ネットワークセキュリティ総合監査とその評価

萩原 洋一，佐藤克巳，美宅成樹

東京農工大学 総合情報メディアセンター

概要

東京農工大学では、学内ネットワークに対する「ネットワークセキュリティ総合監査」を実施した。この監査は、外部監査、内部監査および体制監査を通じて情報セキュリティの主な問題点を把握すると共に、情報セキュリティポリシーを策定し、対策を実施する上で留意すべき点を明らかにすることを目的とした。この監査は、①インターネット経由の不正侵入、②内部関係者による不正侵入や踏み台としての利用、③日常の管理体制・手続、問題点が発見された時の対応などの観点から総合的に調査することを目的とした。

Network security synthesis audit and its evaluation

HAGIWARA Yoichi, Sato Katsumi, Mitaku Shigeki

General Information Media Center, Tokyo University of Agriculture and Technology

Abstract

In Tokyo University of Agriculture and Technology, "network security synthesis audit" to an intramural network was carried out. This audit aimed at clarifying the point that it should mind when coping with it by deciding upon information Security Policy, while grasping the main problems of an information security through an external audit, an internal audit, and organization audit. This audit aimed at conducting the following investigations. 1. Unauthorized entry method via the Internet. 2. Unauthorized entry by the internal persons concerned, and use as step. 3. Method of correspondence when everyday management organization, procedure, and problem are discovered.

1. はじめに

東京農工大学では､学内ネットワークに対する｢ネットワークセキュリティ総合監査」を実施した。この監査は、外部監査、内部監査および体制監査を通じて情報セキュリティの主な問題点を把握すると共に、情報セキュリティポリシーを策定し、対策を実施する上で留意すべき点を明らかにすることを目的とした。

ネットワークセキュリティ総合監査の結果は、次に行うべきリスク分析や情報セキュリティポリシー策定における重要な基礎情報であり、リスクの発掘につながるものでなければならない。したがって、単に、サーバやネットワークが有している脆弱性の指摘に留まらず、そうした問題点が発見された場合の対応の具体的方法、そして、その体制的問題点の抽出、および、遡及して指揮系統などの管理体制に潜在する脆弱性まで含めて明らかにされなければならない。

2. 監査概要

(1) 入札： 一般競争入札
(2) 実施期間： 2001 年 12 月 4 日(火)～21 日(金)
(3) 監査結果報告会： 2002 年 1 月 17 日(木)
(4) 調査対象：
・外部監査 308IP アドレス
(スクリーニング解除申請のもの)
・内部監査 7 セグメント
・体制監査 5 名インタビュー
(センター関係者 4 名、情報学科１名)
(5) 監査者：
インターナショナル・ネットワーク・セキュリティ株式会社 監査責任者 石井宏幸、他 5 名

3. 監査方法

ネットワークセキュリティ総合監査は、「外部監査」、「内部監査」および「体制監査」をあわせて実施する監査である。

「外部監査」とは、不正侵入者と同等の立場に立ち、インターネットからアクセス可能な大学内ネットワーク上のコンピュータへの不正侵入の可能性等、探査し得るすべてのセキュリティホールの検証およびその対策を提示する検査である。

「内部監査」とは、大学内ネットワーク上のコンピュータから大学内外のサーバ等に対する不正侵入の可能性等、探査し得るすべてのセキュリティホールの検証およびその対策を提示する検査である。

「体制監査」とは、問題点の予防や発見された問題点への対応方法などの管理体制に関する問題点およびその対策を提示する検査である。

3.1 外部監査

(1) 調査用コンピュータの設置場所
- 監査会社の社内ネットワーク上
- インターネット経由で対象 IP アドレスに対して調査。

(2) 調査対象
- スクリーニング解除申請が出ている 308IP アドレス(大学から事前に提示)。

(3) 調査方法(簡易調査)
- ICMP を用いたアクセス確認ならびに経路調査。
- TCP ポートに対するアクセス確認。
- 送信元ポート番号を偽造した場合の TCP ポートに対するアクセス確認。
- アクセスが可能な TCP ポートに対するバナーチェック。
- DNS サーバに対し、ゾーン転送の可能性、登録内容の妥当性ならびに外部かのアクセスの必要の調査。

(4) 調査方法(詳細調査)
- ユーザ認証を伴うサービスへのアクセスが可能な場合、ユーザ ID およびパスワードの推測を行い、正規ユーザに成りすました侵入の可能性。
- 簡易調査で列挙した脆弱性に対する攻撃の可否
- Web サーバについては、既知のセキュリティ上の問題点が指摘されている CGI および ASP プログラムの存在。
- Ftp サーバについては、匿名接続(anonymous 接続) の可否、および、接続が可能な場合、ディレクトリやファイルへのアクセス制御。
- Smtp サーバについては、不正中継の可否。

3.2 内部監査

(1) 調査セグメント
工学部情報コミュニケーション工学科、工学部電気電子工学科、独立大学院(BASE）棟、事務局、附

属図書館、総合情報処理センター
(2) 調査対象
調査用コンピュータを設置したセグメント上に接続されている全てのコンピュータ、ネットワーク機器。
(3) 調査方法
外部監査と同様に簡易調査、詳細調査を実施した。

3.3 体制監査
(1) インタビュー対象者
- 総合情報処理センター 4 名、情報学科 1 名

(2) 調査項目
- ユーザ ID、パスワードの管理
- ユーザ認証およびデータへのアクセス制御
- サーバ設置およびアクセス制御
- サーバの管理
- 文書管理
- 監査・監視
- 運用手順・手続き
- 教育・トレーニング

4. 監査結果

4.1 外部よりアクセス可能なサービスポート
4.1.1 外部から主なサービスポートへのアクセス可能な機器数

protocol	port	台数
ftp	21/tcp	52
ssh	22/tcp	26
telnet	23/tcp	41
smtp	25/tcp	47
dns	53/tcp	32
http	80/tcp	41
pop3	110/tcp	32
sunrpc	111/tcp	34
https	443/tcp	4
X11	6000/tcp	6

*スクリーニング解除 308 台中

4.1.2 主なサービスポートの管理状況
(1) ftp (21/tcp)
- 52 台中、8 台の機器で匿名接続(anonymous)が可能だった。
- 約 2/3 の機器で脆弱性が報告されているバージョンを使用していた。
- 新しいバージョンを使用している機器の多くは、tcp_wrapper などによるアクセス制御が設定されていた。

(2) telnet (23/tcp)
- finger コマンドを用いて取得したログイン中のユーザ ID のパスワードがユーザ ID と同じ 機器があった。
- デフォルト設定のユーザ ID にパスワードが設定されていない機器を 1 台確認した。
- 41 台中、16 台の機器で ssh(22/tcp) も稼動。
- 約半数の機器で、tcp_wrapper などによるアクセス制御が設定されていた。

(3) smtp (25/tcp)
- 47 台中、6 台の機器で電子メールの不正中継が可能であることを確認した。

(4) dns (53/tcp)
- 32 台中、6 台の機器で脆弱性が報告されているバージョンを使用していた。
- ゾーン転送が可能な機器を 1 台確認した。

(5) http (80/tcp)
- マイクロソフト社の IIS を利用している機器を 6 台確認した。詳細調査対象の 2 台は修正プログラムが適用されていた。

4.1.3 体制監査の結果
(1) コンピュータ等への学外からのアクセス設定(ファイアウォールの設定) は、申請により実施している。しかし、ポート単位での申請は少なく、多くの場合、IP アドレス単位でのアクセス許可申請となっている。
(2) 基本的に申請通り許可(設定)しており、申請内容に対する指導もしくはアドバイスは行っていない。ただし、NetBIOS をはじめ udp を含めた 32 ポートは、強制的に通信を禁止している 。

4.2 学内機器に対する管理
4.2.1 内部監査の結果
(1) Windows サーバへの侵入
Windows は NetBIOS を利用することにより、登録されている全てのユーザ情報を入手することができる。入手したユーザ ID に対してパスワード推測を行ったところ、管理者権限を有しているにも関わらずユーザ ID と同じパスワードを設定している

ユーザ ID が存在していた。
(2) ネットワークプリンタ等へのアクセス
ネットワークプリンタやネットワーク機器にはリモート管理機能を有しているが、多くのプリンタで初期パスワードが設定されていない。今回、5 台のプリンタと 1 台のネットワーク機器への接続に成功した。

4.2.2 体制監査の結果
(1) PC 教室およびメールサーバなどでも、パスワードの定期的な変更、推測が困難なパスワードの設定など関して、ガイドラインや講義での啓蒙は行われている。しかしながら、システム的な制約がないため、ユーザにとって、パスワード管理の重要性を認識していないと考えられる。
(2) 総合情報処理センター内システムの利用方法やウイルス等のセキュリティ情報が web サーバ上で公開されているが、研究室のサーバ管理者に対して、サーバを管理する上で必要となる情報提供が不十分である。
(3) 総合情報処理センターの教職員を含め、研究室や事務局の管理者が学外(企業)主催のトレーニングを受講する機会が制度としてない。

5. 監査結果に対する評価と改善提案

5.1 評価

5.1.1 外部監査結果総評
(1) 学外からのアクセスが不要と思われるサービスポートへのアクセスが可能な機器が多数存在した。
(2) 学外から、メールの不正中継をはじめとする不正侵入・攻撃を受ける可能性が高い機器が存在する。
(3) 各機器に対する対策は言うまでもなく、学外との接続部分のファイアウォールの設定ルールを根本的に見直す必要がある。

5.1.2 内部監査結果総評
(1) 部署による管理レベルの差が顕著に現れていますが、全体的な傾向として、不要なサービスポートへの対策が疎かになっている。
(2) 複数のサーバへの侵入が可能であった。
(3) アクセス管理が不備なネットワークプリンタが多数確認できた。
(4) 機器導入時の基本的なセキュリティ対策の全学的な浸透が急務である。

5.1.3 体制監査結果総評
(1) 管理内容や決定プロセスに、個人に強く依存している部分が多く存在している。
(2) これは、研究・教育としての業務(作業) と、組織としての管理業務(作業) が明確に分離されていないことに起因すると判断した。
(3) 各機器の管理者の技術レベルを一定レベルに底上げするとともに、その維持のための仕組みが必要である。

5.2 改善提案

(1) 外部からのアクセスを許可するサービスポートの制限
研究・教育的用途を考慮しても、外部からアクセスする必要のあるサービスは、極少数に限られる。現状でも、強制的にアクセスを拒否しているサービスもあるが、逆に極少数のサービスの中から、さらに必要なもののみを申請により許可する方法の導入を薦める。
(2) 機器導入時のセキュリティ対策の徹底
メールの不正中継、DNS のゾーン転送、デフォルト設定ユーザ ID などの問題は、機器もしくはサービスを導入した際の初期設定操作の不備に起因する。外部からのアクセスを許可する機器の技術的要件を明確にし、導入時および定期的に準拠性を調査すること。
(3) DNS・メール運用管理
1 つの組織において各 DNS サーバに外部から直接アクセスできる必要はない。プライマリおよびセカンダリサーバのみアクセスを許可し、他の DNS サーバの登録内容への参照が必要な場合は、セカンダリ設定により学外からの参照に対応すること。メールに関しても、学内外で送受信する全てのメールを特定の代理(proxy) サーバを経由させ、各サーバへ学外から直接アクセスを禁止することを勧める。
(4) 送信元 IP アドレスによるアクセス制御
ftp, ssh, telnet に対しては、tcp_wrapper などにより、送信元 IP アドレスによるアクセス制御を義務付ける。
(5) ネットワーク接続機器の技術的要件の整備

サーバおよびクライアントについての最低限のセキュリティ要件を明文化し、新規接続時および定期的に要件を満たしていることを調査することを勧める。これは、研究室と総合情報処理センターのセキュリティ管理領域を明確に分離する上でも必要となる。

(6) 管理者向けセミナーの実施

研究室の管理者(主に学生)を含め、ネットワーク接続機器の管理に携わる人を対象とした教育が必要である。高額・長期間の受講は非現実的なので、総合情報処理センター主催のセミナーを開催し、管理者の受講を義務付ける方法が考えられる。

6. 提言

6.1 提言１　「情報」の扱い

(1)「情報(データ)」の所轄部署が管理責任を負う。

(2) 「情報」の管理とは、情報の追加、修正、削除、保管、バックアップなど。

(3) 何をしなければならないのか？

(4) 情報(データ) の所轄部署の明確化

(5) 情報の価値と重要度(機密性、可用性、完全性)の明確化(価値と重要度に依存した管理策の決定)

(6) 価値と重要度の決定は所轄部署。各情報の価値と重要度の妥当性を評価する仕組みが必要。

6.2 提言２「情報を扱う環境」の管理

(1) 学部・学科・研究室と総合情報処理センターの責任範囲の明確化。

(2) 研究室セグメント内は研究室において管理（ただし、全学的なセキュリティレベルの維持のために、ある程度の制限は必要)。

(3) 事務部門と総合情報処理センターの責任範囲の明確化。

(4) 中途半端な管理分担は、管理作業を煩雑にするだけでなく、セキュリティレベルの低下を招く。

(5) 事務部門内に管理のための専任部署を設けることができない場合、全面的に総合情報処理センターに管理を任せる。

6.3 提言３　組織体制

全学的な管理体制の整備、学生の位置付け。

(1) 全学的な管理体制の整備

少なくとも、『 情報セキュリティ管理』に関しては､既存の教官組織､事務官組織の枠組みを超えた、新しい管理組織体制を整備し、その体制の下で管理枠組み(ISMS: Information Security Management System) を 確立する必要がある。

(2) 学生の位置付け

学生も大学の構成員であり、情報と情報環境に関しては一定の関わりがある。さらにリスクの発生原因の比重は職員以上である。

セキュリティ管理は、専攻分野に関わらず、社会人としての必須要件となっていますので、教育の一環として、職員と同様に、大学の構成員としてセキュリティポリシーの対象に加えるべきである。

6.4 提言４　ISMS の構築

・ISMS(Information Security Management System) 構築を前提としたセキュリティポリシーの作成

6.5 提言５　大学におけるセキュリティ管理モデル

(1) 教官・事務官を横断した大学としてのセキュリティ管理を検討・決定する委員会、および、セキュリティ管理の統括責任者の設置が不可欠である。（図１．参照）

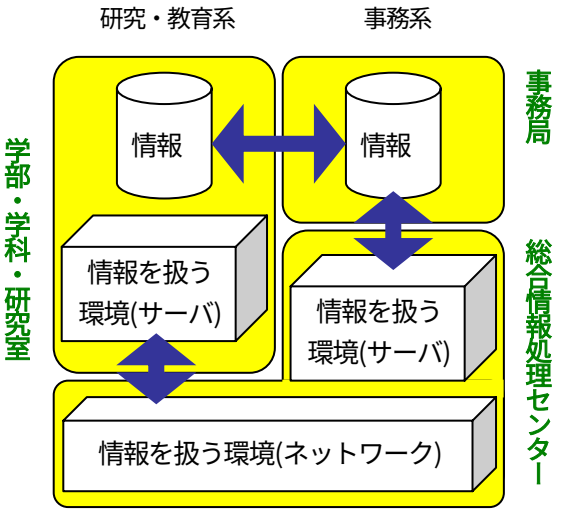

図１．大学におけるセキュリティ管理モデル

7．今後の展開における視点

(1) 今回の監査で得られた課題の中で、優先度の高いもの(緊急性、実現可能性に基づいて判断)に対

策の力を入れる。
(2) その効果は、計画・-実行・チェック・見直しを繰り返して充実させる。
(3) セキュリティに強い人材育成を計画的に推進し、リーダグループを作る。
(4) ポリシー定着に向けた、教職員、学生に対する教育プログラムの準備と教育の通年化を実施する。
(5) 単なるアウトソースや全て自前で行うよりも、必要に応じて、コンサルタントなどの外部の力を活用する。

参考文献

[1] 東京農工大学ネットワークセキュリティ総合監査報告書，インターナショナル・ネットワーク・セキュリティ(株)，2002.01.17
[2] 情報セキュリティポリシーに関するガイドライン，情報セキュリティ対策推進会議，2000.07.18
[3] 大学の情報セキュリティポリシーに関する研究会，(事務局) 国立情報学研究所，http://www.sinet.ad.jp/info/policy/index.html
[4] 大学における情報セキュリティポリシーの考え方, 大学の情報セキュリティポリシーに関する研究会，2002.03.29，http://www.sinet.ad.jp/info/policy/tousin.html
[5] 情報セキュリティポリシーに関するガイドライン，金沢大学総合情報処理センター，2000.02.06，http://www.ipc.kanazawa-u.ac.jp/
[6] インターナショナル・ネットワーク・セキュリティ株式会社，http://www.insi.co.jp/
[7] CRL通信総合研究所非常時通信グループ，不正アクセス関連情報 http://www2.crl.go.jp/jt/a114/incident_top.html
[8] 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律，総務省 http://www.soumu.go.jp/joho_tsusin/top/denki_h.html