

ネットワーク・セキュリティ分野で必須の用語 infomaticsI-028

テスト前や授業で触れたときに振り返るようにして覚えていくのがよいと思います。

覚えれば共通テストで点を取れるというようなものではありません。覚えていないと問題の意味がわからなくなるかもしれないので、その対策として必須の用語です。

3学期期末テストでは、ここから 15 問(15点分)の知識確認問題を出します。選択肢形式で、意味を選んでもらう形式です。

この知識確認問題以外では、ここで扱う用語は当然知っているものとして出題します。

- ・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

- ・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

- ・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
- ・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
- ・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
- ・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
- ・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
- ・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
- ・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

- ・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
- ・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
- ・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

- ・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: ウィ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

3 学期期末テストで出す予定の、選択肢形式で、意味を選んでもらう形式の例。

(例)以下の用語①～⑮の説明として正しいものを解答群のア～んから選んで答えよ。

① クライアント

② サーバ

- ・
- ・
- ・

解答群

ア. 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

イ. 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

ウ. 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

- ・
- ・
- ・

参考

情報処理学会情報入試委員会「情報科全教科書用語リスト」(CC BY-SA 4.0)