

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. 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 <b>リスクベース認証に該当するもの</b> 問 4-23 <b>FIDO UAF1.1 に基づく認証処理</b> ※解答・解説の問番号の順序が逆になっております。
2	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。
3	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、 <b>ZSK</b> 秘密鍵で DS レコードに署名する。
4	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 <b>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</b> を設定する。
5	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。)	( <b>デジタル署名</b> 認証方式の場合。網掛けは暗号化。 IKEv2 ヘッダは省略。)
6	P. 380 上から 17, 18 行目	<b>WPA3-パーソナル</b> 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。	<b>WPA3-パーソナル</b> において、 <b>WPA2 の鍵交換方式の 4Way ハンドシェイクの前に、SAE という新しい鍵交換方式が追加され、接続ごとの PSK が動的に共有されるようになった。</b>
7	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: <b>client for URL</b> コマンド など
8	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>B</b> (クライアント) 右側: Web サービス <b>A</b> (サービスプロバイダ)
9	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。