社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DPS－126（18）
2006－CSEC－32（18）
2006／3／16

# 仮想アドレスを用いたプライベートネットワーク間相互通信方式のオンデマンド VPN への適用

有馬 一閣　　鴨田 浩明　　星川 知之　　山岡 正輝

株式会社 NTT データ　〒104-0033 東京都中央区新川 1-21-2
E-mail:　{arimakn, kamodah, hoshikawat, yamaokam}@nttdata.co.jp

**概要** 筆者らは接続要求に応じて即座に VPN を構築できる方式をオンデマンド VPN として既に提案している．しかしながら，VPN 接続する２つのネットワークが同一アドレス体系を持つプライベートネットワークであった場合，正しく通信することができなかった．本論文では，仮想アドレスを用いることで同一アドレス体系を持つプライベートネットワーク間通信をオンデマンド VPN 上で可能にする方式を提案する．また，この方式を実装したオンデマンド VPN ルータの機能評価と性能評価の結果について示す．

# A Case of On-demand VPN with a Method for Communication between Independent Private Network Areas Using Virtual Address

Kuniharu ARIMA, Hiroaki KAMODA, Tomoyuki HOSHIKAWA and Masaki YAMAOKA

NTT DATA Corporation 1-21-2 Shinkawa, Chuoku-ku, Tokyo, 104-0033 Japan
E-mail:　{arimakn, kamodah, hoshikawat, yamaokam}@nttdata.co.jp

**Abstract** On-demand VPN (Virtual Private Network) system makes it possible to set up and control a VPN simply and securely between any set of routers on the Internet, as needed. However, it is impossible for the On-demand VPN system to communicate between different private network areas, if same local IP addresses are used in the two private network areas. In this paper, we propose a method for communication between independent private network areas using virtual address. We also evaluate the functionality and performance of the method by using On-demand VPN router prototype.

## 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，多くの企業が，仮想専用線ネットワーク(以下 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，予め専門の知識を持った者が，VPN の構成情報や通信の暗号化に用いる鍵情報等を生成し，設定する必要がある．そのため，VPN 開設までのコストや時間がかかること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 は，VPN の制御を行う VPN 管理サーバと実際に接続を行う VPN 機器によって IPsec-VPN を構築するシステムである．ユーザが，VPN 接続したい VPN 機器に対して VPN 開設の要求を行うと，VPN 管理サーバで VPN の構成情報を生成し，VPN 機器に配信する．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 IPsec-VPN が自動的に構築される．

一般に企業などの組織は，拠点毎にローカルアドレスを用いてプライベートネットワークを構築している．異なるプライベートネットワーク間で IPsec-VPN 通信を行う場合には，通信を行うためにプライベートネットワーク間のアドレス競合を解決する必要と，プライベートネットワーク間で IPsec-VPN を実現する必要がある．プライベートネットワーク間で IPsec-VPN を実現するための方式は，IPsec-VPN と NAT[2]または NAPT[3]技術（以降まとめて NAT と呼ぶ）を併用し実現する以下の２つの既存方式がある．

① IPsec 処理を行った後で NAT 処理を行う．
② IPsec 処理内部で NAT 処理を行う．

①の方式は IPsec NAT-Traversal[4]である．IPsec NAT-Traversal は，IPsec の暗号化処理や認証処理の後でパケットが変更され，適切に通信できない問題を，IPsec 適用後のパケットを UDP でカプセリングすることで解決する．

②の方式は IPC－NAT[5]である．IPC－NAT は，アドレスが変換されたパケット内容と IPsec のセキュリティポリシーの内容が一致しないため，適切に通信できない問題を，IPsec のセキュリティポリシーの記述内容を NAT 処理に一致するように動的に変更することで解決する．

しかし，IPsec NAT-Traversal や IPC－NAT の技術を使用するためには，既存の IPsec モジュールの改造が必要であり，IPsec の実装方式によっては対応が難しいという課題がある．さらに，これらの既存技術には IP アドレスが競合する場合に通信が行えない問題が残る．

本論文では，仮想アドレスを用い，アドレス競合の問題を解決する方式を提案する．さらに，既存の IPsec モジュールの改造の必要がない事前 SP チェック方式を用い，プライベートネットワーク間で IPsec-VPN を実現する方式を提案する．これらの提案方式を用い，オンデマンド VPN でプライベートネットワーク間の接続を実現する方式を示し，実装したプロトタイプの評価結果について示す．

## 2. オンデマンド VPN

本章では提案方式を適用するオンデマンド VPN の概要について説明する．

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．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 VPN コネクションを実際に開設する機器であり，一般にはルータが VPN 機器となる．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，ユーザの要求に基づき IPsec-VPN を自動的に構築するシステムである．

オンデマンド VPN システムを使用する場合のフェーズは，事前準備フェーズと利用フェーズの 2 つに分けられる．事前準備フェーズは，VPN 機器が正当なものであるかを機器管理サーバに確認し，VPN 管理サーバに VPN を構成するための情報を伝えるフェーズである．利用フェーズは，利用者から挙げられた接続要求に対して VPN 管理サーバ上で VPN 接続に必要となる IPsec 構成情報を生成し，VPN 機器に配信することで，自動的に VPN 機器間で IPsec-VPN を構築するフェーズである．オンデマンド VPN システムの構成図を図 1と図 2 に示す．図 1は事前準備フェーズの流れを，図 2は利用フェーズの流れをそれぞれ示している．

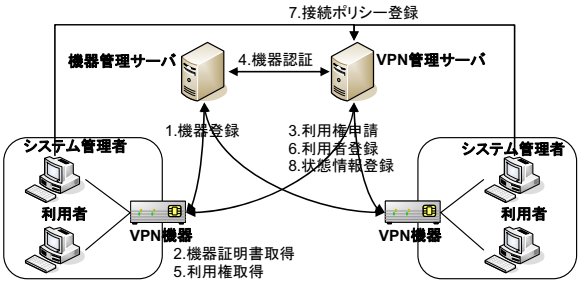


図 1 オンデマンドVPN構成(事前準備フェーズ)

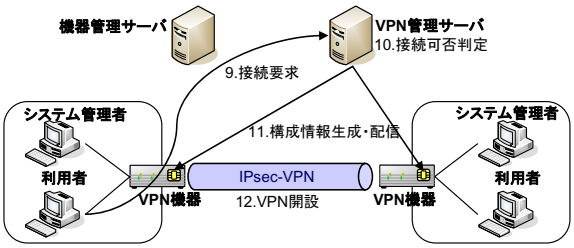


図 2 オンデマンドVPN構成(利用フェーズ)

## 3. 仮想アドレスを用いたプライベートネットワーク間相互通信方式

### 3.1. 方式概要

オンデマンド VPN でプライベートネットワーク間の相互通信を実現するためには，通信元の端末やルータに通信先の端末の情報を与える必要がある．提案方式は，仮想アドレスを用いて通信先の情報を保持することにより，オンデマンド VPN システムでプライベートネットワーク間相互通信を可能にする方式である[6]．この方式は次の 3 つの処理から構成される．

1. 仮想ネットワーク構築：各ルータ内に実際の通信先ネットワークに対応した仮想的なネットワークを構築する処理を行う．
2. 変換規則ネゴシエーション：パケットの変換を行うための規則を自動的にルータ間でネゴシエーションする処理を行う．
3. パケット変換：パケットの通信元情報や通信先情報をルータ上で変換する処理を行う．

次節から，3 つの処理について概要を述べる．

### 3.2. 仮想ネットワーク構築

最初に，プライベートネットワークとグローバルネットワークの境界に位置する各ルータ（以降，単にルータと記述した場合には，境界

に位置するルータを指す）に，通信先のプライベートネットワーク空間と対になる仮想ネットワークを構築する．この仮想ネットワークによって，通信先のプライベートネットワークをあたかも隣接ネットワークであるようにルータ配下の端末に認識させることが可能になる．仮想ネットワークは，ルータ配下にプライベートネットワークとして割り当てられている IP アドレス空間以外の IP アドレス空間を任意に選択して構築する．ルータは通信先の端末名と仮想ネットワーク上の仮想 IP アドレスとの対応付けを行う．通信を行う場合に，通信元の端末は仮想ネットワークの仮想アドレスに対して通信を行う．仮想ネットワーク構築の概念図を図 3に示す．

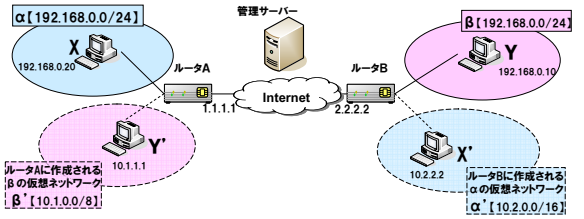


図 3 仮想ネットワーク構築

### 3.3. 変換規則ネゴシエーション

仮想ネットワーク構築処理の後に，通信元端末は，通信先端末に対応する仮想アドレスに対して通信を開始する．しかし仮想アドレスはインターネット上で有効なアドレスではない．そのためルータで，通信に含まれる仮想アドレスの情報を，インターネット上で有効なアドレスに変換する必要がある．つまり仮想アドレスからグローバルアドレスへの NAT 処理が必要となる．この処理に必要となる変換規則を通信元のルータと通信先のルータでネゴシエーションを自動的に行い定義する．変換規則ネゴシエーションの処理手順を以下に示す．

i. 通信元ルータは，通信元端末の IP アドレスとポート番号に，通信元ルータの IP アドレスとポート番号を対応付ける．
ii. 通信元ルータは，通信先である通信元仮想 IP アドレスに対応した端末名と通信先ポート番号を，通信先ルータに通信要求として通知する．この際にiで対応付けた通信元ルータの IP アドレス・ポート番号も通知する．
iii. 通信要求を受けた通信先ルータは，通信先端末に一致する IP アドレスとポート番号に，通信先ルータの IP アドレスとポート番号を対応付ける．
iv. 通信先ルータは，iiiで対応付けた通信先ルータのポート番号を通信元ルータに伝える．

このネゴシエーションで決定した情報を双方のルータが変換規則として保持する．通信終了時には，この変換規則は破棄される．図 4 に変換規則ネゴシエーションの概念図を示す．

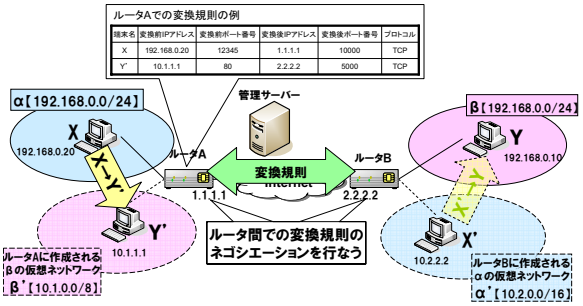


図 4 変換規則ネゴシエーション

### 3.4. パケット変換

変換規則ネゴシエーションにより作成された変換規則を用いて，通信元・通信先ルータ上で仮想 IP アドレスとグローバルアドレス，及び，ポート番号の変換が行われる．これにより，プライベートネットワーク間の相互通信を行うことが可能になる．図 5にパケット変換の概念図を示す．

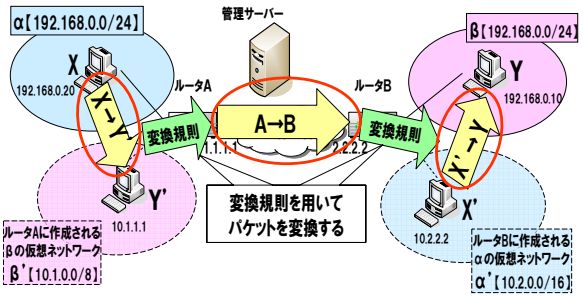


図 5 パケット変換

## 4. オンデマンド VPN への実装

### 4.1. IPsec と仮想アドレス方式の併用

ユーザの要求に基づき IPsec-VPN を自動的に構築するオンデマンド VPN に，前章で提案した仮想アドレスを用いたプライベートネットワーク間相互通信方式を適用すると，プライベートネットワーク間のアドレス競合を解決することができる．

しかし，IPsec と仮想アドレス方式を併用した場合，仮想アドレス方式でパケット変換を行うため，プライベートネットワーク間で IPsec-VPN を実現する場合と同様の問題が発生する．そこで，IPsec-VPN と NAT を併用する際に使用する既存技術の適用を検討する．

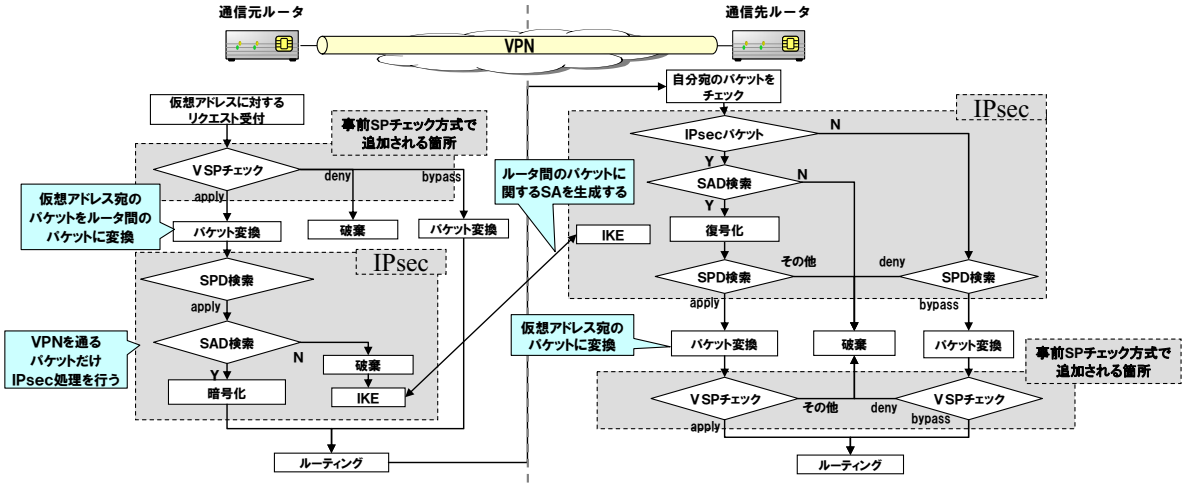


図 6 事前SPチェック方式のフロー図

仮想アドレス方式を IPsec NAT-Traversal と併用すると，UDP でカプセリングするパケットは仮想アドレスを含むことになる. この場合, 通信先プライベートネットワークに到達しても, 正しく通信が行えないという問題が生じる.

仮想アドレス方式を IPC-NAT と併用すると, 異なるプライベートネットワーク間で IPsec-VPN を用いた通信ができない問題を解決することができるが, 既存の IPsec モジュールに対して改造を行う必要があり，IPsec の実装方式によっては対応が難しい.

そこで仮想アドレス方式をオンデマンド VPN に適用する際に，IPsec モジュールを改造しない方式として NAT 処理を行った後で IPsec 処理を行う事前セキュリティポリシーチェック方式(以降，事前 SP チェック方式と呼ぶ)を考案し実装を行った.

### 4.2. 事前 SP チェック方式

通常の IPsec 処理を行う場合，IP パケットの処理方法を記述したセキュリティポリシーが存在する．IPsec 処理を行う前に NAT 処理を行う場合，IPsec 処理されるパケットは全てルータ間のパケットとして扱われる. この状態で IPsec-VPN を構築すると，IPsec のセキュリティポリシーはルータ間の通信は全て IPsec の暗号化処理を行ってしまう.

そこで事前 SP チェック方式は，ルータに独自のセキュリティポリシー(VSP)を設定することで，NAT 処理を行う前に IPsec による暗号化処理を行う通信を選別する.

事前 SP チェック方式を仮想アドレス方式と組み合わせる場合は，IPsec に設定するセキュリティポリシーはルータ間の通信について設定し，独自のセキュリティポリシーには，仮想アドレスに対する通信について設定する. 図 6 に仮想アドレス方式と組み合わせた場合の事前 SP チェック方式のフロー図を示す.

仮想アドレス方式と事前 SP チェック方式を組み合わせたオンデマンド VPN は，以下の処理手順を実装することで実現した.

i. ユーザから VPN の接続要求があり，構成情報を配信された時に，ルータは，通信元のルータと通信先のルータで IPsec-VPN を構築する.
ii. ルータは接続要求の情報を元に VPN を適用すべき通信のリストを作成する.
iii. 通信元のルータで仮想アドレスに対する通信を検知し，iiで作成したリストから IPsec の暗号化処理を適用すべき通信かを判断する.
iv. IPsec の暗号化処理を適用すべき通信である場合には, 仮想アドレス変換の処理を行う.
v. 仮想アドレス変換の処理が行われたパケットに対して，IPsec モジュールで IPsec の暗号化処理を行う.

オンデマンド VPN に実装した際のルータのモジュール構成図を図 7に示す.

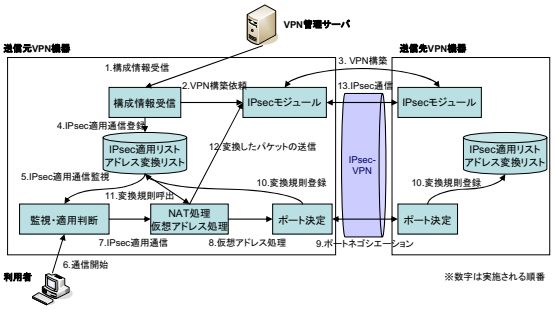


図 7 オンデマンドVPNに実装した際のルータ構成図

## 5. 評価

本章では，既存のオンデマンド VPN ルータ(以降，旧 OD-VPN ルータと呼ぶ)と，検討した内容を元に実装を行ったルータ(以降，新 OD-VPN ルータと呼ぶ)を機能と性能の面で評価を行った結果を述べる．

### 5.1. 機能評価

本節では，機能面での評価について述べる．

旧 OD-VPN ルータと比較して，新 OD-VPN ルータは，同じアドレス体系のプライベートネットワーク間の通信を，仮想アドレス方式を適用することで，正しく通信を行うことを可能とした．しかし，新 OD-VPN ルータには以下の 2 点の制約がある．

- 今回実装したルータは，通信ポートを使用して同じアドレス空間での通信を実現している．そのため，ICMP 等のポート番号を持たないプロトコルで通信を行うためには通信規則ネゴシエーションで使用するポート番号の代替となるものが必要であり，プロトコル毎に対応する必要がある．例としては ICMP の場合，ポート番号の代替としてクエリ ID を使用することで実現する必要がある．
- 今回実装したルータは，IP アドレスを変換しているため，NAT 等と同じようにアプリケーションデータ内部にアドレスに依存する情報を持つプロトコルでの通信はできない．対処方法は，データ部にアドレスに依存する情報を持つプロトコル毎に，アドレスの変換を行う際にデータ部のアドレスの変換についても行う必要がある．現在は FTP などの使用頻度の高いプロトコルには対応しているが，IRC や H.323 などの通信には対応していない．

これらの評価から，本方式はポート番号を持たないプロトコルとアプリケーションデータ部にアドレス情報を持つプロトコルには個別に対応する必要があるが，同じアドレス体系のプライベートネットワーク間の通信が可能となることが分かった．例えば HTTP などのデータ部にアドレスに依存したデータを持たない TCP/UDP の通信であれば対応している．しかし，H.323 等のプロトコルには今後個別に対応していくことが必要である．

### 5.2. 性能評価

#### 5.2.1. 評価方法

今回の評価は，旧 OD-VPN ルータと新 OD-VPN ルータを用いて以下の 2 点について測定し，性能を比較した．

① VPN 接続要求を出してから，接続が完了するまでの時間，並びに VPN 切断要求を出してから，切断が完了するまでの時間を測定する．

② VPN を構築した後で，異なるサイズ(1k,10k,100k,1M,10M 単位は byte)のデータを連続して送信を行い，その時の平均所要時間をセッション数ごとに測定する．

図 8に評価環境を示す．旧 OD-VPN ルータの場合，同じアドレス空間での相互通信は不可能であるため，アドレス空間を送信元と送信先で異なるものにして実験を行った．①の実験は Ethereal[7]を使用して測定を行い，②の実験は PCATTCP[8]を使用して測定を行った．

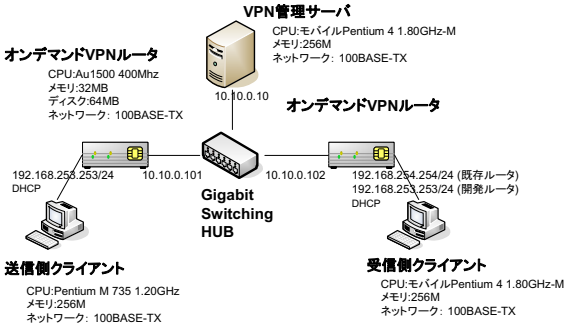


図 8 評価環境

#### 5.2.2. 結果・考察

実験①で接続が完了するまでに要した時間と切断するまでに要した時間を 5 回測定し，それらを平均した結果を図 9に示す．新 OD-VPN ルータは，旧 OD-VPN ルータと比較して，接続時，切断時共に 2~3 秒程度遅延があることが判明した．これは，IPsec の暗号化処理を適用する通信を行う前に変換規則ネゴシエーションを行っているために遅延が発生しているものと考えられる．

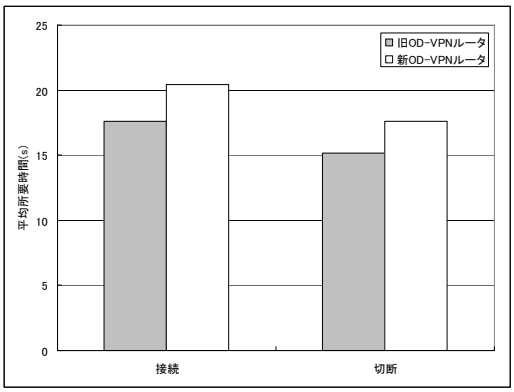


図 9 実験①での測定結果

新 OD-VPN ルータは旧 OD-VPN ルータと比較して VPN を接続／切断するまでに 1.15 倍の時間がかかるが, 既存ルータでかかっていた時間との差が 2~3 秒であることから，オンデマンド VPN のユーザに体感的な差がないと考えられる.

実験②の 1k,10k,100k(単位は byte)のデータを送信した際の測定結果を図 10 に，1M,10M(単位は byte)のデータを送信した際の測定結果を図 11に示す．旧 OD-VPN ルータと比較して，新 OD-VPN ルータは遅延が発生する. この遅延は変換規則ネゴシエーションを行っている為であると考えられる．また，送信データサイズ・同時セッション数が増加するに従い，遅延が増加していることがわかる.

送信データサイズによって, 遅延が増加しているのは, データサイズが増加したことによりルータへの負荷がかかっているためであると考えられる.

また, セッション数が増加することによって, 遅延が増加しているのは, 変換規則ネゴシエーションの回数が増加しているためであると考えられる．新 OD-VPN ルータは，1 回通信を行うごとに, 変換規則ネゴシエーションを行う構造になっているため，1 回の変換規則ネゴシエーションによる遅延が大きいと, セッション数の増加によって遅延の幅が大きくなってしまう. そのため，変換規則ネゴシエーションの遅延を減少させる方式や, あらかじめ変換規則ネゴシエーションを行うことでネゴシエーションの回数を減少させる方式を今後検討する必要がある.

## 6. まとめ

本稿は仮想アドレスを用いたプライベートネットワーク間の相互通信を実現する方式を提案した．この方式をオンデマンド VPN に適用し，ルータに実装を行ったことで，相互通信が実施できることを確認した.

機能評価において, 提案方式は同じアドレス体系のプライベートネットワーク間の通信を実現可能であることを確認したが, プロトコルによっては, 個別に対応する必要があることが分かった．また，性能測定結果よりルータの性能や，変換規則ネゴシエーションを行う回数・処理手順が課題となることが分かった.

今後は, 変換規則ネゴシエーションで発生している遅延を少なくする方式について検討を行う予定である．また，プロトコル別に対応を行い，TV 会議等のアプリケーションへの対応を行う予定である.

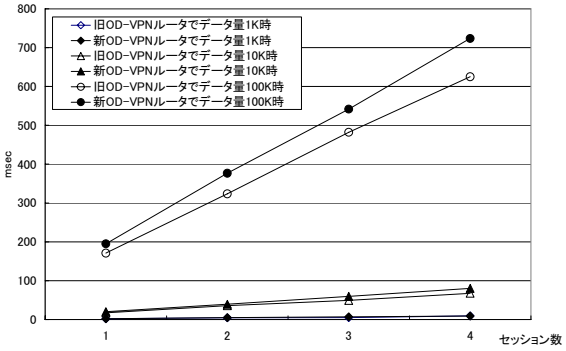


図 10 1k,10k,100k(byte)のデータ送信時の平均時間

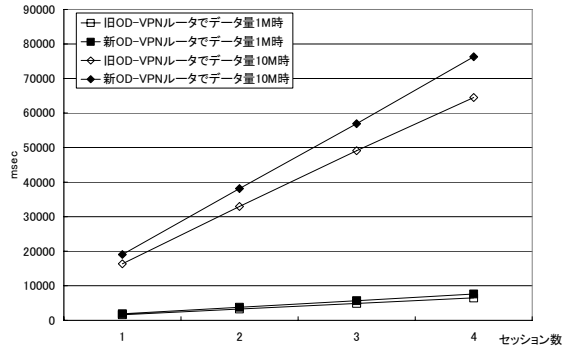


図 11 1M, 10M(byte)のデータ送信時の平均時間


## 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.


## 文　献


[1] 早川晃弘，星川知之，高橋成文，鎌仲裕久．オンデマンド VPN アーキテクチャの提案. 2005 情報処理学会 第 67 回全国大会講演論文集，分冊 3, no.1B-4，pp.329-330，March, 2005.

[2] K. Egevang and P. Francis, The IP Network Address Translator (NAT)，RFC1631, May, 1994.

[3] P. Srisuresh and M. Holdrege, IP Network Address Translator (NAT) Terminology and Considerations, RFC 2663, August, 1999.

[4] T. Kivinen，B. Swander，A. Huttunen and V. Volpe, Negotiation of NAT-Traversal in the IKE，RFC3947, January，2005.

[5] P. Srisuresh，Security Model with Tunnel-mode IPsec for NAT Domains，RFC2709，October，1999

[6] 有馬一閣，鴨田浩明，早川晃弘，山岡正輝．仮想アドレスを用いたプライベートネットワーク間相互通信方式. 信学技報, Vol.105, No.280, pp.7-12, September，2005.

[7] Ethereal, http://www.ethereal.com/.

[8] PCATTCP, http://www.pcausa.com/Utilities/pcattcp.htm.