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
磯原（いそはら）　隆将（たかまさ）

株式会社KDDI総合研究所
情報システム・セキュリティ部
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1回会合が、2022年5月10日～20日に、遠隔会議（Virtual Meeting）の形式で開催された。会合には、日本からの24名を含む、39か国・諸機関の281名が参加した。提出された寄書は101件（うち日本から9件）で、331件の臨時文書（Temporary Document）が発行された。

2. SG17全体に関わる結果

2.1 課題構成と運営体制

今回の会合は、新しい研究会期の初会合となる。WPの構成と、議長及び副議長は前会期と同様の体制を継承することが合意された。各課題のラポータとアソシエイトラポータは、一部を除いて前会期と同様の体制が引き継がれた。表1にSG17の体制を示す。

■表1. SG17の体制（敬称略）

SG	WP	課題	タイトル	議長／ラポータ	副議長／アソシエイトラポータ
17	Security セキュリティ			Heung Youl Youm（韓国）	Samir Andelgawad（エジプト） Laial Almansoury（クウェート） Afnan Alromi（サウジアラビア） Abderrazak Bachir Bouiadjra（アルジェリア） Gökhan Evren（トルコ） 三宅 優（日本） Lia Molinari（アルゼンチン） Kwadwo Osafo-Maafo（ガーナ） Greg Ratta（英国） Pushpendra Kumar Singh（インド） Arnaud Taddei（英国） Wala Turki Latrous（チュニジア） Liang Wei（中国）
	1	Security strategy and coordination セキュリティ戦略とコーディネーション		Vasiliy Dolmatov（ロシア）	Jonghyun Kim（韓国）
		1	Security standardization strategy and coordination セキュリティ標準化戦略とコーディネーション	Mohamed Elhaj（スーダン） Juhee Ki（韓国）	Greg Ratta（英国） Yiwen Wang（中国）
		15	Security for/by emerging technologies including quantum-based security 新興技術のためのセキュリティと新興技術によるセキュリティ（量子関係技術を含む）	Dong-hi Sim（韓国）	釼吉 薫（日本） Chun Seok Yoon（韓国） Chen Zhang（中国）
	2	5G, IoT and ITS security 5G、IoT、ITSのセキュリティ		三宅 優（日本）	Zhiyuan HU（中国） Philip Mills（英国）
		2	Security architecture and network security セキュリティアーキテクチャとネットワークセキュリティ	Zhiyuan Hu（中国） Heung Ryong Oh（韓国）	
		6	Security for telecommunication services and Internet of Things 通信サービスとIoTのセキュリティ	Jonghyun Baek（韓国） Junzhi Yan（中国）	Gunhee Lee（韓国） 高橋 健志（日本） Bo Yu（中国）

		13	Intelligent transport system（ITS）security ITSのセキュリティ	Sang-Woo Lee（韓国）	Seungwook Park（韓国） 磯原 隆将（日本） Yi Zhang（中国）
	3		Cybersecurity and management サイバーセキュリティと管理	中尾 康二（日本）	Lia Molinari（アルゼンチン）
		3	Telecommunication information security management and security services 通信事業者向けの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（日本）	Jinghua Min（中国） 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	Jong-Hyun Kim（韓国） Yanbin Zhang（中国）	Changoh Kim（韓国）
	4		Service and application security サービスとアプリケーションのセキュリティ	Jae Hoon Nah（韓国）	Xiaoyuan Bai（中国）
		7	Secure application servicesセキュアなアプリケーションサービス	Jae Hoon Nah（韓国）	Feng Gao（中国） Lijun Liu（中国）
		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のセキュリティ	Liang Wei（中国）	Mark Mcfadden（英国）
		14	Distributed ledger technology（DLT）security 分散台帳技術のセキュリティ	門林 雄基（日本） Kyeong Hee Oh（韓国）	Xiaoyuan Bai（中国） Ke Wang（中国）
	5		Fundamental security technologies 基本的なセキュリティ技術	Zhaoji Lin（中国）	
		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） John George Caras（米国）	Keundug Park（韓国） 武智 洋（日本） Junjie Xia（中国） Jason Kim（韓国）
		11	Generic technologies（such as Directory, PKI, Formal languages, Object Identifiers）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（ディレクトリ、PKI、形式言語、オブジェクト識別子）	Jean Paul Lemaire（フランス）	Dieter Hogrefe（ドイツ）

2.2　X.509に関するワークショップの開催

今回の会合に先立つ2022年5月9日に「ITU-T X.509 Day」と称するワークショップが、遠隔会議の形式で開催された。X.509は、公開鍵基盤等を実現する要素技術として広く浸透しており、最も活用されている勧告と位置付けられる。ワークショップでは、公開鍵暗号と公開鍵基盤の概観、X.509の及ぼした影響とユースケース及びX.509の規格の将来の方向性をテーマとするセッションが開催された。また、X.509の勧告案のエディターらSG17の関係者と関連標準化団体や産業界の関係者らによるパネルディスカッションが行われた。今回のSG17会合では、このワークショップにおいてX.509に関連する標準化団体が参加する「X.509 Advisory Group」の設立に関する検討が合意されたことが報告された。

2.3　CG-SECAPAの設立

WTSA-20の決議50／決議98にて、SG17に対して、他のSG及び別の標準化団体とセキュリティに関する活動について連携を推進することを求めており、これに対応する形で、英国と韓国からSG17としての取組み提案が寄書として提出された。英国からは本件に関する勧告案「Security Capabilities Definitions」の提案が行われており、これを議論するためのコレスポンデンスグループとして、CG-SECAPAが設立された。

2.4　遠隔形式による会議の効率化

2021年8月～9月のSG17会合において遠隔形式による会議の効率化を検討するコレスポンデンスグループCG-SG17-meetingが設立され、その結果を確認するためのスペシャルセッションが開催された。会議運営の方針をまとめたガイドラインについては、おおむね合意が得られたが、新しい課題レポート、WPレポートの雛形について対立する複数の意見が出たため、継続の議論が必要となった。そのため、コレスポンデンスグループの活動を継続して議論を行うことが承認された。

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、セキュリティロードマップの発行と、セキュリティコンペンディアムの更新が同意された。
- 課題15では、WTSA-20の決議50（Cybersecurity）でSG17に対して新たに追加された指示事項への対応として「セキュリティケイパビリティ」の定義を審議する勧告案X.secadef（Security capabilities definitions）と、ネットワークのセキュリティ機能を統合的に管理することを目的とするミドルプラットフォームアーキテクチャを審議するテクニカルレポートTR.smpa（Security middle platform architecture）が新規ワークアイテムとして設立された。また、TR.sec-ai（Guidelines for security management of using artificial intelligence technology）と、TR.hyb-qkd（Overview of hybrid approaches for key exchange with QKD）の発行が同意された。そして、X.1715（Security requirements and measures for integration of QKDN and secure storage network）がコンセントされた。

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、5Gネットワークを用いてVertical Serviceを提供する場合のコアネットワーク機能におけるセキュリティ要件を審議する勧告案X.5Gsec-srocvs（Security Requirements for the Operation of 5G Core Network to Support Vertical Services）、複数のCPN（Computing Power Network）が連携する場合のユースケースを審議するテクニカルレポートTR.cpn-col-sec（Security consideration of collaboration of multiple computing power networks）及び5Gネットワークに対して組み込むセキュリティ機能を提案するテクニカルレポートTR.5Gsec-bsf（Guidelines of Built-in Security Framework for the Telecommunications Network）が新規ワークアイテムとして設立された。また、X.1812（Security framework based on trust relationship for IMT-2020 ecosystem）がTAPを経て合意され、XSTP-5Gsec-RM（5G Security Standardization Roadmap）のテクニカルペーパーとしての発行が合意された。そして、X.1813（Security requirements for the operation of vertical services supporting ultra- reliable and low latency communication（URLLC）in the IMT-2020 private networks）と、X.1814（Security guidelines for the IMT-2020 communication system）がデターミネーションされた。
- 課題6では、IoT機器の利用環境において、中央装置からIoT機器向けにブロードキャストしたコマンドを対象機器のみが実行するターゲットブロードキャスト認証システムの概念モデル及びセキュリティ要件を審議するテクニカルレポートTR.ba-iot（Broadcast authentication schemes for IoT system）が新規ワークアイテムとして設立された。また、X.1352（Security Requirements for IoT devices and gateway）がデターミネーションされた。
- 課題13では、X.1379（Security requirements for roadside units in intelligent transportation systems）がコンセントされた。

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、今会合で合意された文書や新規ワークアイテムの設立は無く、既存のワークアイテムの審議が行われた。
- 課題4では、標的型電子メール攻撃の定義と攻撃を防御するためのセキュリティ要件及び対策を審議する勧告案X.sr-ctea（Proposal for new work item：Security requirements and countermeasures for targeted email attacks）、ホスト端末へのマルウェア攻撃に対するストレージ保護のためのセキュリティフレームワークを審議する勧告案X.spmoh（Proposal for new work item：Security framework for storage protection against malware attacks on hosts）及びRCSメッセージングにおけるスパム対策のためのガイドラインを審議する勧告

案X.sgc_rcs（Proposal for new work item-Guidelines for countering spam over RCS messaging）が新規ワークアイテムとして設立された。また、X.1246Amd1（Revised baseline text for Amendment 1 to X.1246：Technologies involved in countering voice spam in telecommunication organizations）と、X.1247Amd.1（Revised baseline text for Amendment 1 to X.1247：Technical framework for countering mobile messaging spam）がTAPを経て合意された。

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、様々な分野のデジタルツインシステムの組合せであるデジタルツインフェデレーション（DTF：Digital Twin Federation）のセキュリティ脅威を分析し、脅威への対策を審議する勧告案X.smdtf（Security measures for digital twin federation in smart cities and communities）、都市を構成するエネルギー・交通・防災等の物理的な資産をモニタリングするIoTサービスにおける脅威とセキュリティ対策を審議する勧告案X.srmpc（Security requirements for monitoring physical city assets）、決済サービス等においてユーザとサービスのインタラクションに注目する不正検知手法の機能要件や仕様を審議する勧告案X.tc-ifd（Technical capabilities of interactive fraud detection）及びデジタルCOVID-19証明書のユースケースを審議する補足文書X.suppl.uc-dcc（Use cases for digital COVID-19 certificates）が新規ワークアイテムとして設立された。
- 課題8では、ビッグデータ環境における機械学習を用いたデータセキュリティのためのガイドラインを審議する勧告案X.gdsml（Guidelines for data security using machine learning in big data infrastructure）と、クラウドコンピューティングのためのセキュリティオーケストレーション・自動化・レスポンス（SORA）のフレームワークを審議する勧告案X.soar-cc（Framework of Security Orchestration, Automation and Response for cloud computing）が新規ワークアイテムとして設立された。
- 課題14では、X.1409（Security services based on distributed ledger technology）がコンセントされた。

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、X.tec-idms（Management and protection techniques for user data protection in distributed identity systems）がワークアイテムから削除された。また、FIDO Allianceの文書を精査して、X.1277（Universal authentication framework）とX.1288（Client to authenticator protocol/Universal 2-factor framework）の改訂等を審議するコレスポンデンスグループであるGC-FIDOの設立が合意された。
- 課題11では、今会合で合意された文書や新規ワークアイテムの設立は無く、既存のワークアイテムの審議が行われた。

4. 今後の会合の予定

次回のSG17会合は、2022年8月23日～9月2日にスイス（ジュネーブ）で、対面形式によって開催される。この会合には、リモート参加も可能であり、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ことが確認された。また、会合前日の8月22日には、5G/B5Gのセキュリティをテーマとしたワークショップを開催する予定である。ITU-Tの他SGや3GPP、GSMA等の関連する関係標準化団体にも働き掛け、5G/B5Gのセキュリティ対策のコンセプトと機能の理解、セキュリティ脅威への対処等について、有識者によるプレゼンテーションと、国際標準化活動における将来展望をテーマとするパネルディスカッションの実施などを計画している。次々回の会合は2023年2月21日～3月3日を予定しており、正式な決定を8月の会合で行う。

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

今回の会合への参加者数は、SG17として過去最高の記録を更新する結果となった。提出された寄書と発行された

■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2中間会合	2022年6月30日	e-meeting	次回会合でデターミネーション予定のX.5Gsec-ecsとX.5G-sslの審議
課題3中間会合	2022年6月～7月	e-meeting	CDC（Cyber Defence Centre）に関するアフリカでのアンケート作成に関する審議
課題10中間会合	2022年7月	e-meeting	課題10のワークアイテムすべて
課題11中間会合	2022年6月27日～7月1日	e-meeting	ISO/IEC/JTC 1/SC6との合同会合
課題13中間会合	2022年6月7日～8日	e-meeting	次回会合でデターミネーション・コンセント予定のX.ipscv、X.edr-sec、X.eivn-sec、X.srcd及びX.fstiscvの審議
課題14中間会合	2022年7月12日～13日	e-meeting	X.srscm-dltとX.sa-dsmの審議と、他SG、FG及び関連標準化団体からの成果文書のレビュー
ワークショップ	2022年8月22日	スイス（ジュネーブ）	5G/B5Gのセキュリティをテーマとしたワークショップ
SG17会合	2022年8月23日～9月2日	スイス（ジュネーブ）	

臨時文書の数も、前回の会合に匹敵する量を維持しており、ITU-Tの中でも最も活動が活発なSGの1つとしての勢いを保つ形で、新しい研究会期を開始した。次回の会合はジュネーブでの開催が決定したことから、感染防止に十分に配慮しながら、対面による審議の形を取り戻すことで、遠隔形式では困難が伴った、きめの細かい議論が叶うことを期待している。

情報通信技術のセキュリティに関する国際標準化は、検討を必要とする技術領域が常に拡大し、その重要性も増している。そのため、活発な新規ワークアイテムの提案が行われている。SG17として、重要な課題にタイムリーに扱っていく必要がある一方で、限られたリソースで有意義な活動を行うために、ITUが扱うことの是非について、提案内容や成熟度等の観点から、しっかりと見極めることも必要となっている。

日本としては、リーダーシップポジションをはじめとする各種の役職を適切に担いながら、各課題における議論、SG17全体に関わる課題や新規ワークアイテムの扱いの対処等に寄与し、国際社会におけるプレゼンスの維持・向上に努めるとともに、貢献を果たしてゆく。