情報基盤部門活動報告

金沢大学の情報セキュリティ事情

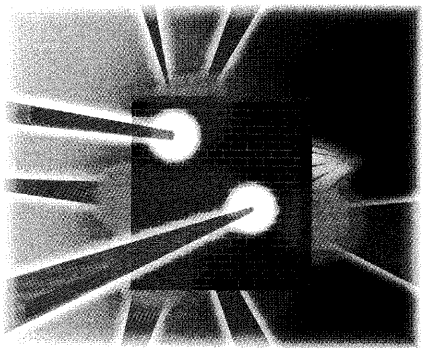
■ 学外からのアクセス件数の調査結果

インターネットの利用者の爆発的な増大に伴い、不正利用等の数も確実に増大しています。図1は、2004年1月から12月までの、金沢大学のファイアウォールに対するアクセス件数です。赤いグラフが一日あたりのアクセス数で、一日あたり200万から300万件のアクセスがあることが分かります。ただしこの件数には、MS-BLASTなどファイアウォール到達以前に遮断されているアクセスの件数は含まれていません。それを含めると、総アクセス数はグラフの数値よりも100万～200万件ほど多いものと推定されます。

しかし、このうち正常なアクセスとして処理されたものは青いグラフで示されるもののみで、残りは全て不正アクセスとして接続拒否されています。不正アクセスの割合はファイアウォールに記録されたものだけで8～9割、それ以前に遮断されたものも考慮すると、おそらく9割以上にのぼると思われます。

多いのはポートスキャンで、これは任意のコンピュータのサービスポートに、ランダムもしくは総なめでアクセスを試みるもので、毎秒数回から数10回のペースで走査されます。もしファイアウォールで接続拒否をしていなかった場合、セキュリティ対策が不十分なサービスのポートがたちどころに発見され、そこを足がかりにコンピュータの乗っ取り、情報の漏洩などの被害が起こり得えます。また、そのコンピュータを足場にしての、他のコンピュータへの攻撃に使われるケースもあり、その場合、そのコンピュータの所有者が、知らない間に被害者ではなく加害者となってしまい、責任を問われることになります。

■ 金沢大学のセキュリティ対策



総合メディア基盤センターでは、これらの実態を踏まえ、学外からのアクセスは原則として全面遮断し、特定のコンピュータの特定のサービスのみについて、接続を許可しています。接続の許可は、教職員からの申請に基づき、審査の上で与えることになっています。

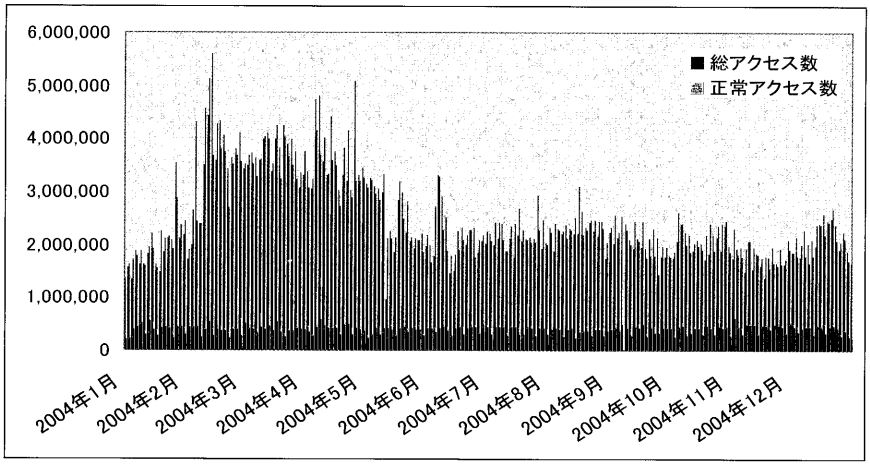


図1　ファイアウォールへの、学外からのアクセス件数（2004年1～12月）

金沢大学のファイアウォールへの、学外からのアクセス件数。赤が総アクセス数。そのうち、青が正常アクセス数。いずれも1日あたりの件数。80～90%が、不正アクセスとして接続拒否されている。

■ ウィルスメールの状況

コンピュータウィルスの感染経路には色々ありますが、そのうち感染件数が最も多く、ウィルスの種類も豊富なのが、電子メールを媒介したものです。これは、電子メールの添付ファイルにウィルスが仕込んであり、そのファイルを開くと感染するものです。感染したコンピュータは、一時間に数百以上のウィルスメールを撒き散らすようになるのが普通です。ほとんど全てのメール系ウィルスが、Microsoft Windows を標的としています。

この電子メールを媒介するウィルスは、感染力が強いだけにその対策にも力が入れられています。色々なメーカからウィルス対策ソフトが販売されていますが、その全てがウィルスメールへの対策を主な機能としています。しかしながら、メール系のウィルスは新種・亜種の発生頻度が極めて高いのも特徴で、フィルタリング用のパターンファイルの提供が後手に回ることも少なくありません。

金沢大学では、学外から配信されてくる電子メールの全てにウィルスチェックを行っています。図２が一日あたりのウィルスメール駆除件数を示したグラフで、１日あたり千通以上が到来していることが分かります。

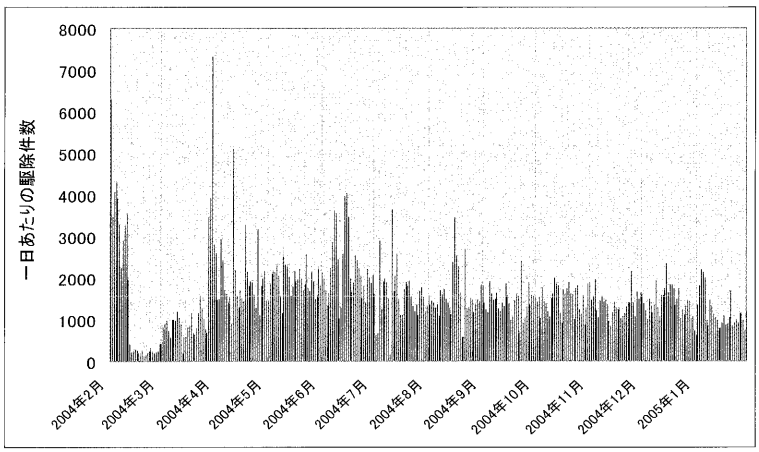


図２ 一日あたりのウィルスメール駆除件数
（2004 年２月～ 2005 年１月）

また、新種・亜種に対応するため、Microsoft Windows で実行できる形式のファイルが添付されているメールは、すぐに配信せずに一旦隔離した上で受信者に通知メールを出し、受信者が Web 上で受信手続きを行って初めて配信される仕組みを構築しています。この仕組みを採用して以来、学内におけるウィルス感染はほとんど無くなりました。

ただし、学外でウィルス感染したノート PC 等を学内に持ち込まれるケースについては、今のところ全学的な対抗手段がありません。各パソコンへのウィルスチェッカ導入など、個人レベルでのセキュリティ対策も徹底する必要があります。

■ スパムメールの状況

ウィルスメールと並んで問題となっているのが、商業的宣伝目的などで無差別にばら撒かれるスパムメールです。図２は金沢大学に配信されてくる一日あたりの全メール数と、そのうちのスパムメールと判断されるメールの数を示したものです。全到来メールのうち、2/3 以上がスパムメールであることが分かります。

金沢大学では、スパムであると判断できるメールを隔離し、１日に一度ユーザにリストを配信していますが、あまりに件数が多いとリストに目を通すだけでも一苦労となります。Web 等にむやみにメールアドレスを載せないなど、標的にされる要素を無くす努力を各自が行う必要があります。

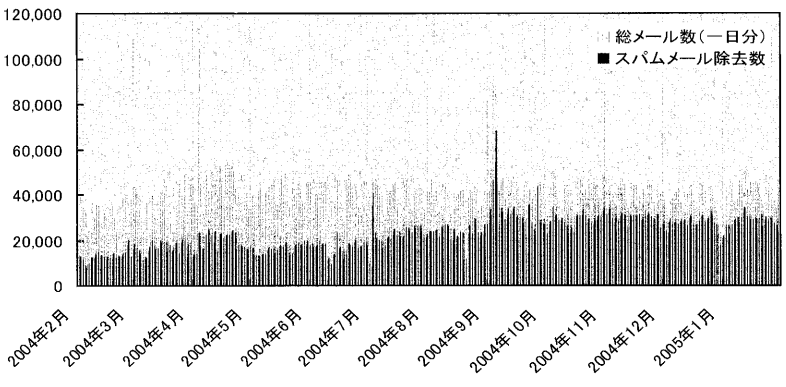


図２ 一日あたりの全到来メール数と、スパムメール数。
（2004 年２月～ 2005 年１月）

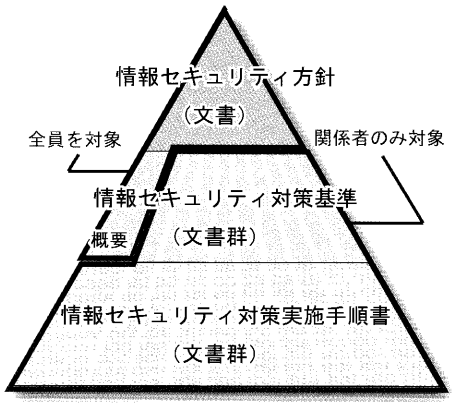
■ 2004 年度の主な活動

活動報告 1　情報セキュリティに関する主な活動

■ 情報セキュリティポリシーの原案策定

事務局情報部等と共に、情報セキュリティポリシーの原案を策定しました。 情報セキュリティポリシーは、全体的な方針を定めた「金沢大学情報セキュリティ方針」、事項ごとのルールを網羅的に記述した「情報セキュリティ対策基準」、より実務的な手順を示した「情報セキュリティ対策実施手順書」から成り、「金沢大学情報セキュリティに関する規程」によって、大学全体への適用が認められます。

平成 17 年度より全学的に施行される予定です。



■ ウィルス・SPAM メール対策の強化

学外からのメールに対して大学の入り口でウィルスチェックすると共に、学内から学内外へ送信されるメールについてもウィルスチェックが施されるよう、ウィルスチェッカ付きの SMTP サーバを設置しました。学内のユーザに送信サーバとしての利用を促すと共に、研究室等に個別に設置してある SMTP サーバからもこちらのリレーされるよう要請してあります。

また、最近爆発的に増加している SPAM メールを隔離し、かつ、誤認識による正常なメールの取りこぼしを防ぐために、隔離された SPAM メールの件名 , 差出人アドレスなどを含むリストを 1 日 1 回配布し、利用者が簡単に確認し取り出せるシステムを作成しました。隔離されたメールは 3 ヶ月間保持され、その後自動廃棄されます。更に、最近増加したフィッシングメールや、詐欺が多発しているアダルト及び出会いサイト系に対応するため、日本語 SPAM フィルターを増強しました。

隔離用の選別フィルタは、実在しないメールアドレスに大量に届いているメールなど、迷惑メールの可能性が極めて高いものから語句等を抽出し、反映させています。玉石まとめて砕くことの無いよう、フィルタ定義は自動化せずに、スタッフの手で毎日行われています。

また、ウィルスの新種・亜種に対応するため、Windows 環境で実行できる形式のファイルが添付されている場合も隔離対象とし、これについては隔離した後、即時通知メールが配信されます。

■ Web ウイルスチェッカーの強化

現在、学生用端末から利用する Web 参照は 3 台でウイルスチェックを行っていますが、利用者の増加に伴いレスポンスが悪くなってきました。これに対応するため、3 台共に搭載メモリを 1GB から 4GB に増強しました。Web ブラウザ上の Proxy サーバ設定により、学生用端末以外からも使用できます。

活動報告 2　情報基盤拡充に関する主な活動

■ 双方向遠隔講義システムに関するネットワーク設計

平成１７年度より稼動予定の双方向遠隔講義システムにおいて、他大学や角間・宝町間との双方向講義が円滑に行えるよう、ネットワークシステム設計を行いました。このシステムでは、各教室ともマルチキャスト対応とし、ネットワークも専用サブネット構成として、セキュリティ面での安全性を考慮しています。また、角間・宝町間では医療画像など高解像の情報（ハイビジョン対応）を取り扱う講義が行えるよう、キャンパス間の速度を 100Mbps から 1Gbps への高速化できるよう計りました。平成 17 年 3 月 7 日からはキャンパス間が 1Gbps で運用されており、双方向遠隔講義システムも平成 17 年 4 月から稼動する予定です。

■ **学生用ファイアウオール及び無線 LAN システムに関する取り組み**

情報教育部門で採択された現代 GP 予算によるプロジェクトの一環として、学生用の無線 LAN システム構築が推進中されています。このシステムについて、暗号化通信、利用者認証、ログ採集及びアクセス制限などを充分に考慮して、セキュリティ及び多人数利用に適した設計を行いました。

■ **学外者用無線 LAN システムに関する取り組み**

近年、学外者の学内におけるネットワーク利用の要望が高まってきていますが、その一方で、学内における機密情報の管理も重要度を増してきています。この矛盾を解決するために、OCN 回線を利用した学外者用ネットワークを新設しました。無線 LAN のセキュリティを高めるため、利用者認証及びログの収集と、IPsec による暗号化通信を組み合わせたシステム構築を行い、平成 17 年 1 月からインキュベーションセンターで試験的に利用されています。他の部局の増設も小額の予算で行うことが可能です。

活動報告 3　サービス拡充に関する主な活動

■ **メーリングリストサーバの提供**

教職員を対象に、メーリングリストのレンタルサービスを開始しました。

■ Web プロクシーキャッシングサーバの強化

学外への Web 参照は、ファイアウォールの負荷を軽減するためにプロクシーキャッシングサーバを経由させていますが、故障時のレスポンス低下を防ぐために、従来の 2 台から 3 台に増強しました。

■ **学生用メールサーバの容量増強**

学生用メールサーバの蓄積容量を、5MB から 10MB に拡張しました。

■ 各種申請書のオンライン

各種申請を、Web を用いてオンラインで行えるようにしました。新たにオンライン化されたのは、主に以下のものです。

- VPN 利用申請
- 遠隔会議システム利用申請
- IP 電話利用申請
- 数式計算ソフト Maple 利用申請

活動報告 4　研究会・セミナー等の開催

■ **金沢大学ネットワーク研究会の立ち上げと、セミナーの開催**

「金沢大学ネットワーク研究会」を立ち上げ、これまでにセミナーを 2 回開催しました。第 1 回は IPv6 についての講演を学外より講師を招いて行った後、金沢大学の IPv6 準備状況について報告を行いました。第 2 回は、個人情報保護と、ウィルス・スパムメールについての 2 テーマについて、講演会を行いました。どちらも時間一杯まで熱心な議論が交わされました。

情報基盤部門　URL http://www.gipc.kanazawa-u.ac.jp/kains/
教　授 車古 正樹　E-mail: shako@office0.ipc.kanazawa-u.ac.jp
助　手 井町 智彦　E-mail: imachi@kenroku.kanazawa-u.ac.jp