不正アクセスの脅威とその対処事例について

掛下 哲郎　　松原 義継
理工学部 知能情報システム学科

インターネットの普及に伴ってコンピュータウイルスや不正アクセス等のコンピュータ犯罪が発生している。本稿では、著者らの研究室で発生した不正侵入事件を取り上げ、対処事例及び事件の教訓をまとめる。

1．まえがき

インターネットの普及は佐賀大学でも着実に進行しており、研究、教育、大学運営等の各方面に対して重要性を増している。インターネットは世界中のコンピュータネットワークを接続して構成された本質的にオープンなネットワークであり、利用者相互間の信頼関係を前提として運営されている。しかし、インターネットの大規模化に伴なって悪質な利用者によるコンピュータ犯罪や一般利用者による無意識の権利侵害なども多発しており、インターネット社会における主要な問題の一つになっている。

平成8年通産省告示第362号[1]（コンピュータ不正アクセス対策基準）では、「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」を不正アクセスと定義している。不正アクセスが行われると、コンピュータシステム上に保存されているデータが不正に流出したり破壊されたりする可能性があるため、情報セキュリティ上の問題が発生する。また、大量の電子メールを送付されたシステムが運用不能になる事例（電子メール爆撃）や、不正なプログラムを送り込まれた後、それを実行される事例（トロイの木馬）なども発生している。

上記で述べた被害を防止するために、通産省は前述の告示第362号及び平成7年告示第429号[2]（コンピュータウイルス対策基準）を定め、コンピュータ利用者、システム管理者等が実施すべき対策についてまとめている。また、JPCERT/CC（コンピュータ緊急対応センター）では、不正アクセスの発見や対策に関する技術情報を公開している[3]。

本稿では、平成9年3月末から4月始めにかけて著者らの研究室で発生した不正侵入事件を取り上げ、侵入の発見から原因究明及び対処に至る対応事例を紹介する。また、コンピュータ犯罪に関する情報源や一般的な対応法/予防法をまとめる。不正アクセスの対象となるのは主にサーバ系のシステムである。しかし、パソコンで電子メールを送受信している利用者もサーバ上に普段使用しないアカウントを持っているため、不正アクセスによる

---

[1] http://www.ipa.go.jp/SECURITY/ciadr/crack-gl.txt
[2] http://www.ipa.go.jp/SECURITY/antivirus/kijun429.txt
[3] http://www.jpcert.or.jp/

被害を受ける可能性がある点に注意されたい。

2．不正侵入内容と原因究明

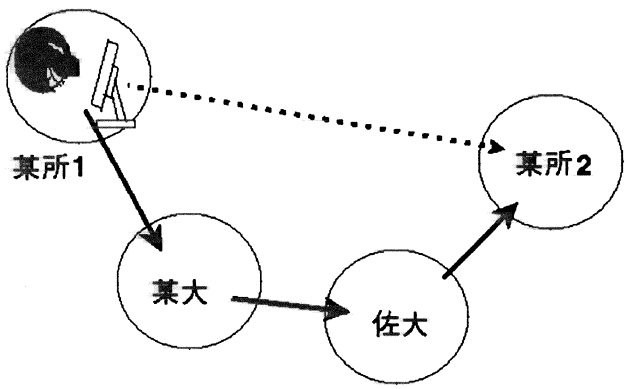
研究室の管理者が不正侵入に気付いたのは平成9年3月30日午後9時30分頃である。パスワードファイル /etc/passwd を編集しようとしたところ、管理者権限を持つ不正なアカウントを発見した。また、同時刻（21時8分～21時17分）に管理者アカウント（root）に対する未知ホストからのログインを確認した。そのため、研究室サーバの root パスワードを変更後、被害状況と侵入経路について調査を開始した。

システムを調査した結果、以下の被害が確認された。

- 管理者権限アカウント（パスワードなし）が不正に作成されていた。
- 上記アカウントに対する不正ログインが行われていた。
- root 及び学生アカウントに対する不正ログインが行われていた。
- 研究室 WWW ホームページが改ざんされていた。
- インターネット上の他サイトに対するログインが行われていた。いわゆる踏台として悪用されたと思われる。

研究室マシンに対する不正侵入は、インターネット上の複数サイト（国内某大学及び国外）から行われていた。このことから、侵入者グループ内でパスワード情報を流し、集中アタックをかけたものと推測される。

図 1 不正侵入の経路



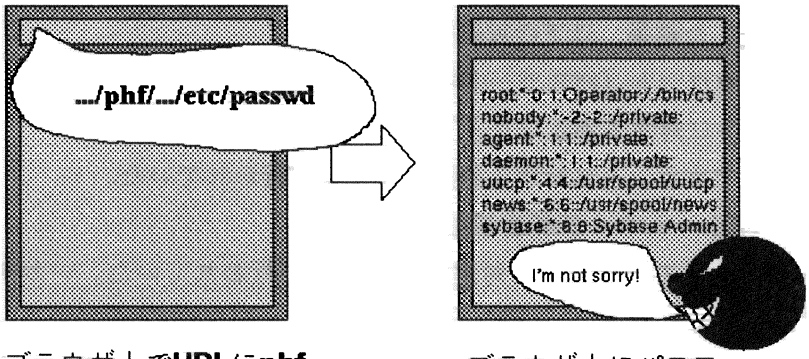
実線経由で破線経由の不正侵入を行う

また、侵入経路についての調査結果を以下に示す。

- 未知ホスト A の IP アドレスを nslookup コマンド及び traceroute コマンドで解釈することにより、ホスト A が所属するネットワーク（国内）を特定した。
- 上記ネットワークの管理者に調査を依頼した結果、不正アクセスを受けた時間帯に、ホスト A に対する不正アクセスが海外から行われていることが判明した。ホスト A に対する侵入経路は、フリーソフトウエアを動作させるために作成したアカウントである。アカウント名と同一のパスワードを付けていたことが侵入の原因と思われた。

- WWW ホームページに対するアクセスログ（access.log）中に /etc/passwd に対するアクセス要求を発見した。アクセス時刻は 3 月 30 日午前 8 時 38 分、アクセス元は米国（ホスト A に対する不正侵入先と同一）である。アクセス方法は、phf と呼ばれる CGI プログラムであった。phf は研究室サーバで使用していた WWW サーバプログラム httpd（NCSA 1.4.2）に付属しているサンプルプログラムである。

図 2　phf を用いたパスワードファイルの不正アクセス



ブラウザ上で**URL**に**phf**を記述して実行させると...

ブラウザ上にパスワードが現れる**!**

phf を用いると指定したファイルの内容を WWW ブラウザ上に表示できる。このようにして得たパスワードファイルは、不正侵入者の間で流通しているハッキングプログラムを用いて分析することにより、比較的短時間でパスワードを推測できることが知られている[4]。本件の侵入者も上記の手法を用いて不正アクセスしたものと思われる。

なお、JPCERT/CC では、平成 9 年 8 月 5 日付で上記 CGI プログラムを httpd のセキュリティホールとしてアナウンスし、不正侵入の発見法と対策を示している。

3．不正侵入への対応と反省点

2.で述べたように侵入経路が発見できたため、以下の対処を行った。

1. 研究室ホスト上における httpd をバージョンアップした。また、不正侵入の原因となった phf プログラムを削除した。
2. 研究室ホスト上の全アカウントに対するパスワード変更を行うことで、流出したパスワードファイルによる不正侵入を不可能にした。
3. 不正に作成されたアカウントの消去及び改ざんされた WWW ホームページを復旧した。これに先立って、改ざんされたファイルを保存して証拠保全を行った。
4. 知能情報システム学科内管理者グループ及び情報処理センターに対して被害報告を行った。今回は行っていないが、必要に応じて JPCERT/CC や IPA などの緊急対応組織に対する被害報告を行う必要がある。この報告を早期に行うことは、不正侵入によ

[4] パスワードの複雑さ（文字種の多さ、既存単語との不一致など）に依存する。

る被害の拡大を防止する上で極めて重要な意味を持つ。

5. 管理者グループでは、学科内のマシンにおける不正侵入をチェックした。その後、httpdの一斉バージョンアップ及びphfの削除を行い、新たな不正侵入に対処した。
6. 対処後は学外からのアクセスに注意を払ったが、不正アクセスは発見されなかった。

上記の対策は不正アクセスが発生した場合の一般的な対応とほぼ合致している。なお、侵入者が特定できた場合には、侵入に伴う損害賠償請求といった法的対応を取る必要も発生する。これについては、警察庁ネットワークセキュリティ相談室が対応しているが、今回はこの手続きを取ってはいない。

この種の犯罪に遭遇した場合、被害を受けたことに対して「恥ずかしい」と考えてしまうため、報告が遅れる場合がある。著者の場合も計算機の専門家として同じような気持ちを持った[5]。全てのセキュリティ情報を把握して対応することは現実的には難しいが、セキュリティ情報に対して比較的無関心だった点については反省する余地が多い。

4．不正アクセスの予防

コンピュータプログラムは人間が作成するため、誤り（バグ）を極めて少なくすることは可能であるが、ゼロにすることは事実上不可能である。セキュリティホールとなるのは、このようなプログラムのバグである。

インターネット上には様々な利用者が存在している。その中にはセキュリティホールを探して、不正アクセスを行うことを目的とする悪意の利用者も存在する。彼らがセキュリティホールを発見すると、その情報はインターネットを通じて瞬く間に全世界に流通する。山口は、不正アクセスにおける最近の傾向として以下を挙げている[1]。

1. パスワードファイルを入手しての不正なシステム侵入を第一目標としている。
2. システム侵入が成功すると、盗聴による管理者パスワードの不正入手、システム内の情報の盗み出し、ファイルの破壊などが行われる。
3. 侵入したシステムを踏台として他のシステムを攻撃する場合が多い。
4. 古いソフトウエアを使用しているシステムや管理者の目が届かないシステムに対する古典的手法による侵入（パスワードの推測など）がかなり多く発生している。
5. インターネット上で広く流通しているプログラム[6]が不正侵入に使われている。
6. システムの運用を妨げることを目的としたサービス不能攻撃が増加している（例：電子メールの大量送付、サーバに対する大量のパケット送信）。

これに対しては、以下に示す日常的なセキュリティ管理対策（詳しくは文献[2,3]等を参

---

[5] 今回のセキュリティホールは、管理者グループの間では周知のことだったらしい。

[6] セキュリティ対策を施すために開発されたもの（例：セキュリティホール検出プログラム）も多い。また、盗聴プログラムのように不正侵入用に開発されたものもある。これらを集めたWWWサイトも存在するが、インターネット上でのこのような情報発信の規制は難しい。

照すること）が必要である。

- パスワード検査プログラムを用いたパスワードの検査を行い、簡単すぎるパスワードを修正する。（例：アカウント名と同一のパスワード、英単語パスワード、数字だけのパスワード）
- ファイルのアクセス権を適切に設定し、他の利用者からのアクセスを防ぐ。
- セキュリティホールを避けるために、できるだけ新しいサーバプログラムを使用する。また、コンピュータのアクセスログを定期的に検査する。

また、日頃からセキュリティ情報に関心を持ち、最新情報の入手及び対策の実施を行う必要がある。セキュリティホールの情報源としては以下が挙げられる。IPA は主としてコンピュータウイルスに関する情報、JPCERT/CC は主として不正アクセスに関する情報を提供している。

情報処理事業振興協会(IPA) 「情報処理の促進に関する法律」に基づいて設立されており、通産省の政策実施機関の一つとして指定されている特別認可法人である。IPA ではセキュリティセンターを設置し以下の活動を行っている[7]。

- セキュリティ関係の各種情報（通産省告示、プレスリリースなど）を提供する。これについては、文献[4]も参照されたい。
- セキュリティ被害（コンピュータウイルス及び不正アクセス）の届け出を受け付け、統計情報及び対策を公開する。
- 暗号アルゴリズムの調査及び登録を行う。

JPCERT/CC(コンピュータ緊急対応センター) 主として技術的な問題に対応して活動している。当初はボランティアベースで運営されていたが、1996 年 10 月より通産省の財政的支援を受けて以下の活動を行っている。

- WWW サービスやメーリングリストを運営して、不正侵入に関する警告と対処に関する技術情報を提供する。
- 海外関連機関（米国 CERT/CC 等）との協調関係を構築する。
- セミナーの開催、勧告文書の作成・配布等を通じた啓蒙活動を行う。

本格的なセキュリティ対策としては、ファイアウォール[5]、暗号化[6]、バックアップの強化などがあり、機密保持を重視する企業では導入が進んでいる。しかし、大学では管理コストの高さや機密情報の少なさなども手伝って導入が遅れている場合が多い。しかし将来的には、この部分の体制強化も必要になろう。

5. むすび

インターネットはオープンなコンピュータネットワークである。これは、ユーザー間の

---

[7] http://www.ipa.go.jp/SECURITY/index-j.html

コミュニケーションを促進し、ネットワークコミュニティが発展するための基礎となっている。しかし一方では不正アクセスを生む土壌にもなっている。佐賀大学でもインターネット利用が急速に普及している現在、不正アクセスに対する正しい知識を持つことは重要である。

本稿では著者らが経験した不正侵入の事例を通じて、不正アクセスが発生した場合の対策をまとめた。また、不正アクセスを防止するための対策も示している。いったん不正アクセスが発生すると、これに対応するための労力は非常に大きなものになる。また、ネットワークに接続されている他のコンピュータにも様々な影響を及ぼす。従って、インターネットを快適に利用するためには、常日頃からの防止対策が重要である。これには、管理者だけでなく、一般利用者の協力も不可欠なのである。

最後になりましたが、本稿を執筆するに当たって各種の情報提供を頂いた方々に感謝致します。

参考文献

[1] 山口、インターネットにおけるセキュリティ問題と緊急対応組織、情報処理、Vol. 38、No. 10、pp.863－869、1997.

[2] 佐々木他著、インターネットセキュリティ－基礎と対策技術－、オーム社、1997.

[3] S. Garfinkel, G. Spafford 著、山口監訳、UNIX セキュリティ、アスキー、1993.

[4] 中村、コンピュータセキュリティ対策－コンピュータウイルスを中心として－、情報処理、Vol. 38、No. 5、pp.415－420、1997.

[5] W. R. Cheswick, S. M.Bellovin 著、田和、鎌形訳、川副監訳、ファイアウォール、ソフトバンク、1995.

[6] B. Shneier 著、道下訳、力武監訳、E-Mail セキュリティ、オーム社、1995.