加盟大学におけるネットワーク不正侵入の実状と対策

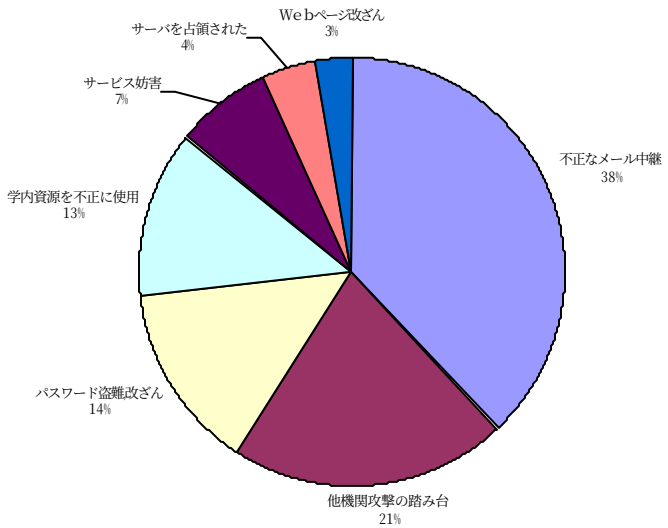
社団法人私立大学情報教育協会

調査依頼：平成１２年２月９日（回答期限：２月１８日）
調査対象：472 校（290 大学、182 短期大学）
回　　答：245 校(52%)（220 大学(76%)、25 短期大学(14%)）
回答内訳：不正侵入有り　71 校（64 大学､7 短期大学）・・・回答校の 3 割
　　〃　無し　174 校（156 大学､18 短期大学）

Ⅰ．被害の概要

回答のあった大学・短期大学の３割が不正侵入を受けている。内訳は、不正なメール中継（ＳＰＡＭメール）や他機関攻撃のための踏み台とされるなど、中継地点として悪用される場合が６割、パスワード盗難・改ざん、学内資源の不正使用、サービス妨害など、学内ネットワークを攻撃する場合が４割となっており、**外部攻撃等の中継地点となった場合、７割は被害を受けた機関等からの告知により発覚している。**また、不正侵入を受けた際の経路がある程度判明しているものは約３割、判らないものが５割近くとなっており、**侵入経路を隠滅する手法が用いられていることが伺える。**

不正侵入被害の内訳



※ 不正なメール中継
　大学の電子メールサーバを勝手に中継して、大量の宣伝・広告目的の文書や、デマなどの迷惑文書を発信する行為。受け取った側には、あたかも大学から送信されたように見える。

※ 他機関攻撃の踏み台
　大学のサーバに侵入し、それを足掛かりにして他機関のサーバを攻撃する行為。いくつものサーバを経由して攻撃する場合が多く、侵入者の追跡・特定が困難となる。

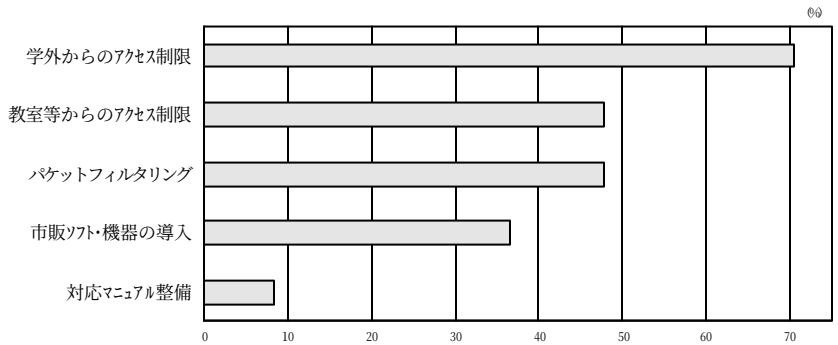
※ サービス妨害
　大量のデータを送り込んでネットワークの帯域を占有したり、プログラムやデータを消去・改ざんして機能不全に陥れるなどの行為。

※ サーバを占領された
　侵入したサーバを使用するために、設定などを操作・変更し、本来の機能を低下・消去してしまう事例がある。広義には学内資源の不正使用に含まれる。

Ⅱ．セキュリティー対策の実施状況と不正侵入の原因

１．　セキュリティー対策の実施状況を見ると、被害を受けた大学の８割は、何らかの対策を講じていながら侵入されている。対策の内訳としては、学外および教室等からのアクセス制限を合わせて実施している大学が５割となっており、その多くは、パケットフィルタリング、市販ソフト・機器による対策も取り入れ、セキュリティーの向上を図っていた。

不正侵入発生時のセキュリティー対策等実施率



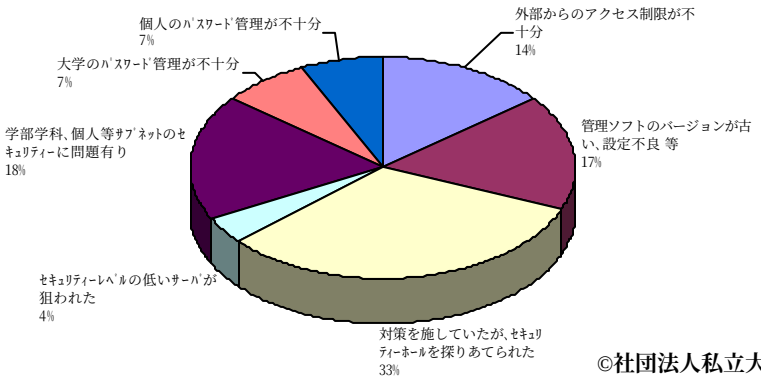
※ アクセス制限
　ルータやサーバにおいて、情報の種類などによって条件を設定し、ネットワークの利用を制限する方法。

※ パケットフィルタリング
　ルータなどの機能を強化し、発信者や発信元の情報などにより通過を制限する方法。

※ 市販ソフト･機器
ファイアウォールソフトウェアやネットワーク監視装置など、セキュリティー向上のための製品。

２．　原因と背景についての自己点検では、セキュリティー上の弱点（セキュリティーホール）などが原因となり侵入されている場合が最も多い。ネットワークサーバのセキュリティーホールは連日のように発見され、専門機関より警告・対処法が発せられているが、学内で即応的、継続的に対応するためには大きな労力が必要で、**セキュリティー対策への対応が追いついていないことが考えられる。**また、特に大規模大学では、学部学科や研究室などの支線ＬＡＮ（サブネットワーク）のセキュリティー対策が不十分であったり、個人のパスワード管理が不十分であることにより侵入を招くことも多く、**全学に統一的な管理基準を設けていないことが伺える。**

不正侵入の原因 背景



III. 再発防止のためにとられた対策

学内への攻撃が行われた場合、全て学内で解決している割合が６割程度となっているが、**外部攻撃の中継地点とされた場合には被害が広範囲に及ぶため、関係する学外機関との連携協力により解決する割合が多くなっている**。再発防止のための対策としては、**セキュリティーホールの解消、アクセス制限の強化、ファイアウォールの整備・機能強化**が図られている。学内への攻撃に対しては、**パスワード管理を強化**する対策が多くとられており、パスワード管理がそれまで不十分であったことが伺える。

（再発防止のためにとられた対策の例）

※ アクセス制限の強化
- 学外からの telnet(サーバの遠隔利用)、ftp(ファイル転送)を禁止した
- 発信元により学内ネットワークへの進入を拒否するプログラムを導入した
- パケット監視装置の導入を検討中

※ ファイアウォールの整備・機能強化
- 個々の教員が所有するサーバにはセキュリティー対策を施せないため、ファイアウォールを導入した
- 次回のネットワーク構成変更の際にファイアウォールを導入することにしている

※ セキュリティーホールの解消
- プログラムを再インストールした
- プログラムをバージョンアップした
- サーバの設定を見直した
- トラフィックの状況をネットワーク運用部会のメンバー全員が参照できるよう異状の発見方法を提供
- WWW サーバ、メールサーバのアウトソーシングを検討中

※ パスワード管理の強化
- 解読しにくいパスワードに変更した
- ワンタイムパスワード(認証の度にパスワードを変更する仕組み)を採用した
- 不要なユーザーアカウントを削除した

※ 利用基準の強化など
- 管理部署では学内ネットワークの末端まで把握できないため、利用基準の充実などにより管理強化を目指している
- 利用・運用に関するガイドラインの制定を準備中

Ⅳ．緊急対応のための留意点

中央省庁や一部の大学においてネットワークに不正侵入し、Ｗｅｂページの内容が改ざんされる事件が発生したことを受け、文部省からも、セキュリティー対策の参考情報が配布され、対策が掲げられているが、その中で、少なくとも以下のような対策を緊急に実施する必要があると思われる。

１．インターネットの出入口でアクセス制限を実施する

外部からの不正侵入を防ぐため、ルータ、ファイアウォールなど、学内ネットワークへの玄関となる場所で、例えば、未知の発信元からの進入を拒否するなど、外部からの利用を制限する。しかし、あまり制限を強固にすると※1、学外との自由な情報通信ができなくなり、教育研究上のネットワーク利用に支障を来たすことも考えられる。利用制限を実施する際には、条件・基準について利用者、管理者による意識統一を行い、学内における利用状況の変化に伴って随時見直すことができる体制を整備する必要がある。

２．各サーバにおける安全対策

(1)不要なプログラムの停止

サーバ、ルータ、ファイアウォールで動作するプログラムの稼動状況を安全検査用のプログラムを用いて点検する。不要なプログラムが稼動している場合には、速やかに停止する。

(2)セキュリティーホールの解消

使用しているプログラム等のバージョンを確認し、最新バージョンへの更新を行う。また、最新のバージョンであっても、セキュリティーホールが発見されているので、などセキュリティー関連機関等※2からの情報収集に努め、セキュリティーホ

※1 最低限度の利用範囲として、電子メールの受発信やＷｅｂページの利用などに限定することが考えられる
※2 JPCERT/CC(Japan Computer Emergency Response Team Coordination Center)など

ール解消プログラム等により早急に解決を図る。

(3)不要な通信ポートの閉鎖

サーバなどの情報の出入口である通信ポートを用いた侵入※3を防止するため、各サーバにある稼動中の通信ポートを点検し、使用していないポートを閉鎖する。

3．WWWサーバの安全性確認

WWWサーバは、各種サーバの中でも特に狙われやすい※4ため、前述の対策に加えて、プログラムの設定確認、データのバックアップ、利用記録の監査などを強化する。ＣＧＩについては、安全性が確認されているプログラム以外は使用を中止※5し、ファイルへのデータの書き換えを検出するプログラムや、通信経路において侵入を検出するプログラムを導入し、監視を強化することが望ましい。

4．利用記録の保存と監査、データのバックアップ

不正侵入の有無を監査し、発生した場合の手口、経路を特定するための資料として、常に利用記録（ログ）を保存しておく必要がある。また、データの改ざん、消去等の被害から早急に復旧するため、重要なデータを頻繁にバックアップすることも重要である。

5．ネットワークの運用管理方針を明確にする

学部・学科や研究室単位に管理するネットワークなどでセキュリティーの弱いサーバが不正侵入を受け、被害が全学的に拡大することがある。学内の全てのネットワークに上述の対策を反映し、安全性を確保するためには、利用できるサービスと制限、

※3 サーバなどの情報の出入口である通信ポートを検索し、侵入の手掛かりを探る手法(ポートスキャン)が横行している。

※4 Web ページの掲載など情報公開を目的としている WWW(World Wide Web)サーバは、利用者からの要求によりプログラムを実行する仕組みであるため、不正侵入の標的となりやすい。

※5 CGI(Common Gateway Interface)プログラムは、WWW サーバ上で検索機能の提供やアンケート受け付けなど、利用者が入力するデータを処理するため、悪用される危険性が高い。

各サーバにて実施する対応策、不正侵入発生時の連絡と対策などについて、全学統一の運用管理方針（セキュリティーポリシー）を明確化し、学内の共通理解を図ることが重要である。