「暗号ハードウェアのセキュリティ」正誤表

---

p.52　4 行目

[誤]　CPA　　[正]　RCA

---

p.53　例 16.

[誤]　$Y = 1\,849 = \cdots$　　[正]　$Y = 3\,897 = \cdots$

---

p.54　脚注

[正]　$\lfloor x \rfloor$ は，床関数で，x 以下の最大の整数 を求める関数。なお，$\lceil x \rceil$ は，
天井関数で，x 以上の最小の整数 を求める関数である。

---

p.62　演習問題 15.

[誤]　$x = 11,\ y = 13$　　[正]　$X = 11,\ Y = 13$

---

p.70　2 行目

[誤]　総数が最少となる　　[正]　総数が最小となる

---

p.95　5 行目

[誤]　$\cdots = \sum_{i=1}^{n} x_i$　　[正]　$\cdots = \sum_{i=1}^{N} x_i$

---

p.96　1 行目

[誤]　$\mathrm{HW}[\mathtt{2b}] = \cdots$　　[正]　$\mathrm{HW}[\mathtt{d}] = \cdots$

---

p.109, p.110　図 5.6（2 箇所），図 5.7（6 箇所）

[正]　正解鍵 $= 2b$ の右辺は “ $2b$ ” ではなく “ $\mathtt{2b}$ ”

---

p.111 下から 2 行目，p.112 式 (5.18) 右辺分母内，式 (5.19) およびその下 1 行目の
正規分布関数第二変数分母内

[誤]　n　　[正]　N

---

p.174　演習問題 38. の解答

[誤]　Specture　　[正]　Spectre
