平成 30 年 1 月 23 日出題分

第 12 回レポート (解答例)

問 1: LAN 上のコンピュータがインターネットからの ping に応答しないようにファイヤウォールのセキュリティルールを定めたい。“ 通過禁止 ” に設定するものはどれか？ 理由も付けて述べなさい。
ア．ICMP　イ．TCP 及び UDP のポート番号 53　ウ．TCP のポート番号 21　エ．UDP のポート番号 123

解答: ア
理由： **ping コマンドで利用されるのが ICMP パケットであるため**、タイプフィールドのタイプ 8 Echo の ICMP パケットを通さないような設定にすれば良い。

問 2: 公開鍵暗号方式によって、N 人が相互に暗号を使って通信する場合、異なる鍵は全体でいくつ必要になるか？

解答: 2N 個
解説： 公開鍵暗号方式で N 人が「**相互に秘密の**」通信を行うには、N 人全員が秘密鍵と公開鍵の 2 つの鍵を持つ必要があるので、異なる鍵は全体で 2N 個必要。
　もし、共通鍵暗号方式ならば、N 人が (自分以外の)N-1 人分の共通鍵をそれぞれ持つ必要があるので、異なる鍵は全体で $\frac{1}{2}N(N-1)$ 個必要。($\frac{1}{2}$ がつくのは 2 人一組で一つの共通鍵を持つから)

問 3: IPv4 と IPv6 の主な違いについて述べなさい。

解答例:

- **IPv4 ではアドレスが 32 ビット、IPv6 ではアドレスが 128 ビット**

(上記の記述があればよい。以下の記述はその他参考程度)
・IPv4 では 8 ビット単位で区切って 10 進数表記、IPv6 では 16 ビット単位で区切って 16 進数表記
・IPv4 ではネットワーク部の長さが固定ではないが、IPv6 ではネットワーク部の長さが 64 ビットで固定されている。
(その他、多数)