2階層PKIを用いたオンデマンドVPNシステム

高橋成文[†1] 東川淳紀[†1] 山本修一郎[†1]
小尾高史[†2] 谷内田益善[†3] 大山永昭[†4]

VPNの普及によりインターネットを利用したセキュアな情報通信が実現可能な環境となった．しかし，VPNの設定やメンテナンスには専門的なスキルが必要であり利用までに時間やコストがかかる問題がある．また，設定後は暗号鍵漏洩や設定情報の複製によるなりすましなどにより機密性が損なわれる問題があり企業や家庭で広く利用されるまでに至っていないのが現状である．筆者らは，H14年度に総務省よりインターネット等において各種通信サービスを安全に行うためのネットワーク基盤技術の調査研究を受託し，鍵を安全に配送するネットワーク基盤技術としてSecure e-key Networkの調査研究を実施している．本稿はSecure e-key Networkの基本構想に基づき，VPN利用者の要求に対しネットワークを利用して即座にVPNをセキュアに開通するオンデマンドVPNシステムを提案する．オンデマンドVPNシステムは，機器認証やサービス認証を行うことでリモート環境からVPN機器にセキュアに設定情報を配信・保存できる．本提案の実用性評価として，ICカードを用いたVPNルータにより検証環境を構成し，任意の拠点をオンデマンドにVPN構築可能であることを検証した．また，そのターンアラウンド時間の測定結果を報告する．

On-demand VPN System Using Two Layer PKI

Shigefumi Takahashi,[†1] Atsunori Higashikawa,[†1]
Shuichiro Yamamoto,[†1] Takashi Obi,[†2] Masuyoshi Yachida[†3]
and Nagaaki Ohyama[†4]

Due to recent progress of VPN technology, secure environment for internet communications becomes available for end users. However the secure communications with VPN is not widely deployed for business or home use at the moment. Because professional skills are expected for configuring and maintaining, extra time and cost are required to employ it to existing networks. Moreover, the users have risks such as spoofing caused by leakage of encryption keys or illegal reproduction of setting information. We have been developing the secure key distribution infrastructure over the Internet, which we call Secure e-Key Network, in a research project supervised by Ministry of Public Management, Home Affairs, Posts and Telecommunications. This paper presents the On-demand VPN system which enables immediate establishment of VPN connections whenever users request. It provides a way of secure distribution of configuration parameters to relevant devices for establishing VPN connections from remote site by authenticating both devices and services. For evaluating its feasibility, we developed a prototype system consists of VPN routers with smart cards and verified if VPN connections could be established on demand between any given sites. Finally we report the evaluation result through the analysis of turnaround time measured during the experiment.

1. はじめに

今日，インターネットを利用したVPNサービスの利用が進んでいる．VPNサービスにはインターネットサービスプロバイダ（ISP）が独自回線を利用する方式と利用者がインターネットを利用して構築する方式がある．ISPが提供するVPNを利用する場合，設置や設置情報の変更に対する日程をISPの都合と合わせる必要があり，コストや時間がかかる問題があるが，利用者は設置作業や開設確認をする必要がないことや，回線がISPの独自網なのでセキュリティ上の

†1 株式会社NTTデータ技術開発本部
Reserch and Development Headquarters, NTT DATA CORPORATION
†2 東京工業大学大学院総合理工学研究科
Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology
†3 東京工業大学像情報工学研究施設
Imaging Science and Engineering Laboratory, Tokyo Institute of Technology
†4 東京工業大学フロンティア創造共同研究センター
Frontier Collaborative Research Center, Tokyo Institute of Technology

安心感があるなどのメリットを持つ．一方，利用者がインターネットを利用して VPN を構築する場合は，ルータの設置や情報の変更に対する自由度はあるものの，利用者自身にネットワークの専門知識が必要なうえ，設定などを間違えると情報セキュリティ上多大な影響が発生する恐れがあるなど，だれもが容易に設置できる状況に至っていない．企業連携や SOHO 連携，個人間の連携などでは，インターネット環境の構築後ただちに VPN を利用した機密情報の授受を必要とする場合があるが，先の問題から利用者が VPN を利用したいときに環境をただちに構築できる状況にないのが現状である．

東京工業大学大山研究室では，これまで高度なセキュリティ機能を持つ IC カードの新たな利用として，機器に IC チップを搭載することでセキュアチップとして機器のセキュリティを確保する仕組みの提案や技術実験を行っている[1)~5)]．これらの研究成果や経験から培ったアイデアをもとに，産学が連携して H14 年度に総務省よりインターネットなどにおいて各種通信サービスを安全に行うためのネットワーク基盤技術の調査研究を受託し，鍵を安全に配送するネットワーク基盤技術として Secure e-key Network の調査研究を実施している[6)]．本調査研究において東京工業大学は NTT データより受託研究契約に基づき共同で調査研究を実施している．

筆者らは，Secure e-key Network のフレームワークを応用し，利用者の要求に応じてネットワークを利用した鍵配送として VPN 鍵を配送し，ただちに VPN を構築可能な環境を構築したので報告する．大学において VPN サービスを具体的に実現するうえでの要件整理や IC チップを利用する鍵管理方式について検討を主導し，企業においてシステム構成検討や実装を分担することで，新たな認証技術を実サービスに近い環境で構成することができた．

2 章で Secure e-key Network のフレームワークを説明し，それを VPN ルータに適用し VPN 鍵を配信するための構成を示す．3 章では，VPN 鍵の配送問題を明らかにし，本方式がセキュアに VPN 鍵を配送する仕組みを示す．4 章は，ネットワークを利用して VPN ルータに鍵を配送するシステムの実装方法について説明し，5 章で利用者の VPN の設定依頼から VPN 構築までの動作手順とターンアラウンド時間を紹介する．6 章，7 章は考察とまとめである．

2. VPN の情報設定

2.1 情報設定の課題

ルータ間で VPN を構築するための設定情報には，機器相互の IP アドレスや鍵情報がある．たとえば，拠点間 VPN に利用される IPsec-VPN では，VPN の鍵交換に IKE（Internet Key Exchange）が一般に用いられている[7)]．IKE は，相手認証や SA（Security Association）の折衝と管理，共有秘密鍵管理などを行い IPsec による VPN の鍵交換機能を受け持つ．このとき，IKE で利用する情報を事前に VPN ルータに設定する必要があるが，これらの情報が漏洩すると機器のなりすましも可能となり，機密情報の漏洩にもつながる．また，VPN ルータの設定にはネットワークの専門知識も必要となり，だれもが簡単・安全に情報設定や設定変更できる状況でない．

そこで，これらの課題を解決する手段として，Secure e-Key Network のフレームワークを応用し，利用者の要求に応じてネットワークを利用して設定情報を安全に配送する仕組みが構築できるのではないかと考え本研究を推進している．

2.2 Secure e-Key Network

オンデマンド VPN システムの構築にあたり，Secure e-key Network のフレームワークを参照している．Secure e-Key Network は IC カードで実現されている基本モデルをネットワークに適用し，ネットワーク機能としてセキュアにサービスの利用権（サービスの鍵）の配送を実現，提供する基盤技術である（**図 1**）．e-Key チップは耐タンパ性を有し 2 階層 PKI 技術を実装している IC チップであり，情報流通機器に組み込むことを想定している．機器管理者は e-Key チップの登録，状態の管理を行い，利用権管理者はチップアプリケーションの設定と利用権の配送を管理する．サービス提供者は，利用権を用いた各種サービスを提

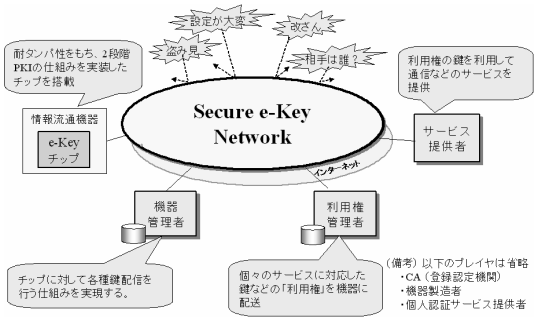


図 1 Secure e-key Network の概念
Fig. 1 Concept of Secure e-key Network.

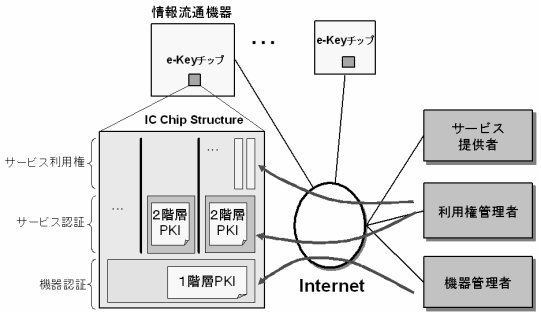


図 2 2 階層 PKI の概念
Fig. 2 Concept of Two Layer PKI.

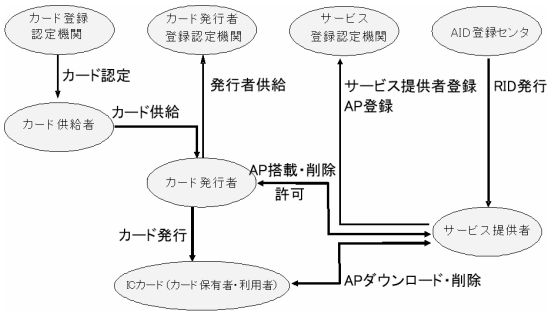


図 3 NICSS フレームワーク（プレイヤモデル）
Fig. 3 NICSS framework (player model).

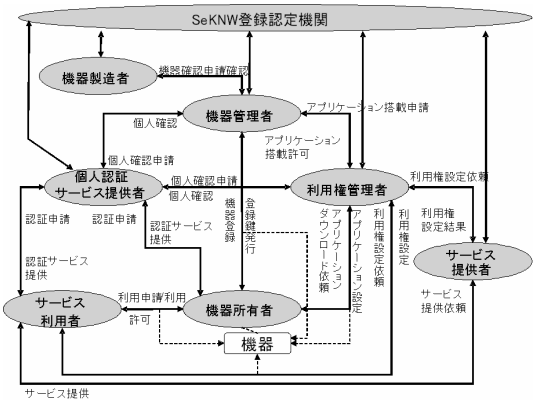


図 4 Secure e-Key Network のフレームワーク（プレイヤモデル）
Fig. 4 Secure e-Key Network framework (player model).

供する．

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チップ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など，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．**図 2** は 2 階層 PKI 情報と利用権の設定概要を示している．まず，e-Key チップを搭載した情報流通機器が機器管理者に認証されると 1 階層目の PKI 情報が設定される．次に，機器管理者より e-Key チップ利用の承諾を得た利用権管理者によって，チップアプリケーションと 2 階層目の PKI 情報が設定される．このとき，1 階層目の PKI 情報を利用したセキュアチャネルにより情報が設定される．なお，各層の PKI 情報はチップ内で生成してもよい．さらに異なる利用権管理者が，機器管理者の承諾を得て新たなチップアプリケーションと 2 階層目の PKI 情報を設定する場合も先と同様な手順で実施される．これにより，e-Key チップ発行後も複数のサービスが登録可能となり，各サービスの登録情報は当該利用権管理者のみ扱うことが可能となる．サービス提供時は，チップアプリケーションと利用権管理者が 2 階層目の PKI 情報を利用したセキュアチャネルにより利用権が設定される．

2 階層 PKI 技術をベースとした IC カードの管理運用モデルとして NICSS フレームワーク[8] が提案されており，Secure e-Key Network フレームワークを構築する際に参考としている．NICSS フレームワークとは，次世代 IC カードシステムの基本仕様を作成するためのモデルとして，システムコンセプト，業務モデル，基本要件，仕様規定範囲を規定している．**図 3** に NICSS フレームワークを示す．

一方，Secure e-Key Network のフレームワークでは，e-Key チップが情報流通機器に内蔵され販売されることや，機器の所有者と機器の利用者が必ずしも一致しない点，それらにともない機器認証が必要となる点などに注意し，プレイヤモデルの確立を行っている．**図 4** に Secure e-key Network のフレームワークを示す．また，プレイヤの役割を**表 1** に示す．

表 1 Secure e-Key Network プレイヤの説明
Table 1 Explanation of Secure e-Key Network Player.

プレイヤ	説明
SeKNW 登録認定機関	Secure e-Key Network 環境を提供するために必要な認証情報を管理する役割
機器製造者	e-Key チップを搭載する機器を製造する役割
機器管理者	e-Key チップを搭載した機器を登録し，e-Key チップ上の資源を管理する役割
個人認証サービス提供者	機器所有者，サービス利用者が本人であることを証明する役割
利用権管理者	利用権管理アプリケーションの発行を行う役割．利用権の発行・管理を行う役割
サービス提供者	サービス利用者にサービスを提供する役割
機器所有者	e-Key チップを搭載した機器を所有する主体
サービス利用者	サービスを利用する主体

NICSS フレームワークが IC カードの貸与を前提

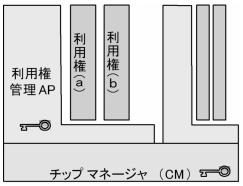


図 5 e-Key チップによる利用権管理イメージ
Fig. 5 Image of right to use management of e-key chip.

とする管理運用モデルであるのに対し，Secure e-Key Network フレームワークでは，機器の販売を前提とする管理運用モデルを確立している．具体的には，以下の点で NICSS フレームワークと異なる．

- 機器の所有権は機器管理者ではなく，機器所有者にある．NICSS フレームワークでは，カードの所有権は発行者にある．
- 利用権管理サービスを提供する利用権管理者とサービス提供者が分離している．NICSS フレームワークでは，サービス提供者が利用権管理サービス相当も提供している．
- 個人認証サービス提供者が分離している．NICSS フレームワークでは個人認証サービスを定義していない．

また，利用におけるフェーズとして，ネットワーク基盤フェーズと利用権管理・配送フェーズに分けることができる．ネットワーク基盤フェーズでは，各プレイヤの登録認定や認証サービス登録，機器登録（1 階層目の PKI 登録），利用権管理 AP 登録（2 階層目の PKI 登録），利用者登録を行う．そして，利用権管理・配送フェーズでは利用権取得のためのサービス利用者のサーバ登録や利用権取得，サービス利用，利用権譲渡が行われる．

利用権の配送により e-Key チップに保存される利用権のイメージを **図 5** に示す．1 階層 PKI の上に利用権管理 AP が独立して 2 階層 PKI として搭載され，その中に利用権が保存される構成となる．

3. オンデマンド VPN システム

3.1 インターネット VPN の現状

インターネット VPN では，VPN の各種設定を利用者自ら行う必要があり，特にネットワーク技術者を持たない企業や家庭では VPN 装置の購入と同時に設置作業も業者に依頼することになり，オンデマンドな VPN 開通が難しい状況にある．さらに，VPN の接続構成を頻繁に変更する場合など，利用者の設定の負担が大きく，VPN の利用促進を阻害しているのが現状である．この状況に対し VPN 設定の利用者の負担を

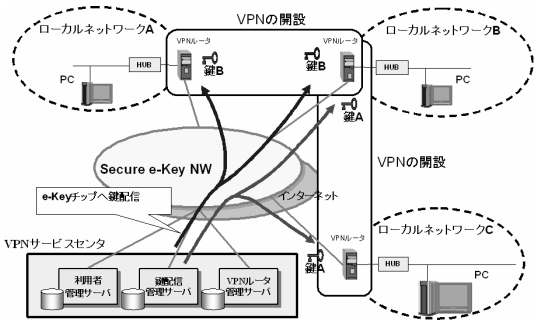


図 6 オンデマンド VPN のサービス例
Fig. 6 Service example of on-demand VPN.

低減する試みとして，辻本ら[9] は，VPN の接続ポリシをセンタで管理し動的に接続可能な構成を提案しているが，利用者があらかじめ VPN ルータに構成情報をセキュアに設定するための仕組みについて提案をしていない．また，アジアビジョン・ジャパン（株）[10] では，IC カードをルータに差し込むことで設定情報を自動でルータに設定する仕組みを実用化しているが，情報の変更が生じた場合には IC カードの配送に時間がかかることからオンデマンドに設定が完了する方式は提供していない．Niwano らは[11]，遠隔環境から IC カードへの書き込み方式として，マルチアプリケーション型 IC カードを扱うプラットフォームを提案しているが，VPN を扱うためのフレームワークの提案や処理方式についての検討は行っていない．

そこで筆者らは，インターネットを利用して VPN を構成する各種情報を利用者の要求に応じてセキュアかつオンデマンドに配信するオンデマンド VPN システムを検討した．遠隔から安全に VPN 機器を制御する仕組みとして，先に紹介した Secure e-key Network を適用した．**図 6** はオンデマンド VPN のサービス例を示している．利用者の VPN 開設要求に対し，鍵配送センタがインターネットを利用して VPN 鍵を VPN ルータに配信している．センタとチップ間で相互認証されセキュア通信路が構築されるため，高いセキュリティを確保して情報の設定が可能となる．配信後，VPN ルータ間で VPN が開設される．

3.2 オンデマンド VPN システムによる情報設定

オンデマンド VPN システムでは，2 章で示した Secure e-Key Network のフレームワークに VPN サービスを適用している．オンデマンド VPN のプレイヤ説明を**表 2** に示す．オンデマンド VPN システムでは，利用権管理者より利用権として VPN 鍵が e-Key チップに設定される．

本フレームワークにおいて，VPN が構築されるま

表 2 オンデマンド VPN のプレイヤ説明
Table 2 Explanation of on-demand VPN Player.

プレイヤ	説明
SeKNW 登録認定機関	Secure e-Key Network 環境を提供するために必要な認証情報を管理する役割
VPN 機器製造者	e-Key チップを搭載する VPN ルータを製造する役割
VPN 機器管理者	e-Key チップを搭載した VPN 機器を登録し，e-Key チップ上の資源を管理する役割
個人認証サービス提供者	VPN 機器所有者，VPN サービス利用者が本人であることを証明する役割
利用権管理者	利用権管理アプリケーション（VPN サービス）の発行を行う役割．利用権（VPN 鍵）の発行・管理を行う役割
VPN サービス提供者	VPN サービス利用者に VPN サービスを提供する役割
VPN 機器所有者	e-Key チップを搭載した VPN 機器を所有する主体
VPN サービス利用者	VPN サービスを利用する主体

での流れを示す．VPN 機器製造者は，SeKNW 登録認定機関より認定を受け，VPN 機器製造時に e-Key チップ内に 1 階層目の PKI 情報を仮鍵として設定し，VPN 機器を販売する．次に，VPN 機器を購入した VPN 機器所有者は，インターネットを利用して，VPN 機器管理者に対して VPN 機器の登録を行う．このとき，SeKNW 登録認定機関より認定された VPN 機器管理者は，e-Key チップに設定された仮鍵で機器認証を行い，認証に成功すれば e-Key チップ内の 1 階層目の PKI 情報を仮鍵から本鍵に再登録する．さらに，VPN 機器所有者が VPN サービス提供者にサービス要求すると，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 サービスのためのチップアプリケーションを e-key チップにダウンロードし，2 階層目の PKI 情報を設定する．また，VPN サービス提供者に対し，VPN 機器所有者より VPN の接続ポリシや VPN 機器を利用可能な利用者の登録が行われる．これで，VPN 機器登録にともなう初期設定が完了する．

VPN サービスを利用する場合は，まず利用者が VPN サービス提供者に対して VPN サービスの依頼を行う．VPN サービス提供者は，VPN 機器所有者が設定したポリシを確認し，接続可能な場合は利用権管理者に VPN 鍵の配送を依頼する．利用権管理者は，VPN 接続する 2 点間の VPN 機器の e-Key チップに設定された VPN サービスアプリケーションと通信し，2 階層目の PKI を利用して相互認証（機器認証）を行い正当な機器であれば VPN 鍵を e-Key チップに配信する．2 点間の VPN 機器に VPN 鍵が配信される

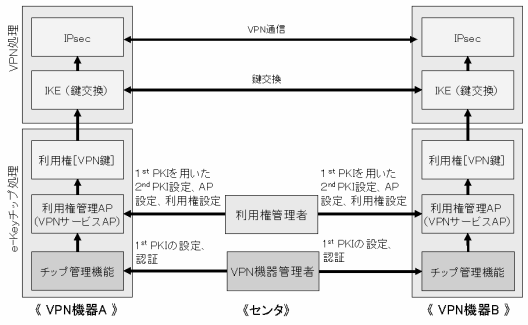


図 7 オンデマンド VPN 構成例
Fig. 7 Configuration example of on-demand VPN.

と VPN 機器は設定された情報を用いて VPN の構築を行う．

図 7 は VPN の構成として鍵交換に IKE（Internet Key Exchange），暗号通信に IPsec を用いた場合の 2 階層 PKI と VPN 構築の関係を示している．まず VPN 機器管理者が，1 階層目の PKI により e-key チップと認証する．次に利用権管理者は，利用権管理 AP のダウンロードおよび 2 階層目の PKI 情報の設定を行う．以後，利用者の VPN 接続要求に基づき利用権管理者は，利用権管理 AP と 2 階層目の PKI を用いて認証を行い利用権をダウンロードする．そして VPN 機器間で IKE，IPsec が利用され VPN が構成される．

4. オンデマンド VPN システムの実装

ADSL ルータを用いてオンデマンド VPN システムのプロトタイプを開発した．開発システムでは，ルータが持つ PCMCIA インタフェースに IC カード R/W を設置し，e-key チップの利用環境を構成した．e-Key チップには，2 階層 PKI 構造を持つ IC カードを用いた．センタ機能として，VPN サービス提供者機能と VPN の利用権管理者機能を 1 台の PC に構成した．利用者からの接続要求を受け付けると，接続ポリシを確認し，VPN 鍵の配信を実行する．また，VPN サービス提供者機能として，ルータの別名と IP アドレスのマッピング情報を提供する VPN ディレクトリセンタを構築した．なお，ルータの登録を行う VPN 機器管理者機能と，利用権管理者機能の一部（利用権管理 AP や 2 階層目の PKI 情報を設定）は，IC カード管理システムで実現検証済みであったため割愛した．ソフトウエア構成を **図 8** に示す．ルータ—センタ間の VPN 鍵にかかわるデータ授受は WWW サーバを介して実装した．

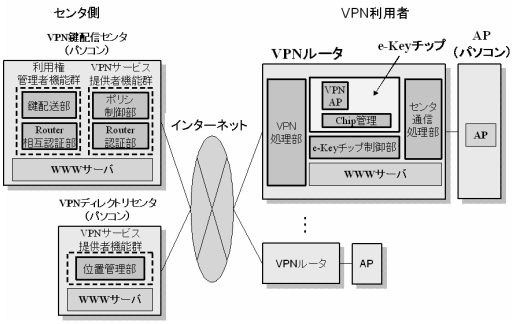


図 8 ソフトウエア構成
Fig. 8 Software configuration.

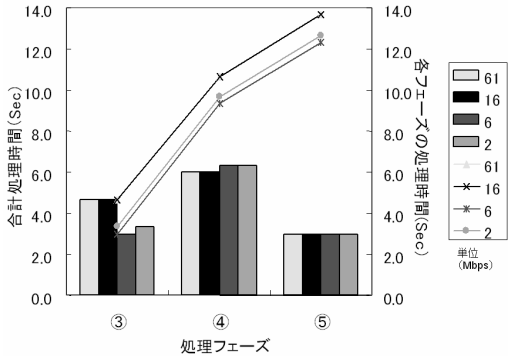


図 9 ターンアラウンド時間
Fig. 9 Turnaround time.

5. プロトタイプシステムの動作手順と動作時間

プロトタイプシステムは，利用者の要求から VPN が開設されるまで以下の手順をとる．

(1) 利用者の PC よりルータにアクセスし，ルータにログインする．ここで，ログイン処理は，VPN 機器登録時に事前に e-Key チップに設定される利用者情報の一致確認によって行われる．

(2) ログインに成功すると，ルータを通して登録された VPN ディレクトリセンタにアクセス可能となり，センタの接続先リストから VPN の接続先を選択する．

(3) 選択した VPN 接続先と自ルータの接続情報をリストにして，自ルータを経由して登録された VPN 鍵配信センタに接続依頼を行う．このとき，e-Key チップでデジタル署名を生成しリストに添付することで依頼元ルータの依頼情報の正当性をセンタ側で検証する．また，VPN 間で VPN 構成ポリシに問題がないか相互確認を行い，相手先ルータが接続に合意していなければ，受付を拒否する．

(4) 署名検証とポリシチェックに成功しいったん VPN 鍵の配信依頼を受け付けると，VPN 鍵配信センタより各リストのルータに鍵の配信が行われる．センタとチップは相互認証とセキュアチャネルにより VPN 鍵をセキュアに e-Key チップに格納する．

(5) VPN 鍵の格納が完了すると，ルータは格納した VPN 鍵をもとに IKE によるセッション鍵交換を行い IPsec による VPN 通信を構築する．

いったん VPN が構築された 2 点間では，利用者の要求により VPN 削除処理が VPN 鍵配信と同様な手順で行うことができる．また，一時的に VPN 鍵を無効化することも可能となっている．

2 点間の VPN 構築時間として，(3)〜(5) で示した動作時間を測定した（**図 9**）．利用するネットワークの通信速度による VPN 構築時間の影響を確認するため，実効通信速度を 4 段階（約 61 Mbps，16 Mbps，6 Mbps，2 Mbps）に設定したときの構築時間を測定した．図 9 より，2 点間の VPN 構築として，(3) における VPN 接続依頼から接続受付完了まで約 4 秒，(4) に約 6 秒（2 点間のルータへの配信），(5) に約 3 秒を要し，全体として 13 秒程度で VPN 構成が可能なことを確認した．通信速度の違いによる VPN 構築時間の影響は，本測定範囲では軽微であった．

6. 考　　察

2 階層 PKI を用いたオンデマンド VPN の効果を 5 章の結果を用いて議論する．一般に VPN 構築では，VPN 機器をインターネットに設置する前に接続する相互の VPN 機器に設定情報を保存する必要がり，VPN 技術者が設置拠点に出張して設置する場合や VPN 機器を技術者に送付して設定してもらう必要があった．これらの手間は数時間から数日かかることが予想され，本システムによればそれらの手間の相当量を削減できる可能性があることが分かった．

VPN 情報の配送・保存において，センタと耐タンパチップが直接暗号通信により設定することで，設定情報の漏洩問題も改善することが確認できた．また，VPN 構築時間のおよそ半分が配送処理にかかわる時間であり，ネットワーク通信速度にそれほど依存しないことから，センタや端末内の配信処理時間の向上が VPN 構築時間の改善に有効なことが分かった．特に，耐タンパチップはメモリ容量や処理速度に制限があることから，VPN 接続拠点数が増加した状況では，チップ側の VPN 情報の受信処理の効率化が課題になると想定される．

実装システムでは既存の ADSL ルータに IC カード

を組み合わせて擬似的に構築しているため，IC カードの脱落，抜き取りによる紛失・盗難の問題が残ることも，今後実用に向けて克服すべき課題である．

7. ま と め

Secure e-Key Network を参照フレームワークとし，2 階層 PKI を利用したオンデマンド VPN システムを開発した．オンデマンド VPN システムは，インターネットで利用が進展している VPN において，設定や設定変更の煩わしさ，セキュリティの課題を解決し，利用者の要求に応じて即時 VPN を開設可能とした．開発システムは，大学において VPN サービスを具体的に実現するうえでのフレームワークや 2 階層 PKI 技術を利用する鍵管理方式について検討を主導し，企業にてシステム構成検討や ADSL ルータを利用した実装を分担することで，新たな認証技術を実サービスに近い環境で構成することができた．

現在，本研究は総務省が実施する平成 16 年度情報通信技術の研究開発である高度ネットワーク認証基盤技術の研究開発を受託し，オンデマンド VPN 技術の研究開発として引き続き産学連携で推進しており，今後は 1 階層目の PKI を利用する機器登録機能の実装や複数拠点での VPN 構築における効率的な VPN 鍵配信技術，配信済み VPN 鍵管理のセキュリティ向上技術などについて検討を進め，インターネットを利用して安全簡単に VPN を取扱い，だれもが安心して情報流通可能な技術の完成に向けて技術開発を進める予定である．

謝辞 本研究は，総務省が実施した H14 年度「インターネット等において各種通信サービスを安全に行うためのネットワーク基盤技術の調査研究」として，「鍵を安全に配送するネットワーク基盤技術」についての調査研究成果を活用したものである．ご協力いただいた関係者各位に感謝する．また，オンデマンド VPN システム開発において，VPN ルータの改造を受け持っていただいた沖電気工業（株），NTT コムウェア（株）に感謝する．

参 考 文 献

1) 大山永昭：ユビキタスネットワークを支える技術（第 3 回）—IC カードと IC タグ，蔵前ジャーナル，8, 973 (2003).
2) 大山永昭ほか：セキュアチップを用いた機器・コンテンツ利用権管理による高度情報サービス基盤の研究開発，通信・放送機構平成 14 年度研究開発成果報告書 (2003).
3) 大山永昭ほか：多機能 IC チップに関するシステム試作報告書，ニューメディア開発協会平成 14 年度報告書 (2003).
4) 小尾高史，山谷泰賀，谷内田益義，山口雅浩，大山永昭：多機能 IC チップを利用した映像メディア配信システムの検討，2003 年情報科学技術フォーラム講演論文集，M-121 (2003).
5) 小尾高史，山谷泰賀，谷内田益義，山口雅浩，大山永昭：セキュアチップを利用したコンテンツ配信システムの開発，第 5 回 YRP 移動体通信産官学シンポジウム講演論文集，pp.96–97 (2003).
6) 小尾高史ほか：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 (2004).
7) 馬場達也：マスタリング IPsec，pp.178–193, オライリー・ジャパン (2001).
8) NICSS（次世代 IC カードシステム研究会）．http://www.nicss.or.jp/
9) 辻元孝博ほか：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（2001 年 7 月 25 日）．
10) アジアビジョン・ジャパン（株）．http://www.avj.co.jp/
11) Niwano, E., Hashimoto, J., Senda, S., Yamamoto, S. and Hatanaka, M.: Smart Card Information Sharing Platform towards Global Nomadic World, *IEICE*, Vol.E87-D No.4 (2004).

(平成 16 年 9 月 2 日受付)
(平成 17 年 2 月 1 日採録)

高橋 成文

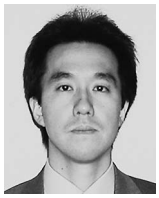
（株）NTT データ技術開発本部勤務．平成元年東京農工大学大学院工学研究科修士課程修了．同年（株）NTT データ開発本部入社．ユビキタスネットワーク技術の研究開発に従事．

東川 淳紀

（株）NTT データ技術開発本部勤務．平成 11 年京都大学大学院工学研究科情報通信工学専攻修士課程修了．同年（株）NTT データ技術開発本部入社．IC カードシステムおよびモバイルセキュリティ等の研究開発に従事．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．



小尾　高史

東京工業大学大学院総合理工学研究科助教授．平成 7 年同大学大学院物理情報工学専攻博士課程修了．同大学教務職員，助手を経て平成 15 年より現職．医用画像処理，医療情報処理，ネットワークセキュリティの研究に従事．電子情報通信学会，応用物理学会，日本医用画像工学会各会員．

谷内田益善

東京工業大学像情報工学研究施設特任助教授．平成元年同大学大学院物理情報工学専攻博士課程修了．高知医科大学助手，平成 3 年（株）リコー入社，平成 13 年より現職．情報セキュリティ，オフィスシステムの研究等に従事．応用物理学会，日本医学放射線学会，日本放射線技術学会各会員．

大山　永昭

東京工業大学フロンティア創造共同研究センター教授．昭和 57 年同大学大学院物理情報工学専攻博士課程修了．同大学助手，助教授を経て平成 5 年より工学部教授となり，平成 12 年より現職．情報処理，医用画像工学の研究に従事．電子情報通信学会，日本放射線技術学会，応用物理学会各会員．