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.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。
2	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。
3	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。
4	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。
5	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。
6	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。
7	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。）
8	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。
9	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

10	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。
11	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）
12	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。