ネットワーク・セキュリティ分野で必須の用語
infomaticsI-028

用語と意味

- サーバ(server):
  管理されたサーバシステム上で動き
  多数のクライアントにサービスを提供するプログラム

- クライアント:
  ユーザごとに起動され
  サーバからサービスを受けるプログラム

用語と意味

- E-mail:
  ネット上で手紙のようにメッセージをやりとりするシステム
- IMAP(Internet Message Access Protocol):
  受け取ったメールを
  サーバ内で保管し整理・アクセスできるプロトコル
- SMTP(Simple Mail Transfer Protocol):
  メールサーバに向けてメールを送るプロトコル
- POP(Post Office Protocol):
  受け取ったメールをダウンロードさせてくれるプロトコル
- メールサーバ:
  メールのサーバプログラムで、
  メールを中継したり受け取ったりする

用語と意味

- ネットワーク:
  網目状の構造を持つもの
- 情報通信ネットワーク:
  コンピュータやその他の情報機器が
  つながっているネットワーク
- LAN(Local Area Network):
  局所的な範囲でつながっているネットワーク
- WAN(Wide Area Network):
  LANを含む、広範囲につながったネットワーク

用語と意味

- ISP(Internet Service Provider):
  学校、家庭、企業などのLANを
  インターネットにつないでくれる事業者
- ハブ:
  LANのインタフェースからの線を集約し相互に接続する機器
- 無線LAN:
  無線で構築されたLAN
- アクセスポイント:
  無線LAN機器の基地局となる機器
- Wi-Fi:
  IEEE802.11規格に準拠した無線LAN機器に
  つけられるロゴ

用語と意味

- ルータ:
  パケットを経路制御表にしたがって
  正しい方向に送る機器
- ルーティング:
  パケットを正しい方向に送ること
- パケット:
  データを決まった大きさの単位に分けたもの
- パケット交換方式:
  データを決まった大きさの単位に分けて
  それぞれに行き先を持たせて送る方式

用語と意味

- インターネット(Internet):
  IPを用いて情報を流通させる
  世界にまたがるネットワーク
- プロトコル:
  通信のために守らなければならない決まり事
- TCP/IP:
  インターネットで使われる通信プロトコルの総称
- IP(Internet Protocol):
  TCP/IPのインターネット層プロトコルで、
  経路制御を受け持つ

用語と意味

- IPアドレス(Internet Protocol address):
  IPが使用する32ビット
  (IPv6では128ビット)のアドレス
- IPv4:
  IPの古くからあるバージョンで
  32ビットのアドレスを用いる
- IPv6(IP version 6):
  IPの新しいバージョンで128ビットのアドレスを用いる

用語と意味

- WWW(World Wide Web):
  インターネット上にまたがってつながる
  ハイパーテキストのシステム
- URL(Uniform Resource Locator):
  WWW上のページ等に対応するアドレス
- ドメイン名:
  TCP/IPでホスト・サイトを識別する英数字の名前
- DNS(Domain Name System):
  TCP/IPでドメイン名とIPアドレスの対応を司るシステム
- DNSサーバ:
  DNSの機能を実現するサーバ

用語と意味

- HTTP(Hypertext Transfer Protocol):
  Webページを取り寄せるのに使うプロトコル
- SSL/TLS:
  暗号化プロトコルSSLとTLSを併せて呼ぶ言い方。
  これらはドメイン名の証明の機能も持つ
- HTTPS(HTTP secure):
  HTTPのかわりにHTTPSとすると、
  ブラウザがTLSを使うようになる

用語と意味

- 平文:
  暗号化する前の、もとの文
- 暗号化:
  もとの文(平文)を暗号文に変換すること
- 復号:
  暗号文をもとの文(平文)に変換すること

用語と意味

- 共通鍵暗号方式:
  暗号化と復号の両方におなじ鍵を使用する暗号方式
- 鍵:
  暗号化で使用するデータ
- 公開鍵暗号方式:
  暗号化と復号の両方に異なる鍵を使用する暗号方式
- 公開鍵:
  公開鍵暗号においてこれを用いて暗号化したものが
  秘密鍵のみで復号できる、公開される鍵
- 秘密鍵:
  秘匿される鍵で、公開鍵暗号では公開鍵で暗号化したものが
  これをもちいてのみ復号できる

用語と意味

- デジタル署名:
  電子文書に対する本人性や非改ざん性を示す方式で、公開鍵暗号技術を用いたもの
- パリティビット:
  パリティチェックのために付け加えたビット

用語と意味

- ファイアウォール(Firewall):
  外部のネットと内部のネットの間に設置し、
  正当でないアクセスを防ぐ機器やソフト
- アンチウイルスソフト:
  ウイルスなどのマルウェアを検出したり
  それから防護したりするソフトウェア
- セキュリティホール:
  ソフトウェアの欠陥で、悪意あるソフトウェアに
  利用される可能性のあるもの