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

Special Publication 800-45
第 2 版

電子メールのセキュリティに関するガイドライン

米国国立標準技術研究所による勧告

Miles Tracy
Wayne Jansen
Karen Scarfone
Jason Butterfield

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 800-45
第 2 版

電子メールのセキュリティに関するガイドライン

米国国立標準技術研究所による勧告

Miles Tracy, Wayne Jansen, Karen Scarfone, and Jason Butterfield

C O M P U T E R S E C U R I T Y

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

2007 年 2 月

米国商務省　長官

Carlos M. Gutierrez

技術管理局　技術担当商務次官

Robert C. Cresanti

米国国立標準技術研究所　所長

William Jeffrey

コンピュータシステム技術に関する報告書

米国国立標準技術研究所（NIST：National Institute of Standards and Technology、以下、NIST と称す。）の情報技術ラボラトリ（ITL：Information Technology Laboratory）は、国家の測定および標準に関する基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。ITL は、テスト、テスト技法、参照データの作成、コンセプト実証のための実装、技術的分析を行い、情報技術の開発と生産的利用の拡大に努めている。ITL の責務は、連邦政府のコンピュータシステムにおいて費用対効果の高いセキュリティと取り扱いに注意を要する非機密扱い情報のプライバシを確保するための、技術的、物理的、および管理的標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、コンピュータセキュリティにおける情報技術ラボラトリの調査、ガイドライン、普及活動と、産業界、政府機関および教育機関との共同活動について報告する。

米国国立標準技術研究所、Special Publication 800-45 Version 2
米国国立標準技術研究所、Special Publication 800-45 第 2 版、139 ページ（2007 年 2 月）

謝辞（第 2 版）

本書執筆陣である Wayne Jansen、Karen Scarfone（ともに NIST）、Miles Tracy（Federal Reserve Information Technology：連邦準備制度理事会情報技術局）および Jason Butterfield（Booz Allen Hamilton）は、この文書の草稿をレビューしてくれた各機関の同僚に感謝の意を表したい。特に、このバージョンのために調査、技術サポートおよび寄稿による協力をしてくれた Linda Antil、Rick Ayers、Bill Burr、Tim Grance および Tim Polk（NIST）に対して最大の謝辞を表すものである。また、パブリックコメント期間に意見を寄せてくれた方々、内部レビュープロセスに協力してくれた方々すべてに対しても同じく感謝する。

謝辞（初版）

本書執筆陣である Wayne Jansen（NIST）、Scott Bisker、Miles Tracy（ともに BAH：Booz Allen Hamilton）は、この文書の草稿をレビューしてくれた両機関の同僚に感謝の意を表したい。特に、この文書のために調査、技術サポートおよび寄稿による協力をしてくれた John Wack、Murugiah Souppaya、Tim Grance（NIST）、Steve Allison、Alexis Feringa、Jonathan Holleran、Kevin Kuhlkin および Mark McLarnon（BAH）に対して最大の謝辞を表すものである。また、パブリックコメント期間に意見を寄せてくれた方々、内部レビュープロセスに協力してくれた方々すべてに対しても同じく感謝する。

目次

付録

図表一覧

（本ページは意図的に白紙のままとする）

要旨

電子メール（E メール）は、ビジネス情報をインターネット上（およびその他のコンピュータネットワーク上）で交換する手段として最も広く使用されているシステムと考えられる。電子メールのプロセスは、最も基本的なレベルにおいて 2 つの主要コンポーネントに分けることができる。すなわち、(1)電子メールを配信、転送、および保管するためのメールサーバと、(2)ユーザに対するインタフェースとなり、ユーザによる電子メール閲覧、作成、送信、および保管を可能にするメールクライアントの 2 つである。この文書は、メールサーバおよびメールクライアントにおけるセキュリティ関連の問題（Web ベースのメールアクセスを含む）に主眼を置くものである。

メールサーバと、メールクライアントの動作するユーザワークステーションは、しばしば攻撃の対象となる。電子メールの基礎となっているコンピューティングとネットワーキングの技術は、あらゆる場所に普及しており、多くの人がその内容を熟知しているが、それは攻撃者にも、セキュリティの弱点を利用した攻撃方法を開発する手段が与えられているということである。メールサーバはまた、信頼のおけない第三者との通信を多少なりとも行う必要があるため、公開 Web サーバと同様、攻撃の対象となりうる。さらに、メールクライアントは、コンピュータにマルウェアを侵入させたり、そのコードを別のコンピュータに伝染させたりするための効果的な手段になり得ることから、攻撃の対象となってきた。したがって、メールサーバ、メールクライアント、およびそれらを支えるネットワーク基盤は、保護する必要がある。電子メールのセキュリティに関する問題の例としては次のようなものがある。

- 電子メールを外部と交換する場合（これはほとんどの組織において必須であろう）、電子メールは当該組織のネットワーク境界部にある防御を通過することが許可される。そのため、基本的なレベルでは、ウイルスやその他各種のマルウェアが電子メールを介して組織内に広がる可能性がある。攻撃者の手口はしだいに高度化しており、組織内部のネットワークにあるユーザワークステーションへの侵入を試みるゼロデイ攻撃を送り込む手段などとして電子メールが利用されている。

- 人間同士のコミュニケーション媒体であるという電子メールの性質から、ソーシャルエンジニアリングの手段として利用される可能性がある。電子メールを利用して、攻撃者が組織内のユーザから情報を収集したり、さらなる攻撃につながるような行動をユーザにとらせたりすることがある。

- メールサーバアプリケーションの不備が、そのアプリケーションが稼働しているサーバコンピュータや接続されているネットワークへの侵入手段として利用される可能性がある。これにより、外部からのアクセスを想定していないファイルやフォルダがアクセスされたり、メールサーバ上でのコマンド実行またはソフトウェアのインストールなどといった無許可のアクセスが行われたりすることがある。

- メールサーバやそのネットワーク基盤に対するサービス運用妨害（DoS）攻撃が行われ、正当なユーザによるメールサーバの利用が困難または不可能になる可能性がある。

- メールサーバに置かれた機密情報が、権限のない個人によって読み取られたり、不正な方法で改ざんされたりする可能性がある。

- メールサーバとクライアントの間で暗号化せずに送受信される機密情報が傍受される可能性がある。広く普及しているいずれの電子メール通信の標準規格においても、ユーザ名、パスワード、電子メールメッセージはデフォルトでは暗号化されずに送信される。

- 電子メールメッセージ内の情報が、送信者と受信者の間の経路上のあるポイントで改ざんされる可能性がある。

- 悪意を持つ者が、メールサーバへの攻撃に成功し、当該組織内ネットワーク上の別の場所にあるリソースに不正にアクセスする可能性がある。たとえば、攻撃者はメールサーバに侵入してユーザのパスワードを入手することにより、組織のネットワーク上にある他のホストにアクセスできるようになることがある。
- 悪意を持つ者が、攻撃に成功したメールサーバホストを踏み台にして、外部の組織への攻撃を行う可能性がある。
- メールサーバの設定が適切でない場合、組織のメールサーバが、悪意を持つ者によるSPAMメールの送信に利用される可能性がある。
- 不適切な情報、専有情報、そのほかの秘密情報を、ユーザが電子メールで送信する可能性がある。場合によっては、これにより組織が法的措置の対象にされることもある。

この文書は、組織による、セキュリティが確保されたメールサーバおよびメールクライアントのインストール、設定、および保守を支援することを目的としている。より具体的には、次の各項目について詳細に述べる。

- 電子メールに関する標準と、それらのセキュリティ上の考慮事項
- 電子メールの署名および暗号化に関する標準
- メールサーバの計画およびマネジメント
- メールサーバが稼働するオペレーティングシステムのセキュリティ対策
- メールサーバアプリケーションのセキュリティ
- 電子メールのコンテンツフィルタリング
- ネットワーク保護メカニズム（ファイアウォール、ルータ、スイッチなど）並びに侵入検知および侵入防止システムの導入および設定にかかわる電子メール特有の考慮事項
- メールクライアントのセキュリティ対策
- セキュリティに配慮したメールサーバ管理（バックアップ、セキュリティテスト、ログレビューを含む）

連邦政府の省庁および機関に対し、セキュリティが確保されたメールサーバの保守に関して次に示す主要ガイドラインを推奨する。

メールサーバの導入にあたっては、そのセキュリティにかかわる側面について注意深く計画し、対策を実施すること。

導入および実装をいったん行った後でセキュリティ対策を実施するのは、先にセキュリティ対策を実施する場合よりもはるかに困難であるため、セキュリティは最初の計画段階で検討するべきである。組織は、詳細かつ適切な設計の導入計画を策定し使用した場合のほうが、コンピュータの設定について、より適切かつ一貫した判断を下す可能性が高い。そのような計画を策定することにより、メールサーバ管理者が、利便性、パフォーマンス、リスクの 3 要素間でトレードオフの選択を迫られた場合に、意思決定の助けとなるであろう。

組織が、メールサーバおよびそれを支える基盤の導入と運用の両段階にかかわる人的リソースの要件を考慮していない場合がしばしば見受けられる。導入計画には、次の事項を盛り込むべきである。

- 必要とされる人員の種類（システムおよびメールサーバ管理者、ネットワーク管理者、情報システムセキュリティ責任者など）
- 担当人員に必要な技能および訓練
- 人員の確保

セキュリティが確保されたメールサーバの保守・運用にあたっては、適切なセキュリティマネジメント活動および管理策を実施すること。

適切なセキュリティマネジメント活動は、セキュリティ保護されたメールサーバの運用および保守にとって不可欠である。セキュリティ活動には、組織の情報システム資産の特定および、情報システムリソースの機密性、完全性、可用性の確保に役立つポリシー、標準、手続き、ガイドラインの策定、文書化、実施が含まれる。

メールサーバおよびそれを支えるネットワーク基盤のセキュリティを確保するために、次の活動を実践すべきである。

- 組織全体を対象とする情報システムセキュリティポリシー
- 設定および変更の制御とマネジメント
- リスクの評価とマネジメント
- 情報システムセキュリティポリシーを満たす、標準化されたソフトウェア設定
- セキュリティに関する啓蒙および訓練
- 緊急時対応計画、運用継続計画、および災害復旧計画
- 承認および運用認可

メールサーバのオペレーティングシステムの導入、設定および管理は、組織のセキュリティ要件を確実に満たす方法で行うこと。

メールサーバのセキュリティを保護するための第 1 歩は、メールサーバが稼働するオペレーティングシステムのセキュリティを保護することである。一般に利用可能なメールサーバのほとんどは、汎用のオペレーティングシステム上で動作する。セキュリティに関する問題の多くは、メールサーバのオペレーティングシステムを適切に設定すれば避けることができる。製造元によって設定されるハードウェアおよびソフトウェアのデフォルト設定は一般に、セキュリティを犠牲にして特長や機能、利便性を強調するものになっていることが多い。製造元では、個別の組織におけるセキュリティニーズを把握できないため、メールサーバ管理者が各自で組織のセキュリティ要件に応じて新規サーバを設定したり、要件の変化に応じて既存サーバの設定を変更したりする必要がある。管理者は、セキュリティ設定のガイドやチェックリストを使用することにより、システムのセキュリティを一貫性をもって効率よく確保することができる。オペレーティングシステムのセキュリティを確保する作業には、一般に次の手順が含まれる。

- オペレーティングシステムへのパッチの適用と更新

■ 不要なサービスおよびアプリケーションの削除または無効化

■ オペレーティングシステムのユーザ認証の設定

■ リソース制御の設定

■ 追加的なセキュリティ管理策のインストールと設定（必要に応じて）

■ オペレーティングシステムに対するセキュリティテストの実施

メールサーバアプリケーションの導入、設定および管理は、組織のセキュリティ要件を確実に満たす方法で行うこと。

メールサーバアプリケーションのインストールおよび設定におけるセキュリティ上の推奨事項は、前述のオペレーティングシステムに関する事項と多くの面で共通である。ここでも、基本的な考え方として、メールサーバの必要最小限のサービスをインストールし、パッチや更新を通じて既知の脆弱性をすべて排除することが重要である。不要なアプリケーション、サービス、またはスクリプトがインストールプログラムによってインストールされた場合は、インストールプロセスの完了後、それらを直ちに削除すべきである。メールサーバアプリケーションのセキュリティを確保する作業には、一般に次のような手順が含まれる。

■ メールサーバアプリケーションへのパッチの適用と更新

■ 不要なサービス、アプリケーション、サンプルコンテンツの削除または無効化

■ メールサーバのユーザ認証およびアクセス制御の設定

■ メールサーバのリソース制御の設定

■ メールサーバアプリケーションに対するセキュリティテストの実施

ユーザ認証および電子メールデータを保護するために、暗号技術の実装を検討すること。

標準の電子メールプロトコルのほとんどでは、デフォルトでは、ユーザ認証が暗号化されず、また、電子メールデータが平文（暗号化なし）で送信される。データが平文で送信されると、攻撃者によってユーザアカウントが容易に乗っ取られたり、暗号化されていない電子メールが傍受され改ざんされたりする可能性がある。ほどんどの組織においては、電子メールデータ自体を暗号化しないにしても、最低限ユーザ認証セッションを暗号化するべきである。ユーザ認証の暗号化は、現在では標準および非標準メールボックスプロトコルのほとんどでサポートされている。

暗号化および署名された電子メールデータに関しては、より複雑な問題が伴う。電子メールの暗号化および署名によって、組織のネットワーク基盤に対する負荷が増大したり、マルウェアの検出処理や電子メールのコンテンツフィルタリングが複雑化したりする可能性がある。また、管理作業の負担が大幅に増大することが多い。とはいえ、多くの組織にとっては、そうしたコストを上回るメリットがあると考えられる。

メールサーバを保護するために、ネットワーク基盤を活用すること。

メールサーバのセキュリティを確保するうえで、メールサーバを支えるネットワーク基盤（ファイアウォール、ルータ、侵入検知システムなど）の役割はきわめて重要である。ほとんどの設定においては、インターネットとメールサーバの間で、ネットワーク基盤が最初の防衛線となるからである。ただし、ネットワークの設計だけでメールサーバを保護することはできない。メールサーバに対する攻撃が

頻繁に行われ、その内容も高度化かつ多様化している現状では、さまざまな防御メカニズムによる多重構造のセキュリティ対策が必要と考えられる。

メールクライアントの導入、設定および使用は、組織のセキュリティ要件を確実に満たす方法で適切に行うこと。

電子メールのクライアント側には、多くの面でメールサーバよりも大きなセキュリティ上のリスクがある。適切なレベルのセキュリティをメールクライアントにおいて確保するには、数多くの問題を注意深く検討し、対策を講じる必要がある。メールクライアントアプリケーションのインストール、設定および使用におけるセキュリティを保護する作業には、一般に次のような手順が含まれる。

- メールクライアントアプリケーションへのパッチの適用と更新
- メールクライアントのセキュリティ機能の設定（メッセージ自動表示の無効化、スパム対策およびフィッシング対策機能の有効化など）
- メールボックスの認証およびアクセスの設定
- クライアントホストのオペレーティングシステムのセキュリティ保護

メールサーバのセキュリティ維持は継続的なプロセスである。

メールサーバのセキュリティ確保を維持するには、組織による不断の努力、リソースおよび警戒が必要である。セキュリティに配慮してメールサーバを日々管理していく作業は、メールサーバのセキュリティにとっては不可欠の要素である。メールサーバのセキュリティを維持する作業には、一般に次のような手順が含まれる。

- ログファイルの設定、保護、分析
- データの頻繁なバックアップ
- マルウェア（ウイルス、ワーム、トロイの木馬など）からの防御
- セキュリティ侵害から復旧するための手順の策定および遵守
- 適切なタイミングでのパッチのテストおよび適用
- 定期的なセキュリティテスト

（本ページは意図的に白紙のままとする）

1. はじめに

1.1 作成機関

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

このガイドラインは、連邦政府機関による使用を目的として用意されたが、非政府組織が自己責任において使用することもできる。その場合は出自を明らかにすることが望ましいが、著作権の制約はない（翻訳者注:著作権に関するこの記述は、SP800-45 第 2 版の英語の原文のことを言っており、日本語へ翻訳した本書の著作権は、独立行政法人情報処理推進機構および NRI セキュアテクノロジーズ株式会社に帰属する）。

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

1.2 目的と範囲

『*電子メールのセキュリティに関するガイドライン（Guidelines on Electronic Mail Security）*』の目的は、公開および非公開のネットワークにおける電子メールシステムの設計、実装および運用に関して、セキュリティ上の推奨実践事項を説明することである。この文書は、連邦政府省庁および政府機関のための推奨事項のガイダンスとして作成されたものであるが、民間組織が自己責任において使用してもよい。

メールサーバは、しばしば攻撃の対象となる。また、さまざまな種類の電子メールコンテンツおよび添付ファイルは、メールクライアントを介してネットワークにウイルスその他のマルウェアを侵入させる有用な手段にもなることが明らかとなっている。ユーザのワークステーションに存在する脆弱性を利用した攻撃を送り込む手段として、あるいは、ユーザをだます各種ソーシャルエンジニアリングの手口の媒体として、電子メールは非常に幅広く使われている。そうした攻撃にさらされると、電子メールクライアントが安全に設定されていても、しばしばユーザのワークステーションのセキュリティが侵害されたり、秘密情報が漏えいしたりする結果になる。既存のメールシステムまたは今後導入するメールシステムのセキュリティ強化に関心を持つ組織にとって、この文書は、電子メール関連のセキュリティインシデントの発生件数および頻度を低減するために有用である。この文書で述べる事項は、あらゆるシステムに該当する一般的な原則である。

メールサーバのセキュリティに関連する次の事項については、このガイダンスの対象としない。

- そのほかの種類のネットワークサーバのセキュリティ確保
- メールサーバの保護に使用されるファイアウォールおよびルータに関して、セクション 6.2.1 の基本的な内容を超える事項
- 大量のトラフィックを処理する複数ホスト構成のメールサーバにおける特殊な考慮事項
- syslog ホスト、ファイルサーバなど、メールサーバを支えるバックエンドサーバにおけるセキュリティ確保
- X.400 標準メッセージングプロトコルに関するセキュリティ

1.3 対象読者と前提条件

この文書は、技術的な性格を持つものだが、扱うトピックについて、読者の理解を助けるための予備知識も提供する。この文書は、次のような読者を対象として想定している。

- メールクライアントの設定および電子メールへのアクセスを行うユーザ
- メールシステムの設計および実装を行うシステムエンジニアおよびアーキテクト
- メールシステムの管理およびアップグレードを行うシステム管理者
- システムのライフサイクルのすべての段階について、十分なセキュリティ対策が確実に考慮されるようにするプログラムマネージャおよび情報技術（IT）セキュリティ責任者

この文書で推奨する実践事項は、電子メールおよびそのほかの既知のセキュリティ問題に伴うリスクの低減を助けることを目的とした各種の対策であり、付録 E に示す他の NIST ガイドラインに示されている実践事項が実施されていることを前提に記述されている。

1.4 文書の構成

この文書の残りの部分は、次の 8 つの主要セクションで構成されている。

- セクション 2 では、電子メールに関係する標準および予備知識を提供する。
- セクション 3 では、署名および暗号化による電子メールメッセージの保護に関する情報を提供する。
- セクション 4 では、メールサーバの計画とマネジメントについて論じる。
- セクション 5 では、メールサーバが稼働するオペレーティングシステムのセキュリティ確保の概要を示す。
- セクション 6 では、メールサーバアプリケーションのセキュリティ確保、サーバを通過するメッセージの保護、およびメールボックスへのアクセスのセキュリティ確保について論じる。
- セクション 7 では、メールサーバを支えるネットワーク基盤を利用したメールサーバの保護を扱う。
- セクション 8 では、メールクライアントのセキュリティに関する情報を提供する。
- セクション 9 では、セキュリティに配慮してメールサーバを日々管理していく作業の基本について論じる。

巻末にはいくつかの付録と参考資料を記載している。

- 付録 A では、この文書で使用している用語を定義している。
- 付録 B には、関係する RFC（Request for Comments）文書の一覧を示す。
- 付録 C には、この文書で使用している参考文献の一覧を示す。
- 付録 D では、電子メールのセキュリティ関連ツールおよびアプリケーションを紹介する。
- 付録 E には、オンラインで利用できる電子メールセキュリティにかかわる情報源の一覧を示す。
- 付録 F に、メールサーバおよびクライアントのセキュリティチェックリストを示す。
- 付録 G には、この文書で使用している頭字語の一覧を示す。
- 付録 H は、この文書の索引である。

2. 背景と標準

2007 年 1 月時点で、全世界のインターネットユーザ人口は 10 億を超えたと推計されている[1]。それらユーザの大半が、1 つないし複数のメールシステム上に電子メール（E メール）アカウントを保有している。1971 年に米国防総省（DoD：Department of Defense）の研究者 Ray Tomlinson が最初の ARPANET 電子メールを自分自身に送信して以来、電子メールは目覚ましい普及を遂げた。インターネットの前身である ARPANET は、地理上のさまざまな位置にあるコンピューティングリソースを透過的に接続する通信プロトコル群の開発を目的とする、米国国防総省高等研究計画局（ARPA：Advanced Research Project Agency）のプロジェクトであった。ARPANET システム上には、メッセージングアプリケーションがすでに存在していたが、それはローカルシステムアカウントのユーザに対してのみメッセージを送信できるものであった。Tomlinson はこれに変更を加え、他の ARPANET 接続されたシステム上のユーザにもメッセージを送信できるようにしたのである。この Tomlinson による改良がほかの研究者らの間に広まると、電子メールは、ARPANET において最もよく使用されるアプリケーションとなった。

ARPANET がインターネットへと発展しても、電子メールは、個人ユーザおよびビジネスユーザに最もよく使用されるアプリケーションの 1 つであり続けた。当初の ARPANET は信頼のおけるユーザから成る小規模のコミュニティであったため、セキュリティの必要性がほとんどなかった。インターネットを使う人の数が増えるにつれて、セキュリティの必要性は大幅に高まったが、初期に成立した標準およびその実装においてセキュリティが重視されなかったことが災いし、電子メールシステムは、必要なセキュリティを備えていなかった。そうした標準との互換性を保つことが、現在、電子メールのセキュリティにとって大きな課題になっている。

2.1 背景

電子メールのメッセージがどのように作成、配信、および格納されるかを理解することは、電子メールのセキュリティを理解するためには有用である。ほとんどの電子メールユーザにとって、いったん作成および送信したメッセージは、送信元のコンピュータを離れて、宛先の受信ボックスへと自動的に届くものである。電子メールの扱いと配信は一見簡単なことのようであるが、実際は最終的な目的地に到達するまでにいくつもの中継地点で処理や仕分けが行われるため、物理的な郵便の仕組みと同様の複雑さを伴う可能性がある。

プロセスは、メッセージの作成から始まる。最も基本的なメールクライアントは一般に、ユーザに対して件名、メッセージ内容、および宛先の入力を求める。ユーザがこれらのフィールドに情報を入力し、メッセージを送信すると、そのメッセージは RFC（Request for Comments）2822『Internet Message Format（インターネットメッセージ形式）』に規定されている特定の標準形式に変換される。最も基本的なレベルでメッセージを構成する 2 つのセクションは、ヘッダおよび本文である。ヘッダセクションには、作成日、送信者、宛先、配信経路、件名、形式情報など、メッセージに関する重要情報が含まれる。メッセージ本文には、当該メッセージの実際の内容が含まれる[2]。

メッセージは、RFC 2822 形式に変換されると送信可能となる。メールクライアント、すなわちメールユーザエージェント（MUA：Mail User Agent）は、何らかのネットワーク接続を使用して、メールサー

---

1 World Internet Usage and Population Statistics（世界インターネット利用状況・人口統計、http://www.internetworldstats.com/stats.htm）による。

2 メッセージヘッダの詳細については、RFC 2822 を参照のこと。付録 B に、電子メールに関係する RFC の網羅的な一覧を示す。一覧には、メールに関係する多数の RFC の参照先 URL も示す。また、標準とみなされている RFC、参考情報として扱われている RFC、標準化の過程にある RFC、および現状におけるベストプラクティス（BCP：Best Current Practice）である RFC をそれぞれ示す。

バ上で稼働するメール転送エージェント（MTA：Mail Transfer Agent）に接続する。通信を開始したあと、メールクライアントは、送信者の識別情報をサーバに提示する。次に、クライアントはメールサーバのコマンドを使用して、宛先が誰であるかをサーバに伝える。宛先の一覧はメッセージにも含まれているが、メールサーバでは、メッセージ内のこの情報は調べない。クライアントは、宛先の一覧全体をサーバへ送信し終えて初めて、メッセージ内容を送信する。この時点より、メッセージの配信は当該メールサーバの制御下に置かれる。

メールサーバがメッセージの処理を開始したあと、宛先サーバの特定、接続の確立、およびメッセージの伝送といったことが行われる。送信元のメールサーバでは、ドメインネームシステム（DNS：Domain Name System）サービスを使用して宛先のメールサーバ（場合によっては複数）を特定する。続いて、サーバは宛先メールサーバへの接続を開き、送信元クライアントと同様のプロセスを使用してメッセージを送信する。この時点で、次の 2 つのいずれかが起きる。送信者と受信者のメールボックスが同じメールサーバ上にある場合、メッセージはローカル配信エージェント（LDA）によって配信される。送信者と受信者のメールボックスが異なるメールサーバ上にある場合、メッセージが受信者のメールボックスに到達するまで、MTA から MTA へと送信のプロセスが繰り返される。

メッセージが LDA の制御下にあるとき、多くのことが起こりうる。設定に応じて、LDA はメッセージを配信したり、あらかじめ定義されたメッセージフィルタに基づいて配信の前にメッセージを処理したりする場合がある（フィルタ処理は、複数のメッセージプロパティに基づいて行われる可能性がある。詳細については 5.2.2 項を参照）。配信されたメッセージは、受信者が MUA を使用してメッセージを対象に何らかのアクション（読み取り、削除など）を実行するまで、受信者のメールボックスに置かれる。図 2.1 に、ここまで説明したメールに関わるさまざまな構成要素を経由するメッセージの流れを示す。1 通の電子メールが送信されるプロセスの概略はこのようになっている。

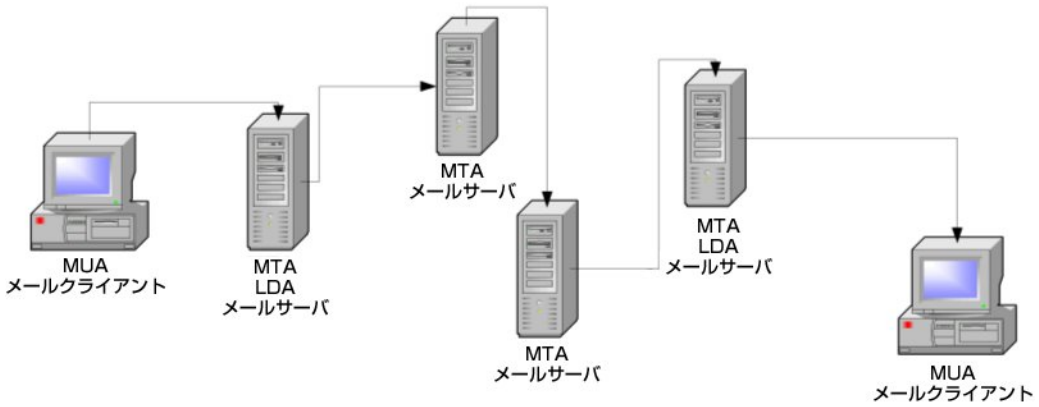

図 2.1：メッセージの流れの例

2.2 MIME(Multipurpose Internet Mail Extensions: 多目的インターネットメール拡張)

RFC 2822 は、テキスト形式のメッセージの伝送に関する標準を定めてはいるが、添付（ワードプロセッサ文書や写真画像など）を含んだメッセージについては規定していない。そこで、RFC 2822 メッセージのヘッダを活用する MIME（Multipurpose Internet Mail Extensions）を使用することで、リッチメッセージコンテンツ構造の記述に関する可能性がほぼ無限に広がることになる。MIME においては、関連付けられたデータのネイティブ表現やエンコーディングを指定する際に、慣例的に、「コンテンツタイプ／サブタイプ」ペアが使用されている。コンテンツタイプの例を次に示す。

■ Audio — オーディオまたは音声データの伝送用

- Application — アプリケーションデータまたはバイナリデータの伝送用
- Image — 静止画像データの伝送用
- Message — 別のメールメッセージのカプセル化用
- Multipart — 複数のメッセージ本文パート（場合によっては異なる種類のデータからなる）を組み合わせて単一メッセージを構成する際に使用
- Text — テキスト情報の表現用。標準化された形式で、多数の文字セットおよび書式付テキスト記述言語を指定可能
- Video — ビデオ（動画像）データの伝送用。コンポジットビデオデータ形式の場合は、オーディオを含むこともある

現行の MIME 標準には、RFC 2045、RFC 2046、RFC 2047、RFC 4289（RFC 2048 からの置き換え）、および RFC 2049 の 5 パートが含まれる（付録 B を参照）。これらの RFC は順に、メッセージ本文の形式、メディアタイプ、非 ASCII（non-American Standard Code for Information Interchange）メッセージヘッダ拡張、登録手続き、および適合基準に関するものである。この付加機能によって、メッセージへのファイル添付やインライン HTML（HyperText Markup Language）などの電子メール機能が実現可能となった。MIME 拡張はバイナリメッセージ内容に対応しているが、そうした内容は、バイナリデータのテキスト表現形式である Base64 エンコーディングを使用して RFC 2822 メッセージ内に組み込まれる[3]。

2.3 メールの伝送に関する標準

さまざまなメールアプリケーション間の信頼性と相互運用性を確保するために、メール伝送の各種標準が確立された。最も単純なシナリオでは、電子メールメッセージはローカルユーザから別のローカルユーザへと送信される。この場合、LDA がメッセージを適切なメールボックスに置く処理を担当する。ローカルでない宛先に送信されるメッセージの場合は、ローカルメールサーバからリモートメールサーバへメッセージを送信するために、MTA が必要となる。伝送に関与するシステムの種類によって、使用される MTA は異なる場合がある。その結果、それぞれが特定のメッセージ転送プロトコルの異なる実装をサポートしていたり、互いに異なる転送プロトコルをサポートしていたりする可能性がある。

最も一般的な MTA 転送プロトコルは、SMTP（Simple Mail Transfer Protocol：簡易メール転送プロトコル）である。SMTP は、インターネットにおける電子メールメッセージ送信の事実上の標準となっており、したがって、どのインターネットメッセージングシステムも、他の電子メールメッセージングアプリケーションと通信を行うには SMTP をサポートする必要がある。似た種類のメッセージングシステム同士で、またはクラスタ化されたメッセージングシステムのあいだで、異なる MTA 転送プロトコルを使用するメッセージングシステムも存在する。ほとんどの場合、そうした MTA は非標準の技術によるものであり、特定のシステムでしか動作しない。2.3.1 から 2.3.2 項では SMTP および SMTP 拡張に関する背景情報について述べ、2.3.3 項では非標準の MTA について述べる。

[3] Base64 エンコーディングは、当初は、Privacy Enhanced Mail（PEM：プライバシ強化メール）に関する RFC 1421 から派生したものである。

2.3.1 SMTP(Simple Mail Transfer Protocol:簡易メール転送プロトコル)

SMTP は、南カリフォルニア大学の Jon Postel によって 1982 年 8 月に開発された。RFC 821『Simple Mail Transfer Protocol』によれば、「SMTP は、より信頼性と効率性の高いメッセージ伝送の手段を確保するために開発された」ものである。最も基本的なレベルにおいては、SMTP は電子メールメッセージ配信のための通信プロトコルを定義する必要最小限の言語である。図 2.2 に、RFC 2821『Simple Mail Transfer Protocol』(従来の RFC821 からの置き換え)に定義されている SMTP コマンドおよびそれらの構文を示す。

HELO <ドメイン>	(Hello)<ドメイン>で指定したサーバに接続する
MAIL FROM:<逆順パス> [メールパラメータ]	送信者識別情報を<逆順パス>で指定してサーバに伝達する
RCPT TO:<正順パス> [宛先パラメータ]	(Recipient)意図する受信者の識別情報を <正順パス>で指定してサーバに伝達する
DATA	メッセージ本文をサーバに伝達する
RSET	(Reset)サーバ接続をリセットする
VRFY <文字列>	(Verify)ユーザが識別されたことの確認を受信側に求める
EXPN <文字列>	(Expand)メーリングリストが識別されたことの確認を受信側に求める
HELP [<文字列>]	ヘルプ情報を取得する
NOOP [<文字列>]	(No operation)何も操作を実行しないという意味だが、送信側がまだ接続されていることを示す(つまり、「生きている」ことを示す)
QUIT	サーバ接続を閉じる

図 2.2: SMTP コマンド

ユーザが電子メールを送信すると、クライアントが SMTP サーバにアクセスし、SMTP 言語による「対話」を開始する。多くの場合、MUA はメールクライアントアプリケーション(Outlook、Eudora など)の一部である。利用可能な MUA がない場合は、SMTP サービスに接続した Telnet クライアントを使用して電子メールメッセージを送信することも可能である。図 2.3 は、Telnet を使用した SMTP 対話の例である。太字部分が、このセッションにおいてユーザの入力した telnet および SMTP コマンドである。手動による SMTP Telnet セッションの間に HELP コマンドを使用して、当該サーバ上でどの SMTP コマンドが有効になっているかを知ることができる。

```
telnet mail.nowhere.com 25
Connected to mail.nowhere.com.
Escape character is '^]'.
220 test.mail.com SMTP Service (Sample Mail Server String)
HELO
250 test.mail.com
MAIL FROM: jdoe@nowhere.com
250 Sender <jdoe@nowhere.com> Ok
RCPT TO: jsmith@somewhere.com
250 Recipient <jsmith@somwhere.com> Ok
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
Hello World!
.
250 Message received: GM1BAR00.F4M
QUIT
221 mail.nowhere.com SMTP server closing connection.
Connection closed by foreign host.
```

図 2.3: SMTP 対話の例

2.3.2 SMTP(Simple Mail Transfer Protocol: 簡易メール転送プロトコル)拡張

電子メールユーザ数の増加に伴い、メールクライアントおよび SMTP サーバに対する機能追加が検討されるようになった。SMTP サーバでこの追加機能をサポートするのために、SMTP には拡張が施され、SMTP サービス拡張の概念が、1993 年、RFC 1425 によって導入された。その後、RFC 1425 に代わるものとして 1994 年には RFC 1651、1995 年には RFC 1869、さらに、2001 年には RFC 2821 が発行された。これらの RFC は、SMTP フレームワークに次の 3 つの要素を加えるものである。

- 新しい SMTP コマンド群(RFC 1425)
- SMTP サービス拡張のためのレジストリ(RFC 1651)
- SMTP MAIL FROM および RCPT TO コマンドの追加パラメータ(RFC 1869)

従来の SMTP サーバとの互換性を保つために、サーバが拡張をサポートしているかどうかをメールクライアントアプリケーションから確認する方法が必要となり、これは「拡張 Hello」(EHLO)コマンドによって実現された。メールクライアントは、サーバに接続する際に、EHLO コマンドを発行することができる。サーバが SMTP 拡張をサポートしていれば、これに対して、成功の応答およびサポートされる拡張の一覧が返される。サーバが SMTP 拡張をサポートしていなければ、コマンド失敗の応答が返され、MUA は従来の HELO コマンドの使用を促されることになる。SMTP の拡張、すなわち拡張 SMTP(ESMTP:Extended SMTP)をサポートするサーバーでは、多くの場合、応答のバナー内に ESMTP と表示される[4]。図 2.4 は、ESMTP サーバに対して EHLO コマンドを使用したトランザクションからの抜粋である。

```
telnet mail.nowhere.com 25
Connected to mail.nowhere.com.
Escape character is '^]'.
220 test.mail.com ESMTP Service (Sample Mail Server String)
EHLO
250 test.mail.com says hello
250-HELP
250-EXPN
250 SIZE 20971520
…
```

図 2.4: ESMTP 対話の例

図 2.4 に示すサンプルサーバの場合、サポートしている拡張は SIZE の 1 つだけであるが、さまざまな SMTP サーバで多数の拡張がサポートされている。表 2.1 に、いくつかの一般的な SMTP 拡張および関連する RFC の一覧を示す。特に RFC 2554 では、ユーザの識別と認証に関する新しいコマンドおよびプロトコルを規定している。ほとんどのメールサーバは、デフォルト設定では認証付きリレーが有効になっていないことが多い。

[4] サーバ上で稼働するアプリケーションサービス(電子メール、Web、FTP など)の多くは、クライアントの要求に対する応答として何らかのバナーを表示する。このバナーは、サーバに関する情報(アプリケーションおよびオペレーティングシステムの種類やバージョンなど)を含んだテキストメッセージである。これは攻撃者にとって有用な情報であるため、後述するとおり変更するべきである。ほとんどのメールクライアントは、エンドユーザに対してバナーを表示しない。

表 2.1：SMTP 拡張

SMTP 拡張	関連 RFC
SMTP Service Extension for Authentication（認証）	2554
SMTP Service Extension for Command Pipelining（コマンドパイプライン処理）	2920
SMTP Service Extension for Delivery Status Notifications（DSNs）（配信ステータス通知）	3461
SMTP Service Extension for Message Size Declaration（メッセージサイズ宣言）	1870
SMTP Service Extension for Message Tracking（メッセージ追跡）	3885
SMTP Service Extension for Remote Message Queue Starting（リモートメッセージキュー開始）	1985
SMTP Service Extension for Returning Enhanced Error Codes（拡張エラーコード返信）	2034
SMTP Service Extension for Secure SMTP over Transport Layer Security（TLS：Transport Layer Security（トランスポート層セキュリティ）により保護された SMTP）	3207
SMTP Service Extensions for Transmission of Large and Binary MIME Messages（巨大なバイナリ MIME メッセージの伝送）	3030

2.3.3 非標準のメール伝送

前述のように、一部のメッセージングシステムでは、SMTP と ESMTP のいずれもサポートしない MTA を使用している。そうした種類の MTA は、閉じたメッセージング環境内で動作するように設計されている。大規模な政府機関、学術機関、および民間組織の多くが、このような MTA を使用している。しかし、これらの組織は、外部のメッセージングシステムとの通信には、SMTP または ESMTP に対応した MTA を利用している。非標準プロトコルを使用するメッセージングシステムの例としては、Lotus Notes および Microsoft Exchange の MTA などがある[5]。独自のメッセージ転送プロトコルのみサポートする MTA を使用することのメリットとデメリットについては、この文書では扱わない。

2.4 クライアントアクセスに関する標準

メッセージが LDA によって配信されたあとは、ユーザがメールサーバにアクセスしてメッセージを取得する必要がある。メールサーバへのアクセスおよび電子メールメッセージの取得には、メールクライアント（MUA）を使用する。ユーザが自身のメールボックスにアクセスする方法は、最も単純な直接アクセスをはじめいくつか存在する。

メッセージングシステムとして最も単純なシナリオと考えられるのは、すべてのユーザが自身のメールボックスに直接アクセスできるシナリオである（Unix オペレーティングシステムで動作するホストにおいては一般的）。システム上に存在する各アカウントに対応するメールボックスが、当該ユーザのホームディレクトリに存在する。メッセージが届くと、ユーザは *mail* または *pine* などコマンドライン型のメールプログラムを使用してメールボックスに直接アクセスできる。この方法は単純明快ではあるが、メールサーバにアクセスしてメッセージを受信するには、すべてのユーザがホストオペレーティングシステム上にユーザアカウントを持ち、コマンドラインインタフェースを使用する必要がある。

[5] これらの製品ファミリには、SMTP MTA と非標準 MTA の両方が用意されている。

ユーザ（特に外部のユーザ）にコマンドラインインタフェースの使用を認めることは、セキュリティ上のリスクが非常に大きい。このリスクを低減するために、メールボックスアクセス用のプロトコルが考案された。最も広くサポートされているメールボックスアクセスプロトコルは、Post Office Protocol（POP）および Internet Message Access Protocol（IMAP）の 2 つである。これらについては、それぞれ 2.4.1 項および 2.4.2 項で説明する。これら以外にも、MTA におけるメッセージ転送プロトコルの場合と同様、商用ソフトウェアメーカーが常用している非標準メールボックスアクセスプロトコルが存在する。非標準のプロトコルについては、2.4.3 項で説明する。POP、IMAP、および非標準プロトコルのほとんどにおいても、デフォルト設定では平文の認証用パスワードが使用されることに注意しなければならない。平文のパスワードは、同じネットワーク上にある別のホストから傍受される可能性がある。2.4.4 項では、Web ベースのメールアクセスに使用されるプロトコルの概要を述べる。

2.4.1 POP(Post Office Protocol: ポストオフィスプロトコル）

POP は、1984 年に開発された。基本的には、POP は単にメールサーバのメールボックスからメールクライアントへとメッセージをコピーする以上の仕組みではなく、文字どおりの郵便受けに手紙が届くようなものであった。メールクライアントは、メールサーバのメールボックスに接続し、電子メールメッセージをダウンロードして、接続を閉じる。RFC 918 に記述されているとおり、当初の POP で使用できるコマンドはわずか 9 種類であった（図 2.5「RFC 918 に基づく基本コマンド」を参照）。

RFC 918 に基づく基本コマンド

USER <名前>	ユーザ名を設定する
PASS <パスワード>	パスワードを設定する
STAT	メールボックスのステータスをチェックする （通常はメッセージ数の取得に使用）
LIST [メッセージ]	メールボックス内のメッセージの一覧を表示する。 任意使用の引数 [msg] でメッセージを指定可
RETR <メッセージ>	メッセージ <msg> を取得する
DELE <メッセージ>	メッセージ <msg> を削除する
QUIT	終了する
NOOP	何も実行しない
RSET	リセット

RFC 1939 に基づく任意使用コマンド

TOP <メッセージ> <n>	メッセージ <msg> の先頭から <n> 行分を取得する
UIDL [メッセージ]	メッセージ [msg] の一意な ID を取得する
APOP <名前> <ダイジェスト>	USER／PASS よりも堅牢な認証を行う

RFC 2449 に基づく拡張コマンド

CAPA	当該 POP3 サーバでサポートされている機能の一覧を取得する

図 2.5: POP3 コマンド

1984 年の登場以降、POP にはいくつかの見直しが行われ、現在は RFC 1939 で定義される第 3 世代の仕様になっている。基本的なコマンドセットはほぼ当初のままの形をとどめているが、POP バージョン 3 には、図 2.5 に示すいくつかの新しいオプションコマンド群が導入された。セキュリティの観点から見ると、APOP コマンドが新設され、平文でのユーザパスワード伝送を回避できるようになったことは重要である。APOP ではユーザ認証の方法としてチャレンジ／レスポンスを採用しており、クライアントは、サーバから送信されるチャレンジをユーザパスワードと組み合わせ、暗号ハッシュを生成

してサーバに返す。POP メールサーバでは、認証対象のユーザについて同様の操作を実行して、そのハッシュを検証する。

RFC 2449『*POP3 Extension Mechanism (POP3 拡張メカニズム)*』には、POP3 サーバに関する追加情報(サポートされている拡張や任意使用コマンドなど)をクライアントから取得できるようにするための POP3 拡張が定義されている。図 2.5 に、この拡張で POP3 に追加されたコマンドを示す。

POP 標準によるメールボックスへのアクセスには、重大な制約がいくつか存在する。一般に、ユーザが電子メールを取得すると、サーバ上に格納されているメッセージのコピーは削除される。つまり、メッセージアーカイブの維持管理は、ユーザが自己の責任において行う必要がある。個人利用のアカウントであれば、これも許容できる可能性はあるが、法的要件を満たすことが求められる企業組織や政府機関などにおいては一般に受け入れられないのがほとんどである。また、ユーザが複数台のワークステーションで電子メールの取得を実行すると、メッセージが複数のホストに拡散することになる。サーバ上から元のメッセージを削除しないように POP を設定することは可能だが、ユーザが別のホストからメールボックスにアクセスすると、新着メッセージだけでなく既読メッセージもすべてダウンロードすることが必要になる。または、保存期限を設定し、サーバ上に置かれたメッセージが一定期間の経過後に自動削除されるようにする必要がある。

2.4.2 IMAP(Internet Message Access Protocol: インターネットメッセージアクセスプロトコル)

上記のような POP の問題を解決するため、1988 年に IMAP が開発された。IMAP プロトコルは、POP バージョン 2 プロトコルの機能的なスーパーセットとなっている。設計の最も基本的なレベルにおいて、IMAP では、ユーザのメールボックスを一元管理できることと、複数のメールクライアントや MUA からのアクセスを受け付けることが考慮されている。

初期の IMAP が提供していた機能は POP を大きく超えていなかったが、1988 年の登場以降に加えられた改良により、現在では堅牢なメールボックスアクセスプロトコルに発展している。現行の IMAP 標準は、RFC 3501『Internet Message Access Protocol – Version 4, Revision 1』(4rev1)である。IMAP 4rev1 は多種多様な機能をサポートしているため、POP よりもはるかに広範なコマンドセットを備えている。図 2.6 に、IMAP 4rev1 のコマンド一覧を示す。また、CAPABILITY コマンドを使用して、当該 IMAP サーバで他の IMAP 拡張をサポートしているかどうかを照会することができる。

```
NOOP                                        何も実行しない
STARTTLS                                    機密性と完全性の保護を確立する
AUTHENTICATE <方式>                         認証方式を選択する
LOGIN <ユーザ> <パスワード>                 指定したユーザ名とパスワードでログインする
LOGOUT                                      現在のユーザをログアウトする
SELECT <メールボックス>                     アクセス対象とするメールボックスを選択する
EXAMINE <メールボックス>                    SELECTと同様、ただし読み取り専用でメールボックスを
                                            開く
CREATE <メールボックス>                     指定した名前のメールボックスを作成する
DELETE <メールボックス>                     選択したメールボックスを削除する
RENAME <メールボックス> <新メールボックス>  メールボックスの名前を変更する
SUBSCRIBE <メールボックス>                  選択したメールボックスを購読する
UNSUBSCRIBE <メールボックス>                選択したメールボックスの購読を解除する
LIST <参照> [パターン]                      (任意指定のパターンに基づいて)現在の参照先の内容
                                            の一覧を表示する
LSUB <参照> [パターン]                      パターンに一致するメールボックス群の一覧を表示する
STATUS <メールボックス> <項目>              選択したメールボックス内の特定項目のステータスを表
                                            示する
APPEND <メールボックス> [フラグ] <メッセージ>
                                            選択したメールボックスにメッセージを追加する
CHECK                                       現在選択中のメールボックスに対しチェックポイントを実
                                            行する
CLOSE                                       現在選択中のメールボックスを閉じる
EXPUNGE                                     メールボックス内の削除済みメッセージを消去する
SEARCH <条件>                               指定した条件に基づいてメールボックス内を検
索する
FETCH <メッセージ> <項目>                   選択したメッセージから特定項目を抽出する
STORE <メッセージ> <項目> <新しい値>        メッセージ内の特定項目を更新する
COPY <メッセージ> <メールボックス>          指定したメールボックスにメッセージをコピーする
UID <コマンド> [引数]                       メッセージ UID に基づいてメッセージに対する操作を実
                                            行する
CAPABILITY                                  サーバの機能を照会する
```

図 2.6: IMAP 4 Revision 1 コマンド

表 2.2 に、各種の IMAP 拡張に対応する RFC の一覧を示す。IMAP には、CRAM (Challenge-Response Authentication Mechanism: チャレンジ／レスポンス認証メカニズム)と呼ばれる、APOP に似たチャレンジ／レスポンス方式のメカニズムを採用した拡張が施されている。CRAM では、サーバから送信されるチャレンジデータを使用して生成した文字列を応答として返すことをクライアントに要求している。この文字列は、ユーザ名、1 文字の空白、および、チャレンジとともに送信されたタイムスタンプに共有の秘密を鍵とする鍵付きハッシュアルゴリズム[6]を適用して求めたダイジェストから構成する必要がある。

表 2.2: IMAP 拡張に関する RFC 文書

IMAP 拡張	関連 RFC
IMAP URL Scheme(URL スキーム)	2192
IMAP/POP AUTHorize Extension for Simple Challenge/Response(簡易チャレンジ／レスポンス方式による認証)	2195
IMAP4 ID extension(ID 拡張)	2971

[6] ほとんどの実装では、広く普及した MD5 と呼ばれる一方向ハッシュ関数を使用している。MD5 は、ディジタル署名用のメッセージダイジェスト生成を目的として Ronald Rivest が開発した関数であり、SHA-1 よりも高速だがセキュリティ強度においては劣ると考えられている。連邦政府機関における情報保護用途に関しては、MD5 の使用は承認されていない。詳細についてはセクション 3 を参照。

IMAP 拡張	関連 RFC
IMAP4 IDLE command（IDLE コマンド）	2177
IMAP4 Login Referrals（代替サーバへのログイン回送）	2221
IMAP4 Mailbox Referrals（メールボックス回送）	2193
IMAP4 Multi-Accessed Mailbox Practice（メールボックスへの多重アクセス手法）	2180
IMAP4 Namespace（名前空間）	2342
IMAP4 non-synchronizing literals（非同期連続送信）	2088
IMAP4 QUOTA extension（QUOTA 拡張）	2087
IMAP4 UIDPLUS extension（UIDPLUS 拡張）	4315

2.4.3 非標準のメールボックスアクセスメカニズム

非標準のメールボックスアクセスプロトコルは、閉じたメッセージング環境内で動作するように設計されている。非標準のメールボックスアクセスプロトコルを使用するメッセージングシステムの例として、Microsoft Exchange や Lotus Notes がある。そうした独自のプロトコルでは、対応するクライアントと組み合わせることで付加的な機能を使用することができる。独自技術によるメッセージングシステムはほぼすべて、ほかの種類の MTA および MUA との相互運用を可能にするために、SMTP、POP、IMAP などの標準プロトコルにも対応している。組織のメールクライアントおよびサーバで非標準のプロトコルをサポートすることが適切かどうかは、当該組織自身において決定しなければならない。前述したように、ほとんどのアクセスプロトコルにおいて（標準、非標準とも）、デフォルトではセキュリティ強度の低い（認証情報を暗号化しない）認証メカニズムが使用される。したがって、セキュリティ強度の高い認証方式をサポートするようにアクセスプロトコルを設定する必要がある。

2.4.4 Web ベースのメールアクセス

クライアントのアクセス手段となる Web ブラウザは、ほぼすべてのインターネット対応デバイスで利用できることから、電子メールサービスの提供形態として、Web ベースのメールアプリケーション、すなわち Web メールアプリケーションが使用される機会が多くなっている。ユーザは、単に Web ブラウザを起動し、目的の Web ベースのメールアプリケーションが稼動している Web サイトに接続するだけでよい。接続は、HTTP（Hypertext Transfer Protocol、ハイパーテキスト転送プロトコル）か、HTTPS(HTTP over Transport Layer Security(TLS))を使用して確立される。HTTPS の場合は通信が暗号化されるため、認証情報と電子メールメッセージ内容の両方が保護される。HTTP は、単独ではいっさい保護機能を持たないため、Web ベースのメールアプリケーション通信には HTTPS の使用を検討すべきである。

Web ベースのメールアプリケーションは、従来のメールクライアントに備わっているメール処理機能の大半を取り入れ、前述したものと同じメールボックスアクセスプロトコル（SMTP、POP、IMAP、非標準プロトコルなど）を使用して対象のメールサーバとの通信を行う。この場合、メールボックスアクセスプロトコルは Web サーバとメールサーバの間でのみ使用され、Web サーバと Web ブラウザの間には介在しない。

（本ページは意図的に白紙のままとする）

3. 電子メールメッセージに対する署名および暗号化

組織で使用される一部の電子メールメッセージを対象として、機密性および完全性の保護がしばしば必要となる。たとえば、電子メールに添付された、個人を特定できるような情報の漏えい防止である。電子メールメッセージの保護は、暗号を使用することにより、次のようにさまざまな方法で行うことができる。

- 電子メールメッセージに署名することで、その完全性を保証し、送信者の本人性を確認する。
- 電子メールメッセージの本文を暗号化することで、その機密性を確保する。
- メールサーバ間の通信を暗号化することで、メッセージ本文とメッセージヘッダの両方の機密性を保護する。

第 1 および第 2 の方法、すなわちメッセージへの署名とメッセージ本文の暗号化は、しばしば組み合わせて使用される。たとえば、暗号化による機密性の保護が必要なメッセージは、ディジタル署名も併せて使用し、メッセージの完全性と署名者の本人性を受信者が確認できるようにするのが普通である。内容の機密性を保護する必要がない場合、ディジタル署名したメッセージは暗号化しないことが多い。

上記第 3 の暗号方式、すなわちメールサーバ間の伝送の暗号化は一般に、2 つの組織間で定期的に送受信される電子メールを保護する場合にのみ適用される。たとえば、組織間に仮想プライベートネットワーク（VPN）を確立し、両者がインターネットを経由するメールサーバ間の通信を暗号化する場合などがこれに該当する。メッセージ本文のみを暗号化する方法と異なり、VPN では、電子メールヘッダ情報（送信者、宛先、件名など）を含めたメッセージ全体を暗号化することができる。場合によっては、ヘッダ情報の保護が必要なことがある。しかし VPN ソリューション単独では、メッセージ署名メカニズムは提供されず、また、送信者から受信者に至る経路全体にわたって電子メールメッセージを保護することもできない[7]。

ほとんどの電子メールメッセージには、ディジタル署名および（必要に応じて）暗号化による個別の保護が適用されるため、このセクションでは、主としてこれらの方式の使用について述べる。メッセージ署名およびメッセージ本文の暗号化に最も広く使用されている標準は、OpenPGP (Open Pretty Good Privacy) および S/MIME (Secure/Multipurpose Internet Mail Extensions：セキュリティ保護付き MIME) である[8]。このいずれも、部分的には公開鍵暗号の概念に基づくものである。公開鍵暗号においては、関連付けられた 2 つ 1 組の鍵をユーザが取り扱う。この鍵ペアは、あらゆるユーザが保持できる公開鍵と、所有者だけが保持できる秘密鍵からなる。公開鍵暗号は大量の演算処理を必要とするため、電子メールのセキュリティにおける採用状況は限定的であり、効率性に優れる対称鍵暗号のほうがはるかに多用されている。

対称鍵暗号においては、通信に関与する主体、すなわち電子メールメッセージの送信者と受信者の間で、同一の鍵が共有される必要がある。そのプロセスとしては、まず送信者がランダムな鍵を生成し、それを使用して対称鍵暗号アルゴリズムによりメッセージを暗号化する。次に送信者は、受信

---

7 VPN の詳細については、NIST SP 800-77『*IPSec VPN ガイド（Guide to IPsec VPNs）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

8 電子メールが発明されて以来、ほかにも多くの保護手法が提案されてきた。1987 年に開発された PEM（Privacy Enhanced Mail）や、MOSS (MIME Object Security Services) などがその例である。いずれの方式も現時点では広く使用されていないため、この文書では説明しない。

者の公開鍵を使用し、対応する何らかの公開鍵暗号アルゴリズムにより暗号鍵を暗号化して、暗号化したメッセージと暗号化した暗号鍵の両方を宛先に送信する。この複合的なプロセスにおいて、公開鍵暗号は暗号鍵の暗号化にのみ使用される。暗号鍵の復号に必要な秘密鍵を保持するのは宛先のメッセージ受信者だけであるため、他者がメッセージを復号して読み取ることはできない。ディジタル署名技術は、暗号ハッシュを使用して情報（すなわち送信するメッセージ）のダイジェストまたは「フィンガープリント」を作成する処理に依拠している。暗号ハッシュに対する署名は、メッセージ全体に対する署名よりも効率的に実行することができる[9]。

連邦政府組織では、連邦政府の承認を受けた暗号アルゴリズムの使用が義務付けられている[10]。連邦政府の承認を受けた暗号化方式は入念にテストされ、安全性が確認されているため、他の組織でも採用を検討してもよい。表 3.1 に、電子メールメッセージの保護を目的として暗号スイートを選択する場合の一般的な推奨事項を示す。

表 3.1：推奨する暗号スイート

推奨する用途	暗号スイート
最高のセキュリティ強度	暗号化：Advanced Encryption Standard（AES）[11] 128、192、または 256 ビット暗号化 認証およびダイジェスト：鍵サイズ 2048 ビット以上の DSS(Digital Signature Standard）または RSA と、ダイジェストサイズ 256 ビットの SHA（SHA-256）[12]
セキュリティおよびパフォーマンス	暗号化：AES 128 ビット暗号化 認証およびダイジェスト：鍵サイズ 1024 ビット以上の DSS または RSA と、SHA-1
セキュリティおよび互換性	暗号化：3DES(Triple Data Encryption Standard)[13] 168／112 ビット暗号化（注：3DES の処理は、AES に比べかなり低速である） 認証およびダイジェスト：鍵サイズ 1024 ビット以上の DSS と、SHA-1
認証および改ざん検出	認証およびダイジェスト：鍵サイズ 1024 ビット以上の DSS と、SHA-1 または SHA-256

3.1 OpenPGP

OpenPGP は、メッセージの暗号化および署名と、公開鍵暗号を使用した証明書作成のためのプロトコルである。OpenPGP の基になった PGP プロトコルは、Phil Zimmerman により策定され、1991 年 6 月にリリースされた製品に初めて実装された。初期の PGP プロトコルは、独自技術によるものであり、知的所有権の制約を受けるいくつかの暗号アルゴリズムを使用していた。1996 年に、PGP バージョン 5.x が IETF RFC 1991『PGP Message Exchange Formats』において規定された。その後、この PGP

---

9 公開鍵暗号の詳細については、NIST SP 800-32『*Introduction to Public Key Technology and the Federal PKI Infrastructure*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

10 連邦政府機関では、連邦情報処理規格（FIPS：Federal Information Processing Standards）において有効性が認められている暗号モジュールに含まれる、FIPS の承認を受けた暗号アルゴリズムを使用することが義務付けられている。暗号化モジュール有効性確認プログラム（CMVP：Cryptographic Module Validation Program）は、NIST およびカナダ政府の通信安全保障局（CSE：Communications Security Establishment、以下 CSE と称す）が共同で実施している取り組みで、特定の FIPS 文書に照らした暗号モジュールの有効性確認を行うものである。CMVP の Web サイト（http://csrc.nist.gov/cryptval/）には、FIPS 承認済みのアルゴリズムの網羅的な一覧が掲載されている。

11 AES の詳細については、http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf を参照のこと。

12 SHA およびこれに関連する SHS（Secure Hash Standard）の詳細については、FIPS PUB 180-2『*Secure Hash Standard (SHS)*』（http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf）を参照のこと。NIST では、SHA-1 の使用を段階的に減らして 2010 年までに廃止し、代わって、SHA-224 およびその他のサイズが大きく強力なハッシュ関数を使用するよう推奨している。詳細については、http://csrc.nist.gov/hash_standards_comments.pdf を参照のこと。

13 DES および 3DES の詳細については、http://csrc.ncsl.nist.gov/cryptval/ を参照のこと。

バージョン 5.x を基にした新しい標準プロトコルとして開発されたのが OpenPGP であり、RFC 2440『OpenPGP Message Format』および RFC 3156『MIME Security with OpenPGP』に定義されている[14]。

現在では、OpenPGP 標準を採用した無料の製品および商用製品が多数存在し、さまざまな Web サイトからそうしたソフトウェアのダウンロードや購入が可能である[15]。OpenPGP ベースの一部製品は、NIST が FIPS PUB 140-2 およびその他の刊行物において連邦政府に対して推奨している暗号アルゴリズム（データ暗号化用として 3DES および AES、ディジタル署名用として DSA(Digital Signature Algorithm)[16]および RSA、ハッシュ用として SHA[17]）を完全にサポートしている。ここで説明しない他の暗号化方式については、一部の OpenPGP 実装がサポートしている。

OpenPGP では、メッセージダイジェストのディジタル署名などいくつかの部分に公開鍵暗号が採用されているものの、メッセージ本文の実際の暗号化には、上で触れたとおり対称鍵アルゴリズムが使用される。OpenPGP を使用してメッセージの署名および暗号化を行う手順の概要は、次のとおりである（一部手順の順序は前後する場合がある）。

- 平文が圧縮される。これは、伝送時間を短縮するため、および、暗号解読時に一般的に行われる平文中のパターン抽出を困難にすることにより、暗号セキュリティを強化するためである。
- 乱数によりセッション鍵が作成される（OpenPGP の一部の実装では、乱数データを生成するためにマウスをウィンドウ内で任意に動かすようユーザに求める）。
- メッセージに対するディジタル署名が、送信者の署名鍵を使用して生成され、メッセージに付加される。
- メッセージと署名が、セッション鍵および対称アルゴリズム（3DES、AES など）を使用して暗号化される。
- セッション鍵は、受信者の公開鍵を使用して暗号化され、暗号化されたメッセージの先頭に付加される。
- 暗号化されたメッセージが受信者宛に送信される。

受信者はこの逆の手順によって、セッション鍵の復元、メッセージの復号、および署名の検証を実行する。Mozilla Thunderbird、Apple Mail、Eudora、Microsoft Outlook など一般に普及しているメールクライアントの場合、OpenPGP で暗号化したメッセージを送受信するにはプラグインのインストールが必要である。このセクションで先に示した OpenPGP 配布サイトには、各種メールクライアントアプリケーションで OpenPGP を使用する方法が説明されている。

また、OpenPGP による電子メールメッセージの暗号化、復号、署名、署名有効性検証をユーザに代わって実行するセキュリティゲートウェイサーバを利用することも可能である。互換性のあるセキュリティゲートウェイサーバを使用している組織同士で電子メールを交換する場合、ユーザは意識せず

---

14 OpenPGP に関する IETF 作業部会の Web サイトは http://www.ietf.org/html.charters/openpgp-charter.html である。

15 Free Software Foundation（http://www.gnupg.org/）、Hushmail（http://www.hushmail.com/）、International PGP（http://www.pgpi.org/）、OpenPGP（http://www.openpgp.org/）および PGP（商用版）（http://www.pgp.com/）などのサイトがある。

16 DSA およびこれに関連する DSS（Digital Signature Standard）の詳細については、FIPS PUB 186-2『*Digital Signature Standard (DSS)*』（http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf）を参照のこと。

17 FIPS PUB 140-2『*Security Requirements for Cryptographic Modules*』、FIPS PUB 180-2『*Secure Hash Standard (SHS)*』、および FIPS PUB 186-2『*Digital Signature Standard (DSS)*』は、http://csrc.nist.gov/publications/fips/index.html で入手することができる。

に OpenPGP を使用することができる。そうしたゲートウェイを一方の組織でのみ使用している場合でも、これを使用してメッセージを保護することは可能だが、相手方の組織に属するユーザは OpenPGP を意識して使用する必要がある。ゲートウェイのユーザが別の組織内の宛先に電子メールを送信すると、実際には受信者にゲートウェイからの通知メールが届く（SSL で暗号化された HTTP セッションを経由するのが一般的）。この通知メールには、保護された電子メールを受信する方法の説明が記載されている。また、一部のゲートウェイでは、複数のユーザ宛てに送信される電子メールに対してこの機能を実行できる場合がある。たとえば、あるユーザが暗号化および署名した電子メールをメーリングリストアドレス宛てに送信すると、ゲートウェイは、この電子メールを復号し、メーリングリストに属する個別の受信者向けに再度暗号化する。これにより、それぞれの受信者が電子メールを復号し、元の署名　を検証することができる。

3.2　S/MIME

S/MIME は、RSA Data Security, Inc.により 1995 年に提案された規格であり、暗号化メッセージのデータ形式については同社独自の（しかし幅広い支持を得ていた）PKCS (Public Key Cryptography Standard)＃7 を基にし、また、ディジタル証明書については X.509 バージョン 3 標準を基にしたものである[18]。S/MIME バージョン 2 は、インターネットメール業界全体に受け入れられ、豊富な採用実績を獲得した。IETF の標準とは見なされていないが、この仕様は参考情報 RFC 2311、2312、2313、2314、2315、および 2268 で定められている。

S/MIME バージョン 3 は、IETF の S/MIME 作業部会によって策定され（現在は同部会が S/MIME 標準の策定作業すべてを取りまとめている）[19]、1999 年 7 月に IETF 標準として採択された。S/MIME バージョン 3 の仕様は次に示す RFC により定められている。

- Cryptographic Message Syntax（暗号メッセージ構文）（RFC 3852）
- S/MIME Version 3 Message Specification（メッセージ仕様）（RFC 3851）
- S/MIME Version 3 Certificate Handling（証明書の取り扱い）（RFC 3850）
- Diffie-Hellman Key Agreement Method（Diffie-Hellman 鍵交換方式）（RFC 2631）
- Enhanced Security Services for S/MIME（拡張セキュリティサービス）（RFC 2634）

S/MIME の最も大きな特長は、その機能がアプリケーションに組み込まれており、ほぼ「自動的」に使用できるという点である。メーカーの多大な協力により、S/MIME の機能は、Mozilla や Outlook Express など一般的なメールクライアントにデフォルトでインストールされている。

S/MIME 対応メールクライアントがメッセージを送信する実際のプロセスは、OpenPGP の場合に類似している[20]。S/MIME バージョン 3.1 では、FIPS PUB 140-2 が推奨する 2 種類の対称鍵暗号アルゴリズムをサポートしている。その 1 つである AES は、推奨されているが適合実装におけるサポートは任意である。もう 1 つの 3DES は、実装におけるサポートが必須とされている。電子メールの保護に S/MIME を使用する組織は、AES または 3DES を使用するべきである（AES は 3DES よりも強力なアルゴリズムであると考えられるため、AES が望ましい）。

18　RSA PKCS 標準の詳細については、PKCS ホームページ（http://www.rsasecurity.com/rsalabs/node.asp?id=2124）を参照のこと。

19　S/MIME 作業部会のホームページは、http://www.ietf.org/html.charters/smime-charter.html である。

20　次の IBM Redbook には、S/MIME の仕組みを示す詳細な例が示されている。
http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg245341.pdf

OpenPGP の場合と同様に、S/MIME による電子メールメッセージの暗号化、復号、署名、署名有効性検証をユーザに代わり実行するセキュリティゲートウェイサーバの利用が可能である。そうしたゲートウェイの機能は、3.1 項で述べたものと非常によく似ており、実際のところ、OpenPGP と S/MIME の両方をサポートするゲートウェイが多数存在する。

3.3 鍵管理

OpenPGP および S/MIME では、いずれも鍵の管理にディジタル証明書を使用する。ディジタル証明書によって、その証明書を発行された主体（ユーザなど）、その主体の公開鍵ペアのうちの公開鍵、および、信頼できる何らかの機関により署名されたその他の情報（有効期限など）が特定される。しかし、ディジタル証明書を使用して信頼を確立するための鍵管理モデルについては、OpenPGP と S/MIME で違いがある。

OpenPGP が採用するデフォルトの伝統的な鍵管理モデルは、「web of trust（信頼の網）」と呼ばれ、鍵を一元的に発行したり承認したりする機関がない。「web of trust」では、マネジメントおよび制御がユーザ個人の判断に委ねられる。たとえば、アリスがボブを信頼しており、キャロルがアリスを信頼している場合、キャロルはボブの電子メールを信頼することになっている。このようなシステムは、個人や非常に小さい組織には好適であるが、ほとんどの中～大規模の組織ではオーバヘッドが大きすぎて実用に耐えない。組織によっては、ユーザが他者の鍵を取得したり自身の鍵を保管したりするための鍵サーバを導入している。これによりスケーラビリティは向上するが、プロセスは主として個々のユーザが制御することになるため、鍵サーバがユーザの身元について十分な保証を提供することを組織として信頼するのは困難な場合が多い。

一方、S/MIME では、組織として信頼することを決めた権限をより階層的な構造で管理する従来型のモデルを採用している。一般的には、登録および承認のマスタ機関、すなわちルート認証局（CA：Certificate Authority）を 1 つ指定する。ルート CA は、同局自身および同局が認める全ての下位 CA に対する公開鍵証明書を発行する。下位 CA は通常、ユーザに対する証明書と、同局のさらに下位に属する CA に対する証明書を発行する。この関係により階層構造が形成される。こうした公開鍵基盤(PKI)を使用することにより、同じ基盤において発行された有効な証明書を保持する任意の 2 ユーザ間に、信頼の連鎖を確立することができる。S/MIME 対応メールクライアントは、S/MIME トランザクションを処理する際、デフォルトでは当該クライアントの直接のマスタ CA における信頼に依拠する。この CA は、何らかのサードパーティ CA[21]であっても、証明書を発行する組織が管理する CA であってもよい。

OpenPGP または S/MIME で保護された電子メールを他の組織と交換できるようにすることは、通常は非常に複雑であり、ユーザがこれまでと同様に電子メールを使用できるようにしようとする場合には、特に複雑なものとなる。最大の課題は、組織間においてどのように鍵の交換および信頼関係の確立を行うかである。各組織が PKI を相互に接続したり、両者が信頼しているサードパーティの PKI を使用したりすることができるが、いずれの場合も、技術的な問題や法規制に関する問題に直面することが多い。また、OpenPGP および S/MIME に対するサポート状況は、使用するメールクライアントに応じて大きく異なる。

信頼関係を確立したりメールアプリケーションの互換性を心配したりすることなく、暗号化した電子メールを組織間で交換することを可能にするサービスがサードパーティから提供されてはいるが、そうしたサービスを利用するには、機密性のあるメッセージをサードパーティのサーバ上に置く必要があ

---

[21] CA の例として、Entrust（http://www.entrust.com/）、Thawte（http://www.thawte.com/）、および Verisign（http://www.verisign.com/）などがある。

り、このこと自体がセキュリティの問題となる。2 つの組織間でメール暗号化ゲートウェイを使用すると、通常は鍵管理上の問題が軽減される。これは、鍵がゲートウェイ上で維持され、信頼関係がゲートウェイ間であらかじめ確立されているからである。

電子メールの署名および暗号化に関する鍵管理上の問題を軽減し得る 1 つの手法について、現在、作業が進められている。ID ベース暗号化（IBE：Identity-Based Encryption）は一種の公開鍵暗号化方式で、任意の文字列を公開鍵として使用することができるようになる。電子メールアドレスを公開鍵として使用すれば、IBE によって鍵管理が簡易化され、送信者は、送信する電子メールをはるかに容易に保護できるようになる可能性がある。ただし、IBE に関しては公開標準がなく、FIPS の承認を受けた IBE 製品が存在しないなど、その採用を阻む深刻な課題もある。現在は、S/MIME による IBE の実行方法について提案する参考情報としての Internet Draft 文書の整備が始められた段階である。

3.4 電子メールの暗号化に関する課題

電子メールを暗号化することによりセキュリティは向上するが、それには相応のコストが必要であるため、電子メールの暗号化に関連する次のような課題の重要度を注意深く検討すべきである。

- 暗号化を行った場合、ウイルスその他のマルウェアのスキャン処理や電子メールコンテンツのフィルタリングをファイアウォールおよびメールサーバにおいて実行するのが非常に複雑になる。ファイアウォールまたはメールサーバが電子メールを復号するための手段を備えていないと、コンテンツを読み取り、それに対してアクションをとることはできない。電子メールの宛先が特定のマルウェアスキャナである場合や、送信者が特定のスキャナ向けに電子メールを暗号化している場合は、スキャナが電子メールを復号することができるが、そうしたソリューションは技術的に複雑であり、使用を強制するのは困難であることが多い。また、全部または一部の電子メールを復号する機能をマルウェアスキャナに持たせる場合、スキャナのホスト自体がマルウェアに感染したり何らかのセキュリティ侵害を受けたりした場合に深刻な結果が生じる可能性がある。マルウェアスキャナによる電子メールの復号が現実的でない場合は、復号を行うメールクライアントのホスト上でスキャン処理を実行する必要が生じる可能性がある。

- 暗号化および復号の処理は、多くの処理時間を要する。したがって、暗号化および復号の負荷に耐えられない機器のアップグレードまたは置き換えが必要となる場合がある。

- 組織全体で暗号化を運用するには、管理作業に多大なオーバヘッドが継続的に発生する可能性がある。たとえば、鍵の配布、鍵の回復、暗号化鍵の失効処理などがこれに含まれる。

- 電子メールを暗号化すると、法執行機関やその他の調査機関による電子メールメッセージの捜査が困難になる可能性がある。

- 暗号化した電子メールを送受信する相手となる組織において強力な暗号化アルゴリズムや鍵サイズがサポートされていなければ、電子メールが十分に保護されない可能性がある。組織内のユーザが暗号化強度の低いメッセージを受信した場合や、強度の低い暗号化方式しかサポートしていない宛先に暗号化されたメッセージを送信しようとした場合、メールアプリケーションからユーザにその旨が確実に通知されるようにするべきである。通知を受けたユーザは、関係する主体に問題を報告し、より強力な暗号化アルゴリズムの使用を要請したり、保護を要する情報の転送に電子メール以外のメカニズムを使用したりすることができる。

■ メールサーバの計画とマネジメント

セキュリティが確保されたメールサーバの導入において最も重要なのは、インストール、設定および導入の前に入念な計画を立てることである。慎重に計画すれば、メールサーバのセキュリティを可能な限り確保し、組織のすべての関連ポリシーに適合させることができる。メールサーバのセキュリティおよびパフォーマンスに関する問題の多くは、計画と管理策の不備にその原因を求めることができる。管理策の重要性は、どれだけ強調してもし過ぎることはない。多くの組織では、IT のサポート体制が非常に細分化されているため、一貫性を欠くことになり、セキュリティ上の脆弱性が生じる原因となり得る。

3.5 インストールおよび導入の計画

セキュリティを最大限に保ち、コストを最小限に抑えるには、システム開発ライフサイクルの最初の計画段階からメールサーバのセキュリティを考慮すべきである。メールサーバの実装・導入前にセキュリティ対策を実施するのに比べ、実装および導入が行われた後にセキュリティ対策を実施する方が、はるかに困難かつ高コストなものになる。始めから詳細かつ適切に設計された導入計画を策定し、使用した場合のほうが、組織は、ホストの設定について、より適切かつ一貫した判断を下す可能性が高い。そのような計画を策定することにより、組織は、利便性、パフォーマンス、リスクの 3 要素間のトレードオフについて、十分な根拠に基づいた判断を下すことが可能になる。導入計画によって、組織は、安全な設定を維持することが可能になり、また、しばしば計画からの逸脱という形で現れるセキュリティ上の脆弱性を特定する際にも役立つ。

メールサーバの計画段階においては、次の事項を検討すべきである。[Alle00]

■ メールサーバの用途を決定する。

  – メールサーバを使ってどのような種類の情報を格納、処理、および伝送するか
  – 当該情報のセキュリティ要件は何か
  – メールサーバが他にどのようなサービスを提供するか（一般に、メールサーバ専用のホストとするのがセキュリティ上、最も安全である）
  – 追加的に提供されるサービスのセキュリティ要件は何か
  – メールサービスの継続性の要件は何か（運用継続計画や災害復旧計画に規定されている要件などか）
  – ネットワークのどこにメールサーバを配置するか（6.1 項を参照）

■ メールサーバが提供するネットワークサービスを明らかにする（組織内の標準サービスとしてすべてのサーバが提供するバックアップやリモート管理などに加えて）。たとえば、標準の電子メールプロトコル（SMTP、POP、IMAP など）および非標準の電子メールプロトコルによって提供されるサービスなど。

■ メールサーバおよび他のすべてのサポートサーバにインストールするすべてのネットワークサービスソフトウェア（クライアント、サーバの両方）を明らかにする。

■ メールサーバおよびすべてのサポートホスト（Web ベースのメールアクセスを提供するサーバを含む）を使用するユーザまたはユーザのカテゴリを明らかにする。

■ メールサーバおよびサポートホストについて、各カテゴリのユーザが保持する特権を決定する。

- メールサーバの管理方法を決定する（ローカル管理、内部ネットワークからのリモート管理、外部ネットワークからのリモート管理など）。
- ユーザを認証するかどうか、ユーザの認証方法、認証データの保護方法を決定する。
- アドレス関連情報について、全てのセキュリティ要件またはプライバシ要件（ユーザ名、ユーザID、組織との関係）を明らかにする。
- どのようにして、情報リソースに対する適切なアクセスが行われるようにするかを決定する。
- 組織の要件を満たすメールサーバアプリケーションを選定する。その際、たとえ一部の機能が劣っているとしても、より強力なセキュリティを実現できるサーバの採用を検討する。考慮すべきいくつかの事項を次に示す。
  - コスト
  - 既存基盤との互換性
  - 既存職員の知識
  - メーカーとの間にこれまでに築いた関係
  - これまでの脆弱性の履歴
  - 機能性
- 計画策定の段階におけるメーカーとの連絡を密にする。

オペレーティングシステムは、選択するメールサーバアプリケーションによって限定される場合もあるが、メールサーバ管理者は、可能な限り次の要件を満たすオペレーティングシステムを選定すべきである。[Alle00]

- 脆弱性が存在する可能性が最小限であること（すべてのオペレーティングシステムについて明確化することができる）
- 管理者レベルまたは root レベルの作業を権限を有するユーザのみに限定できること
- 利用を意図した情報以外のサーバ上の情報へのアクセスを拒否できること
- オペレーティングシステムまたはサーバソフトウェアに組み込まれている可能性のあるネットワークサービスのうち不要なものを無効にできること
- 侵入およびその試みを検出するために適切なサーバ動作のログを記録できること

これに加え、サーバおよびサーバ製品を管理するために、技能と経験を持ったスタッフの確保を検討すべきである。多くの組織は、厳しい経験を通じて、特定の運用環境についての能力と経験を持つ管理者が、別の環境でも同程度に能力を発揮するとは限らないことを学んできた。

メールサーバは、機密性が高い性質のものであるため、物理的に安全性の高い場所に設置することが重要である。メールサーバの設置場所を計画する際には、次の事項を考慮すべきである。

- 適切な物理的セキュリティ保護メカニズムがあるか。たとえば、施錠、カードリーダアクセス、セキュリティ警備、物理的な侵入検知システム（モーションセンサ、カメラ）など。
- 湿度や温度について必要な条件を維持するために、適切な環境調整機能があるか。

- 予備電源があるか。
- 既知の自然災害の影響を受ける可能性がある立地の場合、そうした災害に対する強化措置が実施されているか、また、被害が生じる可能性がある地域の外に緊急時対応サイトが確保されているか。

3.6 セキュリティマネジメントスタッフ

メールサーバのセキュリティは、組織の全般的な情報システムセキュリティ状況と密接に関係するため、メールサーバの計画、実装、管理については、IT およびシステムセキュリティに携わる多くの人々が関心を持つと考えられる。この項では、そうした人々の職務ごとに、メールサーバのセキュリティに関する役割分担を示す。ただし、組織によっては役割などが異なる場合や、ここでの説明に該当する職務が存在しない場合がある。

3.6.1 上級 IT マネジメント／最高情報責任者（CIO）

上級 IT マネジメント／CIO は、当該組織のセキュリティが適切な状況となるようにする。組織全体の情報システム保護について、上級 IT マネジメントは方針を示し、助言を与える。メールサーバに関連する次の活動については、上級 IT マネジメント／CIO が責任を負う。

- 組織内の情報セキュリティポリシー、標準、手続きの策定および維持作業を調整する
- 組織内の変更管理およびマネジメント手続きの策定および維持作業を調整する
- 組織全体を通じて、各部門に対する、一貫したIT セキュリティポリシーの確立およびその遵守を徹底する
- 電子メール利用ガイドライン（個人使用、監視、暗号化など）に関する公式ポリシーおよびプロセスの策定について、上位マネジメント、広報、その他関連する人員と調整する

3.6.2 情報システムセキュリティプログラムマネージャ

情報システムセキュリティプログラムマネージャ（ISSPM：Information Systems Security Program Manager）は、組織のセキュリティポリシーに指定されている標準、ルール、規制の実装およびそれらの遵守を監督する。メールサーバに関連する次の活動については、ISSPM が責任を負う。

- セキュリティ手続きを確実に策定および実装する
- セキュリティのポリシー、標準、要件の遵守を徹底する
- すべての重要システムを特定し、それらの重要システムについて緊急時対応計画、災害復旧計画、運用継続計画を確実に整備する
- 重要システムを特定し、各システムに対応するセキュリティポリシー要件に従って定期的なセキュリティテストのスケジュールを確実に策定する

3.6.3 情報システムセキュリティ責任者

情報システムセキュリティ責任者（ISSO：Information Systems Security Officer）は、特定の組織主体における情報セキュリティのあらゆる側面を監督する責任を負い、組織の情報セキュリティプラクティスを、組織および部門のポリシー、標準、手続きに確実に適合させる。メールサーバに関連する次の活動については、ISSO が責任を負う。

- メールサーバおよびその稼働を支えるネットワーク基盤を対象とした内部セキュリティ標準および手続きを策定する
- 協力して、セキュリティツール、メカニズム、および問題軽減のテクニックを策定・実装する
- 当該組織の管理下にある、メールサーバおよびその稼働を支えるネットワーク基盤（オペレーティングシステム、ファイアウォール、ルータ、メールサーバアプリケーションその他を含む）について、標準的な設定プロファイルを維持する
- セキュリティテストの実施によりシステム運用の完全性を維持する。また、重要システムに対し、スケジュールされたテストを担当の IT 専門家に確実に実施させる

3.6.4 メールサーバおよびネットワーク管理者

メールサーバ管理者は、メールサーバの全体的な設計、実装、保守に責任を持つシステムアーキテクトである。ネットワーク管理者は、ネットワークの全体的な設計、実装、保守に責任を持つ。メールサーバおよびネットワーク管理者は、担当するシステムのセキュリティ要件に対応するための日常的な活動を行う。セキュリティ上の問題およびその解決策は、外部からもたらされる場合（メーカーまたはコンピュータセキュリティインシデント対応チームから提供されるセキュリティパッチや修正など）もあれば、組織内（セキュリティ担当部署など）で生まれる場合もある。メールサーバに関連する次の活動については、メールサーバおよびネットワーク管理者が責任を負う。

- 組織のセキュリティポリシーと標準のシステム／ネットワーク構成に適合するようにホストのインストールおよび設定を行う
- ホストを安全に保つ作業（頻繁なバックアップ、適切なタイミングでのパッチ適用など）を行う
- システムの完全性、保護のレベル、および、セキュリティに関連するイベントを監視する
- 組織内の情報システムリソースに関して、検知したセキュリティ上の異変に対処する
- 要件に応じてセキュリティテストを実施する

3.7 マネジメントのプラクティス

セキュリティが確保されたメールサーバの運用および保守においては、適切なマネジメント活動が不可欠である。セキュリティ活動には、組織が持つ情報システム資産を明らかにすることおよび、情報システムリソースの機密性、完全性、可用性を確保するためのポリシー、標準、手続き、ガイドラインの策定、文書化、実施が含まれる。

メールサーバおよびそのネットワーク基盤についてセキュリティを確保するために、組織は次の活動を実践すべきである。

- **組織の情報システムセキュリティポリシー** — セキュリティポリシーは、基本的な情報システムセキュリティの精神およびルール、並びに意図する内部的な目的を定めたものである。また、ポリシーは、情報セキュリティの個々の領域（実装、適用、監査、レビューなど）について、組織内における責任の所在の概略を定める。このポリシーが実効性を持つためには、ポリシーが、組織全体にわたり一貫して適用されなければならない。一般に、組織のセキュリティポリシーの原案の作成には、CIO および上級マネジメントが責任を持つ。
- **構成／変更コントロールおよび管理** — システムの設計、ハードウェア、ファームウェア、ソフトウェアに加えられる変更をコントロールするプロセスは、システム実装の前後および中途におい

て、不適切な変更が導入されることからシステムが保護されることについて、十分な保証を提供する。構成コントロールによって、組織の情報システムセキュリティポリシーとの整合性の維持が実現される。従来より、構成コントロールは、情報システムに対して提案されるすべての変更について最終的な決定権を持つ構成コントロール委員会によって監督される。

- **リスクアセスメントおよびマネジメント** — リスクアセスメントは、リスクを分析および解釈するプロセスである。これには、アセスメントの対象範囲と方法論の決定、リスク関連データの収集と分析、および、リスク分析結果の解釈という作業が含まれる。リスクデータを収集および分析するには、資産、脅威、脆弱性、防御策、影響、および攻撃が成功する確率を明確化する必要がある。リスクマネジメントは、組織にとって受容可能なレベルまでリスクを低減するための管理策を選定・実施するプロセスである。

- **標準的な設定** — 広く使用されているオペレーティングシステムおよびアプリケーションについて、標準となる安全な設定を策定すべきである。これは、メールサーバおよびネットワーク管理者にとって、システムを安全に設定し、組織のセキュリティポリシーに対する整合性と適合性を確保するためのガイダンスとなる。安全な設定がされていないホストが 1 台でもあれば、ネットワークへの侵入が可能となるため、多数のホストを運用する組織においては特に、この推奨事項を実践することが奨励される。セクション 5 に、標準的な設定に関する補足情報を示す。

- **セキュリティの意識向上およびトレーニング** — セキュリティトレーニングプログラムは、組織全体のセキュリティ体制を形成するために不可欠である。ユーザおよび管理者にセキュリティに関する自分の責任を意識させ、正しいプラクティスを教育することで、セキュリティベストプラクティスに適合した行動をとるよう変化を促すことができる。また、情報システムセキュリティを改善させる上で重要な手段である個人の説明責任をサポートするためにもトレーニングは有用である。

- **緊急時対応、運用継続、および災害復旧の計画** — 緊急時対応計画、運用継続計画、および災害復旧計画は、情報システムに障害が発生した時に、組織または施設の運用が継続できるようにすることを目的として事前に策定される[22]。

- **承認および運用認可** — 情報システムセキュリティの文脈における承認とは、組織のすべてのセキュリティ要件をどの程度満たしているかについて、システムが分析されたことを意味する。システムが組織のセキュリティ要件を満たしていることを組織のマネジメント層が認めた場合に、運用認可が行われる[23]。

3.8 システムセキュリティ計画

システムセキュリティ計画の目的は、情報システムリソースの保護を強化することである[24]。情報資産を十分に保護する計画は、マネージャおよび情報の所有者（情報および／または処理能力から直接的な影響を受け、またそれらに直接関心を持つ者）に対して、彼らが管理する情報資産が、損失、誤用、不正アクセスまたは改ざん、利用不能な状況、および検知されない活動から十分に保護されることについて、確信を持たせる必要がある。

---

22 詳細については、NIST SP 800-34『*IT システムにおける緊急時対応計画ガイド（Contingency Planning Guide for Information Technology Systems）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

23 承認および運用認可の詳細については、NIST SP 800-37『*連邦政府情報システムのセキュリティに対する承認および運用認可ガイド（Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

24 システムセキュリティ計画の詳細については、NIST SP 800-18 Revision 1『*連邦情報システムのためのセキュリティ計画作成ガイド（Guide for Developing Security Plans for Federal Information Systems）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

システムセキュリティ計画の目的は、システムのセキュリティおよびプライバシ要件の概要を示し、それらの要件を満たすために実施済みまたは計画中の管理策について説明することである。また、そのシステムにアクセスするすべての個人が負う責任と期待される行動の概要も示す。システムセキュリティ計画は、システムに対する十分かつコスト効率のよいセキュリティ保護を計画するための系統立ったプロセスを文書化したものと考えるべきである。したがって、システムに関して責任のあるさまざまなマネージャ(情報の所有者、システムの所有者、および、機関の上級情報セキュリティ責任者(SAISO)を含む)の意見が反映されなければならない。

連邦政府機関においては、すべての情報システムが何らかのシステムセキュリティ計画の対象となっていなければならない。その他の組織においても同様に、組織の個々のシステムについてシステムセキュリティ計画を完成させることを強く検討すべきである。通常、情報システムの所有者[25]は、セキュリティ計画の策定・維持および、合意されたセキュリティ要件に従ったシステムの導入・運用について責任を負う。

一般に、システムセキュリティ計画に実効性を持たせるためには、次の事項を盛り込むべきである。

- **システム識別情報**:システムセキュリティ計画の冒頭のセクションでは、対象システムに関する基本的な識別情報を示す。これには、システムに関する主要な連絡先、システムの用途、システムの機密性レベル、および、システムが導入されている環境などの一般情報が含まれる。
- **管理策**:計画の管理策セクションでは、情報システムの保護要件を満たすことを目的とした(実施済み、または計画中の)管理策について説明する。管理策は、次の 3 つに分類される。
  - マネジメント上の管理策:コンピュータセキュリティシステムのマネジメントと、システムのリスクマネジメントを主眼とする[26]。
  - 運用上の管理策:主としてシステムではなく人によって導入および実行される。多くの場合、技術的または専門的な知識を必要とし、マネジメント活動および技術的な管理策に依拠する。
  - 技術的な管理策:コンピュータシステムにおいて採用されるセキュリティメカニズムである。技術的な管理策は、不正アクセスや誤用からの自動的な保護、セキュリティ違反の検出の推進、およびアプリケーションとデータのセキュリティ要件のサポートを提供することができる。ただし、技術上の管理策を実装するには、運用について十分に検討することが不可欠であり、また、組織内のセキュリティ管理との整合性を持たせる必要がある。[Swan06]

3.9 人材に関する要件

メールサーバを開発して安全に維持するうえで、最大の課題およびコストは、必要な機能を十分に実行できる人材の確保である。メールサーバを安全に運用するために必要な費用と技能の大きさを、多くの組織は十分に理解していない。このことは、しばしば職員の過剰労働やシステムのセキュリティ上の不備が生じる原因になる。必要な人的リソースの要件については、最初の計画段階で明らかにしておく必要がある。適切かつ十分な人的リソースは、メールサーバのセキュリティにおける最も

---

[25] 情報システム所有者は、システムの運用パラメータ、許可する機能、およびセキュリティ要件を定義する責任を負う。システムが格納、処理、または伝送する情報の所有者は、情報システムの所有者と同じである場合もあればそうでない場合もある。また、単体のシステムで複数の情報所有者の情報を使用してもよい。

[26] マネジメント上、運用上、および技術的な管理策の詳細については、NIST SP 800-53『*連邦政府情報システムにおける推奨セキュリティ管理策(Recommended Security Controls for Federal Information Systems)*』、および NIST SP 800-100『*Information Security Handbook: A Guide for Managers*』(http://csrc.nist.gov/publications/nistpubs/)を参照のこと。

重要な側面である。また、一般に、技術的なソリューションは技能と経験を持つ人材を代替するものではないという事実も考慮すべきである。

メールサーバの開発および導入に伴う人的リソースについては、その必要性を考慮して導入計画に次の事項を盛り込むべきである。

- **必要な人材** — どのような種類の人材が必要とされるか。これには、システムおよびメールサーバ管理者、ネットワーク管理者、ISSO などが含まれる可能性がある。
- **必要な技能** — メールサーバの計画、開発、保守を、セキュリティに十分配慮して行うにはどのような技能が必要とされるか。これには、たとえばオペレーティングシステム管理、ネットワーク管理、コンテンツに関する実地の知識、およびプログラミングなどが含まれる。
- **調達可能な人材** — 組織内からどのような人材を調達できるか。それらの人材は、現状でどのような技能を備えているか、その技能はメールサーバをサポートするのに十分であるか。組織の既存の人材では十分でないという結論に至る場合が多く、その場合は次の選択肢を考慮する必要がある。
  - 既存の人材を対象としたトレーニング — 人員は確保できるものの、必要な技能を有していない場合、必要な技能をトレーニングによって与えることが選択肢となる。これは優れた選択肢ではあるが、トレーニングを受ける人員が、必要となる全ての前提条件を確実に満たしていなければならない。
  - 新しい人材の雇用 — 確保できる人員が不足しているか、必要な技能を備えていない場合、新しい人材の雇用が必要となる可能性がある。

プロジェクトに必要な人材を割り当て、メールサーバが稼働し始めたあとも、担当者の数と技能が十分なものとなるようにする必要がある。メールサーバなどのホストの脅威および脆弱性のレベルは常に変動しており、テクノロジーもまた変化している。したがって、今日十分であるものが明日もそうであるとは限らない。

3.10 情報システムセキュリティに関する一般原則

メールサーバのセキュリティ上の課題に取り組む際、セキュリティに関する次のような一般原則を念頭に置いておくことは非常に有用である。[Curt01] および [Salt75]

- **単純さ** — セキュリティのメカニズム（および情報システム全般）は、可能な限り単純であるべきである。複雑さは、多くのセキュリティ上の問題の原因となっている。
- **耐障害性** — 障害が発生したとき、システムは、セキュリティ管理策や設定が有効な状態を維持し、かつ適用されることによって、安全性を保ちながら停止すべきである。通常、セキュリティが損なわれるよりは機能が損なわれるほうが望ましい。
- **アクセスの完全な間接化** — 情報への直接的なアクセスを提供するのではなく、アクセスポリシーを実行する仲介者を介在させるべきである。たとえば、ファイルシステムのアクセス許可、プロキシ、ファイアウォール、メールゲートウェイなどがこれに該当する。
- **オープンな設計** — システムのセキュリティは、実装やその構成要素の秘密性に依存すべきでない。「不知によるセキュリティ」は信頼できるものではない。
- **特権の分離** — 可能な範囲で機能を分離し、できる限り細分化するべきである。この考え方は、システムと、オペレータおよびユーザの両方に適用できる。システムの場合、読み取り、編集、

書き込み、実行などの各機能を分離すべきであるし、システムオペレータおよびユーザの場合は、役割をできるだけ分離すべきである。たとえば、リソース面で可能であれば、システム管理者の役割とセキュリティ管理者の役割は分離するべきである。

- **最小特権** — 個々のタスク、プロセス、ユーザに対しては、それぞれの作業を実行するために必要となる最小限の権限を付与すべきである。この原則が一貫して適用されていれば、タスク、プロセスまたはユーザが侵害されても、被害の範囲は侵害されたエンティティが利用できるリソースに限定される。

- **心理的な受け入れ** — ユーザは、セキュリティの必要性を理解すべきである。これは、トレーニングおよび教育によって達成できる。また、既に導入されているセキュリティメカニズムは、ユーザに対して、日常的に必要な使い勝手が得られる実用的な選択肢を提示するべきである。ユーザにとってセキュリティメカニズムが煩雑すぎるものであれば、ユーザはそれに対処する方法を案出するか、あるいは妥協案をとることが考えられる。ただし、この原則の目的は、セキュリティをユーザにとって理解可能で受け入れることができるものにするためにセキュリティを弱めることではなく、利便性と実効性に優れたセキュリティメカニズムおよびポリシーを訓練、教育、設計することである。

- **メカニズム共用部分の最小化** — 何らかの機能をシステムに提供する際には、システムの他の部分に同じ機能を付与することなく、プロセスまたはサービスがその機能を利用できるようにするのが最善である。たとえば、メールサーバのプロセスがバックエンドデータベースにアクセスすることが可能である場合、システムの別のアプリケーションがバックエンドデータベースにアクセスすることが可能であるべきではない。

- **多重防御** — 単独のセキュリティメカニズムだけでは、概して防御が不十分であることを理解すべきである。単一のセキュリティメカニズム（防御）を突破しただけで、ホストやネットワークに侵入されてしまうことができないように、セキュリティメカニズムを多重化する必要がある。情報システムのセキュリティに万能の解決策は存在しない。

- **攻撃側のコストの観点** —システムまたはネットワークのセキュリティ機能を破るためにどれだけの労力が必要かを把握しておくべきである。攻撃者が侵入に成功することで得るものの価値よりも、システムまたはネットワークに侵入するために必要な労力の方が大きくなければならない。

- **侵害の記録** — 侵害が発生した場合に攻撃の証拠を組織が利用できるよう、記録およびログを保存しておくべきである。この情報は、侵害の発生後にネットワークおよびホストのセキュリティを確保するためにも、また、攻撃者が使用した手法や悪用の手口を特定するためにも役立ち、将来、ホストやネットワークのセキュリティを強化するための参考になる。また、攻撃者を特定して告発するためにも有用である。

3.11 メールサーバの計画と管理のためのチェックリスト

完了	アクション
	メールサーバのインストールおよび導入に関する計画
☐	メールサーバの機能を明らかにする
☐	メールサーバが保存、処理、伝送する情報のカテゴリを明らかにする
☐	情報のセキュリティ要件を明らかにする
☐	メールサービスの継続性の要件を明らかにする
☐	メールサーバを稼働させる専用ホストを特定する
☐	メールサーバが提供またはサポートするネットワークサービスを特定する
☐	メールサーバを使用するユーザおよびユーザのカテゴリを明らかにし、ユーザのカテゴリごとに付与する権限を決定する
☐	メールサーバの管理方法を決定する（ローカル管理、リモート管理など）
☐	メールサーバにおけるユーザ認証方式を決定する
☐	電子メールアドレス関連情報のセキュリティまたはプライバシ要件を明らかにする
	メールサーバの稼働に適したオペレーティングシステムの選定
☐	脆弱性が存在する可能性が最小限であること
☐	管理者レベルまたは root レベルの作業を権限を有するユーザのみに限定できること
☐	利用を意図した情報以外のサーバ上の情報へのアクセスを拒否できること
☐	オペレーティングシステムまたはサーバソフトウェアに組み込まれている可能性のあるネットワークサービスのうち不要なものを無効にできること
☐	侵入およびその試みを検出するために適切なサーバ動作のログを記録できること
☐	サーバおよびサーバ製品を管理する技能と経験を持ったスタッフの調達可能性
	メールサーバの設置場所の計画
☐	適切な物理的セキュリティ保護メカニズム
☐	温度や湿度の必要条件を維持する適切な環境調整機能
☐	予備電源
☐	既知の自然災害に対する備え

（本ページは意図的に白紙のままとする）

4. メールサーバのオペレーティングシステムのセキュリティ対策

メールサーバを侵害から保護するには、悪意を持つ者がメールサーバに直接攻撃を仕掛けることを防ぐために、メールサーバが稼働するオペレーティングシステム、メールサーバアプリケーション、およびネットワークのセキュリティを強化する必要がある。メールサーバのセキュリティを保護するための第 1 歩として、このセクションでは、メールサーバが稼働するオペレーティングシステムのセキュリティ強化について詳細に述べる（メールサーバアプリケーションおよびネットワークのセキュリティ確保については、それぞれセクション 6 および 7 で取り上げる）。

一般に利用可能なメールサーバは、すべて、汎用のオペレーティングシステム上で動作する。セキュリティに関する問題の多くは、メールサーバのオペレーティングシステムを適切に設定すれば避けることができる。製造元によって設定されるハードウェアおよびソフトウェアのデフォルト設定は一般に、セキュリティを犠牲にして特長や機能、利便性を強調するものになっていることが多い。製造元では、個別の組織におけるセキュリティニーズを把握できないため、メールサーバ管理者が各自で組織のセキュリティ要件に応じて新規サーバを設定したり、要件の変化に応じて既存サーバの設定を変更したりする必要がある。ここで推奨するプラクティスは、メールサーバ管理者が組織のセキュリティ要件を満たすメールサーバの設定と導入に役立てられるように構成されている[27]。既存のメールサーバを管理するメールサーバ管理者は、そのシステムが先に述べた事項に対応しているかどうか確認すべきである。

セキュリティを強化するためのテクニックは、オペレーティングシステムごとに大きく異なるため、このセクションでは、ほとんどのオペレーティングシステムのセキュリティ確保に共通する一般的な手順を説明する。さまざまなオペレーティングシステム向けに、セキュリティ設定ガイドやチェックリストが公に入手可能である。通常、そうした文書には、デフォルトのセキュリティレベルを改善するための推奨設定が記載されているほか、システムのセキュリティを確保するための具体的な手順が記載されていることもある[28]。また、組織固有の要件に応じて独自のガイドラインを用意している組織も多い。オペレーティングシステムのセキュリティを強化するための自動化ツールもいくつか存在しており、そうしたツールの使用は強く推奨される。

オペレーティングシステムの基本的なセキュリティを維持するには、次の 5 つの基本手順が必要である。

1. メールサーバ用ホストオペレーティングシステムおよびその他コンポーネントのインストールと導入の計画を立てる
2. 必要に応じてホストオペレーティングシステムへのパッチの適用および更新を行う
3. 適切なセキュリティ対策のためにホストオペレーティングシステムの強化・設定を行う
4. 追加的なセキュリティ管理策をインストールおよび設定する（必要な場合）

---

[27] Web ベースのメールアクセスを提供する場合、管理者は、関連する Web サーバ（オペレーティングシステム、Web サーバソフトウェア）についてもセキュリティを適切に確保する必要がある。詳細については、NIST SP 800-44『*Guidelines on Securing Public Web Servers*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

[28] NIST が発行する、各種オペレーティングシステムやアプリケーションのチェックリストおよび実装ガイドは、http://checklists.nist.gov/ から入手することができる。NIST のチェックリストプログラムについては、同 Web サイトにある NIST SP 800-70『*IT 製品のためのセキュリティ設定チェックリストプログラム (Security Configuration Checklists Program for IT Products)*』を参照のこと。

5. 上記 4 つの手順でセキュリティ上のすべての課題が十分に対策されていることを確認するために、ホストオペレーティングシステムをテストする

手順 1 については、4.1 項で説明したとおりである。その他の手順については、5.1 項および 5.2 項で述べる。

4.1 オペレーティングシステムの更新および設定

この項では、上記の手順 2～4 について概要を説明する。これらの手順を組み合わせることにより、メールサーバのオペレーティングシステムについて、十分な保護を確保できるはずである。

4.1.1 オペレーティングシステムへのパッチの適用と更新

オペレーティングシステムをインストールした後は、既知の脆弱性を修正するために必要なパッチの適用または更新を行うことが不可欠である。どのようなオペレーティングシステムにも既知の脆弱性は存在するため、メールサーバのホストオペレーティングシステムとして使用する前にそれらを修正しなければならない。脆弱性の検出および修正を適切に行うために、メールサーバ管理者は次を実行すべきである。

- パッチ適用プロセスの策定・導入[29]
- 脆弱性および該当するパッチの特定[30]
- 必要があり、かつ、可能であれば、（パッチを入手し、テストおよびインストールを行うまでの間）一時的に脆弱性を緩和させる
- 恒久的な修正（パッチ、ホットフィックス、サービスパック、更新プログラムなどと呼ばれる）のインストール

管理者は、パッチ適用作業中のメールサーバ（特に新設のもの）が十分に保護されるよう留意しなければならない。たとえば、パッチの適用がまだ完全ではないあるいは、セキュリティ設定がされてないメールサーバが、パッチ適用中に外部からアクセス可能な状態におかれると、脅威による侵害を受ける可能性がある。管理者は、新しいメールサーバの導入に向けて準備する際には、次のいずれかに従うべきである。

- すべてのパッチをネットワーク以外の手段（CD など）によりサーバに転送してインストールを完了し、5.1 項に示すその他の設定手順が完了するまで、サーバはネットワークに接続しないか、隔離された「保守用」ネットワークにのみ接続する。
- 仮想ローカルエリアネットワーク（VLAN）上、または、ネットワーク上のホストが実行できる操作やホストに対する通信を厳重に制限できるようなその他のネットワークセグメント上にサーバを配置し、ホストへのパッチの適用および設定を行うのに必要なイベントだけを許可するようにする。5.1 項に示す全ての設定手順が完了するまで、通常のネットワークセグメントには移行しない。

---

[29] 詳細については、NIST SP 800-40 Version 2.0『*パッチおよび脆弱性管理プログラムの策定（Creating a Patch and Vulnerability Management Program）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。オペレーティングシステムとアプリケーション（メールサーバおよびクライアントソフトウェアを含む）の両方を単一のパッチ管理プロセスによって管理してもよい。

[30] オペレーティングシステム、サービス、およびその他のアプリケーションに存在する脆弱性については、NIST National Vulnerability Database（米国国家脆弱性データベース、以下、NVD と称す）（http://nvd.nist.gov/）で確認できる。

一般に、メールサーバへのパッチの適用は、まず同じ設定を持つ別のサーバに適用してテストした後に行うべきである。これは、意図しない運用上の問題がパッチによって発生することがあるためである。パッチを自動的にダウンロードするようにメールサーバを設定してもよいが、テストを行うことなく自動的にパッチが適用されるようには設定すべきでない。

4.1.2 不要なサービスおよびアプリケーションの削除または無効化

メールサーバは、専用の単一の用途に使われるホストで運用するのが理想的である。オペレーティングシステムを設定する際には、明示的に許可するもの以外はすべて無効にする。すなわち、すべてのサービスとアプリケーションをいったん無効にし、メールサーバに必要なものだけを有効にしてから、不要なサービスおよびアプリケーションを削除する。可能であれば、オペレーティングシステムのインストールは、メールサーバアプリケーションに必要な最小限の設定で行うことが望ましい。「最小インストール」の選択肢がある場合はそれを選択することで、不要なサービスを削除する手間を最小化する。アンインストールを実行するスクリプトやプログラムは不完全なものが多く、サービスの全てのコンポーネントが完全に削除されない場合があるため、通常、不要なサービスは最初からインストールしないのが望ましい。一般的な種類のサービスおよびアプリケーションのうち次のようなものは、必要でなければ通常は無効にすべきである。

- ファイルおよびプリンタの共有サービス（Windows Network Basic Input/Output System [NetBIOS]ファイルとプリンタ共有、Network File System [NFS]、File Transfer Protocol [FTP]）
- デフォルトの Web サーバ
- ワイヤレスネットワークサービス
- リモート制御およびリモートアクセスプログラム、特に、通信に強力な暗号化を使用しないもの（Telnet など）[31]
- ディレクトリサービス（Lightweight Directory Access Protocol [LDAP]、Kerberos、Network Information System [NIS]など）
- プログラミング言語のコンパイラおよびライブラリ
- システム開発ツール
- システムやネットワークの管理ツールおよびユーティリティ（SNMP (Simple Network Management Protocol)など）

不要なサービスやアプリケーションは、単に設定で無効にするのではなく削除することが望ましい。設定を変更することにより、無効になっているサービスを有効にしようと試みる攻撃は、該当する機能コンポーネントが完全に削除されていれば成功し得ないからである。また、無効にしたサービスは、人為的ミスにより有効になる可能性もある。

不要なサービスを削除または無効化することにより、次のようにいくつかの面でメールサーバのセキュリティが強化される。[Alle00]

- 有効になっていないサービスが侵害されることはないため、それを使用してホストを攻撃したり、メールサーバのサービスを妨害したりすることはできない。ホストのサービスが 1 つ増えるごとに、

[31] 通信に強力な暗号化を使用しないリモート制御またはリモートアクセスプログラムが不可欠な場合は、SSH（Secure Shell）や IPSec（IP Security）など暗号化機能を持つプロトコルを使用して、通信をトンネルさせるべきである。

攻撃者のアクセスに使用される可能性のある経路が 1 つ増えることになるため、ホストが侵害されるリスクが高くなる。この場合、サービスの数が少ない方が、安全性が高い。

- 不要なサービスに欠陥が含まれている可能性や、メールサーバ自体との互換性に問題がある可能性があるため、不要なサービスを無効化または削除することにより、それらがメールサーバやその可用性に影響を与えることが防止される。
- ホストが、特定のサービスの要件により適合するように設定される可能性がある。サービスによっては、要求されるハードウェアおよびソフトウェアの設定が異なる場合があり、それが、不要な脆弱性につながったり、パフォーマンスに悪影響を及ぼしたりする可能性がある。
- サービスを減らすことで、ログおよびログ項目の数が減り、予期しない動作を発見しやすくなる（セクション 9）。

メールサーバでいずれのサービスを有効にするかについては、組織として決定しておくべきである。メールサーバサービスに加えてインストールする可能性のあるサービスとしては、組織のユーザディレクトリにアクセスするためのディレクトリプロトコルや、リモート管理サービスなどがある。こうしたサービスは、場合によっては必要であるが、サーバのリスクが高くなる可能性もある。リスクの大きさがメリットを上回るかどうかは、組織ごとに判断する必要がある。

Web ベースのメールアクセスを提供する場合、メールアプリケーションを実行する Web サーバは、メールサーバとは別のホストに配置すべきである。Web サーバとメールサーバのホストを別々にしておくことにより、両サーバが同一ホスト上で動作する場合に比べ、いずれかが侵害された場合の影響を限定することができる。Web サーバとメールサーバを同一ホスト上で動作させた場合、両サーバがネットワークを経由せず、同一ホスト内で直接通信することができるため、通信の効率と保護の点でメリットがある。

4.1.3 オペレーティングシステムのユーザ認証に関する設定

メールサーバの場合、オペレーティングシステムの設定を行うことができるユーザは、指名された少数のメールサーバ管理者に限られる。一方、メールサーバにアクセスできるユーザの数は、無制限の場合もあれば、組織の職員の一部である場合もある。ポリシーによる制限を適用するために、メールサーバ管理者は、必要があれば、アクセスを許可されていることの証拠をユーザに要求することにより、ユーザ認証を行うようにオペレーティングシステムを設定する必要がある。

ホストコンピュータでの認証を有効にするには、オペレーティングシステム、ファームウェア、およびアプリケーション（ネットワークサービスを実装するソフトウェアなど）の設定を部分的に変更する。高価値／高リスクサイトの特殊なケースにおいては、トークンやワンタイムパスワード装置などの認証用ハードウェアを使用することも考えられる。認証情報（パスワードなど）が再利用可能であったり、認証情報を平文でネットワークに送信するような認証メカニズムの使用は避けることを強く推奨する。これは、攻撃者が認証情報を傍受し、許可されたユーザになりすます可能性があるためである。

適切なユーザ認証を確実に機能させるには、次の手順を実行する。[Alle00]

- **不要なデフォルトのアカウントおよびグループを削除または無効化する。**オペレーティングシステムには、デフォルトで、ゲストアカウント（パスワードあり／なし）、管理者または root レベルのアカウント、および、ローカルサービスやネットワークサービスに関連付けられたアカウントが含まれていることが多い。そうしたアカウントの名前とパスワードはよく知られている。機密性の高い情報が格納されているコンピュータのゲストアカウントなど、不要なアカウントは、攻撃者に使用されるのを防ぐため削除または無効化する。ゲストのアカウントまたはグループを残しておく

必要がある場合は、当該アカウントのアクセスを厳しく制限し、また、組織のパスワードポリシーに従ってデフォルトのパスワードを変更すること。デフォルトアカウントを残す必要がある場合は、アカウント名を変更し（可能な場合。特に、管理者または root レベルのアカウント名は必ず変更すべき）、パスワードも組織のパスワードポリシーに従って変更する。デフォルトアカウントの名前とパスワードは、攻撃者コミュニティではよく知られている。

- **インタラクティブでないアカウントを無効にする。**存在が必要であってもインタラクティブにログインする必要がないアカウント（および対応するパスワード）は無効化する。Unix システムの場合、ログインシェルを無効化するか、ヌル機能のログインシェルを指定する（/bin/false など）。

- **ユーザグループを作成する。**ユーザを適切なグループに割り当てる。その後、導入計画に記載してあるとおりにグループの権限を割り当てる。個別のユーザに権限を割り当てる方法は、ユーザ数が多い場合には現実的でないため、グループに権限を割り当てる方法の方が望ましい。

- **ユーザアカウントを作成する。**導入計画には、いずれのユーザに対していずれのコンピュータおよびサービスの使用を許可するかが明記されている。作成するアカウントは必要なものだけにすること。アカウントの共用は、ほかに実際的な代替手段がない場合に限って認めること。

- **組織のパスワードポリシーを確認する。**アカウントのパスワードは、ポリシーに従って設定する。このポリシーは、次の事項について言及したものであるべきである。

  – **長さ** — パスワードの最低限の長さ。少なくとも 8 文字を要求すること。

  – **複雑さ** — 使用する文字種の要件。アルファベットの大文字／小文字を併用することと、少なくとも 1 つは英数字以外の文字を使用することを必須とし、「一般的な」単語[32]の使用を禁止すること。

  – **有効期間** — 1 つのパスワードを変更せず使用し続けてよい期間。ユーザにはパスワードを定期的に変更するよう要求すること。管理者または root レベルのパスワードは、30～120 日ごとに変更すべきである。ユーザレベルのパスワードも定期的に変更すべきだが、その間隔は、保護する情報の機密性に応じて要求されるパスワードの長さおよび複雑さによって決定する。適切な有効期間を決定する際には、ユーザパスワードがどの程度露出するかについても考慮すること。

  – **再利用性** — パスワードを再使用してよいかどうか。ユーザによっては、以前に使用したのと同じパスワードを指定することで有効期間を回避しようと試みることがある。可能であれば、元のパスワードの先頭または末尾に文字を追加しただけのパスワードを使用できないようにすること（たとえば、元のパスワードが「mysecret」である場合、変更後のパスワードを「1mysecret」や「mysecret1」にすることは許可しない）。

  – **許可権者** — どのユーザがパスワードの変更またはリセットを実行できるのか。また、変更操作を開始する場合にどのような証明を要求するか。

  – **パスワードのセキュリティ** — パスワードをどのような方法で保護するか。たとえば、パスワードをメールサーバ上に暗号化せず格納することの禁止や、管理者がメール管理用アカウントとその他の管理用アカウントに同じパスワードを使用することなどを禁止する。

- **パスワードを推測されないようにコンピュータを設定する。**権限のないユーザがコンピュータにアクセスしようとする際、自動化したソフトウェアツールを使用してあらゆるパスワードを試すの

---

[32] 辞書や単語表に記載されている可能性があるすべての人名、地名、専門用語、単語を含む。

は比較的容易である。ログインの失敗後に再試行を許すまでの時間の長さをオペレーティングシステムの設定により変更できる場合は、これを延長すること。そのような設定ができない場合は、代替策として、ログインの失敗が一定回数（たとえば 3 回）に達したらログインを拒否するように設定する。通常、規定の回数だけログインに失敗したアカウントは、一定時間（たとえば 30 分）にわたって、または適切な権限を持つ者が、アカウントを再度有効化するまで「締め出される」。

ログインを拒否するようにするかどうかは、メールサーバ管理者がセキュリティと利便性のバランスを考慮して決定を下す必要がある状況の別の一例である。この推奨事項を実施することにより、ある種の攻撃を防ぐことが期待できる一方、ログイン試行の失敗を繰り返すことでユーザのアクセスを妨げ、結果的にサービス運用妨害（DoS）と同様の状況を作り出すことを攻撃者に許す可能性もある。

ネットワークログインの失敗によって、権限を有するユーザや管理者がコンソールからログインすることが妨げられるべきではない。ただし、ネットワーク経由かコンソールかにかかわらず、ログイン試行の失敗はすべてログに記録されるべきである。リモート管理を実装しない場合は（8.5 項を参照）、管理者または root レベルアカウントによるネットワーク経由のログインを無効にしておくこと。

- **その他のセキュリティメカニズムをインストール・設定することにより認証を強化する。**メールサーバ上に置かれる情報の内容に応じて、必要であれば、その他の認証メカニズム（バイオメトリクス、スマートカード、クライアント／サーバ証明書、ワンタイムパスワードシステムなど）の使用を検討すること。これには多くの費用がかかり、実装にも困難を伴うが、状況によってはそれが正当化されることもある。そのような認証メカニズムや装置を使用する場合は、それに合わせて組織のポリシーを変更すべきである。

すでに述べたように、ネットワークを平文で伝送されるパスワードは、攻撃者がネットワークスニファを使用して容易に傍受することができる。とはいえ、伝送時の保護が適切であれば、パスワードは経済的かつ有効なメカニズムである。伝送中のパスワードを保護するためには、認証および暗号化テクノロジーとして、SSL(Secure Sockets Layer)／TLS(Transport Layer Security)、SSH(Secure Shell)、または VPN(仮想プライベートネットワーク)（リモートユーザ用）などを実装する。サーバサイド認証と暗号化テクノロジーを組み合わせて使用することを必須にすれば、中間者攻撃の成功する可能性を低下させることができる。

4.1.4 リソース制御の適切な設定

一般に普及している最近のサーバオペレーティングシステムはすべて、個々のファイル、ディレクトリ、装置、その他のコンピュータリソースに対して個別にアクセス権限を指定する機能を備えている。アクセス制御を注意深く設定し、アクセス権限のない者を受け付けないようにすることにより、セキュリティ侵害を減らすことができる。たとえば、ファイルおよびディレクトリに対する読み取りアクセスを拒否すれば情報の機密性の保護に役立ち、不要な書き込み（変更）アクセスを拒否すれば情報の完全性の維持に役立つ。システム関連ツールのほとんどについて、権限を有するシステム管理者にのみ実行権限を与えることによって、ユーザが、セキュリティを低下させる可能性のある設定変更を行うことを防止することができる。また、それらのツールを攻撃者が利用して当該システムやネットワーク上にある他のシステムを攻撃する能力を制限することができる。

4.1.5 追加的なセキュリティ管理策のインストールおよび設定

オペレーティングシステム、サービス、およびアプリケーションのセキュリティを十分に確保するために必要な全てのセキュリティ管理策を、オペレーティングシステムは備えていない場合が多い。不足している管理策を補うには、管理者が追加ソフトウェアを選定、インストール、および設定する必要がある。一般的に追加が必要となる管理策の例を次に示す。

- マルウェア対策ソフトウェア：ウイルス対策ソフトウェア、スパイウェア対策ソフトウェア、ルートキット検出ソフトウェアなど。ローカルオペレーティングシステムをマルウェアから守り、マルウエアに感染した場合には、その検知・除去を行うために使用する[33]。マルウェア対策ソフトウェアが役立つ状況の例としては、感染したメディアがメール管理者によってメールサーバに持ち込まれた場合や、ネットワークサービスワームがサーバにアクセスし、感染しようとした場合などが考えられる。このソフトウェアは、メールサーバを通過する電子メールをスキャンするためのマルウェア対策ソフトウェアとは無関係である。多くのメールシステムにとっては、OS を保護するために必要なマルウェア対策ソフトウェアはウイルス対策ソフトウェアのみである。
- ホストベースの侵入検知および侵入防止ソフトウェア：メールサーバに対して実行される攻撃を検出するために使用する。7.2.2 項に、ホストベースの侵入検知および侵入防止ソフトウェアに関する補足情報を示す。
- ホストベースのファイアウォール：不正アクセスからサーバを保護するために使用する[34]。
- パッチ管理ソフトウェア：脆弱性に迅速に対処するために使用する。パッチ管理ソフトウェアを使用してパッチの適用だけを行う場合と、メールサーバのオペレーティングシステム、サービス、アプリケーションにおいて新しく発見される脆弱性を特定する目的にも使用する場合がある。

一つまたはそれ以上のホストベースの侵入検知ソフトウェアをサーバにインストールしているメールサーバ管理者もいる。たとえば、ファイルの完全性チェック用ソフトウェアを使用すると、重要なシステムファイルに加えられた変更を特定することができる。

セキュリティ管理策の計画を策定する際、メールサーバ管理者は、セキュリティ管理策の実行に必要となるリソースについても考慮すべきである。管理策を実行するための十分なメモリと処理能力をサーバが備えていなければ、サーバのパフォーマンスが低下する可能性がある。

4.2 オペレーティングシステムのセキュリティテスト

定期的にオペレーティングシステムのセキュリティテストを行うことは、脆弱性を発見するため、および、導入済みのセキュリティ対策が有効に機能していることを確認するために不可欠な方法の一つである。オペレーティングシステムのテスト方法として、脆弱性スキャンおよびペネトレーションテストがある。脆弱性スキャンでは、通常、自動化された脆弱性スキャナを使用して 1 台のホストまたはネットワーク上のホストグループをスキャンし、アプリケーション、ネットワーク、オペレーティングシステムに存在する脆弱性を検出する。ペネトレーションテストは、攻撃者のツールおよび手法を使用してネットワークを侵害するよう設計されたテストプロセスである。ネットワークの最も弱い部分を反復的に特定して悪用し、ネットワークの残りの部分へのアクセスを獲得し、最終的には、ネットワークの

---

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

[34] ファイアウォールの詳細については、NIST SP 800-41『*Guidelines on Firewalls and Firewall Policy*』(http://csrc.nist.gov/publications/nistpubs/)を参照のこと。

全てのセキュリティを侵害する。脆弱性スキャンは、定期的に（毎週、毎月など）実施すべきであり、ペネトレーションテストは少なくとも年に 1 回実施すべきである。これらのテストテクニックは、メールサーバアプリケーションのテストにも適用できるため、これについては 8.4 項でも詳細に述べる[35]。

4.3 メールサーバのオペレーティングシステムのセキュリティ確保チェックリスト

完了	アクション
	オペレーティングシステムへのパッチの適用と更新
☐	パッチ適用プロセスの策定・導入
☐	オペレーティングシステムに必要な全てのパッチおよび更新プログラムの特定・テスト・インストール
	不要なサービスおよびアプリケーションの削除または無効化
☐	不要なサービスおよびアプリケーションの削除または無効化
☐	Web サーバ、ディレクトリサーバ、そのほかのサーバに別々のホストを使用する
	オペレーティングシステムのユーザ認証の設定
☐	不要なデフォルトのアカウントおよびグループの削除または無効化
☐	インタラクティブでないアカウントの無効化
☐	対象コンピュータにおいてユーザグループを作成する
☐	対象コンピュータ用においてユーザアカウントを作成する
☐	組織のパスワードポリシーを確認し、適切な（長さ、複雑さなど）アカウントパスワードを設定する
☐	パスワードを推測されないようにコンピュータを設定する
☐	その他のセキュリティメカニズムのインストール・設定により、認証を強化する
	リソース制御の適切な設定
☐	ファイル、ディレクトリ、装置、そのほかのリソースのアクセス制御を設定する
☐	ほとんどのシステム関連ツールの利用権限を権限を有するシステム管理者にのみ限定する
	追加的なセキュリティ管理策のインストールおよび設定
☐	オペレーティングシステムが備えていない必要な管理策を提供するために、追加ソフトウェアの選定・インストール・設定を行う
	オペレーティングシステムを対象としたセキュリティテストの実施
☐	初期インストール後のオペレーティングシステムを対象にテストを行い、脆弱性を検出する
☐	オペレーティングシステムを対象に定期的にテストを行い、新たな脆弱性を検出する

[35] これら、およびその他のテストテクニックの詳細については、NIST SP 800-42『*ネットワークセキュリティテストにおけるガイドライン（Guideline on Network Security Testing）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

5. メールサーバおよびコンテンツのセキュリティ保護

メールサーバアプリケーションのセキュリティを強化することは、メールサーバを侵害から守るための重要な手順の 1 つである。このセクションでは、セキュリティに配慮したメールサーバのインストールおよび、オペレーティングシステムとメールサーバのアクセス制御の設定のための推奨事項を示す。また、サーバによって伝送される電子メールコンテンツの保護(コンテンツのフィルタリング、マルウェアのスキャン、スパム対策など)もメールセキュリティの重要な要素である。通信の暗号化(Web ベースのメールアクセスを含む)によるメールボックスへのアクセスのセキュリティ保護についても、このセクションで述べる。電子メールコンテンツのセキュリティには、機密性を維持するための電子メール暗号化と、完全性および否認防止をサポートするためのディジタル署名も使用される。これらについてはセクション 3 で説明した。

5.1 メールサーバアプリケーションのセキュリティ強化

メールサーバのオペレーティングシステムのセキュリティ対策を確実に実施した後に、メールサーバアプリケーションをインストールし、発生の可能性が高い脅威に対するセキュリティ対策を実施する。これら 2 つのアクションについて、以降の各項で概要を説明する。

5.1.1 セキュリティに配慮したメールサーバのインストール

メールサーバアプリケーションのインストールおよび設定におけるセキュリティ上の推奨事項は、セクション 4 に示した、オペレーティングシステムに関するプロセスと多くの面で共通である。ここでも、基本的な考え方として、メールサーバに必要なサービスだけをインストールし、パッチや更新を通じて既知の脆弱性をすべて排除することが重要である。不要なアプリケーション、サービス、またはスクリプトがインストールされた場合は、インストールプロセスの完了後、それらを直ちに削除するべきである。メールサーバのインストール時には、次の手順を実行すべきである。

- 専用のホストにメールサーバをインストールする
- 既知の脆弱性を修正するパッチまたは更新プログラムをすべて適用する
- メールボックス専用の(オペレーティングシステムやメールサーバアプリケーションとは分離した)物理ディスクまたは論理パーティションを作成するか、メールボックスを別のサーバでホストする
- メールサーバアプリケーションによってインストールされたサービスのうち不要なもの(Web ベースのメール、FTP、リモート管理など)をすべて削除または無効化する
- メールサーバのインストール時に作成された不要なデフォルトのログインアカウントをすべて削除または無効化する
- メーカーの文書をサーバからすべて削除する
- サンプルおよびテスト用ファイルをサーバからすべて削除する
- 適切なセキュリティテンプレートまたはセキュリティ強化スクリプトをサーバに適用する
- SMTP、POP、IMAP サービスのバナー(必要に応じて別の箇所も)の設定を変更し、メールサーバやオペレーティングシステムの種類とバージョンを表示しないようにする(メールサーバの種類によっては不可能な場合がある)
- 危険性のあるメールコマンドや不要なメールコマンドを無効化する(VRFY、EXPN など)

5.1.2 オペレーティングシステムおよびメールサーバのアクセス制御の設定

ほとんどのサーバホストオペレーティングシステムは、当該ホスト上にある個々のファイル、装置、その他のコンピュータリソースに対して個別にアクセス権限を指定する機能を備えている。これらの管理策を利用してメールサーバからアクセスできるすべての情報は、潜在的に、メールサーバにアクセスするすべてのユーザに配布される可能性がある。メールサーバソフトウェアには、その運用形態に応じて、ファイル、装置、リソースに対する追加的なアクセス制御を提供するメカニズムが組み込まれていることが多い。オペレーティングシステムとメールサーバアプリケーションには、同一内容のアクセス許可を設定することが重要である。そうでなければ、ユーザには、過剰または過小なアクセス権限が付与される可能性がある。メールサーバ管理者は、自組織の公開メールサーバに格納されている情報を保護するためにアクセス制御をどのように設定するのが最善であるかを、次の 2 つの観点から検討すべきである。

- メールサーバアプリケーションからアクセスできる範囲をコンピュータリソースのサブセットに限定する
- より詳細なレベルのアクセス制御が必要な場合は、メールサーバによって適用される追加的なアクセス制御を使用してユーザのアクセスを限定する

アクセス制御を適切に設定することは、一般への公開を意図していない機密または制約のある情報が開示されるのを防ぐために役立つ。また、メールサーバに対して DoS 攻撃が行われた場合のリソース消費を制限するためにも、アクセス制御は有効である。

アクセス制御の対象とすべき代表的なファイルとしては次のようなものがある。

- アプリケーションソフトウェアおよび設定ファイル
- セキュリティメカニズムに直接関係するファイル
  - 認証に使用されるパスワードハッシュファイルおよびその他のファイル
  - アクセス制御に使用される権限情報を含むファイル
  - 機密性、完全性、否認防止のサービスに使用される暗号鍵素材
- サーバのログファイルおよびシステム監査ファイル
- システムソフトウェアおよび設定ファイル

メールサーバアプリケーションが、非常に厳しいアクセス制限が課せられた固有のユーザ ID およびグループ ID のもとにおいてのみ実行されるようにすること。そのために、メールサーバソフトウェア専用の新しいユーザ ID とグループ ID の作成が必要となる。このユーザおよびグループは、他のすべてのユーザおよびグループと無関係な固有のものとすべきである。これは、次に示す手順におけるアクセス制御を実装する前提条件となる。サーバが必要な TCP ポートにバインドするために、最初は root（Unix）または Administrator／System（Windows）の権限で動作する必要がある場合でも、そのアクセスレベルのままで動作が継続するようにしてはならない。

さらに、メールサービスのプロセスからアクセスできるファイルを、メールサーバのオペレーティングシステムを使用して制限する。メールサービスのプロセスには、サービスの実行に必要なファイルに対する読み取り専用アクセス権限を与え、その他のファイル（サーバのログファイルなど）に対するアクセス権限はいっさい付与しない。また、メールサーバホストのオペレーティングシステムに備わっているアクセス制御を使用して、次の制限を適用する。

■ メールサーバアプリケーションによって作成される一時ファイルは、適切に保護された特定のサブディレクトリに配置する（可能な場合）

■ メールサーバアプリケーションによって作成される一時ファイルに対しては、当該ファイルを作成したメールサーバプロセスに限りアクセスを許可する（可能な場合）

メールサーバに対して専用に割り当てられている指定のファイル階層構造の外にファイルを保存できないようにすることも必要である。これは、サーバソフトウェアの設定を選択すること、あるいは、オペレーティングシステムがサーバプロセスを制御する方法を選択することにより行う。指定のディレクトリ階層の外にあるディレクトリやファイルの場所を知っているユーザであっても、それらのディレクトリやファイルへのアクセスが不可能であるようにしておくこと。

Linux および Unix のホストにおいては、メールサーバアプリケーションに対して「chroot jail 」の適用を検討すべきである。chroot を使用し、メールサーバがホストファイルシステムを参照する際の「視界」を変更して、真のファイルシステムのルートディレクトリではなく、ファイルシステムの一部のディレクトリを、ルートディレクトリに見せかけることができる。その結果、攻撃者がメールサーバの侵害に成功しても、chroot によりアクセス可能な、限定された一部のファイルシステムにしかアクセスできない。これは非常に強力なセキュリティ対策である。

特定の種類の DoS 攻撃による影響を低減するには、メールサーバの設定により、メールサーバが使用できるオペレーティングシステムリソースの量を制限する。たとえば、次のような設定が考えられる。

■ ユーザのメールボックスを、オペレーティングシステムやメールサーバアプリケーションとは別のサーバ（推奨）、別のハードディスク、または別の論理パーティションにインストールする

■ ハードディスクまたはパーティションの空き領域を全て使い切ることがないように、メールサーバアプリケーションを設定する

■ 添付ファイルの許容サイズを制限する

■ ログファイルの格納場所に十分なサイズを確保する

システムクラッシュの原因となり得る外部からの不適切な情報でメールサーバのホストオペレーティングシステムのファイルシステムを占有しようとする攻撃は、これらの対策によってある程度防御することができる。また、不要なプロセスによって主記憶装置(primary random access memory)を占有し、システムのパフォーマンス低下やクラッシュを発生させてメールサーバの可用性を制限しようとする攻撃に対しても有効な防御となる。このような攻撃を認識するには、メールサーバホストのオペレーティングシステムによって記録されるログ情報が役立つ。9.1 項で述べるように、可能な限りメールサーバのログは集中化されたログサーバに格納し、さらに、現実的に可能であればローカルにもログを記録すべきである。攻撃によってメールサーバが侵害された場合、ローカル環境にあるログは、攻撃に関する情報を隠蔽するために改ざんまたは消去される可能性がある。そのような場合、集中化されたログサーバにログのコピーが残っていれば、管理者がメールサーバの侵害を調査する際により多くの情報を得ることができる。

5.2 マルウェアからの電子メールの保護

電子メールは、バイナリファイルを添付ファイルとして送信するための手段として使用されることが多くなっている。当初、添付ファイルはサイズの小さいワードプロセッサ文書や写真などがほとんどであったため、深刻なセキュリティ上のリスクを生じることはなかった。しかし、日々の共同作業に電子メールを使用する組織が増えるにつれ、添付ファイルのサイズは増大し、種類も多様になった。

現在、送信される多くの電子メールメッセージに、実行可能ファイル、画像、音楽、音声などのファイルが添付されている。ウイルス、ワーム、トロイの木馬、スパイウェアなどさまざまな形態の多くのマルウェア（ユーザのプライバシ侵害を目的とするもの）も、添付ファイルとして伝送される。さらに、まだ広く知れわたる前の脆弱性を利用し、特定の組織を狙ったゼロデイ攻撃を送り込む手段として電子メールが利用されることが増えている。ゼロデイ攻撃は、ユーザのワークステーションの制御を奪うために、しばしばオフィス生産性ソフトウェアを標的として行われる。制御権を掌握した攻撃者は、それを利用して、権限の昇格、機密情報へのアクセス、ユーザによるアクション（キー入力など）の監視など、悪意のある行為を実行する。

特定の種類のファイルの添付を許可するかについては、場合によっては難しい判断が必要となる。いっさいの添付ファイルを禁止すると、システムを単純化することができ、セキュリティも向上すると考えられるが、同時に利便性も著しく損なわれ、職員は「用件を済ませる」ためにエンコーディングの工夫などで制約を回避しようとする可能性がある。したがって、最終的には、少なくとも電子メールへの何らかの添付ファイルを認めることになる。

組織は、許可する添付ファイルの種類を決定しておくべきである。最も単純なアプローチは、すべての添付ファイルを許可することであるが、その場合は、既知のマルウェアの侵入を防ぐために何らかのマルウェアスキャナ（ウイルス対策ソフトウェア、スパイウェア対策ソフトウェアなど）をメール伝送経路にインストールすべきである。また、添付された実行可能ファイルによる無用な操作が実行されるのを防ぐために、動作をブロックする何らかのユーティリティをクライアントにインストールすることなども考えられる。よりよいアプローチとしては、潜在的な危険性のある種類の添付ファイル（拡張子.vbs、.ws、.wsc を持つファイルなど）を、メールサーバまたはメールゲートウェイでフィルタ処理し、許可された種類のファイルについてはマルウェアスキャンを実行するという方法がある。このような拡張子を持つファイルをフィルタリングするのは、対策の出発点としてはよいが、攻撃者が拡張子を変更する可能性があるため、その有効性は限られる。添付ファイルのフィルタリングでは、ファイルの拡張子をチェックするだけでなく、ファイルのヘッダやフッタ、その他ファイルの種類の判定材料となる情報を可能な限りチェックすべきである。また、電子メールの送信元が当該組織内または組織外のいずれであるか、あるいは、信頼できる組織かどうか（たとえば、.gov や.milドメインであれば信頼するなど）によって、異なるルールを設定することも考えられる。ただし、後者の場合、電子メールアドレスのなりすましに注意が必要である。

添付ファイルのフィルタリングに完全な有効性を発揮させるには、すべての添付ファイルをブロックしなければならないが、それは現実的ではない。最も有用な種類の添付ファイル（オフィス生産性スイートのファイルなど）の一部は、最もリスクの高い部類にも入る。また、高度な攻撃者は、さまざまな方法で添付ファイルの真の悪質性を隠蔽することができる。たとえば、電子メールにはハイパーリンクを含め、その参照先であるリモート Web サイトに悪質なファイルを置くことがある。ハイパーリンクが HTTP でなくHTTPS であれば、ユーザがこれをクリックすると悪意のあるファイルは、HTTPS で保護されてダウンロードされるため、ネットワークベースのセキュリティ管理策による検出から回避される。このような手口を防ぐために、電子メールメッセージに記載されたアクティブなハイパーリンクをフィルタリングすることは可能であるが、ユーザにとっての利便性が低下しかねない。また、ファイルを添付する代わりにファイルへのハイパーリンクを記載する方法は、メールサーバの負荷を軽減するため、むしろ望ましいと考えられる場合もある。

添付ファイルについては、許容する最大ファイルサイズに制限を設けることも検討すべきである。これには、メールキュー遅延、必要なストレージ容量、サーバプロセッサの性能要件の低減など、メールサーバにとっていくつかの面でメリットがある。これらのメリットを総合すれば、サイズの大きいメッセージの大量送付による DoS 攻撃が成功する可能性を低減することができる。[Mell05] ただし、添

付ファイルサイズの上限を低く設定すると、意図に反して正当な内容までブロックし、メールシステムの利便性と価値を低下させるおそれがある。

電子メールを暗号化することにより、フィルタ処理が困難または効果がないものとなりがちである。メールサーバや境界セキュリティ装置におけるフィルタリングは、それらが、メッセージを復号した後に、スキャンを行い、再び暗号化する能力を備えていない限り、暗号化されたメッセージに対しては効果がない。このような処理には、非常に高いパフォーマンスが求められるため、実効性が問題になる。また、この種のソリューションにおいては、プライバシなどにかかわる懸念も存在する。一般論として、暗号化を広範囲で使用する場合は、エンドポイント(メールクライアントユーザのワークステーション)においてフィルタリングを行うことになるが、これは迂回されやすい。

見落とされがちであるが、電子メールで送付されるマルウェアが侵入するもう 1 つの経路は、Web ブラウザを介してアクセスする個人メールアカウントである。組織内のコンピュータから個人メールアカウントへアクセスすることが適切かどうかを判断し、適切であると判断するのであれば、ユーザが個人アカウントにアクセスする際に組織の資産を危険にさらすことがないよう対策を講じる必要がある。

マルウェアは、添付ファイルに限らず、電子メールを使用して別の方法でも伝送される可能性がある。たとえば、多くのメールクライアントは HTML ベースのメッセージをサポートしている。HTML メッセージには、クライアントサイドスクリプト言語またはコントロールオブジェクトの形でアクティブコンテンツが含まれている場合が多く、それらによってクライアントが影響を受ける可能性がある。最も広く使われているアクティブコンテンツ形式は、ActiveX、Java、JavaScript、および VBScript (Visual Basic Script)である。電子メールメッセージ内のアクティブコンテンツ、またはアクティブコンテンツフォームを許可するか、ブロックするかを決定する必要がある[36]。また、HTML ベースのメッセージには、スパムメッセージやフィッシング攻撃など、望ましくない内容が含まれていることが多い[37]。フィッシングとは、コンピュータを使った詐欺の手段であり、個人をだまして、機微性の高い個人情報を開示させることを指す。たとえば、攻撃者は、あたかもオンライン企業やクレジットカード会社、金融機関などの有名な組織から送信されたかのように見える電子メールメッセージをユーザに送付する。その目的は、ユーザをだまして電子メールの内容に応答させ、個人情報を開示させることである。

メールサーバにマルウェアスキャンソフトウェア(ウイルス対策ソフトウェア、スパイウェア対策ソフトウェアなど)がインストールされていない、あるいは、インストールされていても効果を発揮していない場合、マルウェアがエンドユーザに与えるセキュリティ上の潜在的脅威は増大する。広く普及している一部のメールクライアントには、マルウェアがクライアントホストに感染し、ほかのユーザにマルウェアを伝送することに利用されるようなデフォルト設定がある。セクション 8 に、メールクライアントをのセキュリティを向上させるためのメールクライアントの設定に関する補足情報を示す。メールクライアントの設定だけでなく、メールクライアントホストでウイルス対策ソフトウェアおよび、可能であれば、その他のセキュリティテクノロジーを使用することも、電子メールによってもたらされる脅威から保護するために重要である。

6.2.1 項では、個別のメールクライアントとメール基盤の両方に対するマルウェアスキャンの必要性について述べる。6.2.2 項では、電子メールによってもたらされる脅威を防ぐために役立つコンテンツ

---

[36] アクティブコンテンツの詳細については、NIST SP 800-28『*Guidelines on Active Content and Mobile Code*』(http://csrc.nist.gov/publications/nistpubs/)を参照のこと。

[37] 電子メールにおける HTML の使用を制限(電子メールの送信と閲覧を書式なしテキストだけで行うよう義務付けるなど)すると、セキュリティ面でメリットがある反面、機能性を大幅に損なう可能性がある(グラフィック、ハイパーリンク、その他 HTML ベースの内容が無効にされたり、まったく使用できなかったりするなど)。機能面のデメリットよりもセキュリティ面のメリットが大きいと判断し、HTML ベースの電子メールを全面的にブロックしている組織もある。

フィルタリングテクノロジーについて述べる。テクノロジーを導入・設定するだけでなく、組織としてユーザ、特に、管理の及ばない外部でコンピュータを使用する在宅勤務者を対象としたトレーニングおよび意識向上活動を実施し、ユーザが悪意のある電子メールメッセージやその添付ファイルをより的確に認識し、適切に対処できるようにすることが重要である。これについては 6.2.3 項で述べる。

5.2.1 マルウェアスキャン

ウイルス、ワーム、およびその他の形態のマルウェアを防ぐには、電子メール配信プロセス内の 1 つまたは複数の地点にマルウエアスキャンを実装する必要がある。マルウェアスキャンは、ファイアウォール、メールリレー、または電子メールデータが組織のネットワークへ入るポイントであるメールゲートウェイアプライアンスのいずれかと、メールサーバ自体、および／またはエンドユーザのホストに実装することができる。いずれの選択肢にも、後述するようにそれぞれ固有の長所と短所がある。一般に、マルウェアスキャンは少なくとも 2 つのレベルーエンドユーザホストのレベルと、メールサーバまたはファイアウォール／メールリレー／メールゲートウェイのレベルーにおいて実装する必要があり、3 つのレベルすべてに実装することも検討すべきである。

多層のマルウェア防御を用意するにあたっては、異なるメーカーの製品を採用することを検討すべきである。複数メーカーの製品を併用することで最新の脅威をブロックできる可能性が高まる。これは、新しい脅威に対応するまでの時間がメーカーによって異なるため、最新の脅威が出現したときに、一定の期間（通常は数時間程度の差、場合によっては数日）、ある製品では別の製品よりもその脅威を早く検出することができるためである。使用している検出方法がメーカーによって異なるため、どのような種類の新しい脅威を検出する能力に優れているかは、製品によって異なる。

5.2.1.1 ファイアウォール、メールリレー、またはメールゲートウェイアプライアンスでのスキャン

第 1 の選択肢は、ファイアウォール（アプリケーションプロキシ）、メールリレー（図 5.1 を参照）、またはメールゲートウェイアプライアンスにおいてマルウェアをスキャンする方法で、この場合、組織のメールサーバに到達する前にメッセージが遮断される。スキャンを実行する装置は、TCP25 番ポートの SMTP 接続をリッスンし、個々のメッセージをスキャンして、マルウェアを含まないメッセージをメールサーバに転送する。この場合、メールサーバは、通常のポート 25 ではなく、特権ポート以外の未使用ポートをリッスンするよう設定する。このアプローチの短所は、SMTP ストリームを常にスキャンするため、ファイアウォール、メールリレーまたはメールゲートウェイのパフォーマンスが低下する可能性があることである。パフォーマンスに与える影響の大きさは、メール負荷（1 日に処理するおよその電子メール件数と、ピーク時のメール件数の両方）およびサービス品質要件により異なる。パフォーマンスを改善する 1 つの方法は、マルウェアスキャンを専用サーバに肩代わりさせることである。

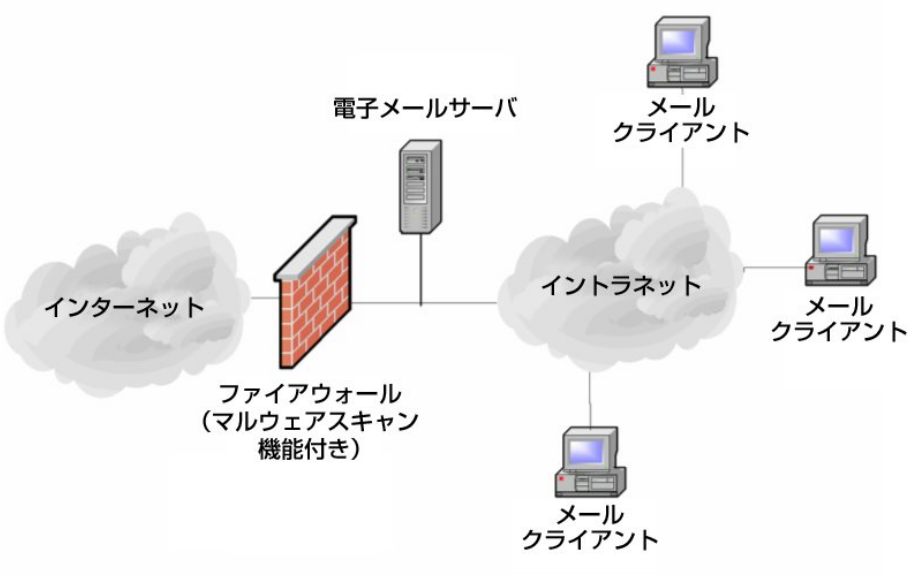

図 5.1：ファイアウォールのマルウェアスキャン実装

電子メールのスキャンをファイアウォール、メールリレー、またはメールゲートウェイアプライアンスにおいて実行することには、次のメリットがある。

- 双方向(組織外のネットワークから組織内のネットワークへの受信(inbound)および、組織内のネットワークから組織外のネットワークへの送信(outbound))について電子メールをスキャンすることができる
- マルウェアを含んだメッセージの大多数を、メッセージが組織内のネットワークに入り、メールサーバに転送される前に、ネットワークの境界部で遮断することができる
- 組織内に入ってくる電子メールのスキャンについては、既存のメールサーバの設定にあまり変更を加えず実装することができる
- メールサーバに到達する電子メールの量を削減することができるため、メールサーバをより低い運用コストでより効率的に運用することができる
- メールサーバが実行するスキャン処理の量が削減されるため、メールサーバの負荷が削減される
- スキャンを集中管理できるため、組織のセキュリティポリシーに対する適合性を確保することができ、また、悪意のあるコードの最新シグネチャを定期的に適用することができる
- 一部のメールファイアウォールアプライアンスでは、Web ベースのメールアプリケーションに対する安全な認証付きアクセスを提供することができる

マルウェアスキャンをファイアウォール、メールリレー、またはメールゲートウェイアプライアンスにおいて実行することには次のデメリットがある。

- 組織内から組織外へ送信される電子メールのスキャンについては、既存のメールサーバの設定に大幅な変更が必要となる可能性がある
- 暗号化された電子メールをスキャンすることができない

- 組織内部のネットワークにマルウェアが侵入したあとは、内部ユーザを保護する手段がない（SMTPトラフィックを専用スキャナに通してからメールサーバに転送するようネットワークが設定されている場合を除く）
- 大規模な組織の負荷を処理するには、高性能（高価）なサーバまたはアプライアンスが必要となる可能性がある

5.2.1.2 メールサーバ自体でのスキャン

メールマルウェアスキャナの設置に関する第 2 の選択肢は、メールサーバそのものへの設置である（図 5.2 を参照）。広く普及しているメールサーバのほとんどに対して、メッセージストアの内容をスキャンするサードパーティ製アプリケーションが多数存在する。それらのアプリケーションは、通常は、組織のファイアウォール、メールリレーまたはメールゲートウェイを通過しない、内部ユーザ間で送受信される電子メールを検査する。メールサーバにおいてスキャンを実行することは、マルウェアに対する保護層を追加することでもあり、内部でマルウェアが急激に拡散するのを防ぐために役立つ。メールサーバによってはアプリケーションプログラミングインタフェース（API）を備えており、マルウェアスキャン、コンテンツフィルタリング、添付ファイルのブロック、その他のセキュリティサービスの MTA への統合をサポートする。

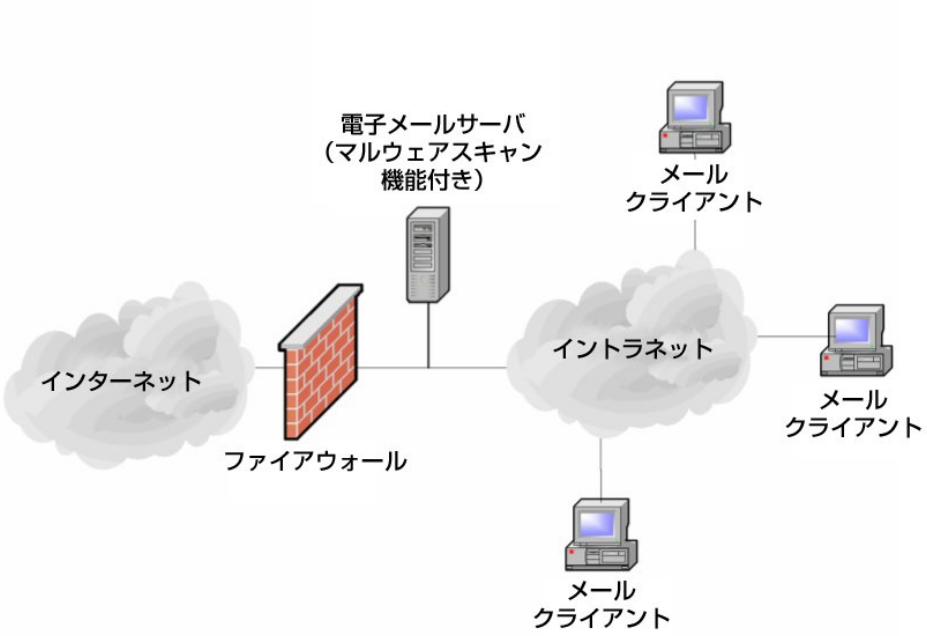

図 5.2：メールサーバのマルウェアスキャン実装

メールサーバにマルウェアスキャンを実装することの最大の短所は、すべてのメッセージをスキャンする必要があるためメールサーバのパフォーマンスに悪影響を及ぼすことである。また、既存のメールサーバの設定を大幅に変更する必要が生じる場合が多いことも短所である。とはいえ、この選択肢には次のようなメリットがある。

- 受信、送信の双方向について電子メールをスキャンすることができる
- 集中管理できるため、組織のセキュリティポリシーに対する適合性を確保することができ、また、更新を定期的に適用することができる
- 組織の内部ネットワークにマルウェアが侵入したあとも内部ユーザが保護される

マルウェアスキャンをメールサーバにおいて実行することには次のデメリットがある。

- 既存のメールサーバの設定に大幅な変更が必要となる可能性がある（最近のほとんどのメールサーバでは、その必要性は比較的小さい）
- 暗号化された電子メールをスキャンすることができない
- 大規模な組織の負荷を処理するには、さらに高性能（高価）なサーバが必要となる可能性がある
- 明らかになっている脅威しか検出できないため、ゼロデイ攻撃に対してはほとんど効果がない

メールサーバベースのマルウェアスキャナを検討する際には、次の特質に着目する。

- 通常、電子メールによって伝送されるすべての種類のマルウェア（ウイルス、ワーム、トロイの木馬、悪意のあるモバイルコード、スパイウェア）を検出・除去できること
- ヒューリスティック（発見的技法）によるスキャンが可能であること（新しい未知のマルウェアにある程度対応できる）
- コンテンツフィルタリングが可能であること（5.2.2 項を参照）
- 電子メールがスキャンシステムを迂回するのを防ぐメカニズムが組み込まれていること
- 管理が容易であること
- 更新を自動的にダウンロードおよびインストールする機能があること
- 更新が頻繁に提供されること（重要）
- コンテンツの種類を識別して異なるルールを適用できること
- 堅牢で、しかも設定の変更が可能な警告メカニズムを備えていること
- 詳細なログを記録できること（9.1 項を参照）

5.2.1.3 クライアントホストでのスキャン

マルウェアスキャナはクライアントホストに配置することもできる（図 5.3 を参照）。この種のマルウェアスキャナは、ユーザワークステーションおよび携帯情報端末（PDA：Personal Digital Assistance）などのモバイル端末にインストールされる。外部から入ってくる電子メールは、ユーザが開くときにスキャンされ、外部に出て行く電子メールは、ユーザが送信を試みるときにチェックされる。このような構成の最大のメリットは、スキャン処理が多数のホストに分散されるため、各ホストのパフォーマンスに対する影響が最小限で済むことである。また、クライアントコンピュータにマルウェアが感染した場合は、マルウエアが、メールサーバやほかのメールクライアントへ拡散することをこの保護層によって防止できる可能性がある。

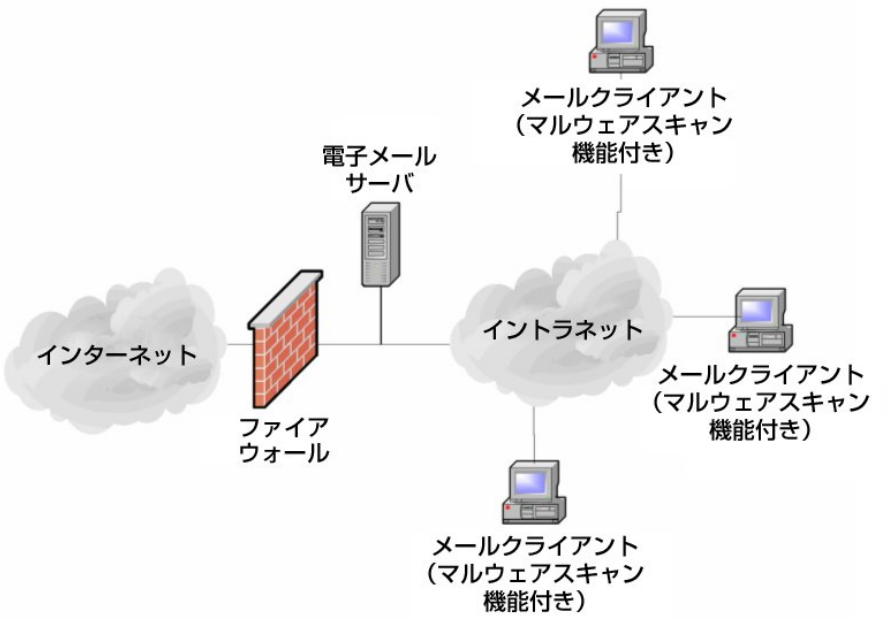

図 5.3：ユーザワークステーションのマルウェアスキャン実装

マルウェアスキャンをユーザワークステーションに実装することの最大の課題は、分散したマルウェアスキャナの管理および定期的な更新が難しいことである。ただし、エンタープライズレベルでマルウェアスキャンを提供するソリューションには、個別ホスト上のマルウェアスキャナを集中管理する手段が用意されている。もう 1 つの短所は、ユーザによるマルウェアスキャナの制御がどの程度許可されるかによるが、その機能の一部または全部がエンドユーザによって（偶発的または意図的に）無効にされる可能性があることである。エンタープライズソリューションには、クライアントサイドスキャナの正しい設定を維持するために、その機能の一部または全部をロックする手段が用意されている。

クライアント側のマルウェアスキャナには、次のようなメリットがある。

- メールサーバにいっさい変更を加える必要がない
- 暗号化されているメールを、ユーザが復号する時点でスキャンできる
- マルウェアスキャン処理が分散されるため、各ホストに対するスキャンの影響は最小限で済む
- 内部ユーザがマルウェアを受信した場合にも内部ユーザが保護される

クライアント側のマルウェアスキャナには、次のようなデメリットがある。

- 集中管理が困難（特に、ラップトップなどのモバイルクライアントホスト）
- ユーザによるマルウェアスキャナの更新が遅れると、組織内でマルウェアの感染拡大を招く可能性がある
- ユーザによって意図的または偶発的に機能を無効にされたり弱められたりする可能性がある
- 明らかになっている脅威しか検出できないため、ゼロデイ攻撃に対してはほとんど効果がない

5.2.2 コンテンツフィルタリング

コンテンツフィルタリングは、ファイアウォールまたはメールサーバにおけるマルウェアスキャンと同様の仕方で機能するが、マルウェア以外の望ましくないコンテンツを含んだ電子メール（スパムや、不適切な語句を含んだ電子メールなど）を探す点が異なる。ファイルタイプの制限およびマルウェアスキャンの実装によって提供されるセキュリティはある一定のレベルでしかない。電子メールメッセージや添付ファイルの内容は、ウイルスや悪意のある実行可能ファイルよりもはるかに深刻な被害を組織に及ぼす場合がある。したがって、何らかのコンテンツフィルタリングメカニズムを導入すべきである。

5.2.2.1 コンテンツフィルタの実装

コンテンツフィルタリングで最大限の効果を得るには、送信・受信されるすべての電子メールを対象として、マルウェアスキャンと同じ場所（ファイアウォール、メールリレーまたはメールゲートウェイ、およびメールサーバとエンドユーザホスト）においてコンテンツフィルタリングを実施すべきである。実際、コンテンツフィルタ、マルウェアスキャン、およびファイルタイプの制限を機能として持つ製品が、一般的なメッセージングシステム向けに多数提供されている（よく使用される製品の一覧については、付録 D を参照）。これらの機能が単一の製品にまとめられていると、セキュリティ管理策を管理する手間が軽減される。

一般には、転送、隔離、保留、除去、ブロック、削除といったルールが定義され、スキャンの結果に基づいて、サーバを通過するあらゆるデータに対していずれかのルールが適用される。フィルタによって捕捉される内容およびそれに対して行われるアクションの代表的な例としては、次のようなものがある。

- 疑わしいアクティブコンテンツ（ActiveX、JavaScript など）を含んだ電子メール：アクティブコードを除去してから受信者に転送する
- スパム電子メールおよびフィッシングの試み：削除するか、疑わしいことを示すタグを付加する
- サイズの特に大きいファイル：オフピークの時間帯まで配信を保留する

コンテンツフィルタリングパッケージが提供するもう 1 つの重要な機能は、外部に出て行くデータのスキャンである。電子メールメッセージをスキャンして字句解析を実行し、組織の電子メールで使用することが適切でないと考えられる語句を探す。また、虚偽の情報やスパムなど不適切な内容（5.3 を参照）が組織から発信されることを字句解析によって防止すれば、訴訟を起こされる可能性が低減される。さらに、企業からの機密データの流出を示すキーワードやフレーズも字句解析によるスキャンの対象になることがある。

組織は、外部ユーザが組織内アドレスからの送信を装って内部ユーザに電子メールを送ることができないようにするなど、電子メールアドレスのなりすましについても予防策を講じるべきである。たとえば WidgetsRUs という企業では、外部から受信したにもかかわらず送信元アドレスが widgetsrus.com ドメインになっている電子メールをすべてメールゲートウェイでブロックするべきである。送信元が組織内ユーザの電子メールアドレスになっている電子メールを、ユーザは正当な電子メールとして信頼する可能性があるため、攻撃者は、内部ユーザになりすまして悪意のある電子メ

ールを送付することがしばしばある。ユーザがなりすましを見分ける方法の 1 つは、電子メールのディジタル署名を確認することである[38]。

何らかのフィルタリングソリューションを導入する前に、既存のネットワークおよびアプリケーションが実際にどのように機能するかを判断することが重要である。その一環として、ネットワークアナライザ（スニファ）の実行、ルータ、ファイアウォールおよびサーバのログファイルの分析、並びに関係するシステムおよびネットワーク管理者の全員を対象とした聞き取り調査を行う。また、組織の現行の情報システムセキュリティポリシーを分析する（まだポリシーが存在しない場合は、原案を作成する）ことも重要である。組織のセキュリティ目標をフィルタのルールへと「翻訳」するにあたり、明確に定義されたセキュリティポリシーの存在はきわめて重要である。フィルタの設定が正確でないと、不適切な内容が排除されない場合や、適切な内容が誤って排除される場合が発生するため、ルールの定義はきわめて慎重に行う必要がある。このような手順を踏むことにより、適切なフィルタソフトウェアの選定と、どのような種類のルールを設定する必要があるかの判断が容易になる。

メールサーバに到達する無用なメッセージの件数を減らすために効果的な別の手段として、メールゲートウェイまたはファイアウォールにおいて LDAP(Lightweight Directory Access Protocol)参照をフィルタリングメカニズムとして使用する方法がある。LDAP 参照を使用すると、ゲートウェイまたはファイアウォールから組織のユーザディレクトリに直接照会してユーザ情報を検索することができる。電子メールを受信したゲートウェイまたはファイアウォールは、ユーザディレクトリにアクセスし、電子メールの宛先が実在のユーザかどうかを確認する。ユーザがディレクトリに存在しない場合、その電子メールは拒否され、メールサーバには到達しない。特定のドメイン宛てに送信されるスパムの大部分は、一般的なユーザ名のデータベースを使用して生成されたものである。生成されるアドレスのほとんどは、現実のドメインには存在しないが、スパム送信者が多数のユーザ宛てに迅速にメッセージを届けるための容易な方法である。LDAP 参照を使用すると、このようなメッセージによるメールサーバのパフォーマンス低下を防止できる。

多くのインターネットサービスプロバイダ（ISP）やサードパーティ企業が、マルウェアスキャンおよびコンテンツフィルタリングサービス（スパムフィルタを含む）を提供している。防護層を増強したいが、それを自ら実装または維持したくない企業にとっては、このようなサービスが有用である。これらのサービスは、組織内のメールサーバに到達する前にメッセージの削除やタグ付けを行うので、メールサーバの効率が向上する。この種のサービスは、多数の組織のために電子メールの監視を実行しているため、新しい無用なメッセージを非常に迅速に識別できることが多い。一方、外部のサービスを利用することには、次のようなデメリットがある。

- **プライバシ**：組織が受信するすべての電子メールが、サービスプロバイダのサーバへとルーティングされ、そこでスキャンされる。
- **フォールスポジティブ**：スパムと見なされた電子メールがサービスプロバイダのフィルタソリューションによって自動的に削除されてしまう場合や、電子メールのタグ付けの妥当性を確認する手段が管理者に提供されない場合がある。
- **可用性**：サービスが利用不能な状態になった場合のために、利用側の組織が電子メールのルーティングを変更してメール配信の遅延を防止できるようになっている必要がある。

---

[38] 電子メール送信元の確認については、Sender ID（現時点の定義は RFC 4406 による）および Sender Policy Framework（現時点の定義は RFC 4408 による）など、いくつかの実験的な規格が登場している。これらのアプローチの詳細については、それぞれ http://www.ietf.org/rfc/rfc4406.txt および http://www.ietf.org/rfc/rfc4408.txt を参照のこと。

5.2.2.2 コンテンツフィルタリングに関する問題

電子メールのコンテンツフィルタリングは、ほとんどの組織のセキュリティ体制に欠かせない要素ではあるが、導入に先立って、法律にかかわる事項を検討すべきである。コンテンツフィルタリングには、明確に定義され、文書化されたセキュリティポリシーによる裏付けが必要である。電子メールポリシーには、コンプライアンスを目的として電子メールの監視が行われる旨の明確な記述、ポリシー違反があった場合に実施される可能性があるすべての管理的または懲戒的措置に関する記述、および、ポリシーを読んで理解したことを職員に対して確認するという要件を盛り込むべきである。ポリシーは、組織がセキュリティに関して持っている考え方、想定、および制限についての概要を示すべきであるが、職員および個人の権利に対しても正当な敬意を表すべきである。たとえば、状況によって、職員自身の個人的な通信については職員がプライバシの権利を有することがある。ただし、組織の代表として行動する場合、職員の言動について組織が法的責任を負うことがある。確立したポリシーがないと、こうした事柄は、解決困難な誤解や問題を生じやすい。

同じように、状況によっては、電子メールメッセージが書面と同等の法的重要性を帯びると見なされる可能性がある（特にディジタル署名付きの場合）。つまり、記録保持の要件に適合するために、職員の個人的なメッセージを含め、メッセージの保管が必要となる可能性がある。こうした事情から、すべての職員にセキュリティポリシーを意識させるべきである。可能な限り広く職員にセキュリティポリシーを周知徹底すべきである。[McKi01] さらに、場合によっては、雇用契約または労働契約の一環として職員にポリシーの承認を要求することと、ポリシーの定期的な再確認を要求することが望ましい。多くの電子メールフィルタアプリケーションには、すべての送受信メッセージに法的免責事項の表示を付加する機能があり、組織を通じてまたは組織から受信した電子メールが有する（または有しない）法的重要性を受信者に理解させるために使用することができる。

ポリシーを策定する際には、法務、プライバシ、人事および人材に関して権限を持つ適切な部門との話し合いを持つべきである。もちろんこれは、ポリシーを専門家に吟味させることにより、法的に誤りがないことと、職員の権利を侵害しないことを確実にするためである。また、組織をすべての領域について調査し、作業者の業務の進め方と、どのようなレベルのセキュリティが最適かを判断することが重要である。インターネットリソースへのアクセスを完全に制限すれば、ほとんどのセキュリティ問題をただちに解決できる可能性があるが、このトレードオフは通常は受け入れられない。このときに電子メールフィルタが役立つ。セキュリティポリシーの理論を実践に移すことを可能にするのである。

個人用の電子メールアカウントは、前述のとおり問題を生じやすい。Web ブラウザを利用してアクセスされるアカウントは、電子メールコンテンツフィルタリングによる管理策が回避されやすいため、とりわけ問題になりやすい。特に、個人用電子メールへのアクセスに SSL による暗号化を利用する Web ページを使用している場合は、SSL で暗号化された HTTPS トラフィックを復号して分析する手段を組織が導入していない限り、通常の経路であれば許可されないようなコンテンツの送受信が許容されてしまう場合がある。また、多くの組織では SSH や IPSec などの暗号化プロトコルが送信方向（内部ネットワークからインターネット）について許可されているが、これを利用して組織外とのトラフィックをトンネリングすれば、フィルタの制約を受けずに情報が送受信される可能性がある。

SMTP などのメールプロトコルを使用したインターネットへの情報の送信をすべての内部ユーザに許可すると、ユーザがメールサーバを独自に設置して、コンテンツフィルタリングが回避される可能性がある。製品やアプリケーションの中には SMTP 電子メールを通信手段として使用するものがあることにも注意が必要である。大規模な組織では、送信方向の電子メールトラフィックのうち、集中管理されたエンタープライズメールサーバとは異なるサーバで生成されたトラフィックが大きな割合を占めていることも珍しくない。そのような電子メールは多くの場合、顧客やビジネスパートナーと通信する電子商取引アプリケーションによって生成される。この問題に対処する 1 つの方法は、境界

部にメールゲートウェイまたはアプリケーションプロキシを設置し、集中管理されたエンタープライズメールサーバ以外のサーバを生成元または伝送先とするメッセージを含め、すべての電子メールを対象として、コンテンツフィルタリングを実施することである。セクション 7 に、ネットワークアーキテクチャとメールゲートウェイの設置に関する補足情報を示す。

5.2.3 ユーザの意識向上

ウイルス対策ソフトウェアやその他のマルウェアスキャンツールの使用と、コンテンツフィルタリングソフトウェアの使用に加え、電子メールによりもたらされるマルウェアがどのような危険を引き起こすか、また、脅威を避けるには、どのような方法が効果的であるかについて、以下の行動を含め、ユーザを教育することも重要である。

- 未知の送信者から送られた添付ファイルは絶対に開かない。
- 送信者が未知か既知かに関わらず、疑わしいあるいは、有害だと思われる名前またはファイル拡張子（attachment.txt.vbs、attachment.exe など）の付いた添付ファイルは絶対に開かない。
- 既知の送信者から送られた電子メールでも、互いの現在の関係から考えて適切と考えにくい件名や内容である場合（たとえば、送信者が同僚の専門家であるのに件名が「I love you（好きです）」など）や、具体性のない件名（たとえば、「Look at this, it's interesting（面白いから見てよ）」など）が付けられている場合は注意する。
- すべての添付ファイルは、開く前にマルウェアスキャンソフトウェアを使って必ずスキャンする。できれば、この作業を自動実行するようにスキャンソフトウェアを設定することが望ましい。
- マルウェアスキャンソフトウェアのシグネチャデータベースを少なくとも毎日更新する。また、マルウェアが大発生しているときにも更新する。
- マルウェアの大発生情報や、マルウェアを含んでいる可能性のある電子メールの見分け方についてユーザに警告する。

ユーザには、フィッシング攻撃の危険性および回避方法についても注意するべきである。米国連邦取引委員会（FTC：Federal Trade Commission）が発表した消費者向け警告書には、ユーザが行うべき事項の概要として次のことが示されている。[FTC06]

- 個人情報または資産に関する情報を求める電子メールメッセージやポップアップ広告に応答しない。
- 電子メールやポップアップ広告に記載されている電話番号を信用しない。VoIP（Voice over IP）テクノロジーを使用すれば任意の市外局番を登録できるからである。
- 個人情報や資産に関する情報を電子メールで送信しない。
- クレジットカードの請求書や銀行口座の利用記録を定期的に確認する。
- 信頼のおけない Web サイトには不用意にアクセスしない。サイトにアクセスするだけで Web ブラウザの脆弱性が悪用される場合がある。また、信頼のおけない電子メールの添付ファイルや、信頼のおけない Web サイトからダウンロードしたファイルは不用意に開かない。
- フィッシングに関係する電子メールは、spam@uce.gov と、なりすましの対象とされた組織宛てに転送する。

■ 年に 1 回、Equifax、Transunion、および Experian の 3 つの信用情報機関から自分の信用情報報告書のコピーを取得する。身元情報を不正に使用して口座が開かれた場合、信用情報にその口座の情報が記載されている可能性が高い[39]。

5.3 スパム送信元サーバのブロック

通信の媒体が何であれ、アイデアや製品を広く宣伝するためにあらゆる通信手段を利用しようとする者は常に存在するものであり、電子メールもその例外ではない。そのようなメッセージを最も一般的に表す UCE（Unsolicited Commercial Email、一方的に送付される商用目的の電子メール）という用語があるが、スパムという呼称のほうがよく普及している。ほとんどの電子メールユーザには、毎日のようにスパムが届く。電子メールに対して規制はほとんど行われていないので、システム管理者は、ユーザに到達するスパムの量を削減するために、サーバを通過する電子メールのトラフィックを規制するべきである。サーバベースのスパム管理策を導入することには、メールボックスのサイズを抑え、ひいては必要なサーバのストレージ容量を少なくできるという付加的なメリットがある[40]。

管理者は、スパムメッセージに対処するために次の 3 つを実施する必要がある。

■ 管理下にあるメールサーバからスパムを送信できないようにする（5.4 項を参照）

■ 受信メッセージに対するスパムフィルタを実装する（6.2 項を参照）

■ 既知のスパム送信元サーバから伝送されるメッセージをブロックする（このセクションのトピック）

インターネットには、集中的な規制機関がないため、非営利団体や営利企業が、一方的な電子メール送付に使用されていることが確認されたメールサーバの一覧を作成している。それらは、しばしばオープンリレーブラックリスト（ORB）または DNS ブラックリスト（DNSBL）と呼ばれる。広く普及しているメールサーバアプリケーションのほとんどは、複数の ORB に照会し、一覧に含まれるメールサーバから送られてくるメッセージを拒否するように設定できる。一覧は毎日更新されているため、それらを使用することでスパムメッセージの配信を大幅に削減することができる。また、ほとんどのメールサーバでは、明示的に指定した一連のドメインからのメッセージを拒否するように設定できる。

ORB に基づくスパム規制も、絶対確実というわけではない。オープンリレーは接続されたり、切断されたりと常に変化している。規制活動に協力したいと考えるメールサーバ管理者は、UCE に関する報告を付録 E に示す Web サイトに送付するとよい。

5.4 認証付きメールリレー

前述のように、メールリレーの認証を設定することにより、特定のメールサーバを使用してスパムを送付される可能性を低減できる。また、セキュリティおよび利便性が向上するというメリットもある。

メールリレーの制御には、2 つの方法を使用できる。1 つは、メッセージの送信元となるサブネットまたはドメインを制限する方法である。これは、メッセージングシステムの境界部が既知のアドレス範囲に属している場合に効果的であるが、アドレス範囲の異なるホストがリモートユーザによって使用される場合は有用でない。リモートユーザに対応するには、より堅牢な設定が必要となる。

---

[39] Fair and Accurate Credit Transactions Act of 2003（公正・正確信用取引法）の規定により、消費者は 12 か月ごとに 1 回、信用情報報告業者 3 社のいずれかに無料で報告書の発行を要求することができる。詳細については、http://www.ftc.gov/os/statutes/fcrajump.htm を参照のこと。

[40] スパムの詳細については、RFC 2505『*Anti-Spam Recommendations for SMTP MTAs*』（http://ietf.org/rfc/rfc2505.txt）を参照のこと。

もう 1 つは、メッセージの送信時に必ず認証を行うことをユーザに要求する方法である。これは認証付きリレーまたは SMTP AUTH（ユーザ認証をサポートする SMTP 拡張）と呼ばれる。残念ながら、ほとんどのメールサーバのデフォルト設定では認証付きリレーが実装されない。したがって、メールサーバ管理者がサーバを適切に設定する必要がある。認証付きリレーを要求する設定はあまり使用されないが、メールサーバの最も強力なセキュリティ機能である（SMTP AUTH の設定方法については、メーカーの文書を参照）。

認証付きリレーを採用する場合、メールサーバ管理者は注意しなければならない。メールサーバが適切に設定されていないと、スパムの送信または中継に悪用されかねず、また、オープンリレーと見なされればメールサーバがブラックリストに掲載される（6.3 項を参照）。ブラックリストを参照しているすべての組織は、リストに掲載されたサーバからの電子メールをいっさい（スパムであれ、正当な電子メールであれ）受信できなくなる。

自分が管理しているメールサーバがブラックリストに掲載されていることを知った場合、メールサーバ管理者はオープンリレーの問題を解決し、テストを実行して、当該サーバがリレーとして利用できなくなったことを確認する必要がある。その上で、いずれのブラックリストに掲載されているかを特定し、各ブラックリストの維持管理者に問い合わせて、一覧からサーバを除外するための手続きを知る必要がある。当該サーバがすべてのブラックリストから除外され、更新後のブラックリストが利用者に伝播するまでは、組織から送信される電子メールが一部の宛先に到達しない可能性が残る。付録 D に、オープンリレー確認用ツールを提供している Web サイトの一覧と、広く使用されているブラックリストの維持管理者の一覧を示す。

5.5 アクセスのセキュリティ保護

セクション 2 では、メール伝送およびメールボックスのアクセスに使用されるプロトコルについて説明した。それらのほとんどは、多くのインターネットプロトコルと同じように、当初は暗号化や暗号認証をいっさい備えていなかった。この欠落が、電子メールユーザにとって 3 つの問題が生じる元となった。第 1 の問題は、メッセージの送信者にとって、送信者から受信者までの経路上にある任意のホストにおいて内容が傍受される可能性や、偽造または改ざんのおそれがあったことである。これは、通常の郵便システムにおけるハガキの問題点に似ている。ハガキの裏に書かれたメッセージは、ハガキを取り扱うすべての人に読まれる可能性がある。第 2 の問題は、メッセージが伝送中に他者によって改ざんされていないか、また、本当に送信者本人から送信されたものかどうかを受信者が確認できなかったことである。第 3 の問題は、ユーザがメールボックスにアクセスする際、再利用不可能な認証情報ではなく、平文のパスワードがネットワークを介して送信されるため、攻撃者による傍受および再利用が容易であったことである。残念ながら、メールクライアントのデフォルト設定はユーザのパスワードを平文で送信する設定になっている場合がほとんどであり、そのままでは、クライアントと同じローカルネットワークセグメント内にある別のコンピュータや、メールサーバへのパスワードの転送に関与するすべてのホストによって傍受される可能性がある。

第 1 および第 2 の問題については、メッセージの保護方法に関するセクション 3 において述べた。第 3 の問題については、ワールドワイドウェブ（WWW）トラフィックの保護に通常使用されているのと同じ方法、すなわち Transport Layer Security（TLS）プロトコルによって解決できる。

TLS は、その基礎となった SSL(Secure Sockets Layer) プロトコルに似ており、POP、IMAP、SMTP と組み合わせることでメールクライアント／サーバ間の通信を暗号化できる。RFC 2595 には、TLS を使用して通信の盗聴を防ぐ方法、メールボックスへのアクセスのセキュリティを保護する方法、および、SMTP AUTH を組み込んだ SMTP MTA をさらに強化する方法が定義されている。図 6.4 は、sendmail の最近のバージョンにおいて TLS サポートを有効にするための設定例である。

```
define(`CERT_DIR', `MAIL_SETTINGS_DIR``certs')dnl
define(`confCACERT_PATH', `CERT_DIR')dnl
define(`confCACERT', `CERT_DIR/CAcert.pem')dnl
define(`confSERVER_CERT', `CERT_DIR/MYcert.pem')dnl
define(`confSERVER_KEY', `CERT_DIR/MYkey.pem')dnl
define(`confCLIENT_CERT', `CERT_DIR/cert.pem')dnl
define(`confCLIENT_KEY', `CERT_DIR/MYkey.pem')dnl
```

図 5.4：Sendmail の TLS 設定例（sendmail.mc より）

5.6 Web アクセスの有効化

メッセージングシステムへのアクセス手段として、Web ブラウザベースのアクセス機能を提供する組織が増えている。この種のアクセスを有効にすることは、クライアント（7.4 項を参照）とサーバの両方にセキュリティ上の問題を発生させる可能性がある。Web サイトのセキュリティは、この文書が扱う話題の範囲から外れるが、従うべき重要な考え方がいくつかある。

- Web サーバとメールサーバを同一のコンピュータ上で稼働させることは避ける。
- Web フロントエンドの認証メカニズムでは暗号化を使用する。
- Web サーバでは、クライアントとの通信をすべて SSL／TLS で暗号化する。
- すべての公開サーバと同様、Web サーバのセキュリティはネットワークに接続する前に強化しておく[41]。

組織によっては、Web サーバを SSL／TLS 通信専用にするための処理能力の要件が受け入れがたいことも考えられる。そのような場合でも、最初の認証については暗号化すべきである。

また、組織によってはハードウェアアプライアンスを使用して Web アクセスソリューションを提供することがある。アプライアンスを使用すると、メールサーバへの安全な Web ベースアクセスだけでなく、ファイアウォール、コンテンツフィルタリング、およびマルウェア保護機能も併せて提供することができる。一般的に、アプライアンスは Web サーバを構築するよりもインストールや保守を容易かつ迅速に行うことができ、また、不要な構成要素がすべてあらかじめ削除または無効化された、セキュリティ強化オペレーティングシステムを搭載していることが多いため、脆弱性の存在する可能性が限られる。一部のアプライアンスは、ユーザグループおよびアクセスに関する粒度の細かい管理、SSL によるセッション暗号化、一定時間使用されていないユーザセッションの自動切断などの付加機能を備えていることもある。非常に広く使われている Web ベースメールシステムをサポートするアプライアンスの入手が可能である。

---

[41] Web サーバのセキュリティ保護の詳細については、NIST SP 800-44『*Securing Public Web Servers*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

電子メールへの Web アクセスの導入を組織として承認する前に、クライアントのセキュリティに関する問題も検討する必要がある。それらについては 7.4 項で述べる。

5.7 メールサーバおよび内容のセキュリティ保護に関するチェックリスト

完了	アクション
	メールサーバアプリケーションのセキュリティ強化
☐	メールサーバソフトウェアは、専用のホストにインストールする（Web ベースのメールアクセスを使用する場合、メールサーバソフトウェアを Web サーバとは別のホストにインストールする）
☐	既知の脆弱性を修正するパッチまたは更新プログラムをすべて適用する
☐	メールボックス専用の（オペレーティングシステムやメールサーバアプリケーションとは分離した）物理ディスクまたは論理パーティションを作成するか、メールボックスを別のサーバでホストする
☐	メールサーバアプリケーションによってインストールされたサービスのうち不要なもの（Web ベースのメール、FTP、リモート管理など）をすべて削除または無効化する
☐	メールサーバのインストール時に作成された不要なデフォルトのログインアカウントをすべて削除または無効化する
☐	メーカーの文書をサーバからすべて削除する
☐	サンプルおよびテスト用ファイルをサーバからすべて削除する
☐	適切なセキュリティテンプレートまたはセキュリティ強化スクリプトをサーバに適用する
☐	SMTP、POP、IMAP サービスのバナー（必要に応じて別の箇所も）の設定を変更し、メールサーバやオペレーティングシステムの種類とバージョンを表示しないようにする
☐	危険性のあるメールコマンドや不要なメールコマンドを無効化する（VRFY、EXPN など）
	オペレーティングシステムおよびメールサーバのアクセス制御の設定
☐	メールサーバアプリケーションからアクセスできる範囲をコンピュータリソースのサブセットに限定する
☐	より詳細なレベルのアクセス制御が必要な場合は、メールサーバによって適用される追加的なアクセス制御を使用してユーザのアクセスを限定する
☐	メールサーバアプリケーションを、厳しいアクセス制限が課せられた固有のユーザ ID およびグループ ID のもとにおいてのみ実行されるように設定する
☐	メールサーバが root または System／Administrator 権限で動作しないことを確認する
☐	ホストオペレーティングシステムを、メールサーバからログファイルへの書き込みのみ許可し、読み取りは禁止するように設定する
☐	メールサーバアプリケーションによって作成される一時ファイルが、適切に保護された特定のサブディレクトリに配置されるようにホストオペレーティングシステムを設定する
☐	メールサーバアプリケーションによって作成される一時ファイルへのアクセスを、当該ファイルを作成したメールサーバプロセスに限り許可するようにホストオペレーティングシステムを設定する
☐	メールサーバに対して専用に割り当てられている指定のファイル階層構造の外に、メールサーバがファイルを保存することができないようにする
☐	Linux および Unix のホストの場合は、メールサーバが chroot jail 内で稼働するように設定する
☐	ユーザのメールボックスを、オペレーティングシステムやメールサーバアプリケーションとは別のサーバ（推奨）、別のハードディスク、または別の論理パーティションにインストールする

完了	アクション
☐	ハードディスクまたはパーティションの空き領域を全て使い切ることがないように、メールサーバアプリケーションを設定する
☐	添付ファイルの許容サイズを制限する
☐	ログファイルの格納場所に十分なサイズを確保する
	マルウェアからの電子メールの保護
☐	許可する添付ファイルの種類を決定する
☐	添付ファイルとして許容する最大ファイルサイズの制限を検討する
☐	組織内のコンピュータから個人メールアカウントへのアクセスを許可することが適切かどうかを判断する
☐	電子メールメッセージ内での使用を許可するアクティブコンテンツの種類を決定する
☐	集中管理されたマルウェアスキャンを実装する（ファイアウォール、メールリレー、メールゲートウェイ、メールサーバのうち 1 つまたは複数に）
☐	すべてのクライアントホストにマルウェアスキャナをインストールする
☐	集中管理されたコンテンツフィルタリングを実装する
☐	疑わしいメッセージ（フィッシング、スパムなど）をブロックまたはタグ付けするようにコンテンツフィルタリングを設定する
☐	疑わしいアクティブコンテンツをメッセージから除去するようにコンテンツフィルタリングを設定する
☐	必要な場合、字句解析を設定する
☐	アドレスのなりすましを防ぐ各種手順を実行する（送信元アドレスに内部アドレスを装った外部からの受信メールをブロックするなど）
☐	コンテンツフィルタリングに関する記述を盛り込んだセキュリティポリシーを策定する
☐	法務、プライバシ、人材に関して権限を持つ適切な部門にセキュリティポリシーをレビューさせる
☐	必要な場合、電子メールに法的免責事項の表示を付加する
☐	マルウェアの危険性およびそれを最小化する方法についてユーザを教育する
☐	マルウェアの大発生時にユーザに通知する
	スパム送信元サーバのブロック
☐	電子メール受信者が実在することを LDAP 参照で確認するようメールゲートウェイまたはファイアウォールを設定する
☐	必要な場合、オープンリレーブラックリストまたは DNS ブラックリストに基づいて電子メールをブロックするようメールサーバを設定する
☐	必要な場合、特定ドメインからの電子メールをブロックするようメールサーバを設定する
	認証付きメールリレーの使用
☐	サーバで認証付きメールリレーを使用するように設定する
	メールサーバへのアクセスのセキュリティ保護
☐	暗号化認証を使用するようメールサーバを設定する
	電子メールへの Web アクセスの有効化
☐	メールへの Web アクセスが必要と考えられる場合に限り、SSL／TLS 経由の Web アクセスのみを可能とするように、メールサーバを設定する

（本ページは意図的に白紙のままとする）

6. 安全なネットワーク基盤の実装

メールサーバのセキュリティを確保するうえで、メールサーバを支えるネットワーク基盤の役割はきわめて重要である。ほとんどの設定においては、インターネットとメールサーバの間で、ネットワーク基盤が最初の防衛線となるからである。ただし、ネットワークの設計だけでメールサーバを保護することはできない。電子メールに対する攻撃が頻繁に行われ、その内容も高度化かつ多様化している現状では、さまざまな防御メカニズムによる多重構造のセキュリティ対策が必要と考えられる。このセクションでは、メールサーバのセキュリティ保護をサポートして全体的なセキュリティを強化するためのネットワーク構成要素について述べる。最も重要なのはセキュリティ問題であるが、ネットワーク基盤についての検討においては、コスト、パフォーマンス、信頼性など、セキュリティ以外の多くの要素の影響を受ける。

6.1 ネットワークの構成および構造

ファイアウォールおよびルータは、ネットワーク間のネットワークトラフィックを制御する装置またはシステムである。TCP/IP（Transmission Control Protocol/Internet Protocol）スイートの本質的な脆弱性からメールサーバを保護し、セキュリティの低いアプリケーションやオペレーティングシステムがかかわるセキュリティ問題の削減に役立つ。ただし、組織としてメールサーバのネットワーク環境を決定する際には数多くの選択肢があり、どのオプションを採用するかの決定において、セキュリティが第一の要因であるとは限らない。ネットワークの構成および構造をどのようにするかは、最初に意思決定が行われることであり、また、多くの面において、メールサーバのセキュリティに影響する最も重要な判断事項でもある。なぜなら、どのようなネットワーク基盤によってメールサーバを保護するかがこれによって決まるからである。たとえば、メールサーバを組織の主ファイアウォールの外に配置すると、このファイアウォールを使用してメールサーバの送受信トラフィックを制御することはできない。また、メールサーバが侵害された場合に、ネットワークの他のどの部分が攻撃にさらされる可能性があるかという点も、ネットワークの構成および構造によって決まる。たとえば、内部の実運用ネットワークに外部からのアクセスが可能なメールサーバを配置する場合、メールサーバが侵害されたときに内部ネットワークが攻撃にさらされる。

6.1.1 望ましくないネットワークレイアウト

組織によっては、公開メールサーバを内部の実運用ネットワーク上に配置することがある。すなわち、メールサーバが内部のユーザおよびサーバと同じネットワーク上に存在することになる。このようなレイアウトの第一の弱点は、内部ネットワークの構成要素が余分なリスクにさらされることである。メールサーバは、しばしば攻撃者による攻撃の的となる。攻撃者によるメールサーバの侵害が成功すると、内部ネットワークへのアクセスが可能になり、より容易に内部ホストを侵害することができる。したがって、このレイアウトは推奨できない。

一般に推奨できないもう 1 つのネットワークレイアウトは、IP フィルタ機能を持つファイアウォールまたはルータの外側にメールサーバを配置する構成である。そのような構成の場合、ネットワークによるメールサーバの保護は（あったとしても）わずかである。メールサーバ自体でセキュリティを確保する必要があるため、ここが single point of failure(単一の箇所で発生した障害が全体の障害となるポイント)となる。この場合、メールサーバのオペレーティングシステムおよびアプリケーションの不要かつ安全でないサービスをすべて無効化し、必要なセキュリティパッチをすべて適用して、セキュリティを非常に強固にすることにより、ある程度の安全性は確保されるが、この構成のセキュリティを維持するために、メールサーバ管理者は、脆弱性と対応するパッチに関する最新情報を常に確認する必要がある。また、この構成の場合、安全なリモート管理機能を提供することはどのような形態であれ、困難である。

6.1.2 DMZ

DMZ（Demilitarized Zone：非武装地帯）は、組織の内部ネットワークとインターネットの間に「中立地帯」として設置されたホストまたはネットワークセグメントを意味する。DMZ は、外部からメールサーバを利用するユーザが組織内部のネットワーク（イントラネット）に直接アクセスするのを防ぐものであり、メールサーバを内部ネットワークに配置することやインターネット上に直接露出させることのリスクを緩和する。これは、ほとんどの組織に対して最小のリスクで最大のメリットを提供することができる妥協策の 1 つである。DMZ 上に配置されたリソースに対しては、内部、外部いずれのユーザもアクセスできる。DMZ の構成にはさまざまな形態があり、それぞれが特有の長所と短所を持つ。

DMZ を作成する際には、組織の境界ルータと内部ネットワークとの間にファイアウォールを設置し、また、DMZ 装置を介してのみアクセス可能な新しいネットワークセグメントを作成する。この新しいセグメント上には、メールサーバまたはメールゲートウェイのほか、外部からアクセスできるようにする必要のある他のネットワーク基盤構成要素を配置する。たとえば、Web ベースのメールアクセスを提供する場合は、それに対応するサーバ類を DMZ に配置することが多い。構成によっては、境界ルータ自体が基本的なファイアウォールとして機能することもある。図 6.1 は、そのような単純な DMZ の例である。DMZ を出入りする特定の種類のネットワークトラフィックを制限するためにアクセス制御リスト（ACL）をもつルータを使用する。

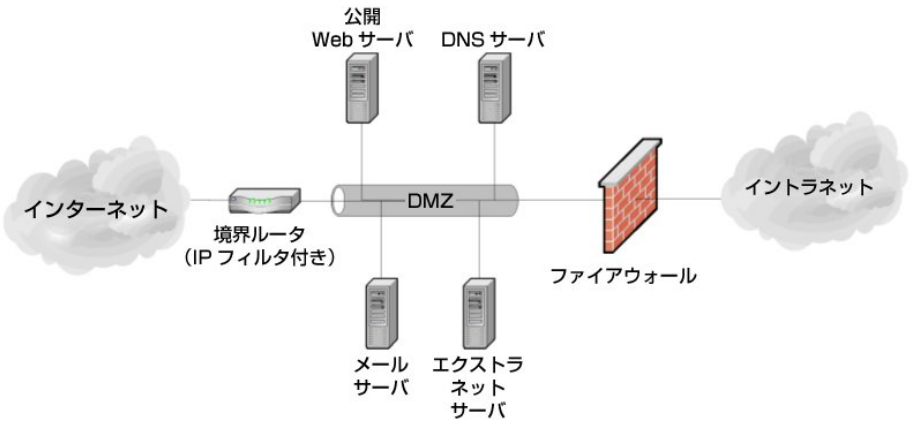

図 6.1：単一のファイアウォールによる単純な DMZ

単独のファイアウォールによる DMZ 構成は、ファイアウォールを 1 基追加する必要があるだけで、既存の境界ルータを DMZ の保護に使用する低コストのアプローチである。これは通常、最小限の脅威に対処する小規模の組織にのみ適している。このアプローチの基本的な弱点として、ルータはネットワークに対するほとんどの攻撃を防げる反面、メールサーバのアプリケーション層プロトコル（SMTP、POP、IMAP など）は認識しない。つまり、メールサーバを狙ったアプリケーション層の攻撃を防ぐことはできないのである。また、受信する電子メールに対するウイルススキャンもルータでは実行できない。図 6.2 に示すように、インターネットと DMZ の間にファイアウォールをもう 1 つ設置する構成のほうが優れている。

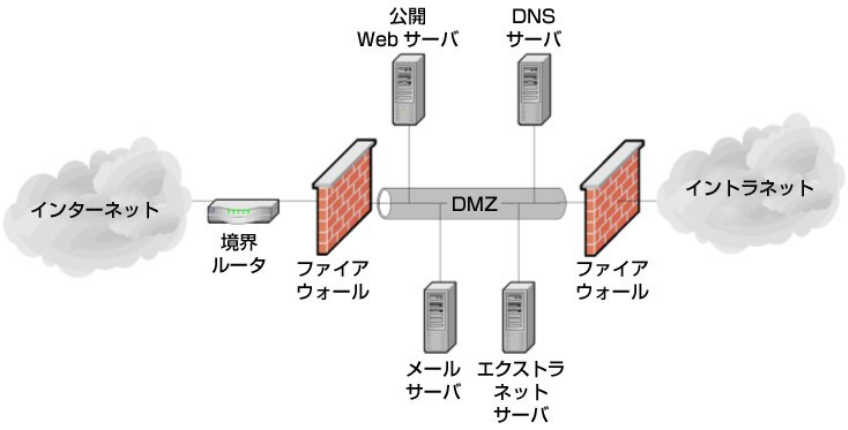

図 6.2：2 基のファイアウォールによる DMZ

2 基のファイアウォールによる DMZ 構成は、ルータと単独のファイアウォールによる DMZ により提供される保護を改良したものといえる。専用ファイアウォールを 2 基設置することで、より複雑かつ強力なセキュリティルールセットを使用できるからである。また、専用ファイアウォールは送受信メールトラフィックを分析する能力を備えていることが多いため、メールサーバを狙ったアプリケーション層の攻撃を検出・防御することができる。ファイアウォールのルールセットの内容と、DMZ に届くトラフィックのレベルによって、この種の DMZ ではいくらかのパフォーマンスの低下が生じることがある。

ファイアウォール 2 基の DMZ が備えるセキュリティは欲しいが、2 基もファイアウォールを購入する余裕がないという組織には、「サービスレッグ」DMZ と呼ばれる選択肢もある。この構成の場合、ファイアウォールには 3 つ（またはそれ以上）のネットワークインタフェースがあり、これらのインタフェースをそれぞれ、境界ルータ、内部ネットワーク、および DMZ に接続する（図 6.3 を参照）。

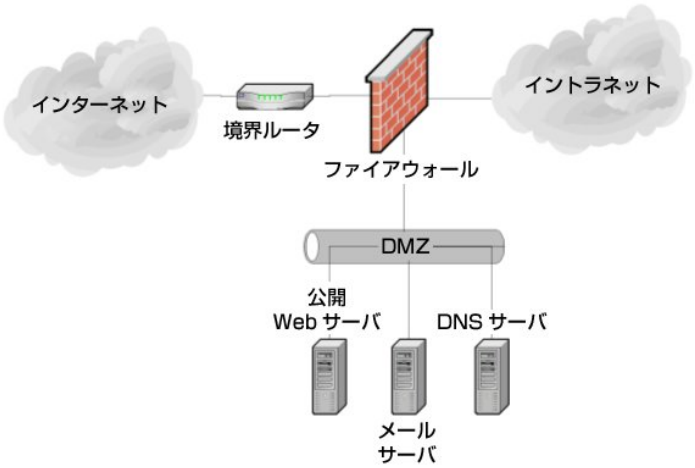

図 6.3：3 つのインタフェースを備えたファイアウォールによる DMZ

この構成は、DMZ を狙った DoS 攻撃によってファイアウォールのサービスが低下するリスクが大きい。前述した基本的な単独のファイアウォールによる DMZ ネットワーク構成の場合、メールサーバを狙った DoS 攻撃は通常、メールサーバにのみ影響する。それに対して、サービスレッグ DMZ ネットワーク構成では、メールサーバに到達する前のネットワークトラフィックをすべてファイアウォールが検査しなければならないため、ファイアウォールがあらゆる DoS 攻撃に耐えることになる。ただし

一方で、DoS 攻撃は DDoS（分散型サービス運用妨害）の形態を採ることが多くなっており、DMZ ファイアウォールに到達する前の段階で、受信方向のネットワーク帯域および関連装置（インターネット境界ルータなど）がすべて消費し尽くされる可能性が高い。

セキュリティの観点から、DMZ には次のようなメリットがある。

- メールサーバの保護を強化し、メールサーバに出入りするネットワークトラフィックを監視できる。
- メールサーバが侵害されても、それによって内部の実運用ネットワークが直接脅威にさらされることはない。
- メールサーバに出入りするトラフィックを制御できることにより、メールサーバのセキュリティをより的確に制御できる。
- DMZ ネットワーク構成は、メールサーバのサポートおよび保護のために最適化できる。

セキュリティの観点から、DMZ には次のようなデメリットがある。

- メールサーバを狙った DoS 攻撃が内部ネットワークに影響する可能性がある。
- DMZ と内部ネットワークの間のトラフィックを制御するファイアウォールの設定によっては、内部ネットワーク上のホストを攻撃または侵害する手段としてメールサーバが使用される可能性がある。つまり、DMZ によって提供される保護はファイアウォールの設定に依拠するところが大きい。

6.1.3 メールゲートウェイ

DMZ 内でメールゲートウェイを使用すると、メールサーバの保護をさらに強化することができる。この追加の層により、メールサーバへの攻撃は大幅に難しくなる。メールサーバの設置場所が DMZ 内であっても、メールサーバは信頼のおけない第三者と通信する必要があり、したがって攻撃者の足がかりとなり得る。メールゲートウェイは、実際のメールサーバとインターネットの間でプロキシとして機能する。すべてのメッセージおよび通信がこのプロキシを通過してからメールサーバに転送されるようにすることで、インターネットとメールサーバの直接の通信経路が断ち切られ、メールサーバに対する攻撃がはるかに困難になる。一般にメールゲートウェイが必要とする機能は限られているため、完全な機能を備えたメールサーバと比べ、そのセキュリティを強化することははるかに容易である。内部ネットワーク上にあるメールサーバのセキュリティをメールゲートウェイによって強化した構成の例を図 7.4 に示す。

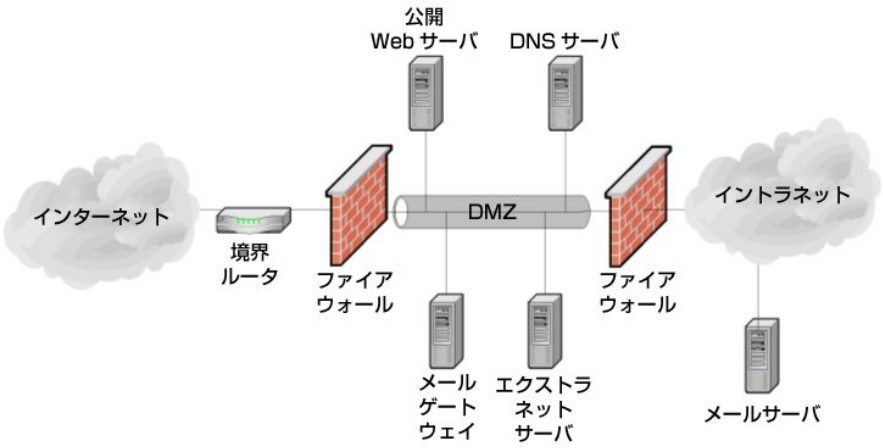

図 6.4: メールゲートウェイ

6.1.4 管理ネットワーク

メールサーバ、ゲートウェイ、およびその他の重要な構成要素を相互に接続して管理する方法としては、組織の標準ネットワークを使用する場合と、「管理ネットワーク」と呼ばれる別のネットワークを使用する場合がある。管理ネットワークを使用する場合、ネットワーク経由で管理される各ホストは、管理ネットワーク接続用の「管理インタフェース」と呼ばれる追加のネットワークインタフェースを装備する。また、管理対象のいずれのホストも、管理インタフェースとそれ以外のネットワークインタフェースとの間ではいっさいトラフィックを通過させることができない。各種メール用の構成要素の管理に使用するコンソールなどのホストは、管理ネットワークにのみ接続する。このアーキテクチャにより、管理ネットワークは、実運用ネットワークから実質的に隔離される。このような構成には、構成要素を一部の攻撃から保護し、問題のある状況下（電子メールによりもたらされたマルウェアが広範囲に感染した場合など）でもそれら構成要素の管理を可能にするというメリットがある。管理ネットワークを使用することのデメリットとしては、ネットワーク機器やその他のハードウェア（コンソール用 PC など）のコストが増加することと、メール用の構成要素の管理者が、管理や監視に別々のコンピュータを使用する必要があるため、不便が生じることが挙げられる。

6.2 ネットワーク要素の設定

メールサーバをネットワークに配置したあとは、これをサポートおよび保護するようにネットワーク基盤の各種要素を設定しなければならない。メールサーバのセキュリティに影響するネットワーク基盤の要素としては、ファイアウォール、ルータ、侵入検知および侵入防止システム、並びにスイッチがある。これらには、それぞれ重要な役割があり、多層防御によってメールサーバを保護するという全体的な戦略のために不可欠である。残念ながら、メールサーバのセキュリティ保護に関して万能の解決策は存在しない。ファイアウォールまたは侵入防止システム単独では、あらゆる脅威や攻撃からメールサーバを十分に保護することはできない。

6.2.1 ルータ／ファイアウォールの設定

ファイアウォールには、いくつかの種類がある。最も基本的なものは、IP パケットのアクセス制御機能を備えたルータである。中程度のレベルにあるのは、IP に加えて TCP および UDP（User Datagram Protocol）ベースのアクセス制御ができる、ステートフルなファイアウォールである。そして、

最も強力なファイアウォールは、電子メールの内容およびコマンドを解釈しフィルタ処理する能力を持った、アプリケーション層ファイアウォールまたはプロキシファイアウォールである[42]。

ファイアウォールや、(ファイアウォールとして機能する)ルータについては、すべてのリスクを排除できるものであるとか、メールサーバの設定ミスやネットワーク設計の不備までも保護できるものであるという誤解がよくある。これらは残念ながら事実ではなく、ファイアウォールやルータ自体が、設定のミスやソフトウェアの脆弱性のような脆弱性を持っている。また、現在はアプリケーション層に対して攻撃が行われることが多いが、ほとんどのファイアウォールは、アプリケーション層における事象にまったく関知しないか、限定的な認識能力しか備えていない。特にメールサーバは、たとえ入念に設定された安全なファイアウォールの内側に設置されていても、さまざまな攻撃に対して脆弱である。

メールサーバを保護するファイアウォールまたはルータ(ファイアウォールとして機能するもの)は、インターネットからメールサーバへのアクセスを、TCP ポート 25(SMTP)などの必要なポート以外はすべてブロックするように設定すべきである。ファイアウォールはメールサーバにとって最初の防衛線であるが、セキュリティを十分にするには、メールサーバ(およびネットワーク)を守る多重の防御層を実装する必要がある。最も重要なのは、すべてのシステムを安全な状態に保つために組織として努力し、攻撃者を阻止するためにルータ、ファイアウォール、その他いかなる単独の構成要素のみに頼ることがないようにすることである。

最近のエンタープライズルータは、ネットワーク層およびトランスポート層のフィルタ(基本的なファイアウォール)としての機能を備えている。ネットワーク層またはトランスポート層のファイアウォールとして機能するルータでは、次のような情報に基づいたフィルタリングを実行できる。[Wack02a]

- 送信元 IP アドレス
- 宛先 IP アドレス
- トラフィックの種類
- TCP／UDP ポートの番号および状態

ルータには次の長所がある。

- 低コスト(ほとんどの組織は、ネットワーク層またはトランスポート層のファイアウォール機能を提供するように設定することが可能な境界ルータをすでに所有している)

ルータには次の短所がある。

- アプリケーション層に対する攻撃に弱い(電子メールの内容またはコマンドを検査できないなど)
- 許可されたポートを経由しての攻撃に弱い(ルータは、アプリケーション層において分析を行わないため、一般にこの点でファイアウォールよりも弱い。ファイアウォールは、これを行うので、許可ポート経由の攻撃をある程度認識できる)
- 設定および管理が難しい
- ログの記録能力に制約がある

---

[42] ファイアウォールの詳細については、NIST SP 800-41『*Guide to Firewall Selection and Policy Recommendations*』(http://csrc.nist.gov/publications/nistpubs/)を参照のこと。

■ ルールセットが複雑な場合、処理能力の制約や負担が大きいことがある（アクセス制御リストなど）

■ ルールセットの表現力およびフィルタリング能力が不十分

現在利用可能な「純粋な」ネットワーク層ファイアウォールは、スモールオフィス／ホームオフィス（SOHO）ファイアウォールアプライアンスや、基本的なパケットレベルのフィルタリングしか実行できないパーソナルファイアウォールのみである。[Wack02a]

ステートフルインスペクション型ファイアウォールは、トランスポート層の装置に TCP 接続の状態を「認識」できる能力を組み込んだものであり、ファイアウォールを経由する接続の状態や一部データストリームの内容など、内部情報をファイアウォールが保持するため、より強力かつ正確なルールセットおよびフィルタを指定できるようになっている。ステートフルインスペクション型ファイアウォールは、フィルタリングルータの能力に、接続の状態に基づいたルールを適用する能力を加えたものである。

アプリケーション層ファイアウォール（アプリケーションプロキシゲートウェイファイアウォールと呼ばれる場合もある）は、ネットワーク層およびトランスポート層のアクセス制御とアプリケーション層に関する機能を組み合わせた高度なファイアウォールである。アプリケーション層ファイアウォールは、インターネットと内部ネットワークの間、または 2 つのネットワークの間でトラフィックを直接伝送することを許可しない。また、通常は広範なログの記録と拡張されたアクセス制御が可能である。

アプリケーション層ファイアウォールは、最も強力な種類のファイアウォールであると考えられており、パケットフィルタリングルータおよびステートフルインスペクション型ファイアウォールと比べ、次のように数多くの点で優れている。

■ ログ記録機能

■ フィルタリング能力（特定の種類の電子メール内容および特定の SMTP、POP、IMAP コマンドをフィルタリングできる）

■ 設定のしやすさ

■ ユーザ認証機能

アプリケーション層ファイアウォールをパケットフィルタリングルータおよびステートフルインスペクション型ファイアウォールと比べた場合の主な短所は次のとおりである。

■ スループットが低い

■ 高コスト（効果的に運用するにはハイエンドのハードウェアが必要）

■ あまり一般的でないプロトコルや新しいプロトコルのサポートが弱い

厳密には制約とはいえないが、アプリケーション層ファイアウォールは汎用のオペレーティングシステム（Windows、Linux、Unix など）が稼働するホストに実装されることがある。この場合、ファイアウォールのソフトウェア自体に加えて汎用オペレーティングシステムのセキュリティも確保する必要があるため、複雑さが増すことになる。そのため、アプリケーション層ファイアウォールは、専用オペレーティングシステムを使用することもあるアプライアンスベースの装置を使用して導入されることが多くなっている。ルータおよびステートフルインスペクション型ファイアウォールも、専用オペレーティングシステム上で稼働するのが一般的である。

ファイアウォールを使用してメールサーバを確実に保護するには、ファイアウォール（アプリケーションおよび基盤となるオペレーティングシステム）に最新または最高セキュリティレベルのパッチが適用されていることと、ファイアウォールに次の機能があり、かつ、これらをサポートする設定になっている必要がある。

- インターネットとメールサーバの間のあらゆるトラフィックを制御する
- 必要なトラフィック（TCP ポート 25 の SMTP など）を除き、メールサーバへの受信トラフィックをすべてブロックする
- IDS または IPS によって、組織のネットワークへの攻撃に使用されていると報告されている IP アドレスまたはサブネットをブロックする（侵入検知または侵入防止システムと組み合わせ（6.2.2 項を参照））
- 信頼のおける外部のセキュリティ対応センターによってブラックリストに登録された既知のネットワークまたはサブネットをブロックする
- 疑わしい挙動について、ネットワークまたはメールサーバの管理者に適切な手段で通知する（ページャ、電子メール、ネットワークトラップなど）
- コンテンツフィルタリング機能
- マルウェアスキャン機能
- DoS 攻撃から保護する
- 次の詳細情報を含む重要なイベントをログに記録する
  - 日付／時刻
  - インタフェース IP アドレス
  - メーカー固有のイベント名
  - 標準の攻撃イベント ID（存在する場合）
  - 送信元および宛先 IP アドレス
  - 送信元および宛先ポート番号
  - ネットワークプロトコル

ハードウェアおよびソフトウェアとして入手可能なファイアウォール装置のほとんどは、受信したトラフィックについて何らかのログを記録する。ほとんどのファイアウォールでは、ログ機能を有効にしておけばログ設定はデフォルトのままでよい。追加の情報をログに記録する必要があると考える管理者は、メーカーの文書を参照すること。ハードウェアベースのファイアウォール製品は、ブランドによっては、ルール別に情報を追跡および記録する能力を備えている。このような機能により、非常に詳細なレベルの説明責任を果たすことが可能になる。

多くのファイアウォールは、ログに記録する情報を選択的に決定する能力を備えている。これにより、1 つの場所から類似のパケットを連続して受信した場合などは、その最初のパケット以外の残りのパケットを記録しないことがある。これは有用な機能ではあるが、悪意のある行動を示す証拠となり得るパケットが記録されなかった場合にどのような結果がもたらされるかを考慮すべきである。説明責任を果たす上で基本的な要素であるログの原則については、8.1 項で詳しく述べる。

オペレーティングシステムや、セキュリティ対策に使用するその他の要素と同様に、ファイアウォールにも更新プログラムの適用が必要である。更新は、ソフトウェアによるファイアウォールの実装ではより一般的に行われているが、ハードウェアおよびルータのファイアウォールも、ファームウェアに更新を適用する機能を備えている。ファイアウォールに更新を適用する具体的な方法は、メーカーの文書に記載されている。管理者は、ファイアウォール用の更新プログラムが提供されているかどうかを頻繁にチェックすべきである。

6.2.2 侵入検知および侵入防止システム

侵入検知システム（IDS）は、システムまたはネットワークで発生しているイベントを監視して、インシデント発生の可能性についての分析を行うアプリケーションである。インシデントとは、コンピュータのセキュリティポリシー、利用規定ポリシー、標準セキュリティプラクティスの違反または差し迫った違反の脅威を意味する[43]。侵入防止システム（IPS）は、IDS のすべての機能に加え、潜在的なインシデントの防止を試みる機能を備えたものである。IDS システムと IPS システムは、共通の機能を多く備えているため、しばしば両方を合わせて「侵入検知および侵入防止システム」（IDPS）と呼ばれる。IDPS は、インシデントの可能性を検知すると、IDPS コンソールメッセージ、電子メール、ページャ、またはその他のメカニズムによって、その旨を管理者に通知する。

電子メールのセキュリティには、ホストベースおよびネットワークベースの 2 種類の IDPS が最も適している[44]。ホストベース IDPS は、単独のホストの特性と、そのホストの内部で発生しているイベントを監視し、疑わしい活動を識別して阻止する。ホストベース IDPS のソフトウェアは、監視または保護の対象となる各コンピュータにインストールする必要がある。対象ホストコンピュータのオペレーティングシステムと非常に緊密に統合される性格のものであるため、ホストベース IDPS は、オペレーティングシステムの種類ごと（さらに、多くの場合はオペレーティングシステムのバージョンごと）に専用に設計される必要がある。ネットワークトラフィック、システムログ、実行中のプロセス、ファイルに対するアクセスと変更、システムやアプリケーションの設定の変更など、ホストのさまざまな側面が、ホストベース IDPS の監視の対象である。

メールサーバに出入りするほとんどのネットワークトラフィックが暗号化される（SSL／TLS または S/MIME が使用される）場合は、特にホストベース IDPS が有用である。なぜなら、ネットワークトラフィックが暗号化されている場合、ネットワークベース IDPS の機能と能力(下記参照)が極端に制限されるからである。また、ホストベース IDPS はサーバで稼働するため、ネットワークベース IDPS では認識できない攻撃や侵入の試みも検知できることがある。ホストベース IDPS はホストのパフォーマンスに悪影響を及ぼす可能性がある。一般に、より広範な検知能力があり、より多くのイベントを監視するほど、ホストのパフォーマンスに与える悪影響は大きくなる。さらに、ある種の DoS 攻撃などネットワークベースの攻撃を検知できないこともある。侵害されたメールサーバにおいてホストベース IDPS が稼働している場合、ホストベース IDPS 自体も攻撃者によって侵害される可能性が大きく、その逆も同様である。

ネットワークベース IDPS は、特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを監視し、ネットワークおよびアプリケーションの各プロトコルの活動を解析して、疑いのある活動を特定し阻止する。ほとんどのネットワークベース IDPS では、あらかじめ定義された「攻撃シグネチャ」群を使用して攻撃の検知・識別を行う。攻撃シグネチャとは、既知の侵入の種類に対応す

---

43 IDPS の詳細については、NIST SP 800-94『*Guide to Intrusion Detection and Prevention Systems (IDPS)*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

44 その他の主要な IDPS の種類としては、ワイヤレスネットワークプロトコルのみを検査するワイヤレス IDPS と、ネットワークトラフィックフローを監視してフローの異変を検知する NBA（Network Behavior Analysis：ネットワークトラフィック解析）ソフトウェアがある。いずれの種類も、電子メールにかかわる活動の解析は行わない。

るパターンである。ネットワークベース IDPS は、異常な活動、プロトコル違反、その他の通常と異なる活動を識別するためにほかの検知方法も使用する。

ホストベースIDPSと違い、ネットワークベースIDPSでは、多数のホストのネットワーク活動を同時に監視することができる。通常、ネットワークベースの攻撃を検知する能力に優れ、ネットワークに対して現在行われている攻撃の全体像をより簡単に提供することができる。ネットワークベース IDPS は、専用ホストにインストールされるため、メールサーバホストのパフォーマンスには悪影響を与えず、メールサーバへの攻撃が成功してもネットワークベース IDPS がすぐに侵害されることはない。

ただし、ネットワークベース IDPS にも制約があり、攻撃のタイミングがネットワークベース IDPS の攻撃検出能力に大きく影響することがある。たとえば、攻撃者が数時間から数日の期間にわたって攻撃のタイミングを分散させた場合、その攻撃が IDPS に検知されない可能性がある。また、非対称ルーティングなどのネットワーク構成が攻撃検出能力に悪影響を与えることや、(IDPS を直接狙ったものでなくても)DoS 攻撃が IDPS を無効化する可能性がある。さらに、ネットワークへのネットワークベース IDPS の組み込み方によっては、IDPS のハードウェア障害がネットワークの可用性を低下させることも考えられる。

ホストベース IDPS およびネットワークベース IDPS のほとんどは、新しい攻撃を認識できるように攻撃シグネチャデータベースを頻繁に更新する必要がある。更新が頻繁でない IDPS では、最新の(しばしば最も多い)攻撃を認識できない。ゼロデイ攻撃に対しては、適切なシグネチャを用意できない可能性が高いため、いずれの種類の IDPS も、ゼロデイ攻撃を検知する能力は限られたものとなる。ただし、ホストベース IDPS のほうが、攻撃者が侵害に成功したあとの行動(新たな権限のない特権アカウントの作成、悪意のあるソフトウェアのインストールなど)を検知できる可能性が高いので、ゼロデイ攻撃を検知しやすいと考えられる。

ファイルの完全性チェッカは、単純な形態のホストベース IDPS である。ファイルの完全性チェッカは、保護の対象となる個々のファイルのハッシュを計算・保管し、ファイルハッシュのデータベースを確立することにより、システム管理者が、ファイルに対する変更(特に不正な変更)を認識するためのツールを提供する。ファイルの完全性チェッカには、スタンドアロン製品として提供されているものと、ホストベース IDPS に付属しているものがある。一部のホストベース IDPS は、ファイルアクセスの試みを監視したり、ファイルに対する疑わしい読み取り、変更、削除、実行の各操作を阻止したりすることができる。この機能を備えたホストベース IDPS を、メールサーバの重要なファイルを保護するように設定することも可能である。

IDPS を使用してメールサーバを確実に保護するには、IDPS に次の機能があり、かつ、これらを実行する設定になっていることを確認する。

- メールサーバに出入りするネットワークトラフィックを監視する
- メールサーバ上の重要なファイルに対する変更を監視する(ファイルの完全性チェック機能)[45]
- メールサーバホストで利用できるシステムリソースを監視する(ホストベース)
- 組織のネットワークへの攻撃に使用されている IP アドレスまたはサブネットをブロックする(ファイアウォールとの組み合わせ)

---

[45] 一部の重要なファイル(ユーザパスワード格納用ファイル、ログファイルなど)は随時変更されるため、ファイルの完全性チェッカで保護するべきではない。詳細は、使用するメールサーバおよびオペレーティングシステムによって異なる。

- 攻撃が疑われる場合は、組織のインシデント対応ポリシーおよび手続きに従い、必要な連絡先（IDPS 管理者、メールサーバ管理者、インシデント対応チームなど）に適切な手段で通知する
- フォールスポジティブの発生を許容レベルに抑えつつ、スキャンおよび攻撃を可能な限り広範囲に検知する
- 次の詳細を含むイベントをログに記録する
  - 日付／時刻
  - センサーIP アドレス
  - メーカー固有の攻撃名
  - 標準の攻撃名（存在する場合）
  - 送信元および宛先 IP アドレス
  - 送信元および宛先ポート番号
  - ネットワークプロトコル
- 分析およびフォレンジックプロセスのために、ネットワークイベントのパケットヘッダ情報を捕捉する
- 新しい攻撃シグネチャの更新を頻繁に適用する（毎日～毎週など。更新のテスト後に適用されるようにするのが一般的）

また、ネットワークベース IDPS は攻撃の対象になることが多いため、ネットワークベース IDPS およびその稼働基盤となるオペレーティングシステムのセキュリティを強化することも非常に重要である。特に、監視インタフェース経由でのシステム照会には、どのような種類の照会であれ応答するべきでない。リモート管理が必要な場合は、帯域外の手段（隔離された別のネットワークなど）を経由して行うようにする。IDPS は管理が難しく、警告の解釈も難しいのが一般的であるが、攻撃からメールサーバを守るために必要な情報をメールサーバ管理者に提供する重要な早期警報システムである。[Scar07]

6.2.3 ネットワークスイッチ

ネットワークスイッチは、同じネットワークセグメントに配置された複数ホストを接続する装置である。ホスト間の通信を可能にする点ではハブに似ているが、ハブよりも「インテリジェント」であり、通信をその送信先となっているホストにのみ伝送する。セキュリティの観点からのベネフィットは、スイッチが導入されているネットワークでは、ホスト間の通信を傍受することがはるかに難しくなる点にある。これは、メールサーバのあるネットワークセグメントが他のホストにも使用される場合にはきわめて重要である。たとえば、ハブを使用していて DMZ にあるホストが侵害されると、攻撃者は DMZ にある他のホストの通信を傍受でき、結果として、それらのホストや、それらがネットワーク経由で通信する情報が侵害される可能性がある。代表的な例として、公開 Web サーバが挙げられる。公開 Web サーバは、メールサーバと同じサブネットに配置されていることが多く、侵害されると、暗号化されていない電子メールトラフィックやパスワードが DMZ 内で傍受されかねない。

多くのスイッチには、悪意のある主体によってスイッチが「打ちまかされる」ことを困難にし、ネットワークのセキュリティをいっそう強化するために特定のセキュリティ設定項目が用意されている。たとえば、ARP (Address Resolution Protocol)の偽装、および ARP ポイズニングといった攻撃のリスクを

最小限に抑える機能がある[46]。スイッチにこれらを防止する機能があれば、有効にしておくべきである（適切なメーカーの文書を参照）。

スイッチは、ネットワークベース IDPS（6.2.2 項を参照）に悪影響を与える可能性がある。ほとんどのネットワークスイッチには、スパンポートと呼ばれる特定のポートがあり、ネットワーク管理者が設定することにより、スイッチのトラフィックをすべて複製して IDPS が使用するポートに送信することができる。これを使用すると、ネットワークベース IDPS は特定ネットワークセグメント上のトラフィックをすべて参照できる。ただし、負荷の高い状況では、スイッチがスパンポートにトラフィックを送信する動作を中止することがあり、その場合には IDPS がネットワークの活動を監視できなくなる。また、スパンポートは IDPS 以外の装置も使用する場合があるが、一般にスイッチのスパンポートの数は限られているため、すべてのスパンポートが使用されている場合には、IDPS を接続できない可能性もある。

[46] ARP ポイズニングは、攻撃者が偽造した ARP エントリによって標的ホストの ARP キャッシュの更新に成功した場合に発生する。この攻撃は一般に、悪意のある目的のためにネットワークトラフィックをリダイレクトするために行われる。

6.3 安全なネットワーク基盤の実装に関するチェックリスト

完了	アクション
	ネットワーク上の設置場所
☐	メールサーバがメールゲートウェイやファイアウォールによって保護されている内部ネットワークに配置されているか、 または、DMZ 内に配置されているか
	ファイアウォールの設定
☐	メールサーバがファイアウォールによって保護されている
☐	メールサーバに対する脅威が大きい場合や、メールサーバが非常に脆弱である場合は、これがアプリケーション層ファイアウォールによって保護されている
☐	ファイアウォールによって、インターネットとメールサーバの間のあらゆるトラフィックが制御されている
☐	ファイアウォールによって、メールサーバへの受信トラフィックが、必要なポート以外すべてブロックされている。必要なポートとは、TCP ポート 25（SMTP）、110（POP3）、143（IMAP）、398（LDAP）、636（Secure LDAP）、993（Secure IMAP）、995（Secure POP）などである
☐	組織のネットワークへの攻撃に使用されていると IDS または IPS によって報告されている IP アドレスまたはサブネットが、ファイアウォールによってブロックされている（侵入検知または侵入防止システムとの組み合わせ）
☐	ファイアウォールによって、信頼のおける外部のセキュリティ対応センターにおいてブラックリスト登録された既知のネットワークまたはサブネットがブロックされている
☐	ファイアウォールによって、疑わしい挙動はネットワークまたはメールサーバの管理者に適切な手段により通知される
☐	ファイアウォールによって、コンテンツフィルタリングおよびマルウェアスキャン機能が提供されている
☐	ファイアウォールが、DoS 攻撃を防ぐように設定されている
☐	ファイアウォールによって、重要なイベントのログが記録される
☐	ファイアウォールおよびそのオペレーティングシステムに、最新または最高セキュリティレベルのパッチが適用されている
	侵入検知および侵入防止システム
☐	IDPS が、メールサーバに出入りするネットワークトラフィックを監視するように設定されている
☐	IDPS が、メールサーバ上の重要なファイルに対する変更を監視するように設定されている（ホストベース IDPS またはファイルの完全性チェッカ）
☐	IDPS が、メールサーバホストにおいて利用できるシステムリソースを監視するように設定されている（ホストベース IDPS）
☐	IDPS によって、組織のネットワークへの攻撃に使用されている IP アドレスまたはサブネットがブロックされる（ファイアウォールと組み合わせ）
☐	攻撃が疑われる場合には、組織のインシデント対応ポリシーおよび手続きに従い、IDPS によって、必要な連絡先に適切な手段でその旨が通知される
☐	IDPS が、フォールスポジティブの発生を許容レベルに抑えつつ最大限の検知を行うように設定されている
☐	IDPS が、イベントをログに記録し、ネットワークイベントのパケットヘッダ情報を捕捉するように設定されている
☐	新しい攻撃シグネチャの更新を頻繁に適用する（毎日～毎週など。更新のテスト後に適用されるようにするのが一般的）
	ネットワークスイッチ

完了	アクション
☐	ネットワークの傍受を防ぐために、ネットワークスイッチが使用されている
☐	ネットワークスイッチが、ARP 偽装攻撃や ARP ポイズニング攻撃を防ぐ高セキュリティモードに設定されている
☐	ネットワークスイッチが、ネットワークセグメント上の全てのトラフィックをネットワークベースの IDPS に送信するよう設定されている

7. メールクライアントのセキュリティ保護

メールクライアントは何万と存在し、稼働するすべてのメールサーバにアクセスしている。どれだけ強力なセキュリティをメールサーバに施しているとしても、クライアント側のセキュリティはやはり重要である。クライアント側には、多くの面でメールサーバよりも大きなセキュリティ上のリスクがある。適切なレベルのセキュリティをメールクライアントにおいて確保するには、数多くの問題を注意深く検討し、対策を講じる必要がある。このセクションでは、ほとんどのメールクライアントアプリケーションに該当する一般的な推奨事項を示す。特定のアプリケーションのセキュリティに特化した推奨事項は、この文書には含まれない。

7.1 クライアントアプリケーションのインストールおよび設定

7.1.1 メールクライアントへのパッチの適用と更新

メールクライアントのセキュリティを確保するために最も重要な手順は、最新または最もセキュリティの強力なバージョンのメールクライアントにすべての必要なパッチを適用したものを、確実にすべてのユーザに使用させることである[47]。主要なメールクライアントのほとんどには、これまでに重大な脆弱性が見つかっている。特定のメールクライアントの脆弱性については、NIST National Vulnerability Database（米国国家脆弱性データベース、以下、NVD と称す）（http://nvd.nist.gov/）で確認することができる。パッチに関する最良の情報源は、該当するメーカーの Web サイトである。付録 E に、メールクライアントのメーカーWeb サイトの一覧を示す。

一部のメールクライアントは、Web ブラウザとの組み合わせで動作するため、更新がやや複雑になる。たとえば、メールクライアントである Microsoft Outlook と、Web ブラウザである Internet Explorer は緊密に統合およびバンドルされているため、ブラウザの設定変更や脆弱性がメールクライアントに影響する。このような場合、メールクライアントと Web ブラウザの両方を常に更新して安全なバージョンおよびパッチレベルを保つことが特に重要である。安全なバージョンのメールクライアントを使用しないと、以下に述べるほかのセキュリティ対策の実効性が低下することになる。

7.1.2 メールクライアントのセキュリティ機能の設定

デフォルト設定では、メールクライアントは安全な状態になっていないことがある。そのため、次のように設定すべきである。

- メッセージの自動プレビューを無効にする。
- メッセージの自動表示を無効にする。
- メッセージに含まれる画像の自動読み込みを無効にする。
- アクティブコンテンツのダウンロードおよび処理を無効にする（ActiveX コントロール、Java アプレット、JavaScript など）。Web ブラウザとバンドルされているメールアプリケーションでは、これらの機能が Web ブラウザで必要とされる場合があるため、この設定変更を行うと問題が発生する可能性がある。そのような場合には、一部のアクティブコンテンツを慎重に、選択的に無効化／有効化することが必要になる。Microsoft Outlook および Internet Explorer の場合は、それぞれ

[47] パッチを適用するタイミングおよび方法には、この文書の本旨から外れる数多くの複雑な問題が含まれる。セキュリティパッチに関する詳細な議論については、NIST SP 800-40 Version 2.0『*パッチおよび脆弱性管理プログラムの策定（Creating a Patch and Vulnerability Management Program）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

に対してセキュリティゾーンを個別に定義できるため、Internet Explorer のセキュリティを Outlook よりも制限の少ない設定にしておくことができる。

- スパム対策およびフィッシング対策機能がある場合は有効にする。これらはデフォルトであまり厳格な設定になっていないことが多いため、セキュリティの観点からは、より高いレベルに設定することが望ましいと考えられる。また、メッセージのタグ付けやフィルタ処理には誤りも発生するため、マークされたメッセージが実際に不適切なものかどうかを自分で確認して判断できるようにユーザを教育する必要がある。メールクライアントによっては、安全な送信者とブロックする送信者の一覧を作成できるなど、ユーザによるフィルタリングを設定できる機能を備えているものがある。

携帯電話や PDA などの携帯機器で動作するメールクライアントについては、特有の考慮事項がある。近年、携帯用メールクライアントの利用は大きく増加した。ユーザには、携帯機器に格納されている情報がリスクにさらされていること、および、携帯機器が紛失または盗難にあった場合に備えて必要な対策を講じておく必要があることを認識させるべきである。物理的なセキュリティ対策は言うまでもないが、それに加え、携帯機器は一般的にデフォルトではセキュリティの弱い設定になっているため、ユーザは設定変更を行うべきである。考慮すべきセキュリティ機能には、以下が含まれる。

- 機器を使用する際にパスワードまたは PIN が要求されるようにする。
- ローカルに保存するデータ（メッセージ、ダウンロードした添付ファイルなど）を暗号化する。
- メッセージの暗号化および署名添付（またはいずれか一方）を行う。たとえば、S/MIME または OpenPGP のサポートとディジタル証明書の管理を行うこと。
- メールクライアントとメールサーバの間の通信を暗号化する。たとえば、SSL ベースの暗号化を使用して POP、IMAP、SMTP の通信を保護する。
- 機器が侵害された場合のために、機器の使用不能化または情報の削除をリモートから実行できるようにする。
- Bluetooth 機器では、不正アクセスを防ぐために Bluetooth 発見用 PIN の番号を変更する。

また、組織のセキュリティポリシーによって携帯用メールクライアントが保護されるようにすることも必要である。たとえば、ウイルス対策ソフトウェアを利用できる場合はそれを有効にすることや、ワイヤレス機能は不使用時にはオフにしておくことを義務付けるなどを盛り込むべきである。電子メールのアクセスに使用することが望ましくない特定の種類の機器がある場合は、セキュリティポリシーにおいてその制限を規定すべきである。

多くの組織では、携帯端末からの社内ネットワークや社内アプリケーションに対する VPN アクセスを設定することで、リモートからサーバに接続できるようにしている。セキュリティのために、これらのアプリケーションへのアクセスを制限するか、不要なアプリケーションを削除することが望ましい。また、ログイン名、パスワード、その他の個人情報は機器上に保存すべきでない。盗難にあった場合、攻撃者が VPN のネットワークログイン情報を使用して内部ネットワークのリソースにアクセスする可能性があるからである。

7.1.3 認証およびアクセスの設定

初期のメールクライアントアプリケーションは、アクセス先がローカルファイルシステム上のメールボックスに限られ、そのメールボックスファイルを当該ユーザが所有していたため、ユーザ認証を必要としなかった。その後 MUA が発展し、POP および IMAP（セクション 2 を参照）を使用してリモートの

メールボックスにアクセスする機能を提供するようになったため、ユーザ認証が必須になった。この認証は、一般的には、ユーザがメールボックスにアクセスする際にユーザ名とパスワードを入力することで行われてきた。その後、より「ユーザフレンドリ」にするために、メールサーバへのアクセスに使用するユーザ名およびパスワードをメールクライアントの設定ファイルに格納(「記憶」)するようになった。しかしこれは、ユーザの利便性を向上する一方でセキュリティの弱点も生み出す。リモートまたはローカルの攻撃者が、メールクライアントのホストに論理的または物理的にアクセスできると、認証情報、ひいてはメールボックスの内容を入手される可能性がある。また、ユーザ入力の自動補完機能が有効になっていると、これを利用してローカルの攻撃者に体系的にパスワードを突き止められる可能性がある。

パスワードを記憶する機能を無効にすることは、メールクライアントのセキュリティを強化するために効果的な方法である。無効にできない場合は、設定ファイルを十分に保護しておくことが重要である。ほとんどのオペレーティングシステムは、ある程度の保護手段となるファイルアクセス権およびアクセス制御の機能を備えている。この制御が可能なホストでは、ファイル所有者だけがメールクライアント設定ファイルへのアクセスを許可されるようにし、かつ、所有者の制御下にあるディレクトリ内にそのファイルを配置すべきである。ファイルアクセス権およびアクセス制御を使用できないホストの場合は、設定ファイルからユーザのパスワードを削除するのが最良の解決策と考えられる。

対策を要するもう 1 つの部分は、メールクライアントとメールサーバのあいだで行われる実際の通信である。セクション 2 で述べたとおり、デフォルト設定の SMTP、POP、IMAP によるネットワーク通信はいっさい暗号化されない。したがって、ユーザ名、パスワード、およびメッセージ内容は、悪意のある者によって傍受および改ざんされる可能性がある。この通信を SSL／TLS で暗号化することにより、クライアント／サーバ間のセキュリティが向上される。SSL／TLS は広く普及しているメールクライアントのほとんどでサポートされているため、可能であればこれを使用すべきである。中でも TLS バージョン 1 を推奨するが、これを使用できない場合は少なくとも SSL バージョン 3 が望ましい[48]。

どのような電子メールアドレスおよびユーザアカウント名を選択するかも認証に影響する。攻撃者が電子メールアドレスからアカウント名を容易に推測できないように、アカウント名を電子メールアドレスに含めることは避けるべきである。ユーザに電子メールアカウント名の選択を任せている組織では、アカウント名と電子メールアドレスが異なっていて、かつ、関連性がないようにするための管理策を導入すべきである。また、組織の必要性に応じて電子メールアドレスに制約を設けてもよい。たとえば、ユーザのタイプを認識しやすいように、ユーザ種別ごとに異なる命名規則を使用し、外国籍の人のアドレスであれば「*名.姓.国コード@domain.gov*」という形式、委託業者のアドレスであれば「*名.姓.業者名@domain.gov*」という形式にすることなどが考えられる。

7.1.4 クライアントホストのオペレーティングシステムのセキュリティ保護

多くのホストオペレーティングシステムには、直接または間接にメールクライアントのセキュリティを向上させるためのいくつかの設定やその他の方法が用意されている。クライアントホスト全体のセキュリティにとって、ホストオペレーティングシステムは重要な要素の 1 つである。ホストオペレーティングシステムのセキュリティを保護するために実行すべき作業は次のとおりである。

- 最も安全なパッチレベルとなるように最新の状態を維持する。
- ローカルに保管されたメッセージおよびクライアント設定ファイルに対しては、適切なユーザのみがアクセスできるように設定する。

---

[48] TLS および SSL の詳細については、NIST SP 800-52『*Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*』(http://csrc.nist.gov/publications/nistpubs/)を参照のこと。

- Windows ホストの場合、次のように Windows Script Host（WSH）を設定する。[Pits01]
  - WSH を削除するか、管理者のみにアクセスを許可する
  - 次のファイル拡張子について、デフォルトのアクションを実行から編集に変更する[49]。
    - JS（JavaScript）
    - JSE（JavaScript エンコードファイル）
    - VBE（VBScript エンコードファイル）
    - VBS（Visual Basic スクリプト）
    - WS（Windows Script ファイル）
    - WSC（Windows Script コンポーネント）
    - WSF（Windows Script ファイル）
    - WSH（Windows Script Host 設定ファイル）
- Windows ホストの場合、拡張子を完全に表示するよう設定する（これにより、「iloveyou.txt.vbs」のような名前の電子メール添付ファイルが単に「iloveyou.txt」と表示されるのを防ぐ）。
- ウイルス対策アプリケーションをインストールし、すべての受信メッセージと、すべての添付ファイル(開かれた時点で)を自動的にスキャンするよう設定する[50]。また、ウイルス対策ソフトウェアが堅牢なスパイウェア処理機能を備えていない場合は、スパイウェア対策アプリケーションをインストールして使用する。クライアント、サーバ、ネットワークのそれぞれの層に対応するマルウェアスキャンについては、6.2.1 項で詳細に説明する。
- 既存のネットワークセキュリティ装置（ネットワークファイアウォールなど）によってすでに十分保護されている場合を除き、パーソナルファイアウォールをインストールして、不正な通信からコンピュータを保護する。
- 悪意のあるコードは、起動時のセキュリティコンテキスト（当該ユーザのアクセスレベル）で動作するため、オペレーティングシステムによって最小特権の考え方が確実に適用されるようにする。たとえば、ユーザは管理者レベルの特権を持たないアカウントを使用して電子メールの読み取りや作成を実行すべきである。
- オペレーティングシステムの重要コンポーネントを、悪意のあるコードから確実に保護する[51]。
- ファイル暗号化アプリケーションを使用して、ローカル環境にあるユーザのハードディスクに保管されている電子メールを保護する（盗難の可能性が大きいノート型パソコンおよび携帯機器では特に重要）。

---

[49] これらの拡張子を持ったファイルを実行しないようオペレーティングシステムが設定されている場合でも、一部の電子メールクライアントは該当ファイルを実行することがある。

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

[51] 詳細については、NIST SP 800-28『*Guidelines on Active Content and Mobile Code*』および NIST SP 800-83『*悪意のあるソフトウェアによるインシデントの防止と対処のためのガイド（Guide to Malware Incident Prevention and Handling）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

■ コンピュータが使用されず一定時間が経過した場合に現在の OS セッションが自動ロックされるようにオペレーティングシステムを設定する。

7.2 メッセージの安全な作成

機密性のある情報を含んだ電子メールには、送信時のセキュリティを保護するために暗号化を使用すべきである。電子メールの暗号化方式としては、主に S/MIME および OpenPGP の 2 つがある。これらについてはセクション 3 で詳しく述べた。提供される保護のレベルは同程度であるが、これらのアーキテクチャは本質的に異なる。S/MIME のサポートは、ほとんどのメールクライアントに組み込まれているのに対し、OpenPGP はプラグイン形式で提供されるのが普通である。いずれの方式を選択するかは、最終的にいずれが組織の要件に合致しているかによる[52]。一般原則として、暗号化されていない電子メールは、ハガキと同様、誰でも読むことができ、書き換えることができるものとして扱うべきである。

OpenPGP または S/MIME を使用してメッセージを保護する場合は、送信者と受信者の両方がディジタル証明書を入手する必要がある。1 件のディジタル証明書は、証明書の発行対象である人の名前と電子メールアドレス、公開鍵とその有効期限、証明書（ディジタル署名を含む）の発行元 CA（認証局）に関する情報、および、証明書のシリアル番号などの要素により構成される。送信者および受信者のディジタル証明書を保持していれば、送信者は、受信者への電子メールメッセージにディジタル署名し、暗号化を施すことができる。メッセージにディジタル署名することは、次の 3 つを保証する意味において重要である。

■ 真正性：対象メッセージが送信者からのものであることを受信者が確信できること。

■ 否認防止：対象メッセージを作成したことを送信者が否認できないこと。

■ 完全性：対象メッセージが、送信者から受信者へ伝送される間に偶然または悪意によって改ざんされていないこと。

ディジタル証明書は、内部の認証局（CA）から取得することも、公共的なサードパーティ CA から取得することもできる[53]。表 3.3 に、サードパーティ CA の一覧を示す。

暗号化されたメッセージを送受信するよう設定されたメールクライアントにおいて、受信したメッセージは、保護を継続する必要がある場合に限り暗号化形式で保存すべきである。その必要がない場合は、どのメッセージを暗号化したままで保存するかをユーザが選択できるようにするのが望ましい[54]。また、完全性が主たる関心事である場合は、暗号化されていないが、認証されているメッセージを送受信するようメールクライアントを設定してもよい。通常の状況において、メールクライアントは、電子メールセッションごとにパスワードを要求するよう設定すべきである。個々のメッセージを開くたびにパスワードを要求する設定にすると、操作に時間がかかり、ユーザが暗号化による電子メールの保護を使用したがらなくなる可能性がある。そのようなレベルのセキュリティは最高レベルのセキュリティニーズがある場合にのみ採用されるのが普通である。

---

52 これには、セクション 3 で述べた暗号に関する要件が含まれる。

53 CA の詳細については、NIST SP 800-32『*Introduction to Public Key Technology and the Federal PKI Infrastructure*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

54 ユーザはほとんどの場合、添付ファイルを暗号化していない状態で保存したり、暗号化されていない電子メールメッセージテキストを印刷したりなど、電子メールメッセージの内容が保護されていない状態にする操作を実行できる。そのような操作を許可している場合、電子メールを暗号化して保存するよう義務付けると、保護されているという誤った安心感が生まれる可能性がある。また、現時点のクレデンシャルの有効期限が切れると、暗号化されている電子メールを読むのが困難または不可能となることがある。

7.3 プラグイン

メールクライアント向けに、さまざまなプラグインが提供されている。そうしたプラグインを使用すると、メールクライアントの基本的な設定以外の付加機能を利用することができる。入手できるプラグインの種類は、メールの暗号化、ウイルス対策、ポップアップブロック、マルウェア防止などをはじめ、多種多様である。中には、高度なフィルタリング機能を提供するものや、新着メッセージについて音声で通知するものもある。プラグインの種類にかかわらず、それらをインストールするときには注意が必要である。一般的には、信頼のおける提供元から入手したプラグインのみをインストールすること。ディジタル署名されたアーカイブの形態でメーカーから配布されたもの以外を使用することには慎重でなければならない。付加機能を提供する一部のプラグインは、ユーザが訪問した Web サイトを追跡するスパイウェアや、ポップアップ広告を配信するアドウェアなどを内蔵しているものがある。そうしたプラグインが、使用しているインターネットブラウザのツールバーとして自動的にインストールされる場合もある。プラグインを入手する際にメーカーの Web サイトを使用するようにすれば、悪意のあるプラグインをインストールする危険性は小さくなる。

7.4 Web ベースのメールシステムへのアクセス

ユーザの立場からすれば、Web ブラウザを介してメールサーバにアクセスできることは効率的で便利な場合がある。しかし、メールサーバへの Web ベースアクセスを導入する前には、セキュリティ上の検討事項をいくつか考慮しなければならない。それらのうち多くは、標準的なメールクライアントの場合と同様の事項である。たとえば、Web ベースのアクセスはデフォルトでは、POP や IMAP のパスワードとデータを平文で送信するように設定されているのが普通である。セキュリティを向上するには、128 ビット SSL／TLS 経由でしか Web 接続を受け付けないようメールサーバの設定を変更することを検討すべきである[55]。それにより、ユーザ認証および電子メール内容の両方が、ユーザの Web ブラウザから Web サーバへの伝送時に暗号化されるようになる。ただし、メールサーバから受信者までの伝送内容が保護されるわけではない。メッセージの機密性が要求される場合は、何らかの電子メール暗号化方式（S/MIME、OpenPGP など）が必要となる。これらは、残念ながらほとんどの Web ベースメールシステムでは直接サポートされていない。解決策としては、別途データを暗号化してからブラウザに貼り付けて送信する方法が考えられる（OpenPGP を使用して容易に実行できる）。

Web ベースのアクセスを有効にするには、メールサーバの全体的なセキュリティ状態を弱いものにせざるを得ない場合が多い。そのリスクを認識したうえで、メールサーバへの Web ベースアクセスを導入すべきかどうか慎重に検討する必要がある（5.6 項を参照）。

Web ベースのメールシステムにおいて深刻なリスクとなるのは、公共のコンピュータから（学校のコンピュータ室、インターネットカフェ、図書館など）のアクセスである。このような環境では、ユーザ名およびパスワードを自動的に保存および記憶するようブラウザが設定されていることがある。その場合、権限を持たない者が保存されたクレデンシャルを利用して組織のメールサーバにアクセスする可能性がある。もう 1 つの危険は、公共の場にあるコンピュータに、メールユーザのキー入力をすべて（ユーザ名やパスワードも含め）記録するキーストロークロガーが組み込まれている可能性である。この場合もやはり、記録されたデータが組織のメールサーバへのアクセス・侵害を行うのに利用される可能性がある。また、Web ブラウザでは、ユーザがログインしたあと一定の期間にわたって、ユーザのクレデンシャルが一時キャッシュに残る。ユーザがメールサーバへのアクセスを終了した

---

[55] SSL/TLS および Web サーバでのそれらの使用の詳細については、NIST SP 800-44『*Guidelines on Securing Public Web Servers*』および NIST SP 800-52『*Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

あと、ブラウザキャッシュを空にしてブラウザを閉じるという操作を怠った場合、権限を持たない者がキャッシュに残っているクレデンシャルを利用して、組織のメールサーバにアクセスする可能性がある。SSL／TLS は、一般に、以上のような危険への対策とはならない。また、Web ブラウザはダウンロードしたファイルをキャッシュに保持したり、一時ファイルを作成したりする。一時ファイルには、電子メールメッセージ、添付ファイル、および Web ベースメールアクセスにより生成されるその他の情報が含まれている可能性がある。キャッシュや一時ファイルがセッションの終了後に Web ブラウザによって消去されない場合、そのコンピュータを使用する別のユーザがこれらのファイルにアクセスする可能性がある。

Web ベースのメールにおけるセキュリティは、ユーザが専門知識を持っていることに依拠する部分が大きい。たとえば、一部の Web ベースメールアプリケーションでは、公共あるいは個人用いずれのコンピュータを使用するかについての選択を求められるが、電子メールの情報を十分に保護するには、ユーザがこの質問に対して「公共」の選択肢を指定する必要がある。したがって、Web ベースメールへのアクセスを認める前に、ユーザのとるべき行動を認識させなければならない。Web ベースのメールを適切に使用するための行動責任および説明責任を確認する「行動規範」についての合意を策定し、各ユーザに署名を求めることも検討すべきである。

7.5 メールクライアントのセキュリティ保護に関するチェックリスト

完了	アクション
	メールクライアントへのパッチの適用と更新
☐	メールクライアントを、最新または最も安全なバージョンに更新する
☐	メールクライアントに、必要なすべてのパッチを適用する（組織のポリシーおよび設定管理に合わせて）
☐	Web ブラウザに、必要なすべてのパッチを適用する（ブラウザと統合されたメールクライアントの場合）
	メールクライアントのセキュリティ機能の設定
☐	メッセージの自動プレビューを無効にする
☐	メッセージの自動表示を無効にする
☐	メッセージに含まれる画像の自動読み込みを無効にする
☐	アクティブコンテンツのダウンロードおよび処理を無効にする（適切な場合）
☐	スパム対策およびフィッシング対策機能を有効にする
☐	携帯用メールクライアント（携帯電話、PDA 用）の設定を変更してセキュリティを向上する
☐	組織のセキュリティポリシーによって携帯用メールクライアントが保護されるようにする（ウイルス対策ソフトウェアのインストールおよび有効化を義務付けるなど）
☐	携帯機器に実装された VPN クライアントまたはそのほかのリモートアクセスアプリケーションへのアクセスを限定するか、不要なクライアント／アプリケーションを削除する
	認証およびアクセスの設定
☐	セキュリティ保護された認証およびアクセスを有効にする
☐	メールクライアントのユーザ名およびパスワードを保存する機能を無効にする
☐	SMTP、POP、IMAP 通信について暗号化（TLS）を使用するようクライアントを設定する
☐	電子メールアドレスの命名規則に制約を設ける（ユーザアカウント名と関連性のないアドレスにさせるなど）

完了	アクション
	メールクライアントホストのオペレーティングシステムのセキュリティ保護
☐	最も安全なパッチレベルとなるように、OS を最新の状態に維持する
☐	ローカルに保管されたメッセージおよびクライアント設定ファイルに対しては、適切なユーザのみのアクセスを許可するよう OS を設定する
☐	Windows Script Host を安全に設定するかまたは削除する（Windows ホストのみ）
☐	Windows Script Host に関連するファイル拡張子のデフォルトのアクションを実行から編集に変更する（Windows ホストのみ）
☐	拡張子が完全に表示されるよう OS を設定する（Windows ホストのみ）
☐	ウイルス対策ソフトウェアをインストールし、受信メッセージおよび添付ファイルをスキャンするように設定する。ウイルス対策ソフトウェアが堅牢なスパイウェア対策機能を備えていない場合は、スパイウェア対策アプリケーションもインストールする
☐	必要な場合、不正な通信からコンピュータを保護するためにパーソナルファイアウォールをインストールする
☐	悪意のあるコードは、起動時のセキュリティコンテキスト（当該ユーザのアクセスレベル）で動作するため、OS によって最小特権の考え方が確実に適用されるようにする
☐	オペレーティングシステムの重要コンポーネントを、悪意のあるコードから確実に保護する
☐	ファイル暗号化アプリケーションを使用して、ローカル環境にあるユーザのハードディスクに保存されている電子メールを保護する（携帯機器について特に重要）
☐	コンピュータが使用されず一定時間が経過した場合に現在のセッションが自動ロックされるよう OS を設定する
	メッセージの安全な作成
☐	電子メールのメッセージ内容に対するセキュリティを提供する（S/MIME、OpenPGP など）
	プラグインの使用
☐	信頼のおける提供元から入手した、絶対に必要なプラグインのみ有効化およびインストールする
	Web ベースのメールシステムへのアクセス
☐	Web ベースメールアクセスでは 、128 ビット SSL／TLS 接続のみ使用するよう設定する
☐	Web ベースメールへのアクセスを認める前に、ユーザのとるべき行動を認識させる

（本ページは意図的に白紙のままとする）

8. メールサーバの管理

メールサーバの初期の導入後、管理者が継続的にセキュリティを維持する必要がある。このセクションでは、メールサーバを安全に管理するための一般的な推奨事項を示す。重要な活動としては、ログファイルの取り扱いと分析、メールサーバの定期的なバックアップ、メールサーバの侵害からの復旧、メールサーバのセキュリティの定期的なテスト、および、安全なリモート管理の実行などがある。

8.1 ログ

ログを記録することは、確かなセキュリティ状態を維持するための基礎である。正しいデータを記録し、そのログを綿密に監視することは必要不可欠である[56]。ネットワークログおよびシステムログは重要であり、特に、S/MIME または OpenPGP（セクション 3 を参照）に対応したメールサーバでは、ネットワーク監視の有効性が劣るため、システムログの重要性が大きい。メール特有のイベントに関係する追加的なログデータを提供するメールサーバソフトウェアもある。

ログのレビューは、単調で受身の作業であるため、それよりも重要度または緊急度が高いと考える別の任務に時間を割くメールサーバ管理者が多い。しかし、疑わしい行動の記録が唯一残されているのがログファイルである場合がしばしばある。情報をログに記録するメカニズムを有効にすれば、ログを利用して、侵入が失敗または成功したことを検知したり、詳細な調査が必要な場合に警告通知を発したりすることができる。ログファイルの処理および分析と、警告通知のレビューを行うには、そのための手続きとツールが導入されている必要がある。

メールサーバのログによって提供される事項は次のとおりである。

- 詳細調査を要する疑わしい活動についての警告
- 攻撃者の活動の追跡
- システムの復旧支援
- イベントの事後調査支援
- 法的手続きに必要な情報

メール管理者がログの記録に関する設定を確立するために従うべき何とおりかの詳細手順を次に示す。いずれの手順を実行するかは、実際に選択および導入するメールサーバソフトウェアによって異なる。メールサーバソフトウェア製品のメーカーによっては、これらの手順に含まれるガイダンスの内容が完全には該当しない場合もある。

8.1.1 一般的ログ設定の推奨事項

メールサーバのログ記録能力は、製品ごとに異なるが、一般的設定に関する推奨事項を次に示す。メールサーバで記録するログの詳細度は、当該組織における標準的なレベルに設定する。ログの全体的な詳細度レベルを決定したあとは、次のイベントが確実に記録されることを確認する（当該メールサーバソフトウェアでサポートされている場合）。

---

[56] ログの詳細については、NIST SP 800-92『*Guide to Computer Security Log Management*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

■ ローカルホスト関連のログ

- IP スタックの設定エラー
- リゾルバ（DNS、NIS など）の設定に関する問題
- メールサーバの設定に関する問題（DNS との不整合、ローカル設定エラー、古いエイリアスデータベースなど）
- システムリソース（ディスク容量、メモリ、CPU）の不足
- エイリアスデータベースの再構築

■ 接続関連のログ

- 失敗したログイン（容量に十分余裕がある場合は成功したログインも）
- セキュリティに関する問題（スパムなど）
- 失敗した通信（ネットワークの問題）
- プロトコル障害
- 接続タイムアウト
- 接続拒否
- VRFY および EXPN コマンドの使用

■ メッセージ関連のログ

- 代理送信（Send on behalf of）
- 代理送信（Send as）
- 無効なアドレス形式
- メッセージコレクションの統計
- エラーメッセージの生成
- 配信の失敗（固定的エラー）
- メッセージの遅延（一時的エラー）

ログ記録用領域の容量は、管理者による当初の見積もりよりもかなり多く必要になることが多いため、これを常に十分確保することも課題の 1 つである。特に、詳細度を高いレベルに設定する場合は注意が必要である。異なるレベルのログが設定されている場合は、割り当てた領域がいっぱいになることがないよう、管理者がログファイルのサイズを注意深く監視しなければならない。場合によっては、サイズの都合上、ログの削除やアーカイブを行う頻度を上げたり、詳細度のレベルを下げたりする必要が生じることがある。

一部のメールサーバプログラムには、所定のアクセス制御に対するプログラム起動時のチェックを強制または無効にできる機能がある。このレベルの制御機能は、たとえば、ファイルアクセスに関する管理作業のミスによってログファイルが意図せずに改ざんされることを防ぐために役立つ場合が

ある。どのような状況下でこのようなチェックを有効にするかは、メールサーバ管理者が判断すべき事項である（本機能がメールサーバソフトウェアによってサポートされている場合）。

8.1.2 ログファイルのレビューおよび記録保持

ログファイルのレビューは、退屈で時間のかかる作業だが、管理者はすでに発生したイベントに関する情報をこれによって得ることができる。ログからの情報は、CPU 稼働率の一時的な急上昇や、IPS から報告される正常でないネットワークトラフィックといった他の証拠の裏づけを得るのにしばしば役立つ。この目的でログを使用する場合は、対象を絞り込んだレビューを行う。たとえば、午前 8 時 17 分、メールサーバへの受信接続において VRFY コマンドの実行が試みられた旨が IPS から報告された場合、午前 8 時 17 分の直前に生成されたログを確認するのが適切である。また、メールサーバのログをレビューして、攻撃またはスパム送信の兆候についても確認すべきである。レビューの頻度をどの程度にするかは、次の要素に応じて異なる。

- サーバが受信するトラフィックの量
- 全般的な脅威レベル（ほかのサイトと比べて攻撃を受ける回数が非常に多いサイトでは、ログをより頻繁にレビューすべきである）
- 特定の脅威（時折、ログファイル分析の頻度を上げることを要する特定の脅威が発生する）
- メールサーバの脆弱性
- メールサーバによって提供されるデータおよびサービスの価値

レビューは定期的に（たとえば毎日）行うほか、疑わしい活動が発見された場合や、脅威について警告が発せられた場合に行うべきである。この作業は、すぐにメール管理者の大きな負担となるのが明らかであるため、負担を軽減するために自動ログ分析ツールが開発されている（8.1.3 項を参照）。

また、長期的な分析や、より綿密な分析を行うことも必要となる。メールサーバに対する攻撃においては、数百件もの異なる要求を送信するのが普通であるため、攻撃者は、個々の要求を送信する間隔を大きくとってメール攻撃を隠そうとすることがある。そのような場合、1 日または 1 週間のログをレビューしただけでは動向を把握できない可能性があり、週、月、あるいは四半期を超えて長期にわたる動向を見るほうが、同じホストやサブネットから複数の攻撃が仕掛けられていることを発見できる可能性がある。

メールサーバが攻撃者によって侵害されたとき、攻撃を隠蔽するためにログファイルが改ざんされないように、ログファイルは確実に保護すべきである。暗号化もログファイルの保護に役立つが、最良の方法は、メールサーバとは別のホストにログファイルを保存することである。そのようなホストを、しばしば「集中化ログサーバ」と呼ぶ。集中化ログへの記録は、標準のログプロトコルである syslog を使用して行われることが多い[57]。また、組織によっては SIEM（Security Information and Event Management：セキュリティ情報およびイベント管理）ソフトウェアを使用する場合もある。SIEM は、集中化サーバによってログの分析を実行し、データベースサーバを使用してログを保存し、各ホストに

[57] syslog の定義については、IETF RFC 3164『*The BSD Syslog Protocol*』（http://www.ietf.org/rfc/rfc3164.txt）を参照のこと。

インストールされるエージェントによって、特定の種類のログ（メールサーバログなど）の解析および集中化サーバへのデータ転送を行う[58]。

ログファイルは、定期的にバックアップし、アーカイブに保管すべきである。一定期間にわたりログファイルをアーカイブに保管することは、特定の法的措置の裏づけや、メールサーバに問題が発生した場合のトラブルシューティングなど、いくつかの理由で重要である。アーカイブにログファイルを保持する期間をどの程度にすべきかは、次を含むいくつかの要素に応じて異なる。

- 法的な要件
- 組織としての要件
- ログのサイズ（サイトのトラフィックおよび記録する詳細項目の数に直接関係する）
- メールサーバのデータおよびサービスの価値
- 脅威のレベル

8.1.3 ログファイル自動分析ツール

ほとんどのメールサーバが受信するトラフィックは大量であり、ログファイルのサイズは短期間で巨大になる。したがって、メールサーバ管理者の負担を軽減するためにログ自動分析ツールをインストールすべきである。ログ自動分析ツールは、メールサーバのログファイルに含まれるエントリを分析し、疑わしい活動や通常と異なる活動を識別するものである。9.1.2 項で触れたとおり、ログを集中化するために SIEM ソフトウェアを使用する組織もあるが、SIEM ソフトウェアにもログファイルの自動分析を実行する機能がある。

定期的な分析をサポートするツールは、商用およびパブリックドメインで多数提供されている。ログ自動分析ツールによって疑わしいと判断されたイベントは、フォローアップ調査を促すために、できるだけ早く担当のメール管理者またはセキュリティインシデント対応チーム宛てに転送されるべきである。組織によっては、ログに記録された攻撃やその他の注目すべきイベントを見落とすリスクを低減するために複数のログ分析ツールを併用することも考えられる。[Kent06]

8.2 メールサーバのバックアップ

メールサーバ管理者の最も重要な役割の 1 つが、メールサーバ上にあるデータの完全性を維持することである。メールサーバは、組織のネットワークにおいて、外部への露出と必要性が最も高いサーバの一つであるため、その完全性を保つことは重要である。いくつかの理由から、メール管理者はメールサーバのバックアップを定期的に行う必要がある。たとえば、悪意のある行動、意図しない行動、あるいは、ハードウェアまたはソフトウェアの障害によって、メールサーバが故障することが考えられる。また、連邦政府機関およびその他多くの組織には、メールサーバデータのバックアップおよびアーカイブに関する規制が適用される。法律上および会計上の理由からも、定期的にバックアップを実行すべきである。

すべての組織は、メールサーババックアップポリシーを策定する必要がある。ポリシーの内容に影響する主な要因は次の 3 つである。

---

[58] syslog および SIEM の実装の詳細については、NIST SP 800-92『*コンピュータセキュリティログ管理ガイド（Guide to Computer Security Log Management）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

■ 法的な要件

- 適用される法律および規制（連邦、州、国際）
- 訴訟にかかわる要件

■ ミッション上の要件

- 契約
- 慣例
- 組織にとってのデータの重要度

■ 組織のガイドラインおよびポリシー

メールサーバのバックアップポリシーは、組織ごとに固有の環境を反映するために内容の差異が生じるが、次の事項が盛り込まれているべきである。

■ メールサーババックアップポリシーの目的

■ メールサーババックアップポリシーの影響を受ける当事者

■ バックアップポリシーの対象となるメールサーバ

■ 主な用語の定義（特に、法律用語と技術用語）

■ 法律、業務、組織それぞれの観点からの詳細要件

■ 求められるバックアップ頻度

■ データが正しく保持および保護されるようにするための手続き

■ 不要になったデータが正しく破棄またはアーカイブされるようにするための手続き

■ 米国情報公開法（FOIA：Freedom of Information Act）による要求、法的調査、その他類似の要求に対応するために情報を保全する手続き

■ データの保持、保護、破棄の活動に関わる者の責任

■ ログに記録する情報の種類ごとの保持期間[59]

■ 中央または当該組織レベルのデータバックアップチームが存在する場合は、そのチームの具体的な任務

バックアップは、完全バックアップ、増分バックアップ、および差分バックアップの 3 種類に大別される。完全バックアップでは、オペレーティングシステム、アプリケーション、および、メールサーバに保存されたデータ（つまり、メールサーバのハードディスクに保存されているすべてのデータ）をバック

---

[59] 電子メールメッセージ、トランザクションログ、その他のメールサーバ関連の記録に関する保持期間については、慎重に検討すべきである。多くの組織には、電子メール記録の保持に影響する法律上および規制上の要件が複数セット適用される。NARA（National Archives and Records Administration: 米国国立公文書館）は、連邦政府の記録管理に関する Web サイトを設置している（http://www.archives.gov/records-mgmt/）。NARA のメール保持関連規制の詳細については、http://edocket.access.gpo.gov/2006/pdf/06-1545.pdf を参照のこと。連邦政府機関では、電子メールを長期（たとえば、1 年またはそれ以上）にわたり保持する場合が多いが、その他の組織では 30～90 日程度が一般的である。

アップする。メールサーバ全体をバックアップ実行時点の状態（設定、パッチレベル、データなど）に容易に復旧できるメリットがある反面、実行に長い時間と大量のリソースを要するというデメリットがある。増分バックアップは、前回のバックアップ（完全または増分）以降に変更のあったデータだけをバックアップするため、完全バックアップのデメリットを削減することができる。

差分バックアップでは、前回の完全バックアップ以降に変更のあったデータをすべてバックアップするため、設定を復旧する際にアクセスしなければならないバックアップセットの数を抑えることができる。ただし、完全バックアップからの経過期間が長くなるにつれて個々の差分バックアップが次第に大きくなり、増分バックアップに比べて長い処理時間と大きなストレージ容量が必要になる。一般に、完全バックアップはあまり頻繁に実行せず（週ごと、月ごと、または大幅な変更が生じた場合など）、増分または差分バックアップをより頻繁に（日～週ごと）実行する場合が多い。バックアップの頻度を決定する要素は、次のようにいくつかある。

- メールサーバに保存されている情報およびメールサーバの設定の変動性
- バックアップするデータの量
- 使用可能なバックアップ装置およびメディア
- バックアップデータのダンプに使用できる時間
- データの重要度
- メールサーバが直面する脅威のレベル
- データバックアップなしでデータを再構築するために必要な労力
- メールサーバが備えるその他のデータバックアップまたは冗長化機能（RAID など）

電子メールデータをアーカイブまたはバックアップする際は、一般に次のガイドラインに従うべきである。

- ライトワンス･リードメニーメディア(write-once, read-many media:書き込みは一回限りだが読み取りは何度でもできるメディア)を採用する（アーカイブした情報が改ざんまたは偶発的に消去されるのを防ぐために使用）
- データが正しくバックアップまたはアーカイブされたことを確認するために検証機能を含める
- 保存する情報の日付および時刻を記録して時系列管理する機能を含める
- バックアップメディアに保存した索引およびレコードを容易に検索できるようにする
- 少なくとも 2 つのコピーを地理的に離れた複数の場所に保管する
- 原本メディアおよび複製メディアの両方に保持されているすべての情報を正確に整理および索引付けする

8.3 セキュリティ侵害からの復旧

ほとんどの組織では、内部ネットワークにある一つあるいは複数のホストが侵害される事態が、いつか発生することになる。侵害から復旧するための最初の手順は、侵入が成功した場合に必要とな

るポリシーおよび手続きを、侵入が行われる「前」に策定・文書化しておくことである[60]。対応手続きには、メールサーバの侵害が成功した場合の対応に必要な各種アクションの概要と、それらアクションの適切な実行順序を規定すべきである（順序はきわめて重要になることがある）。ほとんどの組織には、専任のインシデント対応チームがすでに設置されており、侵害の疑いまたは確証がある場合には、ただちに当該チームに連絡すべきである。また、組織が、コンピュータおよびネットワークフォレンジックの分野に詳しいスタッフを組織内に確保したいと考えることもあるだろう[61]。

メールサーバ管理者は、インシデント処理に関する組織のポリシーおよび手続きに従うべきであり、また、セキュリティ侵害の疑いまたは確証を得たあとは、アクションを実行する前に、インシデント対応チームに連絡して助言を求めるべきである。侵害の成功を発見したあとに実行される一般的な手順には、たとえば次のようなものがある。

- 当該インシデントについて、組織のコンピュータインシデント対応チームに報告する
- 侵害されたシステムを隔離するか、その他の手順によって攻撃を封じ込め、詳細情報を収集できるようにしておく[62]
- 必要に応じてマネジメント、弁護士、法執行当局などにただちに相談する
- 類似のホスト[63]を調査し、攻撃者が同様に別のシステムも侵害していないか確認する
- 侵入について次のように分析する
  - 最も早く失われるデータ（現在のネットワーク接続、メモリダンプ、ファイルのタイムスタンプ、ログインしているユーザなど）から順に、サーバの現在の状態を採取する
  - システムのソフトウェアおよび設定に加えられた変更
  - データに加えられた変更
  - 攻撃者が置き去りにしたツールまたはデータ
  - システムログ、侵入検知、ファイアウォールのログファイル
- システムを復旧する
  - 次のいずれかを実行する
    - オペレーティングシステムを新規インストールする

---

60 この領域の詳細については、NIST SP 800-61『*コンピュータセキュリティインシデント対応ガイド（Computer Security Incident Handling Guide）*』および NIST SP 800-18 Revision 1『*連邦情報システムのためのセキュリティ計画作成ガイド（Guide for Developing Security Plans for Federal Information Systems）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

61 コンピュータおよびネットワークフォレンジックの詳細については、NIST SP 800-86『*インシデント対応へのフォレンジック技法統合化ガイド（Guide to Integrating Forensic Techniques into Incident Response）*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

62 証拠を収集する意図がある場合、システムの隔離は多大な慎重さをもって行う必要がある。攻撃者の多くは、侵害されたシステムがネットワークから切り離されたり再起動されたりした場合に証拠が隠滅されるようにシステムの設定を変更する。隔離の方法としては、直近の上流スイッチまたはルータの設定変更などが考えられる。

63 類似のホストとは、侵害されたホストと同じ IP アドレス範囲に属するもの、同じまたは類似のパスワードが設定されたもの、ホスト同士の信頼関係を確立しているもの、同じオペレーティングシステムやアプリケーションが稼働しているものなどである。

  - バックアップから復旧する（場合によってはより大きなリスクがある。バックアップ内容が侵害発生後のものである可能性があり、復旧後も攻撃者のアクセスを受け入れることになりかねない）
  - 不要なサービスを無効にする
  - すべてのパッチを適用する
  - すべてのパスワードを変更する（侵害されてないホストについても必要に応じて変更する）
  - ネットワークセキュリティ要素（ファイアウォール、ルータ、IPS）の設定を、保護および通知を強化するよう変更する
- システムをテストし、セキュリティが確保されていることを確認する
- システムをネットワークに再接続する
- システムとネットワークを監視し、攻撃者が再びシステムやネットワークにアクセスしようとしている徴候に注意する
- 得られた教訓を文書化する

侵害されたシステムのオペレーティングシステムを再インストールするか、バックアップから復旧するかは、組織のポリシーおよび手続きに基づいてシステム管理者が決定すべきである。判断は、次のような要素を考慮して行われることが多い。

- 攻撃者が獲得したアクセスのレベル（root、ユーザ、ゲスト、システムなど）
- 攻撃者の種類（内部、外部）
- 侵害の目的（電子メールのなりすまし、不正ソフトウェアリポジトリ、さらなる攻撃への踏み台）
- システム侵害に使用された手法
- 侵害行為の実行中および実行後に攻撃者がとった行動（ログファイル、侵入検知報告などより）
- 侵害行為が行われた時間の長さ
- ネットワーク内における侵害の波及範囲（侵害されたホストの台数など）
- マネジメントおよび弁護士との話し合いの結果

攻撃者の獲得したアクセスレベルが低いほど、また、攻撃者のとった行動についてメールサーバ管理者の理解が深いほど、バックアップを使って復旧し、脆弱性にパッチを適用することのリスクは小さくなる。攻撃者の行動をあまり把握できない場合や、攻撃者に高レベルのアクセスを獲得された場合、オペレーティングシステムおよびアプリケーションはメーカーから入手した配布メディア原本を使用して再インストールし、メールサーバのデータは正常であることを確認済みのバックアップから復旧することを推奨する。

法的措置を検討する場合は、侵害後のホストの取り扱いに関するガイドラインをシステム管理者が認識している必要がある。必要に応じて、弁護士および法執行当局とも話し合いを持つこと。

8.4 メールサーバのセキュリティテスト

公開のメールサーバについては、定期的なセキュリティテストが不可欠である[64]。これを行わなければ、現時点の保護手段に実効性があることや、メールサーバ管理者によって適用されたばかりのセキュリティパッチが発行元の説明通りに機能することは保証されない。セキュリティテストの手法には、さまざまな種類が存在するが、最も一般的なのは脆弱性スキャンである。脆弱性スキャンは、脆弱性を特定する作業と、既存のセキュリティ対策に実効性があるかどうかを確認する作業についてメールサーバ管理者を支援する。また、ペネトレーションテストも使用されるが、これが実施される頻度は低く、組織のネットワーク全体に関するペネトレーションテストの一環としてのみ行われるのが普通である[65]。

8.4.1 脆弱性スキャン

脆弱性スキャナは、脆弱性およびホストの設定ミスを特定するために使用される自動ツールである。また、発見した脆弱性を緩和するための情報を示す機能を備えるものも多い。

脆弱性スキャナは、スキャン対象ホストに存在する脆弱性の特定を試みることにより、バージョンが古くなったソフトウェアや適用されていないパッチおよびシステムのバージョンアップを見つけたり、組織のセキュリティポリシーに対する適合性の可否、ポリシーからの逸脱の有無を確認したりする作業を支援する。これは、ホスト上で稼働するオペレーティングシステムや主要ソフトウェアアプリケーションを識別して既知の脆弱性と照合することにより行われる。脆弱性スキャナは、一般的に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、脆弱性の大規模なデータベースを利用する。

しかし、脆弱性スキャナには大きな弱点がある。それは、表面的な脆弱性の特定はできるが、スキャンの対象となったメールサーバ全体としてのリスクレベルはわからないということである。スキャンプロセスは自動化されているが、フォールスポジティブエラー（存在しない脆弱性を誤認して報告すること）が高い確率で発生するため、メールサーバのセキュリティと管理に関する専門知識のある人間がスキャン結果を見て判断する必要がある。また、独自に開発したコードやアプリケーションに含まれる脆弱性は、一般に脆弱性スキャナでは発見できない。

スキャナで最新の脆弱性を認識するには、脆弱性データベースを定期的に更新しなければならない。どのようなスキャナであれ、実行する前に脆弱性データベースに最新の更新を取り込むべきである。更新が提供される頻度は、脆弱性データベースによって違いがある（脆弱性スキャナを選定するにあたり、更新の頻度は重要な考慮事項である）。

単一のスキャナ製品がすべての既知の脆弱性にタイミングよく対応するのは不可能であるため、脆弱性スキャナは、あまり知られていない脆弱性よりも、よく知られている脆弱性に対してより良好な検知能力を示すことが多い。また、メーカー各社は、自社のスキャナの速度を高く維持することを考えている（より多数の脆弱性を検出しようとすると、実行するテストの量が増え、スキャンの全体的な処理速度が低下する）。こうした事情から、使用しているメールサーバまたはオペレーティングシス

---

64 Web ベースのメールアクセスを提供する場合は、そのアクセスを提供している Web サーバの定期セキュリティテストも必要となる。Web サーバを対象としたセキュリティテストの実行については、NIST SP 800-44『*Guidelines on Securing Public Web Servers*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

65 脆弱性スキャン、ペネトレーションテスト、およびそのほかのテストテクニックの詳細については、NIST SP 800-42『*ネットワークセキュリティテストにおけるガイドライン*（Guideline on Network Security Testing）』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

テムがあまり一般的なものでない場合や、カスタム開発したアプリケーションを使用している場合、脆弱性スキャナはほとんど役立たない可能性がある。

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なサービス（ポート）、脆弱なサービス（ポート）の特定
- アプリケーションの特定およびバナーの取得
- オペレーティングシステムの特定
- 検知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遵守されているかどうかのテスト

オペレーティングシステムおよびメールサーバアプリケーション類に最新のセキュリティパッチが適用され、最新バージョンが使用されていることを確認するために、脆弱性スキャンを実施すべきである。脆弱性スキャンは、スキャン結果の解釈作業に人手を要する部分が大きい、非常に手間のかかる作業である。ネットワークの帯域幅が占有され、応答速度が低下し、スキャン対象となっているサーバやアプリケーションの可用性に悪影響が生じる可能性もあるなど、運用の妨げにもなる可能性がある。しかし、攻撃者に発見され悪用される前に、可能な限り早期に脆弱性を緩和するためにはきわめて重要であるため、毎週から毎月の頻度で脆弱性スキャンを実施すべきである。また、多くの組織では、採用しているスキャナアプリケーション用の新しい脆弱性データベースが提供されるたびに脆弱性スキャンを実行している。スキャンの結果は文書化し、発見された欠陥は是正すべきである。

脆弱性スキャナは、複数種類を併用することも組織として検討すべきである。前述のとおり、既知の脆弱性すべてを検知できるスキャナは存在しないが、2 種類のスキャナを使用すれば、検知できる脆弱性の数は一般に向上する。そこで、商用のスキャナ製品を 1 つとフリーウェアのスキャナを 1 つ使用することが広く行われている。ネットワークベースおよびホストベースの脆弱性スキャナが、無料または有料で流通している。

8.4.2 ペネトレーションテスト

ペネトレーションテストとは、「評価者がシステムの設計および実装に対する自身の理解に基づいて、当該システムのセキュリティ機能の迂回を試みることにより行う、セキュリティテストの一種」[NISS99]である。ペネトレーションテストの目的は、一般的なツールと攻撃者によって開発されたテクニックを使用してシステム保護（特に、攻撃の兆候に対する人的な対応）の訓練を行うことである。複雑なシステムや重要度の高いシステムについては、ペネトレーションテストの実施を強く推奨する。

あらゆる組織の情報セキュリティプログラムにとって、ペネトレーションテストはきわめて価値の高いテクニックとなり得る。しかしその反面、実施にはひじょうな手間がかかり、対象となるシステムのリスクを最小限に抑えるための高度な専門性も必要となる。少なくともネットワーク探査や脆弱性スキャンによって組織内ネットワークの応答速度が低下する可能性があり、場合によっては、テストの実施中にシステムが損傷したり運用不能な状態に陥ったりすることも考えられる。実施者がペネトレーションテストについて豊富なノウハウを持っていれば、こうしたリスクは小さくなるが、リスクを完全に排除することはできない。

ペネトレーションテストには次のメリットがある。[Wack02b]

- 攻撃者と同じ方法論やツールを使用してネットワークをテストできる
- 脆弱性が存在するかどうかを検証できる
- 表面的な脆弱性が見つかるだけでなく、脆弱性が反復的に悪用され、アクセスが拡大される可能性を示すことができる
- 脆弱性が純粋に仮定上のものでないことを実証できる
- セキュリティの問題に取り組む必要性に「現実味」を与えることができる
- 人的な手続きや、ソーシャルエンジニアリングに対する人的要素の弱さをテストできる

8.5 メールサーバのリモート管理

メールサーバのリモート管理は、そのリスクを慎重に考慮していない限り許可しないよう強く推奨する[66]。いっさいのリモート管理を禁止するのが最も安全であるが、そうすることが現実的でない組織もある。リモート管理を可能にすることで生じるリスクの大きさは、ネットワークのどこにメールサーバを設置するかによって大きく異なる（6.1 項を参照）。メールサーバがファイアウォールの内側にある場合、内部ネットワークからのリモート管理は、若干のリスクを伴うものの比較的安全に実装することができる。組織の外部にあるホストからのリモート管理は、当該組織のリモートアクセスソリューション（VPN など）を経由して当該組織の制御下にあるコンピュータから行う場合を除き、一般に許可すべきでない。

メールサーバのリモート管理が必要と判断される場合は、可能な限り安全なリモート管理を実装するために次の手順に従うべきである。

- 強力な認証メカニズムを使用する（公開／秘密鍵ペア、2 要素による認証など）。
- リモート管理に使用可能なホストを次のように限定する。
  - 権限を有するユーザに限定する
  - （ホスト名でなく）IP アドレスで制限する。たとえば、内部ネットワーク上にある一部または全部のホストを許可、または、組織のエンタープライズリモートアクセスソリューションを使用するホストを許可
- SSH(Secure Shell)、HTTPS(Secure HTTP)など、暗号化によりパスワードとデータの両方が保護されるセキュリティプロトコルを使用する。セキュリティの劣るプロトコル（Telnet、FTP、NFS、HTTP など）は許可しないが、使用せざるを得ない場合は、必ず暗号化プロトコル（SSH、SSL、IPSec など）によりトンネリングする。
- 最小特権の考え方をリモート管理に適用する（たとえば、リモート管理用のアカウントには最小限のアクセス権のみ付与する）。
- インターネットを経由したファイアウォール越しのリモート管理は、VPN など強力なセキュリティメカニズムを使用しない限り許可しない。

---

[66] Web ベースのメールアクセスに使用する Web サーバについても同様の注意が必要である。詳細については、NIST SP 800-44『*Guidelines on Securing Public Web Servers*』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

■ リモート管理用のユーティリティまたはアプリケーションに設定されているデフォルトのアカウントやパスワードはすべて変更する。

■ 内部ネットワーク上のファイル共有をメールサーバからマウントしない。また、メールサーバ上のファイル共有を内部ネットワークからマウントしない。

8.6 メールサーバの管理に関するチェックリスト

完了	アクション
	ログ
□	IP スタックの設定エラーを記録する
□	リゾルバ（DNS、NIS など）の設定に関する問題を記録する
□	メールサーバの設定に関する問題（DNS との不整合、ローカル設定エラー、古いエイリアスデータベースなど）を記録する
□	システムリソース（ディスク容量、メモリ、CPU）の不足を記録する
□	エイリアスデータベースの再構築を記録する
□	ログインを記録する（失敗のみ。容量に十分余裕がある場合は成功も）
□	セキュリティに関する問題（スパムなど）を記録する
□	失敗した通信（ネットワークの問題）を記録する
□	プロトコル障害を記録する
□	接続タイムアウトを記録する
□	接続拒否を記録する
□	VRFY および EXPN コマンドの使用を記録する
□	代理送信（Send on behalf of）を記録する
□	代理送信（Send as）を記録する
□	無効なアドレス形式を記録する
□	メッセージコレクションの統計を記録する
□	エラーメッセージの生成を記録する
□	配信の失敗（固定的エラー）を記録する
□	メッセージの遅延（一時的エラー）を記録する
□	別個のログサーバにログを保存する
□	組織の要件に従ってログをバックアップおよびアーカイブする
□	ログのレビューを毎日行う
□	ログのレビューを毎週行う（長期的な動向を把握するため）
□	ログファイル自動分析ツールを使用する
	メールサーバのバックアップ
□	メールサーバのバックアップポリシーを策定する
□	メールサーバの差分または増分バックアップを、1 日単位から週単位で作成する
□	メールサーバの完全バックアップを、週単位から月単位で作成する
□	バックアップを定期的にアーカイブする
	侵害からの復旧
□	インシデントを組織のコンピュータインシデント対応チームに報告する
□	侵害されたシステムを隔離するか、そのほかの手順によって攻撃を封じ込め、証拠を収集できるようにする

完了	アクション
☐	必要に応じてマネジメント、弁護士、法執行当局などにただちに相談する
☐	類似のホストを調査し、攻撃者が同様に別のシステムも侵害していないか確認する
☐	侵入について分析する
☐	システムを復旧する
☐	システムをテストし、セキュリティが確保されていることを確認する
☐	システムをネットワークに再接続する
☐	システムとネットワークを監視し、攻撃者が再びシステムやネットワークにアクセスしようとしている兆候に注意する
☐	得られた教訓を文書化する
	セキュリティテスト
☐	メールサーバとそれを支えるネットワークを対象に脆弱性スキャンを定期的に実施する
☐	テストの前に脆弱性スキャナを更新する
☐	脆弱性スキャナにより特定された欠陥を是正する
☐	メールサーバとそれを支えるネットワーク基盤を対象にペネトレーションテストを実施する
☐	ペネトレーションテストにより特定された欠陥を是正する
	リモート管理
☐	強力な認証メカニズムを使用する（公開／秘密鍵ペア、2 要素による認証など）
☐	リモート管理に使用可能なホストを、IP アドレスまた許可を与えたユーザに基づいて限定する
☐	暗号化によりパスワードとデータの両方が保護されるセキュリティプロトコルを使用する（SSH、HTTPS など）
☐	最小特権の考え方をリモート管理に適用する（たとえば、リモート管理用のアカウントには最小限のアクセス権のみ付与する）
☐	リモート管理用のユーティリティまたはアプリケーションに設定されているデフォルトのアカウントやパスワードをすべて変更する
☐	インターネットを経由したファイアウォール越しのリモート管理は、VPN などのメカニズムを使用しない限り許可しない
☐	内部ネットワーク上のファイル共有をメールサーバからマウントしない。また、メールサーバ上のファイル共有を内部ネットワークからマウントしない。

付録A—用語集

Address Resolution Protocol（ARP、アドレス解決プロトコル）— ノードの物理アドレスの取得に使用されるプロトコル。クライアントステーションは、通信したいターゲットノードの IP（Internet Protocol）アドレスを指定してネットワーク上に ARP 要求をブロードキャストする。該当するアドレスを持つノードは、応答として自身の物理アドレスを返信する。これにより、ターゲットノードへのパケット伝送が可能となる。

本文（Body）— 電子メールメッセージにおいて、当該メッセージの実際の内容が含まれるセクション。

非武装地帯（DMZ：Demilitarized Zone）— 組織の内部ネットワークとインターネットの間に「中立地帯」として挿入されるホストまたはネットワークセグメント。

ヘッダ（Header）— 電子メールメッセージ内において、当該メッセージに関する重要情報（送信日、送信者、宛先、配信パス、件名、形式情報など）が含まれるセクション。本文が暗号化される場合でも、ヘッダは一般に平文のまま残されるのが普通である。

Internet Message Access Protocol（IMAP、インターネットメッセージアクセスプロトコル）— IETF RFC 3501 で定義されるメールボックスアクセスプロトコル。最も一般的に使用されているメールボックスアクセスプロトコルの 1 つである。IMAP には、POP と比較してはるかに広範なコマンドセットが用意されている。

ローカル配信エージェント（LDA：Local Delivery Agent）— メールサーバ上で動作するプログラム。送信者と受信者のメールボックスが同じメールサーバ上にある場合に両者の間でメッセージの配信を行う。配信の前に、あらかじめ定義されたメッセージフィルタに基づいメッセージを処理する場合もある。

メールサーバ（Mail Server）—「電子郵便」機能を提供するホスト。受信メールをユーザに配送するために保管し、送信メールを転送する。この用語は、当該サービスを実行するアプリケーション（他のサービスと同じコンピュータ上で動作することも可能）だけを意味する場合があるが、この文書においては、メールサーバアプリケーション、ホストオペレーティングシステム、およびそれらを支えるハードウェアを含めたホスト全体を指すものとする。

メールサーバ管理者（Mail Server Administrator）— メールサーバにとってシステム管理者に相当する人。メールサーバの全体的な設計および実装に責任を持つシステムアーキテクトである。

メール転送エージェント（MTA：Mail Transfer Agent）— メールサーバ上で動作するプログラム。メールユーザエージェントまたは別の MTA からメッセージを受信し、それらをまた別の MTA に転送するか、当該 MTA 上の宛先に宛てられたメッセージについては、受信者に配送するためにローカル配信エージェント（LDA）に引き渡す。一般的に使用されている MTA には、Microsoft Exchange および sendmail などがある。

メールユーザエージェント（MUA：Mail User Agent）— エンドユーザがメールサーバにアクセスして電子メールメッセージの読み取り、作成、および送信を行うために使用するメールクライアントアプリケーション。一般的に使用されている MUA には、Microsoft Outlook および Mozilla Thunderbird などがある。

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

Multipurpose Internet Mail Extensions（MIME、多目的インターネットメール拡張）— IETF RFC 2822 メッセージのヘッダを利用してリッチメッセージ内容の構造を記述するプロトコル。

ネットワーク管理者（Network Administrator）— 組織内のネットワークを管理する人。ネットワークのセキュリティ、新しいアプリケーションのインストール、ソフトウェアアップグレードの配布、日常における稼働状況の監視、ライセンス契約の遵守、ストレージ管理プログラムの策定、定型的なバックアップの提供などを職責とする。

Open Pretty Good Privacy（OpenPGP）— 公開鍵暗号を使用したメッセージの暗号化および証明書の作成に関する、IETF RFC 2440 および 3156 で定義されたプロトコル。ほとんどのメールクライアントは、OpenPGP をデフォルトではサポートしていないため、サードパーティ製プラグインをメールクライアントと組み合わせて使用する。OpenPGP では、「web of trust（信頼の網）」モデルを使用して鍵管理を行っており、管理および制御がユーザに委ねられているため、中～大規模の実装には適さない。

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「主幹制御アプリケーション」というべきソフトウェア。コンピュータの電源が入ると最初に読み込まれるプログラムであり、その中核的なコンポーネントであるカーネルはメモリ上に常駐する。オペレーティングシステムにより、当該コンピュータ上で動作するすべてのアプリケーションプログラム（メールサーバなど）に適用される標準が設定される。アプリケーションによるユーザインタフェース操作およびファイル管理操作のほとんどは、オペレーティングシステムと通信することによって行われる。

パッチ（Patch）— プログラムに対する「補修作業」。「修正」とも呼ばれる。特定された問題に対する直接的な解決策としてユーザに提供されるものであり、ソフトウェアメーカーの Web サイトからダウンロードできる場合もある。パッチは、問題に対する最良の解決策であるとは限らず、開発者が次期リリース向けに製品をパッケージ化する際にパッチよりも優れた解決策が提供されることもしばしばある。パッチは、コンパイル済みコード（すなわち、バイナリファイルやオブジェクトモジュール）に対する差し替えまたは挿入の形で作成および配布されるのが一般的である。多くのオペレーティングシステムでは、パッチのインストールを管理および追跡するための特別なプログラムが提供されている。

フィッシング（Phishing）— コンピュータを利用した詐欺手段を通じて個人をだまし、機密情報や個人情報を開示させること。

Post Office Protocol（POP、ポストオフィスプロトコル）— IETF RFC 1939 で定義されるメールボックスアクセスプロトコル。最も一般的に使用されているメールボックスアクセスプロトコルの 1 つである。

Secure Multipurpose Internet Mail Extensions（S/MIME、セキュリティ保護付き MIME）— 公開鍵暗号を使用したメッセージの暗号化および証明書の作成に関する、IETF RFC 3850～3852 および 2634 で定義されたプロトコル。普及している多くのメールクライアントで、デフォルトインストールにおいてサポートされる。S/MIME は、認証局に基づいて鍵管理を行う従来型の階層構造の設計が採用されているため、中～大規模の実装に適する。

Simple Mail Transfer Protocol（SMTP、簡易メール転送プロトコル）— IETF RFC 2821 で定義される MTA プロトコル。最も一般的に使用されている MTA プロトコルである。

スパム（Spam）— 一方的かつ大量に送付される商用目的の電子メールメッセージ。

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

システム管理者（System Administrator）— コンピュータシステム（オペレーティングシステムおよびアプリケーションを含む）を管理する人。ネットワーク管理者と同様の職責を担う。

脆弱性（Vulnerability）— オペレーティングシステム、その他のシステムソフトウェア、またはアプリケーションソフトウェア構成要素に含まれる、セキュリティ上の不備。さまざまな組織が、ソフトウェアのバージョン番号ごとに整理された脆弱性データベースを維持し、一般に公開している。それぞれの脆弱性が悪用された場合には、システムやネットワークが侵害される原因となる可能性がある。

Web サーバ（Web Server）— インターネット上でワールドワイドウェブ（WWW：World Wide Web）サービスを提供するコンピュータ。これには、ハードウェア、オペレーティングシステム、Web サーバソフトウェア、および Web サイトコンテンツ（Web ページ）が含まれる。内部向けにのみ使用され外部に公開されない Web サーバは、「イントラネットサーバ」と呼ばれる。

（本ページは意図的に白紙のままとする）

付録B—電子メール関連の RFC

この付録では、電子メールおよび電子メールのセキュリティに関連する IETF RFC の一覧を示す。最初の一覧では、多数の RFC を RFC の番号順に示す。以降の一覧は、最初の一覧のサブセットであり、IMAP4、POP、SMTP、および MIME などの特定のプロトコルを中心に示す。

電子メール関連の RFC（RFC 番号順）

RFC 番号	RFC カタログ[67]	RFC 名	URL	差し替え／更新
1731	ST	IMAP4 Authentication Mechanisms	http://www.ietf.org/rfc/rfc1731.txt	
1732	IT	IMAP4 Compatibility with IMAP2 and IMAP2BIS	http://www.ietf.org/rfc/rfc1732.txt	
1733	IT	Distributed Electronic Mail Models in IMAP4	http://www.ietf.org/rfc/rfc1733.txt	
1870	STD 10	SMTP Service Extension for Message Size Declaration	http://www.ietf.org/rfc/rfc1870.txt	RFC 1653
1939	STD 53	Post Office Protocol - Version 3	http://www.ietf.org/rfc/rfc1939.txt	RFC 1725
1957	IT	Some Observations on Implementations of the Post Office Protocol (POP3)	http://www.ietf.org/rfc/rfc1957.txt	RFC 1939（更新）
1985	ST	SMTP Service Extension for Remote Message Queue Starting	http://www.ietf.org/rfc/rfc1985.txt	
1991	IT	PGP Message Exchange Formats	http://www.ietf.org/rfc/rfc1991.txt	
2015	ST	MIME Security with Pretty Good Privacy (PGP)	http://www.ietf.org/rfc/rfc2015.txt	
2034	ST	SMTP Service Extension for Returning Enhanced Error Codes	http://www.ietf.org/rfc/rfc2034.txt	
2045	ST	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies	http://www.ietf.org/rfc/rfc2045.txt	RFC 1521, RFC 1522, RFC 1590
2046	ST	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	http://www.ietf.org/rfc/rfc2046.txt	RFC 1521, RFC 1522, RFC 1590
2047	ST	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text	http://www.ietf.org/rfc/rfc2047.txt	RFC 1521, RFC 1522, RFC 1590
2049	ST	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples	http://www.ietf.org/rfc/rfc2049.txt	RFC 1521, RFC 1522, RFC 1590
2061	IT	IMAP4 Compatibility with IMAP2BIS	http://www.ietf.org/rfc/rfc2061.txt	
2062	IT	Internet Message Access Protocol – Obsolete Syntax	http://www.ietf.org/rfc/rfc2062.txt	
2087	ST	IMAP4 QUOTA extension	http://www.ietf.org/rfc/rfc2087.txt	
2088	ST	IMAP4 non-synchronizing literals	http://www.ietf.org/rfc/rfc2088.txt	
2177	ST	IMAP4 IDLE command	http://www.ietf.org/rfc/rfc2177.txt	
2180	IT	IMAP4 Multi-Accessed Mailbox Practice	http://www.ietf.org/rfc/rfc2180.txt	

[67] RFC はそれぞれ次の 4 つの分類のいずれかに属する。BCP(Best Current Practice、現状におけるベストプラクティス)、IT(Informational Track、情報提供トラック)、ST(Standards Track、標準化トラック)、または STD(Standard、標準。標準の番号が続く)

RFC 番号	RFC カタログ[67]	RFC 名	URL	差し替え／更新
2192	ST	IMAP URL Scheme	http://www.ietf.org/rfc/rfc2192.txt	
2193	ST	IMAP4 Mailbox Referrals	http://www.ietf.org/rfc/rfc2193.txt	
2195	ST	IMAP/POP AUTHorize Extension for Simple Challenge/Response	http://www.ietf.org/rfc/rfc2195.txt	RFC 2095
2221	ST	IMAP4 Login Referrals	http://www.ietf.org/rfc/rfc2221.txt	
2268	IT	A Description of the RC2 Encryption Algorithm	http://www.ietf.org/rfc/rfc2268.txt	
2311	IT	S/MIME Version 2 Message Specification	http://www.ietf.org/rfc/rfc2311.txt	
2312	IT	S/MIME Version 2 Certificate Handling	http://www.ietf.org/rfc/rfc2312.txt	
2313	IT	PKCS #1: RSA Encryption Version 1.5	http://www.ietf.org/rfc/rfc2313.txt	
2314	IT	PKCS #10: Certification Request Syntax Version 1.5	http://www.ietf.org/rfc/rfc2314.txt	
2315	IT	PKCS #7: Cryptographic Message Syntax Version 1.5	http://www.ietf.org/rfc/rfc2315.txt	
2342	ST	IMAP4 Namespace	http://www.ietf.org/rfc/rfc2342.txt	
2384	ST	POP URL Scheme	http://www.ietf.org/rfc/rfc2384.txt	
2440	ST	OpenPGP Message Format	http://www.ietf.org/rfc/rfc2440.txt	
2442	IT	The Batch SMTP Media Type	http://www.ietf.org/rfc/rfc2442.txt	
2449	ST	POP3 Extension Mechanism	http://www.ietf.org/rfc/rfc2449.txt	RFC 1939（更新）
2505	BCP	Anti-Spam Recommendations for SMTP MTAs	http://www.ietf.org/rfc/rfc2505.txt	
2554	ST	SMTP Service Extension for Authentication	http://www.ietf.org/rfc/rfc2554.txt	
2595	ST	Using TLS with IMAP, POP3 and ACAP	http://www.ietf.org/rfc/rfc2595.txt	
2630	ST	Cryptographic Message Syntax	http://www.ietf.org/rfc/rfc2630.txt	
2632	ST	S/MIME Version 3 Certificate Handling	http://www.ietf.org/rfc/rfc2632.txt	
2633	ST	S/MIME Version 3 Message Specification	http://www.ietf.org/rfc/rfc2633.txt	
2634	ST	Enhanced Security Services for S/MIME	http://www.ietf.org/rfc/rfc2634.txt	
2645	ST	On-Demand Mail Relay (ODMR) SMTP with Dynamic IP Addresses	http://www.ietf.org/rfc/rfc2645.txt	
2683	IT	IMAP4 Implementation Recommendations	http://www.ietf.org/rfc/rfc2683.txt	
2821	ST	Simple Mail Transfer Protocol	http://www.ietf.org/rfc/rfc2821.txt	RFC 821, RFC 974, RFC 1869, RFC 1123（更新）
2822	ST	Internet Message Format	http://www.ietf.org/rfc/rfc2822.txt	RFC 822
2846	ST	GSTN Address Element Extensions in E-mail Services	http://www.ietf.org/rfc/rfc2846.txt	
2852	ST	Deliver By SMTP Service Extension	http://www.ietf.org/rfc/rfc2852.txt	RFC 1894（更新）
2920	STD 60	SMTP Service Extension for Command Pipelining	http://www.ietf.org/rfc/rfc2920.txt	RFC 2197
2971	ST	IMAP4 ID extension	http://www.ietf.org/rfc/rfc2971.txt	
3030	ST	SMTP Service Extensions for Transmission of Large and Binary MIME Messages	http://www.ietf.org/rfc/rfc3030.txt	RFC 1830
3156	ST	MIME Security with OpenPGP	http://www.ietf.org/rfc/rfc3156.txt	RFC 2015（更新）

RFC 番号	RFC カタログ[67]	RFC 名	URL	差し替え／更新
3191	ST	Minimal GSTN address format in Internet Mail	http://www.ietf.org/rfc/rfc3191.txt	RFC 2303, RFC 2846（更新）
3192	ST	Minimal FAX address format in Internet Mail	http://www.ietf.org/rfc/rfc3192.txt	RFC 2304, RFC 2846（更新）
3206	ST	The SYS and AUTH POP Response Codes	http://www.ietf.org/rfc/rfc3206.txt	
3207	ST	SMTP Service Extension for Secure SMTP over Transport Layer Security	http://www.ietf.org/rfc/rfc3207.txt	RFC 2487
3348	IT	The Internet Message Action Protocol (IMAP4) Child Mailbox Extension	http://www.ietf.org/rfc/rfc3348.txt	
3461	ST	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)	http://www.ietf.org/rfc/rfc3461.txt	RFC 1891
3462	ST	The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages	http://www.ietf.org/rfc/rfc3462.txt	RFC 1892
3463	ST	Enhanced Mail System Status Codes	http://www.ietf.org/rfc/rfc3463.txt	RFC 1893
3464	ST	An Extensible Message Format for Delivery Status Notifications	http://www.ietf.org/rfc/rfc3464.txt	RFC 1894
3501	ST	Internet Message Access Protocol - Version 4rev1	http://www.ietf.org/rfc/rfc3501.txt	RFC 2060
3502	ST	Internet Message Access Protocol (IMAP) – MULTIAPPEND Extension	http://www.ietf.org/rfc/rfc3502.txt	
3503	ST	Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP)	http://www.ietf.org/rfc/rfc3503.txt	
3516	ST	IMAP4 Binary Content Extension	http://www.ietf.org/rfc/rfc3516.txt	
3691	ST	Internet Message Access Protocol (IMAP) UNSELECT command	http://www.ietf.org/rfc/rfc3691.txt	
3798	ST	Message Disposition Notification	http://www.ietf.org/rfc/rfc3798.txt	RFC 2298, RFC 2046（更新）, RFC 3461（更新）
3848	ST	ESMTP and LMTP Transmission Types Registration	http://www.ietf.org/rfc/rfc3848.txt	
3865	ST	A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension	http://www.ietf.org/rfc/rfc3865.txt	
3885	ST	SMTP Service Extension for Message Tracking	http://www.ietf.org/rfc/rfc3885.txt	RFC 3461（更新）
3886	ST	An Extensible Message Format for Message Tracking Responses	http://www.ietf.org/rfc/rfc3886.txt	RFC 3463（更新）
3974	IT	SMTP Operational Experience in Mixed IPv4/v6 Environments	http://www.ietf.org/rfc/rfc3974.txt	
4141	ST	SMTP and MIME Extensions for Content Conversion	http://www.ietf.org/rfc/rfc4141.txt	
4289	BCP	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures	http://www.ietf.org/rfc/rfc4289.txt	RFC 2048
4314	ST	IMAP4 Access Control List (ACL) Extension	http://www.ietf.org/rfc/rfc4314.txt	RFC 2086
4315	ST	Internet Message Access Protocol (IMAP) - UIDPLUS extension	http://www.ietf.org/rfc/rfc4315.txt	RFC 2359

IMAP 関連の RFC（RFC 番号順）

RFC 番号	RFC カタログ	RFC 名	URL	差し替え／更新
1731	ST	IMAP4 Authentication Mechanisms	http://www.ietf.org/rfc/rfc1731.txt	
1732	ST	IMAP4 Compatibility with IMAP2 and IMAP2BIS	http://www.ietf.org/rfc/rfc1732.txt	
1733	IT	Distributed Electronic Mail Models in IMAP4	http://www.ietf.org/rfc/rfc1733.txt	
2061	IT	IMAP4 Compatibility with IMAP2BIS	http://www.ietf.org/rfc/rfc2061.txt	
2062	IT	Internet Message Access Protocol – Obsolete Syntax	http://www.ietf.org/rfc/rfc2062.txt	
2087	ST	IMAP4 QUOTA extension	http://www.ietf.org/rfc/rfc2087.txt	
2088	ST	IMAP4 non-synchronizing literals	http://www.ietf.org/rfc/rfc2088.txt	
2177	ST	IMAP4 IDLE command	http://www.ietf.org/rfc/rfc2177.txt	
2180	IT	IMAP4 Multi-Accessed Mailbox Practice	http://www.ietf.org/rfc/rfc2180.txt	
2192	ST	IMAP URL Scheme	http://www.ietf.org/rfc/rfc2192.txt	
2193	ST	IMAP4 Mailbox Referrals	http://www.ietf.org/rfc/rfc2193.txt	
2195	ST	IMAP/POP AUTHorize Extension for Simple Challenge/Response	http://www.ietf.org/rfc/rfc2195.txt	RFC 2095
2221	ST	IMAP4 Login Referrals	http://www.ietf.org/rfc/rfc2221.txt	
2342	ST	IMAP4 Namespace	http://www.ietf.org/rfc/rfc2342.txt	
2595	ST	Using TLS with IMAP, POP3 and ACAP	http://www.ietf.org/rfc/rfc2595.txt	
2683	IT	IMAP4 Implementation Recommendations	http://www.ietf.org/rfc/rfc2683.txt	
2971	ST	IMAP4 ID extension	http://www.ietf.org/rfc/rfc2971.txt	
3348	IT	The Internet Message Action Protocol (IMAP4) Child Mailbox Extension	http://www.ietf.org/rfc/rfc3348.txt	
3501	ST	Internet Message Access Protocol - Version 4rev1	http://www.ietf.org/rfc/rfc3501.txt	RFC 2060
3502	ST	Internet Message Access Protocol (IMAP) – MULTIAPPEND Extension	http://www.ietf.org/rfc/rfc3502.txt	
3503	ST	Message Disposition Notification (MDN) profile for Internet Message Access Protocol (IMAP)	http://www.ietf.org/rfc/rfc3503.txt	
3516	ST	IMAP4 Binary Content Extension	http://www.ietf.org/rfc/rfc3516.txt	
3691	ST	Internet Message Access Protocol (IMAP) UNSELECT command	http://www.ietf.org/rfc/rfc3691.txt	
4314	ST	IMAP4 Access Control List (ACL) Extension	http://www.ietf.org/rfc/rfc4314.txt	RFC 2086
4315	ST	Internet Message Access Protocol (IMAP) - UIDPLUS extension	http://www.ietf.org/rfc/rfc4315.txt	RFC 2359

MIME および S/MIME の RFC（RFC 番号順）

RFC 番号	RFC カタログ	RFC 名	URL	差し替え／更新
2015	ST	MIME Security with Pretty Good Privacy (PGP)	http://www.ietf.org/rfc/rfc2015.txt	
2045	ST	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet	http://www.ietf.org/rfc/rfc2045.txt	RFC 1521, RFC 1522,

RFC 番号	RFC カタログ	RFC 名	URL	差し替え／更新
		Message Bodies		RFC 1590
2046	ST	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	http://www.ietf.org/rfc/rfc2046.txt	RFC 1521, RFC 1522, RFC 1590
2047	ST	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text	http://www.ietf.org/rfc/rfc2047.txt	RFC 1521, RFC 1522, RFC 1590
2049	ST	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples	http://www.ietf.org/rfc/rfc2049.txt	RFC 1521, RFC 1522, RFC 1590
2268	IT	A Description of the RC2 Encryption Algorithm	http://www.ietf.org/rfc/rfc2268.txt	
2311	IT	S/MIME Version 2 Message Specification	http://www.ietf.org/rfc/rfc2311.txt	
2312	IT	S/MIME Version 2 Certificate Handling	http://www.ietf.org/rfc/rfc2312.txt	
2313	IT	PKCS #1: RSA Encryption Version 1.5	http://www.ietf.org/rfc/rfc2313.txt	
2314	IT	PKCS #10: Certification Request Syntax Version 1.5	http://www.ietf.org/rfc/rfc2314.txt	
2315	IT	PKCS #7: Cryptographic Message Syntax Version 1.5	http://www.ietf.org/rfc/rfc2315.txt	
2630	ST	Cryptographic Message Syntax	http://www.ietf.org/rfc/rfc2630.txt	
2632	ST	S/MIME Version 3 Certificate Handling	http://www.ietf.org/rfc/rfc2632.txt	
2633	ST	S/MIME Version 3 Message Specification	http://www.ietf.org/rfc/rfc2633.txt	
2634	ST	Enhanced Security Services for S/MIME	http://www.ietf.org/rfc/rfc2634.txt	
3156	ST	MIME Security with OpenPGP	http://www.ietf.org/rfc/rfc3156.txt	RFC 2015（更新）
4141	ST	SMTP and MIME Extensions for Content Conversion	http://www.ietf.org/rfc/rfc4141.txt	
4289	BCP	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures	http://www.ietf.org/rfc/rfc4289.txt	RFC 2048

OpenPGP および PGP 関連の RFC（RFC 番号順）

RFC 番号	RFC カタログ	RFC 名	URL	差し替え／更新
1991	IT	PGP Message Exchange Formats	http://www.ietf.org/rfc/rfc1991.txt	
2015	ST	MIME Security with Pretty Good Privacy (PGP)	http://www.ietf.org/rfc/rfc2015.txt	
2440	ST	OpenPGP Message Format	http://www.ietf.org/rfc/rfc2440.txt	
3156	ST	MIME Security with OpenPGP	http://www.ietf.org/rfc/rfc3156.txt	RFC 2015（更新）

POP 関連の RFC（RFC 番号順）

RFC 番号	RFC カタログ	RFC 名	URL	差し替え／更新
1939	STD 53	Post Office Protocol - Version 3	http://www.ietf.org/rfc/rfc1939.txt	RFC 1725
1957	IT	Some Observations on Implementations of the Post Office Protocol (POP3)	http://www.ietf.org/rfc/rfc1957.txt	RFC 1939（更新）
2195	ST	IMAP/POP AUTHorize Extension for Simple Challenge/Response	http://www.ietf.org/rfc/rfc2195.txt	RFC 2095
2384	ST	POP URL Scheme	http://www.ietf.org/rfc/rfc2384.txt	
2449	ST	POP3 Extension Mechanism	http://www.ietf.org/rfc/rfc2449.txt	RFC 1939（更新）
2595	ST	Using TLS with IMAP, POP3 and ACAP	http://www.ietf.org/rfc/rfc2595.txt	
3206	ST	The SYS and AUTH POP Response Codes	http://www.ietf.org/rfc/rfc3206.txt	

SMTP 関連の RFC（RFC 番号順）

RFC 番号	RFC カタログ	RFC 名	URL	差し替え／更新
1870	STD 10	SMTP Service Extension for Message Size Declaration	http://www.ietf.org/rfc/rfc1870.txt	RFC 1653
1985	ST	SMTP Service Extension for Remote Message Queue Starting	http://www.ietf.org/rfc/rfc1985.txt	
2034	ST	SMTP Service Extension for Returning Enhanced Error Codes	http://www.ietf.org/rfc/rfc2034.txt	
2442	IT	The Batch SMTP Media Type	http://www.ietf.org/rfc/rfc2442.txt	
2505	BCP	Anti-Spam Recommendations for SMTP MTAs	http://www.ietf.org/rfc/rfc2505.txt	
2554	ST	SMTP Service Extension for Authentication	http://www.ietf.org/rfc/rfc2554.txt	
2645	ST	On-Demand Mail Relay (ODMR) SMTP with Dynamic IP Addresses	http://www.ietf.org/rfc/rfc2645.txt	
2821	ST	Simple Mail Transfer Protocol	http://www.ietf.org/rfc/rfc2821.txt	RFC 821, RFC 974, RFC 1869, RFC 1123（更新）
2822	ST	Internet Message Format	http://www.ietf.org/rfc/rfc2822.txt	RFC 822

RFC 番号	RFC カタログ	RFC 名	URL	差し替え／更新
2846	ST	GSTN Address Element Extensions in E-mail Services	http://www.ietf.org/rfc/rfc2846.txt	
2852	ST	Deliver By SMTP Service Extension	http://www.ietf.org/rfc/rfc2852.txt	RFC 1894（更新）
2920	STD 60	SMTP Service Extension for Command Pipelining	http://www.ietf.org/rfc/rfc2920.txt	RFC 2197
3030	ST	SMTP Service Extensions for Transmission of Large and Binary MIME Messages	http://www.ietf.org/rfc/rfc3030.txt	RFC 1830
3207	ST	SMTP Service Extension for Secure SMTP over Transport Layer Security	http://www.ietf.org/rfc/rfc3207.txt	RFC 2487
3461	ST	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)	http://www.ietf.org/rfc/rfc3461.txt	RFC 1891
3462	ST	The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages	http://www.ietf.org/rfc/rfc3462.txt	RFC 1892
3463	ST	Enhanced Mail System Status Codes	http://www.ietf.org/rfc/rfc3463.txt	RFC 1893
3464	ST	An Extensible Message Format for Delivery Status Notifications	http://www.ietf.org/rfc/rfc3464.txt	RFC 1894
3798	ST	Message Disposition Notification	http://www.ietf.org/rfc/rfc3798.txt	RFC 2298, RFC 2046（更新）, RFC 3461（更新）
3848	ST	ESMTP and LMTP Transmission Types Registration	http://www.ietf.org/rfc/rfc3848.txt	
3865	ST	A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension	http://www.ietf.org/rfc/rfc3865.txt	
3885	ST	SMTP Service Extension for Message Tracking	http://www.ietf.org/rfc/rfc3885.txt	RFC 3461（更新）
3886	ST	An Extensible Message Format for Message Tracking Responses	http://www.ietf.org/rfc/rfc3886.txt	RFC 3463（更新）
3974	IT	SMTP Operational Experience in Mixed IPv4/v6 Environments	http://www.ietf.org/rfc/rfc3974.txt	
4141	ST	SMTP and MIME Extensions for Content Conversion	http://www.ietf.org/rfc/rfc4141.txt	

（本ページは意図的に白紙のままとする）

付録C—参考文献

[Alle00] Julia Allen, et al., *Securing Network Servers*, CERT, 2000 年, http://www.sei.cmu.edu/pub/documents/sims/pdf/sim010.pdf

[Curt01] Matt Curtin, *Developing Trust: Online Privacy and Security*, 2001 年 11 月

[FTC06a] Federal Trade Commission, *How Not to Get Hooked by a 'Phishing' Scam*, 2006 年 10 月, http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm

[Kent06] Karen Kent and Murugiah Souppaya, NIST Special Publication 800-92, *Guide to Computer Security Log Management*, 2006 年 9 月, http://csrc.nist.gov/publications/nistpubs/

[McKi01] Ashley McKinnon, "Web and Email Filtering", *PC Magazine*, 2001 年 12 月

[Mell05] Peter Mell, et al., NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, 2005 年 11 月, http://csrc.nist.gov/publications/nistpubs/

[NISS99] *National Information System Security Glossary*, NSTISSI No. 4009, 1999 年 1 月

[Pits01] Trent Pitsenbarger, *Email Security in the Wake of Recent Malicious Code Incidents*, 2001 年, http://www.nsa.gov/snac/

[Salt75] Jerome H. Saltzer and Michael Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE*, Volume 63, pages 1278-1308

[Scar07] Karen Scarfone and Peter Mell, NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, 2007 年 2 月, http://csrc.nist.gov/publications/nistpubs/

[Swan06] Marianne Swanson, et al, NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, 2006 年 2 月, http://csrc.nist.gov/publications/nistpubs/

[Wack02a] John Wack, et al., NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, 2002 年 1 月, http://csrc.nist.gov/publications/nistpubs/

[Wack02b] John Wack, et al., NIST Special Publication 800-42, *Guideline on Network Security Testing*, 2002 年 2 月, http://csrc.nist.gov/publications/nistpubs/

（本ページは意図的に白紙のままとする）

付録D—電子メールのセキュリティ関連ツールとアプリケーション

以下の一覧には、役に立つツールとリソースの例を示す[68]。

集中管理されたマルウェアスキャンとコンテンツフィルタリングのアプリケーション

メーカー	ツール	Web サイト	Linux／UNIX	Win32	コスト
Aladdin Knowledge Systems	**eSafe Gateway, eSafe Mail**	http://www.aladdin.com/esafe/email_security.asp		✓	$$$
説明	*Microsoft Exchange、IBM Lotus Domino、およびSMTP ベースのメールサーバをサポート。*				
Barracuda Networks	**Barracuda Spam Firewall**	http://www.barracudanetworks.com/ns/products/spam_overview.php			$$$
説明	*アプライアンスベースのソリューションで、メールサーバとは別に、伝送時の電子メールメッセージを監視。*				
BorderWare Technologies	**MXtreme Mail Firewall**	http://www.borderware.com/products/mxtreme/			$$$
説明	*アプライアンスベースのソリューションで、メールサーバとは別に、伝送時の電子メールメッセージを監視。*				
CipherTrust	**CipherTrust Edge, CipherTrust IronMail**	http://www.ciphertrust.com/products/index.php			$$$
説明	*アプライアンスベースのソリューションで、メールサーバとは別に、伝送時の電子メールメッセージを監視。*				
Clearswift	**MIMEsweeper**	http://www.mimesweeper.com/		✓	$$$
説明	*Microsoft Exchange、IBM Lotus Domino、およびSMTP ベースのメールサーバをサポート。*				
F-Secure	**F-Secure Anti-Virus, F-Secure Internet Gatekeeper, F-Secure Messaging Security Gateway, F-Secure Spam Control,**	http://www.f-secure.com/products/products_a-z.html	✓	✓	$$$
説明	*Microsoft Exchange、SMTP、およびPOP3 をサポート。*				
GFI Software	**GFI MailEssentials, GFI MailSecurity**	http://www.gfi.com/mailsecurity/		✓	$$$
説明	*Microsoft Exchange およびSMTP ベースのメールサーバをサポート。*				
GROUP Technologies	**iQ Suite**	http://www.group-software.com/en/products/iq_suite/iq_suite.php	✓	✓	$$$
説明	*Microsoft Exchange、Microsoft ISA、IBM Lotus Domino、およびMicrosoft SMTP ベースのメールサーバをサポート。*				
IronPort Systems	**IronPort**	http://www.ironport.com/products/			$$$
説明	*アプライアンスベースのソリューションで、メールサーバとは別に、伝送時の電子メールメッセージを監視。*				

[68] この付録に示すアプリケーションは、電子メールのセキュリティを目的として使用するアプリケーションの網羅的な一覧ではない。また、この文書は製品を保証するものでもない。

メーカー	ツール	Web サイト	Linux／UNIX	Win32	コスト
Kaspersky Lab	**Kaspersky Anti-Spam, Kaspersky Anti-Virus, Kaspersky SMTP-Gateway**	http://usa.kaspersky.com/products/corporate-security.php	✓	✓	$$$
説明	*Microsoft Exchange、IBM Lotus Domino、およびSMTP ベースのメールサーバ(Sendmail、qmail、Postfix、CommuniGate Pro、およびExim を含む)をサポート。*				
MailScanner/Julian Field	**MailScanner**	http://www.mailscanner.info/	✓		Free
説明	*通常、SpamAssassin およびClamAV とともに使用。さまざまなSMTP ベースのメールサーバ(Postfix、Exim、およびZMailer を含む)をサポート。*				
Marshal	**MailMarshal**	http://www.marshal.com/pages/products.asp		✓	$$$
説明	*Microsoft Exchange およびSMTP サーバをサポート。*				
McAfee	**McAfee GroupShield, McAfee Secure Messaging, McAfee SpamKiller**	http://www.mcafee.com/us/enterprise/products/anti_virus/email_servers/index.html	✓	✓	$$$
説明	*Microsoft Exchange、IBM Lotus Domino、およびSMTP ベースのメールサーバをサポート。*				
Mirapoint	**RazorGate**	http://www.mirapoint.com/products/			$$$
説明	*アプライアンスベースのソリューションで、メールサーバとは別に、伝送時の電子メールメッセージを監視。*				
Panda Antivirus	**EnterpriSecure**	http://www.pandasoftware.com/home/empresas/default	✓	✓	$$$
説明	*Microsoft Exchange、IBM Lotus Domino、およびSMTP ベースのメールサーバ(Sendmail、Qmail、およびPostfix を含む)をサポート。*				
Proofpoint	**Proofpoint Messaging Security Gateway, Proofpoint Protection Server**	http://www.proofpoint.com/products/index.php	✓		$$$
説明	*SMTP ベースのメールサーバをサポート。*				
Sendmail	**Sendmail Mailstream, Sendmail Sentrion**	http://www.sendmail.com/products/	✓	✓	$$$
説明	*SMTP ベースのメールサーバをサポート。*				
SonicWALL	**SonicWALL Email Security**	http://www.sonicwall.com/us/Email_Security.html		✓	$$$
説明	*Microsoft Exchange およびSMTP ベースのメールサーバを監視。*				
Sophos	**Sophos ES4000 Email Security Appliance, Sophos MailMonitor, Sophos PureMessage**	http://www.sophos.com/products/es/gateway/	✓	✓	$$$
説明	*Microsoft Exchange、IBM Lotus Domino、およびSMTP ベースのメールサーバ(Sendmail、Postfix、Sun Java System Messaging Server、およびSunOne Messaging Server を含む)をサポート。*				
SurfControl	**SurfControl E-mail Filter, SurfControl RiskFilter**	http://www.surfcontrol.com/		✓	$$$

メーカー	ツール	Web サイト	Linux／UNIX	Win32	コスト
説明	*Microsoft Exchange、IBM Lotus Domino、GroupWise、Sendmail、およびそのほかの SMTP ベースのメールサーバをサポート。*				
Symantec	**Symantec AntiVirus, Symantec Mail Security**	http://www.symantec.com/enterprise/products/index.jsp	✓	✓	$$$
説明	*Microsoft Exchange、IBM Lotus Domino、および SMTP ベースのメールサーバをサポート。*				
Trend Micro	**ScanMail**	http://www.trendmicro.com/en/products/email/overview.htm	✓	✓	$$$
説明	*Microsoft Exchange、および IBM Lotus Domino をサポート。*				
Tumbleweed Communications	**MailGate**	http://www.tumbleweed.com/products/mailgate/index.html		✓	$$$
説明	*Microsoft Exchange および SMTP ベースのメールサーバを監視。*				

$$$=対象製品が有料であることを示す。

オープンリレーツール

ツール	機能	Web サイト	Web ベース	コスト
メールリレー確認用ツール				
DNSExit Mail Relay Testing Tool	**メールリレーツール**	https://www.dnsexit.com/Direct.sv?cmd=testMailServer	✓	無料
説明	*指定の SMTP ポート経由でメールサーバに telnet を実行し、そのサーバにメッセージの配信を試みる。メールサーバが正しく設定されているかどうか検出する。*			
Mail Relay Testing Tool	**メールリレーツール**	http://abuse.net/relay.html	✓	無料
説明	*メールリレーを特定する管理者を支援する。*			
Spam Relay Checker	**スパムリレーツール**	http://www.3dmail.com/spam/	✓	無料
説明	*システム管理者が、スパムの生成源を特定するためにスパムソースを追跡するのに役立つ。スパム送信者によって乱用されているサーバの Postmaster への通知を支援する。*			
ブラックリスト[69]				
Composite Blocking List (CBL)	**ブラックリスト**	http://cbl.abuseat.org/	✓	無料
説明	*CBL は、非常に広範なスパムトラップのソースデータに基づき、オープンプロキシテストをまったく行わずに、さまざまな種類のオープンプロキシ（HTTP、SOCKS、AnalogX、WinGate など）に固有の特徴を示す IP の一覧のみを示す。これらのオープンプロキシは、スパム、メールの直接転送を行うワームやウイルス、トロイの木馬または「ステルス」型スパムウェアを送信するために悪用されているものである。*			

[69] ブラックリストリソースの詳細については、http://dmoz.org/Computers/Internet/Abuse/Spam/Blacklists/を参照のこと。

ツール	機能	Web サイト	Web ベース	コスト
Distributed Server Boycott List (DSBL)	**ブラックリスト**	http://dsbl.org/main	✓	無料
説明	*DSBL の一覧には、特別なテストメッセージを listme@listme.dsbl.org にリレーしたサーバの IP アドレスが含まれる。これは、サーバがオープンリレー、オープンプロキシ、または他に、任意の人がそのサーバを経由して任意の宛先に電子メールを配信できるような脆弱性をもつ場合に起こり得る。*			
NJABL.ORG	**ブラックリスト**	http://njabl.org/	✓	無料
説明	*NJABL.ORG には、電子メールへのタグ付けや電子メールの拒否、そして少なくとも一部のスパムを防止できるように、既知の、かつ潜在的なスパムソース（オープンリレー、オープンプロキシ、HTTP メールゲートウェイのためのオープンフォーム、動的 IP プール、およびダイレクトスパマ）の一覧が含まれる。*			
The Spamhaus Block List (SBL)	**ブラックリスト**	http://www.spamhaus.org/sbl/	✓	無料
説明	*SBL は、確認済みスパムソース（スパム業者、スパムギャング、およびスパムサポートサービスを含む）の、IP アドレスのリアルタイムデータベースである。これは、Spamhaus Project チームによって維持されており、電子メールの管理者による受信メールストリームの管理を支援する無料のサービスとして提供されている。*			
MX **レコード参照**				
DNS MX record lookup	**MX レコード参照**	http://airlinknetworks.com/exchange/MXrecordLookup.html	✓	無料
説明	*このツールは、ドメインの MX サーバの参照を可能にする。*			
Domain Mail Server/ Exchanger (MX Records) Lookup	**MX レコード参照**	http://www.hashemian.com/tools/domain-email.php	✓	無料
説明	*このツールは、指定の電子メールアドレスが使用するメールサーバの特定を試みる。これは、電子メールの真正性を確認したり、特定のアドレスの電子メールを処理する主体の確認に役立つ。*			
MX Record Lookup	**MX レコード参照**	http://www.webmaster-toolkit.com/mx-record-lookup.shtml	✓	無料
説明	*MX Record Lookup ツールは、指定の電子メールアドレスが使用するメールサーバの検出を試みる。これは、電子メールの真正性を確認したり、特定のアドレスの電子メールを処理する主体の確認に役立つ。*			

付録E—電子メールセキュリティのオンライン資料

この付録では、メールサーバの管理者その他のユーザにとって、電子メールセキュリティの理解を深め、メールサーバ、クライアント、およびメールシステムの他の構成要素のセキュリティを維持するのに役立つオンライン資料を示す。

セキュリティに関する一般的な資料

資料／資料名	URL
Center for Education and Research in Information Assurance and Security (CERIAS)	http://www.cerias.purdue.edu/
CERT/CC	http://www.cert.org/
Computer Security Resource Center (CSRC)	http://csrc.nist.gov/
National Information Assurance Partnership (NIAP)	http://www.niap.nist.gov/
National Vulnerability Database (NVD)	http://nvd.nist.gov/
Office of Management and Budget Circular No. A-130	http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
Open Source Vulnerability Database (OSVDB)	http://www.osvdb.org/
RISKS Forum	http://catless.ncl.ac.uk/Risks/
Security Configuration Checklists Program for IT Products	http://checklists.nist.gov/
SecurityFocus Vulnerability Database	http://www.securityfocus.com/vulnerabilities
U.S. Computer Emergency Response Team (US-CERT)	http://www.us-cert.gov/
U.S. Department of Energy Computer Incident Advisory Capability (CIAC)	http://www.ciac.org/ciac/

電子メールと電子メールのセキュリティに関する一般的な資料

資料／資料名	URL
Email Issues, SANS Reading Room	http://www.sans.org/rr/whitepapers/email/
Internet Mail Consortium	http://www.imc.org/
Tips and Tricks Guide to Secure Messaging	http://www.microsoft.com/securemessaging/ebook/default.mspx

電子メールの暗号化に関する資料

資料／資料名	URL
Guide to Using S/MIME	http://www.mozilla.org/projects/security/pki/psm/smime_guide.html
IETF OpenPGP Working Group	http://www.ietf.org/html.charters/openpgp-charter.html
IETF S/MIME Working Group	http://www.ietf.org/html.charters/smime-charter.html
OpenPGP Alliance	http://www.openpgp.org/
S/MIME Gateway Certification	http://www.opengroup.org/smg/cert/
Securing Email Through Proxies: Smap and Stunnel	http://www.sans.org/reading_room/whitepapers/email/579.php
Securing POP Mail on Windows Clients	http://sewpsc.sewp.nasa.gov/documents/pop.mail.pdf
Securing POP Mail on Windows Clients	http://csrc.nist.gov/fasp/FASPDocs/SecurPOPwSSH.htm

マルウェアおよびスパイウェアに関する資料

資料／資料名	URL
Anti-Spyware Coalition (ASC)	http://www.antispywarecoalition.org/
Anti-Virus Information Exchange Network (AVIEN)	http://www.avien.org/
Common Malware Enumeration (CME)	http://cme.mitre.org/
Computer Antivirus Research Organization (CARO)	http://www.caro.org/
European Institute for Computer Antivirus Research (EICAR)	http://www.eicar.org/
SecurityFocus Virus	http://www.securityfocus.com/virus/
Spywaredata.com	http://www.spywaredata.com/
Virus Bulletin	http://www.virusbtn.com/
Viruslist.com	http://www.viruslist.com/en/
WildList Organization International	http://www.wildlist.org/

フィッシングに関する資料

資料／資料名	URL
Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
FTC, “How Not to Get Hooked by a ‘Phishing’ Scam”	http://ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
Internet Crime Complaint Center (ICCC)	http://www.ic3.gov/
Phish Report Network	http://www.phishreport.net/

スパムに関する資料

資料／資料名	URL
Coalition Against Unsolicited Commercial Email (CAUCE)	http://www.cauce.org/
Distributed Server Blackhole List (DSBL)	http://www.dsbl.org/
Federal Trade Commission (FTC) Spam Home Page	http://www.ftc.gov/spam/
GetNetWise	http://spam/getnetwise.org/
Messaging Anti-Abuse Working Group	http://www.maawg.org/
Not Just Another Bogus List	http://njabl.org/
OnGuard Online	http://onguardonline.gov/index.html
Open Relay Database	http://www.ordb.org/
Spam.abuse.net	http://spam.abuse.net/
Spamhaus	http://www.spamhaus.org/
Spam Prevention Early Warning System (SPEWS)	http://www.spews.org/
SPAM-L Mailing List Frequently Asked Questions (FAQ)	http://www.claws-and-paws.com/spam-l

メールサーバのセキュリティパッチに関する資料

サーバ／メーカー	URL
602LAN Suite (Software602)	http://www.software602.com/products/ls/
ArGoSoft Mail Server (ArGoSoft)	http://www.argosoft.com/rootpages/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/patch-upgrades.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/technet/prodtechnol/exchange/downloads/2003/default.mspx
Postfix (Wietse Venema)	http://www.postfix.org/download.html
Sendmail (commercial version) (Sendmail, Inc.)	http://www.sendmail.com/support/
sendmail (freeware version) (Sendmail Consortium)	http://www.sendmail.org/
Xmail (Davide Libenzi)	http://www.xmailserver.org/

メールクライアントのセキュリティパッチに関する資料

クライアント／製造者	URL
Balsa (GNOME Project)	http://balsa.gnome.org/download.html
Barca (Poco Systems)	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	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	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

クライアント／製造者	URL
Mozilla	http://www.mozilla.org/security/
Mutt	http://www.mutt.org/download.html
Nisus Email (Nisus Software)	http://www.nisus.com/NisusEmail/FAQ.php?PHPSESSID=0ba9f9639672d1fdf836a97f3ad29383#HowUpgradeOS9
Outlook (Microsoft Corporation)	http://office.microsoft.com/en-us/officeupdate/default.aspx
Outlook Express (Microsoft Corporation)	http://www.microsoft.com/downloads/search.aspx?displaylang=en&categoryid=7
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	http://sylpheed.good-day.net/en/
Thunderbird (Mozilla)	http://www.mozilla.com/thunderbird/
VM	http://www.wonderworks.com/vm/download.html

システムおよびネットワークセキュリティに関する NIST の刊行物[70]

刊行物	URL
SP 800-18 Revision 1, *Guide to Developing Security Plans for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf
SP 800-27, *Engineering Principles for Information Technology Security*	http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf
SP 800-28, *Guidelines on Active Content and Mobile Code*	http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf
SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*	http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
SP 800-34, *Contingency Planning Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
SP 800-37, *Federal Guidelines for the Security Certification and Accreditation of Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
SP 800-41, *Guide to Firewall Selection and Policy Recommendations*	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
SP 800-42, *Guideline on Network Security Testing*	http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf
SP 800-43, *Guide to Securing Windows 2000 Professional*	http://csrc.nist.gov/itsec/guidance_W2Kpro.html
SP 800-44, *Guidelines on Securing Public Web Servers*	http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf
SP 800-46, *Security for Telecommuting and Broadband Communications*	http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf
SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security Implementations*	http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf

[70] これらすべての刊行物を入手できる主たる Web サイトは、http://csrc.nist.gov/publications/index.html である。

刊行物	URL
SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf
SP 800-61, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
SP 800-63, *Electronic Authentication Guideline*	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*	http://csrc.nist.gov/itsec/download_WinXP.html
SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*	http://csrc.nist.gov/itsec/guidance_WinXP_Home.html
SP 800-83, *Guide to Malware Incident Prevention and Handling*	http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf
SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
SP 800-92, *Guide to Computer Security Log Management*	http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*	http://csrc.nist.gov/publications/nistpubs/

（本ページは意図的に白紙のままとする）

付録F—電子メールセキュリティのチェックリスト

メールサーバの計画とマネジメント

完了	アクション
	メールサーバのインストールおよび導入に関する計画
☐	メールサーバの機能を明らかにする
☐	メールサーバが保存、処理、伝送する情報のカテゴリを明らかにする
☐	情報のセキュリティ要件を明らかにする
☐	メールサービスの継続性の要件を明らかにする
☐	メールサーバを稼働させる専用ホストを特定する
☐	メールサーバが提供またはサポートするネットワークサービスを特定する
☐	メールサーバを使用するユーザおよびユーザのカテゴリを明らかにし、ユーザのカテゴリごとに付与する権限を決定する
☐	メールサーバの管理方法を決定する（ローカル管理、リモート管理など）
☐	メールサーバにおけるユーザ認証方式を決定する
☐	電子メールアドレス関連情報のセキュリティまたはプライバシ要件を明らかにする
	メールサーバの稼働に適したオペレーティングシステムの選定
☐	脆弱性が存在する可能性が最小限であること
☐	管理者レベルまたは root レベルの作業を権限を有するユーザのみに限定できること
☐	利用を意図した情報以外のサーバ上の情報へのアクセスを拒否できること
☐	オペレーティングシステムまたはサーバソフトウェアに組み込まれている可能性のあるネットワークサービスのうち不要なものを無効にできること
☐	侵入およびその試みを検出するために適切なサーバ動作のログを記録できること
☐	サーバおよびサーバ製品を管理する技能と経験を持ったスタッフの調達可能性
	メールサーバの設置場所の計画
☐	適切な物理的セキュリティ保護メカニズム
☐	温度や湿度の必要条件を維持する適切な環境調整機能
☐	予備電源
☐	既知の自然災害に対する備え

メールサーバのオペレーティングシステムのセキュリティ保護

完了	アクション
	オペレーティングシステムへのパッチの適用と更新
☐	パッチ適用プロセスの策定・導入
☐	オペレーティングシステムに必要な全てのパッチおよび更新プログラムの特定、テスト、インストール
	不要なサービスおよびアプリケーションの削除または無効化
☐	不要なサービスおよびアプリケーションの削除または無効化
☐	Web サーバ、ディレクトリサーバ、そのほかのサーバに別々のホストを使用する
	オペレーティングシステムのユーザ認証の設定
☐	不要なデフォルトのアカウントおよびグループの削除または無効化
☐	インタラクティブでないアカウントの無効化
☐	対象コンピュータにおいてユーザグループを作成する
☐	対象コンピュータにおいてユーザアカウントを作成する
☐	組織のパスワードポリシーを確認し、適切な（長さ、複雑さなど）アカウントパスワードを設定する
☐	パスワードを推測されないようにコンピュータを設定する
☐	その他のセキュリティメカニズムのインストール・設定により、認証を強化する
	リソース制御の適切な設定
☐	ファイル、ディレクトリ、装置、そのほかのリソースのアクセス制御を設定する
☐	ほとんどのシステム関連ツールの利用権限を権限を有するシステム管理者にのみ限定する
	追加的なセキュリティ管理策のインストールおよび設定
☐	オペレーティングシステムが備えていない必要な管理策を提供するために、追加ソフトウェアの選定・インストール・設定を行う
	オペレーティングシステムを対象としたセキュリティテストの実施
☐	初期インストール後のオペレーティングシステムを対象にテストを行い、脆弱性を検出する
☐	オペレーティングシステムを対象に定期的にテストを行い、脆弱性を検出する

メールサーバおよび内容のセキュリティ保護

完了	アクション
	メールサーバアプリケーションのセキュリティ強化
☐	メールサーバソフトウェアは、専用のホストにインストールする（Web ベースのメールアクセスを使用する場合、メールサーバソフトウェアを Web サーバとは別のホストにインストールする）
☐	既知の脆弱性を修正するパッチまたは更新プログラムをすべて適用する
☐	メールボックス専用の（オペレーティングシステムやメールサーバアプリケーションとは分離した）物理ディスクまたは論理パーティションを作成するか、メールボックスを別の

完了	アクション
	サーバでホストする
☐	メールサーバアプリケーションによってインストールされたサービスのうち不要なもの（Web ベースのメール、FTP、リモート管理など）をすべて削除または無効化する
☐	メールサーバのインストール時に作成された不要なデフォルトのログインアカウントをすべて削除または無効化する
☐	メーカーの文書をサーバからすべて削除する
☐	サンプルおよびテスト用ファイルをサーバからすべて削除する
☐	適切なセキュリティテンプレートまたはセキュリティ強化スクリプトをサーバに適用する
☐	SMTP、POP、IMAP サービスのバナー（必要に応じて別の箇所も）の設定を変更し、メールサーバやオペレーティングシステムの種類とバージョンを表示しないようにする
☐	危険性のあるメールコマンドや不要なメールコマンドを無効化する（VRFY、EXPN など）
	オペレーティングシステムおよびメールサーバのアクセス制御の設定
☐	メールサーバアプリケーションからアクセスできる範囲をコンピュータリソースのサブセットに限定する
☐	より詳細なレベルのアクセス制御が必要な場合は、メールサーバによって適用される追加的なアクセス制御を使用してユーザのアクセスを限定する
☐	メールサーバアプリケーションを、厳しいアクセス制限が課せられた固有のユーザ ID およびグループ ID のもとにおいてのみ実行されるように設定する
☐	メールサーバが root または System／Administrator 権限で動作しないことを確認する
☐	ホストオペレーティングシステムを、メールサーバからログファイルへの書き込みのみ許可し、読み取りは禁止するように設定する
☐	メールサーバアプリケーションによって作成される一時ファイルが、適切に保護された特定のサブディレクトリに配置されるようにホストオペレーティングシステムを設定する
☐	メールサーバアプリケーションによって作成される一時ファイルへのアクセスを、当該ファイルを作成したメールサーバプロセスに限り許可するようにホストオペレーティングシステムを設定する
☐	メールサーバに対して専用に割り当てられている指定のファイル階層構造の外に、メールサーバがファイルを保存することができないようにする
☐	Linux および Unix のホストの場合は、メールサーバが chroot jail 内で稼働するように設定する
☐	ユーザのメールボックスを、オペレーティングシステムやメールサーバアプリケーションとは別のサーバ（推奨）、別のハードディスク、または別の論理パーティションにインストールする
☐	ハードディスクまたはパーティションの空き領域を全て使い切ることがないように、メールサーバアプリケーションを設定する
☐	添付ファイルの許容サイズを制限する
☐	ログファイルの格納場所に十分なサイズを確保する
	マルウェアからの電子メールの保護
☐	許可する添付ファイルの種類を決定する
☐	添付ファイルとして許容する最大ファイルサイズの制限を検討する
☐	組織内のコンピュータから個人メールアカウントへのアクセスを許可することが適切かどうかを判断する
☐	電子メールメッセージ内での使用を許可するアクティブコンテンツの種類を決定する

完了	アクション
☐	集中管理されたマルウェアスキャンを実装する（ファイアウォール、メールリレー、メールゲートウェイ、メールサーバのうち 1 つまたは複数に）
☐	すべてのクライアントホストにマルウェアスキャナをインストールする
☐	集中管理されたコンテンツフィルタリングを実装する
☐	疑わしいメッセージ（フィッシング、スパムなど）をブロックまたはタグ付けするようにコンテンツフィルタリングを設定する
☐	疑わしいアクティブコンテンツをメッセージから除去するようにコンテンツフィルタリングを設定する
☐	必要な場合、字句解析を設定する
☐	アドレスのなりすましを防ぐ各種手順を実行する（送信元アドレスに内部アドレスを装った外部からの受信メールをブロックするなど）
☐	コンテンツフィルタリングに関する記述を盛り込んだセキュリティポリシーを策定する
☐	法務、プライバシ、人材に関して権限を持つ適切な部門にセキュリティポリシーをレビューさせる
☐	必要な場合、電子メールに法的免責事項の表示を付加する
☐	マルウェアの危険性およびそれを最小化する方法についてユーザを教育する
☐	マルウェアの大発生時にユーザに通知する
	スパム送信元サーバのブロック
☐	電子メール受信者が実在することを LDAP 参照で確認するようメールゲートウェイまたはファイアウォールを設定する
☐	必要な場合、オープンリレーブラックリストまたは DNS ブラックリストに基づいて電子メールをブロックするようメールサーバを設定する
☐	必要な場合、特定ドメインからの電子メールをブロックするようメールサーバを設定する
	認証付きメールリレーの使用
☐	サーバで認証付きメールリレーを使用するように設定する
	メールサーバへのアクセスのセキュリティ保護
☐	暗号化認証を使用するようメールサーバを設定する
	電子メールへの Web アクセスの有効化
☐	メールへの Web アクセスが必要と考えられる場合に限り、SSL／TLS 経由の Web アクセスのみを可能とするように、メールサーバを設定する

安全なネットワーク基盤の実装

完了	アクション
	ネットワーク上の設置場所
☐	メールサーバがメールゲートウェイやファイアウォールによって保護されている内部ネットワークに配置されているか、 または、DMZ 内に配置されているか
	ファイアウォールの設定
☐	メールサーバがファイアウォールによって保護されている

完了	アクション
☐	メールサーバに対する脅威が大きい場合や、メールサーバが非常に脆弱である場合は、これがアプリケーション層ファイアウォールによって保護されている
☐	ファイアウォールによって、インターネットとメールサーバの間のあらゆるトラフィックが制御されている
☐	ファイアウォールによって、メールサーバへの受信トラフィックが、必要なポート以外すべてブロックされている。必要なポートとは、TCP ポート 25（SMTP）、110（POP3）、143（IMAP）、398（LDAP）、636（Secure LDAP）、993（Secure IMAP）、995（Secure POP）などである
☐	組織のネットワークへの攻撃に使用されていると IDS または IPS によって報告されている IP アドレスまたはサブネットが、ファイアウォールによってブロックされている（侵入検知または侵入防止システムとの組み合わせ）
☐	ファイアウォールによって、信頼のおける外部のセキュリティ対応センターにおいてブラックリスト登録された既知のネットワークまたはサブネットがブロックされている
☐	ファイアウォールによって、疑わしい挙動はネットワークまたはメールサーバの管理者に適切な手段により通知される
☐	ファイアウォールによって、コンテンツフィルタリングおよびマルウェアスキャン機能が提供されている
☐	ファイアウォールが、DoS 攻撃を防ぐように設定されている
☐	ファイアウォールによって、重要なイベントのログが記録される
☐	ファイアウォールおよびそのオペレーティングシステムに、最新または最高セキュリティレベルのパッチが適用されている
	侵入検知および侵入防止システム
☐	IDPS が、メールサーバに出入りするネットワークトラフィックを監視するように設定されている
☐	IDPS が、メールサーバ上の重要なファイルに対する変更を監視するように設定されている（ホストベース IDPS またはファイルの完全性チェッカ）
☐	IDPS が、メールサーバホストにおいて利用できるシステムリソースを監視するように設定されている（ホストベース IDPS）
☐	IDPS によって、組織のネットワークへの攻撃に使用されている IP アドレスまたはサブネットがブロックされる（ファイアウォールと組み合わせ）
☐	攻撃が疑われる場合には、組織のインシデント対応ポリシーおよび手続きに従い、IDPS によって、必要な連絡先に適切な手段でその旨が通知される
☐	IDPS が、フォールスポジティブの発生を許容レベルに抑えつつ最大限の検知を行うよう設定されている
☐	IDPS が、イベントをログに記録し、ネットワークイベントのパケットヘッダ情報を捕捉するように設定されている
☐	新しい攻撃シグネチャの更新を頻繁に適用する（毎日～毎週など。更新のテスト後に適用されるようにするのが一般的）
	ネットワークスイッチ
☐	ネットワークの傍受を防ぐために、ネットワークスイッチが使用されている
☐	ネットワークスイッチが、ARP 偽装攻撃や ARP ポイズニング攻撃を防ぐ高セキュリティモードに設定されている
☐	ネットワークスイッチが、ネットワークセグメント上の全てのトラフィックをネットワークベースの IDPS に送信するよう設定されている

メールクライアントのセキュリティ保護

完了	アクション
	メールクライアントへのパッチの適用と更新
☐	メールクライアントを、最新または最も安全なバージョンに更新する
☐	メールクライアントに、必要なすべてのパッチを適用する（組織のポリシーおよび設定管理に合わせて）
☐	Web ブラウザに、必要なすべてのパッチを適用する（ブラウザと統合されたメールクライアントの場合）
	メールクライアントのセキュリティ機能の設定
☐	メッセージの自動プレビューを無効にする
☐	メッセージの自動表示を無効にする
☐	メッセージに含まれる画像の自動読み込みを無効にする
☐	アクティブコンテンツのダウンロードおよび処理を無効にする（適切な場合）
☐	スパム対策およびフィッシング対策機能を有効にする
☐	携帯用メールクライアント（携帯電話、PDA 用）の設定を変更してセキュリティを向上する
☐	組織のセキュリティポリシーによって携帯用メールクライアントが保護されるようにする（ウイルス対策ソフトウェアのインストールおよび有効化を義務付けるなど）
☐	携帯機器に実装された VPN クライアントまたはそのほかのリモートアクセスアプリケーションへのアクセスを限定するか、不要なクライアント／アプリケーションを削除する
	認証およびアクセスの設定
☐	セキュリティ保護された認証およびアクセスを有効にする
☐	メールクライアントのユーザ名およびパスワードを保存する機能を無効にする
☐	SMTP、POP、IMAP 通信について暗号化（TLS）を使用するようクライアントを設定する
☐	電子メールアドレスの命名規則に制約を設ける（ユーザアカウント名と関連性のないアドレスにさせるなど）
	メールクライアントホストのオペレーティングシステムのセキュリティ保護
☐	最も安全なパッチレベルとなるように、OS を最新の状態に維持する
☐	ローカルに保管されたメッセージおよびクライアント設定ファイルに対しては、適切なユーザのみのアクセスを許可するよう OS を設定する
☐	Windows Script Host を安全に設定するかまたは削除する（Windows ホストのみ）
☐	Windows Script Host に関連するファイル拡張子のデフォルトのアクションを実行から編集に変更する（Windows ホストのみ）
☐	拡張子が完全に表示されるよう OS を設定する（Windows ホストのみ）
☐	ウイルス対策ソフトウェアをインストールし、受信メッセージおよび添付ファイルをスキャンするように設定する。ウイルス対策ソフトウェアが堅牢なスパイウェア対策機能を備えていない場合は、スパイウェア対策アプリケーションもインストールする
☐	必要な場合、不正な通信からコンピュータを保護するためにパーソナルファイアウォールをインストールする
☐	悪意のあるコードは、起動時のセキュリティコンテキスト（当該ユーザのアクセスレベル）で動作するため、OS によって最小特権の考え方が確実に適用されるようにする

完了	アクション
☐	オペレーティングシステムの重要コンポーネントを、悪意のあるコードから確実に保護する
☐	ファイル暗号化アプリケーションを使用して、ローカル環境にあるユーザのハードディスクに保存されている電子メールを保護する（携帯機器について特に重要）
☐	コンピュータが使用されず一定時間が経過した場合に現在のセッションが自動ロックされるよう OS を設定する
	メッセージの安全な作成
☐	電子メールのメッセージ内容に対するセキュリティを提供する（S/MIME、OpenPGP など）
	プラグインの使用
☐	信頼のおける提供元から入手した、絶対に必要なプラグインのみ有効化およびインストールする
	Web ベースのメールシステムへのアクセス
☐	Web ベースメールアクセスでは、128 ビット SSL／TLS 接続のみ使用するよう設定する
☐	Web ベースメールへのアクセスを認める前に、ユーザのとるべき行動を認識させる

メールサーバの管理

完了	アクション
	ログ
☐	IP スタックの設定エラーを記録する
☐	リゾルバ（DNS、NIS など）の設定に関する問題を記録する
☐	メールサーバの設定に関する問題（DNS との不整合、ローカル設定エラー、古いエイリアスデータベースなど）を記録する
☐	システムリソース（ディスク容量、メモリ、CPU）の不足を記録する
☐	エイリアスデータベースの再構築を記録する
☐	ログインを記録する（失敗のみ。容量に十分余裕がある場合は成功も）
☐	セキュリティに関する問題（スパムなど）を記録する
☐	失敗した通信（ネットワークの問題）を記録する
☐	プロトコル障害を記録する
☐	接続タイムアウトを記録する
☐	接続拒否を記録する
☐	VRFY および EXPN コマンドの使用を記録する
☐	代理送信（Send on behalf of）を記録する
☐	代理送信（Send as）を記録する
☐	無効なアドレス形式を記録する
☐	メッセージコレクションの統計を記録する
☐	エラーメッセージの生成を記録する
☐	配信の失敗（固定的エラー）を記録する
☐	メッセージの遅延（一時的エラー）を記録する
☐	別個のログサーバにログを保存する

完了	アクション
☐	組織の要件に従ってログをバックアップおよびアーカイブする
☐	ログのレビューを毎日行う
☐	ログのレビューを毎週行う（長期的な動向を把握するため）
☐	ログファイル自動分析ツールを使用する
	メールサーバのバックアップ
☐	メールサーバのバックアップポリシーを策定する
☐	メールサーバの差分または増分バックアップを、1 日単位から週単位で作成する
☐	メールサーバの完全バックアップを、週単位から月単位で作成する
☐	バックアップを定期的にアーカイブする
	侵害からの復旧
☐	インシデントを組織のコンピュータインシデント対応チームに報告する
☐	侵害されたシステムを隔離するか、そのほかの手順によって攻撃を封じ込め、証拠を収集できるようにする
☐	必要に応じてマネジメント、弁護士、法執行当局などにただちに相談する
☐	類似のホストを調査し、攻撃者が同様に別のシステムも侵害していないか確認する
☐	侵入について分析する
☐	システムを復旧する
☐	システムをテストし、セキュリティが確保されていることを確認する
☐	システムをネットワークに再接続する
☐	システムとネットワークを監視し、攻撃者が再びシステムやネットワークにアクセスしようとしている兆候に注意する
☐	得られた教訓を文書化する
	セキュリティテスト
☐	メールサーバとそれを支えるネットワークを対象に脆弱性スキャンを定期的に実施する
☐	テストの前に脆弱性スキャナを更新する
☐	脆弱性スキャナにより特定された欠陥を是正する
☐	メールサーバとそれを支えるネットワーク基盤を対象にペネトレーションテストを実施する
☐	ペネトレーションテストにより特定された欠陥を是正する
	リモート管理
☐	強力な認証メカニズムを使用する（公開／秘密鍵ペア、2 要素による認証など）
☐	リモート管理に使用可能なホストを、IP アドレスまた許可を与えたユーザに基づいて限定する
☐	暗号化によりパスワードとデータの両方が保護されるセキュリティプロトコルを使用する（SSH、HTTPS など）
☐	最小特権の考え方をリモート管理に適用する（たとえば、リモート管理用のアカウントには最小限のアクセス権のみ付与する）
☐	リモート管理用のユーティリティまたはアプリケーションに設定されているデフォルトのアカウントやパスワードをすべて変更する
☐	インターネットを経由したファイアウォール越しのリモート管理は、VPN などのメカニズムを使用しない限り許可しない
☐	内部ネットワーク上のファイル共有をメールサーバからマウントしない。また、メールサーバ上のファイル共有を内部ネットワークからマウントしない。

付録G—略語一覧

3DES	Triple Data Encryption Standard（トリプルデータ暗号化標準）
ACL	Access Control List（アクセス制御リスト）
AES	Advanced Encryption Standard（次世代標準暗号化方式）
API	Application Programming Interface （アプリケーションプログラミングインタフェース）
ARP	Address Resolution Protocol（アドレス解決プロトコル）
ARPA	Advanced Research Project Agency（米国防総省高等研究計画局）
ASCII	American Standard Code of Information Interchange （情報交換用米国標準コード）
BCP	Best Current Practice（現状におけるベストプラクティス）
CA	Certificate Authority（認証局）
CIO	Chief Information Officer（最高情報責任者）
CMVP	Cryptographic Module Validation Program （暗号化モジュール有効性確認プログラム）
CPU	Central Processing Unit（中央処理装置）
CRAM	Challenge-Response Authentication Mechanism （チャレンジ／レスポンス認証メカニズム）
CSE	Communications Security Establishment（通信安全保障局）
DDoS	Distributed Denial of Service（分散型サービス運用妨害）
DMZ	Demilitarized Zone（非武装地帯）
DNS	Domain Name System（ドメインネームシステム）
DNSBL	Domain Name System Blacklist（ドメインネームシステムブラックリスト）
DoD	Department of Defense（米国国防総省）
DoS	Denial of Service（サービス運用妨害）
DSA	Digital Signature Algorithm（ディジタル署名アルゴリズム）
DSN	Delivery Status Notification（配信ステータス通知）
DSS	Digital Signature Standard（ディジタル署名標準）
ESMTP	Extended Simple Mail Transfer Protocol（拡張 SMTP）
FIPS	Federal Information Processing Standards（連邦情報処理規格）
FISMA	Federal Information Security Management Act （連邦情報セキュリティマネジメント法）
FTP	File Transfer Protocol（ファイル転送プロトコル）
HTML	Hypertext Markup Language（ハイパーテキストマークアップ言語）
HTTP	Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）
HTTPS	Hypertext Transfer Protocol Secure （セキュアなハイパーテキスト転送プロトコル）
IBE	Identity-Based Encryption（ID ベース暗号化）
IDPS	Intrusion Detection and Prevention System （侵入検知および侵入防止システム）

IDS	Intrusion Detection System（侵入検知システム）
IETF	Internet Engineering Task Force（インターネット技術特別調査委員会）
IMAP	Internet Message Access Protocol （インターネットメッセージアクセスプロトコル）
IP	Internet Protocol（インターネットプロトコル）
IPS	Intrusion Prevention System（侵入防止システム）
IPsec	Internet Protocol Security（インターネットプロトコルセキュリティ）
ISP	Internet Service Provider（インターネットサービスプロバイダ）
ISSO	Information Systems Security Officer（情報システムセキュリティ責任者）
ISSPM	Information Systems Security Program Manager （情報システムセキュリティプログラムマネージャ）
IT	Information Technology（情報技術）
ITL	Information Technology Laboratory（情報技術ラボラトリ）
LDA	Local Delivery Agent（ローカル配信エージェント）
LDAP	Lightweight Directory Access Protocol（軽量ディレクトリアクセスプロトコル）
MD5	Message Digest 5（メッセージダイジェスト 5）
MIME	Multipurpose Internet Mail Extensions（多目的インターネットメール拡張）
MOSS	MIME Object Security Services（MIME オブジェクトセキュリティサービス）
MTA	Mail Transfer Agent（メール転送エージェント）
MUA	Mail User Agent（メールユーザエージェント）
NARA	National Archives and Records Administration（米国国立公文書館）
NetBIOS	Network Basic Input/Output System（ネットワーク基本入出力システム）
NFS	Network File System（ネットワークファイルシステム）
NIS	Network Information System（ネットワーク情報システム）
NIST	National Institute of Standards and Technology（米国国立標準技術研究所）
NVD	National Vulnerability Database（脆弱性データベース）
OMB	Office of Management and Budget（行政管理予算局）
OpenPGP	Open Pretty Good Privacy（オープン PGP）
ORB	Open Relay Blacklist（オープンリレーブラックリスト）
OS	Operating System（オペレーティングシステム）
PC	Personal Computer（パーソナルコンピュータ）
PDA	Personal Digital Assistant（携帯情報端末）
PEM	Privacy Enhanced Mail（プライバシ強化メール）
PGP	Pretty Good Privacy（プリティグッドプライバシ）
PIN	Personal Identification Number（個人識別番号）
PKCS	Public Key Cryptography Standard（公開鍵暗号標準）
PKI	Public Key Infrastructure（公開鍵基盤）
POP	Post Office Protocol（ポストオフィスプロトコル）
RAID	Redundant Array of Inexpensive Disks （安価なディスクによる冗長ディスクアレイ）
RFC	Request for Comments（インターネット技術に関する IETF 発行文書）
SAISO	Senior Agency Information Security Officer

	（政府機関の上級情報セキュリティ責任者）
SHA-1	Secure Hash Algorithm-1（安全なハッシュアルゴリズム—1）
SHS	Secure Hash Standard（安全なハッシュ標準）
SIEM	Security Information and Event Management （セキュリティ情報およびイベント管理）
S/MIME	Secure Multipurpose Internet Mail Extensions（セキュリティ保護付き MIME）
SMTP	Simple Mail Transfer Protocol（簡易メール転送プロトコル）
SNMP	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SOHO	Small Office Home Office（スモールオフィス／ホームオフィス）
SP	Special Publication（特別刊行物）
SSH	Secure Shell（セキュアシェル）
SSL	Secure Sockets Layer（セキュアソケットレイヤ）
TCP	Transmission Control Protocol（伝送制御プロトコル）
TCP/IP	Transmission Control Protocol/Internet Protocol （伝送制御プロトコル／インターネットプロトコル）
TLS	Transport Layer Security（トランスポート層セキュリティ）
UCE	Unsolicited Commercial Email（一方的に送付される商用目的の電子メール）
UDP	User Datagram Protocol（ユーザデータグラムプロトコル）
U.S.	United States（合衆国）
VBScript	Visual Basic Script（Visual Basic スクリプト）
VLAN	Virtual Local Area Network（仮想ローカルエリアネットワーク）
VPN	Virtual Private Network（仮想プライベートネットワーク）
WSH	Windows Scripting Host（Windows スクリプティングホスト）
WWW	World Wide Web（ワールドワイドウェブ）