ISO/IEC27001
2022年版移行審査の手引き

ARM Standard

アームスタンダード株式会社

ISO/IEC27001:2022 への移行の手引き

目次

頁 NO.

1　2022 年版への移行について　2

2　移行審査までの流れ　3

2.1　2022 年版に移行するためのプロセス

2.2　各プロセスの解説　4

Step1　新規格の理解

① 改訂の概要

② 本文の改訂について

表１：要求事項の追加・改訂の有無

③ 附属書 A 管理策の変更点

④ 2022 年版を基準とした管理策の対比表　6

表２：2022 年版管理策の対比表

Step2　差分の理解　9

① 要求事項の追加・変更

② 附属書 A 情報セキュリティ管理策の新規管理策

Step3　文書類の改訂　14

Step4　スケジュール　15

Step5　関係者へ通知

Step6　運用開始　16

Step7　内部監査

Step8　マネジメントレビュー

3　付表　～2013 年版を基準とした管理策の対比表～　17

©アームスタンダード株式会社 All Rights Reserved.

1　2022 年版への移行について

情報セキュリティマネジメントシステム（ISMS）の適用規格である ISO/IEC27001 が改訂され、2022 年 10 月 25 日に ISO/IEC27001:2022 が発行されました。
これに伴い、弊社で認証を取得している組織様におかれましては、従来の ISO/IEC27001:2013 から ISO/IEC27001:2022 への移行が必要となります。ISO のマネジメントシステム規格は変化する社会の要請に対応して随時見直しが行われています。
この規格は国際標準として策定されておりますので、組織の皆様におかれましても、新しい要求事項の下で運用していただく必要がございます。

2025 年 10 月 31 日以降、ISO/IEC 27001:2013 は無効となります。

旧規格版にて認証を取得されている組織のご担当者様におかれましては、当資料をご活用の上計画的に 2022 年版への移行をご準備いただければ幸いです。

Ⅰ　これから 2022 年版移行の準備を開始する方

まずは当資料の「2 移行審査までの流れ」にて、全体のスケジュールをご確認いただき、STEP1 から順番に取り組みを始めることをお勧めいたします。

Ⅱ　ISO 規格の情報を収集しようとお考えの方

アームスタンダードでは講師によるセミナーや、無料でご覧いただける動画配信など情報提供を行っています。
セミナーに関しては「セミナー総合案内」を、無料動画配信については「e ラーニング総合案内」または下記Ⅳに記載の URL からご覧ください。

Ⅲ　現行システムの見直しに着手しようとお考えの方

現在運用中のマネジメントシステムと新規格の差分を抽出し、どこを見直すべきかをご検討ください。

Ⅳ　アームスタンダードの e ラーニングをご活用ください

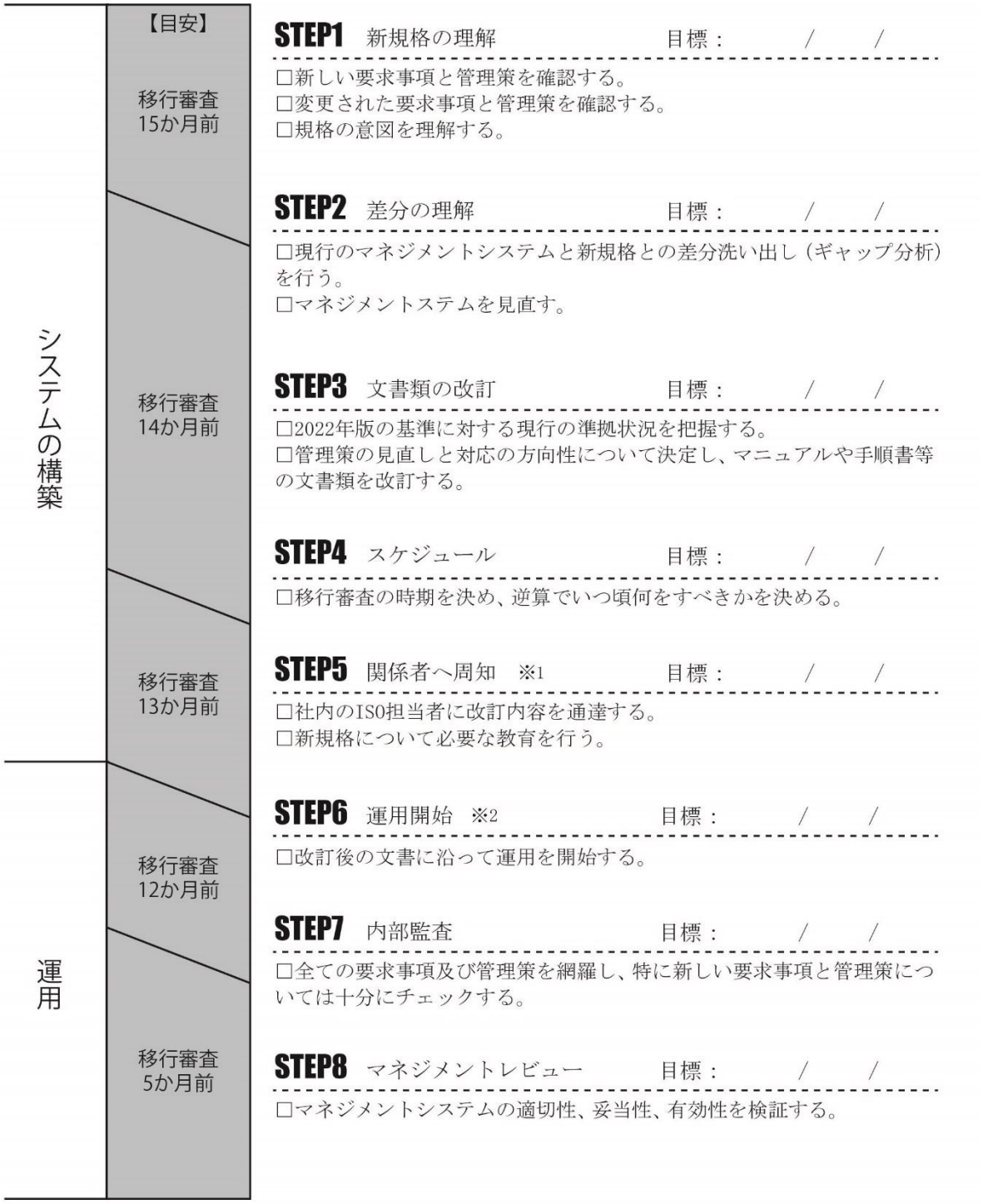
アームスタンダードのアカデミーコースでは、e ラーニングを提供しております。
ホームページにご案内を掲載しておりますので是非ご活用ください。
また、アームスタンダードのホームページでは「ISO/IEC27001:2022　規格改訂解説動画」を無料で視聴いただけます。

https://www.armstandard.com/useful-information/iso27001-revision/

©アームスタンダード株式会社 All Rights Reserved.

2　移行審査までの流れ

2.1　2022 年版に移行するためのプロセス



※1　移行審査は、通常の定期審査/再認証と合わせて実施することができます。ただし、再認証審査と同時に移行審査を受ける場合は、有効期限の 3 か月以上前に受審されることを推奨しております。

※2　適切な運用期間は組織様にてご判断いただく必要がございますが、運用のサイクルが一巡し、内部監査とマネジメントレビューを完了した状態でなければ移行審査を受審することはできません。サイクルを一巡させるまでには、一般的には 1 年～半年程度の運用が必要であると考えられます。

©アームスタンダード株式会社 All Rights Reserved.

2.2　各プロセスの解説

Step1 新規格の理解

①　改訂の概要

ISO/IEC 27001:2022 への改訂において、2013 年版からの本文の追加・変更は少なく、要求事項にも大きな追加・変更はありません。

今回の改訂では、2022 年 2 月に改訂された ISO/IEC27002:2022 に併せて附属書 A が全面的に改訂されています。新規管理策も 11 項目追加されていますので、見直しが必要になります。

②　本文の改訂について

今回の改訂において、本文についての追加・変更の内容は以下の通りです。

・ISO/IEC27001:2022 の構造とテキストに、最新版の規格として共通の形式が反映されました。

・ISO31000 の改訂に対応して、本規格で参照している ISO31000 の箇条番号が変更されました（参照する内容についての変更はありません）。

各項番ごとの改訂、及び要求事項の追加・変更の有無は下記の表を参照してください。

表１：要求事項の追加・改訂の有無　　*は 2022 年版で新しく追加された項番です。

(ISO/IEC27001:2022)		改訂の有無	要求事項の追加・変更
0. 序文	0.1 概要		
	0.2 他のマネジメントシステム規格との両立性		
1. 適用範囲			
2. 引用規格			
3. 用語及び定義			
4. 組織の状況	4.1 組織及びその状況の理解	有	無
	4.2 利害関係者のニーズ及び期待の理解	有	無
	4.3 情報セキュリティマネジメントシステムの適用範囲の決定		
	4.4 情報セキュリティマネジメントシステム	有	無
5. リーダーシップ	5.1 リーダーシップ及びコミットメント	有	無
	5.2 方針		
	5.3 組織の役割、責任及び権限	有	無
6. 計画策定	6.1 リスク及び機会に対処する活動		
	6.1.1 一般		
	6.1.2 情報セキュリティリスクアセスメント		
	6.1.3 情報セキュリティリスク対応	有	無
	6.2 情報セキュリティ目的及びそれを達成するための計画策定	有	有
	*6.3 変更の計画策定	有	有
7. 支援	7.1 資源		
	7.2 力量		

©アームスタンダード株式会社 All Rights Reserved.

(ISO/IEC27001:2022)		改訂の有無	要求事項の追加・変更
	7.3 認識		
	7.4 コミュニケーション	有	(有)
	7.5 文書化した情報		
	7.5.1 一般		
	7.5.2 作成及び更新		
	7.5.3 文書化した情報の管理		
8. 運用	8.1 運用の計画策定及び管理	有	有
	8.2 情報セキュリティリスクアセスメント		
	8.3 情報セキュリティリスク対応		
9. パフォーマンス評価	9.1 監視、測定、分析及び評価	有	無
	9.2 内部監査		
	*9.2.1 一般	有	無
	*9.2.2 内部監査プログラム	有	無
	9.3 マネジメントレビュー		
	*9.3.1 一般	有	無
	*9.3.2 マネジメントレビューへのインプット	有	有
	*9.3.3 マネジメントレビューの結果	有	無
10. 改善	*10.1 継続的改善	有	無
	*10.2 不適合及び是正処置	有	無

③　附属書 A 管理策の変更点

附属書 A 管理策は、ISO/IEC27002:2022 の箇条５～箇条８に規定したものがそのまま取り入れられており、両者の整合が保たれています。

2013 年版からの変更点として、管理策体系の簡素化のため、その主な側面に基づき 4 群にまとめられました。また、ISO/IEC27002:2022 における管理目的の扱いが変更されたことに対応して、管理目的への言及が削除されました。

項番	追加された新規管理策（11 項目）
5.7	脅威インテリジェンス
5.23	クラウドサービスの利用における情報セキュリティ
5.30	事業継続のための ICT の備え
7.4	物理的セキュリティの監視
8.9	構成管理
8.10	情報の削除
8.11	データマスキング
8.12	データ漏えいの防止
8.16	監視活動
8.23	ウェブ・フィルタリング
8.28	セキュリティに配慮したコーディング

内訳	項目数
新規	11
統合	24
更新	58
削除	0

©アームスタンダード株式会社 All Rights Reserved.

ISO/IEC 27002:2022	
2022 年版の管理策体系	項目数
5 組織的管理策	37
6 人的管理策	8
7 物理的管理策	14
8 技術的管理策	34
合計	93

ISO/IEC 27002:2013	
2013 年版の管理策体系	項目数
5 情報セキュリティのための方針群	2
6 情報セキュリティのための組織	7
7 人的資源のセキュリティ	6
8 資産の管理	10
9 アクセス制御	14
10 暗号	2
11 物理的及び環境的セキュリティ	15
12 運用のセキュリティ	14
13 通信のセキュリティ	7
14 システムの取得、開発及び保守	13
15 供給者関係	5
16 情報セキュリティインシデント管理	7
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	4
18 順守	8
合計	114

④　2022 年版を基準とした管理策の対比表

ISO/IEC27001:2022 のそれぞれの管理策に対して、どの項目が属しているかを一覧したい場合に参照してください。

表２：2022 年版管理策の対比表　　*は 2022 年版で新しく追加された項番です。

ISO/IEC27001:2022			ISO/IEC27001:2013	
5 組織的管理策	5.1	情報セキュリティのための方針群	A.5.1.1	情報セキュリティのための方針群
			A.5.1.2	情報セキュリティのための方針群のレビュー
	5.2	情報セキュリティの役割及び責任	A.6.1.1	情報セキュリティの役割及び責任
	5.3	職務の分離	A.6.1.2	職務の分離
	5.4	管理層の責任	A.7.2.1	経営陣の責任
	5.5	関係当局との連絡	A.6.1.3	関係当局との連絡
	5.6	専門組織との連絡	A.6.1.4	専門組織との連絡
	*5.7	脅威インテリジェンス	－	
	5.8	プロジェクトマネジメントにおける情報セキュリティ	A.6.1.5	プロジェクトマネジメントにおける情報セキュリティ
			A.14.1.1	情報セキュリティ要求事項の分析及び仕様化
	5.9	情報及びその他の関連資産の目録	A.8.1.1	資産目録
			A.8.1.2	資産の管理責任
	5.10	情報及びその他の関連資産の許容される利用	A.8.1.3	資産利用の許容範囲
			A.8.2.3	資産の取扱い
	5.11	資産の返却	A.8.1.4	資産の返却
	5.12	情報の分類	A.8.2.1	情報の分類
	5.13	情報のラベル付け	A.8.2.2	情報のラベル付け
	5.14	情報の転送	A.13.2.1	情報転送の方針及び手順
			A.13.2.2	情報転送に関する合意
			A.13.2.3	電子的メッセージ通信
	5.15	アクセス制御	A.9.1.1	アクセス制御方針
			A.9.1.2	ネットワーク及びネットワークサービスへのアクセス
	5.16	識別情報の管理	A.9.2.1	利用者登録及び登録削除
	5.17	認証情報	A.9.2.4	利用者の秘密認証情報の管理
			A.9.3.1	秘密認証情報の利用

©アームスタンダード株式会社 All Rights Reserved.

ISO/IEC27001:2022			ISO/IEC27001:2013	
			A.9.4.3	パスワード管理システム
5 組織的管理策	5.18	アクセス権	A.9.2.2	利用者アクセスの提供
			A.9.2.5	利用者アクセス権のレビュー
			A.9.2.6	アクセス権の削除又は修正
	5.19	供給者関係における情報セキュリティ	A.15.1.1	供給者関係のための情報セキュリティの方針
	5.20	供給者との合意における情報セキュリティの取扱い	A.15.1.2	供給者との合意におけるセキュリティの取扱い
	5.21	情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理	A.15.1.3	ICT サプライチェーン
	5.22	供給者のサービス提供の監視、レビュー及び変更管理	A.15.2.1	供給者のサービス提供の監視及びレビュー
			A.15.2.2	供給者のサービス提供の変更に対する管理
	*5.23	クラウドサービスの利用における情報セキュリティ	-	
	5.24	情報セキュリティインシデント管理の計画策定及び準備	A.16.1.1	責任及び手順
	5.25	情報セキュリティ事象の評価及び決定	A.16.1.4	情報セキュリティ事象の評価及び決定
	5.26	情報セキュリティインシデントへの対応	A.16.1.5	情報セキュリティインシデントへの対応
	5.27	情報セキュリティインシデントからの学習	A.16.1.6	情報セキュリティインシデントからの学習
	5.28	証拠の収集	A.16.1.7	証拠の収集
	5.29	事業の中断・阻害時の情報セキュリティ	A.17.1.1	情報セキュリティ継続の計画
			A.17.1.2	情報セキュリティ継続の実施
			A.17.1.3	情報セキュリティ継続の検証，レビュー及び評価
	*5.30	事業継続のための ICT の備え	-	
	5.31	法令、規制及び契約上の要求事項	A.18.1.1	適用法令及び契約上の要求事項の特定
			A.18.1.5	暗号化機能に対する規制
	5.32	知的財産権	A.18.1.2	知的財産権
	5.33	記録の保護	A.18.1.3	記録の保護
	5.34	プライバシー及び個人識別可能情報(PII)の保護	A.18.1.4	プライバシー及び個人を特定できる情報（PII）の保護
	5.35	情報セキュリティの独立したレビュー	A.18.2.1	情報セキュリティの独立したレビュー
	5.36	情報セキュリティのための方針群、規則及び標準の順守	A.18.2.2	情報セキュリティのための方針群及び標準の順守
			A.18.2.3	技術的順守のレビュー
	5.37	操作手順書	A.12.1.1	操作手順書
6 人的管理策	6.1	選考	A.7.1.1	選考
	6.2	雇用条件	A.7.1.2	雇用条件
	6.3	情報セキュリティの意識向上、教育及び訓練	A.7.2.2	情報セキュリティの意識向上，教育及び訓練
	6.4	懲戒手続	A.7.2.3	懲戒手続
	6.5	雇用の終了又は変更後の責任	A.7.3.1	雇用の終了又は変更に関する責任
	6.6	秘密保持契約又は守秘義務契約	A.13.2.4	秘密保持契約又は守秘義務契約
	6.7	リモートワーク	A.6.2.2	テレワーキング
	6.8	情報セキュリティ事象の報告	A.16.1.2	情報セキュリティ事象の報告
			A.16.1.3	情報セキュリティ弱点の報告
7 物理的管理策	7.1	物理的セキュリティ境界	A.11.1.1	物理的セキュリティ境界
	7.2	物理的入退	A.11.1.2	物理的入退管理策
			A.11.1.6	受渡場所
	7.3	オフィス、部屋及び施設のセキュリティ	A.11.1.3	オフィス，部屋及び施設のセキュリティ
	*7.4	物理的セキュリティの監視	-	
	7.5	物理的及び環境的脅威からの保護	A.11.1.4	外部及び環境の脅威からの保護
	7.6	セキュリティを保つべき領域での作業	A.11.1.5	セキュリティを保つべき領域での作業
	7.7	クリアデスク・クリアスクリーン	A.11.2.9	クリアデスク・クリアスクリーン方針
	7.8	装置の設置及び保護	A.11.2.1	装置の設置及び保護
	7.9	構外にある資産のセキュリティ	A.11.2.6	構外にある装置及び資産のセキュリティ
	7.10	記憶媒体	A.8.3.1	取外し可能な媒体の管理
			A.8.3.2	媒体の処分
			A.8.3.3	物理的媒体の輸送
			A.11.2.5	資産の移動
	7.11	サポートユーティリティ	A.11.2.2	サポートユーティリティ
	7.12	ケーブル配線のセキュリティ	A.11.2.3	ケーブル配線のセキュリティ
	7.13	装置の保守	A.11.2.4	装置の保守
	7.14	装置のセキュリティを保った処分又は再利用	A.11.2.7	装置のセキュリティを保った処分又は再利用

©アームスタンダード株式会社 All Rights Reserved.

ISO/IEC27001:2022			ISO/IEC27001:2013	
8 技術的管理策	8.1	利用者エンドポイント機器	A.6.2.1	モバイル機器の方針
			A.11.2.8	無人状態にある利用者装置
	8.2	特権的アクセス権	A.9.2.3	特権的アクセス権の管理
	8.3	情報へのアクセス制限	A.9.4.1	情報へのアクセス制限
	8.4	ソースコードへのアクセス	A.9.4.5	プログラムソースコードへのアクセス制御
	8.5	セキュリティを保った認証	A.9.4.2	セキュリティに配慮したログオン手順
	8.6	容量・能力の管理	A.12.1.3	容量・能力の管理
	8.7	マルウェアに対する保護	A.12.2.1	マルウェアに対する管理策
	8.8	技術的ぜい弱性の管理	A.12.6.1	技術的ぜい弱性の管理
			A.18.2.3	技術的順守のレビュー
	*8.9	構成管理	－	
	*8.10	情報の削除	－	
	*8.11	データマスキング	－	
	*8.12	データ漏えい防止	－	
	8.13	情報のバックアップ	A.12.3.1	情報のバックアップ
	8.14	情報処理施設・設備の冗長性	A.17.2.1	情報処理施設の可用性
	8.15	ログ取得	A.12.4.1	イベントログ取得
			A.12.4.2	ログ情報の保護
			A.12.4.3	実務管理者及び運用担当者の作業ログ
	*8.16	監視活動	－	
	8.17	クロックの同期	A.12.4.4	クロックの同期
	8.18	特権的なユーティリティプログラムの使用	A.9.4.4	特権的なユーティリティプログラムの使用
	8.19	運用システムへのソフトウェアの導入	A.12.5.1	運用システムに関わるソフトウェアの導入
			A.12.6.2	ソフトウェアのインストールの制限
	8.20	ネットワークのセキュリティ	A.13.1.1	ネットワーク管理策
	8.21	ネットワークサービスのセキュリティ	A.13.1.2	ネットワークサービスのセキュリティ
	8.22	ネットワークの分離	A.13.1.3	ネットワークの分離
	*8.23	ウェブフィルタリング	－	
	8.24	暗号の利用	A.10.1.1	暗号による管理策の利用方針
			A.10.1.2	鍵管理
	8.25	セキュリティに配慮した開発のライフサイクル	A.14.2.1	セキュリティに配慮した開発のための方針
	8.26	アプリケーションセキュリティの要求事項	A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
			A.14.1.3	アプリケーションサービスのトランザクションの保護
	8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	A.14.2.5	セキュリティに配慮したシステム構築の原則
	*8.28	セキュリティに配慮したコーディング	－	
	8.29	開発及び受入れにおけるセキュリティテスト	A.14.2.8	システムセキュリティの試験
			A.14.2.9	システムの受入れ試験
	8.30	外部委託による開発	A.14.2.7	外部委託による開発
	8.31	開発環境、テスト環境及び本番環境の分離	A.12.1.4	開発環境，試験環境及び運用環境の分離
			A.14.2.6	セキュリティに配慮した開発環境
	8.32	変更管理	A.12.1.2	変更管理
			A.14.2.2	システムの変更管理手順
			A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
			A.14.2.4	パッケージソフトウェアの変更に対する制限
	8.33	テスト用情報	A.14.3.1	試験データの保護
	8.34	監査におけるテスト中の情報システムの保護	A.12.7.1	情報システムの監査に対する管理策

©アームスタンダード株式会社 All Rights Reserved.

Step2 差分の理解

移行に際して、現行のマネジメントシステムと新規格との差分の洗い出しが必要となります。
ここでは文書類の改訂等、実作業が必要となるものについて掲載いたします。

① 要求事項の追加・変更

6.2 情報セキュリティ目的及び それを達成するための計画策定 d)

変更点	情報セキュリティ目的に関する要求事項を列挙する中に、「d) （情報セキュリティ目的を）監視する」が追加された。	
変更の趣旨	MSS 共通テキストにおける注記の追加を反映する変更	
要求事項の追加・変更	有	

6.2 情報セキュリティ目的及び それを達成するための計画策定 g)

変更点	情報セキュリティ目的に関する要求事項を列挙する中に、「g) 文書化した情報として利用可能な状態にする」 が追加された。	
変更の趣旨	MSS 共通テキストにおける注記の追加を反映する変更	
要求事項の追加・変更	有	ISO/IEC27001:2013 でも、この直後の文で情報セキュリティ目的に関する文書化した情報を保持することが求められている。要求事項の追加は、「利用可能な状態にする」ことである。

6.3 変更の計画策定

変更点	新規に項目が追加された。	
変更の趣旨	MSS 共通テキストの改定を反映して、ISMS の変更を行う場合に、 計画的に行うべきことが追加された。	
要求事項の追加・変更	有	

8.1 運用の計画策定及び管理 第 1 段落

変更点	第 1 文の変更： ・「箇条 6 で決定した活動を実施するために」 ← 「箇条 6.1 で決定した活動を実施するために」 前版の第 2 文（「6.2 で決定した情報セキュリティ目的・・」）の削除 ・計画策定及び管理の方法を追加：「－プロセスに関する基準の設定」、「－その基準に従った、プロセスの管理の実施」	
変更の趣旨	箇条 6（計画）を受けて、箇条 8 でその実施を求めることが、6.1.2 と 8.2、6.1.3 と 8.3 の対応も含めて、包括的に表現された。	
要求事項の追加・変更	有	MSS 共通テキストで一般的な表現を採っている部分。 前版との対応も、一般的な要求事項として同等と見られる。 この 2 項目は実施方法を定めている点で要求事項を追加しているとも見られる。 また、8.2 及び 8.3 は、MSS 共通テキストに沿って 8.1 に追加された 2 項目を ISO/IEC 27001 において具体化しているという側面もある。

©アームスタンダード株式会社 All Rights Reserved.

8.1 運用の計画策定及び管理 第 4 段落

変更点	・ 管理対象について：「外部から提供されるプロセス、製品又はサービ ス」←「外部委託したプロセス」 ・ 管理する範囲が ISMS に関連するものであることを明示した。	
変更の趣旨	MSS 共通テキストの変更が反映された。本来、外部から提供される製品及びサービスも管理すべきであるため。	
要求事項の追加・変更	有	外部から提供される製品及びサービスの管理が要求事項として追加された。 ISO/IEC 27002:2013、同 2022 における供給者関係についての管理策（ISO/IEC 27002:2022, 5.20 他）で製品及びサービスの調達を扱っていることと整合する ISO/IEC 27001 の変更。

9.3 マネジメントレビュー

変更点	9.3 の内容を維持しつつ、三つの細分箇条「9.3.1 一般」、「9.3.2 マネジメントレビューへのインプット」及び「9.3.3 マネジメントレビューの結果」に分けて構成が明確にされた。 マネジメントレビューのインプット（9.3.2）に、利害関係者のニーズ及び期待の変化が追加された。	
変更の趣旨	MSS 共通テキストの変更が反映された。	
要求事項の追加・変更	有	マネジメントレビューのインプットに、利害関係者のニーズ及び期待の変化が追加された。

② 附属書 A 情報セキュリティ管理策の新規管理策

5.7 脅威インテリジェンス

管理策	情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築しなければならない。
目的	適切なリスク低減処置を講じることができるように、組織の脅威環境についての認識をもつため。
管理策の主旨	組織に脅威インテリジェンスの構築を求める。
説明	･脅威インテリジェンスとは、①情報セキュリティの脅威についての情報を集め、②集めた情報を整理し、③使える状態に置くことである。このための組織、人、知識・能力、プロセスを持つことが前提となる。 ･ISO/IEC 27001 において、脅威を含むリスク源の特定は、情報セキュリティリスクアセスメントにおける情報セキュリティリスク特定の前提となる。この管理策では、脅威情報を集め、使える状態にして維持するまでの活動が加えられた。これによって、状況の変化及び情報セキュリティインシデントの発生に備える。 ･脅威インテリジェンスには、ぜい弱性情報の収集や攻撃手法の分析などの、高い専門性を必要とする分野もある。「5.6 専門組織との連絡」によって専門組織から情報を得ることは、脅威インテリジェンスの手段にもなる。 【情報例】 ゼロデイ攻撃、マルウェア、フィッシング、中間者攻撃、サービス拒否（DoS）攻撃など

©アームスタンダード株式会社 All Rights Reserved.

5.23 クラウドサービスの利用のための情報セキュリティ

管理策	クラウドサービスの取得、利用、管理及び終了のプロセスを、組織の情報セキュリティ要求事項に従って確立しなければならない。
目的	クラウドサービスの利用における情報セキュリティを規定及び管理するため。
管理策の主旨	組織がクラウドサービスの調達、利用、管理及び終了の プロセスを持つことが求められている。
説明	･この管理策では、組織が利用するクラウドサービスを組織内のそれぞれの部門や場面で検討したり採用したりする前提として、クラウドサービスの調達、利用、管理及び終了についての一般的なプロセスや規則を持つことが求められている。 例：・クラウドサービスを利用してよい条件の規定（組織の機能、クラウドサービスの種類 等）クラウドサービスの利用を承認する権限の所在 ・クラウドサービスの利用に関するトピック固有の方針を持つことも、この管理策の要求を実施する一部になりうる。 【クラウドサービスの例】SaaS、PaaS、IaaS 等

5.30 事業継続のための ICT の備え

管理策	事業継続の目的及び ICT 継続の要求事項に基づいて ICT の備えを計画、実施、維持及び試験しなければならない。
目的	事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。
管理策の主旨	組織における事業継続計画(BCP)の一環として、 ICT（属性は可用性のみ)の継続性、すなわち可用性の維持が求められている。
説明	関係する管理策に、「 5.29 事業の中断・阻害時の情報セキュリティ」がある。 【手順の概要】 ※参考 ① 事業を支える業務を洗い出す ⇒中心業務は何か、その概要、主管部署など ② 業務が中断することによる影響を特定する ⇒定量的(金額的影響)と定性的(非金銭的影響) ③ 業務復旧優先度を決定する ⇒先に手を付ける業務と後回しにする業務を選別 ④ 目標復旧時間:RTO と目標復旧レベル:RLO の設定 ⇒優先業務について RTO と RLO を決定する ⑤ 各業務に必要な資源を特定する ⇒人→どのような力量を持った要員を何名等

7.4 物理的セキュリティの監視

管理策	施設は、認可されていない物理的アクセスについて継続的に監視しなければならない。
目的	認可されていない物理的アクセスを検知し、抑止するため。
管理策の主旨	敷地、建屋、部屋などへの物理的アクセスを監視することが求められている。
説明	・監視手段の例： 警備員の配置、物理的侵入検知（監視カメラ、赤外線センサー等)、物理的破壊検知 【関係する管理策】 ・物理的セキュリティ境界：7.1 物理的セキュリティ境界 7.2 物理的入退 7.3 オフィス、部屋及び施設のセキュリティ ・不正な物理的アクセスの監視：7.4 物理的セキュリティの監視

©アームスタンダード株式会社 All Rights Reserved.

8.9 構成管理

管理策	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視及びレビューしなければならない。
目的	ハードウェア、ソフトウェア、サービス及びネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更又は誤った変更によって構成が変えられないことを確実にするため。
管理策の主旨	ハードウェア、ソフトウェア、サービス及びネットワークについて構成管理の実施が求められている。
説明	実施例：新規導入時の設定／初期設定の更新・無効化／運用中の継続的な維持／管理責任者の設置／継続的監視 【関係する管理策】　8.8 技術的ぜい弱性の管理 情報システムの構成要素（主にソフトウェア）のぜい弱性情報を継続的に取得し、ぜい弱性を解消する。

8.10 情報の削除

管理策	情報システム、装置又はその他の記憶媒体に保存している情報は、必要でなくなった場合は削除しなければならない。
目的	取扱いに慎重を要する情報の不必要な漏えいを防止し、情報の削除に関する法令、規制及び契約上の要求事項を順守するため。
管理策の主旨	記憶媒体上にある情報は、必要がなくなったときに削除することが求められている。
説明	情報漏えい対策として。特に個人情報の扱い等について法令遵守も意識した管理策である。 ･適切な削除方法を選ぶ。 　データ削除ソフトウェアの使用／媒体の物理的破壊（破砕、穿孔等）／消磁／復号鍵の消去 等 ･証拠として削除の記録を採る。 ･外部のサービスを使う場合、削除したことの証拠を取得する。

8.11 データマスキング

管理策	データマスキングは、適用される法律を考慮して、アクセス制御に関する組織のトピック固有の個別方針及びその他の関連するトピック固有の個別方針、並びに業務要求事項に従って使用しなければならない。
目的	PII（personally identifiable information）を含む、取扱いに慎重を要するデータの 開示を制限し、法令、規制及び契約上の要求事項を順守するため。
管理策の主旨	組織の方針、事業上の要求事項及び法令を考慮して、人・役割に応じて、データ項目を選んで隠すことが求められている。
説明	・データマスキングの方法例 　・データを伏せる。例えば、一定の文字、数値等に置き換える。 　・データを復元不可能な方法で置き換える。例えば、ハッシュ値に置き換える。 　・データを暗号化する。特定の人に復号鍵を持たせる。 　・データレコード単位のアクセス制御を適用する。例えば、データベースソフトウェアの機能の使用にて。 ・組織内においても、人・役割に応じてアクセスを認めるデータの範囲を設定するためにデータマスキングを使用する。 　・端末画面に表示するデータ項目を、人・役割に応じて決め、制御する。

©アームスタンダード株式会社 All Rights Reserved.

8.12 データ漏えいの防止

管理策	データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用しなければならない。
目的	個人又はシステムによる情報の認可されていない開示及び抽出を検出し防止するため。
管理策の主旨	情報システム、ネットワーク及びその他の機器におけるデータ漏えいの防止が求められている。
説明	･対象とするデータと場面を特定する。 例：メール、ファイル転送、モバイル機器、可搬記憶媒体等。 ･データの移動を監視し、漏えいを阻止する。 ･データの漏えいに繋がる行為（例：装置への可搬記憶媒体の接続）を検知し、阻止する。 【関係する管理策の例】8.12 は、以下の管理策を補う。 7.14 装置のセキュリティを保った処分又は再利用 8.1 利用者のエンドポイント機器 8.20 ネットワークのセキュリティ 8.27 セキュリティに配慮したアーキテクチャ及びシステム構築の原則

8.16 監視活動

管理策	情報セキュリティインシデントの可能性がある事象を評価するために、ネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、適切な処置を講じなければならない。
目的	異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため。
管理策の主旨	ネットワーク、システム及びアプリケーションの挙動を監視し、情報セキュリティインシデントであるか否かを評価することが求められている。
説明	･広範な監視対象候補の中で、事業上の要求、情報セキュリティの要求及び法令を考慮して監視対象を選ぶ。 候補：ネットワークトラフィック、情報・機器・アプリケーションへのアクセス、 　　イベントログ、リソース使用状況 等 ･挙動が異常であるか否かを判定する基準を持つ。 ･検知した異常をあらかじめ定めた役割を持つ人に通知する。 ※ISO/IEC 27002:2013 の「12.4 ログ取得及び監視」は、標題に監視を含むが、内容はログ取得の範囲であった。

8.23 ウェブ・フィルタリング

管理策	悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理しなければならない。	
目的	システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。	
管理策の主旨	不正なウェブサイトによるシステムへの悪影響を防ぎ、認可されていない資源へのアクセスを防止するために、外部ウェブサイトへのアクセスを管理することが求められている。	
説明	･ アクセスを禁止するウェブサイトの例 ☞既知の悪性ウェブサイト ☞禁止リスト／許可リスト ☞シグネチャによる判定	･アクセスをさせない仕組みの例 ☞禁止リスト／許可リスト ☞コマンド コントロールサーバ ☞違法コンテンツを提供するウェブサイト

©アームスタンダード株式会社 All Rights Reserved.

8.28 セキュリティに配慮したコーディング

管理策	セキュリティに配慮したコーディングの原則をソフトウェア開発に適用しなければならない。
目的	ソフトウェアがセキュリティに配慮して書かれ、それによってソフトウェアの潜在的な情報セキュリティのぜい弱性の数を減らすことを確実にするため。
管理策の主旨	ソフトウェアのぜい弱性を排除するために、ソフトウェア開発においてセキュリティに配慮したコーディング（セキュアコーディング）の原則を適用することが求められている。
説明	･組織としての管理：プロセスの確立／外部から調達するソフトウェア構成要素への適用等 ･計画時の考慮：採用するコーディング原則の決定／既知のぜい弱な手法についての知識／ソフトウェア開発ツールの利用／開発者の資格／セキュリティに配慮した設計及びアーキテクチャの採用等 ･コーディング中の考慮：セキュリティに配慮したコーディング手法の採用／禁止するプログラミング手法の明示等

Step3 文書類の改訂

Step2 で要求事項及び管理策の新しい要素について理解したら、差分について、まず 2022 年版の基準に対する現在の準拠状況の把握を行い、管理策の見直しと対応の方向性についてまとめます。
以下は進め方の一例（参考）となります。

① ISO/IEC27001:2022 の各管理策に対し、現在の準拠状況と対応の方針について情報を整理します。
例：

2022 年版管理策	現在の取組み状況	追加・変更すべき活動	対応方法
5.7 脅威インテリジェンス 情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築しなければならない。	同業他社で発生した情報セキュリティの脅威に関連する情報を収集し、蓄積している。	蓄積した情報を整理し、分析・評価・考察を加えたものに変換する構造を用意する。	情報セキュリティチームより担当者を選出し、脆弱性及び発生頻度の観点から分析・評価・考察を行うプロセスを業務マニュアルに追加する。

② 以上のように情報の整理が済んだら、次に附属書 A に示す管理策と比較し、必要な管理策が見落とされていないか、また新規管理策に漏れなく対応しているかをレビューします。
③ このレビューに対して、規格の要求事項と照らし合わせ、適用宣言書を改訂します。
④ 改訂が全て完了したら、最後に改訂した MS マニュアル全体をレビューします。改訂の際は適切性と妥当性に着目して当該文書を全てレビューする必要があります。

- ■ 適切性：文書が規格及び規定のような他の信頼できる情報源に合致している、文書内及び関連する文書と整合している。
- ■ 妥当性：文書に記載されている内容が必要充分である。

©アームスタンダード株式会社 All Rights Reserved.

Step4 スケジュール

移行全体の大まかなスケジュールを策定します。
移行はおよそ 1 年から 1 年半程度の期間が必要となるので、完了時期から遡って計画しましょう。
ここではスケジュール策定の前提と目安について紹介します。
前提：
・規格発行後、3 年後である 2025 年 10 月 31 日までに移行完了する。
・移行審査の時期を定期審査の時期に合わせるのか、再認証審査の時期に合わせるのかを検討する。
・認証機関との調整が必要なので、移行計画の提案ができた段階で調整を行う。

期間の目安	ステップ	概要	内容
～16 ヶ月前	Step1	新規格の理解	・新しい要求事項と管理策を確認する。 ・変更された要求事項と管理策を確認する。 ・規格の意図を理解する。
	Step2	差分を洗い出す	・現在のマネジメントシステムと新規格との差分を洗い出す。 ・マネジメントシステムを見直す。
～15 ヶ月前	Step3	文書類の改訂	・2022 年版の規格の基準に対する現行の準拠状況を把握する。 ・管理策の見直しと対応の方向性について決定し、マニュアルや手順書等の文書類を改訂する。
	Step4	スケジュール	・移行審査の時期を決め、逆算でいつ頃何をすべきかを決める。
～14 ヶ月前	Step5	関係者へ周知	・社内の ISO 担当者に改訂内容を通達する。 ・新規格について必要な教育を行う。
	Step6	運用開始	・改訂後の文書に沿って運用を開始する。
～12 ヶ月前	Step7	内部監査	・全ての要求事項を網羅しているか内部監査を行う。
～5 ヶ月前	Step8	マネジメントレビュー	・適切性、妥当性、有効性の観点からトップマネジメントによるマネジメントシステムの検証を行う。
当月	Step9	移行審査	・現地での審査を行う。

詳細は弊社の規格改正ページ(https://www.armstandard.com/iso27001-revision/)をご覧ください。

Step5 関係者へ周知

2022 年版の規格について実務担当者まで周知します。
新規格の理解が深められるよう、以下のセミナーを開催しております。

名称	概要	セミナー	e ラーニング	受講対象
ISO/IEC27001:2022 規格改訂解説動画	2022 年版への改訂の概要をまとめた e ラーニングです。	-	●	改訂内容を学習したい方
入門セミナー	ISO の基礎を解説するセミナーです。	● (Web)	●	ISO を初めて学ぶ新入社員 新任の ISO 担当者等
規格ポイント解説 セミナー	規格要求事項のポイントを解説するセミナーです。	● (Web)	●	規格の概要を理解したい ISO 担当者等
内部監査員養成 セミナー	内部監査員に必要な知識と技能を実践的な講義と演習で習得していただけるセミナーです。	● (集合)	●	新たな内部監査員候補の方

※アカデミーコースでの受け放題対象サービスは e ラーニングのみとなります。セミナーは有料にて提供しております。

©アームスタンダード株式会社 All Rights Reserved.

Step6 運用開始

改訂したマニュアル、手順書に沿って運用、開始、測定を行います。

Step7 内部監査

全ての要求事項及び管理策を網羅し、特に新しい要求事項と管理策については十分にチェックします。

Step8 マネジメントレビュー

マネジメントシステムの適切性、妥当性、有効性を検証します。

©アームスタンダード株式会社 All Rights Reserved.

2.3　付表　【2013 年版を基準とした管理策の対比表】

ISO/IEC27001:2013 管理策が、どの管理策に対応しているかを一覧したい場合にご参照ください。

ISO/IEC27001:2013		ISO/IEC27001:2022	
A.5	情報セキュリティのための方針群		
A.5.1	情報セキュリティのための経営陣の方向性		
A.5.1.1	情報セキュリティのための方針群	5.1	情報セキュリティのための方針群
A.5.1.2	情報セキュリティのための方針群のレビュー		
A.6	情報セキュリティのための組織		
A.6.1	内部組織		
A.6.1.1	情報セキュリティの役割及び責任	5.2	情報セキュリティの役割及び責任
A.6.1.2	職務の分離	5.3	職務の分離
A.6.1.3	関係当局との連絡	5.5	関係当局との連絡
A.6.1.4	専門組織との連絡	5.6	専門組織との連絡
A.6.1.5	プロジェクトマネジメントにおける情報セキュリティ	5.8	プロジェクトマネジメントにおける情報セキュリティ
A.6.2	モバイル機器及びテレワーキング		
A.6.2.1	モバイル機器の方針	8.1	利用者エンドポイント機器
A.6.2.2	テレワーキング	6.7	リモートワーク
A.7	人的資源のセキュリティ		
A.7.1	雇用前		
A.7.1.1	選考	6.1	選考
A.7.1.2	雇用条件	6.2	雇用条件
A.7.2	雇用期間中		
A.7.2.1	経営陣の責任	5.4	管理層の責任
A.7.2.2	情報セキュリティの意識向上,教育及び訓練	6.3	情報セキュリティの意識向上、教育及び訓練
A.7.2.3	懲戒手続き	6.4	懲戒手続
A.7.3	雇用の修了及び変更		
A.7.3.1	雇用の修終了又は変更に関する責任	6.5	雇用の終了又は変更後の責任
A.8	資産の管理		
A.8.1	資産に対する責任		
A.8.1.1	資産目録	5.9	情報及びその他の関連資産の目録
A.8.1.2	資産の管理責任	5.9	情報及びその他の関連資産の目録
A.8.1.3	資産利用の許容範囲	5.10	情報及びその他の関連資産の許容される利用
A.8.1.4	資産の返却	5.11	資産の返却
A.8.2	情報分類		
A.8.2.1	情報の分類	5.12	情報の分類
A.8.2.2	情報のラベル付け	5.13	情報のラベル付け
A.8.2.3	資産の取扱い	5.10	情報及びその他の関連資産の許容される利用
A.8.3	媒体の取扱い		
A.8.3.1	取外し可能な媒体の管理	7.10	記憶媒体
A.8.3.2	媒体の処分	7.10	記憶媒体
A.8.3.3	物理的媒体の輸送	7.10	記憶媒体
A.9	アクセス制御		
A.9.1	アクセス制御に対する業務上の要求事項		
A.9.1.1	アクセス制御方針	5.15	アクセス制御
A.9.1.2	ネットワーク及びネットワークサービスへのアクセス	5.15	アクセス制御
A.9.2	利用者アクセスの管理		
A.9.2.1	利用者登録及び登録削除	5.16	識別情報の管理
A.9.2.2	利用者アクセスの提供（provisioning）	5.18	アクセス権
A.9.2.3	特権的アクセス権の管理	8.2	特権的アクセス権
A.9.2.4	利用者の秘密認証情報の管理	5.17	認証情報
A.9.2.5	利用者アクセス権のレビュー	5.18	アクセス権
A.9.2.6	アクセス権の削除又は修正	5.18	アクセス権
A.9.3	利用者の責任		
A.9.3.1	秘密認証情報の利用	5.17	認証情報
A.9.4	システム及びアプリケーションのアクセス制御		
A.9.4.1	情報へのアクセス制限	8.3	情報へのアクセス制限
A.9.4.2	セキュリティに配慮したログオン手順	8.5	セキュリティを保った認証
A.9.4.3	パスワード管理システム	5.17	認証情報
A.9.4.4	特権的なユーティリティプログラムの使用	8.18	アクセス権

©アームスタンダード株式会社 All Rights Reserved.

ISO/IEC27001:2013		ISO/IEC27001:2022	
A.9.4.5	プログラムソースコードへのアクセス制御	8.4	ソースコードへのアクセス
A.10	暗号		
A.10.1	暗号による管理策		
A.10.1.1	暗号による管理策の利用方針	8.24	暗号の利用
A.10.1.2	かぎ管理	8.24	暗号の利用
A.11	物理的及び環境的セキュリティ		
A.11.1	セキュリティに配慮したログオン手順を保つべき境界		
A.11.1.1	物理的セキュリティ境界	7.1	物理的セキュリティ境界
A.11.1.2	物理的入隊管理策	7.2	物理的入退
A.11.1.3	オフィス、部屋及び施設のセキュリティ	7.3	オフィス、部屋及び施設のセキュリティ
A.11.1.4	外部及び環境の脅威からの保護	7.5	物理的セキュリティの監視
A.11.1.5	セキュリティを保つべき領域での作業	7.6	物理的セキュリティの監視
A.11.1.6	受渡場所	7.2	物理的入退
A.11.2	装置		
A.11.2.1	装置の設置及び保護	7.8	装置の設置及び保護
A.11.2.2	サポートユーティリティ	7.11	サポートユーティリティ
A.11.2.3	ケーブル配線のセキュリティ	7.12	ケーブル配線のセキュリティ
A.11.2.4	装置の保守	7.13	装置の保守
A.11.2.5	資産の移動	7.10	記憶媒体
A.11.2.6	構外にある装置及び資産のセキュリティ	7.9	構外にある資産のセキュリティ
A.11.2.7	装置のセキュリティを保った処分又は再利用	7.14	装置のセキュリティを保った処分又は再利用
A.11.2.8	無人状態にある利用者装置	8.1	利用者エンドポイント機器
A.11.2.9	クリアデスク・クリアスクリーン方針	7.7	クリアデスク・クリアスクリーン
A.12	運用のセキュリティ		
A.12.1	運用の手順及び責任		
A.12.1.1	操作手順書	5.37	操作手順書
A.12.1.2	変更管理	8.32	操作手順書
A.12.1.3	容量・能力の管理	8.6	操作手順書
A.12.1.4	開発環境, 試験環境及び運用環境の分離	8.31	開発環境、テスト環境及び本番環境の分離
A.12.2	マルウェアからの保護		
A.12.2.1	マルウェアに対する管理策	8.7	マルウェアに対する保護
A.12.3	バックアップ		
A.12.3.1	情報のバックアップ	8.13	情報のバックアップ
A.12.4	ログ取得及び監視		
A.12.4.1	イベントログ取得	8.15	ログ取得
A.12.4.2	ログ情報の保護	8.15	ログ取得
A.12.4.3	実務管理者及び運用担当者の作業ログ	8.15	ログ取得
A.12.4.4	クロックの同期	8.17	クロックの同期
A.12.5	運用ソフトウェアの管理		
A.12.5.1	運用システムに関わるソフトウェアの導入	8.19	運用システムへのソフトウェアの導入
A.12.6	技術的ぜい弱性管理		
A.12.6.1	技術的ぜい弱性の管理	8.8	技術的ぜい弱性の管理
A.12.6.2	ソフトウェアのインストールの制限	8.19	運用システムへの 12 ソフトウェアの導入
A.12.7	情報システムの監査に対する考慮事項		
A.12.7.1	情報システムの監査に対する管理策	8.34	監査におけるテスト中の情報システムの保護
A.13	通信のセキュリティ		
A.13.1	ネットワークセキュリティ管理施設		
A.13.1.1	ネットワーク管理策	8.20	ネットワークのセキュリティ
A.13.1.2	ネットワークサービスのセキュリティ	8.21	ネットワークサービスのセキュリティ
A.13.1.3	ネットワークの分離	8.22	ネットワークの分離
A.13.2	情報の転送		
A.13.2.1	情報転送の方針及び手順	5.14	情報の転送
A.13.2.2	情報転送に関する合意	5.14	情報の転送
A.13.2.3	電子的メッセージ通信	5.14	情報の転送
A.13.2.4	機密保持契約又は守秘義務契約	6.6	秘密保持契約又は守秘義務契約
A.14	システムの取得, 開発及び保守		
A.14.1	情報システムのセキュリティ要求事項		
A.14.1.1	情報セキュリティ要求事項の分析及び仕様化	5.8	秘密保持契約又は守秘義務契約
A.14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	8.26	アプリケーションセキュリティの要求事項
A.14.1.3	アプリケーションサービスのトランザクションの保護	8.26	アプリケーションセキュリティの要求事項
A.14.2	開発及びサポートプロセスにおけるセキュリティ		

©アームスタンダード株式会社 All Rights Reserved.

ISO/IEC27001:2013		ISO/IEC27001:2022	
A.14.2.1	セキュリティに配慮した開発のための方針	8.25	セキュリティに配慮した開発のライフサイクル
A.14.2.2	システムの変更管理手順	8.32	変更管理
A.14.2.3	オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー	8.32	変更管理
A.14.2.4	パッケージソフトウェアの変更に対する制限	8.32	変更管理
A.14.2.5	セキュリティに配慮したシステム構築の原則	8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
A.14.2.6	セキュリティに配慮した開発環境	8.31	開発環境、テスト環境及び本番環境の分離
A.14.2.7	外部委託による開発	8.30	外部委託による開発
A.14.2.8	システムセキュリティの試験	8.29	開発及び受入れにおけるセキュリティテスト
A.14.2.9	システムの受入れ試験	8.29	開発及び受入れにおけるセキュリティテスト
A.14.3	試験データ		
A.14.3.1	試験データの保護	8.33	テスト用情報
A.15	供給者関係		
A.15.1	供給者関係における情報セキュリティ		
A.15.1.1	供給者関係のための情報セキュリティの方針	5.19	供給者関係における情報セキュリティ
A.15.1.2	供給者との合意におけるセキュリティの取扱い	5.20	供給者との合意における情報セキュリティの取扱い
A.15.1.3	ICT サプライチェーン	5.21	情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理
A.15.2	供給者のサービス提供の管理		
A.15.2.1	供給者のサービス提供の監視及びレビュー	5.22	供給者のサービス提供の監視、レビュー及び変更管理
A.15.2.2	供給者のサービス提供の変更に対する管理	5.22	供給者のサービス提供の監視、レビュー及び変更管理
A.16	情報セキュリティインシデント管理		
A.16.1	情報セキュリティインシデントの管理及びその改善		
A.16.1.1	責任及び手順	5.24	情報セキュリティインシデント管理の計画策定及び準備
A.16.1.2	情報セキュリティ事象の報告	6.8	情報セキュリティ事象の報告
A.16.1.3	情報セキュリティ弱点の報告	6.8	情報セキュリティ事象の報告
A.16.1.4	情報セキュリティ事象の評価及び決定	5.25	情報セキュリティ事象の評価及び決定
A.16.1.5	情報セキュリティインシデントへの対応	5.26	情報セキュリティインシデントへの対応
A.16.1.6	情報セキュリティインシデントからの学習	5.27	情報セキュリティインシデントからの学習
A.16.1.7	証拠の収集	5.28	証拠の収集
A.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		
A.17.1	情報セキュリティ継続		
A.17.1.1	情報セキュリティ継続の計画	5.29	事業の中断・阻害時の情報セキュリティ
A.17.1.2	情報セキュリティ継続の実施	5.29	事業の中断・阻害時の情報セキュリティ
A.17.1.3	情報セキュリティ継続の検証, レビュー及び評価	5.29	事業の中断・阻害時の情報セキュリティ
A.17.2	冗長性		
A.17.2.1	情報処理施設の可用性	8.14	情報処理施設・設備の冗長性
A.18	遵守		
A.18.1	法的及び契約上の要求事項の順守		
A.18.1.1	適用法令及び契約上の要求事項の特定	5.31	法令、規制及び契約上の要求事項
A.18.1.2	知的財産権	5.32	知的財産権
A.18.1.3	記録の保護	5.33	記録の保護
A.18.1.4	プライバシー及び個人を特定できる情報（PⅡ）の保護	5.34	プライバシー及び個人識別可能情報(PII)の保護
A.18.1.5	暗号化機能に対する規制	5.31	法令、規制及び契約上の要求事項
A.18.2	情報セキュリティのレビュー		
A.18.2.1	情報セキュリティの独立したレビュー	5.35	情報セキュリティの独立したレビュー
A.18.2.2	情報セキュリティのための方針群及び標準の順守	5.36	情報セキュリティのための方針群、規則及び標準の順守
A.18.2.3	技術的順守のレビュー	5.36 /8.8	情報セキュリティのための方針群、規則及び標準の順守/技術的ぜい弱性の管理

©アームスタンダード株式会社 All Rights Reserved.

発行元： アームスタンダード株式会社
〒103-0012 東京都中央区日本橋堀留町1-10-15
JL日本橋ビル1F
TEL: 03-3666-8788 / (営業部) 03-3666-8814
URL https://www.armstandard.com/
本書の無断複写は、著作権上での例外を除き、禁じられています。