情報セキュリティ

私たち人間は、ウイルスや細菌などの「病原体」によって病気になります。同じように、コンピュータにも「病原体」が存在します。コンピュータにおける「病原体」とは「コンピュータウイルス」です。

人間に潜むウイルスや細菌と違い、「コンピュータウイルス」は悪意を持って人工的に作られます。

コンピュータウイルスに感染すると、データやプログラムが破壊されたり、機密情報を盗み取られたりします。コンピュータウイルスはIT社会において大変危険な存在です。

また、インターネットを通して国や企業などのシステムに侵入し、データを盗んだり破壊したりする行為も生まれました。このような行為を「**サイバー攻撃**」といいます。

情報セキュリティ

情報セキュリティとは、**情報資産をさまざまな脅威から保護**することです。

情報資産とは、個人情報や企業情報などのあらゆる情報を指しています。例えば、紙媒体やパソコン、サーバ、外付けストレージなどに保存しているすべてのデータは情報資源です。

情報セキュリティのリスク要因「**脅威**」といいます。情報セキュリティの脅威には、3つの種類があります。

* **人的脅威**
* **技術的脅威**
* **物理的脅威**

人的脅威  
人的脅威とは、**人間が原因となる脅威**です。意図的な不正アクセスのみならず、誤操作によるシステム障害といった人間のミスも人的脅威です。

主な人的脅威は以下のとおりです。順に説明します。

* クラッキング
* ソーシャルエンジニアリング

クラッキング  
クラッキング（Cracking）とは、**悪意を持ってコンピュータに侵入し、データを盗み見たり破壊する不正行為**です。

クラッキングではパスワードやIDを盗んだり、OSの脆弱性を狙ったりして、コンピュータに入り込みます。

ソーシャルエンジニアリング  
ソーシャルエンジニアリングとは、、情報通信技術ではなく**人間の心理的な隙や行動のミスを利用して秘密情報を手に入れること**です。

ソーシャルエンジニアリングには「**ショルダーハック**」や「**トラッシング**」などの例があります。

ショルダーハックとは、**IDやパスワード等を入力している人の肩越しにモニター画面やキーボードを盗み見して、秘密情報を得る行為**です。

トラッキングとは、**捨てられた記憶媒体や書類からIIDやパスワード等の秘密情報を盗み出す行為**です。

IT技術を必要としないので「だれでもできそう」なのがソーシャルエンジニアリングのポイントです

情報セキュリティにおけるソーシャルエンジニアリングの例として、適切なものはどれか。

技術的脅威

技術的脅威とは、**技術的な手段（不正プログラム）を使った脅威のことです。**

技術的脅威の裏には犯人（人間）がいるため人的脅威と区別しづらい面があります。「ソフトウェア」や「メール」、「パスワード特定」など不正行為の説明に情報技術を使う場面が出てきたら「技術的脅威」と考えてください。

主な技術的脅威は以下のとおりです。

* マルウェア
* ボット
* スパイウェア
* ランサムウェア
* トロイの木馬
* RAT
* フィッシング
* SPAMメール
* DoS攻撃
* 総当たり攻撃
* 辞書攻撃
* パスワードリスト攻撃
* クロスサイトスクリプティング
* セキュリティホール

「マルウェア」から順に説明します。

#### **マルウェア**

マルウェア（Malware）とは、**悪さをするソフトウェアの総称**です。

マルウェアの例

* コンピュータウイルス
* ボット
* スパイウェア
* ランサムウェア

#### **ボット**

ボット（Bot）とは、**外部からの遠隔操作を実行するプログラム**のことです。

ボットはロボットの略称で、自動投稿機能のような決まった操作を繰り返すプログラムを指すこともあります。一方情報セキュリティの関連語としてはパソコンを乗っ取るための不正プログラムという意味で使われます。

ボットに感染したパソコンは攻撃者の一斉命令を実行するので、迷惑メールを送信したり、サーバー攻撃をしたりと不正行為に加担させられる危険性があります。

#### **スパイウェア**

スパイウェア（Spyware）とは、利用者の知らないうちにインストールされ、利用者の許可なく個人情報の収集などを行うプログラムのことです。スパイウェアに感染すると、利用者が訪問したWebサイトやパスワードなどの個人情報が流出してしまいます。

#### **ランサムウェア**

ランサムウェア（Ransomware）とは、パソコン内のファイルやパソコンそのものを暗号化し利用者が使えないようにした後、元の状態に戻すための「身代金（ランサム）」を要求するソフトウェアです。

身代金目的の誘拐と同じく、金銭を払っても人質であるデータが正常復帰するとは限らないのが厄介な所です。

#### **トロイの木馬**

トロイの木馬とは、**有益であるように偽装してパソコンにインストールさせ、個人情報などを盗み出そうとするソフトウェアのことです。** です。トロイの木馬に感染すると、個人情報流出やクレジットカードの不正利用など、さまざまな被害を受けます。

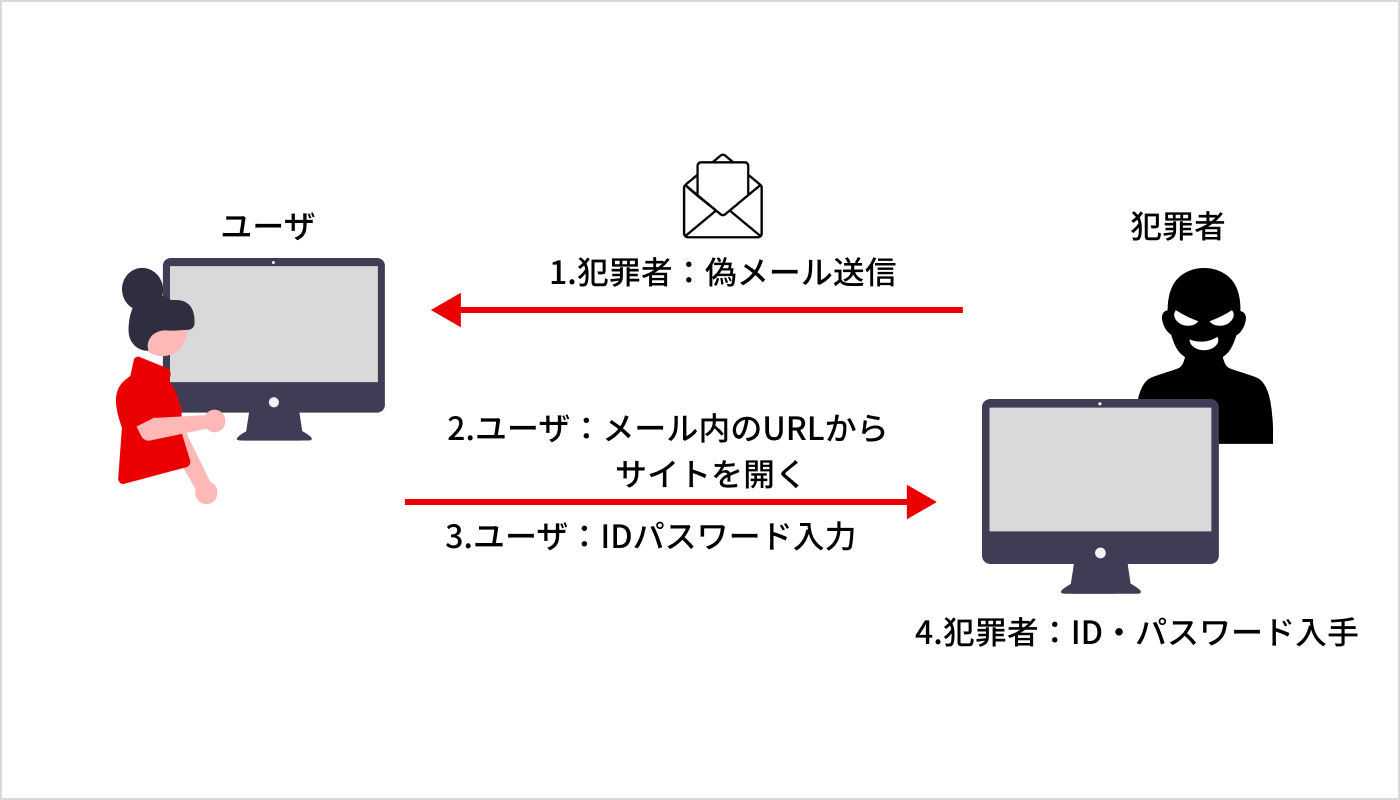
#### **RAT**

RAT（Remote Administration Tool / Remote Access Tool）とは、**パソコンを遠隔操作するマルウェア**です。

遠隔操作してくるマルウェアという点ではボットと似ています。しかしロボットのような単純で限定的な動きしかしないボットとは違い、RATは画面共有やWebカメラの操作など感染したパソコンの全アクセス権を乗っ取るという違いがあります。

また、不特定多数にばらまかれるボットに対して、少数のパソコンに感染するのがRATです。

#### **フィッシング**



フィッシング（Phishing）とは、**偽サイトに誘導して個人情報を取得しようとする不正行為**です。

例えば、フィッシングの犯人はクレジットカード会社を装って「アカウント情報を確認しないと取引が停止してしまう」というメールを送ります。ユーザーは慌ててメール内のURLをクリックし、開いたクレジットカード会社のサイトにパスワードやクレジットカードの番号などを入力するでしょう。

しかし、ここで開いたサイトは偽物で、IDやパスワード、クレジットカードの番号などを盗み取るために犯人が仕掛けたものだったのです。

この例のように、フィッシングにはメールが利用されることが多いです。

#### **SPAMメール**

SPAMメールとは、**受信者の許諾なしに無差別に送りつけられるメール**です。例えば、広告宣伝メール、架空請求メール、詐欺メール、なりすましメール、ウイルスメールなどがあります。

#### **DoS攻撃**

DoS攻撃（ディオーエス攻撃：Denial of Service Attack）とは、**1台のコンピュータから攻撃対象のWebサーバなどに対し、電子メール要求などを大量に送りつけてサービスを使えなくすること**です。

1台ではなく複数のコンピュータから大量にデータを送りつける「**DDoS攻撃**」という方法もあります。

#### **総当たり攻撃**

総当たり攻撃（Brute Force Attack）とは、**パスワード設定用の文字列を使ってすべての組み合わせを試し、パスワードを特定しようとする攻撃**です。例えば、パスワードが数字4桁のシステムの場合「0000～9999」までの1万とおりを自動入力します。

#### **辞書攻撃**

辞書攻撃（Dictionary Attack）とは、**辞書の単語や人物の名前などの組み合わせをすべて試して、パスワードを割り出す攻撃**です。パスワードリスト攻撃  
パスワードリスト攻撃（List Based Attack）とは、**別サービスを攻撃して入手したIDとパスワードの一覧を使って、不正アクセスする攻撃**です。IDやパスワードを使いまわしている場合、この攻撃の対象になる可能性があります。

#### **クロスサイトスクリプティング**

クロスサイトスクリプティング（Cross Site Scripting）とは、**悪サイト運営者とは関係ない第三者が悪意のあるスクリプトをサイト内に埋め込み、個人情報などを取得しようとする攻撃のことです。**。

悪意のあるスクリプトをサイトに埋め込むことで、以下のような行為が可能です。

* ユーザーを偽の会員サイトに自動で転送させ、パスワードを盗む
* 別のサイトにユーザーの**cookieを送信、cookieを盗む**
* 本物のサイトの上に偽のサイトを表示させ、偽情報を流す

#### **セキュリティホール**

セキュリティホール（Security Hole）とは、**コンピュータシステムやネットワークに存在する「弱点」や「欠陥」のこと**です。セキュリティホールを放置すると、不正アクセスされやすくなります。

物理的脅威  
物理的脅威とは、**物理的な手段によって施設や機器などが直接損害を受ける脅威**です。

例えば、盗難、停電、破壊、災害などがあります。

また、次の事例は人的脅威と混同しがちです。

「サーバー室に侵入者があり、データを盗まれた」

**これは、サーバーという物理対象に対する盗難なので物理的脅威となります。**

まとめ  
  
・情報セキュリティとは、情報資産を様々な脅威から保護すること

・情報セキュリティに関する脅威には、人的脅威・技術的脅威・物理的脅威の3種類がある

| **用語** | **説明** |
| --- | --- |
| 人的脅威 | 人が原因となる脅威 種類は以下のとおり ・クラッキング ・ソーシャルエンジニアリング |
| クラッキング（Cracking） | 悪意を持ってコンピュータに侵入し、データを盗み見たり、破壊したりする不正行為 |
| ソーシャルエンジニアリング | 情報通信技術ではなく人間の心理的な隙や行動のミスを利用して秘密情報を手に入れること |
| 技術的脅威 | 技術的な手段（不正プログラム）を使った脅威 種類は以下のとおり ・マルウェア ・ボット ・スパイウェア ・ランサムウェア ・トロイの木馬 ・RAT ・フィッシング ・SPAMメール ・DoS攻撃 ・総当たり攻撃 ・辞書攻撃 ・パスワードリスト攻撃 ・クロスサイトスクリプティング ・セキュリティホール |
| マルウェア（Malware） | 悪さをするソフトウェアの総称 |
| ボット（Bot） | **外部からの遠隔操作を実行するプログラム** **できることは限定的** |
| スパイウェア（Spyware） | 知らないうちにインストールされ利用者の許可なく個人情報などを収集するプログラム |
| ランサムウェア（Ransomware） | パソコンなどを使用不能にしておき、元の状態に戻すための身代金を要求するソフトウェア |
| トロイの木馬 | 有益であるように偽装してコンピュータに侵入するソフトウェア |
| RAT（Remote Administration Tool / Remote Access Tool） | パソコンを遠隔操作するマルウェア パソコンの全機能にアクセスできる |
| フィッシング（Phishing） | **偽サイトに誘導して個人情報を取得しようとする不正行為** |
| SPAM | 受信者の承諾なしに無差別に送りつけられるメール |
| DoS攻撃（Denial of Service Attack） | 電子メール要求などを大量に送りつけてサービスを使えなくすること |
| 総当たり攻撃（Brute Force Attack） | 「すべての組み合わせ」を試して、パスワードを特定しようとする攻撃 |
| 辞書攻撃（Dictionary Attack） | **辞書の単語や人物の名前などの組み合わせをすべて試して、パスワードを割り出す攻撃** |
| パスワードリスト攻撃（List Based Attack） | 別サービスを攻撃して入手したIDとパスワードの一覧を使って不正アクセスする攻撃 |
| クロスサイトスクリプティング（Cross Site Scripting） | 第三者が悪意のあるスクリプトをサイトに埋め込むことでcookieなどを盗み出す攻撃 |
| セキュリティホール（Security Hole） | コンピュータシステムやネットワークに存在する「弱点」や「欠陥」のこと 放置することで不正アクセスされやすくなる |
| 物理的脅威 | 物理的な手段によって施設や機器などが直接損害を受ける脅威 種類は以下のとおり ・盗難 ・停電 ・破壊 ・災害 |

リスクマネジメント

企業を取り巻く環境には、経営資源を脅かすさまざまなリスクが潜んでいます。あらゆるリスクを事前に洗い出し、適切に対処するのが「**リスクマネジメント**」です。

また、企業にとって「情報」は大切な経営資源です。企業では、経営情報や財務情報などさまざまな情報を扱います。これらの情報を守るのが「**情報セキュリティマネジメント**」です。

「情報セキュリティマネジメント」は「リスクマネジメント」の中に含まれる概念です。

リスクマネジメント（Risk Management）とは、**「組織活動のあらゆるリスク」を特定・分析・評価し、最小限の費用でリスク対応するための手法**です。

マネジメント系では「プロジェクトリスクマネジメント」を学習しましたが、対象範囲が異なります。

プロジェクトリスクマネジメントは「**プロジェクトにおけるリスク**」が対象であるのに対し、リスクマネジメントは「**組織活動のあらゆるリスク**」が対象です。

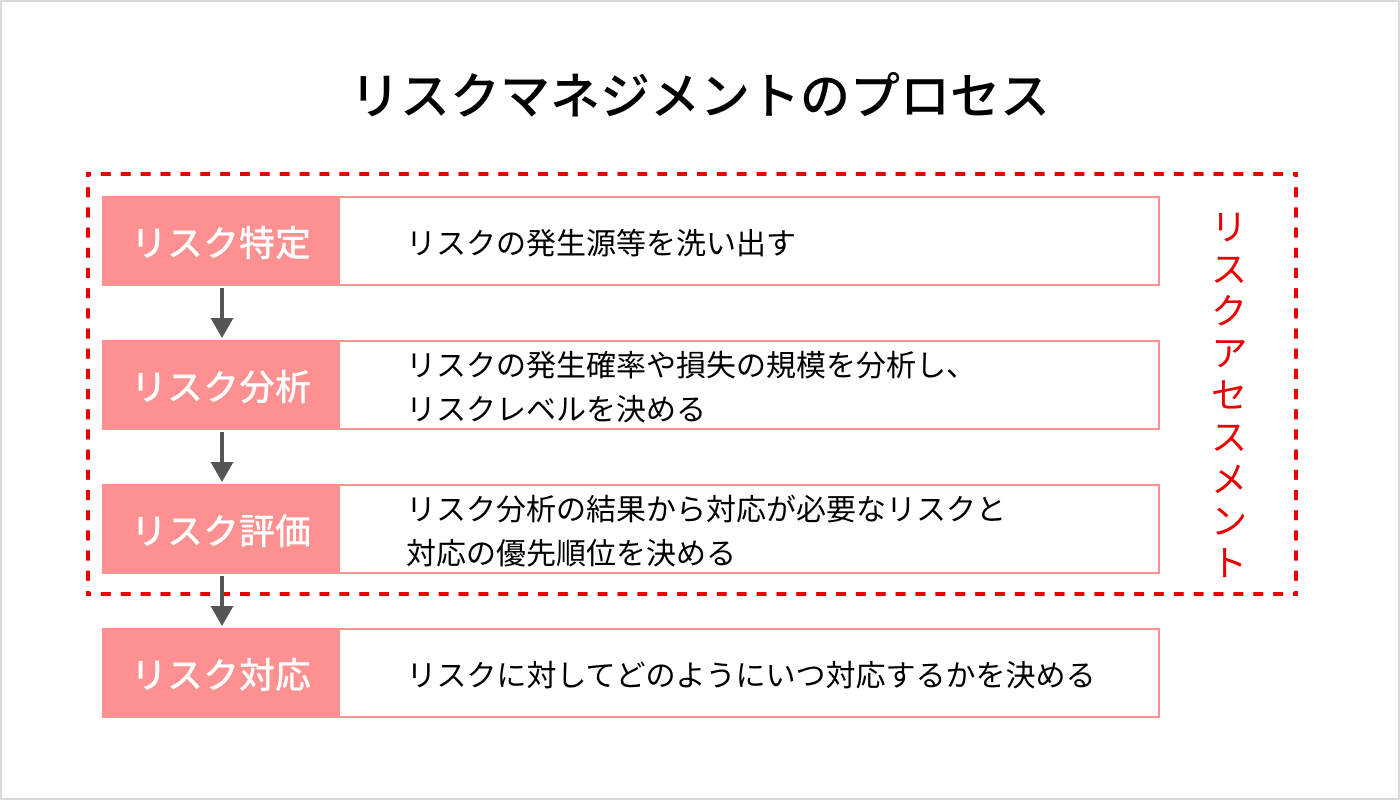
#### **リスクマネジメントの必要性**

企業活動には、さまざまなリスクが想定されます。しかし、すべてのリスクに対して対策を講じていては、費用が膨大にかかります。

ここで必要なのがリスクマネジメントです。リスクマネジメントでは、リスク対応のコストパフォーマンスを上げるために、4つのプロセスを実行します。

#### **リスクマネジメントのプロセス**

リスクマネジメントには、「**リスク特定**」「**リスク分析**」「**リスク評価**」「**リスク対応**」の4つのプロセスがあります。各プロセスの流れは、以下のとおりです。



「リスク特定」「リスク分析」「リスク評価」を合わせて、「**リスクアセスメント**」といいます。

「リスク対応」はリスクアセスメントに入っていない点に注意しましょう。

### **4つのリスク対応策**

リスクマネジメントの4つ目である「リスク対応」では、特定したリスクに対して **「①どのような対処を」「②いつまでに行うか」** を決めます。

リスク対応には、4つの方法があります。

| **リスク対応策** | **説明** |
| --- | --- |
| リスク回避 | リスクの要因を取り去って、**リスクが発生する可能性を除去する**こと |
| リスク低減 | 情報セキュリティ対策をして**リスク発生率を下げる**こと |
| リスク移転 | **保険をかけるなどして、リスクを他社に肩代わりしてもらうこと** |
| リスク受容 | 起こりうるリスクは許容範囲内とし、**何もせず受け入れること** |

プロジェクトリスクマネジメントで学習した4つの対応策とほとんど同じといえます。

異なる点は、以下のとおりです。

* プロジェクトリスクマネジメントは、**プロジェクトを行う場合のリスク対応策**
* リスクマネジメントは、**経営資源に対するリスク対応策**

また、プロジェクトマネジメントでは「リスク**軽**減」と呼ばれていた概念が、リスクマネジメントでは「リスク**低**減」と呼ばれている点にも違いがあります。

## **情報セキュリティマネジメントを学ぼう**

情報は会社にとって重要な経営資源の一つです。情報をそのまま保存しておくと、悪意ある第三者に盗まれる危険性もあるため対策が必要です。

情報セキュリティマネジメントとは、**組織的、体系的に情報を守るための管理手法**です。

具体的には、企業情報や個人情報、情報を扱うシステムを守ることになります。情報セキュリティマネジメントは、情報を守る金庫のようなものと考えてください。

情報セキュリティマネジメントは、前述したリスクマネジメントに含まれる要素です。情報セキュリティマネジメントの費用対効果を考えながら実装する枠組みに「ISMS」があります。

### **ISMS**

ISMS（Infomation Security Management System：情報セキュリティマネジメントシステム）とは、**組織の情報資産が「機密性」「完全性」「可用性」の3つを維持できるようにするための枠組みのこと**です。

ここでいう「情報資源」とは、企業情報や個人情報など、あらゆる情報を指しています。

情報セキュリティマネジメントを行うにもさまざまな方法があり、それぞれに対して費用が掛かってきます。そこでコストパフォーマンスの良い対策を適時選択していく必要があります。

ISMSは情報セキュリティマネジメントの対費用効果を考慮しつつ、情報を守っていくための枠組みです。

#### **ISMSにおけるPDCA**

情報を取り巻く環境は、日々進化しています。パソコンのセキュリティソフトを起動したときに、「ウイルスファイル定義を更新してください」と表示されたことはありませんか。

これは、毎日のように新しいマルウェアが誕生しているからです。

情報セキュリティ対策は一度行えば、それでよいというものではありません。新しい脅威に対応できるよう、対策を見直していくプロセスが必要になります。

ISMSではPDCAサイクルによって、情報セキュリティ対策の見直し・改善を行います。

| **PDCAサイクル** | **ISMSで実施する内容** |
| --- | --- |
| **P（Plan：計画）** | ISMSの**目標、方針の策定** |
| **D（Do：実行）** | ISMSの**導入**と**運用** |
| **C（Check：点検）** | ISMSの**監視**とレビュー |
| **A（Act：処置）** | ISMSの**是正、改善** |

ITパスポート試験では、ISMSにおけるPDCAの各段階でどのような内容を実施するのかが出題されます。またPDCAの内容から、どの段階を指しているのか選択する問題も出ます。

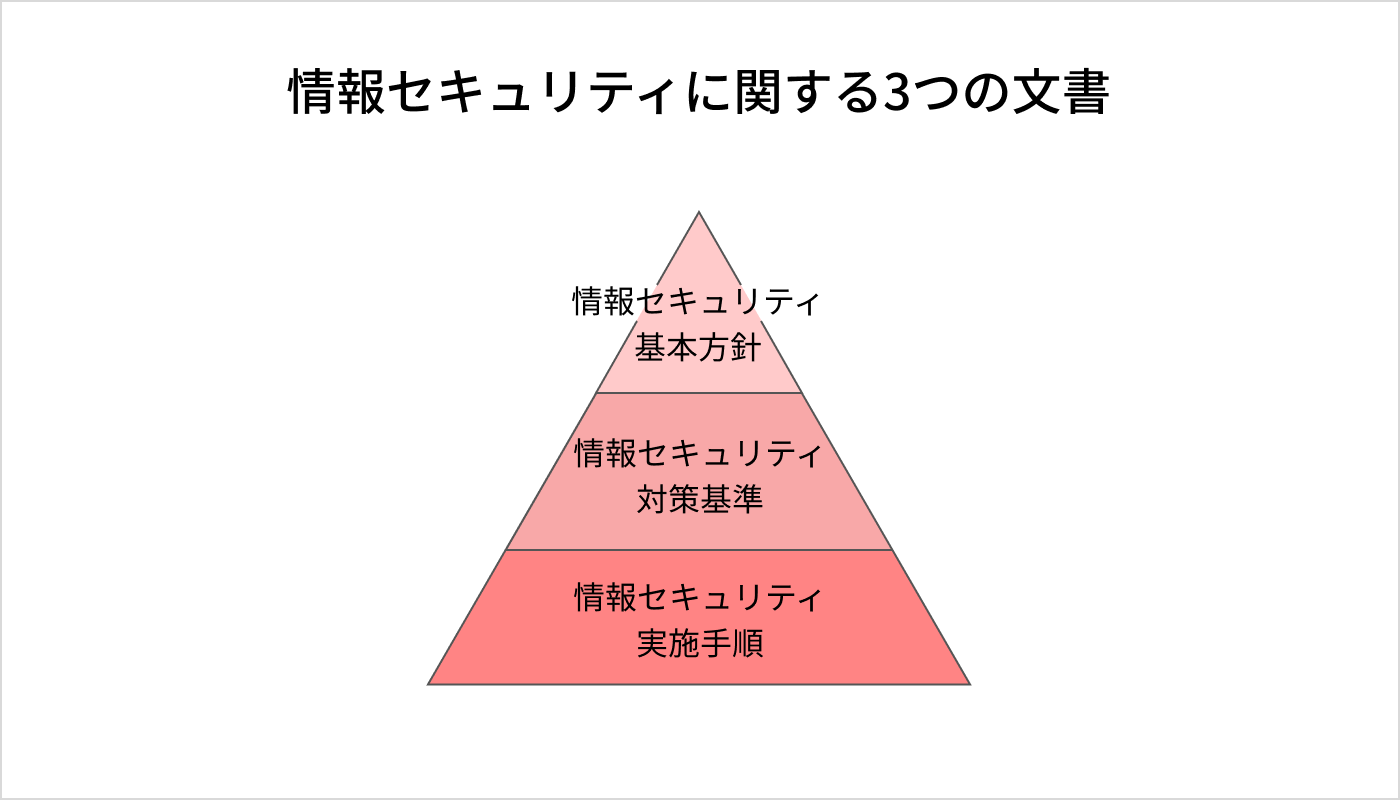
### **情報セキュリティポリシ**

ISMSにおけるPDCAサイクルの「Plan」にあたるのが、情報セキュリティポリシの策定です。

情報セキュリティポリシとは、**情報セキュリティに関する目標、組織の姿勢、具体的な実施手順などをまとめた文章**です。

情報セキュリティポリシは、次の3つの文章で構成されます。

* 情報セキュリティ基本方針
* 情報セキュリティ対策基準
* 情報セキュリティ実施手順



三角形の下になるほど、より具体的で詳細な文章になります。

情報セキュリティ基本方針から順に説明します。

#### **情報セキュリティ基本方針**

情報セキュリティ基本方針とは、**情報セキュリティに関する組織の基本的な方針や取り組み姿勢を示す文章**です。

これは、企業の経営層が策定します。情報セキュリティ基本方針は、企業のトップ層がすべての従業員と社外の利害関係者に対して、情報セキュリティに関してどのような方針をとっていくのかを公表するための文章です。

公表することで、組織が情報セキュリティに対して本格的に取り組んでいるということを社内外に示せます。

情報セキュリティ基本方針もPDCAの対象となりますが、見直しの結果内容を改定した場合もう一度社内外に知らせる必要があります。

#### **情報セキュリティ対策基準**

情報セキュリティ対策基準とは、**情報セキュリティにおける目標を達成するための一般規則集**です。情報セキュリティ対策基準では、一般的なルールを決めます。

情報セキュリティ対策で **「何をするのか＝What」** を具体化したものです。この文章は、情報セキュリティ基本方針に基づいて作成します。

具体的には、「人事規定」「就業規則」が挙げられます。

#### **情報セキュリティ実施手順**

情報セキュリティ実施手順とは、**情報セキュリティ対策基準を守るために実施すべき具体的な行動を明らかにした手順書**です。この文章は、情報セキュリティ対策基準に基づいて作成します。

実施手順書では情報セキュリティ対策を「**どのように行うのか＝HOW**」を記述します。文章の作成や管理は、各部門の役割となります。

なお、情報セキュリティ実施手順は、社外秘となります。情報を守る手順が悪意のある人に知られると、手順をすり抜けた攻撃を仕掛けられかねないからです。

次に、「情報セキュリティポリシ」と一緒に出題されやすい「サイバーセキュリティ基本法」について解説します。

##### **サイバーセキュリティ基本法**

サイバーセキュリティ基本法とは、**サイバー攻撃から国を守るための基本理念を定めた法律**のことです。

国、地方公共団体や教育機関などの責務だけでなく、**国民の努力義務**について定めていることにも注意しましょう。

ITパスポート試験では、「情報セキュリティポリシ」と「サイバーセキュリティ基本法」の違いについて出題されます。

* 情報セキュリティポリシは企業を対象とした「**ローカルルール**」
* サイバーセキュリティ基本法は国民すべてにかかわる「**法律**」

次に、情報セキュリティマネジメントの三大特性について説明します。

### **情報セキュリティにて維持・管理すべき３つの特性**

情報セキュリティでは、情報資源の「何を」守るかをしっかり意識しておくことが大事です。**ISMSでは**情報資源について維持・管理すべき特性として **「機密性」「完全性」「可用性」** の３つを挙げています。

| **特性** | **説明** |
| --- | --- |
| **機密性（Confidentially）** | アクセスする許可を持つ人だけが情報を閲覧できること |
| **完全性（Integrity）** | 情報が正しく、改ざん、破壊されていないこと |
| **可用性（Availability）** | ユーザーが必要とするとき、問題なく情報にアクセスできること |

例えば、試験では以下のような問題が出題されます。

・次の情報セキュリティに係る事象において、機密性、完全性及び可用性のうち、損なわれたものだけをすべて挙げたものはどれか。

職場のファイルサーバにおいて、サーバ上のファイルをすべて暗号化して保存していたが、サーバがウイルスに感染し、一部のファイルが削除されてしまった。ウイルスの駆除とファイルの復旧に数時間を要し、その間は業務が行えない状態となり、利用者に迷惑をかけてしまった。  
ア 機密性  
イ 機密性，完全性  
ウ 完全性，可用性  
エ 可用性  
「出典：平成29年度 秋期分 ITパスポート試験 問90」

**正解は「ウ」です。**

* 「サーバがウイルスに感染し、一部のファイルが削除されてしまった」→情報が改ざん、破壊されてしまったので**完全性**が損なわれた。
* 「その間は業務が行えない状態となり、利用者に迷惑をかけてしまった」→利用者が必要な時に使えないので**可用性**が損なわれた。

このように、実際の試験では「完全性」と「可用性」について具体例が問われることが多いです。ただし、どのような具体例が出題されるかは予想できません。

過去問に登場する具体例そのものを覚えるのではなく、３つの特性の意味から正解を導けるようにしましょう。

ここまでは、情報セキュリティで維持すべき3つの特性について学んできました。次は、人が不正を働く場合について学習します。

#### **不正のトライアングル**

不正のトライアングルとは、**「機会」「動機」「正当化」の3つの条件がそろった時に不正行動が生まれるという理論**のことです。

実際のITパスポート試験では、3つの条件が何であるかが問われます。

企業での内部不正などの不正が発生するときには、"不正のトライアングル"と呼ばれる3要素のすべてがそろって存在すると考えられている。"不正のトライアングル"を構成する3要素として、最も適切なものはどれか。

ア　機会，情報，正当化  
イ　機会，情報，動機  
ウ　機会，正当化，動機  
エ　情報，正当化，動機

「出典：平成31年度 春期分 ITパスポート試験 問65」

**正解は「ウ」です。**

この問題のように、不正のトライアングル問題では選択肢に「情報」というキーワードがたびたび現れます。

ITパスポート試験は情報に関する分野が頻出するので、「情報」は正しい選択肢に見えてしまいます。

しかし、不正のトライアングルはもともと組織犯罪研究から生まれたものであり、情報犯罪に特化した言葉とはいえません。

例えば、デスクに置きっぱなしの札束を横領するとき、情報は必ずしも不正に必要な要素とはいえないでしょう。このような偽のキーワードにだまされないように注意してください。

まとめ

リスクマネジメントと情報セキュリティマネジメントについて学びました。試験に出題されやすい用語は、以下のとおりです。

* リスクマネジメントとは、**組織活動のあらゆるリスクを特定・分析・評価し、最小限の費用でリスク対応するための手法**
* 情報セキュリティマネジメントとは、**組織的、体系的に情報を守るための管理手法**

| **用語** | **説明** |
| --- | --- |
| リスクマネジメントの4つのプロセス | リスク特定→リスク分析→リスク評価→リスク対応 |
| ISMS（Infomation Security Management System） | 情報セキュリティマネジメントシステムのこと 組織の情報資産について「機密性」「完全性」「可用性」を維持するための枠組み |
| PDCA | 改善プロセスのこと Plan（計画）、Do（実行）、Check（点検）、Act（処置）を繰り返し実施する |
| 情報セキュリティポリシ | 情報セキュリティに関する組織の取り組みや対策をまとめた文章のこと 具体的には「情報セキュリティ基本方針」「情報セキュリティ対策基準」「情報セキュリティ実施手順」の3つの文章からなる |

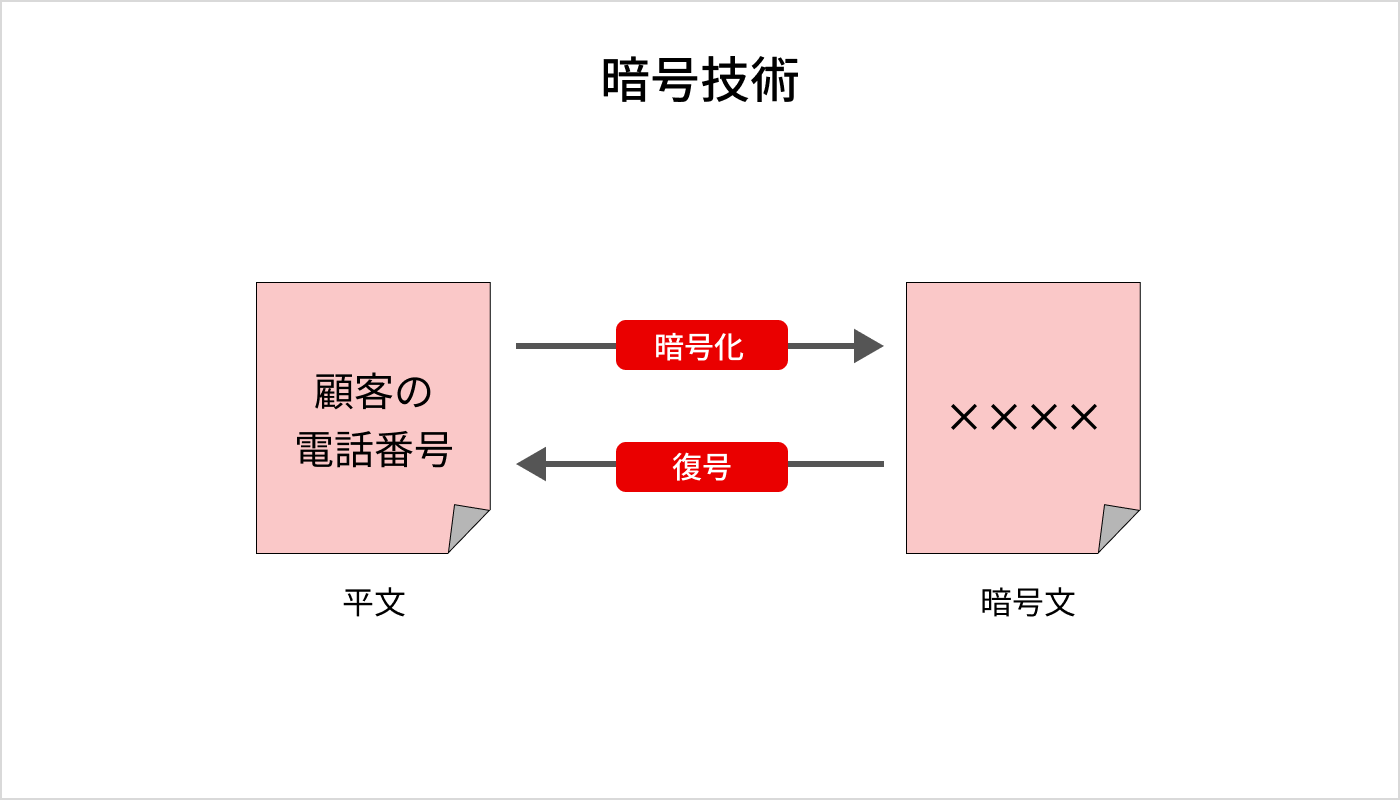
暗号技術  
暗号技術とは、**データを他人に読まれないよう変換する技術**です。

暗号化する前のデータは、平文と呼びます。平文は誰でも読めるため、情報が盗まれやすいです。

例えば、社外秘の顧客情報を平文で送ると、悪意のある人に盗み取られてしまうかもしれません。

このような危険を避けるためには、情報の受け手のみが内容を読めるようにする暗号技術が必要です。  
平文を暗号文にすることを「**暗号化**」といいます。逆に、暗号文を平文に戻す場合は「**復号（ふくごう）**」といいます。

ITパスポート試験では「復号**化**」とはいわず、「**復号**」というので注意してください。



HDDやSSDなど、補助記憶装置に保存されているデータ全部を暗号化することを「**ディスク暗号化**」といいます。

一方、ファイルを暗号化することを「**ファイル暗号化**」といいます。

次は、暗号技術の一種である「共通鍵暗号方式」と「公開鍵暗号方式」についての説明です。

### **共通鍵暗号方式**

共通鍵暗号方式とは、暗号化するときも複合するときも**同じ鍵を使う暗号化方式**です。

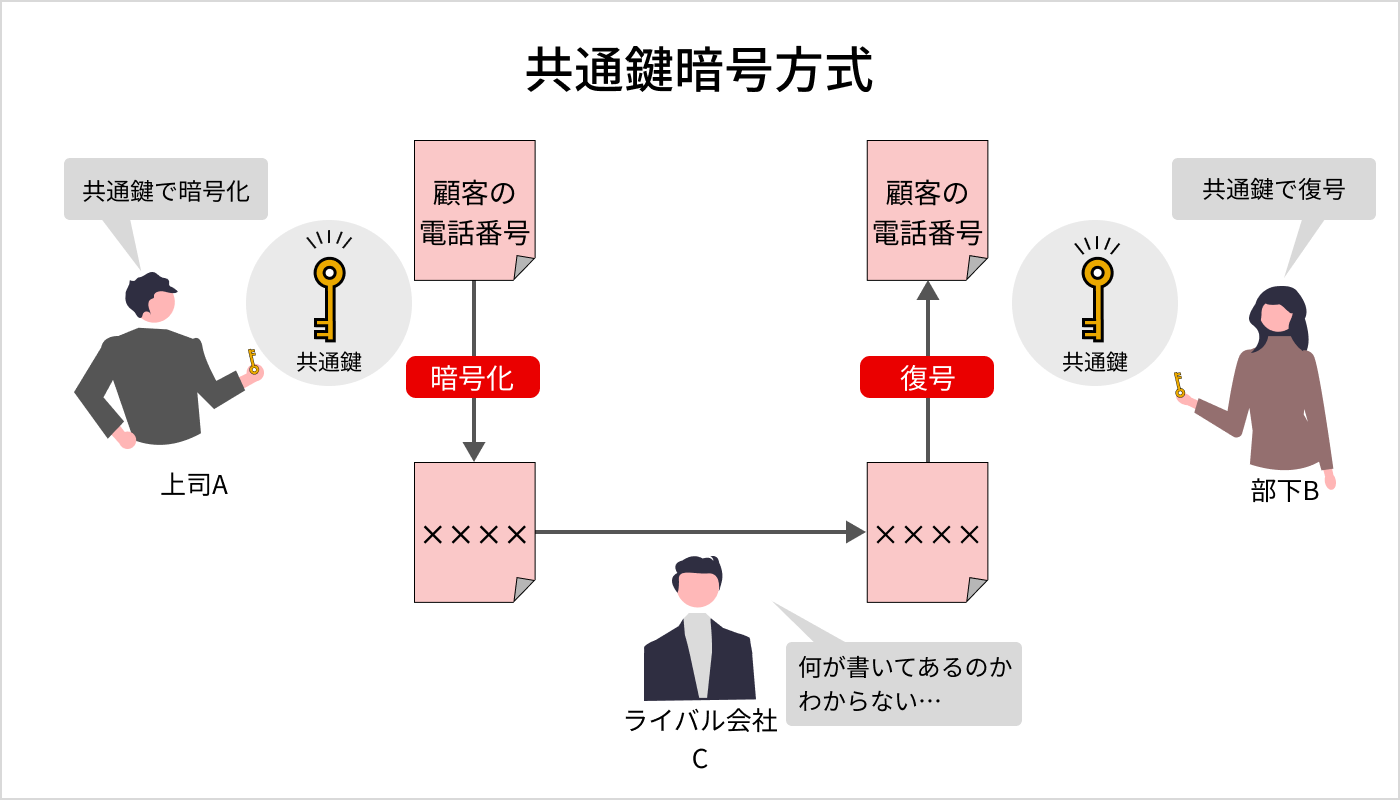
これは、金庫などの鍵のイメージと同じです。

扉を開けるときも、閉めるときも同じ鍵を使っていますね。

では共通鍵暗号方式の具体例として、部下Bさんに顧客の電話番号を送りたい上司Aさんの場合を考えてみましょう。

まず、AさんはBさんに共通鍵を送って共有しておきます。その後Aさんは平文の電話番号を共通鍵で暗号化し、Bさんに送ります。

Bさんは共通鍵で電話番号を復号します。共通鍵を持っていないライバル会社のCさんは、送信される電話番号を読み取れません。



#### **共通鍵暗号方式の欠点**

共通鍵暗号方式の欠点は、**共通鍵を送るときに盗まれる危険性が高い**ことです。

共通鍵暗号方式で暗号化されたデータは、鍵を持っている人なら誰でも複合が可能です。つまり第三者に鍵を奪われることなく、情報の受け手にのみ共通鍵を渡せるかどうかが重要なのです。

ところが、共通鍵を安全に送るのはかなり難しいです。鍵をメールで送ればそのメールが盗聴されるかもしれません。郵送しても、紛失・盗難リスクがあります。

このように共通鍵暗号方式には **「鍵を安全に受け渡ししづらい」** という致命的な欠点が存在するのです。

### **公開鍵暗号方式**

公開鍵暗号方式とは、暗号化するときの鍵と複合するときの鍵を分ける暗号化方式です。暗号化するときの鍵を **「公開鍵」**、復号するときの鍵を **「秘密鍵」** といいます。

公開鍵暗号方式で使用する「公開鍵」と「秘密鍵」の違いは、下表のとおりです。

| **種類** | **説明** |
| --- | --- |
| **公開鍵** | 誰でも入手できる複製可能な鍵 **暗号化**するときに使用する |
| **秘密鍵** | 自分だけが持っている1つしかない鍵 **復号**するときに使用する |

第三者に盗まれてはいけないはずの鍵が「誰でも入手できる」、この逆転の発想が公開鍵暗号方式の大きな特徴です。

#### **公開鍵暗号方式の仕組み**

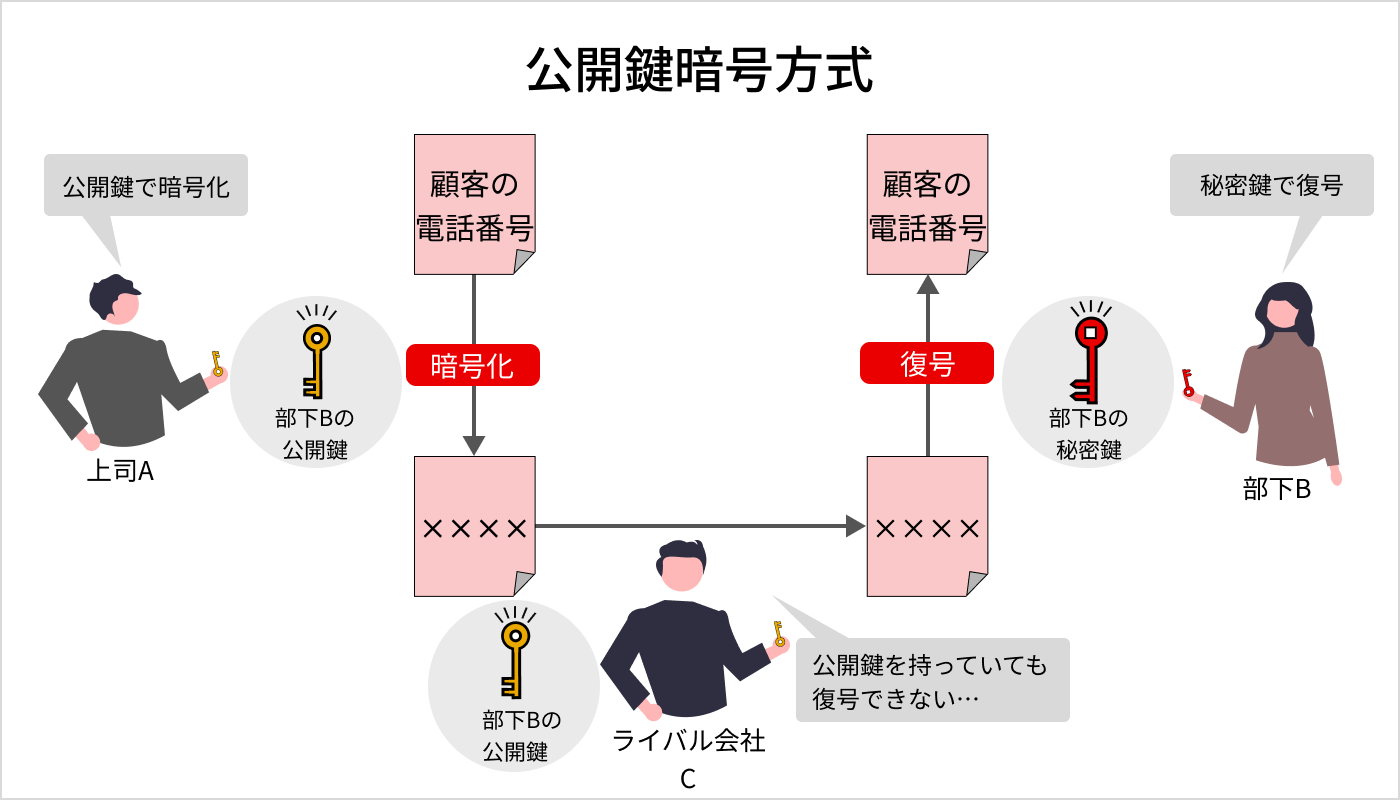
ここからは、公開鍵暗号方式の仕組みを解説します。

公開鍵暗号方式の最大のポイントは、「公開鍵と秘密鍵がペアになっている」という点です。

公開鍵は秘密鍵から作られます。**そして公開鍵で暗号化された文章は、公開鍵のペアになっている秘密鍵でしか復号できません。**

ここで具体例をみてみましょう。上司Aさんから部下Bさんへ顧客の電話番号を送るときに、公開暗号鍵方式を使うとします。

1. Bさんは秘密鍵から公開鍵を作る
2. Bさんは公開鍵を公開し、秘密鍵は自分の手元で保管する
3. AさんはBさんの公開鍵を使って顧客の電話番号（平文）を暗号化し、Bさんに送る
4. Bさんは秘密鍵を使ってAさんの暗号を復号し、顧客の電話番号を手に入れる



ここでライバル企業のCさんが、Aさんの作ったBさん宛ての暗号を盗んだとしましょう。

Bさんの公開鍵は誰でも手に入れられるので、Cさんも入手しています。しかし、CさんはBさんの秘密鍵を持っていないので盗んだ暗号を復号できません。

Cさんにできるのは、「Bさんのみが復号できる暗号を作ること」だけです。

| **人物** | **持っている鍵** | **できること** |
| --- | --- | --- |
| 上司Aさん（送り手） | Bさんが作った公開鍵 | 平文の暗号化のみ |
| 部下Bさん（受け手） | Bさんが作った公開鍵と秘密鍵 | 平文の暗号化と復号 |
| ライバルCさん | Bさんが作った公開鍵 | 平文の暗号化のみ |

ここで注目してほしいのが、共通鍵暗号にとってネックだった「鍵の受け渡しプロセス」が登場しない点です。**公開鍵暗号方式では、復号に必要な秘密鍵を送信する必要がありません。**

Bさんの秘密鍵は誰の目にも触れず、Bさんのみが管理できます。その一方でBさんのみが復号できる暗号は、誰もが作成できるのです。

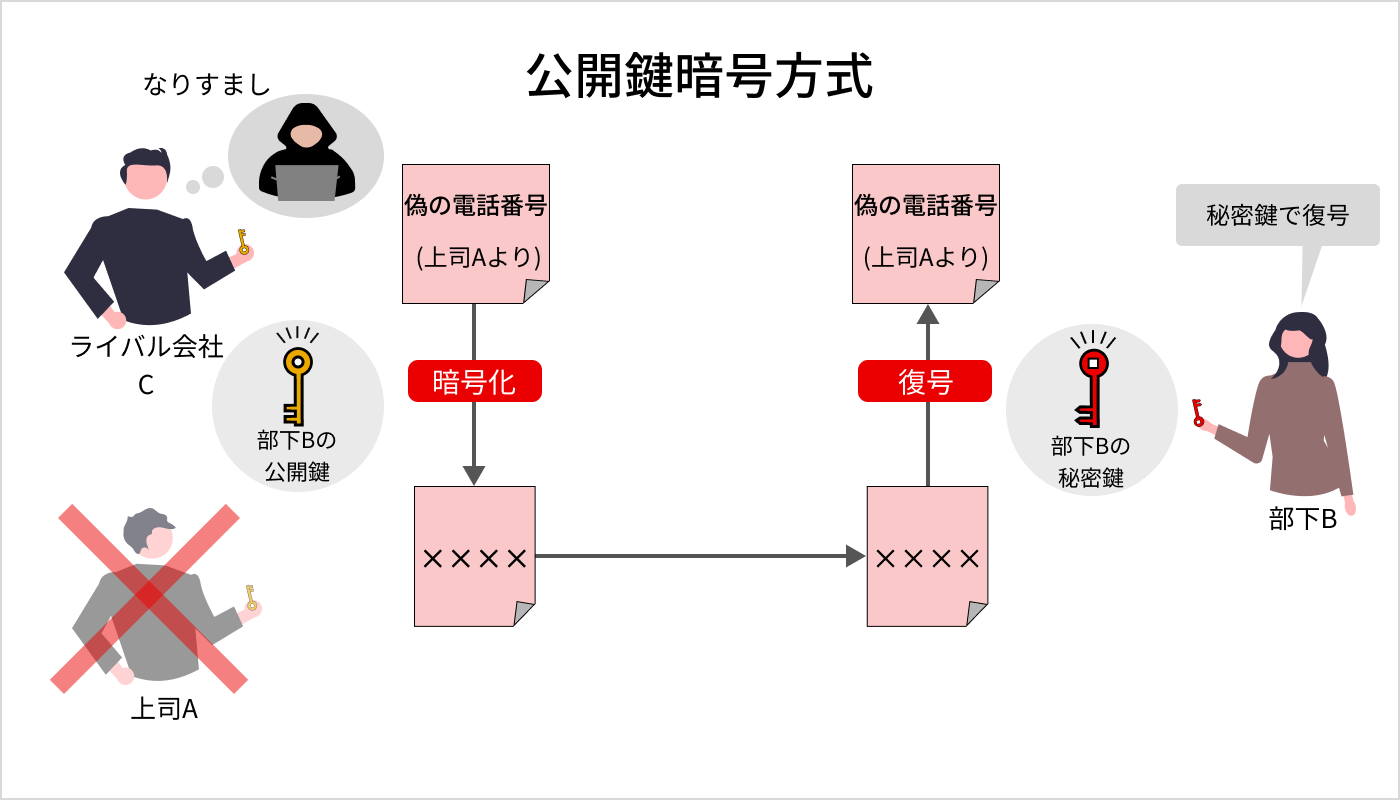
このように公開鍵暗号方式は、共通鍵暗号方式の欠点を克服した暗号方式です。

#### **公開鍵暗号方式の欠点**

公開鍵暗号方式は、**誰でも暗号化できるため**「**なりすまし**」の危険性があります。

例えば、ライバル会社のCさんが上司Aさんになりすまし、でたらめな電話番号を顧客のものと偽って部下Bさんに送ることも可能です。

BさんはAさんからメッセージを受け取ったと思い込み、メッセージを復号。偽の電話番号を顧客のデータベースに書き込んでしまう、そんなこともあり得るのです。



このような「なりすまし」を防ぐ技術が「**ディジタル署名**」です。

ディジタル署名の技術を使えば、差出人が本人であることを証明することが可能です。

ディジタル署名に関しては、[25章](https://terakoya.sejuku.net/programs/121/chapters/1509)で詳しく説明します。

また、公開鍵暗号方式には、共通鍵暗号方式と比較して暗号化と復号に時間がかかるという欠点があります。この欠点を補えるのが、**ハイブリッド暗号方式**です。

##### **ハイブリッド暗号方式**

ハイブリッド暗号方式とは、**共通鍵暗号方式と公開鍵暗号方式の両方を組み合わせた暗号化方式のこと**です。

「ハイブリッド暗号方式」では、平文自体は「共通鍵」で暗号化します。その後「共通鍵」を「公開鍵」で暗号化します。そして **「暗号化した平文」と「暗号化した共通鍵」** を相手に送るのです。

受信者は**秘密鍵で共通鍵を復号した後、その共通鍵で平文を復号**します。

こうすれば、共通鍵を安全に受け渡しできる上、復号の速度も早くなります。

「ハイブリッド暗号方式」は、共通鍵暗号方式の高速である点と公開鍵暗号方式の安全である点をあわせもっています。

まとめ

・暗号化技術とはデータを他人に読まれないよう変換する技術のこと

・共通鍵暗号化方式とは、暗号化と復号で同じ鍵を使う暗号化方式のこと

・公開鍵暗号方式とは、公開鍵と秘密鍵の２つの鍵を使う暗号化方式のこと

・共通鍵 共通鍵暗号方式で暗号化と復号時に使用する共通の鍵

・公開鍵 公開鍵暗号公式で暗号化するときに使用する鍵、誰でも入手が可能でいくつでも複製できる

・秘密鍵　公開鍵暗号化で復号するとき使用する鍵、公開鍵作成者（復号する人）のみが所有している鍵

## **ディジタル署名と認証局**

暗号化された文章が「信頼のおける人物」から送信されたものであることを証明するために利用されるのが「ディジタル署名」です。

### **ディジタル署名**

ディジタル署名とは、**データに電子的な署名を行い内容が改ざんされていないと証明する技術のこと**です。

ディジタル署名が使われるのは、インターネットを利用して文章を送るときです。

#### **ディジタル署名の利用シーン**

ディジタル署名は、**インターネットを通じて見積書や請求書を送るとき**に使用します。

このようなインターネット上のデータが「信頼できる人」から送られていることを示すために、印鑑やサインの代わりに「**ディジタル署名**」を使うのです。

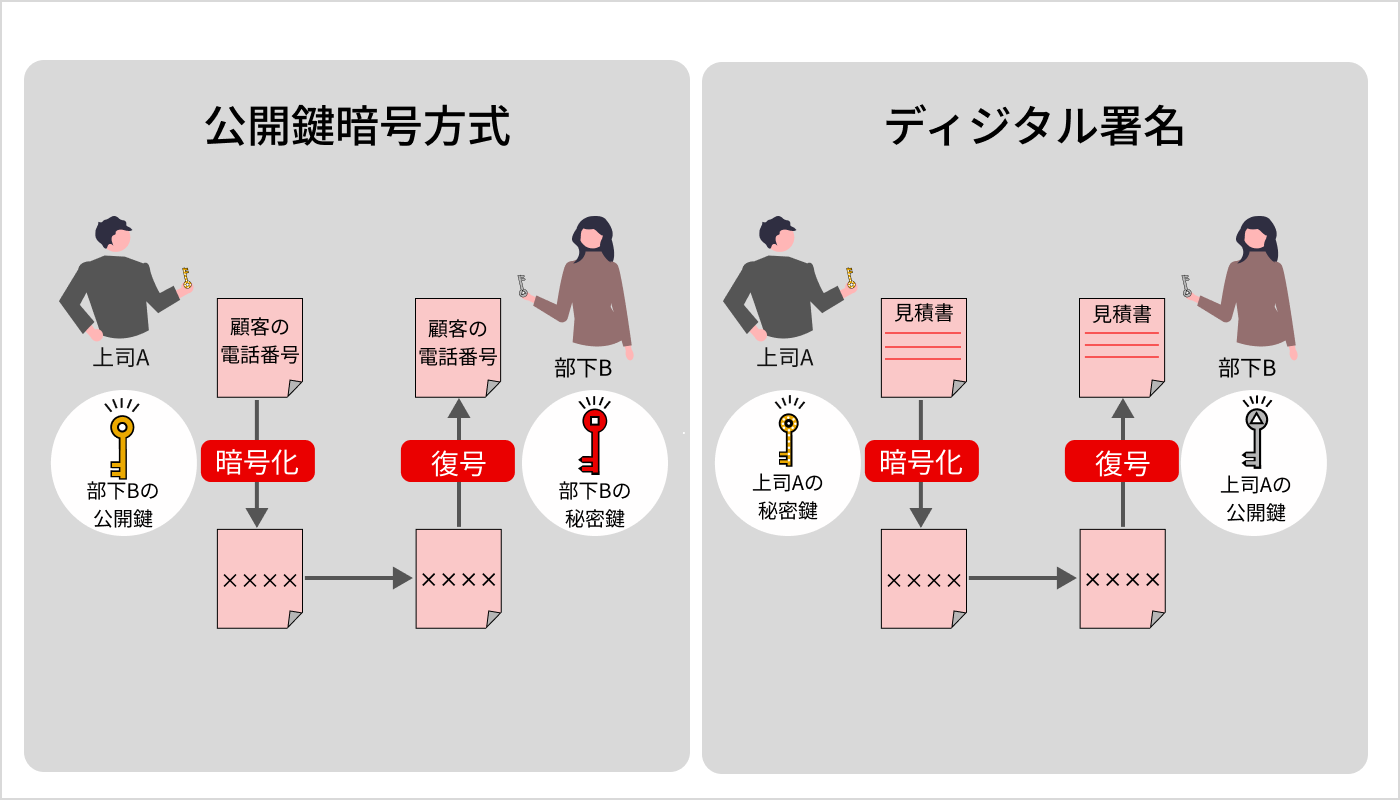
ディジタル署名に使われているのは、前章で登場した**公開鍵暗号方式**の応用技術です。

公開鍵暗号方式には、次のような特徴があります。

**・公開鍵で暗号化された文章は、ペアになっている秘密鍵でしか復号できない**

一方ディジタル署名で使われる技術には、次の特徴があります。

**・秘密鍵で暗号化された文章は、ペアになっている公開鍵でしか復号できない**



図を見ると、暗号化と復号で使う鍵が反対になっているのが分かります。

受信者のBさんは、Aさんの公開鍵で暗号を復号できたので「この暗号はAさんが作ったのだ」と分かるという仕組みです。

もし第三者の秘密鍵で作った暗号だった場合、Aさんの公開鍵で復号できないからです。

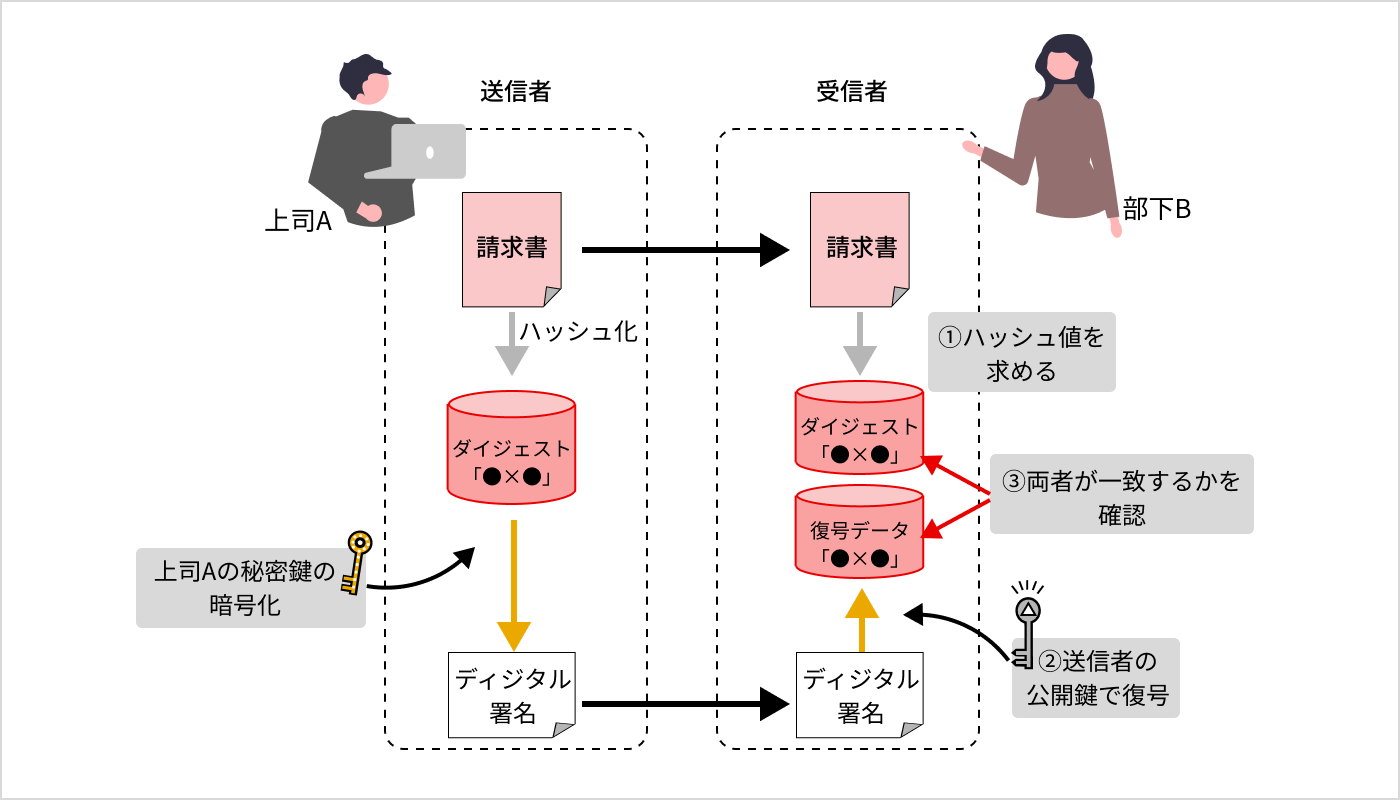
#### **ディジタル署名とハッシュ関数**

実際のディジタル署名では、**ハッシュ関数**という仕組みを使います。ハッシュ関数は、任意の文字列を**ダイジェスト**という一定の文字列に変換（ハッシュ化）します。

同じ文字列を、同じハッシュ関数を使ってハッシュ化すると、**その値は一致**します。また、**一度ハッシュ化した文字列は元に戻せません。**

では、ディジタル署名の技術を使い、請求書を送信する例を見てみましょう。

1. 送信者のAさんは請求書（平文）をハッシュ化し、**ダイジェスト**を作る
2. Aさんはダイジェストを**Aさんの秘密鍵**で暗号化する
3. 暗号化されたダイジェストを**署名**として請求書とともにBさんに送る
4. 受信者のBさんは次の3つの手順を実行する
   1. 請求書をハッシュ化し、**ダイジェスト**を作る
   2. **暗号化されたダイジェスト**をAさんの公開鍵で復号する
   3. iとiiの結果を比べ、**内容が一致することを確かめる**



このような仕組みをとることで、「なりすまし」と「送信内容の改ざん」を防げます。

* **なりすまし**を防ぐ仕組み：秘密鍵で暗号化されたダイジェストはペアの公開鍵でしか復号できない
* **送信内容の改ざん**を防ぐ仕組み：ダイジェストが一致しなければ送信内容が改ざんされている

なお送信者の公開鍵は誰でも入手できるため、送信経路などで情報漏洩が発生すると、暗号化されたデータでも簡単に復号されてしまう危険性があります。そのため、公開鍵暗号方式で内容を暗号化しつつ、**ディジタル署名**を利用するのが一般的です。

### **認証局**

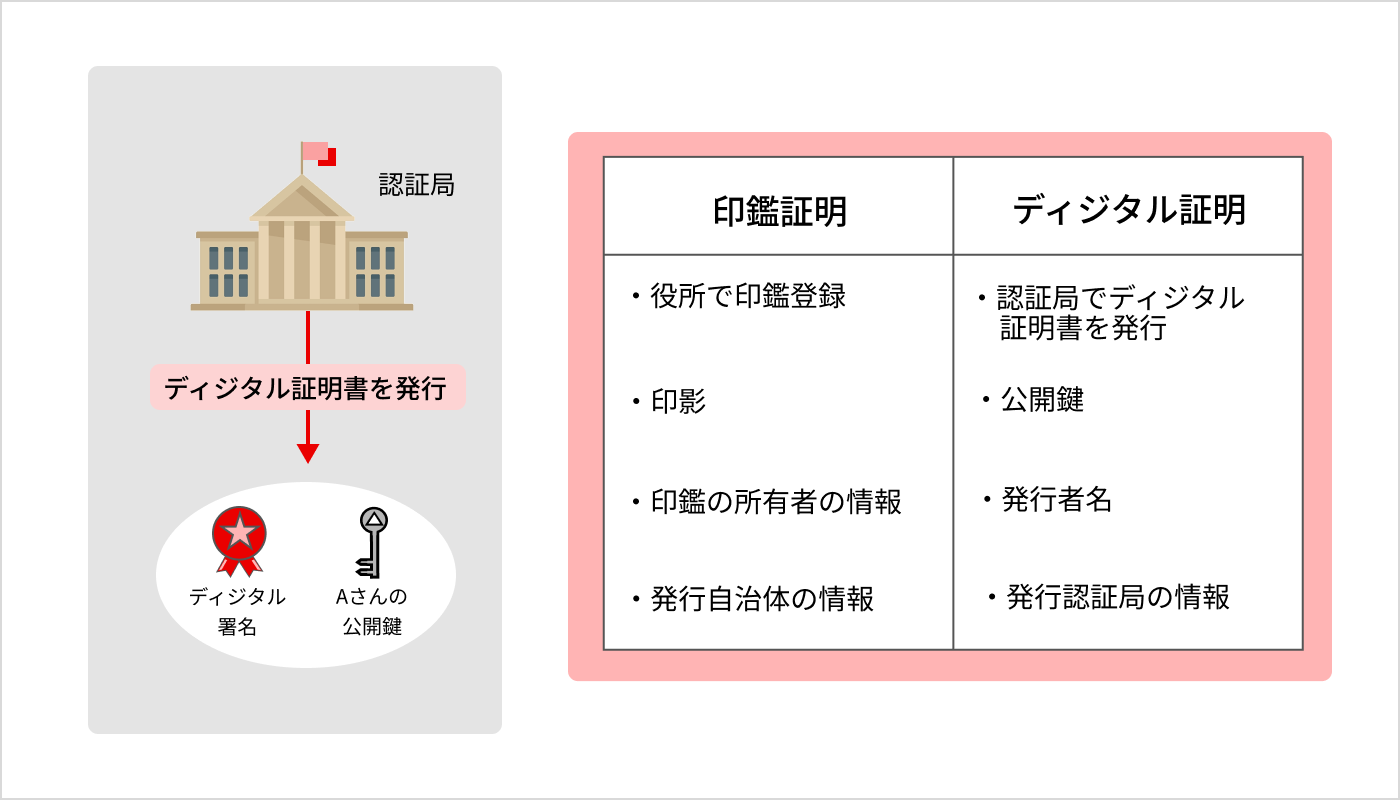
認証局とは、**「この公開鍵は確かに本人のものである」というディジタル証明書を発行する第三者機関**のことです。

ITパスポート試験では、**CA（Certification Authority）** と呼ばれることもあります。また、ディジタル証明書の別名は**電子証明書**です。

公開鍵を認証局に認定してもらうのは、役所で印鑑登録をするシステムに似ています。

印鑑登録とは印影や持ち主の情報を登録し、「この印鑑はこの人だけのものだよ」と役所に証明してもらう仕組みです。

一方、ディジタル証明書は公開鍵と公開鍵作成者の情報を登録し、「この公開鍵は確かにこの人のものだよ」と認証局に証明してもらう仕組みです。こうして発行されるディジタル証明書には、**登録者の公開鍵と認証局のディジタル署名**が含まれています。



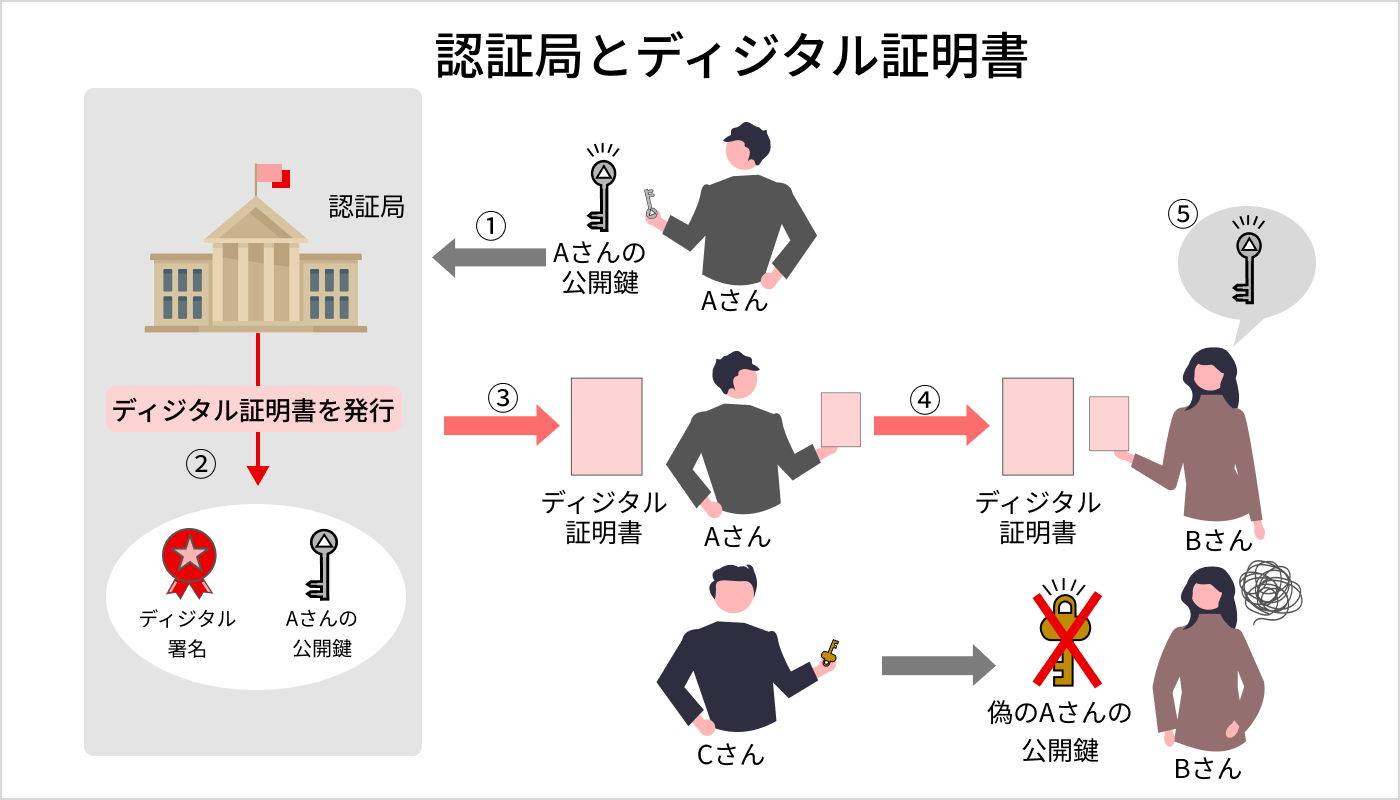
認証局がなければ、Aさんの偽物CさんがAさんになりすまして偽の公開鍵をばらまくことも可能です。

例えばBさんが、Aさんのものだと信じたCさんの公開鍵で大事な書類を暗号化し、Aさんに送信したとします。しかし、Aさんは自分の秘密鍵で書類を復号できません。かわりに、情報を盗み取ったCさんが書類を復号できてしまいます。

ここで、Aさんが認証局からディジタル証明書を発行してもらった場合を考えてみましょう。

Aさんはあらかじめディジタル証明書をBさんに送ること（①）で、公開鍵の正当性を証明できます（②）。AさんはBさんは暗号化のステップで、ディジタル証明書（④）から本物のAさんの公開鍵を取り出して（⑤）使用できます。

CさんはAさんになりすまそうとしても、証明書がないためBさんから信用されません。

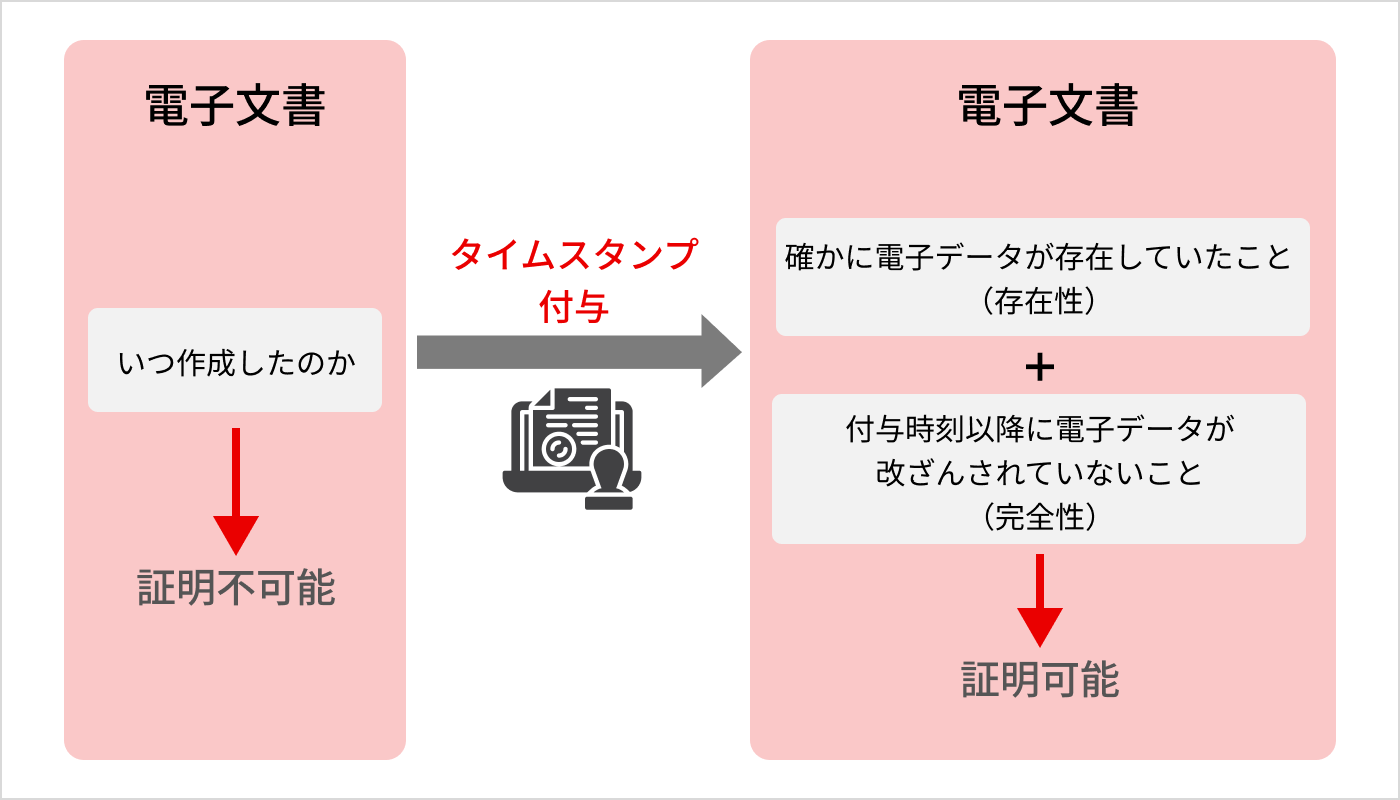


### **PKI**

PKI（Pubulic Key Infrastructure：公開鍵基盤）とは、**公開鍵の正当性を保証してくれるインフラ（基盤）** です。

認証局を使ってなりすましを防ぐ仕組みが「**PKI**」にあたります。

次は、電子データの改ざん対策である「タイムスタンプ」について説明します。



タイムスタンプとは、**スタンプが付与された時刻に確かに電子データが存在していたこと（存在性）＋付与時刻以降に電子データが改ざんされていないこと（完全性）を証明する**技術です。

修正や複製が簡単にできる電子データの特性は、データの内容が改ざんされやすいという欠点にもつながります。そこで、タイムスタンプを使って電子データの存在と改ざんされていないことを証明する必要が出てくるのです。

まとめ

* ディジタル署名とは、**データに電子的な署名を行い内容が改ざんされていないと証明する技術**
* 認証局とは、公開鍵が本人のものであることを証明する第三者機関のこと

| **用語** | **説明** |
| --- | --- |
| ディジタル証明書（電子証明書） | 公開鍵の所有者が本人であると証明する電子データのこと 認証局が発行する |
| PKI（Pubulic Key Infrastructure） | 公開鍵基盤 **「公開鍵」の正当性を保証してくれるインフラ（基盤）** |

## **人的セキュリティ対策を学ぼう**

人的セキュリティ対策とは、**人が原因である脅威への対策**のことです。

ここでは、3つの人的セキュリティ対策について説明します。

* のぞき見防止フィルム
* データの完全消去
* アクセス権の設定

### **のぞき見防止フィルム**

のぞき見防止フィルムとは、**パソコンやスマートフォンなどの画面に貼りつけて、第三者からののぞき見を防ぐフィルム**のことです。

のぞき見防止フィルムを付けた画面は、正面以外から内容を見られなくなります。

他人の秘密の情報（パスワードなど）を肩越しに盗み見る「**ショルダーハック（Shoulder Hack）**」への防止対策として有効です。

### **データの完全消去**

ハードディスクやSSDなどの記憶装置を破棄するときは、データを完全消去して復元できない状態にします。

完全消去の方法は、以下のとおりです。

* 専用ツールを用いて、乱数や無意味な文字列などの**ランダムなデータで記憶装置を複数回上書き**する
* 記憶装置を**物理的に破壊**する

### **アクセス権の設定**

アクセス権とは、ファイルの**読み書き**に関する権限のことです。

アクセス権には以下の3種類があります。

* **読み取り**（Readable）
* **書き込み**（Writable）
* **実行**（Executable）

アクセス権は通常、「ユーザごと」「ファイルごと」に設定します。

例えば、データの内容を書き換えられたくない場合は管理者が「読み取り専用」のアクセス権を一般利用者に与えます。こうすることで、人的ミスでデータが消去されるリスクを防げます。

## **物理的セキュリティ対策**

パスポート試験では「物理的セキュリティ対策」の用語がよく出題されます。特に「**バイオメトリクス認証**」は高確率で出題されるので、確実に暗記しましょう。

物理的セキュリティ対策とは、**重要なデータが保管された施設などが破壊されたり、不正な侵入を受けたりする危険性への対策**です。

ここでは、2つの物理的セキュリティ対策について説明します。

* バイオメトリクス認証
* 2要素認証

### **バイオメトリクス認証**

バイオメトリクス認証とは、**身体的特徴や行動的特性による認証方式**のことです。身体的特徴と行動的特性の例は、以下のとおりです。

| **特徴** | **例** |
| --- | --- |
| 身体的特徴 | **指紋**、**目**（**虹彩**（瞳孔の外側）、**網膜）**、**静脈パターン**、声紋、顔など |
| 行動的特性 | **文字を書く速度や筆圧、キータッチの力加減、歩き方のリズム**など |

#### **本人拒否率と他人受入率**

バイオメトリクス認証システムを評価する数値に、**本人拒否率**と**他人受入率**があります。

指紋認証などでスマートフォンを開けようとしても、乾燥などで指紋の形が変わってしまい本人なのに他人であると認識されてしまう場合があります。このように本人を認識しない割合を、本人拒否率といいます。

他人のことを本人であると誤認してしまう割合は、**他人受入率**です。

バイオメトリクス認証では、どちらの率が高くても使いづらいシステムになってしまいます。

### **2要素認証**

2要素認証とは、2つの異なる要素を使って**本人確認を行う認証方式**のことです。

2要素認証で使われる要素は、以下の3つから選びます。

| **要素** | **例** |
| --- | --- |
| 記憶情報 | パスワード、暗証番号、秘密の質問など |
| 所有物 | キャッシュカード、乱数表、USBトークンなど |
| 生体の情報 | 指紋、顔、虹彩など |

「**2段階認証**」と似ていますが、まったく違う認証方法なのできちんと区別しておく必要があります。

| **認証方式** | **内容** |
| --- | --- |
| 2要素認証 | 別々の要素から1つずつ2つの証拠を使って本人確認を実施する 例：銀行のATMでキャッシュカード（所有物）と指紋（生体の情報）を使い、お金を引き出した |
| 2段階認証 | 要素の被りを気にせず2つの段階を経て本人確認を実施する 例：パスワードを入力後、秘密の質問に答えてログインした（どちらも記憶情報を使っている） |

#### **その他の物理的セキュリティ対策に関連する重要用語**

その他の重要な物理セキュリティ対策に関する用語は、以下になります。

| **用語** | **説明** |
| --- | --- |
| 入退室管理システム | 誰が入退室したのか記録・管理するシステム |
| クリアデスク | 自席から離れるときに書類やパソコンを放置せず、安全な場所に保管すること |
| クリアスクリーン | 自席を離れるときにパソコンをログオフするなどし、第三者が情報にアクセスできないようにすること |
| アンチパスバック | ID登録による入退室管理を行うことで、共連れ（1人が認証して2人以上で入退室すること）を防ぐ 例：入室記録がないIDなのに、退出記録がある（誰かが部屋に入ったのと同時に入室している不正な行為） |

まとめ

| **用語** | **説明** |
| --- | --- |
| のぞき見防止フィルム | 人的セキュリティ対策の1つ のぞき見を防ぐためのフィルム ショルダーハックの防止に役立つ |
| データの完全消去 | 人的セキュリティ対策の1つ **ランダムなデータで複数回上書きをすることでデータを完全に消去する** |
| バイオメトリクス認証 | 物理的セキュリティ対策 **身体的特徴（指紋、顔、虹彩など）や行動的特性（筆圧、キータッチの力加減など）による認証方式**など |
| 2要素認証 | **2つの要素を使って本人確認する認証方式** |

## **技術的セキュリティ対策**

「技術的セキュリティ対策」について説明します。ITパスポート試験では、特に **「WAF」「SSL/TLS」「WPA2」** の出題頻度が高い

技術的セキュリティ対策とは、**技術的な脅威への対策**です。

この章では、以下の15個の技術的セキュリティ対策について簡単に説明します。

* ランサムウェア対策
* 不正アクセスを防ぐ３つのシステム（ファイアウォール、IDS/IPS、WAF）
* DMZ
* SSL/TLS
* HTTPS
* WPA2
* VPN
* ペネトレーションテスト
* ワンタイムパスワード
* シングルサインオン
* 耐タンパ性
* セキュリティバイデザイン
* セキュアブート
* リスクベース認証
* ブロックチェーン

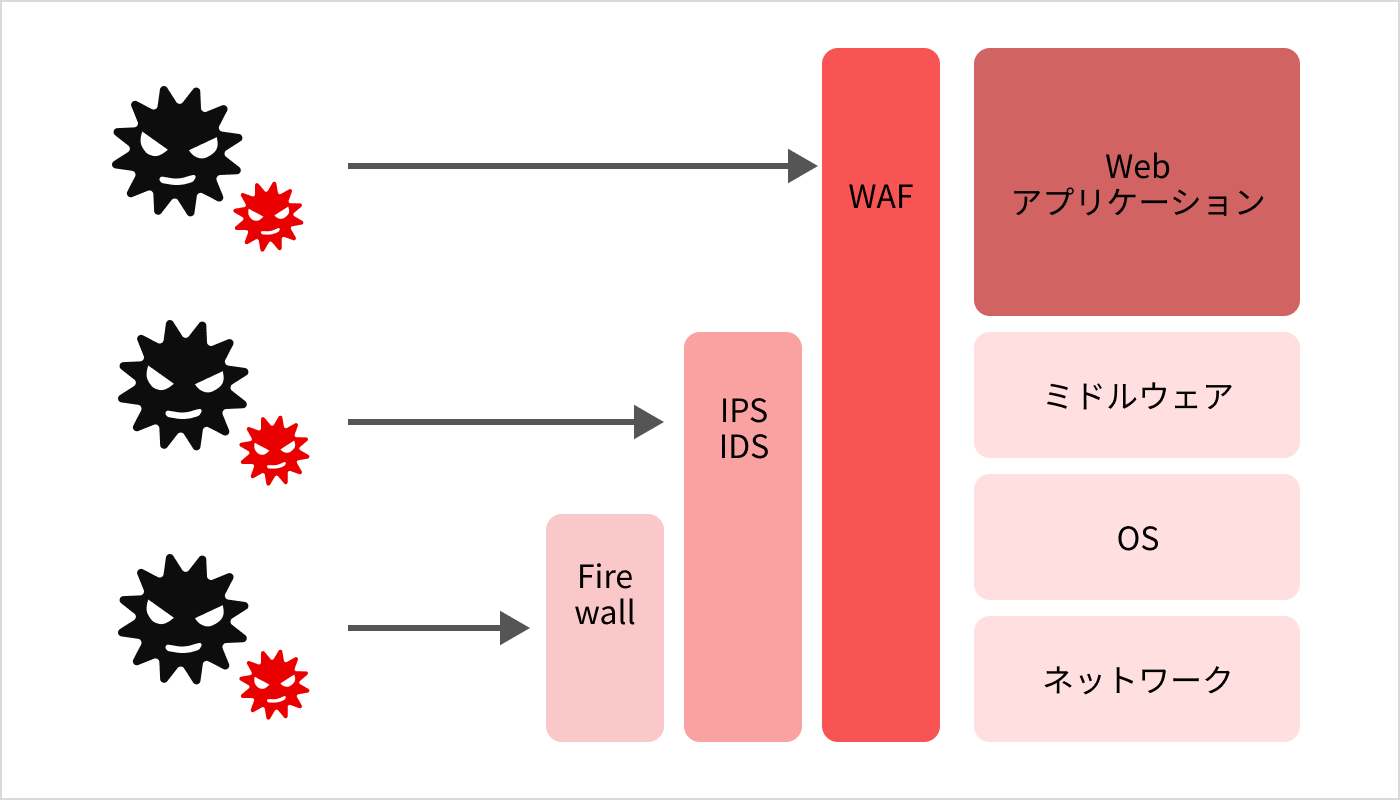
### **ランサムウェア対策**

ランサムウェア（Ransomware）とは、パソコン内のファイルやパソコン自体を使用不能にして、回復と引き換えに金銭を要求するソフトウェアです。（テクノロジ系[22章](https://terakoya.sejuku.net/programs/121/chapters/1506)）

**ランサムウェアへの対応策**は、**データを外部記憶装置にバックアップすること**です。外部記憶装置にバックアップすることで、コンピュータ内のデータが使用不能になってもデータを復元することが可能です。

### **不正アクセスを防ぐ３つのシステム**

攻撃者からの不正アクセスを防ぐシステムは「**ファイアウォール**」「**IDS/IPS**」「**WAF**」の3種類があります。



#### **ファイアウォール**

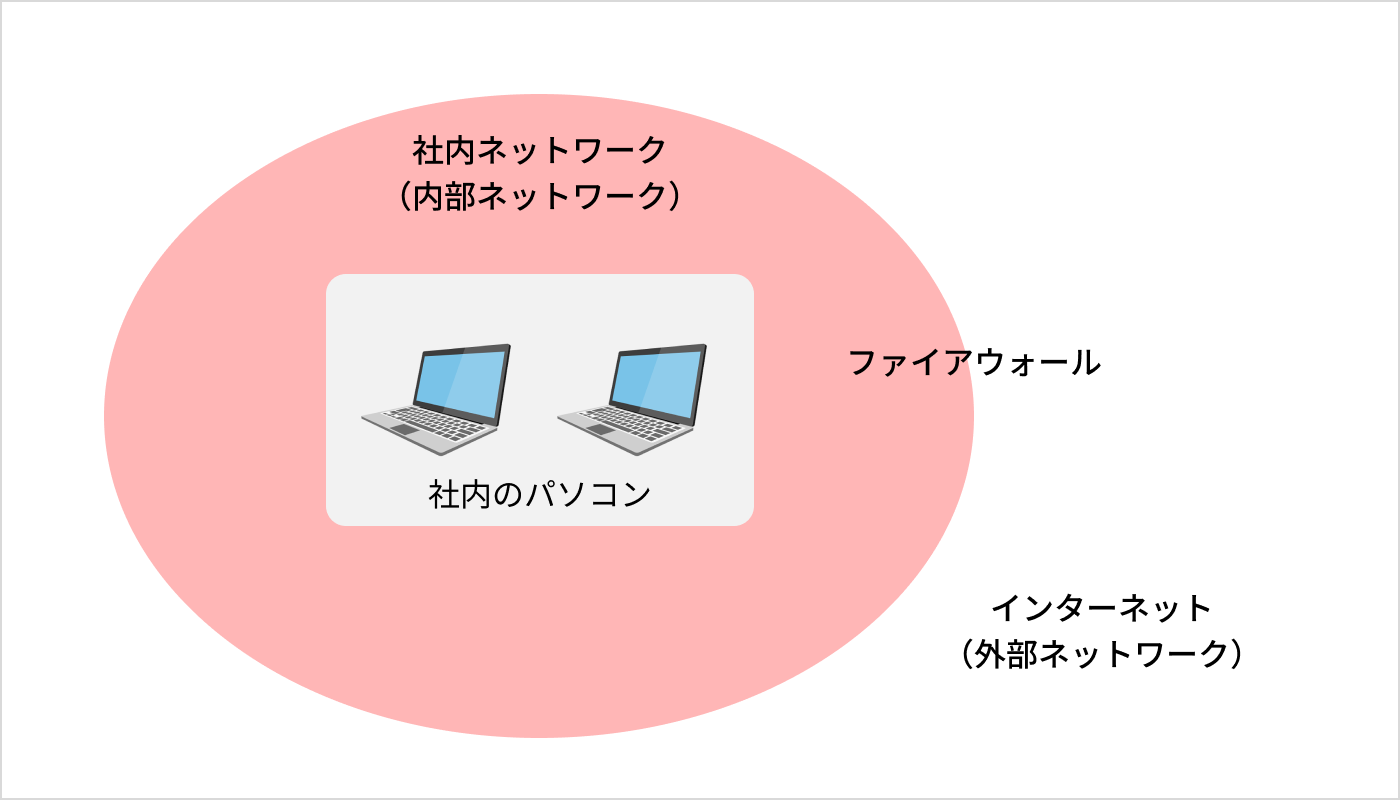
1つ目のシステムは「**ファイアウォール**」になります。

ファイアウォール（Firewall）とは、**外部ネットワーク経由の不正アクセスから内部のネットワークを守るための仕組み**です。

Firewallとは「防火壁」という意味で、外部からの攻撃を火事に例えています。

用語の意味からわかるように、ファイアウォールは「**外部ネットワーク**」と「**内部ネットワーク**」の間に設置されます。

外部ネットワークとは、インターネットのような世界中をつないでいるネットワークのことです。一方、内部ネットワークとは社内ネットワークのような組織内ネットワークのことです。



ファイアウォールは「**ポートスキャン**」という攻撃に対して有効な防御法です。

ポートスキャンとは、**攻撃者がポート（ケーブルやコネクタの差込口）に順次アクセスして外部から利用可能かどうかを調べる行為**です。

主にセキュリティホール（設計ミスなどによって生じたセキュリティ上の弱み）を探すときに使われます。

ファイアウォールを設置すれば、攻撃者によるポートへのアクセスを遮断できます。

#### **IDSとIPS**

2つ目のシステムは「**IDS**」と「**IPS**」です。2つのうち1つをネットワークや社内OSを守るために使います。これらのシステムは、ファイアウォールを乗り越えてしまう脅威を発見できます。

IDS（Intrusion Detection System：侵入**検知**システム）とは、外部からの不正アクセスを検知し、管理者に通知するシステムです。

IPS（Intrusion Prevention System：侵入**防御**システム）とは、外部からの不正アクセスを検知、通知するだけでなく、アクセス遮断まで行うシステムです。

IDSとIPSは、「DoS攻撃」や「OSやWebサーバのぜい弱性をターゲットにした攻撃」を防ぐことが可能です。  
DoS攻撃とは、要求を大量に送りつけてサーバをパンクさせる攻撃のことをいいます。

#### **WAF**

3つ目のシステムは「**WAF**」です。WAF（ワフ：Web Application Firewall）は、ぜい弱性のある**Webアプリケーションを狙った攻撃からシステムを守ります**。

WAFは、「SQLインジェクション」に対して有効です。SQLインジェクションとは、Webアプリケーションのぜい弱性を突き、データベースを不正に操作する攻撃です。

SQLインジェクションなどを防ぐためには、「サニタイジング（Sanitizing）」という技術を使います。ITパスポート試験では、用語の定義を問われることがあります。

例えば、悪意あるユーザーがユーザーフォームにプログラミングコードを入力し、データベースを誤作動させようとする場合があります。

サニタイジングは、フォームにデータベースを操作するようなコードが入力された場合、一部を書き換えて実行されないようにする技術です。

3つのシステムの特徴と違いは、以下のとおりです。

| **項目** | **ファイアウォール** | **IDS/IPS** | **WAF** |
| --- | --- | --- | --- |
| 監視するもの | IPアドレス、ポート | パケットの中身 | パケットの中身 |
| 守るもの | **ネットワーク** | **OS、ミドルウェア** | **Webアプリケーション** |
| どの攻撃に有効か | **ポートスキャン** | **DoS攻撃** | **SQLインジェクション** |

※パケットとは、通信回線やネットワークを流れる情報のことです。

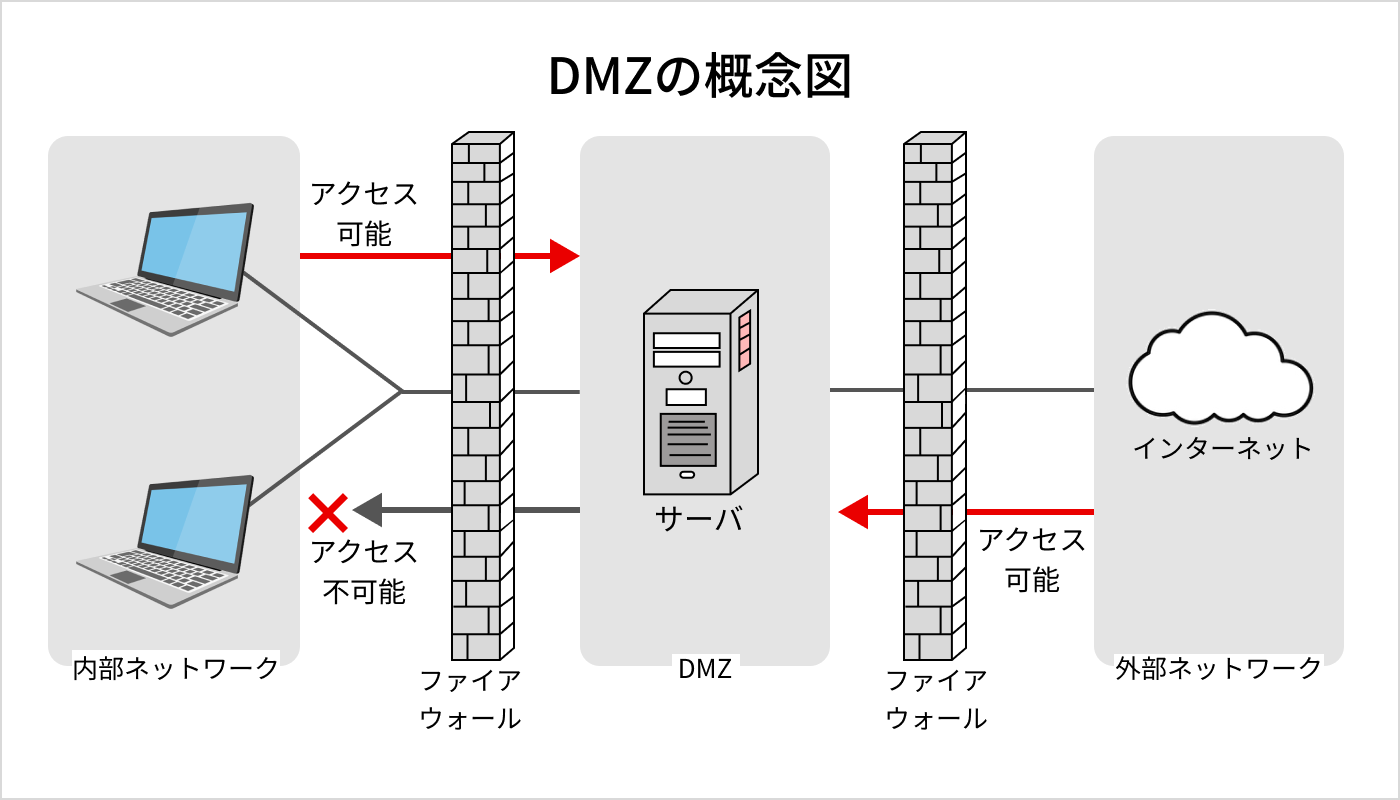
ファイアウォールや、IDS/IPSなどさまざまな脅威に対するセキュリティ対策を1つに統合して管理することを「**UTM（Unified Threat Management：統合脅威管理）**」といいます。

UTMを用いると、コストや運用管理の負担を軽減できます。

### **DMZ**

DMZ（DeMilitarized Zone：非武装地帯）とは、**外部ネットワークと内部ネットワークの両方から独立したネットワーク領域**です。

ITパスポート試験では「企業内ネットワークからも外部ネットワークからも論理的に隔離されたネットワーク領域」と出題されることがあります。



Webサーバやメールサーバは、外部ネットワークと通信する必要があるため常に危険にさらされています。

もし、サーバが悪意のある第三者に乗っ取られたり、マルウェアなどに感染したりした場合、それらと通信している社内システムも被害を受ける可能性が高いです。

そこで登場するのが「**DMZ**」です。  
DMZには、次の特徴があります。

* 外部ネットワーク、内部ネットワークのどちらからもDMZへのアクセスが可能
* DMZから内部ネットワークへのアクセスは不可能

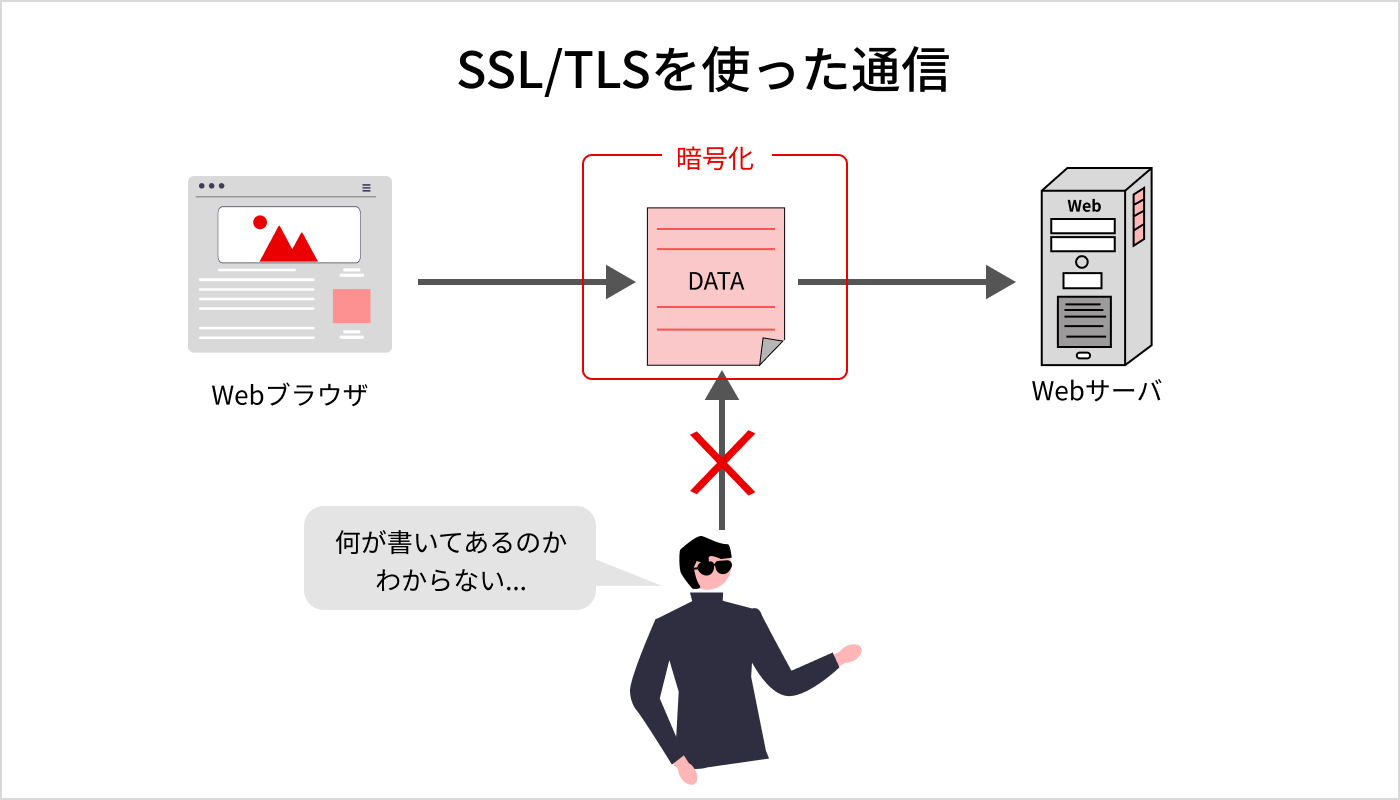
Webサーバやメールサーバなど、社外に公開するサーバはDMZ内に配置します。

万が一、DMZ内のサーバがマルウェアなどに感染した場合でも、DMZから社内ネットワークには入れないので社内のシステムに影響はありません。

### **SSL/TLS**

SSL/TLS（Secure Sockets Layer/Transport Layer Security）とは、**パソコンとサーバ間の通信を「暗号化」する通信上の規約（プロトコル）** です。

SSL/TLSを利用するとインターネット上でやり取りされる情報が暗号化され、盗み見を防げます。



SSLのぜい弱性に対応した新しいプロトコルがTLSで、現在はTLSの方が主流です。SSLとTLSは別物ですが、知名度はSSLの方が高く、SSL/TLSとセットで言及されることが多いです。

### **HTTPS**

HTTPS（HTTP over SSL/TLS）とは、SSL/TLSで確立された安全な接続上で**HTTP通信（データ通信）を行う方式です。**

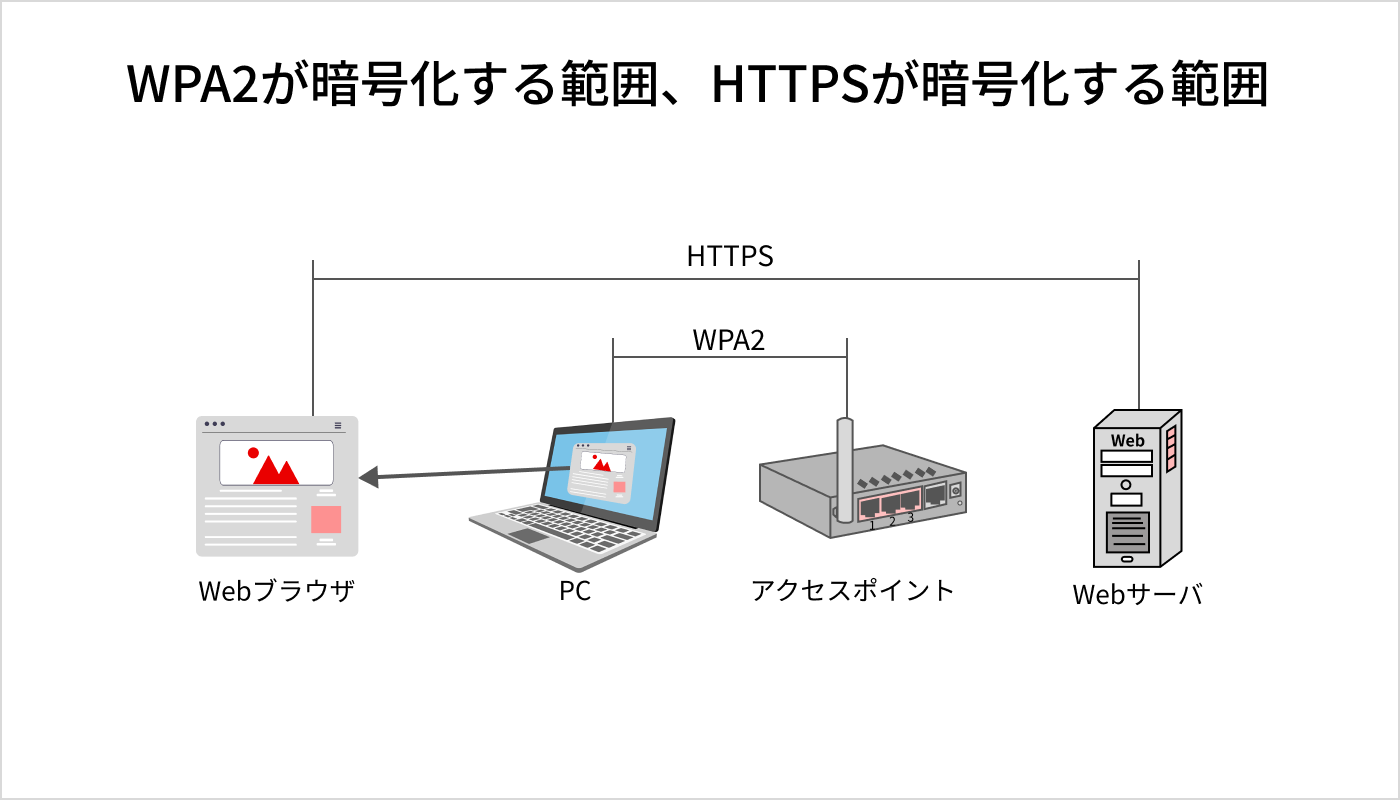
なお、「https://」で始まるURLはSSL/TLSを使用しています。

従来のHTTP通信は暗号化されていなかったため、通信の盗聴や改ざんリスクがありました。HTTPSは共通鍵を使用して暗号化通信を確立し、データやり取りの安全性を高めます。

### **WPA2**

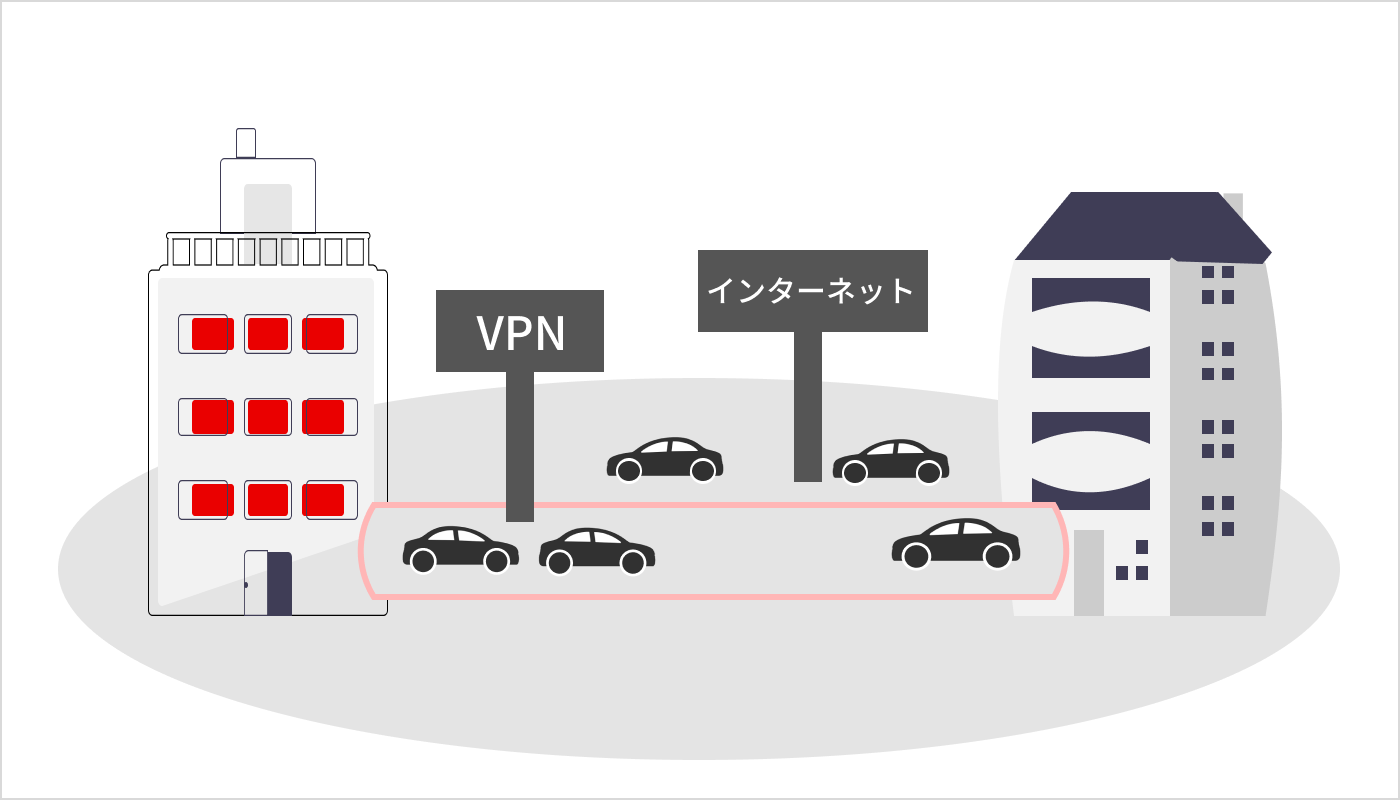
WPA2（Wi-Fi Protected Access 2）とは、**無線LAN通信を暗号化するセキュリティ規格**です。HTTPSとは異なり、パソコンからアクセスポイントまでの通信を暗号化している点に注意しましょう。

なお、WPA2の弱点を克服した後続の規格として、2018年にWPA3が発表されています。



| **項目** | **説明** |
| --- | --- |
| WPA2とWEPの関係 | WPA2の登場以前に広く使われていた**WEP**には、**短い時間で暗号が解読されてしまう問題**があるため、安全性の高い暗号化を行うためにWPA2が策定された |
| WPA2が暗号化する範囲 | **パソコンからアクセスポイント**までの通信を暗号化する |

### **VPN**



VPN（Virtual Private Network）は、**外部ネットワークであるインターネット（公衆回線）を会社の専用回線のように利用できる技術**です。

最近はリモートワークが進んでおり、外出先から職場のネットワークにアクセスする機会も多いでしょう。このようなときにVPNを利用すれば、安全な通信が可能になります。

### **ペネトレーションテスト**

ペネトレーションテストとは、**システムを実際に攻撃することでセキュリティ上のぜい弱性を発見しようとするテスト手法**のことです。

システムをリリースする前に、攻撃に耐えられるかを検討することは非常に重要です。ペネトレーションテストには、OSやサーバソフトウェアに対して実施されるものと、Webソフトウェアに対して実施されるものがあります。

### **ワンタイムパスワード**

ハードウェアトークン

ワンタイムパスワードとは、**使い捨てパスワード**のことです。

イラストのような、ハードウェアトークンなどを使ってランダムな数字などをパスワードとして生成します。

また、メールアドレスやSMSにワンタイムパスワードを送信する場合もあります。

**一度しか使えないワンタイムパスワード**なら、**不正アクセスを防止**できます。

同じパスワードを使いまわしていると、情報が漏れたときになりすましを防げなくなります。

### **シングルサインオン**

シングルサインオンとは、**最初に認証が成功すれば、その後は許可された複数のサーバやアプリケーションの認証手続きを省略できる仕組みです。**

WebサービスごとにIDやパスワードを要求され、辟易した経験がある人は少なくないでしょう。シングルサインオンは、このような不便を解消できる仕組みです。

### **耐タンパ性**

耐タンパ性とは、**システム内部データの「解析のしにくさ」を表す度合い**のことです。タンパ（Tamper）は「改ざん」という意味です。

例えば、銀行のキャッシュカードにはICチップが埋め込まれています。このICチップには、こじ開けられそうになると壊れる、ダミー回路をもっているなど、耐タンパ性を高める工夫が施されています。

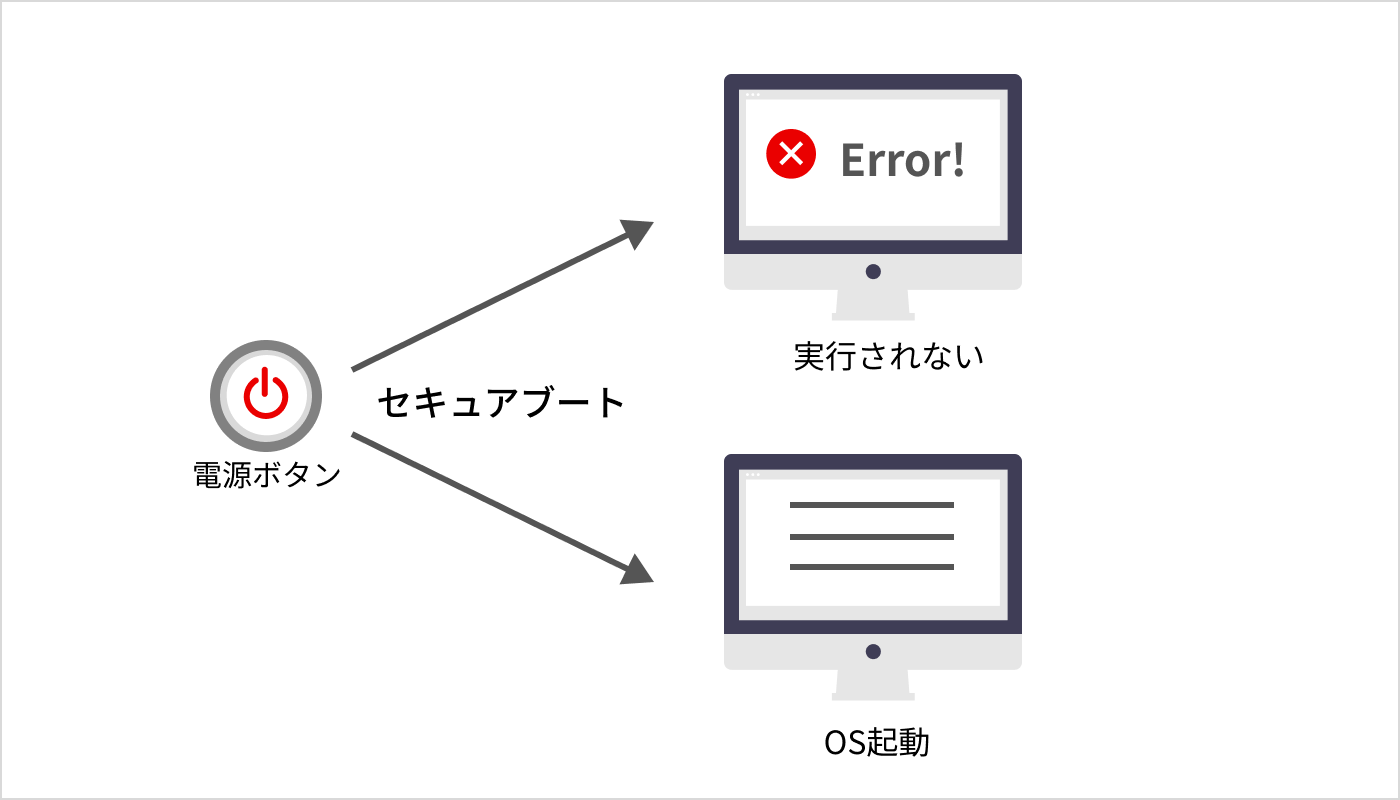
### **セキュリティバイデザイン**

セキュリティバイデザイン（Security By Design：SBD）とは、**システムや製品の企画・設計時点から、セキュリティを確保する設計手法**です。

セキュリティ対策にかかる費用を削減できるメリットがあります。

### **セキュアブート**

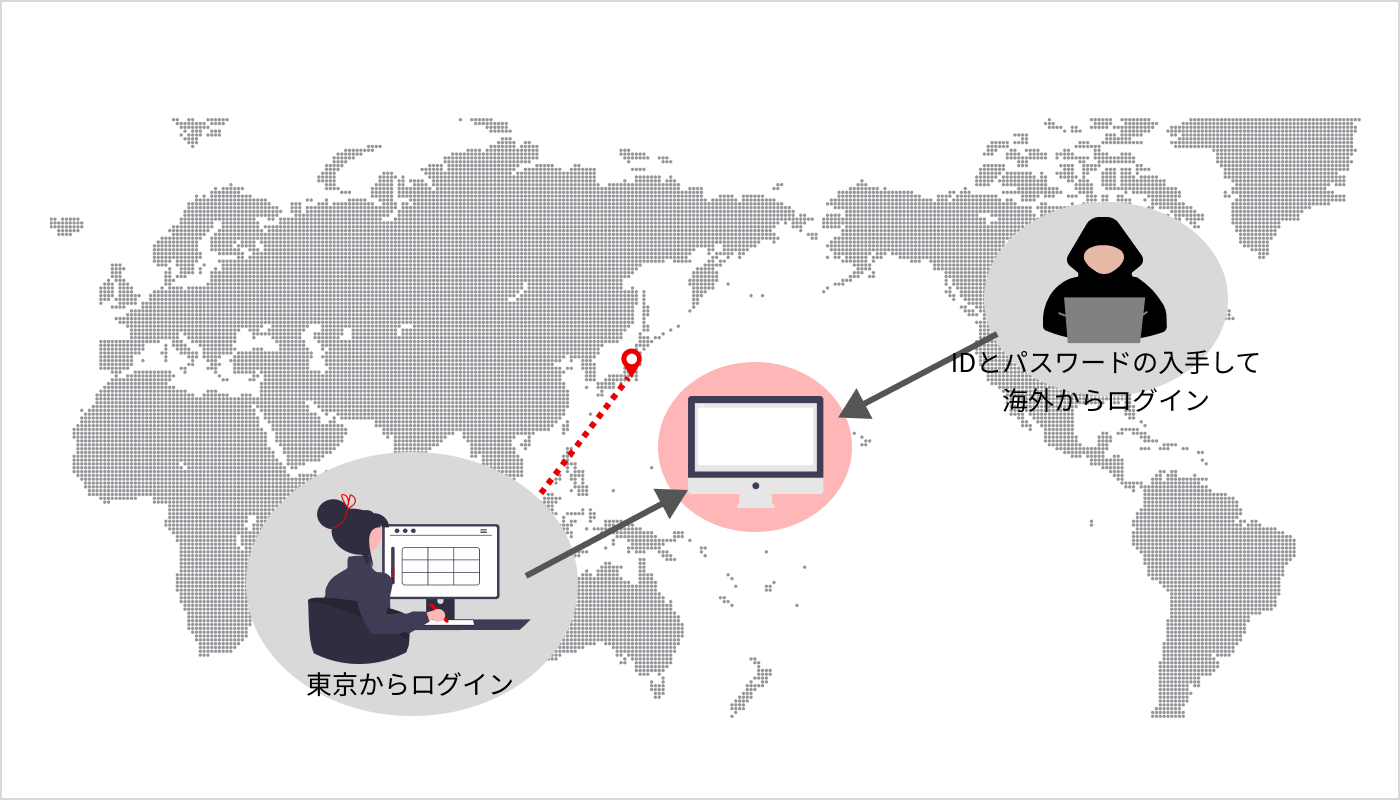
セキュアブート（Secure Boot）とは、**パソコンの起動時にOSのディジタル署名を調べて、偽のOSが実行されるのを防ぐ技術**です。マルウェア（悪意のあるソフトウェアのこと）に感染した可能性のあるOSの実行を防止できます。



### **リスクベース認証**

リスクベース認証とは、**普段とは異なる場所やデバイスからのアクセス、異常なログイン回数などのリスクを評価し、リスクが高いと判断した場合に追加認証を行う認証方式**です。

例えば、普段は東京からログインしているシステムに対して、海外からログインした場合などが該当します。



### **ブロックチェーン**

ブロックチェーンとは、**複数のコンピュータによって構成されたネットワーク上で、データを分散して保存することです。  
改ざんや不正アクセスを防止する技術**です。

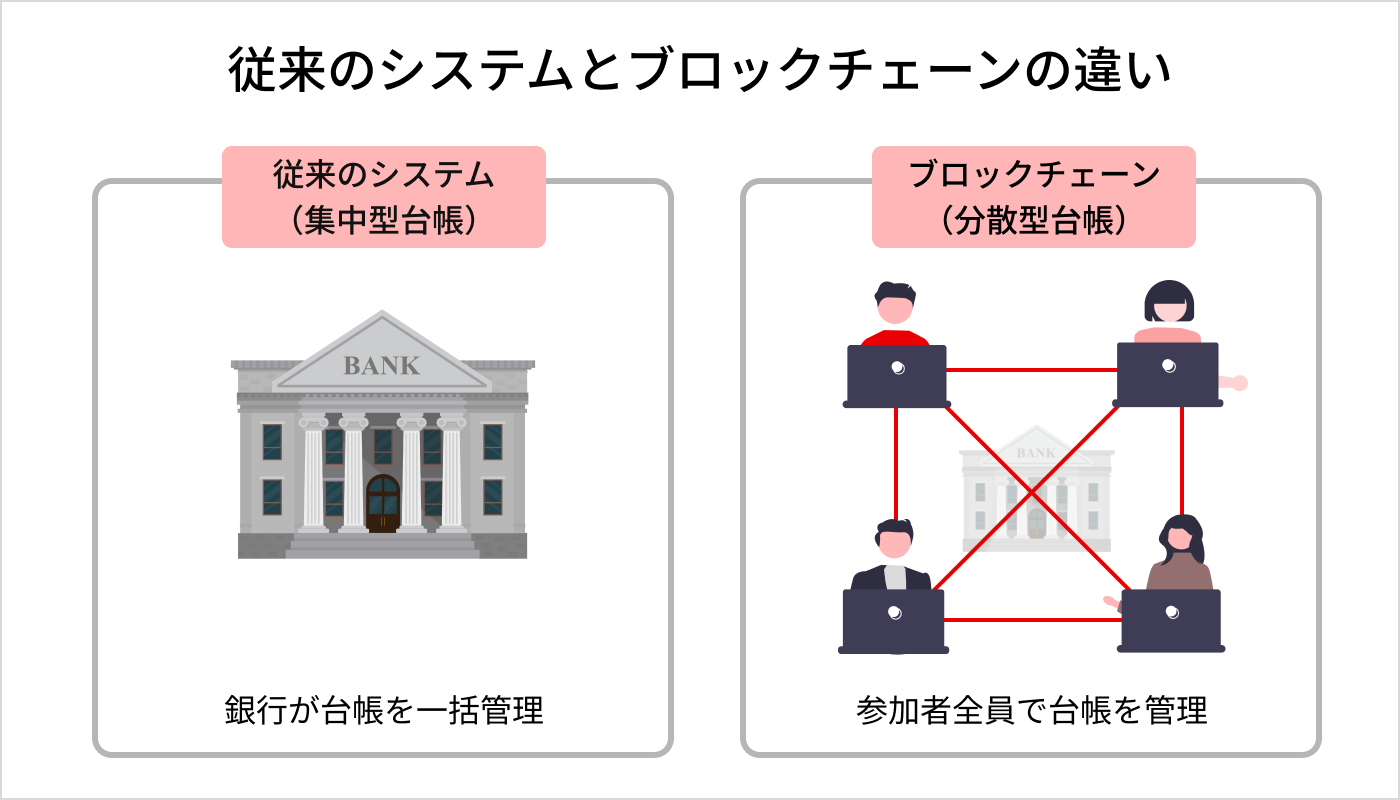
ブロックチェーンは、**暗号資産に必要不可欠な技術の1つ**といえます。

日本円や米ドルなどの従来の通貨では、銀行が台帳（取引履歴）を一括で管理していました。これを、集中型台帳といいます。

集中型台帳では、一括管理されたデータが改ざんされると、復旧が困難になるというデメリットがあります。

ブロックチェーンは、参加者全員で台帳を管理する「**分散型台帳**」です。分散型台帳は、改ざんされにくく、セキュリティ性が高いという利点があります。

集中型台帳と分散型台帳のイメージは以下のとおりです。



まとめ

| **用語** | **説明** |
| --- | --- |
| ファイアウォール（Firewall） | 外部の不正アクセスから内部ネットワークを守るための仕組み |
| ポートスキャン | ポートに順次アクセスして外部から利用可能かどうかを調べる攻撃 |
| IDS（Intrusion Detection System） | 侵入検知システム外部から不正アクセスがあった場合、「システム管理者に通知」するシステム |
| IPS（Intrusion Prevention System） | 侵入防御システム 外部から不正アクセスがあった場合、「システム管理者に通知」だけでなく「そのアクセスを遮断」するシステム |
| DoS攻撃 | サーバへの要求を大量に送りつけてサーバをパンクさせる攻撃 |
| WAF（ワフ：Web Application Firewall） | ぜい弱性のあるWebアプリケーションを狙った攻撃からシステムを守るための仕組み |
| SQLインジェクション | Webアプリケーションのぜい弱性を突いて、SQL文を挿入することでデータベースを不正に操作する攻撃 |
| サニタイジング（Sanitizing） | 入力された文字列を無害化する技術 |
| UTM（Unified Threat Management） | 統合脅威管理 さまざまな脅威に対するセキュリティ対策を1つに統合して管理すること |
| DMZ（DeMilitarized Zone） | 非武装地帯 外部ネットワークと内部ネットワークの両方から独立したネットワーク領域 |
| SSL/TLS（Secure Sockets Layer/Transport Layer Security） | パソコンとサーバ間の通信を「暗号化」するプロトコル |
| HTTPS（HTTP over SSL/TLS） | SSL/TLSで確立された安全な接続上でHTTP通信を行う方式 |
| WPA2（Wi-Fi Protected Access 2） | 無線LAN通信を暗号化する規格 |
| VPN（Virtual Private Network） | インターネット通信回線を会社の専用回線のように利用できる技術 |
| ペネトレーションテスト | 実際にシステムを攻撃することでセキュリティ上のぜい弱性を発見しようとするテスト手法 |
| ワンタイムパスワード | 一使い捨てのパスワードのこと |
| シングルサインオン | 最初の認証が成功すれば、許可された複数のWebサービスやアプリケーションの認証手続きを省略できる仕組み |
| 耐タンパ性 | システム内部データの「解析のしにくさ」を表す度合い |
| セキュリティバイデザイン（Security By Design：SBD） | システムや製品の企画・設計時点から、セキュリティを確保する設計手法 |
| セキュアブート（Secure Boot） | パソコンの起動時にOSのディジタル署名を調べて、偽のOSの実行を防ぐ技術 |
| リスクベース認証 | 普段とは異なる場所やデバイスからのアクセス、異常なログイン回数などのリスクを評価し、リスクが高いと判断した場合に追加認証を行う認証方式 |
| ブロックチェーン | 複数のコンピュータによって構成されたネットワーク上で、データを分散して保存することで、改ざんや不正アクセスを防止する技術 |