情報セキュリティとは

情報セキュリティ（Information Security）とは、情報や情報システムなどを＿＿＿＿＿＿＿＿＿＿や漏洩、改ざん、破壊から守ることである。

守る対象としては、財務情報、人事情報、技術情報、人の記憶や知識などの組織にとって価値のあるものであり、これを＿＿＿＿＿＿という。

ハードウェア、ソフトウェア、ネットワークなどに電子的に蓄積されているものもあれば、紙などに記載されているものもある。

日本工業規格（Japanese industrial standards：JIS）においては、情報セキュリティを

「情報の機密性、完全性、および可用性を維持すること。さらに、真正性、責任追跡性、否認防止および信頼性のような特性を維持することを含めてもよい」

として定義している。

JIS（日本工業規格）とは、我が国の工業標準化の促進を目的とする工業標準化法（昭和24年）に基づき制定される国家規格です。

英語の頭文字をとって「＿＿＿」とも呼ばれる

この定義文章の中の

「＿＿＿＿＿」、「＿＿＿＿＿」、「＿＿＿＿＿」

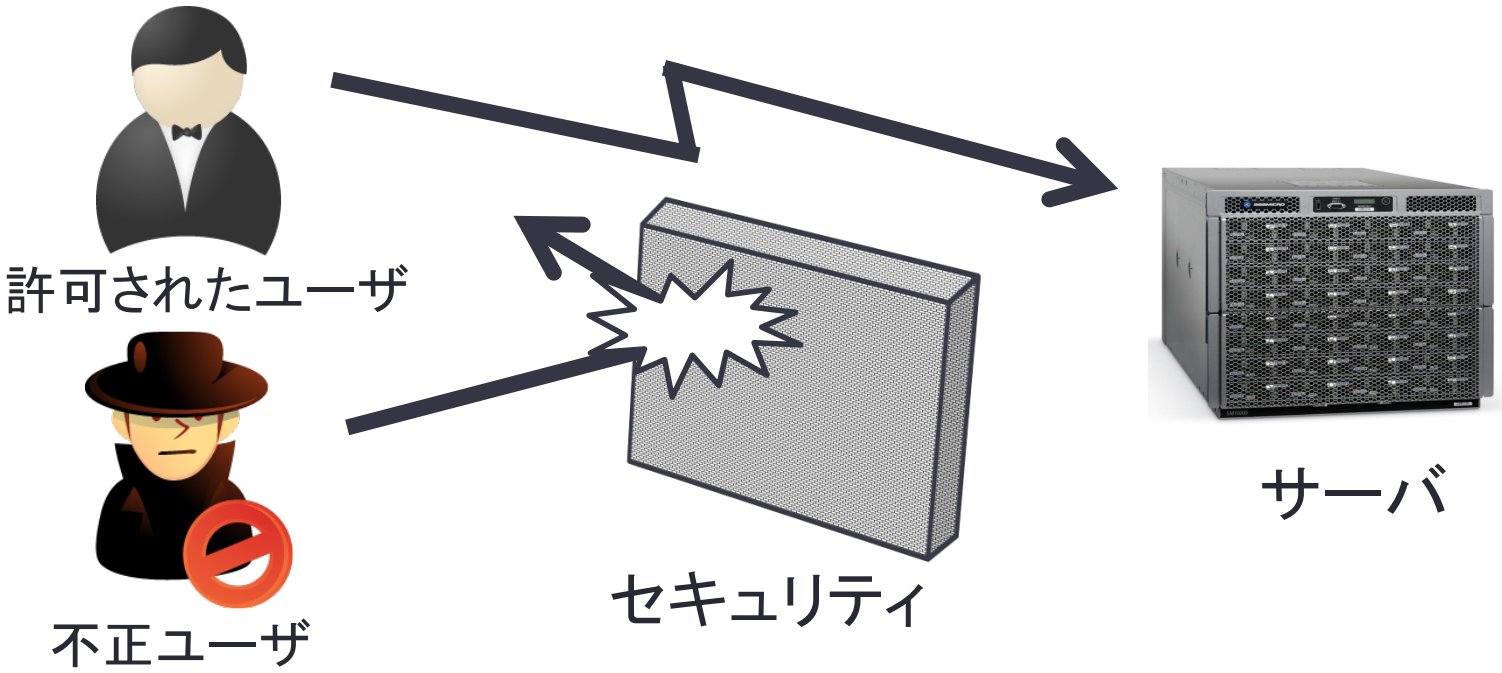
は情報セキュリティの３要素と呼ばれる。

機密性 Confidentiality

entity　process

「認可されていない個人、エンティティまたはプロセスに対して、情報を＿＿＿＿＿または＿＿＿＿＿にする特性」

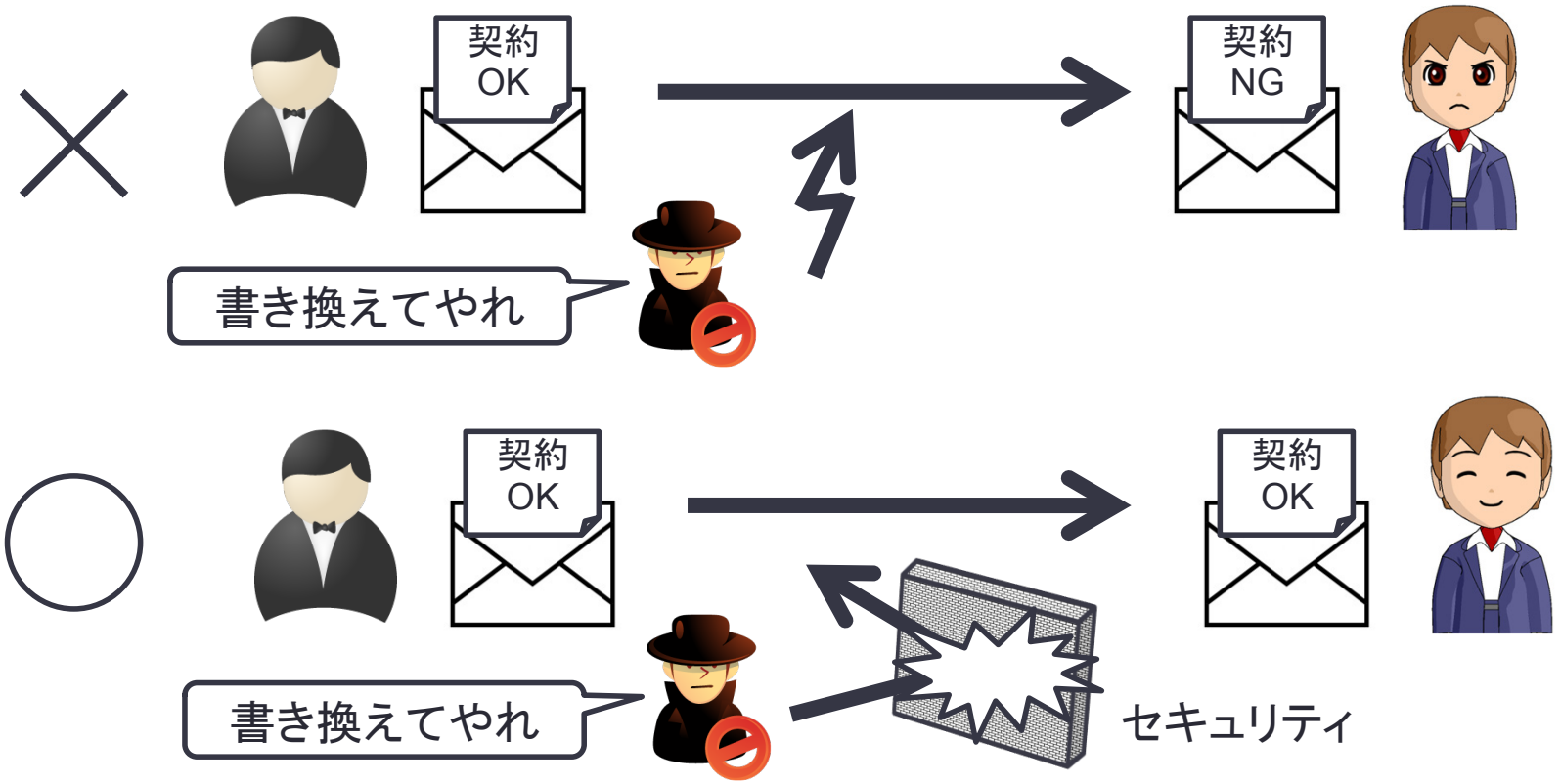
つまり、許可された者だけが情報にアクセスできるということである。



完全性　Integrity

「情報資産の＿＿＿＿＿および＿＿＿＿＿を保護する特性」

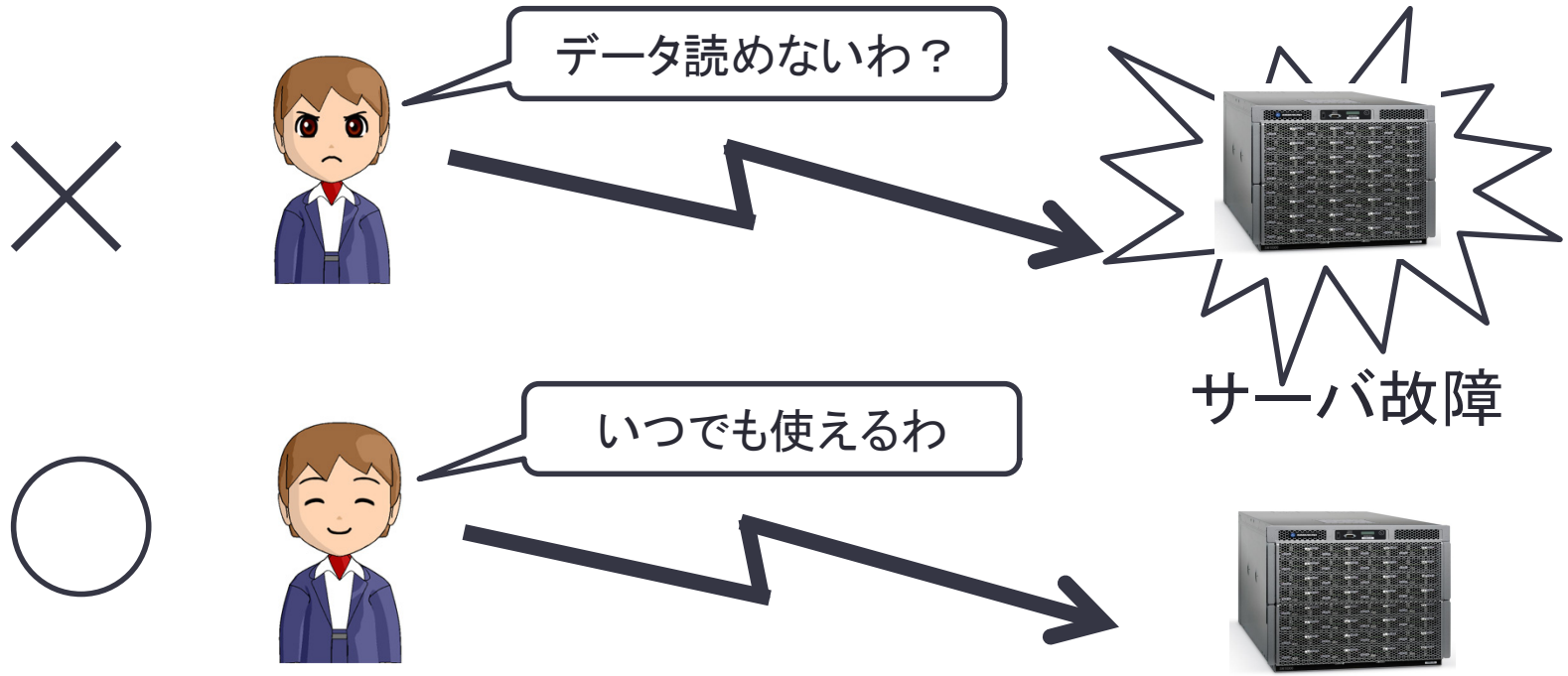
つまり、途中で情報が書き換えられることなく、正確かつ完全である状態を保つことである。



可用性　Availability

「認可されたエンティティが要求したときに、アクセスおよび使用が可能である特性。」

つまり、サーバなどに故障がなく、許可された利用者が＿＿＿＿＿＿＿＿＿＿できるということである。



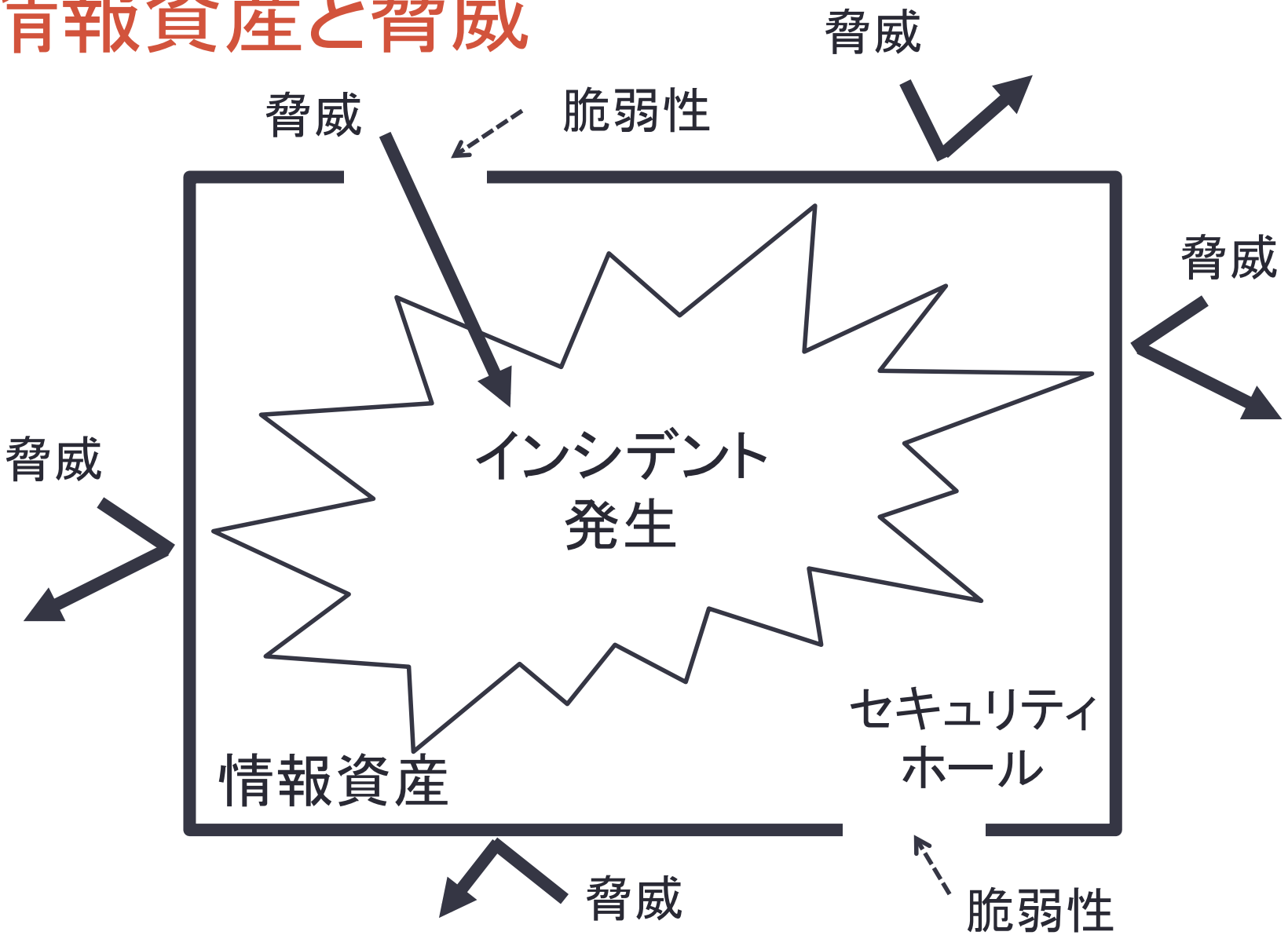
その他の情報セキュリティ要素

要素	説明
真正性 （Authenticity）	ある主体または資源が、主張どおりであることを確実にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
責任追及性 （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
信頼性 （Reliability）	意図した動作および結果に一致する特性
否認防止 （Non-Repudiation）	ある活動または自称が起きたことを、後になって否認されないように証明する能力

セキュリティを脅かす脅威

- 情報セキュリティは、組織として価値がある情報資産を機密性、完全性、可用性を阻害しうる要因である「＿＿＿＿」（Threat）から守ることである。
- 脅威によって、情報資産が損なわれる可能性を「＿＿＿＿」（Risk）とよぶ
- 脅威がつけ込むことのできる情報資産がもつ弱点のことを 「＿＿＿＿」（Vulnerability）という。同じ意味で「＿＿＿＿＿＿＿＿＿＿＿＿」と呼ぶこともある。
- 実際に情報資産が損なわれてしまった状態は、「＿＿＿＿＿＿＿＿」（Incident）と呼ばれ、重大な事故に至った場合を含むこともある。

情報資産と脅威



脅威の種類

_____的脅威 ・・・・ 自然災害など環境に依る脅威

_____的脅威 ・・・・ 人が介在する脅威

- _____的脅威 ・・・・ 不慮の事故などによる脅威
- _____的脅威 ・・・・ 故意に損害を与えようとする意思に基づく脅威

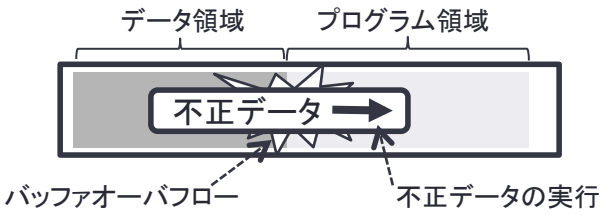
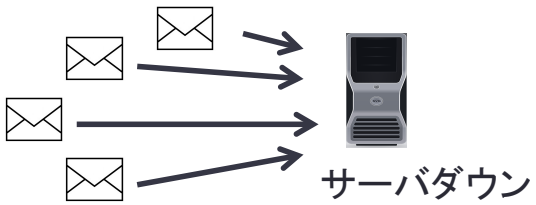
意図的に脅威を与えようとする人 → クラッカー ↓

- 不正アクセス ・・・・ 許可されていない者が外部から不正に侵入する行為
- サービス妨害 ・・・・ サーバが本来の仕事をでいなくする行為

不正アクセス

種類	説明
盗聴	第三者がネットワークに流れている機密情報などのデータを不正に盗むこと
なりすまし	他人のユーザIDやパスワードを使って、本人のふりをしてシステムを利用したり、虚偽の取引をおこなったりすること
改ざん	Webページやメールの内容を不正に書き換えること
破壊	データやプログラムを破壊、消去すること
不正利用	コンピュータやネットワークなどを第三者が不正に操作すること
不正プログラムの埋め込み	ユーザが知らない間に情報を外部に漏洩したり、ファイルを破壊したりするなどの不正なプログラムを埋め込むこと
	不正アクセスを行う場合の中継地点とすること

サービス妨害

種類	説明
DoS攻撃 （Denial of Service）  	意味のない大量のデータをサーバやルータに送り、それらの装置の処理能力以上の処理させ、通常のサービスを利用できなくさせる攻撃。特に多数のコンピュータに攻撃用のプログラムを仕込んで一斉に攻撃することをDDoS（Distributed DoS）攻撃という。
バッファオーバフロー攻撃  	コンピュータがプログラムを実行する場合、データをバッファと呼ばれるメモリに一時的に蓄える必要がある。そのバッファに対して許容量を超えるデータを送り、システムを機能停止状態にさせる攻撃
メール攻撃  	DoS攻撃の一種で、メールサーバに対して大量のメールを送り、メールサーバに正規のメール処理できなくさせる攻撃

その他の脅威

種類	説明
ソーシャルエンジニアリング Social Engineering	関係者を装ってシステム管理者に電話で情報を聞き出したり、パスワードや情報をユーザの背後からのぞき見したり、ゴミ箱から情報を入手したりするなどのコンピュータの技術を利用せず機密情報を入手すること。
	メールなどを用いて、実在する企業のWebサイトを装った偽のWebサイトにユーザを誘導し、クレジットカード番号、ID、パスワードなどを入力させて盗みとること。
P2P（Peer to Peer）ファイル交換ソフト（ファイル共有ソフト）	本来、ユーザが意図したファイルのみを交換させるファイル共有ソフトウェアをコンピュータウィルスの感染などにより勝手に機密情報なども流出させること。

マルウェア　Malware　　不正プログラムの総称

種類	説明
コンピュータウィルス Computer Virus	電子メールにファイルとして添付されたり、Webページからダウンロードされたりしてコンピュータに知らない間に取り込まれ、他のファイルやプログラムに寄生して不正を行うマルウェア
	単独で自分自信を複製して、ネットワークやメディアを経由して他のコンピュータに拡散する性質をもつマルウェア
	有益なプログラムのふりをしてユーザの知らない間に不正な行為を行うマルウェア
	宣伝や勧誘、いたずら目的で大量に送られてくる迷惑なメール

コンピュータウィルスの定義

経済産業省のコンピュータウィルス対策基準によれば、

> 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であり、次の機能を一つ以上有するもの

（1）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また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。
（2）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
（3）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

コンピュータウィルスの感染経路の例

感染経路	具体例
ネットワーク	・電子メールの添付ファイル ・電子メール本文のリンク先への遷移 ・ウィルス感染したWebページの閲覧 ・インターネットからのダウンロード　　など
記憶メディア	・CD　・DVD　・USBメモリ　など

コンピュータウィルスの種類

タイプ	説明
_____感染型	実行可能なプログラムファイルに感染するウィルス。感染したプログラムを実行することで他のファイルにも感染する。
_____感染型	Word、Excelなどの文書ファイルのマクロ言語で作成されたウィルス。感染した文書ファイルを開くと感染し、感染したファイルが電子メールなどに添付されると感染が拡大するため、最も感染力の強いウィルスである。
_____感染型	コンピュータの起動システムに感染するウィルス。以前はフロッピーディスク、現在はUSBメモリを介して感染が拡大。

情報セキュリティ対策の分類

2013年10月に厚生労働省から出された「医療情報システムの安全管理に関するガイドライン第4.2版」によると、情報セキュリティ対策を情報システムの安全管理として、

- ✓ _____的安全管理対策
- ✓ _____的安全対策
- ✓ _____的安全対策
- ✓ _____的安全対策

の4方針を策定している。

情報セキュリティ対策の分類

セキュリティ対策	説明
＿＿＿＿＿＿＿＿ セキュリティ対策	ネットワーク、サーバ、コンピュータやシステムなどを情報技術を用いて守ること。
＿＿＿＿＿＿＿＿ セキリティ対策	災害や人的破壊などから、施設、設備、装置、記憶媒体などを物理的な方法で守ること。
＿＿＿＿＿＿＿＿ セキュリティ対策	情報資産を扱う上での手続きやルール（入退室管理規則やマニュアルなど）の遵守徹底、責任体制の確立、セキュリティポリシーの策定など。

組織的セキュリティ対策（組織的安全管理対策）

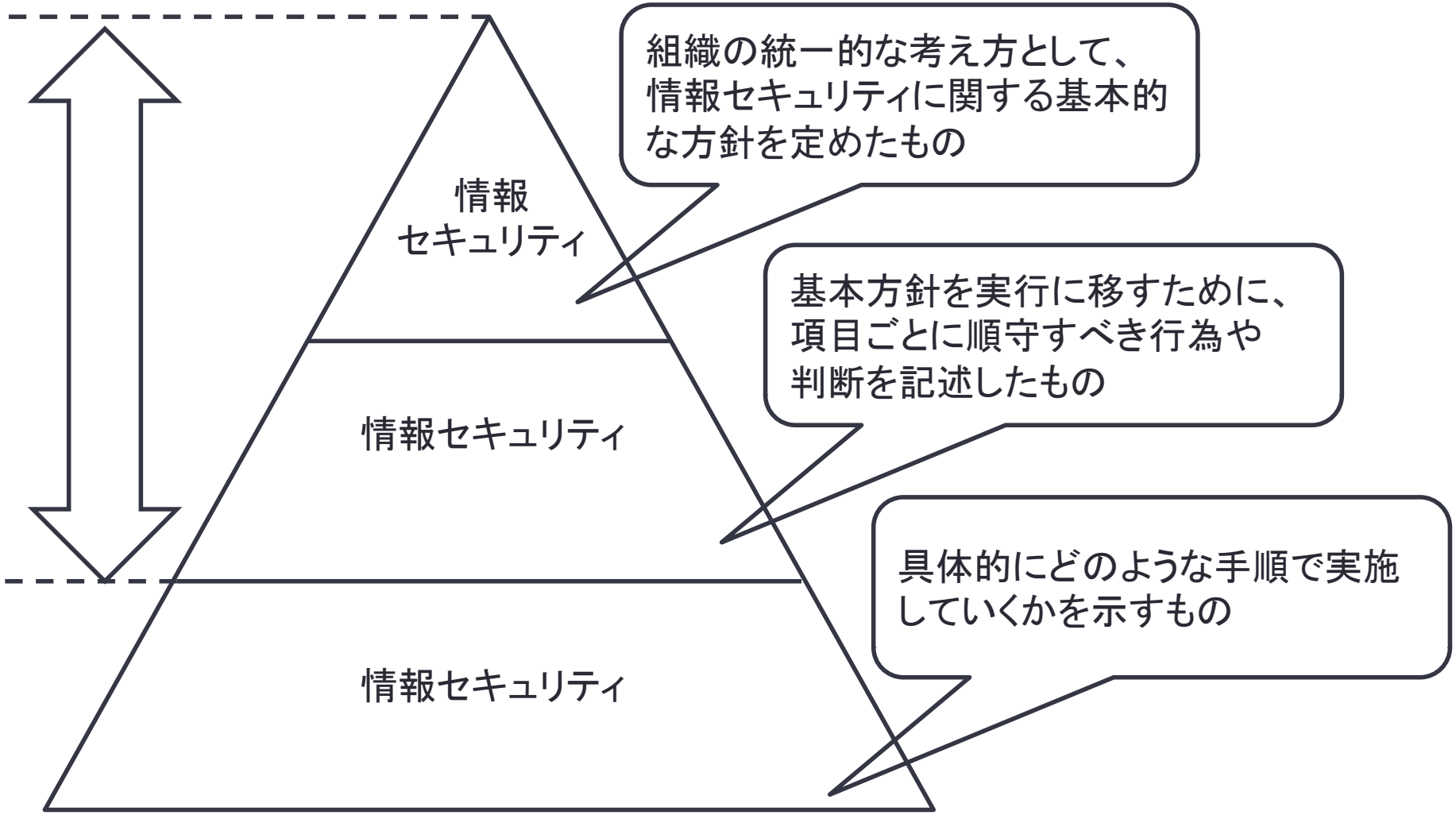
組織として情報資源を守るためには、

- 職員の＿＿＿＿＿＿＿＿を明確に定める
- 安全管理に関する規定や手順書を整備し運用する
- 安全管理の実施状況を日常の＿＿＿＿＿＿などによって確認する

「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」の策定や社内倫理規定の見直しなどが重要となる。

組織が情報資産に対してどのように取り組み、職員がどのように行動すべきか、という方針を明文化したもの。

情報セキュリティポリシーの階層構造



情報セキュリティマネジメントシステム

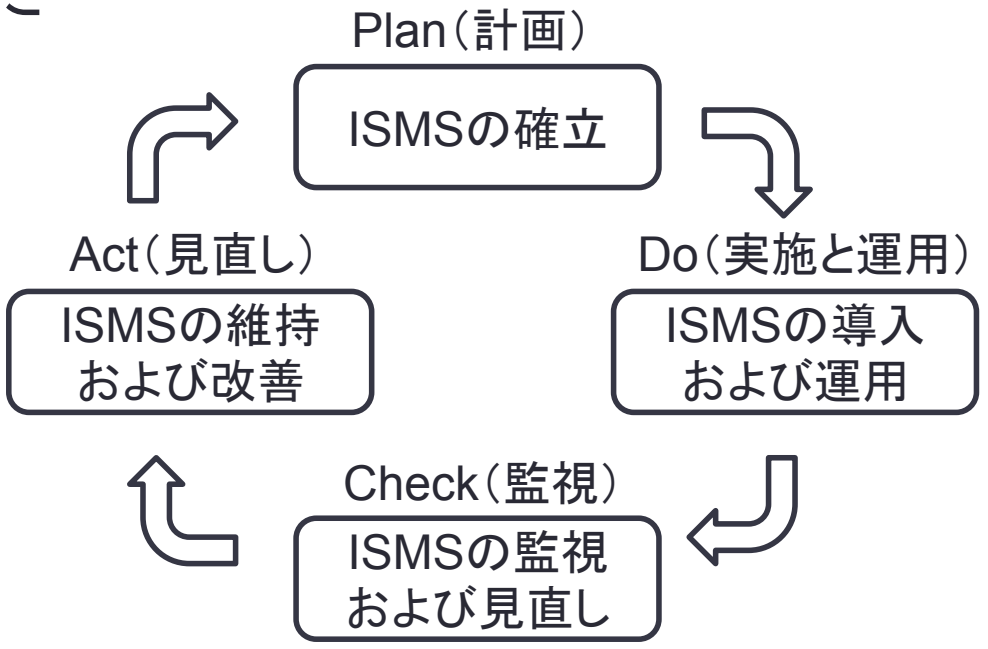
ISMS：Information Security Management System

ISMSとは、組織が情報を適切に管理し、機密を守るための取り組みであり、コンピュータシステムに対する情報セキュリティ対策だけでなく、具体的に

- ＿＿＿＿＿＿
- ＿＿＿＿＿＿
- ＿＿＿＿＿＿
- ＿＿＿＿＿＿

を行い、

＿＿＿＿＿＿＿＿に
よって改善していく
仕組みである。



ISMSのPDCAサイクル

物理的セキュリティ対策（物理的安全対策）

情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、情報媒体などを物理的な方法によって保護することである。

物理的セキュリティ対策	具体的な施策
コンピュータ室への入退室管理	・コンピュータ室の施錠 ・不許可者への入室の制限 ・入退室時間の管理 ・入室時の名札の着用義務 ・防犯カメラの設置　など
地震などの災害対策	・転倒、落下防止対策 ・防火、防水対策 ・停電時の代替電源の確保　など
機器、装置、記憶媒体などの盗難や紛失への対策	・機器、装置へのチェーン施錠 ・記憶媒体や書類などの持ち出し禁止 ・私有コンピュータの利用の禁止 ・不要な書類のシュレッダーや焼却 ・机上、書庫などの整理整頓 ・書類の放置禁止　など

人的セキュリティ対策（人的安全対策）

人的セキュリティ対策は、情報資産を守るために人による誤りを防止することである。

守秘義務と違反時の罰則に関する規定書類を作成し、ユーザに対して教育、訓練を行う必要がある。

情報生キュリティポリシーに基づき、職員がどのような行動をとるべきか、また、違反したときにどのような影響があり、処罰されるかを規定すると同時に、情報資産をどのように取り扱うかを示した＿＿＿＿＿＿＿＿＿＿の作成が必要である。

定期的にユーザに対して、情報資産の安全管理に関する教育や訓練を行わなければならない。また、職員が退職後に、在職中に知り得た情報についての取り扱いも規定すべきである。

技術的セキュリティ対策（技術的安全対策）

技術的セキュリティ対策は、コンピュータやネットワーク技術を利用して、情報資産を保護することである。たとえば、利用者の識別・認証やアクセス制限、不正ソフトウェア対策、不正アクセス防止などである。具体的には以下のような技術を利用する。

a) セキュリティパッチ
b) コンピュータウィルス対策ソフトウェア
c) ユーザ管理
d) 暗号化技術
e) デジタル署名
f) ファイアウォール
g) その他のセキュリティ技術
   - VPN
   - SSL / TSL
   - S / MIME

セキュリティパッチ

オペレーティングシステムやアプリケーションソフトウェアに脆弱性であるセキュリティホールがあると、そこを突破口としてウィルス感染や不正にアクセスされる場合がある。そこで、セキュリティホールを＿＿＿＿＿＿＿＿と呼ばれるソフトウェアでふさがなければならない。

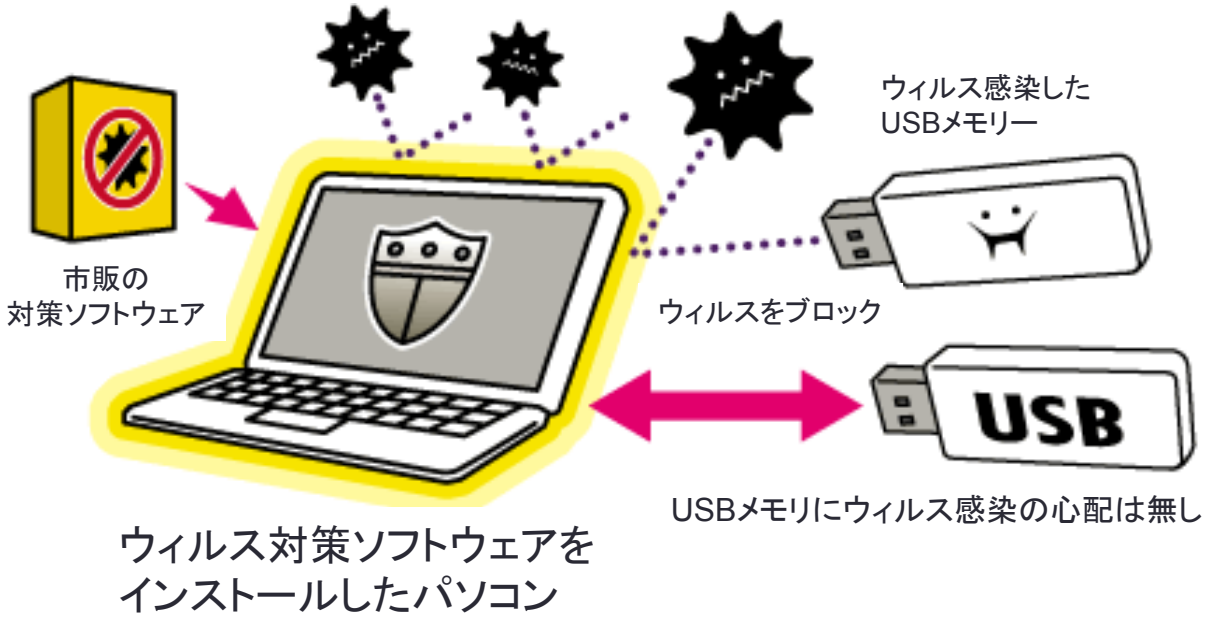
ソフトウェアのメーカーは、多くのセキュリティパッチを順次インストールする手間を省くために、定期的に多数のセキュリティパッチを1つのプログラムにまとめて配布している。Windowsには、自動的にセキュリティパッチをダウンロードして更新するWindows Updateと呼ばれる機能がある。

コンピュータウィルス対策ソフトウェア

コンピュータウィルスの感染に対して、コンピュータウィルス対策ソフトウェア（別名：ワクチンソフトウェア、アンチウィルスソフトウェア）をインストールし、未然に防止する必要がある。

コンピュータウィルスはウィルス特有のパターンをもっている。そこで、コンピュータウィルス対策ソフトウェアは事前に所有しているコンピュータウィルス定義ファイル（パターンファイル）とコンピュータ内部のデータを比較してウィルスを検出する。

ただし、未知のウィルスには対応できないため、定期的にコンピュータウィルス定義ファイルを更新する必要がある。



ユーザ管理

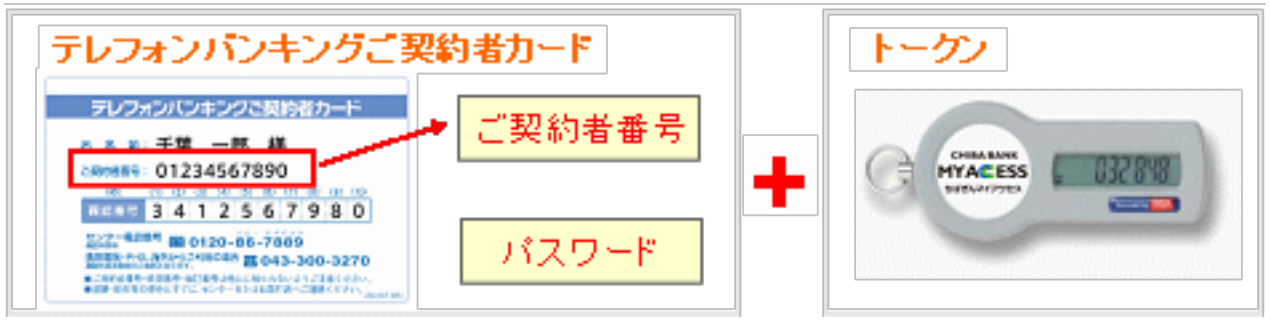
機密性の確保のために、許可された者のみが許可された情報だけにアクセスできる対策が必要である。

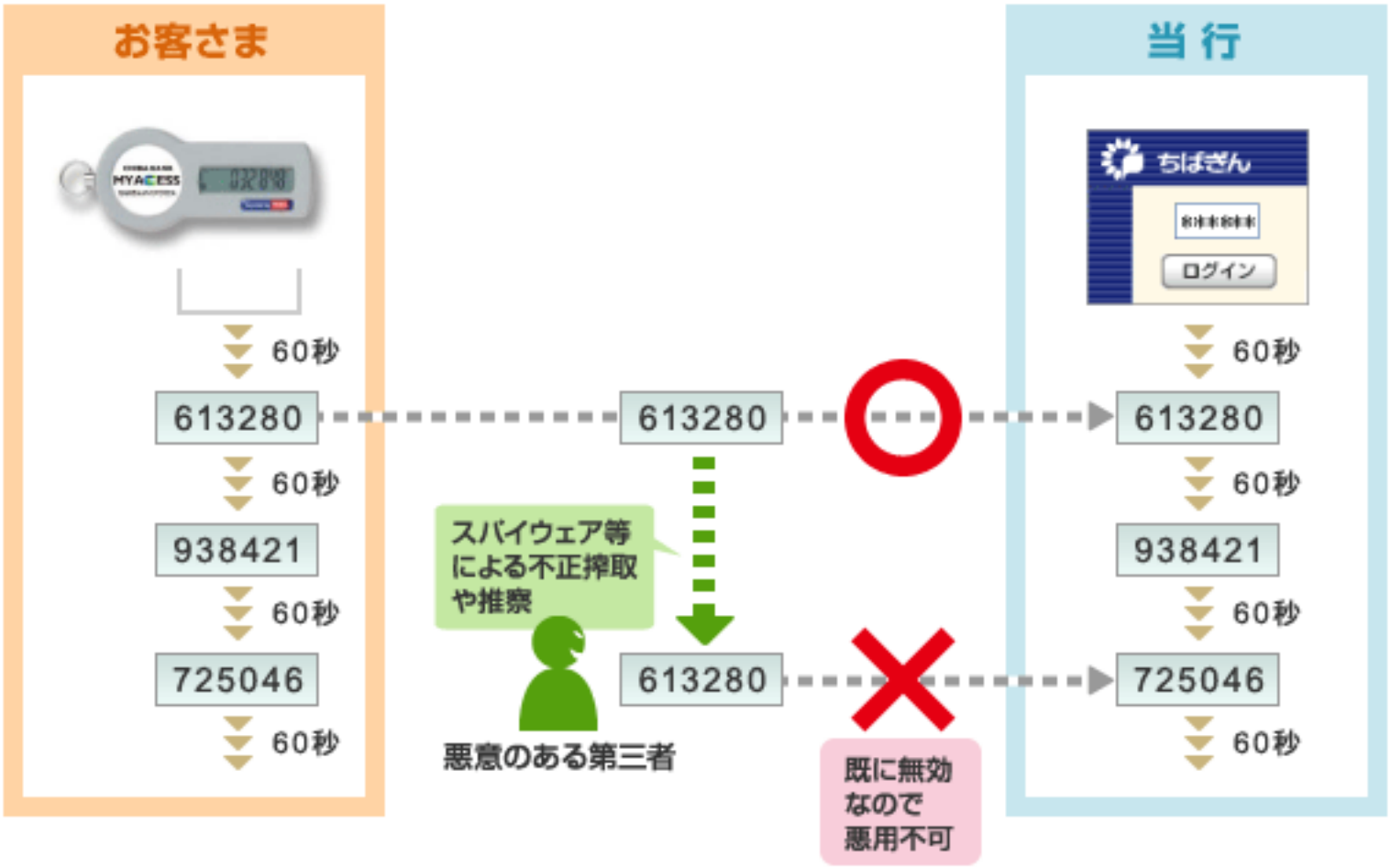
情報システムにユーザを登録し、正規ユーザであることを認証する。代表的な認証技術には、

- パスワード認証 → 1回限りの使い捨てのパスワードを使った認証
- ICカード認証
- 生体認証 → バイオメトリクス認証（biometrics）ともいい、人の身体的特徴や行動的特徴によって認証するする方法である。
  - 指紋認証
  - 虹彩（アイリス）認証
  - 声紋認証
  - 顔認証
  - 指静脈認証　など

などがある。

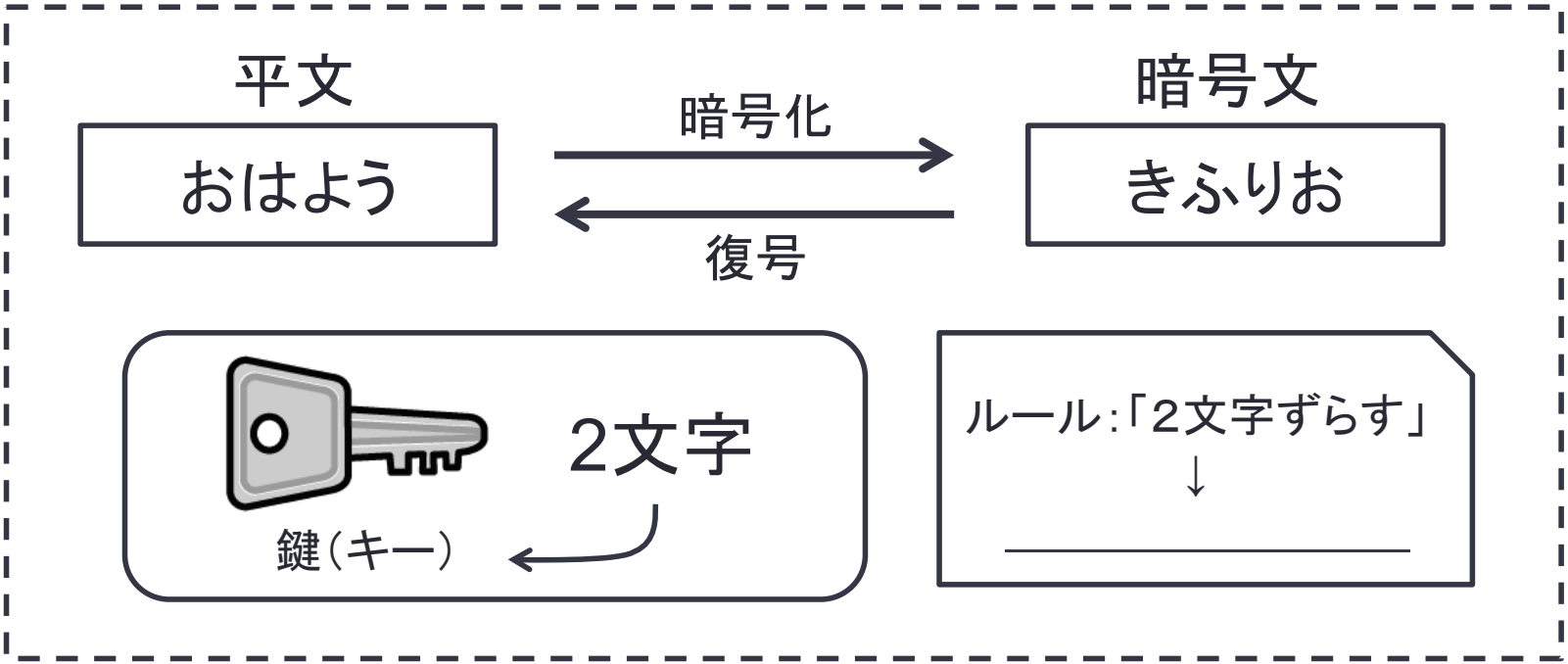
- ファイルへのアクセス権には、読み出し権限、書き込み権限、実行権限があり、これらを必要（職種）に応じ、組み合わせて設定する。 → _____
- アクセスした利用者名、日付時刻、行った操作などを記録する。→ _____


テレフォンバンキングご契約者カード
テレフォンバンキングご契約者カード
01234567890
3 4 1 2 5 6 7 9 8 0
ご契約者番号
パスワード
トークン
CHIBA BANK
MYACCESS


お客さま
当行
MYACCESS
ちばぎん
ログイン
60秒
613280
938421
725046
スパイウェア等
による不正搾取
や推察
悪意のある第三者
既に無効
なので
悪用不可

暗号化技術

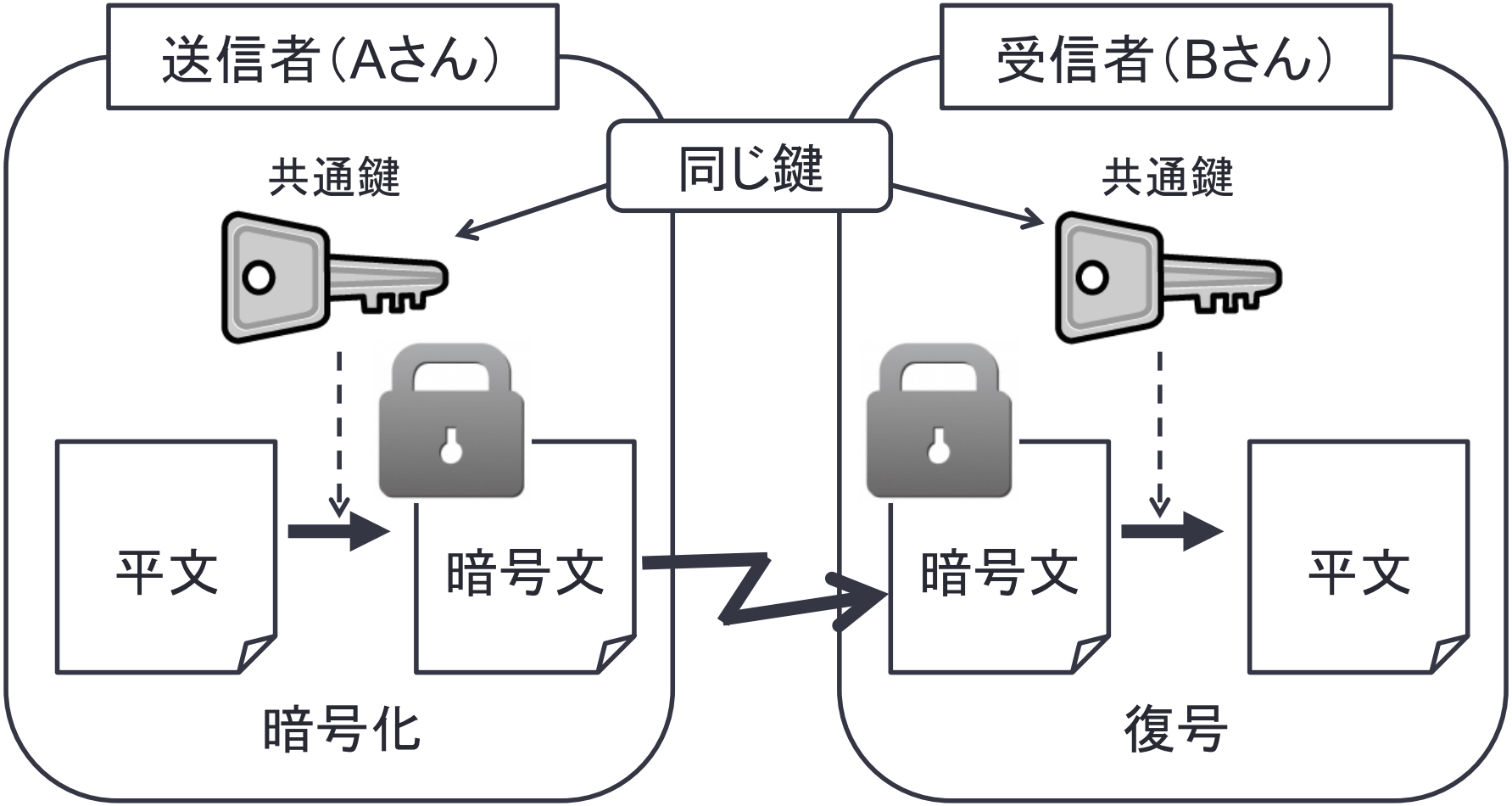
暗号化（Encryption）とは、ある一定のルールに基づいて
データを変換し、第三者に知られないようにする技術である。



現在、利用されている暗号化技術は、＿＿＿＿暗号方式と
＿＿＿＿暗号方式の二つに大別できる。

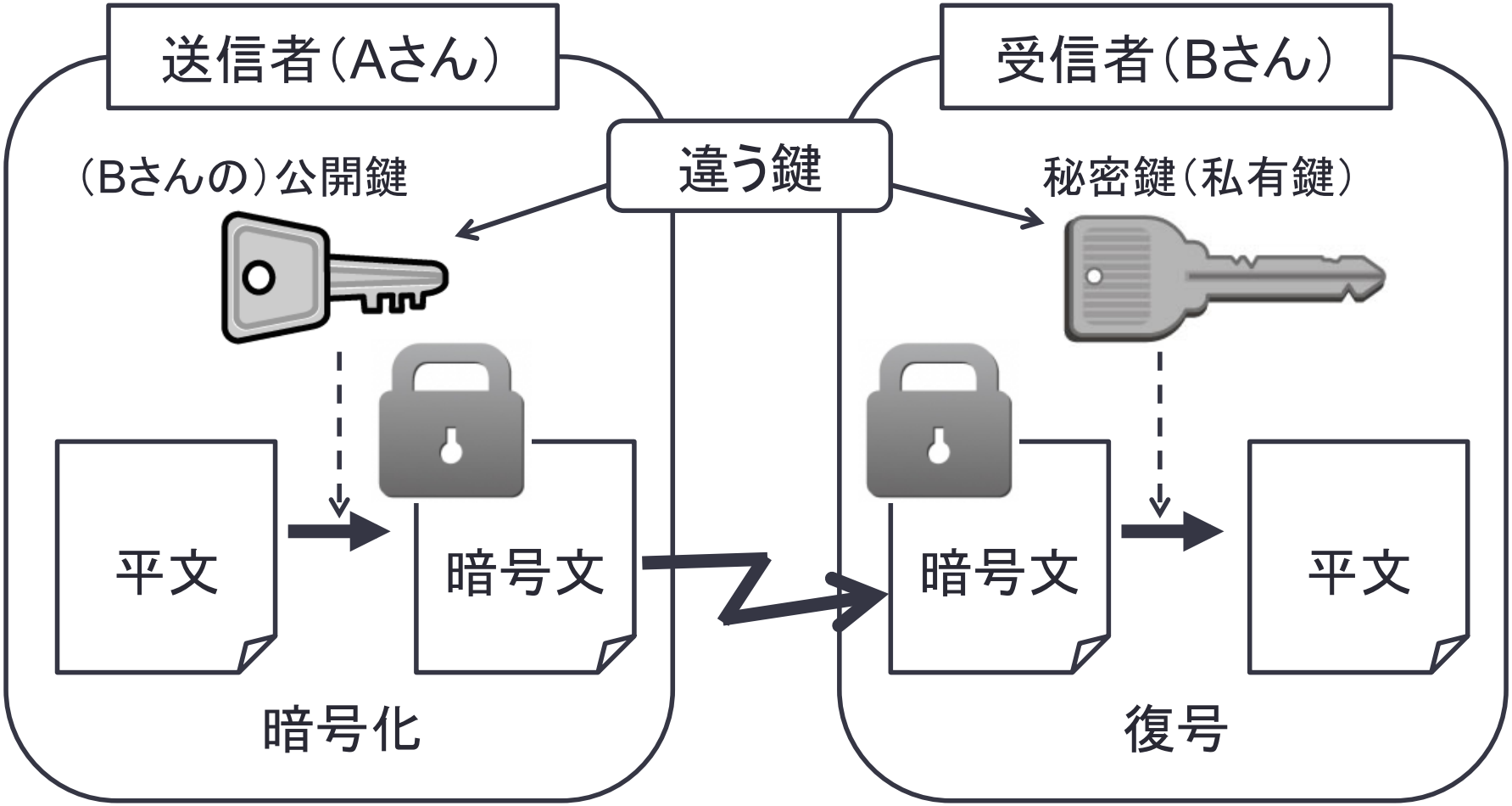
暗号方式

利点：高速に暗号化・復号できる
欠点：共通鍵を安全に相手に渡す必要がある

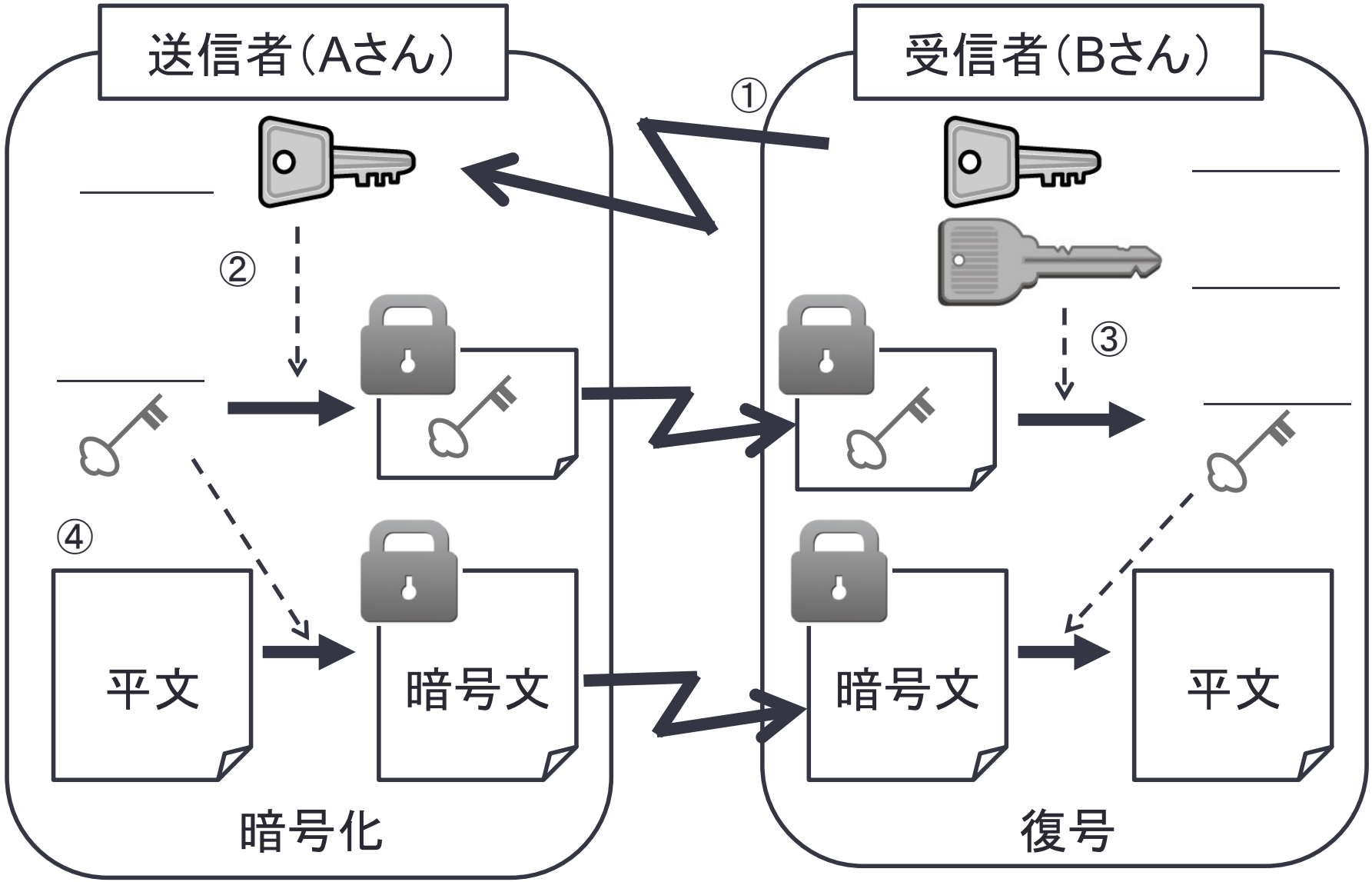


暗号方式

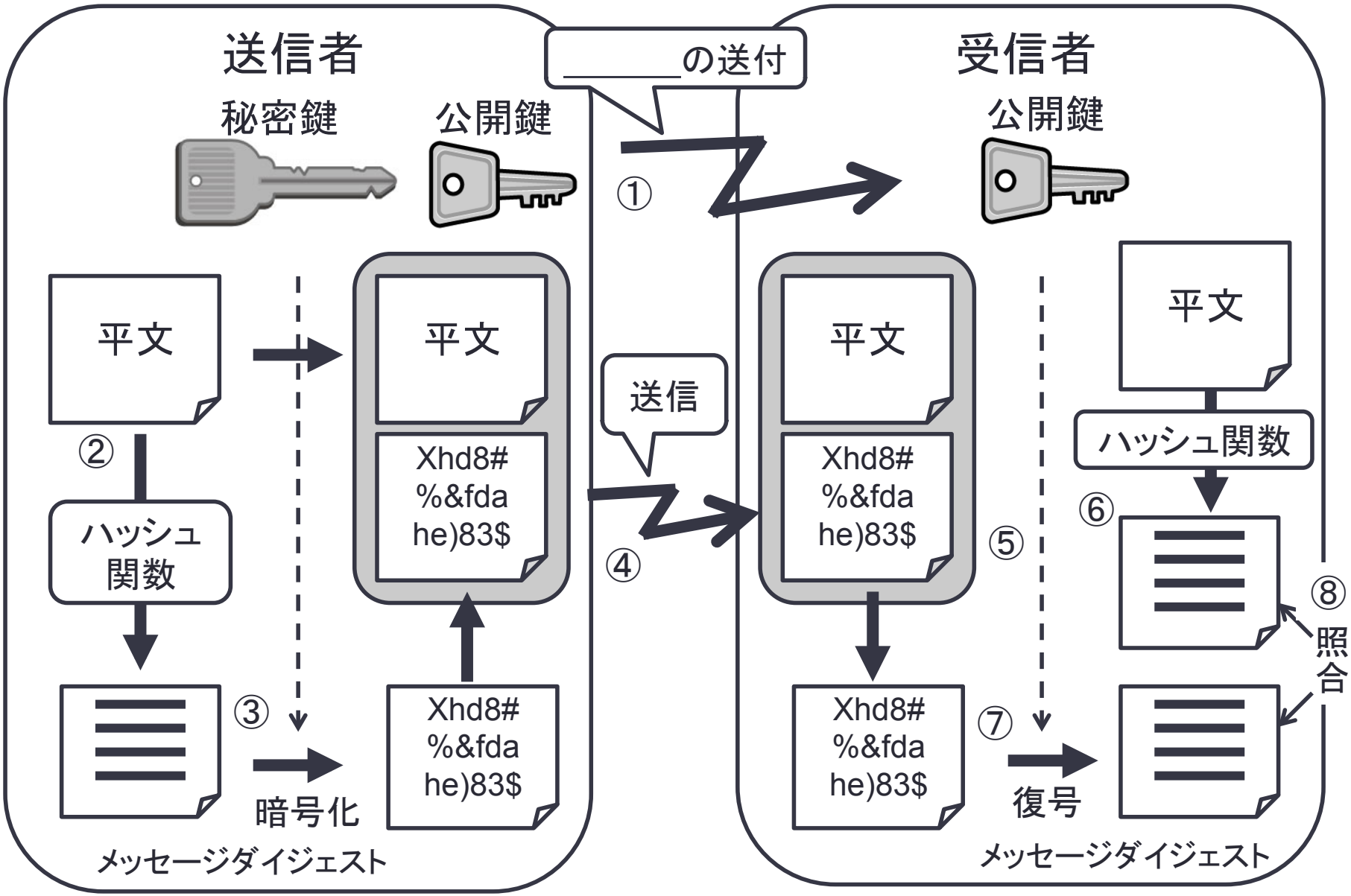
利点：安全に鍵を相手に渡せる
欠点：暗号化・復号の仕組みが複雑で処理に時間がかかる



ハイブリット暗号方式

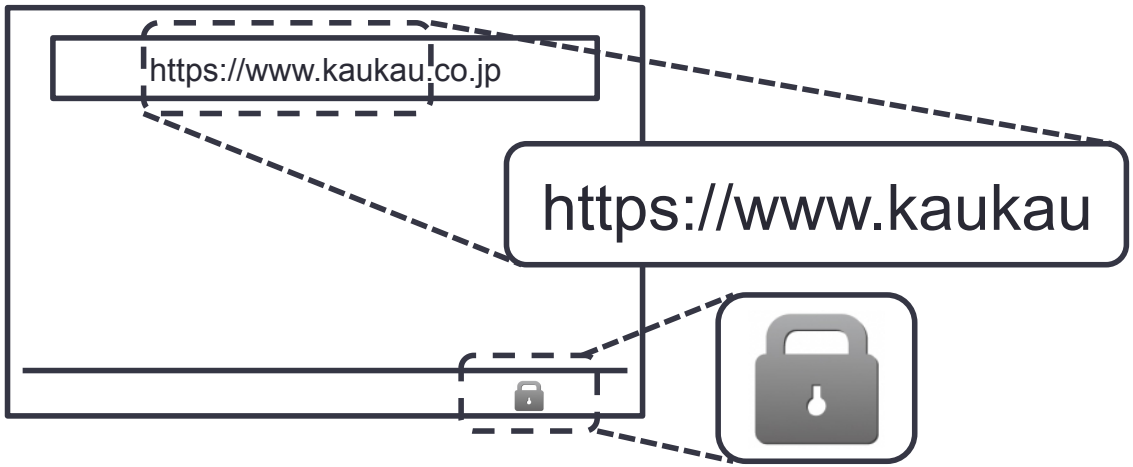


デジタル署名（電子署名）


送信者
受信者
_____の送付
秘密鍵
公開鍵
公開鍵
①
平文
②
ハッシュ関数
③
暗号化
平文
Xhd8#
%&fda
he)83$
送信
④
平文
Xhd8#
%&fda
he)83$
⑤
平文
ハッシュ関数
⑥
⑦
復号
⑧
照合
Xhd8#
%&fda
he)83$
メッセージダイジェスト
メッセージダイジェスト

SSL / TSL

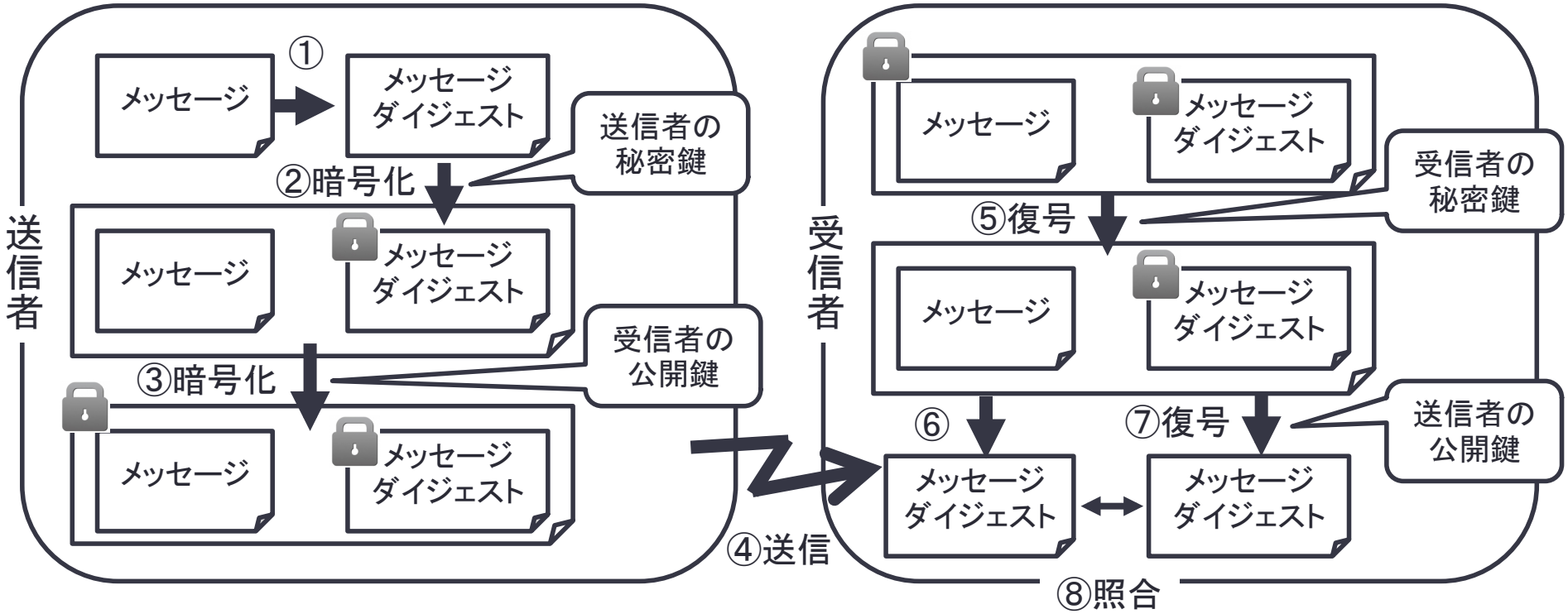
- SSL（Secure Socket Layer）は、その改良版である TLS（Transport Layer Security）とともにSSL/TSLとも呼ばれ、インタネット上でやりとりされる情報を、＿＿＿＿＿＿暗号方式により送受信する方法である。
- なりすまし、盗聴、改ざんなどを防ぐことができる。
- SSLによって提供される安全なHTTP通信を HTTPS（Hypertext Transfer Protocol Secure）という。



Webブラウザのアドレス欄に「https://」のように入力して利用する

S / MIME

- S / MIME（Secure / Multipurpose Internet Mail Extensions）は、＿＿＿＿＿＿のための暗号化技術である。
- 公開鍵暗号方式あるいはハイブリット暗号方式とデジタル署名技術を組み合わせて使用する。
- メールの宛先と送信元アドレス以外が暗号化され、MIME形式の＿＿＿＿＿＿として送信される。



20XX年　国家試験問題

医療情報システムの安全管理で誤っているのはどれか。

1. 電子保存の三原則は真正性、見読性、保存性である。
2. 職種によってアクセスできる資源の種類を制限しない。
3. 不正アクセスを防止するために生体認識方式を用いる。
4. ユーザがアクセスした情報内容を記録する。
5. ユーザの登録を義務化する。

2008年（平成19年2月） 国家試験問題

情報セキュリティ対策で関係ないのはどれか。

1. ユーザ認証
2. デジタル署名
3. データの暗号化
4. HL7（Health Level 7）
5. VPN（Virtual Private Network）