Class 7 -3

情報セキュリティの基礎

問題解説資料

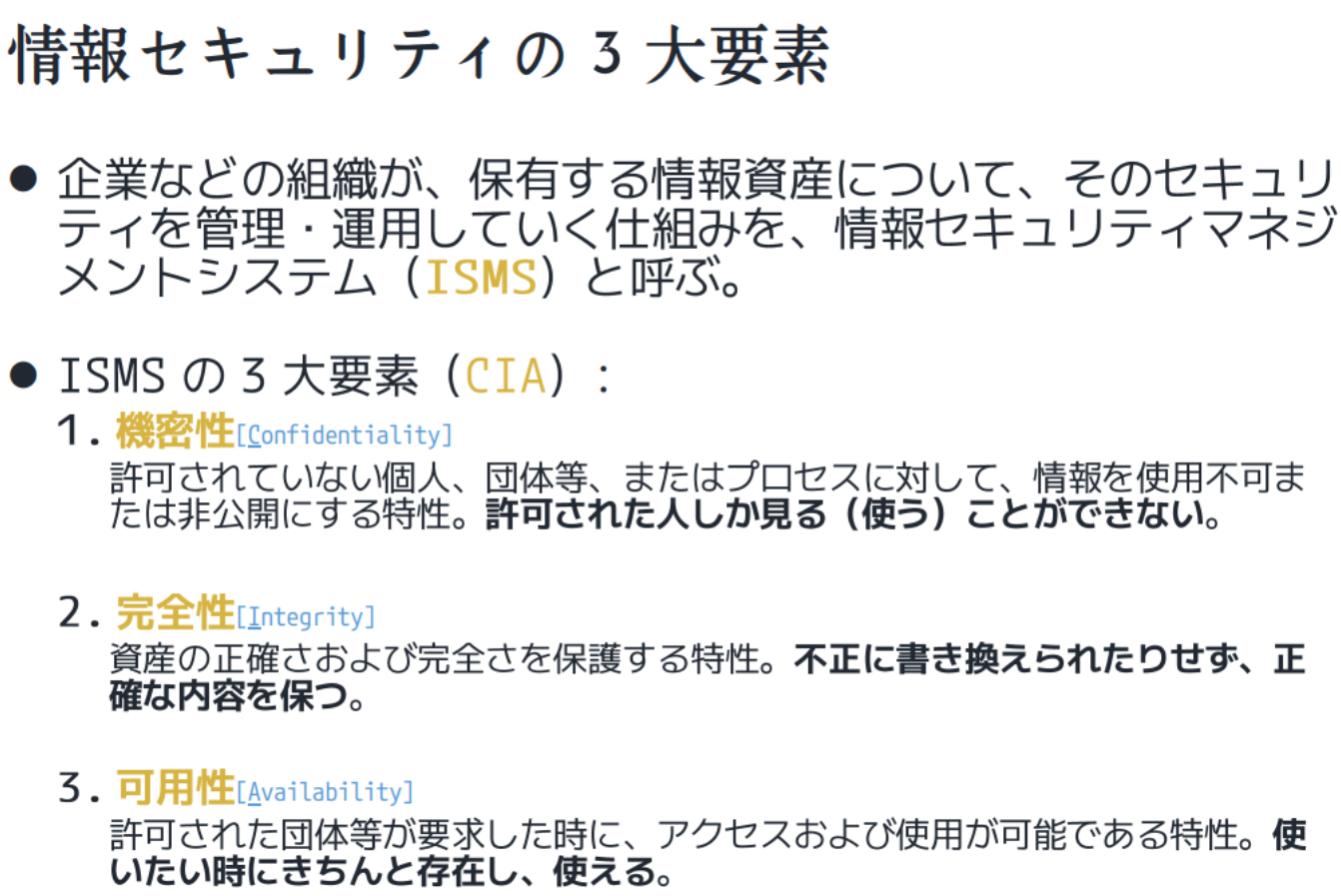
情報資産と脅威

- 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。

企業や組織には、重要な営業機密に関する情報や、顧客、社員などの個人情報など、多くの情報が保管されています。また、企業や組織のシステムに不具合が生じ、サービスが停止してしまうことで、社会的に大きな影響を与えてしまう場合もあります。情報通信技術が発達した社会においては、企業や組織が適切な情報セキュリティ対策を取ることは、当然の責務であるといえます。

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。



企業や組織における情報セキュリティとは、企業や組織の情報資産を「機密性」、「完全性」、「可用性」に関する脅威から保護することです。

。

企業や組織においては、保有する情報資産の特質をよく検討して、機密性、完全性、可用性のバランスを考慮しながら情報セキュリティ対策を行うことが大切です。

機密性（confidentiality）とは

機密性とは、情報に対するアクセス権限を徹底して保護・管理することです。

情報を外部に見せない、漏らさないことを意識することで、高い機密性を保持できます。逆に、企業内に保持する情報に誰でもアクセスできる状況にあれば、それは機密性の低い状態です。

情報の機密性が低ければ、情報漏えいや情報の破損などの原因になりかねません。機密性を高めるためには、アクセスコントロールのルール設定やパスワード認証、情報自体の暗号化などといった手法が利用されます。

機密性を高める必要がある情報には、例えば次のようなものが挙げられます。

- 社員の個人情報
- 顧客情報
- 新製品の開発情報
- システムへアクセスするためのパスワード

では、機密性を高めるためには、具体的に何をすればよいのでしょうか。

具体的な施策には以下が挙げられます。

- 情報を保存した HDD などは、アクセスコントロールされた場所（データセンターなど）に設置する
- パスワードに「123456」などの安易なものを設定しない
- ID/パスワードをメモなどに残さない
- 情報を外部へ持ち出さない
- 正当な権限を持つ者だけが情報にアクセスできる仕組みを作る

完全性（integrity）とは

完全性は、改ざんや過不足のない正確な情報が保持されている状態を指します。完全性が失われると、そのデータの正確性や信頼性が疑われ、信頼性が疑わしいデータは利用価値が失われます。

例えば、企業の Web サイトの改ざんが起こった場合には、企業としての信頼を失うことにもつながりかねません。

完全性を保持する方法には以下のような対策が考えられます。

- 情報にはデジタル署名をつける
- 情報へのアクセス履歴を残す
- 情報の変更履歴を残す
- バックアップなどの情報を保管するルールを決める

もし、一般的な企業の情報に完全性がなければ、企業自身はもちろん、その企業の取引先などにも大きな混乱と損失を招く事態になる可能性があります。

また、IoT が普及する社会の中で情報の完全性が保てなくなると、医療やスマートカーなどで、人命にかかわる被害が出る恐れもあるのです。

可用性（availability）とは

可用性は、情報をいつでも使える状態を保持することです。必要なときに情報へアクセスでき、目的を果たすまでアクセスやデータ処理が中断されないシステムは、可用性の高いシステムだといえるでしょう。

例えば、クラウドサービスでは、24 時間 365 日（メンテナンス時間を除く）いつでもデータやシステムにアクセス可能です。これにより、クラウドストレージに保存しているデータは、パソコンやスマートフォンでいつでもアクセスできますし、ファイルはいつでも編集できます。

可用性を保つためには、以下のような施策が考えられます。

- システムの二重化（多重化）
- HDD の RAID 構成
- UPS（無停電電源装置）
- BCP（事業継続対策）
- システムのクラウド化

可用性については、オンプレミスでも実現可能です。しかし、管理・運用コストやトラブル時の対応工数、また近年多くの企業で進められている DX（デジタルトランスフォーメーション）への取り組みでもクラウドの積極的な利用が増えています。

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

完全性(Integrity)とは、情報セキュリティマネジメントの概念の一要素で、情報に矛盾がなく完備され、改ざん・破壊されていない特性をいいます。また完全性とともに情報セキュリティマネジメント三要素に位置付けられている特性に「機密性」と「可用性」があります。

機密性

許可された正規のユーザだけが情報にアクセスできる特性を示す。

可用性

システムが正常に稼働し続けることの度合い。ユーザが必要な時にシステムが利用可能である特性を示す。

各選択肢の事例がどの要素を脅かすものかを考えます。

- Web ページの改ざん
  正しい。完全性を脅かす攻撃です。
- システム内に保管されているデータの不正コピー
  機密性を脅かす攻撃です。
- システムを過負荷状態にする DoS 攻撃
  可用性を脅かす攻撃です。
- 通信内容の盗聴
  機密性を脅かす攻撃です。

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。

情報セキュリティ 7 要素に含まれる 4 つの新要素

情報セキュリティには、先に紹介した 3 要素に加えて、新たな 4 つの新要素があります。

- 真正性（Authenticity）
- 信頼性（Reliability）
- 責任追跡性（Accountability）
- 否認防止（non-repudiation）

これらは主に、情報へのアクションが「誰の行為か」を確認できるようにすることや、システムが確実に目的の動作をすること、また、情報が後から否定されない状況を作ることで情報セキュリティを確保するものです。

それでは、4 つの新要素の内容を見ていきましょう。

真正性（Authenticity）とは

真正性とは、情報にアクセスする企業組織や個人あるいは媒体が「アクセス許可された者」であることを確実にするものです。情報へのアクセス制限は、情報セキュリティにおいても重要な要素です。

真正性を実現する具体的な施策には、以下のようなものが挙げられます。

- デジタル署名
- 二段階認証
- 多要素認証（生体認証を含む）

信頼性（Reliability）とは

信頼性は、データやシステムを利用した動作が、意図した通りの結果を出すことです。

データやシステムは、ヒューマンエラーやプログラムの不具合（バグなど）によって、期待する結果が得られないこともあります。情報セキュリティには、このような事態を防ぐための施策が必要です。

信頼性を実現する具体的な施策には、以下のようなものが挙げられます。

- システムやソフトウェアが不具合を起こさない設計を行う
- 不具合のない設計をもとに構築を行う

- ヒューマンエラー（操作ミスなど）が起こっても、データが改ざんされたり消失したりしない仕組みを施す

責任追跡性（Accountability）とは

責任追跡性とは、企業組織や個人などの動きを追跡することです。これにより、データやシステムへの脅威が何であるのか、あるいは誰のどのような行為が原因なのかを追跡します。

責任追跡性の具体的な施策には、次のようなものが挙げられます。

- アクセスログ
- システムログ
- デジタル署名
- 操作履歴
- ログイン履歴

否認防止（non-repudiation）とは

否認防止は、情報が後に否定されないように証明しておくことです。

例えば、組織や個人が情報の改ざんや情報利用をした場合、本人がそれを後から否認できないようにログを取っておくなどの措置が否認防止にあたります。

否認防止は、責任追跡性の施策にて実現でき、主にデジタル署名や各種ログが利用されます

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。

ISMS（Information Security Management System）とは、情報セキュリティマネジメントを行うための仕組みのことです。

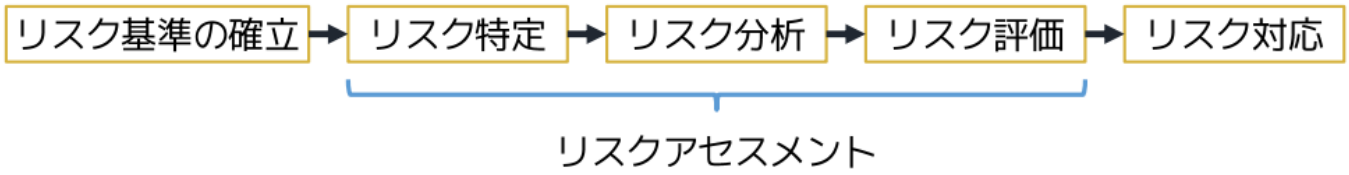
簡単にいうと、**組織がもつ情報の外部流出を防ぐとともに、利用しやすい状態で情報を保護するための仕組み**です。

社内の情報を守るためには、社員一人ひとりが心がけるだけではいけません。また、一部の専門家だけが理解している状態でも意味がありません。組織として情報を適切に管理できる体制を構築する必要があり、そのための仕組みが ISMS です。**ISMS の要求事項を適切に満たして第三者機関の審査を受けることで、ISMS 認証を取得できます。**ISMS 認証の取得は、セキュリティ体制が整備されている証明になるため取引先や顧客の信頼につながります。**ISMS の対象が企業全体または一部の組織で所有する情報全般**であるのに対し、**P マークの対象は企業全体で所有する個人情報**です

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）

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。

暗号化とは、**元のデータや通信内容を不規則な文字列に変換する処理**のことです。

仮に個人情報が流出したとしても、**データはランダムな文字列で表示されるため、第三者による解読や悪用を防止**できます。

暗号化の身近な例が、「インターネット通信」です。

インターネット通信に暗号化が施されていなければ、万が一サイバー攻撃を受けた際に、顧客が入力したクレジットカード情報などが第三者に盗み取られる恐れがあります。

そこでユーザーが利用するブラウザとサーバー間の通信を『暗号化』することで、**第三者にデータを解読されることのない安全なインターネット環境を構築できる**というわけです。

暗号化では、システムやソフトウェアを用いて、テキストメッセージや電子メールのような平文（元のデータ）を、**「暗号テキスト」と呼ばれる解読不可能な文字列**に変換します。

そして受信者がデータにアクセスすると、情報は元の形式に変換されます。

これを**「復号化」**といいます。

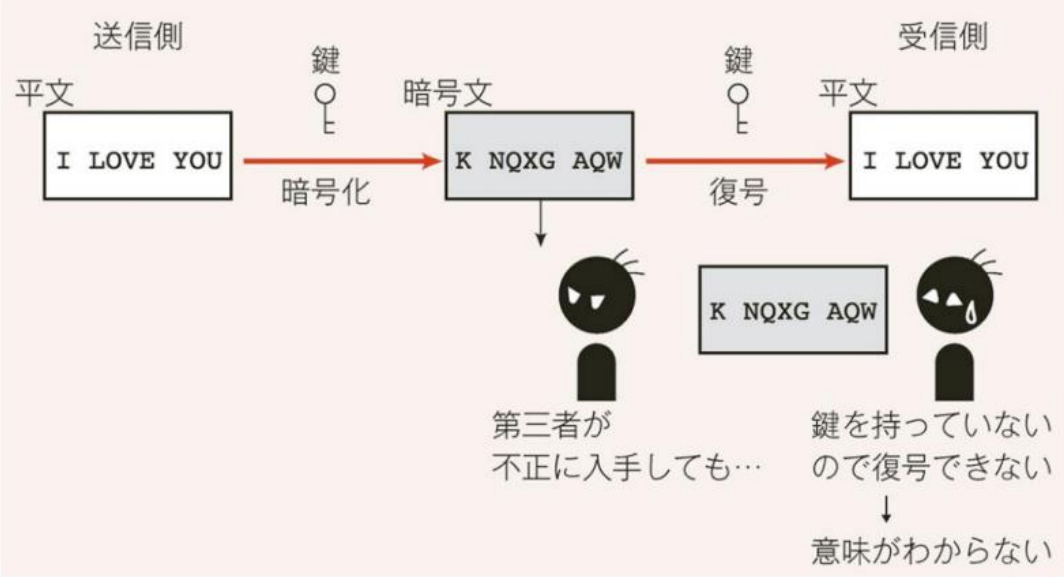
暗号化のポイントは「鍵」です。

暗号鍵がなければ、データの暗号化と復号化はできません。

また見方を変えれば、暗号鍵が他者に渡ってしまうと、データを解読されてしまいます。

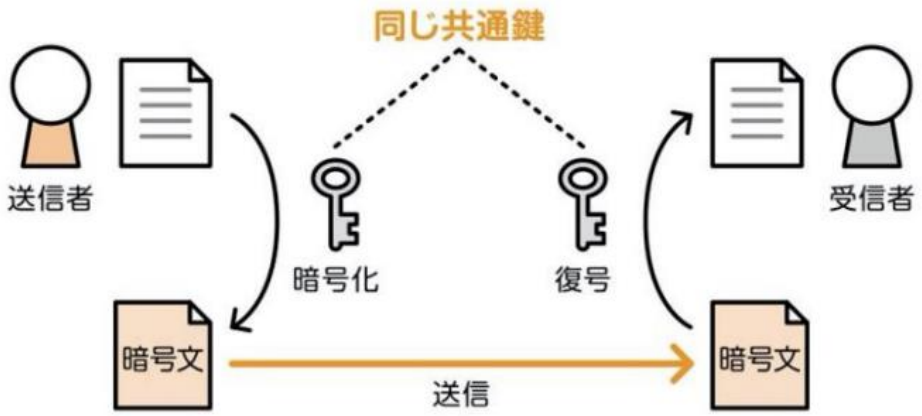
そのため、**暗号鍵は厳重に保管しなければいけません**。

暗号化の流れ


送信側
受信側
鍵
鍵
平文
暗号文
平文
I LOVE YOU
暗号化
K NQXG AQW
復号
I LOVE YOU
K NQXG AQW
第三者が
不正に入手しても…
鍵を持っていない
ので復号できない
意味がわからない

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。



「共通鍵暗号方式」とは、**データの暗号化と復号化に同じ鍵（共通鍵）を用いる方式**です。

主にファイルの暗号化に使用されます。

共通鍵暗号方式のメリットは、簡単な暗号アルゴリズムを用いるため、**データの暗号化と復号化の処理速度が早いこと**です。

一方で、暗号鍵をデータ受信者に渡す途中で、第三者に鍵を盗まれるリスクがあります。

また、**データのやり取りをする相手ごとに異なる暗号鍵を用いる必要があり、鍵の管理が大変になる**デメリットもあります。

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。

「公開鍵暗号方式」とは、**データの暗号化と復号化で別々の鍵を用いる方式**です。

暗号化に用いる鍵を**「公開鍵」**、復号化に用いる鍵を**「秘密鍵」**と呼びます。

公開鍵暗号方式の流れは、以下の通りです。

1. 1.データ受信者が公開鍵と秘密鍵を作成
2. 2.公開鍵のみ一般公開（送信者に共有）
3. 3.データ送信者は公開鍵を用いて、データの暗号化を実施
4. 4.暗号化したデータを送信
5. 5.受信者は秘密鍵を用いてデータを復号

「公開鍵」で暗号化したデータは、対となる「秘密鍵」でなければ復号できないため、一般公開しても問題ありません。

また公開鍵暗号方式では、復号化に用いる**「秘密鍵」を管理するのはデータ受信者のみ**。

鍵の盗難リスクがないことに加え、複雑な暗号アルゴリズムを用いる点も踏まえると、**安全性が高い方式**だと言えます。

また、やり取りする相手ごとに鍵を用意する必要がないため、鍵の管理が楽です。

一方で、複雑なアルゴリズムを用いるため、**処理速度が遅い**デメリットがあります。

前へ

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。

「ハイブリッド暗号方式」とは、**共通鍵暗号と公開鍵暗号を組み合わせた方式**を示します。

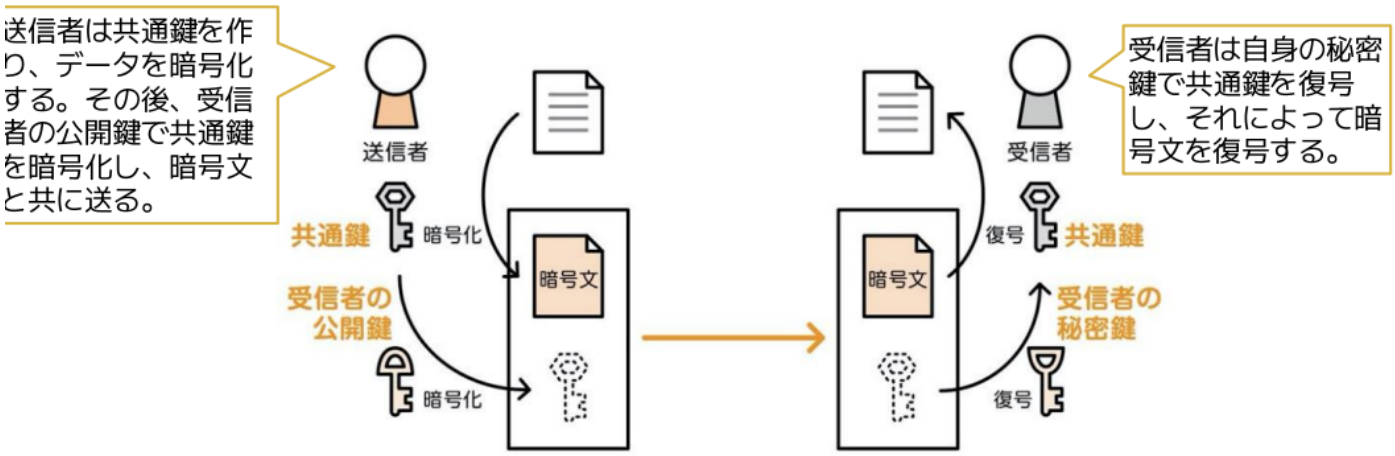
ハイブリッド暗号方式の流れは以下の通りです。

1. 1.**【受信者】**公開鍵と秘密鍵を作成する
2. 2.**【受信者】**公開鍵をデータ送信者に送る
3. 3.**【送信者】**共通鍵を作成しデータを暗号化する
4. 4.**【送信者】**公開鍵で共通鍵を暗号化する
5. 5.**【送信者】**暗号化した共通鍵とデータを受信者に送る
6. 6.**【受信者】**秘密鍵で共通鍵を復号する
7. 7.**【受信者】**復号した共通鍵でデータを復号する

ハイブリッド暗号方式では、「共通鍵」を利用して暗号化し、その共通鍵の受け渡しには、データの受信側で作成した「公開鍵」を使います。

そうすることで、**共通鍵を安全に手間をかけずに送ることが可能**です。

またその共通鍵は送信側で 1 回の通信だけで使い捨てるものとして作られるため、**コンピュータへの負荷が少ない**点も大きなメリットです。



【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。

2 つの暗号方式には以下のような特徴があります。

共通鍵暗号方式

暗号化と復号に同じ鍵を使用する暗号方式。暗号化通信を行う前にあらかじめ使用する鍵を相手に安全に送る必要がある。

ロジックが単純なためシステムに組み込みやすく、計算量も少ないため暗号化・復号に要する処理時間が短いという利点がある。

代表的なアルゴリズムは DES、AES、IDEA など

公開鍵暗号方式

暗号化と復号に異なる鍵を使用する暗号方式。暗号化鍵は誰もが使用できるように公開し(公開鍵)、復号鍵は受信者が厳重に管理する(秘密鍵)。

暗号化鍵と復号鍵は一対のペアとして生成され、1 つの暗号化鍵で暗号化されたデータは、その鍵のペアである復号鍵でしか元のデータに戻せないため、復号を行えるのは正当な受信者のみであることが保証されている。送信データの改ざん検知に使用するディジタル署名は公開鍵暗号式の技術を応用した仕組みである。

代表的なアルゴリズムは RSA、楕円曲線暗号など

- 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。
  共通鍵暗号方式では 2 人が共通の鍵を使用するので 1 つ、公開鍵暗号方式では公開鍵と秘密鍵のペアを使用するため 2 つが必要です。したがって暗号化通信する相手が 1 人のときには共通鍵暗号方式のほうが鍵数が少なくなります。
- 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。
  共通鍵が漏えいすると通信の秘匿を保てないので厳重に管理しなくてはなりません。
- 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。
  正しい。共通鍵暗号方式は公開鍵暗号方式と比較して暗号化・復号に必要な計算量が少ないため処理時間が短いという利点があります。
- 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。
  公開鍵暗号方式の特徴です。共通鍵暗号方式では鍵ペアを作成することはありません

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

公開鍵暗号方式を使用した暗号化通信は、以下の手順で行います。

1. 送信者は、**受信者の公開鍵**を使ってデータを暗号化し、相手に送信する
2. 受信者は、**自分の秘密鍵**を使って受信したデータを復号する

図　公開鍵暗号通信

この暗号化通信は「暗号化は誰でもできるが、復号できるのは正規の秘密鍵を持つ受信者だけ」という性質を持ちます。データが途中で傍受されても、秘密鍵を持たない者には復号を行うことができないため安全性が確保されます。

送信者はＡさん、受信者はＢさんですから、電子メールの復号に使う鍵は「Ｂさんの秘密鍵」になります。

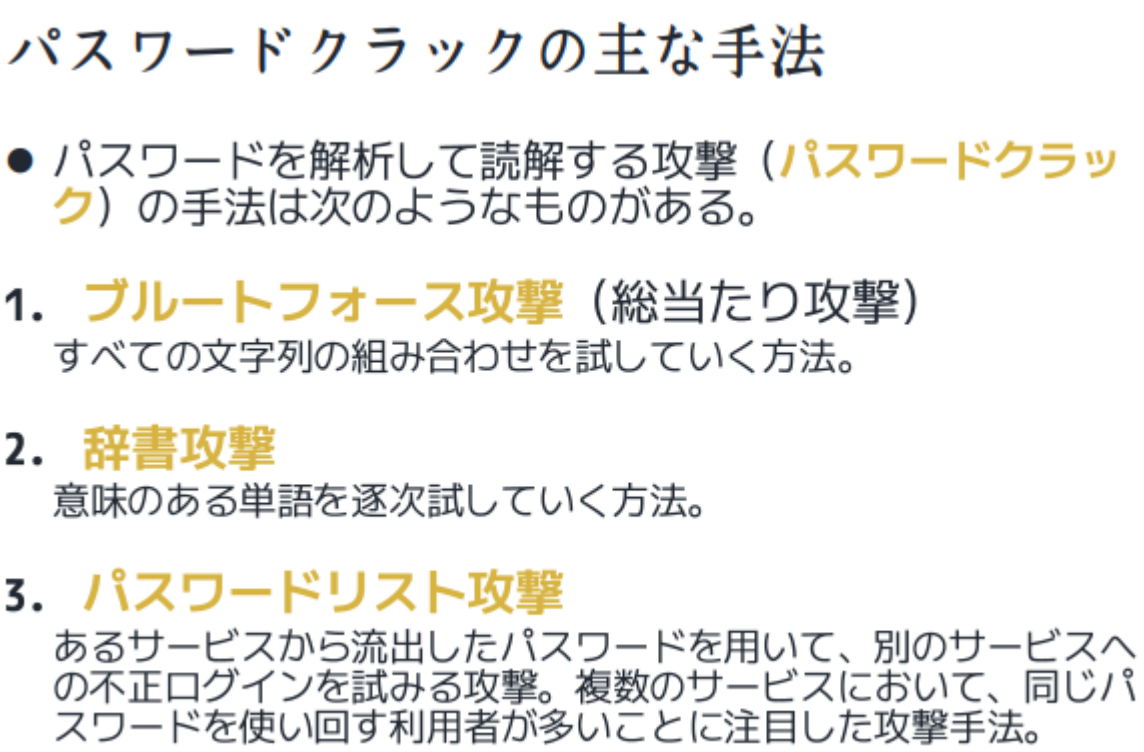
」

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。



・ブルートフォース：力ずくでという意味

・辞書に載っている単語を元にパスワードに使われていそうな文字列を辞書化

片っ端から試す

改竄→かいざん

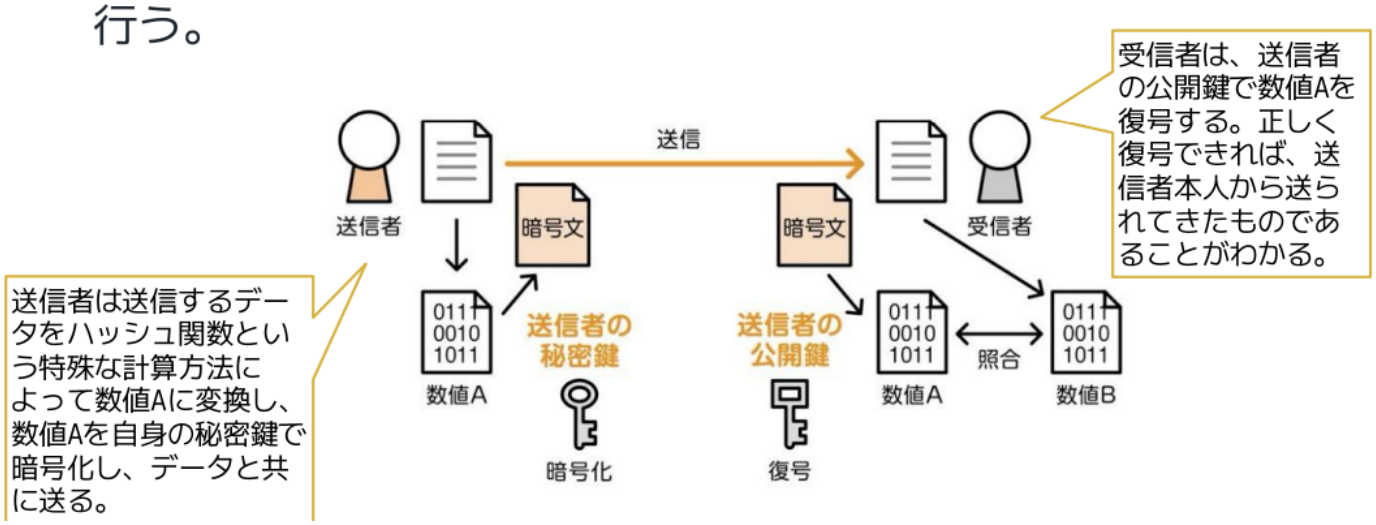
その他のユーザ認証技術

- **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（てのひらじょうみゃく）	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

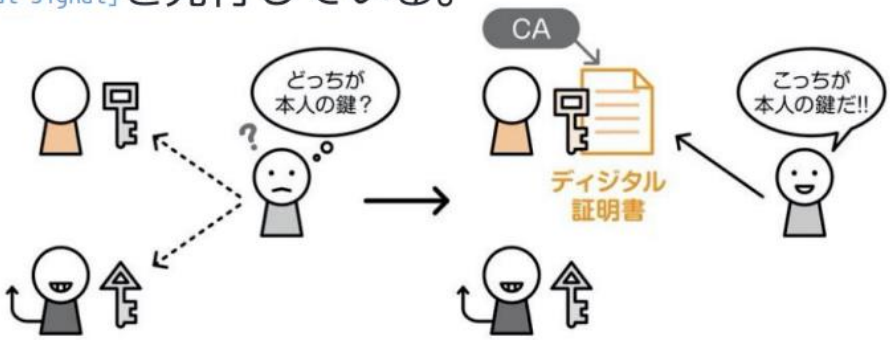
- デジタル署名とは、ユーザ認証(**なりすまし検知**)とメッセージ認証(**改竄の検知**)を行うことができる技術。デジタル署名は、公開鍵暗号方式の応用とも言える方式で認証を行う。



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。

プロトコル：コンピュータでデータをやりとりするために定められた手順や規約、信号の電気的規則、通信における送受信の手順などを定めた規格

前へ