経済経営研究所のセキュリティ対策

経済経営研究所　國本光正

１．はじめに

経済経営研究所では平成１２年１月のシステム更新以降、専用サーバや専用ソフトを用いてセキュリティ対策を行ってきました。本稿では経済経営研究所で行っている（１）不正アクセス対策（２）ウィルス対策について紹介していきます。

２．不正アクセス対策

２．１　ファイアウォールでの不正アクセス対策

経済経営研究所（以下 研究所）では不正アクセス対策として Check Point 社の FireWall-1[1]を導入し、研究所セグメントをすべてファイアウォールで保護しています。

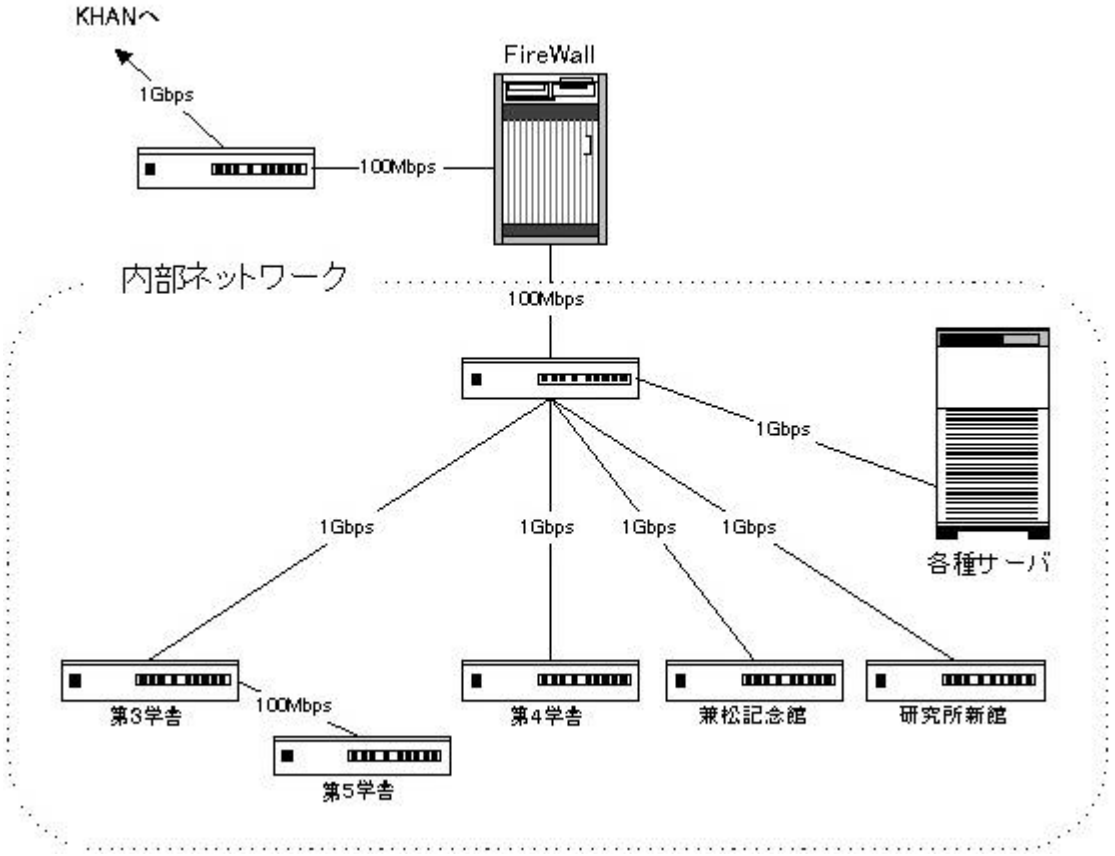

図１　ネットワーク構成

[1] http://www.checkpoint.co.jp/products/firewall-1/index.html

研究所では複数の建物に数名から数十名ずつばらばらに教職員が存在します。これらばらばらに存在する人たちすべてをVLANなどを利用して１つのセグメントに入れることにより、すべてのマシンをファイアウォール内部に閉じ込めています。

研究所で行っているFireWall-1の設定はそれほど特別なものではありませんが、設定上注意する点がいくつかあります。これは研究所で導入した当初はわからず、ユーザからの苦情で判明したものがほとんどです。

- 図書検索ソフトや図書業務ソフト
- StarOffice，Norton AntiVirusなど事務が使用しているソフト
- AOLやMSN Messengerなど特別なポートを使用しているソフト

図書検索ソフトは図書サーバにあるCD-ROMをネットワークドライブとして使用するために、図書検索サーバに対してアクセスの許可をしておかなければ使用できなくなってしまいました。また、研究所には図書室・文献センターがあるため図書が使用している業務ソフトに対してのアクセスも許可する必要がありました。

StarOfficeやNorton AntiVirusなどの事務が使用しているソフトのアクセス許可も必要となります。また、事務ではこれらのソフトのインストールを Windows のファイル共有を使用してサーバ上のディスクから行うために、インストールサーバに対して Windows ファイル共有のアクセス許可もする必要があります。

ファイアウォールを導入して一番効果を上げている点としては、システム管理者のセキュリティ対策に要する時間が圧倒的に減ったということです。研究所にはテスト用マシンを含めてSGI IRIX，Sun Solaris，Linux などの１０台近いあらゆるサーバが存在します。セキュリティホールが発見される度にこれらのサーバのセキュリティ対策を行う時間も人手もありません。また、これからはクライアントマシンも WindowsXP や MacOS-X などのリモートから操作され得るマシンも増えてくるために、サーバだけではなくクライアントのセキュリティ対策も重要となってきます。クライアントを含めるととてもではありませんが、１台１台セキュリティ対策を行うことはできません。管理者の負担を低減し、確実なセキュリティ対策としては、ファイアウォールの導入はとても効果的です。

ファイアウォールを導入し、外部からの不正アクセスは防御することができています。しかし、ファイアウォールに頼りすぎると、マシン自身のセキュリティホールがそのまま残っているという状況が発生してしまいます。これは、ファイアウォール内部からの不正アクセスにはとても弱いことになります。今後の研究所の課題としては、どのようにしてサーバ群をファイアウォール内部からの不正アクセスから防御するかということです。サーバ群を別ネットワークに隔離して内部からの不正アクセスを防ぐというのも１つの方法かもしれません。

２．２　WindowsXP でのセキュリティ対策

WindowsXP では、標準でパーソナルファイアウォール機能がついています。このファイアウォール

機能はＰＣから外部へ出ていくパケットの制限はできませんが、外部からＰＣへのアクセスについて制限することができます。これだけでもかなり有効な対策になります。

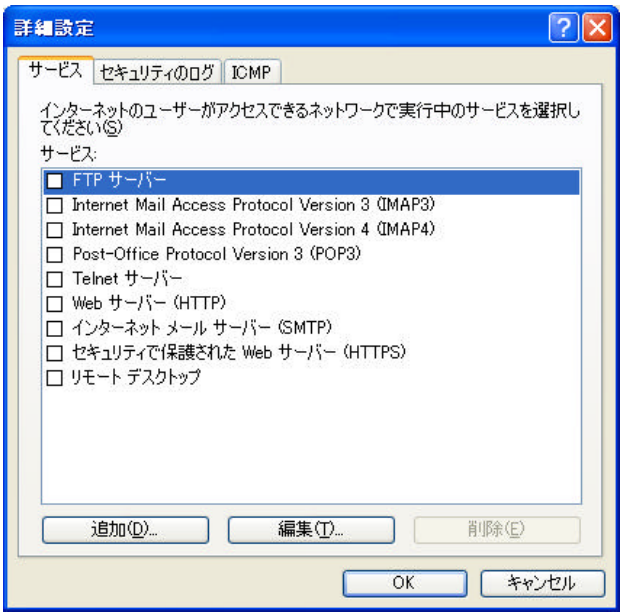

図２　WindowsXP のパーソナルファイアウォール設定画面

WindowsXP のファイアウォール機能を使用する上で注意する点は、外部からのアクセスをすべて拒否してしまうために、Windows のファイル共有も使用できなくなってしまう点です。もし、WindowsXP でファイル共有を行いたい場合は、図２の画面で個別にアクセス許可の設定をする必要があります。

３．ウィルス対策

３．１　パソコンでのウィルスチェック

研究所では、まず各教職員に配布している共通ＰＣ４４台すべてに Symantec 社の Norton AntiVirus 2000[2]を導入しました。これにより、ウィルス対策としてはかなりの効果を上げていますが、以下の理由から完全なウィルス対策とはなっていません。

- 管理がユーザ任せとなってしまうので、ウィルス定義ファイルが最新のものに更新されていない場合がある[3]。
- 教官個人のＰＣに関しては、すべてウィルス対策ソフトが導入されているわけではない。
- 教官個人のＰＣにウィルス対策ソフトがインストールされている場合でも設定が正しく行われていない場合がある。（ウィルス定義ファイルの自動更新が１ヶ月に１度など）

また、Norton AntiVirus 2000 を導入してからの問題点として、１年に１度更新作業をしなければいけないという点があります。Norton AntiVirus 2000 などのウィルス対策ソフトは１年間しか使用することができません。それ以後も使用するためには、更新手続きを行ってシリアル番号をソフトに入力

2　http://www.symantec.com/region/jp/products/nav/index.html
3　自動アップデートの設定をしていてもユーザがキャンセルしてしまうケースが多い。

する必要があります。この更新作業はシステム管理者の大きい負担となっています。また、教官が個人で購入した場合は、更新手続きを行わずウィルス定義ファイルの更新ができないまま使用している場合もあります。この問題点を解決するにはサーバ側でクライアントの設定がコントロールできるSymantec 社の Norton AntiVirus Enterprise Solution[4]というソフトが有効かもしれません。

3．2　サーバでのメールウィルスチェック

クライアントのウィルスチェックだけでは不十分だからといって、管理者がすべてのＰＣを回って設定を確かめることなど不可能です。そこで、研究所では最近のウィルスはメールの添付ファイルを介して感染するものが多いことに注目し、Symantec 社の Norton AntiVirus for Gateways[5]（以下 NAVGW）を導入しました。これはサーバ上でメールのウィルスチェックを行ってくれるソフトです。

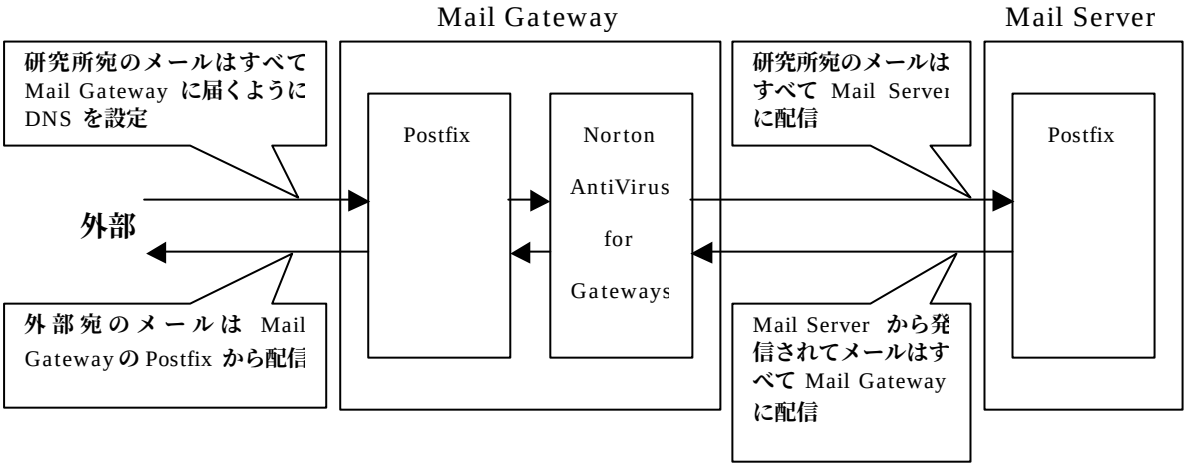

図 3　システム構成

研究所では図３のように、メールサーバとは別にメールゲートウェイとなるマシンを用意し、すべての研究所メールはこのサーバを経由してメールウィルスのチェックを行っています。メールゲートウェイを別に設置せずにメールサーバ上で Postfix や Sendmail の代わりに NAVGW を使用することもできます。しかし、研究所では以下の理由から別サーバを設置しました。

- メールサーバは IRIX6.5 であるが、NAVGW が Solaris 用か Windows 用しか販売されていない
- 特定ユーザのみ外部からのリレーを許可しているが、そのようなリレーに関する詳細な設定が NAVGW ではできない
- メールゲートウェイを置くことでメールサーバを外部から隠すことができる

また、メールゲートウェイでは NAVGW の他に Postfix をインストールし、外部とのメール送受信はすべて Postfix で行うようにしています。この理由としては、NAVGW に以下のような仕様があったためです。

- 送信先の DNS サーバより Authoritative Answer を得られなければ送信しない[6]

---

4 http://www.symantec.com/region/jp/products/nav_es45/index.html

5 http://www.symantec.co.jp/region/jp/products/nav25sg/index.html

6 Norton AntiVirus for Gateways 2.5でこの部分は改善されNon-authoritative answer でも配信できるよう設定可能となった

・ DNS の MX レコードに指定されたホスト名が alias の場合は送信しない

これらの理由で Postfix や Sendmail では配送できるのに、NAVGW からはメールが配信できないという現象が発生しました。NAVGW はこのメール送受信の部分がもう少し改善されると、もっとよいソフトになると思います。

３．３　サーバでの Web アクセスウィルスチェック

以上のクライアントとメールゲートウェイによる２重のウィルスチェックでほとんどのウィルスに対応することができていました。しかし、nimda ウィルスのようなホームページを見るだけで感染してしまうタイプのウィルスが出現し、研究所のウィルス対策では完全なものとは言えなくなりました。

２００１年９月末時点ではまだ導入できていませんが、Symantec 社の Symantec Web Security 2.0[7]という Proxy サーバでウィルスチェックを行うウィルスチェックソフトの導入を検討しています。これは nimda ウィルスのような Web を見ただけで感染してしまうようなタイプのウィルスに有効です。

Symantec Web Security はそれ自身、Proxy サーバとして動作します。また、FireWall-1 と連携して透過的 Proxy として動作させることも可能です。単体で Proxy サーバとして設定した場合には、Internet Explorer や Netscape などの Web ブラウザで Proxy サーバとして Symantec Web Security のサーバを指定することにより http と ftp プロトコルに対してウィルスチェックをしてくれます。

４．おわりに

以上、現在研究所で行っているセキュリティ対策を紹介してきました。他にもゲートウェイ型のファイアウォールなど色々な製品があります。これからも良い製品はどんどん取り入れて、エンドユーザが安全で使いやすい環境を整えて行きたいと思います。

---

7 http://www.symantec.com/region/jp/products/sws20/index.html