サイエンティフィック・システム研究会 2011 年 9 月 8 日
2011 年度教育環境分科会 第 1 回会合

# インシデント発生を抑えるための取り組み

熊本大学 総合情報基盤センター
杉谷賢一

［アブストラクト］
インターネットの脅威から組織内のネットワークを守るために、ファイアウォール(FW)や侵入防止システム(IPS)などの導入が多くなっているが、色々なインシデントの発生は無くなることは無い。それは、攻撃者の手口が巧妙になってきていることに拠るものもあるが、組織内のユーザの情報リテラシーの低さに拠るものの方が圧倒的に多いと考えられる。
本稿では、インシデント発生の低減を目指して熊本大学で行っている情報リテラシー教育やインシデント検知システム等について報告する。

［キーワード］
インシデント、情報リテラシー教育、情報セキュリティ、個人情報保護、ウィルス対策

## 1. はじめに

インターネットの脅威や構成員の不注意などによるインシデントは、各所で発生している。インターネットの脅威から組織内のネットワークを守るために、ファイアウォール(FW)や侵入防止システム(IPS)などの導入が多くなっているにも関わらず、インシデントの発生は無くなることは無い。それは、攻撃者の手口が巧妙になってきていることに拠るものもあるが、組織の(システム管理者を含む)構成要員の注意不足による、あるいは無意識の行動に拠るものの方が圧倒的に多いと考えられる。
本稿では、情報関連のインシデントの事例ならびにそれらに対する一般的な対策について述べた後、インシデント発生の低減を目指して熊本大学で行っている情報リテラシー教育やインシデント検知システム等について報告する。

## 2. インシデントとは

インシデントという言葉は、一般的には「重大事故に至る可能性がある事態が発生し、なおかつ実際には事故につながらなかった潜在的事例」のことを指すことが多いようだが、情報関連分野では潜在的事例に留まらず、セキュリティへの侵害など実際に事故に至ってしまった事態を指す。
文部科学省が発表している平成22年度に発生した不正アクセスの一覧を眺めてみると、次のような事象が多く発生している。

- ssh の辞書攻撃
- spam メールの大量受信
- Web ページの改ざん
- システムのパスワード漏洩
- 著作権違反ファイルのダウンロード

不正アクセス以外にも、インシデントとしては次のようなものも度々発生している。

- ウィルス感染
- 個人情報などの情報漏洩

これらのインシデントを発生させる要因をまとめてみると、次のようなものが考えられる。

- サーバが乗っ取られ、設定を書き換えられ、各種ソフトが仕込まれ、そのサーバから攻撃が行われる
- PC がウィルスやワームに感染し、ボット化する
- p2p ソフトを利用して不正ファイルを共有する
- 可搬端末やストレージを紛失する

## 3. インシデントへの対策

インシデントの発生を低減するには、次のようなことに注意する必要がある。

- パスワード管理の徹底
- サービスソフト管理の徹底
- セキュリティ設定の徹底
- OS を含むソフトのアップデートの徹底
- ウィルス(マルウェア)対策ソフト導入の徹底
- 可搬端末やストレージの持ち出し管理の徹底

また、インシデントが発生したら、できる限り早くそれを検知して、対策を施す必要がある。検知の手段としては、IDS の導入、FW や各種サーバのログの監視などが、主なものである。

インシデントを検知したら、できる限り迅速に対象である機器を特定し、ネットワークから切り離す。その後、その機器で動いている不審なソフトの探索・削除を行った上で、できる限り OS の再インストールを行う。

## 4. 熊本大学での取り組み

上記のようにインシデントは、基本的にネットワーク機器の管理の不備によって発生する。ということは、取りも直さず機器を管理している人(構成要員)の注意不足によって発生すると言っても良いと言える。ただし、「注意不足」には、次のようにいくつかの段階がある。

1) 注意すべき事項を知らない
2) 注意すべき事項をある程度知っているが、すべき行動をしない
3) 知っている注意すべき事項を基に行動するが注意すべき事項の知識が少ない
4) 注意すべき事項をほぼ把握しているが、行動が不完全である
5) (ほぼ)完全に注意すべき事項を基に行動する

上記のレベルの内、1)および2)の人は、3)以上のレベルに引き上げないと、高い頻度でのインシデント発生が予想される。また、システム管理者が3)や4)のレベルであると、一般ユーザが安心してシステムを利用することができなくなる。これらを改善する方法は、基本的には教育ということになるが、ほとんどの対象者には、直接業務と関わりのない教育となるため、モティベーションが上がらない。そのため、システム側から警告を出すような仕組みを作る必要がある。

そこで熊本大学では、構成員への教育とシステムの両方からインシデント発生を抑える取り組みを行っている。ただし、研究上ネットワークが自由に利用できるよう、FW の設定は最低限のガードのみを行っている。

### 4.1 教育に関する取り組み

**1) 1年次生全員への情報基礎科目の実施**

この科目では、情報リテラシーの演習の他に、情報セキュリティや情報倫理について年間を通して学習する。情報倫理の学習については商用のコンテンツによる演習の他に、著作権侵害や名誉毀損などネットワーク上の法的責任に関しては、実際に起こった訴訟の例を見ながら学習を行う。メールの配送の仕組みについては本学で開発した Seemit というソフトを利用して、また、サイトライセンス契約している Windows 用のウィルス対策ソフトについての紹介もこの科目の中で行っている。

また、以前、留学生向けに一部のテキストは英語化を行ったが、学部生として入学する留学生は日本語が結構理解できるため、最近は行わなくなった。

**2) サーバ管理者向けの講習会の実施**

研究室等で Web サーバ等を運用したい人を対象に、Linux サーバの講習会を行っている。講習会では、実習用の PC を準備して実際に OS のインストールから始めて、Web サーバ等の設定ならびにセキュリティ設定を体験してもらっている。ただし、ここ数年は開催していない。

**3) 情報セキュリティ対策パンフレットの配布**

熊本大学のセキュリティポリシー策定ワーキンググループで作成したパンフレットを全学に配布している。以前のパンフレットは、学内での色々な場面を想定して沢山の脅威を示していたが、昨年度からは特に重要で身近な注意点に絞ったものに変更した。

**4) 個人情報を守るための学習コンテンツの提供**

商用の学習コンテンツを LMS 上に置き、全教職員が自学できるようにしている。

### 4.2 システム側からの警告に関する取り組み

#### 1) DNS のクエリログ監視による検知

ssh 攻撃を受けたり、多量の spam メールを受信したりすると、攻撃元を含む DNS クエリが組織内の DNS サーバに大量に送られる。この性質を利用して、DNS サーバに残されるクエリログを監視し、統計処理を行うことで、攻撃元やウィルス感染端末をある程度特定することができる、という研究を行っている。この研究の成果を学内の DNS サーバに実装して、常時監視を行い、必要に応じて攻撃元を FW でブロックしたり、ウィルス感染端末の対処を行ったりしている。

#### 2) FW のアクセスログで特定ポートを監視することによるウィルス感染端末の検知

ウィルスに感染した端末は多くの場合、感染を広めるため外に向かって盛んに攻撃を試み続ける。そのため、FW で特定のポートを監視もしくはブロックしておくと、アクセスログ(もしくはブロックログ)に、感染した端末の IP が非常に多く残るため、この情報を基に、当該端末の管理者へ連絡及び対応の指導を行っている。

#### 3) 主要サーバの定期的なセキュリティ監査

全学的にサービスを行うサーバを新規に構築したり、OS のバージョンアップ等を行う時には、アクセス制限を含めたセキュリティ設定を徹底的に行う。行った後に、オープンソースのセキュリティ監査ツールを用いてスキャンを行い、設定の不備が無くなるまで、設定変更・スキャンを繰り返し行う。さらに、運用に入ってからも、年に1度から2度程度セキュリティ監査を行い、新しく判明したセキュリティホール等への対応を行っている。

## 5. おわりに

インシデント発生の低減を目指して熊本大学で実施している情報リテラシー教育やインシデント検知システム等について報告した。最近はインターネットの脅威に関する情報が新聞にも載るようになったので、以前に比べればだいぶ認識は高まっていると思われるが、いまだに研究室の PC がウィルス感染したり、踏み台にされたりたりするインシデントが発生する。これらは、OS のセキュリティアップデートやウィルス対策ソフトのインストールなど、必ず行わなければならない基本的な対策を行っていないことで発生している。更に徹底した情報の提供と教育体制の確立が必要である。また、日本語のほとんど分からない大学院への留学生については、情報リテラシー教育を受ける機会が無いが、今のところ特にインシデント発生の対象にはなっていないようである。

今後ますます攻撃の手段が巧妙になり、インシデント発生の可能性が増えると予想されるが、個人個人が行うべき基本的なことをきちんと実行するだけで、インシデントの発生の多くは抑えられるので、構成員の意識レベルが更に向上するよう力を注いでいく必要があると考える。