ITU-T SG17第5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5回会合が、2024年2月20日（火）～3月1日（金）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25名を含む、55か国・諸機関の333名（現地参加161名、リモート参加172名）が参加した。提出された寄書は187件（うち日本から10件）で、520件の臨時文書（Temporary Document）が発行された。なお、第4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 生成AIのセキュリティとプライバシーに関するワークショップの開催

今回の会合に先立つ2月19日（月）に「Generative AI: Challenges and Opportunities for Security and Privacy」と称するワークショップが開催された。本ワークショップは、ISO/IEC JTC1 SC27、ETSI、OECD等の関係者も招待し、生成AIのセキュリティとプライバシーに関する標準化活動状況や各研究機関での取組み状況等が紹介された。パネルディスカッションを含む4つのセッションが開催され、ワークショップ全体としては、17件の講演が行われた。はじめに、生成AIを含むAIに関するセキュリティとプライバシーの懸念、リスク、脅威に焦点を当てた議論が行われた。次に、生成AIに関するセキュリティとプライバシーの懸念を軽減するための対策に焦点を当て、効果的な対策を実現する方法についての議論が2セッション行われた。最後にパネルディスカッションが行われ、今後の生成AIに関するセキュリティとプライバシーの標準化の方向性の検討と、SG17における将来の活動に対する推奨事項について議論がなされた。本ワークショップを受けて、AIセキュリティに関する情報交換の場として、コレスポンデンスグループCG-AI Securityを設立した。また、AIセキュリティに関連する標準化活動を調査し、今回のワークショップの成果を共有するために、ITU-T SGs、ETSI SAI、OECD、IEEE AIS Trust and Agency Committee、ISO/IEC JTC 1/SC 27/WG 4 & WG 5、ISO/IEC JTC 1/SC 42/WG 3にリエゾンを送付した。

2.2 サイバーセキュリティ対応組織の構築運用に関するミニワークショップの開催

今回の会合期間中の2月22日に、「ITU-T X.1060: Exploring an Operational Framework for Cybersecurity」と称するミニワークショップが開催された。本ワークショップは、日本からの貢献によりSG17で勧告化されたX.1060（Framework for the creation and operation of a cyber defence centre）の活動の紹介と、ベストプラクティスの情報交換及び堅牢なセキュリティ対策の実装に関する実用的なガイダンスが示された。2つのセッションが開催され、既存のセキュリティ対策組織をX.1060が提唱する「サイバーディフェンスセンター」のモデルに成功裡に移行した事例等の紹介や、FIRST CSIRT Framework等の既存フレームワークとX.1060の連携を議論する2つのセッションが開催され、日本からの講演1件を含む計6件の講演が行われた。

2.3 WTSA-24準備に関する特別セッション

WTSA-24準備に関する特別セッションが、計4回（2月21日、2月22日、2月26日及び2月27日）開催された。本セッションでは、前回会合以降に実施されたコレスポンデンスグループCG-SG17-WTSA24-PREPの活動の成果物と、本セッションに提出された各国寄書を対象に、WTSA-24後のSG17の体制検討を審議した。日本からも、課題15にあるインキュベーションプロセスの課題1への移設と課題7を分割してメ

タバースに関する活動を含めること、課題3を単独で残す、または課題10とマージすること及び課題14を課題11に統合することを提案する寄書を提出した。議論の結果、課題15にあるインキュベーションプロセスの課題1への移設とSG17の課題数を12に維持することについて合意された。今回の特別セッションの成果を受けて、第4回会合で合意しているとおり、WTSA-24後のSG17の体制検討を行うコレスポンデンスグループCG-SG17-WTSA24-PREPの活動を現在の研究会期の末まで継続し、2024年7月のTSAG会合前にSG17としての提案を取りまとめることとした。

3. 会合の主な審議内容と結果

3.1 WP1：セキュリティ戦略とコーディネーション

WP1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、量子ベースのセキュリティを含むセキュリティ全般の新技術（エマージングテクノロジ）について、そのインキュベーションメカニズムなどを検討する課題15から構成されている。

- 課題1では、既存勧告案のX.cs-raを補完するものとして、サイバーセキュリティ参照アーキテクチャのセキュリティ要件を抽出するためのユースケースに関する技術レポートTR.cs-uc（Use cases for extracting the security requirements for cyber security reference architecture）ほか2件の新規ワークアイテムが設立された。
- 課題15では、NISTで標準化検討中のPQCと親和性の高い先進的な暗号アルゴリズムを紹介し、5G/B5Gにおける暗号アルゴリズムの適用に関する技術指針を提供するTR.ac-pqc（Guidance on use of advanced cryptography based on PQC）ほか8件の新規ワークアイテムが設立された。また、X.1713（Security requirements for the protection of quantum key distribution node）とAmendments to X.1715（Security requirements and measures for integration of quantum key distribution network and secure storage network）が合意された。そして、TP.inno-2.0（Description of the incubation mechanism and ways to improve it）の発行が合意された。

3.2 WP2：5G、IoT、ITS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、電気通信サービスとIoTのため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）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、SG13で議論されているCPN（Computing Power Network）の1要素であるComputing Power Centerの相互接続に関するセキュリティガイドラインである技術レポートTR.sec-int-cpc（Security considerations for interconnection of computing power centers）ほか3件の新規ワークアイテムが設立された。また、X.1819（Security Capabilities of Network Layer for IMT-2020/5G Edge Computing）とX.1820（Security Requirements for the Operation of IMT-2020/5G Core Network to Support Vertical Services）が凍結された。そして、TR.zt-acp（Guidelines for zero trust based access control platform in telecommunication network）が合意された。
- 課題6では、IoT機器のセキュリティに関する技術要件を提供し、データの収集・保管・セキュリティ分析に関する要件と、IoT機器のセキュリティアラートと可視化に関する要件を提案するX.sm-iot（Technical requirements of security situation monitoring for Internet of things（IoT）device）ほか2件の新規ワークアイテムが設立された。また、X.1352Amd（Amendment 1 to Recommendation ITU-T X.1352：Security requirements for Internet of things devices and gateways）がTAP投票を経て合意された。そして、X.1353（Security methodology framework based on blockchain for zero-touch deployment in massive IoT）とX.1354（Security Controls for Internet of Things（IoT）system）が凍結された。
- 課題13では、Advanced Air Mobility（AAM）において取り扱われるデータの分類とそれらに対するセキュリティガイドラインであるX.aamd-sec（Security guidelines for categorized data in advanced air mobility（AAM））が新規ワークアイテムとして設立された。また、X.1373rev（Secure software update capability for intelligent transportation system communication devices）がTAP投票を経て合意された。そして、X.1384（Security requirements and guidelines for vehicular edge computing）が凍結された。

3.3 WP3：サイバーセキュリティと管理

WP3は、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と、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3では、X.1060を改訂するX.1060-rev（Framework for the creation and operation of a cyber defence/security centre）ほか2件の新規ワークアイテムが設立された。

●課題4では、マルウェア攻撃に対するネットワーク上のストレージ保護のためのセキュリティフレームワークX.nspam（Security framework for network storage protection against malware attacks）ほか1件の新規ワークアイテムが設立された。また、X.1237（Technical security framework for protection of personally identifiable information while countering mobile messaging spam）が凍結された。

3.4　WP4：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）のセキュリティ課題の整理とDLTをセキュリティに活用する方法を検討する課題14から構成されている。

●課題7では、リコメンデーションサービスにおけるセキュリティの脅威の特定と、それらに対するセキュリティ要件を定めるX.str-irs（Security threats and requirements for information recommendation service）ほか3件の新規ワークアイテムが設立された。また、X.1150（Security assurance framework for digital financial services）がTAP投票を経て合意された。そして、X.1471（A reference monitor for online analytics services）が凍結された。さらに、X.1144rev（The revision of eXtensible Access Control Markup Language）、X.guide-ccd（Security guidelines for combining de-identified data using trusted third party）、X.sg-dtn（Guidelines for Digital Twin Network）及びX.smsrc（Security measures for smart residential community）が合意され、補足文書X.suppl.uc-dcc（Use cases for digital COVID-19 certificates）の発行が合意された。

●課題8では、クラウド基盤のDDoS対策に関するガイドラインX.gapci（Guidelines on Anti-DDoS protection for cloud infrastructure）ほか3件の新規ワークアイテムが設立された。

●課題14では、NFTなどのデジタル収集サービスのセキュリティ要件X.sg-dcs（Security guidelines for DLT-based digital collection services）ほか5件の新規ワークアイテムが設立された。

3.5　WP5：基本的なセキュリティ技術

WP5は、ID管理と生体認証を通信環境で利用する際のアーキテクチャ及びメカニズムを検討する課題10と、X.509を含むPKI関連技術や統一モデリング言語（UML：Unified Modeling Language）等の安全なアプリケーションを支援する基盤技術について検討する課題11から構成されている。

●課題10では、NISTがSP800-63-4の初期公開草案を公表してITU-TのX.1254の改訂を提案していることを受けて、既存勧告のX.1254をNISTの活動と整合させるためのX.1254rev（Entity authentication assurance framework）ほか4件の新規ワークアイテムが設立された。また、X.1280（Framework for out-of-band server authentication using mobile devices）とX.1281（APIs for interoperability of identity management systems）がTAP投票を経て合意された。そして、X.gpwd（Threat Analysis and guidelines for securing password and passwordless authentication solutions）が凍結された。

●課題11では、ITU-T X.510 | ISO/IEC 9594-1のセキュリティとユーザビリティの強化に資する拡張を行うX.500：The Directory：Overview of concepts, models and servicesほか9件の新規ワークアイテムが設立された。

3.6　今会合で設立された新規ワークアイテム一覧

今回のSG17会合では、61件の新規ワークアイテム提案が寄せられ、そのうち55件を設立した。通常よりも多くの提案となったため、新規に設立したワークアイテムの情報について、表1に整理する。

■表1. SG17第5回会合で設立された新規ワークアイテム

課題	ワークアイテム名称	勧告名称
課題1	TR.cs-uc	Technical report : Use cases for extracting the security requirements for cyber security reference architecture
課題1	TR.cs-sc	Technical report : Collection of Security Concerns to support X.cs-ra Cyber Security Reference Architecture
課題1	CRAMM Roadmap	SG17 Cyber Security Reference Architectures, Models and Methodologies Roadmap
課題2	TR.sg-lmcs	Technical report : Security guidelines for DLT-based lifecycle management of computing services
課題2	TR.sec-int-cpc	Technical report : Security considerations for interconnection of computing power centers
課題2	TR.sd-cnc	Technical report : Security guidelines for data of coordination of networking and computing
課題2	X.ztmc	Guidelines for high level Zero trust model and its security capabilities in telecommunication networks
課題3	X.cdc-csirt	Relationships between Cyber Defence/Security Centre and Computer Security Incident Response Team
課題3	X.1060-rev	Framework for the creation and operation of a cyber defence/security centre
課題3	X.1058-rev	Information security, cybersecurity and privacy protection-Code of practice for personally identifiable information protection
課題4	X.nspam	Security framework for network storage protection against malware attacks
課題4	X.gpmr	Guidelines and security measures for prevention and mitigation of ransomware
課題6	TR.st-iot	Technical report : Security threat scenarios in Internet of things
課題6	X.sm-iot	Technical requirements of security situation monitoring for Internet of things（IoT）devices
課題6	X.gnssa-iot	Guidelines of implementing network security situational awareness for IoT systems
課題7	X.fr-vsasi	Functional requirements for visualization service of network security assets and security incidents based on digital twin
課題7	X.ias	Functional requirements for the unified authentication service of telecommunication operators
課題7	X.str-irs	Security threats and requirements for information recommendation service
課題7	X.sgrtem	Security guidelines for real-time event monitoring and integrated management in smart city platforms
課題8	X.FR-MSP	Functional Requirements of Microsegmentation Platform in a cloud-based environment
課題8	X.ckrp	Framework of cryptographic key resource pool for cloud computing
課題8	X.mbaas-cs-sec	Security requirements and framework of collaboration service for multiple blockchain as a service platforms
課題8	X.gapci	Guidelines on Anti-DDoS protection for cloud infrastructure
課題10	X.1254rev	Entity authentication assurance framework
課題10	X.oob-pacs	Framework for out-of-band physical access control systems using beacon-initiated mutual authentication
課題10	X.tis	Telebiometric authentication based on information splitting
課題10	TR.divs	Technical report : Rationale and initial approach of a decentralized identity verification system（DIVS）based on verifiable data
課題10	TR.SIMRegBio	Technical report : Guidelines for SIM Identity and Biometrics Registration.
課題11	X.500Amd.1	The Directory : Overview of concepts, models and services
課題11	X.501Amd.2	The Directory : Models
課題11	X.509Amd.1	The Directory : Public-key and attribute certificate frameworks
課題11	X.510Amd.1	The Directory-Protocol specifications for secure operations
課題11	X.511Amd.1	The Directory : Abstract service definition
課題11	X.518Amd.1	The Directory : Procedures for distributed operation
課題11	X.519Amd.1	The Directory : Protocol specifications
課題11	X.520Amd.1	The Directory : Selected attribute types
課題11	X.521Amd.1	The Directory : Selected object classes
課題11	X.525Amd.1	The Directory : Replication
課題13	X.aamd-sec	Security guidelines for categorized data in advanced air mobility（AAM）
課題14	X.qsdlt-ca	Guidelines for building crypto-agility and migration for quantum-safe DLT systems
課題14	TR.dw-lasf	Technical report : A landscape analysis and security features for a digital wallet
課題14	X.1400rev	Terms and definitions for distributed ledger technology
課題14	X.sr-dpts	Security requirements for DLT data on permissioned DLT-based distributed power trading systems

課題14	X.sg-dcs	Security guidelines for DLT-based digital collection services
課題14	TR.gscim-dlt	Technical report : Guidelines for security consideration for incident management by DLT service provider
課題15	X.sr-da-gai	Security threats and requirements for data annotation service of generative artificial intelligence
課題15	X.sgGenAI	Security Guidelines for Generative Artificial Intelligence Application Service
課題15	X.ig-dw	Implementation guidelines for digital watermarking
課題15	X.sc-sscti	Guidelines on Security Capabilities for Software Supply Chain in the Telecommunications Industry
課題15	TR.se-ai	Technical report : Security Evaluation on Artificial Intelligence Technology in ICT
課題15	X.srm-fml	Security requirements and measures of federated machine learning
課題15	X.pg-cla :	Procedural guideline for continual learning to actively respond to network attacks
課題15	TR.ac-pqc	Technical report : Guidance on use of advanced cryptography based on PQC
課題15	TR.QKDN-SP	Technical report : Overview of security profile for Quantum Key Distribution Networks in hybrid mod

4. 今後の会合の予定

次回のSG17会合は、次に述べる2つのオプションが提案された。1つ目のオプションは、6月下旬か7月上旬にスイス（ジュネーブ）以外を開催地として2週間の会合を実施するものであり、会期の前日には、デジタルツインとメタバースのセキュリティとプライバシーに関するワークショップを開催する。もう1つのオプションは、7月11日と12日にWTSA準備のためのオンラインの会合を実施し、9月にスイス（ジュネーブ）にて1週間の会合を実施するものである。3月末時点で開催地の立候補が無かったため、2つ目のオプションが選ばれることとなり、9月の会合は2日～6日が予定されている。

次回までに開催される中間会合等の予定を**表2**に示す。

5. おわりに

今回の会合では、当時の時点で現研究会期の最高の件数を記録した前回会合の実績値である153件を2割程度上回る、187件の寄書が提出された。そして、これらのうち、61件が新規ワークアイテム提案であった。提出された新規ワークアイテム提案の対象の技術分野は、分散台帳、量子鍵配送、AIに関するものが多く、また、提出国は中国が約半数を占め、それに韓国が続いた。こうした状況は、新興技術の隆盛に伴ってセキュリティ分野で検討すべき課題が継続的に発生する様相を如実に示している。同時に、審議にあたる参加メンバーのリソースは限られているため、審議が進行中の勧告草案も含めて過去に前例のない件数を扱う状況について、限られた時間で精緻な審議を行うための会合の在り方についても検討と考慮が必要と考える。こうした対応は、ITU-Tの勧告が、真に意義のある成果であると社会から適格を得るためにも、重要な課題である。この課題に対して、日本が世界の情報通信技術の発展と安定に、その存在感を発揮しながら貢献すべく、標準化活動への取組みを進めていく。

■表2. 今後の関係会合の予定

会合名	開催期間	開催地	会合内容
課題1中間会合	2024年5月17日	ソウル（韓国）	セキュリティマニュアル、TR-Suss及び課題1に関する将来的なワークアイテムすべてのレビュー
課題3中間会合	2024年6月5日	e-meeting	X.shcdの審議
課題3中間会合	2024年6月6日	e-meeting	X.1058-revとX.1053-revの審議
課題3中間会合	2024年6月11日～12日	e-meeting	Sup-cdc、X.gsm-cdc及びX.1060-revの審議
課題4中間会合	2024年5月24日	e-meeting	課題4のすべてのワークアイテムの審議
課題7中間会合	2024年5月21日～22日	杭州市（中国）	課題7のすべてのワークアイテムの審議
課題8中間会合	2024年5月21日～22日	杭州市（中国）	課題8のすべてのワークアイテムの審議
課題10中間会合	2024年5月16日～27日の間で1日	検討中	課題10のすべてのワークアイテムの審議
課題13中間会合	2024年6月4日～5日	e-meeting	X.evtol-secとX.sup-cv2x-secの準備と課題テキストの審議
課題15中間会合	2024年6月4日～6日	e-meeting	インキュベーションセッションに関する新規課題と既存課題の審議
課題15中間会合	2024年7月	e-meeting	量子鍵配送に関する新規課題と既存課題の審議
SG17会合	①2024年7月11日～12日 ②2024年9月2日～6日	①e-meeting ②スイス（ジュネーブ）	