東北大学全学ファイアウォールの運用に関する報告

野田 大輔 [1)], 森 倫子 [1)], 水木 敬明 [2)], 曽根 秀昭 [2)]

1) 東北大学 情報部情報基盤課

2) 東北大学 サイバーサイエンスセンター

noda@cc.tohoku.ac.jp

概要:東北大学では、学内ネットワーク TAINS のセキュリティ向上を目的として、2014 年 7 月より TAINS と学外ネットワークとの対外接続点に全学ファイウォールを導入した。本稿では、全学ファイアウォールが TAINS のセキュリティにおいて担う役割と運用状況について報告する。

1 はじめに

東北大学(以下、本学という。)では、学内ネットワーク TAINS（Tohoku Academic/All-around/Advance/ Information Network System）のセキュリティ向上を目的として、2014 年 7 月より全学ファイアウォールを導入した。この全学ファイアウォールは TAINS と学外ネットワークとの対外接続点に設置され、学外ネットワークから TAINS へ向けた通信のうち、部局からの事前の申請に基づいた必要なものだけを許可し、不必要な情報が学外ネットワークへ公開されることを防止している。

2 全学ファイアウォールの導入背景

2013 年 12 月、本学のネットワークセキュリティのさらなる強化を検討する目的で「全学ネットワークのセキュリティ強化検討プロジェクト・チーム」（以下、「セキュリティ強化 PT」という。）が設置された。セキュリティ強化 PT での検討において、本学が部局にグローバルアドレスを割り当て、管理を移譲する分散管理となっていることにより、十分なセキュリティ対策なしに情報機器が学外ネットワークに公開されるケースの可能性が指摘された。そこで TAINS と学外ネットワークの接続点に透過型のファイアウォールを導入してグローバルアドレスの利用を申請登録制とする集中管理を行う必要性が確認され、全学ファイアウォールを導入することが決定された。

3 全学ファイアウォールについて

3.1 概要

全学ファイアウォールは TAINS と学外ネットワークの対外接続点に設置されている透過型のファイアウォールであり、TAINS と学外ネットワーク間の通信を管理している（図 1 参照)。

全学ファイアウォールは学外ネットワークから TAINS へ向けた通信はデフォルトで不許可としており、学外ネットワークへサービスを提供する場合は部局を通して情報シナジー機構へ通信許可を申請し登録する必要がある。これによりグローバルアドレスの集中管理を実現しセキュリティ対策のなされていない情報機器が意図せず学外ネットワークへ公開されることを防止している。

一方で、TAINS から学外ネットワークへ向けた通信はその応答を含めて全て許可している。従って、利用者端末からのウェブ閲覧等、学外ネットワークへの通信は全学ファイアウォールの影響を受けず一般利用者が全学ファイアウォールを意識する必要はない。ただし 2015 年 6 月より著作権侵害コンテンツの発信を防止する目的で、TAINS から学外ネットワークの通信であっても一部の P2P アプリケーションの通信を遮断している。

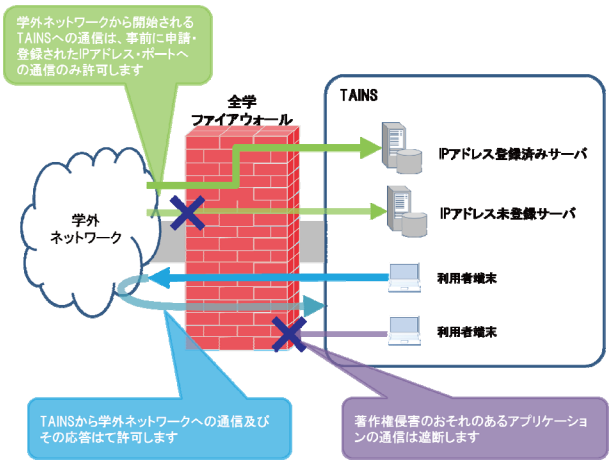

図 1:全学ファイアウォール概要図

2.2 ポート設定

全学ファイアウォールのポート設定は以下の通りである。

1. 全不許可
   - ➢ 全ての通信を遮断する
2. ウェブサーバのみ(80, 443/tcp)許可
   - ➢ ウェブサービス用ポート(80, 443/tcp)のみ許可する
3. 全許可
   - ➢ 全ての通信を許可する

デフォルトのポート設定は「1. 全不許可」となっており、学外ネットワークから開始される TAINS への通信は全て遮断される。学外ネットワークからの通信を許可するポート設定は、HTTP 通信と HTTPS 通信のみを許可する「2. ウェブサーバのみ(80, 443/tcp)許可」と制限のない「3. 全許可」を用意している。学外ネットワークへサービスを提供する場合は、サービスを提供するグローバルアドレス毎に、提供サービスに合わせてこれらいずれかのポート設定を選択して情報シナジー機構へ申請し登録する必要がある。

ポート設定については導入初期に予想される多数の申請と申請対応にあたる人的リソースを考慮しシンプルな設定から開始することとした。今まで通り制限なく使用できる「3. 全許可」に加え、情報発信のため多数の利用が予想されるウェブサーバを保護するため、ウェブサーバ用のポート(80, 443/tcp)のみを許可するポート設定を提供することとした。

ポート設定のメニューについては今後拡張を検討していく予定である。

2.3 遮断アプリケーション

本学では 2011 年 4 月より民間事業者による「インターネット上の著作権を侵害している疑いのある P2P 通信の検知・通知サービス」を利用し、著作権侵害に関するインシデントの未然防止に努めてきた[1]。しかしながら、前記サービスは学外ネットワークへ発信されている P2P 通信を検知するものであり、著作権侵害にあたるコンテンツが学外ネットワークへ発信されること自体を防止するものではなかった。

これに対し全学ファイアウォールはアプリケーション識別機能を有し、著作権侵害コンテンツの発信に利用される可能性のあるアプリケーションの通信を選択的に遮断可能であり、そのような遮断することで、著作権に関するインシデントの未然防止が期待されていた。

そして 2015 年 6 月より、全学ファイアウォールによる BitTorrent 等の著作権侵害コンテンツの発信のおそれがある P2P アプリケーションの遮断を開始した。

なお遮断アプリケーションについては TAINS のウェブページ上で学内公開しており、研究等に必要であれば申請により使用することが可能となっている。

3 全学ファイアウォールの運用

3.1 事前申請について

全学ファイアウォールの導入にあたっては、導入前に約 1 ヵ月間の期間を設け、部局からの事前申請を受け付けた。事前申請では申請漏れを極力少なくするため、部局毎に当該部局が保有しているグローバルアドレス一覧を記載した専用の事前申請書を作成して使用した。事前申請書を各部局に送付し記載された全てのグローバルアドレスに対し全学ファイアウォールの導入時に希望するポート設定を記入いただいた上で情報シナジー機構へ申請いただいた。

3.2 申請について

全学ファイアウォールの登録申請は、TAINS で提供している他のサービスと同様に部局の技術担当者を介してメールで申請書を情報シナジー機構へ送付する形式としている。申請書にはグローバルアドレス、ポート設定、利用目的等を記載する。申請書の受理後 1 両日中に全学ファイアウォール

のポート設定を実施している。

全学ファイウォールの運用開始から現在までの申請件数の推移を図 2 に示す。全学ファイアウォールの運用開始直後は月 10 件以上の申請があったが、これらは事前申請の漏れや見落としの修正のためと思われる。運用開始から 1 年経過した現在では申請件数は落ち着いてきており月 3, 4 件程度となっている。

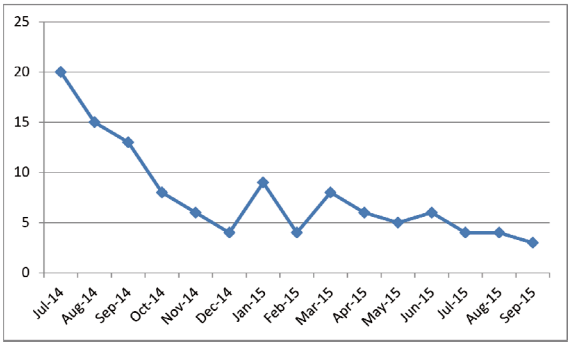

図 2:全学ファイアウォール申請件数推移

3.3 運用費用について

全学ファイアウォールの導入費用及び初年度の運用費用は、セキュリティ対策の緊急性から総長裁量経費により措置された。2 年目以降の運用費用についてはセキュリティ強化 PT の報告に従い、保有するグローバルアドレスの数及び全学的基盤経費の負担額に応じて各部局で按分することとなっている。

具体的にはグローバルアドレス 1 つあたりの負担金額を定め、保有するグローバルアドレ数に応じて各部局の負担金を算出する。これを保有グローバルアドレス比例分とし、年間運用費用のうち 3 分の 2 程度を賄う。不足額を全学的基盤経費比例分として全学的基盤経費の負担額に応じて各部局に按分する。各部局は保有グローバルアドレス比例分と全学的基盤経費比例分の合計金額を全学ファイアウォールの年間の負担金として負担いただくこととしている。負担金は当該年度 1 月 1 日の保有グローバルアドレス数と当該年度の全学的基盤経費の負担額に基づいて算出し、当該年度の 3 月 31 日支払としている。

4 おわりに

本稿では、本学の全学ファイアウォールの概要とこれまでの運用について述べた。

全学ファイウォールは当初の目的であるグローバルアドレスの集中管理を達成し、著作権侵害に関するインシデントの未然防止の役割を担うにいたった。今後もポート設定の拡充等さらなるセキュリティ対策の強化が期待される。

一方で全学ファイアウォールの運用に投入できる人的リソースには限りがあるため、強化する機能の選択と効率的な運用方法を検討していく必要がある。

参考文献

[1] 東北大学情報シナジー機構、著作権侵害の疑いのある P2P 公衆送信の検知の運用、東北大学情報シナジー機構 TAINS ニュース 、No.39、pp.4、2011,