情報セキュリティと情報の暗号化

情報Ⅰ　第43回授業

06情報通信ネットワークのしくみ

対応ファイル：23exp43.xls

復習

- インターネットは、世界中の人が集まる場所
- インターネット上は、「ハガキ」程度のセキュリティ
- 悪意をもった人も中には存在
- それぞれの「しくみ」に応じたセキュリティ対策が必要！
- 悪意の「手口」を理解し、「身を守る」方法につなげる！

情報セキュリティ対策の3つの側面

- 技術的な側面
  - 機器やソフトウェア等を用いて対策
- 人的・組織的な側面
  - 利用者の教育や啓発を行うことによる対策
- 法的な側面
  - 不正アクセス禁止法などによる対策

情報セキュリティ対策の3つの側面

- 技術的な側面
  - 機器やソフトウェア等を用いて対策
- 人的・組織的な側面
  - 利用者の教育や啓発を行うことによる対策
- 法的な側面
  - 不正アクセス禁止法などによる対策

技術的な対策

- 対策の例（P.176～）
  - ファイアウォール
    - ルータや専用ソフトウェアの導入
    - パケットフィルタリング（不正なパケットの遮断）
  - セキュリティホールの修復
    - OSやソフトウェアのアップデート
  - ウイルス対策ソフトウェアの導入
  - 暗号化
    - ネットワーク上では簡単に「盗聴」できてしまう

      → 知られてもすぐには分からないように「暗号化」する

暗号の必要性（p.178～）

特定の相手にのみ情報を伝達したいが、その他の人にも知られてしまう可能性がある場合

例）

- 試合で見方だけに作戦を伝えたい

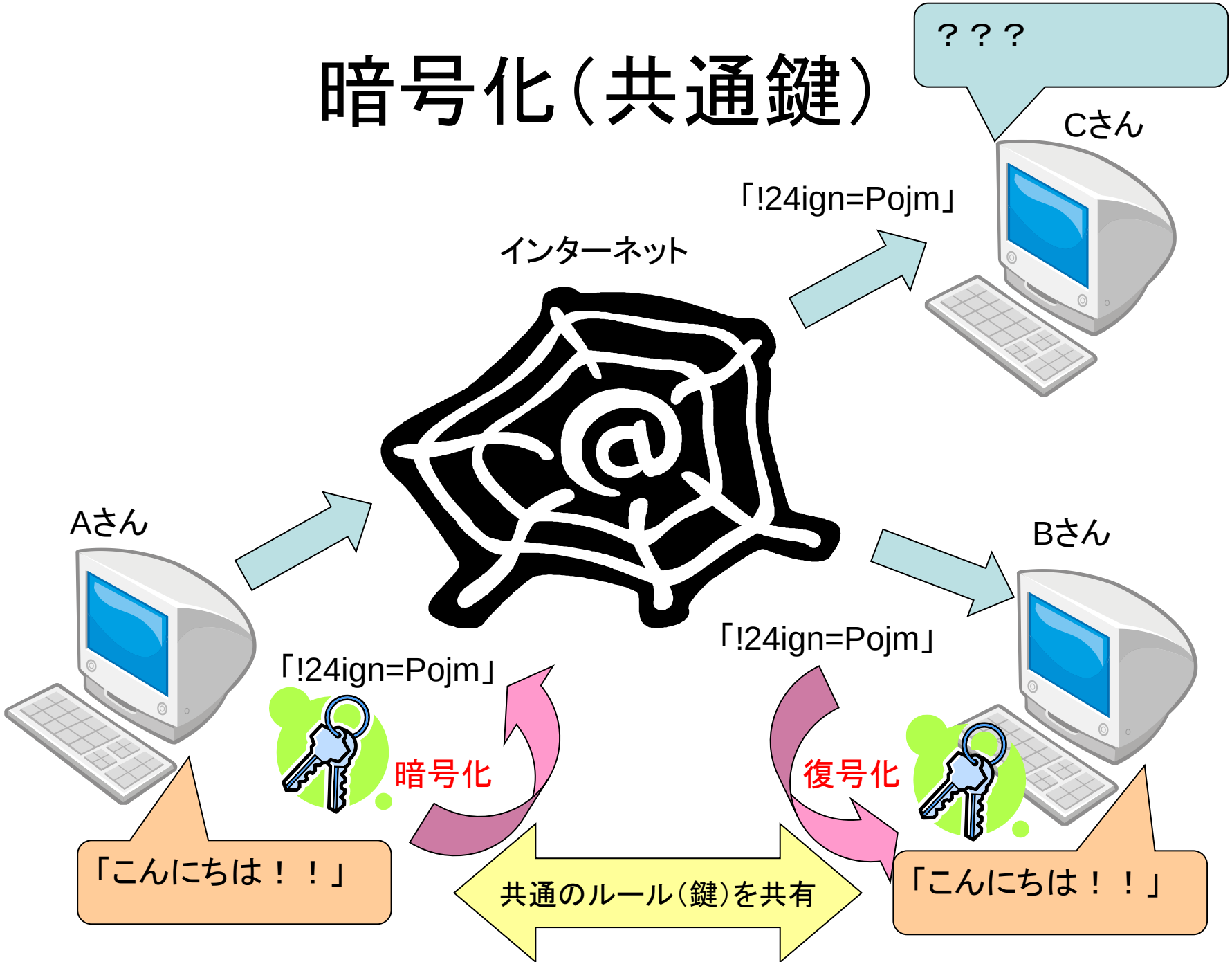
暗号化の例

- 特定の「方式」と「ルール」を秘密裏に共有する
  - まこやんにやちまやは
    - 鍵　：　ブドウ、モモ
  - はおはげんはきでははすはか
    - 鍵　：　speaking
- 自分（相手）しか解読できない「しくみ」を使う
  - あとで説明

共通鍵暗号方式（P.178）

- シーザー（カエサル）暗号
  - 「Khoor」
    → 「Hello」
  - 「むてづ」
    → 「まちだ」（鍵：ー2）
  - 一般的に、辞書順に3文字「ずらした」ものだが、3文字以外でも「シーザー暗号」と呼ぶことがある。
  - このように、文字を置き換える暗号を「換字式暗号」ともいい、専用の「読替表」が用いられることもある。（→ この「読替表」が「共通鍵」となる）

暗号化（共通鍵）


？？？
Cさん
「!24ign=Pojm」
インターネット
Aさん
Bさん
「!24ign=Pojm」
「!24ign=Pojm」
暗号化
復号化
「こんにちは！！」
共通のルール（鍵）を共有
「こんにちは！！」

共通鍵暗号方式の弱点

使う人全員が共通の鍵　→「家の鍵」をイメージすると・・・

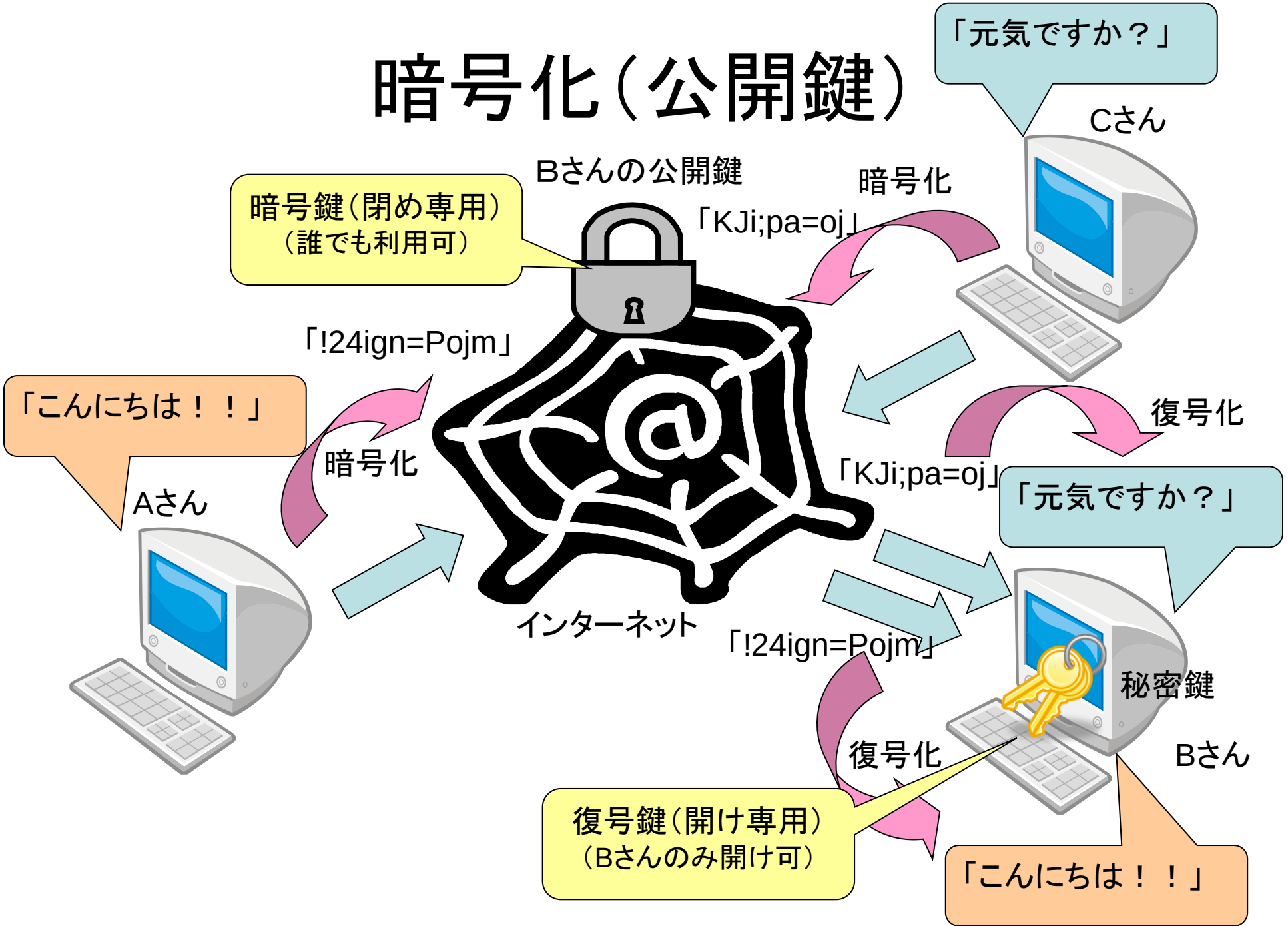
- 鍵を落としたら全員取り替え
- 扉の数だけ鍵の種類が必要
  - やりとりする相手の数だけ鍵の種類が必要
- 【大問題！】事前に「鍵」を相手に渡しておく必要性
  - ネットショッピングなど、「会ったことがない」場合はどうする？

・・・・・　など

公開鍵暗号方式（P.178）

- 自分専用の「閉めるためだけの鍵（暗号鍵）」をだれでも使えるように広く公開（公開鍵）
- 「開けるためだけの鍵（復号鍵）」を自分だけが秘密裏に持つ（秘密鍵）
- 途中で誰かに盗聴されても、開けられるのは自分だけ
- 鍵も、自分宛てのもの1つで良い！

暗号化（公開鍵）


「元気ですか？」
Cさん
Bさんの公開鍵
暗号鍵（閉め専用）
（誰でも利用可）
暗号化
「KJi;pa=oj」
「!24ign=Pojm」
「こんにちは！！」
暗号化
Aさん
「KJi;pa=oj」
復号化
「元気ですか？」
インターネット
「!24ign=Pojm」
秘密鍵
復号化
Bさん
復号鍵（開け専用）
（Bさんのみ開け可）
「こんにちは！！」

公開鍵暗号方式の応用（逆の発想）

- 自分専用の「復号鍵（開けるためだけの鍵）」をだれでも使えるように広く公開（公開鍵）
- 「暗号鍵（閉めるためだけの鍵」を自分だけが秘密裏に持つ（秘密鍵）
- 公開された鍵で開けられるのは自分が閉めた鍵だけ

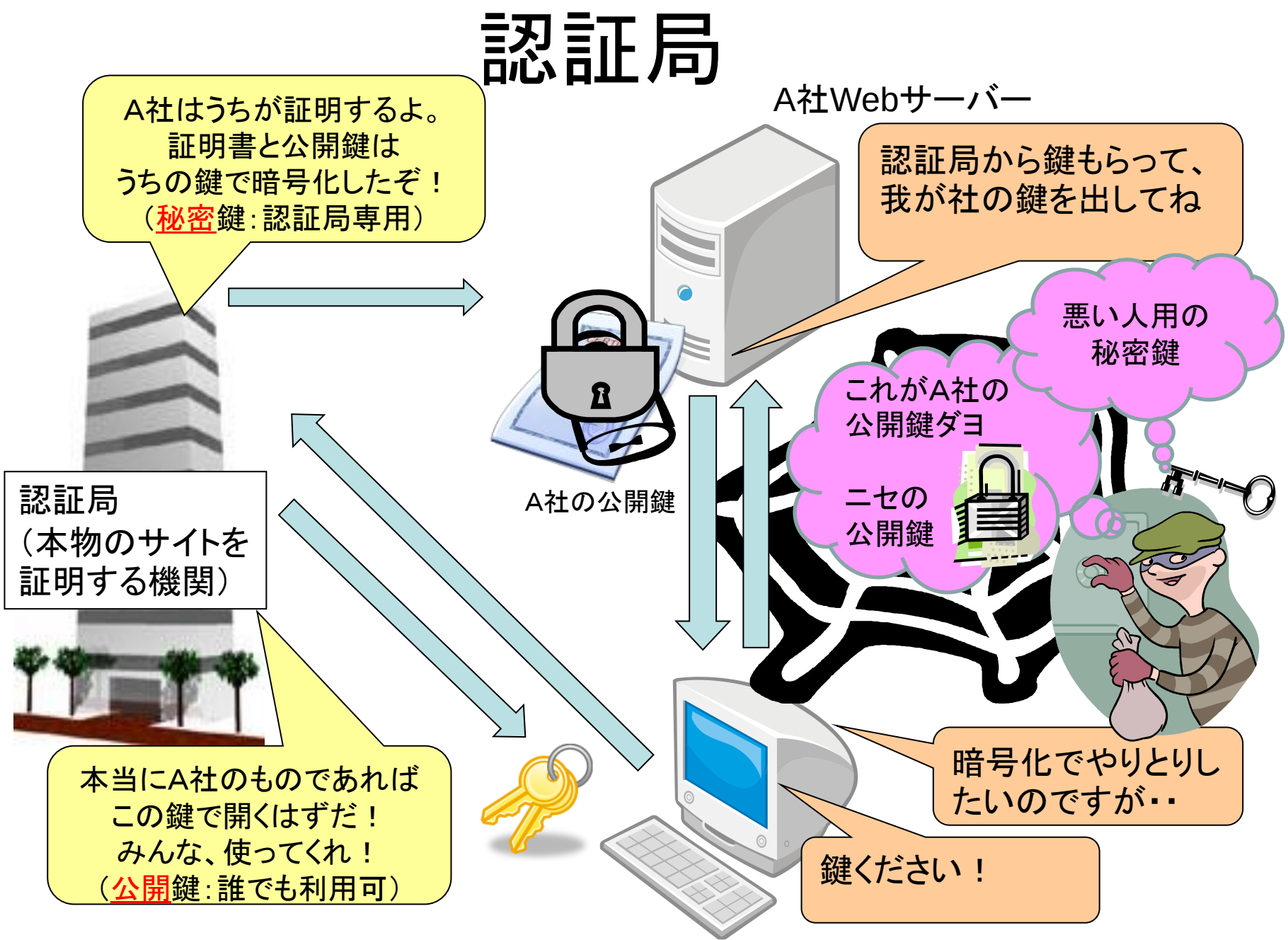
→ 「自分が閉めた」、即ち「自分のデータ」と言えるのでは!?

※実際には、「証明書」の添付など、さらなる「仕組み」が必要！

公開鍵暗号方式の弱点

- そもそも、そんな鍵って作れるの？
  - 「ある式の計算」はすぐにできるが、「逆の計算」は時間がかかり解読するのに非現実的なもの
  - 「素因数分解」などの計算を利用（→ RSA暗号など）
  - 複雑な計算が必要となるため高速処理が難しい
    - ただし、「量子コンピュータ」が実用化されたら比較的簡単に開けられる
      → 「量子暗号」など、最新の暗号が検討されている
- この鍵は本当にその人の鍵？
  - 「ニセの鍵」が出てきたら・・・

認証局


A社はうちが証明するよ。
証明書と公開鍵は
うちの鍵で暗号化したぞ！
（秘密鍵：認証局専用）
A社Webサーバー
認証局から鍵もらって、
我が社の鍵を出してね
悪い人用の
秘密鍵
これがA社の
公開鍵ダヨ
ニセの
公開鍵
A社の公開鍵
認証局
（本物のサイトを
証明する機関）
本当にA社のものであれば
この鍵で開くはずだ！
みんな、使ってくれ！
（公開鍵：誰でも利用可）
暗号化でやりとりし
たいのですが・・
鍵ください！

メリットとデメリット

	メリット	デメリット
共通鍵方式	・暗号化・復号化が同じ鍵なので速度が速い。	・事前に鍵を渡しておく必要がある。 ・相手の数だけ鍵が必要。
公開鍵方式	・1つの鍵を公開すれば良いので、多数の相手とやりとりしやすい。	・鍵を作成するのに数学的な処理が必要で、高速処理が難しい。

※実際の処理では、双方の長所を組み合わせ短所を補って通信を行っていることが多い。（ハイブリッド方式）

まとめ

情報セキュリティ対策

- 暗号化などの対策
  - 共通鍵暗号方式
    - 互いに同じ暗号鍵・復号鍵を持って共有する
  - 公開鍵暗号方式
    - 暗号鍵と復号鍵を別々にする
      - 暗号鍵は公開、復号鍵は自分が秘密に持つ
    - 復号鍵を公開、暗号鍵を秘密に持つ
      - 公開鍵暗号方式と逆バージョン
      - 他の技術と合わせ、「自分が差出人」であることを示せる