ITU-Tにおけるサイバーセキュリティの議論について

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）

1. はじめに

ITU-Tにおいては、Study Group 17（SG17、Security）において、ITU-T全体のセキュリティに関する議論が行われている。SG17では、現時点では14の課題により幅広いセキュリティに関するトピックを議論しているが、サイバーセキュリティも重要なトピックの1つである。本稿では、SG17における活動を中心に、ITU-Tにおけるサイバーセキュリティの取組状況を紹介し、今後の課題を整理する。

2. WTSAにおけるサイバーセキュリティの議論

ITU-Tでは、4年ごとに世界電気通信標準化総会（WTSA: World Telecommunication Standardization Assembly）を開催し、SG構成の確定、SG及びTSAGの議長・副議長の任命、勧告の承認、研究課題案の承認、決議の承認を行っている。ITU-Tで取り上げるべき重要なトピックについては決議を作成して背景と実施内容を明確化しているが、サイバーセキュリティに関連して以下の2件の決議が作成されている。

2.1　決議50　サイバーセキュリティ

2004年に開催されたWTSAにおいて制定された決議で、その後、各WTSAで更新されている。この決議では、主に、以下のことを求めている。

- ITU-T内でこの作業に高い優先度を与えること。
- 情報と電気通信システムをサイバー脅威やサイバー攻撃から守り、堅固にする必要性を引き続き認識し、情報通信ネットワークセキュリティの分野における技術情報の交換を促進するために、適切な国際機関及び地方組織間の連携促進を継続すること。
- サイバーセキュリティの用語を含め、電気通信／ICTの利用における信頼性及びセキュリティの構築に関連する用語及び定義の作成及び改訂についての作業を継続すること。
- サイバー攻撃から保護するため、また攻撃の出所の追跡を容易にするため、標準及びガイドラインの作成のために協力することが要請されるべきこと。
- インシデント対応の関連情報を共有するため、世界的かつ一貫した、また相互運用可能な手続が促進されるべきこと。
- ICT利用における信頼とセキュリティを高めるために、危機と脅威を緩和するため、地域と国際協力を強化することに緊密に協力すること。

サイバーセキュリティ全般においてITU-Tとして積極的に取り組み、国際連携、国際協力が必要であるとしている。

2.2　決議52　スパムへの対策／対抗

サイバーセキュリティにおいて特にスパムメール（迷惑メール）への対策を求めたものが別決議となっている。これは、世界的にスパムメールが電気通信事業に与える影響が大きいことと、広告メールのみではなく、攻撃を目的としたメッセージも多く存在することによる。本決議も2004年に制定されてから更新され続けており、主に、以下のことを求めている。

- 既存または将来の脅威に適切に対処するためにスパムに関するITU-T SG17の作業（勧告作成等）を促進すること。
- スパムに対する方針、規制、経済問題とその影響に関連する技術教育セッションやワークショップ活動を地域別に提供すること。

スパムの対象として電子メールのみではなく、SMS（Short Message Service）、音声通話、IP電話、マルチメディアサービス等での迷惑行為も含まれている。

3. ITU-T SG17におけるサイバーセキュリティ検討

ITU-T SG17においては、WTSA決議に従ってWP2（Cyberspace Security）がサイバーセキュリティを主に取り扱っており、2つの課題（課題4：サイバーセキュリティ、課題5：技術的手法によるスパム対策）で構成されている。本章では、SG17の状況として、この2つの課題の活動内容と、セキュリティに関する文書の整備、SG17に設立された地域活動について紹介する。

3.1　課題4　サイバーセキュリティ

課題4では、ネットワーク経由の攻撃への対策やセキュリ

ティ情報の交換に関する勧告を作成してきた。攻撃手法が高度化するにつれて防御のみではシステムを守ることは難しくなっているため、脆弱性を最小限にすることと信頼できるコミュニティと情報を共有することが重要となっており、課題4におけるプロジェクトの1つとして「サイバーセキュリティ情報交換フレームワークCYBEX（Cybersecurity information exchange framework）」に取り組み、これに関連する各種勧告を発行してきた。CYBEXは、サイバーセキュリティに関する情報を各機関で交換するためのフレームワークを提供しており、全体概要を示す勧告X.1500（Overview of cybersecurity information exchange）においては、技術的な視点から以下の6つのクラスターに分類されている。

(1) 弱点、脆弱性、状態に関する情報の交換を行うクラスター
(2) イベント、インシデント、ヒューリスティクに関する情報の交換を行うクラスター
(3) 情報交換のポリシー関する情報の交換を行うクラスター
(4) 識別、発見、問い合わせに関するクラスター
(5) 情報の正当性に関するクラスター
(6) 情報交換のためのプロトコルに関するクラスター

これらのクラスターごとに複数の勧告が作成されてきたが、これらの中には、外部機関で作成された文書または標準をITU-Tの勧告としたものも多い。例えば、米国のMITREで作成されたCVE（Common Vulnerabilities and Exposures）やCWSS（Common Weakness Scoring System）、FIRST（Forum of Incident Response and Security Teams）で作成されたCVSS（Common Vulnerability Scoring System）、IETFでRFC化されたIODEF（Incident object description exchange format）等がITU-T勧告として発行されている。広く利用されている既存の仕組みを利用しながら、全体のフレームワークを作りあげてきた。

3.2　課題5　技術的手法によるスパム対策

課題5では、これまでに電子メール、IPベースのマルチメディアサービス、SMSに対するスパム対策の勧告（対策技術、対策フレームワーク、等）を作成し、現在は、モバイルアプリケーションにおける広告、インスタントメッセージ、電話サービスに対する迷惑行為の対策のための勧告、補足文書作成を行っている。

3.3　セキュリティに関連する文書の整備

SG17では、セキュリティ活動に関連した文書の作成も進めている。セキュリティ・マニュアルと呼ばれている文書（Security in Telecommunications and Information Technology）では、ITU-Tでのセキュリティ活動概要、ICTシステムにおけるセキュリティ要件、セキュリティアーキテクチャ、ネットワークインフラのセキュリティ強化、インシデントレスポンス等について、勧告と関連付けて説明が行われている。現時点で第6版が発行されており、第7版に向けた改訂作業が進められている。「ICT Security Standards Roadmap」は、ITU-T、ISO/IEC、IETF、OASIS、3GPP、3GPP2、ATIS、ETSI、IEEE、RAISS Forum等で行われているセキュリティ関連の標準化状況、将来的に必要とされているトピック、ベストプラクティ等が紹介されている。これらの文書は、ITU-Tホームページからダウンロード可能となっている。
https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

3.4　地域活動

WTSA決議において地域における取組みを求めていることから、SG17傘下にアフリカの地域グループ（ITU-T SG17 Regional Group for Africa）とアラブの地域グループ（Regional Group for Arab Region）が設立された。これらの地域グループでは定期的に会合を実施し、各国におけるサイバーセキュリティ上の課題を検討するとともに、必要に応じてSG17会合への寄書の提出を行っている。地域で集まって検討を行うことにより、各国のサイバーセキュリティの取組みを活性化することに貢献している。この活動により、近年、アラブ、アフリカ地域からのSG17に対する寄書が増加している。

4．今後の取組みに向けた活動

通信ネットワークや通信サービスに対する攻撃が高度化することにより、セキュリティ対策の取組みも広げる必要が出てきている。現在、ITU-T SG17においては、SG全体のコーディネーションを行う課題1を含めて、14の課題が存在している。上記に紹介した課題4、課題5の取組み以外にも、通信システム（5Gを含む）、IoT、コネクテッドカー、クラウドネットワーク、Webサービス、等に対するセキュリティ対策の勧告作成を行っている。SG17の活動と成果を効率的なものにし、必要とされている取組みに応えるために課題構成の見直しが必要な時期に来ており、そのための活動も

行われている。本章では、今後の取組みに向けた活動について報告する。

4.1　CTO Consultation Meeting

ITU-Tでは、CTO（Chief Technology Officer）ミーティングを定期的に開催している。ICT企業におけるCTOが参加し、ICT業界における課題等を議論し、ITU-Tにおける検討に反映することを目的としている。2018年5月に米国で開催されたCTOミーティングでは、セキュリティに関して以下の2件のトピックが議論された。

1件目は、AIや機械学習（ML：Machine Learning）におけるセキュリティ、プライバシー、トラストである。AI・MLを利用したアプリケーションが、それらの有効性と効率性に着目して開発されており、セキュリティに対する配慮が欠けているのではないかとの指摘である。そのため、セキュリティの観点を考慮しないAI・MLの利用が、問題を起こす可能性があるとされている。一方で、AI・MLのセキュリティ分野への活用は、セキュリティアナリストの負担を軽減し、セキュリティ対策の高度化に貢献すると考えられている。SG17に対して、この両面から本件に関わる標準化の検討が求められた。

もう1件は、5Gにおけるエンド・ツー・エンドでのセキュリティへの移行である。5Gシステムは、SDN（Software-defined networking）、NFV（Network Function Virtualization）、クラウドコンピューティングの機能を包含していき、現在のネットワークから大幅にネットワークアーキテクチャや管理システムが変わってくるとされている。このような変更に伴い、5Gシステムのセキュリティの重要性が増すとともに、エンド・ツー・エンドでのセキュリティへの移行が加速すると考えられている。このような通信アーキテクチャやシステムの変化をサポートするような標準化が必要とされた。

4.2　CG-XSS

CG-XSS（Correspondence Group on Transformation of Security Studies）は、2017年9月から開始したSG17で取り扱うセキュリティ関連トピックとその検討方法を議論するための活動である。現時点で議論が行われている最中であるため、今後の議論において変更される可能性はあるが、これまでに出てきた今後取り扱うべきセキュリティトピックとしては、以下のものがある。

- AIのセキュリティ
  - いくつかの側面があり、AIのためのセキュリティ、セキュリティソリューションをサポートするためのAI、AIを利用したサイバー攻撃への対応、等がある。
- 量子暗号と鍵配送、量子コンピュータでも解読できない暗号アルゴリズムの利用
  - 現在の公開鍵暗号方式が危殆化する場合に備えた取組みを行う。
- ロボティックス
  - ロボット利用におけるセキュリティ対策、プライバシー対策が必要とされている。
- サイバー保険
  - サイバーセキュリティに対する保険の実施には、セキュリティリスクの評価や被害の影響度を計測できる必要がある。サイバー保険が広がる中で、これらの標準化が求められる可能性がある。
- ビッグデータ
  - ビッグデータが活用される中で、安全に管理、利用する方法は標準化されておらず、今後必要になる可能性がある。
- サイバーセキュリティ・サービス
  - サイバーセキュリティに関するサービスを利用する際に参照できる標準、ガイドラインの策定の検討。利用者の立場から、必要とされるサービスの基準、判断を行うことが難しいために、セキュリティ機能の導入が遅れることもあるため、それをサポートするような取組みを行う。
- SDN/NFV、5Gセキュリティ
  - 次世代のネットワークにおけるセキュリティ対策の検討を行う。

今後、SG17で取り扱うべきセキュリティトピックの検討とともに、現在の課題構成から新しい課題構成への移行方法等を議論することになっている。

5.　ITU-Tにおけるサイバーセキュリティに関する今後の課題

本章では、ITU-Tにおけるサイバーセキュリティの取組みにおいて課題となるポイントについて説明する。

5.1　新たなサービスやシステム、アプリケーションへの対応

4章で述べたとおり、ICT分野においては常に新たなネットワークサービス、ネットワークアーキテクチャが導入されようとしている。また、IoTやConnected Car等に見られるように、ネットワークの接続先が急激に拡大している。さ

らに、AI・MLの利用に見られるように、サービスの利便性を高める新たな仕組みがICT分野でも使われてきている。このような新しい技術やサービスに対して、セキュリティ部分の対応が不十分になりがちである。分野横断的な対応も必要となるため、幅広い分野を取り扱えるITU-Tにおいても、必要とされる対応を先取りする形で検討を行い、ガイドライン作成等に取り組むべきと考えられる。

5.2　ベストプラクティスをベースとした取組み

新たな攻撃が次々と開発される中で、セキュリティ対策はなるべく短い期間で迅速に行う必要がある。有効な対応策を普及させるには、各国が行っているセキュリティ対策のベストプラクティスをベースにして展開する取組みができれば、その有効性を確認しつつ、成功例を多くの国と共有できる可能性がある。各国の成功事例を展開できるような取組みが必要であると考えられる。

5.3　サイバーセキュリティ分野での国際連携、国際貢献

ITU-Tには、政府レベルで発展途上国を含めた数多くの国が参加している。サイバーセキュリティ対策は各国における重要な課題となっており、多種多様な提案が行われている。各国によってセキュリティ及びプライバシーに対する考え方や、ネットワークサービスの提供形態が異なることから、ITU-Tとして実施する内容として合意が得られにくい場面もあるが、政府レベルで議論が行える場であることから、サイバー攻撃に対する国際連携について、どのような取組みができるかを検討することは重要であると考えられる。また、発展途上国を中心としてセキュリティ対策の取組みを国レベルで向上させるべきとの認識がある中で、ITU-D等との活動と連携しながら、全体的なセキュリティレベルの底上げに貢献する勧告等の作成が必要である。

6. おわりに

ネットワーク経由のサイバー攻撃の手法が高度化し、攻撃自体の検出も難しくなってきている。また、IoT、5G、SDN/NFV、AI・ML、といった新たなネットワーク技術やサービスが展開される中で、それらに対するセキュリティ対策も必要となってきている。サービス利用者側のみでのセキュリティ対策では防ぐのが難しくなってきている面もあり、国レベルの取組みや国際連携の取組みにより安全性を強化する必要性が高まってきている。ITU-Tは、国レベルの取組みを議論できる数少ない標準化活動であるため、将来の安全なネットワークサービスの提供やネットワーク利用のためにも、有益な議論ができればと思う。