TTCに寄せて

セキュリティに関わる国際標準化活動を振り返って

～総務大臣表彰を受賞して～

株式会社KDDI総合研究所
三宅　優

1．はじめに

この度は、「ネットワークセキュリティに関する国際標準化への貢献」に対して、情報通信技術賞　総務大臣表彰という名誉ある賞をいただき、大変光栄に感じております。これまで、セキュリティに関わる研究開発や標準化活動をご一緒に進めてきた皆様のご支援とご協力の賜物と思います。この場をお借りして、関係者の皆様に深く感謝を申し上げます。

国際電信電話株式会社（当時）に入社後、ネットワークに関わる研究に従事し、OSI ネットワークを扱う ISO/IEC JTC1 SC6 や、ローカルエリアネットワーク／無線ネットワークを扱う IEEE802 委員会等の国際標準化活動も行っていました。その後、ネットワークにおけるサービス利用が広がる中でサイバー攻撃の懸念が高まり、セキュリティに関わる研究にも従事することになりました。その後、2005 年から ITU-T Study Group 17（以下「SG17」と記す）に参加して通信に関係するセキュリティの標準化に関与することになりました。SG17 に参加以降、ネットワークを利用した各種サービスの拡大により不正利用が増えてきたことによりセキュリティに関わる問題も増加し、SG17 で取り扱うセキュリティに関するトピックも増えて来ました。今後も、ネットワークの高機能化（5G から Beyond 5G/6G への移行）や通信インフラの高度化・複雑化、AI 技術等の発展により、セキュリティ対応が重要な課題になると考えられます。本稿では、これまでの SG17 における自身の標準化活動を振り返るとともに、セキュリティに関わる国際標準化の課題や今後について自身の思いを述べさせていただきます。

2．通信ネットワークのセキュリティ対策

モバイルネットワークを含めた通信ネットワークは、制御通信とデータ通信の分離等によりインターネットに比べて比較的安全と言われており、モバイルネットワーク特有の無線部分のセキュリティも脆弱性対策が進められながら発展をしていきました。しかし、インターネットの発展により、電話等のネットワークもコア部分はインターネット技術を利用したパケット交換網の活用が進み、モバイルネットワークにおいてもインターネットとの融合が進んで来ました。特に IMT-2020/5G 世代のネットワークにおいては、以下のような大きな変化が起こっています。

- モバイルネットワークにおいてもネットワークの制御にインターネットで利用されているプロトコルの導入が進み、インターネットとの接続がよりシームレス化された。
- ネットワークスライシング、マルチアクセス・エッジ・コンピューティング（MEC: Multi-access Edge Computing）等、ネットワーク側での高度な機能の提供が行われるようになってきた。
- ネットワーク機能の仮想化（NFV: Network Functions Virtualization）により、ソフトウェアで仮想化されたネットワーク機能を組み合わせてネットワークのインフラ構築が可能となった。
- ソフトウェア定義ネットワーク（SDN: Software-Defined Networking）により、ネットワークの構成や制御をソフトウェアで集中管理するアーキテクチャを利用できるようになった。

このような変化により、通信ネットワークが複雑化するとともに数多くの新規サービスが立ち上がっていくことにより、攻撃の対象となるポイントが増加することになりました。モバイルを含む通信ネットワークでの不正行為や障害を発生させるような攻撃は社会的な影響が甚大となるため、米国や欧州は国家レベルで 5G セキュリティの対応を進めることとなり、日本としても総務省を中心として検討が行われ、5G ネットワークの安全性を確保するための包括的な指針として「5G セキュリティガイドライン」を 2022 年発行しました。本文書の作成に私が関わっていたため、本文書の内容をベースとしたものを ITU-T 勧告化することを提案し、2024 年に勧告化されました。

IMT-2020/5G のセキュリティ対策で顕著になったのは、通信ネットワークとインターネットの融合の促進、通信ネットワーク側から提供される機能の多様化、通信ネットワークのインフラの仮想化とオープン化により複雑性が増しセキュリティ上配慮すべき事項が増えてきたことです。今後もその傾向は続くものと考えられますが、セキュリティ対策の観点からも負担が増加している状況で、ネットワーク全体で統一的なセキュリティアーキテクチャで対応を行うなどの仕組みが重要になってくると考えられ、標準化の立場からもこの動きを支援できると思います。

3．迷惑メール対策

ITU-T SG17 では、2005 年に迷惑行為に対する技術的対策を議論する課題、Countering spam by technical means を設立しました。各種の迷惑行為を対象としていますが、主たるものは迷惑メール対策となっていました。当時から、全体の電子メールに対する迷惑メールの割合は 50% 以上を占めており、先進国、発展途上国を問わず、インターネットを利用している多くの国において社会問題化していました。

ITU-T では、迷惑メール対策の勧告が作られてきましたが、これとともに、補足文書として迷惑メール対策の情報を共有する Supplement 6 to ITU-T X-series Recommendations: ITU-T X.1240 series – Supplement on countering spam and associated threats が米国の提案により作成されました。本文書では、迷惑メール対策に関する国際的な活動と米国の取り組み事例が含まれていましたが、この文書を更新する形式で日本の事例を含むための改訂作業を行い、2009 年に更新版が発行されました。日本においても迷惑メールは社会問題化していたため、総務省が中心となって官民連携の取り組みを行い、協議会の設立や法制度の整備（特定電子メールの送信の適正化等に関する法律、等）、通信事業者における技術的な対策（OP25B や送信者認証技術の導入）や事業者間連携を進めてきました。これらの取り組みを通じで、国単位の迷惑メールの送信数は、2005 年時点において全世界で９位であったものが 2009 年には 33 位となり、日本におけるインターネットの普及状況を考慮すると効果が発揮されている状況でした。現在では各国でも法整備や技術的な対策の導入が進んでいますが、日本の先進的な取り組みを文書に記してアピールすることにより、各国での取り組みに貢献できたと思います。

現在では、個人間の情報交換ではチャットサービスに移行してきていますが、企業間や企業と個人の連絡には、電子メールが広く利用されている状況には変わりはありません。迷惑メールへの技術的な対策は進んできましたが、迷惑メール送信者もそれを回避するような取り組みを行っており、全メールに対する迷惑メールの割合は極端には減っていない状況です。インターネットでは、金融資産やポイントを取り扱うサービスが増えている状況で、金銭的に被害を与えるフィッシング詐欺も増えているとともに、企業等に対して脅迫行為を行うランサムウェア攻撃の入り口にもメールが使われています。特に、2025 年初頭からの日本の証券会社を対象としたフィッシング攻撃により不正な取引が行われ、サービス利用者に大きな被害が出ました。生成 AI 技術の発展により、迷惑メールの文章も洗練された日本語が使われるようになり文面のみでは不正なメールと見分けがつかなくなったことと、アカウントを乗っ取るための手法も高度化してきていることから、フィッシングメールを見抜くのが困難になってきています。また、世界的に見ても日本に対してフィッシング攻撃を目的とした迷惑メールが急激に増加している状況です。サービスを提供している各社は認証方法の高度化等の対策を進めていますが、攻撃の入り口となる迷惑メールの対策も重要課題であるため、今後も継続的な取り組みが必要かと考えられます。

4．ネットワークサービスにおけるプライバシーに関わる情報の取り扱い

ネットワーク上のサービスが多様化するにつれて、個人のプライバシーに関わる情報もサービスに提供する必要が生じてきました。KDDI 総合研究所では、サービスの利用者が自身のプライバシーに関する情報の提供を制御できるフレームワークとして PPM（Privacy Policy/Preference Manager）を 2012 年に提案し、そのコンセプトをベースに各種の実証実験等を行ってきました。また、KDDI が提供する「au ID ポータル」のプライバシー設定機能としても利用されました。これらの成果をベースに標準化の取り組みも実施しました。最初に、異なる IoT プラットフォームやデバイス間の相互運用性（インターオペラビリティ）を実現するための共通のフレームワークを提供することを目的とした oneM2M の活動においてプライバ

シー情報の制御技術として提案し、2019 年に発行された「ONEM2M TECHNICAL SPECIFICATION TS-0001 Functional Architecture」、「ONEM2M TECHNICAL SPECIFICATION TS-0003 Security Solutions」に標準仕様として反映されました。これらの文書は、ITU-T SG20 において Y.4500.1、Y.4500.3 として 2023 年に勧告化されています。また、本コンセプトを一般的なシステムに適用できるようにしたものを「X.1363 Technical framework of personally identifiable information（PII）handling in Internet of things（IoT）environment」として、SG17 で 2020 年に ITU-T 勧告化しました。

現在のスマートフォン等ではアプリ単位でサービス事業者側に提供する情報の可否を設定するための機能が標準的に備わっており、サービス事業者側でも提供されたプライバシーに関わる情報の制御を利用者に行わせるための機能を持っているものが増えてきています。生成 AI 技術等の発展により、より多くのセンシティブな情報の提供を求めるサービスが増えてくる中で、情報の管理機構の透明化や基準作りが求められており、プラットフォームやサービスごとに異なる仕組みでは利用者にとっての利便性が低下するのみではなく、意図しない情報の流出も考えられます。また、プライバシーに関わる考え方は国や地域で異なることもあり、統一化は容易ではないとも考えられます。国際標準化を通じて利用者に寄り添った仕組みが提供されることを期待したいと思います。

5．おわりに

2005 年から ITU-T の活動に参加し 20 年が経過しました。社員としての主たる業務は研究員としての活動でしたが、ITU-T SG17 においてはセキュリティ標準化の活動を行い、2011 年からは TTC セキュリティ専門委員会の委員長として日本国内の活動の取りまとめも行わせていただきました。これらの活動においては、研究と標準化の双方の活動がお互いに役に立ったと感じています。

ITU-T SG17 の標準化において感じたことは、対象とする分野が広いということです。対象とする範囲が情報通信分野に関わるセキュリティとのことで、セキュリティアーキテクチャ、通信・ネットワークシステムのセキュリティ、情報セキュリティマネジメントシステム、サイバーセキュリティ、迷惑メール対策、IoT・デジタルツイン・メタバースのセキュリティ、サービスセキュリティ（AI セキュリティを含む）、クラウドセキュリティ、テレバイオメトリクス、ID 管理、公開鍵認証（PKI）、ITS セキュリティ、分散型台帳技術（DLT）セキュリティ、量子技術を利用したセキュリティ（量子鍵配送（QKD）を含む）が現時点で議論の対象となっています。セキュリティの検討を行うには対象となる分野の技術的な仕組みを熟知した上でそのセキュリティ上の問題点と対策を検討する必要があるため、かなりの専門性を要求されます。また、１つのトピックにおいても複数の観点からのセキュリティ検討の必要があり、議論されている勧告案の内容を的確に把握するには、広い範囲のセキュリティの知識を必要とされます。そのため、ワークアイテムが設立されてもそのワークアイテムの勧告案を更新するための寄書はワークアイテム提案者のみになることが多く、複数の国から寄書が提出されて技術的な議論が行われるケースが少なくなっている印象がありました。有益な勧告にするためには多くの人が興味を持ち、関与しながら作成して完成度を向上させていくことが重要ですが、提案者のみが寄書を提出して勧告案を更新していくスタイルでは、文書の品質上の問題が発生する可能性があります。ワークアイテム設立時のテンプレートでは寄書提出の意向がある組織を複数記入する仕組みも設けましたが、状況は改善していないため、さらに踏み込んだ対策が必要かと思われます。

セキュリティの標準については、大雑把にですが、各社が開発したシステムを相互接続させるための技術仕様を定めたものと、必要とされるセキュリティ要件を示すものに分類することができます。後者は特にセキュリティの標準化としては重要なもので、多くのセキュリティ上の問題が存在する中で、どのようなセキュリティ対策がどのレベルまで必要とされるかが規定されていれば、実装者や運用者はセキュリティ対策を行いやすくなります。ITU-T SG17 においてもそのような勧告は多く存在しますが、どの程度利用されているかは分かりにくい状況です。本来であれば、ITU-T 勧告によるセキュリティ対策を満たしているものに対しては認証を付与してその付加価値を高めることができればよいのですが、認証機構の立ち上げや認証プロセスの運用は多大なコストがかかるため、ITU 内でも議論はされることがありますが、実現されていません。多くのシステムやサービスでセキュリティ対応が必要とされている中で、クラウドサービス等に対

してはセキュリティ認証の仕組みがあるものの、この仕組みが必要とされるその他の分野に広がっているとはいいがたい状況です。標準化の取り組みの観点からも、利用者が納得して利用できるように、サービスやアプリケーションのセキュリティの対応状況を可視化できる世界を実現することが必要かと思います。

通信ネットワークの高機能化やサービスの多様化、新技術の導入により、今後もセキュリティ対策は重要な取り組みの１つであることは続くと考えられます。通信インフラの重要性を鑑みると、セキュリティ事故の発生を先回りして予測し、その対策技術を普及させるとともに、事故が発生しても復旧時間を最小にするための仕組みが求められます。そのためには、個々の組織のみで対応するのではなく、国レベルや国際連携による対応も重要になってくると思われます。その意味において、政府と民間が参加する ITU の取り組みは、これを議論するには最適な場かもしれません。事故が発生して注目されるのがセキュリティ分野ではありますが、サービスやシステムの発展に従ってもたらされるリスクを先読みして対応していく取り組みにより、重要なインフラである通信サービス利用者の安全を確保していくことが必要かと思います。

最後になりましたが、標準化活動を含めて各種の活動で私をご指導いただいた先輩方、同僚の皆様、および、活動をともにしていただいた各社・機関の皆様に心よりお礼を申し上げます。