Vol.2013-IOT-22 No.7
2013/8/1

機器および時間・場所などの情報を用いたネットワーク制御システムの開発

最所 圭三[a)]　平川 健一[1,†1]　宮崎 貴充[1,†2]

概要：ネットワークインフラの充実により，様々な場所でインターネットの利用が可能となり利便性が向上している．その反面，関係のないネットワークアクセスにより，本来行うべき作業に滞りを生じさせることが発生している．また組織内においては，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 IT 資産の管理が必要である．我々はこのような問題を解決するため，特定ユーザの不要なネットワークアクセスを自動的に制限できるシステムやネットワーク管理者の資産管理の負担を軽減するシステムの開発を行っている．本稿では，この 2 つのシステム総合し，さらに教務システムと連携することで，学内ネットワークにおける授業中のネットワーク制御が可能なシステムの設計と開発について報告する．

1. はじめに

ネットワークインフラの充実により，いつでもどこでもインターネットの利用が可能となり利便性が向上しており，大学や企業などにおいても，ネットワーク利用は必要不可欠なものとなっている．しかし，知識のないユーザの PC がコンピュータウィルスに感染し，それに気づくことなく個人情報や機密情報を流出する問題や，職務中や授業中に関係のないインターネットアクセスを行ってしまい，本来行うべき作業に滞りが生じる問題が発生している．また，組織内においては，情報資産を守るためにセキュリティーポリシーを定め，それに基づいた情報資産の管理が必要となっている．一般的に情報資産の管理は，組織内の情報部門やネットワーク管理者が資産台帳などを用いて行っているが，組織内の情報機器数の増加に伴い，それらの管理が管理者にとって大きな負担となっている．

セキュリティ向上や不要なアクセスの制限を目的としたシステムの研究 [1], [2] や製品 [3] がある．これらのシステムは，情報機器を用いているユーザ情報やアクセス内容によりアクセス制御を行っている．しかし，一つの情報機器を様々な状況で使用することも多くなっており，利用者や機器情報以外にも，その機器の利用場所や時間などに応じたアクセス制御が必要になってきている．例えば，モバイル機器では場所によってアクセス制限の内容が変わるべきであり，仕事中や授業中では本来の作業を妨げるようなネットワークアクセスは制限されるがそれ以外は制限しないなどの制御が必要である．これらを実現するために，我々は，予約の概念の基づいて情報機器のアクセス制御を自動的に行うシステム [4] を提案した．

一方，情報機器の管理を行うために，統合管理システムと呼ばれる様々なソフトウェアが提供されている [5], [6], [7]．これらのソフトウェアは企業を対象に開発されているため，大学などの個人の情報機器が使用される機会の多い組織への導入が難しい点も多い．例えば，管理のために PC に管理用のソフトウェアの導入が必要な場合があり，個人の PC を持ち込むことが多い大学では実現が困難である．このため，我々は Web ベースでネットワーク機器の管理を行うネットワーク機器管理システムを提案した [8]．このシステムは，IP アドレスや MAC アドレスをはじめとした機器情報の自動取得，候補を例示するなどの情報登録の支援により，機器管理の登録の負担を軽減する．

本稿では，我々がこれまで開発してきた 2 つのシステムを連携したシステムについて述べる．このシステムは，大学の構内を想定して設計しており，大学内の授業に関連する情報や学生に関する情報を管理する教務システムや，侵入検知システム (IDS, Intrusion Detection System) との連携を行うことで，より柔軟なネットワーク制御および管理を実現する．

2. システムの概要

本システムは，大学での使用を想定しており，授業ごと

[1] 香川大学
Kagawa University
[†1] 現在，株式会社ケイ・オプティコム
Presently with K-Opticom Corporation
[†2] 現在，株式会社 STNet
Presently with STNet, Incorporated
[a)] sai@eng.kagawa-u.ac.jp

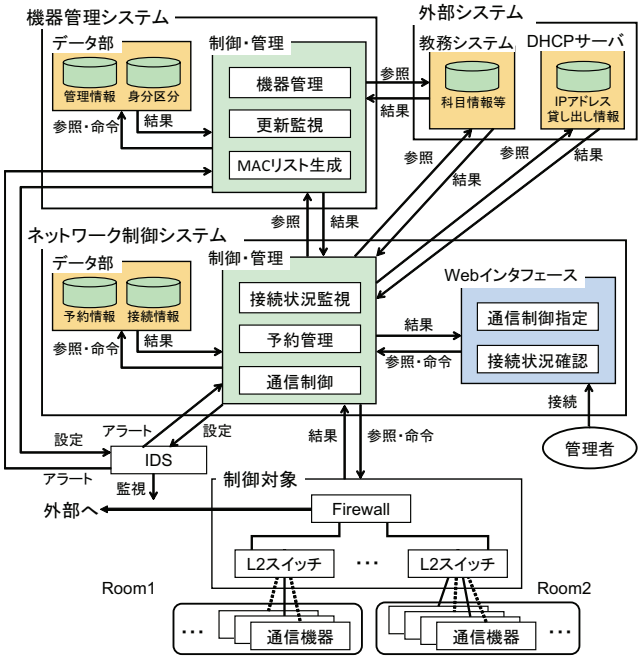

図 1 ネットワーク制御システムの構成
Fig. 1 Structure of the network control system

にネットワーク使用の禁止，禁止している場合でも特定のサイトへのアクセス許可，身分ごと (教員，補助，学生など) のアクセス制御を目標に開発している．図 1 にシステムの構成を示す．本研究においては，図中の機器管理システムとネットワーク制御システムを開発を行っている．

2.1 機器管理システム

機器管理システムでは，個人 PC を含めた学内 LAN に接続する可能性のある情報機器の機器情報を管理している．機器管理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情報である．学生とその学生が使用する情報機器の MAC アドレスが紐付けされているので，教務システムから学生の履修情報を取得することにより，ある科目の授業で持ち込まれる可能性のある機器の MAC アドレスの集合を把握することができる．科目を担当する教員の情報機器についても同様である．また，情報機器の中には，OS の更新やアンチウイスル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．このため，IDS を用いて更新のためのパケットを観測することで，管理機器の更新が行われているかどうかの判断を行う機能を機器管理システムに追加する．

2.2 ネットワーク制御システム

ネットワーク制御システムは本システムの中心となるシステムである．機器管理システムから授業関係者の機器情報，教務システムから授業科目や授業が行われる時間帯を取得する．そして，それらの情報と管理者からの指示に従ってネットワークアクセスの可否を判断し，ファイアウォールや L2 スイッチを制御する．また，教員の PC のパケットを IDS に観測させ，アクセスしたサイトへのアクセスを一時的に許可することも行う．ここでいう管理者とは，授業中のネットワーク制御を行う者を指し，本システムでは教員を指す．アクセス制御を機器単位で行っているので，アクセス対象となる情報機器の接続状況を把握しなければならないが，DHCP サーバや L2 スイッチを監視することで接続状況を得るようにする．

2.3 教務システム

本研究では，学生の履修情報や授業の休講情報などを得るために教務システムとの連携を行うことを考えている．しかし，実際に運用されている教務システムでは多くの個人情報を扱っており，連携に必要な情報だけを取り出す仕組みが教務システム側に必要となる．このため，本研究では，以下の情報を提供できる仮想的な教務システムを構築して開発を行う．

- 授業科目情報 (科目と担当教員や TA の情報を含む)
- 授業の行われる教室・時間情報
- 教員・学生情報
- 履修情報 (科目と受講生の情報を含む)
- 休講・補講情報

3. 機能設計

本節では，授業ごとのネットワーク制御を行うための機能および IDS を用いたネットワーク制御と更新監視機能について述べる．

3.1 授業ごとのネットワーク制御

図 2 に，ネットワーク制御の流れを示す．細い枠は管理・制御用のデータ，太枠は機能，点線の枠はサーバまたはネットワーク機器を表す．以下，授業ごとのネットワーク制御を行うための機能について説明する．

MAC アドレスリスト生成機能

授業ごとにネットワーク制御を行うために，授業と受講する学生が所有する機器の MAC アドレスとの対応を示す MAC アドレスリストが必要となる．図に示すように，MAC アドレスリストは，科目，MAC アドレス，身分およびアクションランクから構成される．身分は機器所有者の授業中の立場を示し，アクションランクは授業中に許可されている行動を表す．許可される行動として，メールの閲覧，ホームページの参照，OS 等の更新などがある．表 1 に本システムで用いた身分とアクションランクの値を示す．例えば，アクションランクの値が 3 であれば，メールや OS 等の更新は許可するが，それ以外は拒否するなどの

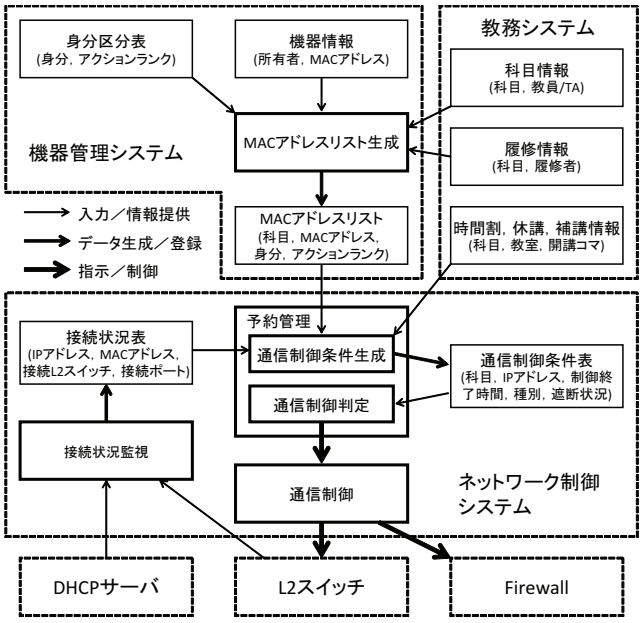

図 2 ネットワーク制御の流れ
Fig. 2 Flow of access control

表 1 身分とアクションランク
Table 1 Status and action rank

	学生	TA	教員	ゲスト
status	1	2	3	4
action	3	5	6	-1

制御が行われる．現時点では，メールサーバや更新サーバが IP アドレスで指定されているものとして実装している．なお，ゲストは外部講師等である．

MAC アドレスリスト生成機能は，教務システムから科目情報と履修情報を取得し，自身が持つ機器情報と身分区分表を組み合わせて MAC アドレスリストを生成する．機器情報には情報機器の所有者と MAC アドレスの組，科目情報には科目と担当教員や TA の組，履修情報には科目と履修者の組，身分区分表には身分とアクションアンクの組が含まれており，これらのデータを結合することにより MAC アドレスリストを生成する．また，ゲストに対応するために，ゲスト機器の情報登録を行い，その情報をゲスト機器の MAC アドレス一覧として管理する．

接続状況監視機能

情報機器の動的な接続，切断が行われる環境でネットワーク制御を自動化するためには，機器のネットワークへの接続状況を常に監視し，対象となりうる機器の接続状況を把握し続ける必要がある．このため，DHCP サーバのログや L2 スイッチの ARP テーブルから IP アドレスと MAC アドレスの組を収集する．さらに，得られた IP アドレスを用いて接続されている可能性のある L2 スイッチ群を特定し，その中から MAC アドレスを用いて接続されている L2 スイッチとそのポート番号を取得し，接続状況表に登録する．

予約管理機能

制御の対象となっている情報機器を管理するために，科目識別子，送信元と送信先の IP アドレス，制御終了時間，種類および遮断状況からなる通信制御条件表を作成し，この表に基づいてネットワーク制御の指示を通信制御機能に送る．種類には 授業時間外/授業中制御/L2 スイッチでの制御 などがあり，遮断状況には 実行/未実行 がある．

予約管理機能は，周期的に呼び出され，通信制御条件生成機能を用いて通信制御条件表を作成し，そのあと通信制御判定機能を用いて通信制御条件表と接続状況表を調べ新たな遮断や解除が必要でないか検査する．新たな遮断や解除が必要な場合は，遮断解除の指令を通信制御機能に送る．

通信制御条件生成機能での処理手順は以下の通りである．

(1) 教務システムから時間割，休講，補講情報を取得し，現在行われている授業がないか調べ，該当する授業がなければ終了する．
(2) 授業が行われている教室のネットワークセグメントを特定し，接続状況監視で取得した情報機器がそのセグメントに接続しているかどうかを調べる．該当する機器が存在しない，あるいは存在しても既に通信制御条件表に全て登録されている場合は場合は終了する．
(3) 機器管理システムから MAC アドレスリストを取得し，該当の情報機器が登録されている場合はアクションランクに応じて各種サーバごとの許可・不許可を，登録されていない場合は通信許可を通信制御条件表に登録する．この時点では，遮断状況は未実行となっている．

登録作業が終わると，通信制御判定機能は通信制御条件表に登録されている遮断状況や制御終了時間を調べ，遮断および解除を判断する．遮断状況が未実行の場合は遮断と判断する．実行の場合は制御終了時間に達していないか調べ，制御終了時間に達している場合は解除と判断するとともにその登録を削除する．それ以外は遮断の継続となる．

通信制御機能

予約管理機能から送られる指示に従い，ファイアウォールまたは L2 スイッチを用いて遮断あるいは解除を行う．

ファイアウォールによる制御では，遮断の場合，遮断対象の IP アドレスや制御の内容によりフィルタリングルールを作成し，チェインリストに追加する．解除の場合は同じフィルタリングルールを破棄する指令を追加する．

L2 スイッチによる通信制御では，L2 スイッチの FDB (フォワーディングテーブル) のモードを static に変更し，遮断対象となる情報機器の MAC アドレスを FDB から削除することで遮断を行う．解除の場合，他に遮断する機器がなければ FDB のモードを dynamic に変更し，それ以外は MAC アドレスを再登録する．

3.2 IDS を用いたネットワーク制御および更新監視

IDS は不正パケットを検出し，そのパケットを送信ある

いは受信した情報機器の特定に用いるが，本システムでは，特定の情報機器からのパケットや特定のサーバへのパケットの検出に用いる．

指定した情報機器がアクセスしたサイトへのアクセス許可

授業中に教員がアクセスしたサイトを学生にもアクセスさせたい場合がある．授業を担当している教員が，一々アクセス先を調べて設定することは困難である．そこで，教員のアクセス先を自動的に把握し，そこへのアクセスを許可する機能をネットワーク制御システムに追加することにした．

この機能は，教員からの指示に従い教員の情報機器の IP アドレスを自動的に取得し，IDS の監視対象に設定する．そして，IDS から発生するアラート情報を取得し，そのアラート情報に記載されている宛先の IP アドレスへのアクセスを許可するルールをファイアウォールに追加する．例えば，IP アドレスが `192.168.2.31` である教員の PC からの全てのパケットに対してアラートが発生するようにするには，IDS として Snort[9] を用いている場合，以下のシグネチャを登録すればよい．`msg:` の後の文字列がアラートログに出力される．

```
alert tcp 192.168.2.31 any ->any any
    (msg:"teacherA"; sid:1000030001)
```

更新監視機能

ソフトウェアの更新はセキュリティ向上のためには欠かせないものである．このため，更新サーバへの通信を監視することで管理している情報機器の更新を IDS を用いて検出する機能を機器管理システムに加えることにした．

IDS にはソフトウェアの更新サーバとの通信パケットを検出するように設定しておく．例えば Windows 更新サーバの 1 つである 210.157.235.1 との間のパケットを検出するためのシグネチャは以下のようになる．

```
alert tcp any any -> 210.157.235.1 any
  (msg:"microsoft_update_1";sid:1000001001)
```

IDS は更新サーバへの通信を検出すると，そのアラートをデータベースに保存する．機器管理システムでは周期的にこのデータベースにアクセスし，アラートが発生していないかどうか調べる．発生している場合は，更新サーバの通信相手が更新していると判断する．そして，更新が一定期間検出されない情報機器や，情報管理データベースに登録されていない情報機器の更新が検出された場合に管理者に警告を出す．

しかし，設定によっては，更新ファイルの存在までチェックし，ダウンロードしないことがある．この場合，更新されていないと判断することにした．ダウンロードファイルのサイズとアラート数の関係を調べたところ，アラート数がサイズにほぼ比例することが分かった．このことから，指定した数以上のアラートが発生したときに更新が行われたと判断することにした．なお，この方式では，更新ファイルがダウンロードされたかどうかは判断できるが，実際に更新まで行われているかどうかまでは判断できない．

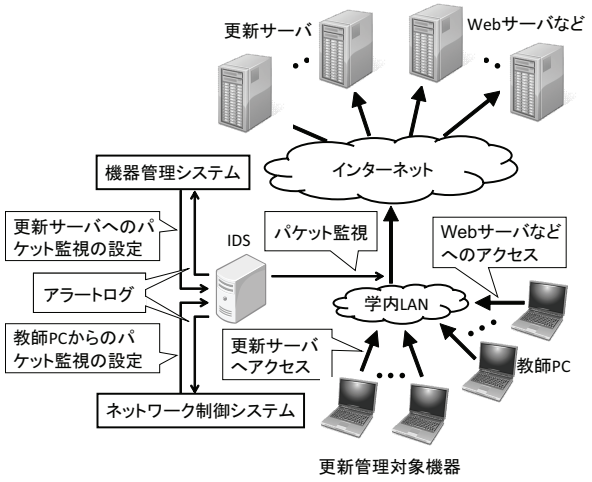

図 3 IDS による更新サーバおよび教師 PC のパケット監視
Fig. 3 Watching update and specified hosts' packets using IDS

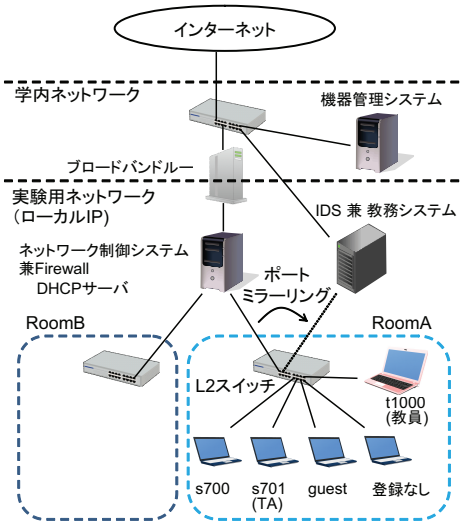

図 4 実験環境
Fig. 4 Expreimental environment

これら 2 つの機能は IDS を共通に用いており，図 3 に示すように統合化できる．IDS に登録するシグネチャのログメッセージがお互いに重ならないようにすることで，どの目的で登録したシグネチャのアラートログであるかを判断できる．

4. 評価

図 4 に実験環境を示す．2 つの教室をシミュレートする実験ネットワークを構築した，機材の関係で IDS での監視は一方の教室 (RoomA) と外部のネットワークとの境界で行った．以下に各サーバのハードウェア仕様を示す．

- ネットワーク制御システム
  CPU：Celeron 2.0GHz, メモリ：1Gbyte,
  NIC：ギガビットイーサネット× 3

guest	2013/02/05 20:49	133.92.147.239	successful	t1000	2013/02/05 20:49	133.92.147.239	successful	
guest	2013/02/05 20:50	133.92.147.239	successful	t1000	2013/02/05 20:50	133.92.147.239	successful	
guest	2013/02/05 20:51	133.92.147.239	timeout	t1000	2013/02/05 20:51	133.92.147.239	successful	制御中
guest	2013/02/05 20:52	133.92.147.239	timeout	t1000	2013/02/05 20:52	133.92.147.239	successful	
guest	2013/02/05 20:53	133.92.147.239	timeout	t1000	2013/02/05 20:53	133.92.147.239	successful	
guest	2013/02/05 20:54	133.92.147.239	timeout	t1000	2013/02/05 20:54	133.92.147.239	successful	
guest	2013/02/05 20:55	133.92.147.239	timeout	t1000	2013/02/05 20:55	133.92.147.239	successful	
guest	2013/02/05 20:56	133.92.147.239	successful	t1000	2013/02/05 20:56	133.92.147.239	successful	

図 5 授業時間のネットワーク制御結果

Fig. 5 Result of network control during class

	外部サイト1アクセス		外部サイト2アクセス		内部サーバアクセス		
s700	2013/02/05 22:14	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:16	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	IDSを用いた制御開始
s700	2013/02/05 22:17	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:18	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:19	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:20	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	外部サイト1アクセス
s700	2013/02/05 22:21	125.6.149.67	successful	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:22	125.6.149.67	successful	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:23	125.6.149.67	successful	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:24	125.6.149.67	successful	207.46.73.113	timeout	133.92.147.239	timeout	外部サイト2アクセス
s700	2013/02/05 22:25	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	timeout	
s700	2013/02/05 22:26	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	timeout	
s700	2013/02/05 22:27	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	timeout	
s700	2013/02/05 22:28	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	timeout	
s700	2013/02/05 22:29	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	timeout	内部サーバアクセス
s700	2013/02/05 22:30	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	successful	
s700	2013/02/05 22:31	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	successful	
s700	2013/02/05 22:33	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	successful	
s700	2013/02/05 22:34	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	successful	
s700	2013/02/05 22:35	125.6.149.67	successful	207.46.73.113	successful	133.92.147.239	successful	IDSを用いた制御終了
s700	2013/02/05 22:36	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:37	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	
s700	2013/02/05 22:38	125.6.149.67	timeout	207.46.73.113	timeout	133.92.147.239	timeout	

学生のアクセス監視結果 (メールサーバ, 機器登録サーバの監視には変化なし)

図 6 IDS を用いたネットワーク制御結果

Fig. 6 Result of network control using IDS

- 機器管理システム
  CPU：Pentium4 2.53GHz，メモリ：1Gbyte，
  NIC：ギガビットイーサネット× 1
- IDS 兼 教務システム
  CPU：i5-3570K 3.4GHz，メモリ：8Gbyte，
  NIC：ギガビットイーサネット× 2

なお，OS はバージョンは異なるが全てのサーバで CentOS を，データベースはネットワーク制御システムと機器管理システムでは PostgreSQL，IDS 兼教務サーバでは MySQL を，開発言語は PHP を，IDS は Snort を，そして Firewall は Linux の iptables をそれぞれ用いた．また，L2 スイッチとしてアライドテレシスの CentreCOM GS916M を用いた．

この実験環境を用いて，各機能が正しく動作していることを確認した．また，ネットワーク制御にかかる時間や MAC アドレスリストの生成時間を測定した．MAC アドレスリストの生成に関しては性能的に問題ないことを確認した．以下，特に重要な授業を想定したネットワーク制御，IDS を用いたネットワーク制御，ネットワーク制御の性能および更新監視機能の結果について示す．

4.1 ネットワーク制御の評価

図 5 に 5 分間の授業を設定したときに，遮断の対象となるゲストの PC (guset) と対象とならない教員の PC (t1000) から学内サーバ (133.92.147.239) に 1 分おきに HTTP でアクセスしたときの結果である．t1000 からの学内サーバへのアクセスは制御中も成功しているが，guest からのアクセスは制御中に失敗しており，ネットワーク制御機能が正しく動作していることが確認できる．

次に，IDS を用いたネットワーク制御の結果を示す．学生の PC (s700) から 3 つのサーバ (livedoor TOP ページ (125.6.149.67)，MSDN Japan TOP ページ (207.46.73.113) および 学内サーバ (133.92.147.239)) に HTTP でアクセスしているときに，IDS によるネットワーク制御を行った．この結果を図 6 に示す．授業中に，教員が IDS によるネットワーク制御を指示したあと，125.6.149.67，207.46.73.113 および 133.92.147.239 の順にアクセスしている．その結果，s700 からもそれぞれのサーバがアクセスされたあとにアクセスできるようになっており，ネットワーク制御機能が正しく動作していることが確認できる．

次にネットワーク制御の性能評価の結果を示す．予約管理機能を呼び出してから iptable の設定スクリプトの生成にかかる時間および iptables への適用時間を図 7 に示す．図から，スクリプトの生成時間が支配的になっており，1,000 人分の PC を制御するために全体で 50 秒ほどかかっている．この結果から，1 分間隔での制御が可能であるが，直ちに設定を反映したい場合は不十分であることが分かる．しかし，実験で用いたサーバは Celeron 2.0Ghz とい

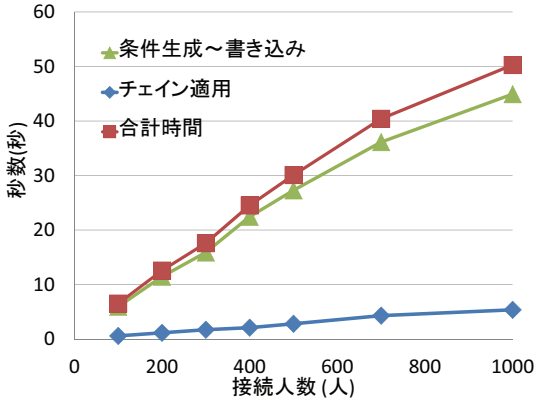

図 7 ネットワーク制御にかかる時間
Fig. 7 Time for network control

表 2 設定条件
Table 2 Setting conditions

	PC-A	PC-B	PC-C
更新設定	更新確認のみ	更新確認のみ	更新ファイル DL
機器情報	登録済み	未登録	登録済み

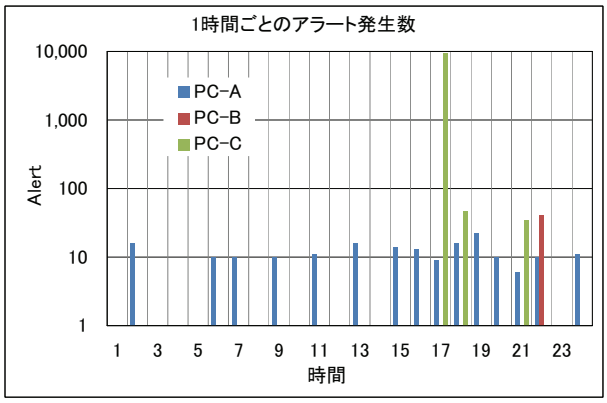

図 8 1 時間ごとのアラート発生数
Fig. 8 Number of alerts per hour

う非常に遅い CPU であり，最新の CPU を用いることにより 1 桁程度の高速化は可能であると考えている．

更新監視機能の評価

Microsoft Update を対象にした実験を行った．表 2 に示す更新設定をした 3 台の PC を L2 スイッチに接続し，Microsoft の Update サーバを監視するように設定した IDS で上流に行くポートを監視するようにした．

図 8 は，2013 年 1 月の Microsoft Update における IDS のアラート発生数を 1 時間ごとに計測した結果である．図よりダウンロード (DL) までの設定を行っている PC-C だけ 9,576 件という非常に大きな値となっており，未登録の PC-B からのパケットも検出されている．機器管理システムでは，未登録の 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た．この結果より，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．

5. おわりに

以上，大学での授業中のネットワーク制御を行うためのネットワーク制御システムの開発および評価について述べた．実験により，提案システムの有効性を確認できた．

しかし，提案システムを実際にシステムに適用するためには，解決しなければならない課題も多い．代表的なものとして以下がある．

- ネットワーク制御の例外設定の実装
  現在，身分に付随したアクションランクというパラメタでネットワーク制御の設定を行っているが，身分が同じでも異なる制御を行いたい場合がある．
- ネットワーク制御の負荷軽減のための予約管理機能の改良
  最新の CPU を用いることにより 1,000 人程度の規模であれば数秒での制御が期待できるが，大規模な環境では不十分である．
- IDS を用いた機能の改良
  ネットワーク制御に関しては，ミラーサーバには対応できていない．更新監視機能に関しては，可能性を示しただけで，実際に用いるためには対処となるソフトウェアの更新先のリストや，更新を行ったかどうかの閾値の設定が重要となる．
- 更新監視機能により検出した更新不備の機器への通信制限の実装
  現在は警告を発するのみでアクセス制御までは至っていない．

参考文献

[1] 吉田祐亮, 高山卓也, 川橋裕: 組織内ネットワークにおける不正利用端末検出および利用位置特定システムの構築, 電子情報通信学会技術研究報告，IN，情報ネットワーク 111(245)，pp.37-42，2011.
[2] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明: キャンパス規模で運用可能な MAC アドレス認証システム OpengateM, 情報処理学会研究報告．IOT，2012-IOT-19(12)，pp.1-6，2012-09-20.
[3] 株式会社日立ソリューションズ, オープンネットガード, 入手先 ⟨http://www.hitachi-solutions.co.jp⟩ (2013.03.05)
[4] 平川健一, 最所圭三: 機器情報を用いたネットワーク管理システムの構築, 電気関係学会四国支部連合大会論文集，16-45，pp.314，2011.
[5] 株式会社日立製作所, 統合システム運用管理 JP1，入手先 ⟨http://www.hitachi.co.jp/Prod/comp/soft1/jp1⟩ (2013.02.25)
[6] エムオーテックス株式会社，LanScope Cat7，入手先 ⟨http://www.motex.co.jp/cat7/index.html⟩ (2013.02.25)
[7] 株式会社日本ダイナミックシステムズ, e-Survey+，入手先 ⟨ http://www.nds-tyo.co.jp/e-survey⟩ (2013.02.25)
[8] 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, 電気関係学会四国支部連合大会論文集，16-45，pp.315，2011.
[9] Snort, 入手先 ⟨http://www.snort.org/⟩ (2013.03.05)