

情報処理技術者スキル標準 2005年11月30日版における更新内容

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	表 紙	3. スキル基準 10 4. 知識体系 27	3. スキル基準 10 4. 知識体系 28	ページ番号修正
情報セキュリティ アドミニストレー タ	表 紙		参考 テクニカルエンジニア(情報セキュリ ティ)と情報セキュリティアドミニストレータの相 違	新規追加
情報セキュリティ アドミニストレー タ	2	1.3 「情報処理技術者スキル標準」の構成  (以下の 、 、 )対象者像に必要な知識・技 術・能力や達成指標を、	(次の 、 、 )対象者像に必要な知識・技術・ 能力や達成指標を、	「以下の」から「次の」へ 置き換え
情報セキュリティ アドミニストレー タ	2	1.3 「情報処理技術者スキル標準」の構成  「情報処理技術者スキル標準」は、以下に示す3 種類の技術的な情報として構成され、	「情報処理技術者スキル標準」は、次に示す3種 類の技術的な情報として構成され、	「以下の」から「次の」へ 置き換え
情報セキュリティ アドミニストレー タ	3	1.4 「情報セキュリティアドミニストレータ」像 とスキル標準  情報セキュリティアドミニストレータに対して は、以下のスキル標準が適用される。	情報セキュリティアドミニストレータに対して は、次のスキル標準が適用される。	「以下の」から「次の」へ 置き換え
情報セキュリティ アドミニストレー タ	3		補注)以降、このスキル標準においては、ディジ タルとアナログの両面を対象とする場合には「情 報セキュリティ」と表記し、主にデジタルのみ を対象とする場合には「セキュリティ」と表記し ている。ただし、他に慣用的な表記方法がある場 合は、その限りではない。	新規追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	4	2．主要業務 図2-1に示す7種類の基本的な「アクティビティ」 に分解されている。	図2-1に示す8種類の基本的な「アクティビティ」 に分解されている。	「7」種類から「8」種類へ 修正
情報セキュリティ アドミニストレー タ	4	2．主要業務 図2-1 情報セキュリティマネジメントプロセス 情報セキュリティ方針の策定	情報セキュリティ基本方針の策定	「基本」を追加、以下同様 に「情報セキュリティ方針」 は「情報セキュリティ基本 方針」に用語統一
情報セキュリティ アドミニストレー タ	4	2．主要業務 図2-1 情報セキュリティマネジメントプロセス 情報セキュリティ基準の策定	情報セキュリティ対策基準の策定	「対策」を追加、以下同様 に「情報セキュリティ基準」 は「情報セキュリティ対策 基準」に用語統一
情報セキュリティ アドミニストレー タ	4	2．主要業務 図2-1 情報セキュリティマネジメントプロセス セキュリティの分析	セキュリティ事件・事故への対応	名称変更
情報セキュリティ アドミニストレー タ	4	2．主要業務 図2-1 情報セキュリティマネジメントプロセス セキュリティポリシーの策定	情報セキュリティポリシーの策定	用語の統一
情報セキュリティ アドミニストレー タ	4	2．主要業務 図2-1 情報セキュリティマネジメントプロセス セキュリティポリシーの見直し	セキュリティ対策の見直し	名称変更
情報セキュリティ アドミニストレー タ	4	2．主要業務 図2-1 情報セキュリティマネジメントプロセス	セキュリティシステムの開発管理	新規追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ		2．主要業務  本スキル標準においては、情報セキュリティマネジ メントプロセスが <u>以下</u> のような形式で提示され る。	本スキル標準においては、情報セキュリティマネ ジメントプロセスが <u>次</u> のような形式で提示され る。	「以下の」から「次の」へ 置き換え
情報セキュリティ アドミニストレー タ	4	2．主要業務  「セキュリティ方針の策定」、「セキュリティ基 準の策定」、「セキュリティシステムの設計」	「情報セキュリティ基本方針の策定」、「情報セ キュリティ対策基準の策定」、「セキュリティシ ステムの機能設計」	用語の統一
情報セキュリティ アドミニストレー タ	4	2．主要業務  「 <u>セキュリティの分析</u> 」、および「セキュリティ の見直し」	「 <u>セキュリティ事件・事故への対応</u> 」、および「セ キュリティ対策の見直し」	用語の統一
情報セキュリティ アドミニストレー タ	4	2．主要業務  「利用者教育」などの業務において、	「利用者教育」、「 <u>セキュリティ対策の見直し</u> 」な どの業務において、	追加
情報セキュリティ アドミニストレー タ	4	2．主要業務  この過程で、「セキュリティポリシーの策定」 ・ ・ ・	この過程で、「 <u>情報セキュリティポリシー</u> の策 定」 ・ ・ ・	用語の統一
情報セキュリティ アドミニストレー タ	4	2．主要業務  ・ ・ <u>業務を通して</u> 役割を果たす。	<u>業務において</u> 、主体的に役割を果たす。	情報セキュリティアドミニ ストレータの立場を明確化

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	4	2. 主要業務  ・ <u>業務を通して役割を果たす。</u>	<u>それ以外の業務においては、主体的に役割を果たす場合と、他者と共同して、または他者の支援を得ながら役割を果たす場合がある。</u>	情報セキュリティアドミニストレータの立場を明確化
情報セキュリティ アドミニストレー タ	5	1. セキュリティ方針の策定	1. <u>情報セキュリティ基本方針</u> の策定	用語の統一
情報セキュリティ アドミニストレー タ	5	1-1 情報資産の評価  (情報システム、データ、人材、 <u>ドキュメント</u> など)	(情報システム、データ、人材、 <u>文書</u> など)	用語の統一
情報セキュリティ アドミニストレー タ	5	1-1 情報資産の評価  ・ ・などを整理し、ヒアリングなどを通じて・ ・	・ ・などを整理し、 <u>文書精査</u> 、ヒアリングなどを通じて・ ・	テクニカルエンジニア(情報セキュリティ)との整合性
情報セキュリティ アドミニストレー タ	5	1-2 <u>脅威の認識</u>	1-2 <u>リスクの認識</u>	扱うべき情報は脅威だけでなく脆弱性も必要であり合わせてリスクと表現する
情報セキュリティ アドミニストレー タ	5	1-2 脅威の認識  現代社会に対する <u>脅威</u> の情報を広く収集し、分析、整理する。	現代社会における一般的なリスク( <u>脅威および脆弱性</u> )の情報を広く収集し、分析、整理する。	扱うべき情報は脅威だけでなく脆弱性も必要である
情報セキュリティ アドミニストレー タ	5	1-3 リスクの識別  脅威がもたらす企業の・ ・	<u>脅威および脆弱性</u> がもたらす企業の・ ・	扱うべき情報は脅威だけでなく脆弱性も必要である
情報セキュリティ アドミニストレー タ	5	1-5 リスクの評価	1-5 リスクの <u>算定と評価</u>	業務概要をより詳しく反映

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	5	1-5 リスクの評価  整理されたすべてのリスクに関して、 <u>発生確率</u> <u>を推定するとともに、定性的、定量的に評価し、</u> <u>リスクの現実化による損害コストとリスク軽</u> <u>減の対策コスト、・・・</u>	整理されたすべてのリスクに関して、 <u>リスクが発</u> <u>現する確立およびリスクが発現した場合の影響</u> <u>の大きさを定量的または定性的に把握すること</u> <u>でリスクの値を算定する。さらに、リスクの現実</u> <u>化による損害コストとリスク軽減の対策コス</u> <u>ト、・・・</u>	テクニカルエンジニア（情 報セキュリティ）との整合 性
情報セキュリティ アドミニストレー タ	5	1-5 リスクの評価  および対策を施しても残存するリスクを考慮 して、 <u>リスク対応にランクをつける。</u>	および対策を施しても残存するリスクを考慮し て、 <u>リスク対策の優先順位を決定する。</u>	テクニカルエンジニア（情 報セキュリティ）との整合 性
情報セキュリティ アドミニストレー タ	5	1-6 セキュリティ方針の策定	1-6 <u>情報セキュリティ基本</u> 方針の策定	用語の統一
情報セキュリティ アドミニストレー タ	5	1-6 セキュリティ方針の策定  企業のセキュリティ方針を策定する	企業の <u>情報セキュリティ基本</u> 方針を策定する	用語の統一
情報セキュリティ アドミニストレー タ	5	2 . セキュリティ基準の策定	2 . <u>情報セキュリティ対策</u> 基準の策定	用語の統一
情報セキュリティ アドミニストレー タ	5	2-1 企業活動一般のセキュリティ規定の作成  規定とセキュリティポリシーに不整合がないか を・・・	規定と <u>情報セキュリティ</u> ポリシーに不整合がない かを・・・	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	5	2-2 情報システムのセキュリティ規定の作成  規定とセキュリティポリシーに不整合がないかを・・	規定と <u>情報</u> セキュリティポリシーに不整合がないかを・・	用語の統一
情報セキュリティ アドミニストレー タ	6	3 . セキュリティシステムの設計	3 . セキュリティシステムの <u>機能</u> 設計	「機能」追加
情報セキュリティ アドミニストレー タ	6	3-2 物理セキュリティのコントロール  物理ネットワーク基盤の保護方法、セキュリティを担保する物理装置(特にモバイル機器)を決定し、	物理ネットワーク基盤の保護方法、(特にモバイル機器に関して)セキュリティを担保する物理装置を決定し、	文書を前後入れ替え
情報セキュリティ アドミニストレー タ	6	3-5 データの機密保持	3-5 データの <u>セキュリティ</u>	より広い意味の表現に変更
情報セキュリティ アドミニストレー タ	6	3-5 データのセキュリティ  データの暗号などの方策を決定する。	データの暗号化などの方策を決定する。	誤りを修正
情報セキュリティ アドミニストレー タ	6	3-6 セキュリティ運用手続きの作成  セキュリティ監視結果の <u>情報</u> の保管方法を決定する	セキュリティ監視結果の <u>データ</u> の保管方法を決定する	分析前のため情報ではなくデータとした

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	7	4-2 セキュリティシステムの開発  セキュリティシステムの設計要件を実装する適 当なセキュリティ製品が存在しない場合、必要に 応じて独自にソフトウェア開発を行う。		5-1 に移動
情報セキュリティ アドミニストレー タ	7	4-3 セキュリティ実装の確認  システム、サーバあるいは・・・	情報システム、サーバあるいは・・・	用語の統一
情報セキュリティ アドミニストレー タ	7		<u>5 . セキュリティシステムの開発管理</u>	新規追加
情報セキュリティ アドミニストレー タ	7		5-1 <u>セキュリティシステムの開発管理</u>  <u>セキュリティシステムの設計要件を満たす適 当なセキュリティ製品が存在しない場合、必要に 応じて独自ソフトウェアの開発を指示し、費用対効 果の確認と工程管理を行う。</u>	4-2 から移動
情報セキュリティ アドミニストレー タ	7	<u>5 . セキュリティシステムの運用管理</u>	<u>6 . セキュリティシステムの運用管理</u>	番号変更
情報セキュリティ アドミニストレー タ	7	<u>5-1 セキュリティ運用手続きの実施</u>	<u>6-1 セキュリティ運用手続きの実施</u>	番号変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	7	5-1 セキュリティ運用手続きの実施  セキュリティシステムの設計結果を実装した運 用手続きをレビューし	実装したセキュリティシステムの運用手続きを レビューし	「設計結果を実装した」を 削除、「実装した」を追加
情報セキュリティ アドミニストレー タ	7	5-2 システム動作の監視と記録	6-2 システム動作の監視と記録	番号変更
情報セキュリティ アドミニストレー タ	7	5-2 システム動作の監視と記録  セキュリティシステムの設計で決定したセキュ リティ監視項目の範囲で、	セキュリティシステムの機能設計で決定したセ キュリティ監視項目の範囲で	「機能」追加
情報セキュリティ アドミニストレー タ	7	5-3 システム保守	6-3 システム保守	番号変更
情報セキュリティ アドミニストレー タ	7	5-4 利用者教育	6-4 利用者教育	番号変更
情報セキュリティ アドミニストレー タ	7	5-3 システム保守  セキュリティ組織（C E R E T / C C）や・・・	セキュリティ組織（JPCERT/CC、IPA）や・・・	誤りを修正
情報セキュリティ アドミニストレー タ	7	5-3 システム保守  ベンダ提供のパッチをシステムに適用する。	ベンダ提供のパッチを情報システムに適用する。	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	7	5-4 利用者教育  利用者が発見できるように、 <u>定期的に</u> ・・・	利用者が発見できるように <u>するための定期的な</u> ・・・	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	8	6 . セキュリティの分析	7 . セキュリティ事件・事故への対応	アクティビティ名称変更、 番号変更
情報セキュリティ アドミニストレー タ	8	6-1 事故の検知	7-1 事故の検知	番号変更
情報セキュリティ アドミニストレー タ	8	6-1 事故の検知  システムの整合性チェック	情報システムの整合性チェック	用語の統一
情報セキュリティ アドミニストレー タ	8	6-2 事故の初動処理	7-2 事故の初動処理	番号変更
情報セキュリティ アドミニストレー タ	8	6-3 事故の分析	7-3 事故の分析	番号変更
情報セキュリティ アドミニストレー タ	8	6-4 事故からの復旧	7-4 事故からの復旧	番号変更
情報セキュリティ アドミニストレー タ	8	6-4 事故からの復旧  事故からシステムを復旧する。	事故から <u>情報</u> システムを復旧する。	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	8	6-4 事故からの復旧 システムの再構成を行う。	情報システムの再構成を行う。	用語の統一
情報セキュリティ アドミニストレー タ	8	6-5 再発防止策の実施	7-5 再発防止策の実施	番号変更
情報セキュリティ アドミニストレー タ	8	6-5 再発防止策の実施 必要に応じて、システムの再構築を行う。	必要に応じて、情報システムの再構築を行う。	用語の統一
情報セキュリティ アドミニストレー タ	8	6-6 セキュリティの評価	7-6 セキュリティの評価	番号変更
情報セキュリティ アドミニストレー タ	8	6-6 セキュリティの評価 セキュリティ事故を模擬する侵入、トラフィック 攻撃などの検査などを定期的に行い、・・・	セキュリティ事故を模擬する侵入検査などを定 期的に行い、・・・	用語の統一
情報セキュリティ アドミニストレー タ	8	6-6 セキュリティの評価 システムの脆弱性、	情報システムの脆弱性、	用語の統一
情報セキュリティ アドミニストレー タ	9	7 . セキュリティの見直し	8 . セキュリティ対策の見直し	用語の統一、番号変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	9	7-1 技術情報の収集と評価	8-1 技術情報の収集と評価	番号変更
情報セキュリティ アドミニストレー タ	9	7-2 運用上の問題点整理と分析	8-2 運用上の問題点整理と分析	番号変更
情報セキュリティ アドミニストレー タ	9	7-2 運用上の問題点整理と分析  セキュリティ方針やセキュリティ基準の関係する箇所を洗い出し、	情報セキュリティ基本方針や情報セキュリティ対策基準の関係する箇所を洗い出し、	用語の統一
情報セキュリティ アドミニストレー タ	9	7-3 技術上の問題点整理と分析	8-3 技術上の問題点整理と分析	番号変更
情報セキュリティ アドミニストレー タ	9	7-3 技術上の問題点整理と分析  セキュリティ方針やセキュリティ基準の関係する箇所を洗い出し、	情報セキュリティ基本方針や情報セキュリティ対策基準の関係する箇所を洗い出し、	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	9	7-4 新たなリスクの整理と分析	8-4 新たなリスクの整理と分析	番号変更
情報セキュリティ アドミニストレー タ	9	7-4 新たなリスクの整理と分析  セキュリティ方針やセキュリティ基準の関係する箇所を洗い出し、	情報セキュリティ基本方針や情報セキュリティ対策基準の関係する箇所を洗い出し、	用語の統一
情報セキュリティ アドミニストレー タ	9	7-5 セキュリティポリシーの更新	8-5 情報セキュリティポリシーの更新	番号変更、用語の統一
情報セキュリティ アドミニストレー タ	9	7-5 セキュリティポリシーの更新  情報セキュリティ業務監査に対応し、	情報セキュリティ監査に対応し、	一般的な語句に修正
情報セキュリティ アドミニストレー タ	9	7-5 セキュリティポリシーの更新  改善勧告に基づきセキュリティポリシーの見直しを行う。	改善勧告に基づき情報セキュリティポリシーの見直しを行う。	用語の統一
情報セキュリティ アドミニストレー タ	9	7-5 情報セキュリティポリシーの更新  さらにセキュリティのシステム設計、実装、	さらにセキュリティシステムの機能設計、実装、	用語の統一、および「の」の位置を変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	10	3．スキル基準  スキル基準は、 <u>7</u> 種類の各アクティビティの「タ スク」ごとに、	スキル基準は、 <u>8</u> 種類の各アクティビティの「タ スク」ごとに、	「7」種類から「8」種類へ 修正
情報セキュリティ アドミニストレー タ	11	1．セキュリティ方針の策定	1． <u>情報セキュリティ</u> 基本方針の策定	用語の統一
情報セキュリティ アドミニストレー タ	11	1-1 情報資産の評価  (情報システム、データ、人材、 <u>ドキュメント</u> )	(情報システム、データ、人材、 <u>文書</u> など)	用語の統一
情報セキュリティ アドミニストレー タ	11	1-1 情報資産の評価  整理された情報資産について、機密性、完全性、 可用性の <u>3</u> つの側面から	整理された情報資産について、機密性、完全性、 可用性の <u>三</u> つの側面から	「3つ」から「三つ」へ修正
情報セキュリティ アドミニストレー タ	11	1-1 情報資産の評価  <u>整理</u> および <u>評価</u> された情報資産について、	<u>評価</u> および <u>整理</u> された情報資産について、	前後入れ替え
情報セキュリティ アドミニストレー タ	11	1-2 <u>脅威</u> の認識	1-2 <u>リスク</u> の認識	扱うべき情報は脅威だけで なく脆弱性も必要であり合 わせてリスクと表現する
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  ・調査情報が正確、かつ完全なものであること	・ <u>脅威および脆弱性</u> に関して <u>広く収集した調査情 報</u> が正確、かつ完全なものであること	扱うべき情報は脅威だけで なく脆弱性も必要であるこ とを追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  ・現状の脅威に関する情報が網羅的に収集され ていること	・現状の脅威および脆弱性に関する情報が網羅的 に収集されていること	扱うべき情報は脅威だけで なく脆弱性も必要であるこ とを追加
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  ・情報資産が関係した事件や事故の事例に関す る知識	・ 情報資産が関係した事件・事故の事例に関す る知識	用語の統一
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  一般的なシステムやネットワークにおける技術 と運用に関する知識	一般的な情報システムやネットワークにおける 技術と運用に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  システムおよびネットワークのアーキテクチャ、 ハードウェア、ソフトウェアに関する知識	情報システムおよびネットワークのアーキテク チャ、ハードウェア、ソフトウェアに関する知識	用語の統一
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  ・社会の情報システムに・・・	・社会で発生した情報システムに・・・	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  ・・・情報システムにおける事件および事故に対 し、・・・	情報システムにおける事件・事故に対し、	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	11	1-2 脅威の認識  ・細部に気がつく能力	・広く情報を収集し、その原因など細部まで分 析整理する能力	表現を詳細化
情報セキュリティ アドミニストレー タ	12	1-3 リスクの識別  ・リスクの発生し得る場所および発生時期が整 理されていること	・リスクの発生し得る場所および発生時期(勤務 時間、勤務時間外、平日、休日または定休日など) が整理されていること	発生時期の具体的表現を追 加
情報セキュリティ アドミニストレー タ	12	1-4 対策の整理と調査  ・識別されたリスクに対し、その対策が決定さ れていること	識別されたリスクに対し、最適化(低減)、回避、 移転、保有(許容)のうち、いずれかの対策また はその組み合わせが決定されていること	リスク対策を詳細化
情報セキュリティ アドミニストレー タ	12	1-4 対策の整理と調査  ・リスクへの対策に関する知識	・リスク対策に関する知識	「への」から「に」へ変更
情報セキュリティ アドミニストレー タ	12	1-4 対策の整理と調査  ・システムおよびネットワークのアーキテク チャ、ハードウェア、ソフトウェアに関する知識	・情報システムおよびネットワークのアーキテク チャ、ハードウェア、ソフトウェアに関する知識	用語の統一
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価	1-5 リスクの算定と評価	業務概要をより詳しく反映

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・整理されたリスクに対して、その <u>発生</u> 確率が 明確にされていること	・整理されたリスクに対して、その <u>発現する</u> 確率 が明確にされていること	用語の統一
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・リスクが <u>発生</u> したときの損害額が算定されて いること	・リスクが <u>発現</u> したときの損害額が算定されてい ること	用語の統一
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・各リスクに対しては、リスク <u>発生</u> 時の損害額 と対策コストのバランスが考慮されていること	・各リスクに対しては、リスク <u>発現</u> 時の損害額と 対策コストのバランスが考慮されていること	用語の統一
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・リスク対策が <u>ランク付け</u> されていること	・リスク対策が <u>優先順位付け</u> されていること	「ランク付け」から「優先 順位付け」に修正
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・リスクの <u>発生</u> 確率についての経験的データに 関する知識	・リスクの <u>発現する</u> 確率についての経験的データ に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・ <u>リスクの発生確率について、一般的によく知</u> られている確率・・・	・一般的によく知られている確率・・・	冗長な表現を削除
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・一般的によく知られている確率 <u>または統計</u> に 関する知識	・一般的によく知られている確率 <u>および統計</u> に関 する知識	誤りを修正

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	12	1-5 リスクの評価  ・社会の情報システムにおける事件および事故に 対し、細部にまで気がつく能力	(削除)	記載に関して十分な必要性 が無いと思われるため削除
情報セキュリティ アドミニストレー タ	13	1-6 セキュリティ方針の策定	1-6 <u>情報セキュリティ基本</u> 方針の策定	用語の統一
情報セキュリティ アドミニストレー タ	13	1-6 セキュリティ方針の策定  ・ <u>個々の</u> 技術に依存しない文書となっていること	・ <u>特定の</u> 技術に依存しない文書となっていること	誤りを修正
情報セキュリティ アドミニストレー タ	13	1-6 セキュリティ方針の策定  ・セキュリティ方針の策定方法に関する知識	・ <u>情報セキュリティ基本</u> 方針の策定方法に関する 知識	用語の統一
情報セキュリティ アドミニストレー タ	13	1-6 セキュリティ方針の策定  ・ポリシー作成中でも情報資産の評価から・・・	・ <u>情報セキュリティ</u> ポリシーの作成中でも情報資産 の評価から・・・	用語の統一
情報セキュリティ アドミニストレー タ	14	2 . セキュリティ基準の策定	2 . <u>情報セキュリティ対策</u> 基準の策定	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・基準には、セキュリティ方針の策定で整理され た対策がすべて網羅されていること	・情報セキュリティ対策基準には、情報セキュリ ティ基本方針の策定で整理された対策がすべて 網羅されていること	用語の統一
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・基準は、経営層、情報セキュリティ関係担当役 員、企画関係者に説明され、承認が得られてい ること	・情報セキュリティ対策基準は、経営層、情報セ キュリティ関係担当役員、企画関係者に説明さ れ、承認が得られていること	用語の統一
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・リスク分析で整理した対策に従って、 <u>以下</u> のよ うな基準が作成されていること	・リスク分析で整理した対策に従って、 <u>次</u> のよう な基準が作成されていること	「以下の」から「次の」へ 置き換え
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  (4) 罰則の規程	(4) 罰則の <u>規定</u>	誤りを修正
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・セキュリティ方針に関する知識	・情報セキュリティ基本方針に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・セキュリティ基準の標準に関する知識	・情報セキュリティ対策基準の標準に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・プライバシー保護に関する知識	・プライバシー保護、個人情報保護に関する知識	表現を詳細化

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・セキュリティに関する事件および事故の事例に 関する知識	・セキュリティに関する事件・事故の事例に関す る知識	用語の統一
情報セキュリティ アドミニストレー タ	14	2-1 企業活動一般のセキュリティ規定の作成  ・セキュリティに関係する事件および事故の事例 を継続的に収集する能力	・セキュリティに関係する事件・事故の事例を継 続的に収集する能力	用語の統一
情報セキュリティ アドミニストレー タ	15	2-2 情報システムのセキュリティ規定の作成  ・基準には、セキュリティ方針の策定で整理さ れた対策がすべて網羅されていること	・ <u>情報セキュリティ対策基準</u> には、 <u>情報セキュリ ティ基本方針</u> の策定で整理された対策がすべて 網羅されていること	用語の統一
情報セキュリティ アドミニストレー タ	15	2-2 情報システムのセキュリティ規定の作成  ・基準は、経営層、情報セキュリティ関係担当 役員、企画関係者に説明され、承認が得られて いること	・ <u>情報セキュリティ対策基準</u> は、経営層、情報セ キュリティ関係担当役員、企画関係者に説明さ れ、承認が得られていること	用語の統一
情報セキュリティ アドミニストレー タ	15	2-2 情報システムのセキュリティ規定の作成  ・リスク分析で整理した対策に従って、 <u>以下</u> のよ うな基準が作成されていること	・リスク分析で整理した対策に従って、 <u>次の</u> よう な基準が作成されていること	「以下の」から「次の」へ 置き換え
情報セキュリティ アドミニストレー タ	15	2-2 情報システムのセキュリティ規定の作成  ・セキュリティ方針に関する知識	・ <u>情報セキュリティ基本方針</u> に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	15	2-2 情報システムのセキュリティ規定の作成  ・セキュリティ基準の標準に関する知識	・ <u>情報セキュリティ対策基準</u> の標準に関する知識	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	15	2-2 情報システムのセキュリティ規定の作成  ・セキュリティに関する事件および事故の事例を継続的に収集する能力	・セキュリティに関する事件・事故の事例を継続的に収集する能力	用語の統一
情報セキュリティ アドミニストレー タ	15	2-2 情報システムのセキュリティ規定の作成  ・事件および事故の事例から、対策を分析する能力	・事件・事故の事例から、対策を分析する能力	用語の統一
情報セキュリティ アドミニストレー タ	16	3 . セキュリティシステムの設計	3 . セキュリティシステムの機能設計	用語の統一
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ・セキュリティ基準を実現するために、以下のシステム設計が行われていること	・情報セキュリティ対策基準を実現するために、 <u>認証と権限に関する次の機能設計</u> が行われていること	用語の統一、「 <u>認証と権限に関する</u> 」追加 「以下の」から「次の」へ置き換え
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ( 2 )バイオメトリックスやデジタル署名技術の・・・	( 2 )バイオメトリックスやデジタル署名技術の・・・	誤りを修正
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ・・・利用について判断されていること	・・・必要性について判断されていること	業務概要をより詳しく反映

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  (4)不正利用者に1つ認証が破られても、そのま までは他の部分へアクセスできないように、	(4)不正利用者に1つ認証が破られても、そのま までは他の部分にアクセスできないように、	誤りを修正
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ・デジタル署名技術に関する知識	・ <u>デ</u> ジタル署名技術に関する知識	誤りを修正
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ・ <u>O S</u> に関する知識	・ <u>OS</u> に関する知識	全角から半角へ
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ・セキュリティ基準から認証と権限に関するシス テム要件を導出する能力	・ <u>情報セキュリティ対策</u> 基準から認証と権限に関 するシステム要件を導出する能力	用語を統一
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ・認証、暗号技術、デジタル署名技術などのセ キュリティ技術を・・	・認証、暗号技術、 <u>デ</u> ジタル署名技術などのセ キュリティ技術を・・	誤りを修正
情報セキュリティ アドミニストレー タ	16	3-1 認証と権限のコントロール  ・バイオメトリックス技術、デジタル署名技術 などを組み合わせて	・バイオメトリックス技術、 <u>デ</u> ジタル署名技術 などを組み合わせて	誤りを修正
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  ・セキュリティ基準を実現するために、 <u>以下</u> のシ ステム設計が行われていること	・ <u>情報セキュリティ対策</u> 基準を実現するために、 <u>物理セキュリティに関する次</u> の機能設計が行わ れていること	用語の統一、「物理セキュ リティに関する」追加 「以下の」から「次の」へ 置き換え

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  (1)・・・	(1)重要な情報資産が物理的に隔離されていることが確認されていること (2)重要な情報資産への物理的アクセスについては厳重な認証が要求されていること (3)隔離された領域で行われる作業は監視および記録されていること (4)情報処理装置は、環境上の脅威(火災、水害、ほこりなど)および第三者による不正なアクセスを軽減するような場所に配置されていること (5)装置が使う電源は、電源異常から保護されていること	業務概要をより詳しく反映するため、主要な業務である物理面での管理業務を詳細化した
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  (1)信号漏洩防御に適した物理媒体が選択されていること	(6)ネットワークケーブルにおいては信号漏洩防御に適した物理媒体が選択されていること	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  (2)ネットワーク切断事故に対して被害を最小限に押さえられるような・・・	(7)ネットワークの障害の影響を最小限に押さえられるような・・・	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  ・・・最小限に押さえられるようなネットワークポロジが・・・	・・・最小限に押さえられるようなネットワークポロジが・・・	冗長な表現「、」を削除

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  ・ネットワークポロジが <u>選択</u> されていること	・ネットワークポロジが <u>構成</u> されていること	「選択」から「構成」に変更
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  (3) 物理的な隔離が確認されていること	(削除)	物理的な隔離の内容を詳細化したためこの文は不要となった
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  (4) 物理装置の配置、人的アクセスおよび使用環境の安全装置が決定されていること	(8) 物理装置の配置、人的アクセスおよび使用環境の安全装置が決定されていること	番号の変更
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール	(9) (委託業者を含め) 全職員に対して、 <u>第三者と見分けをつけるために身分証明書を配布し、着用を義務づけていること</u> (10) 印刷装置(プリンタ、ファクシミリ、複写装置)は、 <u>第三者がアクセスしづらく、職員からよく見える場所に配置されていること</u>	物理面の管理として新規追加された
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  ・ <u>通信ケーブル</u> からの盗聴に関する知識	・ <u>ネットワークケーブル</u> からの盗聴および電磁波漏洩に関する知識	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール	・ネットワーク経路制御に関する知識	物理面の管理として新規追加された
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  ・ネットワークのハードウェア、ソフトウェアに関する知識 ・セキュリティ製品に関する・・・	・ネットワークのハードウェア、ソフトウェアに関する知識 ・災害に関する知識 ・電源に関する知識 ・身分証明書に関する知識 ・セキュリティ製品に関する・・・	達成指標の追加に対応して新規追加
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  ・セキュリティ製品に関する知識	・セキュリティ製品に関する次の知識 ・ <u>物理的認証装置（バイオメトリックス、ICカード、ハードウェアトークン）</u> ・ <u>物理的アクセス制限装置</u> ・ <u>物理的監視装置</u> ・ <u>電源保護装置（多重供給、無停電電源、バックアップ電源）</u> ・ <u>警報装置</u> ・ <u>災害対策装置（防火扉、消火装置、排煙装置など）</u>	達成指標の追加に対応して新規追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール	<ul style="list-style-type: none"> <li>・ <u>オフィスのセキュリティに関する次の知識</u></li> <li>・ <u>レイアウト上の配慮</u></li> <li>・ <u>入退室の管理と記録</u></li> <li>・ <u>来訪者の管理</u></li> <li>・ <u>クリアデスク</u></li> </ul>	達成指標の追加に対応して 新規追加
情報セキュリティ アドミニストレー タ	17	3-2 物理セキュリティのコントロール  ・セキュリティ基準から物理装置のセキュリティ に関するシステム要件を導出する能力	・ <u>情報セキュリティ対策基準</u> から物理装置のセキ ュリティに関するシステム要件を導出する能力	用語の統一
情報セキュリティ アドミニストレー タ	18	3-3 論理セキュリティのコントロール  ・セキュリティ基準を実現するために、以下のシ ステム設計が行われていること	・ <u>情報セキュリティ対策基準</u> を実現するために、 <u>論理セキュリティに関する次の機能設計</u> が行わ れていること	用語の統一、「論理セキ ュリティに関する」追加 「以下の」から「次の」へ 置き換え
情報セキュリティ アドミニストレー タ	18	3-3 論理セキュリティのコントロール  ・フィルタリングの原理に関する知識 ・TCP/IPに関する基本的な知識 ・ルーティングに関する知識	<ul style="list-style-type: none"> <li>・フィルタリングの原理に関する知識</li> <li>・<u>TCP/IPに関する基本的な知識</u></li> <li>・ルーティングに関する知識</li> </ul>	全角から半角へ
情報セキュリティ アドミニストレー タ	18	3-3 論理セキュリティのコントロール  ・セキュリティ基準から論理セキュリティに関す るシステム要件を導出する能力	・ <u>情報セキュリティ対策基準</u> から論理セキ ュリティに関するシステム要件を導出する能力	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	18	3-3 論理セキュリティのコントロール  ・セキュリティ技術をシステム設計に適用する能力	・セキュリティ技術を機能設計に適用する能力	用語の統一
情報セキュリティ アドミニストレー タ	18	3-4 ネットワーク基盤上データの信頼性確保  ・セキュリティ基準を実現するために、以下のシステム設計が行われていること	・情報セキュリティ対策基準を実現するために、ネットワーク基盤上のデータ信頼性確保に関する次の機能設計が行われていること	用語の統一、「ネットワーク基盤上のデータ信頼性確保に関する」追加 「以下の」から「次の」へ置き換え
情報セキュリティ アドミニストレー タ	18	3-4 ネットワーク基盤上データの信頼性確保  (2) ネットワークサービスに関して、サポートするサービスやプロトコルが選択され、・・・	(2) ネットワークサービスに関して、提供されるサービスやプロトコルが選択され、・・・	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	18	3-4 ネットワーク基盤上データの信頼性確保  ・ネットワークアーキテクチャに関する知識	ネットワークアーキテクチャに関する知識	誤りを修正
情報セキュリティ アドミニストレー タ	18	3-4 ネットワーク基盤上データの信頼性確保  ・TCPプロトコルに関する知識	・TCP/IPプロトコルに関する知識	再送制御はTCPではあるが、TCPの理解にはTCP/IP自体の理解が必要である
情報セキュリティ アドミニストレー タ	18	3-4 ネットワーク基盤上データの信頼性確保  ・セキュリティ基準からデータ整合性に関するシステム要件を導出する能力	・情報セキュリティ対策基準からデータ整合性に関するシステム要件を導出する能力	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	18	3-4 ネットワーク基盤上データの信頼性確保  ・セキュリティ技術をシステム設計に適用する能力	・セキュリティ技術を機能設計に適用する能力	用語の統一
情報セキュリティ アドミニストレー タ	18	3-4 ネットワーク基盤上データの信頼性確保  ・CERT/CCやIPAおよびベンダが提供するネットワークサービスの・・・	・JPCERT/CC、IPAおよびベンダが提供するネットワークサービスの・・・	用語の統一
情報セキュリティ アドミニストレー タ	18	3-5 データの機密保持	3-5 データのセキュリティ	用語の統一
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持  ・セキュリティ基準を実現するために、以下のシステム設計が行われていること	・情報セキュリティ対策基準を実現するために、データのセキュリティに関する次の機能設計が行われていること	用語の統一、「データのセキュリティに関する」追加 「以下の」から「次の」へ置き換え
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持  (1) リスク分析により、不正利用されたとき最もリスクが大きいデータが暗号化されるように設計されていること	(1) リスク分析により、不正利用されたときリスクが大きいデータが暗号化されるように設計されていること	一種類のデータだけを暗号化するわけではないため「最も」を削除

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持	<p>(4)リスク分析により、改ざんされたときにリスクが大きいデータに電子署名が付与されるように設計されていること</p> <p>(5)リスク分析により、利用できなくなった時にリスクが大きいデータがバックアップされるように設計されていること</p>	新規追加
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持	<ul style="list-style-type: none"> <li>・電子署名に関する知識</li> <li>・バックアップ/リストア方法に関する知識</li> </ul>	新規追加
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持  ・セキュリティ基準からデータ機密保持に関するシステム要件を導出する能力	・情報セキュリティ対策基準からデータ機密保持に関するシステム要件を導出する能力	用語の統一
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持  ・セキュリティ技術をシステム設計に適用する能力	・セキュリティ技術を機能設計に適用する能力	用語の統一
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持  ・暗号化の <u>必要な</u> データを決定する能力	・暗号化を行う <u>必要のある</u> データを識別する能力	わかりやすい表現に修正

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持	・電子署名を付与する必要があるデータを識別する能力	新規追加
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持 ・暗号鍵の管理体制を作る能力	・暗号鍵の管理体制を構築する能力	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	19	3-5 データの機密保持	・電子証明書の管理体制を構築する能力 ・バックアップの必要なデータを識別する能力 ・バックアップ媒体の管理体制を構築する能力	新規追加
情報セキュリティ アドミニストレー タ	20	3-6 セキュリティ運用手続きの作成 ・セキュリティ基準を実現するために、利用者からの意見を聞き、以下の事項に示す・・・	・情報セキュリティ対策基準を実現するために、利用者からの意見を参考とした上で、次の事項に示す・・・	用語の統一、わかりやすい表現に修正 「以下の」から「次の」へ置き換え
情報セキュリティ アドミニストレー タ	20	3-6 セキュリティ運用手続きの作成 (6)個人情報が含まれる監査データに対するプライバシー保護への準備	(6)個人情報が含まれる監査データに対する個人情報保護への準備	正確な表現に修正

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	20	3-6 セキュリティ運用手続きの作成  ・記憶媒体に関する知識	・記録媒体に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	20	3-6 セキュリティ運用手続きの作成  ・プライバシー保護に関する知識	・プライバシー保護、個人情報保護に関する知識	追加
情報セキュリティ アドミニストレー タ	20	3-6 セキュリティ運用手続きの作成  ・セキュリティ基準からバックアップに関するシ ステム要件を導出する能力	・情報セキュリティ対策基準からバックアップに 関するシステム要件を導出する能力	用語の統一
情報セキュリティ アドミニストレー タ	20	3-6 セキュリティ運用手続きの作成  ・セキュリティ事件または事故を検出するた めのデータ範囲を決定する能力	・セキュリティ事件・事故を検出するためのデー タ範囲を決定する能力	用語の統一
情報セキュリティ アドミニストレー タ	20	3-6 セキュリティ運用手続きの作成  ・セキュリティ基準から、セキュリティを実際 に運用する場面で用いる手続きを作成する能力	・情報セキュリティ対策基準から、セキュリティ を実際に運用する場面で用いる手続きを作成す る能力	用語の統一
情報セキュリティ アドミニストレー タ	20	3-7 利用者への啓発および教育訓練計画  ・セキュリティ基準を実現するために、 <u>以下</u> の事 項が実施されていること	・情報セキュリティ対策基準を実現するために、 <u>次の</u> 事項が実施されていること	用語の統一 「以下の」から「次の」へ 置き換え

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	20	3-7 利用者への啓発および教育訓練計画  ・ <u>セキュリティ一般</u> の新しい分野に関する知識	・ <u>セキュリティ全般</u> の新しい分野に関する知識	誤りを修正
情報セキュリティ アドミニストレー タ	21	4-1 セキュリティ製品の選定および導入  ・必要機能の動作が確認されていること	・必要 <u>な</u> 機能の動作が確認されていること	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	21	4-1 セキュリティ製品の選定および導入  ・ <u>国際標準の準拠性の必要性が確認されていること</u>	・製品を選択する上で、 <u>国際標準に準拠している必要性の有無を判断していること</u>	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	21	4-1 セキュリティ製品の選定および導入  ・ <u>ISO15408</u> に関する知識	・ <u>ISO/IEC 15408 (JIS X 5070)</u> に関する知識	正確な表現に修正
情報セキュリティ アドミニストレー タ	21	4-2 セキュリティシステムの開発	(移動)	5-1 に移動
情報セキュリティ アドミニストレー タ	21	4- <u>3</u> セキュリティ実装の確認	4- <u>2</u> セキュリティ実装の確認	番号変更
情報セキュリティ アドミニストレー タ	21	4-3 セキュリティ実装の確認  ・実際に攻撃を行う <u>侵入検査</u> が行われていること	・実際に攻撃を行う <u>セキュリティ侵犯テスト</u> が行われていること	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	21	4-3 セキュリティ実装の確認  ・ <u>侵入検査の内容は、セキュリティに関する最新情報が反映されていること</u>	・ <u>セキュリティ侵犯テストの内容は、セキュリティに関する最新情報が反映されていること</u>	用語の統一
情報セキュリティ アドミニストレー タ	21	4-3 セキュリティ実装の確認  ・ <u>セキュリティ機能の検証またはセキュリティホールのチェックを行うツールに関する知識</u>	・ <u>セキュリティ機能の検証または脆弱性の存在チェックを行うツールに関する知識</u>	用語の統一
情報セキュリティ アドミニストレー タ	22		5 . セキュリティシステムの開発管理	4-2 の 5-1 への移動に伴い 新設
情報セキュリティ アドミニストレー タ	22	4-2 セキュリティシステムの開発	5-1 セキュリティシステムの開発管理	「管理」を追加、4-2 から 移動
情報セキュリティ アドミニストレー タ	22	4-2 セキュリティシステムの開発  ・ <u>該当するセキュリティ製品がないかどうか十分調査されていること</u>	(削除)	削除
情報セキュリティ アドミニストレー タ	22	4-2 セキュリティシステムの開発	・ <u>開発プロジェクトが適切に管理されていること</u>	新規追加
情報セキュリティ アドミニストレー タ	22	4-2 セキュリティシステムの開発  ・ <u>必要機能の動作が確認されていること</u>	・ <u>必要な機能の動作が確認されていること</u>	わかりやすい表現に修正

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	22	4-2 セキュリティシステムの開発	・ <u>工程管理に関する知識</u>	新規追加
情報セキュリティ アドミニストレー タ	22	4-2 セキュリティシステムの開発  ・開発されたシステムがセキュリティ機能要件を 満たしているかをチェックする能力	・開発された <u>情報</u> システムがセキュリティ機能要 件を満たしているかをチェックする能力	用語の統一
情報セキュリティ アドミニストレー タ	22	4-2 セキュリティシステムの開発  ・コンピュータおよびネットワークシステムの <u>O</u> <u>S</u> レベルの処理を理解する能力	コンピュータおよびネットワークシステムの <u>OS</u> レベルの処理を理解する能力	全角から半角へ
情報セキュリティ アドミニストレー タ	23	5 . セキュリティシステムの運用管理	<u>6</u> . セキュリティシステムの運用管理	番号変更
情報セキュリティ アドミニストレー タ	23	<u>5</u> -1 セキュリティ運用手続きの実施	<u>6</u> -1 セキュリティ運用手続きの実施	番号変更
情報セキュリティ アドミニストレー タ	23	5-1 セキュリティ運用手続きの実施  ・セキュリティポリシー(セキュリティ方針とセ キュリティ基準)に従って運用が実施され、機 能が果たされていること	・ <u>情報</u> セキュリティポリシー( <u>情報</u> セキュリティ基 本方針と <u>情報</u> セキュリティ対策基準)に従って運 用が実施され、機能が果たされていること	用語の統一
情報セキュリティ アドミニストレー タ	23	5-1 セキュリティ運用手続きの実施  ・手続きの実施過程で起きた問題は、記録され ていること	・手続きの実施過程で起きた問題が、記録されて いること	誤りを修正

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	23	5-1 セキュリティ運用手続きの実施  ・セキュリティポリシーを遵守するセキュリティ 運用手続きに関する知識	・情報セキュリティポリシーを遵守するセキュリ ティ運用手続きに関する知識	用語の統一
情報セキュリティ アドミニストレー タ	23	5-1 セキュリティ運用手続きの実施  ・運用手続きの裏技を発見し、裏技を阻止する 能力	・運用手続きの抜け道を発見し、その悪用を阻止 する能力	口語調な表現を修正
情報セキュリティ アドミニストレー タ	23	5-2 システム動作の監視と記録	6-2 システム動作の監視と記録	番号変更
情報セキュリティ アドミニストレー タ	23	5-2 システム動作の監視と記録  ・セキュリティシステム設計で決定したトラフィ ックが監視され、記録されていること	・セキュリティシステム機能設計で決定したトラ フィックが監視され、記録されていること	用語の統一
情報セキュリティ アドミニストレー タ	23	5-2 システム動作の監視と記録  ・些細な記録から重大な攻撃の事実を <u>発見した り、予兆したりする能力</u>	・些細な記録から重大な攻撃の事実 <u>または攻撃の 予兆を発見する能力</u>	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	23	5-2 システム動作の監視と記録  ・セキュリティ違反を速やかに対処する能力	・セキュリティ違反に <u>速やかに対処する能力</u>	誤りを修正

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	23	5-3 システム保守	6-3 システム保守	番号変更
情報セキュリティ アドミニストレー タ	23	5-3 システム保守  ・ <u>メーカー</u> から提供される最新パッチが評価さ れ、・・・	・ <u>ベンダ</u> から提供される最新パッチが評価され、	用語の統一
情報セキュリティ アドミニストレー タ	23	5-4 利用者教育	6-4 利用者教育	番号変更
情報セキュリティ アドミニストレー タ	23	5-4 利用者教育  ・教育計画に盛り込んだ機能が果たされているこ と	・教育 <u>訓練</u> 計画に盛り込んだ機能が果たされてい ること	「訓練」追加
情報セキュリティ アドミニストレー タ	23	5-4 利用者教育  ・ <u>セキュリティ事件および事故</u> に関する知識	・セキュリティ事件・ <u>事故</u> に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	23	5-4 利用者教育  ・ <u>セキュリティ事件および事故</u> をわかりやすく 説明する能力	・セキュリティ事件・ <u>事故</u> をわかりやすく説明す る能力	用語の統一
情報セキュリティ アドミニストレー タ		5-5 <u>セキュリティ技術者教育</u>	(削除)	削除

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	24	<u>6</u> . セキュリティ事件・事故への対応	<u>7</u> . セキュリティ事件・事故への対応	番号変更
情報セキュリティ アドミニストレー タ	24	<u>6</u> -1 事故の検知	<u>7</u> -1 事故の検知	番号変更
情報セキュリティ アドミニストレー タ	24	6-1 事故の検知  ・システムの整合性が定期的にチェックされて いること	・ <u>情報</u> システムの整合性が定期的にチェックされ ていること	用語の統一
情報セキュリティ アドミニストレー タ	24	6-1 事故の検知  ・システムのアクセスログに関する知識	・ <u>情報</u> システムのアクセスログに関する知識	用語の統一
情報セキュリティ アドミニストレー タ	24	6-1 事故の検知  ・些細な記録から重大な攻撃の事実を <u>発見した り、予兆したりする能力</u>	・些細な記録から重大な攻撃の事実または攻撃の <u>予兆を発見する能力</u>	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	24	<u>6</u> -2 事故の初動処理	<u>7</u> -2 事故の初動処理	番号変更
情報セキュリティ アドミニストレー タ	24	6-2 事故の初動処理  ・セキュリティポリシーに関する知識	・ <u>情報</u> セキュリティポリシーに関する知識	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	24	6-2 事故の初動処理  ・CERT/IPAなどと連絡をとって適切な処理が行 えるように行動する能力	・JPCERT/CC、IPAなどと連絡をとって適切な処理 が行えるように行動する能力	用語の統一
情報セキュリティ アドミニストレー タ	24	6-3 事故の分析	7-3 事故の分析	番号変更
情報セキュリティ アドミニストレー タ	24	6-3 事故の分析  ・セキュリティ事件および事故に関する知識	・セキュリティ事件・事故に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	24	6-3 事故の分析  ・CERT/IPAなどと連絡をとって事故原 因を報告するとともに事故を客観的に分析す る能力	・事故を客観的に分析する能力	事件・事故に関する連絡、 事故の初動処理で行うこと になっている
情報セキュリティ アドミニストレー タ	25	6-4 事故からの復旧	7-4 事故からの復旧	番号変更
情報セキュリティ アドミニストレー タ	25	6-4 事故からの復旧  ・事故からの復旧が迅速に行われ、必要に応じ て、システムの再構成が行われていること	・事故からの復旧が迅速に行われ、必要に応じて、 情報システムの再構成が行われていること	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	25	6-4 事故からの復旧  ・復旧後、セキュリティの見直しが行われていること	・復旧後、セキュリティ <u>対策</u> の見直しが行われていること	「対策」追加
情報セキュリティ アドミニストレー タ	25	6-5 再発防止策の実施	7-5 再発防止策の実施	番号変更
情報セキュリティ アドミニストレー タ	25	6-5 再発防止策の実施  ・必要に応じて、システムの再構築が行われていること	・必要に応じて、 <u>情報</u> システムの再構築が行われていること	用語の統一
情報セキュリティ アドミニストレー タ	25	6-5 再発防止策の実施  ・再発防止策の決定後、セキュリティの見直しが行われていること	・再発防止策の決定後、セキュリティ <u>対策</u> の見直しが行われていること	「対策」追加
情報セキュリティ アドミニストレー タ	25	6-5 再発防止策の実施  ・企業のシステム構築に関する知識	・企業の <u>情報</u> システム構築に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価	7-6 セキュリティの評価	番号変更
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・ <u>侵入</u> 検査を行い、	・ <u>セキュリティ</u> 侵入テストを行い、	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・セキュリティポリシーの遵守状況が評価されて いること	・ <u>情報セキュリティ</u> ポリシーの遵守状況が評価され ていること	用語の統一
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・ <u>侵入検査</u> は継続的に実施されていること	・ <u>セキュリティ侵害テスト</u> は継続的に実施されて いること	用語の統一
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・ <u>侵入検査</u> で不備がある場合は、	・ <u>セキュリティ侵害テスト</u> で不備が発見された場 合に、	用語の統一
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・侵入検査で不備がある場合は、	・セキュリティ侵害テストで不備が発見された場 合に、	口語調な表現を修正
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・セキュリティの評価情報が、セキュリティの見 直しで利用されていること	・セキュリティの評価情報が、セキュリティ <u>対策</u> の見直しで利用されていること	「対策」追加
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・セキュリティ <u>検査項目</u> に関する知識	・セキュリティ <u>テスト項目</u> に関する知識	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	25	6-6 セキュリティの評価  ・外部の <u>検査サービス</u> に関する知識	・外部の <u>セキュリティ診断サービス</u> に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	26	<u>7</u> ．セキュリティ対策の見直し	<u>8</u> ．セキュリティ対策の見直し	番号変更
情報セキュリティ アドミニストレー タ	26	<u>7</u> -1 技術情報の収集と評価	<u>8</u> -1 技術情報の収集と評価	番号変更
情報セキュリティ アドミニストレー タ	26	7-1 技術情報の収集と評価  ・・社内システムに適用できるかどうか評価 されていること	・・社内 <u>情報</u> システムに適用できるかどうか評 価されていること	用語の統一
情報セキュリティ アドミニストレー タ	26	7-1 技術情報の収集と評価  ・セキュリティ事件および事故に関する知識	・セキュリティ事件・事故に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	26	7-1 技術情報の収集と評価  ・企業のシステムおよびネットワークに関係す るセキュリティホール情報、・・	・企業の <u>情報</u> システムおよびネットワークに関係 するセキュリティホール情報、・・	用語の統一
情報セキュリティ アドミニストレー タ	26	<u>7</u> -2 運用上の問題点整理と分析	<u>8</u> -2 運用上の問題点整理と分析	番号変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・ ・ ポリシ実施上の問題点が ・ ・	・ ・ <u>情報セキュリティ</u> ポリシを遵守する上での問題点が ・ ・	用語の統一
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・ ・ <u>ポリシ実施上</u> の問題点が ・ ・	・ ・ <u>情報セキュリティ</u> ポリシを遵守する上での問題点が ・ ・	正確な表現に修正
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・ 整理された問題点について、情報セキュリティ ポリシ変更に対する分析が行われ、	・ 整理された問題点を元に、情報セキュリティ ポリシ変更の必要性に関する分析が行われ、	「について」から「を元に」 変更
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・ ・ セキュリティポリシ変更に対する分析が行 われ、	・ ・ <u>情報セキュリティ</u> ポリシ変更の必要性に対す る分析が行われ、 ・ ・	用語の統一、「の必要性」追 加
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・ ・ ポリシの見直しが行われていること	・ ・ <u>必要に応じて</u> ポリシの見直しが行われている こと	「必要に応じて」追加
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・ 事故の再発防止策の実施によってセキュリテ ィポリシの受ける影響が分析され、ポリシの見 直しが行われていること	・ 事故の再発防止策の実施によって <u>情報セキュリ</u> <u>ティ</u> ポリシに与える影響が分析され、 <u>必要に</u> <u>応じ</u> <u>て</u> ポリシの見直しが行われていること	用語の統一、「の受ける」か ら「に与える」に変更、「必 要に応じて」追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・ <u>企業のシステムおよびネットワーク構成に関 する知識</u>	(削除)	削除
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・企業のシステムおよびネットワークにおける 運用に関する知識	・企業の <u>情報</u> システムおよびネットワークにおけ る運用に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	26	7-2 運用上の問題点整理と分析  ・分析された問題点に対し、セキュリティポリ シを見直す能力	・分析された問題点に対し、 <u>情報</u> セキュリティポリ シを見直す能力	用語の統一
情報セキュリティ アドミニストレー タ	26	7-3 技術上の問題点整理と分析	8-3 技術上の問題点整理と分析	番号変更
情報セキュリティ アドミニストレー タ	26	7-3 技術上の問題点整理と分析  ・新技術の開発により、影響を受けるセキュリ ティポリシーの箇所が識別され・・・	・新技術の開発により、影響を受ける <u>情報</u> セキュ リティポリシーの箇所が識別され・・・	用語の統一
情報セキュリティ アドミニストレー タ	26	7-3 技術上の問題点整理と分析  ・セキュリティ分析の評価結果から、影響を受 けるセキュリティポリシーの箇所が識別され・・・	・セキュリティ分析の評価結果から、影響を受け る <u>情報</u> セキュリティポリシーの箇所が識別され・・・	用語の統一
情報セキュリティ アドミニストレー タ	26	7-3 技術上の問題点整理と分析  ・整理された問題点について、セキュリティポリ シ変更に対する分析が行われ、	・整理された問題点について、 <u>情報</u> セキュリティ ポリシー変更に対する分析が行われ、	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	26	7-3 技術上の問題点整理と分析  ・整理された技術情報から、セキュリティポリ シ（方針、基準）の問題点を分析する能力	・整理された技術情報から、 <u>情報</u> セキュリティポリ シ（方針、基準）の問題点を分析する能力	用語の統一
情報セキュリティ アドミニストレー タ	26	7-3 技術上の問題点整理と分析  ・分析された問題点に対し、セキュリティポリ シを見直す能力	・分析された問題点に対し、 <u>情報</u> セキュリティポリ シを見直す能力	用語の統一
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析	8-4 新たなリスクの整理と分析	番号変更
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析  ・新たなリスクにより、影響を受けるセキュリ ティポリシーの箇所が識別され、整理されている こと	・新たなリスクにより、影響を受ける <u>情報</u> セキュ リティポリシーの箇所が識別され、整理されている こと	用語の統一
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析  ・整理された問題点について、セキュリティポリ シ変更に対する分析が行われ、・・・	・整理された問題点について、 <u>情報</u> セキュリティ ポリシー変更に対する分析が行われ、・・・	用語の統一
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析  ・セキュリティ事件 <u>および</u> 事故に関する知識	・セキュリティ事件 <u>・</u> 事故に関する知識	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析  ・セキュリティ事件および事故の事例情報を収集し、整理する能力	・セキュリティ事件・事故の事例情報を収集し、整理する能力	用語の統一
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析  ・事例からセキュリティ事件および事故の原因を特定し、対応策を分析する能力	・事例からセキュリティ事件・事故の原因を特定し、対応策を分析する能力	用語の統一
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析  ・整理された技術情報から、セキュリティポリシ（方針、基準）の問題点を分析する能力	・整理された技術情報から、 <u>情報</u> セキュリティポリシ（方針、基準）の問題点を分析する能力	用語の統一
情報セキュリティ アドミニストレー タ	27	7-4 新たなリスクの整理と分析  ・分析された問題点に対し、セキュリティポリシを見直す能力	分析された問題点に対し、 <u>情報</u> セキュリティポリシを見直す能力	用語の統一
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシの更新	8-5 <u>情報</u> セキュリティポリシの更新	番号変更、用語の統一
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシの更新  ・セキュリティポリシ更新の体制・・	・ <u>情報</u> セキュリティポリシ更新の体制・・	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・セキュリティポリシー更新の体制を整備されていること	・情報セキュリティポリシー更新の体制が整備されていること	誤りを修正
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・分析結果からポリシーの変更部分について、再度リスク分析が行われ、ポリシーが更新されていること	・分析結果から、 <u>情報セキュリティポリシーの変更に伴う影響について、適切なリスク分析が行われ、変更の妥当性を検証していること</u>	情報セキュリティアドミニストレータの業務としては、変更の妥当性を検証することになる
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・セキュリティポリシーの更新について、経営層、・・・	・ <u>情報</u> セキュリティポリシーの更新について、経営層、・・・	用語の統一
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・継続的にセキュリティポリシーが見直されていること	・継続的に <u>情報</u> セキュリティポリシーが見直されていること	用語の統一
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・セキュリティポリシー変更手続きに関する知識	・ <u>情報</u> セキュリティポリシー変更手続きに関する知識	用語の統一
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・セキュリティポリシーに関する知識	・ <u>情報</u> セキュリティポリシーに関する知識	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・セキュリティポリシー（方針、基準）作成方法に関する知識	・ <u>情報</u> セキュリティポリシー（方針、基準）作成方法に関する知識	用語の統一
情報セキュリティ アドミニストレー タ	27	7-5 セキュリティポリシーの更新  ・継続的にセキュリティポリシーを精査する能力	・継続的に <u>情報</u> セキュリティポリシーを精査する能力	用語の統一
情報セキュリティ アドミニストレー タ	28	4．知識体系  情報セキュリティアドミニストレータにとって必要な知識体系は、 <u>以下の</u> 2種類からなる。	情報セキュリティアドミニストレータにとって必要な知識体系は、 <u>次の</u> 2種類からなる。	「以下の」から「次の」へ置き換え
情報セキュリティ アドミニストレー タ	28	4．知識体系  I T 共通知識体系の7種類の分野につき、 <u>以下の</u> 技術レベルで知識が問われることになる。	I T 共通知識体系の7種類の分野につき、 <u>次の</u> 技術レベルで知識が問われることになる。	「以下の」から「次の」へ置き換え
情報セキュリティ アドミニストレー タ	28	4．知識体系  「B．セキュリティポリシーの策定」	「B． <u>情報</u> セキュリティポリシーの策定」	用語の統一
情報セキュリティ アドミニストレー タ	28	4．知識体系  「C．セキュリティシステムの設計と実装」	「C．セキュリティシステムの <u>機能</u> 設計と実装」	「機能」追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	29	【情報セキュリティアドミニストレータ実務知 識体系・コア知識体系】 1.2 攻撃の動機  1.2.1 無知、 <u>不用意</u>	1.2.1 無知	無知と不用意は意味合いが異なるので、別々の項番号に変更
情報セキュリティ アドミニストレー タ	29		1.2.2 <u>不用意</u>	番号の変更
情報セキュリティ アドミニストレー タ	29	1.2 攻撃の動機	1.2.3 <u>いたずら</u>	番号の変更
情報セキュリティ アドミニストレー タ	29	1.2 攻撃の動機  1.2.3 自己顕示	1.2.4 <u>自己顕示欲</u>	番号の変更 「欲」を追加
情報セキュリティ アドミニストレー タ	29	1.2 攻撃の動機	1.2.5 <u>金銭</u>	番号の変更
情報セキュリティ アドミニストレー タ	29	1.2 攻撃の動機	1.2.6 <u>テロ</u>	番号の変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	29	1.2 攻撃の動機	1.2.7 戦争	番号の変更
情報セキュリティ アドミニストレー タ	29	1.2 攻撃の動機  1.2.6 復讐	1.2.8 怨恨	より妥当な言葉に変更
情報セキュリティ アドミニストレー タ	29	2.1 システムの脆弱性	2.1 情報システムの脆弱性	用語の統一
情報セキュリティ アドミニストレー タ	29	2.1.1 プロトコルの脆弱性 (TCP、ICMP、 UDP、RIP、NNTP、HTTP、SMTP、 FTP、NFS/NIS、SNMP、DNS、 TFTP、whois、finger)	2.1.1 プロトコルの脆弱性 (TCP、ICMP、UDP、 RIP、HTTP、SMTP、FTP、NFS/NIS、SNMP、DNS、TFTP など)	全角から半角に変更 whois、finger 削除 「など」追加
情報セキュリティ アドミニストレー タ	29	2.1.2 製品システムの脆弱性  WWWブラウザ、	Webブラウザ、	用語の統一
情報セキュリティ アドミニストレー タ	29	2.1.2 製品システムの脆弱性  バッファオーバーフロー、 スクリプトによる自動実行)	バッファオーバーフロー、メモリーク、 スクリプトによる自動実行、SQLインジェクショ ン、クロスサイトスクリプティングなど)	脆弱性三点、「など」を追加
情報セキュリティ アドミニストレー タ	29	2.1.3 開発システムの脆弱性 (開発システム、 ツールの脆弱性)	2.1.3 開発されたシステムの脆弱性 (同上)	システムの脆弱性は同一と 考えられるため統一した

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	29	2.1.4 システム設定の脆弱性（サーバ、ルータ およびファイアウォールの設定）	2.1.4 システム設定の脆弱性（サーバ、ルータ およびファイアウォールの設定 <u>など</u> ）	「など」追加
情報セキュリティ アドミニストレー タ	29	2.1.5 システム運用の脆弱性  （ <u>ユーザID</u> 、パスワードの管理）	（ <u>利用者ID</u> 、パスワードの管理など）	用語の統一、「など」追加
情報セキュリティ アドミニストレー タ	29	2.1.6 <u>ソーシャルエンジニアリングによる脆 弱性（電話対応、紙ゴミからの情報漏洩）</u>	（削除）	システムの脆弱性ではない ため削除
情報セキュリティ アドミニストレー タ	29	2.1.7 物理的アクセスの脆弱性（警備不備によ る不正侵入）	2.1.6 物理的アクセスの脆弱性（警備不備によ る不正侵入 <u>など</u> ）	番号変更、「など」追加
情報セキュリティ アドミニストレー タ	29	2.1.8 開発手法による脆弱性（デバッグ時のバ ックドアの除去し忘れ）	2.1.7 開発手法および <u>ツール</u> による脆弱性（デ バッグ時のバックドアの除去し忘れ、 <u>ツールに内 在する脆弱性</u> など）	番号変更、ツールに関する 記述追加
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類  2.2.3 なりすまし	2.2.3 なりすまし（ <u>スプーフィング</u> ）	スプーフィングも一般的に 使われている用語であるた め追加
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類  2.2.4 サービス妨害攻撃（Denial of Service）	2.2.4 サービス妨害攻撃（Denial of Service （ <u>DoS</u> ）攻撃）	DoS攻撃も一般的に使われ ている名称のため追加
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類	2.2.6 <u>コンピュータワーム</u>	追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類	2.2.7 <u>スパイウェア</u>	追加
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類	2.2.8 <u>アドウェア</u>	追加
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類	2.2.9 <u>ボット、ボットネット</u>	追加
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類  2.2.6 <u>ソーシャルエンジニアリングを利用し た攻撃</u>	2.2.10 <u>ソーシャルエンジニアリングを利用した 攻撃（電話対応、紙ゴミからの情報漏洩など）</u>	番号の変更、2.1.6の記載事 項を移動
情報セキュリティ アドミニストレー タ	30	2.2 攻撃の種類  2.2.7 <u>セキュリティ管理ツール（自動的にセキ ュリティホールや脆弱性の情報を収集）</u>	2.2.11 <u>セキュリティ管理ツール（自動的にセキ ュリティホールや脆弱性の情報を収集）</u>	番号の変更
情報セキュリティ アドミニストレー タ	30	3.1 関連法令  <u>3.1.1 著作権法</u>	<u>3.1.1 不正競争防止法</u>	番号の変更（著作権法は 3.1.6へ移動）
情報セキュリティ アドミニストレー タ	30	3.1 関連法令  <u>3.1.3 個人情報保護法</u>	<u>3.1.3 個人情報保護関連法</u>	正確な表現に修正
情報セキュリティ アドミニストレー タ	30	3.1 関連法令  <u>3.1.4 不正競争防止法</u>	<u>3.1.4 電子署名法</u>	追加

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	30	3.1 関連法令	3.1.5 e-文書法	新規追加
情報セキュリティ アドミニストレー タ	30	3.1 関連法令	3.1.6 著作権法	番号の変更
情報セキュリティ アドミニストレー タ	30	3.2 国際標準と国内基準 3.2.1 <u>ISO15408</u>	3.2.1 <u>ISO/IEC 15408 (JIS X 5070)</u>	正確な表現に修正
情報セキュリティ アドミニストレー タ	30	3.2.2 <u>ISO17799 ( B S 7799 )</u>	3.2.2 <u>ISO/IEC 17799 (JIS X 5080)</u>	正確な表現に修正
情報セキュリティ アドミニストレー タ	30	3.2 国際標準と国内基準 3.2.3 <u>情報セキュリティポリシーに関するガ イドライン (2000年7月18日)</u>	3.2.3 <u>ISO/IEC 27001</u>	「、、、ガイドライン」を 「ISO/IEC 27001」で置き換 え
情報セキュリティ アドミニストレー タ	30	3.2 国際標準と国内基準 3.2.4 <u>ISO13335</u>	3.2.4 <u>ISO/IEC 13335</u>	正確な表現に修正

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	30	3.2 国際標準と国内基準	<u>3.2.5 JIS Q 15001</u> <u>3.2.6 OECD プライバシ原則</u> <u>3.2.7 OECD セキュリティ原則</u> <u>3.2.8 コンピュータウイルス対策基準</u> <u>3.2.9 情報システム安全対策基準</u> <u>3.2.10 ソフトウェア管理ガイドライン</u> <u>3.2.11 コンピュータ不正アクセス対策基準</u> <u>3.2.12 情報セキュリティ監査基準</u>	追加
情報セキュリティ アドミニストレー タ	31	B . セキュリティポリシーの策定	B . <u>情報セキュリティポリシーの策定</u>	用語の統一
情報セキュリティ アドミニストレー タ	31	1.1.2 情報資産の評価方法（機密性、完全性、 可用性に関する重要度、致命度、危険度）	1.1.2 情報資産の評価方法（機密性、完全性、 可用性に関する重要度、 <u>真正性、</u> <u>責任追跡性（説明責任）、信頼性、情報資</u> <u>産の価値の数値化、情報資産の損失が及ぼ</u> <u>す致命度、危険度）</u>	追加
情報セキュリティ アドミニストレー タ	31	1.2 脅威の認識	1.2 <u>リスクの認識</u>	他章と表現を統一
情報セキュリティ アドミニストレー タ	31	1.3.1 リスクの存在箇所（サーバ、クライアン ト、ネットワーク、ルータ、 ソフトウェア、開発ツール、記憶媒体）	1.3.1 リスクの存在箇所（サーバ、クライアン ト、ネットワーク、ルータ、 ソフトウェア、開発ツール、記録媒体）	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	31	1.4 対策の整理  <u>1.4.1 予防的対策</u> <u>1.4.2 緊急時への対策</u> <u>1.4.3 災害時への対策</u> <u>1.4.4 防護的対策</u> <u>1.4.5 保守への対策</u> <u>1.4.6 侵入検知および分析</u>	(削除)	削除
情報セキュリティ アドミニストレー タ	31	1.4 対策の整理	1.4 対策の整理と調査	他章と表現を統一
情報セキュリティ アドミニストレー タ	31		1.4.1 <u>抑止、予防、検知、回復</u>	スキル標準の記述との整合 性をとって追加
情報セキュリティ アドミニストレー タ	31		1.4.2 <u>最適化(低減)、回避、移転、保有</u>	スキル標準の記述との整合 性をとって追加
情報セキュリティ アドミニストレー タ	31		1.4.3 <u>物理的、管理的、人的、技術的</u>	スキル標準の記述との整合 性をとって追加
情報セキュリティ アドミニストレー タ	31	1.5 リスクの評価	1.5 リスクの <u>算定と評価</u>	他章と表現を統一
情報セキュリティ アドミニストレー タ	31	1.6 セキュリティ方針の策定	1.6 <u>情報セキュリティ基本</u> 方針の策定	用語の統一

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	32	2 セキュリティ基準の策定	2 <u>情報</u> セキュリティ <u>対策</u> 基準の策定	用語の統一
情報セキュリティ アドミニストレー タ	32	2.2.5 アプリケーションインストール規定 (ネットワークに接続した <u>マシン</u> に対す るアプリケーションのインストールと利 用に関する規定)	2.2.5 アプリケーションインストール規定 (ネットワークに接続した <u>情報システム</u> に対するアプリケーションのインストー ルと利用に関する規定)	用語の統一
情報セキュリティ アドミニストレー タ	32	2.2.7 コンピュータウイルス対策運用規定 (外部とのデータ授受を行う <u>マシン</u> に対 するコンピュータウイルス対策に関する 規定)	2.2.7 コンピュータウイルス対策運用規定 (外部とのデータ授受を行う <u>情報システ ム</u> に対するコンピュータウイルス対策に 関する規定)	用語の統一
情報セキュリティ アドミニストレー タ	32		2.2.9 災害時対応の規定 (災害による緊急対 応時の対処に関する規定)	追加
情報セキュリティ アドミニストレー タ	32	2.2.9 セキュリティ監査の規定 (セキュリテ ィ検査や監視、セキュリティ <u>監査</u> に関す る規定)	2.2.10 <u>情報</u> セキュリティ監査の規定 (セキュ リティ検査や監視、 <u>情報</u> セキュリティに 関する規定)	番号変更、用語の統一
情報セキュリティ アドミニストレー タ	32		2.2.11 情報システム管理者の規定 2.2.12 システム開発の規定 2.2.13 規定の承認手続き	番号変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	33	C . セキュリティシステムの設計と実装	C . セキュリティシステムの機能設計と実装	「機能」追加
情報セキュリティ アドミニストレー タ	33	1 セキュリティシステムの設計	1 セキュリティシステムの機能設計	「機能」追加
情報セキュリティ アドミニストレー タ	33	1.1.1 安全なパスワード（ <u>S / Key</u> パスワード、ワンタイムパスワード）	1.1.1 安全なパスワード（満たすべき複雑さ、ワンタイムパスワード）	S/Keyはワンタイムパスワードシステムのひとつであり冗長なため削除
情報セキュリティ アドミニストレー タ	33		1.1.2 認証デバイス（ICカード、USBトークンなど）	追加
情報セキュリティ アドミニストレー タ	33	1.1.2 認証メカニズム（ <u>PPP、TACACS</u> 、 <u>S+</u> 、 <u>RADIUS</u> 、 <u>Kerberos</u> 、 <u>DCE</u> 、 <u>FORTEZZA</u> ）	1.1.3 認証メカニズム（ <u>RADIUS</u> 、 <u>TACACS+</u> 、 <u>Kerberos</u> ）	番号変更、全角から半角 PPPは認証を含んではいるが、それ自体は回線接続確立が主な目的である、DCEとFOETEEZZAは一般的とはいえないため削除
情報セキュリティ アドミニストレー タ	33	1.1.3 その他の認証技術（バイオメトリックス（指紋、虹彩など）、 <u>デジタル署名</u> ）	1.1.4 その他の認証技術（バイオメトリックス（指紋、虹彩など）、 <u>電子証明書</u> ）	用語の統一
情報セキュリティ アドミニストレー タ	33	1.4.1 外部ネットワークとの接続（ファイアウォール、 <u>NAT</u> 、プロキシサーバ、 <u>IP</u> マスカレード）	1.4.1 外部ネットワークとの接続（ファイアウォール、 <u>NAT</u> 、 <u>NAPT</u> 、プロキシサーバ）	全角から半角 IPマスカレードはNAPTの一種

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	33	1.4.4 攻撃への防護策（不正アクセス、スプ ーフィング攻撃、公開サービスへの攻撃 〔DOS攻撃など〕）	1.4.4 攻撃への防護策（不正アクセス、スプ ーフィング攻撃、公開サービスへの攻撃 〔DoS攻撃など〕）	誤りを修正
情報セキュリティ アドミニストレー タ	34	1.5 データの <u>機密保持</u>	1.5 データの <u>セキュリティ</u>	他章と表現を統一
情報セキュリティ アドミニストレー タ	34	1.5.2 暗号化技術とその応用（AES、RSA、SSL、 PKI、認証局、IPsec、楕円曲線暗号方式）	1.5.2 暗号化技術とその応用（AES、RSA、SSL、 PKI、認証局、 <u>X.509</u> 、 IPsec、楕円曲線暗号方式）	誤りを修正、「X.509」追加
情報セキュリティ アドミニストレー タ	34	1.5.3 電子署名書（ <u>X.509</u> ）	1.5.3 電子署名（ <u>ハッシュ関数、MAC</u> ）	誤りを修正 「X.509」から「ハッシュ関 数、MAC」に変更
情報セキュリティ アドミニストレー タ	34	1.7.2 技術教育（ <u>テクニック面</u> ）	1.7.2 <u>IT技術に関する教育</u>	わかりやすい表現に修正
情報セキュリティ アドミニストレー タ	34	2.2 セキュリティシステムの開発	（移動）	3 . に移動
情報セキュリティ アドミニストレー タ	34	2.3 セキュリティ実装の確認	2.2 セキュリティ実装の確認	番号変更
情報セキュリティ アドミニストレー タ	34	2.3.1 侵入検査サービス	2.2.1 侵入検査サービス	番号変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	34	2.3.2 攻撃ツール	2.2.2 攻撃ツール	番号変更
情報セキュリティ アドミニストレー タ	34	2.3.3 セキュリティ情報 (CERT/CC、 <u>JPCERT/CC、IPA</u> )	2.2.3 セキュリティ情報 (JPCERT/CC、IPA)	番号変更、全角から半角 CERT/CC削除
情報セキュリティ アドミニストレー タ	34		3 セキュリティシステムの開発管理	2.2 が移動
情報セキュリティ アドミニストレー タ	34		3.1 <u>セキュリティシステムの開発管理</u>	新規追加
情報セキュリティ アドミニストレー タ	34		3.1.1 費用対効果	2.2.1が移動
情報セキュリティ アドミニストレー タ	34		3.1.2 <u>工程管理</u>	新規追加
情報セキュリティ アドミニストレー タ	35		2 <u>セキュリティ事件・事故への対応</u>	名称変更
情報セキュリティ アドミニストレー タ	35	2.3 事故の分析	2.3.3 <u>コンピュータフォレンジックス</u>	新規追加
情報セキュリティ アドミニストレー タ	36	3 <u>セキュリティの見直し</u>	3 <u>セキュリティ対策の見直し</u>	名称変更

スキル標準	頁	誤	正	修正内容
情報セキュリティ アドミニストレー タ	36	3.5 セキュリティポリシーの更新	3.5 <u>情報</u> セキュリティポリシーの更新	用語の統一
情報セキュリティ アドミニストレー タ		奥付 2005/1/14 独立行政法人 情報処理推進機構	奥付 2005/11/30 独立行政法人 情報処理推進機構	日付の変更
情報セキュリティ アドミニストレー タ			<u>【参考】テクニカルエンジニア(情報セキュリティ)</u> と情報セキュリティアドミニストレータの相 違	文書追加

スキル標準	頁	誤	正	修正内容
テクニカルエンジニア（情報セキュリティ）	15	1.3 リスクの算定 ・整理されたリスクに対して、その発生する確率が明確にされていること	・整理されたリスクに対して、その発現する確率が明確にされていること	用語の統一
テクニカルエンジニア（情報セキュリティ）	15	1.3 リスクの算定 ・リスクが発生したときの損害額が定量的または定性的に算定されていること	・リスクが発現したときの損害額が定量的または定性的に算定されていること	用語の統一
テクニカルエンジニア（情報セキュリティ）	15	1.3 リスクの算定 ・各リスクに対しては、リスク発生時の損害額と対策コストのバランスが考慮されていること	・各リスクに対しては、リスク発現時の損害額と対策コストのバランスが考慮されていること	用語の統一
テクニカルエンジニア（情報セキュリティ）	15	1.3 リスクの算定 ・リスクの発生する確率についての経験的データに関する知識	・リスクの発現する確率についての経験的データに関する知識	用語の統一
テクニカルエンジニア（情報セキュリティ）	16	1-4 リスクの評価 ・リスク対策が優先順位づけされていること	・リスク対策が優先順位付けされていること	「づけ」から「付け」に修正
テクニカルエンジニア（情報セキュリティ）	16	1-5 リスク対策の選択 ・リスクへの対策に関する知識	・リスク対策に関する知識	「への」削除

スキル標準	頁	誤	正	修正内容
テクニカルエンジニア（情報セキュリティ）	39	1.5.1 <u>予防的対策</u>	1.5.1 <u>抑止、予防、検知、回復</u>	詳細な表現に変更
テクニカルエンジニア（情報セキュリティ）	39	1.5.2 <u>緊急時への対策</u>	1.5.2 <u>最適化（低減）、回避、移転、保有</u>	置き換え
テクニカルエンジニア（情報セキュリティ）	39	1.5.3 <u>災害時への対策</u>	1.5.3 <u>物理的、管理的、人的、技術的</u>	置き換え
テクニカルエンジニア（情報セキュリティ）	43	1.4.2 緊急対応マニュアル	1.4.2 緊急時対応マニュアル	語句の修正
テクニカルエンジニア（情報セキュリティ）	45	2.1 システムの脆弱性	2.1 <u>情報</u> システムの脆弱性	用語の統一
テクニカルエンジニア（情報セキュリティ）	45	2.1.2 製品システムの脆弱性（Webブラウザ、メールシステム、バッファオーバーフロー、メモリリーク、スクリプトによる自動実行、SQLインジェクションなど）	2.1.2 製品システムの脆弱性（Webブラウザ、メールシステム、バッファオーバーフロー、メモリリーク、スクリプトによる自動実行、SQLインジェクションなど）	用語の統一（「メモリー」から「メモリ」へ）
テクニカルエンジニア（情報セキュリティ）	45	2.1.3 開発システムの脆弱性（ <u>開発システム、ツールの脆弱性</u> ）	2.1.3 <u>開発されたシステム</u> の脆弱性（同上）	システムの脆弱性は同一と考えられるため統一した
テクニカルエンジニア（情報セキュリティ）	45	2.1.7 <u>ソーシャルエンジニアリングによる脆弱性（電話対応、紙ゴミからの情報漏洩など）</u>	（削除）	システムの脆弱性ではないため削除

スキル標準	頁	誤	正	修正内容
テクニカルエンジニア（情報セキュリティ）	45	2.1.8 物理的アクセスの脆弱性（警備不備による不正侵入など）	2.1.7 物理的アクセスの脆弱性（警備不備による不正侵入など）	番号変更
テクニカルエンジニア（情報セキュリティ）	45	2.1.9 開発手法およびツールによる脆弱性（デバッグ時のバックドアの除去し忘れなど）	2.1.8 開発手法およびツールによる脆弱性（デバッグ時のバックドアの除去し忘れ、ツールに内在する脆弱性など）	番号変更
テクニカルエンジニア（情報セキュリティ）	45	2.1.9 開発手法およびツールによる脆弱性（デバッグ時のバックドアの除去し忘れなど）	2.1.8 開発手法およびツールによる脆弱性（デバッグ時のバックドアの除去し忘れ、 <u>ツールに内在する脆弱性</u> など）	追加
テクニカルエンジニア（情報セキュリティ）	46	2.2.4 サービス妨害攻撃（Denial of Service、DoS攻撃）（踏み台、分散サービス妨害など）	2.2.4 サービス妨害攻撃（Denial of Service（ <u>DoS</u> ）攻撃）（踏み台、分散サービス妨害など）	DoSはDenial of Serviceの省略形であることを示した
テクニカルエンジニア（情報セキュリティ）	46		2.2.9 <u>ボット、ボットネット</u>	追加
テクニカルエンジニア（情報セキュリティ）	46	2.2.9 ソーシャルエンジニアリングを利用した攻撃	2.2.10 ソーシャルエンジニアリングを利用した攻撃（電話対応、紙ゴミからの情報漏洩など）	番号変更
テクニカルエンジニア（情報セキュリティ）	46	2.2.9 ソーシャルエンジニアリングを利用した攻撃	2.2.10 ソーシャルエンジニアリングを利用した攻撃（ <u>電話対応、紙ゴミからの情報漏洩</u> など）	2.1.7で削除したソーシャルエンジニアリングの詳細を追加
テクニカルエンジニア（情報セキュリティ）	46	2.2.10 セキュリティ管理ツール（自動的にセキュリティホールや脆弱性の情報を収集）	2.2.11 セキュリティ管理ツール（自動的にセキュリティホールや脆弱性の情報を収集）	番号変更

スキル標準	頁	誤	正	修正内容
テクニカルエンジニア（情報セキュリティ）	46	3.1.1 著作権法 3.1.2 不正アクセス禁止法 3.1.3 個人情報保護関連法 3.1.4 不正競争防止法 3.1.5 電子署名法	3.1.1 著作権法 3.1.2 不正競争防止法 3.1.3 不正アクセス禁止法 3.1.4 電子署名法 3.1.5 個人情報保護関連法	順番変更 「不正競争防止法」を「不正アクセス禁止法」に置き換え
テクニカルエンジニア（情報セキュリティ）	46	3.1.6 e文書法	3.1.6 e_文書法	- を追加
テクニカルエンジニア（情報セキュリティ）	46	3.2.4 JIS X 0160 3.2.5 ISO/IEC TR 13335	3.2.4 ISO/IEC 13335 3.2.5 JIS X 0160	順番変更
テクニカルエンジニア（情報セキュリティ）	46	3.2.5 ISO/IEC TR 13335	3.2.4 ISO/IEC 13335	TR削除
テクニカルエンジニア（情報セキュリティ）	47	1.3.2 バイオメトリクス	1.3.2 バイオメトリックス	用語の統一