

ITU-T SG17 (セキュリティ) 第5回会合報告



株式会社KDDI総合研究所
サイバーセキュリティグループ
研究マネージャー

いそはら たかまさ
磯原 隆将



株式会社KDDI総合研究所
スマートセキュリティグループ
グループリーダー

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、2019年1月22日(火)~1月30日(水)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17名を含む、38か国・諸機関から178名の参加があった。提出された寄書は117件(うち日本から7件)で、381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 AIセキュリティに関するワークショップの開催

会合前日の1月21日(月)に、「ITU Workshop on Artificial Intelligence, Machine Learning and Security」が開催された。AIを利用したセキュリティ対策、AIによるサイバー攻撃、AI自体に対する攻撃等について発表が行われた。ITU-T SG17での取組みへの反映については、各課題において、必要に応じてAIのトピックを入れることとした。これに伴い、課題2のToR(課題テキスト)について、AI/MLに関する記述を追加する更新を行い、TSAGに送付した。課題5もToRの更新を検討したが、次回の会合まで検討を継続することとなった。

2.2 SG17の体制見直しに関する議論

2021年からの研究会期のSG17の体制見直しを進めるための活動であるコレスポネンスグループ(CG-XSS: Correspondence Group on Transformation of Security Studies)について、活動を継続することとした。また、WTSA-2020に向けたSG17としての準備を行うために、新たなコレスポネンスグループを設立した。

2.3 Quantum communicationをテーマとするミニワークショップの開催

1月23日(水) 午後にQuantum communicationをテーマ

とするミニワークショップが開催され、約50名が参加した。日本、韓国、中国、英国、ETSI、ISOから計7件のプレゼンテーションが行われ、ID QuantiqueとSKTがQKD関連製品の展示を行った。日本からは、NICTがTokyo QKD Networkの紹介とそれをベースとした標準化活動、東芝がETSIで行っているQKDの鍵配送APIの標準化活動について紹介を行った。ITU-T SG13、ETSI、ISOの標準化動向などプレゼンテーションには多くの情報があり、参考となった。特にQKD Networkのアーキテクチャの標準化についてはITU-T、ETSI、ISOの間でCoordinationが必要との認識が示され、次回9月のTSAGで議論になると予想される。また、中国が行った2件のプレゼンテーション(発表タイトルは、「Practical attacks on implementation of quantum key distribution」、「Standardizing security certification of QKD in ISO/IEC JTC 1/SC27」)では、QKDの実装と研究で一歩進んでいるとの印象を受け、今後の検討への示唆を含んでいる。

2.4 量子コンピュータに対して安全な相互接続通信のための新規課題設立提案

韓国より、新規課題「Security aspects of interoperable quantum safe communications」の設立提案が寄書により行われた。対象はQKDによる通信のセキュリティ対策の勧告化である。本寄書に対して英国から次会期の課題構成検討において設立の必要性を検討すべきとの寄書が提出され、英国を支持する国が多かったことから、今回の会合では新課題設立は見送られた。

3. 会合の主な審議内容と結果

3.1 課題1: 電気通信/ICTのセキュリティに関する調整

課題1は、各WPから独立して活動を行っており、SG17全体の調整及び他のSGやTSAG、標準化団体等との関係



において、SG17全体に関わる案件を担当している。今回の課題1においては、前回のSG17会合からの継続審議案件となっていたJCA-COP (Joint Coordination Activity on Child Online Protection) の再開提案について、再開せずに現在のまま休眠状態とすることとした。また、次回のSG17会合前日にFintechセキュリティに関するワークショップを開催することとした。その他の報告事項として、セキュリティマニュアルのレビューメンバーを選定し、マニュアル文書の完成後に内容確認を行うこととしたこと、セキュリティ標準ロードマップを更新し、新たに8つの標準化団体から155の標準を追加したこと、テクニカルレポートX.Truss (Successful use of security standards) の更新を検討し、PKIとDLTに関する技術が必要との認識で合意が形成され、Living Documentsとして常時更新する文書とされたこと、がある。

3.2 WP1: 電気通信 / ICTセキュリティ

WP1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の検討を行う課題2、ISO/IEC JTC1 SC27との連携をベースに通信事業者における情報セキュリティマネジメントに関する検討を行う課題3、モバイルセキュリティやUSN (Ubiquitous Sensor Network) セキュリティ、IoTセキュリティに関連した検討を行う課題6、ITSセキュリティの検討を行う課題13から構成されている。

- ・課題2では、今回の会合では、X.sdnsec-3 (Security framework and requirement of Service Function Chain based on software-defined networking) を合意した。本勧告案は、SDN (Software Defined Networking) の利用においてネットワークポリシーを展開する機能に対する脅威とセキュリティ対策について説明するものである。なお、タイトルが「Security guideline of Service Function Chain based on software defined network」から変更された。
- ・課題3では、X.sup-myuc (Code of practice for information security control base on ITU-T X.1051 for Malaysian telecommunications organizations information and network security management) を補足文書として発行することに同意した。本文書は、マレーシア電気通信事業者の情報及びネットワークセキュリティ管理のための、X.1051を基にした情報セキュリティ管理策である。また、X.rgm (Risk management implementation guidance on the assets of telecommunication organizations accessible by global IP-based networks) について、今

回の会合での合意が次回に延期された。新規ワークアイテムとして、X.ciag (Cyber insurance acquisition guideline for Information and Communication Technologies (ICT) services provider) を設立した。本勧告案は、マレーシアからの新規提案によるもので、サイバー保険の有益な使い方のためのガイドラインとして、ISO/IEC 27102をベースにICTサービスプロバイダ向けの内容に形成し、既にマレーシアで施行している文書をITUでの勧告化に持ち込んだものである。

- ・課題6では、勧告案X.1042 (X.sdnsec-1, Security services using the software-defined networking) を決定した。また、新規ワークアイテムとして、5Gセキュリティ関係の勧告案である、X.5Gsec-ecs (Security framework for 5G edge computing services)、X.5Gsec-guide (Security guidelines for 5G communication system based on ITU-T X.805) の2件を新規ワークアイテムとして設立した。
- ・課題13では、本会合で予定されていたX.itssec-2 (Security guidelines for V2X communication systems) とX.stcv (Security threats in connected vehicles) のデターミネーションを次回会合に延期した。

3.3 WP2: サイバー空間のセキュリティ

WP2は、CYBEXをはじめとするサイバー空間上の様々な脅威に対する具体的な対策やガイドラインの検討を行う課題4、技術的な観点からスパム対策の検討を行う課題5、ブロックチェーンの要素技術である分散台帳技術のセキュリティについて検討を行う課題14から構成される。

- ・課題4では、前回の会合でデターミネーションされた勧告案X.1215 (X.ucstix, Use Cases for Structured Threat Information Expression (STIX)) を決定した。また、新規ワークアイテムとして、4件を設立した。具体的には、サイバーセキュリティ関連で、動的な動作分析に基づく未知のマルウェア検出の要求条件を検討するX.rdmase (Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment)、量子関連で、QKDネットワークによる暗号鍵生成を検討するX.cf_QKDN (The use of cryptographic functions on a key generated in Quantum Key Distribution networks)、QKDネットワークの鍵管理のセキュリティ要件を検討するX.sec_QKDN_ov (Security requirements for Quantum Key Distribution network-Overview) と、X.sec_QKDN_



km (Security requirements for Quantum Key Distribution network-key management) である。

- ・ 課題5では、前回の会合でデターミネーションした勧告案 X.1249 (Technical framework for countering mobile in-application advertising spam) を決定した。その他のワークアイテムについては、継続して審議が行われている。
- ・ 課題14では、10件の既存勧告案について継続的な審議が行われ、本文が改訂された。また、標準化ロードマップを更新し、関連標準化団体の取組み動向の反映を行った。

3.4 WP3：アプリケーションセキュリティ

WP3は、Webサービスやアプリケーションサービス、P2Pで必要とされるセキュリティ技術の検討を行う課題7、クラウドコンピューティングにおけるセキュリティに関わる検討を行う課題8、仕様記述言語や統一モデリング言語 (UML)、開放型分散処理 (ODP) などの検討を行う課題12から構成される。

- ・ 課題7では、新規ワークアイテムとして、データの匿名化に対する要求を規定するX.rdda (Requirements for data de-identification assurance) を設立した。また、その他6件の既存の勧告案について、継続的な議論を実施した。
- ・ 課題8では、新規ワークアイテムとして、エッジとこれを集約するリージョンに分散されたクラウド環境におけるセキュリティ脅威の分析とセキュリティ要求を規定するX.sgdc (Security guidelines for distributed cloud) と、クラウドベースの低遅延かつ高信頼性を有するアプリケーションに対するセキュリティ要求を規定するX.sr_cphr (Security Requirements for Cloud-based Platform to Support Low Latency and High Reliability Application Scenarios) の2件を設立した。その他、6件の既存の勧告案について、継続的な議論を実施した。
- ・ 課題12では、Z.109rev, Specification and Description Language-Unified modeling language profile for SDL-2010をワークアイテムから削除した。現時点で、TTCN-3を除くワークアイテムはメンテナンスモードにあり、30件の勧告案を議論している。

3.5 WP4：ID管理及び認証

WP4は、生体認証技術を通信環境で利用するための標準規格の検討を行う課題9、ID管理に関連する技術やサービスについて検討する課題10、X.509を含むPKI関連技術

とASN.1/OID関連の検討を行う課題11から構成される。

- ・ 課題9では、X.tab (Telebiometric authentication using bio-signals) が合意された。現時点で3件の勧告案を議論している。
- ・ 課題10では、既存ワークアイテムである、X.1254rev (Entity authentication assurance framework)、X.1252rev (Baseline identity management terms and definitions)、X.eaasd (Framework of enhanced authentication in telebiometric environments using anti-spoofing detection mechanisms) 及びX.Sup-1254rev (Supplement to X.1254rev on use cases and high level abstract implementations) に関して、継続的な議論を実施している。
- ・ 課題11では、X.894 Corrigendum 1 (Cryptographic Message Syntax (CMS) profile) が合意された。現時点で、X.509 (PKI) シリーズの更新を主として22件の勧告案を議論している。

4. 今後の会合の予定について

次回のSG17会合は、2019年8月27日 (火)～9月5日 (木) にスイス (ジュネーブ) で開催される。また会合前日の8月26日 (月) には、Fintechをテーマとしたワークショップを開催する予定である。

次回までに開催される中間会合等の予定を表に示す。

5. おわりに

今回の会合では178名の参加登録があり、前回会合に引き続き、多数の寄書及び臨時文書が発行され、ITU-Tの中で最も活動が活発なSGの1つとなっている。今回の会合では、AI/ML関連のセキュリティ対策勧告化を推進する方針について合意が形成された。今後、サイバーセキュリティ対策の高度化を中心として、SG17で検討が促進されることが考えられる。また、量子暗号通信の議論も活発化しており、特に、中国、韓国及びQKD関連製品を販売しているスイス、米国の会社が推進に積極的である。韓国は、量子鍵配送 (QKD: Quantum Key Distribution) に関する新課題設立提案を行ったが、これに対しては、英国、日本、カナダ等が次回WTSAで検討することを主張し、先送りされた。今後も、ITUが取り組むべき範囲について議論を行うなかで、他の標準化団体との連携を前提として、効率良く有益となる方向性を見いだしていく必要があると考えられる。



■表. 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3中間会合	2019年6月17日の週	E-meeting	課題3のワークアイテム全て
課題4中間会合	2019年6月(予定)	未定(中国の予定)	QKDに関するワークアイテム
課題6中間会合	2019年5月または6月	未定	課題6のワークアイテム全て
課題7中間会合	2019年6月18日~19日	中国(重慶)	課題7のワークアイテム全て
課題8中間会合	2019年6月11日~12日または6月13日~14日	中国(北京)	課題8のワークアイテム全て
課題10中間会合	2019年4月	E-meeting	未定(課題3、7、9との合同)
課題10中間会合	2019年6月	E-meeting	未定(課題3、7、9との合同)
課題11中間会合	2019年4月22日~26日	中国(北京)	ISO/IEC/JTC1/SC6/WG10との合同会合
課題13中間会合	2018年6月11日~12日(予定)	中国(北京)	課題13のワークアイテム全て
課題14中間会合	2019年5月または6月	E-meeting	課題14のワークアイテム全て
ワークショップ	2019年8月26日	スイス(ジュネーブ)	Fintechをテーマとしたワークショップ
SG17会合	2019年8月27日~9月5日	スイス(ジュネーブ)	

国際航海を行う船舶局に必須の書類 好評発売中!



**船舶局局名録
2018年版**



**海岸局局名録
2017年版**



**海上移動業務及び
海上移動衛星業務で使用する便覧
2016年版**

お問い合わせ: hanbaitosho@ituaj.jp

