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

2007－ＣＳＥＣ－38 (25)
2007／7／19

ネットワーク構成に依存しない動的認証VLANの構成方法に関する提案

坂本 和俊† 鈴木 春洋†† 岩田 彰†

† 名古屋工業大学大学院 〒466-8555 名古屋市昭和区御器所町
†† 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
E-mail: †skmt@mars.elcom.nitech.ac.jp, iwata@nitech.ac.jp, ††Suzuki.Shunyou@cti.co.jp

あらまし 地理的に離れた拠点間を仮想的な専用ネットワークで繋ぐものとして，Virtual Private Network(VPN) という技術がある．VPNを構築するものは多くあるが，その内の一つとして，OpenVPNというものがある．OpenVPNを用いることでネットワークセグメントを跨いだVirtual Local Area Network(VLAN) を構築することが可能である．しかし，OpenVPNは，接続条件として設定ファイルを事前に端末に登録しておかなければならないので，静的なVPN接続となってしまう．そこで本稿では，IEEE802.1X認証システムと組み合わせることで，設定ファイルをダウンロードすることにより，動的にVPNの接続を変更するシステムを提案する．
キーワード OpenVPN，動的認証VLAN，IEEE802.1X，RADIUS

A composition method of network-independent dynamic authentication VLAN

Kazutoshi SAKAMOTO†, Shunyo SUZUKI††, and Akira IWATA†

† Nagoya Institute of Technology Gokisocho, Showa-ku, Nagoya-shi, 466-8555 Japan
†† Chuden CTI CO.,LTD 1-27-2 Meieki-Minami, Nakamura-ku, Nagoya-shi 450-0003 Japan
E-mail: †skmt@mars.elcom.nitech.ac.jp, iwata@nitech.ac.jp, ††Suzuki.Shunyou@cti.co.jp

Abstract Virtual Private Network (VPN) is a technology that constructs a private network between bases geographically away. OpenVPN is one of the technologies that construct VPN. OpenVPN can construct Virtual Local Area Network (VLAN) over public network. However, because OpenVPN should register the configuration file in the terminal as connected condition, it becomes a static VPN connection. In this paper, we proposes the system that dynamically changes the VPN connection by downloading the configuration file by using the IEEE802.1X authentication system.
Key words OpenVPN, dynamic authentication VLAN, IEEE802.1X, RADIUS

1. まえがき

パソコンの性能向上や価格低下のため，企業や大学などでは，パソコンの台数が非常に多くなっている．そのまま，スイッチングハブに接続すると，ブロードキャストフレームが増加し，ネットワークの性能が落ちてしまう．そこで，Virtual Local Area Network(VLAN) という技術が注目された．

VLANは，物理的なネットワーク構成に依存せずに，仮想的なグループを設定することができる．VLANにはポートVLAN，プロトコルVLAN，タグVLANなど，さまざまな種類が存在する．その中でも，IEEE802.1X認証システムを用いた認証VLANは，不正接続を防止する役割も持ち、優れた技術である．しかし，認証VLANだけに限らず，VLANはすべてスイッチの機能として動作している．つまり，LAN内のみの利用に限られてしまう．

そこで，OpenVPN [1] の仮想的なLANに注目した．OpenVPNはVirtual Private Network(VPN) という，仮想的な専用ネットワークを構築するためのソフトウェアである．VPNは公衆ネットワークを利用していながら，セキュリティを確保した通信を行うことが可能であるため，専用線の変わりに利用される．VPNはトンネリングと暗号化により，セキュリティを確保する．トンネリングは従来通信するパケットを，別のプロトコルのパケットで包むこと (カプセル化) により行われる．OpenVPNはレイヤ2またはレイヤ3でカプセル化することが可能であるが，レイヤ2でカプセル化することにより，ネットワークセグメントを跨いで仮想的なLANを構築することが可

能になるという特徴がある．つまり，LAN 内だけでなく，ネットワークセグメントを跨いで，VLAN を構築している．

しかし，OpenVPN は事前に端末に登録した設定ファイルにより，VPN の構築を行う．ユーザが端末を変更すると，変更後の端末にはユーザの設定ファイルが無く，VPN の構築ができなくなってしまう．つまり，静的な VPN 接続であり，ユーザがどの端末を利用しても，VPN の構築が可能になる，動的な VPN 接続が必要である．

そこで，本稿では，IEEE802.1X 認証システムを用いることにより，設定ファイルを登録する必要なく，ユーザ認証に成功した場合に限り，設定ファイルをダウンロードすることにより，動的な VPN 接続を行うシステムの提案を行う．

2. IEEE802.1X

IEEE802.1X 認証システムは，LAN スイッチや無線 LAN アクセス・ポイントから LAN を利用可能にする前に，ユーザ認証を行うための技術である．

図 1　IEEE802.1X 認証システム

IEEE802.1X 認証システムは，図 1 のように，サプリカント，オーセンティケータ，認証サーバの組合せにより構成されている．サプリカントは，認証を受ける端末に必要な認証クライアントソフトであり，オーセンティケータは，LAN スイッチや無線 LAN アクセス・ポイントのことで，認証に応じてポートを開閉する機能を持っている．また，オーセンティケータは，サプリカントから受け取った認証に必要な情報を，認証サーバに転送する．認証サーバは，サプリカントから送られてきた情報をもとに，ユーザの認証を行うサーバのことである．認証サーバとしてよく使用されているのが，RADIUS サーバである．

サプリカントとオーセンティケータ間は EAPoL，オーセンティケータと RADIUS サーバ間は EAP over RADIUS で通信する．認証プロトコルである EAP は，さまざまな認証方式を使用することが可能であり，パスワードで認証する EAP-MD5 や，公開鍵証明書を利用する EAP-TLS などがある．

図 2 に IEEE802.1X 認証システムによる，認証手順を示す．

3. 動的認証 VLAN

VLAN は，図 3 に示すように，物理的なネットワーク構成に依存することなく，仮想的にネットワークをグループ化するための技術である．

VLAN の中でも，IEEE802.1X 認証システムを利用した動的認証 VLAN は，LAN 構成の自由度を高め，またセキュリティに配慮された優れたシステムである．IEEE802.1X 認証システム

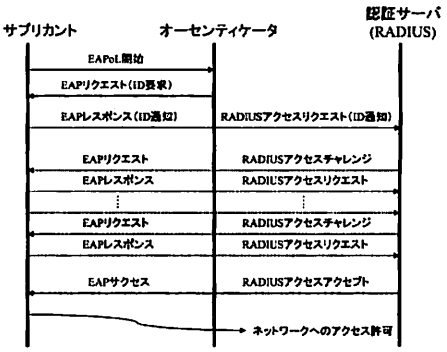

図 2　認証手順

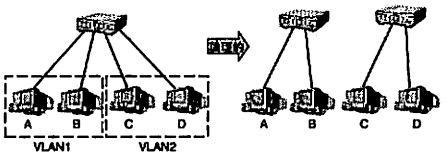

図 3　VLAN

ムは，クライアントがアクセスしてきたときに認証を行う．認証に成功すると，ユーザごとに設定されたポリシーを適用するという動作が可能である．この技術を VLAN と組み合わせることで，ユーザ認証に成功したときに，ユーザがどの VLAN に接続するのかを決定でき，ユーザがアクセスしてきたポートを特定の VLAN に組み込むことで，動的な認証 VLAN を構成している．

VLAN はスイッチの機能として動作するため，LAN 内だけに限定され，ネットワークセグメントを跨る VLAN を構成することはできない．この課題は，ネットワークセグメントを跨いで，仮想的な LAN を構築することのできる，OpenVPN を利用することで対応することができる．

4. OpenVPN

4.1 概　　要

OpenVPN は，VPN を構築するためのソフトウェアである．特別なハードウェアを必要とせず，オープンソースであるため導入コストを抑えることができる

特徴として，次のようなことがあげられる．

- オープンソースである．
- さまざまなプラットフォームで動作する．
- TUN/TAP デバイス [4] を利用することで，カプセル化，暗号化を行う．
- カプセル化はレイヤ 2 もしくはレイヤ 3 で行う．
- 実際の通信には UCP，TCP を選択することが可能である．
- OpenSSL がサポートする任意のアルゴリズムによる暗号通信が可能である．
- LZO による通信圧縮が可能である．

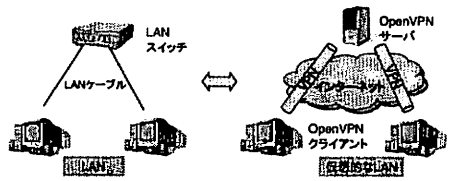

図 4　通常の LAN と仮想的な LAN の比較

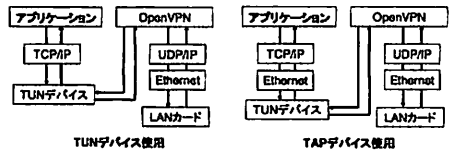

図 5　OpenVPN の流れ

- 接続条件の記された設定ファイルをもとに起動する．

TUN デバイスを利用した場合には，レイヤ 3 でカプセル化を行い，TAP デバイスを利用した場合には，レイヤ 2 でカプセル化を行う．レイヤ 2 でカプセル化を行うと，図 4 のように，ネットワークセグメントを跨る仮想的な LAN を構築することが可能である．また，実際の通信に TCP を用いることにより，NAT やプロキシを介しての通信も行うことができる．

VPN を構築するためには，デバイスに TUN，TAP のどちらを利用するのか，実際の通信に用いるプロトコルは TCP，UDP どちらにするのかなど，さまざまな設定が必要になってくる．OpenVPN は，これらの設定を，設定ファイルに記述し，事前に端末に登録しておく．そして，起動時にこの設定ファイルを参照し，VPN の構築を行う．設定ファイルの一部を以下に示す．

port　通信に使用するポート番号
dev　使用する仮想デバイス（tun もしくは tap）
remote　接続先サーバのホスト名もしくは IP アドレス，およびポート番号
ca　CA 証明書のパス指定
cert　サーバ証明書のパス指定
key　サーバ秘密鍵のパス指定
dh　DH 鍵のパス指定

上述したように，設定ファイルの中には，接続先 OpenVPN サーバの IP アドレスも記されている．つまり，OpenVPN クライアントは設定ファイルにより，接続先サーバが決定される．接続先サーバが決定されるということは，どの仮想的な LAN に接続するかが決定されることになる．

OpenVPN での通信の流れを図 5 に示す．まず，アプリケーションのデータは TCP/UDP や Ethernet プロトコルを通過し，TUN/TAP デバイスに届く．TUN/TAP デバイスは届いたデータを，OpenVPN へと渡す．OpenVPN は暗号化などの処理を行い，TCP/UDP，IP などのプロトコルを使用して，送信先へと送られる．

4.2　VLAN の課題解決

第 3 章で述べたように，VLAN はスイッチの機能として動作しているので，LAN 内だけに限定され，ネットワークセグメントを跨る VLAN を構成することが不可能である．OpenVPN は，レイヤ 2 でカプセル化することでネットワークセグメントを跨る仮想的な LAN を構築することが可能である．この仮想的な LAN は，接続するサーバーごとに変わる．つまり，接続するサーバーが違う場合には，別の仮想的な LAN に繋がることになる．よって，これはネットワークセグメントを跨る VLAN であると考えることができる．

4.3　課　　題

しかし，OpenVPN の仮想的な LAN を用いることで，ネットワークセグメントを跨る VLAN を構築することはできるが，そのためには，設定ファイルを事前に端末に登録しておく必要がある．前述したように，設定ファイルには，接続するサーバの IP アドレスも記述されている．どのサーバに接続するか，つまりどの VLAN に接続するかは，使用する端末により決定されていしまう．

例えば，ユーザが端末を変更した場合，今まで利用していた設定ファイルが変更後の端末にはなく，今まで通りに VPN 接続をすることができなくなる．同じように構築するためには，同じ設定ファイルを，変更後の端末に登録する必要がある．

つまり，通常の OpenVPN は静的な VPN 接続であり，ネットワークセグメントを跨る VLAN は静的なものとなってしまうという課題がある．

5.　提案システム

4.3 節で述べたように，OpenVPN クライアントは，起動時に設定ファイルを参照する．設定ファイルには，さまざまな VPN 接続条件が記されており，その条件をもとに VPN 接続を行うが，この設定ファイルは事前に端末に登録しておく必要があるため，VPN 接続が静的なものとなる．そこで，OpenVPN と IEEE802.1X 認証システムを組み合わせることにより，動的な VPN 接続を行うシステムを提案する．

5.1　概　　要

提案システムでは，設定ファイルを事前に個々の端末に登録せずに，IEEE802.1X 認証システムによる認証に成功したときに限り，認証サーバ端末から OpenVPN クライアントに，設定ファイルを送信することで，動的に VPN の接続を行う．

また，OpenVPN による VPN 接続では，SSL/TLS での相互認証のために，認証局証明書，クライアント証明書，クライアント秘密鍵が必要となる．そのため，これらのファイルも，設定ファイルと同様に，認証に成功したときに送信する．

このように，ファイルを認証の度にダウンロードすることにより，ユーザが使用する端末を変更した場合でも，VPN 接続に使用するファイルは全てユーザ自身のものとなる．つまり，どの端末を利用しても，ユーザは自分の仮想的な LAN に繋が

ることが可能になる.

認証には EAP-TLS を利用することで，証明書を用いた認証を行う．よって，ユーザは，IC カードなどにより自分の証明書を持ち運ぶだけで，どの端末を利用しても自分の証明書の検証を行ってもらい，自分のファイルを送信してもらうことができる.

図 6 に提案システムの概要図を示す.

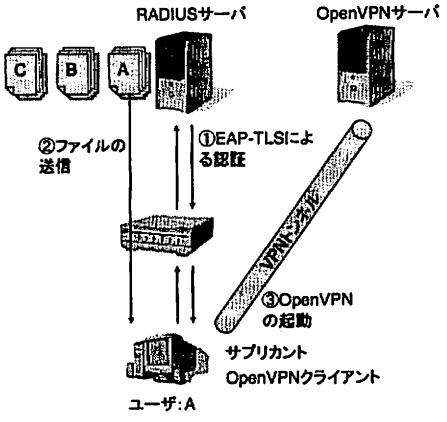

図 6 提案システム

5.2 動作手順

以下に提案システムの動作を示す。

（1） ユーザが IC カードなどで持っている，個人の証明書を，IEEE802.1X 認証システムを用いた EAP-TLS により検証する.

（2） 認証に成功した場合、ユーザに応じた OpenVPN 設定ファイル、認証局証明書、クライアント証明書、クライアント秘密鍵を認証サーバ端末から OpenVPN クライアント端末へと送信する．認証に失敗した場合、認証サーバ端末は何も OpenVPN クライアント側に送信しない.

（3） OpenVPN クライアント端末は受信したファイルをもとに、自動で OpenVPN を起動する.

（4） OpenVPN が終了したときに認証サーバ側から送られてきたファイルを全て削除する.

一番最初に利用するときに，事前の準備として，認証サーバー端末にユーザごとの設定ファイル，認証局証明書，クライアント証明書，クライアント秘密鍵を保存しておく必要がある.

5.3 ファイルの削除

提案システムでは，OpenVPN 終了時に認証サーバから送信されてきた各種ファイルを削除する．削除せずに，端末に残したままにしておくと，別のユーザがその端末を利用したときに，IEEE802.1X 認証システムによる認証に成功せず，ファイルが送信されてこなくても，端末に残っているファイルを使用することで，VPN 接続を行うことが可能になってしまい，勝手に別のユーザの仮想的な LAN に繋がってしまうからである.

6. 実　　装

6.1 RADIUS パケットキャプチャ

提案システムでは，認証に成功した場合に限り，認証サーバ端末から OpenVPN クライアント端末に，各種ファイルを送信する．そのためには，IEEE802.1X 認証システムによる認証に成功したのか，失敗したのかを判断する必要がある.

IEEE802.1X 認証システムにおいて，認証サーバに RADIUS を用いた場合，RADIUS サーバとオーセンティケータ間での通信は RADIUS プロトコルにより行う．RADIUS プロトコルは UDP/IP プロトコルを利用して送受信される．RADIUS プロトコルのフォーマットを図 7 に示す.

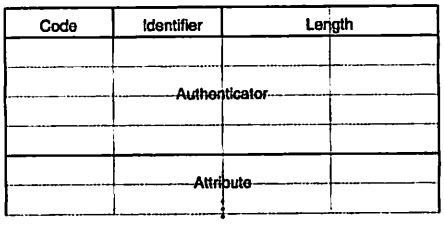

図 7 RADIUS プロトコルフォーマット

図 7 からわかるように，RADIUS パケットの先頭には種別コード（Code）がある．RADIUS パケットは，この Code により，用途がわけられる．Code の後には複数の要求を区別するための識別子（Identifier），RADIUS パケットの長さ（Length），データの偽造を防止するために使用する認証符号（Authenticator）が続く.

Code の中に Access-Accept(2) というものがある．この Code の RADIUS パケットは，認証許可の応答パケットである．よって，認証に成功したかどうかは，RADIUS パケットをキャプチャし，その Code の部分をチェックし，Access-Accept(2) であるかどうかにより判断する.

また，RADIUS プロトコルでは属性値ペア（Attribute Value Pair）というフォーマットでさまざまな情報を交換できるようになっている．属性値ペアのフォーマットを図 8 に示す.

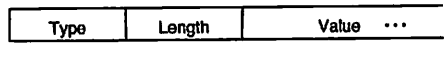

図 8 属性値ペアフォーマット

属性値ペアは属性タイプ（Type），属性の長さ（Length），属性値（Value）により構成されている．Type の一つとして，User-Name(1) があり，これはユーザ名の情報が格納されている．よって，User-Name(1) という属性値ペアを調べることで，ユーザの判断を行う.

Access-Accept パケットは，User-Name の属性値ペアを持っていることにより．Access-Accept パケットと User-Name の属性値ペアを持ったパケットとの対応付けを行う必要は無く，

Access-Accept パケットだけを確認するだけで，認証に成功したユーザを正しく判断できる．

7. 評　　価

提案システムにより，OpenVPN クライアントの端末が変更しても，同じ OpenVPN サーバに接続されるかについて評価を行った．

7.1 評価環境

提案システムの評価環境を図 9 に示す．表に

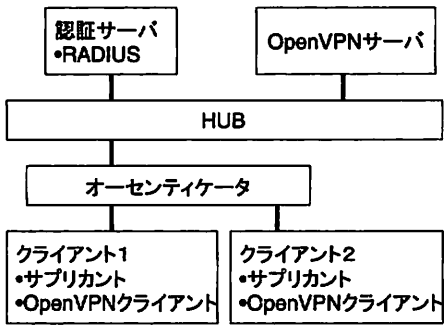

図 9　評価環境

認証サーバ端末　認証サーバとして，FreeRADIUS を使用した．RADIUS パケットをキャプチャし，ファイルを送信するプログラムを実装している．また，OpenVPN クライアントに必要なファイルは，すでに登録済みである．端末の仕様は表 1 に示す．

表 1　認証サーバ仕様

OS	Microsoft Windows XP Professional SP2
IP アドレス	192.168.0.1

オーセンティケータ　オーセンティケータとして，Cisco Catalyst 2950 を使用した．

OpenVPN サーバ　OpenVPN サーバの設定ファイルは図 10 に示すような設定となっており，証明書などはすでに登録済みである．OpenVPN サーバ端末の仕様は表 3 に示す．

サーバ設定

```
port 1194
proto udp
dev tap
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
```

図 10　OpenVPN サーバ設定ファイル

クライアント　クライアント端末には，サプリカントと OpenVPN クライアントが実装されている．サプリカントとして，Windows 2000 標準のサプリカントを使用．OpenVPN クライアントの設定は図 11 に示す．この設定ファイル，また，証明書などは，クライアント端末でなく認証サーバに登録されている．端末の仕様は表 3 に示す．

表 2　OpenVPN サーバ仕様

OS	Microsoft Windows XP SP2
IP アドレス	192.168.0.2

クライアント設定

```
client
proto udp
dev tap
remote 192.168.0.2 1194
ca ca.crt
cert client.crt
key client.key
```

図 11　OpenVPN クライアント設定ファイル

表 3　クライアント仕様

OS	Microsoft Windows 2000 SP2
IP アドレス（クライアント 1）	192.168.0.3
IP アドレス（クライアント 2）	192.168.0.4

7.2 評価結果

評価環境のもと動作させた結果，認証成功時に各種ファイルを送信することが確認できた．また，そのファイルをもとに OpenVPN クライアントが起動すると，OpenVPN サーバと VPN 接続ができ，VPN による通信が可能であることが確認することができた．

また，クライアントの端末を変更して，同じように動作させた．クライアント端末を変更したが，送信されてくるファイルは同じであり，VPN 接続する OpenVPN サーバも同じであった．

端末を変更しても，同じ OpenVPN サーバに接続することが可能であり，動的な VPN 接続ができているこが確認できた．

8. 考　　察

8.1 ファイル送信時のセキュリティ

IEEE802.1X 認証システムによる認証成功により，各種ファイルを認証サーバ端末から，OpenVPN クライアント端末に送信するが，この通信を盗聴し，他人のファイルを利用することが可能となってしまう．また，これらファイルは重要なものが多く，他人に見られることさえ避けるべきである．

そこで，これらファイルをユーザの公開鍵により暗号化し送信する方法をとる．これで通信を盗聴されていても，内容はわからず，安全にファイルの送信が可能となる．

8.2 ファイル複製の対処

設定ファイルなど，認証サーバ端末から送信されるファイルは，OpenVPN 終了とともに削除することで，端末に残ることはなくなるが，OpenVPN が終了する前にコピーすることが可能である．コピーしたファイルがあれば，その設定ファイルにより，誰でも VPN 接続が可能になってしまい，設定ファイルのユーザの仮想的な LAN につながってしまう．

そこで，この課題に対し，設定ファイルなどをユーザの公開鍵で暗号化することで対応する．ユーザの公開鍵で暗号化することで，復号できるのは本人のみとなり，他人がファイルをコピーしても，復号できず全く意味のないファイルとなる．

また，もう 1 つの提案として，VPN 接続時にユーザ名とパスワードを入力する方法をとる．もし，他人の設定ファイルを複製し，利用しようとしても，パスワードは本人しか知らず，パスワードがわからないため，VPN 接続ができない．

9. ま と め

OpenVPN はネットワークセグメントを跨いで仮想的な LAN を構築することができるが，そのために必要な設定を設定ファイルとして事前に端末に登録しておく必要がある．そのため，OpenVPN での VPN 接続は静的なものになっていた．

そこで，OpenVPN と IEEE802.1X 認証システムを組み合わせることにより，設定ファイルを事前に登録せずに，IEEE802.1X 認証システムによる認証に成功したときに送信することで，動的に VPN 接続を変更することを可能とした．

また，通常の動的認証 VLAN では不可能だった，ネットワークセグメントを跨いだ動的認証 VLAN の構築が可能となった．

文　献

[1] OpenVPN
http://openvpn.net/

[2] Jonathan Hassell, 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

[3] freeRADIUS
http://www.freeradius.org/

[4] Universal TUN/TAP driver
http://vtun.sourceforge.net/tun/

[5] WinPcap
http://www.winpcap.org/