情報セキュリティの基礎1

テキスト P11–58

http://cobayasi.com/koza/security/1_basic1.pdf

守りたい対象を整理し、セキュリティの適切なコストを算定する

情報のCIA

情報のCIA テキストP12-16

■情報の形態

保存形態：CD-RやDVD-R、紙、HDD、など

伝送形態：メール、FAX、手渡し、立ち話など

■情報セキュリティの考え方（指針）

情報の機密性(Confidentiality),完全性(Integrity),
可用性(Availability)を確保し、維持することにより、
様々な脅威から情報システム及び情報を保護し、
情報システムの信頼性を高めること

■情報を保全して安全に業務遂行するための指標

機密性(C)　完全性(I)　可用性(A)

■　機密性

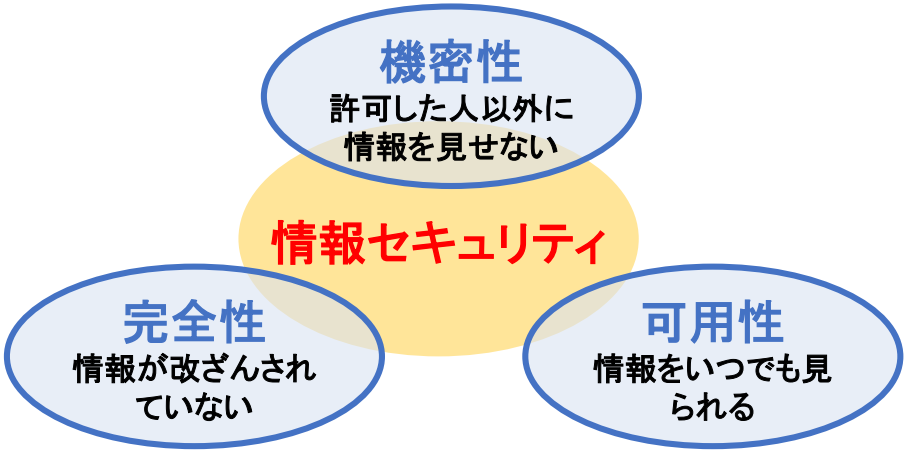
情報資源に対してアクセスをコントロールすることで、正当な権限を持った利用者だけが利用できる

■　完全性

情報が完全で正確であり、改ざんや喪失していないこと

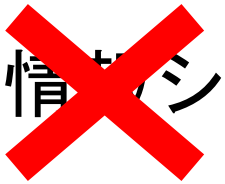
■　可用性

利用者が情報を利用したいときに、いつでも利用できることを保証する



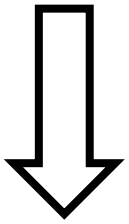
情報セキュリティの目的

クラッカーから情報システムを保護する



操作ミス

クラッカー



災害

故障

① 情報資産の保護（と管理）
② 顧客からの信頼獲得
③ 競争力、収益力の維持と向上

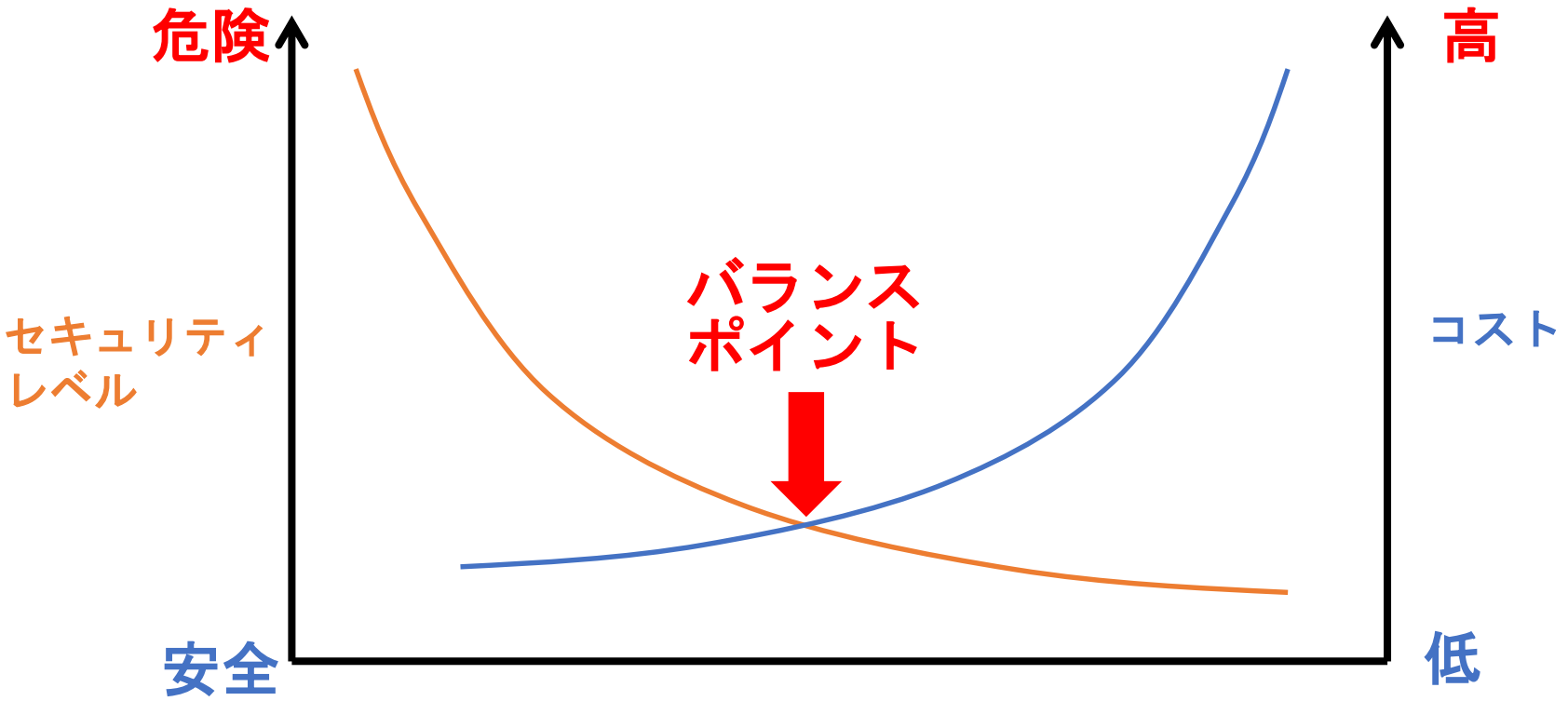
セキュリティ管理にはコストがかかる

セキュリティ管理にかかるコストの例

- セキュリティ機器の購入
- 業務手順の煩雑化
- 警備員の導入　など

すべての社員の協力が必要
経営層の参加が必須

セキュリティとコストのバランス



セキュリティ投資とコストには, バランスポイントが生じる
バランスポイントを見つけて上手に運用することが必要

情報資産，脅威，脆弱性

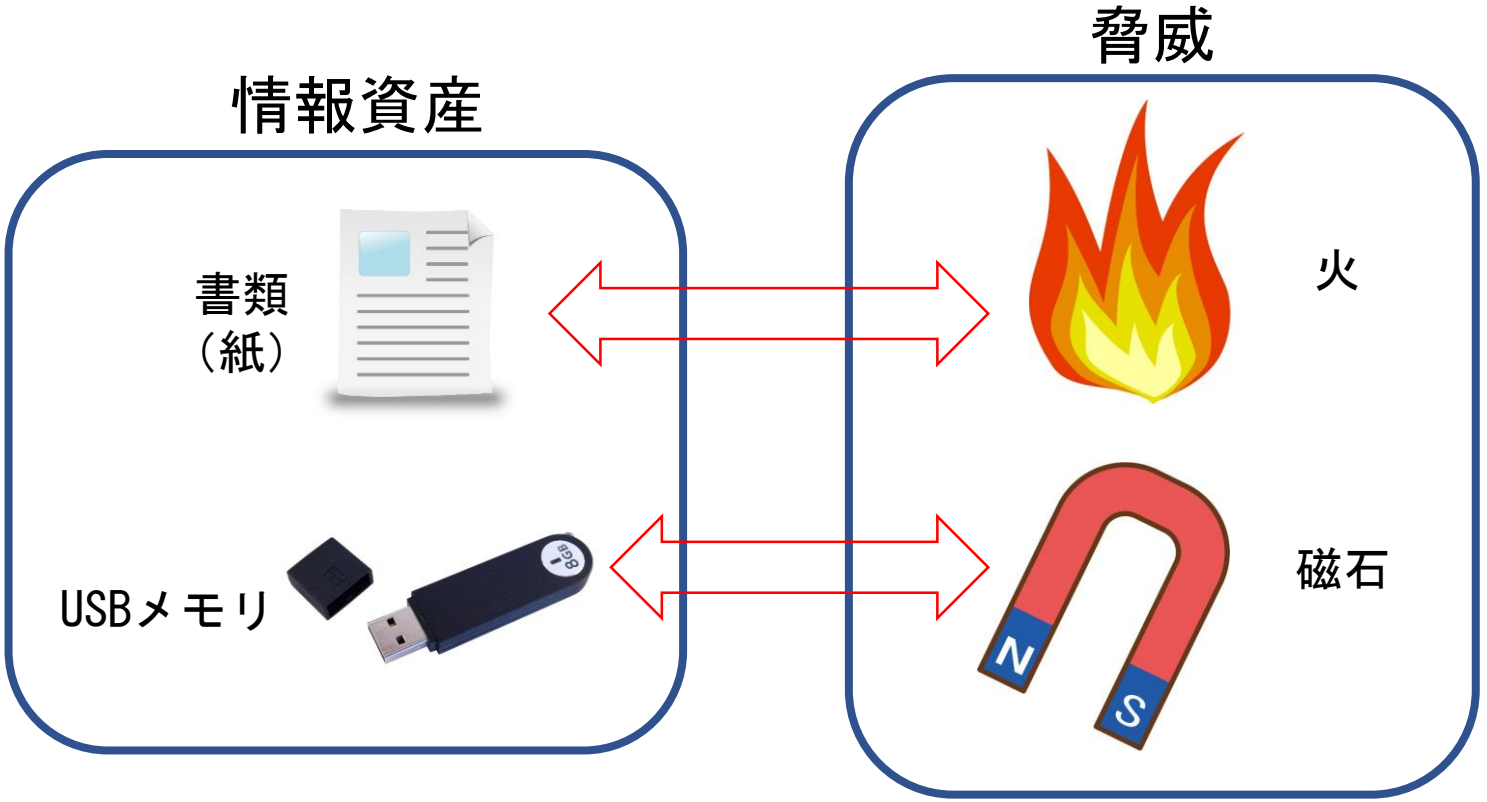
1. 情報資産・脅威・脆弱性
2. 脅威の種類
3. 脆弱性の種類

企業が業務を行う上で生み出される価値あるもので、目に見えないもの

情報資産と脅威 テキストP18-32

情報資産の明確化

情報セキュリティの中で保護されるべき対象（情報資産）を明確にし、これに対する脅威を明らかにする



情報資産管理台帳

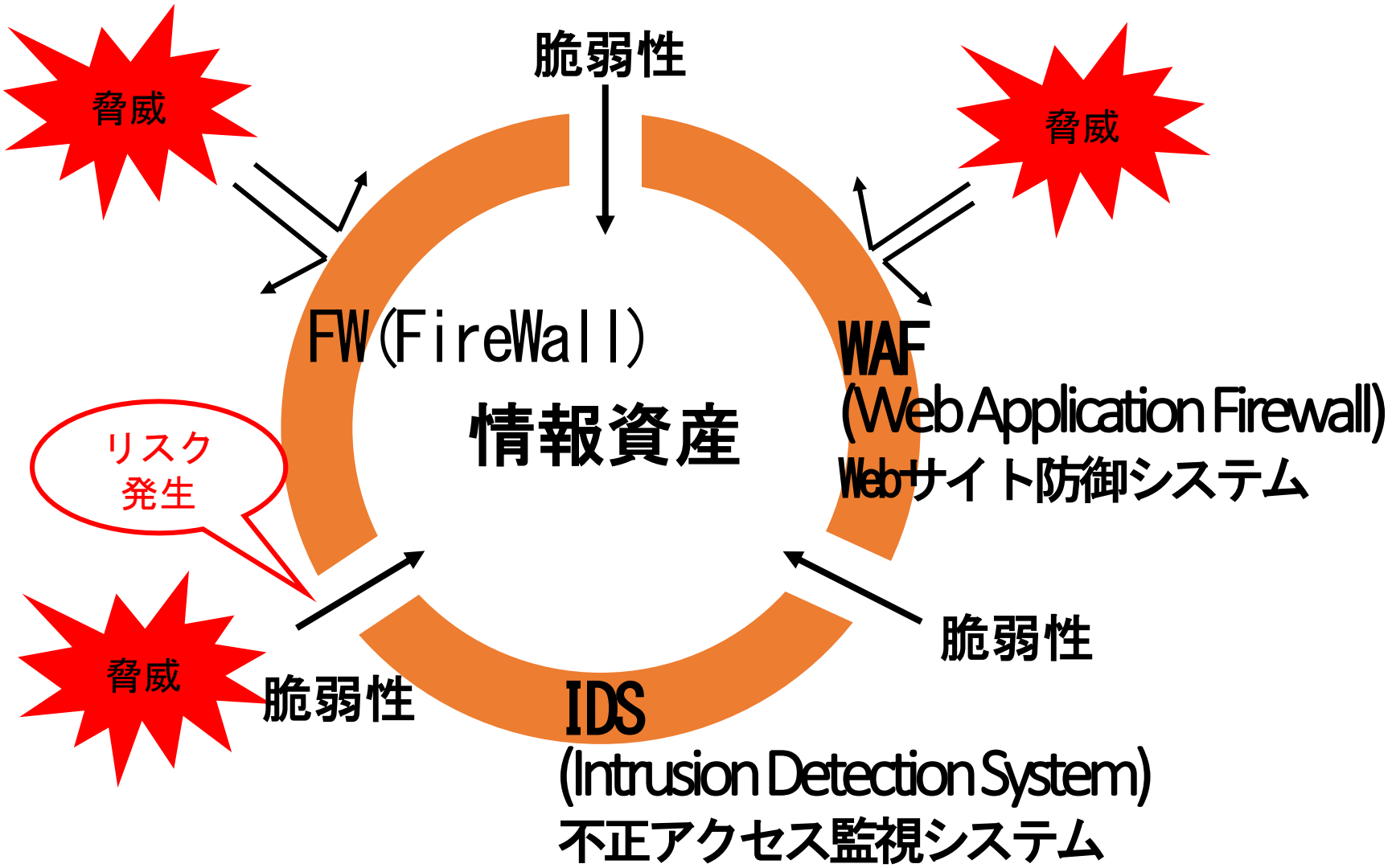
情報資産を明確に把握するための情報(業務名, データ名など)を一覧できる台帳

情報資産管理台帳												
部門名：										作成日：		
										作成者：		
番号	業務名	書類・データ名	詳細内容	管理責任者	保管責任者	所在・保管場所			保管期間		個人情報を含む	備考
						紙	電子データ		紙	電子データ		
							サーバ／クライアント	媒体				

情報資産管理台帳の一例

リスクが顕在化する状況

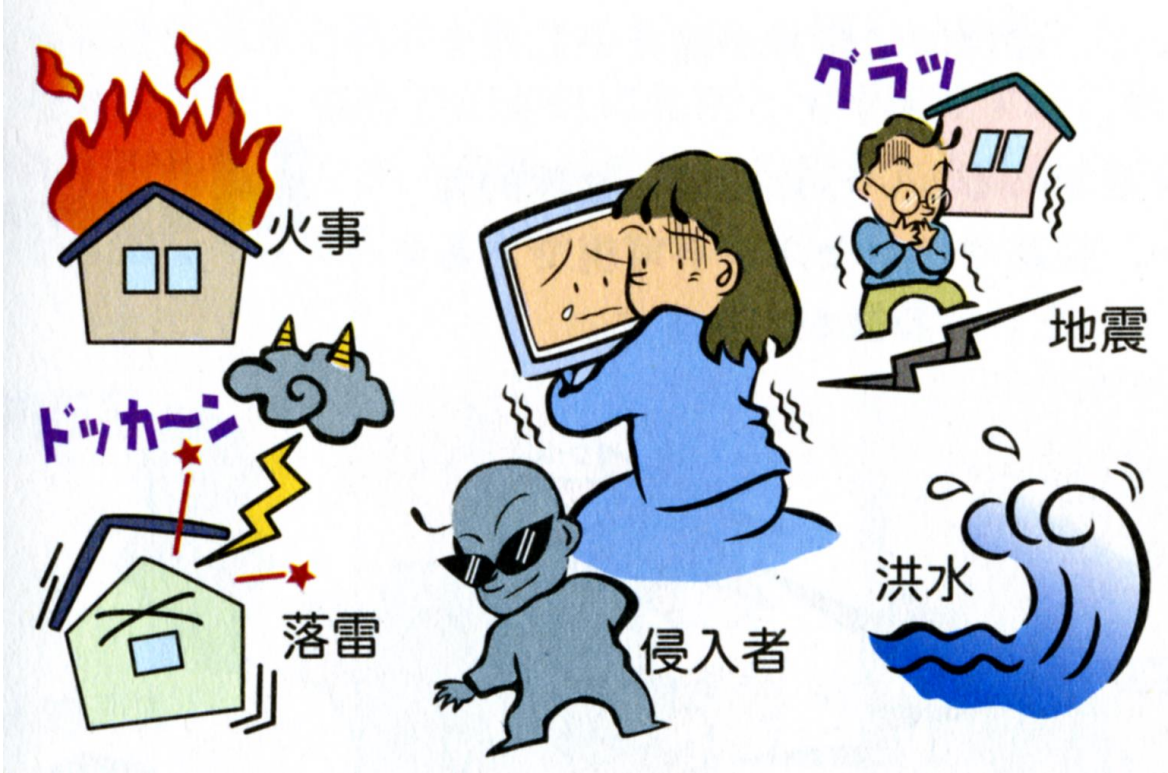
脆弱性の存在



脅威の種類

物理的脅威

火災や地震、侵入者によって機器の破壊など、
直接的に情報資産が破壊される脅威

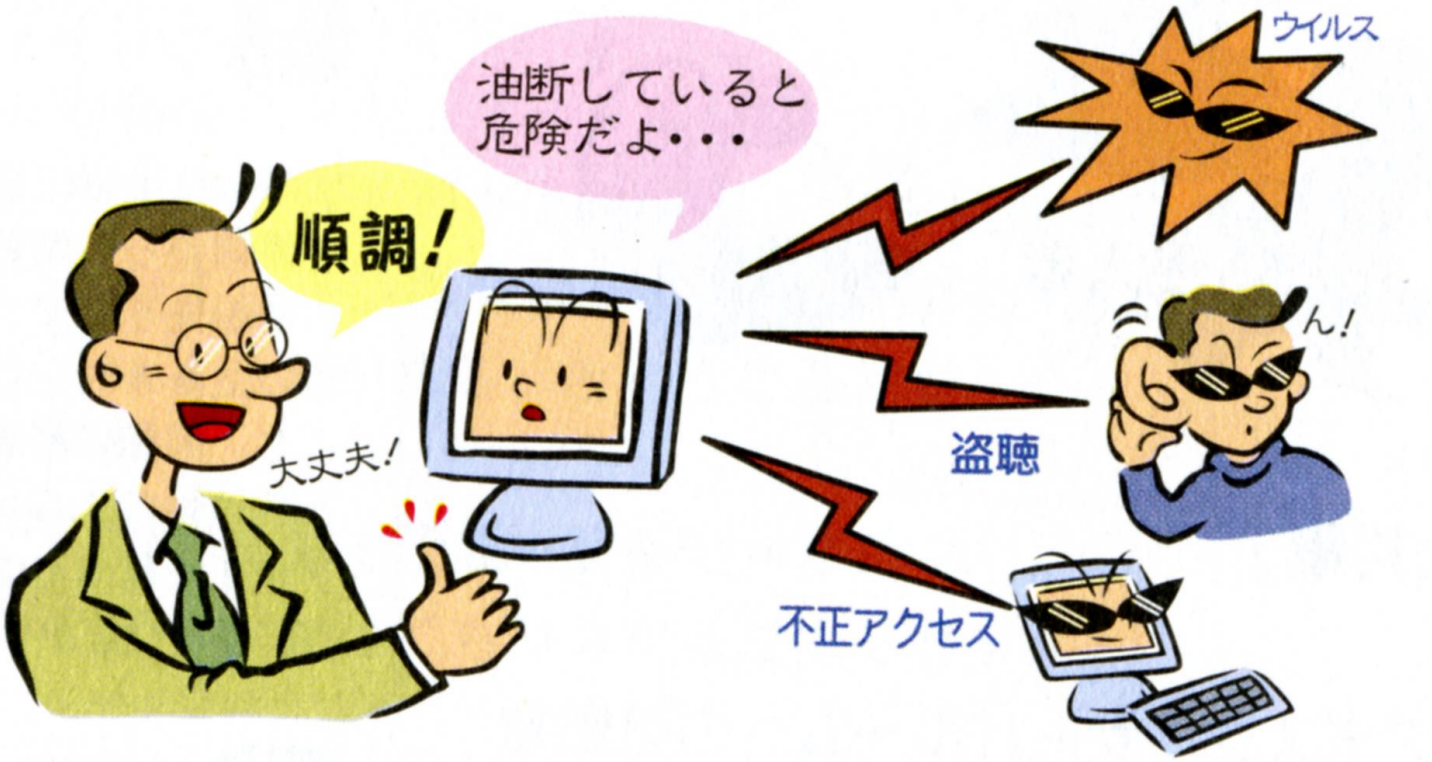


物理的脅威の種類と対策

種類	対策
火災	防火壁の導入、クリアデスク、可燃物の持込み禁止など
地震	バックアップサイトの設置、免震構造社屋、データの遠隔地保存など
落雷や停電	予備電源の確保、避雷針の設置、UPSやCVCFの設置など
侵入者による物理的な破壊や盗難	警備員の設置、入退室管理の徹底、モバイル機器や書類の施錠管理など
過失による機器やデータの破壊	バックアップの取得、フールプルーフ設計、一般事務室とサーバルームの分離など
機器の故障	機器の二重化、予防保守の実施、ライフサイクルの管理など

技術的脅威

ソフトウエアのバグやコンピュータウイルス、不正アクセスなど、**論理的に情報が漏洩したり、破壊されたりする脅威**

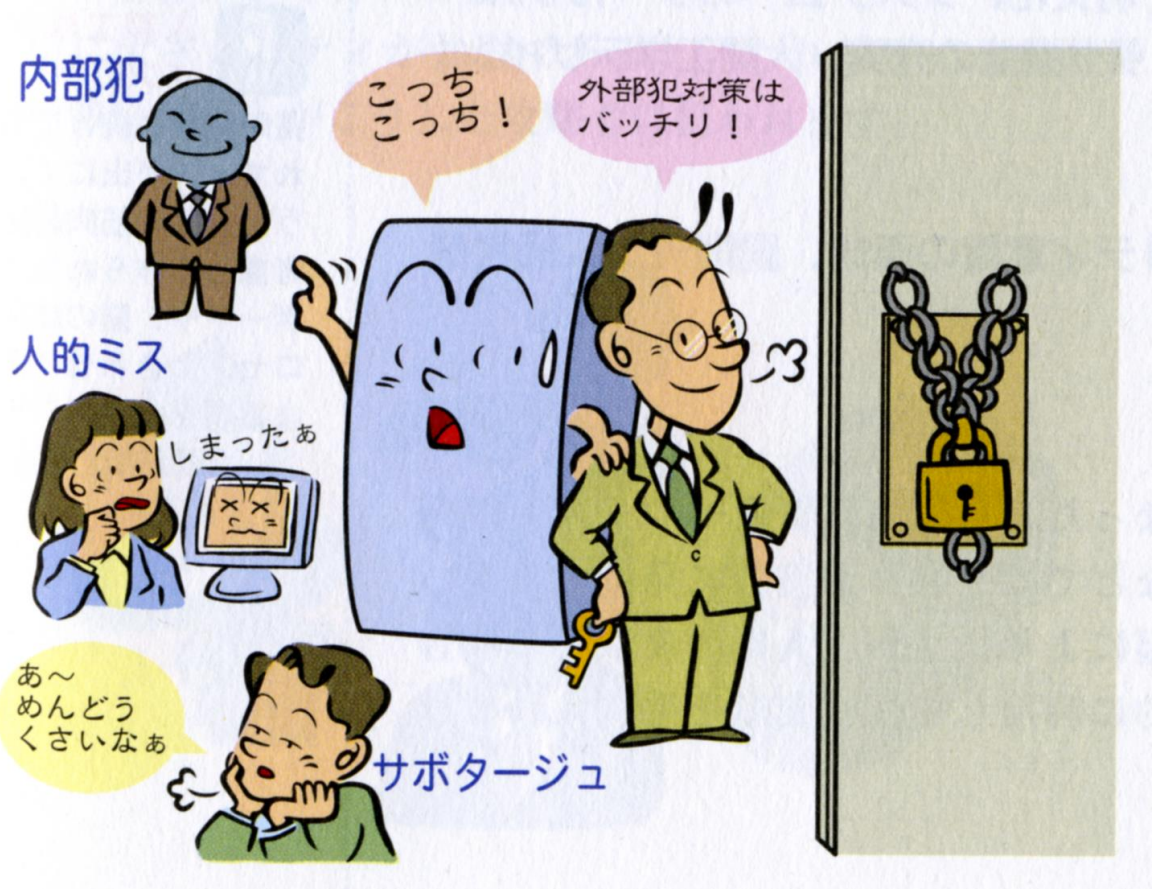


技術的脅威の種類と対策

種類	対策
不正アクセス	認証の設置、ログの監査など
盗聴	データの暗号化など
コンピュータウィルス	入手経路が不明なファイルの取扱い規定、ウィルスチェックソフトの導入など
ソフトウェアのバグ	ソフトウェア設計の規定、テスト規定の策定、ソフトウェアライフサイクル管理など

人的脅威

人的ミスによるデータや機器の破壊、組織内部の人間による確信的な犯行によって情報資産が漏洩したり、失われたりする脅威



人的脅威の種類と対策

種類	対策
内部犯	セキュリティリテラシの向上、継続教育によるセキュリティ意識の醸成など
人的ミス	業務手順の明確化・明文化、システムへのフールプルーフ機構の導入など
サボタージュ	教育によるセキュリティ意識の醸成、罰則規定の策定など

人間は必ずミスを犯します。セキュリティ侵害が起こる最も大きな原因の一つが人的なミスである

攻撃者の目的

知的好奇心

ハッキングの動機として、最も割合が高く、システムの詳細な仕様を知りたい、企業活動の秘匿されている部分を知りたい、などの知的好奇心を満足させることが目的。

金銭

近年に増加傾向で、盗み出した情報を金銭に変えることが目的。内部犯の犯行が多い。

自己顕示欲

自分の情報システムの知識を見せびらかすことが目的。ホームページの改ざんなどに多く見られる。

攻撃者の種類

ハッカー

もともと「情報システムに詳しいユーザ」の敬称。クラッカーとは異なり、非犯罪的な目的で、情報システムへの侵入などを行い、知的好奇心の発露とする。近年は、こうした行為も犯罪になる。

クラッカー

犯罪的な目的で、情報システムへの攻撃を行い、業務妨害やテロの手段として利用する。

スクリプトキディ

ITスキルが未熟なユーザが、いたずら目的や愉快犯などで、情報システムを攻撃するもの。

クラッカーなどが、作成した攻撃ツールを使って攻撃するので、適切なセキュリティ対策を施したシステムに対しては防御できる。

内部犯

正当なシステム権限を用いて情報資産を盗用・流用できるもの。

攻撃者としての割合が高く、大きな被害額になる場合がある。最近のセキュリティ対策は、内部犯に対する対策が主になりつつあるが、業務遂行に業務データなどのアクセスが必要不可欠であるため、完全な対策は取りにくい。

脆弱性の種類

物理的脆弱性

「社屋やコンピュータルームが耐震構造でない」「コンピュータルームに可燃物が放置されている」「社屋への進入路が解放されている」など、物理的な対策でコントロール可能な弱点を指す。

耐震・耐火構造の不備
ファシリティチェック(社屋に入れる人員のコントロール)の不備
機器故障対策の不備
紛失対策の不備

技術的脆弱性

「ソフトウェア製品のセキュリティホール」「コンピュータシステムへのウィルス混入」「アクセスコントロールの未実施」など、システムの設定やアップデートでコントロール可能な弱点を指す。

近年、ネットワークの常時接続によって、この対策の必要性が増している。

アクセスコントロールの不備
コンピュータウィルス対策の不備
セキュリティホール対策の不備
テストの不備

人的脆弱性

「内部犯のよる情報源の持ち出し」「オペレータの過失によるデータの喪失や誤入力」など、人間が介在する弱点を指す。

「人材の流動化やシステムの複雑化・分散化」「情報の持ち運び易さの拡大」などの要因で、コントロールが難しい。

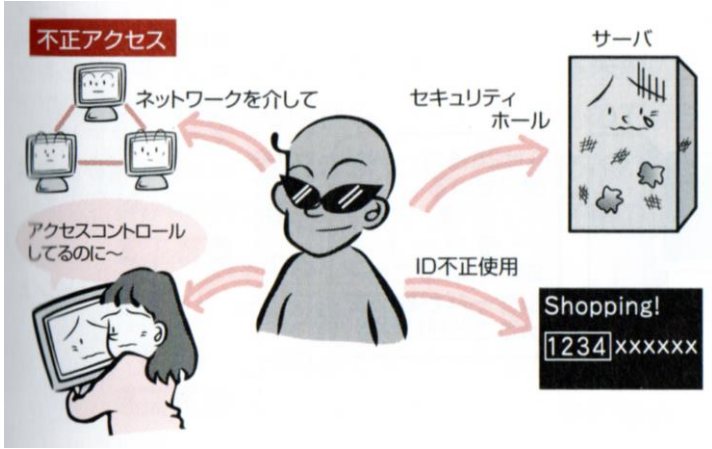
組織管理の不備
過失
権限の明確化
状況的犯罪予防
不正のトライアングル
（機会, 動機, 正当化）

サイバー攻撃手法

1. 不正アクセス
2. 盗聴
3. なりすまし
4. サービス妨害
5. その他の攻撃手法

不正アクセス

テキストP35-40



システムを利用する者が、与えられた権限によって許可された以上の行為を、ネットワークを介して意図的に行うことを、**不正アクセス**と呼ぶ

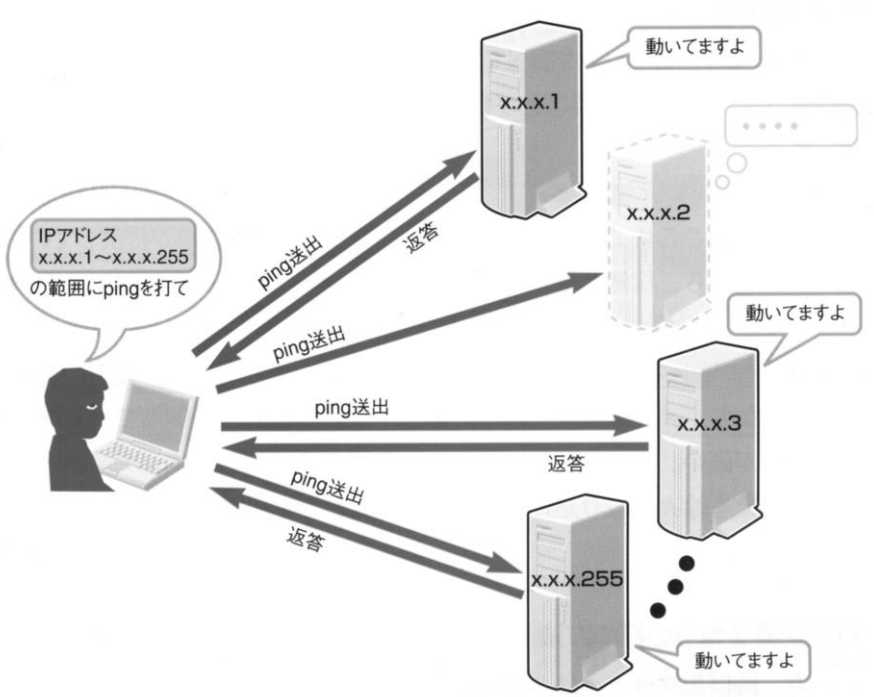
不正アクセス行為（他人のパスワードを使うなど）や不正アクセス助長行為（他人のパスワードを流出する行為など）を禁止する法律に、「不正アクセス禁止法（正式名称：不正アクセス行為の禁止等に関する法律」がある

アクセスコントロールされているシステムが保護対象（コントロールの方法は対象外）

不正アクセスの方法

ネットワークスキャン

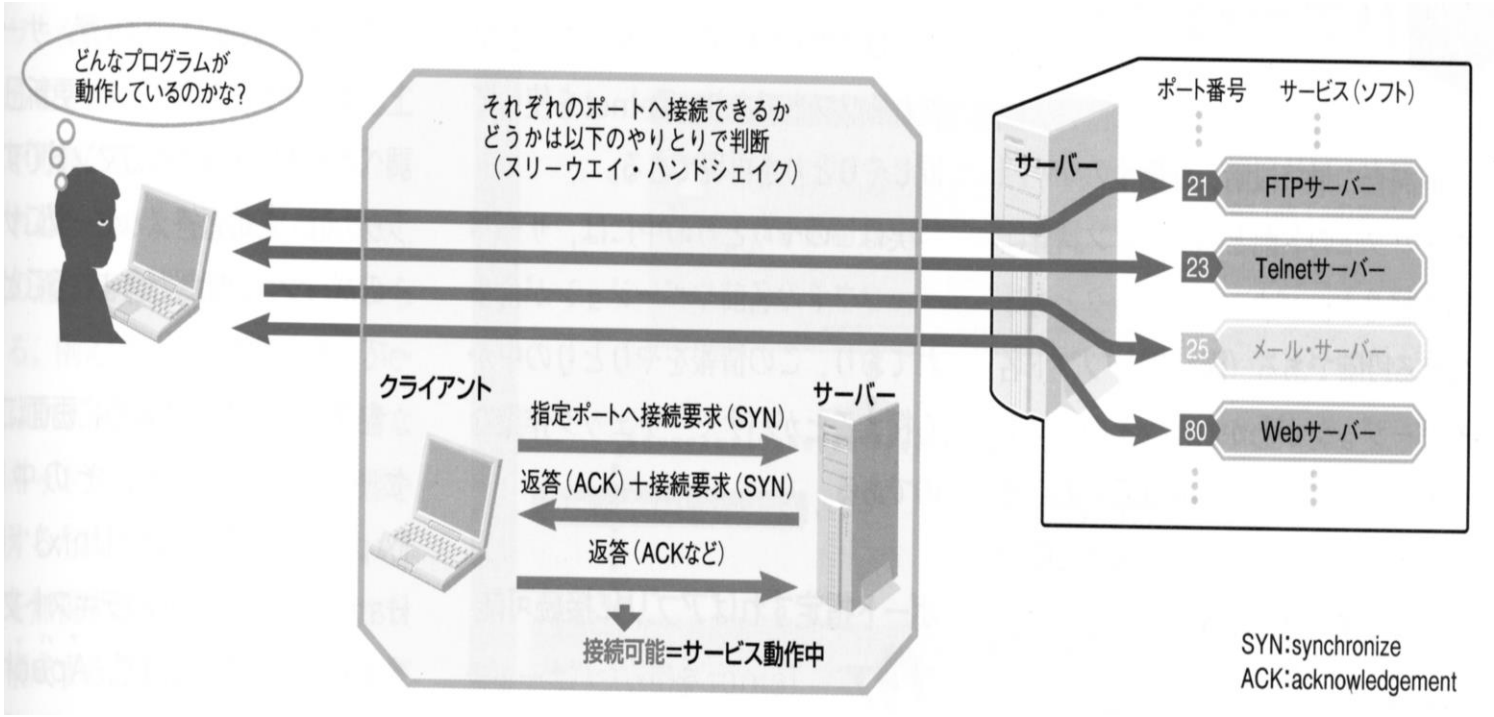
攻撃対象のシステムを特定するための準備行為として、考えられるIPアドレスに対してネットワークコマンドpingを実行して、攻撃相手のシステムの存在を確認する



ポートスキャン

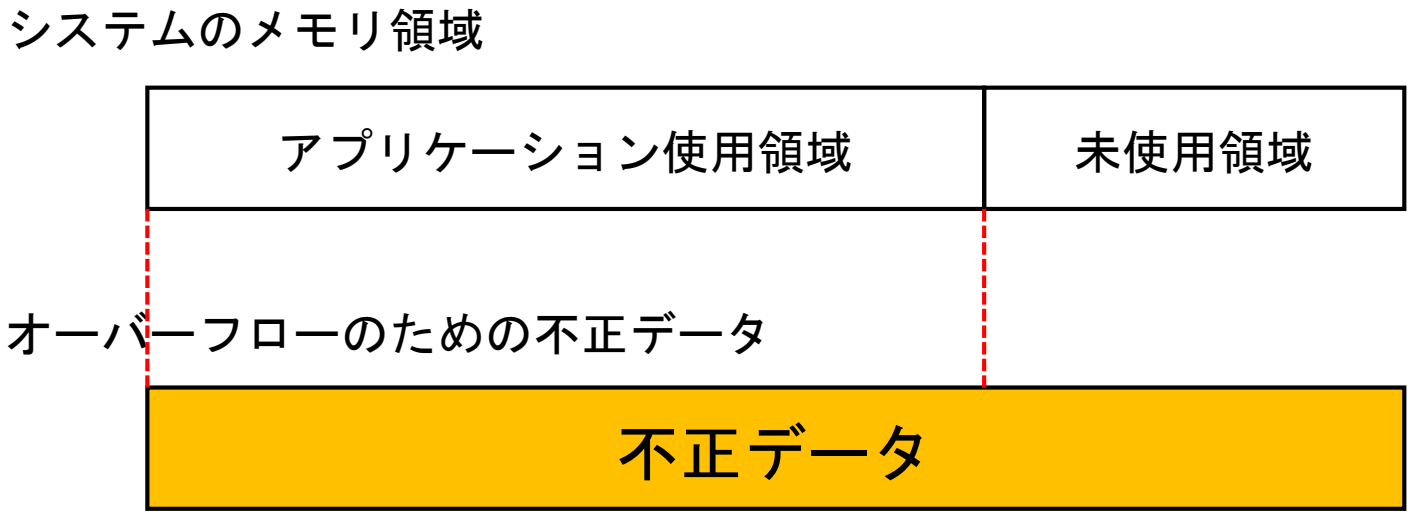
攻撃相手のシステムで使用されているアプリケーションの動作を確認する。システムの用途や管理者のスキルの程度を知り、システムの脆弱性を見つける。

＜対策＞
「不必要なポートを閉じる」「ポート開放時には認証する」「公開サーバはDMZ(非武装地帯)に設置する」



バッファオーバーフロー

攻撃相手のシステムへの進入行為として、**システムで使用しているメモリの容量を超える不正データで内容を書き換え、システムを不正な動作に導く。**



＜対策＞
「システムの設計・開発時にチェック機能を盛り込む」「セキュリティホールの情報を常にチェックして、セキュリティパッチを当てる」

パスワードの取得方法と対策

管理者権限を奪うための簡単な手段

ブルートファースアタック（Brute Force Attack/Brute Force Password Cracking：総当たり法）

考えられる全てのパスワードの組み合わせを試みる

＜対策＞
「長いパスワードを利用する」「パスワードを頻繁に変更する」「何回かログインに失敗した場合に、アカウントロックする」

辞書攻撃

パスワードの候補として使用される単語を体系化したデータベースを利用して、パスワードを探る。

攻撃対象が明確に定まっている場合に有効で、事前に管理者の「生年月日」「ペットの名前」「電話番号」などを入手して、データベースに登録する。また、ブルートファースアタックと併用することで、効果的に目的のパスワードへ到達することができる。

＜対策＞
「辞書に載っているパスワードは使わない」「できる限り、長いパスワードを使う」「小文字, 大文字, 数字, 記号を混在したパスワードを使う」「個人情報（生年月日など）を使ったパスワードは使わない」

パスワードリスト攻撃

あらかじめ用意したいくつかのパスワードを試みる。

管理者の中には、数種類のパスワードを、複数のシステムで、使いまわしている場合がある。これらのパスワードを使って、不正アクセスを行う。

＜対策＞
同じパスワードを、複数のシステムで使用しない

侵入後の危険性と対策

一度不正アクセスに成功した侵入者は、侵入の証拠を隠滅したり、再侵入のための布石をうつ。(準備をする)

ログの消去

侵入者が、侵入した経路や(侵入者の)マシンを特定されないように、ログを消去して、侵入の痕跡や証拠を抹消する

＜対策＞
「侵入者の推測しにくい場所にログファイルを置く」「ログファイルをを暗号化する」

バックドア

侵入者が、再侵入する際の時間と手間を短縮するために、特別な進入路（バックドア）を確保する。

侵入後に、システムのパスワードやデータが変更されたことを知らせる機能などが盛り込まれた監視プログラム。

＜対策＞
「ファイヤーウォールの設置」「システムから送信されるデータをチェックする」

盗　聴　テキストP41-44

　ネットワーク上に流れるデータを取得する行為を指し、積極的な攻撃行為をしなくても、盗聴行為できる可能性がある

盗聴方法と対策

スニファ(Sniffer)

インターネットに関する技術の標準を定める団体(IETF)が正式に発行する文書

　ネットワーク上を流れるパケットをキャプチャして、内容を解析する。パケットの内容は、RFC(Request For Comments)で標準化しているので、簡単に解析できる。

＜対策＞
「データの暗号化」「入退室管理の実施」「情報資産管理の徹底」

電波傍受

無線LANの通信内容を傍受して、パケットの内容を解析する。

＜対策＞
「ステルスモードでの運用」「ANY接続での運用禁止」「WAP2などによる暗号化パスワードによる接続」

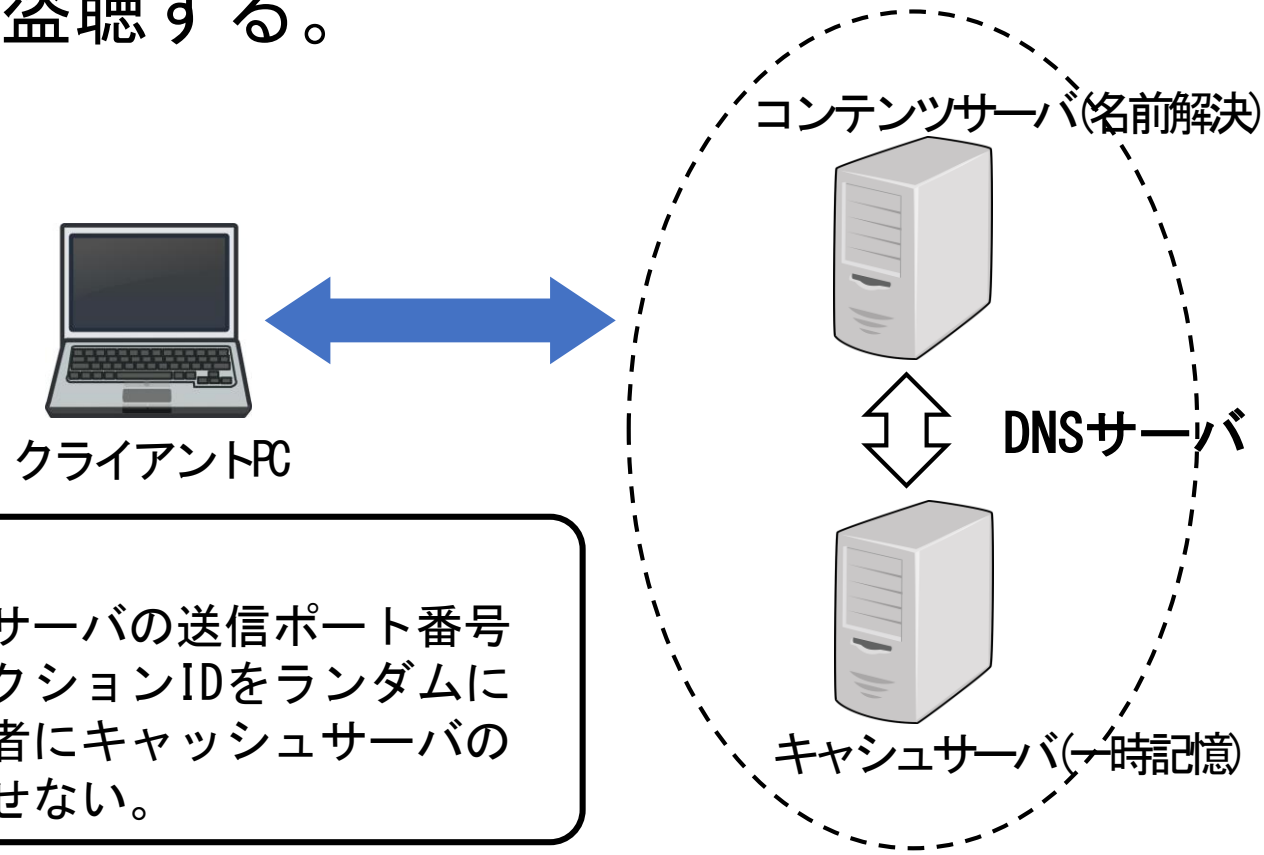
キーボードロギング

あらかじめコンピュータに、キーボードのタイプ履歴が記録できるログ・プログラム(キーロガー)をインストールして、タイプした内容を盗聴する。

＜対策＞
「不正ファイルの存在をチェックする」「共有・公共のコンピュータで重要情報などを入力しない」

DNSキャッシュポイズニング(DNS cache poisoning)

DNSサーバ(キャシュサーバ)に、偽りの情報を覚え込ませる。問い合わせに対して、この偽り情報を流して、他のサーバに誘い込み情報を盗聴する。



＜対策＞
キャッシュサーバの送信ポート番号やトランザクションIDをランダムにして、盗聴者にキャッシュサーバの存在を知らせない。

ディレクトリトラバーサル

通常はアクセスできないファイルやフォルダやディレクトリの内容を取得する

＜対策＞
ファイル名のみを入力できるようにし、/などのディレクトリの変更するための記号は、入力できないようにする

なりすまし　テキストP45-48

正規のユーザになりすまして、不正に情報を利用する権限を得る行為

なりすましの方法と対策

ユーザIDやパスワードの偽装

不正な手段で得たユーザIDやパスワードで、他人になりすます

＜対策＞
パスワード利用規定の整備

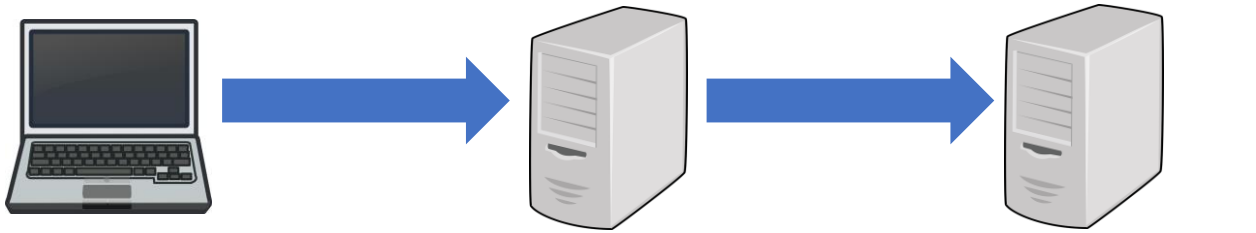
IPスプーフィング(IP spoofing)

不正な手段によって得た、**他人のコンピュータのIPアドレス**を使って、他人になりすます

＜対策＞
IPアドレスのチェックだけでなく、より上層(第4層や第5層以上)の情報を使って、本人認証をする

踏み台

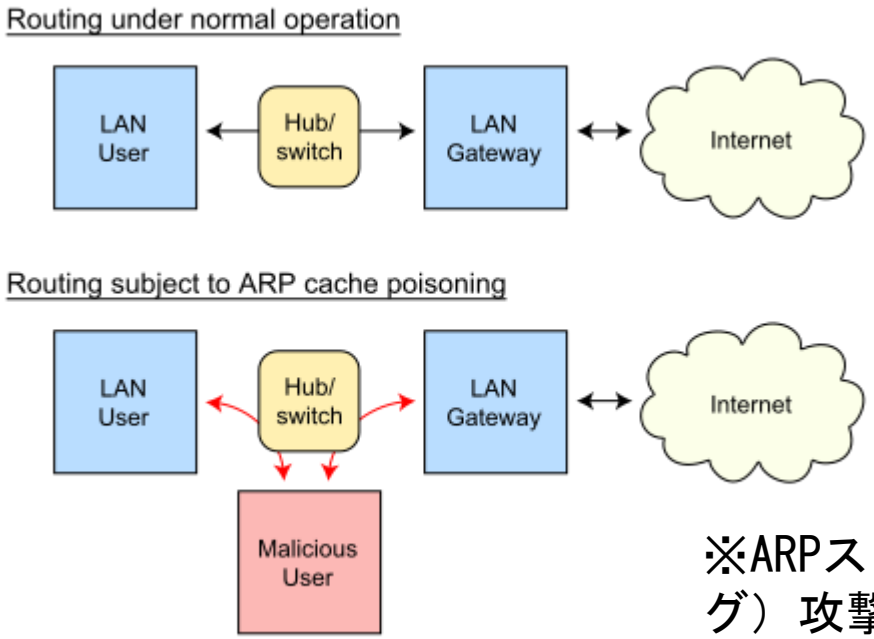
アクセスログを利用して、攻撃目的のコンピュータではなく、**第三者のコンピュータを介して、目的のコンピュータに不正アクセスする**



＜対策＞ 公開サーバ(第三者のサーバ)のセキュリティを強化する

ARPスプーフィング

ARPプロトコルの応答(ARP応答)を偽装することにより、LAN上で通信機器のなりすましを行なう



※ARPスプーフィング（ポイズニング）攻撃が成功すると、攻撃者がルーティングを変更できる

＜対策＞
ARPテーブル(IPアドレスとMACアドレスを対応づける表)を監視する

セッションハイジャック

ネットワーク上で一対の機器間で交わされる一連の通信（セッション）を途中で乗っ取り、片方になりすましてもう一方から不正にデータを詐取したり操作を行なう

＜対策＞
「セッション番号の割り当てに、乱数を使う」「ポート番号をランダムに振り分ける」「通信内容を暗号化する」

リプレイ攻撃

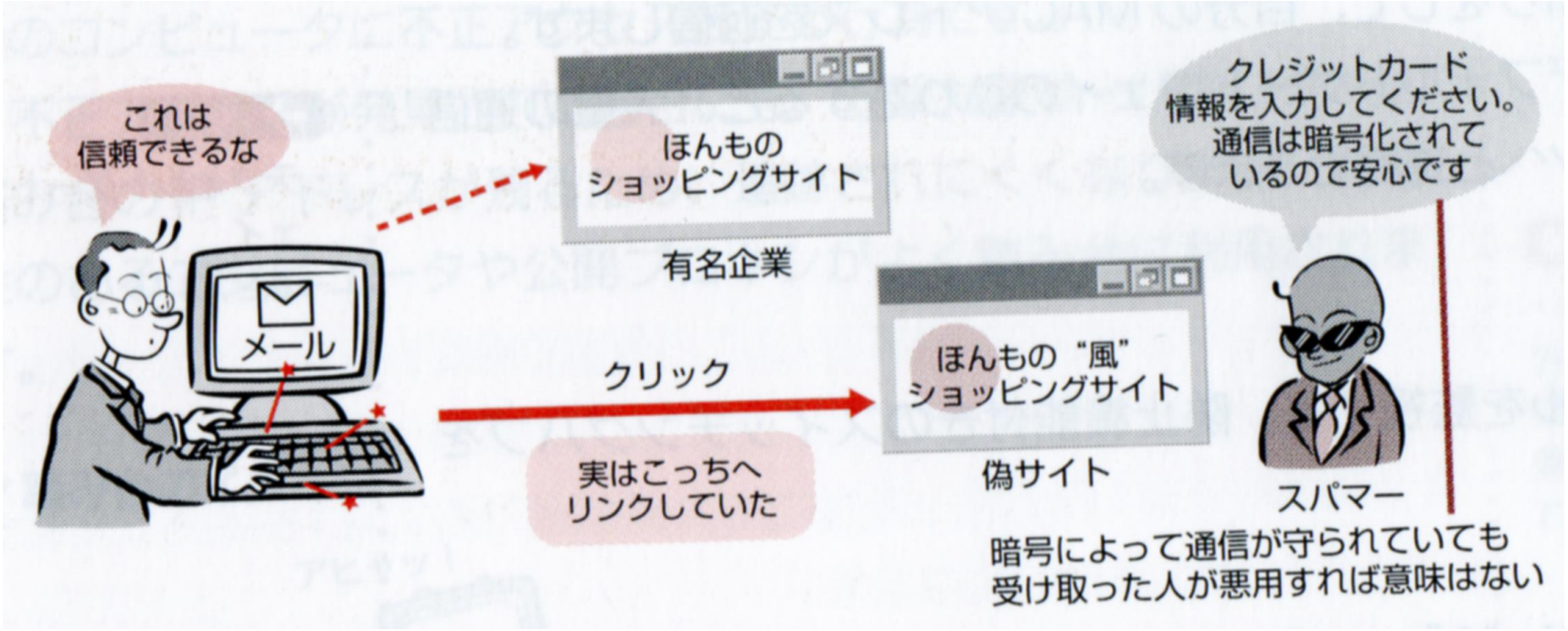
ユーザーがログインするときにネットワークを流れるデータを盗聴してコピーし、コピーしたデータを認証サーバーへ送ることでシステムへ不正にログインしようとする

＜対策＞
「使い捨てパスワードを使う」「ワンタイムパスワードを使う」

リプレイ攻撃

有名サイトや信頼サイトになりすます行為を指す。こうしたサイトになりすますことで、個人情報や重要な情報を取得することができる。

＜対策＞
「メールで送られてきたリンク先へはアクセスしない」「セキュリティ対策ソフトのフィッシング機能を使う」



標的型攻撃

特定のシステムを狙って攻撃する行為。サイバー攻撃の一種。周到な準備で行われ、多くの場合、目的のシステム(企業)へコンピュータウィルスの添付したメールを送り込み、実行が開始される。

＜対策＞
「利用者のリテラシを上げる」「外部への通信を監視する」

サービス妨害(Dos:Denial of Services)

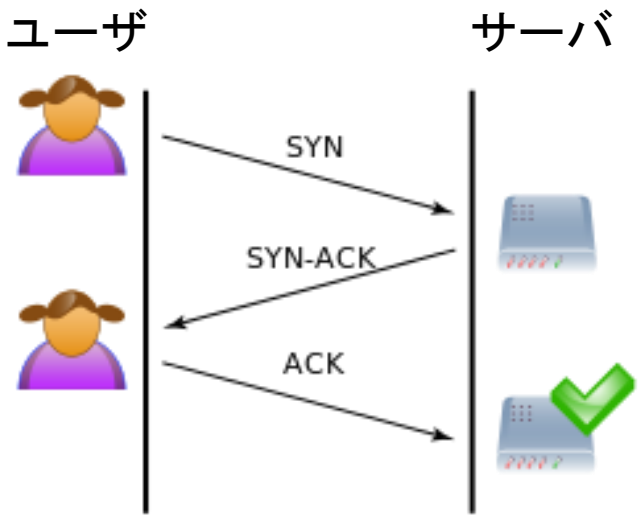
テキストP49-51

サーバに負荷を集中させるなどしてサービスを使用不可能にすること。営業妨害に利用される。

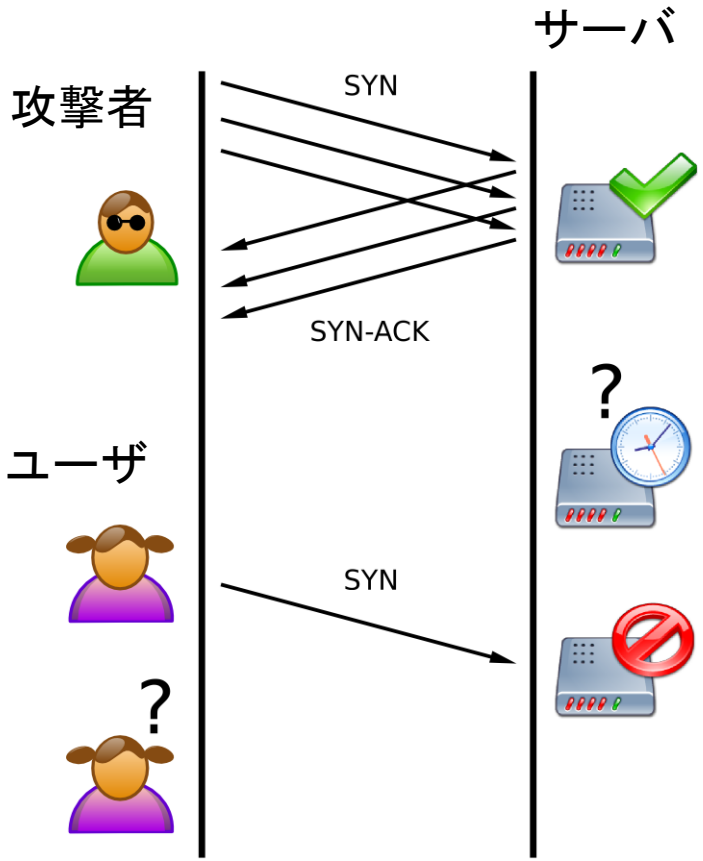
サービス妨害の種類と対策

SYNフラッド攻撃(TCP SYN Flood)

TCP通信の3ウェイハンドシェイクの際にやり取りされる、**最後のACK(クライアントからの応答)を、何らかの方法でサーバへ届かなくする**。このことで、サーバの機能(TCP通信機能)を低下させることができる。



通常のTCP通信の接続では、3つの段階からなる手順を踏んで、ユーザとサーバが接続する



攻撃者は、SYN パケットを大量に送り、サーバの返答を無視する。サーバは返答が来るか、あるいは一定時間が経過するまで記憶領域を保持しつづけなければならず、この間、通常のユーザの接続は受けられない。

＜対策＞
「一定時間を過ぎた不成立コネクションは、強制的に接続終了する」
「不正アクセスしているIPアドレスからの通信を遮断する」

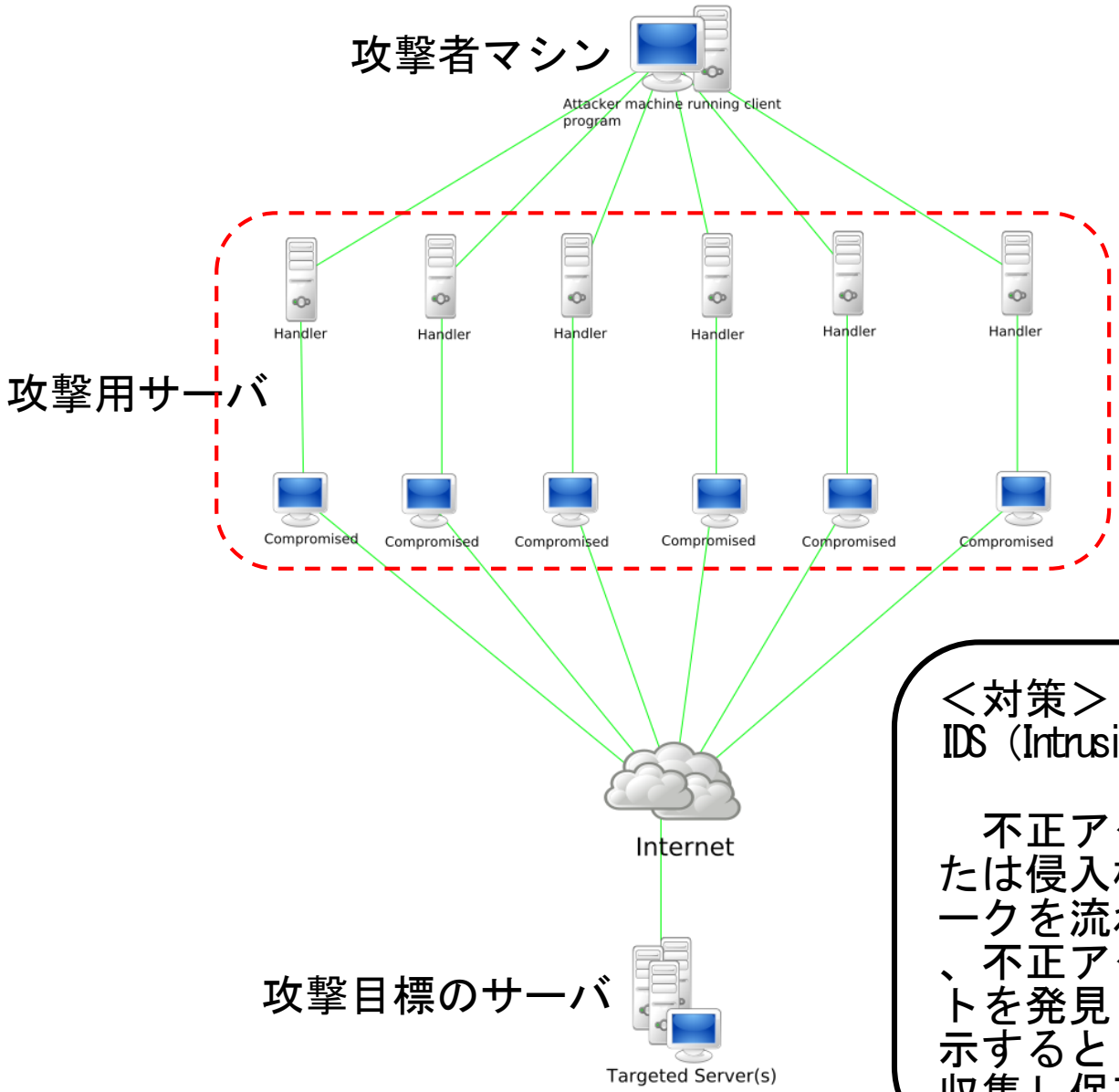
Ping of Death

通常、pingパケットのサイズは64バイトであり、最大サイズ(IPパケットの最大サイズ)でも1,500バイトである。通常のサイズより大きなpingを送ることで対象のコンピュータをクラッシュさせる。

＜対策＞
セキュリティパッチを適用する

DDos攻撃(Distributed Denial of Service attack):分散Dos攻撃

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、特定のネットワークやコンピュータへ接続要求を送出し、通信容量をあふれさせて機能を停止させてしまう

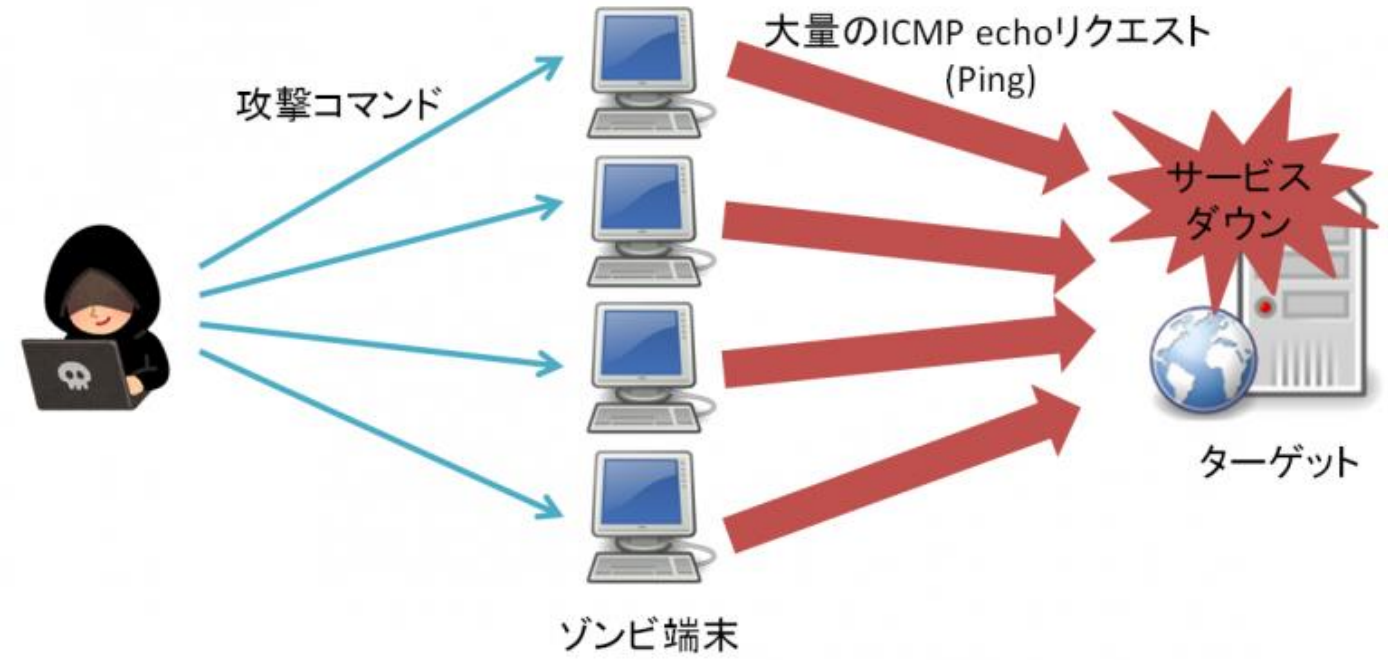


＜対策＞
IDS（Intrusion Detection System）を導入する

　不正アクセス監視システム、または侵入検知システム。ネットワークを流れるパケットを監視して、不正アクセスと思われるパケットを発見したときにアラームを表示するとともに、当該通信記録を収集し保存する仕組み。

ICMP Flood

攻撃対象にICMP(Ping)パケットを大量に送信することで機能不全に陥らせる



＜対策＞

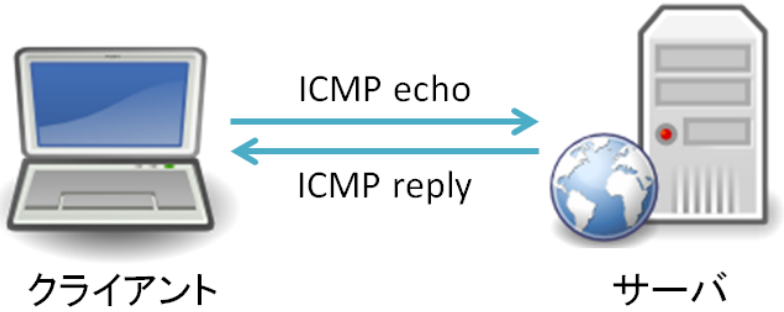
「Pingに応答しないように設定する」「IDSやIPSの導入」

IPS(Intrusion Prevention System):サーバやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知して攻撃を未然に防ぐシステム

smurf

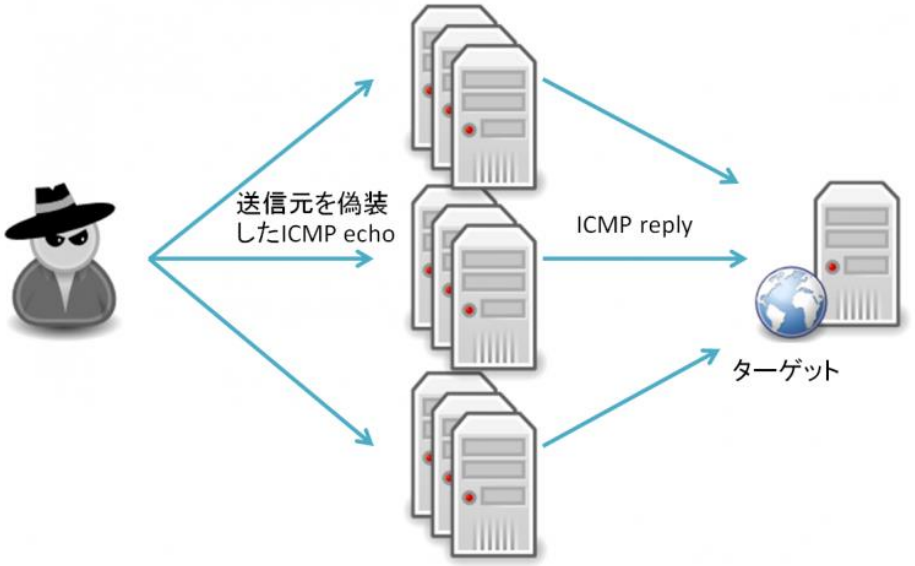
ICMP(ping)パケットの送信元を偽装し、相手のコンピュータに大量の偽のパケットを送りつける

＜対策＞ ブロードキャストアドレスを使ったpingの使用を禁止する



pingはクライアントからサーバに対してネットワークの疎通確認をするときに利用する。左図のようにクライアントがICMPechoを送信して、サーバがそれに応じたreplyを返すのが正常の動作である。

smurf攻撃では、まず送信元のIPアドレスを詐称して、攻撃対象となるサーバのIPを指定する。ICMPechoを受けたサーバはICMPreplyを攻撃ターゲットとなるサーバに送信する。送信されたICMPreplyが少量であれば特に問題ないが、DDoSのように大量な踏み台サーバを利用して偽装したICMPechoを送信すると、大量のICMPreplyを攻撃ターゲットに送信することが可能になり、大量のICMPreplyを受信したターゲットサーバはCPUやメモリ、ネットワーク帯域等のリソースの枯渇によりサービスを提供できなくなる。



その他の攻撃方法 テキストP52-55

ソーシャルエンジニアリング

技術的な方法ではなく、人的な脆弱性を利用して情報を搾取する方法

ショルダーハッキング

ユーザIDやパスワードを入力してるユーザの**肩口から盗み見て**情報を取得する

＜対策＞
「重要な情報を入力する時には、周囲に他人がいないことを確認する」
「モニターにフィルタを貼ったり、囲いをする」「素早くキー操作をする」

スキャビンジング

ごみ箱に捨てられた情報をつなぎ合わせて情報を復元（取得）する。廃棄情報は、意外と「ぞんざい」に扱われることが多い。

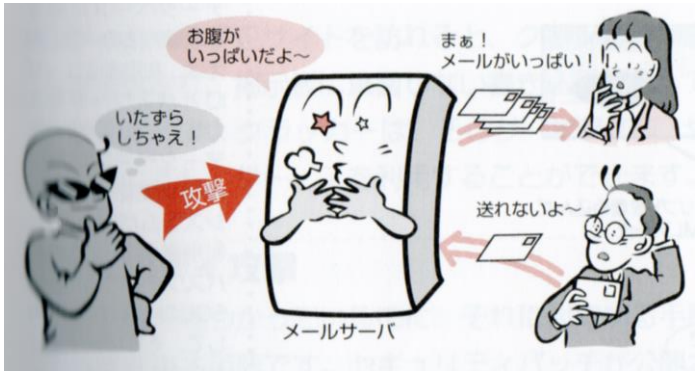
＜対策＞
「シュレッダを使って、確実に裁断する」「廃棄業者に廃棄物を依頼するときには、守秘義務契約などを結ぶ」「磁気データを廃棄する際には、消磁や物理的破損（磁気記録装置を壊す）などして、確実にデータを抹消する」

会話

業務担当者や関係者同士の会話から情報を取得する

＜対策＞
「重要事項の会合や話し合いは、開催場所に注意する」「パスワードの問い合わせなどに関する取扱い規定や手順、本人確認方法を整備する」

スパムメール



受信者の意向を無視して、無差別かつ大量に一括してばらまかれる、各種ネットメディアのメッセージのことで、無断で送りつける広告メールや無意味な大量メール（ねずみ講、チェーンメール）を指す

スパムメールの送信者は、第三者中継を許可しているメールサーバを利用している場合が多く、この場合には、正規のメールサービスに支障をきたす恐れがある。

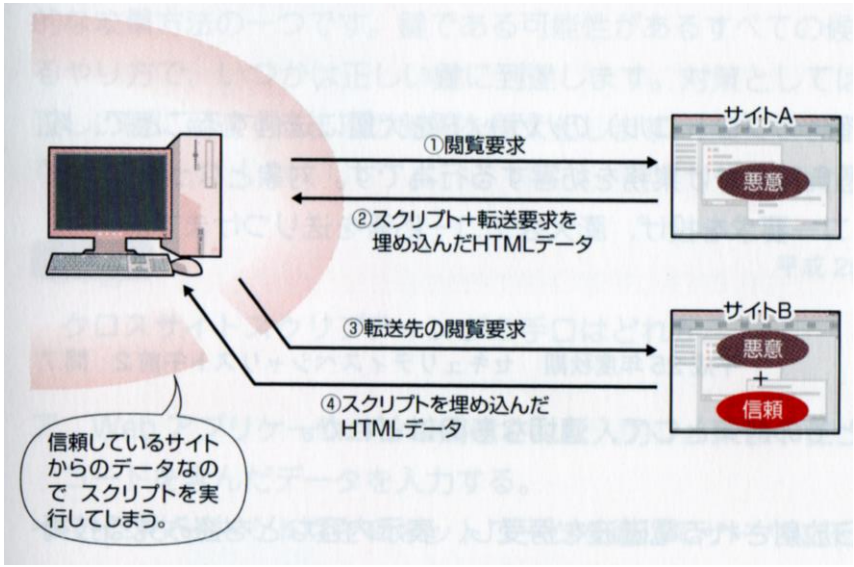
未承諾の報告メールの送信禁止

＜対策＞
「メールサーバのセキュリティ強化」「オプトインを実体化するための法的・技術的な環境を整える」

クロスサイトスクリプティング

保安上の弱点(脆弱性)のあるWebサイトを踏み台に、悪意のあるプログラムを、このサイトの訪問者に送り込む

Webページ上の動的なコンテンツは、スクリプト言語(JavaScriptなど)を使って記述している。スクリプト言語は、悪意のあるコードを埋め込み易く、埋め込んだコードは、ユーザのコンピュータに被害を与えることがある。



クロスサイトリクエストフォージェリ

Webサイトにスクリプトや自動転送(HTTPリダイレクト)を仕込むことによって、閲覧者に意図せず別のWebサイト上で何らかの操作(掲示板への書き込みなど)を行わせる

ゼロディ攻撃

ソフトウェアにセキュリティ上の脆弱性(セキュリティホール)が発見されたときに、問題の存在自体が広く公表される前に、この脆弱性を悪用する