セキュリティ

http://cobayasi.com/koza/kihon/5_security.pdf

1. 情報セキュリティ 
2. コンピュータウィルス 
3. 暗号化と認証 
4. ネットワークセキュリティ 

1. 情報セキュリティ

- 情報セキュリティとは
- 情報資産における脅威
- リスクアセスメント
- 情報セキュリティマネジメントシステム
- 情報漏えいを防ぐ方法

● 情報セキュリティとは

情報資産（大事なデータ）の漏洩を防ぐための**機密性**、改変を防ぐための**完全性**、システムの停止を防止するための**可用性**を確保し、それを維持して行くこと
（1992年経済協力開発機構「情報システムのセキュリティに関するガイドライン」より）

● **機密性**　情報資産が**第三者に漏れない**ようにすること
（Confidentiality）

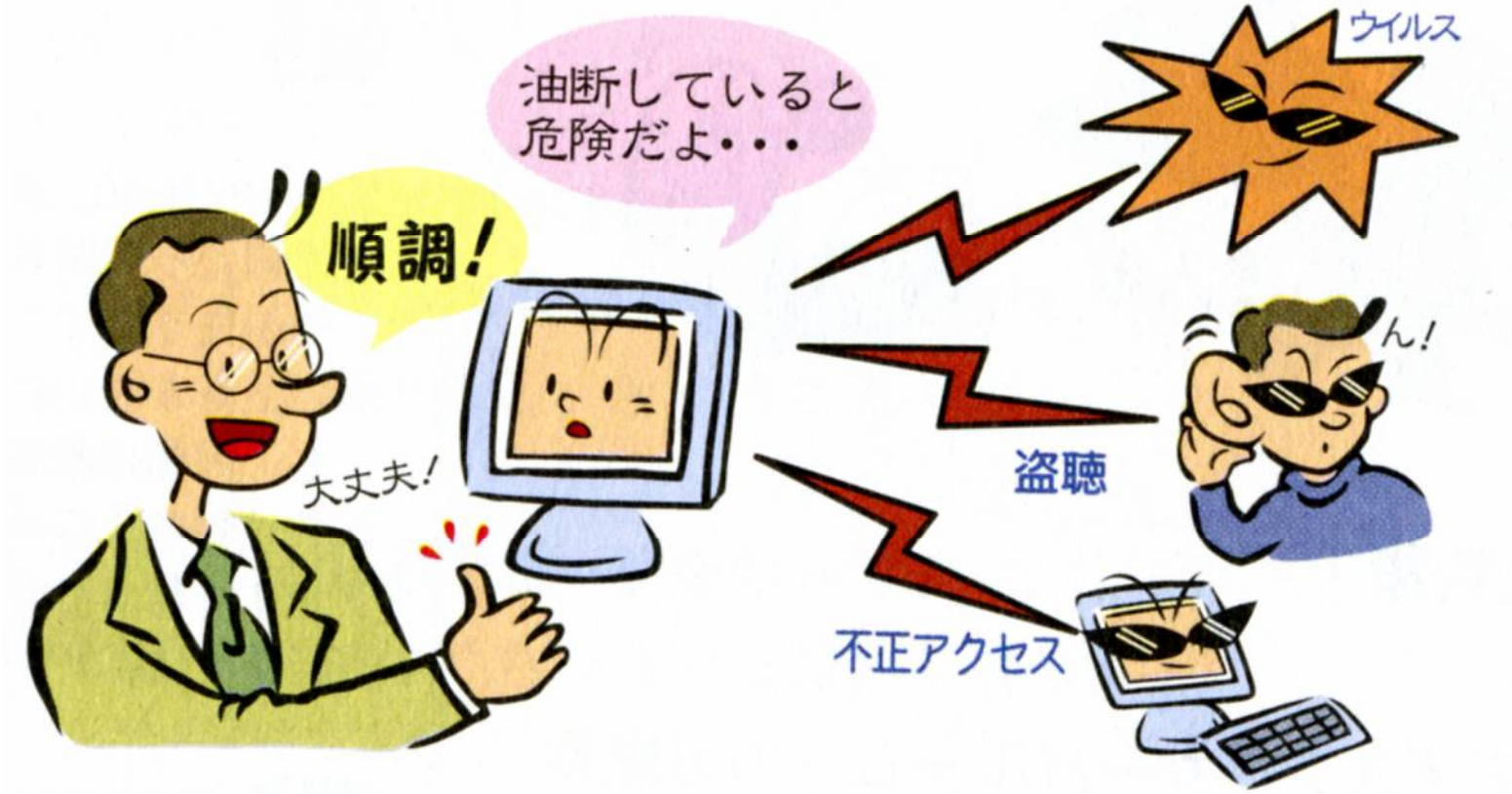
● **完全性**　情報資産が**正確で完全に維持される**こと
（Integrity）

● **可用性**　情報資産が**定められた方法で、いつでも利用できる**ようにすること
（Availability）

● 情報資産における脅威

- 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



- **技術的脅威の手口や攻撃方法**

✓ **フィッシング**

偽りのWebサイトにアクセスさせて、ユーザの暗証番号やパスワードなどの個人情報をだまし取る

✓ **DNSキャッシュポイズニング**

DNSサーバに誤ったドメイン情報を覚えさせ、偽りのサーバに誘導して、誘導したコンピュータを攻撃する

✓ **SEOポインズニング**

検索サイトの検索結果の上位に悪意のあるサイトが入るように工夫する

✓ **SQLインジェクション**

Webアプリケーション上に、悪意のある問い合わせや操作する命令文を入力して、データベースのデータを改ざんしたり、不正にデータを取得する

✓ **Dos攻撃**

サーバに大量のデータを送信して、サーバの様々な機能を停止させる

✓ **ディレクトリ・トラバーサル攻撃**

管理者が公開していないパス（ディレクトリやファイルの保存場所）で、Webサーバ内のファイルを不正に閲覧する

✓ **Webビーコン**

Webページなどに極小サイズの画像を埋め込んで、ユーザのアクセス状況などの情報を収集する

✓ **スパイウェア**

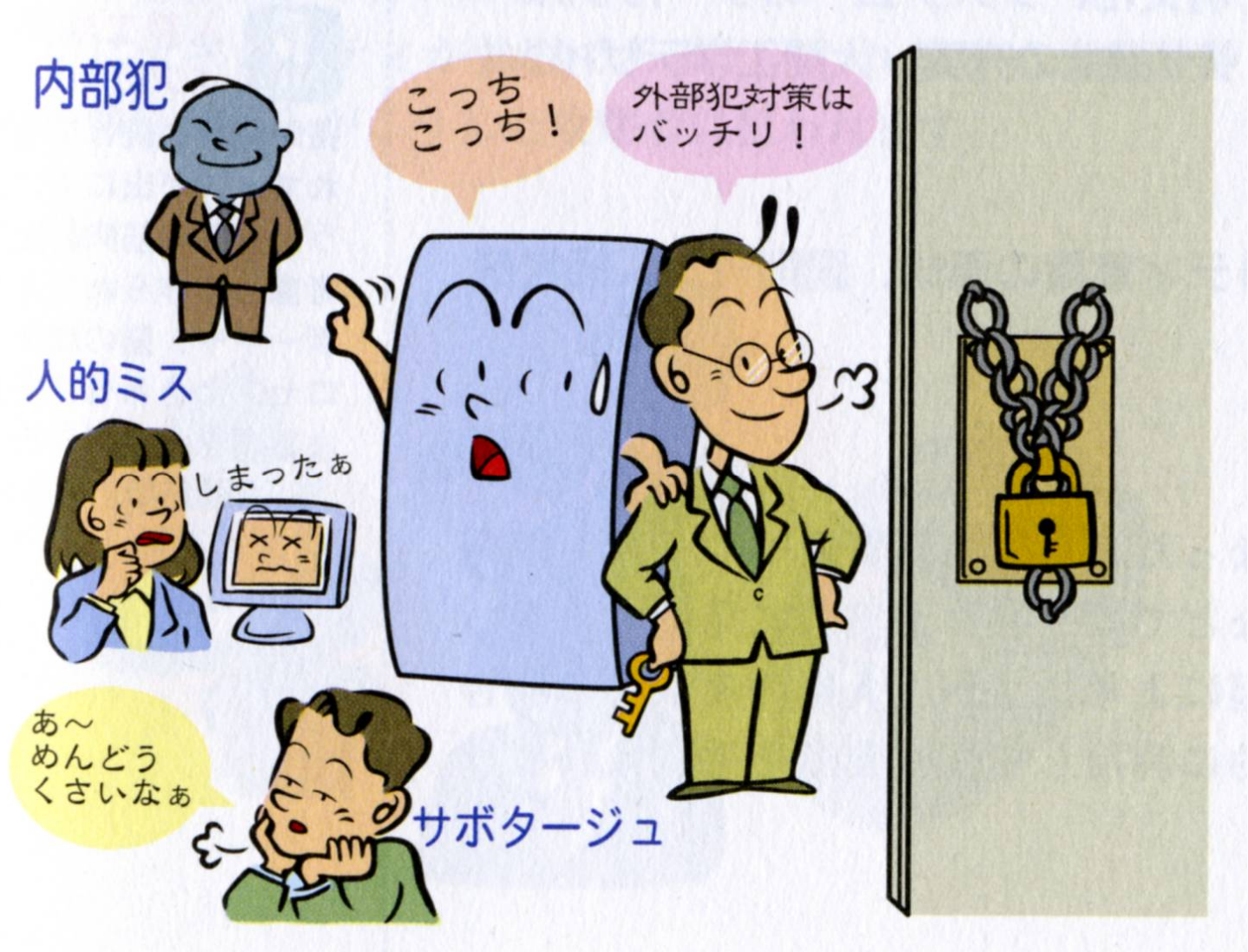
利用者が知らいないうちにPCにインストールし、利用者の個人情報やアクセル履歴などの情報を収集するプログラム

✓ **ブルートフォース（bruteforce）攻撃**

暗号解読の手法を使って、暗号文に対して総当たりで、鍵を割り出す攻撃

- **人的脅威**

人的ミスによるデータや機器の破壊や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**



- **人的脅威の手口や攻撃方法**

  ✓ **ソーシャル・エンジニアリング**

  他人を装ってパスワードを聞き出したり、緊急事態を装って組織内部の機密情報を聞き出したりする。

  人間の心理の隙間をついて、様々な情報を盗む行為

  ✓ **なりすまし**

  盗んだIDやパスワードなどを使って、ネットワーク上で他人に成りすます

  ✓ **サラミ法**

  不正行為がわからない程度に、多くの情報資産から少しずつだまし取る

- **物理的脅威**

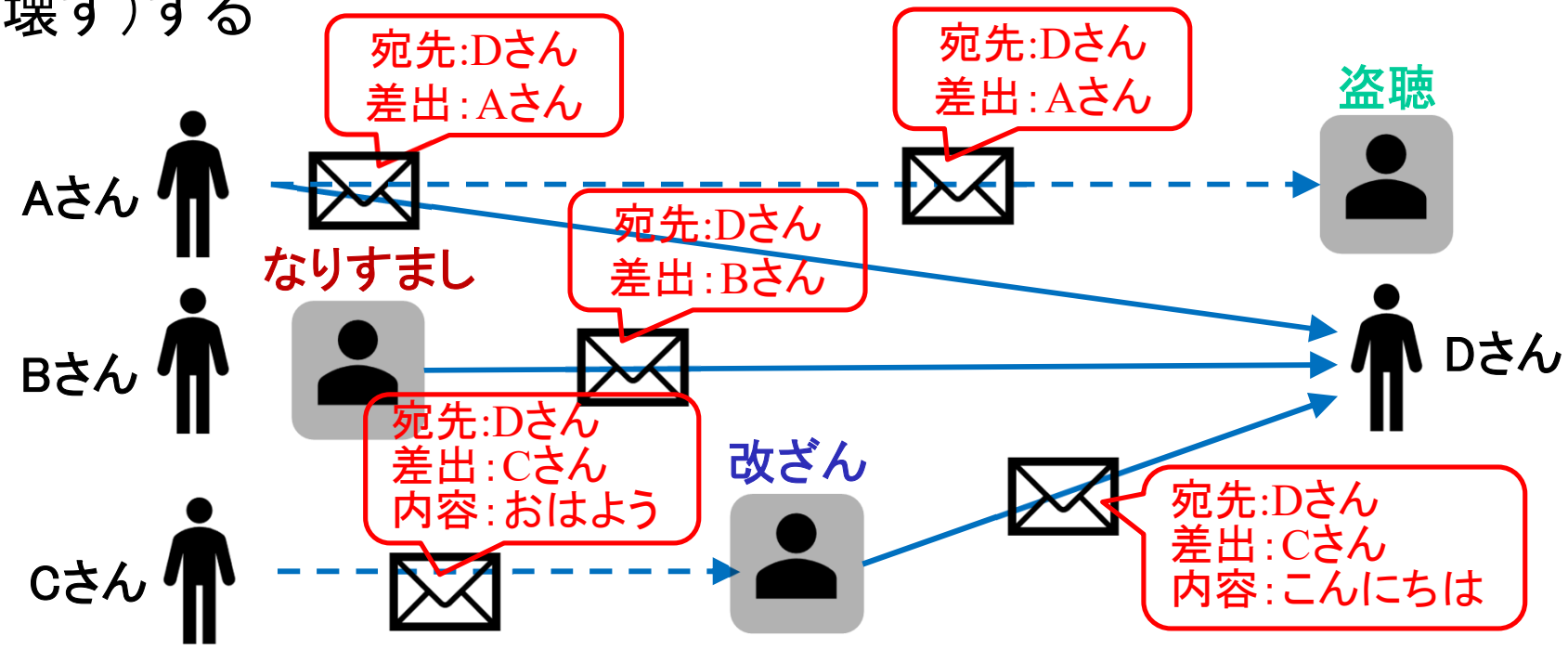
火災や地震、侵入者によって機器の破壊など、**直接的に情報資産が破壊される**

＜盗聴，なりすまし，改ざんとは＞

✓ 盗聴
　データの送信中に第三者によって、不正に通信内容を盗む

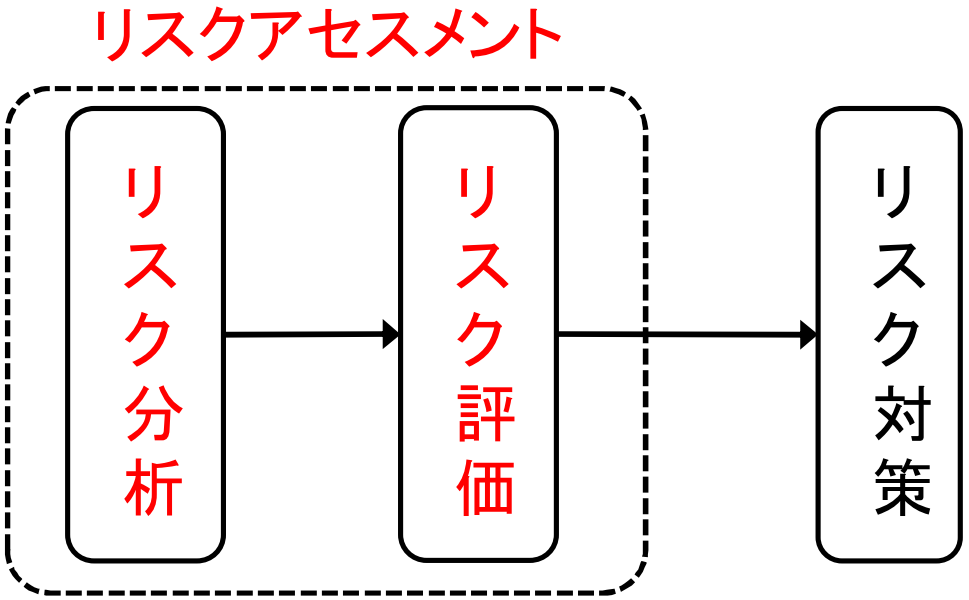
✓ なりすまし
　第三者が本来の利用者を偽って、詐欺行為を行う

✓ 改ざん
　不正な手段により、データの改変（内容を変える）や破壊（内容を壊す）する



● リスクアセスメント

情報資産に対するリスク（脅威が発生する可能性）を洗い出（リスク分析）し、リスクによって発生する可能性のある損害を明らか（リスク評価）にして、リスクに対応した対策（リスク対策）を立てるときの一連の過程を、リスクアクセスメントと呼ぶ



リスク対策

リスクが発生したときの損失額とリスクの発生率を定量的に評価するための対策

■ リスク回避

リスクの原因を排除する。この対策は、損害額が大きく、発生率が高いリスクで行う。

■ リスク移転（または共有）

リスクを他の人に肩代わりしてもらう。この対策は、損害額が大きく、発生率が低いリスクで行う。

■ リスク軽減

リスクによる損失を、許容範囲内に収める（軽減する）。この対策は、損害額が小さく、発生率が高いリスクで行う。

■ リスク保有

リスクに対する対策は講じない（そのままにする）。この対策は、損害額が小さく、発生率も低いリスクで行う。

● 情報セキュリティ・マネジメントシステム

ISMS(Information Security Management System)

情報セキュリティ・マネジメントシステムは、情報セキュリティを維持するために、情報資産を適切に管理し、機密を保護し、継続的に改善するために必要な仕組み

■ ISMSの確立手順

①リスク分析 ②評価

情報資産のリスクを洗い出し⇒リスク分析、リスクの発生する可能性のある損害を明らかにし⇒リスク評価、分析によって得られた損失額と発生確率から、リスク発生時の損害の大きさを検討する

③リスク対策のための管理目的及び管理策の選択

リスク評価の結果に優先度を付け⇒管理目的、その対策(リスク回避、リスク移転、リスク軽減、リスク保育)を立てる⇒管理策

④適用宣言書の作成

情報資産の管理目的やリスク対策について、書面で明確に宣言する

【過去問題】

リスク共有(または移転)に該当するものはどれか

ア　損失の発生率を低下させる
イ　保険への加入などで、他との間でリスクを分散する
ウ　リスクの原因を除去する
エ　リスクを扱いやすい単位に分解して集約する

リスク共有は、リスクを他の者と共有し分散すること

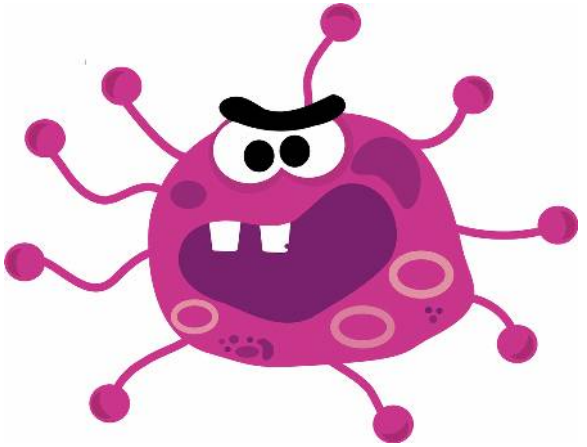
【過去問題】
　リスクアセスメントに関する記述のうち、適切なものはどれか。

ア　以前に洗い出された全てのリスクへの対応が完了する前にリスクアセスメントを実施することは避ける。
イ　将来の損失を防ぐことがリスクアセスメントの目的なので、過去のリスクアセスメントで利用されたデータを参照することは避ける。
ウ　損失額と発生確率の予測に基づくリスクの大きさに従うなどの方法で、対応の優先順位を付ける。
エ　リスクアセスメントはリスクが顕在化してから実施し、損失額に応じて対応の予算を決定する。

リスクアセスメント(Risk Assessment)は、リスクマネジメントにおける「リスクの特定」から「リスクの評価」までの一連の活動である

2. コンピュータウィルス

- コンピュータウィルスとは
- コンピュータウィルスの種類
- コンピュータウィルスの対策



● コンピュータウィルスとは

第3者のデータなどに対して、意図的に被害を及ぼすプログラム

経済産業省「コンピュータウィルス対策基準」で定義

■ コンピュータウィルスの機能

① 自己伝染機能

自分自身を、他のコンピュータにコピーして伝染させる

② 潜伏機能

特定の日時や処理回数に達するまで、症状を出さない

③ 発病機能

ファイルやデータ、プログラムを破壊したり、予期しない動作をする

これも
知っとこ

マルウェア

コンピュータウィルスを含む、悪意のあるソフトウェアの総称

種類	特徴
スパイウェア	コンピュータ利用者の個人情報を収集して、外部へ送信する
ポット	感染した第3者のコンピュータを、指示通りに動かす

● コンピュータウィルスの種類

種類	特徴
マクロ型	マクロ機能を悪用して、アプリケーションソフトに寄生し、ファイルを開くだけで、感染する。
トロイの木馬型	普通のファイルのように見せかけて、その裏で、データの破壊などの不正な処理をする。自己増殖しない。
ワーム型	自分自身をコピーしながら、ネットワークを介して他のコンピュータへ感染する

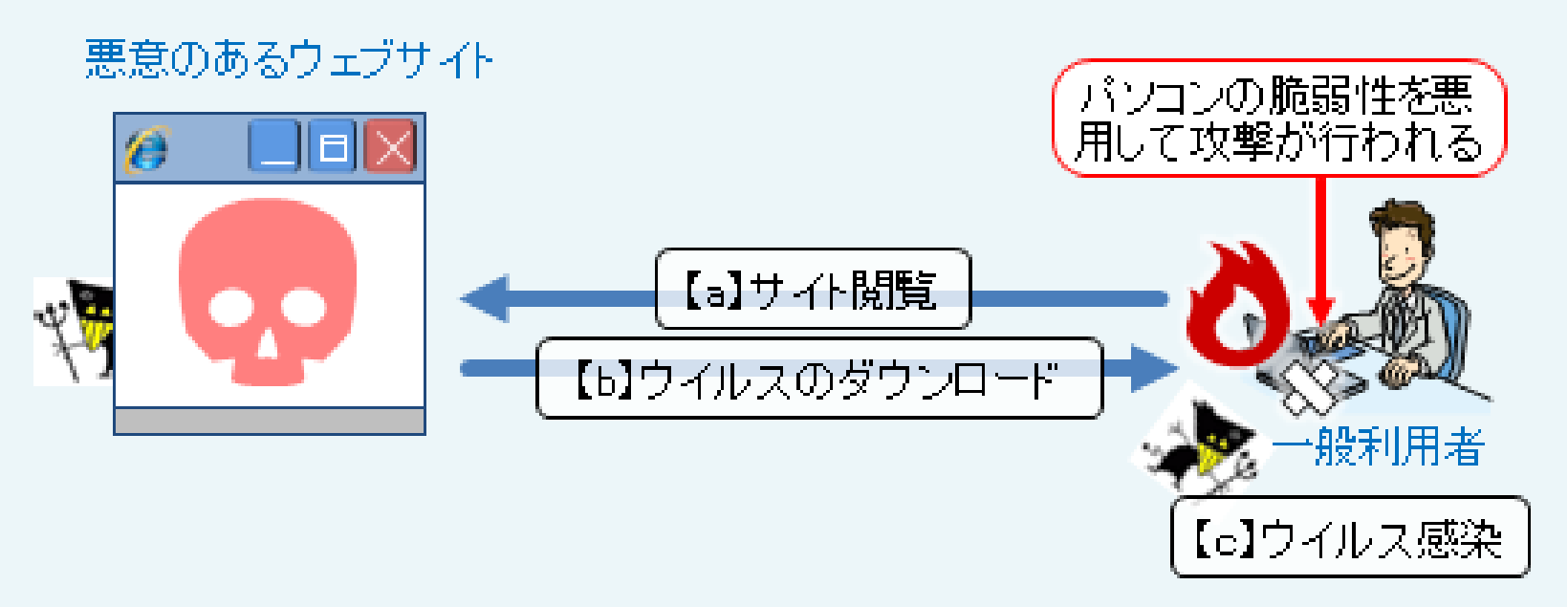
ココが出る！

ココが出る！

これも
知っとこ

ドライブバイダウンロード攻撃

ウェブサイトを閲覧したときに、パソコン利用者の意図に関わらず、ウイルスなどの不正プログラムをパソコンにダウンロードさせる攻撃。この攻撃は、主に利用者のパソコンのOS やアプリケーションなどの脆弱性を悪用する。



● コンピュータウィルスの対策

コンピュータウィルスの「予防」「検知」「感染後」の対策は、通商産業省の「コンピュータウィルス対策基準」にまとめられている

- ウィルスの予防
  - ✓ 電子メールについては、知らない人からの添付ファイルは開かない
  - ✓ Webサイトについては、あらしいWebサイトは表示ない設定にする
  - ✓ OSやアプリケーションの修正パッチは、必ず適用する
- ウィルスの検知
  - ✓ コンピュータには、必ずウィルス対策ソフトを入れる
  - ✓ ウィルス対策ソフトのウィルス定義ファイルは、常に最新のものを使う
- ウィルス感染後の対応
  - ✓ コンピュータを直ちにネットワークから切り離す

【過去問題】
　データの破壊や改ざんなどの不正な機能をプログラムの一部に組み込んだものを送ってインストールし、実行するものはどれか

ア　DoS攻撃
イ　辞書攻撃
ウ　トロイの木馬
エ　バッファオーバフロー攻撃

キーワード:「データの破壊や改ざんなどの不正行為」
「プログラムの一部に組み込んだ」

【過去問題】
スパイウェアに該当するものはどれか。

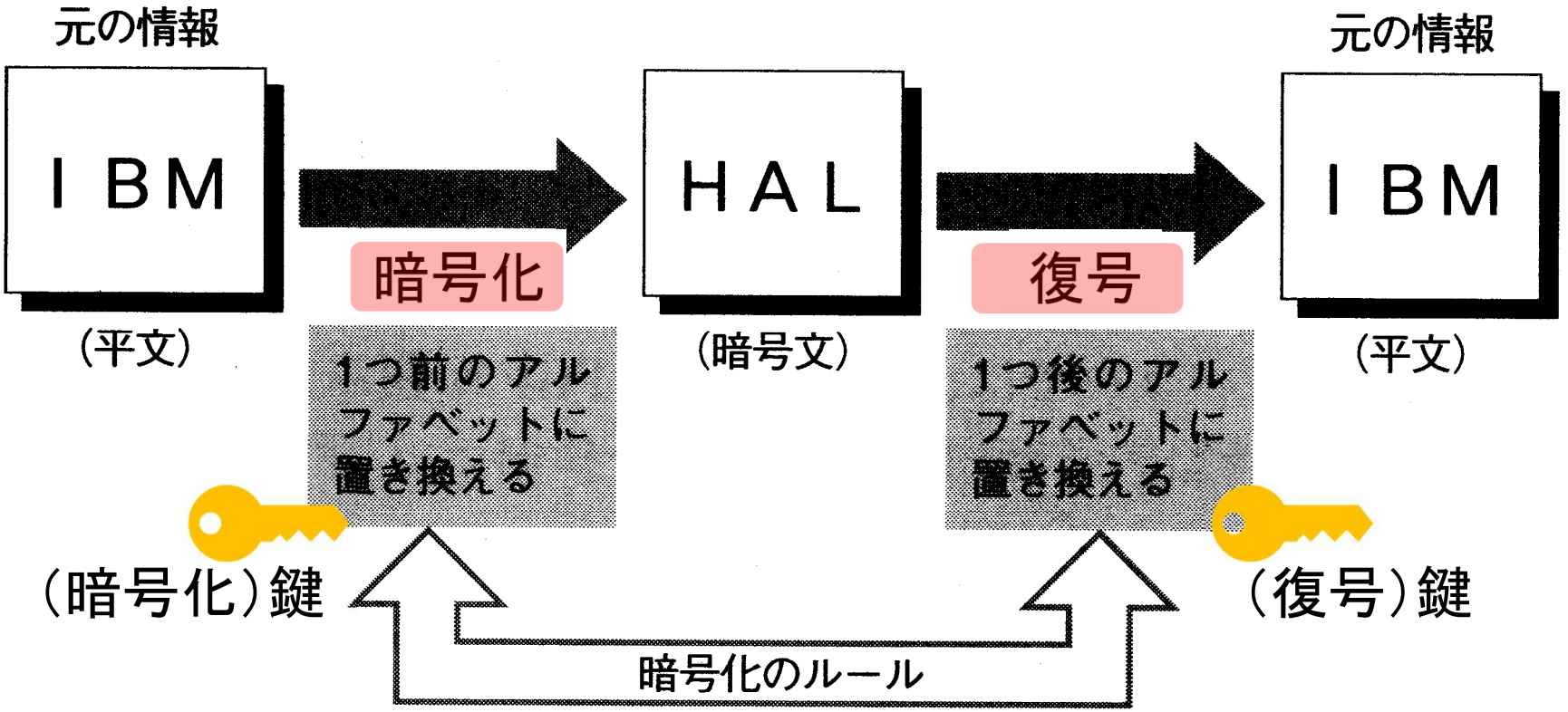
ア　Webサイトへの不正な入力を排除するために、Webサイトの入力フォームの入力データから、HTMLタグ，JavaScript，SQL文などを検出し、それらを他の文字列に置き換えるプログラム
イ　サーバへの侵入口となり得る脆弱なポートを探すために、攻撃者のPCからサーバのTCPポートに順番にアクセスするプログラム
ウ　利用者の意図に反してPCにインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム
エ　利用者のパスワードを調べるために、サーバにアクセスし、辞書に載っている単語を総当たりで試すプログラム

スパイウェア(Spyware)は、利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴及びキーストロークなどの情報を秘密裏に収集し、勝手に外部の組織や個人に送信する不正プログラム。
システムの改ざんやファイルの破壊などの目立つ活動は行わないことが多く、インストールされていることをユーザから隠す。

3. 暗号化と認証

- データの暗号化
- ディジタル署名
- 認証局
- SSL

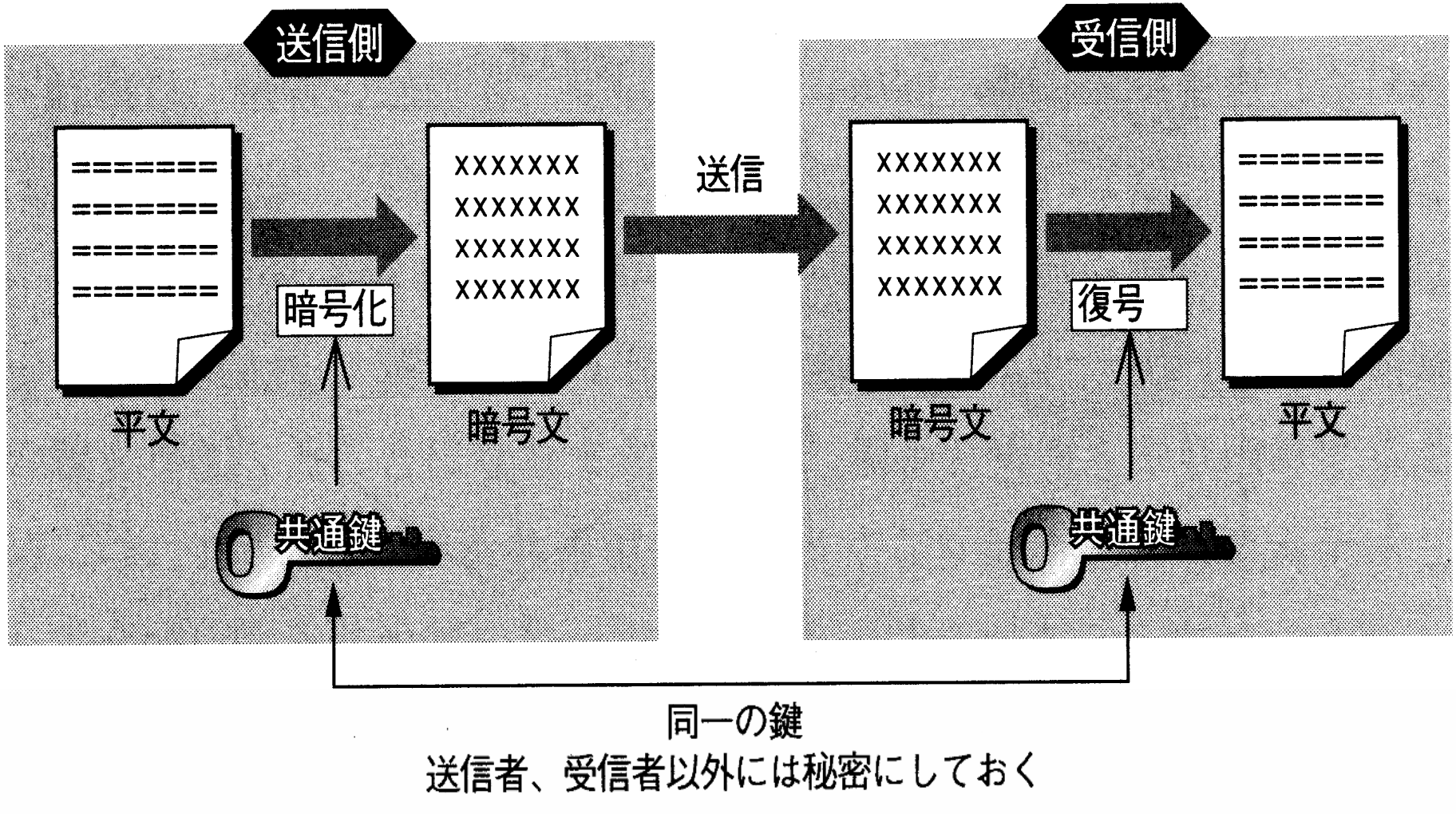
● データの暗号化（暗号化とは）



Ｉ Ｂ Ｍ
↓ ↓ ↓ 1つ前のアルファベットに置き換える
Ｈ Ａ Ｌ
↓ ↓ ↓ 1つ後のアルファベットに置き換える
Ｉ Ｂ Ｍ

● 暗号化方式

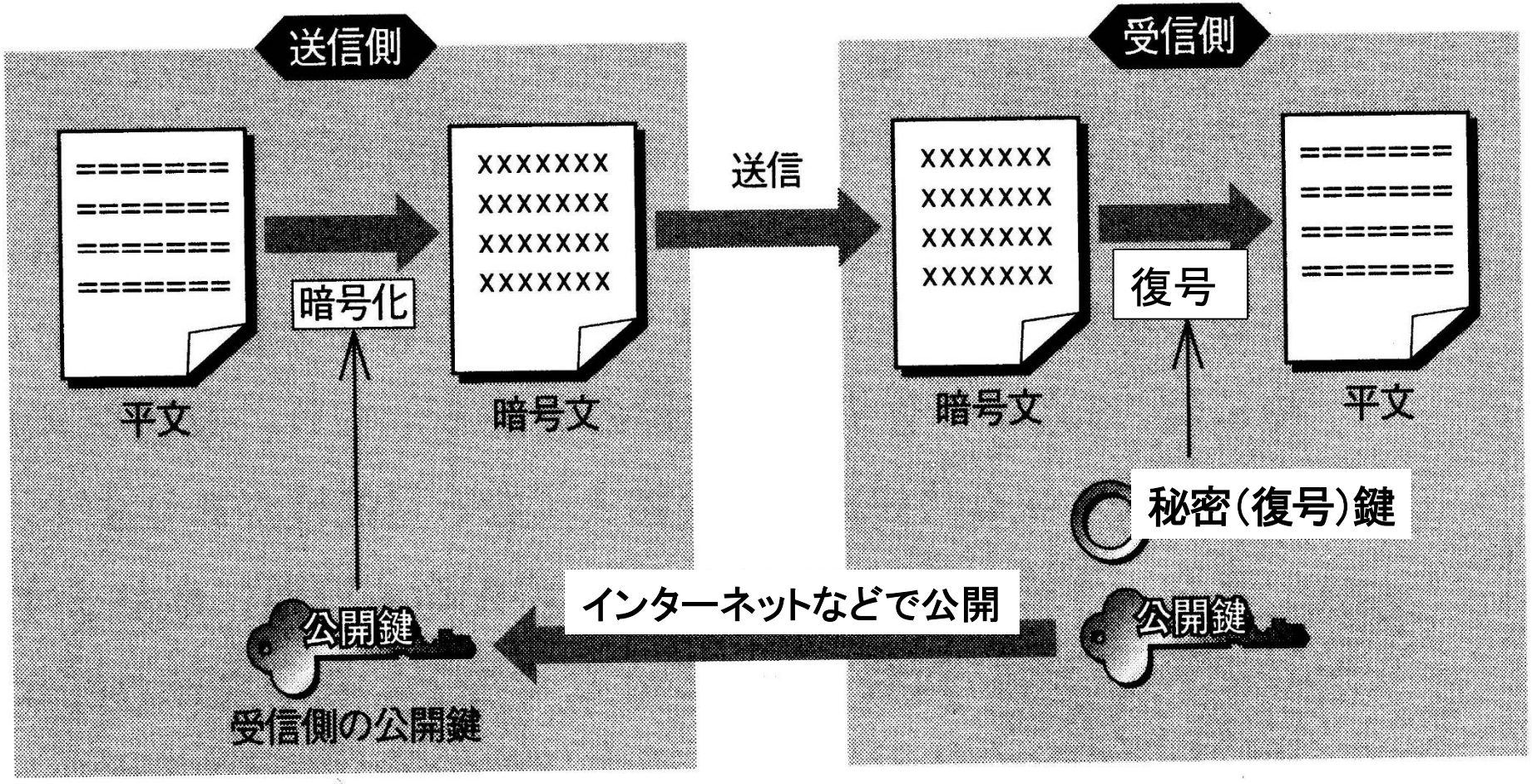
• 共通鍵暗号化方式



＜共通鍵暗号化方式の特徴＞

- 送信者と受信者が共通のルール（共通鍵）で本文を暗号化する
- 共通鍵の交換に問題あり
- 処理速度は速い
- 多人数に送る場合には不向き
- 鍵数= n(n－1)/2 ※nは利用人数
- DES(Data Encryption Standard),AES(Advanced Encryption Standard)など

• 公開鍵暗号化方式


送信側
受信側
平文
暗号化
暗号文
送信
暗号文
復号
平文
秘密(復号)鍵
公開鍵
インターネットなどで公開
公開鍵
受信側の公開鍵

＜公開鍵暗号化を使った通信手順＞

① 受信側が生成した公開鍵と秘密（復号）鍵のうち、公開鍵を認証局（CA）に登録して公開する
② 送信側は、CAから受信側の公開鍵を取得し、この鍵で送る平文を暗号化する
③ 暗号文を受取った受信側は、自分の秘密鍵で復号する

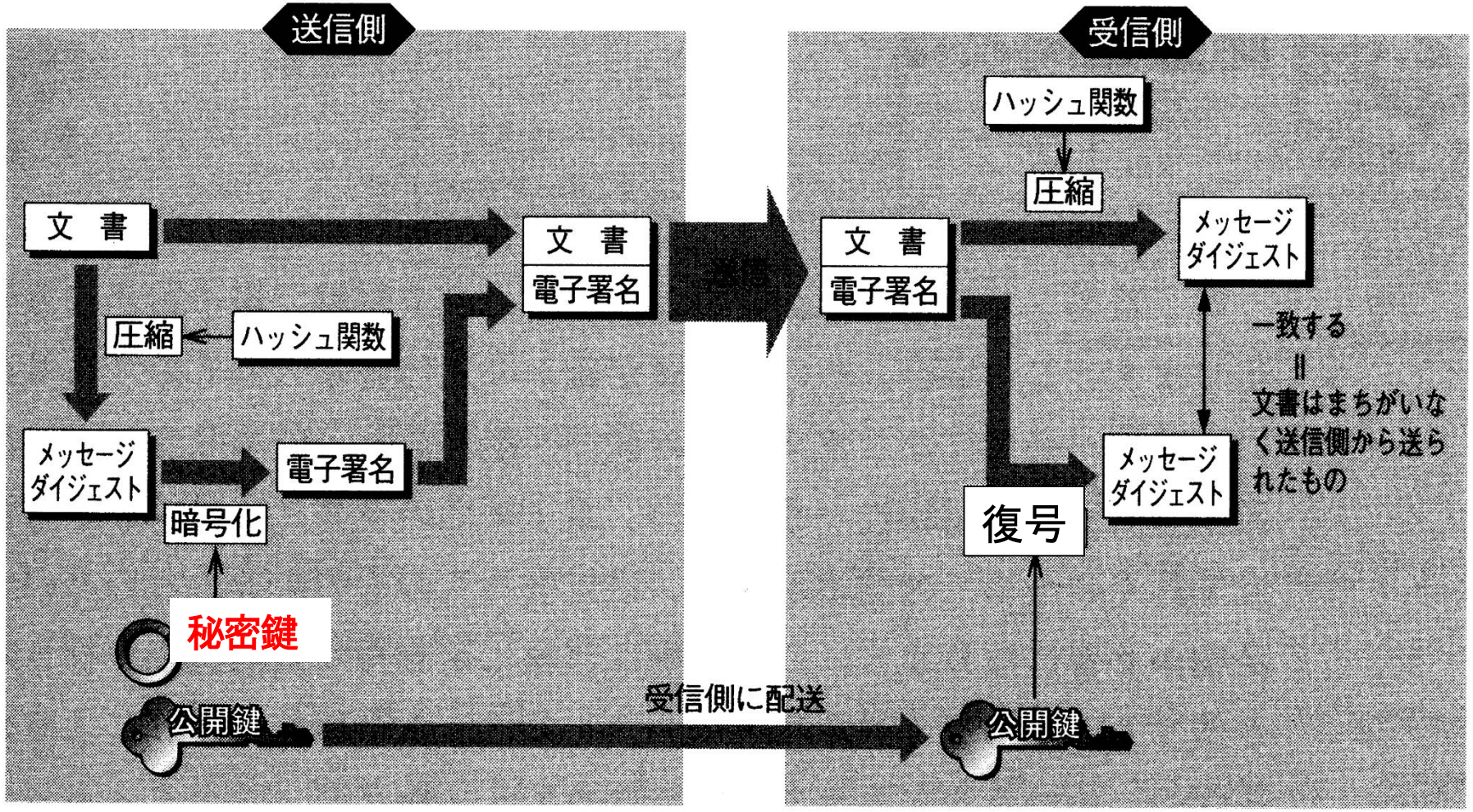
＜公開鍵暗号化方式の特徴＞

- 平文を公開鍵で暗号化し、秘密鍵で復号する
- 公開鍵は、認証局に登録し公開する
- 多数の人に送る場合に適している
- 処理が遅い
- 鍵数=2n　※nは利用人数
- RSA（素因数分解の困難さを使った）など

● ディジタル(電子)署名

認証技術

～送ったデータが本物であるか？証明する～

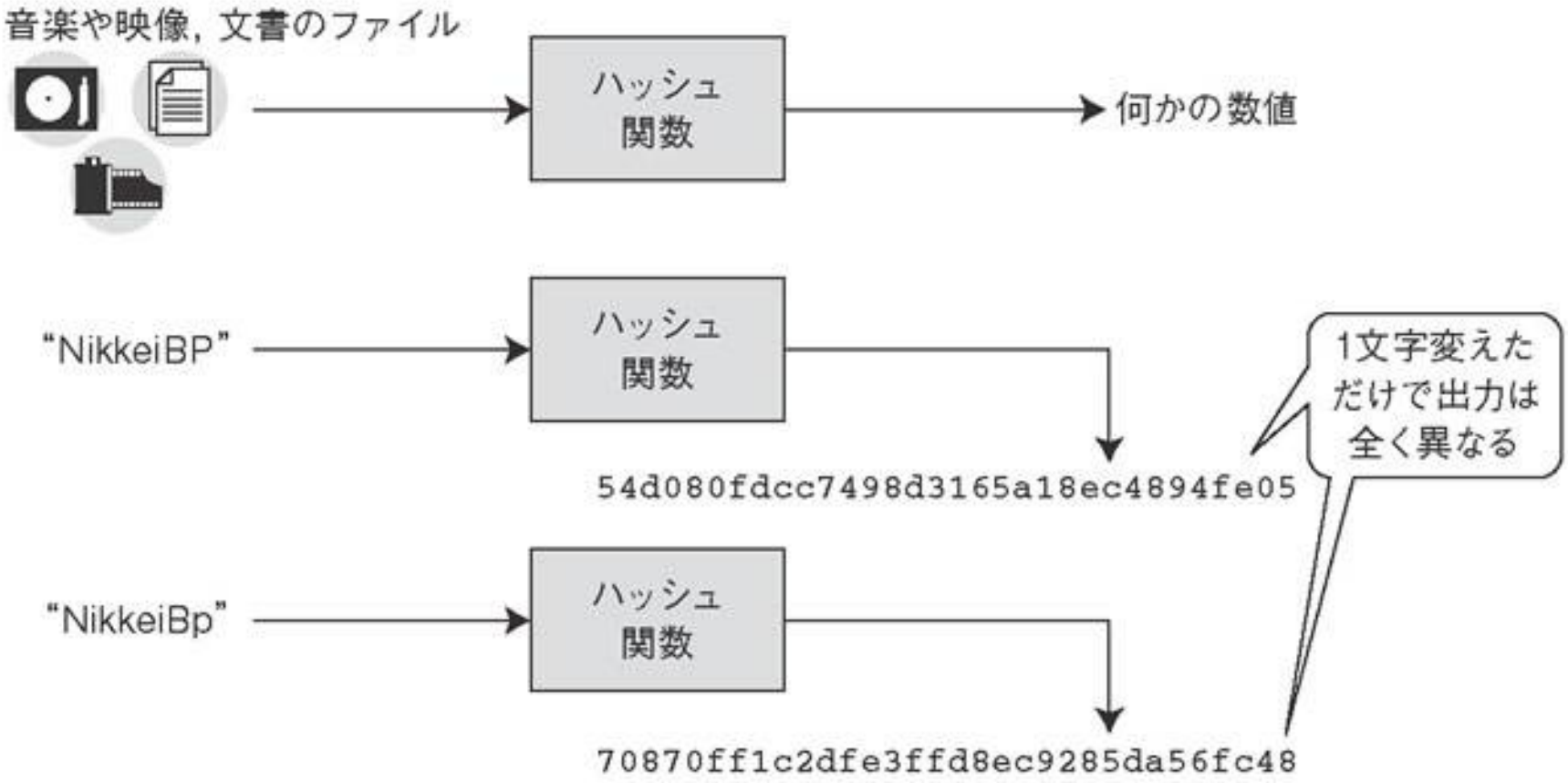


＜ディジタル署名の通信手順＞

① 送信側は、秘密鍵と公開鍵を生成し、公開鍵のみを認証局に登録する
② 送信データからハッシュ関数でダイジェストを作成する
③ ダイジェストを送信側の秘密鍵で暗号化し、これを送信データに添付して送る
④ 受信側は、認証局から送信側の公開鍵を取得し、この鍵で受信したダイジェストを復号する
⑤ 送信側と同じハッシュ関数で、受取った送信データからダイジェストを作成し、④で復号したダイジェストと比較する
⑥ ダイジェストの比較結果が、OKならばデータには間違いない

＜ハッシュ関数とは＞

　与えられたデータから、規則性のない固定長のデータを生成する関数



●認証局(CA:Certification Authority)

- 公開鍵が、本人(データの送信者)のものかを証明する第3者機関
- 電子商取引推進協議会(ECOM)が発表した「認証局運用ガイドライン」に、従って運営されている認証業務機関

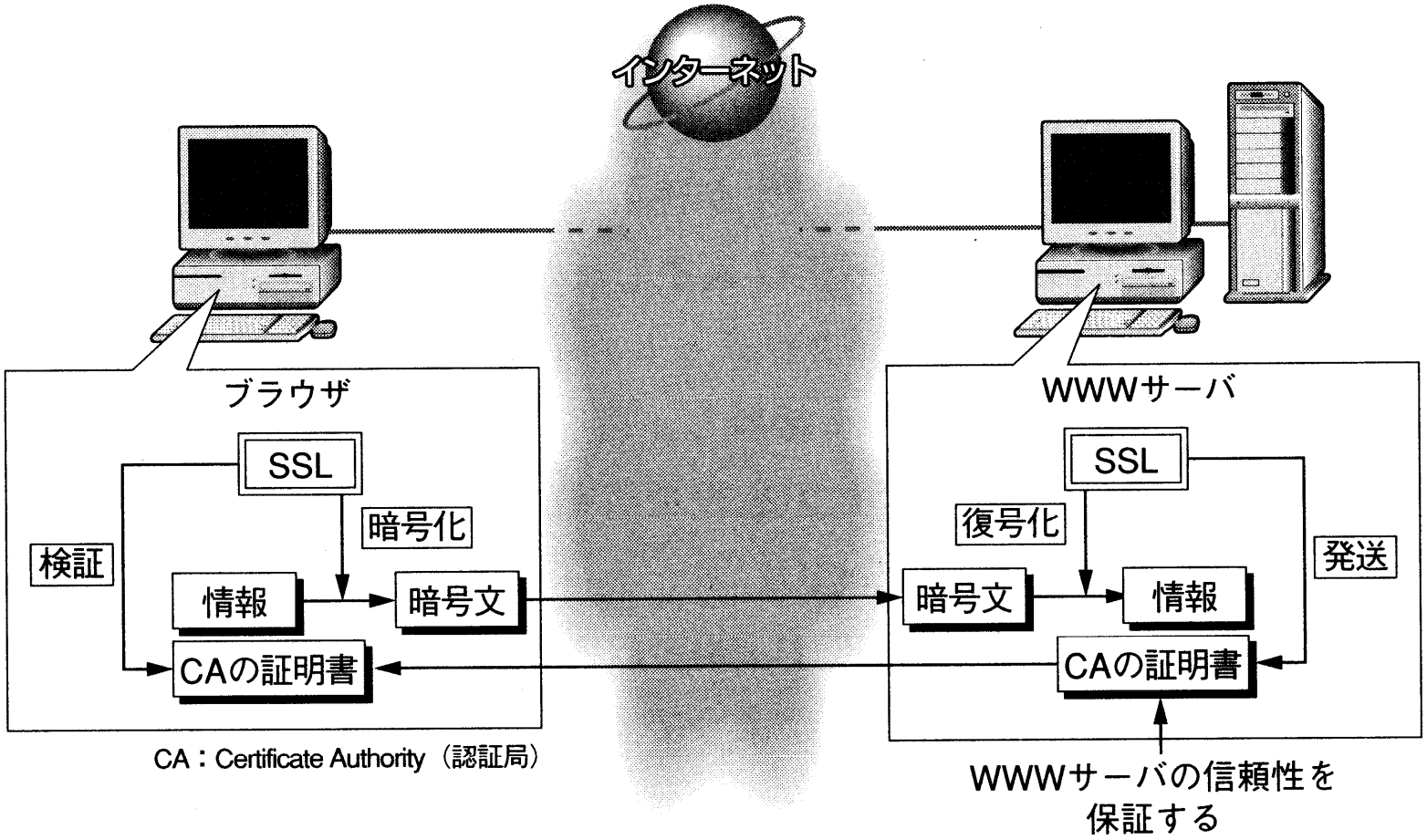
主な認証局

- 電子認証登記所(商業登記認証局)・各都道府県の法務局
- 日本電子認証株式会社
- 株式会社NTTネオメイト
- 株式会社帝国データバンク　など

- 本人からの申請で、公開鍵の正当性を証明するディジタル証明書を発行

● SSL（Secure Sockets Layer）

SSLにより
・WWWサーバはCAの証明書をブラウザに送り、ブラウザはそれを検証してWWWサーバの信頼性を確認する
・ブラウザからWWWサーバへは情報を暗号化して送る（WWWサーバからブラウザへも同様）



【過去問題】
公開鍵暗号方式を採用した電子商取引において、
認証局(CA)の役割はどれか。

ア　取引当事者間で共有する秘密鍵を管理する。
イ　取引当事者の公開鍵に対するディジタル証明書を発行する。
ウ　取引当事者のディジタル署名を管理する。
エ　取引当事者のパスワードを管理する。

認証局(Certificaion Authority:CA)は、公開鍵暗号方式を用いたデータ通信において、利用者(主にサーバ)の公開鍵の正当性を保証するためのディジタル証明書を発行する第三者機関である。

4. ネットワークセキュリティ

- ネットワークセキュリティ技術
- ユーザ認証
- ファイアウォール
- パケットフィルタリング
- プロキシ
- ベネトレーションテスト
- 侵入検知システム

● ネットワークセキュリティ技術

コンピュータをネットワークに接続したとき、他のコンピュータから不正アクセスされるのを防止するための様々な技術。

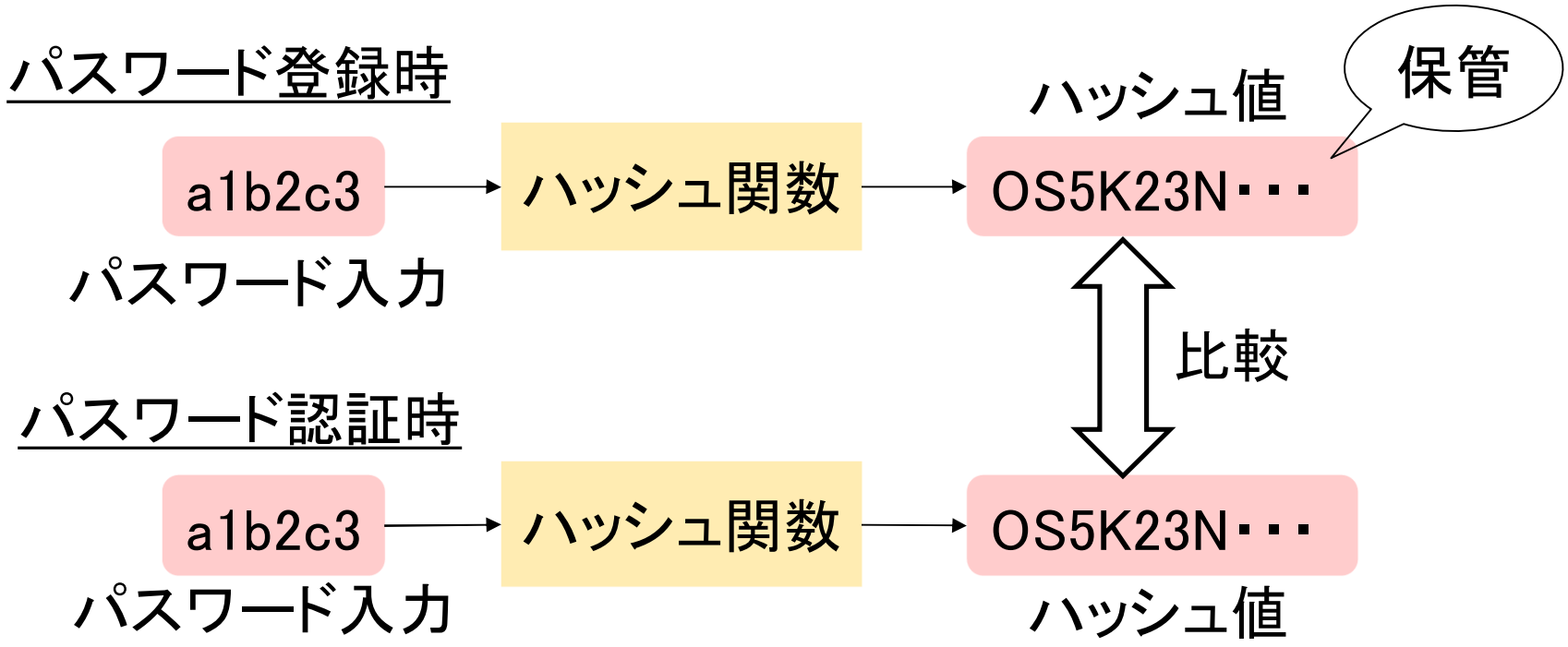
● ユーザ認証

データにアクセスするときに、(ユーザ)IDとパスワードを使って、ユーザ本人によるアクセスであることを確認する。

パスワードは、定期的に変更することが望ましいが、以下のパスワード以外の方法を併用(2要素認証)して、安全性を高める方法もある。

- パスワードのハッシュ化

パスワードをハッシュ関数で変換したハッシュ値で保管し、認証時もハッシュ値で比較する



ハッシュ値が流出しても、パスワードそのものを得ることはできない

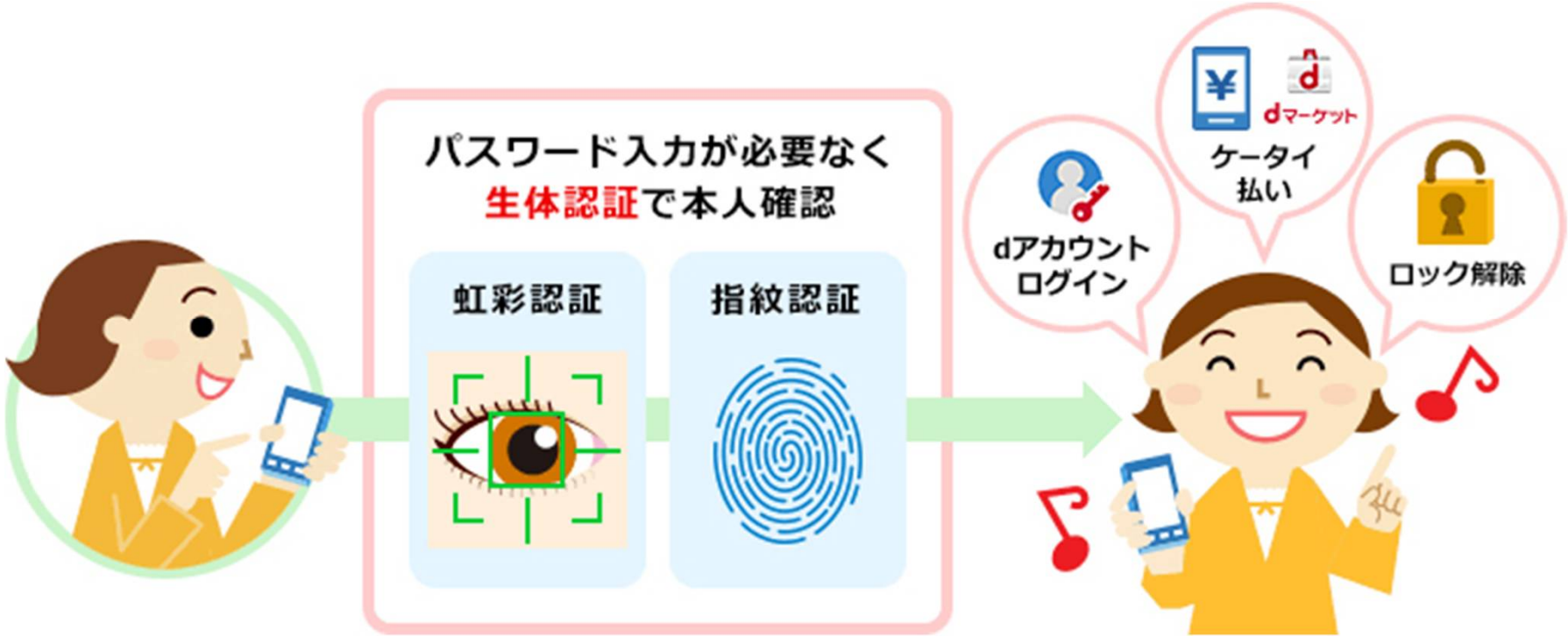
- CAPTCHA：キャプチャ
  （ Completely Automated Public Turing test to tell Computers and Humans Apart ）

自動入力による不正アクセスを防止するために、ゆがんだ画像や一部分が隠れた画像から、文字を入力する

- バイオメトリクス認証

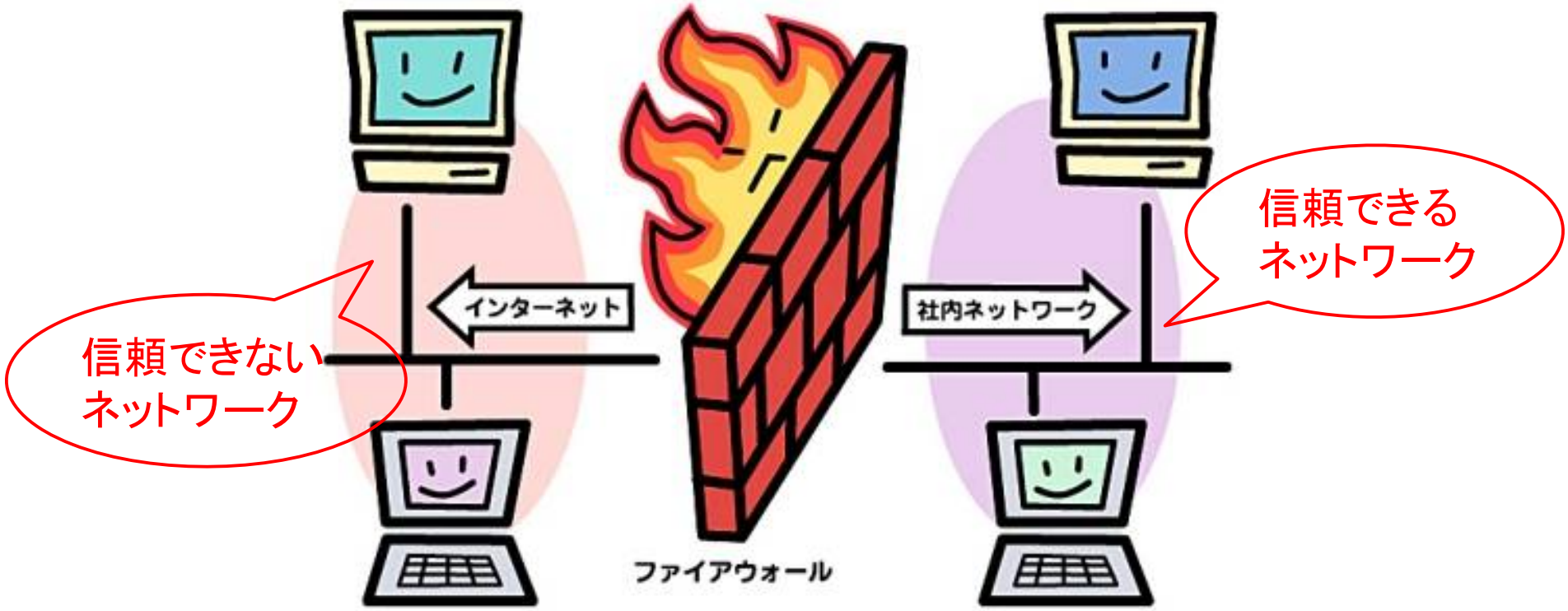
人間の生体情報（指紋や虹彩など）を使って本人認証する。

人間の生体情報（指紋や虹彩など）は、個体によって特徴があり、本人を正確に識別できる。また、この情報は、盗難や置き忘れなどの心配がない。

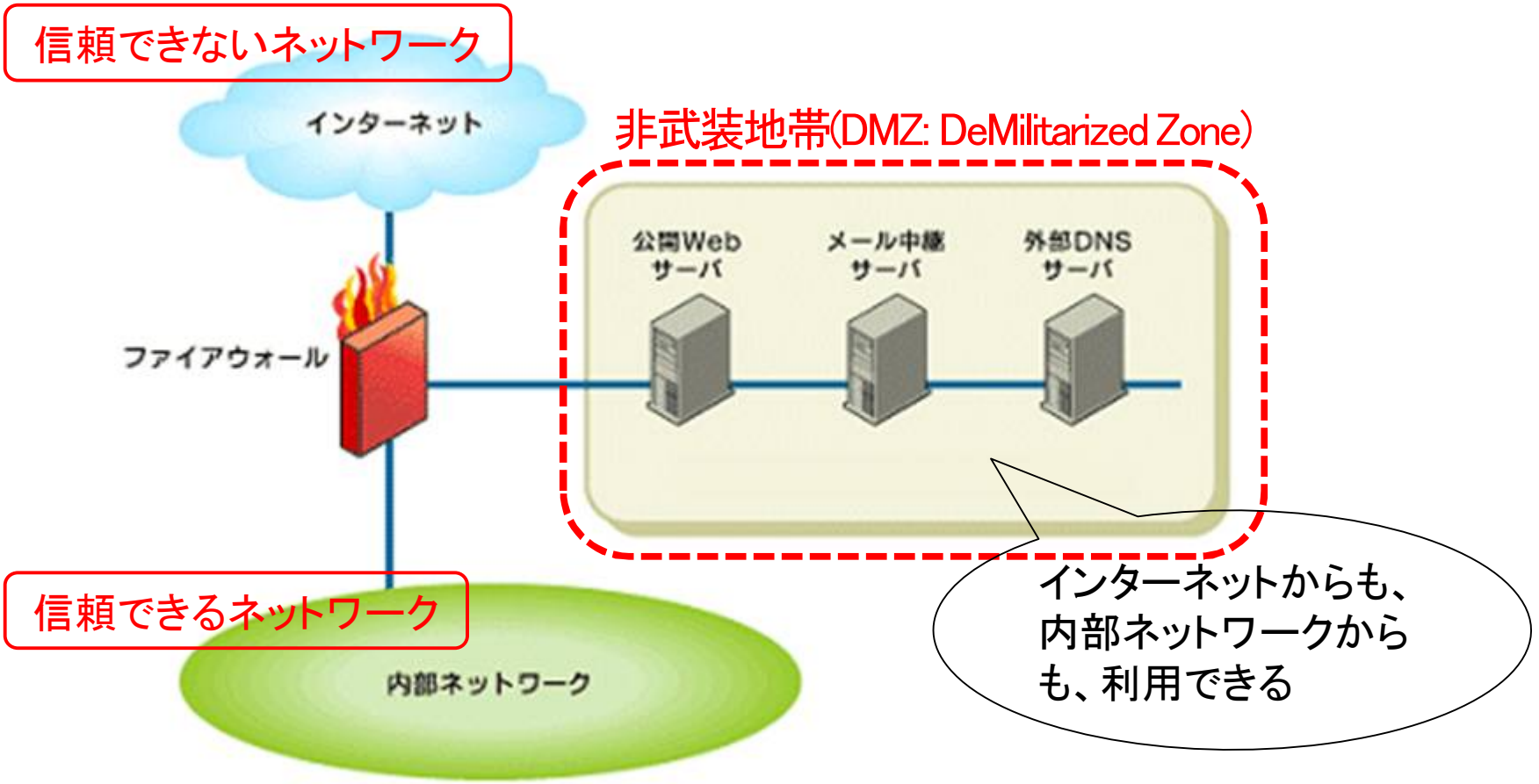


● ファイアウォール

「信頼できるネットワーク」（内部ネットワーク）と「信頼できないネットワーク」（外部ネットワーク）の二つのネットワーク間のアクセスを制御するために使われる。実際には、機器もしくはソフトウェアで実現する。

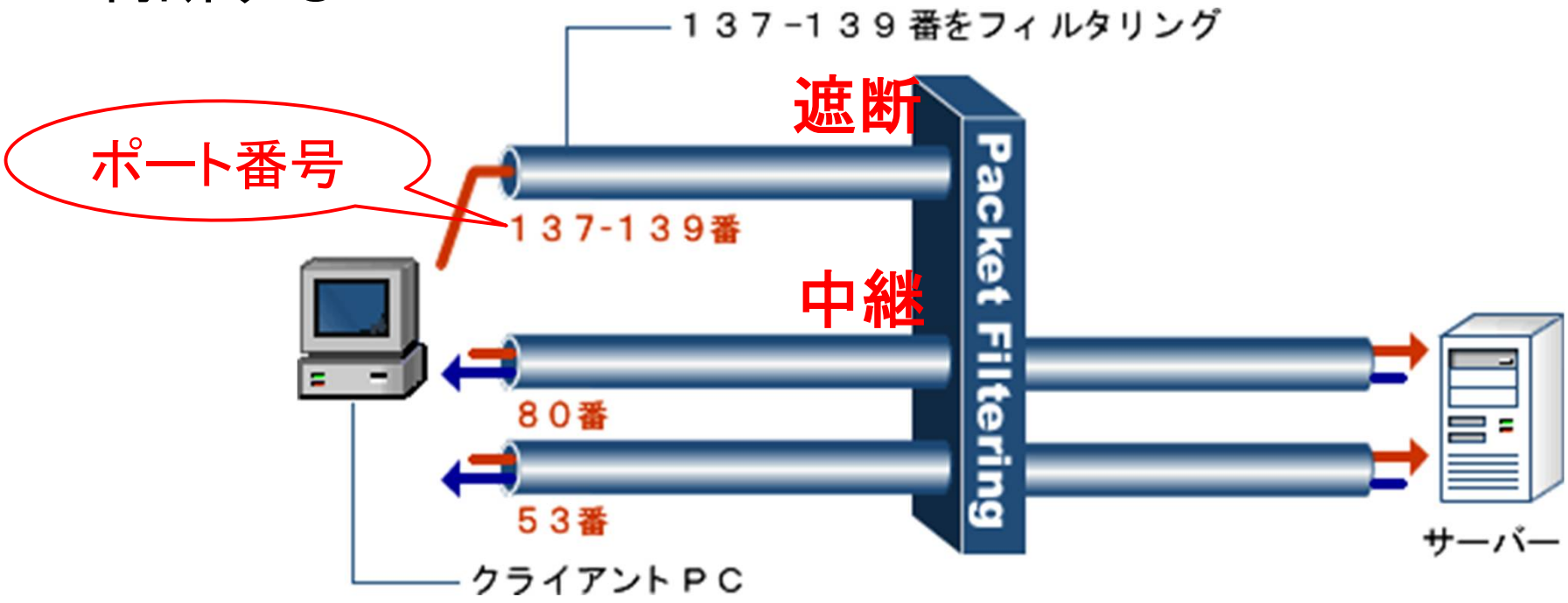


ファイアウォールを設置すると、
「信頼できないネットワーク」と「信頼できるネットワーク」の中間に置かれる区域を、非武装地帯(DMZ: DeMilitarized Zone)と呼び、Webサーバやメールサーバなどインターネットに公開しなければならないサーバを設置できる。



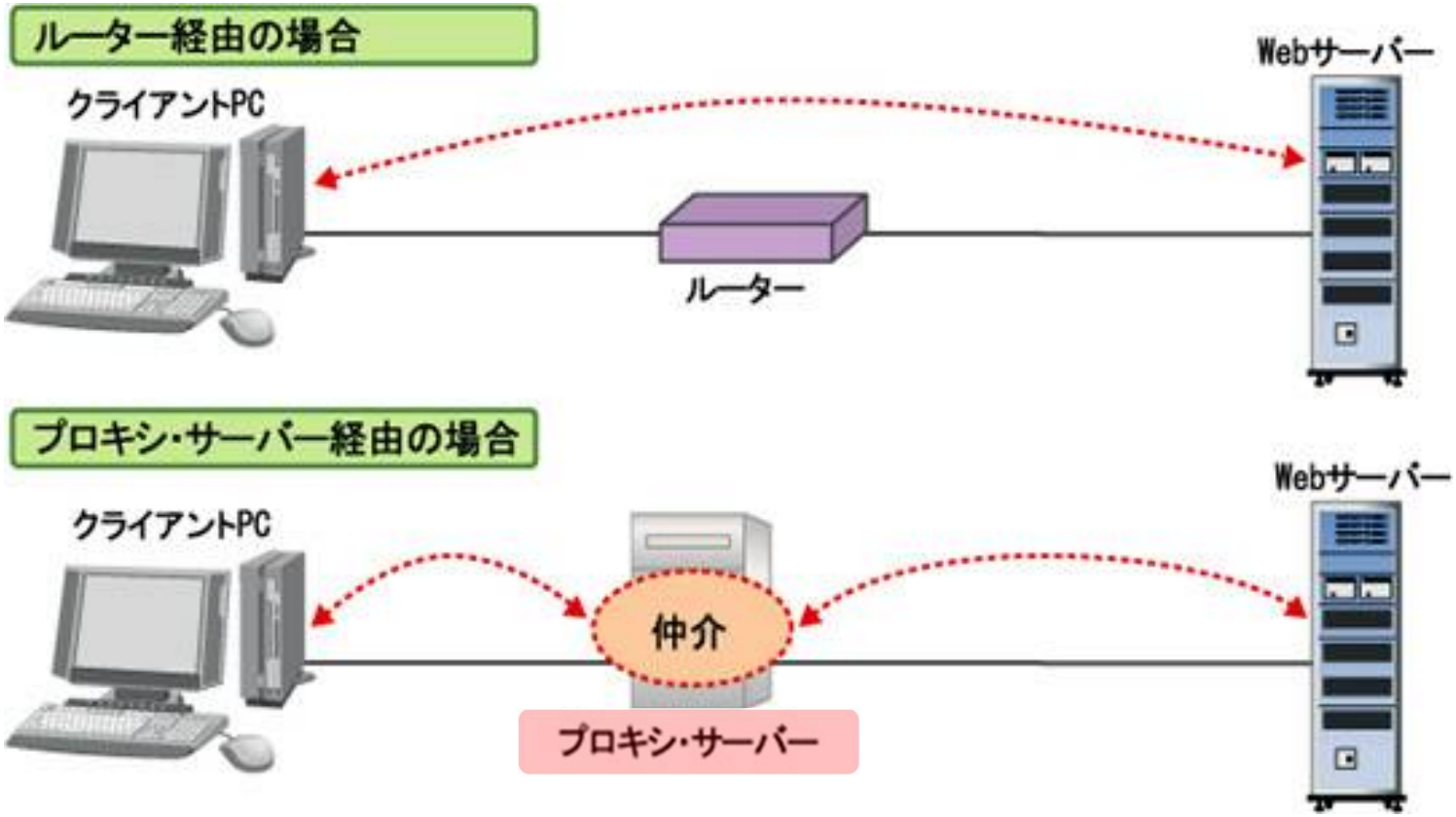
● パケットフィルタリング

ルータやファイヤーウォールなどを経由して行われる通信（データ・パケット）に対して、IPアドレスやポート番号などの情報によって、送られてきたパケットを中継（許可）するべきか、それとも遮断（拒否）するべきかを判断する



● プロキシ（サーバ）

内部ネットワークからインターネット接続を行うとき、主にセキュリティ確保と高速アクセスを実現するために設置されるサーバを、プロキシ「代理」サーバと呼ぶ。ユーザーに代わって業務を代行するサーバを示す。



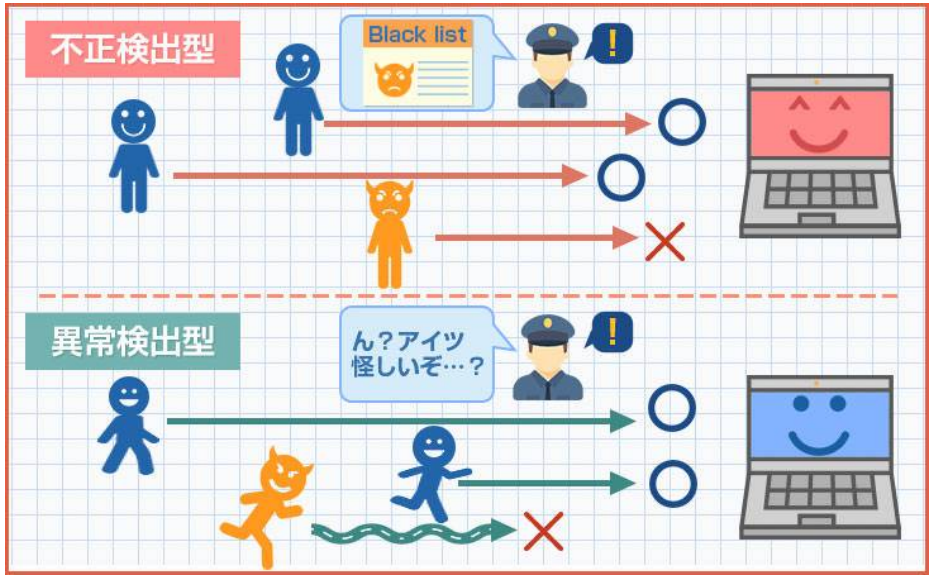
● ペネトレーションテスト

通信ネットワークで、外部と接続されたコンピュータシステムの安全性を調査するテスト方法。既に知られている手法を用いて、実際に侵入や攻撃を試みる。

●侵入検知システム

（IDS: Intrusion Detection System）

コンピュータやネットワークに対する不正行為を検出し、通知するためのシステム。



令和元年度 秋期
基本情報処理技術者試験問題・解答（セキュリティ）

【問39】

情報セキュリティにおいてバックドアに該当するものはどれか。

ア アクセスする際にパスワード認証などの正規の手続が必要なWebサイトに、当該手続を経ないでアクセス可能なURL

イ インターネットに公開されているサーバのTCPポートの中からアクティブになっているポートを探して、稼働中のサービスを特定するためのツール

ウ ネットワーク上の通信パケットを取得して通信内容を見るために設けられたスイッチのLANポート

エ プログラムが確保するメモリ領域に、領域の大きさを超える長さの文字列を入力してあふれさせ、ダウンさせる攻撃

一度不正侵入に成功したコンピュータやネットワークに、いつでも再侵入できるように、攻撃者によって設けられた仕掛けのことを指す。外部からの問い合わせに呼応するプログラムを潜り込ませたり、OSの設定ファイルを書き換えたりして、仕掛ける。

平成31年度 春期
基本情報処理技術者試験問題・解答（セキュリティ）

【問44 】
侵入者やマルウェアの挙動を調査するために、意図的に脆弱性をもたせたシステム又はネットワークはどれか。

ア　DMZ　　イ　SIEM　　ウ　ハニーポット　　エ　ボットネット

脆弱性を含むダミーのシステムを用意し、おびき寄せた侵入者の挙動などを監視する仕組み。記録されたログを分析してシステムのセキュリティ対策に繋げたりする目的で設置する。
ハニーポットとは、悪意を持ったハッカー（侵入者、攻撃者）をおびき寄せる甘いわなを意味する。