

正 誤 表

下記の部分に誤りがありましたので訂正させていただきます。
ご迷惑をおかけし大変申し訳ございません。

セキュリティ技術の教科書 第1版 第1刷

No	訂正箇所	誤	正
1	P. 28 図表 2-11	IT パケット長 (16)	IP パケット長 (16)
2	P. 31 (3)5 行目	…いずれも 192. 168. 20/24 で同じです。	…いずれも 192. 168. 10 /24 で同じです。
3	P. 45 5 行目	⑥FTP クライアントから FTP クライアントヘデータ用 TCP コネクションを確立する。	⑥FTP サーバ から FTP クライアントヘデータ用 TCP コネクションを確立する。
4	P. 95 図表 4-10 「アルゴリズムの分類」 2 行目	楕曲線暗号	楕円 曲線暗号
5	P. 168 (5)1 行目	5. 1. 2 節で個々に説明した機能のうち、…	5. 2. 2 節で個々に説明した機能のうち、…
6	P. 186, 187 図表 6-16, 6-17	⑤PUT serach.html HTTP/…	⑤PUT search .html HTTP/…
7	P. 242 本文 (ii), (iii)	(ii) 通常の名前解決では、問合せの送信元ポート番号と… (以下、省略) (iii) 通常の名前解決では、問合せの IP アドレスと… (以下、省略)	(iii) 通常の名前解決では、問合せの送信元ポート番号と… (以下、省略) (ii) 通常の名前解決では、問合せの IP アドレスと… (以下、省略) ※(ii)と(iii)の説明を丸ごと入れ替える。
8	P. 253 1 行目	あるいは、DH 鍵共有アルゴリズム (4. 4. 2 節参照) や DH アルゴリズムを強化した…	あるいは、DH 鍵共有アルゴリズム (4. 1. 2 節参照) や DH アルゴリズムを強化した…

No	訂正箇所	誤	正
9	P. 253 6, 7 行目	真正性・クライアントがサーバを認証するサーバ認証は必須仕様で、公開鍵暗号認証方式によって認証します。	真正性・クライアントがサーバを認証するサーバ認証は必須仕様で、 公開鍵認証方式 によって認証します。
10	P. 279 (1)13 行目, 図表 9-29 内, P. 281 (3)8, 9 行目	DAIMETER	DIAMETER

法令・規格・ガイドラインの更新情報

書籍に掲載している以下の内容につきまして、法令・規格・ガイドラインの更新がありましたので、お知らせ致します。

セキュリティ技術の教科書 第1版 第1刷

No	該当箇所	更新情報
1	P. 56 3.1.1 脅威の分類	出典の JIS Q 13335-1:2006 は、2017 年 12 月 20 日に廃止されました。セキュリティ対策において対象となる脅威には、意図的な脅威だけではなく、偶発的、環境といった観点があることも大切なので、この三つの観点を理解しておきましょう。
2	P. 91 図表 4-3	CRYPTREC 暗号リスト（平成 30 年 3 月 29 日版）が、2018/7/11 に公開されました。本書に記載している電子政府推奨暗号リストに関しては、共通鍵暗号の 3-key Triple DES が、次のように推奨暗号リストから外れて、運用監視暗号リストに移りました。 図表 4-3 電子政府推奨暗号リストの共通鍵暗号アルゴリズム 平成 29 年 3 月 30 日版：64 ビットブロック暗号 3-key Triple DES 平成 30 年 3 月 29 日版：64 ビットブロック暗号 該当なし