

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2刷

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
3	P. 263 FAQ 図表 9-13	TLS1.3 に関して、2018/3 に IETF がドラフト 28 を正式に承認しました。最新のドラフト 28 では、TLS1.2 との互換性に配慮して、ChangeCipherSpec が復活して規定されています。

株式会社アイテック