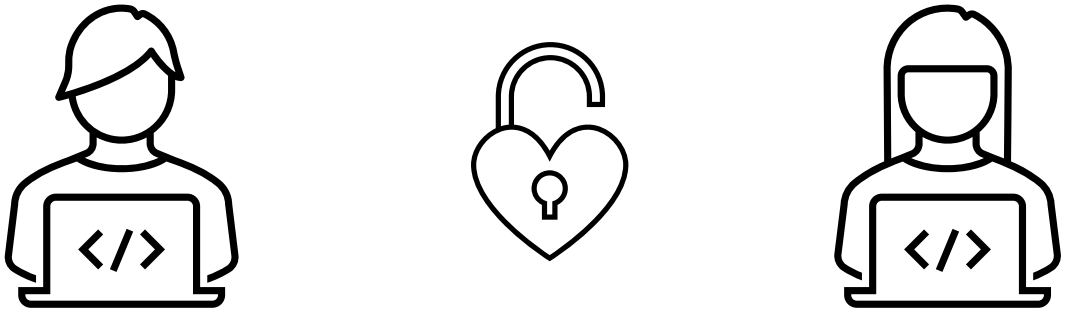
リモートアクセス・ネットワークセキュリティ

情報実験 第 8 回 (2026/06/19)



北海道大学　理学院　宇宙理学専攻
博士課程 1 年　吉川 颯真

本日の情報実習

■リモートアクセスとは？

■ネットワークセキュリティの考え方

- ✓計算機が通信を行う上でのセキュリティ
  - ➢暗号技術 (暗号化・電子署名・ハッシュ・認証)
  - ➢リモートアクセスで用いられるプロトコル
- ✓計算機のシステムのセキュリティ
  - ➢ポート管理・アクセス管理・セキュリティホール

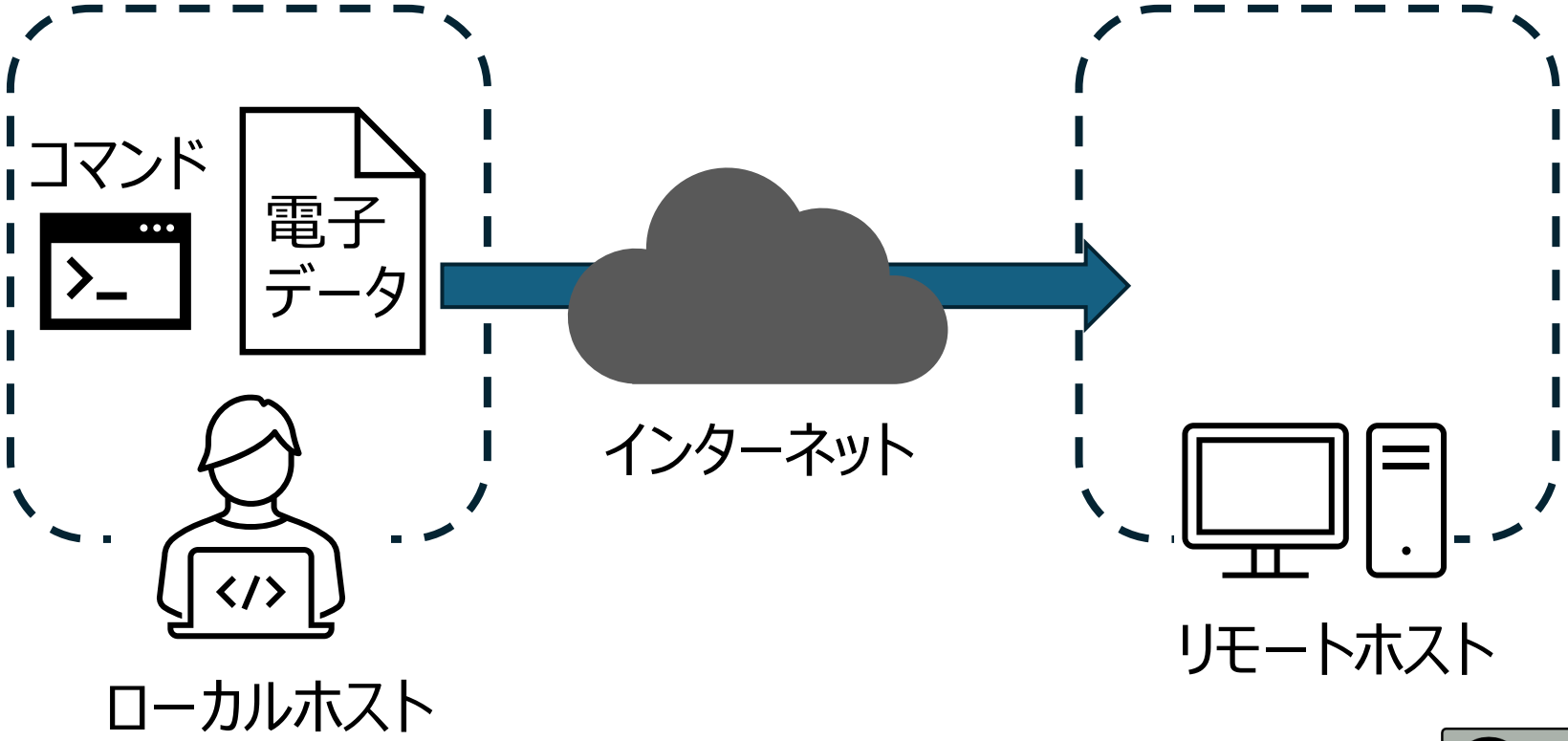
本日の情報実習

- ■リモートアクセスとは？
- ■ネットワークセキュリティの考え方
  - ✓計算機が通信を行う上でのセキュリティ
    - ➢暗号技術 (暗号化・電子署名・ハッシュ・認証)
    - ➢リモートアクセスで用いられるプロトコル
  - ✓計算機のシステムのセキュリティ
    - ➢ポート管理・アクセス管理・セキュリティホール

リモートアクセスとは

■ 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



リモートアクセスの必要性

■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・学外の計算サーバにアクセスし、数値計算を実行
- ✓なよろ天文台の観測データを学内の計算機に転送
- ✓Web サーバにアクセスし、Web ページを編集

リモートアクセスの危険性

■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

■リモートアクセスを行う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

本日の情報実習

- ■リモートアクセスとは？
- ■ネットワークセキュリティの考え方
  - ✓計算機が通信を行う上でのセキュリティ
    - ➢暗号技術 (暗号化・電子署名・ハッシュ・認証)
    - ➢リモートアクセスで用いられるプロトコル
  - ✓計算機のシステムのセキュリティ
    - ➢ポート管理・アクセス管理・セキュリティホール

ネットワークセキュリティの考え方

■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

■何を・何から・どのように守るか

計算機の通信のセキュリティ

◆リモートアクセスを用いた通信の場合 …

■何を守るか

✓ファイルの中身 (機密性・完全性)

■何から守るか

✓ファイルの中身の盗聴、改竄

✓通信相手のなりすまし

■どう守るか

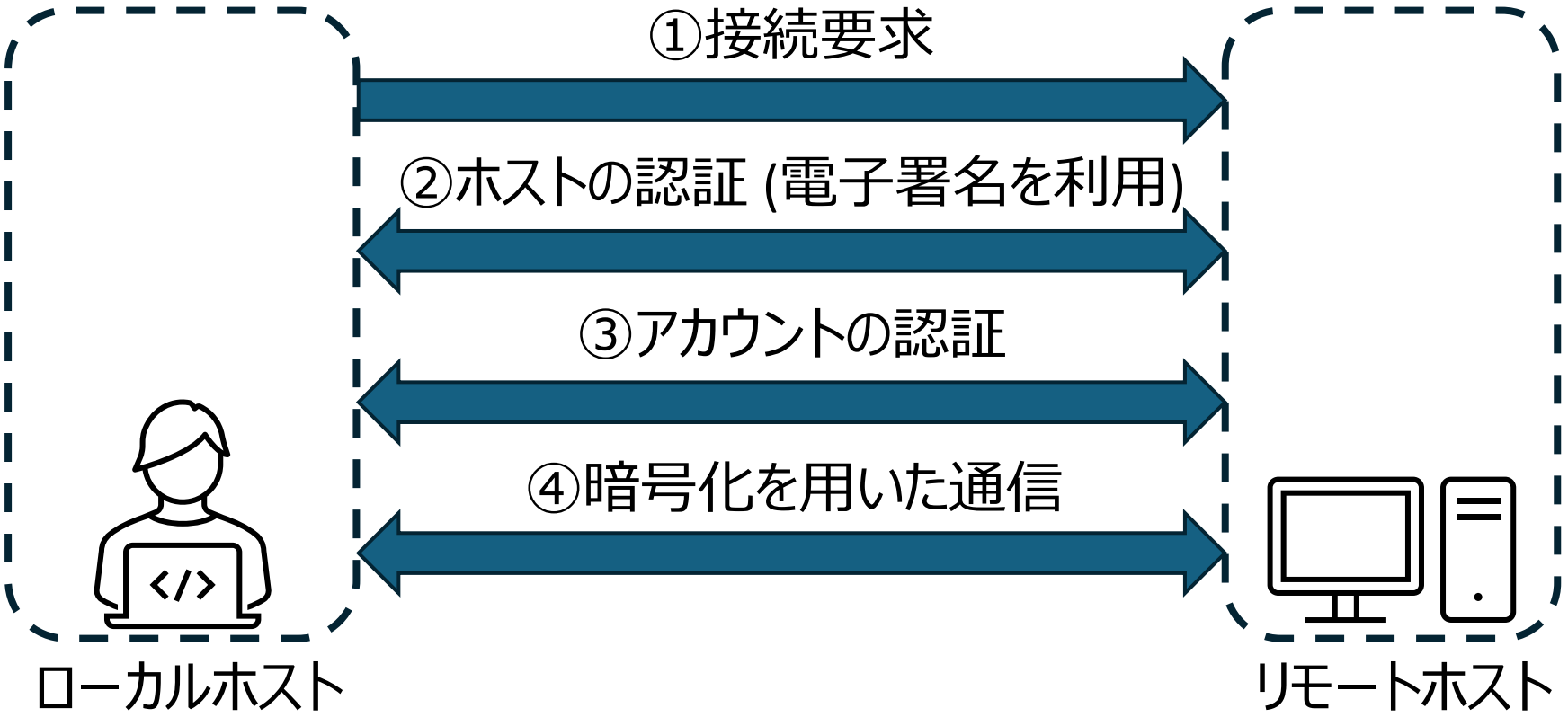
✓暗号化を用いて内容を秘匿

✓電子署名を用いて改竄を検知

✓信頼できる認証方式を用いてなりすまし防止

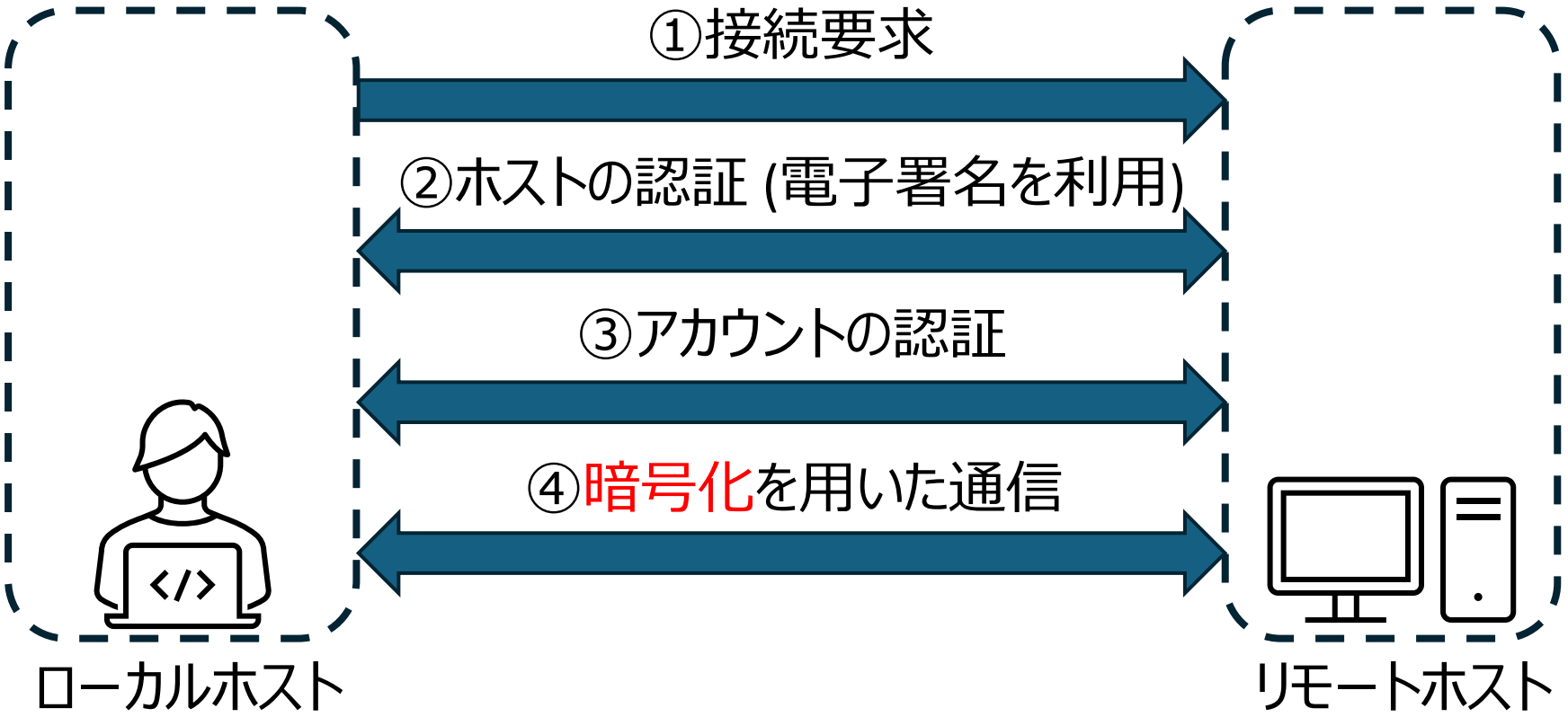
リモートアクセスの概念図

■近年のリモートアクセスに用いられるプロトコルは
暗号化、電子署名、認証技術を組み合わせて
セキュリティを維持している



リモートアクセスの概念図

■近年のリモートアクセスに用いられるプロトコルは
暗号化、電子署名、認証技術を組み合わせて
セキュリティを維持している



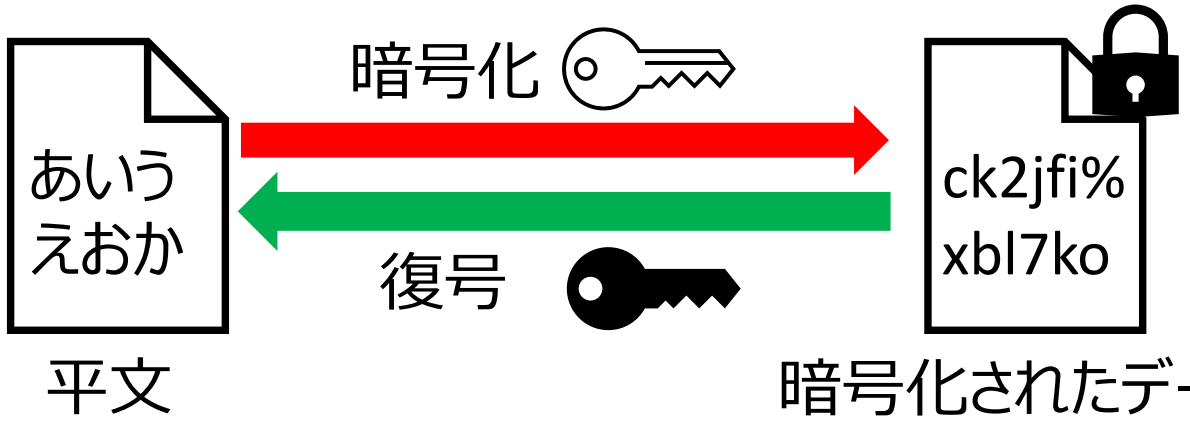
暗号化と復号

■情報通信の機密性を守るしくみ：暗号化技術

✓暗号化 … 平文を部外者が読めない状態にすること

➢平文 (ひらぶん) … 誰でも読める状態の情報

✓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

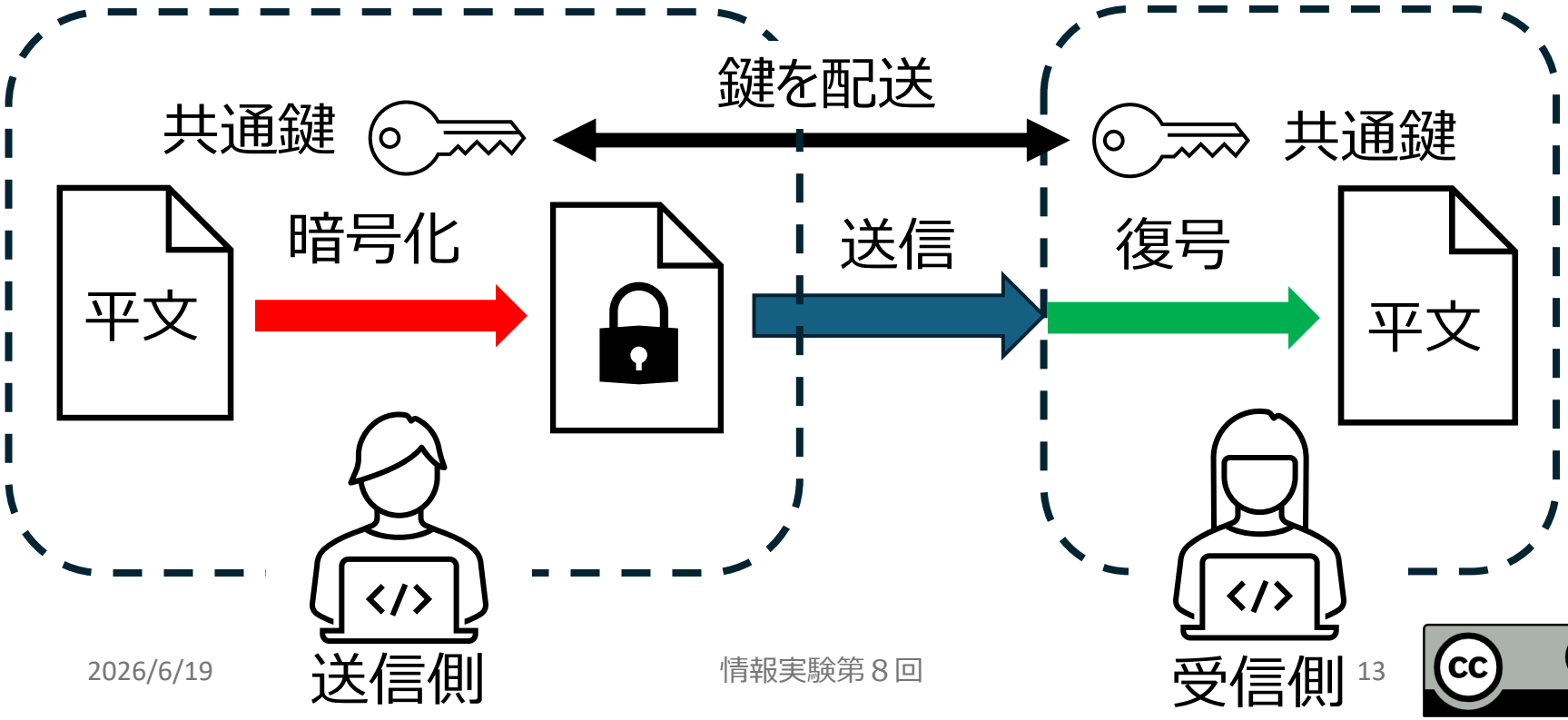
✓鍵の例：シーザー暗号における、ずらす文字数

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

✓共通鍵を秘密裏に配送するのが難しい

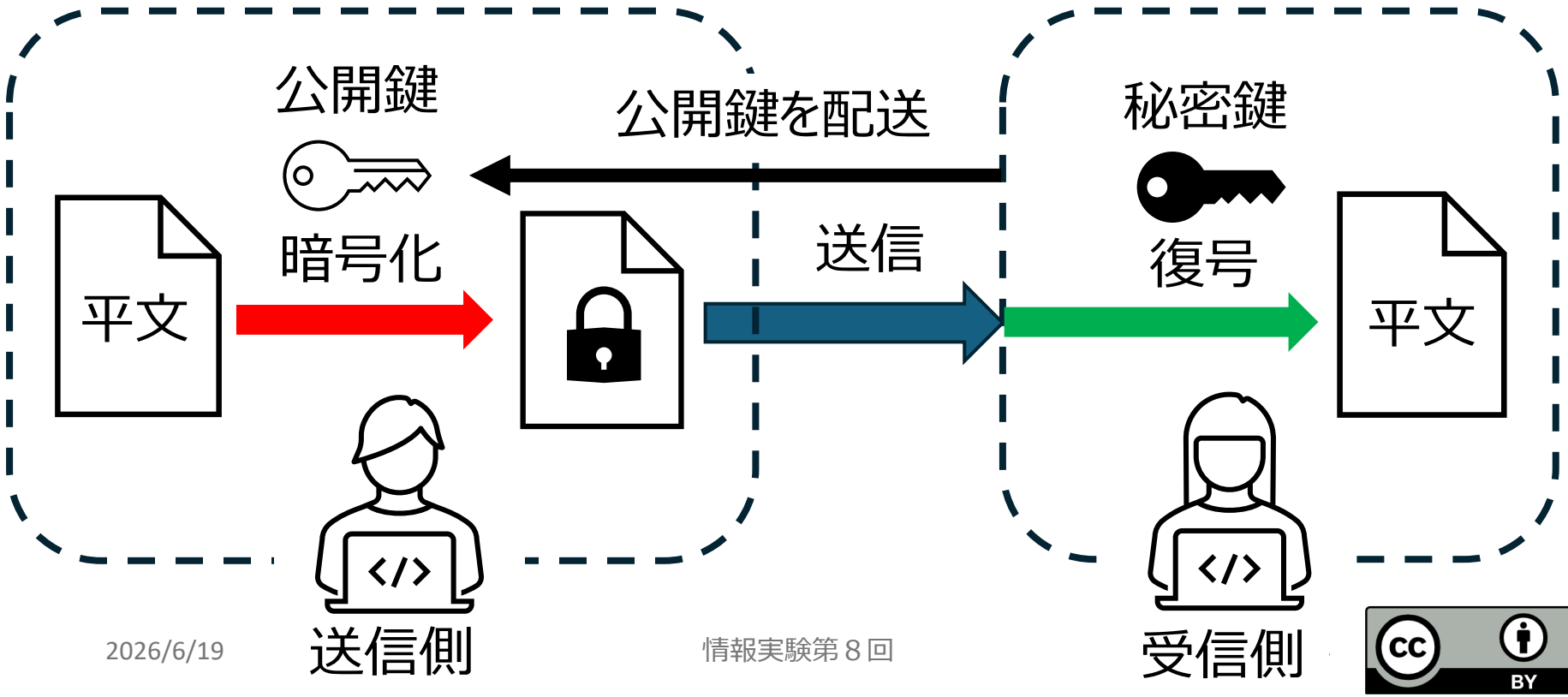


公開鍵による暗号化

■暗号化と復号で異なる鍵を使う

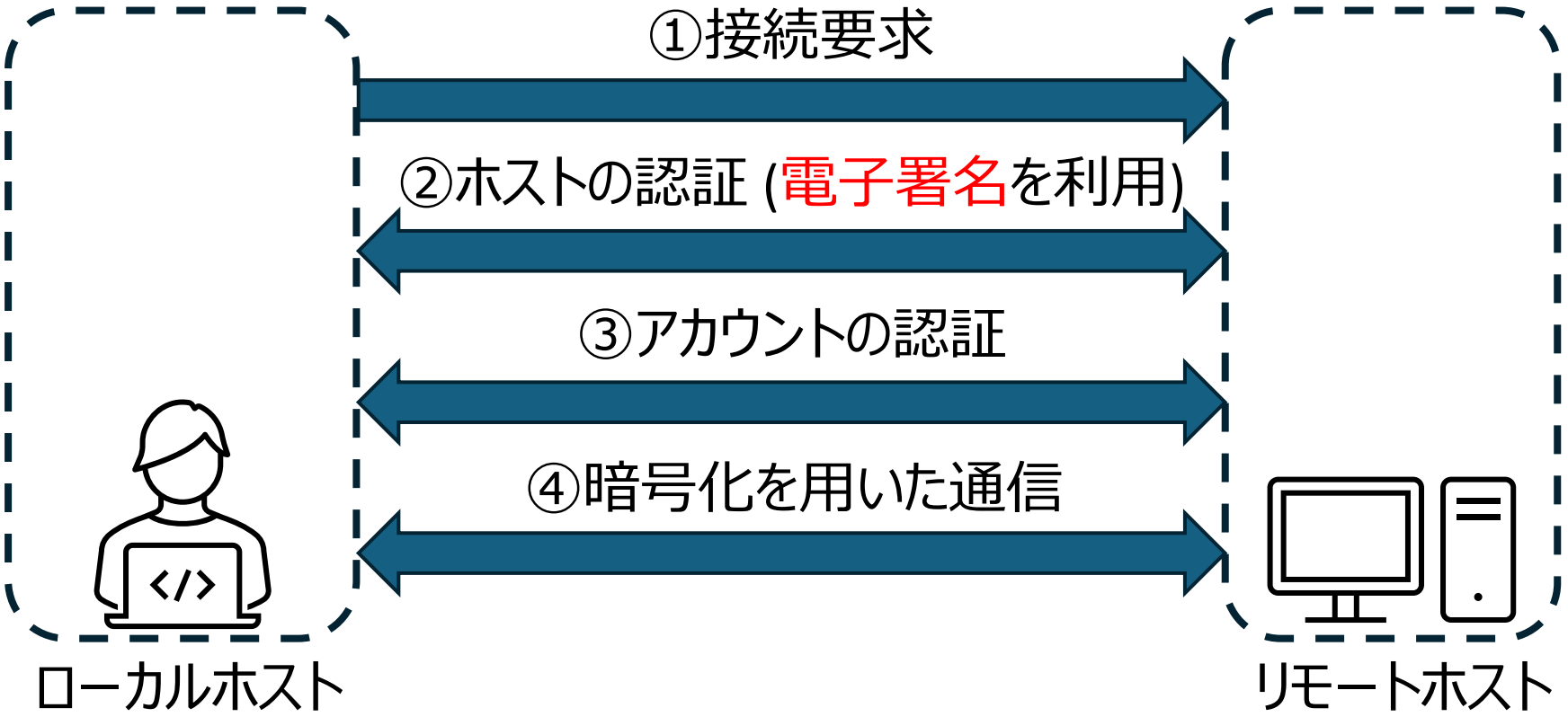
✓『公開鍵』、『秘密鍵』のキーペア

✓公開鍵で暗号化し、秘密鍵でのみ復号できる



リモートアクセスの概念図

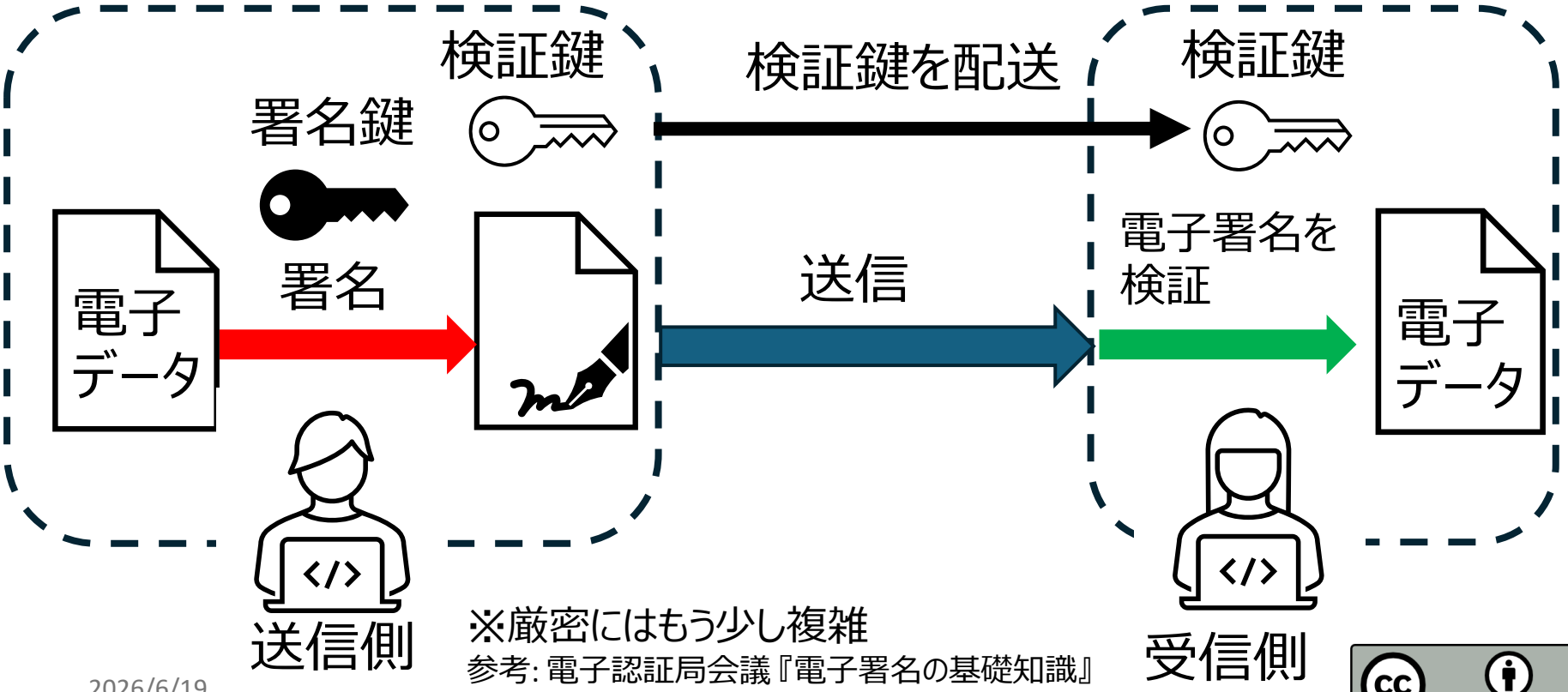
■近年のリモートアクセスに用いられるプロトコルは
暗号化、電子署名、認証を組み合わせて
セキュリティを維持している



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

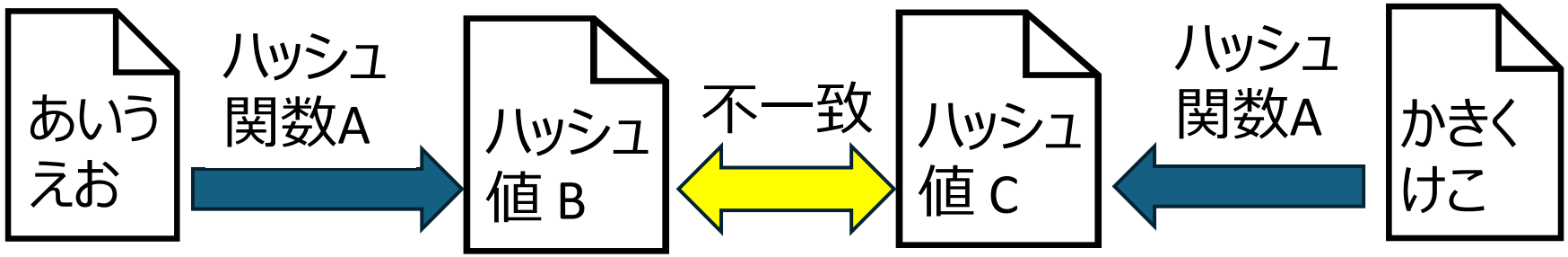
■あるデータに対応する値を求めるための手法

✓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

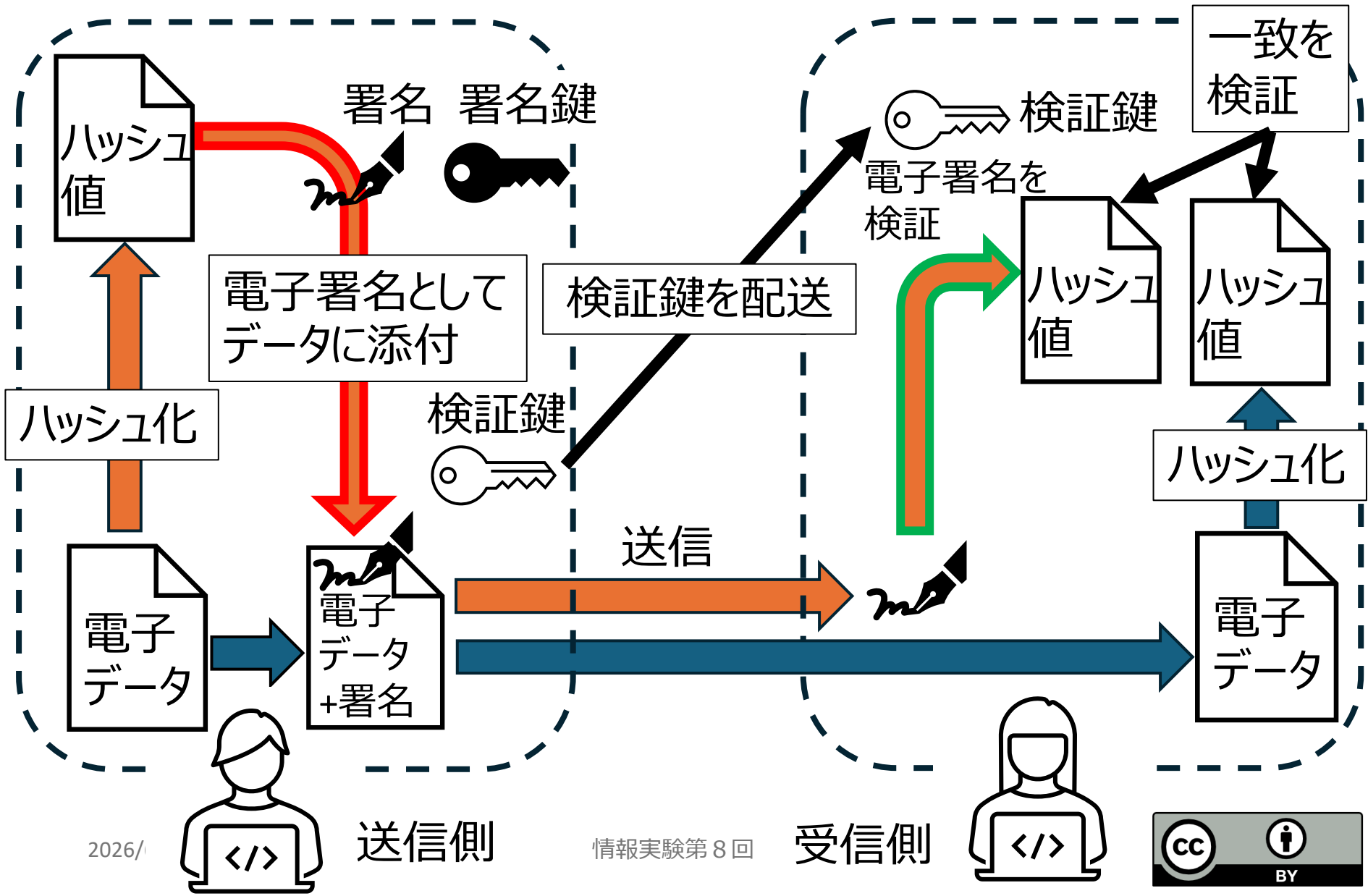
✓異なるデータから求めたハッシュ値は原則異なる
➡改竄検出に有効

✓ハッシュ値から元のデータは求められない

※ハッシュ関数の例: SHA2, SHA3

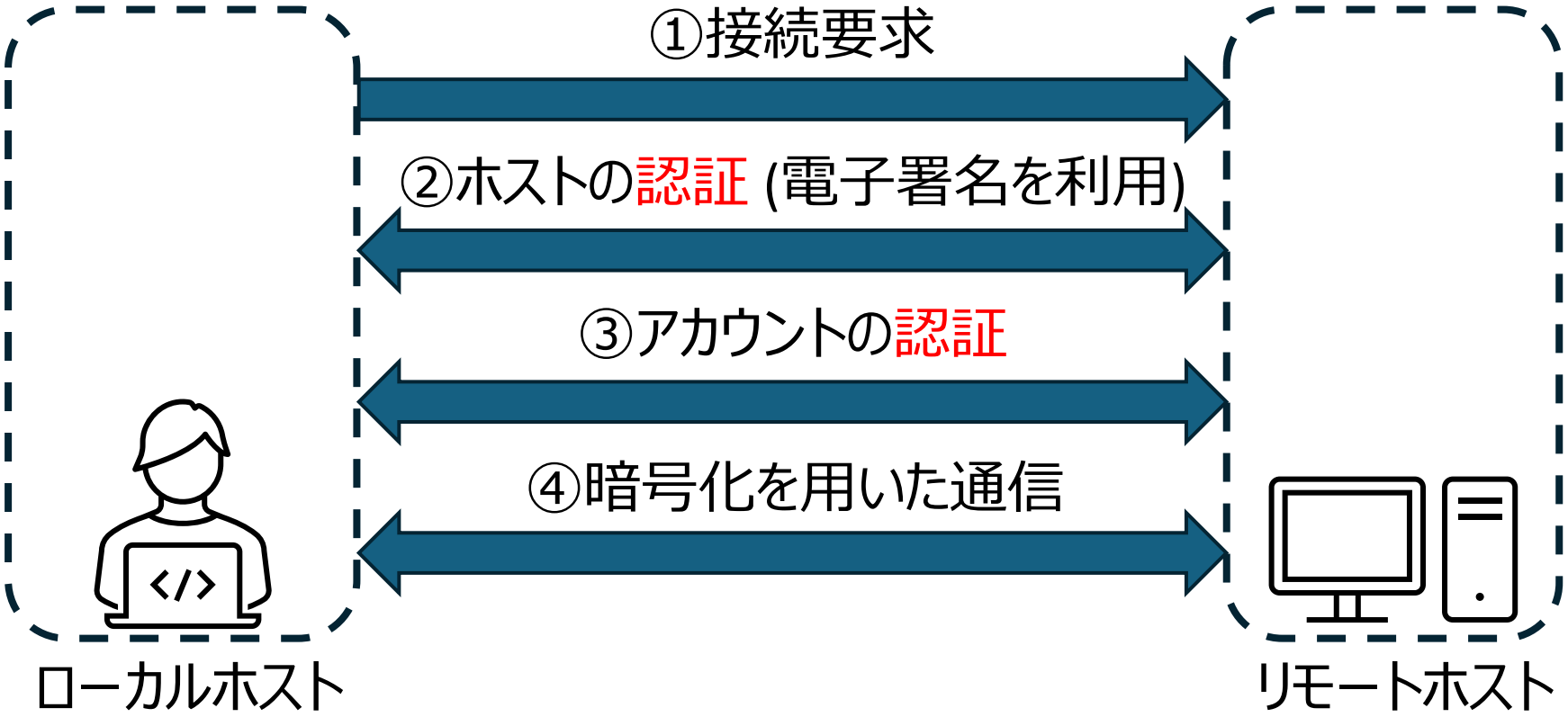


電子署名 (詳解図)


ハッシュ値
署名
署名鍵
電子署名として
データに添付
検証鍵を配送
検証鍵
検証鍵
電子署名を
検証
一致を
検証
ハッシュ値
ハッシュ値
ハッシュ化
ハッシュ化
電子
データ
電子
データ
+署名
送信
電子
データ
送信側
受信側

リモートアクセスの概念図

■近年のリモートアクセスに用いられるプロトコルは
暗号化、電子署名、認証を組み合わせて
セキュリティを維持している

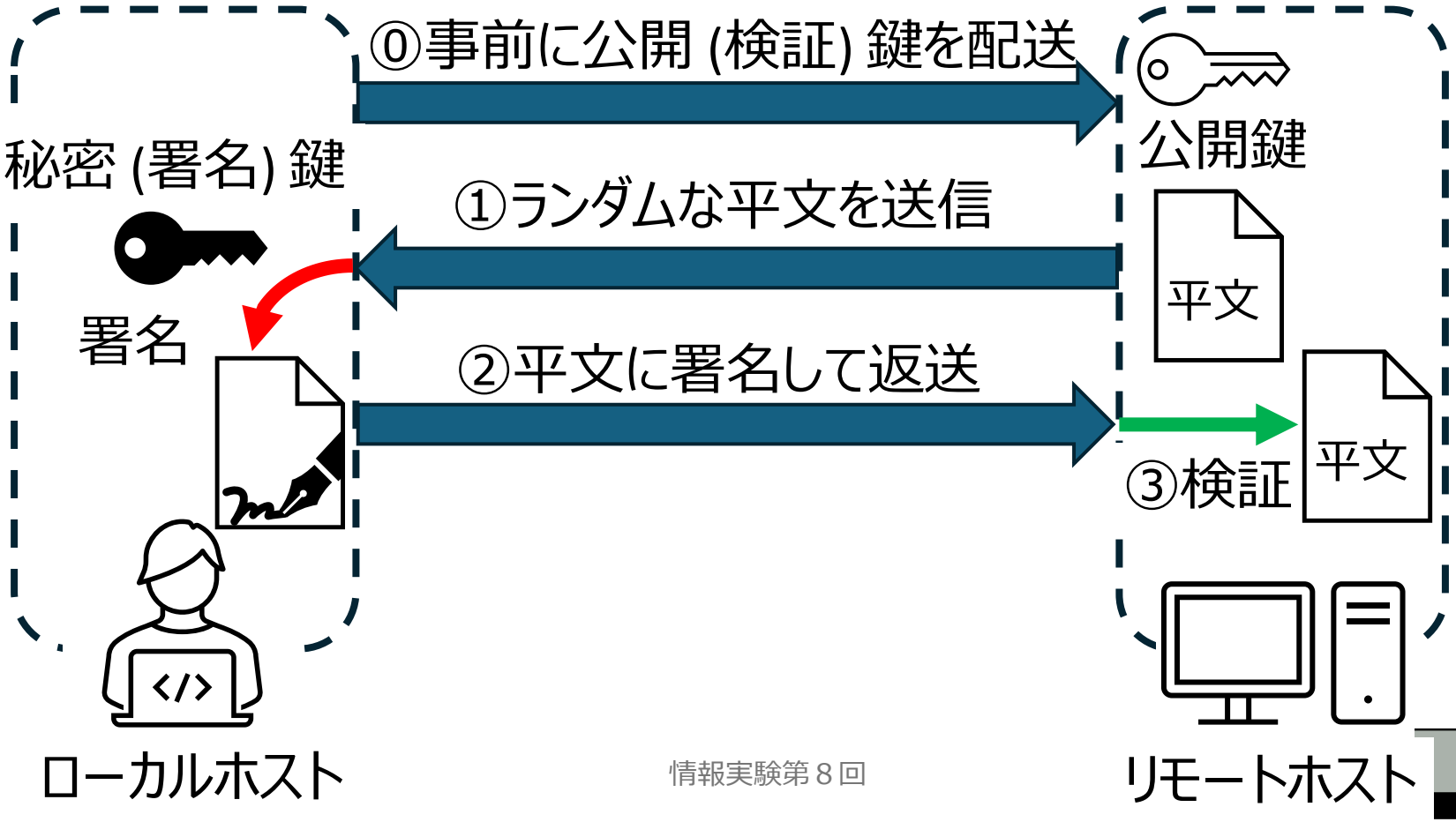


認証

■認証 …相手計算機を識別すること

✓パスワード認証 (第 2 回) や生体認証、公開鍵認証など

■公開鍵認証

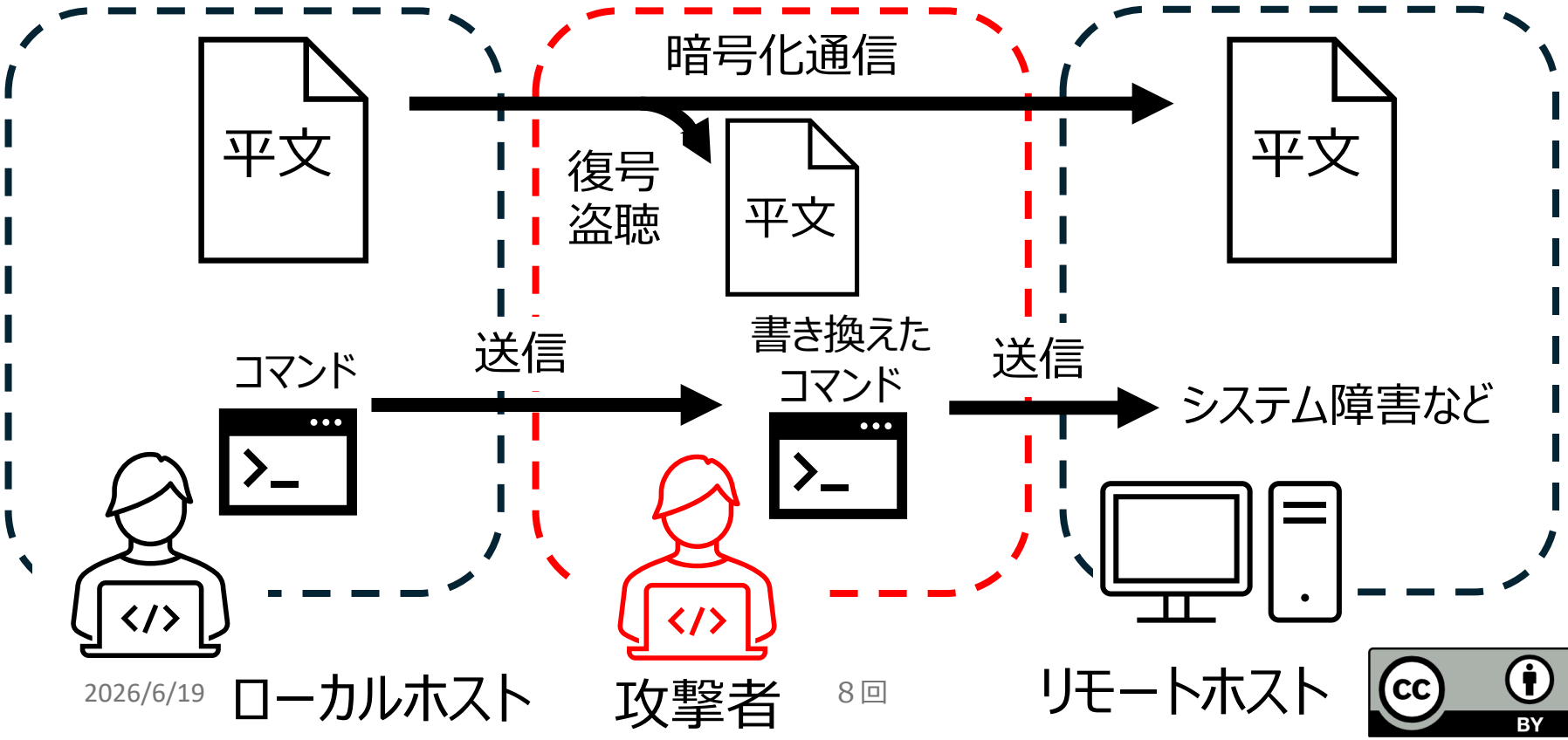


中間者攻撃

■通信経路の中間で通信傍受や改竄を行う攻撃

■暗号化の導入時に特に注意

✓暗号化通信・電子署名を行う前の鍵配送など

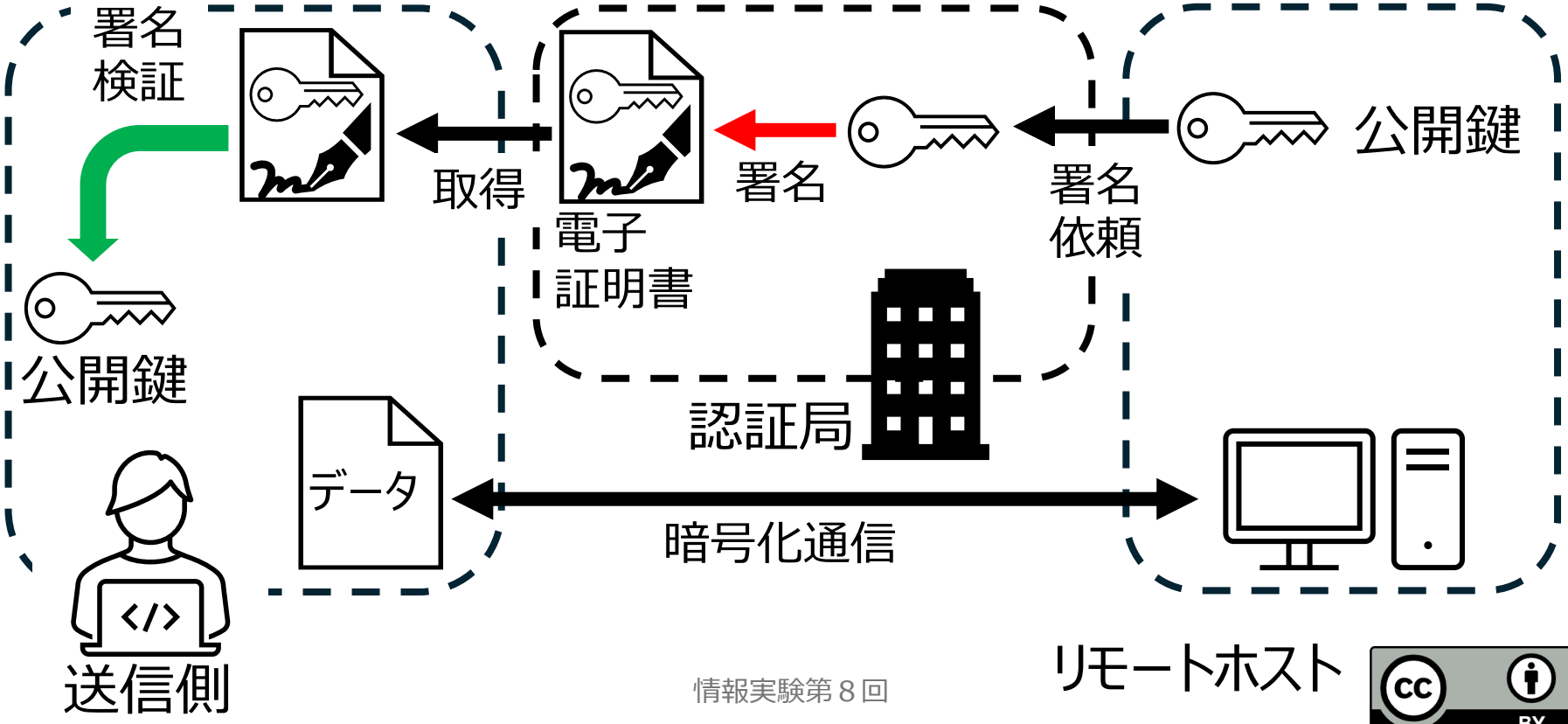


公開鍵認証基盤 (PKI)

■公開鍵を「信頼できる第三者」に電子署名してもらう方法

✓中間者攻撃の対策

■認証局に自分の公開鍵の電子証明書の作成を依頼



リモートアクセスに用いられるプロトコル

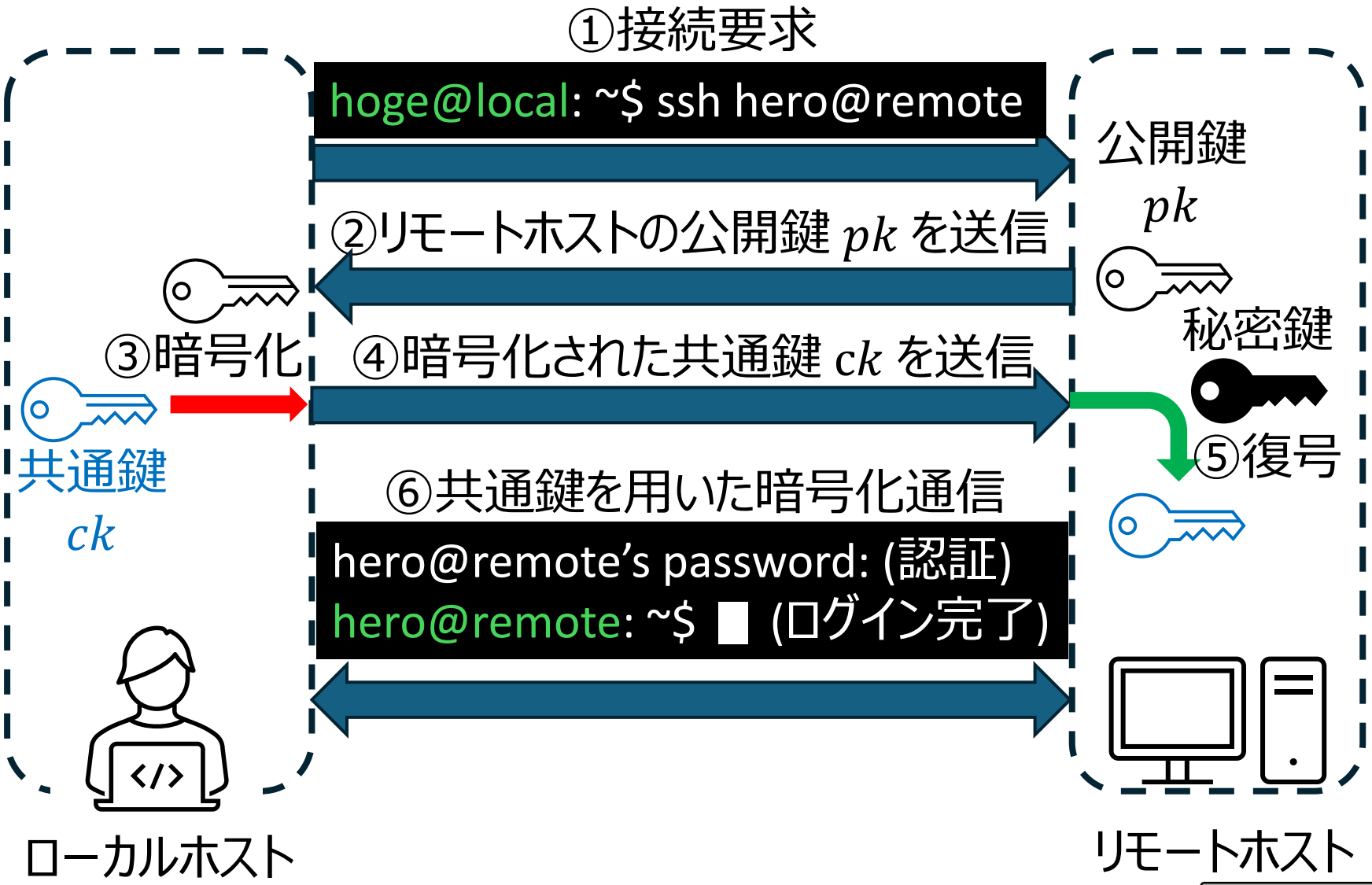
■リモートアクセスの基盤となるプロトコル

- ✓SSH (Secure SHell): リモートアクセスで推奨される
  - ➢リモートホスト環境提供からセキュリティ管理までを司る
- ✓SSL/TLS: インターネット通信を行う際に用いられる
  - ➢暗号化や鍵の共有などのセキュリティ管理を行う

■アプリケーション層のプロトコル

- ✓SFTP (SSH FTP): ファイル転送で推奨される
  - ➢SSH を用いたファイル転送
- ✓HTTPS (HyperText Transfer Protocol Secure)
  - ➢SSL/TLS で暗号化された Web ブラウザとサーバ間のデータ通信で推奨されている
  - ➢信頼できる電子証明書を使ったサイトに接続しよう

SSH を使ってログインするまで



本日の情報実習

- ■リモートアクセスとは？
- ■ネットワークセキュリティの考え方
  - ✓計算機が通信を行う上でのセキュリティ
    - ➢暗号技術 (暗号化・電子署名・ハッシュ・認証)
    - ➢リモートアクセスで用いられるプロトコル
  - ✓計算機のシステムのセキュリティ
    - ➢ポート管理・アクセス管理・セキュリティホール

計算機のシステム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

✓計算機内部への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

✓ポート … インターネットの通信送受信口

➢用途ごとに特定の番号が推奨されている
(SSH: 22番、HTTPS: 443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

アクセス制限

- 機密性を保つために、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
    - ➢(許可するサービス):␣(許可する IP, ホスト名)
    - ➢(例) sshd: ep.sci.hokudai.ac.jp
  - ✓/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 (第 7 回)

■発見した未対応の脆弱性は自分で公表せず、情報技術推進機構 (IPA) に届け出る

■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

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
- ■計算機が通信を行う上でのセキュリティ
  - ✓暗号化・電子署名・認証
  - ✓SSH, SFTP, SSL/TLS, HTTPS
- ■計算機管理のセキュリティ
  - ✓ポート管理・アクセス制限・セキュリティホール対応

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
- IPUSIRON, 暗号技術のすべて, 翔泳社, 2018年7月5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

(すべて最終閲覧日 2026年6月11日)