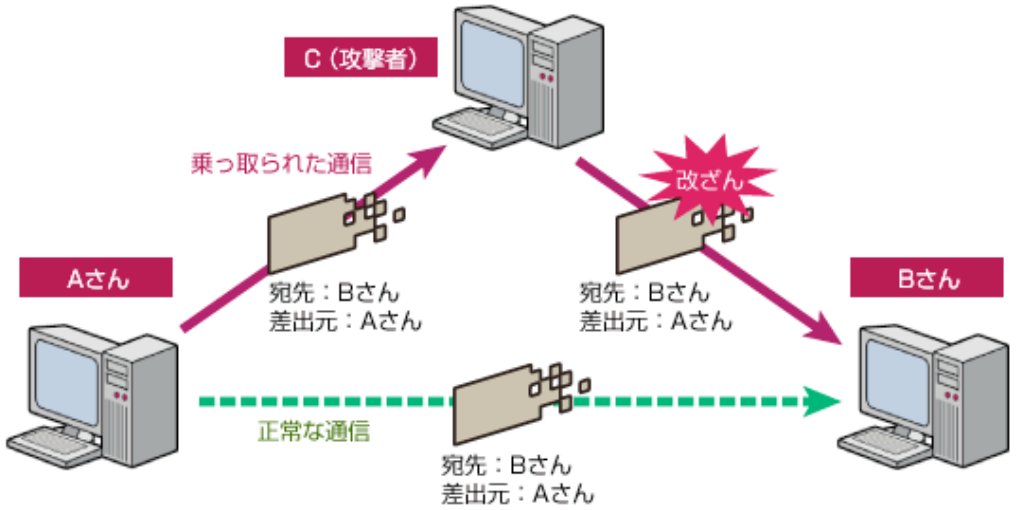
10. ネットワーク・セキュリティ

要点

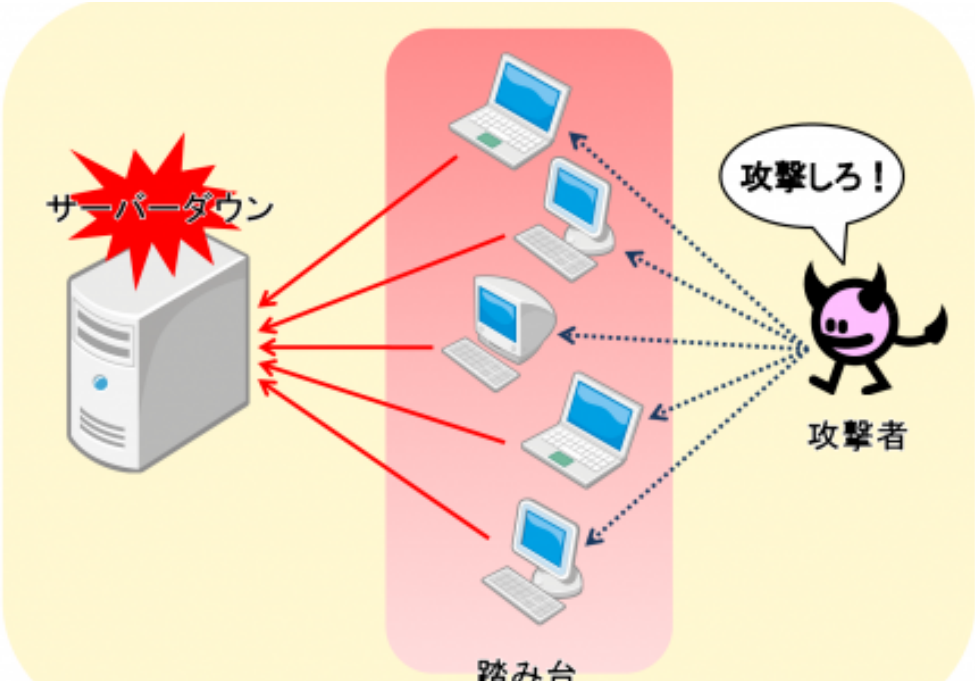
- ネットワーク上の脅威とセキュリティの確保
  - ネットワーク上には盗聴，中間者攻撃，DoS 攻撃，なりすましなどの脅威がある.
  - セキュリティ確保の手段としては，ネットワークの隔離，認証，認可がある.
- ネットワークの部分隔離のためファイアウォールがつかわれる.
- 暗号には共通鍵暗号と公開鍵暗号があり，後者を使用して Web の暗号化・認証 (TLS/SSL) などが実現されている.
- 認証のため パスワードや公開鍵暗号を使用した電子署名が使用される.
- アクセス権限の認可にもとづいて，ファイアウォールなどではポリシー規則などにもとづくアクセス制御がおこなわれる.
- 無線 LAN のセキュリティのため, WEP, WPA, TKIP など，さまざまな方法が開発されている.

ネットワーク上の脅威

- 盗聴 (eavesdropping)
  - 通信路上の暗号化していないパスワードをぬすむなど.
- 中間者攻撃 (man-in-the-middle attack)
  - 通信経路を勝手に変更するなどして盗聴したり, メッセージをかきかえたりするなど.
- DoS 攻撃 (denial-of-service attack)
  - サーバに多量のパケットを送信してサービスできなくするなど.
  - 多数の踏み台をつかうものを DDoS (分散 DoS) という.



http://ma-ke.blog.ocn.ne.jp/security_trend/2010/04/37ddos_021f.html

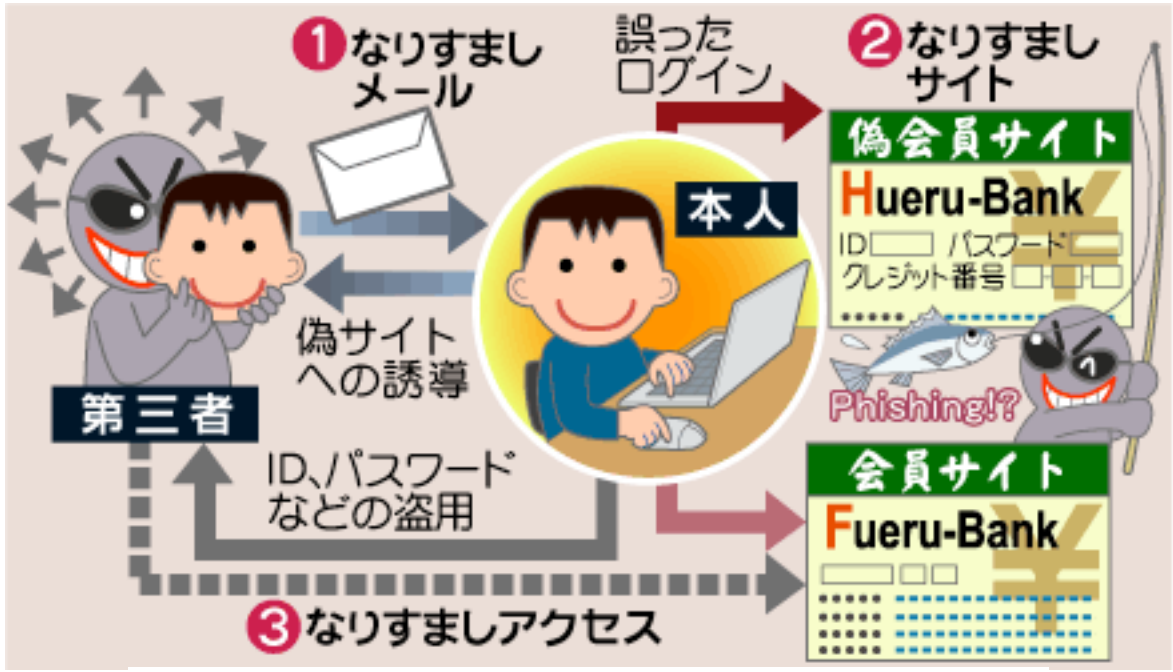


http://ma-ke.blog.ocn.ne.jp/security_trend/2008/10/3_944e.html

ネットワーク上の脅威 (つづき)

■ なりすまし (spoofing)

◆ にせのサーバや
にせのユーザに
偽装してパスワード
などの情報をぬす
む.



http://www.yomiuri.co.jp/net/column/security/20050928nt0c.htm

コンピュータへの侵入の方法と対策

■ クラッカー (ハッカー) は認証の壁をやぶって侵入する.

◆ リモート・アクセスして，スーパーユーザのパスワードをぬすんで侵入する.

◆ 暗号を使用した認証なら，平文による認証より安全である.

図14・3 スーパーユーザとクラッキングの対象

セキュリティ確保のための方法

- 隔離
- 暗号化
- 認証
- 認可

■ ネットワークの隔離

- ◆ プライベート・ネットワークを構築して，物理的または論理的にインターネットから隔離された環境をつくる.
- ◆ 物理的に完全に隔離するのがもっともセキュアだが，それができないときはインターネットとのあいだにファイアウォールを設置する.

■ 暗号化 (encryption)

- ◆ 通信内容が暗号化されていれば，盗聴されても情報漏洩しない.

■ 認証 (authentication)

- ◆ 人などがネットワークや通信を利用する権限をもっていることを確認する.
- ◆ 認証の手段としてパスワードや電子証明書などがある.

■ 認可 (authorization)

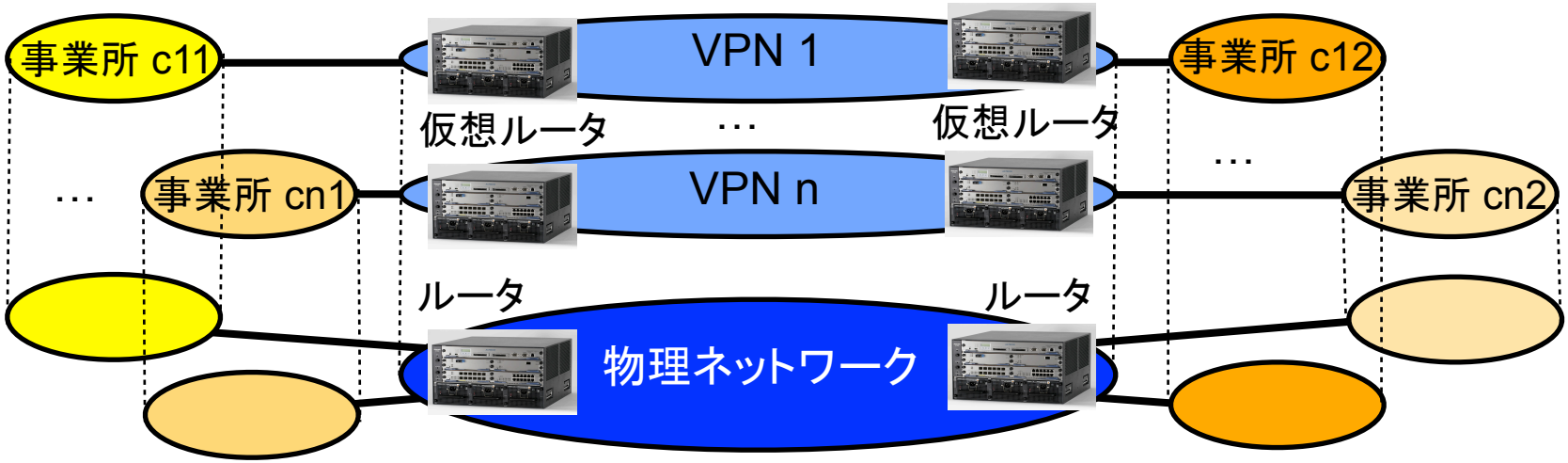
- ◆ ネットワークや資源 (サーバなど) にアクセスする権限を設定する.
- ◆ 認証された (アイデンティティが確立された) ユーザごと，またはそれ以外のユーザ (一律) に権限が設定される.

プライベート・ネットワークによる隔離

- 隔離
- 暗号化
- 認証
- 認可

■ プライベート・ネットワークをつくることでインターネットから隔離され，セキュリティが確保できる．

◆ 物理的なプライベート・ネットワークと仮想的なプライベート・ネットワーク (VPN) とがある．



■ 完全に隔離すると不便なので，ファイアウォールを使用する．

ファイアウォールによるネットワークの隔離と接続

- 外部ネットワークから完全に隔離できないとき，ファイアウォールを設置して内部 (組織内ネットワーク) を脅威からまもる.
- 外部から隔離できない理由は，外部サービスの利用，外部へのサービスの提供など.

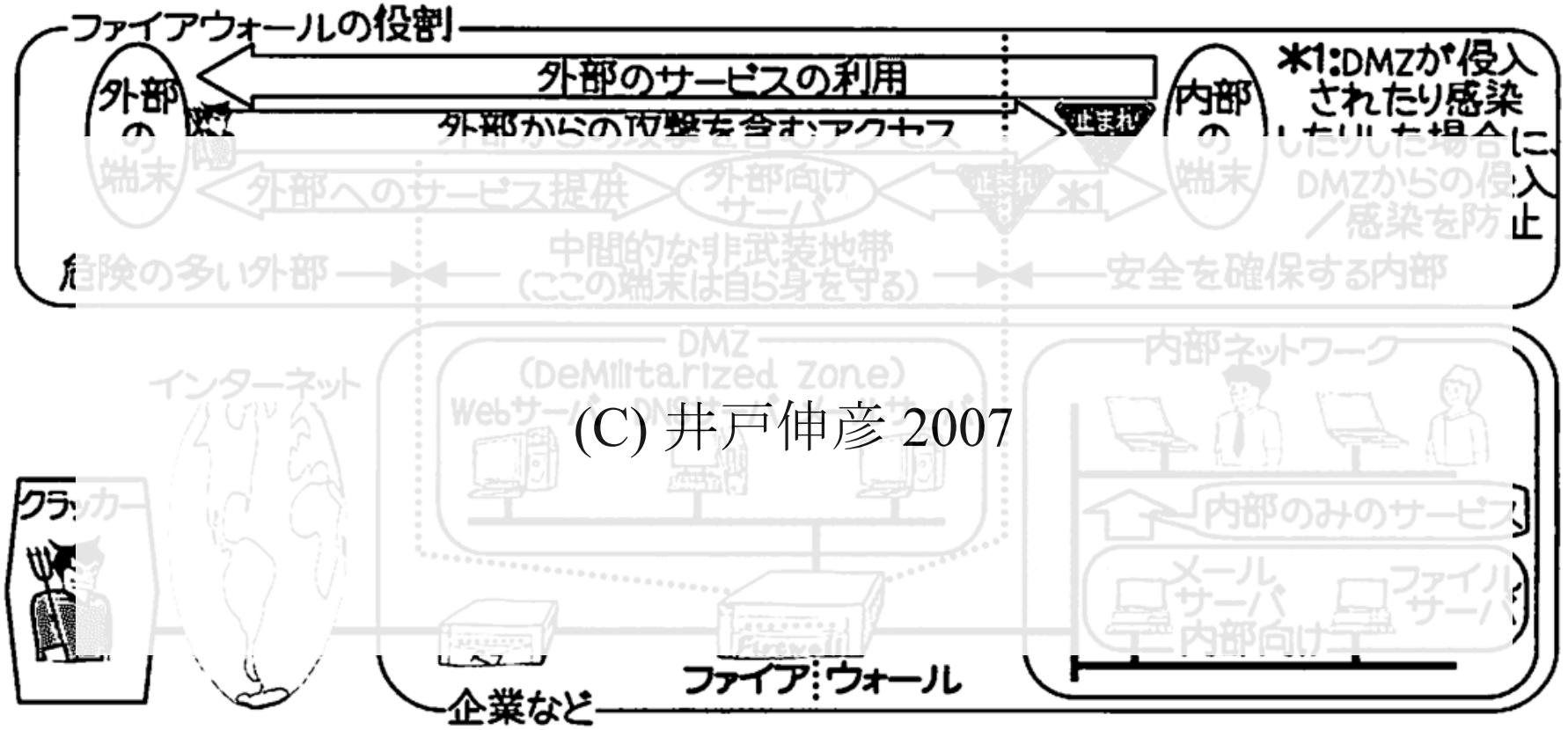
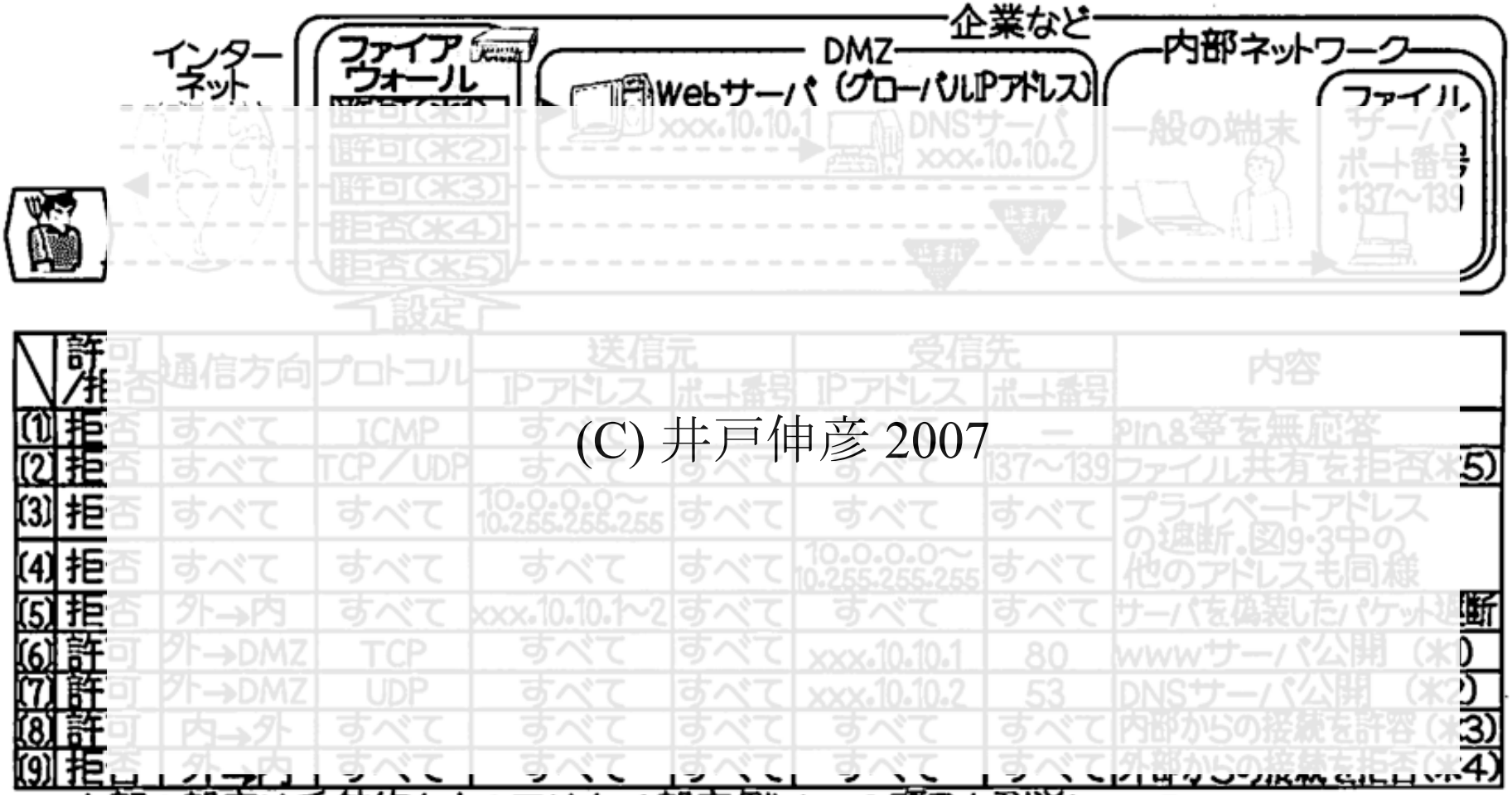


図14-14 ファイアウォール(Firewall)の役割と構成例

ファイアウォールにおけるパケット・フィルタ

■ ファイアウォールにはパケット・フィルタ規則が設定される.



※ 上記の設定は系統的なものではなく、設定例としての項目を列挙している。
※ 防御される攻撃の例： Pin&スイープ(図14・6(a))←(1)、 IPスプーフィング(図14・8)←(3)、ICMPスプーフィング(図14・11(d))←(1)(3)(5)

図14・15 ファイアウォールでのパケットフィルタリングとその設定例

パソコンのファイアウォール

■ パソコンにもファイアウォールを設定することができる.

◆ ファイアウォールはパソコンと外部との通信を監視する.

◆ 家庭 / 職場内ネットワークの外部からのアクセスはきびしく制限する.

図14・17 Windows PCでのファイアウォールの設定

暗号とその種類

- 隔離
- 暗号化
- 認証
- 認可

■ 暗号とは?

◆ 特別な知識なしでは通信内容がわからないように通信文を変換する方法.

■ 暗号の種類

◆ 共通鍵暗号 (対称暗号)

●暗号化と復号化とに同一の鍵 (秘密鍵) を使用する暗号方式.

◆ 公開鍵暗号

●公開鍵によって暗号化した暗号文が秘密鍵を知らないと復号化できない暗号方式.

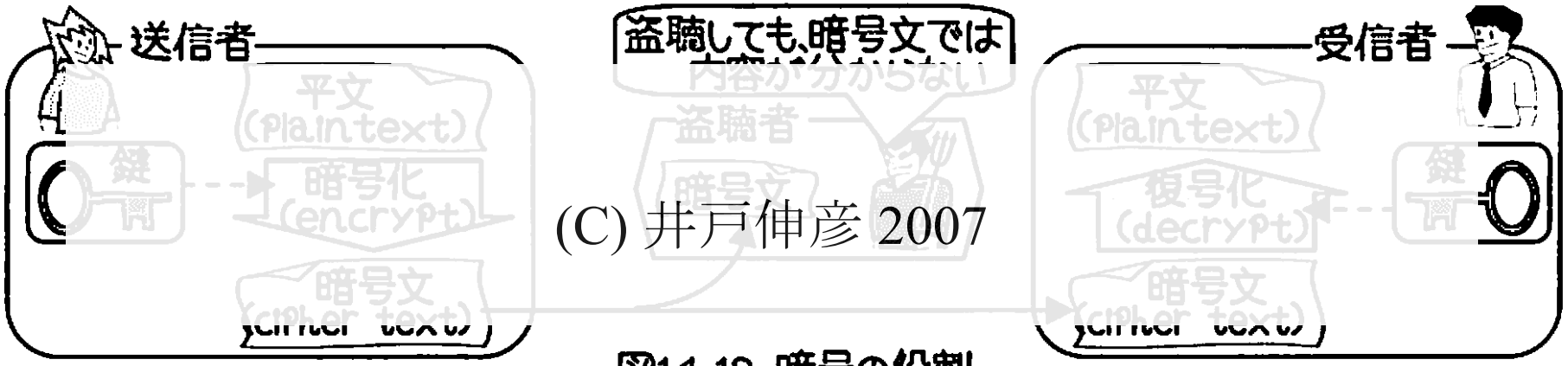
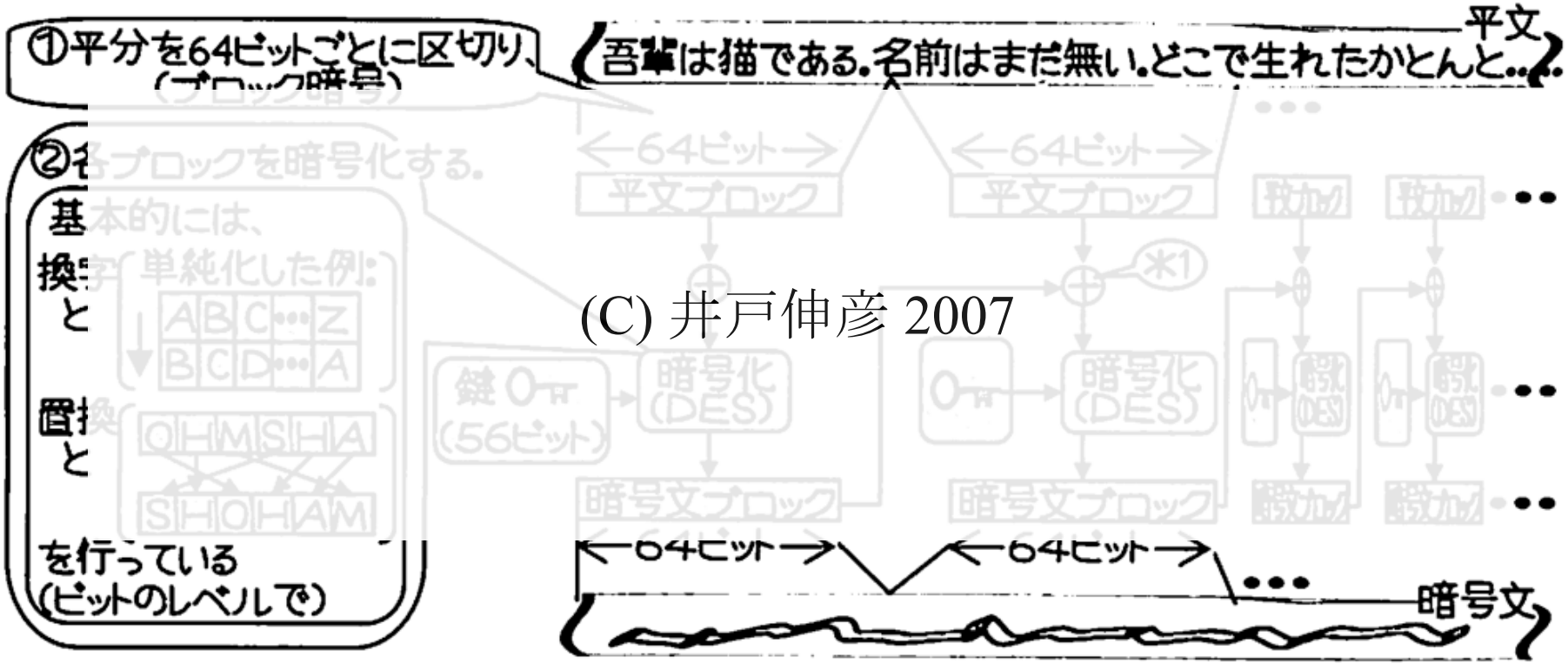


図14-18 暗号の役割

共通鍵暗号

- 暗号化と復号化とに同一の鍵 (秘密鍵) を使用する暗号方式.
- 基本的に 1 対 1 の通信だけに使用される.
- 共通鍵暗号の例: DES (Data Encryption Standard)

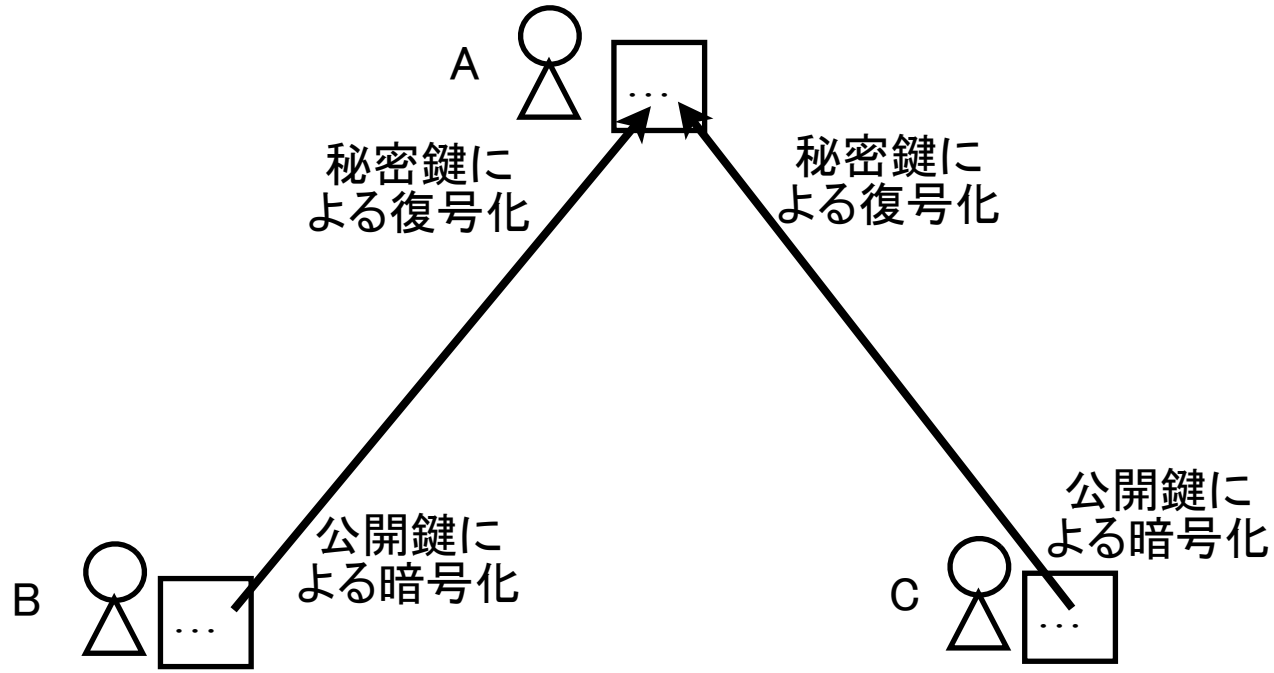


*1:同じ平文ブロックが同じ暗号文ブロックになるようなことを避けるために、前の暗号化ブロックを足しこんでいる(排他的論理和)。このような繰り返し方法を「モード」と呼ぶ(図とは違う方法もある)。

図14・20 DES(Data Encryption Standard)での暗号化の概要(対称暗号の例)

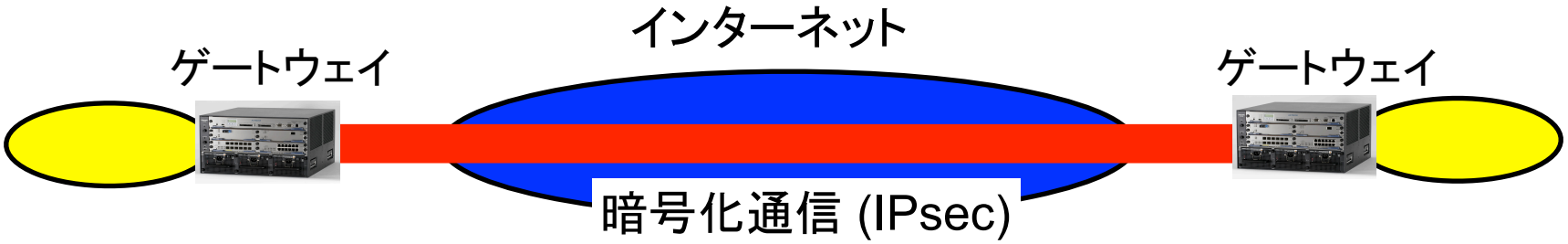
公開鍵暗号

- 公開鍵によって暗号化した暗号文が，秘密鍵を知らないと復号化できない (復号化に天文学的な時間がかかる) 暗号方式.
- 多対多の通信に使用できる.



暗号化通信のためのプロトコル IPsec

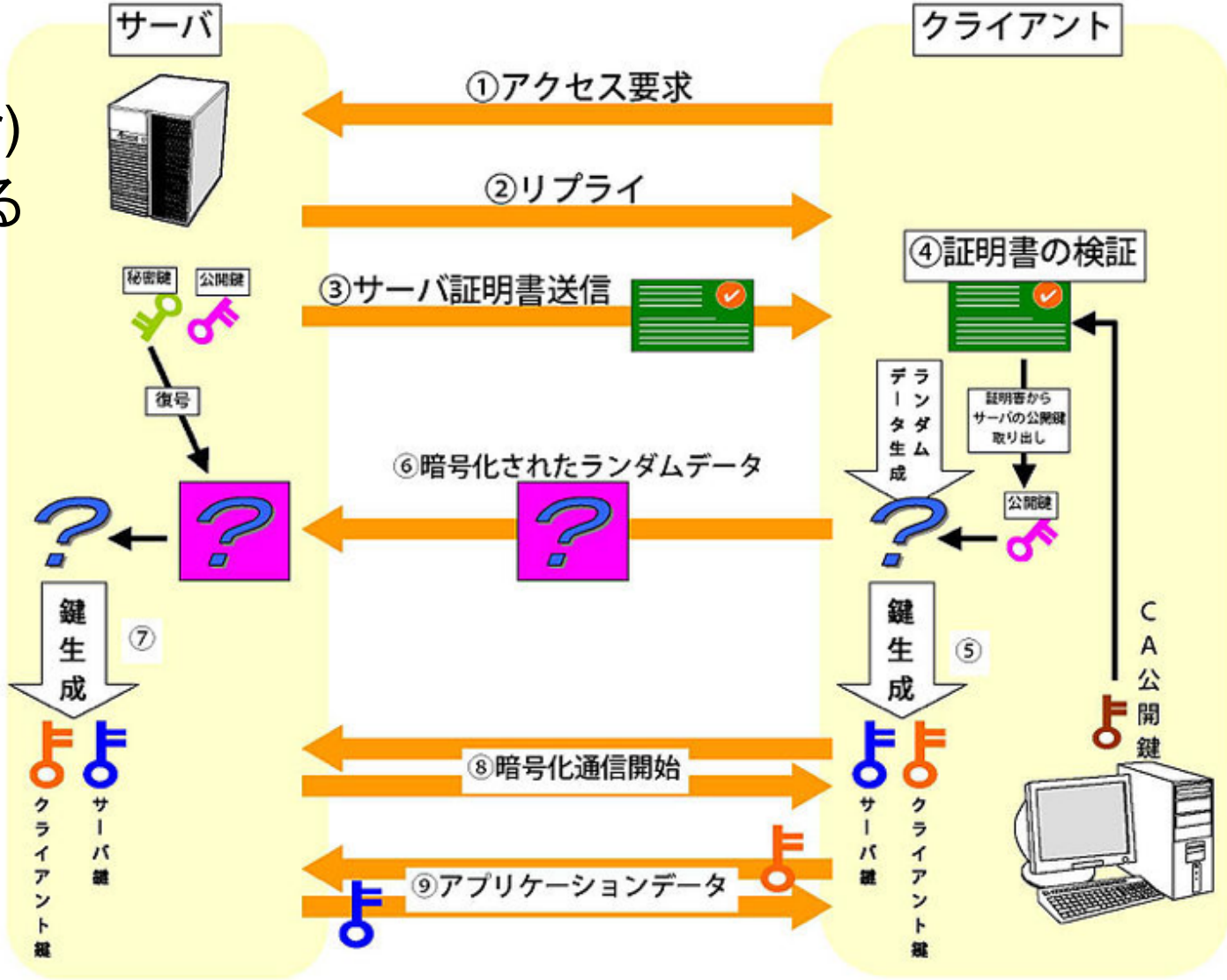
- IPSec はネットワーク層 (IP) において暗号化と認証をおこなうためのプロトコルである.
- IPSec は VPN における暗号化のためにも使用される.
  - Internet VPN (IPsec VPN) においてはインターネット上で暗号化通信をする.



  - IPsec によってカプセル化する.

TLS と SSL

- TLS (Transport Layer Security) は TCP の暗号化機構である.
- SSL (Secure Socket Layer) は TLS のふるい版である.



TLS と SSL (つづき)

■ TLS/SSL は Web の暗号化によく使用される.

◆ SSL は Netscape Navigator (Web ブラウザ) のために開発された.

※IE7 の場合は🔒が表示されません。

認証の方法

- 隔離
- 暗号化
- 認証
- 認可

- 認証とは，人などのアイデンティティを確認し，ネットワークや通信を利用する権限をもっていることを確認することである.
- 認証の手段
  - パスワード
  - 電子署名

パスワード認証の弱点

■ パスワードは漏洩しやすい

◆ パスワードはくりかえし入力 (送信) される.

◆ 漏洩したパスワードをそのままつかえば認証される.

■ パスワードは発見されやすい

◆ みじかいパスワードはランダムに生成してもあてられる.

◆ パスワードにはおぼえやすいつづりがつかわれることが多い.

●生年月日, こどものなまえ, など.

パスワード認証の改良: ワンタイム・パスワード

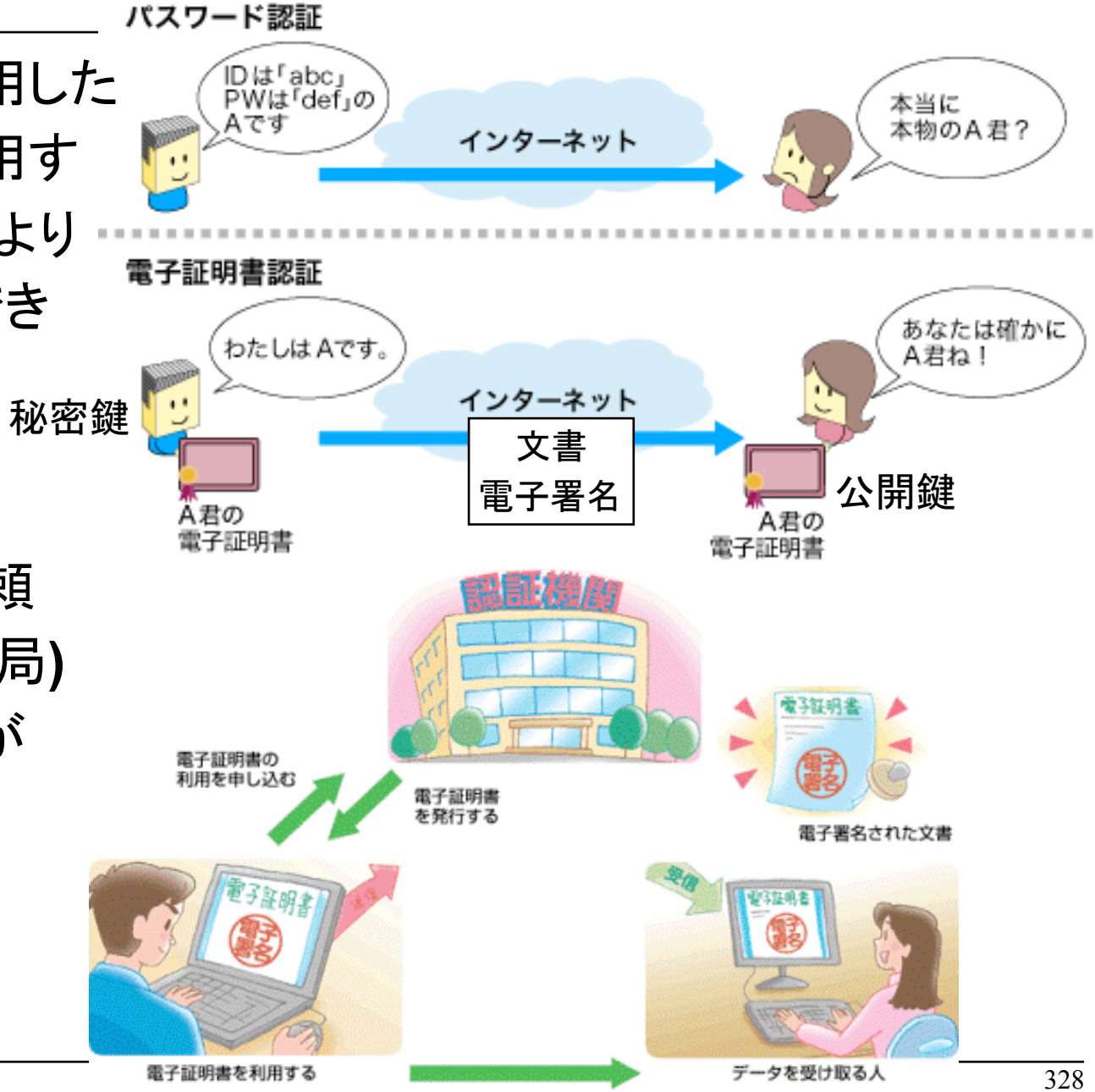
- 毎回ことなるパスワードを入力することによって，ぬすまれるのをふせぐ.
- 手でパスワードを計算するのは困難なので，PC がパスワードを生成してサーバにおくったり，「トークン」を使用したりする.
  - いずれの方法もサーバとユーザとが秘密情報 (関数など) を共有する必要がある.

- 2 つの方法
  - 時刻同期方式 (タイムスタンプ方式)
    - サーバとユーザ側とで時刻同期してパスワードを計算する.
    - ユーザは「トークン」に表示されたパスワードを入力する.
  - チャレンジ・レスポンス方式
    - サーバからランダムな値をおくり，ユーザ，サーバ双方がそれにもとづく関数値を計算する. サーバがその値が一致するかどうかしらべる.

電子証明書による認証

■ 公開鍵暗号を使用した電子証明書を使用すれば，パスワードよりセキュアに認証できる.

■ 電子証明書は信頼できる機関 (認証局) が発行する必要がある.



認可とアクセス制御

- 隔離
- 暗号化
- 認証
- 認可

- 認可とは，ネットワークや資源 (サーバなど) にアクセスする権限を設定すること.
  - 認証された (アイデンティティが確立された) ユーザごと，またはそれ以外のユーザ (一律) に権限が設定される.
- 認可にもとづいてネットワークや資源へのアクセス制御がおこなわれる.
  - ファイアウォールにおいても，外部から内部，内部から外部へのアクセス制御がおこなわれる.
- アクセス制御には，ポリシー規則やアクセス制御リスト (ACL) が使用される.
  - ポリシー規則は “if 条件 then 動作” のかたちの規則.

無線 LAN のセキュリティ

■ MAC アドレス・フィルタリングによって，特定の MAC アドレスをもつコンピュータだけがつなげるようにできる．

図1■「MACアドレスフィルタリング」の仕組み

織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

無線 LAN のセキュリティ（つづき）

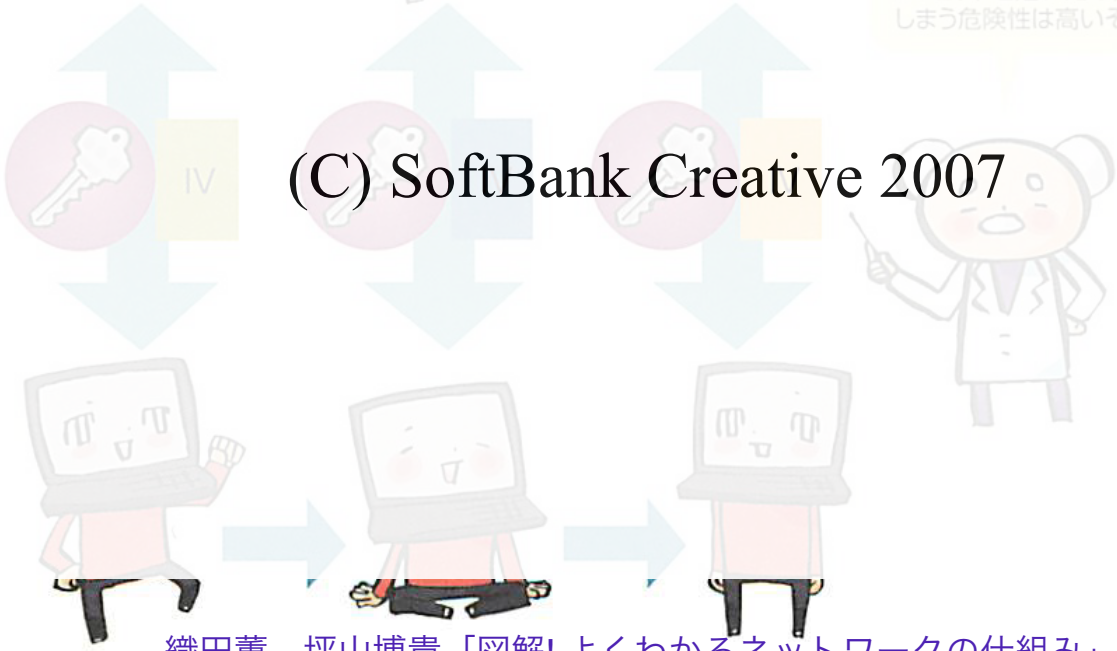
■ WEP, WPA, TKIP などのしくみで暗号化通信ができる.

◆ 適切なしくみをえらんで，または自動的な方法で設定すればよい.

図2■「WEP」の仕組みと脆弱性について

WEP = Wired Equivalent Privacy
WPA = WiFi Protected Access
TKIP = Temporal Key Integrity Protocol

WEPの場合，いつも同じ暗号キーを利用しておる。パケットごとにIVを変更することで解読しにくくしているが，IV自体の長さが24ビットと短いため，解読されてしまう危険性は高いぞ



織田薫，坪山博貴「図解! よくわかるネットワークの仕組み」，SoftBank Creative

ネットワーク・セキュリティのまとめ

- ネットワーク上の脅威とセキュリティの確保
  - ネットワーク上には盗聴，中間者攻撃，DoS 攻撃，なりすましなどの脅威がある.
  - セキュリティ確保の手段としては，ネットワークの隔離，認証，認可がある.
- ネットワークの部分隔離のためファイアウォールがつかわれる.
- 暗号には共通鍵暗号と公開鍵暗号があり，後者を使用して Web の暗号化・認証 (TLS/SSL) などが実現されている.
- 認証のため パスワードや公開鍵暗号を使用した電子署名が使用される.
- アクセス権限の認可にもとづいて，ファイアウォールなどではポリシー規則などにもとづくアクセス制御がおこなわれる.
- 無線 LAN のセキュリティのため, WEP, WPA, TKIP など，さまざまな方法が開発されている.