

正誤表

よくわかるマスター
CompTIA Security+問題集 試験番号:SY0-101対応

FPT0417

【改版時期】

奥付日付	版数
2004年11月23日	第1版
2007年09月03日	第2版
2008年08月11日	第3版

【修正箇所】

ページ数	誤	正	修正版数
P 30	問題 89 c. 信頼性	c.冗長性	第3版
P 64	問題 89 解答 c 解説 5行目 ・・・ユーザの信頼性を確保することが できます。そのため、選択肢cが 正解となります。 解説 8～9行目 完全性とは、データの改ざんや破壊を 防ぐことをいいます。	解答 d 解説 5行目 ・・・データの完全性を確保することができま す。そのため、選択肢dが 正解となります。 解説 8～9行目 完全性とは、・・・ (削除)	第3版
P142	問題7 選択肢 d. 否認防止	d. 機密性の確保	第3版
P151	問題7 解答 d 解説 1行目 デジタル署名では、改ざん検出と否認 防止が実現できます。 解説 5行目 盗聴を防止することができません。 解説 7行目 可用性、完全性は情報セキュリティ全 般に使われる言葉です。	解答 c 解説 1行目 デジタル署名では、完全性を確保するた めの改ざん検出が実現できます。 解説 5行目 機密性を確保するための盗聴防止は実現 されません。 解説 7行目 可用性はデジタル署名には関連していま せん。	第3版

【修正箇所】

ページ数	誤	正	修正版数
P158	問題26	(最終行に追加) メッセージダイジェストも改ざんを検知するために利用される技術ではありますが、デジタル署名では、メッセージダイジェストを作成した上、それを更に送信者の秘密鍵で暗号化することで、より完全性を高められます。	第3版
P 10	2 受験費用 ComTIA Security +認定資格は	2 受験費用 文章を全て削除	第2版
P 10.	2 受験費用 表内の受験料 ¥28,140	¥29,853	第2版
P 10..	2 受験費用 表の下 (※2004年8月現在)	(※2007年8月現在)	第2版
P 16	問題8 a. Bonik	a. Boink	第2版
P 17	問題11 選択肢 b.パケットを送るとき(毎回)	問題11 選択肢 b.パケットを送るとき(任意のタイミング)	第2版
P 19	問題25 問題文 ワンタイムパスワード方式と同じ認証方式はどれですか。	ワンタイムパスワード方式で用いられる認証情報・機器はどれですか。	第2版
P 29	問題79 ハッシュ化されたパスワードが脆弱となる攻撃手法はどれですか。	パスワードがハッシュ化されていても実行が可能で、かつ実行が容易な攻撃手法はどれですか。 ※問題文を変更。選択肢は変更なし。また、60ページの解答解説も変更。	第2版
P 31	問題1 解説 1行目後半 またはパケットスニファアと	またはパケットスニファア、ネットワークアナライザア、プロトコルアナライザアなどと	第2版
P 33	問題8 解説 2行目 ・・・同様の攻撃をBonikといます。	・・・同様の攻撃をBoinkといます。	第2版

【修正箇所】

ページ数	誤	正	修正版数
P 60	問題79 解説 Man in the Middle攻撃とは・・・ (以下全文)	Man in the Middle攻撃とは、通信を行う2者間に入り込み、送信先のホストになります攻撃手法です。たとえば、AとBの2者間で通信が行われていた場合、悪意のある第三者をCとすると、CはAに対して自分がBであるようにデータを送信させ、ハッシュ化したパスワードはそのまま流用したうえで、Bに対し自分があたかもAであるように改ざんしたデータを送信します。 リバースエンジニアリングとは、システムを分解、解析することによってシステムの構成要素や仕組みを解説する方法です。 DDoS (Distributed Denial of Service) 攻撃とは、踏み台とした複数のコンピュータから攻撃対象に向けて一斉に攻撃させる手法です。 ブルートフォース攻撃とは、感がえられるすべてのパスワードを総当りで試すパスワードクラック手法です。 このうち、パスワードがハッシュ化されていても実行が可能なのは、aとdですが、ブルートフォース攻撃は、一度ハッシュパスワードを取得すれば、ツールを用いて比較的簡単に攻撃できるのに対し、Man in the Middle 攻撃は、通信を行う2者間に入り込んでタイミングよくなりすます必要があるので、辞書攻撃に比較すると一般的に攻撃難易度が高いと考えられます。 よって、選択肢dが解答となります。	第2版
P 60.	問題79 解答 a	解答 d	第2版
P 72	問題18 選択肢 d. UDP1723とTCP1701	d. TCP1723とUDP1701	第2版
P 83	問題6 解説 3行目 ・・・正解となります。	・・・正解となります。しかし、WEPの暗号化強度は弱いため現在ではWPA、WPA2などのより強度の高い暗号化方式の企画が用いられることも多いです。	第2版
P 88	問題19 解説 5行目 WEPは、40ビットまたは128ビット・・・	WEPは、40ビットまたは104ビット・・・	第2版
P 94	問題37 解説 7～8行目 ・・・RFC2246で標準化されており、SSLとの相互互換性を有しています。	・・・RFC2246で標準化されていますが、SSLとの相互運用性はありません。	第2版
P 95	問題41 解説 3～4行目 ・・・TLSはSSLと互換性があり、・・・	・・・TLSはSSLと類似性があり、・・・	第2版

【修正箇所】

ページ数	誤	正	修正版数
P 99	問題54 解説	WebサーバにおいてCGI(Common Gateway Interface)を用いる場合、フォームなどを利用し、Webブラウザからのリクエストを受け付けます。HTMLファイルが置かれているディレクトリに対し、必要以上に権限を与えてしまうと、CGIプログラムに脆弱性が見つかった場合、サーバ内部を攻撃される可能性が高くなります。そのため、HTMLファイルのように決まったファイル名のものを参照するだけであれば、読み込み(そのディレクトリの中身を見たり、中のファイルを検索する許可)および書き込み(ディレクトリの中にファイルを作ったり、ディレクトリのファイルを削除したりする許可)権限は与えるべきではありません。このため、HTMLファイルが置かれているディレクトリに対しては、実行権限(ディレクトリのファイルにアクセスする権限)のみ与えるべきです。そのため、選択肢aが正解となります。(解説を丸ごと差し替え)	第2版
P106	問題9 選択肢 c. スイッチにてブロードキャスト通信を禁止している	c. スイッチにてポートミラーリングを禁止している	第2版
P108	問題19 問題文 特定のあて先ホストに到達するまでのルータ・・・	特定のあて先ホストに到達するまでの経路・・・	第2版
P109	問題24 選択肢 a. セキュリティ侵害の可能性を検出し、ユーザを強制的にログオフさせる。	a. セキュリティ侵害の可能性を検出し、通知する。	第2版
P114	問題49 問題文 ・・・対策として当てはまらないものはどれですか？	・・・対策として当てはまるものはどれですか？	第2版
P115	問題54 選択肢 a. UPS(Uninterruptible Power Supply)	a. IDS (Intrusion Detection System)	第2版
P119	問題9 解説 5行目 ・・・パケットを解析するように、ブロードキャスト通信を・・・ 7行目 通常のスイッチでは、ブロードキャスト通信が・・・	・・・パケットを解析するように、ポートミラーリングを・・・ 通常のスイッチでは、ポートミラーリングが・・・	第2版

【修正箇所】

ページ数	誤	正	修正版数
P124	問題24 解説 5～7行目 ・・・管理者へ警告を通知し、場合によっては・・・シャットダウンさせます。そのため、選択肢aが正解となります。	・・・管理者へ警告を通知します。そのため、選択肢aが正解となります。	第2版
P133	問題49 解答 d 解説 2行目 ・・・選択肢a、b、cとなります。 10行目 ・・・そのため、選択肢dが正解となります。	解答 a 解説 2行目 ・・・選択肢aとなります。 10行目 「そのため、」以降を削除	第2版
P135	問題54 解説 6行目～8行目 UPS(Uninterruptible Power Supply)・・・稼働させるための電源装置のことです。	IDS(Intrusion Detection System)は、日本では侵入検知システムとも呼ばれます。すなわち、コンピュータやネットワークに対する不正行為を検出し、通知するためのシステムのことです。 文章丸ごと変更	第2版
P149	問題2 解説 3行目 X.509ではバージョン3から・・・	X.509ではバージョン2から・・・	第2版
P153	問題14 解説 5行目 致命的な弱点が報告されていません。	ファイルの破損確認のためのチェックサム発行時や、APOPパスワード送信時など広く用いられています。	第2版
P177	問題40 問題文 電磁波のセキュリティ対策として、・・・ 問題42 選択肢 a.OSスキャン	電磁波のセキュリティ対策を考えるとときの脆弱性について、・・・ a.ポートスキャン	第2版
P186	問題20 解答 a 解説 6行目 ・・・選択肢aが正解となります。	b ・・・選択肢bが正解となります。	第2版
P194	問題42 解説 6行目 OSスキャンとは、ポートスキャンのことをいいます。	削除	第2版
P183	問題12 解説8行目 定量的リスク分析では、リスク値を数値で表します。	定性的リスク分析では、リスク値を数値で表します。	第0版