多重帰属 VPN サービスにおけるセキュリティアーキテクチャ

谷本 茂明† 村山 純一‡ 関 良 明‡

†千葉工業大学
275-0016 千葉県習志野市津田沼 2-17-1
‡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
shigeaki.tanimoto@it-chiba.ac.jp

あらまし 近年，企業におけるイントラネット環境は，広域無線LANやブロードバンドサービスの進展等に伴いユビキタス環境での利用が可能になってきている．我々は，これまでに企業における業務の多様化に対応する観点から複数のVPNに帰属可能とする多重帰属VPNサービスを提案している．本論文では，ユビキタス環境において多重帰属VPNサービスを安心・安全に構築するためのセキュリティアーキテクチャについて述べる．

A Study of Security Architecture in Multi-homing VPN Service

Shigeaki Tanimoto† Junichi Murayama‡ Yoshiaki Seki‡

†Chiba Institute of Technology
2-17-1 Tsudanuma Narashino-Shi Chiba, 275-0016 Japan
shigeaki.tanimoto@it-chiba.ac.jp

‡NTT Information Sharing Platform Laboratories
3-9-11 Midori-cho Musashino-Shi Tokyo, 180-8585 Japan
murayama.junichi@lab.ntt.co.jp seki.yoshiaki@lab.ntt.co.jp

Abstract In recent years, as for the intranet environment in a company, use in ubiquitous environment is being attained with progress of broader-based wireless LAN and broadband service etc. We have proposed the multi-homing VPN service whose attribution in two or more VPN is enabled from a viewpoint corresponding to diversification of the business in a company until now. This paper describes the security architecture for building a multi-homing VPN service secure and safety in ubiquitous environment.

1 はじめに

ユビキタス環境の進展に伴い，イントラネット環境からエクストラネット，さらには仮想組織、いわゆるサイバーソサイエティ実現に向けての検討が進んできている [1]-[3]．企業においては，このようなユビキタス環境や ICT 化の進展，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おり，例えば一人の社員が複数の業務を兼務する，営業部に所属しつつ開発部に所属する等の業務形態が見られるようになってきている[4]-[5]．このような状況を ICT 技術で支援するには，社員が所属する営業部のネットワーク環境（以降，NW 環境と略す）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, 例えば内部からの不正アクセス等が顕在化している[7]-[12].

我々はこれまでに, 利便性確保の観点から複数 VPN への帰属, セキュリティ確保の観点から内部も含めた不正アクセスに対処可能となる VPN 構築, これら利便性とセキュリティを同時に実現可能とする多重帰属 VPN サービスを提案している[4]-[5]. 本論文では, 今後の進展が見込まれるユビキタス環境下においても, これら利便性確保とセキュリティ確保の両者を同時に実現可能とする多重帰属 VPN サービスにおけるセキュリティアーキテクチャについて述べる.

以降, 2. で多重帰属 VPN サービスについて, その概要, 実現方式について述べ, 3. では, そのシステム構成, セキュリティアーキテクチャを示す. 4.で今後の課題とまとめを述べる.

2 多重帰属 VPN サービス

2.1 サービス概要

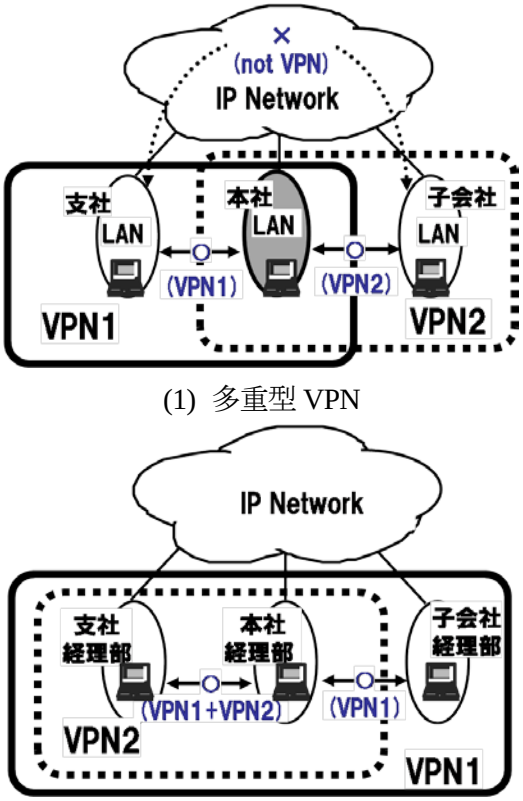
多重帰属 VPN サービスは, インターネット等の IP ネットワークを利用して, 複数の VPN に同時に帰属できるサービスである. 本サービスの特徴を以下に示す.

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
2)既存の NW 環境, 端末に何ら変更を要せず, サーバ設置によりサービス提供可能とする

多重帰属 VPN サービスでは, VPN の包含関係により図1に示す2つの形態(多重型, 多段型)を有する. これらにより, 例えばいろいろな VPN に接続されているリソース(DB Server 等)の共有が容易に利用可能となる(図 1(1):多重型), 内部からの不正アクセス対処がより強化できる(図 1(2):多段型).

2.2 要件定義

多重帰属 VPN サービスを実現するために必要となる主な要件・内容を表1に示す.



(1) 多重型 VPN

(2) 多段型 VPN

図 1 多重帰属 VPN サービス
Figure 1 Multi-homing VPN service

表1 多重帰属 VPN サービスにおける要件定義
Table 1 Requirements for the Multi-homing VPN Service

要件	内容	観点
複数 VPN に帰属可能	・多重帰属 VPN 管理	セキュリティ確保
既存 NW 環境及び端末利用が可能	・サーバ型アーキテクチャ	利便性確保

2.2.1 複数 VPN に帰属可能

表 1 における「複数 VPN に帰属可能」とするためには, 多重帰属 VPN 管理機能として, 以下に示す論理グループ形成, 多重帰属 VPN 構成管理が必要となる.

(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 を形成する場合,

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．従来技術では，端末にネットワークインタフェースを複数有し，それぞれの VPN に直接接続する物理的な構成等が考えられるが，システム全体が高価となるばかりでなく，システムの追加・削除・更新等の NW 運用管理が煩雑となる．従って，多重帰属 VPN サービスを実現するためには，出来るだけ管理が容易となる論理的な VPN 構成が必要である．

(2) 多重帰属 VPN 構成管理

VPN メンバ間の通信を行う場合，双方に通信パス(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．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ことになる．従って，多重帰属 VPN 構成管理では，通信用の暗号鍵管理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必要である．

2.2.2 既存 NW 環境及び端末利用が可能

「既存 NW 環境及び端末利用が可能」の要件に関しては，従来の NW サービスでは，新規にサービスを実現する場合，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．これに対し，多重帰属 VPN サービスでは，イントラネット環境への適用を想定しており，経済的な NW サービスの提供が望まれる．従って，既存の NW 環境や端末環境をそのままにして，提供が可能なサーバ型アーキテクチャ[6]が必要である．

2.3 サービス実現方式

ここでは，**2.2** の要件定義を基にした多重帰属 VPN サービスの実現方式について示す．

2.3.1 多重帰属 VPN 管理方式

(1) 論理グループ形成方式

論理的な VPN 形成方式として，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：新たにグループ管理用のグループ ID を用意しグループ内個別通信を可能とする．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等の使用を可能とする．

これらを比較した場合，既存の NW 環境の利用が可能である等の利点より，また，イントラネットのような企業向け NW サービスにおいては，経済性の優先度が高いこと等から，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．

(2) 多重帰属 VPN 構成管理方式

インターネット上で VPN を形成する場合，暗号通信が必要である．この場合，メンバ間の通信パス毎に暗号鍵を事前に用意しておく必要がある．即ち，複数のメンバと暗号通信する場合，セキュアルータ等の NW 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．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)が必要となる．この通信鍵テーブルには，静的に保持する方式(静的管理方式)と動的に保持する方式(動的管理方式)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 との接続などの構成変更に迅速に対応できない．これに対し，動的管理方式では，構成変更が動的に可能であるため，多くの VPN を対象とする多重帰属 VPN サービスに適している．従って，多重帰属 VPN サービスでは，動的管理方式を用いる．

2.3.2 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，NW サービスを擬似することが必要となる[6]．即ち，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となる．

3. セキュリティアーキテクチャ

3.1 システム構成

多重帰属 VPN サービスのシステム構成は，図 2 に示すように，多重帰属 VPN 管理サーバ（MMS: Multi-homing VPN Management Server），多重帰属 VPN 実行サーバ（MES: Multi-homing VPN Execution Server）からなる．

(1) 多重帰属 VPN 管理サーバ：MMS

VPN を形成するために必要な VPN ID（VPN 単位の暗号鍵に対応する ID）とそれに 1:1 に対応した暗号鍵を管理する．

(2) 多重帰属 VPN 実行サーバ：MES

多重帰属 VPN サービスでは，一つの VPN を 1 個の暗号鍵で実現する．即ち，VPN に属するメンバ間で同じ暗号鍵を共有し，メンバ間の通信をこの暗号鍵で暗号化・復号化する．この VPN 単位の暗号鍵を複数管理し実行することにより，多重帰属 VPN サービスを実現する．

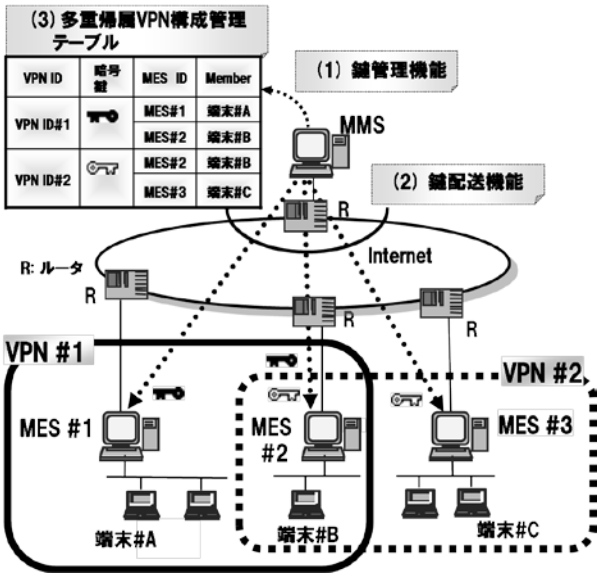


図 2 システム構成

Figure 2 System Configuration

図 2 は，VPN1 を識別する VPN ID#1 が多重帰属 VPN 実行サーバ MES#1と MES#2に，VPN2 を識別する VPN ID#2 が MES#2 と MES#3 に初期登録され，その結果，MES#2 配下にある端末 B（TE#B）が VPN1 と VPN2 に多重帰属している様子を示している．

次に，これらのサーバが有する主な機能について説明する．多重帰属 VPN 管理サーバ MMS の有する主な機能として NW 運用管理機能である多重帰属 VPN 管理機能を，多重帰属 VPN 実行サーバ MES の有する機能では，VPN を構成する端末間の暗号化を自動的に行う鍵探索プロトコルについて説明する．

3.2 多重帰属 VPN 管理機能

3.2.1 鍵管理機能

多重帰属 VPN 管理サーバ（MMS）は図 2(3)に示すように，VPN 毎に対応付けられた VPN ID 及びそれに 1:1 に対応した暗号鍵を生成・管理する．即ち，MMS が管理対象とする多重帰属 VPN 実行サーバ（MES #n）の構成情報（名称，鍵配送のための公開鍵，IP アドレス等）を作成・登録する．多重帰属 VPN サービスでは，同一の VPN ID が登録された MES #n 及び MES #n 配下の端末は同一の VPN に帰属する．具体的には，図 2 (3)に示す MMS の構成情報テーブルにより， VPN #1 は，VPN ID が VPNID1であり，構成メンバが，多重帰属 VPN 実行サーバ MES #1 及びその配下の端末 A と MES #2 及びその配下の端末 B となる．同様に，VPN #2 では，構成メンバは，多重帰属 VPN 実行サーバ MES #2，端末 B と MES #3，端末 C である．その結果，MES #2 配下にある端末 B は，VPN #1 と VPN #2 に多重帰属している．

3.2.2 鍵配送機能

鍵配送機能は，鍵管理サーバから各暗号装置（MES #n）に対して VPN ID 及びこの ID に対応する暗号鍵を MES #n に対して公開鍵暗号を用いてセキュアに配送する（図 2 (2)）．3.2.1 で示したように，この VPN ID を VPN の識別子として用いている．ここで,暗号鍵を直接使用せず暗号鍵 ID を用いているのは，3.3 で説明する VPN 形成のための鍵探索プロトコルを平文（ICMP ECHO/REPLY を利用）にて送受信するために，暗号鍵に 1:1 に対応した VPN ID を用いている．

実際の VPN を形成するための暗号鍵（鍵配送のための公開鍵，VPN 用の暗号鍵の 2 種類

必要)は，初期設定時や更新時に，MMS において生成する．これらの暗号鍵の配布に関しては，図 3 に示すように MMS から各 MES に対し，公開鍵はオフラインで事前に各 MES に配送しておき(同図(1))， VPN 用の暗号鍵はその公開鍵を用いてオンラインで配送する(同図(2))．

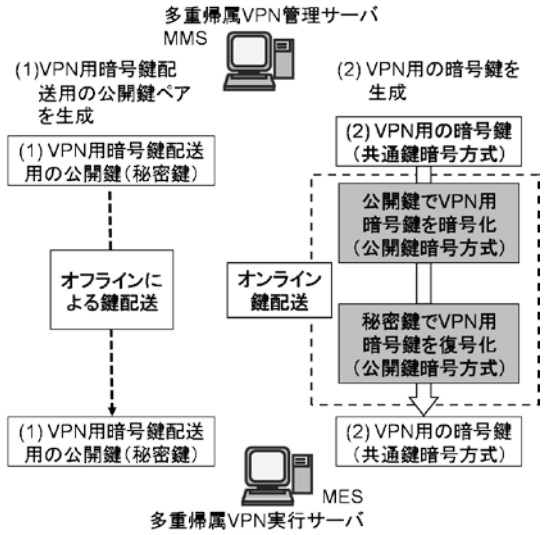


図 3 鍵配送機能

Figure 3 Key Distribution Function

3.3 鍵探索プロトコル

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 MES)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，サーバ型アーキテクチャを実現するために，既存の端末が具備している ICMP ECHO/REPLY パケットを利用するのが特徴である．図 4 により鍵探索プロトコルを説明する．

3.3.1 送信元探索

① 端末 B が端末 A 宛のパケットを送信する．

② MES #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．

③ 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．

④ 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鍵探索応答パケット(ICMP REPLY を利用)を送信する．

⑤ 端末Bからの鍵探索応答パケットを受信することで MES #2 は，端末 B から 1 段目の暗号処理サーバであることを認識し，このパケットを終端する(中継しない)．

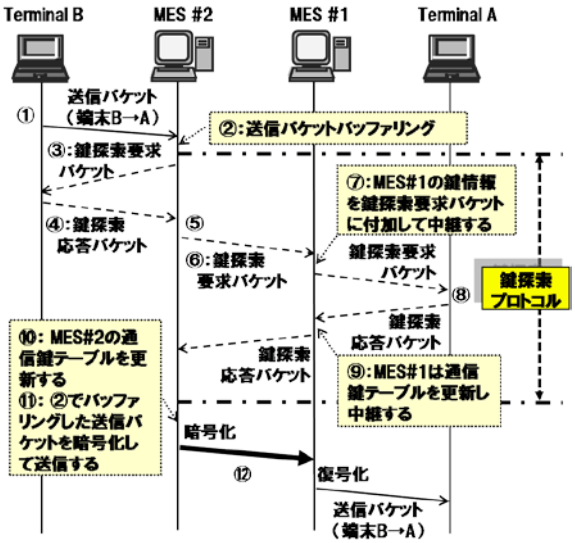


図 4 鍵探索プロトコル

Figure 4 Key Search Protocol

3.3.2 宛先探索

⑥ 次に MES #2 は，端末Bの宛先である端末A宛に鍵探索要求パケットを送信する．

⑦ MES #1 は，端末 A 宛の鍵探索要求パケットを受信すると，MES #1 の有する鍵情報を鍵探索要求パケットに追加して中継する．

⑧ 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鍵探索応答パケット(ICMP REPLY)を送信する．

⑨ 鍵探索応答パケットを受信した MES #1 は，通信鍵テーブルを更新した後，中継する，この更新の意味は，通信パス情報(IP アドレス，VPN ID)を設定することである．

⑩ MES #1 により中継された端末 A からの鍵探索応答パケットを受信した MES #2 は，端末 B-A 間の通信パス情報を通信鍵テーブルに登録する．

⑪ MES #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.

⑫ 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 間の通信を行う.

以上のように鍵探索プロトコルにより, 通信鍵テーブルは自動的に作成され, 宛先に応じた暗号鍵が選択可能となるとともに,複数のVPN構成が容易に可能となる. 通信鍵テーブルに登録した情報は一定時間アクセスがなければエージングし, 動的に情報を保持することにより構成変更等に柔軟に対応することが出来る.

4. おわりに

本論文では, ユビキタス環境において安心・安全に多重帰属 VPN サービスを実現するためのセキュリティアーキテクチャについて述べた. 具体的には, 利便性確保とセキュリティ確保の両者を同時に実現する点を特徴とする多重帰属VPNサービスにおける要件定義を明らかにし, サービス具現化のための方式として多重 VPN 管理方式について述べた. 次に, この方式を基にしたセキュリティアーキテクチャについて, 特に具体的なシーケンスを用いて明らかにした.

今後の課題としては, ユビキタス環境の一層の進展に対し, より利便性及びセキュアに対応可能とするためにPKIとの連携を行う予定である. 例えば, 鍵配送機能では, 多重帰属 VPN 実行サーバの公開鍵は多重帰属 VPN 管理サーバが生成し, オフラインで各多重帰属VPN実行サーバに配布しているが, これをPKIと連携させることによりオンライン化が可能となりセキュアでかつ利便性の向上がさらに見込まれる. 今後, 具体的な方式に関して詳細に検討を進めていく予定である.

参考文献

[1] 本田治他, “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と実装”, 情処論文誌, Vol.47, No.7, July 2006

[2] 中村嘉隆他, “安全な多重帰属制御を実現する VPN 分散管理プロトコルの提案”, 情処論文誌, Vol.48, No.2, Feb. 2007

[3] 阪本裕介他, “コンタクト ID 変更に対応したユーザ主導型コミュニケーション手段選択方式の提案と評価”, 情処研究報告, 2009-GN-71

[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] 谷本茂明他, “サーバ型多重帰属VPNサービスアーキテクチャ”, 信学技報, OIS2007-24, Jul. 2007

[7] 村山純一, [招待論文]高度 VPN 通信技術の動向,信学技報, IN2008-48, Sep. 2008

[8] 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)

[9] 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

[10] 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

[11] 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

[12] 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

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

[14] 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

[15] 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

[16] 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)

[17] 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