滋賀大学のネットワークシステムとセキュリティ対策のポイント

情報処理センター　中川 雅央

情報革命の時代

第４次情報革命とも言われる今、IoT（Internet of Things）やIndustrie4.0といった言葉が日常的に使われるようになりました。これらは、身の周りのあらゆるモノが新しい技術でつながっていくことで産業界のみならず、私たちの暮らしにも変化をもたらすことを示しています。

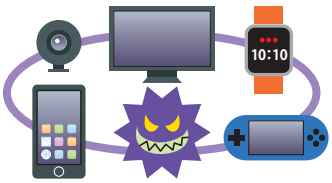

図1：あらゆる機器が攻撃対象

一方、このようにネットワークが形成されれば、それを媒体とする犯罪、いわゆるサイバー攻撃を受ける可能性も出てくることになります。図１に示すようなスマートフォンやＩＰカメラなど、有線・無線を問わずネットワークに接続される機器は、すべて攻撃対象になっているとも言われています。

本稿では、このような変化の著しい世界において、私たち滋賀大学はどのような形で対策を講じているのか、その一部を簡単に紹介し、学生の皆さんに注意喚起したいと思います。

滋賀大学スマート・ラーニング・コモンズ

これまで整備されてきた学内のスペースに対して、ICTを援用したグループワークなどの創造的な活動のための場とすることで、より高度な学習資源が利用可能な「スマート・ラーニング・コモンズ」として新たに整備しました。図２に示すように、近い将来のBYOD（bring your own device）という学習者自身が使っている情報デバイスで違和感なく自然に学習できるスタイルを想定して、特定の空間だけではなくキャンパス全域において、いつでも、どこでも、自ら学習や教育指導を受けることができる環境を想定して整備しました。

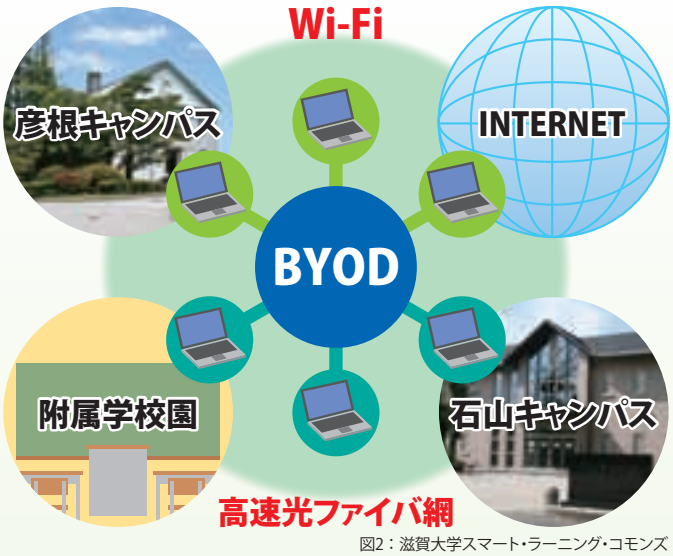

図2：滋賀大学スマート・ラーニング・コモンズ

モバイル情報機器のリスク

スマートフォンなどの高性能なモバイル情報機器が広く普及することで、プライベートな情報もインターネットを必ず経由する形に変化しています。暗号化などの技術的な情報保護の仕組みはあるものの、利用者の誤った設定や操作によって、コンピュータウイルスなどの不正なアプリが紛れ込むリスクは小さくありません（図３）。また最近の標的型攻撃と呼ばれる手口では、特定の個人に対して宅配便業者や銀行員など実在の人物を騙って、個人情報や暗証番号をだまし取ろうとします。ネット上の便利なサービスに似せたフィッシング詐欺サイトも多数確認されていますので、正規のサイトか否かよく確認しましょう。

図3：モバイル情報機器を取り巻くリスク

セキュリティ対策

このような脅威からスマート・ラーニング・コモンズに接続される皆さんのモバイル情報機器を守るために、滋賀大学のネットワークシステムは図４に示すようにUTM（Unified Threat Management）装置を活用する構成にしています。このUTM装置は旧来のファイアウォールと違い、利用するアプリの種類に応じて通信を監視したり制限したりすることができるなど、これまでよりも高度な機能によってセキュリティを確保する仕組みになっています。さらに、皆さんのパソコンやスマートフォンなどにセキュリティ対策ソフトを必ずインストールして、スマート・ラーニング・コモンズを大いに活用してください。しかし、これでも万全とは言えません。やはり皆さんの知識と行動が重要なポイントです。

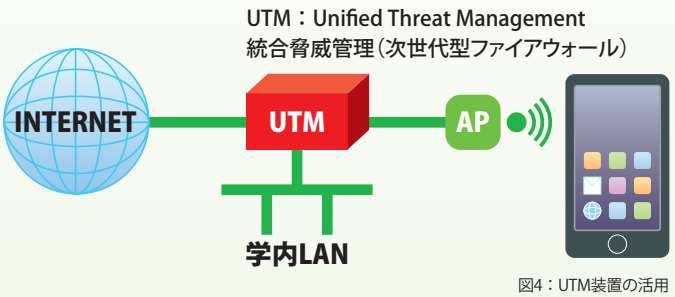

図4：UTM装置の活用