C-08

高頻度なリンクアップとリンクダウンをおこなう端末を擁するネットワーク監視に基づく MARS の拡張

Extension of function of “MARS” based on monitoring management network which is connected to terminals high-frequency perform link-up and link-down

石田 慎秀†　　川橋 裕‡
Chikahide Ishida　Yutaka Kawahashi

1. はじめに

情報化社会への進展に伴い，様々な組織運用において LAN は必要不可欠なものとなっている．同時にユーザも，提供される LAN に対して個々の多様な目的に適した環境を構築するようになった．したがって，ネットワーク管理者はネットワーク障害が発生した際に，自身が運用するバックボーンネットワークだけでなく，エンドポイントであるユーザ端末にも注意を払わなければならなくなった．ネットワーク管理者はユーザから報告されるネットワーク障害に対して，原因はユーザ側に存在するのか，管理者側のバックボーンネットワークに存在するのかといった障害原因の切り分けをおこなわなければならない．そのため，管理者は障害発生時および発生前後の LAN 内の状態を調査し，障害原因の切り分けに必要な情報を可能な限り収集する必要がある．しかし，これには多くの時間が必要となる．

和歌山大学では先行研究である MARS(Monitoring, Analysis and Response System)[1]を運用することで，各ユーザ端末のネットワーク接続を監視している．MARS では，LAN 内の端末の IP アドレス，MAC アドレス，場所，利用時間をリアルタイムで記録および保存している．これらにより管理者は障害発生時に早急に障害原因の切り分けを行う事が出来る．しかし，MARS を用いても障害発生時に，管理者が LAN 内に存在する端末の接続状況を把握する事が困難な場合が存在する．その一つに，正規の利用でありながら，ユーザ側の利用目的によっては，端末がリンクアップとリンクダウンを高頻度で繰り返すことがある．MARS では一度のリンクアップからリンクダウンまでの時間を利用時間として記録している．したがって，高頻度で端末がリンクアップとリンクダウンを繰り返す場合，短期間のログの中に同一端末の接続情報が大量に含まれることになる．障害のため，早急に接続端末を把握したい場合，管理者はこの大量の情報の中から必要な情報を適宜選択していかなければならない．これには多くの時間と管理者への負担が伴う．

本研究では，リンクアップとリンクダウンを高頻度で繰り返す端末を擁する LAN 内において，必要な情報を迅速に収集する事が可能な情報管理によって，ネットワーク管理者の負担を軽減する事を目的とする．MARS 上の接続情報から，リンクアップとリンクダウンを高頻度で行う端末の動作は 3 つのカテゴリに分類できるという事を発見した．提案する MARS の拡張システムではこれらの端末の接続情報を必要に応じて分離し，カテゴリ分けが行われた情報を管理者に提示する．これにより高頻度なリンクアップとリンクダウンを繰り返した場合の，大量の情報の中でも，ネットワーク管理者は必要な情報を迅速に収集する事が出来る．

本論文では提案したシステムの実装および評価について述べる．

2. 技術概要

本節では，本研究を進めるにあたり，基礎となる技術を述べる．

2.1 総合監視システム

総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，既存の総合監視システムについて述べる．

2.1.1 Nagios

Nagios[2]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[3]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がある．

2.1.3 MAC-IP 監視管理システム

MAC-IP 監視管理システム[4]は，研究室内などでの端末の接続管理を，機器管理責任者の管理の下におこなう，分散管理によりシステム管理者の負荷を分散させている．また，MAC アドレスや設置部屋を Web 上から簡単に登録することが出来る．

2.2 問題点

これらの総合監視システムは監視対象の端末を把握するため，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．しかし利用申請書を提出せずに勝手に IP アドレスを使用したり，申請内容に変更があった際にも申告をおこなわないといった，ユーザの不正利用が多発している．利用申請制の導入に際し，ユーザには利用申請書の提出を義務付けているが，これらの事例に対する抑止力にはなっていない．このため，管理者は端末の接続状況を正確に把握することが困難となっている．同時に，ネットワーク障害が発生した際に，管理者は障害の発生源を特定することが困難になっている．

3. 先行研究

本章では、ネットワーク接続を監視することにより障害原因の切り分けを支援する先行研究の MARS について述べる．

†和歌山大学大学院システム工学研究科
Graduate School of System Engineering Wakayama University

3.1　MARS

本節では MARS の動作と端末情報，および MARS の問題点について述べる．

3.1.1 動作と端末の接続情報

MARS は RADIUS 認証プロトコル[5]を用いて，エッジスイッチが通知する端末の接続情報を収集する．ここで，エッジスイッチとは組織内ネットワークの端末であり，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，ダイヤルアップによるリモート接続時の認証プロトコルである．近年ではダイヤルアップだけでなく，ブロードバンド接続や VPN，VLAN，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(課金管理)にも利用されている．

先行研究ではエッジスイッチにネットワーク認証の設定を施す．これにより RADIUS 認証プロトコルを利用した，エッジスイッチと MARS の連携を可能にする．エッジスイッチと MARS 間の動作を図 3.1 と下記に示す

(1) 端末がエッジスイッチに接続する
(2) エッジスイッチが接続要求を 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) エッジスイッチは端末が接続開始，または終了した事実を MARS に通知する

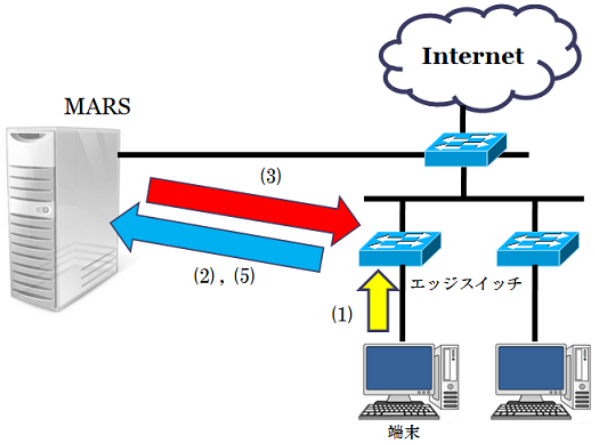

図 3.1 MARS の動作手順

動作手順(2)における認証では，RADIUS サーバは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．接続要求の際にエッジスイッチが MARS に通知する情報を下記に示す．

・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
・接続開始もしくは終了状態
・接続開始もしくは終了時刻

MARS はエッジスイッチから収集した情報を，パッチ情報と連携することにより，端末の接続場所である部屋名を特定する．また，端末が接続を開始してから終了までの時間をセッションとして定義している．収集される端末の接続情報は各セッションごとに管理している．端末の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

端末の接続開始が通知されると，MARS は上記で示した管理項目のうち接続終了時刻を除く情報をデータベースに格納する．端末の接続終了が通知されると，セッション ID と端末の IP アドレスが一致するレコードに終了時刻を追加する．

3.1.2 インタフェース

MARS は管理インタフェースを Perl[6]および PHP[7]で記述した Web アプリケーションにより実装している．したがって，OS への依存性が少なく，特別なソフトウェアを必要としない．管理インタフェース上で提示される情報を下記に示す．

・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

管理者は，提示された情報を基に障害特定をおこなう．第 3.1.1 項で示したように，収集される端末の接続情報は，接続開始から接続終了までの各セッションごとに管理している．実際に管理者が閲覧できるインタフェース画面を図 3.2 に示す．

図 3.2 MARS のインタフェース画面

3.1.3 問題点

MARS はインタフェース画面に提示される情報から，管理者が LAN に接続した端末の各セッション時の情報を把握できる仕組みとなっている．しかし，これらは各セッションごとに情報が分けられているため，端末がリンクアップとリンクダウンを高頻度に繰り返すと，セッションを記録するレコード数が大幅に増加することになる．この状態が発生すると，管理者が特定の時間にセッションをおこなっていた端末を検索したい場合，検索結果内に大量の同一端末による接続情報が提示される．管理者はこの大量のレコードを一つずつ確認し，必要な情報を適宜選択しなければならないため，大きな負担となっている．

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．そのためには迅速かつ正確なネットワークの状況把握が必要となる．そこで，本学では第 3 章で述べた 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 を利用しても，管理者がネットワークの状況を把握するために，大きな負担がかかる場合がある．MARS では LAN へのリンクアップからリンクダウンまでの通信を一つのセッション情報として管理している．したがって，エッジスイッチに対して，リンクアップとリンクダウンを高頻度に繰り返す端末が LAN 内に存在する場合，同一端末からの大量の接続情報が MARS に蓄積されることになる．管理者は，この大量の接続情報を含むデータ群を一つずつ確認し，障害対応に必要な情報を抽出しなければならない．これは管理者に大きな負担がかかる．よって，管理者への負担を軽減するために，同一端末からの頻繁なセッションによる接続情報をシステム側で抽出し，管理者が扱いやすい情報へと変換したうえで提示する必要がある．

本研究では，高頻度なリンクアップとリンクダウンをおこなう端末を擁するネットワーク環境下においても，管理者の負担を最低限に抑える接続情報を MARS に提示させることで，管理者の障害対応を支援することを目的とする．

5. 提案手法

本章では，第 4 章で述べた目的を実現するための手法を述べる．

5.1 接続情報の管理手法

LAN の利用目的によっては，高頻度なリンクアップとリンクダウンを繰り返す端末が接続される場合がある．これにより，同一端末からの大量のログが MARS に蓄積される．しかし，正規な利用であるにもかかわらず，そのような挙動を行う端末に対して干渉すると，ユーザの求める利用環境が制限される可能性がある．よって，高頻度なリンクアップとリンクダウンをおこなう端末が使用される前提で，システム側で収集した接続情報を管理する必要がある．したがって，高頻度な短時間の連続セッションによる，大量の情報をそのまま管理者へ提示するのではなく，より少ないレコード数へと集約したうえで，管理者に情報提示をおこなう手法を提案する．

5.1.1 接続情報の特徴

短時間内にリンクアップとリンクダウンをおこなう端末は，本学で実際に運用されている MARS においても複数確認されている．ここで述べる短時間内とは，5 分以内にリンクアップとリンクダウン，および再リンクアップがおこなわれる挙動とする．管理インタフェースより提示される情報を収集および分析したところ，その挙動は大きく三つのカテゴリに分類できることを発見した．提案手法では，これらの特徴を持つ接続情報を分類したのち，接続情報を管理者に提示する．三つのカテゴリを以下に定義する．

(1)複数 IP アドレス所持型

一つの MAC アドレスを持つ端末が複数の IP アドレスを短時間の間に何度も切り替えるもの．一つの IP アドレスによるセッション終了直後に別の IP アドレスでセッションを開始する．三つのカテゴリのうち最もリンクアップとリンクダウンの頻度が高い．実際に本学の MARS にて観測されたレコードを図 5.1 に示す．

IP Address	MAC Address	SW IPaddr	SW Port	Start Time	Stop Time
192.[redacted].71	6c70.9[redacted]dbd	133.[redacted].205	Gi0/6	2016-11-11 23:30:20	2016-11-11 23:30:33
192.[redacted].74	6c70.9[redacted]dbd	133.[redacted].205	Gi0/6	2016-11-11 23:29:12	2016-11-11 23:30:20
192.[redacted].71	6c70.9[redacted]dbd	133.[redacted].205	Gi0/6	2016-11-11 23:28:43	2016-11-11 23:29:12
192.[redacted].74	6c70.9[redacted]dbd	133.[redacted].205	Gi0/6	2016-11-11 23:27:51	2016-11-11 23:28:43

図 5.1 複数 IP アドレス所持型

(2)定期的リンクアップ型

前回のリンクアップ時刻から 5 分以内に一定の時間周期で再度セッションを開始する．リンクアップからリンクダウンまでの時間は不定期だが，連続したセッションのリンクアップ時刻の差は一定である．稀に長時間のセッションも見られる．また，同様の挙動を行う端末の MAC アドレスを分析したところ同一ベンダーである．実際に本学の MARS にて観測されたレコードを図 5.2 に示す．図 5.2 では 4 分 30 秒ごとにリンクアップを繰り返している．

IP Address	MAC Address	SW IPaddr	SW Port	Start Time	Stop Time
133.[redacted].187	1cb1.[redacted]9b1	133.[redacted].210	Gi0/26	2016-12-05 20:49:50	2016-12-05 20:52:50
133.[redacted].187	1cb1.[redacted]9b1	133.[redacted].210	Gi0/26	2016-12-05 20:45:20	2016-12-05 20:48:20
133.[redacted].187	1cb1.[redacted]9b1	133.[redacted].210	Gi0/26	2016-12-05 20:40:50	2016-12-05 20:43:50
133.[redacted].187	1cb1.[redacted]9b1	133.[redacted].210	Gi0/26	2016-12-05 20:36:20	2016-12-05 20:39:20

図 5.2 定期的リンクアップ型

(3)不定期型

(1)複数 IP アドレス所持型および(2)定期的リンクアップ型のいずれの特徴にも当てはまらないもの．短時間内に何度もリンクアップとリンクダウンを繰り返すこと以外に一貫性はみられない．

5.1.2 分類方法

第 5.1.1 項で分類した接続挙動の分類方法について図 5.3 と下記で説明する．

(1) 同一 MAC アドレスによるセッション通信で，前回のリンクアップ時刻から，5 分以内にリンクアップが行われている
(2) 同一 MAC アドレスによるセッション通信で，前回の接続時とは異なる IP アドレスを使用している
(3) リンクアップ時刻が常に等間隔である

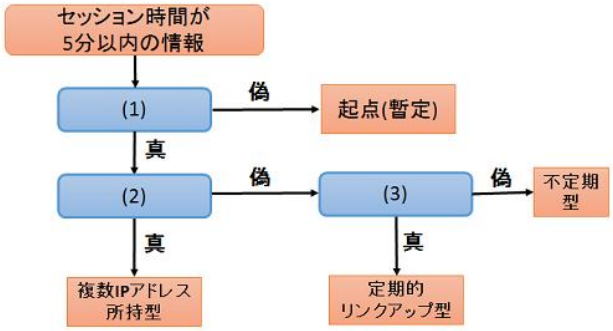

図 5.4 分類方法

MARS で収集された情報のうち，セッション時間が 5 分以内の記録にのみカテゴリ分けを適用する．最初に，(1)の条件を満たしているか判定する．満たす場合，短い期間にリンクアップとリンクダウンを繰り返したと判定する．満たさない場合は短時間にリンクアップとリンクダウンを繰り返してはいないが，このセッションが繰り返す挙動の最初の 1 回目である可能性が存在する．したがってこのセッションを，連続したリンクアップとリンクダウンの起点として暫定的に扱う．次の同一 MAC アドレスからのセッションが，いずれかのカテゴリに分類されたとき，暫定的に起点として扱っていたセッションを最初の 1 回目として確定させる．(1)を満たすセッションのうち，(2)を満たすものを複数 IP アドレス所持型と分類する．また，(2)を満たさずに(3)のみを満たすものを定期リンクアップ型と分類する．最後に(2)および(3)の両方を満たさないものを不定期型と分類する．これらの分類を行ったのち，データベースに情報を格納する．

5.1.3 情報の提示手法

短時間内にリンクアップとリンクダウンの繰り返しがおこなわれた際，その一連の情報を統合したレコードを生成する．統合したレコードでは，挙動の起点となったセッションの開始時刻と，一連の挙動の最後におこなわれたとされるセッションの終了時刻までを，一つのセッションとして表示する．また，レコード内に内包されているセッション数および，第 5.1.2 項で示した分類結果を表示する．これにより，リンクアップとリンクダウンが高頻度で繰り返されたことによる大量のセッション情報を，一つのレコードに集約することが出来る．統合する前の実際のレコード群を図 5.4 に，統合後のレコードを図 5.5 に示す．

IP Address	MAC Address	Building	Place	SW IPaddr	SW Port	Start Time	Stop Time
169.254.185.18	0420.9a45.2120			172.16.20.20	Gi1/0/11	2017-02-07 15:07:28	2017-02-07 15:09:43
169.254.185.18	0420.9a45.2120			172.16.20.20	Gi1/0/11	2017-02-07 15:04:23	2017-02-07 15:06:52
169.254.185.18	0420.9a45.2120			172.16.20.20	Gi1/0/11	2017-02-07 15:01:26	2017-02-07 15:03:46
169.254.185.18	0420.9a45.2120			172.16.20.20	Gi1/0/11	2017-02-07 14:58:32	2017-02-07 15:00:49
169.254.185.18	0420.9a45.2120			172.16.20.20	Gi1/0/11	2017-02-07 14:55:30	2017-02-07 14:57:53
169.254.185.18	0420.9a45.2120			172.16.20.20	Gi1/0/11	2017-02-07 14:52:37	2017-02-07 14:54:53

図 5.4 情報統合をおこなう前の接続情報

IP Address	MAC Address	Building	Place	SW IPaddr	SW Port	Start Time	Stop Time	カテゴリ	遷移UD回数
169.254.185.18	0420.9a45.2120			172.16.20.20	Gi1/0/11	2017-02-07 14:52:37	2017-02-07 15:09:43	3	6

図 5.5 情報統合をおこなった後の接続情報

情報を集約したレコードを，一連の挙動による大量のレコードの代わりに表示することで，MARS 上で管理者が接するレコード数を減少させる．これにより管理者が，同一端末による大量の接続情報から特定の情報を抽出する状況を避けることが出来る．また，情報が統合されたレコードに内包されている短時間のセッション数およびその挙動の特徴も把握する事が出来る．しかし，情報の統合により，本来表示されていた短期間内のリンクアップとリンクダウン個々の時間情報が提示されなくなる．つまり，もし障害特定の際にこれらの情報が必要となる場合は，正確な情報を管理者が把握できなくなる．したがって，本システムでは従来の管理情報と併用して，統合時の情報を別途に閲覧できる管理インタフェースとする．

5.2 セッション情報の処理

第 5.1.2 項で述べた接続挙動の分類，および第 5.1.3 項で述べた，情報を統合したレコード生成のためのセッション情報の処理手順を図 5.6 と下記に示す．

(1)前回のセッション情報の参照
(2)セッション分類の確定
(3)情報統合
(4)管理者への情報提示

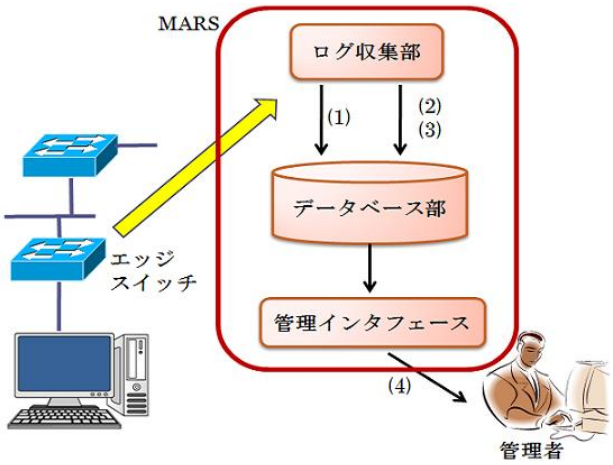

図 5.6 システムの処理手順

本節では上記で示した，前回のセッション情報の参照，セッションの分類，情報統合の処理内容および管理者への情報提示手法の各処理内容について説明する．

(1)前回のセッション情報の参照
この処理はMARSにおいて，接続開始情報が格納される直前におこなう．MARSに記録されている，同一のMACアドレスによる前回のセッション情報を参照する．この情報をもとに，今回のセッションに対して，第5.1.2項で述べた分類方法を適用する．ただし，ここでの処理はリンクダウン時刻が格納される前であるため，短時間のセッションであるかどうかは未確定である．したがって，暫定的に処理中のセッションの時間を5分以内であるとして，接続情報のカテゴリ分けをおこなう．セッション時間が5分以内であると確定したとき，ここでのカテゴリ分類を正しいものであると決定する．また，第5.1.3項で示したように，管理者に情報提示を行う際，統合したレコードは内包しているセッションのレコード数を提示する．このレコード数を連続セッション番号と定義する．ここではレコードの統合の際，連続セッション番号を算出するために，一時的に前回のセッションにおける連続セッション番号も接続開始情報とともに格納する．

(2)セッション分類の確定
この処理は，MARSにおいて，接続終了情報が格納される直前におこなう．リンクアップからリンクダウンまでの時間差を算出する．この値が5分以内であった場合短時間のセッションであると判断できる．短時間のセッションであると判断された場合，(1)でおこなったカテゴリ分類を確定情報として保存する．また，短時間のセッションでなかった場合は，このセッションをカテゴリ分類の対象外として保存する．次に連続セッション番号を算出する．(1)の処理にて前回の連続セッション番号が格納されているため，この値をインクリメントして，このセッションの連続セッション番号として格納する．短時間のセッションでない場合は0を格納する．

(3)情報統合
この処理は，エッジスイッチからMARSに通知される接続終了情報を，格納した直後におこなう．格納された接続情報が，連続した短時間におけるリンクアップとリンクダウンの繰り返しの一部であった場合，接続情報を一つのレコードに集約する処理をおこなう．格納された接続情報の連続セッション番号が2であった場合，短時間にセッションを繰り返したと判断できる．よって，一連のセッションを集約するためのレコードを生成する．このレコードを統合レコードと定義する．統合レコードは連続セッション番号が1である，短時間にリンクアップとリンクダウンを繰り返す挙動の起点となったセッションのレコードを複製して，これをベースとする．このベースレコードの連続セッション番号を2へ，接続終了時刻を連続セッション番号が2のレコードに保存されている時刻に変更する．以降連続セッション番号が3以上のレコードが格納されるたびに，統合レコードの連続セッション番号と接続終了時刻を更新する．

(4)管理者への情報提示
第5.1.3項でも述べたとおり，統合された情報だけでは把握できない情報も一部存在する．したがって従来の管理インタフェースと併用して統合時の情報のみを別途に閲覧できるモードを追加する形で実装する．統合時の情報を閲覧できるモードでは，カテゴリ分類の対象外レコードと統合レコードのみを表示する．

6. 運用実験
本章では，提案手法を実装するにあたり必要な動作環境および，運用実験の内容と結果を述べる．

6.1 ネットワーク環境
エッジスイッチとなる機器にCisco[8]社製Catalystスイッチを用いた，提案システムを実装するためにはMARSが動作するための環境が必要である．MARSを動作させるためにスイッチが認証機能を有している必要があるため，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 3560 (Cisco IOS 12.2(50)SE 以降)
・Catalyst 2960 (Cisco IOS 12.2(50)SE 以降)

6.2 ソフトウェア環境

5章で述べた提案手法をオープンソフトウェアのApache[9]，MySQL[10]，rsyslogを用いて実装した．いずれも広く利用されており，安定性が高い．提案システムはこれらの環境にbash[11]，PerlおよびPHPを用いて実現した．

6.3 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，高頻度なリンクアップとリンクダウンを繰り返す端末が，複数接続されているエッジスイッチから，収集される端末接続情報を観察する．提案手法を実装した場合のインタフェース画面と，従来のインタフェース画面によって提示されるそれぞれのレコード数を比較する．実験は2月10日12:00から13:00までの1時間でおこない，その間に接続された端末の情報をMARSに提示させ，管理者の負担を調査する．

6.4 実験結果
実験内容にて示した実験をおこなった結果，従来のMARSによる情報提示と，提案手法による情報提示に以下のような差が出た．

・従来のMARSによる提示レコード
実験時間内の接続を示すレコード数は全部で28件確認できた．

・提案手法による提示レコード
実験時間内の接続を示すレコード数は全部で6件確認できた．

従来のMARSによって提示された接続情報は非常に数が多く，実験中に接続された端末をすべて把握するためには，レコードを順番に確認し，一度確認した端末であるかどうか，メモを取らなければならないほどであった．提案手法による情報提示はレコード数が圧倒的に少なく，実験中に接続された端末をすべて把握するまでにほとんど時間を必

要としなかった．したがって，従来の MARS に比べて管理者にかかる負担を軽減することができた．

7. 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．

7.1 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および先行研究の MARS との比較評価をおこなう．

7.1.1 既存技術との比較

第 2 章で述べた総合監視システムでは，各端末から通信速度や，通信方式などを取得する．そのためにはあらかじめ全ての端末を把握しておかなければならない．しかし，利用申請をせずに，不正に接続するユーザが後を絶たない．そのため，接続情報を正確に把握する事は困難である．

本研究では，先行研究である MARS を利用している．これにより，管理者が負担なく正確な情報を得るために，ユーザに対して制限を設ける必要がない点で優れている．

7.1.2 MARS との比較

第 3 章で述べたとおり，MARS は端末がリンクアップをしてからリンクダウンをおこなうまでを 1 セッションの情報として保存している．管理者は障害対応の際に，MARS から提示される各セッション情報の中から必要な情報を適宜選択することとなる．しかし，ネットワーク内にリンクアップとリンクダウンを高頻度で繰り返す端末が存在すると，同端末からの大量のセッション情報が蓄積される．これにより，管理者は同端末からの大量のセッション情報を含有した情報群から，一つずつ要否の判断をおこない，情報の抽出をおこなわなければならなくなる．本研究では，これらの同端末による高頻度なリンクアップとリンクダウンの繰り返しによる情報を一つのレコードへと集約して管理者へ提示するため，過剰な数のセッション情報を管理者が閲覧する必要がなくなる．したがって，管理者に負担がかからないという点で優れている．

7.2 考察・今後の課題

本節では，本研究の考察と今後の課題を述べる．

7.2.1 カテゴリ分類の精度向上

本研究では，情報を統合する際に一連のセッションの挙動によるカテゴリ分けをおこない，これを管理者に提示する手法を提案した．しかし，同じ挙動をおこなっていたとしても，これらが同じ要因によるものであるとは限らない．また，具体的な共通点のないものを不定期型として分類している．すなわち，セッション時間の観点から見える特徴と使用 IP アドレスの変化といった情報による分類だけでは，同じカテゴリであると正確に決定するには情報が不足している．より正確なカテゴリ分けをおこなうためには別の観点からの情報を増やす必要がある．その情報の候補としてベンダーコードが挙げられる．本学内における定期リンクアップ型の挙動をおこなう端末の共通点として，MAC アドレスが同一のベンダーに属していることが判明している．これを考慮すれば，ネットワーク機器による挙動であるのか，ソフトウェアによるものであるのかといった判別が可能だと考えられる．また，他にもセッション中の端末の通信状況といった情報が挙げられる．TRAFL[12]などのパケットキャプチャが可能なシステムから得られる情報を参照し，接続中の通信に使用される送信先のポート番号や，通信先に注意すれば，何を目的とした接続であるのか絞ることができると考えられる．そして同時に，接続の目的が分かれば，どういった意図および原因によってリンクアップとリンクダウンを繰り返しているのかといった，より精度の高いカテゴリ分けができると考えられる．

8. おわりに

本研究では，高頻度なリンクアップとリンクダウンを繰り返す端末を擁するネットワークにおいても，管理者に負担がかかることのない MARS による情報提示を可能とした．リンクアップとリンクダウンを繰り返す一連の挙動の特徴をカテゴリに分類し，セッション情報を一つのレコードに統合したうえで提示する手法を提案した．これにより従来の MARS よりも，管理者が要否を判断していかなければならないレコード数を減少させることが確認できた．既存研究のようにユーザに対して制限を設ける必要がない点で有用性を示した．今後は，リンクアップとリンクダウンを繰り返す端末挙動の分類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．

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] ″Nagios - The Industry Standard in IT Infrastructure Monitoring″,http://www.nagios.org/
[3] ″ZABBIX-JP - Japanese Zabbix Community″, http://www.zabbix.jp/
[4] 清水さや子 ″キャンパスネットワーク運用評価と MAC-IP 監視管理システムの構築″
学術情報処理研究 Journal for academic computing and networking
[5] ″Remote Authentication Dial In User Service (RADIUS)″,
http://tools.ietf.org/html/rfc2865
[6] ″The Per Programming Language″,http://www.perl.org/
[7] ″PHP: Hypertext Preprocessor″, http://php.net
[8] ″Cisco Systems″, http://www.cisco.com/
[9] ″Welcome to The Apache Software Foundation!″, http://www.apache.org/
[10] ″MySQL :: Developer Zone″, http://www.mysql.org/
[11] ″GNU Bash″, http://www.gnu.org/software/bash/
[12] 釼本 倫章 ″トラフィックグラフとフローに基づくネットワーク管理支援システム TRAFL の構築と運用″
2015 年度修士論文 和歌山大学大学院システム工学研究科