セキュリティ対策のアウトソーシング事例

北，祐一郎
九州大学情報基盤センターネットワーク管理掛

https://doi.org/10.15017/1470655

出版情報：九州大学情報基盤センター広報 : 学内共同利用版. 3 (1), pp.8-13, 2003-03. 九州大学情報基盤センター
バージョン：
権利関係：

セキュリティ対策のアウトソーシング事例

北　祐一郎*

1　はじめに

近年ネットワークは高速化されており、九州大学のネットワークも平成12年度の補正予算により新ネットワーク（ギガビット級ネットワーク）が構築されました。基幹ネットワークは1Gbpsへ、支線ネットワークは各建屋の各階までは1Gbps、その配下は100Mbpsへ生まれ変わりました。非常に高速なネットワークへ変わったわけですが、同時に悪質なウィルスメールやサーバに対するクラッカーの攻撃による被害が年々増加しているという現実も考慮しなければなりません。ウィルスに感染したりサーバをクラックされれば、被害は自分だけでなく九大内の他の部局、或いは他大学や企業、一般の方へも及びます。

これらの被害を防ぐためには利用者や管理者の意識改革が必要で、今後はインターネットを使用するにはコンピュータをネットワークに接続するだけでよいという認識から、セキュリティ対策を行っていなければコンピュータをネットワークに接続してはいけないという認識へと変えていかなければなりません。

とはいえ、サーバ等のセキュリティ対策は支線LAN管理者やサーバ管理者にとって、本来の仕事ではなくボランティアで行っている方が殆どなので、頭の痛い問題だと思います。

情報基盤センターで支線LAN管理者に対してアウトソーシングに関するアンケートを行いましたが、回答者の約半数の方々は「料金によってはアウトソーシングを利用したい」、約３割の方々は「アウトソーシングを利用したい」ということで、回答者の約８割の方々がアウトソーシングを希望しています。特にソフトウェアのバージョンアップやセキュリティ対策の面で管理者に負担がかかっているようなので、アウトソーシングを行えば管理者の負担はかなり軽減されるのではないかと思います。

情報基盤センターはアウトソーシングを行っている部局を把握しているわけではありませんが、ネットワーク障害等で各部局を訪問した際に支線LAN管理者から伺った情報ではアウトソーシングを行っている部局は少ないようです。

そこで本稿ではサーバのセキュリティ対策として、ファイアーウォールやサーバ類のアウトソーシングを行っている大学院薬学研究院へインタビューした結果をもとに、その状況や契約内容を紹介していきたいと思います。

*情報基盤センター ネットワーク管理掛
E-mail:kita@cc.kyushu-u.ac.jp

2　導入前・導入後の状況

今回、サーバ類のアウトソーシングを行っている大学院薬学研究院へ導入前と導入後の状況を簡単にインタビューしました。

本章では、そのインタビューの内容を紹介します。

2.1　導入前の状況

・端末状況

Mac、WindowsPC、ワークステーションを使用しており、Macはメールやワープロ及び実験データの処理が主で、WindowsPCは上記用途の他に計測機器の制御に使用されている。

また、ワークステーションは各講座保有のメールサーバの他に、機器制御用及びデータ解析用に使用されている。

・導入前のサーバ類の管理状況

メールサーバ等を分散して保有管理しており、講座によっては管理者の不足で管理が困難な状況であり、老朽化や容量不足によりトラブルの頻度も高かった。

また、セキュリティホールの情報等は殆ど入らず修正プログラム適用作業も殆ど行われていなかった。

・運用状況

各講座保有のメールサーバにトラブルが高い頻度で起こっていたが、それがアタックによるものかの判別はつかなかった。

しかし、ファイアーウォール導入後のフィルタリング[1]されたパケットの件数によりアタックはかなりあったのではないかと推測される。なお、改竄等の実被害は受けていない。

メールサーバのトラブルの際は各講座の管理者が対処していたが、手に負えない場合は支線LAN管理者が対処していた。

この際、学部内にメールサーバが非常に多数存在していたため、支線LAN管理者の負担は大きかったと思われる。

[1] ここではパケットフィルタリングのことをいい、ネットワーク上のデータを選別し、そのパケットの通過を許可したり拒否したりすること。

2．2　導入後の状況

・導入後のサーバ類の管理状況

メールアカウントの設定、廃止、フォワーディング先の変更、ホームページ作成等の簡単な作業は部局のサーバ管理者が行っている。

一方、セキュリティ情報の提供や修正プログラム適用作業などは部局の担当者が行うには非常に負担がかかるため、契約業者の担当者が来学あるいはリモートにより行っている。

・ファイアーウォールの管理状況

基本的にはファイアーウォールで出口を厳しく制限し、運用を見ながら必要な通信を通過させている。

今までに図書館のデータベースを使用する際や、外部からのPOP3へのアクセス許可などでポートの開放の要望があったが、POP3へのアクセスに関しては出来る限り外部へのメールアドレスの転送により対処してもらうようにした。

なお、ファイアーウォールのポートの開閉は支線LAN管理者と希望者との話し合いで決定し、管理は契約業者が行っている。

下記はファイアーウォールを運用するにあたっての基本ポリシーである。

① 内部から内部へ（133.5.226,227,228）は全て許可
② 内部から外部へは殆ど許可
③ 外部から内部へはホスト指定で最小限のサービスポートのみ許可

・運用状況

フィルタリングされたパケットの件数は導入直後に比べ減少しており、アタックによる実際の被害は起こっていない。

しかし、メールウィルスの被害はファイアーウォールでは防御できないため[2]現在も稀にみられる。

3　契約内容

大学院薬学研究院よりファイアーウォールおよびサーバ類の管理に関する契約内容と保守に関するデータを頂きました。

本章ではその内容を紹介します。

---

[2] ファイアーウォールは一般的にポート番号（メールの送信はSMTP:tcp/25、メールの受信はPOP:tcp/110）あるいはアプリケーションごとに制御するので、例えばtcp/25を閉じてしまうとメールの送信ができなくなるためファイアーウォールでウィルスを防ぐことはできません。

3.1 契約内容

大学院薬学研究院の請負業者は「千代田興産株式会社[3]」で保守契約内容は表1のようになっており、毎月システムのログや障害状況を報告してくれることになっている。

現在大学院薬学研究院が保守契約しているサーバ数は5台である。

表1 薬学研究院の契約内容

請負業者	千代田興産株式会社
請負事項	九州大学大学院薬学研究院メールサーバ等運用支援業務
請負場所	九州大学大学院薬学研究院
対象システム	Mail・DNS・POP3・Firewall・WWWサーバ
請負期間	平成14年4月1日～平成15年3月31日（単年度契約）
業務内容	（1）日々の以下の稼働情報監視と、緊急時の対応 ・システムログ（障害発生メッセージ） ・ディスク使用状況 ・Webサーバへのアクセスログ ・Webサーバでのエラーログ ・メール送受信でのエラーログ ・ルータ、ファイアーウォールでのエラーログ （2）稼働状況をまとめた月次の報告書の提出 （3）電話及びメールでの相談対応 （4）OS設定等のリモートメンテナンス

3.2 保守データ

保守データの報告は月単位で行われており、その作業内容やファイアーウォールのログ等をまとめて報告してくれるようになっている。

以下は平成13年5月の報告例である。

[3]保守契約の金額は規模や契約内容等によってかわりますので、詳細は「千代田興産株式会社」にお尋ねください。
担当者 末金・吉田
TEL 092-533-2983
FAX 092-533-2999

報告例（平成13年5月）

① 全体の運営状況

５月度はsadmind/IISというワーム（ウィルス）が猛威を振るい、国内に設置されているSolaris, WindowsのServerで多数の被害が発生しています。

貴部門のServerの安全な運営を図る上で、主要なSoftwareの更新を実施しました。

② サーバの運営状況

サーバの運営上で、大きな問題はありませんでした。

③ 作業内容

5/23	bind-8.2.4 への更新（ Rigel, Vega ）
	apache-1.3.20 への更新（ HomePage ）
	ntpd-4.0.99k23 への更新（ HomePage ）
	Firewallのフィルタリング定義変更
5/28	Firewallのフィルタリング定義変更（ PHS関連のMailトラブル対応 ）

＊ソフトウェアのバージョンアップはCERTやCERT-JP、ディストリビュータ、各オープンソフトプロジェクトからの情報をもとに契約業者が実施しています。

情報が公開されて数日以内に契約業者から大学院薬学研究院へアップデートの許可申請があり、許可が下りると契約業者がアップデートを行います。

ただし、緊急性かつ重要性の高いものについてはアップデート後に報告がくることもあります。

④ ファイアーウォールによるフィルタリング状況

５月度にFirewallでフィルタリングされたパケットのレコード件数は、2,469,174件でした。

４月度と比較して1,900,000件ほど大幅増加（約４倍）しています。

上記フィルタリングされたパケットの内訳は下記の通りです。

TCPパケット	62,944 件
UDPパケット	2,396,590 件
ICMPパケット	9,640 件

4　おわりに

今回、サーバのアウトソーシングを紹介しましたが、これでセキュリティが完全に守られるわけではありません。例えばウィルスメールはファイアーウォールを導入したり、サーバのセキュリティを向上しても防御することはできないため、別途ウィルスチェックソフトが必要で、さらに毎日ウィルスパターンファイルのアップデートが必要になります。

このように今やセキュリティの問題はネットワークを使用する上で切っても切り離せない問題となっています。

しかしながら、クラッカーによる攻撃等は基本的に弱点がありそうなコンピュータを探し出してそのコンピュータへ攻撃するわけですから、サーバのアウトソーシングを行うことでセキュリティが強化されれば、攻撃やクラックされる可能性は少なくなると思います。

セキュリティ強化を行うと、それに比例してコストが上がり使い勝手も悪くなるためどこまでセキュリティを強化すればよいかというのは判断が難しいところではありますが、今後の管理の選択肢のひとつとして本稿で紹介したアウトソーシングを考えて頂ければと思います。

最後に、本稿を執筆するに当たってご協力頂いた大学院薬学研究院の方々に感謝致します。