セキュリティガイドラインの策定

山田 真介* 八木 秀樹 アフマド ルリィ 岩田 一

早稲田大学メディアネットワークセンター

1 はじめに

早稲田大学メディアネットワークセンター（以下、MNC）では、研究室や事務所などの諸機関に対して自主管理を条件に IP アドレスやネットワークを年度単位で貸与し、自由度の高いネットワーク環境（以下、自主管理ネットワーク）を提供している。自主管理ネットワークを利用することで学外から学内にいるときと同じように研究活動を行うことができ、研究成果を世界に向けて発信することも可能になる。一方、その便利さと引き換えに学外からの攻撃を受けることになるため、適切に管理・運営していくことが必要である。

これまで MNC では、ネットワーク情報管理システムの導入 [1, 3]、IP360 を用いてインシデントを起こしたサーバに対する再発防止策 [2] などを行ってきた。しかしながら、自主管理ネットワークでセキュリティインシデントを起こすサーバやクライアントは減少していない（図 1）。どのようなインシデント事例が多いかを調べてみると、管理者がいない場合や、経験のない人が管理している場合が多く、2005 年度は、適切に管理していれば防ぐことのできた SSH のブルートフォースアタックによりクラックされた事例が目立つ。

大学では、人の入れ替わりが激しく、管理者が卒業したり、それまで管理経験のない人がいきなり管理者を任されたりする状況を避けられないことも多い。また、研究室では、研究の片手間にネットワークを管理している場合がほとんどであり、インシデントが発生するまでは何の対策も取られていないことも多い。そのため、経験のない管理者がどのようにインシデント対策を立て、運用していけば良いのかを知る手助けとなるようなガイドラインが必要となる。ところが、既に公開されているのガイドラインやセキュリティポリシーは、基幹ネットワーク等で適用するようなものが多く、未熟な管理人でも対処がしやすいと思われるガイドラインは見当たらない。そこで、MNC ではネットワーク管理を行う上で指針となるセキュリティガイドラインの策定に着手した。本発表では、ガイドラインの概要と策定にあたって注意した点について報告する。

*shinsuke@mnc.waseda.ac.jp

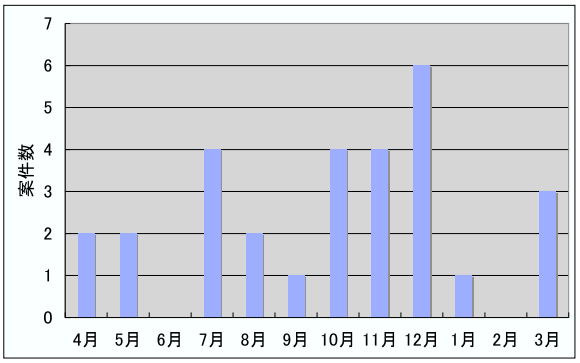

図 1: 2005 年度 Abuse 案件数

2 ガイドラインの目標と策定過程

既に述べたように、セキュリティガイドラインの目標は、ほとんど経験のない管理者に対して実行可能なガイドラインを簡潔に示すことである。研究室の学生が管理者することを念頭において策定にあたったが、個人的に運用しているような小規模ネットワークの管理者にも適用できるよう注意を払った。なお、本ガイドラインでは、MNC 助手である筆者らの他にも MNC の職員や早稲田大学 IT センターの職員が共同で策定にあたった。

3 ガイドラインの概要

今回我々が策定したガイドラインは、A4 で 6 ページ程度の分量で、大きく分けて 3 つの節からなる：

- はじめに
- 情報機器の運用について
- 緊急時対応について

以下、各節の概要について紹介する。

3.1 はじめに

本節では、ガイドラインの目的や次節以降の構成、種々の用語の定義（管理者、利用者、関連機関、情報機器）について説明している。用語の定義にあたっては、早稲田大学の学内に特化した記述とならないように注意し、外部のネットワーク管理者でも参照しやすいよう心がけた。

3.2 情報機器の運用について

本節は、平常時の運用の指針となるものであり、具体的には、以下の 7 項目について説明している：

- 運用体制表（組織表）の作成
- ドキュメントの作成
- 後継者とユーザの教育
- 情報収集
- 狭義のセキュリティ対策
- ドキュメントの定期的更新
- 申請情報の更新

ここでは、詳細なセキュリティ対策ではなく、インシデント情報なども含んだ情報共有の重要性を強調するように心がけた。

3.3 緊急時対応について

パッチ等の適用や情報共有が適切に行われていたとしても、新たな手法で攻撃されて被害を受けてインシデントが発生することも十分に考えられる。本節では、そのようなインシデントが起こった場合にどのような対処をすれば良いのかについて以下の 5 項目に分けて説明している：

- インシデントの定義
- 緊急対応（アクション）
- 報告
- 調査
- 今後への対策

MNC では、インシデントを起こした管理者からインシデントの原因や再発防止策についての報告書の提出を義務づけているが、その報告書からは経験の浅い管理者ほど対応に苦慮している姿が浮かび上がる。そのため、インシデント発生時のフェーズを 3 つに分け、各フェーズ毎にどのような対処をすれば良いかが明確にするように注意した。

4 おわりに

本発表では、経験の非常に浅い管理者をターゲットとしたセキュリティガイドラインについて述べた。本ガイドラインの特徴としては、技術的な側面よりも情報共有やインシデント発生時の対応を強調するようにしたことが挙げられる。特に大学の研究室では、人の入れ替わりも激しく、情報共有のなされていないことが多いため、この特徴は大変重要であると考えている。本学がこれまで行ってきた対策にガイドラインが新たに加わったことで、これまで以上にインシデント発生の芽を摘むことができるようになるものと期待される。しかしながら、セキュリティホールに対して開発者たちが対策を講じ、同時に悪意のあるユーザーたちも手を替え品を替え新たな攻撃方法を考える、という状況に変化が訪れるとは少なくとも現状では考えられない。そのため、これまでの対策に加え、インシデント発生を水際で防ぐ方策を考えることが今後の課題である。

謝辞

早稲田大学 IT センター佐藤雄一氏より、2005 年度 Abuse 案件数についてのデータを提供して頂いたことに感謝いたします。

参考文献

[1] 渥美章佳、赤城剛朗、新城直樹、小泉大城、アフマドルリィ、「キャンパスネットワークに置けるセキュリティ確保とネットワーク情報管理について」、平成 16 年度情報処理教育研究集会、名古屋大学、2004 年 11 月

[2] 小泉大城、新城直樹、若林久芳、「早稲田大学における学内ネットワークセキュリティ保全について」、2005PC カンファレンス、新潟大学、2005 年 8 月

[3] 八木秀樹、アフマドルリィ、山田真介、岩田一、「学内ネットワークにおけるセキュリティ確保のための情報管理」、2006PC カンファレンス、立命館大学、2006 年 8 月