# 情報セキュリティについて

ＩＴ支援係長　阪　部　　清　　指導主事　藪　田　真　孝
Sakabe Kiyoshi　　Yabuta Masataka
指導主事　宮　崎　博　文　　指導主事　廣　田　清　雄
Miyazaki Hirofumi　　Hirota Kiyoo

**要　　旨**

情報セキュリティポリシーの策定と所員の情報セキュリティに対する意識の向上に向けて、ネットワーク上の脅威・被害の内容やその手口について調査・研究し、脅威・被害から組織の情報資産を守る対策及び機器や環境面に関するセキュリティ対策について検討した。

キーワード：　情報セキュリティポリシー、ファイアウォール

## １　はじめに

情報セキュリティ[*1]対策を立てる際に重要なことは、ネットワークにどのような危険性があるかを把握し、それらの危険性から情報資産をどのように守るかを明確にすることである。

例えば、インターネットからの不正なアクセスを防ぐ対策としてファイアウォールが構築されている。しかし、ファイアウォールは完璧なものではなく、それ自体が危険と判断して通信を遮断するわけではない。何が危険であるかを組織内で十分検討して情報セキュリティポリシー[*2]（以下、「ポリシー」という。）を策定し、そのポリシーをファイアウォールに適用することが必要である。

また、組織内のネットワークにおいて、各個人の様々な要求に応じれば、セキュリティに対する共通の基準がなくなり、問題が発生しても迅速かつ適切な対応ができない。そこで、ポリシーを確立し、共通認識しておくことが重要となってくる。

本研究では、当研究所内において情報セキュリティシステムを構築し、情報資産を安全に活用するための方途を探るとともに、適切なポリシーの策定にむけて検討したいと考えた。

## ２　研究目的

ネットワークを効果的に利用することにより、業務の効率化や情報の共有化が図られる。しかし、ネットワークに接続することでどのような危険があるか、またその対策については、あまり関心がもたれていない面がある。そこで、本研究では所内の情報セキュリティ対策について検討し、独自のセ

---

＊１　情報資産(情報システム並びにシステム開発、運用及び保守のための資料等)の機密性、完全性及び可用性を維持すること。

＊２　組織が所有する情報資産の情報セキュリティ対策について、総合的・体系的かつ具体的にとりまとめたもので、どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定のこと。

キュリティシステムを構築した上で、適切なポリシーの策定に向けて検討した。また、ポリシー策定の過程において、所員全体の情報セキュリティに対する意識の向上も図りたい。

## 3　研究方法

(1)　脅威・被害についての調査

(2)　脅威・被害をもたらす手口についての調査

(3)　脅威・被害から組織の情報資産を守る対策の検討

(4)　機器や環境面に関するセキュリティ対策の検討

(5)　情報セキュリティポリシーの検討

## 4　研究内容

(1)　脅威・被害についての調査

今日、様々な場面でコンピュータによる処理が行われており、システム全体が正常に安定して稼働し続けることは、大変重要である。また、コンピュータで扱うデータは、消されたり、盗まれたりしないように管理する必要がある。

一般的なネットワーク形態である、サーバとクライアントは、大変有効に使われているが、第三者がデータを盗んだり、不正に遠隔操作したりする可能性があるので危険を伴う。

データに関することでの脅威・被害は、盗用、改竄(かいざん)、消去、漏洩(ろうえい)である。

盗用…データは簡単に複製でき、しかも物のようになくなるわけでないので気付かない。知らない間に他の場所で流用されていることがある。

改竄(かいざん)…Webサーバ上にあるWebページが違うものにすりかえられたり、発見しにくい例としては、画像データに音楽CDや映画DVDが埋め込まれる場合がある。また、Webサーバに侵入されて、フィッシング詐欺サイトを埋め込まれた例もある。

消去…重要なファイルを消されることである。例えば、パスワードファイルを消されると、ファイルの共有や、データのやりとりをする処理等ができなくなり、組織全体に被害をもたらす。

漏洩(ろうえい)…内部の人間の不注意か犯行で起きることがほとんどだが、中には、ウィルスやスパイウェアが忍び込んだことで内部情報が漏洩する例がある。

データに関すること以外の脅威・被害は、第三者にハードディスクを初期化される等のシステム破壊、Webサーバ、mailサーバ、DNSサーバの機能を停止させるサービス妨害、SPAMメールの発信源になる踏み台がある。犯罪者の多くは不正侵入する場合、痕跡を残さないために、乗っ取ったサーバを経由して侵入する。乗っ取られた側は、知らない間に加害者になっていることになる。

システムが破壊されると、正常な業務ができなくなり、復旧のためのＳＥの人件費も負担しなければならない。更に、データがなくなっていれば、それを復元する労力等も必要となる。

サービスを妨害されると、電子メールの送受信、WebページでのＰＲ活動、インターネットを使った調べ学習等ができなくなる。

更に物理的な被害以上に大きな被害は、信用をなくすことである。例えば、組織が管理しているmailサーバが踏み台になっていれば、インターネット上のブラックリストに掲載される。また、組

織内の一人がウィルスに感染し、感染した人が管理しているメールアドレスのリストにウィルスをばらまけば、多くの人に迷惑をかける。

特に、公共機関においてはネットワークシステムが脆弱(ぜいじゃく)なセキュリティしか保たれていないということが発覚したら、社会からの信用をなくすことになり、損害賠償請求に及ぶこともある。

そして、このような脅威・被害は、普段直接目に見えないので、通常では意識されていない。

(2) 脅威・被害をもたらす手口についての調査

ネットワーク上での攻撃手口として、まず、システム侵入が挙げられる。その手口は、パスワード盗用、バックドア、セキュリティホールの利用である。攻撃者側の最終目標は、管理者権限のあるパスワードを取得することにある。例えば、組織内の一人が電子メールのパスワードを簡単なものに設定していると、そのパスワードを利用して侵入し、あらゆる手段を使って管理者権限のあるパスワードを解析しようとする。もし、攻撃者が管理者権限のあるパスワードを取得したら、その時点で、すべての操作が可能になる。

パスワード盗用の手口としては、パスワード解析ソフトがよく利用される。このソフトは、簡単なパスワードの解析から辞書を使った高度な解析､言葉の組み合わせを総当たりする解析ができる。ほかには、パスワードを書いたメモが残っていてそれが悪用されるなど、パスワードが十分に管理されていないことが挙げられる。

バックドアとは、管理者が気付かない侵入路を確保することである。その際、ウィルス等を使いプログラムを埋め込んだり、WebサーバのCGIを利用したりする。

セキュリティホールとは、プログラムの脆弱(ぜいじゃく)な部分のことで、プログラムが想定外の動作をしたりして非常に危険な状態になることがある。ただ、セキュリティホールのないプログラムはないのが現状である。

その他、ネットワーク上に流れる他人の通信情報を盗み見する手口として、特に無線機器の電波から通信を傍受することが挙げられる。盗まれた情報に認証用のユーザIDとパスワードがあれば、攻撃に利用される危険性がある。

サーバへの攻撃としては、同時に大量のリクエストを送り続けたり、大量の電子メールを連続的に送信することによって動作不能状態にするといったことが挙げられる。

(3) 脅威・被害から組織の情報資産を守る対策の検討

管理者側の立場から考えれば、ネットワーク上の脅威・被害から組織を守るためには、利用者側の要求をすべて受け入れるわけにはいかないということは明らかである。そこで、許可できる範囲を決め、できないものはできないという断固たる態度をとることも必要である。そのためには、明確な指針を示さなければ、利用者側に納得してもらえない。

ネットワーク上での脅威・被害を利用者に理解してもらい、多くの利用者が納得できる方針を当初より明確にする。更に、新しい脅威・被害など予期できない不備に対応できるように絶えず見直しも必要となる。

ネットワーク上の脅威・被害から組織をどのようにして守るのかということを、学校の防犯セキュリティシステムと比較して考えると、次の表１のようになる。休業時の学校では警備保障に守られていても、各部屋や重要書類の入った机の引き出しは、各個人で鍵をかけなければならない。ネットワークセキュリティシステムも同様に、個人としてしなければならないことと組織としてしな

ければならないことがある。

**表１　防犯セキュリティシステムとネットワークセキュリティシステム**

| | 防犯セキュリティシステム | ネットワークセキュリティシステム |
|---|---|---|
| 組織 | 玄関の施錠 | ファイアウォールの構築 |
| | 警備保障会社との契約 | ログの監視 |
| 個人 | 各部屋の施錠 | パソコンのパスワード管理 |
| | 金庫や机の引出の施錠 | ファイルのパスワード設定 |

個人としてしなければならないことは、個々が扱っている重要なデータをネットワーク上の脅威・被害から守ることを絶えず考えることである。これは、個々によって守る対象が違うので守る方法も違うためである。

例えば、データを運ぶためのUSBメモリーに個人情報や重要なデータファイルが入っているならば、厳重に管理しパスワードを設定する必要がある。

更に、決められたポリシーを遵守することである。例えば、次のようなことが挙げられる。

・成績処理のファイルにはパスワードを設定する。
・無線LANについては、アクセス権の設定や通信経路の暗号化をする。放置している無線機器があれば、外部侵入をさけるため機器の電源を切る。

もし、利用者がポリシーに納得できない部分があれば、セキュリティ担当者に質問をする。それが組織として取り上げるべきものであれば、議論や研修を行い、より一層よいものにしていこうとする取組が必要である。

組織でしなければならないことは、外部との接続点を一ヶ所にし、その場所を集中的に守ることである。電子メールや、インターネットのデータは必ずここを通るので、ここに堅牢な門番としてのファイアウォールを置き、ログの監視やウィルスの検疫ができるシステムを構築する。

例えば、電子メールのウィルス検疫所を設けることにより、外から送られてくる電子メールに対しても、中から送られる電子メールに対してもウィルスチェックができる。

ただし、ファイアウォールの構築方法には特に決まった形式があるわけではなく、その組織のポリシーによって大きく異なるので、それぞれ組織独自のファイアウォールシステムを構築することが必要になる。

次に、被害を受けた場合の対策を前もって立てておく必要がある。攻撃への対応については、発見時の緊急連絡体制を確立しておく、被害を拡大させないために物理的に遮断する部分や止めるサービスを決めておく、状況を把握するための該当ログの解析がすぐできるようにしておくこと等が考えられる。

迅速な復旧のために、攻撃内容を想定し、このような対策を決めておく。また、再び同じことが起きないように、必要に応じてポリシーを改善すれば、弱点が減り、組織のセキュリティレベルが向上する。

(4)　機器や環境面に関するセキュリティ対策の検討

公開しているインターネットサーバは、世界中の不特定多数の人々を相手にしながら運用しているので、「インターネットを通してつながっている世界中の人々全員が善人であるというわけでは

ない」ということを常に考えて運用しなければならない。また、組織内のインターネットにつながるコンピュータも同様に考える必要がある。

更に、組織が学校の場合は、児童生徒にどこまでネットワークを開放するか等の問題について教育的な配慮をしながら運用しなければならない。

次に、外部から内部への攻撃、内部から内部のサーバへの攻撃、内部から外部への攻撃を想定し、通信の方向性を考えながらファイアウォールの機器構成を決める。ファイアウォールの設計段階で、通さない通信と安全に通す通信を明確にする。そして、既知の攻撃に対して対策ができているかを確認した上で、常時安定稼働させる。

環境面については、常に人間に危害が及ばないかを確認することが必須である。不安定な電源や電気設備を使用していたり、熱対策用の空調設備がなかったり、落雷等に対して対策がとれていないLAN配線があれば、火災の恐れがあり、その結果として人命が脅かされる。

国や県が示す営繕仕様の工事が法律に従って施工されていることが前提であるが、人体に悪影響を及ぼしにくい機器を使用するなど、環境面に配慮して施設・設備を整えていかなければならない。

(5)　情報セキュリティポリシーの検討

ポリシーで重要なことは、情報資産を守っていく方針を明確にすることと、策定したポリシーを厳重に守ることである。もし、ポリシーの守られていないセキュリティのあまい部分が一ヶ所でもあれば集中的に狙われ、ネットワーク全体が危険にさらされる。管理者には、決められたポリシーを厳重に守り続ける態度が求められる。

しかし、それぞれの組織には個別の要件があり、守るべきもの、守るためにかけられるコストも違う。また、個々のスキルや管理職の考え方の違いなど、ポリシーに絶対的なものはない。つまり、段階的によりよいものを目指し、地道に着実に理解を得ながら進めなければならない。また、ポリシーに問題が発見されれば、適切な変更ができることも重要である。

また、ネットワーク環境の整備が進んだことによって、音声や動画等のデータの配信や、データの共有等が可能になった。このことにより、データをどのように送るか、また、受け取ったデータをどのように処理するか等の利用面については関心がもたれるが、毎日使っているコンピュータの安全性については、十分に留意されていないと思われる。このような状況の中で、ポリシーを検討する際には、一人一人が普段扱っているデータの重要性が再認識でき、組織全体にネットワークセキュリティの意識を根付かせることが重要課題となってくる。

具体的にポリシーを策定する場合、人的セキュリティと物理的セキュリティ、技術的セキュリティなどについての基準を定めなければならない。

人的セキュリティとして、組織の中での役割と責任の明確化、ポリシーを理解して実践するための教育・訓練、セキュリティに関する事故やシステム上の欠陥に対する報告、パスワードの管理がある。

例えば、セキュリティ担当者がポリシーに従って厳重にパスワード認証システムを構築しても、パスワードをメモに書いて机に貼ったりする人が一人でもいれば、セキュリティが保てなくなる。このように、セキュリティは利用者の行動によるところが大きいので、セキュリティに関する教育を計画的に実施する必要がある。

また、物理的セキュリティとして、盗難や災害、過失、物理的破壊などへの対処がある。例えば、

施設の施錠と入退室管理、防水工事や耐震・耐火構造の採用、無停電電源装置の採用、予備システムの導入、データのバックアップ等が挙げられる。不審人物が簡単に施設の中に入れないようにするのは当然であるが、ネットワークにおいても末端までどのような状態であるか日常的に把握しておく必要がある。

技術的セキュリティでは、コンピュータ及びネットワークの管理、アクセス制御、システム開発・導入・保守等、コンピュータウィルス対策、セキュリティ情報の収集がある。例えば、情報へのアクセスは業務要件に従って許可される必要があり、許可された利用者が、必要なときに、関連する情報資産へ確実にアクセスできるよう、利用者の登録の手順や責任などについて定めなければならない。

## 5　おわりに

毎日安全にシステムを安定稼働させていることは、特に情報発信をしている公共機関にとっては重要なことだが、現実は、ネットワークの運用に関する知識や資格があっても実務経験のない人がネットワークを管理している場合も多い。インターネットサーバの構築経験のない人が、外部からの脅威について理解してネットワークの設計・運用ができるかは疑問である。また、ネットワークの新しい脅威に対応するためにも、年に複数回専門家によるセキュリティシステムの動作検証などを受け、ポリシーの改善を検討することが必要である。

なお、今後の検討事項として、セキュリティ対策の専門的な知識や技術を蓄積するために、それぞれの組織間の連絡会議のような情報交換の場をつくり、研修の機会を設定していかなければならないと考える。