大学キャンパスネットワークのための自己防衛型ネットワークの設計法に関する考察

On a Method of Designing Self-Defending Campus Networks

喜家村　奨

Susumu Kiyamura

要　約

ウィルス，スパイウエア，ハッカーの攻撃など様々な脅威が存在する今日，ネットワークはただのインフラではなく一つのセキュリティシステムとして設計する必要がある．しかしセキュリティシステムとしてネットワークを設計する手法についてまだ確立されたものがない．このような現状から，本論文では自己防衛型ネットワーク[1)]という概念を用いて大学におけるキャンパスネットワークを設計するその方法について考察する．

第１章　はじめに

第１節　研究の背景

現在，ファイアウォール，ウィルスゲートウエイ，侵入検知装置など多くのセキュリティ製品が販売されているがそれらをどのように配置すれば効率よくかつ確実に多くの脅威からネットワークシステムを守れるのか．従来まではインターネットの出入り口にファイアウォールを設置すれば脅威からある程度システムを守れたが今ではリモートアクセス環境，VPN環境，無線LAN環境など，ネットワークのあらゆるところからハッカーに侵入され被害を受ける可能性がある．また，大学のおける教育・研究用ネットワークは，その性質上，ユーザの利便性を無視できない．このような観点から大学キャンパスネットワークのための自己防衛型ネットワークの設計法について考える．

本論文ではまず，ネットワークシステムを表現するために，抽象的なネットワークモデルを定義する．次にそのモデルを用いて自己防衛型ネットワークを定義する．最後にその定義した自己防衛型ネットワークの性質を満たす現実のネットワークの設計法を示す．

第2節　キャンパスネットワークにおける自己防衛型ネットワークの必要性

ネットワークに接続された端末が全てハードディスクレスでリムーバブルメディアも装着できないようなPCなら，それらの端末からの脅威は少なくてすむであろう．しかし，大学ではその教育・研究機関という性質からユーザの利便性を無視できない．例えば本学におけるネットワーク利用のための運用ポリシーは以下のとおりである．

- 非常勤講師などのために持ち込みPCによるインターネットアクセスを許す．
- 学生は演習用PCをどの演習室でも同じように利用できる．
- 研究室のPCは申請し，IPアドレスさえ取得すれば教員が自由に設置できる（機種の変更等も可）．
- 申請さえすれば，他部署（事務や図書館など）はPCをネットワークに接続できる．

上記のように本学のネットワークはユーザに柔軟な対応ができるようにサービスを提供している．このような環境であるため，ネットワークに接続されるPCのセキュリティが完全であるかどうかはわからない．よって，ネットワークシステムがインフラというだけでなくみずからセキュリティを守る，つまり“自己防衛型ネットワークシステム”として機能することは非常に重要であると思われる．

第2章　準備

この章では，まず，抽象的なネットワークモデルを定義し，次に自己防衛型ネットワークを定義する．

第1節 抽象的ネットワークモデルの定義

ネットワークは以下の2つのオブジェクトで構成される．

定義1（ポット）PTはフローの送信元または受信元となる装置，または複数の装置である．PTはポットIDを持つ．

定義2（フロー）FWはネットワーク上のサービスの双方向のデータの流れを表す．FWは（要求ポットID，提供ポットID，カラー，レベル）の4字組みで，それぞれの意味は以下の通りである．

要求ポットID：サービスを要求するポットのID

提供ポットID：サービスを提供するポットのID

カラー：提供するサービスを表す

レベル：最大トラフィック量（時間と量の対で表現）

最大トラフィック量　MAXT = { (t. l)| t:時刻，l:時刻tの最大トラフィック量 }

第 2 節　自己防衛型ネットワークモデルの定義

次に上記ネットワークモデルを用いて自己防衛型ネットワークを定義する．

（自己防衛型ネットワークとは）以下の異常を検知し，被害を広めないようにできるネットワークをいう．

異常1.　規定されていないフローが流れた

（ア）ポットへ規定されたフローと異なるフローが流れた

（イ）規定されたカラーと異なるカラーのフローが流れた

異常2.　ポット（またはフロー）が汚れた

異常3.　フローが指定されたレベルを超えた

ここで汚れるとは，一般的にみえればそのサービスのための許される通信データであるが，実際には悪意をもつオペレータやウィルスによって生成された通信データが流れているフローのことを示す．

第 3 章　自己防衛型ネットワークの設計

この章では簡単な例を用いて自己防衛型ネットワークの設計について説明する．

第 1 節　ネットワークの構成

例とするキャンパスネットワークは図3.1のとおりである．またそれぞれのコンピュータが要求または提供するサービスは表3.1にまとめてある．ここで持ち込みPCとは演習室に持ち込んで利用可能なPCのことである．

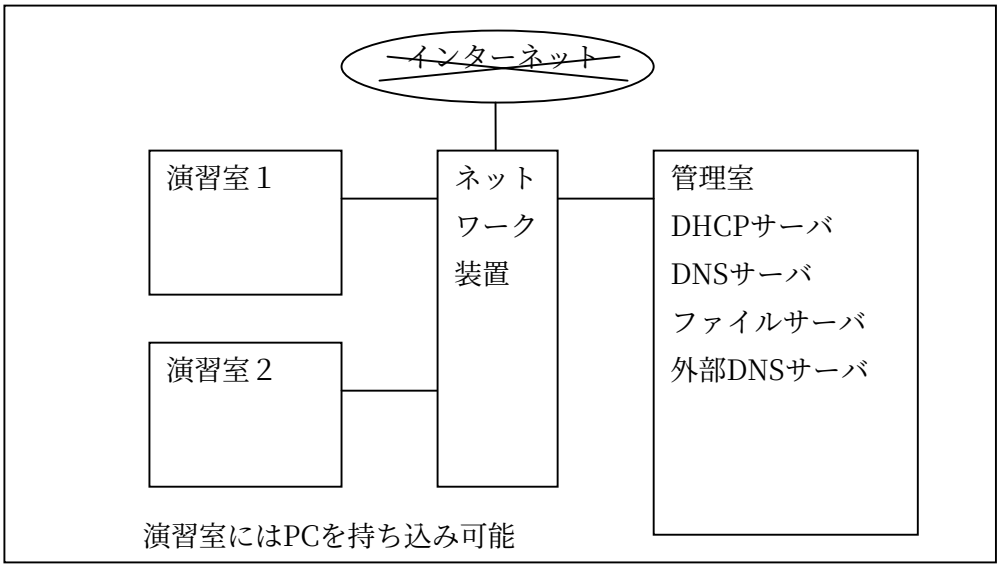

図3.1　ネットワーク構成図

設置場所又はPC	要求または提供するサービス
演習室１のPC	DHCPサービスを要求 DNSサービスを要求 ファイルサービスを要求 インターネットアクセスを要求
演習室２のPC	同上
持ち込みPC	DHCPサービスを要求 DNSサービスを要求 インターネットアクセスを要求
DHCPサーバ	DHCPサービスを提供
内部DNSサーバ	DNSサービスを提供および外部DNSに要求
ファイルサーバ	ファイルサービスを提供
外部DNSサーバ	DNSサービスを提供

表3.1　要求されるサービスリスト

第２節　抽象的ネットワークの構成

表3.1の情報から定義１と２を用いて抽象的ネットワークを構築する．最初にこのネットワークシステムで流れるフローを求め次にそのフローの送信元，受信元となるポットを求める．

第１項　フローを求める

構築するシステムで提供するサービスからフローを求める．表3.1から作成されるフローは表3.2のようになる．

要求または提供するサービス
FW（PT（演１），PT（DHCP），DHCP，＊） FW（PT（演１），PT（DNS），DNS，＊） FW（PT（演１），PT（ファイル），ファイル，＊）
FW（PT（演２），PT（DHCP），DHCP，＊） FW（PT（演２），PT（DNS），DNS，＊） FW（PT（演２），PT（ファイル），ファイル，＊）
FW（PT（持），PT（DHCP），DHCP，＊） FW（PT（持），PT（DNS），DNS，＊）
FW（PT（DNS），PT（外部DNS），DNS，＊）
注）本例では最大トラフィック量は設計において考慮しないので＊で表現

表3.2　フローリスト

第２項　ポットを求める

次の点に考慮してポットを求める．

●　全ての従事するフローが同じカラー，同じ相手とのフローである装置は同一のポットとする．

例えばこの例では，演習１と演習２は同じ内容のサービスを同じ相手と通信するので１つのポットとできる．

●　他のネットワークへの接続口は１つのポットとする．

例えばインターネットアクセスについては実際のネットワークでは他のネットワークとの接続口にあたるが，本設計手法ではこのような他のネットワークへの接続口も１つのポットとする．

以上により，演習１と２のフローをまとめ，PT（インターネット）を付加した最終のポットとフローを表3.3にまとめる．また，その構成は図3.2のようになる．この図で矢印はそれぞれのフローを表す（矢先がサービスの提供側）．

設置場所又はPC	要求または提供するサービス
PT（演）	FW（PT（演），PT（DHCP），DHCP，＊）
	FW（PT（演），PT（DNS），DNS，＊）
	FW（PT（演），PT（ファイル），ファイル，＊）
	FW（PT（演），PT（インターネット），ALL，＊）
PT（持）	FW（PT（持），PT（DHCP），DHCP，＊）
	FW（PT（持），PT（DNS），DNS，＊）
	FW（PT（持），PT（インターネット），ALL，＊）
PT（DHCP）	FW（PT（演），PT（DHCP），DHCP，＊）
	FW（PT（持），PT（DHCP），DHCP，＊）
PT（DNS）	FW（PT（演），PT（DNS），DNS，＊）
	FW（PT（持），PT（DNS），DNS，＊）
	FW（PT（DNS），PT（外部DNS），DNS，＊）
PT（ファイル）	FW（PT（演），PT（ファイル），ファイル，＊）
PT（外部DNS）	FW（PT（DNS），PT（外部DNS），DNS，＊）
PT（インターネット）	FW（PT（演），PT（インターネット），インターネット，＊）
	FW（PT（持），PT（インターネット），インターネット，＊）

表3.3　ポットとフローリスト

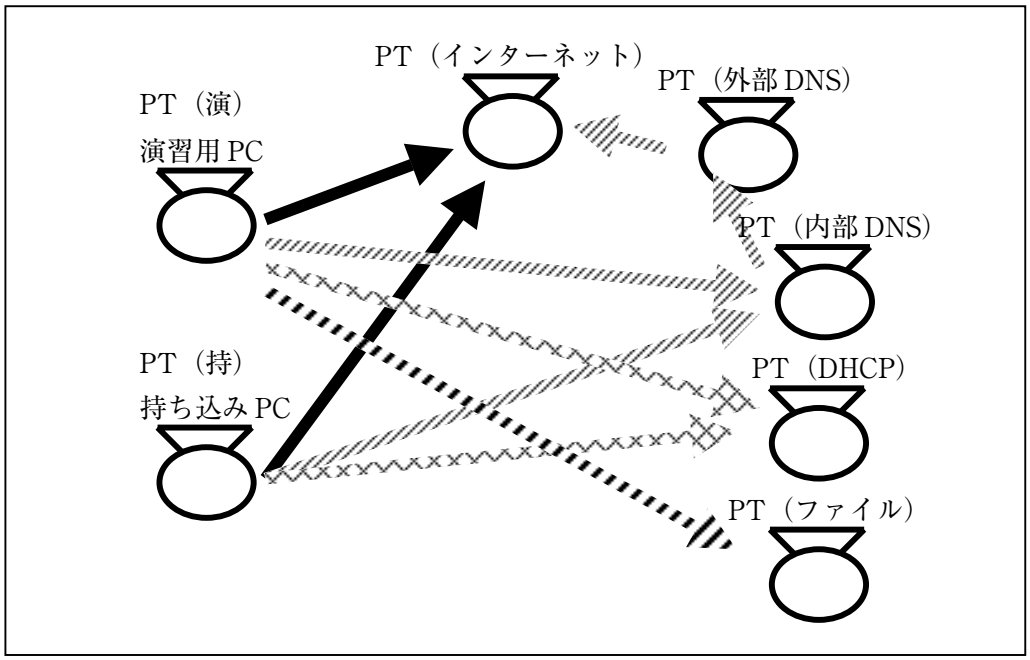

図3.2　各ポットとフローの関係図

第３節　自己防衛型ネットワーク化

次に２章で示した３つの異常を検知，対処するための１つの実装法を示す．

第１項　ポットの分割

抽象的なネットワークモデルでは，共通化できるポットは共通化した．しかし，実装の際に共通化すると不具合が生じる場合もあるだろう．例えばこの例では抽象的ネットワークモデルの設計時に演習室１と２を共通化したが，２つの演習室は距離が離れており，かつ，多くの演習用PCを配置するのでブロードキャストドメインを分割したほうがよいなどの理由が考えられる．
このような現実の実装を加味してポットを再編成する（今回は演習室に関しては同じでも差し支えないとし分割しない）．

第２項　VLANの分割

次に効率よく異常を検知するためのVLANの分割法を１つ紹介する．それはポット毎にVLANを分割しフローの流れる経路のみVLAN間をルーティングすることである．この例では図3.3のように７個のVLANに分割しそれぞれフローの経路どおりルーティングを許可する．これにより異常１（ア）の指定されていない宛先のフローが流れることを防止できる．他の異常については，

- 異常１（イ）：各VLANのパケットをモニターリングし規定されているサービス以外のパケットが流れれば異常とする．
- 異常：各VLANにIDS等を設置，パケットを監視する．
- 異常３：各VLANのトラフィックモニタを設置，フローに規定されたトラフィックを超えないか監視する．

このようにポット毎のVLANを設定することで効率良く異常を検出できる．

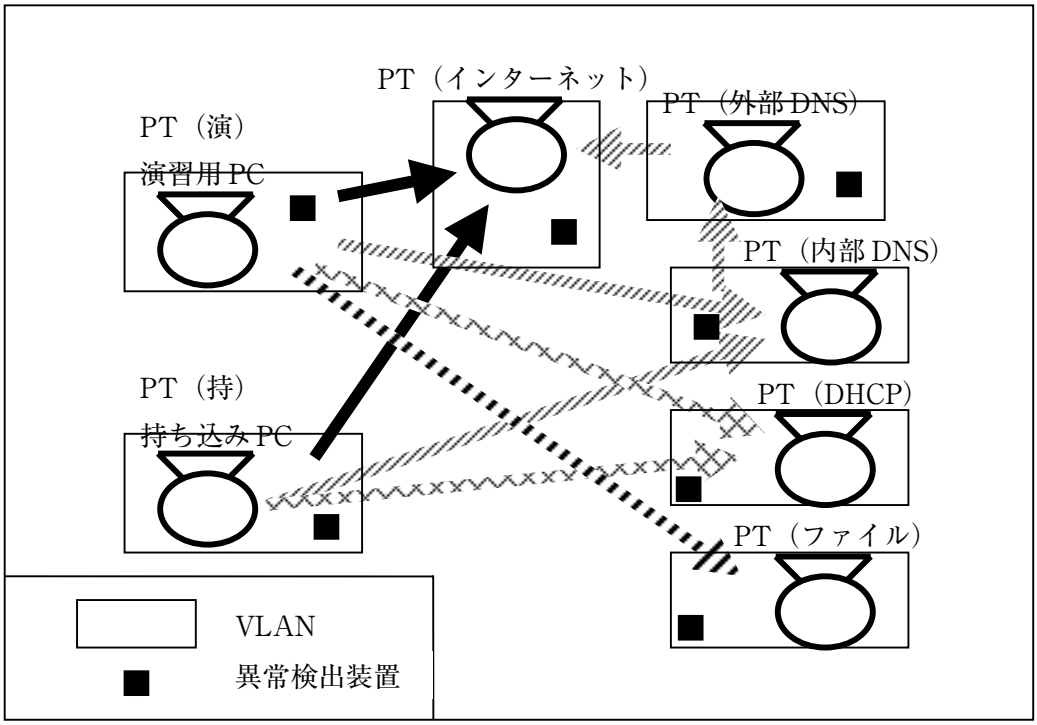

図3.3　VLANの設定例

第 3 項　ポットの隔離

異常の原因となるポットが見つかった場合，そのVLANのルーティングを停止すればいい．しかし，ポットはある装置のグループである場合がある（PT（演習）など）．この場合はそのポット内（VLAN内）で異常の元となる端末を検出しその端末を遮断する．

第 4 章　今後の課題

第 1 節　抽象的防衛オブジェクトの必要性

第 3 章で例として提示したネットワークは小規模なネットワークであった．より大規模なネットワークを設計するためには抽象的ネットワークからそのまま実装を考えるのではなく，設計した抽象的ネットワークにまず，抽象的な防衛オブジェクトを配置し，それからそれらの防衛オブジェクトと実際の製品機能と照らし合わせてVLAN等の設計を含めて具体的な設計を決める必要があると考えられる．抽象的ネットワークのための防衛オブジェクトは以下の 3 つが考えられる．

フローモニタ：フローの汚染を監視するオブジェクト

フローレベルメータ：フローのトラフィック量を監視するオブジェクト

ゲート：フローの流れを制御するオブジェクト

第 2 節　ポットの汚染について

ポットには汚れやすいポットと汚れにくいポットがある．例えばインターネットの出入り口にあたるポットはいつ汚れるかわからないし，アンチウィルスソフトがインストールされ，いつも人が触れないサーバ室のサーバをあらわすポットなどは汚れにくいだろう．このことからポットの汚れやすさ，または汚れに対してなんらかの基準が必要であるように思う．その基準に沿って防衛オブジェクトを配置し，実際の実装をおこなうことが必要であろう．

第 3 節　個人情報の漏洩について

今回提案した自己防衛型ネットワークでは個人情報の漏洩を防止するということは考慮されていない．例えばユーザが正規のルートでファイルサーバから個人情報の入ったファイルを入手しそれをリムーバブルメディアにコピーするような行為は本論で扱った自己防衛型ネットワークでは異常として検知されない．このように危機に関しては端末にユーザの操作を監視するようなソフトをインストールしコピー操作などを抑制することや，セキュリティ機能付のファイルサーバを利用するなどの対策が必要であろう．

第 5 章　おわりに

本論文では，大学研究・教育環境のための自己防衛型ネットワークを構築するために，まず，抽象的なネットワークモデルを定義し，そのモデルを用いて自己防衛型ネットワークを設計する 1 手法を示した．

今回の論文では小規模なネットワークを用いて設計法を展開したが，より具体的なシステムに本設計法を適用して自己防衛型ネットワークを構築すること，また，実際に自己防衛型ネットワークの異常検知のためには，どのようなセキュリティ装置をどのように配置すれば効率良くかつ確実にセキュリティが保てるのか考察してみたいと思う．

謝　辞

ネットワーク関連の資料を提供していただいたシスコシステムズ株式会社の早川浩平氏に感謝します．また，今まで，著者の研究に関わっていただいた帝塚山学院大学 人間文化学部の山本正樹教授をはじめとする全ての研究者に感謝します．そしてこの研究の機会を与えてくださった帝塚山学院大学 人間文化学部に感謝します．最後にいつも笑顔で見守ってくれている愛する妻と子に感謝します．

参考文献

[1] プロフェッショナルネットワーク 設計・分析・管理のすべて, 戸根勤, 株式会社 日本実業出版社

[2] マスタリングTCP／IP ネットワークデザイン編, Tony Kenyon著, 苅田幸雄監訳, 株式会社 オーム社

URL

[1] シスコシステムズ自己防衛ネットワークのページ
http://www.cisco.com/japanese/warp/public/3/jp/solution/netsol/security/sdn/

[2] シスコシステム自己防衛ネットワークの構築および事例のページ
http://www.cisco.com/japanese/warp/public/3/jp/solution/netsol/security/sdn/literature.shtml

注

1）本論文でいう自己防衛型ネットワークという言葉は一般的な“自己防衛”という意味で使用してる.