セキュリティ・ウイルス

～ウイルスに対するセキュリティ対策～

細江 則彰，中尾 昌広
Noriaki HOSOE，Masahiro NAKAO

1　はじめに

近年，常時接続などのインターネットサービスの普及に伴い，電子メールなどの利用者も急増している．その一方で，コンピュータウイルス（以下はウイルスとする）による被害が増大している．企業の被害額は年間 4400 億円とも言われており，各企業では様々な対策が講じられている．本稿では，ウイルスとそれに対するセキュリティの対策について述べる．

2　ウイルス

2.1　ウイルスとは

ウイルスとは，PC の動作を異常にしたり，データやプログラムを破壊したりすることを目的にした，不利益をもたらす「不正プログラム」全般のことを言う．ウイルスは感染の有無，活動する条件，活動場所などで分類されていたが，近年は１つのウイルスの性質が複数持つことが多く，明確に分類することが難しくなっている．

かつてウイルスの侵入経路は，FD や CD-ROM や MO など外部記録メディアが主流であった．しかし，インターネットの普及と共にネットワークを経由するケースが増加し，なかでも電子メールの添付ファイルによる感染が大半を占めている．

Fig. 1 はウイルスの被害届出数である．セキュリティに関心が高まる一方で，被害届出数は増加の傾向にある．

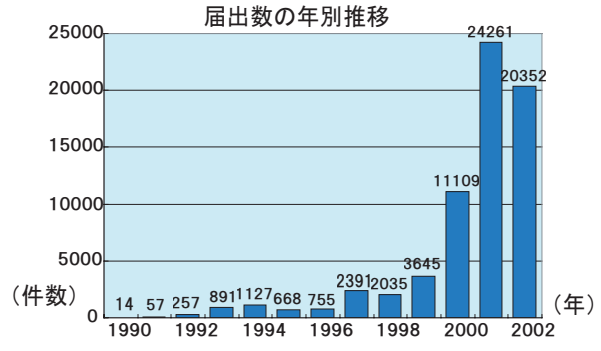

Fig. 1　ウイルスの被害届出数

ウイルスによる被害は，大きく３つに分類できる．

- システムの変更，破壊
- システム資源の浪費
- システム利用の妨げ

具体的には，開発してきたアプリケーションが消失してしまったり，個人情報などが流出してしまったりする．

次の節では，最近ウイルス対策ソフトなどによって，駆除し難いウイルスの技術について述べる．

2.2　ウイルスのステルス技術

ステルス技術は，ウイルスプログラムの存在や，ウイルスプログラムの動作を隠蔽するための技術である．その目的は，ウイルスを特定できる文字列やコードなどをキーにして検出しているウイルス対策ソフトなどに，駆除され難くすることである．

ステルス技術の一例として，自分自身を書き換える手法を挙げる．基本的な技術は以下の３つである．

- ウイルスプログラムを分割して順番を入れ替える．
- 実行しても意味のないプログラムを挿入する．
- 同じ動作をする別の命令群に置き換える．

Fig. 2 はウイルスプログラムを分割して順番を入れ替える図である．同じウイルスでも違うパターンを持つウイルスが現れるため，後に述べるパターンマッチング方式などによる検出が意味をなさないこととなる．

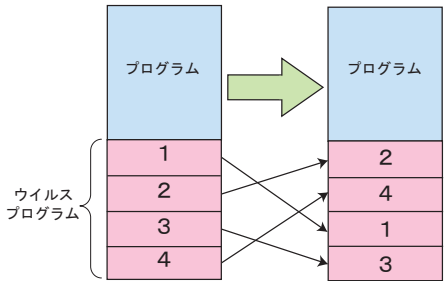

Fig. 2　ステルス技術の例

一般にステルス機能を持ったウイルスをウイルス対策ソフトウェアが検出することは困難である．なぜなら同じウイルスでも同じパターンを持つウイルスが二度と現れない可能性もあるからである．

次の章では，セキュリティ対策の方法について述べる．

3　セキュリティ

セキュリティとは，PC やネットワークの安全性やデータの保護を意味し，主に外部からの不正な侵入に対して

コンピュータを守り，データの流入や流出，破壊や改ざんを防止することである．本章では，ウイルスの被害を防ぐためのセキュリティ技術について述べる．

3.1 セキュリティ対策

企業や大学では，ウイルスの被害を食い止める，または最小限に抑えるために様々な仕組みを導入している．主に用いられる技術として，ファイアウォール，IDS，ウイルス対策ソフトであり，一般的にこれらを複合させて企業内ネットワーク環境の安全を図っている．

Fig. 3 に，ファイアウォール，IDS を用いてセキュリティを行っている図を示す．そして内部ネットワークにある各 PC にウイルス対策ソフトウェアを導入することによって，セキュリティがより強固なものになる．

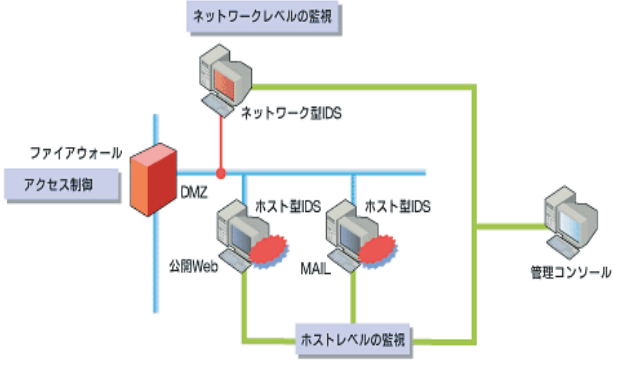

Fig. 3 トータルセキュリティの実現

以下の節で，各技術について詳細を述べる．

3.2 ファイアウォール

ファイアウォールとは，外部から組織内のコンピュータネットワークに侵入されるのを防ぐシステムであり，インターネットなどの外部ネットワークを通じて第三者が侵入することのないように，外部との境界を流れるデータを監視し，不正なアクセスを検出・遮断する機能を持っている．

しかし，近年ネットワークの多様化により，通信そのものは不正でなくても，その通信を利用した攻撃が生まれるなど，ファイアウォールだけでは防げなくなっている．こうしたファイアウォールで検知できない攻撃や不正進入の対策手段として用いられる IDS を次の節で取り上げる．

3.3 IDS（Intrusion Detection System）

IDS とは侵入検知システムと呼ばれ，通信回線を監視し，ネットワークへの侵入を検知して管理者に通報するシステムである．ネットワーク上を流れるパケットを分析し，パターン照合により不正アクセスと思われるパケットを検出して，管理者に通知する．IDS は監視する対象によって，ネットワーク型とホスト型に分類される．

ネットワーク型 IDS とは，ネットワークを流れるパケットを監視する IDS のことである．センサとマネージャという機能に分かれ，ネットワークの数箇所に配置したセンサで収集した情報をマネージャに集めネットワーク全体を統合的に監視する．

ホスト型 IDS とはサーバ上の動作を監視する IDS のことである．定期的にファイル，プロセスやシステムリソースを監視し，システムにおけるユーザの挙動やファイルの改ざんなどの不正アクセスを監視する．

3.4 ウイルス対策ソフトウェア

ファイアウォールや IDS 以外には，各 PC にウイルス対策ソフトを導入する方法もあり，前述の方法では防げない．添付メールでの感染や，モバイル PC 等で外部から感染することから守ることができる．以下に 3 つの検知方法を説明する．

1. パターンマッチング方式
   ウイルスプログラム内の特徴的な部分をパターンとしてデータベース化しておき，それを検索対象のファイル内容と照合する方法である．
2. ルールベース方式（動作監視方式）
   ウイルスの活動を分析してルール化し，プログラムの動作を監視し，ルールと合致する動作をするプログラムをウイルスとして判定する方法である．
3. チェックサム方式（整合性チェック方式）
   ハードディスク内の実行可能ファイルの状態をあらかじめ記憶しておき，その内容が改変されていないかどうかを常時監視する方式である．

一般的に，ウイルス対策ソフトウェアなどではこれらの方式を組み合わせて用いている．

4 おわりに

ウイルス対策ソフトウェアのベンダは，新たなウイルスに対応するアンチウイルス技術を開発しているが，現状では攻撃側であるウイルス作成者の方が 1 歩先に進んでいる状況である．そのため，ウイルスに感染する可能性を少しでも減らすために，ファイアウォール，IDS，ウイルス対策ソフトウェアを効果的に用いることが非常に重要である．

また，各個人のユーザがセキュリティに関心を持ち，知識を得ていくことも非常に重要なことである．

参考文献

1) IT 用語辞典，e-Words，http://e-words.jp/
2) アットマーク IT
   http://www.atmarkit.co.jp/
3) IDS（前編）
   http://www.texiv.jp/techreview/ids1.html