社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (3)
2008－CSEC－ 40 (3)
2008／3／6

仮想計算機環境における動的認証 VLAN 機能の実装方式

鈴木 春洋† 三宅 猛†† 北野 文章† 村瀬 晋二† 若山 公威††† 岩田 彰††

†株式会社 中電シーティーアイ 〒461-0005 名古屋市東区東桜 1-3-10
††名古屋工業大学大学院 〒466-8555 名古屋市昭和区御器所町
†††名古屋外国語大学 〒470-0197 愛知県日進市岩崎町竹ノ山 57 番地
E-mail: † {Suzuki.Shunyou, Kitano.Fumiaki, Murase Shinji} @cti.co.jp
††takes@mars.elcom.nitech.ac.jp, ††iwata@nitech.ac.jp, †††wakayama@nufs.ac.jp

あらまし 仮想計算機環境では内部の個々の仮想計算機に対し、認証結果に応じて VLAN を割り当てることが困難である．本研究では、認証ネットワークにおける認証機能を、仮想計算機上の仮想認証機能デバイスドライバとして実装して、認証結果に応じた VLAN ID を付加する機能を加えこの課題に対応した．

キーワード 仮想計算機 ネットワークアクセス認証 PKI RADIUS IEEE802.1X VLAN デバイスドライバ ARP

Mounting method of dynamic authentication VLAN function in virtual machine environment

Shunyo SUZUKI† Takeshi MIYAKE†† Fumiaki KITANO† Shinji MURASE†
Kimitake WAKAYAMA††† Akira IWATA††

†Chuden CTI CO.,LTD. 1-3-10 Higashisakura, Higashi-ku, Nagoya, Aichi 461-0005 Japan
††Nagoya Institude of Technology Gokisocho, Shouwa-ku Nagoya, Aichi 466-8555 Japan
†††Nagoya University of Foreign Studies 57 Iwasakicho-Takenoyama, Nisshin, Aichi 470-0197 Japan
E-mail: † {Suzuki.Shunyou, Kitano.Fumiaki, Murase Shinji} @cti.co.jp
††takes@mars.elcom.nitech.ac.jp, iwata@nitech.ac.jp, †††wakayama@nufs.ac.jp

Abstract In the virtual machine environment, it is difficult to allocate for VLAN dynamically to each virtual machine inside.

It supported this problem by loading an authentication feature about the authentication network into the this research as the virtual authentication functional-device driver on the virtual machine and having the function to add VLAN ID into this.

.Keyword Virtual machine, Network Access Control, PKI, RADIUS, IEEE802.1X, VLAN, Device Driver, ARP

1. はじめに

計算機性能の向上に従い、1 台の計算機上に複数の仮想計算機環境を構成して、同時に稼動することが可能になり近年急速に普及しつつある．このような環境を仮想計算機システムという．

仮想計算機システムのサーバ機能への用途では、複数のアプリケーションサーバの稼動や、異なる OS で動くシステムを集合稼動させるなど、効率的な運用管理面での効果が期待されている．また、旧バージョンの OS で稼動するソフトウェアの稼動や可用性向上にも効果的である．

一方、利用者端末環境では、電子メールや Web アク

セスなどの情報共有系業務、勤怠管理や会計処理などの社内基幹系業務、営業管理やアプリケーション開発など個別業務など、種類の異なる業務を遂行している．

このような業務を1台の計算機上に複数の仮想計算機環境を作って遂行することが、機能上あるいはセキュリティ上好ましい．特にアプリケーション開発の現場では、異なるOSのプログラム開発など、利用者端末の安定度が損なわれる用途では、利用者端末での仮想計算機環境の利用価値は非常に高い．

ここで、計算機へのVLAN適用を考える．計算機がサーバ用途の場合、各々の仮想計算機のVLAN IDは固定的に設定され、頻繁に変更されることはない．また、デバイスドライバで固定的にVLAN IDを割り当てる方法について LINUX[1]では一般的に準備され、Windowsでも DDK[2]で紹介されており実現可能である．

利用者端末用途の場合には、検疫ネットや認証状況に応じたVLAN IDの割り当てをしたい場合がある．本稿では利用者端末用途での仮想計算機環境の VLAN 適用について考察する．

なお、情報管理の観点から利用者端末で利用サービス毎に情報資源にシンクライアントなどでアクセスして課題解決方法もあるが、通信環境が悪い場所での作業や、サーバと異なるOSでのアプリケーション開発環境でなど、利用者端末上で実施したい作業がある．このような条件が想定される場合は、シンクライアント環境は不向きである．その為、利用者端末での仮想計算機環境をそれぞれの業務に対応させることが機能的である．

2. 認証 VLAN システム

認証ネットワークシステムは、ネットワークを利用したい端末の電子証明書などのユーザ情報に基づいて接続可否の判断をして、認証可の場合に予め登録されたユーザの権限に基づきネットワークを利用可能な状態にする．認証ネットワークシステムとしては、IEEE802.1X 認証ネットワークシステムが多く利用されているので、本稿ではこのシステムの利用を前提としている．

また、VLANシステムはイーサネットで構成されたネットワークを幾つかの論理ネットワークに分割して、組織内ネットワークを形成するなど、セキュリティを向上する仕組みである．VLANを構成したい場合幾つかの選択肢があるが、本稿では IEEE802.1Q システムを前提としている．

認証ネットワークシステムでは、VLANシステムと組み合わせて、認証時のユーザ情報に基づいて VLAN ID を認証スイッチに設定することにより、動的に論理VLANへの接続を可能にする認証LANシステムを構成することが出来る．

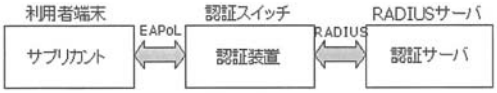

図1 IEEE802.1X認証ネットワークシステム

認証ネットワークシステムを図1示す．システム構成は、利用者端末にはサプリカント機能が、認証スイッチには認証装置機能が、RADIUSサーバは認証サーバ機能を持つ．

認証動作時、サプリカントと認証装置間はEAPoLで認証装置間と認証サーバ間はUDP上のRADIUSプロトコル上のEAPで認証動作を行う．

認証動作は、図2に示すように、認証装置からのEAPリクエストから始まりEAP Success/Failureで終わる一連の認証動作で行われる．

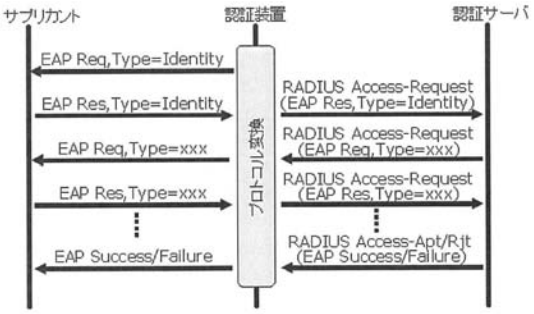

図2 認証動作

サプリカントは認証装置の指示に従い、利用者端末の電子証明書などユーザ情報を認証装置にEAPプロトコルで送信する．認証装置は、EAP でサプリカントから送られた情報を RAUIUS プロトコルに乗せて認証サーバに送る．認証サーバは、送付された電子証明書の有効性などのユーザ情報を、登録されたユーザ情報と照合して、認証の可否をVLAN IDなど接続条件とともに認証装置に返信する．その後、認証装置はその結果をサプリカントに通知することで一連の認証手順が完了する．

このように認証は、利用者端末のユーザ情報に基づいて行われるのである．従って必ずしも利用者端末自身を認証していることではない．このような性質を利

用して、組織内の共用利用者端末からユーザ認証に応じた情報資源アクセス管理や、動的認証 VLAN システムを構成して組織内の利用者端末の移動に際してユーザ認証の柔軟的な対応に効果的な技術である.

3. 仮想計算機システム

仮想計算機システムは、一台の実計算機上に複数の仮想計算機を稼動させるシステムである. 近年の計算機性能の向上により身近な技術になってきたが、VMware[2]や Xen[3]など実用的なシステムが提供されるようになってきた.

先に述べたようにサーバ用途として、ブレードサーバやネットワークデータサーバと連携して、保守性や可用性を大幅に向上させる解決策として応用が進んでいる.

一方、利用者端末での仮想計算機の利用は大規模で組織的に利用される例は少ないものの、VLAN システムとの連携で、可用性やセキュリティの高いシステムを実現する可能性がある. 仮想計算機システムでのネットワーク構成を図 3 に示す.

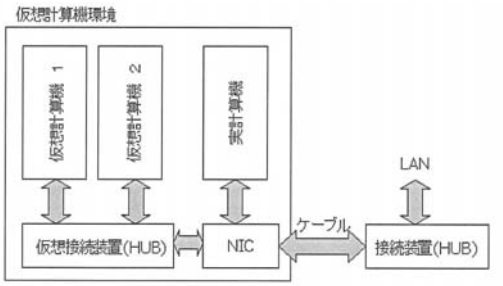

図 3　仮想計算機環境のネットワーク構成

仮想計算機環境におけるネットワーク構成について説明する.

図 3 に示すように仮想計算機環境では仮想計算機各々に論理的な仮想ネットワークアダプタが用意されている. 仮想計算機システムはこのアダプタを介して仮想接続装置(HUB)に接続され、実際のネットワークアダプタを通して外部ネットワークに接続される.

このような接続のため、通常は仮想計算機間の通信に制限はない. また、仮想ネットワークアダプタの MAC アドレスは、仮想計算機環境から割り当てられる論理的なものである.

4. 仮想計算機環境での認証 VLAN システム適用の課題

仮想計算機環境では、仮想計算機が仮想 HUB を通じて接続されるので、認証ネットワークシステムでの認証スイッチに相当する機能を配置することができない. 従って、仮想計算機毎の認証動作、ネットワーク接続の制御、認証で得た VLAN ID の付与が困難である.

先に述べたが、各仮想計算機のネットワークドライバの機能で、固定的に VLAN ID を割り当てることが可能である. サーバなど設置位置が決められ VLAN ID に変化無い場合にはこれで十分といえるが、利用者端末のように、組織内を移動する可能性がある端末については、利用者認証時に組織ネットワーク側の接続装置の VLAN パケット通過設定と、仮想計算機内の VLAN ID 付与が連動して動作する必要があるため、現状の仕組みでは対応できない課題がある.

これとは別に、ネットワーク全般の脅威として、ネットワーク接続が許されていない端末接続の危険性がある. 認証ネットワークを利用したとしても、管理者の意図しない接続変更などで接続される可能性がある. その対策として、ネットワークケーブルの施錠や、ARP Spoofing 技術を利用した不正接続排除方法などがあるが、設置や設定に労力がかかり運用に課題がある.

5. 提案方式

仮想計算機システムのネットワークへの接続認証時における、ネットワーク接続する認証スイッチへのトランクポート設定、各仮想計算機への認証結果に応じた VLAN ID 割り当てと、認証システムと同期した不正接続防止機能を備えたシステムを提案する.

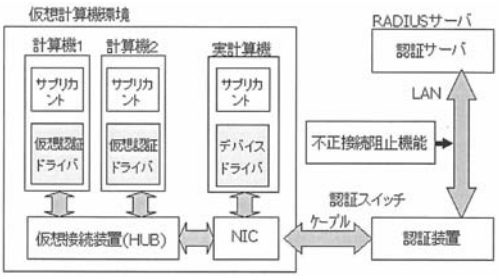

図 4：提案の認証システム構成

5.1. 仮想計算機環境のネットワーク認証

仮想計算機環境上の各仮想計算機を認証する前に、まず仮想計算機環境自身がネットワークに接続する必要がある. 仮想計算機環境のサプリカントとネットワ

ークを接続する認証スイッチ、認証サーバで構成する認証システムで、仮想計算機環境のユーザ認証を行う．

仮想計算機環境上がユーザ認証に成功した場合には、ユーザ設定された VLAN ID を通過させるよう、認証スイッチをトランクポート設定に変更する．

5.2.仮想計算機への VLAN ID の割り当て

仮想計算機環境において、各々の仮想計算機がそれぞれの VLAN に独立して接続するために、各仮想計算機のネットワークドライバ上に仮想認証ドライバ追加する．仮想計算機の認証システムの構成は、仮想計算機上のサプリカントと仮想認証ドライバ、認証サーバで構成される．認証システムで、仮想計算機のユーザ認証を行う．

仮想計算機のユーザが認証された場合には、認証サーバより VLAN ID が付与されネットワークに接続される．

順次その他の仮想計算機も同様にそれぞれのユーザ認証を経て、VLAN ID を付与される．

なお、仮想計算機環境のネットワークドライバの機能拡張ではなく、仮想 HUB の機能を拡張することでも対応可能であるが、本稿では実装の容易性、仮想計算機環境への適用性を考慮して、各仮想計算機への実装とした．

仮想認証ドライバのへ追加機能は、認証時の EAP 電文の中継と、に RADIUS サーバからの認証結果に応じた、接続の可否と VLAN ダグの付与である．

仮想認証ドライバとサプリカント間の通信は 802.1X 上の EAP で行われ、一方 RADIUS サーバと仮想認証スイッチ間は RADIUS プロトコル上の EAP で行われる．そのため、サプリカントの EAP メッセージを RADIUS 電文に変換する必要が生じる．

RADIUS 電文には、認証符号が含まれており、RADIUS クライアントが生成する乱数、共有鍵情報が含まれているため RADIUS システムのセキュリティ機能の要であるため注意が必要である．

5.3.不正接続の阻止

IEEE802.1X システムでは、管理者が意図しない接続装置の増設での不正接続を阻止できない課題がある．不正接続阻止として、ブロードキャストドメイン内の ARP の挙動を監視することによる不正接続阻止方式が有効である．この方式としてよく知られている ARP spoofing を利用した方式[4][5][6]では、予め許可された IP アドレス又は MAC アドレスを登録する必要がある．認証ネットワークへの適用として、ネットワーク構成機器など最低限の登録は必要なものの、認証で得られる MAC アドレスと認証状態と組み合わせて許可アドレスとして不正接続阻止対策とした．

本提案では、不正接続阻止機能を許可接続検出機能、不正接続阻止機能で構成する．許可接続検出機能は、認証状況を把握して接続許可利用者端末の MAC アドレスを記憶する．また、予め登録された最小限度の MAC アドレスを併せて許可アドレスとして不正接続阻止機能に伝える．

不正接続阻止機能は、ブロードキャストドメイン内の ARP ブロードキャストを監視して、許可接続検出機能から送られた MAC アドレスと比較して、存在しない場合不許可アドレスとして認識し、ARP テーブルに該当の MAC アドレスを持つ端末に対し、定期的に別の適当な MAC アドレス準備し ARP リクエストを用いて書き換えることで、実質的なネットワーク活動を阻止する．

悪意のある不正接続者は ARP ブロードキャスト無しに接続を試みる可能性があるので、ネットワーク接続機器やサーバなど、特に守る必要のある機器のポートをミラーして不許可 MAC アドレスの検出をする．

6. 実装

仮想認証ドライバの機能を Windows XP 用のデバイスドライバとして、また不正接続検出および阻止機能を LINUX プログラムとして実装した．

6.1. 仮想認証装置デバイスドライバ

認証ネットワークにおいて認証機能は、サプリカントと認証サーバの間に直列に配置される．本稿の認証機能は、利用者端末に内に配置するため、ネットワークデバイスドライバへの追加機能として実装した．利用者端末のネットワーク通信は、全てこのドライバを経由して行われる．

ネットワークデバイスドライバ[7][8][9]に認証機能を追加する実装方法は幾つか考えられるが、EAP の RADIUS プロトコルへの変換機能をどこに持たせるかにより構成が異なる．本稿では、サプリカントを OS 標準で提供されているものを利用したかったため、仮想スイッチサービスとして OS の USER MODE で動作するプログラムとして実装し、サプリカント、フィルタ（中間ドライバ）、仮想スイッチサービス、IP プロトコルドライバで構成した．

図 6 に利用者端末内のプログラム配置を示す．サプリカントと IP プロトコルドライバは OS 標準の機能を利用する．仮想スイッチサービスは EAP パケットの RADIUS プロトコルへの変換機能を含む．フィルタは MAC アドレスの置き換え、アクセス制御、IEEE802.1X

パケットのリダイレクトを行う．

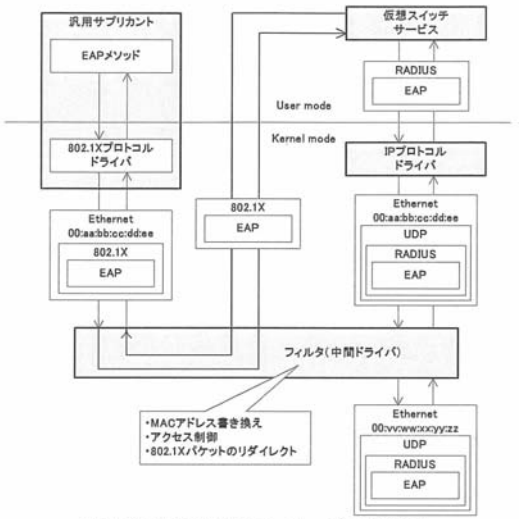

図 6 利用者端末内のプログラム配置

図 7 デバイスドライバの組込イメージ

6.2. 許可接続検出機能

本システムでの接続許可の定義は、ネットワーク機器など最小限の登録端末と認証許可済みの利用者端末である．従って、許可端末の MAC アドレス情報を把握してそれ以外の MAC アドレスを持つ端末は不正接続として判断する．

認証許可端末の判断は、認証装置と認証サーバ間の RADIUS プロトコルを監視して「ユーザ名」「Calling-Station-Id」「許可ステータス」「VLAN ID」属性を取得して認証状況を確認して判断する．また認証許可端末に関しては、定期的に Ping リクエストで接続維持を確認し、応答がなくなった場合には許可端末のエントリから排除して管理する．

このようにして得た許可 MAC アドレスは、不正接続阻止組織能に引き渡される．

なお、RADIUS パケット内の認証符号で、サーバと認証装置間のセッションが管理されているので、事前共有鍵や暗号シーズの適切な管理がなされていれば、改ざんやなりすましの危険性は極めて低いので、偽装認証パケットによる誤動作は考えにくい．

6.3.不正接続阻止機能

不正接続監視機能は、ネットワーク内の ARP 挙動を監視して、登録外の端末接続を発見した場合には、当該端末の ARP テーブルを書き換える動作を定期的に行い、ネットワーク内の通信を阻害する．不正接続端末が静的な ARP テーブル設定をした場合、ARP ブロードキャストが生じないことから、不正接続を発見しにくい．このケースの対応として、サーバやゲートウェイなどユーザ共用のポートにミラーポートに設定し、ARP 情報を監視することにより不正接続を監視する．不正接続の端末の ARP テーブルが静的に設定されている場合、外部から変更できないが、通信相手の機器の ARP テーブルを変更することにより通信を阻止することが出来る．

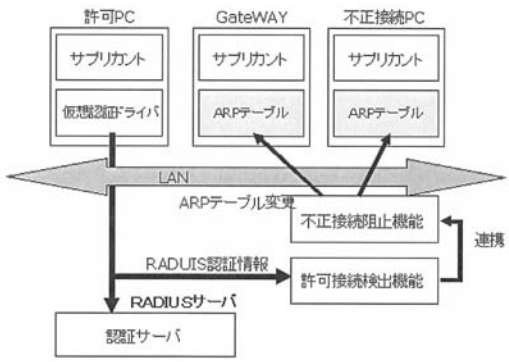

図 8 不正接続の検出と阻止

7. 考察

7.1. 脅威面の考察

脅威面評価として、RADIUS 認証システムに纏わるものと、不正端末阻止方法に関する課題を考察する．

RADIUS 認証システムは、事前共有鍵の長さや、暗号シーズの乱数を適切に管理することにより一定のセキュリティが保たれるとされている[10]ため、RADIUS 認証システムを適用する際には、これらの対策が必要で

ある．本稿ではこれら対策が適切に行われている環境を前提とする．

本提案では、RADIUS 認証電文の内容を根拠として認証可否を判断することから、この電文の信憑性を確保する必要がある．すなわち、管理者が設置していない RADIUS サーバ通信や、RADIUS 認証電文の偽装動作が懸念される．この課題に対しては、事前共有鍵の共有や RADIUS 電文内の認証符号を確認することにより対応可能である．

次に、不正接続を阻止する ARP Spoofing の有効性について考察する．本提案では、認証過程を経て許可 MAC アドレスを得る方法をとっているので、事前許可 MAC アドレスは、ネットワーク機器、サーバ機器、プリンタ機器などに限られるため、事前許可登録 MAC アドレスを用いた不正接続の確率を減らすことが出来、また認証状況を把握することから認証許可 MAC アドレスの不正接続を減らすことが出来る．

一方悪意を持った不正侵入者は、更に巧妙な手段で接続を試みることが予想される．

ネットワークスイッチを基本としたネットワークでは、基幹ネットワークに全てのネットワーク電文が流れるわけではない．従って ARP ブロードキャストを生じないアドレス解決は、ip-sentinel などの一般的な ARP Spoofing を利用した手法では阻止することが困難である．そこで本提案では、ルータなどのゲートウェイ機器やサーバ機器については、それらが接続されるネットワークスイッチにミラーポートを設けて不許可 MAC アドレスを検出することにより、不正接続を検出して双方の MAC アドレスに ARP テーブルを書き換える作業をする．不正接続端末が ARP で静的に MAC アドレスを設定していても、少なくとも共用機器側の ARP テーブルを書き換わるので通信を阻害することが出来る．

7.2. システム面の考察

評価環境は仮想計算機環境である VMware 上に、クライアント機能として Windows 標準のサプリカントとクライアント証明書、図 6 で示した仮想スイッチモジュールとフィルタモジュールを配置した．

動作確認のためにモニタ機能として仮想計算機環境のネットワーク電文を Ethereal[11]で観察し、認証動作状況を確認した．

結果は Ethereal で認証状態を観察した結果、想定通り稼動することを確認した．

8. 今後の課題

計算機性能が高性能化されるにつれ、仮想計算機環境を利用する機会が増えてくると予想される．しかし、本提案のような計算機環境の場合、仮想計算機毎にユーザの証明が必要になってくる．

現状の認証ネットワークの場合、社員証や従業員証を利用する機会が多い．しかし、これらは通常 1 名に 1 枚しか発行されない．今回のように仮想計算機毎にユーザ認証が必要な場合は、利用する論理ネットワーク毎にユーザ認証が必要なり、一人に複数のユーザ ID を割り当てることが煩雑である．そこでシングルサインオン的な連携システムで利便性を高めていく必要がある．

9. まとめ

本稿では、利用者端末の仮想計算機環境で、各仮想計算機への動的な VLAN ID 割り当てを可能にするシステムを提案し実装して課題を解決した．そして、認証ネットワークで懸念される、管理者が意図しない不正接続を阻止する機構を組み合わせることにより、セキュリティを向上した．

文献

[1] LINUX VLAN ドライバ構成例
http://www1.jpn.hp.com/products/software/oe/linux/mainstream/support/doc/option/nic/exp_bondvlan.html

[2] VMware
http://www.vmware.com/jp/

[3] Xen を使ってみよう
http://www.valinux.co.jp/contents/tech/techlib/xen/index.html

[4] ip-sentinel
http://www.nongnu.org/ip-sentinel/

[5] IntraPOLICE
http://biz.national.jp/Ebox/i_breaker/intrapolice/

[6] L2BLOCKER
http://www.l2bloker.com/

[7] Windows XP デバイスドライバ プログラミング
浜田憲一郎 著 技術評論社

[8] Microsoft Windows Driver Development Kit 3790.1830 PASSTHRU.SYS-Sample NDIS Intermediate Driver.

[9] Microsoft Windows Driver Development Kit 3790.1830 NDIS connection-less protocol driver sample

[10] RADIUS—ユーザ認証セキュリティプロトコル
Jonathan Hassell (著),オライリージャパン

[11] Ethereal
http://www.ethereal.com