情報社会論

情報社会における
セキュリティの問題

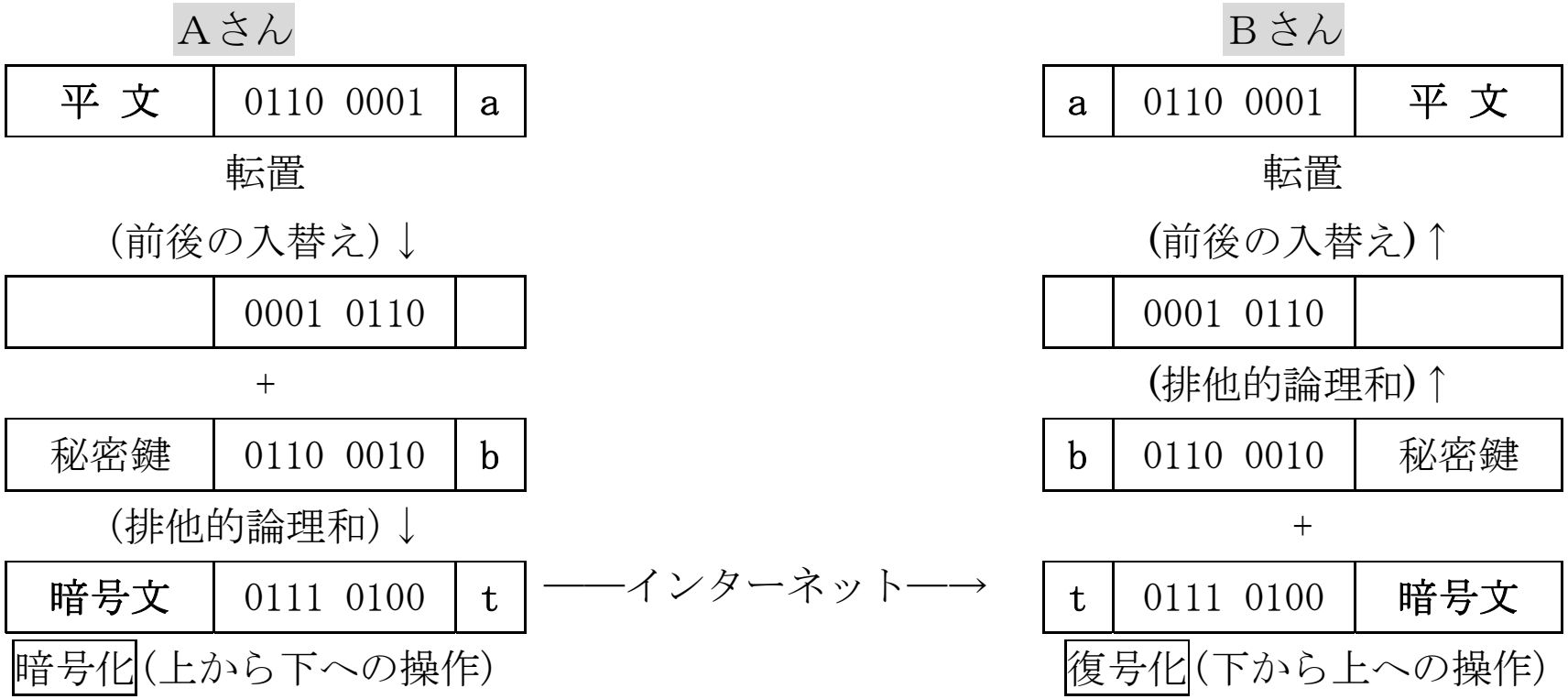
インターネットにおける
デジタルデータの伝わり方

- ネットでの情報のやりとりは，バケツリレーのようにルーターからより近くのルーターへと伝わる。
  - 通信途上のデータは盗聴が容易である。（プライバシー・セキュリティ問題）
  - 通信を中継ぎしているコンピュータにおいてデータの改ざんが容易である。
  - 電子メールなどの情報の発信者は容易に他人になりすますことができる。
- 暗号化，電子署名，電子認証が必要になる。

デジタル情報と暗号化

- アナログの時代から，情報を暗号化して伝えるということは，戦争遂行においても，企業活動においても重要で，結果を左右することであった。
- 初歩的な暗号方式として，共通鍵暗号方式という方式がある。
  - 送信者と受信者が共通の当事者にしか分からない秘密（共通）鍵で暗号化および復号化する方式である。
  - 複数の者が1つの秘密鍵を管理するので，漏洩の恐れがある。
  - 手広くやるには管理の手間がかかる。

共通(秘密)鍵暗号方式



排他的論理和:0+0=0,0+1=1,1+0=1,1+1=0で計算させる。

公開鍵暗号方式

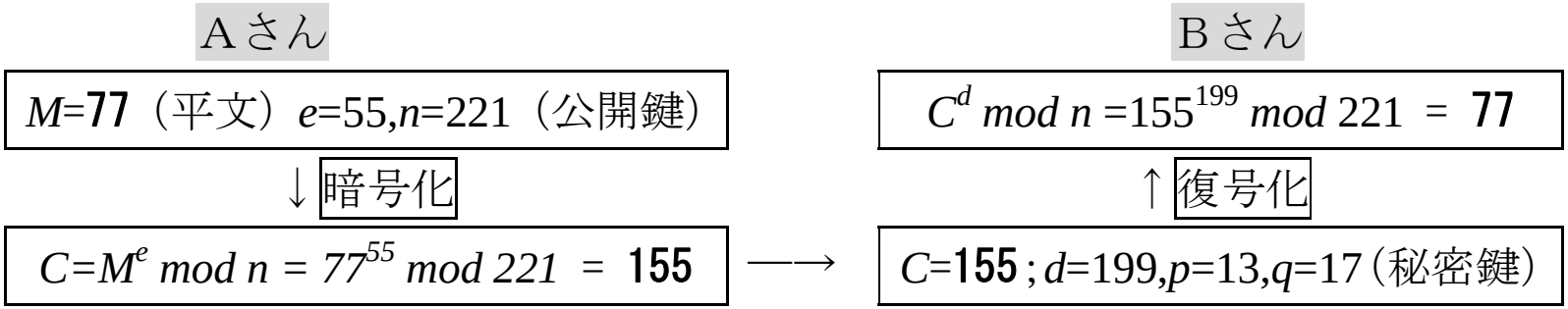
- 公開する鍵と，秘密にする鍵を使い分ける。
  - 秘密鍵は自分だけで管理する。（漏洩の恐れが小さい）
  - 公開鍵は広く知らせる。
  - 暗号化には公開鍵で行う。公開鍵では復号化できず，秘密鍵でしか復号化できない。
  - 秘密鍵で「署名」すると，署名が真正であるかどうかは共通鍵によってのみ行える。本人のみ知りうる秘密鍵で署名した物でしか公開鍵は反応しない。（本人確認）
  - 共通鍵暗号方式の弱点を克服。

公開鍵暗号の手順

- Bさんは2つの素数p,qを選んで，$n=pq$ ，$m=(p-1)(q-1)$を計算し，適当な$d(<n)$を選んで$e \cdot d \bmod m = 1$となるeを計算する。（n,eは公開鍵，dは秘密鍵）
- BさんはAさんにn,eを伝える（公開）。
- Aさんは平文Mを$C = M^e \bmod n$で計算した結果Cを暗号文としてBさんへ送る。
- Cは公開鍵では復号化できない。
- Bさんは受信したCを$C^d \bmod n$で計算する。（dは秘密鍵）この結果が平文となる。

具体例

※　M=77,p=13,q=17, n=pq=221, m=192,d=199,(e=55)
の場合。[秘密鍵d=199,p=13,q=17]



鍵を破られるリスクが低い（経済的に見合わない）ことに，この暗号の強さがある。

公開鍵暗号と電子署名

- BさんからAさんへ文書を送る時，その文書が，確かにBさんが発したものであること，そして内容が改竄されていないことの確認するためにBさんは電子署名をおこなう。
- 公開鍵暗号方式の秘密鍵は，本人しか知り得ないものであるので，これを本文にリンクさせることで署名を行う。受け取った人は，公開鍵で，真正であることを確認できる。
- 本文の改竄があったり，署名に他の文章を付けると，瞬時に見破ることができる。

認証の必要性

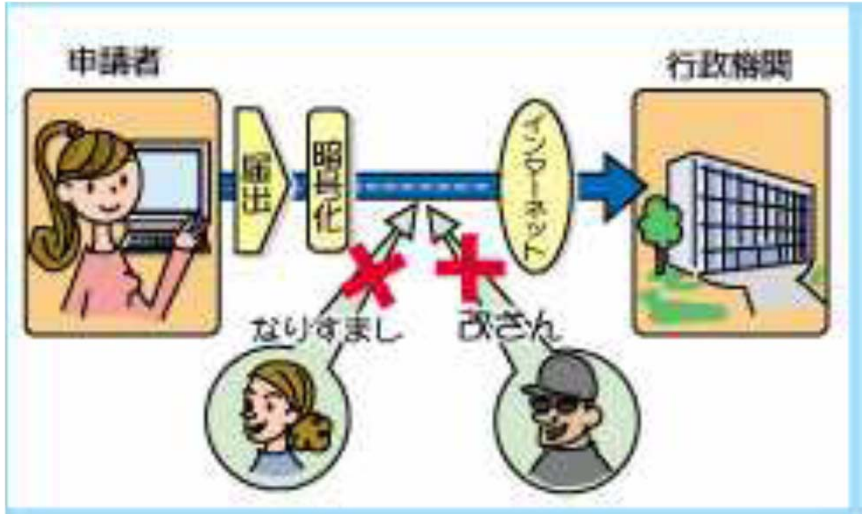
- 依然として，Aさんにとって次のような問題は残る。
  - たしかにBさんの公開鍵であるかどうか。（公開鍵の一意性の問題）
  - 公開鍵を提示して取引を求めているのが確かにBさん自身であるのか。（なりすまし問題）
- アナログデータでは，欧米のサイン，日本の捺印にあたるものが，偽造される問題以外に，なりすましの解決をはかる必要がある。→認証

暗号化と認証

- 暗号化は書かれている内容を他人に読まれないようにする技術である。
- 認証は、書かれている内容が確かに真正で改竄されておらず、差出人も他人の成りすましでなく本人であることを保証する技術である.
  - 元々は、印鑑やサインで保証していた.
  - ネット上の書類（デジタル署名）では一般に公開鍵暗号方式を利用する.
    - デジタル署名は、データの正当性（改竄されていない、あるいは他の文書に署名が付加されていないか. ）を同時に検証するものである.

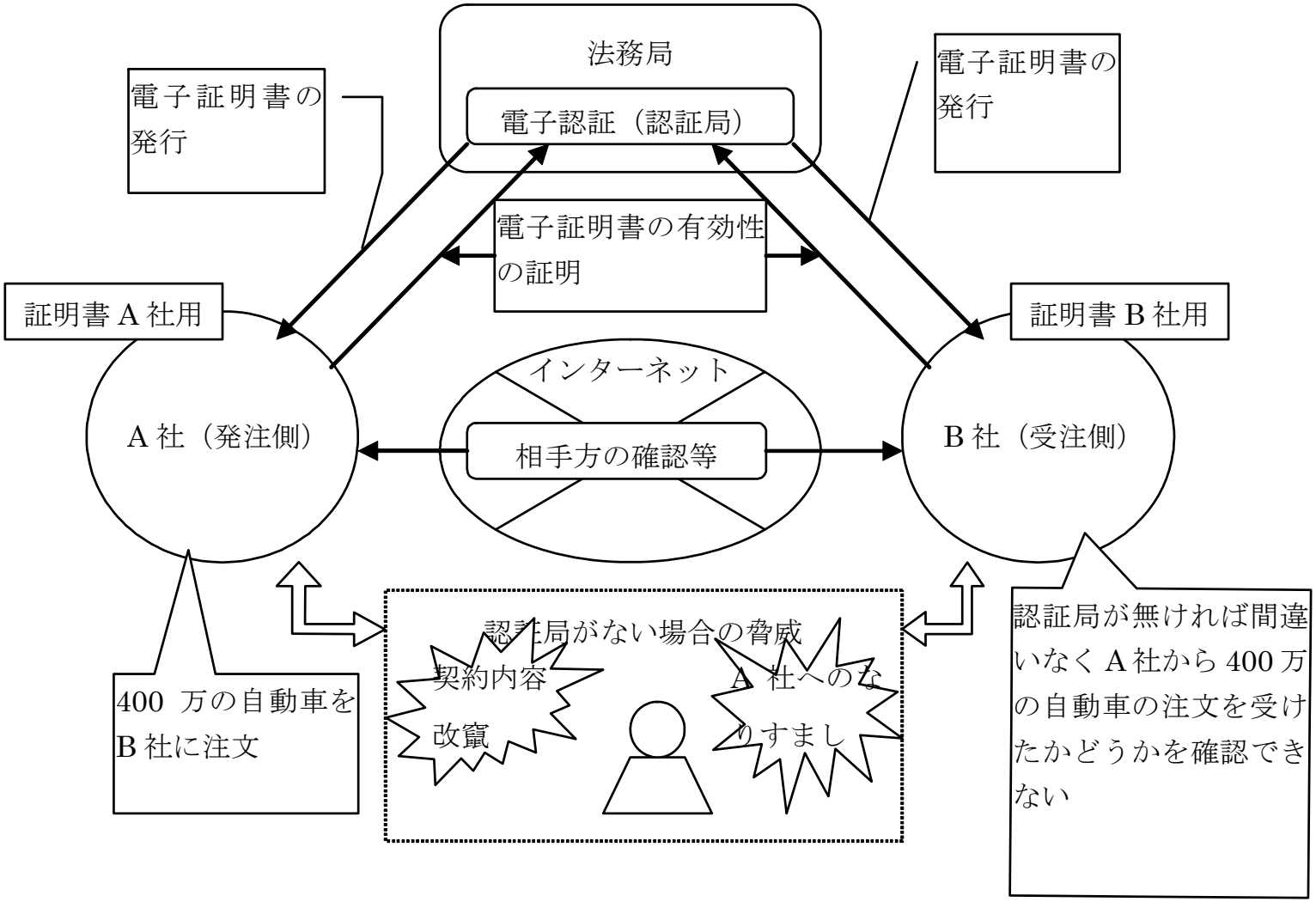
公的個人認証サービス

- 市区町村で発行される認証サービスの発行機関
  1. 住基カードの入手
  2. 電子証明書の発行を受ける（データとして格納）
  3. クライアントソフト・申請用ソフトなどを起動して手続。
- http://www.jpki.go.jp/



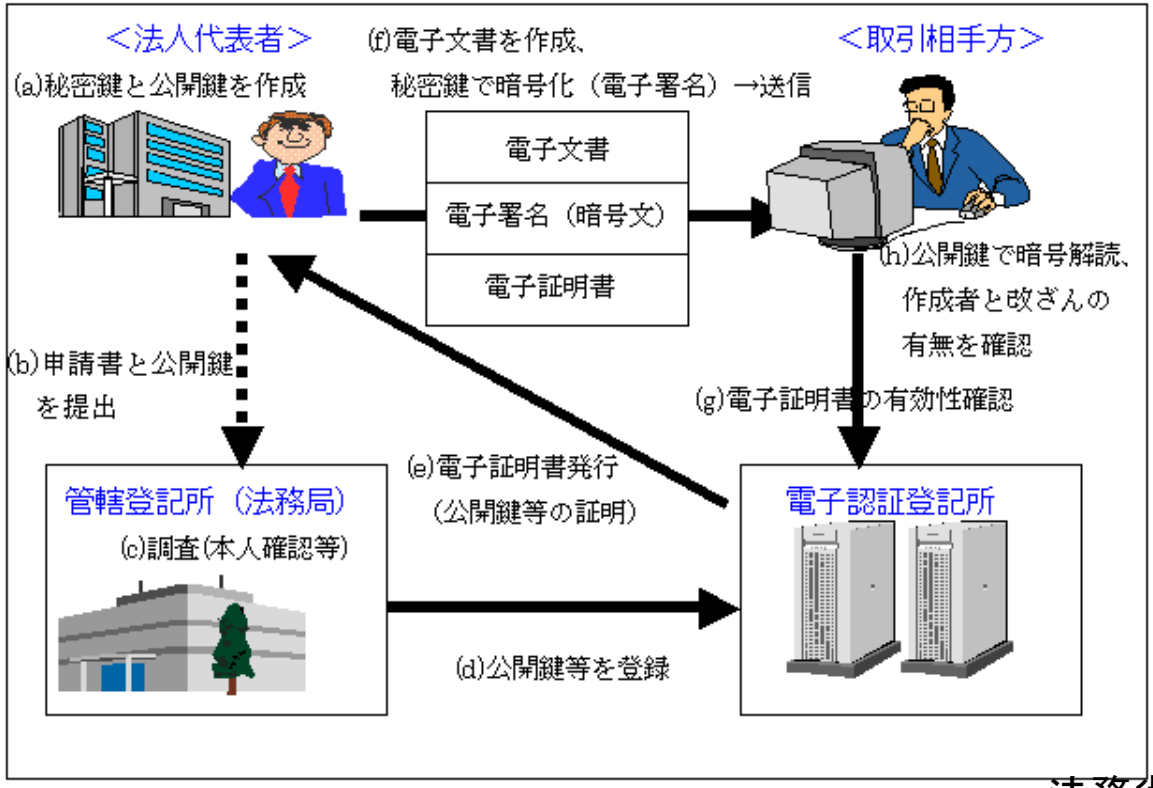
出所：公的認証サービス都道府県協議会「公的認証サービス利用者ガイド」

認証の仕組み（公的認証の例）



商業登記に基づく電子認証

- 企業取引において取引相手の「本人性」「法人の存在」「代表権限の存在」を確認するために、登記所が発行する証明書が利用される。



法務省民事局「howTV」

暗号化と著作権保護

- 音楽配信に伴って，暗号化技術を応用した著作権保護が行われるようになってきた.
- DRM：デジタルデータ（音楽など）の著作権保護（複製や利用を制限）する技術の総称。ネットからキーをダウンロードするものやハードそのものDRM機能を組み込む方式がある。
- DVDレコーダーの普及に伴い，暗号化技術CPRM（Content Protection for Recordable Media）によるコピー（ダビング）防止が図られるようになってきている.
- 再生専用メディアにはCPPM（Content Protection for Prerecorded Media） という方式が用意されている.
- デジタル放送も同様にCPRMによってプロテクトされているものが多い.

デジタルネットワークにおける権利保護に暗号の果たす役割

- 共通鍵方式（秘密鍵方式）と公開鍵方式
  - DES：共通鍵方式
  - RSA：公開鍵方式
- ブラウザの右下の鍵マークはSSL保護付きの意味である。（128ビット、VeriSign社のRSA）

絶対破られない暗号－量子暗号－

- 量子物理学を応用した量子暗号が実用化の段階を迎えている。
- 現在主流の公開鍵暗号方式は、コンピュータの飛躍的な発展や、数学上の発展（特に素数に関する）があった場合、簡単に破られるようになる恐れがある。
- 残された課題は、長距離を通信させること。応用したソフトや機器の普及がこれからであることである。