SAMAC
一般社団法人 IT資産管理評価認定協会

IT資産管理プロセスのJIS化について

ISO/IEC JTC1 SC7/WG21
主査　高橋快昇
2018年6月8日

アジェンダ

- 国際標準化の動向
- なぜプロセスの標準化なのか？
- JIS 0164-1 ITAMシステム 要求事項

国際標準化の動向

IT資産管理国際規格（ISO/IEC 19770）の動向

ISO/IEC 19770-X シリーズ（ITAMの規格群）

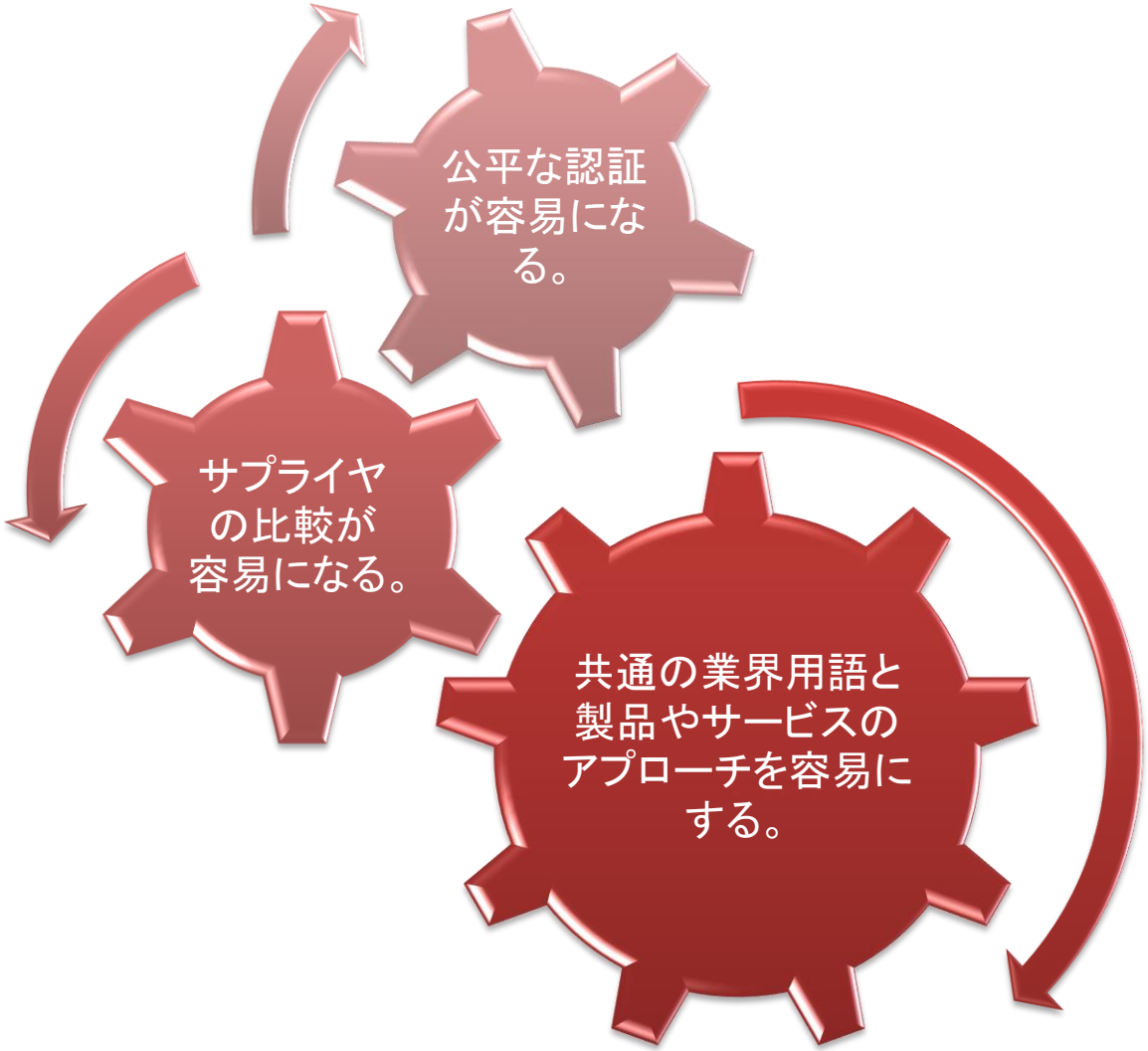
概要	19770-5:2015（第2版） 概要及び用語	第3版企画中　JIS X 0164-5 開発中
プロセス	19770-1:2017（第３版）ITAMシステム要求事項	JIS X 0164-1
	19770-8: 19770シリーズと業界標準のマッピング作成のガイドライン	DIS投票中
	19770-10: ITAMシステムガイドライン	
	19770-11: ITAMシステムの監査と認証を行う機関への要求事項	CD準備中
情報構造（タグ）	19770-2:2015（第2版）ソフトウェア識別タグ	第3版を企画中　NWIP　JIS X 0164-2
	19770-3:2016（第1版）権利スキーマ	JIS X 0164-3
	19770-4:2017（第1版）資源利用状況測定	JIS X 0164-4
	19770-6: ハードウェア識別	
	19770-7: インベントリスキーマ	

凡例: 出版済　開発中　企画中

凡例　DIS:国際規格原案、CD:委員会原案

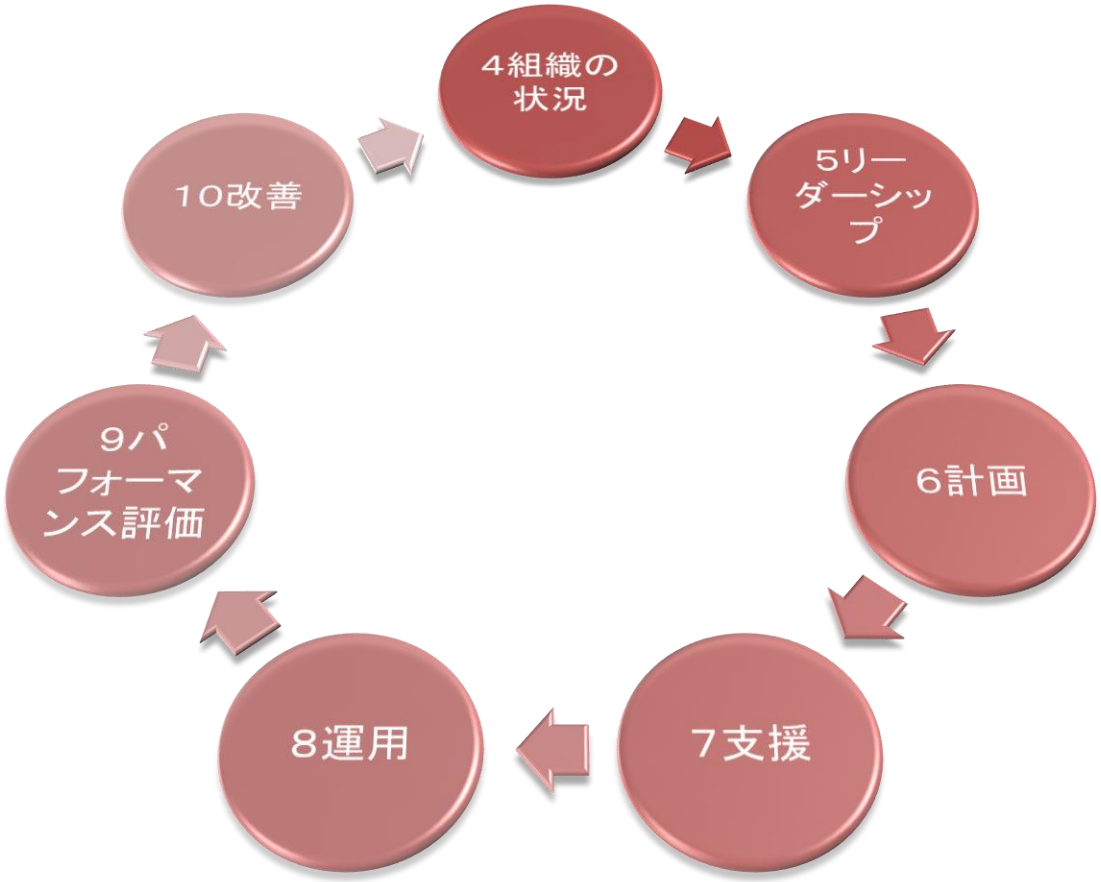
なぜプロセスの標準化なのか？

なぜ、プロセス標準が必要なのか？



ISO 新マネージメントシステム（MSS ）の PDCA

ISOが専門業務用指針の附属書SLで提唱するマネージメントシステム



ISO新マネージメントシステムの標準テキスト(付属書SL)

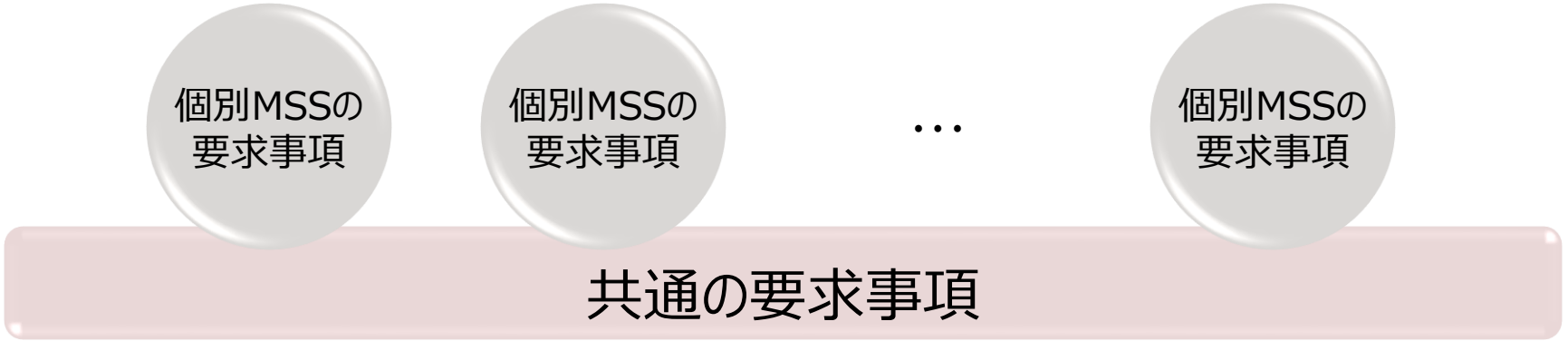
目次	
序文	**7. 支援**
1. 適用範囲	7.1 資源
2. 引用規格	7.2 力量
3. 用語及び定義	7.3 認識
4. 組織の状況	7.4 コミュニケーション
4.1 組織及びその状況の理解	7.5 文書化した情報
4.2 利害関係者のニーズ及び期待の理解	7.5.1 一般
4.3 XXX マネージメントシステムの適用範囲の決定	7.5.2 作成及び更新
4.4 XXX マネージメントシステム	7.5.3 文書化した情報の管理
5. リーダーシップ	**8. 運用**
5.1 リーダーシップ及びコミットメント	8.1 運用の計画及び管理
5.2 方針	**9. パフォーマンス評価**
5.3 組織の役割、責任及び権限	9.1 監視、測定、分析及び評価
6. 計画	9.2 内部監査
6.1 リスク及び機会への取り組み	9.3 マネジメントレビュー
6.2 XXX 目的及びそれを達成するための計画策定	**10. 改善**
	10.1 不適合及び是正処置
	10.2 継続的改善

SAMAC
一般社団法人IT資産管理評価認定協会

ISOの新MSSの狙い

管理システムの要求事項を共通化（ISO/IEC 専門業務指針第 1 部附属書SL）

- マネジメントシステム間の整合性向上
- 共通の用語定義
- 要求項目の共通テキスト化



■ISO 22301:2012（事業継続マネジメントシステム）
■ISO 39001:2012（道路交通安全マネジメントシステム）
■ISO/IEC 27001:2013（情報セキュリティシステム）
■ISO 55001:2014（資産管理システム）
■ISO 9001:2015（品質マネジメントシステム）
■ISO 14001 :2015（環境マネジメントシステム）
■ISO/IEC 19770-1:2017（IT資産マネジメントシステム）
■ISO/IEC 20000-1:????（サービスマネジメントシステム）

JIS 0164-1 ITAMシステム 要求事項 （ISO/IEC 19770-1:2017）

ISO/IEC19770-1:3rdの目次（2017）

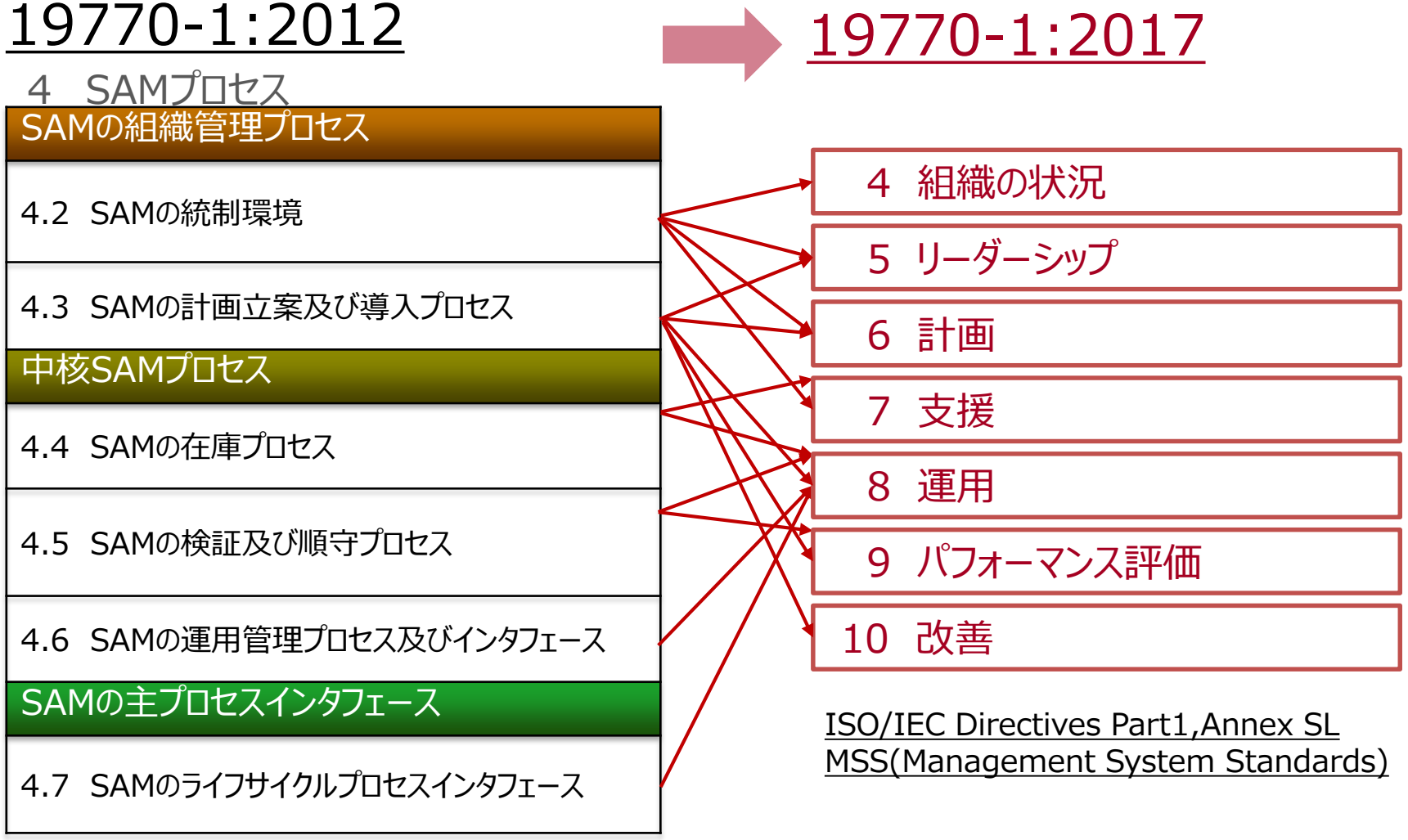
目次

序文
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
　4.2 利害関係者のニーズ及び期待の理解
　4.3 IT資産 マネージメントシステムの適用範囲の決定
　4.4 IT資産 マネージメントシステム
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
　5.2 方針
　5.3 組織の役割、責任及び権限
6. 計画
　6.1 リスク及び機会への取り組み
　　6.1.1 一般
　　6.1.2 IT資産リスク評価
　　6.1.3 IT資産リスク対応
　6.2 IT資産管理 目的及びそれを達成するための計画策定
　　6.2.1 IT資産管理の段階仕様
　　6.2.2 関係する段階のIT資産管理目的
　　6.2.3 全IT資産管理の目的
　　6.2.4 IT資産管理目的を達成するための計画策定
7. 支援
　7.1 資源
　7.2 力量
　7.3 認識
　7.4 コミュニケーション
　7.5 情報要求事項
　7.6 文書化した情報
　　7.6.1 一般
　　7.6.2 所有権及び責任のトレーサビリティ
　　7.6.3 許可及び違反の監査証跡
　　7.6.4 作成及び更新
　　7.6.5 文書化した情報の管理
8. 運用
　8.1 運用の計画及び管理
　8.2 変更の管理
　8.3 中核データの管理
　8.4 ライセンス管理
　8.5 セキュリティ管理
　8.6 他の管理
　8.7 アウトソーシングとサービス
　8.8 組織と個人の混在責任
9. パフォーマンス評価
　9.1 監視、測定、分析及び評価
　9.2 内部監査
　9.3 マネジメントレビュー
10. 改善
　10.1 不適合及び是正処置
　10.2 予防処置
　10.3 継続的改善
附属書A（規定）IT資産管理の段階
附属書B（規定）IT資産管理のプロセス領域
附属書C（参考）IT資産の特徴
附属書D（参考）ISO 55001からの変更

凡例　青地:ISO、黒字:ISO55001:2014　赤字:ISO/IEC 19770で追加された箇条

SAMAC
一般社団法人 IT資産管理評価認定協会

19770-1:2012 （第2版からの大幅な変更）



4．組織の状況

MSSの基本：組織内外の課題，ニーズ及び期待，適用範囲，ITAMシステム構築責任

4.1 組織及びその状況の理解

- ITAMシステムに影響を及ぼす内外の課題をリスク管理の観点で明確化

4.2 利害関係者のニーズ及び期待の理解

- 利害関係者を明確にし，要求事項，意思決定のための規準，報告事項の決定

4.3 IT資産管理システムの適用範囲の決定

- 上記及び他管理システムとの相互作用を考慮したITAMシステムの適用範囲の決定と文書化

4.4 IT資産管理システム

- この規格の要求事項に従ったITAMシステムのPDCAを実践すること

5．リーダーシップ

4 組織の状況
5 リーダーシップ
6 計画
7 支援
8 運用
9 パフォーマンス評価
10　改善

リーダーシップ及びコミットメント（方針の制定/資源の割当）の明確化

5.1 リーダーシップ及びコミットメント

- ITAMの方針が組織のものと両立すること
- ITAMの要求事項が組織の事業プロセスと統合していること
- ITAMシステムに必要な資源（人的、物理的）を割り当てること
- ITAM要求事項への適合の重要性を徹底させること
- 成果達成に向けあらゆる支援（指揮，横断的な協調，継続的改善など）をすること
- 関連する管理層への働き掛け

5.2 方針

- 組織の目的に対して適切か，目的制定の枠組みを示しているか，目指す要求事項と継続的改善のコミットを含んでいるか
- 組織的な計画、他のMSSの方針と整合していること、ITAMの規模、企業と個人の責任が適切であること、定期的な改善が行われていること
- 文書化され、組織内に伝達され、利害関係者が必要に応じて入手できること

5.3 組織の役割，責任及び権限

- ITAMの計画，実施、周知，評価/監査，報告の責任及び権限を割当てること

6．計画（続く）

4 組織の状況
5 リーダーシップ
6 計画
7 支援
8 運用
9 パフォーマンス評価
10　改善

リスク及び機会を決定し，ITAMの目的を定義し，計画を策定する

4.1組織及びその状況の理解

4.2利害関係者のニーズ及び期待の理解

課題

要求事項

視点（～するために）	取組む必要があるﾘｽｸ/機会
意図した成果の達成	
望ましくない影響の防止及び低減	
継続的改善を達成	

→ その取組みの　IT資産管理システムプロセスへの統合及び導入　の計画

→ その取組みの　有効性の評価　の計画

6．計画（続く）

IT資産のリスクアセスメントとリスク対応への要求事項の強化

6.1.2 IT資産リスクアセスメント

（リスク基準の設定と一貫性の保証）

リスクの特定
- ✓ 機密性，完全性及び可用性の喪失に伴うリスク
- ✓ 事業継続リスク
- ✓ 法律及び規制、ﾗｲｾﾝｽを含む契約遵守に関連するリスク

リスクの分析
- ✓ 起こり得る結果についてアセスメント
- ✓ 起こりやすさについてのアセスメント
- ✓ リスクレベルの決定

リスクの評価
- ✓ 基準との比較
- ✓ リスク対応のための優先順位付け

文書化

6.1.3 IT資産リスク対応

リスクアセスメントの結果

リスク対応の選択肢を選定

実施に必要な全ての管理策を決定

IT資産リスク対応計画を策定

IT資産所有者の承認

文書化

6．計画（続き）「運用のプロセス定義」

ITAMで要求される管理の保証の程度に応じて，適切な運用プロセスを決定しなければならない。

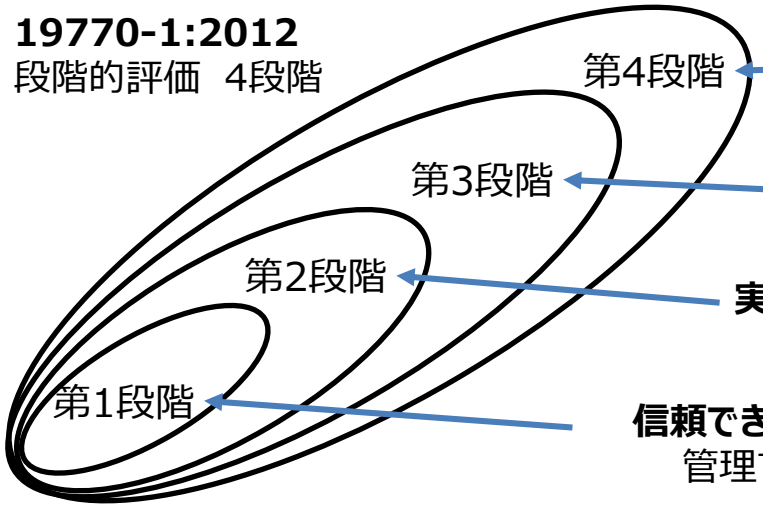
付属書Aで規定

※ 段階は認証（自己認証または独立系認証）の目的のために定義されている

凡例: ? ? 段階

参考:第2版から変更した段階”Tier“の考え方

19770-1:2012
段階的評価　4段階



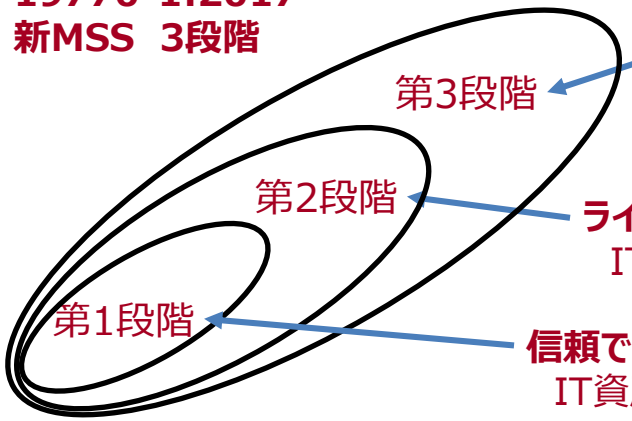
ISO/IEC SAMへの完全適合
組織で最適な戦略的SAMの達成

運用統合
効率及び有効性の改善

実用的マネジメント
マネジメント管理策の改善&直接的な便益の確保

信頼できるデータ
管理できるように手持ちのものが何かを知る

19770-1:2017
新MSS　3段階



最適化
横断的に機能管理領域を集約することにより一層の効率と効果を達成している段階

ライフサイクルの統合化
IT資産のライフサイクルを通して、より一層の効率と効果を達成している段階

信頼できるデータ
IT資産を管理できる情報が正確に入手できる段階

7．支援

4 組織の状況
5 リーダーシップ
6 計画
7 支援
8 運用
9 パフォーマンス評価
10　改善

計画を実行する上で重要となる各種支援についての要求事項をまとめて明示

- ITAMの要求事項を達成する資源、要員の力量の確保と要員の認識を維持すること
- ITAMで要求されるコミュニケーションの内容、実施時期、対象者、方法を決めること
- IT資産の特殊性を考慮した情報要求事項を決定すること
  - IT資産の特殊性を考慮した契約遵守の管理要件を満たす情報が確保できること
  - 識別可能な属性及び品質要件の情報がいつどのようにして収集し、解析され、評価されるか
  - 情報の管理プロセスの明確化と導入及び維持ができること
  - 財務及び非財務データの対応付け，トレーサビリティに関する要求事項
- 文書化の要求事項
  - 作成から廃棄までの一般的な要求事項
  - 所有権と責任のトレーサビリティ及び承認の監査証跡に耐える文書化の要求事項

8．運用（続く）

ITAMの計画に必要なプロセスを計画し，実施し、かつ管理する

8.1　運用の計画及び管理
8.2　変更の管理
8.3　中核データ管理
8.4　ライセンス管理
8.5　セキュリティ管理
8.6　他のプロセス
8.7　アウトソーシングとサービス
8.8　組織と個人間の複合責任

ITAMで追加された箇条

BYODや3rdパーティの
持ち込み機器を想定

ＩＴアセットマネジメントシステム標準におけるプロセス構造

ITアセットのマネージメントシステムプロセス

ITアセットの機能的管理 プロセス領域

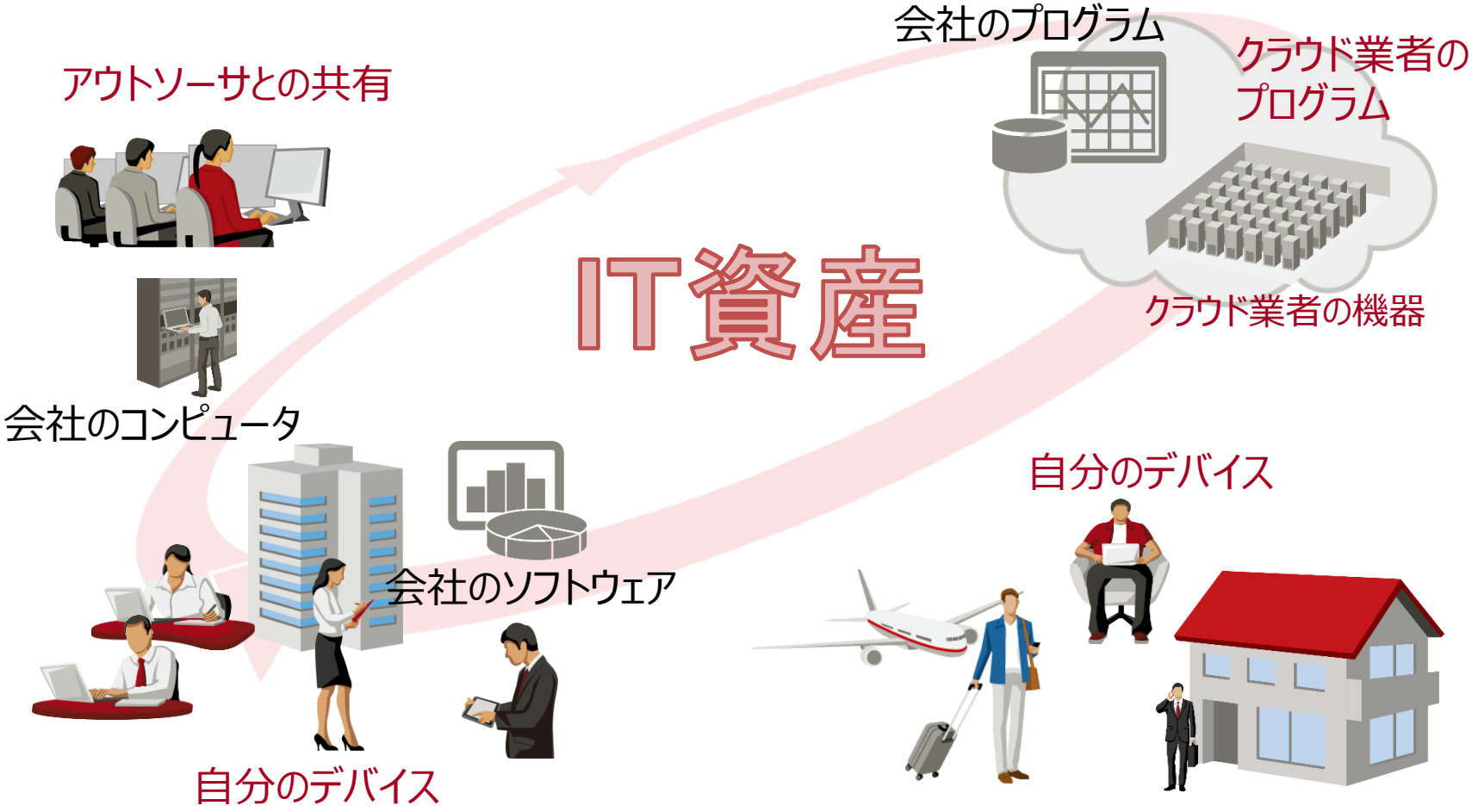
- 変更管理
- データ管理
- ライセンス管理
- セキュリティ管理
- 関係/契約管理
- 財務管理
- サービスレベル管理
- 他のリスク管理

ITアセットライフサイクル管理プロセス

- 仕様
- 調達
- 開発
- リリース
- 展開
- 運用
- 廃棄

８．運用（続き）　複合責任及びアウトソーシングの要求事項

複合責任のIT資産及びアウトソーシングが管理対象として明示された



9．パフォーマンス評価

対象の明確化と評価の実施，内部監査、マネジメントレビュー

9.1　監視，測定，分析及び評価

- 対象の明確化と監視，測定，分析及び評価の方法の決定
- 結果の文書化

9.2　内部監査

- ITAMシステムの要求事項に対する内部監査の実施
- 監査基準及び範囲，スケジュール，要員の選定，報告，文書化

9.3　マネジメントレビュー

- 決められた間隔でのITAMシステムのレビュー
- 前回までの処置、内外の課題の状況、パフォーマンス評価、継続的改善の機会の考慮と結果の文書化

１０．改善

評価に基づき、不適合の是正、予防処置を行い継続的な改善を行う

10.1　不適合及び是正措置

■ 不適合への対処、原因の明確化、是正処置の有効性のレビュー、ITAMシステムの改善及び文書化すること

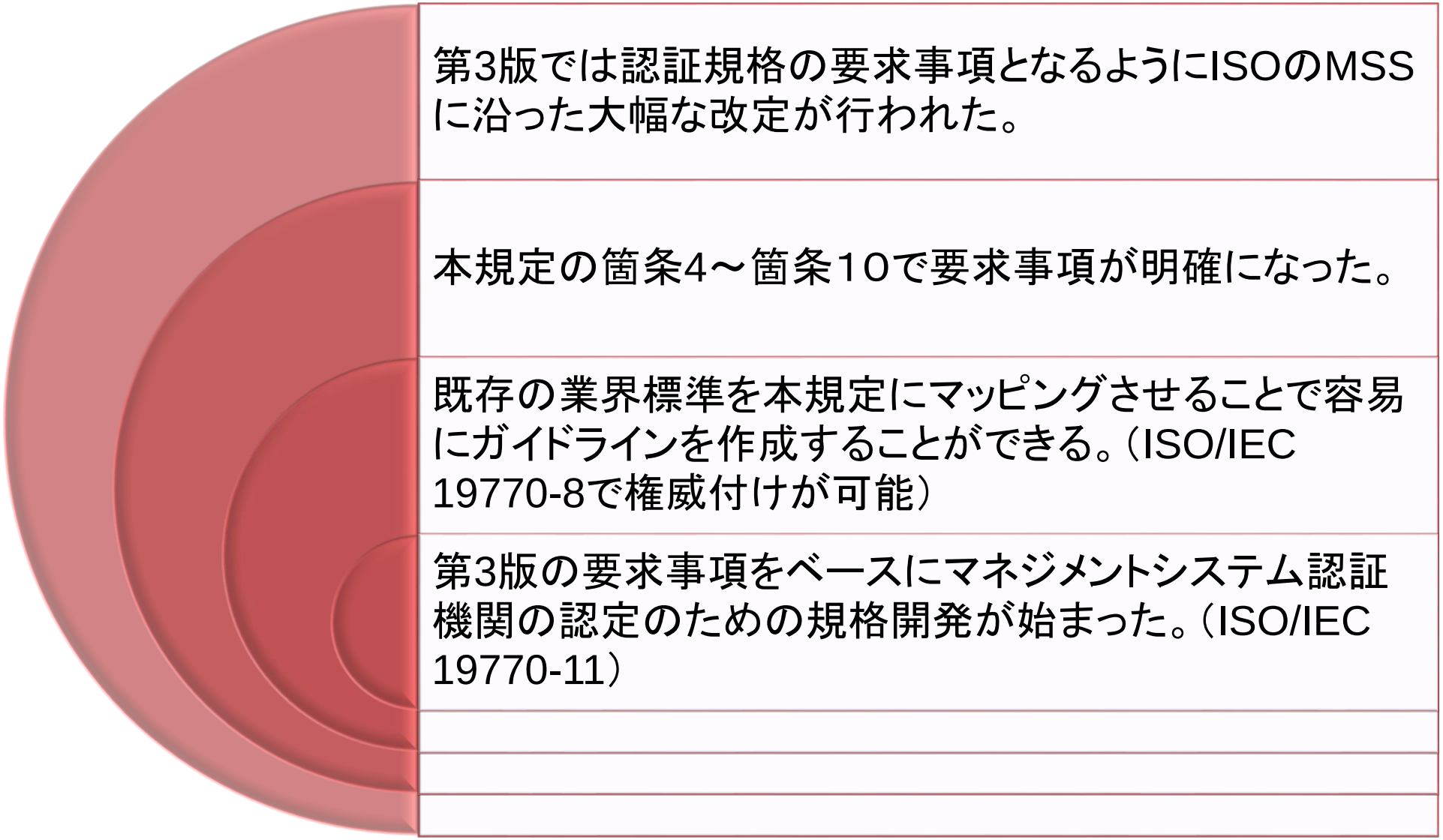
10.2　予防処置

■ 潜在的不適合への能動的対処の必要性を評価すること

10.3　継続的改善

■ ITAMとそのシステムの適切性，妥当性及び有効性を継続的に改善すること

まとめ



SAMAC
一般社団法人IT資産管理評価認定協会

一般社団法人IT資産管理評価認定協会