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

八木 秀樹† アフマド ルリィ 山田 真介 岩田 一

早稲田大学 メディアネットワークセンター

† hideki@mnc.waseda.ac.jp

1 はじめに

近年，大学内のネットワークの拡大・多様化に伴い，学内諸機関におけるネットワークから外部ネットワークへの直接接続の要求が高まっている．早稲田大学では，審査を通してドメインの自主管理や学外直接接続IPアドレスの使用を許可しているが，学外ネットワークに直接接続することにより，不正アクセスなどのセキュリティ・インシデントが発生する可能性が増している．さらに，教育機関においては人の入れ替わりが激しいため，IPアドレスの管理者や対応するネットワーク情報が適切に更新されない，セキュリティ教育が適切に行われない，などの問題も多い．

これらの対策として本学では，セキュリティ教育手段として新規ネットワーク管理者，及び学外直接接続利用者を対象とした，**セキュリティセミナー**を実施している [1, 2]．これにより，セキュリティ・インシデントの危険性について注意を促し，安全性確保への意識の向上を図っている．しかしながら，既に使用していない学外直接接続や必要のない学外直接接続が学内ネットワークに数多く存在しているのが現状である．

そこで，本学では2004年に学内ネットワーク情報を一元管理するための**ネットワーク情報管理システム（NIMS）を導入**した．また，2005年から**学外直接接続IPアドレスの申請方法を改訂**し，IPアドレスの使用期限を年度単位に改めた．さらに，IPアドレスを継続使用する際には，IPアドレスの管理者に改めてオンデマンド授業形式のセキュリティセミナーを受講することを義務付けた．これにより，学外直接接続IPアドレスの情報を正確に把握し，不必要なIPアドレスの返却を促すことが可能となる．また，年度ごとに管理者情報も更新することができ，学内ネットワークのセキュリティ向上につながると考えられる．本稿では，本学におけるセキュリティ向上のため，ネットワーク情報管理システム（NIMS）を用いたネットワーク情報管理方法について述べる．また，それによる学外直接接続IPアドレス数の変化などを報告する．

2 早稲田大学のネットワーク

2.1 学内ネットワークサービス

早稲田大学メディアネットワークセンター（Media Network Center: MNC）では，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環境を提供してきた．以下では，MNCが研究室等に提供している学内ネットワークサービスの代表例を紹介する．

バックボーンネットワーク接続

学内諸機関において利用される端末をバックボーンネットワークに接続するサービスである．早稲田大学では「133.9.*.*」のグローバルアドレスを申請者に対して貸与する．ただし学内ネットワークはファイアウォールで守られており，学内ネットワークに接続するだけでは，外部の端末と直接通信することはできない．外部への通信にはプロキシサーバを利用する必要があり，MNCでは需要の高いWWW，Telnet，FTP等のサービスに対して，外部接続用プロキシサーバを用意している．

学外直接接続

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．通常のバックボーンネットワーク接続サービスでは，プロキシサーバを通した外部への通信を一部許可しているだけであるが，一方で学外サーバへのPOP，SMTP接続等の要求も多く，また外部公開のためのWebサーバ設置などの需要も高い．MNCでは審査の上，申請者に対して学外直接接続を許可している．これにより，外部との通信に制限がなくなるが，反面，セキュリティ・インシデントの危険性は高まる．

上述の申請を行う際，管理責任を請う**設置責任者**，及び実際の運用を行う**技術担当者**を登録することを義務付けている．設置責任者は本学の教職員に限定しており，技術担当者は設置責任者の責任のもとに指名される．なお，技術担当者は学生が担当することも可能である．本稿では，設置責任者と技術担当者をまとめて**管理者**と呼ぶことにする．学内ネットワークのセキュリティを確保するため，管理者はネットワーク機器を適切に運用・管理し，ユーザを教育する必要がある．

2.2 セキュリティ・インシデントの要因

近年，学内のネットワークにおいて，不正アクセスなどの**セキュリティ・インシデント**が多発しており，その数は年々増加している．以下に，学内ネットワークにおけるセキュリティ・インシデントの主な要因を以下に示す．

管理者の引継ぎ作業の不徹底

大学では，学生が技術担当者としての役を担うことが多い．一定の期間が過ぎると技術担当者の学生は卒業し，他の学生が新たに技術担当者に就くことになる．この際，引継ぎ作業が徹底されず，学外直接接続 IP アドレスが適切に管理されないことが多い．また，技術担当者の情報自体も MNC が管理できないことがある．この場合には，新たな技術担当者がセキュリティ・セミナーを受講しないため，学内ネットワークを利用する際のポリシーや注意事項も理解されない可能性が高い．

不必要な学外直接 IP アドレスの存在

IP アドレスの使用申請から時間が経過すると，適切に管理されないネットワーク機器が増加する．また，引継ぎ作業が徹底されずに，管理者が自分で管理するべき学外直接接続 IP アドレスを知らないというケースも見られる．この様な場合，長い間セキュリティ・パッチが当てられていないネットワーク機器が学外からの不正アクセスの標的になる可能性がある．

中央管理機関による情報把握が困難

学内ネットワークは非常に複雑であり，中央管理機関（MNC）で全ての情報を把握することが困難となっている．担当者の変更を報告してくる箇所は非常に少なく，不正アクセスがあった場合には，管理者と連絡が取れずに，被害が拡大してしまう可能性がある．

2.3 学内ネットワークの課題

近年，学外直接接続された端末が不正アクセスなどのセキュリティ・インシデントを起こす事例が非常に多く，MNC としては可能な限り学外直接接続を廃止したいと考えている．学外直接接続は研究・教育を行うために必要不可欠な場合もあるが，その場合は管理者に責任を持って管理してもらうことを徹底したい．また，MNC が管理する学外直接接続 IP アドレスとそれに対応する管理者やネットワーク機器を正確に把握し，変更があった場合には速やかに情報を更新する必要がある．さらに，不必要な IP アドレスが学外直接接続になったままで放置される要因は速やかに取り除く必要がある．

以上を踏まえ，学内ネットワークの管理方法には以下の 3 点が望まれると考えられる：

- 不必要な学外直接接続 IP アドレスを回収する．
- 技術担当者間の引継ぎを確実に行うよう促す．また，技術担当者の変更情報を MNC が正確に管理する．
- MNC が開催するセキュリティセミナーを技術担当者に定期的に受講してもらい，セキュリティ・情報倫理に関する知識を向上させる．

これらの要件に対し，本学では学外直接接続 IP アドレスの申請方法を改訂し，年度ごとの使用申請を義務付けた．

3 ネットワーク情報管理システム

3.1 ネットワーク情報の集中管理

前述のように，学内ネットワークは日々変化しており，MNC において正しい情報の把握が困難であった．このような状況は，セキュリティ・インシデント発生時の対応の遅れの原因となるだけでなく，利用者が知らない間に学外直接接続 IP を利用しているといった，セキュリティ上好ましくない状況が生まれる原因となる．MNC ではネットワーク情報を集中管理するため，各管理者から収集した情報をデータベースに納め，後述するネットワーク情報管理システムと連動させるようにした．

3.2 利用可能な機能

MNC では 2004 年 7 月に**ネットワーク情報管理システム**(Network Information Management System: NIMS) を導入した．ネットワーク情報管理システム

は，収集したネットワーク情報をデータベースに格納し，またそれを閲覧，変更するためのインターフェースを提供する．NIMS は Web ブラウザを通して利用できるため，プラットフォームを選ばず利用可能である．学内ネットワーク利用者は NIMS を通して以下の機能を利用できる．

- バックボーンネットワーク接続申請
- 学外直接接続申請
- サブネットアドレス申請 ※
- 自主管理ドメイン設置申請 ※

※は，継続・廃止の申請のみ可能．

学内ネットワークの利用者は，ユーザ登録により NIMS を使用できる．利用者は NIMS を通して上述の申請ができる他，各種サービスの申請状況の閲覧，技術担当者の変更手続きなどが可能である．学内ネットワークでは，利用状況や卒業に伴う技術担当者の変更が頻繁に起こるため，NIMS を利用して手続きを簡略化することは非常に有効であると考えられる．

また，データベースにはセキュリティ・インシデントの履歴が格納されている．MNC はこれらの情報をもとに，セキュリティ・インシデントが多発する箇所への指導・警告，及び学外直接接続の停止などの処置をとっている．

4 学外直接接続の申請方法の改訂

4.1 改訂の目的と内容

学外ネットワークのセキュリティを確保するため，学外直接接続の IP アドレスの申請方法を改訂した．

この改訂では，学内ネットワークのセキュリティ向上のため，以下の 3 点を目的とする．

(1) 不必要な学外直接接続の IP アドレスの回収
(2) 定期的な管理者情報の更新
(3) 管理者のセキュリティに関する知識の向上

新しい申請方法の内容を以下にまとめる．

(1) 学外直接接続 IP アドレスの使用期限を年度単位に定め，年度ごとの使用申請を義務付ける
(2) オンデマンド授業型のセキュリティセミナーの受講を義務付ける
(3) 管理するネットワーク構成図とネットワーク機器の種別を提出する

申請の更新や登録情報の変更は NIMS を通してオンラインで行うことが可能である．なお，予め定めた期限までに使用申請の更新が行われない IP アドレスの使用は停止する．期間内に申請を更新すれば，以前に使用していた IP アドレスとサブドメインをそのまま使用できるものとする．

4.2 スケジュール

使用申請の更新の際は，できる限り使用者の利便性を損ないように作業を進める必要がある．主な実施スケジュールを以下に記す．

- 2006 年 2 月 1 日： 申請更新の依頼
- 2006 年 3 月 31 日： 申請更新の締め切り
- 2006 年 4 月 1 日： 第 1 回リマインダメール発送
- 2006 年 5 月 6 日： 第 2 回リマインダメール発送
- 2006 年 5 月 31 日： 最後通知
- 2006 年 6 月 15 日： 更新申請がなされない IP アドレスの使用停止

更新作業の準備では，NIMS 上に登録されている管理者と IP アドレスの情報をもとに， 対象者のリストアップした．一人の設置責任者が複数の IP アドレスを使用し，それぞれのアドレスに違う技術担当者を配備している場合には,【設置責任者，技術担当者】 のペアを一組として扱い，申請更新の依頼を出した．これにより，各技術担当者に対して申請情報の更新とセキュリティセミナーの受講を義務付けることが可能となる．

4.3 実施結果

ここで新しい学外直接接続の申請方法の実施結果について述べる．図 4.3 は申請数の月ごとの推移を表す帯グラフである．グラフの横軸には集計時期をとり，集計時期は **(1) 3 月 31 日**，**(2) 4 月 30 日**，**(3) 5 月 31 日**とする．また縦軸は申請数を表し，**(1) 更新申請数**，**(2) 廃止申請数**，**(3) 連絡無し**に分ける．更新作業の対象数（設置責任者と技術担当者の組）は 338 件であった．

ここで結果について考察する．2006 年 3 月のデータは申請の案内メールを送信してから 1ヵ月後（案内メール内の締め切り）を表すが，この時点での申請数の割合は 80.4%（更新申請：72.1%，廃止申請：

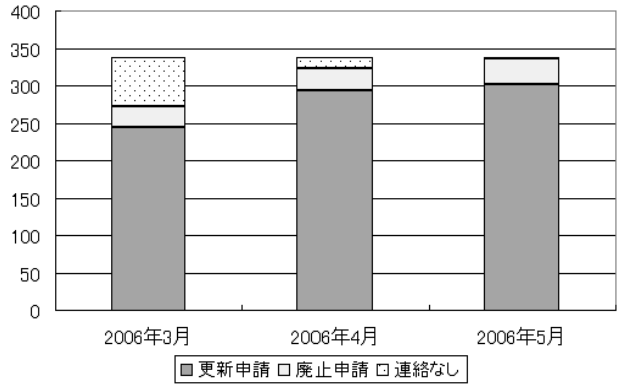

図 1: 申請数の推移

8.2%）であった．また，その 1 月後には申請数の割合が 95.5%（更新申請：86.7%，廃止申請：8.9%），2ヵ月後には 99.4%（更新申請：89.3%，廃止申請：10.1%）となり，ほぼ全ての対象者からの回答が得られた（6 月 2 日の時点で全ての申請を得ている）．また，不必要な IP アドレスの廃止申請は比較的早い時期に行われており，新しい申請方法が有効に働いていることが分かる．

5 まとめ

本稿では，早稲田大学におけるセキュリティ確保のためのネットワーク情報管理手法について述べた．また，学外直接接続 IP アドレスの申請方法を改訂し，その実施結果を報告した．

NIMS は，運用・管理側及び学内一般ユーザ側で情報を共有することにより，情報の不一致を減らし，年度更新手続きや担当者の変更手続きを簡略化することができる．これにより，不正アクセス発生時の対応を迅速に行うことができ，また MNC が現状のネットワーク情報を確実に管理できるようになる．

新しい学外直接接続 IP アドレスの申請方法により，不必要な IP アドレスを減らし，継続して使用する IP アドレスの適切な管理を促すことができる．また，学生などの技術担当者の引継ぎを適切に行わせることができる．さらに，セキュリティ・セミナーの受講により，管理者のセキュリティに関する意識・知識の向上も期待できる．使用する IP アドレスの更新申請，使用する機器の変更，技術担当者の変更は NIMS を通じてオンラインで行うことができる．これにより，利用者の負担も軽減できていると期待される．

学内ネットワークのセキュリティ確保のためには，適切な教育，指導が必要であり，また中央管理機関において正確な情報を把握することが重要である．日々ネットワークサービスが多様化する現在，中央管理機関として大学の研究，教育に必要なサービスを提供し，一方で確実なセキュリティを確保するため，柔軟な対応が期待される．

謝辞：

本研究の利用者データを提供してくださいました，早稲田大学 ITC の佐藤雄一氏をはじめ，MNC・ITC の皆様に感謝致します．

参考文献

[1] 渥美，赤木，新城，小泉，ルリィ，“キャンパスネットワークにおけるセキュリティ確保とネットワーク情報管理について,” 平成 16 年度情報処理教育研究集会予稿集, pp.590–593, 名古屋，2004 年 11 月．

[2] 赤木，秋岡，渥美，新城，伊藤，大前，史 “学内の自主管理セキュリティ向上を目的としたセキュリティセミナー／アンケートについて,” 平成 15 年度情報処理教育研究集会予稿集, pp.323–326, 札幌，2003 年 11 月．