

「IT-Text ネットワークセキュリティ」正誤表

(版によっては修正済み)

2022年8月

| ページ | | 誤 | 正 |
|----------|------------------|---|---|
| p.5 | 20行目 | セキュリティとは | 情報セキュリティとは |
| p.6 | 表1. 2 | 脅威 | 要素 |
| p.6 | 表1. 2 | 例 | 脅威の例 |
| p.7 | 表1. 3 | 脅威 | 要素 |
| p.7 | 表1. 3 | 例 | 脅威の例 |
| P26 | 問1アドレス変換表 | pcA4 (内側) でのパケット観測 | pcA3 (内側) でのパケット観測 |
| P27 | 問2, 4行目 | 疑陽性と偽陰性を求めよ | 偽陽性と偽陰性を求めよ |
| P34 | 脚注 | hardwar key logger | hardware key logger |
| P73 | 4行目 | ord(2)=ord(3)= | ord(2)=ord(4)= |
| P100 | 問1 | | 削除 (p. 41 4章問1と同一であるため) |
| P191 | 第2章 問1 (1) | 200.0.0.1 | 11.22.0.1 |
| P191 | 第2章 問1 (3) | 200.0.0.1 | 11.22.0.1 |
| P191 | 第2章 問2 | 偽陽性は0,偽陰性は 1/8(2行目) | 偽陽性は 2 行目,偽陰性はなし |
| P191 | 第2章 問3 (2) | deny all, allow sip=20, allow sip=10 dp =53, allow sip=10 dp=80 | deny all, allow sip=20, allow sip=10 dp =53, allow dip =20 dp=80 |
| P192 | 第4章 問2 (3) | $C_1 = P(A5_{(16)} \oplus 3) = P(10100010_{(2)}) = 2A_{(16)}$ | $C_1 = P(A5_{(16)} \oplus 3) = P(10100010_{(2)}) = AA_{(16)}$ |
| P192 | 第4章 問2 (3) | $C_2 = P(60_{(16)} \oplus 2A_{(16)}) = P(10100010_{(2)}) = 49_{(16)}$ | $C_2 = P(60_{(16)} \oplus AA_{(16)}) = P(10100010_{(2)}) = 69_{(16)}$ |
| P192 | 第4章 問3 (2) | $M_2 = C2_{(16)}$ | $M_2 = FE_{(16)}$ |
| P193 | 第6章 問3 | $FAR = (2+1)/(10+10) = 3/20 = 0.15$ | $FAR = (2+2)/(10+10) = 4/20 = 0.2$ |
| P195 | 第10章 問1 (1) | MK_4, MK_{10} | MK_5, MK_{11} |
| P195 | 第10章 問1 (2) | { MK_7, MK_9, MK_2 } | { MK_3, MK_8, MK_{10} } |
| P195 | 第10章 問1 (3) | { MK_7, MK_5, MK_{14} } | { MK_6, MK_8 } |
| p. 61 | 第4章3節 図4.16 | 不可逆性 | 一方向性 |
| p. 61 | 第4章3節 図4.16 | 二次不可逆性 | 二次原像計算困難性 |
| p. 51 | 4.2節1. 6行目 | $M = 1010_{(2)} = B_{(16)}$ | $M = 1010_{(2)} = A_{(16)}$ |
| p. 52 | 4.2節2. 11行目 | 最後の暗号ブロック C_2 を復号 | 最後の暗号ブロック C_3 を復号 |
| p. 65 | 5.1節 5行目 | ユーザ数nに対して 2^n に比例 | ユーザ数nに対して n^2 に比例 |
| p. 136-7 | 9.1節 136最後から次ページ | HTTPによる通信 (③, ⑤) | HTTPによる通信 (③, ⑥) |
| p. 141 | 9.2節 2行目 | ①~⑦までは主にサーバ管理者が, ⑧~⑨はブラウザ側の利用者 | ①~⑤, ⑦, ⑨は主にサーバ管理者が, ⑥, ⑧はブラウザ側の利用者 |
| p. 150 | 9.2節7. 6行目 | サーバSの公開鍵証明書 | サーバAの公開鍵証明書 |
| p. 163 | 10.2節 上から7行目 | CRPM/CPRM | CPPM/CPRM |