SAMAC
一般社団法人 IT 資産管理評価認定協会

IT資産管理の国際規格状況（ISO/IEC 19770）

ISO/IEC JTC1 SC7/WG21主査（富士通）
高橋快昇

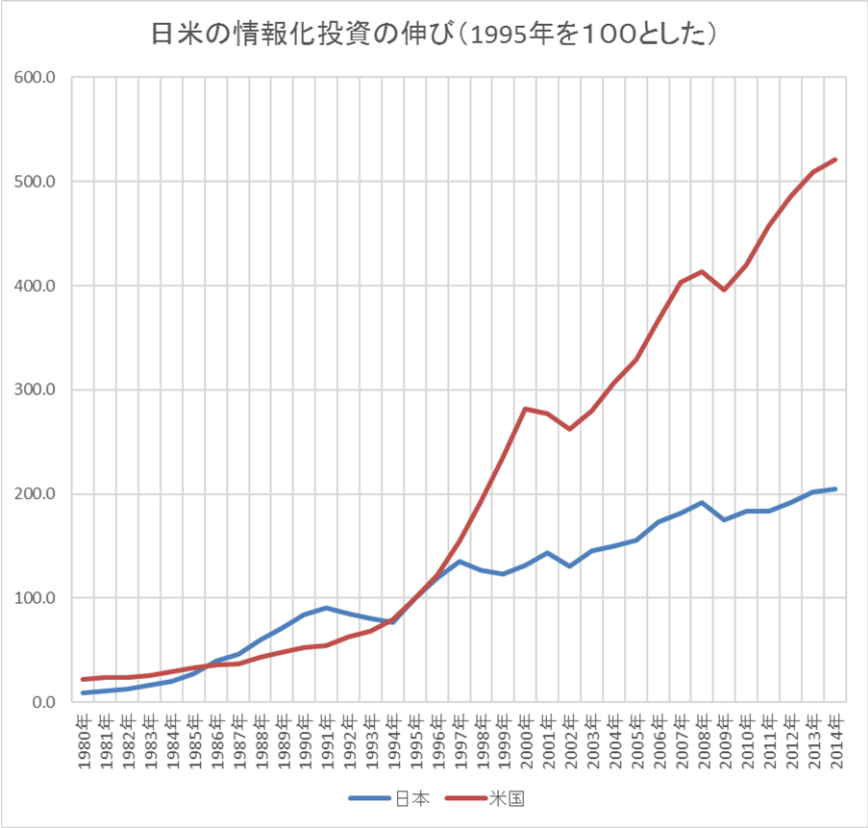
2017年6月9日

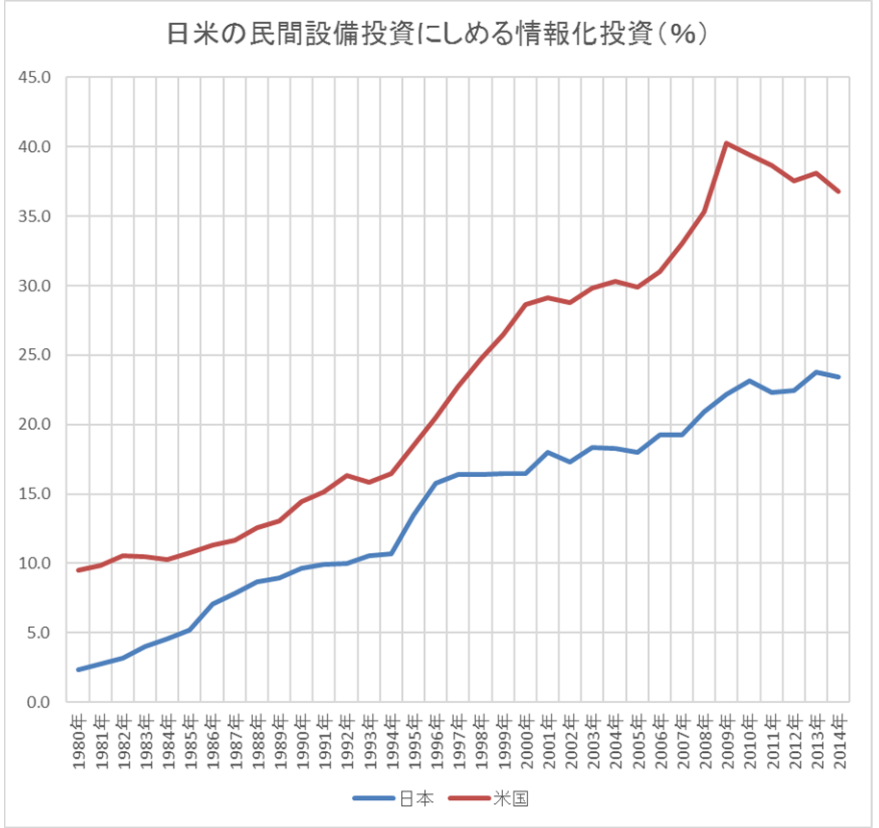
目次

- ITAM関連の国際標準化動向
- プロセスの標準化
- タグ関連の標準化

日米情報化投資の比較

情報化投資の伸び及び民間設備投資にしめる情報化投資とも低い





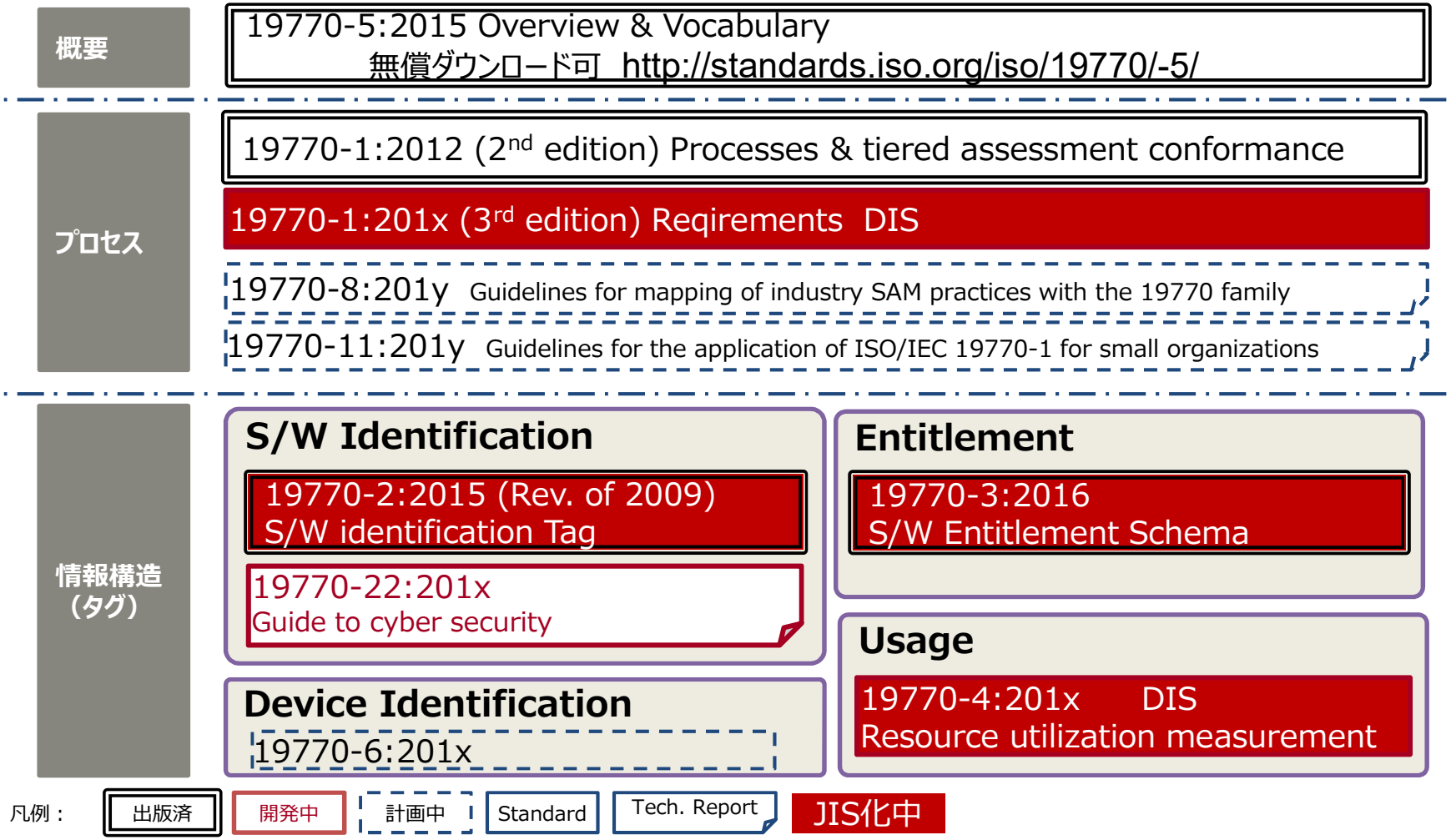
ICT の経済分析に関する調査報告書
平成28 年3 月総務省 情報通信国際戦略局情報通信政策課 情報通信経済室 より

ITAM関連の国際標準化動向

SAMAC
一般社団法人 IT 資産管理評価認定協会

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）



プロセスの標準化

SAMAC
一般社団法人 IT 資産管理評価認定協会

ISOの新しい管理システム標準（MSS）の狙い

管理システムの要求事項を共通テキスト化（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:DIS（IT資産マネジメントシステム）
- ISO/IEC 20000-1:CD（サービスマネジメントシステム）

凡例　DIS:国際規格原案、CD:委員会原案

ISO新マネージメントシステムの標準テキスト(AnnexSL)

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 XXX マネージメントシステムの適用範囲の決定

4.4 XXX 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

6.2 XXX 目的及びそれ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 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 運用の計画及び管理

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 継続的改善

ISO/IEC19770-1:3rdの目次（DIS）

目次

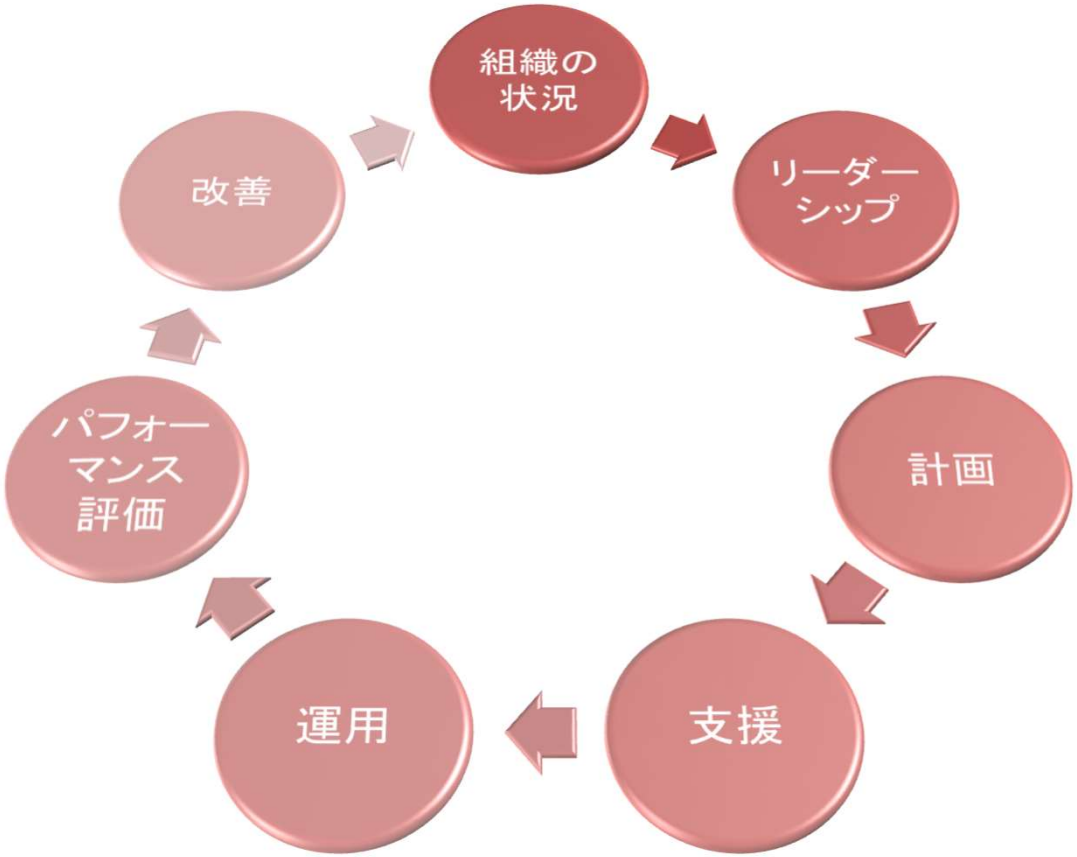
序文
1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 組織の状況
　4.1 組織及びその状況の理解
　4.2 利害関係者のニーズ及び期待の理解
　4.3 IT資産 マネージメントシステムの適用範囲の決定
　4.4 IT資産 マネージメントシステム
5. リーダーシップ
　5.1 リーダーシップ及びコミットメント
　5.2 方針
　5.3 組織の役割、責任及び権限
6. 計画
　6.1 リスク及び機会への取り組み
　　6.1.1 一般
　　6.1.2 IT資産リスク評価
　　6.1.3 IT資産リスク対応
　6.2 IT資産管理 目的及びそれを達成するための計画策定
　　6.2.1 IT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 黒字：ISO+ISO55001:2014 赤字：ISO/IEC 19770で追加された節

SAMAC
一般社団法人 IT 資産管理評価認定協会

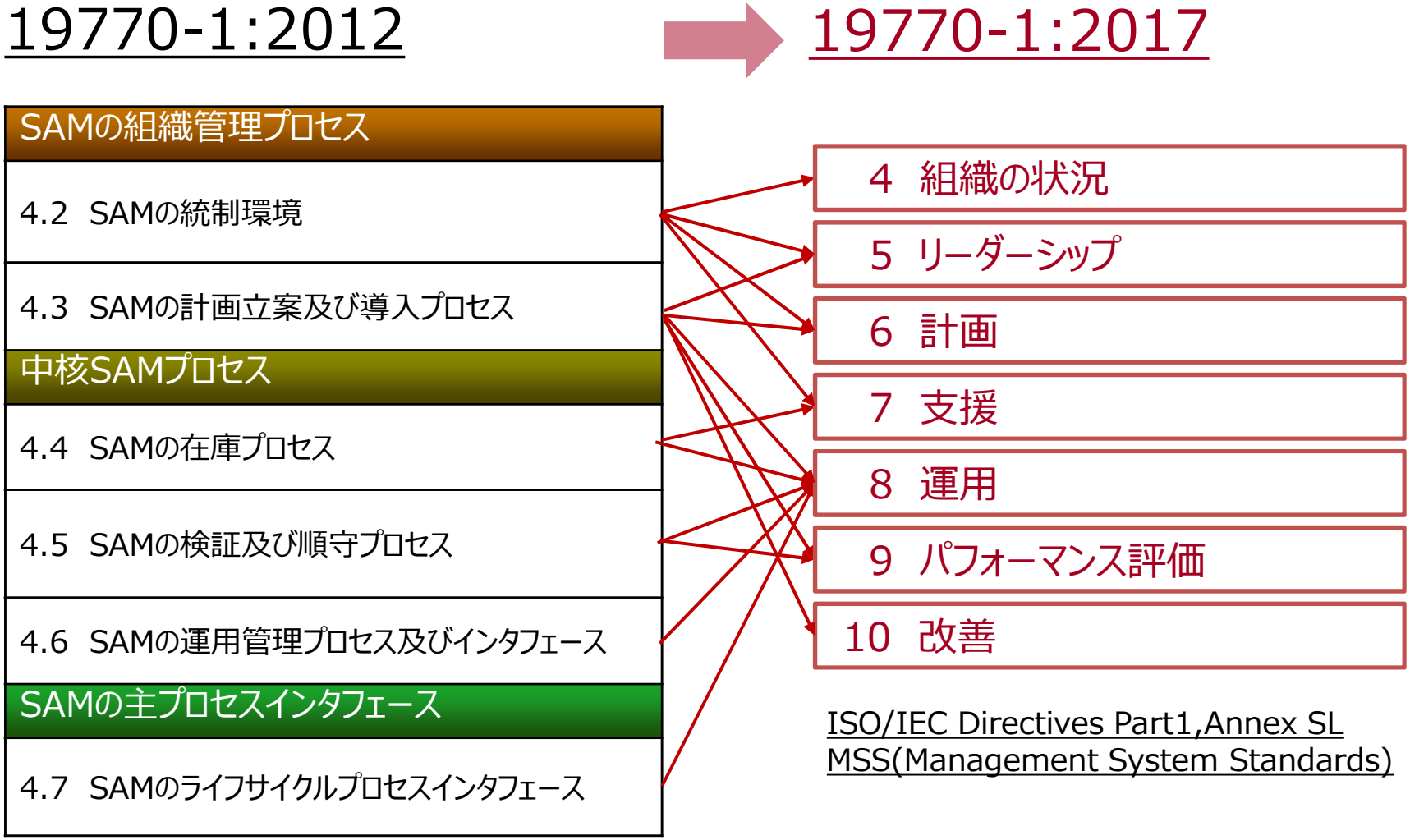
ISO 新MSS の PDCA

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



19770-1:2012 からの移行

- ISO/IEC Directives, AnnexSL(新MSS)への対応 -



4．組織の状況

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

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

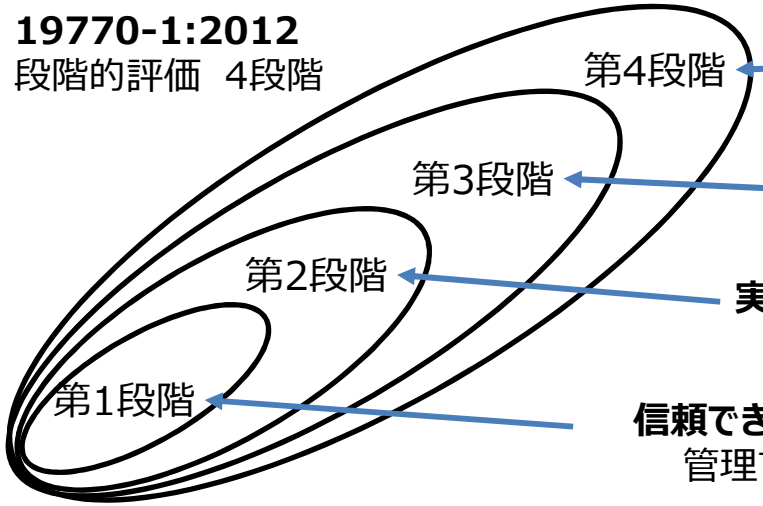
IT資産所有者の承認

文書化

6．計画（続く）「参考：認証のための段階”Tier“」

市場の実態に合わせ３つの段階に簡略化

19770-1:2012
段階的評価　4段階



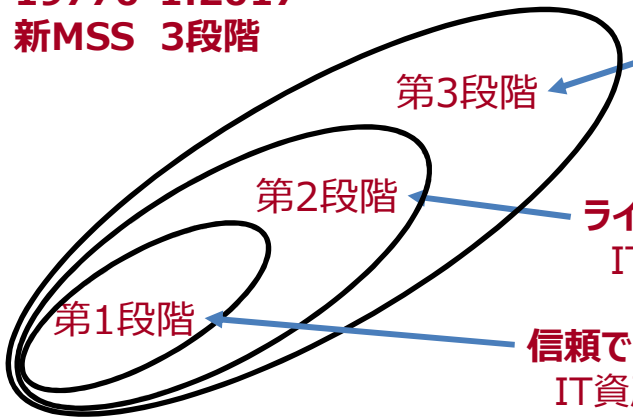
ISO/IEC SAMへの完全適合
組織で最適な戦略的SAMの達成

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

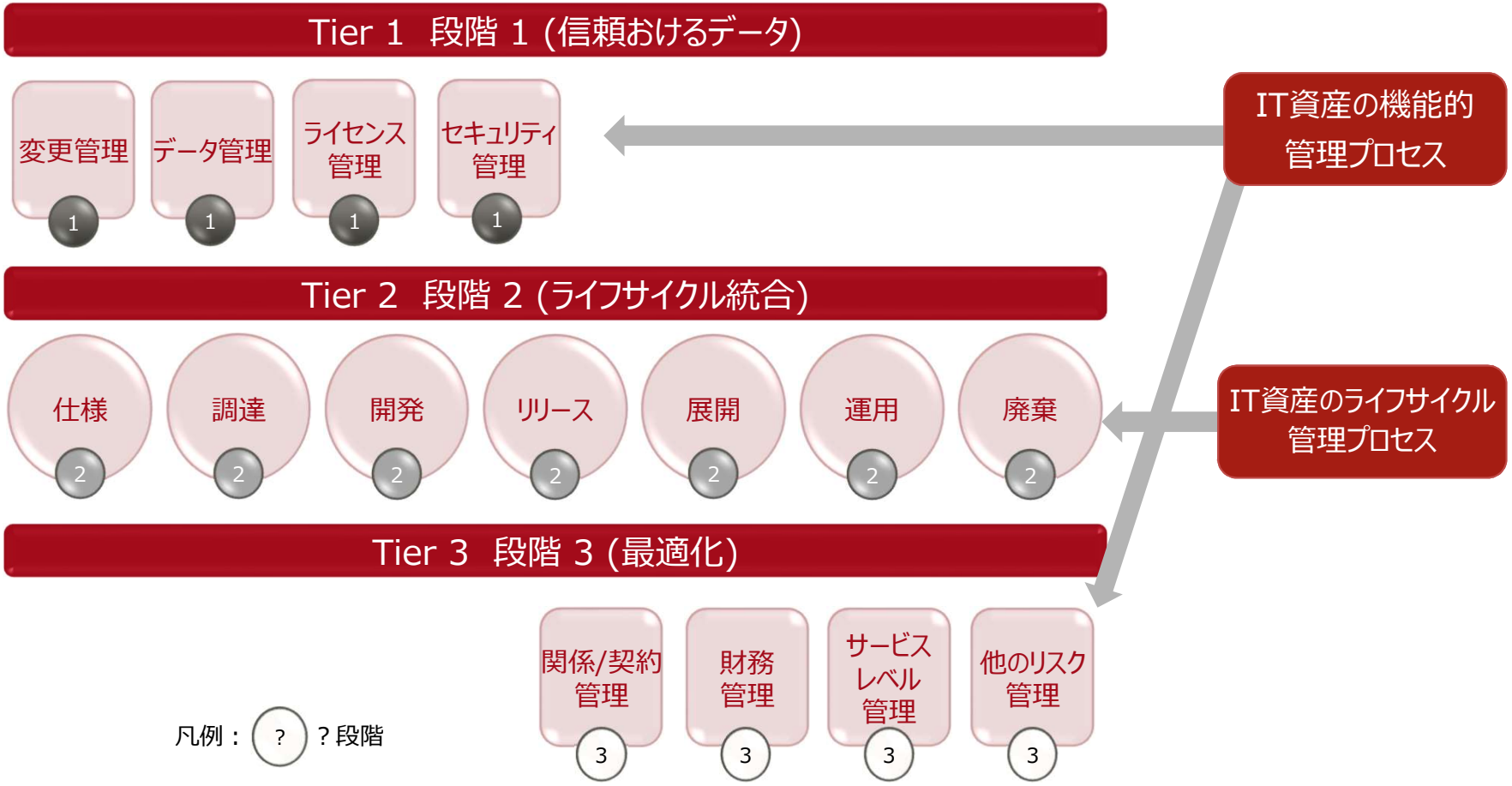
ライフサイクルの統合化
IT資産のライフサイクルを通して、より一層の効率と効果を達成している段階

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

SAMAC
一般社団法人 IT 資産管理評価認定協会

6．計画（続き）「段階毎のプロセス領域」

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



SAMAC
一般社団法人 IT 資産管理評価認定協会

7．支援

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

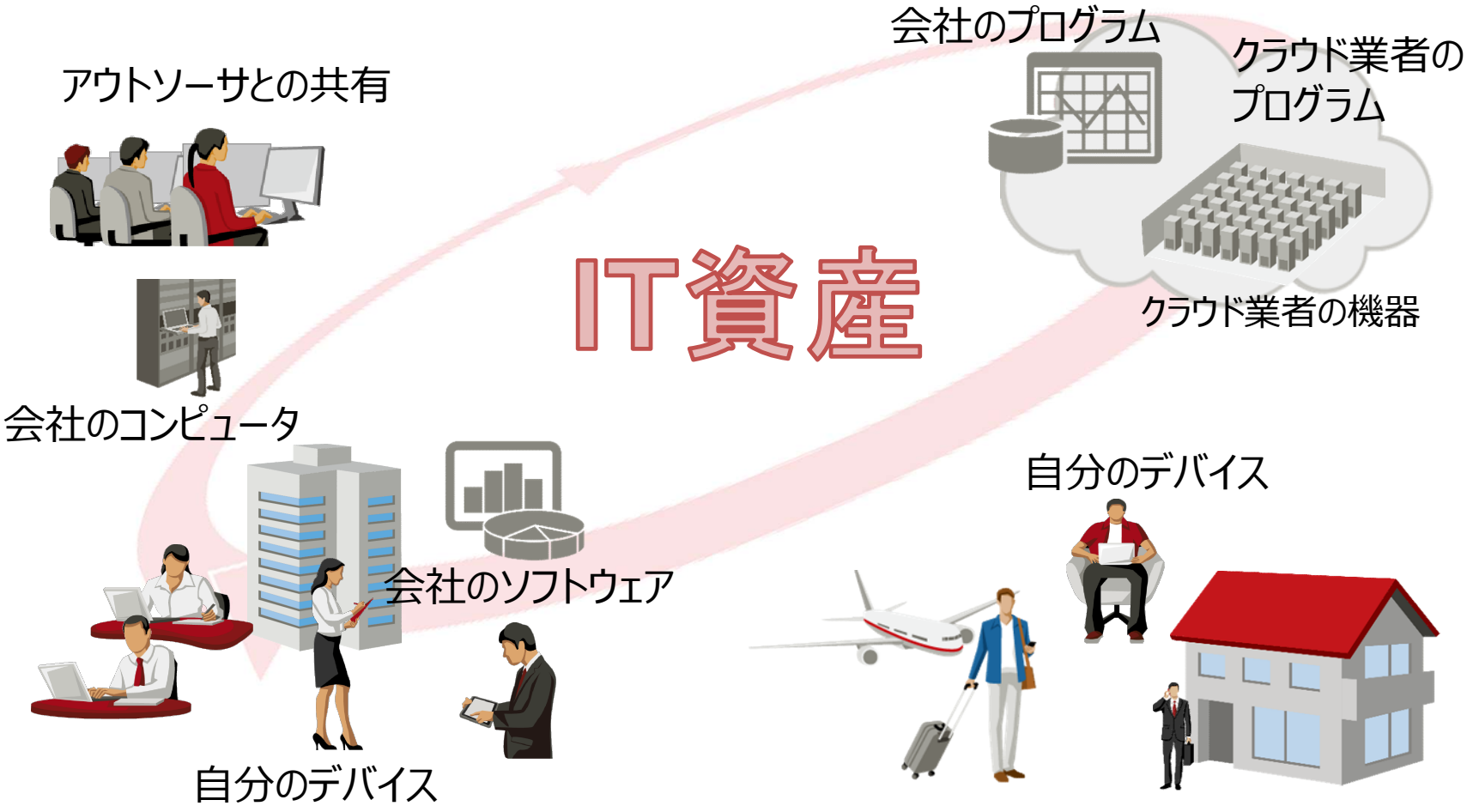
8.1　運用の計画及び管理
8.2　変更の管理
8.3　中核データ管理
8.4　ライセンス管理
8.5　セキュリティ管理
8.6　他のプロセス
8.7　アウトソーシングとサービス
8.8　組織と個人間の複合責任

ITAMで追加された節

BYODや3rdパーティの持ち込み機器を想定

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

プロセスの標準化まとめ

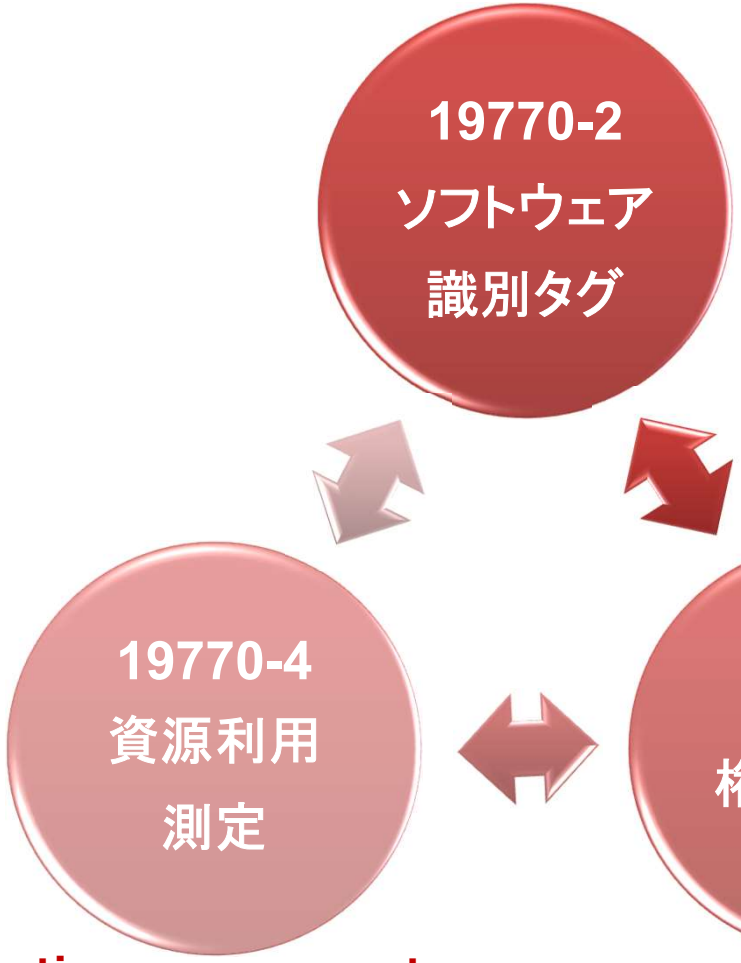
- SAMの標準からITAMの標準に進化した
- IT資産の組織と個人の複合責任のリスクが新たに取り込まれた
- 認証規格のベースとなる要求事項の規格ができた
- 本年度のＪＩＳ化に申請されている

タグ関連の標準化

SAMAC
一般社団法人 IT 資産管理評価認定協会

ITAMの３つのタグの狙い

3つのタグが連携してソリューションを提供



SWID tag
Softwere identification

RUM
Resourse utilization mesurement

ENT schema
Entitlement schema

SAMAC
一般社団法人 IT 資産管理評価認定協会

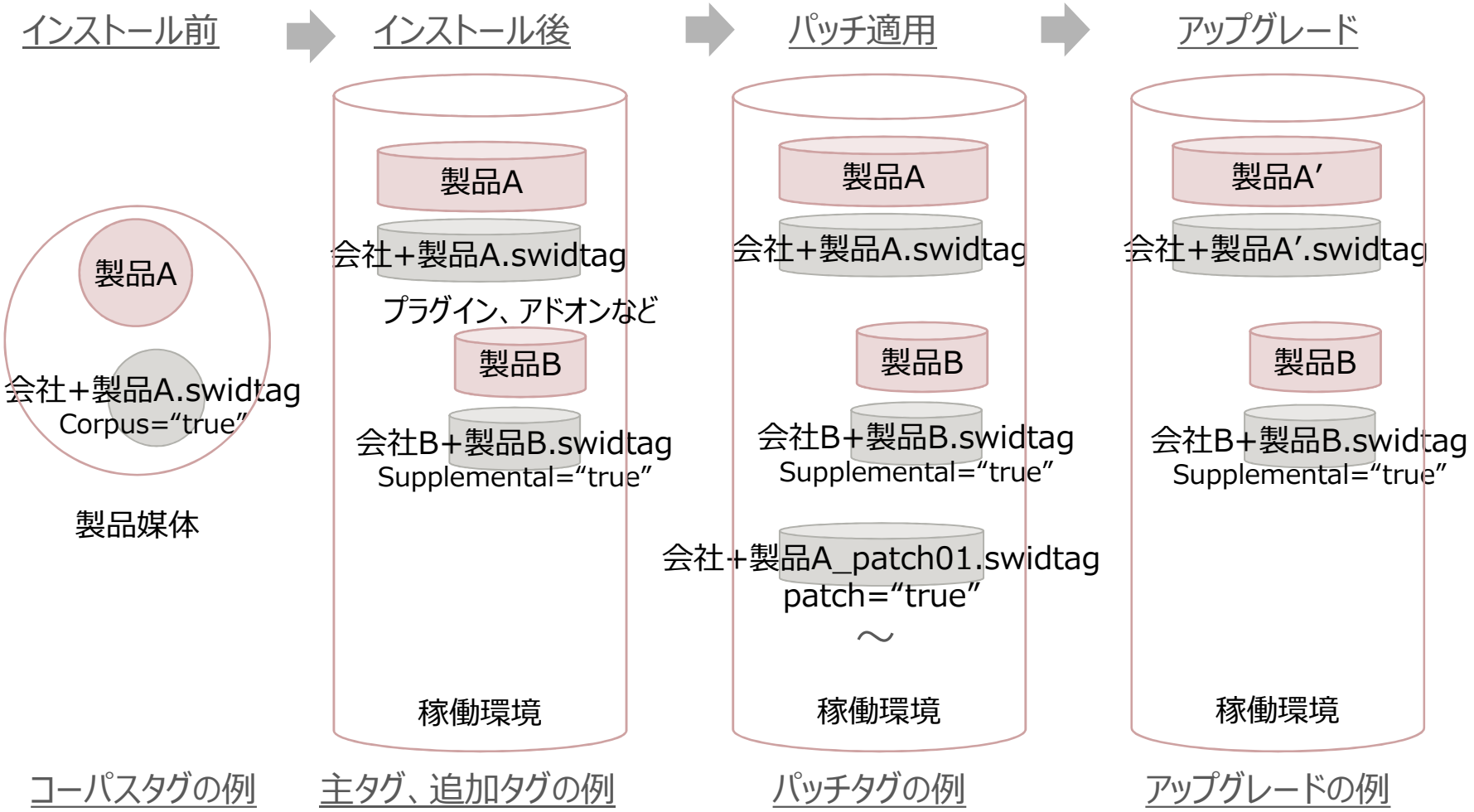
ソフトウェア識別タグでなにが定義できるか？

ファイル名：組織名_プロダクト名.swidtag

要素			説明
ルート(SoftwareIdentity)			ソフトウェア識別についてのルート属性を記述する。 タグの種類、製品名、バージョンなど
子要素	組織情報(Entity)	タグを生成した組織は必須，他は選択	このSWIDタグに対して責任のある組織の情報を記述する。タグ生成者、ソフトウェア開発者、ライセンス提供者…
	リンク情報(Link)	選択	他のファイルの参照関係を記述する。関係するファイルやダウンロード元，脆弱性データベース，使用権なども定義できる。
	メタ情報(Meta)	選択	このSWIDに関する任意の情報を記述する。 開発者が付与したソフトウェアの詳細な製品名、ﾊﾞｰｼﾞｮﾝ、エディションなど
	ソフトウェアの本来情報(Payload)	選択	インストールされるファイルについて本来の情報を記述する。 ファイルの名前、サイズ、ハッシュ値など
	ソフトウェアの実際情報(Evidence)	選択	SWIDタグが見つからないソフトウェアのシステム検査結果を記述する。
	署名情報(Signature)	選択	このSWIDタグに対して責任のある組織の署名情報を記述する。

SWIDのライフサイクル

ルート要素の属性（“corpus”,”patch”,”supplemental”）を指定することでライフサイクルを定義できる



ENT schema 権利スキーマで何が定義できるのか？

ファイル名：組織名_プロダクト名_entId.ent

要素			説明
ルート(Ent)			権利についてのルート属性を記述する。契約のentId、タイプ（ライフサイクル例参照）、日付などを定義する。
子要素	組織情報(Entity)	EntCreatorは必須, 他は選択	Entが定義している権利に関連する組織の情報を記述する。
	契約メタ情報(EntMeta)	必須	契約に関する情報をまとめて保有する。契約の内容、契約製品の情報、測定情報など任意の契約情報が定義できる。（次頁参照）
	リンク情報(Link)	選択	他のファイルの参照関係を記述する。関係するファイルやダウンロード元，脆弱性データベース，使用権なども定義できる。
	メタ情報(Meta)	選択（1個のみ）	この契約に関する任意の情報を記述する。
	署名情報(Signature)	選択	このEntに対して責任のある組織の署名情報を記述する

Entファイル（ライセンス）の定義例

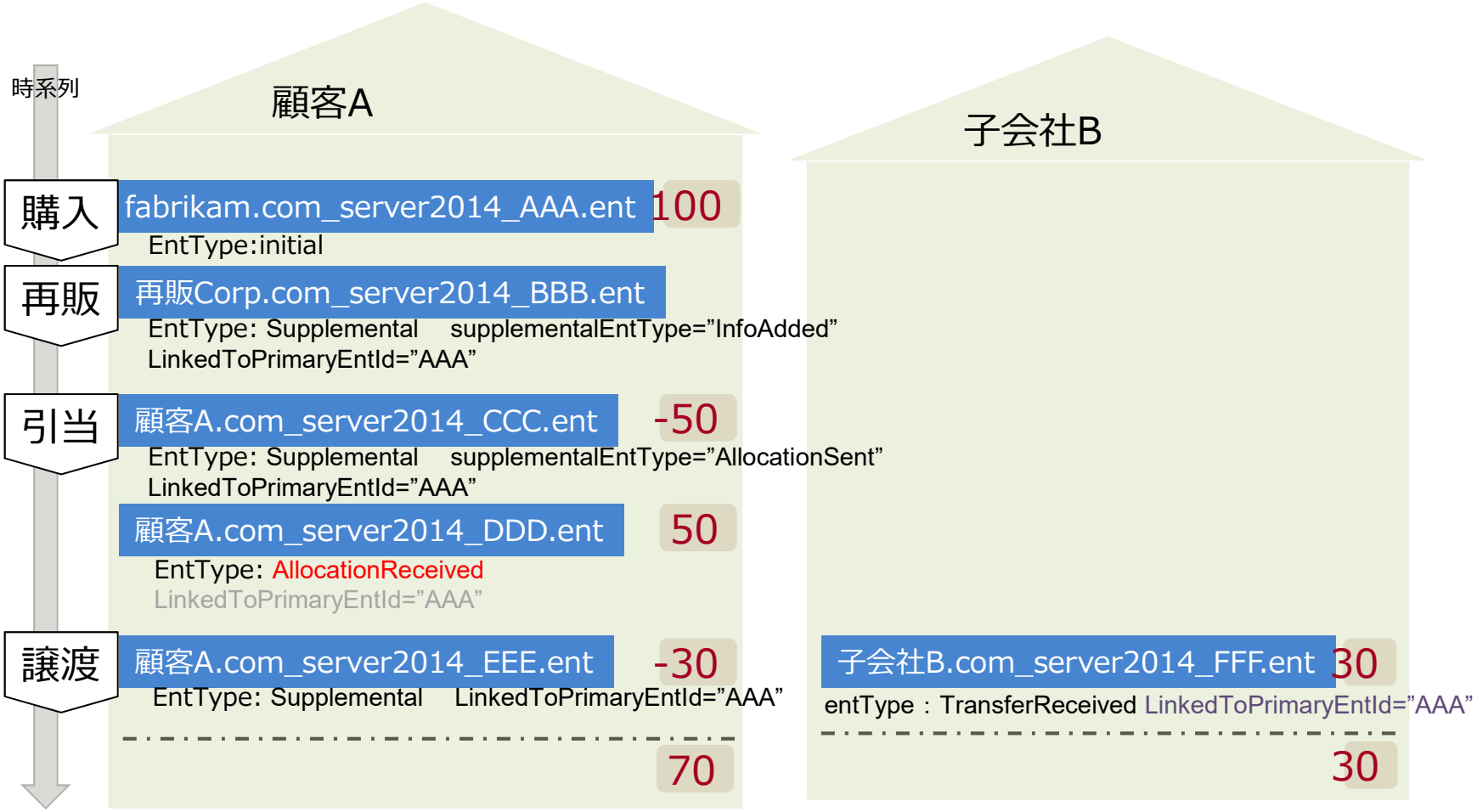
顧客Aがfabrikam社のサーバライセンスを100購入した。インストールライセンスが100、CALライセンスは1CPU単位に5CALある。

fabrikam.com_server2014_AAA.ent

```
<ent  entId=”AAA”  entType=”Initial”  entCreationDate="2014-10-13T15:09:10+00:00">
   <Entity  name="Fabrikam“ regid="fabrikam.com“ role="softwareCreator  entCreator"/>
   <Entity  name=“顧客A” regid=“顧客A.com“ role=”entitledEntity“ alias=“本社”/>
   <EntMeta  products=“server2014”  entitlementType =“License” >
     <Quantification  quantity="100“  >                    ライセンス数とそのカウント方法
        <Metric metricName="per Server"  metricType=“Device”>
           <TestMethod testName=“For SWIDTAG“/>          SWIDでのライセンスのカウント方法
           <TestScript=“tagId={GUID} server2014 tagCreatorRegid =fabrikam.com “/>
        </Metric>        </Quantification>
     <Right  rightId=“1”  rightName=“installLicense” >
        <LimitTime isPerpetual=“true”/>                   サーバライセンスの権利定義
     </Right>
     <Right  rightId=“2”  rightName=“CAL” >
        <LimitTime isPerpetual=“trure”/>
        <Quantification quantity=”5” />                   サーバCALライセンスの権利定義
     </Right>
   </EntMeta>
    ・・・
```

Entファイルのライフサイクル例

顧客Aは，　Fabrikam社が発行した100ライセンスを購入したが、その取引で 再販Corpが情報を付加した。顧客Aは社内の部門に50ライセンス引き当て、その後，30ライセンスを子会社Bに譲渡する。



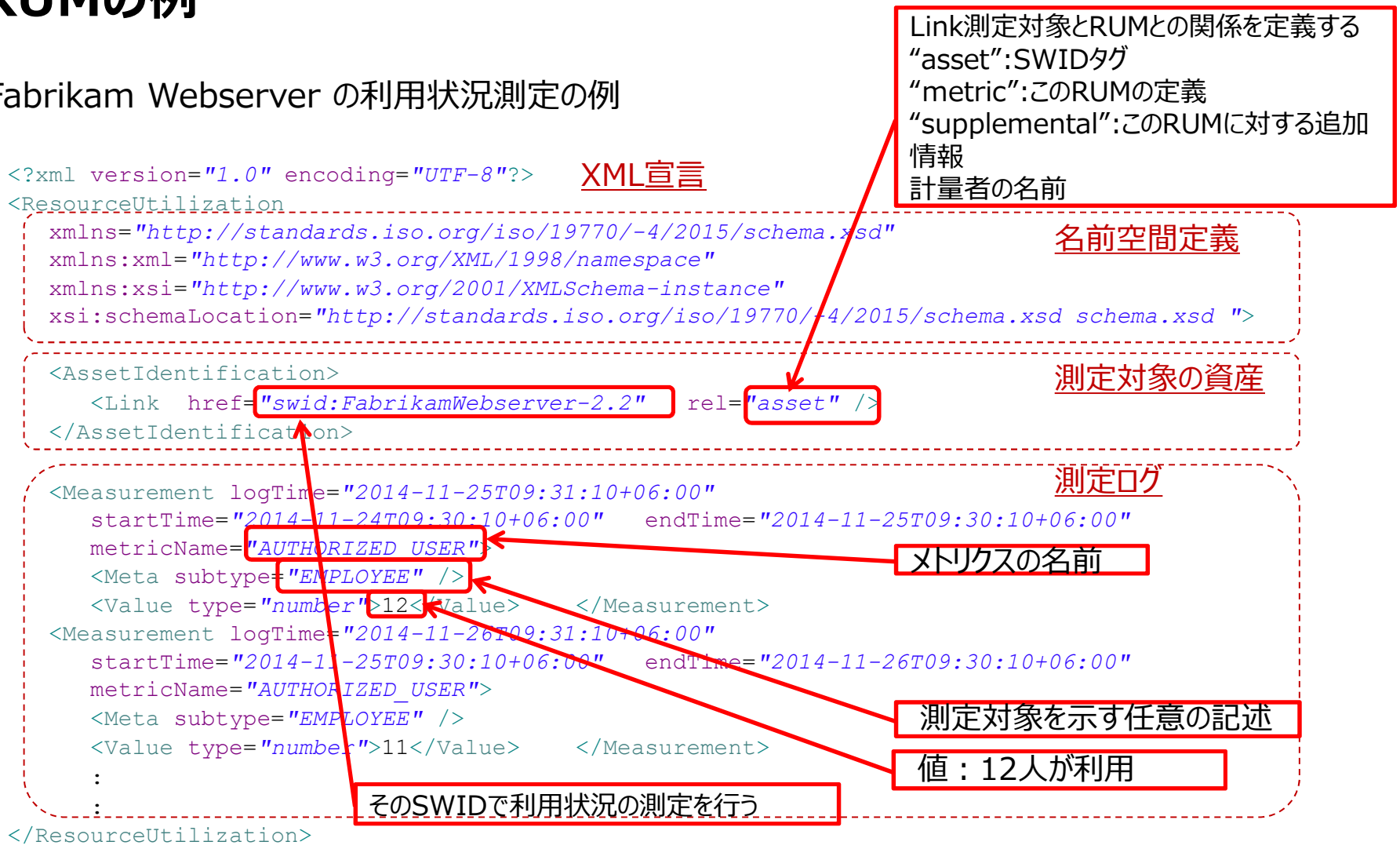
RUM 資源利用測定で何が定義できるのか？

ファイル名：SWIDタグファイル名.ログファイル名.数字.rum

要素			説明
ルート(ResourceUtilization)			属性の定義はない。
子要素	資産識別子 (AssetIdentification)	必須 （１個のみ）	IT資産の識別子
	メタ情報 (Meta)	選択 （１個のみ）	このRUMに関する任意の情報を記述する。 製品名、製品IDなど任意の拡張ができる
	測定情報 (Measurement)	必須 （１個以上）	測定データ

RUMの例

Fabrikam Webserver の利用状況測定の例

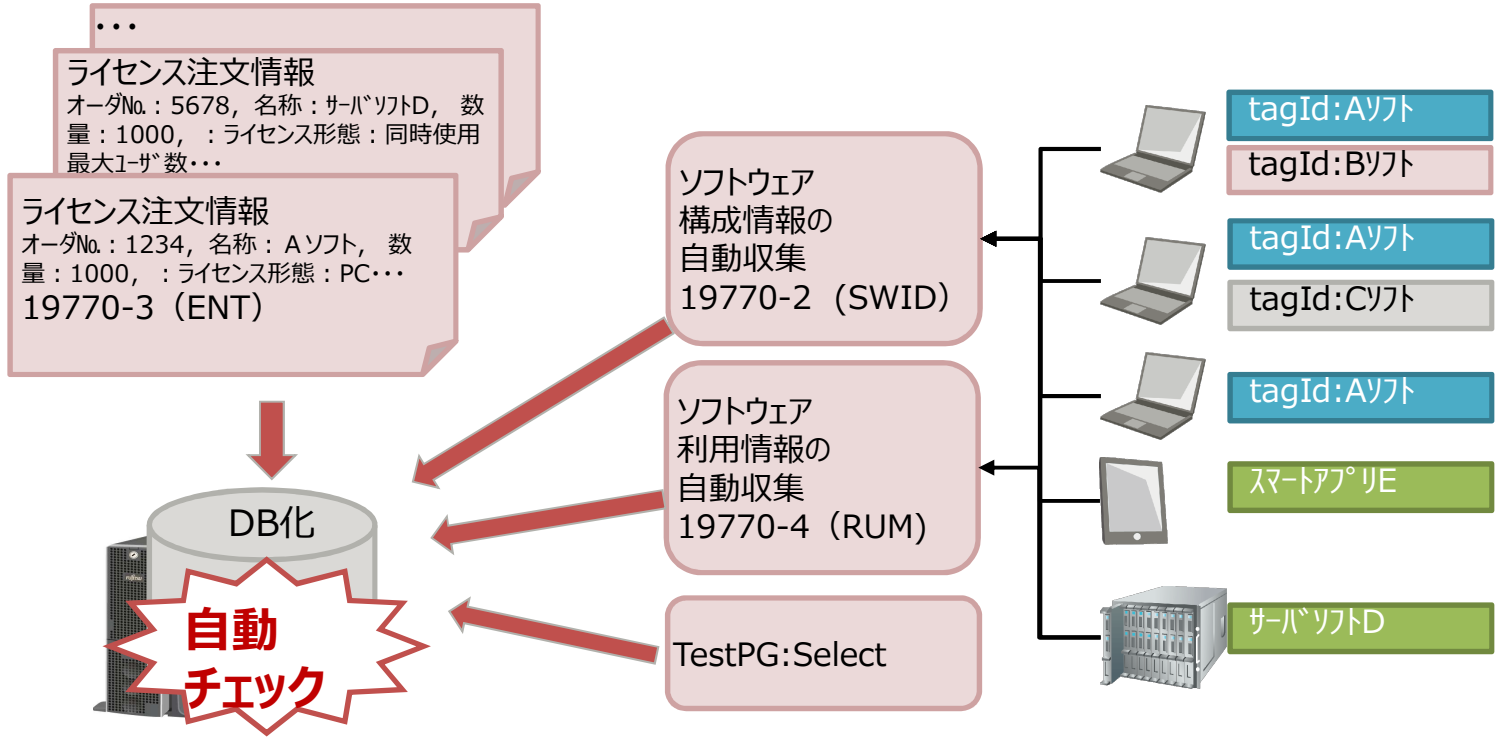



```
<?xml version="1.0" encoding="UTF-8"?>
<ResourceUtilization
  xmlns="http://standards.iso.org/iso/19770/-4/2015/schema.xsd"
  xmlns:xml="http://www.w3.org/XML/1998/namespace"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://standards.iso.org/iso/19770/-4/2015/schema.xsd schema.xsd ">
  <AssetIdentification>
     <Link  href="swid:FabrikamWebserver-2.2"  rel="asset" />
  </AssetIdentification>
  <Measurement logTime="2014-11-25T09:31:10+06:00"
     startTime="2014-11-24T09:30:10+06:00"   endTime="2014-11-25T09:30:10+06:00"
     metricName="AUTHORIZED_USER">
     <Meta subtype="EMPLOYEE" />
     <Value type="number">12</Value>    </Measurement>
  <Measurement logTime="2014-11-26T09:31:10+06:00"
     startTime="2014-11-25T09:30:10+06:00"   endTime="2014-11-26T09:30:10+06:00"
     metricName="AUTHORIZED_USER">
     <Meta subtype="EMPLOYEE" />
     <Value type="number">11</Value>    </Measurement>
     :
     :
</ResourceUtilization>
```

ライセンスコンプライアンスでの例

ENTスキーマで記述されたライセンスをSWIDタグ、RUMで検証できる

Entファイルで契約書を電子的に入手し、DB化する。DB化された契約情報のメトリックスからライセンスのカウント方法を確認する。SWIDタグからカウントできるもの、RUM（資源利用測定）でカウントできるもの確認し、権利違反を自動チェック仕組みを検討する。

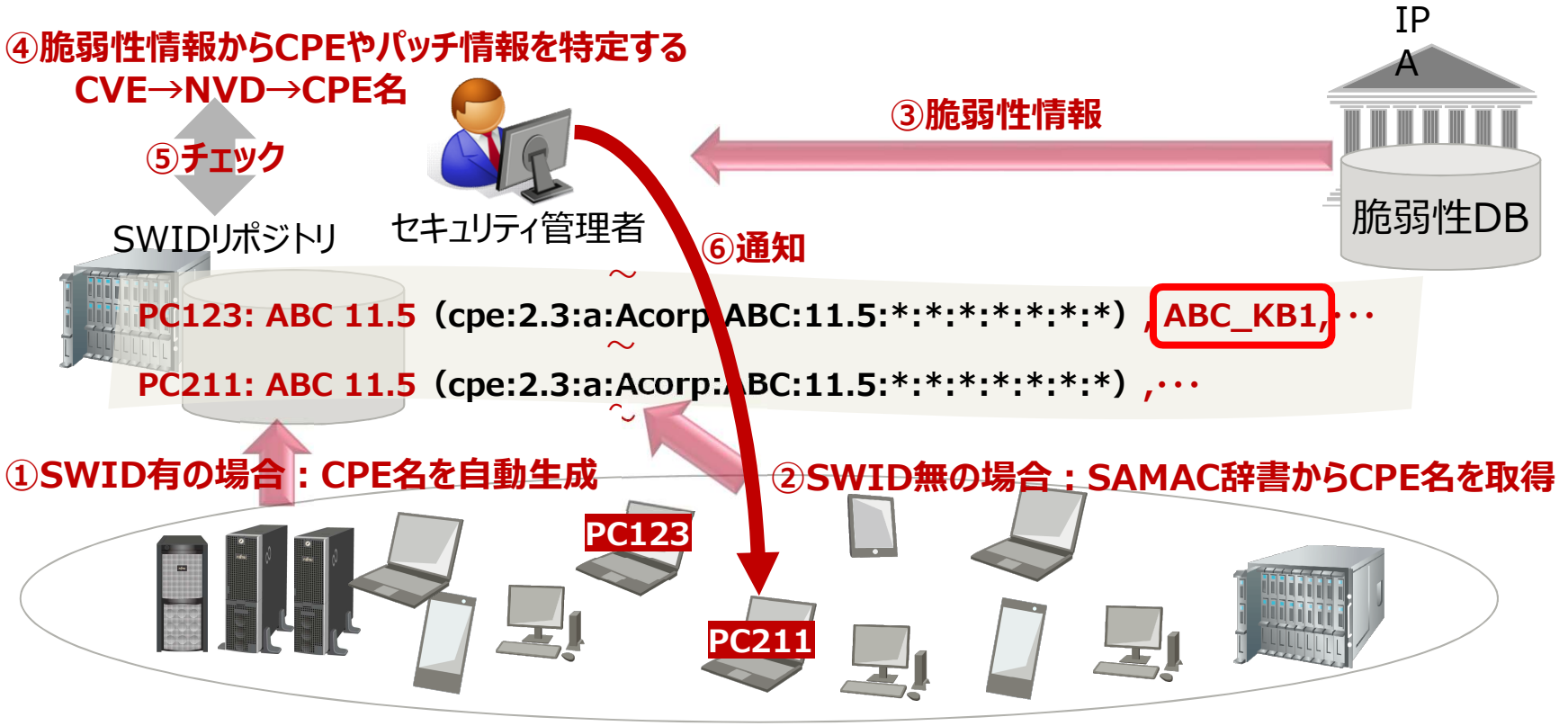


SAMAC
一般社団法人 IT 資産管理評価認定協会

セキュリティ管理の例　～19770-2:2015（SWID）を活用した脆弱性対策～

脆弱性情報から該当プログラムが正確に検出され(SWIDの場合),自動化が可能となる

例　AcorpのABCソフト、バージョン11.1から11.7、バージョン12.0から12.1（12.1から12.1まで）に脆弱性。バージョン12.2以降で修正。修正パッチは ABC_KB1がある；SWIDリポジトリを調べ、ABC 11.5の導入されたPC123とPC211を発見するが、PC123にはパッチABC_KB1が当たっているため、**PC211**のみに脆弱性がある。



凡例　CVE:共通脆弱性識別子, NVD:国際脆弱性DB, CPE:共通プラットフォーム一覧

実現させるために

- ソフトウェア開発者がNISTIR 8060のUS３（脆弱性エンドポイントを特定できるレベルの運用パターン）に従ったSWIDの生成を実施する。
- SWIDに対応しないソフトウェアとの共存のために以下の対策が考えられる：
  - ✓SAMAC辞書とIPAの脆弱性対策情報データベース との連携をSWIDの運用と共存させる。
  - ✓SAMAC辞書のCPE名をもとにSWIDを作成し、資産管理ツールベンダーに提供する。
- NVDに登録されるCPE名がSWIDから自動生成されるようにする。（NISTIR 8085で自動生成するPGが公開されている）
- SWIDの信頼性を保証するために電子署名を導入する。

- NISTIR 8060 “Guidelines for the Creation of Interoperable Software Identification (SWID) Tags”
- NISTIR 8085 “Forming Common Platform Enumaration(CPE)Names from Software Identification(SWID)Tags”

凡例　NISTIR:National Institute of Standards and Technology Interagency Report

タグ標準化のまとめ　（タグの普及について）

- SWIDタグは、IT資産の構成情報を定義し、セキュリティ対策の基本となる。
- SWIDタグ、ENTスキーマが国際標準となり、RUMが国際標準の最終手続き中である。
  ITAMの省力化が現実となりつつある。
- SWIDタグはJIS化原案作成完了、 ENTスキーマ、RUMはJIS化申請中。

- **ITベンダーがプロダクト開発と同じレベルでタグに対応すること。**
- **タグが正しく設定されていることをチェックする機関の設立。**

参考：米国の動向

TagVault.org（IEEE-ISTOの非営利下部組織）

設立時のボード会員：

CA、Microsoft、ModusLink、Symantec

主要メンバー：

HP, EMC^2, IBM、 Anglepoint, Eracent, Gothaer Systems GmbH, iQuate, MITRE, Scalable Software, Open iT, US ARMY, *国防総省*(DoD), 国土安全保障省(DHS), 連邦政府調達局(GSA), US NAVY,国立標準技術研究所(NIST)

アライアンスパートナー：

Agnitio Advisors, Cicala and Associates, CyberPack Ventures,IAITAM,IEEE-IS

SWIDタグ適用ソフトウェア開発者：

Microsoft, Symantec, Adobe, IBM（約 300 product /月）など

ツールベンダー：

CA Technologies（ IT Client and Asset Manager）， Hewlett Packard -DDMI , Microsoft – SCCM, Symantec –Altiris, Aspera, Asset Metrics, Eracent, Express Metrix, Flexera, iQuate, Magnicomp, Software Management.org

Caphyon’s Advanced Installer， Flexera Software’s InstallShield， Flexera Software’s InstallAnywhere， Open Source - Windows Installer XML Toolset (WiX)など

一般社団法人 IT 資産管理評価認定協会