

IT資産管理の省力化を目的とした情報構造の 標準化と利用方法

IT資産管理評価認定協会

TAG WG 高橋快昇

2018年6月8日

アジェンダ

- 国際標準化の動向
- ITアセットの情報構造標準化の狙い
- JIS X 0164-2:2018 SWIDタグ
- JIS X 0164-3:2019 ENTタグ
- JIS X 0164-4:2019 RUMタグ

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 * : JIS化

凡例 DIS:国際規格原案、CD:委員会原案

ITアセットの情報構造標準化の狙い



ITアセットの各種情報構造のタグ化の狙い

ITアセットマネジメントの品質向上

- SWID: ソフトウェア識別のための情報構造の規定
- ENT: 権利(ライセンス)定義のための情報構造の規定
- RUM: ITアセットの利用状況測定のための情報構造の規定

ITアセットマネジメントの省力化

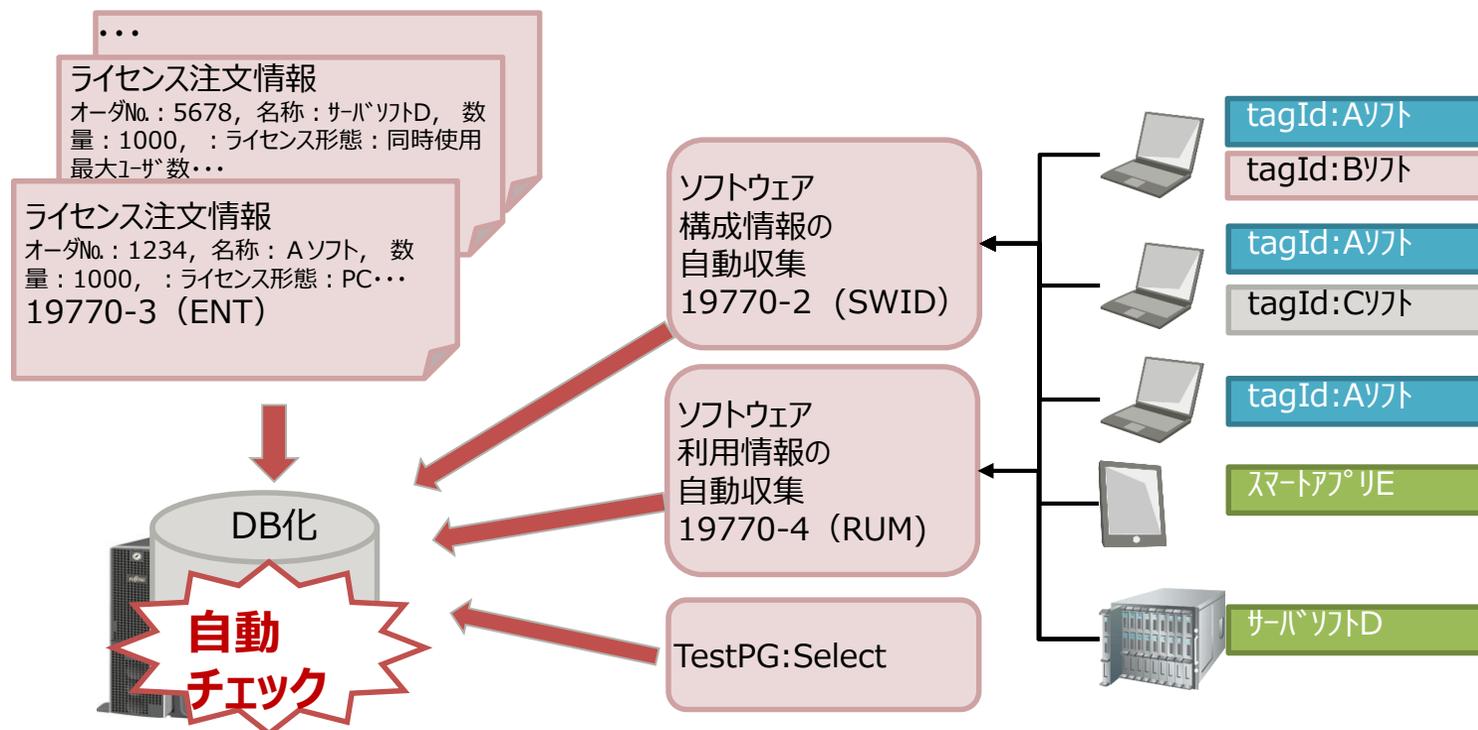
- SWID,END,RUMによるライセンス監査データの自動作成
- 米国が進めているSCAP(情報セキュリティ対策の自動化プロトコル)の推進

SWID (Software Identification)
ENT schema (Entitlement schema)
RUM (Resource utilization measurement)
SCAM (Security Content Automation Protocol)

ライセンスの調停作業を自動化する例

ENTスキーム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
の確認し、権利違反を自動チェック仕組みを検討する。

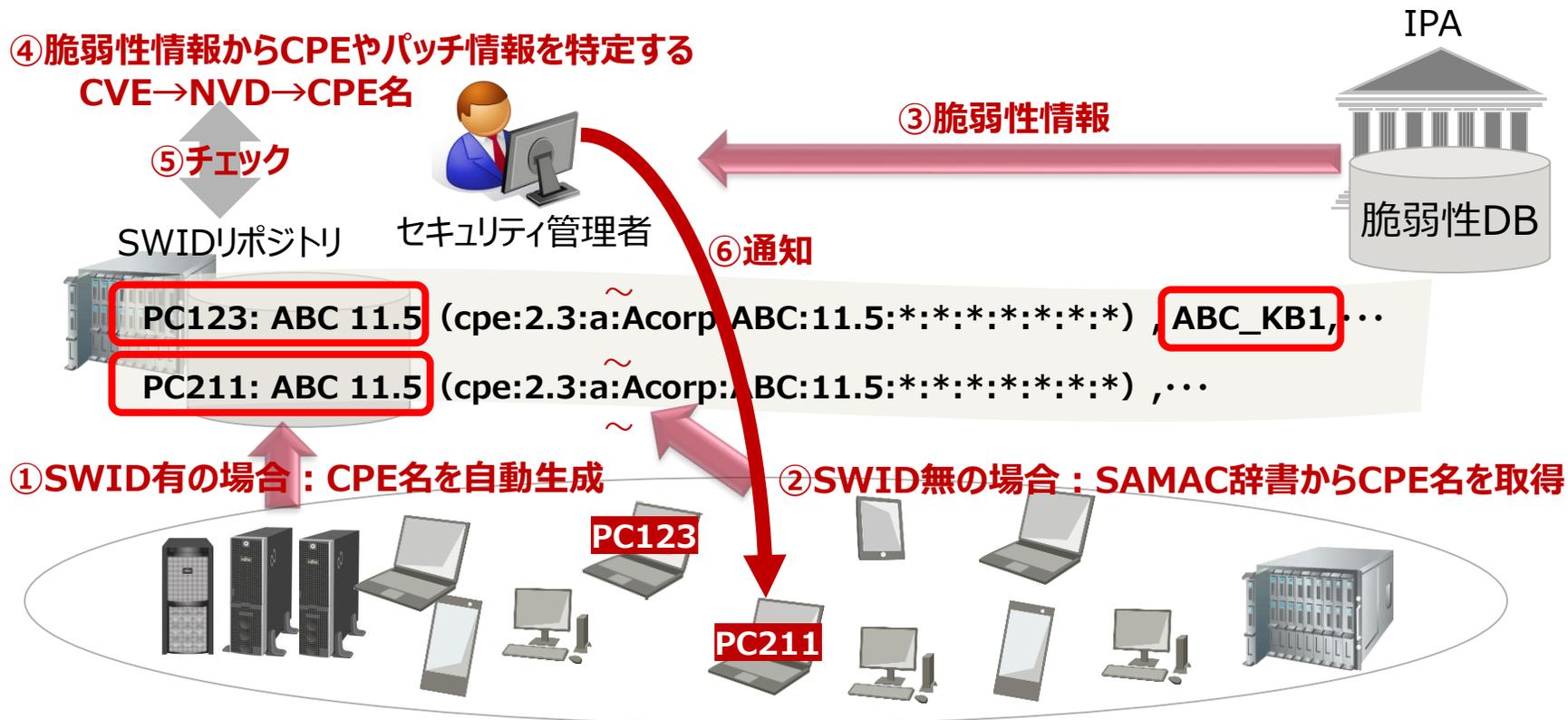


情報セキュリティ管理の例

～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

JIS X 0164-2:2018 SWIDタグ (ISO/IEC 19770-2:2015)

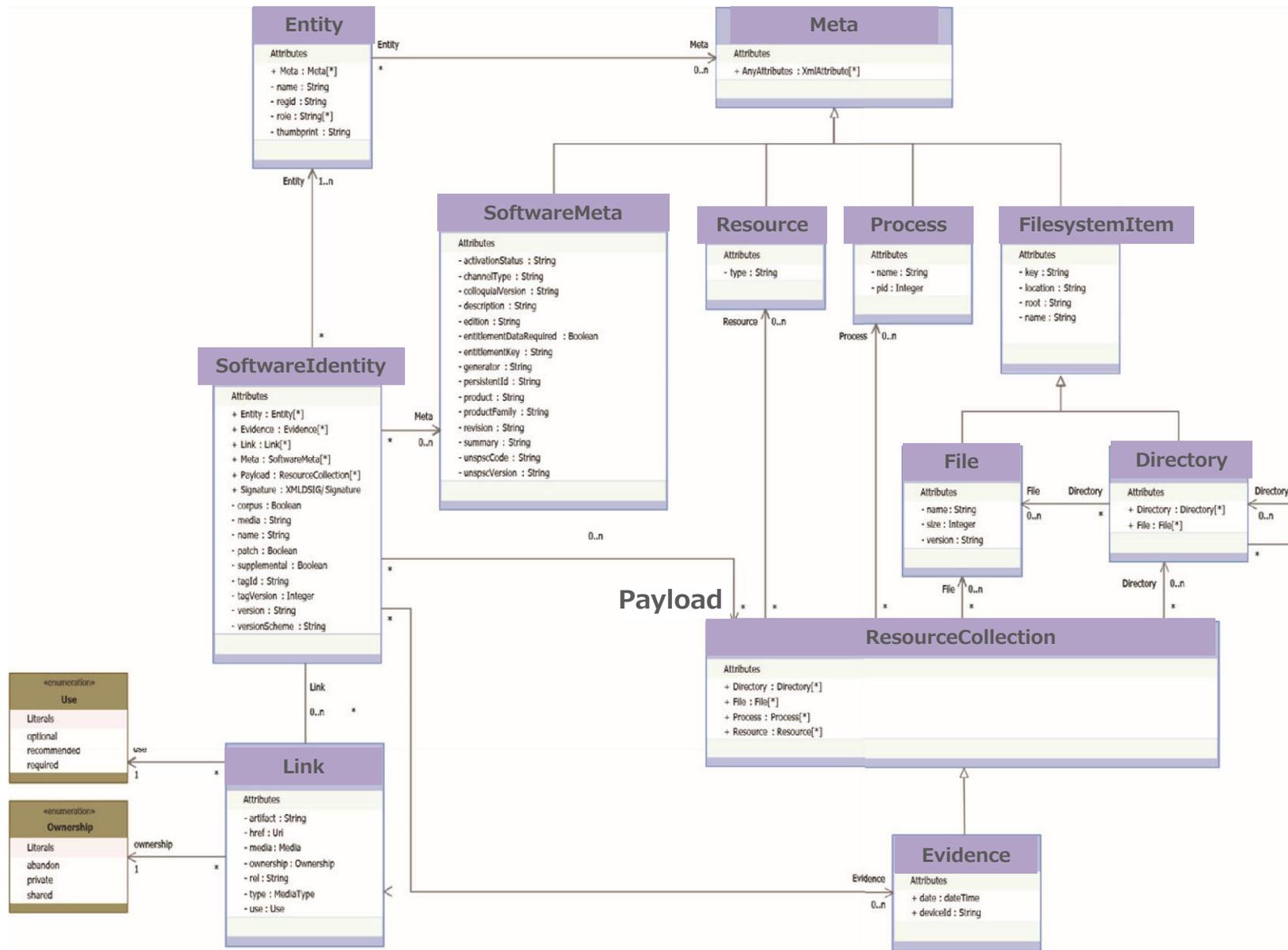


ソフトウェア識別タグでなにが定義できるか？

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、バージョン、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タグのUMLダイアグラム (参考)



SWIDタグ 例 (Fabrikam Writer 2013)

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<SoftwareIdentity
  xmlns="http://standards.iso.org/iso/19770/-2/2014/schema.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:SHA256="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
  name="Fabrikam Writer 2013"
  tagId="{GUID}FabrikamWriter-2013"
  version="12.1.1"
  versionScheme="multipartnumeric">
  <Entity name="Fabrikam Corporation" regid="fabrikam.com" role="softwareCreator
  licenser tagCreator" />
  <!-- also requires the C++ runtime -->
  <Link rel="requires" href="swidpath:/SoftwareIdentity/Meta[@persistentId='EAB2F277-
  0920-4F8C-B466-6FE0CA7D59DF' ] ownership="shared" />
  <Payload>
    <File name="writer.exe" size="1024000" location="../bin/"
      SHA256:hash="c4128c2dc663ae7a6b6bc6787594057396e6b3f569cd50fd5ddb4d1bbafd2b6a" />
    <File name="writer.dll" size="524012" location="../bin/"
      SHA256:hash="96e6b3f569cd50fd5ddb4d1bbafd2b6ac4128c2dc663ae7a6b6bc67875940573" />
  </Payload>
</SoftwareIdentity>
```

XML宣言

19770-2デフォルト名前空間

W3C XMLスキーマ名前空間

デジタル承認名前空間

ハッシュ名前空間

タグの名前

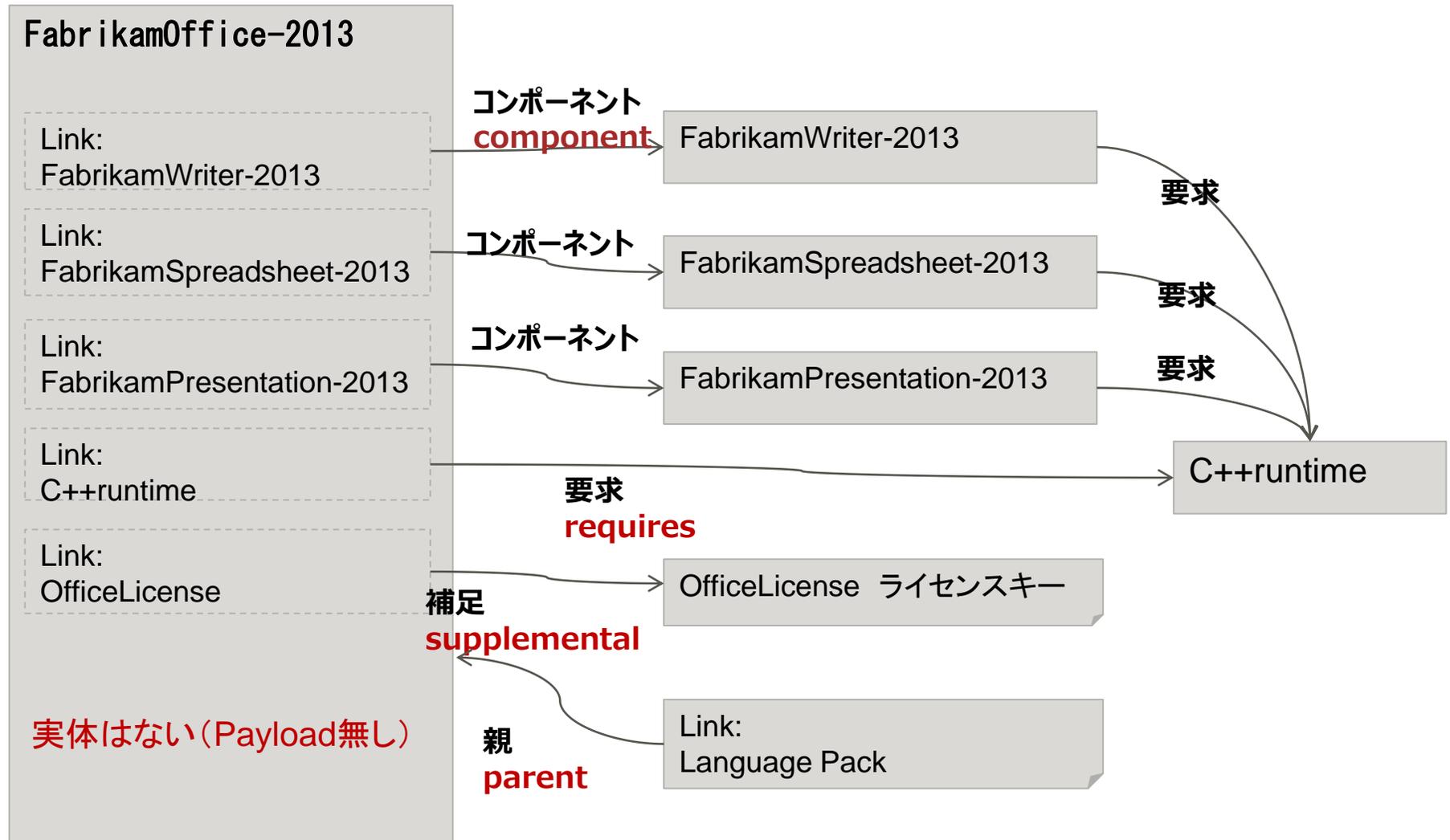
判り易くするために記述しているが、16バイトのGUID (例えば、2df9de35-0aff-4a86-ace6f7dddd1ade4c) を記述する。

persistentIdが'EAB2---'であるSWIDタグが示しているプロダクト

C++が共用されている

writer.dllの正しいサイズ、位置、Hash情報

スウィート製品SWIDタグのリンク関係



□ : タグファイル (?.swidtag)、

□ : 補足タグファイル (?.swidtag)、

← : リンク関係

スイーツ製品のSWIDタグ 例

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
```

```
<SoftwareIdentity
```

```
  xmlns="http://standards.iso.org/iso/19770/="
  xmlns:xsi="http://www.w3.org/2001/XMLSchema="
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
```

```
  name="Fabrikam Office 2013"
  tagId="{GUID}FabrikamOffice-2013"
  version="12.1.1"
  versionScheme="multipartnumeric">
```

名前が“Fabrikam Office 2013”で
tagIdが“={GUID}FabrikamOffice-2013”
のSWIDタグ。

SWIDタグのtagIdが{GUID}Fabrikam2013
のソフトウェアはFabricam Office 2013のコンポーネント
で推奨されている。

```
<Entity name="Fabrikam Corporation" regid="fabrikam.com" role="softwareCreator licensor
tagCreator" />
```

このコンポーネントはオプション

```
<Link rel="component" href="swid: {GUID}FabrikamWriter-2013" use="recommended" />
```

```
<Link rel="component" href="swid: {GUID}FabrikamSpreadsheet-2013" use="recommended" />
```

```
<Link rel="component" href="swid: {GUID}FabrikamPresentation-2013" use="optional" />
```

```
<!-- also require
```

同じディレクトリに“FabrikamOfficeLicense.swidtag”の補足タグがある

```
<Link rel="requires" href="swidpath:/softwareidentity/meta[epersistencid= EAB21277-0920-
4F8C-B466-6FE0CA7D59DF' ]" ownership="shared" />
```

```
<Link rel="supplemental" href="./FabrikamOfficeLicense.swidtag" />
```

```
<Meta entitlementDataRequired="true" />
```

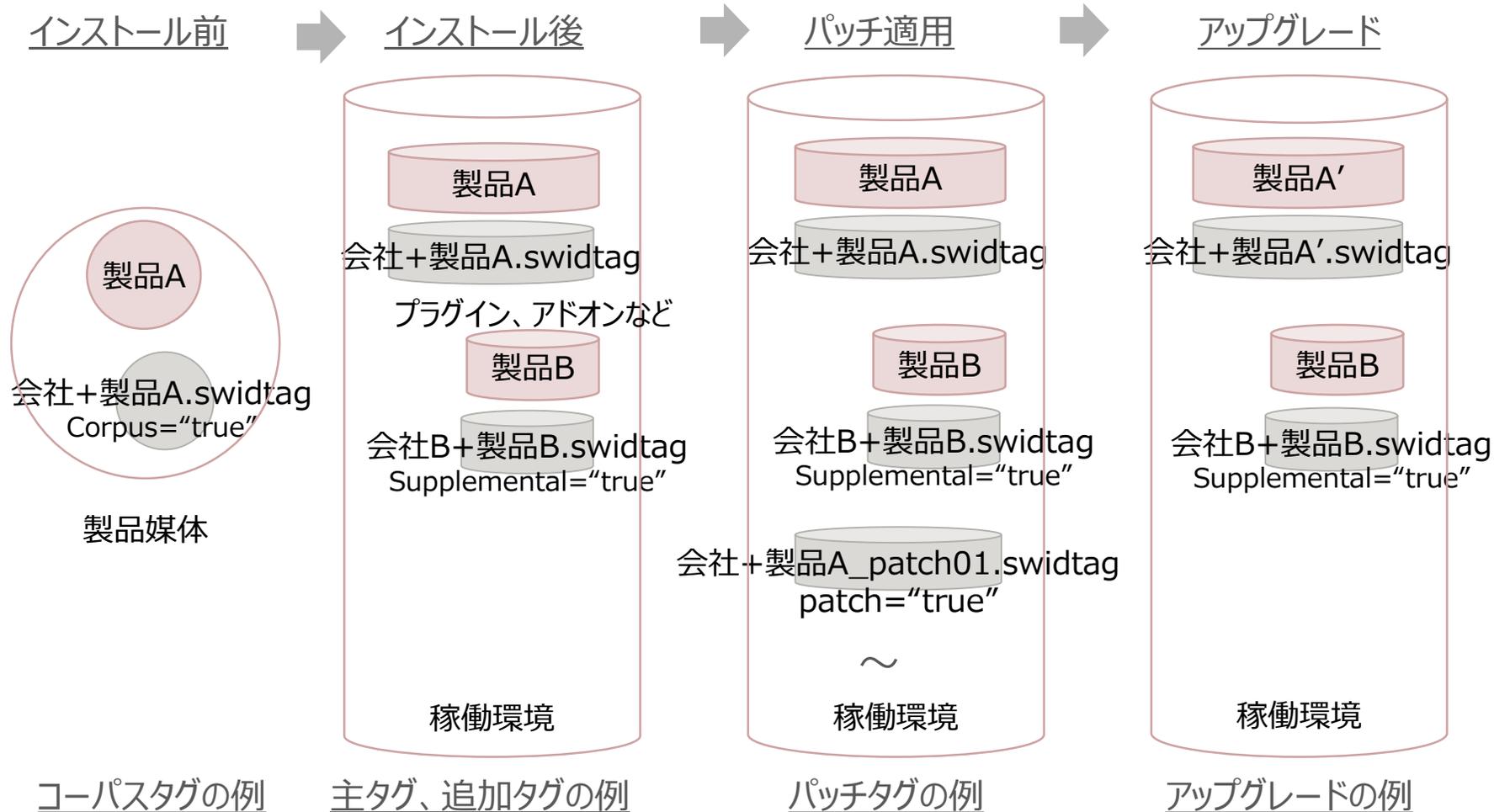
```
<Meta SKU="FabrikamOfficeStandard-2013-Retail" />
```

```
</SoftwareIdentity>
```

アクティベーションキーが要求されている

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



JIS X 0164-3:2019 ENTタグ (ISO/IEC 19770-3:2016)

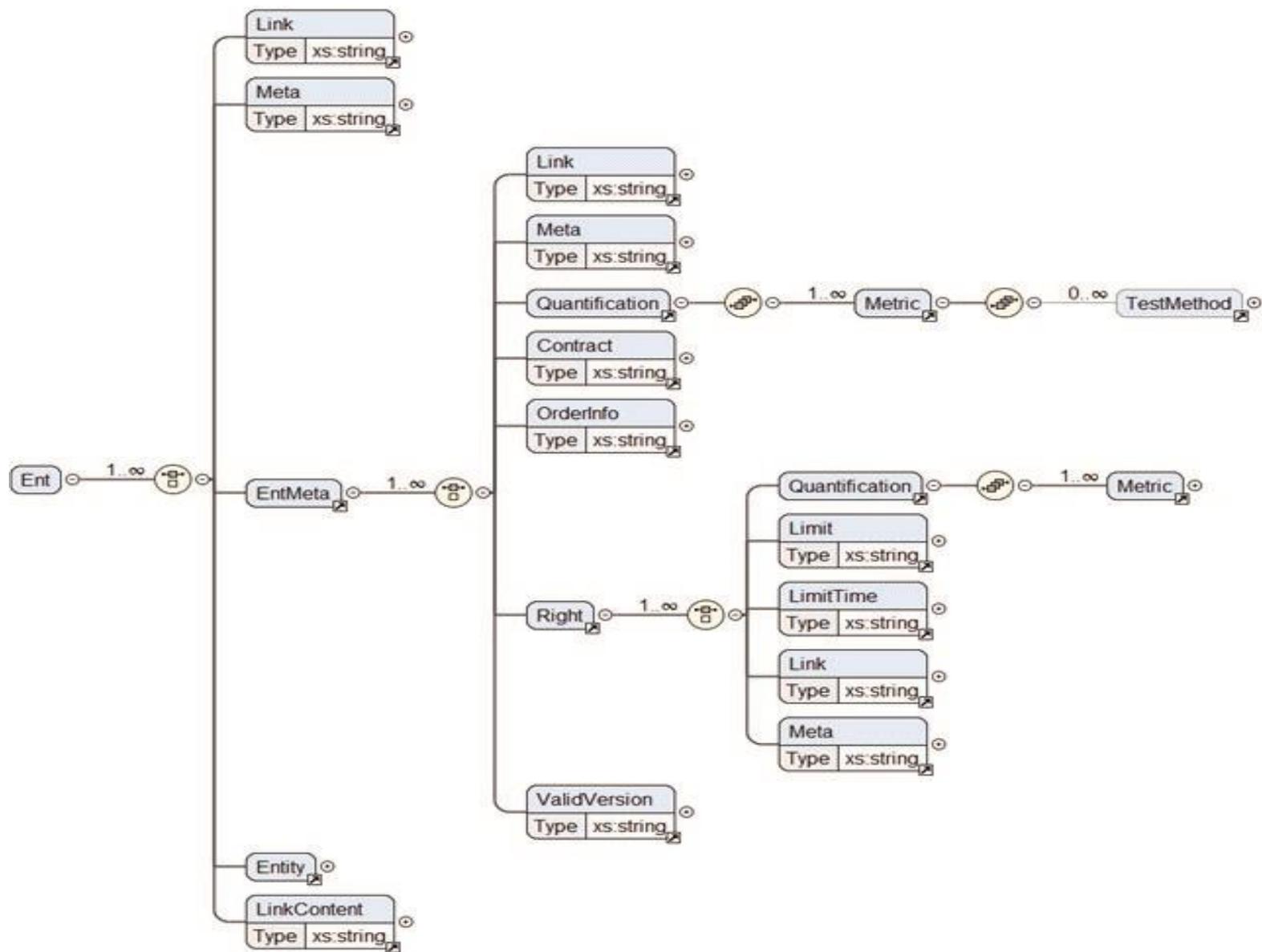


ENT schema 権利スキーマで何が定義できるのか？

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タグのUMLダイアグラム (参考)



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1 CPU単位に5 CAL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" >
      <Metric metricName="per Server" metricType="Device">
        <TestMethod testName="For SWIDTAG"/>
        <TestScript="tagId={GUID} server2014 tagCreatorRegid =fabrikam.com "/>
      </Metric>
    </Quantification>
    <Right rightId="1" rightName="installLicense" >
      <LimitTime isPerpetual="true"/>
    </Right>
    <Right rightId="2" rightName="CAL" >
      <LimitTime isPerpetual="true"/>
      <Quantification quantity="5" />
    </Right>
  </EntMeta>
  ...
</ent>
```

ライセンス数とそのカウント方法

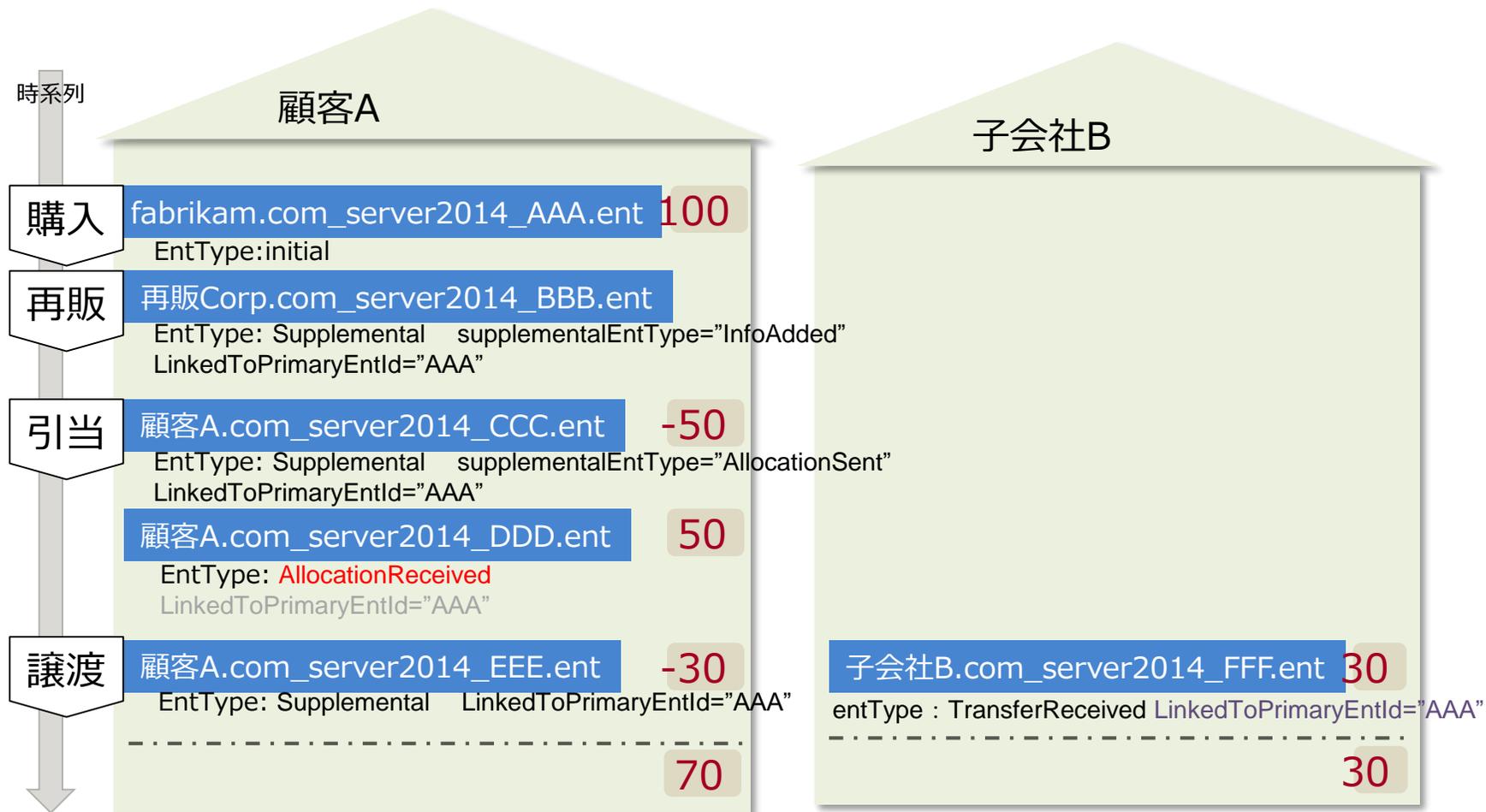
SWIDでのライセンスのカウント方法

サーバライセンスの権利定義

サーバCALライセンスの権利定義

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。



権利譲渡の例

顧客A社は、fabrikam社から購入したライセンス100のうち30を子会社Bに譲渡

fabrikam.com_server2014_AAA.ent

```
<ent entId="AAA" entityType="Initial" entCreationDate="2014-10-13">
  <Entity name="Fabrikam" regid="fabrikam.com" role="softwareCreator entCreator"/>
  ...
```

顧客A.com_server2014_EEE.ent

Entファイルのリンク関係

```
<ent entId="EEE" entityType="Supplemental" supplementalEntType="TransferSent"
  LinkedToPrimaryEntId="AAA" entCreationDate="2015-05-13">
  <Entity name="顧客A" regid="顧客A.com" role="entCreator" alias="本社"/>
  <EntMeta
    <Right rightId="1" rightName="installLicense" >
      <LimitTime isPerpetual="true"/> </Right>
    <Quantification quantity="-30">
  ...
```

譲渡するEnt

Entタイプが補足

30ライセンスの譲渡

子会社B.com_server2014_FFF.ent

```
<ent entId="FFF" entityType="TransferReceived"
  LinkedToPrimaryEntId="AAA" entCreationDate="2015-05-13">
  <Entity name="子会社B" regid="子会社B.com" role="entCreator"/>
  <EntMeta
    <Right rightId="1" rightName="installLicense" >
      <LimitTime isPerpetual="true"/> </Right>
    <Quantification quantity="30">
  ...
```

譲渡を受ける組織で作成されるEnt

JIS X 0164-4:2019 RUMタグ (ISO/IEC 19770-4:2017)

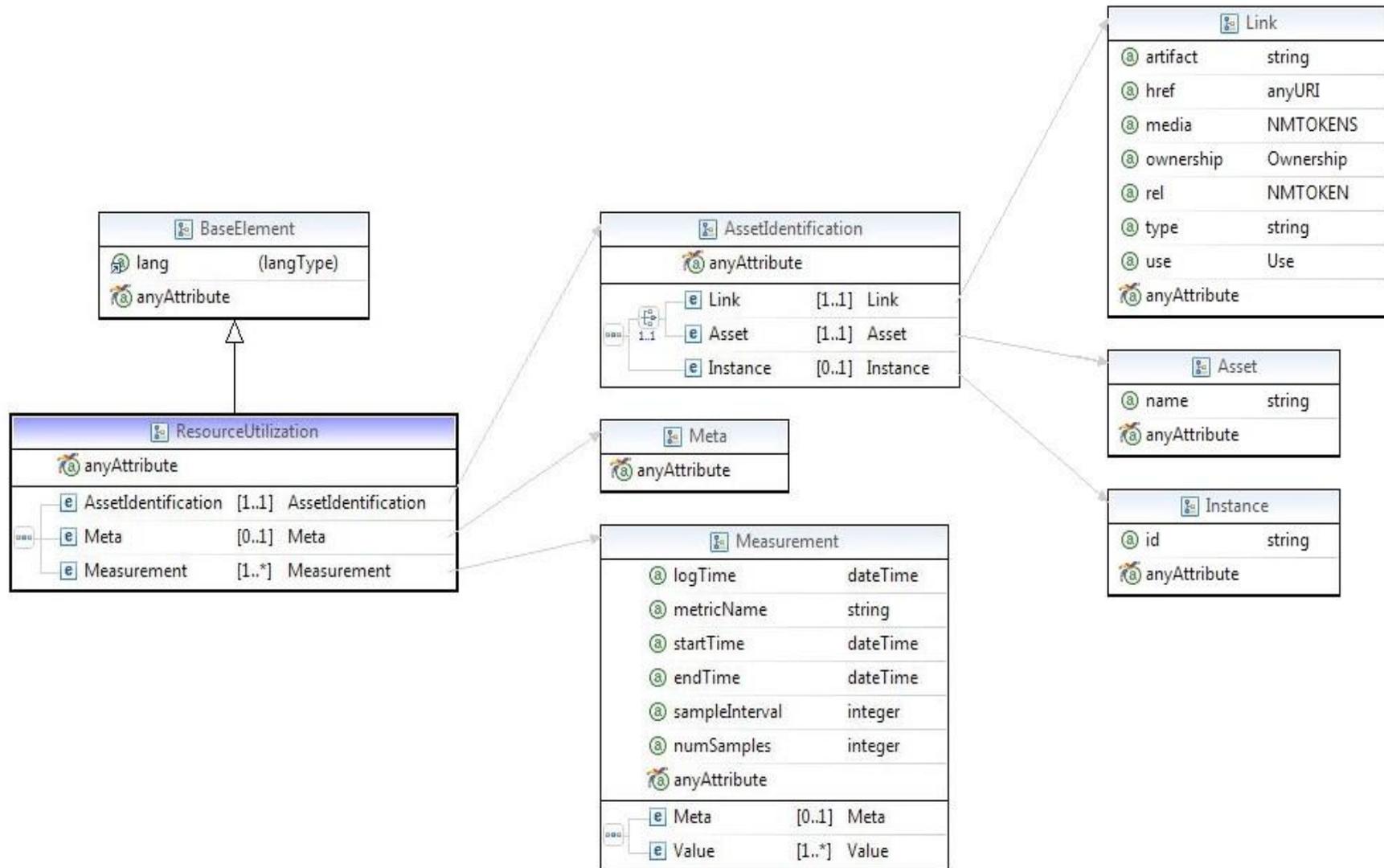


RUM 資源利用測定で何が定義できるのか？

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 SWIDのある資産、ない資産の識別を定義
	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UMLダイアグラム (参考)



RUMの例

Fabrikam Webserver の利用状況測定の例

Link測定対象とRUMとの関係を定義する

- "asset": SWIDタグ

- "metric": このRUMが参照するメトリック情報。

- "supplemental": このRUMに対する追加情報。測定技術など

```
<?xml version="1.0" encoding="UTF-8"?>
```

XML宣言

```
<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 ">
```

名前空間定義

```
<AssetIdentification>
```

```
  <Link href="swid:FabrikamWebserver-2.2" rel="asset" />
```

```
</AssetIdentification>
```

測定対象の資産

```
<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>
```

測定ログ

メトリックの名前

測定対象を示す任意の記述

値：12人が利用

そのSWIDで利用状況の測定を行う

今年度、規格開発開始予定の規格と欧米の状況



今年度、開発開始が許可される予定の情報構造に関する規格

ISO/IEC 19770-6 ハードウェア識別タグ

- ネットワーク機器を含むハードウェア識別のための情報構造の規定

ISO/IEC 19770-7 インベントリスキーマ

- インベントリの収集における情報構造の規定

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, EMC², 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

最近の主な更新 (2017年5月現在)

- TagvaultのSWID Tag Signing WG が電子署名のガイドラインを掲示 (public review)
- MITREがSWIDタグの電子署名ツールのアルファ版をリリース
- GSA がUS政府ソフトウェア (特にDoD) のSWIDタグのリポジトリを構築中
- DoDのIT標準申請で必須になっている (January 5, 2017の標準及びガイダンスのリスト)
- IBMは、- 4 の使用法を作成
- IBMのILMT、BigFixは2015版に対応

The logo for SAMAC consists of the letters S, A, M, M, A, and C. The 'S', 'A', and 'C' are red, while the two 'M's are blue. The letters are bold and sans-serif.

一般社団法人IT資産管理評価認定協会