ＩＳＯ／ＩＥＣ　WG21（IT Asset Management／IT資産管理）

１９７７０－１：３ｒｄ開発会議（11/26-27）

国際会議出席報告書

2015年11月25日

委員会名：SC7/WG21
報告者氏名（富士通）：高橋快昇

１．開催場所：ローマ（イタリア）

２．開催期間：2015.11.26-2015.11.30　（11/26-27 :19770-1 3rd 開発WG会議）

３．参加国数／出席者数：
19770-1 3rd 開発WG会議：　４カ国，１２名　英，米，伊，日本（相田，篠田，高橋快昇）が参加
WG21 中間会議：議長(Roger Cummings，米)，セクレタリ(Peter Beruk，米)，米，英、独、ブラジル、アイルランド，伊、日本，BSI，TagVolt, IAITAM, NIST、SAMAC。

４．特記事項：

４．１　19770-1 開発会議

1）当面のスケジュール

a. F2F 会議の修正結果の配信（添付）
b. 11 月 15 日までにレビューコメント（特に SC27 WG1）
c. 11 月 12 日の-1 開発チームの会議で CD までの詳細スケジュールの承認
d. 11 月 19 日の Tel 会議の延期（11/12 の会議で 12 月 9 日に決定）

2）WD の主要問題に対する議論

a. information assets について

1) 情報資産（例えば、DB の内容とか知的所有権）は扱わないことを 1.1“Purpose”の注で明記する.
2) 個人情報のような IT 資産で管理される情報のリスクは ISO/IEC 27000 を参照すべきと言う注を 6.1.2 “IT asset risk assessment”c)に追記する.

b. リスクの扱いについて

33001 の流れを採用している 27001 に合わせ、6.1.2“IT asset risk assessment”と 6.1.3“IT asset risk treatment”を追加し、55000 で書かれた 6.2.4.k)の‘risk’を取る。

c. セキュリティ管理について

「セキュリティ管理」を「リスク管理」に変更するかという議論があったが、IT 資産のリスク管理はセキュリティ管理やライセンス管理も含まれるので 8.4 ライセンス管理が節としてある限り、「セキュリティ管理」を別物とし

て残すことになった。

d. 承認（Authorization）に関する要求事項

承認と承認の実行の監査証跡だけでなく、所有権と責任についてもそのトレーサビリティを追記し、所有権のない IT 資産についても組織内で利用される場合は合わせて報告することを 7 節に追記し、 8.3 データ管理で SANS/CIS critical security controls で言っている、承認されていない資産もデータ管理の対象であることを明示する。

e. 資産の改竄について

Annex B のセキュリティ管理の記述を以下のようにした。“セキュリティ管理プロセスの目的はスコープ内のすべての IT 資産のために IT 資産管理の活動における情報セキュリティを管理し、承認された要求事項を支援すること。特にアクセスと統合コントロールに注意すること。ソフトウェアだけでなくハードウェアを含むすべての IT 資産とその情報について適用すること。このプロセスは、セキュリティ要求事項の遵守に関する検証も含んでいる。”

f. 物理（Non-IT）資産にない IT 資産の特徴と要求事項

1.1“Purpose”の注で組込みソフトやファームの管理にこの規格が適用できるかどうかは明らかではないことを書いておくことになった。

g. Media の記述について

Media の管理は、以前の 19770-1 では述べられていたが今回記述がなかったが、明確に記述することになり、以下の注記を 4.3“Determining the scope of the IT asset management system”に追加した。

NOTE The IT asset portfolio is the collection of all IT assets that are to be managed by the IT asset management system. It will typically include for example hardware, software, media (physical and electronic), and entitlement information, possibly limited by platform, publisher, or other criteria. See ISO 55000 3.2.4.

h. Business continuity の記述について

事業継続のリスクは 6.1.2“IT asset risk assessment”でリスクアセスメントで注目する一つであることを明記することになった。

i. 8 節、9 節の構造について

i. Annex B で機能プロセスと検証プロセスを統合させる
ii. 機能プロセスに ‘other risk management’を追記する。
iii. セキュリティ管理を tier 3 にする。
iv. ‘retirement’ を ‘repurposing/retirement’にする。

まだ、継続審議中。

j. ソフトウェア資産と IT 資産の定義

WG21 に提案する

3）その他

- Tier を改版でどうするかについて提議された。4 レベルでよいのか？3 レベルにすべきでは？
  その後、3 層にすることで決定。

４．２ WG21 中間会議

1）19770-5 Edition 2 (Overview & Vocabulary) の状況
8/1 に出版されているが、http ://standards.iso.org/ittf/PubliclyAvailableStandards で無償参照できる。
今回、新たに 19770-1 から IT asset, ITAM などの提案を受け一緒に検討した。案は 19770-1 3rdWD に採用された。

2）19770-7 (Tag Management) の状況
IT 資産のライフサイクルに沿ったテクニカルレポートとして目次案が出てきた。

3）19770-4 (Resource Usage Measurement) の状況
－２に合わせて Tag を見直しと SAM から ITAM への変更を行い WD を執筆中ている。
IBM での RUM 収集と状況表示のデモンストレーションが行われた。

4）19770-3 (Entitlement Schema) の状況
Metric 要素が追加された、これは前回の DIS 投票でライセンスの検出方法が書けないといったコメントは日本と UK から出ていたがこれに対応した要素である。
日本は、Quantification の要素の中で Meta 的に定義しようとしていたが、正式に Metric 要素は定義された。

5）19770-2 Edition 2 (SWID Tag) の状況
IBM でリリースされる全製品に対して Tag への対応が行われているとの報告があった。

6）19770-1 Edition 3 (IT Asset Mgmnt Sys Reqs) の状況
上記 DG 会議の状況を篠田委員から報告。

7）19770-22 (Asset Management info use for Cyber Security) の状況
“Guidance for the use of 19770-2 Software Identification Tag information in Cyber Security” の NWIP のドキュメントがレビューされ承認された。

8）WG21 の Strategic Plan (Rev 9.5 N1502) を今回のミーヒング内容を反映し修正した。

５．今後の開催予定

- ✓ Plenary Meetings：2016-05 中国（確定）、2017-05 マレーシア（確定）、2018-05 インド（確認中）
- ✓ Interim Meeting ：2016-10 ドイツ（確認中）

以上.