ITU-T SG17第2回会合報告

株式会社KDDI総合研究所
ユーザブルトラストグループ
グループリーダー
磯原（いそはら）　隆将（たかまさ）

株式会社KDDI総合研究所
リスクマネジメント・DX推進部
部長
三宅（みやけ）　優（ゆたか）

1. はじめに

ITU-T SG17（セキュリティ）の第2回会合が、2025年12月3日（水）～11日（木）に、スイス（ジュネーブ）のITU本部において開催された。この会合には、日本からの28名を含む、54か国・諸機関の408名（現地参加224名、リモート参加184名）が参加した。提出された寄書は221件（うち日本から、カナダと共同提出の寄書1件を含む9件）で、627件の臨時文書（Temporary Document）が発行された。なお、第1回会合と同様に、今回の会合もリモート参加が可能であり、リモート参加については、Working Partyレベルまでの議論には参加が可能であるが、Study Groupのオープニング、クロージングの各プレナリセッションにおける合意形成には参加できないとされた。

2. SG17全体に関わる結果

2.1　課題再編に関するSG17での合意形成

2025年4月の第1回SG17会合以降、課題再編と活動の近代化の議論を目的とするコレスポンデンスグループCG-RES-MODERNにおいて、課題再編の議論が進められた。本会合では、この議論に基づく課題再編案として、課題3と課題10を統合した新たな課題10の設立、AIセキュリティに関する新たな課題（課題16を予定）の設立とこれに伴う課題7の役割の改訂について、SGレベルでの合意が形成された。この再編案はTSAGに送られ、承認を経た後に、次回のSG17会合から新しい体制として確立される予定である。課題3と課題10の統合の理由は、1）セキュリティマネジメントとデジタルID管理の技術的重複が増加しており統合した審議体制が合理的であること、2）Agentic AI等の進展によりセキュリティマネジメントとデジタルID管理の更なる連携の必要が見込まれること、3）これら技術的潮流を踏まえた課題数の削減はSG17の活動の近代化を推進する手段として合理的であることに整理される。今回の会合では、これらの内容が日本とカナダの共同提案の寄書として入力された。また、AIセキュリティに関する新たな課題の設立と課題7の役割の見直しの背景には、AI関連の新規ワークアイテムが課題7を筆頭に、課題4、課題8、課題10など複数の課題に分散する状況で急増していることがある。そのため、AIセキュリティを扱う専門の課題を設立し、AI関連の審議の一元化と、関連標準化団体との調整の明確化を図り、同時に、課題7の活動をアプリケーションセキュリティやサービスセキュリティに集中させることを狙いとしている。また、Agentic AIとデジタルID管理に関連するワークアイテムの議論については、前述した課題3と課題10が統合された新たな課題10との連携を強化して勧告成立に取り組むこととしている。

2.2　SG17の活動の近代化を検討する特別セッション

SG17活動の近代化の検討に関連する特別セッションが開催された。本セッションでは、前回のSG17会合以降、13回のe-meeting会議を実施したコレスポンデンスグループCG-RES-MODERNの活動の成果に基づく議論が行われた。CG活動では、2.1に述べた課題再編のほか、会合の開催形式の改革案として、中間会合、ワークショップ、WPプレナリ会合を一堂に会して実施するContent Weekと称する会合を、SG17プレナリ会合の間に実施する案などを中心とする2028年までの会合開催計画等が議論された。今回の特別セッションでは、それらの内容が報告されるとともに、Content Weekの実施が承認された。また、2026年6月のSG17会合までを期限とするCG活動を継続することとなった。CG活動の共同コンビナーは、引き続き、SG17議長、日本、中国及び韓国が務める。

3. 会合の主な審議内容と結果

3.1 WP1：デジタルID、量子ベースのセキュリティ、PKI及びセキュリティ基盤技術

WP1は、ID管理とテレバイオメトリクスのアーキテクチャ及びメカニズムを検討する課題10、安全なアプリケーションを支援するための基盤技術を検討する課題11及び量子ベースのセキュリティを検討する課題15から構成されている。

- 課題10では、X.1250rev（Baseline capabilities for enhanced identity management and interoperability）がTAP投票を経て合意された。X.1280rev（Framework for out-of-band mutual authentication using mobile devices）、X.1901（Information security, cybersecurity and privacy protection—Age assurance systems—Part 1：Framework）、X.1286（Access control platform using distributed ledger technology（DLT）-based authentication method）がデターミネーションされ、X.1096（Requirements for biometric variability management）、X.1268（Framework for out-of-band physical access control systems using beacon-initiated mutual authentication）、X.2310（Security requirements for decentralized identity management systems using distributed ledger technology）、X.1097（Telebiometric authentication using speaker recognition）、X.1098（Telebiometric authentication based on information splitting）がコンセントされた。さらに、新規ワークアイテムとして、DLTを用いた金融認証の実装指針であるX.sup-dsa（Implementation guidelines for DLT-based secure authentication in digital financial services）、リモート／クラウド電子署名の安全性と相互運用性を定義するX.remote-qes（Security and interoperability framework for remote and cloud qualified electronic signatures）、エージェントAIのID管理に必要な用語と設計原則を示すX.dpidm-aAI（Terminology and Design Guidelines for Agentic AI Identity Management）、DID（Decentralized Identifier）における選択的開示の実現に必要なセキュリティ能力を定義するX.sc-sd（Security capability for implementing selective disclosure system in the decentralized identity system）、VCデータフォーマットの相互運用性を確保するための指針であるX.sg-dfivc（Security guidelines for data format interoperability of verifiable credential in decentralized identity system）、人・組織・AIを含むグローバルなID相互運用の課題を整理するXSTR.gidi（Globally Interoperable Digital Identity（including Humans/Entity/Non-Humans i.e. Agentic AI））、高セキュリティAPI向けのOAuthベースのプロファイルであるX.f2sp（FAPI 2.0 Security Profile）、FAPI 2.0における攻撃者モデルを定義するX.f2am（FAPI 2.0 Attacker Model）が設立された。
- 課題11では、新規ワークアイテムとして、量子時代への移行準備に関するベストプラクティス指針であるXSTR.qrbp（Quantum Readiness, Best Practices and Guidelines）、暗号アルゴリズム移行の一般手法を定義するX.migration（Generic methods for migration of cryptographic algorithms）、ディレクトリの安全な操作プロトコル仕様を改訂するX.510rev（The Directory–Protocol specifications for secure operations）、特権管理基盤を独立した枠組みとして定義するX.pmi（The Directory：Attribute certificate framework）、公開鍵証明書と属性証明書の枠組みを更新するX.509rev（The Directory：Public-key and attribute certificate frameworks）、鍵管理とPKI運用の仕様を改訂するX.508rev（The Directory：Key management and public-key infrastructure establishment and maintenance）が設立された。
- 課題15では、X.1711（Framework of quantum key distribution（QKD）protocols in QKD network）、X.1718（Security requirements for Quantum Key Distribution Network interworking）がコンセントされた。さらに、新規ワークアイテムとして、QKDNを連結モデルで相互接続する際のセキュリティ要件を定義するX.sec_QKDNi_ccm（Security requirements and measures for quantum key distribution network interworking–Concatenated model）、QKDNへゼロトラストを適用した場合の技術的影響を整理するテクニカルレポートXSTR.QKDN-nq-ZTA（Technical implications of applying zero trust architecture into quantum key distribution network）、QKDNとユーザネットワーク統合時のセキュリティ要求を明確化するX.sec-QKDN-un-req（Security requirements and measures for the integration of quantum key distribution network and user network）が設立された。

3.2 WP2：国際移動通信システム、IoT、ITS/コネクテッド自動運転車のセキュリティ

WP2は、各種サービスに必要とされるセキュリティアーキテクチャとフレームワークを検討する課題2、電気通信

サービス、IoT、デジタルツイン及びメタバースのセキュリティを検討する課題6及び高度道路交通システム（ITS：Intelligent Transport Systems）とコネクテッド自動運転車（CAV：Connected Autonomous Vehicle）のセキュリティを検討する課題13から構成されている。

- 課題2では、X.1821（Guidelines and technical requirements for the analysis of IMT-2020/5G network asset security risk）がデターミネーションされた。また、テクニカルレポートXSTR.sd-cnc（Data security guidelines for coordination of networking and computing）、XSTR.sg-lmcs（Security requirements and guidelines of DLT-based lifecycle management for computing services）の発行が合意された。さらに、新規ワークアイテムとして、コンピューティングパワーネットワーク取引プラットフォームのセキュリティ要求を定義するX.cpn-tp-sec（Security requirements and capabilities of computing power network transaction platform）、コンピューティングパワーネットワークゲートウェイのセキュリティ要求と強化アーキテクチャを定義するX.cpn-gw-sec（Security requirements and security-enhanced architecture of the CPN gateway）、IMT-2020以降におけるネットワークとコンピューティング協調のセキュリティ要求を整理するX.5Gsec-CNC（Security requirements and guidelines for Coordination of networking and computing in IMT-2020 networks and beyond）、通信事業者向けセキュリティテストベッドの機能アーキテクチャを定義するX.fast（Functional Architecture of Security Testbed for Telecommunication Operators）が設立された。
- 課題6では、X.1128（Security features to assess mobile terminal security）とX.1129（Security guidelines for mobile terminal integrity protection）がTAP投票を経て合意され、X.1350（Security requirements for the industrial Internet of things in smart manufacturing）がデターミネーションされた。また、XSTR.trust-metaverse（Technical challenges to achieving trustworthy metaverse）の発行が合意された。さらに、新規ワークアイテムとして、信頼できるデータ利用に基づきメタバースの信頼性を確保するための構成要素の要件を規定するX.tdu-mv（Requirements for components of trusted data use in building a trustworthy metaverse）、太陽光発電システムのセキュリティ脅威を明らかにしセキュリティ要求を定義するX.sr-ppgs（Cybersecurity requirements for photovoltaic power generation system）、DLTを用いたeSIM搭載IoT機器の認証におけるセキュリティ考慮事項を示すテクニカルレポートXSTR.sec-Dba-eSIM（Security considerations for DLT-based authentication of IoT devices with eSIM）、メタバース及びデジタルツインに関するセキュリティ標準化動向・ギャップ分析・方向性を示すテクニカルレポートXSTR.MVDTsecRM（Metaverse and digital twin security standardization roadmap）、IoTセキュリティ標準化の全体像を整理し課題と今後の方向性を示すテクニカルレポートXSTR.IoTsecRM（IoT security standardization roadmap）が設立された。
- 課題13では、新規ワークアイテムとして、会計ベースのチケッティングにおける脅威・脆弱性を分析しセキュリティ要求と実装指針を示すX.abt-sec（Security guidelines for accounting-based ticketing in intelligent transport systems）と車載ネットワークに対する最新の脅威と検知手法を反映してIDSガイドラインを改訂するX.1375-rev（Guidelines for an intrusion detection system for in-vehicle networks）が設立された。

3.3 WP3：サイバーセキュリティと管理、セキュリティ戦略とコーディネーション

WP3は、SG17の運営に関わるコーディネーション（全体の進捗管理や課題間の調整など）及びITU-T全体のセキュリティに関わるコーディネーションを主な目的とする課題1と、ISO/IEC JTC1 SC27との連携をベースとして電気通信における情報セキュリティマネジメントとセキュリティサービスについて検討する課題3及びサイバーセキュリティとスパム対策について検討する課題4から構成されている。

- 課題1では、セキュリティコンペンディウム、セキュリティロードマップ及びSG17のWTSA決議への対応状況に関する文書が合意された。さらに、新規ワークアイテムとして、サイバーセキュリティ標準化に向けた戦略とロードマップを示すテクニカルレポートXSTR.CRAMMS（Cyber Security Reference Architectures, Methodologies, Models and Strategies Roadmap）、ユーザーの信頼を高める同意管理のフレームワークを定義するX.te-consent（Framework for Trust Enhancing Consent Management）、ソフトウェアのサイバーレジリエンスを保証するための枠組みを規定するX.crta（Framework for Cyber Resilience Testing and Assurance）、赤十字国際委員会が提唱する「デジタル保護標章」の国際標準化について整理するテクニカルレポートであるXSTR.diem（Technical

Report：Digital International Humanitarian Law Emblems)、OT（Operational Technology）資産の不適切な露出問題をデジタル・エンブレムで緩和するアプローチに関するテクニカルレポートであるXSTR.diem-assets (Digital emblems as a key solution in resolving the issue of inappropriately exposed OT assets in the cyber space)、端末やサービス間で一貫したペアレンタルコントロールを実現する共有原則を扱うX.PARCEP (Interoperable Parental Control Enforcement Principles for Child Online Protection）が設立された。

- 課題3では、X.1062（Framework for human capability development in information security）がTAP投票を経て合意され、X.1060-rev（Cyber Defence/Cyber Security Centre framework）がコンセントされた。さらに、新規ワークアイテムとしてAIシステムを安全かつ信頼性高く導入・運用するためのAIセキュリティ管理の包括的フレームワークを提供するテクニカルレポートXSTR.AIsmf（AI Security Management Framework）が設立された。
- 課題4では、X.1238（Guidelines for countering spam over rich communication service（RCS）messaging）がTAP投票を経て合意された。X.2105（Security threats to the software supply chain）がデターミネーションされ、X.2014（Guidelines of using digital twin of network for network security）とX.1560（Security framework for network storage protection against malware attacks）がコンセントされた。さらに、新規ワークアイテムとして、Security as a service領域におけるセキュリティ要件を定めるX.SecaaS-Req（Security requirements in the domain of security as a service)、生成AIサービスに関するセキュリティインシデント管理の指針を示すX.sim-gai (Guidelines for security incident management of generative artificial intelligence services)、エンドツーエンド暗号化がプライバシー及び中央集権化に与える影響を分析するテクニカルレポートXSTR.e2ecis（Impact of End-to-End Encryption on Privacy and Centralization)、AIを利用したサイバーセキュリティシミュレーションプラットフォームの構築と分析を行うテクニカルレポートXSTR.da-AIcsp（Development and Analysis of an AI-Based Cybersecurity Simulation Platform)、2036・2038・2106年などのタイムスタンプロールオーバー問題に関する国際的な調整要件を整理するテクニカルペーパーXSTP.epoch（Technical Paper on Global Coordination Requirements for 2038-class rollover events（including but not limited to 2036, 2038, 2106））が設立された。

3.4 WP4：AI及びクラウドコンピューティングサービスとアプリケーションのセキュリティ

WP4は、安全なアプリケーションサービスの実現に寄与する技術を検討する課題7、クラウドコンピューティングとビッグデータ基盤のセキュリティを検討する課題8及び分散台帳技術（DLT：Distributed Ledger Technology）のセキュリティを検討する課題14から構成されている。

- 課題7では、X.1130（Technical guidelines for fraud detection of malicious applications in mobile devices）とX.1457（Security threats and requirements for information recommendation service）がTAP投票を経て合意された。X.2210（Implementation guidelines for digital watermarking）とX.1910（Technical capabilities of interactive deception risk detection）がデターミネーションされた。また、テクニカルレポートXSTR.AIsec（Artificial intelligence security standardization overview)、XSTR.dpama（A landscape analysis for data protection of avatars in metaverse applications)、XSTR.saAIoT (Security Threat Analysis for Artificial Intelligence of Things on Devices)、XSTR.se-AI（Security Evaluation on Artificial Intelligence Technology in ICT）の発行が合意された。さらに、新規ワークアイテムとして、生成AIの学習・推論段階におけるデータやり取りのセキュリティ要件を定めるX.rg-dis（Requirements for guidelines for data interaction security in training and inference stages of Generative Artificial Intelligence)、AIエージェントに対するセキュリティ評価手法をまとめるテクニカルレポートXSTR.sem-AIA（Security evaluation methods for artificial intelligence agent)、基盤モデルのセキュリティベンチマーク指針を示すテクニカルレポートXSTR.AI-GSB（Guidelines of security benchmark for foundation models)、マルチエージェントシステムによるアプリ脆弱性検知のガイドラインを示すX.gavd-mas（Guidelines for application vulnerability detection based on multi-agent system)、機密コンピューティングを用いたLLMのデータセキュリティ指針を定めるX.LLMCC（Guidelines for Large Language Model data security based on Confidential Computing)、端末上のAIマルチエージェ

ントシステムに関するセキュリティ要件を定めるX.sr-taimas（Security requirements for terminal-based artificial intelligence multi-agent system）、Agentic AI における信頼・リスク・セキュリティのランドスケープを整理するテクニカルレポートXSTR.ltf-AAI（Landscape of Trust Framework for Agentic AI）、AIベース画像生成システムの脅威・要件・保護策を示すX.srg-AIgis（Security requirements and guidelines for artificial intelligence-based image generation system）、具現化AIシステムの特有脅威と要求事項を示すX.sg-eAI（Security requirements and guidelines for embodied artificial intelligence systems）、インテリジェントカスタマーサービスのセキュリティ要求と評価指針を示すX.sreg-ICS（Security Requirements and Evaluation Guidelines for Intelligent Customer Services）、生成AIデータライフサイクル全体のセキュリティ指針を示すX.sg-GenAId（Security Guidelines for Generative Artificial Intelligence Data Life Cycle）が設立された。

- 課題8では、X.1753（Guidelines for data security using machine learning in big data infrastructure）、X.1649（Security guidelines for multi-cloud）、X.1631rev（Information security, cybersecurity and privacy protection—Information security controls based on ISO/IEC 27002 for cloud services）がTAP投票を経て合意された。X.1651（Framework of Security Orchestration, Automation and Response for cloud computing）、X.1607（Requirements of Attack Surface Management for cloud computing）がデターミネーションされ、X.1416（Security requirements and framework of collaboration service for multiple blockchain as a service platforms）がコンセントされた。さらに、新規ワークアイテムとして、AIクラウドプラットフォームのセキュリティ要件であるX.sr-aicp（Security Requirements for Artificial Intelligence Cloud Platform）、AI強化型協調クラウドインフラのセキュリティ要件であるX.sr-AIec（Security Requirements for AI-Enhanced Collaboration in Cloud Computing Infrastructure）、ビッグデータインフラ横断データ共有のセキュリティガイドラインであるX.sgds-bdi（Security guidelines for data sharing across big data infrastructures）が設立された。
- 課題14では、X.1418（Security guidelines for DLT-based digital collection services）、X.1417（Security requirements for DLT data on permissioned DLT-based distributed power trading systems）がデターミネーションされ、X.1400rev（Terms and definitions for distributed ledger technology）がコンセントされた。さらに、新規ワークアイテムとして、分散型台帳技術に関するセキュリティ標準化のロードマップを整理・更新するテクニカルレポートXSTR.SR4DLTsec（Standardization roadmap for DLT security）が設立された。

4. 今後の会合の予定

次回のSG17会合は、2026年6月2日（火）～11日（木）にスイス（ジュネーブ）で開催される。これまでの間に、ISO/IECと共同で開発される勧告案の承認のため、2月6日（金）と4月9日（木）にe-meeting形式のSG17プレナリ会合を開催する。また、SG17活動の近代化の一環として、各課題の中間会合とデジタルIDに関するワークショップ及びWPプレナリ会合を合同で実施する独自の取組みとなるContent Week会合が2026年3月30日（月）～4月2日（木）にスイス（ジュネーブ）で開催される。

次回までに開催されるプレナリ会合と中間会合等の予定を、表1と表2にそれぞれ示す。

■表1. 今後のプレナリ会合の予定

会合名	開催期間	開催地	会合内容
SG17プレナリ会合	2026年2月6日	e-meeting	X.1058revのデターミネーション
第1回 SG17 Content Week	2026年3月30日～4月2日	ジュネーブ	各課題の中間会合（詳細は表2を参照） WP1プレナリ会合 WP2プレナリ会合 WP3プレナリ会合 WP4プレナリ会合 デジタルIDワークショップ
SG17プレナリ会合	2026年4月9日	e-meeting	X.1901のデターミネーション

■表2. 今後の中間会合の予定

会合名	開催期間	開催地	会合内容
課題1中間会合	2026年3月4日	e-meeting	トラスト関連及び課題1のワークアイテムの審議
課題1中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	トラスト関連の審議
課題2中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	XSTR.FMSC-IMT2030, X.ztmc, XSTR.sa-ran, XSTR.sec-int-cpc and XSTR.srsecの審議 新規WI候補検討
課題3中間会合	2026年2月2日	e-meeting	X.1058rev TAP審議結果の共有
課題3中間会合	2026年2月4日	e-meeting	X.cdc-csirt の審議
課題4中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	課題4のワークアイテムの審議
課題6中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	JCG-IoTSec関連の審議
課題7中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	AIセキュリティを含むアプリケーションセキュリティに関する勧告案の審議
課題7中間会合	2026年5月	e-meeting	AIセキュリティ戦略に関する審議
課題8中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	課題8のワークアイテムの審議 新規ワークアイテム候補の審議
課題10中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	X.srm-sscを含む課題10のワークアイテムの審議
課題10中間会合	2026年5月	e-meeting	課題10のワークアイテムの審議
課題11中間会合（Joint RGM）	2026年4月13日～17日	ソウル（大韓民国）	ISO/IEC JTC1/SC6/WG10との合同会議
課題13中間会合	2026年3月30日～ 4月1日	ジュネーブ+e-meeting	X.idse, X.af-sec, X.evpnc-sec, X.fod-secの審議 課題13のワークアイテムの審議 新規ワークアイテムに関する審議
課題13中間会合	2026年7月8日～9日	ソウル+e-meeting	課題13のワークアイテムの審議 新規ワークアイテムに関する審議
課題14中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	課題14のワークアイテムの審議 新規ワークアイテム候補の審議
課題15中間会合	2026年3月30日～4月1日	ジュネーブ+e-meeting	TR.kdc_qkdn、TR.QKDN-SPの審議 新規ワークアイテムに関する審議
課題15中間会合	2026年4月27日～30日	日本	TR.kdc_qkdn、TR.QKDN-SPの審議 課題15のワークアイテムの審議
SG17会合	2026年6月2日～11日	ジュネーブ	

5. おわりに

今回のSG17会合には、408名の参加者が集まり、221件の寄書の入力を記録し、いずれも過去最高を更新した。参加者については、招待された専門家が前回の9名から37名へと大幅に増加した。また、新規セクターメンバーとして、ThalesやAmazonなどの4組織が加わり、セキュリティの標準化を推進する団体としての今後の価値向上が期待される。新規ワークアイテムについては、提案65件のうち85%にあたる55件が承認された。これらは、Agentic AIや生成AI、デジタルIDやトラスト、クラウドなど、セキュリティ標準化が重要な技術に関するものが多く含まれる。こうしたポジティブな状況を更に加速させるために、CG-RES-MODERNでは、標準化活動の効率化や成果物の品質向上、関連標準化団体や産業界との連携強化、活動の可視化を柱とし、「近代化」を掲げた将来のSG17の在り方を検討・決定していく。日本としては、共同コンビナーの役割を最大限に活用・発揮し、世界における日本の存在感と影響力を維持・向上させるとともに、セキュリティ技術の標準化を通じて、安全・安心な情報社会の実現に貢献していく。