解説

ネットワークサーバのセキュリティ確保のための方策

名古屋大学大型計算機センター
E-mail:hasegawa@sagita.cc.nagoya-u.ac.jp
長谷川 明生

ネットワークサーバのセキュリティ確保に役立つ情報は，WEB等で多数公開されている．また，書籍も多数出版されるようになった．しかし，内容が英文であったり，断片的であったり，逆に詳細すぎて，手軽に参照できるものは少ないのが実情である．本稿では，ネットワークサーバのセキュリティ確保に関する基本的な事項を，運用に即して解説する．

最近のセキュリティ情勢

インターネットと通信でき，何らかのサービスを提供するコンピュータ機器をネットワークサーバと呼ぶことにすると，ネットワークにつながっている大半の機器がネットワークサーバとして機能していることになる．その中でも，ネームサーバやメールサーバは，他のサーバがインターネットの機能を利用する上で欠かせない基幹的役割を持っている．この種のサーバのトラブルは，ネットワークサービスの継続に不可欠な機能を失うことになる．また，近年，あらゆる分野で情報提供の重要な手段として利用されているWEBサーバのダウンや，サーバ上のコンテンツの外部からの改ざんは，閲覧者の期待するサービスの阻害にとどまらず，コンテンツを提供している組織の信用にかかわる問題となる．しかし，ネットワークやネットワークサーバの持つ役割の重要性にもかかわらず，その危機管理対策やセキュリティ対策の現状は必ずしも十分とはいえず，各種のセキュリティ情報WEBサイトやCERT等の警告にもかかわらず，有名企業や組織のWEB改ざん被害は後を絶たない．さらにADSLをはじめとするブロードバンド技術の急速な普及が，SOHOサーバの被害だけでなく，SOHOサーバを踏み台とした攻撃を急増させている．CodeRedやNimdaの被害状況を見るまでもなく，企業等の組織のサーバ防衛だけでなく，SOHOサーバの防衛なくしては，e-Japan計画は絵に描いた餅にすぎない．

本稿では，ネットワークサーバのセキュリティに関して，リスクの分析，サーバ導入の考え方，セキュリティ確保の方策およびセキュリティ問題が発生した場合の対応について，技術的問題を中心に考察する．ネットワークサーバの問題を取り上げているが，インターネットと組織内ネットワークの間には，ファイアウォールのようなアクセス制限機構とIDSのような侵入検知機能が存在することを前提とする．

ネットワークサーバのセキュリティリスク

セキュリティ問題とは，ネットワークやそれに接続されたホストのCIAすなわち情報資源の機密性（Confidentiality），完全性（Integrity）および可用性（Availability）を侵害するような問題をいう．機密性とは情報資源へのアクセス権限の管理の問題であり，完全性とは提供される情報資源の内容をいかに正しく保つかという問題で，可用性とは，情報資源を必要とする人に必要とされる時に届けられるかどうかという問題である．これらを侵害する要因をセキュリティリスクと呼ぶ．ここではセキュリティリスクを，おおまかに物理的問題，技術的問題と人的組織的問題に分類して考える．

■物理的問題

ネットワーク機器やサーバ機器のハードウェアの故障は避けられないので，可用性を向上するための方策は必要であるが，ここで問題とするのは機器の設置環境の問題がセキュリティに与えるリスクである．大学の研究室等でのサーバ機器設置環境は，多くの場合，問題がある．ネットワークケーブルがスパゲッティ状態のことがままあり，ケーブル接続先の間違いや足で引っ掛けて接触不良を起こすという例が多数ある．このようなトラブルは，可用性を阻害する要因である．このような環境は，また，だれでもが機器の電源を切断できたり，リセット操作が可能だったりもする．悪意のある人間がコンソールに触れると，実に簡単にシステムを破壊したり，ソフトウェアを改ざんしたりすることが可能である．これは極端な例であるが，ある施設の開所式典デモの最中にメインフレームのシステムダウンが発生した．原因は，招待された見学者がコンソールのSTOPボタンを押したことであった．ネットワークサーバの設置にあたっては，配線等の管理は

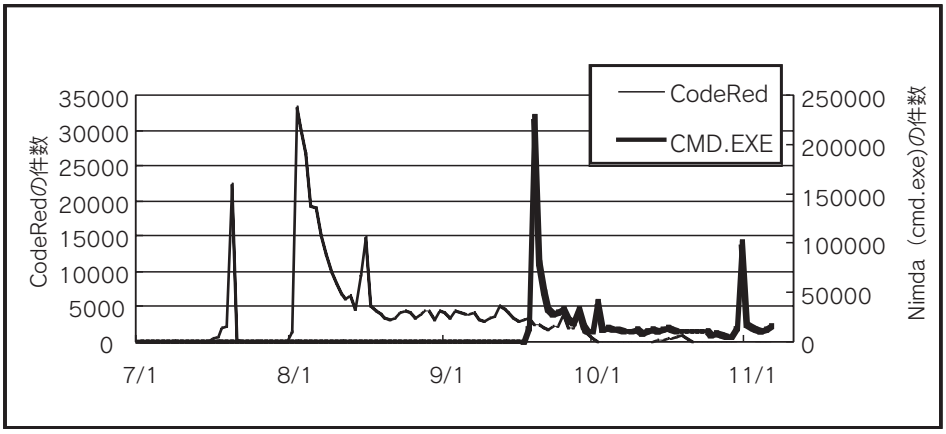

図-1　CodeRed とNimdaによる攻撃件数

当然として，さらに入退室管理や利用者管理を実施すべきである．

■技術的問題

ネットワークサーバのソフトウェアの弱点を狙った攻撃は無視できない問題となっている．このような攻撃には，システムの可用性を損なうことを目的としたサービス不能攻撃（DoS: Denial of Services）やメール爆弾，システムの機密性を損なう盗聴（Sniffing），およびシステムの完全性を破るためのWEBコンテンツ改ざんやシステム改ざんがある．これらの問題から組織内のネットワークやコンピュータを守るために，ファイアウォールのような障壁をインターネットと組織のネットワークの境界に設置して，ネットワークをイントラネットと外から見える非武装地帯（DMZ: De Militarized Zone）に分割することが一般化しつつある．ファイアウォールを信頼した構成では，内部ネットワークに接続された機器のセキュリティ対策はゆるくしか実施されていないことが多い．しかし，最近話題となったNimdaワームは，ファイアウォールを，いとも簡単に乗り越えて，イントラネット内にも大きな被害を与えた．

ここで，筆者の組織で観測したCodeRed系およびNimda系ワームによる攻撃件数を**図-1**にグラフで示す．それぞれ，代表的な攻撃パターンに着目してカウントしたものである．CodeRed系の件数はグラフの左側軸の数値，Nimda系は右側軸の数値で示されている．CodeRedの件数は，IISのインデックスサービスへのバッファオーバーフロー攻撃パケット数，Nimdaについては，cmd.exeへのアクセス件数である．Nimdaの場合，cmd.exe以外に文字コードの脆弱性を攻撃するパケットやCodeRed IIの残したバックドアへのアクセスも付随しているので，Nimda攻撃に起因するパケット数は，図の表示の数倍となる．これだけのパケットが外部からくると，インターネットとの接続速度にもよるが，内部感染がなくてもサービス不能攻撃を受けたのと同等の被害がある．すなわち，アプリケーションの利用に際して速度低下や接続不能といった問題が発生する．

こういったワーム以上に無視できないのは，PC UNIXやUNIXワークステーションおよびWindowsサーバのセキュリティホールを狙った攻撃である．

ここで，私たちのネットワークの入り口に設置したIDSによって検出されたTCPおよびUDPを利用したホストスキャンの観測データを**図-2**に示す．ここでは，少なくとも1サブネット全体をスキャンしたものだけを数えることにする．これは，IDSの誤検出の影響を排除するためである．データ採取期間は，2001年4月1日から10月31日の間である．この図-2から，ほぼ毎日のようにホストスキャンが行われていることが分かる．サーバへの攻撃には流行があるが，脆弱性の発見されたサービスへのスキャンが，攻撃前に多発することが観測されている．さらに，データを詳細に見ると，スキャン後に攻撃を行う場合と，スキャンと同時に攻撃を行う場合とがあることが分かる．

これらの攻撃元の大半は，海外プロバイダのADSLやCATVといったブロードバンドサービスを受けている端末かダイアルアップ端末である．しかも，比較的限られたプロバイダからのものが多い．

現状では，国内発のホストスキャンは，ワームを除けば，ほとんどないが，昨今のブロードバンド接続の国内での普及は，国内のSOHOサーバのセキュリティ問題の急増を予感させる．常時接続環境にあるSOHOサーバの危険性は，強調してもしすぎということはないと思える現状である．

さて，以下に，侵入されたりウィルスやワームに感染したホストに共通する問題点を箇条書きにして示す．

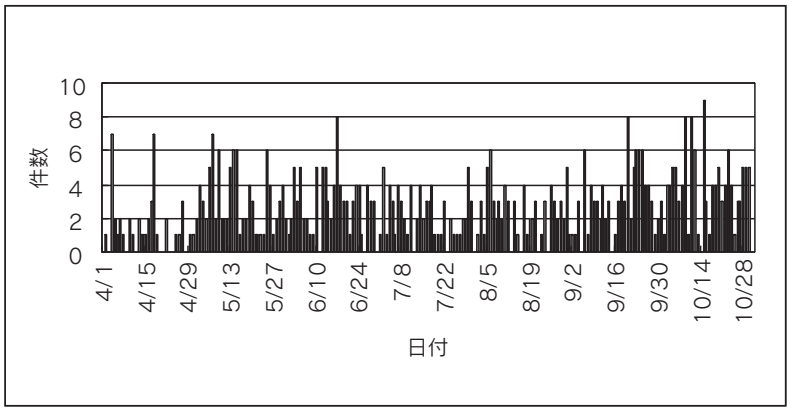

図-2　ネットワーク走査件数

- システムが導入時のままの状態で利用されている.
- 学生や職員の異動等で，サーバの管理者が不在である.
- 意図しないサービス（例，匿名FTPサービス）が自動起動されている.
- 手動で対策をし，自動起動スクリプト等の削除を忘れている．このような場合，リブートすると無防備な状態に戻る.
- 問題サイトへのアクセスやメールの添付ファイルの危険性に対して無頓着である.
- セキュリティ情報に気づいていても，まさか自分がという気分がある.

ネットワークやホストの管理者なら，だれでも思い当たる点があるのではないだろうか．インターネット環境の普及に伴って，攻撃用ツールの流通やワームの拡散速度は飛躍的に上がっている．筆者の学内でも，購入したばかりの機器が設定中に攻撃を受けて侵入されたとか，Nimdaに感染したサーバを修復している最中に再感染したという例が複数ある．これは，脅威となる問題の発見から対策に着手するまでの時間的余裕がほとんどないということを意味している.

■人的組織的問題

セキュリティ対策は，マイナスの要因をゼロに近づける努力の連続である．このため，多くの組織では，利益を生まない部署として軽視されがちである．大学でも，セキュリティ対策はホスト管理者のついで（ホストの管理業務そのものも本業のついでの場合が多い）の仕事といった感があるが，実際の被害は，管理の不十分なコンピュータに多発している．しかしながら，何か問題が発生した場合に，ネットワークやコンピュータなしではすまない現在の環境では，その回復にかかるコストは膨大なものとなることは想像に難くない．ようやく国内でも，セキュリティポリシーの重要性が喧伝され，セキュリティポリシーの策定が行われはじめている．ところが，その策定に着手してみるとセキュリティポリシー策定以前の問題が明確になっていない組織が多いのではないかと思われる．私たちが，セキュリティポリシーの策定作業中に直面した問題を大雑把に列挙しておく．以下に掲げた問題は，現在のところ完全には解決できていない.

- 組織としてのIT戦略の欠如
- 組織体制の不備
- 情報管理や公開の基準の不備
- 機器調達の基準および調達機器の管理基準の欠如

だれがどんな情報資源をどのように管理すべきかといったことさえ明確になっていないために，結果として，Sircamウィルスといったメールウィルスを介しての機密情報の漏洩やオンラインアンケート，住所録データの流出といったトラブルが後を絶たない．このような問題は，各種の情報資源が，業務を担当している組織にではなく，業務担当者と担当者のコンピュータに張り付いている現状に起因していると考えられる.

また，アウトソーシングを考える場合にも，確固としたIT戦略やセキュリティポリシーがないと，何を外注するかといった基本的なことがらを明示することは不可能である.

ネットワークサーバ導入の考え方

近年，導入コストが低いという理由で，パーソナルコンピュータにLinuxやFreeBSDといったPC UNIXでサーバを構成することが流行している．また，GUIで制御できて，管理が容易という理由でWindows NTやWindows 2000 Serverの普及も著しい．しかしながら，機器導入にあたっては，導入コストだけではなく，保守に要する費用も込みにしたコストを考えて導入する必要がある.

■PC UNIXは本当に安いか？

PC UNIXは，導入も含めて「at your own risk」が前提であることを見逃してはならない．実験システムを構築するとか，最新のソフトウェアが利

用できるといった魅力はあるが，その利点は，貧弱なドキュメンテーションとか，ソースプログラムを見ながらのトラブルシューティングといった問題点と裏腹である．

また，オープンソースを原則とするシステムにあっては，だれでもがシステムの内部情報にアクセスできるわけで，普及度が高いシステムほど，バグ発見の可能性もセキュリティリスクも高くなっていることを承知しておかなければならない．保守コストの問題は，市販システムでも考慮しておかなければならないが，運用システムとしてのPC UNIXの利用では，導入が簡便になってきた分だけ，保守に要するコストが無視されるか，低く見積もられる傾向があるように思える．ホストスキャンの傾向を見ていると，PC UNIXを狙ったと思われる攻撃がWindowsへの攻撃とともに圧倒的多数を占めている．これは，単に普及度が高いというだけでなく，攻撃の成功率が高いことが原因であると考えられる．別の見方をすれば，インターネット上に，保守状態のよくないPC UNIXが大量に存在していることの証明でもある．最近では，このような事態も改善されつつあるが，それでも安易なPC UNIXの導入は，多くのネットワークの管理者にとって，頭痛の種の1つであることにかわりはない．

■Windowsは簡単か？

いろいろな設定が，GUIで簡単にできるという理由で，Windowsサーバが採用されることがある．しかし，GUIで簡単に設定できるが，ほとんどの機能がブラックボックスであるために，トラブルが発生すると，原因の究明や対処に大変な手間がかかってしまう．

メーカの対応も徐々に改善されてはきているが，セキュリティパッチの相互依存関係に注意を払っていないと，塞がれたはずのセキュリティホールが開いたり，場合によっては，サービスパック適用によって起動しなくなるといったトラブルをよく耳にする．パッチにまつわるトラブルは，Windowsに限った話ではないが，重大なセキュリティ上のバグや，パッチにまつわるトラブルが少し多すぎる気がする．

また，管理者に多大のノウハウが要求され，かつバージョンが変わると，過去の経験の蓄積が生かされにくいという点でも，コスト的に大変なシステムのように感じられるが，どうであろうか？

■サーバ導入に何を考慮すればよいか

一般に，研究室や部署に1台しかコンピュータがないという環境は，ある程度の大きさの組織では考えられない．複数台のコンピュータの導入にあたっては，コストとセキュリティを考慮すべきである．そうすると，オペレーティングシステムの種類は少ない方がよい．種類が1種類ならば，手間は最悪でも台数分だけだが，システムの種類が増えると保守にかかるコストは加速度的に増加する．大学の研究室にありそうな，サーバのショーケースのような環境は，コスト的にもセキュリティ的にも問題である．

また，1台のホストに複数のネットワークサービスを受け持たせることは避けなければならない．特に，ネットワークの基幹となるネームサーバ等には，本来のサービス以外の機能を置かない構成にした方がよい．さらに言えば，ネームサーバやWEBサーバ等が研究室の計算サーバも兼ねるような設計は悪夢である．サービスの種類が多いほど，アクセスする人間の数が多いほどセキュリティリスクが増加するからである．

WEB等の情報提供サービスを除いて，ワールドワイドにサービスを提供する必要はないので，アクセス制限をするとともに，システム関係のファイルやコンテンツの改ざん検知を可能としておく必要がある．

■SOHOおよび家庭の場合

小規模な事業所，ホームオフィスや家庭でも，ケーブルテレビネットワークやADSLといったブロードバンド技術の普及によって常時接続が一般化してきた．このような高速の常時接続環境の実現によって，ネットワーク的にみれば自由度が格段に高くなったわけである．SOHOが大企業並みのIT利用の可能性を手にするということは，ネットワークセキュリティ対策に対する責任も相応に負わなければならないということでもある．回線速度が壁となっていたISDNの常時接続やダイアルアップの場合には，電子メールやWEBを介したウィルスに注意していればよかったが，ブロードバンドの常時接続ではセキュリティ対策に，それなりのコストが必要とされる．

実際に，ブロードバンドネットワークの利用者からは，まったく無関係のホストのファイルやフォルダが見えてしまうといった話も報告されている．また，ホストスキャンが大量にくるようになったとか，ルータの電源を入れた途端，すなわち，DHCPでアドレスがリースされた瞬間に，「トロイの木馬」プログラムに宛てたと思えるトラフィックが検出された（直前にそのアドレスを使っていたホストが踏み台になっているという明白な証拠である）といった話も聞こえてくる．したがって，独自にサーバを持つなら，これまでのウィルス対策に追加してSOHOや家庭内ネットワークの入り口にファイアウォール等の導入やアクセス制限の設定といったことが最低限必要となる．セキュリティ対策上からは，SOHOかそうでないかで質的な差はない．

SOHOの場合，自前のハードウェアを持ちシステムを構築する場合とプロバイダ等からサービスを購入するという場合のセキュリティ対策に

かかるコストを十分に比較検討する必要がある.

家庭のようにパソコンが1台だけの環境であっても，ウィルス対策以外に，パーソナルファイアウォールソフトウェア等によるアクセス制限，システム設定の見直しや日常のソフトウェア更新作業といった作業が，これまで以上に重要となる.

ネットワークサーバのセキュリティ対策

ネットワークサーバの管理者は，ファイアウォールが存在したとしても，ファイアウォールを全面的に信用してはいけない．ファイアウォールの設定にミスがないわけではないし，メールやWEBを媒介とするワームも存在する．さらに，クラッカーが内部にいないという保障はない．ファイアウォールに頼った管理をしていると，内部にワームが侵入した場合，被害が急速に拡大していくことは，CodeRedの例でも実証された.

いわゆる不正アクセス防止法の下でも，サーバが侵入されて踏み台に利用されたからといって管理者が刑事責任を問われることはない．しかし，セキュリティパッチを適用するといった常識的な管理を怠っていると，民事による損害賠償請求を受ける可能性がある．ましてや，古くて保守対象外となってしまったシステムを使い続けることは，インターネットに対して犯罪的ですらある．また，買ったばかりのコンピュータ等の機器をネットワークに接続して設定を実行するのも同様である．この章ではサーバ機器類の設定について概観する.

■アカウント管理

UNIXの場合，まだまだワンタイムパスワードといったアカウント管理は一般的でなく，パスワード方式が広く使われている．UNIXのパスワード暗号化アルゴリズムは，安全性が高いとされているが，安易に選ばれたパスワードは推測されやすい．そのためのツールも広く出回っている．最低限，Crackのようなツールで，問題のあるパスワードを使っている利用者がいないか定期的に監査し警告するといった作業の必要がある．このような作業を実行していない場合は，筆者の経験でも，20％から25％の利用者のパスワードが，だれでも入手できるツールで簡単に破られてしまう．次に対処しなければならないのは，セキュリティ上問題のあるアカウントの存在である．システムによってはdemoといったパスワードのないアカウントが存在する．また，業者が保守用に設定したアカウントも危険である．問題のあるアカウントのリストは，たとえばE.Knight[1)] によってコンパイルされWEB上で公開されている.

■プロセスアカウントおよびログ機能

課金の必要のないシステムではプロセス統計を採取していないことが多い．しかし，これでは，問題が発生した場合には，トラブルシューティングに必要な情報すら得られない．課金の必要がないシステムであってもプロセスアカウントを採取すべきである.

侵入された場合，pacct等のファイルは，証拠隠滅のために改ざんされることが多い．プロセスアカウントを処理するプログラムは容易に変更可能なので，これらを改造して一定間隔で利用者からアクセスできない場所にバックアップコピーを作成するとよい．バックアップ先は，書き換えできないメディアが望ましい.

■ネットワークサービス設定

UNIXやWindowsサーバは，インストールが簡単化された分，標準インストール状態では，余計なサービスが動作していることが普通になっている．使わないサービスの起動はセキュリティリスクを増大させる．サーバの設定にあたっては，必要のないサービスは起動しないように設定しなければならない.

多くのUNIXでは，ネットワークサービスの起動は，inetdから行われ，その設定はinetd.confで行う．このファイルを眺めてみれば，使う予定のないサービスがたくさん自動的に起動されるようになっていることが理解できるだろう．起動スクリプトについても，利用しないサービスに関しては，名前の変更等を行ってブート時に起動されないようにするといった対策を忘れてはならない.

情報処理センター等のサービス用ホスト以外では，利用者の範囲は限定されているはずで，利用者のいる端末やホストからのアクセスのみを許可するようにする．安易な無線ネットワーク装置の設置やVPNの設定およびSSHのポート転送機能の利用にも注意しなければならない.

■基幹ネットワークサーバの設定

ネットワークのインフラストラクチャの一部と考えられるネームサーバ，メールサーバやWEBサーバ等の設定には，一般のサーバ以上に注意しなければならない.

重要なサーバには，予備ディスク装置やファイルシステム上にブート可能なシステムを運用システムとは独立に用意しておくと，CD-ROMや起動フロッピーから起動する手間が省けて，迅速なトラブルシューティングが可能となる.

(1) ネームサーバ

ネームサーバには，ISCのbindが利用されることが多いが，利用者が多いだけにセキュリティホールも，かなりの頻度で発見されている．セキュリティ情報に気をつけて，問題が発見されれたら，バージョンアップをするとかパッチを当てるといった作業がかかせない．また，ネームサーバのゾーン情報の転送制御に注意を払っておかないと，ホストスキャンやクラックのための情報を簡単

に外部に与えてしまう.

(2) WEBサーバおよびWEBキャッシュ

WEBサーバのセキュリティトラブルで目に付くのは，コンテンツの改ざんと，だれにでもアクセスできるWEBのキャッシュサーバの問題である．ソフトウェアのバグフィックス作業とともに，サーバの設定に注意する必要がある．WEBサーバの場合，コンテンツ保護のためのファイル改ざん検出機能は必須である．内容保障が必要なら，電子透かし技術等の導入も考慮しなければならない.

■ホストIDSやトラップの利用

重要なサーバには，snortのようなIDSをホストIDS的に利用するとか，tcp_wrapperのブービートラップ機能を利用するとよい．このようなソフトウェアを導入して，異常なアクセスを検出可能にしておくと，侵入の防止や問題発生時の対応のためのデータの収集に役立つ.

サーバの日常管理と運用

セキュリティ対策は，常に新たに発見されるセキュリティホールを追いかける宿命にある．したがって，たとえ低い確率であっても，侵入された場合に備えて準備しておく必要がある．ネットワークサーバ単体では，必ずしもセキュリティ確保に十分な情報が得られるわけではないので，この章では，IDSやファイアウォールの利用を前提とする．IDSの利用の仕方やホストのログ監視のノウハウについてまず説明する．ついで，IDSやホストのログをもとにした侵入発見の方法について解説する.

■IDSやファイアウォールの日常運用と問題点の検出

日常的なセキュリティ管理には，CERT情報[2]やJPCERT[3]やIPA[4]が役立つ．IDSやファイアウォールのログを世界的に共有するdshield[5]も役立つ.

IDSのログに以下のような兆候が見られたら，標的とされたサーバが侵入された可能性を疑う必要がある.

- **深夜の定時のリモートでのコマンドの実行．たとえば，SSHの22番ポート以外での実行.**
- **ホストスキャンの標的となったホストからの攻撃元に対してのSSH等による接続およびIRCのJOIN.**
- **「cdコマンドで，'␣..' や '..␣' に移動しようとした．」また，「PATHに，このようなディレクトリが指定された.」**
- **administratorやrootでのログイン．suコマンドの実行.**
- **表-1に示すようなポートへのアクセス.**
- **その他，IDSの発する警告．ただし，誤報が多いことも承知していなければならない.**

表-1は発見頻度の高い「トロイの木馬」プログラムの使用ポートについて調べたものである．ポート番号は，インストールによって変化することに注意されたい．より詳細なリストは，たとえばNiteRydersのリファレンスデスク[6]で入手可能である.

問題ツール名称	標的システム	ポート番号等
Back Orifice系	Windows	31336/UDP 31337/UDP 31666/UDP
NetBus	Windows	1/TCP 2/TCP 12345/TCP 12345/UDP 12346/TCP 12631/TCP 20222/TCP
SubSeven	Windows	1243/TCP 27374/TCP 27444/UDP 27573/TCP 2773/TCP 54283/TCP 6711/TCP 6712/TCP 6713/TCP 7000/TCP 7215/TCP
Stacheldraht	Linux,Solaris	16600/TCP 65000/TCP 65535/TCP 65535/UDP ICMP_ECHOREPLY
trin00	Solaris	27665/TCP 27444/UDP 31335/UDP
TFN	UNIX	ICMP_ECHOREPLY

表-1　代表的問題ツールとポート番号

■ホストの日常管理

この節では，パッチ作業，ログの確認，セキュリティツールやコマンドでの監査および日常の情報収集について述べる.

(1) パッチ作業と問題点

ネットワークサーバの運用にあたって，定期的なパッチ作業は不可欠である．セキュリティパッチ公表の間隔は，近年短くなってきており，2週に一度は，新規パッチがないか確認する必要がある．もちろん，緊急度の高いものについては，この限りではない．ただし，作業にあたって，以下の点に注意が必要である.

- **システムソフトウェアを置き換えている場合，パッチによってソフトウェアがOS標準のものに戻ってしまう.**

- rcスクリプトやinetd.confに手を入れている場合，パッチによってファイルが置き換わることがある．
- ファイルのモードがパッチにより，セキュリティ対策以前の状態に戻ってしまう．
- パッチ適用により起動しなくなってしまう．

(2) ログの確認

日常的なホストのログ監視はハードウェア，ソフトウェアの異常検出やセキュリティ保持のために不可欠である．執拗なログイン失敗や権限のない利用者からの複数のsuの失敗に注意しなければならない．ログの1日あたりの容量は，なんらかの異常がないかぎり変動は少ない．容量が少ないとか記録の時間間隔が極端に長いといった点に注意しなければならない．ログ監視の補助として，analogのようにapacheのログ監視に特化したソフトウェアやswatchとかlogsurferといったログ監視を半自動化するソフトウェアがよく利用されている．

(3) セキュリティツールやコマンドを使った定期的な監査

Tripwire等によるファイル改ざん検出ツールをcronで，定期的に起動するように設定しておくと，ログがroot宛てにメールされる．ISS，Nessusといった攻撃型の監査ツールを使ったワークステーションの検査も有効である．Crackのようなパスワード確認ツールを用いての安易なパスワードのチェックも定期的に実行すべきである．findコマンドで，全ファイルシステム上のrootやbinにsetuidされたファイルをチェックする．ツールに関しては，CERTのセキュリティ改善モジュールのページ[9]が参考になる．

(4) 日常の情報収集

昨今，クラッキングツールの伝播のスピードは著しく速い．したがって，最新のセキュリティ情報について，常に注意を払っておかなければならない．以下に，広く利用されているセキュリティソースを掲げておく．

- CERT情報[2]，CERT Advisoryと呼ばれているセキュリティ情報が重要である．
- JPCERT情報[3]，各種の情報が日本語化されている．
- IPA情報[4]，国内のウィルス情報が充実している．
- Dshield情報[5]，最新の世界的なスキャンの動向が確認できる．
- NetSecurity情報[7]，セキュリティ情報の日本語ポータル．
- SecurityFocus情報[8]，緊急のセキュリティ情報．
- Neohapsisアーカイブ[9]，セキュリティ関係メーリングリストのアーカイブ．

ほかにも，各種あるが，ここに掲げた情報を見ていれば日常運用には支障がない．

侵入事象とその対応

本章では，侵入の検知と侵入された後の対策について説明する．CERTのガイドライン[10]は必読である．

■侵入検出のための手法と補助ツール

以下に，侵入の兆候を箇条書きにまとめておくので参考にされたい．

- アカウントの異常
  登録したはずのないエントリが/etc/passwdや/etc/shadowにある．
  rootやadministratorでログインできなくなった．
- ログ情報の異常
  ログに空白の時間帯がある．lastやlastcommの出力が連続していない．深夜の時間帯のリブートやcronで不審なプログラムの動作記録がある．
- ファイルの異常
  '..␣' や '...' といったディレクトリが存在する．ネットワークデーモンとまぎらわしい名前のファイルが本来の場所でない所にある．
- システムプログラムのcoreファイルがある．
- コマンドの動作異常
  コマンドオプションがエラーになる．たとえばnetstatやpsコマンド．
- プロセスの異常
  負荷の異常．プロセスとプロセスが開いているポートの関係の異常．
- ネットワークの異常
  特異なポートでの通信の記録．定時に特定のホストとの通信でのシェルコマンドの実行．負荷の異常．
- 利用者からの通報
  使っていないのに課金請求が来たとか，見覚えのないファイルがあるといった相談．
- その他の異常
  ディスクのアクセス音が激しくするとか，ネットワークインタフェースのアクセスランプが激しく点滅する．

内容的に一部重複するが，侵入検出に役立つソフトウェアを**表-2**にまとめて示す．これらの入手やインストールについては，CERTのSecurity Improvement Modules[11]が参考になる．これらのソフトウェアの入手に際しては，「トロイの木馬」が組み込まれたものが出回ったこともあるので，ファイルのチェックサムやフィンガープリントを確認するといった考慮が必要である．

■侵入への対処

この節では，侵入への対応について説明する．

(1) 侵入の確認

侵入された疑いが強い場合には，プロセスやネットワーク接続状況を記録しておく．調査には，コマンドの改ざんの可能性も考えて，CD-ROMから起動して調査するといったように健全なシステムを用いるとよい．不用意なシャットダウンやリブ

名前	機能	起動タイミング	備考
tcpd	アクセス制限，記録	inetdから起動	フリー
snort	攻撃やスキャンの検出	ブート時起動	フリー
logsurfer	自動ログ監視	ブート時起動	フリー
swatch	自動ログ監視	ブート時起動	フリー
tripwire	ファイルの整合性の検査	cronにより定期的に起動する	ASRは教育機関にかぎりフリー
snoop	パケットモニタ	コマンド	Solarisコマンド
tcpdump	パケットモニタ	コマンド	フリー
sps	プロセス状態確認	コマンド	フリー
top	負荷の重いプロセスの表示	コマンド	フリー
lsof	開かれているファイルやソケットとプロセスの関係の表示	コマンド	フリー
ifstatusやcpm	ネットワークインタフェースの状態確認	コマンド	Solaris用フリー
find_ddos	trin等のDDoSツール検出	コマンド	フリー，Linux,Solaris
chkrootkit	rootkit検出	コマンド	フリー，Linux,Solaris
truss	プロセスの動作トレース	コマンド	システムコマンド

表-2　侵入検出のためのツールおよびコマンド一覧

ートは，ログや証拠となるファイルの喪失につながることもある．以下に，大雑把な調査手順を示す．

UNIXでのトラブルシューティングでは，rootでログインできたら，作業が終了するまでroot権限を手放さないようにしなければならない．侵入された場合，root権限を手放すと，再度rootでログインできるとは限らないからである．

- **利用者や外部に対して，デマ情報が流れないように，利用者に正確な情報を的確に提供する．**
- **問題のホストの通信先を確認しておく．**
- **調査項目は，CERTのIntruder Detection Checklist[12]を基本にするが，find_ddosやchkrootkitといったツールでの調査も必要である．これらの調査結果は，必ず記録しておく必要がある．**

以上が終了したら，資料や証拠とするためにシステムのダンプを採取し，ファイルのバックアップも試みる．これらの作業が不可能なら，CD-ROM等から起動してファイルのバックアップを残す．これらのダンプやバックアップに利用するメディアは，書き換えできないものがよい．ただし，侵入調査のためであっても，権限のない他のシステムにログインしたりすることは行ってはならない．

(2) 被害拡大の防止

ホストの調査と並行して，hostsファイル，hosts.equivや.rhostsファイルに記述されているホストに影響が及んでいないか，また，IDSやファイアウォールのログ等から，他に影響が及んでいないかを調査しなければならない．これらの調査で，他のホストへの影響の懸念があれば安全な手段で通知する．

(3) 復旧処理

システムの復旧は，書き換えられない安全なメディアから，フォーマットしたディスクに対して，再インストールすることで行う．バックアップテープからのシステム復元では復旧後のシステムの安全性は保障されない．また，作業が完了しないうちにネットワークに接続すると作業中に侵入される可能性がある．利用者のパスワードは，強制的に変更し，利用者が再設定したパスワードはCrack等のツールを用いて強度を確認する．

(4) その他の対処

対処に自信を持てない場合には，有償となるが，業者に依頼することも可能である．被害対応について，警察に助言を求めることもできる．また，踏み台として利用され他のシステムに被害を与えたり，侵入により重要な被害を受けたりした場合には，警察に被害届けを提出することも考慮しなければならない．踏み台にされて他者に被害を与え，損害賠償問題に発展したりすると，被害届けが警察に提出されているかどうかで事後の対応が変わる可能性があるからである．

おわりに

本稿は，大学ネットワークの運用管理の中で，セキュリティ上問題と考えていること，収集した情報や利用しているソフトウェア情報を中心にまとめたものである．

最近は，ずいぶんとセキュリティ対策に関する書籍や文献が入手できるようになってきた．セキュリティポリシーの構築には，RFC2196[14]が役立つ．また，その補完としてRFC2504[15]は，利用者を対象にした内容となっており，システム管理者は一度は，目を通しておくとよいであろう．セキュリティ管理技術について詳細に解説したものとしては，たとえば，文献16）～18）がある．

参考文献（URLは2001.11.16確認済み）
1）Knight, E. ed.: http://www.securityparadigm.com/defaultpw.htm
2）CERT情報: http://www.cert.org/
3）JPCERT情報: http://www.jpcert.or.jp/
4）IPA情報: http://www.ipa.go.jp/
5）Dshield情報: http://www.dshield.org
6）NiteRydersのリファレンスデスク: http://www.nethog.com/feeds/niteryder/trojans.htm
7）NetSecurity情報: http://www.netsecurity.ne.jp/
8）SecurityFocus: http://www.securityfocus.com/
9）Neohapsisアーカイブ: http://archives.neohapsis.com/
10）Steps for Recovering from UNIX or NT System Compromise: http://www.cert.org/tech_tips/win-UNIX-system_compromise.html
11）CERT Security Improvement Modules: http://www.cert.org/security-improvemnet/
12）Intruder Detection Check lists: http://www.cert.org/tech_tips/intruder_detection_checklist.html
14）Fraser, B. Ed.: Site Security Handbook, RFC2196 (1997).
15）Guttman, E. and Leong, L.: Users' Security Handbook, RFC2504 (1999).
16）Chapman, D.B. and Zwicky, E.D.（歌代和正監訳，鈴木克彦訳）: ファイアウォール構築, オライリー・ジャパン (1996).
17）Garfinkel, S. and Spafford, G.（山口英監訳，谷口功訳）: UNIX & インターネットセキュリティ第2版, オライリー・ジャパン (1998).
18）Scambray, J. et al.（宇野みれ訳, 宇野俊夫監修）: クラッキング防衛大全, 翔泳社 (2001).

（平成13年12月7日受付）