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

2007－ＤＤ－62（11）
2007／7／27

サーバ型多重帰属 VPN サービスアーキテクチャ

谷本　茂明†

†NTT 情報流通プラットフォーム研究所　〒180-8585　東京都武蔵野市緑町 3-9-11
E-mail:　†s.tanimoto@m.ieice.org

あらまし　近年，企業におけるイントラネット環境は，FW や NAT 等の NW セキュリティ技術の進展に加え，無線 LAN の高速・広域化等により，様々な場所での利用，いわゆるユビキタス環境での利用が可能になり，一層の利便性向上が図られている．このようなイントラネット環境の進展に伴い，関連グループとの業務効率化等の観点から，例えば認証局を利用したエクストラネット構築の動きが進んでいる．さらに,今後の ICT 社会における新たなコミュニティ手段として，サイバーソサイエティの実現に向けての検討も進められている．このような仮想的なネットワーク環境においては,さらなる利便性の観点，例えば，業務効率化の観点等から，個人が複数のネットワークに帰属できることが望まれる．一方,負の問題としては，内部からの不正アクセスが顕在化している．これらを背景に，本論文では，多重帰属 VPN サービスを提案するものである．本サービスは，1)複数の VPN 帰属（多重帰属），2)内部からの不正アクセス対処するための VPN 内 VPN 構築（多段帰属），を特徴とし，業務効率向上と不正アクセス対処を同時に実現するものである．さらに，経済的にかつ早期にサービスを具現化する観点から，既存の端末，NW 環境をそのまま利用可能なプラグ&プレイ型のサービスを実現するサーバ型アーキテクチャを提案する．

キーワード　多重帰属，VPN，イントラネット，エクストラネット，仮想組織

A Proposal of server type Multi-homing VPN service architecture

Shigeaki TANIMOTO†

†NTT Information Sharing Platform Laboratories, 3-9-11 Midori-Cho Musashino-Shi Tokyo 180-8585 Japan
E-mail:　†s.tanimoto@m.ieice.org

Abstract Recently, Intranet environment of the enterprise is becoming more convenient by development of NW security technology and widening of a wireless LAN. Consideration of the extranet environment in the enterprise is also developed from the point of view which is business efficiency with development of such intranet environment. Moreover it's considered for realization of a cyber society as a new community way. For example it's wished for improvement of further advantage convenience by such virtual network environment that an individual is able to belong to more than one network. On the other hand, hacking from the interior is clarifying as a negative problem. In this paper, Multi-homing VPN service is proposed newly from such background. Business efficiency improvement and illegal access handle are achieved at the same time by this service. And, the server type architecture is proposed to achieve a plug and play type service from a cost-saving point of view.

Keyword　Multi-homing,　VPN,　Intranet,　Extranet,　virtual organization

1. はじめに

企業内のイントラネットの進展に伴い，例えば関連グループとの業務の効率化や取引の円滑化のためにイントラネット構築に加え，認証局等を利用したセキュリティを確保したエクストラネット上に仮想組織を形成するサイバーソサイエティの実現に向けての検討が進んできている [1]-[3]．また，企業においては，IT 化の進展や 2007 年問題等の社会現象に伴い，業務の効率化や多様化の検討が進んできており，一人の社員が複数の業務を兼務する，例えば営業部に所属しつつ開発部に所属する等の業務形態が多く見られるようになってきている[4]-[5]．このような状況を IT 技術で支援するには，営業部の NW 環境に加え，開発部の NW 環境にも同時にアクセスできること，即ち，複数の NW 環境に帰属し，同時にアクセス可能な NW 環境が必要となる．一方，インターネットにおいては，コンピュータウィルス，不正アクセス等による被害が増加しており，セキュリティ対策はますます重要な課題となっている．イントラネットにおいても，普及する一方で，内部からの不正アクセスが増えている[6]-[12]．

本論文では，これらの背景の下，業務の効率化向上の観点から複数の VPN への帰属を可能とし，また，例えば，内部からの不正アクセスへの対処として VPN 内 VPN 構築を実現する，これらを同時に実現可能な多重帰属 VPN サービスを提案するものである．さらに，サービス提供の迅速性，経済的なサービス構築等の観点

から，既存の環境（ネットワーク，端末）下において，サーバを追加するだけでサービスを容易に実現させるためのアーキテクチャを併せて提案する．以降，2. で提案するサーバ型多重帰属 VPN サービスの位置づけと実現のための諸課題について述べ，3. ではこれらの課題を実現するための具体的な方式を提案し，4. でシステム構成，サービスアーキテクチャを詳細に示すとともに，サービス性評価により提案方式の有効性を明らかにし，5. でまとめと今後の予定について示す．

2. サーバ型多重帰属 VPN サービス

2.1. サービスの位置づけ

従来の多重帰属 VPN に関する報告のほとんどが，NW側に機能を設ける方式である．すなわち，VPN-GW にポリシー制御を設ける方式[1]-[3]，あるいは，プロバイダ側の VPN アクセスポイントで制御する方式[13]-[14]，レイヤ 2 認証におけるサイト多重帰属[15]，等である．これらは，図 1 (1)に概要を示すように，ネットワーク側に何らかの装置を設けることにより，多重帰属を実現しており，スケーラビリティ等の観点からは優位であるが，多重帰属というサービス性の観点，すなわち頻繁に帰属先を変更する（例えば頻繁に業務の変更等がある場合等を想定）等，ユーザ側の観点からは，必ずしも使い勝手の良いものでは無い．

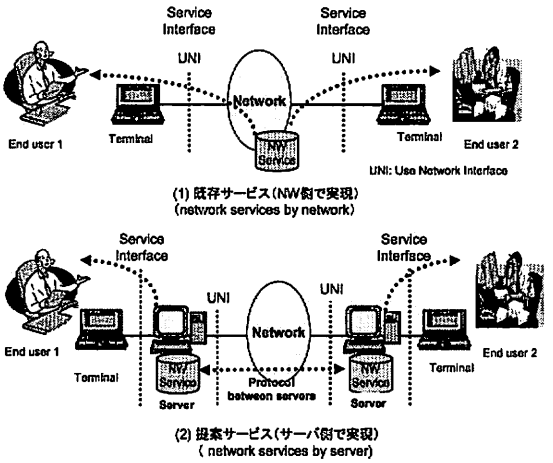


図 1　既存サービスとの比較

Figure 1 Comparison with existing service

本論文で提案するサーバ型多重帰属 VPN サービスでは，図 1 (2)に示すように，サービスをネットワーク側ではなくサーバ側で実現することにより，1)既存の端末，ネットワーク環境での新規ネットワークサービスの提供，2)サービスの変更が容易に可能，を特長としている．表 1 に，サービスの追加・削除の容易性の観点から比較した結果を示す．

表 1　既存方式との比較

Table 1 Comparison with existing method

方式		サービス追加の容易性	サービス脱着性	サービス適用範囲
既存方式	ネットワーク型	難：NW変更を伴う	難：計画性が必要	大：NW 全体
提案方式	サーバ型	易：NW, 端末等の変更不要	易	中：サブネット単位等

表 1 に示すように提案するサーバ型ＮＷサービスでは，既存の端末やネットワークに全く依存することなく，サーバを追加するだけで容易にネットワークサービスの提供を可能とする．さらに，サーバによる提供のため，サービスが不要になった時点でサーバを外すことにより，サービス自体の脱着が容易となる．これらにより，従来のネットワーク型サービスの場合，いわゆるレディメード型のサービス提供形態であったのに対し，サーバ型サービスは，ユーザ側でのカスタマイズ，オーダーメードが容易に実現できるサービス提供形態が可能となる．また，サービス適用範囲（スケーラビリティ）の観点でも，提案方式は，例えばサブネット単位にサーバを設置する等，ある程度まとまった単位でのサービス提供が可能である．以下に，提案するサーバ型多重帰属 VPN サービスの概要とそれを実現するための要件定義について示す．

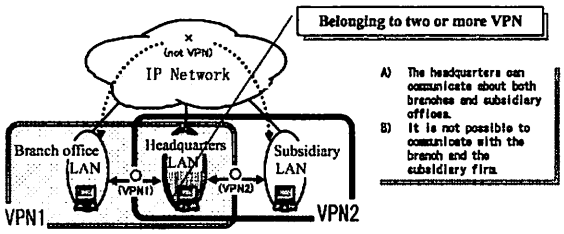
2.2. サーバ型多重帰属 VPN サービス

本論文で提案するサーバ型多重帰属 VPN サービスではインターネット等の IP ネットワークを利用して，複数の VPN に同時に帰属できるサービスである．VPN の包含関係により図 2 に示す 2 つの形態（多重型，多段型）を有する．本サービスの特徴は，

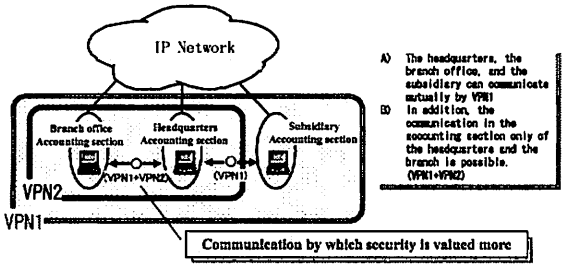
1) *LAN または端末を仮想的に複数の VPN に帰属させることを可能とする．複数の VPN に帰属する端末は，各 VPN 内の端末と相互通信が可能であるが，各 VPN の独立性やセキュリティを損なうことはない．*

2) *既存の NW 環境，端末には何ら変更を要せず，新規にサービスサーバを設置することによりサービス提供する．*

である．これらにより従来の物理的な LAN セグメントに制約されない論理的な VPN を構築し，かつ端末が同時に複数の VPN に帰属可能とすることにより，例えば各 VPN に接続されているリソース（DB Server 等）が容易に利用可能となる．



(1) 多重型 VPN (Service type of multi-homing VPN)



(2) 多段型 VPN (Service type of multi-nesting VPN)

図２ 多重帰属 VPN サービスの定義
Figure 2 Definition of multi-homing VPN service

2.3. サービス実現のための要件定義

2.2 で示すサーバ型多重帰属 VPN サービスを具現化するための要件定義を表２に示すとともに，これらの内容について詳細に記す．

表２ 多重帰属 VPN サービスにおける要件定義
Table 2 Problems for the Multi-homing VPN service achievement

	要件	内容	備考
1	複数VPNに帰属	・多重帰属VPN管理（論理グループ形成，多重帰属VPN構成管理）	要開発
2	既存NW環境，端末の利用が可能	・サーバ型アーキテクチャ	要開発
3	各 VPN の独立性，セキュリティ確保	・多重帰属 VPN 間セキュリティ ・FW 等とのインターワーキング	既存技術適用（コンピュータ・NW セキュリティ）

2.3.1. 多重帰属 VPN 管理

(1) 論理グループ形成

一般にインターネット上で IP サブネット単位に VPN を構成し多重帰属 VPN を形成しようとすると，多重帰属する端末は複数の IP サブネットのアドレスを保持する必要がある．従来の技術では，たとえば端末にネットワークインタフェースを複数装備しそれぞれの VPN に直接接続する物理的な接続が考えられる．しかし，この場合システム全体が高価となるばかりでなく，ネットワーク変更が容易でかつ自由なグルーピングができない．したがって，多重帰属 VPN 形成においては出来るだけ管理が容易となる論理的な VPN 構成（グルーピング）が要求される．

(2) 多重帰属 VPN 構成管理

インターネット上に VPN を形成する場合の次の課題としてセキュリティのための管理がある．一般に VPN を形成するメンバ間の通信を許可するには，双方の VPN に通信パス（IP サブネット間または端末間の発着信アドレス）毎の通信可否情報を，ネットワーク機器（ファイアウォール等）の通信テーブルに初期登録する必要がある．このため，VPN のメンバが多地点に散在すると初期登録のための管理稼動が大きくなる．また，VPN 内の端末増設等の VPN 構成変更に対して迅速に対応できない．さらに，これらの VPN に多重に帰属することから管理稼働はさらに増加する．したがって，多重帰属 VPN 管理においては通信テーブルの自動構成など管理稼動を出来る限り低減することが重要となる．

2.3.2. サーバ型アーキテクチャ

2.1 項に示したように，既存の方式が新規サービス実現時，ネットワークもしくは端末に何らかの変更が必要となるのに対し，提案するサーバ型ＮＷサービスは，既存のネットワーク環境や端末環境をそのままにして，図１（2）に示すように，サーバを介して各種ネットワークサービスを実現する．

2.3.3. 多重帰属 VPN 間セキュリティ

多重帰属を実現する際のもう一つの課題として多重帰属 VPN 間のセキュリティがある．図２に示すように端末が VPN1 と VPN2 に多重帰属する場合，VPN1 の他の端末が多重帰属端末を経由して VPN2 の端末に不正アクセスする可能性（踏み台攻撃）がある．踏み台攻撃は既存のコンピュータセキュリティとして捉えられ，基本的にはこれらの技術を適用すれば良い．例えば，多重帰属する端末がクライアントならばログインされる可能性がなく問題無い．端末がサーバの場合はこれまでに検討されている踏み台攻撃に対する対策[16]等の適用検討が今後必要となるが，基本的には既存技術とのインテグレーションで可能と思われる．

2.3.4. FW 等とのインターワーキング

一般にインターネットに接続された企業ネットワークはファイアウォールによって VPN を形成している．このような VPN を跨って新たな多重帰属グループを形成する場合，ファイアウォールを安全に超えるための技術を確立することが重要である．

3. サービス実現方式

ここでは,サーバ型多重帰属 VPN サービスを実現するために，2.3 の要件定義に基づき，特に新たな開発が必要となる,多重帰属 VPN 管理方式,サーバ型アーキテクチャについて,概説し，詳細については，4.のサービスアーキテクチャにおいて述べる.

3.1. 多重帰属 VPN 管理方式

3.1.1. 論理グループ形成技術

多重帰属のための論理的なグループ形成として，一般に，以下に示す案が考えられる.

案 1) グループアドレス（クラス D）の利用：既存のルータなどの中継機器にグループアドレスを識別させる必要があり現実的ではない.

案 2) サービスリソースを新たに導入：新たにグループを管理するためのグループ ID を用意しグループ内個別通信を可能とするもので，グループ ID を管理するサーバ，クライアントを設けることで既存の中継機器の使用を可能とする.

これらを比較した結果，既存のネットワークが利用可能である等の観点から案２のサービスリソースを新たに導入する案が適していることから,この案とする.案２におけるグループ内の通信は，サーバがそれぞれグループ ID を識別しグループに応じたセキュリティを確保した通信(暗号通信)及びプロトコルによって，各グループの独立性と閉域性を確保するものである.

3.1.2. 多重帰属 VPN 構成管理技術

インターネット VPN のように，インターネット内で VPN を形成する場合，暗号通信が必要となる．この場合，メンバ間の通信パス毎に暗号鍵を用意して通信が行われる．すなわち，複数のメンバと暗号通信する場合，セキュアルータ等の暗号装置は複数の暗号鍵を持ち，宛先に応じて暗号鍵を選択する必要が生じる.

このため，暗号装置内部に宛先アドレスと暗号鍵の対応テーブル（以下，通信鍵テーブルと呼ぶ）を静的に保持する方式（以下，静的管理方式と呼ぶ）と動的に保持する方式（以下，動的管理方式と呼ぶ）が考えられる．一般に，静的管理方式では，VPN 内の端末の増設や新規 VPN との接続など，ネットワークの構成変更に対して迅速に対応できない．また，通信鍵テーブルの初期登録や変更の人的稼働が大きいといった問題もあり，多重帰属 VPN サービスのように，多くのグループを対象とする場合，現実的な方式ではない．したがって，多重帰属 VPN サービスにおいて動的管理方式を用いる.

3.2. サーバ型アーキテクチャ

サーバ型ＮＷサービスを実現するためには，端末から見てサーバがあたかもネットワークであるかのように振舞うことで，ネットワークサービスを擬似することである．これにより，ユーザは，既存の環境を何ら変更することなく新たなネットワークサービスの使用が可能となる．このためには，サーバ間でサービス実現可能とするためのプロトコルの規定が必要である.

4. サービスアーキテクチャ

ここでは，サーバ型多重帰属 VPN サービスを具現化するためのアーキテクチャについて示す.

4.1. システム構成

図３にシステム構成を示す．同図に示すように，本システムは，VPN ID の管理を司る鍵管理サーバ（KMS: Key Management Server）と VPN を形成する暗号処理サーバ(EPS: Encryption Processing Server)からなる．鍵管理サーバ:KMS は VPN を形成するために必要な VPN ID すなわち VPN 単位の暗号鍵 ID（以降 VPN ID を暗号鍵 ID と記す)とそれに 1:1 に対応した暗号鍵を管理するものであり，暗号処理サーバ：EPS は，実際に暗号化／復号化するための暗号装置として位置づけられる.

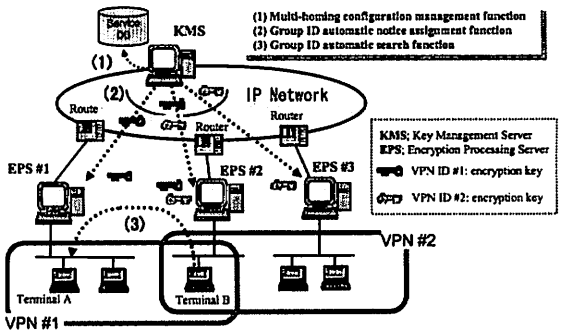


図 3 システム構成

Figure 3 System Configuration

4.2. 鍵管理サーバ:KMS

鍵管理サーバである KMS は，4.1 で示したように，各 VPN に対応した暗号鍵 ID とその暗号鍵の管理と暗号鍵を暗号処理サーバに配送する鍵配送機能を有している．以下に各機能に関して詳細に説明する.

4.2.1. 鍵管理機能

鍵管理サーバは VPN 毎に対応づけられた暗号鍵 ID 及びそれに 1:1 に対応した暗号鍵を生成･管理する(図３（1)）．具体的には，管理対象とする暗号処理サーバ（EPS #n）の情報（名称，鍵配送のための公開鍵，設置場所等）を編集・登録する.

4.2.2. 鍵配送機能

鍵配送機能は，鍵管理サーバから暗号処理サーバに対して暗号鍵 ID を配送する機能である（図３（2））．

同一の暗号鍵 ID が鍵管理サーバより配送された暗号処理サーバは同一の VPN に帰属することになる．すなわち，暗号鍵 ID を VPN の識別子として用いている．図３のシステム構成では，VPN #1 を識別する暗号鍵 ID1(VPN ID#1)が暗号処理サーバ#1（EPS #1）と#2（EPS #2）に，VPN #2 を識別する暗号鍵 ID2(VPN ID#2)が暗号処理サーバ#2（EPS #2）と#3（EPS #3）に初期登録され，端末 B が VPN #1 と VPN #2 に多重帰属している様子を示している．

4.3. 暗号処理サーバ:EPS

暗号処理サーバは，サーバ型 NW サービスを実現するためのプロトコルを有する．すなわち，暗号処理サーバ（EPS #n）間で，端末から出されたパケットを契機に暗号処理サーバ間で通信可能かどうか（同一 VPN かどうかの判定を行う）について，自動的に探索するプロトコル(鍵探索プロトコル)を具備している(3.1.2 で述べた動的管理方式）．以下に，鍵探索プロトコルについて詳細に示す．

鍵探索プロトコルは，暗号処理サーバ配下の端末から出されたパケットを契機に自動的に VPN 間通信を可能とするために対象となる暗号処理サーバ（同じ暗号鍵を有する EPS）を探索するためのプロトコルである．鍵探索プロトコルでは，サーバ型 NW サービスを実現するために，既存の端末がデフォルトで具備している ICMP ECHO/REPLY パケットを利用している．図４に鍵探索プロトコルにおけるシーケンスを，図５にプロトコルスタックを示す．

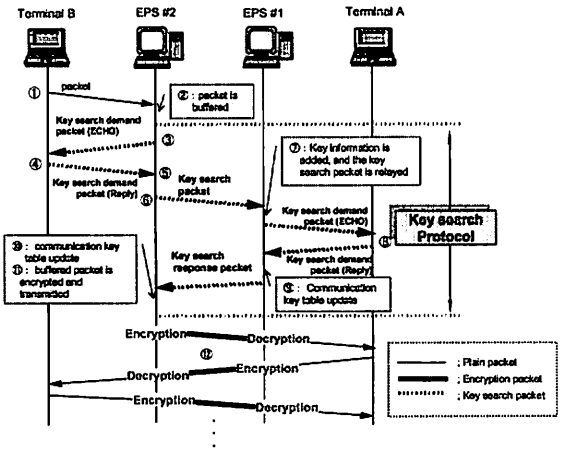


図４　鍵探索プロトコル

Figure 4 Key search protocol

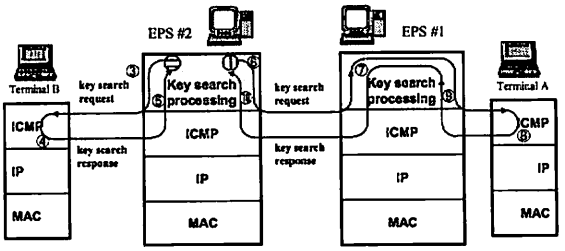


図５ プロトコルスタック

Figure 5 protocol stack

図４のシーケンスを用いて鍵探索プロトコルを詳細に説明する．なお,図中の番号（①～⑫）は処理の流れを示している．

（図４①）端末 B が端末 A 宛のパケットを送信する．

（図４②）暗号処理サーバ #2（EPS #2）は，自身で持つ通信鍵テーブルを検索し，登録が無い場合，端末 B からのパケットをバッファリングする．登録がある場合は，その登録内容に従い，パケットを暗号中継，平文中継，あるいは廃棄する．

（図４③）パケットの送信元端末 B 宛に鍵探索要求パケット（ICMP　ECHO 利用）を送信する．

（図４④）鍵探索要求パケットを受信した端末 B は，このパケットに対して応答（ICMP　ECHO に対して REPLY を返す）を送信する．

（図４⑤)端末 B からの鍵探索要求パケットの REPLY パケットを受信することで暗号処理サーバ #2（EPS #2）は，端末 B から１段目の暗号処理サーバになることを認識し，このパケットを終端する（中継しない）．

（図４⑥）次に暗号処理サーバ#2（EPS #2）は，パケットの送信先端末である端末 A 宛に鍵探索要求パケットを送信する．

（図４⑦）暗号処理サーバ #1（EPS #1）では，端末 A 宛の鍵探索要求パケットが ECHO パケットであるため，暗号処理サーバ #1（EPS #1）の鍵情報を追加して中継する．

（図４⑧）鍵探索要求パケットを受信した端末 A は，このパケットに対して応答を送信する．

（図４⑨）端末 A からの鍵探索パケット（REPLY パケット)を受信した暗号処理サーバ #1(EPS #1)は，このパケットが REPLY パケットであるため，通信鍵テーブルを更新後，中継する．

（図４⑩）暗号処理サーバ #1（EPS #1）により中継された端末 A からの鍵探索パケットを受信した暗号処理サーバ #2（EPS #2）は，このパケットが REPLY パケットであるため,端末 B-A 間の通信パス情報(IP アドレス，鍵 ID 等）を通信鍵テーブルに登録する．

（図４⑪）暗号処理サーバ #2（EPS #2）では，⑩で登録した端末 B-A 間の通信パス情報に従って，②でバッファリングしたパケットを暗号化して送信する．（図４⑫）以降，通信鍵テーブルに登録した通信パス情報に従い，端末 B-A 間の通信を暗号／復号する．

4.4. サービス性評価

2. において，仮想的なネットワークサービスではサービスの運用保守が重要であることを述べた．ここでは，主に運用保守面の観点から従来方式と提案方式との比較を行う．従来方式として，一般的に用いられているセキュアルータ（IPsec 利用）を評価対象とする [5]．表 3 に比較評価結果を示す．同表に示すように，特に企業内において，このような多重帰属 VPN サービスをタイムリーに実現するためには，管理稼働等のコスト削減，将来の拡張性，等の観点から提案方式が適しているといえる．

表３　比較評価結果

Table 3 Comparative evaluation result

	VPN 形成のための暗号鍵数	VPN 形成のための初期管理ﾃｰﾌﾞﾙ量	大規模化への対応（暗号鍵数，ﾃｰﾌﾞﾙ量，更新稼動）	評価
従来方式	1	1	・VPN を構成するﾒﾝﾊﾞｰに依存 ・分散設置されているため変更時の稼動が困難	×
提案方式	0.8	0.2	・VPN 数にのみ依存 ・鍵管理ｻｰﾊﾞによる集中管理のため変更は容易	◎

（注）表中の数字は，従来方式を１として正規化している

5. おわりに

本論文では，主に業務効率化等の観点，タイムリーなサービス提供等の観点より，複数の VPN に多重帰属可能なサーバ型多重帰属 VPN サービスアーキテクチャを提案した．

具体的には，まずサービスの要件定義を明らかにし，この要件定義を下に，サービス具現化のための方式として，多重 VPN 管理方式，サーバ型アーキテクチャを提案した．特に，本提案の核であるサーバ間のプロトコルである鍵探索プロトコルに関しては，シーケンスを用いて動的に管理できることを明らかにした．また，サーバ型アーキテクチャに関しては，システム構成において，鍵管理サーバと暗号処理サーバについて説明し，これらのサーバ間のプロトコルにより，従来の端末やネットワークに特に手を加えることなく，本提案のサーバ型多重帰属 VPN サービスが実現できることを示した．最後に，サービス運用面の観点から，従来方式との比較により提案方式の有効性についての検証を行った．

今後は，既存のコンピュータ及びネットワークセキュリティ機能とのインテグレーション，鍵配布，性能条件など，定量的な評価を中心に検討を進めていく予定である．

文　献

[1] 木村旭他，“ポリシーに基づく多重帰属の制御が可能な VPN アーキテクチャの提案”，信学技報，NS2003-362，IN2003-317(2004-03)

[2] 原義博他，“利用者が複数の VPN に多重帰属できる階層化 VPN アーキテクチャ”，信学技報，NS2003-107，IN2003-73，CS2003-82(2003-09)

[3] 原義博他，“利用者が複数の VPN に多重帰属できる VPN アーキテクチャの提案”，信学技報，IN2003-50，(2003-07)

[4] 谷本茂明他，“多重帰属グループサービスアーキテクチャの検討”，信学技報，OIS2006-47(2006-11)

[5] 谷本茂明他，“多重帰属 VPN サービスの提案”，信学技報，IN97-114，Oct. 1997

[6] 寺田真敏他，“企業内不正アクセス対策情報サービスシステムの構築”，信学技報，ISEC2000-49(2000-07)

[7] 福士賢二他，“不正アクセス被害解析支援システムの試作”，信学技報，ISEC2002-16(2002-07)

[8] 北野博之，“企業における情報セキュリティと認証制度”，情処研報，2003-IS-86，2003

[9] 大谷尚通他，“依存モデルを用いたセキュリティ・アセスメントのための被害予測システムの検討”，情処研報，2002-CSEC-16，2002-DPS-106，2002

[10] 宮地利雄，”ネットワーク・セキュリティの現状と課題”，電学論 C，124 巻 8 号，2004 年

[11] 渡邊晃他，“イントラネット閉域通信グループの物理的位置透過性を可能にする動的処理プロトコルの提案”，信学会論文誌，D-I，vol. J84-D-I，No. 3，2001

[12] http://www.soumu.go.jp/joho_tsusin/policyreports/japanese/group/internet/net-1.html

[13] 岡山聖彦他，“階層化 VPN のためのＬＤＡＰサーバを用いた経路制御手法”，情処研報，2003-DSM-29，2003

[14] 福井健太他，“階層化 VPN における効率的なアクセスポリシ管理手法”，情処研報，2003-DSM-30，2003

[15] 石川雄一他，“レイヤ２認証におけるサイト多重帰属方式”，信学技報，NS2004-12 (2004-04)

[16] ASAKA M, et al., “Network Software. Public Information Server for Tracing Intruders in the Internet”, IEICE Trans Commun (Inst Electron Inf Commun Eng), VOL. E84 - B, NO. 12, 2001