- 本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください。

- インターネットセキュリティ
  ウィルスの原理と対策

2002年11月1日　初版第一刷発光

監修　　三輪信雄

著者　　一瀬小夜

　　星澤裕二

発行者　稲葉俊夫

発行所　ソフトバンク　パブリッシング株式会社

ウィルスの原理と対策

渡辺研究室

040427493 間宮領一

第1部　ウィルスの仕組み

- 1章　従来のウィルス
- 2章　進化するウィルス

第2部　ウィルス対策

- 3章　ウィルス対策ソフト
- 4章　クライアント対策
- 5章　サーバー対策
- 6章　感染後の対応

1章　従来のウィルス

- ウィルスの種類として
  - 1.1 ファイル感染型
  - 1.2 ブート感染型
  - 1.3 マクロ感染型
  - 1.4 複合型
  - 1.5 トロイの木馬

以上の5つに分けられる

1章　従来のウィルス

- ファイル感染型

拡張子が「.com」、「.exe」、「.scr」などの実行ファイルに感染する。

メモリ常駐型と非常駐型の2種類がある。

メモリ非常駐型として、

「上書き型」「追記型」「キャビティ型」の3つに大別できる。

1章　従来のウィルス

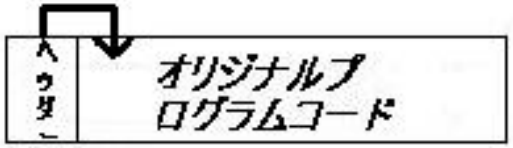
上書き型

感染前：

感染後：

追記型

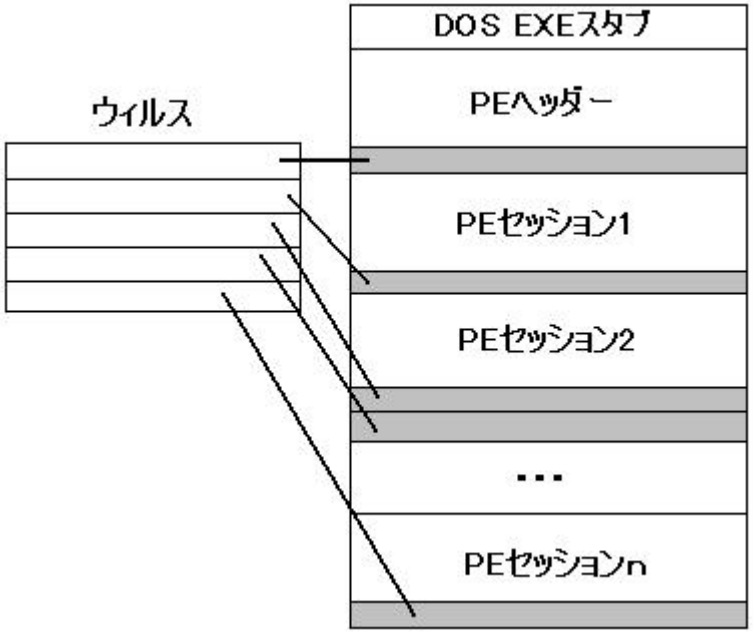
感染前：



感染後：

1章　従来のウィルス

キャビティ型



1章　従来のウィルス

- ブート感染型

コンピュータ特有の機能を利用しハードディスクとフロッピーディスクのシステム領域、ブートセレクターやパーティションテーブルに感染。

ブートセレクタやパーティションテーブルのサイズは約500バイトと小さいため、ウィルスプログラムをメモリに常駐させ自身をコピーするプログラムを記述するのは難しいため、感染前にブートセレクタを他のセレクタに移動し、その後ブートセレクタをウィルスコードで書き換える。

1章　従来のウィルス

- マクロ感染型

Microsoft WordやExcelなどのアプリケーションプログラムが持つマクロ機能を利用してデータファイルに感染。

これらのアプリケーションファイルが動く環境であればファイルを開くだけで感染するため、ハードウェアやOSに依存しないので被害が広がりやすい。

1章　従来のウィルス

- 複合型（マルチパータイト）

ブート感染型ウィルスとファイル感染型ウィルスの両方の感染メカニズムを持つ。

1.感染プログラムを実行するとブートセレクタに感染を広げる
2.感染しているブートセレクタから起動メモリに常駐したウィルスが実行可能ファイルにも感染を広げる

1章　従来のウィルス

- トロイの木馬

ウィルスやワームと異なり他のファイルへの感染、ネットを介して自己増殖もしない。

データ破壊型、情報収集型、バックドア型などがある。

1.データ破壊型

実行されると、特定のデータを削除したり、ハードディスクをフォーマットしたりする。

1章　従来のウィルス

- トロイの木馬

2.情報収集型

特定のコンピュータのログイン名やパスワードといった個人情報を盗み匿名アドレスに送る。

3.バックドア型

特定のコンピュータに再侵入するための裏口を仕掛けておき、遠隔操作できるようにする。

1章　従来のウィルス

- トロイの木馬

4.その他

上記以外にネットワーク攻撃やシステム状態の変更をするタイプも存在。

サービス拒否攻撃(Denial of Service Attack)などのツールが多数存在している。

2章　進化するウィルス

- ワームの登場

ワームとは単体で動作するプログラムのことを指し、

宿主が必要なく自分自身のコピーを作成して流布することで感染を広げていくもの。

1988年に出現したOSのセキュリティーホールを利用して、人の手を介せずに広がっていったモーリスワームが最初のワームである。

2章　進化するウィルス

- メール添付型ワーム

HAPPY99, LoveLetter , MTX , Hybris ，Magistr ，Sircam

- IM (Instant Messaging)を利用するワーム

choke

- クライアントソフトのセキュリティホールを利用したワーム

Badtrans.B ，CoolNow

- サーバソフトのセキュリティーホールを利用したワーム

モーリスワーム , Ramen , Lion , sadmind/IIS , CodeRed , CodeRedⅡ , Nimda

2章　進化するウィルス

- HAPPY99

1999年1月発見。

通常のメールと同時にワームを送信。メールに添付されてくる「HAPPY99.exe」を実行すると、新年を祝う花火を表示してユーザーの目を欺き、その間に感染活動をする。

最近ではユーザーがダブルクリックするように誘惑してくる。また、2重拡張子などで安全なファイルだと安心させる手も増えてきた。

2章　進化するウィルス

- LoveLetter

2005年5月発見。

特徴として添付ファイルが2重拡張子。Outlookのアドレス帳に登録されたメールアドレスへ、自分のコピーを添付して送信。ハードディスク上の拡張子が「.css」「.hta」などを「.vbs」などに上書き変更。内容を上書きするために駆除しても復元できない。

2章　進化するウィルス

- Choke

2001年6月発見。

MSN Messengerを利用して感染を広げる。友達リストやメンバーリストと呼ばれるリストに登録されたユーザに対してメッセージと同時に発信する。

実行するとエラーメッセージで目を欺き感染活動を行う。

2章　進化するウィルス

- Badtrans.B

2001年12月発見。

不正なヘッダーが原因でInternet Explorerが電子メールの添付ファイルを実行。

アドレスを抽出してその情報を元にメールを送信する。メーラーを使用せずに、自力でメールを送信するため履歴がのこらない。

ハッキングツール的役割も果たす。

2章　進化するウィルス

- サーバーソフトのセキュリティホールを利用したワーム

サーバーを狙うワームは自身を自力で実行し、勝手に拡散していく。そのため、「ワームは任意のコマンドを実行可能な」セキュリティホールを利用。それらのセキュリティホールは「バッファオーバーフロー」などがある。

2章　進化するウィルス

- バッファオーバーフロー

プログラムに与える文字列中に機械語を含ませ、リターンアドレスとなる部分にその機械語が格納されているアドレスを記述。

C言語で記述されたプログラムは、通常メインルーチンとなるmin()関数と、サブルーチンとなる複数の関数で構成されている。

2章　進化するウィルス

- バッファオーバーフロー

main()関数から始まりfunction1()が呼び出されるとそこへジャンプ。処理が終了し、return;が実行されるとmain()関数のfunction1()関数が呼び出された場所に戻る。以下同様。

プログラムはreturn;を実行したときにmain()関数の何番地に戻るべきかを覚えておかなければならない。

この戻るべき番地をリターンアドレスという。

```
function1()
{
return;
}
function2()
{
return;
}
function3()
{
return;
}
main()
{
function1
    …
function3
    …
}
```

2章　進化するウィルス

- バッファオーバーフロー

Function1()が右のような処理だったら

ここで5行目Strcpy(buf,str);によってstrが示す文字列がbufにコピーされる。例えばここで、strがaaaa・・・という16バイトより大きいものだった場合文字列はbufの領域からあふれ、周辺メモリを書き換えてしまう。

return;が実行されると本来戻るべき位置であるがなかろうと、無条件でリターンアドレスが示す場所にジャンプする。よってプログラムは以上終了する。

```
function1()
{
Char buf[16];
  …
Strcpy(buf,str);
  …
return;
}
```

2章　進化するウィルス

- CodeRed
- 動作環境：Index Serverがインストールされており、IISが稼動しているサーバー

ホワイトハウスへDos攻撃、Webページ改ざんなどを行う。このワームはファイルとしての実態を持たず1つのHTTPリクエストだけで感染、増殖を行う。

IISをインストールする際に、DDLファイルがインストールされ、そのうちのひとつIndexServer/IndexingServicesのコンポーネントidq.dllというのがある。これは.idqファイルに対してHTTPリクエストを処理する際URLの長さをチェックしないためバッファオーバーフローが起きる。

2章　進化するウィルス

- CodeRed

感染後、感染したWebサーバーが英語版だった場合Webページを改ざんする。これに感染するとWebサーバーがHTTPリクエストを受信するとワームがそれに対して返答をするようになる。

感染1日から19日の場合、増殖活動を行う。

ランダムなIPアドレスの80番ポートに対して、感染したときと同じ構成のHTTPリクエストを送信。

20日から27日の場合ホワイトハウスのWebサーバーに大量のSYNパケットを送信して攻撃をする。

3章　ウィルス対策ソフト

- ウィルス対策ソフトの役割

ウィルスやワームの検出および駆除を行う。

- 検出方法

1. パターンマッチング方式

既知のウィルスのパターンが登録されているウィルス定義ファイルと検査の対象となるファイル、メモリ、ブートセレクタなどを比較し検出

3章　ウィルス対策ソフト

2.チェックサム方式

実行可能ファイルが改変されていないかを確認することにより検出。

3.ヒューリスティックスキャン方式

実行ファイルをスキャンするときファイル全体の構造やプログラムのロジックなどからプログラムの振る舞いを収集しリスト化。次にリストを評価し行動パターンから検出。

3章　ウィルス対策ソフト

4.ルールベース方式

ウィルスが実行されると、システム領域の書き換、実行ファイルへの書き込み、特殊なメモリに常駐といった挙動を示すためこれらの行動を監視し感染を防ぐ。

- 駆除

ウィルスに感染するとファイルにウィルスコードが埋め込まれるためそれを削除したり無害なものに上書きしたりすること。ワームの場合は削除する必要がある。

3章　ウィルス対策ソフト

- 削除ツール

駆除ツールは主に、以下のことを行う。

◇ウィルスのプロセスの終了
◇レジストリの修復
◇作成されたファイル(ワームのコピーなど)の削除
◇感染したファイルの修復
◇改変されたシステムの修復

3章　ウィルス対策ソフト

- 駆除ツール

ウィルスやワームはレジストリの書き換えをするものが多く、これらは手動で修復しなければならないが、ウィルス対策ベンダーから提供されているものを使えるものがある場合使用したほうが無難

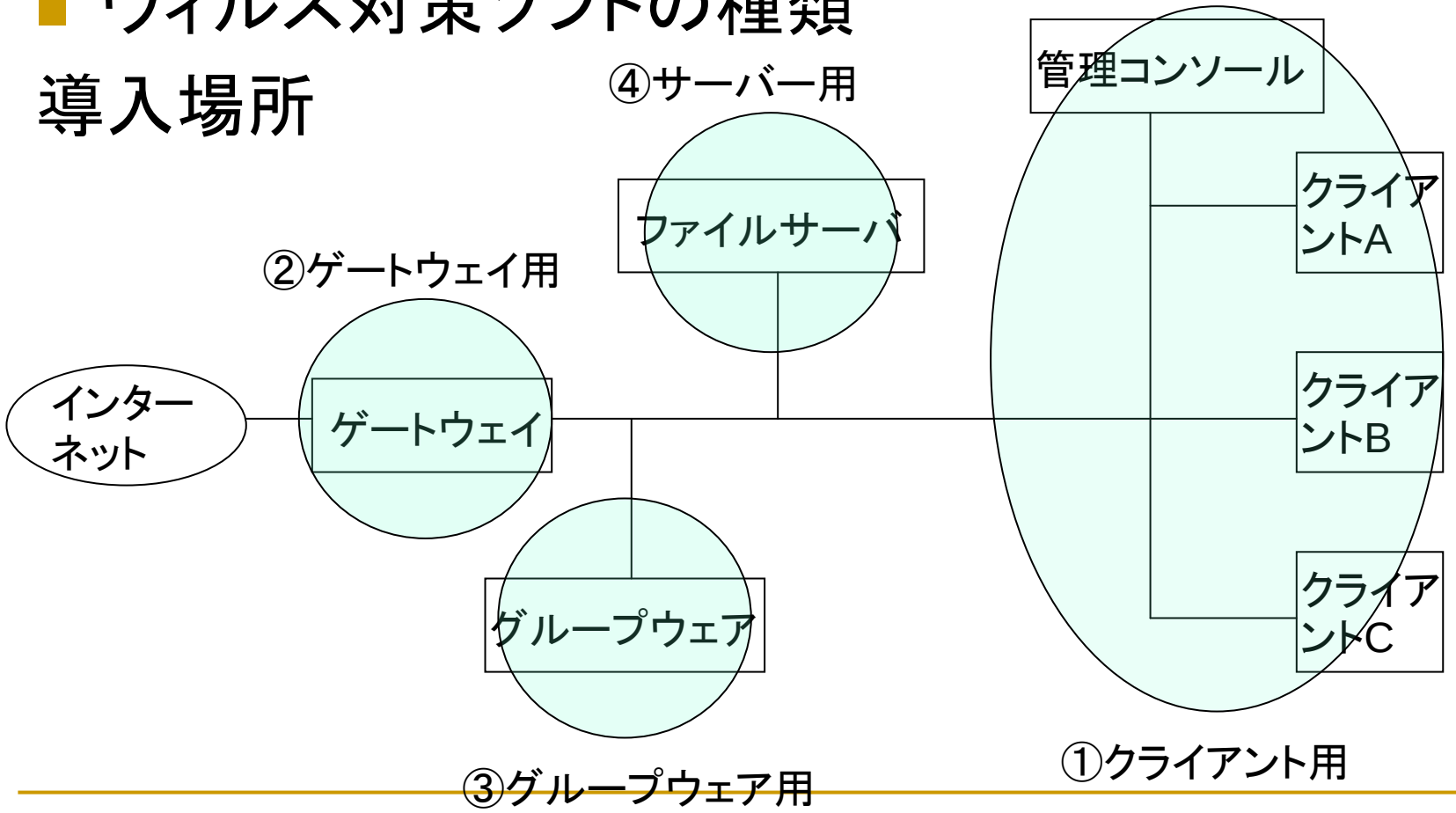
- 主なベンダー

シマンテック、トレンドマイクロ、CSE、マカフィーなど

3章　ウィルス対策ソフト

- ウィルス対策ソフトの種類

導入場所



3章　ウィルス対策ソフト

- ウィルス対策ソフトの種類

◇クライアント

ウィルスやワームの感染経路すべてを対象とし検出。

一括管理型とスタンドアロン型の2つに分けられる。

◇ゲートウェイ

LANとインターネットの間に設置されゲートウェイを介して行われる通信を監視、検出。特定の場所で一括して検出が行える。

3章　ウィルス対策ソフト

◇ SMTP

メール添付ファイルを監視、ウィルスやワームをフィルタリングする。添付ファイル以外の情報漏えいを防ぐ機能も持つ。

◇ HTTP

クライアントとWebサーバ間のトラフィックを監視。

Webページのウィルスや不正なActiveX、JavaScriptなどを受信する前に検出、フィルタリングをする。

◇ FTP

FTPによるファイルダウンロードを監視ウィルスや不正プログラムをフィルタリングする。

3章　ウィルス対策ソフト

- 導入

全ての実行、感染はクライアントから始まるため、最初に導入するべきはクライアント。

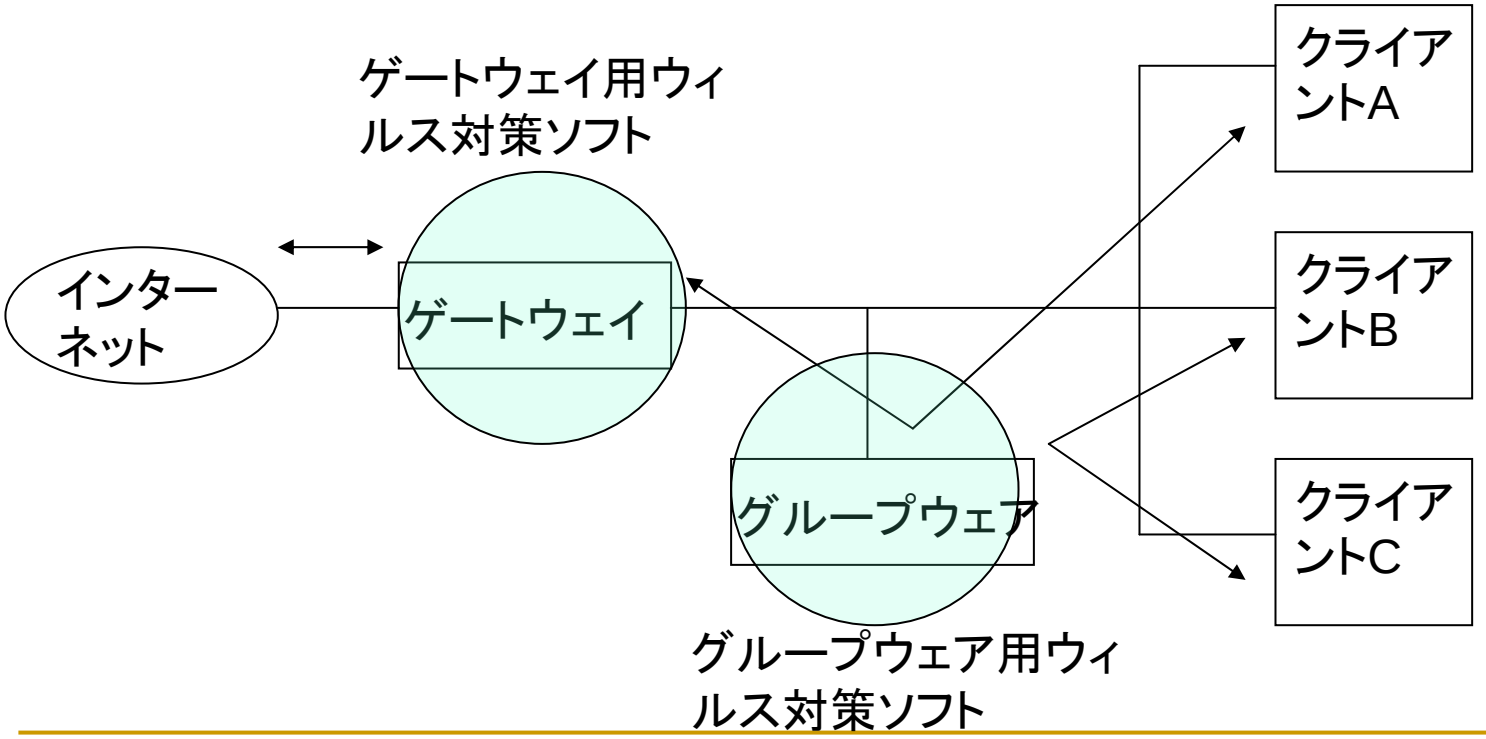
何を守るかをよく考える。ゲートウェイ用対策ソフトではどう導入したら、効率的かを考えなければネットワークが遅延して業務効率が下がることが起こりかねない。

管理のしやすさパフォーマンス、サポートを考えた上で対策ソフトを選ぶ。

3章　ウィルス対策ソフト

- 構成例

メールの添付ファイル



3章　ウィルス対策ソフト

- 運用

ウィルス対策ソフトを導入する比率が非常に高くなっているが感染被害が耐えないのは、導入後の運用が適切に行われていないことが原因といえる。

ウィルス対策ソフトはパターンマッチングが最も一般的なため定期的にアップデートし、常に最新のものにしておく事が必要。

3章　ウィルス対策ソフト

- ウィルス対策ソフトの限界

ウィルス対策ソフトを適切に導入して運用していれば、クライアントを狙うウィルスやワームに感染することは少なくなる。しかし未知のものに対しは、方法があるにしろ検出は困難だし、既知のものでも対策ソフトをかいくぐるものもある。

現在では発覚から数時間で世界に蔓延するため、クライアントホストとそれを使用するユーザが一番注意をしなければならない。

4章　クライアント対策

- ウィルス対策ソフトの運用

クライアントホストにスタンドアロン型のウィルス対策ソフトを導入している場合は、以下のことを徹底しなければならない。

◇定期的にウィルス定義ファイルをアップデートする

◇パッチの低起用、バージョンアップ

◇常駐検査を行う

◇定期的にディスク全体をチェックする

4章　クライアント対策

- 添付ファイルは実行しない

ワームが送られてくるのは、知人からのメールの確立が高い。

添付ファイルが安全に見えるように2重拡張子になっているものがある。

- パッチの運用、バージョンアップを行う

セキュリティーホールを突くワームがあるため、アプリケーションやOSに関するパッチやバージョンアップは速やかに対応するべき。

4章　クライアント対策

- むやみにファイルを実行しない

ファイルのダウンロードファイルなど実行する前に必ず手動でチェックする。

- バックアップの必要性
- マシンの設定

Microsoft製品のInternet ExplorerやOutlookは一般に広く使われているため、危険度の高いセキュリティホールが発見されているため攻撃の的になっているので、きちんとした設定が必要。

5章　サーバー対策

- ウィルス対策ソフトでは守れない危険

サーバーのリモートからの不正アクセス。

ウィルス対策ソフトはこれの検出に適さない。Webサーバーのように外部から頻繁にアクセスがある場合、常駐検査を行うとレスポンスの遅延に繋がるためよくない。

セキュリティーの向上、レベル維持が重要。

- 社内ネットワークに潜む危険

5章　サーバー対策

- セキュリティの向上
- 不要なサービスの停止

必要ないポートなどは空けない。DNSのセキュリティーホールに気をつける。

- 最新のアプリケーションを使用
- パッチを適用

セキュリティホールに対するパッチ

- 適切な設定を行う

セキュリティ向上のためのホストの設定

5章　サーバー対策

- ファイアウォールの有効活用

Webサーバを狙うワームは、HTTPリクエストを利用している。Webサーバ以外にも、DNS、FTPなど外部に公開してサービスを狙ったワームはファイアウォールでは防げない。しかし有効な活用法として2つが考えられる。

5章　サーバー対策

- ファイアウォールの有効活用

1.外部に公開する必要のないサービスを守る

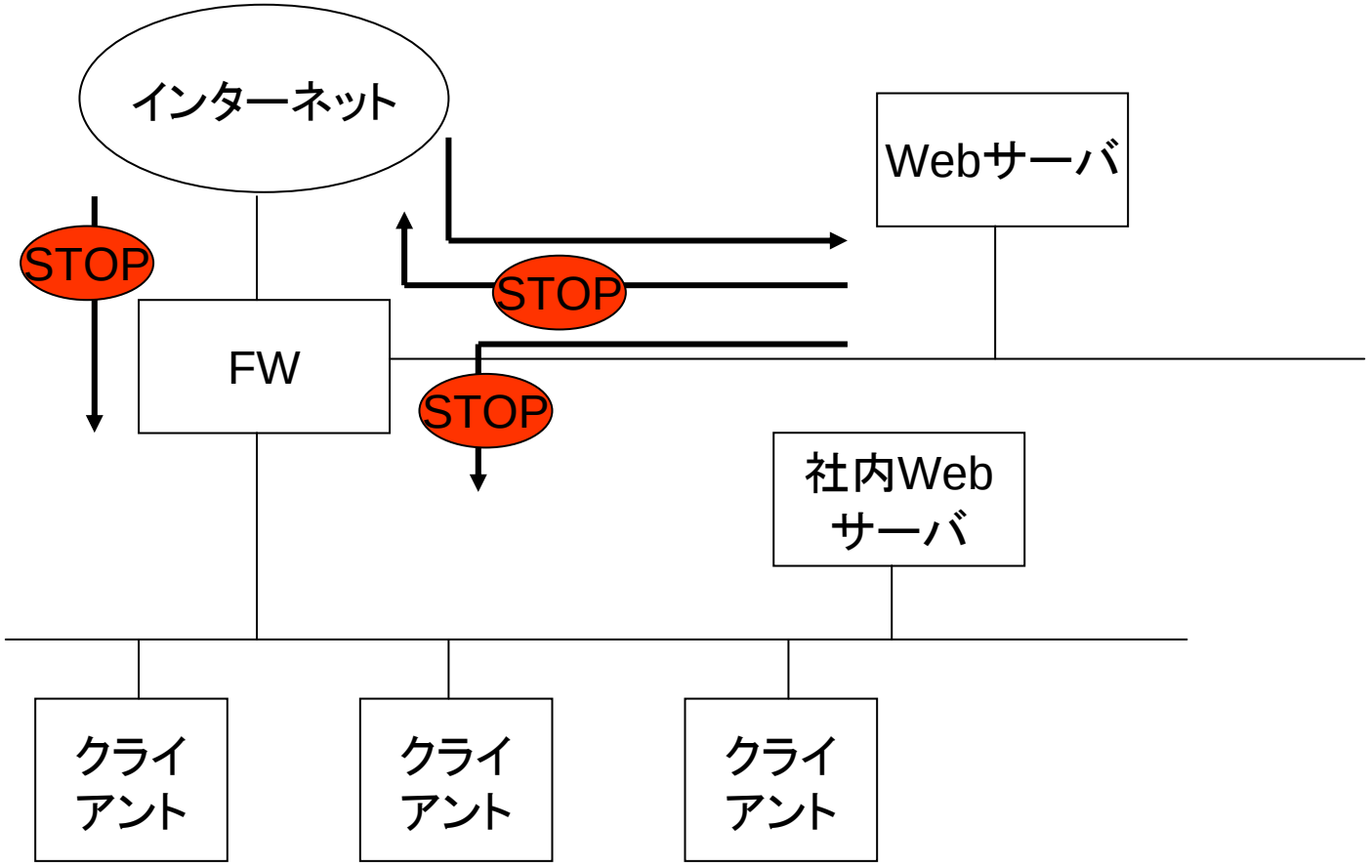
外部に公開する必要のないサービスのセキュリティホールを利用しているワームがあるため、ファイアウォールがこれらのサービスへのアクセスを拒否していれば感染は免れる。

2.サーバから外部・内部へのワームの流出を阻止

ファイアウォールは2次感染を防ぐ方法として有効。

5章　サーバー対策

- 例


インターネット
Webサーバ
STOP
STOP
FW
STOP
社内Web
サーバ
クライ
アント
クライ
アント
クライ
アント

5章　サーバー対策

- サーバー上で余計な作業をしない

サーバー本来の目的外では使わない。Webページ閲覧はもってのほか。

- バックアップの必要性
- どんなセキュリティホールが危険度が高いか知る

セキュリティホールを利用した攻撃はリモートからかローカルからか、攻撃ツールが公開されているか

- 情報収集をし、対策方法を知る

6章　感染後の対応

- ブート感染型の場合

ハードディスク上のマスターブートレコード又はブートレコードを修復できない場合、救急ディスクセットを使い復元。これはウィルス対策ソフトについてくるか、対策ソフトから作ることが出来る。

マスターブートレコードに感染した場合、ハードディスクをフォーマットするだけではウィルスは削除できない。

6章　感染後の対応

- メモリ常駐型の場合

コンピュータをクリーンな状態で再起動し除去する。クリーンな状態で再起動せず対策ソフトを使った場合、検査した全てのファイルがウィルスに感染する可能性がある。

◇W95.CIHウィルス

Windows95/98のみで動作する。常駐後にアクセスされたファイル全てに感染。無限ループを使ってハードディスクを先頭からシステムがクラッシュするまで書き換える。また、Flash BIOSを攻撃し、保存されているデータを破壊することによりOSの再インストールすら出来なくする。

6章　感染後の対応

- ネットワーク感染型の場合

メールやネットワークを使って感染を広げるため、感染しているコンピュータのネットワークを切断した後に対策ソフトにより検査する。

- レトロウィルス(ワーム)の場合

発見を逃れるために対策ソフトを攻撃するウィルスのこと。こういったものが蔓延した場合、数千台に定義ファイルを配布するだけでなく、対策ソフトを再インストールが必要になる場合がある。

6章　感染後の対応

- まとめ

ウィルス対策はひとつに偏りすぎてはいけない。

ユーザーは人間である以上、どんな教育を実施しても感染する行動を起こしてしまう可能性があるため、ウィルス対策ソフトが検出できないものをユーザーが、ユーザーが誤ってウィルスなどを実行したときは対策ソフトがというようにお互いが補完しあうのが理想である。