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

小泉 大城　　新城 直樹　　若林 久芳

早稲田大学メディアネットワークセンター*

{dkoizumi, aragusuku}@mnc.waseda.ac.jp, h.wakabayashi@waseda.jp

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) は学内の情報利用環境の整備や提供を行う組織であり，学科や研究室等の学内組織に教育・研究の目的に限り，年度更新にて自主管理ネットワークの利用サービスを提供している．しかしながら，不正アクセスやコンピュータウィルスなどのインシデントによる被害は後をたたず，セキュリティ保全には多くの課題がある．そこで本学では，こうした不正アクセス手口の高度化やコンピュータウィルス被害の大規模化等への対策のひとつとして，2004 年度より脆弱性チェックツールによるリスク診断の試みを始めた．具体的には，自主管理ネットワークの年度更新手続きの際に，脆弱性チェックツールによる診断を行い，セキュリティ上の脆弱性を数値化したスコアに基づいてセキュリティレベルの把握を行うというものである．そして，スコアがある一定以上のネットワークに対しては個別にセキュリティ対策の指導を行うことによって，従来より効率的な学内ネットワークのセキュリティ保全を目指すものである．本稿ではこのような本学における取り組みについて実例を交えて紹介を行う．

2 本学のネットワーク環境およびその問題点

2.1 本学の自主管理ネットワーク

本学の学内ネットワークの運用とその問題点については [1] に詳述されているが，現在もそれほど変わりないためここでは概略のみを述べる．MNC は学科や研究室あるいは研究所などの学内の組織に対し，研究・教育の目的に限り年度更新にて自主管理ネットワークの利用サービスを提供している．たとえば，ある学内組織からの自主管理ネットワークの利用申請があると，MNC は organization.waseda.ac.jp のようなドメイン名および複数個のグローバル IP の利用環境を年度更新にて提供するというものである．これによりこの学内組織は，organization.waseda.ac.jp なるドメイン名を使って DNS やメール, Web 等のサービスを自主的に運用することができる．このようなサービス提供は本学に限らず，各大学でも行われているものと思われるが，残念ながらこの環境の不適切な運用や管理体制の不備等が原因で，不正アクセスやコンピュータウィルスの被害は後をたたない．

2.2 自主管理ネットワークにおけるインシデントの原因と対策

[1] によれば，前節で指摘したようなインシデントの発生原因として以下の 3 つが挙げられている：

- 利用者がセキュリティ対策を行っていない
- 自主管理ネットワークの管理情報等を MNC が把握していない
- MNC が事前に不正アクセスを防ぐことが困難である

上記のうち 2 番目の原因については，従来は紙ベースの事務処理で行っていた管理情報のやりとりを Web データベースを用いた「ネットワーク (N/W) 情報管理システム」を活用するという方針のもと，2003 年度より同システムの開発を開始した．このシステムは 2005 年度より本格的な運用を開始している．

3 番目の原因については，本学のネットワーク環境の規模の大きさもあり，直接的な対策は難しいため，学内の自主管理ネットワークの管理担当者を対象に講義形式にてセキュリティセミナーを開催し，利用者に対しセキュリティについての意識向上を図ってきた [1].

残る 1 番目の原因については，従来は利用者からの個別の問い合わせがあれば，MNC の担当者が助言等を行う形式を取ってきた．しかし，利用者からみると，MNC としてのセキュリティに対する基準や考え方等が必ずしも明確でなく，一貫性に欠けるという問題があった．そこで MNC では 2004 年度より脆弱性チェックツールを試験的に導入し，このツールがネットワークの脆弱性を数値で算出したスコアを使ってネットワークの利用状況を把握し，利用者のセキュリティ対策のレベル向上に役立てると共に学内ネットワーク保全を目指す，という試

*169-8050 東京都新宿区戸塚町 1-104 TEL:03(3203)6301

みを始めた．次章ではこの脆弱性チェックツールについて紹介する．

3 脆弱性チェックツール

3.1 脆弱性チェックツールの概要

本稿では「脆弱性チェックツール」を,「ネットワークのセキュリティを診断するハードウェア，ソフトウェア，またはその両方」，という意味で用いている．しかし，その名称は必ずしも統一されているわけではなく,「セキュリティ診断ツール」「セキュリティスキャナ (Security Scanner)」などと呼ばれることもあるようである．現在利用されている脆弱性チェックツールの主な仕様としては，ネットワーク経由にて診断対象となるサーバにパケットを送信し，接続要求への応答を分析することで脆弱性を診断するものが多いようである．このような脆弱性チェックツールには無償のものと有償 (商用) のものがあるが，前者はソフトウェアで提供されるものが多く，後者はハードウェアとソフトウェアの両方で提供されるものが多いようである．

無償の脆弱性チェックツールとしてよく知られているものには，

- Nessus Open Source Vulnerability Scanner [3]
- Nmap - Free Security Scanner [5]
- Nikto Web Scanner [4]

などがある．いずれもソフトウェアの形式にて無償で提供されている．Nmap は多機能な port scanner で，さまざまな種類の port scan 手法によって診断が行える．Nessus は port scan の他にサーバソフトや CGI の脆弱性診断も行える総合的なチェックツールである．また，Nessus は Nmap や CISCO 社製品等の診断プラグインを組み込むことができ，柔軟性に富んでいる．Nikto は Web サーバのみの脆弱性診断が可能である．図 1 は Nmap の実行例である (IP アドレスや FQDN は架空のものである)．目的のホストに対してスキャンを行うと，開いているポートの情報が出力されているのがわかる．

MNC においては，当初 (2003 年度) は Nessus のテスト運用を行ったが，Nessus 自体の脆弱性チェックの機能は十分であるものの，適切なオプションを設定しないと調査対象のホストがダウンすることがあった．また，Nessus 自体には出力結果のデータベース化の機能がなく，トータルの運用コストを軽減することが難しい点などを考慮した結果，2004 年度中に商用の nCircle IP360^{TM1}[2] を導入することとなった．しかし，上記に

[1] nCircle および IP360 は米国 nCircle Network Security 社の商標である．

```
% nmap -O -sS 133.9.x.x
Starting nmap 3.50 ( http://www.insecure.org/
nmap/ ) at 2005-06-11 01:46 JST
Interesting ports on test.waseda.ac.jp (133.9
.x.x):
(The 1651 ports scanned but not shown below a
re in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
106/tcp   open  pop3pw
110/tcp   open  pop3
143/tcp   open  imap
5680/tcp  open  canna
22273/tcp open  wnn6
Device type: general purpose
Running: FreeBSD 4.X
OS details: FreeBSD 4.6.2-RELEASE - 4.8-RELEA
SE
Uptime 25.575 days (since Mon May 16 11:58:59
2005)
Nmap run completed -- 1 IP address (1 host up)
 scanned in 18.349 seconds
```

図 1: Nmap の実行例

ついては運用方針に多分に依存することでもあり，ネットワークの脆弱性チェックを行うという目的に関して，上記で挙げた無償のソフトウェアが機能的に不足であるということは決してないことを強調しておきたい．

3.2 MNC が導入した脆弱性チェックツール

MNC で導入した nCircle IP360 ^{TM}[2] は，米国 nCircle 社の製品で，専用のハードウェアとソフトウェアで構成される脆弱性チェックツールである．ハードウェアとしては，脆弱性チェックを行う「Device Profiler」，チェックの結果を管理したり，最新のセキュリティ情報をインターネット経由で自動的に入手したり，侵入検知を行ったりする「VnE Manager」，侵入検知のルールの自動修正を行う「Threat Monitor」という 3 種類から構成されている．大きさは最大のものでも 19 インチラックマウント 2U 程度であり，ほとんどの操作は Web ブラウザを使って SSL 経由で接続して行うことができる．機能についての詳細は割愛するが，本稿で取り扱う Device Profiler の主な特色として以下が挙げられる：

- 脆弱性診断時に相手ホストにかかる負荷が比較的少ない
- 脆弱性のリスクがスコアによって数値化されて出力される

まず，1 番目のホストにかかる負荷という点についてであるが，たとえば Nessus では目的のホストを調査するときに設定画面にて「Enable all but dangerous plugins」というオプションをチェックしていない場合，ホストに

かなりの負荷をかける調査を実行する．場合によってはこれが原因で調査対象のホストがダウンする，という現象が MNC 内部でのテスト運用時に散見された．同様に Nmap でも場合によっては実行時のオプション設定に注意する必要性があるものと思われるが，IP360 を使うことでこのようなリスクにある程度対応できる可能性がある．

2 番目の脆弱性のスコアによる数値化という点について，Nessus や Nmap は開いているポートや脆弱性を一覧表示するのみなのに対し，IP360 では一覧表示に加え，脆弱性の深刻度やその脆弱性が発見されてからの時間などをパラメータとして個々の脆弱性の細かい数値化を行い，スコアを算出することが可能である．nCircle 社によれば，このスコア ($Score$) の算出式は以下のようになっている．

あるホストに N 個 $i = 1, 2, \cdots, N$ の脆弱性が存在するとする．個々の脆弱性について，t_i をその脆弱性が公開されてからの日数，r_i をその脆弱性の深刻度 (6 段階)，s_i をその脆弱性を突いて攻撃をするためのスキルの難易度 (6 段階) として，そのホストの脆弱性の $Score$ を以下で算出する：

$$Score = \sum_{i=1}^{N} V_i, \quad (1)$$

$$V_i = \frac{r_i! \sqrt{t_i}}{s_i^2}. \quad (2)$$

式 (2) で示されているように，ある脆弱性のスコア V_i は，その深刻度および発見されてからの時間の関数で評価されている．これは深刻な脆弱性を長く放置しておくほどスコアが大きくなることを意味する．

セキュリティの詳細にそれほど詳しくない利用者にとって，自分の管理しているネットワークについてこのようなスコアを見せられるということは，それなりのインパクトとなる可能性がある．これによって利用者のセキュリティ改善へむけた対応が促進されることにつながるのではないかと予想される．次節で本学 MNC における運用例を示す．

3.3 MNC における脆弱性チェックツールの運用例

本節では，IP360 の本学 MNC における実際の運用について例を挙げて説明する．(ただし，以下の例については，セキュリティ上の理由により部分的に改変を行っている．)

ある学内組織は，長年，自主管理ネットワーク内でサーバ運用を行っていたが，ここ数年，学外から不正アクセスをされたり，コンピュータウィルスをばらまいたりというインシデントが頻発していた．そこで，MNC ではこの自主管理ネットワークの管理者の了解を得たうえで，IP360 による脆弱性チェックを行った．その結果，図 2 のような出力を得た．

nCircle IP360 Technical Analysis 2004-11-15

Report Summary

Hosts	1	Vulnerabilities	38
Asset Value	0	Applications/Services	15
Average Host Score	18071	Attack Count	0

Vulnerabilities

Vulnerability	Hosts	Score
Apache Error Log Escape Sequence Injection Vulnerability	1	11154
Apache Chunked-Encoding Memory Corruption Vulnerability	1	2375
ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability	1	1072
Apache Mod ReWrite Rules Bypassing Image Linking Vulnerability	1	928
ProFTPD STAT Command Denial Of Service Vulnerability	1	638
OpenSSH SCP Client File Corruption Vulnerability	1	440
OpenSSH Buffer Mismanagement Vulnerabilities	1	412
OpenSSH Multiple Buffer Management errors	1	412
OpenSSH Reverse DNS Lookup Access Control Bypass Vulnerability	1	172
PHP Post File Upload Buffer Overflow Vulnerabilities	1	105
ISC BIND SIG Cached Resource Record Buffer Overflow Vulnerability	1	90
ISC Bind Version 8 Multiple Vulnerabilities 2002	1	90
Samba SMB/CIFS Packet Assembling Buffer Overflow Vulnerability	1	82
Apache HTAccess LIMIT Directive Bypass Configuration Error Weakness	1	52
NetBIOS Name Table	1	39
BIND Version	1	30
ISC BIND OPT Record Large UDP Denial of Service Vulnerability	1	26
AFP cleartext/no password	1	24
SSHv1 Protocol Available	1	24
Apache Connection Blocking Denial Of Service Vulnerability	1	23
ISC BIND 8 Invalid Expiry Time Denial Of Service Vulnerability	1	18
ISC BIND Negative Cache Poison Denial Of Service Vulnerability	1	12
Apache mod_php Global Variables Information Disclosure Weakness	1	11
Multiple Apache HTDigest and HTPasswd Component Vulnerabilites	1	1
Recursive DNS Available	1	0
FTP Available	1	0
POP3 Available	1	0
POP3 Banner Available	1	0
Identd available	1	0
Apache Remote Username Enumeration Vulnerability	1	0
FTP Banner Available	1	0
Apache WebServer Available	1	0
Auth Available	1	0
SSH Banner Available	1	0
NetBIOS SSN Available	1	0
HTTP Available	1	0
DNS Available	1	0
SSH Protocol Available	1	0

図 2: IP360 による出力例

図 2 に示されているように，IP360 によって算出されたスコアは 18000 点以上となり，MNC による事前の推測とこの組織のサーバの実態が一致した結果となった．MNC の担当者は管理者にこの結果を報告するとともに，サーバの現状の運用形態について問い合わせたところ，導入時に購入したサポート期限が終了しており，セキュリティパッチをあてていない状態で運用を行っていたことが判明した．そこで，MNC では，以下の 2 つのうちどちらかの対策を取るよう提案した：

- 新たなサーバを導入して運用
- 学内で提供しているホスティングサービスに移行

この提案に対し，管理担当者は現在のサーバを早急に廃止し，新たな利用形態を検討すると回答してきた．

上記のような事例は，ネットワークやサーバの管理が年を経るにつれて不十分となる典型的なケースであるが，以前はインシデントが起こらない限りは MNC としても対策を取ることができず，結果的に 2.2 節で述べたような「MNC が事前に不正アクセスを防ぐことが困難である」という場合となることが多かった．しかし，脆弱性

チェックツールを活用することにより，目的のサーバについて脆弱性の詳細な把握を行うことが可能となった．さらに，出力結果をもとに管理者とセキュリティ改善についての具体的な対策を話し合うことができるようになった．また，脆弱性がスコアという数値によって出力されるため，管理担当者の対応が従来よりも迅速であったことも指摘しておきたい．また，別の管理担当者からは「新たに対策を講じたので，再度スコアを測定してほしい」という依頼もあった．

なお，MNC では 2005 年度からこの脆弱性チェックツールの本格的な運用を開始した．具体的には図 3 に示すように脆弱性の診断を自主管理ネットワークの利用更新手続きに組み込み，スコアが基準値を上回る学内組織についてはセキュリティ対策を指導していくようなフローを作成し，運用を行っている．ただし，脆弱性チェックツールの算出するスコアが絶対的に正しいとは限らないと考えられるため，基準値の設定については余裕を持たせたり，新たな OS 等のリリースに合わせて定期的に見直すなどの措置が必要であると思われる．

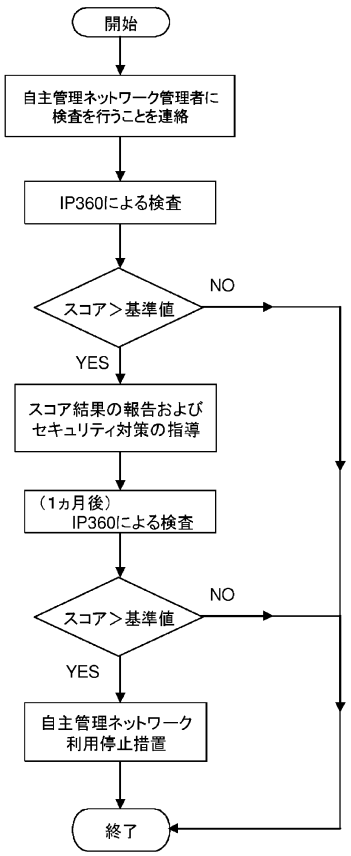

図 3: MNC における IP360 運用のフローチャート

4 まとめおよび今後の課題

本稿では脆弱性チェックツールを利用した学内セキュリティ保全について実例を交えて紹介を行った．脆弱性チェックツールには十分な機能を備えかつ無償のものもあるので，運用を工夫すれば莫大な予算がなくとも効果的なセキュリティ保全を行える可能性がある．本学では有償でかつ脆弱性をスコアで数値化可能なチェックツールを導入しているが，このツールの実際の運用例や，自主管理ネットワークの利用更新手続きのフローに組み込んで活用した例の紹介も行った．今後の課題としては，スコアの基準値のより適切な設定方法の検討や，利用更新手続きのフローを運用する際の効率化の検討，また今回紹介した脆弱性チェックツールとネットワーク侵入検知システム (IDS) とを統合したシステムの検討などが挙げられる．

謝辞

著者らは，本稿の執筆にあたり IP360 の記述について相談に乗っていただいた京セラコミュニケーションシステム株式会社の新井英俊氏，および Nessus の実験を手伝っていただいた早稲田大学非常勤講師の赤木剛朗博士，同メディアネットワークセンターの山田真介助手に厚く御礼申し上げます．

参考文献

[1] 赤木剛朗, 秋岡明香, 渥美章佳, 新城直樹, 伊藤敦, 大前研二, 史虹波, 「学内の自主管理ネットワークのセキュリティ向上を目的としたセキュリティセミナー/アンケートについて」, 第 16 回情報処理教育研究集会, 北海道大学, 2003 年 11 月.

[2] “nCircle IP360,” http://www.kccs.co.jp/security/ncircle/

[3] “Nessus Open Source Vulnerability Scanner Project,” http://www.nessus.org/

[4] “Nikto Web Scanner,” http://www.cirt.net/code/nikto.shtml

[5] “Nmap - Free Security Scanner For Network Exploration & Security Audits.,” http://www.insecure.org/nmap/