卒業論文　　2003年度(平成15年度)

イーサネットスイッチ間の情報共有による LAN内セキュリティ向上機構

指導教員

慶應義塾大学環境情報学部

徳田 英幸

村井　純

楠本 博之

中村　修

南　政樹

慶應義塾大学環境情報学部

佐川　昭宏

卒業論文要旨　　2003年度(平成15年度)

イーサネットスイッチ間の情報共有による LAN内セキュリティ向上機構

インターネットなど外部ネットワークから企業などの内部ネットワークに対する攻撃が増加し、情報の改竄や、管理者権限の奪取などさまざまな問題を引き起こしている。そこで、それらを防ぐファイアウォールや侵入検知システム (IDS) などの解決策が広く使われている。

しかしこれらの対策は内部ネットワーク内の攻撃を想定していないため、内部ネットワークにおいても安全性を向上させる必要がある。そこで、イーサネットスイッチに変更を加え、安全性を向上させる機構 Dynamic DeFense Switch (DDFS) を提案する。DDFS によって、この問題を解決し、より安全なネットワークを提供する。

慶應義塾大学 環境情報学部

佐川 昭宏

Abstract of Bachelor's Thesis

LAN Security Improvement System Using Infomation Sharing Between Ethernet Switches

Increasing computer security attacks from external networks like the Internet to internal local area networks (LAN) like office networks, lead to some problems such as falsification of information and loss of administrative right. There are some widely used defense systems against these attacks — firewall and an Intrusion Detection System (IDS). However, these defense systems do not assume any attacks between LAN hosts. We should pay attention to security for LAN and its hosts. We propose Dynamic DeFense Switch (DDFS) which improves existing LAN switches. DDFS solves the LAN security problems and realizes the more secure LAN.

Akihiro Sagawa

Faculty of Environmental Information
Keio University

目 次

図 目 次

表 目 次

第1章　序論

1.1　研究動機

インターネットに代表される情報通信技術の発展により、社内ネットワークや学内ネットワークなどの Local Area Network(LAN) が発達し、多くのホストが LAN に接続されている。数年前まで LAN がインターネットなど外部ネットワークに接続する機会は少なく、多くの場合一部のホストがダイアルアップによって断続的に接続するという使い方が一般的であった。しかしここ数年、ADSL や光ファイバに代表される高速でかつ安価なアクセス回線が普及したことにより、多くの環境で LAN がそのままルータやモデムを経由して常時インターネットに接続されるようになった。組織内の信頼できる人物が利用する LAN に比べ、インターネットには不正アクセスや脆弱性調査などの攻撃や、コンピュータウィルスが数多く存在する。インターネットへの常時接続は我々の利便性を向上させる反面、攻撃やコンピュータウィルスの接続機会を増加させることで我々のセキュリティを脅かす一因となっている。そこで多くの組織では LAN とインターネットの境界にファイアウォールと呼ばれる機構を導入し、インターネットから LAN への通信を制限・監視することで、セキュリティの確保に努めている。ファイアウォールによって、インターネットから行われる許可されない LAN 内のホストへの接続は拒絶されるため、LAN が攻撃を受ける余地はないと考えがちである。

しかしファイアウォールシステムは万能でなく、公開されたサービスの脆弱点や LAN 内部の人物がアクセスした Web ページ、電子メールなどを介して悪意ある攻撃やプログラムが LAN 内部に入り込む可能性がある。また最近では LAN 環境の変化により組織外部からの侵入路はインターネットに限らないといえる。例えば、IEEE 802.11a/b/g に代表される無線 LAN システムが盗用され建物外から LAN に組織外の端末が接続される例や、外部でコンピュータウィルスに感染した端末が組織に持ち込まれ LAN に接続される例が挙げられる。これら外部からの侵入路を経由し、LAN 内のホストが悪意あるプログラムを実行したり、攻撃を行う恐れがある。さらに、LAN に侵入した攻撃者やコンピュータウィルスは LAN を介し、インターネットからは直接到達できない

LANやホストに対して接続し、より機密性の高い情報の入手や改ざん、さらなる侵入ホストの確保、LAN構成の調査やネットワークの運用妨害などを行える。

LAN内部においてアクセスを制御・監視する方法として、LANに接続する個々のホストで対策する方法がある。ホストでの対策ではクライアントの認証を行うなどホストごとにきめ細やかな制限が可能である。だが、ホストごとに行う対策ではホストへの侵入や感染を防げても、コンピュータウィルスに感染したホストがネットワークに対し行う伝搬活動や、侵入したホストが他ホストに行う調査活動を防ぐことはできないという構造上の問題がある。また、ホストで対策を行えないネットワークプリンタのような機器やLAN内のホストを無条件に信用するような認証システムではアクセスを防げないという運用上の問題も多く存在する。

そこで本論文では既存のイーサネットスイッチや無線LAN基地局を置き換え、LAN内のセキュリティを向上させるDynamic DeFense Switch (DDFS)を提案する。通常のイーサネットスイッチや無線LAN基地局はOSI参照モデルの第2層で動作し、ホスト間の通信を中継する。しかしDDFSではフレームに含まれるIPアドレスやポート番号など上位層の情報を利用することで、ホスト間に存在するファイアウォールとして動作し、ホスト間の通信を制限・監視する。さらに他のDDFSと設定情報や動的に更新されるARPテーブルなどの情報を共有することでLAN全体の構成情報を入手し、単独のファイアウォールでは難しい偽造ARP応答の発見などを行い、セキュリティ向上を図る。

1.2 研究の目的および意義

情報通信技術の発展により、現在では非常に多くのLANがインターネットに接続されている。またインターネットのみならず、無線LANシステムや外部からの持ち込み端末など、LANと外部との接続点は多様化している。そのようなLANと外部の接続点を経由し、LAN内に悪意ある人物やプログラムが侵入した場合、不正アクセスやコンピュータウィルスの伝搬がLAN内部で行われ深刻な問題となっている。しかし、多くのLANではLANとインターネットの境界部もしくはホスト単位でのみしかアクセスを監視・制限していないため、LAN内で行われる活動を防ぐことは不可能である。

DDFSはイーサネットスイッチや無線LAN基地局に代わり、ホストのアクセスを中継・監視し、LAN内ホスト間の攻撃やコンピュータウィルスの伝搬を防止する。さらに、複数のDDFS間で情報を共有することでLANを対象に行われる攻撃を防止する。

その結果、コンピュータウィルスや不正アクセスに影響されにくいセキュリティ水準の高い LAN を構築できる。

1.3　本論文の構成

本論文は全 6 章で構成される。第 2 章では本論文の背景について述べ、LAN 内部で行われる攻撃・調査の例を挙げる。第 3 章では本論文に関連する研究、事例を述べる。第 4 章で本論文で提案する DDFS の設計と、DDFS を構成する各機能を詳説する。第 5 章では DDFS の評価を行い、第 6 章でまとめと今後の課題を述べる。

第2章　背景

本章では本研究の背景について説明する。

2.1　LANの問題点

従来のLANは組織内に存在するワークステーションなど固定ホスト同士が接続し、インターネットなど外部ネットワークへの接続はほとんど行われなかった。従って外部からLANに参加するには、最低限施設内への物理的侵入が必要であった。

しかし、今日のLANではデスクトップPCなどネットワークに固定して使うホストだけでなく、内部者が部外から持ち込んだラップトップの接続を許容し、インターネットをはじめとする外部ネットワークとLANが常時接続されている。さらに、IEEE 802.11a/b/gに代表される無線LANの普及により建物外でも電波が届く範囲内であれば機器に直接接続することなく、内部LANへ参加できる。また、ファイアウォールを通過したワームやトロイの木馬などによって利用者ホストの管理権限を奪い、外部の人物が内部ネットワークに参加することも可能である。

従来のLANに比べ、現在のLANでは外部の侵入者が以前より容易に侵入可能であるといえる。これらの手法によりLANに接続した悪意ある人物がLAN内のホストに対し、攻撃や調査を行いLANのセキュリティを脅かすと考えられる。

攻撃者が内部LANを対象として行う攻撃や調査の代表的手法として以下の3つが挙げられる。これらの攻撃や調査は利用者や管理者に気づかれることなく行えるという特徴がある。

- ARP応答の偽造による盗聴
- ブロードキャストフレームの解析
- コンピュータウィルスの伝搬

2.1.1　コンピュータウィルスの伝搬

一般に組織内部などの LAN では外部からのアクセスは境界のファイアウォールによって制限されることが多い。このため内部ホストでのアクセス制限は比較的緩く設定されていることが多く、ネットワークプリンタやセンサなどアクセス制限機能を持たない機器も存在する。

しかし、図 2.1 と図**??**に示すように MS-Blaster[5] や Nimda[3]、Slammer[4] に代表されるワームに感染したホストが組織内部に持ち込まれた場合、境界部の防御システムでは対処できない組織内部にワームが蔓延する可能性がある。さらに、攻撃者がトロイの木馬や無線 LAN を盗用し接続したホストを経由し情報収集活動を行った場合でも、同様に境界部の防御システムでは検知できないという問題がある。

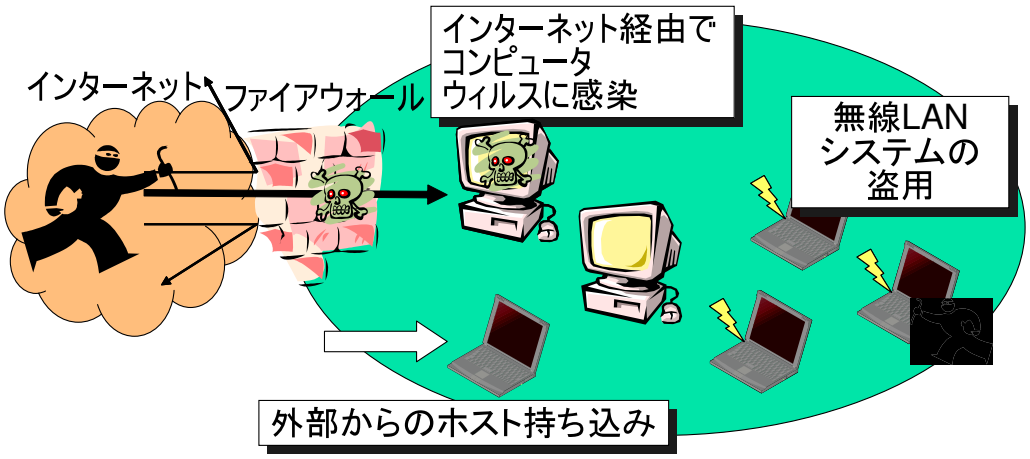

図 2.1: 現在の LAN

2.1.2　ブロードキャストフレームの解析

ブロードキャストフレームは、同一セグメント上のすべてのホストを対象として送出されるフレームである。主に、サービスを提供するノードの探索やノード自身の情報を通知するために使われる。イーサネットスイッチなどを介してブロードキャストフレームを受信したノードはフレーム内容を判断し、必要なければソフトウェア内でその内容を廃棄する。しかし、攻撃者が受信したブロードキャストフレームを廃棄せずに解析した場合、ホストやネットワーク構成を把握できる。

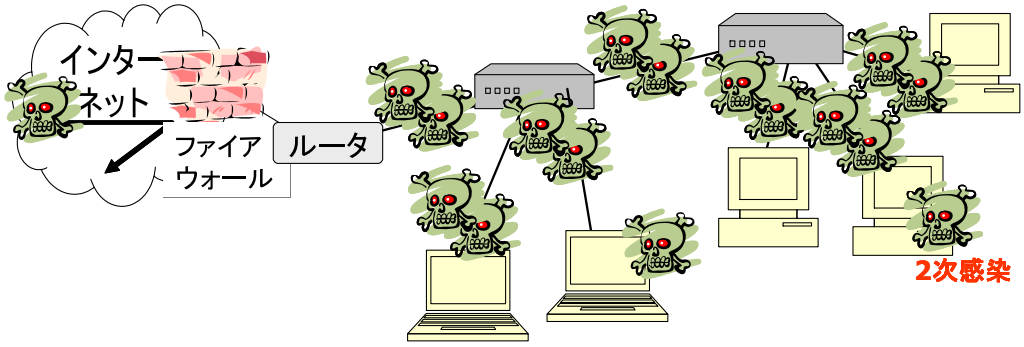

図 2.2: LAN 内部でワームが伝搬する

ブロードキャストフレームを使うプロトコルの多くは設定や構成によって抑止可能である。しかし、工場出荷時の初期設定では有効なことが多い。また、ブロードキャストはイーサネット上の様々なサービスで使われているため抑止することは現実的でない。

ブロードキャストを利用しサービスを探索するプロトコルの 1 つとして Dynamic Host Configration Protocol (DHCP) [6] が挙げられる。DHCP はホストに対し使用する IP アドレスや DNS サーバ、デフォルトルータアドレスなどホスト環境に必要となる設定値を伝達するプロトコルである。DHCP によって個別のネットワーク設定をする必要がなくなるため、情報コンセントを用いたオープンエリアのように端末が頻繁に入れ替わる環境や、多数の端末が存在するネットワークなど多くの環境で使われている。DHCP による設定は以下の流れで行われる。

1. DHCP による環境設定を要求する DHCP クライアントは、要求する 設定項目を列記した DHCPDISCOVER メッセージをブロードキャストし DHCP サーバを検索する。

2. DHCPDISCOVER メッセージを受け取ったすべての DHCP サーバは DHCPOFFER メッセージによってクライアントに DHCP サーバの存在をブロードキャストし、設定値を返答する。

3. DHCPOFFER メッセージを受け取った DHCP クライアントは応答のあった DHCP サーバを 1 つ選び DHCPREQUEST メッセージによって設定を要求する。

4. DHCPREQUEST メッセージを受け取ったサーバは設定値を調べ IP アドレス重複などの問題がなければ DHCPACK を送り設定を反映する。

DHCP サーバの存在するアドレスは要求を行うクライアントにとって未知であるため、クライアントから行われる DHCPDISCOVER ならびに DHCPREQUEST メッセージはブロードキャストを用いて行われる。攻撃者をはじめとする同一セグメント上のホストはこれらの通信を傍受し、解析することでクライアントホストの設定内容を知ることができる。攻撃者は DHCP サーバの存在を知ることで、設定の要求や以下に示すホスト詐称行為が可能である。

クライアントの詐称

DHCP サーバでは DHCPOFFER の送信元 MAC アドレスによって応答の有無や IP アドレスなどの設定値を変更できる。クライアントが DHCPOFFER メッセージを送信し、サーバが DHCPOFFER メッセージを応答した場合、クライアントの MAC アドレスは有効なアドレスとして DHCP サーバに登録されているといえる。攻撃者はこれらの通信を追跡し、DHCP が有効な MAC アドレスを収集できる。攻撃者は攻撃者ホストの MAC アドレスを記録したアドレスに変更することで、そのクライアントになりすまし、有効な設定値を取得できる。

DHCP サーバの詐称

攻撃者のホストに対しても、DHCPDISCOVER メッセージが送られてくるため、要求クライアントに対し攻撃者が用意した偽の DHCP サーバも応答できる。攻撃者の用意した偽の DHCP サーバは、要求クライアントに対し偽の構成情報を与える。偽の構成情報によって要求ホストのデフォルトルータを攻撃者のホストとし、攻撃者ホストが本来のホストに中継することで、送受信内容の盗聴が行える。また、偽の DNS サーバを指定することであるドメイン名に対して別の IP アドレスを返答し、ドメインを利用した利用者を別のホストに誘導できる。

2.1.3 ARP の詐称

Address Resolution Protocol (ARP) [10] は、ある IP アドレスに対応するデータリンク層の MAC アドレスを求めるために利用されるプロトコルである。ARP によって対象ノードの MAC アドレスを取得する手順は以下の通りである。

1. 対象ノードの MAC アドレスを取得するため、要求ホストは自身の IP アドレス

と MAC アドレス、対象ホストの IP アドレスを含んだブロードキャストフレームを送出する。(ARP 要求)

2. 同一セグメント上の全ホストはブロードキャストされた ARP 要求を受信する。各ホストは ARP 要求に含まれる対象ホストの IP アドレスが自身の IP アドレスと一致するか調査する。
   一致する場合は要求元の IP アドレス、MAC アドレスに加え、自身の IP アドレスと MAC アドレスを含んだパケットを生成し要求ホスト宛に送信する。(ARP 応答)
   一致しない場合、そのホストは応答せずパケットは破棄される。

3. ARP 応答を受け取ったノードはノードごとに管理されている「ARP テーブル」を更新し、IP アドレスと MAC アドレスの組み合わせを一定時間保存する。

しかし対象ノードとは異なるノードが、自身の MAC アドレスと対象ホスト IP アドレスを含んだ偽の ARP 応答を生成し、要求元に送付した場合、要求元は新たな応答を優先し、実際とは異なった IP アドレスと MAC アドレスの組み合わせを ARP テーブルに保存する。このため、対象 IP アドレス宛のパケットを別ノードに誘導できる。偽の ARP 応答を用いた攻撃の例として盗聴 (sniffing) や送信先アドレスのブロードキャスト化、サービス妨害 (Denial of Service, DoS) が挙げられる [12]。イーサネットスイッチによって他ホスト宛の通信が傍受できない環境であっても偽の ARP 応答を用いた誘導によって盗聴を行う様子を図 2.3 に示す。
(1) ノード A とノード B がイーサネットスイッチを介し通信を行っている。イーサネットスイッチを用いているためリピータハブと異なり、イーサネットスイッチに MAC アドレスが学習されている限りノード AB 間の通信は攻撃者であるノード C には到達せず傍受できない。
(2) ノード C がノード A とノード B に対し、ノード C の MAC アドレスを含んだ偽の ARP 応答を行うと、ノード A とノード B の ARP テーブルに誤った組み合わせが登録される。
(3) その結果、ノード A はノード C をノード B だと思い、ノード B はノード C をノード A だと思いパケットを送信する。したがってノード C は、ノード A、ノード B の送出するパケットを入手できる。この状態でノード C が誘導したパケットを正しい宛先に再送すると、存在を隠したまま通信内容を盗聴できる。

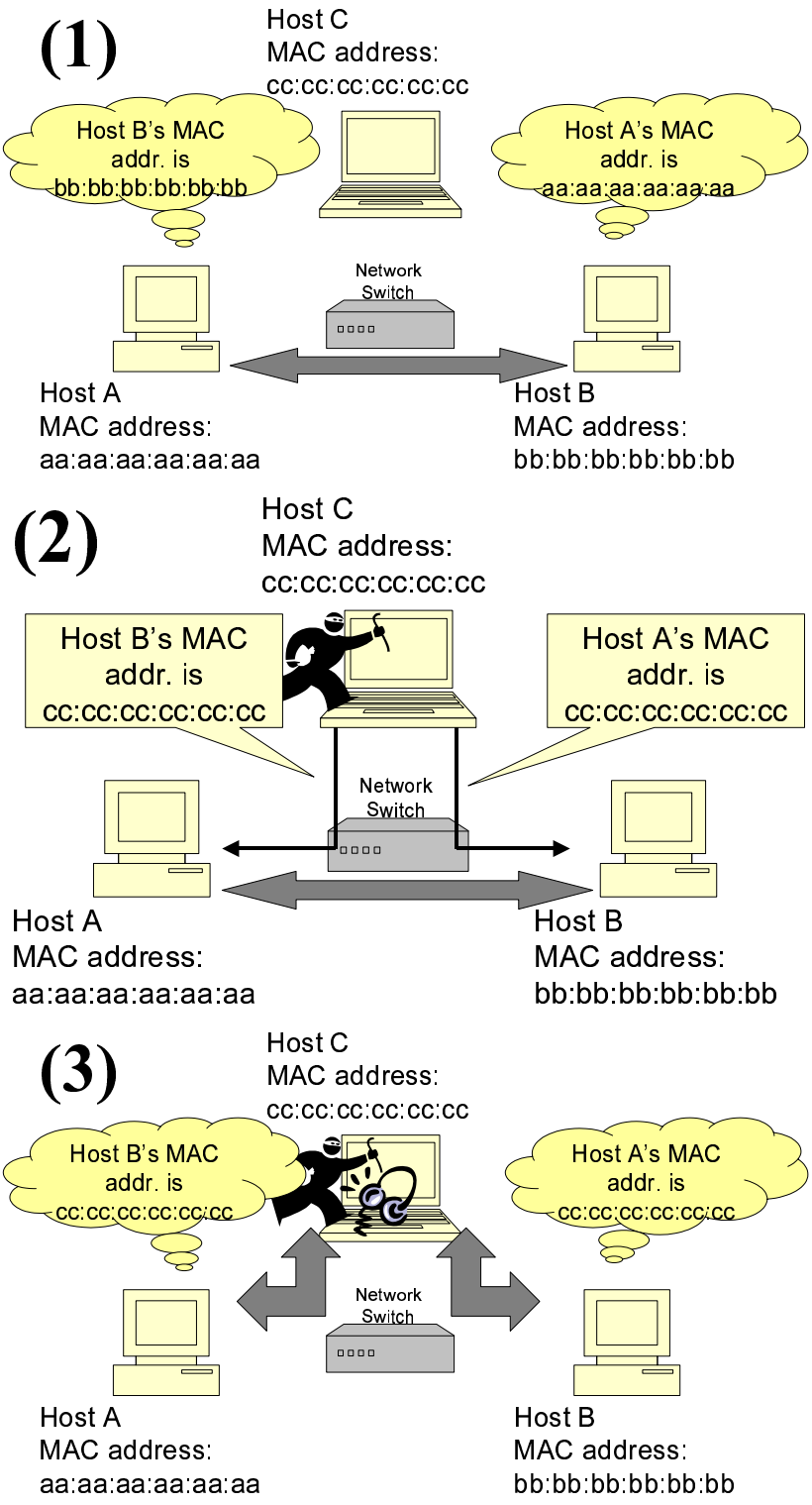

図 2.3: ARP 応答の偽造による盗聴例

第3章　関連する研究・事例

本章では、DDFS に類似した問題意識を扱った関連研究を紹介する。

3.1　個人向けファイアウォール

ノートンパーソナルファイアウォール [9] や ZoneAlarm[13] に代表される個人用ファイアウォール製品はクライアントホストに導入し、ホスト単位でのファイアウォールを実現するソフトウェアである。クライアントホスト上で動作することにより、所属するネットワークに依存しないアクセス制限や、アプリケーションごとなどの柔軟なアクセス制限が可能である。しかし、パーソナルファイアウォールでは導入済みのホストをワームなどの攻撃から防御できるが、未導入のホストやネットワークに行われる攻撃を防ぐことはできない、導入先の OS を選ぶという問題がある。また、ホストごとの導入が必要であるため不特定多数の端末が参加するキャンパスネットワークなどの環境には不向きである。これに対し、DDFS ではノード間で通信を監視遮断することで、ワームが行う攻撃を防御できる。また、DDFS 間で攻撃を行ったノードの情報などを共有することで、ネットワーク全体での防御ができる。

3.2　Distributed firewalls

Distributed Firewalls[2] はインターネットなど外部ネットワークとの境界に存在するファイアウォール機能をホストごとに分散させセポリシを配布し、ホスト上で対策を行う仕組みである。

ファイアウォールを複数のホストで分散動作させることにより単一故障点を排除しているが、前述の個人向けファイアウォール同様にネットワークや未導入のホストに対する攻撃を防げないという問題がある。

3.3 MACトレースバック

MACトレースバック [14] は、LAN内で行われた分散型サービス妨害攻撃ノードをダイジェストテーブルを用いて特定する機構である。従来のIPトレースバック技術 [11] では攻撃の行われたネットワークのルータまでしか特定できず、LAN内に存在するノードの特定までは行えなかった。MACトレースバック技術は、分散型サービス妨害(DDoS)を主眼とした防御法であるが、DDFSではファイアウォール機能を利用したアクセス制御や偽造ARP応答の防止、ブロードキャストフレームの伝搬防止など様々な攻撃に対処できる。

第4章　設計

本章では本論で提案するDDFSの設計について述べる。DDFSはOSI参照モデルの第2層(データリンク層)で動作するイーサネットスイッチや無線LAN基地局に代わってノード間の通信を中継・監視し、IPアドレスやポート番号などより上位層の情報をさらにDDFS間でARPテーブルや攻撃動向などの情報共有を図ることでセキュリティの高いLANを構築する機構である。

4.1　想定ネットワーク

DDFSの利用が想定されるLANを図4.1に示す。想定LAN環境ではイーサネットスイッチを中心とする有線LAN環境と無線LAN基地局を中心とする無線LAN環境が同一セグメントで接続している。想定LAN環境を構成するノードとしては、デスクトップPCやワークステーション、ネットワークプリンタ以外に情報コンセントや無線LANを経由して外部から持ち込んだラップトップPCやPDAなどが存在する。さらに、想定LAN環境からルータを経由してインターネットと常時接続されており、ファイアウォールによって外部ネットワークからの攻撃を防いでいる。

また、想定ネットワーク環境では以下の条件が成り立つと仮定する。

- 有線LAN環境上のすべてのノードはイーサネットスイッチ上のインタフェースに直接接続されており、ホストとイーサネットスイッチ間にはリピータやブリッジなど他の中継機器は存在しない。
- 無線LAN環境では無線LAN基地局を介してすべての通信が行われるインフラストラクチャモードにて通信が行われている。ただし、現在の無線LANの実装ではWEPを用いてデータリンク層で暗号化した場合でもクライアント間では共通のWEPキーが使われる。このためWEPを利用した場合でも他ホストが送受信するフレームを傍受し内容の解読できる問題がある。DDFSではこの問題は解決できないため、IPSec[8]によって上位層を暗号化するなど他の方法によって特

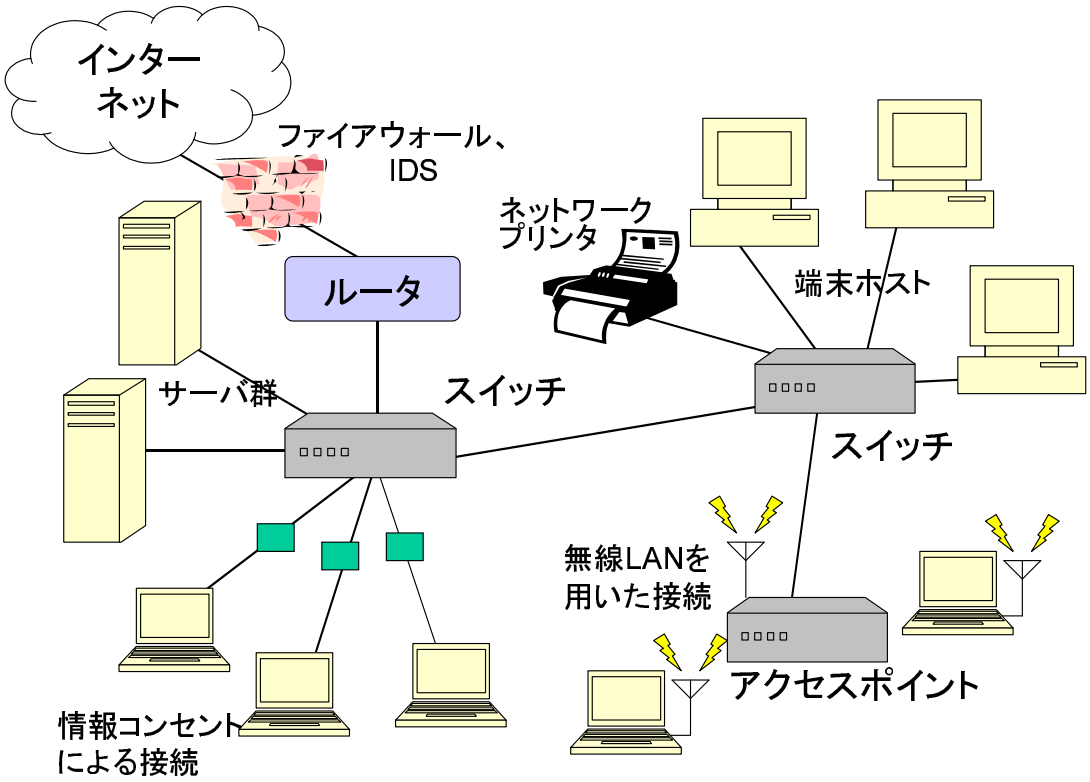

図 4.1: 想定 LAN 環境

定ホスト宛の通信は傍受が行えても解読できない対策が取られているとする。

DDFS で守られるネットワークは、上記想定環境中のイーサネットスイッチや無線 LAN 基地局を DDFS に置き換えることで実現される。

4.2 動作概要

DDFS は LAN 内でフレームの中継・監視を行う。また、DDFS 間の通信で中継・監視を行った情報を共有し、LAN 全体のセキュリティ向上に役立てる。図 4.2 に DDFS の概要を示す。DDFS が持つ機能を以下に挙げる。

- 連携機能
  DDFS 間でネットワークを構成し、定期的に情報の共有を図る。

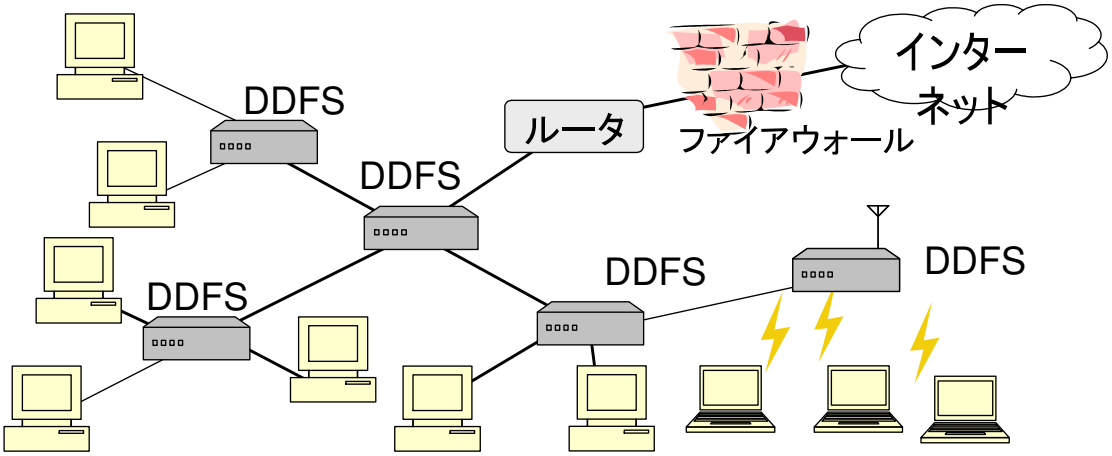

図 4.2: 現在の LAN

- ファイアウォール機能
  パケットフィルタリングや侵入検知防御システム (IDPS) によって攻撃を検知し、該当ホストを隔離する。
- フレーム転送機能
  上位の DDFS にフレームを転送し、ファイアウォール処理を行う。
- ブロードキャスト転送先限定機能
  すべてのポートにフレームを送出せずに一部のポートのみに送出する。
- 偽造 ARP 応答防止機能
  偽造された ARP 応答を検出し、廃棄する。

DDFS 内の各機能間の流れ、フレームの流れを図 4.3 に示す。

DDFS で守られたネットワークでは、ノード間の通信はすべて DDFS を経由して行われる。DDFS はノード間で行われるすべての通信を中継し、攻撃などの検知ができる。

4.2.1 連携機能

DDFS 間で情報共有を図るため、DDFS 間で階層構造を作成する。

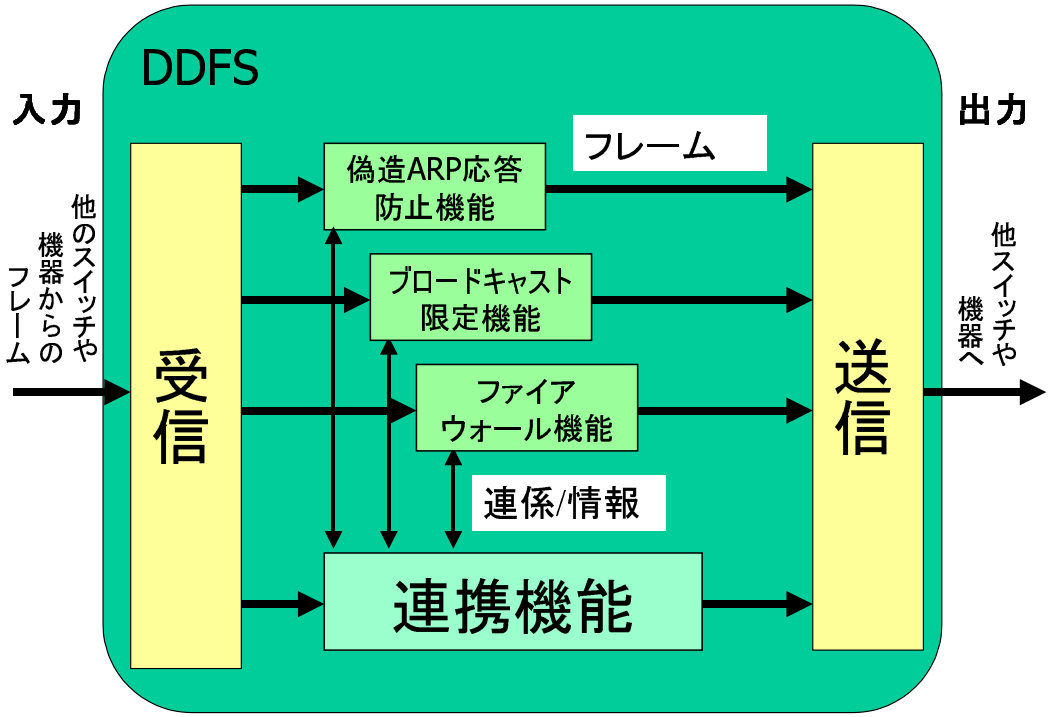

図 4.3: DDFS でのフレームの流れ

階層構造の構築

DDFS 間のネットワークは図 4.4 のように構築する。図 4.4 で示すように DDFS 間でネットワークを作成する。

1. 各 DDFS から定期的にフレームを送出し、木構造を作成。
2. 木構造の根に位置する DDFS — Root DDFS
3. Root DDFS が接続されたポート — Root port

連携情報の伝達

次に DDFS 間の連携を図 4.5 に示す。

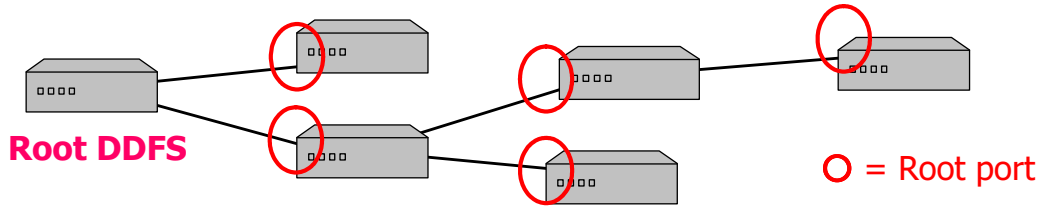

図 4.4: DDFS 間の構築

1. 各 DDFS は定期的にフレームを送出し、優先度に基づき Root DDFS を選出する
2. 各 DDFS は定期的にアドレス、ワーム検知回数などの情報を Root DDFS に送信する
3. Root DDFS は情報を併合し、下位の DDFS に宛てて送出する
4. Root DDFS からの情報を受信した DDFS は自身の情報を更新する

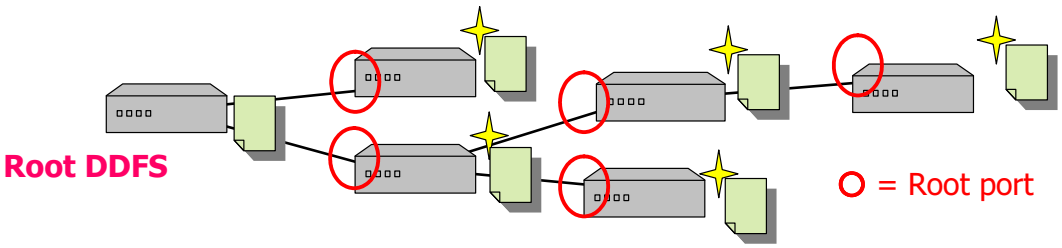

図 4.5: DDFS 間の連携

4.2.2 ファイアウォール機能

ファイアウォール機能では、DDFS 上でフレームに含まれる MAC アドレス、IP アドレス、TCP,UDP ポート番号などに基づいたパケットフィルタリングと既知の攻撃パターンを利用したコンテンツフィルタリングを行う。DDFS はパケットフィルタリングによって許可しないホストからの接続やホスト、サービスへの接続を遮断する。また、コンテンツフィルタリングによって既知の攻撃情報に一致するフレームを廃棄し、既知の脆弱性を狙ったワームの伝搬を防止する。

DDFS では制限したノードの情報を他の DDFS に伝達する。他の DDFS への伝達により、場所を変えながら繰り返し制限される接続を試みるノードを検知できる。さらに検知回数が閾値を超えた場合には、MAC アドレスを接続拒否リストに登録する。接続拒否リストを DDFS 間で共有することで、DDFS で守られたネットワークから対象ホストを隔離する。また、MAC アドレスでの制限によって DDFS 上で動作するコンテンツフィルタリングによる負荷の軽減が期待できる。

図 4.6 に、本機能を用いた DDFS 間の連携によるワームの伝搬阻止を示す。(1) 感染ホストが LAN に接続すると伝送路を経由してワームの伝搬活動が行われる。(2) 感染ホストが接続した DDFS はワームの伝搬活動を検知し、それらのフレームを廃棄する。(3) また、感染ホストが接続した DDFS は Root DDFS に向けて、感染ホストの MAC アドレスや情報を送信する。Root DDFS は、それらの情報を他の DDFS に送信し、感染ホストの情報はネットワーク上の全 DDFS に伝達される。(4) その結果感染ホストが移動し、他のスイッチを使った場合でも、(5) 感染ホストの MAC アドレスが接続した DDFS に登録されており、他のホストへの通信を遮断するため、他のホストへの接続を行えない。

4.2.3　フレーム転送機能

LAN 内で伝搬するワームや既知の脆弱点を狙った攻撃から LAN 内のホストを守るために、LAN 上のすべてのイーサネットスイッチや無線 LAN 基地局が、フレームを再構築し検査を行うコンテンツフィルタリング機能を持つことが望まれる。しかし、コストやシステムプロセッサ処理能力などからイーサネットスイッチ、無線 LAN 基地局ごとにファイアウォール機能を組み込むことは難しい。

そこで、DDFS では処理能力の低い機器を中継するフレームを一度上位のファイアウォール機能を持った DDFS に転送しファイアウォール処理を行うフレーム転送機能を定義する。フレーム転送機能によって処理能力の低い機器のみを介して行われる通信でもファイアウォール機能の恩恵を享受でき、より安全性の高い通信が行える。

4.2.4　ブロードキャスト転送先限定機能

2.1.2 節で述べたようにブロードキャストフレームはすべてのノードを対象に送出されるため、攻撃者もそのフレームを傍受・解析できるという問題がある。しかし、ブ

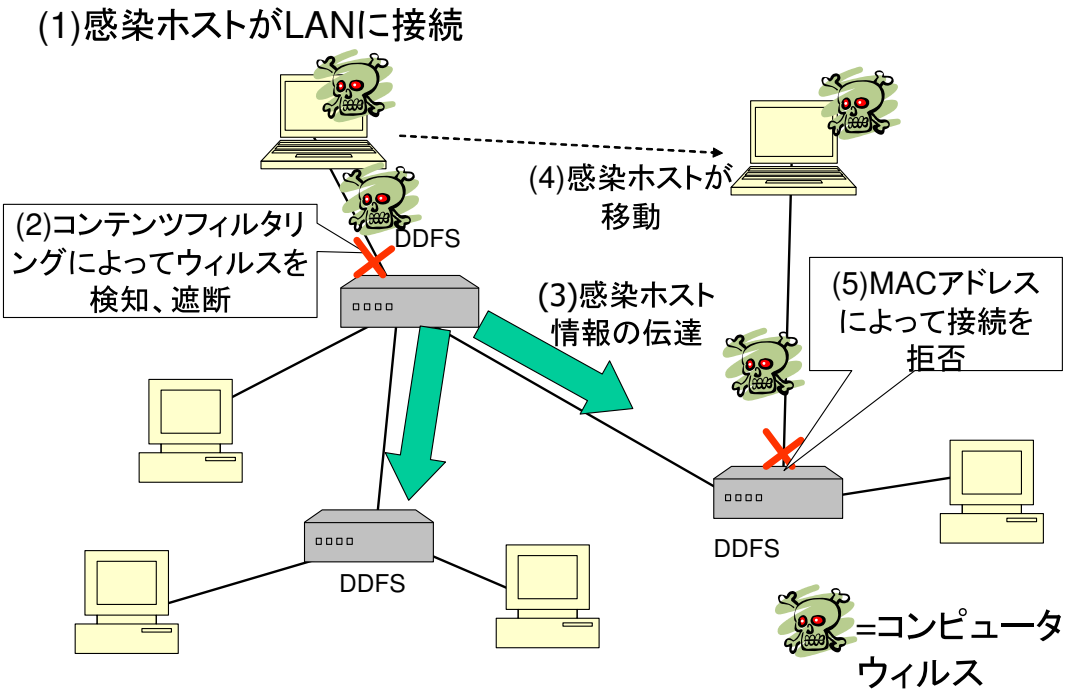

図 4.6: ファイアウォール機能の連携

ロードキャストはイーサネット上の様々なサービスで使われているため抑止することは現実的でない。

そこで DDFS ではサービス提供ノードを探索するためのブロードキャストフレームの転送先をサービス提供者のみに制限し、この問題を部分的に解決する。DDFS が受信したブロードキャストフレームがサービス提供ノード探索を目的とする DHCP などであった場合に、DDFS の連携機能で得た DHCP サーバの位置するインタフェースのみにフレームを転送する。ブロードキャストフレームの転送先をサービスが提供されているインタフェースに限定することで、他のノードにはホスト探索を目的とするブロードキャストフレームが送られなくなる。ブロードキャストフレームの現象によって攻撃者の傍受・解析機会を減少できる。

DDFS を用いて DHCP クライアントが DHCP サーバにアドレスを要求する様子を図 4.7 に示す。まず、左下のホストが DHCP サーバに DHCPDISCOVER メッセージを送信す

る。DHCP クライアントが接続された DDFS はフレームを受信した際に DHCP パケットと検知すると、DDFS はこのフレームをスイッチにつながる全インタフェースから送出するのではなく、DHCP サーバの接続された上流 DDFS にのみ限定して送信する。上流 DDFS は同様に転送先を DHCP サーバのつながるインタフェースに限定して送信する。この振る舞いにより、クライアントから送信される DHCP メッセージの傍受を防止できる。

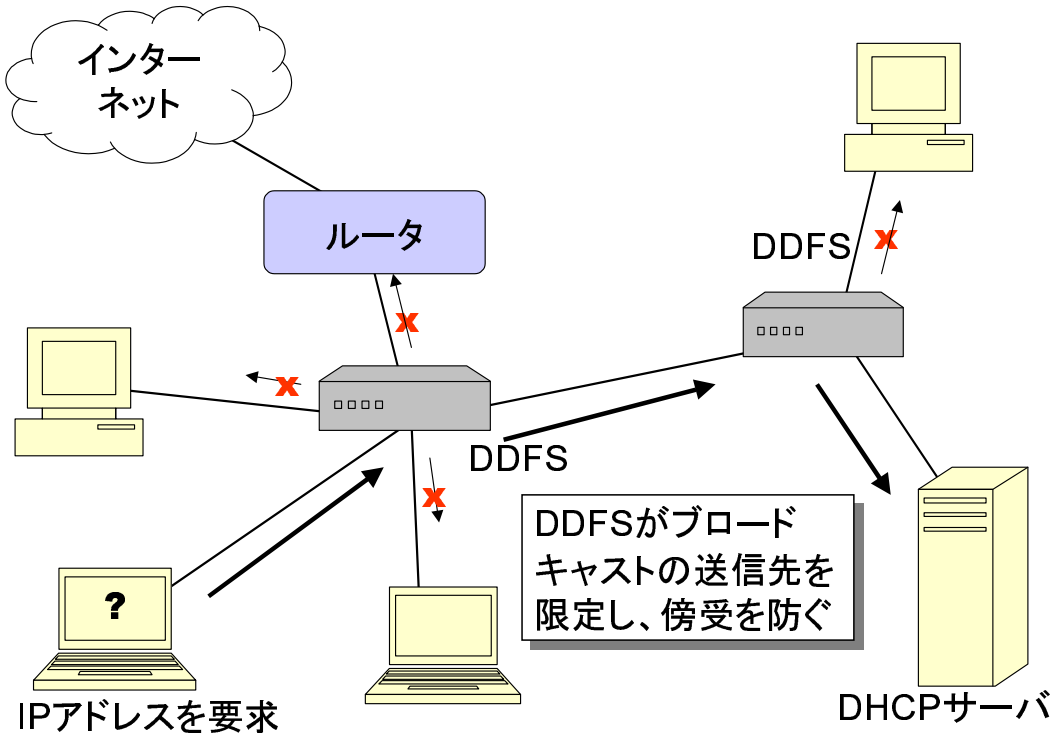

図 4.7: DDFS による DHCP パケットの限定

4.2.5　偽造 ARP 応答防止機能

DDFS ではある MAC アドレスに対応する IP アドレスは 1 つ

DDFS の偽造 ARP 応答防止機能では、フレームを転送する際に送信元の MAC アドレスと IP アドレス、転送元インタフェースを ARP テーブルに記録する。

DDFS が ARP 応答を受信すると ARP テーブルを検索し、ARP 応答に含まれる IP アドレス、MAC アドレス、到着インタフェースの対応が正しいかを確認する。IP アドレスの登録が確認されたにもかかわらず、MAC アドレス、接続インタフェースが異なる場合、当該 ARP 応答は偽造されていると判断しフレームを廃棄する。

各 DDFS は保持している ARP テーブルを連携機能によって定期的に Root DDFS に送信する。Root DDFS では各 DDFS から送られた ARP テーブルを併合し、送信元の DDFS に配信する。各 DDFS は配信された ARP テーブルから現状の ARP テーブルを更新する。

第5章　評価

本章では、これまで述べてきたDDFSについて本機構の有用性を検討するために行った3章で取り上げたパーソナルファイアウォール、MACトレースバックとの定性評価および予備実験について述べる。

5.1　既存研究との比較

既存研究との比較として、LAN内のセキュリティ向上が可能であるか以下の点について行った。

- 導入コスト
  導入にあたり管理者に求められる労力
- オーバーヘッド
  運用時にLANに対して負荷をかけるか
- 汎用性
  様々な攻撃に対処可能か
- 監視範囲
  当該機構で監視を行える範囲

表5.1に比較結果を示す。

導入コストという点では、パーソナルファイアウォールはホストごとの導入が必要であるため、管理者に対する負荷が高い。また、DDFSはイーサネットスイッチ、無線LAN基地局の置き換えが必要となるため、パーソナルファイアウォールほどではないものの、導入に対するコストは高いと考えられる。

ネットワークに対するオーバヘッドという観点では、DDFSが情報共有のため、MACトレースバックはブリッジMIBに対するアクセスのために帯域を消費するため若干のオーバヘッドが生じる。一方パーソナルファイアウォールは、情報の共有や他のノー

表 5.1: DDFS と既存研究との比較

	パーソナル ファイアウォール	MAC トレースバック	DDFS
導入コスト	×	○	△
オーバヘッド	◎	○	△
汎用性	○	△	◎
監視範囲	×	○	○

ドに対するアクセスを行わないため、ネットワークに対するオーバヘッドは少ないといえる。

汎用性という点では、MAC トレースバックが DDoS に特化した対策であるのに対し、パーソナルファイアウォールや DDFS はパケットフィルタリングによって様々な攻撃を防げる。さらに DDFS では連携機能や偽造 ARP 応答防止機能、ブロードキャスト転送先防止機能により数多くの攻撃に対処可能である。

監視範囲では、パーソナルファイアウォールは監視する範囲がインストールされたホストに限られる。一方、DDFS や MAC トレースバック技術では LAN 内全体を対象とすることができ、パーソナルファイアウォールでは防ぐことのできないネットワークに対する攻撃も防ぐことができる。

以上の比較から、本論文で提案する DDFS は他の手法に比べ LAN 内のセキュリティ向上に有効であることを示すことができた。

5.2 実験ネットワークにおけるパケットの受信・解析

本実験の内容は、あるネットワーク構成の調査を目的とし、端末にてネットワークを流れるブロードキャストパケットを受信し、その内容解析から構成を把握するという内容である。

実験対象となるネットワークとしてキャンパス内の研究ネットワーク (ネットマスクが 255.255.254.0 のネットワーク) を利用した。また、パケットの受信・解析には FreeBSD 上で動作する Ethereal[7] を用いた。

調査時間を 1 時間とし、午前 2 時 10 分から午前 3 時 10 分にかけて計測を行った。その結果、4325 パケットのブロードキャストフレームを受信した。受信したフレーム数

の内訳を図 5.1 に示す。

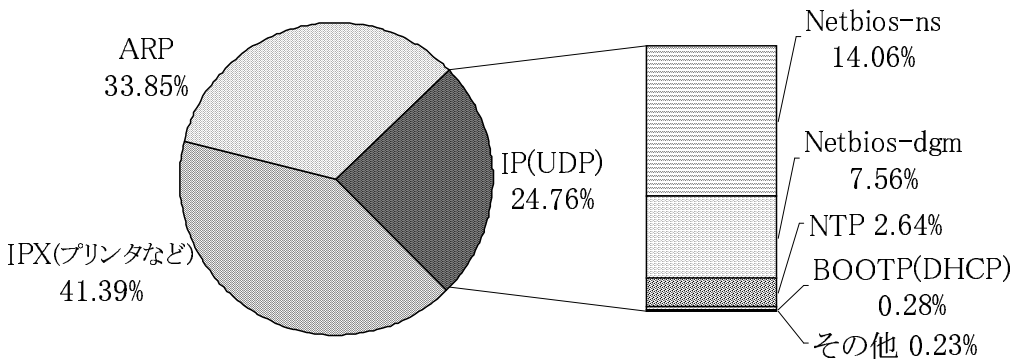

図 5.1: 受信したブロードキャストフレームの内訳 (N=4325)

受信フレームを解析することで以下の情報を得た。

- MAC アドレスの調査から、対象ネットワークには少なくとも 68 ホストが存在する。
- MAC アドレス中の先頭 3 バイトで構成される OUI(ベンダコード) の調査から、PC/AT 互換機以外に、Sun Microsystems 社製のホストや Apple Computer 社製のホスト、ネットワークプリンタが存在することが伺える。
- ARP 要求パケットの観察からあるホストは EtherLeak[1] の問題を抱えたドライバを利用していることがわかる。
- 多数の NetBIOS over TCP/IP のパケットが受信されていることから、多くの Windows ホストが稼働するネットワークと推測される。
- NetBIOS によってそれぞれの IP アドレスとホスト名の対応付けができる。
- DHCP パケットを受信したため、ネットワーク内には DHCP サーバが存在する。

この実験によって、内部ネットワークではブロードキャストが多用され、多くの情報を攻撃者に与えることが確認できた。情報が入手されることを防ぐためにブロードキャストを防ぐことも有用だが、ブロードキャストの全く使えないネットワークは、クライアントの多い内部ネットワークに適さない。DDFS のブロードキャスト制限機能では不用意なブロードキャストの伝搬を防ぎ、ネットワークに接続した攻撃者に多くの情報を与えない環境を提供する。

第6章　まとめ

6.1　まとめ

本論文では、LAN 内ホスト間の攻撃やウィルス伝達を防ぎ、連携によってセキュリティ向上を図るイーサネットスイッチを提案した。

ファイアウォールを通過したメールや外部からのノード持ち込みを経由して引き起こされる事例を例に LAN 内部でのセキュリティ対策の必要性を論じた。

LAN を対象とした既存のセキュリティ技術や研究を取り上げ、DDFS の設計を行った。さらに設計を行った DDFS の定性評価を行い、本論文で提案する DDFS が他の手法に比べ LAN 内のセキュリティ向上に有用であることを示した。

6.2　今後の課題

本節では、以上を踏まえて今後の課題と展望について述べる。

6.2.1　セキュリティ

現在 DDFS は接続する DDFS を信頼し、情報の共有を図っている。しかし、DDFS が共有する情報は LAN 内セキュリティに密接に関係する。偽の DDFS によって誤った情報が共有された場合正規ホストが接続できないなどの問題が生じる。従って、DDFS 間で認証や暗号化を行うなど DDFS 間でセキュリティを確立する必要がある。

6.2.2　情報共有の頻度

DDFS 間で行われる情報共有の頻度として、どの程度の間隔が最適であるか検討する。

謝辞

本研究を進めるにあたり、御指導を頂きました慶應義塾大学環境情報学部教授徳田英幸博士に深く感謝致します。

間 博人氏、斉藤 匡人氏、高橋 ひとみ氏、峰松 美佳氏、滝澤 允氏をはじめとする慶應義塾大学徳田研究室 ECN グループの諸氏また徳田・村井・楠本・中村・南研究室の方々には、研究会の活動を通じて数多くの御意見、御助言を頂きましたこと拝謝します。

最後に私の研究を陰ながら支えてくれた両親と、研究の日々を共に過ごした多くの友人に感謝し、謝辞と致します。

2003 年 12 月 29 日

佐川 昭宏

参考文献

[1] Ofir Arkin and Josh Anderson. @Snake, Inc. Security Advisory, EtherLeak: Ethernet frame padding information leakage, January 2003.

[2] Steven M. Bellovin. Distributed firewalls. *;login:*, Vol. 24, No. Security, November 1999.

[3] CERT Advisory CA-2001-26 Nimda Worm, September 2001. http://www.cert.org/advisories/CA-2001-26.html.

[4] CERT Advisory CA-2003-04 MS-SQL Server Worm, January 2003. http://www.cert.org/advisories/CA-2003-04.html.

[5] CERT Advisory CA-2003-20 W32/Blaster worm, August 2003. http://www.cert.org/advisories/CA-2003-20.html.

[6] Ralph Droms. *Dynamic Host Configuration Protocol*, March 1997. RFC 2131.

[7] Ethereal free network protocol analyzer for Unix and Windows. http://www.ethereal.com.

[8] Stephen Kent and Randall Atkinson. *Security Architecture for the Internet Protocol*, November 1998. RFC 2401.

[9] Norton Personal Firewall 2004, October 2003. http://www.symantec.com/region/jp/products/npf/.

[10] David C. Plummer. *Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Etherne t address for transmission on Ethernet hardware*, November 1982. RFC 826.

[11] A. C. Snoren, C. Partridge, L. A. Sanches, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Stayer. Hash-based ip traceback. In *SIGCOMM 01*, 2001.

[12] Sean Whalen. An Introduction to ARP Spoofing.
http://www.node99.org/projects/arpspoof/, April 2001.

[13] Zone Alarm 4.5, November 2003. http://www.zonelabs.com/store/content/home.jsp.

[14] 櫨山寛章, 大江将史, 門林雄基. ＭＡＣトレースバック：hash-based ip トレースバック拡張方式の提案. 研究報告 「高品質インターネット」, Vol. 004, , August 2002.