e-ビジネス情報技術講座
第10回
電子認証

講師　：　片岡　信弘

教科書第12章

ポイント

- インターネットの世界は危険がいっぱい

  その一方で

  - 電子商取引の金額はBtoBで200兆円，BtoCで14兆円
  - 電子商取引はどのような仕組みで安全性を担保しているのか
  - パスワード，クレジットカード番号など送信の安全性の担保の方法

12.1.電子認証の目的

インターネットの世界は様々に脅威が存在する

脅威の事例と対応策

- 「盗聴」の脅威
- 「なりすまし」の脅威
- 「改ざん」の脅威
- 「否認」の脅威
  - ◆自分が行った行為を否定し責任逃れする

電子認証とは

- インターネットを利用した商取引において
  1. 機密性　　盗聴を防ぐ
  2. 認証　　なりすましを防ぐ
  3. 完全性　　改ざんを見抜く
  4. 否認防止　　否認を防ぐ

  を実現する仕組み
- これを支える技術が「暗号」
  - ◆暗号はローマ時代から存在

12.2.暗号化方式

電子認証の暗号には

「共通鍵暗号」

「公開鍵暗号」

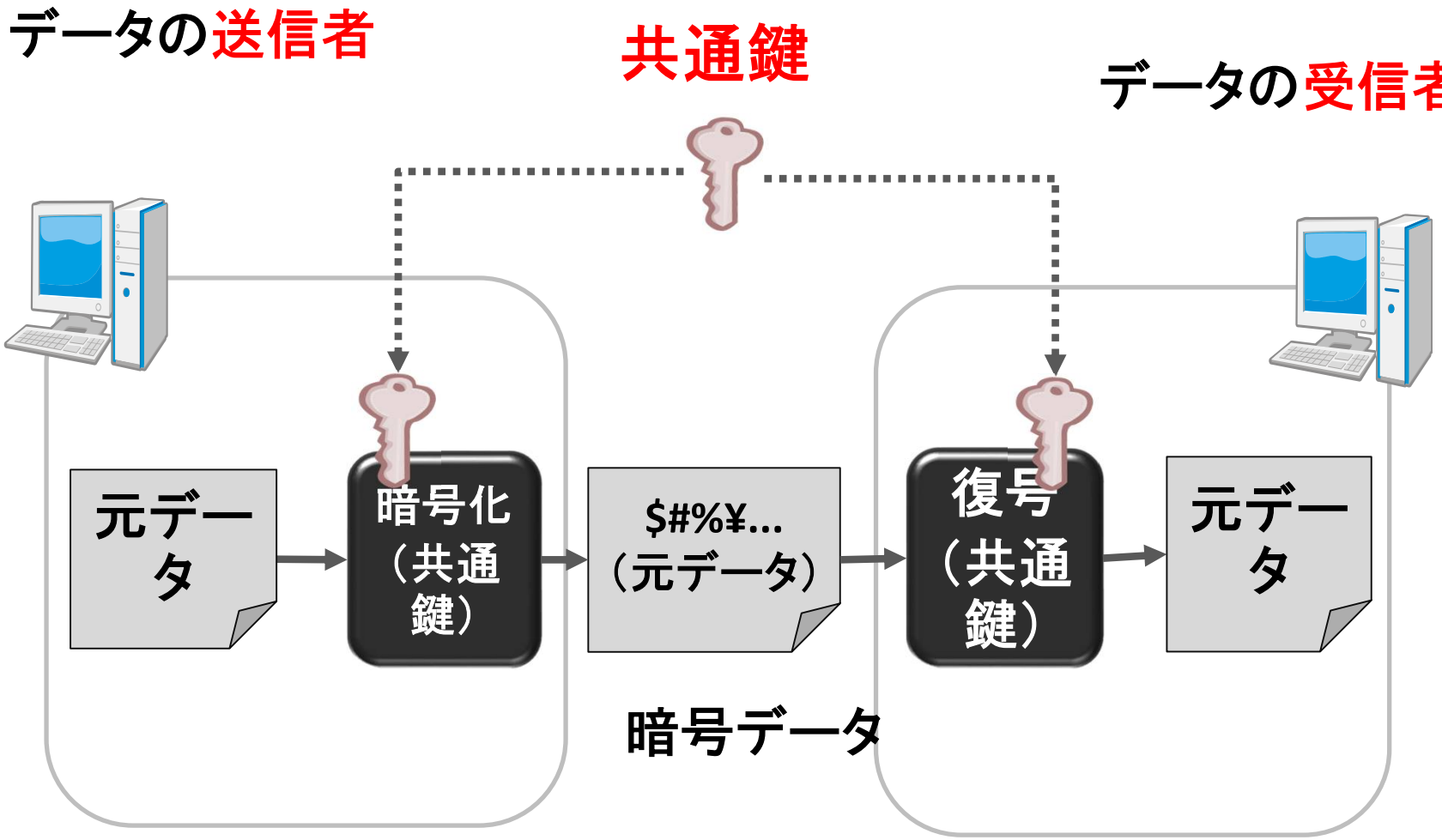
「一方向暗号」がある

(1) 共通鍵暗号方式

- 送信側と受信側が同じ暗号鍵を利用
- 特徴
  - 処理が高速
    - 大量のデータに利用
  - 鍵の管理方式が課題

- Quiz1
  - Wordで作成したサークル等名簿をネットで送付する方法

図12.2 共通鍵暗号　p138



ファイルを暗号化して送付するのも同じ

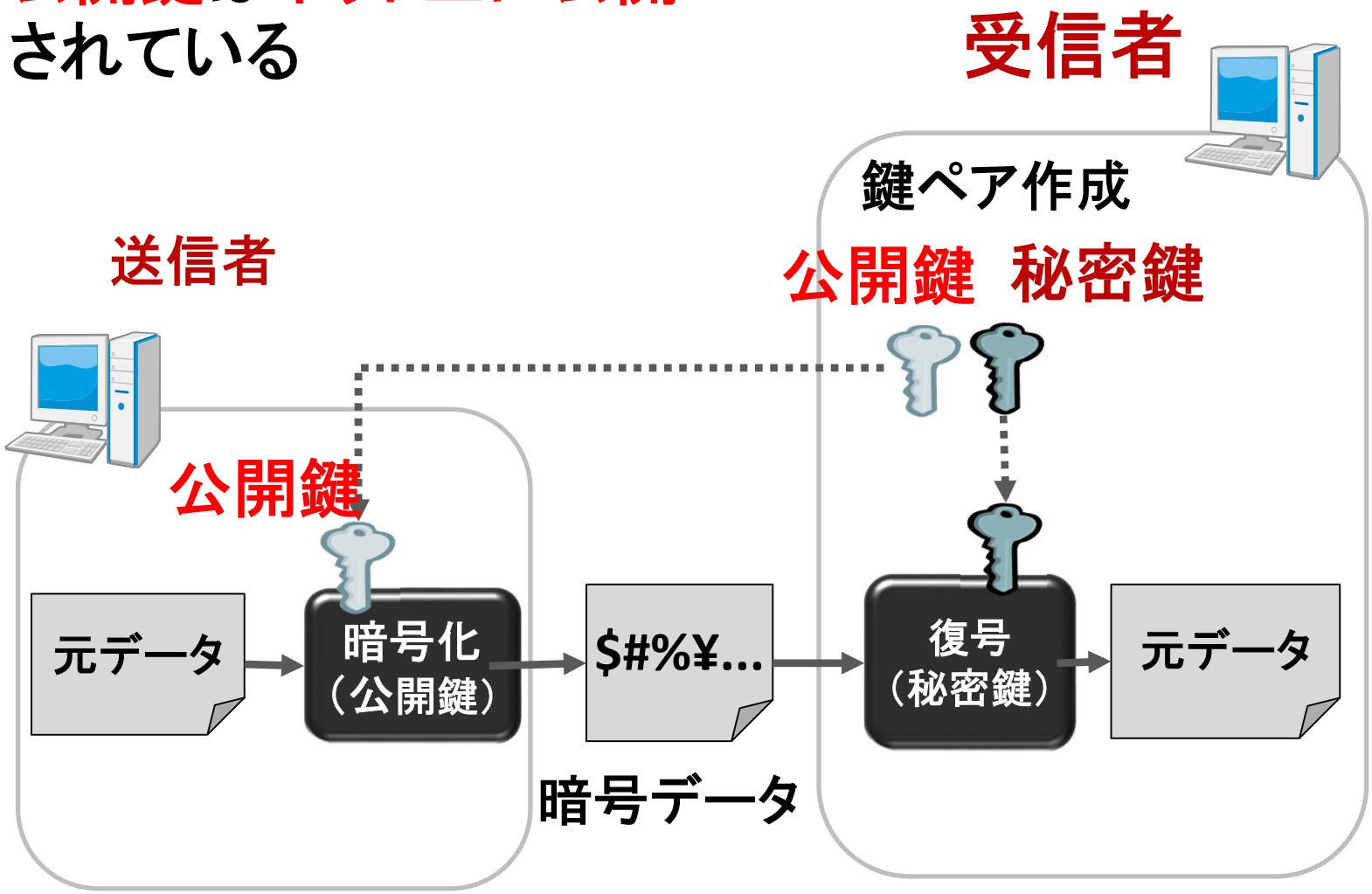
(2)公開鍵暗号

- 公開鍵と秘密鍵の鍵ペアを利用
- 片方の鍵で暗号化，他の鍵でのみ復号可能
- 鍵ペアを作るのはデータ受信者
  - 受信者毎に鍵ペアが存在
- 秘密鍵は厳重に保管，公開鍵は公開する
- データ送信者は公開鍵で暗号化，受信者は秘密鍵で復号化(公開鍵では復号できない)
- 特徴
  - 公開鍵を秘密にする必要がない
  - 暗号化処理が共通鍵より遅い

公開鍵，秘密鍵の作り方(番外)

図12.3 公開鍵暗号方式 p139

公開鍵は**ネット上に公開**されている



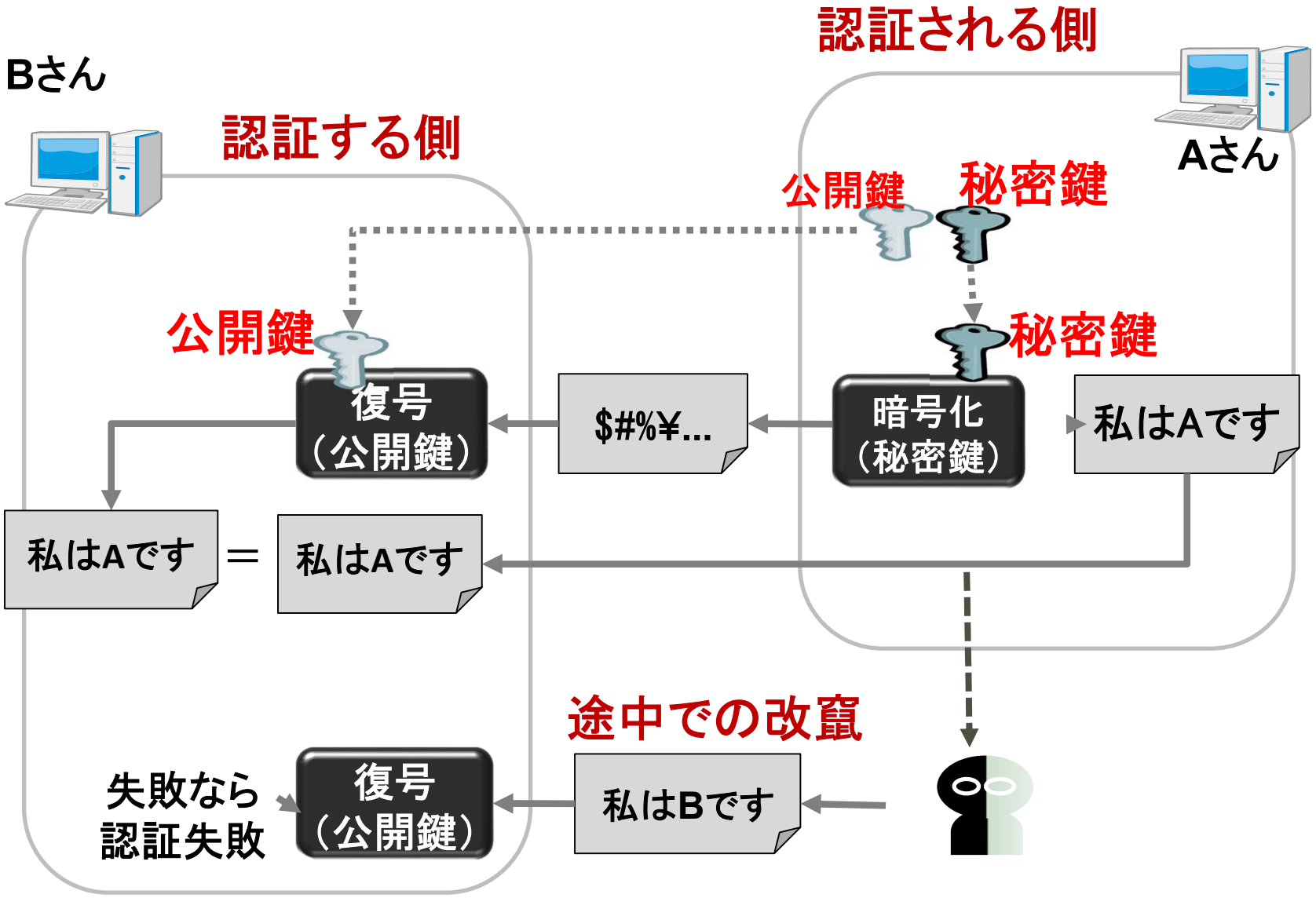
データを送信は，公開されている相手の公開鍵で暗号化する

ポイント

- 公開鍵で暗号化されたものは，そのペアである秘密鍵でしか復号できない
- 秘密鍵は厳重保管

- 何かおかしい??
- 詐欺師がAさんの偽鍵を公開したらどうする
  - ◆詐欺師は，Aさんの宛ての情報をネットで盗み偽鍵の秘密鍵で復号して情報を盗む

図12.5 公開鍵による電子署名 P141



公開鍵暗号による電子署名

- 認証される側は適当なデータと，そのデータを秘密鍵で暗号化したデータを送る
- 認証する側は，この暗号データを公開鍵で復号し，元データと一致すれば相手は，秘密鍵の持ち主であることが判明

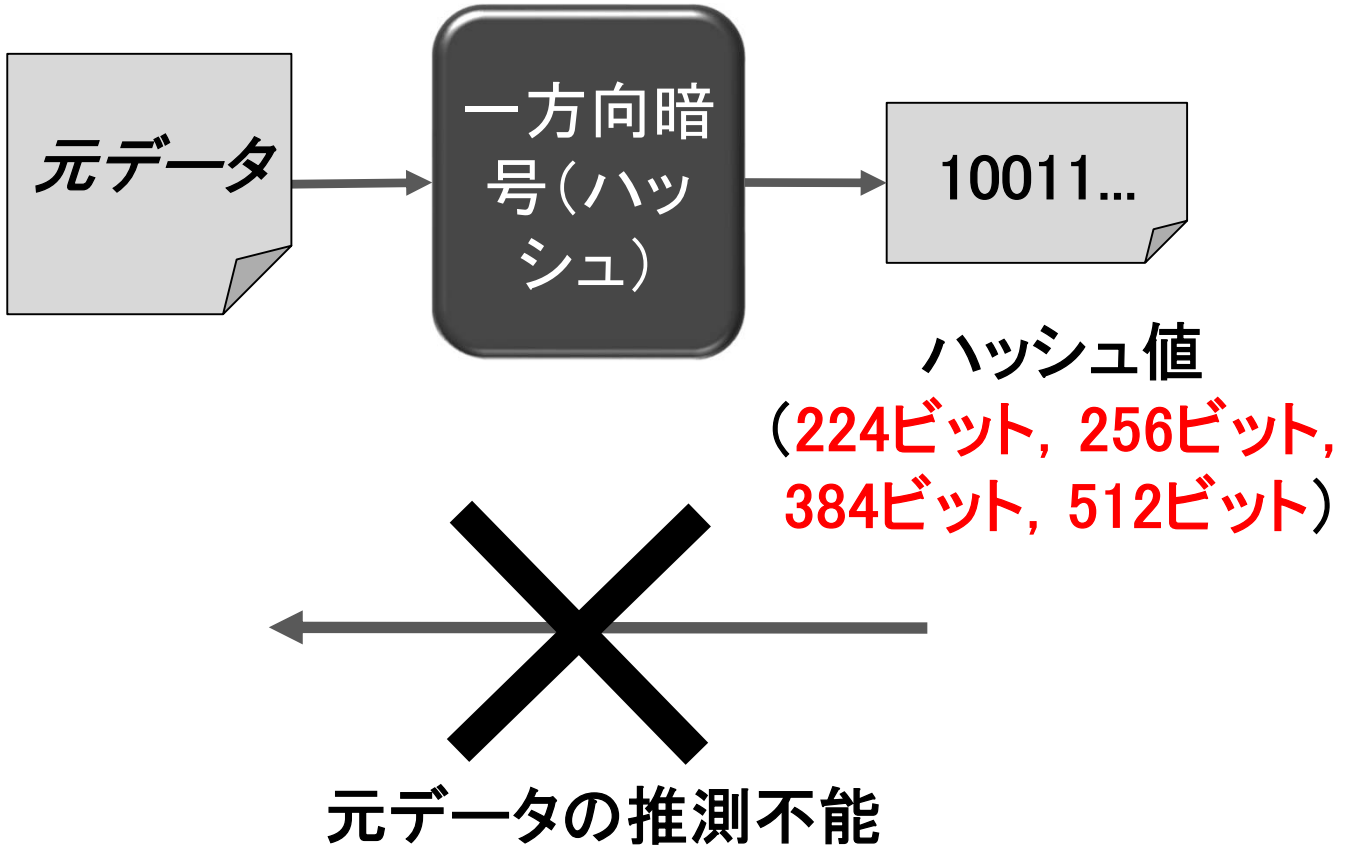
- すなわち正しい相手だと確認できる

- 本人の秘密鍵で暗号化されているためこのデータの内容を否認不可
- 文章の内容を否認できない

(3) 一方向暗号(ハッシュ関数)

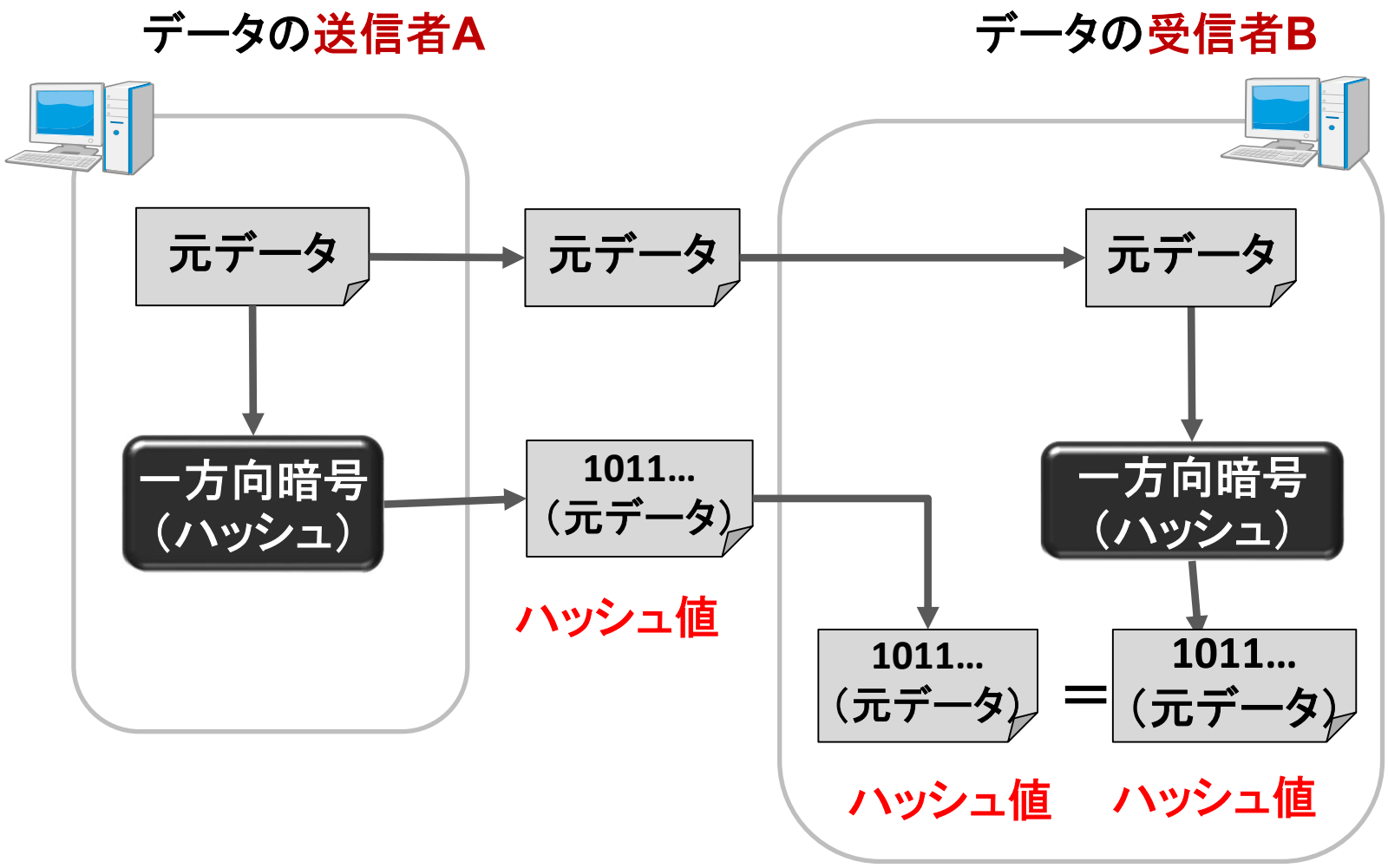
- データを一方向に暗号化する技術
  - 一方向とはもとに戻せないことを
  - ハッシュ関数とも呼ばれる
- 元データ大きさにかかわらず，一定の長さの短いデータに変換
  - 得られたデータはハッシュ値やメッセージ・ダイジェストと呼ばれる
- 二つのデータが同じかどうかを判別するときに利用
  - 両者からハッシュ値を取って比較する
  - 大量の元データ全体を比較する必要なし
  - データが改ざんされていないことの確認に利用

図12.2 一方向暗号 p138~~改定~~



- 異なるデータが同じハッシュ値になることはないのか

図12.3 一方向暗号による改ざんの検出 p139



- 100万円の領収書が10万円に改竄されることは無い

Quizその2

- 公開鍵方式はどの様の詐欺が考えられるか
  - A. 秘密鍵を盗み，情報を盗む
  - B. 公開鍵を盗み，情報を盗む
  - C. 他人に成りすまし，公開鍵をネットに公開

12.3.PKI(公開鍵基盤)

・公開鍵が本人のものであることを保障する方式

・秘密鍵が盗まれたときの対処方式

PKI(Public Key Infrastructure)とは

- 公開鍵基盤と呼ばれ，公開鍵の技術を利用しセキュリティ対策を実現する仕組み
- 電子商取引や通信を行うとき，相手および自分自身が本人であることを認証する
- 法的な根拠に基づき公的に認められた第三者がその基盤を運用
- 運用組織を認証局(CA局)と呼ぶ
  - 電子証明書の登録
  - 電子証明書の発行
  - 電子証明書の検証

図12.6 認証局の業務内容　p142

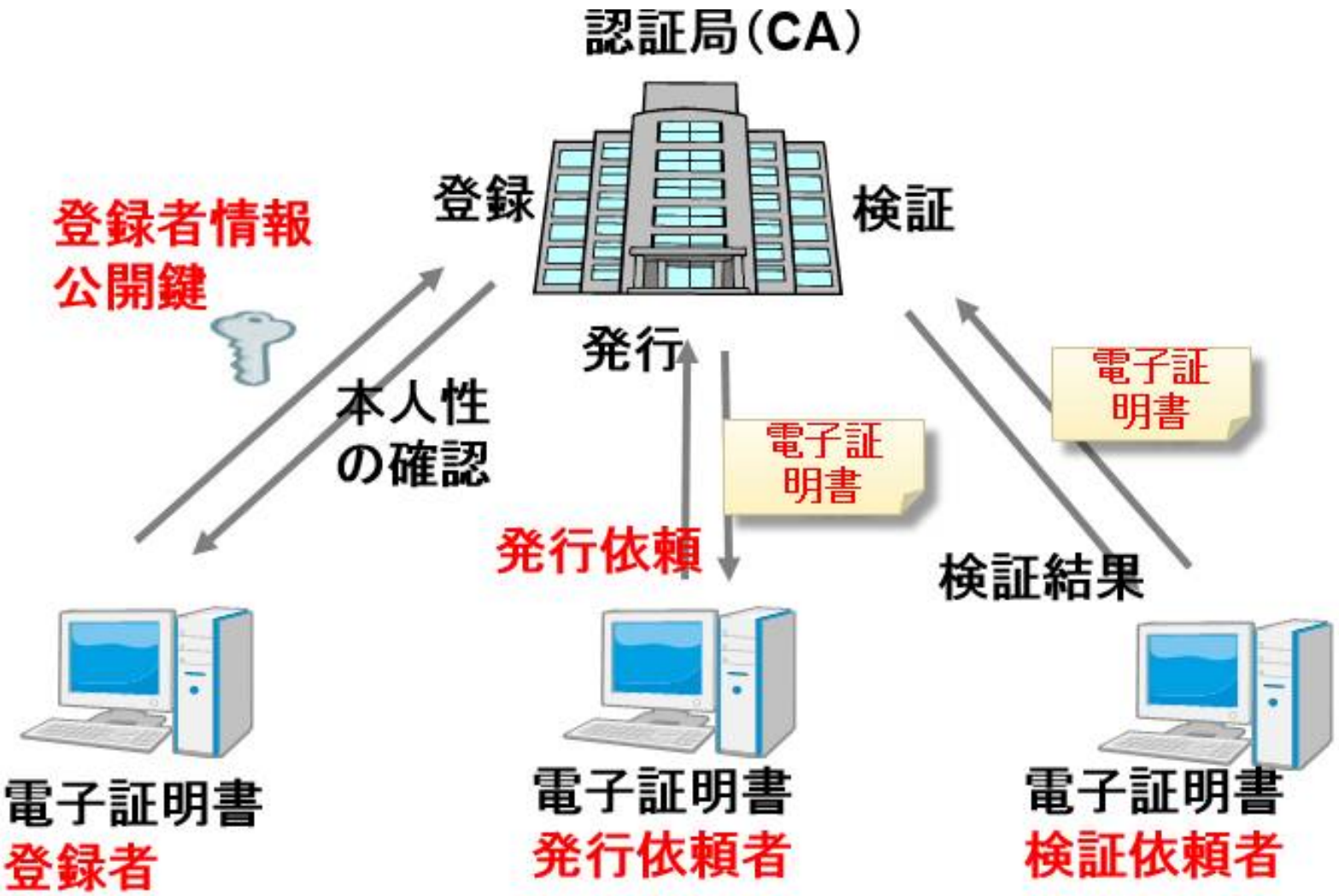


図12.8 電子証明書 p143

証明書形式のバージョン
証明書のシリアル番号
署名アルゴリズム
発行者（認証局）
有効期間（開始と終了）
サブジェクト（証明書所有者）
公開キー（公開鍵、公開鍵暗号方式）

認証局の役割

- 電子証明書の登録
  - 登録申請者の本人性の確認
  - 登録申請者が公開鍵に対応する秘密鍵の所有者であることの確認
- 電子証明書の発行
  - 電子証明書発行
  - 電子証明書失効リスト発行
- 電子証明書の検証
  - 認証局の署名の確認
  - 有効期間の確認
  - 失効情報の確認

図12.9 SSL/TSL通信電子証明書 p144

Quizその2　Answer

- 公開鍵方式はどの様の詐欺が考えられるか

  A.秘密鍵を盗み，情報を盗む

  ⇒盗まれたら電子証明書無効を届ける

  B.公開鍵を盗みその人に成りすます

  C.他人に成りすまし，公開鍵をネットに公開

  ⇒認証局を騙すことはできない

12.4. PKI(公開鍵基盤)の活用事例

・契約書などのディジタル文書に電子署名を行い確実に受け渡しする手順

・Webサイトでのパスワード等を安全に受け渡しする手順

電子署名法

- PKIに基づいた電子商取引を正式な商取引とするために制定された法律
- 正式名称「電子署名及び認証業務に関する法律」
- 2000年5月に制定，2001年4月に施行
  - 電子署名が紙の契約書で使う実印と同様に本物であることを証明できることを規定
  - 認証機関の運用主体を民間に任せることができることを規定

署名された電子文書の受け渡し課題

- 企業間の取引で，署名捺印された書類をどのように確実に受け渡すか

- 確認すべきこと
  - 電子文書が本人から送付されたものか
  - 文書が改竄されていないか

(注)文書の暗号化はここには入っていない

署名された電子文書の受け渡し方式

送信側

①電子証明書(**公開鍵**)

②電子文書

③電子文書のハッシュ値
秘密鍵で暗号化されている

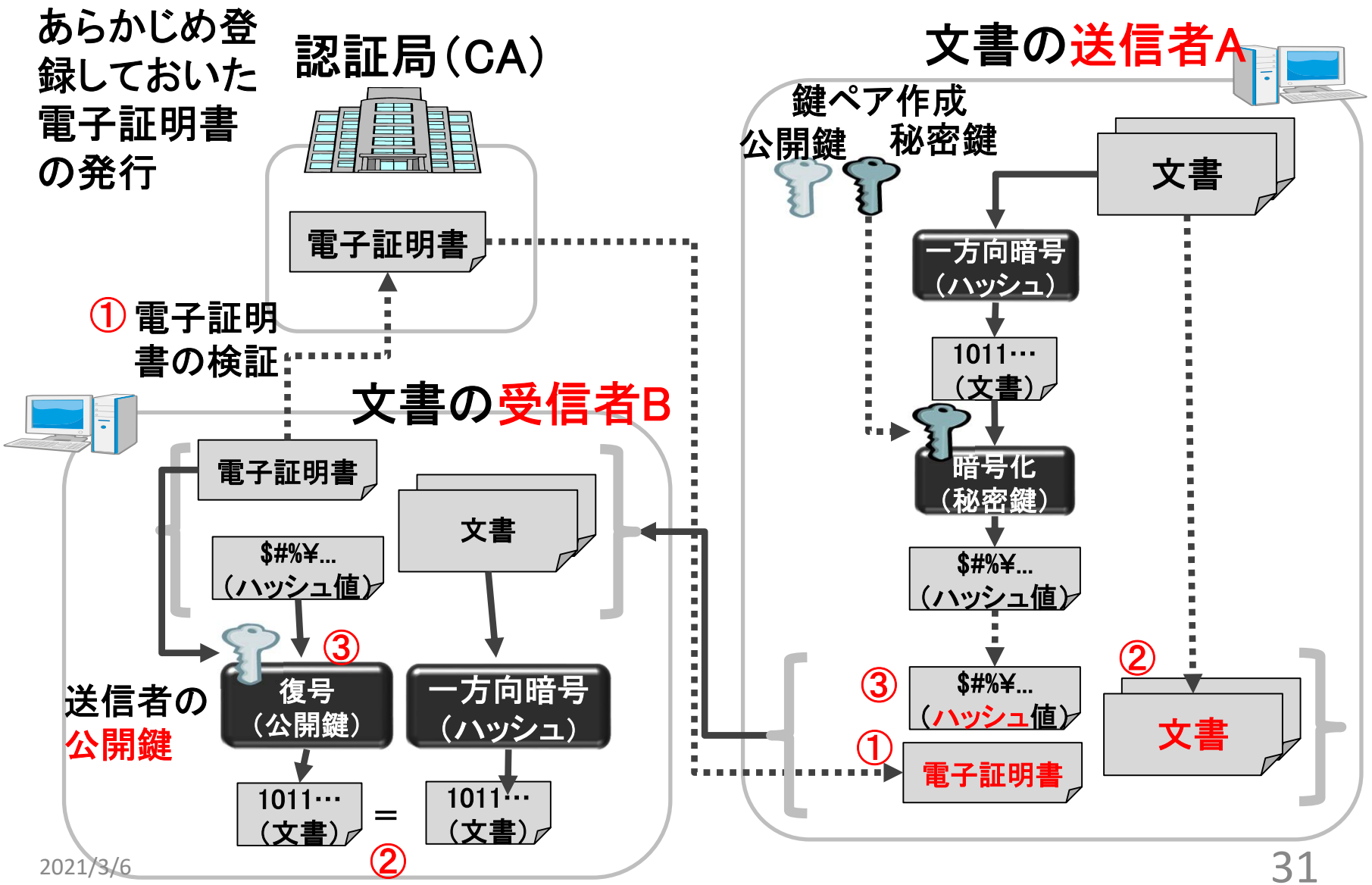
受信側

①電子証明書から**公開鍵**取り出し

(2)電子文書の**非改竄性**確認
・ハッシュ値を**公開鍵**で復号化
・電子文書本体のハッシュ値作成
・二つのハッシュ値を比較

③**本人確認**⇒公開鍵で復号できたこと

図12.15 電子署名の手順　p148



12.5.ユーザ認証

電子証明書を持っていない個人の
安全な通信をどのように行なうか.

ユーザ認証の方法

- ユーザID，パスワード入力
  - 平文での入力のサイトもある(危険)
  - SSLを利用した入力サイト(安全)
    - 暗号化して通信している

    httpS://login.yahoo.co.jp
- ワンタイムパスワード
  - 時刻から毎回異なるパスワードを生成する装置を利用(1分ごとに変化)
  - ログインの時は表示されたパスワードを入力
  - サーバ側にも同じ仕組みを備えた装置で，送られてきたパスワードが一致するか認証

図12.12 ワンタイム・パスワード　P146

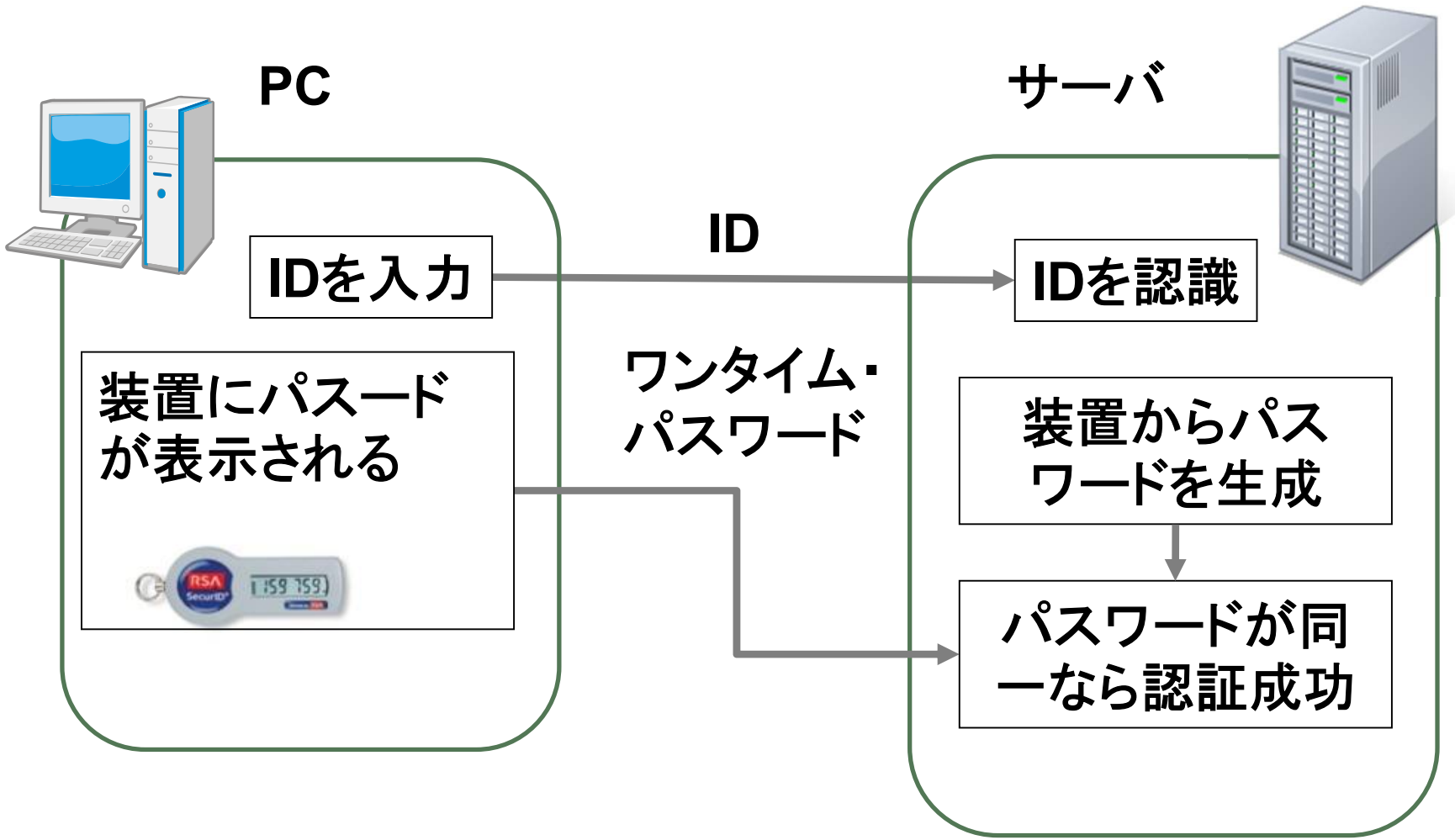
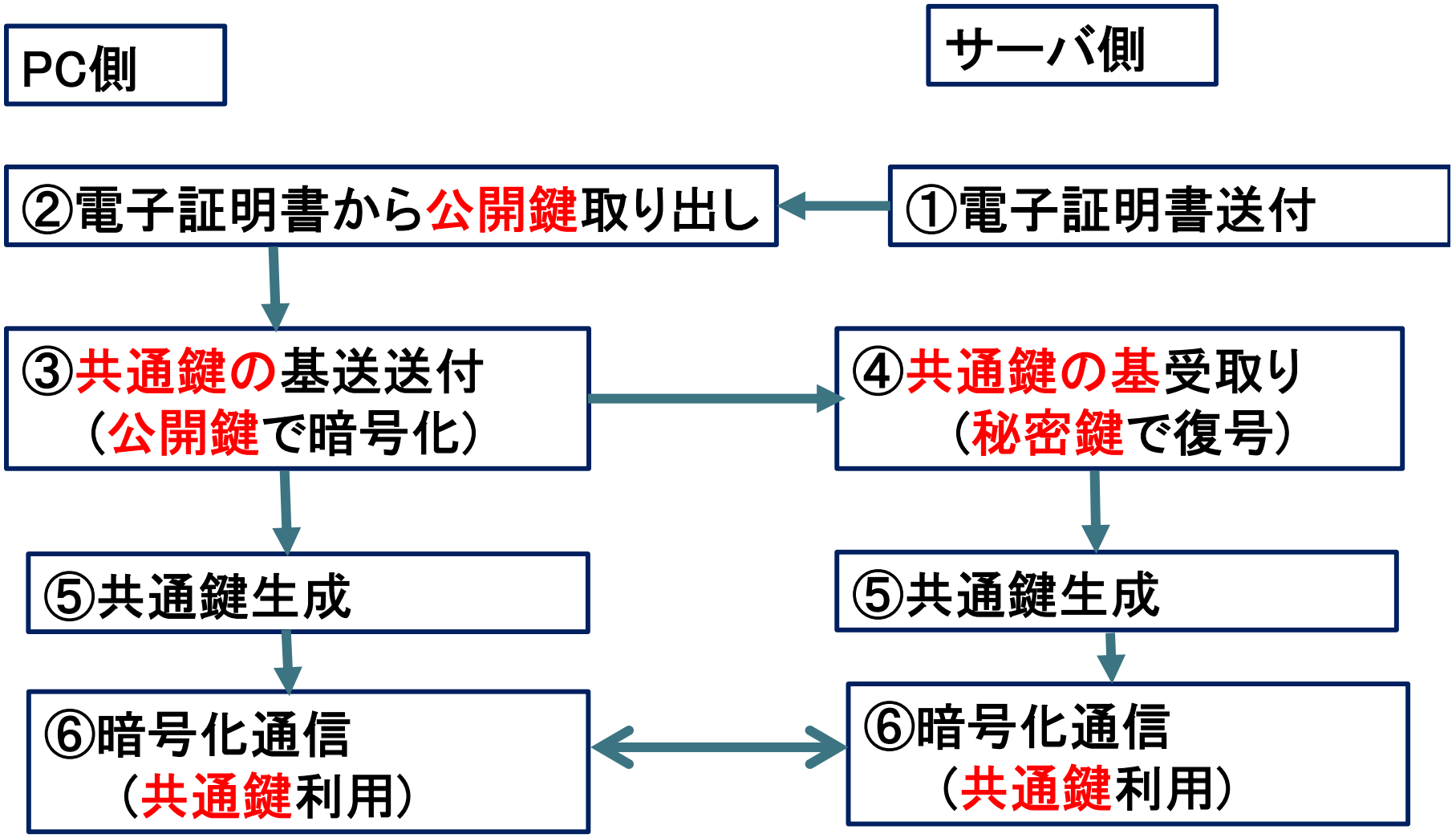


図12.13 ワンタイム・パスワード生成装置
(RSA社　提供)　　P146

SSL(Secure Socket Layer)通信式



ポイント　PC側からは、暗号送信可
サーバからは、暗号送信不可

Quizその3

- SSLで暗号化して送付いるのになぜワンタイム・パスワードなどで安全性を確保するのか?

A. 暗号が破られるから
B. 暗号化する前に盗まれるから
C. SSLは信用できないから

まとめ

- 電子認証の意味と必要性
  - 「盗聴」「なりすまし」「改竄」「否認」の脅威
  - 「機密性」「認証」「完全性」「否認防止」で対抗
- 暗号技術の3種類
  - 共通鍵暗号，公開鍵暗号，一方向暗号
- 電子証明書を発行する第三者機関CAがある
- 署名された電子文書の送付では，非改竄性と本人確認が行なわれる
- Webサイトとサーバのやりとりはは SSL方式によりデータを共通鍵で暗号化して送付する
  - 共通鍵ではセッションの度に作り出される