オンデマンドVPNシステムの実装と評価

鴨田浩明[†] 星川知之[†]
山岡正輝[†] 山本修一郎[†]

インターネット接続可能な小型端末と無線ネットワークの急速な普及により，いつでもどこからでもインターネット接続可能なユビキタス環境が整備されつつある．また，IPsec 等の暗号化技術を用いた VPN の普及により，安価にセキュアな通信路を構築することも可能である．しかしながら，これらの技術を組み合わせてセキュアなユビキタス環境を実現するためには，不正利用への対策や，機器設定の複雑さ等の課題が残されている．筆者らは，これまでにセキュアなユビキタス環境を実現するための基盤となるオンデマンド VPN システムの研究を実施してきた．オンデマンド VPN システムは IC チップを組み込んだ VPN 機器を利用することにより，厳密なセキュリティを確保した VPN 通信を可能とする．また，ポリシ制御技術と IPsec 構成情報生成技術により，任意の 2 地点間で自動的にオンデマンドに IPsec を用いた VPN 接続を行うことが可能である．本論文では，オンデマンド VPN システムの実装方式およびプロトタイプを用いた性能評価の結果，実証実験による運用評価の結果について報告する．

Implementation and Evaluation of the On Demand VPN System

Hiroaki Kamoda,[†] Tomoyuki Hoshikawa,[†] Masaki Yamaoka[†]
and Shuichiro Yamamoto[†]

The availability of mobile devices and ad-hoc network technology will result in ubiquitous computing. It has also become possible to easily establish a secure network tunnel on the Internet by using encryption technologies such as IPsec. However, there still remain some problems to be solved to realize secure ubiquitous computing and network. For example, we have to develop a technology to prevent an illegal use of the devices and the complex operation to set up network devices should be removed. We have developed the on demand VPN framework, which is able to establish infrastructure for secure ubiquitous network. The on demand VPN system uses tamper-proof chip for the strict device authentication. It is also possible to automatically establish VPN connection between any two points without complex configuration by using the automatic IPsec configuration technology. In this paper we report the implementation and evaluation of the on demand VPN system.

1. はじめに

インターネットを利用可能な携帯電話や PDA 等の小型端末の普及により，いつでもどこからでもネットワークを介したサービスを利用可能なユビキタス環境が整いつつある．また，従来はセキュアな通信路を確保するために高価な専用線の利用が一般的であったが，IPsec [14] 等の暗号化技術を用いた VPN（Virtual Private Network）の普及により，セキュアな通信路を安価に実現することが可能となった．これらの技術を用いることにより，セキュアなユビキタス環境が実現可能となりつつある．

しかしながら既存の技術を用いてセキュアなユビキタス環境を構築するためには，解決しなければならない課題がいくつか残されている．第 1 に，端末の小型化にともない端末の盗難によるなりすましがユビキタス環境では脅威となる．従来よりなりすましの解決策の 1 つとして公開鍵証明書による認証方式が利用されているが，公開鍵証明書の保存された端末自体が盗難にあった場合には，なりすまされる可能性が高くなるという課題がある．第 2 に，VPN 接続を行うために必要な情報を事前に特定することができない点が課題の 1 つとしてあげられる．一般に VPN 接続を行うためには，VPN 通信を行う接続元・接続先双方のネットワーク機器に対して暗号化アルゴリズムや鍵情報等の複雑な設定を事前に行っておく必要がある．これまでは，たとえば会社のネットワークと社員の自宅の端末

† 株式会社 NTT データ
NTT Data Corporation

を接続するといったぐあいに，接続元と接続先機器のIP アドレスや使用する暗号化アルゴリズム等の VPN 接続に必要な情報はある程度既知であることが前提であった．そのため，VPN 接続の設定作業は煩雑ではあるものの，大きな障害とはならなかった．一方で，ユビキタス環境では，接続元と接続先機器の IP アドレスや暗号化アルゴリズム等の VPN 接続に必要となる具体的な情報が事前に特定されているとは限らない．したがって，事前に VPN 接続に必要な情報を通信機器に設定しておくことは不可能である．そこで，任意の 2 地点間で VPN 接続に必要な構成情報を要求に応じて自動的に生成するための技術が必要となる．第 3 に，ユビキタス環境では，接続先や接続元の環境が動的に変化する可能性があるため，従来の IP アドレスによる認証や，ID とパスワードによる認証のみでは不十分であるという課題がある．たとえば，時間帯や位置情報，ユーザの属性情報，端末種別に応じて，柔軟に VPN 接続の可否を制御可能であることが要求される．セキュアなユビキタス環境を構築するためにはこれらの課題を解決する必要がある．

第 1 の課題を解決する方式として，馬場ら[15] は，組織内のネットワークに不正な端末が接続されたことを検知し，自動的に隔離するための方式を提案している．しかしながら，すでに認証されたネットワーク内の端末が不正に持ち出され，外部で悪用されることを防ぐことまではできない．また，第 2 の課題を解決する方式として，たとえば，Bandara ら[1] は，QoS 分野において，KAOS[4] アプローチを応用することにより各ネットワーク機器の構成情報を自動的に導出する手法に関して提案している．しかしながら，VPN の構成情報生成に関しては言及されていない．また，Fu ら[2] は接続元と接続先がネゴシエーションすることにより，IPsec-VPN 構成のための暗号化や認証方式の情報を自動的に生成する方式について提案している．Wang ら[12] は，設定された IPsec のセキュリティポリシの矛盾を検出し，自動的に修正する方式について提案している．しかしながら，どちらの方式も接続元と接続先は既知であるか信頼されている相手であることが前提である．ユビキタス環境では，接続先が未知であっても，相手が信頼できる相手であるかどうかを確認したうえで接続できることが重要であり，これらの方式では対応することが難しい．

筆者らはこれまでにオンデマンド VPN 技術に関する研究開発を実施してきた[13]．オンデマンド VPN 技術は，セキュアなユビキタス環境を VPN 機器が導入されたネットワーク間で実現するための基盤となる技術であり，第 1 の課題を 2 階層 PKI 技術に対応した耐タンパ IC チップによる厳密な機器認証技術により解決する．さらに，第 2 の課題を IPsec 構成情報自動生成技術により，第 3 の課題をポリシ制御技術によりそれぞれ解決する．本論文では，オンデマンド VPN の実装方式およびプロトタイプシステムを用いた性能評価の結果，実証実験での運用評価の結果について報告する．

本論文の構成は次のとおりである．2 章でオンデマンド VPN システムの実装方式について説明する．3 章でオンデマンド VPN システムの利用方法について説明する．4 章でプロトタイプシステムを用いた性能評価結果と運用評価結果および今後の課題について説明する．最後に 5 章でまとめを述べる．

2. オンデマンド VPN システムの実装

2.1 システム構成

オンデマンド VPN は，機器管理サーバ・VPN 管理サーバ・VPN 機器から構成されるシステムである．オンデマンド VPN システムの全体構成を**図 1** に示す．機器管理サーバは VPN 機器の真正性を保証するためのサーバである．VPN 管理サーバは，機器管理サーバに認証された機器による VPN 接続を制御するサーバである．VPN 機器は実際に VPN コネクションを開設する機器であり，一般にはルータが VPN 機器となる．機器管理サーバ，VPN 管理サーバ，VPN 機器の機能構成図をそれぞれ**図 2**，**図 3**，**図 4** に示す．機器管理サーバ・VPN 管理サーバ・VPN 機器間の通信には SSL を用い，機器間の相互認証を行うとともに，送受信するメッセージを盗聴・改ざんから保護する．

オンデマンド VPN システムは，これらのサーバ・機器が協調しセキュアなユビキタス環境を実現するシステムである．オンデマンド VPN システムで実装される主要な技術として 2 階層 PKI 技術，IPsec 構成情報生成技術，ポリシ制御技術がある．次に，これら

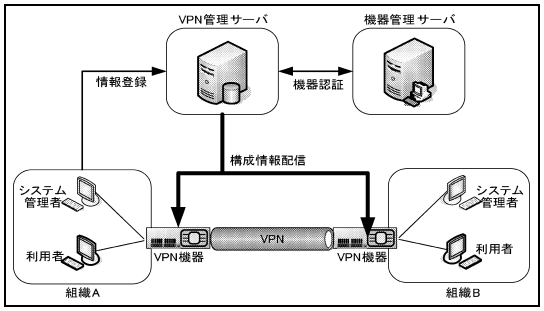


図 1 オンデマンド VPN システム全体構成
Fig. 1 Architecture of the On Demand VPN.

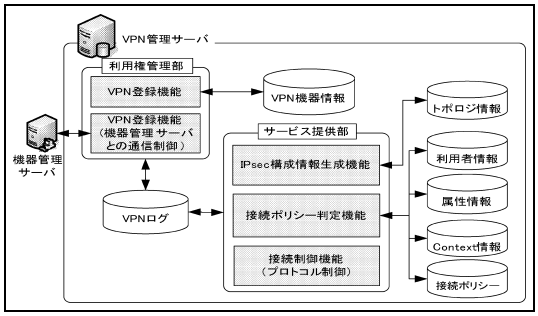


図 2 VPN 管理サーバの機能構成
Fig. 2 Architecture of the VPN management server.

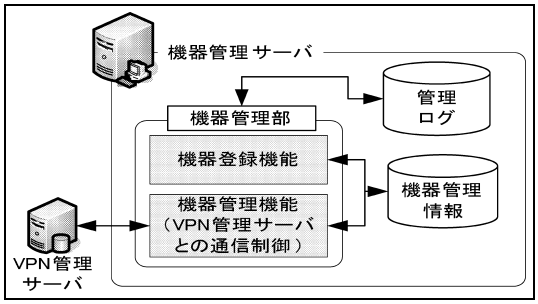


図 3 機器管理サーバの機能構成
Fig. 3 Architecture of the device management server.

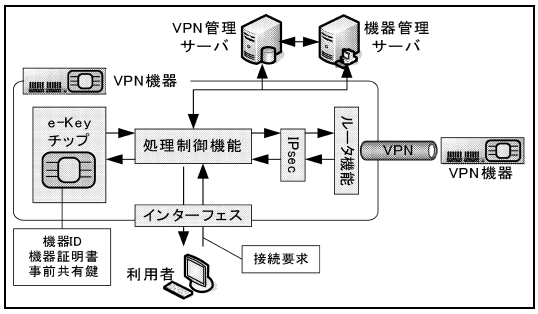


図 4 VPN 機器の機能構成
Fig. 4 Architecture of the VPN device.

の技術と実装方式について説明する．

2.2 2 階層 PKI 技術

オンデマンド VPN システムでは IPsec を用いた VPN を構築する．IPsec ではパケットの暗号化を行うための鍵交換に IKE（Internet Key Exchange）[3] を利用することが一般的である．IKE は相手認証，SA（Security Association）の折衝と管理，共有秘密鍵管理等を行うプロトコルであり，暗号化を行うための鍵交換を行うこともできる．従来，IKE を行うために必要となる情報を，VPN 接続を行う相互のルータに事前に設定しておく必要があった．そのためこれらの情報が漏洩すると機器のなりすましが可能となり，機密情報の漏洩につながるという危険性があった．そこで

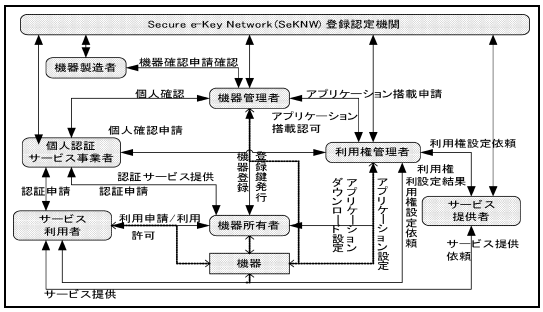


図 5 Secure e-Key Network（SeKNW）フレームワーク
Fig. 5 Secure e-Key Network (SeKNW) framework.

オンデマンド VPN システムでは，IPsec による VPN 接続に必要な情報を VPN 管理サーバで一元的に管理し，利用者の要求に応じて VPN 機器に配信するセンタ型システムとすることで事前にルータに情報を設定しておくことを不要とした．また，耐タンパデバイスである e-Key チップを VPN 機器に組み込むことにより，機器のなりすましを防止するとともに，初めてデータをやりとりする相手とも安全な通信を行うことを可能にした．本節では e-Key の仕組みについて説明する．

e-Key チップは Secure e-Key Network（SeKNW）のフレームワークの中で情報流通機器に内蔵された状態で販売されることを前提とされている．SeKNW は 2 階層 PKI 技術をベースとした IC チップの管理運用モデルの 1 つであり，NICSS フレームワーク[6] を参考に策定されたものである．SeKNW のフレームワークを**図 5** に示す．2 階層 PKI 技術は，1 階層目の PKI を利用して e-Key チップ発行後でも自由にアプリケーションを発行・設定し，各チップアプリケーションが独自に 2 階層目の PKI を利用してサービスを提供できる等，サービス間のセキュリティを保ちながら幅広いサービスが提供可能な技術である．オンデマンド VPN では，1 階層目の PKI 情報を VPN 機器の認証のために，2 階層目の PKI 情報を VPN サービスの利用権認証のためにそれぞれ利用することにより，安全性の高いサービスを容易に実現することを可能とした．

2.3 IPsec 構成情報生成技術

オンデマンド VPN システムは VPN 管理サーバ上で VPN 接続に必要となる IPsec 構成情報を登録情報と VPN 接続要求に含まれる情報から動的に生成・配信することにより，VPN コネクションを構築する．オンデマンド VPN では IPsec の暗号化処理に Linux 上で動作可能な FreeS/WAN [5] を利用することとした．VPN 管理サーバ上で構成し VPN 機器に配信しなけ

ればならない IPsec 構成情報は大きく 4 つある．以下にそれぞれについて説明する．

(1) **セキュリティポリシーデータベース（SPD）**：SPD は，IPsec による暗号化処理対象パケットを選別するための情報が記述されたデータベースであり，VPN 機器から VPN 管理サーバへ通知された IP アドレスを元に生成・配信する．具体的には，VPN 機器の配下に存在する VPN 接続要求を行った利用者端末の IP アドレスと，VPN 接続要求先端末の IP アドレスが記述された SPD を生成する．VPN 機器は，パケットを受信するごとに SPD を検索し，そのパケットが暗号化の対象となるパケットであるか否かの判定を行う．オンデマンド VPN では，SPD により明示的に暗号化が指定されたパケットのみを暗号化処理の対象とする．配信された情報は ipsec.conf の中に記述される．

(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 を生成するために必要となる情報である．たとえば，認証方式や暗号化アルゴリズム，SA の有効期間等の情報が含まれる．FreeS/WAN の場合 IKE で使用するアルゴリズムは変更できないため，ipsec.conf に記述するべき情報をサーバ内に静的に設定しておき，接続要求があった場合に，IPsec 動作設定情報を生成・配信する．

(3) **事前秘密共有鍵**：オンデマンド VPN では IKE を行う際の認証方式として事前共有秘密鍵方式を用いる．そのために必要となる鍵は，VPN 管理サーバで接続要求ごとに乱数を用いて新規に作成され，SSL 経由で VPN 機器の e-Key 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鍵は VPN 機器どうしが VPN 接続を行っているときにしか知りえないようにしている．

(4) **ルーティングテーブル**：ルーティングテーブルは IP パケットの経路情報を記述したものである．VPN 接続の相手先への IP パケットが，適切な暗号通信路を経由するように VPN 管理サーバがルーティングテーブルを生成し，各 VPN 機器に配信する．配信された情報は iptables.conf に反映される．

VPN 管理サーバの IPsec 構成情報生成に関する機能構成図を**図 6** に示す．IPsec 構成情報生成技術により，事前に VPN 接続に必要となる情報を VPN 機器に設定することなく，オンデマンドに VPN 接続を実現することが可能となる．

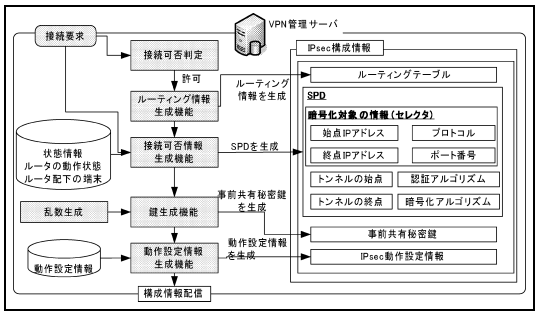


図 6 IPsec 構成情報生成処理
Fig. 6 Building IPsec configuration.

2.4 ポリシ制御技術

VPN 接続により，本来ファイアウォール等によりアクセスが制限されているローカルネットワークに外部から接続することが可能となる．従来，企業等が VPN を構築する場合，VPN サービスを利用するのはその企業の社員であることが前提であり，IP アドレスや ID 等による情報から個人を特定することができた．そのため，IPsec のアクセス制御を行う Security Policy Database（SPD）や RADIUS 等の技術を用いることで，セキュリティを保つことが可能であった．しかしながら，オンデマンド VPN システムでは VPN 接続を実現するために必要な接続元・接続先の IP アドレスや ID 等の情報が事前に特定されていないことが前提となる．そのため，従来のように VPN 接続を制御する情報を SPD や RADIUS サーバに事前に静的に設定しておくことは不可能である．つまり，IP アドレスやユーザ ID 等のように特定の端末やユーザ固有の情報ではなく，相手の組織名や接続する端末の種別・時間帯・ユーザの属性情報といった単位でアクセス制御を実現可能であることがセキュリティ確保のために必要となる．VPN 管理サーバは，VPN 機器が利用されている組織名や VPN 機器が設置されている場所の情報を管理している．さらに VPN 機器は，VPN 接続要求を行った端末の種別やユーザの属性情報を取得することが可能である．端末種別の例として，事務用 PC・モバイル機器・医療用機器等が，ユーザ属性の例として，医師・看護師・医療スタッフ等がある．オンデマンド VPN では，これらの VPN 管理サーバや VPN 機器が取得可能な情報を用いて VPN の接続を制御することを可能にするため，XACML[7] を用いたアクセス制御技術の実装を行った．

XACML は OASIS で標準化されている XML を用いた次世代のアクセス制御記述言語であり，粒度の異なる種々の情報に基づいてアクセスの許可・禁止を宣

```
<Policy Policy ID="001"
   RuleCombiningAlgId="First Applicable">
  <Target>
   //VPN 接続元，VPN 接続先，日時条件の指定
  </Target>
  <Rule RuleId="rule001" Effect="Permit">
  <Target>
   <Subjects>
    <Subject>(VPN 接続元の情報)</Subject>
   </Subjects>
   <Resources>
    <Reource>(VPN 接続先の情報)</Resource>
   </Resources>
   <Actions>
    <Action>"VPN 接続"</Action>
   </Actions>
  </Target>
  <Condition>
   (日付・曜日・時間帯条件)
  </Condition>
 </Rule>
</Policy>
```

図 7 XACML ポリシの構造
Fig. 7 Structure of XACML policy.

言することができる汎用的な言語である．XACML に記述する主な要素として Subject・Resource・Action・Condition がある．オンデマンド VPN システムでは，Subject に “VPN 接続元の情報” を定義し，Resource に “VPN 接続先の情報” を定義する．そして Action には “VPN 接続” のみを定義する．Condition は “接続可能な日付・曜日・時間帯” の条件を記述するために用いる．オンデマンド VPN システムの接続制御に用いる XACML ポリシの構造を**図 7** に示す．XACML を利用することにより，たとえば，ある組織の特定のマシンを使ってユーザ A が接続する場合のみ接続を許すといった限定的なポリシから，5:00〜6:00 までの VPN 接続はすべて禁止するといった大局的なポリシまでを容易に定義することが可能となる利点がある．また，XACML ポリシは標準化されている言語であり，他システムとの相互運用性が高いという利点もある．

セキュリティを厳密に確保するためにネットワーク管理者は，自ネットワークへの VPN 接続を制御するだけではなく，自ネットワークから外部への VPN 接続を制御することも必要となる．これは，自ネットワークの端末が，セキュリティの確保されていない外部ネットワークに VPN 接続することによりウィルスに感染したりすることを防ぐためである．そのためオンデマンド VPN では，発信用と受信用の 2 つの VPN 接続ポリシをネットワーク管理者が設定できるようにしている．発信用ポリシには，自ネットワークから他ネットワークへの VPN 接続の可否に関するポリシを定義する．受信用ポリシには，他ネットワークから自ネットワークへの VPN 接続の可否に関するポリシを定義する．VPN 接続の要求が発生してから VPN 接続の可否が判定されるまでの処理の流れを**図 8** に示す．たとえばネットワーク A に所属する端末 a からネットワーク B に所属する端末 b へ VPN 接続を行う場合を考える．最初に端末 a は端末 b に対する VPN 接続要求を VPN 管理サーバに送信する．VPN 管理サーバは受信した情報からポリシ照合に必要となる XACML 要求コンテキストを生成する．要求コンテキストとは XACML 形式のリクエスト文であり，接続要求を送信した接続元の情報と接続先の情報が記述されている．最初に，生成された要求コンテキストとネットワーク A の発信用ポリシとを照合する．照合の結果，接続許可となった場合には，接続元情報と接続先情報を入れ替えた要求コンテキストを再度生成しネットワーク B の受信用ポリシと照合する．照合の結果，接続許可となった場合には，端末 a から端末 b への VPN 接続が許可される．どちらか一方の照合で接続不許可となった場合には VPN 接続は許可されない．

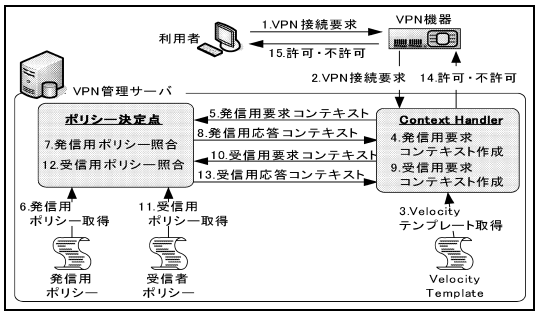


図 8 XACML ポリシ判定処理
Fig. 8 Flow of the XACML policy matching.

オンデマンド VPN システムのポリシ制御機能を実装するにあたり，ポリシの可否判定エンジンには SUN の公開している Sun's XACML Implementation [10] を利用した．ただし，プロトタイプシステム開発時点で，当該エンジンが曜日に関する情報を扱うことができなかったため，Condition に曜日が含まれている場合に正しくポリシの照合が行えるように拡張を行った．また，VPN 機器から受信した VPN 接続要求から発信用要求コンテキストおよび受信用要求コンテキストを生成するために，テンプレートエンジンである Velocity [11] を利用することにより実装を簡略化した．

3. オンデマンド VPN システムの利用方法

本章ではオンデマンド VPN システムの利用方法について説明する．オンデマンド VPN システムを利用するためには，大きく事前準備フェーズと利用フェー

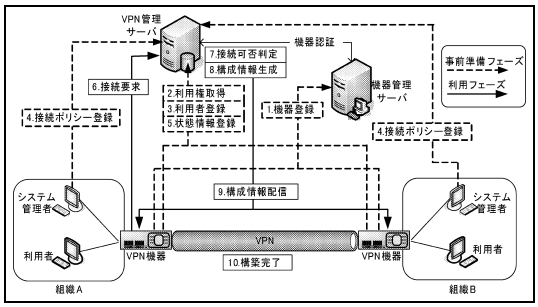


図 9 オンデマンド VPN システム構成図
Fig. 9 Architecture of the On Demand VPN System.

ズの 2 つのフェーズが必要となる．事前準備フェーズはオンデマンド VPN サービスを利用するために必要な環境を構築するフェーズであり，利用フェーズは構築された環境を利用してオンデマンド VPN サービスを利用するフェーズである．**図 9** にその概要を示す．以下に図 9 を用いて利用手順について説明する．

3.1 事前準備フェーズ

オンデマンド VPN システムを利用するためには，事前に SeKNW 登録認定機関により認可された製造者が製造した VPN 機器を利用する必要がある．VPN 機器には e-Key チップが搭載されており，機器の製造者が VPN 機器製造時に e-Key チップ内に正当な機器であることを証明するための仮の公開鍵証明書を保存しておく．次にオンデマンド VPN システムを利用する利用者が所属するネットワークのシステム管理者がこの VPN 機器を購入し，オンデマンド VPN システムを利用するための登録・設定を行う必要がある．VPN 機器の登録までの処理が事前準備フェーズとなる．事前準備フェーズで登場する各プレイヤの役割を **表 1** に示し，事前準備フェーズの詳細を以下に記述する．

(1) **機器登録**：SeKNW 登録認定機関より認定された VPN 機器管理者の管理するサーバを機器管理サーバとする．最初に VPN 機器所有者は VPN 機器を用いて機器管理サーバにアクセスし，VPN 機器の登録を行う．VPN 機器管理サーバは，事前に VPN 機器の e-Key チップ内に保存された仮の公開鍵証明書を用いて VPN 機器の認証を行う．認証後 VPN 機器と機器管理サーバ間で正式な公開鍵証明書・秘密鍵を作成し，チップ内の仮の証明書と置き換える．これらを 1 階層目の PKI 情報と呼ぶ．その後機器管理サーバは，VPN 機器から送信された VPN 機器の設置場所や所属組織等の機器情報およびシステム管理者の情報登録を行う．機器情報を登録することにより機器の盗難によるなりすましを防止することが可能となる．

表 1 オンデマンド VPN のプレイヤ
Table 1 Players of the On Demand VPN.

VPN 機器管理者	VPN 機器に搭載された e-Key チップ上の資源を管理する
VPN 機器所有者	e-Key チップを搭載した VPN 機器を所有・管理する
VPN サービス提供者	オンデマンド VPN サービスを提供する
サービス利用者	オンデマンド VPN サービスを利用する
システム管理者	オンデマンド VPN サービスの利用申請・利用者登録等を行う
VPN 利用権管理者	VPN サービスを利用するためのアプリケーションと利用権の発行・管理を行う

(2) **利用権取得**：次に，システム管理者は VPN サービス提供者に VPN サービスの利用申請を行う．VPN 利用権管理者は VPN 機器管理者にチップアプリケーションの搭載許可を得る．そして，VPN 機器管理者によって構築されるセキュアチャネルを用いて VPN サービス利用のためのチップアプリケーションを e-Key チップ内にダウンロードし 2 階層目の PKI 情報を保存する．

(3) **利用者登録**：システム管理者は実際に VPN サービスを利用する VPN 利用者情報を VPN 管理サーバへ登録する．VPN 管理サーバは 2 階層目の PKI 情報を用いて VPN 機器を認証し，送信されてきた利用者の ID/パスワード等の情報を登録する．

(4) **接続ポリシ登録**：システム管理者は，VPN 利用者が VPN 接続を行うことを許可・禁止する相手先情報，および自ネットワークへの接続を許可・禁止する相手先の情報をそれぞれ受信用ポリシ・発信用ポリシとして登録する．

(5) **状態情報登録**：VPN 機器は，VPN 機器自身と VPN 機器配下に存在する VPN サービスを利用する端末の IP アドレスや端末種別等の状態情報を取得する．VPN 機器は VPN 管理サーバへ状態情報を通知し，VPN サーバはこの情報をデータベースへ登録する．登録された状態情報は公開され VPN 接続先を選択する際に利用される．

3.2 利用フェーズ

事前準備フェーズで登録された情報を元に，VPN 接続を行うのが利用フェーズである．VPN サービスを利用したい VPN 利用者が VPN 管理サーバに VPN 接続の要求を行ってから，VPN が構築されるまでのフェーズが利用フェーズの対象である．下記の (6)〜

(10) に利用フェーズの詳細を記述する．

(6) **接続要求**：オンデマンド VPN 利用者は接続したい VPN 機器を選択し接続要求を行う．オンデマンド VPN 機器は利用者の要求に対して VPN 管理サーバへ接続を行い 2 階層目の PKI 情報による利用権認証を実施したうえで，接続先検索の機能を提供する．接続先の情報は事前準備フェーズで登録された状態情報から取得する．

(7) **接続可否判定**：VPN 管理サーバは接続要求と接続ポリシを照合し，要求された VPN 接続が許可される要求か禁止される要求かを判定する．接続が禁止される場合には，VPN の構築作業を中止する．

(8) **構成情報生成**：接続が許可される場合には，状態情報と利用者の接続要求から VPN 構成に必要となる IPsec 構成情報と，IKE 用の事前共有秘密鍵を生成する．

(9) **構成情報配信**：VPN 管理サーバから構成情報と事前共有秘密鍵を接続要求元・要求先それぞれの VPN 機器へ配信し，搭載されている e-Key チップへ格納する．

(10) **構築完了**：受信した構成情報と事前共有秘密鍵を用いて IKE を実行し，VPN を構築する．以降，接続元と接続先は開設された VPN を経由した通信が可能となる．VPN 通信完了時には切断要求をあげ VPN コネクションを破棄する．

4. オンデマンド VPN システムの評価

2 章で説明した各機能を実装した機器管理サーバ・VPN 管理サーバ・VPN 機器のプロトタイプをそれぞれ作成した．機器管理サーバと VPN 管理サーバの各機能は Red Hat Enterprise Linux ES 上で実装を行った．また，Linux カーネルを搭載し e-Key チップを内蔵したルータを開発し，VPN 機器として利用した．VPN 管理サーバには管理者が VPN の接続状況を監視することができるための VPN 接続ビューワ（**図 10** 参照）を実装した．さらに，VPN 機器には VPN 利用者が接続要求を行うことができるようにするための Web アプリケーションを実装した．接続要求アプリケーションは，VPN 管理サーバと連携し VPN 接続先として登録されている機器を自動的に取得することにより，VPN 利用者がブラウザから接続先を選択し容易に VPN 接続要求を行うことを可能にする．これら一連のプロトタイプを用い，利用フェーズにおける性能評価として VPN 接続時間の評価・VPN による転送効率の評価・ポリシ制御技術の評価を実施した．

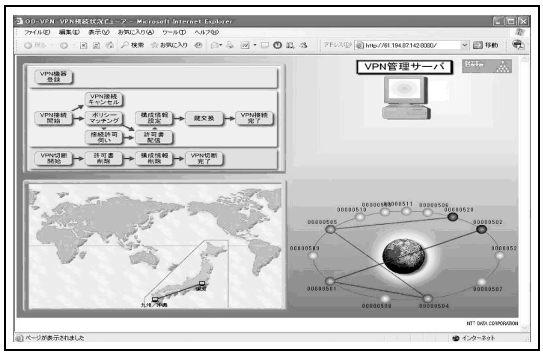


図 10 VPN 管理サーバ画面
Fig. 10 VPN management viewer.

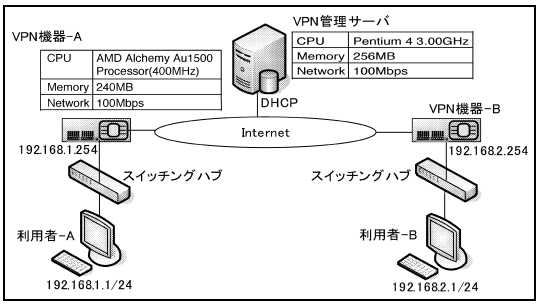


図 11 VPN 接続時間測定実験環境
Fig. 11 Test bed network for time measurement.

さらに，フィールド評価を実施し事前準備フェーズおよび利用フェーズの利便性評価を実施した．本章ではこれらの評価内容と結果・考察について記述する．

4.1 VPN 接続時間の評価

本節では，VPN 接続時間の評価方法と結果・考察について述べる．評価を行った実験環境を**図 11** に示す．図 11 において VPN 機器-A と VPN 機器-B は同じ性能である．開発したプロトタイプにより VPN が接続されるまでに必要とする時間を評価するために，以下の項目 (1)〜(4) に関して VPN 接続に必要な手順ごとに処理に要する時間をそれぞれ測定した．VPN 接続の手順と各項目の関係を**図 12** に示す．

(1) **ユーザ側応答時間**：利用者-A が VPN 機器-A に接続し，利用者-B の端末への VPN 接続開始ボタンを押下してから VPN 接続確認ダイアログが表示されるまでの時間．

(2) **ルータ側応答時間**：VPN 管理サーバ上で VPN 接続要求を受信してから VPN 接続完了通知を返信するまでの時間．

(3) **VPN 接続元への構成情報配信時間**：VPN 管理サーバが接続元の VPN 機器に対して，IPsec 構成情報配信を開始してから，VPN 機器で構成情報が設定され，構成情報設定完了通知を受信する

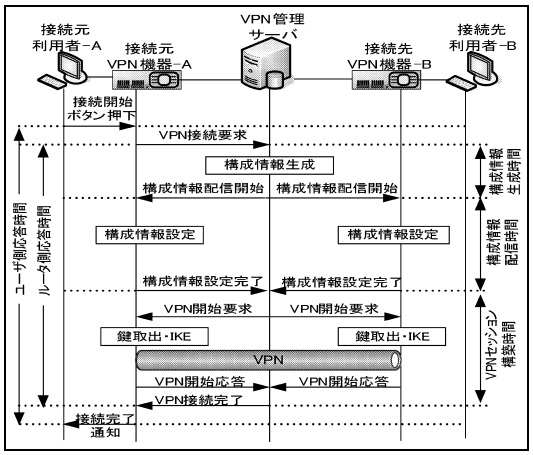


図 12 VPN 接続手順
Fig. 12 Flow for the VPN connection establishment.

までの時間.

(4) **VPN 接続先への構成情報配信時間**：VPN 管理サーバが接続先の VPN 機器に対して，IPsec 構成情報配信を開始してから，VPN 機器で構成情報が設定され，構成情報設定完了通知を受信するまでの時間.

VPN 接続要求を開始してから VPN 接続が完了するまでの処理を 10 回実施し，それぞれの処理に要した時間を計測した．実験結果を**図 13** に示す．ルータ側応答時間は，10 回中 8 回は約 15.8 秒，2 回は約 25.9 秒と測定結果にばらつきが生じた．応答時間のばらつきの原因を調査した結果，今回のプロトタイプに使用した FreeS/WAN の IKE の実装方法に原因があることが明らかとなった．FreeS/WAN の実装では，接続処理を頻繁に行うと IKE のネゴシエーション時にリトライ処理が発生する．このことが計測時間のばらつきの原因となっていた．リトライの間隔と回数は，FreeS/WAN の設定ファイルで変更可能であり，調節することにより処理に要する平均時間を短縮することが可能であると考えられる．

リトライ処理が発生しなかった場合の各処理ごとの平均処理時間と，ユーザ側応答時間を 1 とした場合の平均処理時間比率を**図 14** に示す．実験の結果，リトライ処理がない場合の VPN 接続処理に要するユーザ側応答時間は平均で約 18 秒であった．また，VPN 管理サーバで VPN 接続要求を受信してから構成情報の配信を開始するまでの構成情報生成時間，VPN 接続元への構成情報配信時間と VPN 接続先への構成情報配信時間の平均である構成情報配信時間，VPN 機器がチップから鍵情報を取り出し IKE のネゴシエーションにより VPN 接続が完了するまでの VPN セッション構築時間は，それぞれ平均で 4.1 秒，6.4 秒，5.3 秒であった．

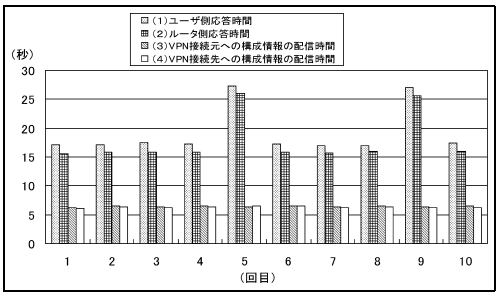


図 13 VPN 接続時間測定結果
Fig. 13 Time measurement result of VPN connection.

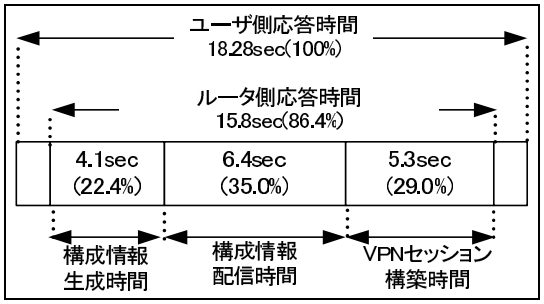


図 14 各処理ごとの VPN 接続時間比率
Fig. 14 Time ratio of the flow for VPN connection.

オンデマンド VPN の利用例として 4.4 節で後述する医療現場での遠隔診療等が想定される．たとえば遠隔診療を行う場合の VPN 接続利用時間は数十分から数時間である場合が一般的である．今回の実験により得られた VPN 接続時間は，VPN 接続利用時間と比較して相対的に十分小さい．したがって遠隔診療を行う場合には，VPN 接続時間の実運用上の影響は少ないと考えられる．しかしながら，たとえば外出先からメールチェックのみを行うために VPN を利用する場合には，その利用時間は数十秒から数分である．したがって VPN 接続に 18 秒を要するシステムが利便性に与える影響を無視することはできず，適用分野によっては接続時間の改善が必要である．

4.2 VPN による転送効率の評価

医療分野では遠隔病理診断のために顕微鏡画像の送受信が行われる．正確な診断のためには，マルチスペクトル顕微鏡を用いて撮影された高精細の大容量画像データを扱うことが必要となる．そこで，オンデマンド VPN システムを導入することにより，大容量データの送受信時の転送効率にどの程度の影響が発生するかを実験により評価した．実験では 2 拠点間で 150 MByte の顕微鏡画像を転送した場合の転送速度

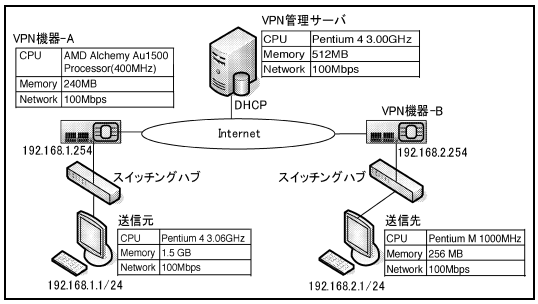


図 15 大容量画像データの転送実験環境
Fig. 15 Test bed network for huge data transportation.

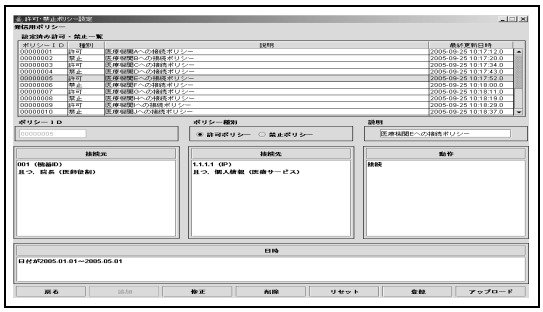


図 17 接続ポリシ登録 GUI
Fig. 17 GUI for the policy definition.

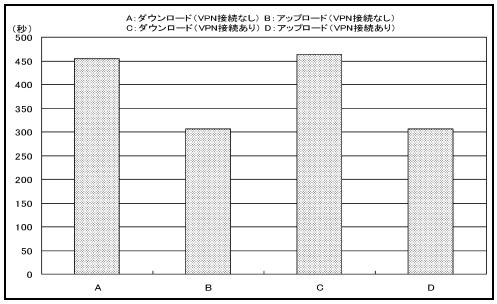


図 16 大容量画像データの転送実験結果
Fig. 16 Time measurement result of huge data transportation.

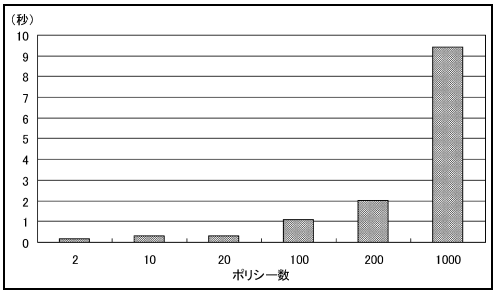


図 18 接続ポリシ可否判定時間
Fig. 18 Time measurement result of policy analysis.

を計測した．オンデマンド VPN の影響を計測するため，VPN 接続を行わない場合の通常通信によるダウンロード・アップロードに要する時間，VPN 接続を行った場合のダウンロード・アップロードに要する時間をそれぞれ測定した．実験環境を**図 15** に，実験結果を**図 16** にそれぞれ示す．

実験結果よりオンデマンド VPN を利用せずにデータを転送するために要した時間と，オンデマンド VPN を利用してデータを転送するのに要した時間はほぼ同一であることを確認することができた．したがって，オンデマンド VPN システム利用の有無はデータの転送効率にほとんど影響を与えないといえる．今回の実験により，オンデマンド VPN システム導入によるデータ転送効率の低下は無視できるほど小さく，大容量データの送受信を行う医療現場への導入に問題がないことを確認することができた．

4.3 ポリシ制御技術の評価

本節では，ポリシ制御技術の性能評価方法とその結果・考察について述べる．ポリシ制御技術の性能を測定するため，登録されたポリシの数に応じて利用フェーズにおける接続可否判定に要する時間がどのように変化するかを評価した．なお，接続ポリシを定義するための専用のアプリケーション（**図 17**）を開発し，GUI を用いて簡単に XACML ポリシを VPN 管理サーバに登録できるようにした．

VPN 管理サーバに同数の接続元ポリシと接続先ポリシを登録し，VPN 管理サーバが接続要求を受信してから可否判定が完了するまでの時間を計測した．実験環境は図 15 と同一である．VPN 管理サーバでは 1 つのポリシを 1 つのファイルとして管理している．今回の評価では，1 つのポリシの中に，単一の Subject・Resource・Action の情報をそれぞれ記述し，可否判定に要する時間を計測した．計測結果を**図 18** に示す．図 18 において，横軸のポリシ数は接続元ポリシと接続先ポリシの合計数を示している．

実験では，VPN 管理サーバが VPN 接続要求を受信してから接続可否判定が完了するまで，ポリシ 1 つあたり約 0.01 秒要することを確認した．つまり接続制御を行うべき接続元・接続先の情報が合計で 100 個程度の小規模環境である場合には，可否判定に要する時間は 1 秒程度であり，十分に実用的であると考えることができる．一方で，登録されるポリシの数が数千個になる大規模環境では，可否判定に数十秒必要であり，可否判定処理の性能向上が課題となる．

今回の実装では，可否判定エンジンの制約により，1 ポリシを 1 ファイルとして管理する方式とした．エンジンの改良を行い，複数ポリシを単一ファイルで管

理できるよう改善することにより，判定時間を短縮することができると考えられる．

4.4 フィールド評価

開発したプロトタイプを沖縄県の 10 カ所の医療機関に実際に導入し，テレパソロジーシステム[9] を用いた遠隔診療を行う実証実験を実施した．本節では，実環境でオンデマンド VPN システムを利用するための運用上の課題について考察する．

4.4.1 実証実験概要

医療分野では近年テレパソロジーシステムが導入されている．テレパソロジーシステムは通信ネットワークを通じて体組織の画像や顕微鏡の映像を送受信し，遠隔地の病理医が診断を下せるようにする遠隔病理診断システムである．テレパソロジーの運用形態には同期接続型と非同期接続型の 2 種類ある．同期接続型は，2 地点でリアルタイムに画像データ等をやりとりして遠隔診断を実施する形態である．非同期接続型とは，遠隔診断に必要なデータをいったんサーバ上に保管し，そのデータを別の医師が読み取ることで診断を行う形態である．

テレパソロジーシステムで送受信されるデータは患者の診断データ等であり，その運用には高度の安全性が求められる．そのため，テレパソロジーシステムを導入している医療機関どうしには専用線を利用した VPN が開設されていることが一般的である．しかしながら，専用線の維持コストは高く，地方等の小規模医療機関でのテレパソロジーシステム導入の大きな障壁となっている．一方でオンデマンド VPN システムは，一般のインターネット網を利用してセキュアな通信路を確保することが可能であり，コストを低く抑えることが可能である．そこで筆者らは，開発を行ったオンデマンド VPN システムを利用することにより，低コストで安全にテレパソロジーシステムが利用できることを確認するために，実際の医療機関にて実証実験を行った．

今回の実証実験では，沖縄県の 10 カ所の医療機関にオンデマンド VPN 機器を設置し，テレパソロジーシステムをオンデマンド VPN システムを通じて利用するための課題を検証した．VPN 管理サーバ・機器管理サーバ・非同期接続用テレパソロジーシステムサーバは東京に設置し実験を実施した．実証実験のネットワーク構成を**図 19** に示す．各医療機関およびセンタは，インターネット網に一般の光ファイバ回線・ADSL 回線を経由して接続されている．

4.4.2 実証実験評価結果

実証実験では，インターネット回線の開設から VPN 機器の設置作業までのシステム設置に関わる評価と，VPN 機器の設定からオンデマンド VPN システム上でのアプリケーション利用までのシステム運用に関する評価を実施した．前者の評価では，事前準備フェーズに必要な作業を実環境において短期間かつ容易に実施可能であるかを中心に評価した．後者の評価では，利用フェーズに必要な作業をエンドユーザが容易に実施可能であるかを中心に評価した．評価方式はアンケートおよびヒアリング調査による評価であり，実運用上のオンデマンド VPN システムに関する課題を明確にした．以下に示す (1)〜(4) が事前準備フェーズで必要となった作業と明らかになった課題であり，(5)〜(7) が利用フェーズで必要となった作業と明らかになった課題である．

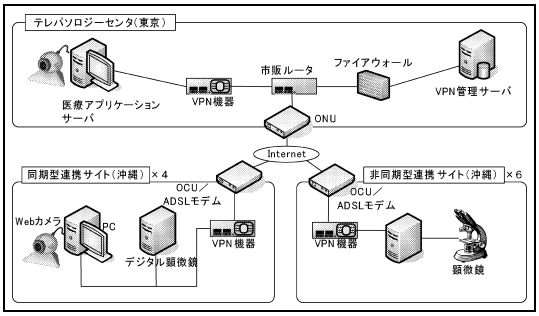


図 19 実証実験ネットワーク構成
Fig. 19 Network for the medical field test.

(1) [インターネット回線開設]：テレパソロジーシステムで送受信されるデータは画像データが主であり，大容量のインターネット回線が必要となる．したがって実証実験では 10 の医療機関すべてに光ファイバ回線を開設することを目標とした．しかしながら，局舎との距離等の制約により光回線の開設が可能な医療機関は 2 カ所のみであり，8 カ所は ADSL 回線で代用した．申し込みから開設までの期間は ADSL が 1〜2 週間程度であったのに対し，光回線の開設には 1 カ月程度を要した．ユビキタス環境の利用促進に向け光回線インフラの普及と開設時間短縮の必要性が明らかとなった．

(2) [利用施設内の回線敷設]：県立の医療機関では，敷設工事を行うために県の認可が必要となる．今回の実証実験では迅速に認可がおりず工事を開始できないケースが発生した．敷設工事に際し事前に関係機関と連携を密にする重要性が認識された．また屋内配線の工事が必要なケースもあり，利用者と施設担当者間の連携も必要となる．

(3) [VPN 機器設置]：オンデマンド VPN ルータの設置作業は通常の通信機器の設置業務と異なる

技術的技能や知識を要求されるものでない．アンケートでは 100%の利用者が，VPN 機器設置作業が容易であると回答した．

(4) ［VPN 機器設定作業］：今回の実証実験では VPN 機器登録作業・利用者登録作業を開発者が実施した．実際に利用者が作業を行うためには，手続きのマニュアル化が必要であると認識した．ただし登録作業は Web ベースで容易に行うことが可能であり，既存の IPsec 設定のように高度なネットワーク知識や機器の知識は不要である．

(5) ［VPN 接続開始］：VPN 接続開始要求は Web システムを用いて容易に行うことが可能である．アンケートでは 100%の利用者が VPN 接続のための作業は容易であると回答した．

(6) ［アプリケーション利用時］：VPN 接続完了後は，テレパソロジーアプリケーションから VPN 機能は遮蔽され意識する必要がない．20%の利用者から「本当に通信が暗号化されているか不安」という回答を得た．VPN 接続状況を可視化して表示することがユーザに安心感を与える意味で重要であると認識した．また，80%の利用者が VPN 接続の利用時間が 1 時間程度と回答した．

(7) ［VPN 切断］：アプリケーションと VPN システムは独立して機能しているため，アプリケーション終了時に VPN 切断を明示的に実施しないと VPN が接続されたままの状態になる．アンケートでは 20%の利用者がアプリケーションと VPN の接続・切断を同期させる必要があると指摘した．

評価の結果，オンデマンド VPN システム利用の前提となるインターネット回線の施設に長期間要するケースがあるものの，事前準備フェーズの作業自体は実環境でも容易に実施可能であることが明らかとなった．利用フェーズにおいては，GUI の改善が一部必要であるものの，オンデマンド VPN サービスを利用する作業をエンドユーザが容易に実施可能であることが明らかとなった．以上により，オンデマンド VPN システムは実環境においても有効なシステムであると考えることができる．

4.5 評価のまとめと今後の課題

本章では，オンデマンド VPN システムプロトタイプを用いて，4 つの観点から評価を実施した結果について説明した．VPN 構築に関する評価では，VPN 回線が構築されるまでに約 18 秒かかることを確認した．VPN 転送効率の評価では，オンデマンド VPN システムを利用することによるデータ転送効率への影響が端末 1 台の場合には無視できるほど小さいことを確認した．ポリシ制御技術の評価では，小規模環境において適切なアクセス制御が十分に短い時間で実現できていることを確認した．フィールド評価では，医療機関にオンデマンド VPN システムを導入することにより，実際の現場での利用が可能であることを確認した．

一方で，それぞれの評価でいくつかの課題があることも明らかになった．以下に評価により明らかになった課題を示す．

(1) **VPN 構築時間に関する課題**：IKE のリトライ回数と時間を調節することにより VPN 構築までの接続時間を短縮することを検討する必要がある．また VPN の利用形態に応じては現在の構築に要する時間を短縮する必要がある．

(2) **VPN 転送効率に関する課題**：複数端末が同時接続を行った場合やインターネットのトラフィック量が，オンデマンド VPN システムの転送効率にどのような影響を及ぼすかを調査する必要がある．

(3) **ポリシ制御技術に関する課題**：VPN 利用者が増加するにつれ，必要となる接続ポリシの数が飛躍的に増加する可能性がある．したがって現状のポリシ制御技術の可否判定処理能力を向上させることが必要である．また，現在の XACML では単独の接続要求を判定することのみが可能であり，他の VPN 接続状況に応じた動的な可否判定を行うことができない．オンデマンド VPN の利用者が増加するに従い回線が混雑し，QoS 制御が必要になると考えられる．そのため，他の接続状況に応じて可否判定の結果を動的に変更することを可能にするポリシの記述方式について検討を行うことが必要である．

(4) **実証実験に関する課題**：今回の実証実験は実施期間が短く，必ずしも十分な評価結果を得ることができていない．今後継続して実証実験を行い，システムのメリット・デメリット・改善事項等を明らかにする予定である．

5. おわりに

本論文では，セキュアなユビキタス環境を実現するための基盤となるオンデマンド VPN システムの実装方式と評価結果について示した．オンデマンド VPN システムは 2 階層 PKI 技術を実装した耐タンパ IC チップによる厳密な機器認証を行うことにより，オンデマンドに安全な通信を実現することを可能にする技術である．本提案システムでは XACML ポリシによる接続可否判定が可能であり，様々な粒度のアクセス制御を容易に実現することが可能である．さらに，複雑

なIPsecのVPN構成情報の生成から各機器への設定までを自動的に行うことが可能であり，従来のVPN構築作業と比較して管理者の作業を大幅に低減することが可能である．プロトタイプを用いた評価の結果，VPNの開設が短時間で完了し，VPN開設後は通常の通信と変わらない転送効率でデータの送受信が可能であることを確認した．また実証実験を通じて，オンデマンドVPNシステムが実環境でも利用可能であることを確認するとともに，運用上の課題を明確にした．

今回開発したプロトタイプを用いた評価では，接続時間の短縮やポリシ制御技術に関する技術上の課題と，実環境での運用上の課題があることを確認した．今後これらの課題を解決するための方式について検討を実施する予定である．また，今回の評価では問題とならなかったが，拠点間をVPNで接続する場合には，同一のアドレス体系で構成されるローカルエリアネットワーク間をVPN接続することができないという課題もある．CIPA[16]やSTUN[8]では，同一アドレス体系間のローカルエリアネットワーク間での相互通信を実現する方式が提案されている．今後これらの技術をオンデマンドVPN機器に実装することにより，同一アドレス空間どうしでのVPN接続を可能にする予定である．また，テレビ会議を行う場合等は1つのVPN機器から同時に多地点のVPN接続を行うことが必要となる．そのため，多地点接続を行った場合の性能評価を今後実施する予定である．

謝辞 本研究は，総務省の平成17年度「高度ネットワーク認証基盤技術の研究開発」の委託を受けた「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．また実証実験に協力してくださった東京工業大学の大山永昭教授，小尾高史助教授，鈴木裕之助手，ピッツバーグ大学メディカルセンターの八木由香子氏に深く感謝する．

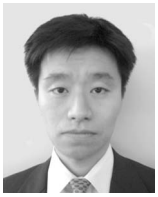
参 考 文 献

1) Bandara, A., Lupu, E., Russo, A., Dulay, N., Sloman, M., Flegkas, P., Charalambides, M. and Pavlou, G.: Policy Refinement for DiffServ Quality of Service Management (May 2005).
2) Fu, Z., Wu, S.F., Huang, H., Loh, K., Gong, F., Baldine, I. and Xu, C.: IPSec/VPN Security Policy: Correctness, Conflict Detection and Resolution, *Proc. Policy 2001: Workshop on Policies for Distributed Systems and Networks*, Bristol, U.K., LNCS 1995, pp.36–43, Springer-Verlag (Jan. 2001).
3) Harkins, D. and Carrel, D.: The Internet Key Exchange (IKE) (1998).
4) Letier, E.: Reasoning about Agents in Goal-Oriented Requirements Engineering (2001).
5) Linux Free S/WAN Project. http://www.freeswan.org/
6) 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.avj.co.jp
7) OASIS, eXtensible Access Control Markup Language (XACML) Version 2.0. OASIS Standard (Feb. 2005). http://www.oasis-open.org/
8) Rosenberg, J. Weinberger, J. Huitema, C. and Mahy, R.: RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (2003).
9) Weinstein, R.S., Descour, M.R., Liang, C., Bhattacharyya, A.K., Graham, A.R., Davis, J.R., Scott, K.M., Richter, L., Krupinski, E.A., Szymus, J., Kayser, K. and Dunn, B.E.: Telepathology overview: from concept to implementation, *Hum Pathol*, Vol.32, No.12, pp.1283–1299 (Dec. 2001).
10) Sun's XACML Implementation. http://sunxacml.sourceforge.net/
11) The Apache Jakarta Project: Velocity, http://jakarta.apache.org/velocity/
12) Wang, H.B., Jha, S., McDaniel, P. and Livny, M.: Security Policy Reconciliation in Distributed Computing Environments, *Proc. 5th International Workshop on Policies for Distributed Systems and Networks* (*Policy 2004*), IEEE, Yorktown Heights, NY (June 2004).
13) 高橋成文，東川淳紀，山本修一郎，小尾高史，谷内田益善，大山永昭：2階層PKIを用いたオンデマンドVPNシステム，情報処理学会論文誌，Vol.46, No.5, pp.1128–1136 (2005).
14) 馬場達也：マスタリングIPsec，オライリー・ジャパン (2001).
15) 馬場達也，角 将高，稲田 勉：動的VLAN制御による統合ワーム対策システムの提案，情報処理学会研究報告，第122回マルチメディア通信と分散処理研究会/第28回コンピュータセキュリティ研究会，Vol.2005, No.33, pp.43–48 (Mar. 2005).
16) 柳沢信成，加藤尚樹，鈴木秀和，渡邊 晃：異なるプライベートアドレス空間端末どうしの通信方式CIPAの提案，マルチメディア，分散，協調とモバイル（DICOMO2005）シンポジウム (June 2005).

(平成17年11月28日受付)
(平成18年 6 月 1 日採録)

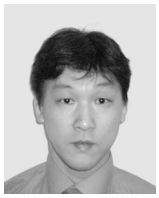
鴨田 浩明（正会員）

（株）NTT データ技術開発本部所属．平成 12 年千葉大学大学院自然科学研究科情報・数理学専攻修士課程修了．同年（株）NTT データ入社．主にネットワークセキュリティおよびソフトウェア工学の研究開発に従事．平成 15 年ドイツ Fraunhofer FOKUS 客員研究員．平成 16 年イギリス Imperial College 客員研究員．平成 13 年情報処理学会第 62 回全国大会奨励賞受賞．



星川 知之（正会員）

（株）NTT データビジネスソリューション事業本部所属．平成 5 年早稲田大学理工学部電子通信学科卒業．同年 NTT データ通信（株）開発本部入社．IC カード技術およびセキュリティ等の研究開発に従事後，IC カードシステムおよび機器認証システムの開発に従事．



山岡 正輝（正会員）

（株）NTT データ情報セキュリティ推進室長．平成 3 年大阪大学大学院工学研究科通信工学専攻修了．同年（株）NTT データ入社．主にパターン認識理解，ネットワークセキュリティの研究開発に従事．平成 4 年 MIT 客員研究員．平成 16 年イギリス Imperial College 客員研究員．博士（工学）．電子情報通信学会会員．

山本修一郎（正会員）

（株）NTT データ技術開発本部副本部長．昭和 54 年名古屋大学大学院工学研究科情報工学専攻修了．同年日本電信電話公社入社．平成 2 年日本電信電話株式会社ソフトウェア研究所主幹研究員を経て，平成 11 年同社情報流通プラットフォーム研究所主幹研究員となり，平成 14 年より現職．ソフトウェア工学，ユビキタスコンピューティングの研究に従事．電子情報通信学会，日本ソフトウェア科学会，人工知能学会，日本データベース学会各会員．平成 13 年度情報処理学会業績賞．平成 14 年度電子情報通信学会業績賞．平成 15 年度通信協会前島賞．博士（工学）．