
Information Technology
セキュリティ
担当：新田

# 情報セキュリティの脅威


情報セキュリティを脅かすもの（リスクを引き起こす要因）

人的脅威

技術的脅威

物理的脅威

## 人的脅威

- 誤操作
- 紛失・破損
- 情報漏洩
- 不正アクセス
- なりすまし
- ワンクリック詐欺
- フィッシング詐欺
- 内部不正

## 技術的脅威

- コンピュータウイルス
- ボット（BOT）
- スパイウェア
- ランサムウェア
- クロスサイトスクリプティング
- SQLインジェクション
- ブルートフォース攻撃
- キーロガー
- DoS攻撃

## 物理的脅威

- 地震
- 洪水
- 火災
- 経年劣化による故障
- 直接的な機器への破壊行為

# 人的脅威

- ヒューマンエラー

  不注意や誤操作によるデータの紛失や漏洩等

  例）

  - 社内の機密情報を保存したUSBメモリを紛失した。
  - 会員向けに一斉メールを送る際、toとbccを誤って入力して送信した。
    （他の受取人が全てのメールアドレスを閲覧可能に）
  - システムの設定ミスで、顧客情報が外部から閲覧可能な状態で保存されていた。

- 意図的な不正行為

  企業に対して悪意を持った人間が情報漏洩やデータの消去等を行う。

  例）

  - 従業員がデータ売却による金銭目的で顧客データを不正に持ち出した。

# クラッキング

企業のシステムなどに不正侵入し、情報を盗み出したり、
データを改ざんしたり、システムを破壊すること

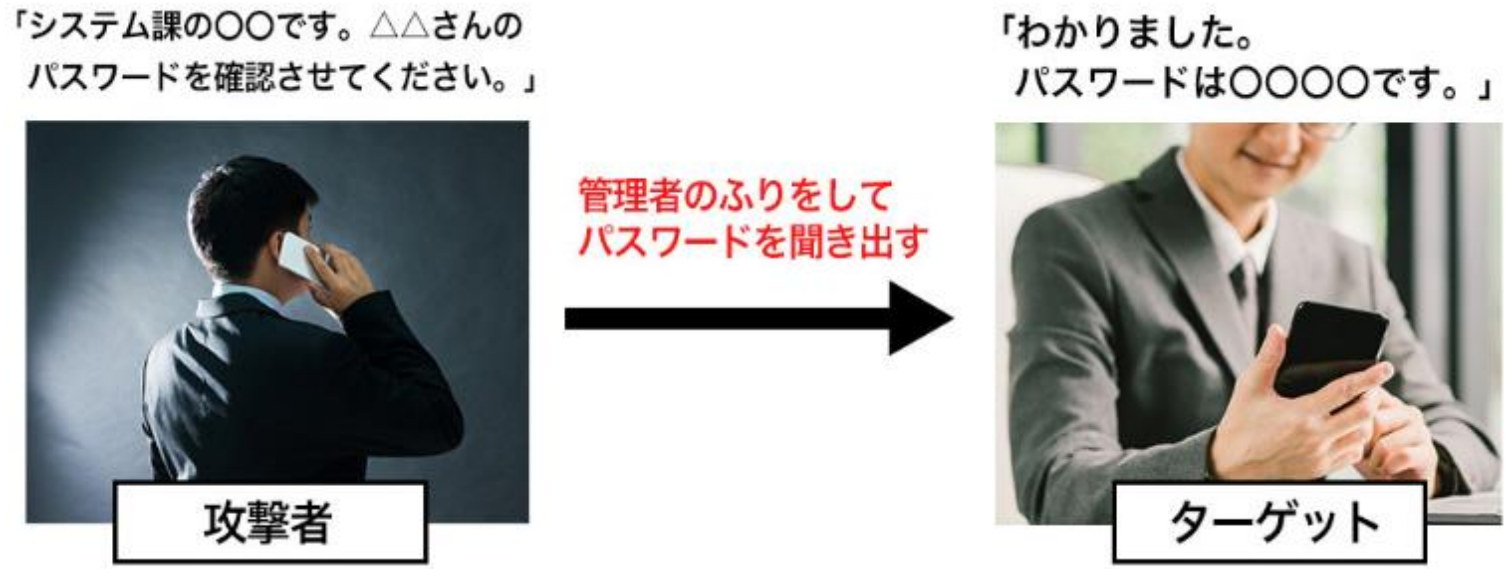
- ログイン情報を盗み出して不正アクセス
- 専用ツールを利用してパスワードを特定する
- マルウェア感染による情報の盗み出し
- OS・ソフトウェアの脆弱性の悪用

ハッキングは、システムの解析や改変、検証等の行為をいう。
クラッキングは明確に悪意のある目的で行われる。

# ソーシャルエンジニアリング

人の心理的な隙や不注意に付け込み、情報を不正に入手する方法

- なりすまして、電話やメールでパスワードを聞き出す
- のぞき見（ショルダーハッキング）
- ゴミ箱をあさる（トラッシング）
- ターゲットから攻撃者に連絡させる（リバースソーシャルエンジニアリング）

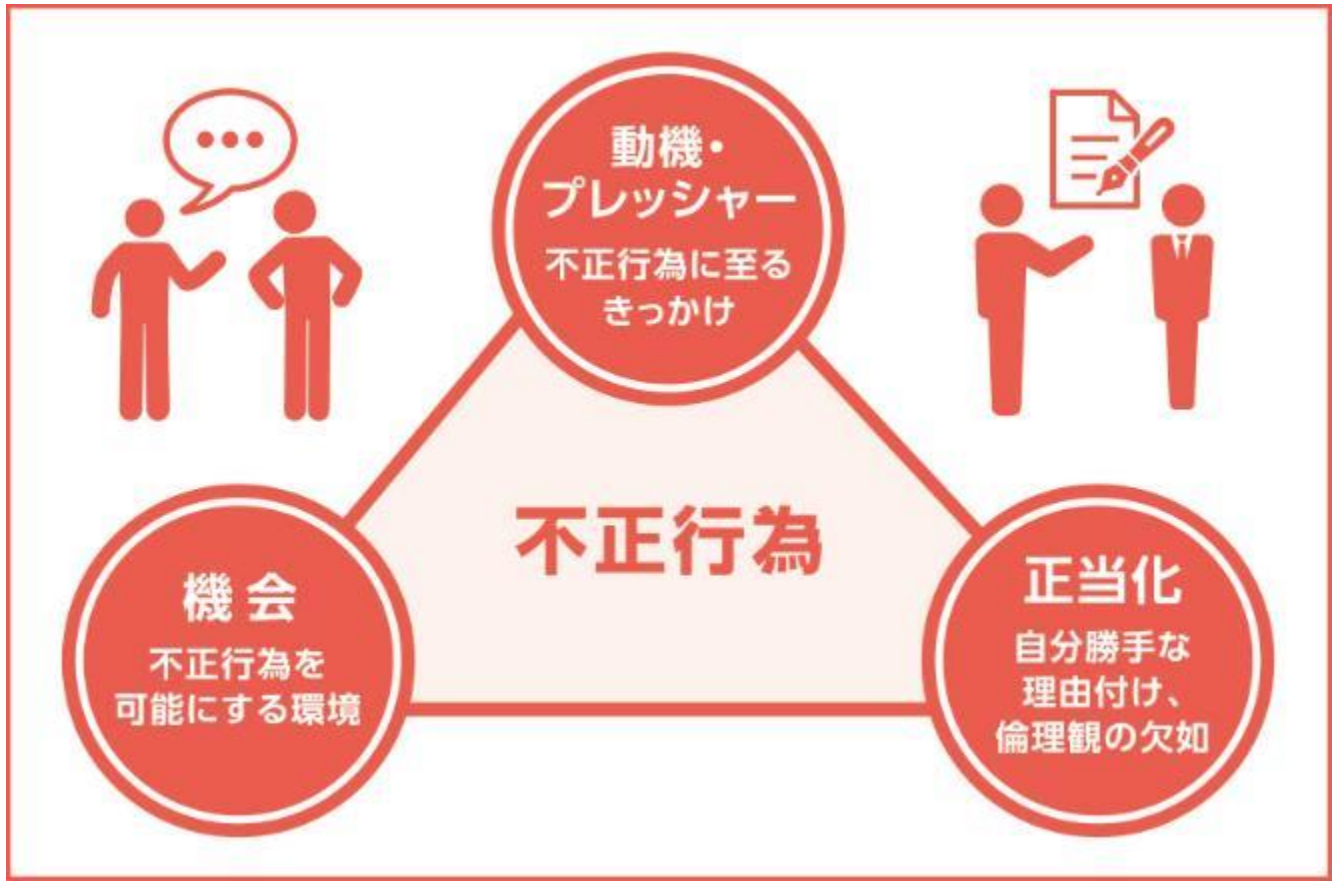


# 内部不正

会社の資産（機密情報・データ・備品等）を不正に利用する。

例）

- 会社の機密情報が記された書類を勝手に持ち出す。
- 自身のUSBメモリに顧客情報や取引情報を取り込む。
- 経費の虚偽申告や私的費用の請求をする。
- 会社から支給されたPCやスマホを私的に利用する。




不正のトライアングル

# 技術的脅威

サイバー空間において行われる**サイバー攻撃**

インターネットやデジタル機器を絡めた手口で、個人や組織を対象に、**金銭の窃取**や**個人情報の詐取**、あるいは**システムの機能停止**などを目的として行われる攻撃

**◆特定のターゲットを狙った攻撃**
・ランサムウェア
・標的型攻撃
・サプライチェーン攻撃
・キーボードロギング
・ドライブバイダウンロード攻撃
・水飲み場攻撃
・スプーフィング攻撃
・ビジネスメール詐欺

**◆不特定多数を狙った攻撃**
・フィッシング詐欺
・ゼロクリック攻撃
・ドメイン名ハイジャック攻撃
・MITM攻撃

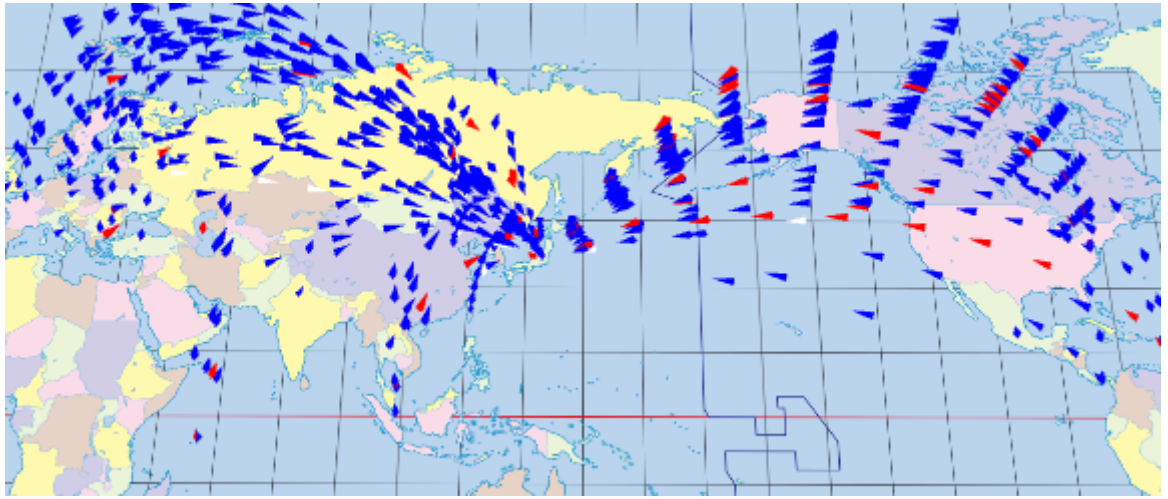
**◆脆弱性を狙った攻撃**
・SQLインジェクション
・OSコマンド・インジェクション
・クロスサイトスクリプティング
・クロスサイトリクエストフォージェリ
・ゼロデイ攻撃
・ルートキット攻撃
・セッションID固定化攻撃
・フォームジャッキング攻撃
・バッファオーバーフロー攻撃
・ディレクトリ・トラバーサル攻撃
・DNSキャッシュポイズニング

**◆サーバーに負荷をかける攻撃**
・DoS攻撃
・DDoS攻撃
  ・フラッド型攻撃
  ・F5アタック
  ・ランダムサブドメイン
  ・スマーフ攻撃
  ・PoD(ping of death)
  ・メールボム攻撃

# サイバー攻撃をリアルタイムで見る！

サイバー脅威マップ
https://cybermap.kaspersky.com/ja


Atlas
https://www.nicter.jp/atlas



# マルウェア（Malware）

悪意をもって作られたソフトウェアの総称

malicious（悪意のある）にsoftware（ソフトウェア）の2つの単語が組み合わさった造語

- ウイルス（コンピューターウイルス）
- ワーム
- トロイの木馬
- スパイウェア
- ボット
- ランサムウェア

# コンピューターウイルス

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラム。

次の機能を１つ以上有する。

### ◆自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

### ◆潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

### ◆発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

## ワーム

有害な動作を行うソフトウェアの一種で、ネットワーク等を通じてコンピュータに侵入し、自身を複製して感染する。自己増殖機能を有し、次々に他のコンピュータへの感染を試みる。

## トロイの木馬

有用なソフトウェアなどを装ってユーザーにインストール・実行をさせ、秘密裏にデータ漏洩や遠隔操作などの有害な動作を行うソフトウェア。

## スパイウェア

有害なソフトウェアの一種で、ユーザーの文字入力内容やWebアクセス履歴などのデータを気付かれないように収集し、インターネットを通じて攻撃者に報告する。

## ボット

コンピュータウイルスやトロイの木馬などの一部として送り込まれ、感染したコンピュータ上に常駐して特定のネットワークに接続して指示を待つ。攻撃者の指示で一斉に特定のネットワークへDDoS攻撃を行ったり、スパムメールの発信元などとして悪用される。

## ランサムウェア

有害なソフトウェアの一種で、感染したコンピュータからデータを抜き取ったり正常に利用できないようにし（操作画面のロックやファイルの暗号化）、復元のために犯人への金品の支払いを要求するもの。

## ★ブルートフォース（総当たり）攻撃

文字列の組み合わせを総当たりで試すことによって、暗号やパスワードを解読する攻撃手法。

## パスワードリスト攻撃

別のサービスやシステムから流出したアカウント名とパスワードのリストを用いてログインを試みる手法

## 辞書攻撃

辞書や人名録など人間にとって意味のある単語のリストを用いてログインを試みる手法

## ★ クロスサイトスクリプティング（XSS）

閲覧者が投稿できる入力フォーム等から、悪意のあるスクリプトを投稿することで、Webサイトのページ内に悪意のあるスクリプトを埋め込む攻撃手法

## ★ クロスサイトリクエストフォージェリ（CSRF）

Webブラウザを不正に操作する攻撃手法の一つで、偽装したURLを開かせて利用者に意図せず特定のサイト上で何らかの操作を行わせるもの。

## ドライブバイダウンロード

Webサイトなどに不正なソフトウェアを隠しておき、閲覧者がアクセスすると気づかないうちに自動でダウンロードして実行する攻撃手法。

## ★ SQLインジェクション

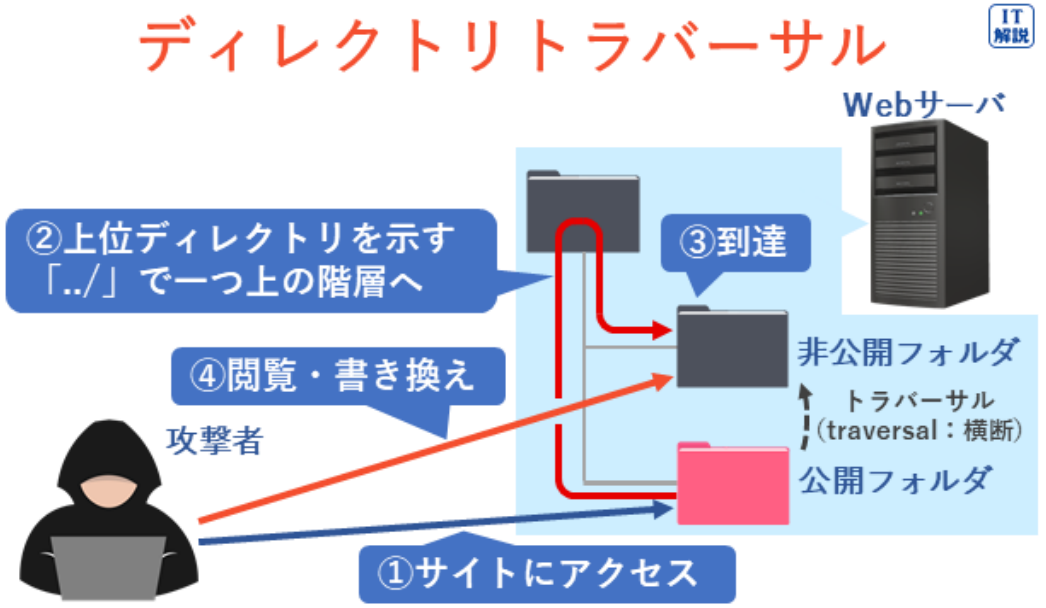
データベースと連動したWebアプリケーションなどに対する攻撃手法の一つで、検索文字列など外部から指定するパラメータの一部にSQL文を混入させ不正な操作を行うもの。

## バッファオーバーフロー攻撃（BOF）

サーバーの処理能力を超える大量のデータや悪意のあるコードを送り、メモリ領域内のバッファの許容量を超えて溢れさせ（オーバーフロー）、プログラムを強制停止したり、DoS攻撃の踏み台にする。

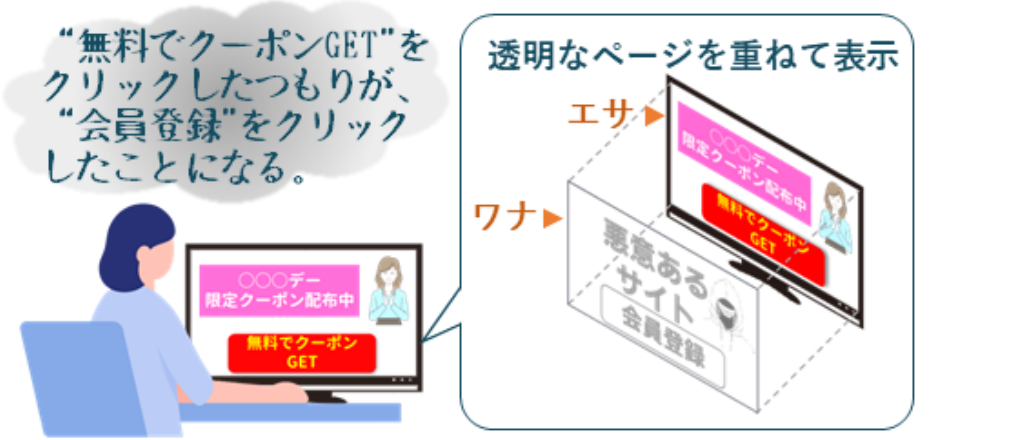
## ディレクトリトラバーサル

ファイル名を扱うようなプログラムに対して特殊な文字列を送信することにより、通常はアクセスできないファイルやディレクトリ（フォルダ）の内容を不正に取得する手法。




## ★クリックジャッキング

攻撃用ページの上に透明表示に細工した外部サイトを重ねて表示し、外部サイト上で利用者の意図しない操作を行わせる手法。



## 中間者攻撃（MITM攻撃 ：Man-in-the-middle）

通信を行う二者の間に割り込んで、両者が送受信する情報を自分が用意したものとすりかえ、気づかれることなく盗聴や通信に介入する手法。

## MITB攻撃（Man-in-the-browser）

攻撃対象のコンピュータにトロイの木馬等の悪意のあるソフトウェアを潜り込ませ、Webブラウザなどの通信を監視し、通信内容の改ざんや操作を乗っ取る手法。

## セッションハイジャック

攻撃者がログイン中の利用者のセッションIDを不正に取得し、セッションを乗っ取る攻撃手法。

## DNSキャッシュポイズニング

DNS情報の探索を行うキャッシュサーバに不正な手段で嘘の情報を覚えさせ、利用者からの問い合わせに答えさせる手法。

## バックドア

攻撃者が侵入に成功したシステムに設ける接続窓口で、管理者や利用者に気づかれないように秘密裏に設置され動作する遠隔操作用のプログラム。

## キーロガー

コンピュータのキーボード操作を監視しして記録する装置やソフトウェア。他人のコンピュータに仕掛けて情報を盗み取るのに悪用される。

## ゼロデイ攻撃

ソフトウェアなどにセキュリティ上の脆弱性が発見されたときに、問題の存在や対策法が広く周知される前に行われる攻撃。

## ★標的型攻撃

特定の個人や組織、情報を狙ったサイバー攻撃。個人情報や企業、国家の機密情報を盗み取る目的で行われることが多い。

## プロンプトインジェクション攻撃

AIサービスに対し悪意のあるプロンプトを入力することで、システム側が想定していない出力禁止情報や誤った情報を生成・出力させる攻撃。

## ★ DoS攻撃（Denial of Services attack）

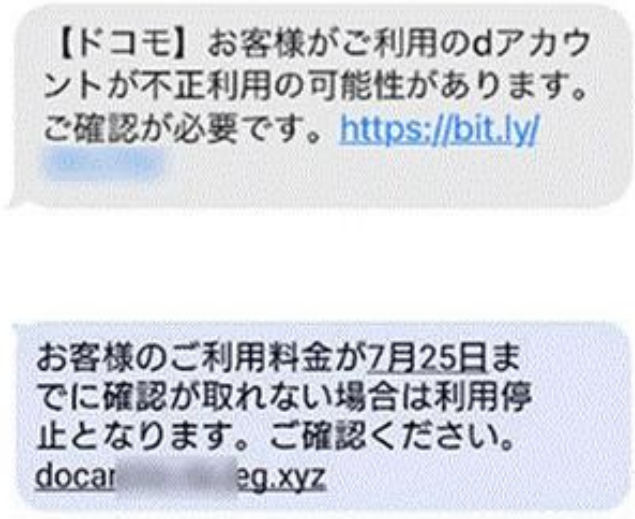
標的となる機器やネットワークなどを機能不全に陥らせる攻撃。大量のデータや不正なデータを送りつけて相手方のシステムを正常に稼働できない状態に追い込む。

## ★ DDoS攻撃（Distributed Denial of Service attack）

インターネット上の多数の機器から特定のネットワークやコンピュータに一斉に接続要求を送信し、過剰な負荷をかけて機能不全に追い込む攻撃手法。

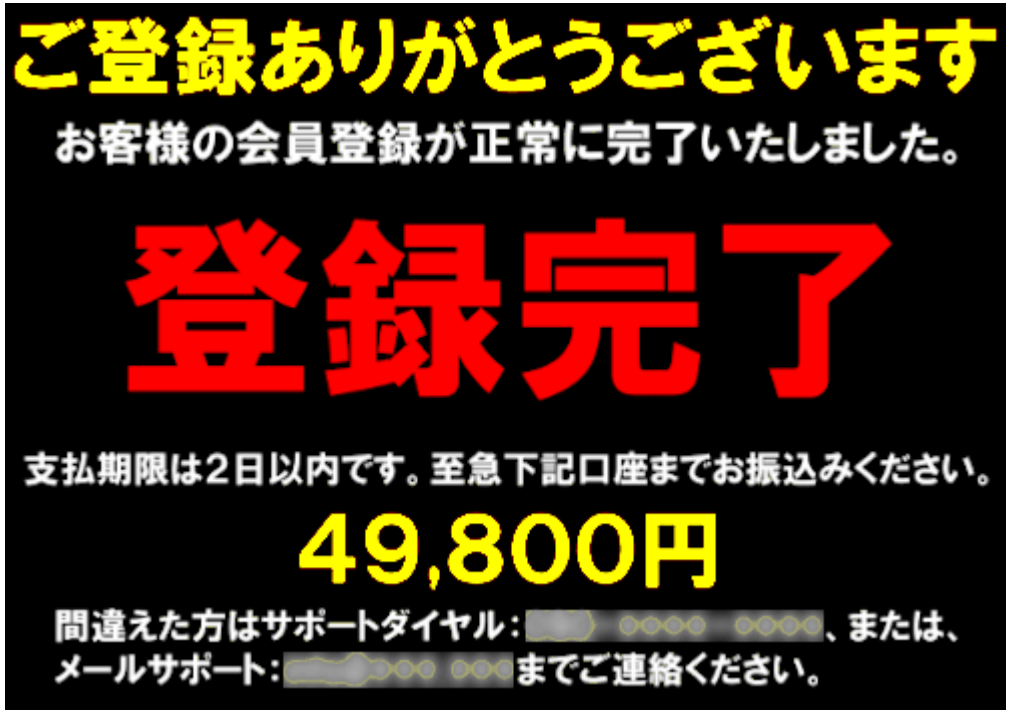
# フィッシング詐欺

金融機関や公的機関などを装った偽の電子メールを送信するなどして、受信者を架空のWebサイトや実在しているWebサイトの偽サイトに誘導し、暗証番号やクレジットカード番号などの情報を不正に取得する行為。




# ワンクリック詐欺

Webサイト・メール・SNSなどに記載されているURLをクリックするだけで、不当な料金を請求される詐欺の手法




# 実際に体験してみましょう！

IPA独立行政法人 情報処理推進機構 偽サイトセキュリティ警告画面の閉じ方体験サイト

https://www.ipa.go.jp/security/anshin/measures/fa-experience.html

詐欺サイト体験

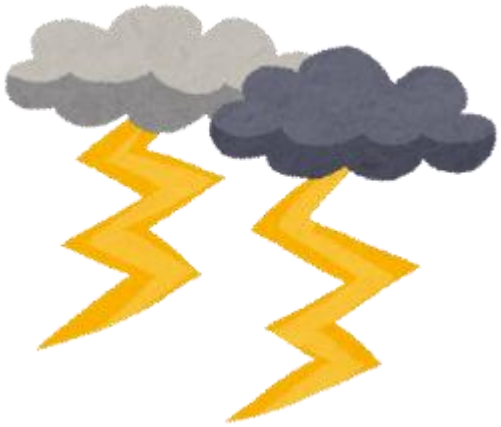
https://techno-kuro.com/phishingSiteDemo/

ワンクリック詐欺体験サイト

http://kentaro-shimizu.com/lecture/fraud/enter.html

# 物理的脅威

- 自然災害（大雨・地震・火事等）に起因するシステム障害
- 落雷等による停電
- 第三者が建物に侵入し、機器を破壊する等の妨害行為



# 情報セキュリティの脆弱性

- コンピュータやソフトウェア、ネットワークなどが抱える保安上の弱点。
- サイバーセキュリティ上の欠陥をセキュリティホールと呼ぶ。

ソフトウェアの実装上の誤りや設計・仕様上の不備

- 不正アクセス
- 情報漏洩
- サービス停止やシステムダウン
- マルウェアやランサムウェアの侵入
- システムの乗っ取り

人間の行動や物理的な問題も脆弱性に該当する

- 機密情報の管理体制の未整備
- 行動規範の不徹底
- 施設の警備や設備の盗難対策の不備

# セキュリティマネジメントの3要素

情報の**機密性**、**完全性**及び**可用性**を維持すること

ISO/IEC27000 JIS Q27000で定義
https://kikakurui.com/q/Q27000-2019-01.html

| 特性 | 意味 | 例 |
|---|---|---|
| **機密性**<br>confidentiality | • 認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また開示しない特性。<br>• データが漏洩せず守られていること。 | • アクセス権限<br>• パスワード管理<br>• データの暗号化 |
| **完全性**<br>integrity | • 正確さ及び完全さの特性。<br>• データの改ざんや削除が発生せず、正確な状態を保つようにすること。 | • ハッシュ関数<br>• バージョン管理<br>• データのバックアップ |
| **可用性**<br>availability | • 認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。<br>• 使いたいデータを必要に応じてすぐに使えるようにしておくこと。 | • 機器の冗長化<br>• 負荷分散<br>• メンテナンス |

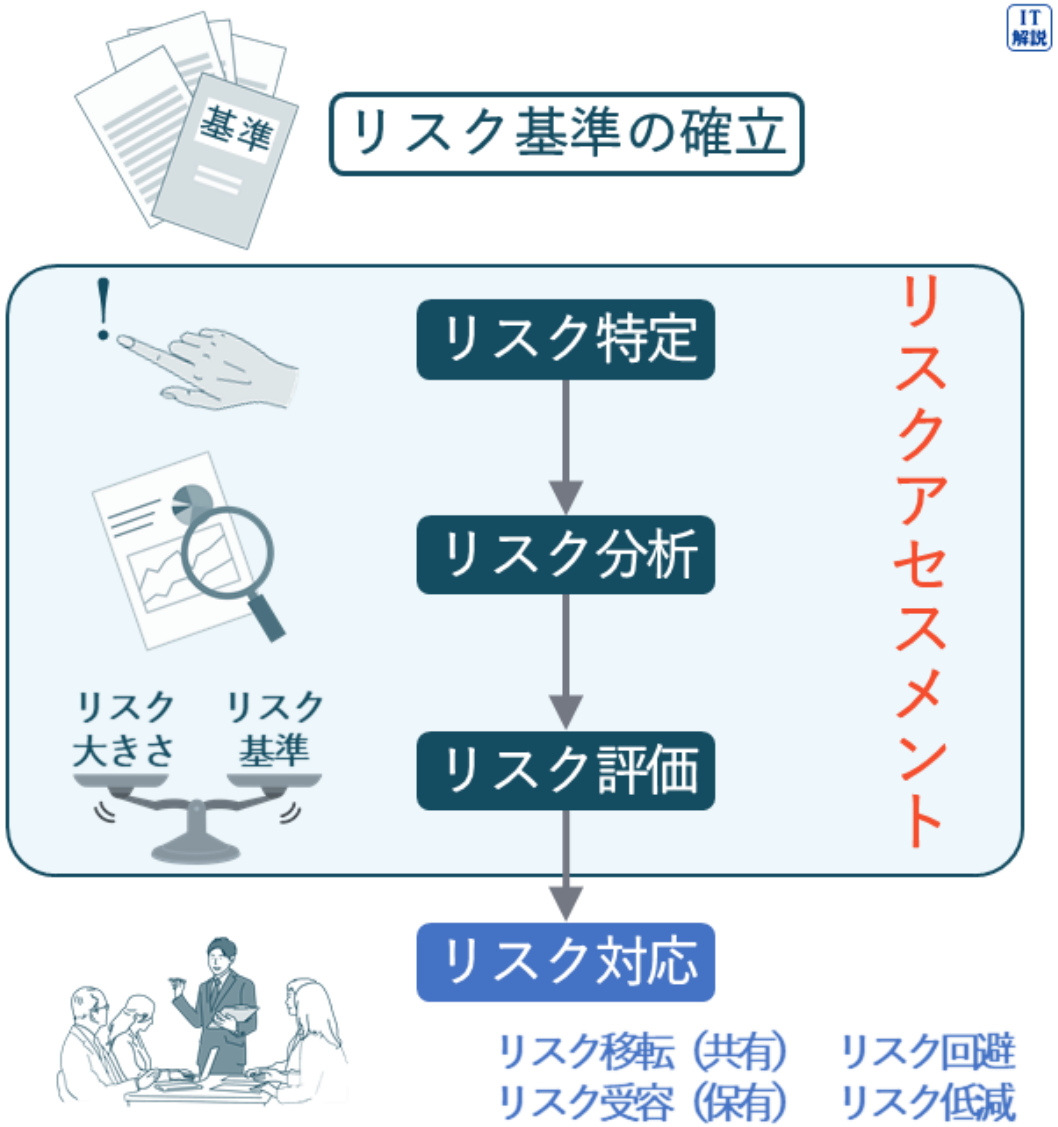
さらに**真正性**、**責任追跡性**、**否認防止**、**信頼性**などの特性を維持することを含めることもある。

ISO/IEC27000 JIS Q27000で定義

| 特性 | 意味 | 例 |
|---|---|---|
| **真正性**<br>Authenticity | • エンティティは、それが主張するとおりのものであるという特性。<br>• 通信相手が本人かどうかを確実にすること。 | • デジタル署名<br>• 二段階認証 |
| **責任追跡性**<br>Accountability | • あるエンティティの動作がその動作から動作主のエンティティまで一意に追跡できることを確実にする特性。<br>• インターネット上の一連の動作を追跡し、後になってインシデントが発覚した際に責任を追求できる状態を維持すること。 | • 操作ログ<br>• アクセスログ<br>• アクセス制御 |
| **否認防止**<br>non-repudiation | • 主張された事象又は処置の発生、及びそれらを引き起こしたエンティティを証明する能力。<br>• 情報システムの利用や操作、データの送信などに関連して、確かにある特定の人物が行なったことを後から証明できるようにする仕組みや技術。 | • デジタル署名<br>• タイムスタンプ<br>• アクセスログ |
| **信頼性**<br>Reliability | • 意図する行動と結果とが一貫しているという特性。<br>• 意図した動作が確実に行われることを担保すること。 | • システム構築時の設計（例外処理やバリデーション） |

# 情報セキュリティの3+4要素（7要素）

# リスクマネジメント




- **リスク特定**

  リスク源、リスクによって生じる事象、それらの原因・起こりうる結果を発見、認識、特定する。

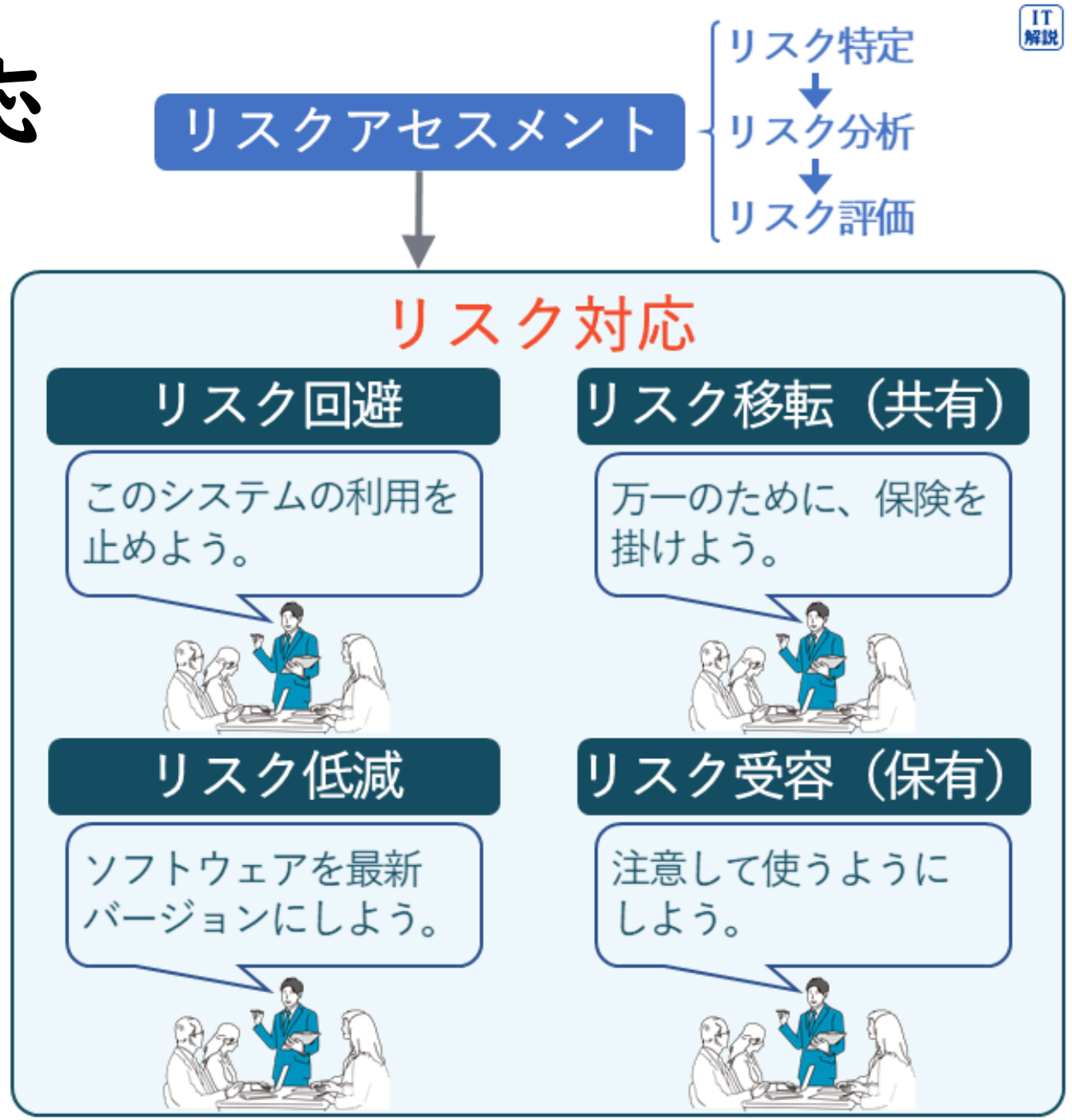
- **リスク分析**

  リスクの特質を理解し、リスクの影響度や発生率を算定し、リスクレベルを決める。

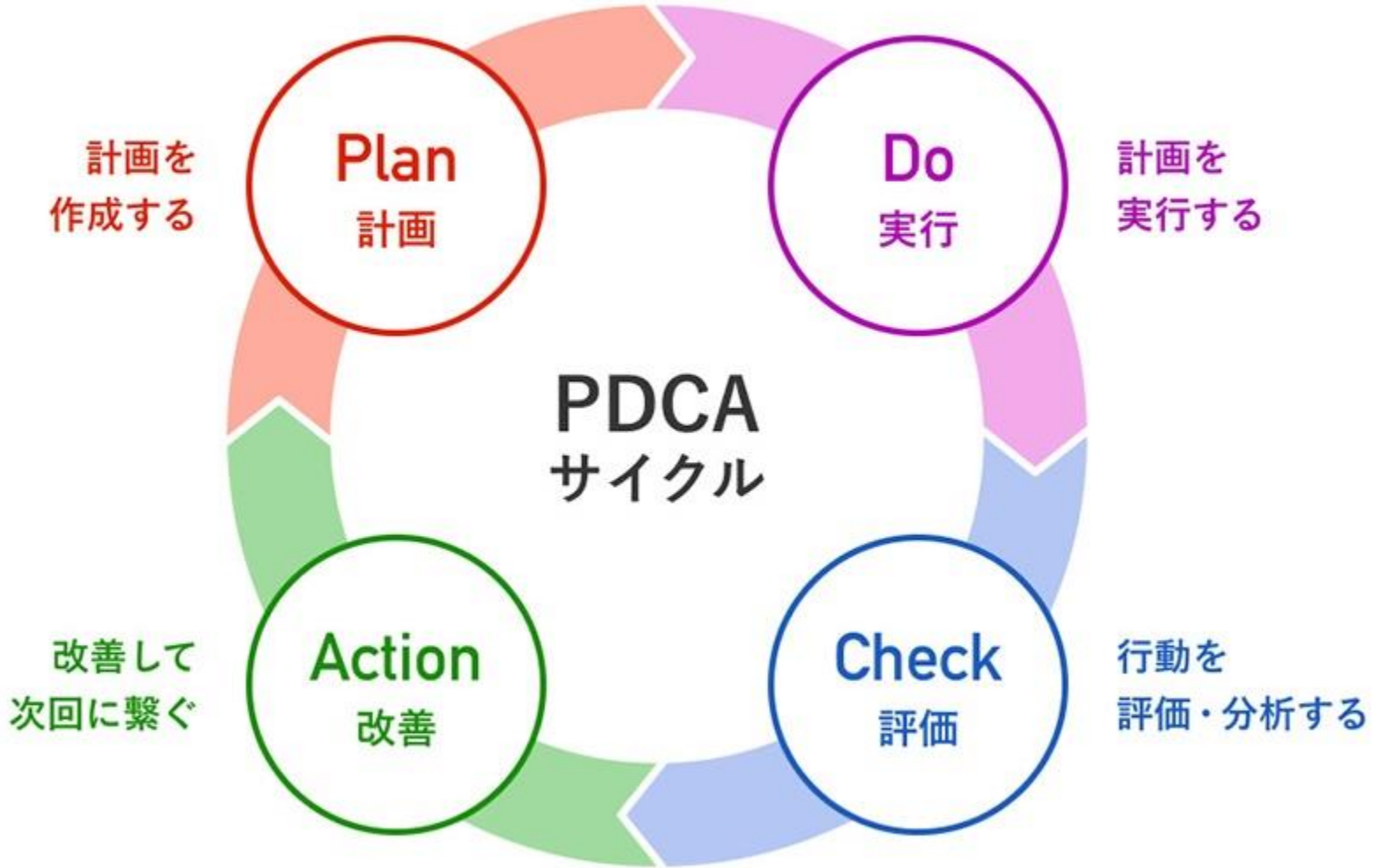
- **リスク評価**

  リスクが受容可能か許容可能か、リスク分析の結果を可視化し、リスクの順位付けを行う。

# リスク対応


IT解説
リスクアセスメント
リスク特定
リスク分析
リスク評価
リスク対応
リスク回避
このシステムの利用を止めよう。
リスク移転（共有）
万一のために、保険を掛けよう。
リスク低減
ソフトウェアを最新バージョンにしよう。
リスク受容（保有）
注意して使うようにしよう。

# PDCAサイクル


計画を
作成する
Plan
計画
Do
実行
計画を
実行する
PDCA
サイクル
改善して
次回に繋ぐ
Action
改善
Check
評価
行動を
評価・分析する

# 情報セキュリティマネジメントシステム
## （ISMS：Information Security Management System）

- 個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用すること。
- 情報の機密性、完全性及び可用性をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えること。

https://isms.jp/isms/

**情報セキュリティポリシ**

企業や組織の情報セキュリティへの取り組み方を規定する文書

# 個人情報保護

## 個人情報

本人の氏名、生年月日、住所等、特定の個人を識別できる情報

## プライバシー

個人や家庭内の私事・私生活、個人の秘密。また、それが他人から干渉・侵害を受けない権利

- 個人情報保護法
- JIS Q 15001
- プライバシーマーク制度


プライバシーマーク（Pマーク）

# 関連用語

- CSIRT
- 情報セキュリティ委員会
- SOC（Security Operation Center）
- コンピュータ不正アクセス届出制度
- コンピュータウイルス届出制度
- ソフトウェア等の脆弱性関連情報に関する届出制度
- ISMAP
- J-CSIP
- J-CRAT（サイバーレスキュー隊）
- SECUTIRY ACTION
- デジタルフォレンジックス

# 人的セキュリティ対策

## アクセス権の設定（アクセス制御）

情報資産に対してアクセスできる権限を付与することで、誰にどの程度の利用を許可あるいは拒否するか設定する。

職務や役割によって必要最低限のアクセスを許可する。

例）開発部門には編集・削除・閲覧権限
　　営業部門には閲覧権限のみ

# セキュリティ教育・啓発・訓練

組織における社員の情報セキュリティ意識を高め、行動を遵守させる。

［組織セキュリティ啓発］

・情報セキュリティポリシの周知
・情報セキュリティに関する社内規定の遵守
・情報セキュリティに関するマニュアルの遵守

教育

情報セキュリティ意識向上

［組織セキュリティ訓練］

訓練用の標的型メール

○○様

大変お世話になっています。
××です。
以前のご契約の件です。

下記に契約書を保存いたしましたので、ご確認ください。

URL:https://……

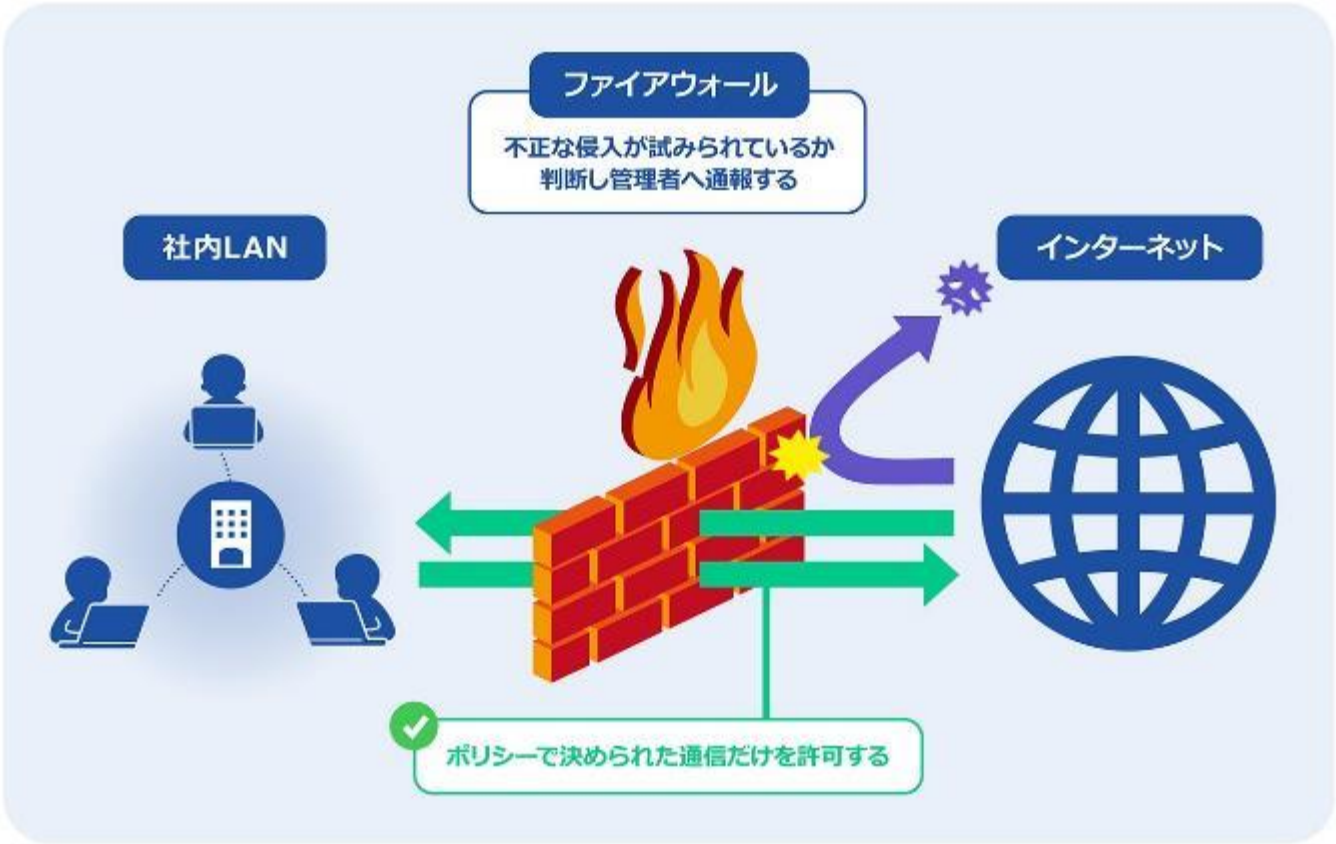
訓練

対応
・メールを開かない
・URLをクリックしない
・情報セキュリティ組織に報告する

# 技術的セキュリティ対策

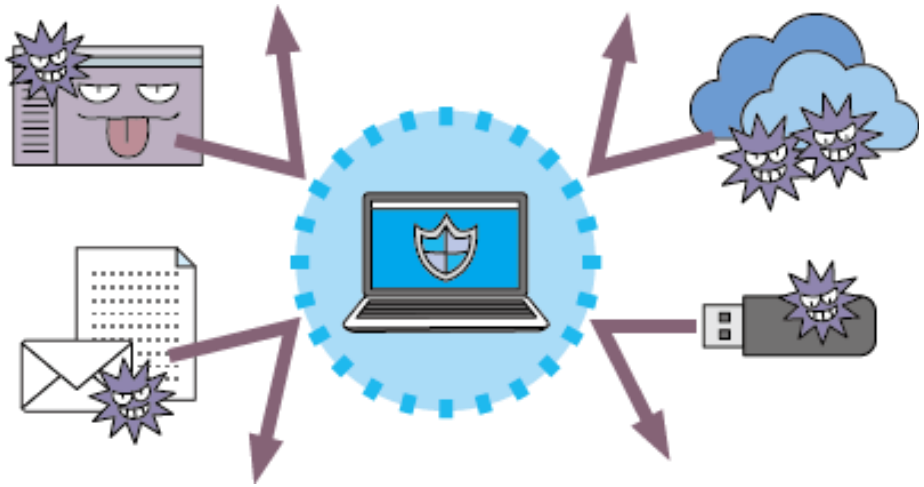
## ファイアウォール

内部ネットワークを外部のネットワークから守る仕組み



# コンピュータウイルス対策

- ウイルス対策ソフトの利用する
- ソフトウェアを最新のバージョンに保つ
- セキュリティパッチを適用する
- 怪しいメールや添付ファイルは開かない
- 怪しいサイトは開かない
- 不審なソフトウェアをダウンロードしない
- バックアップを定期的に残す



対策についてはこちらの講座資料も参照↓

https://hau-pu.xrea.jp/x/file/%E8%AC%9B%E5%BA%A7%E8%B3%87%E6%96%99/%E6%83%85%E5%A0%B1%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3.pdf

# サイバーキルチェーン


サイバー攻撃の段階を説明した代表的なモデルの一つ。

サイバー攻撃を7段階に区分して、攻撃者の考え方や行動を理解することを目的としている。

サイバーキルチェーンのいずれかの段階でチェーンを断ち切ることができれば、被害の発生を防ぐことができる。

# 関連用語

- コールバック
- WAF
- DMZ
- VPN（Virtual Private Network）
- MDM
- 電子透かし
- デジタルフォレンジックス
- ペネトレーションテスト
- 耐リンパ性
- ブロックチェーン
- 検疫ネットワーク
- IDS（Intrusion detection System）
- IPS(Intrusion Prevention System)
- サニタイジング
- マルウェア・不正プログラム対策
- スパム対策
- URLフィルタリング
- MACアドレスフィルタリング
- セキュリティパッチ

# 物理的セキュリティ対策

## 入退室管理

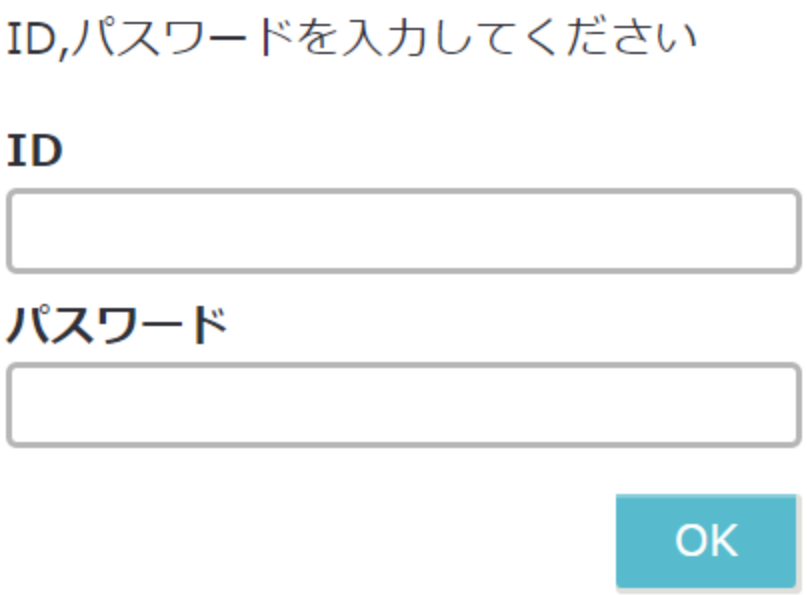
サーバ室や資料室など重要情報を取り扱う場所への入退室を
顔認証端末や指紋、ICカードを用いて管理する。

- 監視カメラ
- 施錠管理
- クリアデスク
- クリアスクリーン
- アンチパスバック
- インターロック

# ユーザ認証

あるシステムへの利用を申し出た人物が、予め登録された利用者本人であるかを確かめること。

## ログイン（利用者IDとパスワード）




利用者ID

ユーザー人一人に割り当てられた識別名

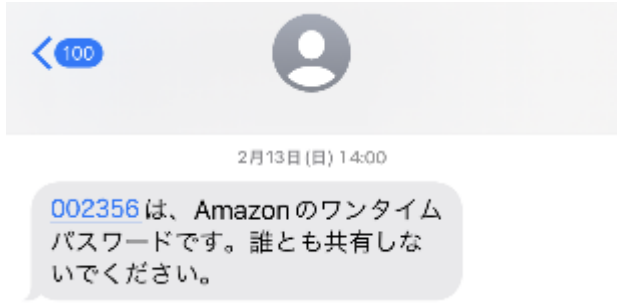
パスワード

ユーザしか知り得ない文字列

## ワンタイムパスワード

1度だけ使える使い捨てのパスワード。

予め登録しておいたスマートフォンのSMS（ショートメッセージ）充にワンタイムパスワードを送信するSMS認証が使われる。

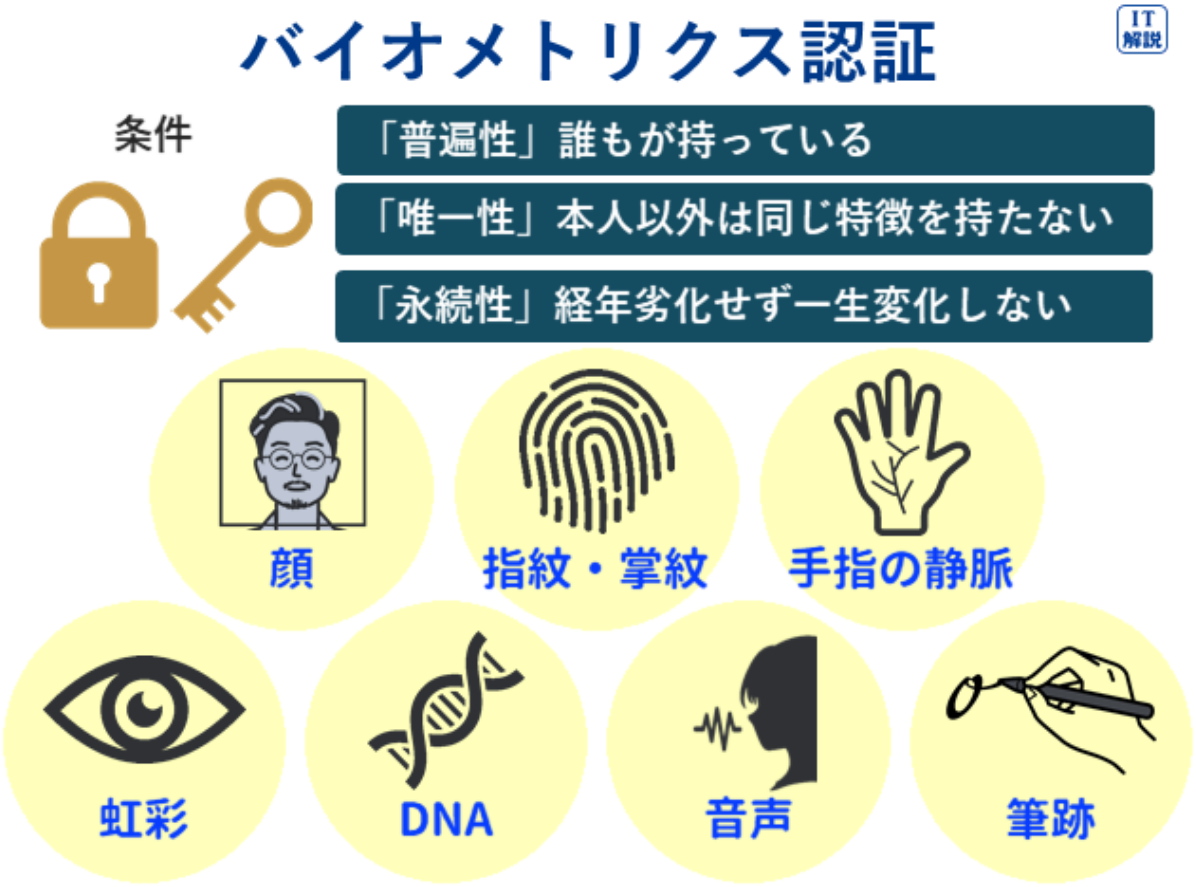



## シングルサインオン

1つのIDとパスワードで複数のWebサービス、アプリケーションにログインする仕組み

# 生体認証（バイオメトリクス認証）

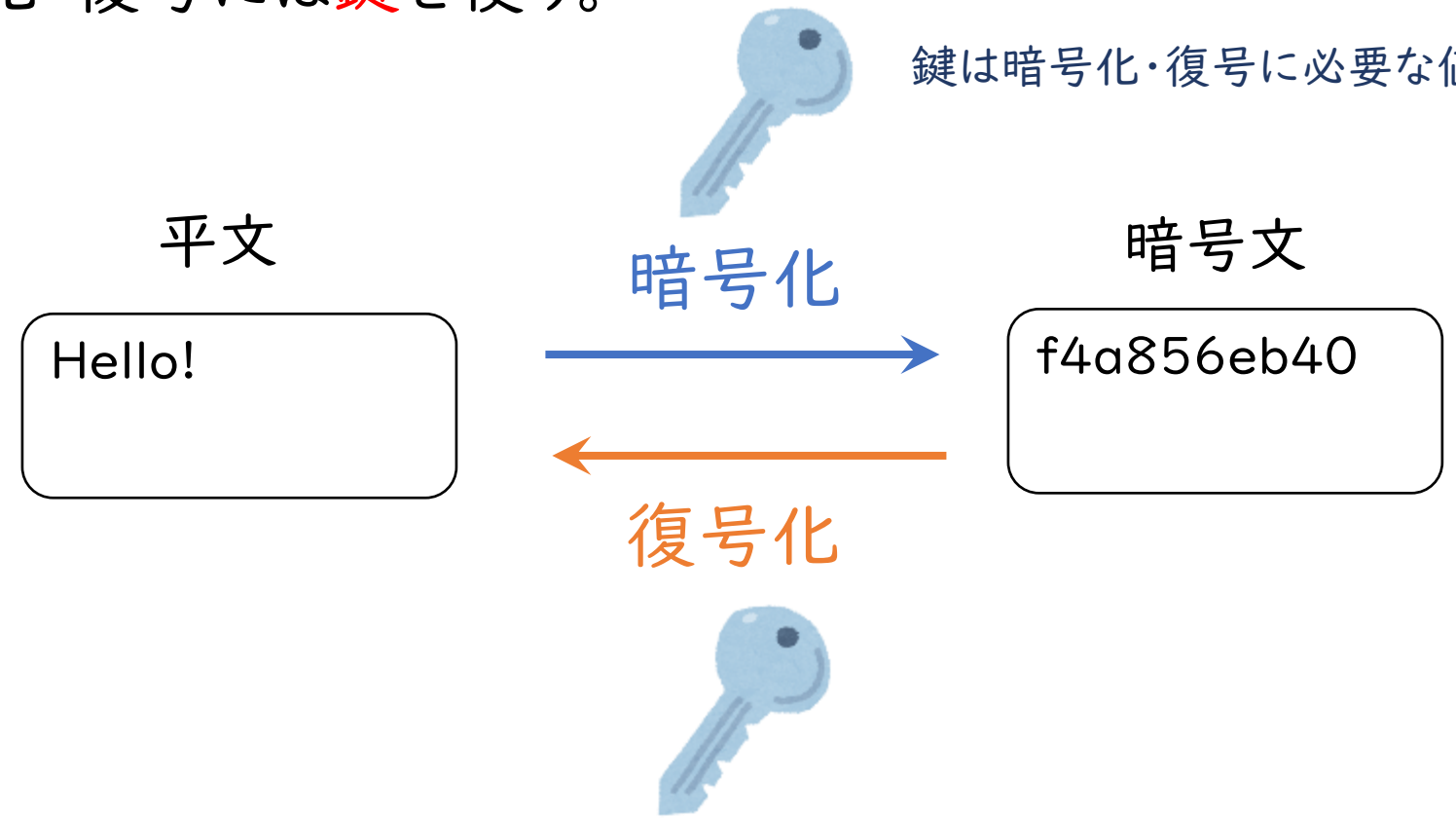
顔や指紋、虹彩などの身体的特徴や、筆跡などの行動的特徴を用いて利用者を認証する方法



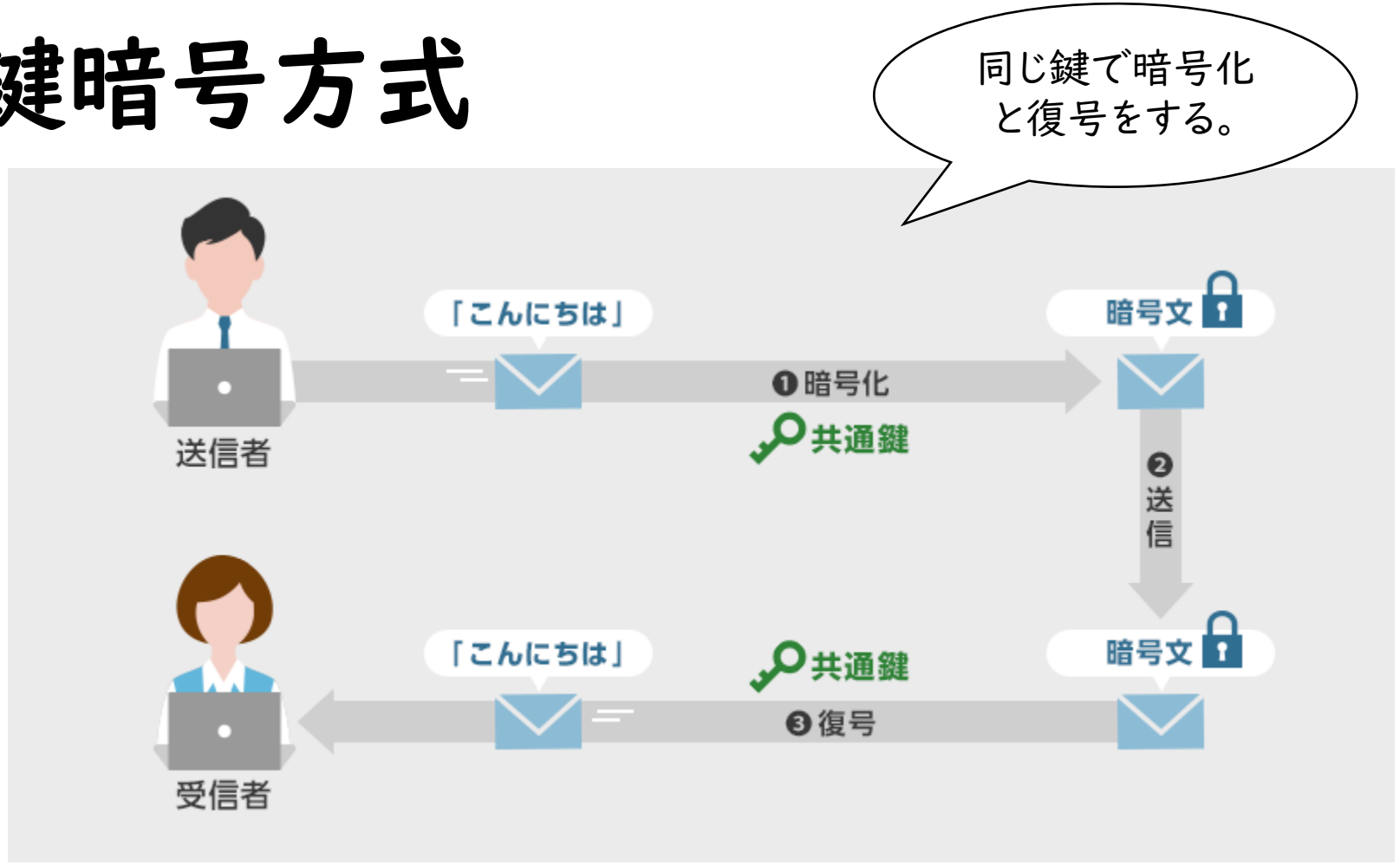
# 暗号化技術

情報を盗み見られる恐れがあるインターネット上では、個人情報やパスワード等を第三者に読まれない様に、データを暗号化して送受信する。

暗号化・復号には鍵を使う。

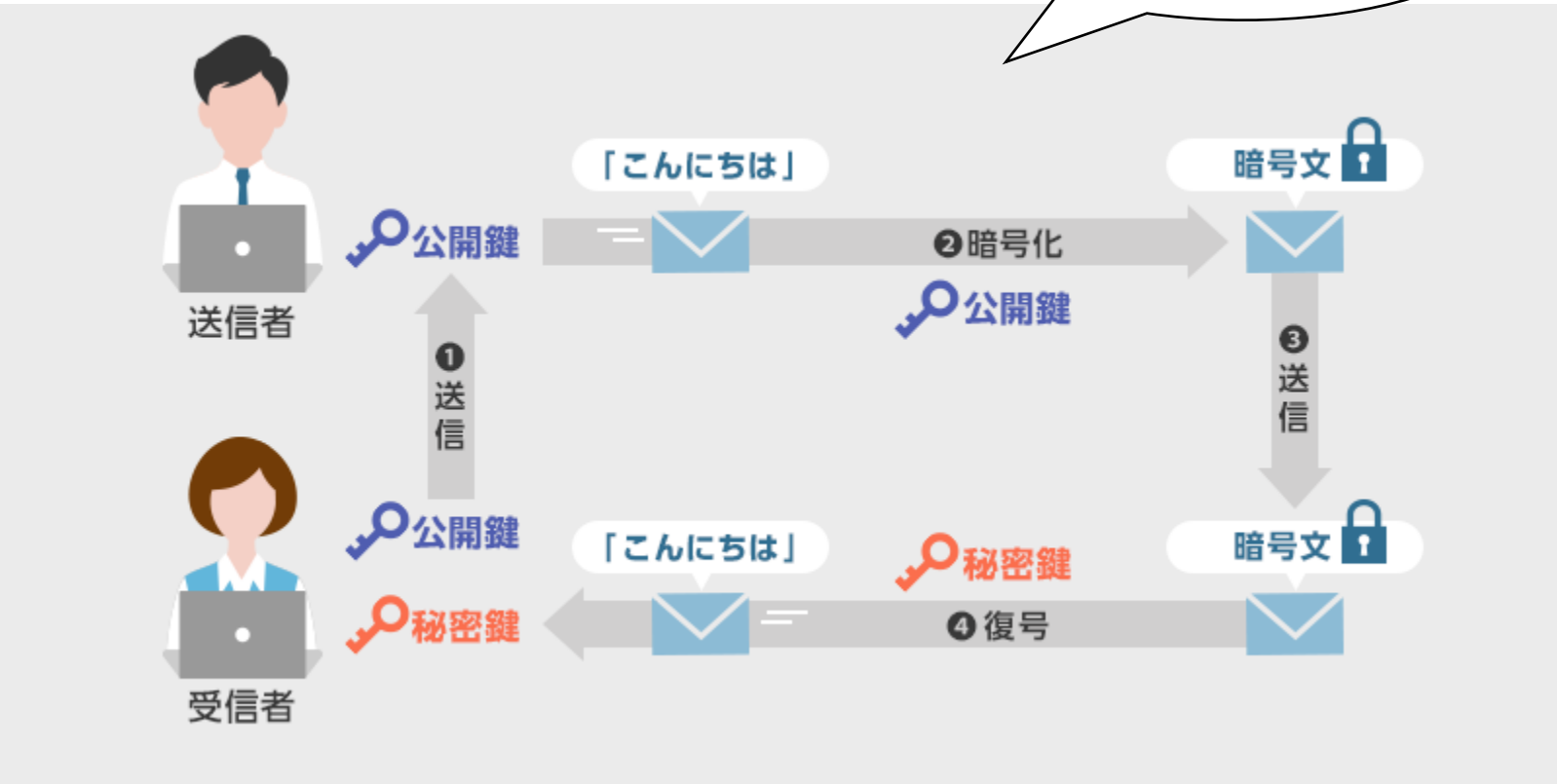


# 共通鍵暗号方式




- 暗号化と復号化に同じ鍵を使う
- 事前に相手と共通鍵を共有する必要がある。(通信相手全員が保持する)
- 共通鍵が外部に漏洩すると、暗号化したデータを読み取られる可能性がある。

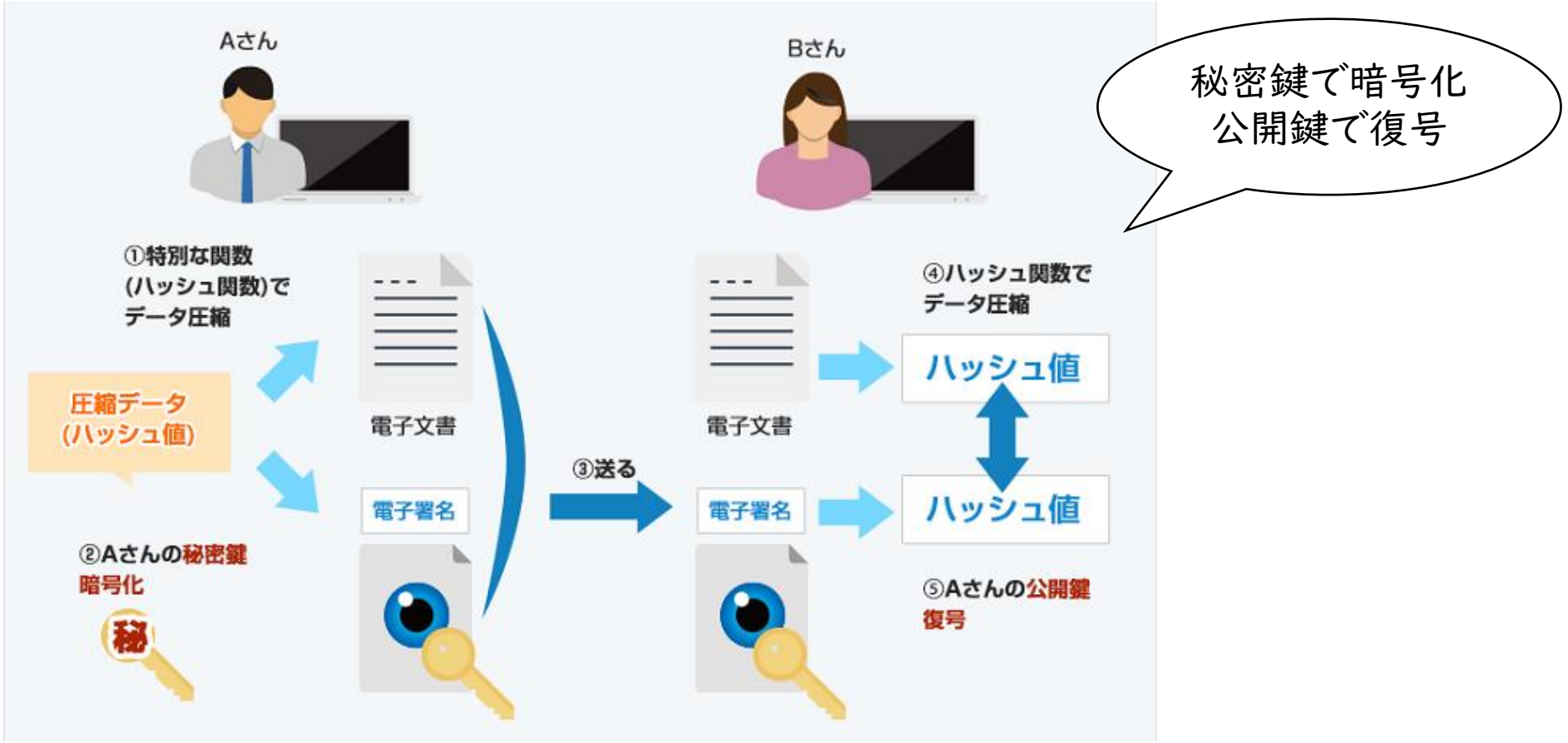
# 公開鍵暗号方式




- 誰でも入手できる公開鍵と、発行元しか知らない秘密鍵を利用する。
- 安全性が高く（盗聴やなりすまし対策）、鍵の管理が容易。
- 暗号化・復号化の処理に時間がかかる。

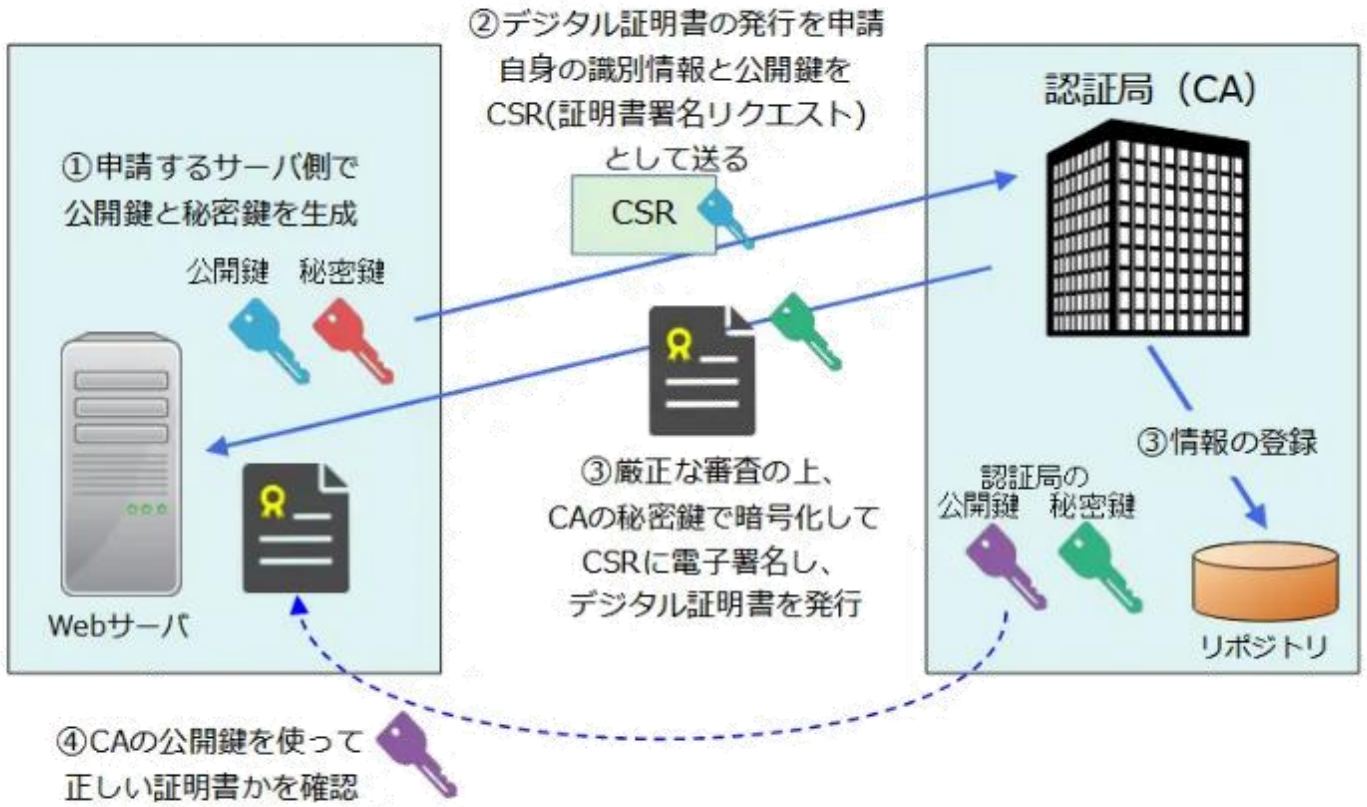
# 電子署名（デジタル署名）

- 文書やメッセージ等のデータの真正性を証明するために付加する短いデータ。
- 作成者を証明し、改ざんやすり替えが行われていないことを保証する。



# 電子証明書（ディジタル証明書）

- 公開鍵を配送する際に、受信者が鍵の所有者を確認するために添付される。
- 一般的には認証局（CA: Certificate Authority)という機関が発行する。



# 公開鍵基盤

PKI：Public Key Infrastructure

公開鍵暗号方式を使って暗号化
通信するための基盤