早稲田大学におけるセキュリティインシデントの対策とその背景

アフマド ルリィ[*1] 八木 秀樹 山田 伸介 新城 直樹 岩田 一

早稲田大学 メディアネットワークセンター

[*1]arully@aoni.waseda.jp

１．はじめに

近年、ネットワークにセキュリティインシデントの増加に伴い，学内ネットワークの適切なセキュリティ対策の必要性が高まっている．この問題の対策のために各組織によってさまざまな方法が作成され実施されている．

早稲田大学では新しい対策を実施しながら，遠隔教育技術[1]などを含む改善の方も継続している．

本論文では、早稲田大学におけるセキュリティインシデントの対策の背景、そしてセキュリティセミナーとセキュリティ用語集とガイドラインを含む対策を述べる。

２．セキュリティインシデントの背景

２．１ 早稲田大学のネットワーク

早稲田大学メディアネットワークセンター（以下 MNC）では，全学の学生を対象として情報利用環境の提供を行う[5]ほかに，研究室を始め学内諸機関に IP アドレスやドメインを貸与し，自主的な管理を条件として，制限の少ないネットワーク利用を提供してきた[2].

学内諸機関が利用できる主な２つサービスはバックボーンネットワーク接続と学外直接接続である．バックボーンネットワーク接続サービスは学内諸機関において利用される端末を本大学が管理している IP アドレススペースを利用してバックボーンネットワークに接続するサービスである．学外直接接続サービスはバックボーン接続申請により貸与された IP アドレスを学外ネットワークに直接接続可能とするサービスである．

バックボーンネットワーク接続サービスでは，学外ネットワークのインターネットをアクセスするためにファイアウォールを経由してプロキシーなどの手続きしないといけない．学外直接接続サービスを合わせて申請すれば直接インターネットをアクセスできて，サーバーなどを立てて外からのアクセス提供が可能となる．

２．１ セキュリティインシデントの背景

基本的に制限されている学内ネットワークに接続するだけでもセキュリティリスクが高くなると考えられる．学外ネットワークに接続することでセキュリティリスクも倍増される．つまり，セキュリティリスクが高くなる状況を避けられない．

ここで MNC の別の役割では，学内におけるインターネットセキュリティの情報センター（IRT : Incident Response Team）として、早稲田大学のネットワークへの不正アクセスへの対応・助言・分析、インターネットセキュリティ技術および情報倫理にかかわる教育・啓発活動なども行っている。

３．セキュリティインシデントの対策

セキュリティインシデントの対策は技術面対策と管理面対策を２つ大きく分けられる．

本大学における技術面対策では，ファイアウォールやプロキシーや侵入検知システム（IDS）などを実施している．ネットワーク監視ツールの導入によってネットワークの状況を握るすることが可能になった．

本稿では，本大学における管理面対策を集中しており，一般学生向けの新入生セキュリティセミナー[4]の他に，abuse チーム，管理者向けのセキュリティセミナー[1]の開催，セキュリティガイドラインの提供，セキュリティ用語集[3]の提供などを実施している．

Abuseチーム

技術担当者の技術レベルやセキュリティ意識の低さが具体的な要因となったセキュリティインシデントが後を絶たない現状が続いている．このようなインシデントに対し MNC では，教職員から構成される abuse チームが

随時対応を行っている．

インシデントの内容としてはワーム，不正なプロキシ利用（Open Proxy），不正アクセスなどがある．これらの案件に対し abuse チームでは技術的なサポートや対策支援を行うとともに，情報倫理教育の観点から面接による指導を実施している．

セキュリティセミナー

本大学ではバックボーンネットワーク接続と学外直接接続サービスを利用する前に，各箇所ネットワーク管理者などを対象としてセキュリティセミナーを受講する義務がある．このセミナーを最初に実施したときに座学で受講してきたが，参加者の都合がつきにくく出席率が低い，内容が多岐にわたるため自分と関係のない内容についても時間を割かなくてはならないという問題点がでてきた．

このような問題に対し，セキュリティセミナー教材のオンデマンド化を進め，セミナー受講の利便性と効率を高めた．現在では，座学で受講する必要はない

セキュリティガイドライン

セキュリティセミナーの内容は技術的な内容が強いが，ポリシー的な内容の必要性を感じていて，セキュリティガイドラインも提供している．

ガイドラインの構成はできるだけ短く簡単に実施できるガイドラインを目的として，「情報機器の運用のためのガイドライン」と「緊急時の対策のためのガイドライン」を分けられる．

情報機器の運用の部分に運用体制に関する指針と、通常時の運用内容について説明している．具体的に運用体制表（組織表）の作成，ドキュメントの作成，後継者とユーザの教育，情報収集，狭義のセキュリティ対応，ドキュメントの定期的更新，申請情報の更新を述べた．

緊急時の対策の部分にはセキュリティインシデント発生時などの緊急時の対策や対応について説明している．具体的にインシデントの定義，緊急対応，報告，調査，今後への対策を述べた．

ガイドラインはセキュリティセミナーと一緒で状況と合わせて改善し続ける．

セキュリティ用語集

一般大学生のセキュリティに対する関心は，ネットワークを利用する機会の多さを考えるとあまり高いといえないのが現状である．情報倫理教育の一環として，大学生のセキュリティに対する知識・関心を高めることを目的として開始されたのが「セキュリティ用語集」である．

３．むすび

本稿では，早稲田大学におけるセキュリティインシデントの背景を説明して，その対策の手法についてのべた．

セキュリティインシデントでは，世の中のネットワーク社会に避けられない状況になってしまい，インシデントがないという状況を目指さなくて，きちんとスムースなインシデント対策を実施することが目指す必要があると考えられる．

参考文献

[1] アフマド ルリィ，渥美章佳，小泉大城，新城直樹，“早稲田大学におけるセキュリティセミナーオンデマンド化について，”2005 年 PC カンファレンス論文集，新潟大学，2005 年 8 月

[2] 八木 秀樹，アフマド ルリィ，山田 伸介，岩田 一，“学内ネットワークにおけるセキュリティ確保のための情報管理，”2006 年 PC カンファレンス論文集

[3] 海老原 崇，渥美 章佳，新城 直樹，齋藤朗宏，“情報倫理教育における「セキュリティ用語集」の効用，”2005 年度 PC カンファレンス，新潟大学，2005 年 8 月

[4] 見崎 研志，三橋 大輔，齋藤 朗宏， 松山 響子，“情報化社会の発展に伴う「新入生コンピュータセキュリティセミナー」のあり方について，”平成 17 年度情報処理教育研究集会，九州大学，2005 年 11 月

[5] メディアネットワークセンター（Media Network Center: MNC），http://www.waseda.jp/mnc/index-j.html