3.1.7. 信頼性確保を前提としたネットワークトポロジーと経路制御方法の検討

3.1.7.1.検証概要

IPv6 マルチキャストにおいても経路の二重化及び、動的な経路切り替えにより高い信頼性のネットワークを検証し、IPv6 マルチキャストを使った通信が頻繁に行われるネットワーク時代の信頼性確保のあり方を検討、評価する。

3.1.7.2.検証の目的

ネットワークにおいては、回線切断やルータ異常など様々な障害が考えられる。万が一このような障害が発生しても一時的な障害にのみに限定するために経路やルータを 2 重化すれば、どちらかの経路に異常が発生しても、もう一方の経路によりアクセスが可能となる。

「e!School ネットワーク」においては、市庁舎と教育センタを結ぶ回線が二重化されている。ネットワーク図（図 3.1.1）のように、市庁舎の IX5005 ルータは教育センタの IX5005 ルータと GR ルータの両方の接続されている。市庁舎 IX5005 ルータは RIPng(IPv6)と OSPF(IPv4)で動的に経路選択が行われるように設定されている。このため、どちらかの回線を切断すれば、自動的に接続されている回線に経路が設定されるはずである。本検証では回線切断時に動的な経路切り替えが正しく行われるかどうか、またそれが使用しているアプリケーションにどの程度影響するかを調査することを目的としている。

3.1.7.3.検証項目

市庁舎には「VOD サーバ」と「IPv6 ビデオ会議サーバ」が設置されている。このため三鷹ポータル及び、TV 会議を実行中に市庁舎 IX5005 ルータと教育センタ IX5005 ルータを結ぶ回線または市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を切断すれば、経路の切り替えの確認とコンテンツ再生ならびに TV 会議への影響を検証できる。

検証方法と評価基準を以下に示す。

表 3.1.23　検証 6 の検証内容と評価基準

項目	検証内容	評価基準
ア)	経路切り替え時のアプリケーションレベルでの動作状況確認	現用系経路切断時にネットワーク機器が、敏速にもう一方の経路に切り替わり、通信が再開されること。切り替え後もアプリケーションレベルで正常な映像受信動作が行われること。切り替え時にネットワーク機器及び、サーバ・クライアントが安定して動作していること。切断した経路を復旧させた後に、もう一度現用系経路を切断しても正常に経路切り替えが行われること。
イ)	ネットワーク機器の通信状態確認	実際にルータのルーティングテーブルが書き変わっていること。
ウ)	ネットワーク機器の経路伝播動作時間の確認	経路が切り替わっても、経路伝播動作時間に変化がないこと。

3.1.7.4. 検証環境

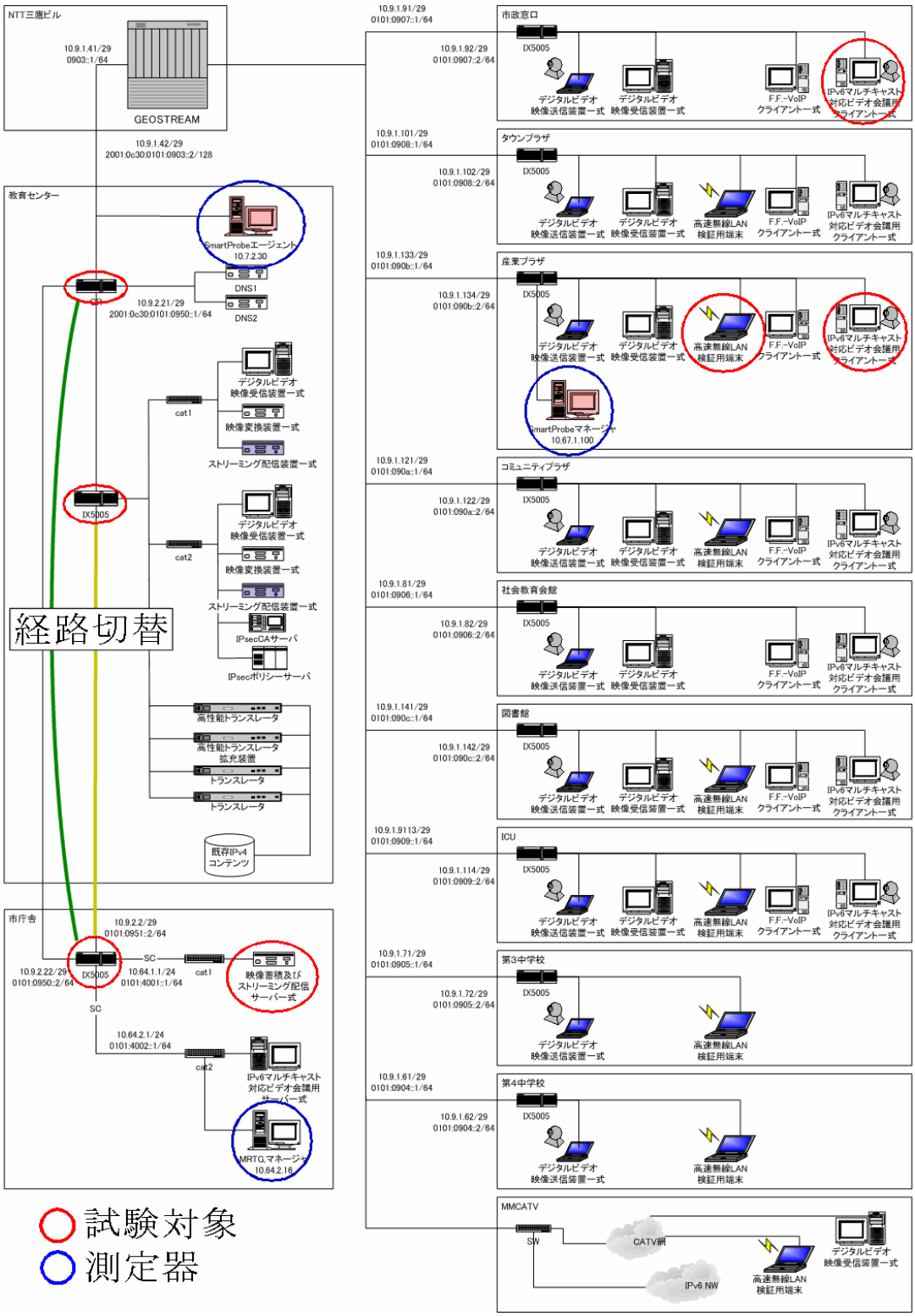


図 3.1.45 試験対象と検証で使用する測定器

3.1.7.5.検証方法と結果

各項目について、検証手順と検証結果を述べる。

3.1.7.5.1.ア）経路切り替え時のアプリケーションレベルでの動作状況確認

(1) 検証方法

①産業プラザと三鷹駅市政窓口にて TV 会議を行った。また、産業プラザ 1F にて無線 LAN 端末を用意し、三鷹ポータルのコンテンツを再生した。

②市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を 5 分間切断する。

③TV 会議が続行可能かどうか、三鷹ポータルのコンテンツ再生が途切れることなく行われているかどうかを確認する。

④市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を接続する。

⑤市庁舎 IX5005 ルータと教育センタ IX5005 ルータを結ぶ回線を 5 分間切断する。

⑥TV 会議が続行可能かどうか、三鷹ポータルのコンテンツ再生が途切れることなく行われているかどうかを確認する。

⑦市庁舎 IX5005 ルータと教育センタ IX5005 ルータを結ぶ回線を接続する。

(2) 検証結果

① 切断前は産業プラザと三鷹駅市政窓口にて TV 会議は正常に可能であった。また、産業プラザ 1F の無線 LAN 端末にて三鷹ポータルのコンテンツは正常に再生可能であった。

② 市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を 5 分間切断すると TV 会議は強制的に退出状態になった。ただし、再度「参加」を実行すると正常に参加できた。三鷹ポータルのコンテンツは途切れることなく再生が続行された。

③ 回線接続後、今度は市庁舎の IX5005 ルータと教育センタの IX5005 ルータを結ぶ回線を 5 分間切断した。TV 会議はそのまま続行可能であった。三鷹ポータルのコンテンツは途切れることなく再生が続行された。今回 TV 会議が切断されなかったのは、接続時の経路が市庁舎 IX5005 ルータと教育センタ GR ルータだったため、回線切断の影響をまったく受けなかったためと思われる。

④ 回線接続後も各アプリケーションの動作は正常であった。

(3) 結論・考察

どちらの経路を切断しても、ＷＭＴコンテンツは途切れることなく再生された。これは Windows Media Player がバッファを持っており（再生の最初にバッファリング中のパーセンテージが表示される)、バッファが空になる前に自動的に再接続が行

われたためと思われる。また、バッファが空になる前に経路の切り替えが完了したことを示している。しかし、TV 会議システムは市庁舎 IX5005 ルータと教育センタ GR ルータを切断した場合、経路が正しく切り替わったにもかかわらず切断されて（退室）しまった。これは TV 会議システムが回線切断により「退室」になる仕様になっているためと思われる。

3.1.7.5.2.　イ）ネットワーク機器の通信状態確認

(1)　検証方法

検証ア）の実行中にルータのルーティングテーブルを調べる

① 産業プラザと三鷹駅市政窓口にて TV 会議を行う。また、産業プラザ 1F にて無線 LAN 端末を用意し、三鷹ポータルのコンテンツを再生する。
② 市庁舎 IX5005 ルータのルーティングテーブルを記録する。
③ 市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を 5 分間切断する。この 5 分間の間に市庁舎 IX5005 ルータのルーティングテーブルを記録する。
④ 市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を接続し、市庁舎 IX5005 ルータのルーティングテーブルを記録する。
⑤ 市庁舎 IX5005 ルータと教育センタ IX5005 ルータを結ぶ回線を 5 分間切断し、この 5 分間の間に市庁舎 IX5005 ルータのルーティングテーブルを記録する。
⑥ 市庁舎 IX5005 ルータと教育センタ IX5005 ルータを結ぶ回線を接続し、市庁舎 IX5005 ルータのルーティングテーブルを記録する。

(2)　検証結果

切断前の市庁舎 IX5005 ルータの RIPng ルーティングテーブルを表 3.1.24 に示す（一部のみ）。Vlan_1 と vlan_4 の両方にルーティングされている。

表 3.1.24　切断前の市庁舎 IX5005 ルータの RIPng ルーティングテーブル

Type	Destination/Prefixlen	[Priority/Metric]	Age	Nexthop
RIPng	::/0	[400/3]	40	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:100::/64	[400/2]	40	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:702::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
	fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:703::/64	[400/2]	40	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:704::/64	[400/2]	40	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:707::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:708::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:709::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70a::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70b::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70c::/64	[400/2]	10	

切断中の 5 分の間の市庁舎 IX5005 ルータの RIPng ルーティングテーブルを表 3.1.25 に示す。すべて経路が vlan_4 に切り替わっている。

表 3.1.25　切断中の 5 分の間の市庁舎 IX5005 ルータの RIPng ルーティングテーブル

Type	Destination/Prefixlen	[Priority/Metric]	Age	Nexthop
Delete	::/0	[1000/16]	300	
RIPng	2001:c30:101:100::/64	[400/3]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:702::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:703::/64	[400/3]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:704::/64	[400/3]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:707::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:708::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:709::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70a::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70b::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70c::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70d::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70f::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:710::/64	[400/2]	20	
	via fe80::200:4cff:fee0:581d@vlan_4			

市庁舎IX5005ルータと教育センタGRルータの回線を接続後のIX5005ルータのRIPルーティングテーブルを表 3.1.26 に示す。Vlan_1 と vlan_4 の両方にルーティングされている。

表 3.1.26　回線を接続後の IX5005 ルータの RIPng ルーティングテーブル

Type	Destination/Prefixlen	[Priority/Metric]	Age	Nexthop
RIPng	::/0	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:100::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:702::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
	fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:703::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:704::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:707::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:708::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:709::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70a::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70b::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70c::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			

今度は市庁舎の IX5005 ルータと教育センタの IX5005 ルータを結ぶ回線を 5 分間切断した。切断中の IX5005 ルータの RIPng ルーティングテーブルを表 3.1.27 に示す。すべて経路が vlan_1 に切り替わっている。

表 3.1.27　切断中の IX5005 ルータの RIPng ルーティングテーブル

Type	Destination/Prefixlen	[Priority/Metric]	Age	Nexthop
RIPng	::/0	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:100::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:702::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:703::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:704::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:707::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:708::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:709::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:70a::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:70b::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:70c::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:70d::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:70f::/64	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			

再度回線接続後の IX5005 ルータの RIPng ルーティングテーブルを表 3.1.28 に示す。経路が vlan_1 と vlan_4 に戻っている。

表 3.1.28　再度回線接続後の IX5005 ルータの RIPng ルーティングテーブル

Type	Destination/Prefixlen	[Priority/Metric]	Age	Nexthop
RIPng	::/0	[400/3]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:100::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:702::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
	fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:703::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:704::/64	[400/2]	10	
	via fe80::240:66ff:fe10:d846@vlan_1			
RIPng	2001:c30:101:707::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:708::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:709::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70a::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70b::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70c::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			
RIPng	2001:c30:101:70d::/64	[400/2]	10	
	via fe80::200:4cff:fee0:581d@vlan_4			

このように市庁舎 IX5005 ルータのルーティングテーブルは切断中されると接続されている回線に切り替わることが確認できた。

(3) 結論・考察

RIPng といった動的ルーティングを用いることにより、回線切断時に自動的に経路がきり代わり、バックアップ回線が使用される。経路の二重化は信頼性向上に有用である。

3.1.7.5.3. ウ）ネットワーク機器の経路伝播動作時間の確認

(1) 検証方法

① 産業プラザと三鷹駅市政窓口にて TV 会議を行う。また、産業プラザ 1F にて無線 LAN 端末を用意し、三鷹ポータルのコンテンツを再生する。
② この状態で各拠点から市庁舎 IX5005 ルータ及び、教育センタ GR ルータ及び、教育センタ IX5005 ルータへの PING の応答時間を計測する。
③ 市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を 5 分間切断する。
④ 各拠点から市庁舎 IX5005 ルータへの PING の応答時間を計測する。
⑤ 市庁舎 IX5005 ルータと教育センタ GR ルータを結ぶ回線を接続する。
⑥ 各拠点から市庁舎 IX5005 ルータへの PING の応答時間を計測する。
⑦ 市庁舎 IX5005 ルータと教育センタ IX5005 ルータを結ぶ回線を 5 分間切断する。
⑧ 各拠点から市庁舎 IX5005 ルータへの PING の応答時間を計測する。
⑨ 市庁舎 IX5005 ルータと教育センタ IX5005 ルータを結ぶ回線を接続する。
⑩ 各拠点から市庁舎 IX5003 ルータへの PING の応答時間を計測する。

(2) 検証結果

表 3.1.29 検証中の市役所 IX5003 ルータへの PING 応答時間の変化

	産業プラザからの PING 到達時間	三鷹駅市政窓口からの PING 到達時間
教育センタ GR ルータ切断前	2～3ms	6～7ms
教育センタ GR ルータ切断中	2～3ms	6～8ms
教育センタ GR ルータ接続	2～3ms	6～8ms
教育センタ IX5005 ルータ切断中	2～3ms	6～10ms
教育センタ IX5005 ルータ接続	2～~3ms	7～9ms

(3) 結論・考察

回線の経路切替が行われても伝播時間に大きな変化はないと考えられる。

3.1.7.6.まとめ

経路が二重化されている場合、どちらかの回線に障害が発生しても自動的に経路の切り替えが行われた。切り替わった様子は市庁舎 IX5005 ルータのルーティングテーブルを確認することで検証された。経路切り替え時 Windows Media Player は途切れることなく再生された。TV 会議は経路切り替え時強制的に「退出」になった。ただし、再度「参加」を実行すれば問題なく続行可能である。経路切り替え終了後は、アプリケーションは問題なく動作した。

Windows Media Player が途切れることなく再生されたのはバッファを持っているからだと考えられる（再生の最初にバッファリング中のメッセージあり）が、バッファといっても、分単位ではなく秒単位のオーダーであると思われ、ルーティングテーブルの書き換えは１分以内に完了していると思われる。

RIPng が経路情報を交換する際には、隣接するネットワークへ 30 秒ごとにレギュラー・アップデート（更新メッセージ）をブロードキャストする。同様に、隣接するネットワークのほかのルータから 30 秒ごとにレギュラー・アップデートを受信する。その際に、あるルータから 180 秒以内にレギュラー・アップデートなどを受信しなかった場合、その相手先ルータにおける障害発生、または、そこに接続されたネットワークが無効になったと見なし、これに該当する経路情報が無効化される（レギュラー・アップデートは 30 秒ごとに送受信されるため、6 回続けて受信できなかった場合が 180 秒となり、これに該当する経路情報が無効化される)。さらにこのように無効になった経路がルーティングテーブルから削除までには、ガベージコレクションタイマと呼ばれる 120 秒の期間が必要になる。したがって、通常は経路情報の書き換えには 5 分が必要である。しかし、これは、ルータ本体に異常が発生した場合であり、今回の回線切断の場合は Link がはずれたため、トリガアップデート機能により経路情報の定期的なアップデート周期を待たずに、更新情報を伝達できたのではないかと推測される。今回の検証では IPv6 の動的ルーティングプロトコルとして RIPng を使用したが、OSPFv3 を使用した場合も Link 切断によりリンクステートが敏速に伝達され、SPF（Shortest Path First）の再計算が行われたのではないかと推測される。ルータ数 2000 のネットワークでの SPF 計算時間は、実測値の最大を用いた試算でも 410 msec 程度、平均を用いた試算では 210 msec 程度となっており、比較的短時間の経路切り替えが可能である。今後より障害に強く、信頼性の高いネットワーク構築を目指して OSPFv3 を用いた経路切り替えの検証やより正確な経路切り替え時間の測定や検証などが必要であろう。

このように経路を二重化することにより、障害に強いネットワークが構築できることが確認された。IPv6 マルチキャストにおいては、UDP でパケットが送信され TCP によるエラー制御が行われないため、障害に強く、信頼性の高いネットワークを構築することはきわめて重要である。

表 3.1.30　検証内容と検証結果まとめ

項目	検証内容	検証結果
ア)	経路切り替え時のアプリケーションレベルでの動作状況確認	経路切り替え時 Windows Media Player は途切れることなく再生された。TV 会議は経路切り替え時強制的に「退出」になった。ただし、再度「参加」を実行すれば問題なく続行可能である。経路切り替え終了後は、アプリケーションは問題なく動作した。
イ)	ネットワーク機器の通信状態確認	ルーティングテーブルが正しく切り替わった。
ウ)	ネットワーク機器の経路伝播動作時間の確認	どちらの経路に切り替わっても経路伝播動作時間に大差は認められなかった。

3.1.8. IPv4 コンテンツを有効利用するためのトランスレート機器の検証及び、評価

3.1.8.1.検証概要

既存の IPv4 コンテンツを IPv6 対応にするための方法として、IPv6 クライアントからのパケットを IPv4 にトランスレートする方法があるが、より効率的に既存コンテンツを IPv6 対応にするための検討と評価を行う。

3.1.8.2.検証目的

平成 13 年度に通信・放送機構が整備した「学校インターネットにおける教材拡充施設整備（三鷹)」における教材拡充施設装置は、学校インターネットにおける教材拡充装置 A、学校インターネットにおける教材拡充装置 B、学校インターネットにおける教材拡充装置 C､学校インターネットにおける教材拡充装置 D､利用者学習履歴参照ソフトウェア、ドリル HTML 教材コンテンツ、ドリル HTML 教材用学習コンテンツ、ポイント HTML 教材コンテンツ、シミュレーション教材コンテンツ、ぼくらの昆虫探検記 HTML コンテンツ、クイッククイズ HTML コンテンツで構成される。

「e!School ネットワーク」では IPv6 ネットワークで構築されている。このネットワーク内は IPv6 環境であり、そのままでは IPv6 クライアントは外部の既存の IPv4 インターネットコンテンツやこれらのコンテンツにはアクセスできない。しかし、コンテンツの基本的な処理は、http プロトコルを用いており WWW サーバ上のコンテンツであることから、IPv4 -> IPv6 のトランスレータにて対応している。トランスレータは 2 台用い、トランスレートが正しく行われ､2 台のトランスレータで負荷分散が行われることを検証するのが目的である。

3.1.8.3.検証項目

既存の IPv4 コンテンツを正常にアクセスできるか、また、2 台のトランスレータに負荷分散が行われているかどうかを検証する。

本検証の検証内容と評価基準を表 3.1.31 にまとめる。

表 3.1.31　検証 7 の検証内容と評価基準

項目	検証内容	評価基準
ア)	アプリケーションレベルでコンテンツ配信が正常に動作することを確認	クライアントにおいて、アプリケーションレベルでコンテンツ配信が正常に行われること。
イ)	様々な既存コンテンツにアクセスし、IPv4 のクライアントと同様に動作するか確認する。	様々なコンテンツが正常にトランスレートされていること。
ウ)	クライアントの数を増やした場合のトランスレータの動作状態を確認する。	トランスレータに高負荷をかけても正常にトランスレートしていること。
エ)	トランスレータを冗長構成にした場合の負荷分散効率をネットワーク上とのトラフィック測定により確認する。	トランスレータを冗長構成にすることにより、トラフィック量が一定の割合で分散されていること。

3.1.8.4. 検証環境

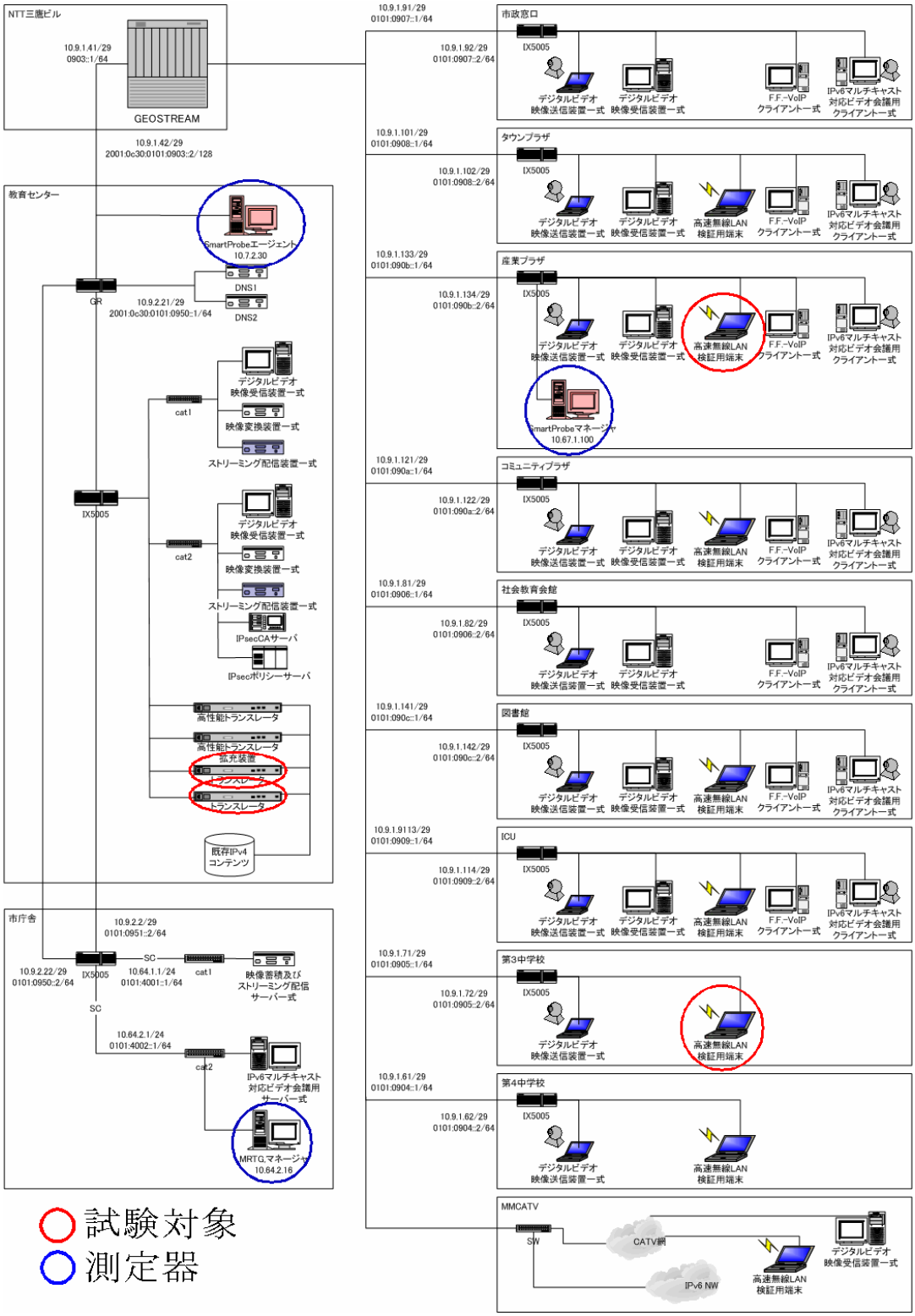


図 3.1.46 試験対象と検証で使用する測定器

3.1.8.5. 検証方法と結果

各項目について、検証手順と検証結果を述べる。

3.1.8.5.1.　ア）アプリケーションレベルでコンテンツ配信が正常に動作することを確認

(1)　検証方法

第三小学校にて既存のコンテンツ「デジタルムービーパーク」をアクセスし正常に表示されることを確認する。

(2)　検証結果

正常に表示された。実際にフィールドで動作している様子が図 3.1.47 である。

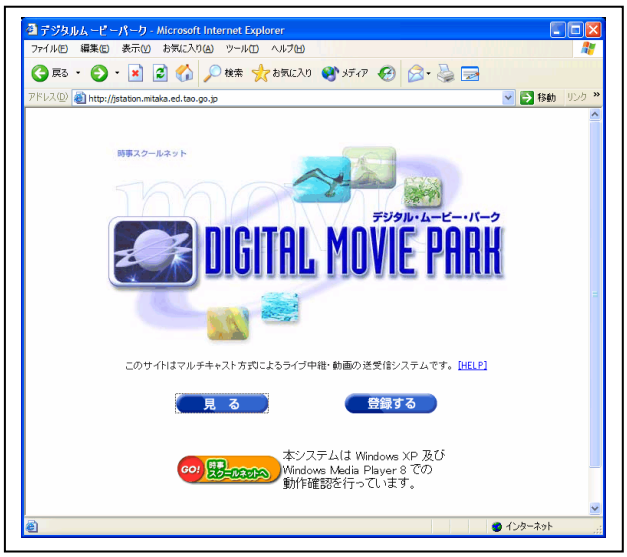


図 3.1.47　正常に表示されている「デジタルムービーパーク」

(3)　結論・考察

クライアントにおいて、アプリケーションレベルでコンテンツ配信が正常に行われる。

3.1.8.5.2.　イ）様々な既存コンテンツにアクセスし、IPv4 のクライアントと同様に動作するか確認する。

(1)　検証方法

第三小学校にて下記の既存のコンテンツにアクセスし正常に表示されることを確認する。産業プラザにおいて下記のコンテンツにアクセスし正常に表示されることを確認する。

- http://www.education.ne.jp/　ネットクラスルーム
- http://jstation.mitaka.ed.tao.go.jp/　デジタルムービーパーク
- http://edu.mitaka.ed.tao.go.jp/jiji/　　時事スクールネット
- http://edu3.mitaka.ed.tao.go.jp ポケット 2
- http://www.education.ne.jp/mitaka/sansho-es/　三鷹市第三小学校

(2)　検証結果

正常に表示された。実際にフィールドで動作している様子が図 3.1.48 である。

図 3.1.48　正常に表示されている様々なコンテンツ

(3)　結論・考察

様々なコンテンツが正常にトランスレートされている。

3.1.8.5.3.　ウ）クライアントの数を増やした場合のトランスレータの動作状態を確認

(1)　検証方法

① トランスレータにログを出力するように設定しておく

② 少なくても 1 週間以上ログを記録する

③ ログを回収し、クライアントの数が 10 台以上でもエラーが発生せず正しくトラン

スレートしていることを確認する

(2) 検証結果

ログを解析してトランスレータの変換数へ直したものが図 3.1.49 である。

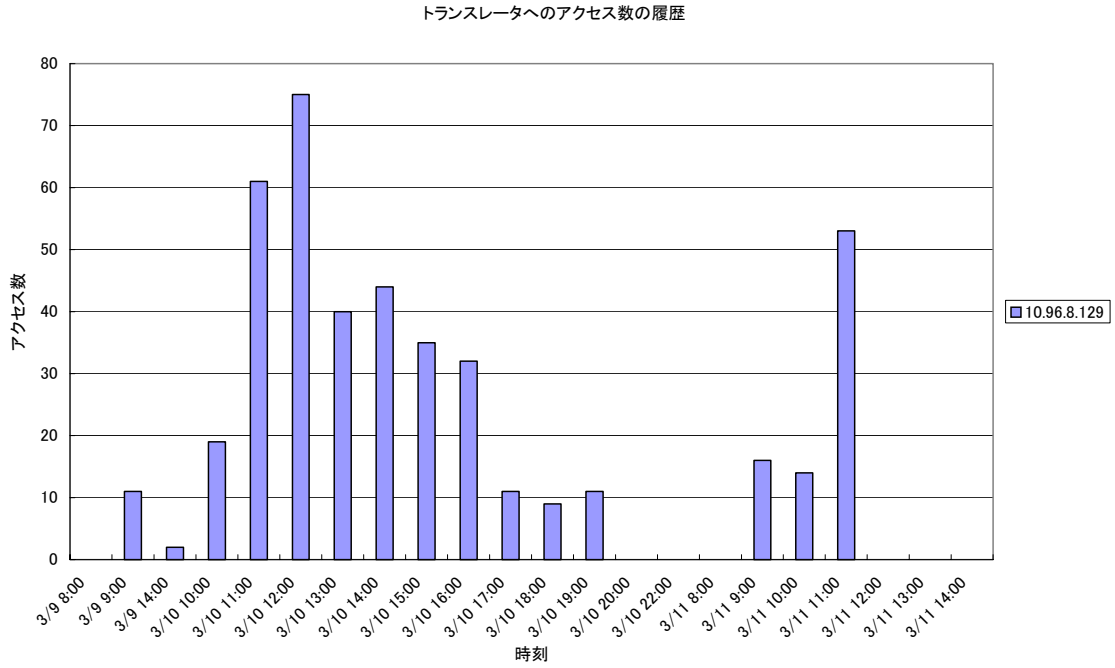


図 3.1.49　トランスレータの変換数の変化

ログには正常にトランスレートされた場合、例として下記のように記録される。

```
Mar  9 08:43:32 10.96.8.130 ttbd http/tcp[28738]: starting http/top relay
Mar  9 08:43:32 10.96.8.130 ttbd http/tcp[28739]: accepted a client from
2001:c30:101:ff02:207:40ff:fe4e:7d3b
Mar  9 08:43:32 10.96.8.130 ttbd http/tcp[28739]: the client is connecting to
2001:c30:101:801::3dcb:fe64
Mar  9 08:43:32 10.96.8.130 ttbd http/tcp[28739]: translating from v6 to v4
Mar  9 08:43:32 10.96.8.130 ttbd http/tcp[28739]: the translator is connecting
to 61.203.254.100
```

エラーが発生した場合、例として下記のように記録される。この例はログを書き込むディスクが full になり、ログが記録できなくなったことを表している。

```
Mar 11 12:22:30 10.96.8.130 last message repeated 74 times
Mar 11 12:22:30 10.96.8.130 /kernel: pid 96382 (sh), uid 0 on /var: file system
full
```

図 3.1.49 をみると 3/10 にアクセス数が増大しているが、ログ上ではこのようなエラーは記録されていなかった。以上のことからアクセス数が増大しても正しくトンランスレートしていると考えられる。

ただしエラーの例のように 11 日にはディスク full になりエラーが発生している。図 3.1.49 見るとトランスレートの数とは相関はなくそのときまでの大量のログによりディスクに書き込めなくなったためであり、トランスレートの性能そのものとは関係がないと考えられる。

(3) 結論・考察

アクセス数が増大しても正しくトンランスレートしていると考えられる。ただし、より大量のアクセスが発生しても正しくトランスレートするかどうかは、今後検証を続ける必要があると思われる。

3.1.8.5.4. エ) トランスレータを冗長構成にした場合の負荷分散効率をネットワーク上とのトラフィック測定により確認する

(1) 検証方法

MRTG にてトランスレータ 2 台の入出力トラフィックを記録する。負荷分散が 1:1 で効率的に行われていれば、2 台のトランスレータの入出力トラフィックはほぼ同等になるはずである。

(2) 検証結果

図 3.1.50 は教育センタに設置している 2 台のトランスレータの入力トラフィックを比較したものである。ほぼ同じトラフィック量が測定されており、効率的に負荷分散が行われていると考えられる。

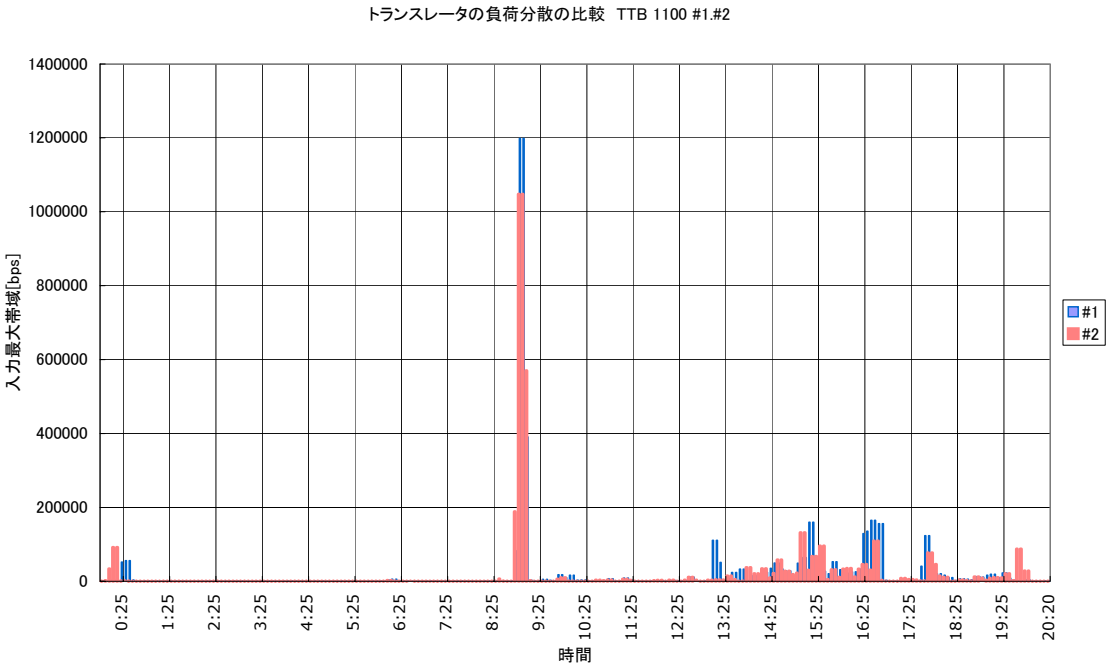


図 3.1.50　トランスレータ 1 とトランスレータ 2 の入力トラフィック

(3)　結論・考察

2 台のトランスレータにおいて効率的に負荷分散が行われていると考えられる。ただし、詳しく見てみているとトランスレータ 1 の方のトラフィックが多い。これは、DNS サーバとのやり取りに原因があると考えられる。IPv6 ホストのユーザがブラウザにアドレスを入力すると、ブラウザはこのホスト名から IP アドレスを得るために DNS サーバに問い合わせを行う。DNS サーバは IPv4 アドレスの場合、必ずトランスレータ 1 に処理を依頼する。トランスレータ 1 は名前解決のため、既存の IPv4 アドレスの内部にある DNS サーバからアドレスを取得し、それに IPv6 のダミープレフィックを付加しクライアントに返す。この際、付加するダミープレフィックスはトランスレータ 1 に割り当てられたアドレスとトランスレータ 2 に割り当てられたアドレスをラウンドロビン方式により交互に付加する。これによりクライアントはトランスレータ 1 と 2 を交互に使用することになり、付加分散が行われるが、最初の名前解決の際は必ずトランスレータ 1 をアクセスすることになる。このため、MRTG の入力トラフィックはトランスレータ 1 の方が高めに出ると思われる。

3.1.8.6.まとめ

IPv6 の普及過程においては、かならず IPv6 ネットワークと IPv4 ネットワークの共存が必要である。IPv6 ネットワークと IPv4 ネットワークを接続する場合、本検証のようにトランスレータにて変換するという手法が有用であることがわかった。これにより同時にすべての部分を IPv6 に置き換える必要はなく、コストの面でも利点である。ただし、現状の「e!School ネットワーク」では問題がないが、クライアントの数が膨大になると、トランスレータに負荷をかけることになるため、比較的小規模の IPv6 ネットワークから外部の IPv4 ネットワークへのアクセスにおいて有用であると考えられる。

表 3.1.32　検証内容と検証結果まとめ

項目	検証内容	検証結果
ア)	アプリケーションレベルでコンテンツ配信が正常に動作することを確認	クライアントにおいて、アプリケーションレベルでコンテンツ配信が正常に行われる。
イ)	様々な既存コンテンツにアクセスし、IPv4 のクライアントと同様に動作するか確認する。	様々なコンテンツが正常にトランスレートされている。
ウ)	クライアントの数を増やした場合のトランスレータの動作状態を確認する。	トランスレータに高負荷をかけても正常にトランスレートされていた。
エ)	トランスレータを冗長構成にした場合の負荷分散効率をネットワーク上とのトラフィック測定により確認する。	トランスレータを冗長構成にすることにより、トラフィック量が一定の割合で分散されていることがわかった。

3.1.9. 異機種間での IPsec を用いた通信接続検証

3.1.9.1.検証概要

IPsec ポリシーサーバによって管理された異種端末に対して、IPsec クライアントがアクセス制御を行うことを確認する。

3.1.9.2.検証目的

IPv6 は、セキュリティ機能である IPsec をプロトコルレベルでサポートしており、その規定は RFC2401 などで定められている。IPsec を用いた通信には、暗号化と認証・改ざん検出を行う ESP と AH の二つの Security Protocol がある。

AH は、パケット全体の認証と再送検出を行うがパケットの暗号化は行わない。ESP は、ペイロードの認証・再送検出と暗号化を行う。

また、エンドエンドでの通信を暗号化するトランスポートモードと、中継ノード間での暗号化を行うトンネルモードの 2 つのモードが用意されている。また、暗号化とともに重要なのが復号に使うための鍵の交換である。不特定多数の送信において、鍵の共有に必要なプロトコルが必要であり、その鍵交換プロトコルが IKE である。

IKE では、鍵と暗号アルゴリズムの合意や鍵交換セッション自体の安全性を考慮して鍵交換を行う。また、認証の方式は「事前に秘密共有」するほかに、「署名を用いた認証」、「公開鍵による暗号化機能を用いた認証 (PKI)」の 3 種類ある。

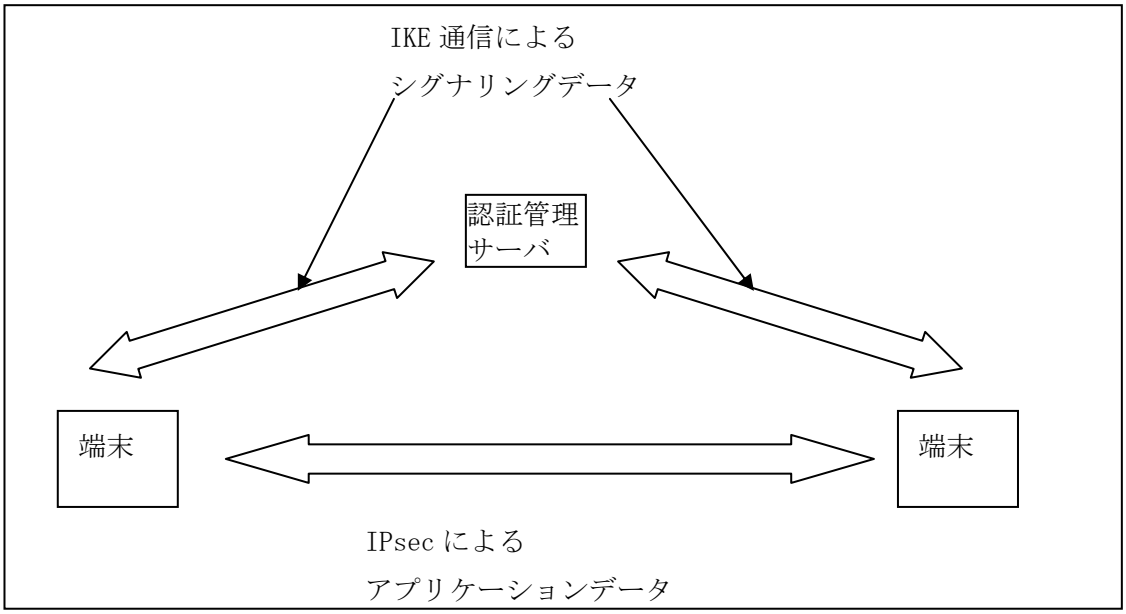


図 3.1.51　IPsec の鍵交換

「e!School ネットワーク」のクライアント・アプリケーションの多くは、認証及び IPsec による暗号化を用いて、セキュリティを確保している。IPsec クライアントソフトは、ユーザの PC から IPsec ポリシーサーバにアクセスし、ポリシー設定に従った認証を受ける。認証に成功したクライアントは通信が許可され、暗号化通信が可能となる。また、認証に失敗したクライアントは、通信することが出来ない。

「e!School ネットワーク」では、教育センタに設置された IPsec ポリシーサーバにより認証を行う。ストリーム配信アプリケーションを用いて、IPsec ポリシーサーバ及び IPsec クライアントのログを確認するとともに、ネットワークを流れるパケットを解析し、正しく認証が行われているかを検証する。

3.1.9.3.検証項目

図 3.1.52　検証 8 の検証内容と評価基準

項目	検証内容	評価基準
ア)	IPsec クライアントにおけるストリーミングアプリケーションの受信状況の確認	IPsec ポリシーサーバの設定に従い実際のストリーム配信アプリケーションが動作可能であったか。
イ)	アナライザによるホスト間の通信状況の確認	アナライザの結果から実際に IPsec 通信が行われていたか。
ウ)	IPsec ポリシーサーバにおける通信ログの確認	正常に通信されたログが残っていたか。
エ)	IPsecCA サーバにおける通信ログの確認	正常に通信されたログが残っていたか。
オ)	非 IPsec クライアントから接続要求があった場合のアプリケーションの動作状況と IPsec ポリシーサーバの通信ログの確認	非 IPsec クライアントからの要求を拒否し、実際にそのログが IPsec ポリシーサーバに残っていたか。

3.1.9.4. 検証環境

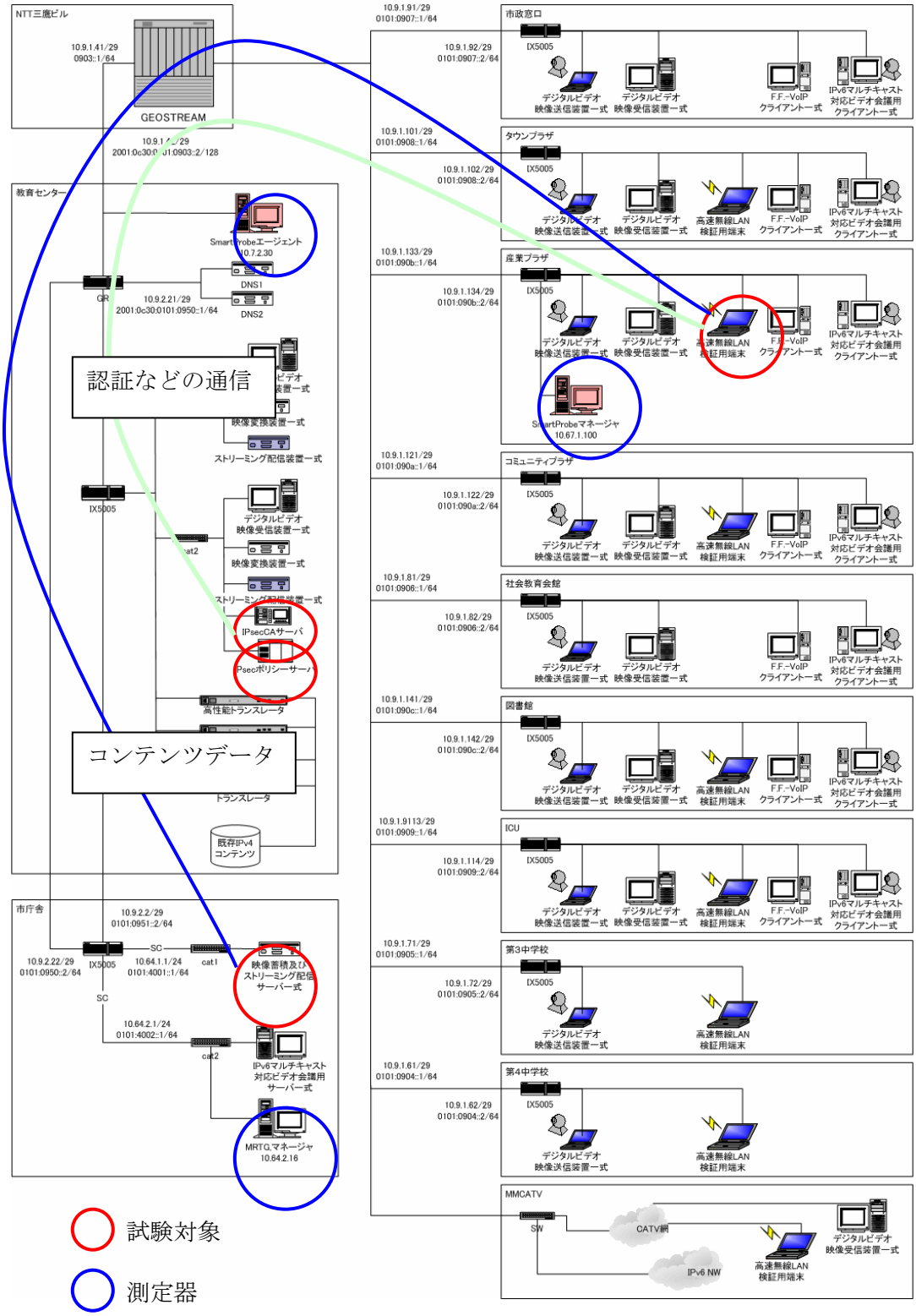


図 3.1.53　試験対象と検証で使用する測定器

3.1.9.5.検証方法と結果

3.1.9.5.1.　ア）IPsec クライアントにおけるストリーミングアプリケーションの受信状況の確認

(1)　検証方法

「三鷹ポータル」は、IKE による鍵交換及び、IPsec による認証・暗号化の機能を持つポータルサイトである。「e!School ネットワーク」では、このポータルサイトにログインし、各コンテンツを利用することにより、セキュリティを確立している。本検証ではこのポータルサイトにログインし、コンテンツを閲覧することにより確認を行う。

① 教育センタに設置されたポリシーサーバにユーザの情報を登録する。
② クライアントで CA サーバから証明書をダウンロードする。
③ 産業プラザのクライアントから Web ブラウザを用いて「三鷹ポータル」の画面を開く。
④ 「コミュニティ」から 1.で登録したユーザ及びパスワードを用いて、産業プラザから「三鷹ポータル」の映像コンテンツの再生を行う。

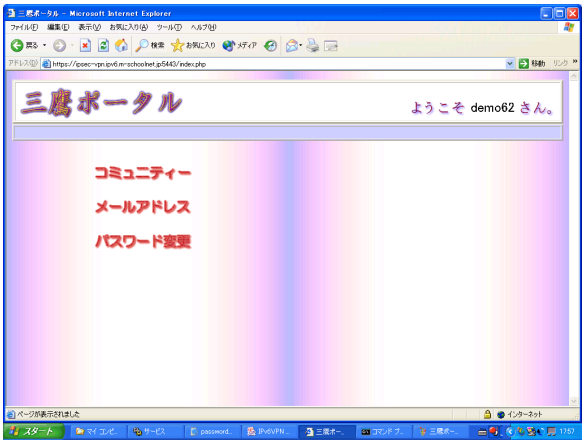
(2)　検証結果

ユーザ及び、パスワードでログインできた。

「三鷹ポータル」ログイン画面：

この画面でアカウントの認証を行う。

図 3.1.54　「三鷹ポータル」ログイン画面

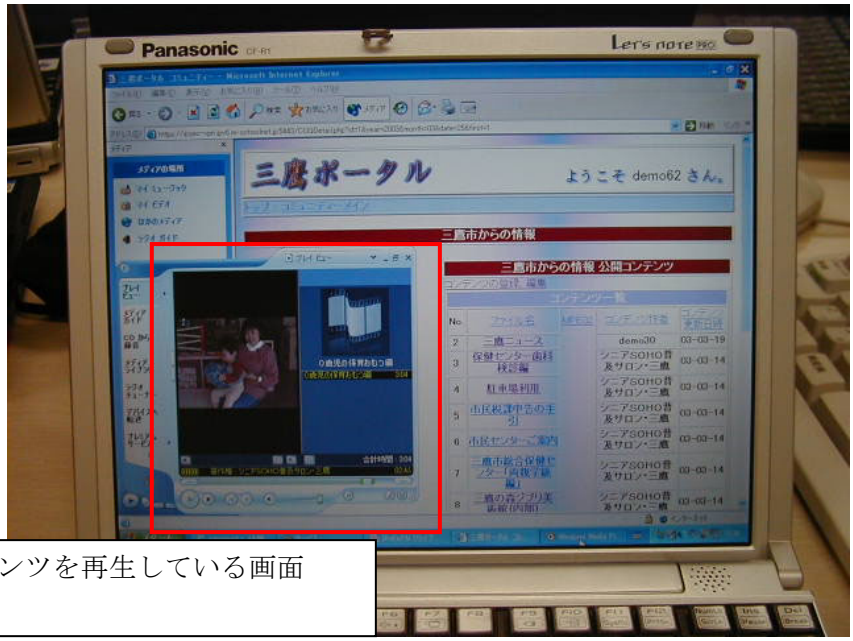


「三鷹ポータル」メイン画面：

認証に成功すると、左の画面に切り替わる。

図 3.1.55 「三鷹ポータル」メイン画面

「三鷹ポータル」の映像コンテンツが再生された。



コンテンツを再生している画面

図 3.1.56 「三鷹ポータル」映像コンテンツ再生の様子

(3) 結論・考察

IPsec ポリシーサーバに登録したアカウントで「三鷹ポータル」にログインし、IPsec クライアントにおけるストリーミングアプリケーションの受信を確認できた。

3.1.9.5.2. イ）アナライザによるホスト間の通信状況の確認

(1) 検証方法

本検証では、クライアントが認証を行っている様子をパケットレベルで確認する。具体的には、パケットキャプチャソフトを利用して、クライアントの通信パケットを取り出し、解析を行う。

パケットのキャプチャには、フリーのパケットキャプチャライブラリである WinPCAP (3.0.a4) とその上位アプリケーションである Ethereal (0.9.11) を利用した。

UNIX で一般的に広く使われているパケットキャプチャソフトに TCPDUMP がある。TCPDUMP は多くの Linux のディストリビューションで標準的にインストールされている。TCPDUMP で用いられているキャプチャライブラリが libpcap であり、WinPCAP はその Windows 版ある。

通常 OS 及び、ドライバは、Ethernet を流れるパケットのうち、自端末に関係ないパケットは廃棄され、アプリケーションには送信しない。パケットキャプチャなど特別な用途のために、OS 及び、ドライバには無差別モード (プロミスカスモード) が用意されている。これを用いると、他の端末のパケットも受信できるようになる。libpcap では、プロミスカスモードを用いて、アプリケーションにキャプチャパケットを送信するためのライブラリである。

また、Ethereal はパケットをグラフィカルに表示するツールである。MAC、IP、トランスポート、アプリケーションレイヤまでの解析を行い、表示を行う。また、libpcap (WinPCAP) と連携し、パケットキャプチャも行うことが出来る。

本検証では、上記ソフトを使用して書き手順で通信状況の確認を行う。

- 教育センタの IPsec ポリシーサーバにユーザを登録する。
- 産業プラザのクライアント側にパケットキャプチャソフトを挿入して測定を行う。
- クライアントから Web ブラウザで「三鷹ポータル」の画面を開く。
- 「コミュニティ」から(1)で登録したユーザ及びパスワードを用いて、産業プラザから「三鷹ポータル」のコンテンツの再生を行う。
- パケットキャプチャソフトの測定から、IPsec による認証が行われているかを確認する。

(2) 検証結果

IPsec のクライアントとサーバの通信状況をキャプチャしたところ、以下のデータを取得した。

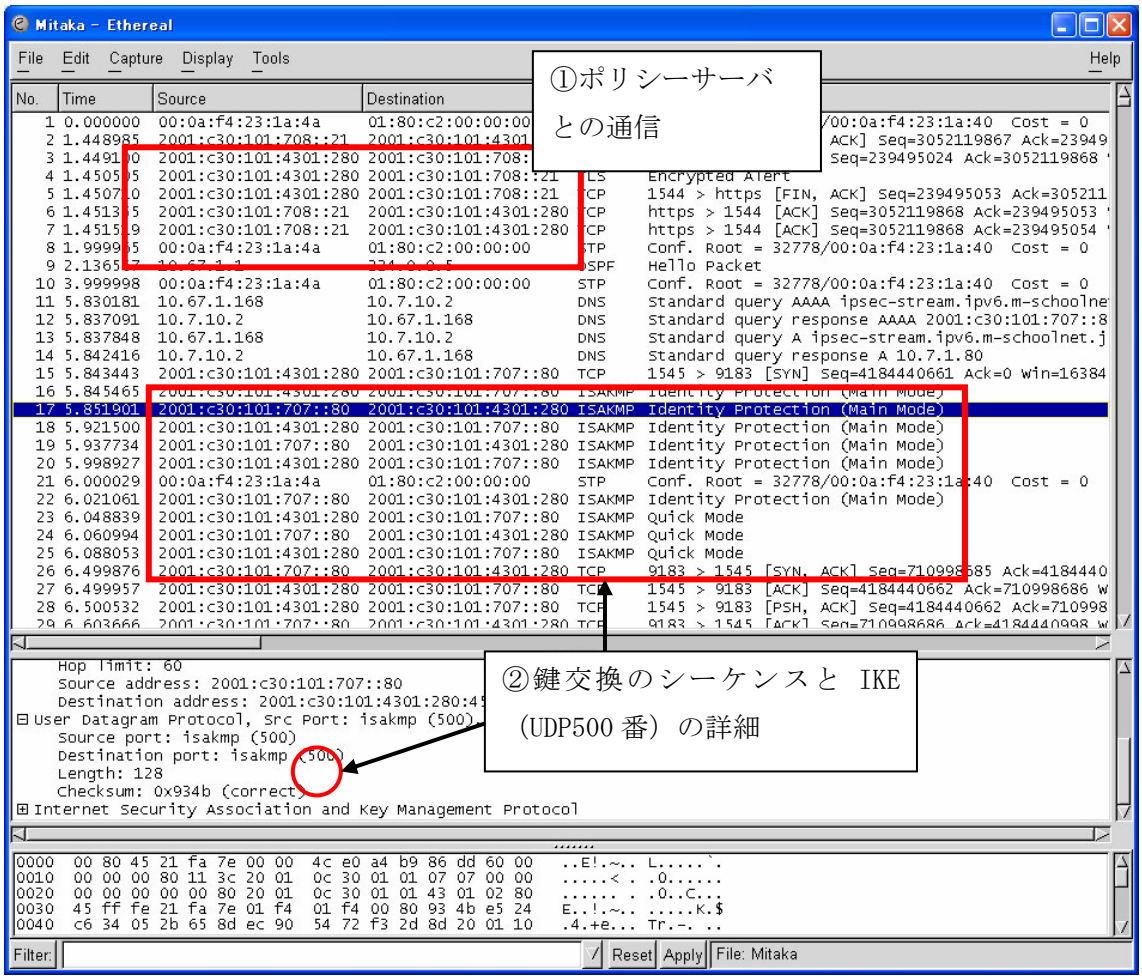


図 3.1.57　IPsec クライアントとサーバの通信状況画面

(3) 結論・考察

はじめに①で、ポリシーサーバと SA (Security Association) をやりとりしている。その後②で、エンドエンド間での鍵交換プロトコル IKE が、制御信号をやりとりするために使用する IKE の制御用チャネル (ISAKMP SA) でネゴシエーションを行っている。

アナライザを用いて、IPsec の通信シーケンスを確認できた。

3.1.9.5.3.　ウ）IPsec ポリシーサーバにおける通信ログの確認

(1)　検証方法

①　教育センタの IPsec ポリシーサーバにユーザを登録する。

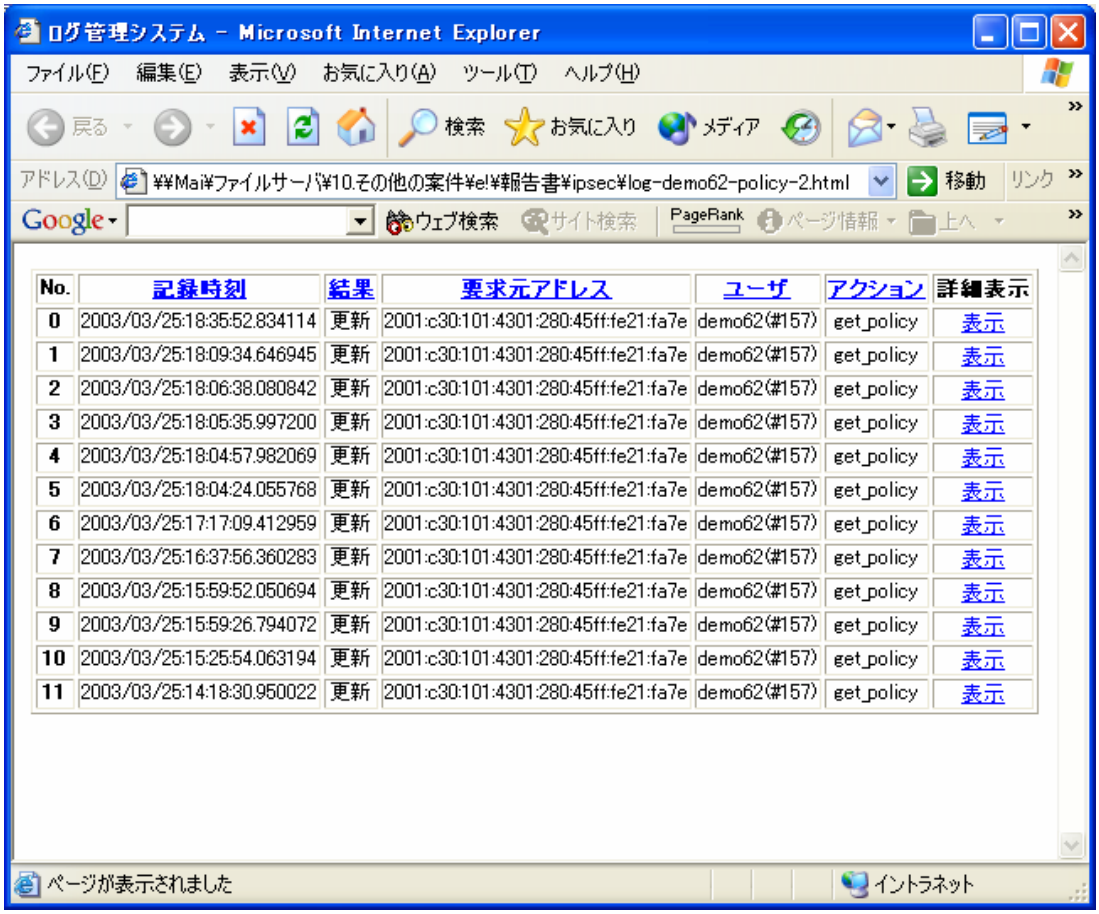
②　産業プラザのクライアントから Web ブラウザで「三鷹ポータル」の画面を開く。

③　「コミュニティ」から(1)で登録したユーザ及びパスワードを用いて、クライアントから「三鷹ポータル」のコンテンツの再生を行う。

④　上記のやり取りの内容を IPsec ポリシーサーバのログにより確認する。

(2)　検証結果

IPsec ポリシーサーバでは、クライアントにポリシーを転送したときのログが以下のように出力された。demo62 でコンテンツのダウンロードを行った際に、ポリシーがダウンロードされているのがわかる。



No.	記録時刻	結果	要求元アドレス	ユーザ	アクション	詳細表示
0	2003/03/25:18:35:52.834114	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
1	2003/03/25:18:09:34.646945	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
2	2003/03/25:18:06:38.080842	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
3	2003/03/25:18:05:35.997200	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
4	2003/03/25:18:04:57.982069	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
5	2003/03/25:18:04:24.055768	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
6	2003/03/25:17:17:09.412959	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
7	2003/03/25:16:37:56.360283	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
8	2003/03/25:15:59:52.050694	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
9	2003/03/25:15:59:26.794072	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
10	2003/03/25:15:25:54.063194	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示
11	2003/03/25:14:18:30.950022	更新	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62(#157)	get_policy	表示

図 3.1.58　ログ管理システム

(3) 結論・考察

IPsec ポリシーサーバの通信ログにより、正常に動作することが確認できた。

3.1.9.5.4. エ）IPsecCA サーバにおける通信ログの確認

(1) 検証方法

① IPsec ポリシーサーバにユーザを登録する。

② CA サーバから証明書をダウンロードする。

③ クライアントから「三鷹ポータル」の画面を開く。

④ 「コミュニティ」から(1)で登録したユーザ及びパスワードを用いて、産業プラザから「三鷹ポータル」のコンテンツの再生を行う。

⑤ 上記のやり取りの内容を IPsecCA サーバのログにより確認する。

(2) 検証結果

CA サーバでは、証明書をダウンロードした履歴を管理する専用のログを持っていない。その代わりとして、クライアントでの証明書の表示を以下に示す。

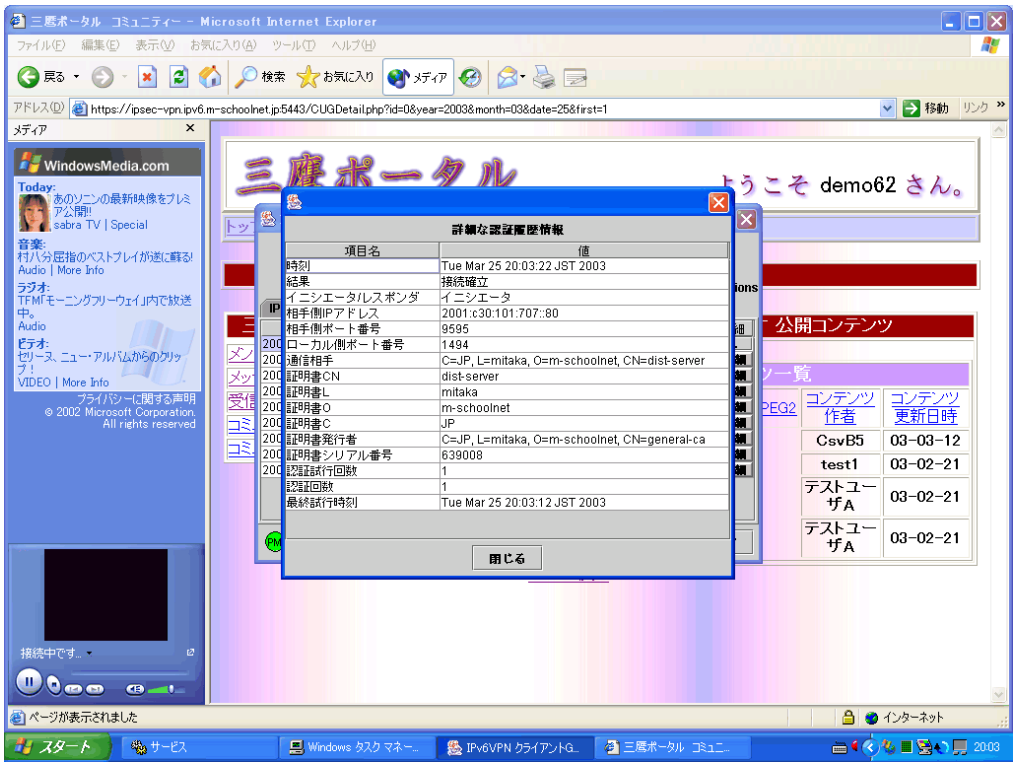


図 3.1.59 クライアントの証明書の設定内容

上の図 3.1.59 から、確かに CA サーバからダウンロードしていることがわかる。

(3) 結論・考察

IPsecCA サーバの通信ログにより、ユーザ認証が正常に動作することが確認が出来なかったが、同等の内容をクライアントのログから確認することができた。

3.1.9.5.5. オ）非 IPsec クライアントから接続要求があった場合のアプリケーションの動作状況と IPsec ポリシーサーバの通信ログの確認

(1) 検証方法

本検証では、IPsec クライアントをインストールしていない端末からアクセスした場合、認証に失敗しコンテンツの閲覧などが出来ないことを確認する。

① 教育センタの IPsec ポリシーサーバにユーザを登録する。

② 産業プラザのクライアントから Web ブラウザで「三鷹ポータル」の画面を開く。

③ 非 IPsec クライアント（IPsec クライアント・アプリケーションを起動せずに）から接続要求を行い、接続できないことを確認する。

④ 上記のやり取りの内容を IPsec ポリシーサーバのログにより確認する。

(2) 検証結果

以下のような画面とログが出力された。

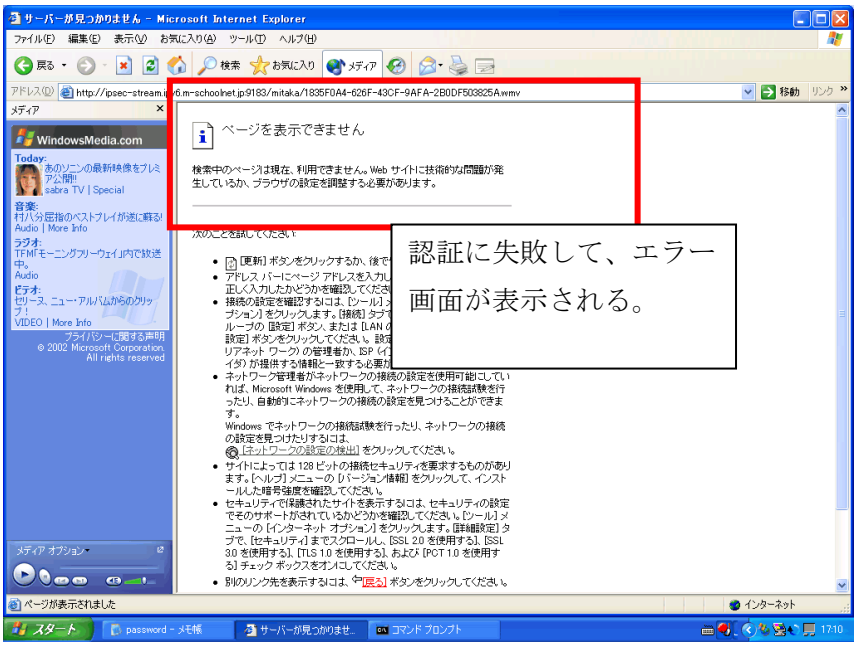


図 3.1.60　認証失敗結果

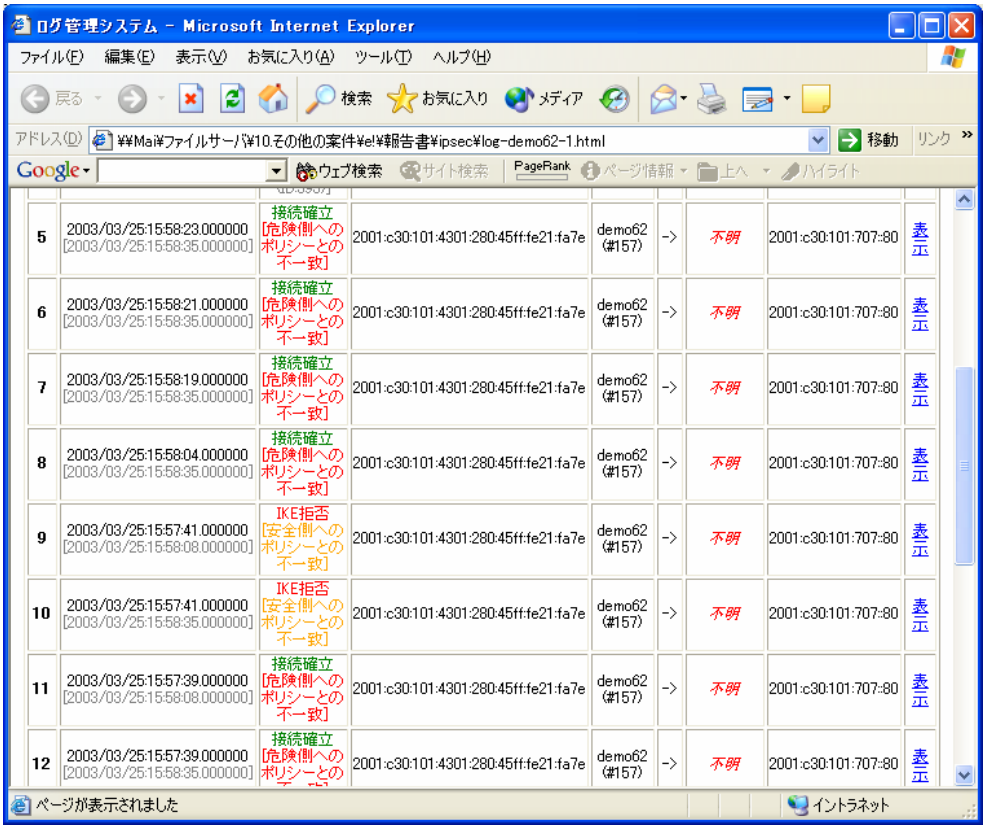


図 3.1.61　ログ管理システム

(3)　結論・考察

非 IPsec クライアントから接続要求があった場合、要求が許可されずに通信できないことが確認できた。

3.1.9.6.まとめ

表 3.1.33　検証内容と検証結果のまとめ

項目	検証内容	結果
ア)	IPsec クライアントにおけるストリーミングアプリケーションの受信状況の確認	IPsec クライアントにおけるストリーミングアプリケーションの受信状況が確認できた。
イ)	アナライザによるホスト間の通信状況の確認	アナライザを用いて、IPsec の通信シーケンスを確認できた。
ウ)	IPsec ポリシーサーバにおける通信ログの確認	IPsec ポリシーサーバの通信ログにより、正常に動作することが確認できた。
エ)	IPsecCA サーバにおける通信ログの確認	IPsecCA サーバの通信ログにより、正常に動作することが確認できた。
オ)	非 IPsec クライアントから接続要求があった場合のアプリケーションの動作状況と IPsec ポリシーサーバの通信ログの確認	非 IPsec クライアントから接続要求があった場合、要求が許可されずに通信できないことが確認できた。

3.1.10. 認証技術と IPsec を組み合わせた場合の Windows XP 等 OS レベルでの問題点の検証と評価

3.1.10.1.検証概要

実際に各 OS に実装された IPsec クライアントが安定して動作するかを検証する。特に当面、世の中の動向としてクライアント OS は Windows XP が主流になることが予想されているので、より詳細な実験を行う。

3.1.10.2.検証目的

IPv6 及び、IPsec は、現在 Windows XP、Windows2000、FreeBSD、Linux など様々な OS 上に実装されている。その中でも、Windows XP はクライアント OS として、主流になることが予想される。本検証では、動作が正しく行われることの確認と、安定した動作の確認を行うとともに、他の OS との親和性についても検証を行う。

IPv6 は、FreeBSD で実装が先行して進められていた。Linux では USAGI プロジェクトなど、日本を中心にいくつかのプロジェクトが進められ、いくつかのディストリビューションにオプションで組み込まれ始めている。クライアント OS で一般的な Windows XP では、標準ではインストールされていないが、コマンドラインから簡単にインストールできるようになっている。また、Windows2000 でも、パッチをダウンロードしてインストールできるようになった。

これらの IPsec をサポートした OS だけでは、ユーザ自らが、認証に関する情報（SA）管理しなければならない。そこで各 OS と連携し、ポリシーや鍵などを管理するシステムであるポリシーサーバや CA サーバ、IPsec クライアントソフトの開発を行った。

本検証では、IPsec クライアントソフトが安定して動作するかを検証する。

3.1.10.3.検証項目

表 3.1.34　検証 9 の検証内容と評価基準

項目	検証内容	評価基準
ア）	長時間の繰り返しのオペレーション（通信接続）を実施し、アプリケーションの動作状況を確認する。	アプリケーションの通信が継続的に成功すること。
イ）	異なる複数の OS 間でのオペレーションを行い、アプリケーションの動作状況を確認する。	OS やアプリケーションがフリーズや動作不安定などの不具合を起こさないこと。
ウ）	ア）イ）の結果について、3.1.9 の検証確認項目により、長期的に確認する。	クライアントに搭載しているほかのアプリケーションに影響しないこと。
エ）	市民ｅモニタの端末から通信ログを定期的に収集し、サーバ側との履歴に相違がないか確認する。	市民ｅモニタの端末の通信ログと、サーバ側の通信ログを比較し、接続成功や失敗の通信ログが一致すること。
オ）	市民ｅモニタにアンケート調査を実施し、実際の使い勝手を確認する。	アンケート調査により、満足できたか。

3.1.10.4. 検証環境

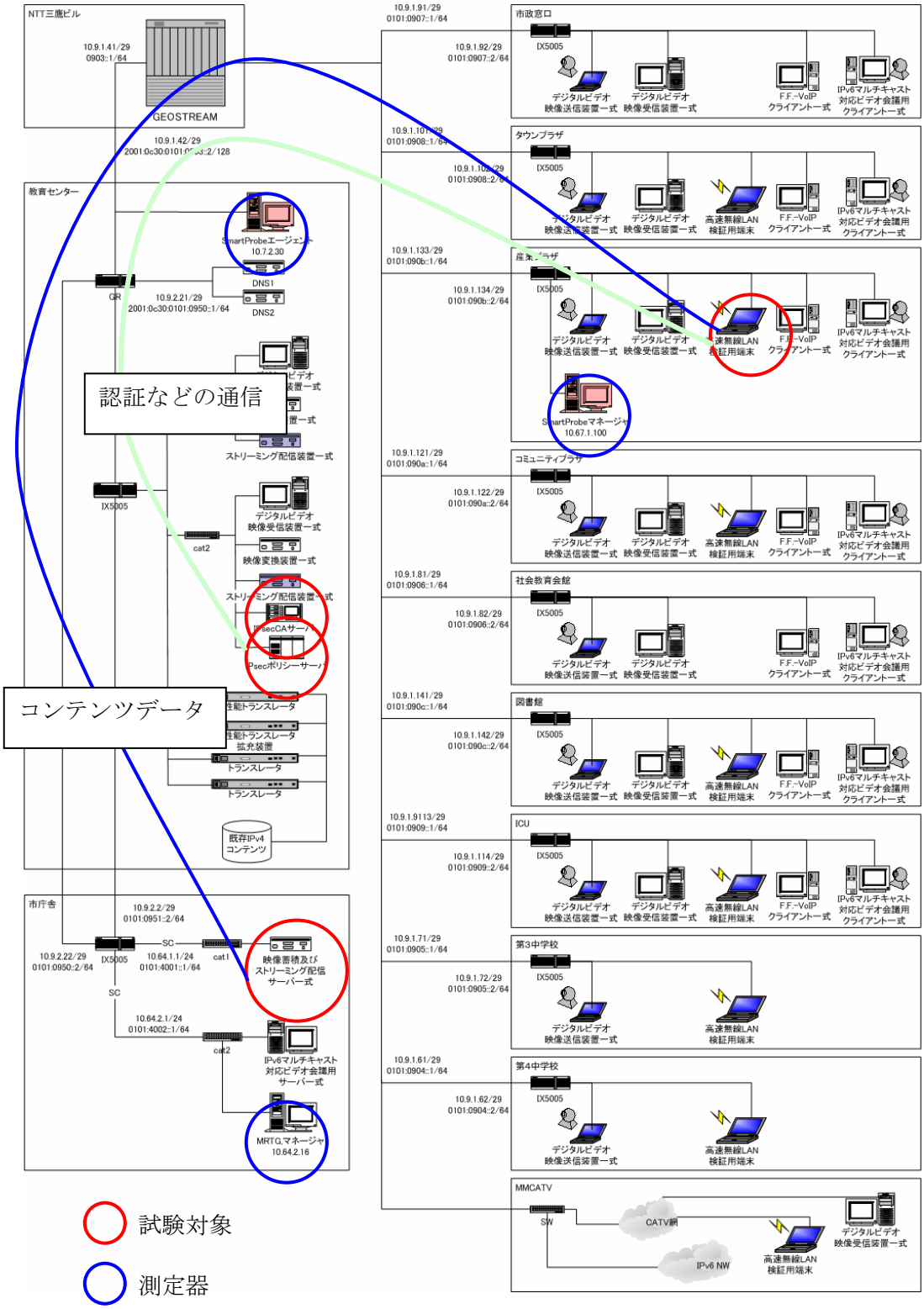


図 3.1.62　試験対象と検証で使用する測定器

3.1.10.5. 検証方法と結果

3.1.10.5.1.　ア）長時間の繰り返しのオペレーション（通信接続）を実施し、アプリケーションの動作状況を確認

(1)　検証方法

コンテンツを連続して何度も視聴することにより、アプリケーションが長時間にわたり、動作し続けることを確認する。一般的な経験則からコンテンツを閲覧するのは数回であると想定される。そこで本検証では、20 回の視聴の繰り返しを十分な検証回数として、動作の確認を行う。

① 産業プラザから、検証用のノート端末を用いて、Web ブラウザで「三鷹ポータル」にログインする。
② 「三鷹ポータル」のコンテンツの 1 つを視聴する。
③ 視聴後、②以外のコンテンツを視聴する。
④ ②及び、③を繰り返し 20 回行う。

(2)　検証方法

上記の①から④の手順どおりにオペレーションを実施して、正常に動作確認できた。

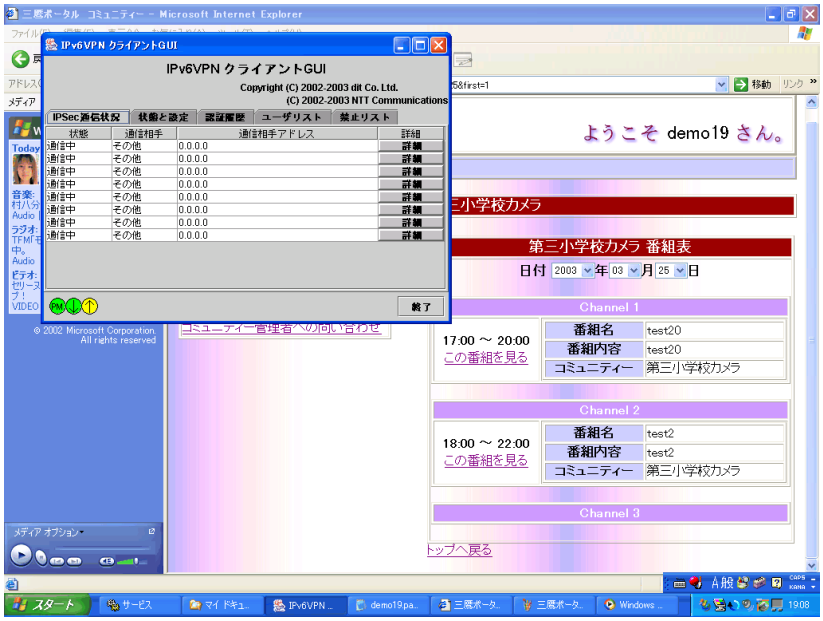


図 3.1.63　クライアント IPsec 通信状況

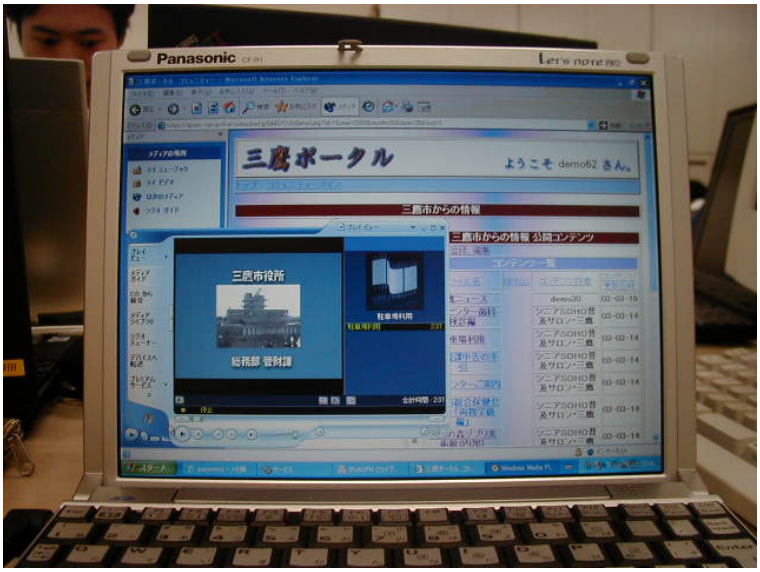


図 3.1.64　「三鷹ポータル」映像コンテンツ再生の様子

実際に作業したメモを示す。

検証作業メモ

検証９のア）２０回コンテンツ再生を行う。(端末 No16)[demo62]
　結果を以下に示す。
　◎三鷹市何でもビデオ
　　17:20 ○[大手町より]　　ＯＫ
　　17:22 ○[三鷹サンプル２] 再生まで時間がかかったが、ＯＫ
　　17:25 ○[三鷹市立図書館] 接続中の状態で、時間がかかり、再生されない。
　　　　<既存のプレイヤで再生する（ブラウザではなく専用プレイヤでの再生で無く
　　　　Windows Media Player が立ち上がる）>を実行したら再生された
　　　　画像がスムーズに流れない
　　17:28 ○[e!三鷹キックオフ村井純氏ビデオレター]
　　　　接続中の状態で、時間がかかり、再生されない。
　　　　<既存のプレイヤで再生する>を実行したら再生された

　◎三鷹市からの情報
　　17:31 ○[三鷹ニュース]　　ＯＫ
　　17:32 ○[保健センタ歯科検査編]　　ＯＫ
　　17:33 ○[駐車場利用]　　ＯＫ
　　17:34 ○[市民税課申告の手引]　　ＯＫ
　　17:36 ○[市民センタご案内]　　ＯＫ
　　17:36 ○[三鷹市総合保健センタ「両親学級編」]　　ＯＫ
　　17:39 ○[三鷹ジブリの森美術館(内部)]　　ＯＫ
　　17:41 ○[三鷹ジブリの森美術館(概観)]　　ＯＫ
　　17:42 ○[屋外スポーツ施設 No2(テニス場等)]　　ＯＫ
　　17:43 ○[屋外スポーツ施設 No1(総合グランド等)]　　ＯＫ
　　17:45 ○[0 歳児の保育遊び編]　　ＯＫ
　　17:46 ○[0 歳児の保育おむつ編]　　ＯＫ
　　17:48 ○[大手町より]
　　　　最初の方で、画像がとびとびになる。声はスムーズ。
　　17:51 ○[大手町より]　　再度試したら、スムーズになった。ＯＫ
　　17:52 ○[0 歳児の保育食事編]　　ＯＫ
　　17:53 ○[第二体育館]　　ＯＫ

(3) 結論・考察

途中、スムーズでない動作をしたが、これらは他の通信の影響であると考えられる。本検証の結果としては、長時間にわたり繰り返し実行した結果、正常に動作することを確認した。

今後、実運用を数ヶ月の期間において継続して監視することにより、さらに安定した動作を確認する必要がある。

3.1.10.5.2. イ）異なる複数の OS 間でのオペレーションを行い、アプリケーションの動作状況を確認

(1) 検証方法

Windows XP のクライアント端末から、コンテンツの視聴を行うことにより、いくつかのサーバにアクセスする。サーバの OS は Windows2000、FreeBSD などがある。

① 産業プラザから Windows XP のノート端末を用いてネットワークに接続する。
② Web ブラウザで「三鷹ポータル」にログインする。
③ 蓄積されたコンテンツ（Windows2000 サーバ）を視聴する。
④ NetG ミニ経由（FreeBSD）で既存コンテンツを視聴する。

(2) 検証結果

コンテンツの視聴を行うことが確認できた。

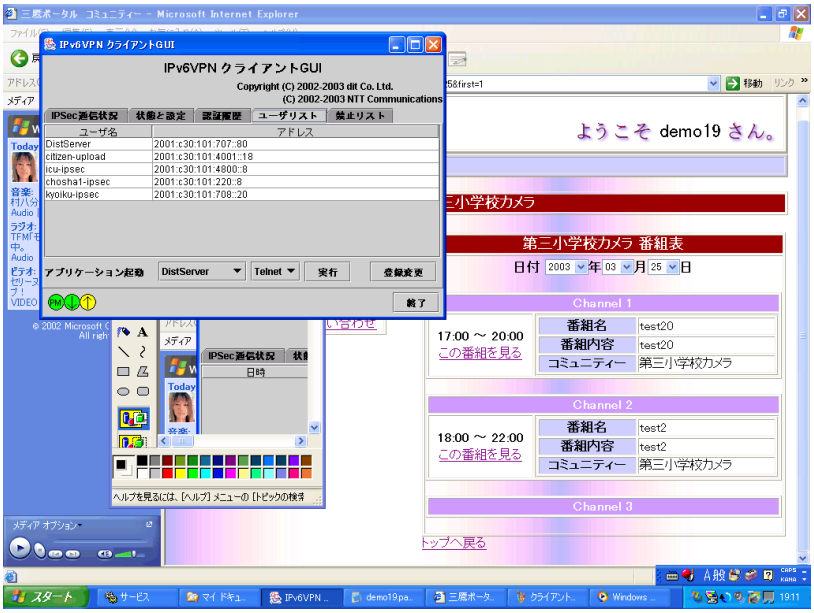


図 3.1.65 IPv6VPN クライアント GUI

(3) 結論・考察

異なる OS でも IPsec を使った通信が行えることが確認できた。現時点では、時間が限られており、またアプリケーションやミドルウェア・OS の対応状況の制約がある。そのため、あまり多くの OS 間の組み合わせによる検証が出来なかった。

今後、MAC や Linux の端末、Linux や Solaris、HP-UX などのサーバなどで動作する、IPv6 及び、IPsec を用いたアプリケーションも登場してくることが見込まれる。これらのクライアント OS・サーバ OS でも相互接続性を検証していく必要がある。

3.1.10.5.3. ウ）ア）イ）の結果について、3.1.9 の検証確認項目により、長期的に確認

(1) 検証方法

① 市民 e モニタによる動作状況をアンケートにて確認する。

② 「三鷹ポータル」のコンテンツ配信、「FF-VoIP」による通信が、長期的に安定していることを確認する。

(2) 検証結果

以下のような、アンケート結果となった。

1.三鷹ポータルの映像コンテンツは正しく表示されましたか？選択肢の中から選択してください。

［選択肢］

「1:表示された」 15%

「2:エラーが表示され、表示されなかった」56%

「3:その他」 29%

6.コンテンツはセキュリティ（IPsec)がかけられ、ｅ！ユーザ以外からは
アクセスできないことをご存知でしたか？選択肢の中から選択してください。

［選択肢］

「1:知っていた」 71%

「2:知らない」 29%

7.IPSEC という認証、セキュリティ技術を聞いたことがありますか？
選択肢の中から選択してください。

［選択肢］

「1:詳しく知っている」

「2:少し知っている」 72%

「3:聞いたことはある」 14%

「4:まったく知らなかった」14%

(3) 結論・考察

数週間ではあるが、正常に動作することが確認できた。まだ利用者が少ない状況であり、今後、さらに長期的な運用を続けていき、安定した動作を確認する必要がある。

3.1.10.5.4. エ）市民ｅモニタの端末から通信ログを定期的に収集し、サーバ側との履歴に相違がないか確認

(1) 検証方法

IPsec のサーバには、クライアントの認証結果ログを定期的に収集する機能がある。本検証では、この機能を用いてログを収集し、履歴を確認する。

① IPsec サーバのログを集計する。

② 市民ｅモニタの端末から送信されてくるクライアントのログを集計する。

③ 上記①、及び、②のログを比較し、相違がないことを確認する。

(2) 検証結果

下記のように、ログが出力された。

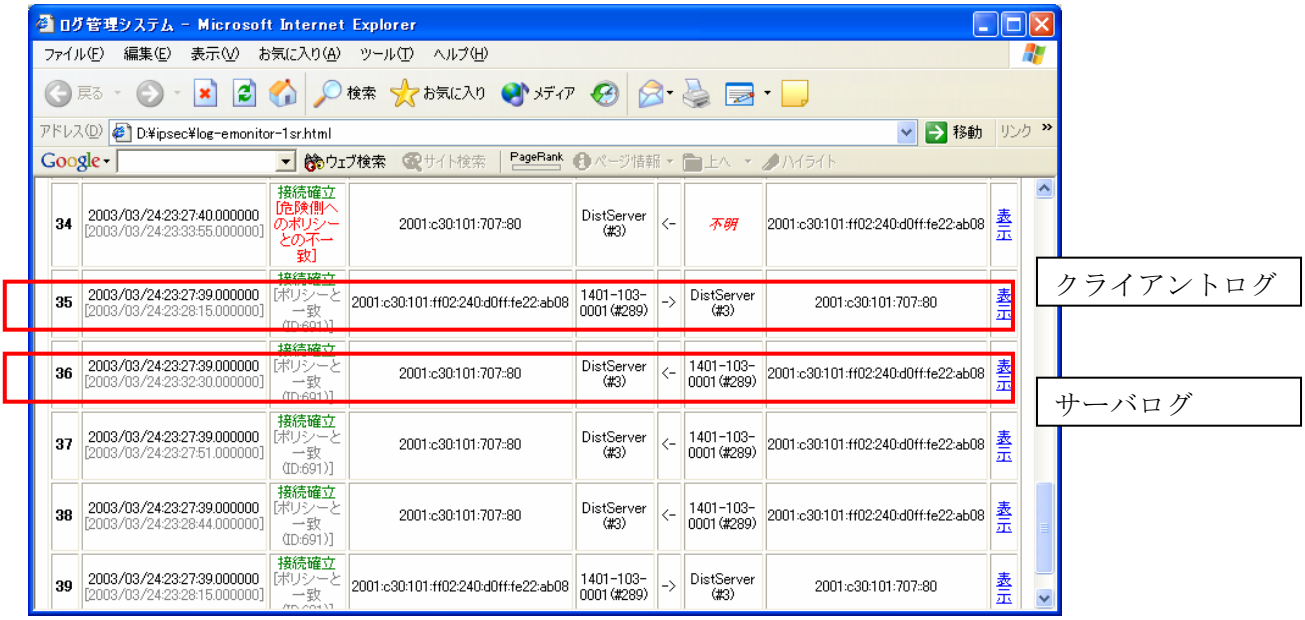


図 3.1.66 ログ管理システム

赤線で囲んだ部分のクライアントログとサーバのログが一致している。

(3) 結論・考察

上記の結果から、サーバ及び、クライアントのログに相違ないことが確認された。

3.1.10.5.5. オ）市民 e モニタにアンケート調査を実施し、実際の使い勝手を確認

(1) 検証方法

① 各アプリケーションの使い勝手を市民 e モニタによる動作状況をアンケートにて確認する。

② アンケートを集計する。

(2) 検証結果

アンケートでは下記のような意見があった。

VPN クライアント：

- 起動時間が長い。
- エラーの表示がわかりにくい。
- パスワードを毎回入力するのは面倒。
- パスワードの変更が出来ない。
- 言葉が難しい。一般の人がわかるようにしてほしい。
- VPN クライアントを起動させておくのは嫌だ。
- VPN クライアントを起動させておくと TELNET などが出来ないことがある。
- 誰と通信しているか、通信相手がわかるのでいい。
- セキュリティが保たれている状態がわかりにくく、安全である実感が無い。

(3) 結論・考察

アンケートの情報だけでは、長時間の動作確認が難しいが、繋がらないこともあるという結果になった。これが、直接 IPsec クライアントの原因であるとはいえないが、原因を究明し、対処する必要がある。

また、使い勝手そのものについては、いくつかの意見を頂いた。ユーザが意識しなくても使えるようにしていく必要がある。さらに数ヶ月以上運用し続け、改良を加えることにより、長期間の安定性や運用面での利便性を高めていく必要がある。

3.1.10.6.まとめ

表 3.1.35　検証内容と検証結果のまとめ

項目	検証内容	結果
ア）	長時間の繰り返しのオペレーション（通信接続）を実施し、アプリケーションの動作状況を確認する。	長時間でも正常に動作する。
イ）	異なる複数の OS 間でのオペレーションを行い、アプリケーションの動作状況を確認する。	FreeBSD と Windows XP での正常動作を確認した。
ウ）	ア）イ）の結果について、7.1.7.8 の検証確認項目により、長期的に確認する。	3 週間程度の期間、正常に動作することを確認した。
エ）	市民 e モニタの端末から通信ログを定期的に収集し、サーバ側との履歴に相違がないか確認する。	サーバ､クライアントの通信ログが一致することを確認した。
オ）	市民 e モニタにアンケート調査を実施し、実際の使い勝手を確認する。	利用者や管理者の手間を減らす改良が必要になる。