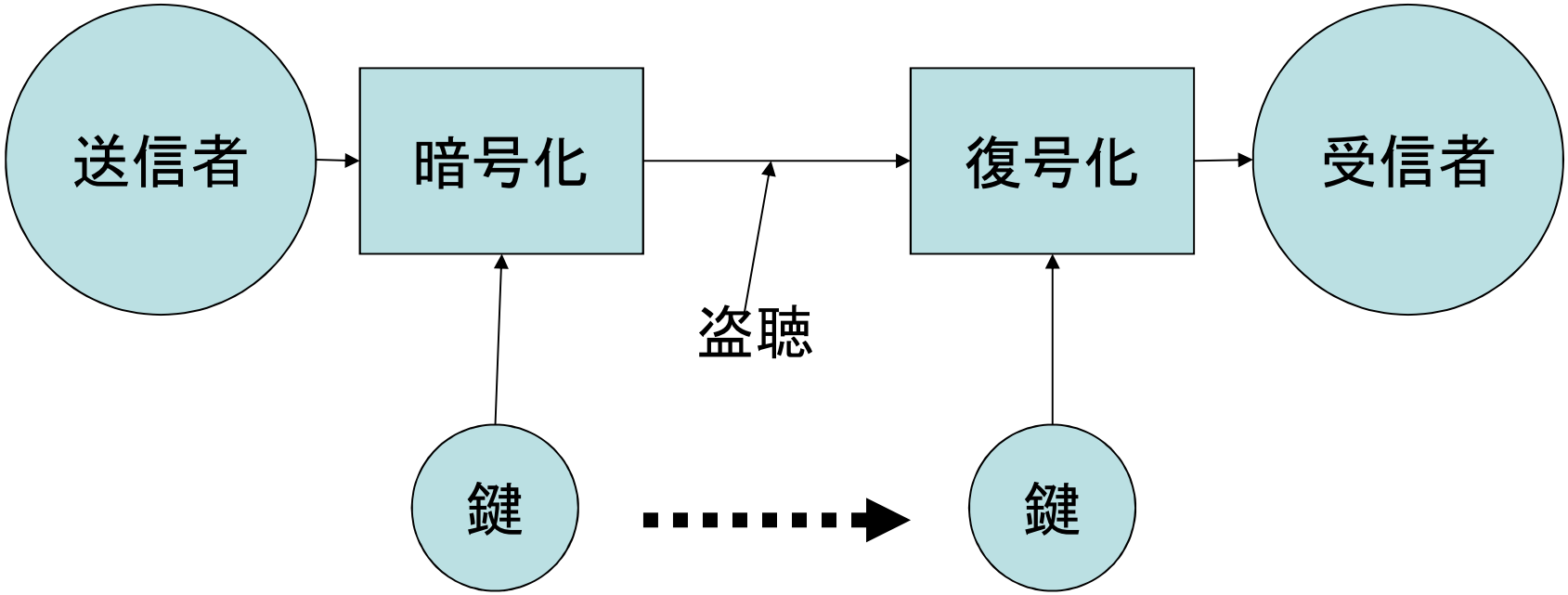
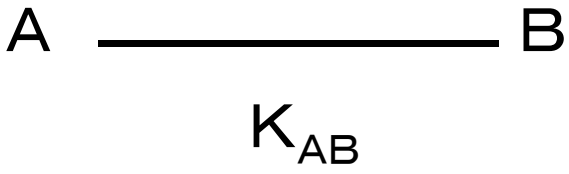
公開鍵暗号の概念とPKI

従来の暗号の問題点（1）



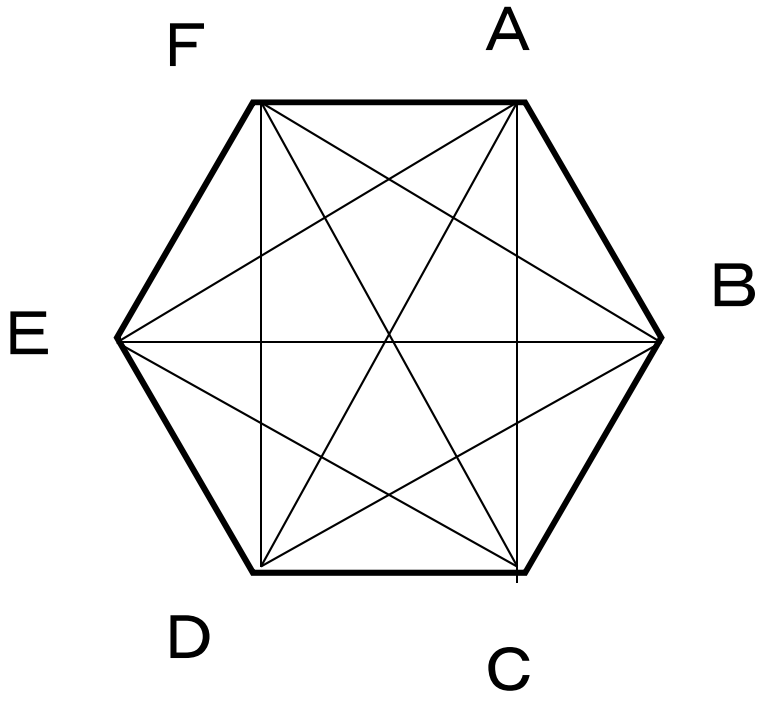
あらかじめ秘密に伝えないといけない

従来の暗号の問題点（2）



ユーザ数＝2の場合、
鍵の数＝1

ユーザ数n人では、鍵の数は
${}_nC_2$となる（1ユーザ当りn-1の
鍵を秘密に管理する必要あり）

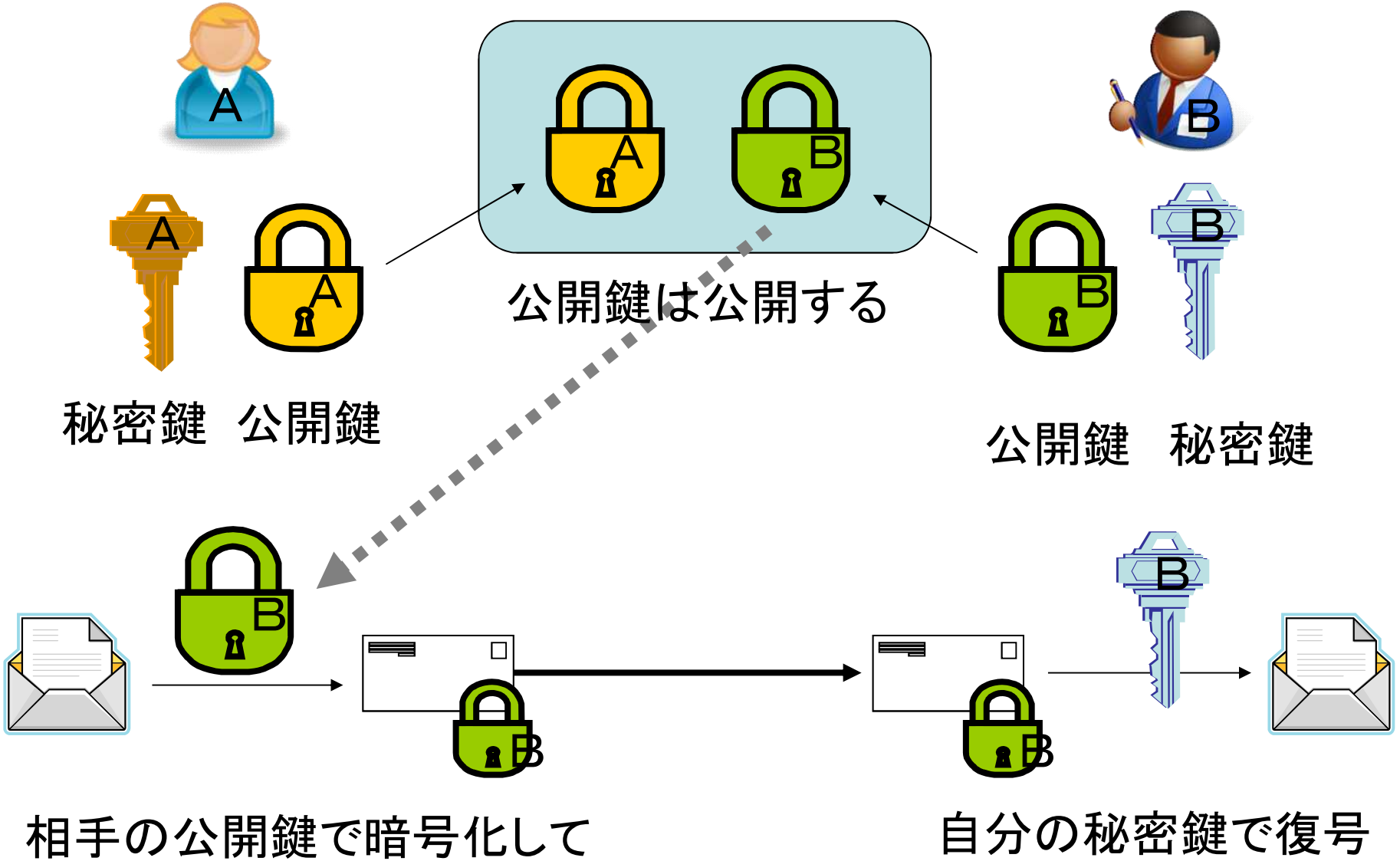


ユーザ数＝8では、
鍵の数＝28

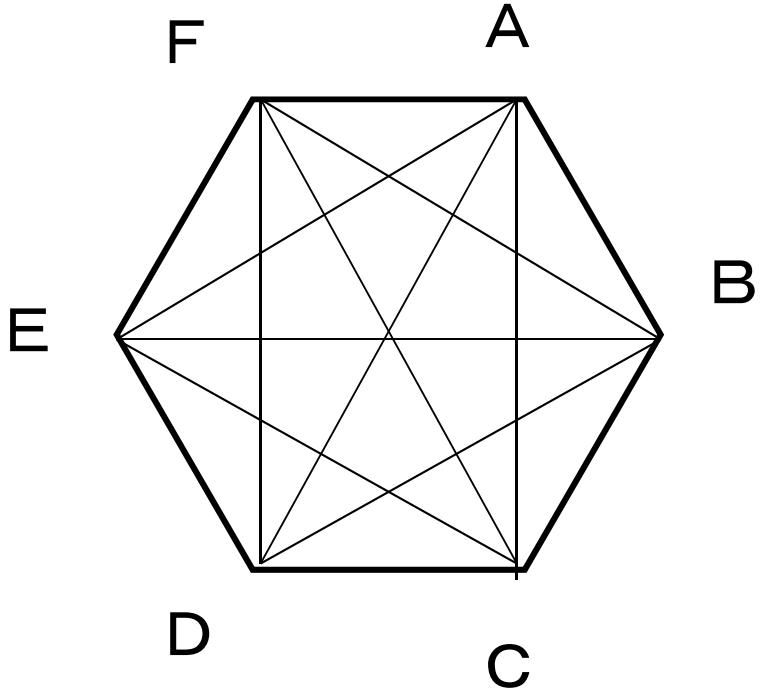
公開鍵暗号

- 1976年、DiffieとHellmanによりその概念が示された
- 公開鍵暗号方式の特徴：
  - 鍵の配送が容易
  - 秘密に保持する鍵の種類が少ない
  - 認証機能がある
- RSA方式が最もひろく使用されている方式
- WWWや電子メールの暗号、認証を行うために広く用いられている

公開鍵暗号とは


A
A
A
秘密鍵　公開鍵
公開鍵は公開する
B
B
B
公開鍵　秘密鍵
B
B
B
B
相手の公開鍵で暗号化して
自分の秘密鍵で復号

公開鍵暗号の利点

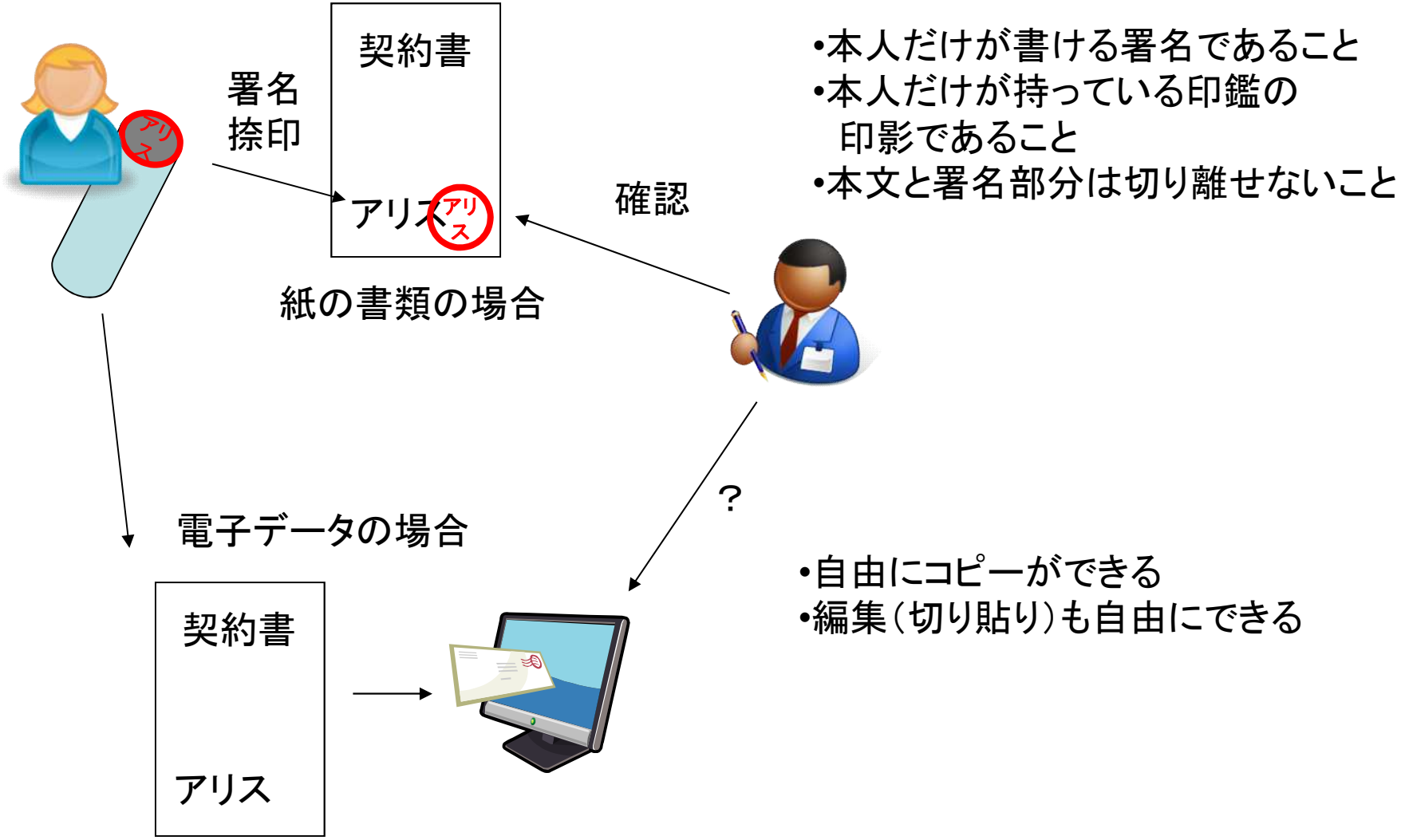


あらかじめ安全な通信チャンネル
を用いて、鍵を共有する必要なし

ユーザ数が多くなっても、
各ユーザが秘密に管理する
鍵は、自分の秘密鍵のみ。

→不特定多数の相手と通信をするネットワーク社会では
必要不可欠な技術

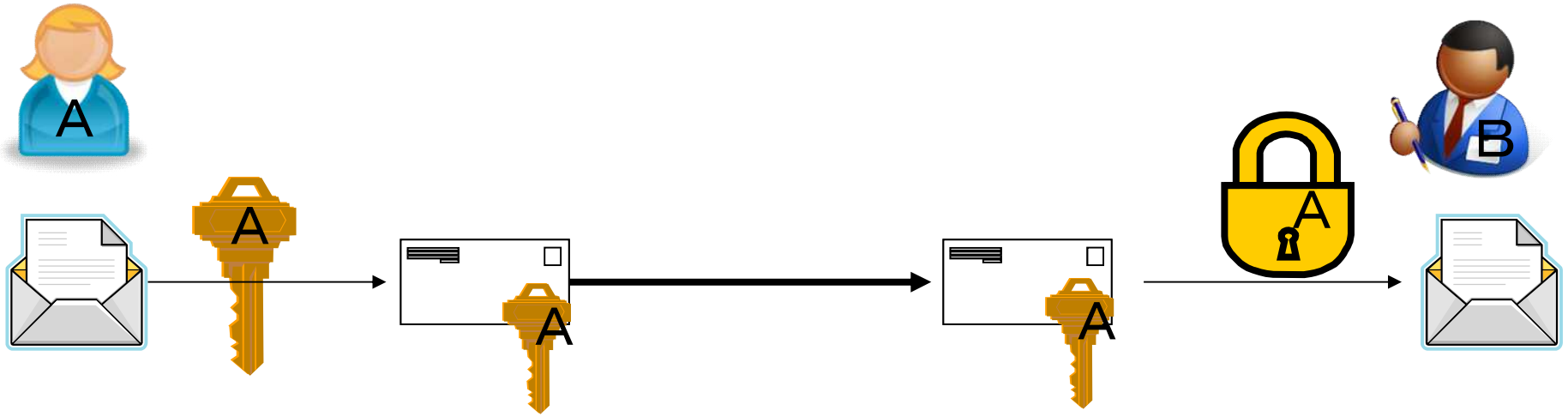
署名とは



- 本人だけが書ける署名であること
- 本人だけが持っている印鑑の印影であること
- 本文と署名部分は切り離せないこと

- 自由にコピーができる
- 編集（切り貼り）も自由にできる

公開鍵暗号による電子署名



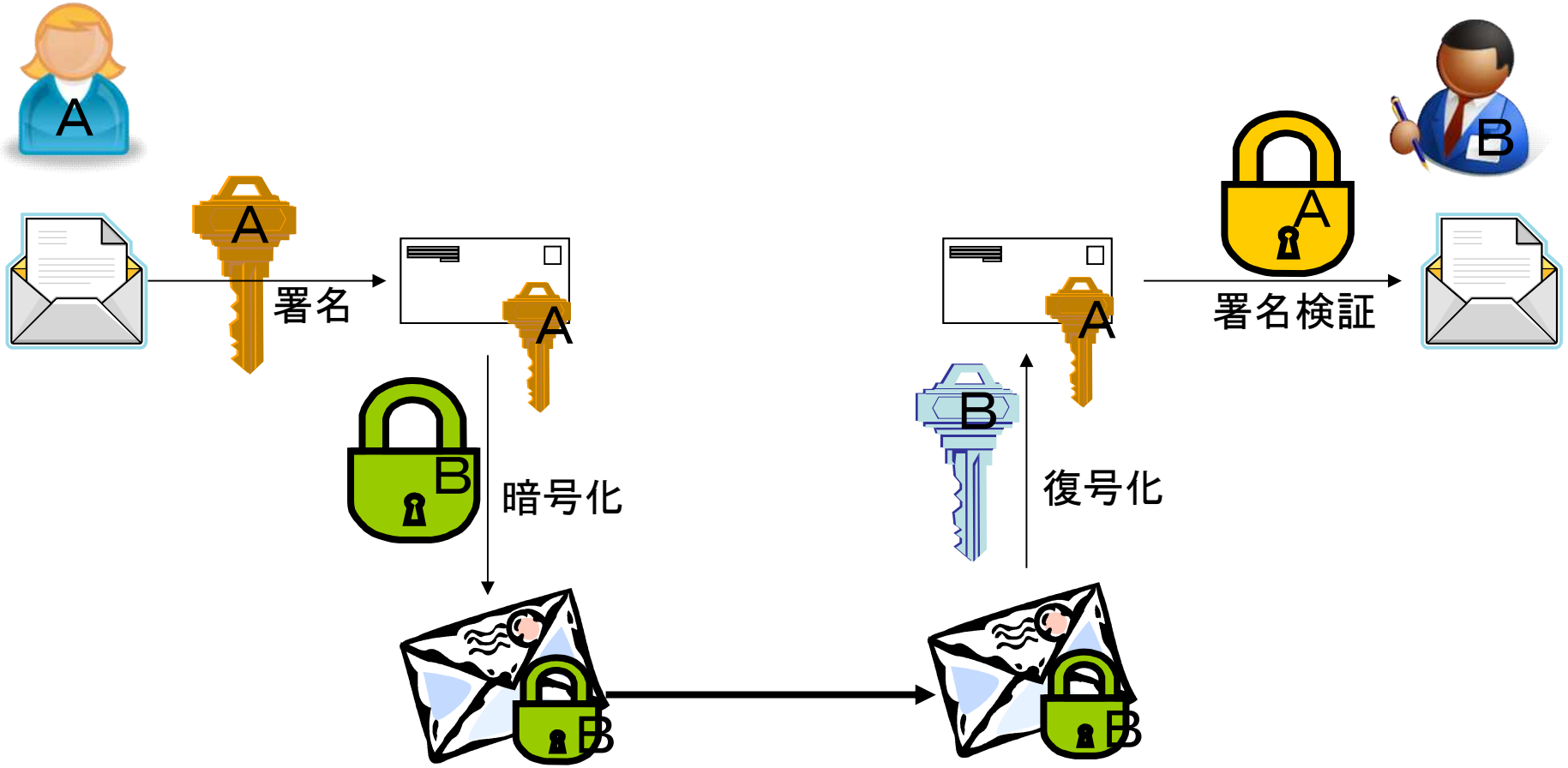
自分の秘密鍵で“変換”して　　相手の公開鍵で復号

Bが正しく復号できれば、
Aが（Aしか持っていない）秘密鍵で“変換”したということ

↓

受信した文書は、たしかにAが送ったものである

電子署名と暗号化の組み合わせ

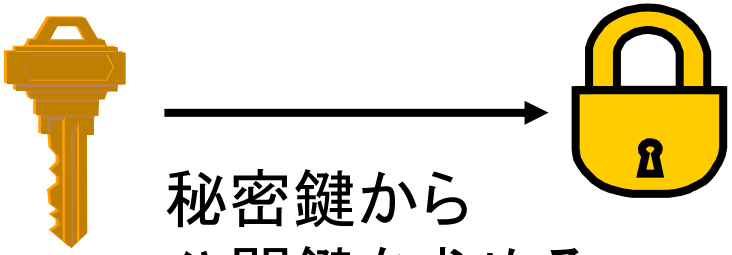


自分の秘密鍵で署名し、
相手の公開鍵で暗号化

自分の秘密鍵で復号し
相手の公開鍵で署名を
検証する

公開鍵暗号の数学的原理

公開鍵から
秘密鍵を求める
のは非常に困難



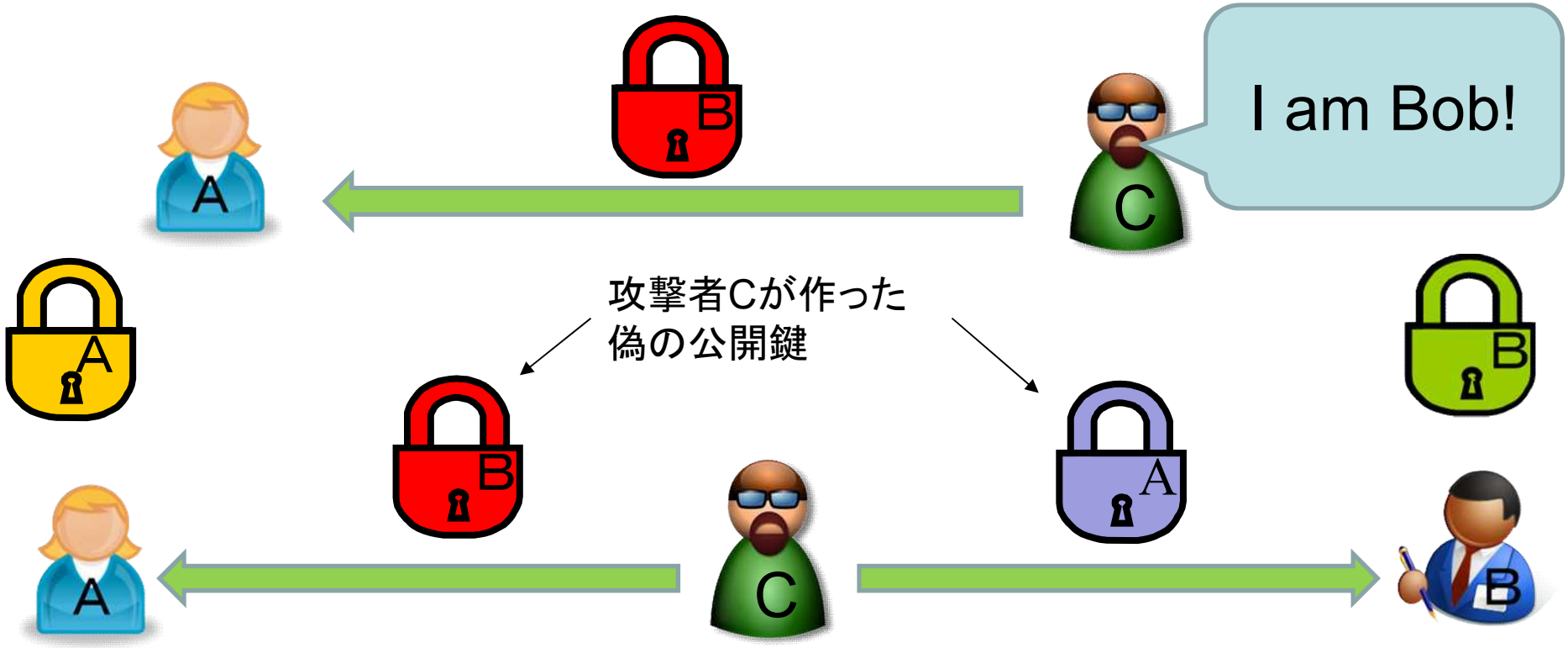
秘密鍵から
公開鍵を求める
のは容易

一方向性関数の利用
$y \leftarrow f(x)$の計算は容易だが、
$f^{-1}(y) \rightarrow x$の計算は非常に困難

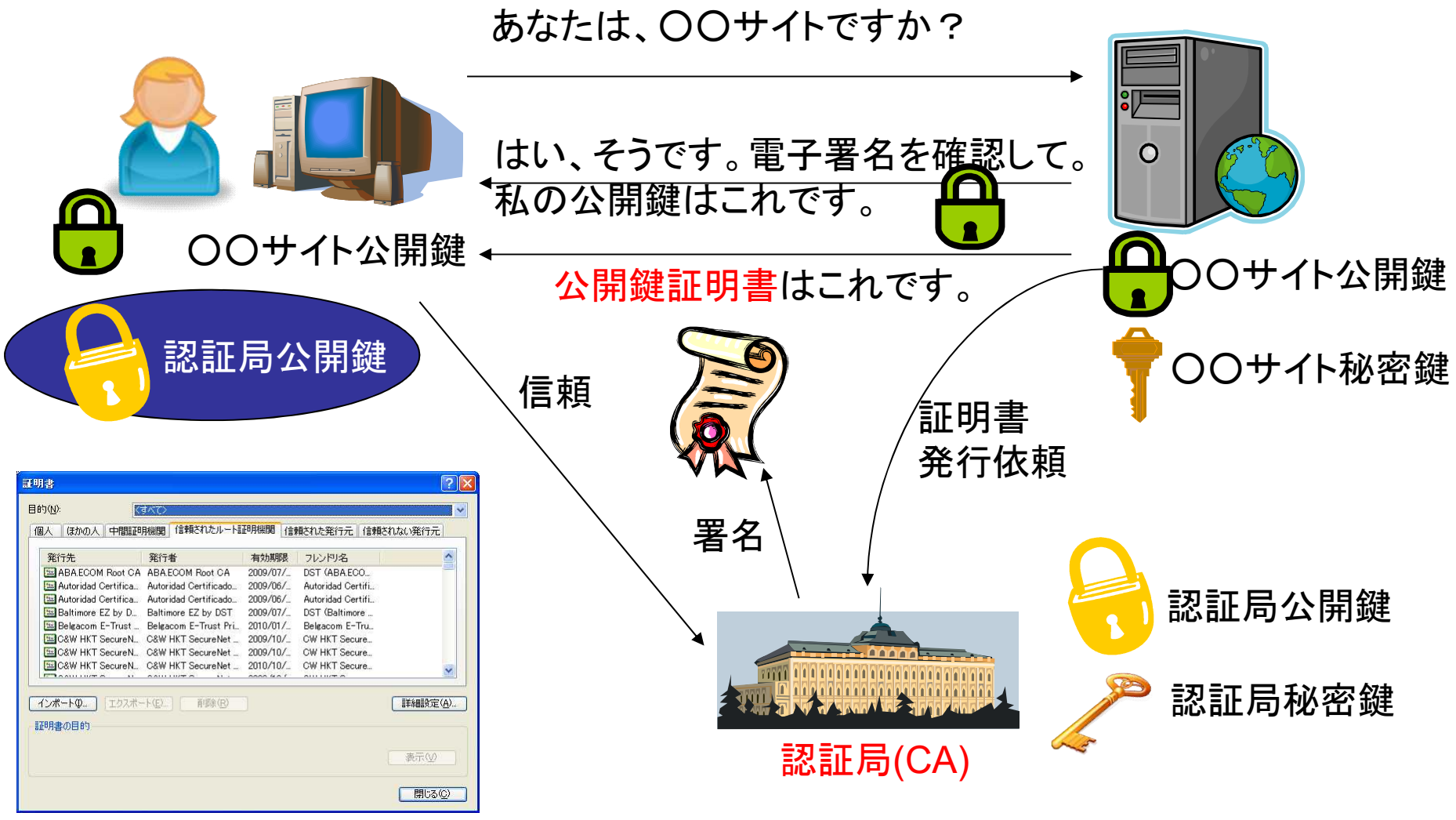
公開鍵暗号を作るには、
「落し戸付き」一方向性関数が必要
$f^{-1}(y) \rightarrow x$の計算は非常に困難だが
ある情報を知っている者には簡単

公開鍵の信頼性

- 公開鍵暗号を使うとき、相手の公開鍵が正しいものかどうかを確認する方法が必要



PKI(Public Key Infrastructure)とは



認証局(CA)の機能

- 登録局機能(RA; Registration Authority)
  公開鍵証明書を利用するユーザの審査、登録。
  どの程度厳格に審査するかはCAのポリシー次第
- 発行局機能(IA; Issuing Authority)
  RAの審査を経た利用者に公開鍵証明書を発行。
- 検証局機能(VA; Validation Authority)
  公開鍵証明書が有効（有効期限内か、CRLに含まれていないか）かどうか検証。
  - CRL(Certificate Revocation List)
  - OCSP(Online Certificate Status Protocol)

公開鍵証明書のフォーマット

- X.509で規定されている
  - バージョン番号(Version)
  - シリアル番号(Serial Number)
  - 証明書発行者名(Issuer)
  - 証明書有効期限(Validity)
  - 利用者名(Subject)
  - 利用者の公開鍵(Subject Public Key Info)
    アルゴリズム識別子と対応する公開鍵
  - 署名アルゴリズム(Signature Algorithm)
  - 認証局の署名

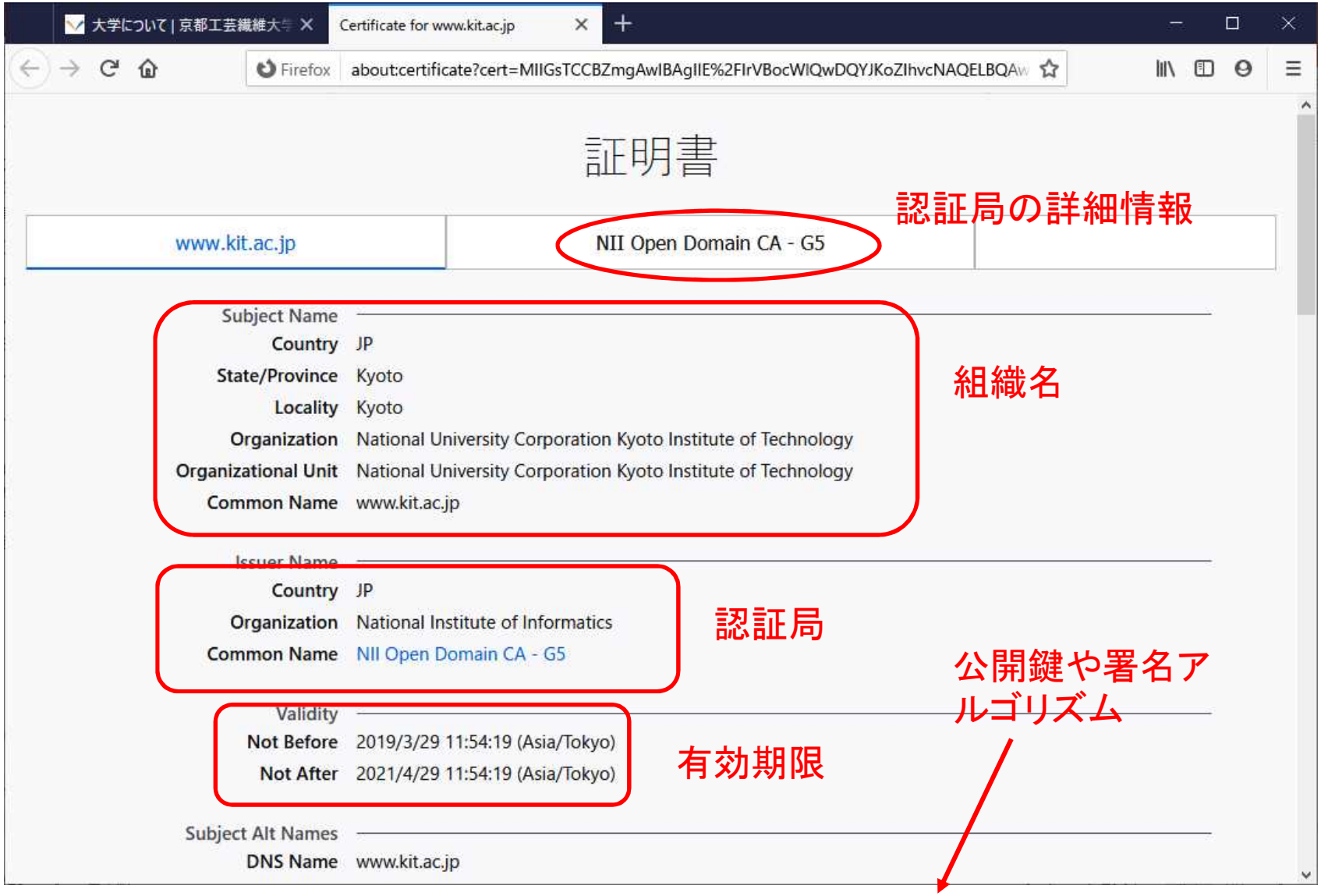
認証局の相互認証

- 複数の認証局間の信頼のパスをつなげる方法
  - 階層型トラストモデル
    ルート認証局、中間認証局の階層モデル
  - 相互認証型トラストモデル
    認証局がお互いに認証し合うモデル
  - ブリッジ認証型トラストモデル
    ブリッジ認証局を介してお互いに認証し合うモデル
  - 相互認定型トラストモデル
    利用者が認証局を相互に認定し合うモデル
  - 証明書信頼リスト型トラストモデル
    利用者が信頼できる認証局の証明書リストを持つモデル

Web証明書の例（1）


https://www.kit.ac.jp/uni_index/
交通アクセス
資料請求
お問い合わせ
サイトマップ
JP / EN
LINE
対象者別
学内専用
京都工芸繊維大学
KYOTO INSTITUTE OF TECHNOLOGY
学部・大学院・センター
産学官連携
入試情報
国際交流
学生生活
進路・就職
大学について
TOP - 大学について
クリック！

Web証明書の例（2）


大学について | 京都工芸繊維大学
Certificate for www.kit.ac.jp
Firefox
about:certificate?cert=MIIGsTCCBZmgAwIBAgIIE%2FIrVBocWIQwDQYJKoZIhvcNAQELBQAw
証明書
www.kit.ac.jp
NII Open Domain CA - G5
認証局の詳細情報
Subject Name
Country JP
State/Province Kyoto
Locality Kyoto
Organization National University Corporation Kyoto Institute of Technology
Organizational Unit National University Corporation Kyoto Institute of Technology
Common Name www.kit.ac.jp
組織名
Issuer Name
Country JP
Organization National Institute of Informatics
Common Name NII Open Domain CA - G5
認証局
Validity
Not Before 2019/3/29 11:54:19 (Asia/Tokyo)
Not After 2021/4/29 11:54:19 (Asia/Tokyo)
有効期限
公開鍵や署名アルゴリズム
Subject Alt Names
DNS Name www.kit.ac.jp