S703341-20，S902026-20

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3版 第1刷（電子書籍版含む）

No.	訂正箇所	誤	正
1	P.30 図表 2-9 のレイヤー5	セョション層	セッション層
2	P.112 図表 4-1 の 1 行目	RSASSA-PKCS-v1_5	RSASSA-PKCS1-v1_5
3	P.121 図表 4-14 の 4 行目	RSASSA-PKCS-v1_5	RSASSA-PKCS1-v1_5
4	P.151 下から 2，3 行目	OSCP サーバは OSCP レスポンダとも呼ばれます。	OCSP サーバは OCSP レスポンダとも呼ばれます。
5	P.188，P.189	問 4-22　FIDO UAF1.1 に基づく認証処理 問 4-23　リスクベース認証に該当するもの	問 4-22　リスクベース認証に該当するもの 問 4-23　FIDO UAF1.1 に基づく認証処理 ※解答・解説の問番号の順序が逆になっております。
6	P.242 (1)②最終行	図表 6-14 のような認証画面を出力する。	図表 6-15 のような認証画面を出力する。
7	P.276 問 6-4　選択肢イ	イ　’ OR ユーザ名 = ’ ユーザ名	イ　’ OR ユーザ名 = ’ユーザ名 ※二つ目の「ユーザ名」の直前の半角アキを詰めております。
8	P.324 ①の最終文	上位 DNS サーバは，KSK 秘密鍵で DS レコードに署名する。	上位 DNS サーバは，ZSK 秘密鍵で DS レコードに署名する。
9	P.344 上から 4 行目	過去の暗号化過信の安全性が保持される特性を PFS（前方秘匿性）といいます。	過去の暗号化通信の安全性が保持される特性を PFS（前方秘匿性）といいます。
10	P.352 下から 1 行目	プロキシサーバ証明書の CN には Web サーバの CN を設定する。	プロキシサーバ証明書の CN 及び SAN には，接続先の Web サーバの FQDN，もしくは Web サーバ証明書の CN 及び SAN を設定する。
11	P.367 下から 7 行目	・DH 鍵共通アルゴリズムによる共通鍵と MAC 鍵の共有	・DH 鍵交換アルゴリズムによる共通鍵と MAC 鍵の共有

12	P.370 上から 1 行目	・DH 鍵共通アルゴリズムによる共通鍵と MAC 鍵の共有	・DH 鍵**交換**アルゴリズムによる共通鍵と MAC 鍵の共有
13	P.370 図表 9-35 のタイトル下	（事前共有鍵認証方式の場合。網掛けは暗号化。IKEv2 ヘッダは省略。）	（**デジタル署名**認証方式の場合。網掛けは暗号化。IKEv2 ヘッダは省略。）
14	P.379 図表 9-39 の最終行	CCMP（AES／CNSA）＋MAC	**G**CMP（AES／CNSA）＋MAC
15	P.380 上から 17，18 行目	WPA3-パーソナルにおいて，脆弱性のある WPA2 の鍵交換方式の 4Way ハンドシェイクに代えて，SAE という新しい鍵交換方式が採用された。	WPA3-パーソナルにおいて，**WPA2 の 4Way ハンドシェイクの前に，SAE という ECDHE を用いる鍵交換及び相互認証を安全に行う新しい方式が追加され，接続ごとに異なる PMK が共有されるようになった。**
16	P.384 問 9-10 の上から 1，6 行目	WPA（Wi-Fi Protected Access）［⇒P.379］や WPA2［⇒P.379］では，（中略）このため，WPA2-Enterprise では，（後略）	WPA（Wi-Fi Protected Access）［⇒P.379］や WPA2［⇒P.379］，**WPA3［⇒P.379］**では，（中略）このため，WPA**3**-Enterprise では，（後略）
17	P.400 左の段　三つ目の用語	curl コマンド：substitute user do コマンド	curl コマンド：**client for URL コマンド など**
18	P.406 下から 8 行目	アクセス権限のある複数のシステムを認証動作なしに利用できるようにする認証の仕組みです。	アクセス権限のある複数のシステムを認証**操作**なしに利用できるようにする認証の仕組みです。
19	P.416 図表 10-15 の直前の文	そのため，攻撃時には，②のセッション（図の青色のメッセージ）は攻撃者と Web サービス A 間，④の Web サービス A へのセッションは利用者と Web サービス A 間という異なるセッションになるので，対策として有効になります。	そのため，攻撃時には，②のセッションは攻撃者と Web サービス A 間，④の Web サービス A へのセッション（図の青色のメッセージ）は利用者と Web サービス A 間という異なるセッションになるので，対策として有効になります。 ※「(図の青色のメッセージ)」の挿入位置を変更しております。
20	P.419 ⑦の上から 4 行目，⑧	PSK（C：TGS）で Skey（C：A1）を暗号化した情報と，PSK（TGS：A1）で ST 及び Skey（C：A1）を暗号化した情報をクライアントに応答する。 ⑧クライアントは，PSK（C：TGS）で Skey（C：A1）を復号する。	**Skey**（C：TGS）で Skey（C：A1）を暗号化した情報と，PSK（TGS：A1）で ST 及び Skey（C：A1）を暗号化した情報をクライアントに応答する。 ⑧クライアントは，**Skey**（C：TGS）で Skey（C：A1）を復号する。
21	P.424 問 10-6　図中上部	真ん中：Web サービス A（クライアント） 右　側：Web サービス B（サービスプロバイダ）	真ん中：Web サービス **B**（クライアント） 右　側：Web サービス **A**（サービスプロバイダ）
22	P.451 上から 3 行目	調査に必要な情報（スナップショットを保存します。	調査に必要な情報（スナップショット**）**を保存します。
23	P.469 図表 11-9 の上から 4 行目	RSASSA-PKCS-v1_5	RSASSA-PKCS**1**-v1_5