E-13

スイッチ情報表示による MARS の拡張

Expansion of the MARS by the switch information indication

白井 奈津美† 川橋 裕‡
Natsumi Shirai Yutaka Kawahashi

1. はじめに

情報化社会が発展するにつれ，インターネットは私たちの生活になくてはならないものとなってきた．それにともない，学術機関・一般企業などでは研究・業務のために必要となるネットワークが組織内に構築されてきた．多くの機関でユーザに組織内ネットワークの環境が提供され，ユーザの利便性は飛躍的に向上している．一方で，ユーザからインターネットに接続できないというネットワーク障害の問い合わせが管理者に多く寄せられてきている．接続できないという症状も，特定の IP アドレスに接続できない，インターネット環境に接続できないなど様々なものが挙げられる．少ない情報の中で，問い合わせを受けた管理者が障害原因を特定することは困難である．ユーザ側から，どこまで通信可能なのかという情報を聞き出すことも困難である．さらに，障害の原因が管理者側の機器にあるのか，ユーザ側の機器にあるのかを判断することも必要である．

一般的に，管理者はファイアウォールやサーバのアクセスログにある IP アドレスを基に事後対応する．そのため，端末識別情報や場所，IP アドレスを把握する必要がある．一方で，利用申請をせずに IP アドレスを使用するユーザ，申請内容の変更時に再申請をしないユーザの不正接続が後を絶たない．このため，正確な接続情報を把握することは困難である．障害原因を切り分けるためには，可能な限りの情報を収集する必要がある．情報を得るためには，ネットワーク機器の確認や，聞き取り調査，現地調査などをおこなう必要があるため多大な時間，労力を必要とされる．

和歌山大学では，先行研究である MARS(Monitoring Analysis and ResponseSystem)[1][2][3][4] を運用している．MARS では，接続している端末の接続時間や，利用場所，端末の IP アドレスや MAC アドレスを一定期間保存している．以上の情報により，障害発生時に原因を迅速に特定することが可能である．しかし，接続している端末の情報を確認できるが，端末の通信速度や通信方式といったスイッチの情報は，MARS では確認できない．そのため，管理者は MARS の情報だけで原因が分からない場合は，当該スイッチにログインして，スイッチの情報を確認している．管理者の中でもスイッチのログイン情報を把握していない管理者や，スイッチに接続する手段を知らない管理者はスイッチの情報を得ることができない．加えて，接続している端末が過去に接続していた端末から異なる端末に変更されていた場合も調査が困難である．それは，過去と異なる端末に変更したことで通信速度や通信方式が変更される場合が存在するためである．一般的に，管理者側スイッチとユーザ側端末の通信性能が高い場合，膨大な通信量であっても，その通信速度に対応可能であると正常に通信できる．しかし，双方の通信性能が高い場合でも障害が起きる可能性がある．管理者側スイッチとユーザ側端末の間に，通信性能が低いハブなどが設置されていた場合，一時的に膨大な量の通信をおこなわれると，スイッチが自身を保護するためにスイッチのポートをシャットダウンする．それにより，通信できなくなる場合がある．この様な障害原因を調査するために，管理者は，ユーザ側が過去に接続していた端末のスイッチ情報を確認する必要がある．しかし，過去のスイッチ情報が記録に残っていないため確認できない．そのため管理者は障害原因を特定するのが困難である．

本研究では，MARS のみでは確認できなかった通信速度や通信方式といったスイッチの情報を，MARS に追加して表示することで，管理者を支援することを目的とする．提案システムは，端末がスイッチに接続された時に，スイッチの情報を取得する．これにより，スイッチのログイン情報を把握していない場合でも，MARS でスイッチの情報を確認できる．加えて，過去のスイッチの情報を記録し，過去に遡ってスイッチの情報を確認できる．したがって，スイッチにログインすることなく MARS を用いることだけで障害原因を調査できるため，管理者を支援することができると考える．

本論文では，第 2 章で既存技術とその問題点について述べる．第 3 章では，先行研究の MARS について述べ，第 4 章で研究目的を述べる．第 5 章および第 6 章では，提案手法とその実装について述べる．第 7 章では，本学内ネットワークにおける提案システムの運用実験の内容と結果について述べる．最後に第 8 章では，本研究の評価と考察について述べる．

2. 既存技術

スイッチの情報取得に関する既存技術とその問題点について述べる．加えて，本研究を進めるにあたって基礎となる技術について述べる．

2-1. 統合監視システム

統合監視システムとは，ネットワークを介して複数のホストを集中監視するシステムである．このシステムは，死活監視やサービス監視，ネットワーク監視など様々なものを監視できる．本節では，オープンソースソフトウェアで広く普及している統合監視システムについて述べる．

2-1-1. Nagios

Nagios[5] は，指定した時間に指定された間隔で，指定されたホストに対して指定した監視を実行する．監視結果を保持し，設定に応じて管理者にメールで異常を通知する機能を備えている．

2-1-2. ZABBIX

ZABBIX[6] は，Web ブラウザからアクセスできるため，ネットワークがある環境であればアクセスできる．データを基にレポートやグラフを作成し表示させる機能がある．異常があった場合，管理者にメールで通知する機能を備え

†和歌山大学, Wakayama University

‡和歌山大学システム情報学センター, Center for Information Science, Wakayama University

ている．

2-1-3. 問題点

これらの統合監視システムは監視対象の端末を把握する必要があるため，ユーザが端末を追加する時に，管理者へ利用申請をおこなう必要がある．しかし，利用申請をせずに IP アドレスを使用するユーザ，申請内容の変更時に再申請をしないユーザが少なからず存在する．したがって，ネットワークに接続されている全ての端末を正確に把握することは困難である．加えて，スイッチの情報を取得するためには各端末へ専用のエージェントのインストールが必要である．

2-2. 基本技術

2-2-1. SNMP(Simple Network Management Protocol)

SNMP[7] とは，ネットワークにおいてルータやスイッチ，サーバなどの通信機器をネットワーク経由で監視，制御するためのプロトコルである．SNMP では，MIB(Management Information Base) と呼ばれるデータモデルで管理している．MIB はツリー構造になっており，目的の情報までを指定した，OID(Object ID)を使用して値を取得する．監視対象であるスイッチの IP アドレスと SNMP でのパスワードの役割であるコミュニティ名を指定してパケットを送受信する．取得したい情報は OID を指定することで取得できる．本研究では，スイッチ情報として通信速度である Speed，通信方式である Duplex を取得する際に使用する．

2-2-2. rsyslog

rsyslog[8] とは，システムの動作状況を監視し，ログとして記録したものを取得するプログラムである．あらかじめユーザが指定した方法でログを特定のサーバに送信することや，指定したファイルに記録することができる．本研究では，rsyslog が記録するリンクのアップダウンしたエッジスイッチの IP アドレス，ポート番号，時刻を利用する．この記録を基に，SNMP でスイッチ情報を取得している．

2-2-3. MARS

MARS とは，端末の接続状況をリアルタイムで監視することにより，障害原因を調査するシステムである．詳しくは第 3 章で述べる．本研究では，MARS の端末接続情報に追加してスイッチ情報を表示させる．そのための基盤となるシステムである．

3. 先行研究

本章では，ネットワーク接続をリアルタイムで監視することにより，障害の原因究明を支援する先行研究の MARS について述べる．

3-1. MARS

3-1-1. 動作と端末の接続情報

MARS は，RADIUS 認証プロトコル[9] を利用してエッジスイッチが通知する端末の接続情報を収集する．エッジスイッチとは，組織内ネットワークの末端でユーザ側の通信機器と接続されているスイッチのことである．

RADIUS 認証プロトコルは RFC2865 で策定されており，ダイヤルアップ接続時のユーザ認証プロコトルである．近年では，ダイアルアップだけでなく，無線 LAN や VLAN，インターネット接続サービス，コンテンツ提供サービスなどの認証とアカウンティングとしても利用されている．

同プロトコルの特徴として，AAA モデルもサポートしており柔軟な拡張性が挙げられる．AAA モデルとは，サービスの提供から記録までの流れを 3 段階に分けたモデルである．利用者の識別である認証(Authentication)，提供の可否である承認(Authorization)，利用の記録であるアカウティング(Accounting) の 3 つから成る．

先行研究では上記の特徴を生かして，エッジスイッチと MARS 間の通信に RADIUS 認証プロトコルを利用する．エッジスイッチと MARS 間の動作手順を図 3.1 と下記に示す．

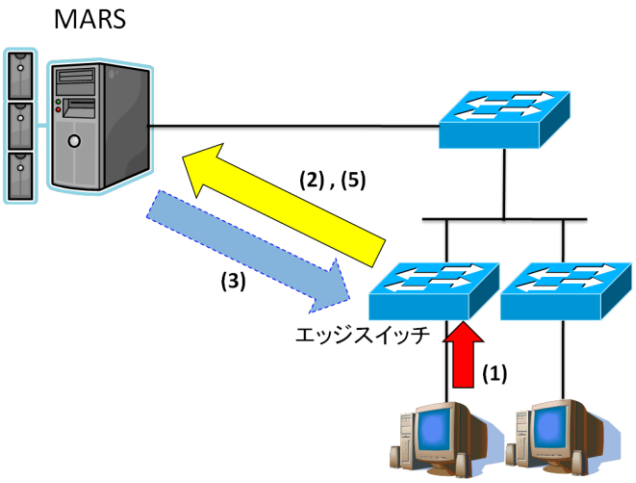

図 3.1：MARS の動作手順

(1) 端末がエッジスイッチに接続する
(2) エッジスイッチは接続要求を MARS(RADIUS サーバ)に送信する
(3) MARS は受信した情報を基に認証し，認証結果をエッジスイッチに通知する
(4) エッジスイッチは通知された認証結果を基に，接続を許可する
(5) エッジスイッチは MARS に，端末が接続を開始，終了した事実を通知する

前述の動作手順における(2) の動作時に，エッジスイッチが MARS に送信している記録情報を示す．

- セッション ID
- 端末の IP アドレス
- エッジスイッチの IP アドレス
- エッジスイッチのポート番号
- 接続開始 or 終了状態
- 接続開始 or 終了時刻

上記のことから，RADIUS 認証プロトコルの特徴を利用して端末の接続情報を管理することができる．加えて，RADIUS サーバが端末の接続に対して全許可という判定および応答をすることで，ユーザに認証を求めない設計としている．これにより，ユーザに認証を求めないという運用ポリシの組織に対して，MARS を導入する際の敷居が低

く利用しやすい．

MARS では，スイッチから取得した情報をパッチ情報と対応させ接続先となる部屋名を特定する．加えて，収集される端末を各セッションごとに管理している．パッチ情報には，エッジスイッチの各ポートと接続先の部屋名が対応付けられた情報が管理されている．セッションは，端末が接続を開始してから終了するまでの通信と定義している．これらの端末接続情報をデータベースに格納する．接続情報として管理される項目を下記に示す．

- セッション ID
- 端末の DNS ホスト名
- 端末の IP アドレス
- 端末の MAC アドレス
- エッジスイッチの IP アドレス
- エッジスイッチのポート番号
- 棟名
- 部屋名
- 接続開始時刻
- 接続終了時刻

MARS は，管理インターフェースを Perl[10] および PHP[11] で記述した Web アプリケーションにより実装している．そのため，OS への依存性が少なく，ネットワーク管理に特別なソフトウェアが不要である．インタフェースでは，端末の接続状況として下記の情報を提示する．

- 端末の DNS ホスト名
- 端末の IP アドレス
- 端末の MAC アドレス
- 棟名
- 部屋名
- エッジスイッチの IP アドレス
- エッジスイッチのポート番号
- 接続開始時刻
- 接続終了時刻

管理者は提示された情報を基に，障害特定をおこなう．

3-1-2. 障害特定手順

実際に MARS を使った障害特定の手順を図 3.2 と下記に示す．

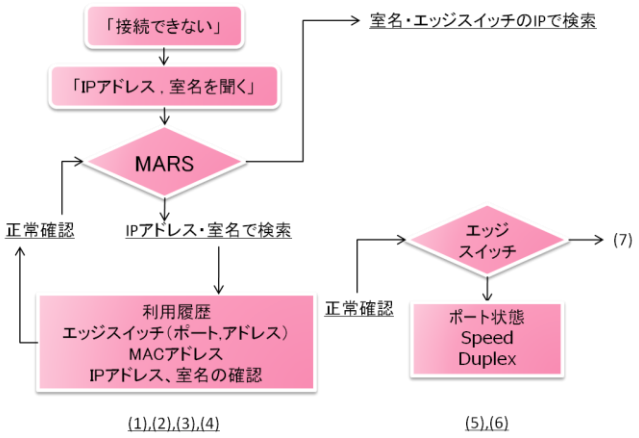

図 3.2： 障害解決の手順

障害が起きた時に，管理者はユーザから接続できないという問い合わせを受ける．管理者はユーザに接続できない端末の IP アドレスと室名を聞く．次に，管理者は MARS を用いて IP アドレスと室名から端末を検索し，利用履歴，エッジスイッチのポート，アドレス，端末の MAC アドレスの確認をおこなう．ここで正常であると確認できた場合は次に，エッジスイッチの IP アドレスと室名で検索をかける．検索結果から利用履歴，エッジスイッチのポート，端末の MAC アドレス，IP アドレスを確認する．その後，スイッチにリモートでログインし，ポートの状態や通信速度，通信方式などを調べる．ここで正常が確認された場合は原因が判明できないため，端末がある現地へ調査に行く必要がある．この様な手順で管理者は，障害の特定をおこなっている．

以上の障害特定の手順によって，切り分けられることができる障害原因は，下記に示すような例が挙げられる．

(1) 端末不良
(2) IP アドレス設定ミス
(3) 端末内アプリケーションの設定ミス
(4) 不正利用による IP アドレス競合
(5) 室内ハブが低性能
(6) 頻繁な挿抜の繰り返し
(7) 不明

(1),(2),(3),(4) は，MARS を用いるだけで障害原因を調査することができる．しかし，(5),(6) の場合，MARS だけでなくスイッチにリモートログインしスイッチの情報を確認する必要がある．

3-1-3. 問題点と課題

第 3.1.2 項で述べたように，(5),(6) のような障害の場合，MARS が収集した端末情報からはスイッチの情報を確認できないため，MARS を用いるだけでは障害原因を特定できない．よって，管理者は障害原因を特定するために多大な時間を要する．加えて，スイッチのログイン情報を把握していない管理者は(1),(2),(3),(4)の障害しか調査することができない．

これらを解決するために，MARS の接続情報に合わせてスイッチの情報を記録する必要がある．加えて，インタフェースに表示し，スイッチの情報を取得する必要がある．

4. 研究目的

ネットワーク運用において管理者は障害発生時に迅速な対応が求められる．第 2 章でも述べたように，端末の接続情報を管理するシステムは存在する．しかし，端末の接続情報やスイッチの情報を取得するためには，ユーザが IP アドレスの申請や，各端末に専用エージェントのインストールをおこなう必要がある．そこで本学においては，第 3 章で述べたような MARS を運用することで端末の接続情報を管理している．しかし，MARS はスイッチの情報を取得することができない．端末の接続情報だけで障害原因を特定できない場合，端末が接続されているスイッチの情報を確認する必要がある．昨今起こる障害原因の多くは，管理者側機器とユーザ側端末の高性能化により双方の間に接続されるユーザ側のハブなどが，双方の性能に対応せず障害を発生させている．そのため，この様な機器を見つけ，対

処する必要がある．既存手法では，過去に接続されていたスイッチの情報を確認できないため，障害原因を特定することが困難である．そのために，管理者への負担を軽減するためには過去のスイッチ情報を確認できることが必要である．

本研究では，MARS のみで障害を特定できるようにMARS にスイッチの情報を付加し，管理者を支援することを目的とする．加えて，過去に遡って接続されていた端末のスイッチ情報を記録できるようにすることで，障害原因を特定することを可能にする．さらに，それらが発生する可能性がある機器を見つけ，障害を予防できるシステムを目指す．以上の条件を満たすシステムをスイッチの監視とMARS の端末情報を関連付けることにより構築する．

5. 提案手法

5-1. スイッチ情報取得の提案手法

昨今，管理者側のエッジスイッチとユーザ側の端末が高性能化している．しかし，双方の間に設置されるユーザ側のハブなどが低性能であるために，通信障害が多く発生する．この様な障害を特定するためには，ユーザが過去に接続していた端末を特定する必要がある．よって，過去のスイッチ情報を確認でき，障害が発生する可能性がある機器を挙げ，障害を予測できる手法を提案する．提案手法の内容について以下で述べる．

5-1-1. スイッチ情報

スイッチの情報は，SNMP を用いて取得する．提案システムは，スイッチの各ポートの通信速度である Speed と通信方式である Duplex を収集する．スイッチの Speed，Duplex を示す SNMP の値は，次の OID で指定する値である．

ifSpeed(OID:1.3.6.1.2.1.2.2.1.5)
ifSpeed は，ビットのインターフェースの現在の帯域幅の推定で，通信速度を示す．単位は Mbps である．

dot3StatsDuplexStatus(OID:1.3.6.1.2.1.10.7.2.1.19)
dot3StatsDuplexStatus は，データの通信方式を示す．値は，unknown，halfDuplex，fullDuplex の 3 種類である．unknown は，取得した時の通信方式が判別できなかった場合に示す．

これらの OID を利用して，スイッチの情報である Speed，Duplex を取得する．

5-1-2. 収集方法

スイッチ情報は，端末によって変更されるため，同じスイッチの同じポートであっても変更されることが考えられる．そのため，SNMP で頻繁にスイッチ情報を取得する必要がある．スイッチ情報の収集と表示方法について図 5.1 と下記で説明する．

(1) 端末がエッジスイッチに接続する度に，リンクのアップダウン情報をログとして記録する．
(2) ログファイルを 1 分毎に監視し，ログファイルに新しく情報が追加された場合，追加された情報を取得する．
(3) 追加された情報を基に，SNMP を用いてスイッチ情報を取得する．
(4) 取得したスイッチ情報をデータベースに格納する．

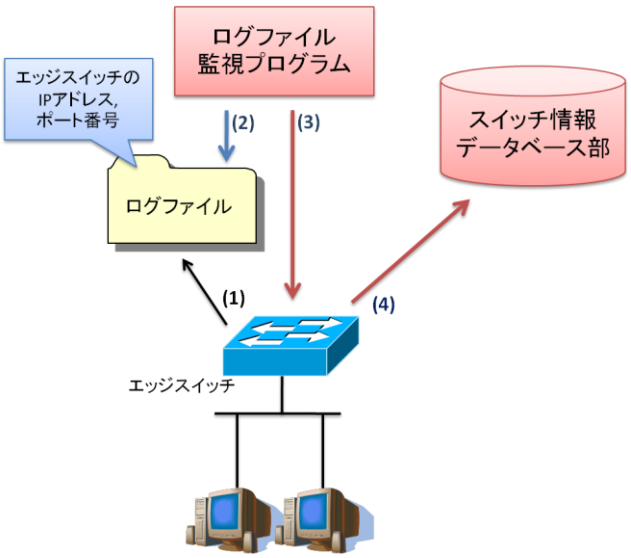

図 5.1： 収集方法

rsyslog では，あらかじめ指定した方法で，ファイルにリンクのアップダウン情報を記録することができる．したがって，(1) で rsyslog を利用し，リンクのアップダウンした端末が接続しているエッジスイッチの IP アドレスとポート番号，接続した時刻をログファイルに記録している．提案手法では，端末がスイッチに接続後，1 分以内にスイッチの情報を取得する．そのため，(2) のように監視して，端末の接続の有無を確認する．ここで，新しくログファイルに情報が追加された場合は，エッジスイッチの IP アドレス，ポート番号を取得する．(3) では，(2) で情報を取得した時に，取得したエッジスイッチの IP アドレスとポート番号を基に該当のエッジスイッチに SNMP を用いて，スイッチの情報を取得する．(4) で，取得したスイッチの情報とその情報を取得した時刻を合わせて，データベースに格納する．

5-1-3. スイッチ情報の表示

スイッチの情報は MARS の端末情報との共通情報を関連付けてインタフェースに表示する．共通情報は，エッジスイッチの IP アドレスとポート番号であるから，これに一致する項目をスイッチの情報を取得した時刻と，MARS の端末の接続開始時間で対応させる．

6. 提案システム

本章では，実装した提案システムについて述べる．提案手法を実装するにあたり必要な動作環境およびシステム構成を以下で述べる．

6-1. ネットワーク環境

本学内のネットワーク環境を参考にし，エッジスイッチとなる機器に Cisco[12]社製 Catalyst スイッチを用いた．提案システムを動作させるためには，MARS が動作する環境が必要である．MARS を動作させるためには，エッジス

イッチがネットワーク認証機能を有している必要がある．そのためネットーク認証機能を有しているスイッチの IOS を使用する．本研究で動作確認した機器は下記の通りである．

Catalyst 2960（Cisco IOS 12.2(52)SE 以降）

6-2. ソフトウェア構成

第 5 章で述べた提案手法をオープンソースソフトウェアを用いて実装した．オープンソースソフトウェアは，Apache[13]，rsyslog，Net-SNMP[14]，MySQL[15] など一般的に利用されている安定性が高いものを採択した．利用したソフトウェアの環境を表 6.1 に，Net-SNMP，MySQL の概要を以下に示す．

表 6.1： ソフトウェア構成

利用用途	ソフトウェア
Web	Apache 2.2.15
ログ収集	Rsyslog 5.8
スイッチ情報収集	Net-SNMP-5.5
データベース	MySQL 5.1.61

Net-SNMP

Net-SNMP は，SNMP プロトコルを実装したオープンソースソフトウェアである．snmpwalk コマンドを用いて OID と監視対象を指定することにより OID 対応する情報を取得することができる．提案システムでは，Net-SNMP のライブラリを用い，スイッチの SNMP エージェントから Speed と Duplex を取得している．

MySQL

MySQL とは，オープンソースソフトウェアのリレーショナルデータベース管理システムである．提案システムでは，SNMP で取得したスイッチ情報をデータベースに格納するために用いた．

6-3. システム構成

提案システムの処理手順と各部について図 6.1 と下記に示す．

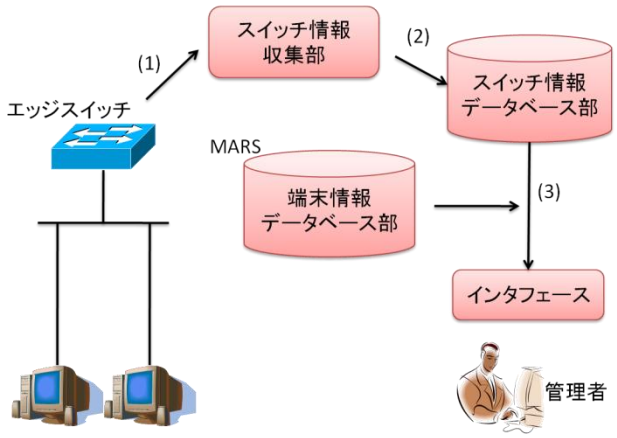

図 6.1： 提案システムの処理手順

(1) スイッチ情報を収集
(2) スイッチ情報をデータベースに格納
(3) MARS の端末接続情報をスイッチ情報と関連付けてスイッチ情報を管理者に提示

次に，提案システムを構成する収集部，データベース部，インタフェース部について述べる．

6-3-1. スイッチ情報 収集部

収集部は，1 分毎に rsyslog を監視し，リンクダウン・リンクアップが起きているかを確認する．リンクダウン・リンクアップが起きていた場合に，該当するエッジスイッチのポートに，第 5.1.1 項で述べた OID を用いて，スイッチ情報を取得する．

6-3-2. スイッチ情報 データベース部

データベースでは，下記の情報を管理している．

- エッジスイッチの IP アドレス
- エッジスイッチのポート番号
- SNMP でスイッチ情報を取得した時刻
- Speed
- Duplex

管理者は、障害原因を調査する時に，過去に遡って接続されていた情報を確認することで障害原因の切り分けをおこなう場合がある．そのため，データベース部では過去に接続されていたスイッチ情報を保存するために，スイッチ情報を取得する度データベースに格納する．

6-3-3. インタフェース部

インターフェースを Perl および PHP で記述した Web アプリケーションにより実装している．検索欄と端末接続情報のインターフェースを図 6.2 と図 6.3 で示す．

図 6.2： 検索欄

図 6.3： 端末接続情報

従来の MARS で確認できた端末の接続情報にスイッチ情報を付け加えることで，リアルタイムでスイッチの情報を確認できる．管理者は図 6.2 の検索欄に，スイッチ情報

であるSpeed やDuplex を入力することで,特定のSpeed, Duplex に該当する接続端末の情報を検索することができる.

6-4. 提案手法の障害特定の手順

提案システムを組み合わせたMARS を利用して,障害を特定する手順について図6.4 と下記で説明する. 図6.4 の(1)～(7) の原因内容は, 第3.1.2 項に示した通りである.

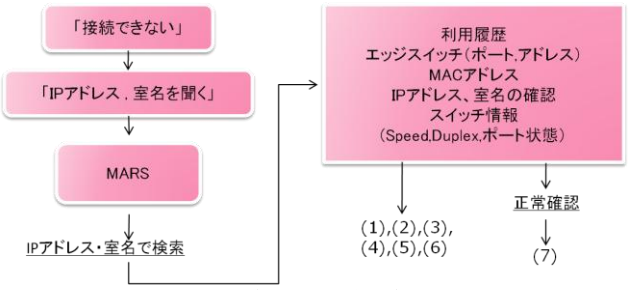

図 6.4： 提案手法の障害解決の手順

障害が起きた時に管理者は, ユーザから接続できないという問い合わせを受ける. 管理者はユーザに接続できない端末のIP アドレスと室名を聞く. 次に, 管理者は, MARS を用いてIP アドレスと室名から端末を検索し,利用履歴, エッジスイッチのポート, アドレス, 端末のMAC アドレスの確認をおこなう. この結果から障害原因を判断することができる. 正常であると確認できた場合は原因が不明なため端末のある現地に調査しに行く必要がある. この様な手順で管理者は, 障害の特定をおこなうことができる.

7. 運用実験

本研究では, 実装したシステムの運用実験をした. 本章では, 運用実験の内容と結果を報告する.

7-1. 実験内容

提案システムを本学内ネットワークに適用し, 運用実験をおこなった. 同実験では, 提案システムを組み合わせたMARS を用いて, 障害に対応した. 加えて, 昨今では管理者側のスイッチとユーザ側の端末が, 高性能なギガビット以上のイーサネット規格である機器が, 多く使われている. しかし, 管理者側のスイッチとユーザ側の端末の間に, 低性能な10Mbps や100Mbps などのハブを設置している場合がある. これが原因でスイッチのポートがシャットダウンして通信できない場合がある. したがって, これらの障害を予防するために,障害が発生する可能性のある端末を1 月 19 日～1 月 26 日の期間に接続された情報を基に調査した. 調査した項目を下記に示す.

(1) 端末のSpeed が10Mbps, Duplex がfullDuplex の場合
(2) 端末のSpeed が100Mbps,Duplex がfullDuplex の場合

7-2. 実験結果

前述で述べた実験をおこなった結果, 第6.4 節で述べたような障害特定の手順に
基づいて, 障害に対応することができた. その結果障害原因を特定するうえで管理者への負担を軽減することができた. 加えて, 調査項目(1),(2) についての結果
を以下に述べる.

調査項目(1)

実環境から得られた結果を図 7.1 に示す. この図からSpeed が10Mbps,Duplex がfullDuplex であることが確認できる. 接続された件数は 62 件であることが確認できた.

全62件

No.	Host Name	IP Address
1	[redacted].wakayama-u.ac.jp	133.42.[redacted]
2	[redacted].wakayama-u.ac.jp	133.42.[redacted]
3	[redacted].wakayama-u.ac.jp	133.42.[redacted]
4	[redacted].wakayama-u.ac.jp	133.42.[redacted]
5	[redacted].wakayama-u.ac.jp	133.42.[redacted]
6	[redacted].wakayama-u.ac.jp	133.42.[redacted]
7	[redacted].wakayama-u.ac.jp	133.42.[redacted]
8	[redacted].wakayama-u.ac.jp	133.42.[redacted]

Start Time	Stop Time	Speed	Duplex
2015-01-22 14:26:37	2015-01-22 17:49:39	10	fullDuplex(3)
2015-01-22 16:33:45	2015-01-22 16:34:05	10	fullDuplex(3)
2015-01-23 08:13:10	2015-01-23 13:02:12	10	fullDuplex(3)
2015-01-22 07:52:23	2015-01-22 19:40:36	10	fullDuplex(3)
2015-01-22 10:43:27	2015-01-22 11:37:05	10	fullDuplex(3)
2015-01-21 19:28:53	2015-01-21 20:06:56	10	fullDuplex(3)
2015-01-25 13:22:22	2015-01-25 13:29:35	10	fullDuplex(3)
2015-01-24 14:37:15	2015-01-24 22:15:11	10	fullDuplex(3)

図 7.1： 調査結果(1)

調査項目(2)

実環境から得られた結果を図 7.2 に示す. この図からSpeed が100Mbps , Duplex がfullDuplex であることが確認できる. 接続された件数は1046 件あることが確認できた.

全1046件

No.	Host Name	IP Address
1	[redacted].wakayama-u.ac.jp	133.42.[redacted]
2	[redacted].wakayama-u.ac.jp	133.42.[redacted]
3	[redacted].wakayama-u.ac.jp	133.42.[redacted]
4	[redacted].wakayama-u.ac.jp	133.42.[redacted]
5	[redacted].wakayama-u.ac.jp	133.42.[redacted]
6	[redacted].wakayama-u.ac.jp	133.42.[redacted]
7	[redacted].wakayama-u.ac.jp	133.42.[redacted]
8	[redacted].wakayama-u.ac.jp	133.42.[redacted]

Start Time	Stop Time	Speed	Duplex
2015-01-25 02:16:14	2015-01-26 02:15:25	100	fullDuplex(3)
2015-01-24 02:16:15	2015-01-25 02:15:25	100	fullDuplex(3)
2015-01-24 02:16:15	2015-01-25 02:15:25	100	fullDuplex(3)
2015-01-23 02:16:14	2015-01-24 02:15:25	100	fullDuplex(3)
2015-01-23 02:16:14	2015-01-24 02:15:25	100	fullDuplex(3)
2015-01-22 12:25:30	2015-01-22 13:02:07	100	fullDuplex(3)
2015-01-19 17:58:28	2015-01-19 23:26:03	100	fullDuplex(3)
2015-01-19 10:00:02	2015-01-21 20:44:12	100	fullDuplex(3)

図 7.2： 調査結果(2)

以上の結果から, 障害原因となり得る端末が存在することが確認できた. これ
らの端末を対処することにより, 障害を予防することができる.

8. 評価・考察

本章では, 本研究で実装したシステムの評価および考察をおこなう.

8-1. 評価

本節では, 本研究で実装したシステムと第2 章で述べた既存技術の比較評価をおこなう. 加えて, 先行研究であるMARS との比較評価をおこなう.

8-1-1. 既存技術との比較

第2 章で述べた統合監視システムでは, 各端末から通信速度や, 通信方式などの情報を取得する. そのため, 全ての端末を把握し, それぞれに専用のエージェントをインストールする必要がある. しかし, 利用申請をせず, 不正に接続するユーザは少なからず存在する. そのため, 接続情報を把握することも困難である.

本研究では, エッジスイッチからスイッチ情報を取得する. そのため, ユーザの端末から直接通信速度や通信方式を取得するのではなくエッジスイッチからスイッチ情報を取得した. よって, 不正接続した端末の情報を取得するこ

とができる．したがって本研究は既存技術のようにユーザ制限を設けない点と，専用のエージェントをインストールする必要がない点で優れている．

8-1-2. MARS との比較

第 7.1 節で述べたように，管理者側のスイッチとユーザ側の端末の間に低性能なハブを設置している場合に，膨大な量の通信をおこなうと，ポートがシャットダウンしてしまい通信ができない．これを特定するためには，過去に該当するポートで接続されていたスイッチの情報が必要となる．しかし，第 3 章で述べた MARS では，スイッチ情報を取得していない．そのため，過去に遡ってスイッチの情報を確認できない．本研究では，スイッチ情報を取得し，MARS と関連付けることで，過去のスイッチ情報を確認できる．これにより，MARS を用いるだけでは切り分けできなかった障害原因を特定することができた．したがって，本研究は従来の MARS よりも障害原因を特定する点で優れている．

8-2. 考察・今後の課題

本研究では，スイッチ情報を取得する提案システムを実装した．提案システムにより，端末のスイッチ情報を取得することができ，MARS のみで障害原因を特定できるようになった．これにより，さらに管理者の負担を軽減できるのではないかと考えている．しかし，提案システムでは，改善すべき課題がある．これらを以下で述べる．

8-2-1. スイッチへのログイン

本研究では，障害原因を特定するために，第 6.4 節で述べたような手順で調査する．しかし，(5),(6) のような原因を特定，解決するためには，スイッチへのログインが必要な場合がある．提案システムを用いることで(5),(6) のような原因を予測することはできるが，実際にポートがシャットダウンしているかどうかを確認できない．これより，原因を解決するにはスイッチにログインする必要があるため，管理者は多大な時間を要する．したがって，これらの障害原因を解決するために，エッジスイッチのポート状態の確認，該当するポートの復旧ができるようにすることで管理者への負担を軽減することできると考えられる．加えて，スイッチのログイン情報を把握していない管理者でも，障害原因を特定し，解決することができると考えられる．

8-2-2. スイッチ情報の精度向上

本研究では，1 分おきにリンクのアップダウン情報を監視し，スイッチの情報を取得している．そのため，SNMP で情報を取得する際に，何度かリンクのアップダウンが起きていた場合，最後に接続された端末のスイッチ情報を取得する．そのため，頻繁にケーブルなどの挿抜が起きたことは確認できるが，端末が変更された場合は確認できない．よって，リンクのアップダウンが起こったと同時に SNMP でスイッチ情報を取得できるようにすることでより正確な情報を取得できると考えられる．

9. おわりに

本研究では，スイッチの情報をリアルタイムで監視し，管理者を支援するシステムを構築した．エッジスイッチの監視と先行研究の MARS との連携による手法を提案し，エッジスイッチにログインすることなく MARS のみで障害原因を特定できることを確認した．既存技術のようにユーザ制限を設けない点と，専用のエージェントをインストールする必要がない点で本研究の有用性を示した．加えて，本提案システムの新規性を示した．今後は，スイッチ情報を取得する精度を向上できるようにシステムを改良していきたいと考えている．

参考文献

[1]. 吉田祐亮 ”ネットワーク接続監視システム MARS の構築”，2012 年度修士論文和歌山大学大学院システム工学研究科

[2]. 吉田祐亮 ”組織内ネットワークにおける端末監視システム MARS の構築と運用”，電子情報通信学会技術研究報告．IN，情報ネットワーク，Vol.11，No.245，pp.37-42，2011

[3]. 川橋裕，坂田渉 ”組織内ネットワークにおける端末監視システム MARS の構築と運用”，学術情報処理研究 Journal for academic computing and networking，No.18，pp.81-89，2014

[4]. 續木涼太，泉裕，齋藤彰一，塚田晃司，“組織内ネットワークにおける MAC アドレストレースバックシステムの開発”，情報処理学会研究報告．DSM，[分散システム/インターネット運用技術] Vol. 2005，No.31，pp.13-18，2005

[5]. ”Nagios - The Industry Standard in IT Infrastructure Monitoring ”
http://www.nagios.org/

[6]. ”ZABBIX-JP | Japanese Zabbix Community ”
http://www.zabbix.jp/

[7]. ”SNMP Research{Secure Internet and Network Specialists ”
http://www.snmp.com/

[8]. ”rsyslog ”
http://www.rsyslog.com/

[9]. ”Remote Authentication Dial In User Service (RADIUS) ”
http://tools.ietf.org/html/rfc2865

[10]. ”The Perl Programming Language ”
http://www.perl.org/

[11]. ”PHP: Hypertext Preprocessor ”
http://php.net/

[12]. ”Cisco Systems ”
http://www.cisco.com/

[13]. ”Welcome to The Apache Software Foundation! ”
http://www.apache.org/

[14]. ”Net-SNMP ”
http://www.net-snmp.org/

[15]. ”MySQL :: Developer Zone ”
http://www.mysql.org/