

1 穴埋め問題 (28)

1. DNS でドメイン名から IP アドレスを調べることは (A) _____ といい、IP アドレスからドメイン名を調べることは (B) _____ という。
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、クラウド企業で作られたソフトを貸出しする方式は (C) _____ 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、サービス提供者が開発したソフトウェアを動かす方式は (D) _____ という。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 IaaS という。
3. 第2次世界大戦でドイツ軍が用いていた暗号器 (E) _____ を解読するため、(F) _____ はコンピュータの原型となった bombe を開発した。(F) は、プログラム内蔵方式を提唱した (G) _____ と、情報理論を考案したクロード・シャノンと共に、コンピュータの基礎を築いた功績者と言われる。
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) _____ 鍵を用いる。

単語群: PaaS, SaaS, Wireshark, エニグマ, 踊る人形, 逆引き, 共通, 公開, 正引き, 万引き, 秘密, 量子暗号, アラン・チューリング, ケビン・ミトニック, フォン・ノイマン, リーナス・トーバルズ

2 説明問題 (22)

以下の2つの説明問題のどちらかについて説明せよ。

1. <https://www.fukui-nct.ac.jp/ei/index.html> といった URL が与えられてブラウザでページが閲覧できるまでの仕組みを説明せよ。
2. ロボット型検索エンジンについて、仕組みを説明せよ。

3 対応付け, ○×問題 (24)

1. 以下の単語に、最も関係のある (a)-(d) を対応づけよ。

ワーム(ウォーム)(___), F5 アタック (___), DNS ポイズニング (___), ランサムウェア (___)

- (a) ウィルス感染させてドメインについて調べる際に間違っただ IP アドレスを教えて、危険なサーバに接続させる攻撃
- (b) Web サーバに負担をかけるために何度も情報を読み出す攻撃
- (c) ネットワーク経由で攻撃を加え自己複製しようとするプログラム
- (d) 感染した端末のファイルを勝手に暗号化して身代金を要求するウィルス

2. ARP (___) CUI (___), RSA (___), SSH (___),

- (a) ネットワーク経由でコマンドなどを暗号化通信のもとで実行する機能
- (b) MAC アドレスと IP アドレスの対応を伝えるプロトコル
- (c) 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
- (d) コンピュータを操作するコマンドをキーボード入力を中心に行う方法

3. 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。

- (___) OS やインストールされているソフトの更新は、脆弱性対策として有効である。
- (___) メールに添付されているワードやエクセルなどでもマルウェアの可能性があるので、慎重な確認が必要である。
- (___) 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、ウィルス・マルウェアに感染する可能性があるため、ウィルス対策ソフトなどで防衛することが重要である。
- (___) ウィルス対策ソフトを正しく使っていればウィルス・マルウェアなどに感染することはない。

4 セキュリティ説明問題 (26)

以下の説明問題から 2 つを選んで説明せよ。

- 1. バッファオーバーフローについて説明せよ。
- 2. ウィルス対策ソフトの仕組みを説明せよ。
- 3. ~~他~~要素認証について説明せよ。

要素