

# SC 27リエゾン報告

2020/11/9（月）

SC27専門委員会 委員長

渡邊 創（産業技術総合研究所）

# ISO/IEC JTC 1/SC 27概要

- SCタイトル : Information security, cybersecurity and privacy protection
- WG構造
  - WG 1: 情報セキュリティマネジメントシステム
  - WG 2: 暗号とセキュリティメカニズム
  - WG 3: セキュリティ評価基準
  - WG 4: セキュリティコントロールとサービス
  - WG 5: アイデンティティ管理とプライバシー技術
- 国際会議開催 : 総会:1回/年、WG:2回/年 → **WG + 総会:2回/年へ**
- 2020年4月20日から24日 WGのみ バーチャル (サンクトペテルブルク)
- 2020年9月12日から9月16日 WG + 総会 バーチャル (ワルシャワ)
  - ・ 総会は27ヶ国91名、WG参加者数は、WG 2,3,4は50人程度、WG 1,5は100人程度

# WG1, WG2

## WG1

- ISMSと関連規格を順次かつ継続的に改訂中。
  - ▶ 27002:情報セキュリティ管理策の実践のための規範 CD
  - ▶ 27005:情報セキュリティのリスクマネジメント CD
  - ▶ 27011:27002に基づく通信機関の情報セキュリティ管理策の実践の規範 WD
  - ▶ 27014:情報セキュリティガバナンス FDIS

## WG2

- PWI: Fully Homomorphic encryption
  - ▶ 準同型暗号 (Homomorphic encryption) : ISO/IEC 18033-6は存在。
  - ▶ 実用性、他の規格との整理等、検討が必要という意見多数。
  - ▶ 現状の整理をすることに。

## WG 3

- ISO/IEC 15408シリーズ：ITセキュリティの評価基準
  - ▶ IT製品のセキュリティ評価認証のためのコモンクライテリア（CC）のISO化。
  - ▶ WG 3の中心的プロジェクトで5パート構成。3つの関連プロジェクトも進行中。
  - ▶ 2008年及び2009年に出版された版の改訂、現在FDIS段階。
- ISO/IEC 19989シリーズ：バイオメトリック製品のセキュリティ評価基準と評価方法
  - ▶ バイオメトリック製品のISO/IEC 15408に基づくセキュリティ評価、3パート構成。
  - ▶ 経済産業省事業の成果を基に、日本が中心になって活動。3パートともに9月に出版。
- ISO/IEC 23837シリーズ：量子鍵配布のセキュリティ要件、テスト及び評価手法
  - ▶ 要件(Part 1)、評価及びテスト手法(Part 2)がCD段階に。
  - ▶ 中国からの提案。

## WG 4

- ISO/IEC PWI 5689 Security reference architecture for cyber-physical systems (CPS)
  - ▶ METIサイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)を提案。
  - ▶ 既存規格との差分とScopeの明確化が必要。PWI継続。
  - ▶ 中間会合を12月に2日間開催予定。
- ISO/IEC 27400 Cybersecurity – IoT security and privacy – Guidelines
  - ▶ 「IoTセキュリティガイドライン」（IoT推進コンソーシアム、総務省、経済産業省）の内容を日本から提案。
  - ▶ ドラフトにセキュリティの管理策として記載。
  - ▶ 3rd CDを作成することに。

## WG 5（国内主査はTC 68国内委員会委員でもある崎村氏）

- 金融サービスのためのプライバシーガイドラインがNWIPへ
  - ▶ その他、金融機関にも適用可能なプライバシー関連のプロジェクトが6件進行中。
- ISO/IEC 29003 Identity Proofing（eKYCとも関連）は、TSで出版するか、ISに切り替えるか、改訂してISにするかを議論。
  - ▶ ID管理関係では、ISO/IEC 29115 Entity authentication assurance frameworkの改訂がキャンセルされ、2つのPWIを開始。
- ISO/IEC 24745 バイオメトリック情報保護は、DISへ
  - ▶ エディタは韓国で、TC 68/SC 2/WG 13のISO 19092と連携。用語定義の一部は、ISO 19092で活用予定。
  - ▶ バイオメトリクス関係では、モバイルデバイスでのバイオメトリクスを使った認証のセキュリティ要件のプロジェクトISO/IEC 27553も進行中。エディタは中国（TC 68/SC 2/WG 13でもエディタを担当するアリペイ技術者）。
- ISO/IEC 29184 Online privacy notices and consent
  - ▶ 2014年10月に経済産業省が公表した「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」をベースに日本が国際規格案を提案。
  - ▶ 2020年6月に発行。