

不正パケット遮断システムのホスト特定機能の 工学部ネットワークへの適用

香川大学工学部信頼性情報システム工学科 卒 業 論 文	
卒 業 年 度	平成 年度 (年度)
指 導 教 員	

香川大学工学部 信頼性情報システム工学科

亀岡志帆

平成 22 年 2 月 9 日

Applying the host specific function of the injustice packet interception system to Campus Network.

Abstract Information protection is the important problem for an individual and an organization in networked society. However, personal and a confidential information flows out from users who have insufficient knowledge and malicious users, and the burdens of the network administrator increase now. In order to deal with the problem an injustice packet interception system using layer two switch (L2 switches) which intercepted the packet of the detected by Intrusion Detection System (IDS). In this study, aiming at being in use the packet interception system in campus network in the faculty of engineering, host identification function for blocking injustice packets is developed and applied to the network.

あらまし ネットワーク社会において情報保護は個人、および組織にとって重要な課題である。しかし現在、十分な知識をもたないユーザが意図しないで、あるいは悪意のあるユーザが意図的に個人情報や機密情報を流出させてしまう場合が増加し、ネットワーク管理者の負担も増大している。この問題に対処するため、侵入検知システム (IDS) を利用して特定したホストのパケットを遮断する、レイヤ 2 スイッチ (L2 スイッチ) を用いた不正パケット遮断システムの設計・開発を行ってきた。本研究では、不正パケット遮断システムを工学部ネットワークでの実用化することを目指し、遮断に至るまでのホスト特定機能を工学部ネットワークにおいて適用した。

キーワード 不正パケット, ホスト特定, IDS, SNMP, L2 スイッチ

目次

1	はじめに	1
2	ホスト特定機能の概要	3
2.1	不正パケット遮断システムの概要	3
2.2	SNMP	4
2.3	ARP テーブルによるホスト特定	5
2.4	DHCP ログによるホスト特定	7
2.5	ユーザ管理データベース	7
2.6	ポリシ	8
3	設計	9
3.1	開発環境	9
3.2	ユーザ管理データベース	10
3.3	機能	12
3.4	ホスト特定機能	12
3.5	ポリシ機能	15
3.5.1	警告メール送信タイミング	15
3.5.2	アラートレベルの決定	17
3.5.3	警告メール送信	19
4	実装と評価	21
4.1	実験環境	21
4.2	アラート情報抽出	21
4.3	ARP テーブルによるホスト及びポートの特定	22
4.4	ポリシ機能の動作	24
4.5	実ネットワークでの運用	25
5	おわりに	30
5.1	まとめ	30
5.2	今後の課題	30
	謝辞	32
	参考文献	33

第 1 章

はじめに

インターネットの普及に伴い、多くの場面で様々なユーザがインターネットを利用している。ユーザにはネットワークや通信などの知識が豊富な者もいるが、誰でも利用できるものとなった現在では知識の乏しいユーザが数多くいる。学校や会社のような組織的なネットワークにおいてもインターネットに接続されたコンピュータが多く、情報流出の危険性が常に付きまとう。組織における情報の重要性は明白だが、不正アクセスやコンピュータウィルスなどによって、個人情報や機密情報を流出させている場合も増加している。このような被害を防ぐため、あるいは早急に対処して影響を最小限に抑えるために、ネットワーク管理者に大きな負担がかかっている。

そこで、これらの問題を解決するため、これまで本研究室では侵入検知システム (IDS: Intrusion Detection System) を利用して不正パケットを送信したホストを特定し、Firewall とポート単位で制御を行うことができるレイヤ 2 スイッチ (L2 スイッチ) を組み合わせ、通信を遮断する不正パケット遮断システムの研究を行ってきた [1][2][3][4]。このシステムは IDS が不正パケットを検知すると、不正パケットを送信したホストを特定し、ホストの不正パケットの利用状況などからポリシー機能によって遮断レベルを決定し、Firewall と L2 スイッチのどちらで遮断を行うか、あるいは遮断を行わないかなどの判断を行い、それに従って自動的に処理を執行する。さらに、ポリシー機能ではユーザのセキュリティ意識を高めるため、不正パケットを発したことをメールなどにより連絡し、自覚を持たせセキュリティ対策に気を配るよう促す。また、管理者が不正ホスト情報の確認や、自動遮断もしくは解除が出来なかったホストに対する処理を、手動で行うためのインタフェースの開発も行われた。昨年度までに自動遮断・自動解除機能、ポリシー機能の実装までが行われてきたが、実用化には至っていない。

本研究では不正パケット遮断システムを工学部ネットワークで実用化することを目標とする。しかし、現在の工学部ネットワークの機能では全ての機能を実現できず、また実ネットワークで行った場合に手違いでシステムを止めてしまう可能性があるため、遮断に至るまでのホスト特定機能を工学部ネットワークに適用することにした。ポリシー機能と警告メール通知機能も実装している。

本論文では不正パケット遮断システムの概要と、工学部ネットワークにおけるホスト特定機能、運用ポリシーについて述べる。第 2 章で不正パケット遮断システムと、ホスト特定機能、ポリシーの概要について述べた後、第 3 章でホスト特定機能とポリシー機能の設計について述べ、第 4 章で実装および評価について述べていく。そして最後に第 5 章で結論と今後の課題について述べる。

第 2 章

ホスト特定機能の概要

本章では、不正パケット遮断システムの概要について述べた後、本研究におけるホスト特定機能の概要およびポリシー機能について述べる。

2.1 不正パケット遮断システムの概要

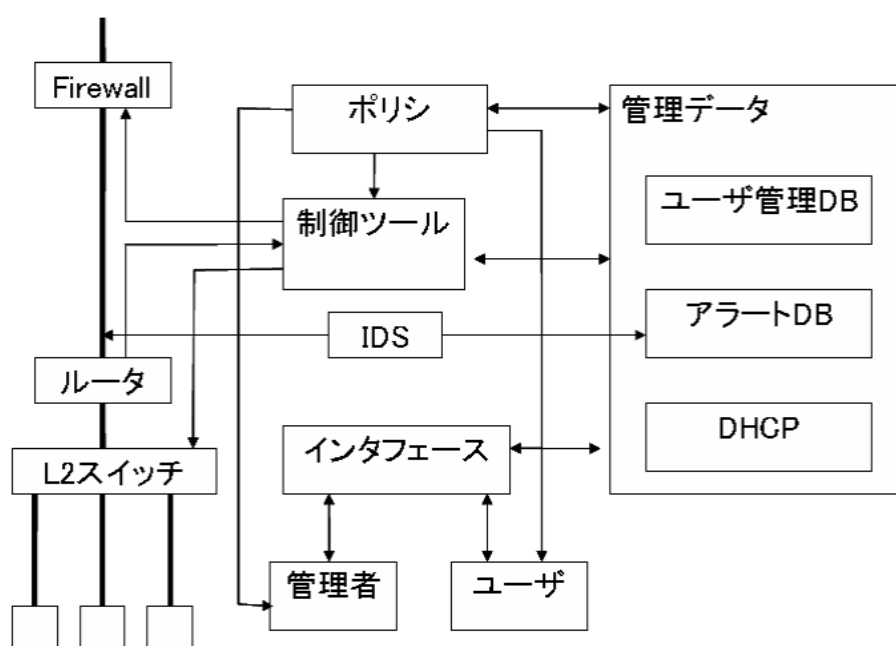


図 2.1: 不正パケット遮断システムの構成

不正パケット遮断システムの構成を図 2.1 に示す。ホストが不正パケットを送信あるいは受信すると、IDS が不正パケットを検知して情報をアラートデータベースに登録し、ポリシーに通知す

る。、それを合図にポリシーがアラートデータベースを参照し、不正ホストを特定すると、遮断レベルを決定し、Firewall か L2 スイッチのどちらで遮断を行うか、あるいは遮断を行わないかといった判断をする。そして制御ツールがポリシーの決定に従って Firewall か L2 スイッチを制御し不正ホストの自動遮断を行う。この遮断により組織内部からの情報流出を阻止する。スイッチの制御には MAC アドレス、不正ホストの接続しているスイッチとポート番号の情報が必要で、昨年度までの研究に用いられたスイッチには接続しているホストの MAC アドレスを自動的に FDB (Forwarding DataBase) に登録する機能があり、この FDB から目的の MAC アドレスを削除すれば通信の遮断が可能であった。その後、管理者と利用者に通知して、利用者には対策すべきことを示すことで復帰を早める手助けをし、また不正パケットを利用していたことを自覚させセキュリティへの意識の向上を促す。遮断後の通知には、ネットワークは使えないので、ユーザ管理データベースから携帯電話などの他のメールアドレスや電話番号を参照し、連絡する。何らかの理由で自動遮断に失敗した場合や、遮断を解除するとき、管理者はインタフェースから Firewall や L2 スイッチを制御する。また、ユーザもインタフェースを介して個人情報などをデータベースに登録する。

昨年度までに自動遮断・自動解除機能、ポリシー機能の実装まで行われているが、実用化にはまだ至っておらず、本研究では不正パケット遮断システムの実用化を目指し、その前段階である遮断に至るまでのホスト特定機能までを工学部ネットワークに適用することにした。また、ポリシー機能については実際のアラート情報に基づき設計しなおした。

なお、現在工学部では Firewall で P2P のパケットを検出し、検出されたときに管理者にアラートメールを送っている。本研究では IDS からのアラートの代わりに本アラートを用いる。

2.2 SNMP

本システムでは、利用したスイッチのポートの特定や ARP テーブルへの問い合わせを行うために SNMP (Simple Network Management Protocol) を使用する。SNMP とは、管理対象のホストやネットワーク機器に SNMP エージェントをインストールし、SNMP マネージャでそれらを管理するものである。エージェントとマネージャ間での情報の交換には MIB (Management Information Base) が用いられ、その情報 (オブジェクト) はツリー構造に階層化されて管理されている [5]。各オブジェクトは OID (Object IDentifire) と呼ばれる識別子で識別され、『.1.3.6.1.2.1』という OID は RFC1213 で規定されている MIB-2 サブツリーの構造であることを示す [6]。MIB-2 サブツリーの中には IP アドレスに関する情報をもつ ip サブツリーや、システム (SNMP エージェント) に関する情報をもつ system サブツリーなどがあり、各ツリーにはさらに下位の階層がある。

また、SNMP エージェントには、コミュニティ名が定義されている。これはエージェントとマネージャと通信するときのパスワードとしての役割を持ち、SNMP を用いて情報を参照するには、OID とコミュニティ名が必要となる。

エージェント問い合わせを行うために、本研究では、Linux マシンを管理サーバとして用い、Net-SNMP というパッケージで用いられている snmpwalk を用いる。snmpwalk では、コミュニティ名、問い合わせを行う SNMP エージェントの IP アドレス、OID を指定する。表 2.1 は、本システムで使用する OID である。

表 2.1: 本システムで使用する OID

OID	説明
.1.3.6.1.2.1.17.4.3.1.1	L2 スイッチに登録されている MAC アドレス
.1.3.6.1.2.1.17.4.3.1.2	L2 スイッチで使用しているポート番号
.1.3.6.1.2.1.4.22	ARP テーブル

2.3 ARP テーブルによるホスト特定

ポートや不正ホストを特定するためには、MAC アドレスが必要となる。しかし、管理者に送られるアラート情報には MAC アドレスは書かれていない。そのため、IP アドレスから MAC アドレスを取得しなければならない。本システムではその方法として、ルータの ARP テーブルの解析を行う。

ARP テーブルとは、IP アドレスと MAC アドレスの組をキャッシュしたものである。通信を行う際、IP アドレスは OSI 参照モデルの第 3 層で規定されるネットワークでのみ使用されるが、第 2 層で規定されるネットワークでは IP アドレスではなく MAC アドレスが使用される。そのため ARP を用いて IP アドレスから MAC アドレスを求めるのだが、毎回求めていては効率が悪いいため、これらの組み合わせをキャッシュしている。ARP テーブルのデータは通信を行っている間は消えることがない。その性質を利用して、本システムではルータの ARP テーブルを用いて IP アドレスから MAC アドレスを取得する。

ARP テーブルは、SNMP を用いて参照できる。snmpwalk を利用してルータに問い合わせを行うと、通信を行っているコンピュータの IP アドレスの一覧が表示される。grep コマンドを用いて目的の IP アドレスの情報のみを抽出すれば、図 2.2 のような形で結果が得られる。この結果は、133.92.146.0/24 のネットワークに接続されているルータの ARP テーブルから、133.92.146.194 を含むものを抽出したものである。

『IP-MIB::ipNetToMediaNetAddress.1460.133.92.146.194 = IpAddress: 133.92.146.194』では、IP アドレスが 133.92.146.194 の MIB ツリー下のアドレスが表示される。図 2.2 の通り、このアドレスには IP アドレスが含まれている。下位が同じ OID を保持しているものが、同一のコンピュータである。つまり、このとき IP アドレスが 133.92.146.194 のコンピュータの MAC アドレ


```
IP-MIB::ipNetToMediaIfIndex.1460.133.92.146.194 = INTEGER: 1460
IP-MIB::ipNetToMediaPhysAddress.1460.133.92.146.194 = STRING: 0:16:e3:17:7e:17
IP-MIB::ipNetToMediaNetAddress.1460.133.92.146.194 = IPAddress: 133.92.146.194
IP-MIB::ipNetToMediaType.1460.133.92.146.194 = INTEGER: dynamic(3)
```

図 2.2: ARP テーブルの問い合わせ結果

スは、『IP-MIB::ipNetToMediaPhysAddress.1460.133.92.146.194 = STRING: 0:16:e3:17:7e:17』で表されたので『0:16:e3:17:7e:17』となる。この情報が正しいことは、133.92.146.194 の IP アドレスを持つ Windows マシンのコマンドプロンプトでも確認できる (図 2.3)。

Ethernet adapter ワイヤレス ネットワーク接続:

```
Connection-specific DNS Suffix . : eng.kagawa-u.ac.jp
Description . . . . . : Atheros AR5005G Wireless Network Adapter
Physical Address. . . . . : 00-16-E3-17-7E-17
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 133.92.146.194
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 133.92.146.1
DHCP Server . . . . . : 133.92.167.20
DNS Servers . . . . . : 133.92.167.2
                        133.92.167.9
                        133.92.6.17
Lease Obtained. . . . . : 2010年1月22日 16:21:04
Lease Expires . . . . . : 2010年1月22日 17:01:04
```

図 2.3: コマンドプロンプトによる IP アドレスと MAC アドレスの確認

また、MAC アドレスが特定できたことによって、L2 スイッチの接続ポートの特定も行える。snmpwalk を利用して L2 スイッチに問い合わせる。表 2.1 に表した OID を用いて、L2 スイッチに登録されている MAC アドレスの一覧を見ると、接続されているスイッチなら、図 2.4 のように特定した MAC アドレスが確認できる。同じスイッチに、今度は L2 スイッチで使用しているポート番号を問い合わせると、図 2.5 のように出力される。ここで、参照している OID 以下の ID が一致するものが対応しているため、MAC アドレスによって L2 スイッチの接続しているポート番号も特定できる。

```

SNMPv2-SMI::mib-2.17.4.3.1.1.0.19.114.189.26.238.0 = Hex-STRING: 00 13 72 BD 1A EE
SNMPv2-SMI::mib-2.17.4.3.1.1.0.19.206.195.149.117.0 = Hex-STRING: 00 13 CE C3 95 75
SNMPv2-SMI::mib-2.17.4.3.1.1.0.20.81.167.174.74.0 = Hex-STRING: 00 14 51 A7 AE 4A
SNMPv2-SMI::mib-2.17.4.3.1.1.0.22.227.23.126.23.0 = Hex-STRING: 00 16 E3 17 7E 17
SNMPv2-SMI::mib-2.17.4.3.1.1.0.22.230.213.226.26.0 = Hex-STRING: 00 16 E6 D5 E2 1A
SNMPv2-SMI::mib-2.17.4.3.1.1.0.23.66.145.226.205.0 = Hex-STRING: 00 17 42 91 E2 CD
SNMPv2-SMI::mib-2.17.4.3.1.1.0.25.185.18.84.160.0 = Hex-STRING: 00 19 B9 12 54 A0

```

図 2.4: L2 スイッチへの MAC アドレスの問い合わせ結果

```

SNMPv2-SMI::mib-2.17.4.3.1.2.0.19.114.177.140.72.0 = INTEGER: 25
SNMPv2-SMI::mib-2.17.4.3.1.2.0.19.114.189.26.238.0 = INTEGER: 8
SNMPv2-SMI::mib-2.17.4.3.1.2.0.20.81.167.174.74.0 = INTEGER: 25
SNMPv2-SMI::mib-2.17.4.3.1.2.0.22.227.23.126.23.0 = INTEGER: 25
SNMPv2-SMI::mib-2.17.4.3.1.2.0.23.66.184.102.190.0 = INTEGER: 25
SNMPv2-SMI::mib-2.17.4.3.1.2.0.25.185.18.84.160.0 = INTEGER: 1
SNMPv2-SMI::mib-2.17.4.3.1.2.0.27.42.195.108.71.0 = INTEGER: 25

```

図 2.5: L2 スイッチへのポート番号の問い合わせ結果

2.4 DHCP ログによるホスト特定

本システムは、Firewall によるアラートメールを受信することを契機として動作する。そのため、不正パケットを検知した時、必ずしもリアルタイムでシステムが動作できるとは限らない。つまり、不正パケットを発信した後システムが動作するまでに通信を終了させてしまうと、通信を行っている IP アドレスと MAC アドレスの組み合わせを残すという ARP テーブルの性質上、ARP テーブルでは MAC アドレスが取得できないという事象が発生する。そこで、本システムでは ARP テーブルで MAC アドレスが取得できない場合、DHCP ログを利用する。

DHCP(Dynamic Host Configuration Protocol) とは、クライアントに対して IP アドレスやサブネットマスクなどの TCP/IP 関連の情報を自動的に割り当てるためのプロトコルで、DHCP サーバでは一般的に、IP アドレス以外のサブネットマスク、デフォルトゲートウェイといった TCP/IP 関連の情報も同時に保存され、クライアントに配布される。DHCP ログには、どの時間からどの時間まで、どの MAC アドレスにどんな IP アドレスを割り当てたかが記録されている。ログファイルは毎分作成されているので、不正パケットを検知した時刻のログファイルを調べれば、一致する IP アドレスと、それに対応する MAC アドレスが取得できる。

2.5 ユーザ管理データベース

ユーザ管理データベースにはユーザ情報テーブル、不正ホスト情報テーブル、ユーザ ID と MAC アドレスを管理するテーブルを用意する。

ユーザ情報テーブルでは、ユーザ ID とユーザや指導教員（上司）の連絡先等の個人情報を管理し、ユーザの環境に変化があれば、環境に応じて更新する必要がある。不正ホスト情報テーブルでは不正ホストの MAC アドレスや利用した不正パケットの情報、アラートレベルなどが管理される。ユーザ ID と MAC アドレスを管理するテーブルでは、他の情報とは異なり、それぞれ重複することも変化することもないユーザ ID と MAC アドレスの組み合わせを管理する。

2.6 ポリシ

ポリシ機能では、ホスト特定後、ホストにどのような対応をするかを決定する。不正パケットの使用状況に応じてアラートレベルを決定し、レベルに応じて使用停止を促す警告メールを送信したり指導教員に通知したりする。

アラートレベルの決定には、使用しているプロトコルの危険度、前回検知からの経過時間、検知回数などを考慮に入れる。プロトコルによってパケットの発信の仕方は異なり、短時間に何度も発信するものがあれば、そうでないものもある。しかし全ての不正パケットに対して警告メールを送信していれば、短時間に大量に不正パケットを発信するホストは、いずれ警告メールを無視してしまいかねない。ポリシ機能の目的は、警告によってホストに不正パケットを使用していることを自覚させることと、再度に亘る使用を防止させることである。

第 3 章

設計

3.1 開発環境

本システムは実ネットワークでの実用化を目的としている。そのため、本研究では工学部ネットワークをに適用するために必要な機能を開発する。本システムの構成を図 3.1 に示す。

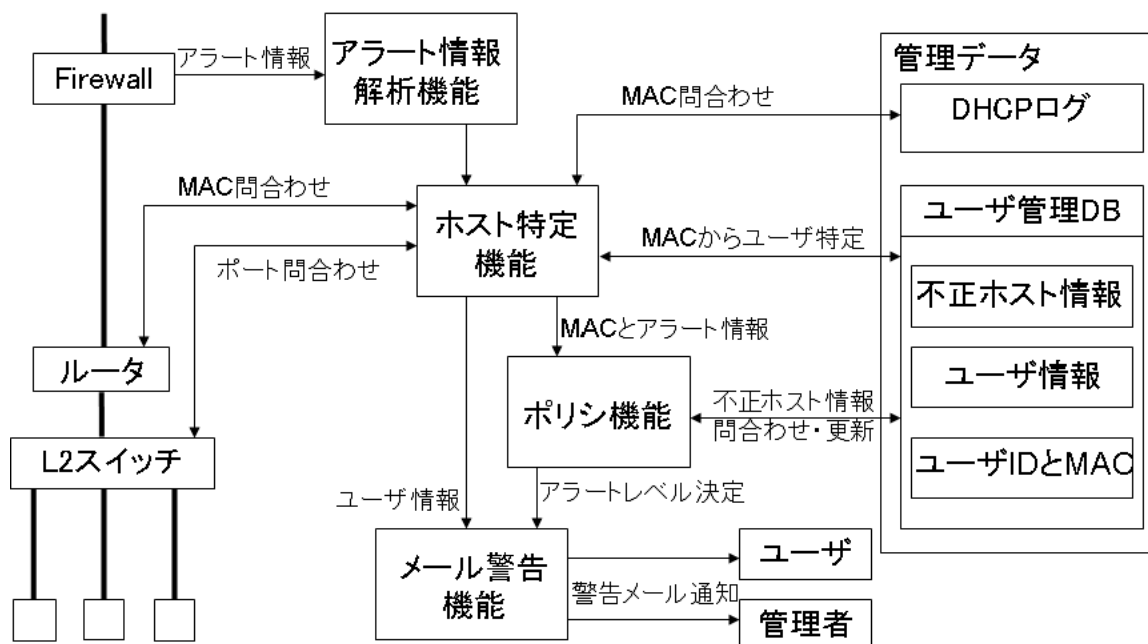


図 3.1: 本システムの構成

昨年度までの研究ではIDSを用いて不正パケットの検出を行っていたが、現在、工学部ネットワークではFirewallからアラートメールが管理者に送られてくるので、そのメールを用いてホス

ト特定を行う。スクリプトの記述には PHP を、データベースには PostgreSQL を使用し、システムの開発は CentOS 上で行う。

PHP (Hypertext Preprocessor) を用いた理由は、以下の通りである。Web サーバに置かれるソフトウェアの Apache モジュールとして動作するスクリプト言語をであり、動的な Web サイトの構築に適した言語である。Apache は多くの Web サーバに実装されているため、PHP を使用できるサーバが多いといえる。また、PHP は文字列処理が容易で、多様なデータベースとの接続も可能である。

3.2 ユーザ管理データベース

ユーザ管理データベースには、ユーザの連絡先等の個人情報を管理する `user_info` テーブル (表 3.1)、不正ホストの情報を管理する `host_info` テーブル (表 3.2)、ユーザ ID と MAC アドレスを管理する `uid_mac` テーブル (表 3.3) を用意する。

ユーザ情報テーブル (`user_info`) では、ユーザを識別するユーザ ID の他、不正パケット検知時に連絡するためのメールアドレス、研究等の目的で利用するため不正パケットと検知しないプロトコルを管理する。メールアドレスは、ユーザ本人への通知用、ユーザの指導教員 (もしくは上司)、さらに管理者へと通知するために登録する。このユーザ情報テーブル内の情報は、ユーザの環境の変化などによって更新の必要がある可能性があり、更新は全て手動で行うことになる。検知しないプロトコルの設定などを行うため情報更新は管理者による更新となるが、必要に応じてユーザ本人で更新できるインタフェースを用意することも可能である。

不正ホスト情報テーブル (`host_info`) では、ホストの MAC アドレスとプロトコル、不正パケットの初回検知時刻、不正パケットの最終検知時刻、検知回数、アラートレベルが保存される。このテーブルを利用して、不正パケットの利用頻度などを判断し、アラートレベルを判定する。不正ホスト情報テーブルは不正パケットを検知し、MAC アドレスを特定する度に更新する。

また、`uid_mac` テーブルでは、ユーザ毎のユーザ ID と MAC アドレスが管理される。このユーザ ID と MAC アドレスは他の情報とは異なり、それぞれ重複することも変化することもないため、システムによって更新することはない。そのため例えば学生であれば、入学時に予め登録しておき、卒業時に削除するといった操作を管理者が行う必要がある。この `uid_mac` テーブルには `user_info` テーブルと `host_info` テーブルを橋渡しする役目があり、不正ホストの MAC アドレスが特定できてもこの `uid_mac` テーブルに情報が無ければユーザへの連絡には至れない。

表 3.1: user_info テーブル

フィールド名	説明
uid	ユーザ ID
mail_add1	アラート通知用メールアドレス
mail_add2	
mail_add3	
proto1	使用を許可するプロトコル
proto2	
proto3	

表 3.2: host_info テーブル

フィールド名	説明
mac	MAC アドレス
alart_lv	アラートレベル
first_alart	初回検知日時
last_alart	最終検知日時
alart_num	検知回数
protocol	プロトコル

表 3.3: uid_mac テーブル

フィールド名	説明
uid	ユーザ ID
mac	MAC アドレス

3.3 機能

本システムにおける主な機能は以下のとおりである。

- 不正パケットに関するアラート情報の解析
- 不正ホストの特定
- ポリシ機能におけるアラートレベルの決定
- メールによる警告

アラート情報解析機能では、以降のホスト特定やアラートレベルの決定に必要な、不正パケットに関する情報を抽出する。アラート情報は Firewall によりメールでサーバに送られる。ここで抽出する情報は、不正パケット検知日時、プロトコル、発信者の IP アドレス、受信者の IP アドレスである。

ホスト特定機能では、アラート情報解析機能によって取り出した IP アドレスを利用し、不正ホストの MAC アドレスを特定する。リアルタイムに MAC アドレスが発見できた場合、使用している L2 スwitch のポート番号まで特定する。これによって、管理者が物理的な位置を知り、通信を遮断することも可能になる。

ポリシ機能では、アラート情報解析機能によって取り出した検知日時やプロトコル、またユーザ管理データベース中の不正パケット使用に関する情報からアラートレベルを決定する。前回検知からの時間間隔、検知回数、プロトコルのそれぞれにパラメタを持たせ、前回のアラートレベルも考慮に入れて決定する。

メール警告機能では、ポリシ機能によって決定されたアラートレベルに応じて、文面や送信相手を変化させたメール通知を行う。また、前回検知からの時間間隔や検知回数によって、送信するかどうかを判断する。

3.4 ホスト特定機能

アラート情報受信からホスト特定までの流れを図 3.2 に示す。

不正パケット情報はアラートメールとして図 3.3 のように管理者に送信されている。それをプログラムにフォワードし、システムは動作を開始する。アラートメール本文を読み込み、字句解析によって必要な情報を抽出する。ここで抽出する情報は、不正パケットを検知した日付、時刻、プロトコル、発信者の IP アドレス、受信者の IP アドレスの 5 つである。

ここで抽出した IP アドレスを元にルータの ARP テーブルへの問い合わせを行う。ARP テーブルにはその時接続されているコンピュータの IP アドレスと MAC アドレスの組がキャッシュされているので、接続が切られていると ARP テーブルには該当する IP アドレスは残らず、MAC

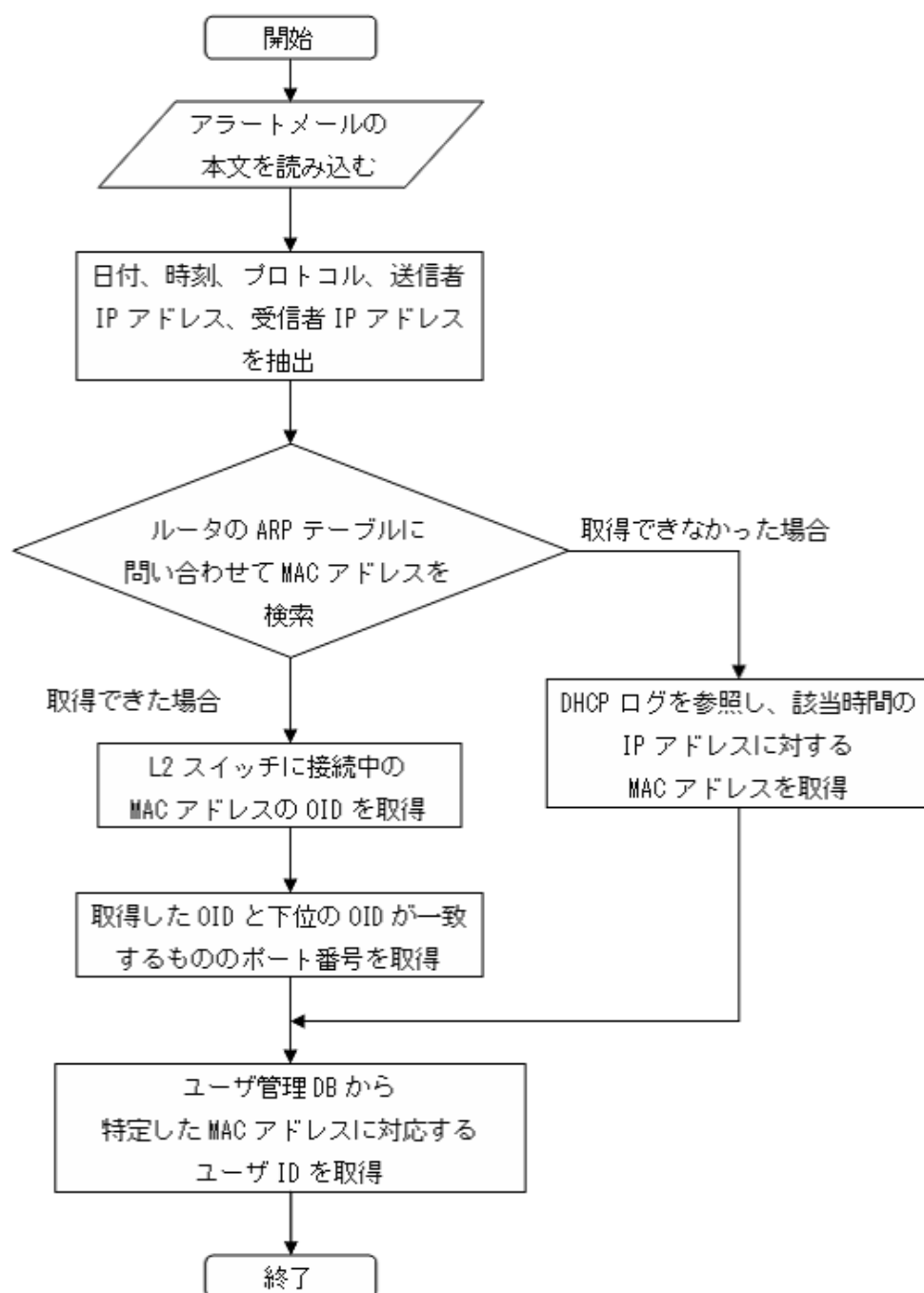


図 3.2: アラート情報取得からホスト特定までのフロー図

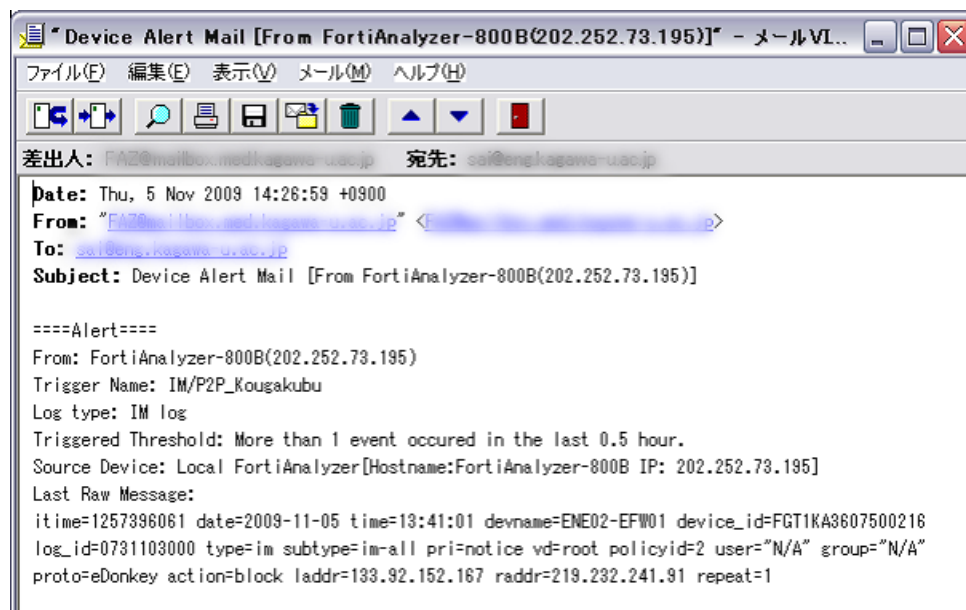


図 3.3: Firewall からのアラートメール

アドレスの取得には至れない。その場合、DHCP サーバのログファイルを参照する。DHCP のログには、どの MAC アドレスに対してどの IP アドレスを配布したか、またその開始日時と終了日時が記録されている。DHCP ログデータは毎分新しく生成され、その日時をファイル名の一部に持たせているので、参照するログファイルには不正パケットを検知した日時のファイルを用いればよい。

例えば 2010 年 1 月 12 日 13 時 33 分に IP アドレスが 133.92.146.142 で接続されていたコンピュータが現在 ARP テーブルで発見できないとき、『DHCPLOG.20100112133300』という DHCP ログファイルを参照し、grep コマンドを用いて IP アドレスを調べると、図 3.4 のような結果が得られ、MAC アドレスが『00-16-e3-17-7e-17』と特定できる。

```
[woodstock@snoopy ~]$ cat DHCPLOG/DHCPLOG.20100112133300 | grep "133.092.146.142"
2010/01/12 12:53:06 2010/01/12 13:33:06 133.092.146.142 00-16-e3-17-7e-17 06t226
```

図 3.4: DHCP ログによる MAC 特定

ARP テーブルから MAC アドレスが取得できた場合は、まだホストがネットワークに接続中なので、接続スイッチのポート番号まで得ることができる。スイッチ毎に持っている IP アドレスが異なるため、IP アドレスだけでもどこのスイッチを利用しているか大まかには分かるが、SNMP を利用することで接続ポートを特定すると、より細かい位置が特定できる。また、本システムでは前述の通り遮断は行わないが、L2 スイッチで遮断を行う場合、ポートの特定も必要となる。工

学部ネットワークでは多数のスイッチが利用されており、複数台のスイッチに接続していたり、スイッチ同士で接続していることもよくある。そのため可能性のある全てのスイッチのポートを調べる。ポートの特定では、最初にスイッチの FDB の MAC アドレス部分を SNMP を用いて参照する。参照した OID と MAC アドレスのペアと、先程取得した MAC アドレスを比較し、該当する OID を抽出する。抽出できた場合、FDB の接続ポートに対応する部分を SNMP を用いて参照する。そして参照した OID と接続ポートのペアと、先程抽出した OID を比較し、接続しているポート番号を抽出する。

MAC アドレスが特定できれば、ユーザ管理 DB からホストが特定できる。uid_mac テーブルに予めユーザ ID とユーザの MAC アドレスを登録しておけば、どのユーザかが分かり、さらに user_info テーブルからそのユーザの連絡先等も取り出すことが出来る。

3.5 ポリシ機能

ポリシ機能の動作を図 3.5 に表す。

ポリシ機能ではアラートレベルを決定し、警告メールの送信を行う。ユーザ管理データベースによって、ユーザの連絡先や、許可しているプロトコル、プロトコル毎の過去の検知状況などが分かるので、それらとアラートメールから解析した情報を基に、警告メールの送信やそれに伴うアラートレベルを決定する。

まずはじめに、user_info テーブルを参照し、検知したプロトコルがそのユーザの許可するものかどうかを確認する。研究や実験のために使う場合に予め許可するプロトコルとして登録しておけば、そのプロトコルは警告の対象としないためである。許可されたプロトコルであれば、そのホストに対する処理を終了する。

3.5.1 警告メール送信タイミング

許可されないプロトコルであった場合、次は警告メールを送信するかどうかを判断する。

実際に不正パケットを検知する度に警告メールを送信しては、量が多すぎて却って迷惑メールのような扱いになりかねない。そこで通知のタイミングには一定件数毎、一定時間毎、検知の頻度に比例させる、プロトコルによって変化させる、アラートレベルによって変化させる、といった方法が考えられた。これは、検知情報のログを確認すると、プロトコルによって短時間に大量にパケットを送信しているものが間々見られたためである。しかし、同じプロトコルを利用しても頻度は状況により変化するので、プロトコル毎に細かく特徴付けることは適切でなく、更にプロトコル毎に対処方法を設定するには汎用性が低いと判断した。また、頻度を判断要素として利用することも考えたが、頻度を算出するためには過去何件分かの検知時刻を履歴として保存する必要がある。短時間に集中してパケットを送信するもの、数時間に 1 回パケットを送信する

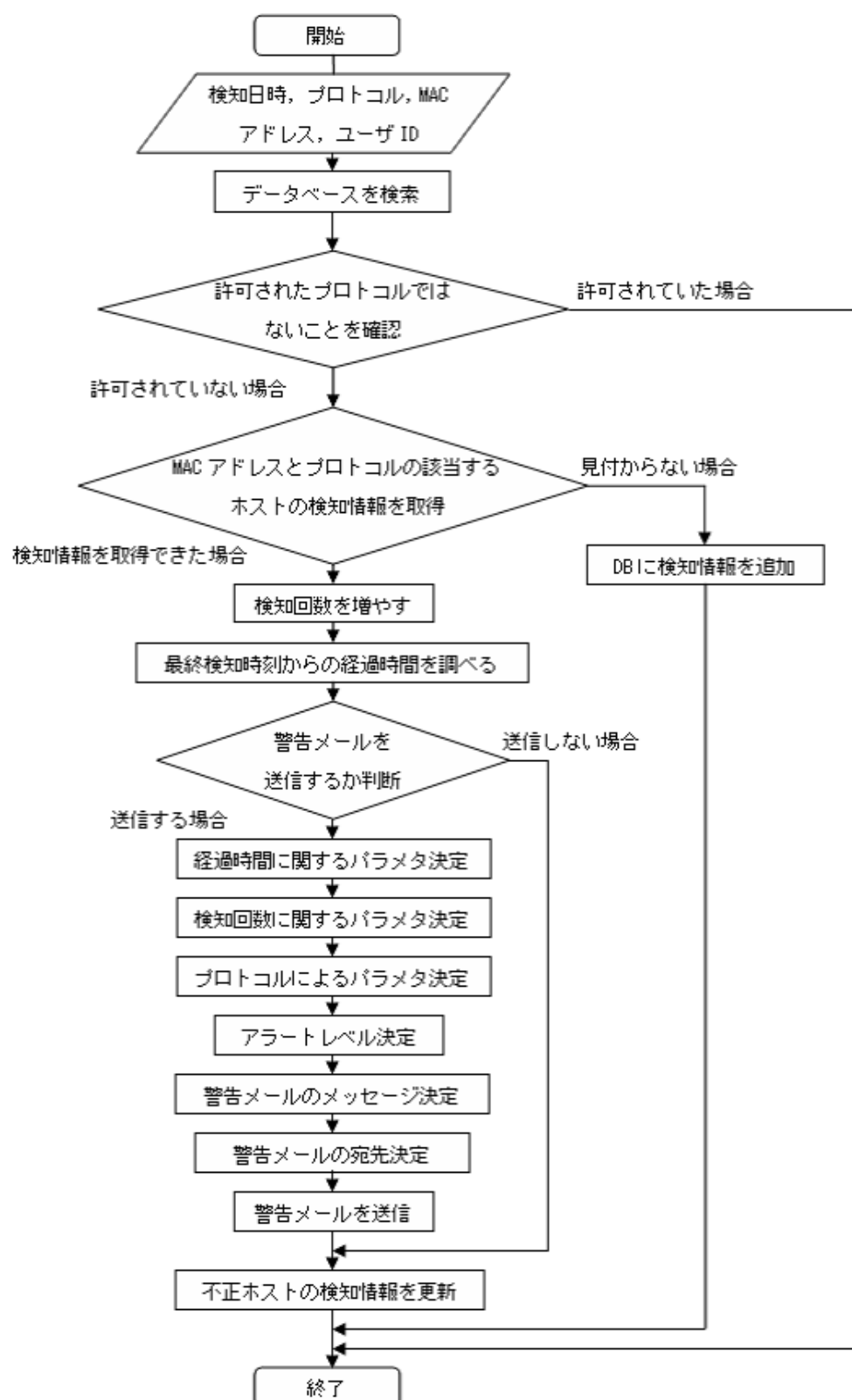


図 3.5: ポリシ機能のフロー図

ものと、検知するタイミングは様々で、その両方に対応するには、一定件数毎、あるいは一定時間は無視するといった方法で充分対応できると考えた。この方法ならば、保存するデータ量や処理回数も少なく済み、最後に検知した日時と過去の検知回数を保存しておけばシンプルな処理で判断できる。そこで、本システム中では警告メール送信の条件として、前回検知から 1 時間以上経過しているか、検知回数が 5 の倍数となることにした。

図 3.6 は、不正パケット検知と警告メール送信のタイミングの一例である。

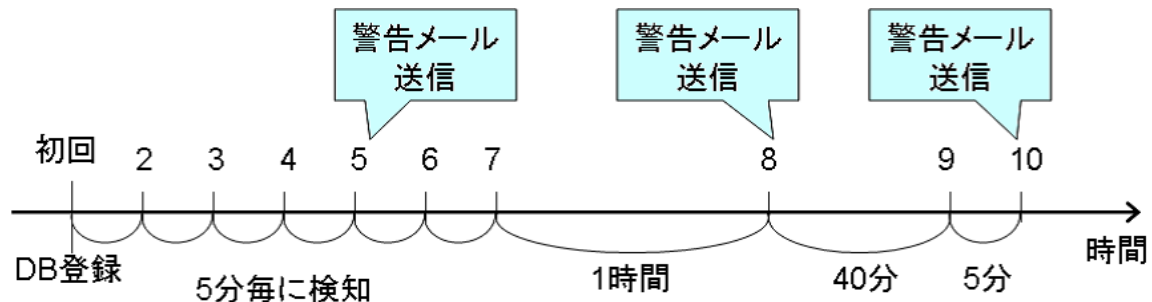


図 3.6: 警告メール送信例

host_info テーブルから MAC アドレスとプロトコルの組が一致するものを参照し、最終検知日時から一定時間以上経過しているか、または検知回数が一定件数毎に警告メールを送信する。このとき、MAC アドレスとプロトコルの組が一致するものが見つからなかった場合、初回検知とみなし新たに host_info テーブルに登録する。初回は誤操作の可能性も考慮し、様子を見るために警告メールは送信しない。

3.5.2 アラートレベルの決定

警告メールを送信する場合、実際に遮断を行うときに遮断レベルを設定することも意識して、悪質なユーザであるほど厳しい対応が出来るよう、アラートレベルを用意する。アラートレベルはレベル 1～6 の 6 段階に分け、高いレベルになると、いくら警告しても不正パケット発信を止めない悪質なユーザであると判断し、本人と管理者だけでなく、不正ホストの上司にも連絡されるようになる。このアラートレベルを決定するために考慮すべき要素として、前回検知からの経過時間、検知回数、プロトコルの危険度、前回のアラートレベルを挙げる。前回検知からの経過時間と検知回数については、警告メールの送信条件としても使われているが、どちらの条件で警告メールを送信するに至ったにしても公平に対応するために、両方ともパラメタとして利用する。プロトコルに関しても、早急な対応が必要なプロトコルであればすぐに高いアラートレベルとならなくてはならず、そこで差をつけるためにパラメタを与える。これによりアラートレベルを決定するためのパラメタは、時間パラメタ、回数パラメタ、危険度パラメタの 3 つになる。これら

のパラメタにより算出した値と前回検知時のアラートレベルにより、新たにアラートレベルを決定する。

では次に、アラートレベルを決定するための 3 つのパラメタについて説明する。

時間パラメタは 5 つの段階に分ける。閾値を 4 つ定めておき、前回検知日時から今回の検知日時までの経過時間と 4 つの閾値の大小関係によってパラメタの値が与えられる。この時間パラメタで用いる最小の閾値は、メール送信条件として用いた値と同じ値を使う。時間間隔が小さいほどパラメタに与える値は大きい。

- 時間パラメタ

- タイミング 1(4) : 1 時間未満
- タイミング 2(3) : 1 時間以上 (メール送信条件)12 時間未満
- タイミング 3(2) : 12 時間以上 1 日未満
- タイミング 4(1) : 1 日以上 1ヶ月未満
- タイミング 5(-1) : 1ヶ月以上

タイミング 5 には他の 4 つと比べて長期間の時間を設定しておき、ホストに対してアラートレベルを下げるための救済措置としてパラメタを割り振ることもできる。『悪質なユーザ』であるとみなすのは、何度警告しても不正パケットの利用を止めないためである。つまり長期間利用しなかった場合、初回と同じ対応には出来ないが、前回利用時より軽い対応にしても構わないと考えた。勿論長期間利用が無かったとはいえ、不正パケットを利用していることに違いないので、アラートレベルにあまり大きく影響しない程度のパラメタ値を設定しておく。

回数パラメタは 4 つの段階に分ける。メールを送信するかどうかを判断したときと同様に検知回数が設定値で割り切れる数のとき、より上位のものを優先し、その設定値毎に定めたパラメタの値を与える。メール送信条件での回数は、回数パラメタで用いる設定値の最低値のものを使う。

- 回数パラメタ

- 4 : 100 回毎
- 3 : 10 回毎
- 2 : 5 回毎 (メール送信条件)
- 1 : 上記以外

危険度パラメタは 5 つの段階に分ける。プロトコルに応じて危険度を設定し、その危険度をパラメタとして利用する。

- 危険度パラメタ

- 1 : eDonkey
- 2 : Gnutella
- 3 : Napster, Morpheus
- 4 : BitTorrent, WinMX, KaZaA
- 5 : Winny

これらのパラメタと前回のアラートレベルを用いて、新たなアラートレベルを算出する。

これをプロトコルを eDonkey として図 3.6 の不正パケット検知パターンで考えると、図 3.7 のように動作する。

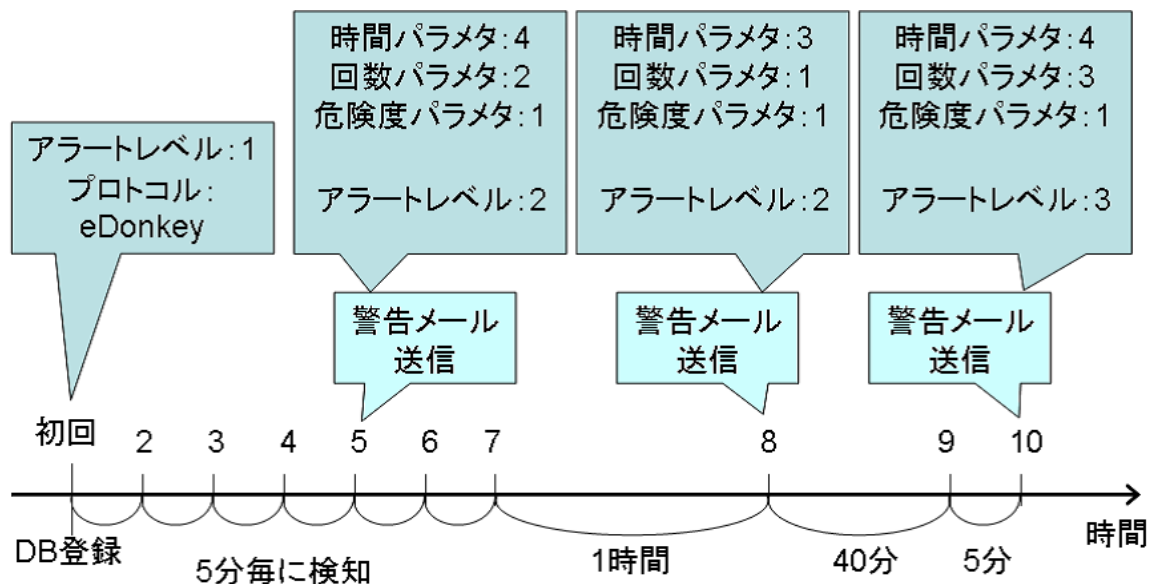


図 3.7: アラートレベルの変化例

尚、これらのパラメタに関する具体的な数値やプロトコルの設定は、汎用性を高めるため容易に変更できるようにしている。

3.5.3 警告メール送信

アラートレベルが決定されると、そのレベルに応じてメールの内容を変化させ、警告メールを送信する。変化させる対象は、宛先と本文である。

- メール宛先
 - レベル 1, 2, 3 : 本人と管理者

- レベル 4 : 本人と指導教員 (上司) と管理者
- レベル 5, 6 : 本人と指導教員 A と指導教員 B と管理者

メールの宛先に利用するメールアドレスは、本人と指導教員 (あるいは上司)、管理人のものである。管理人のメールアドレスはシステム中に設定ファイルとして埋め込み、本人と指導教員のメールアドレスは、ユーザ管理データベースの `user_info` テーブルに登録してあるものを使う。レベル 4,5,6 で連絡する指導教員は、日頃直接指導にあたっている教員で、ユーザの所属する研究室の教授や CA の教員となる。レベル 5,6 で連絡する指導教員は、例えば学科長のような、さらに上位の教員とする。

- メール本文

- レベル 1, 2 : ユーザ ID、不正パケットを検知した事、パケット検知情報、アラートレベル、使用停止を促す注意文
- レベル 3, 4 : レベル 1, 2 の内容に加え、次のアラートレベルでは通知の連絡先が増える旨
- レベル 5, 6 : レベル 1, 2 の内容に加え、早急な使用停止を求める警告文

警告メールの本文には、本人以外に受け取った人間が、誰が不正パケットを利用したか分かるように不正ホストのユーザ ID が記され、それから不正パケットを検知した日時、プロトコルといった不正パケット情報を明記される。またそれが何回目の検知であるか、アラートレベルがいくらかであるかも表記し、第三者への通知前にはそれを報せることで、不正パケット利用を停止するきっかけとさせる。

警告メールの送信が終わると、アラートレベルや最終検知日時、検知回数が増えているため `host_info` テーブルを更新する。

第 4 章

実装と評価

4.1 実験環境

本システムの実験環境を示す。

- OS : Linux CentOS
- SNMP エージェント : net-snmp
- データベース : PostgreSQL
- 開発言語 : PHP
- クライアントの OS : WindowsXP
- クライアントの IP アドレス (実験時): 133.92.157.156
- クライアントの MAC アドレス : 00-16-E3-17-7E-17

4.2 アラート情報抽出

不正パケットを検知して送られるアラートメールを元に、システムを動作させるためのダミーメール (図 4.1) を送信する。ダミーメールの本文中には次の情報を含ませてある。

date=2010-01-29

time=20:20:20

proto=eDonkey

laddr=133.92.157.156

raddr=123.456.789.102


```

====Alert====
From: FortiAnalyzer-800B(202.252.73.195)
Trigger Name: IM/P2P_Kougakubu
Log type: IM log
Triggered Threshold: More than 1 event occurred in the last 0.5 hour.
Source Device: Local FortiAnalyzer[Hostname:FortiAnalyzer-800B IP:
202.252.73.195]
Last Raw Message:
itime=1257398243 date=2010-01-29 time=20:20:20 devname=ENE02-EFW01
device_id=FGT1KA3607500216 log_id=0731103000 type=im subtype=im-all
pri=notice vd=root policyid=2 user="N/A" group="N/A" proto=eDonkey
action=block laddr=133.92.157.156 raddr=123.456.789.102 repeat=1

```

図 4.1: ダミーメール

送信前に『00-16-E3-17-7E-17』に関するホスト管理テーブルを確認すると図 4.2 のような不正ホスト情報が得られる。ダミーメールでは eDonkey をプロトコルとするので、eDonkey の利用情報を参照すると、アラートレベル『1』、初回検知日時『1001121333』、最終検知日時『1001291625』、検知回数『4』といった情報が取得できる。

```

woodstock=> select * from host_info where mac = '00 16 E3 17 7E 17';

```

mac	alart_lv	first_alart	last_alart	alart_num	protocol
00 16 E3 17 7E 17	1	1001121333	1001121333	1	BitTorrent
00 16 E3 17 7E 17	1	1001121333	1001291625	4	eDonkey

(2 rows)

図 4.2: ダミーメール送信前の host_info テーブル

このとき、上記のような情報をもつダミーメールを送信すると、図 4.3 のような解析結果が得られる。

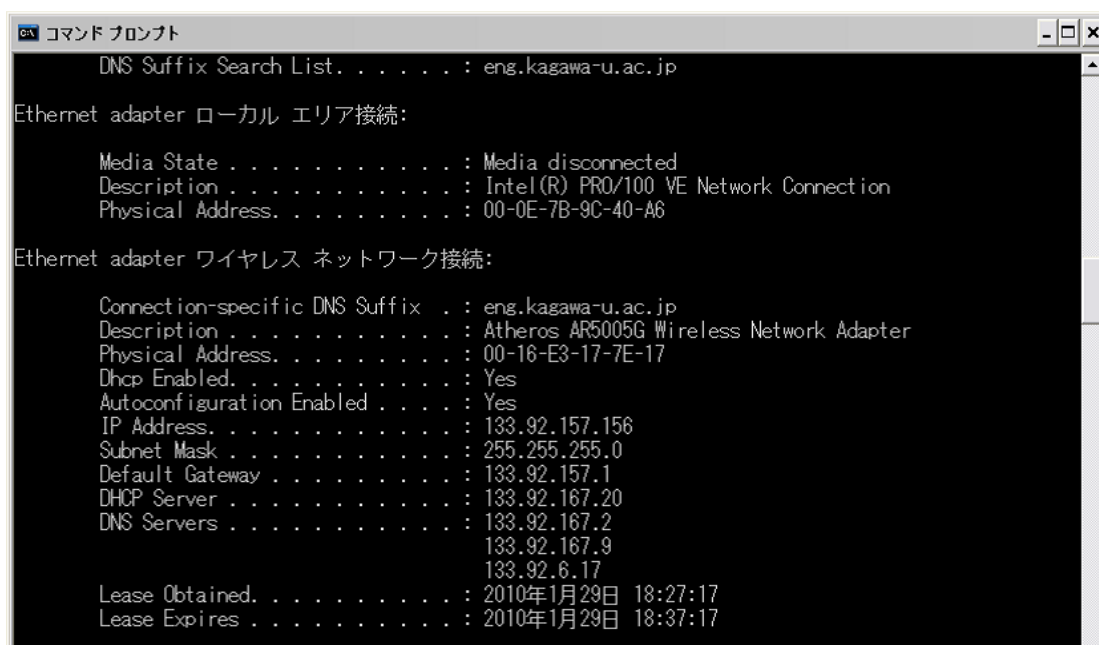
これによって、ダミーメールに載せた不正パケット情報が正確に抽出されたことがわかる。

4.3 ARP テーブルによるホスト及びポートの特定

続けて、ホスト特定機能の動作について確認する。図 4.4 のとおり、先述の IP アドレスでネットワークに接続した状態でダミーメールを送信しているので、ARP テーブルによってホスト特定できると考えられる。

```
=====
date = 2010-01-29
time = 20:20:20
proto = eDonkey
laddr = 133.92.157.156
raddr = 123.456.789.102
```

図 4.3: ダミーメールの解析結果



```
コマンド プロンプト
DNS Suffix Search List. . . . . : eng.kagawa-u.ac.jp

Ethernet adapter ローカル エリア接続:

    Media State . . . . . : Media disconnected
    Description . . . . . : Intel(R) PRO/100 VE Network Connection
    Physical Address. . . . . : 00-0E-7B-9C-40-A6

Ethernet adapter ワイヤレス ネットワーク接続:

    Connection-specific DNS Suffix . : eng.kagawa-u.ac.jp
    Description . . . . . : Atheros AR5005G Wireless Network Adapter
    Physical Address. . . . . : 00-16-E3-17-7E-17
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . : Yes
    IP Address. . . . . : 133.92.157.156
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 133.92.157.1
    DHCP Server . . . . . : 133.92.167.20
    DNS Servers . . . . . : 133.92.167.2
                           133.92.167.9
                           133.92.6.17
    Lease Obtained. . . . . : 2010年1月29日 18:27:17
    Lease Expires . . . . . : 2010年1月29日 18:37:17
```

図 4.4: ネットワーク接続状態

ダミーメールによるホストの特定結果は図 4.5 のようになった。ホストの IP アドレスから MAC アドレスを正しく求めることに成功している。また同時に、L2 スイッチの接続ポート番号が特定されていることが分かる。

```
=====
2010-01-29 20:20:20 proto=eDonkey
add=133.92.157.156 MAC=00 16 E3 17 7E 17
SW IP:133.92.157.2 PORT:8

add=123.456.789.102
=====
```

図 4.5: ホスト特定結果

4.4 ポリシ機能の動作

ホストが特定できたところで、ポリシ機能の処理に移行する。MAC アドレスが『00-16-E3-17-7E-17』でプロトコルが『eDonkey』の組は、最終検知日時『1001291625』、検知回数『4』だったので、ダミーメールから新たに抽出された不正パケット情報と比較すると、最終検知からの経過時間は 1 時間以上、検知回数は 5 回となる。これは警告メール送信条件を満たしている。

時間、回数、プロトコルの各パラメタについて考える。経過時間は 1 時間以上 12 時間未満であるのでパラメタは『3』、検知回数は 5 回目なのでパラメタは『2』、プロトコルは eDonkey なのでパラメタは『1』となる。これらのパラメタと、現在のアラートレベルが 1 であることから、新たなアラートレベルは『2』となる。

システムの動作終了後、host_info テーブルから MAC アドレス『00-16-E3-17-7E-17』のホストの情報を参照すると、図 4.6 のように更新されていることが確認できた。また、警告メールも図 4.7 のようにホストが受信したことを確認できた。

```
woodstock=> select * from host_info where mac = '00 16 E3 17 7E 17';
+-----+-----+-----+-----+-----+-----+
| mac | alert_lv | first_alert | last_alert | alert_num | protocol |
+-----+-----+-----+-----+-----+-----+
| 00 16 E3 17 7E 17 | 1 | 1001121333 | 1001121333 | 1 | BitTorrent |
| 00 16 E3 17 7E 17 | 2 | 1001121333 | 1001292020 | 5 | eDonkey |
+-----+-----+-----+-----+-----+-----+
(2 rows)
```

図 4.6: 更新された host_info テーブルの確認

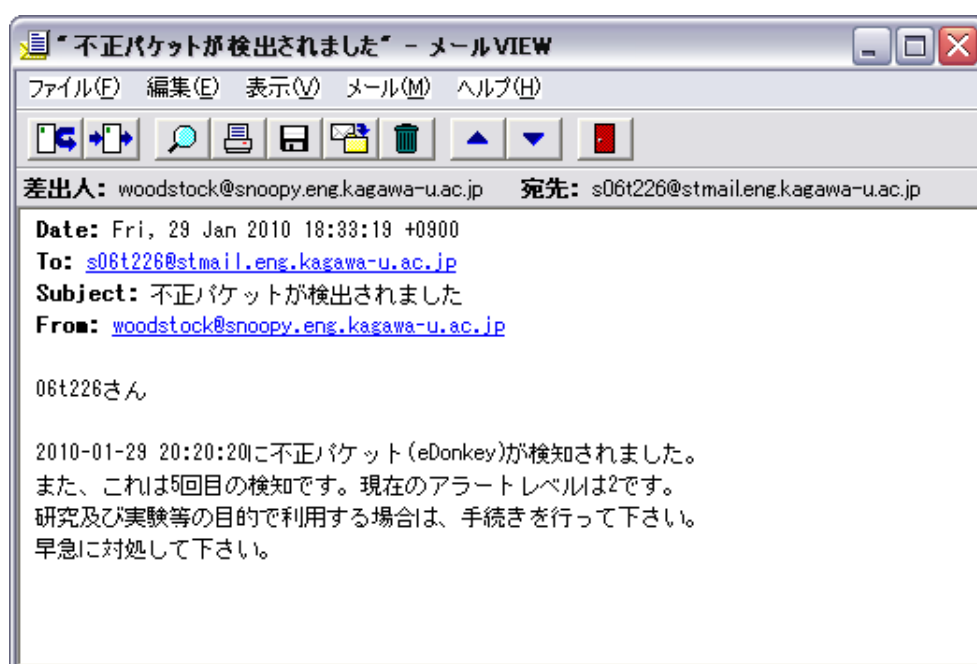


図 4.7: ホストの受信した警告メール

4.5 実ネットワークでの運用

本システムは実際に Firewall からのアラート情報を用いて、工学部ネットワークでのシステムの動作を確認している。現在、ユーザ情報テーブルと uid_mac テーブルには情報が入っていないため、ユーザ ID を『kameoka』で固定しているが、これらのテーブルに十分な情報を登録しておけば、同様の動作が期待できる。

図 4.8～図 4.12 は本システムにより実際に送られた警告メールである。また、図 4.13 は不正パケットを検知し、ホスト特定まで行ったもののログである。

アラートレベルが変化し、正常に動作していることが確認できた。

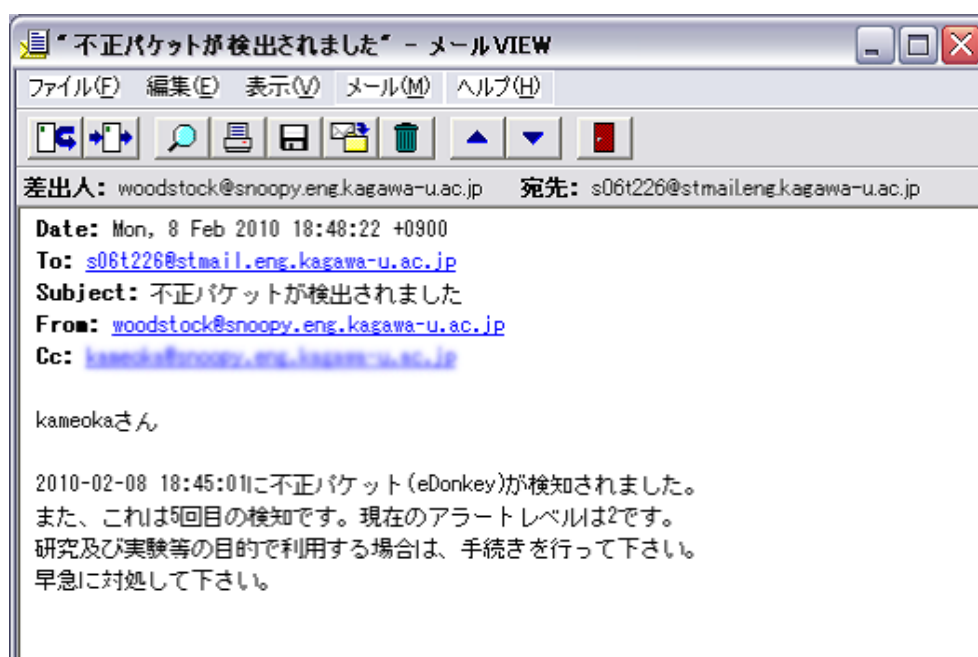


図 4.8: 警告メール

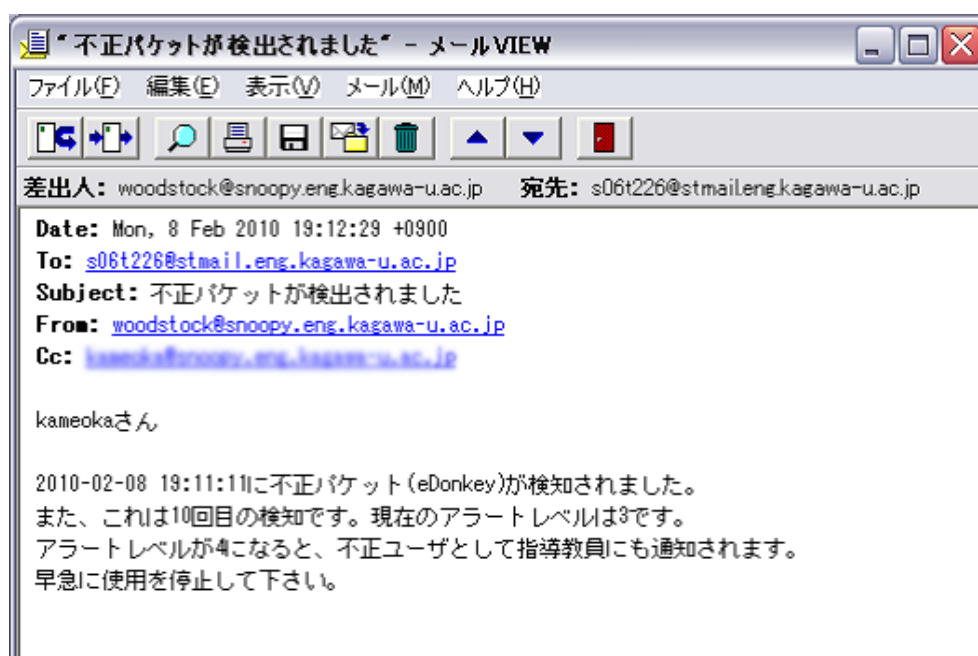


図 4.9: 警告メール

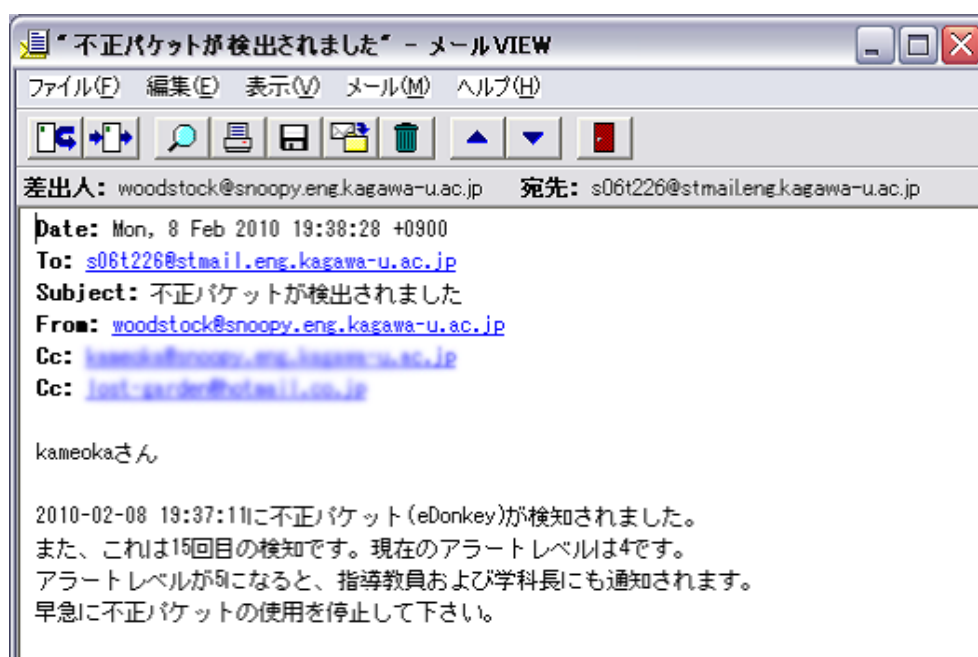


図 4.10: 警告メール

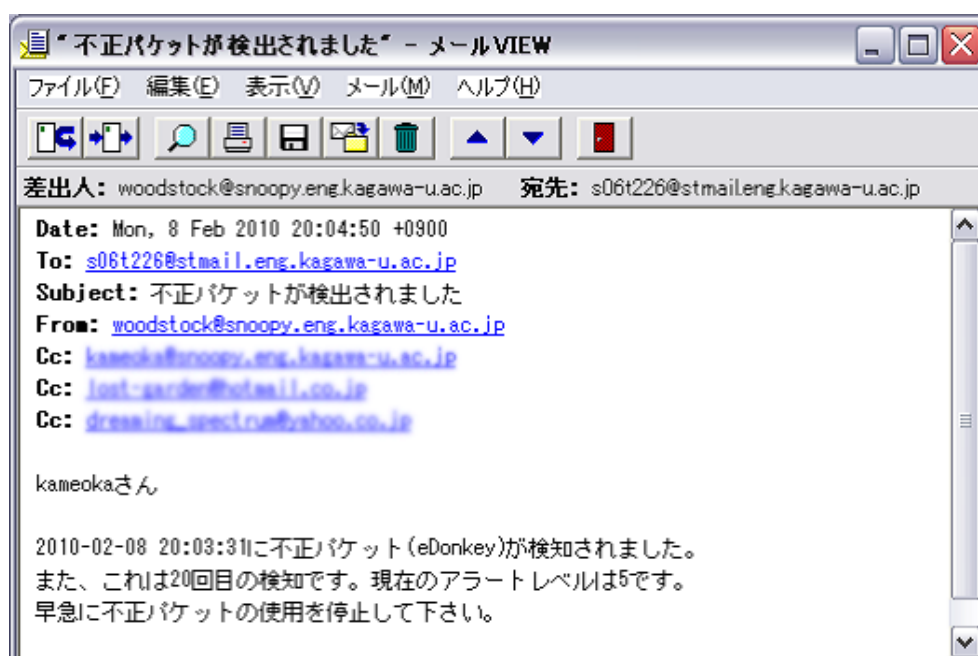


図 4.11: 警告メール

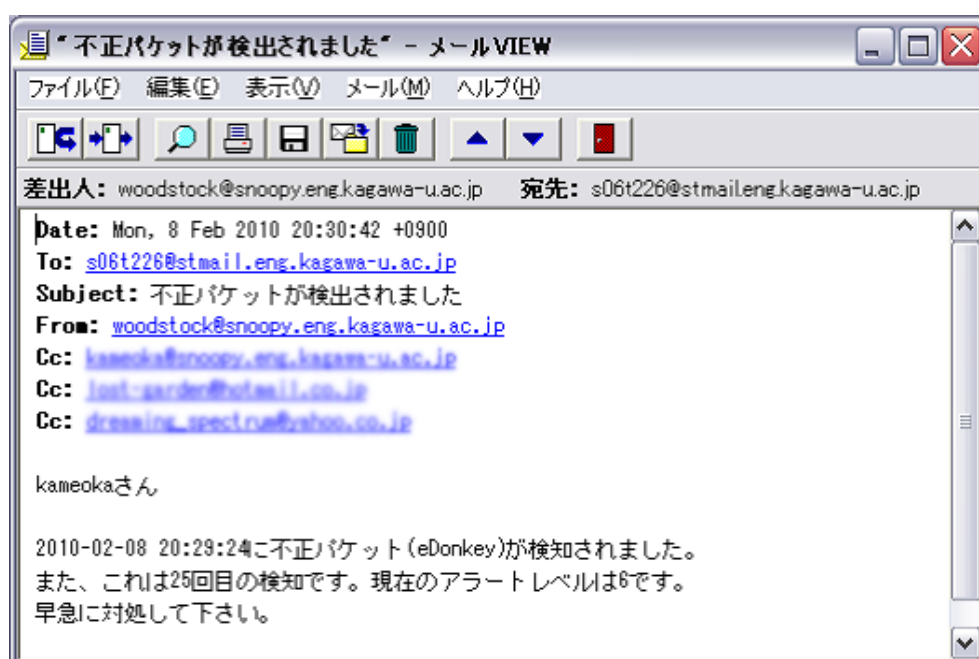
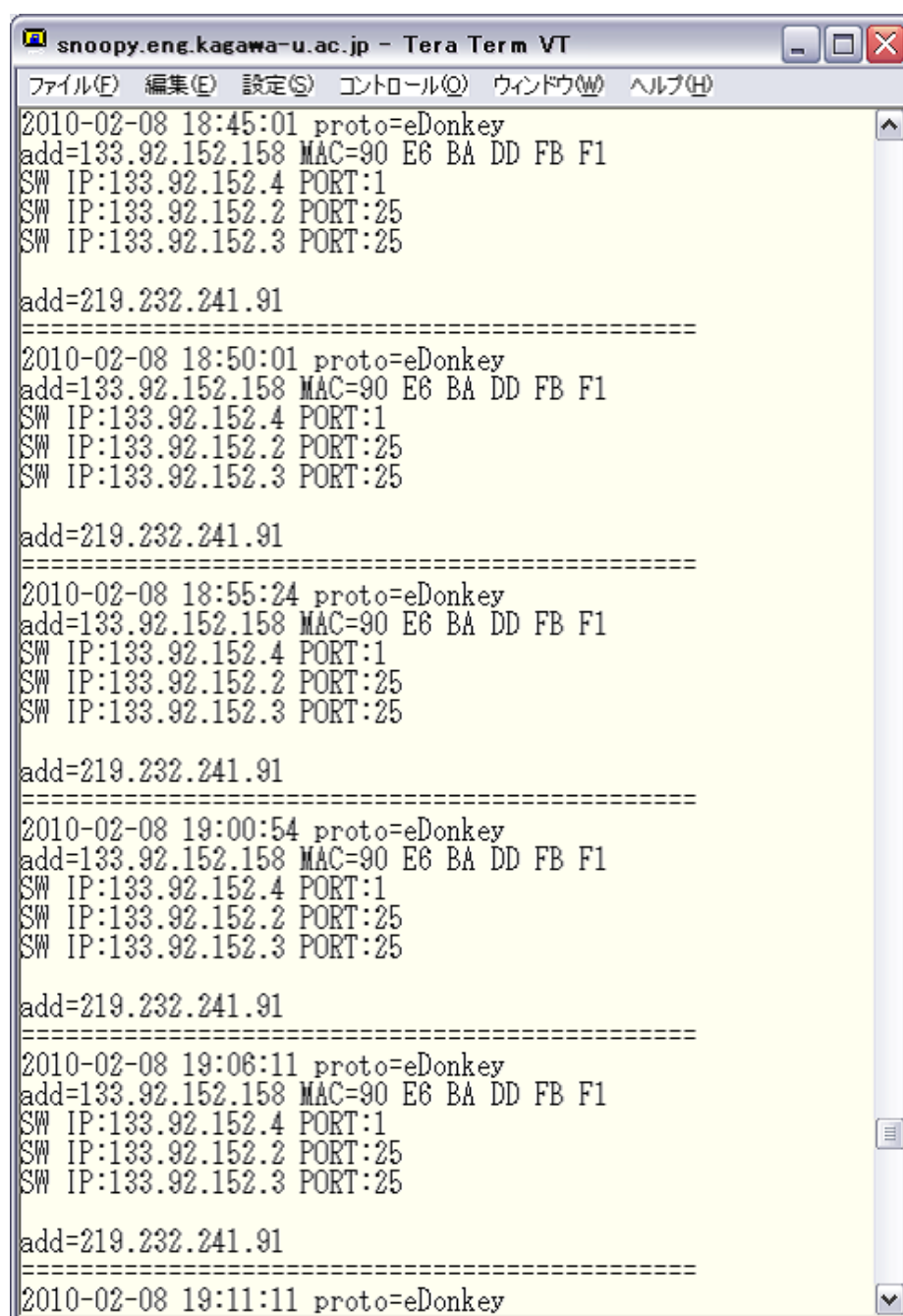


図 4.12: 警告メール



```
snoopy.eng.kagawa-u.ac.jp - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
2010-02-08 18:45:01 proto=eDonkey
add=133.92.152.158 MAC=90 E6 BA DD FB F1
SW IP:133.92.152.4 PORT:1
SW IP:133.92.152.2 PORT:25
SW IP:133.92.152.3 PORT:25

add=219.232.241.91
=====
2010-02-08 18:50:01 proto=eDonkey
add=133.92.152.158 MAC=90 E6 BA DD FB F1
SW IP:133.92.152.4 PORT:1
SW IP:133.92.152.2 PORT:25
SW IP:133.92.152.3 PORT:25

add=219.232.241.91
=====
2010-02-08 18:55:24 proto=eDonkey
add=133.92.152.158 MAC=90 E6 BA DD FB F1
SW IP:133.92.152.4 PORT:1
SW IP:133.92.152.2 PORT:25
SW IP:133.92.152.3 PORT:25

add=219.232.241.91
=====
2010-02-08 19:00:54 proto=eDonkey
add=133.92.152.158 MAC=90 E6 BA DD FB F1
SW IP:133.92.152.4 PORT:1
SW IP:133.92.152.2 PORT:25
SW IP:133.92.152.3 PORT:25

add=219.232.241.91
=====
2010-02-08 19:06:11 proto=eDonkey
add=133.92.152.158 MAC=90 E6 BA DD FB F1
SW IP:133.92.152.4 PORT:1
SW IP:133.92.152.2 PORT:25
SW IP:133.92.152.3 PORT:25

add=219.232.241.91
=====
2010-02-08 19:11:11 proto=eDonkey
```

図 4.13: 不正パケット検知ログ

第 5 章

おわりに

5.1 まとめ

本論文では、不正パケット遮断システムの実用化に向けたホスト特定機能の開発について述べた。

本システムは、不正ホストの特定、警告メールによる通知の機能をもつ。不正ホストの特定では、IP アドレスから MAC アドレス、場合によっては接続している L2 スイッチのポート番号までを取得し、MAC アドレスに対応するユーザ ID を特定する。そして、警告メールによる通知では、不正パケットの利用状況に応じて変化するアラートレベルを設定し、不正ホスト本人のみならず、その上司にまで検知連絡を行うといった対応を自動で行うことができた。

現段階では実際に不正ホスト本人にメールを送るまでは至っていないが、ユーザ管理データベースのユーザ情報テーブルと uid_mac テーブルを作成すれば、いつでも運用することが可能である。

本システムを導入することで、不正ホスト一人一人に不正パケット利用についての意識を高めさせ、健全なネットワーク環境をつくることが期待でき、ネットワーク管理者の負担を減らすことができる。

5.2 今後の課題

今後の課題として、以下の点が挙げられる。

- ユーザ情報テーブル用インタフェースの作成

ユーザ管理データベースのユーザ情報テーブルは、不正ホスト情報テーブルや uid_mac テーブルと異なり手動で情報を更新しなければならない場合がある。そこで、ネットワーク上にインタフェースを作成すれば、入力項目なども分かりやすく、より容易に情報を更新できると考えられる。

- 不正パケット検知情報確認インタフェースの作成

警告メール送信機能によってネットワーク管理者にも不正パケット検知情報が送られる。しかし管理者は多数のホストのアラート情報を受け取ることになり、情報の把握が難しくなる。また、警告メールを受け取ってすぐに確認出来るわけではない。これらを考慮して、管理者用の不正パケット検知情報のログを統計的に確認出来るインタフェースがあれば、管理者の対応もより円滑に進められるのではないかと考えられる。

- 遮断機能および遮断解除機能の実装

本研究で不正ホスト特定機能と、ポリシーによる警告メール通知機能まで工学部ネットワークに適用することができたが、遮断機能と遮断解除機能の実装は出来ていない。

謝辞

本研究にあたって終始ご指導や励まし、ご助言を頂きました最所圭三教授には、心より感謝を申し上げます。また、本研究に協力してくださった同研究室の皆様にもお礼を申し上げます。

参考文献

- [1] 高橋巧, “組織内における不正パケット遮断システムの運用ポリシー設計および実装”, 香川大学大学院工学研究科修士論文, 2007.
- [2] 原田知弘, “不正パケット遮断システムにおける自動制御ツールの開発”, 香川大学工学部卒業論文, 2007.
- [3] 岡原聖, “不正パケット遮断システムのユーザインタフェース開発,” 香川大学工学部卒業論文, 2007.
- [4] 松木崇, “不正パケット遮断システムにおけるポリシー機能の実装と評価”, 香川大学工学部卒業論文, 2008.
- [5] ITmedia エンタープライズ, “SNMP におけるネットワークモニタリング”,
<http://www.itmedia.co.jp/enterprise/special/0705/snmp/>
- [6] “RFC1213 - Management Information Base for Network Management of”,
<http://www.faqs.org/rfcs/rfc1213.html>