富山大学におけるネットワークリスクの対策と現状

山田　純一

富山大学　総合情報基盤センター

1. 概要

富山大学のネットワークは, 2006 年 2 月の情報システム更新から約 4 年間, 様々なリスクに対して対策を講じてきた。本報告では，これまでに行った対策とこれから導入予定の対策，今後の課題について報告する。

2. 過去に発生したリスク

過去に発生したネットワークのリスクは以下の通りである。

①　ネットワークの運用・管理側

- 負荷に耐えられないファイアウォール
- DHCP で使用可能な情報コンセント
- 認証のない無線 LAN

②　ネットワークの利用側

- セキュリティが不十分のまま運用されているサーバ
- セキュリティ対策のない機器

これらのリスクに対して，これまで様々な対策を講じてきた。

3. これまでの対策

①　ネットワークの運用・管理側

以前のファイアウォールは学外からの攻撃等による負荷で，頻繁にダウンしていた。そのため，2006 年にファイアウォールの更新を行い，2007 年にはファイアウォールのログを取得する専用の装置を導入した。これにより，ファイアウォールがダウンすることがなく，更には学内のコンピュータウィルス等の不正な通信を早期に発見し，即座に対策することが可能になった。2009 年 3 月にはファイアウォールのポリシー強化を行い，セキュリティの向上を図った。今後は更に厳しいポリシーの設定も視野に入れている。

キャンパス内の一部においては，学外者でも誰でも，すぐに DHCP で接続可能な情報コンセントを設置していた。ただし, 利用者が分からない機器の接続やコンピュータウィルスの発生など, セキュリティ上の問題が多発した。そのため, 2008 年 7 月から 10 月にかけて固定 IP アドレスへの切り替えと対応を行い, DHCP の廃止を行った。ただし, 全ての DHCP が廃止されたわけではなく，一部の講義室系統においては，授業の関係で DHCP を残しており，今後は認証対応を行う予定である。

情報コンセントと同様に，以前の無線 LAN はセキュリティが不十分で誰でも使用可能なものが 57 台も存在した。これに関しては，順次廃止を行った。2006 年 2 月には LDAP を用いてユーザ認証が一元化されたため，2007 年から 2009 年にかけて利用者認証機能を用いた無線 LAN をこれまでに 59 台導入し，不正な通信が発生した場合には利用者の特定が可能になった。

②　ネットワークの利用側

セキュリティが不十分のまま運用されているサーバへは，注意喚起を行った後，キャンパス内全域のポートスキャンによるセキュリティ調査を行った。2008 年に第 1 回の調査を行い，脆弱性のあるサーバへはセンターから早急な対応を指示した。同様に 2009 年 5 月，7 月にも調査を行い，現在早急な対応をお願いしているところである。

サーバ以上にセキュリティが不十分なのは，各研究室で使用している機器である。中には対策を全くしていない機器が散在することから，もちろんセキュリティの意識が低く，昨年から今年にかけては，USB メモリなどの外部記憶メディアに感染する W32/Autorun の感染が非常に多く発生した。W32/Autorun の感染に対しては，センター職員全てを動員し，何日間か専用の対応窓口を用意して対応を行った。現在は感染のピークも過ぎたが，それでも月に何件かの感染を発見し，即座に駆除を行うなどの対応を行っている。

図 1 は，昨年から今年にかけての W32/Autorun の感染報告数である。ただし，センターに報告のあったものだけなので，実際にはこれ以上の感染があったものと考えられる。

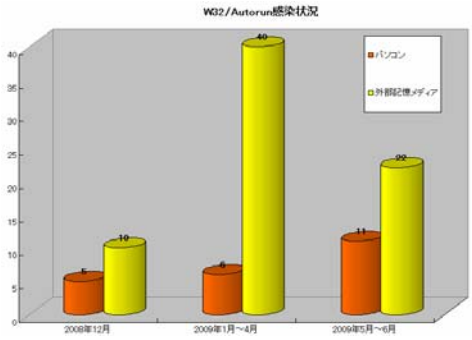

図 1　W32/Autorun 感染状況

感染報告数を分析した結果，コンピュータウィルス感染の一部は，研究室内に設置したルータ配下に接続する機器，もしくは当センターに接続の申請がされていない機器に発生していることが判明した。このため，2009 年 6 月からルータ配下，無線 LAN 配下に接続する機器に関しても当センターに接続の申請を行う体制にした。この他に接続申請がされていない機器を確認するため，2009 年 5 月からキャンパス内の教員に対し，学内ネットワーク接続機器調査票の作成と提出を依頼した。 7 月初旬までに 86%の返答があり，未提出の教員に対しては，現在も提出を依頼している。

4. 今後の対策と課題

今後，キャンパス内のセキュリティ向上のために計画している対策は以下の 3 つがある。

① 一部のファイアウォール更新

② 有線 LAN 認証システム

③ ネットワーク機器構成情報管理システム

対策の詳細だが，まず学内の一部のファイアウォールを更新する。一部のファイアウォールには URL フィルタリングの導入を予定し，セキュリティを高める。次に「有線 LAN 認証システム」によって，当キャンパスの講義室系統に提供している DHCP 利用者を認証する。これにより誰が使用しているかが分かるため，セキュリティの向上につながる。「ネットワーク機器構成情報管理システム」は，ネットワーク機器の利用状態の確認を行うことが可能で，異常が発生した場合はすぐに対応が可能になる。

これらのシステムの導入により，不正利用者の排除，障害やインシデント発生時の利用者の特定，コンピュータウィルスの侵入や情報漏洩等を防止するための高いセキュリティを備えたネットワークが構築される。

しかし，ネットワークの運用・管理側のセキュリティは非常に高いものになるが，利用者側のセキュリティを高めるにはどうするかが今後の課題である。また，運用・管理側においても人と金が必要であり，その確保も今後の課題である。

5. まとめ

過去に発生したリスクに対しては様々な対策を行ってきた。今後もセキュリティ向上のために，更に有効な対策を計画，実施している。その一方で継続中の課題等，様々な課題があり，その課題に挑みながら，更に高いセキュリティを目指す次第である。