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

2007－ＣＳＥＣ－38 (18)
2007／7／19

仮想認証スイッチによる認証ネットワークシステムの提案

鈴木 春洋† 北野 文章† 三宅 猛‡ 岩田 彰‡

†株式会社 中電シーティーアイ 〒450-0003 名古屋市中村区名駅南 1-27-2
‡名古屋工業大学大学院 〒466-8555 名古屋市昭和区御器所町
E-mail: †{Suzuki.Shunyou, Kitano.Fumiaki}@cti.co.jp
‡takes@mars.elcom.nitech.ac.jp, iwata@nitech.ac.jp

あらまし IEEE802.1X認証システムはLANへの不正接続防止に有効である．しかし、全ての端末接続にIEEE802.1X認証システムに対応するポートを設ける必要があり、既存のLANから移行するためには多大な費用や労力が必要であるという課題がある．そこでIEEE802.1X認証システムのうち、通常はネットワークスイッチに実装されるAUTHENTICATOR機能を、接続する端末内で動作させることにより課題を解決したシステムを提案する．

キーワード IEEE802.1X,RADIUS,L2 SWITCH,EAP,MAC,ARP,Device Driver,Supplicant

An authentication network system using virtual authenticator module

Shunyo SUZUKI† Fumiaki KITANO† Takeshi MIYAKE‡ Akira IWATA‡

† Chuden CTI CO.,LTD. 1-27-2 Meieki-Minami, Nakamura-ku Nagoya 450-0003 Japan
‡ Nagoya Institude of Technology Gokisocho, Shouwa-ku Nagoya 466-8555 Japan
E-mail: †{Suzuki.Shunyou, Kitano.Fumiaki}@cti.co.jp
‡takes@mars.elcom.nitech.ac.jp, iwata@nitech.ac.jp

Abstract The IEEE802.1X authentication network system is effective to an illegal, connected prevention to the LAN . However, the shift from standard LAN to the authentication network system has problems in cost and the labor now. In this proposal, it proposes the system that solves the problem by including virtual authenticator module on the client-PC.

Keyword IEEE802.1X,RADIUS,L2 SWITCH,EAP,MAC,ARP,Device Driver,Supplicant

1. はじめに

組織内のネットワークへの接続では、無線接続や外部からの接続を除いて、十分な対策がとられている状況に無い．この課題に対し企業内のＬＡＮではネットワーク・アクセス・コントロールの一環として対策が進んでおり、IEEE802.1X認証システム技術を利用した実施例が増えている．IEEE802.1X認証システムはネットワーク接続制御，VLAN，動的認証 VLAN，検疫的接続手法に活用されつつある．

IEEE802.1X 認証システムはポートベースでの接続を基本としており、接続される端末の認証要求に対し、接続ポートを開放することで接続を認可するものである．

この認証システムは端末の接続管理に効果的であるが、IEEE802.1X認証システムに対応するポートを接続する端末の数だけ準備する必要がある。従って、従来技術で構成された LAN では全てのポートをIEEE802.1X 認証システム対応に交換する必要があり、多大な費用と労力を必要とする．

本提案では、IEEE802.1X認証システムの機能のうち、AUTHENTICATOR 機能を接続する端末にソフトモジュール形式で内蔵させることにより、従来のネットワーク構成を大きく変更することなく、IEEE802.1X認証システムを構成することを可能にして課題解決を目指した．

また、本提案システムによって生じる副作用について考察し対応策も併せて提案する ．

2. IEEE802.1X 認証システム

IEEE802.1X 認証システムは SUPPLICANT, AUTHENTICATOR, AUTHENTICATION SERVER で構成されている.

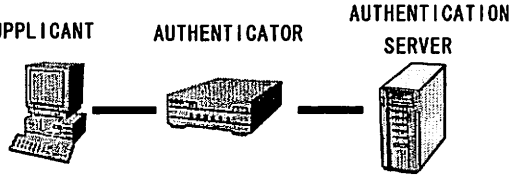


図 1　IEEE802.1X 認証システムの構成

SUPPLICANT は接続を要求する端末に配置され、認証時に端末内での認証手順に対応する.

AUTHENTICATION SERVER はネットワークに接続する組織内の認証情報を管理しており、SUPPLICANT からの認証要求に対して、認証要求情報を確認して認可を与える機能を持つ.

AUTHENTICATOR は SUPPLICANT（端末）と AUTHENTICATION SERVER（認証サーバ）の中間に位置して、認証手順のプロトコル変換と認証サーバからの認可情報によるネットワーク接続制御を役割とする.

通信プロトコルは SUPPLICANT と AUTENTICATOR の間が IEEE802.1X(EAPoL)、AUTENTICATOR と AUTHENTICATION SERVER の間が RADIUS プロトコルである.

認証手順は、SUPPLICANT からの認証要求に対して AUTENTICATOR が中継し、AUTHENTICATION SERVER が認証要求に応じた認可情報を AUTENTICATOR に伝えて最終的に SUPPLICANT に伝達する. その際、AUTENTICATOR は認可情報に基づき端末接続動作を行うことで、端末がネットワークに接続される.

3. IEEE802.1X 認証システム導入の課題

IEEE802.1X 認証システムはネットワークへの端末接続制御に効果的であり、検疫ネットや VLAN 技術と組み合わせて、ネットワーク管理のために重要度が高い技術である.

しかし、既存ネットワークへの IEEE802.1X 認証システム導入は、その概念がポートベース制御であるため、全ての端末接続ポートを IEEE802.1X システム対応に置き換える必要が生じてくる。これには多大な費用と労力が生じることが懸念され、この認証システム普及の阻害要因の一つになっている.

また、IEEE802.1X 認証システムを導入しても、基幹ネットワークへの故意又は不注意なポート増設への対応や、ポートへのリピータハブの接続など、ネットワーク管理者が意図しない接続を完全には排除しきれない課題が残存する.

4. 課題解決方法の提案

4.1. 課題解決方法

前述のように IEEE802.1X 認証システムは SUPPLICANT, AUTHENTICATOR,AUTHENTICATION SERVER で構成されており、それぞれ、端末・認証スイッチ・認証サーバに機能配置されている.

本提案では、AUTENTICATOR の機能を端末に包含することにより、既存ネットワークから IEEE802.1X 認証ネットワークシステムへ移行する際に、IEEE802.1X 認証システム対応の認証スイッチ設置を不要にして、端末へのソフトウェア導入作業が伴うものの、移行の際に生じる費用や労力を最小限度にして課題を解決しようとするものである.

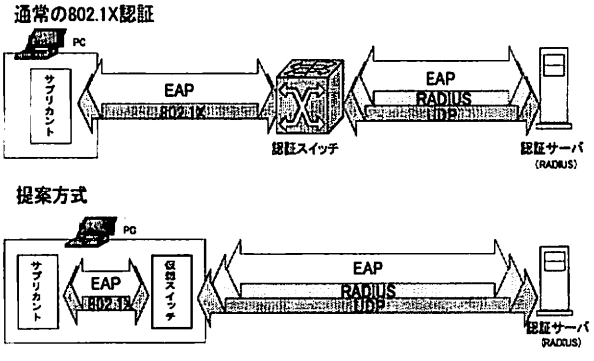


図 2　提案方式の概要

4.2. 提案の問題点

IEEE802.1X 認証ネットワークシステムでは、AUTHNTICTOR すなわち認証スイッチをネットワーク境界として端末の接続を制御するシステムである.

本提案では、この境界を端末内に持つことから問題が生じる.

通常の IEEE802.1X 認証システムは、認証サーバの認可応答に応じて認証スイッチのポートが開いて端末のネットワーク接続が可能になる. 一方、提案のシステムでは、ネットワーク側で AUTENTICATOR 機能を持つ端末かそうでないかを区別することが出来ないので、AUTENTICATOR 機能を有していても差別化できず、どのような端末も自由にネットワークへの接続が出来てしまうことになる.

4.3. 問題点の解決

前項で述べた問題点はかなり根本的な課題で見過ごすことができない.

本提案では、ネットワーク接続認証時における認証

結果に応じたネットワーク接続管理機能を付加することでこの問題を解決する.

IEEE802.1X認証システムでの認証時には、端末の情報を認証サーバに送り、サーバはその情報を元に接続の可否を決定する.その際SUPPLICANTは端末のユーザ情報と共にMACアドレスを認証サーバに送る.

ネットワーク接続管理機能は、図3に示すように認証サーバからの認証情報に望づきネットワーク利用を制御するものである. 本提案では、認証サーバからの認証情報に替えて、認証時の認証動作を傍受してこの機能を代替した. 従って認証許可検出機能と通信無効化機能で構成する.

認証許可検出機能は、認証動作中のパケットを傍受して、許可された端末のMACアドレスとユーザ情報を記憶して、許可MACアドレスリストを作り通信無効化機能に通知する. 通信無効化機能は、ネットワークに流すべきパケット（MAC アドレス）とそうでないパケットの判別を行う. ネットワークに存在してはいけないMACアドレスをもつパケットは、ARP偽装技術を利用して通信を阻害して実質的な接続を阻害する.

ARP テーブルの偽装制御によるネットワーク制御はARP spoofingとして知られており、ip-sentinelのようなソフトウェアとして実装されている.

ネットワークに接続されたARPテーブルを制御して、あらかじめ登録された端末以外の通信を妨害する仕組みである.

従来の ARP spoofing ツールの利用に際し、本提案への適用では端末接続時の認証情報に基づいて制御するため、端末情報の登録の必要が無い. 従って最小限度のネットワーク構成機器の設定を除き、端末等のMACアドレス等の登録は不要である.

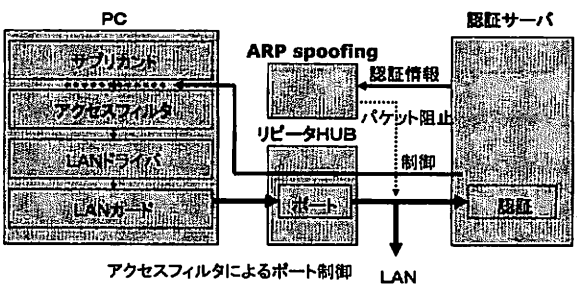


図3 提案システムの機能構成

5. 実装

5.1. クライアントモジュール

クライアントモジュールはWindows2000について実装した.

端末には、SUPPLICANT、AUTHENTICATOR 機能を配置する. SUPPLICANTは市販のものを利用することとして、通常はネットワークスイッチが担うAUTHENTICATOR機能をクライアントモジュールとして端末に実装する.

アクセスフィルタの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. 本提案では変換機能を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、SUPPLICANT、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する.

SUPPLICANT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.

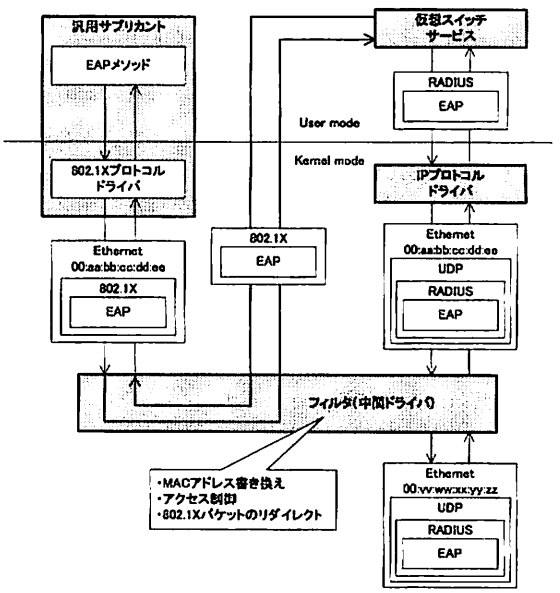


図4 端末内処理の構成

フィルタ（中間ドライバ）で行うMACアドレスの書き換え、アクセス制御、MAC アドレスの変換はARP spoofing機能が識別容易なように特別なMACアドレスを付与している.

このMACアドレス変換する機能は、認証動作時に一時的にARP spoofing 機能を保留するために利用する. 特別な範囲のMACアドレスに変換することにより、通信無効化機能がクライアントモジュールからの認証動作を許し、ネットワーク接続管理機能からの認証認可

可否情報によって認証ネットワークを制御する.

クライアントモジュールは認証実施時にAUTHENTICATION SERVER(RADIUS)と通信を行い、RADIUSの許可指示に従い接続の動作を実施する.

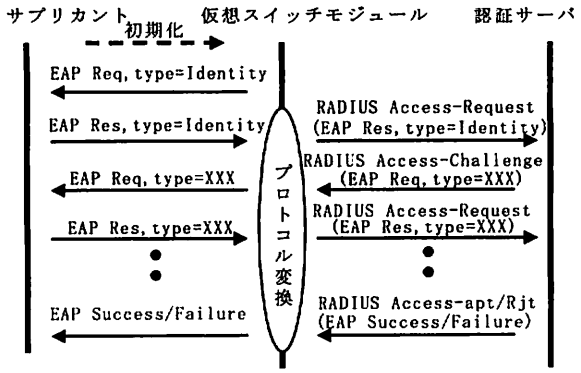


図5 プロトコル変換処理イメージ

5.2. ネットワーク接続管理機能

先に述べたように、本提案でのクライアントモジュールとAUTHENTICATION SERVERの設置により、基本的なネットワーク接続の認証は可能であるが、クライアントモジュールのインストールされていない端末や管理者の意図しない接続に対し無力である. 本提案ではネットワーク接続管理機能を設けてこの課題に対応している. ネットワーク接続管理機能は、認可状態を把握する認証許可検出機能と、未許可端末通信を阻害する通信無効化機能で構成される.

5.2.1. 認証許可検出機能

認証許可検出機能は、IEEE802.1Xシステムにおいて AUTHENTICATION SERVER と AUTHENTICATOR 間のRADIUSプロトコル上のEAP-TLS認証状況を監視して、認証成功のMACアドレスを検出する。検出したMACアドレスを正規接続端末として通信無効化機能に通知する.

5.2.2. 通信無効化機能

通信無効化機能は、ネットワーク内のトラフィックを監視して、あらかじめ登録されたネットワーク機器の通信と、認証許可検出機能で検出された正規端末以外の端末通信を妨害する. 通信無効化の方法は無効化する端末のARP情報を制御することにより、対象端末の要求する通信を阻害して、実質的な通信を不能にする. このような通信無効化手法はARP spoofing技術として実用化されており、既に適用された製品が市場で入手可能であるため、本提案ではこの技術を利用することにする.

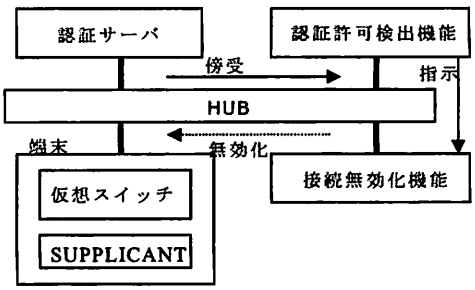


図6 提案の認証システムの実装構成

6. 評価

6.1. 認証システムの評価

今回は本提案の実現性と有効性の確認の中心となる仮想スイッチの動作について評価した.

6.2. 評価環境

評価環境は VMware 上に、クライアント機能としてWindows標準のSUPPLICANTとクライアント証明書、図4で示した本提案で実装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.

また、動作確認のためにモニタ機能としてEtherealで認証動作状況を確認した.

評価環境の詳細及び設定内容は下記の通りである.

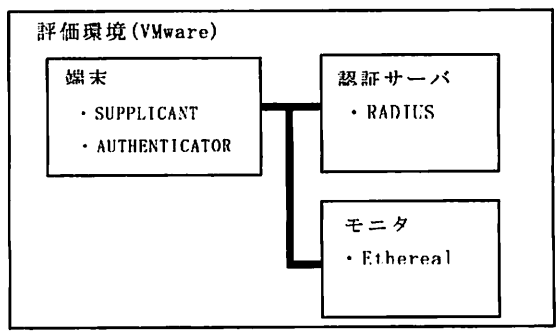


図7 評価環境のイメージ

(1)モニタ

VMwareホストマシンとして実装.

ア. 仕様

ホスト名	orca
IPアドレス	172.17.20.172
MACアドレス	00:12:3F:98:AD:9E
OS	Microsoft Windows XP Professional Version 2002 Service Pack 2
CPU	Pentium4 2.8GHz
メモリ	2GB

イ. 使用ソフトウェア

a. 仮想マシン

VMware Server Console Version 1.0.0

build-28343

b．パケットキャプチャ

Ethereal Version 0.10.14

WinPcap version 3.1

(2)認証サーバ

VMware ゲストマシンとして実装．

ア．仕様

ホスト名	salmon
IP アドレス	172.17.20.67
MAC アドレス	00:0c:29:74:42:B0
OS	CentOS release 4.3　(2.6.9-34.EL)

イ．使用ソフトウェア

FreeRADIUS 1.1.2（RADIUS サーバ）

ウ．FreeRADIUS 設定（追加・変更部分のみ）

user.conf（RADIUS アカウント設定）

```
"TEST1 Takeshi"          Auth-Type := EAP
        Tunnel-Type = VLAN,
        Tunnel-Private-Group-ID = 1,
        Tunnel-Medium-Type = IEEE-802

DEFAULT                  Auth-Type := Reject
```

eap.conf（EAP-TLS 設定）

```
default_eap_type = tls
fragment_size = 1024
include_length = yes
check_crl = no
check_cert_cn = "TEST1 Takeshi"
check_cert_issuer = "/C=JP/ST=Some-State/
O=NIT/OU=Ailab/CN=TM CA"
cipher_list = "DEFAULT"
```

clients.conf（Authenticator 設定）

```
clients 172.17.20.171 {
        secret          = ********
        shortname       = w2kprovm
}
```

(3)端末 Supplicant／Authenticator

VMware ゲストマシンとして実装．

ア．仕様

ホスト名	w2kprovm
IP アドレス	172.17.20.171
MAC アドレス	00:0C:29:32:5B:50
OS	Windows 2000 Professional Service Pack4

イ．使用ソフトウェア

SUPPLICANT ソフトウェア

Microsoft 802.1XSUPPLICANT

（Windows 2000 Service Pack4 標準）

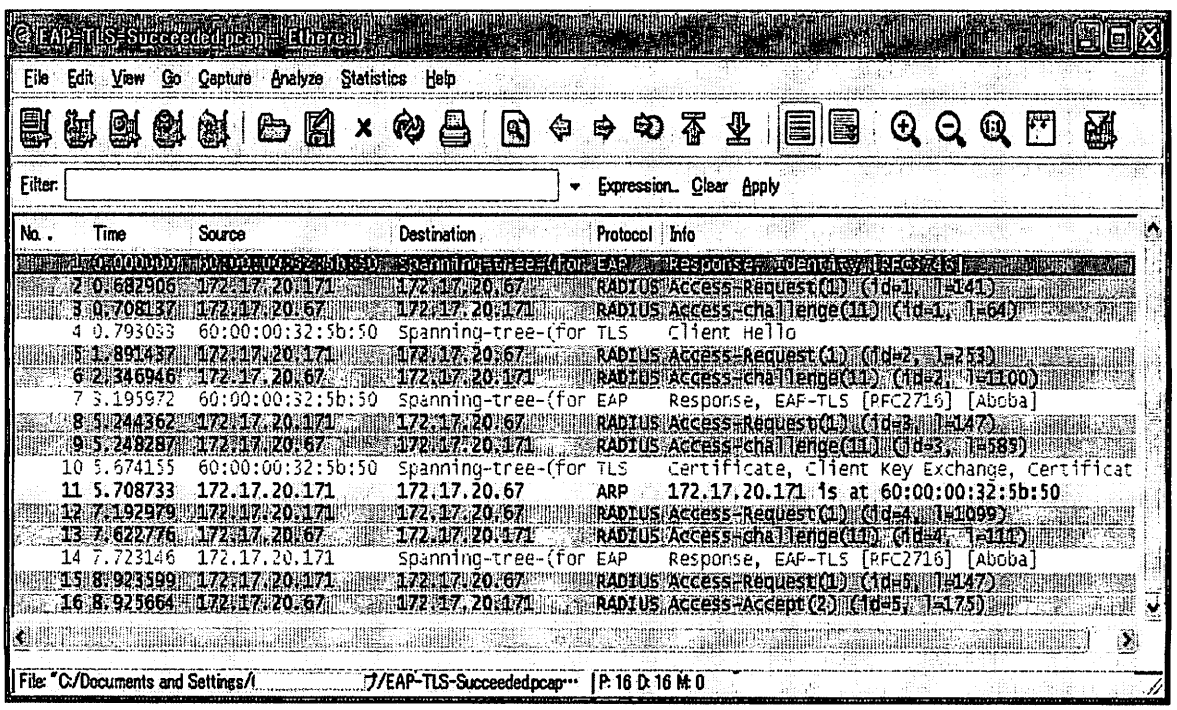
Authenticator ソフトウェア

本件開発ネットワークドライバ

RADIUS サーバの IP アドレスとして 172.17.20.67 を指定

仮想 MAC アドレスとして 60:00:00:32:5B:50 を指定

図 8　認証動作結果



評価の考察

評価環境で実際に認証動作を Ethereal でキャプチャした内容を図８に示す.

キャプチャしたデータではクライアントモジュールのプロトコル変換の動作を見ることが出来る. キャプチャしたデータを見る限り図５で示した変換処理を忠実に反映しており、IEEE802.1X 認証システムとして稼動していることを表している. また、実際に RADIUS が応答をしていることから意図した通り動作していることが判る.

認証処理に時間が掛かっているのは、必要であるが、SUPPLICANT とフィルタドライバ間の通信の同期に起因するものであり、今後改善すべきだと考えている.

具体的な不正 MAC アドレス排除方法の検討とその実装・評価時にこの改善を再度検討したい.

6.4. その他

Windows XP 以前の場合、IEEE802.1X 認証の動作の前に Active Directory ドメインのログイン認証動作が実行される.

IEEE802.1X 認証前にはネットワーク的にドメイン・コントローラへのアクセスが許可されていないので、結果的に OS 付属の SUPPLICANT では、Active Directory を利用することができない場合がある. このような場合は、サードパーティ製の SUPPLICANT で対応する.

本提案では、この課題に対してクライアントモジュールに、立ち上げ時のドメイン・コントローラへのアクセスを例外的に許可する機能を含むことにより対応する.

最新の OS である Windows VISTA の SUPPLICANT では改善されているようであるが、本提案では今回開発したクライアントモジュールのフィルタ(中間ドライバ)部に実装し、この問題に対応するよう工夫した.

7. 今後の課題

本研究では接続端末へ AUTENTICATOR 機能の実装と評価を中心に行った.端末用の AUTENTICATOR 機能は提案通りの動作することが確認されたので、認証システムとして動作することが期待できる状況である. しかしながら、ネットワーク接続管理機能（認証許可検出機能・通信無効化機能)の実装と評価を行っていない.

認証結果をモニタする機能については同時並行的に進めている別研究の成果を待って実装する予定である.

通信無効化機能については、既に商品化されている IntraPOLICE、L2BLOCKER、ip-sentinel などの実績のあるものを使用することとしているが、本システムでは IEEE802.1X 認証システムの認可結果に基づいたパケット阻止機能を必要としているため、許可 MAC アドレスとしての反映時間が懸念事項である. この部分を除けばシステムとして大きな課題はないので、今後はこれらの実装を行った後、ワークグループ規模での実証試験、一般の IEEE802.1X 認証システムとの混用動作試験を実施して行きたい.

また、本研究では今後の展開としては、Windows 2000 以外の OS への対応、EAP-TLS 以外の認証手順への対応、ダグ VLAN 機能、ＶＰＮの実装を考慮したい.

8. まとめ

本提案は IEEE802.1X 認証システムの AUHENTCATIOR 機能をモジュールとして端末にインストールして IEEEE802.1X 認証システムを構成することを目標として、認証システムを提案し実証及び評価を行った.

既存ネットワークから IEEE802.1X 認証システムシステムへの移行は多大な労力と費用が必要であるが、本提案は端末へのモジュール導入という煩雑さが伴うものの、IEEE802.1X 認証システムシステムへ移行時での部分的な認証スイッチの置き換えや、認証スイッチを全く使用しない認証システムへの展開が期待される.

文献

[1] Windows XP デバイスドライバ プログラミング
浜田壺一郎 著 技術評論社

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

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

[4] FreeRADIUS
http://www.freeradius.org/

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

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

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

[8] Cisco Networks 2006
シスコの認証・検疫ソリューション SEC-201

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