

勉強の方針

1. 必ず、実例として、それが扱われているのかを覚えること。
2. 必ず、言葉ではなく、イラストを用いて覚えること。
3. 必ず、知識の『点』と『点』を繋ぎ、『線』にしろ
4. 必ず、まとめることでインプットしているだけなので、口頭で説明してアプトプットしろ。
5. キタミ式で大枠をとらえて、過去問で肉付けしていく。

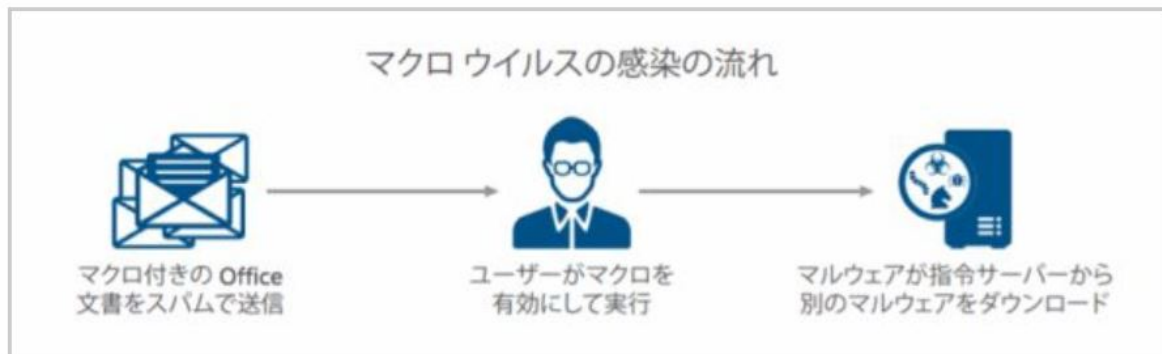
13-01. Malware の種類と特徴

◇ Malware の語源

『malicious（悪意のある）+ software（ソフトウェア）』

◇ Macroウイルス

Wordなどのワープロアプリや、Excelなどの表計算アプリに感染



◇ Worm

自己複製し、1つのコンピュータから、4つの経路（ネットワーク、メール、共有フォルダ、USB）を辿って、他のコンピュータに感染を広げていく。パソコンがグローバルIPで直接インターネットに接続していると感染しやすい。ワームを防ぐためには、パソコンにプライベートIPアドレスを設定し、NATやNAPTなどを介して、インターネットに接続させる必要がある。

【具体例】

共有フォルダ経由での感染拡大

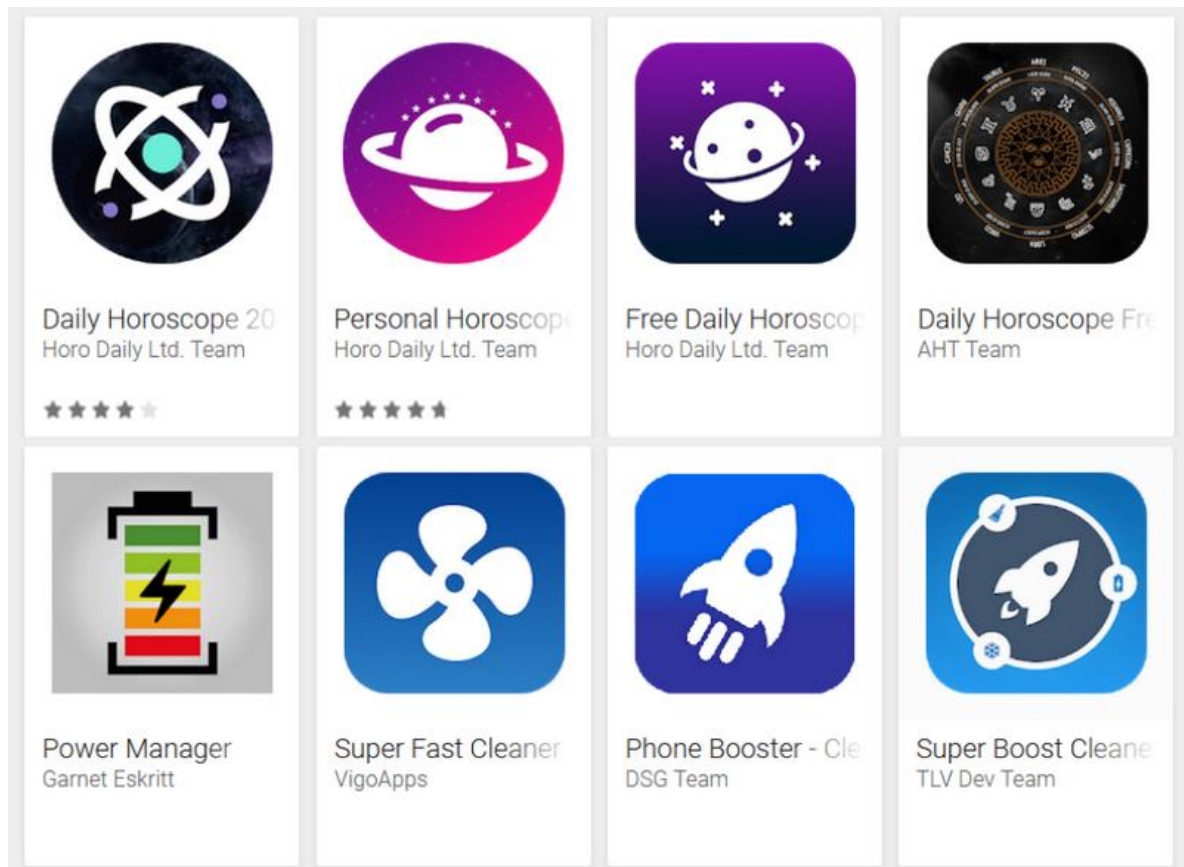
1. コンピュータ上のワーム
2. ネットワークの共有フォルダにワームをコピー
3. ネットワークの共有フォルダにワームをコピー



◇ トロイの木馬

【具体例】

Google play で、過去にアプリとして忍び込んでいたトロイの木馬

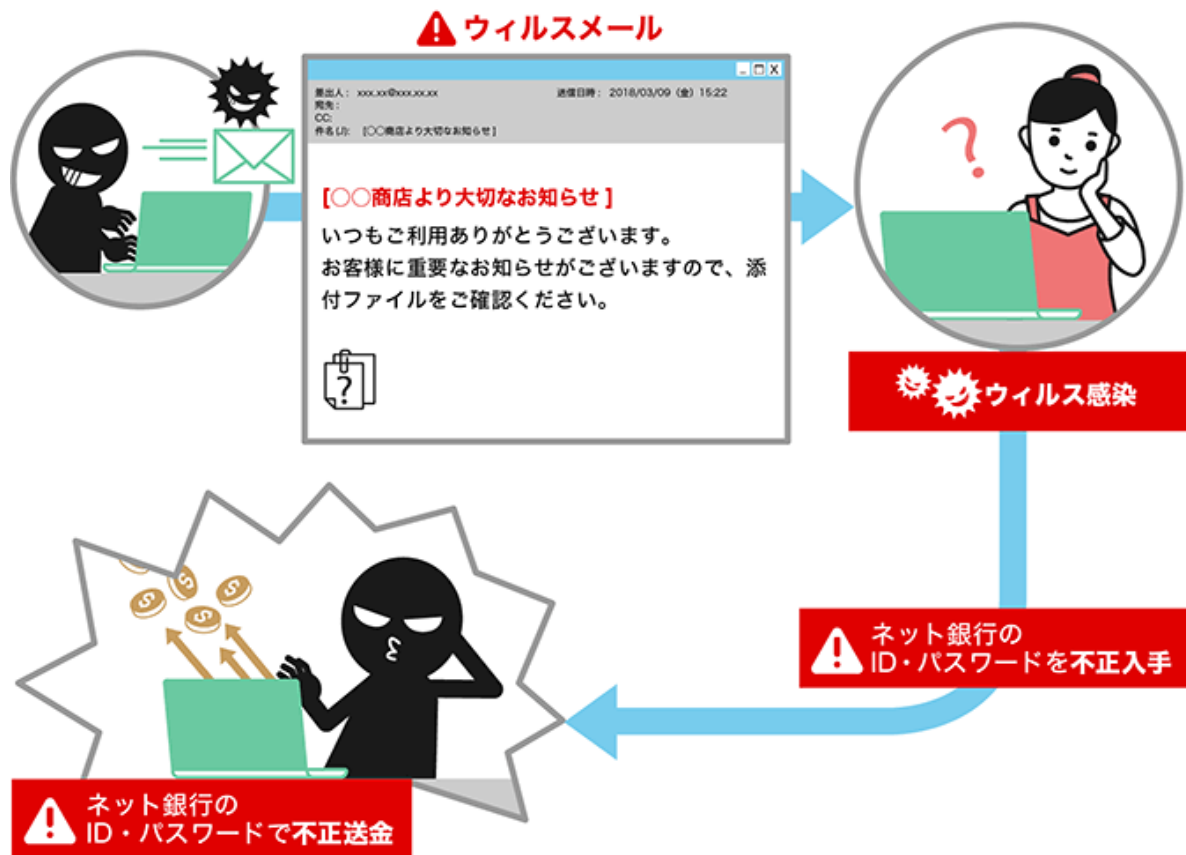


感染方法がギリシャ神話上のトロイの木馬に似ていることに由来する。有用なプログラムであるように見せかけて、パソコン利用者に実行させることで感染。裏で不正な処理を行う。

※トロイの木馬はギリシャ神話に登場する。ギリシャ軍は難攻不落のトロイ城を陥落させるため、中に精鋭部隊を忍び込ませた木馬をトロイ城の近くに置いて帰った。戦利品だと勘違いしたトロイ軍は、城内に木馬を持ち帰った。夜中、木馬の中に隠れた精鋭部隊が自軍の兵士をトロイ城に引き入れ、城を制圧した。

◇ Spyware

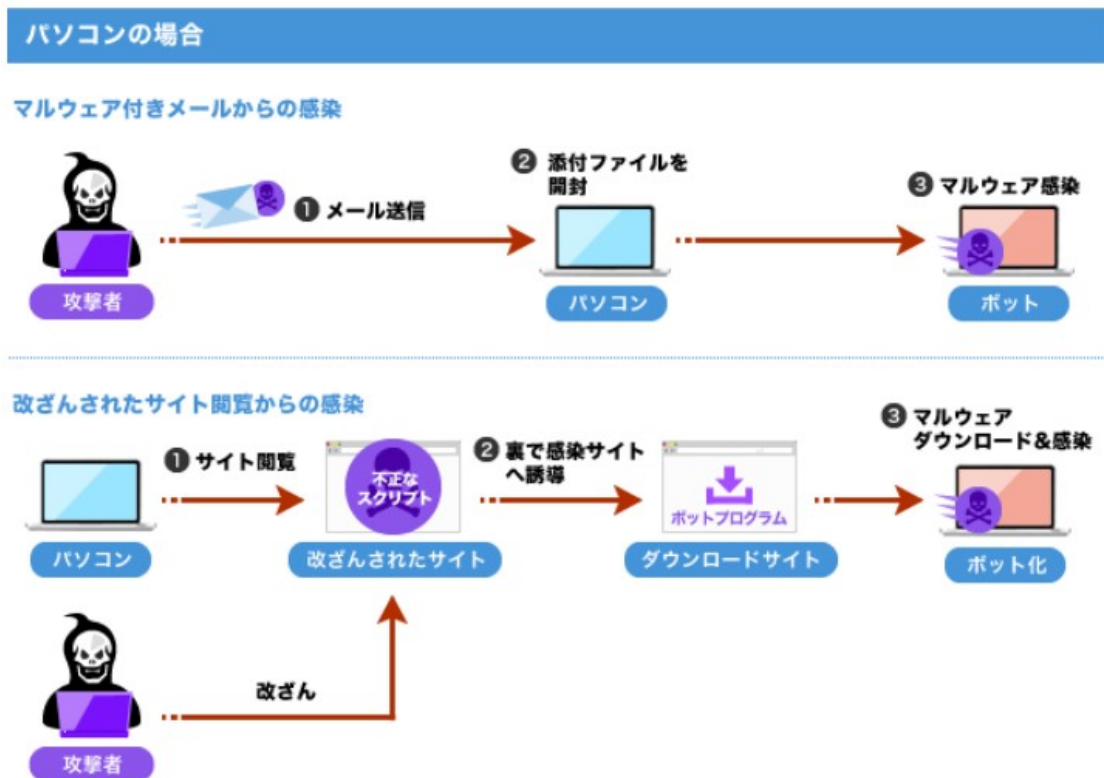
パソコン利用者の個人情報を収集し、外部に送信する。



◇ Bot

あらかじめBot化させておいたパソコンを踏み台として、攻撃者の命令通りに動かす。

- パソコンがボット化するまでのプロセス



- スマホがボット化するまでのプロセス

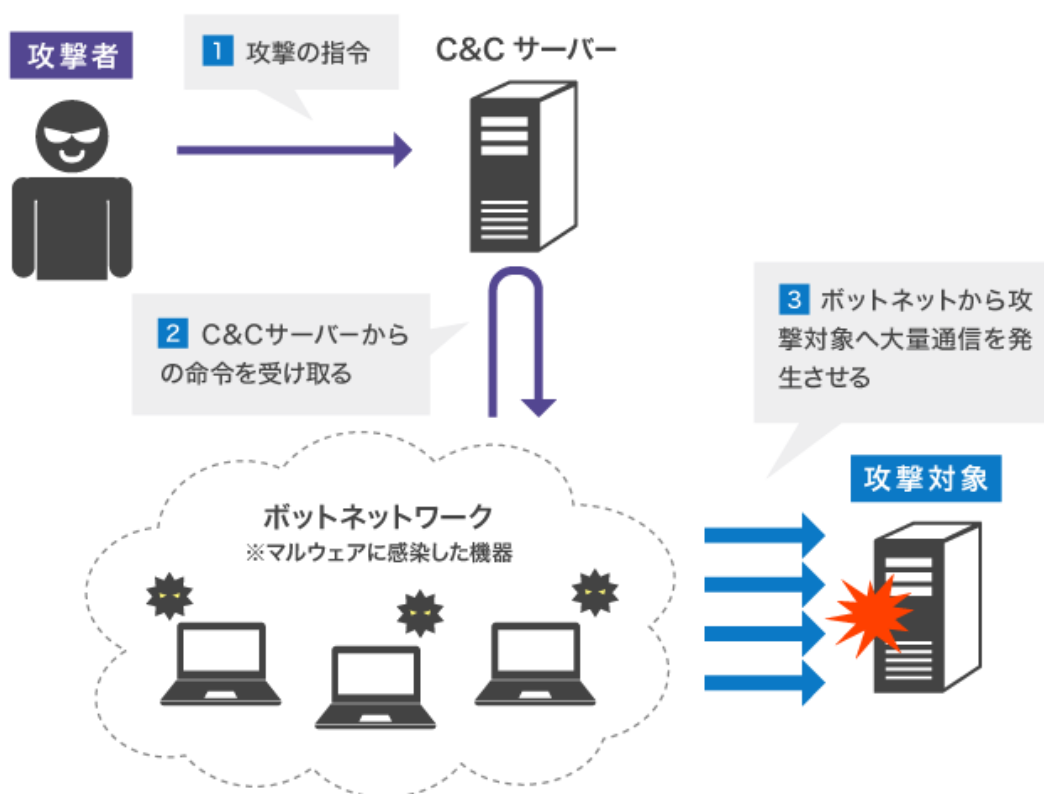
スマートフォンの場合

不正アプリのインストールからの感染



• Bot の使われ方

まず、攻撃対象のネットワーク内にあるパソコンをBot化させる。攻撃者は、Bot化したパソコンを踏み台としてサーバーを攻撃させるように、C&Cサーバーに命令を出す。



13-02. 不正アクセスと対策

◇ ソーシャルエンジニアリング

技術的な手法ではなく、人の弱みに付け込んでパスワードを取得し、アクセスする手法。

◇ 踏み台攻撃

対象のインターネット内のパソコンに攻撃プログラムを仕込んで置き、攻撃者からの命令でサーバを攻撃させる手法（※ボットを用いた攻撃など）

◇ パスワードリスト攻撃

漏洩したパスワードを用いて、正面から正々堂々とアクセスする手法。

◇ Brute-force 攻撃

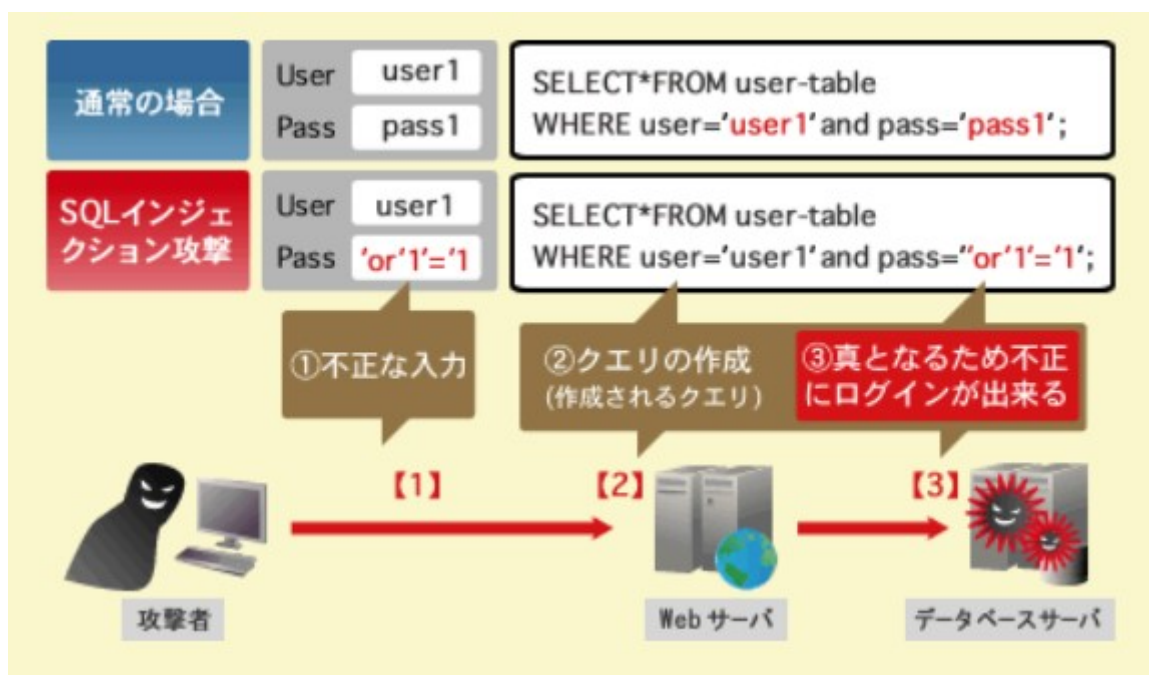
Brute-forceは力ずくの意味。IDを固定して、パスワードを総当たりで試す手法。例えば、5桁数字のパスワードなら、9の5乗通りの組み合わせを試す。

◇ Reverse Brute-force 攻撃

パスワードを固定して、IDを総当たりで試す手法。

◇ SQL Injection

データベースのSQLクエリのパラメータとなる入力に、不正な文字列を入力して不正なSQLクエリを実行させ、データベースの情報を抜き取る手法。ただし、近年は減少傾向にある。



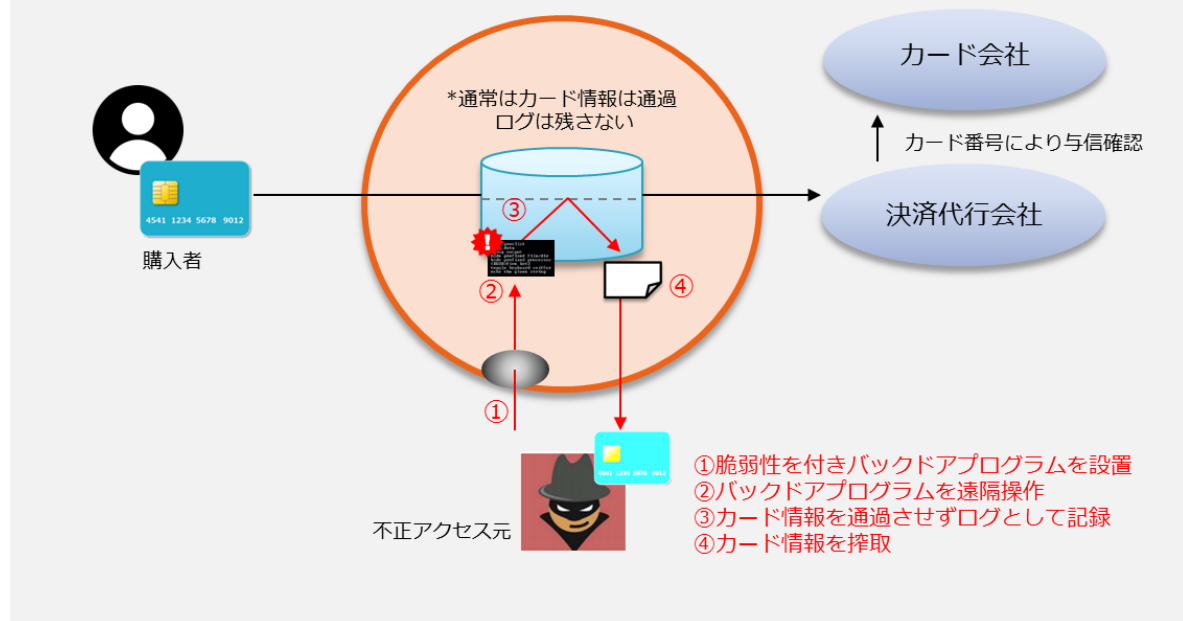
• 対策

データベースのSQLクエリのパラメータとなる入力では、SQLで特別な意味を持つ、『シングルクォーテーション』や『バックスラッシュ』を無効化させる。

◇ Back Door

例えば、Webサイトのカード決済画面やサーバに潜ませることによって、カード情報を第三者に送信する手法。

カード情報通過型の加盟店での情報漏洩

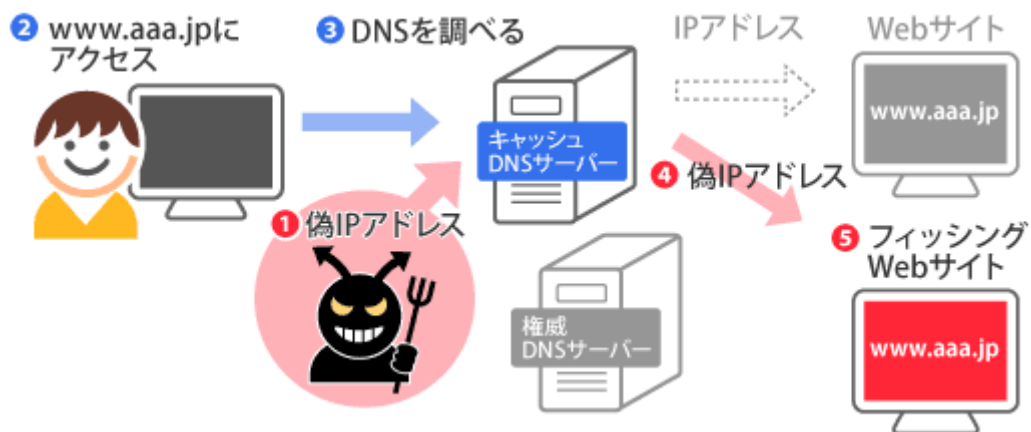


◇ Rainbow 攻撃

ハッシュ化された暗号から、元のパスワードを解析する手法。

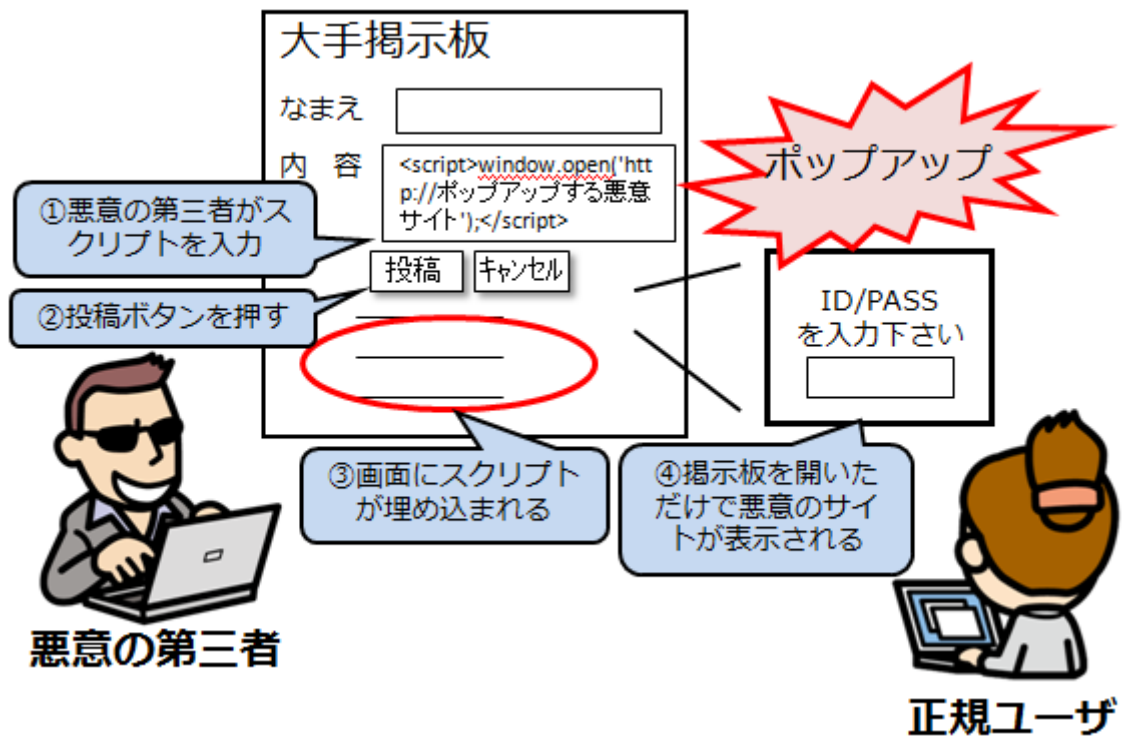
◇ DNS Cache Poisoning

キャッシュDNSサーバーがもつIPアドレスを偽のIPアドレスに変え、偽のWebサイトに強制的にアクセスさせる手法。



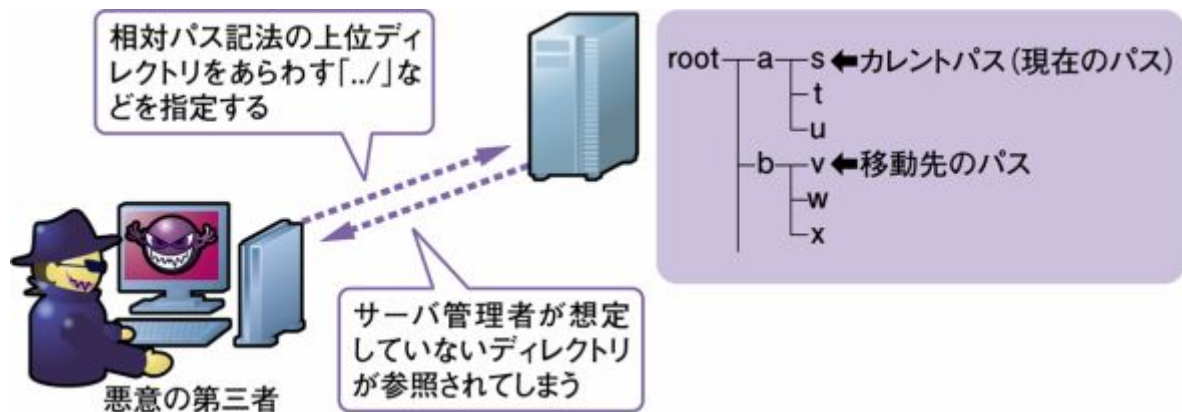
◇ XSS : Cross Site Scripting

WebアプリケーションによるHTML出力のエスケープ処理の欠陥を悪用し、利用者のWebブラウザで悪意のあるスクリプトを実行させる。



◇ Directory traversal

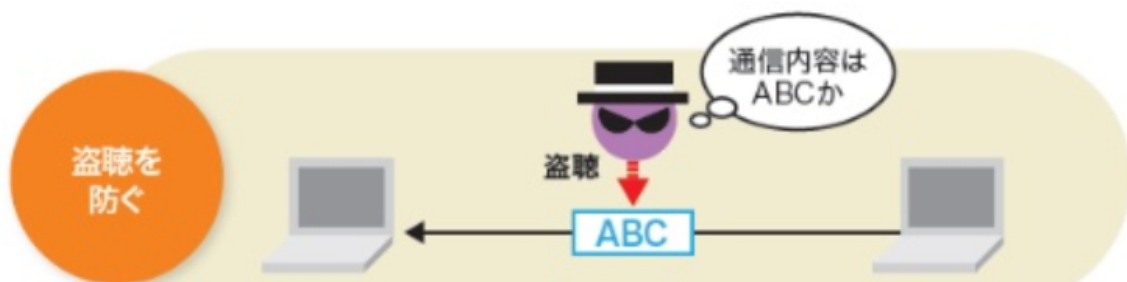
パス名を使ってファイルを指定し、管理者の意図していないファイルを不正に閲覧する。



13-03. セキュリティ技術の役割

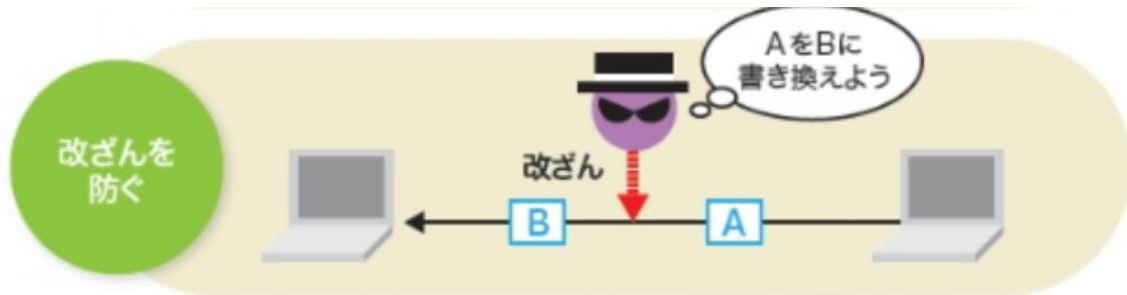
◇ 盗聴（データの盗み取り）を防ぐ

『共通鍵暗号方式』や『公開鍵暗号方式』によって実現される。暗号アルゴリズムに基づく暗号方式を用いてデータを暗号化することによって、盗聴を防ぐ。



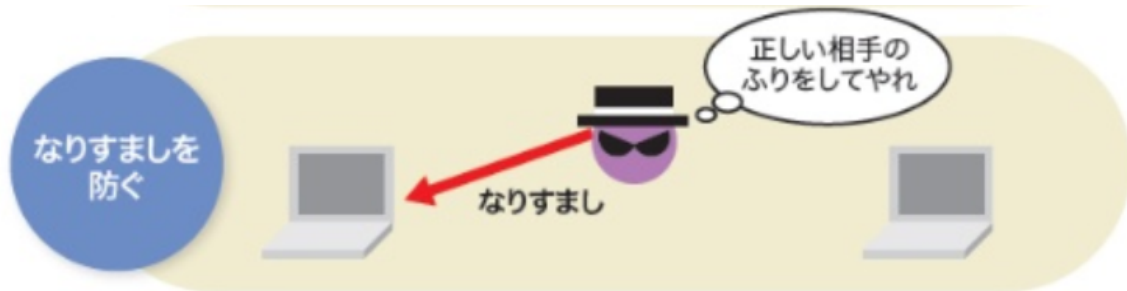
◇ 改竄（データの書き換え）を防ぐ

『ハッシュ関数』によって実現される。相手に送ったデータと相手が受け取ったデータが同じかどうかを確認することによって、改竄を防ぐ。



◇ なりすましを防ぐ

『デジタル署名』によって実現される。正しい相手であることを証明することによって、なりすましを防ぐ。



13-04. 暗号アルゴリズムの種類

次章における暗号方式の理論を実装するためのアルゴリズムを紹介していく。

◇ 共通鍵暗号アルゴリズム

- DES 暗号 : Data Encryption Standard
- AES 暗号 : Advanced Encryption Standard

◇ 公開鍵暗号アルゴリズム

- RSA 暗号 : Rivest-Shamir-Adleman cryptosystem

13-05. 暗号アルゴリズムに基づく暗号方式

◇ 暗号方式の種類一覧

	共通鍵暗号方式	公開鍵暗号方式	ハイブリッド暗号
暗号化アルゴリズム	RC4、DES、3DES、AES	RSA、ElGamal	両方の暗号化アルゴリズム
使用する暗号鍵	共通鍵	公開鍵、秘密鍵	共通鍵、公開鍵、秘密鍵
鍵の管理方法	通信接続先ごとに作成	通信接続先の数に関係なく1つだけ作成	両方の鍵管理方法
鍵の交換方法	第三者に知られないよう安全に交換	作成した公開鍵を一般に公開	両方の鍵交換方法
データの処理時間	速い	遅い	両方の暗号方式の中間

◇ 共通鍵暗号方式

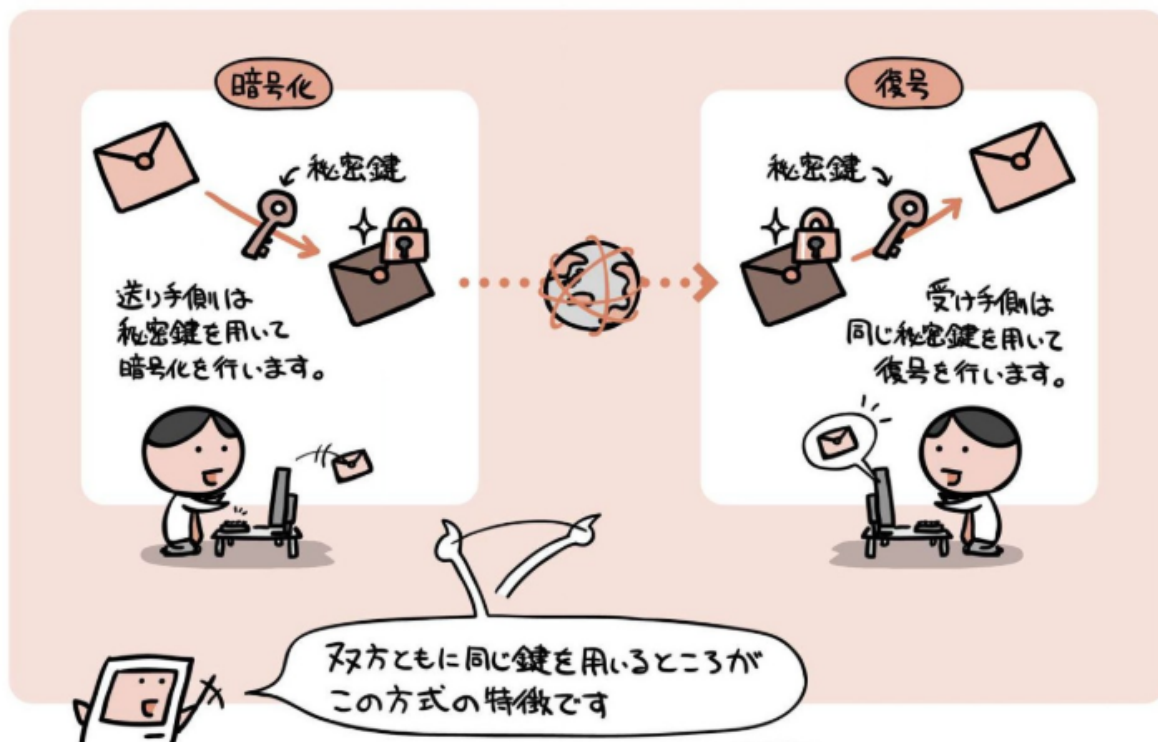
送信者にあらかじめ秘密鍵を渡しておく。鍵の受け渡しを工夫しないと、共通鍵が傍受され悪用される可能性がある（**鍵配送問題**）。

【具体例】

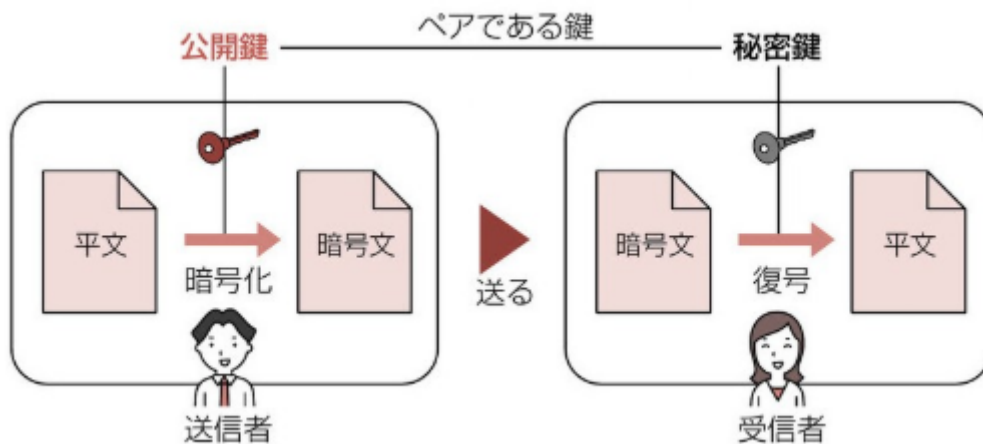
エクセルのファイルロック

長所：処理が速い

短所：鍵の配布が大変



◇ 公開鍵暗号方式 ⇒ 『受信者』に、秘密鍵による本人証明が必要



公開鍵暗号方式でも記載の通り、共通鍵暗号方式の鍵配送問題を解決すべく開発された。『RSA暗号』などによって実装される。送信者にあらかじめ公開鍵を渡しておく。公開鍵は暗号化しかできない。送信者は公開鍵で情報を暗号化する。自分はそれを秘密鍵で復号する。受信する場合、相手から公開鍵をもらう。

長所：鍵の配布が簡単

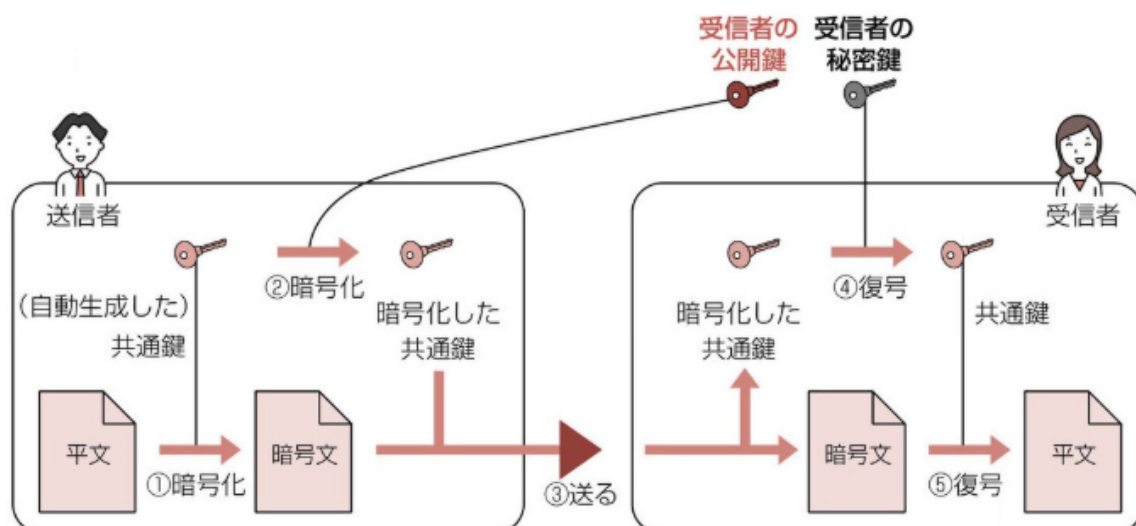
短所：処理が遅い

- 盗聴を防ぐことができる

受信者の公開鍵で暗号化した場合、受信者の秘密鍵でのみ復号可能。すなわち、第三者に復号（解読）されることはないと判断可能。

◇ ハイブリッド暗号方式 ⇒ 『受信者』に、秘密鍵による本人証明が必要

共通鍵暗号方式と公開鍵暗号方式を組み合わせた暗号方式。両方の方式の長所と短所を補う。



13-06. デジタル署名と公開鍵基盤

◇ デジタル署名 ⇒ 『送信者』に、秘密鍵による本人証明が必要

『公開鍵暗号方式とは逆の本人証明』と『ハッシュ関数』を利用したセキュリティ技術。『なりすまし』と『改竄』を防ぐことができる。

【送信者】

1. 平文をハッシュ化し、ダイジェストにする。
2. ダイジェストを秘密鍵（署名生成鍵）で暗号化し、暗号ダイジェスト（デジタル署名）を作成する。
3. 『平文』と『暗号ダイジェスト（デジタル署名）』の両方を送信

【受信者】

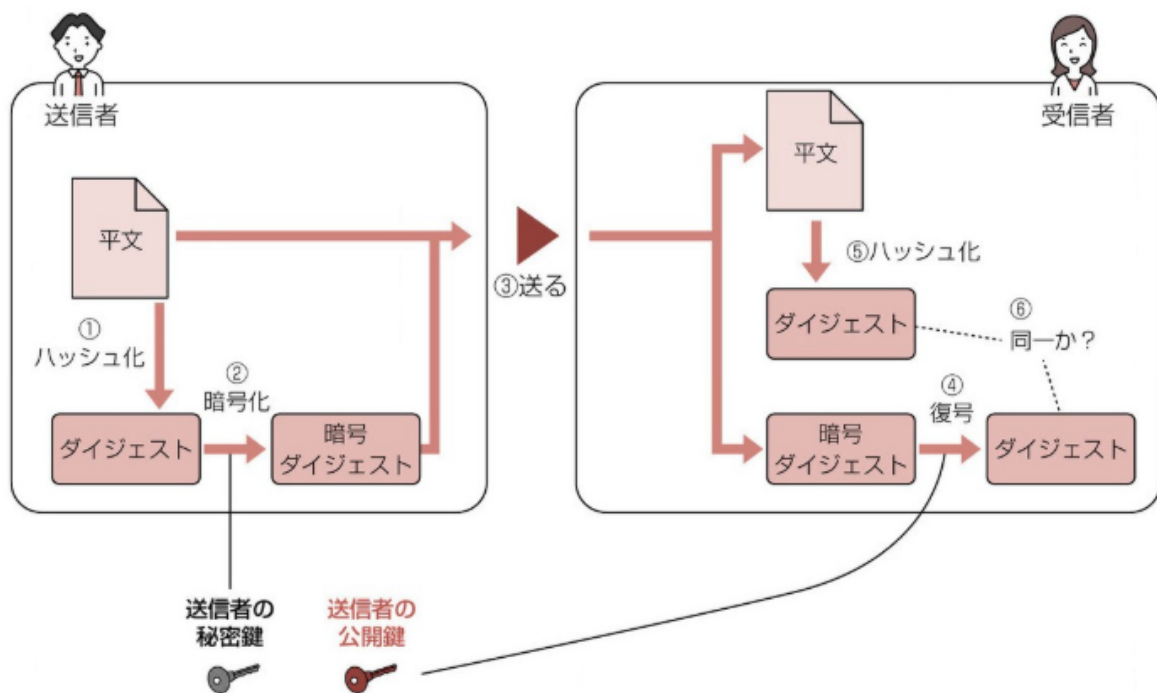
4. 『平文』と『暗号ダイジェスト（デジタル署名）』の両方を受信し、暗号ダイジェストを公開鍵（署名検証鍵）で復号し、ダイジェストにする。
5. 平文をハッシュ化し、ダイジェストにする。
6. 上記2つのダイジェストが同一なら、『なりすまし』と『改竄』が行われていないと判断

• なりすましを防ぐことができる

特定の秘密鍵を持つのは、特定の送信者だけ。したがって、確かに送信者によって暗号化されたものだと判断可能。

• 改竄を防ぐことができる

送信者から送られた『平文』と『暗号ダイジェスト』のどちらかが、通信の途中で改竄された場合、これらのダイジェストが同じになることは確率的にありえない。したがって、確かに改竄されていないと判断可能。

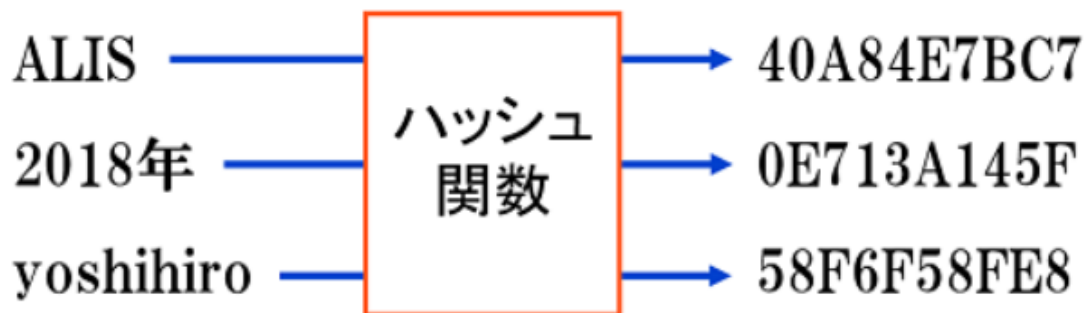


• ハッシュ関数

何かのデータを入力すると、規則性のない一定の桁数の値を出力する演算手法。

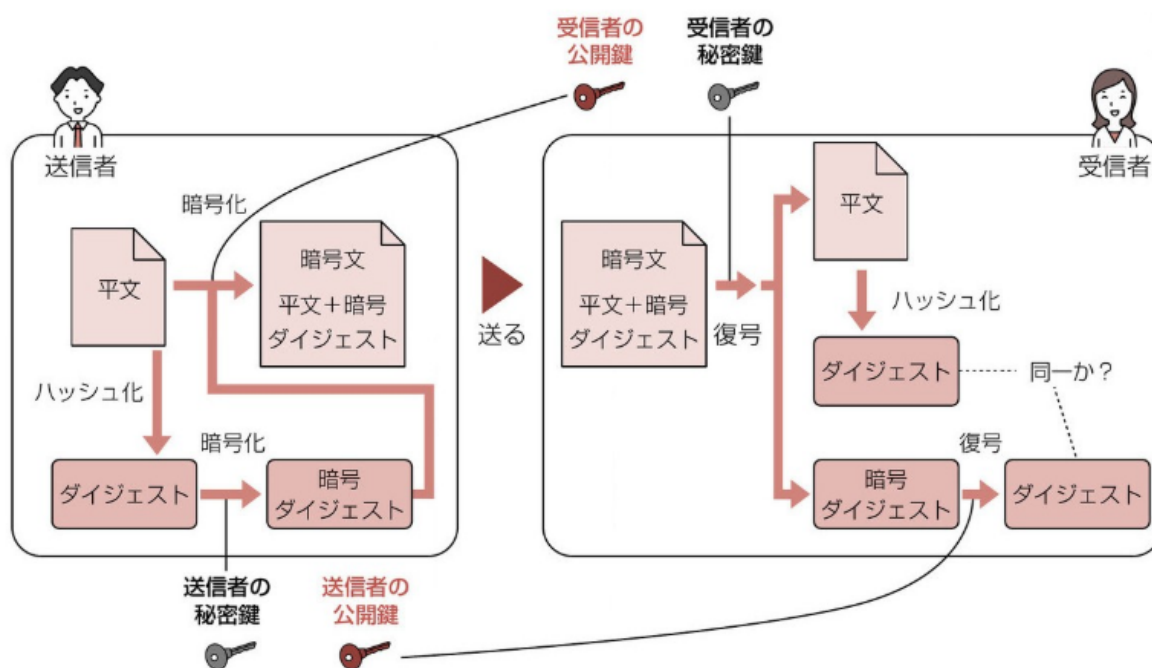
入力値

出力値(=ハッシュ)



◇ 公開鍵暗号方式を組み込んだデジタル署名

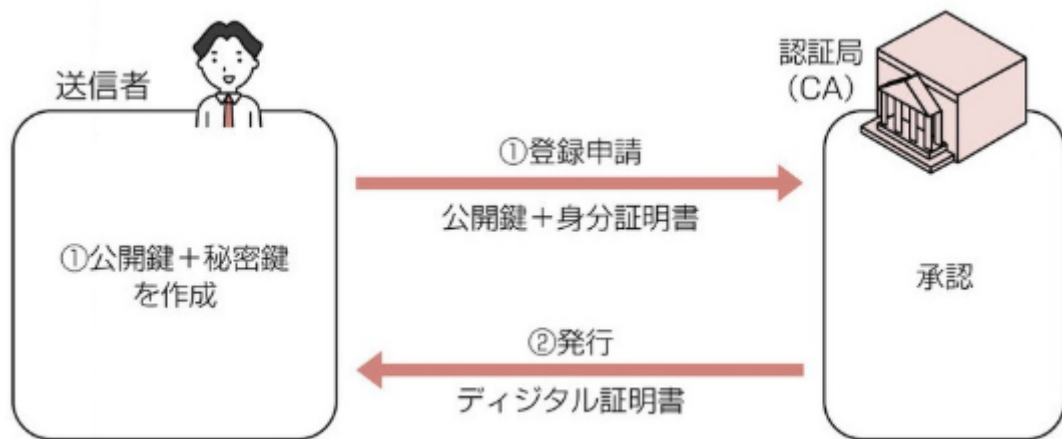
『なりすまし』と『改竄』を防げるデジタル署名に、『盗聴』を防げる公開鍵暗号方式を組み込んだセキュリティ技術。



◇ PKI : Public Key Infrastructure (公開鍵基盤)

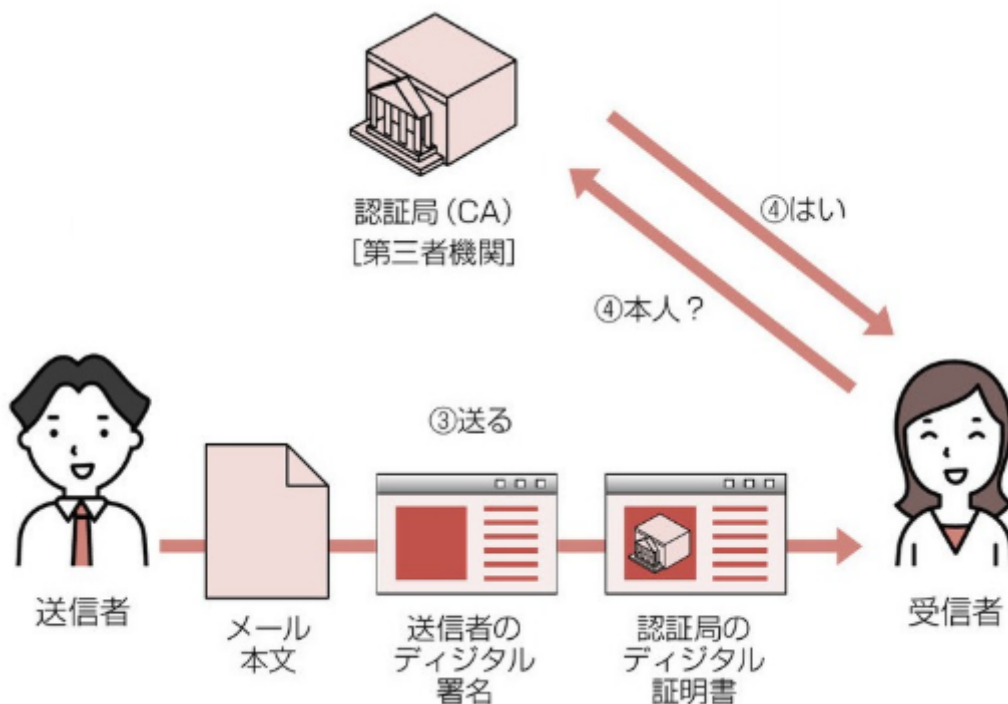
デジタル署名を用いたセキュリティインフラ技術

1. 送信者は、公開鍵と秘密鍵を作り、認証局に公開鍵とデジタル証明書を提出。
2. 認証局は、デジタル署名の入ったデジタル証明書を発行。



3. 送信者は、受信者にメール、デジタル署名、デジタル証明書を送信。

4. よくわからない。

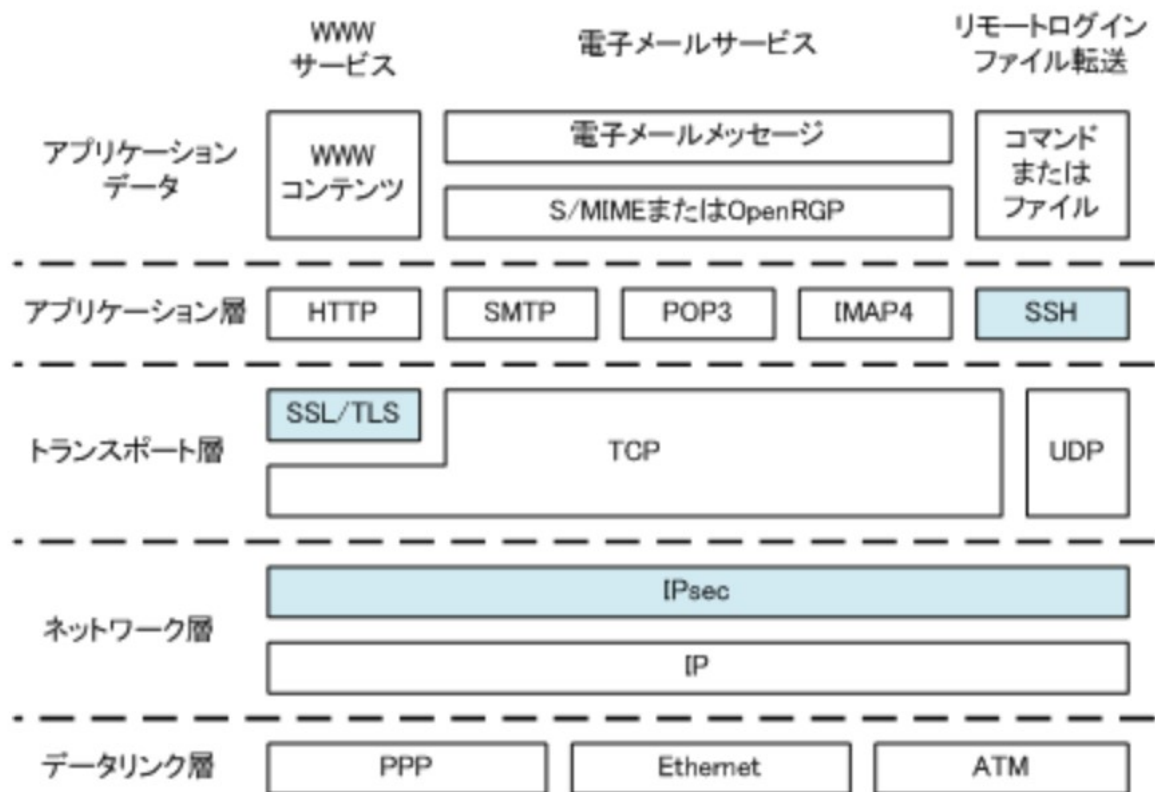


13-07. パケット交換方式におけるセキュリティ技術

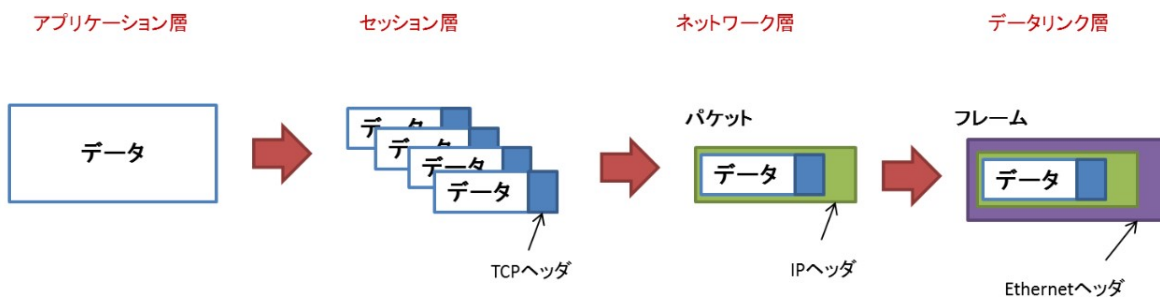
◇ TCP/IP階層モデルとOSI参照モデルの対応関係（再掲）

OSI参照モデル	TCP/IPの階層モデル	TCP/IPプロトコル	コンピュータ上の処理
アプリケーション層	アプリケーション層	HTTP, SMTP, POP3 FTP, SSH, RIP, SNMP...	通信アプリケーション プログラム
プレゼンテーション層			
セッション層			
トランスポート層	トランスポート層	TCP, UDP	OS
ネットワーク層	インターネット層	IP, ARP, ICMP, OSPF...	
データリンク層	ネットワーク インターフェース層	Ethernet, PPP...	デバイスドライバ NIC
物理層			

◇ OSI参照モデルにおける各プロトコルの分類（再掲）



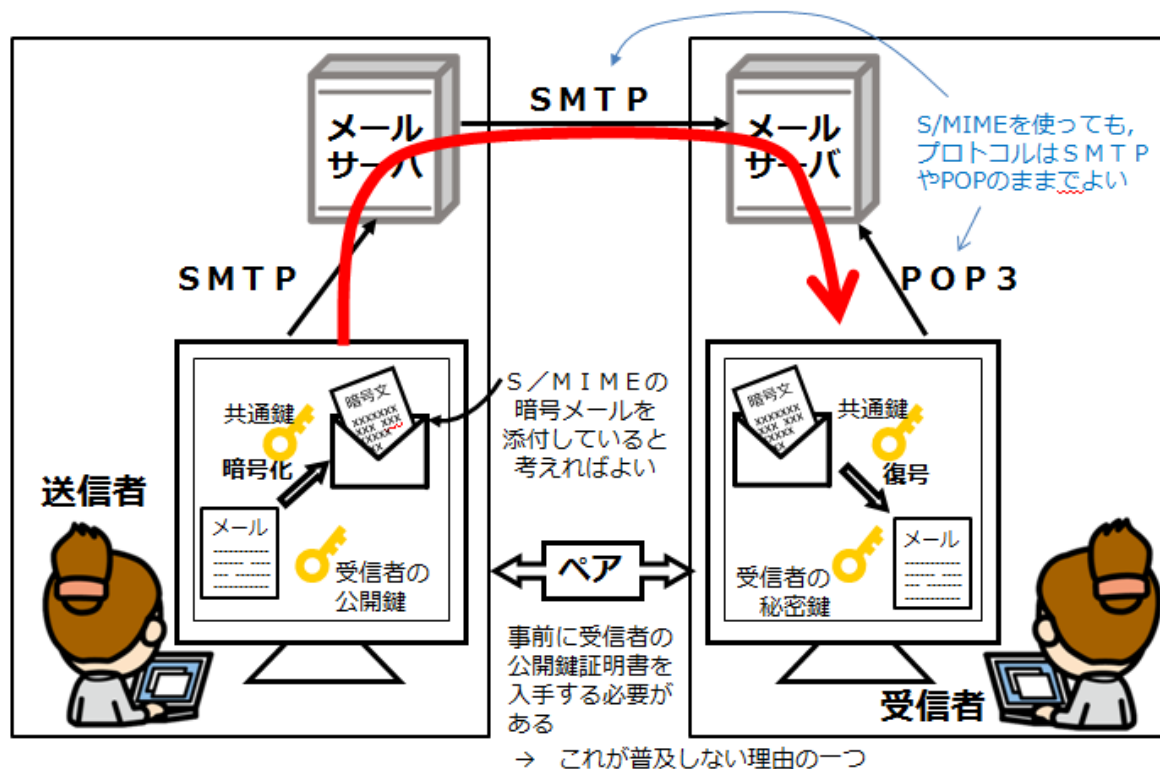
◇ データへのヘッダ情報追加とカプセル化（再掲）



13-08. アプリケーションデータのセキュリティ技術

◇ S/MIME : Secure MIME

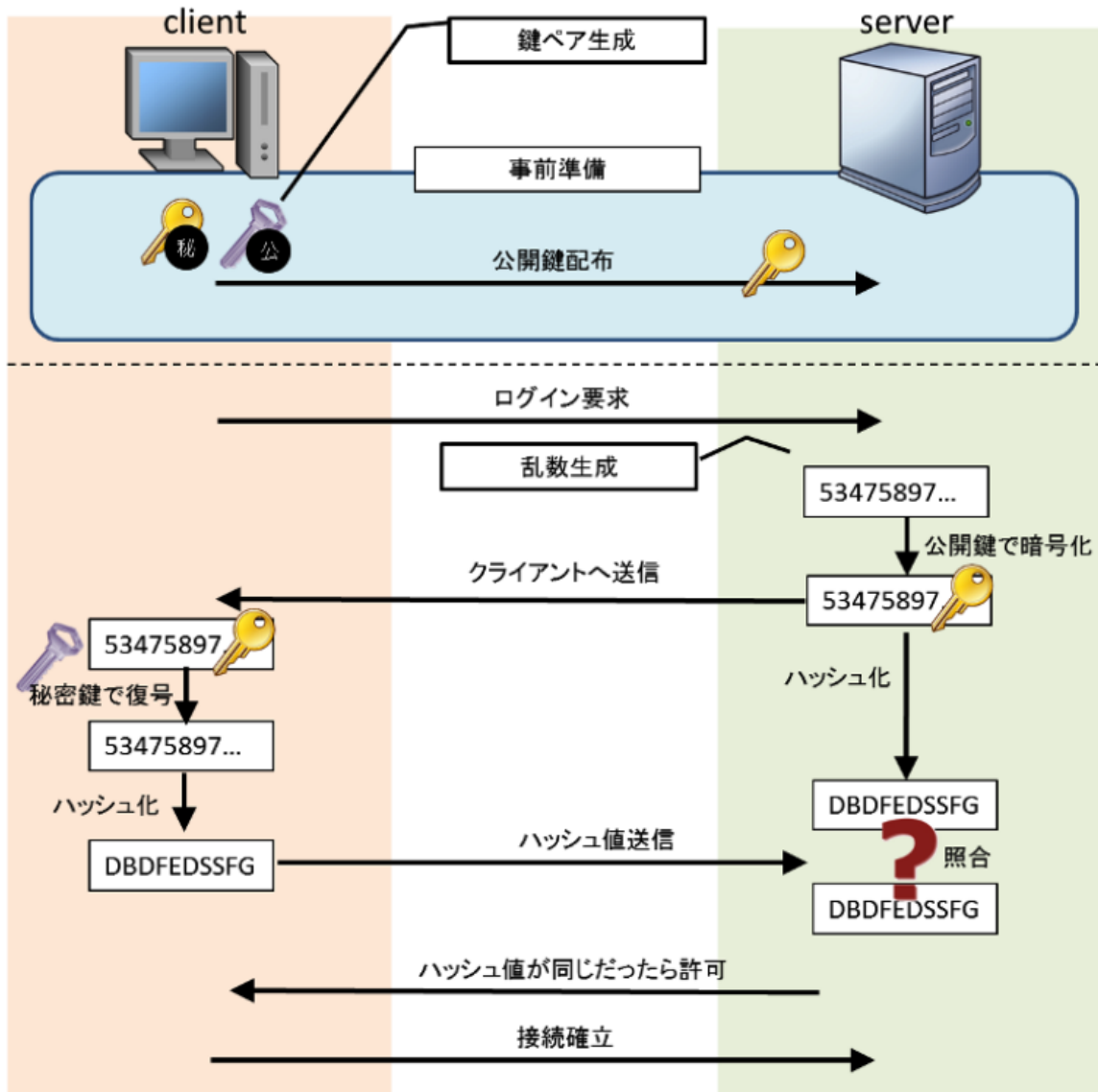
公開鍵暗号方式に基づく技術。アプリにおいて、デジタル署名による認証の機能を、メールに追加することができる。



13-09. アプリケーション層のセキュアプロトコル

◇ SSH : Secure Shell

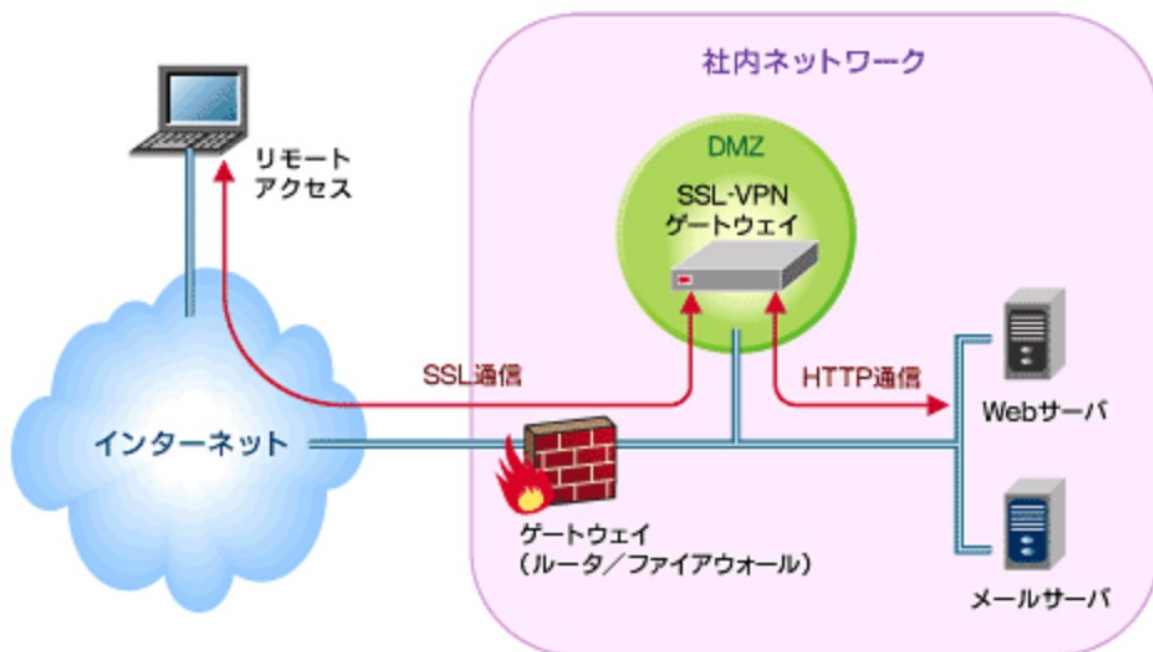
公開鍵暗号方式に基づくセキュアプロトコル。アプリケーション層で、データの暗号化を担う。暗号方式と認証方式の技術を用いて、リモートコンピュータとの通信を安全に行う。公開鍵暗号方式が用いられる。例えば、クライアント側SSHソフトには、『OpenSSH』、『Apache MINA/SSHD』があり、またサーバ側SSHソフトには、『OpenSSH』、『TeraTerm』、『Putty』がある。



13-10. トランスポート層のセキュアプロトコル


◇ SSL/TLS

ハイブリッド暗号方式に基づくセキュアプロトコル。トランスポート層で、パケットのヘッダ情報の暗号化を担う。インターネットVPNの実現のために用いられる。



【具体例】

Chromeでは、SSL接続に不備があると、以下のような警告が表示される。



この接続ではプライバシーが保護されません

■■■■■■■■■■ では、悪意のあるユーザーによって、パスワード、メッセージ、クレジットカードなどの情報が盗まれる可能性があります。詳細


NET::ERR_CERT_COMMON_NAME_INVALID

☐ セキュリティに関する事象についての詳細を Google に自動送信する。 [プライバシー ポリシー](#)

詳細設定

クリックすると以下が表示

セキュリティで保護されたページに戻る



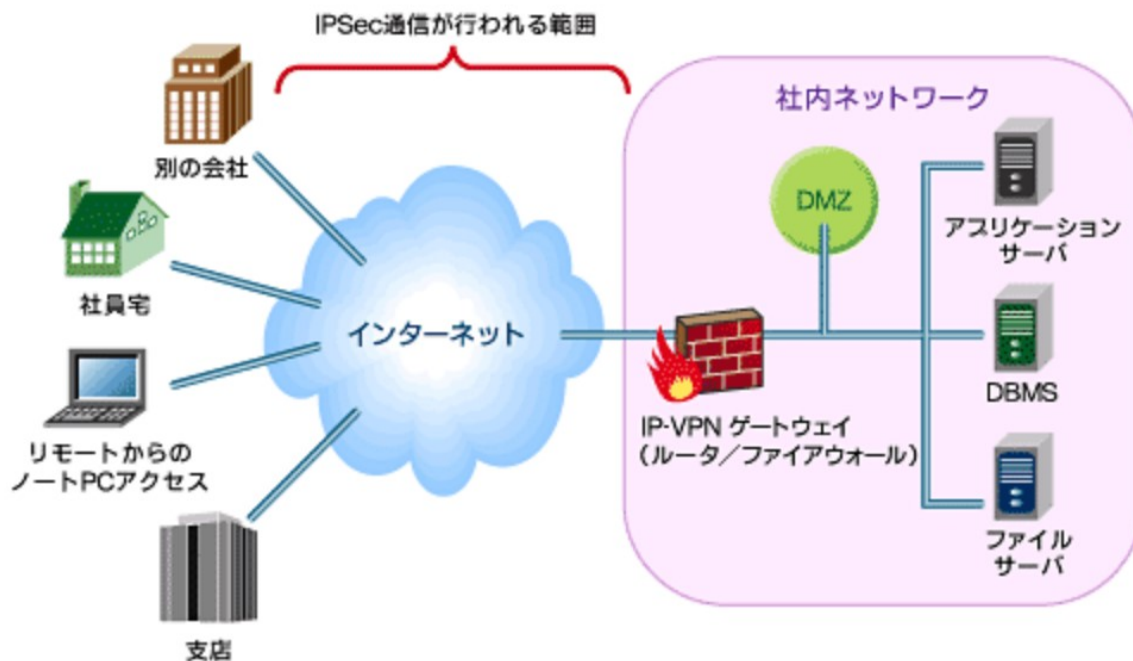
このサーバーが ■■■■■■■■■■ であることを確認できませんでした。このサーバーのセキュリティ証明書は ■■■■■■■■■■.com から発行されています。原因としては、不適切な設定や、悪意のあるユーザーによる接続妨害が考えられます。

■■■■■■■■■■ にアクセスする (安全ではありません)

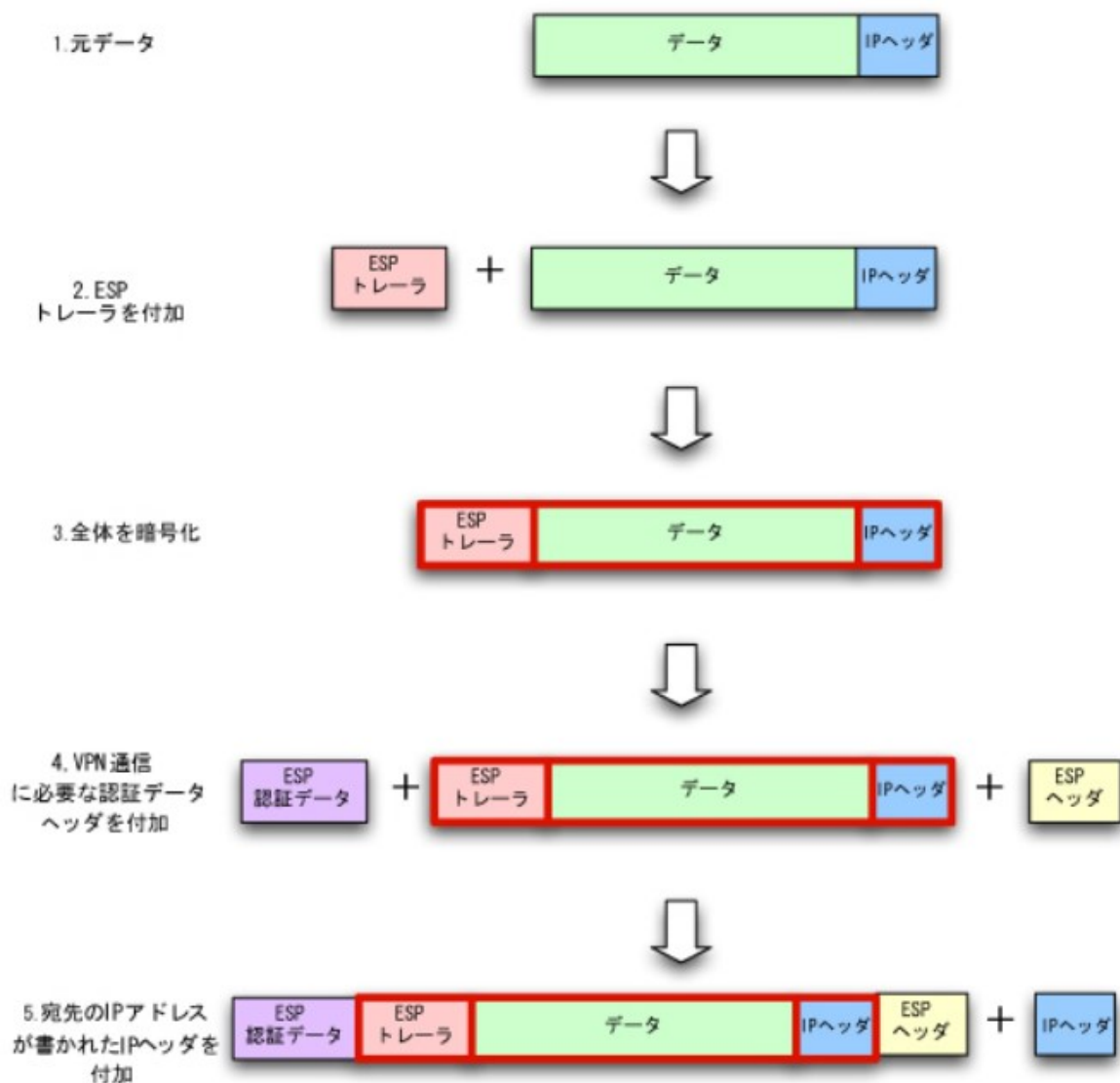
13-11. ネットワーク層のセキュアプロトコル

◇ IPsec

共通鍵暗号方式に基づくセキュアプロトコル。ネットワーク層で、パケットのヘッダ情報の暗号化を担う。インターネットVPNの実現のために用いられる。盗聴を防ぐことができる。

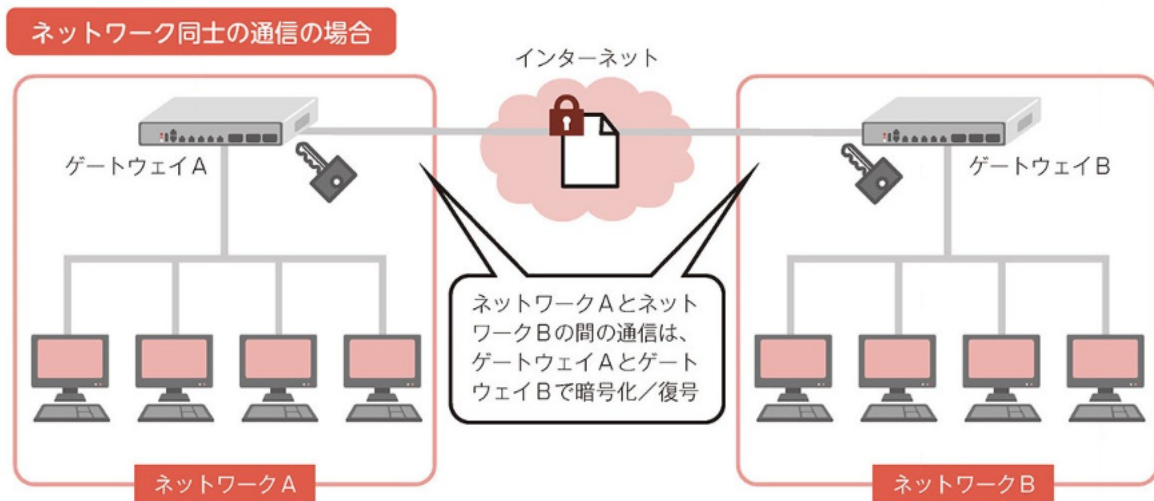


• IPsecによるパケットのカプセル化



◇ VPN : Virtual Private Network (仮想プライベートネットワーク)

異なるネットワーク間で安全な通信を行うための仕組み。IPsecやSSL/TLSによって実現される。



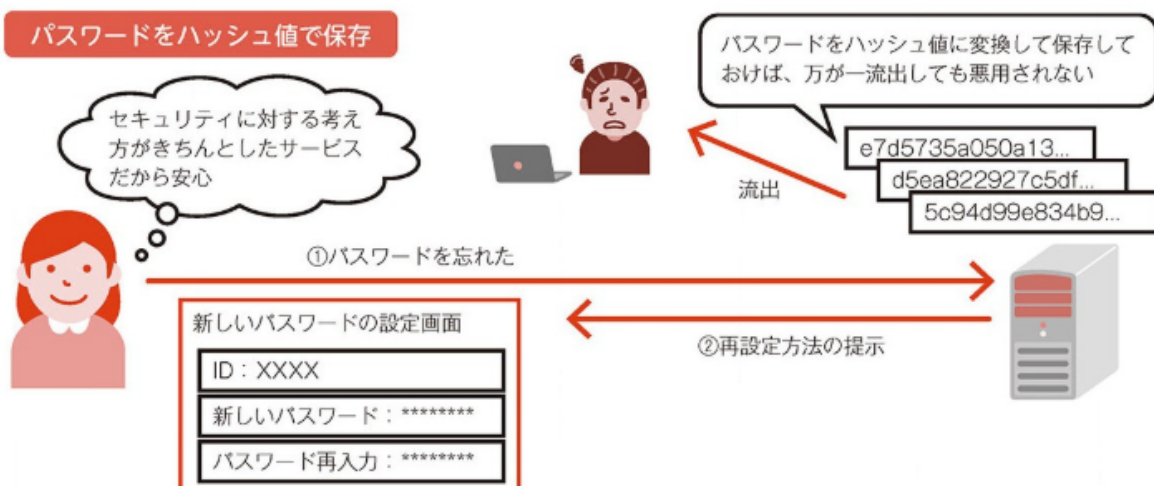
13-12. その他のセキュリティ技術

◇ メール受信におけるセキュリティ

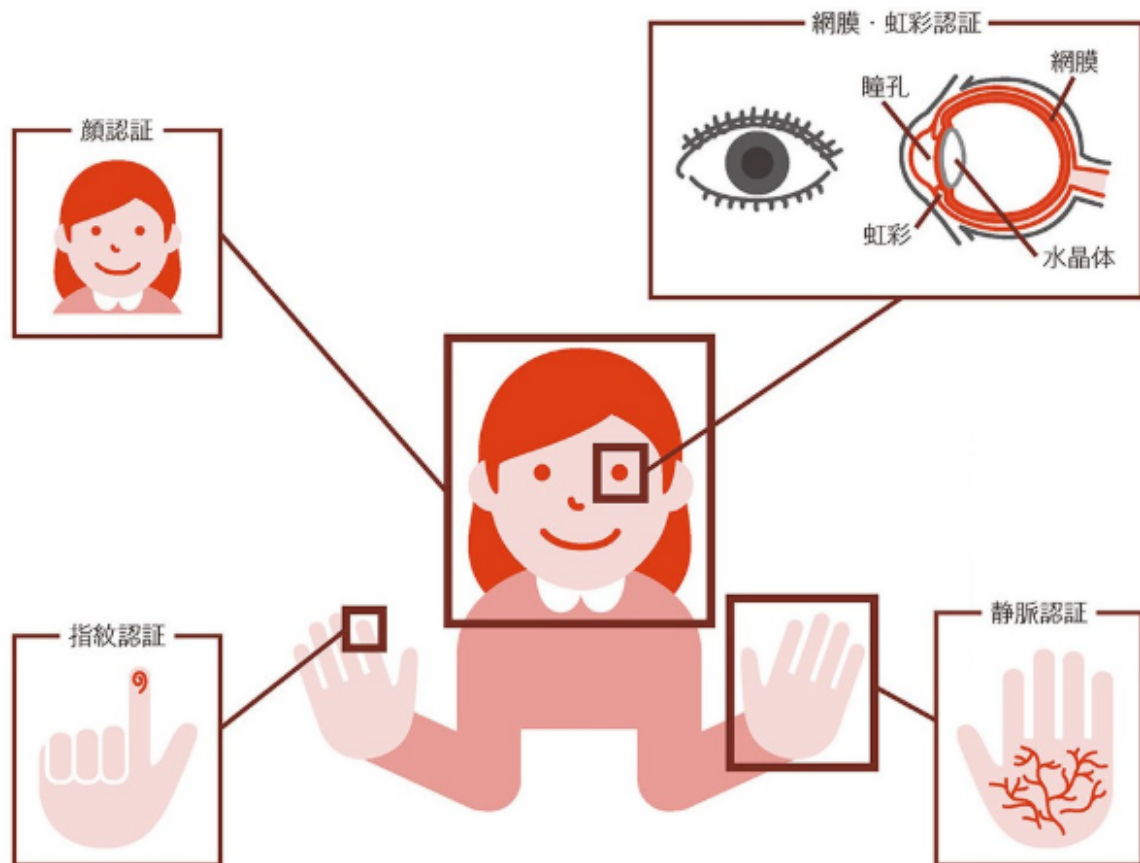
- OP25B (Outbound Port 25 Blocking)
- SPF (Sender Policy Framework)

◇ パスワードの保存方法

平文で保存しておく、流出した時に勝手に使用されてしまうため、ハッシュ値で保存するべきである。

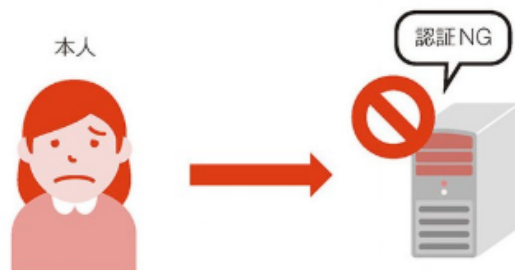


◇ 生体認証



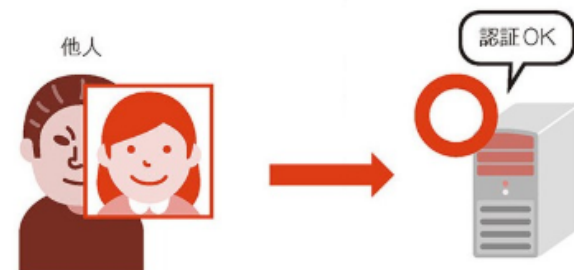
本人拒否率

本人が認証に失敗する確率のことです。



他人受入率

他人が認証に成功する確率のことです。



◇ Web beacon

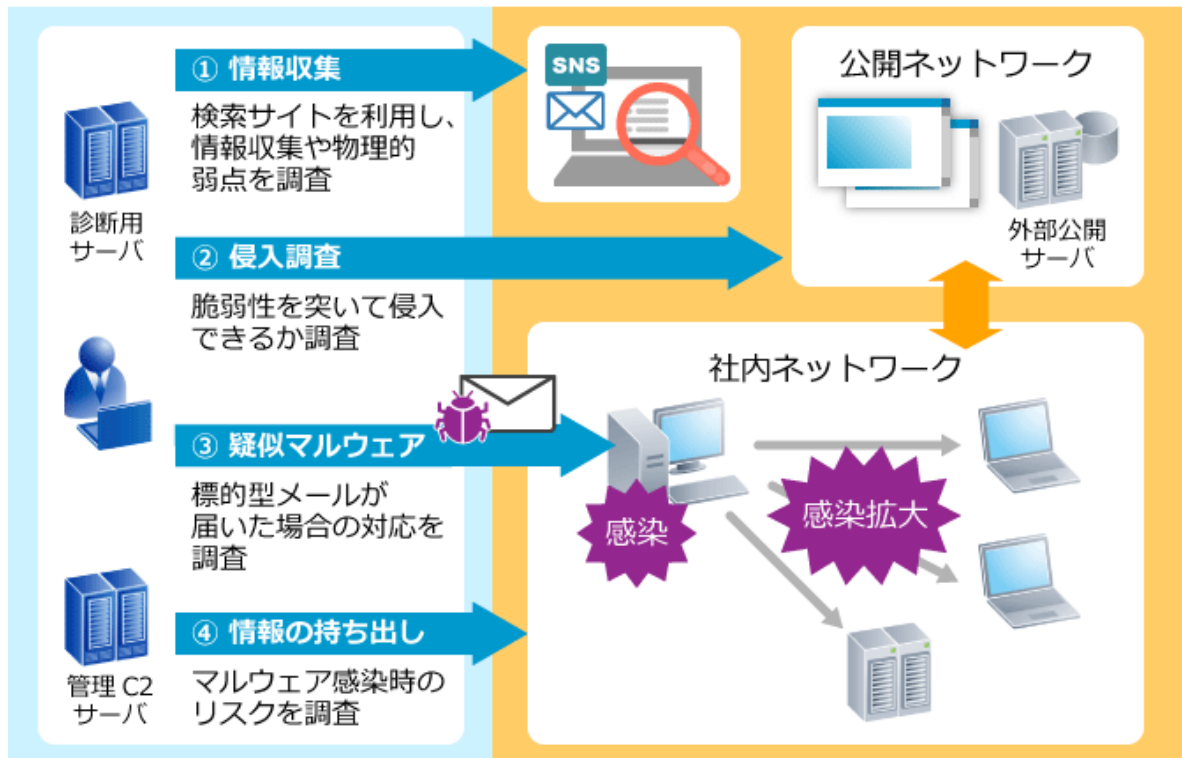
webページに、サーバに対してHTTPリクエストを送信するプログラムを設置し、送信されたリクエストを集計するアクセス解析方法。例えば、1x1の小さなGif「画像」などを設置する。

◇ Penetration テスト

既知のサイバー攻撃を意図的に行い、システムの脆弱性を確認するテストのこと。

【具体例】

株式会社LACによるPenetration テストサービス



13-13. セキュリティガイドライン

◇ セキュリティマネジメントの3要素



- **Confidentiality (機密性)**
許可された人のみが情報にアクセスできるようにすること。
- **Integrity (完全性)**
情報が書き換えられないこと。
- **Availability (可用性)**
許可された人が必要な時に必要な情報を利用できること。

◇ セキュリティポリシー

◇ プライバシーマーク

◇ サイバーセキュリティ経営ガイドライン