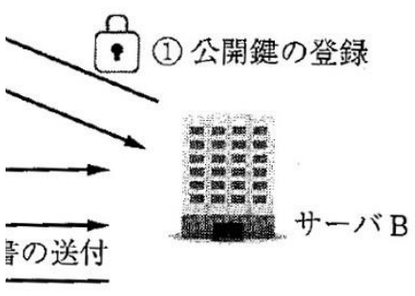
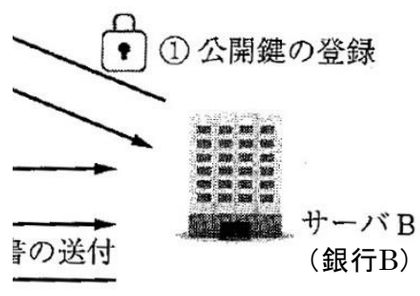
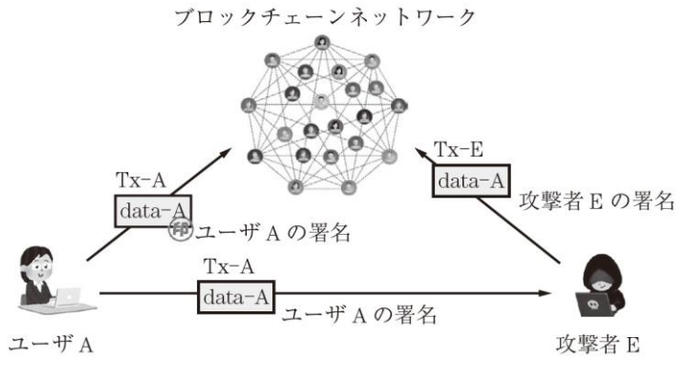
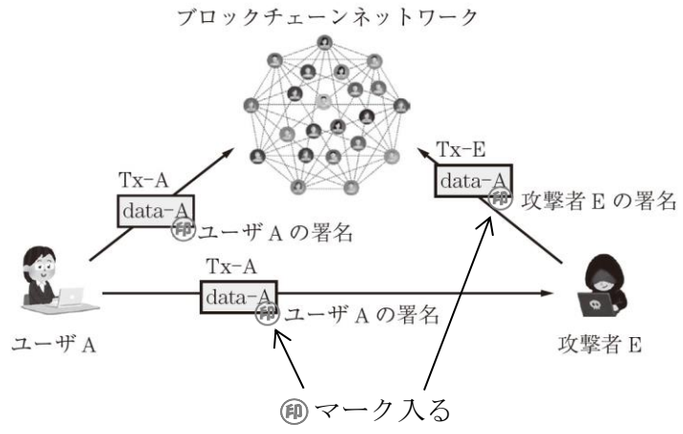
『入門 サイバーセキュリティ　理論と実践』　正誤表

このたびはお買い上げ誠にありがとうございます。本書には、下記のような誤記がありました。お詫びして訂正いたします。　（コロナ社）

ページ	箇所	誤	正
10	上から7行目	型攻撃で侵入…	型サイバー攻撃で侵入…
14	下から2行目	② ユーザがブラウザを…	② ユーザが脆弱なブラウザを…
15	上から2行目	される。	され，マルウェアに感染する。
21	引用・参考文献　2)	2) Japan Vulerability…	2) Japan Vulnerability…
36	3.1節　上から3行目～	…自然数aとの積…	…自然数cとの積…
38	上から14行目	… $q_{i-1} = r$と代入…	… $a_{i-1} = r$と代入…
39	上から8行目 （関係式の最終行）	$= \begin{pmatrix} -3 & 4 \\ 13 & 3 \end{pmatrix} \cdots$	$= \begin{pmatrix} -3 & 4 \\ 13 & -17 \end{pmatrix} \cdots$
41	例題3.4　解答 加算表 +0の列の数字	0 0 0 0 0	0 1 2 3 4
	例題3.4　解答 加算表の一番下の行 +1の列の数字	5	0
57	上から7行目	…まで波及するについて…	…まで波及するかについて…
65	引用・参考文献　1), 2)	1)　Diffie.W., Hellman,M. E. … 2)　Vanhoef, M., Piessens, F. …	1)　Vanhoef, M., Piessens, F. … 2)　Diffie.W., Hellman,M. E.　…
69	上から12行目	コミットメントの…	ナイーブなコミットメントの…
76	上から6行目	ワードk_{A}が奪取される。	ワードp_{A}が奪取される。
79	上から4行目	…銀行Bの公開鍵と…	…銀行Bのサーバの公開鍵と…
80	上から8行目	…が銀行Bに	…が銀行Bのサーバに
	下から4行目	…が銀行BにTLSで…	…が銀行BのサーバにTLSで…
81	図5.7の最下部	⑨　$E_k(m)$の送付	⑨ $E_{k'}(m)$の送付
	上から1行目	はkを使って…	はkから導出されたk'を使って…
	下から4行目	…わかる。サーバは全ユーザ公開鍵を…	…わかる。ユーザは全サーバの公開鍵を…
82	下から12行目	…いくつ0が並ぶか…	…いくつ0ビットが並ぶか…
107	下から6行目	…それから $x \in Z_q$をランダムに選び, $y = g^x \bmod p$ を…	…それから $s \in Z_q$をランダムに選び, $y = g^s \bmod p$ を…
	下から5行目	…秘密鍵$sk = x$を…	…秘密鍵$sk = s$を…
108	上から4行目	…，my^r $mod\, p$)　…	…，$m\, y^r \, mod\, p$)　…　（m，yはイタリック）
	上から6行目	… = c$^{-\lambda j(0) f(i_j)}$ …	…= $c^{-\lambda_j(0) f(i_j)}$　…　（c はイタリック。λj の添字 j は下付き）
111	上から14行目	…すなわち，$k \geq$ L という…	…すなわち，$k \geq L$ という…　（L はイタリック）
128	下から4行目	… FOWARED …	…　FORWARD　…
141	例題9.1 解答の2行目	…　$P(X_2 \mid Y)$　…	…　$P(X_{\mathrm{B}} \mid Y)$　…
	例題9.1 解答の式 2行目	$= \dfrac{P(Y \mid X_2)P(X_2)}{P(Y \mid X_1)P(X_1) + P(Y \mid X_2)P(X_2) + P(Y \mid X_3)P(X_3)} = \cdots$	$= \dfrac{P(Y \mid X_{\mathrm{B}})P(X_{\mathrm{B}})}{P(Y \mid X_{\mathrm{A}})P(X_{\mathrm{A}}) + P(Y \mid X_{\mathrm{B}})P(X_{\mathrm{B}}) + P(Y \mid X_{\mathrm{C}})P(X_{\mathrm{C}})} = \cdots$
143	下から5行目	…を積すること…	…を乗ずること…
158	図10.9　右側		
168	下から6行目	…（Altcoin）…	…（altcoin）…
170	上から10行目	…やイーアリアムなど…	…やイーサリアムなど…
195	図11.19 ①の右側	ガス	ETH（送金）
	上から1行目	…をセットする。② …	…をセットする。また，必要に応じてコントラクトに対するETHの送金をトランザクションに記載する。② …
200	上から2行目	になる。また，…	になる。さらに，不正な取引を強引にブロックに格納し，正しい取引として承認させる攻撃が可能である。また，…
202	上から11行目	…を実行した	…を実行する

ページ	箇所	誤	正
203	下から1行目	…する。さらに，秘	…する。さらに，
204	下から9行目	…を盗難したい…	…を窃取したい…
	下から1行目	…は盗難される。…	…は窃取される。…
205	上から5～6行目	…盗難された。**図12.4** は，盗難された…	…窃取された。**図12.4** は，窃取された…
	図12.4タイトル	盗難されたXEMの…	窃取されたXEMの…
206	上から4行目	盗難された…	窃取された…
	上から7行目	…と，盗難さ…	…と，窃取さ…
	上から12行目	…に盗難された…	…に窃取された…
207	図12.5		
209	上から5行目	必要になるのである。	必要になることに注意する。

最新の正誤表がコロナ社ホームページにある場合がございます。下記URLにアクセスして[キーワード検索]に書名を入力して下さい。
https://www.coronasha.co.jp