無線 LAN 接続状況の可視化と無線 LAN アクセスポイントの動作解析

Visualization of Wireless LAN access and Behavior Analysis of Wireless LAN access points

内藤郁之†，望月源†‡，佐野洋†‡
Takashi Naito†, Hajime Mochizuki†‡, Hiroshi Sano†‡

naito_takashi@tufs.ac.jp, motizuki@tufs.ac.jp, sano@tufs.ac.jp

†東京外国語大学総合情報コラボレーションセンター
‡東京外国語大学総合国際学研究院

†Information Collaboration Center, Tokyo University of Foreign Studies
‡Institute of Global Studies, Tokyo University of Foreign Studies

概要

本学では，無線 LAN アクセスポイントを学内に設置し，ユーザ向けにネットワーク接続を提供している．現行システムの導入後から無線 LAN アクセスポイントの障害が多発したことにより，原因究明および対策のため，アクセスポイントの動作状況の把握および動作解析を行った．さらに，無線 LAN アクセスポイント経由でアクセスしているユーザの一覧を取得するスクリプトの作成により監視精度の向上を図った．

キーワード

ネットワーク管理，無線 LAN，SNMP

1. はじめに

本学の無線 LAN アクセスポイントは，エッジスイッチを経由してコアスイッチに接続されている．特に無線 LAN を経由したアクセスは，個人持ち込みの PC およびスマートフォン，タブレットでの学内ネットワークへの接続に利用され，その安定性は日増しに高まっている．

本学において，当初，無線 LAN アクセスポイントの不具合が多発し，アクセスポイントがダウンしたため，状態の把握が必要となり，ネットワーク監視ソフトウエア以外に無線 LAN チェッカーの導入およびアクセスポイントのシステム情報を任意のタイミングで取得する監視用のスクリプトの作成，および取得した情報の可視化を行った．

2. ネットワーク構成

無線 LAN アクセスポイントとコアスイッチまでの物理接続は，PoE インジェクター，エッジスイッチを経由してコアスイッチ，認証スイッチと接続されている（図 1）．PoE インジェクター以外の機器は，SNMP の情報の

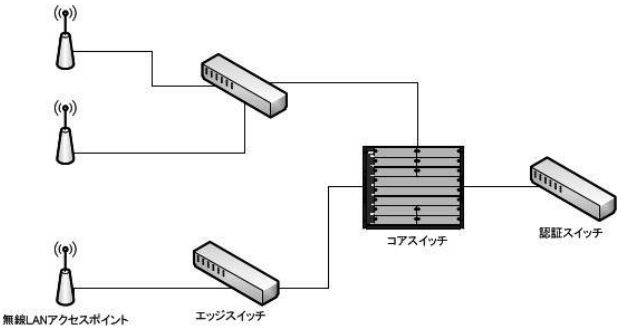

図 1 ネットワーク構成

取得，syslog へのログ転送機能があり，状態を把握することが可能である．これらの機器では，監視ソフトウエアによる死活監視および統計情報の取得をおこなっている. PoE インジェクターが, リモートから管理が行えず, 設置場所で動作 LED を確認する必要があり, 障害発生時の切り分けに手間がかかることが問題である.

ネットワーク機器の監視には，死活および流量監視に Nagios を利用し，流量の取得に Cacti を利用している．さらに，各機器で取得したログを syslog サーバに集約している．これらの構成を図 2 に示す.

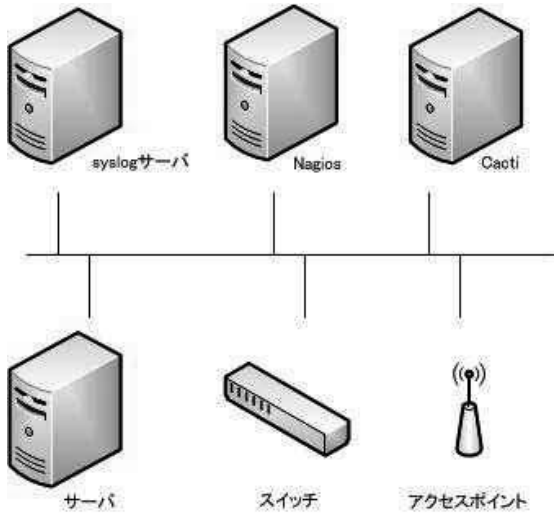

図 2 監視の構成

3. 無線 LAN 接続の障害の概要

無線 LAN 接続環境の障害は，無線 LAN アクセスポイントの機器の不良によるものと，その後の認証クライアント数の増加にともなうものがあり，それぞれ，以下に詳細を説明する.

3.1. 無線 LAN アクセスポイント

本学の無線 LAN アクセスポイントは, 2011 年 11 月まで，ダウンする機器が発生するという障害が頻繁に起こっていた．図 3～図 5 に 9 月から交換前までの 1 日あたりの障害発生件数を示す．この障害は，発生条件，発生頻度等には偏りが無く，原因究明は困難であり，対策の方を重視する運用を行っていた．対策は，ダウンしたアクセスポイントの電源を入れ直すというものであった．アクセスポイントのログは，syslog により syslog サーバに集約されていたが，syslog サーバでは，特にエラーに関する情報は確認できなかった．アクセスポイントのコンソールでログを表示させることが可能であり，これと syslog サーバに転送されたログの比較を行ったところ，一部のログだけが転送されていることが判明した．これに対し，スクリプトにより，任意のタイミングでログを取得することを試みた．最終的に，この障害は，機器の不良により発生したことが判明し，交換となったので，交換後は，発生していない.

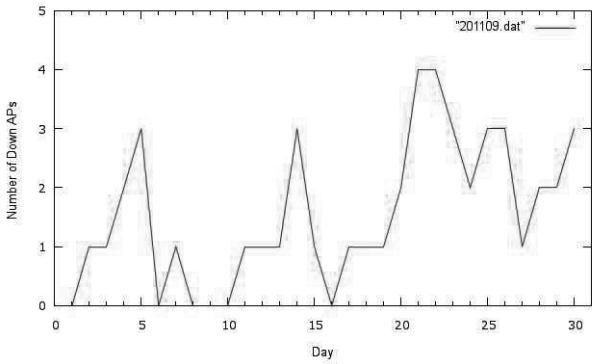

図 3　ダウンしたアクセスポイント数(9 月)

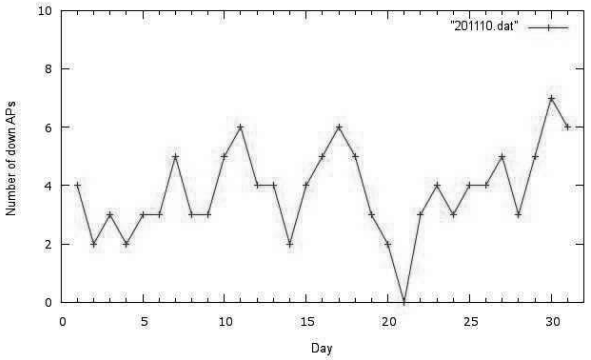

図 4 ダウンしたアクセスポイント数(10 月)

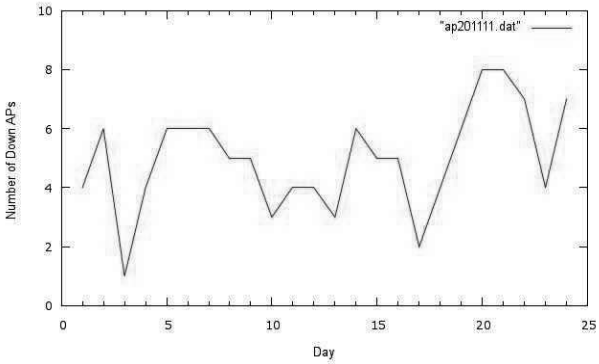

図 5 ダウンしたアクセスポイント数(11 月)

無線 LAN アクセスポイントの syslog 取得により，無線 LAN アクセスポイントとクライアントとのネゴシエーションの発生に関する動作が判明した．本学の無線 LAN 接続では，認証を行わなければ，ネットワークの利用はできないが，無線 LAN アクセスポイントは，クライアントとの通信を行い，クライアントに対して，アクセスポイントの存在を通知する．このとき，認証を行わなくても，アクセスポイントでは，検知されたクライアントとして扱われるので，人の集まる場所では，多数のクライアントが検出され，そのため，アクセスポイントの負荷の上昇につながっている．また，このアクセスポイントの仕様として ARP テーブルのリフレッシュが行われず，情報を蓄積していくため，適切なタイミングで電源を再起動する必要がある．

3.2. 認証スイッチの障害

認証スイッチの CPU 負荷の上昇(図 6)および新たな無線 LAN 接続のクライアントの認証不能という事態が発生した．これは，認証スイッチに認証の要求が届く件数が増加したためである．直接的な原因は，クライアントが増加したためであり，主に，無線 LAN 接続をサポートしているスマートフォンおよびタブレットの増加にともなうものである．また，これは，クライアントから DHCP での IP アドレス割り当て要求が発生し，その後，認証にリダイレクトされるようになっているが, ここで，認証の操作を行わない場合でも，認証の処理が行われるためである．この障害に対しては，スイッチの処理能力が限界に達したと判断し，より高性能の機器に入れ替えた．その結果，CPU 負荷の上昇は，発生はするものの 5 分以内に解消し，多くのユーザの認証を行える状況に好転した．

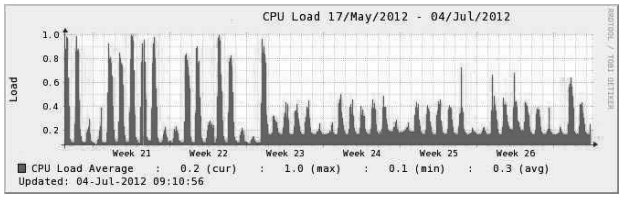

図 6　認証スイッチの負荷

4. 監視状況

監視は，リアルタイムに SNMP を利用した監視ソフトウエアによるものと syslog 転送機能を利用し，ログサーバでのログ確認の 2 本立てで行っている．

リアルタイムの監視では，Nagios による死活監視および流量監視と Cacti による流量監視を行っている. また，Nagios のアラートに対して，適宜，snmpwalk および ping 応答の確認を行っている．Nagios の監視条件は，以下のようになっている．

表 1 監視項目の設定

監視項目	間隔(分)
ping	5
ネットワーク流量	30
サービス	10

Nagios では，フラッピングの回避を行っているので，状態の変化から 30 分後に通知が発生するようになっている. Cacti では, 5 分間隔でネットワークの流量を取得し，流量グラフの出力に加えて，閾値監視として，一定の流量を継続して超えた場合に，メール通知を行う設定となっている．Nagios では，SNMP での流量監視は，変化率で評価するため，閾値監視を行う上では，扱いにくいので, 現在, ネットワーク監視に関しては, Nagios から Cacti へ移行を図っている．

4.1. 無線 LAN アクセスポイント

無線 LAN アクセスポイントの監視は，共通的な前述の設定に加え，任意に snmpwalk および ping の応答の確認を行っている．さらに，第 2 節で触れたように，syslog 転送を行っており，syslog サーバでログを集約している．現在，syslog で収集できるログは，無線 LAN アクセスポイントに関しては，アクセスポイント内に蓄積されているログの一部しか転送されない仕様であることが判明しているので，スクリプトにより，適宜，ログを取得するように変更している．

4.2. 認証スイッチ

無線 LAN アクセスポイントのセグメントに関しては，認証が一つのスイッチで行われるため，認証されたクライアント情報がスイッチに格納されている. この情報は，MIB で定義されているものの外部からアクセス不能に設定されており，同じ情報は，スイッチのコンソールからコマンドを入力することで閲覧することが可能となっている．この認証情報は，無線 LAN アクセスポイント経由のアクセスのほぼ現在の利用状況に一致する情報が取得できる．認証は，ユーザが切断しない場合，接続が確認できなくなってから解除されるまで 30 分の設定となっているので，一部，接続していないユーザも含まれていることになる．

4.3. 監視状況の可視化

Nagios および Cacti では，ウエブインタフェースにより結果が可視化されている．Nagios では，アクセスポイントの状態，また，Cacti では，パケット情報が可視化されている．一方，認証情報に関しては，前節で述べたようにスイッチのコンソールからコマンドを入力し確認する方法しかない．これに対し，認証情報を取得し，html ファイルとして出力し，管理用のウエブページに表示するようなプログラムを実装した．これは，Python およびシェルスクリプトにより実装し，認証が維持される最大時間 30 分の半分の 15 分間隔で cron により自動的に情報を更新する設定である．その結果，最大で，750 ユーザの認証が通っている状況になっている．スイッチで取得できる情報は，クライアントのユーザ ID，MAC アドレス，IP アドレス，接続先ポートである．これらの情報に加えて，コアスイッチの情報も取得して，マッチングを行い利用状況の可視化が行えればよいと考えている．

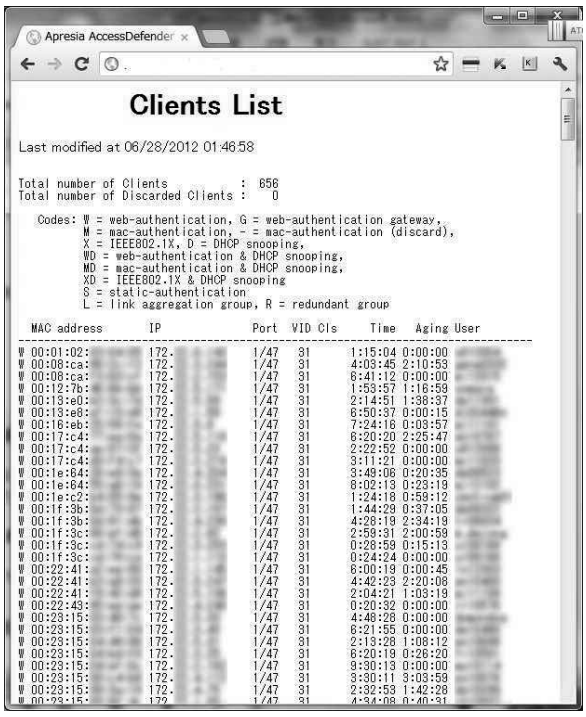

図 7　無線 LAN 認証クライアント一覧

現状では，無線 LAN アクセスポイント経由で認証を行うスイッチのみの情報を取得し，管理ウエブサイトで表示するようになっているが，全体の利用状況を取得することが，ネットワークの利用状況の把握に欠かせないので，無線 LAN セグメント以外のスイッチに対しても認証状況の可視化を行っていく予定である．さらに，コアスイッチの情報とのマッチングをはかり，正確な利用者分布を把握することを目指している．

4.4. 無線 LAN アクセスポイントの syslog 取得

無線 LAN アクセスポイントの syslog に関しては，アクセスポイント本体で保存されているログの取得を試み，アクセスポイントのコンソールでのコマンドの実行結果をローカルにダウンロードするためのスクリプトを開発した．これは，Python のネットワーク関係のライブラリを利用して syslog の取得を行うものである．これを利用して，アクセスポイントでのクライアントの動きが分かるようになる．

また，無線 LAN 認証スイッチ，エッジスイッチ，およびコアスイッチについても取得情報の絞り込みをはかり

5. まとめ

本報告では，無線 LAN アクセスポイントの障害の解析および監視状況について述べた．ネットワークは，状況に把握には，統計データの取得，ログの解析が欠かせない．また，機器単独での情報では，全体がわかりにくいので，統合的に，複数の機器からの情報をまとめて，監視の効率を上げる仕組みを構築していく予定である．また，syslog によるログ収集に関しては，本報告では，触れなかったが，ログ収集だけでなく，ログ解析の部分の強化を図り，障害への対応力の強化を図っていく予定である．

参考文献

[1]内藤郁之，望月源，佐野洋，「オンデマンドおよびスケジュール監視を併用した無線 LAN アクセスポイント監視システムの構築」，第 74 回情報処理学会全国大会，2012 年 3 月

[2]内藤郁之，「無線 LAN 接続環境の安定化」，東京外国語大学総合情報コラボレーションセンター年報　第 6 号, 2012 年