

## 2-6 ITセキュリティ

東京大学 数理・情報教育研究センター

2021年4月30日

# 概要

- 本節では IT(情報技術)セキュリティの概略とその用語について学びます。
- 次いで、情報セキュリティに関連の深い情報技術について学びます。

# 本教材の目次 1/2

1. セキュリティ(security)とは	P.5
2. 情報とは	P.6
3. 情報セキュリティ	P.7
4. 機密性(Confidentiality)	P.8
5. 完全性(Integrity)	P.9
6. 可用性(Availability)	P.10
7. 真正性(Authenticity)	P.11
8. 責任追跡性(Accountability)	P.12
9. 否認防止(non-repudiation)	P.13
10. 信頼性(Reliability)	P.14
11. 情報の分類	P.15
12. 情報セキュリティリスク	P.16

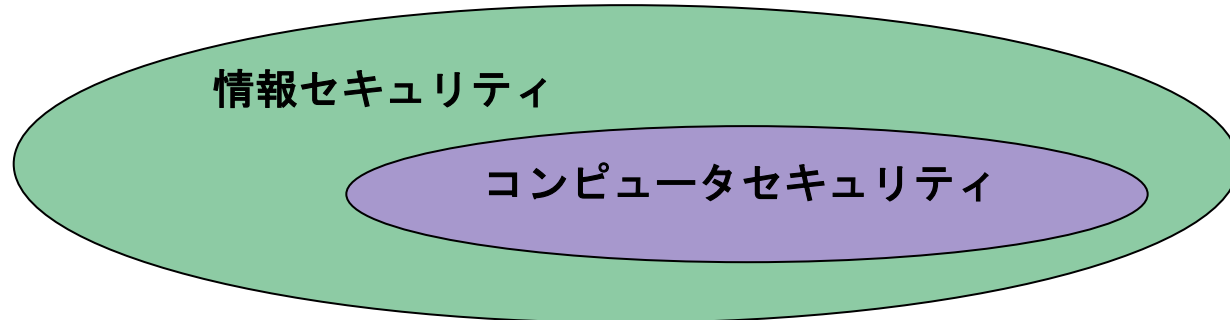
# 本教材の目次 2/2

13. リスク対応	P.17
14. 情報セキュリティに関連する技術など	P.18
15. 暗号で使われる用語	P.20
16. 簡単な暗号の例：シーザ暗号	P.21
17. 共通鍵暗号方式	P.22
18. 公開鍵暗号方式	P.23
19. ハッシュ値	P.24
20. デジタル署名	P.25
21. 公開鍵基盤(Public Key Infrastructure:PKI)	P.26
22. PKIの応用：Web サーバの真正性、通信の秘匿性	P.27
23. アクセス制御	P.28
24. 認証	P.29,30
25. バックアップ・冗長化	P.31

# セキュリティ(security)とは

国語辞書「スーパー大辞林」では以下のように示されています：

1. 安全, 防犯, 安全保障。
  2. (有価) 証券。
  3. コンピューターセキュリティ  
“コンピューターを利用する上での安全性。コンピューターへの不正アクセスやデータの改竄（かいざん）などの問題を扱う分野”
- 本節の IT セキュリティでは、狭義の③コンピュータセキュリティだけではなく、より広義の情報の①安全をあつかいます。  
例えば、個人情報が漏洩するような事象では、データの漏洩経路としてコンピュータネットワーク、印刷物などが考えられます。どちらの経路でも情報セキュリティの問題であることは変わりません。一方、前者はコンピュータセキュリティの問題ですが、後者はそうではありません。
  - この資料は、情報セキュリティマネジメント体系（Information Security Management Systems: ISMS）をとりあつかった日本産業規格 JIS Q27000:2019 系列文書に沿った内容としています。



# 情報とは

文脈に依存するが、日本産業規格（JIS X 0001-1994）では情報とデータを以下のように定義している。

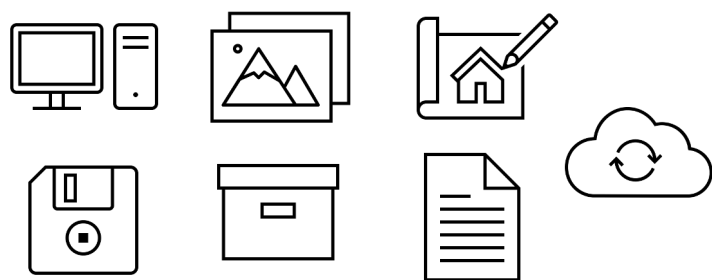
**情報**：“事実、事象、事物、過程、着想などの対象物に関して知り得たことであって、概念を含み、一定の文脈中で特定の意味をもつもの。”

**データ**：“情報の表現であって、伝達、解釈又は処理に適するように形式化され、再度情報として解釈できるもの。”

情報セキュリティにおける「情報」には上の「データ」の意味も含まれる。さらに ISMS では「文書化した情報」を以下のように定め、適切な取り扱いを求めている。

組織が管理し、維持するよう要求されている情報、及びそれが含まれている媒体。文書化した情報は、あらゆる形式及び媒体の形をとることができ、あらゆる情報源から得ることができる。

注）管理、維持が要求されている情報であれば該当する。すなわち、意図的に記録、保存していなくても該当する。



あらゆる形式・媒体



あらゆる情報源

# 情報セキュリティ

以下の情報セキュリティの **3要素**(CIA)を維持すること。

1. 機密性 (Confidentiality)
2. 完全性 (Integrity)
3. 可用性 (Availability)

さらに、維持対象として以下を加え **7要素**とする場合もある。

4. 真正性 (Authenticity)
5. 責任追跡性 (Accountability)
6. 否認防止 (non-Repudiation)
7. 信頼性 (Reliability)

# 機密性(Confidentiality)

許可されていない個人、組織、プログラムなどに情報を使用させず、開示しない特性。

- パスワード流出・個人情報漏洩など多く報道されている。企業の製品設計図や、未発表論文のデータ漏洩なども機密性に関わるもの。
- 機密性に関する問題は多岐にわたっている。漏洩経路だけをみても、ネットワークの盗聴・記憶装置の流出といった情報機器を介するだけでなく、内部協力者・廃棄文書といった古典的なものも少なくない。

機密性にかかわる事象と影響の例：

- 試験問題の漏洩によって、試験の公正性・公平性を損なう。
- 新商品の情報が競合他社に漏れ、競争上の不利益になる。
- 個人情報の漏洩によって、当局から多額の制裁金を課される。



# 完全性(Integrity)

情報の正確さ及び完全さの特性。

- 情報が最新・正確に維持されること。
- データ破壊や悪意を持つもの（内部、第三者）による改ざんも含まれる。
- データ破壊の原因には、機器故障・操作ミス・有害なソフトウェア（マルウェア）によるものに加え、媒体の経年劣化や、通信路のノイズによるものも含まれる。
- データ改ざんは不正行為の隠蔽を目的としておこなわれたこともある。

完全性にかかわる事象と影響の例：

- 試験採点結果が誤って記録され、成績評価に影響した。
- 取引先の連絡先情報が古いままで更新されておらず、必要な連絡がとれない。
- 組織ホームページが書き換えられ、信用失墜につながる。

# 可用性(Availability)

認可された利用者やプログラムなどが要求したときにアクセスおよび使用が可能である特性。

- 情報を利用しなければならないときに利用できること。  
利用するのはヒトだけではなくコンピュータプログラムも含まれます。
- 廃棄によるデータ（文書）の**消失**、情報**サービスの停止**もこの特性に関わる。ここでの停止の原因は計画的・事故を問わない。

可用性にかかわる事象と影響の例：

- 試験当日に試験問題冊子が紛失し、試験が実施できない。
- 秘伝のレシピを知る唯一の料理人が急病で、開店できない。
- 銀行の ATM が取引中に突然停止した。キャッシュカードも返却されず、必要な買い物ができなかった。

# 真正性(Authenticity)

利用組織及び人、設備、ソフトウェア及び物理媒体などがそれが主張するとおりのものであること。

- 情報サービス、媒体の利用者、提供者が**なりすまし**ではないこと。

真正性にかかわる事象と影響の例：

- 試験をなりすましで受験され、試験の公正性・公平性を損なう。
- なりすましの取引先から発行された請求先に送金し、損失を被った。
- 発行元の不明なソフトウェアをコンピュータにインストールしたところ、それは**マルウェア**\*であり、内部情報を搾取されたうえ重要なデータを削除された。

(\*)不正かつ有害な動作をするコンピュータソフトウェア

# 責任追跡性(Accountability)

- 誰が情報に対する操作をおこなったかを後から追跡できること。  
作成・読み・更新・削除といった操作に加え、権限付与も含まれる。
- 情報機器のアクセスだけではなく、建造物・部屋などへの入退室記録も責任追及性に関わる。

責任追跡性にかかわる事象と影響の例：

- 学生からの申告で試験成績が改ざんされたことは明らかとなったが、誰が・いつ改ざんをおこなったかが不明。
- システム管理者（複数）には業務上の都合からあらゆる操作を許す特権的アクセスが与えられていた。特権操作による事故が発生したがどの管理者が操作したかあきらかにできない。

# 否認防止(non-repudiation)

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（実体）を証明する能力。

- いわゆるしらばっくれを検出できる特性のこと。合意した内容を後から否定することができない。

否認防止にかかわる事象と影響の例：

- 価格・納期を決めて売買契約を締結したが、後で契約を否定され損害を被る。

# 信頼性(Reliability)

意図する行動と結果とが一貫しているという特性。

- バグによるシステム誤動作がこの特性に関係している。
- 情報システムだけではなく人や組織が想定した結果を出せないことも含まれる。

信頼性にかかわる事象と影響の例：

- ソフトウェアをバージョンアップしたが新旧バージョンで動作が異なる、旧バージョンに依存していた業務が滞る。
- 通販サイトで発注したものと違ったものが届く、納品遅れ・返品などでコストがかかる。

# 情報の分類

すべての情報に対しセキュリティ特性（3 or 7 要素）を最高レベルで維持することは現実的ではない。一方で個別の情報の内容ごとに異なる対応をとることも現実的ではない。

- ISMS では情報を格付け（分類）し、必要なレベルで管理する方法が示されている。例えば、機密性については以下のような分類が考えられる。
  - a. 開示されても損害が生じない。
  - b. 開示された場合に、軽微な不具合が生じる。
  - c. 開示された場合に、重要な短期的影響が及ぶ。
  - d. 開示された場合に、組織の存続が危機にさらされる。

情報ごとに求められる特性は異なるため、分類にあたってはそれぞれの特性も考慮する必要がある。

- 一部のみ重要：商品のマニュアルは開示されても損害が生じないが内容の正確性は求められる。すなわち、機密性【低】・完全性【高】といった分類がされる。
- 時間によって格付けが変わる：新製品の情報は発表前は機密性【高】と分類されるが、発表後は公知となり機密性【低】となる。。

# 情報セキュリティリスク

## 情報セキュリティリスク

- 脅威が弱点に付け込み、その結果、組織に損害を与える可能性に伴って生じる。

## 脅威

- 損害を与える可能性がある、望ましくない事態の潜在的な原因。

## リスク

- 目的に対する不確かさによる期待からの乖離（ズレ）のこと。乖離には好ましいものも含まれる。
- 不確かな「事象」の起こりやすさと、その結果の組み合わせとして表現されることも多い。



# リスク対応

リスクを修正する活動（プロセス）のこと、以下の事項が含まれます。

以下の対応例では、管理者権限でおこなうコンピュータ操作におけるリスクに対するものを示しました。  
注）コンピュータに対する操作にはシステムを破壊するものも含まれます。Windows などの OS では危険な操作は管理者権限でのみ実行できるようにし、一般利用者には必要なときのみ管理者権限を与えるようにしています。

リスク対応の事項	対応の例
リスクを生じさせる活動をおこなわないことで、回避する。	データが破壊される可能性があるため、管理者権限での操作を禁止する。
機会を追求するために、リスクをとるまたは増大させる。	業務の効率を上げるため、全ての一般利用者に常時管理者権限を与える。
リスク源を除去する。	危険な操作をおこなうプログラムをすべて消去する。
結果を変える。	いつ破壊されても復元できるようにバックアップの回数を多くする。
他者とリスクを共有する。	管理者権限が必要な操作は他社に外注する。
リスクを評価したうえで、リスクを保有する。	事故が発生しても業務への影響は軽微なので、そのまま様子を見る。

リスク対応があらたなリスクを生じさせたり、既存の別のリスクを増大させることもあります。

# 情報セキュリティ：まとめ

- 情報の機密性(C), 完全性(I)及び可用性(A)（情報セキュリティの3要素）を維持すること。真正性, 責任追跡性, 否認防止, 信頼性（7要素）を加えることもある。
- 対象はあらゆる形式及び媒体の形をとることができ、あらゆる情報源から得ることができます。
- リスク対応にはリスク除去以外にもさまざまな方法があります。リスクを評価したうえで保有しつづけることも含まれます。

# 情報セキュリティに関連する技術など

これまでに説明した情報セキュリティの維持にはさまざまな技術・手法が使われています。以下について説明します。

先に暗号技術を取り上げます。

- 暗号技術  
簡単な暗号の例/共通鍵暗号/公開鍵暗号/ハッシュ値/電子署名/公開鍵基盤
- アクセス制御
- 認証
- バックアップ・冗長化

# 暗号で使われる用語

**暗号化**：秘匿化を目的にデータを権限を与えられていない者にとって意味のわからないデータに変換する操作

平文：変換前のデータ

暗号文：変換後のデータ

**復号化**：暗号から平文に変換する操作

アルゴリズム：暗号化・複合化の手続き

鍵：アルゴリズムの結果を決定する情報

解読：第三者が暗号から平文に変換する操作

メッセージ：交換される情報\*

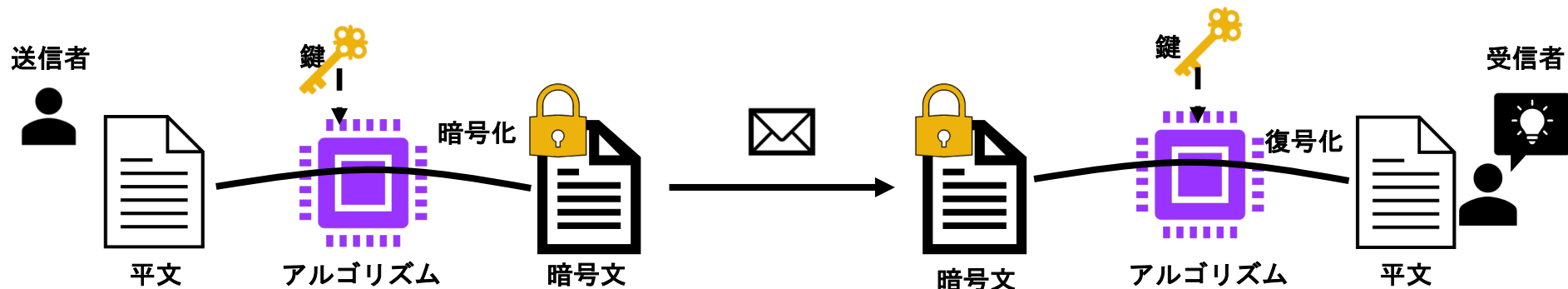
古典暗号：アルゴリズム・鍵の両方を秘匿する。

現代暗号：アルゴリズムは公開し、鍵だけを秘匿する。

アルゴリズムはプログラムなどで利用者に配布する必要があり、秘匿することは事実上不可能です。

一方、公開によって第三者の安全性評価が可能となり信頼性が向上するという利点があります。

(\*) 暗号は情報交換を前提に設計されることからこの用語がよく使われる。



# 簡単な暗号の例：シーザ暗号

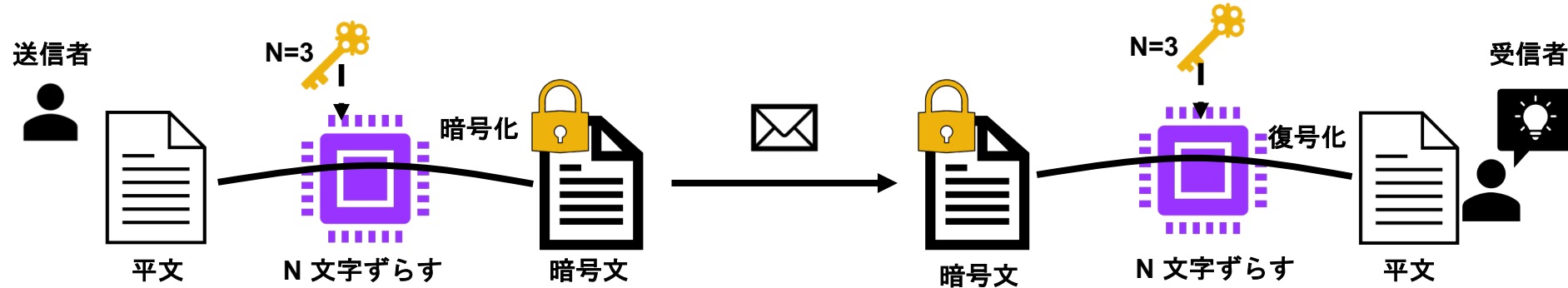
紀元前から使われている方式です。平文の文字をアルファベット順に3文字ずらして暗号文に変換します。平文と暗号文の文字の対応を以下に示します。

平文	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
暗号文	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

例えば、平文“ICAMEISAW”は暗号文“LFDPHLVDZ”と変換されます。例では平文で“I”が2回登場しており、暗号文では両方とも“L”に変換されます。  
前項の用語との対応は以下のように書けます。

アルゴリズム：文字をアルファベット順に鍵の数だけずらした文字と置き換える。  
鍵：3文字

シーザー暗号の解読方式として、アルファベットでは使われる文字の頻度に差があり、この差を利用する方式がよく知られてます。  
例えば母音文字“AEIUO”はその他の子音よりも頻度が高く、対応する文字“DHLXR”の頻度も高くなります。



# 共通鍵暗号方式

暗号化と復号化で同じ鍵を使用します。前のシーザ暗号や最初の現代暗号の DES\*を含めて、多くの方式が考案されています。

秘匿性の維持には鍵は第三者に知られないことが必要です。個人のスマホデータの暗号化では鍵は当人で管理すればよくあまり問題は生じません。しかし、暗号文を電子メールなどで交換するには送受信者で鍵を安全に、すなわち第三者に知られないように共有する必要があります。

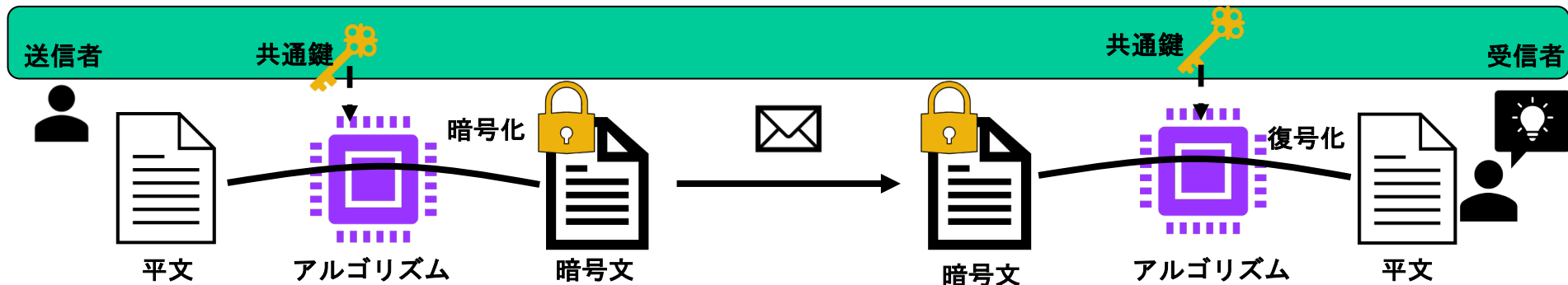
課題：この方式では送受信者が増えると鍵の共有が問題になります。共有方針には大きく分けて以下が考えられます。

1. すべての相手に同じ鍵を共有
2. 相手ごとに異なる鍵を共有

1.は送受信者が増えるに従って鍵が漏洩する可能性が高くなります。

2.では送受信者を  $N$  とすると必要な鍵の数は  ${}_NC_2 = \frac{N(N-1)}{2}$  となり、 $N$  が大きくなると鍵の数が膨大（爆発）となり実用には耐えられません。次に紹介する公開鍵方式を用いることで実用的な鍵の共有ができるようになりました。

(\*) Data Encryption Standard の略、1976 年に合衆国で採用された暗号標準



# 公開鍵暗号方式

暗号化にだれにでも公開してよい公開鍵を、復号化で所有者以外に知られない秘密鍵の鍵ペアを使用する暗号方式で、RSA 暗号\*がよく知られています。秘匿性の維持だけではなく、完全性・真正性の維持にも利用されます。

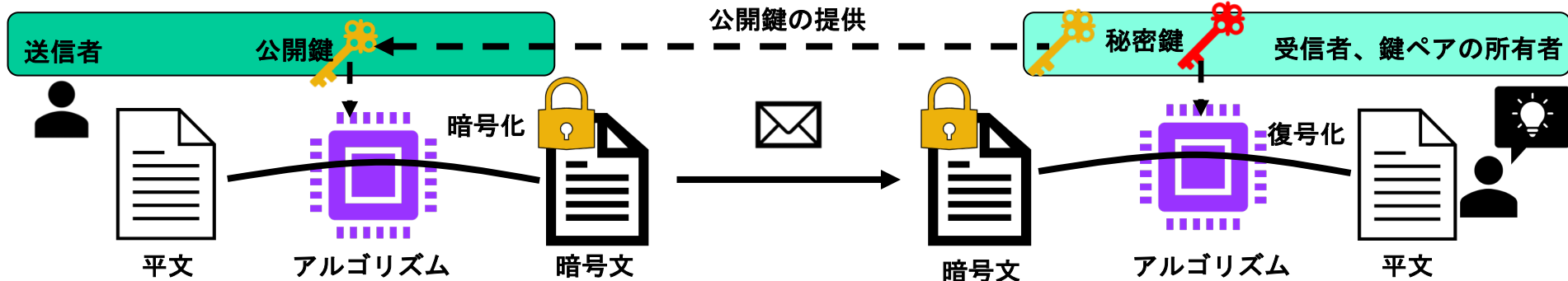
公開鍵から秘密鍵の割り出しや暗号文の解読が事実上不可能なアルゴリズム・鍵ペアが利用されます。

公開鍵暗号方式の処理は遅いので動画のような大きなメッセージの暗号化では効率が悪くなります。このため、メッセージ本体の暗号化は共通鍵暗号方式でおこない、比較的サイズの小さい共通鍵のみを公開鍵で暗号化して送受信者で共有する方式が利用されています。

必要な鍵の数：公開鍵暗号方式では送受信者がそれぞれの鍵ペアを作成し、公開鍵を全員に公開するだけで秘匿性が維持できます。すなわち、N 人のメッセージ交換に必要な公開鍵の総数は N 個となり、共通鍵方式で課題となった鍵の数の爆発は抑えられます。

課題：この方式では公開鍵の真正性が問題になります。すなわち、使用する公開鍵が確実に所有者から提供されている必要があります。

\* 1977 年に Rivest-Shamir-Adleman によって発表された公開鍵暗号方式、広く利用されています。



# ハッシュ値\*

ハッシュ関数は特定のアルゴリズムを用いて任意のメッセージを短い固定長のデータ（ハッシュ値）に変換します。二つの情報のハッシュ値を比較することで、元のメッセージの同一性（内容が同じであること）が検証できます。情報セキュリティでは改ざん検出など完全性の検証に利用されており、SHA-256 などが広く使われています。

ハッシュ関数に求められる代表的な性質を以下に示します。

- 同じメッセージに対して同一のハッシュ値が得られる（決定性）
- 同一のハッシュ値が得られる（意味のある）メッセージを作成することが不可能（耐衝突性）

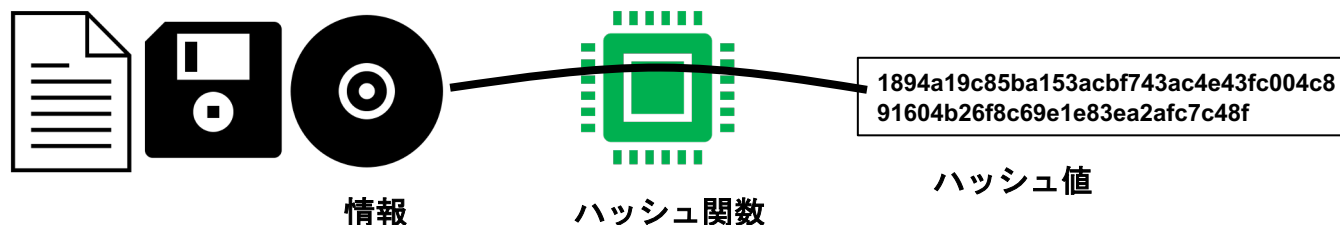
以下に類似した情報（文字列）の SHA-256 ハッシュ関数のハッシュ値を示しました。それぞれハッシュ値は大きく異なり、元の情報が異なることを容易に検出できます。

元データ	SHA-256 ハッシュ値
“Hello world”	1894a19c85ba153acbf743ac4e43fc004c891604b26f8c69e1e83ea2afc7c48f
“Hello world ” 最後に空白あり	1bece7cd4104d3cba6e58a41e6aaf6474b6a5e1fa45adb97739b8623af0f2c4a
“Hello World” W が大文字	d2a84f4b8b650937ec8f73cd8be2c74add5a911ba64df27458ed8229da804a26

大きなデータの比較には時間を要しますが、データの小さなハッシュ値の活用で効率的に同一性を検証できます。

- 過去のデータが失われてもハッシュ値さえ保存されていれば改変を検出できます。
- 膨大な数のファイルについて改変場所を特定が必要な場合でもハッシュ値が異なるファイルのみを取り出して比較するといった方法で、作業が効率化できます。

(\*) ハッシュ関数は暗号ではありませんが、暗号技術と組み合わせて利用されることが多いためここで取り上げます。。





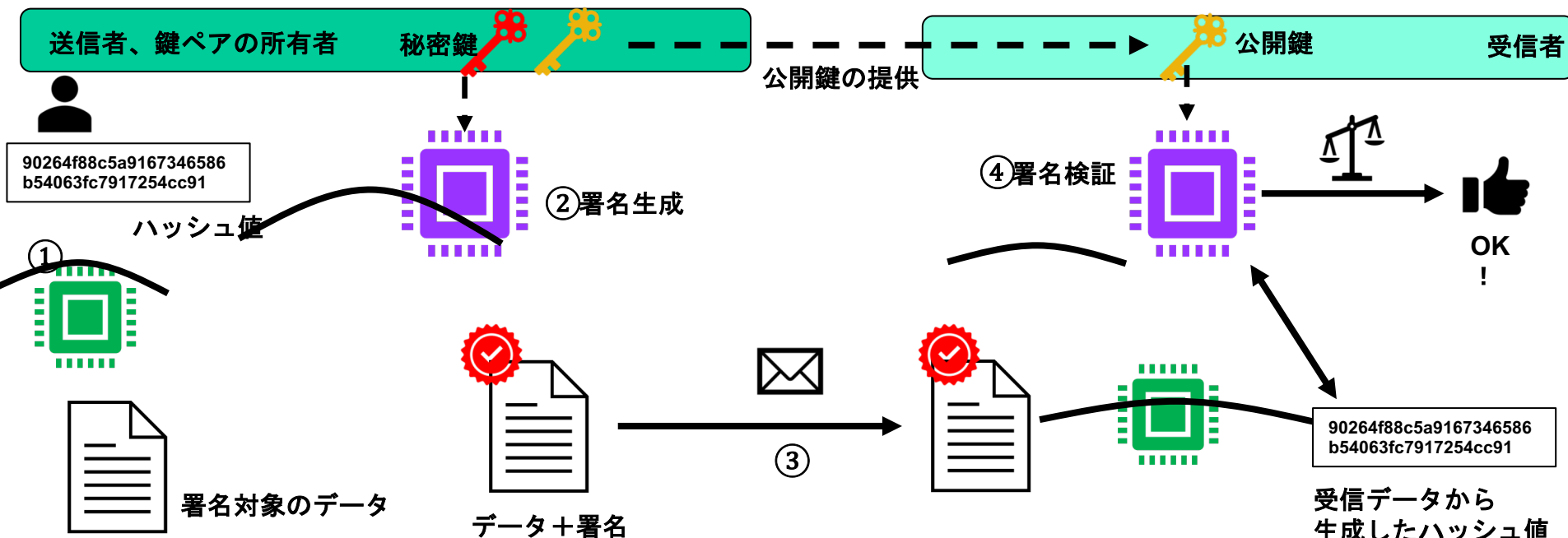
# デジタル署名

受信者がメッセージの出所を確認できるように付加されるデータを指し、真正性、完全性を維持します。署名生成に所有者以外に知られない秘密鍵を、署名検証に誰にでも公開してよい公開鍵を利用します。公開鍵で検証に成功する署名生成には秘密鍵が必要なため、署名者のなりすましを検出できます。マルウェアによるリスクを下げる目的でソフトウェアの配布元の検証にも用いられています。

デジタル署名処理の流れは以下のようになっています。

1. 署名対象のメッセージをハッシュ関数に与えハッシュ値を求めます。
2. ハッシュ値から秘密鍵を利用して署名を生成します。
3. メッセージと署名を併せて送ります。
4. メッセージから生成したハッシュ値、署名、公開鍵を利用して署名を検証します。  
検証に成功すれば、メッセージの出所は公開鍵の所有者であることを確認できます。

課題：この方式でも公開鍵の真正性が問題になります。公開鍵が本人になりすましたものから提供されていないことを検証する必要があります。



# 公開鍵基盤(Public Key Infrastructure:PKI)

公開鍵と所有者の真正性を保護する仕組みとして広く利用され  
ていますが、公開鍵暗号方式やディジタル署名と課題を  
公開鍵がほんと開証します。

## PKI の用語と役割：

証明書：公開鍵と所有者情報（名前、会社名など）が含まれており、認証局がその情報が信頼できることをデジタル署名によって証明したデータ

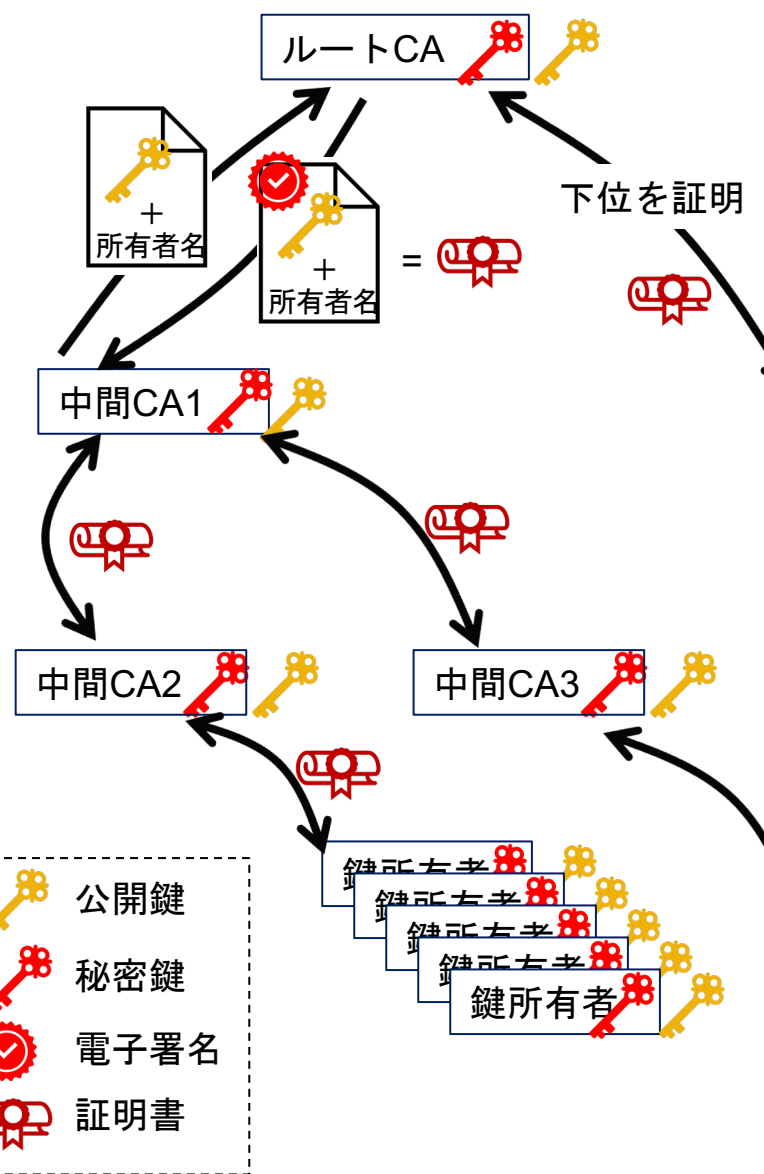
認証局（Certification Authority：CA）：公開鍵と所有者情報が信頼できることを確認し、証明書を発行します\*。CA 自身の証明書を他の CA から発行してもらうこともできます。この場合、発行元を上位 CA とする中間 CA と呼ばれます。

ルートCA：他のCAから証明書が発行されない特別なCA、信用点（トラストアンカー）とも呼ばれる。証明書はルートCA自身が署名し、自己署名証明書と呼ばれます。

CA の信頼関係を木構造（右図）で構成し、最上位のルートCA だけ信頼できれば、信頼がつながっている下位の証明書、すなわち公開鍵と所有者情報を信頼してよい。

ルートCA の証明書は OS、Web ブラウザなどにあらかじめ組み込まれており、組み込まれたルートCA につながる中間証明書であれば誰から提供されたものでも信頼して良い。このため、利用者はPKI の知識や、ルートCA の導入といった手順なしにPKI が提供する仕組みを享受できる。

(\*) 信頼性の確認にはさまざまな方法でおこなわれています。登記簿・電話確認が必要な厳格なものや、オンラインだけで完了する簡易なものまであります。




# PKIの応用：Web サーバの真正性、通信の秘匿性

- Web サーバがアクセスした URL(\*) の登録名のものかどうかの検証に利用されています。
- Web サーバが提供する証明書について Root 認証局からの信頼関係が確認できない場合、や有効期限が切れている場合は、ユーザに警告し、閲覧への注意を促します。
  - 証明書の公開鍵を利用してその後の通信は暗号化され、通信内容は秘匿されます。


左下の図は文部科学省トップページ (<https://www.mext.go.jp>)の証明書の内容と信頼関係を表示させています。

(\*) URL(Uniform Resource Locator) : Web ブラウザなどで利用されるインターネット上の資源を特定する <https://example.com/sample.html> といった形式の文字列のこと。登録名は example.com が該当する。




**www.mext.go.jpへの接続は暗号化されています。**


デジタル証明書による暗号化により、https Webサイト"www.mext.go.jp"との間での送信時に情報が非公開になります。



Baltimore CyberTrust Root

↳ 

Cybertrust Japan Public CA G3

↳ 

www.mext.go.jp

Root 認証局証明書、あらかじめ組み込まれている

中間認証局証明書

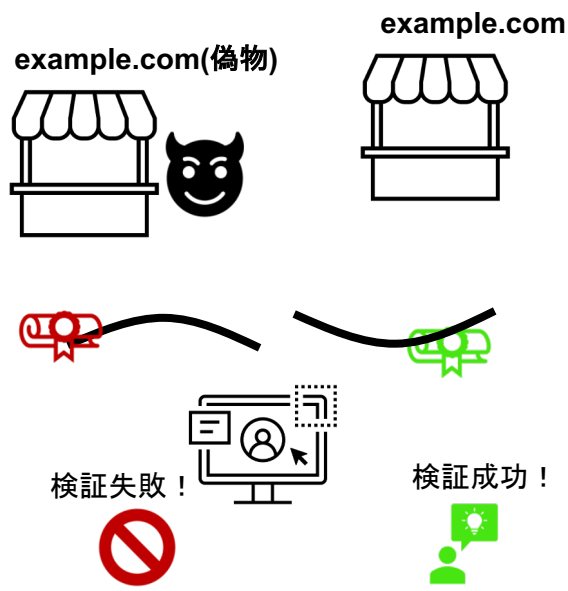
証明書本体、中間認証局のものも含めて  
サイト閲覧時にはじめて提供される。

拡張領域    サブジェクト代替名 (2.5.29.17)

重大    いいえ

DNS名    www.mext.go.jp

登録名：署名されたデータに含まれることから完全性が、上位認証局から証明書によって真正性が保護される。



# アクセス制御

情報および情報処理施設へのアクセス（接触・接続）を認可及び制限する手段を提供します。  
秘匿性・完全性・可用性すべての特性に関わります。

情報システムのアクセス制御によって実現される機能の例を示します。

1. 他人を利用者登録できない。（完全性）
2. 他人のファイルを読めない。（秘匿性）
3. 他人のパスワードを変更できない。（完全性）
4. 他人のファイルを削除できない。（完全性、可用性）

（）は直接維持できる特性を示しますが、行為が許されると他の特性に影響がおよびます。  
例えば、「3. 他人のパスワード変更」できると、他人へのなりすましによって秘匿性・可用性に影響する「2. ファイル閲覧」や「4. ファイル削除」も可能になります。

アクセス制御の例：

- Windows などの OS ではファイルごとに操作の許可/禁止を設定できます。例えば、他のユーザに読み出しは許可、書き込みは禁止といったアクセス制御を設定できます。
- IC カードや写真つきID カードを用いた入構・入室管理もアクセス制御に含まれます。

利用者ごとに制御を変える場合は、利用者ごとに真正性を確認する認証も必要となります。

# 認証 1/2

相手の真正性を検証する。例えば、ネット通販事業者は購買者が登録された利用者本人かどうかを検証し、なりすましによる未払いなどの被害を防ぐ必要があります。

利用者認証で代表的なものを挙げます。

- ID / Password : 利用者が入力する ID(識別子, Identifier) とパスワードが、登録されたものと一致するかを検証する。ID は重複を防ぐため電子メールアドレスなどが使われる。
- SMS, 電話, メール認証 : 利用者が ID を入力すると、登録された連絡先にランダムに生成した情報が送られる。利用者がその情報を正しく入力できるかどうかを検証する。パスワード再設定用の URL が送られる方式も含まれる。
- 証明書 : 利用者が署名した電子署名を(PKI で説明した)証明書で検証する。秘密鍵・証明書は ICカードで保存される。秘密鍵の利用時には持ち主に暗証番号(文字列)を入力させる。この暗証番号は Personal Identification Code(PIN) コードとも呼ばれる。
- 生体認証 : 人間の身体的な特徴や行動的な特徴を利用する認証方式のこと。指紋・静脈・虹彩を利用する方式が使われている。
- 認証器 : 利用者が持つデバイスから提供される一定間隔で更新される文字列を入力させる。認証器はトークンと呼ばれる物理デバイスやスマートフォンアプリケーションとして提供される。ネット銀行の振り込みなどで利用されている。

## 認証 2/2

ID / Password は複数のサービスで使いまわされることが多く、なりすましのリスクが高い。実際なりすましによる被害も大きくなっている。最近では、最初の認証に成功したのち、さらに別の認証を求める２段階認証も使われ始めている。

第一段階で ID/Password 認証を要求し、２段階目で認証器による認証をもとめる方式が使われ始めている。

# バックアップ・冗長化

可用性・完全性を高める技術として利用されています。

**バックアップ**：記憶装置のデータを別の記憶装置に複製（コピー）しておき、障害時には複製からデータを復旧させます。

スマートフォンのデータをインターネット経由でバックアップし、故障時の機器交換の復旧で活用することは広くおこなわれています。また、操作を誤ってデータを破壊した際の復旧にも活用できます。

**冗長化**：2台以上の機器を用意し一部に障害が発生しても正常な機器で代替します。可用性の維持には効果的ですが、コストも増大します。

コンピュータのハードディスクドライブ（HDD）では古くから利用されてきました。

**多地域展開**：冗長化の一種で、情報システムを地理的に離れた地域に配置します。停電による電力喪失や災害による建物倒壊といったリスクにも対応できます。従来はコストが高く金融システムなどに限られていましたが、近年ではコストも下がりWebサービス、SNSなどで広く使われています。

バックアップの媒体のみを遠隔地に保管する方法も採られています。

# 情報セキュリティ技術：まとめ

これまで紹介した技術について情報セキュリティの特性の視点でまとめます。

## 暗号技術

- 共有鍵と公開鍵暗号方式が使われる。
- 秘匿性に加え、完全性、真正性の向上にも利用されています。

## アクセス制御

- アクセス（接触・接続）を認可及び制限する。
- 秘匿性・完全性・可用性の全ての特性に関わります。

## 認証

- 相手がなりすましでないこと（真正性）を検証する。

## バックアップ・冗長化

- 情報の複製や複数機器の同時利用で可用性・完全性を向上させる。