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無許可のアクセスや漏洩、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。← 医療では、医療情報、患者情報など

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＿＿＿性、＿＿＿性、および＿＿＿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。

この定義文章の中の

「機密性」、「完全性」、「可用性」

は情報セキュリティの３要素と呼ばれる。

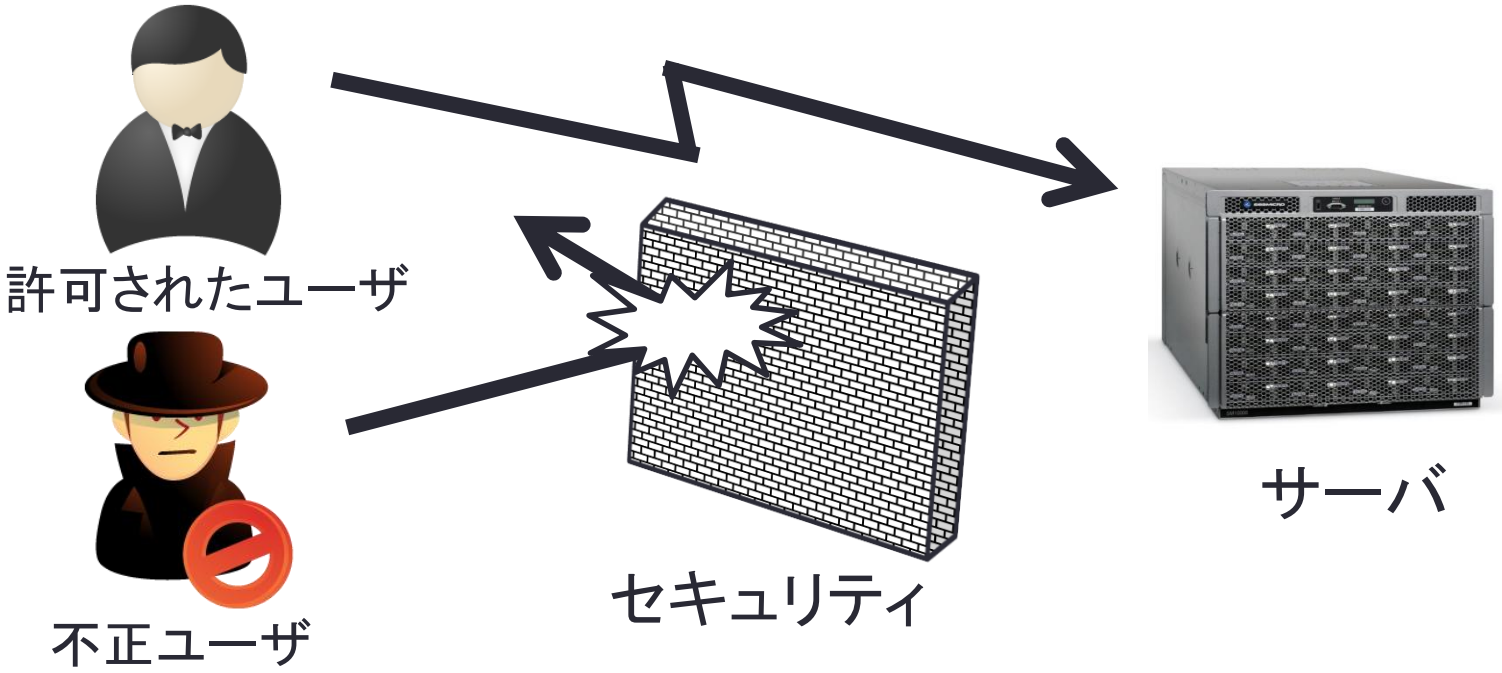
英語の頭文字をとって「CIA」とも呼ばれる

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、情報を使用不可または非公開にする特性」

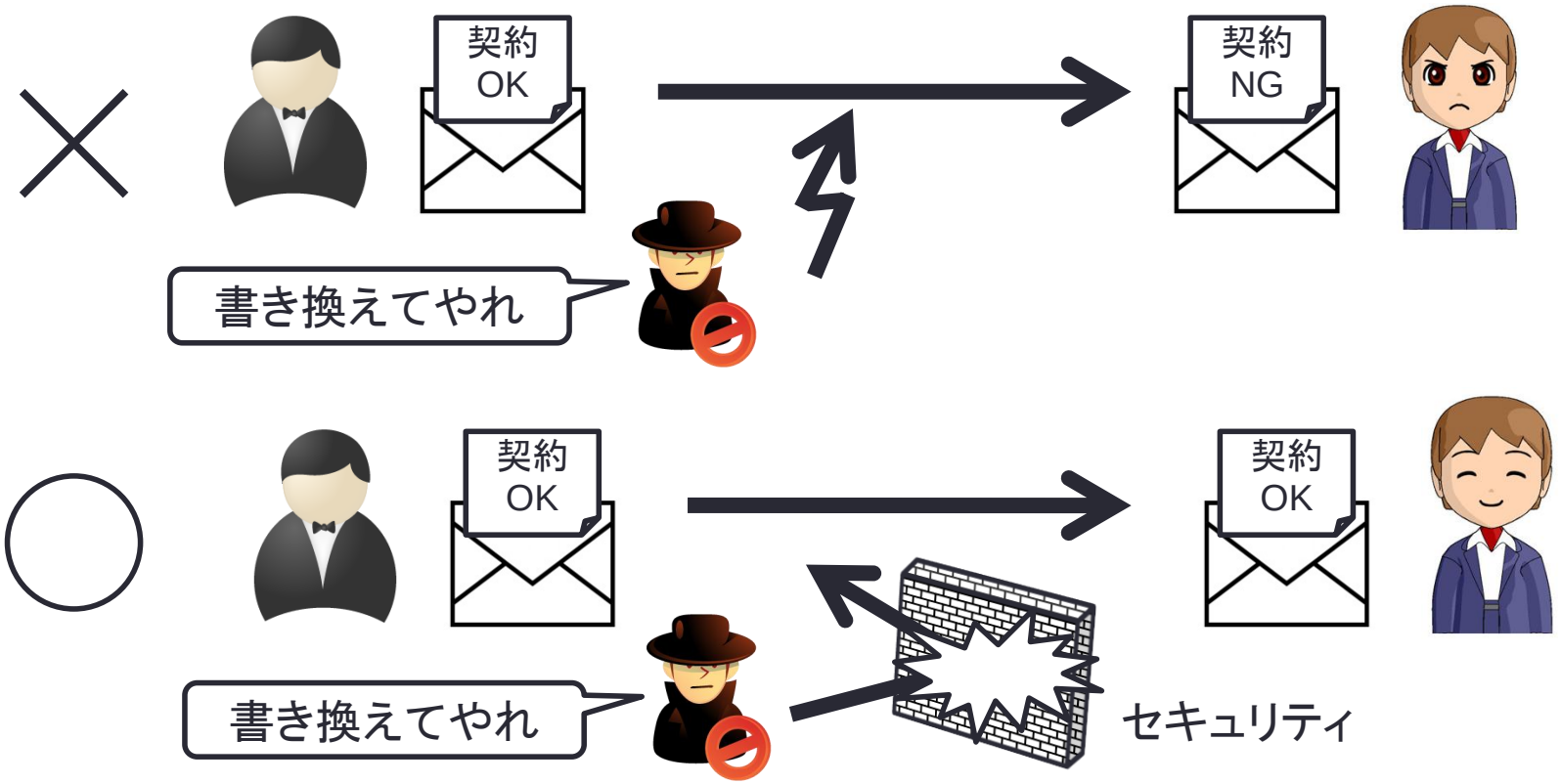
つまり、許可された者だけが情報にアクセスできるということである。



完全性　Integrity

「情報資産の正確さおよび完全さを保護する特性」

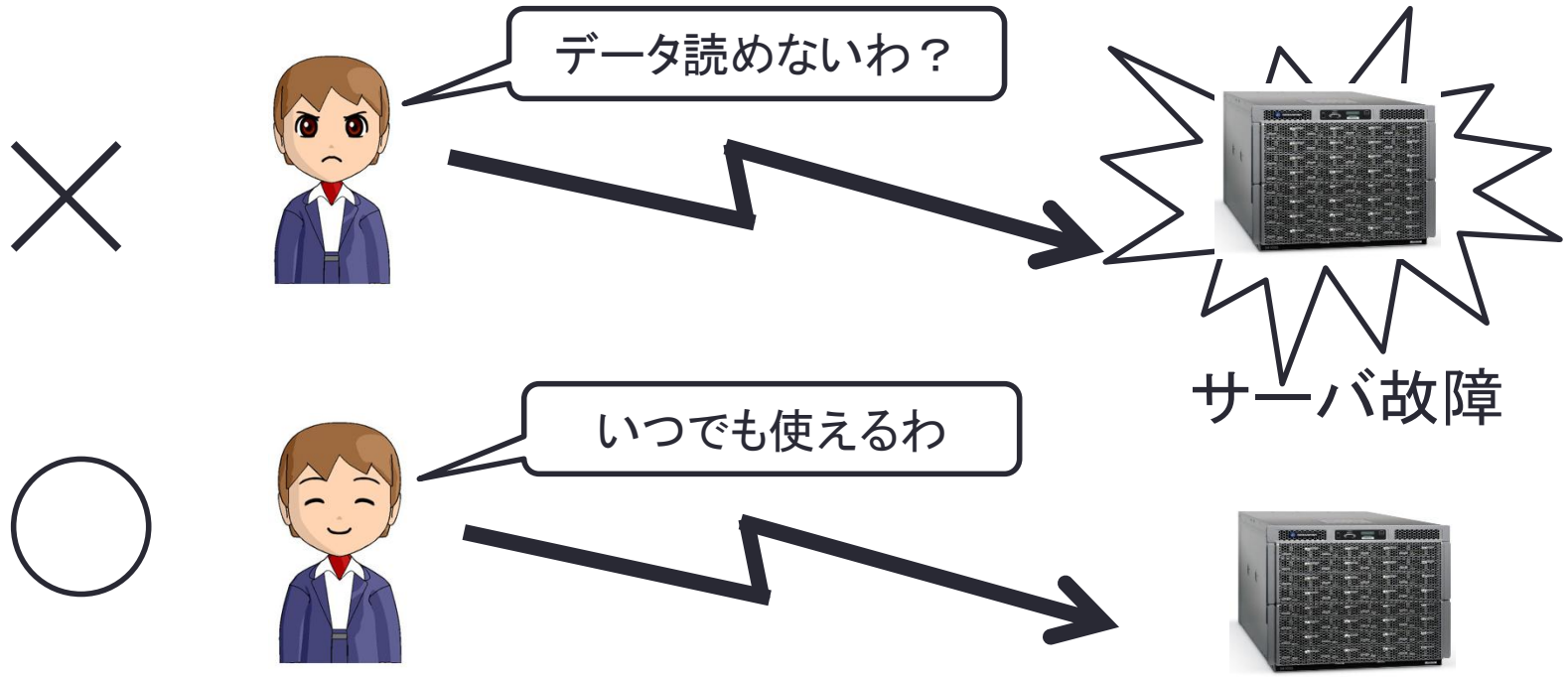
つまり、途中で情報が書き換えられることなく、正確かつ完全である状態を保つことである。



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。」←見読性と同等

つまり、サーバなどに故障がなく、許可された利用者が必要なときにアクセスできるということである。



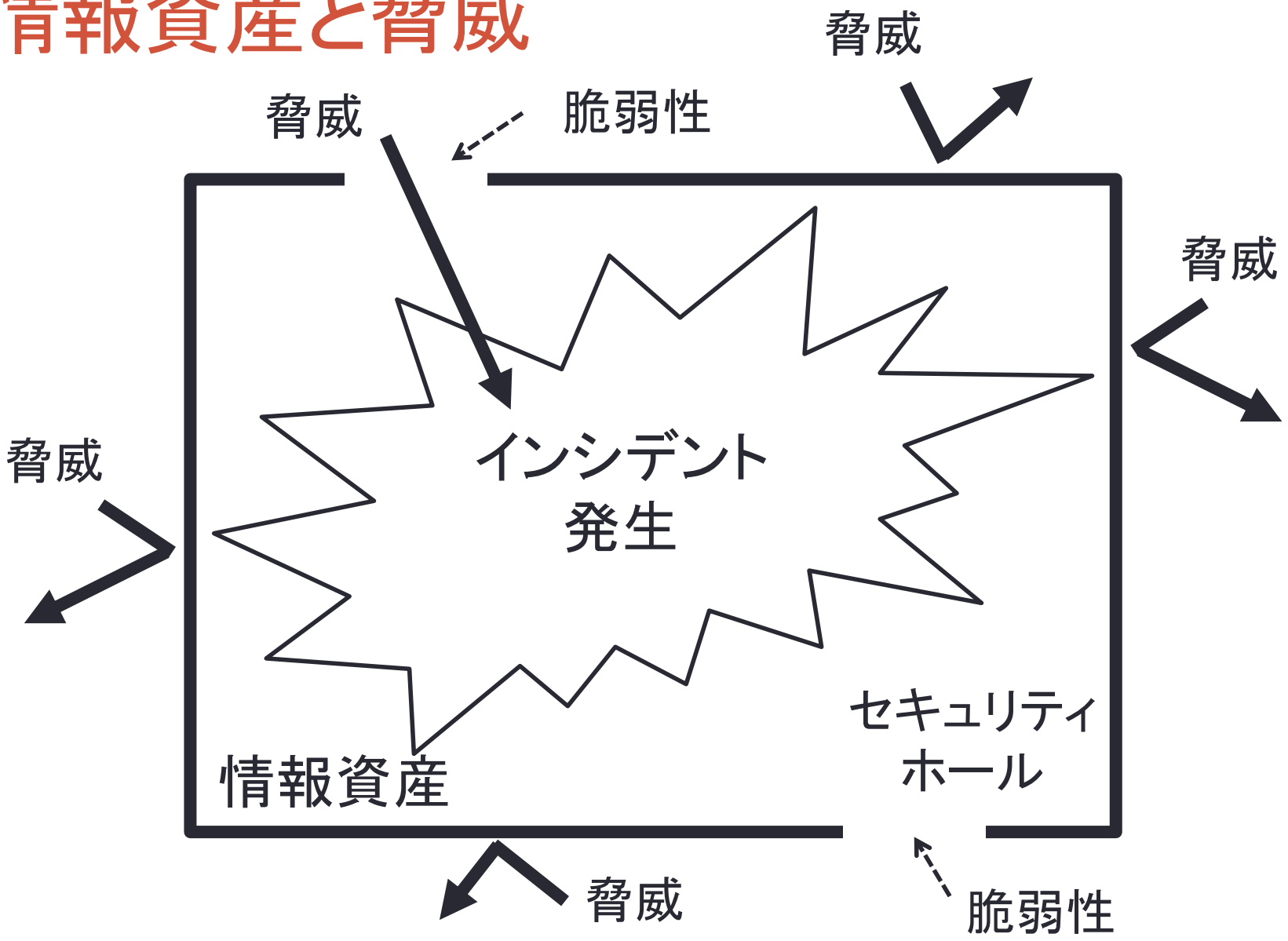
その他の情報セキュリティ要素

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「リスク」(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「セキュリティホール」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、「インシデント」(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

環境的脅威 ・・・・ 自然災害など環境に依る脅威

的脅威 ・・・・ 人が介在する脅威

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

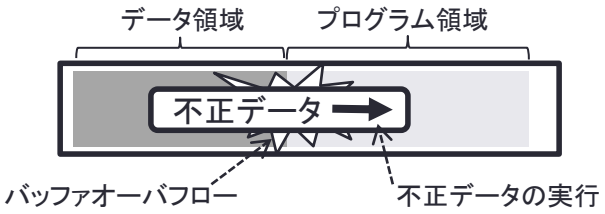
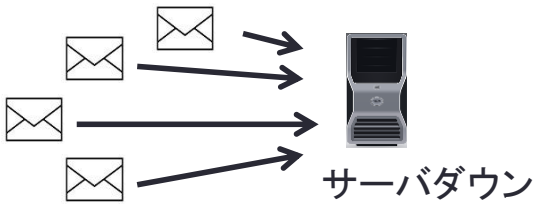
意図的に脅威を与えようとする人 → クラッカー

- 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きなくする行為

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
	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
	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
ワーム	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。感染したコンピュータ内に潜伏しなんらかのトリガーで活動する
マクロウィルス	アプリケーションの持つマクロ機能を悪用して感染するマルウェア　→Excelのマクロ機能など
キーロガー／スクリーンロガー	利用者のキー入力や画面のキャプチャを別の装置へ送信するマルウェア。パスワード等の取得に用いられる
ボット	感染後、外部からの指示に従って動作するマルウェア
	データを強制的に暗号化して使えない状態し、解除のために身代金を要求する画面を表示するマルウェア。金銭を搾取するため使われる

マルウェアの挙動

挙動	内容
破壊	ファイルシステムの破壊、ファイルの削除、記憶装置にランダムな書き込みを行う、など
OSダウン、 OSリブート	強制的にOSをダウンさせる、あるいは、リブートさせる
パスワード、 アカウント収集	_____等で、クレジットカードの暗証番号やアカウント情報をを盗み出す
DoS攻撃	感染したコンピュータ（踏み台）から別のコンピュータに対し無意味な大量のデータを送り付ける。同時に多数のコンピュータから送りつけることも（DDoS）
	感染したコンピュータから別のコンピュータに対し大量のメール（　　メール）を送りつける
ファイル公開	感染した端末内のファイルを勝手に公開する
	攻撃者がコンピュータをコントロールできるようにするために、端末に裏口を作成する。

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）＿＿＿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
ファイル感染型	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。
システム領域感染型	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

2005年3月（2021年1月第5.1版改定）に厚生労働省から通達された「医療情報システムの安全管理に関するガイドライン」では、

- ✓ _____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。

「医療情報システムの安全管理に関するガイドライン」が要求する基本的安全管理対策の概要

①安全管理方針を制定し公表すること
②情報セキュリティマネジメントシステム（　　）を実践すること
③組織的、物理的、技術的、人的な安全管理対策を立てること
④情報を破棄する際の対策を立てること
⑤情報システムの改造と保守の際の対策を立てること
⑥情報および情報機器の持ち出しについて対策を立てること
⑦災害、サイバー攻撃等の非常時の対応について対策を立てること
⑧外部と個人情報を含む医療情報を交換する場合の安全管理について対策を立てること
⑨法令で定められた記名・押印を電子署名で行う場合の管理策を立てること

情報セキュリティ対策の分類

セキュリティ対策	説明
人的・組織的 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。
物理的 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。
技術的 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。

組織的セキュリティ対策（組織的安全管理対策）

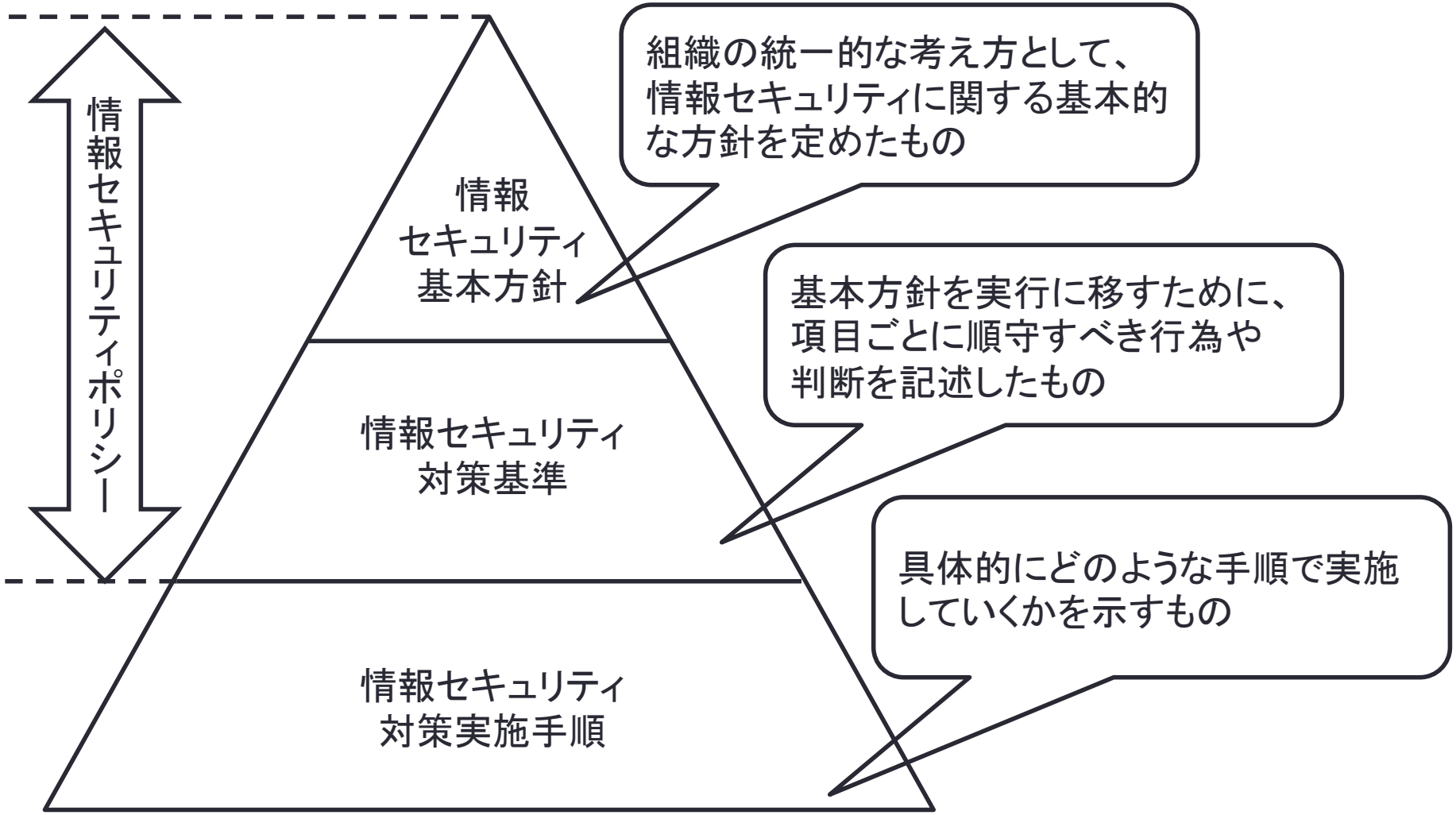
組織として情報資源を守るためには、

- 職員の責任と権限を明確に定める
- 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自己点検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



大　学
情報セキュリティポリシー

注意事項	情報セキュリティポリシーのうち「Ⅱ　対策基準」の部分については**「学外秘」**となっているので取扱いには十分留意すること。

平成　　年　　月　　日策定
平成　　年　　月　　日改定
平成　　年　　月　　日改定
平成　　年　　月　　日改定
平成　　年　　月　　日改定
令和　　年　　月　　日改定
令和　　年　　月　　日改定
令和　　年　　月　　日改定
令和　　年　　月　　日改定

大学　　委員会

手順書

- PCセキュリティ対策実施手順 PDF（PDF）
- ・・・　手順書 PDF（PDF）
  ・・・　管理台帳 EXCEL（Excel）
- ・・・　手順書 PDF（PDF）
  ・・・　管理台帳 EXCEL（Excel）
- ・・・　手順書 PDF（PDF）

情報セキュリティマネジメントシステム

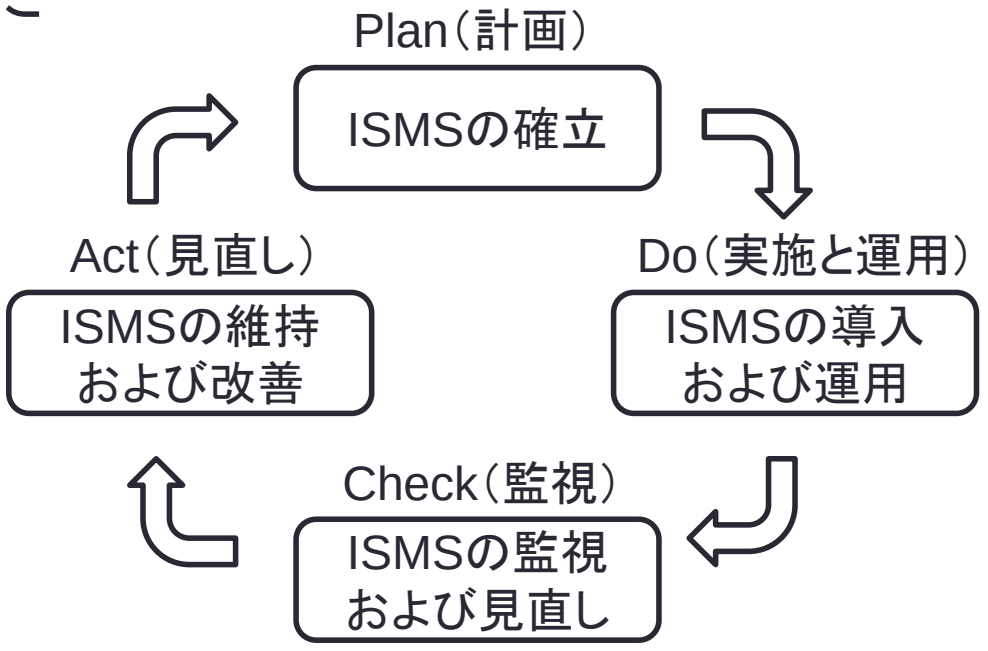
ISMS：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

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

- 計画（Plan）
- 実施と運用（Do）
- 監視（Check）
- 見直し（Act）

を行い、

＿＿＿＿サイクル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＿＿＿＿＿＿＿＿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ユーザマニュアル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。

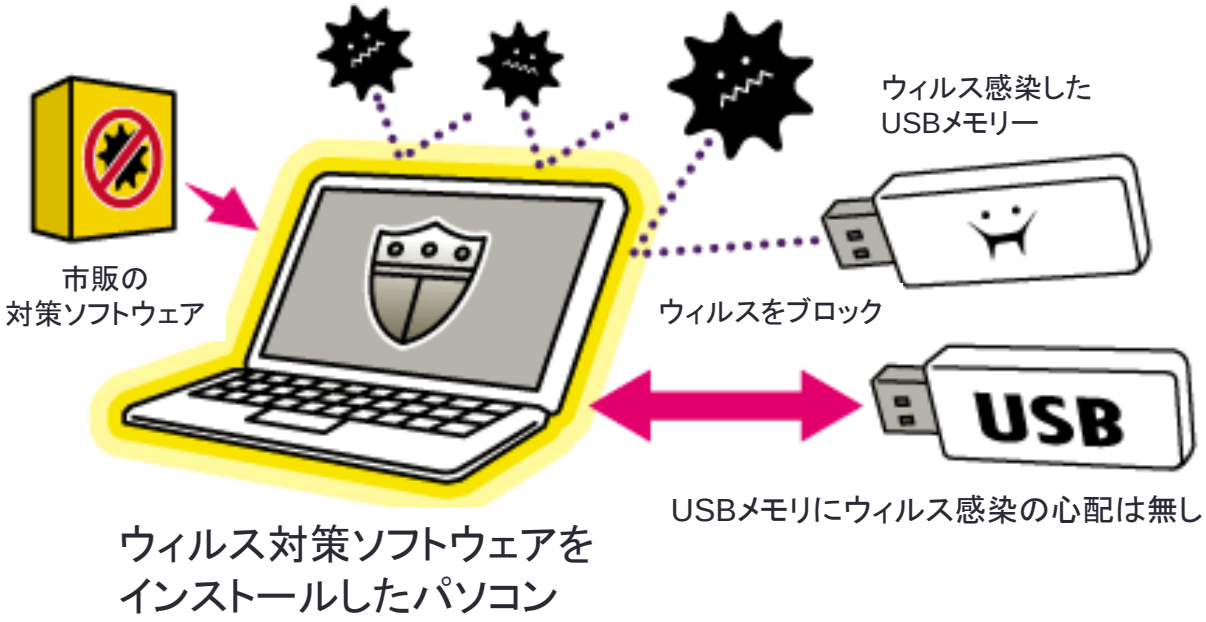
ソフトウェアのメーカーは、多くのセキュリティパッチを順次インストールする手間を省くために、定期的に多数のセキュリティパッチを1つのプログラムにまとめて配布している。Windowsには、自動的にセキュリティパッチをダウンロードして更新するWindows Updateと呼ばれる機能がある。

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（　　）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、

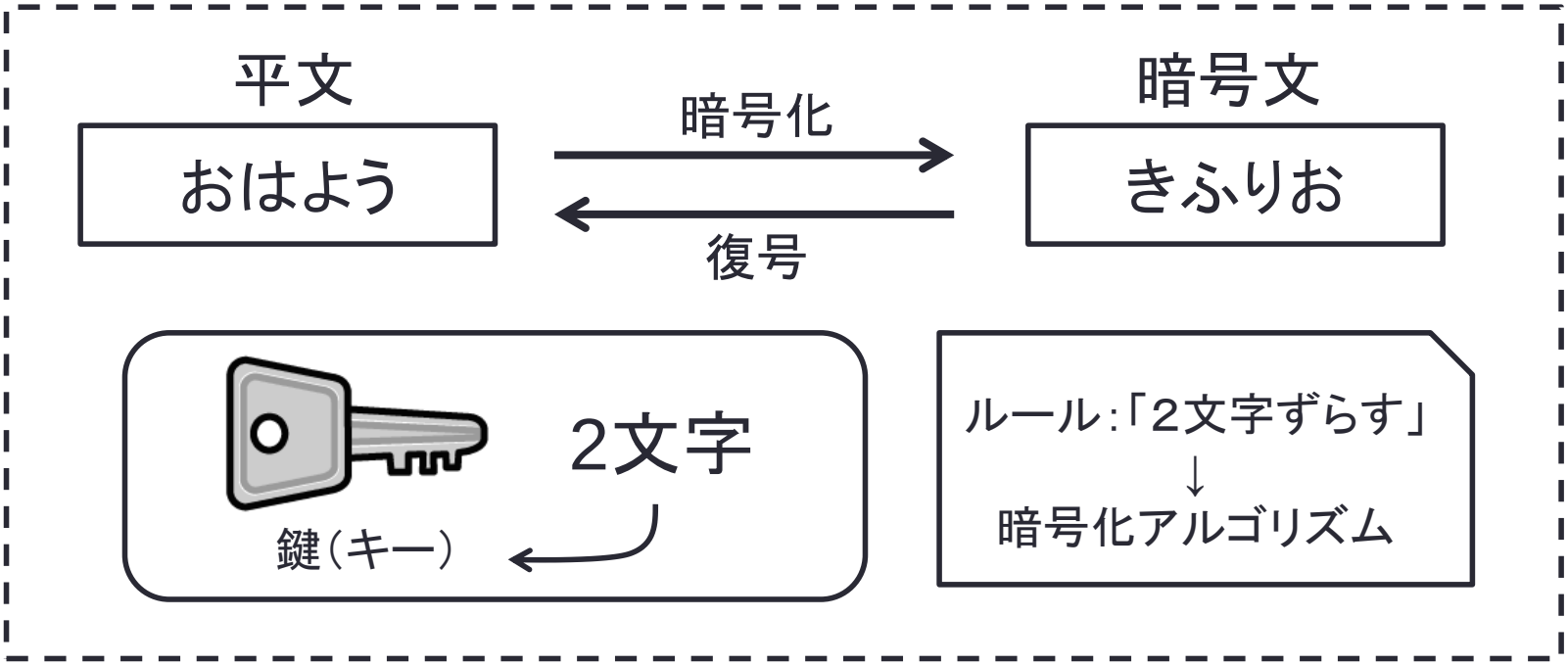
- パスワード認証
- ＿＿＿＿＿パスワード認証 → 1回限りの使い捨てのパスワードを使った認証
- ICカード認証
- 生体認証 → バイオメトリクス認証（biometrics）ともいい、人の身体的特徴や行動的特徴によって認証するする方法である。
  - 指紋認証
  - 虹彩（アイリス）認証
  - 声紋認証
  - 顔認証
  - 指静脈認証　など
- ＿＿＿＿認証

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。 → アクセス制御
- 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。→ アクセスログ

暗号化技術

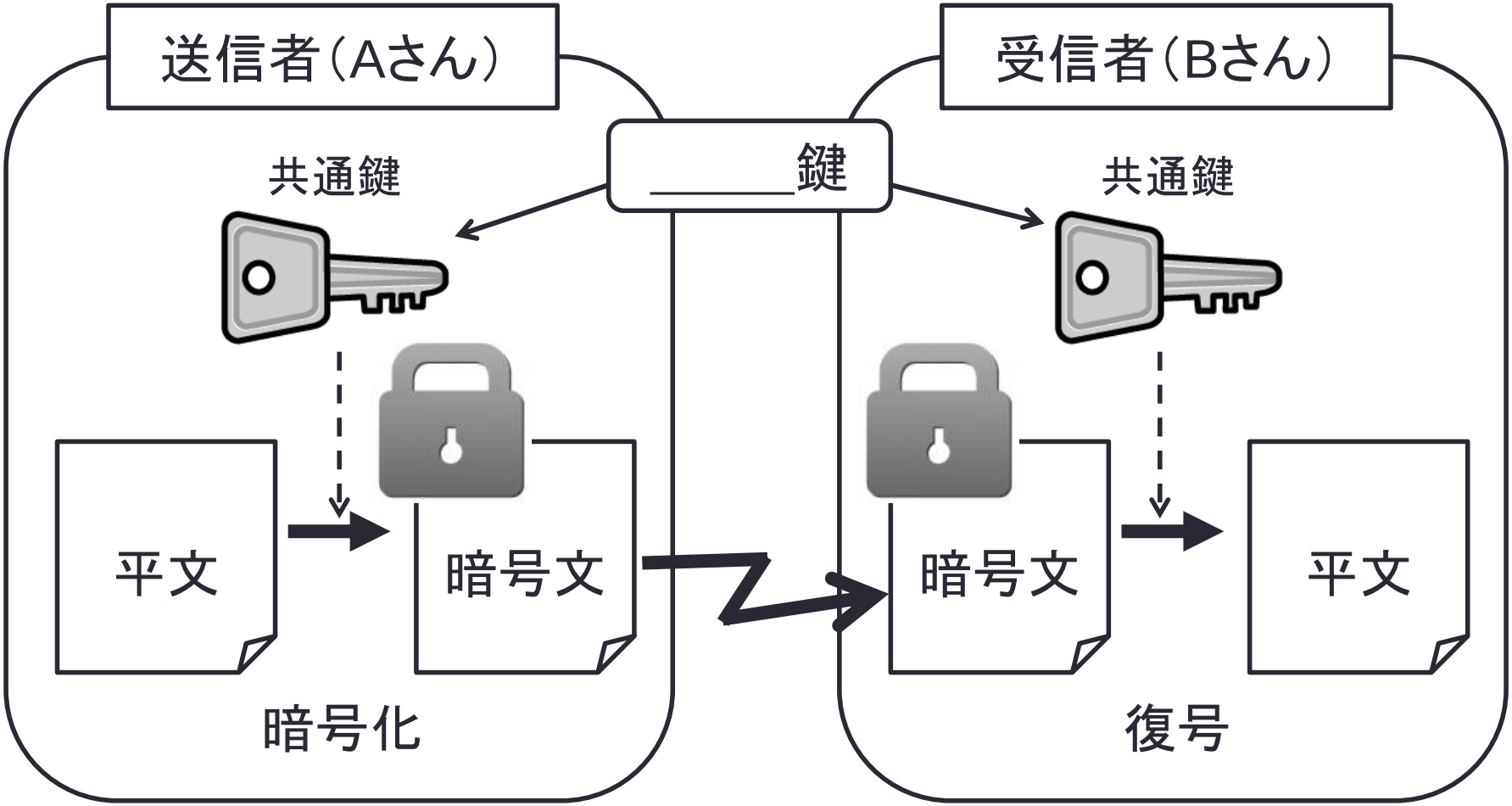
暗号化（Encryption）とは、ある一定のルールに基づいて
データを変換し、第三者に知られないようにする技術である。



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

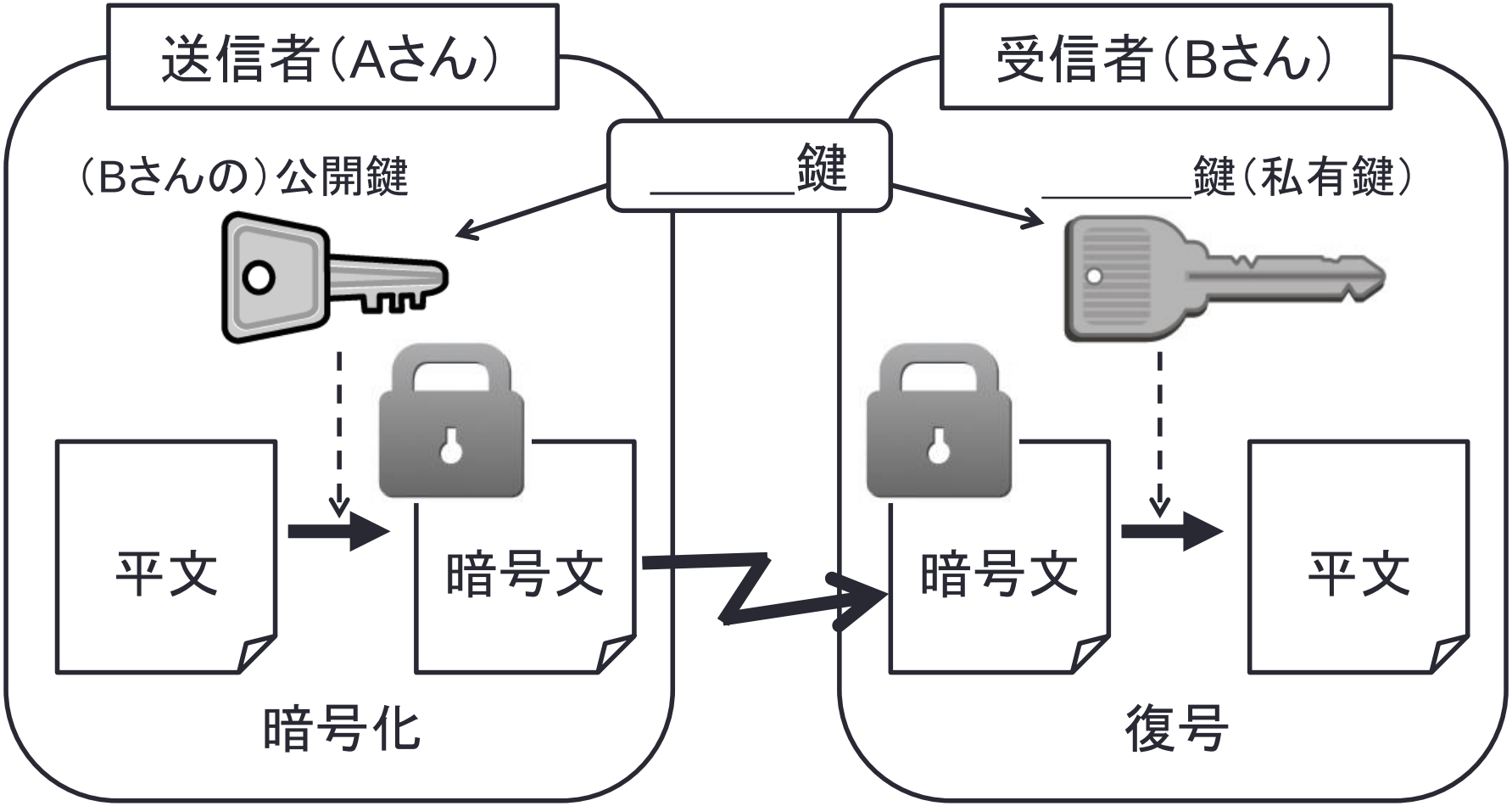
共通鍵暗号方式

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



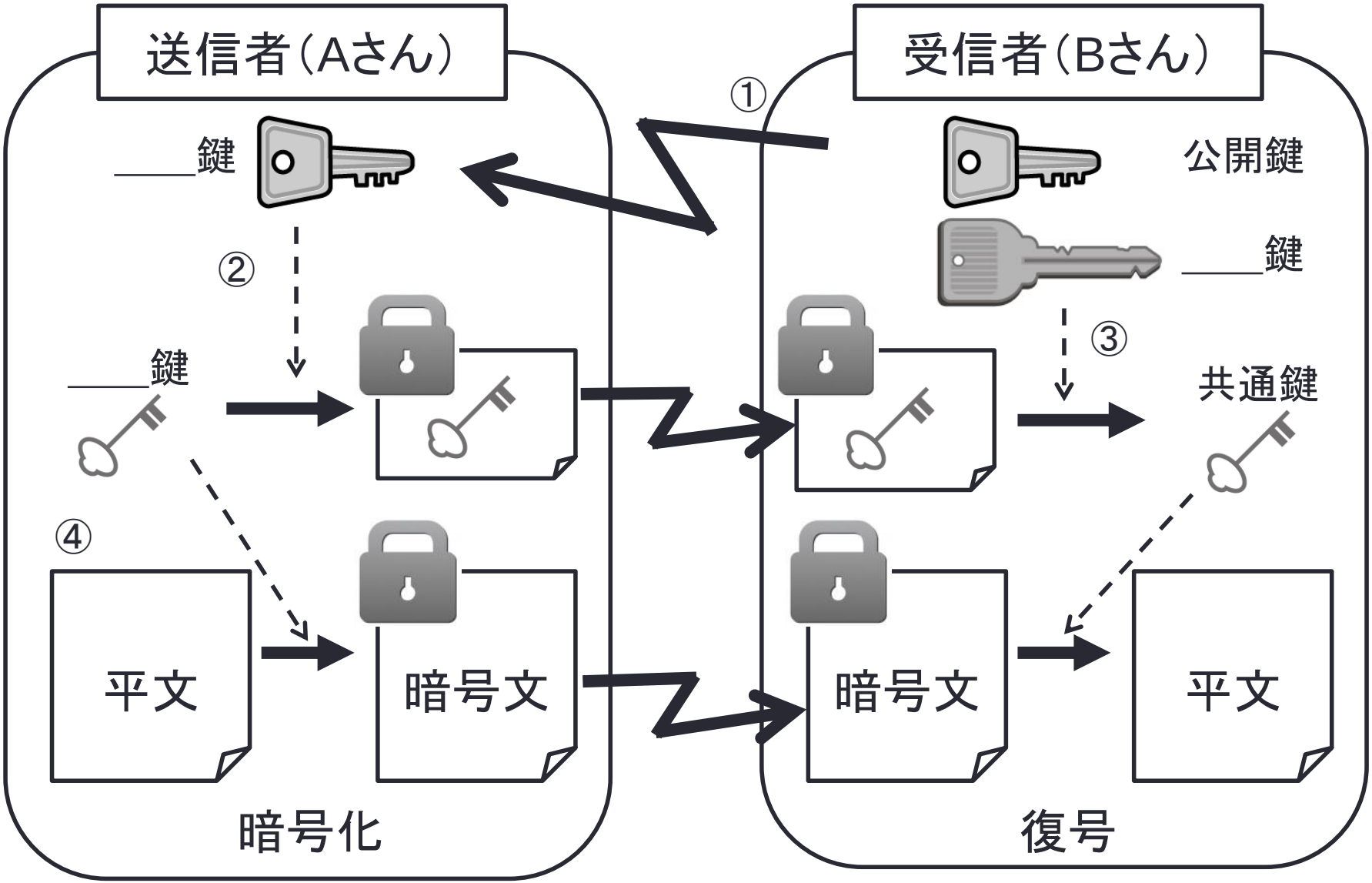
公開鍵暗号方式

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

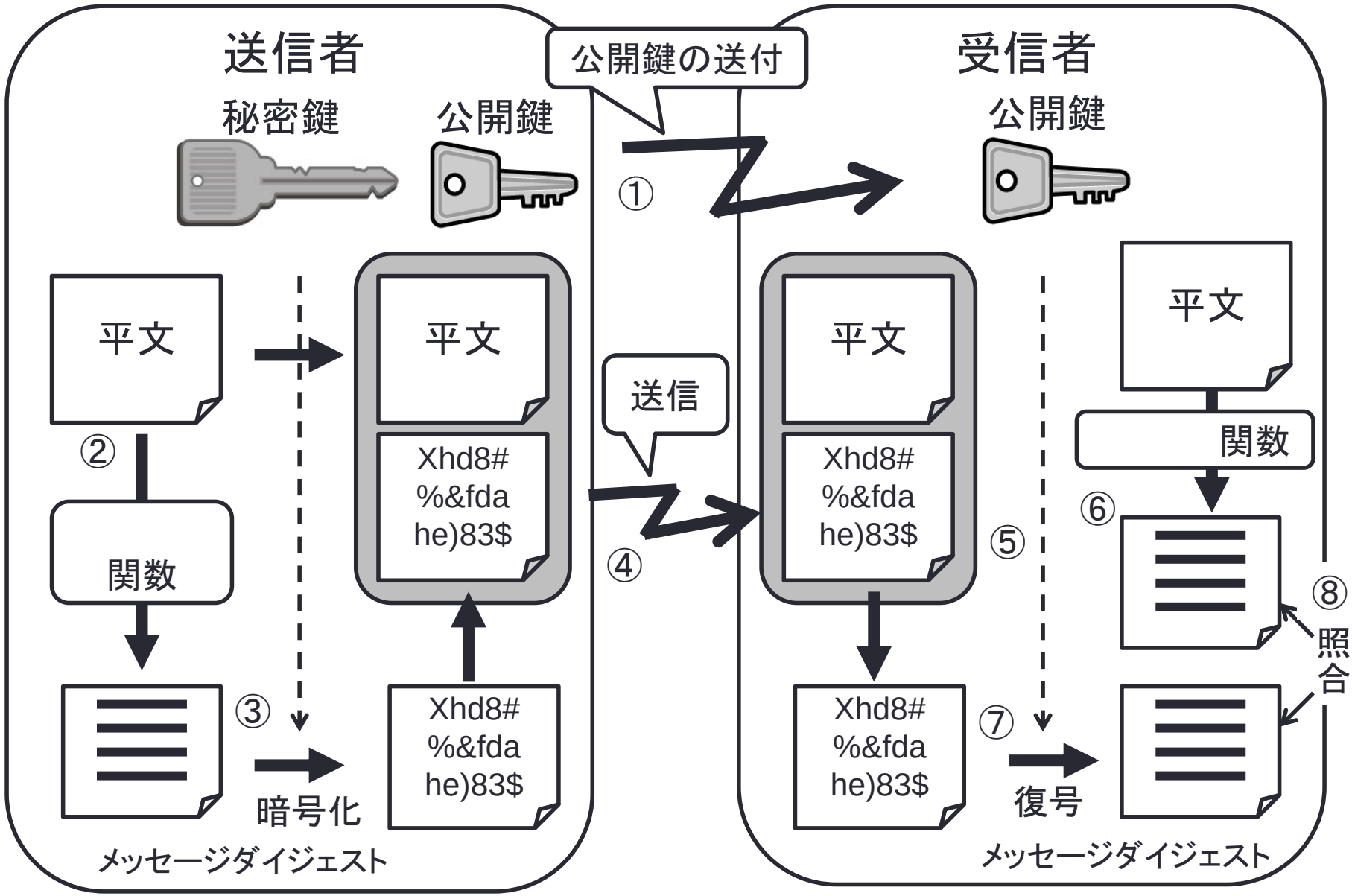


ハイブリット暗号方式

←電子署名やSSL・TLS等で利用されている

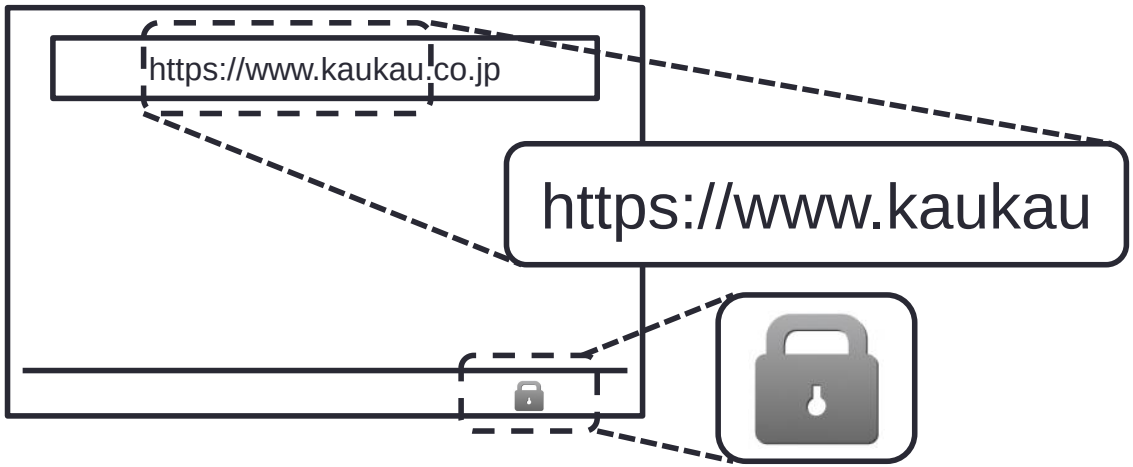


デジタル署名（電子署名）


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

SSL / TSL

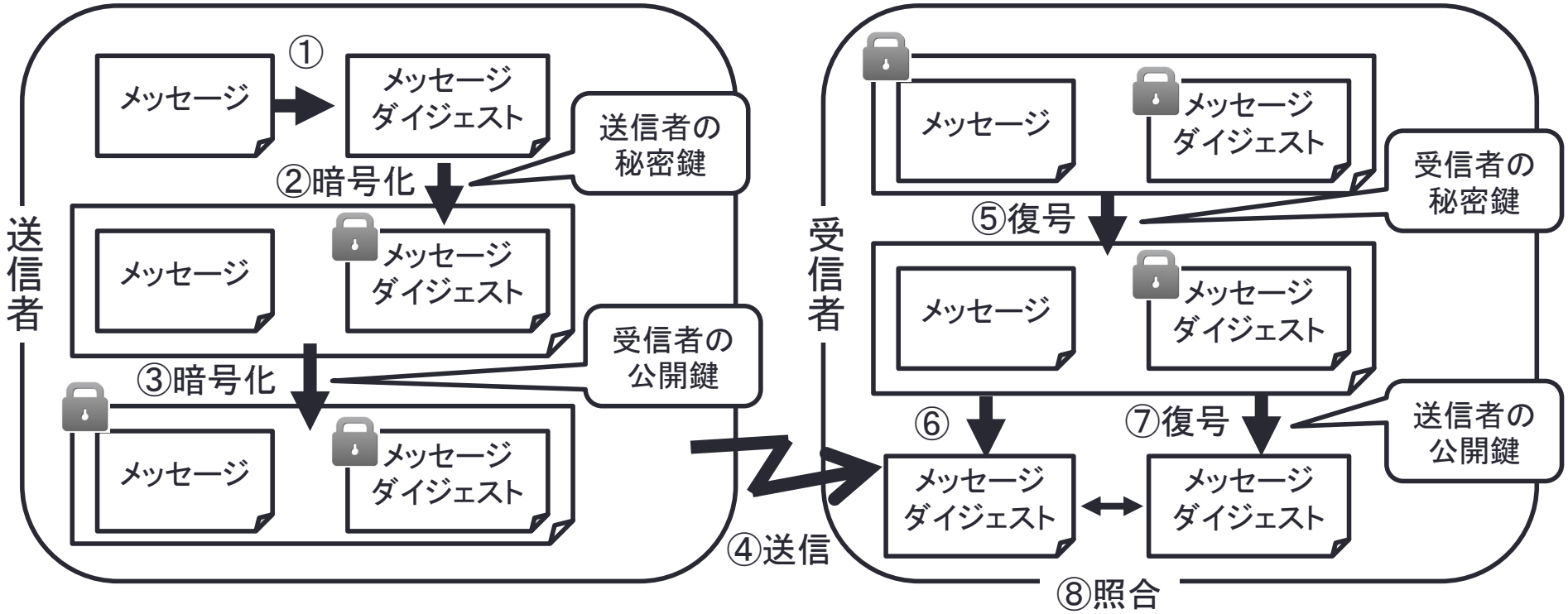
- SSL（Secure Socket Layer）は、その改良版である TLS（Transport Layer Security）とともにSSL/TSLとも呼ばれ、インタネット上でやりとりされる情報を、＿＿＿＿＿＿暗号方式により送受信する方法である。
- なりすまし、盗聴、改ざんなどを防ぐことができる。
- SSLによって提供される安全なHTTP通信を HTTPS（Hypertext Transfer Protocol ＿＿＿＿）という。



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

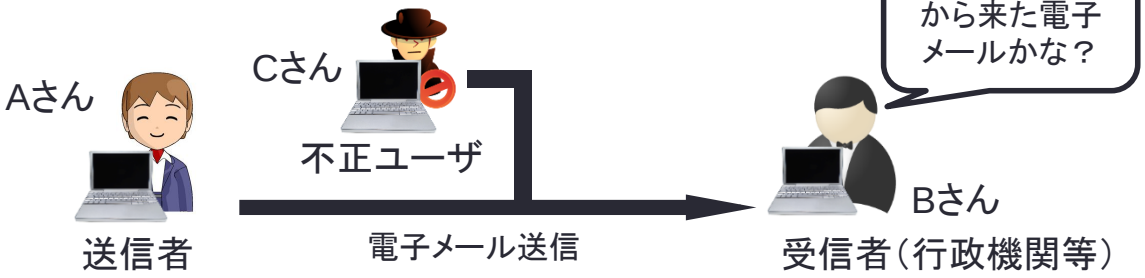
- S / MIME（Secure / Multipurpose Internet Mail Extensions）は、電子メールのための暗号化技術である。
- 公開鍵暗号方式あるいはハイブリット暗号方式とデジタル署名技術を組み合わせて使用する。
- メールの宛先と送信元アドレス以外が暗号化され、MIME形式の＿＿＿＿＿＿として送信される。



デジタル社会における課題

➢ _____

←インターネット上のデジタル文章については、文章作成者の特定が困難



例えば、sato@abcsesaku.co.jpというメールアドレスで、ABC政策株式会社という名義で文章が送られて来たとしても・・・・・

- 「ABC政策株式会社」が実在しないかもしれない
- 「佐藤」さんが実在しないかもしれない
- 第3者が実在する「ABC政策株式会社」の「佐藤」さんのメールアドレスを乱用しているかもしれない

という疑いが解消できない

➢ 改ざん

←送信途上でメッセージを書き換えることが容易

デジタル文章は、手書き文章と異なり、改ざんされても痕跡が残らず、改ざん箇所を発見することが困難

➢ 送信否認

←送信内容の否認を防止することが困難

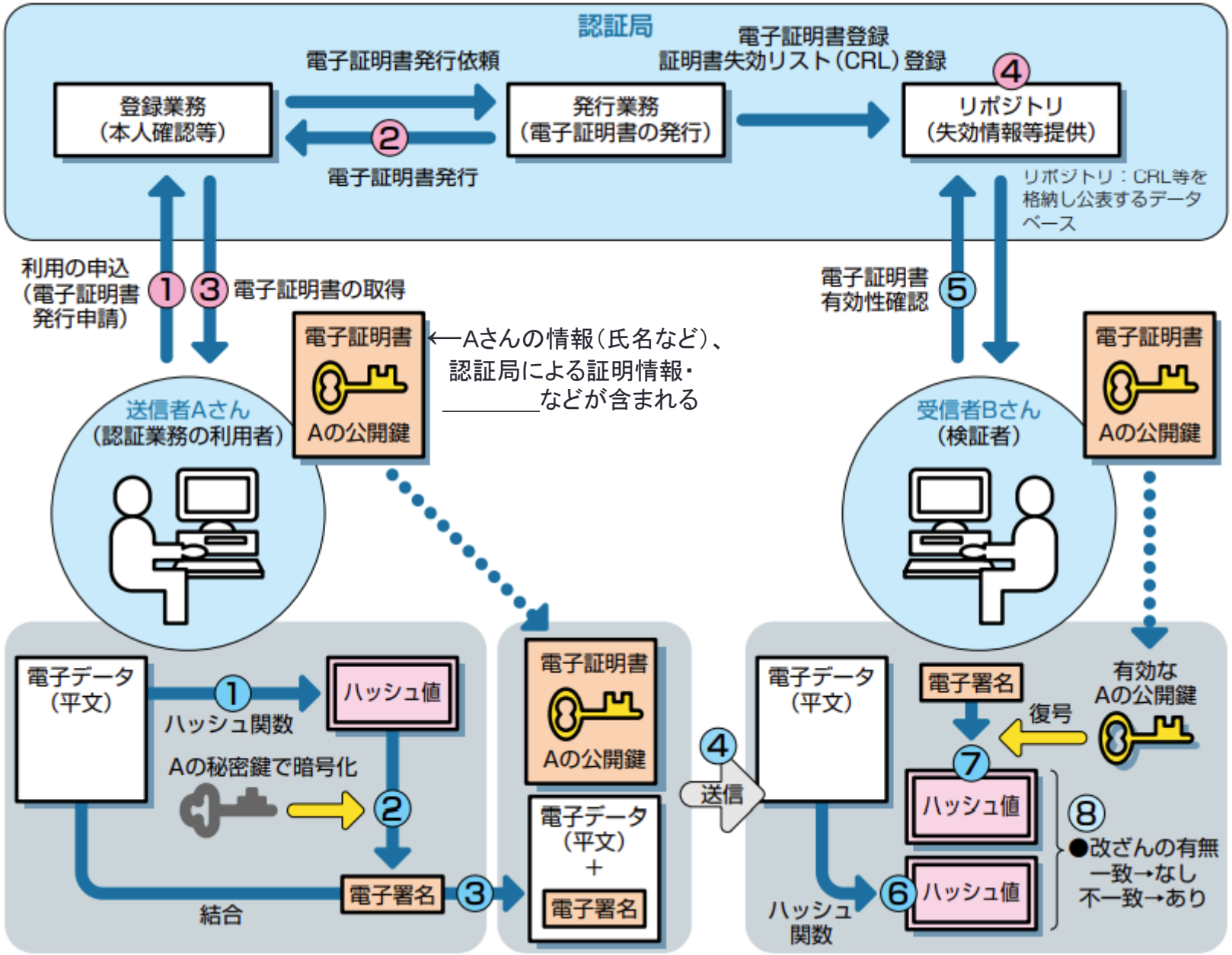
オンラインで送信されて来た申請・届出に基づいて、手続きを進行させていたところ、送信者からそのような送信はしていないと否認される危険性がある

PKI（Public Key Infrastructure）
公開鍵（認証）基盤

- 公開鍵暗号方式に基づく電子認証の技術基盤
- 公開鍵とその公開鍵の持ち主の対応関係を保証するための仕組み
- 秘密鍵による暗号化（電子署名）、公開鍵による復号化、＿＿鍵の電子証明書を組み合わせることで本人性の確認や文章の改ざんの有無の検知を行うもの
- 公開鍵とその持ち主の対応関係を＿＿＿＿（CA、Certification Authority）という第三者機関を用いて保証する
- 公開鍵の所有者が確実に本人であることを保証する公開鍵証明書（public key certificate）＝電子証明書を登録・発行して利用する
- 認証局は公開鍵証明書などの電子証明書を発行する実体である

← 電子認証登記所（法務省）、日本電子認証株式会社など

PKI・電子署名・認証の仕組み（公開鍵暗号方式に基づく）



出典：総務省HP 電子署名・認証・タイムスタンプ その役割と活用（リーフレット）https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/pdf/090611_1.pdf

HPKI（Healthcare Public Key Infrastructure）
保健医療福祉分野 公開鍵（認証）基盤

① 電子署名を付与した人物の身分証明情報 ←PKI電子証明書に含まれる基本情報

＋

② 保健医療福祉分野の＿＿＿＿＿ →医師など27種
③ 医療施設での管理者資格 →病院長など5種

↑
①に加えて、HPKI電子証明書で格納される情報

ISO IS 17090という国際標準に準拠した基盤として整備されている

HPKI電子証明書の発行・認証を行う認証局

- ✓ 医療情報システム開発センター（MEDIS-DC）
- ✓ 日本医師会
- ✓ 日本薬剤師会

1. HPKIが推奨されていること
2. その文書がその時間に存在していたという時間を証明する必要があること
3. 有効な電子署名を用いる必要があること

かみくだくと

1. 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI認証局又は認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと
2. 電子署名を含む文書全体にタイムスタンプを付与すること
3. タイムスタンプを付与する時点で有効な電子証明書を用いること

「医療情報システムの安全管理に関するガイドライン」第5.1版
−6.12 法令で定められた記名・押印を電子署名で行うことについて
−C項 最低限のガイドライン（必ず守るべきガイドライン）

HPKIに格納できる医療国家資格と管理責任者の情報

資格名【国家資格】	
医師 (Medical Doctor)	社会福祉士 (Certified Social Worker)
歯科医師 (Dentist)	介護福祉士 (Certified Care Worker)
薬剤師 (Pharmacist)	救急救命士 (Emergency Medical Technician)
臨床検査技師 (Medical Technologist)	精神保健福祉士 (Psychiatric Social Worker)
診療放射線技師 (Radiological Technologist)	臨床工学技士 (Clinical Engineer)
看護師 (Registered Nurse)	あん摩マッサージ指圧師 (Massage and Finger Pressure Practitioner)
保健師 (Public Health Nurse)	はり師 (Acupuncturist)
助産師 (Midwife)	きゅう師 (Moxibustion Practitioner)
理学療法士 (Physical Therapist)	歯科衛生士 (Dental Hygienist)
作業療法士 (Occupational Therapist)	義肢装具士 (Prosthetist and Orthotist)
視能訓練士 (Orthoptist)	柔道整復師 (Judo Therapist)
言語聴覚士 (Speech Therapist)	衛生検査技師 (Clinical Laboratory Technician)
歯科技工士 (Dental Technician)	公認心理師 (Certified Public Psychologist)
管理栄養士 (National Registered Dietitian)	
資格名 【医療機関の管理責任者】	
病院長 (Director of Hospital)	
診療所院長 (Director of Clinic)	
管理薬剤師 (Supervisor of Pharmacy)	
薬局開設者 (Proprietor of Pharmacy)	
その他の保健医療福祉機関の 管理責任者 (Director)	

お問い合わせ

Medis
Medical Information System Development Center

厚生労働省認可電子証明書　HPKI　Healthcare Public Key Infrastructure

保健医療福祉分野公開鍵基盤 電子認証局のご案内

一般財団法人医療情報システム開発センター(MEDIS)

MEDISは厚生労働省が定めた保健医療福祉の27種の国家資格者、医療機関の5種の管理責任者の他、医療従事者の資格が空欄の医療事務職員等向けのHPKIカードを発行しています。

HPKIは、
厚生労働省が定めた唯一の
医療従事者の電子認証です。

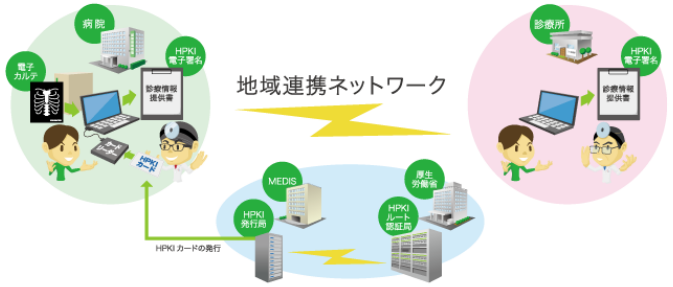
HPKIは、暗号技術である
公開鍵基盤(PKI)を活用した
安全・安心な仕組みです。

HPKIの使い方（例）と活用事例

医療従事者がHPKIカードを使い電子署名することで、記録内容や記録時間をあとから証明することができます。

- 電子カルテに記載した内容を確定して電子保存する際の電子署名
- 紙のカルテをスキャンして電子保存する際の電子署名
- 診療情報提供書や患者紹介状を電子的に発行する際、医師であることの電子的証明
- 自分が作成した電子ファイルを広く公開する際に、自分が作成したことの電子的証明（私有鍵と公開鍵の活用）
- 医療従事者の資格等を証明

HPKIの活用例概念図



出典：一般財団法人 医療情報システム開発センターHP
https://www.medis.or.jp/8_hpki/

76

午　前

◎ 指示があるまで開かないこと。

（令和 6 年 2 月 15 日　9 時 30 分 ～ 12 時 05 分）

47　HIS における情報セキュリティ管理の目的で正しいのはどれか。

1. 病院の経営改善
2. 患者診療情報の保護
3. 医薬品安全情報の提供
4. 診療行為の妥当性の担保
5. 放射性廃棄物の適切な処理

71

午　前

◎ 指示があるまで開かないこと。

(平成 31 年 2 月 21 日　9 時 30 分 ～ 12 時 05 分)

49　医療情報の安全管理の観点から正しいのはどれか。

1. 個人所有のパソコンに患者情報を保存する。
2. 他施設と電子メールで患者情報の交換を行う。
3. 電子カルテで部署共通のアカウントを使用する。
4. 不正アクセスを防止するため生体認証方式を用いる。
5. 電子カルテ端末の通信には無線 LAN は使用してはならない。

67

午　後

◎ 指示があるまで開かないこと。

（平成 27 年 2 月 26 日　13 時 25 分 ～ 16 時 00 分）

49　用語の説明で正しいのはどれか。**2 つ選べ**。

1. DICOM は医用画像と通信の標準規格である。
2. SSL は情報を暗号化して送受信するプロトコルである。
3. CAD はコンピュータによる自動確定診断システムである。
4. テレラジオロジーとは医用画像を外部保存することである。
5. HL7 は RIS からモダリティ装置へ患者基本情報を送る標準規格である。

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。

2014年（平成25年2月） 国家試験問題

医療情報システムの安全管理で正しいのはどれか。

1. 電子メールで他施設と患者情報の交換を行う。
2. 利便性のために個人のソフトをインストールする。
3. バックアップのために個人の外部メディアに保存する。
4. 不正アクセスを防止するために生体認証方式を用いる。
5. 電子保存の三原則は、真正性、再現性および保存性である。

2013年（平成24年2月） 国家試験問題

医療情報システムにおける個人情報保護で正しいのはどれか。2つ選べ。

1. 生体情報認証システムの導入
2. アクセスログの定期的な監視
3. 患者本人の了解がない家族への情報開示
4. 電子メールを用いた院外者との患者情報の交換
5. 紛失を避けるための医療従事者個人でのデータ保存

2011年（平成22年2月） 国家試験問題

正しいのはどれか。2つ選べ。

1. SSLはデータを暗号化する方式である。
2. RISは物流管理システムのことである。
3. HISは医用画像保管管理システムのことである。
4. テレラジオロジーとは放射線治療情報のことである。
5. ファイアウォールはセキュリティ対策に有効である。

61

午　前

◎ 指示があるまで開かないこと。

（平成 21 年 2 月 26 日　9 時 30 分 ～ 12 時 00 分）

97　正しい組み合わせはどれか。2つ選べ。

1. セキュリティシステム　------　ICDコード
2. 放射線情報システム　------　RIS
3. 病院情報システム　---------　HL7
4. 医事会計システム　---------　DICOM
5. 物流システム　---------------　JPEG

2009年（平成20年2月）　国家試験問題

正しい組み合わせはどれか。2つ選べ。

1. SSL ---------- セキュリティ対策
2. HIS ---------- 画像管理転送システム
3. 指紋 ---------- ディタル署名
4. ファイアウォール ----- トロイの木馬型
5. 遠隔医療システム --- テレラジオロジー

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）