第２章　コンピュータシステムとセキュリティ

第１節　コンピュータシステムに対する脅威

（１）　ミスや故障、災害による情報の破戒

(a) 人間のミスによるもの

(b) コンピュータシステムの故障

(c) 災害によるもの

対策

物理的保護　　建物、コンピュータ室の管理

障害対策　　多重化

バックアップ

（２）人間の意図的な行為による情報の盗聴、不正使用、改ざん、窃盗、破壊

－　コンピュータ犯罪

対策

Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ

password：　コンピュータシステムの利用者のチェック

認証：　コンピュータへアクセスした人間本人が確認する。

firewall：　あるローカルネットワークへの入り口において、パケット発信元などをチェックし、ネットワーク内に入るものを選別する電子的な防火壁

機密保護　　署名と暗号化

computer virus　　ワクチン（Anti-virus soft）

バックアップ

第２節 コンピュータウイルスとウイルス
犯罪事例

２－１　Computer Virus

通常、母体プログラムの一部に特別な動作をするプログラムが付加されている（寄生している）
誰かが意図的に作ったもの
テキストデータにはウイルスは寄生させられない

（１）　ウイルスの自己増殖
（ａ）　自己増殖をしないもの
　　プログラムに寄生しているが、その他のプログラムには影響を及ぼさない
　　そのプログラムをコピーしたときだけひろがる。
　　「爆弾」あるいは「トロイの馬」と呼ばれることもある。
（ｂ）自己増殖をするもの
　　ウイルスが寄生しているプログラムを実行すると、ウイルス部分が動作し、他のファイルに自分をコピーして広がる（感染する）もの。
　　他のファイルに感染するときは、感染することが可能なファイルをさがし、そのファイルに書き込む。
　　母体を持たないプログラムはワームと呼ばれる。
（２）　ウイルスが引き起こす動作（症状）
　(a)　妙なメッセージや音をだす。
　(b)　ファイルやディスクが破壊される。
　(c)　システムがうごかなくなる。
（３）　ウイルスが入り込む経路

(a) 出所不明のソフト（フロッピーなどでコピーしたもの）を読み込む

(b) ネットワークからフリーソフトを読み込む

（４）ウイルス対策

(c) 予防　出所不明のソフトは利用しない

(d) 検知

ワクチン　　過去に発見された方法のウイルスの存在を検知し、システムの侵入を防ぐプログラム

新しい方式のウイルスには対処できない

©　復旧　ウイルスに感染したプログラムを元の状態に戻すプログラムもあるが完全とは言い切れない。

バックアップから復旧する。

（５）ワクチンプログラム　　以下のような方法がある。

(a)　コンペア法

正常なファイルの全体や管理情報などを保管し、これと検査対象ファイルを比較してウイルスの存在を調べる。

（ｂ）スキャン法

既存の各ウイルスに対し感染した場合にどう変化するかというデータを用意し、ておき、そのデータに基づき、ウイルスの発見、ファイルの修復を行う。

©　接種法

アプリケーションプログラムのファイルを予め加工して、感染の可能性がある場所にウイルスの検知のためのデータを埋め込む。

参考文献

芝宮実他：　実践ソフトウエア開発工学シリーズ、セキュリティ管理の技術、日科技連（１９９３）

２－２　コンピュータウイルスの事例

（１）メリッサ

- 1999年3月に猛威を振るったワーム
- Word,Outlook,Outlook Expressを利用しているコンピュータに感染
- Outlookのアドレス帳の上から50人にWord形式メッセージが自動的に送信
- メッセージを受け取ったファイルを開くと感染し、同様に50人に送信する。

(2)I　Love　You

- 2000年5月に猛威を振るったワーム
- Microsoft社のソフトに広く実装されているVBscript（スクリプト言語）で書かれている
- 電子メールにスクリプト言語のファイルが添付　これを開くと感染プログラムが実行
- 感染すると、パスワードを検出し、ワームの作者のサイトに送る
- さらに、システムディレクトリに自分自身の複製を作成し、コンピュータを起動するたびにワームが実行されるよう設定する
- いくつかの拡張子のついたファイルをすべて破壊してしまう。
- さらに、同じチャットルームに参加しているすべてのユーザに自らの複製を送信
- 甚大な被害
  － Microsoft,Ford　Motor、米軍など被害
  － FBIも捜査に乗り出す。
- 発生から1週間でフィリピンの専門学校生が逮捕された。

(3)SirCam

- ネットワークで自己増殖を繰り返すワーム
- 2001年8月頃猛威
- 自分自身を添付した電子メールを作成、ユーザに知られないように、色々なアドレスにばらまき、他のコンピュータに感染
- ユーザのコンピュータから電子メールのアドレスなどの宛先にメールをばらまく。
- このとき、いくつかの拡張子のファイルのワームを追加して添付
- ワームが広がるとともに、内部ファイルが他人に読まれる危険性がある
- メールの送信元アドレスや添付ファイル名も変化するのでわかりにくい

（４）　Code　Red

- Windows　NT/2000のWebサーバの安全保護の脆弱性を利用するワーム
- 2001年に、出現から数日で世界中のサーバに広がった
- 上記サーバに感染し、IISとDLLというソフトのセキュリティホールからコンピュータに侵入
- 侵入した後、自己複製による増殖
- ホワイトハウスなどへのDDoSアタックを行う
- DDos:　複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバへパケットを送出し、通信路をあふれさせて機能を停止させてしまう攻撃

（５）　Nimda

- 2001年9月にインターネットで猛威を振ったワーム
- WindowsOSのコンピュータに感染する様々な手段で感染する初の複合型ウイルス
- Nimdaは公開されているWebサイトのHTMLファイルにJavaScriptによるプログラムとして

潜入

- 多様な手段で感染する。
  - Internet Explorerを介して閲覧者のコンピュータに感染
  - Webサーバのセキュリティホールを突いて侵入
  - 電子メールの添付ファイルに潜んでOutlook Expressを介して感染
  - LAN上でファイル共有機能を通じて自身の複製を作成する
- Nimdaは感染したサーバ上にあるWebページを開いたり、感染したコンピュータから送られてきた電子メールをプレビューするだけで感染してしまうという極めて強力な感染力を持つ。
- Nimdaの数ヶ月前に猛威を振るっていたCode Redと同様の手法でWebサーバの弱点を突き、サーバ内に侵入する。
- Nimdaは、コンピュータに感染すると、ハードディスク内と他のコンピュータの共有フォルダ上にあるHTMLファイルを書き換え、Internet Explorerで閲覧するとNimdaに感染するように書き換える。
- その際、プログラムの中に自分自身を埋め込む。

（６）　Blaster

- 2003年8月に猛威を振るったWindowsに感染するワーム
- Windows２０００とXPのコンピュータの脆弱性を突いて侵入し、侵入すると起動ごとに自分が立ち上がるように設定
- 感染した後、自らのIPアドレスに近いアドレスのコンピュータに次々に攻撃をしかける。
- 感染したコンピュータは、副作用として短時間のうちに異常終了と再起動を繰り返すようになる。
- Microsoft社は無償の緊急対策用CD-ROMをユーザに配布した。

第３節　個人情報保護
(Privacy Protection)

３－１　個人情報漏洩事件

・京都府宇治市の住民情報漏洩事件（１９９９年５月）
京都府宇治市がシステム開発に際して、住民データの入力を業者に委託。その業者が再委託した孫請業者のアルバイト社員が、住民情報２１万人分のデータを複写して名簿業者に販売した。
国内で最初の大規模個人情報漏洩事件。
住民が宇治市と開発委託業者に対して損害賠償訴訟を起こし、原告１人あたり３万円の損害賠償支払いを命ずる一審判決が出た。（最終判決は、原告１人あたり１万円）
　宇治市は開発業者に対し、庁舎外での作業（住民情報の持ち出し）を認めており、にもかかわらず守秘契約も締結していなかった。
委託先の社員の犯罪であり、宇治市も終始「被害者」との立場をとったが、最終的にはずさんな委託先管理が問題視され、「管理者責任」を問われた。
判決内容に関しては、個人情報が悪用されて具体的な被害があったわけではなく、個人情報が流出しただけという抽象的な損害に過ぎないのではないかという見方もあったが、「自分の情報を不特定多数の者にいつ購入され、いかなる目的で利用されるかわからない、という不安感」がプライバシー侵害と認定され、損害賠償の対象とされた。

・ヤフーBB　顧客情報流出事件
２００３年１月時点で、同社のデータベース内にあったすべての加入者の情報が抜き取ら

れていた。
容疑者は、ソフトバンクＢＢ社に勤めていた元派遣社員を通じて知ったＩＤやパスワードを使って、同社のデータベースに侵入し、ヤフーＢＢの加入者情報を抜き出していた。
容疑者は２００２年６月に約４７０万人分の情報を抜き取っていた。
それ以前も含め、データベースに記録されていた約６６０万人分の加入者情報をすべて抜き取った。
ソフトバンクを恐喝

・ジャパネットたかた(通販）事件
2004 年 3 月 9 日　同社の顧客情報が大量に漏洩していたことを明らかにした。
元従業員 2 名（元システム担当者とその上司）が情報漏洩の犯人
彼らは 1998 年 2 月頃ダイレクトメール作成目的で、データベースから購入歴が 1995 年 2 月から 1998 年 2 月までの顧客情報約 40 万人分の抽出
流出数は、社内調査で約 51 万人
一部は、職業や勤務先などのデータも含まれていた。
今回の漏洩事件で、売上高減は約 150 億円に達するとのこと

・アッカ・ネットワークス事件（ ADSL 接続サービス会社）
2004 年 3 月 24 日に、顧客情報が漏洩したことが、公表された
201 人分の漏洩は間違いない、しかし、件数は最大の場合で全顧客数に当たる 110 万件に上る可能性がある
内部からのデータベースへのアクセスによる情報漏洩の線が濃厚

・秋田県湯沢市事件
2004 年の事件
ファイル交換ソフト「Winny」を通じて広まっているウイルスに市職員の PC が感染し、市民 11,255 人分の個人情報がインターネット上に流出
市職員は合併協議会事務局に出向していた際、事務局員が共同で使用する PC 上で Winny を使用していた
Winny を通じて感染したウイルスは、感染した PC の HDD にある Office ドキュメントやデスクトップのスクリーンショットを Winny のネットワークに流出させる
2003 年に旧湯沢市が実施した市町村合併に関するアンケート用の名簿で、旧湯沢市民 11,255 人分の氏名や住所も含まれていた。
このアンケート書類を市民に配布した旧湯沢市行政員 234 人分の名簿や旧湯沢市職員 384 人分の名簿、旧湯沢市議会議員 24 名分の名簿も流出。
湯沢市の対応策

市民への説明と 2 次被害の防止のため、名簿に記載されていた市民などに対し 4 月 18 日までにお詫び状を発送。
市広報号外を発行して、事件の経緯と内容、今後の対応、想定される 2 次被害への注意を呼びかけ、市広報の特集記事で 2 次被害の防止について周知させる。
個人情報漏洩に伴う処分
Winny のウイルスに感染した市職員を 3 カ月間の停職
当時、旧湯沢市など 4 市町村の合併協議会会長を務めていた湯沢市長を 2 カ月間にわたり減給 10 分の 1
この他の最近の情報漏洩事件
2005 年 4 月
・鈴鹿サーキットランド、携帯サイトでの F1 日本 GP 観戦券購入者 29 人分。ウェブ編集ミス。
・三重県津市の県立津工業高校、生徒 276 人分。ノート PC 盗難。
・リコー、顧客 1 万 8700 社分。ノート PC 盗難。
2005 年 3 月
・みずほ銀行、全国 167 カ店で合計約 27 万人分。口座情報・各種金融申込書等。内部紛失の可能性。
・みずほ信託銀行本店・福岡/鹿児島支店、計約 6,800 人分。口座情報・各種金融申込書等。内部紛失の可能性。
・アメリカンファミリー生命保険、約 17,800 人分。各種保険情報等。内部紛失の可能性。
・ジェーシービー、約 7,600 人分。カード情報。FD 紛失。
・岡山市の訪問介護施設「コスモケアサービス」、約 90 人分。ファイル紛失。
・東京電力千葉支店、16 人分。口座番号等紛失。
・名古屋市の水道局、28 人分。領収書等紛失。
・昭和シェル石油系列のガソリンスタンド(横浜市)、700 人分。クレカ伝票。盗難。二次被害（カード不正利用）138 件。
・旅行会社のクラブツーリズム(近畿日本ツーリスト系列)、約 9 万人分。ID・パスワードほか。不正アクセス。

個人情報漏洩事件 36 件の内訳
　個人情報保護法施行後 約一ヶ月、ニュースになった個人情報 漏洩事件を分析
ＰＣ関連 13
　PC 盗難（自宅持ち出し）７、PC 盗難（会社保管中）　３　ウイルス　２
　ＰＣ廃棄－処理不十分　１
誤送付、誤送信 9
　郵送 5　FAX３　Ｅメール１　社員不正１

書類紛失盗難等 11
　紛失８　盗難　３　システム不備
（CCN サイトより）http://www.careercity.net/policy/p_m12_news.shtml

３－２　情報漏洩事件の影響

情報漏洩に対するデメリットは、社会的信用の失墜だけでなく、賠償問題に発展する
メディアの大容量化、モバイル PC の高性能化によって、大量のデータが一瞬で持ち出しできる
データを簡単にコピーされてしまうことで、事実上被害の復旧は不可能になる
情報漏洩の事実は、顧客を含めた外部からしか発見されない。管理体制の不備が大きく問われる

３－３　個人情報盗用のハイテク技術

ハッキング Hacking
　不正アクセス
スパイウエア Spyware
　ユーザに気付かれないように個人情報などを収集し、ソフトウェアの開発元などに送信してしまうソフトウェア
　集めた個人情報は広告の配信などに利用。
　企業が配布しているフリーソフトウェアなどに添付されていることが多く、広告などを強制的に表示する機能を持ったものもある。
　スパイウェアはフリーソフトやシェアウェアなどに添付されていることが多く、そのソフトをインストールすると一緒にインストールされる。
　常時起動するように設定され、そのユーザのメールアドレスなどの個人情報や、Web ブラウザのアクセス履歴やクッキーに記録された情報などを配布元に送信する。
　配布もとの企業等はこの情報を基に広告を配信したり別の業者に情報を売ったりして利益を得る。
　スパイウェアがインストールされているかどうかを調べ、発見したスパイウアを取り除くソフトがある。
　Lavasoft 社の「Ad-aware」
　Patrick Kolla 氏「Spybot　Search&Destroy」 などが有名
　いずれも無料でダウンロードし利用可能
スキミング Skimming

他人のクレジットカードやキャッシュカードの磁気記録情報を不正に読み出してコピーを作成し、使用する犯罪行為。

「スキマー」と呼ばれるカード情報を読み取る装置を用いて情報を複製する。

手口

飲食店などで客の上着に入ったクレジットカードから情報を盗み出す。

空巣に入ってカードは盗まず情報だけを取り出す。

クレジットカード取扱店の CAT 端末(加盟店信用照会端末)に細工をしてスキマーを仕掛ける。

フィッシング Phishing

釣り」(fishing) ではなく (Phishing)

Phreaking(ハッキングの意味)と fishing の合成による造語説

実在の銀行・クレジットカード会社やショッピングサイトなどを装ったメールを送付、リンクを貼り付けて、その銀行・ショッピングサイトにそっくりな「罠のサイト」に呼び込み、クレジットカード番号やパスワードなどを入力させて入手

現在アメリカで被害が急増､フィッシング型の迷惑メールが 2003 年 9 月では 279 件､2004 年 3 月には 21 万 5643 件にまで達した。

ファーミング Farming

可能な限り多くのユーザーを、本来訪れようとしている合法の商業ウェブサイトから悪意あるウェブサイトへ自動的に導く

被害者たちが知らぬ間に誘導される偽サイトは、見た目は本物のサイトと変わらない。

だがユーザーが自分のログイン名とパスワードを入力すると、その情報はサイバー詐欺師たちに盗まれてしまう

ファーミング詐欺は 1 度で何人もの被害者をまとめてつかまえられる。

小規模なファーミング詐欺

電子メールを通じて拡がり、感染した個々のパソコンのローカルホスト・ファイルを書き換えるウイルスを使って行なわれてきた。

ホストファイルが書き換えられていると、ユーザーが正しい URL を入力しても、不正なウェブサイトにつながってしまう。

DNS ポイズニング Poisoning

DNS(ドメイン・ネーム・システム)は、ドメイン名と電子メールの IP アドレスを変換する

DNS サーバーを「毒に汚染される」､すなわち、どのドメイン名がどの IP アドレスに相当するかという情報に手が加え、偽の情報に書き換えると、ユーザーが正しい URL を入力しても、知らないうちに偽のサイトにつながるようになる。

DNS システムの設計に脆弱性への攻撃

３－４　個人情報漏洩の対策

Yahoo!BB の対策

組織面の対策

社外のメンバーから成る個人情報管理諮問委員会の設置によって情報管理についての審議・提言

情報セキュリティ管理責任者に常務取締役を任命し、情報セキュリティポリシーを策定し、部門ごとにも責任者を任命

情報保護のための物理的対策

情報システム開発業務と他の業務とを切り離し、顧客情報を扱う情報システム運用/コールセンターの業務は高セキュリティエリアで実施

高セキュリティエリアへは入室制限を行い、CISO が入室許可を出すようにする。高セキュリティエリアからの添付メールの禁止、外部記憶装置の持ち込み禁止、メール監査機能の追加などを行う。

運用面の対策

　顧客情報への常時アクセス権限を持つ人数を制限し、3 名まで絞る予定。

　顧客情報は他記憶媒体へコピー・印刷できないようにする。

顧客情報へのアクセス記録は半永久的に保存する。

従業員向けの対策

　派遣社員を含む従業員に個人情報保護教育を施し、また再度誓約書を結ぶ。

　全ての派遣会社および従業員と再度誓約書を締結し、情報セキュリティポリシーおよび運用ルールの違反者には処罰を与える。

業務委託先との契約をすべて見直し、契約書に次の項目を必ず含めて再締結する。

o 機密保持義務 o 再委託に関する事項

o 事故時の責任分担 o 契約終了時の個人情報の取り扱い o 個人情報に関する取り扱い状況の監査権

アッカ・ネットワークスの対策

１．顧客データベースへのアクセス管理の強化

すべての顧客情報データベースに常時アクセス可能な権限を廃止。

顧客情報データベースへアクセスできる者は、事件発覚当時の 466 人から 61 人にする。情報セキュリティ最高管理者がネットワークの障害対策上必要と認める者にアクセスを認める。

　上記のアクセス権を持つ者は、通常のオフィスから隔離された高セキュリティールームでのみ可能とし、アクセスしたユーザ、日時、アクセス内容の記録は半永久的に保存する。高セキュリティルームは、入室権限者の限定、事前登録制による作業、監視人員による監視の下での作業、全ての端末からインターネット接続は不可、端末外部へのデータ出力不

可、私物の持込不可とする。
２．顧客情報参照用の社内共有アカントを廃止。
情報システム部門のアクセス権限の制限を行う。具体的には、情報システム部内に入室できる権限を情報システム部員に限定する。また、情報システム開発者が顧客情報データベースにアクセスする必要がある場合には、アクセス権限の有効期限を一日以内に制限する。
３．データの管理強化
社内のパソコンで、フロッピーや MO などの外部記憶装置の使用ができない環境に整備。
社外向けのメールをすべて保存し、監督者が常時閲覧できるようにする。
顧客サービス運用部門ではインターネットの利用を禁止。
３．情報セキュリティ監査の実施
情報セキュリティ監査では、ビジネスプロセスの分析や情報資産の洗い出し等の事前調査の実施後に、外部機関による監査を行い、その後のリスク評価に基づいた改善策の策定と実施までを行っていく。
情報システムの技術面、情報システムの開発・運用管理面、及びビジネスプロセス・体制面からセキュリティの現状を総合的に監査
特に、以下の３つの観点を重点に監査を実施する。
個人情報保護の管理体制・プロセス
情報セキュリティの管理体制・プロセス
システムセキュリティの確保
４．情報セキュリティ教育の実施
上記監査の実施に合わせて、事業内容、対象者の役職等に応じたセミナー形式の集合教育と ｅ ラーニングの組み合わせを作成し、それに基づく情報セキュリティ教育を、正社員および派遣社員に対し全社的に行う。
同教育を通じて情報セキュリティおよび顧客情報保護の重要性に対する社員等の理解を促すと同時に、情報セキュリティに関するルール遵守を徹底させ、情報セキュリティの強化を図る

（４）情報漏洩対策のポイント（１）
セキュリティポリシーの策定
セキュリティ対策の全体方針策定
セキュリティ管理の責任者の体制
高セキュリティルームの設置
とくに重要な個人情報のファイルを保存するスペース
入退室の制限と入退室の記録
外部記憶装置の持込禁止
高セキュリティ室からの外部アクセス禁止

インターネットに接続しない
個人情報データへのアクセス管理
アクセス権の管理（システム、ファイル単位）
 アクセスログの記録と保存
組織メンバーのセキュリティ管理の徹底
派遣社員・アルバイトを含めた従業員に対する
　　セキュリティ教育
機密保持違反に関する契約
セキュリティ監査
組織外部の人間によるセキュリティ管理体制の監査
基本技術
認証技術
暗号化技術
PC 操作等のログ取得・保管・活用技術
不正アクセス防止・ウイルス対策

個人情報保護法
個人の権利と利益を保護する為に、個人情報を取得し取り扱っている事業者に対し、様々な義務と対応を定めた法律
2005 年 4 月より全面施行
（NTT コミュニケーションズ　個人情報保護法ガイド）
（http://www.ntt.com/business/p-info/gaiyo.html
義務と罰則
個人情報を収集する際には利用目的を明確
目的以外で利用する場合には、本人の同意を得る必要。
個人情報を収集する際利用目的を通知・公表
情報が漏洩しないよう対策を講じ従業員だけでなく委託業者も監督
個人の同意を得ずに第三者に情報を提供してはならない。
本人からの求めに応じ情報を開示しなければならない。
公開された個人情報が事実と異なる場合、訂正や削除に応じなければならない。
個人情報の取扱いに関する苦情に対し、適切・迅速に対処しなければならない。
主務大臣の命令に違反した場合や、報告義務に違反した場合には罰則が科せられる。
命令に対する違反の場合　6 月以下の懲役または 30 万円以下の罰金
報告義務違反の場合　30 万円以下の罰金
米国における個人情報漏洩と保護対策

松尾和洋：“行き届いたサービスか、プライバシー保護か” 、情報処理、２００５、Vol.46.No.5、ｐｐ。５７８－５７９

３－５　米国における情報漏洩の現状

2004 年度
米国における ID 窃盗による詐欺の被害者は約 930 万人
被害総額は 526 億ドルに及ぶという調査報告あり
手口
PC,紙ファイル、郵便物など個人情報の書かれた媒体の盗難という従来の方法が大半をしめる。
インターネットを利用した、フィッシング、ハッキング、スパイウエアなどの技術的に高度なものはまだ比率が小さいが、今後増加が予想される
PC の盗難
2004 年 12 月
カリフォルニア州　Delta 血液銀行　10 万人の献血者情報
UCLA　14 万 5000 人文の献血者の情報漏洩
UC　Berkley　10 万人の卒業生、学生、過去　の入学志願者の情報漏洩

対策：　簡単に情報を読めない仕組みを記憶装置や PC に組み込む技術は可能
ハッキング
2004 年 2 月
カリフォルニア州政府のデータベースに侵入
140 人分の住民の個人情報が流出
2005 年 1 月
バージニア州　George　Mason 大学がハッキング
教員や学生の個人情報 3 万人分が流出
携帯電話会社　T-Mobile　システム侵入　多量の顧客情報流出
スパイウエア
当初オンライン広告に必要な情報を吸い上げる目的で Clara 社が開発。
悪用すれば個人情報を盗用可能
実態は把握できていない。
大手 ISP 業者　EarthLink の推定
ネットワークに接続された PC の９０％にスパイウエアが入っており、1 台あたり平均 25 種類

フィッシング、ファーミング
フィッシング：
　米国では増加を続けている
対策団体　APWG（Anti-Phishing Working　　Group）の集計
今年２月　フィッシングサイト　2，600以上
サイトの継続期間は平均5．7日
フィッシングメール　昨年7月から月２６％で増加
月に1．3万件

フィッシングサイト
主は　金融機関、大手オンラインショップ
人気小説「ハリーポッター」の最新本販売サイトも
対策
２種類以上の個人認証手段を使う
予防的スキャンソフトを使う
eBay　利用者の連絡に電子メールを使わず、
　　マイメッセージという独自の機能でメッセー　　ジを伝達する方法を取り入れた
新たな手口　ファーミング
ボットネット（ゾンビネット）
ネットワークエージェント技術を悪用
　（エージェント：　（ロ）ボット、または、ゾンビと呼ぶ）
ハッキングまたはウイルスにより、多数のコンピュータにエージェントプログラム侵入させる
ネットワーク通信でコントロール可能
いくつかの機能がプログラム化され、遠隔指示で機能が働く
中央指示プログラムを通じて、多数のコンピュータのエージェントを一斉に同じ動作をさせる。

悪用方法
コンスタントに各コンピュータの内部情報を収集して中央に送信
一斉に各コンピュータの内部情報を収集
一斉に各コンピュータデータを破壊
一斉に各コンピュータから、特定Webやコンピュータに、攻撃メールを送出（Web攻撃）
サイバーテロ攻撃にも利用される

米国政府の対応

米国では、個人情報の盗難とそれを悪用した犯罪について一括して扱うところがない。

個人情報保護法は 1968 年に制定、1984 年に改定「電気通信プライバシー法」

さらに広いプライバシー保護　一般、オンライン、金融、医療など個別の分野ごとに法律が制定されている。

連邦政府と州政府が別個に制定

州権が強い米国

　ネットワーク犯罪　－　州を越えた犯罪になる。

　　捜査が難しい