



主役登場

エンジニアリングから研究所へ

奥田 哲矢

NTT社会情報研究所
研究主任

大学生のころからエンジニアリングが好きで、研究よりWebアプリ開発に熱意がありました。入社後はWebサービス開発を行い、現在の専門はセキュリティプロトコルの設計です。

前職のエンジニア時代に、常時SSL/TLS化、完全HTTPS化、というWebサービス業界のトレンドを経験しました。その後、研究所に戻ってからはSSL/TLS等の暗号利用に関する事業相談窓口を担当していました。その過程で、暗号を利用するセキュリティプロトコルの奥深さに夢中になりました。Webサービスで一般的に利用されるプロトコルの多くのデファクトスタンダードを定めるIETF(Internet Engineering Task Force)の会合に時々参加しており、IETFが発行する標準仕様書のRFC(Request For Comment)を読むのが日課であり趣味となっています。以前は、事業会社の問合せが多いSSL/TLSを中心に読むことが多かったのですが、セキュア光トランスポートにかかわり始めてからIPsecも読むようになりました。その知見がセキュア光トランスポートのアーキテクチャ設計に活かされていると信じています。

本特集記事『セキュア光トランスポートネットワーク』は、光・量子といった物理学に基づく装置と、耐量子暗号という代数に基づく仕組みを、形式検証という論理的なツールに基づいて検証した、Integrateの大変なプロジェクトです。アーキテクチャ設計という観点では、多少は貢献できていると信じたいのですが、実際は、それぞれの分野の研究者やエンジニアに頼りに頼ってプロジェクトが進行中です。

これからのICT産業についても、理論と実装・実践の

双方が求められることは明らかで、NTTも優秀な研究開発エンジニアを育てられるように、各自が研鑽と発信を行っていくことが大事だと考えています。

なお、本特集記事『データから価値を連鎖的に生み出すトラステッド・データスペース』にもかかわっていることもあり、現在の私のマイブームは、TEE(Trusted Execution Environment)を中心とするTrustedな技術群と、TEEを含む機器認証に利用するRemote Attestationです。Trustedと呼ばれる技術群は、多くの場合、外部から信頼性や正当性を検証可能であることが要求されます。TEEはRemote Attestationというプロトコルによって、遠隔からハードウェア&ソフトウェアの信頼性を検証できます。検証可能なハードウェア&ソフトウェアの属性情報としては、IETFの議論にのっとれば、ハードウェアID/製造者/モデル/バージョン、ソフトウェアID/作成者/パッケージ/バージョン/コードハッシュ値などがあります。

Remote Attestationプロトコルで保証する属性情報を、より人間社会や産業に近い分野に拡張すれば、遠隔のコンピュータを、自分の代理(デジタルツイン)として働かせる未来に貢献できると考えています。さらに、デジタルツインは、周囲のヒト・モノ・環境と相互作用しながら、その信頼性や正当性をRemote Attestationして、Trustedな世界を広げていくことでしょう。

これら技術群を自ら開発して、NTTグループの幅広い産業領域に適用・応用していくことが、現在の私の主要なミッションであり、日々ロマンを感じながら研究開発業務を推進しています。