

『IT Text ネットワークセキュリティ』（第1版 第1～5刷用）正誤表

頁	行	誤	正
48	上5行	…, 米国 MIT の Rivets 教授ら…	…, 米国 MIT の Rivest 教授ら…
51	上9行	…例えば, $M=1010_{(2)} = B_{(16)}$, …	…例えば, $M=1010_{(2)} = \mathbf{A}_{(16)}$, …
52	上12行	…, 最後の暗号ブロック C_2 を復号した後で, …	…, 最後の暗号ブロック C_3 を復号した後で, …
65	上6行	…ユーザ数 n に対して 2^n に比例…	…ユーザ数 n に対して $\mathbf{n^2}$ に比例…
137	上1行	…信 (③, ⑤), HTML に関わる処理…	…信 (③, ⑥), HTML に関わる処理…
141	下 14～13行	…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が…	…①～⑤, ⑦, ⑨までは主にサーバ管理者が, ⑥, ⑧はブラウザ側の利用者が…
150	上10行	…クライアント C はサーバ S の公開鍵証明書を…	…クライアント C はサーバ A の公開鍵証明書を…
163	上7行	CRPM/CPRM では, LKH 法を…	CPPM /CPRM では, LKH 法を…
191	第2章 問3 (2)	…dp=53, allow sip=20 …	…dp=53, allow dip =20 …
192	問2 (3) 2行目	$C_2 = P(60_{(16)} \oplus 2A_{(16)}) = P(01001010_{(2)}) = 49_{(16)}$	$C_2 = P(60_{(16)} \oplus \mathbf{AA}_{(16)}) = P(01001010_{(2)}) = \mathbf{69}_{(16)}$