ネットワーク制御システムのための機器管理システムの拡張

11G489 宮崎貴充（最所研究室）

ネットワーク管理者の資産管理における負担を削減する目的でこれまで開発してきたネットワーク機器管理システムの拡張を行う．本稿では，拡張内容である履修情報と連携したMAC アドレスリスト管理と，更新監視機能について述べる．

1. はじめに

情報化の進展に伴い，大学などの教育機関や企業をはじめとした多くの組織では，組織内の情報資産を守るためにセキュリティーポリシーを定め，それに基づいた資産管理を行うことが求められている．近年，資産管理を行うツールとして統合システム運用管理JP1[1]などの製品が提供されているが，このような製品は企業を対象に開発されており，大学などでそのまま用いるには難しい点も多い．これまで，ネットワーク管理者の機器管理における負担を削減するシステムとしてネットワーク機器管理システムの開発を行ってきた[2]．また，本研究室では，機器，場所，時間の情報を用いて，本来行うべき作業に関係のないネットワーク利用の制限を目的とした，ネットワーク制御システムの開発を行っている[3]．本研究では，ネットワーク機器管理システムを拡張し，管理情報をネットワーク制御システムで利用できるようにする．更に，管理機器がOSなどの更新を行っているかどうかを監視する更新監視機能を実現する．本稿では，拡張内容である大学での運用を想定した，履修情報と連携したMACアドレスリスト管理と，管理機器の更新監視機能について述べる．

2. ネットワーク機器管理システムの概要と拡張内容

ネットワーク機器管理システムは，大学などの組織におけるネットワーク管理者の資産管理における負担を削減することを目的としたものである．機器情報の自動取得などによって登録の支援を行うことで，資産管理台帳に記載する情報を収集し，管理する．本システムで管理する情報は，機器名やMACアドレスなどの機器情報と，所有者のユーザ情報である．これらの情報から，ある学生とその学生が使用する機器のMACアドレスを紐付けすることが可能である．

このような情報をネットワーク制御システムで利用することで，より柔軟なネットワーク制御が可能になると考え，教務システムと連携することで履修情報を取得し，ネットワーク制御システムが必要とする情報を提供できるように拡張することとした．更に，IDSを用いて，本システムで管理している機器の中にOSなどの更新が行われていない機器が存在するかを監視する，更新監視機能を実現する．以下ではそれぞれの拡張内容について詳しく述べる．

3. 履修情報を用いたMACアドレスリスト管理

本研究室で開発を行っているネットワーク制御システムの主な目的は，大学において，教員が学生に対して講義中のネットワークの利用を制限することである．この時，制御の対象となるのは，講義を受講している学生が所持している情報機器である．また，制御を行う立場である教員や，その下で働いているTAの所持する機器は，学生とは違う制御を行うことがあるので，それぞれの立場に応じて区別する必要がある．

そこで本研究では，講義ごとに使用される機器のMACアドレスリストの管理に，身分とアクションランクという情報を付加して管理することとした．ネットワーク制御システムではアクションランクごとに決められた制御を行う．ネットワーク機器管理システムは機器情報を管理しており，これに加えて教務システムによって管理されている履修情報を用いることで，講義ごとの教員や受講者と，その講義中に使用される機器のMAC アドレスを求めることが可能である．更に外部の講師などに対応するためにゲスト機器用のMACアドレスリストも管理する．なお，本研究では，教務システムを想定したデータベースを持つ仮想的な教務システムを構築し，そこから履修情報が得られるという仮定で開発を行うこととした．

4. 更新監視機能

ネットワークを利用する機器の中には，OS のアップデートやアンチウイルスソフトの更新を正しく行っておらず，セキュリティ上の問題を抱えたままの機器が存在する．これらの機器はネットワーク内のウイルス蔓延などの原因となる可能性があり，このような機器を放置しておく事は望ましくない．このような問題に対して本システムでは，IDSによりネットワーク上の通信を監視することで，更新が行われているかの判断をすることとし

た. 図1 に概要を示す. 学内LAN と外部インターネットの境界にIDS を設置し, 通信の監視を行う. IDSは予めアップデートサーバへのアクセスを検出するように設定しておく. 本システムでは, 一定期間内にIDSのアラートが指定したしきい値を超えた機器は更新を行っているとみなすこととした.

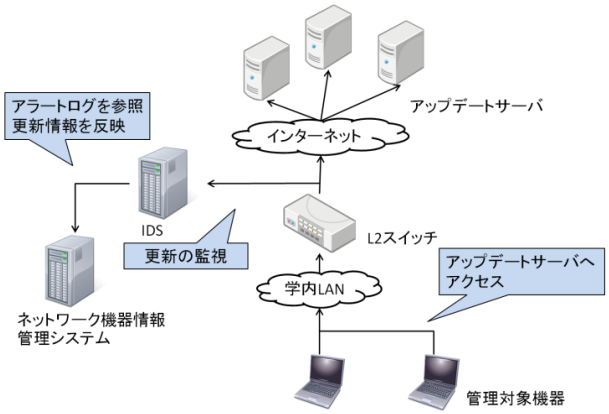

図1. 更新監視機能の概要図

5. 評価

はじめに, MACアドレスリスト管理の評価を行う. 学生100人, 教員30人からなる履修情報を用意し, MACアドレスリストが正しく生成されるかどうかを調べた. 本システムで生成されたリストの例を図2に示す. ここで図中のstatusの1は学生, 2はTAを表す値であり, 講義科目とMACアドレス, 立場に応じた身分とアクションランクが正しく登録できることが確認できた.

次に学生数とリストの生成に要する時間の関係を調査した. その結果, 処理時間は100人の時3.4秒, 500人の時22.8秒であった. リストの生成は頻繁に行われるものではないので処理時間に問題はないが, 実験に用いたサーバはPentium4を使用していたため, より性能の良いサーバを用いることで改善は可能である.

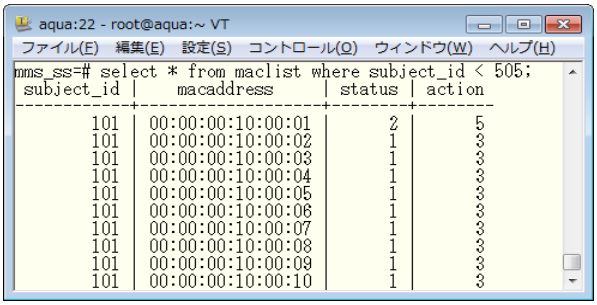

図2. 生成されたMACアドレスリスト

最後に更新監視機能について評価を行う. 表1に示す条件を設定した3台の機器を接続したハブを研究室内ネットワークに導入し, 監視を行った. 2013年1月のMicrosoft Updateにおけるアラート発生数を1時間ごとに計測した結果が図3である. 図より更新の行われたPC-Cだけ9576件という非常に大きな値が確認できる. またこの時, ネットワーク機器管理システムに登録されていないPC-Bは不明な機器として, PC-Cは更新が行われた機器として検出されていた. 以上の結果より, 更新の有無の判断に, IDS のアラート発生数を用いる手法の有効性が確認できた.

表1. 設定条件

	PC-A	PC-B	PC-C
実験中の動作 機器管理システム	更新確認のみ 登録済み	更新確認のみ 未登録	更新ファイルDL 登録済み

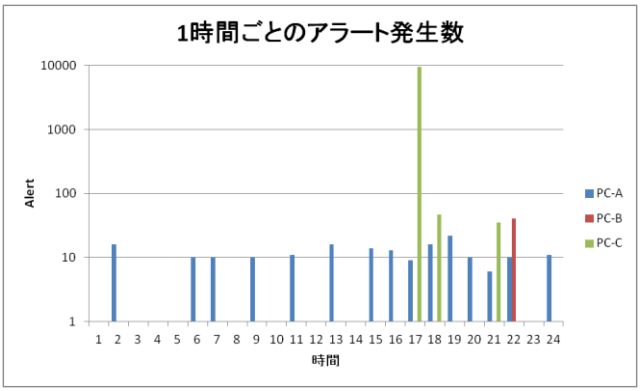

図3. 1時間ごとのアラート発生数

6. まとめと今後の予定

本稿では, ネットワーク機器管理システムの拡張機能である, 履修情報を用いた講義ごとMAC アドレスリスト管理と, 更新監視機能について述べた. 今後は以下に示す課題を解決していく必要がある.

- アクションランク設定の柔軟性
- ルールセットの自動生成
- 更新が行われていない機器への対応
- 実運用に近い環境での評価

参考文献

[1] 株式会社日立製作所, 統合システム運用管理JP1, “http://www.hitachi.co.jp/Prod/comp/soft1/jp1/”

[2] 宮崎貴充 最所圭三, “ネットワーク機器情報管理システムにおける登録支援機能の開発”, 平成23年度 電気関係学会四国支部連合大会論文集, 16-46, p.315, 2011

[3] 平川健一 , “機器および時間・場所を用いたネットワーク制御システムの開発”, 香川大学大学院工学研究科, 修士論文, 2012