3F-5

公開鍵証明書によるオンデマンドVPNシステムの提案

有馬　一閣　　星川　知之　　鎌仲　裕久　　中嶋　正臣

株式会社ＮＴＴデータ

1. はじめに

今日，ブロードバンドネットワーク回線と暗号化技術の普及により，仮想専用線ネットワーク(VPN)を用いて拠点間のセキュアな通信路を構築することが可能となった．しかし，VPN の開設には，専門知識を有する者による VPN の構成情報や通信の暗号化に用いる鍵情報等の生成・設定が必要である．そのため，VPN の開設にかかるコスト及び時間が課題となっている．

筆者らはこの課題を解決するためにオンデマンド VPN の研究開発を行っている[1]．オンデマンド VPN では，VPN の制御を行うサーバ（VPN 管理サーバ）と実際に接続を行う機器（VPN 機器）を用いて IPsec-VPN を構築する．ユーザが接続したい VPN 機器に対して VPN 開設の要求を行うと，VPN 管理サーバは事前共有鍵と構成情報を生成し，VPN 機器に配信・設定する．これにより，ユーザの所有する VPN 機器と要求先の VPN 機器の間で自動的に IPsec-VPN が構築される．

今後，オンデマンド VPN を利用する機器の増加に伴い，管理主体の異なる VPN 管理サーバの増加が想定される．そのような状況では，管理主体の異なる VPN 機器間での相互接続が必要になると考えられる．想定される相互接続に対応するために，IPsec-VPN を構築する際に実施する鍵交換プロトコル(IKE)で行う相手認証の方式として，公開鍵証明書(PKC)を利用するデジタル署名方式について検討を行った．

本稿では，オンデマンドに PKC 及び構成情報を配信し IPsec-VPN の構築を可能にするオンデマンド VPN システムの方式を提案し，評価を行う．

2. 公開鍵証明書を用いた方式

2.1. 2階層 PKI

オンデマンド VPN は，NICSS[2]で提唱されている２階層 PKI を応用し実現されている．２階層 PKI には以下の特徴がある．

- チップ管理の認証とアプリケーション利用に関する認証を，独立したレベルの異なる鍵を用いて実現することにより利用権を安全に配送することが可能
- 多様なサービスを，チップを使用することにより便利かつ安全に利用することが可能

２階層 PKI では以下の PKC を使用している．

- **１階層目の PKC(1stPKC)**：機器の正当性を証明
- **２階層目の PKC(2ndPKC)**：VPN サービスを使用できる正当な機器であることを証明

2.2. 方式の提案

IKE で行う相手認証の方式であるデジタル署名方式をオンデマンド VPN に適用するために，以下の点で方式検討を行う．

- デジタル署名方式では，署名および検証を行うための PKC が必要となる．オンデマンド VPN に適用する際に，どのような PKC を用い，デジタル署名による正当な相手認証を効率よく実現するかについて検討を行う
- 通常の IPsec-VPN を構築するには，接続が許可され構成情報が設定された状態が前提条件となるが，オンデマンド VPN では VPN 管理サーバから VPN 機器に構成情報が配信される．この構成情報の中に含まれる接続許可情報を安全に配信するための，接続許可情報のデータ形式について検討を行う

2.2.1. IKE の相手認証で使用する PKC

IKE でデジタル署名方式を使用する際の PKC として，以下の２つの PKC を使用した方式が考えられる．

- **２階層 PKI の 2ndPKC を使用する方式：**事前に配布してある 2ndPKC を再利用することにより，管理する情報量を削減することが可能になる
- **VPN 接続のために新たに発行された PKC(3rdPKC)を使用する方式：**PKC を新たに発行し，サービスの認証に使用する PKC とは異なる PKC を使用することにより，サービス加入と接続を厳密に区別して管理することが可能になる

On-demand VPN Using Public Key Certificate
Kuniharu ARIMA (arimakn@nttdata.co.jp)
Tomoyuki HOSHIKAWA (hoshikawat@nttdata.co.jp)
Hirohisa KAMANAKA (kamanakah@nttdata.co.jp)
Masaomi NAKAJIMA (nakajimam@nttdata.co.jp)
NTT DATA CORPORATION

表 1 検討方式の比較表

相手認証のPKC	接続許可情報のデータ形式	時間	セキュリティ	情報の管理
2ndPKC	未加工	○	△ 改ざん検証ができない	○
	署名付加	△ 署名の検証が必要	○	○
	属性証明書	△ 証明書の検証が必要	○	△ 属性証明書の管理が接続毎に必要になる
	PKC	△ 証明書の検証が必要	○	△ PKCの管理が接続毎に必要になる
3rdPKC	未加工	○	△ 改ざん検証ができない	△ 3rdPKCの秘密鍵の管理も必要になる
	署名付加	△ 署名の検証が必要	○	△ 3rdPKCの秘密鍵の管理も必要になる
	属性証明書	△ 証明書の検証が必要	○	× 3rdPKCの秘密鍵の管理に加え属性証明書の管理が接続毎に必要になる
	PKC	× 接続毎にPKCを生成 証明書の検証が必要	○	× 3rdPKCと秘密鍵の管理が接続毎に必要になる

2.2.2. 接続許可情報のデータ形式

接続許可情報のデータ形式として，以下の４つの形式が考えられる．

- 接続許可の情報を加工しない形式(未加工)
- 接続許可の情報に署名を付加した形式(署名付加)
- 接続許可の情報を属性の一部として扱った属性証明書形式(属性証明書)
- 接続許可の情報を含めた PKC 形式(PKC)

3. 提案方式の評価

オンデマンド VPN でデジタル署名方式を使用し IPsec-VPN を構築する方式として，2.2.1と2.2.2で検討した方式の組み合わせによる 8 つの方式を評価した．結果を表 1に示す．相手認証の PKC として 3rdPKC を使用することについては，鍵等に関する情報の増加に伴う管理負担の増加と，2ndPKC を使用した場合でも接続の管理を VPN 管理サーバで行えることから用いないこととした．これを踏まえ表 1の結果から，以下の２つの方式が優れていると考える．

- 2ndPKC で相手認証＋未加工の接続許可情報
- 2ndPKC で相手認証＋署名を付与した接続許可情報

表 1のセキュリティの項目における改ざん検証ができないことについては，以下の理由から改ざんに対するリスクが少ないと考えられる．

- オンデマンド VPN では，認証を行った後に，構成情報を暗号化して配信するため，第三者が通信路上で構成情報を改竄することは困難である．
- 接続許可情報は，受信直後から IKE を実行するまでの短期間でのみ利用されるため，第三者が受信後の接続許可情報を改竄することは困難である．

これらのことから，接続許可情報に対して署名を付加することによる効果は薄いと考えられる．よって，“2ndPKC で相手認証＋未加工の接続許可情報”を実現方式として採用することとした．

4. まとめ

本稿では，オンデマンド VPN でデジタル署名方式を使用した IPsec-VPN を構築するための方式案を複数検討し，評価を行った．評価の結果，“2ndPKC で相手認証＋未加工の接続許可情報”とする方式を採用した．今後は採用した方式を実際にオンデマンド VPN へ適用を行う．

謝辞

本研究は，総務省の平成 18 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」として実施したものである．関係者各位に感謝する．

参考文献

[1] 鴨田浩明，星川知之，山岡正輝，山本修一郎．オンデマンド VPN システムの実装と評価．情報処理学会誌，Vol.47，No.8，pp.2371-2383，August, 2006.

[2] NICSS (the Next generation Ic Card System Study group): 次世代 IC カードシステム研究会 http://www.nicss.or.jp/