情報セキュリティインシデントデータベースの運用と最近のインシデント発生状況

竹　内　義　則

ウィルス感染などのセキュリティインシデントが発生したときの連絡や処置状況を明確にするために,「情報セキュリティインシデントデータベース」を構築し（図1参照），平成16年7月から運用を開始してきた。

情報セキュリティインシデントデータベースは，3種類のユーザ層を想定している。まず，一般ユーザは，自分のパソコンが外部と通信できない場合に，IPアドレスを入力することによって，ルータで遮断されているかどうかを調べることができる[1]。また，インシデントの発生日時，対処状況などを閲覧することが可能である。

つぎに，一般管理者は，部局等のネットワーク管理者を想定している。一般管理者は，自分のIDでログインすることによって，インシデントデータベース内のすべてのデータを閲覧することが可能となる。主に，自分の責任ネットワークアドレス内でインシデントが発生しているかどうかを調べ，発生している場合は適切に対処を行う。このデータベースによって，インシデントやユーザへ迅速に対応することが可能になる。現在，14名の一般管理者が登録されている。

最後に，スーパーバイザである。スーパーバイザは，データベースの閲覧だけでなく，インシデントの登録が可能となる。スーパーバイザが，侵入検出装置からの警告などによりインシデントを発見した際には，まず，データベースへの登録を行う。IPアドレスを入力することによって，その管理者を自動的に検索し，ウィルスに感染している旨を通知する電子メールを送信することも可能である。当該端末の管理者がウィルスを駆除し連絡を受け取った場合には，再度データベースに登録し，ルータの遮断を解除し，当該端末の管理者へ連絡する。これらの送信メールも，すべてデータベースに記録される。このように，感染端末が処置されているのかどうかの記録が一目でわかる。現在，処置されずに放置されたままのインシデントは，146件に上る。また，どのようなウィルスに感染したかという情報も蓄積される。

情報セキュリティインシデントデータベースの運用を約2年間続け，合計877件のインシデントが記録された。すなわち，1日に1件以上インシデントが発生している計算になる。最近約1年のデータを月ごとに統計を取ると表1のようになる。表から，インシデントはまとまって発生する傾向にあることが分かる。特に，6月の146件のうち，6月5日のインシデント発生件数は，60件になる。インシデントのほとんどは，Bot系ワームによるものである。これは，普段はウィ

1　http://sidb.nagoya-u.ac.jp/sidb/

ルス検出ソフトによってウィルス感染が防がれているが，ウィルス検出ソフトで検出できない新種のウィルスに学内の端末が１台でも感染すると，ネットワークを通じて蔓延したためと考えられる。ウィルス感染は，大学内で電子メールを使用しているときだけとは限らない。学内に持ち出して使用しているときに，ウィルスに感染し，そのコンピュータを学内のネットワークにつないだとたん，感染が広まるという事件が発生している。学外へ持ち出したパソコンを学内のネットワークにつなぐときは，細心の注意が必要である。特に，海外出張では，新種のウィルスに感染している恐れがある。ネットワークに接続する前に，別のコンピュータで最新のウィルス定義ファイルをダウンロードし，持ち出したコンピュータをチェックすることが必要である。

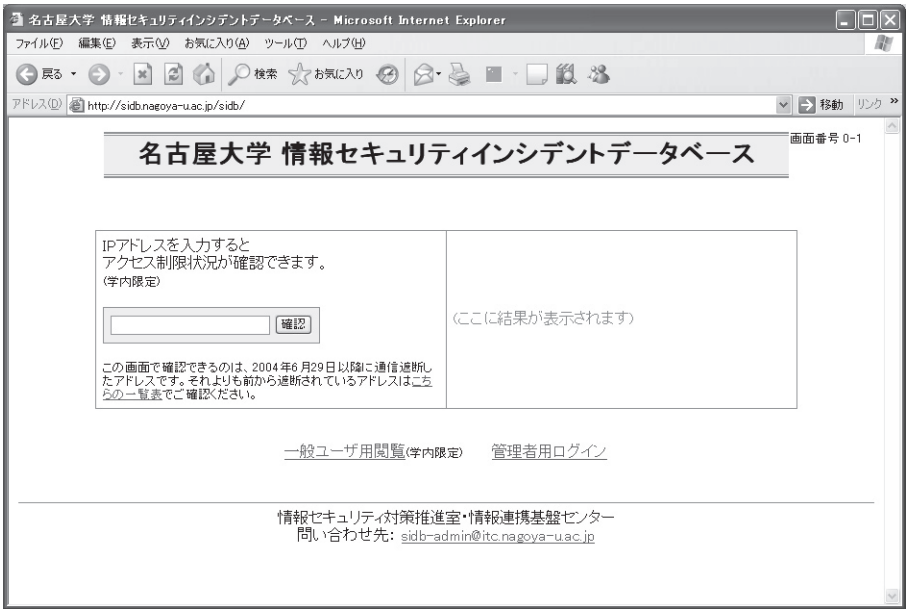
最近では，bot 系のワームによる感染が大部分を占める。これは，亜種が多く，ウィルス対策ソフトもすべてに対応し切れていないため，防ぐのが難しいためであると考えられる。また，外部への攻撃を始めないと感染していることに気づかないため，感染したまま放置されているものも多いと考えられる。また，遠隔から乗っ取られ，ssh brute force attack の踏み台に使われる端末も多い。

bot 系ウィルスは，ウィルス検出で検出できないことが多く，感染のさせ方も巧妙化している。ウィルス検出ソフトウェアのパターンファイルをアップデートしているから安心だとか，OS のアップデートを行っているから安心だということは決してない。さらに，rootkit によってウィルス感染自体を隠してしまうため，感染したことに気がつかない。その結果，ユーザは，自分の知らないうちに他者を攻撃する加害者になってしまう。ウィルス感染から身を守るためには，各ユーザの情報セキュリティに対する意識の向上が不可欠である。

情報戦略室では，ウィルスへの防衛を含めた情報セキュリティ啓発活動を行っている。

表１　月別インシデント発生件数

年月	インシデント発生件数	主要なワーム，ウィルス
2005/08	20	bot 系ワーム
2005/09	9	bot 系ワーム，UNIX への侵入
2005/10	71	bot 系ワーム，UNIX への侵入
2005/11	9	bot 系ワーム，UNIX への侵入
2005/12	19	bot 系ワーム，UNIX への侵入
2006/01	5	UNIX への侵入
2006/02	9	bot 系ワーム，UNIX への侵入
2006/03	4	bot 系ワーム
2006/04	40	bot 系ワーム
2006/05	16	bot 系ワーム，UNIX への侵入
2006/06	146	bot 系ワーム
2006/07	4	bot 系ワーム，UNIX への侵入
2006/08	2	トロイの木馬（持ち込み PC）



一般利用者向けアクセス制御確認画面

インシデント一覧（学内専用）画面

図１　情報セキュリティインシデントデータベースの画面

（たけうち　よしのり：名古屋大学情報連携統括本部情報戦略室）