セキュリティゼミナール

山口 英（奈良先端科学技術大学院大学）
佐野 晋（日本電気（株））
白橋 明弘（ネットワンシステムズ（株））
歌代 和正（(株）インターネットイニシアティブ）

1998 年 12 月 16 日

Internet Week 98　国立京都国際会館

（社）日本ネットワークインフォメーションセンター編

目次

1　概要

インターネッサーバト環境での不正アクセスは、日々増加しています。このような不正アクセスは、次のような方法で防止できます。

- セキュリティポリシーを策定して、一貫性のある対策を施す
- あらかじめ不正アクセスについての情報を入手し、適切な対策を施す

また、不正アクセスを防止するために有効なファイアウォール製品が多数商品化され利用できるようになっています。ただし、このような商用ファイアウォールを利用するときにも、提供されている機能と限界を理解する必要があります。

2　目的

現在、インターネットは日々進歩していますが問題も多発していますユーザ。また、インターネットでのセキュリティ管理技術も、日々進歩していますが、対するクラッキング技術も同じように進歩しています。さらに、行政によって不正アクセス法制などが検討され、社会的にもインターネット利用に対する法規制が整備されようとしています。

そして、このようなインターネット利用環境では、他のサービスとは異なり、サービスを受けるユーザ側でも、システムがクラックされたり不正アクセスされないためにセキュリティ技術を学ぶ必要があります。ここでは、第1部「インターネットにおける不正アクセスとその対策」で不正アクセスの現状とオペレーションのためのセキュリティポリシーを、第2部「不正アクセス対策とセキュリティツール」で不正アクセスに対する対策技術を、第3部「ファイアウォール構築技術」でファイアウォールの具体的な構築技術をそれぞれ説明します。

第 1 部 インターネットにおける不正アクセスとその対策（佐野 晋）

3　現状

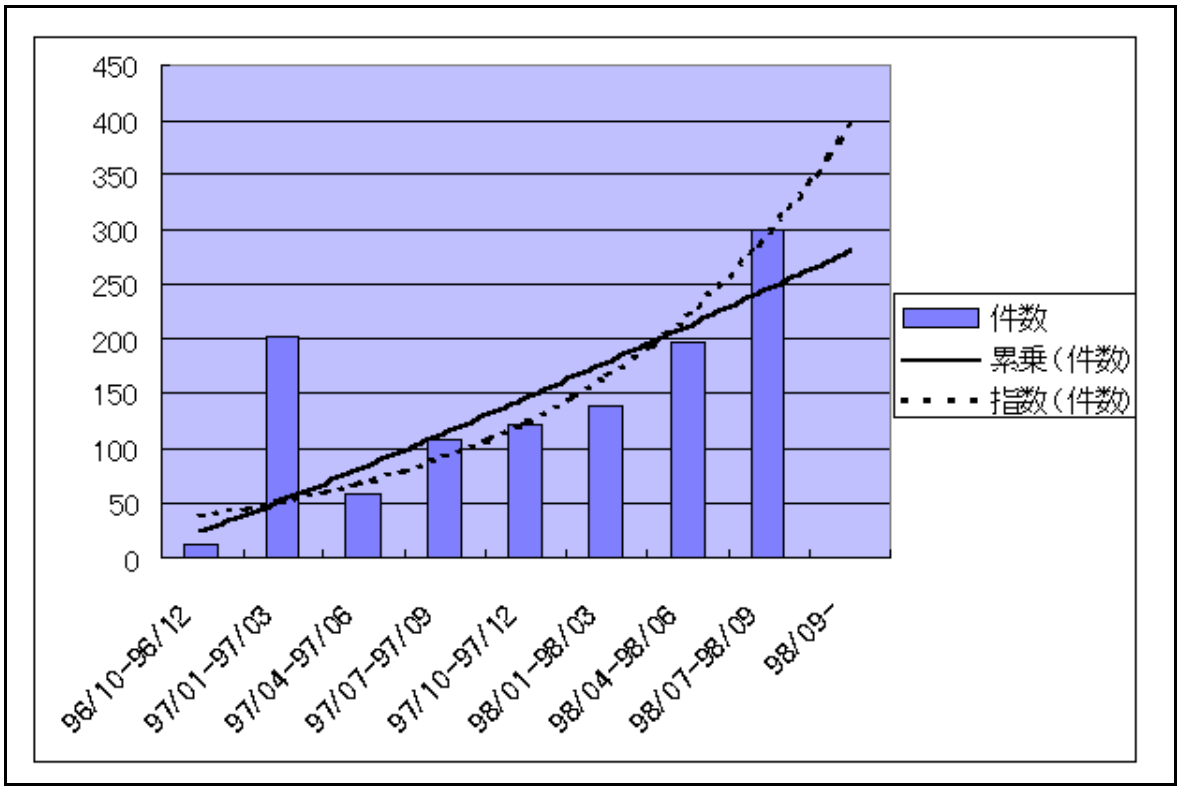
不正アクセスは日々増加しています。たとえば、1998 年 7 月 1 日から 9 月 30 日までに不正アクセスとして報告された件数は 299 件で、関連するサイトは 3,266 箇所に及んでいます。また、このうちの 26 サイトでは管理者権限の詐取が発生しています。ただし、これらの数値は、JPCERT/CC に報告されている件数でしかなく、実際にはより多くの不正アクセスが発生しているものと思われます。

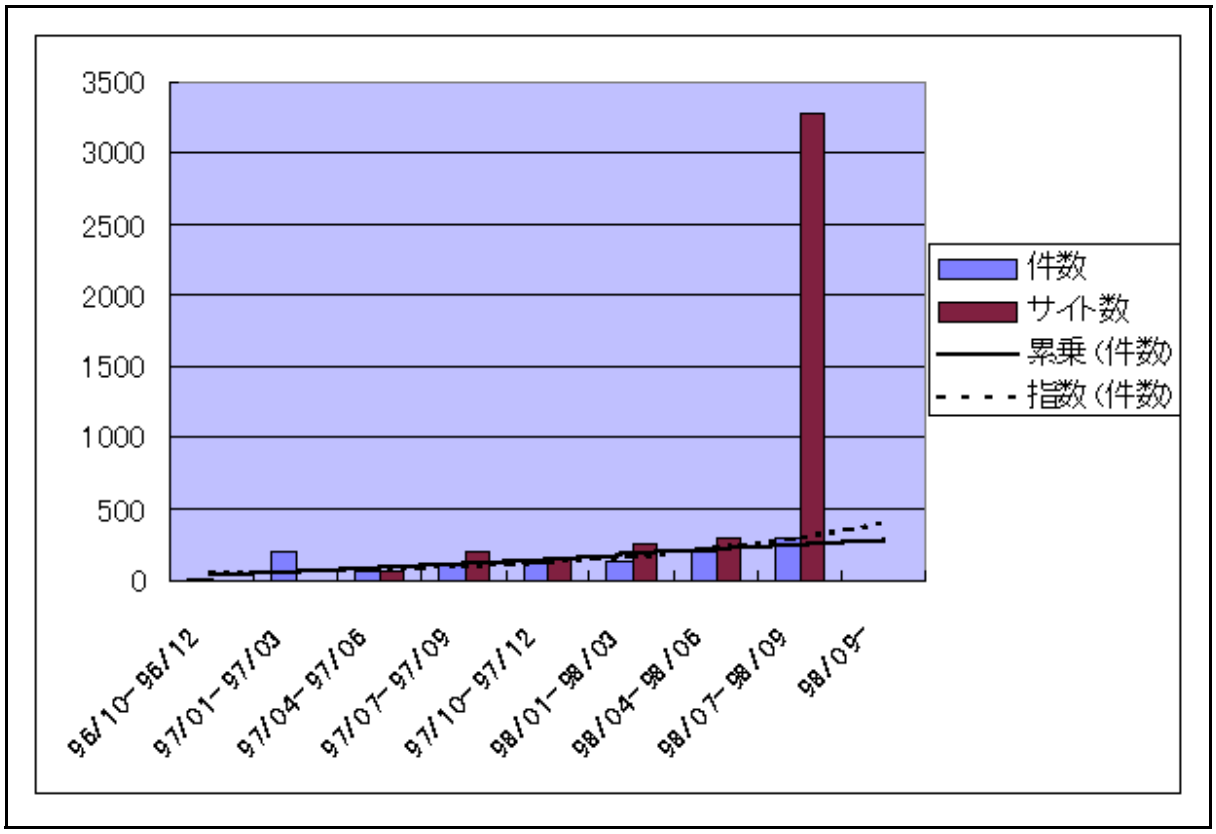
次に、この情報で報告されている不正アクセスの主な内容を示します。

- システムに存在するサービスや弱点の探査
- 電子メールの不正な中継、電子メール爆撃
- statd サーバを悪用した攻撃
- システムへの不正侵入と管理者権限の詐取
- Web サーバの cgi-bin プログラムを悪用した攻撃
- ネットワークやホストの運用を妨害しようとする攻撃
- ネットニュースのコントロールメッセージを悪用した攻撃
- パケット盗聴プログラムによる攻撃
- anonymous FTP サービスの不正利用
- named サーバを悪用した攻撃

このような情報は、JPCERT/CC が開設している Web サイト *http://www.jpcert.or.jp* から入手できます。

次に、これまで JPCERT/CC より報告されている不正アクセスの発生件数と関連サイト数を示します。





このような不正アクセスは、大きく次の 3 種類に分類できます。

- ポートスキャンによる新たな不正アクセス
- プログラムのセキュリティ上の弱点を利用した既知の不正アクセス
- メール中継や anonymous FTP などのサービスの不正利用

1 番目の不正アクセスでは、それまでの侵入手口であったピンポイント攻撃が網羅的な攻撃に変わっています。このようなポートスキャンによる侵入は、次のような順序で実施されています。

1. DNS を検索し、特定のドメインに属しているサイトを発見する
2. 探索によってホストサービスを発見する
3. statd、named、nfs、X などのセキュリティ上の既知の問題点の有無を発見する
4. その問題点を利用して不正侵入する

このような侵入方法については、ネットワーク上でスキャン用プログラムが公開されたり、エラー処理や侵入後のアクセス方法を示したドキュメントも用意されています。ここに示した手順によって管理者権限が不正に取得されたり、システムへの不正アクセスが試みられた関連サイトは、先ほど示した被害サイト数のうち 3,000 件にも及んでいます。また、このような侵入のための探索が国内サイトに対して大規模に実施された可能性もあります。このようなポートスキャンによる不正アクセスを防止するためには、次のような対策が有効なものとなります。

- 不要なポート（サービス）を停止したり制限する
- 関連ソフトウェアをバージョンアップする

先ほど示した不正アクセスのうち 2 番目と 3 番目に分類されるものは、適切に情報を入手し対策しておくことで事前に防止できます。このうち 2 番目の項目に分類される不正アクセスでは、statd や named などのサーバのセキュリティ上の問題点を悪用して、スタックオーバーフローを発生させ、ファイルを流出したり改竄し、管理者権限によってコマンドを実行するといったものとなります。このような不正アクセスを防止するためには、不要なサービスを実行しないようにしたり、ソフトウェアをバージョンアップすることが有効な対策となります。

また、3 番目の項目に分類される無関係なサイトへのメールの中継は、メール爆弾や不正メールの発信元として利用されるだけでなく、CPU やネットワークを浪費することにもなります。このようなメールの不正な中継は、ISP やユーザによるスパム対策（フィルタリング）を迂回したり、対象となる中継サイトへの嫌がらせや成り済ましが目的となっています。

メールの不正な中継を防止するためには、次のような対策が有効なものとなります。

- sendmail のバージョンアップ
- sendmail に対して中継を制限するように設定する

多くの不正アクセスは既知の方法によるものであるため、適切な対策を施すことによって影響を抑えることができます。ただし、それでも完全な対策は困難であるため、被害を最小限とするためにインシデントに対する準備やポリシーに基づく一貫した対策が必要となります。

4 不正アクセスとは

4.1 特徴

業務、取引、公共サービスなどのさまざまな範囲にインターネットの利用が拡大し、経済的な価値を持つ情報が受け渡されるようになったことで、不正アクセスも増加してきています。また、インターネットの利用ユーザ数も増加したことで、ユーザの考えやスキルがさまざまなものとなっていることも不正アクセスが増加する原因となっています。

このような原因から増加している不正アクセスには、次のような特性があります。

- 地球規模でのコンピュータネットワークが利用できるため、国境を越えた侵入が可能
- 誰でも利用できプロトコル仕様が公開されているため、解析やツールの開発が容易
- 高速化や定額料金によって、反復的なアタックや力ずくのアタックが可能
- 侵入者の身元を隠す匿名性
- 人に見られずに侵入できる

このような特性を持つ不正アクセスによって、システムへの不正な侵入が実施したときには、次のような問題が発生する可能性があります。

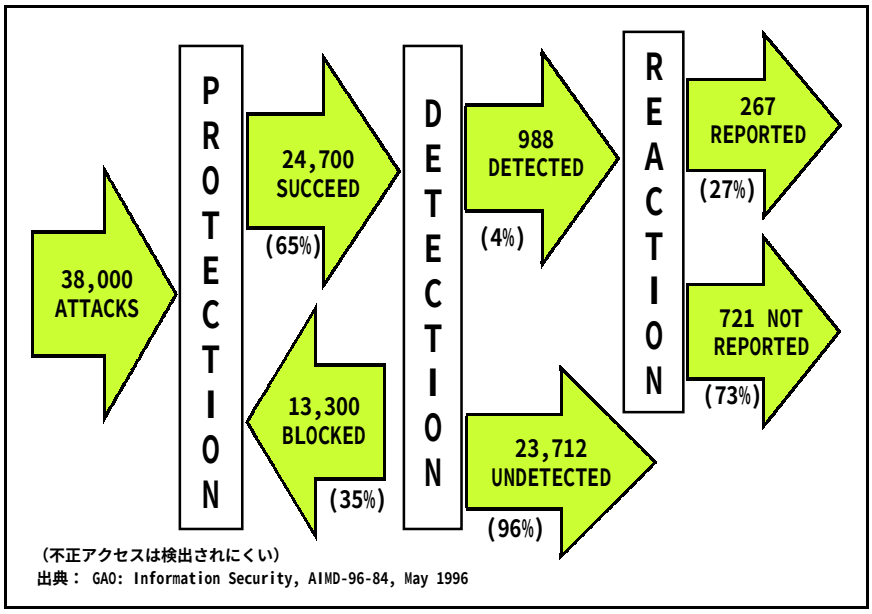
- コンピュータ資源の不正利用
- 妨害や破壊
- 悪戯
- 踏み台
- 成り済まし
- メッセージの偽造
- 情報の漏洩、改竄、破壊

このため、システムの運用や情報の利用から考えて、次のような項目を保護する必要があります。

- 正常な運用を維持するための可用性
- 侵入や踏み台の防止
- 盗聴を防止するための機密性
- 改竄を防止し検知するための完全性
- 送信者の正当性を確保するための真正性

不正アクセスを実施する侵入者が利用する手口には既知のものもありますが、全体的にはより複雑で高度なものや巧妙なものを組織的に使用するようになってきています。また、ユーザ側では、インターネットが一種のブームとなり、不正アクセスを適切に認識せず対策も不十分な状態で、漠然とした不安を抱いたままで安易に接続し続けています。さらに、技術面では、情報や技術者の不足や、技術自体も未発達で製品も少ないため、侵入者とのイタチごっことなっています。

次の図は、1996 年 5 月に米国会計監査院から提出された『GAO: Information Security』で示されているものですが、不正アクセスが検出されにくいという傾向を表しています。この図からもわかるように、38,000 件の不正アクセスの試みに対して 35 パーセントしか防ぐことができず、侵入された後に検出できたものも 4 パーセントしかなく、報告されたものは 267 件でしかありませんでした。



このようなインターネットにおけるシステムへの不正侵入は、複数の組織による国際的なものとなり、侵入の手口も高度なものとなっています。このため、緊急に対策を実施する必要があり、関連組織間の調整役として JPCERT/CC が設立されています。また、現在の不正アクセスでは、侵入者間でセキュリティに関する情報を交換するためにメーリングリスト、Web サーバ、FTP サーバ、FAQ、雑誌などが存在し、侵入方法、侵入のためのソフトウェア、流出したパスワードや電話番号のリストなどが受け渡されています。このため、ユーザ側でも常にセキュリティについて関心を持ち、最新情報を入手して不正アクセスからシステムを保護するように努力しなければなりません。

4.2 法律面での問題点

次のように「不正アクセス」には、いくつかの定義が存在しています。

- 不法または有害な意図をもって行われる無権限アクセスや傍受（『コンピュータ関連犯罪－立法政策の分析』OECD、1986 年）
- 不正な手段により、ユーザ以外のものが行うアクセスまたはユーザが行う権限外のアクセス（『情報システム安全対策指針』平成 9 年国家安全委員会告示第 9 号）
- システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと（『コンピュータ不正アクセス対策基準』平成 8 年通商産業省告示第 362 号）

また、不正アクセスには、次の 3 種類の視点が存在しています。そして、これらの視点が微妙に異なっているため、それぞれの要求を満たすことが難しいものとなっています。

- 情報や資源の所有者の視点
- システム管理者の視点
- 法律上の視点

現在、日本国内では、次のような刑法によって、貯金元帳ファイルなどへの不正データの入力や、データベースやファイルなどのデータ消去は、違法な不正行為となっています。

- 電子計算機使用詐欺（刑法 246-2）
- 電子計算機損壊等業務妨害（刑法 234-2）
- 電磁的記録不正作出（刑法 161-2）
- 電磁的記録毀棄（刑法 258、259）
- 器物損壊（刑法 261）
- 電子計算機損壊等業務妨害（刑法 234-2）

ただし、パスワードの類推やソフトウェア検出によるパスワードの入手、そのパスワードの売買、システムへの侵入については、現在は法整備が検討されている段階であり、違法な不正行為とはなっていません。

警察庁は、1998 年 11 月 17 日に発表した不正アクセス法の案について、1998 年 12 月 16 日まで公開コメントを募集しました。このような法が立案された背景には、インターネット犯罪に対抗するための不正アクセスの可罰化と、コンピュータ犯罪への国際的連携の必要性があります。

この法案で注目すべき点には、次のようなものがあります。

- 法の趣旨が「犯罪の防止を目的として不正アクセスを禁止」している
- 対象となる計算機を「事業用に供され、公衆回線に接続されているもの」としている
- アクセスコントロールを「パスワードや ID などの利用者識別情報によって利用者を制限する」ものとしている
- 不正アクセスを「他人の ID やパスワードを冒用する行為」や「システムのセキュリティホールを攻撃する行為」としている
- 対象となる計算機の使用者義務として「アクセスログを取り 3 カ月間保存」を課している

同様に、1998 年 11 月 25 日には、郵政省からも電気通信法の改定案として不正アクセスに関する考えが提示されました。

4.3 不正アクセスの手口

不正アクセスの例としては、次のようなものがあります。

- IP パケット偽造による成り済まし
- 制御パケットの偽造による運用妨害
- ネットワーク盗聴
- WWW サーバの情報改竄
- 通信の乗っ取り
- セキュリティホールの利用
- 電子メール攻撃や電子メール偽造
- システム侵入

次に、このような不正アクセスで使用されている手口を示します。

4.3.1 セキュリティホールの利用

セキュリティホールには、プログラム上の論理ミス、バッファオーバー、隠し機能や、設定ファイルや設定パラメータでの設定の誤りがあります。そして、このような誤りが侵入のために使用されます。セキュリティホールを悪用した不正アクセスは、OS のシステムコールや NFS だけでなく、statd、named、sendmail などの各種アプリケーション、異常に長い IP パケットや SYN 攻撃などによる通信プロトコルなどといった、さまざまな範囲に及んでいます。

4.3.2 盗聴

盗聴では、ネットワーク上で受け渡されている情報を監視し、ログイン名やパスワードを詐取します。このような不正アクセスの 1 つにスニーファ攻撃があります。スニーファ攻撃では、最初に組織内のノードへの侵入が試みられ、ネットワーク監視用プログラムがインストールされます。そして、ネットワーク上で受け渡される通信情報からログイン名とパスワードが抽出され、侵入者に転送されます。

このような盗聴を防止するためには、スイッチィングハブを利用したり、ホストやファイアウォールを適切に設定することが有効です。

4.3.3 コネクションハイジャック

コネクションハイジャックは、TCP セッションを監視し、認証の完了後に確立した論理的な通信路を乗っ取り、第三者のふりをして通信する不正アクセスです。

コネクションハイジャックを防止するためには、IPSec やフィルタリングが有効です。

4.3.4 NFS の利用

NFS（Network File System）は、本来 LAN 環境での利用を前提に設計されています。このため、不用意に外部から NFS が利用できるようになっていると、不正アクセスによって悪用されることがあります。

NFS の不正利用を防止するためには、NFS や UDP のパケットが外部に出ないようにすることとなります。

4.3.5 Web 内容の改竄

この不正アクセスは、Web サーバに侵入し Web ページの内容を改竄してしまうもので、対外的に影響の大きな不正アクセスです。このときには、通常の侵入方法のほかに CGI プログラムの問題点を利用して Web サーバに侵入されることもあります。

また、今後の Web システムでは、危険なプラグインコマンドをユーザにダウンロードさせる行為の発生が懸念されます。

4.3.6 ソーシャルエンジニアリングアタック

これは、システムの運用者や利用者に対して、メールでの特定ファイルの送付、パスワードの失念、緊急アカウントの設定要求などによって情報を入手し、不正アクセスしようとする行為です。

4.3.7 踏み台

これは、システム内で制限のゆるいホストやネットワークを利用して、侵入元や侵入経路を特定しづらくし、システムに侵入する行為です。このようなときに利用されたシステムは、運用者が知らぬ間に侵入者に加担していることになります。

たとえば、従業員宅からのアクセスを許しているシステムでは、ファイアウォールによって社外からのアクセスを規制していたとしても、従業員宅のコンピュータを踏み台として利用されたときには不正アクセスを防止できなくなる可能性があります。

このような不正アクセスを防止するためには、同一のポリシーでシステム全体を運用し、踏み台として利用されたときにはシステム内のホストやネットワークを 1 つずつ検証していく必要があります。

5 セキュリティポリシー

5.1 セキュリティポリシーとは

実際にセキュリティ対策を施すためには、まずユーザ要求、予測リスク、最新技術動向などに基づいてセキュリティポリシーを策定します。そして、実施計画を立案した後、実際に技術的な対策や教育などが実施されていることを監査しながら対策全体を見直していきます。このため、セキュリティポリシーは、管理範囲内のコンピュータシステムのセキュリティに関する目的、方針、運用管理手順などを記述した文書となり、セキュリティ施策に対する基本仕様書となります。

セキュリティポリシーの内容は、情報の価値に対する評価やリスクの予測、管理体制などによって各組織で異なったものとなります。ただし、その目的は、次のように共通したものとなります。

- 関係者での合意と情報の共有
- 関係者の役割と責任の明確化
- 実施計画の基準
- 監査やレビューの判断基準

また、セキュリティのための対策を施すときには、組織内ではユーザ、ネットワーク管理者、意志決定者が関係し、組織外ではコンサルタント、プロバイダ、ベンダー、緊急対応チーム、警察などが関係してきます。

さらに、セキュリティ対策では、意志決定者である経営者の合意が必要です。このような合意を得ていないと、権限の拠り所がなくなり、実施が曖昧になり、緊急時の判断が遅れてしまいます。また、組織内のシステム管理者やユーザの合意も必要です。これらの関係者の合意を得ていないと、実際のセキュリティ対策の実行が不可能となったり、多数の抜け穴が発生してしまいます。

セキュリティポリシー自体を策定していなかったときには、次のような問題が発生します。

- 機能やセキュリティ対策についての判断に対して意志決定できない
- 利用ツール、確認項目、アクセス制限事項などのセキュリティに関する施策を判断できない
- 施策の妥当性を確認できない
- 関係者の合意を得られない
- セキュリティに関する施策に一貫性がなくなり、コストやリスクが増加する

セキュリティポリシーについての参考文献としては、
『Site Security Handbook』（RFC2196、1998 年 9 月発行）や『コンピュータ不正アクセス対策基準解説書』（日本情報処理開発発行）があります。

5.2 セキュリティポリシーの策定

セキュリティポリシーの策定は、基本的に次のような手順となります。

1. 守るべき対象の候補の列挙
2. 守るべき対象の抽出と決定
3. 予期される脅威の列挙
4. 保護する手段の実施
5. レビューと改善

このときには、問題が発生したときに受ける損害や復旧のための有形の費用や無形の費用が、防御のための費用より大きなものであることも検討します。

守るべき対象は、インターネットでは、機密情報、価値のある情報、知的財産権のある情報となります。また、システム全体では、これらの項目に加えて、ハードウェア、バックアップメディア、サプライ品などとなります。ただし、このような項目は、組織によって異なるため、最初にすべてを列挙した後、その中から取捨選択するようにします。

また、資産への脅威を明確にすることも必要です。すでに示してきたように、検討すべき脅威には次のようなものがあります。このような脅威のうちいずれのものから資産を守ろうとしているのかを検討し、具体的な損失の可能性を予測するようにします。

- 資源、情報への不正アクセス
- 意図しない、不正な情報の公開
- 情報の改竄
- 破壊
- CPU 資源の利用
- 踏台
- サービス妨害

さらに、相反する要素間でのトレードオフや投資対効果から適切に目標を設定します。このうち、相反する要素間でのトレードオフでは、サービスの提供によるリスクとセキュリティへの影響や、操作性とセキュリティとのトレードオフを検討する必要があります。また、投資対効果では、セキュリティ対策のための費用と問題発生時の損失を考慮するようにします。

実際のセキュリティポリシーの策定では、次のような項目を実施する必要があります。

- 文書として表明
- 実現可能
- ユーザ、管理者、経営管理者の責任の範囲の明確な定義
- 関係者のレビューと合意や理解
- 技術者や弁護士などの専門家に対するレビュー
- 柔軟性
- ポリシーの定期的なメンテナンスの手順

策定するセキュリティポリシーには、ある程度の柔軟性が必要です。このような柔軟性には、セキュリティポリシーの変更を容易なものとするためのコンセプトと実現方法の分離、更新のための手続きや参画者の明文化、例外事項の明確化などがあります。

5.3 セキュリティ施策

セキュリティポリシーを策定した後には、その内容に基づいて具体的な計画を立案します。このようなセキュリティのための施策には、次のような項目が含まれます。

- システムの構成
- サービスの選別
- システム基盤へのセキュリティ施策
- サービスごとのセキュリティ施策
- 履歴の記録や管理保存
- 異常検出方式やその手順
- トレーニング

このうち履歴となるログの記録は、不正アクセスの調査や検出に利用したり、不正アクセス自体の証拠となります。このため、ログインやログアウトに関するログだけでなく、次のような利用状況も記録するようにします。

- スーパーユーザアクセス
- 重要なシステムの変更
- 重要なサービス処理の記録
- 許可されない処理の要求の記録

収集したログは、不正アクセスによって消去されたり、改竄されたり、流出してしまったり、ログの記録自体が停止させられてしまわないような安全な場所に保存します。また、このようなログは、緊急時にもアクセスできるようにし、必要に応じて次のような複数箇所に保存するようにします。

- ローカルホストのファイル
- リモートホストのファイル
- 追記型デバイスに記録
- ラインプリンタ

ログのバックアップも、不正アクセスによるインシデント発生後の復旧やインシデント自体の解析のために必要となります。このため、インシデント発生前のバックアップを確保するために、バックアップメディアを複数組用意し、適切に管理する必要があります。

5.4 インシデント対応

実際に不正アクセスが発生してしまったときには、その場で速やかな判断が必要となり、誤った判断を下すことで損害を大きくしてしまうことがあります。このため、適切な判断を下すための手順をあらかじめ明確にし、インシデント発生後に必要となる対策や準備を実施しておくようにします。

実際にインシデントが発生したときには、次のような項目の実施を判断しなければなりません。

- サービスの提供を停止するか継続するか
- 解析を優先するか復旧を優先するか
- 誰に連絡し、どう連係するか
- 事実を公開するか、秘密にするか

また、被害を最小限に抑えるために、次の項目についてもあらかじめ検討しておきます。

- 顧客対策
- 経済的な損失
- マスコミ対策
- 法律的対策
- 被害を受けた関連サイトへの法律的責任

さらに、インシデントの判定方法や判定基準も検討しておきます。たとえば、インシデントの発生を判定するための兆候には、次のようなものが考えられます。

- システムクラッシュ
- システムの再起動
- メッセージログやコンソールでの異常の記録
- 性能の低下
- 未知のユーザアカウント
- 未知ファイルの存在や既知ファイルの消失
- アカウンティング情報やシステムログの不整合
- ファイル長や更新日付の変化
- ログイン不能
- 標準コマンドの消失や所定動作の不能

ただし、このような兆候は、インシデントの発生以外にも発生する可能性があるため、判定時には十分な注意が必要です。次に、CERT が提示しているインシデント発生のチェックリストを示します。

1. ログファイルの確認
2. setuid、setgid 付きファイルの不正作成を確認
3. システムバイナリファイルの不正変更の確認
4. ネットワーク監視プログラムの不正利用の確認
5. cron や at で実行されるプログラムの確認
6. 不正なサーバの不正な追加を確認
7. パスワードファイルの調査
8. ネットワーク設定ファイルの不正変更を確認
9. 隠れファイルの作成を確認
10. さらに関連する LAN 上の計算機も確認

そして、インシデントが発生してしまったときには、同一の設定では再度同様の侵入手口で不正アクセスが試みられてしまうため、原因を究明するようにします。このとき、侵入手口が明確となっているときには、ほかにも同一の問題点がないかを検討します。

また、侵入手口が不明なときには、推定によって対策を施したり、部分的にサービスを停止したり、ログの記録を強化するようにします。また、インシデント発生時には侵入者によって他の侵入手口が仕掛けられている可能性があるため、システムをインストールし直すことが最短時間でシステムを復旧する方法となります。

さらに、インシデント発生時の対応では、社内の広報担当者などを活用した報道機関への発表も必要となります。このためには、発表時期や発表内容を検討する必要があります。このうち発表内容は、詳細内容での技術的な説明を低く抑え、推測を含まず、証拠能力が守られるようにし、報道機関側の論理に振り回されないようにします。また、侵入者が内部犯であったときには、その上司や人事部門との連携も必要となります。

6　第 1 部のまとめ

これまでに示してきたように、不正アクセスに対処するためには関係者間での合意を得、責任分担を明確にすることが必要です。このためには、不正アクセスに対する意識や問題点を共有し、セキュリティポリシーとして文書化しておくようにします。ただし、最初からセキュリティについてのすべての項目を作成しようとするのではなく、できる部分から実施していくようにします。

また、不正アクセスを防止するためには一貫性が必要です。このため、無駄な努力を費やしていないことや抜けがないことを確認するために、セキュリティポリシーが重要なものとなります。さらに、完全な防御は不可能ですので、インシデント発生時の対応方法もあらかじめ検討しておくようにします。また、技術者や法律専門家をアドバイザとして確保し、常に最新情報を入手するようにし、適切に対策を施し続けるようにします。

第 2 部 不正アクセス対策とセキュリティツール（白橋 明弘）

7　不正アクセスの手口

不正アクセスの典型的な手順は、次のようなものとなっています。

1. ポートスキャンで（不用意に開いてる）サービスを見つけ
2. sendmail、INN、phf、imap、pop、rpc.statd、named などのアプリケーションのセキュリティホールを利用し
3. /etc/passwd などのファイルを入手し
4. パスワードクラックでアカウントを詐取し
5. OS のセキュリティホールをついて root 権限を詐取し
6. トロイの木馬を仕込んだり
7. パケット盗聴プログラムを仕掛けたりする

また、このような手順は、実行のためのツールを容易に入手できるため、技術的な知識をほとんど必要としません。また、アプリケーションのセキュリティホールとして最近悪用されることが多いバグには、ファイアウォールでは防げないものもあるため注意が必要です。

最近の JPCERT/CC の活動報告では、次のような不正アクセスの発生が報告されています。このうち、上位 4 項目については、アプリケーションのセキュリティホールを悪用したものとなっています。

- sendmail への攻撃
- INN を悪用した攻撃
- Web サーバの CGI プログラムを悪用した攻撃
- IMAP サーバを悪用した攻撃
- パスワードの推測、パスワード破り
- ルート権限の詐取
- パケット盗聴プログラムによる攻撃
- トロイの木馬プログラム

7.1 sendmail への攻撃

1996 年末から 1997 年始めに、国内の多数のサイトに対して sendmail のかなり古いバージョンである R5 のセキュリティホールを悪用した不正アクセスが発生しました。この不正アクセスでは、/etc/passwd ファイルがメールで送信され不正に入手されたようです。また、wftpd のセキュリティホールや設定のわかりづらさから、anonymous FTP でのアップロードに関する誤設定を悪用して root ディレクトリへのアクセス権を不正に入手する試みも実行されました。

このような不正アクセスについての届出が 100 件以上となったため、JPCERT/CC は、1997 年 1 月 9 日付けで『96 年末から 97 年始にかけての不正アクセスに関する緊急報告』を提示しました。このような不正アクセスを防ぐためには、アプリケーションをきちんとバージョンアップし、不要なデーモンを停止することが必要です。

7.2 INN を悪用した攻撃

この不正アクセスは、ネットニュースサーバ INN に対するコントロールメッセージを処理しているスクリプト parsecontrol のチェック不足を悪用し、不正なシェルスクリプトを実行するコントロールメッセージを投稿して、/etc/passwd や /etc/initd.conf のファイルをメールで送信させるものです。

ただし、この不正アクセスによって実際に被害が発生したかどうかは未確認です。JPCERT/CC では、1997 年 3 月 18 日に『ネットワークニュースのサービスを悪用したアタックに関する緊急報告』を提示しました。このような不正アクセスに対しては、ファイアウォールは直接的には有効なものとはなりません。

7.3 Web サーバ CGI を悪用した攻撃

この不正アクセスでは、Web サーバのかなり古い CGI である phf を悪用し、/etc/passwd ファイルを入手して、辞書引き攻撃であるパスワードクラックによって詐取したアカウントでの侵入が試みられます。これに対して JPCERT/CC は、1997 年 8 月 5 日に『phf CGI プログラムを悪用したアタックに関する緊急報告』を提示しました。ただし、現在でも、この既知バグを含んだ phf を利用している Web サイトが多数存在しています。また、nph、webdist、count、php などの多くの CGI にはバグが含まれています。

7.4 IMAP サーバを悪用した攻撃

この不正アクセスは、ワシントン大学で実装された IMAP/POP サーバでのバッファオーバーランのバグによって、外部から root 権限でコマンドが実行できてしまうことを悪用しています。JPCERT/CC は、1997 年 9 月 9 日付けで『IMAP サーバプログラムを悪用したアタックに関する緊急報告』を提示しています。現在の BSD/OS や Linux の配布パッケージでは、デフォルト状態でインストールすると、この IMAP/POP サーバを含めた多くのサービスが自動的に起動されるように設定されていることのほうが問題なのかもしれません。

7.5 パスワードの推測とパスワード破り

通常実施される不正アクセスでは、安易に設定されたパスワードを推測したり、不正に入手した /etc/passwd ファイルからパスワードクラックという辞書引き総当たり攻撃によって、アカウントが詐取され利用されています。

このような不正アクセスを防止するためには、メールサーバなどの多数のユーザを登録しているサーバをファイアウォール外に設置しないことが必要です。また、ユーザに対するパスワード管理の教育活動も必要です。

7.6 ルート権限の詐取

パスワードの推測やパスワード破りによって入手した一般ユーザのアカウントは、システムに侵入するために悪用されます。そして、システムへの侵入後に、setuid によって実行可能となっているプログラムのバッファオーバーランなどを利用してオペレーティングシステムのセキュリティホールから root 権限が詐取されます。

7.7 パケット盗聴プログラムによる攻撃

root 権限を詐取すると、そのホスト上に LAN 環境で受け渡されているパケットを盗聴するスニーファプログラムが仕掛けられます。このようなパケットを盗聴することで、他のシステムにログインするためのユーザ名やパスワードが詐取され、それを使って他のシステムへの侵入が繰り返されます。

7.8 トロイの木馬プログラム

このような盗聴プログラムは、通常のシステムプログラムやアプリケーションを不正な機能を実行するものに入れ替えて隠されます。また、アカウントログ関連のプログラムも入れ替えられ、不正侵入の痕跡を消去したりアカウント情報の詐取のために利用されます。

8　サービス妨害攻撃

サービス妨害攻撃とは、サーバやサービスを利用不能に追い込む一種の業務妨害で、英語表記の Denial of Service attack から「DoS アタック」とも呼ばれています。また、サービス妨害攻撃は、TCP SYN Flood、Ping of Death、OOB、Land attack などの TCP/IP やアプリケーションの実装上の問題を悪用したものがほとんどです。

このため、基本的には実装上のバグをパッチで解消することで対応できますが、利用製品が広範囲に渡っているため対応が困難な部分もあります。また、TCP/IP レベルでのサービス妨害攻撃に対しては、ファイアウォールでのトランスポート層レベルの中継が有効な防御となります。

8.1　TCP SYN Flood 攻撃

このサービス妨害攻撃では、TCP の SYN のみを送って不完全な接続を多数生成させることで、バッファを確保したままとしシステム内で待ち行列をあふれさせ、外部から接続できないようにします。この攻撃に対する根本的な対策はありませんが、現在の OS では待ち行列に確保できる数を大きくするなどの対策が施されているため、ある程度の攻撃には耐えることができます。

8.2　Ping of Death

このサービス妨害攻撃は、TCP/IP の実装上のバグを悪用したもので、規約サイズである 64K バイト以上のオーバーサイズパケットを送り、分割されたパケットをまとめさせることでバッファをオーバーフローさせ、システムのクラッシュ、フリーズ、リブートを発生させます。このようなサービス妨害攻撃は、ping コマンドだけではなくさまざまなプロトコルで実行可能であり、プラットフォームも広範囲にわたるため、パッチが存在していないものもあります。

8.3　OOB attack

このサービス妨害攻撃は、Windows NT の port 139 に TCP の urgent flag（Out Of Band option）を設定したパケットを送り、Windows NT 自体のバグを悪用してシステムをフリーズさせるものです。ただし、現在ではサービスパック 3 で対策されているようです。

最近、このような Windows NT のセキュリティホールを悪用した妨害攻撃が多数報告されています。これは、Windows NT の利用が拡大しているためで、Microsoft 社も対応に努力しているようです。ただし、基本的には、port 137 ～ 139 はフィルタリングし、不要なアクセスは停止しておくべきです。

8.4 Chargen/Echo 攻撃

このサービス妨害攻撃は、IP のデバッグ / ネットワークチェック用基本組込みサービスである Chargen と Echo を利用したもので、文字列を生成する Chargenと文字列を返すEchoをループさせることでネットワークトラフィックを飽和させます。このサービスは、TCP と UDP の両方にありますが、UDP ではソースアドレスの偽造が容易なため、攻撃が簡単なものとなっています。この攻撃を防止するためにも、不要なサービスを停止したりフィルタリングすることが必要です。

8.5 LAND attack

このサービス妨害攻撃は、主にルータを対象としたものですが、送信 IP アドレスと受信 IP アドレスが同一で送信ポートと受信ポートが同一という奇妙な TCP SYNC パケットを送り、TCP/IP の実装によってカーネル内でループを発生させハングアップさせます。このようなルータに対する不正アクセスでは、ネットワークが利用できなくなるだけでなく、ネットワーク情報が盗まれる可能性もあります。

このサービス妨害攻撃は、処理性能についての検討が必要となりますが、アクセスリストの設定によって回避できます。また、このようなサービス妨害攻撃では IP スプーフィングが利用されていますので、ファイアウォールも有効な防御手段となります。

8.6 Smurfing

このサービス妨害攻撃は、ブロードキャストアドレスに対して ICMP エコー要求のパケットを送り、多数の ICMP エコー応答を返させることでホストや回線を麻痺させます。このとき、送信アドレスには、第三者のアドレスが悪用され偽造されています。このため、この攻撃では、受信側となった第三者の回線も麻痺してしまうことがあります。この攻撃は、ブロードキャストに対する ping コマンドに応答しないようすることで防止できます。

9　ホストの守り方

これまでに示してきた不正アクセスの多くでUNIXがターゲットとなっている理由は、インターネット環境で UNIX システムが多数利用されているためです。ただし、UNIX は、適切に管理すればセキュリティ上の問題を発生しづらいものにできます。また、UNIX は、情報がオープンなため、問題の発見や対策が比較的早期に実施され、システム上の機能不足をフリーソフトウェアなどで補うこともできます。このため、セキュリティについての情報を積極的に収集することで、多くの不正アクセスを防止することができます。現在利用されている UNIX システムでの問題点は、ワークステーションの普及によって経験の浅い root が急増していることです。

これに対して Windows NT や Windows 95, 98 による環境では、LAN 環境での使いやすさを優先してきたため、セキュリティ上の重要な情報を安易に漏らしてしまうことがあります。また、デフォルトでの設定にセキュリティ面で弱い部分もあり、旧システムとの互換性を維持するために簡単にセキュリティを強化できなかったり、ログに記録される情報が十分ではないなどの問題点もあります。さらに、サービス妨害攻撃に対する弱点が多数発見され、クラッキングツールも盛んに開発されています。このため、Windows 環境も、リモートログインできないからといって安心することができなくなってきています。

このような UNIX や Windows 環境によるホストを不正アクセスから守るためには、次のような項目に注意すべきです。

- CERT Advisory などでセキュリティホールに関する情報を頻繁にチェックし、必要に応じてパッチをあてたりデーモンを入れ替える
- パスワードを管理するために、ユーザを教育し、crack などのツールを使ってチェックする
- 不正アクセスを監視し記録し排除するために、tcp_wrapper などによって詳細なログを記録する
- 侵入を発見する

9.1 セキュリティホールの解消

セキュリティホールを塞ぐためには、CERT Advisory などのセキュリティ情報を活用し、ベンダーから提供されるパッチをあてたり、問題のあるデーモンなどを入れ替えるようにします。ただし、パッチによっては日本語版への対応が遅れることがあり、この対応時期の遅れが問題となることがあります。また、バッファーオーバーフローについて注意するようにします。さらに、手作業によるミスを防ぐために、システム設定にセキュリティ監査ツールなどを活用するようにします。

セキュリティ監査ツールには、システムの設定ファイルをチェックする内部監査ツールと、ネットワーク経由で攻撃に対する問題点をチェックする外部監査ツールがあります。このうち内部監査ツールである COPS（Computed Oracle and Password System）では、次の項目がチェックされます。

- システム関連のファイル、ディレクトリ、デバイスのアクセス権
- root およびユーザの設定ファイルのアクセス権
- group、passwd、cron などの各ファイルの内容
- setuid プログラム

また、外部監視ツールには、SATAN（Security Administrator Tool for Analyzing Networks）や ISS（Internet Security Scanner）などの市販の監視ツールがあります。このようなツールでは、問題箇所についてのデータの蓄積が製品間の提供機能の違いとなっています。また、外部監視ツールを適切に利用するためには、チェック結果を判断する専門的な知識が必要です。

9.2 パスワードの問題

これまでパスワードは、英数記号 8 文字程度で構成され、暗号化したものが /etc/passwd ファイルに収められていました。このため、辞書に存在する語、人名、地名、英文字のみなどの安易なパスワードは、辞書引き攻撃によって簡単に詐取されてしまいます。このようなパスワードの問題を解決するためには、ユーザの教育が必要です。

ユーザに対する教育では、AntiCrack によるパスワード設定時の検査や、passwd+ や npasswd による定期的なパスワードの変更を利用できます。また、日本語辞書やルールの拡張が必要ですが、crack を使ってパスワードを検査することもできます。crack によるパスワード検査では、数十パーセントのパスワードが破られてしまうこともあります。このような状況が発生すると、ユーザにパスワードを修正させる作業自体が困難なものとなることもあります。

また、パスワード自体が平文でネットワーク上で受け渡されていると、盗聴される危険性があります。とくに、外部からのログイン処理では、スニーファが仕掛けられている可能性もあるため危険性が増します。このような問題を解決し安全にリモートログインするために、最近では、使い捨てパスワードである One Time Password や、SSH、SSL-telnet、PET などの認証や暗号化が利用できるようになってきています。

9.3 アクセス制御

アクセス制御の基本は、必要ないサービスは停止し、必要な箇所に対するアクセスのみを認めることです。このような許可や不許可を判断するときの条件項目は、IP アドレス、ドメイン名、ユーザ情報などとなり、判断を実施する箇所は、ルータ、ファイアウォール、inetd によるサービスの呼び出し、アプリケーションなどとなります。現在、シングルサインオン環境が要望されていますが、まだ特定の状況でのみ利用できるレベルだと思います。

また、アクセス制御のために、次のようなプログラムを利用することもできます。

- xinetd
  inetd と置き換えることで、アクセスを制限したりログを強化できます。
- tcp_wrapper
  inetd から tcpd を経由してサービスが呼び出されます。これによって、アクセスを制限したりログを強化できるだけでなく、コマンドも実行できるようになります。ただし、tcp_wrapper の利用によって、新たに別の不正アクセスが発生しないように注意する必要があります。
- ucpspi-tcp
  inetd 経由でなく、サービスごとに tcpserver がデーモンとして常駐しサービスを呼び出します。

さらに、ログの記録では、tcp_wrapper などで提供されているログ機能を使って接続ログを記録したり、アプリケーションレベルでの認証の成功 / 失敗、実行されたコマンドの内容やその結果を記録するようにします。また、記録されるログ内容が不十分なデーモンは交換するようにします。さらに、使い捨てパスワードである S/Key や One Time Password に対応している logdaemon を利用することで、telnetd や rlogind のログ機能も強化できます。

9.4 侵入の発見

TripWire というツールを利用することで、システムの整合性をチェックし、不正アクセスによる侵入を発見できます。TripWire では、ファイル属性とメッセージダイジェストが定期的に検査されデータベースの内容と比較されることで、改変されたファイルが発見されます。また、ディレクトリごとにチェック内容を細かく設定することもできます。ただし、TripWire を利用するときには、そのシステムやデータベースは、読込み専用とするかオフラインの安全な場所に保存しておく必要があります。

また、BSD 系 UNIX では、ネットワークインターフェイスの状態が promiscuous モードとなっているかを確認し、スニーファが仕掛けられている可能性を検査する cpm（check promiscuous mode）を利用することもできます。さらに、watcher や swatch を使って記録中のログ内容から特定パターンを検出し、メール通知やコマンド実行によってログ監視を自動化することもできます。

最近では、ネットワーク上の通信を監視し不正な攻撃を検出して、管理者に通知したりネットワークの遮断を実行する侵入検知システム（IDS: Intrusion Detection System）も製品化されてきています。このような侵入検知システムは、ファイアウォールを補完するもので、ファイアウォールを利用できない状況で有効なものとなります。ただし、侵入検知システムで検知できないような低帯域によるスキャンや複数箇所からのスキャンなどの手法も開発されていますし、侵入検知システムの機能を悪用したサービス妨害攻撃を仕組まれる危険性もあります。

10 ファイアウォールの活用と限界

多数のホストを不正アクセスから守ることは困難です。このため、ファイアウォールという壁を設置し、外部からのアクセスを必要最小限のものにし、少数のホストのみをファイアウォール外に配置して厳重に守るようにします。ただし、電子メール爆弾、ウィルス感染、危険なオブジェクトのダウンロード、Web ブラウザのバグなどのファイアウォールでは防げない攻撃も存在しています。このため、ファイアウォールの限界を認識した上で、アプリケーションのバグ、サービス妨害攻撃、コンテンツフィルタリングにそれぞれ対応する必要があります。

ファイアウォールによって安全な中継が可能となります。ただし、INN のバグなどのアプリケーションのセキュリティホールを悪用した不正アクセスも存在しているため、ファイアウォールによってすべてのアプリケーションのプロトコルの正当性を保証することはできません。このような不正アクセスはファイアウォールを飛び越して実施されますが、ファイアウォールによって侵入者の行動が大幅に制限されるため、ファイアウォールの設置はある程度有効なものとなります。

ファイアウォールでのフィルタリングでは、スパムメール、ウィルス、Java/ActiveX による危険なオブジェクト、URL フィルタリングなどが対象となります。スパムメールについては、ブラックリストの管理が課題となっています。ウィルスについては、すでに実用的なレベルに達しています。Java/ActiveXで記述された危険なオブジェクトのダウンロードは今後の課題ですし、不適切なサイトへのアクセスの排除などの URL フィルタリングは、本質的には外部からの不正アクセスに対するセキュリティの課題ではありませんが需要はあるようです。

11 安全なアクセスのための技術

現在の認証技術は、次の 3 種類に分類できます。

- パスワードや暗証コードなどの「ある知識」を知っていることによる認証
- ID カードや鍵などの「ある物」を持っていることによる認証
- 指紋などの「ある特徴」を持っていることによる認証

このうち、コンピュータ利用では、ソフトウェアのみで実現できることからパスワードによる認証が多数利用されています。また、パスワードには、固定パスワードである Reusable Password と使い捨てパスワードである One Time Password があります。固定パスワードは、パスワード自体を侵入者に知られてしまうと、繰り返し攻撃に利用されてしまう可能性があります。これに対して、使い捨てパスワードは、侵入者に知られても再利用できないため安全なパスワードとなります。

使い捨てパスワードでは、秘密情報がそのままネットワーク上で受け渡されません。使い捨てパスワードのチャレンジ & レスポンス型では、ホストから受け取ったチャレンジデータをローカルマシン上でパスワードと組み合わせて演算し、結果をレスポンスとして返します。また、同期型では、時刻やカウンタで同期をとり、チャレンジデータの代わりにその時刻やカウンタが利用されます。このような使い捨てパスワードには、フリーソフトウェアの S/Key や OTP、商用の TokenCard があります。このうち Token Card には、次のような製品があり、1 万円以上と高価ですが、すでにいくつかの企業で利用されています。

- Security Dynamics による SecurID
- Secure Computing による SafeWorld
- AssureNet による SecureNetKey

使い捨てパスワードである One Time Password の問題点は、入力などが面倒なためユーザに敬遠され利用されないことです。ただし、この入力の手間を解消するために、dotkey95 や optsock for Windows 95 などの Windows 95 で利用できる S/Key や OTP の自動入力ツールが提供されています。このようなツールを利用すると、チャレンジデータをカットアンドペーストするだけでレスポンスを返すことができるようになります。

インターネット経由でのリモートログインでは、安全な認証や暗号化が必要です。このような機能は、SSL-Telnet、SSH（Secure Shell）、PET（Privacy Enhanced Telnet）や、VPN によるリモートアクセスで実現されています。

このうち SSH では、暗号化のために DES、Triple-DES、IDEA、RC4 が使用されています。また、認証では、RSA によるチャレンジ & レスポンスが使用され、256 ビットの乱数をサーバが公開鍵で暗号化して送り、クライアントが秘密鍵で復号化してメッセージダイジェストを返すことで検証されています。さらに、SSH では、ポートフォワーディングという仕組みも提供され、X や POP などの特定のアプリケーションを利用することもできます。ただし、この仕組みは、VPN のようにすべてのアプリケーションで利用することはできません。

このような SSH を普及させるためには、Windows 環境で動作するクライアントの普及が重要となります。現在、SSH に対応している Windows 用クライアントには、SSH Windows Client、F-Secure がありますが、日本語処理が提供されていません。ただし、TeraTerm 用の SSH プラグインを利用することで、TeraTerm を SSH に対応させ日本語を利用することができます。

インターネット経由でのメールの取得では、チャレンジ & レスポンスによるパスワードの暗号化が利用できる APOP を使用します。現在、APOP には、メールサーバとして qpopper や DeleGate が対応し、クライアントとしては Eudora PRO、Winbiff、Becky!、AL-Mail32 などが対応しています。ただし、Netscape 社と Microsoft 社が APOP に対応していないため、APOP 利用を普及させるための問題点となっています。

12 スパムメール対策

スパムメールとは、多数のユーザを対象として配布される商業メールです。スパムメールでは、送信側のコストは非常に低く、受信側のユーザや ISP が多大なコストを負担しなければなりません。また、メールアドレスの収集や売買、スパムメールを配送する業者も登場してきています。

スパムメール対策は、大きく 2 つに分かれます。1 つは、自ドメインが受け取るスパムメールへの対策です。そして、もう 1 つは、スパムメールの中継に利用されないための対策です。

自ドメインが受け取るスパムメールへの対策は、次のようなものとなります。

- スパムメールの送信元であるアドレスやドメインからのメールの受信を拒否する
- 送信元アドレスが実在することを確認する

スパムメールの送信元であるアドレスやドメインは、ブラックリストとして管理する必要があります。ただし、このようなアドレスやドメインを個人や一企業のみで管理することは困難です。この問題を解決する方法として、非商用ですが VIX/MAPS RBL や DORKSLAYERS/ORBS を利用する方法があります。

もう一方の対策である送信元アドレスの存在の確認では、送信元アドレスを基に DNS からメールが返信可能かどうかを判断し、返信できないときには受信を拒否する方法があります。ただし、このような受信拒否では、悪意がなく単に送信元アドレスが正しく設定されていないメールも受け取れなくなるため、過剰防衛となってしまう可能性もあります。このため、このような受信拒否方法を利用するときには、あらかじめログを記録し、実状を把握してから対策の実施を判断すべきだと思います。

スパムメールの中継に利用されないための対策は、次のようなものとなります。

- 外部から受け取り、外部へ配送するメールは拒否する
- 中継時に配送元ホスト名、IP アドレス、配送先メールアドレスなどのトレース情報をヘッダにきちんと残す

1 番目の項目は、ISP などでは必須の設定項目となります。また、スパムメールの中継を放置しておくと、スパムメール中継サイトとしてブラックリストに記載されてしまうことがあるため注意が必要です。

さらに、メーリングリストもスパムメールやメール爆弾の対象となるため、運用には注意が必要です。メーリングリストでは、登録メンバー以外からの投稿を拒否したり、メンバーのメールアドレスを公開しないようにします。また、本人の承諾なしにメーリングリストに登録されないように、管理者経由や確認処理を介して登録するようにします。

第 3 部 ファイアウォール構築技術（歌代 和正）

13 ファイアウォールのアーキテクチャ

ファイアウォールは、境界防御を実現する仕組みの総称で、要塞ホスト、Proxy ゲートウェイ、パケットフィルタリングなどを組み合わせて構成されます。また、ファイアウォールは、厳格なセキュリティ管理と、利用ユーザや内部ホストへの容易なサービス中継という相反する2つの機能を実現しなければなりません。さらに、ファイアウォールによって内部のネットワーク構成を外部のネットワーク構成に適切に関係させることで、ネットワークアドレス空間の不足を補うという副次的な効果もあります。

ファイアウォールでの境界とは、共通の管理方針によって管理される領域を取り巻く部分で、統一的なセキュリティポリシーが共有されます。境界防衛では、このような同一のセキュリティ境界を矛盾なく管理する必要があります。たとえば、次のような項目が存在していたときには、セキュリティ境界に矛盾が生じることになります。

- バックドア
- 外部からのモデムアクセス
- 内部からのダイヤルアップ接続

また、このようなネットワークに対するセキュリティだけでなく、建物、計算機室、居室などに対しても統一されたセキュリティポリシーを適用することが重要です。

13.1 要塞ホスト

ファイアウォールの構成要素の 1 つである要塞ホストは、直接インターネットと接続しているポイントで、厳格なホストセキュリティの管理対象となります。通常、要塞ホストは、2 つのネットワークインターフェイスを持ち、ホストとしての機能を提供します。

13.2 ファイアウォール構築ツール

ファイアウォールを構築するときには、ホストセキュリティの強化やサービスの中継のための何種類かのツールを組み合わせて利用します。このうち、セキュリティ強化ツールは、次の 2 種類に大別できます。

- アクセス制御
- セキュリティホールの検査

アクセス制御では、発信元アドレス、送信先アドレス、サービスの種類、利用者、利用時間帯などによってアクセスが制御されます。また、利用履歴を管理することもできます。このようなツールには、xinetd や tcp_wrapper などがあります。これに対して、セキュリティホールの検査では、システムが適正に設定されていることが検査されます。このようなツールには、cops、crack、ISS、SATAN、TripWire などがあります。

13.3 パケットフィルタリング

パケットフィルタリングは、ネットワーク層の IP パケットレベルを制御するもので、現在販売されているほとんどのルータに実装されています。また、この機能を提供しているものには、ルータのほかに、Altavista Firewall、FireWall-1 などのワークステーションベースのファイアウォール製品や、screend、IP Filter などの FreeBSD や Linux で利用可能なフリーソフトウェアがあります。

パケットフィルタリングでの処理は、「通したいものだけを通す」ことが基本となり、接続許可の判断対象によって次の 3 種類に分かれます。

- 接続を許可するホストからのパケットだけを通す、アドレスによるフィルタリング
- 利用可能なサービスのパケットだけを通す、サービスによるフィルタリング
- 外部に向かう接続だけを通す、接続方向によるフィルタリング

13.3.1 NAT

RFC1631 で規定されている NAT（Network Address Translation）は、IP アドレスの不足と、直接インターネットに接続する必要のないネットワークに対処するために考え出されたものです。NAT では、RFC1918 で規定されているプライベートアドレス空間の発信元アドレスや送信先アドレスをグローバル空間に対応付けています。この結果、内部ネットワークの構造を隠ぺいし、アクセスを制御することができます。また、このような対応付けには、静的なものと動的なものがあります。ただし、いずれの対応付けでも、ポートは変更されません。

これに対して IP Masquerade や NAPT（Network Address Port Translation）では、ポート番号も変換されます。この機能によってアドレス変換を実行しているルータのアドレスだけでインターネット環境を利用することができるため、端末型ダイヤルアップで利用されています。

13.4 サーキットゲートウェイ

サーキットゲートウェイは、アプリケーション層で動作しますが、アプリケーションプロトコル自体は理解していません。このため、トランスポートレベルゲートウェイと呼ばれることもあります。主なサーキットゲートウェイには、socks、udprelay、plug-gw があります。socks は汎用的な TCP Proxy ゲートウェイで、udprelay は汎用的な UDP Proxy ゲートウェイです。また、plug-gw は、TIS Firewall Toolkit に含まれている汎用的な TCP Proxy ゲートウェイです。

13.5 アプリケーションゲートウェイ

アプリケーションゲートウェイでは、アプリケーションプロトコルレベルでデータが中継され、そのプロトコルに応じた制御や監視情報の取得が可能です。また、ユーザに対する認証も実施できます。このようなゲートウェイ機能を本来から意識して作成されているソフトウェアには、sendmail、INN、C-News、NTP、Named などがあります。また、当初は直接クライアントとサーバが接続されているものとして作成されていたが、インターネット経由での利用のためにゲートウェイ機能を意識することが必要となったソフトウェアには、HTTP、Gopher、telnet、ftp、RealAudio、StreamWorks などがあります。

13.6 透過型 Proxy

これまでに示してきたパケットフィルタリング、サーキットゲートウェイ、アプリケーションゲートウェイのセキュリティに関する強度は、次の順序となります。

1. アプリケーションゲートウェイ
2. サーキットゲートウェイ
3. パケットフィルタリング

ただし、アプリケーションゲートウェイでは、新たなプロトコルが利用されるようになるごとに新たにゲートウェイも必要となるため、柔軟性はもっとも低くなります。また、アプリケーションゲートウェイでは、ユーザがアプリケーションごとに接続方法を考慮しなければなりません。このような問題を解決する技術が透過型 Proxy です。

透過型 Proxy は、本来は自分宛ではないパケットを横取りして自動的にゲートウェイとして機能します。このとき、クライアントは、透過型 Proxy を意識する必要がないため、相手先と直接通信しているときと同様に動作できます。また、透過型 Proxy は、原則として TCP レベルでの中継で IP パケットレベルでの中継ではないため、NAT や IP Masquerade とは本質的に異なるものとなります。

14 商用ファイアウォール

これまでに示してきた技術を組み合わせることで、ファイアウォールを構築できます。そして、このような技術を組み合わせているものの 1 つが商用ファイアウォールです。また、個々の技術を提供しているツールを組み合わせることで、独自にファイアウォールを構築することもできます。

このようなファイアウォールの構築は、少人数な SOHO などでサーバを利用するときにも必要です。ただし、SOHO などでは、構築や運用の手間からファイアウォールが設置されていないことがあります。このようなときには、使用したいサーバ機能を提供するアウトソーシングサービスを利用することで、容易にファイアウォールを実現できます。

商用ファイアウォールサービスは、次のような理由から登場してきました。

- コンピュータやネットワークを専門としないユーザが増加してきたため、サポートや管理サービスの必要性が高まっている
- 安全で手軽にインターネットを利用できる環境が必要となっている
- 攻撃手法が高度化している
- インターネットサービスが複雑化し、専門家以外の対応が限界に達している

また、単にツールを組み合わせるだけでは、ファイアウォールを安全に運用できません。このため、パケットフィルタリングやアプリケーションゲートウェイなどのさまざまなツールと、コンサルティング、構築サービス、教育、セミナーなどのサービスを統合した商用ファイアウォールサービスが提供されています。そして、最近の商用ファイアウォールサービスでは、Windows NT 向けのファイアウォール、製品が複雑化しアウトソーシング指向となっていることによる管理サービス、パケットフィルタリングとアプリケーションゲートウェイを組み合わせたハイブリッド型ファイアウォール、オールインワン型マルチサーバに対するファイアウォールなどが注目されています。

次に、代表的な商用ファイアウォール製品を示します。

表１：代表的なファイアウォール製品

製品名	ベンダー名
Altavista Firewall	Digital Equipment Corporation（Compaq）
FireWall-1	Checkpoint Software Technologies
CyberGuard Firewall	CyberGuard Corporation
Gauntlet	Network Associates
Eagle	Raptor Systems, Inc.
Portus	Livermore Software Laboratories, Inc.
Sidewinder	Secure Computing Corporation
SunScreen	Sun Microsystems, Inc.

また、米国で販売されているファイアウォール製品については、ICSA が提供している Web ページ（*http://www.icsa.net/services/consortia/firewalls/certified_products.html*）で詳細情報や評価結果を得ることができます。

このような商用ファイアウォール製品に対する選択基準としては、次のような項目が考えられます。

- 必要なアプリケーションは使えるか
- 拡張性はあるか
- 処理能力は十分か
- ソースコードが必要か
- サポート体制は満足できるものか
- 管理コストはいくら必要か
- どの環境で動作するのか
- 導入費用としていくら支払えるか

ただし、今後は、各製品での提供機能の差は小さくなると思えるため、それぞれのベンダーの設計コンセプトを重視すべきだと思います。また、新たな機能をいち早く採用している製品は、不安定となる可能性もあるため導入には注意が必要です。このような製品の機能そのものよりもサポート内容を重視すべきだと思います。さらに、ファイアウォールだけでは守りきれない部分に対しても、ベンダーからの提案などを参考にしてきちんと考慮すべきだと思います。

15 暗号技術の応用

次に、情報セキュリティの要件を示します。

- 秘密を保持するための秘匿性
- 内容を保証するための完全性
- 正しく通信相手を認識するための認証
- 通信の事実を保証するための否認防止

このような情報セキュリティの要件を満たすために、暗号技術として共通鍵暗号と公開鍵暗号が利用されています。

共通鍵暗号では、通信する両者で共通の秘密鍵を所持しておき、暗号化と復号化に同一の鍵を使用します。このような共通鍵暗号には、DES、FEAL、RC2、RC4、IDEA などがあります。共通鍵暗号は、通信相手が少数であるときには問題とはなりませんが、多数となったときには鍵の管理が複雑化してしまいます。

これに対して公開鍵暗号では、公開鍵と秘密鍵という 2 種類の鍵を使用し、本人が秘密鍵を所持し、他の不特定多数の通信相手に対して公開鍵を公開します。通信相手が公開鍵を使って暗号化することで、秘密鍵を持つ本人以外が復号化できなくなります。これによって、各ユーザは、1 組の鍵だけを管理すればよくなります。また、データの一方向ハッシュ値を自分の秘密鍵で暗号化したデジタル署名をデータに添付することで、通信相手は、公開鍵で復号化したデジタル署名とデータを照合し、送信元を認証できるようになります。

このような暗号技術を使って公衆網で受け渡すデータを暗号化することで、データの安全性が確保できるようになります。そして、ホスト間、ファイアウォール間、ネットワーク間でそれぞれ受け渡されるデータを暗号化することで、各データの安全性が確保できます。

VPN（Virtual Private Network）では、ネットワーク間のパケットをカプセル化してインターネット上に配送されます。これによって、プライベートアドレスで運用しているネットワークをインターネット経由で相互接続し、仮想的な専用線で接続されているのと同等のネットワーク環境が構築できます。ただし、本当の意味でのプライベートネットワークであるためには、通信経路における安全性の確保が不可欠です。

このような VPN がファイアウォールの機能とともに実装されている製品がありますが、この 2 つの技術の機能面には関連性はほとんどありません。したがって、LAN 間接続、公衆網接続、暗号化をそれぞれ適切に実現している製品を目的に合わせて選択すべきです。

16 侵入検知システム

ファイアウォールでは、Web サーバや FTP サーバなどのファイアウォール外に設置されているホストに対する攻撃は防ぐことができません。また、すでに内部に存在している侵入者を発見したり、ポートスキャンなどの回線資源を浪費する攻撃や未知の攻撃を防ぐこともできません。このような不正アクセスを検出するための製品として侵入検知システム（IDS: Intrusion Detection System）があります。ここでは、侵入検知システムの概要のみを示します。侵入検知システムについての詳細は、体系的にまとめられている Web ページ *http://www.cs.purdue.edu/coast/intrusion-detection* などを参考にしてください。

侵入検知システムで利用される方式は、ホストベース、マルチホストベース、ネットワークベースの 3 種類に分かれます。ホストベースの侵入検知システムは、単一のホストに関する情報に基づいて動作します。これに対して、マルチホストベースの侵入検知システムは、複数のホスト上で動作しているエージェントからの情報に基づき、ネットワークベースの侵入検知システムは、ネットワーク上で受け渡されている情報に基づいて動作します。

このような3種類の方式によって収集された情報から侵入を検知するモデルには、次の 2 種類があります。

- Anomaly detection model
- Misuse detection model

Anomaly detection model は、通常のユーザやシステムの活動とは異なる動きを捜査して侵入を検出するモデルです。この検出方法では、比較的少ない情報から侵入を検知できますが、そのルールを記述することが困難な作業となります。

これに対して、Misuse detection model は、既知の侵入手口を使った痕跡やシステムの問題点を悪用した活動を捜査して侵入を検出するモデルです。ただし、このモデルでは、過去の実績を利用しているため未知の攻撃には対処できません。

次に、いくつかの商用侵入検知システムを示します。

- The Kane Security Monitor
  The Kane Security Monitor は、Intrusion Detection（*http://www.intrusion.com/*）による Windows NT 用の侵入検知システムで、ネットワークベースでの情報源を利用しています。

- RealSecure
  RealSecure は、Internet Security systems（http://www.iss.net/）による侵入検知システムで、ネットワークベースでの情報源を利用しています。
- Stalker シリーズ
  このシリーズは、Haystack Labs（http://www.haystack.com）による侵入検知システムです。このシリーズの Stalker は、マルチホストベースでの情報源を利用しています。また、WebStalker では、Web サーバへの不正アクセスやコンテンツの書換えがチェックされます。
- NetRanger
  NetRanger は、1998 年に Cisco に吸収された WheelGroup Corporation（http://www. wheelgroup.com/）による侵入検知システムで、ネットワークベースでの情報源を利用しています。
- Session Wall-3
  Session Wall-3 は、AbirNet（http://www.abirnet.com）による侵入検知システムで、Windows 95 と Windows NT 上で動作する比較的安価な製品です。
- Network Fright Recorder（NFR）
  NFR は、Network Fright Recorder, Inc.（http://www.nfr.net/）による侵入検知システムで、ソースコードがフリーで配布され、BSD/OS、HP-UX、Linux などで動作します。この製品は、ネットワークベースの情報源が利用され、パケットの収集と解析が実施されます。また、Java 対応の Web ブラウザによって収集データを参照することもできます。

このほかにも、次のような商用の侵入検知システムがあります。

- SAIC による CMDS（Computer Misuse and Detection System）
- TTI による INTOUCH INSA（Network Security Agent）
- Axent による OMNIGUARD Intruder Alert
- Digital による POLYCENTER Security Intrusion Detector
- InfoStream による Watch Dog

現在、商用の侵入検知システムの成熟度はあまり高くありませんが、今後注目しておくべき分野だと思います。ただし、基本的には、ネットワーク利用状況をきちんと把握することのほうが重要だと思います。