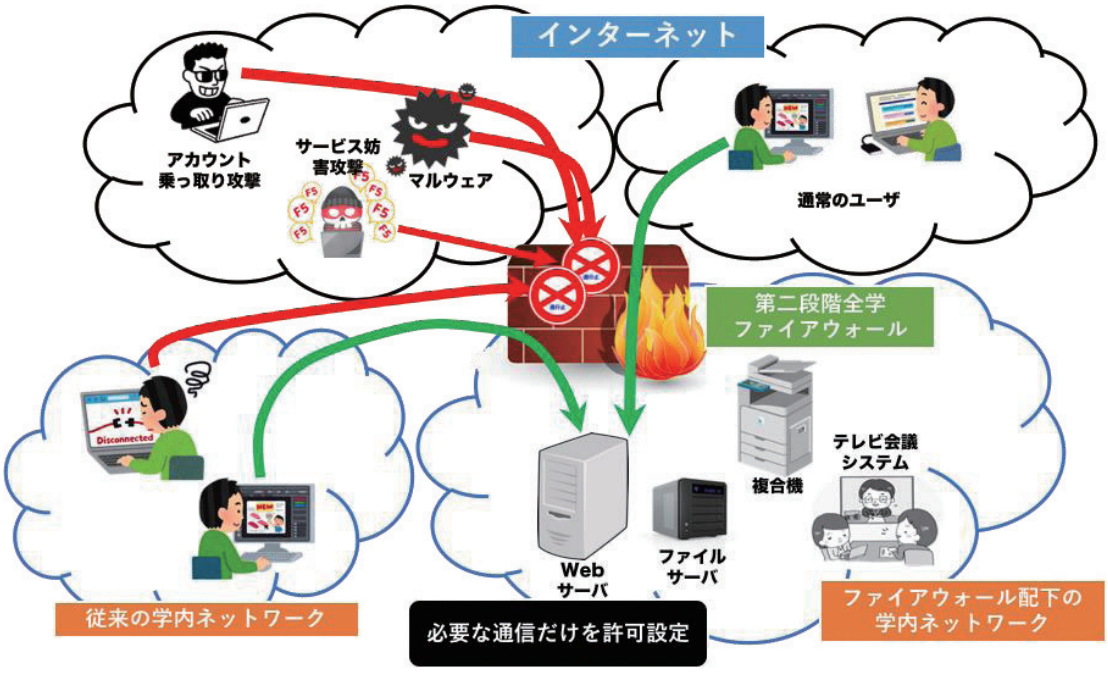
第二段階全学ファイアウォールの概要

現在、各部局の皆様に対してセキュリティを強化した「PROTECTED ネットワーク」の提供を行っております。これは、「第一段階全学ファイアウォール」として 2016 年 12 月から提供されているネットワークであり、主に利用者端末を守るためのネットワークです。現在までに、21 部局の方にご利用頂いています。

この「PROTECTED ネットワーク」に続く次の段階のファイアウォールとして、「第二段階全学ファイアウォール」の提供が予定されています。以前から全学ファイアウォール説明会や UTNET ミーティング等で、ネットワーク担当者の方には情報をお伝えしておりましたが、この度その概要と提供時期が固まりましたので、ご報告します。

第二段階全学ファイアウォールは、主にサーバ等の外部からアクセスされる機器を守るためのネットワークを提供します。外部からアクセスされる機器とは、例えば Web サーバ、ファイルサーバ、テレビ会議システム等です。これらの機器に対する学外からのアクセス、ならびに学内からのアクセスも、次の図に示すようにネットワーク単位もしくは IP アドレス単位で通信を制御することができます。



第二段階全学ファイアウォールの動作概要

第二段階全学ファイアウォールに対する通信制御の設定は、部局ネットワーク管理者、もしくは部局ネットワーク管理者から権限委譲を受けたネットワーク管理者が行うことができます。この設定のために、専用のポータルサイトを提供します。ポータルサイトでは、UTIP と呼ばれるグローバルアドレスの利用者を管理する機能と、UTAC と呼ばれる通信制御設定を行う機能が提供されます。

ポータルサイトにおける UTIP（左）UTAC（右）の画面

外部からアクセスされる必要のある機器に対して、必要なポート番号とアクセス範囲を設定することができます。部局ネットワーク管理者や部局ネットワーク管理者から権限を委譲されたネットワーク管理者には、このポータルサイトのアカウントが発行されます。自身のアカウントでログインして頂くと、設定する権限を持つネットワークに対して UTIP と UTAC の機能を利用し、IP アドレスの利用者の登録や IP アドレスに対するアクセスリストを設定することができます。

このように、第二段階全学ファイアウォールは、第一段階の PROTECTED ネットワークとは異なるものとして提供されます。以下にまとめますと、

（第一段階）PROTECTED ネットワーク
　主に利用者端末を守るためのネットワーク提供
　一律な設定と機能を提供
第二段階全学ファイアウォール
　外部からアクセスされるサーバ等の機器を守るためのネットワーク提供
　部局ネットワーク管理者による設定が可能

となります。第二段階全学ファイアウォールは、2018 年 10 月から試験提供が開始される予定です。また、第一段階の PROTECTED ネットワークも引き続き提供されますので、用途に応じて必要なネットワークを選択してください。また、第二段階全学ファイアウォールの試験提供開始後となりますが、第一段階ならびに第二段階ファイアウォール配下のネットワークに対して VPN サービスを提供する予定です。

第二段階全学ファイアウォールに関する概要は、この原稿の執筆時点のものですので、まだ変更があるかもしれません。最新の情報に関しては以下を御覧ください。

本サービスのご案内 Web サイト（Web ページ）
　https://www.ut-portal.u-tokyo.ac.jp/wiki/index.php/ 全学ファイアウォール整備
お問い合わせ用メールアドレス
　fw-request @ itc.u-tokyo.ac.jp

（ネットワーク研究部門　関谷 勇司）