# 8年間のITU-T SG17（セキュリティ）副議長を終えて

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　三宅（みやけ）　優（ゆたか）

## 1. はじめに

2016年のWTSAでITU-T SG17副議長を拝命し、2017～2024年の期間でその役職を担当してきました。ITU-T SG17の活動に参加したのは2005年であり、約20年間の月日が経過しましたが、副議長職退任にあたり、ITU-Tにおける最近の自身の活動やITU-T SG17に期待することについて述べさせていただきます。

## 2. 副議長時代の活動について

### 2.1　WP（Working Party）議長

コロナ禍により副議長1期目の期間が2017～2021年、2期目の期間が2022～2024年となりましたが、1期目はWP1議長、2期目はWP2議長を担当しました。WPの番号は異なりますが所属している課題（Question）は同じで、通信ネットワーク、IoT（Internet of things）、ITS（Intelligent Transport System）のセキュリティを扱っていました。新しい通信サービスが展開される中で、通信ネットワーク自体のセキュリティ対策やそれらのサービスに利用されるデバイス等のセキュリティ対策が主な対象となっており、日本からも積極的に寄書を提出し勧告作成に貢献しました。

自身は、これらの活動に対してIoTサービスで収集されるパーソナル情報の制御機構やIMT-2020（5G）／IMT-2030（6G）に関わるセキュリティについて勧告作成に貢献してきました。特に5Gのセキュリティについては、ネットワークの構成、展開されるサービス、ネットワークインフラの構築方法が大きく変わるため、そのセキュリティに対して懸念が示されてきたこともあり、ITU-Tとして何ができるかを検討しました。そこで、5Gセキュリティタスクフォースを立ち上げ、他の標準化機関やフォーラム等が発行している5Gセキュリティに関する資料を整理してITU-T SG17として実施すべき内容を示した「5Gセキュリティ標準化ロードマップ」を作成して公表するとともに、日本からの提案を含めて5Gセキュリティに関わる複数の勧告作成に貢献しました。

### 2.2　FG NET-2030（Focus Group on Technologies for Network 2030）副議長

2018年にITU-T SG13（Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures）がFG NET-2030を設立しました。これは、2030年を目途としたネットワークのユースケースと要件及び要件を満たすために必要な機能に関する検討を目的としたITU-Tのメンバー以外も参加できる活動です。議論の結果は成果文書（Deliverables）としてまとめられ、ITU-Tの関連するSGで勧告の作成を進めることとなります。このFGの設立時にSG13からSG17に対してセキュリティを担当するFG副議長推薦の要請があり、SG17副議長の中で通信事業者から参加している筆者が担当することになりました。活動期間は2年で、新しいサービスやアプリケーションの検討とこれらの実現に必要となる機能の整理が行われ、8件の成果文書が作成されました。この検討において通信プロトコルとして「New IP」の必要性が主張されましたが、既存のTCP/IPを置き換えるものとして捉えられたことによりIETFも巻き込んでこの取組みの停止を求める意見が出てきました。そのため、SG13において成果文書をベースとした勧告化を進めることに対して反対する国が増えたため、このFGの結果の反映は成果文書の一部のみとなりました。検討は興味深いものでしたが、政治的な面も強い活動となりました。

## 3. ITU-Tにおけるセキュリティ標準化について

副議長を担当したSG17は、ITU-T全体のセキュリティに関する検討を行っています。SG17の標準化活動を通じて感じたことを本節で述べさせていただきます。

### 3.1　セキュリティ標準化の対象

ITU-Tは様々なトピックを取り扱っていますが、その多くに対してセキュリティ上の問題を検討する必要があります。また、ITU-Tで取り扱っていないトピックであっても、電気情報通信に関わるサービスやアプリケーションについてのセキュリティや電気情報通信設備のセキュリティ対策について


も検討の対象になり得ます。すべてのセキュリティに関する項目をITU-Tで議論することは難しいため、ISO/IEC等の他の標準化機関との棲み分けや連携は課題の1つになっています。基本的なセキュリティ機能や安全性の評価が必要なもの（例えば、暗号アルゴリズムや暗号プロトコル等）、セキュリティやプライバシーに関わるポリシーを決めるようなものは勧告化の対象外とされていますが、新規ワークアイテムとして提案されているものにはITUで取り扱うには不適切と考えられるものも増えてきています。SG17として無尽蔵に議論に時間を費やすことができるわけではありませんので、業界にとって有益となる勧告が何であるかを考えながら明確な基準を決めてワークアイテムの設立の可否を判断していく必要があると感じています。

### 3.2　セキュリティ標準化の種類

SG17で議論される勧告案はいくつかの種類に分類されます。一般的な通信やネットワークに関わる標準化では、異なるメーカーの機器であっても相互に接続して通信が行えるようにするための仕組みを規定するものが多く、セキュリティの分野でもそのような勧告が存在しますが、セキュリティ分野で特徴的なのは、必要とされるセキュリティの基準を定めるものです。各種の攻撃からデータやインフラを守るためには多層的なセキュリティ対策が必要とされますが、何をどの程度まで行う必要があるかを決めるのは容易ではないため、その指針を示すために各種サービスやシステムに対するセキュリティ要件やガイドライン的な勧告が増えつつあります。実装者やサービス提供者にとっては、セキュリティ対策を検討する上で参考にはなるものの、勧告作成の段階で求められるセキュリティ要件の妥当性を評価することが難しいことと、勧告のセキュリティ要件に従って実装されたものとそうでないものとの差が分かりにくいことから、有効に活用できていない印象があります。例えば、クラウドセキュリティの世界では各種のセキュリティ認証が提供され、事業者側が認証を取得したことを示すことにより安全性が確保されていることを利用者に示すことができます。ITU-Tでは現時点ではそのような認証制度を持っていないため、勧告に応じてセキュリティ対策を行ってもその有効性をアピールできない印象があります。文書で示すだけではなく、勧告が利用されるための枠組みの検討も必要かと感じています。

## 4. おわりに

ITU-Tの標準化活動は他の標準化活動に比べて多くの国々が集まることが特徴で、各国の状況が把握できる貴重な場だと思います。特に、サイバーセキュリティ対策については多くの国で課題となっており、国際連携等により安心・安全なネットワーク環境を構築できることが必要とされていることを感じています。ITU-Tで取り扱うトピックが広がり、それに応じてSG17で取り扱うトピックが増えてきて作成されるセキュリティ関連の勧告数は多くなっていますが、利用されているものが少ないとの意見もあります。研究会期が変わり新しく就任した議長は産業界との連携と標準化活動の近代化を掲げており、議論の方向性も変わってくる可能性があります。通信・ネットワーク事業者やサービス事業者、機器ベンダー等が利用しやすく、さらに、サービス利用者が安心・安全なサービスであることを認識できるような取組みが進むことを期待したいと思います。

（2025年1月24日 ITU-T研究会より）