ISO 27001：2013
具体的な移行ステップと移行審査のポイント

2014年10月

日本マネジメントシステム認証機関協議会
情報技術委員会
委員長　中村 春雄

はじめに:2013年版への移行

2013年版の主な変更点

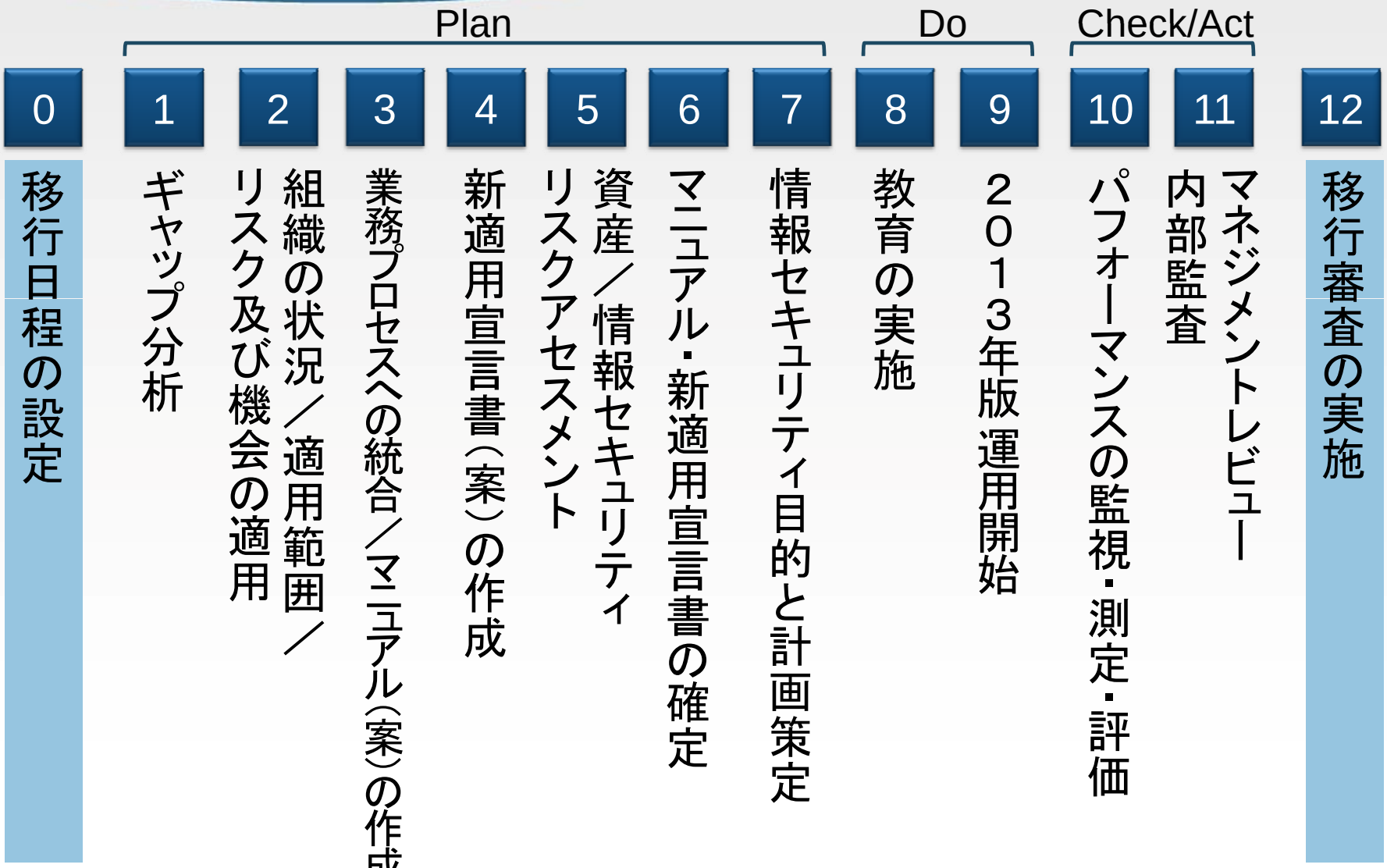
- 経営的視点の明確化
- 業務プロセスへの統合
- 目的の設定と計画策定
- パフォーマンスの評価
- 管理策の新設と廃止
- 汎用化されたリスク管理

確実に、すみやかに
移行したい

移行を契機に
より有効になるように
見直したい

2013年版 移行の流れ

ー確実に、すみやかに移行を目指すー



ステップ0：移行日程の設定

- 移行審査は定期/更新審査との同時実施を推奨。よって、自社の定期/更新審査の時期を明確にし、移行審査の実施日程を定める
- 移行期限が迫っている場合、定期/更新審査の時期を繰り上げて実施することも可能。また、定期/更新審査と移行審査の同時実施が困難な場合、単独での移行審査も可能。

ステップ1:ギャップ分析

1. 共通要素採用よる変更
2. 管理策の新設と廃止
3. 汎用化されたリスク管理

1. 共通要素採用による変更

(1) 組織の状況、適用範囲、リスク及び機会
（成果は出ているか）

(2) 業務プロセスへの統合
（ダブルスタンダードになっていないか）

(3) 目的の設定と計画策定

(4) パフォーマンスの評価

3. 汎用化されたリスク管理

(1) リスクの定義の変更
リスク：目的に対する不確かさの影響

(2) 汎用的リスクアセスメント
資産、脆弱性による分析に限定せず

2. 管理策の新設と廃止

(1) プロジェクトの情報セキュリティ

(2) ソフトウェアのインストール制限

(3) 情報システムの開発
（方針、構築の原則、開発環境、試験）

(4) 供給者関係
（方針、サプライチェーン）

(5) 情報セキュリティインシデント
（事象の評価、文書化した手順）

(6) 情報処理施設の可用性

ステップ1：ギャップ分析

JTC1/SC27 N13143 – Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002 –
（JIPDEC ホームページ参照：
http://www.isms.jipdec.or.jp/ikou/27001_2013/ISO_IEC_27001_TransitionMaps.html）

本文

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
4.1	組織及びその状況の理解	8.3	予防処置
4.2 a)	利害関係者のニーズ及び期待の理解		新規
⋮	⋮	⋮	⋮
10.2	継続的改善	4.2.4 a) b) d)	ISMSの維持及び改善
		5.2.1 f)	経営資源の提供
		8.1	継続的改善

今回追加された要求事項

＋ ISO/IEC 27001：2005から削除された要求事項

ISO/IEC 27001管理策

ISO/IEC 27002:2005	ISO/IEC 27002:2013	ISO/IEC 27002:2013	ISO/IEC 27002:2005
5.セキュリティ基本方針		5.情報セキュリティのための方針群	
5.1 情報セキュリティ基本方針	5.1 情報セキュリティのための経営陣の方向性	5.1 情報セキュリティのための経営陣の方向性	5.1 情報セキュリティ基本方針
5.1.1 情報セキュリティ基本方針文書	5.1.1 情報セキュリティのための方針群		
		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	新規
6.1.2 情報セキュリティの調整	削除		

今回削除された管理策

今回新たに追加された管理策

ステップ1：ギャップ分析

管理策の新旧対比表

2013年版	2005年版
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	A.6.1.3　情報セキュリティ責任の割当て A.8.1.1　役割及び責任
A.6.1.2　職務の分離	A.10.1.3　職務の分割
A.6.1.3　関係当局との連絡	A.6.1.6　関係当局との連絡
A.6.1.4　専門組織との連絡	A.6.1.7　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	（新設）
A.6.2　モバイル機器及びテレワーキング	（A.11.7 モバイルコンピューティング及びテレワーキング）
A.6.2.1　モバイル機器の方針	A.11.7.1　モバイルのコンピューティング及び通信
A.6.2.2　テレワーキング	A.11.7.2　テレワーキング
⋮	⋮

ステップ2：組織の状況／適用範囲／リスク及び機会の適用

従来

事業
組織
所在地
資産
技術
→ 適用範囲

変化 ↕

他組織の事件・事故
事象の傾向
→ 予防処置

現場的視点

考え方

目的・成果を意識／広い視野で

今回見直し例

目的）ITサービスの提供／安心・安全な社会基盤
成果）CIAを維持／顧客信頼確保
事業）「ハウジングに加えホスティングサービス開始」
組織）ホスティング組織の編成
所在地）ホスティングセンターの開設
資産）顧客とのSLA情報
技術）ネットワークの増強

内外の課題

力量ある技術者確保
サイバー攻撃の増加
直下型地震の発生予測
クラウドの普及
法令の改正（派遣法、番号法等）

→ 目的／成果を意識した適用範囲かを確認

→ リスク及び機会を洗い出し

経営的視点

ステップ3：業務プロセスへの統合、マニュアル（案）の作成

移行のポイント

- ISMSの活動が日常の業務プロセスに統合されているか
- 形骸化した活動はないか
- 何のためにやっているかわからない活動はないか

- 既になくなっている資産が資産目録に登録されている
- ログをとるだけで分析していない
- 法令順守を機械的に確認
- ライセンス管理を申告だけで確認
- 事業継続テストをいつも避難訓練だけで済ませている
- 役割分担と承認（確認しないで判を押す）
- マトリックス／最上位のマニュアル（審査のためだけに作成し、内容のチェックがされていない）
- 資産管理責任者（取りあえず部門長）
- 目標が組織の目的とかい離

ステップ3：業務プロセスへの統合、マニュアル（案）の作成

審査のためだけの文書は作成しない

2. 規格が要求する文書化した情報の確認

従来の「文書」に相当	従来の「記録」に相当
4.3　ISMSの適用範囲	7.2 力量の証拠
5.2　情報セキュリティ方針	8.1 プロセスが計画通り実施されたことの証拠
6.1.2　情報セキュリティリスクアセスメントのプロセス	8.2 情報セキュリティリスクアセスメントの結果
6.1.3　情報セキュリティリスク対応のプロセス	8.3 情報セキュリティリスク対応の結果
d) 適用宣言書	9.1 監視及び測定した結果の証拠
6.2　情報セキュリティ目的	9.2 監査プログラムの実施及び監査結果の証拠
	9.3 マネジメントレビューの結果の証拠
	10.1 不適合の処置/是正処置の結果の証拠

ステップ3：業務プロセスへの統合、マニュアル（案）の作成

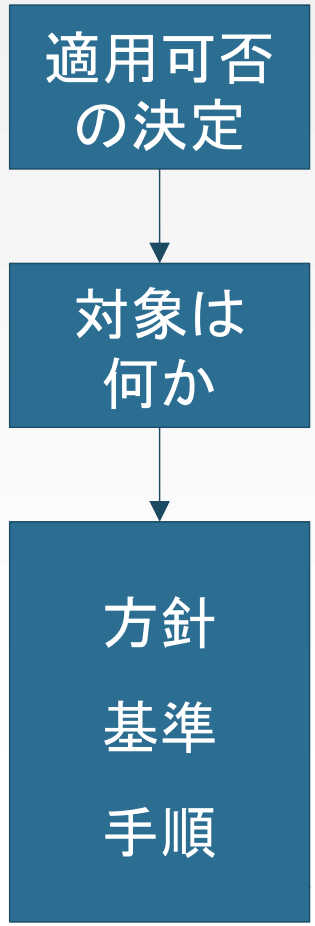
審査のためだけの文書は作成しない

2. 規格が要求する文書化した情報の確認

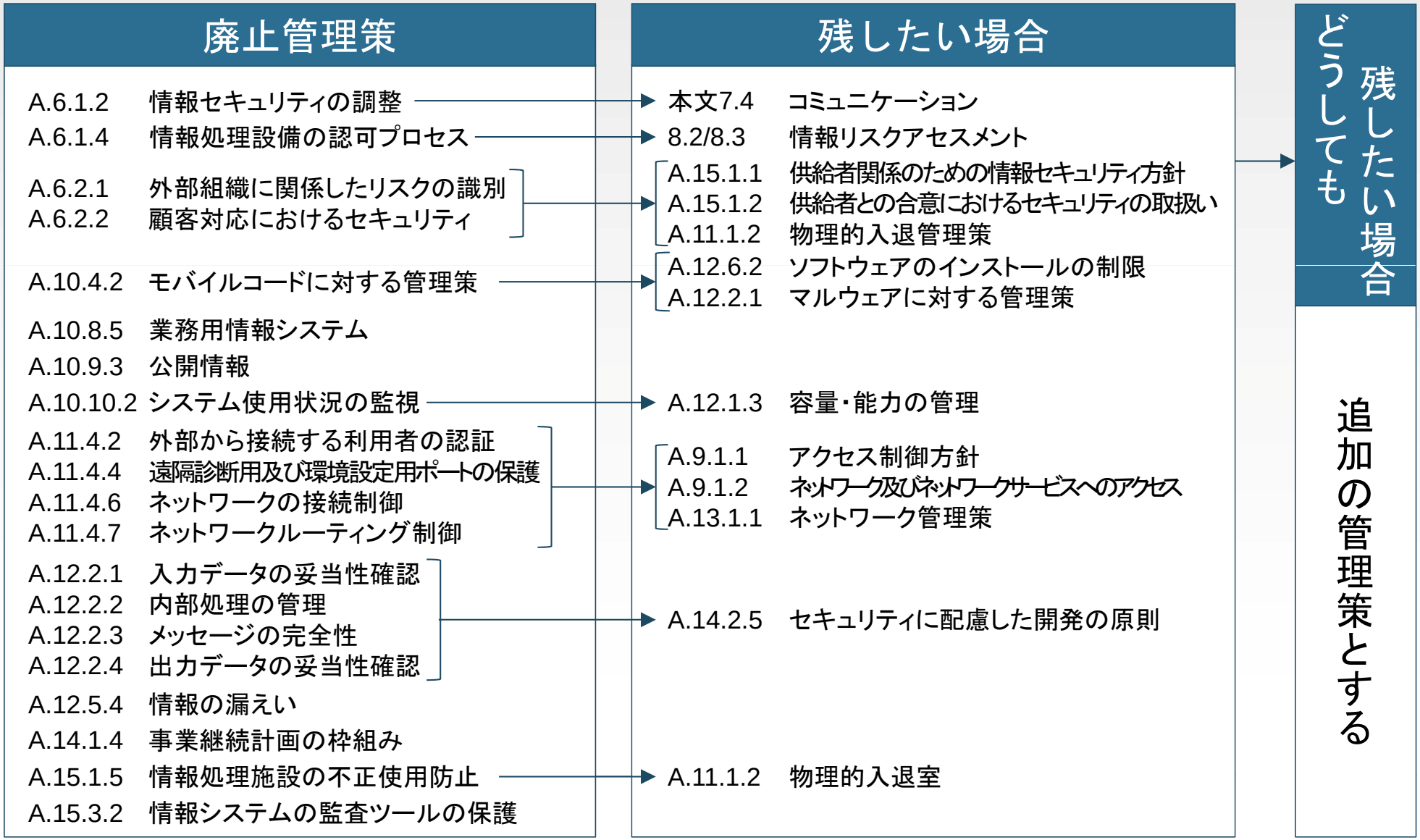
該当管理策を採用した場合必要
A.8.1.1　資産目録
A.8.1.3　情報の利用の許容範囲並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則
A.9.1.1　アクセス制御方針
A.12.1.1　操作手順
A.13.2.4　秘密保持契約又は守秘義務契約のための要求事項
A.14.2.5　セキュリティに配慮したシステムを構築するための原則　【新設】
A.15.1.1　供給者のための情報セキュリティ方針　【新設】
A.16.1.5　情報セキュリティインシデントへの対応手順　【新設】
A.17.1.2　情報セキュリティ継続のプロセス、手順及び管理策　【文書化要求が追加】
A.18.1.1　法令、規制及び契約上の要求事項

ステップ4：新適用宣言書（案）の作成
－新設管理策対応－

1. プロジェクトにおける情報セキュリティ（A.6.1.5）
2. ソフトウェアのインストール制限（A.12.6.2）
3. 情報システムの開発は適用範囲内か
   - セキュリティに配慮した開発のための方針（A.14.2.1）
   - セキュリティに配慮したシステム構築の原則（A.14.2.5）
   - セキュリティに配慮した開発環境（A.14.2.6）
   - システムセキュリティの試験（A.14.2.8）
4. 適用範囲内に供給者関係はあるか
   - 供給者関係のための情報セキュリティ方針（A.15.1.1）
   - ICTサプライチェーン（A.15.1.3）
5. 情報セキュリティインシデント管理
   - 情報セキュリティ事象の評価及び決定（A.16.1.4）
   - 情報セキュリティインシデントへの対応（A.16.1.5）
6. 情報処理施設の可用性（A.17.2.1）



ステップ4：新適用宣言書（案）の作成
－廃止管理策対応－



ステップ4：新適用宣言書（案）の作成

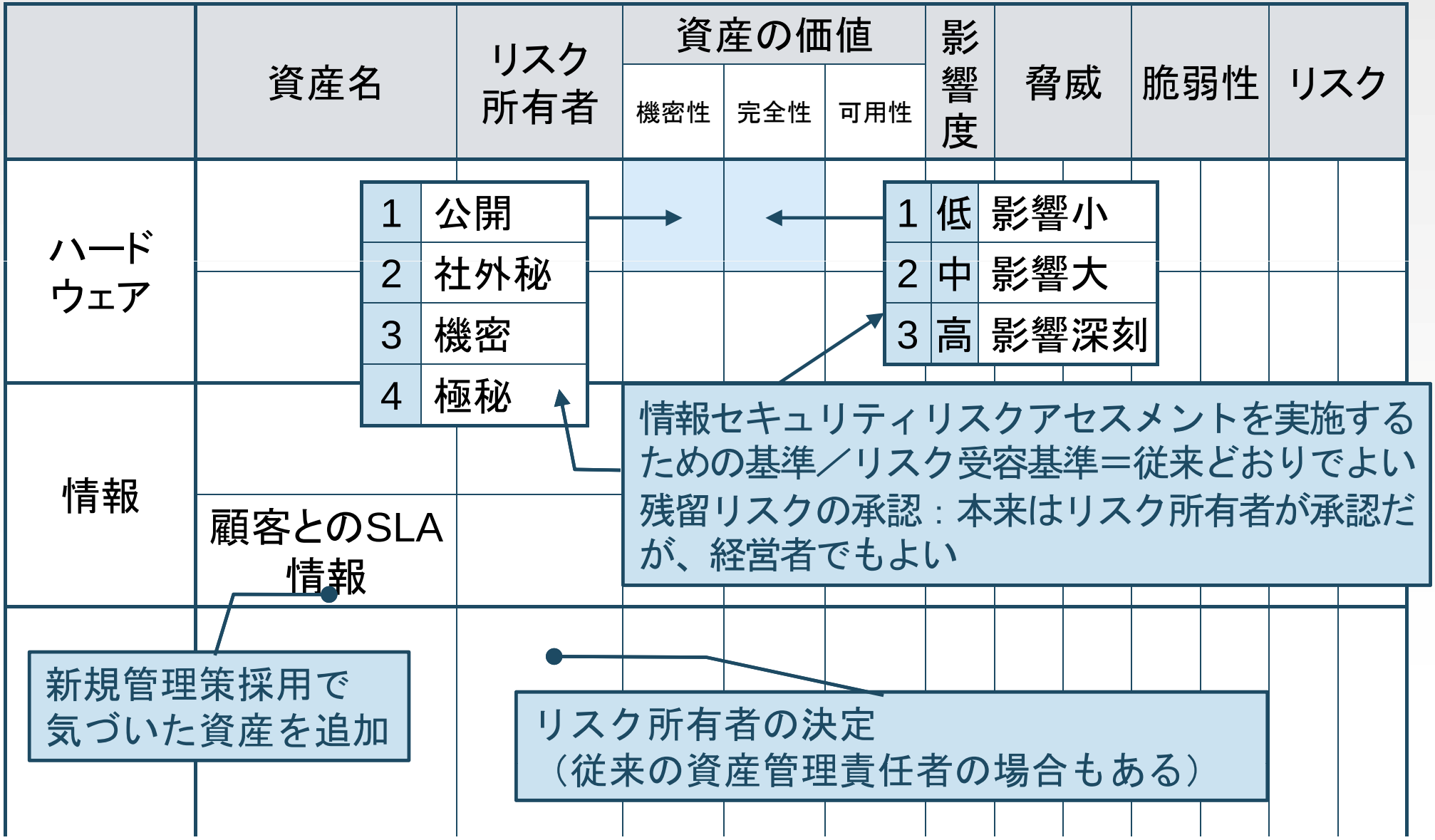
新A.6.1.1から引用 ← 対比表を参照して → 旧A.6.1.3から引用

項番	管理目的／管理策	目的／要求事項	採用可否	採用理由	備考
A.6.1	内部組織				
A.6.1.1	情報セキュリティ責任の割当て	すべての情報セキュリティ責任を明確に定めなければならない	○	ISMSの実施、運用統制のため	職務分掌にて規定
⋮	⋮	⋮	⋮	⋮	⋮
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	プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては情報セキュリティに取り組まなければならない	○	プロジェクトのセキュリティ確保のため	プロジェクト計画書にプロジェクトとして取り組むセキュリティ対応を記載
⋮	⋮	⋮	⋮	⋮	
A.19　個人情報の保護					
A.19.1	取得、利用及び提供に関する原則				
A.19.1.1	利用目的の特定	事業者は、個人情報を取得するに当たっては、その利用目的をできる限り特定し、その目的の達成に必要な限度において行わなければならない	○	個人情報保護法遵守のため	文書にて利用目的を明示して入手
⋮	⋮	⋮	⋮	⋮	⋮

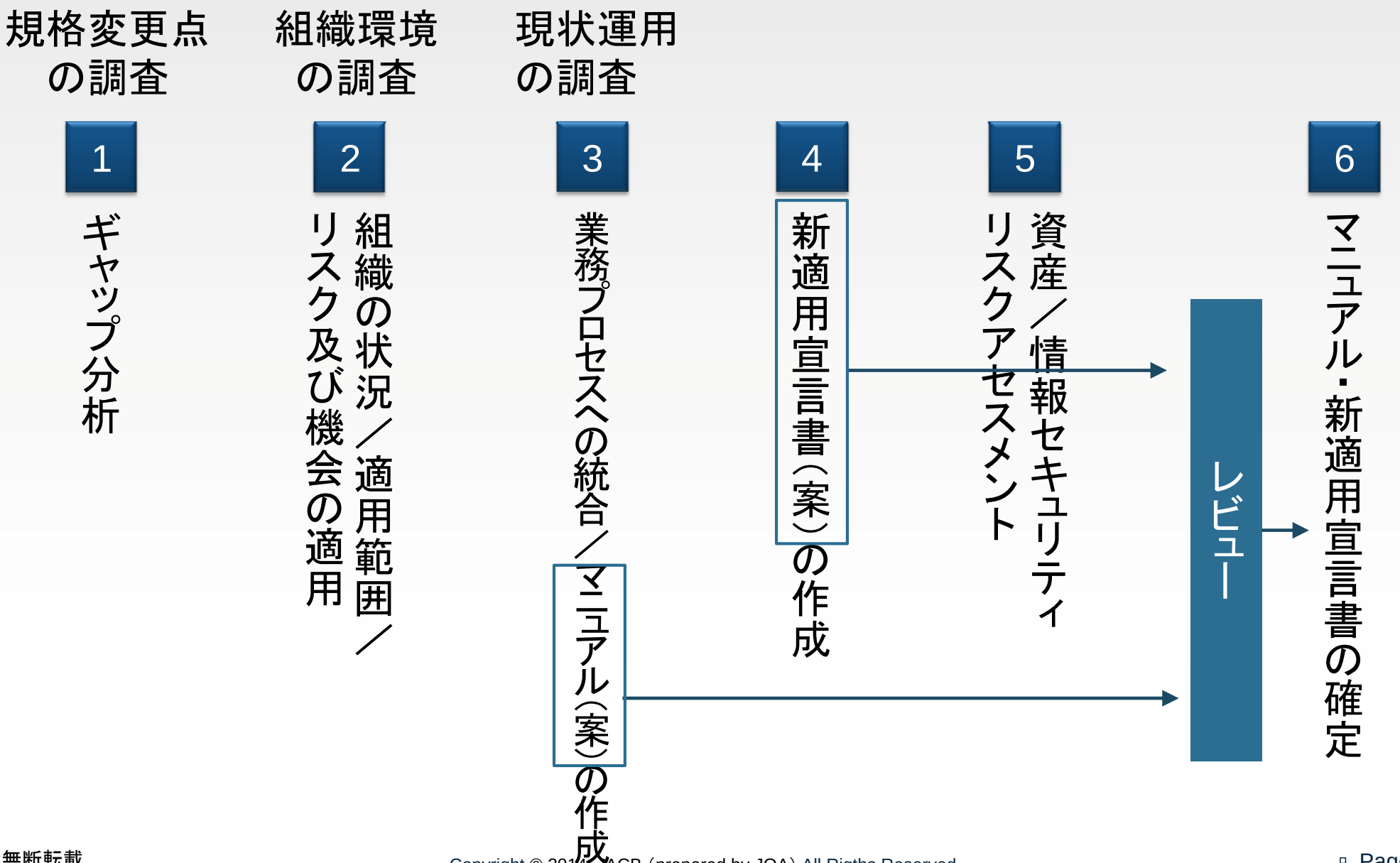
新規に作成

追加の管理策

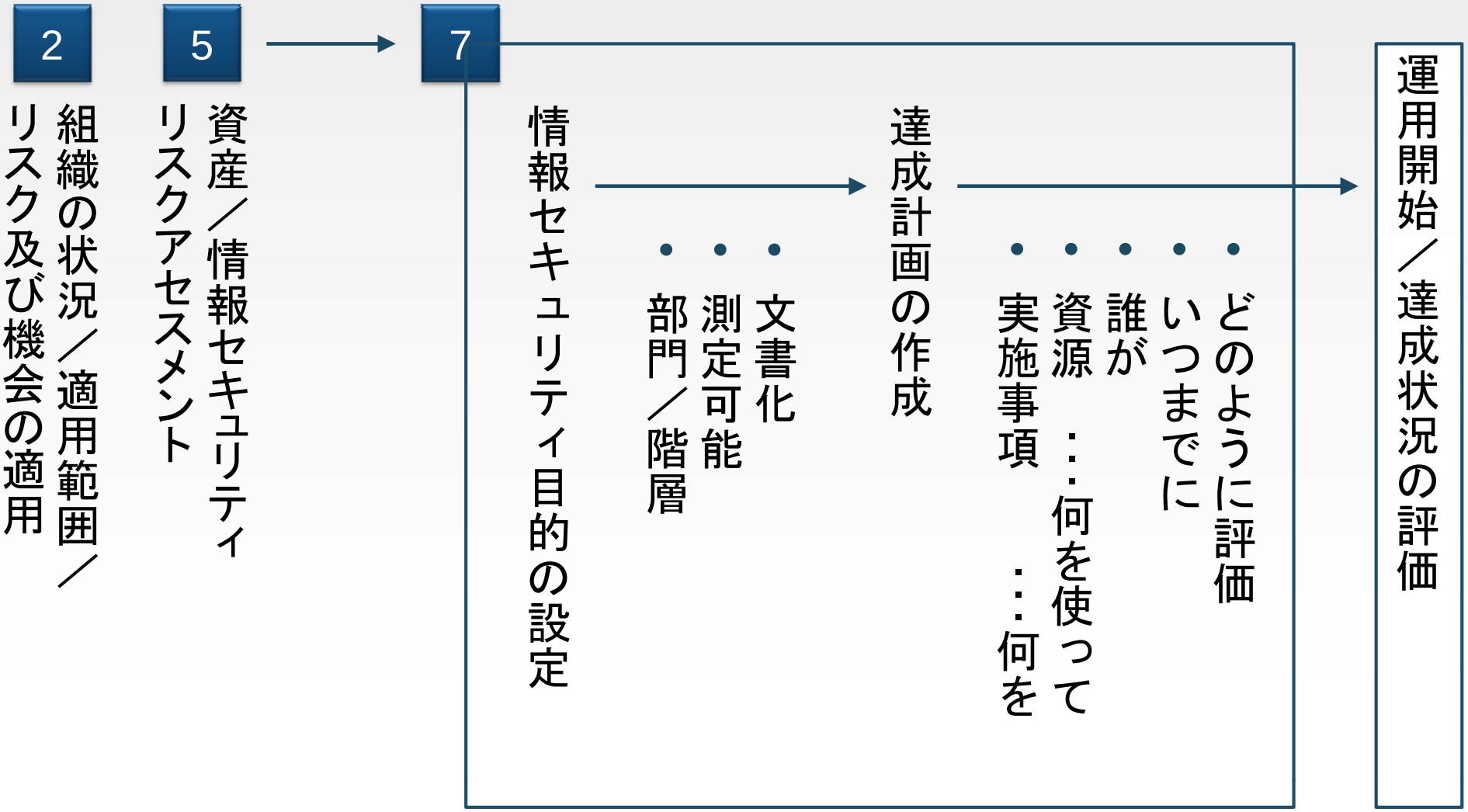
ステップ5：資産／情報セキュリティリスクアセスメント



ステップ6：マニュアル・新適用宣言書の確定



ステップ7：情報セキュリティ目的と計画策定



ステップ8:教育の実施
ステップ9:2013年版 運用開始

情報セキュリティ委員への教育

- 資産の洗い出しとリスク分析
- 情報セキュリティ目的と達成度報告
- 管理策の変更

一般社員への教育

- 情報セキュリティ目的の周知、徹底
- 新規要求事項、新設管理策と順守事項
  1）プロジェクトメンバーは計画書に記載のセキュリティ手順の順守
  2）フリーソフトを含むソフトウェアインストールルールの順守
  3）情報セキュリティインシデントへの対応手順の順守
- 改訂したマニュアルの説明

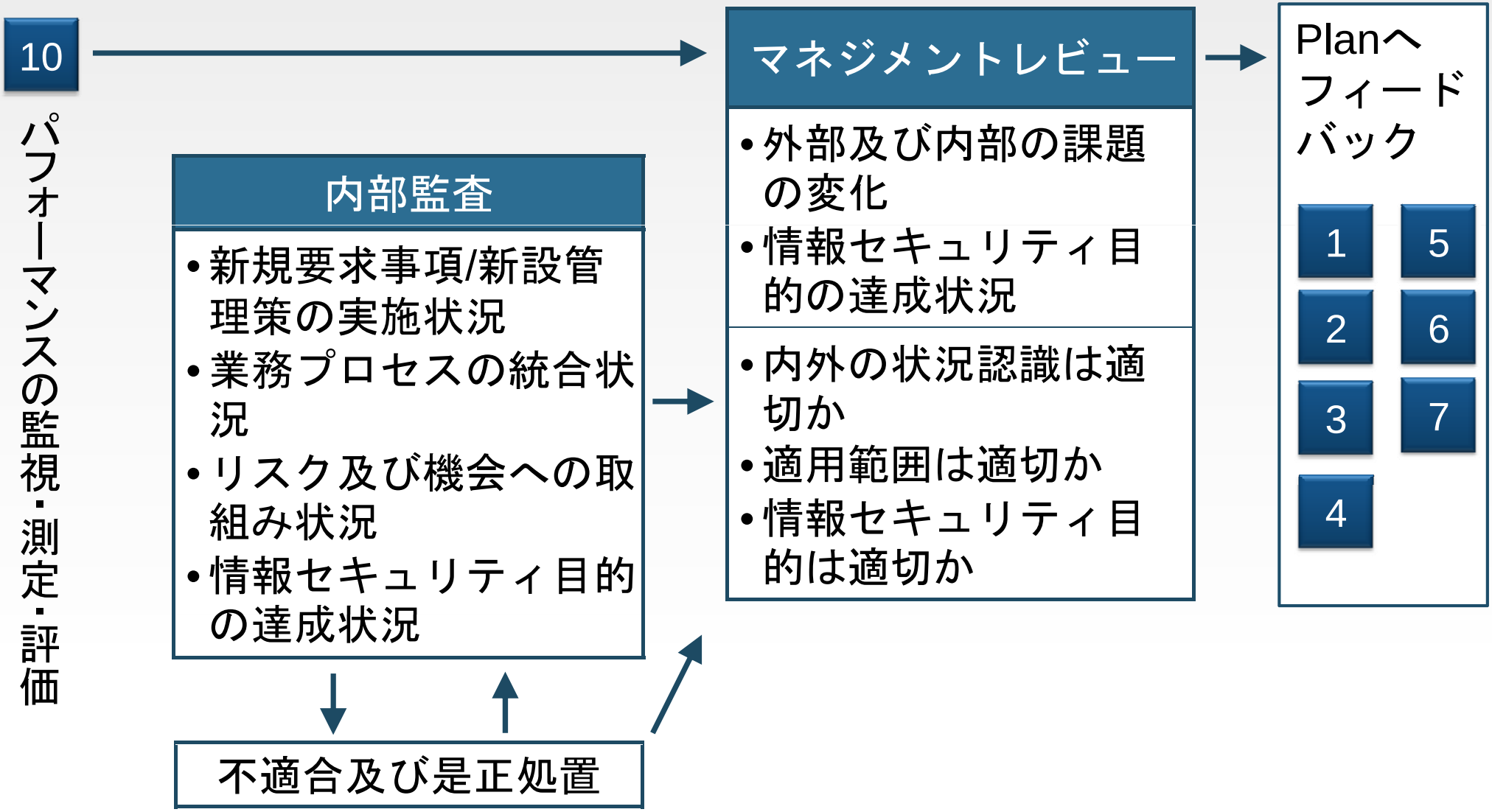
➡ 運用開始

ステップ10：パフォーマンスの監視・測定・評価

変更点を中心に、パフォーマンス及びISMSの有効性を評価

監視測定対象			評価方法	監視・測定の時期	実施者	分析・評価	
						時期	実施者
情報セキュリティ目的（目標）			達成率による評価				
リスク及び機会に対処する活動			6.1で定めた有効性評価方法				
何を測定するかは、成果、課題、リスクを考慮して選択							
新規に必要となる項目							
管理策の有効性	A.7.2.2	教育訓練	試験の点数	整理して記載			
	A.13.2.3	電子メッセージ送信	誤送信の件数				
	A.6.1.5	プロジェクトにおける情報セキュリティ	新規管理策				
	A.12.6.2	ソフトウェアのインストール制限					

ステップ11：内部監査／マネジメントレビュー



ステップ12：移行審査の実施

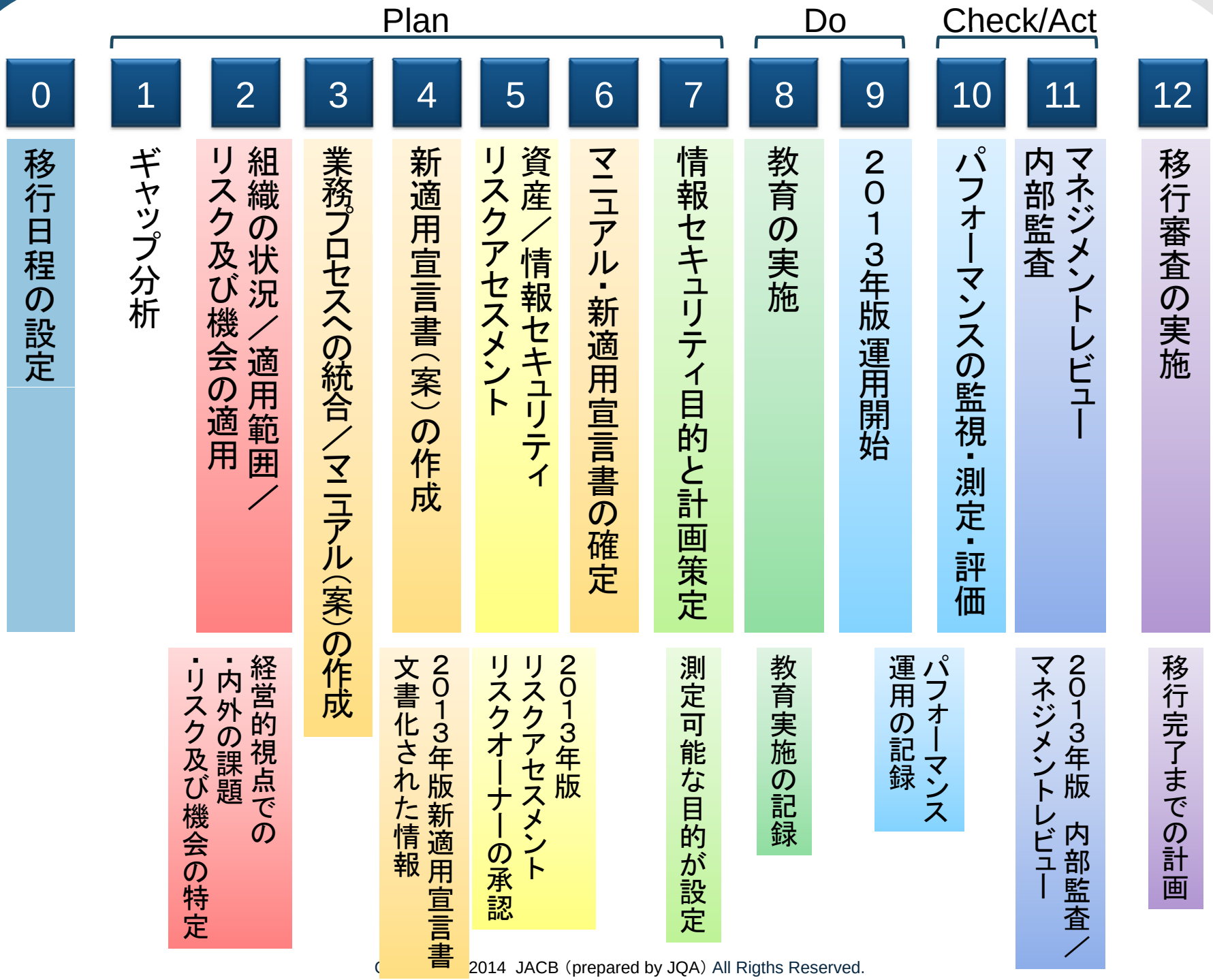
移行が可能となる条件

- 新適用宣言書が作成されている
- 2013年版での運用実績があることが基本 ＊
- 内部監査実施済み（2013年版での運用に基づく）
- マネジメントレビュー実施済み（2013年版での運用に基づく）

⇒ 基本的に審査前に確認

＊ 運用実績が不十分なものについては、
マイナー不適合（JIS Q 17021：2011 9.1.15 c））
の可能性があります

移行審査のポイント



ご清聴ありがとうございました。