教育ネットワークにおける情報流通(2)

有害情報の抑制技術の現状と KIU の対応

Distribution of Information on Education Network (2)

-Present Status of Technology to Control Harmful Information, and the Measures taken by KIU

久保美和子[1]
Miwako Kubo
Miwako_Kubo@reitaku-u.ac.jp
（麗澤大学国際経済学部）

•

瀧口樹良[2]
Kiyoshi Takiguchi
taki@kiu.ad.jp
（駒澤大学大学院人文科学研究科社会学専攻修士課程）

Abstract: There are several front lines of defense against undesirable information, such as router gateway base filter, proxy base filter, client base filter, and so on. In case the network is star structure, it becomes possible to control information by any of these methods. When the definition of unnecessary information is given, it is easy to implement these filters. In this paper, we shall report the advantages and disadvantages of each filtering method. We shall also introduce the technique of constructing a partial Intranet without making information public on the Internet.

Keywords: Education Network, Filtering, Security

1. はじめに

インターネットは、われわれの社会生活に多くの影響を与えている。電子メールや WWW(World Wide Web)はビジネススタイルを劇的に変化させた。手軽に多くの人と時差を気にすることなくコミュニケーションすることや、個人レベルでの情報の発信といったことが可能になった。学校や家庭においても普及がめざましい。産業、教育、交通、政治、地域生活、スポーツ、趣味、娯楽といったあらゆる面で利用が拡大している。

このようにインターネットは脚光を浴びているが、同時に他のメディアと同様に影の部分も存在する。例えば、システム不正侵入、盗聴、システム不正利用、情報改竄、有害情報へのアクセス、個人情報保護の問題、利用者のインターネット依存症候群の問題、ネットワーク上の利用者間のトラブルなどさまざまな問題が上げられる。従来から大学等の教育機関では、これらの問題を、ネチケット（ネットワーク上のエチケット）教育や利用規定等で対応してきた。しかし、商業用ネットワークの普及拡大にともなって氾濫する情報も爆発的に増加し、関連書籍等も多くみられ対応に苦慮することも多い。

教育ネットワークでは、このような影の部分への教育的、技術的対処が重要であろう。とりわけ、インターネット上に氾濫する「有害情報」の問題や児童・生徒の「個人情報保護」の問題には、ソフトウェア的な手法（教育的方法）だけでなくハードウェア的手法（技術的方法）での対応が極めて重要であると考えられる。

[1] KIU 技術部会
[2] KIU 技術部会・KIU 教育技術部会

ここでは、前報に引き続いて「有害情報」の排除と「個人情報保護」という２側面について技術的対応法を検討する。さらに、千葉県柏地域に構築された地域教育ネットワーク、柏インターネットユニオン(KIU)での取り組みと問題点を紹介する。

2. フィルタリングとセキュリティ技術

教育ネットワークでの流通情報の制御には２つの方向性がある。１つは情報を受け取らない技術であり、有害[3]とされる情報を排除することを意味する。ここでは、これをフィルタリングと呼ぶ。２つ目は、重要な情報または部外者への提供が許されない情報の流失を防ぐ技術である。これを本稿ではセキュリティ技術と呼ぶ。情報システムにおいてセキュリティという用語は、システム侵害、不正侵入、不正利用、情報傍受盗聴、情報改竄等に対して使われる用語であるが、ここでは限定的に用いることとする。

3. フィルタリング

情報を受信する側で有害とされる基準に沿って情報を選別（フィルタリング）して排除すれば、有害情報の取得を阻止することができる。例えば、暴力の情報の取得を禁止し、町の歴史に関する情報の取得は許可する基準を設定すれば、暴力の情報は排除されることになる。

情報を選別するには、基準のリストを作成する必要がある。基準のリストに沿って情報を受け入れるか排除するかの判定を行う。リストに記述する項目は、用語や実際に有害または有用な情報のある場所やサービスなどがその対象となる。リストアップは人の手によって行うことになるので、情報量の多いインターネットでは膨大な作業量となる。

有害情報のフィルタリングの方略には２つの方式がある。「ホワイトリスト」方式と「ブラックリスト」方式である。

「ホワイトリスト」方式は、明示的に許可された情報だけを許可する方法である。いいかえれば、リストにないものはすべて禁止される。

「ブラックリスト」方式は、明示的に禁止された情報以外は許可する方法である。「ホワイトリスト」方式とは逆に、リストアップされたものが禁止され、それ以外の情報は全て通過できる。

「ホワイトリスト」方式では、許可されたものだけがフィルタを通過するため、リストアップさえ誤らなければ禁止されるべき情報がフィルタを通過することはない。このため防止効果は高い。しかし、ホワイトリストからもれた情報はすべて禁止されるため、有用な情報を得ることができなくなる欠点がある。一方、「ブラックリスト」方式では、ブラックリストからもれた有害情報を通す危険性がある。反面、有害ではない、新しい情報にも常にアクセスが可能という利点がある。「ブラックリスト」方式、「ホワイトリスト」方式とも一長一短であり、どちらの方法がより効果的であるかについての実験的報告等は今のところ見当たらない。

いずれにしても、このようなリスト方式ではリストのメンテナンスに多くの労力が必要となる。なお、この２つのリストを混在させる方略もある。

3.1 フィルタリング対象

フィルタリングを行う対象には、IP アドレス、サービス、ドメイン、URL、文脈の 5 種類が考えられる。

3.1.1 IP アドレス

TCP/IP で用いられるホストアドレスやネットワークアドレスを用いて制御を行う方法。この場合は、最小単位がホストとなるので、対象となるホストからの一切のアクセスを許可または抑止することとなる。ルータや特殊なブリッジによって実現できる。

3.1.2 サービス

TCP/IP のサービスポート番号をベースに

[3] 有害情報については前報で述べた。

フィルタする方法。TCP/IP では HTTP (WWW), Telnet, FTP, SMTP (E-Mail)等それぞれのサービスにサービスポート番号が付けられているので、そのポート番号によってフィルタが可能である。ルータや特殊なブリッジによって実現できる。

3.1.3 ドメイン名

ホストをインターネット上で識別する名称がドメイン名である。ドメイン名は DNS によって IP アドレスと対応づけれられている。電子メールアドレスや URL に使われる。このドメイン名をフィルタやアクセス制御の対象に利用することができる。通常サーバベースで利用することになる。

3.1.4 URL

URL(Uniform Resource Locator)はインターネットの画期的な発明の一つである。情報にアクセスするための手段と、ドメイン名によるホストの特定、ホスト内の情報の位置を特定することが可能である。さらに、IP のサービスポート番号まで指定することも可能である。フィルタの対象としては、もっとも適切なものである。インターネットでよく使われるサービスは WWW であるから URL によって不適切な情報、または適切な情報が定義できればフィルタリングは容易である。

3.1.5 文脈

転送される情報を全てチェックして、テキスト中の特定の単語や文章をフィルタの対象とする方法。この方法では、リストを特にメンテナンスしなくても、ある程度の有害情報を検出できることになる。URL やドメイン名も文脈に含めることが可能。通常は、クライアントベースでの利用になるが、後述の Porxy サーバへ組み込むことも可能である。

3.2 フィルタリング技術

有害情報のフィルタリングを行う実装点には、ルータ部分、Proxy サーバ部分（ファイアウォール)、クライアント部分の３個所が考えられる。以下にそれぞれの部分でのフィルタリングの特徴を示す。

3.2.1 ルータ方式

標準的な機能を持つルータでは、宛先の IP アドレスや TCP/IP サービス(telnet や WWW 等）ポート番号を基にパケットを振るい落とす機能がある。この機能を利用して有害情報のフィルタリングを行うことができる。既存のネットワーク機器を利用できるため安価に実現できる。

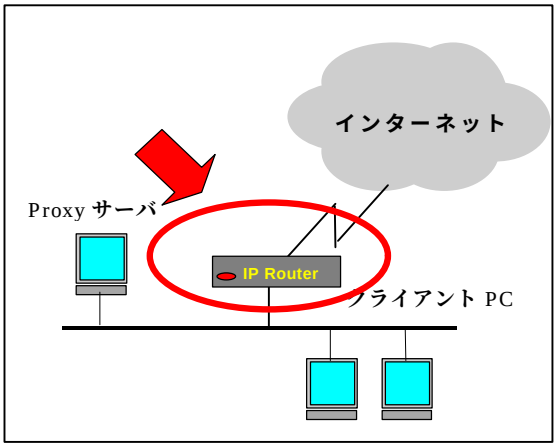

図 1.ルータの位置

この方法では、ルータの設定が煩雑であるため、フィルタリングの対象リスト項目があまりに増えると、構築ミスをしたり、維持が難しいなど運用上の問題が発生する可能性がある。また、ルータ自体の転送効率が低下するなどの弊害が起りうる。さらに、設定単位が IP アドレスやサービスポートとなるので

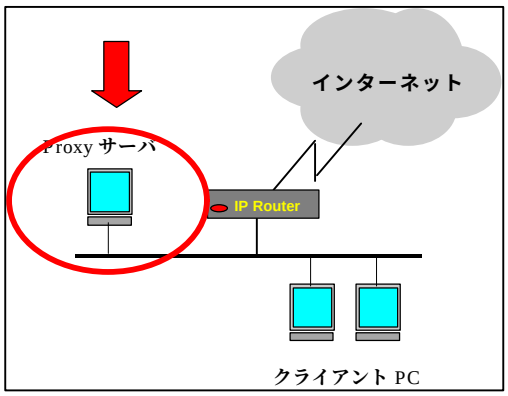

図 2　Proxy サーバの位置

リストに上げられるホスト全体が抑止または通過の対象となる。従って、詳細な設定はできないという欠点を持つ。

フィルタリングを行う単位はルータが設置されるネットワーク単位となる。

3.2.2 PROXY 方式

Proxy サーバとはアクセスを代行し、サービスの中継を行うサーバのことである。Proxy サーバ方式は、クライアントが外部にアクセスする場合には必ず Proxy サーバを経由するような設定を行い、「ブラックリスト」や「ホワイトリスト」を基に有害情報の制御を行うものである。IP アドレスやドメイン名、サービス、URL、文脈単位での制御が実装可能[4]である。

この方法では、Proxy サーバ単位に設定を行うため、１ヶ所ですべてのクライアントに対して有効である。しかし、組織毎に異なるリストの運用は難しく、フィルタリングポリシーをネットワーク全体で決定するか、ポリシー毎に Proxy サーバを運用する必要がある。ネットワーク全体でポリシーを決定する場合、合意形成のために時間を要することになれば、タイムリーな設定は期待できない。

なお、ユーザがクライアント PC の設定を変更し Proxy サーバを使用しないようにした場合には効果がなくなる。このため、ルータ方式と併用して Proxy サーバを通らないクライアントからのパケットはすべて許可しないというルールを設定する必要がある。

3.2.3 ファイアウォール方式

ファイアウォールは広義にはパケットフィルタリング機能をもつルータなども含まれるが、ここでは狭義の意味のファイアウォール[5]とする。ファイアウォール方式と Proxy サーバ方式は理論的には同じである。

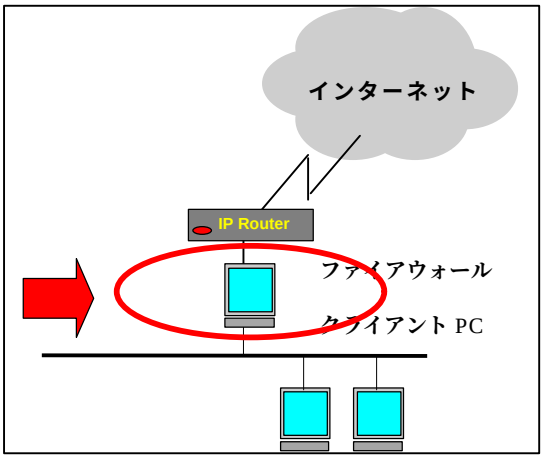

図 3.ファイアウォールの位置

ファイアウォールは外のネットワークと内部のネットワークを分割し、両者からのアクセスを中継し、場合によっては排除する役割を持っている。このため、有害情報のフィルタリング機能を実装[6]しやすく、Proxy 方式のようにルータを併用する必要がない。また、外部ネットワークから不正侵入等を防御できるため、セキュリティレベルも高くなる。

この方法では、専用サーバが必要であるためコストがかかり、維持管理に手間がかかるという欠点がある。また、ファイアウォールは製品として提供されているので、改造は困難となる。

3.2.4 クライアント方式

この方法は、ユーザが実際に使用するクライアントパソコンに、フィルタリング機能をもったアプリケーションをインストールし「ホワイトリスト」または「ブラックリスト」に基づいて情報を選別する方法である。サービスやアプリケーション毎の選別が可能なソフトウェアもある。また、十分とは言えないが、この機能を持つ WWW ブラウザもある。GUI を取り入れた設定画面を持つソフトウェアも多く、専門の知識がなくても扱うことができる。クライアント毎に排除したい有害情

[4] 現時点でこの目的で動作する proxy サーバは見当たらない。既存の proxy サーバを改造する必要がある。ここでは、実装の可能性のみを議論している。

[5] アプリケーションレベルファイアウォールを指す。本来ファイアウォールは外部からの不正侵入を防ぐものとして用いられる。

[6] 特定のネットワークやサービスは容易に排除できる。特定の URL を排除する機能を持つファイアウォール製品もある。民間企業等では転職情報等も有害情報として扱われることがある。

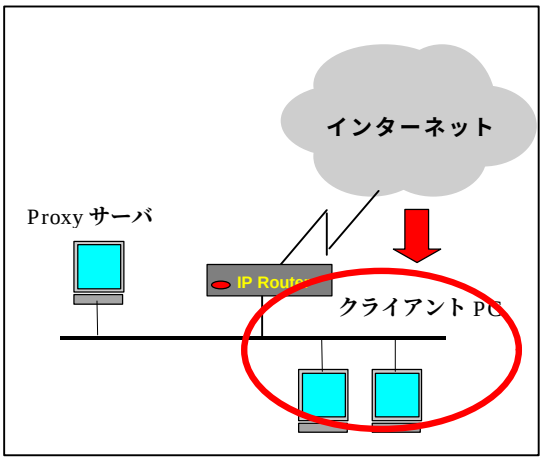

図４.クライアントの位置

報基準を変えるなどの細かい設定が可能である。また、文脈によってテキストベースでフィルタリングを行う機能を持つ製品もある。この方法では組織単位のフィルタリングポリシーを決定することができる。このため、機動的に対応が可能となるが、学校単位で対応に差が生じる可能性も否めない。この方式には、台数が多くなれば運用の手間やコストがかかるという欠点がある。

3.3　フィルタリング技術と KIU での対応

KIU では(1)ルータ方式、(2)Proxy 方式、(3)クライアント方式でフィルタリングが可能である。(1)の場合 KIU 全体であればバックボーン接合部分のルータでフィルタ可能である。また、(2)の場合は KIU の一次キャッシュサーバ部分とルータで行うことができる。(3)の場合は、参加組織内部での実装になるが、クライアントベースのフィルタリングソフトの不足する部分をルータやキャッシュで補完することは可能である。

ただし、このことは KIU が独自にフィルタリングを行うということを意味しない。KIU は所詮プロバイダーであるから、情報の検閲に相当するポリシーを決定することはできない。KIU へ参加する組織によっては全ての情報へのアクセスを希望する場合もあろう。しかしながら、上述のようにフィルタリングを実装する点を提供することは可能である。つまり、適切な機関[7]でポリシーが決定されれば、それを実装するための物理的な制御点を持つということを意味する。KIU は教育ネットワークであるから、このような合意形成は容易であろう。また、方法によっては参加組織単位に異なるポリシーを実装できることになる。KIU 全体での合意形成が必要となるかもしれないが、教育ネットワークの特徴を考えれば実現可能な対応である。

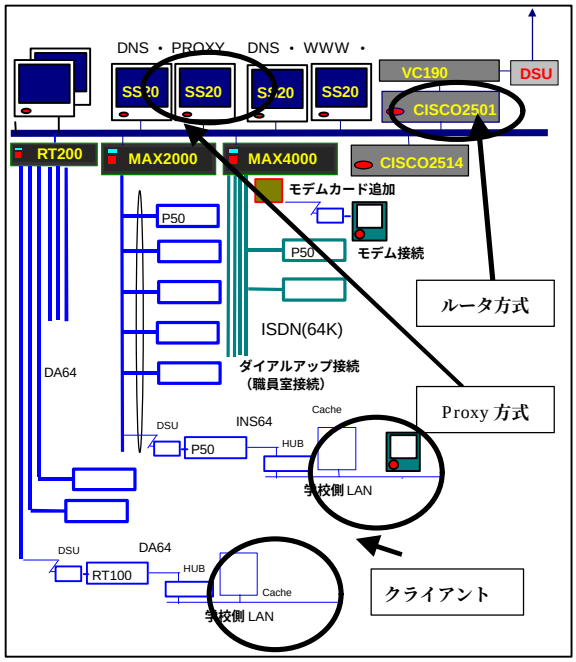

図５.KIU での対応可能点

3.4　フィルタリング技術の限界と対策

フィルタリング技術は完全に有害情報を取り除けるわけではない。

たとえば、クライアントパソコンを不正利用される可能性がある。クライアント方式では、ソフトウェアがインストールされていないパソコンをネットワークに持ち込まれれば効力を持たなくなる。また、導入されているソフトウェアの機能を解除されるケースも想定される。Proxy サーバ・ファイアウォール・ルータ方式の場合でも迂回路（ダイアルアッ

[7] この場合、自治体、議会、地域の教育委員会等の意思決定機関と KIU 総会（または運営委員会）の合意形成がなされればよいだろう。

プ接続など）があると意味がない。このような場合、運用方法の強化を行うことで完全ではないが回避することが可能である。管理者以外はクライアントパソコンの設定や変更ができない設定にすれば、ユーザがダイアルアップ接続やソフトウェアの設定変更を行えないので、不正に利用される危険性[8]は下がる。

有害情報がリストから漏れる可能性もある。URL の変化（新設、移動、削除等）は激しいのでリストから漏れる可能性は高い。これらの作業は手作業に依存するため完全に防御することは不可能となる。リストではなく、テキストから文脈で有害情報を選別する方法では、文字データにのみ対応するため、画像・動画・音声などには対応できていない。

このため、フィルタリング技術と運用面での配慮、そしてユーザ教育など総合的に取り組まなければ効果的な対応とはならない。

4. セキュリティ

情報には、すべての人に公開したい・してもよい情報と、一部には公開したいがそれ以外からは保護したい・公開したくない情報がある。これらの情報を保護するためには、公開したい範囲別に何らかの方法で分類する必要がある。

4.1 セキュリティ技術

ネットワーク上での情報保護の方法は(1)情報を公開しない、(2)公開情報へのアクセスを制限する、(3)公開情報を分離する、(4)ネットワーク自体を分離するなどの方法がある。ここでは、(1)を除いた 3 つ方法について述べる。

4.1.1 公開制限

基本的には情報公開するがサーバプログラムの設定によりアクセスするユーザやホスト、ネットワークを制限する方法である。例えばHTTP(WWW)のサーバでは、動作設定を加えることで、通常特定のファイルに記述した範

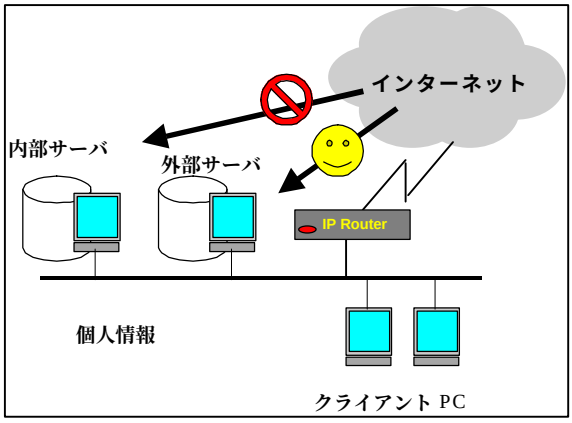

図６.内部サーバと外部サーバの運用

囲のホストのみが利用できるようになる。この場合、特定のネットワークやホストを利用する者しか情報にアクセスできない。ただし、この場合そのホストを利用しているのが誰かの特定はできない。

一方、WWW 等一般に公開されるサービスでも、ユーザ名とパスワードによって利用者を特定することもできる。ただし、パスワード設定の場合はそのパスワードが保護されなければ意味がない。利用者が変化するようなサービスには向かない。ユーザ管理をする必要があり、それなりの労力が必要となる。

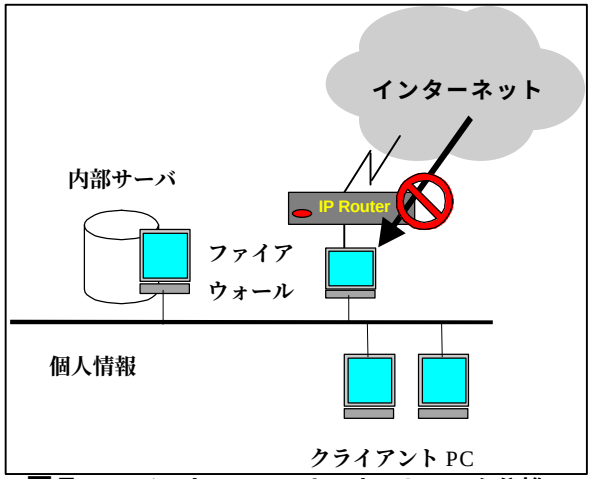

図７.ファイアウォールによるネットワーク分離

4.1.2 公開情報の分離

広く公開する情報と一部にだけ公開する情報を分離するには、情報を提供するサーバ自

[8] 学校等では想定しにくいが、大学や企業では配慮されなければならない対処点の一つである。

教育ネットワークにおける情報流通(2)　　**久保美和子**