移行期にあるネットワークサービスセキュリティ WG 活動成果報告

只木　進一
佐賀大学 工学系研究科知能情報システム学専攻

高等教育機関や研究機関などにおける教育、研究、組織業務は、情報システムへの依存度をますます増している。増大する依存度に比して、それらの組織による情報システムへの投資は、金額だけでなく人員の点でも不足しており、結果として情報システム部門への負担が大きくなっている。こうした状況に対応策の一つとして、クラウド活用が現実的解として浮上している。

一方、組織内ネットワークの基盤であった IPv4 サービスは、アドレス枯渇が現実に発生した。今後増え続ける情報機器の接続のため、IPv6 への対応を真剣に考える時期にも来ている。

このように、高等教育機関や研究機関などの情報サービスは大きな移行期に来ている。このような時期のセキュリティについて、本 WG では、クラウド活用と IPv6 利用の二点から検討を行った。

クラウドサービスは、急速な成長を見せている。アプリケーションサービスを提供するものから、データベースや Web サービスなどの基盤サービスを提供するもの、OS そのものを提供するものなど様々である。価格も手ごろとなり、自組織保有のコストに比べて安い場合も多い。個人向けの無償あるいは廉価なサービスも充実してきている。そのため、民間企業ではクラウドサービス活用が進んでいる。

一方で、高等教育機関や研究機関などのクラウドサービス利用は、あまり進んでいない。高等教育機関や研究機関などのデータには、個人情報や組織の機密情報などが含まれるため、セキュリティへの不安感があることと、どのように利用を開始して良いかが分からないことが原因であろう。そこで、クラウドサービスのデータやシステムの独立性、同一サービス内でのデータ秘匿性などを調べ、自組織がそのサービスを利用可能であることを判定できる指標作りを WG の一つのテーマとした。

クラウドサービスにおけるセキュリティ事故の状況から始め、自組織システムと異なるセキュリティの確認ポイントを整理し、チェックシート様式とした。なお、このチェックシートは、広島大学の様式を参考とした。

現在の IPv4 アドレスの枯渇が 1990 年代前半から指摘され始め、IPv4 の次の版として IPv6 が 1995 年に提案された。2011 年には、アジア太平洋地域で IPv4 アドレスの枯渇が現実のものとなった。一方で、個人用 PC をはじめとした情報端末は着々と IPv6 対応となっている。

このような状況の下、組織ネットワーク管理者が IPv4 しかサービスしていないと考えていても、組織内ネットワークから IPv6 通信が外部に漏れる状況が発生している。本 WG では、この点をセキュリティの観点から検討し、IPv6 ネットワークのトンネル通信の方法とその対策を整理した。特に、ファイアウォールでの設定ポイントをまとめた。また、IPv4 ネットワークを利用している組織の IPv6 への向き合い方についても、一つの方法を提案した。

高等教育機関や研究機関などの情報システムのクラウド利用は着実に進むと予想される。また、IPv6 通信への対応も必要となることが予想される。本報告書が、会員組織の、クラウド利用や IPv6 利用におけるセキュリティ対策の参考になることを望む。