8　IPv6 の技術的考察

8-1　DVoverIP 転送技術

8-1-1 概要

今回 DVoverIP での双方向対話を実現するために、DVoverIP 経路制御装置を開発した。この装置は以下のような動作を行い、対話を実現する。

ホスト A がホスト B と対話を開始しようとする場合、送信元のホスト A は、ある特定の宛先（以下、DVoverIP 経路制御装置とする）に対してパケットを送信する。DVoverIP 経路制御装置は Web サーバ機能、メッセージ転送機能、呼制御機能、ユーザ管理機能をもち、自己の保有するテーブルに各ホストのアドレスを収容している。対話を開始したいホストはあらかじめ誰と対話を行いたいかをこのテーブルに登録し、DVoverIP を DVoverIP 経路制御装置宛てに送信することで対話の開始要求を行う。DVoverIP 経路制御装置は、受信したパケットの送信元アドレスとテーブルを照らし合わせ、登録されている宛先へそのパケットをリダイレクトする。登録が無い場合はデフォルトの宛先に転送されるが、本実証実験の場合はこれが総合案内窓口である。対話が開始される前は、「着信中」や「呼出中」といったメッセージが DVoverIP で送信元及び転送先に送られ映像として表示される。相手から DVoverIP での返信があると発着信メッセージは両方の映像に切替えられ、対話が開始される。

以後、ホスト A はこの宛先にしかパケットを送信しないが、ブラウザを使って制御することで DVoverIP 経路制御装置の転送先テーブルをその転送先を都度変更することにより対話相手を変えることが可能である。

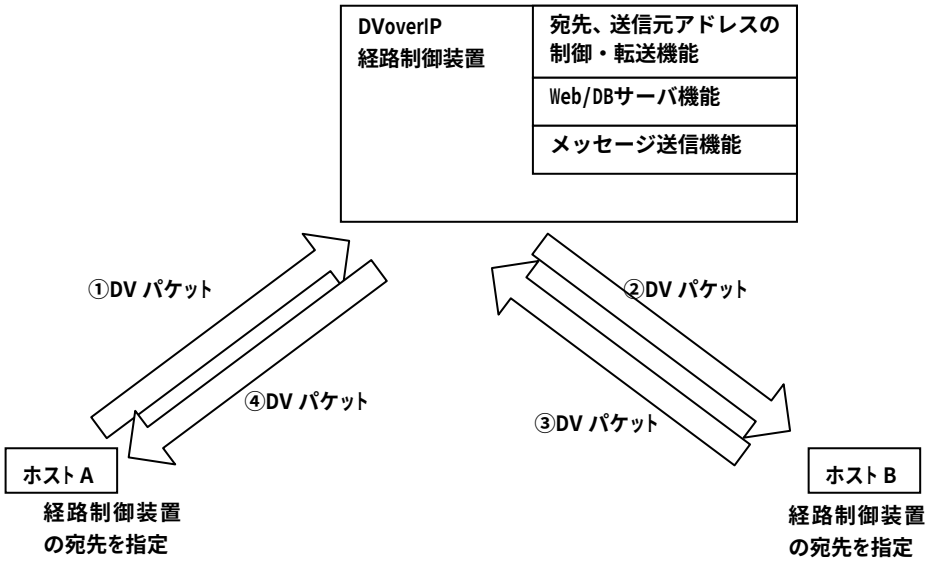

図 8-1-1　DVoverIP 経路制御装置を介した DV による対話

8-1-2 適合するアプリケーション

本アプリケーションは、DVoverIP を利用した高精細な映像対話をボタンポンによる開始・終了といった簡単な操作で実現するために開発したものであり、今回のように呼制御手順を持たない映像伝送アプリケーションを使って対話を行うような用途に有効である。また、多地点対話のようなアプリケーションの場合一箇所で集中して管理する構成は、映像の合成や操作等が容易で一層効果的である。

DVoverIP 経路制御装置による DVoverIP の転送は相手端末をダイレクトに指定する必要があるため、ネットワーク間に NAT があると動作しない。そのため、IPv6 ならではの利用方法であると言うことができる。

8-1-3 メリット

DVoverIP 転送技術を利用することで、以下のようなメリットがある。

(1)　低遅延

双方向映像対話をスムーズに行うためには転送遅延時間が小さいことが重要であり、これが大きいと実際の対面での対話と違い、話すタイミングを窺ったり、同時に話し出してしまったりする等の不都合が生じる。

DVoverIP転送技術による対話では、DVoverIP自体の遅延が小さく、転送による遅延も無視できるぐらい小さいため、映像対話の一巡遅延時間は約 200msec

となる。これは、他の対話（Netmeeting®[15]、MPEG2[16]）と比較して最も小さく対話に違和感を与えることはなかった。各対話の比較を表 8-1-1に示す。

表 8-1-1　各対話での映像の比較

対話方式	一巡遅延時間	対話	画質
DVoverIP	約 0.2 秒	スムーズな対話が可能	良好。テレビ品質。
MPEG2	約 1 秒	違和感がありスムーズな対話ができない	良好。テレビ品質。
H.323[17] (Netmeeting)	約 0.5 秒	スムーズな対話が可能 MPEG2 よりは遅延が少ないが、DVoverIP よりは大きな遅延がある	やや劣る

表から分かるように、帯域を少なくするために MPEG2 等の高画質なフレーム間圧縮を行うと遅延が大きくなり、逆に画質を落とすと画質が劣化し、どちらの場合も自然な対話を再現することが難しくなる。

(2)　クライアントソフトの軽量化

DVoverIP転送技術はクライアントソフトにDVoverIPの送受信機能以外を必要としないため、アドレスの解決やSIP[18]のような呼制御といった制御機能を作りこむ必要がない。また、既存のDVoverIP伝送ソフトウェアをそのまま利用することができ、DVTS[19]やDVcommXP®[20]等といった異なるソフト間での対話が可能になる。

(3)　対話途中における宛先変更

映像の送信元は常に DVoverIP 経路制御装置宛にパケットを送信し続けており、その宛先が DVoverIP 経路制御装置によって変えられていても全く意識しないですむ。通信途中において端末がセッションを変更することなく通信先を変更するといった今までにない制御が可能になる。

(4)　途中経路での通信内容の修正・変更が可能

対話映像は DVoverIP 経路制御装置を中継するために、DVoverIP 経路制御装置により映像の加工や修正を行ったり、全く別の映像に変更して再送信したりすることが可能である。この機能を利用して、発着信メッセージを生成したり、多地点間の対話等を合成して配信したりといった高度な対話も可能になる。

⑸　集中管理

全ての対話を DVoverIP 経路制御装置が集中管理しているため、トラフィックの発生状況をリアルタイムに監視できる。また、映像対話の利用ログを集中的に管理できる。

8-1-4 問題点と対策

⑴　DVoverIP 経路制御装置への負荷の集中

DVoverIP 転送技術の問題点は DVoverIP 経路制御装置への負荷の集中である。全ての対話を DVoverIP 経路制御装置が集中して制御するために DVoverIP 経路制御装置に大きな負荷がかかる。対話の数を 1、2、…と変化させていったときの対話の数と CPU 使用率の関係を図 8-1-2に示す。

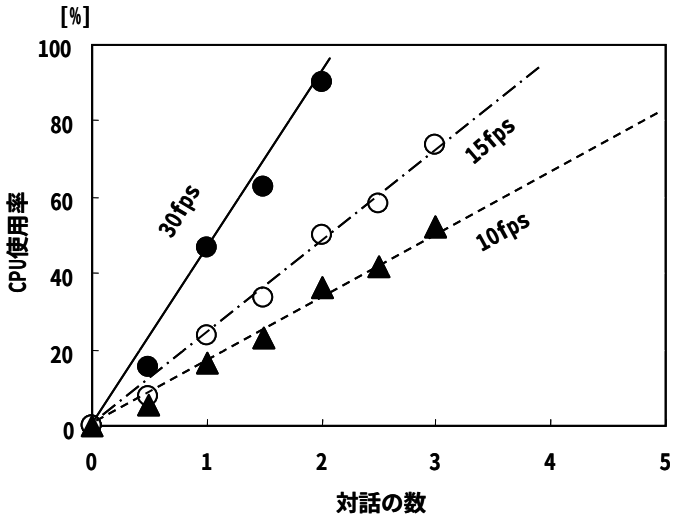

図 8-1-2　対話の数と CPU 使用率の関係

図中の縦軸が CPU 使用率、横軸が対話の数である。対話の数が増加に比例して CPU 使用率が増加する。

CPU 使用率が 100%を超えない場合、全ての対話においてパケットロスは 0 であったが、CPU 負荷が 100%となる対話が生じた場合は各対話に均等にパケットロスが発生する。

上記の結果から 1 台の DVoverIP 経路制御装置でフルフレームの DV 対話が可能な対話数は 2 対話までであり、1/2 フレームの場合は 4 対話、1/3 フレームの場合は 6 対話であることが分かる。

1 台の DVoverIP 経路制御装置が制御（処理）できる映像対話の数は装置性能

に依存するため、多くの対話を同時に行うためには、DVoverIP 経路制御装置を複数設置して制御可能な映像対話の数を増加させる必要がある。

(2)　帯域の圧迫

DV 伝送は、30Mbps 以上の帯域を必要とするため、ネットワークの輻輳状況により、パケットロスが発生する可能性がある。

パケットロスはトラフィックが回線や機器の許容を超えるとランダムに発生するため、発生要因が対話によるものであってもネットワーク上の他の通信に影響を与えうる。例えば、パケットロスが頻発すると TCP 通信であっても緊急時通報が到達しなかったり、個人情報や金銭を扱う情報が通信エラーとなったりすることがある。TCP 通信による到達確認を行わない音声や映像通信の場合、パケットロスはそのまま映像データの欠損となり雑音や映像の乱れを生じる。

また、全ての映像対話を DVoverIP 経路制御装置が集中的に処理する方式であるため、DVoverIP 経路制御装置に大きな処理負荷がかかる。このため、CPU 性能を超える多数の映像対話を制御する際に、パケットロスを引き起こす可能性がある。

そのため、対話トラフィックが増加し、帯域や機器の処理能力を圧迫するような状況が発生したとしても、パケットロスを制御することで、重要通信をエラー無く伝送し、音声・映像を適切な品質で伝送できるQoS技術による対策が必要である[14]。

8-2　IPsec 技術

8-2-1 概要

IPsec は IP レイヤでセキュアな通信を行うためのプロトコルである。構成要素を表 8-2-1に示す。

表 8-2-1　IPsec の構成要素

IPsecの構成要素	利用されるアルゴリズム等
認証ヘッダ	Keyed-MD5、HMAC-MD5、HMAC
暗号ペイロード	DES-CBC
鍵交換	DOI、IKE、SKIP

認証ヘッダは、IPパケットにメッセージ認証の機能を提供する。暗号ペイロードは、VPN[21]の暗号化やトンネリング[22]の機能を提供する。これらの仕組みは独立して動作するので、IPパケットのメッセージ認証の機能を利用したい場合は認証ヘッダを利用し、データの暗号化やトンネリングの機能を利用したい場合は暗号ペイロードを利用すれば良い。また、両方を組み合わせて利用することも可能である。IPv6 でIPsecが利用される場合には、通常、IPv6 ヘッダの後に、認証ヘッダ、暗号ペイロードと続く。しかし、IPv6 の拡張ヘッダとして、中継点オプションヘッダ[23]や経路制御ヘッダ[24]、断片ヘッダが使用されている場合は、その後に認証ヘッダと暗号ペイロードが続く

⑴　セキュリティポリシー（SP）

IPsec では、実際に IPsec による処理を適用するかどうかを、個々の通信パケットの内容に応じて選択できる。選択できる処理には以下のものがある。

パケットを破棄する
IPsec を適用せずに通常の処理を行う
IPsec を適用する

これらは、通信パケット内の送信元IPアドレス、宛先IPアドレス、プロトコル、宛先ポート番号によって判断される。このような通信パケットを選択する項目を総称してセレクタと呼ぶ。このセレクタと実際に適用する処理の内容を含んだものをセキュリティポリシー（SP）と呼ぶ。SP内ではIPsecを適用する場合のIPsecプロトコル（AH、ESP、IPComp[25])やモード(トランスポート、トンネル)等も指定する。

⑵　セキュリティ・アソシエーション(SA)

IPsec では、暗号化や認証に使用するアルゴリズムを規定していないため、様々な種類のアルゴリズムの中から利用したいものを選択することが可能である。しかし、相手側がどのアルゴリズムを使用して暗号化したのか、どのアルゴリズムを利用して認証しているのかということが分からなければパケットを受け取ることができない。

このような情報を保持するために、IPsec ではセキュリティ・アソシエーション（SA）を利用する。

SA には、使用する暗号化アルゴリズムの種類、暗号化アルゴリズムのモード、暗号化アルゴリズムで使用する初期ベクトル（IV）の長さ、認証アルゴリズムの種類、認証アルゴリズムのモード、暗号化鍵、認証鍵等の情報が保持される。

⑶　トンネルモードとトランスポートモード

IPsec のカプセリングの方式にはトンネルモードとトランスポートモードの二つのモードがある。この二つの方式には、それぞれ長所と短所がある

①　トンネルモード

トンネルモードと呼ばれるモードでは、IP パケット全体を暗号化し、それを新しい IP パケットにカプセル化（包み込む）する。こうすることで、データだけではなく、IP ヘッダも暗号化されるので、送信元アドレスや宛先アドレス、使用しているプロトコル（アプリケーション）等の情報を隠すことができる。

このモードの長所としては、内部ネットワークでプライベートアドレスを利用している場合でも、VPN 機器にグローバルアドレスが付与されていれば、VPN 機器のグローバルアドレスを含む IP ヘッダが付加されるので、インターネットを経由してプライベートアドレス同士の端末間で通信をすることが可能となる。

また、この機能を利用することにより、内部ネットワークで IPv6 を使用している場合では、その IPv6 パケットを IPv4 パケットにカプセル化することも可能なことから、利用者は IPv4 ネットワークを意識することなく IPv6 パケットを流すこともできる。

一方、短所は、暗号化されたパケットに新たに IP ヘッダを付加するため、その分パケットのサイズが大きくなり配送中にパケットの分割が起こり、スループットが下がる可能性があることである。

②　トランスポートモード

このモードでは、IP ヘッダは暗号化せずに、IP パケットのユーザデータ（トランスポート層以上の部分）のみを暗号化する。このモードは主に、端末間でのセキュリティを提供するために利用される。

このモードの長所として、トンネルモードのようにパケットのサイズが大きくならずに済むことが挙げられる。

また、短所としては、トンネルモードと違い、オリジナルの IP ヘッダをそのまま利用して送られるので、宛先や送信元の端末がプライベートアドレスを使用している場合は、インターネットを介して通信することができない、IP ヘッダは暗号化されない等が挙げられる、

8-2-2 適合するアプリケーション

今回は端末間で複数の PeerToPeer アプリケーションを利用するために IPsec のトランスポートモードを利用した。IPsec を利用しているため映像対話のような UDP 通信もセキュアに保つことができる。

一般にIPsecを利用すると暗号化や複合化等の処理が必要となりスループットは低下し、トランスポートモードではクライアントがその処理を行うためクライアントにかかる負荷が増加する[15]、[16]。

今回の実証実験でも IPsec を適用する場合、IPsec を適用しない場合に比較して FTP のスループットが約 1/2 になるという結果となった。

しかしながら、DVoverIP では IPsec を適用する場合は、IPsec を適用しない場合に比較して、スループットが約 7～8%程度低くなるだけの結果となった。

これは DVoverIP が 30Mbps という一定の帯域を利用するため、IPsec の処理能力が十分大きければ、スループットが 1/2 に低下しても低下後のスループットが 30Mbps 以上であれば、その影響が現れにくいからである。

そのため、今回の映像対話型電子申請・交付のような高精細な映像を扱うアプリケーションであっても、スループットが 30Mbps 以上維持できるようであれば十分利用することができる。昨今の目覚しいコンピュータの処理能力の向上を考えると IPsec による処理能力の低下についてその影響が少なくなってきていると言える。

8-2-3 メリット

(1) End-End でのセキュリティ保護

IPsec を利用することで PeerToPeer なサービスのセキュリティを End-End で行うことが可能になる。このため、LAN 内でのセキュリティに対する脅威についても耐性を持ち、ファイア・ウォール等のボトルネックが生じない。

これまで、IPsec は IPv4 で広く普及している NAT 技術との整合性が悪く End to End のセキュリティ保護につかわれることはあまりなかったが、IP アドレスが豊潤に存在し NAT が不要な IPv6 では IPsec による End-to-End の包括的なセキ

ュリティ保護が可能となる。

⑵　UDP に対するセキュリティ保護

TCP は特定の周期で到達確認を行うため遅延がスループットと直結する。そのため、広帯域映像通信は一般に UDP を利用して行われる。UDP は広帯域伝送には適しているが TCP 通信で一般的な TLS/SSL を適応することができない。

しかしながら、IPsec では UDP を利用した映像対話にも暗号化を適用することができる。

DVoverIP という負荷のかかるデータの送受信も行ったが、データが大きいほど IPsec 処理にかかる単位量あたりの時間が、IPsec を使用しなかった単位量あたりの時間に近づき、またパケットロスもほとんどみられなかった。

トランスポートモードで利用する IPsec は、IPsec 通信を行う 2 者の途中経路に NAT があると動作しない。これは NAT を改竄されたと検知してしまうためである。トランスポートモードで利用する IPsec も IPv6 ならではの機能ということができる。

8-2-4 問題点と対策

⑴　操作性、利便性

IPsec は多くの設定項目があり、設定が難解である。また、今回利用したようなトランスポートモードでの利用は正式にサポートされていないために、標準化されていない技術を組み合わせて利用する場合もある。このような状況であるため、パソコンの各種基本ソフトでの IPsec のサポートも、現状でも不十分であり、設定が複雑で IPv6 のサポートが完全でない。今後、利用者が IPsec の細かな設定を意識せず簡単に利用できるようにするために、基本ソフト等への IPsec の実装に改善の必要がある。

⑵　マルチキャスト(26)対応

IKE(27)は 2 者間での鍵交換プロトコルであるので、複数のホストとの間で利用することができない。多地点での相談をマルチキャストでセキュアに実施する等の応用のためにはIPsecのマルチキャスト対応の検討が必要である[17]。

⑶　DoS(28)攻撃に対する耐力

DoS 攻撃は、傍受や改竄ではなくサービスを不能にしてしまうことを目的としており、パケット伝送そのものが攻撃になりうるためにその防止が困難である。IPsec は特に高負荷な処理であるため、他のサービスに比べ攻撃を受けたときの

影響も大きい。IPsec 以外の実装で DoS 攻撃等に対する配慮も必要になる。