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

アフマド ルリィ　渥美章佳　小泉大城　新城直樹
早稲田大学 メディアネットワークセンター
{arully, akiyoshi.a, dkoizumi, aragusuku}@aoni.waseda.jp

１．はじめに

近年の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．早稲田大学では，各箇所ネットワーク管理者などを対象として座学でのセキュリティセミナーを開催してきたが，この方法では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あった．

このような問題に対し早稲田大学では，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．一方で，早稲田大学キャンパスネットワークにおける不正アクセスの傾向分析,及びセミナー教材への反映を目的として，侵入検知システム（IDS）を導入し，攻撃パターンの解析を行っている．

本論文では，早稲田大学におけるセキュリティ教育とセミナーのオンデマンド化，及び侵入検知システムによる攻撃パターンの解析結果について論じる．

２． セキュリティセミナー

２．１ 従来の学内セキュリティ対策

近年のインターネットの急速な普及に伴い，大学等の研究・教育機関においてもセキュリティに関する問題は増加している．特に大学では，各研究室にグローバル IP が貸与され,ネットワークの管理を研究室の教員・学生が行う場合も少なくない．早稲田大学においても，研究・教育目的に限り，教員・学生を技術担当者とした自主管理ネットワークの利用サービスを提供している．しかしながら，技術担当者の技術レベルやセキュリティ意識の低さが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早稲田大学メディアネットワークセンター（以下 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．

また，技術担当者のセキュリティ意識の低さが招くインシデントの例も過去に多く存在した．そこで本学では，学内ネットワーク管理者（技術担当者）の教育を目的としたセキュリティセミナーを実施してきた．セミナーによる管理者のセキュリティ意識が高まり,インシデントも減少傾向にあることから，セミナー開催による効果はあったといえる．しかしながら座学によるセミナーは参加者の都合がつきにくく，また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多く割かねばならないという問題点があった．

２．２ セキュリティセミナーオンデマンド化

前節で述べた問題点に対し早稲田大学では，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．オンデマンド教材は学内の各種サーバ群，及びネットワーク状況を考慮し，提供するトピックをユーザ教育編，Windows 編，サーバ編，ルータ編に分類し，それぞれ独立に受講できるものとした．

ユーザ教育編では，ユーザによる不正アクセスのケーススタディを主に説明し，ユーザの知識レベルの底上げ，及びセキュリティ意識の向上を目的としている．

Windows 編では，マイクロソフト Windows をデスクトップとして安全に使用するための方法を主とした，Windows Update，アクセス制限，ウイルス対策ソフトなどについて説明している．

サーバ編では，各種サーバアプリケーション利用の際の注意点などについて述べる.一方で,学内ホスティングサービスの存在を周知し，サービスの利用によるメリット，デメリットの説明，自主管理の甘さによるインシデント発生を防ぐために，本サービスの利用を促している.

ルータ編では，安全なネットワーク構成など図例を用いて示し，OS の選び方やアクセス制御，DMZ と NAT などについて解説する.

オンデマンド教材は，HTML 形式による教材の提示,及び動画,スライド形式の教材によって構成される.ユーザからは，動画で表示される講師がスライドを変更しながら講義を進めていくように見える．さらに HTML 形式の教材による知識の補完,各種ツールへのリンクなどでより詳細な情報を提供している.

３．学内の不正アクセスパターン

３．１ 侵入検知システム

本学内における不正アクセスの傾向分析，及びセミナー教材への反映を目的として，侵入検知システム（Intrusion Detection System: IDS）を導入し，攻撃パターンの解析を行った.導入する IDS として，オープンソースの Snort[1]を用いた．IDS のマシンは MNC 内に設置し,学外から直接アクセス可能な(ファイアウォールに守られていない）状態で監視を行っている.

３．２ 解析結果

2005 年 1 月から 4 月までに検出された不正アクセスタイプを表 1 に示す.

表 1. 早稲田大学 MNC 内で検出された不正アクセス種別（2005 年 1-4 月）

順位	不正アクセスパターン	件数
1	WEB-IIS View source via translate header	752
2	(http_inspect) BARE BYTE UNICODE ENCODING	295
3	SHELLCODE x86 NOOP	175

実際には不正 ping パケットが最も多いが,これは誤検出の可能性が大きいため表 1 には載せていない.表 1 より Windows 上で動作する IIS ウェブサーバに対する不正アクセスが多いことが確認できる．理工系学部では UNIX 系 OS をベースとするウェブサーバが多い一方，UNIX 系 OS に余り馴染みのない文系学部などの箇所では数多くの IIS サーバが稼動しており，潜在的に非常に高い危険性をはらんでいることが想定される.また,研究室等で管理されているサーバは，ネットワーク規模が比較的小規模であることから，x86 プロセッサ搭載サーバが少なくないため，SHELLCODE x86 NOOP のアラートの多さにも十分注意が必要と言える．従来のオンデマンド教材には学内で検出された実データは含まれていないため，これらの実例をオンデマンド教材に反映し指導することは，ユーザのセキュリティ意識をより高めるために非常に有効であると考えられる.

４．まとめと今後の課題

本稿では，早稲田大学における技術担当者を対象としたセキュリティセミナーについて論じた．大学等の教育機関では，学生が技術担当者である場合が多く，またそれが短期間で入れ替わるため，技術レベルやセキュリティ意識の維持が問題となる．今回のセミナーのオンデマンド形式により，さらなるセキュリティ意識の向上，インシデント数の減少を期待することができる.

一方，集計した侵入検知システムのデータは短期間のものであるため，解析パターンの結果が不十分であることも考えられる．今後も継続的にデータを収集し，結果の分析を基に学内ネットワークセキュリティの保全に役立てて行く予定である.

参考文献

[1]”Snort - the de facto standard for intrusion detection/prevention,” http://www.snort.org/