動的な多重帰属制御を実現するポリシーに基づいた VPN 分散管理手法の提案

木谷 友哉 †, 中村 嘉隆 ††, 木村 旭 ††, 山口 弘純 ††, 中田 明夫 ††, 東野 輝夫 ††

† 奈良先端科学技術大学院大学 情報科学研究科, †† 大阪大学 大学院情報科学研究科

Policy-based Dynamic Multiple Association Control Method for VPNs

Tomoya Kitani†, Yoshitaka Nakamura††, Akira Kimura††,
Hirozumi Yamaguchi††, Akio Nakata††, and Teruo Higashino††

†Graduate School of Information Science, Nara Institute of Science and Technology,
††Graduate School of Information Science and Technology, Osaka University

1 はじめに

離れた地点間の安全な通信を実現するための手段として，専用線の代わりに公衆回線を利用した VPN（Virtual Private Network）が普及してきている．公衆網を使う VPN では専用線を使った通信と比較して，コストが小さいというメリットがある．また，公衆網に仮想的なリンクを張るため，一対多の接続も容易に実現できる．そのため，会社などの組織において，地理的に離れた部署間で安全に通信を行ったり，外出先から安全に組織内にアクセスしたり，特定のビジネスパートナーに対して安全に情報を提供したりすることを安価に実現することが可能となった．さらに，現在では，サービスの多様化から，サイト（VPN を構成する最小単位）が複数の VPN に同時に帰属（多重帰属）したいという要求が起こっている．

一般的に VPN で接続されるサイト間には，同じ組織に属すことや，ある特定の規則に従ったコミュニティのメンバーであるなどの関係があり，VPN へ帰属するためにはその VPN が設定する帰属受理に関する条件（ポリシー）を充足する必要がある．ポリシーとしては，使用する暗号プロトコルや（登録済みの）特定のサイトであることの制限などが考えられる．そのため，あるサイトが複数の VPN に多重帰属するためには，それらの VPN が持つポリシーを全て満たす必要がある．従来の VPN を構築するプロトコルでも，帰属要求の受理に関する設定をあらかじめ静的に行なっておくことや，帰属要求に対して手動で対応することで多重帰属の制御を実現することは可能である．しかし，前者は全ての可能性をあらかじめ設定しておく必要があり，動的な帰属要求に対応することは難しい．また，後者は応答速度や規模の面で非現実的である．これに対し，文献 [1] では，帰属要求に対するポリシーの判定を自動で効率的に行なうポリシーベースの制御法について提案されている．

上述した従来の多重帰属制御では，帰属要求を出すサイトが所属している VPN と帰属要求を受けた VPN のポリシーを元に要求を受理するか否かを判定する．しかし，複数の VPN に同時に帰属するサイトがある場合，そのサイトをゲートウェイとすることで異なる VPN 間が間接的に通信可能となるため，離れた VPN 間で情報漏洩が起こる可能性がある．例えば，営利的に競合関係にある企業同士ではそのような情報漏洩の可能性を排除するため間接的にでも VPN の接続を拒否すると考えられる．そのためには，従来のような帰属要求の送信元・送信先の二つの VPN のポリシーのみをもとにした帰属制御ではなく，それら VPN が持つ現在の間接的な接続関係も考慮に入れて，帰属の可否を決定する必要がある．

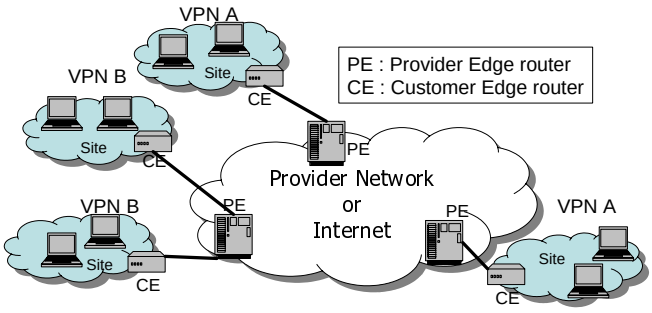

図 1: Typical network structure of VPN

そこで本稿では，既存の VPN アーキテクチャ上で，各 VPN の接続に関する情報と，ポリシーを効率的に収集し，それらの情報に応じて帰属の可否を判定することで，動的に多重帰属の制御を行なう VPN 帰属制御プロトコルを提案する．提案手法で対象とする VPN のアーキテクチャは，サービスプロバイダが提供する PPVPN (Provider Provisioned VPN) を想定する．PPVPN は，サービスプロバイダが提供する IP ネットワークにおいて，サイト側に用意されるカスタマエッジ (CE) ルータと，プロバイダのサービスネットワークに接続するプロバイダエッジ (PE) ルータから構成され，VPN の通信は既存のプロトコルを用いるものとする．各 VPN が持つポリシーとして，従来の帰属制御に使われていたような (a)“ある VPN に帰属する

サイト数は帯域確保のため一定数以下に制限する”，“ある特定の暗号化を利用する” といった直接帰属する VPN において遵守すべきポリシーの他に，(b)“ビジネスとして競合関係にある会社に属するサイトと間接的な接続関係にあるサイトの帰属を排除する” といった特定のサイト間の間接的な **接続関係** についてのポリシーを定義できるとする．これらのポリシーは，特定の VPN の接続関係，特定のサイトの帰属関係を元にして論理式で表現する．

VPN の規模が大きくなった場合，接続関係にある全ての VPN の間のポリシーを効率的に収集し，判定しなければ，収集時間や帯域，制御情報を保持するための記憶領域が非常に大きくなり，スケーラビリティが得られない．そこで，全 VPN から集めるポリシーを VPN の接続関係のみに関するものにのみ限定し，各 VPN が持つ VPN 同士の接続状態を PE に保持させ，間接的に接続している VPN の集合ごとに該当する VPN の情報を持つ PE のみからなる情報収集木を構築する．これを用いて各 PE の分散処理で情報を収集することで，制御にスケーラビリティを持たせる．

2 VPN の多重帰属

2.1 多重帰属の定義

本稿では VPN V にサイト S が含まれている場合，サイト S は VPN V に帰属すると定義する．また，あるサイトが複数の VPN に同時に帰属することを **多重帰属する** と定義する．

図 2 において，サイト S_1 は VPN A と VPN B に，サイト S_2 は VPN B と VPN C に，サイト S_3 は VPN A，VPN B，および VPN C に多重帰属しているという．このとき，サイト S_1 は VPN A，VPN B に帰属しているサイトと，サイト S_2 は VPN B，VPN C に帰属しているサイトと，サイト S_3 は VPN A，VPN B，VPN C に帰属しているサイトと通信可能である．

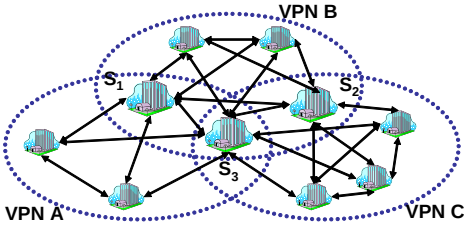

図 2: 多重帰属の例

2.2 従来の VPN での帰属制御

従来の VPN では，各組織に VPN GW (VPN Gateway) ルータが設置されており，サイトはそのルータに帰属要求を出し，GW は登録されたサイトかどうか，あらかじめ設定されたポリシーに合っているかどうかを判定した後，帰属の受理または棄却を行う．そのため，VPN の管理者の間で通信プロトコルの選定やアクセス制限などの事前調整を行い，ルータの設定を変更することで多重帰属を実現することができる [1]．しかし，このアプローチはあらかじめ各サイトが多重帰属する場合を想定して静的な設定を行っておくか，帰属要求に対して手動で設定を変更することで実現されており，その帰属制御は非効率的である．

一方，サイト内で VLAN などによるグルーピングを行い，各ホストがそれぞれで VPN ごとに認証を受けることで VPN への帰属が可能である MAVPN アーキテクチャ [2] が提案されている．このアーキテクチャでは，グループごとにアクセス制御を行うことで，従来の VPN に比べ効率のよい多重帰属を実現している．また，ポリシーベースの VPN アーキテクチャ [3, 4, 5] では，サイトの状況に応じてルーティングテーブルを構成する，というようなポリシーを設定できるので，ポリシーの設定次第で多重帰属の動的な制御も可能である．

2.3 多重帰属の問題点

前述した VPN アーキテクチャでは，多重帰属自体の実現は可能であるが，次のような帰属の制御問題は想定されていない．多重帰属において問題となるのは，次のような場合である．例えば，A，B，C の 3 つの組織があり，それぞれが独自の VPN を構成しているとする．A と B，B と C はそれぞれ友好関係にあるが，A と C が競合関係にあるとする．今，A が構成する VPN と B が構成する VPN が通信可能な状態にある (A と B の両 VPN に多重帰属しているサイトが存在する) とする．このとき，C のサイトが B に対して帰属要求を発生させた場合，A は C への情報流出の可能性がある以上，友好関係にある B の帰属も認めたくないという立場をとることも考えられる．つまり，ここで A のポリシとして，B が自身（A）と通信可能な状態にあるときには B において C のサイトの帰属は認めないが，それ以外の状態では認める，といったものが考えられる．

また，このような形の情報流出は，中間 VPN のホストに悪意があって中継されてしまう場合だけではなく，スパイウェアなどによって，同時に帰属しているサイトに無意識のうちに中継される可能性があるため，十分な脅威となる．

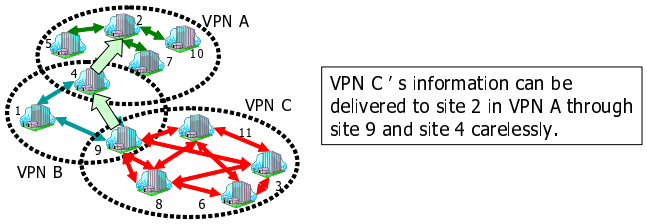

図 3: 多重帰属下における情報流出の危険性

文献 [3, 4] では，ポリシの設定次第で自身の状態に応じた帰属制御が可能であるが，他のサイトの状態も考慮に入れたポリシを設定することは想定されていないため，このような帰属制御の実現は困難である．また，PPVPN において，ルーティングや VPN 通信の設定はすべてプロバイダが行うため，ユーザが状況に応じて VPN を変化させることは難しい．

3 提案手法

3.1 対象とするアーキテクチャ

提案手法は，プロバイダの用意するプロバイダエッジ（PE）ルータとサイト側で用意するカスタマーエッジ（CE）ルータで構成される一般的な PPVPN アーキテクチャ上での制御を対象とする（図 4）．CE はサイトの VPN への帰属要求や離脱要求を PE に送信したり，自身の規定するポリシーを管理するための機能を持つ．CE は一つの PE に所属し，PE を介して他の CE と通信を行う．PE はサイトの要求に基づいて通信設定を変更したり，各 VPN が規定するポリシを管理するための機能と，PE 間でポリシなどの情報を交換する機能を持つ．この PE でデータのフィルタリングを行なうことで，複数の VPN のデータを分けて配送することができる．また，PE には所属している CE の VPN 情報や，PE 間のルーティングテーブルを保持するためのメモリ領域が確保されているものとする．

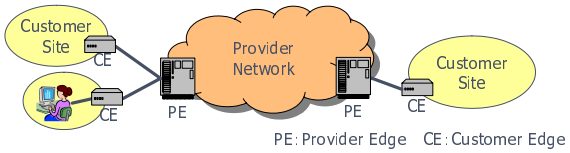

図 4: アーキテクチャの概観

3.2 提案手法の概要

提案手法では，多重帰属による間接接続の制御を問題とするため，判定するポリシーとしてサイト間の不可達条件のみを考慮する．不可達条件であるポリシーはネットワークにおけるサイトの存在情報を元に判定する．したがって，ネットワーク全体のサイト情報を収集する必要がある．

この情報をすべての CE を辿って収集することは非効率的であり，また，すべての CE を辿ったという保証ができないため，該当サイトが存在しないことを必ず保証することはできない．また，CE はカスタマー側に設置するため，そのカスタマーに都合のよいように情報を返さない設定がなされる可能性もある．しかし，PPVPN では各 CE は必ず PE を介して通信を行い，各サイトの VPN への帰属情報を PE で管理することが可能である．そこで，各サイト情報を持っている PE を辿ることで，これらの情報を収集することを考える．このとき，探索が必要な PE は，調べたいサイトが帰属している VPN が多重帰属サイトを介して間接的に接続している VPN の集合（VPN 群）に所属している PE のみでよい．一つの PE には一つ以上の CE が所属しているため，サイト数，すなわち CE 数が n のとき，辿る PE 数も高々 n である．このとき，それらの PE 間に木構造の情報収集用ネットワークを張りサイト情報を収集することで，収集のコストを $O(n)$ から $O(\log n)$ に抑えることができる．

PE の保持する情報　以下，サイトが複数の VPN に多重帰属することで間接的に接続する VPN の集合を VPN 群と呼ぶことにする．PE は各サイト（CE）がどの VPN および VPN 群に帰属しているかの情報を保持する必要がある．これらは，代表ノード（ここでは，最初に参加したノード）の ID とその VPN（VPN 群）が誕生した時間のタイムスタンプから生成する．ここで，ノードとは VPN では帰属している各 CE となり，VPN 群では所属している各 PE となる．PE は所属している各 CE についての 帰属 VPN，所属 VPN 群情報と，各 VPN 群についてのルーティング情報を持つ．

表 1 は，ある PE（PEID=1）が保持するテーブルの例である．この PE には CEID が 1, 2, 3 である CE を持つサイトが所属しており，それぞれのサイトは異なる VPN に属している．また，CEID=1 のサイトと CEID=2 のサイトはそれぞれが属す VPN のあるサイトが多重帰属していることによって間接的に接続関係にあるため，同じ VPN 群ラベルを持つことになる．下側の表は，VPN 群の情報収集を行うための木構造ネットワークの隣接 PEID である．

表 1: PE(PEID=1) の保持する情報

CEID	VPN ラベル	VPN 群ラベル
1	1200605012302	1200605012302
2	2200605011202	1200605012302
3	3200604282302	3200604282302
...	...	...

VPN 群	隣接 PEID(1)	隣接 PEID(2)
1200605012302	2	3
3200604282302	10	7
...	...	...

ポリシー　ポリシーとなる不可達サイト条件は各サイトがそれぞれ規定する．同一 VPN 内での各サイトのポリシーの論理和がその VPN のポリシーとなり，VPN 群内の各 VPN のポリシーの論理和が VPN 群のポリシーとなる．

3.3 PE からなる情報収集木

情報を収集するための情報収集木（以下，PE-Tree）を構築する．この PE-Tree は，同じ VPN 群に所属する PE から構成され，直径が最小となるようなスパニング木として構築される．ここで，情報収集木は木上の各 PE 間の距離が最小，すなわち木の直径が最小となるように構築する．ここでは，早く参加したものから中心に集まるように構築する．

PE-Tree の例を図 5 に示す．

3.4 VPN の参加手順

まず，参加を開始するサイトは，参加する VPN のあるサイトに参加要求メッセージを送出する．これと同時に，自らの所属する VPN 群の PE-Tree によって，VPN 群のサイト情報を収集する．収集から判定までの間にサイト情報に変化のないよう，情報の収集時に PE に対して所属サイト情報の変更を禁じる．すなわち新たな要求を受け付けないようにロックをかける．

参加要求メッセージを受けとったサイトは，同様に自らの所属する VPN 群の PE-Tree によってサイト情報を収集し，各 PE をロックする．

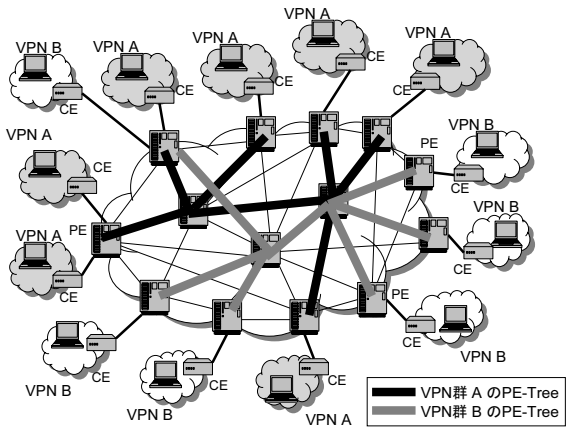

図 5: PE-Tree の例

収集したサイト情報をお互いに交換し，自らのポリシーと合わせて判定する．その後，VPN 固有のポリシー（接続サイト数，接続時刻，利用する暗号方式）等を判定する．

すべてのポリシーが満たされたならば，要求を出したサイト，受けたサイト双方が，所属している PE での CE-VPN の関連付け情報を更新する．この多重帰属成立によって VPN 群が連結するため，VPN 群情報をタイムスタンプの古い方に統一する．この処理は，新しい方の VPN 群の PE-Tree 上にメッセージを流すことで実現する．

PE-Tree への新たな連結を行う必要がある場合は，PE を参加要求先のサイトが所属する PE に接続することで PE-Tree へ仮に連結を行っておく．仮連結後に PE-Tree 上に PE のロックを解除するメッセージを流す．これは，ロック時間を短縮するためである．その後，この PE-Tree に新たに参加する PE は，まずルートノード（VPN 群のラベル ID となっているサイト）にメッセージを投げる．ルートノードに接続できるようならばルートノードが PE にメッセージを返信して接続し，接続できない場合はルートノードが自らの持つルーティングテーブルに基づいて情報収集木にメッセージをブロードキャストする．メッセージを受信した PE は接続する余裕があるようならば，メッセージを出した PE に返信し接続する．このように接続することで，PE-Tree の各 PE 間の距離を最小に保つ．

3.5 VPN からの離脱手順

離脱するサイトは，離脱要求を帰属 VPN 内の各サイト（CE）に送信する．各サイトは所属する PE での自分の VPN 情報（CE と VPN に関するテーブル）を更新する．この離脱サイトが多重帰属していた場合（テーブルで該当 CE と VPN の対応が複数あった場合）は，VPN 群を分割し既存の VPN 群代表ノードと反対側に新たな VPN 群を構築する（VPN 群ラベルを更新する）．

3.6 PE-Tree の再構築

正確な情報の収集の観点のみからは，PE-Tree の再構築を行う必要はない．頻繁な木の再構築は，情報の誤りや，古い情報の伝達を引き起こす反面，再構築をしない場合は，余計な PE が接続した PE-Tree 上で，すでに情報を持っていないより多くの PE を探索することになるのみである．

しかし，探索時間はネットワークをロックする時間に影響するので，できるだけ PE-Tree を最適な木に再構築したい．そこで，周期的に木の再構築を行う期間を設定し，その間は要求を受け付けないことで，安全に木を最適化する．

4 まとめ

従来の帰属制御では，サイトの多重帰属によって生じる VPN 間の間接的な接続関係は考慮されておらず，意図せず情報が漏れてしまう危険性があった．本稿では，サイトの多重帰属によって生じる VPN 間の間接的な接続関係を考慮した VPN の帰属制御についての提案を行った．提案手法は，プロバイダが提供する PPVPN を対象にし，サイトが規定するセキュリティポリシと現在の VPN 構成情報に基づいて，動的な多重帰属制御を実現した．このとき，プロバイダ側で管理する PE によって現在の VPN 構成情報を管理し，PE 間で木状に情報交換を行なうことで，判定のための情報を正確かつ効率よく収集できるようにした．

今後の課題としては，実環境における性能評価，VPN アプリケーションのプロトタイプ実装などがあげられる．

参考文献

[1] Hamed, H., Al-Shaer, E. and Marrero, W.: Modeling and Verification of IPSec and VPN Security Policies, *Proceedings of the 13th IEEE International Conference on Network Protocols (ICNP 2005)*, pp. 259–278 (2005).

[2] Honda, O., Ohsaki, H., Imase, M., Murayama, J. and Matsuda, K.: A Prototype Implementation of VPN Enabling User-Based Multiple Association, *Proceedings of the Ninth IASTED International Conference on Internet & Multimedia Systems & Applications (IMSA 2005),*, pp. 59–64 (2005).

[3] Beak, S. J., Jeong, M. S. and Park, J. T.: Policy-based Hybrid Management Architecture for IP-based VPN, *Proceedings of the 2000 IEEE/IFIP Network Operations and Management Symposium (NOMS 2000)*, 1, pp. 987–988 (2000).

[4] Barrere, F., Benzekri, A., Grasset, F. and Laborde, R.: A Multi-domain Security Policy Distribution Architecture for Dynamic IP Based VPN Management, *Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks (POLICY 2002)*, pp. 5–7 (2002).

[5] Beigi, M., Calo, S. and Verma, D.: Policy Transformation Techniques in Policy-based Systems Management, *Proceedings of the 5th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2004)*, pp. 13–22 (2004).