UTACL 運用開始のお知らせ

第二段階全学ファイアウォールのサービス提供が開始され、一年が経過しようとしています。Digital Life Vol.32 にて第二段階全学ファイアウォールのサービス概要を紹介しましたが、その際に UTACL という機能を紹介しました。

この UTACL 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にある一つの機能です。UTACL を利用することにより、各部局の全学 FW 運用担当者は自部局が有するネットワークに対して、自由に IP ACL（アクセスリスト）を設定し、さらにウィルス検知や攻撃検知、URL フィルタリングを行うことができます。

この度、全学 FW WG による UTACL 機能の整備が整い、第二段階 FW 利用者に UTACL 機能を利用してもらうことが可能になったため、この場にて紹介させて頂きます。

IPAC には https://ipac.adm.u-tokyo.ac.jp/ からアクセスできます。IPAC にログインすると、図 1 に示すように、管理権限を有するネットワークに対して IP アドレス情報管理機能（UTIP）とアクセスリスト管理機能（UTACL）のリストが表示されます。また、上部メニューから「UTACL」を選択しても、IP ACL 管理権限を持つネットワーク一覧が表示されます。

図 1 : IPAC ログイン画面

図 2 は、UTACL に表示されるネットワーク一覧から、130.69.XXX.XXX/24 のネットワークを選択した場合です。この画面において、「テンプレート」と「詳細指定」のどちらかを用いて ACL を設定します。

「テンプレート」は ACL の簡易設定機能であり、Web Server、SSH Server、CONFERENCE といったある程度一般的な用途に対する設定を簡易に行うことができます。例えば、130.69.XXX.25 という IP アドレスに遠隔会議システムを設置した場合には、Type を CONFERENCE に、Address Range に 130.69.XXX.25 を入力し、「ACL 作成」ボタンを押すことで IP ACL 設定が入力されます。

入力した ACL 設定は「追加待」の状態になります。これは、追加したルールが即時に適用されるのではなく、全学 FW 管理者が ACL 設定を確認した後に適用される

ことを意味します。入力した ACL 設定が即時適用されないのは、ACL の設定ミスを防ぐためであり、まずはこのような運用にて UTACL の提供を開始しています。

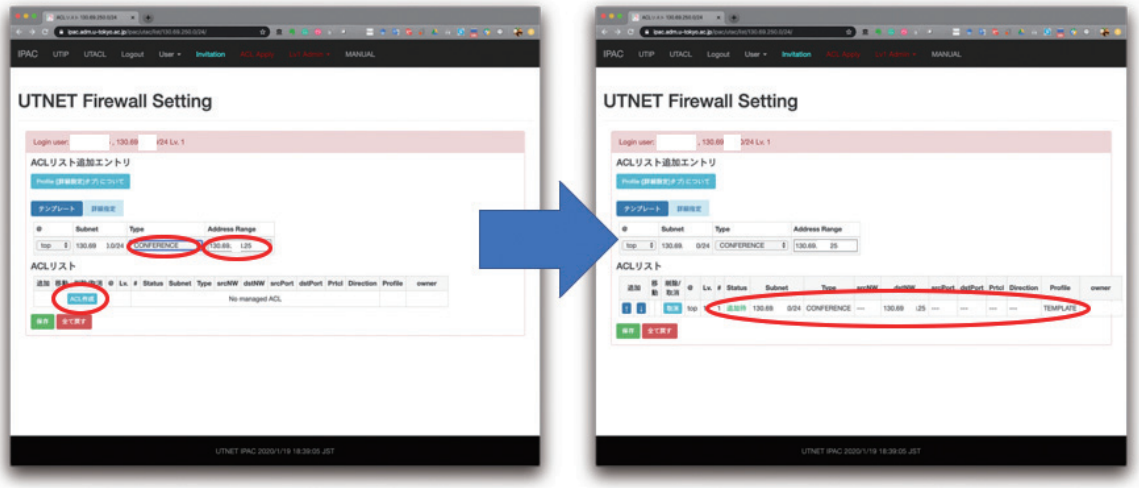

図 2 : UTACL へのテンプレート機能を利用した IP ACL 設定

設定したいすべての ACL を入力したら、左下の「保存」ボタンを押すことで、全学 FW 管理者の確認待ち状態になります。通常は 2 営業日以内に確認され、第二段階 FW に反映されます。

また、「詳細指定」においては、送信元 IP アドレス範囲、宛先 IP アドレス範囲、送信元ポート番号、宛先ポート番号を指定して IP ACL を設定できます。詳細設定にて ACL を設定する場合を図 3 に示します。

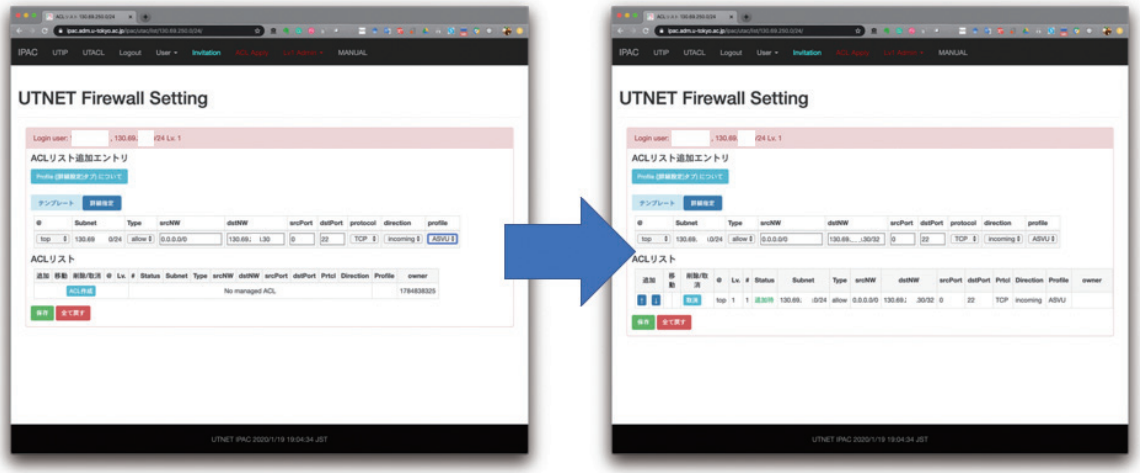

図 3 : UTACL への詳細指定機能を利用した IP ACL 設定

詳細指定は、ルータやファイアウォールといった機器で ACL を設定したことのある方であれば、すぐに使い方は理解できると思われます。列の最後に「Profile」という項目がありますが、これは設定した IP ACL ルールに対して、ウィルス検査や脆弱性をついた攻撃の検知、URL フィルタリング等を追加で設定する項目となります。Profile の詳しい説明は、列の上部にある「Profile（[詳細指定] タブ）について」のボタ

ンを押して頂けると、簡易的な説明が表示されます。

Profile も含め、UTACL の詳細な使い方を知りたい場合は、IPAC の上部メニューにある「MANUAL」をクリックしてください。UTIP、UTACL を含む IPAC ポータルサイト全体の最新操作マニュアルを見ることができます。

UTACL 機能が整備され公開されたことにより、第二段階全学 FW 管理下ネットワークに対して IP ACL を設定して頂くことが可能となりました。UTACL は、さらに管理の利便性を増すために、全学 FW WG によって改善が続けられます。機能に対する要望や質問は、下記の問い合わせ先までお願い致します。

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

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）