トレーサビリティネットワークの構築
Construction of traceability network

沖野浩二 †, 山田純一 †, 布村紀男 †, 柴田啓司 ‡

Koji Okino†,Junichi Yamada†,Norio Nunomura†,Keiji Shibata‡

{okino,j_yamada,nori2}@itc.u-toyama.ac.jp, shibata@eng.u-toyama.ac.jp

富山大学 総合情報基盤センター †
富山大学 大学院 理工学研究部 ‡
Information Technology Center,University of Toyama.†
Graduate School of Science and Engineering for Research, University of Toyama‡

概要

不特定多数が利用するネットワークでは、コンピュータ・ウィルスに感染したノードや不正なユーザによる利用が発生する場合がある。このような場合に対応するために認証を行い通信記録を取得する必要があるが、このようなトレーサビリティネットワークを構築するためには、メーカー独自の機構を利用したり専用装置を導入する必要があった。本論文では、既存ネットワークの構成を変更せずに導入可能な、トレーサビリティネットワークの構築手法を提案し、トレーサビリティネットワークを構築するに当たり、利用形態に基づいた階層とそれらの階層における要件の定義と提案手法の実装を行った。結果として、既存の無線 LAN AP やインテリジェントスイッチを用いて、ユーザ情報 (IP アドレス-MAC アドレス-利用者) の収集を行い、それぞれの階層において想定される不正利用を抑止することが可能になった。

キーワード

ネットワークセキュリティ, 情報コンセント, ユーザ認証

1 はじめに

昨今では、軽量なノート PC やスマートフォンの普及によって、各自の情報端末を持ち歩き、利用する機会が増えている。これに伴い、大学においても、旧来の固定 IP アドレスによる運用だけでなく、パブリックスペースでの情報コンセントや無線 LAN AP の整備が求められている。このような不特定多数が利用する環境では、IP アドレスではなく利用者単位で認証を行う仕組みが必要であり、不正利用が起きた場合には追跡調査できるような仕組みが不可欠である。

ネットワークにおける認証機構は、鈴木 [1] らや大谷 [2] らによるゲート認証方式と、石橋 [3] らや大江 [4] らによるエッジ側のコントロール機能を利用した方式に大別される。ゲート認証方式では、ゲートへの誘導やゲートの処理能力が課題になり、エッジコントロール方式では専用のネットワーク構成や無線 LAN に特化した方法など、エッジの種類に応じてそれぞれ対処することが必要になる。

実際に複数の異なるベンダーの機器が導入されている組織において、ゲート認証方式を導入する例が多いのは、エッジの種類ごとに対応することが難しいためだと考えられる。そこで本論文では、多くのメーカがサポートしている認証機構、無線 LAN での PEAP 認証機構および有線 LAN におけるエッジの MAC アドレス認証及び Web 認証を利用することにより、遠隔キャンパスも含めた組織内全域において適応可能なトレーサビリティネットワークを、エッジコントロール方式で実現する手法を提案する。

2　トレーサビリティネットワーク

2.1　要件

本論文におけるトレーサビリティネットワークとは、

1. いつ
2. どこで
3. だれが
4. 何をしたか

を、管理者が追跡することが可能なネットワークと定義する。

1. いつ　と　4. 何をしたかは、FW や組織内サーバ等に記録された通信記録の内容とする。2. どこでに関しては、一般にネットワークにおいて、FW 等のログに記録される IP アドレスしかわからない。IP アドレスから実際の利用者を特定するのは、組織によって採用されている IP アドレス等の管理方法に依存する。

本論文におけるトレーサビリティの確保とは

特定 正規の利用者がネットワークを利用した場合に、利用者（責任者）が特定できること

不正防止 他人へのなりすましや、身元を隠した状態でネットワークにパケットを送出できないこと

と定義する。

2.2　必要とされる要件と現実の問題

トレーサビリティを実現するには、FW 等に記録される IP アドレスとその IP アドレスの利用者とのひも付けを行うことが必要である。

組織内における IP アドレスの管理方法は、利用者の申請に基づいて固定的に割り当てる方法と自動的にネットワーク設定を取得する DHCP による運用の 2 種類に分けられる。申請制が適切に運用されている場合には、IP アドレスから利用者の特定は容易である。DHCP による運用では、IP アドレスから対応する MAC アドレスを調べ、MAC アドレスから利用者を特定する必要がある。

実際に、トレーサビリティネットワークを適切に運用するためには、管理者が

1. IP アドレス-利用者
2. MAC アドレス-利用者
3. MAC アドレス-IP アドレス

に関する正しい情報を収集し、これらの間のひも付けを保証する必要がある。

しかし、組織の規模が大きくなるにつれて、サブネットごとに別の責任者に管理業務が委任されるなど、階層的に管理されている場合も多く、組織全体における IP アドレス-利用者や MAC アドレス-利用者等に関する情報のひも付けを適切に行うことは難しいのが現状である。

本学においても、学部の研究室では固定 IP アドレスの申請制を採用し、教室や会議室などでは DHCP による運用を行っている。利用者が申請書を提出せずに勝手に利用する事例や PC を更新しても申請内容を訂正しないなどの事例が多発していた。そのため、IP アドレス-利用者等の情報に関して、適切にひも付けを行うことが難しく、障害対応の際の問題となっていた。

2.3　考えられる脅威

トレーサビリティを確実なものにするためには、

1. ユーザが正しく設定し、正しく情報提供していた場合
2. ユーザが誤った設定あるいは誤った情報提供をしていた場合
3. ユーザが意図的にトレースを回避し、不正利用を行った場合

の 3 つのパターンに対応する必要がある。1 パターンの場合は、申請書に記載された IP アドレスや MAC アドレスにより利用者は特定できる。しかし、実際には、悪意のない利用者においても 2 のパターンが発生する確率がかなりの程度ある。

なぜならば、現在仕様されている多くの PC には、有線用と無線用の 2 種類の MAC アドレスが割り当ててあり、この 2 つを区別して正しく申請できる利用者は多くないという現実がある。加えて、Windows では Tunnel adapter や IEEE1394 などが加わり、ユーザが実際に利用している IP アドレスや MAC アドレスを正しく認識することはより難しくなっている。そのため、申請制によるひも付け情報を利用したトレーサビリティの確保は、利用者の増大とともに難しくなることが考えられる。

3 のパターンのユーザが意図的にトレースを回避する場合に対応するためには、IP アドレスおよび MAC アドレス偽装について考慮する必要がある。

2.4　LAN の分類

組織内におけるネットワークは、利用形態に基づいて、次の 3 種類に分類することができる。

a. 管理された LAN 管理組織が確実に管理し、接続されている PC が固定化されている LAN。本学においては、情報センター端末室や事務室の PC を収容する LAN に相当する。

b. 委任された LAN 下位組織に管理が委任されている LAN。利用形態は多種多様であり、HUB を経由し、PC だけでなく、サーバやプリンタなどが接続される。上位の管理組織が実際の利用者を知ることはできない。本学においては研究室内 LAN に相当する。

c. 認証 LAN 構成員のうち誰が利用するかわからない LAN。認証によりユーザを特定する必要がある。アクセス方式により無線 LAN と有線 LAN に分けられる。本学においては、会議室や講義室などで提供される認証 LAN に相当する。

2.5 トレースレベル

上記の 3 つの LAN はそれぞれ求められるトレースレベルが異なっている。

管理された LAN では、組織的に管理された PC と IP アドレスが利用されるということが前提であり、MAC アドレス偽造や IP アドレス偽造は行われないものとする。実際の利用者を特定するには、PC 利用申請者の特定を行えばよい。

委任された LAN では、IP アドレスや MAC アドレスの積極的な偽造は行われないが、IP アドレスの設定間違いや MAC アドレス申請の際の間違い等は発生するものとする。利用者の特定を行うためには、接続されている情報コンセントの位置と管理者が誰であるかが判明すればよい。上位管理者は、下位組織管理者からの申請に基づき、IP アドレスと MAC アドレスの突き合わせを行い、適切に利用されているかを監視する必要がある。

認証 LAN では利用者の特定が必要である。また、認証の回避や IP アドレスおよび MAC アドレスの偽造が行われる可能性があることに注意する必要がある。LAN ごとに必要な確認範囲を表 1 に示す。

表- 1: LAN ごとの確認項目

	IP-MAC 確認	ユーザ認証
管理された LAN	任意	必要
委任された LAN	必要	委任側
認証 LAN	必要	必要

管理された LAN は、ログイン時認証など別の手段でトレースするものとし、委任された LAN 及び認証 LAN を対象として検討を行った。

3 求められる性能

組織全域で運用するトレーサビリティネットワークにおいて求められる要件としては、下記の 5 つがあげられる。

性能と拡張性 大規模なネットワークにも対応できる性能と拡張性を有すること

既存システムとの親和性 新規に導入する際、既存のネットワークを大きく変更する必要がないこと

メーカ非依存性 特定の製品でしか実現できないものでないこと

運用コスト システム運用のコストが大きく増大しないこと

追跡性の確保 トレーサビリティを確保できること。具体的には、IP アドレスと MAC アドレスと利用者の関係に関する情報が取得できること。

これらの要件を鑑み、本学のトレーサビリティネットワークを構築する際の、基本的要件を以下のように定義した。

1. 富山大学全域に対する広域サービス
   遠隔キャンパスにも対応でき、マシン台数 10,000 台に対応できること。OS は、Windows, Mac, Linux, Android, iOS に対応すること。
2. 性能低下の防止
   10,000 台のマシンが同時に利用しても著しい性能低下を起こさないこと。
3. メーカ依存の禁止
   本学では現在、CISCO 社製製品を主に利用しているが、今後の更新等に際して束縛とならないよう CISCO 社製以外の製品にも対応できること。
4. 導入コスト、運用コストの低減
   既存の機器を更新することなくそのまま利用できること。また、現在の運用手段が大きく変化しないこと。
5. 事前情報登録作業の削減
   MAC アドレスや IP アドレスの登録作業が必要でないこと。
6. 認証データの統合 (学内認証基盤との同一 ID)
   学内認証基盤の ID,Password を利用して認証を行えること。
7. IP-MAC アドレステーブルの監視
   IP-MAC アドレス対応表を監視でき、長期間利用していない IP アドレス等の把握ができること。

4　実現方式

4.1　製品比較

前記の基本要件を満たす製品を調査したところ、認証システムとして CISCO 社製 Cisco Secure Access Control System[5] を検討したが、3 及び 6 の仕様を満たすことができなかった。また、ネットワーク管理システムとしてダイキン工業社製 PNDDA[6] を検討したが、これは、仕様 6 を満たすことができなかった。ゲート認証方式も検討を行ったが、仕様 1 及び 4 を満たすことが難しいと判断した。

4.2　システム構成

そこで、3 節で定義したトレーサビリティネットワークに求められる性能の基本的要件を満たすため、エッジコントロール方式のトレーサビリティシステムを 3 つのシステムを組み合わせて構築した。構築したトレーサビリティシステムの構成を図 1 に示す。

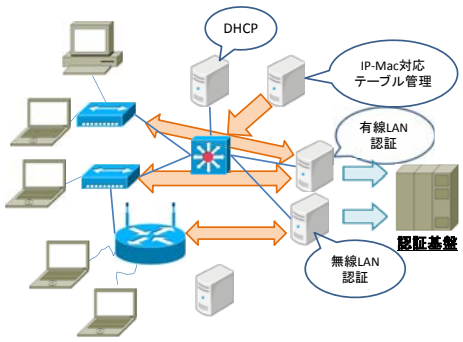

図- 1: システム構成図

システムは、MAC-IP 対応テーブル管理システム、無線 LAN 認証システム、有線 LAN 認証システムからなる。

4.3　MAC-IP 対応テーブル管理システム

MAC-IP 対応テーブル管理システムは、基幹スイッチ (L3) に接続して IP アドレスと MAC アドレスの対を取得して管理する。これは、次の項目で構成される。

- 基幹スイッチ IP リスト
- SNMP ポーリングプログラム
- MAC-IP アドレスリスト
- 差分抽出プログラム

一定時間ごとに、基幹スイッチに対して SNMP ポーリングを行い、MAC ー IP アドレスリストを作成する。これを一つ前のタイミングのリストと比較して、変更があった場合に、次のデータをメールで管理者に送付する。

- PC の新規接続 (New)
- 同一 IP アドレスに対する MAC アドレスの変化 (IP)
- 同一 MAC アドレスを複数の IP アドレスで利用 (Mac)

メールの具体例を次に示す。

```
New ---------------------------------
New  160.26.12.110  F8:0F:41:19:60:CC
Duplicate IP Address -----------------
IP   160.26.11.220  00:00:11:8F:77:88
        <- 00:12:23:45:AE:20
Duplicate MacAddress -----------------
Mac  00:00:CE:EE:D2:10 160.26.66.13
        <- 160.26.66.45 YAMAHA CORPORATION
Mac  00:00:CE:EE:D2:10 160.26.66.45
        <- 160.26.66.13 YAMAHA CORPORATION
```

加えて、週に一度、IP-MAC アドレスの対情報を管理者に送付する。

本学では、基幹スイッチ (Catalyst6500) の標準 ARP Table 保持時間が 4 時間であり、4 時間のうちに一度でも接続した場合には基幹スイッチ上に IP-MAC アドレスのテーブルが残ることから、ポーリングの頻度は、1 時間に 1 回としている。

4.4　無線 LAN 認証システム

無線 LAN については、EAP の一種である PEAP 認証を利用し、Radius サーバ経由で学内認証基盤のデータを用いて、ユーザ認証を行うことした。[7]

CISCO 社製 AP における設定例は次の通りである。

```
aaa new-model
!
aaa group server radius rad_eap
 server 160.26.ZZ.YY \\
   auth-port 1812 acct-port 1813
aaa authentication login \\
    eap_methods group rad_eap
!
dot11 ssid toyama
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   guest-mode
interface Dot11Radio0
 encryption mode ciphers aes-ccm tkip
 ssid ITC
!
radius-server attribute 32 \\
```

```
    include-in-access-req format %h
radius-server host 160.26.ZZ.YY \\
    auth-port 1812 acct-port 1813 key ZZZZZZ
radius-server vsa send accounting
```

PEAP 認証におけるシーケンスは図 2 に示すとおりである。

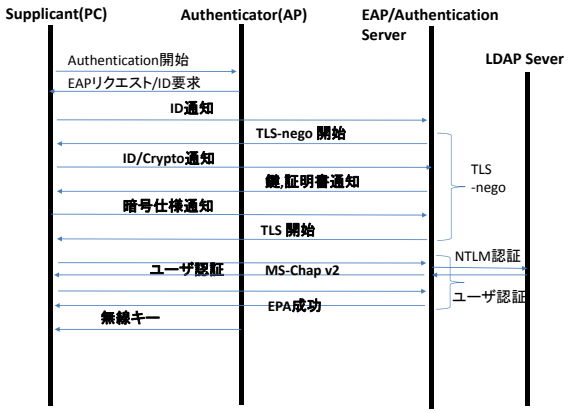

図- 2: PEAP 認証シーケンス図

IP アドレスから利用者を特定するのは、Radius サーバの記録

```
Sun Jun 26 12:28:58 2011 : Auth: Login OK:
[xxxx.ttt/<no User-Password attribute>]
(from client library2F_read2 port 11691
cli 0012.9d33.5b55)
```

DHCP サーバの記録

```
Jun 26 12:28:58 dhcpsvg dhcpd: DHCPREQUEST
for 160.26.YYY.204 from 00:12:9d:33:5b:55(ZZZ)
via 160.26.YYY.10
```

により可能となる。MAC アドレスの偽造は、認証時に記録されるため不可能であり、IP アドレスを手動で設定した場合には、認証時の MAC アドレスが Radius サーバに記録されており、Mac アドレスから MAC-IP 対応テーブル管理システムでその時に利用していた IP アドレスと MAC アドレスの対を確認することで可能である。PEAP 認証は、WPA/WPA2 において標準に組み込まれており、業務向けの Wi-Fi Alliance の承認機器で利用できる。

4.5 有線 LAN 認証における問題点

無線 LAN AP においては、認証手法が標準化されているため、メーカに依存しないシステムの構築が可能であった。しかし、有線 LAN 認証においては、下記に述べるのようないくつかの問題点がある。

1. メーカごとに認証部分の実装方法が異なる。
2. ネットワーク配下に HUB が接続される可能性がある。特に 802.1X 認証においてはポートあたり一台の機器が接続されると想定されており、HUB 経由で複数台が接続した場合の動作が不定である。
3. ファームウェアの更新によって、システムの動作が変更される場合がある。

4.6 有線 LAN 認証システム

有線 LAN 認証については、エッジスイッチで MAC アドレス認証と Web 認証を組み合わせて利用することとした。現在 MAC アドレス認証や Web 認証は多くのメーカで採用されている。MAC 認証はポートあたり複数の MAC アドレスの認証に対応し、Web 認証は IP アドレスごとに認証が行われるため、エッジスイッチの 1 つのポートに複数のユーザが同時に接続しても認証を行うことが可能である。

MAC アドレス認証や Web 認証を行うには、Radius サーバが必要となる。前述の問題点 1 と 3 を解決するために、有線 LAN 認証用の専用 Radius サーバを開発した。認証をすべて専用 Radius サーバで行い、Radius 側にメーカごとに対応した設定および attribute 属性を持たせることとした。これにより、メーカおよびファームウェアの違いによる動作の差異を吸収することができた。専用 Radius サーバは、機種や attribute が異なる認証スイッチからの認証を振り分ける機能、Mac アドレス認証機能、ユーザ認証からなる。MAC アドレス認証部分には三井情報社製の MKI SmartAuth Server を利用し、振り分け機能部分とユーザ認証の認証基盤への連携部分の開発を新たに行った。専用 Radius サーバの構成を図 3 に示す。

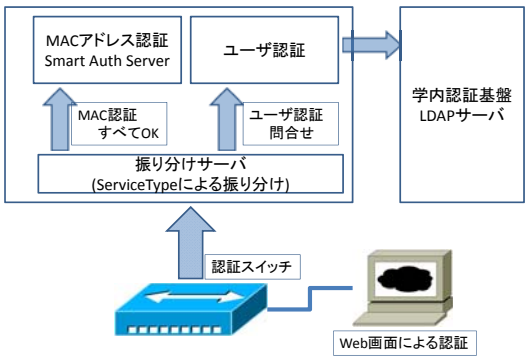

図- 3: 有線 LAN 認証用 Radius サーバ構成図

CISCO 社製 HUB における設定例は次の通りである。

```
aaa accounting auth-proxy default \\
   start-stop group radius
aaa accounting dot1x default \\
   start-stop group radius
aaa accounting network default \\
   start-stop group radius
!
ip device tracking
ip admission name rule1 proxy \\
   http inactivity-time 60
!
interface GigabitEthernet0/47
 switchport access vlan TTT
 switchport mode access
 ip access-group policy1 in
 authentication host-mode multi-auth
 authentication order mab webauth
 authentication port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 1
 spanning-tree portfast
 ip admission rule1
!
radius-server attribute 8 \\
   include-in-access-req
radius-server host 160.26.X.Y \\
   auth-port 1812 acct-port 1813 key ZZZ
radius-server vsa send authentication
```

有線 LAN 認証におけるシーケンスを図 4 に示す。

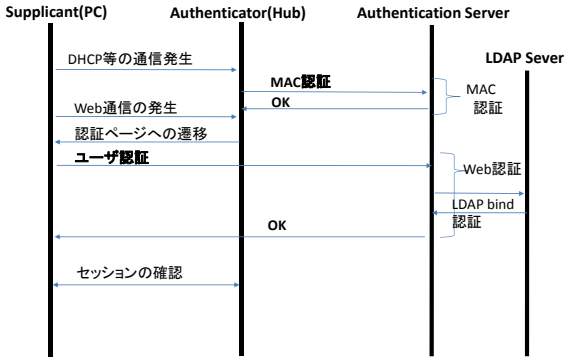

図- 4: 有線 LAN 認証シーケンス図

Radius サーバにおけるシーケンスを図 5 に示す。

利用記録は、Radius サーバ内にエッジの IP ごとのフォルダーに分けて格納される。利用記録の具体例を示す。MAC アドレス認証記録は、

```
Thu Jun 23 17:08:41 2011
    Acct-Session-Id = "0000033A"
    User-Name = "f0aabb086eee"
    Acct-Authentic = RADIUS
    Acct-Status-Type = Start
    NAS-Port-Type = Ethernet
    NAS-Port = 50047
    NAS-Port-Id = "GigabitEthernet0/47"
    Called-Station-Id = "00-12-CC-45-DD-FF"
    Calling-Station-Id = "F0-AA-BB-08-6E-EE"
    Service-Type = Framed-User
    NAS-IP-Address = 160.26.XX.101
    Acct-Delay-Time = 0
    Acct-Unique-Session-Id = "1c6bfff9ac26d8"
    Timestamp = 1308816521
```

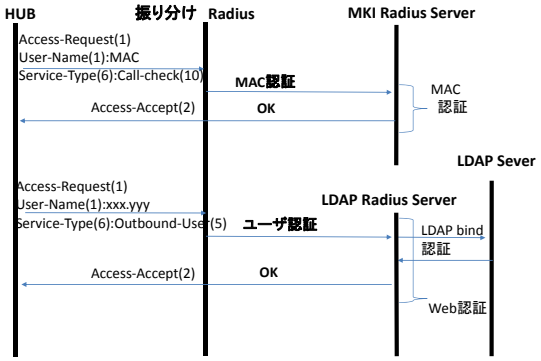

図- 5: サーバにおける Radius シーケンス図

```
    Request-Authenticator = Verified
```

と記録され、MAS-Port-ID から利用しているポートが、Calling-Station-ID から MAC アドレスを取得することができる。Web 認証の記録は、

```
Thu Jun 23 17:08:58 2011
    Acct-Session-Id = "0000033C"
    Calling-Station-Id = "160.26.24.178"
    NAS-Port = 50047
    NAS-Port-Id = "Gig"
    User-Name = "xxx.yyy"
    Acct-Authentic = RADIUS
    Acct-Status-Type = Start
    NAS-Port-Type = Ethernet
    NAS-Port = 50047
    NAS-Port-Id = "GigabitEthernet0/47"
    Service-Type = Outbound-User
    NAS-IP-Address = 160.26.XX.101
    Acct-Delay-Time = 0
    Acct-Unique-Session-Id = "074f11862693a4"
    Timestamp = 1308816538
    Request-Authenticator = Verified
```

と記録され、IP アドレスは、Calling-Station-Id 欄に記録され、ユーザ名は、User-Name に記録されることにより、IP アドレスからの利用者の特定が可能となる。

提案手法は、IP-MAC アドレスの対情報は MAC-IP 対応テーブル管理システムで確認しているため、ユーザを特定するためには、IP アドレス又は MAC アドレスのどちらか一方が特定されれば良い。

有線 LAN 認証システムでは、ユーザ確認の手段として学内認証基盤の統一 ID とパスワードを利用し Web 認証を行っている。本認証システムでの MAC アドレス認証の利用目的は、MAC アドレスがどの HUB のどのポートに接続されたかに関する情報を取得するためであり、認証の手段としては利用していない。そのため、Radius サーバは、すべての MAC アドレスに対して認証 OK を返答するように設計をしている。

MAC アドレスを認証のための手段として利用しない理由は、MAC アドレスは偽造が容易であるため、認証

用の個体識別番号として利用することは意味がないからである。

攻撃者が、調査のためにネットワークに接続した場合やMACアドレスを偽造した場合は、MACアドレス認証によって接続したエッジとそのポートが記録される。IPアドレスを手動で設定した場合には、Web認証によりIPアドレスが記録される。

加えて、有線LAN認証システムは、ポートごとに接続情報収集を目的とするMACアドレス認証と、ユーザ認証を目的とするMACアドレス認証かつWeb認証を管理者が選ぶことができる。具体的には、MACアドレス認証かつWeb認証の場合には、

```
authentication order mab webauth
```

と設定し、ポートに接続される機器のトレースが目的ならば

```
authentication order mab
no ip admission rule1
```

と設定すればよい。これにより一台のエッジスイッチで、委任されたLANと認証LANの機構を提供することができる。

5 システム評価

今回設計したシステムを、先述の7つの要件に基づいて評価する。

1. 富山大学全域に対する広域サービス
   PCごとの管理は、エッジによる認証で行われるため、エッジ機器のハードウェア性能による台数制限は存在するが、全体として利用数に対する制限はない。エッジとRadiusサーバとの間で通信が可能であれば、遠隔キャンパスであっても問題なく導入できる。三井情報社製Radiusの保証台数は、60,000台であり、本学での運用においては十分であると判断している。
   また、無線LAN認証はWindows, Mac, Android, iOS搭載機器については動作確認している。Linuxについては、ユーザから動作報告がある。有線LAN認証については、OSに依存しない実装となっている。

2. 性能低下の防止
   認証時には、認証サーバの負荷が問題となる可能性があるが、一度認証されると、すべての負荷はエッジの処理能力に依存する。認証機能を有しているエッジには専用ハードウェアが実装されており、性能限界に達することは少ないと考えられる。またエッジあたりの処理台数も、高々そのエッジに接続される台数である。本学の事例では、エッジあたりの収容数は、最高が90台で、平均は25台であった。認証サーバの負荷は、通信量とRadiusサーバの性能に依存する。一回の認証に必要な通信量は、無線LAN認証では、EAPメッセージで512Kbyte以下である。一方有線LAN認証では、Web認証とMAC認証の2回で8Kbyte以下である。そのため、ネットワークへの負荷はないと判断している。Radiusサーバによる認証はSmartAuth Server側が毎秒2,000台処理でき、認証基盤側は毎秒300回程度ならば問題なく認証できていることを確認している。

3. メーカ依存の禁止
   本認証システムでは、機種依存部分は有線LAN認証システムだけである。CISCO社以外のエッジに対応するためには、Radiusサーバの改良及びattribute追加にて対応することが可能である。

4. 導入コスト、運用コストの低減
   導入に際しては、既存のHUBのファームウェアをアップデートし、認証機能を追加することで対応した。導入から5年以上経過した認証に対応していないエッジに関しては更新が必要であったが、ユーザ数が少ない場合には上流のエッジで認証を行うことで対応できた。ネットワーク構成の変更の必要がなかったため、運用コストに関しては変化しなかった。認証システム側でユーザの追跡が可能となり、管理コストは低減できた。増加したコストとしては、認証用Radiusサーバの導入・保守コストがある。この費用については既存のRadiusサーバと統合により削減していく予定である。

5. 事前情報登録の削減
   MACアドレスやIPアドレスの登録作業は必要がない。頻繁に変更されるIPアドレスやMACアドレス等が発見された場合は、MAC-IP対応テーブル管理システムからの通知を受けて、管理者からユーザに問い合わせを行っている。IP-MACアドレスの対情報が正しいかの確認は別途行う必要がある。これについては毎年別途実施している実態調査により、突き合わせを行うことにより確認している。

6. 認証データの統合（学内認証基盤との同一ID）
   学内認証基盤のIDを利用し認証を行っている。このためID、パスワードを別途配布する必要がなく、導入をスムーズに行うことが可能となった。ユーザからの問い合わせも少なくなった。

7. IP-MACアドレステーブルの監視
   利用されていないIPアドレスはIP-MACアドレ

ステーブルの記録が存在しないことになる。これにより長期間利用していない IP アドレス等の把握ができる。

次に、LAN ごとのトレースレベルに対応しているかの評価であるが、委任された LAN において、情報コンセントごとに利用している IP アドレスと MAC アドレスの対情報を取得することは、エッジ側の設定を MAC アドレス認証モードで運用することにより可能である。また、認証 LAN においては無線 LAN、有線 LAN ともに利用者と IP アドレスと MAC アドレスの対情報を取得することが可能である。

最後に、脅威への対応であるが、認証 LAN においては認証情報を不正に利用されなければ、IP アドレス、MAC アドレスのどちらの偽造にも対応できる。委任された LAN において、IP-MAC アドレスの一方を実際に存在する機器と同一に設定すればトレースを回避することが可能であるが、このような場合には、正規の機器接続がされないことが必要である。もし同時に接続された場合には、MAC アドレス衝突はスイッチ側で MAC アドレスフラップとして検出され、IP アドレス衝突は正規の利用者側にエラーが発生する。このため、管理者が近くにいる委任された LAN では、このような攻撃の発生、または、その攻撃が成功する可能性は低いと判断している。

6　制限事項

現在、CISCO 社製 HUB の認証は、ポートあたり 8 台までという制限がある。そのため、多数の PC を接続している研究室において、そのままでは本システムによる認証が利用できないことが判明している。

このような 1 ポートに多数の接続を行う箇所については、今後、無線 LAN の利用の促進や情報コンセントの増設を検討している。

7　おわりに

既存ネットワークに導入可能なトレーサビリティネットワークを、MAC-IP 対応テーブル管理システム及び無線 LAN、有線 LAN 認証システムの構築により実装した。

これにより、不正利用の防止に寄与するだけでなく、ネットワークのレベルに応じた MAC-IP アドレスの対情報の保証、または、MAC-IP アドレス-利用者の対を取得することが可能となった。

現在、無線 LAN システムは全キャンパスで運用しており、有線 LAN 認証システムはキャンパスの一部にて運用を開始している。

今後は、このシステムを全学に広げるとともに、管理者が認証や利用状況のデータを Web から閲覧できるシステムの開発を検討している。

参考文献

[1] 鈴木 彦文，永井 一弥，浅川 圭史，今井 美香，不破 泰,”UTM を用いたユーザ認証ネットワーク「セキュアネット 2010」の構築”, 学術情報処理研究,No.14 p.21-30, 2010.

[2] 大谷 誠, 江藤 博文, 渡辺 健次, 只木 進一, 渡辺 義明,”シングルサインオンに対応したネットワーク利用者認証システムの開発”, 情報処理学会論文誌 Vol. 50 No. 3 1-9, 2010.

[3] 石橋 勇人, 山井 成良, 安倍 広多, 阪本 晃, 松浦 敏雄,”利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式”, 情報処理学会論文誌, Vol42 No1. p79-88, 2001.

[4] 大江　将史, 櫨山　寛章, 山本　成一, 白畑 真,”IEEE802.11 ワイヤレスネットワーク管理システムの構築と検証” , 電子情報通信学会論文誌. B, 通信 J87-B(10), p1607-1615, 2004

[5] CISCO Secure Access Control System

`http://www.cisco.com/web/JP/product/hs/security/acs/acs/index.html`

[6] ダイキン社製　PNDDA

`http://www.comtec.daikin.co.jp/IM/prd/pndda/`

[7] 沖野 浩二, 小林 大輔, 布村 紀男,”学外者向け認証無線 LAN の構築”, 富山大学総合情報基盤センター広報 ,Vol7 p.46-49, 2010.

[8] 沖野 浩二, 布村 紀男,”富山大学における認証基盤の整備による業務軽減評価”, 学術情報処理研究,No.14 p.31-38, 2010.

[9] Jonathan Hassell 著, アクセンス・テクノロジー訳, ”RADIUS ユーザ認証セキュリティプロトコル ”, オライリー・ジャパン,2003.