北九州学術研究都市におけるネットワークの構築と運用

佐藤　敬† 上原　聡† 福永　泰之‡

†北九州市立大学国際環境工学部
808-0135 福岡県北九州市若松区ひびきの 1-1
{tsatoh,uehara}@env.kitakyu-u.ac.jp

‡（財）北九州産業学術推進機構
808-0135 福岡県北九州市若松区ひびきの 2-1
y-fukunaga@ksrp.or.jp

あらまし　理工学系の大学・研究機関を集積した北九州学術研究都市では，キャンパス内に整備された情報ネットワークの一体的な管理運営を行っている．小稿では，学術研究都市におけるネットワーク構築と運用に関する先駆的な取り組みについて紹介する．また，その取り組みの一つであるコンピュータウイルス対策を通じて，これまでに明らかになったネットワークの問題点を述べるとともにその解決策を探る．最後に，本ネットワークの抱える課題について議論を行う．

Design and Operation of the On-Campus Network in Kitakyushu Science and Research Park

Takashi SATOH†, Satoshi UEHARA† and Yasuyuki FUKUNAGA‡

†Faculty of Environmental Engineering
The University of Kitakyushu
1-1 Hibikino, Wakamatsu-ku, Kitakyushu
Fukuoka, 808-0135 Japan
{tsatoh,uehara}@env.kitakyu-u.ac.jp

‡Kitakyushu Foundation for the Advancement
of Industry, Science and Technology
2-1 Hibikino, Wakamatsu-ku, Kitakyushu
Fukuoka, 808-0135 Japan
y-fukunaga@ksrp.or.jp

Abstract　The main feature of the Kitakyushu Science and Research Park is the fact that universities and research institutes in science and technology both in Japan and overseas are integrated onto one campus. The Campus Administration Center carries out the efficient operation and comprehensive management of the on-campus information network in the Park.

In this paper, we introduce about several advanced challenges on the design and operation of the network, and describe problems which has become clear through until now operation with respect to countermeasures for computer viruses. Further, we explore the solution for the problems, and discuss the issue of our network.

1. 北九州学術研究都市

北九州学術研究都市は，北九州市が 21 世紀における創造的な産業都市として再生するためのルネッサンス構想 4 大プロジェクトとして掲げた構想の一つであり，アジアの中核的な学術研究拠点の形成と新たな産業の創出，技術の高度化を目指している．[1)] 北九州学術研究都市の試みは国内でも例をみないものであり，同一キャンパスには，北九州市立大学国際環境工学部，九州工業大学大学院生命体工学研究科，早稲田大学理工学総合研究センター九州研究所，英国クランフィールド大学日本北九州研究所，(ドイツ国立情報処理研究所）GMD-Japan 研究所，福岡県リサイクル総合研究センター，通信・放送機構北九州 IT 研究開発支援センター等の国内外の国公私立大学や研究機関だけでなく，ベンチャー企業も多数集積している．

2. 学術研究都市における先駆的な取り組み

北九州市では，学術研究都市の情報基盤整備にあたり,「北九州学術・研究都市情報通信基盤実施計画書」を作成し，同計画書に基づき 1999 年よりネットワークの運用と設計に関する仕様策定を行った．以下では，学術研究都市における情報システムの設計と運用に関する先駆的な取り組みの一部について紹介する．

2.1 ネットワーク運用の外部委託

学術研究都市においては，複数の大学・研究機関等が同一のキャンパスで共通の理念と方針の下に施設設備等の共同利用などで相互に協力・連携しながら教育研究を行っていくという新しいキャンパス運営を行うこととしている．情報基盤についても同様な取り組みが行われ，情報基盤の一体的な運営や情報処理教育施設の共同利用を図るなど既存の情報基盤の管理運用と異なっていることが学術研究都市における情報基盤の最大の特徴である．

学術研究都市内の情報通信基盤を円滑に運用するために学術情報センターが設置されている．後述するように，学術情報センターは都市内各施設の外部との通信を担う情報基盤の中枢である．学術情報センターにおけるネットワークの運営は（財）北九州産業学術推進機構のネットワーク管理課が担当しているが，ネットワークの監視業務等，専門的な知識を必要な各所は外部へ委託し，専任の要員を常駐させることにより専門的機能を確保している．

2.2 ユーザ情報の一元管理

ユーザのアカウントは各組織からの申請に基づき，組織単位ではなく学術研究都市内各システム共通として発行している．アカウントの新規申請については，各組織が学術情報センターにあらかじめ指定された情報を CSV 形式で提出することによりユーザ管理システムからアカウントが発行されるようになっている．同システムでは仮パスワードの自動設定，パスワード忘却者への対応などが容易に行えるようになっており，アカウント発行，管理業務の省力化を図っている．また，学術研究都市内では OS の異なった多数のシステムが利用されているためにどのシステムでも同一のアカウントが使用できるようにユーザ情報（ID とパスワード）の統一的管理を行っている．

2.3 キャンパスネットワークの設計

幹　線　系

キャンパスネットワークの核である幹線系については仕様策定時点の国内外の動向を鑑み，画像系とデータ系をそれぞれ ATM と Gigabit Ethernet で別々に構成する網構成をとっている．キャンパスネットワークのバックボーンには，学術情報センターを中心として北九州市立大学国際環境工学部，産学連携センター，早稲田大学理工学総合研究センター九州研究所等の各建物をスター型で接続した Gigabit Ethernet を採用している．また，高画質を要求するマルチメディアの実験に対応したデータ通信や遠隔会議などを可能とするために ATM ネットワークを補完的に構築している．図 1 に学術研究都市のキャンパスネットワーク図を示す．

IP アドレスの枯渇のため，キャンパスネットワークの基本はクラス A のプライベートネットワークとし，各組織においてグローバルアドレスを準備することにしている．

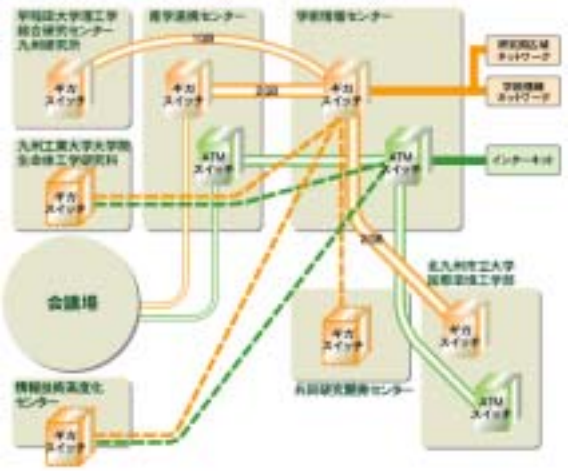

図 1　学術研究都市のキャンパスネットワーク

支　線　系

一方，各建物内には，ギガスイッチを配置し各フロアにスイッチングハブを設置している．ネットワークの拡張，変更作業が容易に行えるように，各組織単位および組織内の業務内容に応じて構成した論理的セグメントによるセグメント設計を行っている．支線系の情報コンセントでは，100BASE-TX（または 1000BASE-X）が利用可能である．

対 外 接 続

国内外の大学・研究機関などの広域的な接続を確保するために，まず商用 ISP へは 6Mbps

の専用線で接続されている．また，北九州市が整備している「北九州地域情報ネットワーク」を介して，学術情報ネットワーク (SINET) の北九州ノードである九州工業大学へ 100Mbps で接続されている☆．さらに，通信・放送機構が整備している研究開発用ギガビットネットワーク (JGN) などの研究用ネットワークへの接続も可能である．

前述のように，学術研究都市のインターネット接続は，学術情報ネットワーク (SINET) および商用プロバイダ (ISP) を利用したマルチホームにより構成されている．学術研究都市内の各機関は，教育研究系と商用系に大きく分けることができる．教育研究系は SINET の利用を，商用系は ISP の利用を原則とすることによって，利用目的の異なるネットワークを分割している．

2.4 セキュリティ方針

本ネットワークの仕様策定時は，各大学，各省庁の WWW サーバが連続して不正侵入を受け，データの改ざんが頻繁に行われる事件が多発していたことがあり，また，不正アクセス防止法の施行等の流れをふまえて，以下の対応を行っている．

- 不正利用および検知装置の設置
  不正アクセス行為の自動検知装置を導入し，インターネットとの通信内容を走査する．万一，通信内容に不正侵入命令が含まれていた場合，該当する通信のみを自動的に遮断することで，内部から外部への不正行為を未然に防止する．
- 通信記録の継続的な採取
  主要なサーバ機器，ファイアウォール，及び不正アクセス検知装置を通過するすべての通信に対し，発信元，発信先等の情報を通信記録として継続的に採取する．
- コンピュータウイルスの侵入防止装置の設置
  既存のクライアント機器を中心としたウイルス対策だけではなく，キャンパスネットワークの基本サービスとして，SMTP/HTTP/FTP を介したコンピュータウイルスの感染予防および駆除が可能な装置を導入する．
- 運用管理
  ファイアウォール等各サーバのログの記録だけでなく，ネットワーク管理・監視システムの導入によりトラフィックの常時監視，不正アクセスの自動遮断等を行っている．

☆ 実効速度は SINET の西日本ループの混雑状況に左右される．

3. コンピュータウイルス対策

3.1 ウイルス対策ソフトウェアの導入

仕様策定時は，クライアントにおいてウイルス検査プログラムを導入することがまだ一般的であったが，インターネット上の電子メールや Web アクセスを介したコンピュータウイルスの蔓延が情報システムにおいて大きな脅威となりつつあると考えられていた．

学術研究都市では，インターネット経由でのコンピュータウイルス侵入の防止を目的に，ウイルス対策ソフトウェアとしてトレンドマイクロ社の InterScan VirusWall[2] を導入し，キャンパスネットワークにおける基本サービスとして電子メールの添付ファイルや FTP，HTTP によるダウンロードファイルに含まれている不正なウイルスの検知・駆除を行っている．

同ソフトウェアを利用したコンピュータウイルス対策の取り組みについては，既に文献[3] 等で報告されている．学術研究都市のウイルス対策はそれらの取り組みに類似したものであるが，情報基盤構築の仕様策定は 1999 年に着手されたものであり独立したものである．

以下では，これまでのコンピュータウイルス対策の運用状況を示すとともに，その問題点を述べ解決策を探る．

3.2 SMTP 経由でのウイルス対策

3.2.1 メールシステムの構成

図 2 に学術研究都市におけるメールシステムの構成の概念図を示す．クライアントまたはインターネットから届いたメールは，ウイルス検査ソフトウェアに引渡されウイルスが含まれているか検査される．検査の結果で問題がなければメールは配送されるが，問題がみつかった場合には送信者・受信者への通知が行われる．

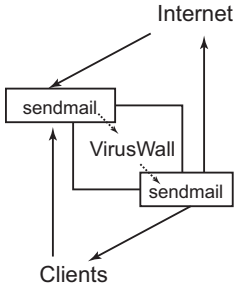

図 2 メールシステムの概念図

3.3 運 用 状 況

本システムは 2001 年 3 月より稼動していた

表 1 SMTP 経由でのウイルス別検出数

ウイルス名	検出数
WORM_FRETHEM.K	817
WORM_KLEZ.H	508
WORM_KLEZ.G	121
WORM_KLEZ.E	70
WORM_BADTRANS.B	19
W97M_MARKER	5
WORM_FBOUND.C	4
	⋮
計	1603

が，2002 年 3 月に一部メールシステムの構成変更を行ったためにメールサーバのウイルスログが残念なことに消えている．したがって，ここでは，2002 年 3 月から 7 月までの 5ヶ月間の運用結果について述べる．

学術研究都市内では 1 日あたり約 4000 通のメールが配送されている．登録ユーザ数 1039 名に対し，ウイルス検査ソフトウェアがなければウイルスメールを受信するはずだったユーザ数は 200 名近くに達する．計算上は，1 年間でユーザ一人あたり 0.4 個のウイルスを受け取る可能性があるが，これまでのログの解析状況をみる限りでは，同一のユーザが繰り返しウイルスメールを受信する傾向が非常に高いが，最近のウイルスに限ると対象となるユーザのは広がりつつある傾向が見られる．表 1 に 2002 年 3 月から 7 月までの検出数を示す．最近話題の WORM_KLEZ や WORM_FRETHEM が他のウイルスに比べて圧倒的に多いことがわかる．

3.4 HTTP, FTP 経由でのウィルス対策

3.4.1 プロキシによる構成

学術研究都市内部ではプライベート・アドレスを基本としているため，外部へのアクセスにはプロキシを経由する必要がある．当初はファイアウォールにウイルス検査ソフトウェアを設置していた．しかし，ファイアウォールの負荷や資源の有効利用の観点から，プロキシにそれを置くように変更している．ユーザーがインターネット上のファイルの閲覧や取得の際には，図 3 に示すようにプロキシを経由しウイルス検査を行うようになっている．

また，FTP/HTTP を対象としたウイルス検査にあたっては，検査時の遅延によるタイムアウトを極力無くすように設定されている（表 2）．

3.4.2 運 用 状 況

次に，これまでの運用から明らかになった本システムの問題点として次の 3 点があげられる．

(1) netscape.com 等に代表される特定サイトからのダウンロードの失敗

(2) 大きなサイズのファイルをダウンロードする際の遅延とタイムアウト

(3) プロキシの耐故障性の脆弱さ

(2) の原因は，プロキシでウイルス検査が完了するまでクライアント側との接続がアイドル状態となるため，アクセスするファイルのサイズが大きい場合には検査に要する時間が長くなり，特にプロキシの負荷が高い場合にはタイムアウトをまねくと考えられる．現時点で，Virus を含むファイルにアクセスしたユーザーに対して Virus 検出の通知が無いため，タイムアウトの理由が分からずにそのファイルへ複数回のアクセスしたことが確認されている．また，(3) については，Web ブラウザなどにおいてはプロキシは通常 1 つしか指定できないために，そのプロキシが故障したときに通信できなくなるというプロキシ運用の問題点があげられる．

また，開学以来 16ヶ月が経過した時点で検出されたウイルスは 476 件 (全 47 種) に及ぶが，複数月にわたって検出される Virus は 6 種類に留まっている．

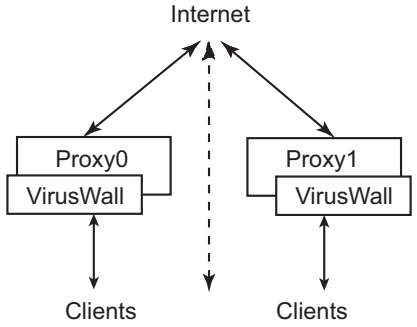

図 3 プロキシの構成図

表 2 プロキシの設定パラメータ

プロセス		タイムアウト	
起動時の生成プロセス数	2	クライアント接続	5 秒
待ちプロセスの再生成時間	3600 秒	サーバ接続	120 秒
最大起動子プロセス数	25		

表 3 複数月で検出されたウイルス

ウイルス名	検出数	検出期間 (月)
JS_EXCEPTION.GEN	198	2001.11-2002.7(9)
JS_SEEKER.E1	9	2002.6-7(2)
WORM_BADTRANS.B	6	2002.1, 2002.4(2)
TROJ_SIRCAM.A	5	2002.7-8, 2002.10(3)
TROJ_HYBRIS.B	3	2002.6, 2002.10(2)
TROJ_HYBRIS.M	3	2002.6-7(2)

この結果からも明らかなように複数月にわたって検出されるウイルスの数は少なく，一時期に集中している．当然のことながら，運用面において新種のウイルスに対する定義ファイルを速やかに更新することが重要である．

3.5 改 善 策

前述のようなダウンロードにおける問題点やプロキシの耐障害性を改善するために，JavaScriptによるプロキシ自動設定ファイル (proxy auto config) を提供することで，安全性の高いと思われる信頼できるサイトに関してはウイルス検査を通らないようにするなどプロキシの自動選択を行うことが可能である．図 4 にプロキシの運用改善の概念図を示す．また，自動設定ファイルを用いることで，日常使用しているプロキシがダウンしている場合，別のプロキシに振り返るなど，プロキシの耐故障性も同時に改善される．既に北九州市立大学国際環境工学部ではこの改善策を一部で採用し良好な結果を得ている．

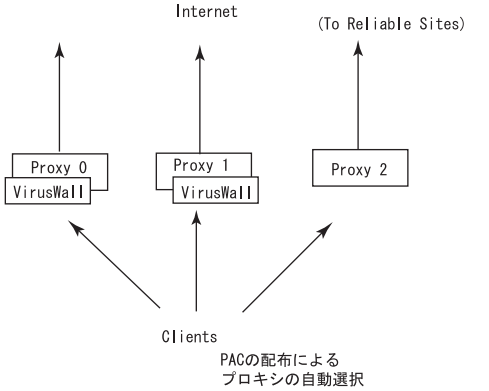

図 4 プロキシの自動設定

3.6 コンピュータウイルス検査の限界と課題

学術研究都市における事例では，電子メールによるウイルスの侵入の試みは全体の 9 割を占めており，文献[4] 等でも指摘されている事実に近い．

これまでの運用を経てウイルス検査で問題になった点を述べる．

- ログファイルの扱い
  ウイルス検査ソフトウェアの出力するログファイルは特殊な形式で保存されており，データの検索や整理は同ソフトウェアのツールからしか読み出せない．データを複数置くことができない仕様になっているために，データファイルを一度動かしてしまうと，読むのに一苦労したり読めなくなったりしてしまうという欠点がある．実際に，メールサーバの構成変更時にその問題に直面することとなった．
- ウイルス対策の限界
  WORM_FRETHEM.K などのウイルスに見られるように非常に広範囲に短時間で蔓延するウイルスには，ウイルス検査ソフトウェアでの限界には対応がある．実際，ウイルス検査メーカーのデータファイルの更新が間に合わず，学術研究都市内でも対策を怠っていたユーザがウイルスの蔓延に一役買うこととなってしまった．コンピュータウイルス対策にあたっては，単にネットワーク運用のシステム面だけでなく，利用者のセキュリティ意識向上が必要であることをあらためて再確認することとなった．

4. 学術研究都市における諸課題

施設の共同利用などで互いに協力するという北九州学術研究都市の試みは国内でも例のないものであり，ネットワークの運用においてもその成果が試されるところである．

特徴の一つであるネットワーク管理の完全な外部委託は，一方で内部でのネットワークに精通した人材が育たなくなるという欠点を持ち合わせている．そのため，現在，北九州市立大学国際環境工学部では，著者らが（財）北九州産業学術推進機構に対しネットワークの運営に関する技術相談にあたるほかに，学生を対象に現業実習を通じたネットワーク管理者の育成を試みている．

また，学術研究都市では情報基盤の共有の一つの実現として，現在その理念に基づき各機関が共同して電子ジャーナルを購読できるように関係機関と調整を図っている．現時点では代理店等の理解がまだ十分得られず，実施できる段階ではないが，国立大学の一部で行われているコンソーシアム形式の導入について模索している．

学術研究都市は様々な価値観を有する大学や企業などの機関が集積し，市民に開かれたオープンキャンパスである．そのために，セキュリティを確保しつつかつ利用者にとって開かれたネットワークにするという課題を抱えている．また，各機関およびその内部の組織ごとに業務内容や要望事項はまちまちである．そのために，ネットワークのセキュリティポリシー等の策定においては各機関およびその組織においても大きな

違いがみられる．最近では，比較的アクセス制限を緩やかにした教育研究系においても UNIX などの OS に比べてその脆弱性が指摘されている Windows が広く使われるようになってきており，従来のように教育研究系であっても，アクセスの自由さだけを求めることが難しくなってきており，利用者へのセキュリティに対する意識の向上を促すことが不可欠となってきている．

このような状況を背景として，学術研究都市内でも情報セキュリティを策定する必要性が認識されてきている．[5] では大学における情報セキュリティポリシーの考え方の一例が示されている．現時点ではまだ試行錯誤を繰り返してネットワークの構築や運営を行っているのが実情であるが，学術研究都市にふさわしいセキュリティポリシーの検討が進められようとしている．

また，学術研究都市では基本としてプライベートネットワークを用いているため，インターネット電話など標準で NAT 変換で対応できないアプリケーションが使えないという問題があるが，各機関で取得したグローバルアドレスを利用することで一応の解決は可能である．IPv4 のアドレスが不足しているキャンパスであるからこそ，先駆的にキャンパス全体へ IPv6 の導入を図る準備を進めるなど，現状に満足することなく最新の動向に対応できるように動いている．

5. むすび

小稿では，学術研究都市におけるネットワーク構築と運用に関する新しい取り組みの一部を紹介し，情報システムの構築に関するこれまでの試みとその試みの一つであるウイルス対策の状況および今後の課題等について言及した．ネットワークのブロードバンド化，モバイル通信，IPv6 の導入など，ネットワーク技術を取り巻く状況は日々刻々と変化しており，それらに柔軟に対応していくことが求められている．北九州学術研究都市においても，今後も高い柔軟性と先端性を兼ね備えた情報システムであり続けるためには不断の努力が欠かせない．

謝辞

小稿の作成にあたり，資料の提供にご協力頂いた (財) 北九州産業学術推進機構ならびに（財）九州ヒューマンメディア創造センターに深く感謝する．

参考文献

1) 北九州学術研究都市ホームページ
http://www.ksrp.or.jp/
2) トレンドマイクロ社ホームページ
http://www.trendmicro.co.jp/
3) サーバにおけるコンピュータウイルス検査システムの設計と運用，敷田 幹文，井口 寧，松澤 照男，情報処理学会論文誌 Vol. 42, No. 12, pp. 2827–2835
4) 国内におけるコンピュータウイルス被害状況調査被害状況報告書，情報処理振興事業協会セキュリティセンター
5) 大学における情報セキュリティポリシーの考え方，大学の情報セキュリティポリシーに関する研究会
http://www.sinet.ad.jp/info/policy/tousin.html