

1 穴埋め問題 (30)

1. `http://tsaitoh.net/~t-saitoh/index.html` といった URL が与えられると、ブラウザは最初の `http://` の部分で通信プロトコルに `http` を使い、通信ポートとして (A) _____ 番ポートを使う。次に DNS にコンピュータ名から IP アドレスを得る。この DNS への問い合わせは、(B) _____ という。調べた IP アドレスのコンピュータに (A) 番ポートに接続し、`/~t-saitoh/index.html` のページをダウンロードし、ブラウザで表示を行う。

最近は暗号化されていない `http` 通信は危険なので、強制的に (C) _____ に切り替えられることもある。

2. クラウド上のコンピュータを利用してサービスを提供する方式で、クラウド企業のサーバを利用して、サービス提供者が OS, Web サーバ, ソフトウェアを構築する方式は (D) _____ という。クラウド企業で準備された OS や Web サーバなどのミドルウェアの上に、サービス提供会社がシステムを構築する方式は PaaS と呼ぶ。これらに対し、サービス提供者が開発したソフトウェアを動かす方式は (E) _____ という。

こういったクラウド上のサーバをメンテナンスする際には、キーボード操作主体で暗号化しながら通信・操作する (F) _____ や、マウス操作で操作する時には (G) _____ が用いられる。

3. 一般的な公開鍵暗号を使った通信では、サーバ側で暗号化を復号するための (H) _____, 暗号化するための (I) _____ を準備しておく。クライアントは (I) をダウンロードし、クライアントで乱数を用いて作成した (J) _____ を (I) を使って暗号化し、サーバに送る。サーバでは (H) を使って復号化し (J) を得る。この後は (J) を使い暗号化通信を行う。

単語群: 22,25,80,119,DaaS, DES, ftp, https, IaaS, irc, “Remote Desktop”, RSA, rsh, SaaS, ssh, telnet, 逆引き, 共通鍵, 公開鍵, 正引き, 万引き, 秘密鍵, 証明書, 量子暗号

2 説明問題 (20)

以下の2つの説明問題のどちらかについて説明せよ。

- 自分のメールソフトから、次のメールアドレス `tohrusaitoh@tsaitoh.net` でメールを送り、`tohrusaitoh` が自分のパソコンでメールを読むまでの仕組みを具体的に説明せよ。この際に使われる、プロトコルなども交えて説明すること。
- ロボット型検索エンジンの仕組みについて説明せよ。

3 対応付け問題・○×問題

以下の単語に、最も関係のある (a)-(d) を対応づけよ。(8x3+3x4)

- (a) 広告や詐欺、ウィルス感染を目的とした迷惑メールの相称。
(b) 文章や画像などの要素をタグで囲んで構造化し、Web ブラウザで表示するための形式。
(c) インターネット上に暗号化された仮想の専用線を設けることで、第三者からの傍受を防ぐ技術。
(d) 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。

HTML (___), RSA (___), spam (___), VPN (___)

- (a) 第2次世界大戦中のドイツの Enigma を解読する機器を開発。
(b) プログラム内蔵方式のコンピュータを提案。
(c) 1990年代の有名なクラッカー。
(d) WWW を考案し http を開発・実装した。

ティム・バーナーズ=リー (___), ケビン・ミトニック (___),
フォン・ノイマン (___), アラン・チューリング (___)

- (a) 複数のコンピュータから標的サーバーに大量アクセスを行い過負荷状態にする。
(b) 連続する大量の IP アドレスにネットワーク攻撃を加える。
(c) データの一時保存場所に、想定以上のデータを書き込む攻撃手法。
(d) 感染した端末のファイルを暗号化して身代金を要求するウィルス。

バッファオーバーフロー (___), DDoS 攻撃 (___), ランサムウェア (___), 絨毯爆撃 (___)

- 以下の説明がセキュリティ対策の考え方として、正しければ○、間違っていれば×を答えよ。

- (___) 公共の Wi-Fi は、暗号化されているから安全に利用できる。
(___) 全てのウィルスは、ターゲットの OS に合わせた機械語で書かれている。
(___) 最新のウィルス対策ソフトを正しく使っていても、ウィルスに感染する可能性がある。
(___) 学校や企業などのファイアウォールの内側のコンピュータでも、ネットワーク攻撃を受けることがある。

4 セキュリティ説明問題(14)

以下の2つの説明問題のどちらかについて説明せよ。

- ファイアウォールの仕組みを説明せよ。
- 様々な SNS やインターネットサイトで、同じパスワードを使うことが危険な理由を説明せよ。