ITU-T SG17（セキュリティ）第4回会合報告

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

三宅（みやけ）　優（ゆたか）

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

磯原（いそはら）　隆将（たかまさ）

1. はじめに

ITU-T SG17（セキュリティ）の第4回会合が、2018年8月29日（水）～9月7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10名を含む、37か国・諸機関から174名の参加があった。提出された寄書は144件（うち日本から6件）で、424件の臨時文書（Temporary Document）が発行された。

2. SG17全体にかかわる結果

2.1 最先端のサイバーセキュリティ攻撃とランサムウェアに関するワークショップの開催

会合前日の8月28日（火）に、「ITU Workshop on Advanced Cybersecurity Attacks and Ransomware」が開催された。サイバー攻撃の手法が高度化、悪質化する中で、攻撃の現状、技術的な対策の取組み、関連する標準化活動の状況、等について発表が行われた。標準化関連については、サイバー脅威の情報共有の仕組みが必要であることと、これらに関連する取組みについてSTIX/TAXIIがOASISで規格化されていることから、STIX/TAXIIのITU-T勧告化について検討を行うこととなった。

2.2 SG17体制の見直しに関する議論

2021年からの会期のSG17の体制見直しを進めるための活動として、コレスポンデンスグループ（CG-XSS：Correspondence Group on Transformation of Security Studies）を設立し、会合期間中は特別セッション「Transformation of Security Studies」を開催している。今回の会合では、新規の検討項目として耐量子コンピュータ暗号の検討を課題4のインキュベーションプロセスで検討を行い、前回の会合で提案されていた課題4、課題5、課題6、課題8の課題テキスト修正については、修正箇所を各課題で議論して、修正案をTSAGに送付した。主な修正箇所は、課題4はサイバーセキュリティフレームワークと脅威・脆弱性分析のためのAI（人工知能）/ML（機械学習）の利用の検討、及び、インキュベーション機能を持つことを追加、課題5はスパムの発信源、電子メールによるマルウェアの拡散、標的型攻撃、ランサムウェアに関する検討の追加、課題6は5Gセキュリティに関する検討の追加、課題8は課題タイトルを「Cloud computing and Big data infrastructure security」とビッグデータを新たに含め、ビッグデータに関する検討を含めたことである。コレスポンデンスグループCG-XSSについては、ToR（Terms of Reference）を更新して今会期中は継続することを合意した。

2.3 耐量子コンピュータ暗号に関する提案についての検討

量子コンピュータにより既存の暗号アルゴリズムが危殆化（解読が容易になること）するとされているため、量子コンピュータでも解読が困難な暗号の利用に関する提案が行われた。これらの提案については新規の取扱いとのことで、課題4に設置されたインキュベーション機能により検討された。提案は大きく2つの種類に分類され、1つは共通鍵暗号であるAESの改良、もう1つは、量子鍵配送（QKD：Quantum Key Distribution）である。AESについては、NISTで仕様化が進められISO/IEC JTC1 SC27で標準化されているため、ITU-Tの範疇ではないとのことからワークアイテム化しないこととなった。量子鍵配送については、まずは、テクニカルレポートのためのワークアイテムを設立して議論を継続することとなった。また、量子鍵配送に関する新規課題設立提案も行われたが、次回の会合で継続議論となった。

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全体にかかわる案件を担当している。今回の課題1においては、活動が停止となっているJCA-COP（Joint

Coordination Activity on Child Online Protection）の再開提案がチュニジアからあり、11月に開催されるITU PP-10の議論を経て次回のSG17会合で本提案を検討することとした。また、次回のSG17会合前日にAI/MLと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。

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、今回の会合では新規のワークアイテムや勧告発行を合意した文書はなく、主に、既存のワークアイテムの更新を行った。次回の会合で、X.sdnsec-3（Security guideline of Service Function Chain based on software defined network）を合意（Consent）する予定となっている。本勧告案では、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している。

・課題3では、ITU-T X.1051（Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations）に対する補足文書、Information security management users' guide for Recommendation ITU-T X.1051の更新に合意した。また、新規のワークアイテムとしてX.sup-csc（Critical security controls for telecommunications organizations information and network security management in support of ITU-T X.1051）を設立した。本文書もITU-T X.1051に対する補足文書となり、本勧告に関するベストプラクティスを含むものとなる。ISO/IEC JTC1 SC27との連携により進めていたX.cins（Guidelines for cyber insurance）については、SC27側で標準化を進めているISO/IEC 27102との方向性の違いにより、ITU-T側でのワークアイテムを削除することとした。

・課題6では、勧告案X.1042（X.sdnsec-1、Security services using the software-defined networking）を決定（Determination）した。SDNの機能を利用したセキュリティ対策について規定している。また、新規ワークアイテムとして、5Gにおける信頼関係に基づくセキュリティフレームワーク、IoTエラーログの標準フォーマット、IoT環境でのグループ認証における一括したメッセージ認証方式、IoTシステムにおけるセキュリティ制御、IoTデバイスとゲートウェイのためのセキュリティ要件の5件を設立した。

・課題13では、イーサネットをベースとした車内ネットワークのセキュリティガイドライン、自動車環境におけるクラウドベースのイベントデータ記録機構のセキュリティガイドライン、コネクテッドカーにおけるセキュリティ脅威情報共有のためのフレームワークの3件を新規ワークアイテムとして設立した。また、勧告X.1373（Secure software update capability for intelligent transportation system communication devices）の改訂作業を開始することを合意した。

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、勧告案X.1521（X.ucstix、Use Cases for Structured Threat Information Expression（STIX））を決定した。本文書では、STIXのユースケースとして、ランサムウェア、暗号通貨へのサイバー攻撃の事例を示している。また、サイバーセキュリティに関する情報交換のための勧告について議論してきたCG-Cybex（Correspondence Group on Cybersecurity Information Exchange Techniques）は、勧告化の作業が一段落したことから、今会合で活動を終了することに合意した。

・課題5では、前回の会合で決定したモバイルアプリケーションに埋め込まれた広告スパム対策の技術ガイドラインを規定する勧告案X.1249を再度決定した。投票においてコメントがあり、そのコメント解決により修正された箇所が多いためである。また、X.sup-ctss（Technical framework for countering telephone service scam）を補足文書として発行することに合意した。

・課題14では、X.srip-dlt（Security requirements for intellectual property management based on DLT）を新規ワークアイテムとして設立した。また、FG-DLT（Focus Group on Application of Distributed Ledger Technology）に対して、課題14の標準化ロードマップ、DLTに関する標準化活動の概要、課題14における用語集を送付し、連携を深めることとした。

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、クライアント・サーバモデルにおけるパスワード認証を強化するX.hakm（Guidelines on hybrid authentication and key management mechanisms in client-server model）及びモバイルインターネットサービスにおけるビッグデータ解析に対するセキュリティ要求とフレームワークを提供するX.srfb（Security require-ments and framework for big data analytics in mobile Internet services）を合意した。また、新規ワークアイテムとして、多要素認証におけるリスク特定のためのテクニカルフレームワークを提供するX.tfrca（Technical framework of risk identification to enhance authentication）を設立した。現時点で6件の勧告案を議論している。

・課題8では、新規ワークアイテムとして、クラウド環境におけるコンテナ仮想化技術に対するセキュリティ脅威の分析とガイドライン及び参照フレームワークの提供を行うX.sgcc（Security guidelines for container in cloud computing environment）を設立した。現時点で7件の勧告案を議論している。

・課題12では、実装者ガイドITU-T Z.Imp.100（Specification and Description Language implementer's guide-Version 3.0.2）を合意した。また、TTCN-3とSDL-2010関連の勧告の改訂版12件を合意した。現時点で27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.tac（Telebiometric Access Control with smart ID Card）を合意した。また、e-Healthに関する5件の勧告案（X.th2、X.th3、X.th4、X.th5、X.th6）が削除され、これら5つを集約した新規ワークアイテムとして、X.b2m（Biology to Machine Protocol）を設立した。現時点で2件の勧告案を議論している。

・課題10では、FIDO仕様の検討を行い、X.ctap（Client To Authenticator Protocol/Universal 2-factor authentication framework）及びX.uaf（FIDO Universal Authentication Framework（UAF））を合意した。現時点で、3件の勧告案と1件の補足文書を議論している。

・課題11では、X.CMS-prof（Cryptographic Message Syntax（CMS）profile）及びX.orf-gs（Object identifier-based resolution framework for IoT grouped services）を合意した。現時点で、8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1月22日（火）～1月30日（水）にスイス（ジュネーブ）で開催される。また会合前日の1月21日（月）には、AI/ML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。

■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13 中間会合	2018年 11月7日～8日	シンガポール	課題13の ワークアイテム全て
課題10 中間会合	2018年 11月12日～13日	日本（東京）	課題10の ワークアイテム全て
課題14 中間会合	2018年 11月12日～13日	日本（東京）	課題14の ワークアイテム全て
ワークショップ	2019年 1月21日	スイス （ジュネーブ）	AI/MLをテーマと したワークショップ
SG17会合	2019年 1月22日～1月30日	スイス （ジュネーブ）	

5. おわりに

今回の会合では174名の参加登録があり、寄書、及び、臨時文書の発行件数が過去最高との報告が行われた。アフリカ、アジア地域の国々からの参加者も多く、ITU-Tの中で最も活動が活発なSGの1つとなっている。多くの国がセキュリティに対して関心を持つ中で、これまでの検討項目から時代に即した検討項目への移行が求められており、今回の会合では量子コンピュータ実現後に必要とされる通信の暗号化対策における取組みの提案が行われた。今後も、同様の新規提案が出てくると考えられる。今回の会合では、ITUとして取り扱う項目範囲について議論が行われ、暗号に関する提案は却下されたが、今後も、多くの標準化団体が活動する中で、ITUが取り組むべき範囲について議論が行われていくと考えられる。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。