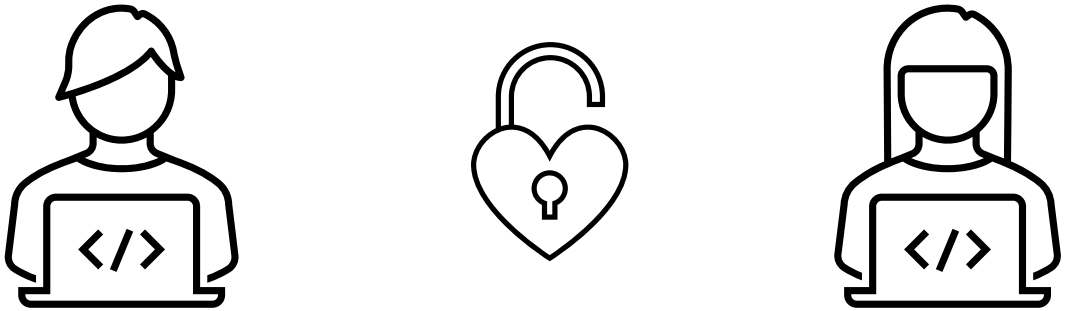
リモートアクセス・ネットワークセキュリティ

情報実験 第８回（2025/06/20）

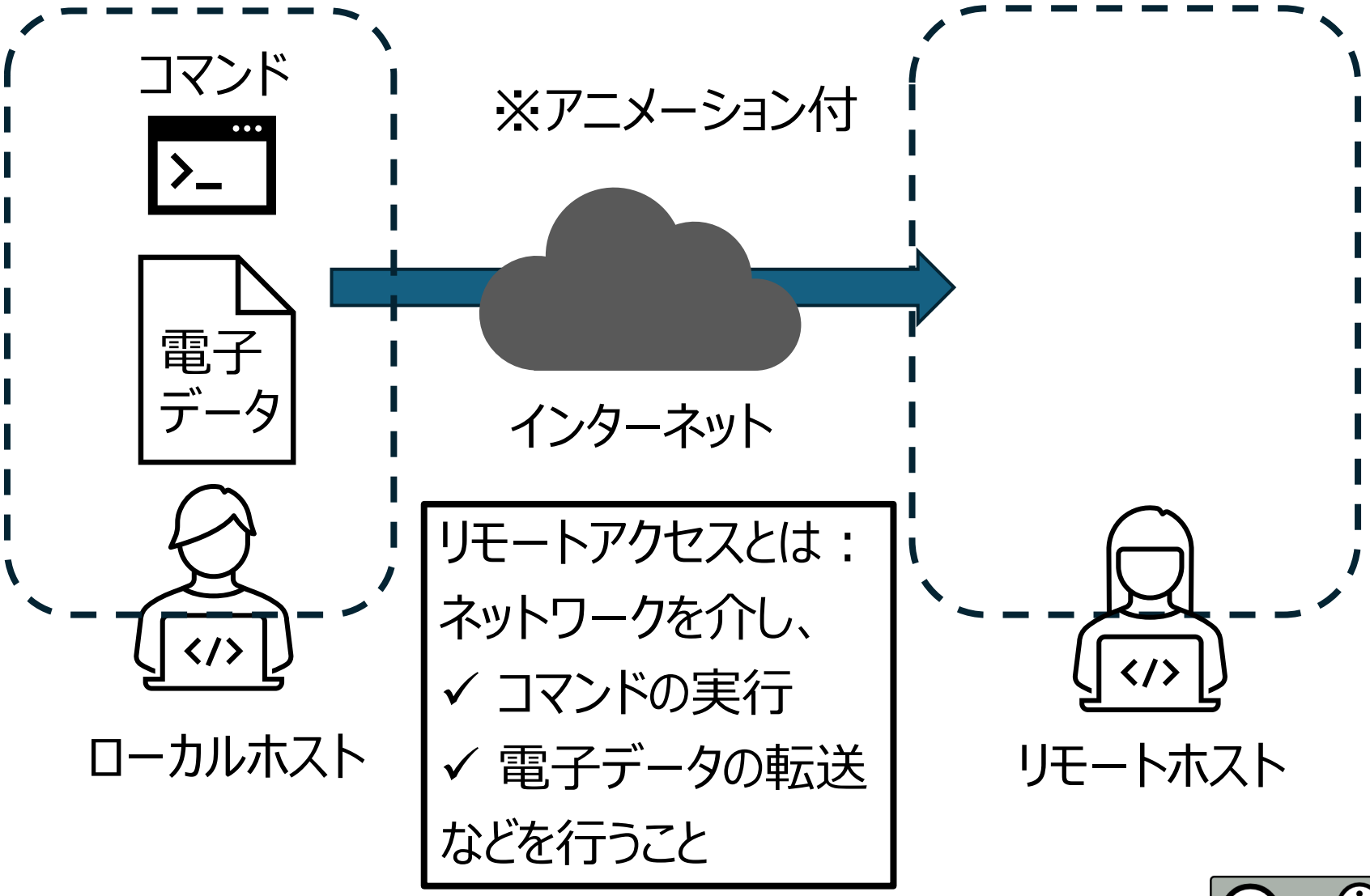


北海道大学　理学院　宇宙理学専攻
修士課程2年　山本峻大

本日の情報実習

- ■リモートアクセス
- ■セキュリティの考え方
- ■ファイル転送のセキュリティ
  - ✓暗号
  - ✓プロトコル
- ■計算機管理のセキュリティ
  - ✓ポート管理・アクセス管理・セキュリティホール

リモートアクセスのしくみ



リモートアクセスとは：
ネットワークを介し、
✓ コマンドの実行
✓ 電子データの転送
などを行うこと

リモートアクセスの必要性

■リモートアクセス

✓手元の計算機 (ローカルホスト) から、
遠隔の計算機 (リモートホスト) に、
ネットワークを介して接続・操作すること

■地球惑星科学分野での研究・サーバ管理に必須

✓個人用のノート PC から、学内の計算サーバに
アクセスし、数値シミュレーションを実行

✓学内の計算機に学外の天文台の観測データを取得

✓Web サーバにアクセスし、Web ページを編集

SSH と SFTP

■リモートホストの操作には SSH、リモートアクセスを用いたファイル転送には SFTP の使用を推奨

■コマンドラインで $ ssh 〈アカウント名〉@〈リモートホスト名〉と打鍵し、リモートホストにログイン

✓下の例はパスワードでログインしている

```
hoge@local: ~$ ssh hero@remote
hero@remote's password:       (パスワード打鍵)

hero@remote: ~$ ■             (リモートログイン完了)
```

✓SFTP も SSH と同様の方法でリモートアクセスできる

リモートアクセスに関する危険性

■リモートアクセスそのものに関する危険性
- ✓インターネットの経路上で盗聴される (パケット盗聴)
- ✓インターネットの経路上でデータを改竄される
- ✓第三者によるなりすまし

■リモートアクセスする計算機に関する危険性
- ✓セキュリティホールを使って外部から侵入される

■リモートアクセスを利用する際は、ネットワークセキュリティに気を配る必要がある
- ✓SSH や SFTP はパケット盗聴やなりすましを防げる (後述)

セキュリティの三要素 (CIA)

■機密性 (Confidentiality)

- ✓許可した人のみが情報に触れることができる
- ✓侵害例：個人情報流出

■完全性 (Integrity)

- ✓情報が本来想定した状態から改竄されておらず、信頼に足る状態である
- ✓侵害例：Web サイトの改竄

■可用性 (Availability)

- ✓情報にアクセスできる人は、いつでもその情報にアクセスできる
- ✓侵害例：DoS/DDoS 攻撃

セキュリティの考え方

■何を守るか

✓Web サーバなら、設定内容 (機密性・完全性)、稼働状態 (可用性)、公開情報 (完全性)など

■何から守るか

✓Web サーバなら、内部侵入、サービス妨害、公開情報の改竄など

■どう守るか

✓Web サーバなら、公開鍵認証 (後述)、ハードディスク冗長化、SQL インジェクション対策など

ファイル転送のセキュリティ

◆リモートアクセスを用いたファイル転送の場合 …

■何を守るか

✓ファイルの中身 (機密性・完全性)

■何から守るか

✓ファイル中身の盗聴、改竄

✓通信相手のなりすまし

■どう守るか

✓暗号化を用いて内容を秘匿

✓電子署名を用いて改竄を検知

✓認証を導入してなりすまし防止

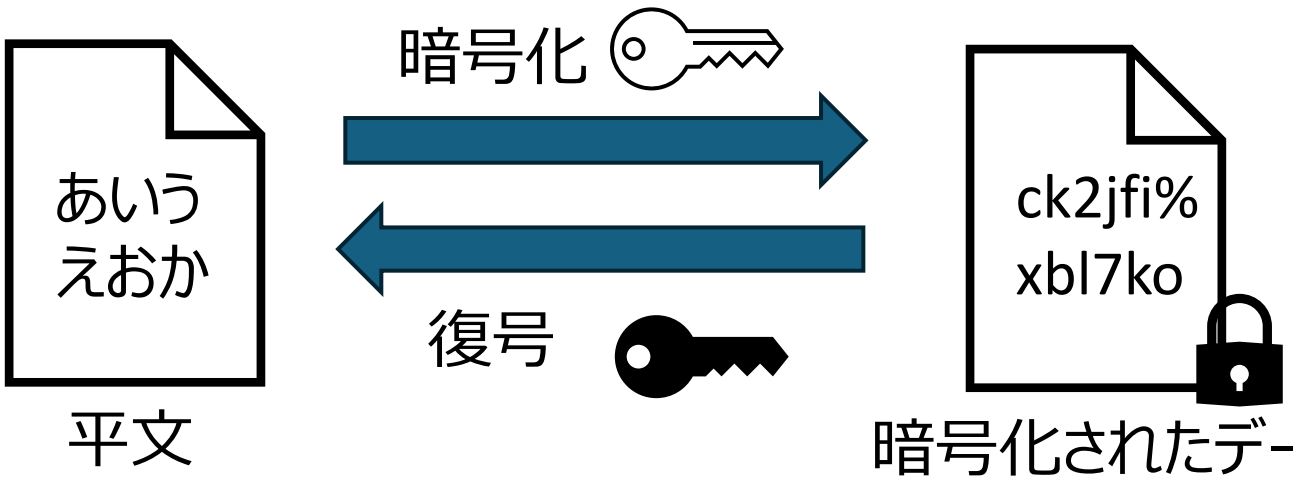
暗号化と復号

■情報通信の機密性を守るしくみ：暗号化技術

✓平文 (ひらぶん) … 誰でも読める状態の情報

✓暗号化 … 平文を部外者が読めない状態にすること

✓復号 … 暗号化された情報を元に戻すこと



■暗号化と復号には暗号アルゴリズムと鍵が必要

✓鍵の例：シーザー暗号における、ずらす文字数

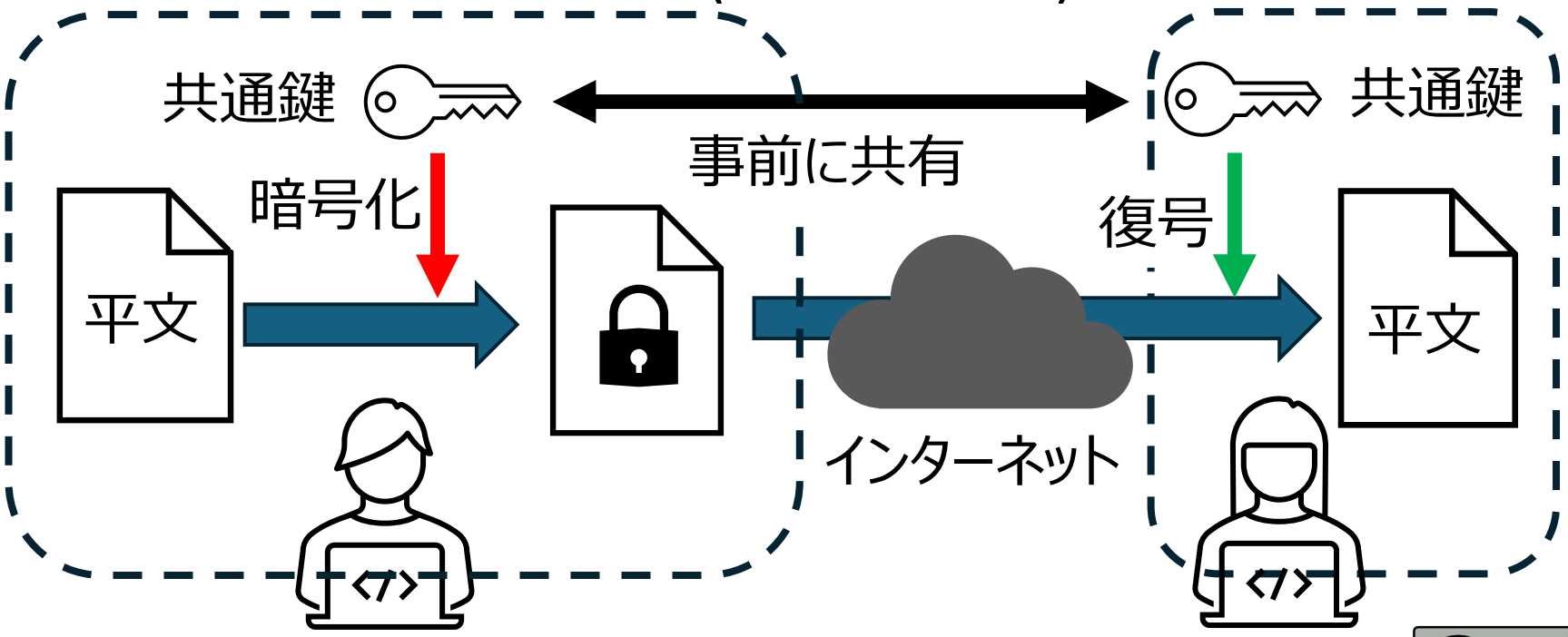
共通鍵暗号による暗号化

■暗号化と復号に同じ鍵を使う

✓比較的高速

✓共通鍵の配送方法が問題 (= 鍵配送問題)

➡ DH鍵共有など (詳細は割愛)

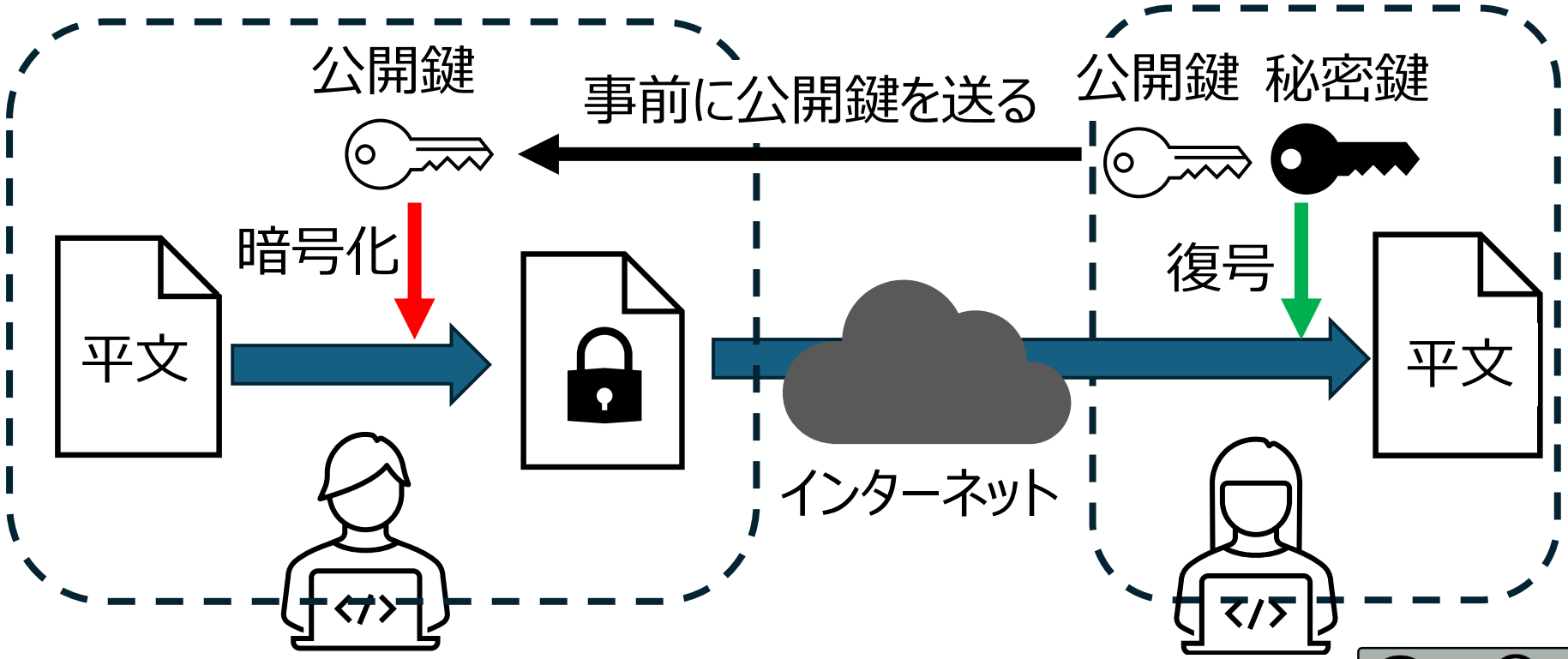


公開鍵暗号による暗号化

■暗号化と復号で異なる鍵を使う

✓『公開鍵』、『秘密鍵』のキーペア

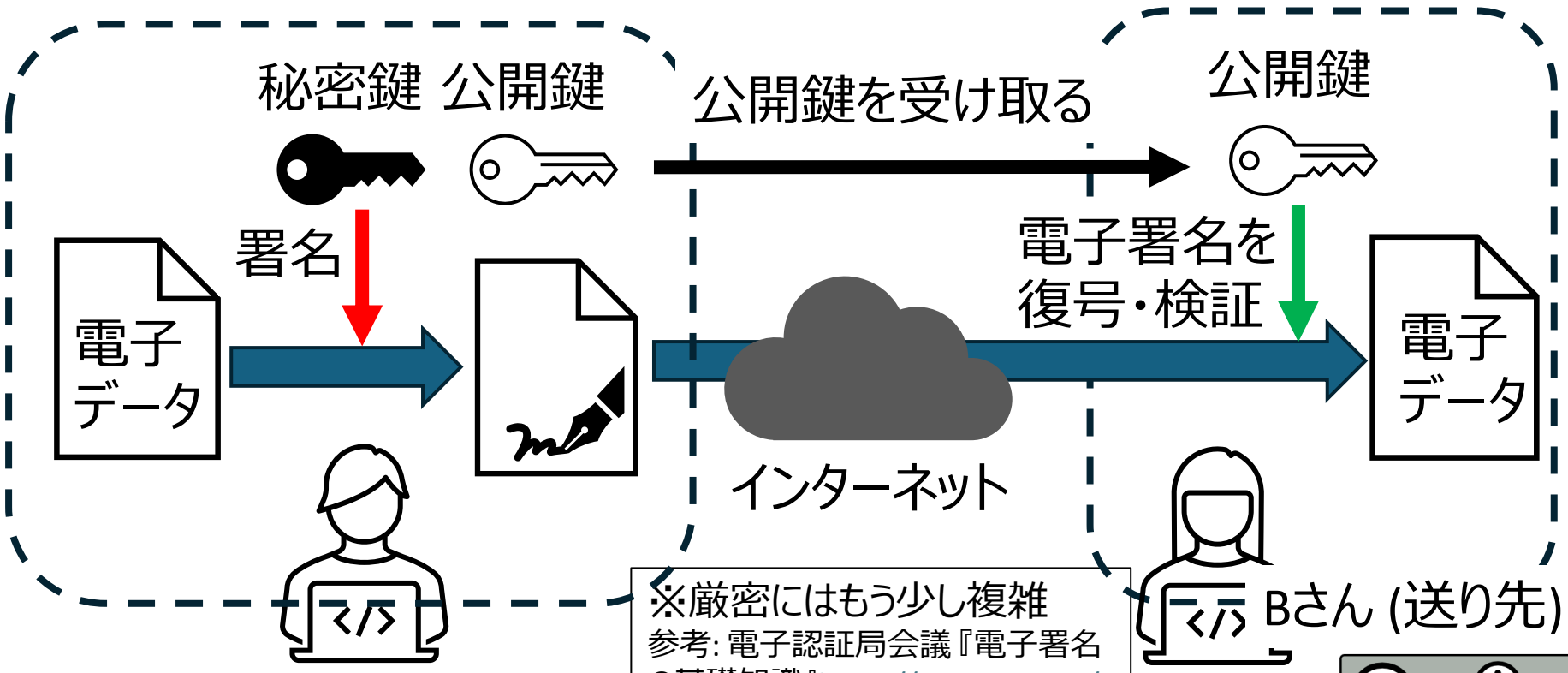
✓片方の鍵で暗号化➡もう片方の鍵でのみ復号可能



電子署名

■電子データの作成者を付与し、改竄されていない (完全性) ことを保証するための技術

✓電子データに対応する署名を暗号で作成・検証

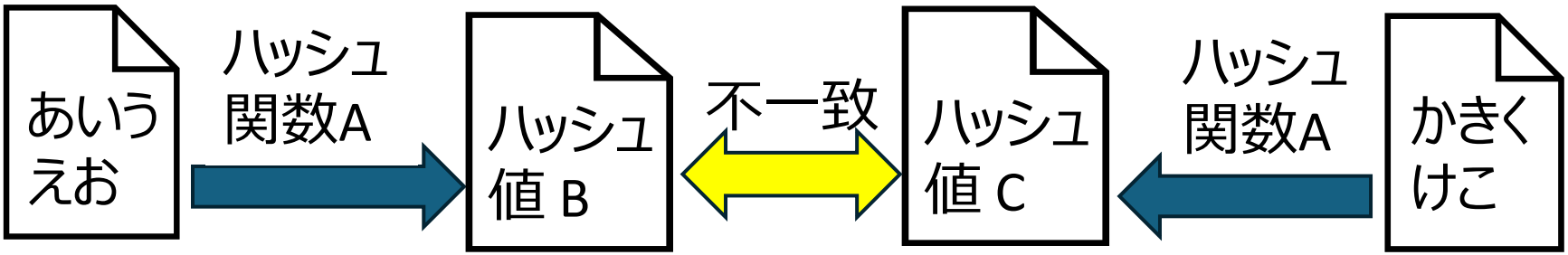


※厳密にはもう少し複雑
参考: 電子認証局会議『電子署名の基礎知識』https://www.c-a-c.jp/about/knowledge.html

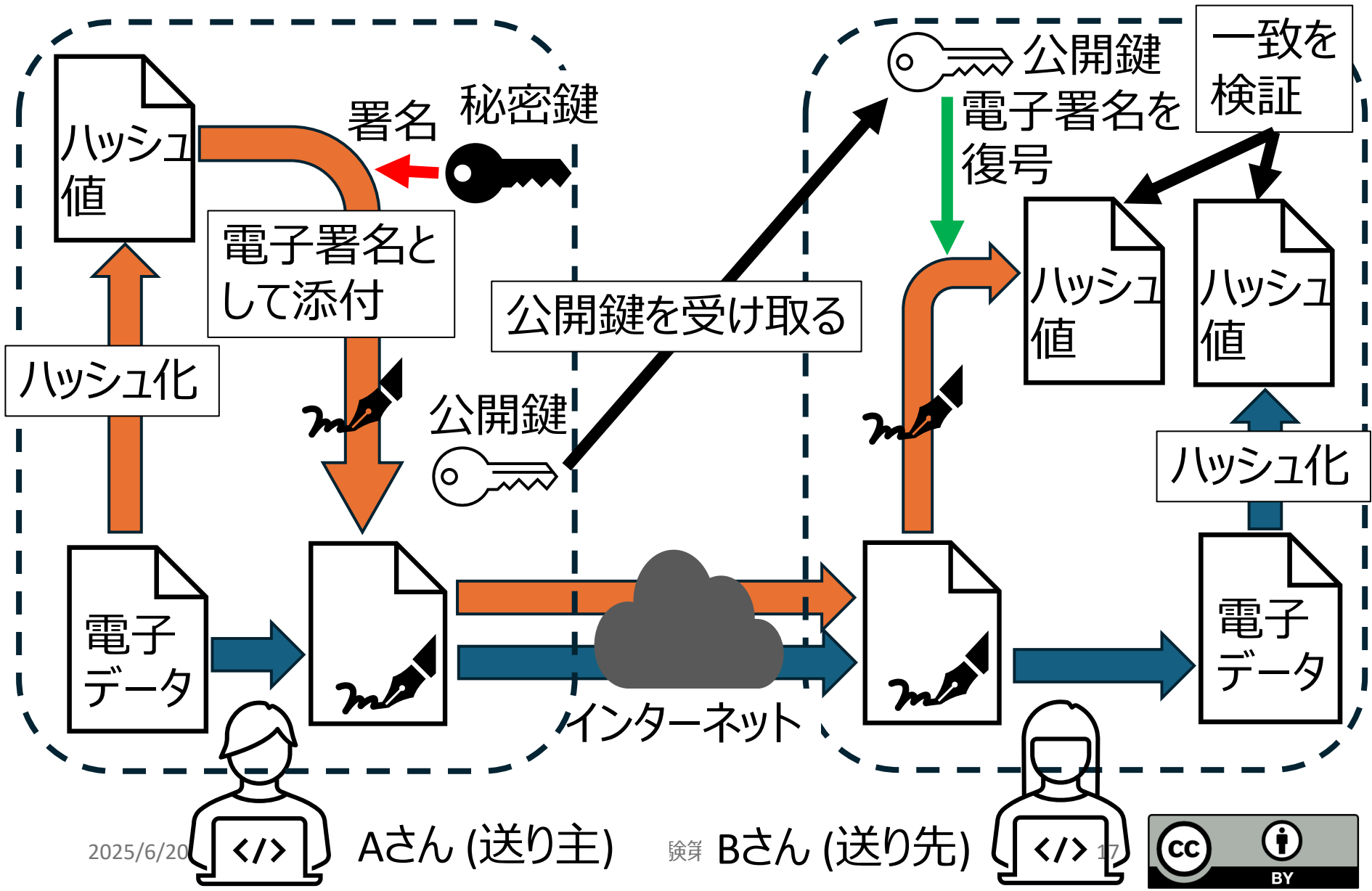
ハッシュ

■あるデータに対応する値を求めるための手法

- ✓同じデータから同じハッシュ関数を使って求めたハッシュ値は常に一致
- ✓異なるデータから求めたハッシュ値は原則異なる
  ➡改竄検出に有効
- ✓ハッシュ値から元の値は求められない
- ✓ハッシュ関数の例：SHA2, SHA3



電子署名 (詳解図)


ハッシュ値
署名
秘密鍵
電子署名として添付
ハッシュ化
公開鍵を受け取る
公開鍵
電子データ
インターネット
公開鍵
電子署名を復号
一致を検証
ハッシュ値
ハッシュ値
ハッシュ化
電子データ
Aさん (送り主)
Bさん (送り先)

公開鍵認証

■認証 … 相手計算機を識別すること

✓リモートアクセスを用いたファイル転送の際は、転送先から認証が求められる

✓パスワード認証 (第 2 回) や公開鍵認証など

■公開鍵認証

① クライアント側で秘密鍵・公開鍵を生成し、サーバに公開鍵を共有

② サーバ・クライアントでセッション ID を生成

③ クライアント側でセッション ID などに秘密鍵で署名して、サーバ側で公開鍵で署名を復号して認証

✓一時的な署名と公開鍵のみ送付 = 比較的安全

リモートアクセスのプロトコル①

■リモートアクセスは SSH (Secure SHell) が推奨

① 公開鍵を使い、リモートホストを認証

② DH 鍵共有した共通鍵でセッションを暗号化

③ パスワードや公開鍵認証などでクライアントを認証

■ファイル転送は SFTP (SSH FTP) が推奨

✓SSH プロトコルを用いたファイル転送

✓電子署名はクライアントが別で行う必要がある

■かつては暗号化されない Telnet や FTP を用いた

✓現在も、サーバのポート確認に Telnet を、匿名のデータ転送に FTP を用いることも

公開鍵認証基盤 (PKI)

■公開鍵を「信頼できる第三者」に電子署名してもらう方法

✓公開鍵をすり替える中間者攻撃などの対策

■公開鍵証明書認証局 (CA) に自分の公開鍵の電子証明書発行を依頼する

■サーバの電子証明書を特にサーバ証明書と言う

✓PKI を導入しているサーバの管理者は、サーバ証明書の発行・更新など、煩雑な管理が必要

リモートアクセスのプロトコル②

■SSL/TLS を用いる方法もある

① リモートホストのサーバ証明書を PKI で検証

② DH 鍵共有した共通鍵でセッションを暗号化

③ クライアント側の認証はオプショナル

■FTPS … SSL/TLS を用いたファイル転送

✓電子署名はクライアントが別で行う必要がある

■Web ページに個人情報を入力するときは、
信頼できるサーバ証明書を使った
HTTPS (HTTP Secure) 接続であることを確認しよう

SSH と SSL/TLS 特徴と用途

■TCP/IP の階層が違う

- ✓SSH はアプリケーション層、SSL/TLS はトランスポート層
- ✓SSL/TLS は既存のアプリケーションの暗号化を図る

■サーバの認証方法が違う

- ✓SSH は一度アクセスしたリモートホストの公開鍵を信用
  ➡小規模の個人・グループが使うサーバに親和性
  - ➢PKI 的なしくみを導入することもできるがオプション
- ✓SSL/TLS はサーバ証明書を用いて、第三者の機関を信用して認証
  ➡世界中の誰とでも、安全に初めて通信可能
  ➡Web サーバに高い親和性

計算機管理のセキュリティ

■何を守るか

✓計算機内の情報 (機密性・完全性)

■何から守るか

✓内部侵入による情報の漏洩・改竄

■どう守るか

✓ポート管理

✓アクセス制限

✓セキュリティホールをなくす

ポート管理

- ■セキュリティのため、使わないポートを閉じる
  - ✓例：Telnet を使わないなら 23番ポートは閉じる
- ■ポート … インターネットの通信送受信口
  - ✓用途ごとに特定のポート番号が推奨されている
    - ➢SSH: 22番, Telnet: 23番 など
- ■デーモン (daemon)
  - ✓Unix 系 OS のバックグラウンドに常駐するプログラム
  - ✓特定サービスのデーモンを止めれば、実質的に そのサービスが使うポートは閉じられると言える
  - ✓元々ギリシャ神話の精霊の意味 (らしい)

デーモンの管理

■デーモンを停止

✓systemctl コマンドを使う

➢# systemctl stop (デーモン名)

➢計算機を再起動するとデーモンも復帰する

■デーモンをアンインストール

✓不要なサービスを提供する
デーモンはインストールしない

daemon イメージ図
drawn by tyama

アクセス制限

■セキュリティのため、不要なアクセスを拒否

■TCP wrapper

- ✓外部からのアクセス制御を行うプログラム
- ✓特定の IP アドレス、ホスト名に対して、特定のサービスを許可・拒否する
- ✓/etc/hosts.allow に許可する組を書く
  - ➢(例) sshd: ep.sci.hokudai.ac.jp
  - ➢(許可するサービス): (許可する IP, ホスト名)
- ✓/etc/hosts.deny に拒否する組を書く
  - ➢(例) ALL: ALL
- ✓hosts.allow の内容が優先される

セキュリティホールへの対応

■最新版のソフトウェアにアップデートする

✓Debian なら apt update で最新のパッケージ情報を取得し、apt upgrade でダウンロード・インストール

■脆弱性の発見から公表まで

① IPA に脆弱性を届け出

② IPA で内容確認の上、JPCERT/CC に通知

③ JPCERT/CC が開発元に対応を働きかける

④ JPCERT/CC のホームページなどで公表

■発見した未対応の脆弱性 (ゼロデイ脆弱性) は自分で公表せず、IPA に届け出る

まとめ

■リモートアクセス

■セキュリティの考え方

- ✓機密性・完全性・可用性
- ✓何を・何から・どう守るか

■ファイル転送のセキュリティ

- ✓暗号化・電子署名・認証
- ✓SSH, SFTP, SSL/TLS

■計算機管理のセキュリティ

- ✓ポート管理・アクセス制限・ソフトウェアアップデート

参考文献

- みやもとくにお & 大久保 隆夫, イラスト図解式 この一冊で全部わかるセキュリティの基本, SBクリエイティブ, 2022年1月11日
- 猪俣 敦夫 & 井上 克郎, サイバーセキュリティ入門: 私たちを取り巻く光と闇, 共立出版, 2016年2月10日
- IPA,情報セキュリティ早期警戒パートナーシップガイドライン概要 日本語版, https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/partnership_guideline_overview_jp.pdf
- 電子認証局会議, 電子署名の基礎知識, https://www.c-a-c.jp/about/knowledge.html
- RFC, The Secure Shell (SSH) Authentication Protocol, https://www.rfc-editor.org/rfc/rfc4252
- RFC, HTTP Semantics, https://www.rfc-editor.org/info/rfc9110

➢(すべて最終閲覧 2025/6/16)