Mem. Fac. Sci. Eng. Shimane Univ.
Series A
34, pp. 105-114 (2000)

ネットワークシステムの危険性について：島根大学情報ネットワーク下位サイトにおける実例

大野　修一
数理・情報システム学科　総合理工学部　島根大学

Risks on the Internet: an incident report from a lower site of Shimane University's information network

Shuichi OHNO
Department of Mathematics and Computer Science, Interdisciplinary Faculty of Science and Engineering
Shimane University

Abstract

Thanks to the development of communication technology and inexpensive Internet connections, the number of users of Internet has been increasing exponentially. The Internet is now an indispensable and elementary tool for many people. A lot of commercial and non-commercial useful services can be found out there. However, it should be noticed that the Internet is inherently insecure. Actually, the number of incident on the Internet has been also increasing. To warn the risks of using the Internet, this paper reports some incident happened at a lower site of Shimane University's information network. Some lesson can be learned from the incident. The opinion on network system administration is also provided.

概　　要

ネットワークの整備が進み，インターネット上で，電子メールのような必要不可欠なサービスが展開され，その利用者が爆発的に増加している．一方，インターネット利用者の増加に伴い，インターネットを悪用したシステムへの不正アクセス・不正利用も増加している．本稿では，ネットワークシステムの危険性を喚起するため，著者が遭遇したネットワークシステムへの不正アクセス・不正利用のいくつかの事例を紹介する．また，その経験から得られた教訓を述べるとともに，ネットワークシステム管理経験者として，ネットワークシステム管理に関する意見を述べる．

1. はじめに

ネットワークの整備が進み，インターネット上でさまざまなサービスが展開され，その利用者が爆発的に増加している．大学においても，電子メールは必要不可欠のツールとなり，多くの大学が，World Wide Web（以下 Web）サーバを運用し，大学案内，講義案内，授業内容，受験情報，研究成果，教育成果などを公開している．また，学内イントラネットを

構築することにより，事務を効率的に行っている例もある．

一方，インターネット利用者の増加に伴い，インターネットを悪用したシステムへの不正アクセス・不正利用も増加している[1]．インターネットに接続した全てのシステムは，システムに不正アクセスし不正利用を試みる者（以下クラッカー）に狙われ，攻撃される危険性を伴う．攻撃が成功すると，情報の漏洩やシステムの破壊などの直接的被害を被る．また，クラッカーは，攻撃に成功したシステムを犯罪に使用したり，そのシステムを踏台に他のシステムへの攻撃を行う．システムが他者へ被害を与えた場合，システムをインターネットに接続した者が加害者となり，その責任を問われる可能性がある．

日本の官公庁や大学の多くはセキュリティ意識が乏しく，クラッカーの格好の攻撃の対象になっていると言われている．実際，多くの官公庁のシステムが不正アクセス・不正利用され，その被害が報告されている．システムの危険性が喚起されていたにもかかわらず，このような事件が発生するのは，システムの運用者が，危険性を認識せず，十分なセキュリティ対策を施さないまま，システムを運用していたからだと思われる．

セキュリティ対策は，セキュリティ対策の必要性を認識することから始まる．インターネットに接続されているシステムが危険に晒されていることを，その利用者は，自覚しなければならない．著者は，島根大学情報ネットワークに接続している下位サイトのネットワークシステムの管理を行っていた．本稿では，ネットワークシステムの危険性を喚起するため，著者が遭遇したネットワークシステムへの不正アクセス・不正利用のいくつかの事例を紹介する．また，その経験から得られた教訓を述べるとともに，ネットワークシステム管理経験者として，ネットワークシステム管理に関する意見を述べる．本稿により，少しでも多くの人が，インターネットの脅威を自覚し，セキュリティ対策およびネットワークシステム管理の重要性について認識していただければ，幸いである．

なお，本稿では，著者が実際に関与した問題のみを述べる．また，著者は，教官業務の一環として，ネットワークシステム管理を担当していただけであり，ネットワークシステムのセキュリティ対策の専門家ではない．問題事例および具体的なセキュリティ対策については，ネットワーク上の資料あるいは文献を参照されたい．

2. インターネットの脅威

本稿では，システムを，あるハードウエアとそのハードウエア上で稼働するソフトウエアの複合体と定義し，ネットワークシステムを，ネットワークとそのネットワークに接続したシステムの集合体とする．

本章では，まず，インターネットにおけるネットワークサービスの仕組みと，インターネットを悪用しようとするクラッカーについて簡単に述べる．そして，著者が実際に経験したネットワークシステムへの不正アクセス・不正利用のいくつかを紹介する．

2.1 ネットワークサービスの仕組み[2]

インターネットは，複数のネットワークを相互接続し，ネットワークに属するシステム間

において透過的なアクセスが可能なネットワークの集合体である．

インターネットにシステム（あるいはマシン）を接続するとき，そのシステムのためのIPアドレスが必要となる．IPアドレスは，インターネット上で一意であり，IPアドレスからインターネット上のシステムを特定することができる．（ただし，プライベートLANは除く．）

インターネット上のネットワークサービスの多くは，クライアント/サーバ型で実現されている．サービスを提供するプログラム（あるいはマシン）をサーバ（サーバマシン），サービスを受けるプログラム（あるいはマシン）をクライアント（クライアントマシン）という．以下，あるマシン上で稼働するサービスプログラムをサーバ，サーバが稼働しているマシンをサーバマシンと定義する．

サーバの提供するネットワークサービスは，ポート番号と呼ばれる数値により分類されている．例えば，電子メールサーバのためのポート番号は25であり，Webサーバのためのポート番号は（通常）80である．クライアントはIPアドレスとポート番号を指定しサーバへ接続要求を行い，サーバはクライアントからの接続要求に応じてサービスを開始する．

2.2 クラッカー

インターネットは，透過的にアクセス可能であり，サーバへは，IPアドレスとポート番号を指定することでアクセスすることができる．これは，不正を企むクラッカーにとっても，同様である．

クラッカーは，サーバへアクセスし，その設定不備やセキュリティホールを攻撃し，サーバが稼働しているシステムへ被害を及ぼす．使用しているシステムに被害が限定できるときは，その被害を自己責任として済ますことができるかもしれない．しかし，攻撃が成功し，そのシステムを拠点にインターネット上の他のシステムへの不正アクセス・不正利用が行われた場合，不正アクセス・不正利用の発信元は，拠点とされたシステムとなる可能性がある．そして，他のシステムへ被害を与えてしまった場合，不正アクセス・不正利用の発信元となっているシステムをインターネットに接続した者が，その責任を問われる可能性がある．

セキュリティの低いシステムを攻撃し，そのシステムの制御を奪うことができた場合，そのシステムから，よりセキュリティの高いシステムへの攻撃が可能である．よって，インターネットの末端にあるシステムや，重要な役割を担っていないシステムは狙われないと考えることはできない．また，プリンタサーバのように，一見重要でないと思われるサーバにも注意が必要である．プリンタサーバを攻撃することで，プリンタサーバを運用しているシステムの制御を奪えることがある．さらに，サーバを意図的に運用していないシステムであっても，安全とは言えない．UNIX系のシステムのように，デフォルトでさまざまなサーバが動作してしまうシステムも存在するし[3][4]，何者かがサーバをインストールしている場合もある．

2.3 メールサーバへの攻撃

不特定多数に送る勧誘電子メールなどをスパムメールと呼ぶ．スパムメールは，受信者にとって不必要で迷惑な電子メールであり，スパムメールを送信することは，モラルに反する行為とされている．しかし，インターネットの商用利用の拡大に伴い，広告等のスパムメールは増加している．

ある配送元からスパムメールが送られた場合，その配送元には，このようなスパムメールを送らないで欲しいという抗議の電子メールや，宛先不備のため戻ってきた電子メールが大量に届く．抗議の電子メールを受けとった配送元の管理者は，スパムメールを送った者のアカウントを取り消すなど，何らかの策を講じるであろう．そこで，スパムメールを送ろうとする者（スパマー）は，電子メールを自由に送信できる環境を手に入れようとする．

配送元から配送先への電子メールの配送は，複数のメールサーバと呼ばれる電子メール配送のためのプログラムによるバケツリレー式の中継により実現されている．電子メール中継のアクセス制御を行っていない，あるいは十分なアクセス制御を行っていないメールサーバにアクセスすると，そのメールサーバを配送元とし，電子メールを送付することが可能である．スパマーは，このようなメールサーバを探し，そこから大量のスパムメールを送付する[5]．

著者らが管理していたメールサーバでも，1998年7月および1999年2月にスパムメールの配送元となり，インターネットのユーザに被害を与えてしまった．一度目のスパムメール送信は，電子メール中継のアクセス制御を行っていないことが原因であった．そこで，サーバプログラムをヴァージョンアップし，アクセス制御を行うよう設定し対処した．二度目のスパムメール送信は，電子メール配送のルールに違反する細工を加えることで，前回講じたアクセス制御を無力化するものであったが，アクセス制御を強化することで対応可能であった．

インターネット上には，スパムメールの配送元となったメールサーバのデータベース[6][7]があり，データベースに登録されているメールサーバからの電子メールの中継および受信を拒否するメールサーバを構築することが可能となっている．

著者らが管理していたメールサーバの二度目のスパムメール送信に対しても，データベースを管理している組織のひとつのORBS（Open Relay Behaviour-modification System）[6]から，つぎの内容の電子メールが届いた．「あなたのサイトのメールサーバよりスパムメールが送信されているようです．あなたのサイトのメールサーバをデータベースに登録しました．あなたのサイトのメールサーバが，ORBSの不正中継チェックにパスすれば，データベースから登録を削除します．」

2.4 Webサーバへの攻撃

一般に，多くの機能を提供するWebサーバのようなサーバは，クラッカーにとっても都合の良い機能が装備されているため，攻撃の対象になりやすい[8]．

Webサーバにおいて，その設定以外，特に注意しなければならないのは，アクセスカウンタ，掲示版，アンケート調査などのサービスを提供するために利用されているCGI[1]と

SSI[2]である．CGIプログラムは，比較的簡単に作成することができる．また，インターネット上から，さまざまなCGIプログラムを入手し利用することができる．しかし，セキュリティ上の欠陥があるCGIプログラムが，Webサーバで実行可能であると，悪意ある者にシステムを不正利用される可能性がある．

よく知られたセキュリティ上の欠点があるCGIプログラムにphf（version 1）がある[8]．phfが実行可能であると，Webクライアントにシステムのユーザのパスワードを取得される可能性がある．一般に，Perlなどの汎用言語によるCGIプログラムは，セキュリティ上の危険性が高いと言われている[9][10]．

著者らが管理していたWebサーバは，サーチエンジンに登録されないよう設定をしており，比較的アクセス数の少ないWebサーバだと言える．しかし，このようなWebサーバに対しても，1999年1年間に，数回のphfによるパスワード搾取の試みがなされている．

2.5 ポートスキャン

システムのポートにアクセスし，そのシステムでどのようなサーバが動作しているのか調べることをポートスキャンと呼ぶ．また，ポートスキャンのためのプログラムをポートスキャナーと呼ぶ．

ポートスキャナーには，管理者が気付かず動作させているサーバや，既知のバグのあるサーバの動作など，システムの弱点を検出するセキュリティ対策用のもの（例えば，[11]，[12]，[13]）と，悪意ある攻撃まで行うクラック用のものがある．ただし，セキュリティツールとして開発されたポートスキャナーでも，クラックに使用できる．また，セキュリティツールといえども，システムをダウンさせる可能性があるので，十分注意して使用しなければならない．

ポートスキャナーは，インターネット上から入手できる．また，ポートスキャナーを用いると，初心者であっても容易にポートスキャンできる．技術力のない者であっても攻撃者になりえることから，ポートスキャナーによるものと思われる不正アクセスも多発している[14]．オペレーティングシステムがUNIX系の場合，システムの利用者の情報を得ることができるfinger，ポートへのアクセスに使用されるtelnet，ファイル転送のためのftpなどによるアクセスは，デフォルトの設定では十分にログに残されない場合が多い．著者らのサイトでは，電子メール中継問題発生後，セキュリティを高めるため，ポートへのアクセス制御を行い，できるだけ多くのログを取るシステムへ変更した[4]．

ログによると，2台のサーバマシンにおいて，1999年1年間に，約100回の不正アクセスがあった．そのほとんどは，ミスや悪戯によるものと思われるが，明らかに不正利用を試みるためと思われるものもあった．

---

[1] Common Gateway Interface. Webサーバがバックエンドプログラムとの間で情報の送受信に用いいるインターフェース．クライアントのアクセスにより，動的に作成されるページに利用される．

[2] Server-Side Includes. CGIはドキュメントそのものが動的ページであるのに対し，SSIはドキュメントの一部が動的である．

2.6 パスワード漏洩

ネットワーク上の通信は容易に盗聴できるため，安全でない方法で重要な情報を送信することは危険である．例えば，ネットワーク経由で暗号化通信方式を用いずパスワードを送信する場合，パスワードはそのままネットワーク上に流れる．そして，ネットワーク上に流れるパスワードを盗聴することにより，パスワードを盗むことができる．

パスワードが盗まれた場合，盗まれたパスワードの所有者だけにその被害が限定されるわけではない．不正にパスワードを取得した者が，そのパスワードを用いて「正規に」システムへログインし，システムの弱点を探し，システムを悪用する可能性がある．この場合，システムの他のユーザはおろか，インターネット上の他のシステムへ被害が及ぶ可能性がある．

盗聴の他に，パスワードを不正に入手するための古典的方法に，辞書を援用したパスワードへの総当たり攻撃がある．著者の属するサイトで，インターネット上で入手できるパスワード破りプログラムで，全ユーザのパスワードを検査したところ，数パーセントのパスワードを破ることができた．

3. システムを守るために

前章で紹介した事例より，以下に挙げる教訓を得ることができた．

1. インターネットに接続すると，どのサイトのどのシステムも狙われる．
2. よく知られた弱点が狙われる．
3. セキュリティ関連情報に注意する．
4. ソフトウエアは，最新安定版を使用する．
5. 運用するサーバと，そのサーバのクライアントを明確にし，アクセス制御を行う．
6. サーバのログをとり，ログを毎日検査する．

どれも，平凡でありふれた事であり，セキュリティ対策の基本である．しかし，正直なところ，実際に被害を受けるまで，管理しているネットワークシステムが狙われるとは思わず，基本的なセキュリテイ対策さえ行なっていなかった．

ネットワークセキュリティの専門家であっても，高度な技術を持つクラッカーの攻撃を完全に防げるわけではない．しかし，攻撃のほとんどは，よく知られたバグや設定の不備を突くものであり，上記3, 4, 5, 6を実行するだけで，ネットワークシステムの安全性はかなり向上すると言える．

3.1 不正アクセス

平成8年通商産業省告示第362号[15]では，「不正アクセス」を，「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」と定義している．また，平成11年8月6日可決・成立し，同8月13日に公布された，「不正アクセス行為の禁止等に関する法律」[16]では，「不正アクセス行為」を「アクセス制御機能を有する特定電子計算機等に電気通信回線を通じて他人の識別符号等を

入力して作動させ，当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為」と定義している[17].

これらの定義に従えば，2.3節で紹介したスパムメールの第一のケースは，モラルに反する行為とは言えるが，スパマーは禁止されていない中継機能を利用しただけであり，スパマーの行為を「不正アクセス行為」と断言することはできない．しかし，第二のケースおよび2.5節で述べたアクセスは，ルール違反あるいは明示的に禁止されているアクセスであるので，明らかに「不正アクセス行為」である．この例からわかるように，「不正アクセス行為」を定義するためには，アクセスを許可するクライアントと不許可にするクライアントを，ただ単に想定するだけではなく，設定において明示しておかなければならない．

3.2 全許可モデルと全禁止モデル

アクセスの許可・禁止の方針を，アクセスポリシーという．ネットワークシステムへのアクセスに限らず，あるサービスの利用の許可と不許可の方針を単純化すると，2つのモデルに分けられる．ひとつは，全てを原則許可とし，不許可にするものを明示するモデル（全許可モデル）であり，もう一方は，全てを原則禁止とし，許可するものを明示するモデル（全禁止モデル）である．

主に研究者が利用していた頃のインターネットでは，全許可が基本的な考え方であった．そのため，ほとんどのサーバのデフォルトの設定は，誰でも自由に利用できる全許可モデルであった．しかし，インターネットにおけるセキュリティ上の問題が増加するに伴い，現在では，全禁止モデルが採用される場合が多い．例えば，古くから，また，現在でも広く使用されている電子メール配送プログラム sendmail[18]のデフォルト設定は，ヴァージョン8.8以前は全許可モデルであったが，ヴァージョン8.9以降は全禁止モデルとなっている．全許可モデルは利便性のための自由を重視し，全禁止モデルは安全性のための規制を重視していると言えるかもしれない．そのため，インターネット利用の自由を重視したい人は，前者を採用したい人が多いであろう．著者も，クライアントのモラルへの信頼を前提にした牧歌的時代のインターネットの考え方に，郷愁を覚える．しかし，セキュリティの観点からは，全禁止モデルが明らかに優れている．なお，全許可モデルであっても，許可できないものは禁止する点に注意していただきたい．前節で述べたように，何も禁止しないことは，誰でもアクセスしてよいと宣言していることになる．従って，サーバプログラムのデフォルト設定が，全許可モデルであっても，しかるべきアクセス制御を行わなければならない．

3.3 ポリシーの明確化

セキュリティ対策の基本は，ルールを正式に表明すること（ポリシーの明確化）であると言われている．つまり，守るべき資産とそのセキュリティ上の問題点を把握した上で，どのようなサービスを，どのようなクライアントへ，どのように提供するのか，また，問題発生を防ぐためにどのような体制で運用するのか，問題発生時にどのように対応するのか等を明確にすることである．3.1節で述べたように，アクセスポリシーが明確でなければ，システムへの不正アクセスおよびシステムの不正利用の定義さえできない．（ポリシーの立案作成

に関しては，例えば，RFC[3] 2196（サイトセキュリティハンドブック）が参考になる．RFC 2196の日本語訳は，情報処理振興事業協会のWebページ[19]等より入手可能.）

サイトのネットワークシステムは，ネットワークの基本要素からなるネットワーク基本部と，ネットワーク基本部に接続する複数のシステムから成り立つ．多くの場合，前者は，サイトの共有資源であるが，後者は，サイトの共有資源とは限らない．

サイトの共有資源の運用管理のポリシー（サイトポリシー）は，サイトのしかるべき意思決定機関で作成される．意思決定機関は，必要に応じて，運用管理作業を行う実務者を任命し，共有資源を集中管理する．そして，共有資源であるネットワークシステムの管理の実務作業を行う者を，ネットワークシステム管理者と呼ぶ．

ネットワークシステム管理者は，作成されたサイトポリシーに従い，共有資源の管理作業を行う．ネットワークシステム管理者は，意思決定機関の依頼により，ポリシーの作成に関与することはあっても，意思決定機関の委嘱なしに，ネットワークシステム管理者のみでサイトポリシーを作成することはない．例えば，サイトの運用管理を外部業者に委託する場合，業者は指示された運用管理以外のことは行わない（行えない）．つまり，共有資源の運用管理の責任者である意思決定機関自身が，セキュリティ上の問題点を把握し，しかるべきサイトポリシーを作成しなければならない．よって，意思決定機関が，ネットワークシステムの安全性に対する決定的な役割を担っていると言える．

ネットワークシステム管理者に過大な期待を抱くべきではない．例えば，緊急時に意思決定機関の承認なしに問題の対処を行えると規定されていなければ，ネットワークシステム管理者は，問題への対策手段を持っていたとしても，それを行使することはできない．

言うまでもないことであるが，サイトポリシーは実現可能でなければならない．また，意思決定機関は，サイトポリシーの実現のため，必要となる予算と人員を確保しなければならない．

ネットワーク基本部に接続する非共有資源であるシステムの運用管理は，サイトに委託されない限り，接続した本人あるいは組織が行うものである．例えば，島根大学情報ネットワークにおいて，島根大学情報ネットワークにシステムを接続した者が，島根大学情報ネットワーク利用規則[21]と島根大学情報ネットワーク利用心得[22]を遵守していたとしても，島根大学情報ネットワークの管理機関である島根大学情報処理センターが，そのシステムのセキュリティ対策を行うわけではない．

運用管理をしない一般ユーザであっても，規定されているポリシーに従うだけでなく，システムを使用するに伴う危険性を把握した上で，システムを使用すべきであろう．ユーザのセキュリティ対策については，RFC 2504（ユーザーズセキュリティハンドブック）を一読されることを薦める．（日本語訳は，[19]等より入手可能.）

---

[3] Request For Comments. IETF (Internet Engineereing Task Force．インターネット上で開発される新しい技術の標準化を促進するため設立されたコンソーシアム.）が発表するドキュメント.

4. ネットワークシステム管理者の現実

数年前であれば，ネットワークシステム管理者は，一度システムを設定すると，ほとんど何もしなくても問題は発生しなかった．しかし，現在は，不正アクセス・不正利用等の問題に対処しなければならないため，ネットワークシステム管理は非常に困難な仕事になっている．

ネットワークシステム管理者は，ネットワークシステム管理のため，ネットワークシステムの仕組みや管理に関する基礎的知識（例えば，[2]，[3]，[4]）を，獲得しておかなければならない．電子メール配送プログラム sendmail の設定を行うため，500ページ以上もある sendmail の解説本[20]を読まなければならない事もある．また，巧妙な不正アクセスに対応しようとすると，ネットワークシステムの構成技術の細部まで調べなければならないこともある．

ネットワークシステム管理者は，その業務内容をユーザに誤解されることにより，不必要な時間を割かなければならないことがある．例えば，ユーザによる要望や質問である．そもそも，ネットワークシステム管理者は，個別のユーザの要望に応えることはできない．要望があれば，サイトの意思決定機関に申し立てるべきである．また，ネットワークシステム管理者は，規定されていない限り，個別のユーザからのシステムやアプリケーションプログラムへの質問に答える義務はない．

ネットワークシステム管理者は，セキュリティ上の対策のため，あるサービスの停止や，以前より不便なサービスへの変更を提案することがある．また，ネットワークシステム管理者は，ネットワークシステムに問題が発生しなければ，ユーザにその存在を意識されることはほとんどない．そのため，ネットワークシステム管理者は，ネットワークシステムに問題が発生しないよう努力しているにもかかわらず，サービス停止あるいは変更による非難を受けることはあっても，その仕事に対する正当な評価を期待することは困難である．

5. おわりに

島根大学情報ネットワークに接続している下位サイトのネットワークシステム管理者として経験した不正アクセス・不正利用の試みのいくつかを紹介するとともに，ネットワークシステム管理経験者としての意見を述べた．

紹介したサーバに対する不正アクセス・不正利用の以外にも，システムを使用不可能にする攻撃やコンピュータウイルスなど数多くの問題がある．また，直接の当事者でないので述べなかったが，当サイト以外の島根大学情報ネットワークにおいても，深刻な問題が発生している．島根大学情報ネットワークシステム全体として，セキュリティに関する情報の共有化，ファイヤウォール[23]の構築などのセキュリティ対策が必要であると思われる．

参 考 文 献

[1] コンピュータ緊急対応センター（JPCERT/CC），
http://www.jpcert.or.jp/

[2] TCP/IP ネットワーク管理第2版，Craig Hunt 著，安藤 進訳，村井 純監訳，オライリー・ジャパン，1999

[3] UNIX システム管理改訂版，AEleen Frisch 著，谷川哲司監訳，黒岩真吾，株式会社ユニテック共訳，オライリー・ジャパン，1998

[4] UNIX&インターネットセキュリティ（第2版），Simson Garfinkel, Gene Spafford 著，山口英監訳，谷口 功訳，オライリージャパン，1998

[5] JPCERT/CC，技術メモ—電子メール配送プログラムの不正利用（予期しない中継）—，JPCERT-E-TEC-97-0001-03，
http://www.jpcert.or.jp/ed/199x/97-0001-02.txt

[6] Open Relay Behaviour-modification System，
http://www.orbs.org/

[7] The Mail Abuse Prevention System，
http://maps.vix.com/rbl/

[8] JPCERT/CC，緊急報告—phf CGI プログラムを悪用したアタック，JPCERT-E-INF-97-0003-01，
http://www.jpcert.or.jp/at/199x/97-0003-01.txt

[9] World Wide Web Consortium Security Resources，
http://www.w3.org/Security/

[10] Web セキュリティ&コマース，Simson Garfinkel, Gene Spafford 著，安藤 進訳，オライリー・ジャパン，1998

[11] SAINT, http://www.wwdsi.com/saint/

[12] Nessus, http://www.nessus.org/

[13] Nmap, http://www.insecure.org/nmap/

[14] JPCERT/CC，緊急報告—ポートスキャンを用いた不正アクセス，JPCERT-E-INF-98-0004-01，
http://www.jpcert.or.jp/at/199x/98-0004-01.txt

[15] 通商産業省報道発表資料，コンピュータ不正アクセス対策基準について，
http://www.miti.go.jp/past/c60806a2.html

[16] 警察庁，不正アクセス行為の禁止等に関する法律，
http://www.npa.go.jp/hightech/fusei-acl/houann.htm

[17] 警察庁，不正アクセス行為の禁止等に関する法律の概要
http://www.npa.go.jp/hightech/fusei-acl/gaiyou.htm

[18] The Sendmail Consortium，
http://www.sendmail.org/

[19] 情報処理振興事業協会（IPA）セキュリティセンター，
http://www.ipa.go.jp/security/index.html

[20] sendmail システム管理，Bryan Costales, Eric allman 共著，中村素典監訳，鈴木克彦訳，1997年9月，オライリージャパン

[21] 島根大学情報処理センター，島根大学情報ネットワーク利用規則，
http://www.ipc.shimane-u.ac.jp/ipc/kisoku/nkisoku.html

[22] 島根大学情報処理センター，島根大学情報ネットワーク利用心得，
http://www.ipc.shimane-u.ac.jp/ipc/nw-setsuzoku.html

[23] ファイアウォール構築，D. Brent Chapman, Elizabeth D. Zwicky 共著，歌代和正監訳，鈴木克彦訳，オライリージャパン