3　共通システムの調査研究

共通システムである IPv6 ネットワークシステム及び PeerToPeer 映像対話型総合案内システムについて、技術的検証を実施するとともに、実際の場でシステムを稼動させることでその利用調査を行い本サービスの社会的な評価を併せて行った。

3.1 DNS-Proxy による IPv4、IPv6　DNS 照会の技術検証

3.1.1　DNS に対するセキュリティ機能の必要性

DNS はホスト名を IP アドレスに変換するサービスである。インターネット利用者は一般に名前を利用してホストを特定する。名前のほうが IP アドレスに比べて分かり易いからである。IPv6 ではそのアドレス空間が 128 ビットと IPv4 の 32 ビットに比べ大幅に拡大され、IP アドレスを直接指定することは IPv4 より一層困難になる。IPv6 を利用するために名前の利用頻度はさらに増加し DNS の重要性も大きくなる。

サーバ・クライアント方式の通信では、クライアントさえサーバの IP アドレスを知っていれば通信を開始することができる。セッションがクライアントからサーバに向けて開始されるため、サーバ側でもアクセスしてきたクライアントのアドレスが分かるからである。しかしながら、映像対話や、遠隔制御のようなどちらからでもセッションを開始する必要がある PeerToPeer アプリケーションでは、お互いが双方の名前の解決をできなければならない。

また、IPv6 ホストは自分のアドレスを自動的に生成することができる。このためネットワークの設定を行う必要がないというのが IPv6 ホストのメリットであるが、DNS への登録が困難になる。IPv6 アドレスが更新されたときに DNS への登録を更新する Dynamic DNS を実装している必要がある。

このように IPv6 を利用することや、映像対話アプリケーションや遠隔制御などダイレクトに相手の端末を指定しセッションを開始することで、DNS の役割はこれまで以上に大きくなる。

もし、DNS がセキュリティ機能を持たないとすると、全く知らない人物が行政窓口に成りすまして対話や遠隔制御を行ったり、行政機関のサイトだと信じ込ませて別のサイトに仕向けられ個人情報を投入させられといった脅威が起こりうる。DNS のセキュリティ確保は非常に重要である。

セキュアな通信を行う技術に IPsec がある。しかしながら、IPsec はパケットが途中経路で改竄されていないこと証明することはできるが、データそのものの認証を行うことはできない。例えば一旦 DNS サーバに不正なレコードが書き込まれてしまうと、そのレコードが正しいものか不正なものかを IPsec で認証することはできない。

3.1.2 DNSのセキュリティ機能

BIND9により実装されているセキュアなDNSとして以下の二つをあげる。

(1) トランザクション署名(TSIG､RFC2845)

トランザクション、つまり問合せや返答など、DNSサーバが送受信する各種メッセージを保護する。また、許可されていないアドレスからの問合せ、ゾーン転送要求、動的更新などを拒否することによって、DNSサーバを保護する。

(2) DNSセキュリティ拡張(DNSSEC､RFC2535)

電子署名によって個々のリソースレコードの完全性、信頼性を保護する。親・子の関係がある DNS サーバについてはこの鍵に親が署名することで委任する。署名付きデータの検証はリゾルバで行う。

TSIGはサーバ･クライアント間及びサーバ･サーバ間での通信を認証するために使い、DNSSECは検索結果の正当性を保証するために使う。

上記の２つの機能について、もう少し詳しく解説する。

3.1.3 トランザクション署名

トランザクション署名（Transaction Signatures、TSIG）は、共有される秘密鍵と単方向ハッシュ関数を使用して、DNSメッセージを認証する。

TSIGレコードはDNSメッセージの付加情報部に追加される。TSIGレコードはDNSメッセージに「署名」をつける役目をし、メッセージの発信者が受信者と同じ秘密鍵を共有していることと、発信後にメッセージが改竄されていないことを保証する。

図 3-1にトランザクション署名のイメージを示す。

①クライアントとサーバで共有の秘密鍵を設定する。

②クライアントは、DNS メッセージ（ゾーン転送要求、動的更新要求等）に共有の秘密鍵を付加したデータから、ハッシュ関数によりダイジェストを計算する。

③クライアントは、DNSメッセージと共に、ダイジェストを含むTSIGレコードを付加して、サーバに送信する。

④サーバは受信したDNSメッセージに、自身が保有している共有の秘密鍵を付加して、ダイジェストを計算する。

⑤このダイジェストと､受信したTSIGレコード内のダイジェストとを比較し、一致すれば、正しいクライアントからの、改竄のないメ

ッセージであると判断する。

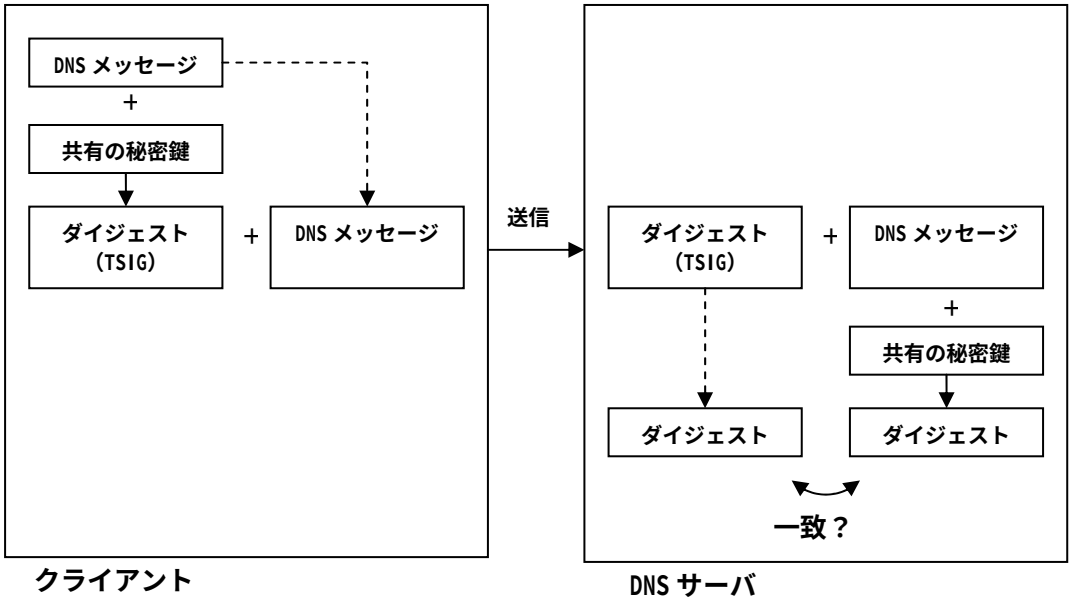


図 3-1　トランザクション署名のイメージ

TSIG を用いることで、DNS サーバは共有の秘密鍵を持っていないホストとの通信に制限をかけることができる。

3.1.4　DNS セキュリティ拡張

DNS セキュリティ拡張(DNSSEC)は、公開鍵暗号方式を使用して、ゾーン管理者がゾーンデータに電子署名をつけ、データの信頼性を保証できるようにしている。図 3-2にDNS セキュリティ拡張のイメージを示す。

①開鍵暗号方式によりゾーンの秘密鍵と公開鍵を生成する。

②サーバにおいて通常のゾーンファイル(例えば xx.co.jp のゾーンファイルとする）の各レコードをゾーンの秘密鍵で署名した署名付（SIG レコード付き）きゾーンファイルを作成する。

③クライアントからサーバに対して A レコードの問い合わせ（例えば aaa.xx.co.jp）を送信する。

④サーバはクライアントに対して、対応する A レコードと共にその A レコードに対する署名である SIG レコードを返答する。

⑤クライアントは返答された SIG レコードを、対応するゾーンの公開鍵で復号化し、ダイジェストを得る。

⑥クライアントは返答されたAレコードからハッシュ関数を用いてダイジェストを計算する。

⑦クライアントは⑤と⑥のダイジェストを比較し、一致すれば返答されたAレコードが正当なサーバからの改竄されていない正しいものと判断する。

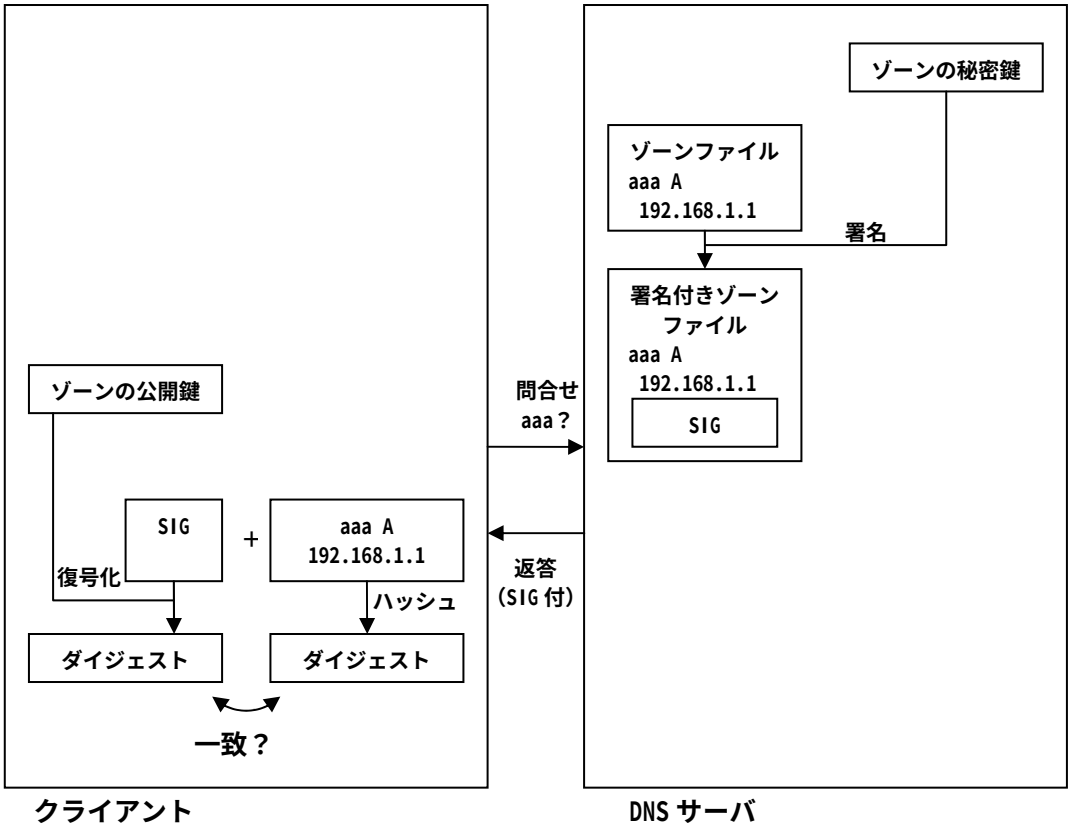


図 3-2 DNSセキュリティ拡張のイメージ

DNSSECを用いることでクライアントはDNSサーバの返答結果の正当性を確認することができる。

3.1.5 検証内容

上記二つのセキュリティ機能によりDNSとの通信でのセキュリティを保護することができる。これら二つのセキュリティ機能の検証を行った。

実験にあたって、マスタ、スレーブ構成の2台のDNSサーバ及びクライアントからなるIPv6/IPv4デュアルスタックホストを準備し、BIND9.2.1を導入した[資料2]。実験に用いたシステム構成を図 3-3に示す。

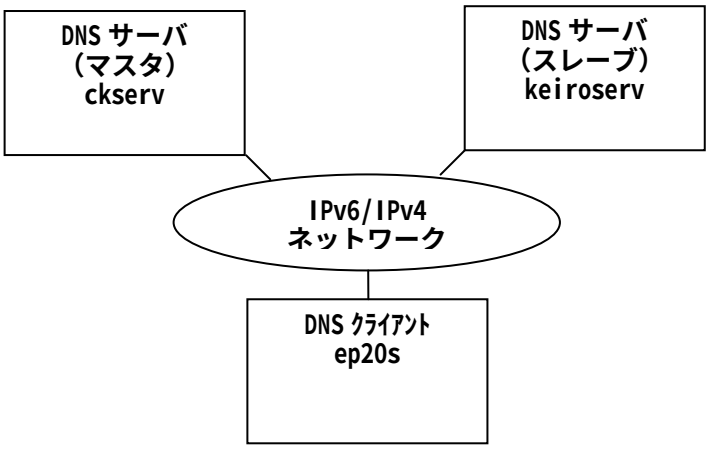


図 3-3 システム構成

検証に用いたホストの情報を
図 3-4に示す。

```
DNS サーバ（マスタ）
        ホスト名：  ckserv.ecity.johosuido.ne.jp
        OS：  FreeBSD 4.6
        IP スタック：  IPv4、IPv6 デュアルスタック
        DNS ソフト：  BIND9.2.1
        IPv4  192.168.1.11
        IPv6  fec0::2e0:4cff:fe83:b218


DNS サーバ（スレーブ）
        ホスト名：  keiroserv.ecity.johosuido.ne.jp
        OS：  FreeBSD 4.6
        IP スタック：  IPv4、IPv6 デュアルスタック
        DNS ソフト：  BIND9.2.1
        IPv4  192.168.1.11
        IPv6  fec0::202:b3ff:feb7:cd51

DNS クライアント
        ホスト名：  ep20s.ecity.johosuido.ne.jp
        OS：  FreeBSD 4.6
        IP スタック：  IPv4、IPv6 デュアルスタック
        DNS ソフト：  BIND9.2.1
        IPv4  192.168.1.202
        IPv6  fec0::2b0:d0ff:fead:4d4a
```

図 3-4 検証に用いたホストの情報

3.1.6　基本動作の検証

(1) 検証方法

DNS サーバ及びリゾルバの正常性の確認を行うため以下の手順を実施する。

クライアントからマスタに対して A レコードを問い合わせる。

マスタからクライアントに対し IPv4 及び IPv6 アドレスが返答される。

(2) 検証結果

図 3-5にマスタからの A レコードの返答を示す。

IPv4 に対応した A レコード、IPv6 に対応した AAAA レコードともに正常に名前解決できているのが分かる。

```
$ nslookup
Default Server:  ckserv.ecity.johosuido.ne.jp
Address:  192.168.1.11

> set type=A
> ep20s.ecity.johosuido.ne.jp
Server:  ckserv.ecity.johosuido.ne.jp
Address:  192.168.1.11

Name:    ep20s.ecity.johosuido.ne.jp
Address:  192.168.1.202

> set type=AAAA
> ep20s.ecity.johosuido.ne.jp
Server:  ckserv.ecity.johosuido.ne.jp
Address:  192.168.1.11

ep20s.ecity.johosuido.ne.jp                    IPv6   address   =
fec0::2b0:d0ff:fead:4d4a
```

図 3-5 マスタからの A レコードの返答

3.1.7　トランザクション署名の検証

(1) ゾーン転送

(i)　検証方法

ゾーン転送がトランザクション署名によりセキュアに行われているのを確認する。

以下の方法で検証を行う。

①マスタとスレーブに共通の鍵を設定してゾーン転送を行う。正しく鍵が設定されて入ればゾーン転送は正常に終了する。

②次にスレーブの鍵を変更し、ゾーン転送を行うと署名の不一致によりゾーン転送が行われないはずである。

(ii) 検証結果

鍵の設定が正しく行うとマスタとスレーブ間で正常なゾーン転送が行われた。このときはマスタより正常な返答が返された。

スレーブの鍵を改竄して不正な鍵にすると、ゾーン転送が行われなかった。このとき、マスタのログメッセージから、スレーブからのゾーン転送要求が不正な署名のため拒否されたことが分かる[資料3]。

図 3-6にマスタのログメッセージを示す。

```
Nov 18 10:43:18.311 client fec0::202:b3ff:feb7:cd51#3429: request has
invalid signature: tsig verify failure
```

図 3-6 マスタのログメッセージ

(2) nsupdate による動的更新

(i) 検証方法

nsupdate がトランザクション署名によりセキュアに行われるのを確認する。以下に検証方法について示す。

①マスタ、クライアントとも共通鍵を正しく設定して、クライアントからマスタに対し nsupdate を実施する。クライアントに正しい鍵が設定されていれば更新は正常に終了するはずである。

②次にクライアントの鍵を不正なものに変更して同様な要求を行ってみると、署名が一致していないためマスタは要求を実行しないはずである。

(ii) 検証結果

クライアントから正常な鍵を指定して nsupdate コマンドで動的更新を要求すると、マスタのゾーン”ecity.johosuido.ne.jp”に、Ａレコードが追加された。

不正な鍵を引数にして動的更新を要求すると、マスタで TSIG の認証エラーになり、更新は行われなかった。

このことからトランザクション署名がただしく機能していることが分かる。[資料4]。図 3-7に 認証エラーメッセージを示す。

```
ckserv#./nsupdate –y
ckserv-keiroserv.ecity.johosuido.ne.jp.:FkN/V3PqbQrOjujKFbqR5
W==
> update add bbb.ecity.johosuido.ne.jp. 3600 A 192.168.1.2
>
; TSIG error with server: tsig indicates error
```

図 3-7 認証エラーメッセージ

3.1.8 DNS セキュリティ拡張の検証

(1) マスタへの直接の A レコード問い合わせ

(i) 検証方法

A レコードの返答が DNSSEC によりセキュアに行われるのを確認する。

以下の方法で検証を行う。

マスタの保有するレコードに正しい署名をつけておく。

クライアントからマスタに対し A レコードの問合せを行うとマスタは A レコードと対応する署名を返答するはずである。署名がついていればクライアントは返答の正当性を検証できる。

次に、その A レコードの内容をマスタ側で改竄する。

クライアントから A レコードの問合せを行うとマスタは改竄された A レコードを返答するはずである。この返答に署名がついていれば返答が改竄されていることを検知できる。

(ii) 検証結果

クライアントから dig コマンドによる問合せを行うと、要求されたＡレコードが署名付きで返答された。この署名を検証することで、レコードが正しいことを確認できる。

次にマスタで IP アドレスを 192.168.1.202 から 192.168.1.22 に不正に改竄すると、要求されたＡレコードが改竄されたまま署名付きで返答された。この署名を検証することで、レコード又は署名が改竄された不正なものであることを確認できる[資料 5] 。DNSSEC を用いたマスタからの A レコードの返答を図 3-8に示す。

```
(a)改竄前

;; ANSWER SECTION:
ep20s.ecity.johosuido.ne.jp. 3600 IN      A       192.168.1.202
ep20s.ecity.johosuido.ne.jp. 3600 IN      SIG     A   1   4   3600
20021206015805    20021106015805    9129    ecity.johosuido.ne.jp.
LaRxjfUpviF9KqNQfZbivpiNcgruZ86zID/+GXRFGkB4hUCYpgsfR2Xw
gQbWesa3aGIMWvOF+jDHv8oQZGhBSg==

(b)改竄後

;; ANSWER SECTION:
ep20s.ecity.johosuido.ne.jp. 3600 IN      A       192.168.1.22
ep20s.ecity.johosuido.ne.jp. 3600 IN      SIG     A   1   4   3600
20021206015805    20021106015805    9129    ecity.johosuido.ne.jp.
LaRxjfUpviF9KqNQfZbivpiNcgruZ86zID/+GXRFGkB4hUCYpgsfR2Xw
gQbWesa3aGIMWvOF+jDHv8oQZGhBSg==
```

図 3-8 DNSSEC を用いたマスタからの A レコードの返答

(2) マスタへの直接のゾーン転送要求

(i) 検証方法

ゾーン転送が DNSSEC を用いてセキュアに行われるのを確認する。

以下の方法で検証を行う。

スレーブからマスタに対してゾーン転送を要求すると、ゾーンデータに署名がついて返答されるはずである。返答に署名が付いていれば返答の正常性を検証できる。

次にマスタのゾーンデータを改竄した後に、再度スレーブからゾーン転送要求を行う。返答されたゾーンデータに署名が付いていれば、ゾーンデータが改竄されていることを検知できる。

(ii) 検証結果

スレーブからマスタに対して直接digコマンドでゾーン転送を要求するとゾーンデータが署名付きで渡された。これによりゾーンデータの正当性を証明できる。

次にクライアント ep20s に対するAレコードのアドレスを 192.168.1.202 から 192.168.1.22 に改竄し、再びスレーブからマスタに対して直接 dig コマンドでゾーン転送を要求した。マスタは要求されたゾーンデータを、改竄された ep20s のAレコードも含めてそのまま返答した。署名付きで返答されるので、署名を検証することでレコードが正しいか否かを受信した側でチェックすることができる[資料6]。図 3-9にDNNSEC を用いたゾーン転送の結果を示す。

```
 (a)改竄前
ep20s.ecity.johosuido.ne.jp. 3600 IN       A        192.168.1.202
ep20s.ecity.johosuido.ne.jp. 3600 IN       SIG      A     1     4     3600
20021206015805       20021106015805       9129       ecity.johosuido.ne.jp.
LaRxjfUpviF9KqNQfZbivpiNcgruZ86zID/+GXRFGkB4hUCYpgsfR2Xw
gQbWesa3aGIMWvOF+jDHv8oQZGhBSg==

(b)改竄後
ep20s.ecity.johosuido.ne.jp. 3600 IN       A        192.168.1.22
ep20s.ecity.johosuido.ne.jp. 3600 IN       SIG      A     1     4     3600
20021206015805       20021106015805       9129       ecity.johosuido.ne.jp.
LaRxjfUpviF9KqNQfZbivpiNcgruZ86zID/+GXRFGkB4hUCYpgsfR2Xw
gQbWesa3aGIMWvOF+jDHv8oQZGhBSg==
```

図 3-9　DNNSEC を用いたゾーン転送

(3) スレーブへの問い合わせ

(i)　検証方法

スレーブからの A レコード返答が DNSSEC を用いてセキュアに行われるのを確認する。以下のような方法で検証を行う。

①クライアントからスレーブに対して A レコードの問合せを行うと正しい署名のついた返答があるはずである。返答に署名が付いていればレコードの正当性を検証できる。

②次にマスタのレコードを改竄し、マスタからスレーブへゾーン転送を行う。このときゾーン転送のデータと署名とが一致しないためスレーブにはデータが反映されないはずである。

③次にクライアントからスレーブに再度 A レコード問合わせを行うと、改竄されたデータはスレーブに反映されていないため、返送されないはずである。

(ii) 検証結果

クライアントから改竄前のクライアントのＡレコードを、スレーブに問合せると正常返答が返された。次に、クライアントのＡレコードのアドレスを改竄後、マスタからスレーブに対しゾーン転送を行った。

スレーブでは、クライアントのＡレコードがその署名と一致しないので、Ａレコードを保持しない。このため、クライアントからスレーブに対してクライアントのＡレコードの問合せを行ってもそのアドレスを返答の中に入れることができない。

マスタとスレーブ間では DNSSEC が正しく機能しており、改竄されたレコ

ードはスレーブにおいて破棄されることが検証できた[資料7]。DNSSEC を用いたスレーブからの返答を図 3-10に示す。

```
; <<>> DiG 9.2.1 <<>> +dnssec ep20s.ecity.johosuido.ne.jp.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 12487
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ep20s.ecity.johosuido.ne.jp.     IN      A

;; Query time: 2 msec
;; SERVER: 192.168.1.10#53(192.168.1.10)
;; WHEN: Tue Nov 12 13:28:11 2002
;; MSG SIZE  rcvd: 53
```

図 3-10 DNSSEC を用いたスレーブからの返答

3.1.9 まとめ

(1) 今回構築した IPv6 ネットワーク環境下においてトランザクション署名を用いて、DNS サーバが送受信する各種メッセージが保護されており許可されていないアドレスからの問い合わせ、ゾーン転送要求、動的更新等の拒否が可能であることを確認した。

(2) DNS セキュリティ拡張を用いて、電子署名によるゾーンデータ保護が可能であることを確認した。

(3) PeerToPeer 通信において重要となるセキュアな DNS のやり取りが可能であることが確認でき、映像対話や遠隔制御といった複合的な行政アプリケーションでの名前解決が安全に行えることが確認された。

3.1.10 課題

(1) クライアントの対応

DNS のセキュリティ機能を搭載したリゾルバがあまり普及していない。特に Windows 系 OS での対応が望まれる。

(2) DNS 設定の自動化

DNS のアドレスを自動的に取得する方法の早期標準化が望まれる。

(3) DNS セキュリティ設定の自動化

DNS のセキュリティ機能を誰でも簡単に扱えるために、認証や鍵の管理・配布方法などを検討する必要がある。

3.2 PeerToPeer 通信におけるリルート技術の調査、検証

DV 伝送を利用した映像対話や対話の転送を実現するためにリルート技術を考案し、リルート技術を利用する PeerToPeer 映像対話型総合案内システムを構築した。構築したシステムにおいてリルート動作の実証、特性の評価を行った。

3.2.1　リルート技術の概要

通常の IP 通信では IP パケットの送信元において宛先を設定し、IP パケット交換網ではその宛先通りにパケットを配送する。この動作は IPv4 でも IPv6 でも同じである。

今回、後述する機能を持つ経路制御装置を開発し、この経路制御装置を介して通信を行うことで送信元があらかじめ指定した宛先以外の別の宛先へ転送するリルート技術を考案した。

経路制御装置は次のような動作を行う。

送信元はパケットの宛先を知らない。それゆえに特定のある決められた宛先（以下、経路制御装置とする）に対してパケットを送信する。

そのパケットを受信した経路制御装置は送られてきたパケットの送信元アドレスを見てソースルーティングをする。

ソースルーティングするときにパケットの宛先アドレスは、経路制御装置から本来通信すべき宛先へ変更される。この宛先アドレスは通信されるパケットが自分のペイロード中で運ぶのではなく、独立した別の手段(例えば http)を用いて経路制御装置に設定される。

宛先アドレスを変更するときに送信元アドレスも併せて変更することで宛先からの返信パケットも制御することができる。図 3-11にリルート動作のイメージを示す。

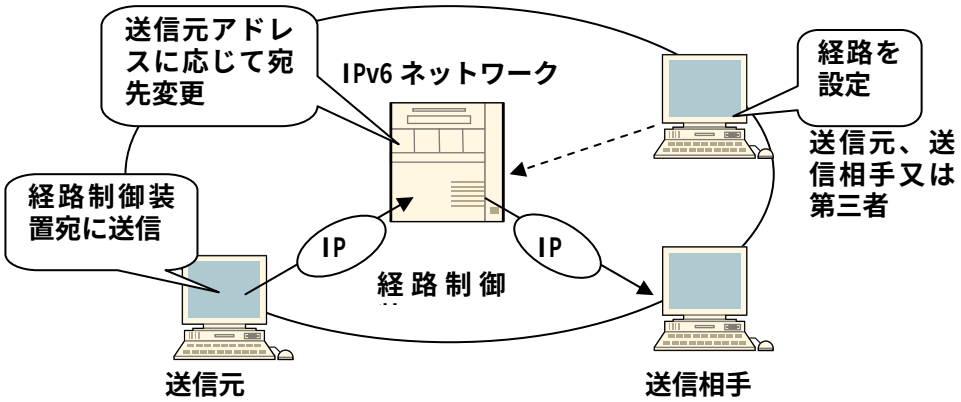


図 3-11 リルート動作のイメージ

このような動作をする経路制御装置を実現することにより以下のような通信制御が可能になる。

送信元は予め通信相手の宛先や名前などを知らなくてもよい。信頼できる通信相手として経路制御装置の宛先を一つだけ知っていればよい。

本人または第三者が通信相手を設定することができる。これは必ずしも通信開始前に設定されている必要はない。通信途中で設定することも可能である。

(1) NAT 技術との相違点

上述の経路制御装置の動作から、NAT（Network Address Translation）技術を連想するかもしれないが、NAT 技術とは以下の点で全く異なる。

一般的にNATは宛先のアドレスを変えるのではなく送信元アドレスを変更する。一方、リルート技術では宛先アドレス自体を変えてしまう。パケットの送信者がその宛先を知らないという意味で根本的に別のものである。

ソースアドレスに対する転送先を決定するアドレス変換テーブルは、リアルタイムに更新される。ルータに予めアドレス変換テーブルを設定しておく操作とは異なる。

リルート技術は、IP アドレスの節約のために利用するのではない。そのため、ポート番号を変換する必要はなく、IPv4 の NAT のようなポート番号の変更に起因する通信の透過性への弊害等は生じない。

(2) プロキシサーバ技術との相違点

プロキシサーバ技術はあるホストに対する通信をあらかじめアプリケーションに指定された代理のサーバ（プロキシサーバ）を経由して行う技術である。これはセキュリティを高めるために外部と自ネット内との直接の通信を遮断する目的でよく使われる。

この場合パケットのヘッダのみを見ると確かにその宛先がプロキシサーバ宛のものからプロキシサーバを経て本来通信したい相手の宛先へと変更されている。しかしながら、本来通信したい相手の宛先はあらかじめ発信元によって設定されたものであり、プロキシサーバは単にその代理として応じているに過ぎない。リルート技術では送信元が事前に宛先が分からないまま経路制御装置にパケットを送信するという意味でプロキシサーバ技術とも異なる。

(3) UDP への適用

いままで述べてきたようにリルート技術とは送信元がセッションを終了させることなく（経路制御装置に対してセッションを張ったまま）その通信相手を切り替えることを可能とする技術である。このような技術を TCP セッションに対してそのまま単純に適応すると、セッションが確立していない相手に対し、セッションが確立してしまっているようなパケットを送信してしまい、通信は途絶する。

一方、UDP のようにコネクションレス型の通信であれば、送信側は一方向にデータグラムを送信し続けつつ、その宛先が切り替わるような動作がなされるが通信は継続する。本技術はコネクションレス型の通信においてより効果的な応用が考えられる。

3.2.2 DVTS

DVTS（Digital Video Transfer System）はリアルタイムプロトコル（RTP）を利用して DV（Digital Video）を伝送するためのソフトウェアであり、WIDE プロジェクトから種々の OS に対応する DVTS ソフトウェアが無償で提供されている。DV の RTP フォーマットは RFC3189 及び RFC3190 で規定されている。

DVTS は、ビデオデッキやカメラといった DV 機器を IEEE1394 インターフェイスを介して端末と接続することで高画質な映像配信を可能とするソフトウェアである。

特に WindowsXP 上では、インターネット経由で受信した DV ストリームを直接ディスプレイに描画することができ、広帯域なネットワークで接続された端末環

境における高画質な動画像放送システムとしても利用することが可能である。

DV フォーマットで伝送されるため DVTS の品質は DV そのものであり非常に鮮明である。

(1) DVTS を利用した対話手順

DVTS は H.323 や SIP のような対話や会議のための手順を持ち合わせていないため対話を行うときは、両者が送信元で宛先を指定する。図 3-12に通常の DVTS による対話を示す。

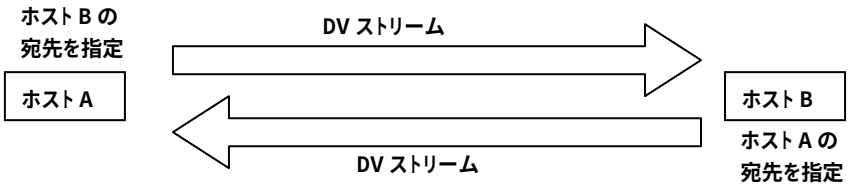


図 3-12　通常の DVTS による対話

対話を行う 2 者は対話を行うにあたり、対話相手の IP アドレスや名前を知ってる必要がある。通信相手のアドレスが分からなければ通信を行うことができない。

また、H.323 や SIP では通信相手の宛先が分からない場合に、対話を行う前段において通信相手のアドレス取得を行うためのサーバが必要になる。対話を開始するホストとそのサーバの間でアドレス登録、取得のための通信手順が決められていなければならない。これらの機能はサーバに加えてクライアントへの実装も必須となるため、クライアントソフトには DVoverIP 規格に準拠したパケットの送受信機能だけでなく、宛先アドレスの解決、対話手順や呼制御といった機能も必要になる。

(2) リルート技術を利用した対話手順

DVoverIP リルート技術はリルート技術を用いて UDP（RTP）で送受信される DV パケットのヘッダを書き換えることによって転送先を制御する技術である。

経路制御装置が対話の中に介在することによって対話相手の IP アドレスを指定せずに対話相手までパケットを転送することが可能になる。図 3-13に経路制御装置を介した DV による対話を示す。

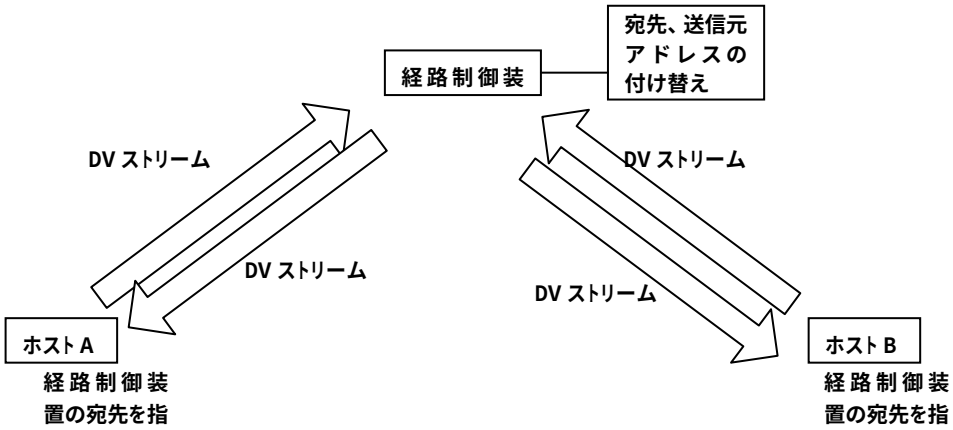


図 3-13　経路制御装置を介した DV による対話

対話を開始するホスト A は経路制御装置宛に DV ストリームを直接送信する。経路制御装置は受信したパケットの送信元アドレスからホスト A からのパケットであることを知る。また、経路制御装置はあらかじめホスト A がホスト B と通信を開始したいことを知っているため、又は、通信途中において宛先を知りえたため受信したパケットの宛先アドレスをホスト B のアドレスに、送信元アドレスを経路制御装置に書換えて再送信する。ホスト B は転送されてきたパケットに答えて対話を行う場合、やはり DV ストリームを経路制御装置に送信する。経路制御装置は受信したパケットの送信元アドレスからホスト B からのパケットであることを知り、ホスト A へ転送する。このようにパケットヘッダを書き換えて転送することで DV 対話を可能とする。

クライアントソフトの機能は経路制御装置宛に DV ストリームを送信するか又は停止するかの 2 種類のみとなる。DVoverIP リルート技術を利用することで、下記のようなメリットがある。

(1) クライアントソフトの軽量化

リルート技術を利用することで対話の宛先を経路制御装置へ指定する機能は完全に DVoverIP から切り離すことができる。このため、アドレスの解決や対話の開始、転送といった機能をクライアントソフトに作りこむ必要がない。

また、既存の DVoverIP に対応したソフトウェアがそのまま利用することができ、DVTS や DVcommXP 等といった異なるソフト間での対話が可能になる。

(2) 利便性の向上

IPv6ホストはIPv6のネイバディスカバリ機能を用いて自動的にIPアドレスを生成する。このため、通信相手のIPv6アドレスを事前に知ることは困難である。IPv6 アドレスでなく名前を利用する場合においても事前にホスト名を知っていなければならない。

本システムはクライアントソフトに対話相手の宛先をその都度設定することなく対話を行うことができる。

(3) 対話途中における宛先変更

映像の送信元は常に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等が可能になる。

(4) 途中経路での通信内容の修正・変更が可能

対話映像は経路制御装置を中継するために、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自動生成したり、複数での同時対話等が可能になる。

(5) 集中管理

全ての対話を経路制御装置が集中管理しているために多くの帯域を消費する DVoverIP 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。

(6) メンテナンスが容易

クライアントソフトはH.323やSIPのように呼制御の手順をもつ必要はなく、特定（経路制御装置）の宛先へ DV 映像を送信する機能と DV 映像を受信する機能のみでよい。それゆえに通信手順の変更や新機能の追加、バグ修正はサーバサイドのみで可能となりクライアントソフトウェアに対する修正が必然的に少なくなる。

3.2.3 IPv6の必要性

IPv4ネットワークはそのアドレス空間の枯渇問題から、プライベートアドレスとNAT技術に頼らざるを得なかった。NAT技術は複数のプライベートアドレス

をポート番号を犠牲にして少数のグローバルアドレスに置き換えるため、外部から見たときポート番号は特定のサービスを指すものではなくなっている。そのため他の PeerToPeer 通信と同様に、本技術により外部から UDP:8000

(DVTS のデフォルトポート番号) でパケットが到来してもそのパケットはプライベートネットワークに入り込む前に捨てられるか、特定の単一ホストに送られるかのいずれかである。

DVoverIP リルート技術は経路制御装置がその仲介を行うが、対話を行う両者宛にパケットが直接到来するという意味で PeerToPeer な通信である。故に、本技術と NAT 技術の相性は悪い。プライベートアドレスで構成される IPv4 ネットワークでこれまで述べてきたようなシステムの実現は困難であり、グローバルアドレスが豊富に存在する IPv6 に対応した技術といえる。

3.2.4 PeerToPeer 映像対話型総合案内システム

IPv6 基盤ネットワークを整備し、DVoverIP リルート技術を用いた経路制御装置、及び DVoverIP の送受信が可能な映像対話コンソールからなる映像対話型の窓口システムを構築した。この窓口システムにおいて、利用者は対話相手の IP アドレスや名前を知らず、利用者側の操作は単に特定の宛先（経路制御装置）へ DV パケットを送信するだけである。DV パケットを受信した経路制御装置がその宛先を該当する窓口へ転送する。構築システムの内容を以下に示す。

(1) システムの概要

本システムは経路制御装置と複数台の映像対話コンソールからなるシステムである。

経路制御装置は DV ストリームのリルートが可能な装置であり、映像対話コンソールとはカメラ映像を DV データとしてとりこみ、DV ストリームとして送信できるとともに、受信した DV ストリームを映像としてモニタに表示させることができる端末機器である。

映像対話コンソールにはボタンデバイスが付いており、利用者（市民）はボタンを押すだけで総合案内窓口と対話を始めることができる。

経路制御装置は映像対話コンソールのボタンが押されたことにより送信される DV 映像を受信し、総合案内窓口の映像対話コンソールへ転送する。また、転送先の映像対話コンソールが返答した DV ストリームを受信し、送信元の映像対話コンソールへ転送する。このように映像対話コンソール間の DV ストリームを中継することで両者の対話を可能とする。

利用者は対話により総合案内窓口の職員に接続する窓口を口頭で伝える。総合案内窓口では、映像対話コンソールから経路制御装置を制御することで

転送先を変更することができる。このため利用者側でなんら操作することなく他の窓口へ転送することができる。

経路制御装置の制御は http で行うこととした。このため、経路制御装置を制御する総合案内窓口等の映像対話コンソールには WEB ブラウザ以外の特別なアプリケーションを必要としない。

(2) システム構成

システム構成を図 3-14に示す。システムは経路制御装置及び映像対話コンソールからなり、IPv6 ネットワーク上で動作する。IPv6 ネットワークは IPv6 ルータやレイヤ 3/2 スイッチなどで構成された一般的なネットワークであるが End to Endo でのスループットが 30Mbps 以上でなければならない[資料 11-14]。図 3-14にPeerToPeer 映像対話型総合案内システムの構成を示す。

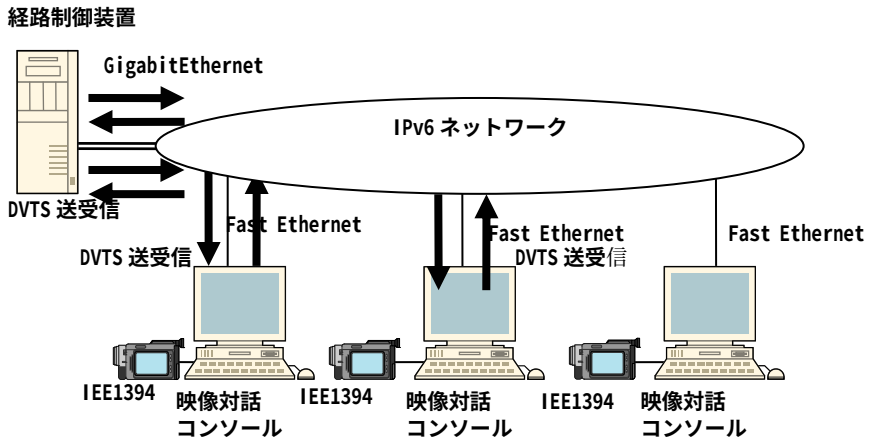


図 3-14 PeerToPeer 映像対話型総合案内システムの構成

(i) 映像対話コンソール

映像対話コンソールは以下の機能を持つ。

①開始ボタンを押すと DV パケットを経路制御装置に送信する。

②停止ボタンを押すと DV パケット送信を停止する。

③経路制御装置から送られてきた DV パケットを映像として表示する。

また、DVoverIP の 30Mbps ストリームが送信されたままになることを防止

するために以下の機能を持たせた。

④UDP:18000 を受信して映像送信を強制的に停止する。

図 3-15に映像対話コンソールの動作フロー、図 3-16にボタンデバイスを示す。

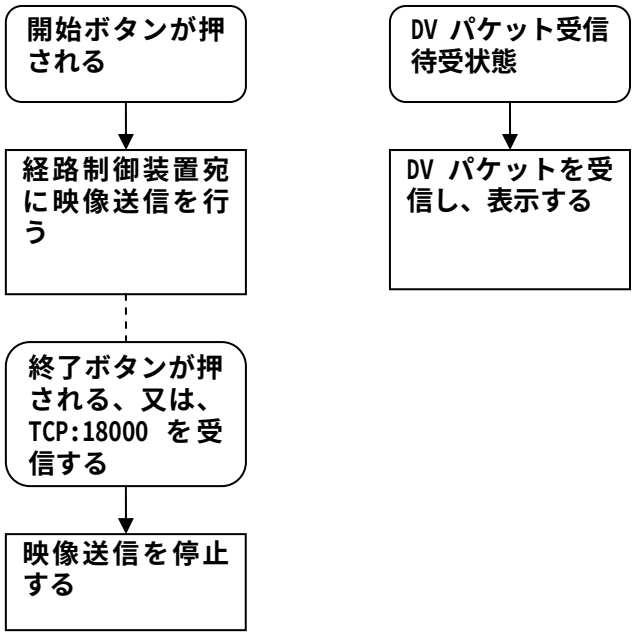


図 3-15 映像対話コンソールの動作フロー

図 3-16 ボタンデバイス

一般市民は映像対話コンソールを用いて、映像対話以外にWEBアプリケーション等を利用するため、OSとしてGUIの優れたWindowsXPを選定した。また、WindowsXP版のDVTSがIPv6の送信に対応していなかったため、映像の送信、受信用に別々のハードウェア構成とし、それぞれ映像送信装置、映像受信装置とした。

映像送信装置のOSとしては負荷が軽く安定しているFreeBSD4.6を採用した。

(ii) 経路制御装置

経路制御装置の機能を以下に示す。

①DVoverIPをリルートする

②利用者情報を管理する

③映像対話コンソールへの緊急停止信号(TCP:18000)を送信する

また、対話に伴い、呼出中、着信中といった呼制御を行う必要がある。そのため下記の機能を持たせることとする。

④呼制御用メッセージを送信する

(3) 経路制御装置の構造

今回リルート技術のみの実証ではなく、総合案内システムとして動作させるために、経路制御装置には経路制御機能の他、WEBサーバ機能、アプリケーションサーバ機能、データベース機能を持たせ総合案内システムとして構築した。

経路制御装置は利用者のアドレスや属性といったデータベースを持ち、許可を持つ利用者はそれらの情報にアクセスすることが可能であり、WEBを利用して閲覧することができる。また、通信相手を特定し利用者毎に専用のページを表示させ、宛先を制御可能な権限をもった利用者にたいしては宛先設定の許可を与える。DV パケットの UDP:8000 のパケットを受信すると設定された情報に基づき該当する宛先を設定しヘッダの変換を行う。図 3-17に経路制御装置の機能ブロック図を示す[資料8、9]、[3]。

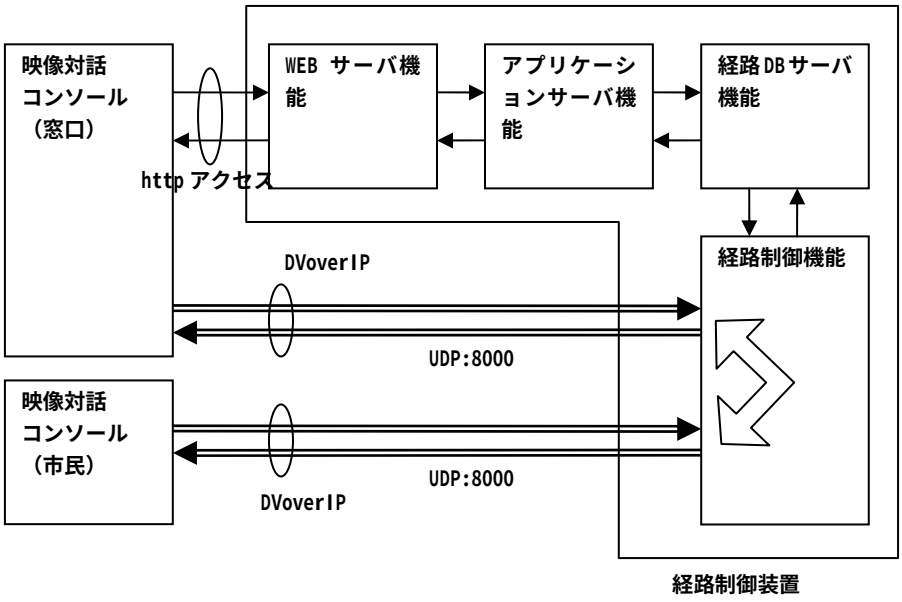


図 3-17 経路制御装置の機能ブロック図

3.2.5 検証内容

実際に映像対話コンソール 2 台と経路制御装置を利用して DVoverIP リルート実験を行い、以下の項目についての調査を行った。

①リルート動作の実証
②CPU 負荷の測定
③リルート遅延の測定

実験にともない構築した IPv6 ネットワークの正常性の確認[資料 10-13]。及び 1 ストリームで 30Mbps の帯域を要する DVTS が End-to-End でロスなく伝送可能であることを確認した。

3.2.6 リルート動作の実証

(1) 基本動作の実証

エッジスイッチのミラーリングにより映像対話コンソール A から受信したパケット、及び映像対話コンソールへ送信したパケットの両方をキャプチャし、その内容を比較した[資料 14]。

この二つのパケットはリルート技術により変換された同一のデータを運ぶものである。これらキャプチャされた二つのパケットを比較するとそれらの IPv6 ヘッダ及び UDP ヘッダに 4 点の相違点がある。リルートにより変換さ

れたパケット間で相違点のあるフィールドを表 3-1に示す。

表 3-1リルートにより変換されたパケット間で相違点のあるフィールド

フィールド	映像対話コンソール A から送信されたパケット	映像対話コンソール B へ送信されたパケット
Source Address	3ffe:516:4931:41::59（A のアドレス）	3ffe:516:4931:41::42（経路制御装置のアドレス）
Destination Address	3ffe:516:4931:41::42（経路制御装置のアドレス）	3ffe:516:4931:41::62（B のアドレス）
Source Port	1039	2444
Checksum	0x03fd	0xfe76

二つのパケット間での宛先アドレスと宛先アドレスの変更は経路制御装置によるものであり、宛先アドレスは経路制御装置のアドレスから転送先のアドレスへ、宛先アドレスは転送元のアドレスから経路制御装置のアドレスへそれぞれ変更されている。また、宛先アドレスの変更に伴い UDP 宛先ポート番号も変更されている。そしてこれらの変更の結果、UDP チェックサムの値が修正されている。

これらのヘッダの変更は全て設計どおりである。以上の事項から分かるように DVoverIP リルートの経路制御の正常な動作が確認された。

(2) パケットロス測定

DVoverIP リルート技術の性能の確認のために転送パケットのパケットロスの測定を行った。測定結果を表に示す。表から分かるように経路制御装置を介した DVTS の映像対話において、1 分間に受信された約 16 万個のパケットにおいてパケットロスは観測されなかった。このことから DVoverIP のリルート機能は良好に動作することを確認した。表 3-2に パケットロス測定の結果を示す。

表 3-2 パケットロス測定の結果

	映像対話コンソール A の受信パケットロス数 受信端末 3ffe:516:4931:41::58 送信端末 3ffe:516:4931:41::59	映像対話コンソール B の受信パケットロス数 受信端末 3ffe:516:4931:41::62 送信端末 3ffe:516:4931:41::63
第 1 回	0	0
第 2 回	0	0
第 3 回	0	0
合計	0	0

（対話時間 1 分間）

3.2.7　CPU 負荷の測定

一台の経路制御装置に複数の DV 対話を処理させることで経路制御装置の負荷を上げ、そのときの CPU 使用率を計測する。このとき、対話の数や転送する 1 秒当たりのフレームレートを変化させ、それらと CPU 使用率との関係を調査する。

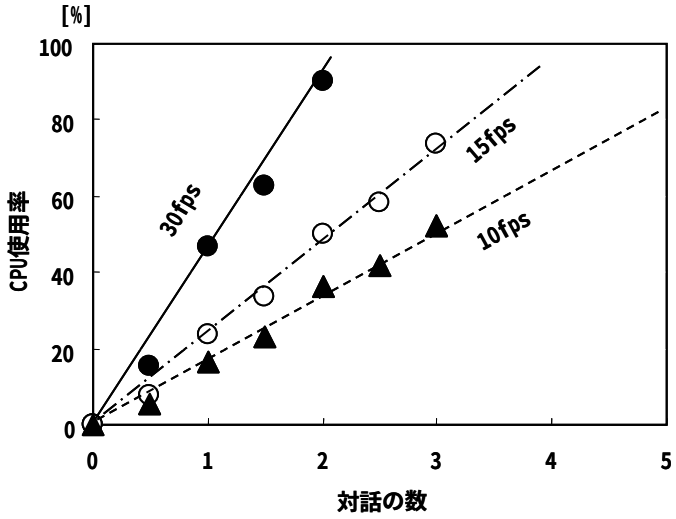


図 3-18 対話の数と CPU 使用率の関係

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 3-18に示す。図中の縦軸が CPU 使用率、横軸が対話の数である。図中横軸の 0.5、1.5 といった小数点は呼び出しのみの片方向通話時であり、双方向通話時は整数の値とした。

対話の数が増加するとともに CPU 使用率はほぼリニアに増加する。

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。

3.2.8　リルート遅延の測定

DVoverIP リルート技術で生じる遅延には対話中に継続的に発生するリルート遅延と、経路設定時、対話開始時等に過渡的に発生する設定遅延がある。このうち、遅延時間が小さいことが重要になるのは対話に直接影響を与えるリルート遅

延であり、たとえ、相手との対話の中でリルート先を設定するために遅延が 1 から 2 秒発生したとしても実用上あまり重要ではない。双方向映像対話をスムーズに行うためにはリルート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、話すタイミングを伺ったり同時にしゃべりだしてしまったりするなどの不都合が生じる。そこで本システムのリルート遅延についての測定を行った。

(1) 実験内容

測定はスイッチのミラーリング機能を利用して行った。送信側の映像対話コンソールから送信されスイッチで受信されるパケットとリルート後、受信側の映像対話コンソールにむけてスイッチから送信されるパケットを同時にキャプチャし、それぞれのキャプチャ時刻を比較した。こうすることで送信、受信の場所でのクロック同期を行う必要がない。リルート遅延の測定系を図 3-19に示す。

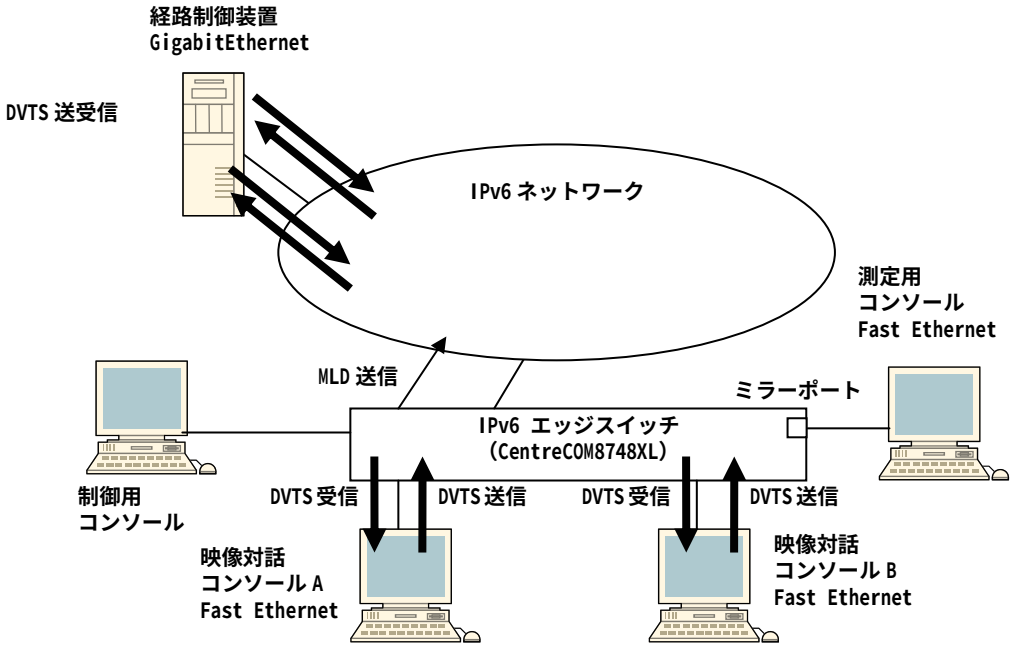


図 3-19 リルート遅延の測定系

(2) 測定結果

測定された遅延時間はこの測定系の測定誤差～1.1msec の範囲内であり、十分に小さく対話に違和感を与えることはなかった[資料 15]。

(3) NetMeeting3 の転送遅延との比較

比較のために NetMeeting 3 を用いて同様な測定を行った。NetMeeting3 の場合、リルートと比較できるような動作が発生しないため、単にネットワークの転送遅延による値となった。この場合の遅延も測定誤差範囲内であり、まったく変わらない結果となった[資料 16]。

しかしながら、実際に対話を行うと DVoverIP を利用したときにくらべ違和感が生じている。これは映像品質が DV のものに比べ劣化していることの他、実際に体感される遅延が DVoverIP よりも大きいことに起因する。このことについては7.1で後述する。

3.2.9 まとめ

(1) 今回DVoverIPのリルート技術を考案しIPv6ネットワーク環境下に対応したPeerToPeer 映像対話型総合案内システムを構築した。そして、構築システムの良好な動作を確認した。

(2) リルートに係る CPU 負荷は対話の数、及び、伝送する映像のフレームレートに比例して増加することを確認した。

(3) リルート遅延時間は～1.1msec とルータ等のネットワーク機器とほとんど変わらないほど小さく、十分対話が可能であることを確認した。

(4) これらの結果から、今回考案したシステムにおいて、DVoverIP による対話とその転送が十分可能であり、行政機関窓口との高精細な対話を遠隔で実現可能であることが確認できた。

3.2.10 課題

本調査研究において、以下のような課題が明らかになった。これらの課題の解決策の検討を行う必要がある。

(1) QoS に関する課題

高精細な映像を提供する DV 伝送は、30Mbps 以上の帯域を必要とするため、サービスの拡大や利用者の増加により、ネットワークの輻輳によるパケットロスが発生する可能性がある。この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、全ての映像対話を経路制御装置が集中的に処理する方式であるため、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。

対話トラフィックが増加しネットワーク帯域、および、経路制御装置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ができ、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仕組み、技術が必要である。

(2) 経路制御装置の多機能化による問題

経路制御装置は総合窓口での受け付けや窓口を切替えるといった経路制御を行う際に、発信側の端末には「呼出中」というメッセージ、受信側の端末には「着信中」というメッセージを送信する。これらのメッセージは、窓口のビジー状態の確認や窓口の呼び出しといった実運用するうえで欠かせないものである。このメッセージ発信処理は、予め登録されている DV 映像ファイルを読込んで送信するというものであるが、ハードディスクからの読み込み処理を行うため、CPU 負荷を上昇させ、同時に行われている他の対に影響を与える。

(3) サーバ複数化によるロードバランシングの必要性

前項にも関連するが、1 台の経路制御装置が制御（処理）できる映像対話の数はマシンスペックに依存する。経路制御装置を複数設置することは、制御可能な映像対話の数を増加させることができ、課題解決の一つの方法となる。しかし、企業内などのイントラネットと異なり、インターネットを利用した行政サービスにおいては、多数の利用者を想定する必要がありロードバランシングのみによる解決は非現実的である。

(4) 多地点対話への対応

今回のリルート技術では双方向で対話を行うが、映像対話は映像対話の実際の利用の場において、複数で同時に対話を行う必要性が生じる。

同時に同じ内容を複数の宛先へ配信する技術としてマルチキャストがあり、IPv6 はマルチキャストの機能を標準で装備している。しかしながら、多地点の同時対話をマルチキャストのみで行おうとすると、対話を行っている

個々の端末にはそのグループの全端末の映像が配信されることになり、ネットワークや端末のリソースを浪費する。このような事態を回避するためには、各端末はユニキャストを利用して映像送信をしつつ、ネットワーク側では、それらのデータを混ぜ合わせた情報をマルチキャストで返信することにより、ネットワークや端末の負荷を増加させることなく多地点の通信を行えるようなマルチポイント対話への応用を検討する必要がある。

(5) 利用者認証技術の必要性

一般にIPv6ホストはネイバディスカバリ機能を使って自己のIPアドレスを自動生成する。そのため、現在接続しているホストをIPアドレスで特定することは困難である。経路制御装置は、リルート技術の仕様上、受信パケットの送信元アドレスに基づきセッションを判別しリルートを行う。そのため、IPアドレスと個人を結びつけるしくみが必要となる。TSIGやDynamic DNSを利用したセキュアな名前解決を行うなどの工夫が必要になる。

3.3 PeerToPeer 映像対話型総合窓口案内サービスの有効性

3.3.1 背景

市役所の取り扱っている業務は市民と直接対応するものが非常に多く、その内容は多種多様である。また、近年においては、業務の効率化の推進や法律改正、新たな条例制定、規制緩和などにより、それらに対応した体制への組織変更などを幾度となく行っている。それゆえ、市役所職員であってもそれら全ての業務がどこの担当部署で取り扱われているのかを完全に把握できている者は、そう多くはない。このような状況の中で、市民が市役所のどの窓口へ行けば自分が望む行政サービスの対応をしてもらえるのか、というのをあらかじめ把握して行動をおこす、ということは非常に困難である。よって、市民と市役所の各担当窓口とをうまく橋渡しをする機能（サービス）は重要であり、市役所においては、庁舎の入り口付近に総合案内をもうけて対応をしている。

このことは、IT を活用して、ホームページ上からの電子申請や、映像対話による行政相談などを行う場合においても同様で、その役割はこれまで、ホームページに記載された説明文で行うしかなかった。

3.3.2 サービスの概要

e！市役所では、市民と市役所の各担当窓口とを橋渡しする機能（サービス）として、映像対話型総合窓口案内サービスを実施した。

映像対話型総合窓口案内サービスとは、利用者が自宅のパソコンにつながれたボタンを押すだけで、自動的に総合案内窓口担当者に接続され、映像対話の中で用件を伝えることにより、希望の担当窓口に転送してもらえるサービスである。

3.3.3 実験の目的

本実験では、映像対話型総合窓口案内サービスが市民にとって、利便性のあるものかどうか、また、どのように利用されるのか、を確認することによりその有効性の検証を行うことを目的とする。

3.3.4 実験環境

e！市役所実験では、100 世帯の自宅モニタ宅に端末を 1 台ずつと、12 の公民館に 1 台ずつ、計 112 台の端末を設置した。また、市役所側の施設内には、総合窓口案内に 2 台、各担当課（福祉事務所、保健センター等）に対して、計 14 台の端末を設置した。モニタ側の 112 台のいずれにも「ボタンポン」デバイスがついており、その「開始」ボタンを押せば、総合窓口案内につながり、総合窓口案内では、映像対話の中で用件を聞きだし、14 の担当課の中の適切な端末へ映像を転送する。

3.3.5　調査方法

本実験における評価項目と、その評価方法は次のとおりである。

(1) 映像対話型総合窓口案内サービスの利便性

サービスの利便性評価の方法として、モニタへ「アンケート」を配布、回収し、回答結果の集計、分析を行う[資料 17]。

(2) 映像対話型総合窓口案内サービスの利用特性

サービスの利用特性評価の方法として、「アクセスログデータ」を収集し、結果を集計、分析を行う。

(3) 総合対話型総合窓口案内システムの操作性

システムの操作性評価の方法として、職員への「インタビュー」を実施し、現行システムを評価し、より職員の利用しやすいシステムに関する考察を行う。

3.3.6　調査結果

映像対話型総合窓口案内サービスの利便性

サービス開始して約１ヶ月後にモニタへアンケートを実施した。モニタ 231 人に対してアンケート用紙を郵送し、98 人から回答を得られた。（回収率は 42.4%）

なお、回答用紙には、属性情報として性別、年齢、職業を記入いただき、名前については無記名とした。

(1) アンケート回答者 98 人の内訳

（i）　性別

男性　69 人（70%）

女性　29 人（30%）

（ii）年齢

本実験の申請対象項目の中に、15 歳以上でなければ申請できないものが含まれており、また、本実験の趣旨を理解していただける年齢として 15 歳以上が妥当であると判断したためモニタへの参加条件を 15 歳以上とした。

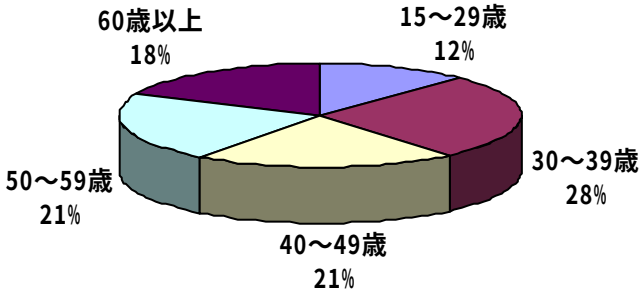
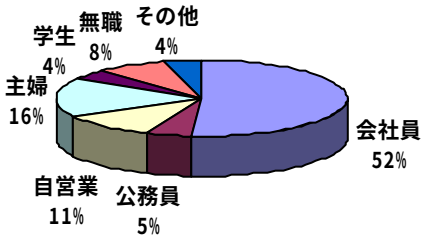


図 3-20 アンケート回答者の年齢

(iii) 職業

職業については、大きく６つの種別にわけ、一番近いと思われるものを選択いただいた。会社員が過半数を占め、次に主婦（16%）、自営業（11%）と続いて多い 。無職の人からも 8 人（8%）の回答があった。



会社員	50 人（52%）
公務員	5 人（5%）
自営業	11 人（11%）
主婦	16 人（16%）
学生	4 人（4%）
無職	8 人（8%）
その他	4 人（4%）

図 3-21アンケート回答者の職業別割合

アンケートの結果は次のとおりである。

Q．市役所の窓口に出向いたり、電話で問い合わせたりすることに対して、パソコンを利用した映像対話型総合窓口案内サービスはいかがでしたか。

とても便利だった	54 人（55%）
どちらかといえば便利であった	32 人（32%）
余り便利とはいえない	5 人 （5%）
必要ない	6 人 （6%）
その他	2 人 （2%）

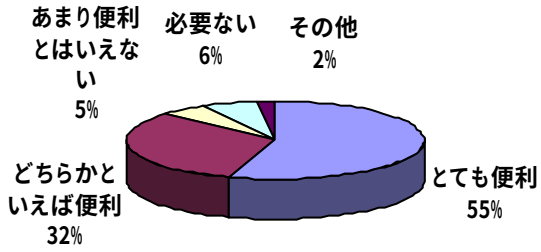


図 3-22 映像対話型総合窓口案内サービスについて

「とても便利だった」(55%)と「どちらかといえば便利であった」(32%)との回答を合わせると、回答者全体の約 9 割の人が映像対話型の総合窓口案内サービスに対して、便利なサービスだと回答した。年代別の傾向を見てみると、特に大きな傾向は見られなかったが、「必要ない」という回答が、比較的若い人に見られた。また、60 歳以上の人に「あまり便利とはいえない」と感じられた人が 2 割ほどいた。

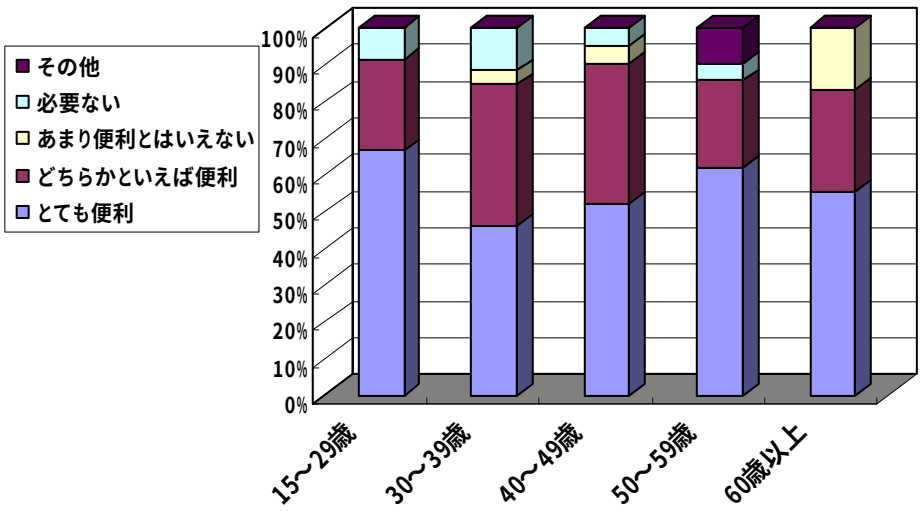


図 3-23 映像対話型総合案内について（年代別傾向）

(2) 映像対話型総合窓口案内サービスの利用特性

2 月 6 日（木）から実験を開始し、3 月 12 日（水）までの 5 週間分のデータを取り、映像対話型総合窓口案内サービスについての利用状況について確

認した。

次のグラフはモニタがボタンポンで総合案内窓口担当者へアクセスしたアクセス数の推移である。期間は実験開始（2 月 6 日）から 5 週間分である。なお、この数値は、自宅や公民館から発信されたアクセス数のみをとっており、実験者や市役所担当者側からの折り返しなどのアクセスを含んでいない。

5 週間で、総合窓口案内へは 267 回のアクセスが寄せられ、担当者によって、187 回対応している（青色）。

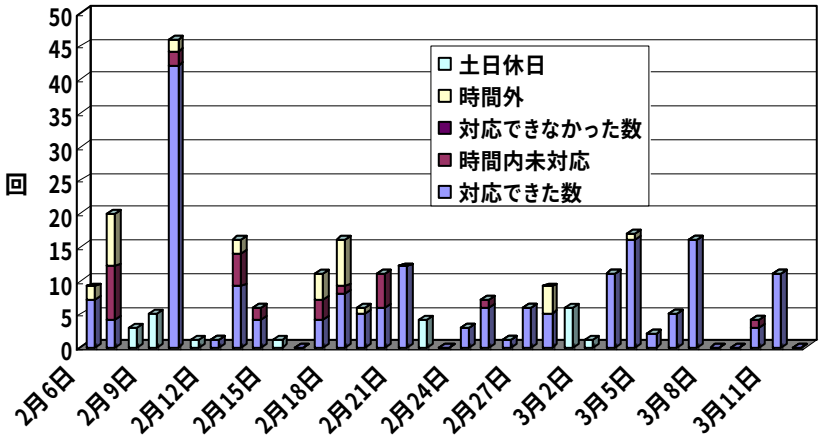


図 3-24 総合窓口案内への日別アクセス数（2/6～3/12）

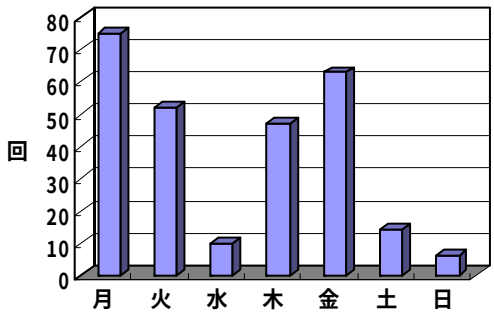
最もアクセスの多かったのが、2 月 10 日（月）で、前日が日曜日、翌日が祝日（建国記念日）と休みにはさまれた日であった

総合案内窓口へのアクセスに対して対応できなかったものには、「時間内未対応」、「時間外」、「土日祝日」がある。合計 80 回のアクセスに対しての対応ができなかったが、その内訳は、

「時間内未対応」 28 回
「時間外」 31 回
「土日祝日」 21 回

であった。これらは、実験開始後約 2 週間に 62 回（対応できなかったもの全体の約 8 割）と集中している。その後はあまり発生していない。

次のグラフは実験開始から 5 週間分の曜日別のアクセス数の合計である。



月曜日	75 回
火曜日	52 回
水曜日	10 回
木曜日	47 回
金曜日	63 回
土曜日	14 回
日曜日	6 回

図 3-25 曜日別総合窓口案内アクセス数

月曜日と金曜日のアクセス数が多く、水曜日が少なかった。これは日別のアクセス数でも確認ができるが、5 週間全ての週においてその傾向が見られた。次のグラフは、時間ごとのアクセス数を集計したものである。

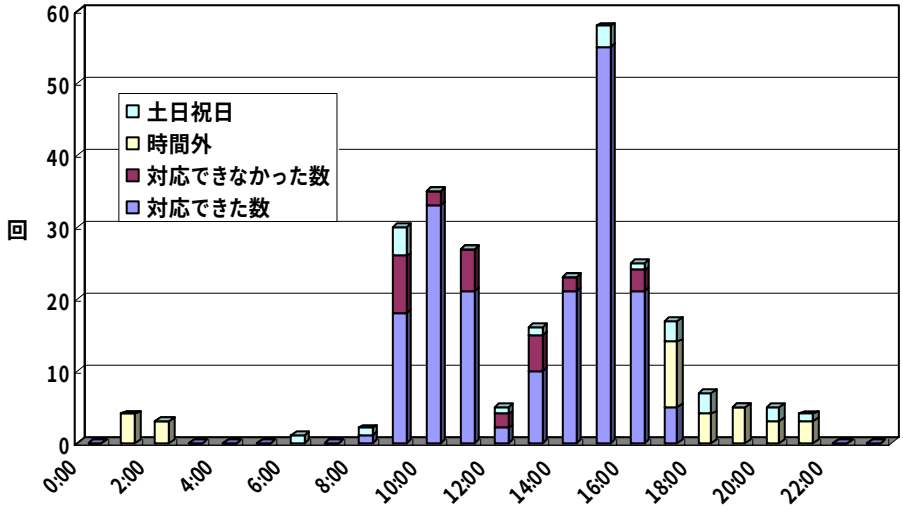


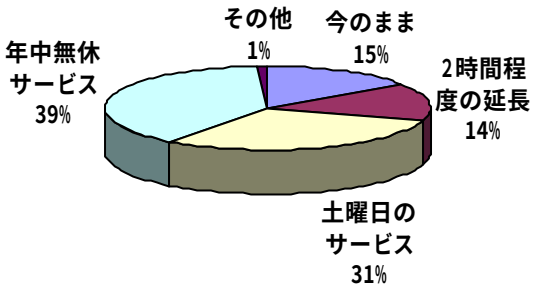
図 3-26 総合窓口案内への時間別アクセス回数(2/6～3/12)

午前中はほぼ均等にアクセスがあるが（9：00 台 35 回、10：00 台 35 回、11：00 台 27 回)、12：00～13：00 にかけて極端に少なく（5 回)、13：00 から徐々に増え、15：00 台に 58 回（全体の 5 分の 1）とピークとなっている。また、サービス終了時間である 17：00 を過ぎても 17：00 台に 17 回、18：00 台に 7 回、19：00 台に 5 回、20：00 台に 5 回とある程度のアクセス数があった。また、深夜の 1：00 台や 2：00 台にもアクセスがそれぞれ数回あった。

次のグラフは本実証実験のサービス時間についてのアンケートの回答で

ある。

Q．今後本実証実験を実用化してゆくにあたり、サービス時間はどうあるのが適切とおもいますか。



今のまま	15 人（15%）
2 時間延長	14 人（14%）
土曜日	30 人（31%）
年中無休	38 人（37%）
その他	1 人（1%）

図 3-27 ｅ!市役所のサービス時間について

アンケートの結果、もっとも多いのが「年中無休サービス」で 38 人（39%）、次に「土曜日のサービス」が 31 人（31%）、「今のまま（平日 9：00～17：00）でよい」15 人(15%)、と続いている。

アンケートの本実証実験に関する感想・意見欄の中にも時間外に対する具体的な要望がいくつか記入されているので列記する。

「平日のみの実験だと、仕事を持っている者には利用しづらい。特定の曜日だけでも早朝か夜利用できるようになればいい。」（50 代会社員）
「理想ですが、日曜日等もやっていただけたらと思いました。」（30 代会社員）
「日中仕事があるので、実験に参加できなかった。」（60 代会社員）
「仕事の関係もあり、平日には家にいることがありません。」（30 代会社員）
「サービスを 24 時間 365 日できるようにして欲しい。そのために手数料が発生しても仕方がない。」（30 代会社員）

次のグラフは、サービス時間についてのアンケートをさらに職業別に集計したものである。

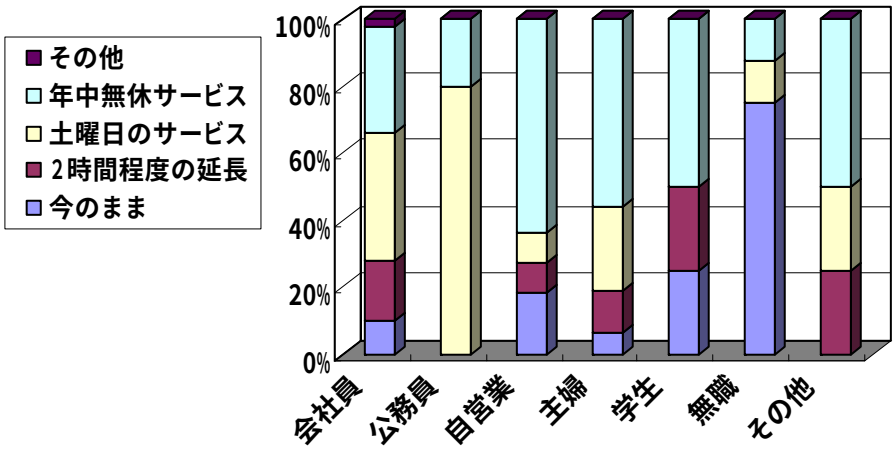


図 3-28 e!市役所のサービス時間について（職業別傾向）

無職の人では「今のままでよい」という割合が 1 番多かったものの、そのほかでは、休日でのサービスを求める割合が多かった。

次に、総合窓口案内から、各担当課へ転送したアクセス数について調査した。総合窓口案内で対応した回数の 187 回のうち、各担当課（本実験では、市民税課と各保健センター、各福祉事務所、IT ヘルプセンタ）への転送が行われたのは 38 回（約 5 分の 1）であった。また、この 38 回のアクセスについて、モニタが総合窓口案内へアクセスしてから、用件を伝え、該当の担当者へ転送されてつながるまでの時間をとったところ次の結果となった。

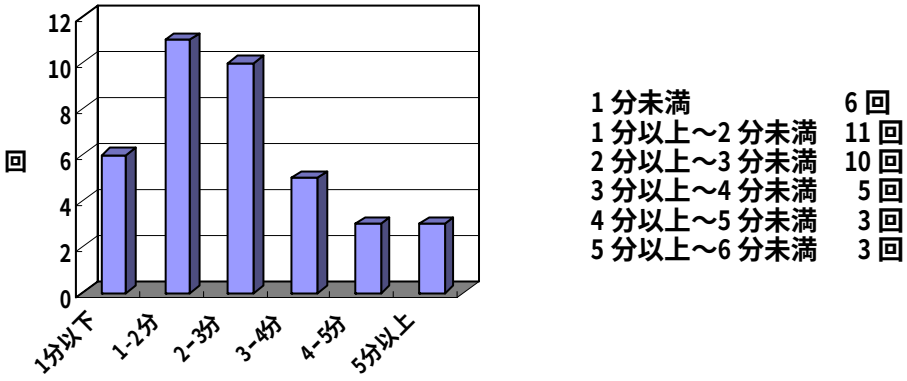


図 3-29 アクセス開始からリルート完了までの時間

総合窓口案内を呼び出して（開始ボタンを押して）から約 7 割が 3 分以内に担当課へ転送が完了している。

なお、最も短いもので 46 秒、最も時間のかかったもので、19 分 53 秒であった。また、全 38 回の平均時間は、約 2 分 52 秒であった。

(3) 映像対話型総合窓口案内システムの操作性

総合窓口案内の担当者へのインタビューを実施（平成 15 年 3 月 10 日）した結果、次のような回答があった。

(i)　着信時について

着信を知らせるベルの鳴る回数としては、鳴りつづけられると困るので、何度か鳴ったらタイムアウトしてしまう方がよい。その場に人がいても、他の対応をしていると出られない場合がある。

携帯電話のように、1 ボタンで、「現在出ることが出来ません」と相手側に出せるようになると便利。

(ii) 転送時について

（他の窓口へ）転送した際にうまくいっているかどうか、最初は不安だった。いまでは、うまくつながらなければまたかけてくるだろうと気にしないことにしている。

電話と同じように保留転送ができればいいと思う。担当課がはっきりしているときは、そのまま転送してしまうが、隣の課だったかどうか曖昧なときには、保留して確認をとって、その課につないでいきたい。

転送の確認を行うために、市民側の端末と同様に転送時だけでなく、待ち受け時にもどこの部署が空いているかが分かればよい。

3.3.7　まとめ（評価）

(1) 映像対話型総合窓口案内サービスの利便性

全体の約 9 割の人が便利だと感じており、映像対話型総合案内窓口サービスは市民にとって利便性の高いサービスであることが分かった。しかし、アンケートの結果より、今後本実証実験を実用化してゆくには、約 7 割の人が土日のサービス又は年中無休サービスを要望していることが分かった。このことから、24 時間 365 日のサービスへ向けた取り組みや、体制づくりに課題があることが分かった。

(2) 映像対話型総合窓口案内サービスの利用特性

市役所の窓口の開いていない時間や日にでもサービスが受けられることを要望する割合が高いことが分かった。

総合窓口案内を利用することで、「開始」ボタンがおされてから 1 分～3 分程度の対話で担当課へ橋渡しをすることができる、ということが分かった。

(3) 総合対話型総合窓口案内システムの操作性

着信時に出られない場合の対処、転送の方法（保留転送機能の必要性）、そして、転送直後における転送完了の確認に課題があることが分かった。