1B-4

オンデマンドＶＰＮアーキテクチャの提案

早川 晃弘　　星川 知之　　高橋 成文　　鎌仲 裕久

株式会社ＮＴＴデータ

1. はじめに

今日，インターネット上で重要な情報を流通させるのに IPsec や SSL を用いた VPN(Virtual Private Network)の利用が進んでいる．さらに，常時接続ブロードバンドネットワークの普及とともに，IP 電話(VoIP)に代表される，ポイントー・ツー・ポイントで好きなときに端末同士を簡単に結ぶ利用形態も増加しつつある．

しかし，IPsec を用いて VPN 接続するには，ネットワークの専門知識が必要であり，誰もが容易に設定し利用できる状況ではない．VPN 接続も，好きなときに簡単に利用できれば，インターネット上での新しい利用形態が実現すると考えられる．

そこで，利用者からの要求により指定された地点を，直ちに VPN 接続するオンデマンド VPN を提案する．

2. オンデマンドＶＰＮ技術

オンデマンド VPN 技術は，利用者からの多様な VPN 接続の要求に対して，直ちに指定された地点間を，IPsec を用いて VPN 接続することを可能にする技術である．

従来の IPsec による VPN 接続では，接続機器を管理する情報システム管理者(以下，管理者)が，接続機器や情報システム毎に定められたシステム・セキュリティポリシーを参照して，VPN 接続の可否を判断する．その後，鍵交換プロトコル(IKE)で用いる認証用の事前共有鍵や，暗号化対象となるパケットの条件等の情報(構成情報)を，接続機器の管理者間の交渉を通して決定し，VPN 接続前に全ての接続機器に設定する．そのため，利用者が指定した機器同士を直ちに VPN 接続するのは困難である．

そこで，IPsec による VPN 接続に必要な情報をセンタで一元的に管理し，利用者の要求に応じて配信するセンタ管理方式を考える．センタが利用者の接続要求を基に接続可否を判断し，IKE で用いる事前共有鍵と構成情報を自動生成し，VPN を実現するルータ等へ配信する．

利用者からの多様な VPN 接続要求に対して，システム・セキュリティポリシーを考慮した接続可否判断の実現するためには，パケットフィルタのような単純な条件設定ではない接続制御機能が必要である．岡田らは，[1]においてスター型の VPN 接続技術である「VPN Exchange」方式を提案し，接続制御機能について述べているが，具体的な処理方式までは言及していない．

また，センタから配信する事前共有鍵等の情報が誤った機器へ配信されると，機器の成りすましも可能となり，機密情報の漏洩にもつながる．そのため，センタ管理方式には，誤った機器への配信等がない安全な配信方式が必要である．辻元らは，[2]においてセンタ管理方式による動的な VPN 接続方式を提案しているが，VPN ルータへの事前共有鍵や構成情報を安全に配信するための仕組みまでは言及していない．

A proposal of On-demand VPN architecture
Akihiro HAYAKAWA (hayakawaak@nttdata.co.jp)
Tomoyuki HOSHIKAWA (hoshikawat@nttdata.co.jp)
Shigefumi TAKAHASHI (takahashisg@nttdata.co.jp)
Hirohisa KAMANAKA (kamanakah@nttdata.co.jp)
NTT DATA CORPORATION

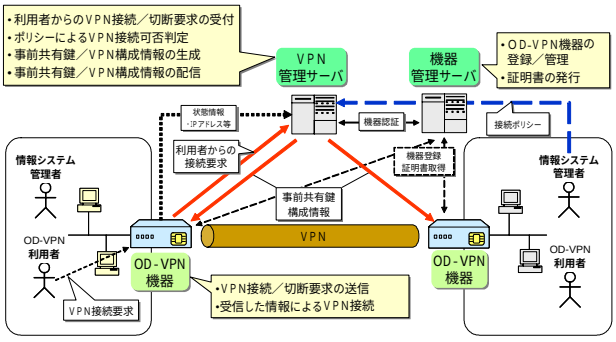

図1 オンデマンド VPN 全体アーキテクチャ

我々は，接続制御機能と安全な構成情報配信機能を有する，センタ管理方式によるオンデマンド VPN アーキテクチャを提案する．接続制御機能は，システム・セキュリティポリシーを基に作成する「if <Condition> then <Action>」形式のポリシー文書(接続ポリシー)を用いたポリシー制御技術で実現する．また，耐タンパ性を有する IC チップ(e-Key チップ)を搭載した機器を用い，2 階層 PKI 技術による Secure e-Key Network フレームワーク[3]を利用して安全な構成情報配信機能を実現する．

3. オンデマンドＶＰＮアーキテクチャ

3.1. システム構成

図 1にオンデマンド VPN の全体アーキテクチャを示す．

VPN 管理サーバは，VPN 接続に必要な情報を管理するセンタとして機能し，利用者からの VPN 接続／切断要求を受付ける．その後，管理者が登録する接続ポリシーを用いて接続可否を判定し，OD-VPN 機器に構成情報等を配信する．OD-VPN 機器は，IPsec による VPN を実現する端末やルータ等の装置である．利用者からの VPN 接続要求を VPN 管理サーバに送信し，配信された構成情報等を用いて VPN を実現する．機器管理サーバは，OD-VPN 機器の所有者等の情報を管理し，機器を識別するための証明書等を発行する．

3.2. 処理フロー

オンデマンド VPN の処理フローを，「事前準備フェーズ」と「VPN 利用フェーズ」に分けて以下に説明する．

3.2.1. 事前準備フェーズ

1. OD-VPN 機器を，機器の所有者等の情報と共に機器管理サーバに登録する．登録完了時に，1 階層目の PKI 情報(1stPKI)である公開鍵証明書等を取得する．
2. OD-VPN 機器を，VPN 管理サーバに登録する．1stPKI を利用して機器を認証し，オンデマンド VPN の利用権を兼ねる 2 階層目の PKI 情報(2ndPKI)である公開鍵証明書等を取得する．
3. OD-VPN 機器を利用するユーザを VPN 管理サーバに登録する．登録時に，第三者による個人認証基盤サービスと連携した個人認証が可能である．
4. 管理者は，管理している機器等のシステム・セキュリティポリシーを参考に，要求された VPN 接続を許可または不許可とする接続ポリシーを作成し，VPN

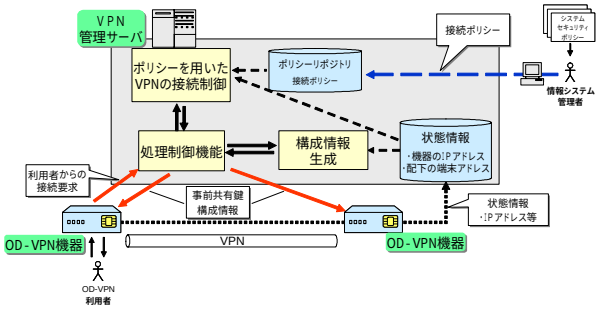

図2 VPN 管理サーバの構成

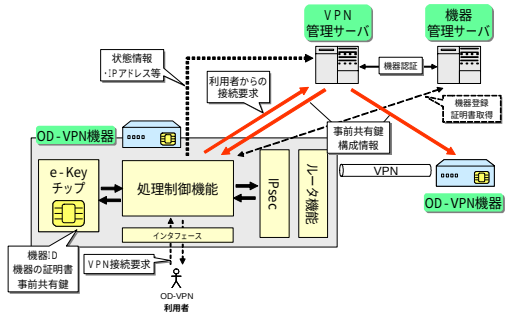

図3 OD-VPN 機器の構成

管理サーバに登録する．

5. インターネットに接続された OD-VPN 機器は，自身の IP アドレスや配下に接続された端末の IP アドレス等を状態情報として VPN 管理サーバへ登録する．

3.2.2. VPN 利用フェーズ

1. 利用者は，OD-VPN 機器を通して VPN 管理サーバへログインする．このとき，利用者認証だけでなく 2ndPKI を使った機器認証が行われ，オンデマンド VPN の利用権が確認される．
2. 利用者は，VPN 管理サーバに登録されている状態情報から目的の接続地点を検索する．
3. 利用者は，接続する地点を指定して，VPN の接続要求を VPN 管理サーバへ送信する．
4. VPN 管理サーバは，接続する各地点の接続ポリシーを参照し，接続の可否を判定する．接続許可の場合は処理を継続し，接続不許可の場合は中止する．
5. VPN 管理サーバは，接続要求を基に VPN 接続するための構成情報と IKE 用の事前共有鍵を生成する．
6. VPN 管理サーバは，生成した構成情報と事前共有鍵を OD-VPN 機器に配信する．
7. OD-VPN 機器は，取得した構成情報と事前共有鍵を用いて IKE を実施し，指定された地点間の VPN 接続を完了する．

3.3. VPN 管理サーバ

VPN 管理サーバの構成を図 2に示す．従来，VPN 接続要求を受けてから設定情報を配信するまでに管理者間の交渉によって実現していた「VPN の接続制御」と「構成情報の生成」の機能を有する．

3.3.1. VPN の接続制御

接続可否判断処理(接続制御)は，「if <Condition> then <Action>」形式で記述されたルールの集合で定義される接続ポリシーを用いたポリシー制御技術により実現する．接続ポリシーの<Condition>部には，VPN 接続を行う時刻や接続先の組織名等に関する条件が記述され，接続要求が<Condition>部の条件を満たしたとき，その接続を許可とするか接続不許可とするかを<Action>部に記述する．各機器の管理者は，システム・セキュリティポリシーを基に接続ポリシーを作成し，VPN 管理サーバのポリシーリポジトリに登録する．

VPN 管理サーバは，接続する地点の各接続ポリシーと VPN 接続要求の内容を比較し，VPN 接続要求が接続ポリシーの<Condition>部を満たせば，そのポリシーの<Action>部の記述(許可または不許可)を判定結果とする．

3.3.2. 構成情報の生成

IPsec による VPN 接続では，暗号化対象となるパケットを構成情報によって指定する．構成情報は，パケットの発信元アドレス，配送先アドレスやポート番号等が用いられる．利用者が指定した地点を VPN 接続するためには，接続要求毎に VPN 管理サーバによって構成情報を生成する必要がある．指定された 2 地点を接続する場合は，接続要求に含まれる地点情報と，VPN 管理サーバに登録されている状態情報から構成情報を生成する．

3 地点以上が指定された場合は，2 地点間の VPN 接続を複数利用して VPN 網を形成し，各地点間の通信を実現する．VPN 上で利用される通信の特性を考慮して，VPN 網のトポロジを決定し，接続する各 2 地点間の構成情報を生成することで，3 地点以上の VPN 接続を実現する．

3.4. OD-VPN 機器

OD-VPN 機器の構成を図 3に示す．耐タンパ性を有する e-Key チップは，2 階層 PKI 技術を実装し，機器管理サーバへの登録時に 1stPKI 情報が，VPN 管理サーバへの登録時に 2ndPKI 情報がチップ内に格納される．VPN 管理サーバとの通信は，2ndPKI 情報によって正しい機器であることが認証された後に行われ，誤った機器への情報配信を防ぐ．さらに IKE で用いる事前共有鍵は，セキュアメッセージング方式により暗号化されたまま e-Key チップ上に格納することで，より強固に情報漏えいを防ぐ．配信された構成情報と事前共有鍵によって，OD-VPN 機器間で IKE が実行され，VPN が開通する．

4. まとめ

本稿では，利用者の要求に応じて，指定された地点を直ちに IPsec を用いて VPN 接続するオンデマンド VPN 技術を実現するセンタ管理方式によるアーキテクチャを提案した．本提案において，e-Key チップを用いた構成情報の安全な配信方式および，従来管理者間の交渉によって実現した VPN 接続の可否判断と構成情報の生成を有する VPN 管理サーバの構成を示した．

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」の委託を受け実施している「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] 岡田,他："個人単位の VPN を実現するネットワークサービス「VPN Exchange」",情報処理学会 CSS2001 論文集,pp.67-72,Oct 01.

[2] 辻元,他："IPv6 IPsec による End-to-End VPN 構築方式に関する考察",情報処理学会 コンピュータセキュリティ 14-28,Sep 01.

[3] 小尾，他："オープンネットワーク環境で安全な鍵配送を実現するネットワーク基盤"，電子情報通信学会 2004 年総合大会予稿集，Mar 2004