【訂正情報】
商品コード：110-4971
改訂 5 版 個人情報保護士認定試験公式テキスト

◎本書の記述において下記のような誤りがありました。訂正してお詫び申し上げます。
【2016 年 12 月 1 日現在】

刷	頁	訂正箇所	訂正前	訂正後
↓ 本文				
1	p28	7 行目	維持することが求められている。	バランスよく維持・改善し、リスクを適切に管理することが求められている。
		16 行目	英国規格 BS 7799-2:2002 を基に国際規格化された **ISO/IEC27001：2005** を～	英国規格 BS 7799-2 を基に国際規格化された **ISO/IEC27001** を～
		17 行目	**JIS Q 27001：2006「情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」**である。	JIS Q 27001 である。2013 年に国際規格が改訂されたことに伴い、国内規格も、JIS Q 27001:2014「情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」に改訂された。
1	p29	図表 1-8 ISMS 適合性評価制度 基準となる規格	JIS Q 27001：2006 ／ISO/IEC27001：2005 （国際基準）	JIS Q 27001：2014 ／ISO/IEC27001：2013 （国際基準）
1	p67	(3)「保有個人データ」に関する義務　1 行目	6 ヶ月以上保有する～	6 ヶ月を越えて保有する～
1	p96	過去問題チェック 2	以下のとおり差し替え **2．個人情報の利用目的による制限に関する以下のアからエまでの記述のうち、誤っているものを 1 つ選びなさい。** ア．個人情報取扱事業者は、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、原則として、あらかじめ本人の同意を得なければならない。 イ．個人情報取扱事業者が、企業の分社化により他の個人情報取扱事業者から事業の承継をすることに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。 ウ．個人情報取扱事業者が、統計法による国勢調査などの基幹統計調査に対する報告を行う場合は、あらかじめ本人の同意を得る必要がある。 エ．個人情報取扱事業者たる健康保険組合の保険者が実施する健康診断等の保険事業について、受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的とした統計調査のために、個人名を伏せて研究者に提供する場合は、あらかじめ本人の同意を得る必要はない。 〈第 40 回出題　問題 14〉	

【訂正情報】
商品コード：110-4971
改訂 5 版 個人情報保護士認定試験公式テキスト

刷	頁	訂正箇所	訂正前	訂正後
↓ 本文				
1	p177	下から 2 行目	災害対策の分野で利用される	災害対策等の分野で利用される。
1	p192	(2) 個人情報ファイル (マイナンバー法 2 条 4 項) 5 行目～	なお、個人情報ファイルは「個人情報」であることが前提なので、個人情報ファイルには死者の情報を含まない。	削除
1	p230	問題 10 上から 14 行目	～あることから、特例的な対応方法が示されている。 〈マイナンバー実務検定2級 第3回出題問題55〉	～であることから、特例的な対応方法が示されている。 ア．Aのみ正しい。 イ．Bのみ正しい。 ウ．Cのみ正しい。 エ．すべて誤っている。 〈マイナンバー実務検定2級 第3回出題問題55〉
1	p270	1 要求される管理体制 3 行目	(35 条)	(31条)
1	p272	(5) 個人情報の苦情・相談窓口 3 行目	個人情報保護法 35 条で要求される	個人情報保護法31条で要求される
1	p312	1 苦情への対応　1 行目	個人情報保護法 35 条	個人情報保護法31条
1	p315	4 本人からの開示請求への対応　2 行目	(28 条)	(25条)

【訂正情報】
商品コード：110-4971
改訂 5 版 個人情報保護士認定試験公式テキスト

刷	頁	訂正箇所	訂正前	訂正後
↓ 本文				
1	p380 ～381	情報システム設備のガイドライン	以下のとおり差し替え	

p380～381

第 4 節 情報システム設備のガイドライン

1 JIS Q 27002:2014 の概要

JIS Q 27002:2014 は、組織が情報セキュリティマネジメントを実施するプロセスにおいて管理策を選定するための参考として用いる手引きを記載している（第 1 章第 2 節 4 「ISMS 適合性評価制度」参照）。

(1) JIS Q 27002:2014 の体系

JIS Q 27002:2014 は、情報セキュリティー管理の管理目的や管理策を規定している。規格書の 1 から 4 では規格の構成、5 から 18 では管理策が記載されている。

1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 規格の構成
5. 情報セキュリティのための方針群
6. 情報セキュリティのための組織
7. 人的資源のセキュリティ
8. 資産の管理
9. アクセス制御
10. 暗号
11. 物理的及び環境的セキュリティ
12. 運用のセキュリティ
13. 通信のセキュリティ
14. システムの取得、開発及び保守
15. 供給者関係
16. 情報セキュリティインシデント管理
17. 事業継続マネジメントにおける情報セキュリティの側面
18. 順守

(2) 「11. 物理的および環境的セキュリティ」の概要

JIS Q 27002:2014 の 11「物理的および環境的セキュリティ」では、オフィスセキュリティに関する管理策が規定されている。

11.1 セキュリティを保つべき領域
目的：組織の情報および情報処理施設に対する許可されていない物理的アクセス、損傷および妨害を防止するため

情報処理施設および情報に対して認可されていないアクセスや損傷、妨害を防御するため、次の 6 つの管理策から構成されている。

11.1.1 物理的セキュリティ境界
物理的セキュリティ境界は、施設および情報を保護するために必要なセキュリティ区画の設定・管理の手引きである。オフィスに対して、物理的に頑丈にする、ゾーニングの設定を行う、有人の受付を作る、などの対策がある。

11.1.2 物理的入退管理策
物理的入退管理策は、許可されたものだけにアクセスを許す方法である。ゾーニング設定を行った領域間で、訪問者の記録をとる入退管理や、ゾーニング内でアクセスカードや二要素認証の仕組みの導入を実施するなどの対策をする。

11.1.3 オフィス、部屋および施設のセキュリティ
情報処理施設などの重要設備の表示を最小限にする、扉や窓は外部からの防御を厳重にするなど、オフィス内部のセキュリティを強化することが重要である。

11.1.4 外部および環境の脅威からの保護
火災、洪水、地震などの自然災害または人的災害からの物理的な保護をする。

11.1.5 セキュリティを保つべき領域での作業
セキュリティを保つべき領域での作業に関する物理的な保護の設計をする。セキュリティを保つべき領域の存在は、知る必要があるものだけが知るという原則を適用する。

11.1.6 受渡場所
許可されていないものが立ち入ることもある場所を管理する。

11.2 装置
目的：資産の損失、損傷、盗難又は劣化および組織の業務に対する妨害を防止するため

資産の損失や劣化および組織の活動に対する妨害を防止するため、装置を物理的に保護する次の 9 つの管理策から構成されている。

11.2.1 装置の設置および保護
装置は、環境上の脅威および災害からのリスク、ならびに許可されていないアクセスの機会を低減するように保護する。

11.2.2 サポートユーティリティ
サポートユーティリティ（たとえば、電気、給水、空調）が正しく機能することを確実にするため、定期的な点検や検査を行うことが望ましい。

11.2.3 ケーブル配線のセキュリティ
電源ケーブルや通信ケーブルは、損傷や傍受から保護することが望ましく、可能な限り地下に埋設する。

11.2.4 装置の保守
装置は、可用性および完全性を維持するために、保守が必要である。保守を実施した場合は、保守装置の搬入出や保守作業の記録を取らなくてはならない。

11.2.5 資産の移動
装置、情報などは、事前の許可なしでは、構外に持ち出さないことが望ましい。

11.2.6 構外にある装置および資産のセキュリティ
セキュリティリスク（たとえば、損傷、盗難、傍受）は、場所によって大きく異なる場合がある。それぞれの場所に応じた最も適切な管理策を設定する。

11.2.7 セキュリティを保った処分または再利用
取り扱いに慎重を要する情報を格納した装置は、物理的に破壊するか確実に上書きすることが望ましい。

刷	頁	訂正箇所	訂正前	訂正後
↓ 本文				
2	p382	情報システム設備のガイドライン	以下のとおり差し替え	

p382

11.2.8 無人状態にある利用者装置
無人状態にある装置が適切な保護対策を実施していること。

11.2.9 クリアデスク・クリアスクリーン方針
書類および取り外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用することが望ましい。