースのデータの収集、検査、および分析について説明した。これらのデータを収集、検査、および分析するための技法とプロセスは、データの種類によって根本的に異なる。セクション 7 では、3 種類のデータソースを集約したアプリケーションデータの収集、検査、および分析について説明した。たとえば、多くのアプリケーションは、データファイルを使用し、OS の構成を変更し、ネットワークトラフィックを生成する。コンピュータセキュリティインシデントなど、多くの状況は、複数の種類のデータソースを分析し、ソース間で事象を相互に関連付けることによって最も効果的に処理できる。

このセクションでは、ディジタルフォレンジックスにおいて複数のデータソースを使用する例を 2 つ示す。それぞれの例では、シナリオを説明し、フォレンジック分析に対する具体的なニーズを示し、フォレンジックプロセスがどのように実行されるかを説明する。また、フォレンジックプロセスがどの程度複雑になるかも示す。このセクションでは、以下の 2 つの例を示す。

- どのワームがシステムに感染したかを判定し、ワームの特性を識別する例。
- 脅迫メールに絡むサイバー事象の流れを再現する例。

8.1 ネットワークサービスからのワーム感染の疑い

ある組織のヘルプデスクが、特定のサーバの応答が遅いというユーザからの苦情の電話を矢継ぎ早に受けた。ヘルプデスクは、監視グループに対してトラブルチケットを送信した。監視グループのネットワーク IDS は、最近、このサーバに関係する異常警告を何度か報告しており、警告を精査した分析担当者は、警告が正しいのではないかと考えた。警告に含まれるデータから、何らかの疑わしい活動がこのサーバに対して行われたことと、現在はこのサーバがほかのシステムに対して同じ活動を生成していることがわかった。侵入検知分析担当者の最初の仮説は、ワームが脆弱なネットワークサービスを攻撃し、このサーバに感染し、今度はほかのシステムに感染しようとしている、というものだった。監視グループは、勤務中のインシデント対応担当者に連絡し、このサーバに発生している可能性があるインシデントの調査を要請した。

このインシデント対応担当者がこのインシデントに関して果たすべき役割は、システムに感染したワームの種類を特定し、そのワーム独特の特性を明らかにすることである。この情報は、インシデント対応チームが封じ込め、根絶、復旧の各活動を効果的に行い、組織内のほかのシステムへの感染を防止するために不可欠である。インシデント対応担当者の調査によってインシデントがワーム以外の何かによって発生した可能性があることがわかった場合は、インシデント対応担当者によって明らかにされた特性が、実際に何が発生したかを知るのにとても役立つはずである。

このインシデントに関連する情報は、複数の場所に記録されている可能性がある。インシデント対応担当者はまず、データソースに関する自分のこれまでの経験や、インシデントに関して当初入手できる情報に基づいて、関連する情報が含まれている可能性が最も高いデータソースを確認するべきである。たとえば、ネットワーク IDS センサが疑わしい活動を検出したのだから、同じネットワークセグメントを監視しているほかのネットワークベースのデータソースにも関連する情報が含まれている可能性がある。組織がセキュリティ事象管理ソフトウェアやネットワークフォレンジック分析ツールを使用している場合は、多くの異なるソースからデータが集められているため、インシデント対応担当者は SEM や NFAT のコンソールからいくつかのクエリを実行するだけで必要なすべての情報を収集できる可能性がある。集中管理されたデータソースが利用できない場合、インシデント対応担当者は以下のような攻撃の特性の潜在的なソースを個別に確認するべきである。

- **ネットワーク IDS。**インシデントの最初の報告はネットワーク IDS センサによって生成されたため、ネットワーク IDS のデータのなかに、該当するネットワーク活動の基本特性に関する情報が含まれている可能性が高い。少なくとも、それらのデータから、どのサーバが攻撃され、どのポート番号が使用され、したがってどのネットワークサービスが標的になったかがわかるはずである。サービスを特定することは、悪用された脆弱性を見つけ、ほかのシステムで同じようになインシデントが発生するのを防ぐための軽減策を立てる上で、ひじょうに重要である。分析の観点からは、標的になったサービスとポート番号を知ることも重要である。これらの情報を使って、ほかのデータソース候補を特定し、それらのデータソースから関連する情報を検索できるためである。配備されているネットワーク IDS によっては、ほかにも有用な情報が記録されている可能性がある。たとえば、Web の要求と応答、電子メールのヘッダや添付ファイル名といったアプリケーションデータである。このようなアプリケーションデータには、特定のワームに関連する単語、語句、またはそのほかの文字列が含まれている可能性がある。

- **ネットワークベースのファイアウォール。**ファイアウォールは、通常、ブロックされた接続の試みをログに記録するように設定されている。この記録には、その接続先となるはずだった IP アドレスとポートが含まれている。したがって、ファイアウォールにはブロックされたワームの活動の記録が含まれている可能性がある。ワームのなかには、複数のサービスまたはサービスポートを悪用しようとするものがある。たとえば、ファイアウォールの記録から、ワームが実際に少なくとも 4 つのポート番号に対して接続を確立しようとしたが、そのうち 3 つのポートを使った接続がファイアウォールによってブロックされたことがわかるかもしれない。このような情報は、ワームを識別するのに役立つ可能性がある。ファイアウォールが、許可された接続を記録するように設定されている場合、ファイアウォールのログから、組織内のどのホストがワームのトラフィックを受信したか、あるいは、どのホストがワームに感染して自身のワームトラフィックを生成したかがわかる可能性がある。この情報は、ネットワーク IDS センサがファイアウォールに到達するすべてのトラフィックを監視していない状況では特に有用である。ワームトラフィックが通過した可能性があるほかのネットワーク境界の機器（ルータ、VPN ゲートウェイ、リモートアクセスサーバなど）にも、ネットワークベースのファイアウォールに記録されたのと同じような情報が記録されている可能性がある。

- **ホストの IDS とファイアウォール。**感染したシステム上で実行されている IDS 製品やファイアウォール製品には、ネットワークの IDS 製品やファイアウォール製品よりも詳細な情報が含まれている可能性がある。たとえば、ホスト IDS はワームによってホスト上のファイルや構成設定に加えられた変更を識別できる。この情報は、封じ込め、根絶、復旧の各活動を計画する際にワームがどのようにホストに感染したのかを明らかにするのに役立つだけでなく、どのワームがシステムに感染したかを識別する際にも役立つ。しかし、多くのワームは、ホストベースのセキュリティ管理策を無効化し、ログエントリを破壊するため、IDS ソフトウェアやファイアウォールソフトウェアのデータは限定的なものであるか、または欠落している可能性がある。ログのコピーを集中管理されたログサーバに転送するようにこれらのソフトウェアが設定されていた場合は、これらのサーバを照会することによっていくらかの情報を得られる可能性がある。

- **ウイルス対策ソフトウェア。**脅威がサーバに到達し、サーバの侵害に成功しているため、ネットワークベースまたはホストベースのウイルス対策ソフトウェアに脅威の記録が含まれている可能性は低い。ウイルス対策ソフトウェアがワームを検出していれば、ワームは阻止されていたはずである。しかし、ウイルス対策ソフトウェアがワームを検出していながら、何らかの理由でワームを阻止できなかった可能性もある。または、感染後にウイルス対策ソフトウェアがワームを認識できる新しいシグネチャによって更新された可能性もある。インシデント対応担当者は、フォレンジックツールキットに含まれているウイルス対策ソフトウェアの最新バージョンを使ってサーバ上のワームをスキャンすることもできる。

- **アプリケーションのログ。**ワームが HTTP や SMTP などの一般的なアプリケーションプロトコルを使用した場合は、それらに関する情報が、アプリケーションサーバのログ、プロキシサーバ、アプリケーション固有のセキュリティ管理策など、複数の場所に記録されている可能性がある。あまり一般的でないアプリケーションプロトコルに関する情報は、おそらくアプリケーションサーバのログにしか存在しない。アプリケーションのログに記録される、活動のアプリケーション固有の特性に関する情報は広範なため、あまり一般的でないアプリケーションからの攻撃の特性を識別するのに特に有効である。

初期の情報収集活動の目標は、ワームを明確に識別するのに必要な特性を識別することである。この識別は、ワームに数多くの変種が存在する場合は特に困難である。これらの変種は、同じような特性を持っていながら、システムに対して異なる影響を与えることが多い。分析担当者は、ウイルス対策ベンダーのマルウェアデータベースに対してクエリを実行することにより、識別された特性（製品名、サービス名、ポート番号、マルウェアに含まれるテキスト文字列、標的上で変更が加えられたファイルや設定など）を検索することができる[126]。主要なマルウェアデータベースには、最新の脅威（数時間前に発生したものなど）を除き、事実上すべてのマルウェアの事例が含まれている可能性が高い。各データベースエントリには、通常、ワームがどのように拡散し、システムにどのような影響を与え（どのような変更を加えるかなど）、どのような方法で根絶できるか（ほかのシステムへの感染を防止する対策を含む）に関して、幅広い情報が含まれている。

マルウェアデータベースの検索がワームの特定につながらない場合、インシデント対応担当者は通常ならマルウェアデータベースのエントリから得られる情報を見つけるために、追加的な調査と分析を行わなければならない可能性がある。組織は、ワームのコピーを組織のウイルス対策ベンダーに送付して分析と特定を依頼することができるが、ベンダーの回答期日が不明なため、そのあいだに独自の分析を行うべきである。詳細な情報を収集するため、分析担当者は次の方法で感染を検査できる。

- **ホストの現在の状態。**分析担当者は、ホストの現在の状態を複数の側面から確認することによってホストを検査できる。この場合、ネットワーク接続のリストを調べて、異常な接続（接続数が多すぎる、予期しないポート番号が使用されている、予期しないホストへの接続があるなど）や予期しない接続待機ポート（ワームによって作成されたバックドアなど）を特定するのが、おそらく最も効果的である。有用と思われるそのほかの措置としては、実行中のプロセスのリストに未知のプロセスがあるかどうかを確認する、ホストのログを調べて、感染に関連する可能性がある異常なエントリを見つける、などがある。

- **ホストのネットワーク活動。**分析担当者は、感染したサーバによって生成されているワームトラフィックをパケットスニファやプロトコルアナライザを使って収集できる。これにより、ワームの特性に関する十分な追加情報が得られ、分析担当者が主要なマルウェアデータベースでワームを特定できる可能性がある。

ワームインシデントでは、感染したシステムが組織の内部や外部にあるほかのシステムを攻撃する可能性があるため、できるだけ迅速な対応が必要とされる場合が多い。また、ワームがバックドアやそのほかのツールをシステムにインストールすることにより、攻撃者が感染したシステムにリモートからアクセスできるようになるため、被害が拡大する可能性がある。したがって、各組織は最初にホストに関するデータの収集を行うのではなく、感染したシステムをネットワークから直ちに切断することもできる。この措置により、分析担当者によるワームの識別やワームがシステムに与える影響の特定がかなり困難になる可能性がある。たとえば、システムがネットワークから切断されると、ネ

[126] マルウェアデータベースは、Computer Associates（http://www3.ca.com/securityadvisor/virusinfo/default.aspx）、F-Secure（http://www.f-secure.com/virus-info/）、Network Associates（http://vil.nai.com/vil/default.aspx）、Sophos（http://www.sophos.com/virusinfo/analyses/）、Symantec（http://securityresponse.symantec.com/avcenter/vinfodb.html）、Trend Micro（http://www.trendmicro.com/vinfo/virusencyclo/）など、いくつかのベンダーが維持している。

ットワーク活動やホスト状態の特定の側面に関する情報は入手できなくなる。このような場合、分析担当者はサーバのより詳細なフォレンジック分析を行わなければならない可能性がある。たとえば、サーバで何が発生したかを正確に知るために、サーバのファイルシステムを収集し、ファイルシステム上に悪意のある活動の兆候（変更されたシステム実行ファイルなど）がないかどうかを調べる。分析担当者は、ワームによって追加された可能性がある管理者レベルのユーザアカウントやグループを探すなど、サーバ OS の不揮発性の特性を調べることもできる。分析担当者は、最終的にはワームの振る舞いを十分に詳しく特定するために必要な情報を収集することにより、インシデント対応チームがインシデントの封じ込めと根絶、およびインシデントからの復旧のために効果的に活動できるようにするべきである。

8.2 脅迫メール

あるインシデント対応担当者が、内部調査への支援要請に対応した。ある職員が、組織の電子メールシステムを使って脅迫的な電子メールを別の職員に送ったとして告発されていた。インシデント対応担当者は、その電子メールの記録が含まれている可能性があるすべてのデータソースを見つけるために調査担当者を支援するように依頼された。この情報は、調査担当者が電子メールの送信者を特定するのに役立つはずである。電子メールは簡単に偽造できるため、利用可能なすべてのデータソースを使って、電子メールの作成、送信、および受信に関する事象の流れを再現することが重要である。また、インシデント対応担当者はフォレンジック的に健全なツール、技法、および手続きを使ってすべての作業を行い、実行したすべての措置を文書化する必要がある。

脅迫メールは、この調査の鍵であり、そのヘッダにはインシデント対応担当者にとって最も重要な情報が含まれている。そこには、電子メールを送信したホストのドメイン名と IP アドレス、電子メールを送信するために使われた電子メールクライアントの種類、電子メールのメッセージ ID、および電子メールが送信された日付と時刻が含まれているはずである。電子メールのヘッダには、メッセージが通過した各電子メールサーバ（ドメイン名と IP アドレス）と、各サーバが電子メールを処理した日付および時刻も列挙されているはずである[127]。この電子メールは、組織の電子メールシステムを使って送信されたことになっているため、電子メールのヘッダには組織内のシステムしか列挙されていないはずである。これが本当だとすれば、インシデント対応担当者は列挙された各システムを確認して、情報を関連付けることができる。

脅迫メールが最も重要であるため、インシデント対応担当者はまずヘッダを含む電子メールのコピーを収集することに集中するべきである。受信者が使った電子メールクライアントの種類とその設定に応じて、電子メールが受信者のワークステーションにダウンロードされた可能性もあれば、電子メールサーバに電子メールがまだ残っている可能性もある。また、電子メールが両方に保存されている可能性もある。インシデント対応担当者は、可能であれば複数のソースから電子メールのコピーを収集し、電子メールの内容が転送中に変更されたり、受信者によって変更されたりしていないことを確認するべきである。

インシデント対応担当者は、ヘッダを確認したら、次に電子メールの送信に関する詳細情報を収集するべきである。ヘッダには、送信者が使用した IP アドレスと電子メールクライアントが記録されているはずである。インシデント対応担当者は、電子メールが送信された時点でどのホストがその IP アドレスを使用していたかを特定するべきである。この IP アドレスには、次の 3 つの可能性がある。

- **ローカルの電子メールクライアント。**この場合、インシデント対応担当者は、ネットワークの記録（DHCP のログなど）を使って、電子メールの送信に使われたデスクトップコンピュータ、ラップトップコンピュータ、PDA、またはそのほかの機器を識別できるはずである。その結果、

[127] 電子メールヘッダのなかでは、これらの記録が逆順で格納されるため、最も新しい記録が最初に現れ、最も古い記録が最後に現れる。電子メールが偽造された場合、虚偽の記録は最も古いため、ヘッダの最後に現れるはずである。

インシデント対応担当者は、識別された機器のイメージを作成し、イメージのコピーを調べることにより、マルウェアや電子メールに関連する記録を探すことができる。たとえば、送信した各電子メールのコピーを保持するように電子メールクライアントが設定されていたり、ユーザが電子メールメッセージの下書きを保存していたりする可能性がある。完全な状態のメッセージがシステム上に見つからない場合は、機器のメモリやファイルシステムから削除されたファイルや一時ファイルを含むデータを収集することにより、電子メールを断片的に特定できる可能性がある。また、機器上のセキュリティ管理策（スパムフィルタリングやウイルス対策ソフトウェアなど）によって、発信された電子メールがスキャンされていたり、ログに記録されていたりする可能性もある。電子メールのコピーが電子メールサーバ上に保存されている可能性も（確率としては低いが）ある。インシデント対応担当者は、ローカルホスト上で電子メールの記録を探すのに加えて、ホスト上の認証記録を分析することにより、電子メールの送信時にどのユーザアカウントが使用されたかを特定するべきである。

- **サーバベースの電子メールクライアント。**組織がサーバベースのクライアント（Web ベースの電子メールインタフェースなど）を提供している場合、IP アドレスはそのサーバに対応している可能性がある。通常、このようなサーバを使用するには、ユーザが自分自身を認証する必要があるため、送信者とされている人物がサーバにログオンした日時とユーザのシステムに使用されていた IP アドレスを示す認証記録が存在する可能性がある。インシデント対応担当者は、その IP アドレスが当時どのシステムに割り当てられていたかを特定し、特定されたシステムのビットストリームイメージを取得し、イメージのコピーを調べることにより、マルウェアや電子メールを探すことができる。たとえば、Web ブラウザの一時ファイルに、電子メールの内容のコピーが含まれている可能性がある。

- **偽装アドレス。**IP アドレスがねつ造されていた場合（たとえば、組織のネットワーク内の有効なアドレスでないなど）、インシデント対応担当者はほかのデータソースを利用して、電子メールメッセージを実際に送信したホストを特定するべきである。

組織の電子メールサーバは、もう 1 つの情報ソースの候補である。電子メールヘッダに列挙された各サーバ IP アドレスには、メッセージ ID 値を含む電子メールの記録が含まれているはずであり、それによって関係する記録をすばやく特定できるはずである。前述したように、リストの最後の電子メールサーバには、電子メールのコピーが格納されている可能性がある。そのサーバのバックアップにも電子メールのコピーが含まれている可能性があるが、それは電子メールのコピーが配信用に数時間以上にわたってそのサーバに保持されていた場合のみである。電子メールに関連するほかのサービス（ウイルス対策ソフトウェアやスパムフィルタなど）にも電子メール活動の基本的な記録が含まれている可能性があるが、詳細な情報が数多く含まれている可能性は低い。考えられるもう 1 つの情報ソースは、認証記録である。ユーザが電子メールを送信する際に認証を要求する電子メールサーバは少ないが、これらのサーバは一般に電子メールをユーザに配信する際にも認証を要求する。ユーザが 1 つのセッションで電子メールの送信と受信を行うことが多いため、認証ログには電子メールを受信した記録が含まれている可能性があり、これらの記録は特定の電子メールを送信したユーザを特定するのに役立つことがある。

考えられるもう 1 つの情報ソースは、電子メールの送信または受信によって生成されたネットワークトラフィックの記録である。ネットワーク活動を監視していたパケットスニファやネットワークフォレンジック分析ツールによって、活動が捕捉された可能性がある。これには、送信ホストや受信ホストの実際の IP アドレス、電子メールの内容とヘッダ、および関連する認証活動が含まれる。

インシデント対応担当者は、最終的には電子メールの送信と受信に使われたホストだけでなく、電子メールを送信者から受信者に転送したすべての中間ホストも識別するべきである。インシデント対応担当者は、関連する各ホストから電子メールと関連情報のコピーを収集し、記録に含まれるタイ

ムスタンプを使って、コンピュータネットワークの観点から事象の流れを再現するべきである。たとえば、次のような流れが考えられる。

> 午前 8:37 に、あるユーザが特定のデスクトップコンピュータにログオンした。午前 10:02 に、付属の電子メールクライアントを使ってそのコンピュータから脅迫メールが送信された。この電子メールは、組織の 3 つの電子メールサーバを通過し、サーバ 4 に格納され、目的の受信者による取り込みを待った。受信者ユーザは、午前 11:20 に特定のラップトップコンピュータにログオンし、午前 11:23 に脅迫メールを含む電子メールをダウンロードした。受信者のコンピュータ上の電子メールの内容やユーザ指定のヘッダフィールド（発信元、送信先、件名など）は、最初のユーザのデスクトップコンピュータ上の送信済みフォルダに保存されているコピーとまったく同じであった。

これらの情報は、その後の調査の土台として使用できる。これらの情報は、コンピュータネットワーク上の活動の記録であるが、発生した事実の全体を示しているわけではない。たとえば、特定できるのはその時点でどのユーザアカウントが使われていたかだけであり、どの人物が実際にデスクトップコンピュータから電子メールを送信したかは特定できない。インシデント対応担当者は、問題のデスクトップコンピュータを分析して、その完全性を検証することができる。たとえば、コンピュータのセキュリティ設定やセキュリティ管理策を組織のベースライン設定と比較したり、コンピュータのクロック設定を確認したり、セキュリティの侵害やそのほかの違反の兆候がないかどうかを確認したりできる。

8.3 推奨事項

このセクションに示した複数ソースのデータの使用に関する主な推奨事項は、次のとおりである。

- **分析担当者は、複数のデータソースを個別に分析し、データソース間で事象を相互に関連付けることにより、多くの状況を最も効果的に処理できる。**各種のデータソースを収集、検査、および分析するための技法とプロセスは、データソースの種類によって根本的に異なる。多くのアプリケーションは、データファイル、OS、およびネットワークトラフィックにデータが捕捉される。
- **各組織は、分析の技術面およびロジスティック面の複雑さを認識すること。**1 つの事象によって、多くの異なるデータソースで記録が生成され、分析担当者が現実的に確認しきれないほどの大量の情報が発生する可能性がある。SEM などのツールは、多くのデータソースの情報を 1 か所に集めることで、分析担当者の役に立つ可能性がある。

付録A—推奨事項

付録 A には、セクション 2 からセクション 8 にかけて示した主な推奨事項を再掲する。推奨事項の最初のグループは、フォレンジックス能力の組織化に対応する。残りの推奨事項は、フォレンジックスプロセスのフェーズ（収集、検査、分析、報告）別に分類されている。

A.1 フォレンジック能力の組織化

- **各組織は、コンピュータ／ネットワークフォレンジックスを行う能力を持つこと。**フォレンジックスは、犯罪や不適切な行為の調査、コンピュータセキュリティインシデントの再構成、運用上の問題のトラブルシューティング、監査記録維持のための注意義務の支援、偶発的なシステム損傷からの復旧など、組織内のさまざまな職務で必要とされている。このような能力を持たない組織は、組織のシステムやネットワークのなかでどのような事象（たとえば、保護されている機密データの露出など）が起きたかを特定するのが困難になる。また、フォレンジック的に適切な方法で証拠を取り扱うことにより、意志決定者は自信を持って必要な措置を取ることができる立場に置かれる。

A.1.1 フォレンジックの当事者

- **各組織は、フォレンジックスの各側面をどの関係者に対応させるかを決定すること。**ほとんどの組織は、フォレンジック作業の実行に自組織のスタッフと外部の者を併用する。各組織は、技能と能力、コスト、対応時間、およびデータの機密性に基づいて、どの関係者がどの作業に対応するべきかを決めるべきである。

- **分析担当者は、適度に幅広い技術的知識を持つこと。**現在のツールは分析機能がやや限られているため、分析担当者はネットワークの動作原理、一般的なネットワークやアプリケーションのプロトコル、ネットワークやアプリケーションのセキュリティ製品、およびネットワークベースの脅威と攻撃手法について、十分な訓練を受け、経験を積み、豊富な知識を持つべきである。

- **インシデント対応チームは、しっかりとしたフォレンジック能力を持つこと。**チームの複数のメンバーが個々の一般的なフォレンジック活動を実行できるべきである。実地訓練や、IT とフォレンジックに関するトレーニングコースは、技能の開発と維持に役立つ可能性がある。新しいツールや技法のデモも同様である。

- **組織内の多くのチームがフォレンジックスに参加すること。**フォレンジック措置を行う各個人は、追加的な支援を得るために必要に応じて組織内のほかのチームや個人と接触できるべきである。フォレンジック活動を支援できるチームの例としては、IT 担当者、管理職層、法律顧問、人事担当者、監査員、物理的セキュリティスタッフなどが挙げられる。これらのチームのメンバーは、フォレンジックスにおける各自の役割と責任を理解し、フォレンジック関連のポリシー、ガイドライン、および手続きに関するトレーニングや教育を受け、フォレンジック措置に関してほかの人への協力と支援を提供できるように備えておくべきである。

A.1.2 フォレンジックのポリシー、ガイドライン、および手続き

- **フォレンジックに関する考慮事項をポリシーのなかで明確に取り扱うこと。**ポリシーは、高次においては、許可された職員が正当な理由によりシステムやネットワークの監視と調査を適切な条件の下で行うことを許可するべきである。各組織は、インシデント対応担当者やフォレンジックにかかわる役割を持つそのほかの者に対する独立したフォレンジックポリシーを持つこともできる。このポリシーによって、適切な振る舞いに関する、より詳細な規則が提供

される。フォレンジック活動への支援を求められる可能性がある者は、フォレンジックポリシーを熟知し、理解するべきである。ポリシーに関するそのほかの考慮事項を以下に示す。

- フォレンジックポリシーでは、組織のフォレンジック活動を実行または支援するすべての人々の役割と責任を明確に規定するべきである。このポリシーでは、関係するすべての内部および外部の者を記載し、さまざま条件下で誰がどの関係者と連絡を取るのかを明確に示すべきである。
- 組織のポリシー、ガイドライン、および手続きでは、通常の状況と特別な状況の下で実行すべきフォレンジック措置と実行すべきでないフォレンジック措置を明確に説明し、反フォレンジックツールや反フォレンジック技法も取り扱うべきである。ポリシー、ガイドライン、および手続きでは、機密情報の偶発的な暴露への対応も取り扱うべきである。
- フォレンジックに関する考慮事項を情報システムライフサイクルに組み込めば、多くのインシデントに、より効率的かつ効果的に対応できるようになる可能性がある。
- 組織のポリシーでは、フォレンジックツールによって捕捉された機密情報の偶発的な開示や長期的な保管について規定し、それらが組織のプライバシやデータ保持に関するポリシーに違反しないことを確認するべきである。
- 組織のポリシーでは、ネットワークの監視についても取り扱い、活動が監視される可能性があることを示す警告バナーをシステムにおいて表示するように求めるべきである。これらのポリシーでは、ユーザのプライバシに対する妥当な期待を考慮に入れるべきである。

■ **各組織は、フォレンジック作業を実行するためのガイドラインと手続きを作成し、管理すること。**ガイドラインには、フォレンジック技法を使ってインシデントを調査するための一般的な方法論を記載し、順を追った手続きによる定型作業の実行方法を説明するべきである。これらのガイドラインと手続きは、訴訟手続きにおける証拠能力の裏付けとなるべきである。電子的なログやそのほかの記録は、改変または操作される可能性があるため、各組織はポリシー、ガイドライン、および手続きによってこのような記録の信頼性と完全性を立証できるように備えておくべきである。また、これらのガイドラインと手続きを定期的に見直して、その正確さを維持するべきである。

A.1.3 技術的な準備

■ **分析担当者は、データの収集、検査、および分析に使用するフォレンジックツールキットを用意すること。**このツールキットには、揮発性データと不揮発性データを収集して検査する機能や、データのすばやい確認と詳細な分析を実行する機能を備えたさまざまなツールを含めるべきである。このツールキットでは、アプリケーションをリムーバブルメディア（フロッピーディスク、CD など）やフォレンジックワークステーションから素早く効率的に起動できるようにするべきである。

■ **各組織は、ネットワーク活動に関連するログに対して十分な記憶領域を用意すること。**各組織は、通常時およびピーク時のログ使用量を見積もり、組織のポリシーに基づいて何時間分または何日分のデータを保持する価値があるかを判断し、十分な記憶領域をシステムやアプリケーションのために確保するべきである。コンピュータセキュリティインシデントに関連するログは、ほかのログよりはるかに長い期間にわたって保管しなければならない可能性がある。

A.2 フォレンジックスプロセスの実行

- **各組織は、一貫性のあるプロセスを使ってフォレンジックスを実施すること。**このガイドでは、収集、検査、分析、報告の 4 つのフェーズからなるフォレンジックスプロセスを示している。各フェーズの詳細は、フォレンジックスに対するニーズに応じて異なる可能性がある。

A.2.1 データの収集

- **各組織は、先を見越して有用なデータを収集すること。**OS に対する監査の設定、集中管理されたログ機能の実装、システムの定期的なバックアップの実行、およびセキュリティ監視管理策の使用によって、将来のフォレンジック活動に必要なデータのソースを生成することができる。

- **分析担当者は、データソース候補の範囲を認識すること。**分析担当者は、物理的な場所を調査し、データソースの候補を認識できるべきである。分析担当者は、組織の内部および外部のほかの場所にあるデータソース候補についても検討するべきである。分析担当者は、一次ソースからデータを収集するのが可能でない場合は、代わりのデータソースを使用できるように備えておくべきである。

- **分析担当者は、考えられるすべてのアプリケーションデータソースを考慮すること。**アプリケーションの事象は、多くの異なるデータソースによって記録される可能性がある。また、1 つのシステム上にインストールされた複数のクライアントプログラムや、Web ベースのクライアントインタフェースなど、複数の仕組みを介してアプリケーションが使用される可能性もある。このような状況では、分析担当者はすべてのアプリケーション構成要素を識別し、重要である可能性が最も高い構成要素を決定し、各構成要素の場所を特定し、データを取得するべきである。

- **分析担当者は、標準的なプロセスを使ってデータの収集を行うこと。**推奨される手順は、データソースの識別、データ取得計画の策定、データの取得、および取得したデータの完全性の検証である。計画では、データの予想価値、データの揮発性、および必要な労力に基づいてデータを取得する順序を確定し、データソースの優先順位を決めるべきである。データの収集を始める前に、将来の訴訟や内部懲戒の手続きにおけるデータの使用に対応する方法で証拠の収集と保全を行う必要性に関して、分析担当者または管理職層が意志決定するべきである。必要性がある場合には、手違いや証拠改ざんの疑いが生じないように、明確に規定された保管引渡し管理に従うべきである。

- **分析担当者は、揮発性 OS データを保全するために適切な行動を取ること。**揮発性 OS データを保全する必要があるかどうかを判断する基準をあらかじめ文書化しておくことにより、分析担当者ができるだけ速やかに十分な情報に基づいて判断を下せるようにするべきである。揮発性 OS データの収集に必要な労力が正当化されるかどうかを判断するには、そのような収集に伴うリスクと重要な情報を回復できる可能性とを比較検討するべきである。

- **分析担当者は、揮発性 OS データの収集にフォレンジックツールキットを使用すること。**フォレンジックツールを使用することにより、システムへの影響を最小限に抑え、ツールを変更から保護しながら、正確な OS データを収集できる。分析担当者は、データの収集時に各ツールによってシステムにどのような影響や変更が加わるかを知っておくべきである。

- **分析担当者は、システムごとに適切なシャットダウンの方法を選択すること。**特定の OS をシャットダウンする方法に応じて、保全されるデータや失われるデータの種類が異なる可能性がある。分析担当者は、各 OS の標準のシャットダウン動作を認識しておくべきである。

- **分析担当者は、ファイルの完全性を保護し、検証すること。**バックアップ中またはイメージの取得中にデータ書き込み防止ツールを使用することで、コンピュータによる記憶媒体への書き込みが防止される。ファイルのメッセージダイジェストを算出して比較することにより、コピー先のデータの完全性を検証するべきである。バックアップやイメージには、できる限り読み取り専用権限でアクセスするべきである。データ書き込み防止ツールを使って、バックアップファイルやイメージファイル、または復元されたバックアップやイメージへの書き込みを防止することもできる。

A.2.2 検査と分析

- **分析担当者は、体系的な手法を使ってデータを調査すること。**フォレンジックスの基本は、分析担当者が体系的な手法を使って、入手可能なデータを分析することにより、入手可能なデータに基づいて適切な結論を導き出すか、または結論をまだ導き出せないと判断することである。訴訟や内部懲戒処分で証拠が必要とされる場合、分析担当者は分析結果と行われた処置を慎重に文書化するべきである。

- **分析担当者は、元のファイルではなく、ファイルのコピーを検査すること。**収集フェーズでは、分析担当者は必要なファイルやファイルシステムの複数のコピー（通常はマスタコピーと作業用コピー）を作成するべきである。これにより、分析担当者は元のファイルやマスタコピーに影響を与えることなくファイルの作業用コピーを使用できる。訴訟や懲戒処分で証拠が必要とされる場合や、ファイル日時情報を保全することが重要な場合は、ビットストリームイメージの取得を行うべきである。

- **分析担当者は、各データソースの忠実性と価値を考慮すること。**分析担当者は、ほかのソースから標準化されたデータを受け取るデータソースよりも、元のデータソースを信頼するべきである。分析担当者は、データの解釈に基づく異常なデータや予期しないデータ（IDS や SEM の警告など）の有効性を確認するべきである。

- **分析担当者は、ファイル拡張子ではなく、ファイルヘッダを利用してファイル内容の種類を識別すること。**ユーザはファイルに任意のファイル拡張子を割り当てることができるため、分析担当者はファイル拡張子が正しいと想定するべきではない。分析担当者は、多くのファイルについて、ファイルのヘッダを検査することにより、格納されているデータの種類を識別できる。ファイルヘッダに変更を加えて実際のファイル形式を隠すことも可能だが、これはファイル拡張子を変更するのに比べればごくまれである。

- **分析担当者は、一般に事象の特性と影響に重点を置くこと。**攻撃者の身元の特定やほかの同様の措置は、一般に多大な時間を要し、達成が難しく、組織が運用上の問題やセキュリティの弱点を是正する助けにはならない。攻撃者の身元情報や意図の特定は、特に結果として犯罪調査が行われる場合に重要だが、そのほかの重要な目標とのバランスを考慮するべきである。

- **各組織は、分析の技術面およびロジスティック面の複雑さを認識すること。**1 つの事象によって、多くの異なるデータソースで記録が生成され、分析担当者が現実的に確認しきれないほどの大量の情報が発生する可能性がある。SEM などのツールは、多くのデータソースの情報を 1 か所に集めることで、分析担当者の役に立つ可能性がある。

- **分析担当者は、さまざまなソースから得られたデータを結び付けること。**分析担当者は、アプリケーション関連事象の詳細な分析や事象の再現を行うために、個々のデータソース（データファイル、OS、ネットワークトラフィックなど）の検査と分析の結果を精査し、情報が互いにどのように結び付いているのかを明らかにするべきである。

A.2.3 報告

- **分析担当者は、各自のプロセスと実践事項を見直すこと。**現在および最近のフォレンジック措置の見直しは、ポリシーの不備、手続き上の誤り、および是正する必要があるそのほかの問題を識別し、組織が技術の動向や法律の変更に確実についていく上で役立つ可能性がある。

付録B—シナリオ

フォレンジックツールやフォレンジック技法をさまざまなシナリオでどのように使用するかに重点を置いた机上演習を行うことにより、技能の開発と維持や、ガイドライン、手続き、ポリシーに関する問題の特定が安価かつ効果的な方法で可能になる。演習の参加者には、簡単なシナリオが提示されたあと、そのシナリオに関していくつかの質問が行われる。参加者は、各質問について議論し、その状況で実際に行うと思われる行動に基づいて回答を作成する。次に、回答を組織のポリシー、手続き、およびガイドラインと比較し、不備や矛盾がないかどうかを確認する。たとえば、ある質問への回答から、参加者が特定のソフトウェアを持っておらず、組織内の特定のチームが就業時間外のサポートを提供していないために、フォレンジック措置が遅れるということがわかるかもしれない。

B.1 項に、ほぼすべてのシナリオに適用できる一般的な質問のリストを示す。B.2 項では、いくつかのシナリオ例を示す。各シナリオのあとには、そのシナリオ固有の追加質問が付いている。これらの質問やシナリオを、各組織の演習に合わせて使用することを推奨する。

B.1 シナリオの質問

1. 潜在的なデータソースとしてどのようなものがありますか？
2. 潜在的なデータソースのうち、有益な情報が含まれている可能性が最も高いのはどれですか？また、それはなぜですか？
3. 最初に確認するデータソースはどれですか？また、それはなぜですか？
4. 使用する可能性が最も高いフォレンジックツールやフォレンジック技法はどれですか？使用する可能性があるそのほかのツールや技法はどれですか？
5. 組織内部のどのグループや個人がフォレンジック活動に関与する可能性がありますか？
6. 外部関係者とどのようなやり取りが発生する可能性がありますか（もしあれば）？
7. フォレンジックの観点から、シナリオが発生した日や時間（勤務時間内と勤務時間外）が異なる場合、行われる措置にはどのような違いがありますか？
8. フォレンジックの観点から、シナリオの発生した場所（現地と遠隔地）が異なる場合、行われる措置にはどのような違いがありますか？

B.2 シナリオ

シナリオ 1：DDoS 攻撃の可能性

ある土曜日の午後、外部ユーザが組織の公開 Web サイトにアクセスする際に問題が発生し始めた。次の 1 時間で問題はさらに悪化し、組織のあらゆる公開 Web サイトへのアクセスの試みがほぼすべて失敗するまでになった。一方、組織のネットワークスタッフは、インターネット境界ルータが自動的に生成した警告に対応し、組織の 2 つの公開 DNS（Domain Name System）サーバによって送受信される異常に大量の UDP（User Datagram Protocol）パケットによって組織のインターネット帯域幅の多くが消費されていると判断した。

このシナリオに対する追加の質問を次に示す。

1. DDoS 攻撃が別の州のネットワークから行われていると考えられる場合、フォレンジック活動はどのように変わりますか？別の国から行われていると思われる場合はどうですか？

2. DDoS 攻撃がビジネスパートナーのネットワークから行われていると考えられる場合、フォレンジック活動はどのように変わりますか？

シナリオ 2：オンライン決済の問題

オンラインの請求書提示と決済に関して組織の問い合わせ回線にかかってくる電話の件数が、ここ一週間で 4 倍に増加した。電話をかけた人のほとんどは、決済情報を何回も再送信しなければならないと訴えており、多くの人が決済を完了できなかった。

このシナリオに対する追加の質問を次に示す。

1. この問題の原因は、新規利用者に対して明確な説明が行われていないなど、非技術的なものである可能性があります。調査の技術的側面と非技術的側面をどのように調整し、バランスを取るべきですか？

2. プライバシへの配慮は、フォレンジックツールやフォレンジック技法の使用にどのように影響しますか？

3. 運用上の問題がこの問題の原因であるとアプリケーション開発者が確信している場合は、フォレンジックツールやフォレンジック技法をどのように使用しますか？

シナリオ 3：正体不明のワイヤレスアクセスポイント

ある月曜日の朝、ある建物の同じ階にいる 5 人のユーザが組織のヘルプデスクに電話をかけ、無線アクセスに問題があることを伝えた。この問題の解決を支援するように求められたネットワーク管理者は、これらのユーザがいる階に、無線機能を備えたラップトップコンピュータを持ち込んだ。無線ネットワークの設定を確認したところ、新しい無線アクセスポイントが利用できるとして表示されていることに気付いた。ネットワーク管理者は、このアクセスポイントが送信する構成設定がセキュリティ保護されていないことから、これは自分のチームが配備したものではないと思った。

このシナリオに対する追加の質問を次に示す。

1. このアクセスポイントの特定を明示的に行う場合は、どのような種類のフォレンジックツールを使用しますか？秘密裏に行う場合はどうですか？

2. このアクセスポイントが正当な業務上の目的（請負業者による現場での一時的な作業など）のために配備されたと判断される場合、フォレンジック活動はどのように変わりますか？

3. 見知らぬ人物がこのアクセスポイントを配備している現場が目撃されていたことがわかった場合、フォレンジック活動はどのように変わりますか？

シナリオ 4：再感染したホスト

あるユーザが、ここ 2 週間のあいだに同じウイルスをラップトップコンピュータから 2 回削除する必要があった。このユーザは、現在も同じような症状を報告している。直前の感染に対応した技術サポートスタッフは、コンピュータ上のウイルス対策ソフトウェアが有効かつ最新だったことを確認しており、ウイルスがどのようにしてコンピュータに再感染したかを特定できなかった。

このシナリオに対する追加の質問を次に示す。

1. ユーザの職場を目視で調査することにより、ほかにどのようなデータソースが見つかる可能性がありますか？

2. ユーザの職場外のデータソースとして最も可能性が高いものは何ですか？

3. 分析担当者は、組織が所有していないデータソースを検査したい場合に、どのような法的な側面を認識するべきですか？

シナリオ 5：誤った身元識別情報

過去 24 時間以内に、組織内の 2 人の職員によって、組織が発行したクレジットカードに不正な購入代金が請求されたことが報告された。この組織は、問題の取引があった品物を販売した会社から頻繁に商品を購入している。その後のアセスメントにより、組織のクレジットカードへの請求が組織全体でこの 3 日間に 30%増加していることがわかった。

このシナリオに対する追加の質問を次に示す。

1. フォレンジックツールやフォレンジック技法は、分析担当者が発生した事態（組織内の職員がなりすましの被害者であることや、資金の不正操作があったことなど）を判断する際にどのように役立ちますか？

2. 職員の金融取引を調査するときに、プライバシにかかわるどのような事項を考慮するべきですか？

シナリオ 6：不要なスクリーンセーバ

組織のヘルプデスクが、コンピュータでの作業中に牧歌的な風景を映し出すスクリーンセーバが起動するというユーザからの苦情の電話を何度か受けた。ユーザがこのスクリーンセーバを解除して作業を続行するには、各自のパスワードを提示する必要があった。同時に、組織のネットワーク侵入検知システムが、ある Web サーバに関する異常な警告を何度か報告した。警告に含まれるデータから、何らかの疑わしい活動がこのサーバに対して行われたことと、現在はこのサーバがほかのシステムに対して同じような活動を生成していることがわかった。侵入検知分析担当者の最初の仮説は、ワームがこの Web サーバ上の脆弱なネットワークサービスを攻撃している、というものだった。

このシナリオに対する追加の質問を次に示す。

1. このシナリオには時間的な余裕がないため、分析担当者は措置の優先順位をどのように決定するべきでしょうか？

2. ワームがネットワーク通信を妨害していた場合、フォレンジック活動はどのように変わりますか？

3. 組織が保護することを求められている機密情報が、感染したデスクトップシステムを使って処理されていた場合、フォレンジック活動はどのように変わりますか？

シナリオ 7：フィッシングの試み

過去 24 時間以内に、複数の職員がヘルプデスクに電話をかけ、組織のクレジットカード提供者からの電子メールの有効性について質問した。これらの電子メールは、金融機関の記録にセキュリティ

侵害があった可能性について言及し、受信者に対して、金融機関の Web サイトへのリンクをたどり、既存のパスワードとアカウント情報を入力して各自の身元確認を行ったあと、新しいパスワードを作成するように求めている。

このシナリオに対する追加の質問を次に示す。

1. このシナリオには時間的な余裕がないため、分析担当者は措置の優先順位をどのように決定するべきでしょうか？

2. 身元情報の盗難による潜在的な問題を軽減するために、ほかのどのような組織に連絡を取るべきでしょうか？

シナリオ 8：暗号化されたファイル

ある職員が突然組織を離れた。その元職員の管理者は、元職員のデスクトップコンピュータに保存されているはずの重要なプロジェクトの情報を取り出すため、そのコンピュータにアクセスすることを許可された。この管理者は、プロジェクトに関連すると思われるファイル名をいくつか見つけたが、ファイルの内容にはアクセスできなかった。システム管理者がシステムを調べた結果、元職員がこれらのファイルを暗号化した可能性があることがわかった。

このシナリオに対する追加の質問を次に示す。

1. 暗号化されたデータを回復するためにどの程度の努力を払うべきかを決定するのは誰ですか？その決定は、どのようにして行われますか？

2. 今後同じような出来事が発生した場合の影響を減らすために、組織のポリシー、ガイドライン、および手続きに対してどのような変更を加えることができますか？

付録C—用語集

『*インシデント対応へのフォレンジック技法の統合に関するガイド*』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。

分析（Analysis）：コンピュータ／ネットワークフォレンジックプロセスの 3 番目のフェーズ。このフェーズでは、法的に正当と認められる手法および技法を使用して、収集と検査を行う契機となった疑問を解決するのに役立つ情報を引き出す。

反フォレンジック（Anti-Forensic）：データを隠蔽または破壊することによって、ほかの人がそのデータにアクセスできないようする技法。

ビットストリームイメージの取得（Bit Stream Imaging）：コピー元の媒体の空き領域やスラック領域を含めたビット単位のコピー。ディスクイメージの取得ともいう。

クラスタ（Cluster）：連続するセクタのグループ。

収集（Collection）：コンピュータ／ネットワークフォレンジックプロセスの最初のフェーズ。このフェーズでは、データの完全性を保護するガイドラインと手続きに従いながら、関連するデータを識別し、ラベル付けし、記録し、予想されるソースから取得する。

データ（Data）：特定の形態に整形されたディジタル情報の個別の断片。

ディジタルフォレンジック（Digital Forensics）：情報の完全性を保護し、データの厳密な保管引渡し管理を維持しながら、データの識別、収集、検査、および分析に科学的手法を適用すること。

ディレクトリ（Directory）：ファイル群をグループにまとめるために使われる組織化構造。

ディスクイメージの取得（Disk Imaging）：コピー元の媒体の空き領域やスラック領域を含むビット単位のコピーを生成すること。ビットストリームイメージの取得ともいう。

ディスクーディスクコピー（Disk-to-Disk Copy）：媒体の内容を別の媒体に直接コピーすること。

ディスクーファイルコピー（Disk-to-File Copy）：媒体の内容を 1 つの論理的なデータファイルにコピーすること。

検査（Examination）：コンピュータ／ネットワークフォレンジックプロセスの 2 番目のフェーズ。このフェーズでは、データの完全性を保護しながら、収集した大量のデータを自動的手法と手動的手法の組み合わせを使ってフォレンジック的に処理することにより、特に注目に値するデータを見定めて抽出する。

フォールスネガティブ（False Negative）：悪意のある活動を誤って害のないものとして分類すること。

フォールスポジティブ（False Positive）：害のない活動を誤って悪意のあるものとして分類すること。

ファイル（File）：論理的に 1 つのエンティティとしてまとめられ、一意の名前（ファイル名など）によって参照される情報の集まり。

ファイルアロケーションユニット（File Allocation Unit）：連続するセクタのグループ。クラスタとも呼ばれる。

ファイルヘッダ（File Header）：ファイルに関する識別情報と（場合によっては）ファイル内容に関する情報を提供するメタデータとを含むファイル内のデータ。

ファイル名（Filename）：ファイルを参照するために使われる一意の名前。

ファイルシステム（Filesystem）：論理ボリューム上のファイルを命名、格納、編成、およびアクセスするための方式。

フォレンジックサイエンス（Forensic Science）：法律に科学的手法を適用すること。

フォレンジック的にクリーンな（Forensically Clean）：ディジタル媒体が、その使用の前に不必要なデータや残存データを含むすべてのデータが完全に消去され、マルウェアがスキャンされ、検証されている状態。

空き領域（Free Space）：媒体上またはメモリ内の未割り当ての領域。

論理バックアップ（Logical Backup）：論理ボリュームのディレクトリおよびファイルのコピー。

論理ボリューム（Logical Volume）：ファイルシステムとしてフォーマットされ、1 つのエンティティとして機能するパーティションまたはパーティションの集まり。

メッセージダイジェスト（Message Digest）：データを一意に識別するハッシュ。メッセージダイジェストを生成するために使われるデータストリームを 1 ビットでも変更すると、まったく異なるメッセージダイジェストが生成される。

メタデータ（Metadata）：データに関するデータ。ファイルシステムの場合、メタデータはファイルの内容に関する情報を提供するデータである。

ネットワークアドレス変換（Network Address Translation）：あるネットワーク上のアドレスを別のネットワーク上のアドレスに対応付けるプロセス。

ネットワーク侵入検知システム（Network Intrusion Detection System）：疑わしい活動を識別し、関連する情報を記録するために、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するソフトウェア。

ネットワークトラフィック（Network Traffic）：ホスト間の有線または無線ネットワークを介して伝送されるコンピュータネットワーク通信。

不揮発性データ（Non-Volatile Data）：コンピュータの電源を切ったあとも存続するデータ。

標準化（Normalize）：異なる形態で整形されたデータを標準化された形式に変換し、一貫した方法でラベル付けするプロセス。

オペレーティングシステム（Operating System）：コンピュータ上で実行され、ほかのプログラムを実行するためのソフトウェアプラットフォームを提供するプログラム。

パケット（Packet）：トランスポート層によって生成される、ネットワーク通信の論理的単位。

パケットスニファ（Packet Sniffer）：有線または無線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ソフトウェア。

パーティション（Partition）：媒体のほかの論理的部分と物理的に独立しているかのように機能する媒体の論理的部分。

プロセス（Process）：実行中のプログラム。

プロトコルアナライザ（Protocol Analyzer）：個別のパケットに基づいてストリームを再構築でき、さまざまなプロトコルを使用している通信を復号できるソフトウェア。

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ソフトウェア。

リモートアクセスサーバ（Remote Access Server）：仮想プライベートネットワーク（VPN）ゲートウェイやモデムサーバなど、ネットワーク間の通信を支援する装置。

報告（Reporting）：コンピュータ／ネットワークフォレンジックプロセスの最後のフェーズ。このフェーズでは、分析結果を報告する。この報告には、使用された措置の記述、ツールと手続きの選択方法の説明、実行する必要があるそのほかの措置（追加のデータソースのフォレンジック検査、識別された脆弱性の安全対策、既存のセキュリティ管理策の改善など）の特定、フォレンジックプロセスのポリシー、ガイドライン、手続き、ツール、およびそのほかの側面の改善に関する推奨事項の提供などが含まれる可能性がある。報告フェーズをどの程度正式なものにするかは、状況によって大きく異なる。

セクタ（Sector）：媒体上のアクセス可能な最小単位。

セキュリティ事象管理ソフトウェア（Security Event Management Software）：複数のデータソースからセキュリティ事象の情報を取り込み、データを標準化し、各データソースの事象を相互に関連付けるソフトウェア。

スラック領域（Slack Space）：ファイルアロケーションブロックまたはメモリページ内の、残存データが格納されている可能性がある未使用領域。

ステガノグラフィ（Steganography）：データをほかのデータのなかに埋め込んで隠すこと。

サブディレクトリ（Subdirectory）：ほかのディレクトリのなかに含まれるディレクトリ。

揮発性データ（Volatile Data）：稼働中のシステム上に存在し、コンピュータの電源を切ると消失するデータ。

完全消去（Wiping）：データの収集を妨げるため、媒体または媒体の一部をランダムな値または一定の値で上書きすること。

データ書き込み防止ツール（Write-Blocker）：コンピュータに接続されているすべての記憶媒体に対する書き込みや変更を防止するツール。

（本ページは意図的に白紙のままとする）

付録D—略語

『*インシデント対応へのフォレンジック技法の統合に関するガイド*』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。

ADS	Alternate Data Stream（代替データストリーム）
ARIN	American Registry for Internet Numbers（米インターネット番号登録機関）
ARP	Address Resolution Protocol（アドレス解決プロトコル）
ASCII	American Standard Code for Information Interchange（情報交換用米国標準コード）
ATA	Advanced Technology Attachment（アドバンストテクノロジーアタッチメント）
BIOS	Basic Input/Output System（基本入出力システム）
CCIPS	Computer Crime and Intellectual Property Section（コンピュータ犯罪および知的財産担当部署）
CD	Compact Disc（コンパクトディスク）
CD-R	CD-Recordable（追記型 CD）
CD-ROM	CD-Read Only Memory（CD 読み取り専用メモリ）
CD-RW	CD-Recordable（書き換え可能 CD）
CDFS	CD File System（CD-ROM ファイルシステム）
CFI	Computer and Financial Investigations（コンピュータおよび財務の調査）
CFRDC	Computer Forensics Research and Development Center（コンピュータフォレンジック研究開発センター）
CFTT	Computer Forensics Tool Testing（コンピュータフォレンジックツール検査）
CMOS	Complementary Metal Oxide Semiconductor（相補型金属酸化膜半導体）
CVE	Common Vulnerabilities and Exposures（一般的な脆弱性と暴露性）
DDoS	Distributed Denial of Service（分散型サービス運用妨害）
DHCP	Dynamic Host Configuration Protocol（動的ホスト設定プロトコル）
DLL	Dynamic Link Library（ダイナミックリンクライブラリ）
DNS	Domain Name System（ドメインネームシステム）
DoD	Department of Defense（米国国防総省）
DVD	Digital Video Disc（ディジタルビデオディスク）または Digital Versatile Disc（ディジタル多用途ディスク）
DVD-R	DVD-Recordable（追記型 DVD）
DVD-ROM	DVD-Read Only Memory（DVD 読み取り専用メモリ）
DVD-RW	DVD-Rewritable（書き換え可能 DVD）
ESP	Encapsulating Security Payload（暗号ペイロード）
ext2fs	Second Extended Filesystem（第 2 世代拡張ファイルシステム）
ext3fs	Third Extended Filesystem（第 3 世代拡張ファイルシステム）
FACCI	Florida Association of Computer Crime Investigators（フロリダコンピュータ犯罪捜査官協会）
FAT	File Allocation Table（ファイルアロケーションテーブル）
FBI	Federal Bureau of Investigation（連邦捜査局）
FIPS	Federal Information Processing Standards（連邦情報処理基準）

F.I.R.E.	Forensic and Incident Response Environment（フォレンジックおよびインシデント対応環境）
FISMA	Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
FLETC	Federal Law Enforcement Training Center（連邦法執行訓練センター）
FTP	File Transfer Protocol（ファイル転送プロトコル）
GB	Gigabyte（ギガバイト）
GUI	Graphical User Interface（グラフィカルユーザインタフェース）
HFS	Hierarchical File System（階層型ファイルシステム）
HPA	Host Protected Area（ホスト保護領域）
HPFS	High-Performance File System（高性能ファイルシステム）
HTCIA	High Technology Crime Investigation Association（ハイテク犯罪捜査協会）
HTTP	Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）
IACIS	International Association of Computer Investigative Specialists（コンピュータ捜査専門家国際協会）
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）
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System（侵入検知システム）
IGMP	Internet Group Management Protocol（インターネットグループ管理プロトコル）
IM	Instant Messaging（インスタントメッセージング）
IMAP	Internet Message Access Protocol（インターネットメッセージアクセスプロトコル）
IOS	Internetwork Operating System
IP	Internet Protocol（インターネットプロトコル）
IPsec	Internet Protocol Security（インターネットプロトコルセキュリティ）
IR	Interagency Report（省庁間報告書）
IRC	Internet Relay Chat
IRQ	Interrupt Request Line（割込み要求線）
ISO	International Organization for Standardization（国際標準化機構）
ISP	Internet Service Provider（インターネットサービスプロバイダ）
IT	Information Technology（情報技術）
ITL	Information Technology Laboratory（情報技術ラボラトリ）
JPEG	Joint Photographic Experts Group（合同写真画像専門家グループ）
KB	Kilobyte（キロバイト）
LACNIC	Latin American and Caribbean IP Address Regional Registry（ラテンアメリカおよびカリブ地域 IP アドレス登録機関）
MAC	Media Access Control（媒体アクセス制御）
MAC	Modification, Access, and Creation（更新、アクセス、作成）
MB	Megabyte（メガバイト）
MD	Message Digest（メッセージダイジェスト）
MISTI	MIS Training Institute

MMC	Multimedia Card（マルチメディアカード）
MO	Magneto Optical（光磁気）
MS-DOS	Microsoft Disk Operating System（Microsoft ディスクオペレーティングシステム）
NAT	Network Address Translation（ネットワークアドレス変換）
NFAT	Network Forensic Analysis Tool（ネットワークフォレンジック分析ツール）
NFS	Network File Sharing
NIC	Network Interface Card（ネットワークインタフェースカード）
NIJ	National Institute of Justice（国立司法研究所）
NIST	National Institute of Standards and Technology（米国国立標準技術研究所）
NLECTC-NE	National Law Enforcement and Corrections Technology Center–North East（米国立法執行および矯正技術センターー北東支部）
NSRL	National Software Reference Library（米国立ソフトウェア資料ライブラリ）
NTFS	Windows NT File System（Windows NT ファイルシステム）
NTI	New Technologies, Inc.
NTP	Network Time Protocol（ネットワークタイムプロトコル）
NW3C	National White Collar Crime Center（全米ホワイトカラー犯罪センター）
OEM	Original Equipment Manufacturer（相手先商標製造会社）
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）
OSR2	OEM Service Release 2（OEM サービスリリース 2）
PCMCIA	Personal Computer Memory Card International Association（PC メモリカード国際協会）
PDA	Personal Digital Assistant（携帯情報端末）
POP3	Post Office Protocol 3（ポストオフィスプロトコルバージョン 3）
RAID	Redundant Array of Inexpensive Disks（安価なディスクによる冗長ディスクアレイ）
RAM	Random Access Memory（ランダムアクセスメモリ）
RCFL	Regional Computer Forensics Laboratory（地域コンピュータフォレンジック研究所）
RFC	Request for Comment（インターネット技術に関する IETF 発行文書）
RIPE NCC	Réseaux IP Européens Network Coordination Centre
SAM	Security Account Manager（セキュリティアカウントマネージャ）
SCSI	Small Computer System Interface（小型コンピュータシステムインタフェース）
SD	Secure Digital
SDMI	Secure Digital Music Initiative
SEM	Security Event Management（セキュリティ事象管理）
SFTP	Secure FTP（セキュア FTP）
SHA-1	Secure Hash Algorithm1（安全なハッシュアルゴリズム—1）
SIP	Session Initiation Protocol（セッションイニシエーションプロトコル）
SMB	Server Message Block（サーバメッセージブロック）
SMTP	Simple Mail Transfer Protocol（簡易メール転送プロトコル）
SNMP	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SP	Special Publication（特別刊行物）
SSH	Secure Shell（セキュアシェル）

SSL	Secure Sockets Layer（セキュアソケットレイヤ）
TB	Terabytes（テラバイト）
TCP	Transmission Control Protocol（伝送制御プロトコル）
TCP/IP	Transmission Control Protocol/Internet Protocol（伝送制御プロトコル／インターネットプロトコル）
TUCOFS	The Ultimate Collection of Forensic Software
UDF	Universal Disk Format（ユニバーサルディスクフォーマット）
UDP	User Datagram Protocol（ユーザデータグラムプロトコル）
UFS	UNIX File System（UNIX ファイルシステム）
UPS	Uninterruptible Power Supply（無停電電源装置）
URL	Uniform Resource Locator
USB	Universal Serial Bus（ユニバーサルシリアルバス）
VoIP	Voice over IP
VPN	Virtual Private Network（仮想プライベートネットワーク）

（本ページは意図的に白紙のままとする）

付録E—印刷資料

Bejtlich, Richard. The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley, 2004.

Carrier, Brian. *File System Forensic Analysis*. Addison-Wesley, 2005.

Casey, Eoghan. *Digital Evidence and Computer Crime*. Academic Press, 2004.

Casey, Eoghan. Handbook of Computer Crime Investigation: Forensic Tools & Technology. Academic Press, 2001.

Davis, Chris, et al. *Hacking Exposed: Computer Forensics Secrets & Solutions*. McGraw-Hill Osborne Media, 2004.

Farmer, Dan, and Wietse Venema. *Forensic Discovery*. Addison-Wesley, 2004.

Honeynet Project. Know Your Enemy: Learning about Security Threats, Second Edition. Addison-Wesley, 2004.

Jones, Keith J., et al. Real Digital Forensics: Computer Security and Incident Response. Addison-Wesley, 2005.

Kruse, Warren G., II, and Jay G. Heiser. *Computer Forensics: Incident Response Essentials*. Addison-Wesley, 2001.

Lucas, Julie, and Brian Moeller. *The Effective Incident Response Team*. Addison-Wesley, 2004.

Orebaugh, Angela. *Ethereal Packet Sniffing*. Syngress, 2004.

Oseles, Lisa. *"Computer Forensics: The Key to Solving the Crime."* October 2001. http://faculty.ed.umuc.edu/~meinkej/inss690/oseles_2.pdf.

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

Schiffman, Mike, et al. Hacker's Challenge 2: Test Your Network Security & Forensic Skills. McGraw-Hill Osborne Media, 2002.

Schweitzer, Douglas. Incident Response: Computer Forensics Toolkit. Wiley, 2003.

Zalewski, Michal. Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks. No Starch, 2005.

（本ページは意図的に白紙のままとする）

付録F—オンラインのツールおよび資料

以下の一覧に、フォレンジック能力の確立やコンピュータやネットワークのフォレンジックの実行に役立つオンラインのツール（特に、無料のものやオープンソースのもの）および資料の例を示す。

フォレンジックをサポートしている組織

組織	URL
Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice	http://www.cybercrime.gov/
Federal Bureau of Investigation (FBI)	http://www.fbi.gov/
Florida Association of Computer Crime Investigators (FACCI)	http://www.facci.org/
High Technology Crime Investigation Association (HTCIA)	http://www.htcia.org/
International Association of Computer Investigative Specialists (IACIS)	http://www.cops.org/
National Law Enforcement and Corrections Technology Center–North East (NLECTC-NE)	http://www.nlectc.org/nlectcne/
National White Collar Crime Center (NW3C)	http://www.nw3c.org/
Regional Computer Forensics Laboratory (RCFL)	http://www.rcfl.gov/
SEARCH: National Consortium for Justice Information and Statistics	http://www.search.org/

技術資料サイト

資料名	URL
Computer Crime Research Center	http://www.crime-research.org/
Computer Forensics Links (compiled by Dave Dittrich)	http://staff.washington.edu/dittrich/
Computer Forensics Links and Whitepapers	http://www.forensics.nl/links/
Computer Forensics Tool Testing (CFTT) Project	http://www.cftt.nist.gov/
Digital Mountain Technical and Legal Resources	http://www.digitalmountain.com/technical_resources
The Electronic Evidence Information Center	http://www.e-evidence.info/
Forensic Focus–Billboard and Links	http://www.forensicfocus.com/
National Institute of Justice (NIJ) Electronic Crime Program	http://www.ojp.usdoj.gov/nij/topics/ecrime/welcome.html
National Software Reference Library (NSRL)	http://www.nsrl.nist.gov/
Technology Pathways Resource Center	http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14
Wotsit's Format	http://www.wotsit.org/

トレーニング資料

トレーニング資料名	URL
CompuForensics	http://www.compuforensics.com/training.htm
Computer Forensic Services	http://www.computer-forensic.com/training.html
Computer Forensics Training Center Online	http://www.cftco.com/
Federal Law Enforcement Training Center (FLETC), Computer & Financial Investigations (CFI) Division	http://www.fletc.gov/cfi/index.htm
Foundstone	http://www.foundstone.com/
IACIS	http://www.iacis.info/iacisv2/pages/training.php
InfoSec Institute	http://www.infosecinstitute.com/courses/computer_forensics_training.html
MIS Training Institute (MISTI)	http://www.misti.com/
New Technologies Inc. (NTI)	http://www.forensics-intl.com/training.html
NW3C	http://www.nw3c.org/ocr/courses_desc.cfm
SANS Institute	http://www.sans.org/

そのほかの技術資料文書

資料名	URL
Basic Steps in Forensic Analysis of Unix Systems, by Dave Dittrich	http://staff.washington.edu/dittrich/misc/forensics/
Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000, by Norman Haase	http://www.sans.org/rr/whitepapers/incident/647.php
Digital Investigation: The International Journal of Digital Forensics & Incident Response	http://www.compseconline.com/digitalinvestigation/
Electronic Crime Scene Investigation: A Guide for First Responders	http://www.ncjrs.gov/
Evidence Seizure Methodology for Computer Forensics, by Thomas Rude	http://www.crazytrain.com/seizure.html
Forensic Analysis of a Live Linux System, by Mariusz Burdach	http://www.securityfocus.com/infocus/1769 (part one), http://www.securityfocus.com/infocus/1773 (part two)
How to Bypass BIOS Passwords	http://labmice.techtarget.com/articles/BIOS_hack.htm
International Journal of Digital Evidence	http://www.utica.edu/academic/institutes/ecii/ijde/
NIST Interagency Report (IR) 7100, PDA Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/index.html
NIST IR 7250, Cell Phone Forensic Tools: An Overview and Analysis	http://csrc.nist.gov/publications/nistir/index.html
NIST SP 800-31, Intrusion Detection Systems	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-44, Guidelines on Securing Public Web Servers	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 800-61, Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-72, Guidelines on PDA Forensics	http://csrc.nist.gov/publications/nistpubs/index.html
NIST SP 800-83, Guide to Malware Incident Prevention and Handling	http://csrc.nist.gov/publications/nistpubs/index.html
An Overview of Steganography for the Computer Forensic Examiner, by Gary Kessler	http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm

資料名	URL
RFC 3164: The BSD Syslog Protocol	http://www.ietf.org/rfc/rfc3164.txt
RFC 3227: Guidelines for Evidence Collection and Archiving	http://www.ietf.org/rfc/rfc3227.txt

フォレンジックソフトウェアの一覧がある Web サイト[128]

ソフトウェアのタイプ	Web サイト名	URL
侵入検知および侵入防止システム	Honeypots.net	http://www.honeypots.net/ids/products/
ネットワークパケットスニッファおよびプロトコルアナライザ	Packet Storm	http://packetstormsecurity.org/defense/sniff/
ネットワークプロトコルアナライザ	Softpedia	http://www.softpedia.com/get/Network-Tools/Protocol-Analyzers-Sniffers/
コンピュータおよびネットワーク用の各種ツール	Forensic and Incident Response Environment (F.I.R.E.)	http://fire.dmzs.com/?section=tools
	Foundstone	http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/freetools.htm
	Freshmeat	http://freshmeat.net/search/?q=forensic&section=projects
	Helix	http://www.e-fense.com/helix/
	Open Source Digital Forensics Analysis Tool Categories	http://www.opensourceforensics.org/tools/categories.html
	Penguin Sleuth Kit	http://www.linux-forensics.com/forensics/pensleuth.html
	Talisker Security Wizardry Portal	http://www.networkintrusion.co.uk/
	The Sleuth Kit	http://www.sleuthkit.org/sleuthkit/tools.php
	The Ultimate Collection of Forensic Software (TUCOFS)	http://www.tucofs.com/tucofs.htm
	Top 75 Security Tools	http://www.insecure.org/tools.html
	Trinux	http://trinux.sourceforge.net/
コンピュータ用の各種ツール	Checksum Tools	http://lists.thedatalist.com/pages/Checksum_Tools.htm
	Computer Forensics Tools, Software, Utilities	http://www.forensix.org/tools/
	Funduc Software	http://www.funduc.com/
ネットワーク用の各種ツール	Common Vulnerabilities and Exposures (CVE)	http://www.cve.mitre.org/compatible/product.html

[128] この一覧に示すアプリケーション群は、フォレンジックに使用されるアプリケーションの網羅的な一覧ではない。また、この文書で特定の製品を暗に推奨しているわけでもない。

（本ページは意図的に白紙のままとする）

付録G—索引

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

は

ひ

ふ

ほ

め

や

ゆ

よ

り

る

ろ