1B-2

オンデマンドＶＰＮにおける構成情報生成に関する一検討

有馬　一閣　　早川　晃弘　　高橋　成文　　鎌仲　裕久

株式会社ＮＴＴデータ

１．はじめに

今日，インターネットを経由した通信は盗聴，改ざんの危険性があり，重要な情報を扱う場合は通信内容を暗号化することが求められ，ＶＰＮ(仮想専用通信回線)が広く使用されている．

特にＩＰｓｅｃによるＶＰＮを構築するにはＶＰＮの接続可否情報の設定，機器間の暗号通信路のための設定，ＶＰＮの経路の設定を行う必要があり，その設定作業は煩雑であるとの問題や，作業の際に起きる情報漏えい等の問題のため，誰もが容易に設定作業を行い使用できるものではなかった．さらにセキュアな通信による多地点会議など，ＶＰＮを多地点で接続するニーズがあるものの実現する機器が高価であるといった問題があった．

オンデマンドＶＰＮは，ＶＰＮ機器への設定値などをセンタから配信することにより，利用者の要求に応じて直ちにＶＰＮを構築する技術であり，上述の問題を解決することができる[1]．本稿では，オンデマンドＶＰＮで任意の地点間を動的に接続するために，ネットワークの状態に応じて機器に設定するパラメータを自動生成するオンデマンドＶＰＮでの構成情報生成機能について整理を行い，多地点接続時に決定するトポロジーの構築に関する検討結果について述べる．

２．オンデマンドＶＰＮの構成情報生成

２．１．構成情報生成機能の概要

オンデマンドＶＰＮでの構成情報とは，ＩＰｓｅｃを用いた暗号通信路を構築するための情報である．構成情報の種別には以下のものが挙げられる．

・　ＶＰＮ接続の可否に関する情報
・　機器間の暗号通信路に関する情報
・　ＶＰＮの経路に関する情報

オンデマンドＶＰＮは，ＶＰＮ構築を容易にするセンタ配信方式を採用しており，構成情報をセンタで生成・管理し，ユーザの要求に応じてオンデマンドＶＰＮ機器(ＯＤ－ＶＰＮ機器)に配信し設定を自動的に行うことができる．センタ配信方式での構成情報の設定方式の概要を図 1に示す．ＶＰＮ管理サーバで生成される構成情報は上記の情報種別ごとに処理され，配信される情報として生成される．ＶＰＮ接続の可否に関する情報に関しては，接続ポリシーを元に，接続ポリシー処理モジュールで生成される．また，機器間の暗号通信路に関する情報はサーバ設定を元に，ＶＰＮ管理サーバで生成される．さらに，ＶＰＮの経路に関する情報は，ＩＰアドレスや接続可能な端末の情報を元に，トポロジー決定モジュールとＩＰルーティングモジュールによって情報が生成される．生成された情報は，機器に実際に設定する形式でＶＰＮ管理サーバから各機器に配信される．配信される情報はＩＰｓｅｃ[2]で定義されているＳＰ(Security Policy)の集合体であるＳＰＤ(Security Policy Database)とＩＰｓｅｃの動作設定情報，ＩＫＥ(Internet Key Exchange)用の事前共有秘密鍵，ルーティング情報になる．

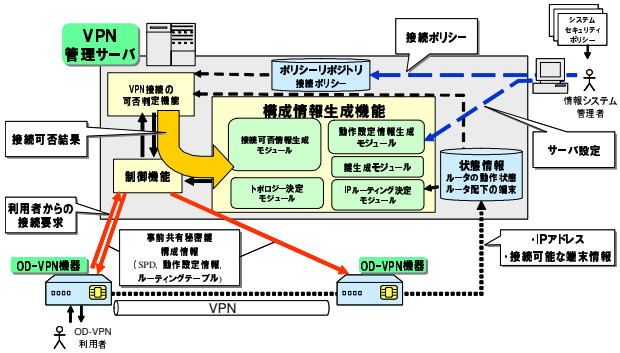


図 1 センタ配信方式での構成情報生成機能の概要

表 1 情報種別と配信される構成情報の対応

情報種別	元となる情報	情報を生成する箇所	実際に配信される構成情報
VPNの接続可否情報	接続ポリシー 状態情報	接続可否情報生成モジュール	SPD
暗号通信路の情報	サーバ設定	鍵生成モジュール， 動作設定情報生成モジュール	IPsecの動作設定情報
			事前共有秘密鍵
経路情報	IPアドレス 接続可能な端末	トポロジー決定モジュール， IPルーティング決定モジュール	SPD
			ルーティングテーブル

情報の種別ごとに，元となる情報，情報の生成する箇所，実際に配信される情報との対応を表 1にまとめた．以下に実際に配信される構成情報ごとに概要を説明する．

２．２．生成・配信される情報

２．２．１．　ＳＰＤ

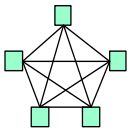
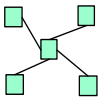
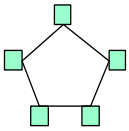
ＳＰＤとは，ＩＰパケットの処理の方法を記述したＳＰが格納されているもので，機器ごとに出力用と入力用の２つが存在する．始点ＩＰアドレス，終点ＩＰアドレス，プロトコル，宛先ポートの組み合わせに対し，ＩＰｓｅｃ適用の有無や，適用した時に何処を接続対象とし，どのようなアルゴリズムで暗号化や認証を行うか等の情報が記述されている．ＳＰＤは，ＶＰＮ接続可否判定機能で管理者より与えられる接続ポリシーと，ＯＤ－ＶＰＮ機器より与えられる状態情報で判定した結果を元に生成される．

２．２．２．　ＩＰｓｅｃ動作設定情報

ＩＰｓｅｃ動作設定情報とは，機器間の IPsec コネクションであるＳＡ(Security Association)を生成するために必要となるパラメータである．具体的にはＳＡを作成するためのＩＫＥに必要なクッキーや乱数値，ＳＡの

A study of creating structure information on On-demand VPN
Kuniharu ARIMA (arimakn@nttdata.co.jp)
Akihiro HAYAKAWA (hayakawaak@nttdata.co.jp)
Shigefumi TAKAHASHI (takahashisg@nttdata.co.jp)
Hirohisa KAMANAKA (kamanakah@nttdata.co.jp)
NTT DATA CORPORATION

表２オンデマンドＶＰＮにおけるトポロジーパターンの特性

		メッシュ型	スター型	リング型	直線型
機器への負担	接続確立によるコスト	△ × 端末にN個分の暗号通信路を設定する必要がある o(N^2)の暗号通信路が用意される	○ ○ 中央の機器以外は1つの暗号通信路を設定すればよい o(N)の暗号通信路が用意される	△ ○ 端末に2つの暗号通信路を設定すればよい o(N)の暗号通信路が用意される	△ ○ 端末に最大2つの暗号通信路を設定すればよい o(N)の暗号通信路が用意される
	通信によるコスト	○ 片道の通信の際に，1回の暗号処理方式が行われるが，遅延は比較的小さい	△ 片道の通信の際に，最大2回の暗号処理が行われ，遅延が比較的大きい	× 片道の通信の際に，最大N/2回の暗号処理が行われ，遅延が大きい	× 片道の通信の際に，最大N-1回の暗号処理が行われ，遅延が大きい
セキュリティ		○ 通信の当事者以外に通信内容を確認されることは無い	× 通信の当事者以外の中継者が通信を確認することが可能になる	× 通信の当事者以外の中継者が通信を確認することが可能になる	× 通信の当事者以外の中継者が通信を確認することが可能になる
接続柔軟性		○ どこかの機器もしくは線が使用できなくても通信を行うことが可能	× 中央の機器が使用できなくなると全ての通信ができなくなる	○ どこかの機器もしくは線が使用できなくても通信を行うことが可能	△ どこかの機器もしくは線が使用できなくなった場合，通信が分断される
情報生成量		× 一つの端末にN-1台分の設定を行うのでN*(N-1)で計算量はO(N^2)	○ 中心の端末はN-1台分，その他の端末は1台分なので2*(N-1)で計算量はO(N)	△ 1つの端末に2台分の設定を行うので2*Nで計算量はO(N)	○ リング型の設定情報より2台分少ないので2*N-2=2*(N-1)で計算量はO(N)
例					

（Nは通信する機器の総数）

有効期間等である．これらの情報は情報システム管理者よりサーバの設定時に与えられ，動作設定情報生成モジュールで生成され，機器間の暗号通信路に関する情報として扱われる．

２．２．３． 事前共有秘密鍵

オンマンドＶＰＮではＩＫＥを行う際の相手認証方式に事前共有秘密鍵方式を用いている．事前共有秘密鍵は管理サーバで生成され，セキュアメッセージングによって通信機器のチップへと書き込まれる．管理サーバではこの事前共有秘密鍵のみを生成し，実際の暗号通信路に使用される秘密共有鍵は，ＯＤ－ＶＰＮ機器同士がＶＰＮ接続を行っている時にしか知り得ないようになっている．

２．２．４． ルーティングテーブル

ルーティングテーブルはＩＰパケットが目的の機器にたどり着くのに，どの経路を通るかを記述したものである．構築するＶＰＮが２地点の場合は，宛先として接続相手の情報を持ち，生成する暗号通信路を通るように記述される．しかし，多地点でＶＰＮを構築する場合，構築するトポロジーの形状は一意には定まらないため，実際のＩＰルーティングを設定する前に，トポロジーの形状を決定する必要がある．トポロジーの構築について 3 章で述べる．

３． トポロジーの構築

多地点でＶＰＮを構築する際にはトポロジーの形状を決定する必要があるが，トポロジーパターンによって特性が異なることが岡田ら[3]によって示されている．オンデマンドＶＰＮではＶＰＮ管理サーバは接続の可否制御，構成情報の生成・配信等の機能を持つだけで，直接ＶＰＮの通信路にならない．ここではオンデマンドＶＰＮにおけるトポロジーの構築について述べる．

代表的なトポロジーパターンにはフルメッシュ型，スター型，リング型，直線型があり，これらのパターンとその複合型でトポロジーは成り立つ．

このトポロジーパターンを次の観点で評価する．

- 機器の負担：機器への負担が大きくなると通信遅延，動作不安定等の症状を引き起こす可能性がある．暗号通信路を構築する初期コストと，通信を行った際の暗号化復号化による通信コストについて評価する．
- セキュリティ：通信の内容に対する第３者の介在性について評価する．
- 接続柔軟性：構築されたＶＰＮに障害が発生した場合にＶＰＮ接続を保てるかを評価する．
- 情報生成量：機器に設定する情報が大きくなるとＶＰＮ管理サーバでの計算量が多くなる．また情報量が多いと機器に設定する通信に遅延が発生すると考えられるため，生成する情報の量について評価する．

オンデマンドＶＰＮでのトポロジーパターンと特性の関係についての検討結果を表 2に示す．

４． まとめ

本稿では，まずオンデマンドＶＰＮの構成情報を分類し，センタ管理方式での構成情報生成機能の概要について示し，実際に配信される情報を整理した．また，VPN を構成するトポロジーの形状によって，機器への負担やセキュリティ，接続柔軟性，情報生成量にどのような影響を与えるかを検討した．今後はオンデマンドＶＰＮの多地点接続についてシミュレーションを行い，機器への負担と情報生成量に着目しトポロジーの評価を行うことで，構成情報生成機能の実環境への適用を検討する．

謝辞

本研究は，総務省の平成 16 年度「高度ネットワーク認証基盤技術の研究開発」の委託を受け，「オンデマンド VPN 技術についての研究開発」に関するものである．関係者各位に感謝する．

参考文献

[1] 早川晃弘，星川知之，高橋成文，鎌仲裕久：”オンデマンドＶＰＮアーキテクチャの提案” 情報処理学会第 67 回全国大会，2005

[2] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Internet Society, Network Working Group, Nov. 1998

[3] 岡田浩一，冨士仁：スター型 End-to-end-VPN を提供する VPN-exchange 方式のスケーラビリティ向上，情報処理学会 コンピュータセキュリティ研究会 研究報告「コンピュータセキュリティ」No.016，Feb 14 2001