2018. 1.23

情報ネットワーク

Ibaraki Univ. Dept of Electrical & Electronic Eng.

Keiichi MIYAJIMA

今後の予定

期末試験までの予定

1月23日（火）IPを助けるプロトコルと技術2（レポート有）

1月30日（火）　まとめ（レポート無）

2月6日（火）　期末試験

IPを助けるプロトコルと技術2

セキュリティ

- セキュリティ対策

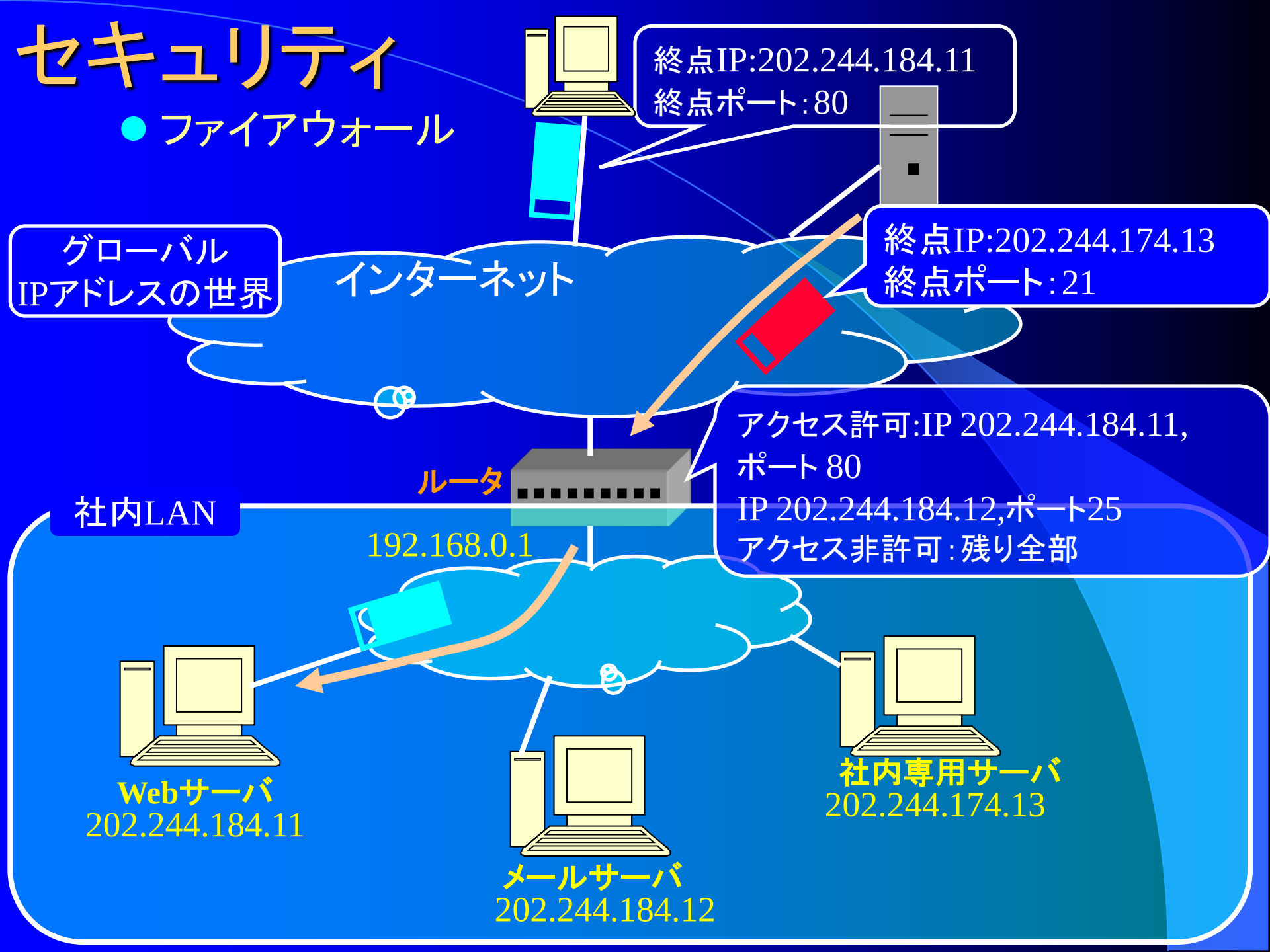
  個人の対策

  - アンチウイルスソフト
  - パーソナルファイアウォール

  無線LANを使う場合は、他人が屋外からアクセスできないようにする必要

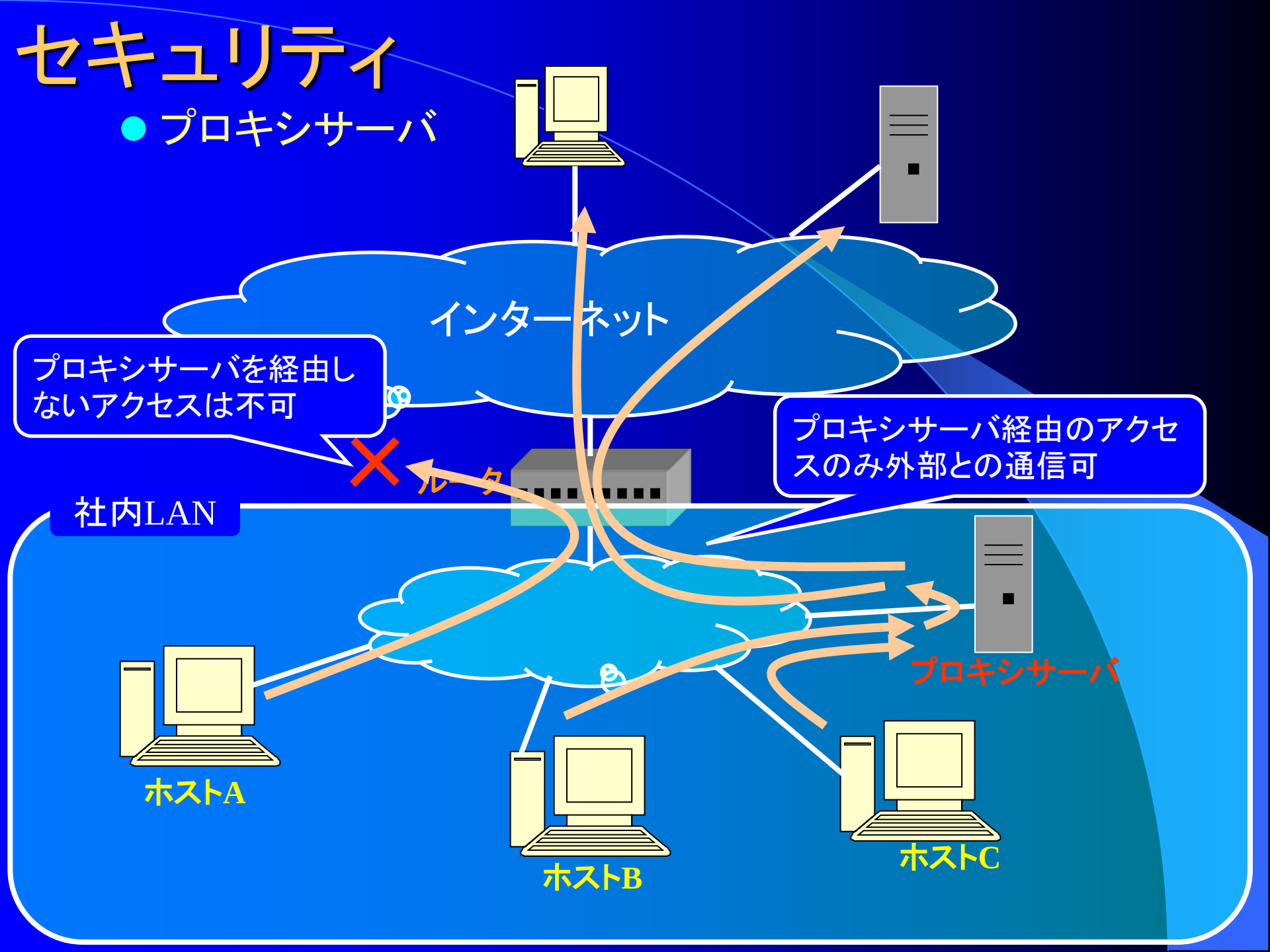
セキュリティ

- ファイアウォール



セキュリティ

- プロキシサーバ



暗号化

- 共通鍵暗号方式と公開鍵暗号方式

•共通鍵暗号方式

１つの共通鍵で鍵をかけたりあけたりする方式

•公開鍵暗号方式

秘密鍵と公開鍵の２つの鍵を使用し、

•秘密鍵で鍵をかけると公開鍵でしかあかない。

•公開鍵で鍵をかけると秘密鍵でしかあかない。

暗号化通信や、個人認証に使用

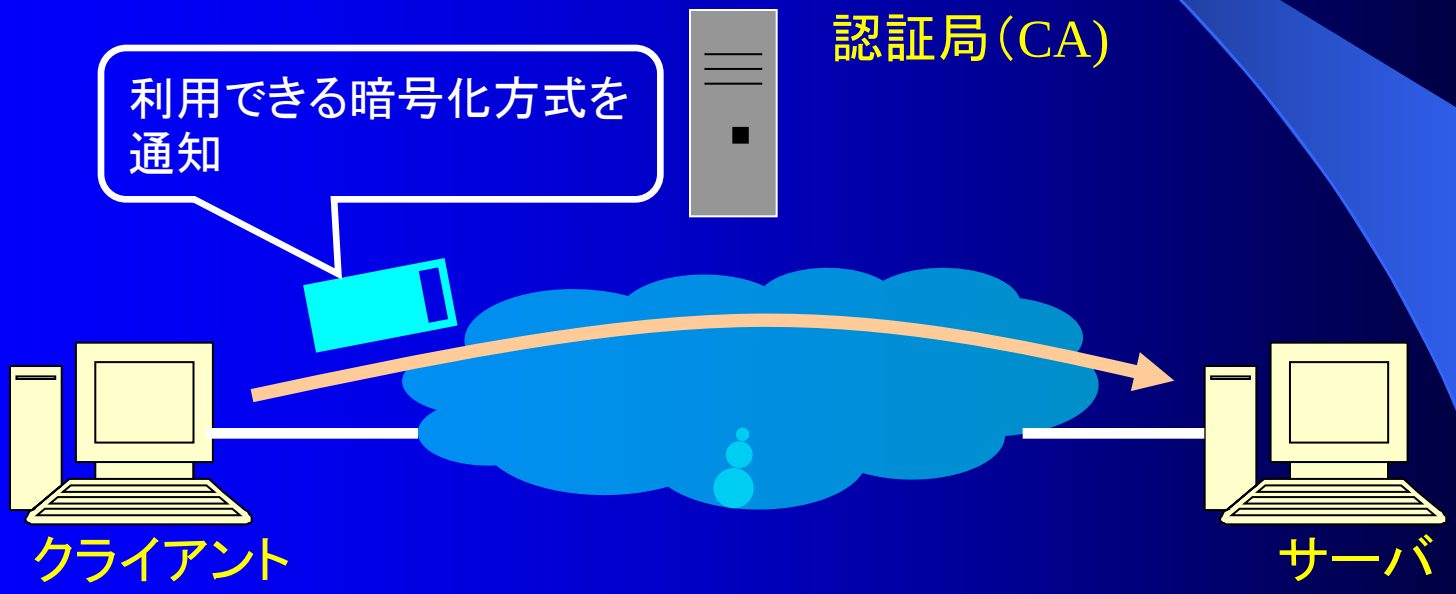
暗号化

- 暗号化を使った通信

  公開鍵暗号方式は便利だが、時間がかかるという欠点がある。

  そこで、

  「公開鍵暗号方式を使って共通鍵暗号方式の鍵を送る」



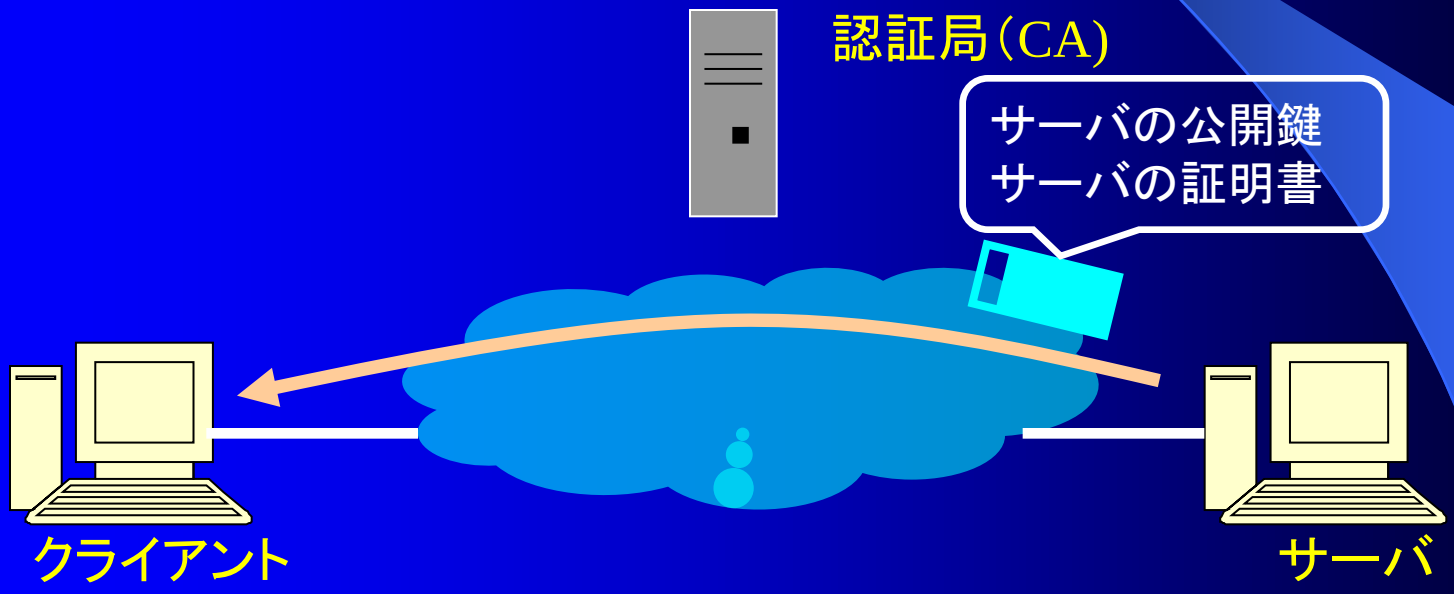
暗号化

- 暗号化を使った通信

  公開鍵暗号方式は便利だが、時間がかかるという欠点がある。

  そこで、

  「公開鍵暗号方式を使って共通鍵暗号方式の鍵を送る」



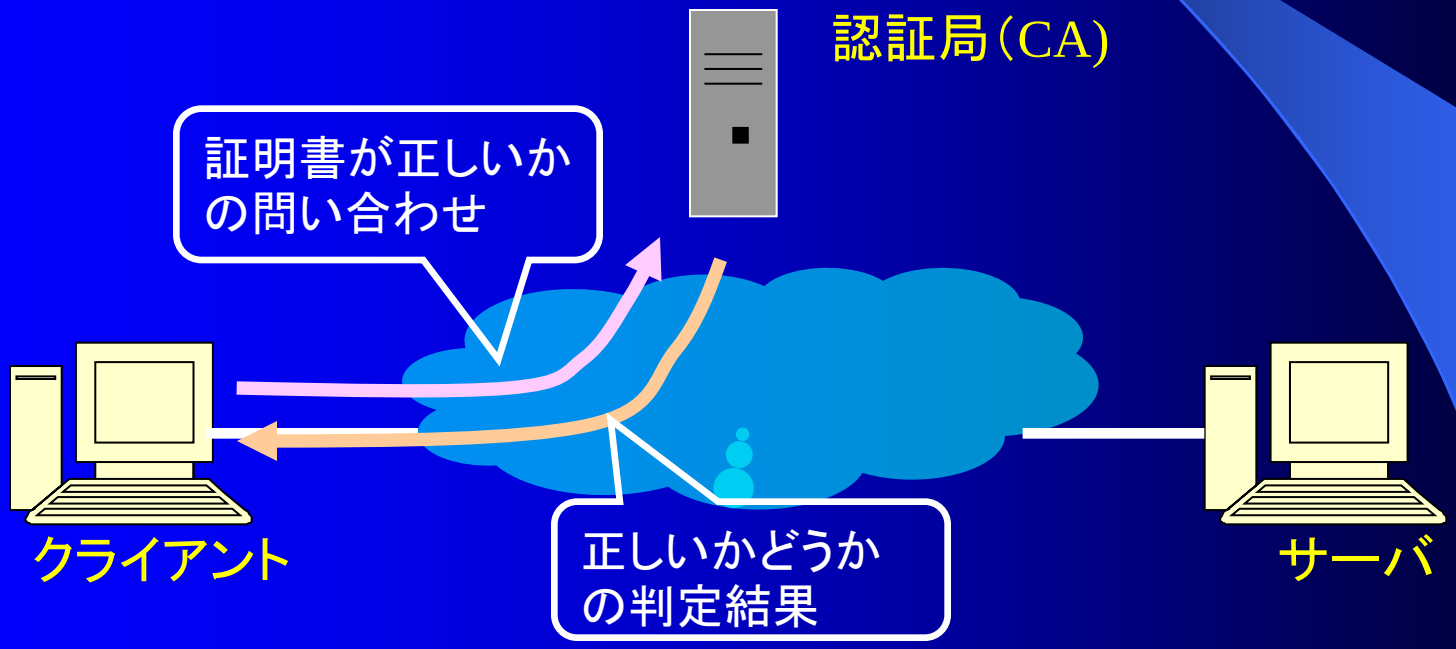
暗号化

- 暗号化を使った通信

公開鍵暗号方式は便利だが、時間がかかるという欠点がある。

そこで、

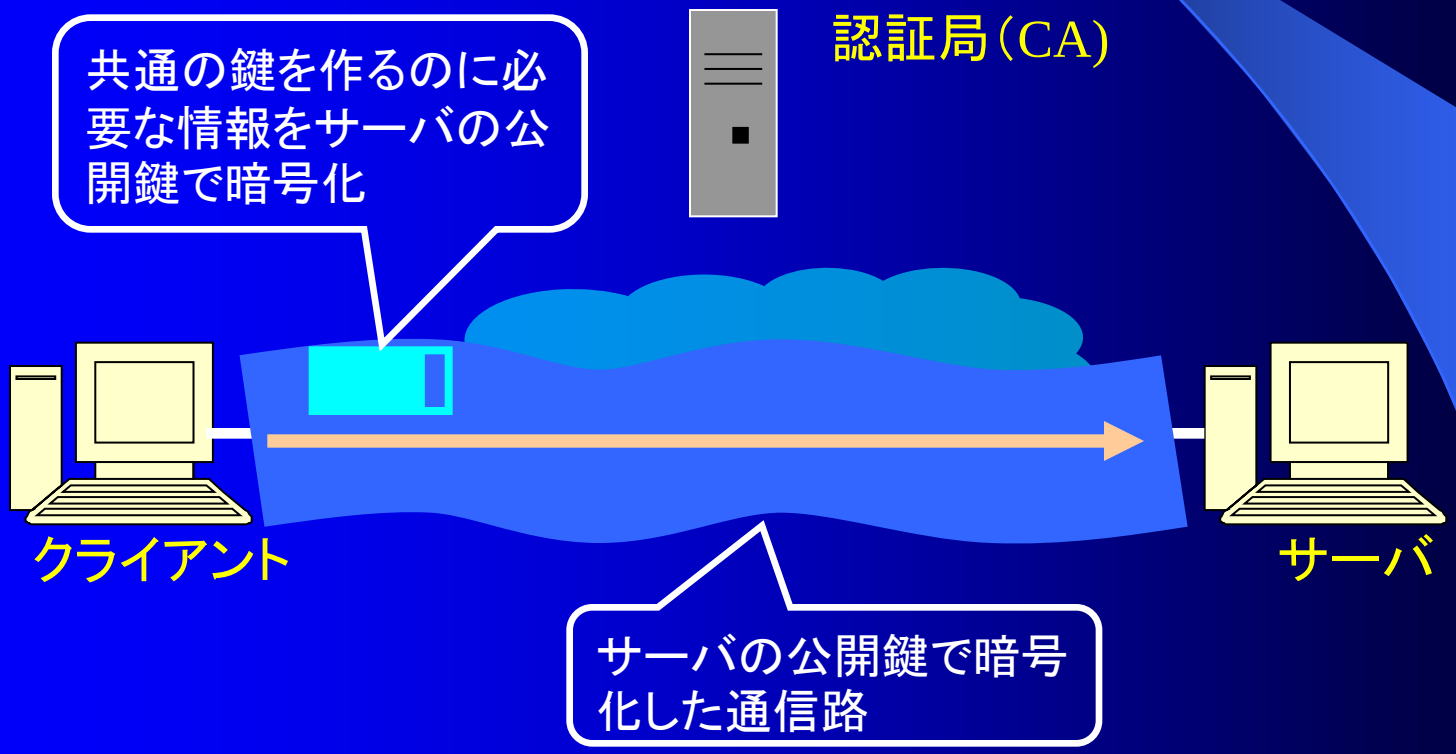
「公開鍵暗号方式を使って共通鍵暗号方式の鍵を送る」



暗号化

- 暗号化を使った通信

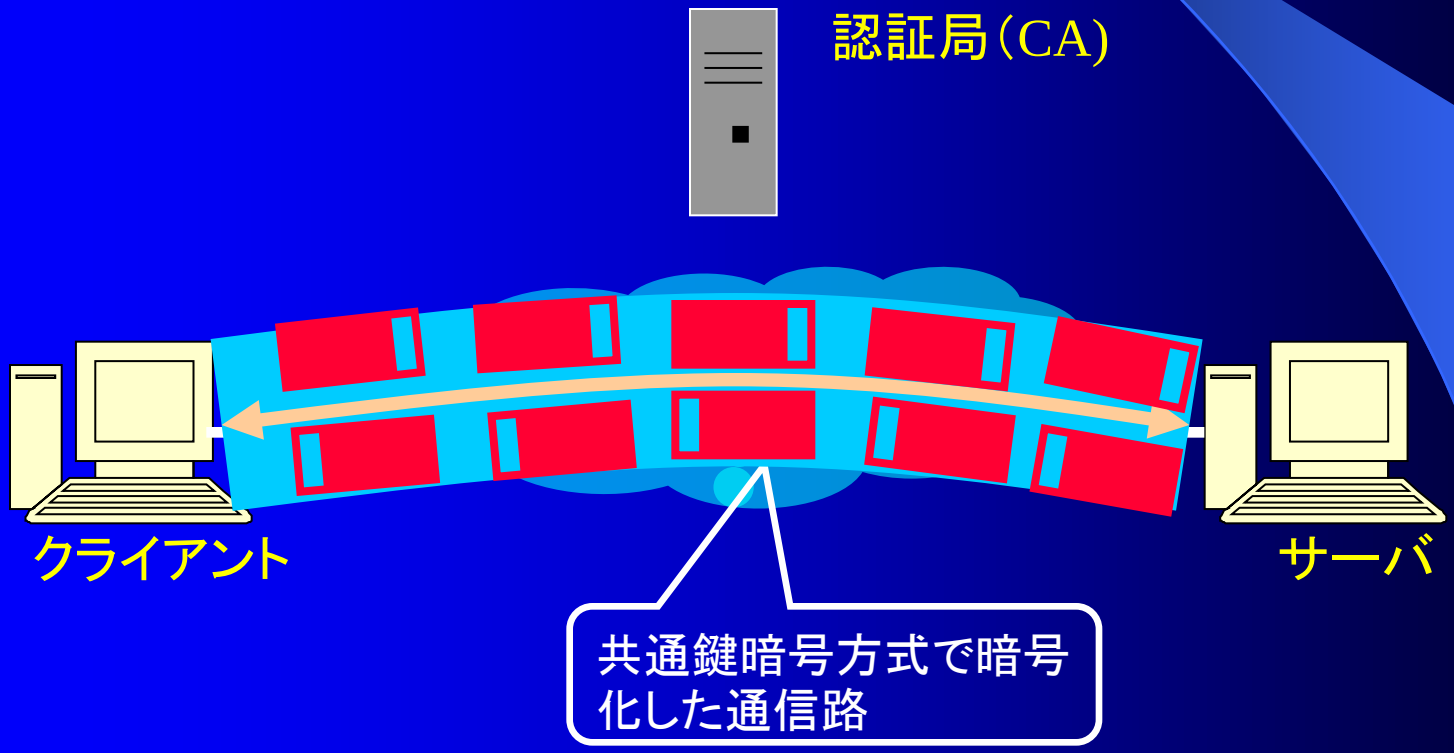
「共通鍵暗号方式の鍵」を作ってサーバの公開鍵で暗号化し送信



暗号化

- 暗号化を使った通信

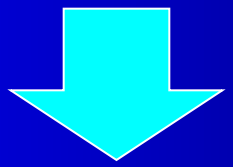
「共通鍵暗号方式の鍵」を作ってサーバの公開鍵で暗号化し送信



IPv6

- IPv6とは？

現在のIPv4では最大2の32乗（約42億）台までしかインターネットに接続できない



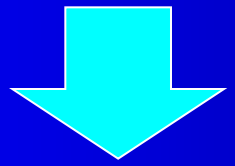
アドレスの長さを128ビットにし、最大2の128乗（3.4×10^38、340澗）台まで接続可能

•プライベートアドレスやNATを使う必要が無くなる

IPv6

- IPv6のアドレス

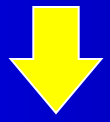
IPv4のアドレス：　192．168．0．1（8ビット単位で10進数表記）



IPv6のアドレス：2001:e38:3560:188:b9b6:1636:df3e:9607

（16ビット単位で16進数表記）

IPv6のアドレス：fe80:0:0:0:203:93ff:fed1:4870



（0が連続するときは省略が可能）

fe80::203:93ff:fed1:4870

IPv6

- IPv6のアドレス

IPv6にも「ネットワーク部」と「ホスト部」が存在する

2001:e38:3560:188:b9b6:1636:df3e:9607

前半の64ビットがネットワーク部で固定

DHCPで自動的にアドレスを割り振ることが可能など、長くて覚えにくいアドレスであるため、できるだけ手作業が入らないよう工夫がなされている。

IPv6

- IPv6とIPv4との通信

  IPv6とIPv4には完全な互換性がないが、いくつかの技術を使いながらIPv6へ少しずつ移行していく

  •IPv6とIPv4をつなぐ技術の例

  デュアルスタック

  NAT-PT

  ６ to ４

本日のまとめ

IPを助けるプロトコルと技術２

- セキュリティ

  ファイヤウォール、プロキシサーバ

- 暗号化

  共通鍵暗号方式、公開鍵暗号方式

- IPv6

本日の課題

1. LAN上のコンピュータがインターネットからのpingに応答しないようにファイヤウォールのセキュリティルールを定めたい。“通過禁止”に設定するものはどれか？ 理由も付けて述べなさい。（ネ 改）

   ア. ICMP　　イ. TCP及びUDPのポート番号53

   ウ. TCPのポート番号21　　エ. UDPのポート番号123

   ヒント：TCPやUDPのポート番号にどんな情報が流れるかは付録C（教科書p.318～320）を参照

2. 公開鍵暗号方式によって、N人が相互に暗号を使って通信する場合、異なる鍵は全体でいくつ必要になるか？（ネ）

3. IPv4とIPv6の主な違いについて述べなさい。（ネ 改）