JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

進化するウイルス
～新型ウイルスの傾向と対策～

園田道夫

不正アクセス調査WG
(株)アイ・ティ・フロンティア
2002 年 11月13日

深刻なウイルス被害

JNSA

- ウイルスによる被害は本当に深刻か？
  - –ウイルス感染すると、そのコンピューターを使った業務は一定時間停止する
    - ウイルス駆除ソフトウエア等を使って現状復旧
    - 同じコンピューター内の他に感染していないかチェックソフトウエアでチェック
    - 同じネットワーク内のほかのコンピューターのチェック
  - –上記合計で駆除3時間、感染チェック2時間、他コンピューターのチェックに2時間×台数。1感染あたりこれだけの業務用の時間が奪い取られる計算になる。業務機会損失などの推定被害抜きで、時間給のみの算定でも7,8万円弱～×感染数。
  - –しかしこれも、ウイルスの破壊力によって変動する。被害が甚大な場合はOSから入れなおして再構築。
    - となると10時間以上は必須か？

推定被害を入れると被害額は増える

JNSA

- 推定被害を入れると被害額はうなぎのぼり
  - –業務機会損失（被害により損失した時間あたりに「有り得た」取引額＝時間当り取引額）
  - –イメージダウン（負の広告効果＝ウイルス被害イメージ浸透規模と同等の影響を得るための広告費用）
  - –他企業、組織に与えた損害（賠償額ベース）
  - –上記部分は1感染あたりの損失時間給の100倍～1000倍まで膨れ上がる。これを加えると10感染あった場合では700～7000万円という被害額になる。

推定被害のいかがわしさ？

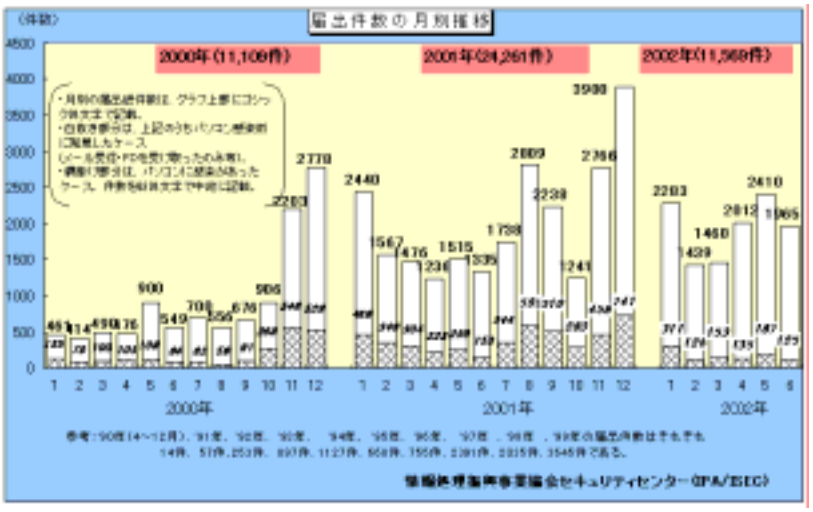
JNSA

- しかし、推定被害を含む被害額のいかがわしさについて指摘している声もある
  - –http://www.hotwired.co.jp/news/news/business/story/20020117105.htmlに取り上げられている数字では、「企業は『ニムダ』の駆除に6億3500万ドルを使い、生産性を落としたという。『コード・レッド』のさまざまな変種に対応するための総費用は、26億2000万ドルだった。『サーカム』は企業から11億5000万ドルを奪い取り、不愉快な『I LOVE YOU』の駆除には87億5000万ドルかかった。」とのことだが、I Love Youひとつで9000億円の社会損失とはどう考えても多すぎる？
- ただし、例え10万円（1感染）でも深刻であることは事実。業務機会損失や利益損失も皆無ではない

感染力が強くなっている現在のウイルス

- 「ワーム」と呼ばれる、特に感染力が強いウイルスが増えている
  - 「ワーム」とは、自動的に自己増殖を繰り返すウイルスのことで、従来型のメール系感染経路だけでなく、ファイル共有やセキュリティホール、ホームページ、IM (Internet Messaging) なども利用する
  - 最も多いメール添付の場合も、「I Love You」「極秘書類」などのように心理的な弱点を突いてくるようになってきている
  - 手当たり次第に周囲のコンピューターに自発的に感染したり、アドレス帳からごっそり宛先を参照したりするようになってきている

届け出ベースの感染数は増えている



目的や機能の多様化

- 目的の多様化、機能の多様化
  - –これまでは感染したコンピューターの機能やファイルを破壊することが主な目的だった
  - –しかし、現在は「キーストローク盗聴」「画面キャプチャー」「情報漏洩」「情報の暴露」などを目的とするものが出現してきている（スパイ行為）。いわば「トロイの木馬」化している
  - –最新凶悪ワーム型ウイルス「バグベアー」は、「システム改変」「セキュリティソフトのプロセス終了」「メール自動送信」「ネットワーク感染」「バックドア作成」「情報漏洩（システムが保持する情報を盗み取る）」という機能を備えている

今後予想されるニュータイプ

- 変わりつつあるデータのやり取り方法
  - –常時接続時代になり、画像配信、インターネットテレビ放映が増えてくる＝ストリームと呼ばれるデータ配信ではウイルスが混入する可能性は低いが、もし誰かが方法を思いつけば爆発的に流行する可能性もある
  - –Webページなどの静的データにとどまらず、小さなソフトウエアをやり取りすることが増えてくる。ソフトウエアにはバグがつきものであり、ウイルスなどが混入する可能性はある
  - –ファイル感染も、例えば普通の画像データなどに引っ付いてくることもある（単に添付ファイルに気をつけていれば良いだけではなくなる？）

最新事例「バグベア」

JNSA

- バグベア騒動は現在進行中
  - 「システム改変」「セキュリティソフトのプロセス終了」「メール自動送信」「ネットワーク感染」「バックドア作成」「情報漏洩（システムが保持する情報を盗み取る）」という機能を備えている
  - 「システムフォルダに熊のアイコンが居たらバグベアに感染しているので、すぐに削除すること！」というデマメールが流布した。しかし、これはまったくのデマで、下記アイコンのファイルは重要なものなので削除してはいけない。
  - 駆除ツールを装った別種のウイルスも出回っている＝「WORM_BOGUSBEAR.A（ボーガスベア）」、「WORM_HOBBIT.G（ホビック）」

Jdbgmgr.exe

バグベア騒動は珍しくない

JNSA

- 今後同種の複合的な騒動が巻き起こる（しかも長期にわたって）可能性がある
  - 数ヶ月前の「クレズ」も未だに流行っている＝今後流行は長期化する傾向にある
  - 複合的ないわゆる「騒動」が引き起こす被害による経済的な打撃は、単純な「復旧時間」×「感染台数」にとどまらない。
    - 感染行為等でネットワークを大量に使用するため、全体あるいは局所的に使用不能などの状況が起きる
    - 情報漏洩による被害は計り知れないが、手元で作成中の見積もりや社内の経営資料、財務資料や、トラブル報告などの書類が勝手に発送されてしまうインパクトは大きい（しかも相手先は自分のコンピュータに入っているデータ＝取引先等である可能性が高い）
    - パスワード等の情報が取られてしまうと、自分のコンピュータをどれだけ防御していても無力化されてしまう

ウイルスをばら撒いた場合の法的責任？

- 法的責任についての見解
  - –http://www.isc.meiji.ac.jp/~sumwel_h/doc/artcl/artcl1998-3.htmによれば、ばら撒きに故意性が認められたら刑事責任を問われる可能性がある。故意性が認められなくても業務上過失で刑事責任んを問われる可能性がある。
  - –また、民事責任という面では主に個人が負わされるが、公務員の場合は国または公共団体が負わされる可能性がある。
  - –現実では法的責任を負わされたケースは希少だが、企業の法的遵守姿勢が厳しく問われている現状では軽視できないリスクである。（保険もある）

現在と今後のウイルス対策

- 一般的なウイルス対策
  - –ウイルス対策ソフトウエア、システムの導入（クライアント、サーバー）
  - –メールの添付ファイルはみだりにオープンしない、などのガイドラインやルールの設定、そして啓蒙教育による人間系対策
- これから必要となるウイルス対策
  - –問われる企業全体の危機管理
    - –何か起きたときにどうするのか？広報、法的遵守、顧客対策、取引先対策、信用回復など
  - –セキュリティポリシーの作成と導入
  - –上記ガイドライン等は実はすべて全体的なセキュリティ対策の一部
    - –ポリシーをつくり、ガイドラインやルールを作り、遵守状況をモニターして改善する
  - –ITインフラ全体のセキュリティ対策

効果的なウイルス対策

- コンピュータを使わない
- コンピュータを使うときは用途や使い方を制限する
  - 最も感染するのはメール
    - メールには添付ファイルをつけない
    - HTML形式の見た目綺麗なメールを用いない
    - メールソフトウエアを比較的安全なものにする
    - メールサーバーに対策ソフトウエアなどを導入する
- データが集中的に流れるところ、集まるところを集中的に防御する
  - Web閲覧も閲覧用代理サーバーに対策ソフトウエアなどを導入する
  - ファイルサーバーにも対策ソフトウエアを導入する（サーバーそのものを使わない手もあるが、別のリスクが発生する）