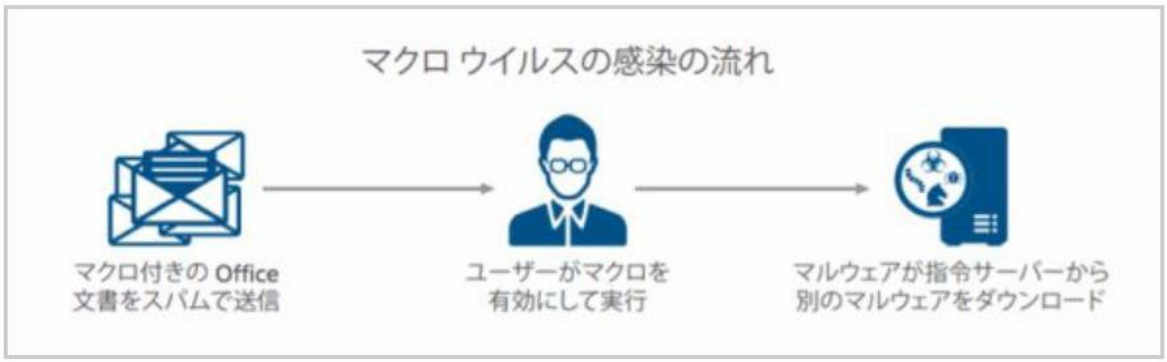
01. Malware の種類と特徴

◆ 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

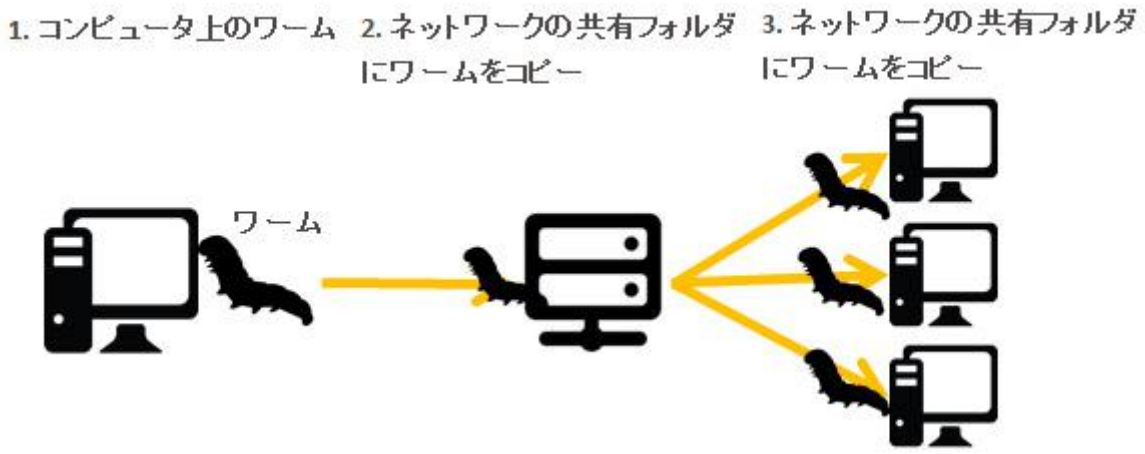


◆ Worm

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】

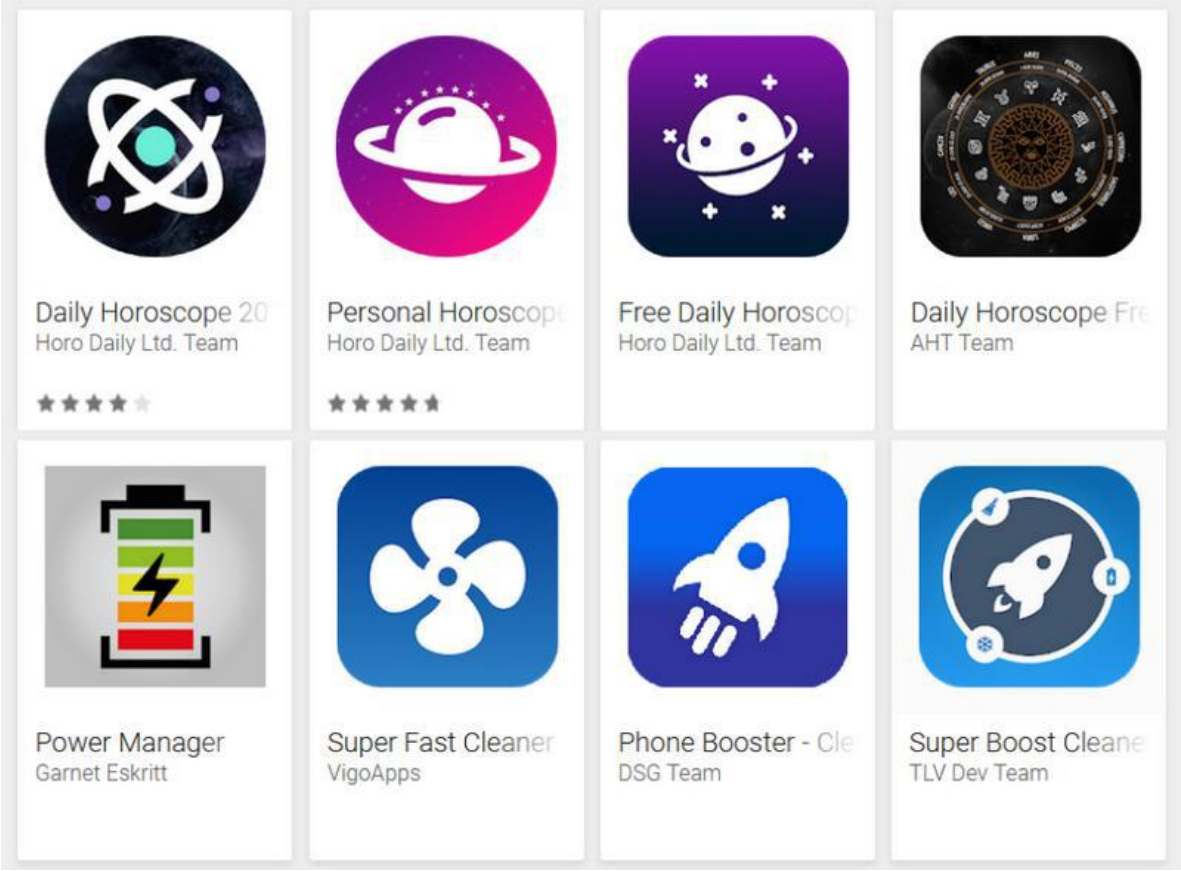
共有フォルダ経由での感染拡大



◆ 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

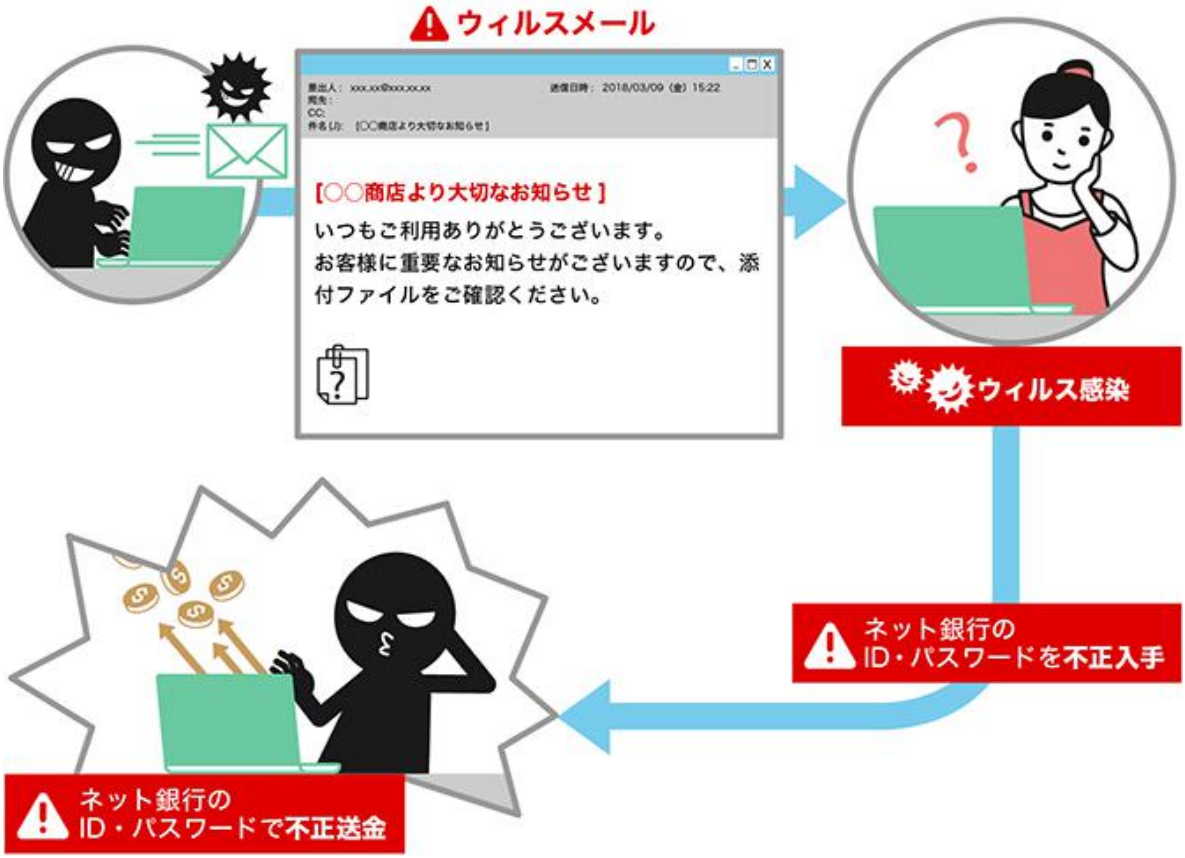


感染方法がギリシャ神話上のトロイの木馬に似ていることに由来する。有用なプログラムであるように見せかけて、パソコン利用者に実行させることで感染。裏で不正な処理を行う。

※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

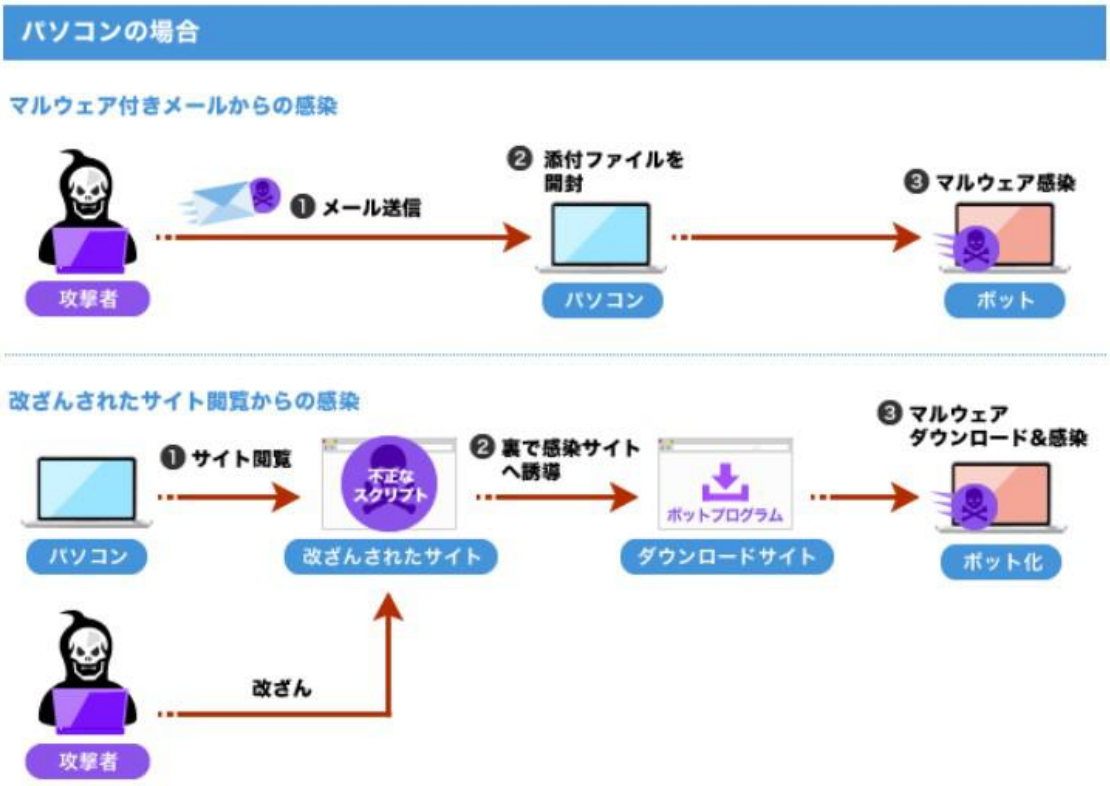
パソコン利用者の個人情報を収集し、外部に送信する。



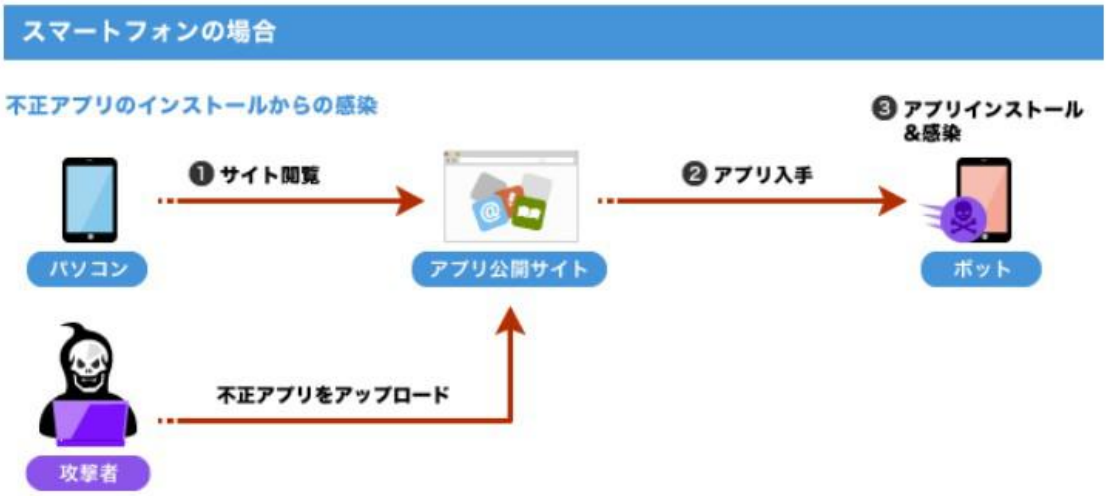
◆ Bot

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**

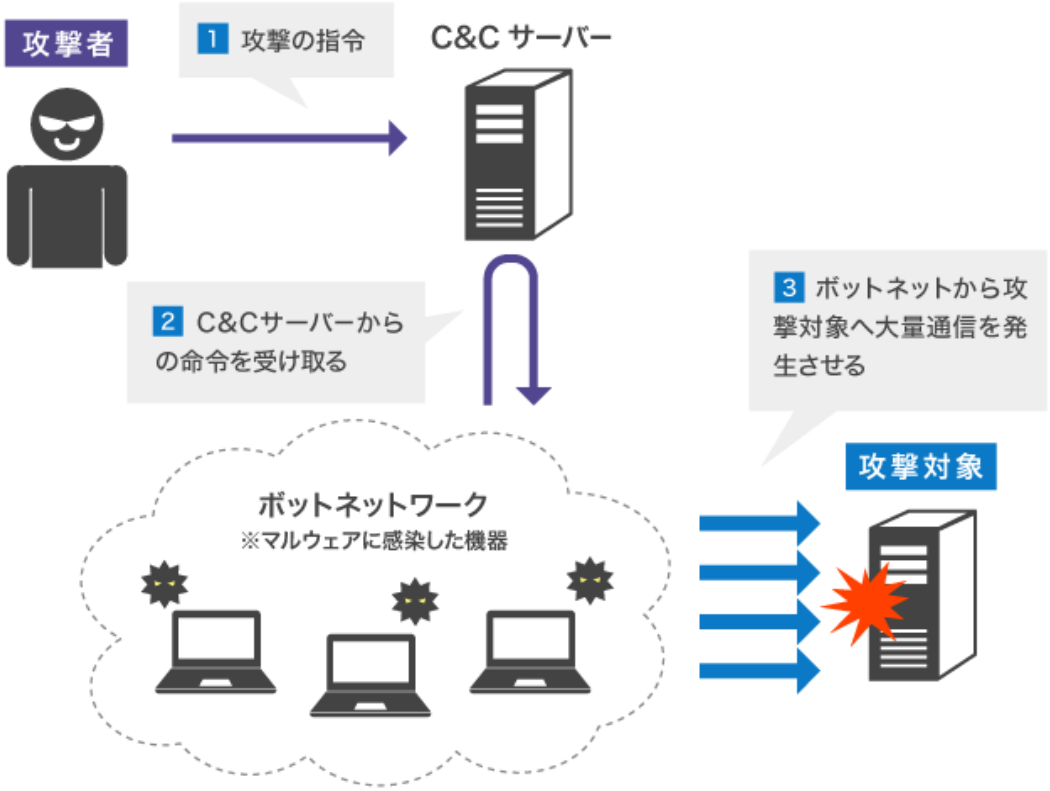


- **スマホがボット化するまでのプロセス**



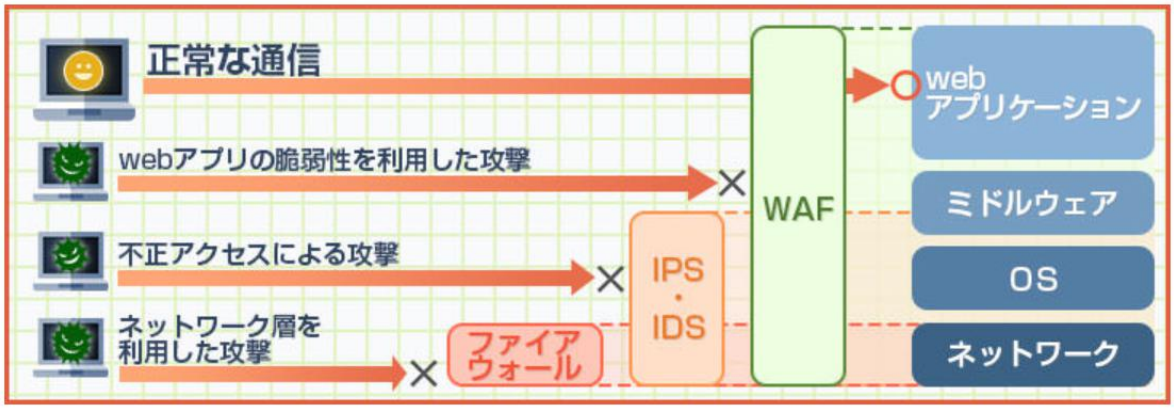
- **Bot の使われ方**

  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。

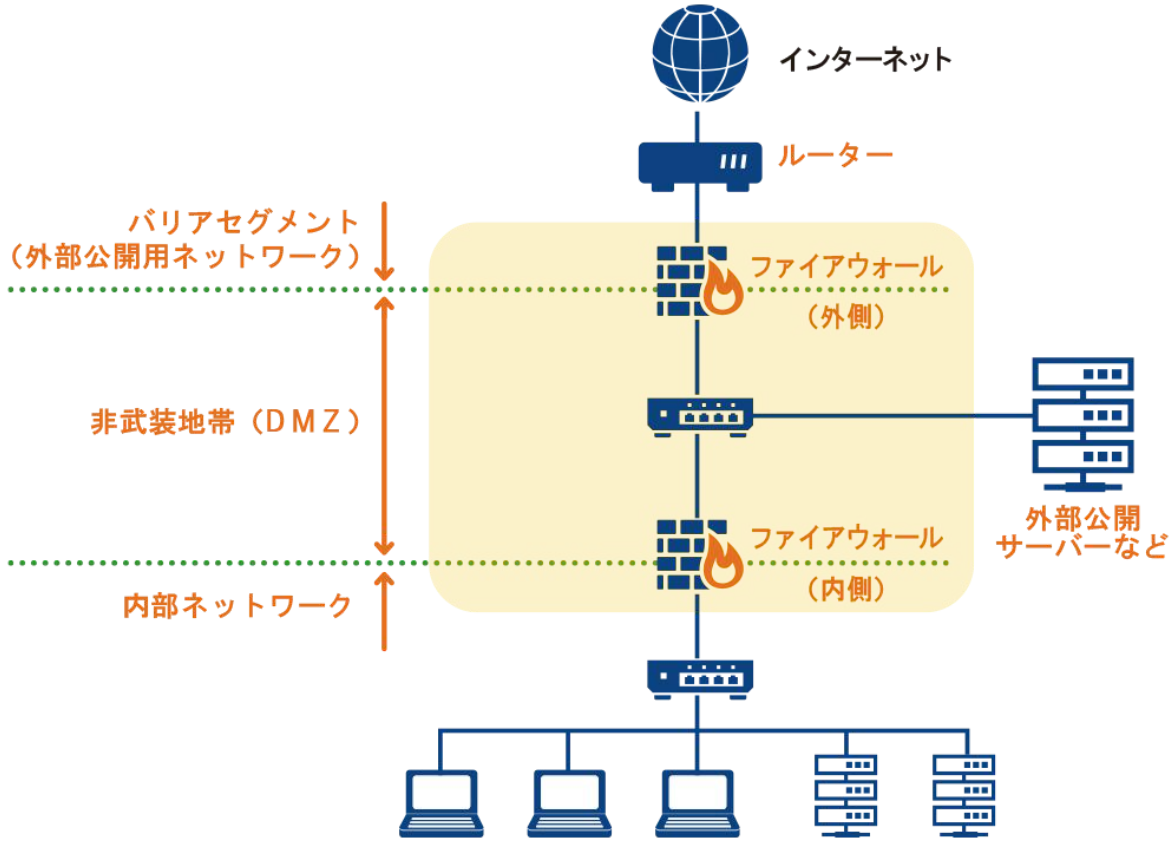


02-01. サイバー攻撃からの防御方法

◆ 防御方法の種類

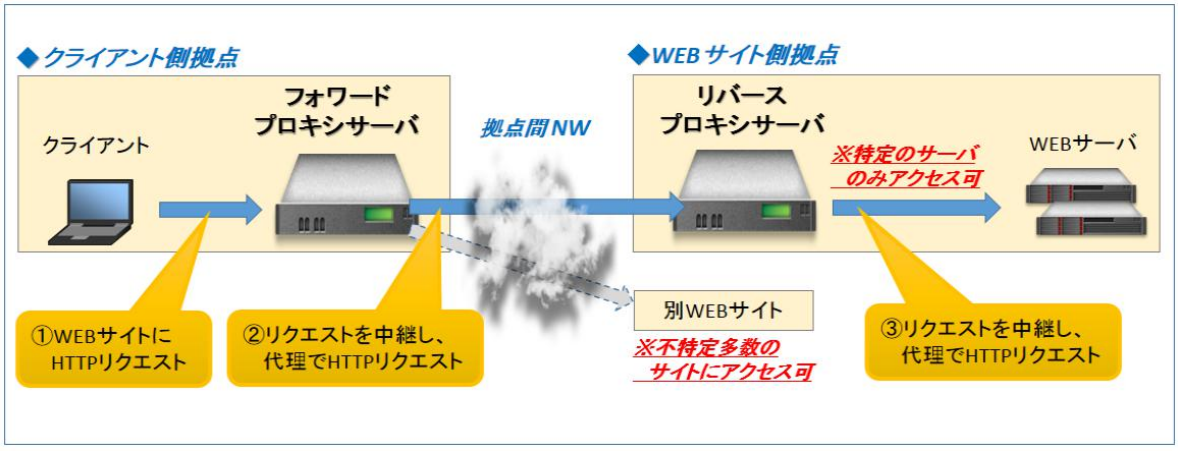


◆ ファイアウォールとは



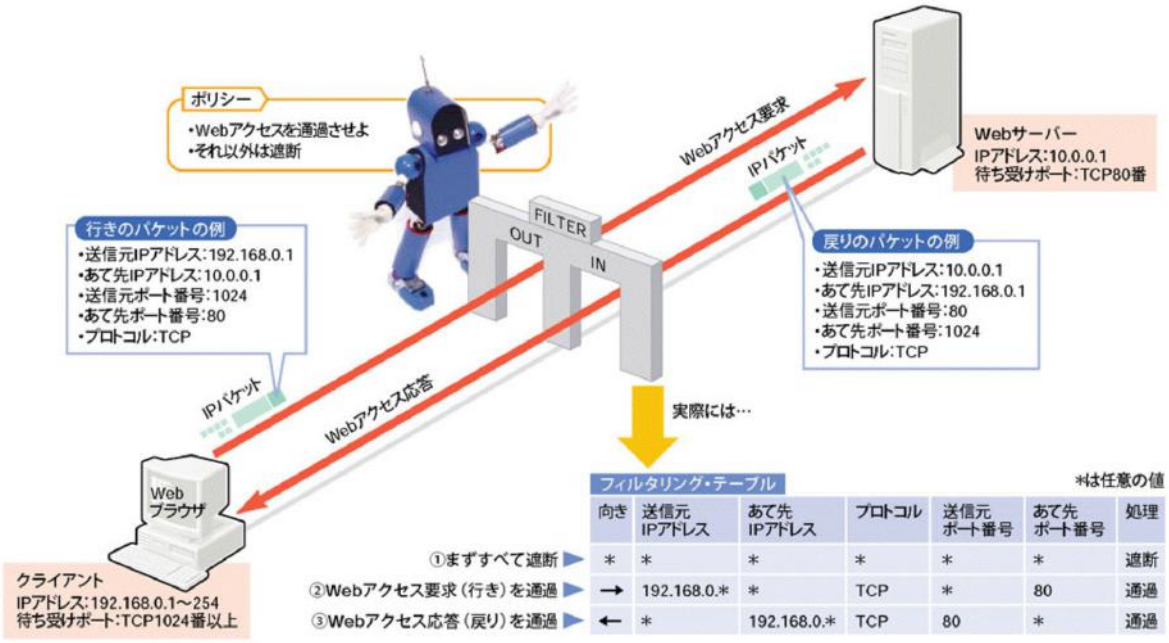
- **アプリケーションゲートウェイ型ファイアウォール（Proxy型）**

Proxyサーバの代理リクエスト機能をファイアウォールとして用いる。Proxyサーバセキュリティ精度を重視する場合はこちら。



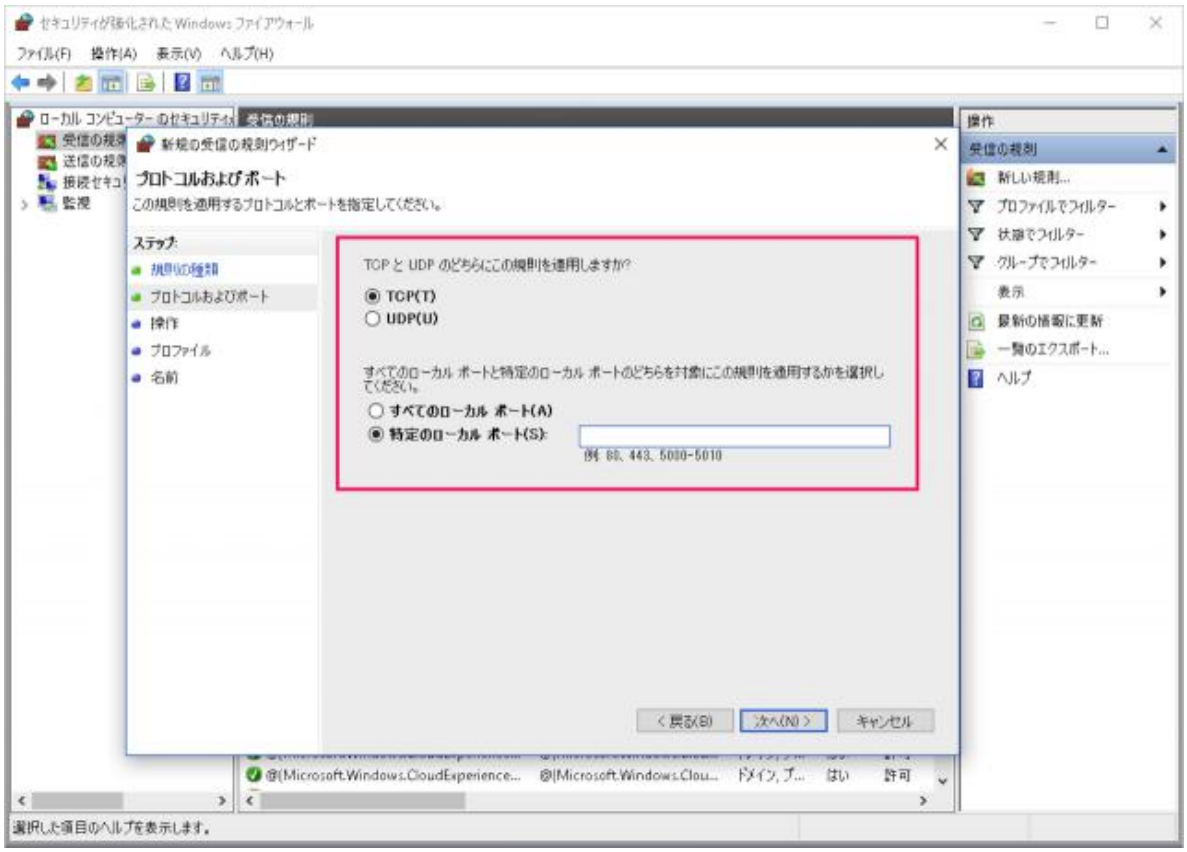
- **パケットフィルタリング型ファイアウォール**

パケットのヘッダ情報に記載された送信元IPアドレスやポート番号などによって、パケットを許可するべきかどうかを決定する。速度を重視する場合はこちら。



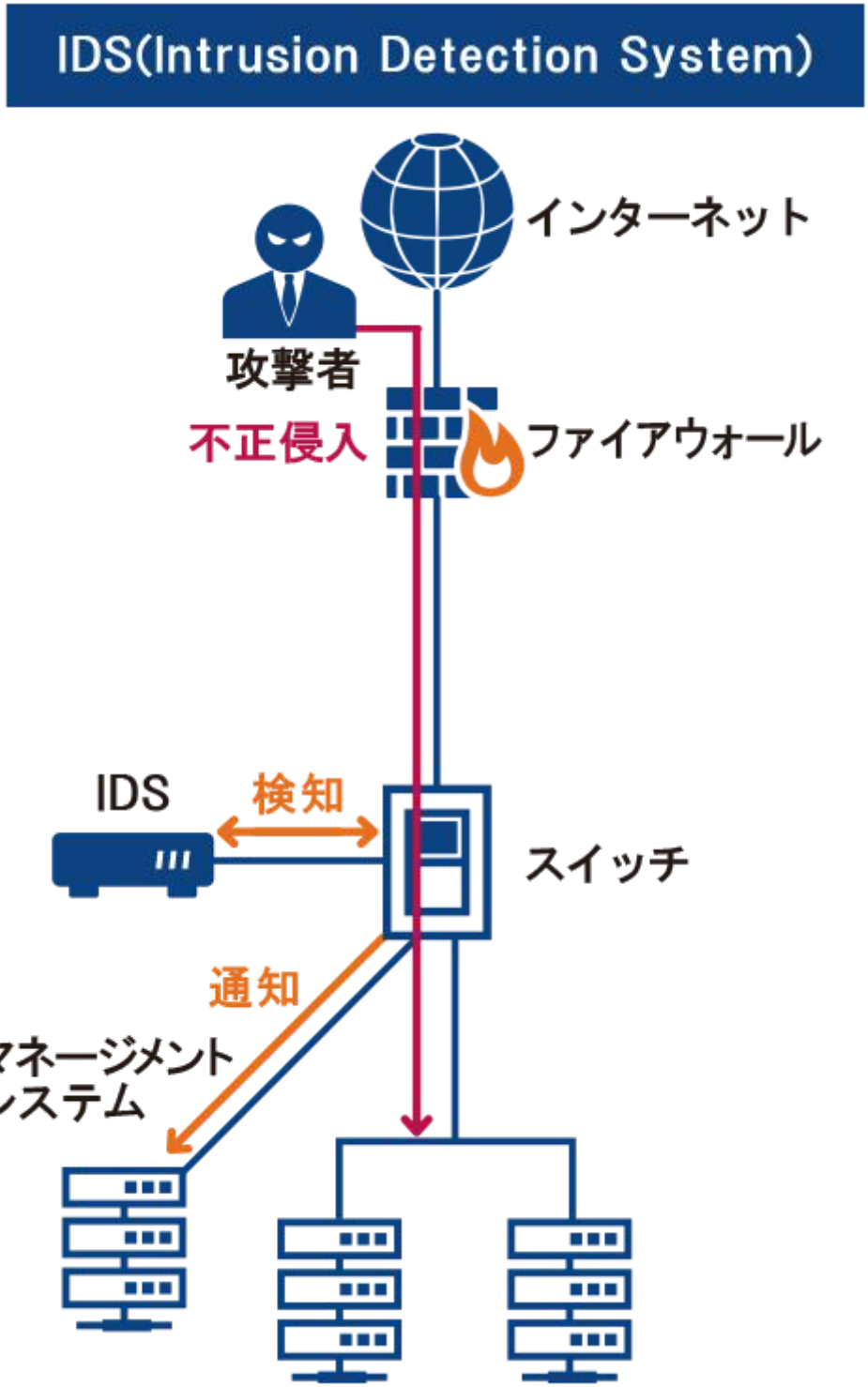
【具体例】

Win10における設定画面



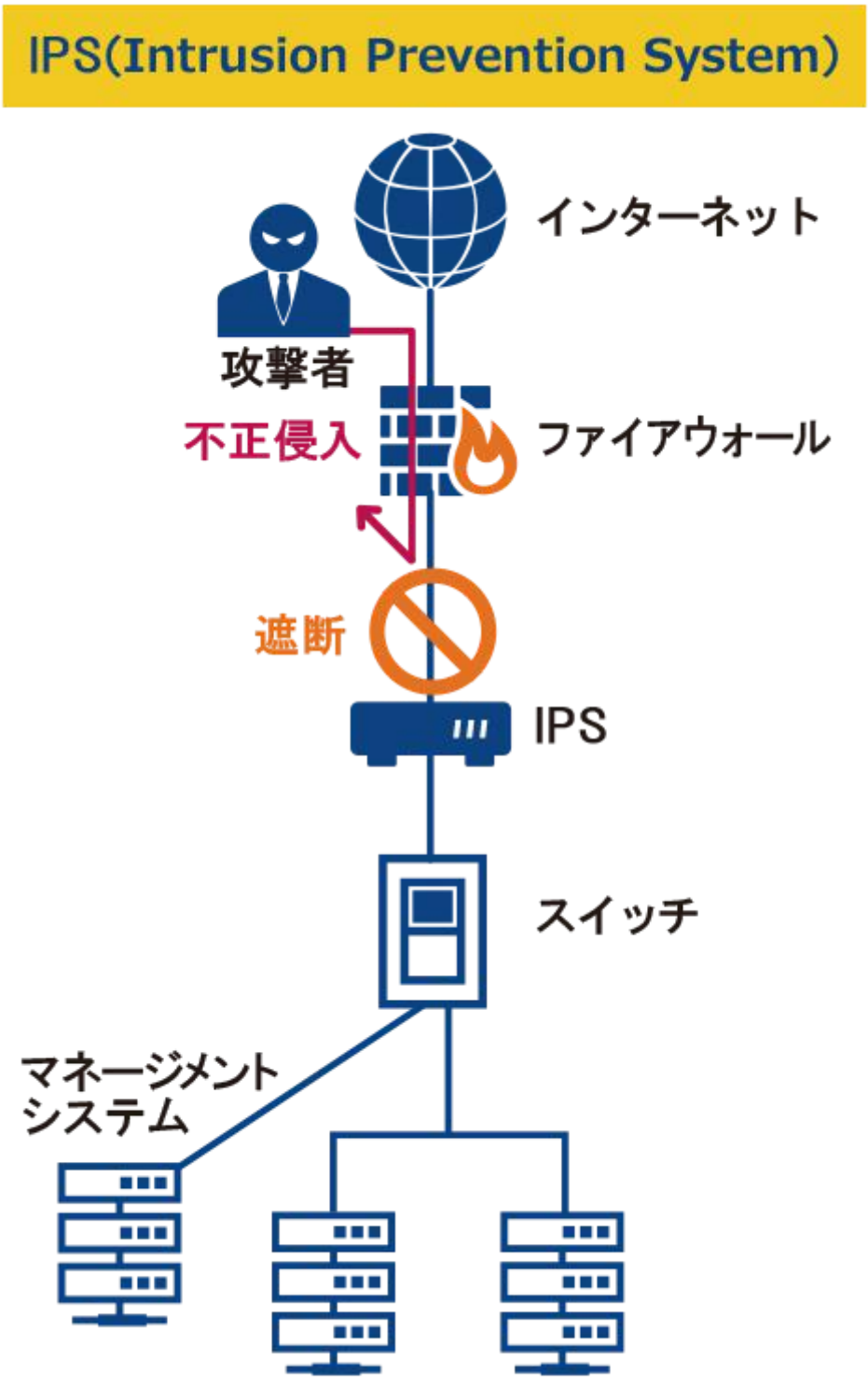
◆ IDS：Instrusion Detection Systemとは

ネットワーク上を流れるトラフィックを監視し、不正アクセスと思われるパケットを検出した時に、管理者に通知するシステム。あくまで通知するだけで、攻撃を防御することはしない。



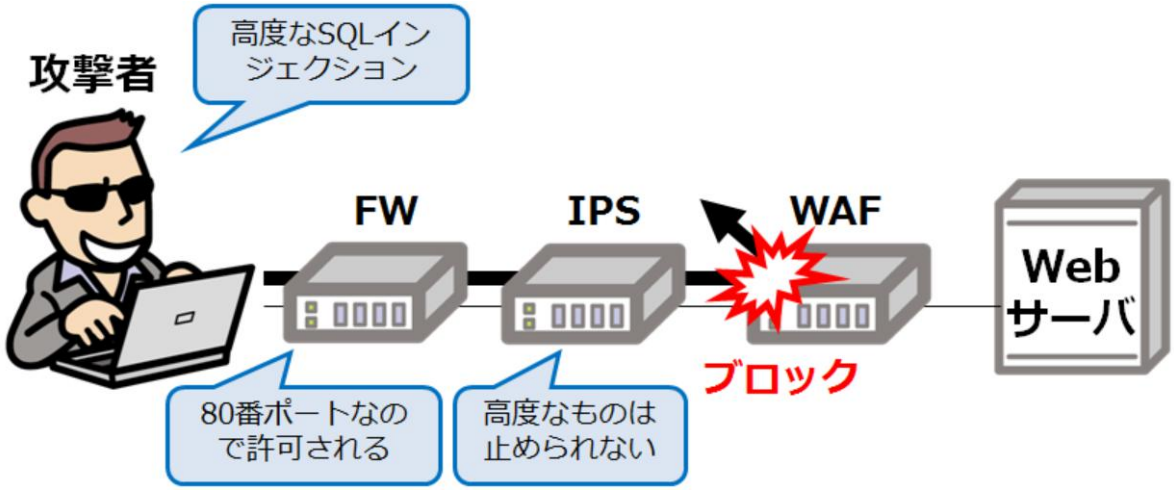
◆ IPS：Intrusion Prevention Systemとは

ネットワーク上を流れるトラフィックを監視し、不正アクセスと思われるパケットを検出した時に、管理者に通知し、さらにパケットの侵入を防ぐシステム。



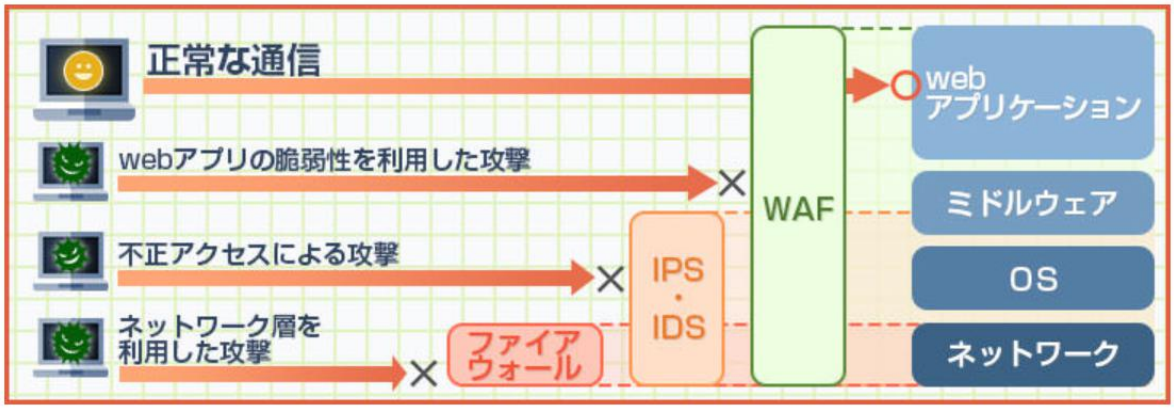
◆ WAF：Web Application Firewallとは

Webアプリケーション自体を保護するシステム。



02-02. IPS・IDSで防御可能なサイバー攻撃

◆ 防御方法の種類（再掲）

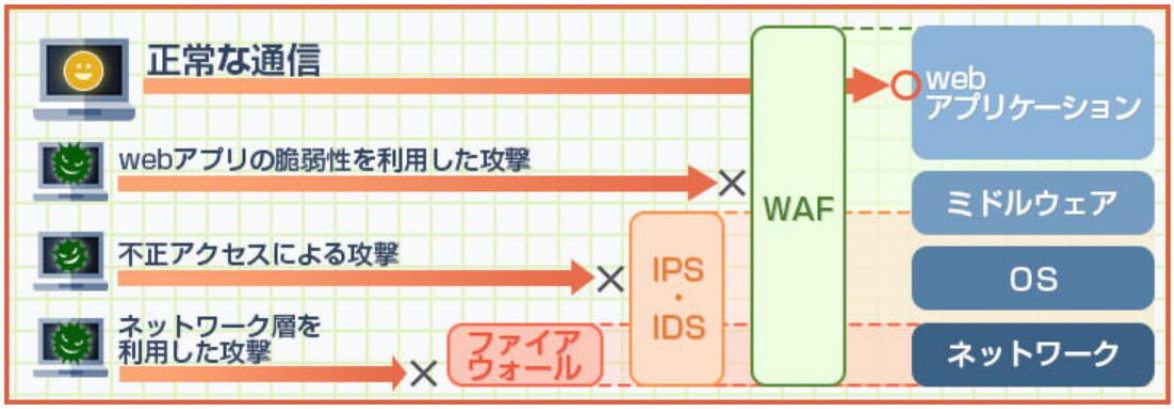


◆ DoS攻撃：Denial of Service

アクセスが集中することでWebサーバーがパンクすることを利用し、悪意を持ってWebサーバーに大量のデータを送りつける手法。

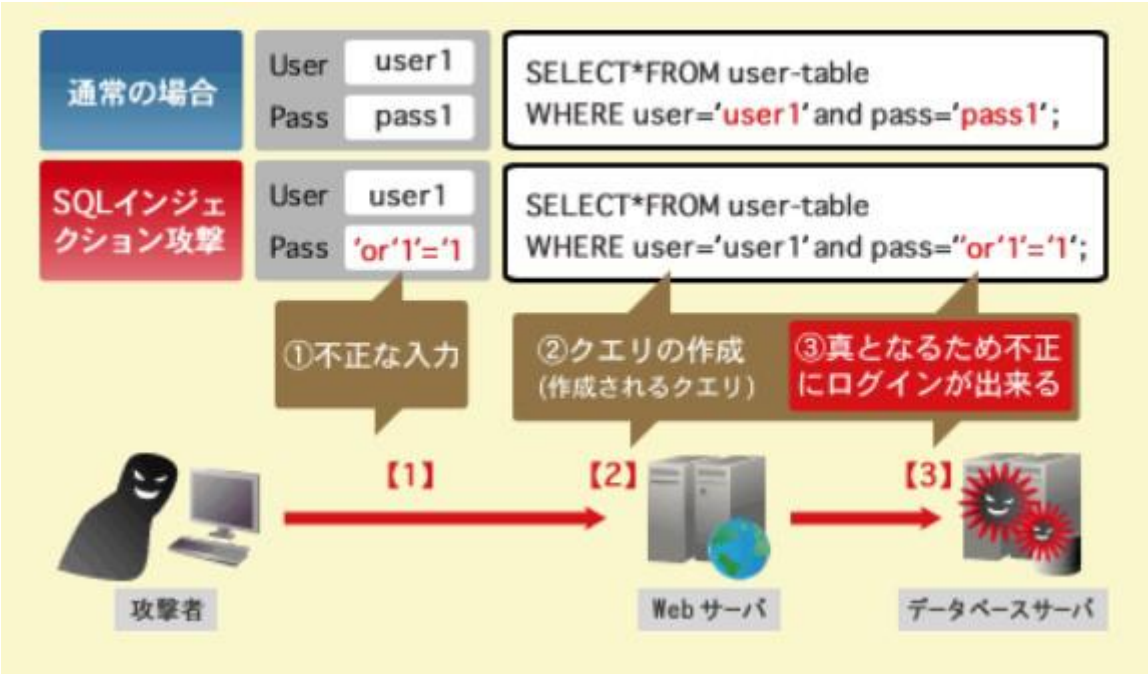
02-03. WAFで防御可能なサイバー攻撃

◆ 防御方法の種類（再掲）



◆ 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。

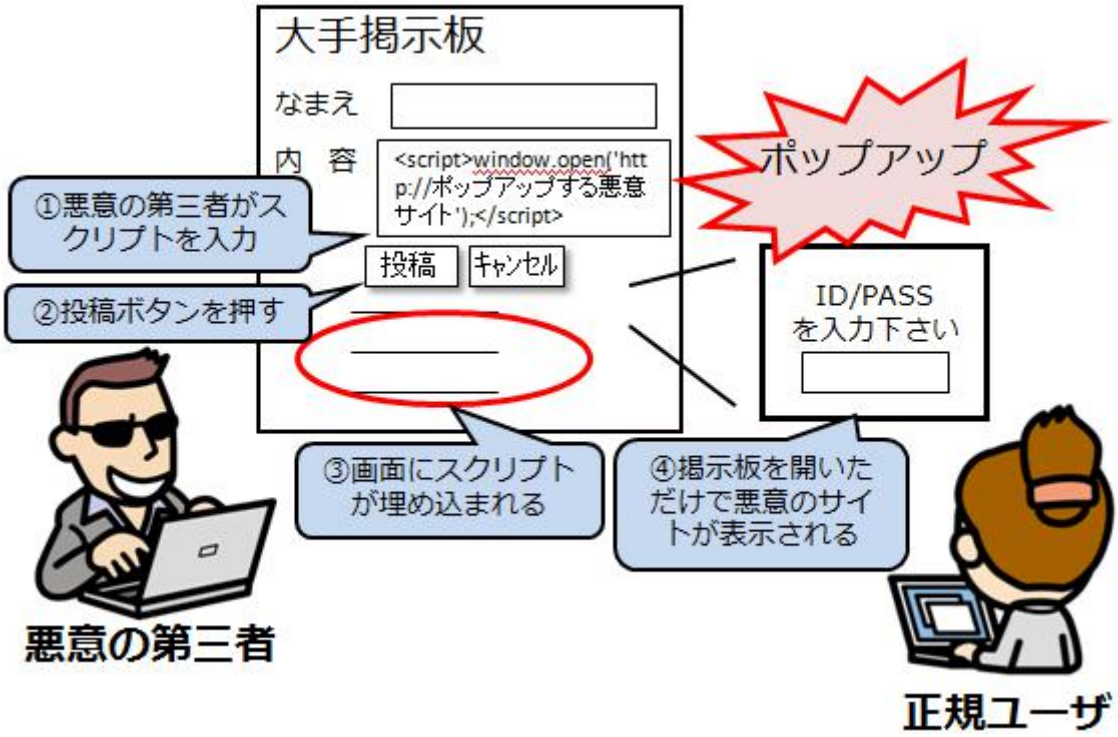


- **対策**

  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、『シングルクオーテーション』や『バックスラッシュ』を無効化させる。

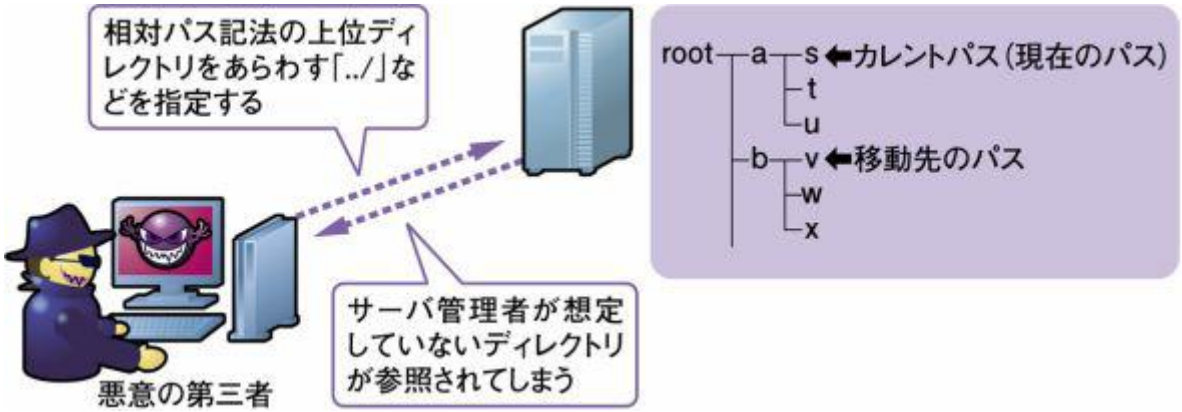
◆ XSS：Cross Site Scripting

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

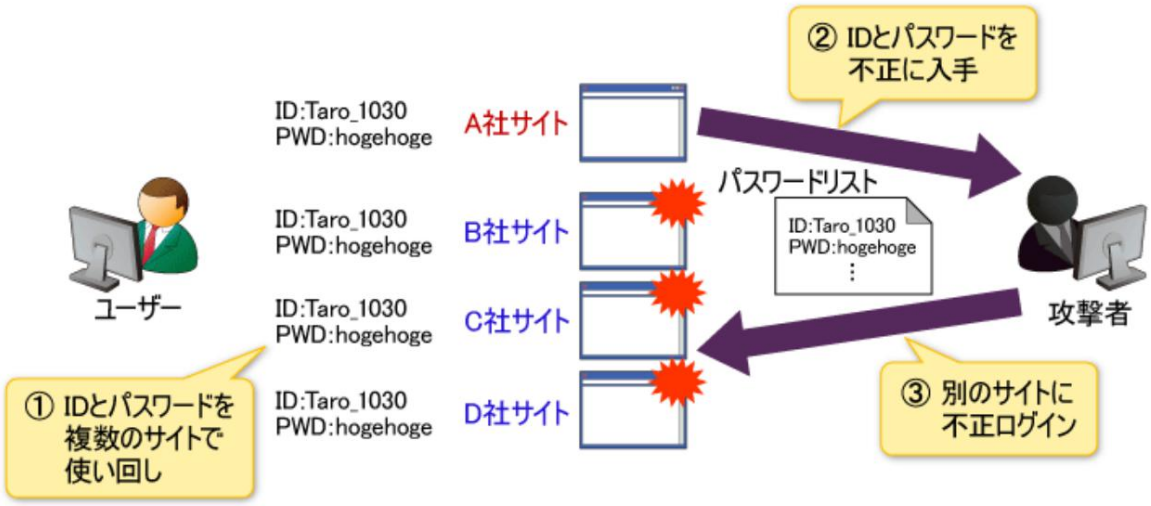
パス名を使ってファイルを指定し，管理者の意図していないファイルを不正に閲覧する。



02-04. パスワードに関するサイバー攻撃

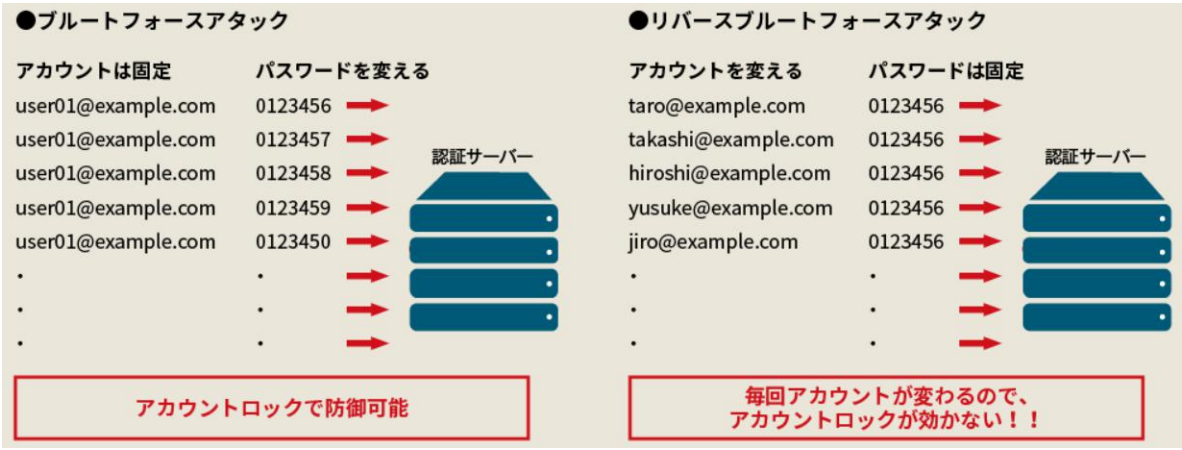
◆ パスワードリスト攻撃

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攻撃とReverse 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。一方で、Reverse Brute-forceは、パスワードを固定して、IDを総当たりで試す手法。



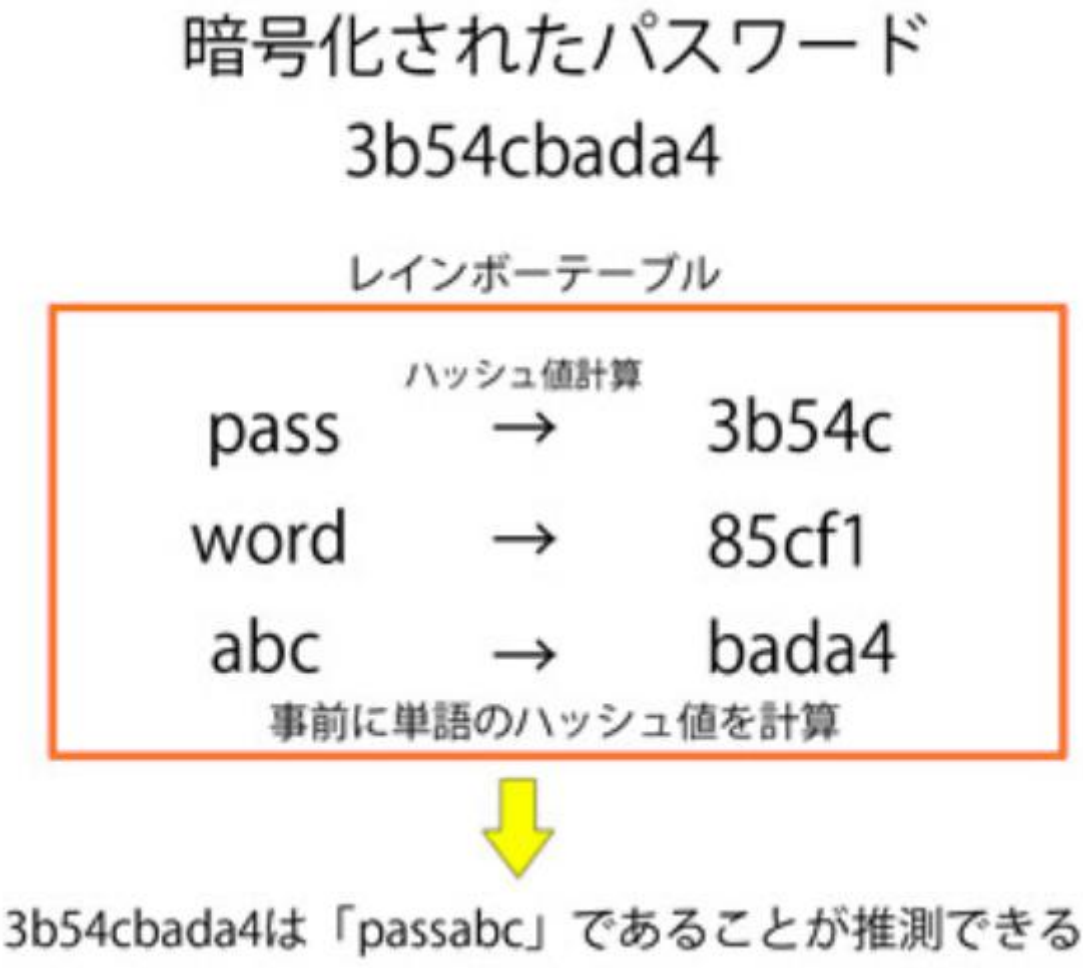
- **パスワードのパターン数**

●数字・英字・記号等を組み合わせたパスワードのパターン数

	4 桁	6 桁	8 桁
数字のみ（10）	1 万通り	100 万通り	1 億通り
数字＋英字（36）	約 170 万通り	約 22 億通り	約 2 兆 8,000 億通り
数字＋英大文字・小文字（62）	約 1,500 万通り	約 570 億通り	約 220 兆通り
数字＋英大文字・小文字＋記号（62 ＋ 32）	約 7,800 万通り	約 6,900 億通り	約 6,100 兆通り

◆ Rainbow 攻撃

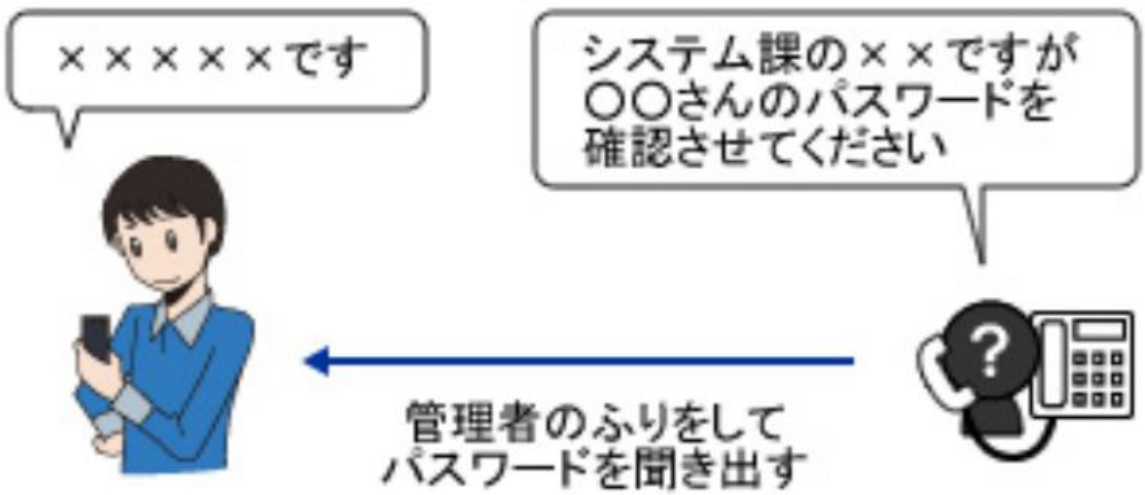
ハッシュ化された暗号から、元のパスワードを解析する手法。



02-05. その他のサイバー攻撃

◆ ソーシャルエンジニアリング

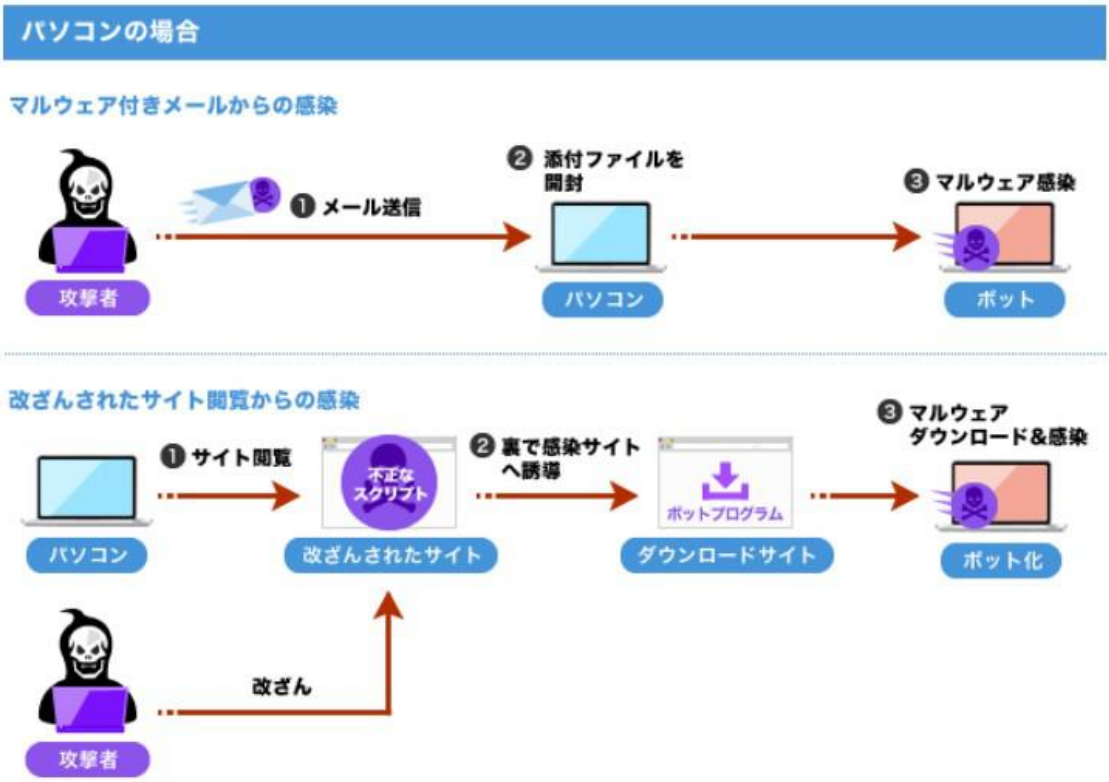
技術的な手法ではなく、成りすましや詐欺によってパスワードを取得し、アクセスする手法。



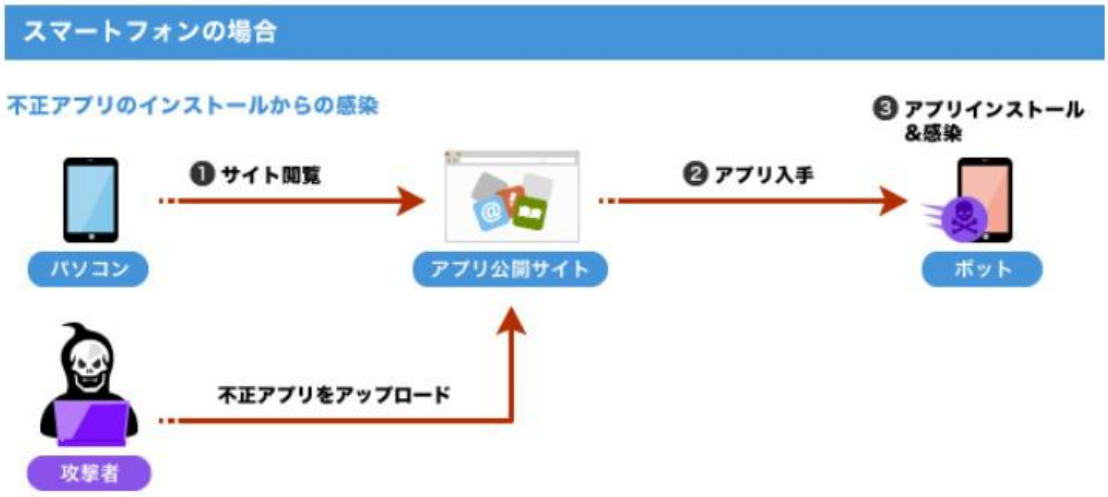
◆ 踏み台攻撃

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）

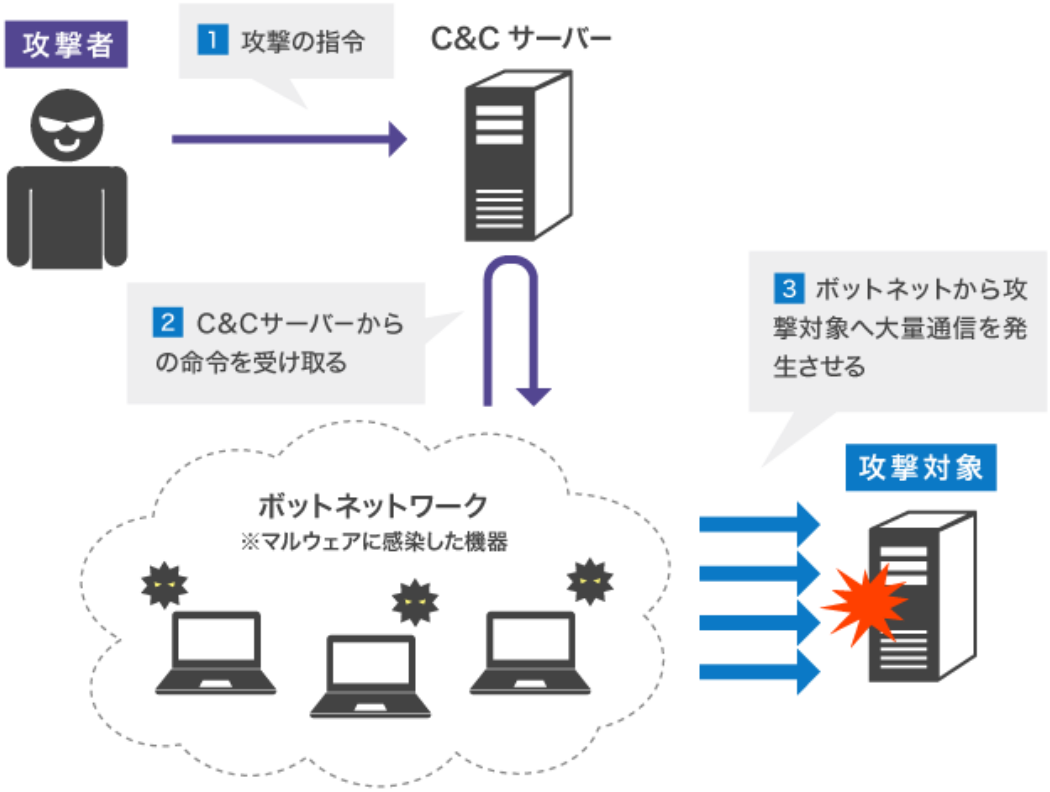
- パソコンがボット化するまでのプロセス（再掲）



- スマホがボット化するまでのプロセス（再掲）

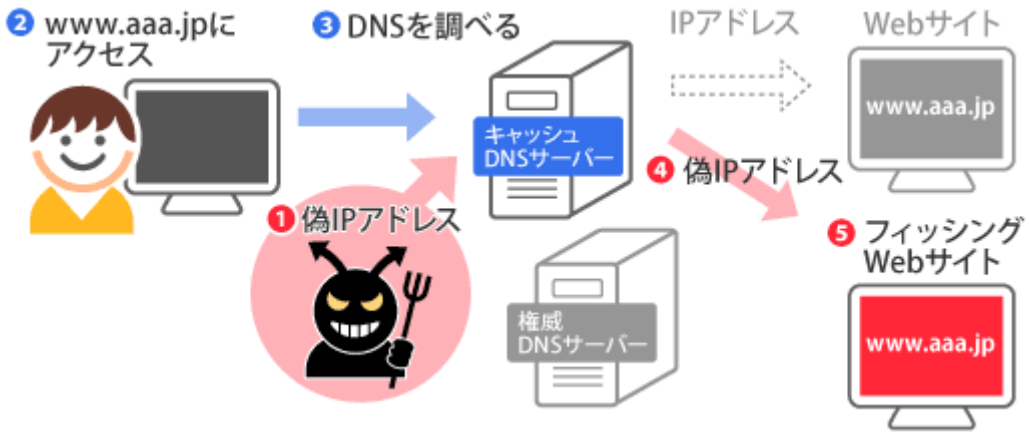


- Bot の使われ方（再掲）



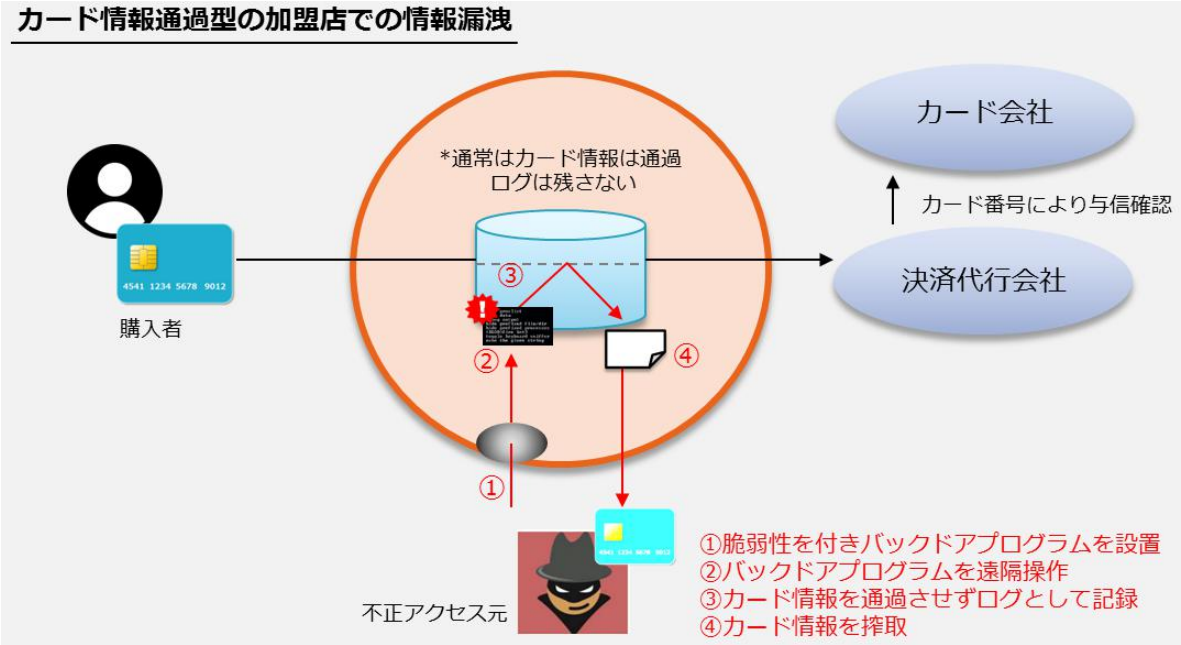
◆ DNS Cache Poisoning

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。



◆ 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。



03-01. 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**

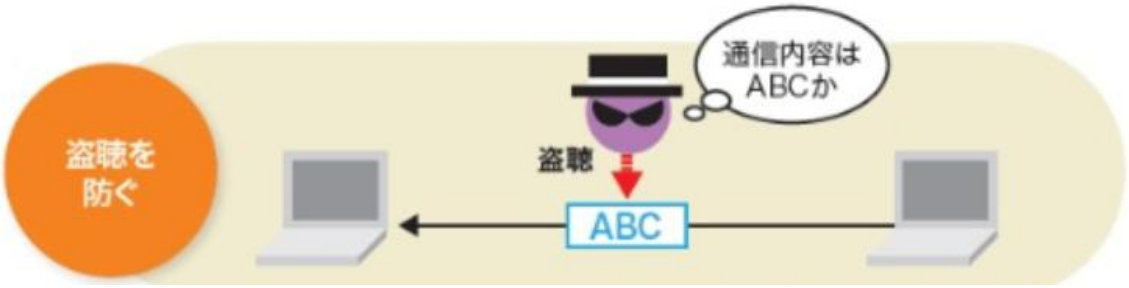
◆ 公開鍵暗号アルゴリズム

- **RSA 暗号：Rivest-Shamir-Adleman cryptosystem**

03-02. データ通信セキュリティの役割

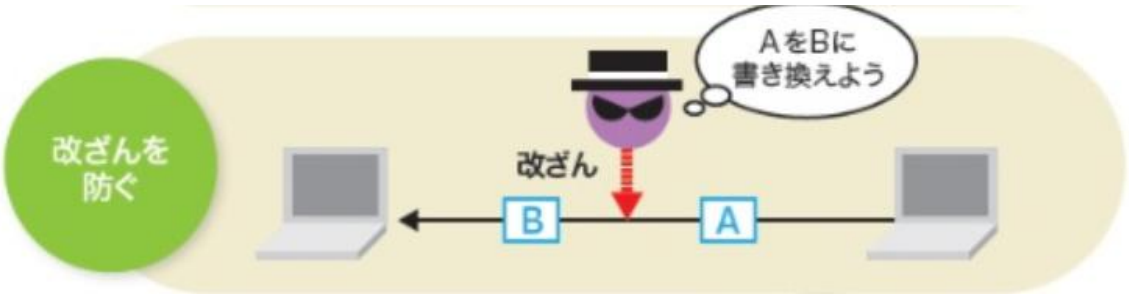
◆ 盗聴（データの盗み取り）を防ぐ

『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。



◆ 成りすましを防ぐ

『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、成りすましを防ぐ。

03-03. 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

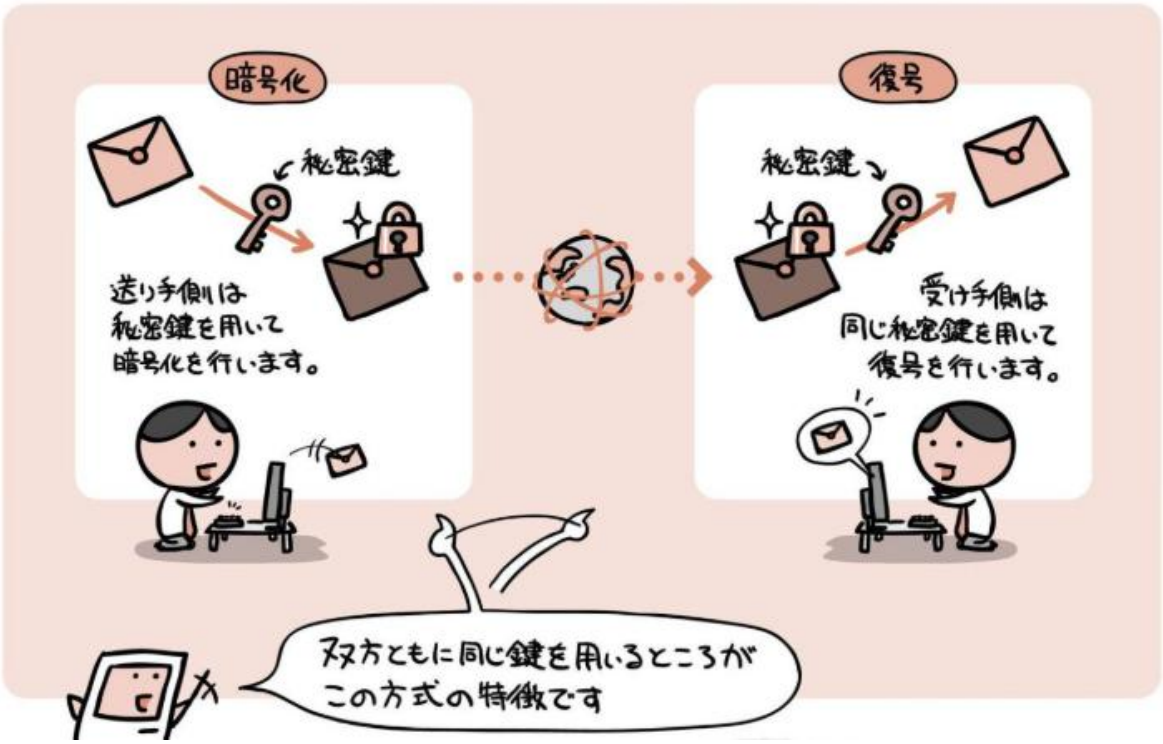
送信者にあらかじめ秘密鍵を渡しておく。鍵の受け渡しを工夫しないと、共通鍵が傍受され悪用される可能性がある（**鍵配送問題**）。

【具体例】

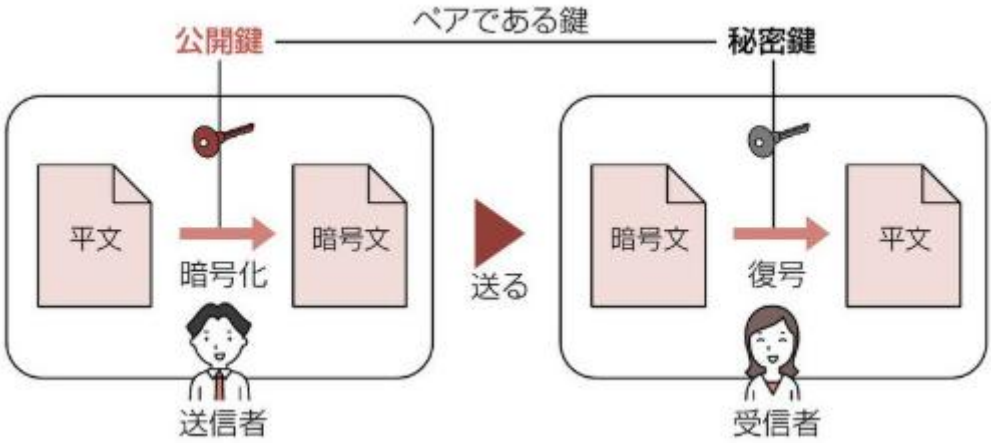
エクセルのファイルロック

長所：処理が速い

短所：鍵の配布が大変



◆ 公開鍵暗号方式



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。

【送信者が行うこと】

1. 送信者は、受信者から公開鍵をもらう。
2. 公開鍵を用いて、情報を暗号化する。

【受信者が行うこと】

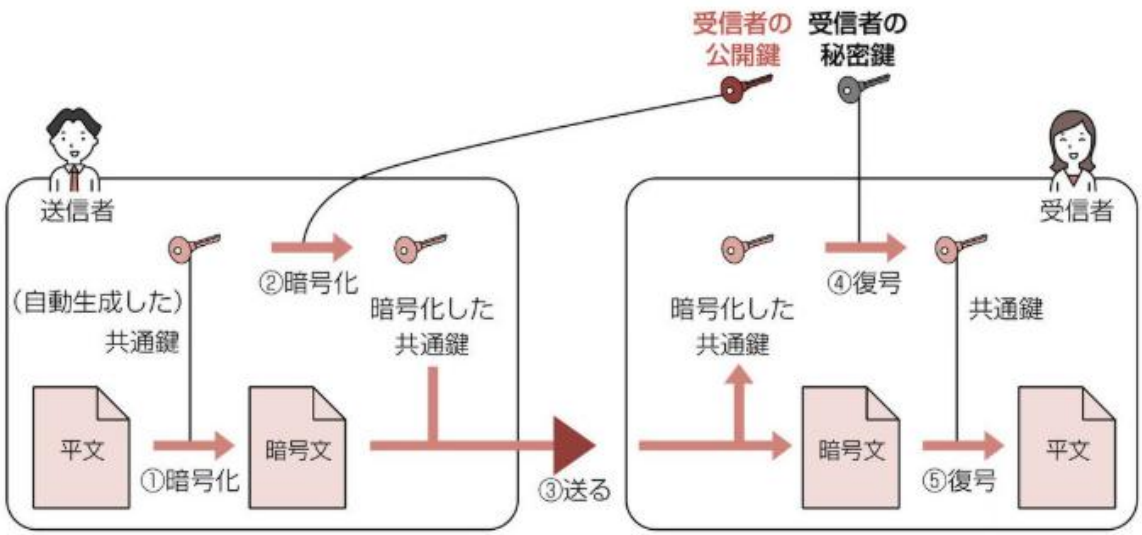
1. 受信者は、秘密鍵で情報を復号する。

- **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。



03-04. 暗号ダイジェスト（デジタル署名）を用いたセキュリティ

◆ 暗号ダイジェスト（デジタル署名）を用いたセキュリティの仕組み

『公開鍵暗号方式とは逆の仕組み（※つまり、公開鍵暗号方式ではない）』と『ハッシュ関数』を利用したセキュリティ技術。『成りすまし』と『改竄』を防ぐことができる。

【送信者が行うこと】

1. 送信者は、受信者にあらかじめ公開鍵を配布しておく。
2. 平文をハッシュ化し、ダイジェストにする。
3. 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。
4. 『平文』と『暗号ダイジェスト（デジタル署名）』の両方を送信

【受信者が行うこと】

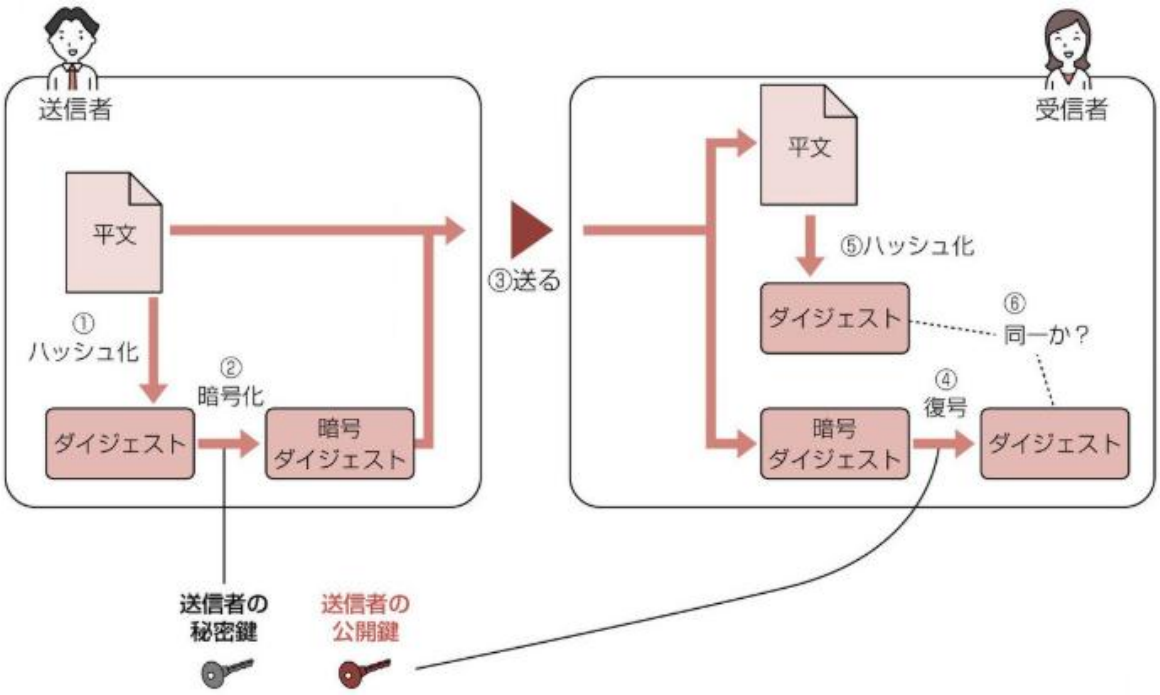
1. 受信者は、『平文』と『暗号ダイジェスト（デジタル署名）』の両方を受信し、暗号ダイジェストを公開鍵（署名検証鍵）で復号し、ダイジェストにする。
2. 平文をハッシュ化し、ダイジェストにする。
3. 上記２つのダイジェストが同一なら、『成りすまし』と『改竄』が行われていないと判断

- **成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。

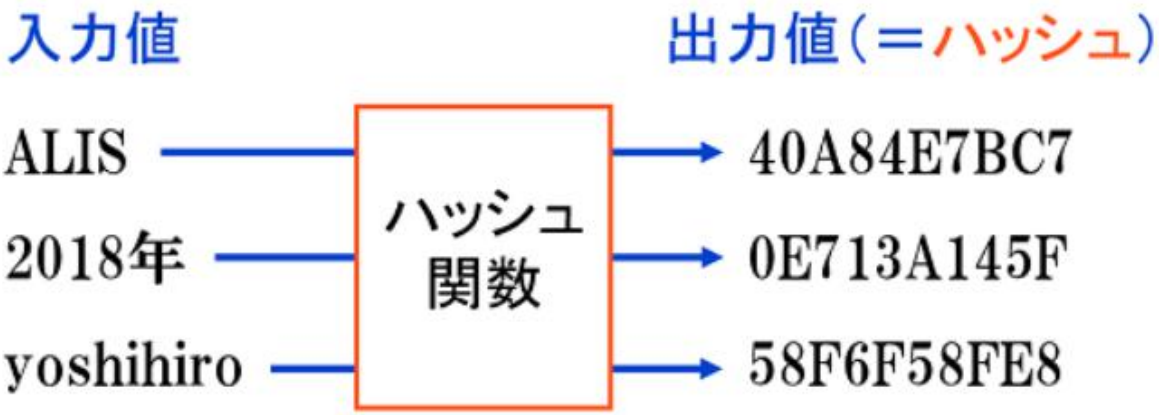
- **改竄を防ぐことができる**

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。



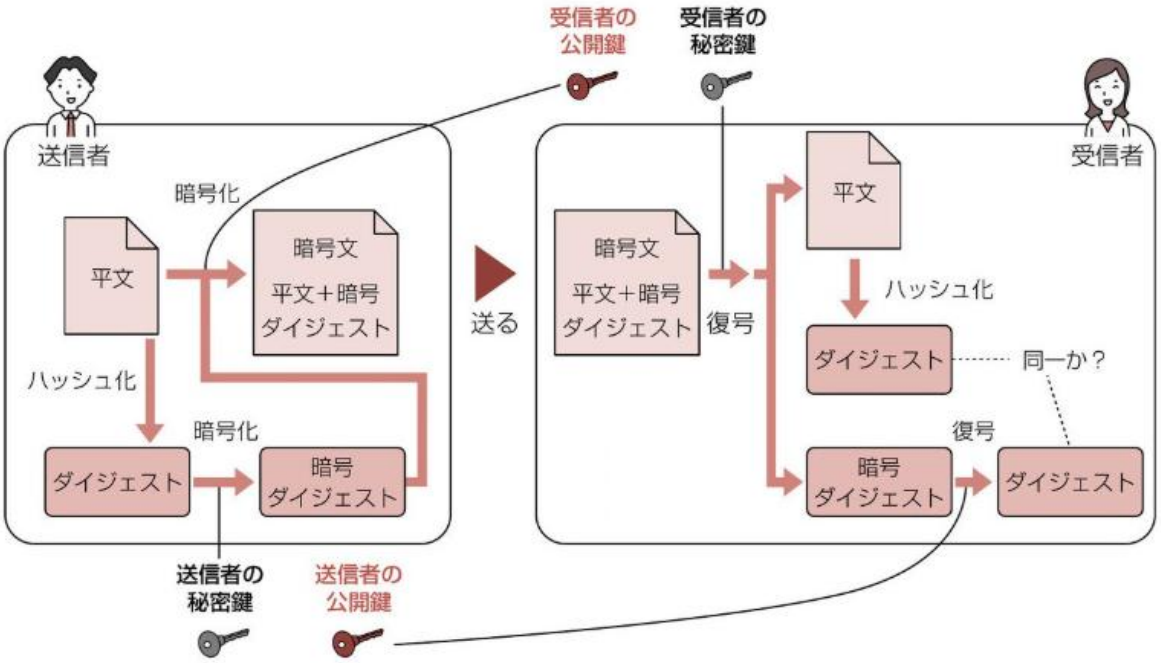
- **ハッシュ関数**

  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。



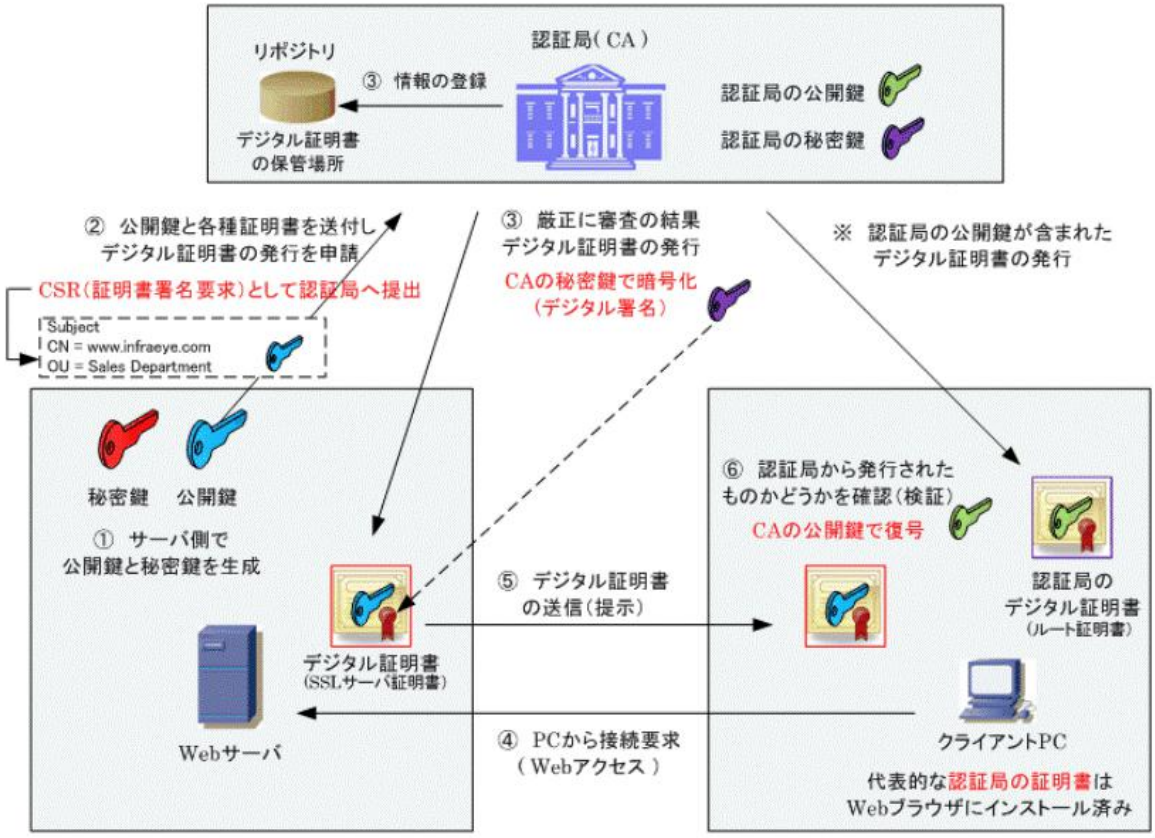
◆ 暗号ダイジェスト（デジタル署名）と公開鍵暗号方式を用いたセキュリティの仕組み

『成りすまし』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）による署名検証鍵の検証

デジタル署名に用いた秘密鍵に対応する公開鍵（署名検証鍵）は、成りすました人物による偽の公開鍵である可能性がある。第三者機関の認証局によって、公開鍵（署名検証鍵）を検証するインフラのことを、公開鍵基盤という。



【送信者が行うこと】

1. 送信者は、公開鍵（署名検証鍵）と秘密鍵を作り、認証局に公開鍵（署名検証鍵）とデジタル署名を提出。

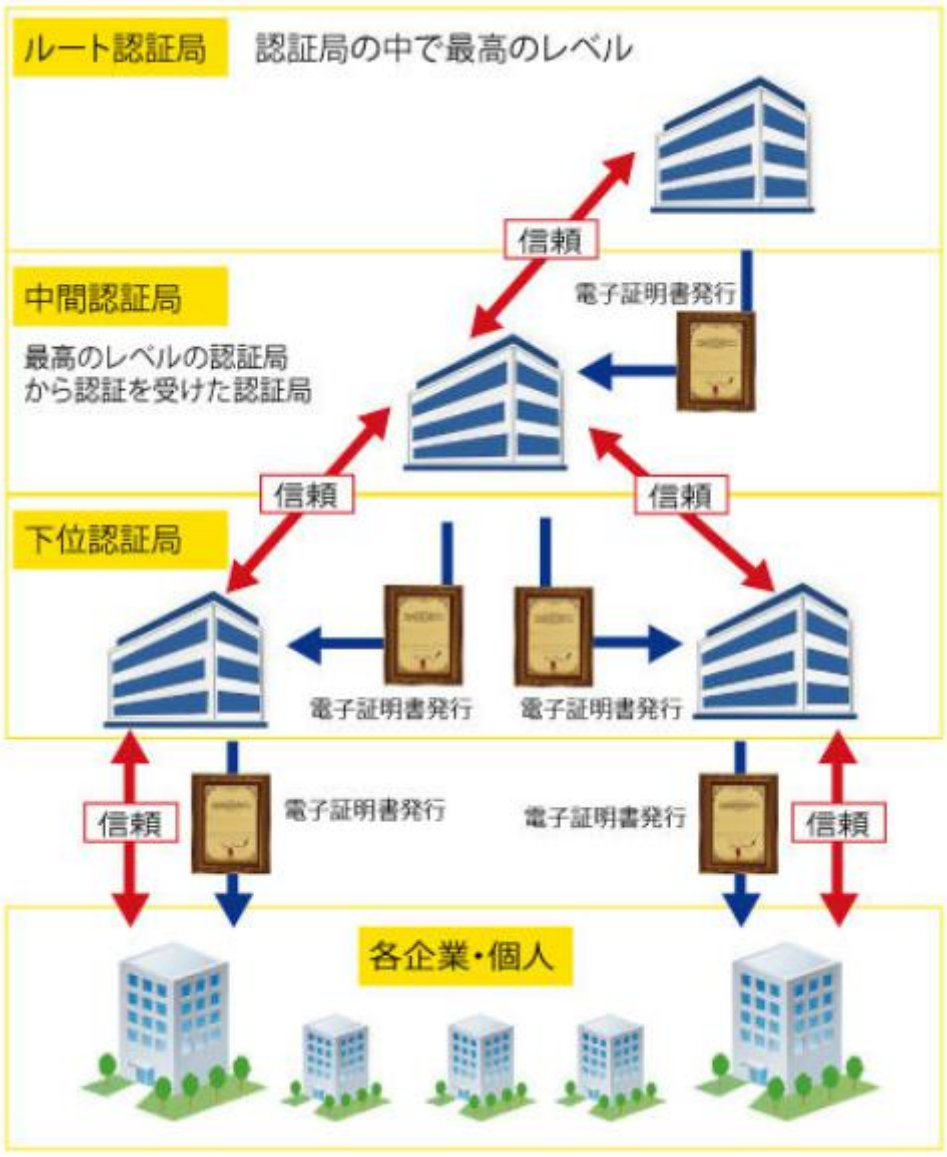
2. 認証局から、暗号ダイジェスト（デジタル署名）を含むデジタル証明書（SSLサーバ証明書）を発行してもらう。デジタル証明書（SSLサーバ証明書）が、公開鍵（署名検証鍵）の本人証明になる。
3. 受信者にメール、暗号ダイジェスト（デジタル署名）の含むデジタル証明書（SSLサーバ証明書）を送信。

【送信者が行うこと】

1. 受信者は、暗号ダイジェスト（デジタル署名）を含むデジタル証明書（SSLサーバ証明書）を受信。
2. 認証局からもらった公開鍵を用いて、デジタル証明書（SSLサーバ証明書）の暗号ダイジェスト（デジタル署名）部分を復号し、ハッシュ値が同じなら、認証局そのものが成りすましでないと判断する。

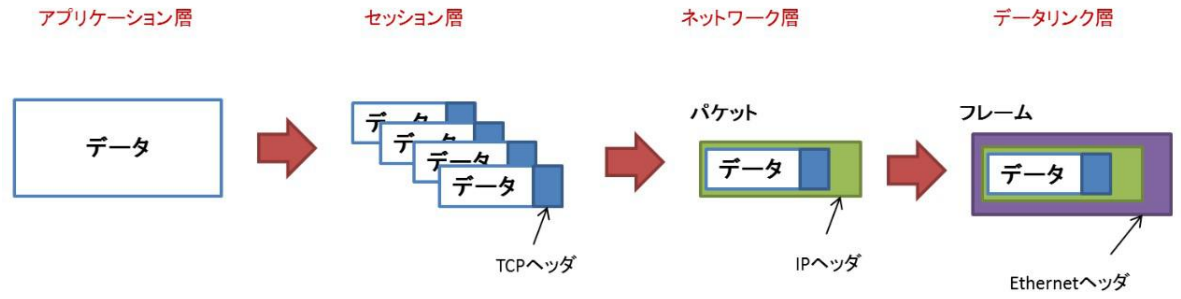
- **認証局そのものの成りすましの防止策**

デジタル証明書（SSLサーバ証明書）を発行する認証局そのものが、成りすましの可能性がある。そこで、認証局をランク付けし、ルート認証局が下位ランクの認証局に権限を与えることで、下位の認証局の信頼性を持たせている。なお、ルート認証局は専門機関から厳しい審査を受けているため、ルート認証局自体がなりすましである可能性は非常に低い。

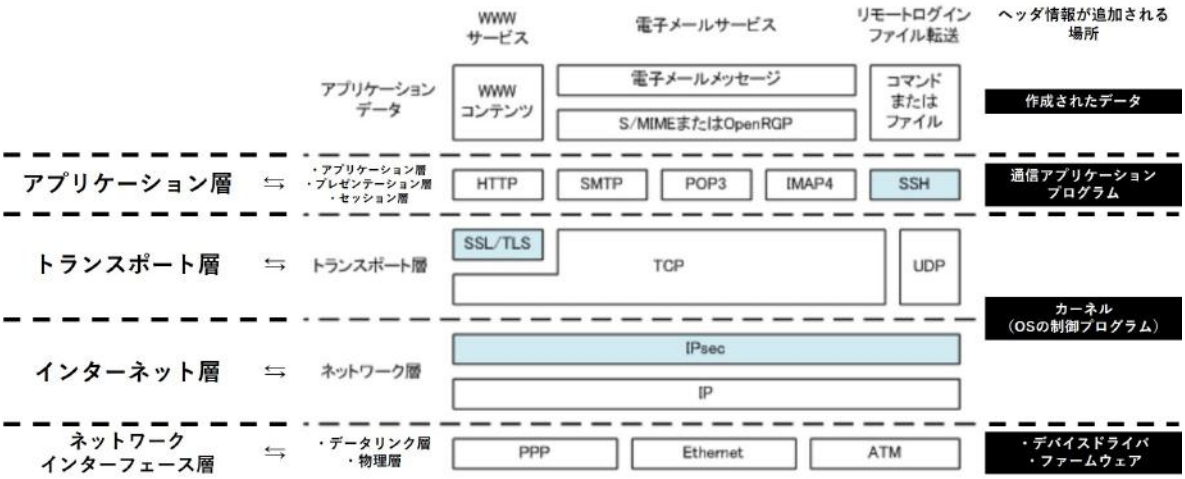


04-01. パケット交換方式におけるセキュリティ

◆ データへのヘッダ情報追加とカプセル化（再掲）



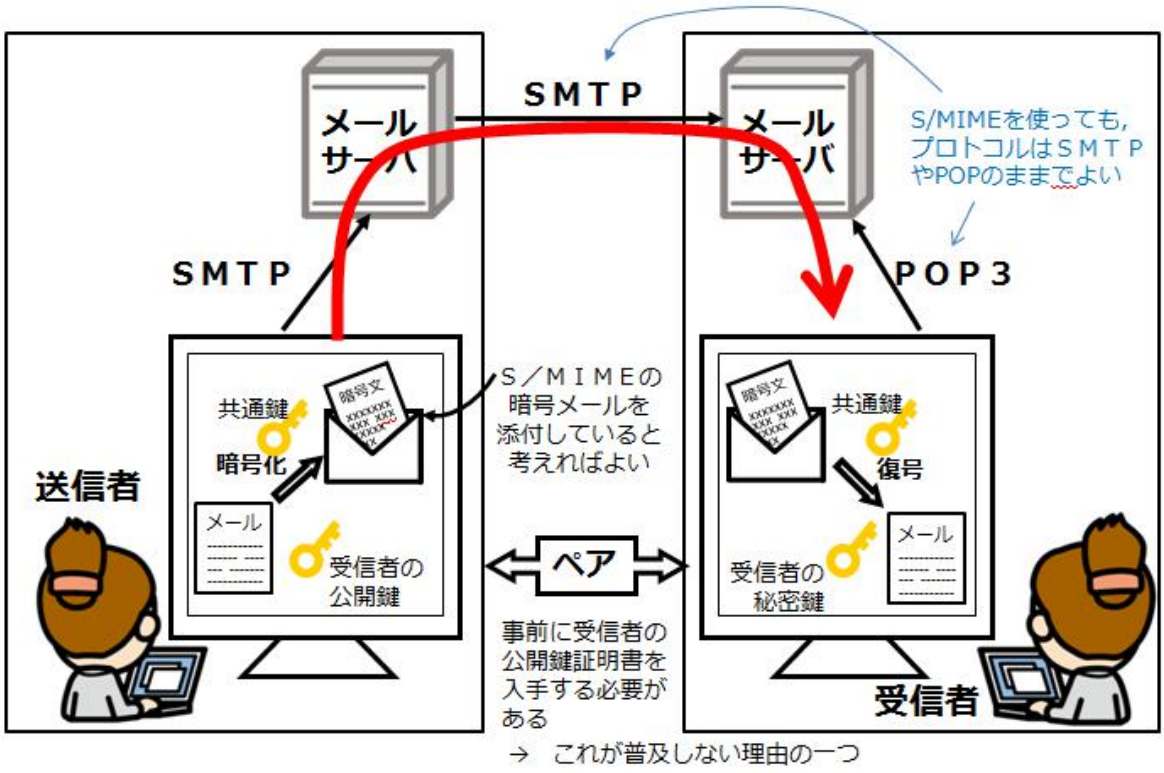
◆ ヘッダ情報追加プロトコルの分類と追加される場所（再掲）



04-02. アプリケーションデータのセキュリティ技術

◆ S/MIME：Secure MIME

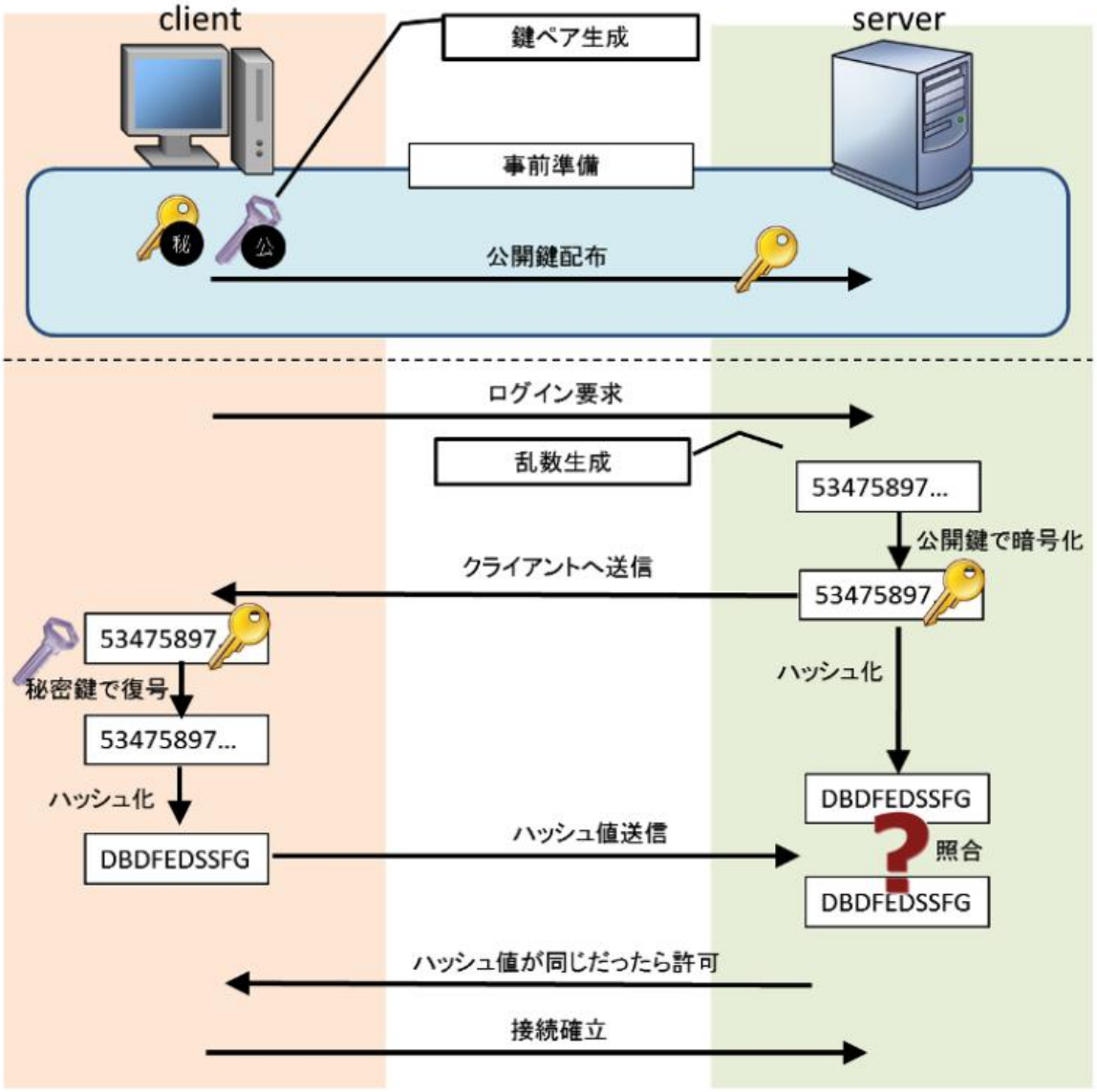
公開鍵暗号方式に基づく技術。アプリにおいて、デジタル署名による認証の機能を、メールに追加することができる。



04-03. アプリケーション層のセキュアプロトコル

◆ SSH：Secure Shell

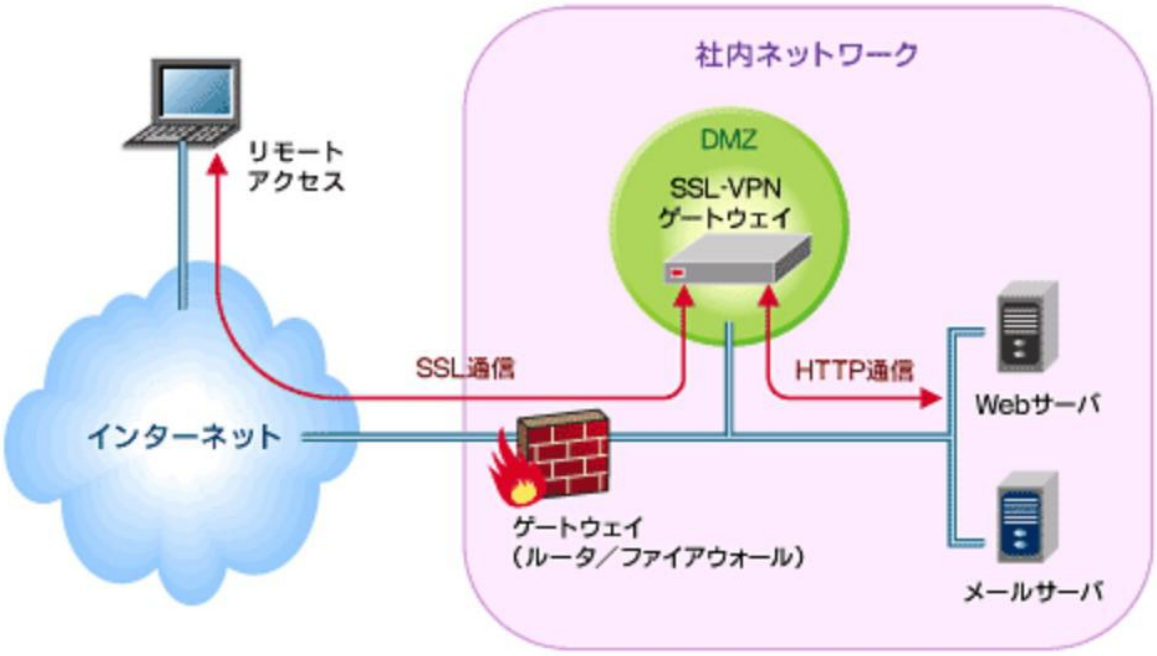
公開鍵暗号方式に基づくセキュアプロトコル。アプリケーション層で、データの暗号化を担う。公開鍵暗号方式と、公開鍵認証方式やパスワード認証方式の技術を用いて、リモートコンピュータとの通信を安全に行う。例えば、クライアント側SSHソフトには、『OpenSSH』、『Apache MINA/SSHD』があり、またサーバ側SSHソフトには、お『OpenSSH』、『TeraTerm』、『Putty』がある。



04-04. トランスポート層のセキュアプロトコル

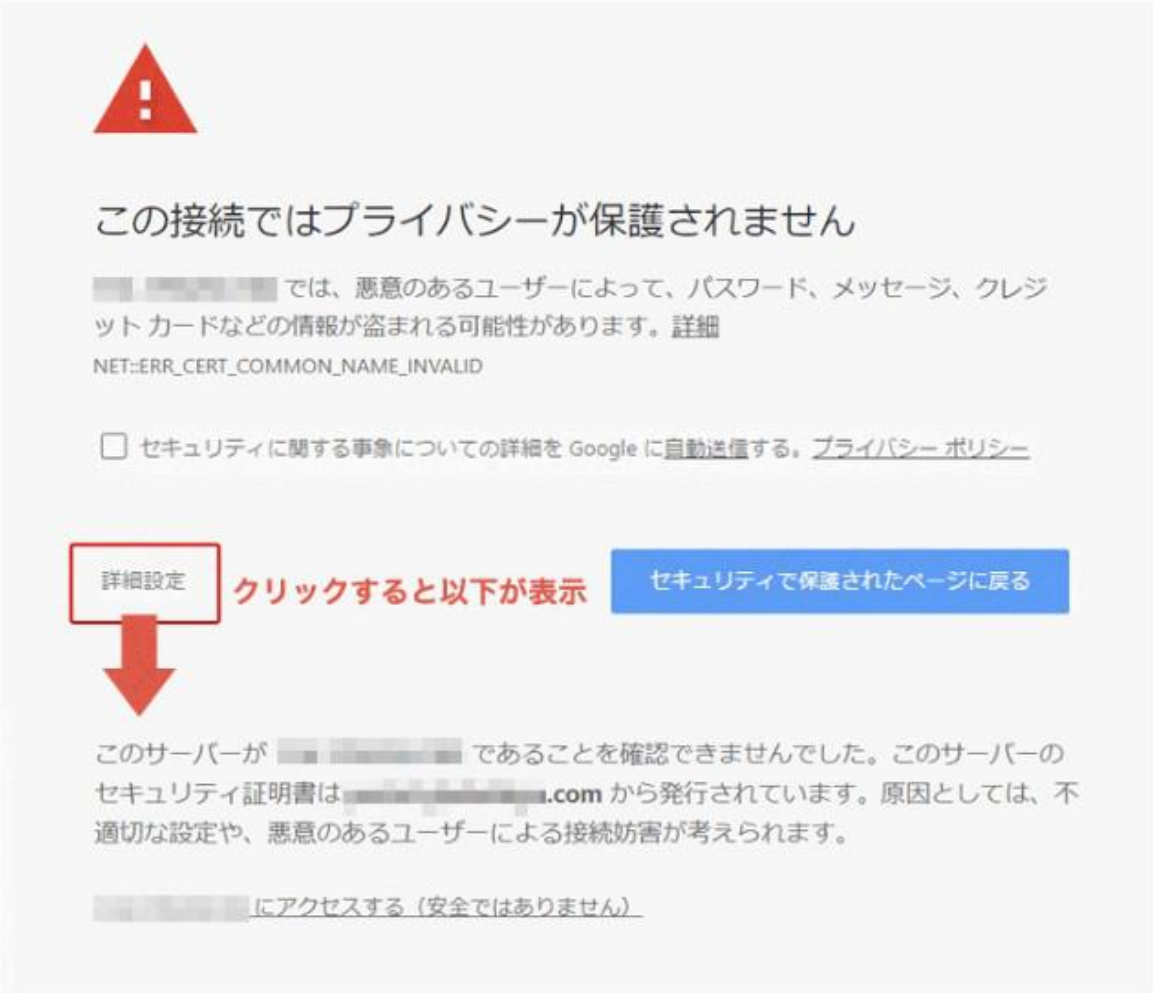
◆ SSL/TLS：Secure Sockets Layer / Transport Layer Security

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。



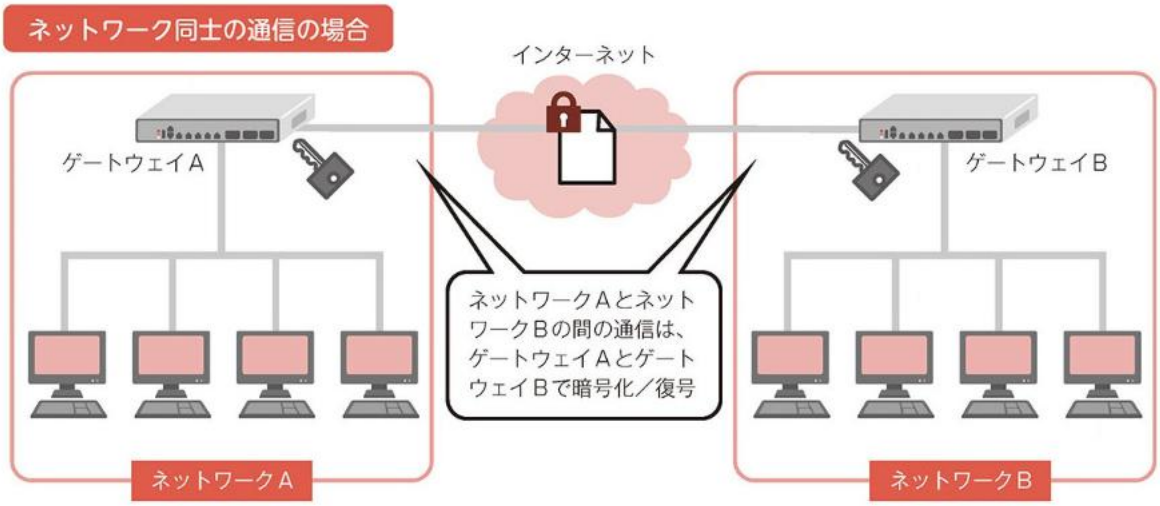
【具体例】

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。



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

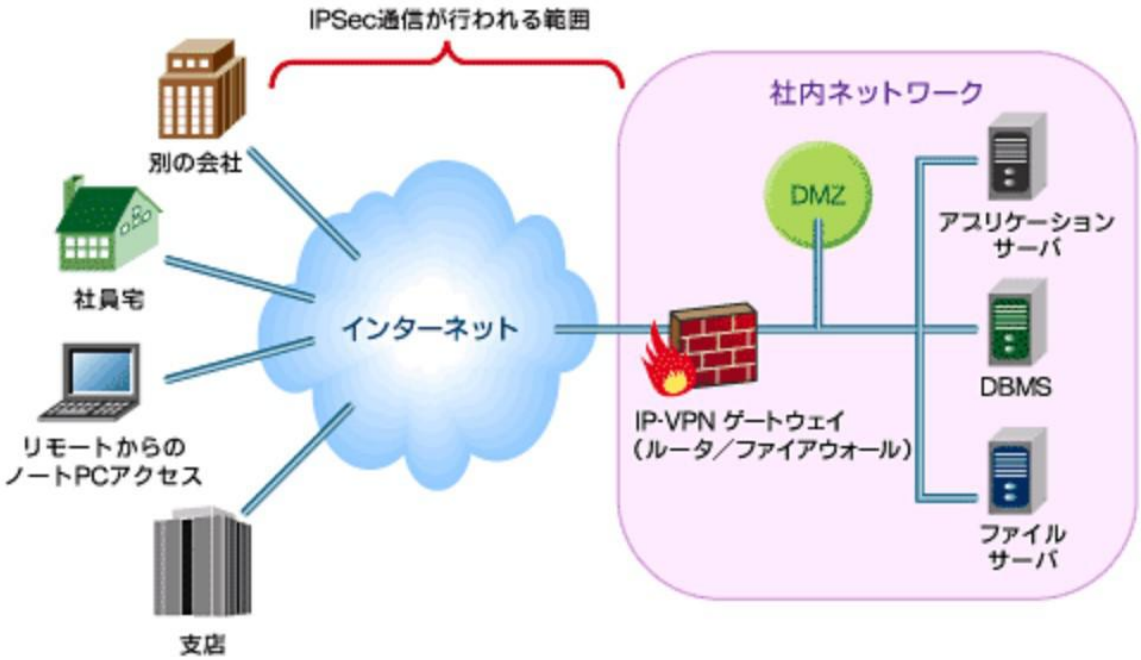
異なるネットワーク間で安全な通信を行うための仕組み。IPsecやSSL/TLSによって実現される。



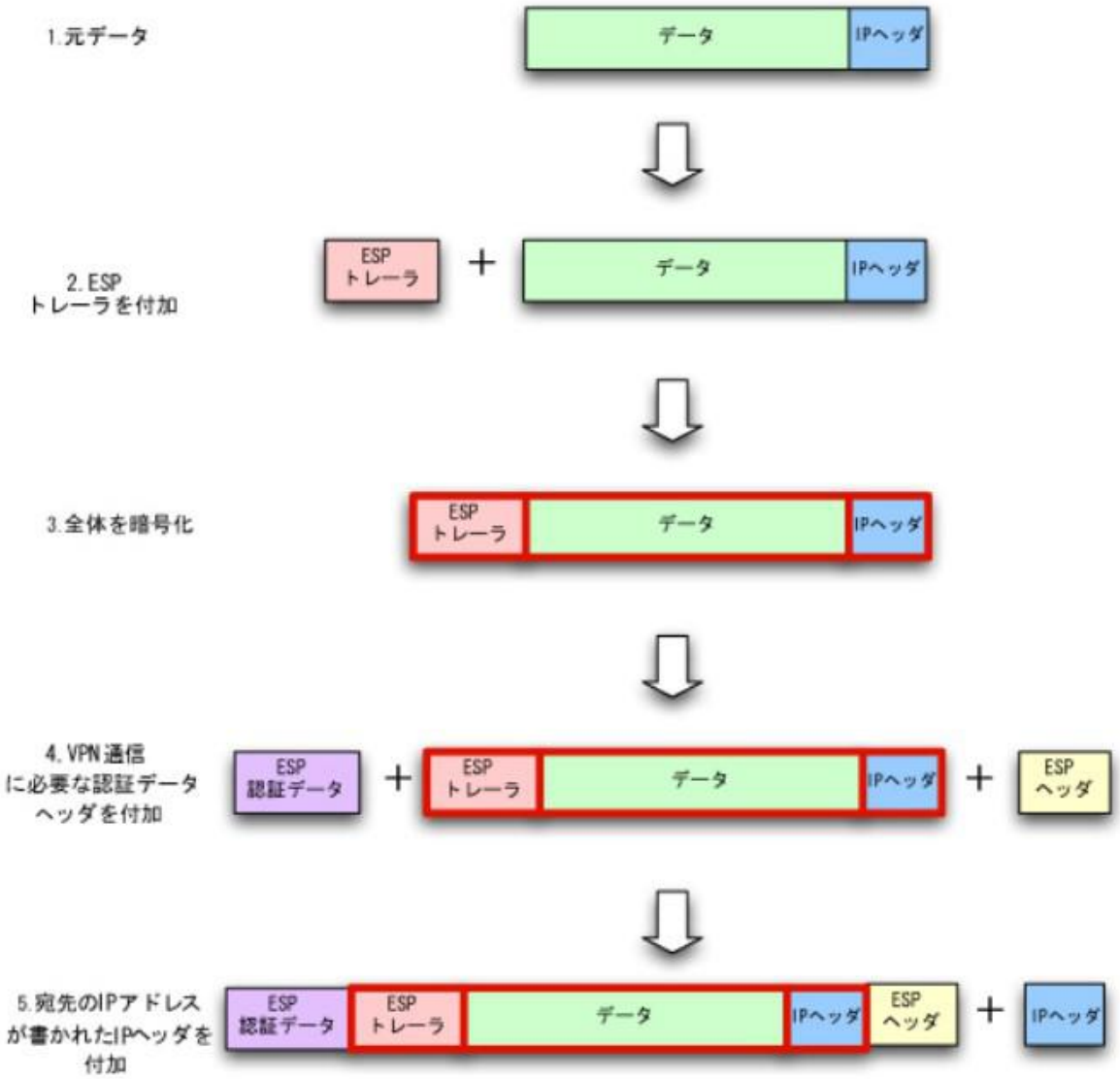
04-05. ネットワーク層のセキュアプロトコル

◆ IPsec：Internet Protocol Security

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。

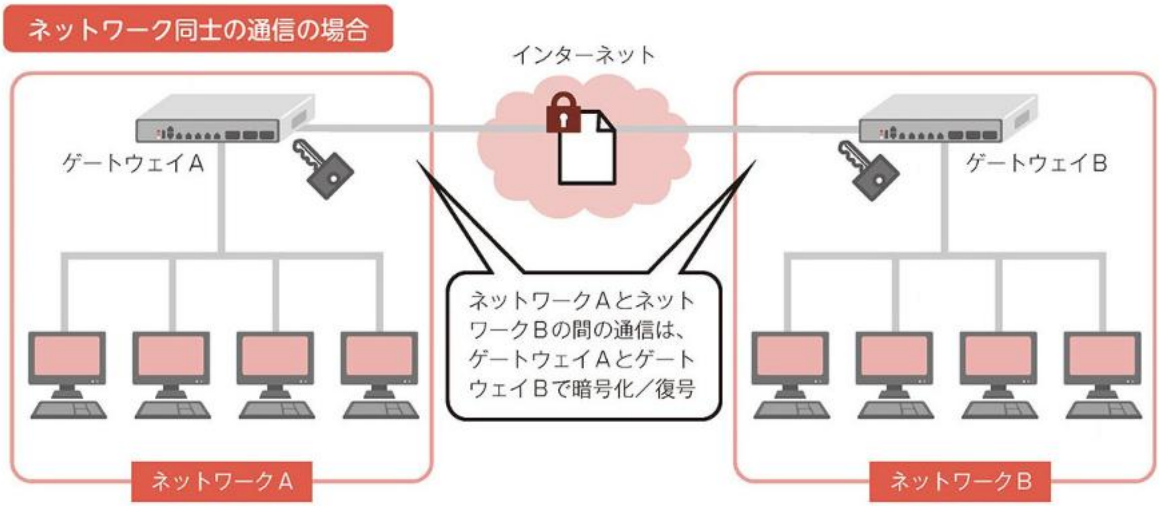


- **IPsecによるパケットのカプセル化**



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

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。



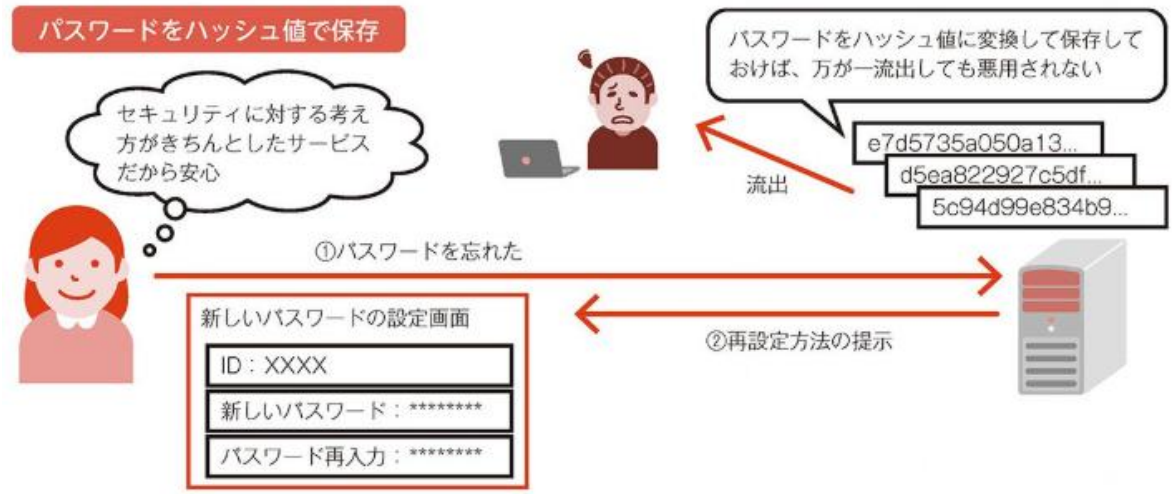
05. その他のセキュリティ技術

◆ メール受信におけるセキュリティ

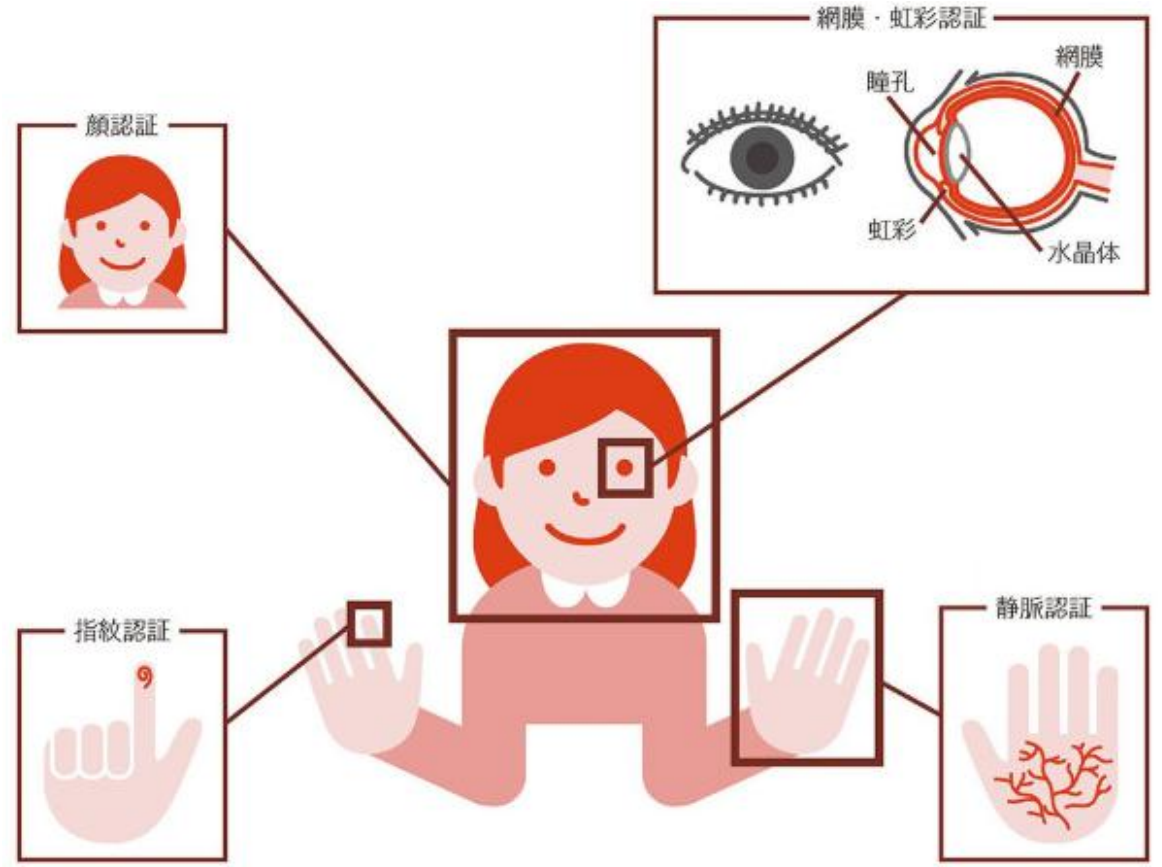
- **OP25B（Outbound Port 25 Blocking）**
- **SPF（Sender Policy Framework）**

◆ パスワードの保存方法

平文で保存しておくと、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



◆ Web beacon

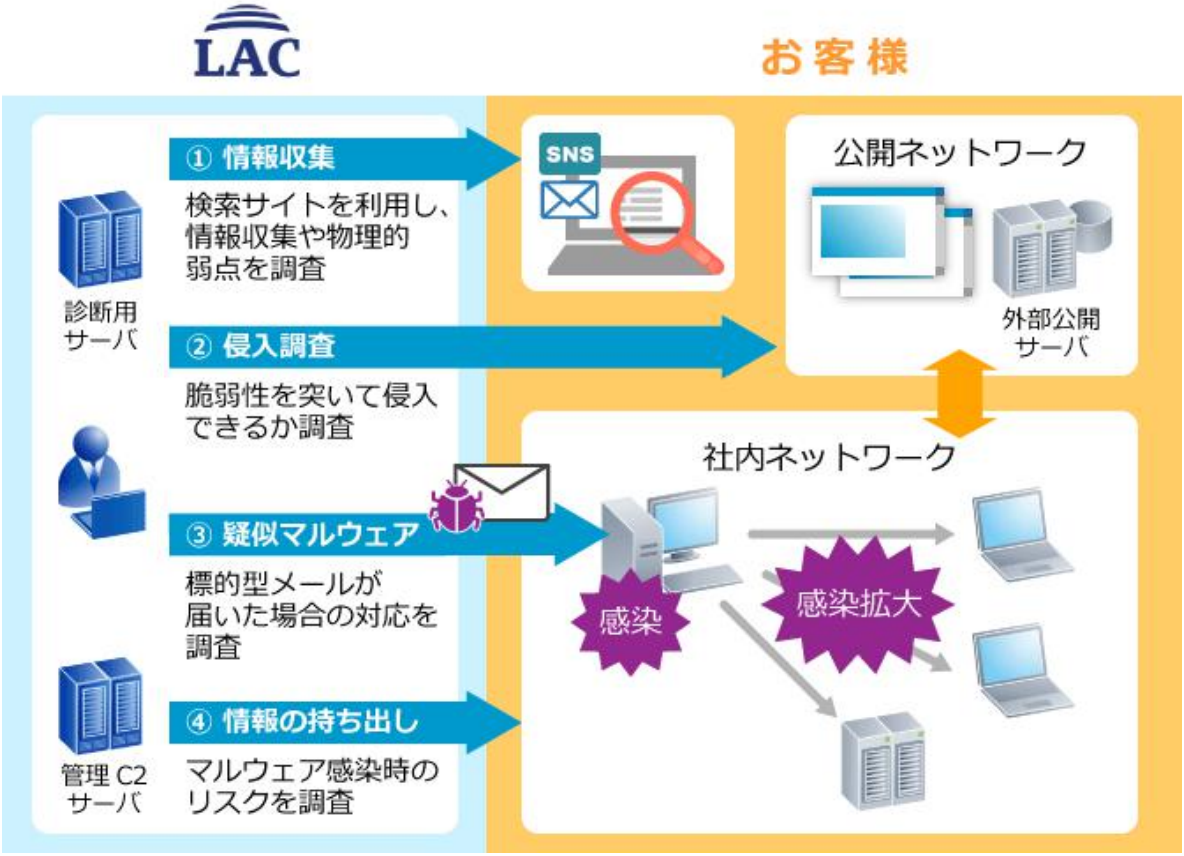
webページに、サーバに対してHTTPリクエストを送信するプログラムを設置し、送信されたリクエストを集計するアクセス解析方法。例えば、1x1の小さなGif「画像」などを設置する。

◆ 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



06-01. セキュリティマネジメント

◆ 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

06-01. CIA

◆ C：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。

【具体例】

- **IDとパスワードによるログイン**

◆ I：Integrity（完全性）

情報が書き換えられることがないこと。

【具体例】

- **データベースの内容が改竄されていないかを定期的に確認**

◆ A：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。

【具体例】

- **システムのデュアル化**
- **データのバックアップ**