Woodland Academy

7.3 セキュリティの基礎

- セキュリティの基本要素
- 暗号化技術
- 認証技術

Shape Your Future

目次

情報資産と脅威

- 企業は多くの**情報資産**[Information Asset]を保有している。情報資産とは、データベース、ドキュメント、ソフトウェア、ハードウェアなどを指す。

- **脅威**[Threat]は、システムの**脆弱性**[Vulnerability]（セキュリティ上の弱点）をついて、情報資産に悪影響を与える。情報資産を守る対策を立てるためには、脅威と脆弱性についてしっかりと把握する必要がある。

Woodland Academy

脅威の 3 分類

- **人的脅威**
  操作ミスや情報漏洩など、人によって引き起こされるもの。

- **技術的脅威**
  ウィルス[Virus]や不正アクセスなど、プログラムなどの技術によって引き起こされるもの。

- **物理的脅威**
  天災や故障、侵入者による物理的な破壊などによって引き起こされるもの。

情報セキュリティの 3 大要素

- 企業などの組織が、保有する情報資産について、そのセキュリティを管理・運用していく仕組みを、情報セキュリティマネジメントシステム（**ISMS**）と呼ぶ。

- ISMS の 3 大要素（CIA）：

1. **機密性**[Confidentiality]
   許可されていない個人、団体等、またはプロセスに対して、情報を使用不可または非公開にする特性。**許可された人しか見る（使う）ことができない。**

2. **完全性**[Integrity]
   資産の正確さおよび完全さを保護する特性。**不正に書き換えられたりせず、正確な内容を保つ。**

3. **可用性**[Availability]
   許可された団体等が要求した時に、アクセスおよび使用が可能である特性。**使いたい時にきちんと存在し、使える。**

Woodland Academy

練習問題

- 【問題 1】

情報の“完全性”を脅かす攻撃はどれか。

ア：Webページの改ざん

イ：システム内に保管されているデータの不正コピー

ウ：システムを過負荷状態にするDoS攻撃

エ：通信内容の盗聴

ISMS 評価制度

- **ISMS 適合性評価制度**
  - 企業などが適切な情報セキュリティ方針を定め、それを実施するための適切な情報セキュリティマネジメントを行っているかどうかを承認する制度。認定用の国内規格（要求事項）としては、JIS Q 27001 が用いられる。

- **P マーク**（プライバシーマーク）制度
  - 企業などが個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークの使用を認める制度。

AAR

- CIA に次ぐ重要な要素として、次の 4 つの概念がある。「情報セキュリティの AAR」などと呼ばれる：
  - **真正性**[Authenticity]
    - 利用者や記録作成者などの、相手の身元主張の正統性が確保できる状態にしなければならないこと。
  - **責任追跡性**[Accountability]
    - 何の情報にいつ誰がアクセスしたのか、といった行為を事後追跡できる状態にしなければならないこと。
  - **否認防止性**[Non-Repudiation]
    - 電子商取引の取引事実や電子メールの送信事実などが、後になって当事者に否認されることのない状態にしなければならないこと。
  - **信頼性**[Reliability]
    - 業務プロセスやシステムが不具合なく正常に機能すること。矛盾したり、異常な結果に終わることが無い状態にしなければならないこと。

Woodland Academy

情報セキュリティポリシー

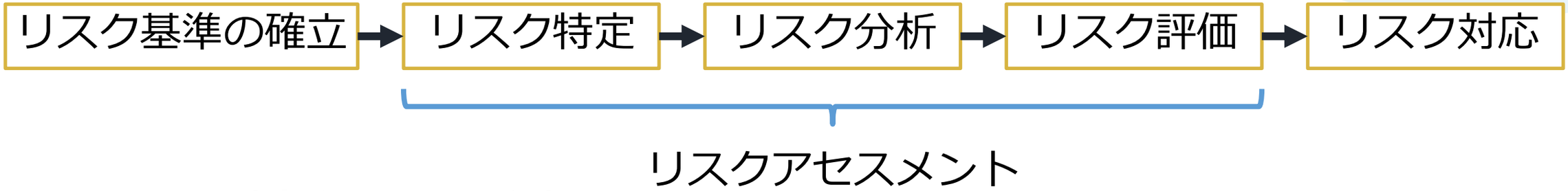
- 企業などの組織が ISMS を運用する時、最初に策定する**ISMS の基本方針**のことを、**情報セキュリティポリシー**という。

- 情報セキュリティポリシー策定の留意点：
  - 企業の**トップ**が策定する。
  - ISMSの適用範囲は、企業の特徴や組織、資産などの特性を考慮した上で策定する。
  - 策定したセキュリティポリシーは**文書化**し、組織内の全員に配布して**周知徹底**する。
  - 一度策定して終わるのではなく、**継続的な改善**を行う。

リスクマネジメント

- ISMS を確立するためには、リスクマネジメントも行う必要がある。リスクとは、脅威が脆弱性をついて企業に損害を与える可能性（危険性）のことを指す。

- リスクマネジメントの流れ：



- リスク対応の 4 分類：

リスク低減（軽減）	リスク回避	リスク移転（転嫁）	リスク受容（保有）
あるリスクの発生確立や被害額を下げる	撤退などによって、リスクのある状況を避ける	リスクに関する負担責任を他社に任せる、共有する	自らリスク負担を負う（受け入れる）

Woodland Academy

Q&A

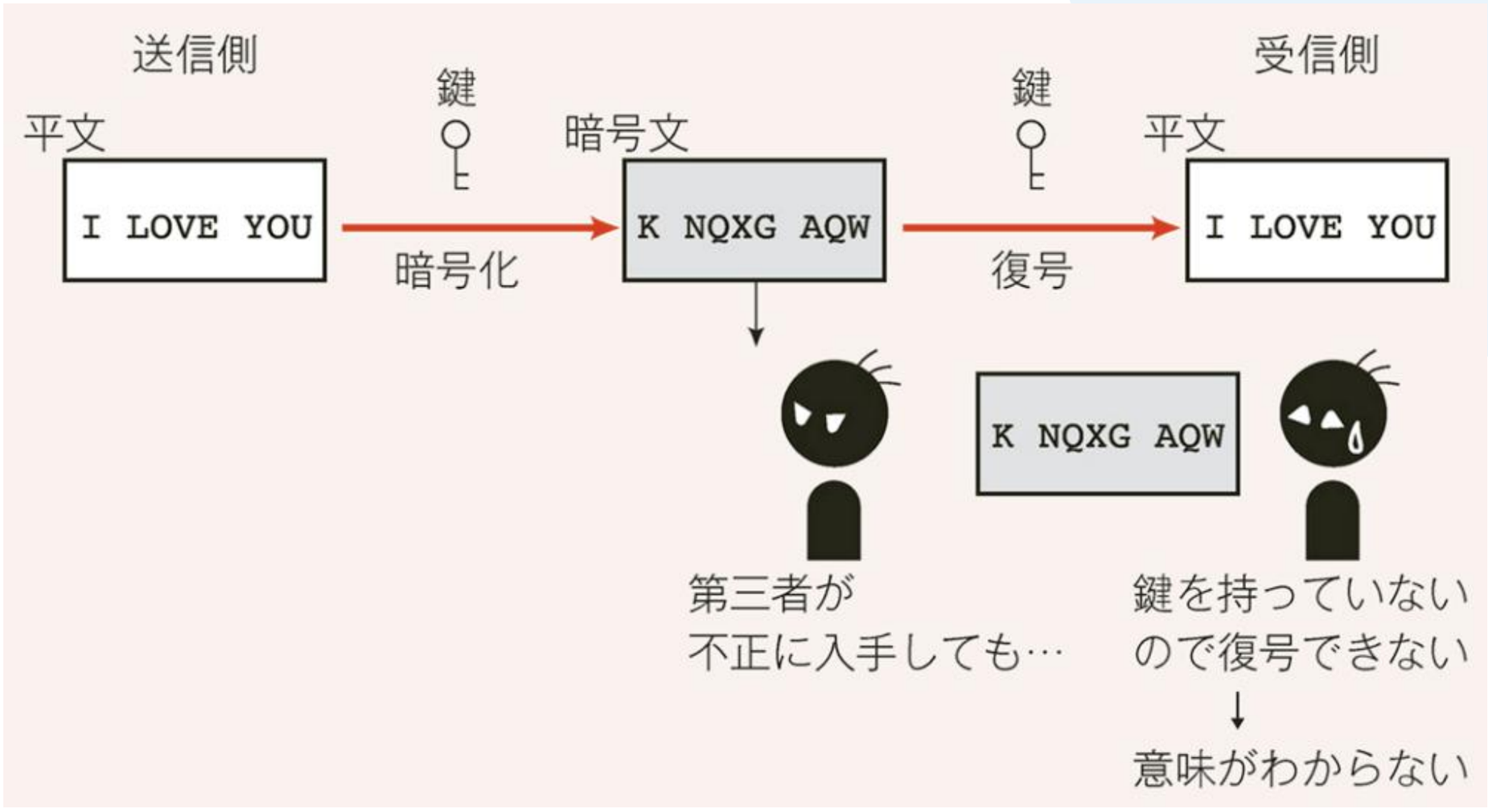
目次

暗号化技術

- インターネットでは、多数のサーバを経由しながらデータを送信する。つまり経由地点のどこかで第三者にデータを盗み取られる（**盗聴**[Eavesdropping]される）危険がある。そこで、元のデータを読み取らせないために「**暗号化**[Encryption]」の技術が利用される。

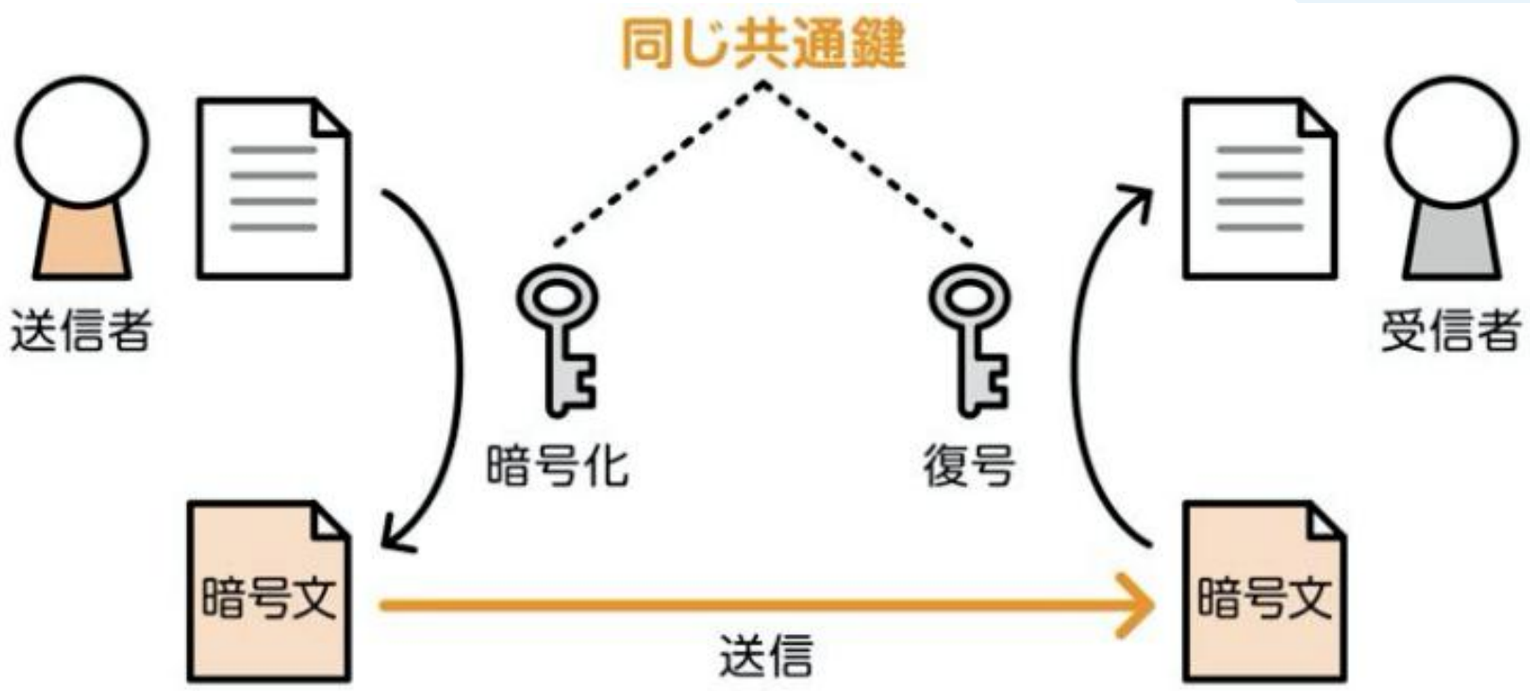
- **暗号化**とは、**平文**[Plaintext]（元の文書）を受信者以外にわからないような、**暗号文**[Ciphertext]に変換すること。暗号化には、**アルゴリズム**（手順）と**鍵**[Key]を使う。暗号化されたデータは、アルゴリズムと鍵がわかれば、元に戻すことができる。これを「**復号化**[Descryption]」と呼ぶ。

暗号化の流れ



共通鍵暗号方式

- **共通鍵暗号方式**[Symmetric Encryption]は、**暗号化と復号に同じ鍵**（共通鍵）を使う。対称鍵暗号方式などと呼ばれたりする。



公開鍵暗号方式

- **公開鍵暗号方式**[Asymmetric Encryption]は、**暗号化と復号に用いる鍵の内容が異なる**。各ユーザは**公開鍵**[Public Key]と**秘密鍵**[Private Key]からなるペアを作成し、**公開鍵の方だけ**を公表する。そしてメッセージを暗号化して送る場合は、以下手順を取る：
  1. 送信者は受信者の**公開鍵で暗号化**した後に送信する
  2. 受信者は受け取った暗号文を受信者の**秘密鍵で復号**する

受信者の秘密鍵は受信者本人しか知らないため、この暗号文を第三者が入手しても内容を知ることはできない。

次へ

Woodland Academy

ハイブリッド暗号方式

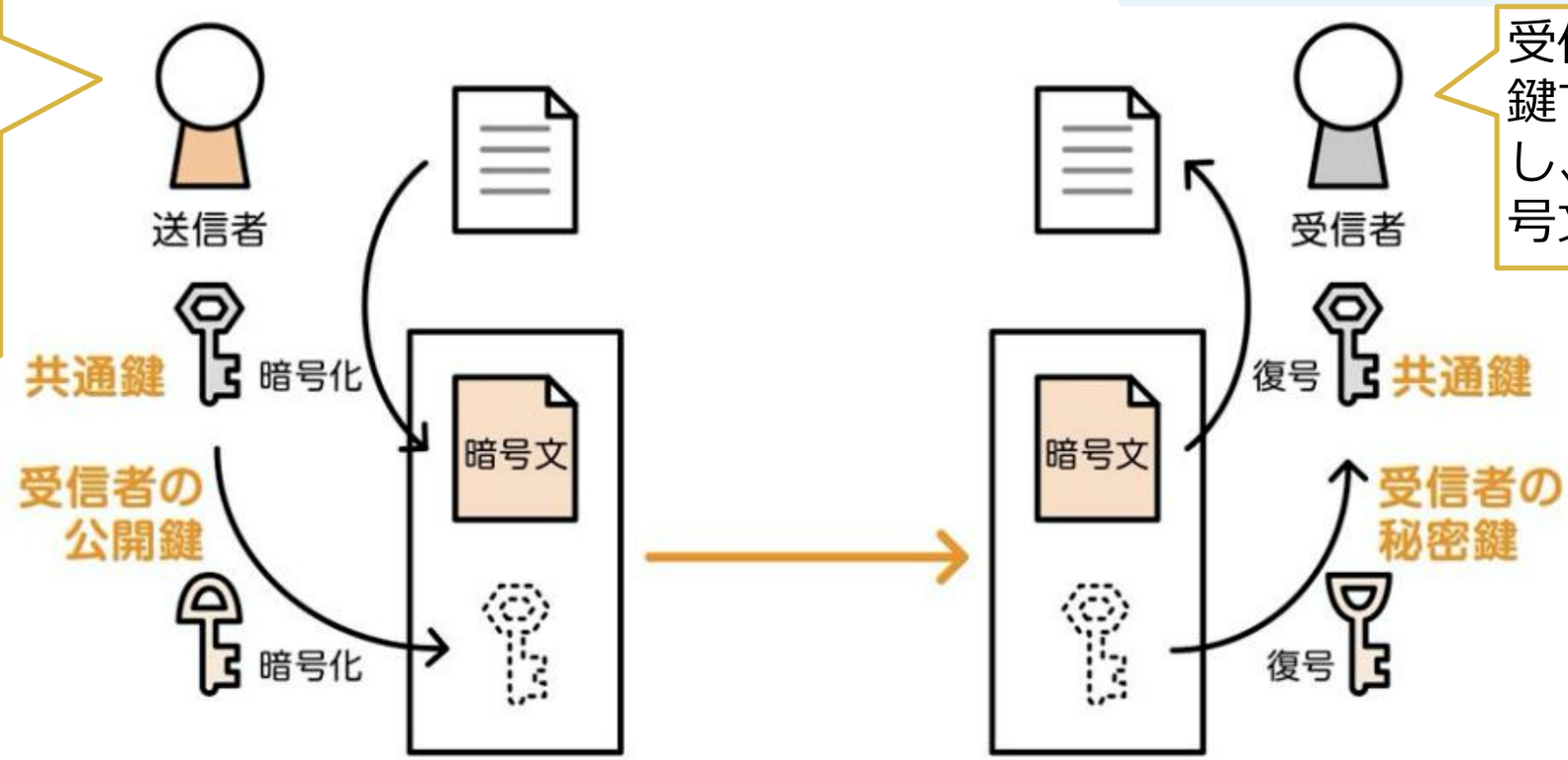
- 共通鍵暗号方式は**処理が高速**だが、鍵の受け渡しに注意が必要になる。公開鍵暗号方式は、事前に鍵の受け渡しが必要なく**安全**だが、処理に時間がかかる。

- そこで、データは共通鍵暗号方式で暗号化を行い、鍵の受け渡しには公開鍵暗号方式を使用する**ハイブリッド暗号方式**（セッション鍵方式）が使われるようになっている。

次へ

前へ

送信者は共通鍵を作り、データを暗号化する。その後、受信者の公開鍵で共通鍵を暗号化し、暗号文と共に送る。



受信者は自身の秘密鍵で共通鍵を復号し、それによって暗号文を復号する。

練習問題

- 【問題 1】

暗号方式には共通鍵暗号方式と公開鍵暗号方式がある。共通鍵暗号方式の特徴として、適切なものはどれか。

ア：暗号化通信する相手が１人のとき、使用する鍵の数は公開鍵暗号方式よりも多い。

イ：暗号化通信に使用する鍵を、暗号化せずに相手へ送信しても安全である。

ウ：暗号化や復号に要する処理時間は、公開鍵暗号方式よりも短い。

エ：鍵ペアを生成し、一方の鍵で暗号化した暗号文は他方の鍵だけで復号できる。

練習問題

- 【問題 2】

AさんはBさんだけに伝えたい内容を書いた電子メールを、公開鍵暗号方式を用いてBさんの鍵で暗号化してBさんに送った。この電子メールを復号するために必要な鍵はどれか。

ア：Aさんの公開鍵

イ：Aさんの秘密鍵

ウ：Bさんの公開鍵

エ：Bさんの秘密鍵

Woodland Academy

Woodland Academy

Q&A

目次

認証技術

- ユーザが間違いなく本人であることを認証するために、様々な技術が開発されている。**ユーザ認証**と**するメッセージ認証**に大別される。
- ユーザ認証：「確かに本人である」ことを確認する。
- メッセージ認証：やりとりするデータの内容に対して「確かにこの内容で間違いない」と確認する。

ID によるユーザ認証

- **ユーザ ID**
  各システムで 1 つしかない、**システム管理者によって各ユーザに割り当てられる識別番号**。

- **パスワード**[Password]
  各ユーザが任意で設定できる文字列で、ユーザ本人しか知り得ない。

パスワードクラックの主な手法

- パスワードを解析して読解する攻撃（**パスワードクラック**）の手法は次のようなものがある。

1. **ブルートフォース攻撃**（総当たり攻撃）
   すべての文字列の組み合わせを試していく方法。

2. **辞書攻撃**
   意味のある単語を逐次試していく方法。

3. **パスワードリスト攻撃**
   あるサービスから流出したパスワードを用いて、別のサービスへの不正ログインを試みる攻撃。複数のサービスにおいて、同じパスワードを使い回す利用者が多いことに注目した攻撃手法。

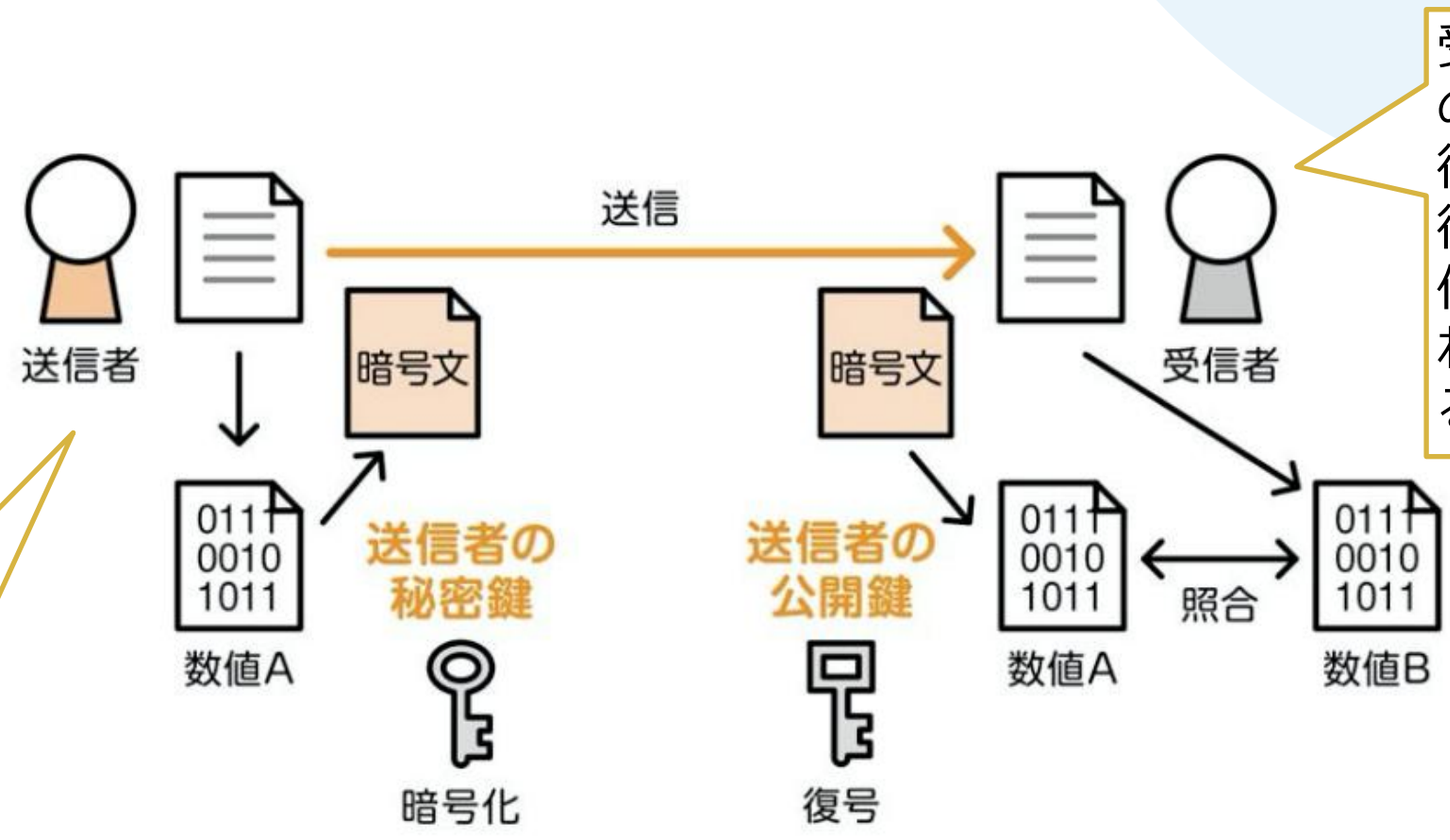
その他のユーザ認証技術

- **バイオメトリクス認証**（生体認証）：各ユーザがもつ生体としての特徴を登録しておき、パスワードのように認証に利用する仕組み。銀行などでよく見かける。

指紋	光学式センサや薄型静電式センサ等を用い、特徴点抽出方式やパターンマッチングにより照合する。
声紋	事前収録した音声の周波数パターンと照合する。
虹彩（こうさい）	目を撮影し、虹彩（眼の奥の模様）のパターンを照合する。
掌静脈（てのひら）	LED光源から近赤外線照射を行い、静脈のパターンを照合する。
顔	撮影した顔の画像を解析し、目や鼻の配置を照合する。

デジタル署名

- デジタル署名とは、ユーザ認証(**なりすまし検知**)とメッセージ認証(**改竄の検知**)を行うことができる技術。デジタル署名は、公開鍵暗号方式の応用とも言える方式で認証を行う。



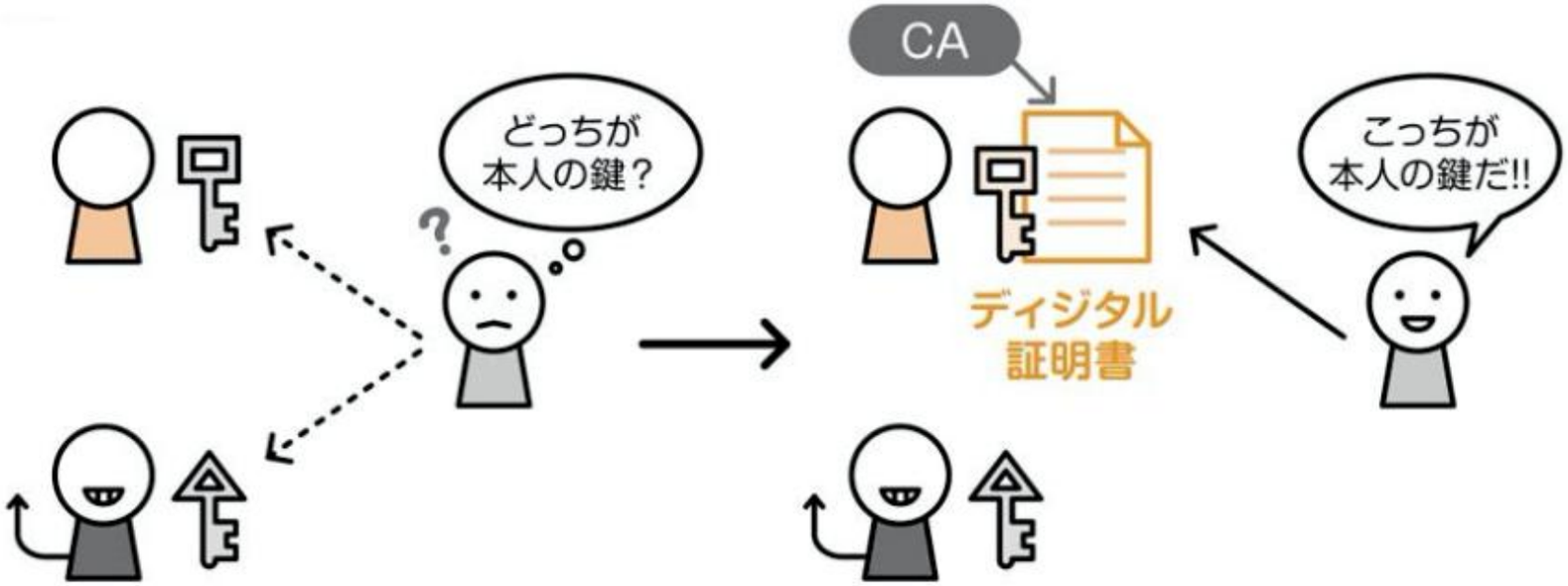
送信者は送信するデータをハッシュ関数という特殊な計算方法によって数値Aに変換し、数値Aを自身の秘密鍵で暗号化し、データと共に送る。

受信者は、送信者の公開鍵で数値Aを復号する。正しく復号できれば、送信者本人から送られてきたものであることがわかる。

認証局

ソフトウェアにデジタル署名を付けたものを
コード署名と呼び、正規品を証明できる。

- デジタル署名では、もしも悪意の第三者が別の送信者になりすまして偽の公開鍵を送ってきた場合、それを用いて署名を検証しても意味がないことになる。そこで、公開鍵の正当性を保証するために、**認証局**[Certificate Authority, CA]という信頼できる機関が申請に基づき、各ユーザの公開鍵に関する**デジタル証明書**[Digital Signal]を発行している。



公開鍵基盤[Public Key Infrastructure, PKI]：デジタル署名など、公開鍵暗号方式による様々なセキュリティの実現を行う環境のこと。

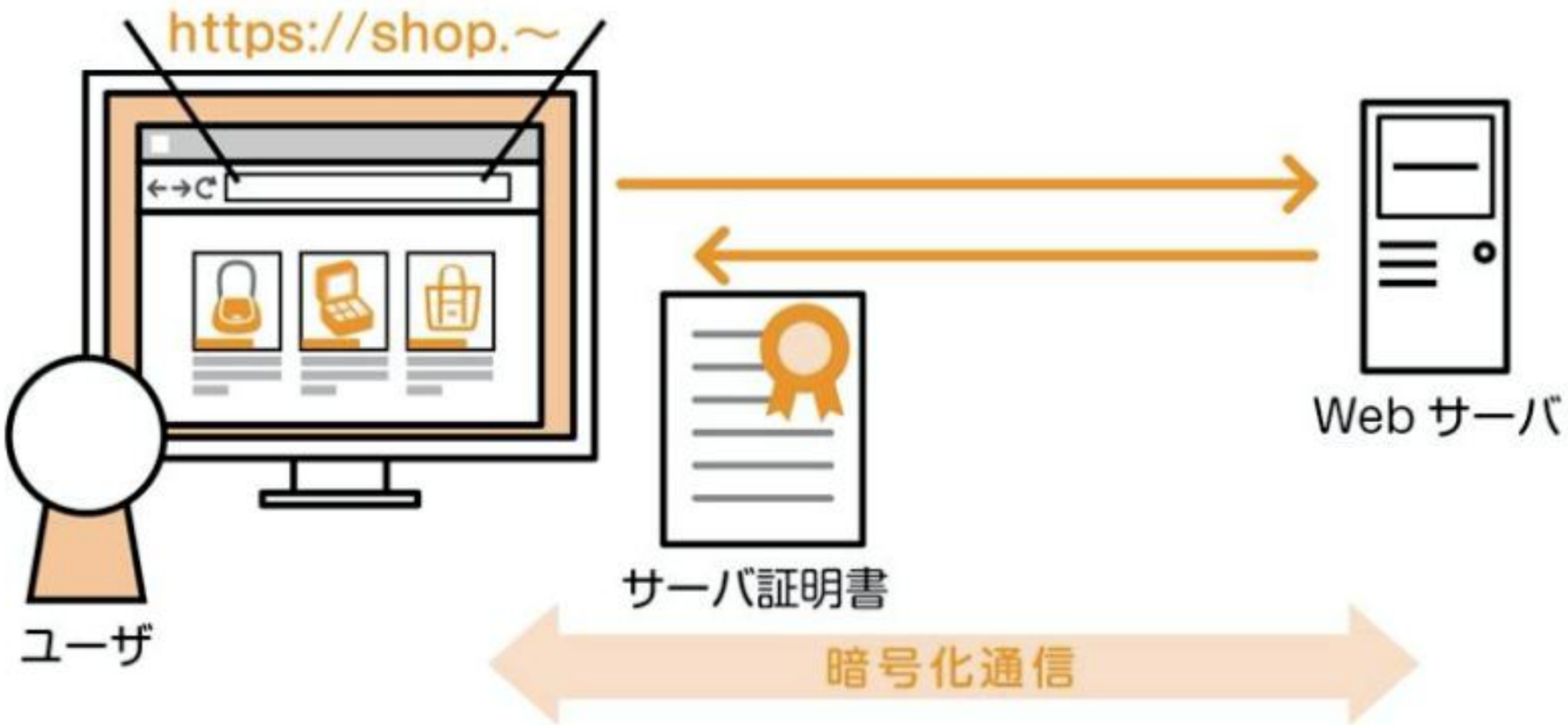
SSL/TLS

- Web サーバと Web ブラウザの間の通信を安全に行えるようにするプロトコルを **SSL**（Secure Sockets Layer）と呼ぶ。

- SSL を利用した通信では、Web サーバの運営組織が正当であることを証明するサーバ証明書を利用するため、Web サイトが偽のサイトではないことが証明される。サーバ証明書は**認証局**が発行し、通信は**暗号化**される。

- SSL はバージョンを重ね、現在は **TLS**（Transport Layer Security）プロトコルに引き継がれているが、SSL の名称が広く普及したため「**SSL/TLS**」のように表記されることが多い。

次へ



Woodland Academy

Q&A

まとめ

Sum Up

1.セキュリティの基本要素：
① 脅威と脆弱性、
② 7 大要素、
③ リスクマネジメント。

2.暗号化方式：共通鍵、公開鍵。

3.認証技術：ユーザ認証、メッセージ認証。

Woodland Academy

Woodland Academy

Thank you!

From Seeds to Woodland — Shape Your Future.

Shape Your Future