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

Special Publication 800-40
Version 2.0

パッチおよび脆弱性管理プログラムの策定

米国国立標準技術研究所（NIST）による推奨

Peter Mell
Tiffany Bergeron
David Henning

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 800-40
Version 2.0

パッチおよび脆弱性管理プログラムの策定

米国国立標準技術研究所
による推奨

Peter Mell
Tiffany Bergeron
David Henning

コンピュータセキュリティ

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

2005 年 11 月

米国商務省　長官

Carlos M. Gutierrez

技術管理局　技術担当商務次官

Michelle O'Neill

米国国立標準技術研究所　所長

William A. Jeffrey

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所(NIST: National Institute of Standards and Technology、以下、NIST と称す)の情報技術ラボラトリ(ITL: Information Technology Laboratory)は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。情報技術ラボラトリは、テストの実施、テスト技法の開発、参照データの作成、実装によるコンセプト実証、技術的分析を通じて、情報技術の開発と生産的利用の発展に努めている。情報技術ラボラトリの責務は、連邦政府の情報システムにおいて、費用対効果の高いセキュリティを施し、国家安全保障にかかわらない情報のプライバシを確保するための技術的、物理的、管理的および運用のための標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、情報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、普及活動並びに産業界、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 800-40 Version 2.0
米国国立標準技術研究所、Special Publication 800-40 Ver. 2.0、75 ページ(2005 年 11 月)

謝辞

本書執筆者である Peter Mell（NIST）、Tiffany Bergeron（MITRE Corporation）、および David Henning（Hughes Network Systems, LLC）は、本文書の作成を支援してくれた Rob Pate（US-CERT: United States Computer Emergency Readiness Team）に感謝の意を表したい。さらに、本文書の初版の共同執筆者であり、今回の版にも重要なアドバイスを提供してくれた Miles Tracy（米国連邦準備制度理事会）と、付録に掲載したパッチ適用のリソースを収集してくれた Tanyette Miller（Booz Allen Hamilton）にも感謝したい。また、洞察に満ちた論評を提供してくれた Timothy Grance（NIST）、Manuel Costa と Todd Wittbold（MITRE Corporation）、Matthew Baum（the Corporation for National and Community Service）、および Karen Kent（Booz Allen Hamilton）と、特に有益な意見や提案を提供してくれた保健社会福祉省、国務省、環境保護局、連邦準備制度理事会、および PatchAdvisor の代表者にも、感謝の意を表したい。

商標について

目次

付録

図

表

要旨

パッチおよび脆弱性管理は、組織内部に存在する IT 脆弱性の悪用を事前に防止するために設計された、セキュリティプラクティスである。その結果として、脆弱性および脆弱性の悪用に対応するための時間と費用の低減が期待される。システムの脆弱性の事前管理を行うことで、悪用の可能性が低減または排除され、悪用された後に対応する場合に比べて必要となる時間と労力が大幅に減少する。

パッチとは、ソフトウェア内の問題（いわゆる「バグ」）を解決するために開発された追加コードである。パッチによって、機能を追加したり、プログラム内部のセキュリティ上の欠陥を解決したりすることができる。脆弱性とは、悪意のある者が、コンピュータシステムに関して許可されている以上のアクセスや特権を得るために、悪意のある者によって悪用される可能性がある欠陥である。脆弱性のなかにはパッチで対応できないものもある。このため、システム管理者は、該当する脆弱性や入手可能なパッチだけでなく、ほかの修正措置（装置やネットワークの構成変更、従業員のトレーニングなど）についても知っておく必要がある。

この文書では、セキュリティパッチおよび脆弱性管理プログラムの作成およびプログラムの実効性のテストに関するガイダンスを提供する。主な対象読者は、このプログラムの設計と実施を担当するセキュリティ管理者である。ただし、この文書には、パッチの適用やソリューションの導入を担当するシステム管理者や運用担当者にとって有用な情報（つまり、パッチのテストやエンタープライズ向けパッチ適用ソフトウェアに関する情報）も含まれる。

一般に、セキュリティ問題に対するタイムリーなパッチ適用は、情報技術（IT）システムの運用の可用性、機密性、完全性を維持するために不可欠なものと認識されている。しかしながら、ユーザがオペレーティングシステムやアプリケーションに対して、常にパッチを適用しているとは限らず、このことはセキュリティや IT の専門家によって明らかにされている、最も一般的な問題の 1 つである。新しいパッチは日々リリースされているが、経験豊富なシステム管理者でさえ、すべてのパッチをタイミングよく適切に導入することは困難である。過去数年間における主要な攻撃のほとんどは、その攻撃が発生する前に既にパッチが準備されている既知の脆弱性を標的にしていた。実際、パッチがリリースされると同時に、攻撃者は連携してパッチのリバースエンジニアリングを速やかに（数日またはわずか数時間の調査を）行い、脆弱性を特定し、脆弱性実証コードを開発してリリースする。それに対し、大部分の組織ではパッチの入手、テスト、および導入までにタイムラグがある。したがって、皮肉なことにパッチをリリースした直後が特に脆弱な瞬間となる。

この深刻化する問題に対応するため、すべての組織は、パッチをタイムリーに導入することによって脆弱性への露出を管理するために、体系的で責任の所在が明確な、文書化されたプロセスを備えることを推奨する。この文書では、組織がこの目標を達成するために使用できる原則と手法について説明する。各組織は、たとえ正式なパッチおよび脆弱性管理プロセスを利用したとしても、パッチの適用や脆弱性の軽減は、簡単なプロセスではないことを認識すべきである。この文書は、パッチ適用に関する運用上の問題に役立つように、パッチの優先順位付け、入手、テスト、および適用などの領域もカバーする。また、パッチ適用プログラムの実効性のテストについて説明し、そのためのさまざまなメトリクスを示す。

NIST は、連邦政府機関が、パッチおよび脆弱性管理に役立つ以下の事項を実施することを推奨する。これらの任務を担当するものは、関連する個々の重要な問題を十分に理解するため、この文書の該当するセクションを読むこと。

各組織は、組織内部でパッチを特定し、配布を円滑に行うために、パッチおよび脆弱性グループ（PVG）を設置すること。

PVG は特に、組織全体のパッチおよび脆弱性管理プログラムの実施を任務とすべきである。PVG は、脆弱性に対する修正措置導入（OS およびアプリケーションへのパッチ適用や構成変更）の中心的存在となる。PVG は現場の管理者と積極的に連携する必要があるため、大規模な組織では、複数の PVG を設置する必要がある場合もある。各 PVG は相互に連携したり、権限を持つ最上位の PVG を主体に階層構造を形成してもよい。PVG の責務には、以下のものが含まれる。

1. 組織の IT リソースのインベントリを作成し、組織内部で使われているハードウェア機器、オペレーティングシステム、およびソフトウェアアプリケーションを確認する。

2. セキュリティソースを監視して、脆弱性の公表、パッチあるいはパッチ以外による修正措置、および PVG のシステムインベントリに含まれているソフトウェアに対応する新たに発生した脅威がないかどうかを確認する。

3. 組織において脆弱性の修正に取り組む優先順位を決定する。

4. 組織に適用する必要がある修正措置のデータベースを作成する。

5. 標準化された構成を使用する IT 機器に対するパッチおよびパッチ以外による修正措置をテストする。

6. 脆弱性に対する修正措置を監督する。

7. 脆弱性および修正措置の情報を現場の管理者に配布する。

8. エンタープライズ向けパッチ管理ツールを使って、IT 機器に対して自動化されたパッチ導入を実施する。

9. 可能かつ該当する場合は常にアプリケーションの自動更新がなされるように設定する。

10. ネットワークおよびホストの脆弱性スキャンにより、脆弱性の修正措置を検証する。

11. 脆弱性の修正措置の適用方法について管理者をトレーニングする。

各組織は、自動化されたパッチ管理ツールを使うことで、システムへのパッチの配布を迅速に行うこと。

広範囲のコンピュータに手作業でパッチを適用する方法は、インストールする必要があるパッチの数が増え、また攻撃者による脆弱性実証コードの開発期間が短くなるにつれて、有効でなくなりつつある。パッチ適用や脆弱性の監視は気の遠くなるような作業に思えることもあるが、組織内の脆弱性を一貫して軽減することは、自動化されたパッチ技術を有効利用した、テスト済みの統合されたパッチ適用プロセスによって実現できる。エンタープライズ向けパッチ管理ツールを使用することにより、PVG（または PVG と緊密に連携するグループ）は、パッチを多数のコンピュータに自動かつ短時間で適用することができる。すべての中～大規模組織は、所有する大部分のコンピュータに対してエンタープライズ向けパッチ管理ツールを使用すべきである。たとえ小規模な組織であっても、何らかの自動化されたパッチ適用ツールに移行すべきである。

各組織は、段階的な方法でエンタープライズ向けパッチ管理ツールを導入すること。

パッチ管理ツールを段階的に実装することにより、パッチアプリケーションの全面導入の前に、小さなグループを使ってプロセスおよびユーザとのやり取りに関する問題を解決できる。ほとんどの組織では、パッチ管理ツールを、まず、標準化されたデスクトップシステム、および同様の構成を持つサーバ群により構成される単一プラットフォームのサーバファームに導入する。これが完了すると、次に組織は、マルチプラットフォーム環境、標準でないデスクトップシステム、レガシーコンピュータ、および例外的な構成のコンピュータを統合するという、より難しい問題に取り組む必要がある。自動化されたパッチ適用ツールが適用できないオペレーティングシステムやアプリケーションのほか、例外的な構成のコンピュータに対しては、手作業による方法が必要となる場合がある。そのような例としては、組み込みシステム、産業用制御システム、医療機器、実験システムなどがある。このようなコンピュータについては、手作業のパッチ管理プロセスに関する明文化された実践済みの手順が必要であり、PVG は現場の管理者による作業の手はずを整える必要がある。

各組織は、エンタープライズ向けパッチ管理ツールの導入に関するリスクを評価し、軽減すること。

エンタープライズ向けパッチ管理ツールはリスクを低減するためには非常に効果的だが、組織にとって新たなセキュリティリスクを生み出す可能性もある。たとえば、攻撃者が中央のパッチ管理コンピュータに侵入し、エンタープライズ向けパッチ管理ツールを利用して悪意のコードを効率的に配布することもできる。各組織は、エンタープライズレベルのアプリケーションの導入時に使用すべき標準的なセキュリティ手法によって、これらのリスクの一部を軽減する必要がある。

各組織は、IT リソースに対する標準化された構成の使用を検討すること。

IT エンタープライズ内の構成が標準化されていれば、パッチおよび脆弱性管理に要する労力が軽減される。構成が標準化されている組織では、パッチおよび脆弱性管理プログラムの実施がきわめて容易かつ低コストで可能になる。また、IT 機器に標準外の構成が使われている場合、PVG はパッチを十分にテストできない可能性がある。すべての IT 機器がそれぞれ独自の構成になっている環境では、個々の構成における各種パッチの副作用を予見できないため、エンタープライズ向けパッチ管理ツールを導入しても効果が得られない可能性がある。構成を標準化していない大規模な組織においては、包括的なパッチおよび脆弱性管理はほぼ不可能である。各組織は、IT リソース全体のなかで大きな部分を占める種類の IT リソースを標準化することに努力を傾けるべきである。NIST Special Publication 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)*』では、標準化の有効なツールとなるセキュリティ設定チェックリストの作成と使用に関するガイダンスを提供している。

各組織は、パッチおよび脆弱性管理プログラムの効果を定期的に測定し、必要に応じて是正措置を適用すること。

パッチおよび脆弱性のメトリクスは、攻撃を受ける可能性の高さ、脆弱性の軽減に要する時間、およびコスト(プログラムの不具合が業務に与える影響のメトリクスを含む)の 3 つに分類される。システムまたは IT セキュリティプログラムに関して、どのパッチおよび脆弱性のメトリクスを重視して測定するかは、パッチおよび脆弱性管理の成熟度に応じて決めるべきである。たとえば、攻撃を受ける可能性の高さのメトリクス(システムあたりのパッチの数、脆弱性の数、およびネットワークサービスの数など)は、一般に成熟度の高いプログラムよりも低いプログラムに対して使うほうが有効である。各組織は、各システムで測定するメトリクスの種類と各メトリクスの詳細を文書化する必要がある。システムの所有者およびシステムのセキュリティ責任者には、各メトリクスの現実的な履行目標を伝える必要がある。これらの目標を達成できたら、さらに意欲的な目標を設定することもできる。パッチおよび脆弱性のセキュリティのレベルをあげる場合は、システムのセキュリティ責任者やシステム管理者が悲鳴をあげることがないように慎重に行うことが重要である。

（本ページは意図的に白紙のままとする）

1. 序論

1.1 作成機関

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

NISTは、すべての政府機関システム [1]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関わるシステムには適用されない。このガイドラインは、行政管理予算局（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。

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ったりするものと解釈してはならない。

1.2 目的および有効範囲

この文書の目的は、組織によるセキュリティパッチおよび脆弱性修正措置プログラムの実施を支援することにある。この文書では、組織的プロセスの作成方法とそのプロセスの効果をテストする方法に焦点を当てる。また、脆弱性の修正に利用できる技術的ソリューションに関する情報提供にも努める。

1.3 対象読者

この文書は、主にセキュリティパッチおよび脆弱性修正措置プログラムの設計および実施を担当するセキュリティ管理者による使用を目的としている。ただし、この文書には、パッチの適用やソリューションの導入を担当するシステム管理者や運用担当者にとって有用な情報（つまり、パッチのテストやエンタープライズ向けパッチ適用ソフトウェアに関する情報）も含まれる。

1.4 背景

2003 年 7 月から 2005 年 6 月までに公表されたコンピュータの脆弱性の数は年平均 2513 件であり、1 日当たり 7 件近くにのぼる [2]。サーバが 1 台しかない小規模な組織でも、毎月いくつもの重要なパッチを確認するために時間を費やすことが予想される。このように脆弱性が絶え間なく出現するため、システムは常に新しい攻撃の脅威にさらされている。

---

1 ここでいう「システム」とは、直接の運営と予算管理の体制が共通であり、同じ機能と任務上の目標を持ち、セキュリティのニーズが本質的に同じであり、同一の一般的な運用環境に存在する一連の情報技術（IT）資産、プロセス、アプリケーション、および関連する IT リソースを指す。すべての IT システムは、NIST Special Publication 800-18 で規定されているように、「一般支援」か「主要アプリケーション」のいずれかに分類される。

2 このデータは、National Vulnerability Database（http://nvd.nist.gov/）に基づく。

攻撃によって受ける損害は、非常に深刻なものになる場合がある。ここ数年、Code Red、Nimda、Blaster、MyDoomなど、数多くのインターネットワーム（インターネット経由の脆弱性を悪用する自己増殖型のコード）がリリースされている。これらのワームの発生にはいくつかの共通点がある。1つは、ワームコードの作成者の手口が巧妙化するにつれ、ワームが拡散する速度が以前より速まっている点である。もう1つは、ワームが世界中の何千何万というコンピュータを攻撃する点である。最も重要な点は、どのワームもパッチやそのほかの軽減手段がすでに公開されている既知の脆弱性を攻撃したことである。[3]ワームの大規模な発生は、いずれも回避可能であった。

かつてベンジャミンフランクリンは、「予防の1オンスは治療の1ポンドに匹敵する」といった。パッチおよび脆弱性管理は「予防の1オンス」であり、インシデント対応は「治療の1ポンド」である。パッチ適用やそのほかの修正手段によって脆弱性をいつどのように軽減するかは、それに費やす時間、リソース、および費用に基づいて決定すべきである。たとえば、新しいコンピュータワームがリリースされたとする。このワームは阻止しない限り急速に拡散し、組織内のワークステーションに損害を与えるおそれがある。脆弱性を軽減しない場合の修復予想コストは、次の式で表される。

> 脆弱性を軽減しない場合の予想コスト＝W×T×R（W：ワークステーションの数、T：システムの修復に要する時間または生産性が失われた時間、R：1時間当たりのコスト）[4]

たとえば、ある組織に修復が必要なコンピュータが1000台あり、各コンピュータの停止時間が平均8時間（作業員がシステムを再構築するための4時間と、コンピュータの所有者がそのコンピュータを使って作業できなかった4時間の合計）で、賃金および手当が1時間当たり＄70の場合は、次のようになる。

> 1000（コンピュータの台数）×8（時間）×＄70／時＝＄560,000（攻撃されたあとに対応した場合のコスト）

これを手作業による監視と予防を行った場合のコストと比べてみよう。ワームが作成される前に、ワームによって悪用される脆弱性とそれに対応するパッチが公表されたとする。過去の悪用事例をみると、本当のゼロデイアタックが発生する頻度は低いので、この仮定は今までのところ正確といえる。1種類のワークステーションに対する新規パッチの公開を手作業で監視するのに要する時間は、1日10分（年60.8時間）ほどでしかない。ワークステーションのパッチを適用するのに要する時間はせいぜい10分である。これをコストの式に当てはめると、次のようになる。

> 60.8（監視に要する時間）×＄70／時＝＄4,256（年間の監視コスト）
>
> 0.16（パッチ適用に要する時間）×1,000（コンピュータの台数）＠＄70／時＝＄11,200（手作業によるパッチ適用にかかるコスト）
>
> システムの保守にかかる総コスト＝＄4,256＋＄11,200／パッチ

1つの脆弱性に対して広範囲に増殖するワームが作成される場合は、ワームに感染した時点で対応するよりも、手作業でシステムの監視とパッチ適用を行ったほうがはるかに費用対効果が高い。しかし、パッチが絶え間なくリリースされる場合、組織の運用環境がごく少数のソフトウェアパッケージで構成される場合（したがって、必要なパッチの総数が少ない）やシステムへのパッチ適用をエン

---

3 1990年代の後半以降、新たに発見される重大な脆弱性の公表から、新たに作成される悪用手段のリリースまでの時間は、月単位から週単位または日単位にまで短縮している。

4 セキュリティインシデントによって発生する費用には、この式によって算出される費用のほかに、組織の評判が悪化することによる損害も含まれる。これは、取扱いに注意を要する情報や活動を任されている組織にとってきわめて重大なことである。組織が脆弱性を軽減しない場合のコストを推定する場合は、組織の評判に対する潜在的な影響を考慮すべきである。

ドユーザに依存している場合（したがって、パッチ適用の負担は分散するが、パッチのインストールを監督する必要が生じる）を除き、手作業によるパッチ適用には法外な費用がかかる。使用するソフトウェアパッケージの数が少ない組織や、システムへの効果的なパッチ適用をエンドユーザに依存する組織はほとんど存在しないため、手作業による広範囲のパッチ適用は費用対効果が高い組織的アプローチではない。[5]

3 つ目の方法は、自動化されたパッチ適用ソリューションへの投資である。これらのソリューションは、必要なパッチを自動的にチェックして導入する。無料のソリューションと商用ソリューションの両方がある。たとえば、商用ソリューションの価格が＄15,000 で、年間保守契約にコンピュータ 1 台当たり＄20 かかるとする。このアプローチは、専任スタッフを 1 人配置して、自動化されたソリューションによる保守、更新、およびパッチ適用を担当させる必要があるとしても、手作業によるソリューションに比べてはるかに安価である。

> 40 時間／週×52 週／年×＄70／時＝＄145,600／年（管理者がパッチ適用ソリューションを運用するのにかかるコスト）
>
> ＄145,600＋1,000（コンピュータの台数）×＄20／コンピュータ＝＄165,600（自動化されたソリューションによるパッチ適用の年間コスト）

パッチをインストールせずに費用を節約することは不可能である。手作業によるパッチ適用はコストがきわめて高く、効果的に実施することが難しい。このため、NIST はすべての組織が自動化されたパッチ適用ソリューションを有効利用することを強く推奨する。

1.5 構成

本文書は以降、次のように構成されている。

- セクション 2 では、セキュリティパッチおよび脆弱性修正措置プログラムの導入について推奨する管理プロセスを説明する。
- セクション 3 では、セキュリティパッチおよび脆弱性修正措置プログラムの成果を測定するために使用するセキュリティメトリクスについて論じる。
- セクション 4 では、セキュリティパッチおよび脆弱性修正措置プログラムの管理におけるさまざまな問題を明らかにする。特に、このセクションではエンタープライズ向けパッチ適用ソリューションを中心に扱う。
- セクション 5 では、米国政府における脆弱性およびパッチ適用のリソースについて簡単に説明する。
- セクション 6 では、この文書の主な結論を要約する。

また、本文書には、次のような付録（関係資料）が含まれている。

- 付録 A に、本文書で使用している一般的な頭字語を示す。
- 付録 B は、本文書で使用している用語の解説を示す。
- 付録 C に、一般的によく利用される種類のパッチ適用リソースについて説明する。
- 付録 D に、よく利用されるパッチ適用リソースの一覧を示す。
- 付録 E に、本文書の索引を示す。

---

[5] 多くのレガシーシステムや特殊なシステムでは、手作業によるパッチ適用が依然として有効である。

（本ページは意図的に白紙のままとする）

2. パッチおよび脆弱性管理プロセス

このセクションでは、パッチおよび脆弱性管理に対する体系的アプローチについて論じる。このアプローチは、組織が必要に応じてその環境に適応させるべきモデルとして示される。このようなアプローチは、増え続ける IT システムの脆弱性に対して、費用対効果の高い方法で対応するために必要である。

2.1 推奨プロセス

NIST は、各組織が、パッチおよび脆弱性管理プログラムの実施を専任する個人で構成されるグループを設置することを推奨する。PVG は、脆弱性に対する修正措置導入（パッチ適用や構成変更など）の中心的存在となる。PVG は現場の管理者と積極的に連携する必要があるため、大規模な組織では、複数の PVG を設置する必要があるかもしれない。各 PVG は相互に連携したり、権限を持つ最上位の PVG を主体に階層構造を形成してもよい。以降では、各組織に PVG が 1 つだけ存在することを前提とする。

修正措置の実施およびテストに関わる負荷は、できるだけ現場の管理者から PVG に移すべきである。これによって、作業の重複（複数のシステム管理者が同じようなコンピュータで同じパッチをテストするなど）がなくなり、自動化されたソリューションを使用することでコストのかかる手動インストールを回避できるようになるため、費用が節約されるはずである。これを実現する最も簡単な方法は、PVG（または PVG と緊密に連携するグループ）が、パッチを多数のコンピュータに自動かつ短時間で適用できる、エンタープライズ向けパッチ適用ソリューションを導入することである。自動化されたパッチ管理ツールを利用できない場合、PVG は現場の管理者の作業を調整する必要がある。

PVG が自動的に導入されるパッチを十分にテストできるように、各組織は IT 機器（デスクトップコンピュータ、ルータ、ファイアウォール、サーバなど）に対して、可能な限り標準化された構成を使用すべきである。すべての IT 機器がそれぞれ独自の構成になっている環境では、個々の構成における各種パッチの副作用を予見できないため、エンタープライズ向けパッチ管理ツールを導入しても効果が得られない可能性がある。

費用対効果の高いPVGを導入するには、PVGの守備範囲を明確に定義する必要がある。PVGは、組織内部で広く使用されているIT技術に関連する脆弱性と修正措置のみを監視し、それらのみを対応する。[6]このIT技術のリストを入念に作成し、現場のすべての管理者が参照できるようにする。現場の管理者は、PVGの守備範囲に入らないIT技術の安全を保つ責任を負う。PVGは、現場の管理者に対して、この職務の遂行方法に関する支援およびトレーニングを提供する。本セクションの以降の部分は、PVGとシステム管理者の役割および責任について詳しく説明する。

2.1.1 パッチおよび脆弱性グループ

PVG は、情報セキュリティと運用の代表者を含めた正式なグループとすべきである。これらの代表者には、脆弱性とパッチの管理に加えて、システム管理、侵入検知、およびファイアウォール管理に詳しい人物を含める。さらに、組織内部で最も多く使われているオペレーティングシステムやアプリケーションの専門家がいると便利である。システムやネットワークの管理、脆弱性のスキャン、または侵入検知システムの操作をすでに担当している要員も、PVG のメンバー候補である。

[6] 組織によっては、組織内部で使われるすべての IT 技術の脆弱性と修正措置を PVG に監視させる場合もある。これは、組織内で使われている IT 技術の種類が比較的少ない場合や、PVG に代わって必要なすべての IT 技術を監視できる外部の脆弱性監視サービス（付録 C で説明するような）を PVG が使用する場合に最も実現可能である。

グループの規模や PVG の責務に費やされる時間は、組織によって大きく異なる。大部分は、組織の規模と複雑さ、組織内のネットワークの規模と複雑さ、組織の予算によって決まる。小規模な組織では、PVG を 1～2 名のメンバーで構成し、対象を重要な脆弱性とシステムのみに絞ることができる。パッチおよび脆弱性管理は、組織の規模やリソースに関係なく、適切な計画とプロセスによって達成できる。

PVG の責務の概要を以下に示す。これ以降のセクションでは、いくつかの責務について詳しく説明する。

1. **システムインベントリを作成する。**PVGは、組織のITリソースに関する既存のインベントリを使って、組織内部で使用しているハードウェア機器、オペレーティングシステム、およびソフトウェアアプリケーションを確認する。PVGは、既存のインベントリでは把握されていないITリソースについても、手作業によってインベントリを管理する。セクション 2.2 に、インベントリの作成に関する詳しいガイダンスを示す。

2. **脆弱性、修正措置、および脅威を監視する。**PVGは、セキュリティソースを監視して、PVGのシステムインベントリに含まれるソフトウェアに対応する脆弱性の公表、パッチやパッチ以外による修正措置、および新たに発生した脅威がないかどうかを確認する。脆弱性、修正措置、および脅威に関する監視対象と監視方法については、セクション 2.3 で説明する。

3. **脆弱性修正措置の優先順位付けを行う。**PVGは、組織における脆弱性修正措置の導入の優先順位を決定する。詳しい情報は、セクション 2.4 を参照のこと。

4. **組織固有の修正措置データベースを作成する。**PVGは、組織に適用する必要がある修正措置のデータベースを作成する。詳しい情報は、セクション 2.5 を参照のこと。

5. **修正措置の一般的なテストを実施する。**PVGは、標準化された構成を使用するIT機器を対象としたパッチおよびパッチ以外による修正措置のテストを実施する必要がある。これにより、現場の管理者が余分なテストを実行せずに済む。PVGは、現場の管理者と緊密に連携して、重要なシステムに対するパッチや構成変更のテストも行う。修正措置のテストに関する情報は、セクション 2.6 を参照のこと。

6. **脆弱性に対する修正措置を導入する。**PVGは、脆弱性の修正措置を監督する。このプロセスに関する情報は、セクション 2.7 を参照のこと。

7. **現場の管理者に対して脆弱性および修正措置の情報を配布する。**PVGは、組織のソフトウェアインベントリに存在し、かつ、PVGの守備範囲に含まれるソフトウェアパッケージの脆弱性と修正措置の情報を、現場の管理者に通知する責任を負う。詳しい情報は、セクション 2.8 を参照のこと。

8. **パッチの自動導入を実施する。**PVGは、エンタープライズ向けパッチ管理ツールを使ってIT機器に自動的にパッチを導入する。または、実際にパッチ管理ツールを実行するグループと緊密に連携することもできる。自動化されたパッチ適用ツールにより、管理者は 1 つのコンソールから数百あるいは数千のシステムを更新できる。デスクトップシステムが標準化されており、各サーバが同様の構成になっている均一なコンピュータプラットフォームの場合、導入はきわめて容易である。マルチプラットフォーム環境、標準でないデスクトップシステム、レガシーコンピュータ、および例外的な構成のコンピュータが組み込まれている場合であっても、自動化されたパッチ適用ツールを使用することができる。エンタープライズ向けパッチ適用ツールについては、セクション 4.1 で説明する。

9. **アプリケーションの自動更新を設定する（可能かつ該当する場合は常に）。**最近のアプリケーションの多くは、ベンダーのWebサイトにアクセスして、適用可能なアップデートが存在するかどうかをチェックする機能を備えている。この機能は、パッチの特定、配布、インストールに必要な労力を最小限に抑える上で非常に有効である。ただし、組織の構成管理プロセスの妨げとなる可能性があるため、この機能の使用を望まない組織もあるだろう。推奨される方法としては、組織のネットワークから、自動更新プロセスを使ってパッチをローカルに入手する方法である。この場合、インターネット経由ではなく、ローカルネットワークからアプリケーションの更新が可能である。このようなツールについては、セクション 4.1 でエンタープライズ向けパッチ適用ツール全般との関連において論じる。

10. **ネットワークおよびホストの脆弱性スキャンにより脆弱性修正措置を検証する。**PVGは、脆弱性に対する修正措置が正常に行われたことを確認する。修正措置の検証については、セクション 2.9 で説明する。

11. **脆弱性の修正措置についてトレーニングを行う。**PVG は、管理者に対して、脆弱性の修正措置の実施に関する教育を施す。コンピュータへのパッチの適用をエンドユーザに委ねる場合、PVG は、エンドユーザに対して、適切な教育を施さなければならない。詳しいガイダンスは、セクション 2.10 を参照のこと。

2.1.2 システム管理者

システム管理者は、該当する IT リソースが組織の標準構成に従っていること、およびそれらの IT リソースが組織の自動パッチ適用システムの対象に含まれることを確実にする責任を負う。自動化されたパッチ適用システムを使用していない組織の場合、システム管理者は PVG を脆弱性修正措置の主要リソースとして使用し、修正措置の適用期間に従って PVG と連携する必要がある。システム管理者は、PVG の守備範囲外にある IT リソースについて、脆弱性と修正措置の監視、修正措置のテスト、および修正措置の適用を行う責任を負う。

2.2 システムインベントリの作成

NIST は、PVG が組織の IT リソースに関する既存のインベントリを使って、組織内部で使用しているハードウェア機器、オペレーティングシステム、およびソフトウェアアプリケーションを確認し、それらのリソースのグループ化と優先順位付けを行うことを推奨する。PVG は、既存のインベントリでは把握されていない IT リソースについても手作業によるインベントリを管理すべきである。システムインベントリと優先順位のリストは、PVG が、脆弱性、パッチ、および脅威の監視によってサポートすべきハードウェアとソフトウェアアプリケーションを特定し、迅速かつ効果的な対応を行うために役立つ。

2.2.1 IT インベントリ

システムの運用認可 [7]に先立って、システムの内部にあるすべてのITリソースのインベントリを作成すべきである。このインベントリは、システムの構成管理プロセスの一環として定期的に更新すべきである。組織の全システムの集合がすべてのITリソースをカバーするように、それぞれのITリソースはいずれかのシステムに割り当てられる必要がある。

システムごとに独立したインベントリを作成して管理する方法は、費用対効果が高くない可能性がある。このため各組織は、すべてのITリソースを含む組織全体を対象としたインベントリを管理する

[7] NIST Special Publication（SP）800-37 には、システムの運用認可に関する詳しい説明が含まれている。この文書は、http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf から入手できる。

方法を選ぶことがある。これは、各ITリソースが 1 つのシステムにのみ対応するようにラベル付けされている限り、まったく問題ない（また、多くの場合推奨される）。各システムに対応するITリソースのリストを出力する機能は必須である[8]。

各組織は、インベントリの作成にあたってどのようなレベルの情報を抽出するかを決定する必要がある。たとえば、各コンピュータにインストールされているソフトウェアを追跡する組織もあれば、ソフトウェアのバージョン番号まで追跡する組織もあるだろう。収集する情報量が少なすぎるのもよくないが、多すぎるのも（さらに）よくないため、各組織は抽出のレベルを慎重に選択すべきである。各組織は、（パッチ管理のほかに）インベントリの用途を決定し、それらの用途に必要な情報のみを収集すべきである。

組織がインベントリに含めることができる項目のリストの例を以下に示す（ただし、項目の中には、すべての IT リソースに当てはまらないものもある）。

1. 対応するシステム名
2. プロパティ番号
3. IT リソースの所有者（メインユーザなど）
4. システム管理者
5. 物理的な場所
6. 接続しているネットワークポート
7. ソフトウェア構成
    a. オペレーティングシステムとバージョン番号
    b. ソフトウェアパッケージとバージョン番号
    c. ネットワークサービス
    d. IP（Internet Protocol）アドレス（静的アドレスの場合）
8. ハードウェア構成
    a. CPU
    b. メモリ
    c. ディスク容量
    d. Ethernet アドレス（ネットワークカードなど）
    e. ワイヤレス通信機能
    f. 入出力機能（USB、Firewire など）
    g. ファームウェアのバージョン

通常、こうした個々の IT リソースの情報をユーザに手作業で入力させるのは現実的でない。このアプローチを試みた組織では、不正確で更新頻度の低い IT リソース情報を大量に含んだインベントリが作られることになるだろう。より効果的なアプローチは、できる限り市販の自動化されたインベントリ管理ツールを使用することである。通常、これらのツールを使用する組織では、各コンピュータにエージェントをインストールする必要がある。このエージェントは、コンピュータの構成変更をア

[8] 多くの場合、組織には IT リソースのインベントリが複数存在する。たとえば、組織が自動資産管理ソフトウェアを使って、機器および機器で実行されるソフトウェアに関するインベントリを作成する場合もある。また、インベントリの作成は、事業継続計画やそのほかの活動の一環として行うこともある。

クティブに監視し、変更があった場合に、中央データベースに報告することによって、システムの IT リソースの正確な状況を PVG や管理職層に提供する。残念なことに、自動化されたツールには限界があり、一部の情報（物理的な位置など）を手動で入力しなければならない。自動化されたツールには、ユーザ記入用フォームを通じて定期的にこの情報を収集するオプションが用意されているはずである。

2.2.2 IT リソースのグループ化と優先順位付け

修正措置の作業をしやすくするために、インベントリ内のリソースをグループ化し、その優先順位を決めるべきである。リソースのグループ化と優先順位付けは、システムに対するリスクを評価する際の参考になるほか、パッチおよび脆弱性管理プログラムにおいて特別な注意を必要とするシステムを特定するのにも役立てるべきである。主たるグループ化は、システムの名称および連邦情報処理規格（Federal Information Processing Standard、以下、FIPSと称す）199 に定義されている影響の程度に応じたものにするべきである [9]。ネットワークの場所ごとにリソースをグループ化するのも有効である。これは、インターネットに直接公開されているリソースや、内部のセキュリティが高い領域に存在するリソースの場合、特に重要である。

このようなグループ化と優先順位付けを行わない場合、組織は、必要以上に費用のかかる修正措置を採用する可能性がある。たとえば、修正措置の優先順位付けを行わない組織の内部で新しい脆弱性が発見されると、システム管理者はすべての脆弱なコンピュータに直ちにパッチを適用するように指示されることが考えられる。その結果、コンピュータへのパッチ適用作業のためにシステム管理者のほかの作業がすべて中断し、大きな混乱が発生するおそれがある。さらに、十分なテストをせずにあわててパッチを適用した結果、組織のシステムが実際に損害を被るおそれもある。組織は、修正措置の優先順位付けを行うことにより、組織の標準的な構成管理プロセスとパッチテスト手順を使用して、一定の時間で脆弱なコンピュータの大部分にパッチを適用できることに気づく。この結果、組織は、当面のパッチ適用作業をリスクが最も高い脆弱なコンピュータ（おそらく、インターネットに直接公開されているコンピュータなど）に集中させることができる。

2.2.2.1 NIST Special Publication 800-18

ITリソースを公式に指定され運用が認可されたシステムへグループ化する際のガイダンスが、NIST Special Publication（SP）800-18 において提供されている [10]。それによれば、同じシステムにグループ化されるITリソースは次の特性を持っている必要がある。

- 各要素は、共通する直接の運営管理体制下にある。
- 各要素は、同じ機能あるいは任務上の目標を持つ。
- 各要素は、同様のセキュリティ運用上の特性とセキュリティニーズを持つ。
- 各要素が同一の一般的な運用環境に存在する。

2.2.2.2 連邦情報処理規格（FIPS: Federal Information Processing Standard）199

FIPS 199 は、連邦政府の情報および情報システムのセキュリティ分類を確立している。ほかの組織も、これらの標準を暫定的に適用したり、より正式なアプローチを採用したりすることもできる。セキュリティ分類は、情報または情報システムの機密性、完全性、または可用性の喪失による潜在的な影響に基づいて決定されている。このセキュリティ分類は、複数のシステムが関与する脆弱性に対して修正措置を導入する際の優先順位を決定するために使用されるべきである。

---

9 FIPS 199 は、http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf からダウンロードできる。

10 NIST SP 800-18 は http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF から入手できる。

2.2.2.3 システム間の優先順位付け

FIPS 199 を使用することにより、システム間での修正措置の作業の優先順位を決定するのに有益な情報が得られるが、多くの場合、これに加えてシステム境界内での優先順位づけが必要となる。PVG およびシステム担当者は、システムのどの IT リソースの優先順位が高いかを文書化する必要がある。一般的な優先順位の高いリソースは、次のいずれか 1 つ以上に分類されることが多い。

+ システムの運用に不可欠なリソース（サーバなど）
+ セキュリティ管理に使われるリソース
+ 組織のネットワーク境界にあるリソース
+ 重要性が高い情報を格納したリソース
+ 外部ユーザからアクセスされるリソース

PVG は、この優先順位付けにインベントリ情報を利用したり、これらの優先順位をインベントリ自体に格納したりすることができる。

2.2.3 IT インベントリの使用と関連する責務の範囲

インベントリは、PVG が組織の IT 構成を理解する際の手がかりであり、PVG が活動するための基盤である。インベントリは主に、PVG がサポートするハードウェア機器、オペレーティングシステム、およびソフトウェアアプリケーションのリストを作成するために使われる。また、PVG と管理者による脅威への迅速な対応を支援し、システム担当者にシステムの保護に役立つ情報を提供する。

2.2.3.1 サポートされるリソースのリスト

PVG は、サポートするハードウェア機器、オペレーティングシステム、およびソフトウェアアプリケーションのセットを定義する。その後、PVG は、サポートするハードウェア、オペレーティングシステム、およびアプリケーションに対応する脆弱性、パッチ、および脅威に関する情報の監視の責任を負う。PVG は、サポートするリソースをシステム管理者に明確に伝達することにより、PVG が、いずれのハードウェア、オペレーティングシステム、およびアプリケーションに対する新しいパッチ、脆弱性、および脅威をチェックするのかが管理者にわかるようにすべきである。サポートするリソースのリストは、インベントリを分析し、組織内部で使用しているリソースを特定することによって作成する。優先順位の高いシステム、取扱いに注意を要するシステム、または多くのシステムで使用されているハードウェア機器、オペレーティングシステム、およびソフトウェアアプリケーションはこのリストに含めるべきである。PVG はこのリストを公開することにより、システム管理者がサポートされていないリソースの有無や、それがいつから存在しているのかを識別できるようにする。システム管理者は、サポートされないハードウェア機器、オペレーティングシステム、およびソフトウェアアプリケーションを、個々に監視して修正するための方法について指導を受けるべきである。

2.2.3.2 システム担当者へのインベントリ情報の提供

PVGは、システムの所有者、システムのセキュリティ責任者、およびシステム管理者にもインベントリ情報へのアクセスを許可すべきである[11]。これにより、組織のシステムをより適切に保護できるようになる。ただし、システムインベントリ情報はその性質上取扱いに注意を要するので、システム担当者には各自が担当するシステムのインベントリへのアクセスのみを許可すべきである。インベント

[11] 通常、システム担当者には既存のインベントリへのアクセス権が与えられているが、PVG のインベントリの中には、PVG の許可なしにはアクセスできない追加的な情報が含まれる場合がある。

リを管理するためにはPVGとシステム担当者が緊密に連携する必要があるため、その意味でもシステム担当者にインベントリへのアクセスを許可することは重要である。

2.3 脆弱性、修正措置、および脅威の監視

PVG は、セキュリティソースを監視して、組織のソフトウェアインベントリに含まれているソフトウェアに対応する脆弱性の公表、パッチやパッチ以外による修正措置、および脅威がないかどうかを確認する責任を負う。PVG は、新たに発見されたすべての脆弱性を確実に把握できるように、さまざまなソースを監視するべきである。

2.3.1 セキュリティ懸案事項の種類

PVG は、担当するソフトウェアの脆弱性、修正措置、および脅威を監視する責任を負う。

- **脆弱性**ー脆弱性とは、システムのセキュリティ上の弱点につながるソフトウェアの欠陥または設定ミスのことをいう。悪意のあるものがポリシーを破るために（たとえば、アクセスが許可されているコンピュータに対して、必要以上に高いアクセス権限やパーミッションを得るために、脆弱性が悪用されるおそれがある。
- **修正措置**ー主な修正措置の方法には、ソフトウェアパッチのインストール、構成設定の調整、影響を受けたソフトウェアの削除の 3 つがある。修正措置の方法の詳細については、セクション 2.7 を参照のこと。
- **脅威**ー脅威とは、悪意のある主体が脆弱性を悪用し、場合によってはコンピュータシステムやネットワークに損害を与えるために開発した機能または手段のことをいう。通常、脅威は不正スクリプト、ワーム、ウイルス、ルートキット、およびトロイの木馬の形を取る。

システム管理者は、各自の管理下にあって、組織のインベントリに含まれていないソフトウェアが実行されているシステムについて、脆弱性、修正措置、および脅威を監視すべきである。

2.3.2 脆弱性、修正措置、および脅威の監視

脆弱性、修正措置、および脅威の状況を監視するために利用できるリソースには、いくつかの種類がある。付録 D には、よく利用されるリソースの一部を示すリストが含まれている。各種リソースには、それぞれの長所と短所がある。NIST は、正確でタイムリーな情報を得るために、複数の種類のリソースを使用することを推奨する。リソースの最も一般的な種類を以下に示す。

- ベンダーの Web サイトおよびメーリングリスト
- サードパーティの Web サイト
- サードパーティのメーリングリストおよびニュースグループ
- 脆弱性スキャナ
- 脆弱性データベース
- エンタープライズ向けパッチ管理ツール
- そのほかの通知ツール

付録 C では、脆弱性、パッチ、および脅威に関する情報を取得するための各種リソースの長所と短所について詳しく説明する。

ベンダーは、自社製品へのパッチに関する情報の信頼できる情報源である。ただし、多くのベンダーはパッチが用意できるまで自社製品の脆弱性を公表しないため、サードパーティの脆弱性リソースも監視することが推奨される。エンタープライズ向けパッチ適用ツールは、通常、サポート対象のベンダーから、入手可能なすべてのパッチのリストを提供する。これによって、PVG に課された、数多くのベンダーのセキュリティ Web サイトやセキュリティメーリングリストを常に監視するという作業が軽減される。

NIST は、各組織が少なくとも以下の種類のリソースを使って脆弱性、修正措置、および脅威を監視することを推奨する。

+ エンタープライズ向けパッチ管理ツール（サポート対象のベンダーから入手できるすべてのパッチを取得するため）
+ ベンダーのセキュリティメーリングリストおよびセキュリティ Web サイト（エンタープライズ向けパッチ管理ツールでサポートされないベンダーから、入手可能なすべてのパッチを取得するため）
+ 脆弱性データベースまたは脆弱性メーリングリスト（National Vulnerability Database など。すべての既知の脆弱性や推奨される修正措置に関して、即入手可能な情報を得るため）
+ 最も重大な脆弱性を明らかにするサードパーティの脆弱性メーリングリスト（US-CERT の Cyber Security Alerts など）。このようなメーリングリストは、より一般的な脆弱性リソースによって公開される無数の脆弱性のなかで、各組織が見落としがちな最も重要な脆弱性に焦点を当てるのに役立つ。

新しい脆弱性、修正措置、または脅威の初期評価の後、PVG はそれらを引き続き監視して、更新や新しい情報がないかどうかを確認すべきである。たとえば、ソフトウェアベンダーが、最初に推奨していたソフトウェアの再設定に取って代わる一時的な修正手段として、新しいパッチをリリースする場合がある。新しい情報の継続的な監視を実施することにより、PVG は新しいパッチが存在することに気付いたり、ソフトウェアの再設定よりも優れた解決策が提供されているかどうかを確認したりすることができる。脆弱性の追加的な分析により、脆弱性の深刻さが当初の予想とは異なることが確認される場合もあるため、その意味でも継続的な監視は重要である。

2.4 脆弱性に対する修正措置導入の優先順位付け

PVGは、脆弱性の修正措置に関する優先順位を決定するときに、組織に対する個々の脅威と、それらの脅威がもたらす潜在的な影響について考慮する必要がある。この評価には、以下の作業が含まれる [12]。

+ 脅威または脆弱性の深刻さを判定する。業務に不可欠なシステムと優先順位の高いそのほかのシステムに重点を置きながら、どのシステムが脆弱なのか、あるいは脅威にさらされているかを調べる。脆弱性が除去されず悪用された場合の、システム、組織、およびネットワークに対する影響を評価する。組織のセキュリティアーキテクチャによって特定の脅威が自動的に軽減され、特定のパッチを緊急に適用しなくても済む場合があることを忘れてはならない。たとえば、ブラウザ内の特定の機能（スクリプト言語など）を無効にしている組織では、それらのスクリプト言語に含まれる脆弱性を修正するパッチの適用は、優先順位が低い。

[12] PVG は、この評価を単独で実施することを期待されていない。システムやネットワークのセキュリティ責任者や管理者が、PVG が提供する脆弱性、修正措置、および脅威の情報に基づいて個々のシステムに対する脅威の影響を評価することによって PVG を支援する場合もある。

+ 関連するワーム、ウイルス、または悪用行為の存在、影響の度合い、および拡散範囲を特定する。悪意のコードが公開されているかどうか、およびどの程度広まっているかを確認する。発生した損害（システムへのアクセス、情報の漏えい、任意のコードの実行、サービス妨害など）を特定する。パッチはすぐにリバースエンジニアリングされてしまうことが多いため、各組織は、脆弱性に対応するパッチが存在する場合、その脆弱性を悪用するコードがすでに悪意のある個人の手に渡っていると想定すべきである。

+ パッチおよびパッチ以外による修正措置の適用に関わるリスクを特定する。修正によってほかのソフトウェアアプリケーションやサービスの機能に影響が出るかどうかを調査やテストを通じて明らかにする。受容できる リスクのレベルを設定する。

PVG は、現場の管理者が持つリソースの制約を認識し、特定された脆弱性に対するパッチやそのほかの修正措置の数の多さに現場の管理者が圧倒されないようにすべきである。小規模な IT 導入の場合を除き、すべての修正措置をタイムリーに行うことは、現場の管理者にとって複雑で困難な作業である。これは、時間やリソースの制約だけでなく、大規模な環境におけるシステムの複雑さや多様性にも起因している。したがって、パッチを適用するシステムの優先順位や適用の順序を設定することが、効果的なパッチプロセスにとって何よりも重要である。

2.5 組織固有の修正措置データベースの作成

PVGは、組織内部で適用する必要がある修正措置のデータベースを作成すべきである。通常、エンタープライズ向けパッチ管理ツールにはこのようなデータベースが用意されているが、場合によってはPVGがパッチ管理ツールでサポートされないIT技術のために個々のデータベースを手作業で管理する必要がある。手作業で管理するデータベースには、パッチのインストールや一時的な解決策の実行によって脆弱性を排除するための作業に関する指示と、該当する場合は実際のパッチを含めるべきである [13]。自動か手作業かにかかわらず、インターネットにアクセスできない場合やベンダーのWebサイトが侵害された場合に備えて、データベースに個々のパッチのコピーを含めるべきである。また、現場の管理者にとっては、ずらりと並んだ入手可能なパッチに圧倒されかねないベンダーのサイトよりも、PVGのデータベースを使用してパッチを適用するほうが、おそらく簡単である。データベースの作成が推奨される一方で、組織のリソースの制約により、各パッチのWebサイトや特定のURL（Uniform Resource Locator）のみを登録することにとどまる場合もある。このような方法は、パッチへのハイパーリンクが、PVGによって文書化されたアドバイスや適用期限に関連付けられている場合に、実現可能である。手作業で管理するデータベースを使用することもできるが、NISTはこのようなデータベースが最初から組み込まれている、自動化されたパッチ適用製品を購入することを強く推奨する。

2.6 修正措置のテスト

組織が標準化されたホスト構成を使用している場合、PVG はそれらの構成を対象にパッチおよびパッチ以外による修正措置のテストを行うことができる。これにより、それぞれのシステム管理者が余分なテストを実行せずに済む。システム管理者は、PVG が監視しないソフトウェアに関して特定された脆弱性や脅威を軽減するためのパッチおよびパッチ以外による修正措置を、テストする責任を負う。

システム管理者は、特定されたパッチおよびパッチ以外による修正措置を適用する前に、予防措置を講じるべきである。修正措置のテストのガイドラインには、以下のものが含まれる。

---

[13] 組織にとって、最も深刻な脆弱性や最も重要なパッチに対する脅威を評価し、その結果を要約したものを現場の管理者や管理職層に配布する、または、修正措置データベースから入手できるようにする、といった作業を PVG に託すことは有効であるこの要約は、修正措置の実行の重要性、および実行しなかった場合の結果を人々に理解させるという面でも有効である。

+ ほとんどのベンダーは、なんらかの認証メカニズムを提供する。ダウンロードしたパッチは、暗号チェックサム、PGP（Pretty Good Privacy）署名、ディジタル証明書を含むベンダーが提供する信頼性確認方法によってチェックすべきである。これらの方法のいくつか（ディジタル署名の検証など）は高度に自動化されており、ユーザの操作をほとんど必要としない。そのほかの方法（SHA-1 チェックサムやMD5 チェックサムなど）では、ユーザがベンダーのWebサイトにアクセスして、そこに表示されるチェックサムとダウンロードしたパッチのチェックサムを比較する必要がある [14]。これらの方法を採用することにより、認証レベルが一段階上がるが、これで安心というわけではない。

+ インストール前のすべてのパッチに対して、ウイルススキャンも実行すべきである。PVG またはシステム管理者は、スキャンを実行する前に、ウイルス対策プログラムのウイルスシグネチャデータベースが最新であることを確認する必要がある。これを実施したからといって絶対に安全とはいえない。たとえば、攻撃者がまったく新しいトロイの木馬を作成し、それをパッチに組み込んだ場合、それをウイルススキャンによって検出できない可能性がある。

+ 修正措置によって意図しない結果が容易に生じる可能性があるため、パッチや構成変更は実運用以外のシステムにおいてテストすべきである [15]。パッチの多くはきわめて複雑で、システムファイルを置き換えたり、セキュリティ設定を変更することがしばしばあるため、システムのさまざまな部分に影響を与える可能性がある。[16]パッチには、複数の脆弱性に対する修正やセキュリティ以外の変更（新しい機能など）が含まれることもある。また、パッチや構成変更は脆弱性をすみやかに修復するために急いでリリースされることが多く、元のソフトウェアに比べて十分にテストされていない場合が多い。パッチのインストール、構成の変更、およびソフトウェアのアンインストールによってシステムの動作が変わり、その結果、ほかのプログラムがクラッシュしたり、動作しなくなったりする可能性もある。

+ あるパッチをインストールすることで、別のパッチが意図せずアンインストールされたり無効になったりする場合もある。依存関係がある場合は、パッチを特定の順序でインストールする必要がある。また、ある特定のパッチをインストールしたときにほかのパッチがアンインストールされるかどうかを確認することも重要である。

+ 想定可能なシステム構成は数多く存在し、ベンダーがそのすべてを対象にテストすることは不可能であるため、PVG は導入済みのシステムの構成を忠実に反映しているシステムのうちのいくつかを対象に、テストを実施すべきである。こうすることで、修正措置によって意図しない結果が生じた場合に影響を受ける構成を、特定の構成に限定することができる。修正措置を実施したあとは、関連するすべてのソフトウェアが正常に動作していることをチェックする。

+ PGV は、修正措置を実施する前、たとえば、パッチを実運用システムに適用する前にテストを実施する時間やリソースが不足している場合などは特に、ほかの担当者がパッチのインストールや使用に関してどのような経験をしたかを知りたいと思う場合があるだろう。たとえば、ほかの担当者の経験から、パッチや構成の調整によって脆弱性が是正されるかどうか、古い脆弱性が再発するかどうか、新しい脆弱性が発生するかどうか、パフォーマンスが低下するかどうか、ほかの必要なアプリケーションとの不整合を起こすかどうか、などがわ

---

[14] 連邦政府機関は、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求められる。SHA-1 は FIPS で承認されたアルゴリズムだが、MD5 は違う。したがって、SHA-1 チェックサムが利用可能な場合、政府機関は MD5 やそのほかのチェックサムではなく必ず SHA-1 チェックサムを使用すべきである。

[15] 各組織は、パッチや構成変更に既存の変更管理プロセスを使用できる場合は、それを使用すべきである。また、テストシステム上や仮想マシン内で標準的な構成のイメージを使用することも、テストプロセスの効率化に役立つ。

[16] 例として、無効になっていたデフォルトユーザアカウントの有効化、デフォルトユーザアカウントのパスワードのリセット、無効になっていたサービスや機能の有効化などがある。

かる場合もある。ただし、ほかの担当者の経験は環境固有の要因、実装の違い、そのほかの理由によって異なる可能性があることに注意することが重要である。

+ 上記の問題に 1 つでも当てはまる場合、PVG はパッチのインストールによるデメリットがメリットを上まわるかどうかを検討する必要がある。修正措置が必要不可欠でない場合は、主たる問題を修正する、より新しいパッチをベンダーがリリースする（よくあることだが）まで待つのが賢明かもしれない。また、パッチの「取り消し」あるいはアンインストールができるかどうかも考慮すべきである。ただし、この機能が提供される場合でも、アンインストールプロセスによってシステムが元の状態に戻るとは限らない。

2.7 脆弱性に対する修正措置の導入

各組織は、ただちに脆弱性が悪用されるリスクがないシステムも含めて、脆弱性のあるすべてのシステムに対して修正措置を導入すべきである [17]。脆弱性に対する修正措置は、組織のホストに対する標準的な構築および設定にも組み込むべきである。影響を受けるシステムに適用できる主な修正措置の手段としては、ソフトウェアパッチのインストール、構成設定の調整、影響を受けるソフトウェアの削除の 3 つがある。

+ **セキュリティパッチのインストール**ーセキュリティパッチ（「フィックス」または「ホットフィックス」ともいう）には、問題を解決することを目的としてソフトウェアアプリケーションを変更するコードが含まれており、セキュリティパッチを適用することによって脆弱性が修正される。ベンダーの Web サイトからダウンロードしたパッチは、通常は最新のものであり、悪意のコードは含まれていないと考えられる。

+ **構成設定の調整**ーアプリケーションやセキュリティ管理の構成方法を調整することにより、攻撃ベクトル [18]を効果的に阻止し、悪用による脅威を軽減することができる。一般的な構成の調整には、サービスの無効化、特権の変更、ファイアウォール規則の変更、ルータのアクセス制御の変更などがある。ファイルの属性やレジストリの設定を調整することにより、脆弱なソフトウェアアプリケーションの設定を変更できる。

+ **ソフトウェアの削除**ー影響を受けるソフトウェアや脆弱なサービスを削除またはアンインストールすることにより、脆弱性および関連する脅威を排除することができる。これは、対象アプリケーションがシステムにとって不要な場合に、実現可能な解決策である。システムの使用方法を決定し、不要なソフトウェアやサービスを削除し、システムにとって必要不可欠なものだけを実行することは、推奨されるセキュリティプラクティスである。

脆弱性と脅威の軽減は、単に構成を変更するだけで済む場合もあれば、まったく新しいバージョンのソフトウェアをインストールするといった複雑な作業を伴う場合がある。すべてのソフトウェアとオペレーティングシステムに対してパッチを簡単に適用する、といった方法はない。修正措置を実施する前に、管理者はパッチを適用するシステムの完全バックアップを実施したほうがよい。それによって、パッチがホストに対して意図しない、あるいは予想外の影響を与えた場合に、システムを以前の状態にタイムリーに復元することができる。

パッチを複数のシステムに適用する作業は管理者にとって絶え間ない試練であり、パッチを数百あるいは数千のサーバやデスクトップシステムに導入する作業は気が遠くなるほど面倒に思えるだろう。このような作業は、エンドユーザのコンピュータに更新を自動配布するアプリケーションを使用することで負担軽減できる。これらのエンタープライズ向けパッチ管理ツールは、ネットワークオペレー

[17] たとえば、システム内の脆弱なサービスが無効にされていれば、そのサービスがただちに悪用されることはないが、そのサービスは過失にせよ故意にせよ有効にされる可能性があり、結果としてシステムが脆弱になる可能性がある。

[18] 攻撃ベクトルとは、セキュリティ上の弱点を突くことによってコンピュータに侵入することのできる経路である。

ティングシステムのソフトウェアに付属されるか、サードパーティのベンダーによって配布されている。その機能は、ツールによってかなり差がある。ツールのなかには、パッチの配布に重点を置き、必要なパッチの特定や、パッチの配信とインストールを行うツールの手配をシステム管理者に依存するものもある。また、必要なパッチを能動的に検索し、入手可能なパッチをシステム管理者に自動的に通知するツールもある。この場合システム管理者は、該当するホストに対して、ツールによるパッチのインストールを承認すればよい。エンタープライズ向けパッチ管理ツールがサポートするオペレーティングシステムやアプリケーションは、ツールによって大きく異なることがある。オペレーティングシステムにバンドルされているツールは、サポートするオペレーティングシステムやアプリケーションの数が少ない傾向がある。サードパーティのベンダーによって配布されるツールは、一般的に広範囲のシステムと互換性がある。自動化されたパッチ配布は、組織のシステム環境が比較的均一で、構成が標準化されている場合に、最も効果を発揮しやすい。エンタープライズ向けパッチ適用ソリューションの詳細については、セクション 4.1 を参照のこと。

各組織で使用しているエンタープライズ向けパッチ管理ツールがサポートしていないオペレーティングシステムやアプリケーションについては、手作業でパッチを適用する必要がある。また、アプライアンス機器の多くは、パッチ管理ツールがサポートするオペレーティングシステムやアプリケーションがその内部で使用されていても、パッチ管理ツールでは更新できない。これは、アプライアンス機器にはカスタマイズされた機能限定版のオペレーティングシステムやアプリケーションが使われることが多く、管理者がアプライアンス機器に直接アクセスすることを想定していないためである。アプライアンス用にカスタマイズされたオペレーティングシステムやアプリケーションも、もともとは標準版のプログラムのコードをベースとしているため、共通の脆弱性による影響を受けやすい。しかし、アプライアンスの場合、製造業者が配布する更新プログラムを使用して、パッチを適用するしかないため、標準機器のように迅速に対応することはできない。多くの組織にとって、アプライアンス機器や、パッチ管理ツールがサポートしていないオペレーティングシステムやアプリケーションに対して手作業でパッチを適用するには、、相当なレベルの労力が必要になる。

自動化されたパッチ適用と手作業による更新のどちらを選択するにしても、推奨される修正措置がもたらすデメリットがメリットを上まわる、とシステム管理者が判断するかもしれない。また、パッチのインストールも構成変更もしないほうがよいと判断するかもしれない。こうした判断の背景にある理由は、文書化し、PVG に伝達し、さらに該当する管理職層にも伝達して承認を得るべきである。

修正措置を遅らせる場合のリスクは、慎重に検討する必要がある。検討事項を以下に示す。

+ **脅威のレベル**ー修正措置を必要とする組織またはシステムが、多くの脅威、重大な脅威、またはその両方に直面しているか？たとえば、外部に公開されている Web サーバやほとんどの連邦政府機関は、高いレベルの脅威に直面している可能性がある。一般に、これらのシステムではタイムリーな修正措置が不可欠である。これに対して、インターネットからアクセスできないイントラネットサイトでは、通常、サイトが直面する脅威のレベルが低いため、しばしば修正措置を遅らせることが可能である。

+ **セキュリティ侵害のリスク**ーセキュリティ侵害が発生する確率はどの程度か？容易に悪用できる脆弱性が存在する場合は、当該脆弱性に対して修正措置をすみやかに適用すべきである。

+ **セキュリティ侵害の結果**ーセキュリティ侵害によってどのような結果が生じるか？システムの重要性が高い場合や、取扱いに注意を要するデータがシステムに含まれる場合は、修正措置をただちに実施すべきである。悪用行為が成功すると、システムのすべての管理権限が、攻撃者の手に渡るおそれがある場合は、たとえ重要でないシステムであっても修正措置をただちに実施すべきである。

修正措置を適用するという判断にも、適用しないという判断にも、残念ながらリスクが伴う。どちらが正しい判断であるかは、常に明確であるとは限らない。PVG、システム管理者、および管理職層は、お互いに協力して、リスクの評価および組織の状況に応じた適切な判断を行うための、体系的なプロセスを作成する必要がある。NIST は、意図しない損害を与えずに IT 機器を保護するために、修正措置のプロセスを既存の構成管理手順に統合することを推奨する。

2.8 管理者への脆弱性および修正措置の情報の配布

PVG がパッチを配布する主な方法は、エンタープライズ向けパッチ管理ソフトウェアを使用することである。ただし、PVG が現場の管理者に直接、修正措置を伝えることが必要な場合もある。脆弱性の優先順位、該当パッチの詳細、構成変更、そのほかの詳細に関する情報を配布するには、メーリングリストが効果的な方法である。しかし、トロイの木馬と化したパッチを含んだ、なりすましの電子メールの出現を抑えるには、PVG は内部の保護された Web サイトから管理者に実際のパッチを配布すべきである（自動化されたパッチ適用ツールを使ってパッチを配布するのが理想である）。パッチやメーリングリスト自体の完全性をサポートするために、追加の管理策（ディジタル署名など）を使用してもよい。異なる種類のシステムを担当する管理者（UNIX 管理者や Windows 管理者など）のために複数のメーリングリストを維持する場合もある。ネットワークや保護された Web サイトが不安定または使用不能な場合は、パッチおよび情報を配布する別の方法（例えばディスクによる配布など）を検討すべきである。

2.9 修正措置の検証

PVGおよびシステム管理者は、脆弱性が意図どおりに修正または軽減されたことを検証すべきである。修正措置が適切に行われたかどうかを確認することで、セキュリティインシデントや意図しないダウンタイムを回避できるという目に見える効果が得られる。この作業は、次のようにいくつかの方法で実行できる [19]。

- 修正措置によって修正されるはずのファイルや構成設定が、ベンダーのマニュアルの記載どおりに変更されていることを確認する。
- 既知の脆弱性を検出できる脆弱性スキャナを使ってホストをスキャンする。
- パッチログを調べて、推奨パッチが適切にインストールされたことを確認する。
- 悪用手順や悪用コードを使って脆弱性の悪用を試みる（ペネトレーションテストを実施する）。

悪用テストは、ネットワーク内部やホスト上で実際に攻撃を行うため、経験豊富な管理者かセキュリティ責任者のみが実施すべきである。一般に、この種のテストは特定の脆弱性のみを対象とし、実運用以外の装置でのみ実施すべきである。テストの実施は、リスクを十分理解している、資格のある担当者のみが行うべきである。

次のセクション以降では、脆弱性スキャナの使用方法、パッチログの確認方法、およびコンピュータを組織のネットワークに接続するときのパッチレベルのチェック方法について詳しく説明する。

2.9.1 脆弱性スキャンの実施

脆弱性スキャナは、多くの組織でホストやネットワーク上の脆弱性を特定するためによく使われている。脆弱性スキャナは、ホストやホスト上で開かれているポートだけでなく、関連する脆弱性も特

[19] 組織は、PVG に十分なリソースがある場合、導入予定の修正措置を、新しいサーバ上で検証させることを検討すべきである。

定する[20]。ホストのオペレーティングシステムとアクティブなアプリケーションを識別し、それらを既知の脆弱性のデータベースと比較する。脆弱性スキャナには次の 2 種類がある。

+ ネットワークスキャナは、組織のネットワークマップを作成し、開かれているポート、脆弱性のあるソフトウェア、および誤った設定のサービスを特定するために使う。ネットワーク上の 1 つのシステムにインストールすればよく、多数のホストをすばやく特定してテストできる。一般にパーソナルファイアウォールを使用しているホストでは、ファイアウォールがネットワークスキャン機能を許可する設定になっていない限り、ネットワークスキャナによる正確な情報収集はできない。

+ ホストスキャナは、テスト対象となるすべてのホストにインストールする必要がある。ホストスキャナは、主に特定のホストオペレーティングシステムおよびホストアプリケーションの設定ミスや脆弱性を特定するために使う。ホストスキャナは検出の粒度が高いため、通常はホストへの（ローカル）権限だけでなく、root または管理者アカウントも必要となる。ホストスキャナのなかには、設定ミスを修正できるものもある。

脆弱性スキャナの機能とパフォーマンスは、製品ごとに大きく異なる。最適検索、および他のシステムに比べてはるかに高速なホスト／ネットワークスキャンが可能なものもある。検出した個々の脆弱性について詳細なレポートと修正措置の情報を提供するものもあれば、検出した脆弱性に関する最も基本的な情報のみを提供するものもある。

脆弱性スキャナは、よく使われるオペレーティングシステムやアプリケーションに関連する脆弱性を特定するために、大規模な脆弱性データベースを利用する。この脆弱性データベースは、スキャナが最新の脆弱性を特定できるように、頻繁に更新する必要がある。一致する情報が見つかると、スキャナは脆弱性の可能性をオペレータに警告する。ほとんどの脆弱性スキャナは、システム管理者が検出された脆弱性を修正するのに役立つレポートも生成する。残念ながら、セクション 3.3.2 で説明するように、脆弱性スキャナは必ずしも正確ではない。一部の脆弱性が発見されない場合や、システムに存在しない脆弱性が特定される場合もある。各組織は、あるスキャナにより生成されたフォールスポジティブ（本当は脆弱性が存在しないのに、「脆弱性がある」と誤検知する場合）の報告を別のスキャナで検証できるように、複数の脆弱性スキャン製品を使用することを検討すべきである。脆弱性スキャナの使用に関する詳しいアドバイスについては、NIST SP 800-42『*ネットワークセキュリティテストにおけるガイドライン（Guidelines on Network Security Testing）*』を参照のこと[21]。

脆弱性スキャナは次の機能を備えている。

+ ネットワーク上のアクティブなホストの特定

+ ホスト上のアクティブで脆弱なサービス（ポート）の特定

+ 検出されたオペレーティングシステムおよびアプリケーションに関連する脆弱性の特定

+ ホストアプリケーションの使用ポリシーおよびセキュリティポリシーが順守されているかどうかのテスト

[20] 脆弱性スキャナを頻繁に実行すると、ネットワーク上の新しいホストおよびそれらの脆弱性を特定するのに役立つ。

[21] NIST SP 800-42 は http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf から入手できる。

脆弱性スキャナを使って、古いバージョンのソフトウェアや適用可能なパッチまたはシステムのアップグレード版を特定することもできる[22]。さらに、設定の誤りや、検出された特定の脆弱性を自動的に修正する機能を備えた脆弱性スキャナもある。

2.9.2 パッチログの確認

ログファイルには、システムの履歴が記録される。パッチログは、PVG やシステム管理者がインストールされたパッチを追跡して検証するのに役立つ。パッチログを使って組織のシステムを監視することで、修正措置実施計画との一貫性や整合性を確保しやすくなる。パッチログを使うと、次のような作業が可能になる。

+ システムにインストールされたパッチを特定することにより、システムに適切なパッチのセットが適用されているかどうかを簡単に確認できる。
+ ログファイルを比較することにより、組織全体で一貫した方法によりパッチが適用されているかどうかを確認する。
+ パッチが適切にインストールされているかどうかを検証する。
+ パッチまたはその後の更新によって以前のパッチが不適切に削除されたり破損したりしていないかを確認する。

2.9.3 パッチレベルのチェック

組織によっては、ホストをネットワークに接続する前に、ホストのパッチレベルを検証したい場合がある。これは、未検証のホストを配置するための、隔離された仮想ローカルエリアネットワーク（VLAN: virtual local area network）を使用することで実現できる。多くの導入環境では、各ホストがさまざまな特性（OS やアプリケーションのパッチ、ウイルス対策ソフトウェアの更新など）を監視するエージェントを実行する。ホストがネットワークに接続しようとすると、ルータなどのネットワーク機器はホストのエージェントから情報を要求する。ホストが要求に応答しない場合や、応答はするものの、ホストへのパッチ適用が完全でないことが判明した場合には、ネットワーク機器はホストを隔離された VLAN に配置する。これにより、各組織はパッチ未適用のホストが実行できる処理を厳しく制限しながら、ホストを更新することができる。VLAN 上のホストにパッチが完全に適用されると、そのホストは VLAN から組織の通常のネットワークに自動的に移動される。VLAN を使った方法は、モバイルホストにパッチを完全に適用したい場合に特に便利である。

2.10 脆弱性に対する修正措置のトレーニング

PVGは組織のソフトウェアインベントリに登録されているソフトウェアの新しいパッチおよび発見された脆弱性を監視するが、現場の管理者がインベントリに含まれていないソフトウェアを使用することもある。PVGにはより一般的に使われているソフトウェアに専念するリソースしかないと管理者層が判断した場合に、このような状況が生じる。このような状況では、現場の管理者が新しいパッチや脆弱性を特定する方法について、ある程度の知識を持っていることが不可欠である。現場の管理者にそのような知識を与えることで、パッチ適用のプロセスに第二の防御線が築かれる。現場の管理者は、セクション 2.3.2 で説明した各種の脆弱性およびパッチ適用のためのリソースについて、PVGからトレーニングを受けるべきである。各組織は、広範囲に使用できることが知られているごく少数のツールを使って、管理者のトレーニングを行うことができる。

---

[22] これを行う場合、一般に、ネットワークベースのスキャナよりもホストベースのスキャナのほうが有効である。スキャナは、古くなったソフトウェアの検索には有効だが、意図的に導入された設定を脆弱性として識別する可能性がある。脆弱性スキャナのレポートを評価する人は、レポートの解釈方法や組織の業務要件と照らし合わせる方法を知っておく必要がある。

さらに、推奨される修正措置を自身の所有するシステムに実施することが期待されるすべてのエンドユーザにも、組織の脆弱性管理プロセスを教育すべきである。これらのエンドユーザは、パッチのインストールやそのほかの修正措置の作業実施に関する指示も受けるべきである。このような教育や指示を作業を最も必要とするのは、遠隔地で作業する職員である（かも知れない）。

2.11 推奨事項

各組織は、組織内部の脆弱性、パッチ、および脅威の特定と対応について、包括的で文書化された説明可能なプロセスを作成する必要がある。考えられる 1 つのアプローチは、現場のシステム管理者のセキュリティ活動をサポートする、正式で中央集権化されたパッチおよび脆弱性グループを作ることである。

パッチおよび脆弱性管理プログラムの実施に関する具体的な推奨事項は、次のとおりである。

1. すべての情報技術資産のインベントリを作成すること。
2. パッチおよび脆弱性グループを作ること。
3. 脆弱性、修正措置、および脅威を継続的に監視すること。
4. パッチ適用の優先順位を決定し、必要に応じて段階的な導入を行うこと。
5. 導入前にパッチをテストすること。
6. エンタープライズ全体を対象とする自動化されたパッチ適用ソリューションを導入すること。
7. 修正措置データベース（多くの場合、エンタープライズ向けパッチ管理ツールに付属する）を作成すること。
8. 必要に応じて自動更新アプリケーションを使用すること。
9. 脆弱性が修正されたことを検証すること。
10. 該当する職員に対して、脆弱性の監視と修正の方法に関するトレーニングを行うこと。

3. パッチおよび脆弱性管理のセキュリティメトリクス

このセクションでは、パッチおよび脆弱性メトリクスプログラムを策定して実施する方法について説明する。すべての組織は、組織のパッチおよび脆弱性管理プログラムの効果を常に測定し、必要に応じて修正措置を適用すべきである。このような機能がない場合、たとえ最適に設計されたセキュリティアーキテクチャであっても、侵入や他の形式の悪用行為を受けやすくなる。

3.1 NIST SP 800-55 を使ったセキュリティメトリクスの実施

NIST SP 800-55『*情報技術システムのためのセキュリティメトリクスガイド(Security Metrics Guide for Information Technology Systems)*』では、セキュリティメトリクスの策定と実施のプロセスを説明している[23]。このプロセスを実施することにより、整備済みのセキュリティの管理策、ポリシー、および手続きが適切かどうかを論証することができる。また、セキュリティ管理策への投資の正当性を判断したり、不十分なセキュリティ管理策に対する是正措置を明らかにするのにも役立つ。SP 800-55 では、セキュリティメトリクスのさまざまな例を示しているが、パッチおよび脆弱性の測定値のメトリクスにまつわる問題については詳しく説明していない。この文書では、SP 800-55 を土台として、パッチおよび脆弱性にかかわる異なる種類の測定値と、それらの測定値の取得に関する問題について説明する。

3.2 メトリクスの策定

このセクションでは、パッチおよび脆弱性メトリクスの策定について、システムごとの特性の測定との関連で説明する。ここでいう「システム」とは、直接の運営と予算管理の体制が共通であり、同じ機能と任務上の目標を持ち、セキュリティのニーズが本質的に同じであり、同一の一般的な運用環境に存在する一連の情報技術(IT)資産、プロセス、アプリケーション、および関連する IT リソースを指す。必ずしも個々のコンピュータを指すとは限らない。このような「システム」という用語の使い方は、NIST SP 800-18 のなかで定義されている。

3.2.1 パッチおよび脆弱性メトリクスの種類

パッチおよび脆弱性メトリクスは、攻撃を受ける可能性の高さ、軽減対処時間、およびコストの 3 つに大きく分類される。このセクションでは、分類ごとのメトリクスの例を示す。

3.2.1.1 システムが攻撃を受ける可能性の高さの測定

組織が攻撃を受ける可能性の高さは、複数の測定値からある程度数値化できる。各組織は、必要なパッチの数、脆弱性の数、および実行されているネットワークサービスの数をシステム単位で測定できる。これらの測定値は、システム内部のコンピュータごとに個別に取得され、その結果は、システム全体の結果を決定する際に総計されるべきである。

加工されていない生データとその割合(たとえば、コンピュータ当たりの脆弱性の数など)の両方が重要である。脆弱性の数、未適用のパッチの数、および公開されているネットワークサービスの数が多いほどシステムが侵入される可能性が高まる。このようなことを考慮すると、上記のような生データを測定することが、システムが直面するリスクの全体を明らかにするのに役立つことがわかる。したがって、多数のコンピュータで構成される大規模なシステムは、同じように構成された小規模なシステムに比べて本質的にセキュリティが低い。このことは、大規模なシステムが小規模なシステムに比べて常にセキュリティが甘いことを意味していない。誤った解釈をさけるためにも、複数のシステムのセキュリティプログラムの効果を比較するときは、割合を使用するべきである。割合(コン

[23] NIST SP 800-55 は http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf からダウンロードできる。

ピュータ当たりの未適用パッチ数など）を使用すると、システム間の比較を効果的に行うことができる。加工されていない生の結果と割合はどちらも有用であり、使用目的がそれぞれ異なるため、システムごとに必要に応じて両方を測定し、公開すべきである。

最初の測定では、攻撃者がシステムのコンピュータの脆弱性に直接アクセスするのを防ぐために必要となる、システムのセキュリティ境界のアーキテクチャ（ファイアウォールなど）については考慮すべきではない。これは、システムが強力なセキュリティ境界によって保護されているかどうかにかかわらず、システム内のすべてのコンピュータのセキュリティを確保することが基本であるからである。これによって、内部の者による攻撃を防いだり、外部から侵入に成功した攻撃者がシステム内のすべてのコンピュータに影響を及ぼすことを防ぐことができる。

ほとんどのシステムでは（さまざまな理由で）セキュリティが完全には確保されないという認識に立ち、システムのセキュリティ境界のアーキテクチャを考慮しながら、測定値を再計算する。これにより、システムが外部の攻撃者から実際に攻撃を受ける可能性について、有意な測定値を得ることができる。たとえば、この 2 番目の測定では、システムが主要なファイアウォールを経由して悪用される可能性がないと判断される場合は、コンピュータの脆弱性の数、ネットワークサービスの数、または必要なパッチの数をを数える必要はない。

システムが攻撃を受ける可能性の高さに関する最初の測定では、システムのセキュリティ境界のアーキテクチャを考慮すべきではないが、個々のコンピュータのセキュリティアーキテクチャについては考慮することが望ましい場合もある。たとえば、ネットワーク接続によって悪用されるおそれがある脆弱性の数は、コンピュータのパーソナルファイアウォールによってそのような悪用行為が防止される場合はカウントしないこともある。コンピュータのセキュリティアーキテクチャの変更によって脆弱性が悪用される可能性があるため、このような措置は慎重に行うべきである。

パッチの数

システムごとに必要なパッチの数の測定は、エンタープライズ向けパッチ管理ツールを導入している組織では、さほど手間をかけずに行うことができる。そのようなデータはパッチ管理ツールによって自動的に得られるためである。必要なパッチの数は、システムが攻撃を受ける可能性の高さを数値化する上で重要ではあるが、特定のセキュリティパッチによって修正される脆弱性は 1 つの場合もあれば複数の場合もあり、脆弱性の深刻度もさまざまである可能性があるため、その効果は限られている。また、対応するパッチが存在しない脆弱性が公開されることも多い。そのような脆弱性により組織のリスクが高まる一方で、必要なパッチの数を測定するだけでは、リスクを把握することができない、といった問題が生じる。この測定値の品質は、パッチを公表したベンダーが「重要」と評価したパッチの数を考慮に入れ、重要なパッチと重要でないパッチの数を比較することで改善される。

脆弱性の数

システムごとに存在する脆弱性の数の測定は、組織が攻撃を受ける可能性の高さを測る尺度としては有効ではあるが、完璧にはほど遠い。脆弱性スキャンツールを採用する組織では、ツールによって必要な統計情報が出力されるため、ほとんどの場合このメトリクスが採用される [24]。パッチの測定と同様に、各組織は脆弱性の深刻度を評価し、測定によって深刻度（または深刻度の範囲）ごとの脆弱性の数が出力されるべきである。各組織は脆弱性の深刻度を評価し、それぞれの深刻度（または深刻度の範囲）に応じて脆弱性の数を測定すべきである。通常、脆弱性データベース（National Vulnerability Database（http://nvd.nist.gov/）など）、脆弱性スキャナ、およびパッチベンダ

[24] セクション 2.9.1 および 3.3.2 で言及するように、脆弱性スキャナは 100 パーセント正確であるわけではない。存在しない脆弱性が報告されたり、存在する脆弱性が報告されないこともある。

一自体によって、脆弱性の評価システムが提供されるが、現在のところ標準化された評価システムは存在しない。これらの評価システム一般的で典型的な組織に対する脆弱性の影響を近似しているだけである。脆弱性の本当の影響は、組織固有のセキュリティインフラストラクチャやアーキテクチャに照らして個々の脆弱性を調べることによってのみ明らかにできる。また、システムに対する脆弱性の影響は、ネットワーク上のシステムの位置によっても異なる（通常、インターネットからアクセスできるシステムでは、脆弱性の深刻さが増す）。

ネットワークサービスの数

攻撃を受ける可能性の高さを示すメトリクスの最後の例は、システムごとに実行されているネットワークサービスの数の測定である[25]。このメトリクスの背景にあるのは、個々のネットワークサービスは潜在的な脆弱性の集合を表しており、システムで実行されるネットワークサービスの数の増加に伴いセキュリティリスクが増大する、という考え方である。大規模なシステムでは、この値を測定するとによって、（現在および将来において）システムがネットワーク攻撃を受ける可能性の高さがわかる。また、複数のシステムを対象に、ネットワークサービスの数を比較することで、ネットワークサービスを効率よく減らして稼動しているシステムを特定することができる。アクティブなネットワークサービスの数が多いからといって、必ずしもシステム管理者の管理が誤っているわけではない。しかし、そのような結果を注意深く調べ、不要なネットワークサービスがすべてオフになっていることを確認すべきである。

3.2.1.2 軽減対処時間

組織がどれだけ迅速に新しい脆弱性を特定・分類し、それに対処し、組織に与える潜在的影響を軽減できるかを測定することも重要である。脆弱性が公表されてから悪用手段が公開されるまでの平均時間はここ数年で劇的に短くなったため、対処時間はますます重要になっている。取得できる主な対処時間の測定値としては、脆弱性およびパッチの特定に要する対処時間、パッチ適用に要する対処時間、および緊急の構成変更に要する対処時間の 3 つがある。

脆弱性およびパッチの特定に要する対処時間

このメトリクスは、PVG が新しい脆弱性またはパッチの情報を知るまでに要する時間を測定する。この時間は、脆弱性またはパッチが公表された時点から始まる。この測定値は、さまざまなパッチと脆弱性をサンプリングして取得すべきである。この測定値には、PVG が情報の収集に使用する各種リソースをすべて含めるべきである。

パッチ適用に要する対処時間

このメトリクスは、システム内の関連するすべての IT 機器にパッチを適用するのに要した時間を測定する。この時間は、PVG がパッチの存在を認識した時点から始まる。この測定値は、PVG が、パッチが正常にインストールされたことを比較的簡単に検証できるパッチについて取得すべきである。この測定には、次の作業に要した個々の時間と合計時間を含めるべきである。

+ PVG によるパッチの分析
+ パッチのテスト

[25] ネットワークサービスやネットワークポートの重要性は、それぞれ異なるため、各組織はネットワークサービスやネットワークポートの数を数えるときに、重み付けすることを検討すべきである。たとえば、1 つのネットワークポートが複数のサービスによって利用されている場合もある。また、あるサービスが、ほかのサービスよりも攻撃される可能性がはるかに高い場合や、より重要な機能を実行している場合もある。

- 構成管理プロセス
- パッチ導入作業

検証は、エンタープライズ向けパッチ管理ツールの使用または脆弱性のスキャン（ホストベースとネットワークベースの両方）によって行うことができる。

重要なセキュリティパッチと重要でないセキュリティパッチでは、通常、組織が使用するプロセスが異なり、タイミングも異なる可能性があるため、必要に応じて両種類のパッチに対して本測定を行うことが有用である。

緊急の構成変更に要する対処時間

このメトリクスは、軽減しなければならない脆弱性がありながらパッチが提供されていないという場合に適用される。このような場合、組織は脆弱性の悪用から組織を保護するために機能を削減するための緊急の構成変更を行わざるを得ない。このような変更は、多くの場合、ファイアウォール、電子メールサーバ、Web サーバ、中央ファイルサーバ、または DMZ 内のサーバで行われる。変更には、特定の電子メール添付ファイル、電子メール件名、ネットワークポート、およびサーバアプリケーションの無効化またはフィルタリングが含まれる場合がある。このメトリクスは、PVG が脆弱性の情報を得た時点から許容できる回避策が適用され、検証される時点までの時間を測定する。多くの脆弱性には緊急の構成変更は必要ないため、このメトリクスはシステムの全脆弱性の一部を対象とする。

通常、これらの作業は緊急時に行われるため、妥当な数の測定サンプルを得ることは難しい。とはいえ作業の重要性を考えれば、これらの緊急プロセスをテストすべきであり、テストケースを通じて対処時間のメトリクスを得ることができる。時間を測定できる緊急プロセスの例を次に示す。

- ファイアウォールまたはルータの構成変更
- ネットワークの切断
- 侵入防止機器の作動または再設定
- 電子メールフィルタリング規則の追加
- コンピュータの隔離
- 職員への緊急通知

システムによっては、テストの対象となる緊急プロセスが大きく異なるため、このメトリクスの結果も大きく異なる可能性がある。各組織は、一貫したテスト結果を得るために、可能な限り標準のシステム緊急事対応プロセスを作成すべきである。各組織は、緊急の構成変更の発生後に必ずメトリクスを取得し、運用報告の一部として評価することにより、緊急変更プロセスにおける次の改善措置や改善領域を明らかにすべきである。

3.2.1.3 コスト

パッチおよび脆弱性管理は、その作業を多数の要員やグループで分担することが多いため、コストの測定が難しい。中央集権化された専任の PVG が、パッチやセキュリティ構成を直接導入するというのが最も簡単なケースである。しかし、ほとんどの組織では、パッチおよび脆弱性にかかわる任務は複数のグループで分担し、作業はフルタイムからパートタイムの職員までさまざまに割り当てられる。コストについて取得すべき主な測定値は 4 つある。1 つ目はパッチおよび脆弱性グルー

プのコスト、2 つ目はシステム管理者またはサポートのコスト、3 つ目はエンタープライズ向けパッチおよび脆弱性管理ツールのコスト、4 つ目はパッチおよび脆弱性管理プログラムの不具合により発生したインシデントに対応するためのコストである。

パッチおよび脆弱性グループのコスト

PVG のメンバーは容易に特定することができ、各人が PVG のサポートに費やす時間の割合は詳細に記録されるため、この測定値はかなり簡単に取得できる。管理職層に対して PVG のコストの正当性を示すときは、PVG に一定の任務を集中させることによって、システム管理者の作業量がどれだけ節減されたかを見積ることが有効である。PVG の重要な部分を外部委託する組織もあるが、そのような外部委託費用もこのメトリクスに含めるべきである。

システム管理者サポートのコスト

この測定値は、通常、正確に取得することが難しいが、重要な測定値である。主な問題は、システム管理者が従来からセキュリティに費やす時間を計算するように求められていない点にある。セキュリティパッチおよび脆弱性管理に費やす時間についてはなおさらである。各組織が IT セキュリティの実際のコストを測定するための、全体的な取り組みを改善するにしたがって、システム管理者によるパッチおよび脆弱性管理のコストの測定も容易になる。

エンタープライズ向けパッチおよび脆弱性管理ツールのコスト

この測定値には、パッチ適用ツール、脆弱性スキャンツール、脆弱性 Web ポータル、脆弱性データベース、および（パッチの検証に使用する）ログ分析ツールを含める。侵入検知ツール、侵入防止ツール、および（侵入検知に使用する）ログ分析ツールは含めない。各組織は、最初に各ソフトウェアパッケージの購入価格と年間保守コストを求める。次に、すべてのソフトウェアの購入価格（各ソフトウェアの購入価格の合計）と年間保守コスト（各ソフトウェアの年間保守コストの合計）含む、年間コストを計算する。このメトリクスを作成するには、各ソフトウェアパッケージの購入価格を推定耐用年数で割ったものに、年間保守コストを加算する。ソフトウェアが定期的にアップグレードされる場合は、購入価格の代わりにアップグレード価格を使用する。

> 概算の年間コスト＝各製品の年間保守の合計＋各製品の（購入価格またはアップグレード価格／推定耐用年数）の合計

たとえば、ある組織に以下のソフトウェアがあるとする。

製品	購入価格	アップグレード価格	推定耐用年数	年間保守
エンタープライズ向けパッチ管理ソフトウェア	$30,000	$15,000	4 年	$3,000
脆弱性スキャナ	$20,000	$10,000	3 年	$2,000

この組織では、脆弱性スキャナは 3 年後にアップグレードする予定だが、エンタープライズ向けパッチ管理ソフトウェアは 4 年後に新しいものに切り替える予定であるとする。概算の年間コストは、（$3,000＋$2,000）＋（$30,000／4）＋（$10,000／3）＝$15,833 である。

プログラムの不具合のコスト

この測定値では、パッチおよび脆弱性軽減プログラムがもっと効果的であれば防止できたはずのすべてのインシデントと、パッチ適用プロセス自体が原因で起きたすべての問題（パッチ適用による

意図しないアプリケーションの破損など）によるビジネスへの影響の総コストを計算する。コストの数値には、有形の損失（作業員の作業時間の損失や破損したデータなど）とともに無形の損失（組織の評判の低下など）も含める。数値は、年間ベースで計算する。この測定の結果は、パッチおよび脆弱性管理プログラムの費用対効果を評価するときに使用する。プログラムの不具合により発生するコストがきわめて高い場合、組織はパッチおよび脆弱性管理プログラムに投入するリソースを増やすことによって、費用を節約できる可能性がある。反対に不具合に伴うコストがきわめて低い場合、組織はパッチおよび脆弱性管理に対するサポートレベルを現状維持するか、あるいは、費用対効果を最適化するためにレベルを下げることも考えられる。

3.2.2 プログラムの成熟度に合わせたメトリクスの導入

システム（または IT セキュリティプログラム）に対して、どのメトリクスに重点を置いてコストを測定するかは、システム（または IT セキュリティプログラム）の脆弱性管理の成熟度に応じて決めるべきである。成熟度の低いプログラムでは、攻撃を受けやすいシステムが存在する可能性があるので、脆弱性の割合などのメトリクスの優先順位を高くすべきである。成熟度の高いプログラムでは、すべての脆弱性が定期的に修正されるため、攻撃を受ける可能性に関するメトリクスはあまり有効ではない。そのようなプログラムでは、新たに発生する脅威や脆弱性への対応時間に関連するメトリクスに重点を置くべきである。成熟度が非常に高いプログラムでは、コストの最適化に重点を置くべきである。プログラムの成熟度にかかわらずすべてのメトリクスが重要であることは確かであるが、ここでの目的はメトリクス導入の優先順位を決定することにある。

NIST SP 800-26『*IT システムのためのセキュリティ自己アセスメントガイド（Security Self-Assessment Guide for Information Technology Systems）*』では、IT セキュリティプログラムのさまざまな側面に関して次のように成熟度を定義している [26]。

- レベル 1－管理目標がセキュリティポリシーに記載されている
- レベル 2－セキュリティ管理策が手続きとして文書化されている
- レベル 3－手続きが実施されている
- レベル 4－手続きとセキュリティ管理策がテストされ、評価されている
- レベル 5－手続きとセキュリティ管理策が包括的なプログラムに全面的に統合されている

図 3-1 に示すように、レベルがあがるほど簡単かつ低コストでメトリクスを計算できるようになる。

[26] NIST SP 800-26 は http://csrc.nist.gov/publications/nistpubs/から入手できる。2005 年 8 月に、『*Guide for Information Security Program Assessments and System Reporting Form*』というタイトルが付けられた更新版の草稿がパブリックコメント用に公開された。

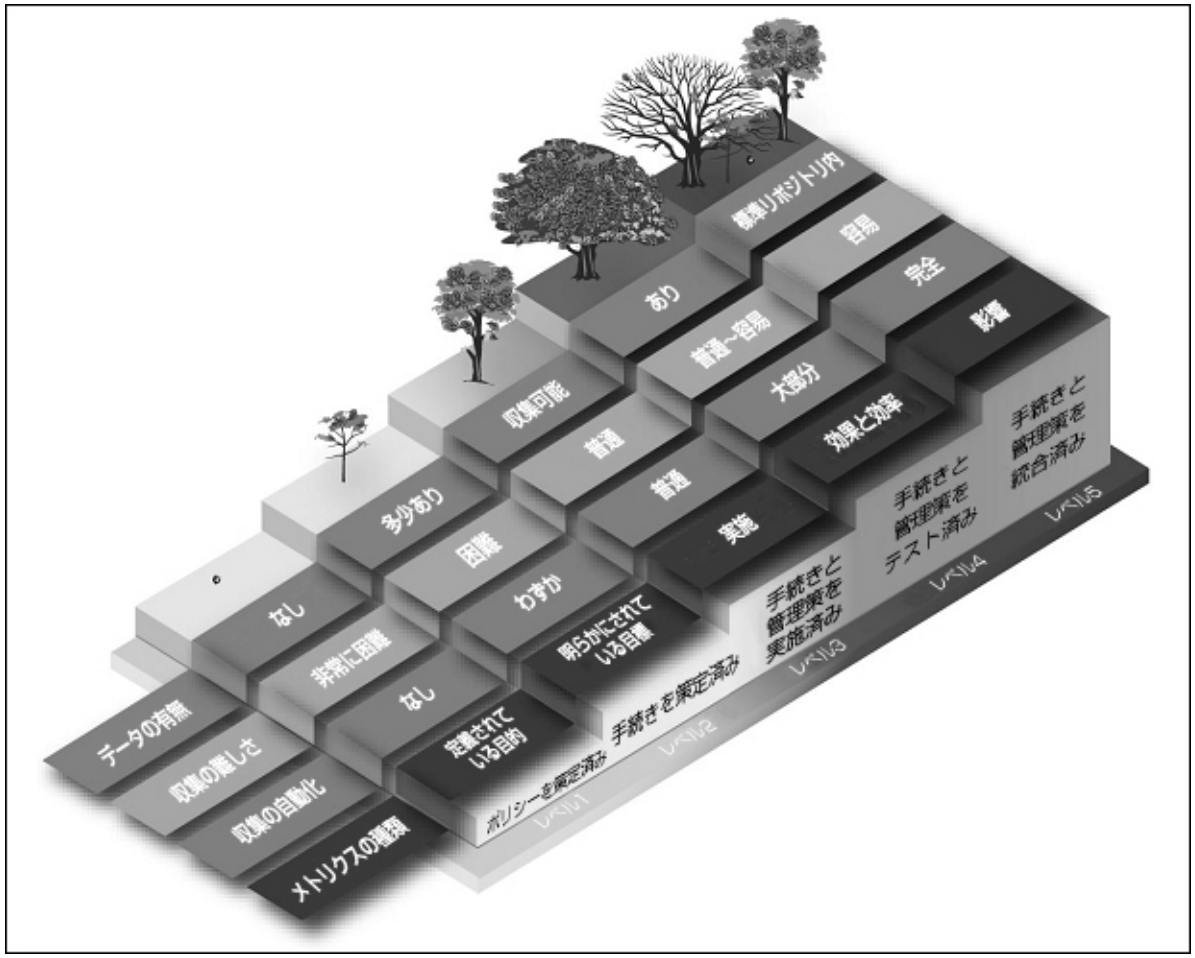

図 3-1. システムメトリクスの成熟度

次のセクションでは、これらの成熟度を使って、ある特定の成熟度を持つシステムおよびプログラムにとってどれが優先順位の高いメトリクスであるかを明らかにする。NIST SP 800-55 のセクション 3.3 では、メトリクスとプログラム成熟度の関係を詳しく説明している。

3.2.3 パッチおよび脆弱性メトリクスの表

次の表は、パッチおよび脆弱性メトリクスについてまとめたものである。これらのメトリクスは、コストに関連するメトリクスを除いてシステム単位で取得すべきである。パッチおよび脆弱性管理が組織レベルで行われている場合は、組織単位でメトリクスを取得してもよい。

表 3-1. パッチおよび脆弱性メトリクス

メトリクス名	単位	対象となる 800-26 成熟度
脆弱性の割合	脆弱性／ホスト	3
未適用のパッチの割合	パッチ／ホスト	3
ネットワークサービスの割合	ネットワークサービス／ホスト	3
脆弱性およびパッチの特定の対処時間	時間	4
パッチの対処時間（重要なパッチ）	時間	4

メトリクス名	単位	対象となる 800-26 成熟度
パッチの対処時間（重要でないパッチ）	時間	4
緊急構成変更に要する対処時間	時間	4
PVG のコスト	金額	5
システム管理サポートのコスト	金額	5
ソフトウェアのコスト	金額	5
プログラムの不具合により発生するコスト	金額	5

3.2.4 メトリクスの文書化と標準化

各組織は、各システムで測定するメトリクスの種類と各メトリクスの詳細を文書化すべきである。NIST SP 800-55 には、セキュリティメトリクスの詳細を指定するための標準的なテンプレートが用意されている。

3.2.5 パフォーマンス目標と費用対効果

システムの所有者およびシステムのセキュリティ責任者には、各メトリクスの現実的な履行目標を伝える必要がある。これらの目標を達成できたら、さらに意欲的な目標を設定することもできる。パッチおよび脆弱性のセキュリティレベルを上げる場合は、システムのセキュリティ責任者やシステム管理者が悲鳴をあげることがないように慎重に行うことが重要である。

プログラムの費用対効果は、プログラムの実行に関連するコストメトリクスと、プログラムの不具合によるコストとを比較することによって計算できる。また、プログラムの実行に関連するコストメトリクスと、プログラムのパフォーマンスを示すメトリクス（応答時間や攻撃を受ける可能性の高さに関するメトリクス）とを比較することによっても計算できる。

3.3 メトリクスプログラムの実施

NIST SP 800-55 では、メトリクスプログラムの実施方法を説明している。このセクションでは、その説明の補足として、パッチおよび脆弱性メトリクスの実施に関する特定の問題についての情報を提供する。

3.3.1 白紙の状態からの開始

多くの組織は、脆弱性スキャンツール（ホストベースとネットワークベースの両方）を使って、システムごとの脆弱性の数を測定することにより、メトリクスプログラムを開始する。初期段階では多くの組織が、スキャンツール内のすべての脆弱性シグネチャを有効にしてから、各システムをスキャンする。その結果、各システム内のすべてのコンピュータを完全に保護するための作業レベルを測定することができる。しかし、脆弱性スキャンの出力はシステム当たり数百（または千）ページにおよぶ可能性があり、システムセキュリティ責任者はそのような大きな課題を抱えて落胆するかもしれない。結果として作業がほとんど進まない可能性がある。

この問題の解決策は、スキャンの範囲を絞り込むことである。それには、脆弱性シグネチャに優先順位を付け、優先順位の最も高いシグネチャだけを使ってスキャンを行う。システムセキュリティ責任者は、より扱いやすい課題に重点を置き、最も深刻な脆弱性の軽減に力を注ぐことができる。一定期間をおいてスキャンに使われる脆弱性シグネチャのリストを増やすことにより、システムセキュ

リティ責任者や管理者が対処できるレベルの作業を常に提示し、最終的にはより高いレベルのセキュリティを確保すことができる。

3.3.2 フォールスポジティブとフォールスネガティブ

パッチおよび脆弱性メトリクスプログラムはすべて、フォールスポジティブとフォールスネガティブにある程度まで対応する必要がある。フォールスポジティブとは、脆弱性などが実際には存在しないのに、測定値に含まれてしまう場合を指す。フォールスネガティブとは、脆弱性などが確かに存在するのに、測定値に含まれない場合を指す。従来、この領域の問題はエンタープライズ向けパッチ管理ツールではほとんど発生せず、ホストベースの脆弱性スキャナではある程度発生し、ネットワークベースの脆弱性スキャナでは最も多く発生していた [27]。しかしながら、たとえエンタープライズ向けパッチ管理ツールが問題なく機能している場合であってもフォールスポジティブが発生する可能性がある。たとえば、あるパッチを特定のサーバに適用できない場合は、（サーバを別のメカニズムによって保護すべきだが）そのパッチの欠落を測定値に含めるべきでない。PVGは、既知のフォールスポジティブおよびフォールスネガティブを追跡し、測定プロセスからそのような問題を取り除く必要がある。

脆弱性スキャナには、多くの場合、情報提供を目的とするシグネチャが含まれている。これらのシグネチャに関する「警告」は、実際の脆弱性には該当しない。これらの情報提供用シグネチャは、脆弱性スキャンプログラムにおけるフォールスポジティブの大きな要因となりうる。

3.4 推奨事項

すべての組織は、組織のパッチおよび脆弱性管理プログラムの効果を常に測定し、必要に応じて是正措置を適用すべきである。これは、パッチおよび脆弱性メトリクスプログラムを策定することによって実現できる。導入するメトリクスは、特定のメトリクスが特定の成熟度を有するパッチおよび脆弱性管理において最も有用であることを踏まえて、成熟度に適したものを選ぶべきである。導入するメトリクスは、特定のメトリクスが特定の成熟度を有するパッチおよび脆弱性管理おいて最も有用であることを踏まえて、成熟度に適したものを選ぶべきである。各組織は、各システムで測定するメトリクスの種類と各メトリクスの詳細を文書化すべきである。システムの所有者およびシステムのセキュリティ責任者には、メトリクスの現実的な履行目標を伝える必要がある。

[27] エンタープライズ向けパッチ適用ツールは、パッチの欠落を検索するだけなので、エラーが発生する確率は低い。ホストベースのスキャナは、より複雑な構成情報や脆弱性を調べるため、多くの場合、エラーが発生する可能性が高くなる。ネットワークベースのスキャナは、スキャン対象のコンピュータに関する情報の一部にしかアクセスできないため、多く場合、最もエラーが発生しやすい。

4. パッチおよび脆弱性管理の問題

4.1 エンタープライズ向けパッチ適用ソリューション

すべての中～大規模組織は、所有する大部分のコンピュータに対してエンタープライズ向けパッチ管理ツールを使用すべきである。たとえ小規模な組織であっても、何らかの自動化されたパッチ適用ツールに移行すべきである。広範囲のコンピュータに手作業でパッチを適用する方法は、インストールする必要があるパッチの数が増え、また攻撃者による脆弱性実証の開発期間が短くなるにつれて、有効でなくなりつつある。独自に構成されたコンピュータや、自動化された方法では更新がうまくできないそのほかのコンピュータ（アプライアンス機器など）には、引き続き手作業でパッチを適用すべきである。

4.1.1 パッチ適用ソリューションの種類

エンタープライズ向けパッチ管理ツールは、大きく 2 つに分類される。1 つはエージェントを使用するツールであり、もう 1 つはエージェントを使用しないツールである。両方のアプローチをサポートし、対象環境において最も効率的なアプローチを管理者が選択できる製品もある。どちらのアプローチの場合も、通常は、中央にコンピュータが存在し、パッチ適用ソリューションにエントリーされたコンピュータへのインストールが可能または必要であるパッチが、すべてそこに置かれている。中央コンピュータは、パッチを適用する管理者が、どのパッチをどのコンピュータに適用するかを管理できるコンソールを備えていることが多い。複数の中央コンピュータを使って冗長性を提供し、パッチ適用の負荷を複数の機器やネットワークに分散する実装もある。

どちらのアプローチでも、中央集権化されたモデルを利用しており、1 台のコンピュータ（または 1 つのコンピュータクラスタ）でパッチ適用ソリューションに参加しているすべてのコンピュータのパッチ適用プロセスを管理している。これは、標準的な Microsoft Windows Update サービスとは対照的である。Microsoft Windows Update サービスでは、完全に分散化されたモデルを使用し、各コンピュータ（または各コンピュータの管理者）がインストールするパッチとインストールのタイミングを決定している。中央集権化モデルと分散化モデルが一体化された機能を持つ製品もある。このようなソリューションは、通常は中央集権化モデルに従うが、特定のパッチをインストールしないことを選択できるようにするなど、エンドユーザにプロセスの制御権を付与している。

エンタープライズ向けパッチ管理ツールの主な 2 つの分類には共通点もあるが、特定のソリューションを購入する際に考慮すべき重要な相違点もある。

非エージェント型パッチ適用ソリューション

非エージェント型パッチ適用ソリューションは、ネットワークベースの脆弱性スキャナに類似している。通常は、ネットワーク経由でコンピュータをスキャンするコンピュータが 1 台存在する。しかし、多くの脆弱性スキャナとは異なり、非エージェント型パッチ適用ソリューションには、通常、自動化されたパッチ適用プログラムに参加しているコンピュータへの管理者権限が与えられる。このため、パッチ適用プログラムでは、単純なネットワークスキャンよりもはるかに多くの情報にアクセスできる。また、参加コンピュータにパッチをインストールすることもできる。非エージェント型パッチ適用ソリューションと脆弱性スキャナとの類似性を考えれば、商用の非エージェント型パッチ適用ソリューションが脆弱性を発見でき、しかも、なかには、コンピュータへの管理者権限によるアクセスを許可されない脆弱性スキャンプログラムよりも高い精度で脆弱性を検出できるものがあることは驚くには値しない。

非エージェント型パッチ適用ソリューションは、ネットワークスキャンを利用するため、ネットワーク帯域幅の大部分を専有する可能性がある。ほとんどの製品では、製品によって専有されるネットワーク帯域幅の割合をパッチの管理者が調整できるようにすることで、この問題を解決している。しかし、

製品が使用できるネットワーク帯域幅が制限されると、ネットワークスキャン完了までの合計所要時間が増える可能性がある。大規模なネットワークでは、求められる速さですべてのコンピュータをスキャンできない可能性があるため、エージェント型ソリューションのほうが望ましいこともある。また、在宅勤務をする職員のコンピュータはスキャンに含まれない可能性がある。非エージェント型パッチ適用ソリューションのもう 1 つの問題は、コンピュータのパーソナルファイアウォールが、スキャン処理を許可するように設定されていない限り、通常はスキャン処理をブロックすることである。パーソナルファイアウォールの普及率が上昇しているため、この問題はますます深刻化している。

エージェント型パッチ適用ソリューション

エージェント型パッチ適用ソリューションでは、前に述べたように、通常、中央集権化されたコンピュータ（またはコンピュータクラスタ）を使用して、すべての参加コンピュータのパッチ適用プロセスを管理する。ただし、このモデルでは個々の参加コンピュータにソフトウェアプログラム（エージェント）をインストールする必要がある [28]。エージェント型パッチ適用プロセスは、製品によって異なるが、全体的なプロセスは次のとおりである。

1. エージェントは中央コンピュータと通信して新しいパッチの情報を得る。通信手段は、実装形式によって異なるが、エージェントが中央コンピュータを定期的にポーリングする、または、中央コンピュータがエージェントに直接接続するなどがある。（後者のほうが効率的）。

2. エージェントは、コンピュータの管理者権限または root 権限を持っており、その権限を用いて、コンピュータに欠落しているパッチを特定する。結果は通常中央コンピュータに送信され、全体的なパッチ適用の管理者（PVG の代表者など）がすべての参加コンピュータの状況を確認できるようになっている。また、これによって中央管理者は、各システムのパッチセキュリティレベルに関するパッチ適用レポートを作成することもできる。

3. エージェントは、インストールすべきパッチとそのインストール方法に関する指示を中央コンピュータから受信する。再起動が必要な場合、中央コンピュータはパッチを適用してからコンピュータを自動的に再起動するようにエージェントに指示する。また、中央コンピュータは、パッチの適用後、コンピュータの再起動が必要なことを（指定された時間内に自動的に再起動するオプションとともに）ユーザに通知するようにエージェントに指示することもある。

エージェント型ソリューションのアーキテクチャでは、非エージェント型ソリューションのようにネットワーク帯域幅が過度に消費されることはない。最大の欠点は、エージェントを各コンピュータにインストールし、管理者権限または root 権限で実行する必要があることである。2 つ目の欠点は、すでに高い負荷がかかっている（CPU やメモリの負荷が高い状態で動作する）コンピュータでは、エージェントのプロセスによってさらにパフォーマンスが低下するおそれがあることである。考えられるもう 1 つの欠点は、プラットフォームによってはエージェントを利用できない場合があることだが、これは、非エージェント型アプローチでも起きうる問題である。

各アプローチの長所と短所

2 つのアプローチには、それぞれ考慮すべき長所と短所がある。

<u>非エージェント型ソリューションの長所</u>:

+ すべての参加コンピュータにソフトウェアエージェントをインストールする必要がない。

[28] セクション 2.7 で説明したように、アプライアンス機器の多くは、管理者がオペレーティングシステムに直接アクセスすることを許可しないため、通常はパッチ適用エージェントをインストールできない。

非エージェント型ソリューションの短所:

+ コンピュータのスキャン中にネットワーク帯域幅の大部分が専有される [29]。
+ 本来システムへの侵入口を閉鎖する一環として無効にするべきポートやサービス(UNIX のリモートプロシージャコール(RPC)や Windows の NetBIOS など)を、使用することが必要な場合がある。
+ 大規模なネットワークのスキャンには長い時間を要する場合がある。
+ パーソナルファイアウォールを使用するホストについては、正確な結果が得られない場合がある。
+ 参加コンピュータへの管理者権限によるアクセスを中央コンピュータに許可することが必要な場合がある [30]。

エージェント型ソリューションの長所:

+ 大規模なネットワークを迅速にスキャンできる。
+ コンピュータをスキャンしている間のネットワーク帯域幅の消費が最小限で済む。

エージェント型ソリューションの短所:

+ すべての参加コンピュータにおいて、ソフトウェアエージェントがインストール、実行、および管理される必要がある。障害や設定ミスによってエージェントが動作していない場合、当該コンピュータにパッチが適用されない。
+ エージェントを管理者または root 権限で実行する必要がある。その結果、エージェントへのリモート攻撃によって攻撃者が管理権限を取得する可能性が生じる。

4.1.2 セキュリティリスク

組織内にエンタープライズ向けパッチ管理ツールを導入すると、組織にとってのセキュリティリスクが新たに生まれる可能性がある [31]。それにもかかわらず、このようなツールは、特にセキュリティリスクや脅威からシステムを保護するためのセキュリティ対策機能がツールに組み込まれている場合、セキュリティの向上がセキュリティの低下をはるかに上回るのが通常である。これらのツールを使った場合のリスクの例を次に示す。

+ ソフトウェアベンダーが、悪意のコードによって改変されたパッチをエンタープライズ向けパッチ管理ベンダーに配布する可能性がある。
+ エンタープライズ向けパッチ管理ベンダーが、悪意のある従業員または攻撃者によって改変されたパッチを提供する可能性がある。
+ 攻撃者が、中央パッチコンピュータに侵入し、エンタープライズ向けパッチ管理ツールを利用して(すべての参加コンピュータへのリモートアクセス権限を取得し)、悪意のコードを効率的に配布することもできる。

---

29 パッチをコンピュータに配信する際の帯域幅は、非エージェント型とエージェント型どちらのソリューションでもほぼ同じと考えられる。

30 中央コンピュータが個々のホストにログオンするのに必要な資格情報を管理することは、個人アカウントの数が多い場合(特に、パスワードが頻繁に(たとえば、月ごとに)変更される場合)はかなり困難である可能性がある。

31 システムにパッチを効果的に適用していない組織は、はるかに大きなリスクに直面する。

- 攻撃者が、非エージェント型システムの中央パッチコンピュータに侵入して、パッチ管理プログラムに参加するすべてのコンピュータの管理者パスワードを盗む可能性がある。
- 攻撃者が、パッチ管理エージェントソフトウェアを使い、ローカルで悪用できる脆弱性を検出する可能性がある。これにより、攻撃者は参加コンピュータに対する権限をユーザレベル権限から管理者権限に昇格することが可能になる。これは、攻撃者がすでにコンピュータに侵入し、権限を獲得していることが前提になる。
- 攻撃者が、パッチ管理エージェントソフトウェアを使い、リモートから悪用できる脆弱性を検出する可能性がある。これにより、攻撃者は参加コンピュータにリモートから侵入し、管理者権限を得ることが可能になる。また、攻撃者は参加コンピュータに対してサービス不能（DoS）攻撃を開始することも可能になる。
- 攻撃者が、エンタープライズ向けパッチ管理ツールのネットワーク通信を傍受し、どのコンピュータにどのパッチがインストールされていないかを特定する可能性がある。

これらのリスクは、エンタープライズレベルのアプリケーションの導入時に使用すべき標準的なセキュリティ手法を適用することによって、部分的に軽減できる。以下に、対策の例を示す。

- ネットワーク接続の暗号化
- ネットワーク通信に対する IP アドレス認証の実施
- 中央パッチ管理サーバ上の不要なポートおよびサービスの無効化
- 導入前のパッチのテスト
- パッチのタイムリーな適用
- パッチが存在しない脆弱性のタイムリーな軽減
- ファイアウォールの適切な使用

4.1.3 組み込みのソフトウェアインベントリ機能

エンタープライズ向けパッチ管理ツールは、個々の参加コンピュータへの管理者権限が必要であり、必要なパッチを特定するために、各コンピュータ上のソフトウェアパッケージのインベントリを作成する必要がある。したがって、このようなプログラムにとって、ソフトウェアインベントリー情報を管理者が入手できるようにし、ソフトウェアインベントリ管理機能を製品に組み込むことは理にかなっている。この機能を備えた製品はますます増えており、これは市場の自然な流れのようである。このようなインベントリ製品は単独でも購入できるが、多くの場合、各コンピュータに別のエージェントをインストールする必要がある。IT管理の観点から見ると、各コンピュータに複数のエージェントをインストールして管理するのはコストがかかるため、同じ製品で両方の機能（パッチ適用とインベントリ作成）を実施できれば理想的である [32]。

4.1.4 組み込みの脆弱性スキャン機能

エンタープライズ向けパッチ管理ツールには、脆弱性スキャン機能も組み込まれ始めている。これにより、管理者はどのパッチが欠落しているかを確認できるだけでなく、それらのパッチにどの脆弱性が関連しているかを理解でき、さらにパッチ未適用のコンピュータに対して実際にどのようなリス

[32] パッチ管理システムのなかには、既知の脆弱性を持つソフトウェアまたはソフトウェアのバージョンのみを認識するものがある。そのようなパッチ管理システムを組織のソフトウェアインベントリ情報の唯一のソースとして使用することはできない。

クが存在するのかを把握できる。この機能により、管理者はパッチが入手可能になる前にコンピュータ内の脆弱性を確認することもできる。新しい脆弱性が公表されるたびに現れる攻撃ツールの開発速度を考えると、これはとても重要である。

これらのツールのなかには、ネットワークベースの脆弱性スキャナよりも正確に脆弱性をスキャンできるものもある。ネットワークベースの脆弱性スキャナの多くは、スキャン対象コンピュータに対する管理者権限を持っていないため、脆弱性の識別は、個々のネットワークポートへのさまざまな入力値に対する応答に基づく、不正確な推測に頼らざるを得ない。エンタープライズ向けパッチ管理ツールには、この点でホストベースの脆弱性スキャナを上回る長所はない。しかし、インベントリ管理ツールと同様に、各コンピュータで 2 つの異なるエージェントをインストールして管理するよりは、1 つのエージェントにパッチ管理機能と脆弱性スキャン機能を統合するほうがよいだろう。

4.1.5 導入戦略

すべての中～大規模組織はエンタープライズ向けパッチ管理ツールを使用すべきだが、これらのツールを組織内に全面的に導入することが困難な場合がある。各組織は、段階的な方法でエンタープライズ向けパッチ管理ツールを導入することが推奨される。これにより、パッチ適用の全面的な導入に先立ち、小さなグループを使ってプロセスの問題やユーザとのコミュニケーションに関する問題を解決できる。

多くの組織では、パッチ管理ツールを導入する際に、まずは標準化されたデスクトップシステム、および同様の構成を持つサーバ群により構成される単一プラットフォームのサーバファームを対象とする。これが完了すると、次に組織は、マルチプラットフォーム環境、標準でないデスクトップシステム、レガシーコンピュータ、および例外的な構成のコンピュータを統合するという、より難しい問題に取り組む必要がある。自動化されたパッチ適用ツールが適用できないオペレーティングシステムやアプリケーションのほか、例外的な構成のコンピュータに対しては、手作業による方法が必要となる場合がある。そのような例としては、組み込みシステム、産業用制御システム、医療機器、実験システムなどがある。このようなコンピュータについては、手作業のパッチ適用プロセスに関する明文化された実践済みの手順が必要である。

標準でないシステムやレガシーコンピュータは広範囲の導入の妨げになる可能性があるが、要員に関する問題のほうがより大きな課題になることもある。システム所有者（およびコンピュータユーザ）は、自分たちのコンピュータへの管理者権限をほかのグループに与えたり、そのグループが自分たちのコンピュータに対して定期的にソフトウェアのインストールや更新を行ったりすることについて、懸念を覚えるかもしれない。懸念事項には、次のようなものが含まれる。

- エージェントソフトウェアによってコンピュータのパフォーマンスや安定性が低下する可能性がある。
- インストールされたパッチによって既存のソフトウェアに予期しない問題が発生する可能性がある。
- エンタープライズ向けパッチ適用アプリケーションがパッチをインストールするためにコンピュータを再起動したときに、ユーザがデータを失う可能性がある。
- エンタープライズ向けパッチ適用アプリケーション自体が新しいセキュリティリスクを生む可能性がある。
- モバイルユーザがネットワークに接続した途端にエンタープライズ向けパッチ適用アプリケーションが大量のパッチをインストールしようとすることで、モバイルユーザのいらだちや混乱を招くおそれがある。

これらの懸念について、システム所有者やコンピュータユーザと話し合うべきである。これらの不安はすべて、良好なコミュニケーション、慎重な段階的導入、および堅牢で安全なエンタープライズ向けパッチ管理ツールの選択によって解消できる。

4.2 適切な購入によるパッチ適用の必要性の低減

ソフトウェア製品のなかには、同じ目的と機能を持つほかの製品よりも多くの脆弱性を抱えるものがある。購入プロセスにおいていくつかの要素を考慮することにより、各組織は将来発生する脆弱性の数を減らし、それによってソフトウェアにパッチを適用する必要性も減らすことができる。脆弱性が将来発生する可能性は、製品購入時に考慮すべき要素のすべてではないが、意思決定プロセスの要素の 1 つにすべきである。もう 1 つの要素は、ベンダーが新しい脆弱性に対するパッチを出す速度である。将来脆弱性が発生する可能性が低い製品を選択するための手法を次のリストに示す。

- 製品のセキュリティを確保するための方法を規定した詳細なチェックリストがある製品を検討する。NISTでは、「Security Configuration Checklists Program for IT Products（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）」を運営し、さまざまなオペレーティングシステムやアプリケーションの評価済みのチェックリストを収集している。NIST SP 800-70 は、このプログラムに関する説明であり、詳しい内容は本プログラムのWebサイト（http://checklists.nist.gov/）から入手できる。

- 脆弱性データベース（National Vulnerability Database（http://nvd.nist.gov/）など）を検索して、検討している製品の既知の脆弱性を確認する。検討している製品に含まれる脆弱性の種類、深刻度、および数を調べる。あまり知られていないソフトウェア製品の場合は、脆弱性の検出（およびパッチのリリース）に時間を要することが多いため、この方法は万全とはいえない。

- 成熟度の高い製品を検討する。リリースしてから日の浅い製品には、通常、より多くの未知の脆弱性が存在する。このような製品は将来パッチが必要となり、リスクにさらされる可能性が高い。

- より単純な製品を検討する。コード、機能、およびサービスが増えるほど、バグ、脆弱性、およびパッチも増えるおそれがある。必要以上の機能が盛り込まれた製品の購入を避けることを検討する。リリースしてから日の浅い主要なオペレーティングシステムまたはアプリケーションの導入は、他の利用者の経験を意思決定プロセスに取り込むことができるまで、可能な限り遅らせる。

- 適切な国家または国際セキュリティ設計基準（暗号化モジュールの場合はFIPS 140-2 など）に準拠する製品を購入する。詳細については、NIST SP 800-23『*Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*』を参照のこと [33]。

- 第三者のテストによって検証されたソフトウェアを検討する。最大の保証を得るには、ソフトウェアのソースコードを評価すべきである [34]。

- 現在サポートされているソフトウェアのバージョンのみを使用する。ライフサイクルを終えた古いソフトウェアには、サポートされている新しいバージョンでのみ解決されている欠陥が含まれることが多い。

---

[33] NIST SP 800-23 は http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf からダウンロードできる。

[34] ソフトウェアソースコードの評価は、メリットがあるにもかかわらず、そのような分析にはコストがかかるため、一般には行われていない。

4.3 標準化された構成の使用

IT リソースに対して標準化された構成を使用すると、パッチの特定、テスト、および適用にかかる労力が軽減され、セキュリティの向上につながる高いレベルの一貫性が確保される。IT リソースに標準の構成を使用する組織では、パッチおよび脆弱性管理プログラムの実施がきわめて簡単かつ低コストで可能になる。大規模な組織で構成を標準化していない場合、包括的なパッチおよび脆弱性管理はほぼ不可能である（少なくとも、非常にコストが高い）。

標準の構成は、IT リソースの主なグループ（ルータ、ユーザワークステーション、ファイルサーバなど）ごとに定義すべきである。各組織は、IT リソース全体のなかで大きな部分を占める種類の IT リソースを標準化することに努力を傾けるべきである。予想される標準化の対象には、エンドユーザのワークステーション、ファイルサーバ、およびネットワークインフラストラクチャの構成要素（ルータやスイッチなど）がある。標準の構成には、次の項目が含まれることが予想される。

- ハードウェアの種類とモデル
- オペレーティングシステムのバージョンとパッチレベル
- インストールされている主なアプリケーション（バージョンとパッチレベル）
- オペレーティングシステムおよびアプリケーションのセキュリティ設定

多くの場合、これらの標準化された構成は集中管理され、構成の変更は参加するすべてのITリソースに反映することができる。新しいコンピュータに標準の設定を反映する作業をハードウェア供給業者に頼る組織は、その業者と緊密に連携して、新しいパッチを含む変更が迅速に導入されるようにすべきである。NIST Special Publication 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）*』では、標準のセキュリティ設定を文書化するための有効なツールとなるセキュリティ設定チェックリストの作成と使用に関するガイダンスを提供している [35]。

4.4 セキュリティ侵害後のパッチ適用

セキュリティ侵害後のパッチ適用は、単に適切なパッチを適用する場合に比べてかなり複雑である。セキュリティ侵害後のパッチ適用によって、悪用された脆弱性は一般に修正されるが、それ以外に侵入者によって加えられた可能性のある変更（ルートキットやバックドア [36]など）は、ほとんど解消されない。たとえば、Code Red IIワームの場合には、感染したシステムにバックドアを仕掛け、その後、Nimdaワームがそれらのバックドアを悪用した。感染したシステムは、ほとんどの場合、再フォーマットおよび再インストールを行うか、安全で信頼できる既知のバックアップから復元すべきである [37]。それができない場合は、感染したシステムに内在する潜在的な危険を管理するためにきわめて高度な専門知識が要求される。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）*』は、セキュリティインシデントへの対応と感染したシステムの復旧に関する詳細なリソースである [38]。

---

35 NIST SP 800-70 は、セキュリティ設定チェックリストの Web サイト（http://checklists.nist.gov/）から入手できる。

36 バックドアとは、攻撃によってセキュリティが侵害されたコンピュータシステムに仕掛けられた、その後の不正アクセスを可能にする秘密の裏口である。

37 各組織で標準の構成にすべてのパッチが適用されたイメージを保持しておくと、役に立つことがある。最新の既知の適切なイメージを侵害されたシステムに入れたあと、データをバックアップからシステムに復元することができる。

38 NIST SP 800-61 は http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf から入手できる。

4.5 推奨事項

NIST は、中～大規模組織に対して、所有する大部分のコンピュータに対してエンタープライズ向けパッチ管理ツールを使用することを推奨する。たとえ小規模な組織であっても、何らかの自動化されたパッチ適用ツールに移行すべきである。独自に構成されたコンピュータや、自動化された方法では更新がうまくできないそのほかのコンピュータ（アプライアンス機器など）には、引き続き手作業でパッチを適用すべきである。

エンタープライズ向けパッチ管理ツールを導入すると、組織にとってのセキュリティリスクが新たに生まれる可能性がある。たとえば、攻撃者がパッチ管理の中心となっているコンピュータに侵入し、エンタープライズ向けパッチ管理ツールを悪意のコードを効率的に配布するツールとして利用する可能性がある。各組織は、エンタープライズレベルのアプリケーションの導入時に使用すべき標準的なセキュリティ手法によって、これらのリスクの一部を軽減する必要がある。

各組織は、段階的な方法でエンタープライズ向けパッチ管理ツールを導入すべきである。これにより、パッチ適用の全面的な導入に先立ち、小さなグループを使ってプロセスの問題やユーザとのコミュニケーションに関する問題を解決できる。ほとんどの組織では、パッチ管理ツールを導入する際に、まずは標準化されたデスクトップシステム、および同様の構成を持つサーバ群により構成される単一プラットフォームのサーバファームを対象とする。これが完了すると、次に組織は、マルチプラットフォーム環境、標準でないデスクトップシステム、レガシーコンピュータ、および例外的な構成のコンピュータを統合するという、より難しい問題に取り組む必要がある。自動化されたパッチ適用ツールが適用できないオペレーティングシステムやアプリケーションのほか、例外的な構成のコンピュータに対しては、手作業による方法が必要となる場合がある。そのような例としては、組み込みシステム、産業用制御システム、医療機器、実験システムなどがある。このようなコンピュータについては、手作業のパッチ適用プロセスに関する明文化された実践済みの手順が必要である。システム所有者やコンピュータユーザは、自分たちのコンピュータへの管理者権限をほかのグループに与えたり、そのグループが定期的にソフトウェアのインストールや更新を行ったりすることについて懸念を覚えるかもしれない。そのような懸念は、良好なコミュニケーション、慎重な段階的導入、および堅牢で安全なエンタープライズ向けパッチ管理ツールの選択によって解消すべきである。

ソフトウェア製品のなかには、同じ目的と機能を持つほかの製品よりも多くの脆弱性を抱えるものがある。購入プロセスにおいていくつかの要素を考慮することにより、各組織は将来発生する脆弱性の数を減らし、それによってソフトウェアにパッチを適用する必要性も減らすことができる。脆弱性が将来発生する可能性は、意思決定プロセスの要素の 1 つにすべきである。もう 1 つの要素は、ベンダーが新しい脆弱性に対するパッチを出す速度である。

各組織がパッチおよび脆弱性管理に関する労力を軽減できるもう 1 つの方法は、IT リソースに標準化された構成を使用することである。構成が標準化されている組織では、パッチおよび脆弱性管理プログラムの実施がきわめて容易かつ低コストで可能になる。構成を標準化していない大規模な組織においては、包括的なパッチおよび脆弱性管理はほぼ不可能である。各組織は、IT リソース全体のなかで大きな部分を占める種類の IT リソースを標準化することに努力を傾けるべきである。

5. 米国政府のパッチおよび脆弱性関連のリソース

ここ数年、米国政府のパッチおよび脆弱性管理製品のほとんどは国土安全保障省の US-CERT（United States Computer Emergency Readiness Team）内に集約された。製品のほとんどは US-CERT によって管理されるが、この分野の文書とガイダンスは NIST が引き続き作成している。このセクションでは、US-CERT のパッチおよび脆弱性管理製品について説明する。

5.1 US-CERT National Cyber Alert System

US-CERT National Cyber Alert System は、Cyber Security Alerts、Cyber Security Tips、および Cyber Security Bulletins の 3 つの製品をまとめたものである。

+ **Cyber Security Alerts** Cyber Security Alertsは、最新のセキュリティ問題、脆弱性、および悪用行為に関するタイムリーな情報を提供する。また、技術に精通していないホームユーザや企業のユーザが、攻撃から身を守るために実行できる処置や対応策の概要を示す。Cyber Security Alertsは http://www.us-cert.gov/cas/alerts/から入手できる。

+ **Cyber Security Tips** Cyber Security Tipsは、技術に精通していないコンピュータユーザのために、一般的なセキュリティ問題について説明し、アドバイスを提供する。アドバイスは 1 つのトピックに限定する。（複雑な問題が複数のアドバイスにまたがることもあるが、ここでは扱わない）個々のアドバイスは、それ以前に公開された情報（用語と内容の両方）をもとにしている。Cyber Security Tipsは http://www.us-cert.gov/cas/tips/から入手できる。

+ **Cyber Security Bulletins** Cyber Security Bulletinsは、1 週間分のセキュリティ問題と新しい脆弱性の要約を提供する。また、リスクを軽減するためのパッチ、回避策、そのほかの対応策も提供する。Cyber Security Bulletinsは http://www.us-cert.gov/cas/bulletins/から入手できる。

5.2 CVE（Common Vulnerabilities and Exposures）標準

CVE（Common Vulnerabilities and Exposures）脆弱性命名標準 [39]は、公に知られているほとんどのIT脆弱性に対する名称の辞書である。この業界標準は、セキュリティ業界や多くの政府組織に広く受け入れられている。US-CERTが資金援助を行い、技術的な分析作業はMITRE Corporationが行っている。CVEの一般的な情報は http://cve.mitre.org/から入手できる。CVEに登録されている脆弱性は、セクション 5.3 で説明するNational Vulnerability Databaseを使用すると最適に表示できる。

CVE は、コンピュータセキュリティのコミュニティに対し、以下のものを提供する。

+ 公に知られている脆弱性の包括的なリスト

+ 新たに公開された脆弱性の信ぴょう性の分析

+ 個々の脆弱性に使用する一意の名前

NISTは、できる限りCVEに対応した脆弱性のリソースを使用することを推奨する。CVEに対応したセキュリティ製品やサービスの一覧については、http://cve.mitre.org/compatible/を参照のこと。

[39] CVE は、正規の標準化団体にはまだ採用されていない。自主的に宣言された標準として広く利用されている。NIST SP 800-51『*Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*』は http://csrc.nist.gov/publications/nistpubs/800-51/sp800-51.pdf から入手できる。

5.3 National Vulnerability Database

National Vulnerability Database（NVD）は、US-CERTのすべての脆弱性軽減製品を統合した脆弱性データベースである。このデータベースには、セクション 5.4 で説明する脆弱性メモと、セクション 5.1 で説明したNational Cyber Alert System製品が含まれる。精度の高い検索エンジンを備えており、ユーザはさまざまな特性を持つ脆弱性を検索できる。たとえば、ユーザは製品の特徴（ベンダー名、製品名、バージョン番号など）や、脆弱性の特性（深刻度、関連する悪用範囲、脆弱性の種類など）に基づいて検索できる。NVDは個々のCVE脆弱性の要約を提供する。個々の要約には、脆弱性の属性（脆弱性の概略や脆弱性が確認されたバージョン番号を含む）と、勧告、パッチ、およびその脆弱性に関連するほかのリソースへのリンクが記載される。NVDは、CVE脆弱性命名標準に則っており、この標準に準拠した検索可能なインタフェースを提供する。またNVDは、セクション 5.5 で説明するOVAL形式による問い合わせもサポートする。NVDは、US-CERTの脆弱性軽減製品スイートをサポートする目的でNISTによって開発され、管理されている。NVDは従来のICAT脆弱性データベース製品の後継であり、http://nvd.nist.gov/で利用できる。

5.4 US-CERT Vulnerability Notes Database

US-CERT Vulnerability Notes Databaseは、脆弱性に関する短い勧告を収録した検索可能なデータベースである。これらの勧告は重要ではあるが、非常に重要というわけではなく、また、US-CERT Cyber Security Alertsとして分類するのに十分な詳細情報を含んでいない。US-CERT Vulnerability Notesでの検索にこだわらない場合は、US-CERT Vulnerability Notesの情報も含み、他のさまざまな脆弱性検索先の情報—スも含まれているNVDを使って脆弱性を検索するとよいだろう。US-CERT Vulnerability Notes Databaseは http://www.kb.cert.org/vuls/から利用できる。

5.5 OVAL（Open Vulnerability Assessment Language）

OVAL（Open Vulnerability Assessment Language）は、セキュリティ専門家がコンピュータシステム上の脆弱性や設定の問題の有無をチェックする方法について技術的詳細を交換するための言語である。脆弱性や設定の問題は、テスト（XML（Extensible Markup Language）形式のOVAL定義）を使って識別される。このテストは、エンドユーザが利用することも、情報セキュリティ製品やサービスに実装することもできる。OVALは http://oval.mitre.org/で利用できる。

5.6 推奨事項

NIST は、各組織が米国政府によって一般に公開されている脆弱性およびパッチ適用のリソースを利用することを推奨する。これらのリソースは、米国政府が公式に認定した脆弱性に関する情報のソースとして直接利用すべきである。各組織は、米国政府が公開している脆弱性およびパッチ適用のリソース並びに標準に準拠している市販の製品も使用すべきである。

これらのリソースは、いくつかの方法で利用できる。たとえば、各組織は OVAL による脆弱性の特定、CVE 名称による脆弱性の一覧表示、および National Vulnerability Database 内の CVE 脆弱性情報へのリンクの提供が可能な脆弱性スキャナの購入を検討すべきである。各組織はまた、一般的な脆弱性サービスを購読している場合でも、米国政府が最も重大であると見なした脆弱性を知るために、US-CERT Cyber Security Alerts も購読すべきである。これにより優先順位の最も高い脆弱性に対して、適切な注意を払うことができる。

6. 結論および主な推奨事項の要約

パッチを扱うプロセスを設計するときは、PVG によるパッチ適用の考え方を構成している原則を考慮する必要がある。それ以外のパッチ適用方法を許容できる場合もあるが、中心となる考え方は選択したパッチ適用の方法論の範囲内で見つけるべきである。これらの考え方には、組織内インベントリの使用、パッチおよび脆弱性の監視、パッチの優先順位付けの手法、組織内のパッチデータベース、パッチのテスト、パッチの配布、パッチ適用の検証、パッチに関するトレーニング、パッチの自動導入、およびアプリケーションの自動更新が含まれる。

最小規模の組織や大規模組織の特別な領域を除き、各組織は速やかに自動化されたパッチ適用の方法に移行すべきである。自動化されたパッチ適用の方法への移行は、サービスの集中化とデスクトップの構成の標準化を目指す、組織の計画と平行して行う。このため、コンピュータセキュリティの担当者は、集中化されたサービスと標準化されたデスクトップモデルの設計に積極的に関わるべきである。

パッチ適用や脆弱性の監視は気の遠くなるような作業に思えることもあるが、組織内の脆弱性を一貫して軽減することは、テスト済みの統合されたパッチ適用プロセスによって実現できる。組織は、成熟したパッチおよび脆弱性管理プログラムを確立することでシステムにとって適切なレベルのセキュリティを、事後対応ではなく、プロアクティブに維持できるようになる。パッチの自動化と予防的な保守を組み合わることで効率が向上する結果、インシデント対応に費やされる時間、リソース、および費用が低減されるはずである。この文書は、この重要でやりがいのある仕事に取り組む人々の手助けになるはずである。

この文書には、組織による効果的なパッチおよび脆弱性管理プログラムの実施を支援するための、さまざまな推奨事項が記載されている。主な推奨事項の要約を以下に示す。

1. パッチおよび脆弱性グループを作ること。
2. 脆弱性、修正措置、および脅威を継続的に監視すること。
3. パッチ適用の優先順位を決定し、必要に応じて段階的な導入を行うこと。
4. 導入前にパッチをテストすること。
5. エンタープライズ全体を対象とする自動化されたパッチ適用ソリューションを導入すること。
6. 必要に応じて自動更新アプリケーションを使用すること。
7. すべての情報技術資産のインベントリを作成すること。
8. IT リソースに対して標準化された構成をできる限り適用すること。
9. 脆弱性が修正されたことを検証すること。
10. 組織のパッチおよび脆弱性管理プログラムの効果を常に測定し、必要に応じて是正措置を適用すること。
11. 該当する職員に対して、脆弱性の監視と修正の方法に関するトレーニングを行うこと。
12. 組織のパッチおよび脆弱性管理プログラムの効果を定期的にテストすること。
13. 必要に応じて米国政府の脆弱性軽減に関するリソースを使用すること。

付録A—略語

『*パッチおよび脆弱性管理プログラムの策定*』で使われている主な略語を以下に定義する。

CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarized Zone
DoS	Denial of Service
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）
IP	Internet Protocol
IT	Information Technology
ITL	Information Technology Laboratory（情報技術ラボラトリ）
NIST	National Institute of Standards and Technology（米国国立標準技術研究所）
NVD	National Vulnerability Database
OMB	Office of Management and Budget（行政管理予算局）
OVAL	Open Vulnerability Assessment Language
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PVG	Patch and Vulnerability Group（パッチおよび脆弱性グループ）
RPC	Remote Procedure Call
URL	Uniform Resource Locator
US-CERT	United States Computer Emergency Readiness Team
XML	Extensible Markup Language

（本ページは意図的に白紙のままとする）

付録B—用語集

『*パッチおよび脆弱性管理プログラムの策定*』で使われている主な用語を以下に定義する。

アプリケーション（Application）：ユーザのためにデータを処理するデータ入力、更新、照会、またはレポートプログラム。

運用認可（Accreditation）：承認（certification）の審査を行い、受容できるレベルのリスクの下でシステムの運用と相互接続が承認されたことを公式に宣言するプロセス。

管理者権限（Administrative Access）：コンピュータのオペレーティングシステムに対し重要な構成変更を実施できる能力を含む、コンピュータまたはアプリケーションへの高度な権限。「特権」または「root **権限**」とも呼ばれる。

可用性（Availability）：IT リソースに対して、承認されたユーザが常にアクセスできることを保証すること。

バックアップ（Backup）：システムのデータまたはアプリケーションのコピー。データが消失または破損した場合に使用できる。

承認（Certification）：システムの技術的および非技術的セキュリティ機能の包括的な評価。運用認可プロセスを支援するために行われ、特定の設計および実装が指定のセキュリティ要件のセットをどの程度満たしているかが確認される。

機密性（Confidentiality）：承認されていない主体やプロセスに対して情報が開示されないことを保証すること。

構成の調整（Configuration Adjustment）：アプリケーションの設定を変更する行為。一般的な構成の調整には、サービスの無効化、特権の変更、ファイアウォール規則の変更などがある。

構成変更（Configuration Modification）：「構成の調整(Configuration adjustment)」を参照。

脆弱性実証コード（Exploit Code）：攻撃者がシステムに自動的に侵入できるようにするプログラム。

ファイアウォール（Firewall）：ネットワーク通信を制限および監視することによって、コンピュータまたはネットワークをほかのネットワークから保護するプログラム。

ホスト（Host）：コンピュータまたは IT 機器（ルータ、スイッチ、ゲートウェイ、ファイアウォールなど）。ホストは、「システム」の非公式な定義と同義である。

ホットフィックス（Hotfix）：セキュリティパッチに対応する Microsoft の用語。

完全性（Integrity）：情報の正確さが意図されたレベルで維持されることを保証すること。

設定ミス（Misconfiguration）：システム内にセキュリティ上の弱点を生み出すおそれがある設定上の誤り。

オペレーティングシステム（Operating System）：コンピュータを動作させる主要な制御プログラム。

パッチ（Patch）：既存のソフトウェアに含まれる問題を解決するために開発された追加コード。

修正措置（Remediation）：脆弱性を修正する行為、または脅威を解消する行為。修正措置には、パッチのインストール、構成設定の調整、およびソフトウェアアプリケーションのアンインストールの 3 種類が考えられる。

修正措置計画（Remediation Plan）：組織のシステムが直面する 1 つ以上の脅威または脆弱性を対象に、修正措置を実施するための計画。この計画には、通常、脅威や脆弱性を取り除くためのオプションと、修正措置を実施する優先順位が含まれる。

リスク（Risk）：特定の脅威によって特定の脆弱性が悪用される可能性。

セキュリティ計画（Security Plan）：特定の正式に定義されたシステムに対して策定し、計画された（管理上、技術上、および運用上の）セキュリティ管理策の詳細を記載した文書。

システム（System）：直接の運営と予算管理の体制が共通であり、同じ機能と任務上の目標を持ち、セキュリティのニーズが本質的に同じであり、同一の一般的な運用環境に存在する一連の IT 資産、プロセス、アプリケーション、および関連するリソース。このような正式な意味で使用しない場合は、「ホスト」と同義である。この用語を使用する場合、どちらの定義を使用しているかは、文脈によって、または明示することによって明らかにする。

システム管理者（System Administrator）：システムの技術的な管理を行う人。

システム所有者（System Owner）：情報技術システムのあらゆる面に関して、管理上、運用上、技術上、および（多くの場合）予算上の責任を持つ人。

脅威（Threat）：システムに損害が与えるおそれがある（故意または偶発の）状況または事象。

ウイルス（Virus）：悪意を持って作成され、複数のコンピュータまたはプログラムに広がる能力を持つプログラム。ほとんどのウイルスは、何らかの種類の悪意のコードを拡散および配信するための条件を定義したトリガメカニズムを持っている。

脆弱性（Vulnerability）：ソフトウェアの設計または設定に含まれる欠陥のうち、セキュリティに影響するもの。さまざまな組織で、一般に公開された脆弱性データベースを維持している。

回避策（Workaround）：特定の脆弱性に起因する脅威を軽減するために、ソフトウェアパッケージまたはそのほかの情報技術リソースに対して行う構成変更。回避策では、通常、（パッチとは異なり）根本的な問題は修正されず、IT リソース内の機能が制限されることが多い。

ワーム（Worm）：悪意のコードの一種で、特にネットワーク接続されたコンピュータを対象にするもの。脆弱なホストを悪用し、自己複製し、プログラムに従って何らかの損害を与えながら、コンピュータネットワークに浸透する自己増殖型のプログラム。

付録C—パッチおよび脆弱性関連のリソースの種類

この付録では、パッチおよび脆弱性に関する情報を提供する各種のリソースについて、その長所と短所を説明する。説明するリソースを次に示す。

+ ベンダーの Web サイトおよびメーリングリスト
+ サードパーティの Web サイト
+ サードパーティのメーリングリストおよびニュースグループ
+ 脆弱性スキャナ
+ 脆弱性データベース
+ エンタープライズ向けパッチ管理ツール
+ そのほかの通知ツール

C.1 ベンダーの Web サイトおよびメーリングリスト

ベンダーの Web サイトは、新しいパッチに関する情報のリソースとして最もよく使われるサイトであると言える。これらのサイトは、大量の情報を提供しており、パッチをダウンロードするための一次提供元になる。ベンダーの Web サイトには、次のようなメリットがある。

+ 製品を開発し、製品のことを最もよくわかっているアプリケーションベンダーがパッチをリリースしている。
+ ベンダーの Web サイトからダウンロードしたパッチは、悪意のコードに汚染されていない可能性が最も高い。
+ ベンダーは、多くの場合、自社アプリケーションに関連する脆弱性の情報（軽減方法、パッチのインストールや使用に関する指示など含む）を数多く提供する。
+ ベンダーには、自社製品に関する独自の専門知識がある。

ベンダーの Web サイトには次のような制約もある。

+ 能動的な通知が行われない場合もあるため、サイトに頻繁にアクセスして確認する必要がある。
+ サポートされるすべての製品を網羅するために、場合によっては数多くのベンダーの Web サイトを監視する必要がある。
+ ベンダーの多くはパッチが準備できるまで脆弱性を報告しようとしないため、新しい脆弱性がタイムリーに掲載されない可能性がある。該当する脆弱性や悪用の情報が、サードパーティの Web サイトやメーリングリストにすでに投稿されている場合がある。

大手ベンダーの多くは、メーリングリストを整備しており、脆弱性、パッチ、および更新に関する電子メールメッセージや通知を製品ユーザに送信している。これらのメーリングリストは特定のベンダー製品系列に存在する新しい脆弱性をユーザに通知するため、ユーザはベンダーのセキュリティ Web サイトに定期的にアクセスせずに済む。これらのメーリングリストの欠点は、PVG やシステム管理者が複数のオペレーティングシステムや数多くのアプリケーションを管理するために、数多くのベンダーのメーリングリストを購読しなければならない可能性があることである。加えて、ベンダー

が自社のメーリングリストをマーケティング目的で使用した場合には、結果としてシステム管理者はメーリングリストからのメッセージをすべて無視したり、フィルタリングしたりする可能性がある。電子メールは安全な配信メカニズムではないため、一般にベンダーは実際のパッチを電子メール添付で配信することはない。もし電子メールでパッチが配信される場合は、電子メールにディジタル署名が付けられるべきであり、受信者はメールを信頼して開く前に、署名をチェックすべきである。

C.2 サードパーティの Web サイト

サードパーティのパッチおよび脆弱性 Web サイトは、アプリケーションベンダーとは無関係のサイトだが、ベンダーのサイトよりも詳しい情報を提供する場合がある。これらの Web サイトには、数多くのベンダーや製品をカバーするものと、特定のベンダーや製品に特化したものがある。ベンダーは脆弱性の確認とパッチ（またはそのほかの脆弱性軽減の方法）の作成が終了するまで通知を遅らせることが多いため、サードパーティの Web サイトがベンダーよりも先に新しい脆弱性を報告することが多い。サードパーティの Web サイトには、次のようなメリットがある。

+ 新しい脆弱性に関する情報がタイムリーに公開される。
+ サイトによっては、次のメリットがある。
  – 複数のベンダーや製品を対象としている場合、システム管理者は情報収集のために数多くの Web サイトにアクセスする必要がない（つまり「ワンストップショッピング」である）。
  – 特定の製品やプラットフォームに特化している（無関係のデータのなかを探さずに済むため、システム管理者の作業時間が節約される）。
+ ユーザに投稿を許可しているサイトでは、次のメリットがある。
  – サードパーティのメーリングリストやニュースグループと同様のメリットがある（セクション C.3 を参照）。
  – フィルタリングやランク付けのメカニズムにより、ユーザは「価値の高い」投稿だけを読むことができる。
+ ベンダーが提示する公式の軽減方法よりも受け入れやすい、代替の方法が提示される可能性がある。
+ ベンダーが提供しようとしない情報が得られる。

サードパーティの Web サイトには、次のようなデメリットがある。

+ サードパーティのパッチのほうが、予期しない結果が生じる可能性や、悪意のコードが含まれている可能性が高い。
+ 脆弱性へのパッチ適用に関する包括的な情報が得られないため、複数のリソースを調査する必要がある。

C.3 サードパーティのメーリングリストおよびニュースグループ

メーリングリストやニュースグループは、電子メールを利用したスレッド方式の討議グループである。これらは、同じ分野に関心を持つユーザの意見交換の場になっている。サードパーティのメーリングリストやニュースグループの最大のメリットは、ベンダーのメーリングリストが単方向の（ベンダーからユーザへの）コミュニケーションしかサポートしないのに対し、システム管理者やそのほかのユーザが双方向でコミュニケーションできる点にある。これにより、システム管理者は自分の経験を共

有したり、質問したりできる。ニュースグループとメーリングリストの主な違いは次のような点にある。ニュースグループは、「公式に」認められたインターネット上の公開討論の場であり、一定の手続きを踏まないと設置することができない。これに対し、メーリングリストは、メールサーバとインターネットへのアクセス環境があれば、誰でも設置できる。メーリングリストでは、仲介役による管理や参加者の制御が可能である。

サードパーティのメーリングリストやニュースグループには、次のようなメリットがある。

+ システム管理者同士の交流が可能である。
+ システム管理者が能動的に探索しなければならないサイトの数が少なくて済む。
+ システム管理者がほかの人々の経験から（たとえば、特定のパッチに関連する問題があるかどうかや、パッチによって本当に問題が修正されるかどうかなどを）直接学ぶことができる。
+ パッチがリリースされるまでの回避策が提示される場合がある。

サードパーティのメーリングリストやニュースグループには、次のようなデメリットがある。

+ システム管理者にとって有用でない可能性のある電子メールが大量に送信される。
+ 取扱いに注意を要する情報が、承認されていない主体に対して公開される可能性がある（あるシステムに関する質問をしたシステム管理者は、気付かないうちにそのシステムの脆弱性の悪用を試みる攻撃者を招き入れる可能性がある）。
+ サードパーティの修正プログラムや回避策は、その作成責任の所在が明らかでない場合があるため、悪意のコードにさらされる可能性が高くなる。
+ 組織が未承諾広告（スパム）にさらされる。
+ 不正確な情報が提供される可能性がある。
+ サイトにアクセスしたホストに対して悪用行為を自動的に開始する自己診断サイトへのリンクが作成される可能性がある（パッチ未適用のシステムがそのサイトにアクセスした場合、問題が発生するおそれがある）。

C.4 脆弱性スキャナ

脆弱性スキャナは、多くの組織でホストやネットワーク上の脆弱性を特定するためによく使われている。脆弱性スキャナは、よく使われるオペレーティングシステムやアプリケーションに関連する脆弱性を特定するために、大規模な脆弱性データベースを利用する。脆弱性スキャナには、ネットワークスキャナとホストスキャナの 2 種類がある。ネットワークスキャナは、開かれているポート、脆弱性のあるソフトウェア、および誤って設定されたサービスを特定するために使う。ホストスキャナは、特定のオペレーティングシステムやアプリケーションの設定ミスや脆弱性を特定するために使う。脆弱性スキャナの詳細については、セクション 2.9.1 を参照のこと。

脆弱性スキャナは、次の機能を備えている。

+ 脆弱性を事前に特定する。
+ リスクに晒されている状態をすばやく簡単に測定する方法を提供する。
+ 検出された脆弱性を自動的に修正する。

- バージョンの古いソフトウェアを特定する。
- 組織のセキュリティポリシーへの適合性を検証する。
- 特定された脆弱性に関する警告とレポートを生成する。

しかし、脆弱性スキャナには次のような弱点がある。

- 脆弱性データベースの定期的な更新に依存している。
- フォールスポジティブエラーが高い確率で発生する傾向がある。
- 大量のネットワークトラフィックが発生する可能性がある。
- ホストに対しサービス不能（DoS）が発生する可能性がある（スキャナのプローブ処理によってシステムが意図せずクラッシュすることがあるため）。

C.5 脆弱性データベース

脆弱性データベースは、情報システムに影響を与える脆弱性に関する情報を、検索可能な形で収集したものである。これらのデータベースの多くは、Web 上で一般に公開されている。これらの Web サイトは、一般にソフトウェアベンダーとは無関係のサードパーティによって運営され、システム管理者やセキュリティ専門家に豊富な情報を提供することができる。また、これらの Web サイトは、ほとんどのオペレーティングシステムやソフトウェアアプリケーションをカバーすることに努めている。ソフトウェアベンダーとは無関係なため、ベンダー（またはベンダーと関連のあるそのほかの組織）によって提供されない情報が提供されることも多い。

脆弱性データベースは新しい脆弱性を最も早く報告する傾向があるが、それはメリットでもあり、デメリットでもある。脆弱性に関する情報がタイムリーに提供されることは、システム管理者がネットワークのセキュリティ確保を成功させる上で、きわめて重要となる可能性がある。

サイトによって情報の量と質に多少のばらつきがあるが、脆弱性データベースには一般に次の種類の情報が含まれている。

- **脆弱性の概要**－脆弱性の紹介。これには、CVE 名、脆弱性の種類、脆弱性が最初に公式に特定された日付、脆弱性またはパッチの情報が最後に更新された日付、および脆弱性の影響を受けるオペレーティングシステム、アプリケーション、またはハードウェアが含まれる。
- **解説または分析**－脆弱性に関する詳しい情報。脆弱性の複雑さに応じて、1 つの段落でまとめられる場合もあれば、、複数のページにわたる場合もある。この解説は、高度に技術的な場合がある。
- **解決策**－脆弱性の軽減や解消に関する詳しい解説。一般に、関係するベンダーのパッチや更新を提供する Web サイトへのハイパーリンクが含まれる。通常そのほかの修正方法がある場合は、それらも含まれる。
- **脆弱性の悪用**－脆弱性の悪用や該当するコードに関する情報、または詳細な情報や脆弱性実証コードが掲載されたほかのサイトへのリンク。これらの情報は、（パッチの適用前または適用後に）システムが悪用行為の対象になるかどうかをシステム管理者が判定するときに役に立つ。ただし、これらの技法を使用する場合は、システムに意図しない損害が発生しないように十分に注意すること。

総じて、脆弱性データベースは現在利用できる最も強力なリソースの 1 つである。脆弱性の情報収集をほかのソースに依存している組織にとっても、脆弱性データベースサイトで提供される一般的なニュースや解説はきわめて貴重だといえる。

C.6 エンタープライズ向けパッチ管理ツール

脆弱性およびそれに対応するパッチの数が増え続けているため、手作業でコンピュータにパッチを適用することはますます困難になり、有効でなくなりつつある。したがって組織の大部分のシステムは、エンタープライズ向けパッチ管理プログラムに参加させるべきである。エンタープライズ向けパッチ管理ツールは、そのパッチ適用ソリューションに参加しているコンピュータの脆弱性の有無をスキャンし、それらのコンピュータに必要なパッチやそのほかのソフトウェア更新に関する情報を提供する。管理者は、この情報を使ってパッチ適用プロセスを決定できる。

エンタープライズ向けパッチ管理ツールは、大きく 2 つに分類される。1 つはエージェントを使用するツールであり、もう 1 つはエージェントを使用しないツールである。どちらのアプローチの場合も、通常は、インストールすることが必要または可能なパッチを格納した中央コンピュータと、パッチ適用の管理者がプロセスを制御するためのコンソールが存在する。2 つのアプローチには、それぞれ考慮すべき長所と短所がある。エージェントを使用しないパッチ管理ツールの最大のメリットは、パッチ適用ソリューションに参加するコンピュータにソフトウェアエージェントをインストールする必要がないことである。ただし、エージェントなしのツールはネットワーク帯域幅の大部分を専有する場合があり、大規模なネットワークのスキャンには長い時間がかかる可能性がある。一方エージェントを使用するソリューションでは、大規模なネットワークをより高速にスキャンでき、使われるネットワーク帯域幅も最小限で済むが、参加する各システムにソフトウェアエージェントをインストールして管理する必要がある。エンタープライズ向けパッチ適用ソリューションの詳細については、セクション 4.1 で説明している。

自動化されたパッチ管理ツールやユーティリティは、さまざまなベンダーから入手できる。これらを使用することで、既知の脆弱性を特定しやすくなり、パッチおよび脆弱性管理プロセスが自動化される。この文書に示したガイダンスは、製品ベンダーのマニュアルや推奨事項の代わりになるものではなく、それらを補足するものである。

C.7 そのほかの通知ツール

脆弱性の報告、パッチのリリース、および脆弱性実証コードの公開を追い続ける負担が大きくなっているため、PVG やシステム管理者に対して、彼らがサポートしているシステムに関する通知を自動化・カスタマイズして提供するための、さまざまなツールやアプリケーションが作成されている。これらのツールは、ベンダーまたはサードパーティによって提供されている。無償の製品もあれば、1 回限りの料金や購読料が必要な製品もある。

これらの通知ツールには、次のようなメリットがある。

+ 通知機能をカスタマイズすることにより、必要なアプリケーションやオペレーティングシステムに対象を限定できる。
+ システム管理者に対してリアルタイムに警告が生成される（Web ページにアクセスする必要がない）。

これらの通知ツールには、次のようなデメリットがある。

+ コスト（料金徴収型のサービスの場合）

+ 情報の品質（情報ソースの品質は、基盤となる情報データベースの品質に左右される）
+ 特定のサービスに固有の遅延時間
+ セキュリティ侵害の可能性（管理者は、使用しているオペレーティングシステムやアプリケーションをサードパーティに伝える必要があるため）

（本ページは意図的に白紙のままとする）

付録D—パッチおよび脆弱性関連のリソース

以下の一覧に、既知の脆弱性を特定したり、一般的なオペレーティングシステムやアプリケーションのパッチを検索、入手、適用したりするのに役に立つリソース（ソフトウェアや Web サイトなど）の例を示す。

一般的なパッチ管理ソフトウェア

ソフトウェア名	ベンダー	URL
Altiris Patch Management Solution	Altiris	http://www.altiris.com/products/patchmanagement/
ANSA	Autonomic Software, Inc.	http://www.autonomic-software.com/patch.html
BigFix Patch Manager	BigFix, Inc.	http://www.bigfix.com/products/products_patch.html
BindView Patch Management	Bindview Corporation	http://www.bindview.com/Solutions/VulnMgmt/ManagePatches.cfm
C5 Enterprise Vulnerability Management Suite	Secure Elements	http://www.secure-elements.com/products/
Ecora Patch Manager	Ecora Software	http://www.ecora.com/ecora/products/patchmanager.asp
eTrust Vulnerability Manager	Computer Associates International, Inc.	http://www3.ca.com/Solutions/Product.asp?ID=4707
GFI LANguard Network Security Scanner	GFI Software Ltd.	http://www.gfi.com/lannetscan/
Hercules	Citadel Security Software	http://www.citadel.com/hercules.asp
HFNetChkPro	Shavlik Technologies, LLC	http://www.shavlik.com/
HP OpenView Patch Manager using Radia	Hewlett-Packard Development Company	http://www.managementsoftware.hp.com/products/radia_patm/index.html
Kaseya Patch Management	Kaseya, Inc.	http://www.kaseya.com/prod1/pl/patch_management.phtml
LANDesk Patch Manager	LANDesk Software	http://www.landesk.com/Products/Patch/Index.aspx
LiveState Patch Manager	Symantec Corporation	http://sea.symantec.com/content/product.cfm?productid=30
ManageSoft Security Patch Management	ManageSoft Corporation Ltd.	http://www.managesoft.com/product/patchmanagement/index.xml
Marimba Patch Management	BMC Software, Inc.	http://www.marimba.com/products/solutions/patch-mgmt.html
NetIQ Vulnerability Manager	NetIQ Corporation	http://www.netiq.com/products/vsm/default.asp
Opsware Server Automation System	Opsware, Inc.	http://www.opsware.com/products/serverautomation/patchmgmt/
PatchLink Update	PatchLink Corporation	http://www.patchlink.com/products_services/patchlink_update.html
PolicyMaker Software Update	DesktopStandard Corporation	http://www.desktopstandard.com/PolicyMakerSoftwareUpdate.aspx
Prism Patch Manager	New Boundary Technologies	http://www.newboundary.com/products/prismpatch/prismpatch_info.htm
SecureCentral PatchQuest	AdventNet, Inc.	http://www.securecentral.com/products/patchquest/
Security Update Manager	ConfigureSoft	http://www.configuresoft.com/SUMMain.aspx
Service Pack Manager	Gravity Storm Software	http://www.securitybastion.com/
Sitekeeper（Patchkeeper モジュール）	Executive Software	http://www.execsoft.com/sitekeeper/sitekeeper.asp
Software Update Services	Microsoft Corporation	http://www.microsoft.com/windowsserversystem/updateservices/evaluation/previous/default.mspx

ソフトウェア名	ベンダー	URL
Systems Management Server	Microsoft Corporation	http://www.microsoft.com/smserver/default.asp
SysUpdate	SecurityProfiling Inc.	http://www.securityprofiling.com/eng/products/sysupdate.shtml
UpdateEXPERT	St. Bernard Software	http://www.patches-management.stbernard.com/
Windows Server Update Services	Microsoft Corporation	http://www.microsoft.com/windowsserversystem/updateservices/default.mspx
ZENworks Patch Management	Novell, Inc.	http://www.novell.com/products/zenworks/patchmanagement/index.html

一般的なオペレーティングシステム

Web サイト名または Web ページ名	URL
Apple	
Apple Support	http://www.apple.com/support/
Apple Downloads	http://www.apple.com/support/downloads/
BSD	
FreeBSD Security Information	http://www.freebsd.org/security/index.html
Getting FreeBSD	http://www.freebsd.org/where.html
OpenBSD Security	http://www.openbsd.org/security.html
Getting OpenBSD	http://www.openbsd.org/ftp.html
Cisco	
Cisco Product Security Incident Response	http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
Improving Security on Cisco Routers	http://www.cisco.com/warp/public/707/21.html
Products & Services Security Advisories	http://www.cisco.com/en/US/products/products_security_advisories_listing.html
Technical Support & Documentation	http://www.cisco.com/en/US/support/index.html
Linux[40]	
Debian GNU/Linux Security Information	http://www.debian.org/security/
Getting Debian	http://www.debian.org/distrib/
Fedora Download	http://fedora.redhat.com/download/
How to Download [Fedora] Updates	http://fedora.redhat.com/download/updates.html
Mandriva Linux Download	http://www.mandrivalinux.com/en/ftp.php3
Mandriva Security Advisories	http://www.mandriva.com/security/
Ubuntu Linux Download	http://www.ubuntulinux.org/download/
Ubuntu Support	http://www.ubuntulinux.org/support/
Microsoft	
Microsoft Download Center	http://www.microsoft.com/downloads/search.aspx?displaylang=en
Microsoft Help and Support	http://support.microsoft.com/default.aspx
Microsoft Security Home Page	http://www.microsoft.com/security/default.mspx
Microsoft Security Notification Service	http://www.microsoft.com/technet/security/bulletin/notify.mspx
Microsoft Windows Update	http://windowsupdate.microsoft.com/
Security Bulletins	http://www.microsoft.com/security/bulletins/alerts.mspx
Novell	

[40] この表は、現在入手可能な何百もの Linux ディストリビューションのうち、最も人気のあるものをいくつか示している。ほかのディストリビューションについては、DistroWatch.com（http://distrowatch.com/）を参照のこと。

Web サイト名または Web ページ名	URL
Novell Security	http://www.novell.com/products/security.html
Novell Support	http://support.novell.com/
Sun	
Solaris Download	http://www.sun.com/software/solaris/get.jsp
Solaris Live Upgrade	http://www.sun.com/software/solaris/liveupgrade/
Sun Update Connection--Patches and Updates	http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
SunSolve Online	http://sunsolve.sun.com/

一般的なクライアントアプリケーション

製品系列	ベンダー	URL
圧縮ユーティリティ		
7-Zip	7-Zip/Igor Pavlov	http://www.7-zip.org/download.html
ArchiveXpert	Concepts for Future	http://archivexpert.com/download/
PicoZip	Acubix	http://www.picozip.com/downloads.html
PKZip	PKWare	http://www.pkware.com/business_and_developers/support/updates/
PowerArchiver	ConeXware, Inc.	http://www.powerarchiver.com/download/
PowerZip	Trident Software Pty Ltd	http://www.powerzip.biz/download.aspx
SecureZip	PKWare	http://www.pkware.com/business_and_developers/support/updates/
StuffIt	Allume Systems Inc.	http://www.stuffit.com/
WinZip	WinZip Computing	http://www.winzip.com/downwzeval.htm
ZipMagic	Allume Systems Inc.	http://www.stuffit.com/win/zipmagic/
電子メールクライアント		
Balsa	GNOME Project	http://balsa.gnome.org/download.html
Barca	Poco Systems, Inc.	http://www.pocosystems.com/home/index.php?option=content&task=category&sectionid=2&id=21&Itemid=38
Eudora	Qualcomm	http://www.eudora.com/download/
Eureka Email	Eureka Email	http://www.eureka-email.com/Download.html
GNUMail.app	Collaboration-world.com	http://www.collaboration-world.com/cgi-bin/project/release.cgi?pid=2
GyazMail	GyazSquare	http://www.gyazsquare.com/gyazmail/download.php
i.Scribe	Memecode Software	http://www.memecode.com/scribe.php
InScribe	Memecode Software	http://www.memecode.com/inscribe.php
KMail	Kmail	http://kmail.kde.org/download.html
Mac OS X Mail	Apple	http://www.apple.com/support/panther/mail/
Mailsmith	Bare Bones Software	http://www.barebones.com/support/mailsmith/updates.shtml
Mercury Mail Transport System	David Harris	http://www.pmail.com/patches.htm
Mozilla	Mozilla	http://www.mozilla.org/security/
Mutt	Mutt	http://www.mutt.org/download.html
Nisus Email	Nisus Software	http://www.nisus.com/NisusEmail/FAQ.php?PHPSESSID=0ba9f9639672d1fdf836a97f3ad29383#HowUpgradeOS9
Outlook	Microsoft	http://office.microsoft.com/en-us/officeupdate/default.aspx
Outlook Express	Microsoft	http://www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=7

製品系列	ベンダー	URL
Pegasus Mail	David Harris	http://www.pmail.com/patches.htm
Pine	University of Washington	http://www.washington.edu/pine/getpine/
PocoMail	Poco Systems, Inc.	http://www.pocosystems.com/home/
Sylpheed	Sylpheed	http://sylpheed.good-day.net/
Thunderbird	Mozilla	http://www.mozilla.org/products/thunderbird/
VM	VM	http://www.wonderworks.com/vm/download.html
FTP クライアント		
BulletProof FTP Client	BulletProof Software	http://www.bpftp.com/download.php
CuteFTP Professional	GlobalSCAPE	http://www.cuteftp.com/downloads/cuteftppro.asp
FileZilla	FileZilla	http://sourceforge.net/projects/filezilla/
FlashFXP	IniCom Networks	http://www.flashfxp.com/download.php
FTP Voyager	Rhino Software	http://www.ftpvoyager.com/dn.asp
gFTP	Brian Masney	http://gftp.seul.org/
NcFTP	NcFTP Software	http://www.ncftp.com/download/
SmartFTP	SmartFTP	http://www.smartftp.com/download/
Transmit 3	Panic, Inc.	http://www.panic.com/transmit/index.html
WS_FTP Professional	Ipswitch	http://www.ipswitch.com/support/WS_FTP/patch-upgrades.html
インスタントメッセージングクライアント		
AOL Instant Messenger	AOL	http://www.aim.com/download.adp?aolp=1
GAIM	GAIM	http://gaim.sourceforge.net/downloads.php
Jabber	Jabber, Inc.	http://www.jabber.com/index.cgi?CONTENT_ID=503
Lumen Instant Messenger	Novell	http://www.novell.com/partnerguide/product/200671.html
Miranda	Miranda	http://sourceforge.net/project/showfiles.php?group_id=94142
MSN Messenger	Microsoft	http://messenger.msn.com/Download/
Trillian	Cerulean Studios	http://www.download.com/Trillian/3000-2150-10047473.html
Vypress Messenger	Vypress	http://www.vypress.com/products/messenger/
Windows Messenger	Microsoft	http://www.microsoft.com/downloads/search.aspx?displaylang=en
Yahoo Messenger	Yahoo	http://messenger.yahoo.com/messenger/security/
マルチメディアユーティリティ		
Flash	Macromedia	http://www.macromedia.com/downloads/
iTunes	Apple	http://www.apple.com/itunes/download/
QuickTime	Apple	http://www.apple.com/support/
Real Player	Real	http://service.real.com/realplayer/security/
Shockwave	Macromedia	http://www.macromedia.com/downloads/
Winamp	Winamp	http://www.winamp.com/player/free.php
Windows Media Player	Microsoft	http://www.microsoft.com/windows/windowsmedia/player/download/download.aspx
オフィス生産性向上ツール		
Acrobat	Adobe	http://www.adobe.com/support/downloads/main.html
AppleWorks	Apple	http://www.apple.com/support/appleworks/
Microsoft Office	Microsoft	http://office.microsoft.com/en-us/officeupdate/default.aspx?displaylang=EN
Microsoft Works	Microsoft	http://www.microsoft.com/products/works/downloads.mspx
NeoOffice	NeoOffice	http://www.planamesa.com/neojava/en/download.php

製品系列	ベンダー	URL
OpenOffice	OpenOffice.org	http://www.openoffice.org/
StarOffice	Sun	http://www.sun.com/download/index.jsp?cat=Patches%20%26%20Updates&tab=3
WordPerfect Office	Corel	http://www.corel.com/servlet/Satellite?pagename=Corel3/Downloads/SupportDownloads
SSH クライアント		
OpenSSH	OpenBSD Project	http://www.openssh.com/
PuTTY	Simon Tatham	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
Reflection for Secure IT	AttachmateWRQ	http://download.wrq.com/
SecureCRT	VanDyke Software	http://www.vandyke.com/support/index.html
SSH Tectia	SSH Communications Security	http://www.ssh.com/support/downloads/
Web ブラウザ		
Camino	Mozilla	http://www.caminobrowser.org/
Firefox	Mozilla	http://www.mozilla.org/security/
Internet Explorer	Microsoft	http://www.microsoft.com/windows/ie/downloads/default.mspx
Konqueror	KDE	http://www.kde.org/download/
Mozilla Suite	Mozilla	http://www.mozilla.org/security/
Netscape	Netscape Communications	http://channels.netscape.com/ns/browsers/default.jsp
Opera	Opera Software	http://www.opera.com/download/
Safari	Apple	http://www.apple.com/support/downloads/safari.html

一般的なサーバアプリケーション

製品名	ベンダー	URL
アプリケーションサーバ		
Apache Tomcat	Apache Foundation	http://jakarta.apache.org/site/downloads/downloads_tomcat.html
BEA Web Logic Server	BEA Systems	http://commerce.bea.com/index.jsp
Borland Enterprise Server	Borland	http://www.borland.com/downloads/download_bes.html
Flash Communication Server	Macromedia	http://www.macromedia.com/support/flashcom/downloads_updaters.html
HAHTsite	HAHT Commerce	http://www.haht.com/HAHTsite/
IBM WebSphere Application Server	IBM	http://www.ibm.com/products/finder/us/finders?pg=ddfinder
Interbase	Borland	http://www.borland.com/downloads/download_interbase.html
JBoss	JBoss	http://www.jboss.org/downloads/index
JRun Application Server	Macromedia	http://www.macromedia.com/support/jrun/updaters.html
Oracle Application Server	Oracle	http://www.oracle.com/technology/software/products/ias/index.html
Orion Application Server	Orion	http://www.orionserver.com/
Pramati Server	Pramati Technologies	http://www.pramati.com/index.jsp?id=downloads_archive&product=psv
Sun Java System Application Server	Sun	http://www.sun.com/download/index.jsp?cat=Patches%20%26%20Updates&tab=3
Zope	Zope Community	http://www.zope.org/Products/
コラボレーションサーバ		
GroupWise	Novell	http://support.novell.com/support_options.html
Lotus Domino	IBM	http://www-132.ibm.com/content/home/store_IBMPublicUSA/en_US/Upgrades.html
Novell Evolution	Novell	http://support.novell.com/support_options.html
SUSE Linux OpenExchange Server	Novell	http://www.novell.com/products/openexchange/download.html
TeamWare Office	TeamWare Group	http://www.teamware.net/Resource.phx/download/index.htx
WebBoard	Akiva	http://www.akiva.com/downloads/index.cfm?id=webboard
Windows SharePoint Services	Microsoft	http://www.microsoft.com/windowsserver2003/technologies/sharepoint/default.mspx
データベースサーバ		
DB2	IBM	https://www-927.ibm.com/search/SupportSearchWeb/SupportSearch?pageCode=SBD&brand=db2
Informix	IBM	http://www-306.ibm.com/software/data/informix/support/
Microsoft SQL Server	Microsoft	http://www.microsoft.com/sql/downloads/default.asp
MySQL	MySQL	http://dev.mysql.com/downloads/
Oracle	Oracle	http://www.oracle.com/technology/software/index.html
Pervasive PSQL	Pervasive Software	http://www.pervasive.com/support/updates/?product=psql
PostgreSQL	PostgreSQL Global Development Group	http://www.postgresql.org/ftp/source/
DNS サーバ		

製品名	ベンダー	URL
BIND	Internet Systems Consortium	http://www.isc.org/index.pl?/sw/bind/
djbdns	D. J. Bernstein	http://cr.yp.to/djbdns/install.html
Microsoft DNS	Microsoft	http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/dns/default.mspx
Nominum Foundation	Nominum	http://www.nominum.com/open_source_support.php?stype=2&sind=2
NSD	NLnet Labs	http://www.nlnetlabs.nl/nsd/index.html
PowerDNS	PowerDNS	http://www.powerdns.com/en/downloads.aspx
電子メールサーバ		
602LAN Suite	Software602	http://support.software602.com/updates/
ArGoSoft Mail Server	ArGoSoft	http://www.argosoft.com/mailserver/download.aspx
CommuniGate Pro	Stalker Software	http://www.stalker.com/CommuniGatePro/
Eudora Internet Mail Server（EIMS）	Glenn Anderson	http://www.eudora.co.nz/updates.html
Eudora WorldMail Server	Qualcomm	http://www.eudora.com/download/worldmail/
Exim	Exim	http://www.exim.org/
IMail Server	Ipswitch	http://www.ipswitch.com/support/imail/releases/imail_professional/index.asp
inFusion Mail Server	CoolFusion	http://www.coolfusion.com/downloads/
Kaspersky SMTP Gateway for UNIX	Kaspersky	http://www.kaspersky.com/productupdates/
Kerio MailServer	Kerio Technologies	http://www.kerio.com/subscription.html
Lotus Domino	IBM	http://www-132.ibm.com/content/home/store_IBMPublicUSA/en_US/Upgrades.html
MailEnable	MailEnable	http://www.mailenable.com/hotfix/default.asp
MailMax	Smartmax Software	http://www.smartmax.com/mmupgradecenter.aspx
MailSite	Rockliffe	http://www.rockliffe.com/userroom/download.asp
MDaemon	alt-n Technologies	http://www.altn.com/download/default.asp?product_id=MDaemon
Merak Mail Server	Merak	http://www.merakmailserver.com/Download/
Microsoft Exchange	Microsoft	http://www.microsoft.com/exchange/downloads/2003/default.mspx
Postfix	Wietse Venema	http://www.postfix.org/download.html
Sendmail（商用版）	Sendmail, Inc.	http://www.sendmail.com/support/download/patch_page.shtml
sendmail（フリーウェア版）	Sendmail Consortium	http://www.sendmail.org/
Xmail	Davide Libenzi	http://www.xmailserver.org/
FTP サーバ		
ArGoSoft FTP Server	ArGoSoft	http://www.argosoft.com/ftpserver/upgrade.aspx
BulletProof FTP Server	BulletProof Software	http://www.bpftpserver.com/download.php
CrushFTP Server	CrushFTP	http://www.crushftp.com/download.html
GuildFTPd FTP Server Daemon	GuildFTPd	http://www.guildftpd.com/
RaidenFTPD	Raiden	http://www.raidenftpd.com/en/download.html
Rumpus FTP	Maxum Development Corporation	http://www.maxum.com/Rumpus/Upgrades.html
Secure FTP Server	GlobalSCAPE	http://www.cuteftp.com/gsftps/upgrade.asp

製品名	ベンダー	URL
Serv-U FTP Server	Serv-U	https://rhinosoft.com/custsupport/index.asp?prod=rs
SurgeFTP	NetWin	http://netwinsite.com/cgi-bin/keycgi.exe?cmd=download&product=surgeftp
Titan FTP Server	South River Technologies	http://www.southrivertech.com/index.php?pg=./download/index&pgr=./purchase/index
Vermillion FTP Daemon	Arcane Software, Inc.	http://www.arcanesoft.com/
WS_FTP Server	Ipswitch	http://www.ipswitch.com/support/ws_ftp-server/patch-upgrades.asp
Web サーバ		
4D WebSTAR	4D	http://www.4d.com/products/downloads_4dws.html
AOLserver	AOLserver	http://aolserver.sourceforge.net/
Apache HTTP Server	Apache Foundation	http://www.apache.org/dist/httpd/
Commerce Server/400	iNet	http://www.inetmi.com/iseries/commerce/ptf.html
Jigsaw	W3C	http://www.w3.org/Jigsaw/
Microsoft Internet Information Services	Microsoft	http://www.microsoft.com/technet/security/prodtech/IIS.mspx
RaidenHTTPD	Raiden	http://www.raidenhttpd.com/en/download.html
Roxen WebServer	Roxen Internet Software	http://download.roxen.com/4.0/
Sambar Server	Sambar Technologies	http://www.sambar.com/download.htm
SimpleServer:WWW	AnalogX	http://www.analogx.com/contents/download/network/sswww.htm
Sun Java System Web Server	Sun	http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage
Tcl Web Server	Tcl Developer Exchange	http://www.tcl.tk/software/tclhttpd/
Zeus Web Server	Zeus Technology	http://support.zeus.com/doc/zws/v4/supported_versions.html

一般的なエンタープライズファイアウォール

製品系列	ベンダー	URL
BorderWare Firewall Server	BorderWare Technologies	http://www.borderware.com/support/
Cisco PIX	Cisco Systems	http://www.cisco.com/en/US/support/index.html
CyberGuard	CyberGuard Corporation	http://www.cyberguard.com/support/index.html?lang=de_EN
DX	Resilience Corporation	http://www.resilience.com/support/support.html
Firebox	WatchGuard Technologies, Inc.	http://www.watchguard.com/archive/service.asp
FireWall-1	Check Point Software Technologies	http://www.checkpoint.com/downloads/index.jsp
FortiGate	Fortinet	http://support.fortinet.com/
GB	Global Technology Associates	http://www.gta.com/support/upgrade/
Kerio Server Firewall	Kerio Technologies, Inc.	http://www.kerio.com/ksf_download.html
NetScreen	Juniper Networks, Inc.	http://www.juniper.net/customers/support/
Sidewinder	Secure Computing Corporation	http://www.securecomputing.com/index.cfm?skey=246
SonicWALL	SonicWALL	http://www.sonicwall.com/products/gav_ips_spyware.html
Sun Cobalt	Sun	http://sunsolve.sun.com/pub-cgi/show.pl?target=cobalt/index&nav=patchpage
Symantec Enterprise Firewall	Symantec Corporation	http://www.symantec.com/downloads/

一般的なエンタープライズネットワーク侵入検知および侵入防止システム

製品系列	ベンダー	URL
Attack Mitigator	Top Layer Networks	http://www.toplayer.com/content/support/index.jsp
Bro	Vern Paxson	http://bro-ids.org/download.html
Captus	Captus Networks	http://www.captusnetworks.com/info/support/index.html
Cisco IPS	Cisco Systems	http://www.cisco.com/en/US/support/index.html
Cyclops	e-Cop.net	http://www.e-cop.net/
DefensePro	Radware, Ltd.	http://www.radware.com/content/security/serviceinfo/default.asp
Dragon	Enterasys Networks, Inc.	https://dragon.enterasys.com/
eTrust Intrusion Detection	Computer Associates	http://www.my-etrust.com/Support/TechSupport.aspx
IntruShield	Network Associates	http://www.mcafee.com/us/downloads/default.asp
iPEnforcer	iPolicy Networks	http://www.ipolicynetworks.com/support/index.html
ManHunt	Symantec Corporation	http://www.symantec.com/techsupp/enterprise/select_product_updates_nojs.html
Mazu Enforcer	Mazu Networks, Inc.	https://supportcenteronline.com/ics/support/default.asp?deptID=735
NetDetector	Niksun	http://www.niksun.com/Support_Technical_Support.htm
Netscreen	Netscreen Technologies	http://www.juniper.net/customers/csc/software/
Proventia	Internet Security Systems	http://www.iss.net/support/
SecureNet	Intrusion Inc.	https://serviceweb.intrusion.com/
Sentivist	NFR Security	http://www.nfr.com/solutions/support.php
Snort	Sourcefire	http://www.snort.org/dl/
Sourcefire	Sourcefire	http://www.sourcefire.com/services/support.html
StealthWatch	Lancope	http://www.lancope.com/customers/

製品系列	ベンダー	URL
StoneGate	StoneSoft Corporation	http://www.stonesoft.com/support/
Strata Guard	StillSecure	http://www.stillsecure.com/strataguard/support/updates.php
UnityOne	TippingPoint Technologies	http://www.tippingpoint.com/support.html
V-Secure	V-Secure Technologies, Inc.	http://www.v-secure.com/support/packages_bundles.asp

一般的なエンタープライズウイルス対策およびスパイウェア対策ソフトウェア [41]

Web サイト	URL
Central Command Vexira AntiVirus	
Downloads	http://www.centralcommand.com/downloads.html
Latest Version Numbers	http://www.centralcommand.com/versions.html
Support	http://www.centralcommand.com/support.html
Computer Associates eTrust Antivirus	
Computer Associates Security Advisory	http://www3.ca.com/securityadvisor/
Computer Associates Support	http://www3.ca.com/support/
Computer Associates Virus Information Center	http://www3.ca.com/securityadvisor/virusinfo/default.aspx
F-Secure Anti-Virus	
F-Secure Radar	http://www.f-secure.com/products/radar/
F-Secure Security Information Center	http://www.f-secure.com/virus-info/
F-Secure Support	http://support.f-secure.com/enu/home/
Lavasoft Ad-Aware	
Download, Support, Upgrade Center	http://www.lavasoftusa.com/
Microsoft Windows AntiSpyware（Beta）	
Using Microsoft Windows AntiSpyware (Beta)	http://www.microsoft.com/athome/security/spyware/software/howto/default.mspx
Network Associates McAfee VirusScan	
Downloads	http://www.mcafee.com/us/downloads/default.asp
McAfee AVERT Alerts	http://vil.nai.com/vil/content/alert.htm
McAfee AVERT Virus Information Library	http://vil.nai.com/vil/default.asp
Sophos Anti-Virus	
Download Latest Virus Identity Files	http://www.sophos.com/downloads/ide/
Sophos Email Notification	http://www.sophos.com/virusinfo/notifications/
Sophos Virus Analyses	http://www.sophos.com/virusinfo/analyses/
Spybot-Search & Destroy	
Downloads	http://www.safer-networking.org/en/download/index.html
Support	http://www.safer-networking.org/en/support/index.html
Symantec AntiVirus	
Symantec Downloads	http://www.symantec.com/downloads/
Symantec Support	http://www.symantec.com/techsupp/
Symantec Security Response–Search and Latest Virus Threats Page	http://securityresponse.symantec.com/avcenter/vinfodb.html
Symantec Security Response–Alerting Offerings	http://securityresponse.symantec.com/avcenter/alerting_offerings.ht

[41] この表は、ウイルス対策およびスパイウェア対策ソフトウェアのうち、最も人気のあるものをいくつか示している。ほかの製品については、Virus Bulletin Web サイト（http://www.virusbtn.com/resources/links/index.xml?ven）の一覧を参照のこと。

Web サイト	URL
	ml
Trend Micro Anti-Spyware および VirusWall	
Support	http://kb.trendmicro.com/solutions/search/default.asp
Trend Micro Virus Encyclopedia Search	http://www.trendmicro.com/vinfo/virusencyclo/
Trend Micro Newsletters	http://www.trendmicro.com/subscriptions/default.asp

そのほかの一般的なセキュリティアプリケーション

製品系列	ベンダー	URL
スパム対策サーバ		
Anti-Spam SMTP Proxy（ASSP）Server	ASSP Server Project	http://sourceforge.net/project/showfiles.php?group_id=69172
BitDefender AntiSpam for Mail Servers	Softwin	http://www.bitdefender.com/site/Main/view/Server-Products-Updates.html
GFiMailEssentials	GFI Software	http://support.gfi.com/
Kaspersky Anti-Spam	Kaspersky	http://www.kaspersky.com/productupdates/
MailShield Server	Lyris Technologies	http://www.lyris.com/store/mailshield/server/upgrade.html?s=sdbr
McAfee SPAMkiller	Network Associates	http://www.mcafee.com/us/downloads/default.asp
Merak Instant Anti Spam	Merak	http://www.merakmailserver.com/Download/
MIMEsweeper	Clearswift	http://www.clearswift.com/support/msw/patch.aspx
NetIQ MailMarshal	NetIQ	http://www.netiq.com/support/default.asp
SPAMfighter	SPAMfighter	http://www.spamfighter.com/Tutorial_Update.asp
パーソナルファイアウォールおよびスイート		
BlackIce	Internet Security Systems	http://blackice.iss.net/update_center/
F-Secure Internet Security 2005	F-Secure	http://support.f-secure.com/enu/home/
Kaspersky Anti-Hacker	Kaspersky Labs	http://www.kaspersky.com/productupdates
Kerio Personal Firewall	Kerio Technologies	http://www.kerio.com/kpf_download.html
McAfee Personal Firewall Plus	Networks Associates Technology, Inc.	http://download.mcafee.com/us/upgradeCenter/?cid=11536
Norton Personal Firewall	Symantec	http://www.symantec.com/downloads/
Panda Platinum Internet Security	Panda Software	http://www.pandasoftware.com/download/
PC-cillin Internet Security	Trend Micro	http://www.trendmicro.com/download/product.asp?productid=32
Sygate Personal Firewall	Sygate	http://smb.sygate.com/download_buy.htm
Tiny Firewall	Tiny Software	http://www.tinysoftware.com/home/tiny2?s=5375286922906826215A1&&pg=content05&an=tf6_download&cat=cat_tf6
ZoneAlarm	Zone Labs	http://download.zonelabs.com/bin/free/information/zap/releaseHistory.html
VPN クライアント		
Cisco VPN Client	Cisco	http://www.cisco.com/public/sw-center/

製品系列	ベンダー	URL
NetScreen-Remote	Juniper	http://www.juniper.net/customers/support/
Nortel VPN Client	Nortel	http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=software&tranProduct=10621
ProSafe VPN Client	Netgear	http://kbserver.netgear.com/downloads_support.asp
SafeNet SoftRemote	CyberGuard	http://www.cyberguard.com/support/
VPN-1 SecuRemote, SecureClient	CheckPoint	http://www.checkpoint.com/downloads/index.html
無線 IDS／IPS		
AirDefense	AirDefense	http://www.airdefense.net/support/
AirMagnet	AirMagnet	http://www.airmagnet.com/support/index.htm
AiroPeek	WildPackets	http://www.wildpackets.com/support/downloads
AirPatrol	Cirond	http://www.cirond.com/support.php
BlueSecure	BlueSocket	http://www.bluesocket.com/products/intrusionprotection.html
Highwall	Highwall Technologies	http://www.highwalltech.com/support.cfm
Red-Detect	Red-M	http://www.red-m.com/Support/
RFprotect	Network Chemistry	http://www.networkchemistry.com/support/
SpectraGuard	AirTight Networks	http://www.airtightnetworks.net/support/support_overview.html

脆弱性管理の一般的なリソース

リソース名	URL
US-CERT National Cyber Alert System	http://www.us-cert.gov/cas/
US-CERT National Vulnerability Database	http://nvd.nist.gov/
US-CERT Vulnerability Notes Database	http://www.kb.cert.org/vuls/
Open Source Vulnerability Database	http://www.osvdb.org/
SecurityFocus Vulnerability Database	http://www.securityfocus.com/vulnerabilities

付録E—索引