1B-5

オンデマンド VPN におけるポリシー制御機能に関する一検討

竹内 陽一　早川　晃弘　高橋　成文
株式会社　NTT データ

1．はじめに

インターネットでは，データの暗号化と相互認証を行うプロトコルとして IPsec[1]による VPN が利用されている．しかし，IPsec による従来のインターネット VPN では，管理者が事前にマニュアルでパラメータを設定する必要があった．また，設定誤りにより正しく動作しない等の問題が指摘されていた．更に，Internet Key Exchange (IKE)を行うための事前情報が漏洩すると，VPN そのものの安全性に問題が生じる．

そこで，我々は，利用者の要求に合わせて IPsec による VPN を自動的に構築するオンデマンド VPN の開発を進めている[2]．具体的には，オンデマンド VPN は，利用者の接続要求を基に，センタで接続の可否を判断し，IPsec による VPN 接続に必要な設定情報を各機器に配信する．

本稿では，オンデマンド VPN において，接続の可否を判断する接続制御機能について述べる．以下，接続制御に用いる接続ポリシーと要求コンテキスト，更に，接続制御の処理方式について説明し，XACML による実装方式を示す．

2．IPsec の接続制御における問題点

IPsec では，通常，パケットの振る舞いを決定する SPD(Security Policy Database)を接続元と接続先にあらかじめ設定しておく．SPD には，利用するセキュリティプロトコルや，暗号アルゴリズム等が記述されている．しかし，SPD の条件部には，パケットの接続元アドレスや接続先アドレス，ポート番号，上位レイヤプロトコル等が記述できるが，例えば，端末のセキュリティレベル等を記述することはできない．

宛先端末のセキュリティレベルに応じて IPsec による接続の可否を決定する様なオンデマンド VPN では，SPD とは別に接続ポリシーを導入し，接続制御機能で接続ポリシーに基づいた接続可否判断を行っている．

3．オンデマンド VPN における接続制御

3.1 接続ポリシーと要求コンテキスト

オンデマンド VPN では，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あらかじめ端末毎に設定しておく．

利用者から接続要求を受け付けると，要求コンテキストが生成され，接続ポリシーと要求コンテキストを比較し，VPN の接続制御を行う．

接続ポリシーは，「if <Condition> then <Action>」形式で記述されたルールの集合で定義される．接続ポリシーの<Condition>部には，VPN 接続を行う時間帯や接続先の組織名等に関する条件が記述される．また，<Action>部には接続要求が<Condition>部を満たした時，その接続を許可とするか不許可とするかを記述する．接続ポリシーの主な記述内容を図 1に示す．

条件部(Condition)
- [**相手先端末**]
  - ･**機器ID＋端末ID**
  - ･**端末のIPアドレス**
  - ･**端末の種別**
  - ･**端末の役割**
  - ･**機器が所属する組織名**
- [**VPNで利用するAPの種類**]
  - ･**サービス名**
- [**相手先利用者の条件**]
  - ･**利用者の役割**
- [**時間**]
  - ･**接続する時間帯**

実行部(Action)
- [**接続判断**]
  - ･**許可または不許可**

図 1　接続ポリシーの主な記述内容

3.2 VPN 接続制御

3.2.1.　接続の可否判断

ユーザの役割を用いて接続制御を行う Role Base Access Control (RBAC[3])等，従来の接続制御は，接続対象(接続先であり，RBAC では object に相当する)が持つ接続ポリシーに基づき，接続の可否を判断する．一方，VPN の接続は，相互に通信可能となる特性を持つため，接続元も接続対象に対して接続ポリシーを設け，接続の可否を判断する．つまり，オンデマンド VPN は，ポリシー制御機能として，接続対象(接続先)が持つ接続ポリシーだけでなく，接続元が持つ接続ポリシーも用いて接続可否を判断する．

3.2.2.　接続制御の処理方式

オンデマンド VPN における接続制御の処理方式について以下に述べる．図 2に示すように，端末 A を操作している利用者から端末 B に対して，VPN 接続要求が発せられた場合を想定して，接続制御の流れを説明する．

① 各機器の管理者は，あらかじめ，ポリシーリポジトリに接続ポリシーを登録する．接続ポリシーには，3.1 で説明した記述内容が含まれている．
② 端末 A を操作している利用者が，端末 B への VPN 接続要求を，VPN 管理サーバに出す．
③ VPN 管理サーバは，VPN 接続要求を受信すると接続要求のパラメータから要求コンテキストを生成する．
④ VPN 管理サーバは，ポリシーリポジトリから，A の接続ポリシーと B の接続ポリシーを抽出する．
⑤ VPN 管理サーバは，抽出した A の接続ポリシーのうち，要求コンテキストと比較して条件部を全て満たす接続ポリシーに対して，実行部をチェックし，許可/不許可を判定する．
⑥ B の接続ポリシーに対して，⑤と同様のマッチング処理を行い，許可/不許可の判定を行う．
⑦ VPN 管理サーバは，VPN 接続判定を行う．A と B 共に，

A study of Policy control on On-demand VPN
† Yoichi TAKEUCHI(takeuchiyui@nttdata.co.jp)
Akihiro HAYAKAWA (hayakawaak@nttdata.co.jp)
Shigefumi TAKAHASHI (takahashisg@nttdata.co.jp)
NTT DATA CORPORATION

許可となった場合， VPN 接続を許可する．

⑧ VPN 管理サーバは，VPN 接続が許可の場合は，接続ポリシーの実行部に従い，IPsec を設定するという SPD を生成し，OD-VPN 機器に設定する．

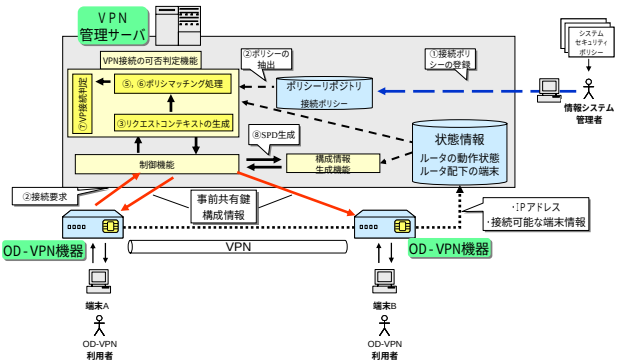

図 2　接続制御の流れ

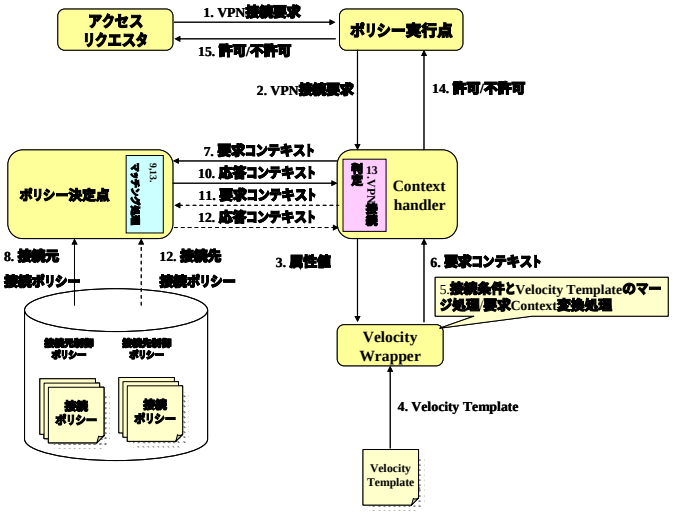

図 3　VPN 管理サーバの処理フロー

4．実装

4.1 VPN 管理サーバの実装方式

本提案手法に，柔軟で拡張性のあるアクセス制御を実現するため，接続ポリシーの記述方法として，XACML（eXtensible Access Control Markup Language[4]）を用いた．また，接続ポリシーを用いてマッチング処理を行うエンジンには，Sun Microsystems が公開している XACML implementation[5]を用いた．VPN 管理サーバの処理フローを図 3に示す．

4.2 要求コンテキストの生成処理の実装方式

XACML では，要求コンテキストを XML 文書の形式で表す．XACML における要求コンテキストは，接続元<Subject>，接続先<Resource>，動作<Action>の 3 つのタグを含んでいる．オンデマンド VPN では， VPN 要求を行う接続元を<Subject>に，接続先を<Resource>に， VPN 接続という動作を<Action>に，それぞれ割り当てる．また，<Subject>や<Resource>の中には，端末の IP アドレスや端末の役割等の属性を<Attribute>タグを用いて記述する．

このように，オンデマンド VPN での要求コンテキストはシンプルな構造をしている．この点に着目し，要求コンテキストをテンプレートを用いて動的に生成することとした．

具体的には，テンプレートエンジン Velocity[6]を用いて実装した．属性値を抽出する Java のコードが埋め込まれたテンプレートをあらかじめ作成しておき，利用者からの接続要求に応じて動的に要求コンテキストを生成する．

また，要求コンテキストは，<Subject>や<Resource>の中に<Attribute>タグの繰り返しを含んでいる．そこで，属性値を抽出する Java のコードをタグの繰り返し分だけ呼び出す．このようにして，<Attribute>タグの数に関わらず１つのテンプレートで要求コンテキストを生成する事が可能となる．

5．まとめ

本稿では，オンデマンド VPN において，接続の可否を判断する接続制御機能について述べた．接続制御に用いる接続ポリシーの記述内容を明らかにし，接続制御の処理方式についても説明した．また，XACML による実装方式を示した．今後は，VPN 管理サーバの接続制御に関して，速度やスループット等の性能の評価を行う予定である．

謝辞

本研究は，総務省からの平成 16 年度「高度ネットワーク認証基盤技術の研究開発」の委託に基づき実施している「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] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, Internet Society, Network Working Group, Nov. 1998

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

[3] R.Sandju, E.Coyne, H.Feinstein and C.Youman, “Role Based Access Control Model”, IEEE Computer, 29(2), Feb.1996

[4] OASIS, “extensible Access Control Markup Language(XACML) Version 1.0” http://www-oasisopen.org/commitees/download.php/2406/oasis-xacml-1.pdf, 2003

[5] Sun’s XACML Implementation, http://sunxacml.sourceforge.net/

[6] Velocity, http://jakarta.apache.org/velocity/