低温研ネットワークインシデント報告

技術部先端技術支援室・ネットワーク委員会　千貝　健

1　序

情報システムにおけるインシデントとは、正当な権限を持たない人がコンピュータを不正に利用するようなコンピュータのセキュリティにかかわる事件、出来事の全般を示す [1]。本文章ではもう少し言葉の意味を広げ、「操作ミスなどを含めたなんらかの原因により、研究活動に不可欠であるコンピュータ・ネットワーク資源の円滑な運用が出来なくなること」をインシデントと定義する。低温科学研究所 (以下、低温研) 技術部およびネットワーク委員会では北海道大学情報基盤センターと連携し、このようなインシデントが発生しないように努め、そして、インシデントが発生した場合にその被害の拡大が最小限になるように対応している。2005 年 4 月から 2006 年 1 月まで低温研内で起こったインシデント例、最近 (2006 年 1 月) 多いインシデントを報告する。

2　低温研全体へ影響を与えたインシデント 3 例の紹介

2.1　ウイルス感染

- **発生日時**: 2005 年 5 月 9 日
- **復旧日時**: 2005 年 5 月 11 日
- **復旧までの影響**: 低温研内および低温研外にウイルスメールを無差別に送信した。
- **状況**:　5/9 18:00 頃から低温研内でウイルスメールが流れる。
  この間に低温研内のマシンがウイルスに感染。
  5/9 19:30 感染したマシンが低温研内外にウイルスメールを発信。
  5/9 20:30 情報基盤センターがウイルスに感染したマシンの通信を無効にする。
  5/11 15:00 情報基盤センターに通信を有効にしてもらう。
- **障害原因**: 世界的に WORM_MYTOB.ED (W32.Mydoom.BO@mm, マイトブ) [2] が流行した。通常、ウイルスが添付されたメールは北大メールゲートウェイで検知され自動的に削除されるが、新種のウイルスのため検知されずに低温研内に無差別に送信された。添付ファイルを開いた低温研内のマシンが感染し、低温研内外にウイルスメールを無差別大量に送信した。
- **対処状況**: 低温研内に流れたメールからウイルスの種類を確定。トレンドマイクロウェブサイト [2] にて対処方法を調査。感染したマシンから対処方法に従ってウイルスを削除。情報基盤センターに報告。
- **事後改善策**: 見知らぬところから来たメールの添付ファイルを開くことの危険性を感染したユーザーに説明。所内メーリングリストに警告メールを流す。低温研ウェブサイトの所内専用情報に警告を出す。

2.2 メール送信不可

- **発生日時**: 2005 年 6 月 8 日 8:30 頃
- **復旧日時**: 2005 年 6 月 8 日 10:30 頃
- **復旧までの影響**: 低温研メールサーバ hassaku からメールが送れない。
- **状況**: hassaku の 25 番 (smtp, Simple Mail Transfer Protocol) ポートにアクセスできない。そのため、hassaku からメールが送れない。
- **障害原因**: hassaku のアクセスログを解析した結果、低温研内のマシンから 1 分間に 1 回、メールの送信 (の再チャレンジ) が行われていることがわかった。同一ホストからの短期間アクセスで、アクセス方法が単調なので hassaku はこれを DoS 攻撃 [3] と認定、メール送信に使うポートを自動的に遮断した。しばらくすると hassaku は、自動的に復活するのだが、すぐに同じマシンからアクセスがあるので再遮断を繰り返した。
- **対処状況**: DoS 攻撃を行っているマシンの管理者に連絡。メール送信に失敗して、何度も自動的に再チャレンジしていた。メール送信に失敗した場合の再送信時間間隔を 1 分間に 1 回から 30 分間に 1 回に設定変更してもらう。

2.3 DHCP 使用不可

- **発生日時**: 2005 年 10 月 27 日頃から断続的に
- **復旧日時**: 2005 年 12 月 6 日 16:00
- **復旧までの影響**: 低温研内で、HINES の DHCP サーバから IP アドレスを発行してもらえない場合がある。
- **状況**: HINES の DHCP サーバから IP アドレス (133.87.219.xxx) が発行されない。192.168.11.xxx という IP アドレスが発行される。その状態ではネットに接続できない。
- **障害原因**: 不正な DHCP サーバが稼働していた。
- **対処状況**: windows XP インストール CD-ROM 中にあるサポート・ツールの dhcploc.exe を用いて、動いている DHCP サーバを検索し、不正 DHCP サーバの IP アドレス・MAC アドレスを特定。情報基盤センターに電話し、上記不正 DHCP サーバの IP アドレス・MAC アドレスを伝え、ポート番号を特定してもらい、その情報から部屋を特定。特定した PC から LAN ケーブルを抜く。ここで、ケーブルを抜くと DHCP サーバが見つからなくなる、ケーブルを繋ぐと DHCP サーバが見つかることを確認。
- **事後改善策**: 不正 DHCP サーバが動いていた PC の再設定を 12 月 7 日に行った。設定方法は、図 1 を参照。

3 最近多いインシデント

低温研内で最近多いインシデントはプローブ (スキャン, scan) である。プローブとは、防御に成功したアタックや、コンピュータ/サービス/弱点の探査を意図したアクセスである。低温研内で主に狙われているポートは、21 (ftp, File Transfer), 22 (ssh, SSH Remote Login Protocol), 80 (http, World Wide Web HTTP), 139 (netbios-ssn, NETBIOS Session Service), 1433 (ms-sql-s, Microsoft-SQL-Server), 3306 (mysql, MySQL), 8080 (http-alt, HTTP Alternate) である。このようなプローブは、自動化ツールを用いて広範囲に渡る任意のホストに対して行なわれている。セキュリティ上の弱点

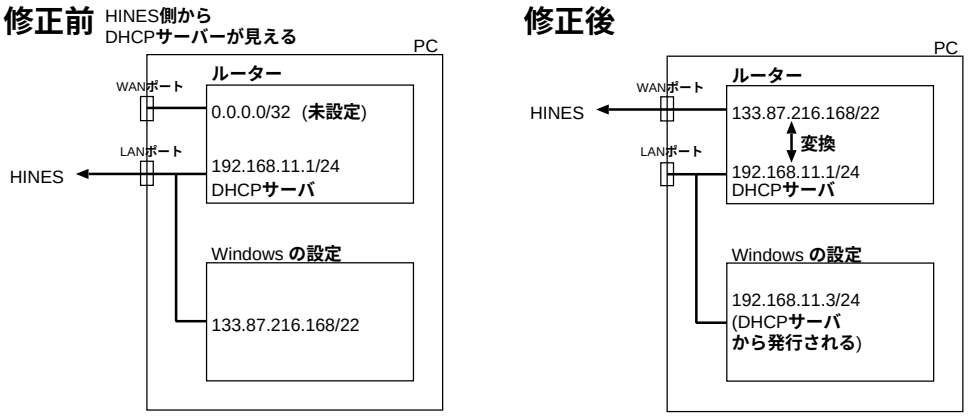

図 1: **不正** DHCP **サーバの再設定**: **ルータ内蔵** PC **で、左図のように** LAN **側のポートを** HINES **側に接続していた為、**HINES **側に** DHCP **サーバが露出していた。内蔵ルータの設定を行い、**WAN **側に接続した (右図)。**

を放置していると、弱点の存在を検出され、ホストへの侵入等さまざまなアタックを受ける可能性があるので注意が必要である。以下では、実際にプローブが行われた際のログの例を示す。

3.1 ssh の例

ssh (secure shell) **とは、主に** UNIX **コンピュータで利用される、ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするためプログラムである。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる** [4]**。そのため、低温研内に設置された自分のコンピュータを、学会等で出張中にも使用できるようにするため、どこからでもアクセスできるように設定している (アクセス制限を行っていない) 場合が多い。**

実際にプローブを受けたマシン (Linux) **のログの一部を示す。このマシンでは、最新版の** SSH **サーバプログラムを使用している以外、全くセキュリティ対策を行っていない。実際の** *hostname* **は、伏字にした。**

/var/log/message **のログ**

```
Jan 26 18:03:27 hostname sshd[14688]:
     Illegal user plant from 210.143.xxx.xxx
Jan 26 18:03:30 hostname sshd[14688]:  Failed password
     for illegal user plant from 210.143.xxx.xxx port 58026 ssh2
Jan 26 18:03:34 hostname sshd[14690]:
     Illegal user ueda from 210.143.xxx.xxx
Jan 26 18:03:37 hostname sshd[14690]:  Failed password
     for illegal user ueda from 210.143.xxx.xxx port 59698 ssh2
Jan 26 18:03:43 hostname sshd[14692]:
     Illegal user ajith from 210.143.xxx.xxx
Jan 26 18:03:45 hostname sshd[14692]:  Failed password
     for illegal user ajith from 210.143.xxx.xxx port 33783 ssh2
...
```

この後、数秒間に 1 **回のアクセスが** 20 **分間続く。**

何度もユーザー名 (太文字で示した) を変えてログインしようとしている。簡単なパスワードを設

定していた場合は、侵入 (intrusion) されていた可能性がある。また、もし最新版のサーバプログラムを使用していなかった場合は、脆弱性を利用されて侵入されていた可能性もある [5]。

以下は、TCP Wrapper を用いて特定のホストからのみ利用できるように制限してあるマシンの場合である。

/var/log/message のログ

```
Jan 26 12:16:55 hostname sshd:
     refused connect from xxxxx.xxxxx.ne.jp (58.81.xxx.xxx)
```

xxxxx.xxxxx.ne.jp からのアクセスが、拒否されている。不特定多数からアクセスされないように、最低でもこれくらいはの設定 (出張前に、出張先のドメイン名等でアクセス制限を設定する) を行って欲しい。ファイヤーウォール (パケットフィルタリング等) を用いて不正なアクセスを検出・遮断すればより良い。

4 まとめ

§2 で紹介した例の原因は、突き詰めれば「ちょっとした不注意 (で添付ファイルを開いてしまった)」「単純な設定ミス (で LAN ケーブルの接続箇所を間違えた)」である。ちょっとした不注意や単純な設定ミスだとしても低温研ネットワーク全体に大きな障害を与える場合があるので、設定の際は慎重さを忘れないようにしなくてはならない。§3 で示したように、敵は毎日こちらの脆弱なところを探して攻撃の隙を伺っている。コンピュータ管理の基本、例えば、システムを常に最新を保つ、ウイルス対策ソフトを使う、パスワードは推測されにくいものにする、使わないサービスは止める等をおさえておかなくてはならない。

今後、今まで低温研内で起こったインシデント事例のデータベース化を行う。過去の同様なインシデントの記録を参照することによるインシデント対応の円滑化を可能にしたい。

参考

[1] JPCERT/CC: http://www.jpcert.or.jp

[2] WORM_MYTOB.ED の詳細: http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FMYTOB%2EED
WORM_MYTOB の亜種はいまだに活動し続けている。例えば 2006 年 1 月 23 日に発見された WORM_MYTOB.OX, http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FMYTOB%2EOX

[3] DoS (Denial of Services), サービス拒否攻撃: ネットワークを通じた攻撃の一つ。相手のコンピュータやルータなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させて相手のネットワークを麻痺させる攻撃。(IT 用語辞典 e-Words, http://e-words.jp より)

[4] IT 用語辞典 e-Words, http://e-words.jp より

[5] JPCERT/CC Alert 2005-03-09: OpenSSH の脆弱性を使ったシステムへの侵入に関する注意喚起: http://www.jpcert.or.jp/at/2005/at050003.txt
侵入を受けてから Web 偽装詐欺 (phishing) の踏み台サーバにされるなどの事例多数ある。