M-071

SIP を用いた VPN 確立手法の提案

Proposal of VPN Connection Method with SIP

岩崎 哲弥 †　門脇 恒平 ‡　小板 隆浩 †　佐藤 健哉 ‡
Tetsuya Iwasaki　Kohei Kadowaki　Takahiro Koita　Kenya Sato

1 はじめに

VPN 技術の発展によって，ユーザは地理的な制約を受ける事無く LAN 同士を相互に接続することが可能になった．現在では，VPN を実現する様々な技術や形態が存在し，ユーザは法人利用・個人利用などの状況に応じて適したものを選択することができる．

VPN は使用する回線種別の観点から，IP-VPN とインターネット VPN に分けることができる．前者は，通信事業者が所有する閉域 IP 網を利用し，後者はインターネットを利用する．両者は商用サービスとして提供されており，設定におけるユーザの負担が少なくなるように工夫がされている．しかし，ユーザが自ら VPN 対応ルータやサーバを用いて，IPSec や PPTP などでインターネット VPN を構築する場合，ユーザは接続先ごとに IP アドレスや経路の設定を行う必要がある．これは VPN ノード数の増加とともに，設定負担の増大という問題を引き起こす．

上記の問題を解決するためには，外部サーバから VPN ノードの情報を一括取得する方法が有効と考え，本研究では，拡張性と動的な情報登録・通知機能を持つ SIP を利用し，VPN を確立する手法の提案を行う．

2 提案手法の概要

提案手法の基本となる構成要素と動作を図 1 に示す．SIP サーバは，VPN ノードから送信された SIP メッセージの受付や VPN ノードへの情報通知を行う．Location サーバは，SIP サーバからの要求に従って，VPN ノードの情報保持，及び要求に対する応答を行う．

各 VPN ノードは，SIP メッセージを用いて，自ノードの IP アドレスや所属グループ名などの情報の登録要請を SIP サーバに対して行った後，同一のグループに所属するノード情報を要求・取得する．ここでのグループとは，VPN ノードが所属する仮想ネットワークを示すものである．本提案では，グループを導入することにより，各々の VPN ノードが，異なる組織の VPN ノードと干渉する事無く，必要となるノードグループの情報を取得できるようにしている．ノード情報を取得した VPN ノードは，取得した情報を元に，同一グループのノードに対して VPN 接続の要求を行う．そして，VPN 接続が接続先ノードに許可されると，双方のノードは VPN 接続に必要な設定を自ノードに自動追加し，VPN を確立する．このようにして，VPN ノードは，ユーザが逐一 VPN 接続先の IP アドレスを設定する事無く，VPN 接続を確立することが可能となる．

なお，この提案手法に用いる SIP メッセージとその動作は，RFC[1, 2, 3] に独自の定義を加えたものに従う．追加定義した箇所については次章にて説明する．

† 同志社大学 工学部 情報システムデザイン学科
‡ 同志社大学大学院 工学研究科 知識工学専攻

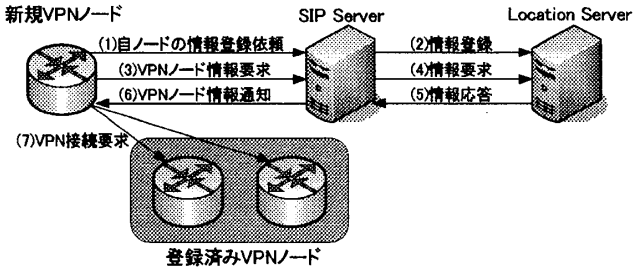

図 1　基本構成と動作

3 SIP による VPN 確立手法

3.1 VPN ノードの情報登録

初めに，新規 VPN ノードは自ノードの情報を登録するために，SIP サーバに対して REGISTER リクエストを送信する．REGISTER リクエストのヘッダフィールドには，VPN ノードの情報として，表 1 で示す情報が格納される．SIP サーバは，受信したリクエストと，既に Location サーバに登録されている VPN ノードの AoR を照合することにより，VPN ノードの重複登録のチェックを行う．登録が許可された場合，VPN ノードの情報が新たに Location サーバに登録される．

RFC には，表 1 に示す UserID と GroupID に相当するフィールドが定義されていなかったため，独自に追加定義を行った．GroupID は，SIP サーバが Location サーバからグループ名をキーとした VPN ノードの検索を行うために用いられる．

また，Location サーバに登録されたノード情報は，SIP メッセージの Expire フィールドで指定された時間だけ管理される．ノード情報は，指定された時間を超えると，自動的に Location サーバから削除されるため，VPN ノードは，定期的に SIP サーバに対して REGISTER リクエストを送信し，情報更新を行う必要がある．

表 1　Location サーバへの登録情報

ヘッダフィールド	目的・意味
To	ノードの論理アドレス (AoR*1)
ContactAddress	ノードの IP アドレス
UserID	ノードの名前
GroupID	ノードの所属グループ名

3.2 ノードリストの要求と取得

次に，新規 VPN ノードは，自ノードが所属するグループの VPN ノードリストを取得するために，SIP サーバに対して情報の要求を行う．情報の要求には，SUBSCRIBE リクエストを用いる．VPN ノードは，リクエストのメッセージボディに，自ノードが所属するグループ名を格納して送信する．SUBSCRIBE リクエストは，情報要求，及び，Location サーバにおけるノードの

*1 Address of Record

登録情報が変更された際の通知予約となる．RFC[2] の規定により，SUBSCRIBE リクエストでは，要求する情報を EVENT フィールドで指定しなければならないため，提案手法では，「grouplist」というフィールド値を独自に追加定義した．VPN ノードは，EVENT フィールドに grouplist を設定することにより，VPN ノードリストの要求であることを SIP サーバに伝えることができる．

要求を受け取った SIP サーバは，要求グループに所属するノードリストを，Location サーバから取得した後，NOTIFY リクエストのメッセージボディに VPN ノードリスト情報を XML 形式 (図 2) で記述し，VPN ノードに通知を行う．SUBSCRIBE リクエストを送信した VPN ノードの情報は，SIP サーバで管理されるため，後に新しい VPN ノードが追加されるなど，Location サーバの情報が更新された際には，既存の全 VPN ノードに通知が行われる．

```
<?xml version="1.0" encoding="UTF-8" ?>
<Grouplist>
   <AoR="R1@example.com">
      <UserID>Tokyo</UserID>
      <GroupID>ExampleCOM</GroupID>
      <ContactAddr>R1@192.168.10.11</ContactAddr>
   </AoR>
   <AoR="R2@example.com">
      <UserID>Kyoto</UserID>
                ⋮
</Grouplist>
```

図 2　XML メッセージ

3.3　VPN 接続の確立

最後に，所属グループのノードリストを受信した新規 VPN ノードは，各々のポリシーに従い，VPN 接続の要求を行う．VPN 接続の要求には，INVITE リクエストを用いる．INVITE リクエストを受信した VPN ノードは，リクエストが，登録プロセスを完了している「信頼性のある」VPN ノードから送信されたものかどうかを判断するために，リクエスト送信元のノード情報が，自ノードに存在するか確認を行う．

接続要求を受信した VPN ノードは，接続要求を許可する場合は「200 OK」，拒否する場合は「403 Forbidden」のレスポンスパケットを，リクエストの送信元ノードに返す．接続が許可された場合，双方の VPN ノードは自ノードに VPN 接続設定を追加する．これによって，VPN 接続確立フローに入り，VPN 接続が確立される．

例として，VPN 確立までの SIP メッセージフローを図 3 に示す．VPN ノード (Z) が新規に VPN グループに参加するノードであり，ノード (X)・ノード (Y) の情報を SIP サーバから得て，VPN の接続要求を行っている．ノード (Z) は，要求を許可して「200 OK」を応答したノード (X) とは VPN 確立フローに入るが，要求を拒否して「403 Forbidden」を応答したノード (Y) とは VPN 確立フローに入らない．

3.4　離脱・登録情報変更

VPN ノードがグループから離脱する際は，SIP サーバに対して，登録の際と同じく REGISTER リクエストを送信する．REGISTER リクエストの Expire フィールドの値を 0 にすることで，即時 Location サーバから該当するエントリを削除することができる．また，VPN ノードの IP アドレスや UserID，GroupID が変更された際も，REGISTER リクエストによって更新が可能である．SIP サーバは，各 VPN ノードを AoR で識別するため，同じ

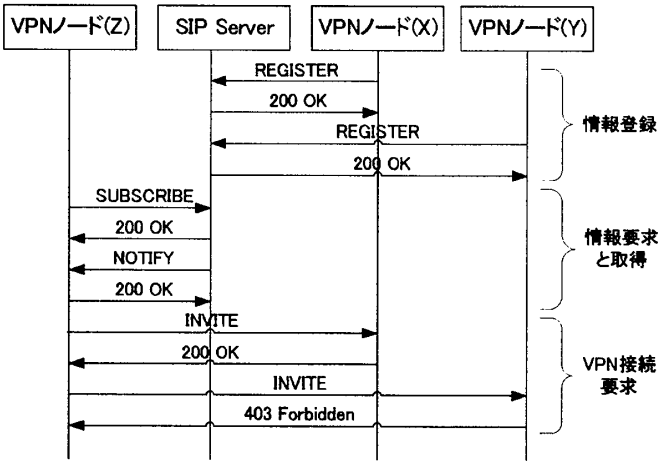

図 3　SIP メッセージフロー

AoR を持つ VPN ノードから異なる内容の REGISTER リクエストを受信した場合にも，随時 Location サーバの登録情報の更新を行う．ゆえに同じ AoR を持つ複数のノードを同時稼動させることは出来ない．

4　考察

本提案手法は，SIP サーバと Location サーバを必要とするため，適用する環境によっては，提案システムの構築コストが，従来の手動設定による VPN 構築のコストよりも大きくなる場合が考えられる．VPN ノード数が少なく，ノード数の増減が起こらない環境では，動的にノード情報を入手できるという本提案手法のメリットが生かせない．そのような環境のユーザに対しては，本提案システムを外部サービスとして提供することで，ユーザ自身がシステムを構築するコストを無くすことが可能である．

5　まとめと今後の課題

本稿では，VPN 設定の煩雑さを解消するために，SIP の登録・通知機能に着目し，SIP を用いた VPN 確立手法の提案を行った．提案手法により，VPN ノードは，リアルタイムに同グループの VPN ノードを発見し，VPN 接続を確立することが可能となる．また，VPN ノードの状態変化に対しても，随時情報の更新と通知が行われるため，VPN ノードの構成を適切に反映した設定維持が可能である．ゆえに，将来的にモバイル環境などの動的に変化するネットワークに適応することで，目的別や組織別グループの VPN が構築可能になり，より大きなメリットが得られると考える．

今後は，本提案手法に従った SIP サーバ，SIP クライアントの開発を行い，VPN アプリケーションと連携させ，詳細な評価を行う．

参考文献

[1] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E.: SIP:Session Initiation Protocol, RFC 3261 (2002).

[2] Roach, A.: Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265 (2002).

[3] Rosenberg, J.: A Presence Event Package for the Session Initiation Protocol (SIP), RFC3856 (2004).