セキュリティ—大切なデータを守る—

山口 英[†]

1. ま え が き

コンピュータセキュリティ、あるいは、ネットワークセキュリティという言葉が最近よく耳にする。近年はコンピュータウィルスの蔓延やインターネット経由での不正アクセス行為などが頻発しているため、セキュリティ保全といえば、何らかの悪意ある行為からコンピュータやネットワーク環境を保護する意味で使われることが多い。しかし、広義にはセキュリティ保全とは、コンピュータあるいはネットワークを利用する場合に、ユーザの期待通りにシステムを利用でき、かつ、業務に障害が発生しない状態を保つ方策および、その実施方法を意味する。したがって、広義のセキュリティ保全には、技術的方策だけでなく、コンピュータやネットワーク機器の設置方法、保守契約のあり方、システム管理者の採用方針と人事管理といった、広範囲な事柄まで対象として考えなければならないことが多い。そして、広義のセキュリティ保全という視点でシステムやネットワークの管理体制を考えることが、企業や大学に関係なくほとんどの組織で行われていないことが、現在のセキュリティ保全上の大きな問題となっている。

また、セキュリティ保全というと、多くの読者は何か特別な手段を用いてシステムを守る方策を思い浮かべるのではないだろうか。ところが、セキュリティ保全の作業の大部分は、従来からの管理作業を「よりの確に」、「よりシステマティックに」、「記録を正しく残しながら」実施することである。そして、たいていのセキュリティ問題は、通常管理作業が適切に行われていないことによって発生している。つまり、たいていのセキュリティ問題は、通常管理作業を的確に行えば発生を防ぐことができるのである。多くの管理者はこの事実を正しく理解していないために、セキュリティ保全は難しいものだと思いがちになっていることも、深刻な問題のひとつである。

本稿では、広義のセキュリティ保全の方策を解説する。また、特定のコンピュータシステムでの具体的なセキュリティ保全方法を解説することは避け、より一般化した事項について解説を行う。本稿の目標は、読者が自分自身の環

境のセキュリティ保全方策を考える場合に、考えるヒントをできる限り多く与えることにある。そして、読者がセキュリティ保全を日々考えていけるための基本的な理解を得てもらうことにある。特定のコンピュータシステムに特化した、セキュリティ保全のための詳細な方策やテクニックについては、システム付随のマニュアルやテクニカルドキュメントを参考にしてもらいたい。

2. 何を守るのか

セキュリティ保全を考える場合に、最初に検討しなければならないのは、下記の問題に対して明確な答えを出すことである。これはセキュリティ保全の検討では、避けて通れないプロセスである。

- (1) セキュリティ保全の対象は何か
- (2) セキュリティ保全にどれだけのコストをかけることができるのか

問題(1)は、セキュリティ保全対象を明確にしなければならないことを意味している。保全対象が明確になっていなければ、どのようなセキュリティ保全方法が有効なのかを考えることができない。また、問題(1)を考えることは、セキュリティ保全作業の目的を改めて考えなおすことにもつながる。

問題(2)は、セキュリティ保全にどれだけの労力・コストをかけてもよいかを決めることを意味する。財務的に見ればセキュリティ保全とは、「何も悪いことが起きないこと」に対してコストを負担することを意味する。通常設備投資等であれば、投資によって生産性向上や人件費圧縮などの効果があり、最終的に収益が向上するといったプラスのROI(Return of Investment)が期待される。ところが、セキュリティ保全に対するコスト負担は、通常投資ではなく、どちらかといえば保険と同種の負担という考え方をすべきである。したがって保険と同じように、セキュリティ保全対象の価値、想定すべき脅威(threat)、各脅威の発生確率予測などを考慮に入れて被害額の期待値を算出し、得られた期待値を元にセキュリティ保全に投入する予算を考えなければならない。一般にこの作業をリスクアセスメントと呼ぶ。リスクアセスメントを行うことで、対応すべき脅威を明確に認識でき、また、セキュリティ保全にかかるコストの妥当性も確認できる。

[†] 奈良先端科学技術大学院大学 情報科学研究科

"Introduction to Network Control Techniques, (11) How to Secure Your Data" by Suguru Yamaguchi (Graduate School of Information Science Nara Institute of Science and Technology, Nara)

リスクアセスメントで想定すべき脅威としては、悪意ある不正アクセスといった人為的な脅威だけでなく、停電や落雷といった電源喪失事故、火災や水害といった自然災害なども考慮に入れるべきである。先に述べた広義のセキュリティの定義に基づけば、自然災害も当然コンピュータの正常な運用を妨げる要因であり、考慮すべき要素であることは明らかである。また、初心者ミスオペレーションによる被害なども想定すれば、当然のことながらトレーニングなどの費用を、またディスクのトラブルを想定すればバックアップの費用を、それぞれ正当化することも可能となる。できる限り多くの面から脅威は想定する方が望ましい。

被害額の期待値からセキュリティ保全に投入する予算の規模を検討する場合には、当然のことながらシステムをとりまく運用環境を考慮して、プライオリティを付しながら検討するのが普通である。そのために、期待値の算定では、適度な重み付けを行うことも考慮に入れる必要がある。

3. セキュリティポリシーの策定

リスクアセスメントの次に行わなければならないのは、セキュリティポリシーの策定である。セキュリティポリシーとは、セキュリティ保全作業の根幹となる方針、考え方をまとめたものである。セキュリティポリシーには、経営者、システム管理者、ユーザに対して、セキュリティ保全作業を行う場合のルール、あるいはガイドラインを与えるものでなければならない。そしてセキュリティポリシーは明文化され、経営者、システム管理者、ユーザがセキュリティルールの遵守する体制を作り出す必要がある。

3.1 セキュリティポリシーの記述

セキュリティポリシーは各サイト毎の事情に応じた記述を行う。セキュリティポリシーには、一般に技術的要素と運営的要素に対する記述を行う。技術的要素では、サービスやシステムに対するアクセス制御、アカウントの発行とパスワード管理、バックアップ、緊急時の対応体制、ソフトウェアのインストール作業、ネットワークサービスの構成と運用などについての方針と作業ガイドラインを記述する。一方、運営的要素では、システム調達方法、プライバシー保護についての考え方、システム運用に関わる人員の人事管理方針、誰がどのような責任と権限を持つのか、セキュリティ保全に関わる予算執行の権限と手順、ユーザやシステム管理者のトレーニングの方法などが記述される。これらの記述は、サイト毎に必要なものを記述すればよい。ポリシーの策定では以下の点について注意しなければならない。

- (1) 実現不可能なことは記述してはならない。
- (2) 責任と権限に矛盾があってはならない。
- (3) セキュリティの記述では不明瞭な点がないようにしなければならない。

- (4) ポリシーの改訂が頻繁に起きないように、特定のシステムや環境について詳細に記述するようなことは避ける。しかし、逆に抽象的になりすぎ難解な記述にはならないように、適度な詳細化も必要である。

3.2 ポリシーの実装

セキュリティポリシーが策定できたら、作成したポリシーに従って必要な運用マニュアルやユーザガイドブックなどを作成することになる。この段階では、特定のシステムや環境に対応したマニュアルを作成しなければならない。当然、作成した運用マニュアルやユーザガイドブックは、それぞれシステム管理者やユーザに配布され、その内容についてシステム管理者やユーザが理解し、その実施を遵守しなければならない。そのために、トレーニングの実施が必要となるだろう。

さらに、ポリシーに基づいて組織構造を変更したり、必要な予算執行体制を整備することも必要になる場合もあるだろう。これらの体制作りは、経営者がセキュリティポリシーについて理解し、その実施に了解していなければ不可能である。このことから、セキュリティポリシーの策定では、経営者側の参画は必須である。

3.3 ポリシーのレビュー

作成したポリシーは定期的に見直す必要がある。例えば、新たなシステムが導入されたり、ネットワーク構成が変更された場合には、それまで利用してきたポリシーについて変更が必要かどうかを検討しなければならない。それ以外にもポリシーの実施に不具合が発見された場合には、ポリシーの変更を行う必要がある。このような理由から、当然のことながら策定したポリシーの改訂を妨げるようなポリシーや体制を作り出してはならない。

4. セキュリティ保全対策の実施

前章までは、セキュリティ保全作業を開始する場合に必要な作業について述べた。本節では、具体的なセキュリティ保全対策について概観する。

4.1 アカウント管理

システムにおけるアカウント管理は、セキュリティ保全の基本である。誰にアカウントを付与するのか、アカウント発行にはどのような手続きを行うのか、アカウント停止はどのように行うのか、利用者の長期出張や休職などによる休眠アカウントはどのように取り扱うのかなどの手順を決める必要がある。また、アカウントの作成は誰が行うのか、アカウント作成時に付随する作業として何を行うのかも決めなければならないだろう。これらはセキュリティポリシーとして記述されることが多い。

アカウント管理の基本は、システムを使用する必要があるユーザにのみ各人にアカウントを与えることである。休眠アカウントや共有アカウントは、できる限り排除することが必要である。また、ユーザの退職などによってアカ

ントを廃止しなければならなくなれば、直ちにアカウントを廃止する作業を行わなければならない。

4.2 パスワード管理

各ユーザには、他人から推定しにくい良いパスワードを使わせる必要がある。UNIXを中心として多くのシステムでは、現在では簡単なパスワードをパスワードとして受け付けられない構造になっていることが多い。しかしながら、管理者は定期的にパスワードの強度をcrackなどのツールを使用して確認した方がよい。

また、モデム経由でアクセスされるシステムや、インターネットから直接アクセスされるシステムでは、使い捨てパスワード(one time password)を使用した方がよい。現在では、使い捨てパスワードシステムとしてS/Key等のフリーウェアの実装や、SecureID等のトークンカードを使用した製品が数多く提供されている。使い捨てパスワードは単純な機構でありながら、ネットワーク環境では比較的強いシステム保護対策となる。

NIS等のネットワーク環境でアカウントを共有する機構は、できる限り注意して運用すべきである。アカウントとパスワードを共有しているシステム群では、1台でも不正アクセスが行われてしまえば、他のシステムも不正アクセスの脅威にさらされることになる。このようなことから、主要なサーバ等では、アカウント共有機構の利用には十分に慎重になるべきである。

4.3 ソフトウェア管理

システムで利用されているソフトウェアの把握、バージョン管理、セキュリティホールの駆除などは、セキュリティ保全における基本作業のひとつで、システム管理者が確実に実施しなければならない作業である。システムで利用しているソフトウェアについてバージョンを把握したり、改ざんを発見するために各ソフトウェアのファイルのMD5ハッシュ値を事前に算出しておいたり、あるいはセキュリティホールに関する情報を収集することが必要である。

4.4 ファイル管理

ファイルの保護モードをどのように設定するかは、各ユーザが注意しなければならない。他人に読まれたくないファイルは、適切な保護モードに設定することが重要である。ファイル保護モードの設定について、ユーザが正しく理解するための教育も必須である。

管理者としては、ファイル保護モードのデフォルト設定に注意すると共に、誰でもが書き込み可能なディレクトリ、ファイルの存在に注意することである。誰でもが書き込み可能なファイル、ディレクトリは、セキュリティ問題の多くを生み出す。したがって、この種のファイル、ディレクトリについては、できる限り排除する努力が必要である。

4.5 ファイル暗号化

ファイルが流出した場合にも有効なデータ保護方法としては、ファイルの暗号化がある。ファイル暗号化のための

ツールは、近年数多く提供されるようになってきている。代表的なツールとしてはPGPがある。

ファイル暗号化を行う場合、暗号化処理時に設定する暗号鍵(あるいはパスフレーズ)は、パスワードと同じように類推されにくく、かつ、忘れにくいものを使用すべきである。また、パスワードと違って、暗号化されたファイルを復号する機会が少ないことから、暗号化に使用した暗号鍵を忘れがちになる。そのことから、暗号鍵の記録も念のため作成し、厳重に保管するようにした方がよいだろう。現在の暗号システムではキーリカバリーの機能はほとんど提供されていないので、いったん暗号鍵を忘れてしまうと、ファイルを復元(復号)することはほぼ不可能となってしまうことは忘れてはならない。

4.6 バックアップ

バックアップの作成は、システム運用で必須の作業である。バックアップは定期的に作成するようにしなければならない。現在では大容量テープデバイスが数多く提供され、また、ジュークシステムも充実している。これらを使用してシステムバックアップを自動的に作成するシステムを運用するのがよいだろう。

作成したバックアップについては、本当にそのバックアップからシステムが復旧できるかどうかを確認することは必須である。バックアップは作成していたが、そのバックアップからシステムを復旧できない状況になっていた、というような話はよく聞くことである。このような状況を避けるために、必ずシステムバックアップが使いものになるかどうかは確認を定期的に行うべきである。また、バックアップに使用するテープなどの媒体については、定期的に新しいものに交換すべきである。媒体の利用頻度を把握することもトラブル回避に重要である。

個人レベルでのバックアップとしては、CD-RやDVD-RAMを利用したバックアップ作成が簡単かつ安価で良い方法だろう。

4.7 ファイアウォールの実装

ファイアウォールを使うと、外部のネットワークからのアクセス制御を一元的に行い、ネットワーク環境でのセキュリティ保全を効果的に実施できる。このようなことから、現在ではファイアウォールを導入するのは、どんな組織においても当たり前となっている。ファイアウォールを構成する場合、ルータの機能を使ってフィルタリングゲートウェイとして構成する方法と、NATなどの機能を利用するトランスポートゲートウェイを構成する方法がある。後者の場合、優良のソフトウェアパッケージとして提供されているものが数多く存在する。どちらの方法でも運用上十分なファイアウォールを構成することができる。

4.8 通信暗号化

インターネット環境で通信データを保護するためには、通信の暗号化を行うことが一般的である。

例えば、電子メールではS/MIME、PGP(Pretty Good

Privacy), ターミナルアクセスではSSH, ルータ間データ暗号化であれば, VPN, WWW アクセスであればSSLあるいはTLSを利用した暗号化アクセスが広く使われるようになってきている。さらに, 通信路レベルでの暗号化であれば, 暗号化機能付モデム(DSU/CSU)が最近では利用可能になっている。これらの技術を利用することは特別なことではなく, 最近では一般ユーザ環境でも利用されるようになってきた。

5. む す び

本稿では, 我々が利用するシステムやネットワーク環境において, セキュリティ保全を実施する場合に必要なセキュリティポリシーの策定, 具体的な保全作業の実施について述べた。しかし本稿では, 必要最低限のセキュリティ保全作業の概要に触れたに過ぎない。当然, 本稿で述べた事項以外にも, 個々のシステムやネットワーク機器に必要なセキュリティ保全作業が存在する。読者においては, 使用

中のコンピュータ, ネットワーク機器のマニュアルや, セキュリティ関連情報の精読と利用が必要であることはいうまでもない。

さらに, セキュリティ保全作業は, 一度やれば終わりというものではなく, 常にシステム運用状況に注意を払いながら, システムの改善・改良に努力していかなければならないものである。

このようなセキュリティ保全作業に, 本稿がシステム運用に関わる人々の一助になれば幸いである。

やまぐち すむる
山口 英 1990年, 大阪大学大学院基礎工学研究科博士後期課程を中退し, 同大学情報処理教育センター助手着任。1992年, 奈良先端科学技術大学院大学情報科学センター助教授。1993年より, 同大学情報科学研究科助教授。大規模分散処理環境構築, ネットワークセキュリティ等の研究に従事。また1988年WIDE Project開始時より, 広域コンピュータネットワークの構築・研究に従事。WIDE Project運営委員, Asian Internet Interconnection Initiatives 代表, コンピュータ緊急対応センター(JPCERT/CC)運営委員長, Cyber Kansai Project 運営委員長など。工学博士。

1998年12月号「ここまで来た! インターネットにおける映像技術」小特集 「セキュリティを目的とした画像技術」論文小特集 予定目次

【ふ お ー か す】	東 大 安田 浩
【小 特 集】	1. 新しい映像ネットワーク技術とサイバーサエティNTT 一ノ瀬 進
	2. インターネットビデオKDD 研 松本修一・宮地悟史
	3. LAN/インターネット映像通信の標準——TIU-T 勧告 H.323——.....KDD 研 酒澤茂之・和田正裕
	4. インターネットにおける中継の実例
	4-1 高校野球実況中継大阪府立大 普天間 智
	4-2 COP 3 生中継京 大 中村素典
【技 術 開 発】	JPEG 2000 の動向三菱電機 小野文孝・上野幾朗・渥美栄司
【講 座】	ネットワーク管理入門(最終回): トラブル対策——転ばぬ先の杖——.....奈良先端大 片山喜章
【てれび・さろん】	ものを作るころ(第34回): MIDI規格開発ストーリーヤマハ 二間瀬 剛
【映像現場訪問記】	東京大学「インテリジェントモデリングラボラトリー」
	理科大 山下真由子・河村貴朗・四方行紀・坂森 聡・佐久間正泰
【小 特 集 論 文】	ウェーブレット変換を用いた画像信号に関する電子透かし方式
	松下電器 井上 尚・島津幹夫・桂 卓史, 九 大 宮崎明雄
	動領域内の肌色推定による顔領域および顔部品抽出.....三洋電機 本郷仁志, 岐阜大 山本和彦
【小 特 集 速 報】	パッチワークとDCTを用いた電子透かし法.....慶 大 記井浩之・大西淳児・小沢慎治
	パッチワークによる電子透かし方式の改良.....慶 大 佐藤 新・大西淳児・小沢慎治
	ビデオ画像上の人の衣服認識法.....九州工大 田房友典・石川聖二・河口英二
【論 文】	非直線ガンマ特性の測定と解析.....北陸先端大 猪野高雄・宮原 誠
	視覚の誘導場を用いた読み易い和文文字列表示.....セイコーエプソン 長石道博
	限定色画像の予備符号化に適したインデックスの割当法.....理科大 松田一朗・安藤 雅・伊東 晋
【研 究 速 報】	センサ面上で2次元動きベクトル検出の提案と設計.....東 大 李 正・石 嵩 透・相澤清晴・羽鳥光俊
	反射板つき4Lポリループアンテナの指向特性.....名城大 山口惣一郎・鳥居甫吉
	ファジー色領域抽出に基づく画像のブラウジングと検索.....九州芸工大 堀田政二・浦浜喜一