

情報セキュリティと情報の暗号化

情報の科学 第18回授業

03ネットワークがつなぐコミュニケーション

対応ファイル: 21exp18.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

技術的な対策

- 対策の例 (P.74～75)
 - 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 of 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.76～)

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

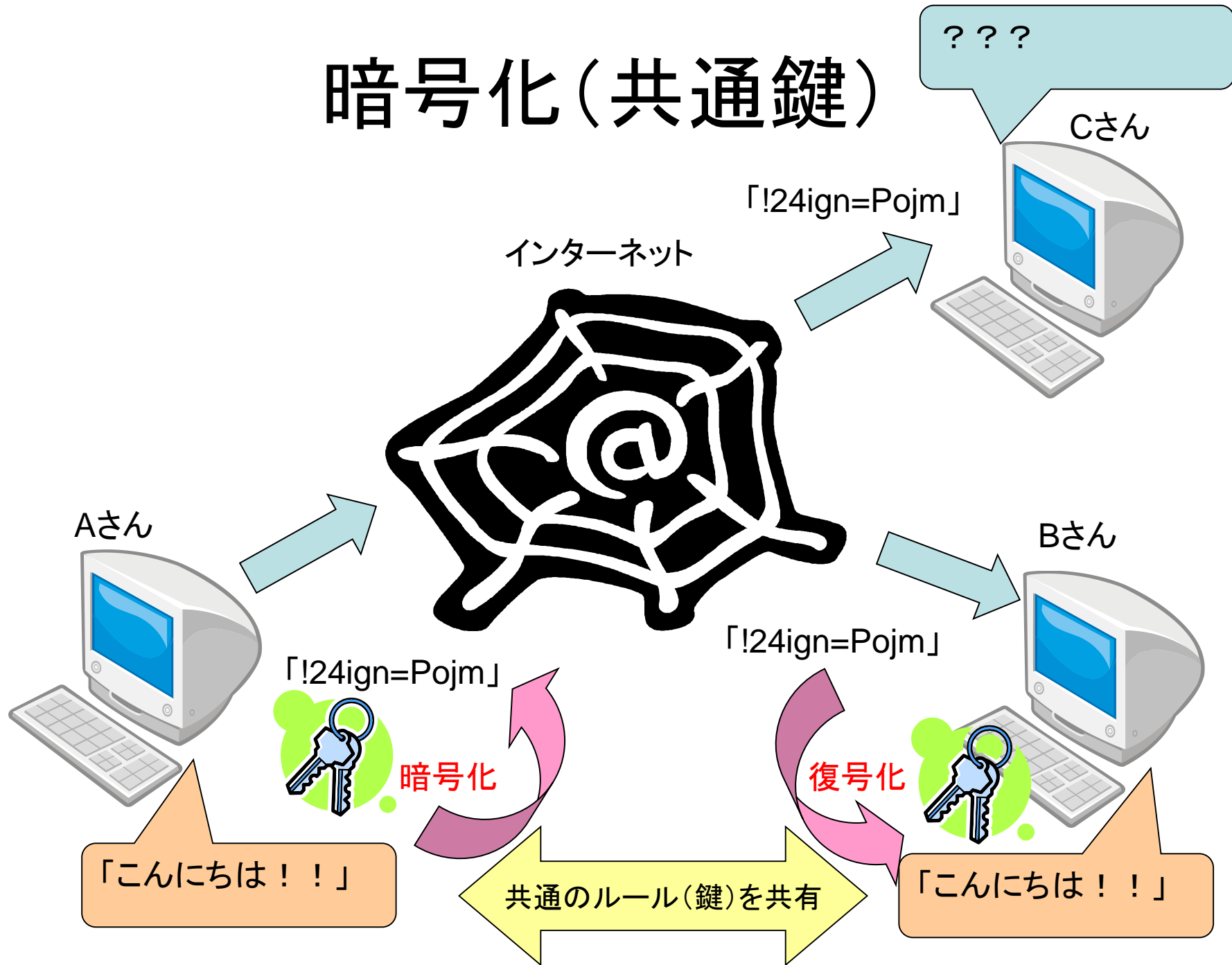
- 特定の「方式」と「ルール」を共有する
 - まこやんにやちまやは
 - 鍵 : ブドウ、モモ
 - はおはげんはきでははすはか
 - 鍵 : speaking
- 自分(相手)しか解読できない「しくみ」を使う
 - あとで説明

シーザー(カエサル)暗号(p.76)

- 「K hoor」
→ 「Hello」
- 「むてづ」
→ 「まちだ」 (鍵: -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

暗号化(共通鍵)



共通鍵方式の弱点

使う人全員が共通の鍵

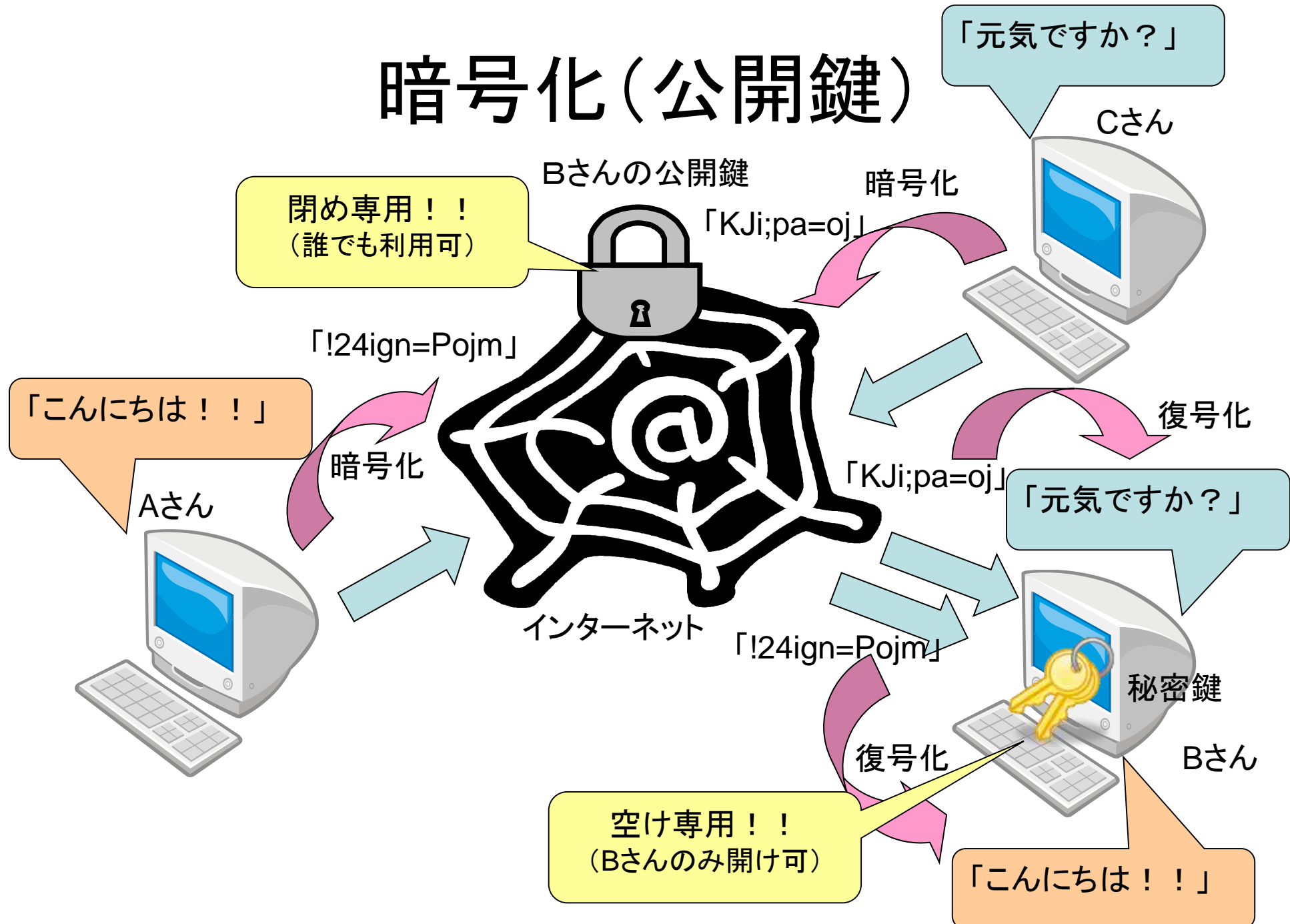
→ 「家の鍵」をイメージすると…

- 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
- 【大問題！】事前に「鍵」を相手に渡しておく必要性
 - 遠くに住む親戚に渡したい時はどうする？
 - など

公開鍵暗号方式

- 自分専用の「閉めるためだけの鍵」をだれでも使えるように広く公開（公開鍵）
- 「開けるためだけの鍵」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、自分あてのもの1つで良い！

暗号化(公開鍵)



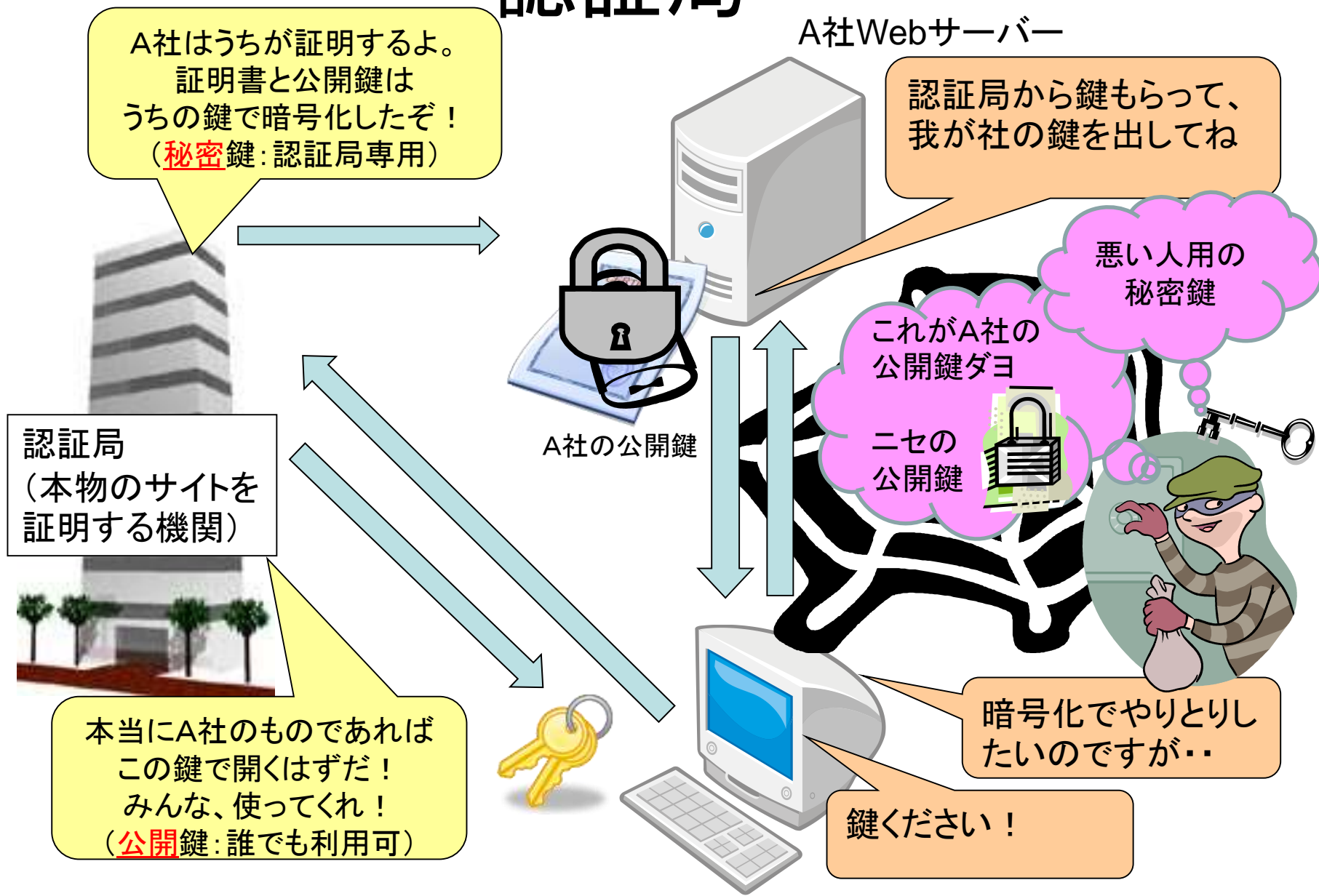
デジタル証明

- 自分専用の「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）
- 「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」、すなわち自分のデータという「証明」
※実際には、「証明書」の添付など、さらなる「仕組み」あり

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(p.77)
 - 複雑な計算が必要となるため高速処理が難しい
- 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



メリットとデメリット

	メリット	デメリット
共通鍵方式	<ul style="list-style-type: none">・暗号化・復号化が同じ鍵なので速度が速い。	<ul style="list-style-type: none">・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	<ul style="list-style-type: none">・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。	<ul style="list-style-type: none">・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

- 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
 - 巧妙化する犯罪や技術の進歩に対応する法律の整備

→ あらゆる側面からの対策・対応の必要性