ITU-T SG17第1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

いそはら　たかまさ
磯原　隆将

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

みやけ　ゆたか
三宅　優

1. はじめに

ITU-T SG17（セキュリティ）の第1回会合が、2025年4月8日（火）～17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19名を含む、57か国・諸機関の374名（現地参加164名、リモート参加210名）が参加した。提出された寄書は189件（うち日本から6件）で、503件の臨時文書（Temporary Document）が発行された。なお、第6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 SG17の新体制

WTSA-24の結果、前会期まで副議長を務めた英国のTaddei氏が新議長に、また、日本の磯原（KDDI）を含む12名が副議長に選出された。12の研究課題（Question）はそのまま継続することが承認された。

新研究会期の初会合となる今回の会合では、WP構成や各課題ラポーターの選任など、SG17の体制に関する議論が行われた。WPの構成については見直しが行われ、5WP体制から4WP体制に変更した。**表1**にSG17の新体制を示す。

表1. SG17の新体制（敬称略）

SG	WP	課題	タイトル	議長／ラポーター	副議長／アソシエイトラポーター
17			Security セキュリティ	Arnaud Taddei（英国）	Samir Abdelgawad（エジプト） Laial Almansoury（クウェート） Afnan AlRomi（サウジアラビア） Farkhad Belonogov（ウズベキスタン） Abdenour Bourennane（アルジェリア） 磯原 隆将（KDDI） Honey Makola（南アフリカ） Kwadwo Osafo-Maafo（ガーナ） Michael Rosa（米国） Preetika Singh（インド） Liang Wei（中国） Mahmut Esat Yildirim（トルコ）
	1		Digital identity, Quantum based security, PKI and Fundamental security technologies 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	Debora Comparin（フランス）	Afnan AlRomi（サウジアラビア） Honey Makola（南アフリカ）
		10	Identity management and telebiometrics architecture and mechanisms 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	Abbie Barbir（米国） 武智 洋（NEC）	Jason Kim（韓国） Keundug Park（韓国） Junjie Xia（中国）
		11	Generic technologies to support secure applications 安全なアプリケーションを支援するための基盤技術	Jean-Paul Lemaire（フランス）	
		15	Quantum-based security 量子ベースのセキュリティ	釼吉 薫（NICT）	Hyung-Soo（Hans）Kim（韓国） Hao Qin（シンガポール）
	2		Security of IMT, IoT, metaverse and ITS/CAV IMT、IoT、メタバース、ITS/CAVのセキュリティ	Bret Jordan（米国）	三宅 優（KDDI）
		2	Security architecture and network security 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	磯原 隆将（KDDI） Heung Ryong Oh（韓国）	Ke Wang（中国）

		6	Security for telecommunication services, Internet of Things（IoT）, digital twin, and metaverse 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	Jonghyun Baek（韓国） Junzhi Yan（中国）	Gunhee Lee（韓国）
		13	Intelligent transport system（ITS）and connected autonomous vehicle（CAV）security 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	Sang-Woo Lee（韓国） Yi Zhang（韓国）	Seungwook Park（韓国）
	3		Cybersecurity and management, security strategy and coordination 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	Changoh Kim（韓国）	Xiaoyuan Bai（中国） Mahmut Esat Yildirim（トルコ）
		1	Security standardization strategy, incubation and coordination 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	Zoe Sungchae Park（韓国） Chen Zhang（中国）	Juhee Ki（韓国） Yiwen Wang（中国）
		3	Telecommunication information security management and security services 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	永沼 美保（NEC）	Thaib Mustafa（マレーシア）
		4	Cybersecurity and countering spam サイバーセキュリティとスパム対策	Yanbin Zhang（中国）	Vincent Mwesigwa（ウガンダ）
	4		Security of AI, cloud computing services and applications 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	Zhiyuan Hu（中国）	Jae Hoon Nah（韓国）
		7	Secure application services 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	Feng Gao（中国） Jae Hoon Nah（韓国）	Lijun Liu（中国） 高橋 健志（NICT）
		8	Cloud computing and big data infrastructure security 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	Fangfang Dai（中国）	
		14	Distributed ledger technology（DLT）security 分散台帳技術（DLT：Distributed Ledger Technology）のセキュリティ	Kyeong Hee Oh（韓国）	Xiaoyuan Bai（中国）

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、会合期間中に4回開催された。一連のセッションでは、WTSA-24以降、今回のSG17プレナリ会合までに活動が行われたCorrespondence Group on SG17 Restructuring（CG-RES）の活動報告が行われたのち、近代化についての議論が行われた。一連の議論では、近代化の5つの柱として、SG17議長より、運営の効率化、成果物の品質、ITU内外の関連標準化団体との連携の改善、可視性の向上及び産業界の誘致が掲げられている。運営の効率化の一例として、SG17関連会合の開催間隔と頻度の見直しが進められ、前研究会期はおよそ半年ごとに2週間のプレナリ会合を開催していた進行を見直し、プレナリ会合の開催間隔を8か月程度に伸ばし、次回のプレナリ会合までの間にWPプレナリ会合や中間会合の開催を行う計画が示され、これに取り組むこととなった。今後の検討の継続について、CG-RESを継承する形で設立されたCG-RES-MODERNにて行うこととされ、この共同コンビナーを、SG17議長、日本、中国及び韓国が務めることとなった。

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.1284（Authentication framework based on one-time authentication key using distributed ledger technology）がTAP投票を経て合意された。そして、X.1250rev（Baseline capabilities for enhanced identity management and interoperability）がデターミネーションされ、X.1285（OpenID Connect Core 1.0 incorporating errata set 2）がコンセントされた。また、情報セキュリティ、サイバーセキュリティ、プライバシー保護の観点から、年齢に基づく適格性判断を可能にするための枠組みをISO/IEC27566-1との共通テキストとして提供するX.aas（Collaboration between ITU-T SG17 and ISO/IEC JTC 1 SC 27 on the development of ISO/IEC 27566）、分散IDにおける信頼の伝播をサポートする

デジタルIDウォレットのセキュリティフレームワークを提供するX.sfdiw（Security framework of digital identity wallet for decentralized identity model）、X.1280の主要な技術的特徴である相互認証をタイトルと本文の両方で強調する改訂を行うX.1280rev（Framework for out-of-band mutual authentication using mobile devices）及びX.1281のID Usage APIを変更し、Authentic Sourcesアクセスに適合させることでEUDIウォレット標準化のギャップをカバーすることを目的とする拡張に関するSIAからの連絡であるX.1281.Amd1（Open Standards Identity APIs（X.1281）extension for Authentic Sources Use Case）が新規ワークアイテムとして設立された。

- 課題11では、今会合において合意された文書及び新たに設立されたワークアイテム等はなく、X.dpki（Public-key infrastructure based on block chain technology）とTR.ac-pqc（Technical Report：Guidance on use of advanced cryptography based on PQC）の新規ベースライン文書が発行された。
- 課題15では、今会合において合意された文書等はなく、衛星QKDNのセキュリティ分析と今後の標準化に関するTR.SQKDN-SC（Technical Report：Security consideration for satellite-based quantum key distribution network）が新規ワークアイテムとして設立された。

3.2　WP2：IMT、IoT、メタバース、ITS/CAVのセキュリティ

WP2は、国際移動通信システム（IMT：International Mobile Telecommunications）を含む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.1010（Guidelines for security orchestration of service access process）がコンセントされた。そして、統合センシング通信（ISAC：Integrated Sensing and Communication）に関するセキュリティガイドラインであるX.s-isac（Security guidelines for integrated sensing and communication in IMT-2020 networks and beyond）、IMT-2020向けのセキュリティ能力インテリジェントオーケストレーションシステム（SCIO：Security Capability Intelligent Orchestration）のフレームワークであるX.5Gsec-scio（Framework of Security Capability Intelligent Orchestration system for IMT-2020 Network）、IMT-2020プライベートネットワークにおけるゼロトラストモデルの適用ユースケースを特定するX.uc-zt-5g（Security threats associated with use cases for applying zero trust to IMT-2020 private network deployments）及びIMT-2030ネットワークにおけるFMSC（Fixed, mobile and satellite convergence）のセキュリティ技術を、一般的な考慮事項、潜在的なリスク、潜在的なセキュリティ技術の観点から整理するTR.FMSC-IMT2030（Technical Report：Security technologies for fixed, mobile and satellite convergence of IMT-2030 networks）が新規ワークアイテムとして設立された。
- 課題6では、X.1355（Security risk analysis framework for Internet of things devices）がTAP投票を経て合意された。そして、X.1128（Security features to assess mobile terminal security）とX.1129（Security guidelines for mobile terminal integrity protection）がデターミネーションされた。また、IoT機器におけるデータセキュリティを検証するための要件を定めるX.iot-dt（Technical requirements for verification of IoT data security）、IoTデバイス固有のRF特性を活用した継続的なデバイス認証のフレームワークを定めるX.IoT-RF-Auth（Security framework for radio frequency characteristics-based IoT device authentication）、スマートシティーにおけるメタバースの仮想空間と物理空間の統合のためのセキュリティガイドラインを定めるX.sg-eimv（Security guidelines for enabling integration of virtual and physical worlds of the metaverses in smart city）、信頼できるメタバースの特徴と実現に関する技術的課題を整理するTR.trust-metaverse（Technical Report：Technical challenges to achieving trustworthy metaverses）、メタバースにおけるサイバーセキュリティリスク、脅威及び危害を整理するTR.cr-mv（Technical Report：Cybersecurity risks, threats, and harms in the metaverse）及びAIを用いたIoTベースの電力インフラのモニタリングシステムにおける脅威分析と対策要件ガイドラインとして整理するTR.sec-iepi-AI（Technical Report：Security guideline for artificial intelligence applications of IoT-based electric power infrastructure monitoring system）が新規ワークアイテムとして設立された。

- 課題13では、X.1385（Security requirements and guidelines for telecommunications in an urban air mobility（UAM）environment）がTAP投票を経て合意された。そして、コネクティッドカーに実装される、外部接続機能を持つECU（本勧告案でecECUと呼ぶ）のセキュリティ要件を定めるX.ececu-sec（Security requirements for externally connected electronic control units of connected vehicles）、車載鍵管理機能のセキュリティ要件とガイドラインX.ivkm-sec（Security requirements and guidelines for the in-vehicle key management）及びコネクティッドカーにおける隠れチャネル（Covert channel）への対策に関するガイドラインX.cov-sec（Security guidelines for countermeasures against covert channels in connected vehicles）が新規ワークアイテムとして設立された。

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を合意した。そして、証明書のリスク評価に関するフレームワークX.rs-certi（Framework for risk assessments of server certificate applications）、ITU-T X.crammsフレームワークの開発に焦点を当てたサイバーセキュリティの参照アーキテクチャ、モデル及び方法論X.cramms（Framework for Cyber Security Reference Architectures, Models and Methodologies Strategy and Roadmap（CRAMMS））及びWTSA-24で指示されたトラストに関するアクションに基づくテクニカルレポートTR.trust（Technical Report：Trust issue for telecommunication/ICTs）が新規ワークアイテムとして設立された。
- 課題3では、X.1062（Framework for Security Human Capability Development）がデターミネーションされた。そして、X.sup-cdc（Supplement to X.1060：X.1060 high level implementation considerations）が合意された。また、通信事業者を対象にサイバー攻撃対策への成熟度のモデルのフレームワークと要件を定義するX.C2M2（Cybersecurity Capability Maturity Model for telecommunication organisations）が新規ワークアイテムとして設立された。
- 課題4では、X.1238（Guidelines for countering spam over rich communication service（RCS）messaging）がデターミネーションされた。そして、X.1646（Security threats to be identified in the domain of security as a service）がコンセントされた。また、組織のセキュリティコントロール全般を対象に基本的なアプリケーションセキュリティ管理のリストとして最小限の実行可能なセキュリティ管理（MVSC）を定めるX.MVSC（Minimum Viable Security Controls）とメールによる攻撃の評価のためのガイドラインX.sg-resso（Security guidelines for reporting email security status to security operations）が新規ワークアイテムとして設立された。

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.1456（Security guidelines for DFS applications based on USSD and STK）がTAP投票を経て合意された。そして、X.1130（Technical guidelines for fraud detection of malicious applications in mobile devices）とX.1457（Security threats and requirements for information recommendation service）がデターミネーションされた。また、X.2013（Security measures for digital twin federation in smart cities and communities）とX.2050（Security requirements for monitoring physical city assets）がコンセントされた。さらに、**表2**に整理する14件が新規ワークアイテムとして設立された。
- 課題8では、X.1648（Guideline on edge computing data security）TAP投票を経て合意された。そして、X.1753（Guidelines for data security using machine learning in big data infrastructure）、X.1631rev（Information security controls based on ISO/IEC 27002 for cloud services）及びX.1649（Security guidelines for multi-

cloud）がデターミネーションされた。また、X.1650（Security guidelines for serverless computing）がコンセントされた。さらに、クラウドサービスのDevOpsにおけるセキュリティ上の脅威と課題を説明する、クラウドサービス向けのDevSecOpsフレームワークの概要と実装に関するガイドラインX.gdso-cs（Guidelines of development, security and operations（DevSecOps）for cloud service）が新規ワークアイテムとして設立された。

- 課題14では、X.1414（Security requirements and framework of cross-chain service for DLT systems）とX.1413（Security controls for distributed ledger technology）がコンセントされた。そして、TR.dw-lasf（Technical report：A landscape analysis and security features for a digital wallet）が合意された。

■表2．課題7で設立された新規ワークアイテム一覧

略語	タイトル	概要
X.SSDHN-AI-Atk	Security Guidelines for Software-Defined Heterogeneous Networks Architecture against AI generated Attacks and Threats	メタバースやデジタルツインシステムのLLMに対する敵対的な攻撃を緩和するための実用的なガイドライン
X.APIRSD	Technical Requirements for Public API Runtime Security risk Detection	公開APIのセキュリティリスクを特定するための、能動的な検知と受動的な監視を行い、実行時のセキュリティ検知を行う技術に対する要求事項を整理
X.sec-va	Security guidelines for vertical applications within the IMT-2020 ecosystem	IMT-2020（5G）エコシステムにおいて垂直アプリケーションを運用するためのセキュリティガイドライン
X.sgfems	Security requirements and guidelines for factory energy management system	工場エネルギー管理システム（FEMS）におけるリスク分析を通じて策定するセキュリティ要件とガイドライン
X.Spud	Security requirements associated with procedures for pseudonymizing unstructured data	仮名化された非構造化データの再識別化を防ぐためのセキュリティガイドライン
TR.lzkml	Technical Report：Landscape analysis of Zero-Knowledge Machine Learning	MLとゼロ知識証明（ZKP）を組合せ、データを公開することなく検証可能な計算を可能にするゼロ知識機械学習（ZKML）を使用した安全なAI導入を保証するための暗号化アプローチ、セキュリティ脅威、ユースケース、PII保護、モデルの完全性などを整理
X.AA-LLM	Guidelines for Preventing and Mitigating Adversarial Attacks on LLMs in Metaverse and Digital Twin Environments	メタバースとデジタルツイン環境における大規模言語モデル（LLM）の安全性を確保するための実用的なガイドライン
X.S-AIA	Security Requirements and Guidelines for Artificial Intelligence Agent	AIエージェントの健全かつ持続可能な発展を促進するため、知覚・認知、計画、記憶、行動などのAIエージェントの能力に対するセキュリティ要件を提案し、その要件を満たすためのAIエージェントのセキュリティガイドライン
TR.saAIoT	Technical Report：Security Threat Analysis for Artificial Intelligence of Things on Devices	モノの人工知能（AIoT）における潜在的なセキュリティ脅威と課題を特定・分析
X.sg-sd	Security guidelines for synthetic data in the context of AI systems	AIの分野における合成データ（アルゴリズムによって生成されたシミュレーションデータ）の様々な応用シナリオに基づく、合成データがもたらすセキュリティガイドライン
TR.AISec	Technical Report：Artificial intelligence security standardization strategies	SG17におけるCG-AISECの成果をまとめ、「AIのためのセキュリティ」と「AIによるセキュリティ」の両方の側面を包含するAIセキュリティの分析を行う
X.AI-gcd	Guidelines for Artificial Intelligence generated content detection	AIが生成したコンテンツの効果的な識別を可能にするための設計、開発、展開、評価のためのガイドライン
X.GenAI-FT	Security guidelines for fine-tuning generative AI model	生成AIモデルにおけるRLHF保護除去攻撃、モデルサプライチェーン攻撃などセキュリティ上の課題に対処しモデルの安全な開発と配備を確実にするための生成AIモデルのファインチューニングに関するセキュリティガイドライン
X.AI-App_policy	Reference architecture for AI-assisted analysis of consistency between App's data usage behaviour and its privacy policy	アプリのデータ利用の実態とプライバシーポリシーの整合をAIに基づいて自動的にチェックするためのリファレンスアーキテクチャ

4．今後の会合の予定

次回のSG17会合は、2025年12月3日（水）～11日（木）にスイス（ジュネーブ）で開催される。また、SG17プレナリ会合の開催間隔の見直しに伴って、各課題における審議を適宜進行すべく、WPプレナリ会合をe-meeting形式で開催することとした。そして、2025年7月11日に、AI for Good Global Summitにおいて、AIセキュリティの現状を検討し取り組むべき挑戦を整理するワークショップ「Challenging the status quo of AI security」の開催と、2025年9月5日に、X.509に関するワークショップ「4th X.509 Day」の開催を、それぞれ予定している。

次回までに開催されるWPプレナリ会合と中間会合等の

予定を、表3と表4にそれぞれ示す。

5. おわりに

2028年までの新しい研究会期における最初の会合となった今回の会合では、参加者数、入力寄書数ともにSG17として過去最高を記録するポジティブなモメンタムを伴う形でのスタートとなった。このことは、情報通信に関するセキュリティの国際標準化が参加各国にとって重要な課題と認識されていることの表れと捉えられる。SG17がこれまでに世界に果たしてきた役割をしっかりと理解し継承する姿勢で、多くの皆様のご理解とご協力を賜りながら、世界における日本の専門家集団の存在感と技術力を示すことで、新しい技術の潮流を先導した世界の安全・安心に寄与してゆく。

■表3. 今後のWPプレナリ会合の予定

会合名	開催期間	開催地	会合内容
WP1プレナリ会合	2025年9月22日	e-meeting	X.aas｜ISO/IEC 27566-1のデターミネーション
WP3プレナリ会合	2025年10月10日	e-meeting	X.1058rev｜ISO/IEC 29151のデターミネーション
WP4プレナリ会合	2025年9月4日～5日	e-meeting	デターミネーション ・課題8：X.soar-cc, X.asm-cc ・課題14：X.sr-dpts, X.sg-dcs コンセント ・課題8：X.mbaas-cs-sec ・課題14：X.DLT-dgi, X.dlt-share, X.1400Rev 合意 ・課題7：TR.AISec, TR.saAIoT, TR.dpama

■表4. 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	2025年4月29日	e-meeting	SCV、CCT、その他SGから寄せられた定義・ターミノロジの審議
課題1中間会合	2025年10月15日	e-meeting	課題1のワークアイテムすべて
課題1中間会合	2025年11月20日	e-meeting	SCV、CCT、その他SGから寄せられた定義・ターミノロジの審議
課題2中間会合	2025年9月25日～26日	e-meeting	X.5Gsec-asra、TR.sg-lmcs、TR.sd-cnc及びTR.srsec 課題2のワークアイテムすべて
課題3中間会合	2025年9月17日～18日	e-meeting	X.1060-rev、X.gsm-dcd、X.cirt-cdc、X.C2M2及びX.srm-sup
課題3中間会合	2025年10月14日	e-meeting	X.1058-rev、X.1053-rev
課題4中間会合	2025年7月または9月	e-meeting	X.sfdtea、X.nspam、X.icd-schemas、X.st-ssc及びX.dtns
課題7中間会合	2025年7月15日～16日	e-meeting	AIセキュリティほか
課題8中間会合	2025年7月2日～3日	e-meeting	次回SG17会合に向けた審議
課題10中間会合	2025年7月8日	e-meeting	課題10のワークアイテムすべて
課題10中間会合	2025年9月15日	未定	課題10のワークアイテムすべて
課題11中間会合	2025年6月2日～6日	英国（ロンドン）	ISO/IEC/JTC 1/SC6/WG10との合同会合
課題13中間会合	2025年7月9日～10日	韓国（ソウル） e-meeting ハイブリッド	課題13のワークアイテム
課題13中間会合	2025年10月16日～17日	e-meeting または 韓国（ソウル） e-meeting ハイブリッド	課題13のワークアイテム
課題14中間会合	2025年7月8日～9日	韓国（ソウル） e-meeting ハイブリッド	次回SG17会合に向けた審議
課題15中間会合	2025年8月	未定	X.sec_QKD_profr、X.sec_QKDNi、TR.kdc_qkdn、TR.QKDN-SP、TR.hyb_qsafe、TR.SQKDN-SC及び入力された寄書
課題15中間会合	2025年10月7日～8日	未定	X.sec_QKD_profr、X.sec_QKDNi、TR.kdc_qkdn、TR.QKDN-SP、TR.hyb_qsafe、TR.SQKDN-SC及び入力された寄書
SG17会合	2025年12月3日～11日	スイス（ジュネーブ）	