

1 穴埋め問題 (3x9)

以下の説明の () の下線部に相応しい単語を単語群から選び答えよ。[] の下線部には、適切な単語を答えよ。

1. DNS では、コンピュータ名 (ドメイン名) から (A) _____ を調べることができる。
fukui.kosen-ac.jp の組織ドメインは [B] _____ である。
2. 相手のメールアドレスが t-saitoh@emc.fukui-nct.ac.jp の場合、[C] _____ の部分を DNS に問い合わせ、通信相手のメールサーバを特定し、通信プロトコルには (D) _____ (およびその暗号化版プロトコル) を使用してメールを送る。
自分宛てのメールをメールサーバから受信をする際には、プロトコルには (E) _____ などが用いられる。
3. http://tsaitoh.net/index.html といった URL が与えられると、ブラウザは tsaitoh.net の部分から (F) _____ を用いて IP アドレスを調べる。また http://の部分から、プロトコルには HTTP を用い、ポート番号には (G) _____ が使われる。
ブラウザは Web サーバに —/index.html— のデータを要求し、帰ってきた HTML 形式の内容に応じたものを表示する。
4. 暗号化通信では、暗号化の鍵と復号化の鍵が共通な場合、通信で鍵を受け渡しする方法が問題となる。このため、公開鍵暗号では、解読するための (H) _____ 鍵と、暗号化するための (I) _____ 鍵に別のものを使う。

単語群:

22,80,110,993,CURL, DoS, DNS, FTP, 秘密, HTTPS, HDMI, IMAP, IP アドレス, 共通, 公開, MAC アドレス, POP, ポート番号, RC4, SMTP, SSH, URI

2 説明問題 (25)

ロボット型の検索エンジンの仕組みや特徴について、他の検索エンジンの方式と対比しながら、説明せよ。

3 対応付け問題 (14x2)

(a)-(d) と最も関係のある単語の欄に、記号を埋めよ。(4=14,3=10,2=7,1=4)

- (a) リモートアクセスのコマンドで暗号化されないので注意が必要。
(b) 通信相手のコンピュータから応答があるか確認するコマンド。
(c) 通信相手までの経路を確認し、途中のルータからの応答を確認するコマンド。
(d) DNS サーバに問い合わせを行うためのコマンド。

nslookup (_____), ping (_____), telnet (_____), traceroute (_____)

- (a) 大きな数の素因数分解が困難なことを利用した公開鍵暗号。
(b) コンピュータを操作するためのコマンドを文字でやり取りする方法。
(c) 通信に必要な IP アドレスを貸し出し、サブネットマスクやゲートウェイの情報を機器に提供する機能。
(d) リモートアクセスのコマンドで相手サーバでコマンドの実行ができるが、通信データの暗号化はされていない。

CUI (_____), DHCP (_____), RSA (_____), RSH (_____)

4 説明問題 (14x2)

以下の2つの設問に答えよ。2つの設問で同じ内容の説明を使わないこと。

- セキュリティ対策の方法を2つあげ、それぞれ対策が効果がある理由を説明せよ。危険な理由や具体的な対策などを交えた説明であること。
- パスワード攻撃で不正アクセスを受けないようにするための対策を2つあげ、対策がどのように不正アクセスを防ぐことになるのかなど仕組みなどを交えながら、説明せよ。