情報セキュリティ
情報セキュリティ技術の活用

情報の科学　第4回授業

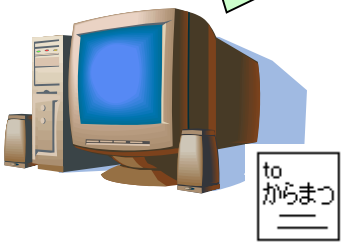
02ネットワークがつなぐコミュニケーション

前回（第3回）の復習

- インターネットは、ネットワークの集まり
- ネットワークごとに、ルータがある
- 「アドレス帳」のようなDNSサーバがある

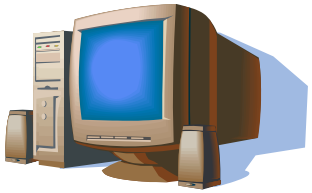
送ったらネットワーク内の
全員に届いちゃうから、
「からまつ」さんだけひろってね

あじさい



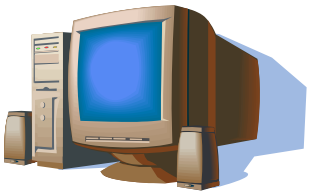
私あてじゃないから
捨てよう

いちょう

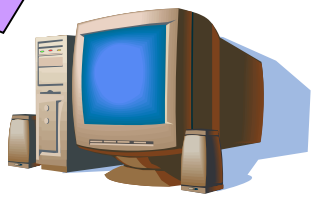


私あてじゃないから
捨てよう

うぐいす



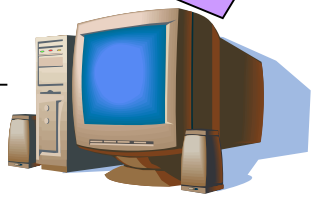
私あてじゃないから
捨てよう



えのぐ

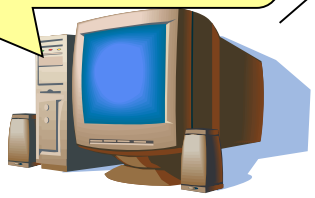
ハブ

私あてじゃないから
捨てよう



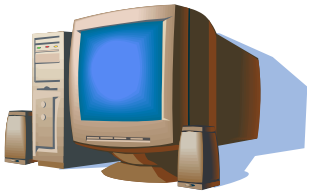
おおわし

おっと、俺あてだ。
とっておこう。



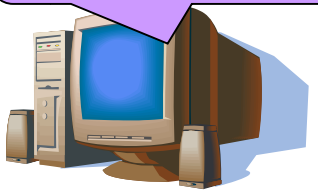
からまつ

私あてじゃないから
捨てよう

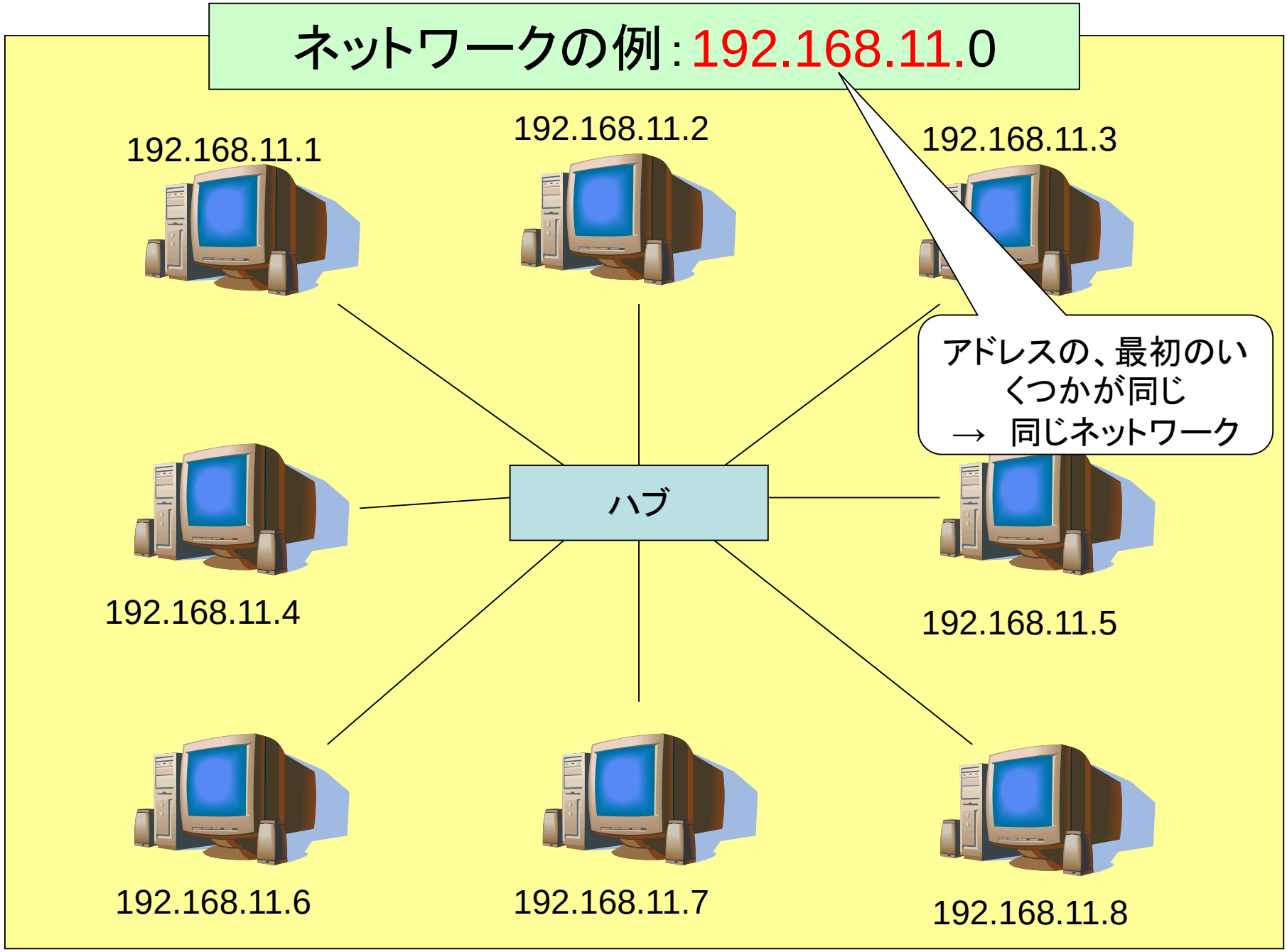


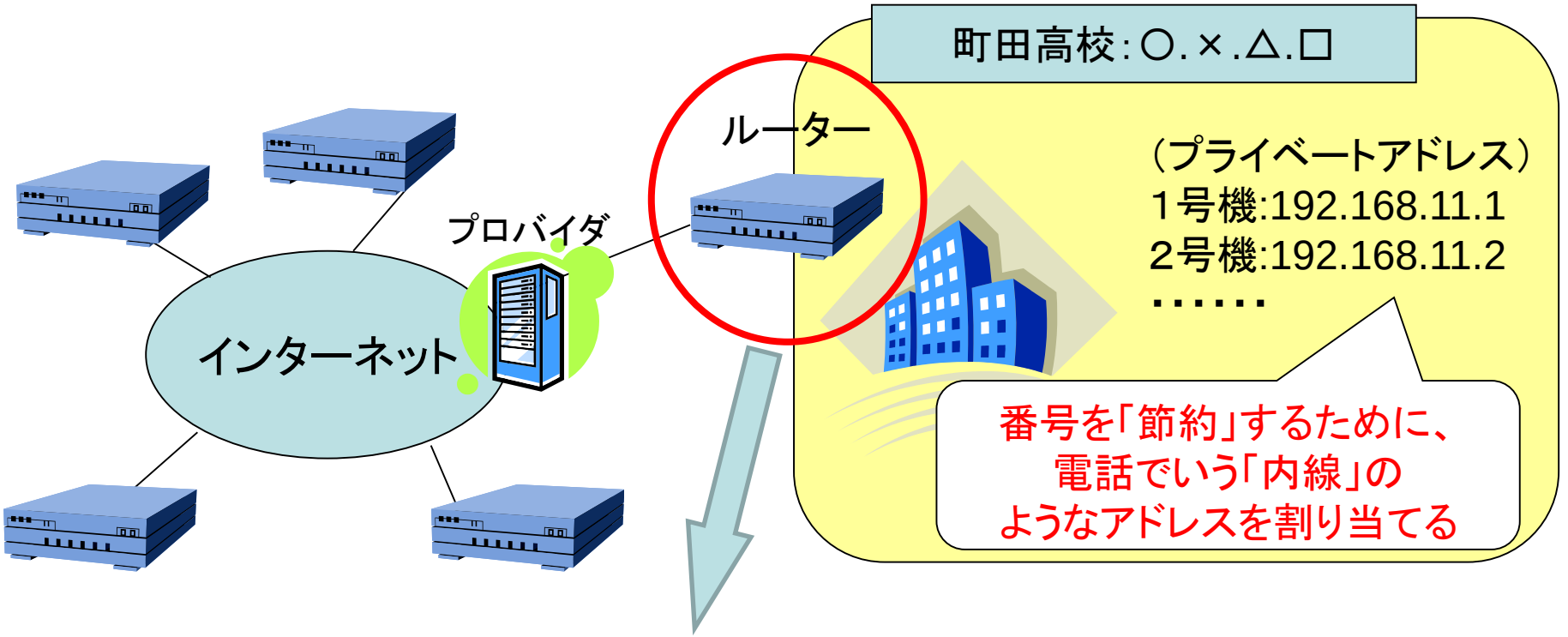
きりぎりす

私あてじゃないから
捨てよう



くすのき


ネットワークの例：192.168.11.0
192.168.11.1
192.168.11.2
192.168.11.3
アドレスの、最初のいくつかが同じ
→ 同じネットワーク
ハブ
192.168.11.4
192.168.11.5
192.168.11.6
192.168.11.7
192.168.11.8

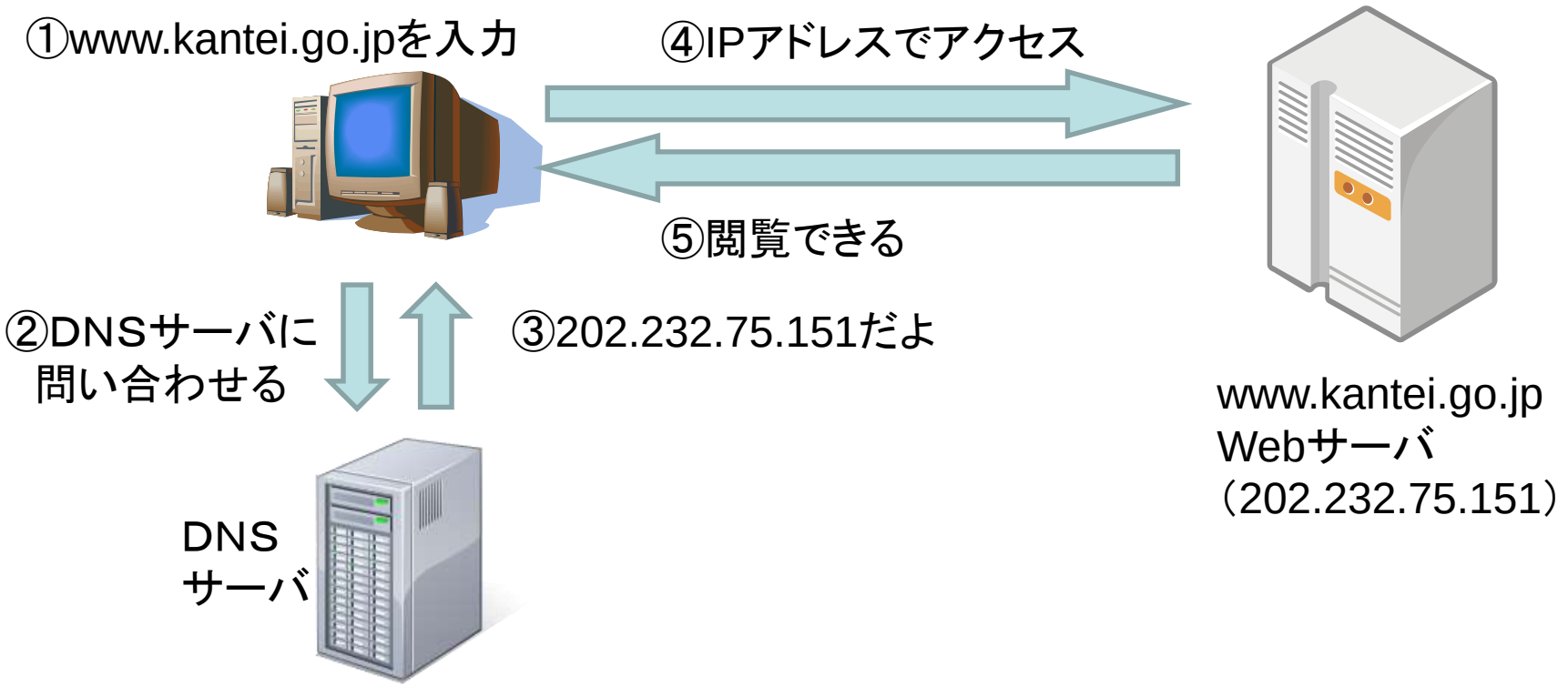


外部（WAN）へ
つなげる所

内部（LAN）へ
つなげる所
（ハブとしても使える）

DNS（p.51）

- IPアドレスとドメイン名を対応させるシステム
- 携帯の「アドレス帳」をイメージすると良い。



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
  - 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

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

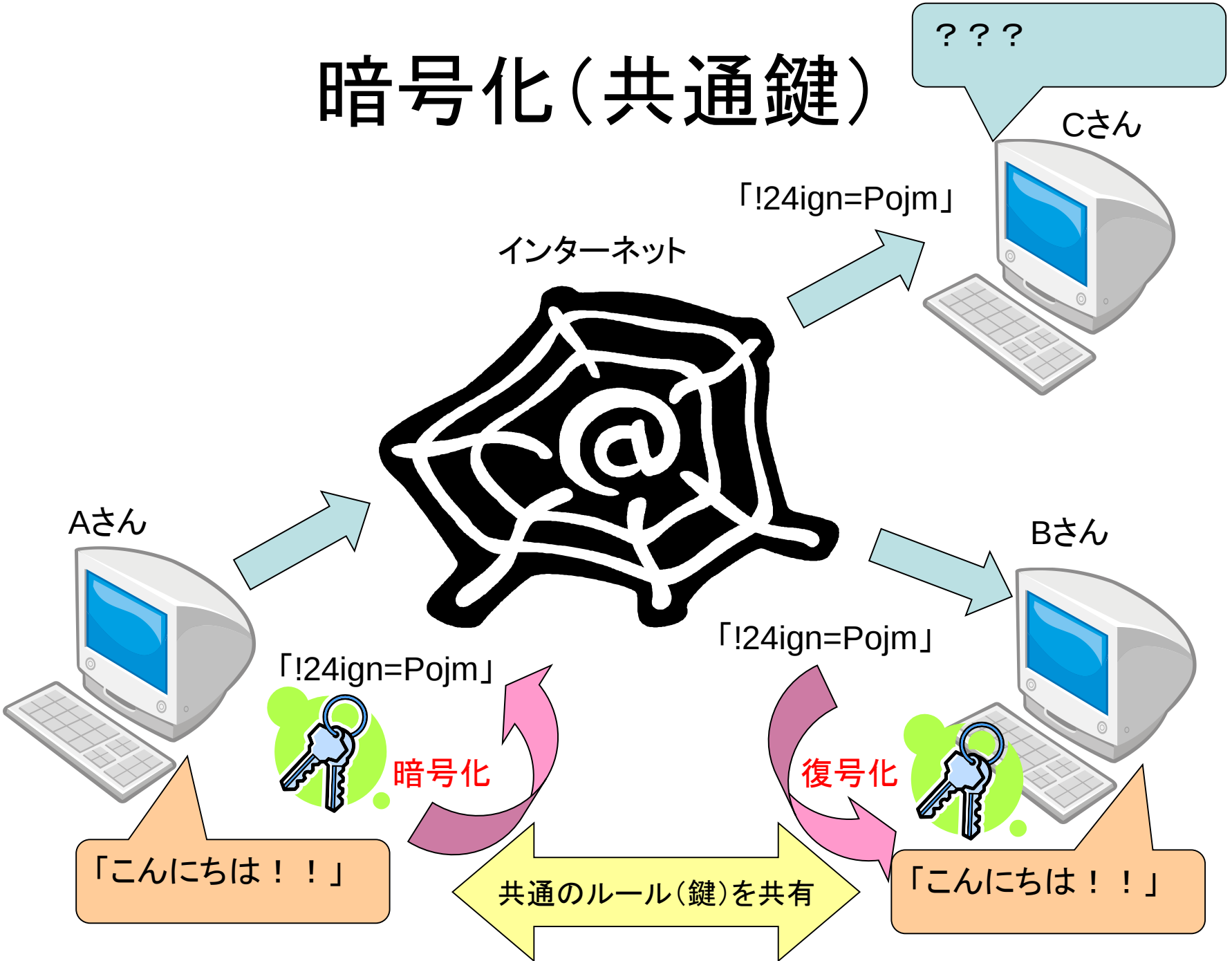
シーザー（カエサル）暗号

- 「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

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・・・

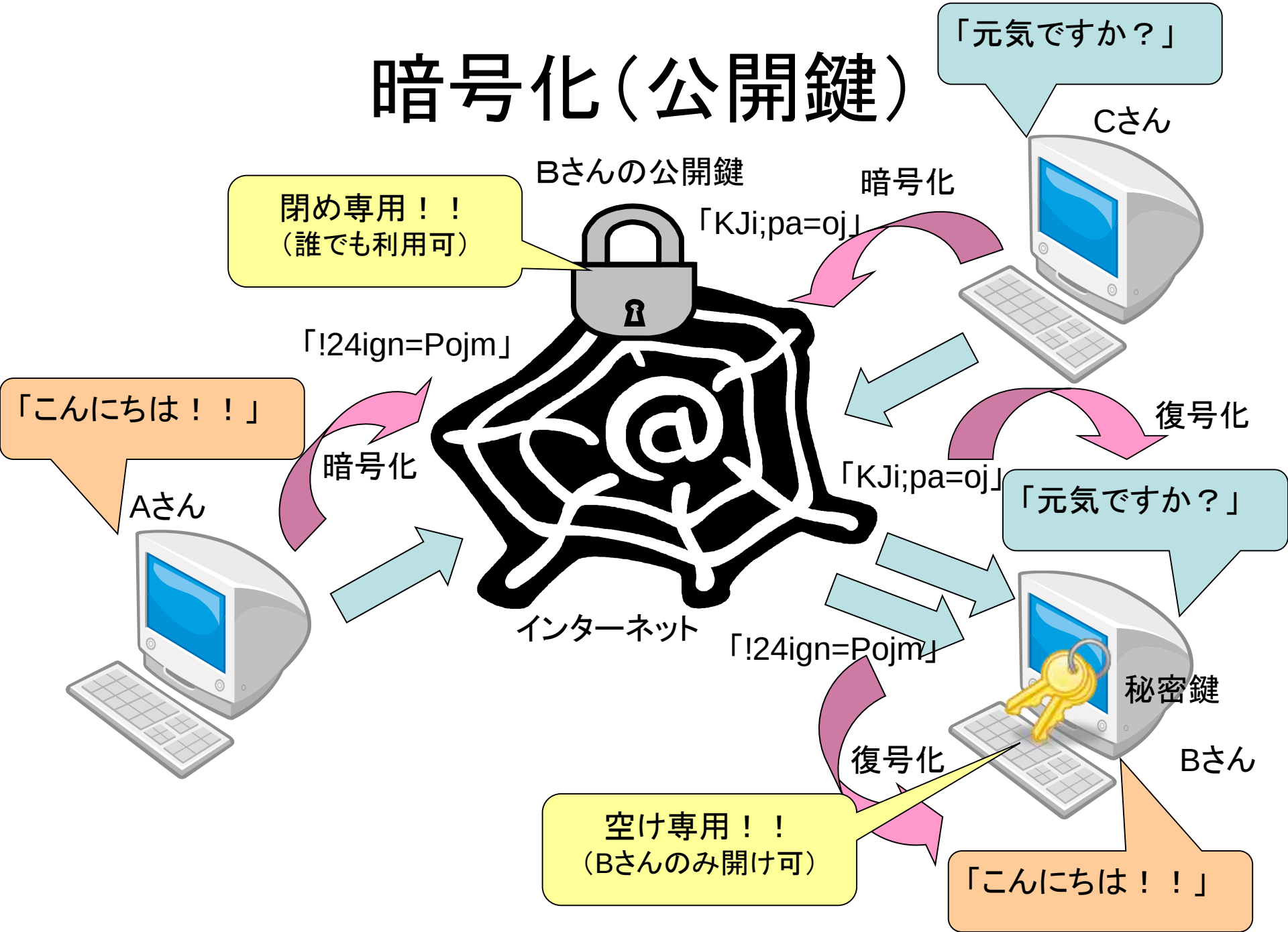
- 扉の数だけ鍵の種類が必要
- 鍵を落としたら全員取り替え
- 事前に「鍵」を相手に渡しておく必要性
  - 遠くに住む親戚に渡したい時はどうする？

・・・・・ 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

暗号化（公開鍵）


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

ディジタル証明

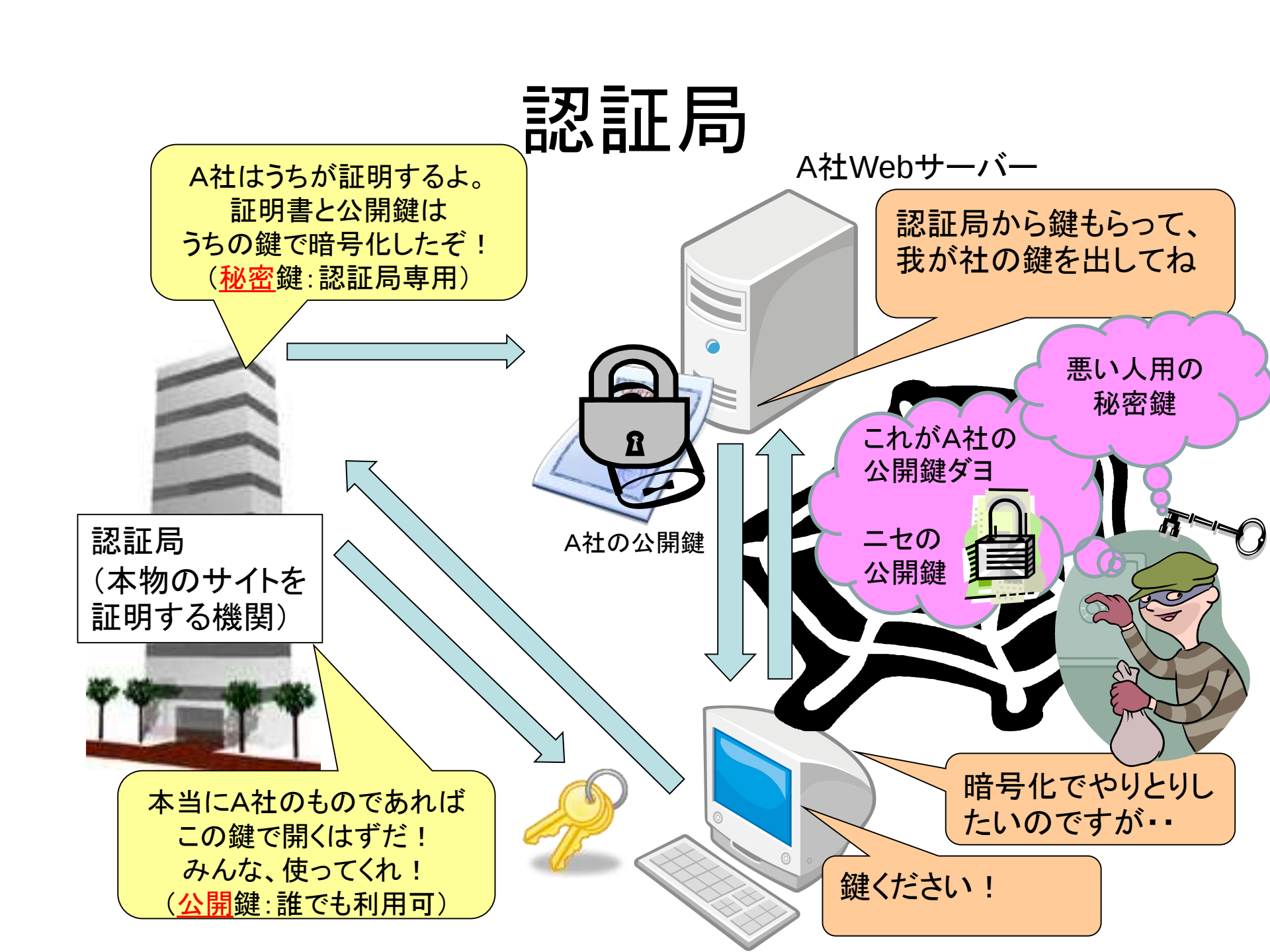
- 自分専用の「開けるためだけの鍵」をだれでも使えるように広く公開（公開鍵）
- 「閉めるためだけの鍵」を自分だけが秘密裏に持つ（秘密鍵）
- 公開された鍵で開けられるのは自分が閉めた鍵だけ

→ 「自分が閉めた」、すなわち自分のデータという「証明」

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
  - 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


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。

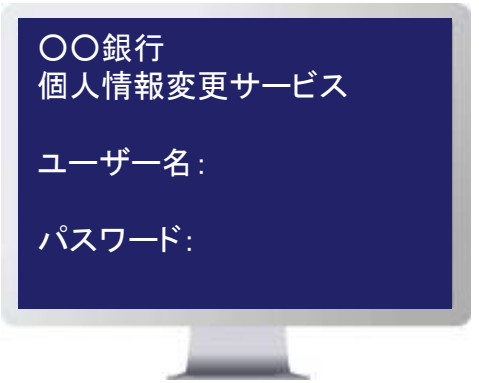
※実際の処理では、双方の長所を組み合わせ短所を補って通信を行っていることが多い。（ハイブリッド方式）

SSL（P.78）

- ハイブリッド暗号の1つで、「https://」で始まる
- 重要な情報をやりとりする時には確認を！

フィッシング詐欺

本物のサイト



②アクセス

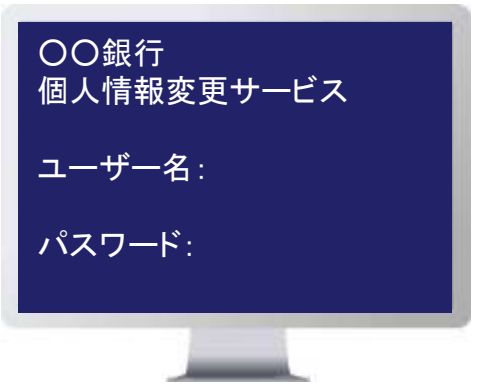
①ニセ
メール

〇〇銀行より

あなたのアカウントが凍結されました！
すぐに以下にアクセスを！

http://www.usonosaite.com/account/・・

ニセのサイト



③ニセのサイトから情報ゲット

認証技術による対策（P.73）

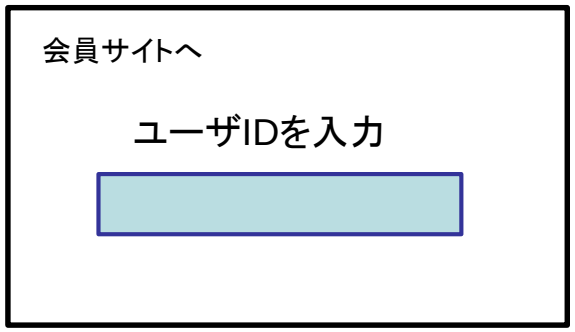
- パスワードの運用
- いろいろな認証技術
  - 生体情報（指紋・静脈など）
  - 記憶情報（パスワード、パターンなど）
  - 所持情報（スマートフォン、トークン）
- 二要素認証、二段階認証

認証技術の例1（パターン）

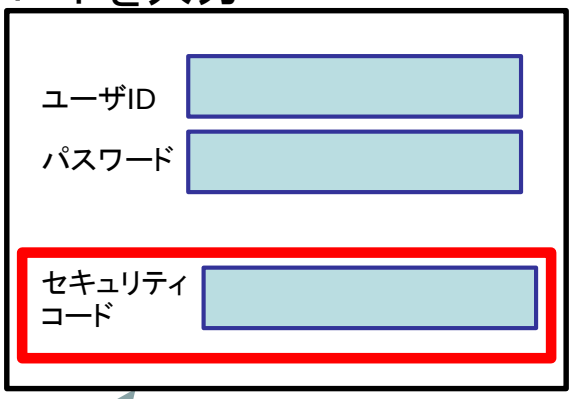
認証技術の例2

- 二要素認証

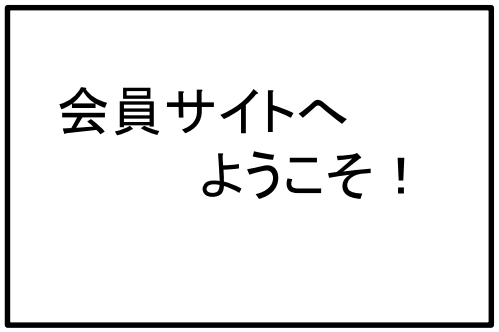
1．IDを入力



3．パスワードとセキュリティコードを入力



4．認証完了



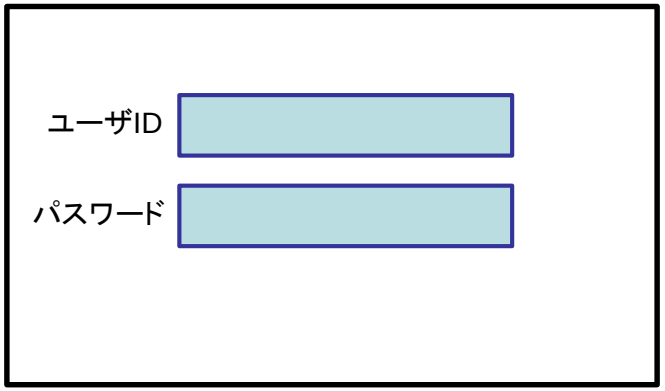
2．登録携帯にSMS等でセキュリティコードを配信

記憶情報（パスワード）と所持情報（スマートフォン）の二要素で認証

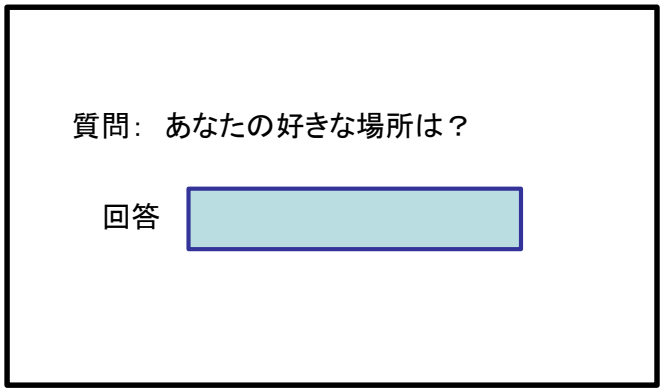
認証技術の例3

- 二段階認証

1. パスワードとパスワードを入力



2. あらかじめ登録してある合言葉（秘密の質問）に回答



記憶情報（パスワード）の後、さらに記憶情報（合言葉）の二段階で認証

情報セキュリティ対策（つづき）

- 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

情報セキュリティの3要素（P.72）

- 機密性
  - パスワードの設定
  - 立ち入り禁止区域の設定
- 完全性
  - ディジタル署名
- 可用性
  - ディスクの多重化（RAID）
  - 無停電電源装置（UPS）

ソーシャルエンジニアリング

- 盗み見たり、ある人物を装うなどして、社会的な手段で不正に情報を得ること。
  - 身分を偽ってパスワードを聞き出す
  - 入力している所を背後から盗み見る
  - パスワードを書いて貼っているものを見る

    ・・・など

ソーシャルエンジニアリング

- 2011年のある企業による調査結果
  - 「脅威（＝恐ろしくおびやかす存在）」と認識
    - ９７％（セキュリティ担当者）
    - ８６％（ITセキュリティ担当者）
  - 実際に攻撃にあった：４３％
  - 被害にあっていないと確信：１６％
  - 攻撃にあったかどうかわからない：４１％

情報セキュリティ対策（つづき）

- 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

【復習】不正アクセス禁止法
（平成25年改正）

- 主な内容（詳細は下部の総務省リンクにて）
  - 三年以下の懲役または百万円以下の罰金
    - 他人のID・パスワードで「なりすまし」ログオン
    - セキュリティホールを突くなどして不正にログオン
  - 一年以下の懲役または五十万円以下の罰金
    - 不正目的で他人のID・パスワードを不正に取得
    - 他人のID・パスワードを別の人に教える
    - 不正目的で不正取得した他人のID・パスワードを保管
    - 本物に似せたサイトに誘導しID・パスワードを騙し取る（いわゆる「フィッシング」）

総務省「国民のための情報セキュリティサイト」
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/09.html