第二段階全学ファイアウォールサービス利用方法

セキュリティを強化した全学ファイアウォールネットワークの提供が開始されて2年が過ぎました。多くの部局にこのネットワークを利用して頂いています。2年前に開始された第一段階全学ファイアウォール（PROTECTED）ネットワークは、主に利用者端末を接続するためのネットワークです。外部からの接続を遮断し、ダウンロードされるファイルをチェックすることで安全な通信を確保しています。一方でサーバや実験機器など、外部からアクセスされる必要のある機器を接続することには適していませんでした。

そこで、前号の Digital Life Vol.31 でも紹介した通り「第二段階全学ファイアウォール」の提供が開始されようとしています。このネットワークは、外部からアクセスされる機器を接続し攻撃から守るためのネットワークです。接続する機器単位で細かなアクセス制御が可能となり、外部からの不要な通信を遮断することができます。2019年1月時点で、全学ファイアウォールが提供するネットワークサービスは、次の二種類となります。

第一段階全学ファイアウォール（PROTECTED）ネットワーク

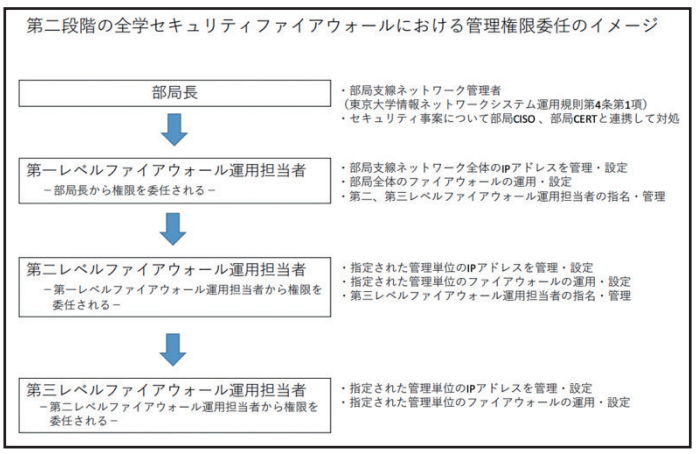
利用者端末を守るためのネットワーク
外部からの接続を一律に遮断
ダウンロード / アップロードされるファイルの検査
カスタマイズ不可能
URL 判別による悪性サイトへのアクセス遮断

第二段階全学ファイアウォールネットワーク

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
ネットワーク管理者によるアクセスリスト設定が可能
ダウンロード / アップロードされるファイルの検査
URL 判別による悪性サイトへのアクセス遮断

第二段階全学ファイアウォールネットワークは、IPAC（東京大学 IP アドレス / 全学 FW 管理システム）と呼ばれるポータルサイトから制御できます。第二段階ファイアウォールの管理権限を持っているユーザは、IPAC にログインすることで、IPAC の機能である UTIP ならびに UTACL を利用することができます。

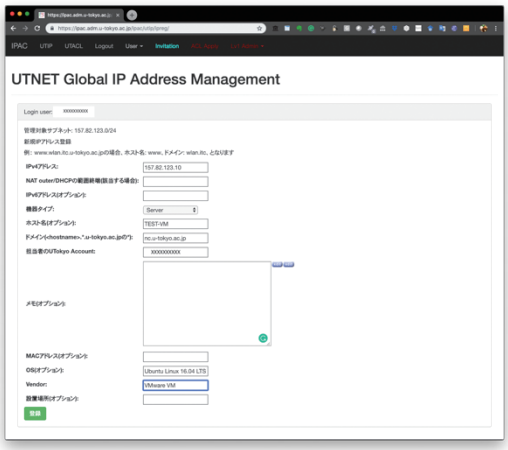
IPAC へのログインアカウントは、部局単位で付与されます。部局長から任命された第一段階管理者が、部局ネットワークのすべての管理権限を有します。さらに、部局が利用しているネットワークの中から、ネットワーク単位で管理者を指定し管理権限を委譲することも可能です。

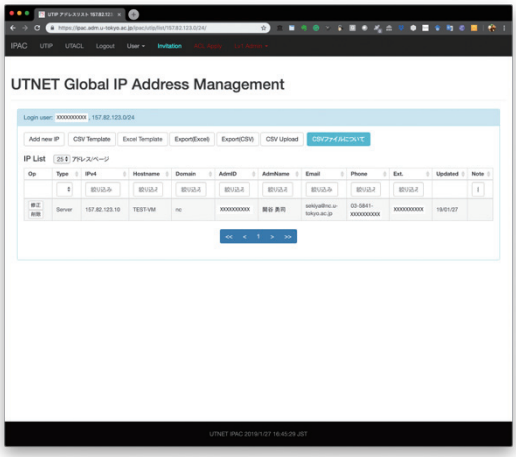


部局の管理者ならびに管理者から権限を委譲されたユーザは、自身が管理権限を持つネットワークに対して UTIP と UTACL の機能を利用することができます。UTIP / UTACL の機能は次の通りです。

UTIP

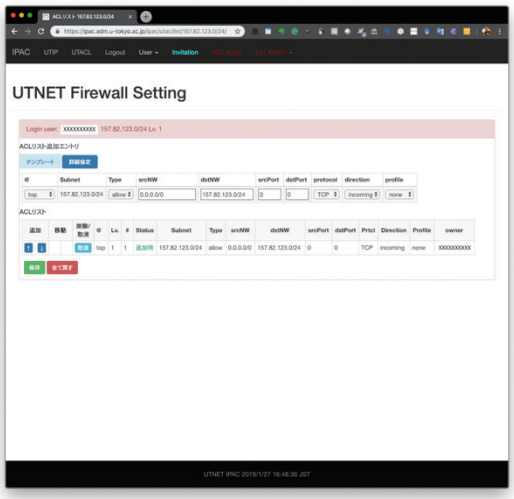
IP アドレスの利用情報や担当者情報を登録





UTACL

管理権限を持つネットワークに対してホスト単位もしくはネットワーク単位でアクセスリストを設定可能
テンプレート機能による簡易設定や詳細設定機能によるアクセスリストの明記が可能



IPAC（東京大学 IP アドレス / 全学 FW 管理システム）

https://ipac.adm.u-tokyo.ac.jp/（学内からのアクセス限定）

全学ファイアウォールの利用方法ならびに申請方法。

https://www.ut-portal.u-tokyo.ac.jp/wiki/index.php/ 全学セキュリティファイアウォール

IPAC 操作マニュアル

上記ページの「3.5 東京大学 IP アドレス / 全学 FW 管理システム（IPAC）操作マニュアル」に操作マニュアル（PDF）へのリンクがあります。

お問い合わせ先メールアドレス

fw-request @ itc.u-tokyo.ac.jp

（ネットワーク研究部門　関谷　勇司）