特集2

# ネットワークと情報セキュリティ

## 情報セキュリティのはなし

総合メディア基盤センター 情報基盤部門助手　井町 智彦

### 年々重要になるセキュリティの確保

90年代半ばまでは，インターネットからの大学等へのアクセスは，比較的自由に行えるのが一般的でしたが，それ以降は外部からのアクセス許可は必要最小限にとどめ，不正アクセスに対する防衛を厳重にするのが常識となっています．

金沢大学においても，インターネットと学内ネットワークの境界で，アクセスの内容，接続先，接続元などの情報を元に，アクセスの可否を決定しています．このアクセスの可否を決定しコントロールする装置を，ファイアウォールといいます．

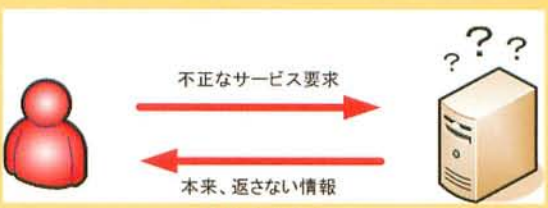
金沢大学には，一日あたり約40万件のアクセスがありますが，その8割以上がファイアウォールにより接続拒否されています．接続拒否されたものは，大半が以下で述べる不正アクセスに相当するものです．

### 不正アクセスとは

Web閲覧にせよ電子メールにせよ，ネットワークを利用する場合は各種サーバにサービス要求を送り，要求内容に応じた情報を得る形態が一般的です．この時，サーバに対して意図的に不正なサービス要求を行うと，サーバが本来返してはいけない情報を返したり，要求を解釈できずに混乱もしくは機能を停止してしまう場合があります．

このような，システムの混乱や情報の不正取得を狙って起こされる，悪意を伴ったアクセスを，不正アクセスいいます．

正常なサービス利用と…



不正アクセス

### セキュリティホールとその対策

もちろん，このような不正なサービス要求に対しては，不正なデータは要求として受付けないなど，サーバ側で対応しているのが普通です．しかしながら，サーバのソフトウェアのプログラムミスや想定外の攻撃を受けた場合などで，不正なサービス要求を受け入れてしまう場合が時々にあります．このような欠陥のことを，セキュリティホールと呼びます．

### 「更新」を怠りなく！

セキュリティホールの発見は，ある程度偶然に頼るしかないのですが，ひとたび発見されたセキュリティホールについては，OSやアプリケーションソフトの供給元から，セキュリティホールの無い新バージョンのプログラムか，セキュリティホールを塞ぐための修正用プログラム（パッチ）が提供されますので，それを使って更新（アップデート）を行わなければなりません．多くのOS，アプリケーションソフトの場合，更新は必要な時にコンピュータが自動的に行うようにできるので，その機能を活用しましょう．特にMicrosoft Windows等のOSについては，必ず自動更新を有効にしておきましょう．

## やはり重要．パスワード

OS やアプリケーションソフトの更新を確実に行っていても，不正アクセスによる被害を完全に防げるわけではありません．現在では，コンピュータの開始時にユーザ ID とパスワードによるユーザ認証を行うのが普通ですが，ユーザ認証に使用されるパスワードは，時として予測が可能な見破られやすいパスワードを使っている場合があります．

不正アクセスを試みる攻撃者は，こういう見破られやすいパスワードを探して，手当たりしだいにユーザ認証を仕掛けてきます．この「パスワードアタック」は，セキュリティホールの有無とは関係なく脅威となります．

### 「良いパスワード」は防御の基本

対策としては，アクセスを許すコンピュータの台数を最少限度に抑え，攻撃対象を少なくする事と，アクセスを許すコンピュータに登録されているユーザについては，パスワードを特に見破られにくいものにすることが大切です．

### SSH 利用者は，特に注意を

最近急激に増加しているのが，SSH に対するパスワードアタックで，これまでは「数撃ちゃ当たる攻撃」に使用されるユーザ名は欧米人の苗字が多かったのですが，最近では日本人の苗字も攻撃に使用されるようになってきました．管理者の皆様には，SSH を利用するユーザのパスワード管理をより慎重に行うとともに，学内外に公開する SSH サーバの数自体も，最少限度に抑えて頂けるよう，お願いいたします．

## コンピュータウィルス

コンピュータウィルスについても，対策を講じておくことが，もはや当たり前のことになりつつあります．

コンピュータウィルスとは，自分自身を他のコンピュータにコピーして，拡散していこうとする性質を持っているので，もし感染した場合，このコンピュータは他のコンピュータに対して攻撃を始めます．つまり，自分が知らないうちに加害者になっている可能性があるので，十分に注意しましょう．

コンピュータウィルスの感染源として最も多いのが電子メールですが，金沢大学のメールアドレス（kanazawa-u.ac.jp で終わるもの全て）については，大学の入り口でウィルスチェックが行われています．現状で，一日あたり 1000 以上のウィルスメールが削除されていますが，最近のウィルスは新種・亜種の発生頻度が高く，チェックをすり抜けて学内に入って来るウィルスも存在しますので，各自のコンピュータにも対策が必要です．

### パソコンにはウィルス対策ソフトを

コンピュータ，特に Microsoft Windows 系の OS には，何らかのウィルス対策ソフトをインストールして，ウィルス検出のパターンファイルを常に最新のものに更新しておきましょう．パターンファイルの更新は大抵の場合自動的に行われることができるので，そういった機能を活用しましょう．

## 情報漏洩にご注意を

不正アクセスやコンピュータウィルスの被害として，もっとも問題とされるのが，コンピュータの中にプログラムを埋め込まれ，それによって情報が漏洩することです．この情報漏えいには，プログラムを埋め込まれるケース以外にも色々なパターンがあります．例えばフィッシングメールと呼ばれるものは，メール中に書かれた URL でカード会社を装った Web ページに誘導してカード番号を入力させたりします．

情報漏えいの危険性は，情報化社会の発展と表裏一体で日ごと大きくなっているので，各自が自分のもつ情報をしっかりと保護する意識を持つことが大切です．不審なメールに記載された Web ページには迂闊にアクセスしないことや，可能な限り，ネットワークにつながったコンピュータに重要な情報を置かないこと，あるいは秘匿性の高い情報は暗号化して保存しておくなどの対策が必要です．