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。

3.1.11. IPsec 管理システムを用いた暗号化通信技術の検証

3.1.11.1.検証概要

IPsec のクライアント間の通信が暗号化され盗聴されない安全な状態で通信されることを検証する。

3.1.11.2.検証目的

IPv6 の特徴のひとつに、IPsec によるプロトコルレベルでの暗号化をサポートしていることが上げられる。IPsec は基本的には TCP/IP レベルで通信経路の暗号化を行うプロトコルであり、VPN(Virtual Private Network)などによく利用されるものである。

本検証では、IPsec による暗号化が正しく行われており、盗聴が不可能な状態になっているかを実際のパケットレベルで確認する。さらにサーバとクライアントのログが一致することも確認する。

3.1.11.3.検証項目

表 3.1.36　検証 10 の検証内容と評価基準

項目	検証内容	評価基準
ア)	アナライザ等を使って IP パケットをモニタリング	通信が暗号化されていること（平文化でないこと)。
イ)	IPsec クライアントにおける通信ログを監視	事前に B に登録された設定のとおりの暗号化通信がなされていること。
ウ)	IPsec ポリシーサーバにおける通信ログの確認	IPsec クライアント及び、IPsec ポリシーサーバの通信ログに接続開始及び終了のログが記録されていること。

3.1.11.4. 検証環境

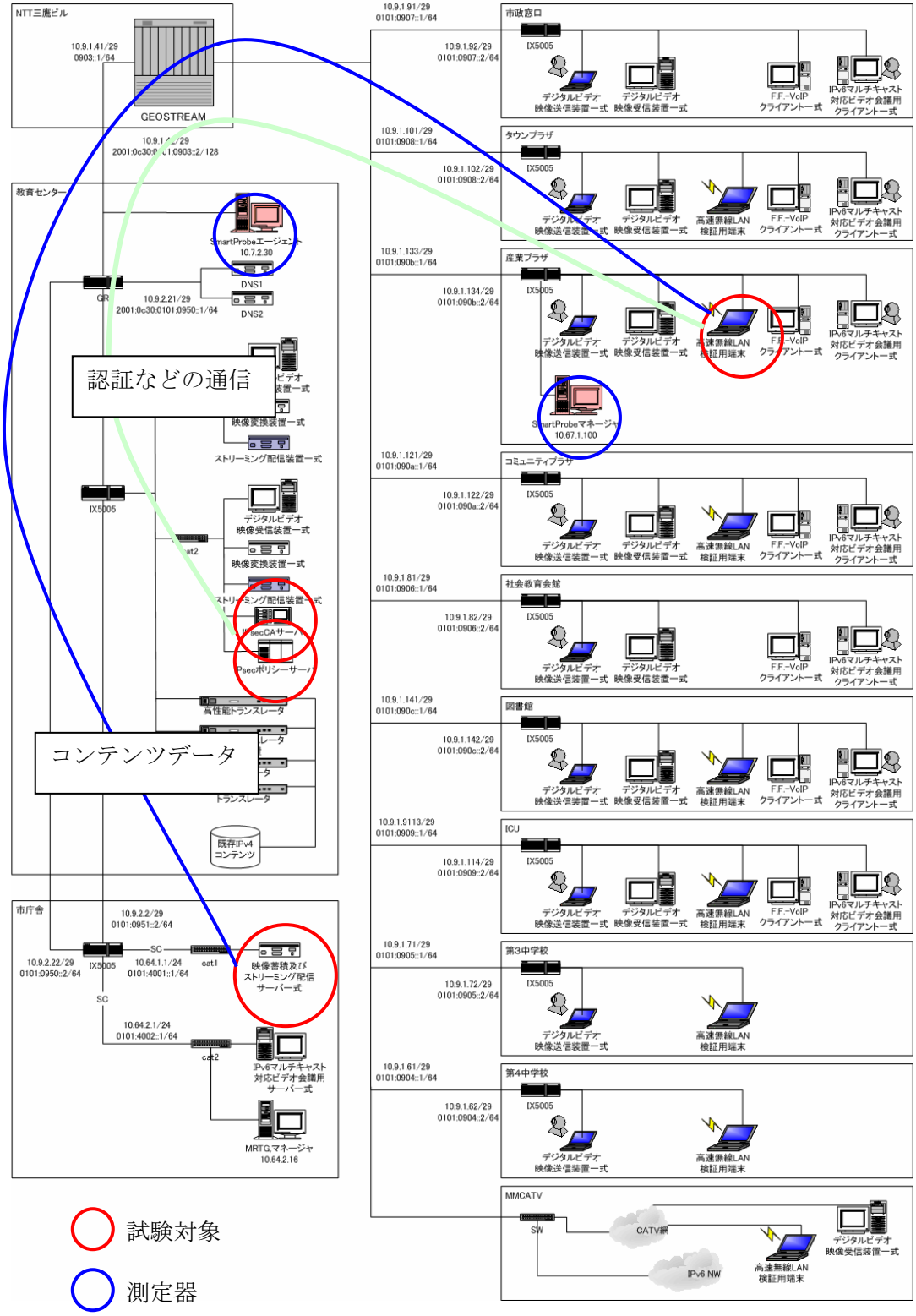


図 3.1.67　試験対象と検証で使用する測定器

3.1.11.5.検証方法と結果

3.1.11.5.1.ア）アナライザ等を使って IP パケットをモニタリング

(1) 検証方法

本検証では、通信経路上でパケットをキャプチャし、ユーザのデータが暗号化されていることを確認する。

① 教育センタに設置してあるトラフィック測定器「SmartProbe」により、キャプチャを開始する。
② 産業プラザでクライアント端末を接続する。
③ 一般のホームページを開く。
④ クライアント端末から「三鷹ポータル」にログインする。
⑤ 「SmartProbe」の測定したキャプチャデータを、産業プラザのマネージャで収集する。
⑥ Ethereal を用いて、キャプチャデータの中身を解析する。
⑦ 3.のとき、HTML ファイルがダウンロードされ、中身が暗号化されていないことを確認する。
⑧ 4.のとき、URL や HTML の本体、ユーザ ID などが見えないことを確認する。

(2) 検証結果

SmartProbe のダンプモードでの測定によりキャプチャを行い、通信されているパケットの中身が暗号化されていることが分かった。

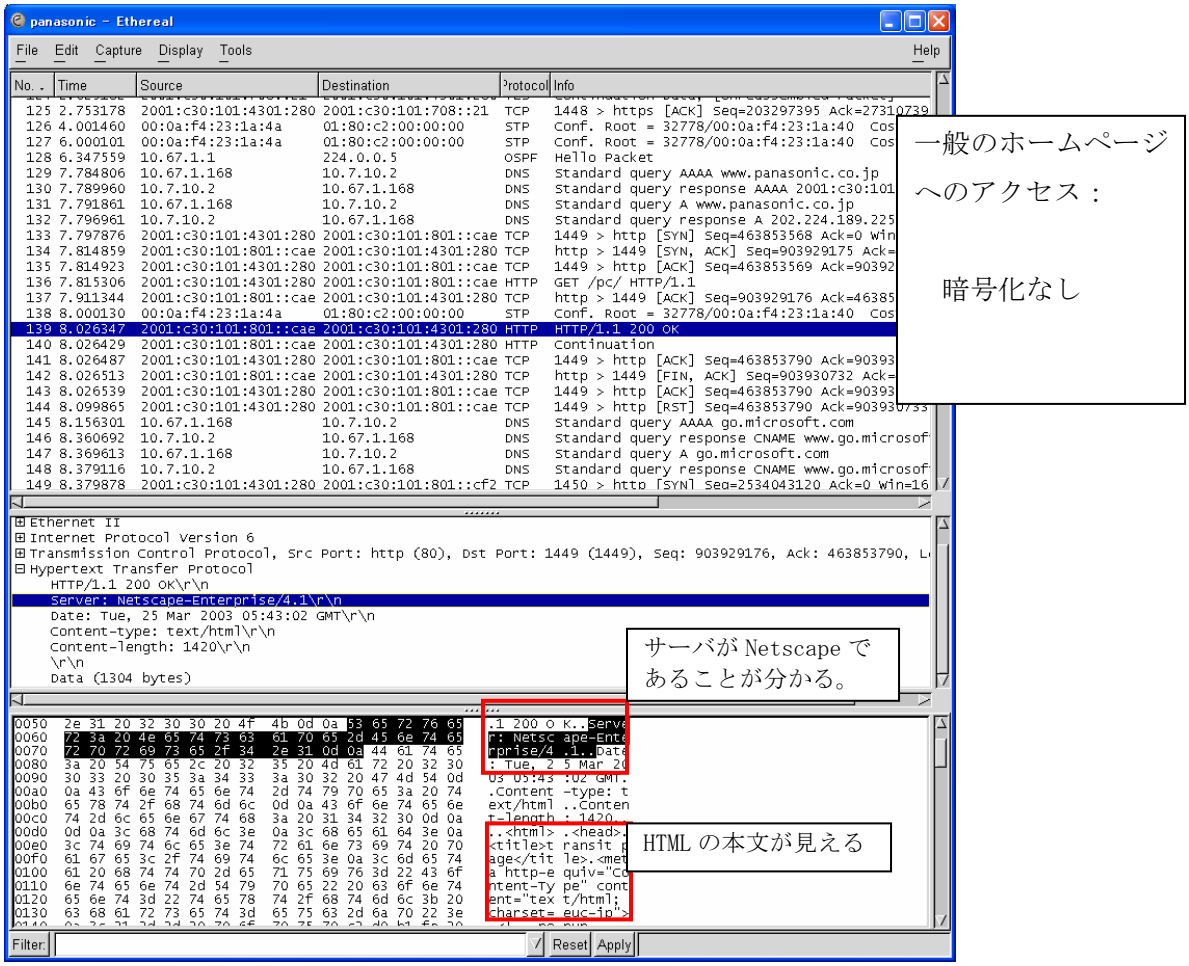


図 3.1.68　一般のホームページへのアクセス

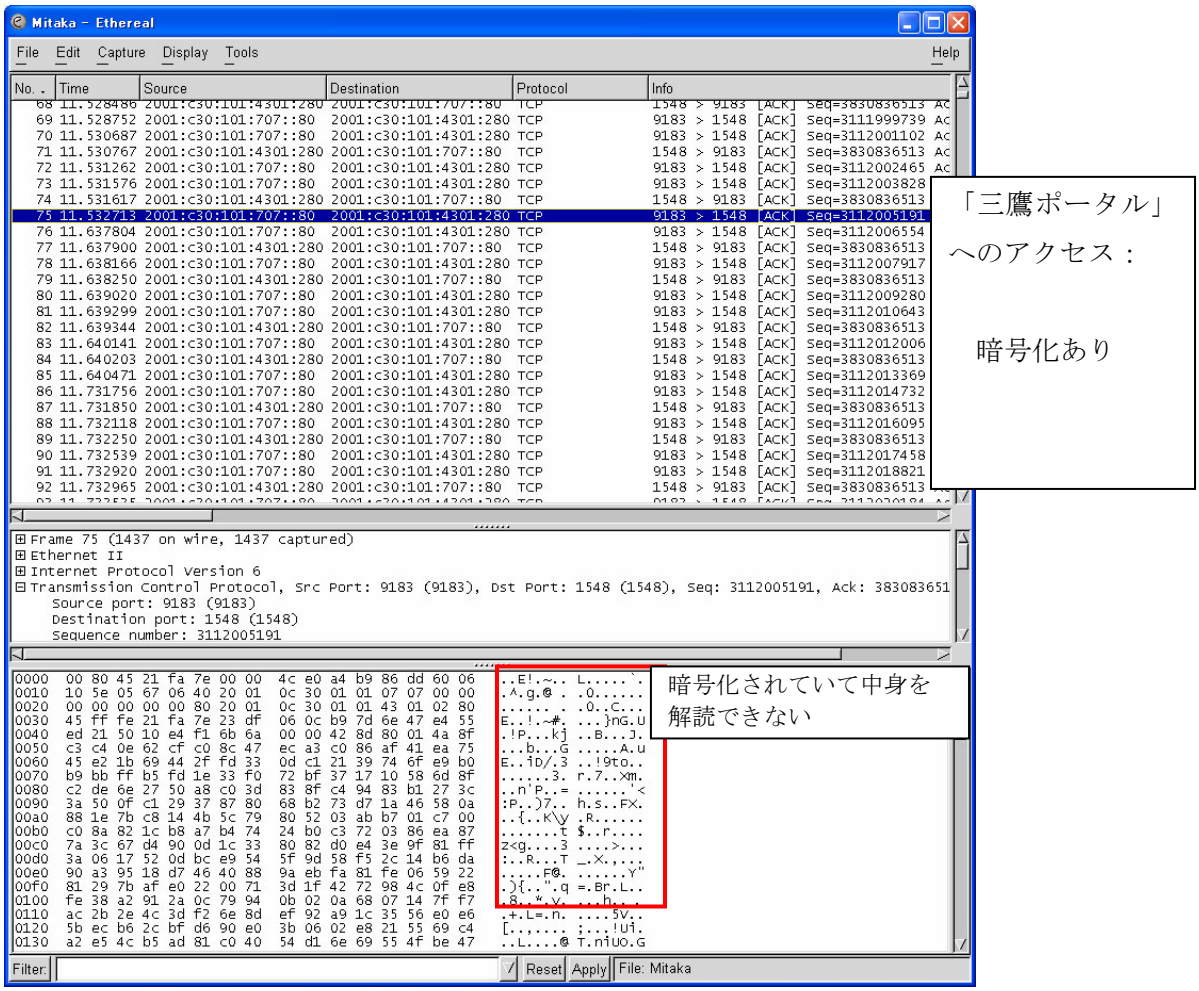


図 3.1.69　「三鷹ポータル」へのアクセス

(3)　結論・考察

IPsec をかけない状態でインターネットからホームページをダウンロードすると、平文で中身が見えた。一方 IPsec による通信で、ユーザのデータが確かに暗号化されていることを確認できた。

3.1.11.5.2.　イ）IPsec クライアントにおける通信ログを監視

(1)　検証方法

① 産業プラザでクライアント端末を接続する。

② クライアント端末から「三鷹ポータル」にログインする。

③ コンテンツを視聴する。

④ クライアントの通信ログで、暗号化されていることを確認する。

(2) 検証結果

クライアントの通信ログから、暗号化を行っていることが確認できた。

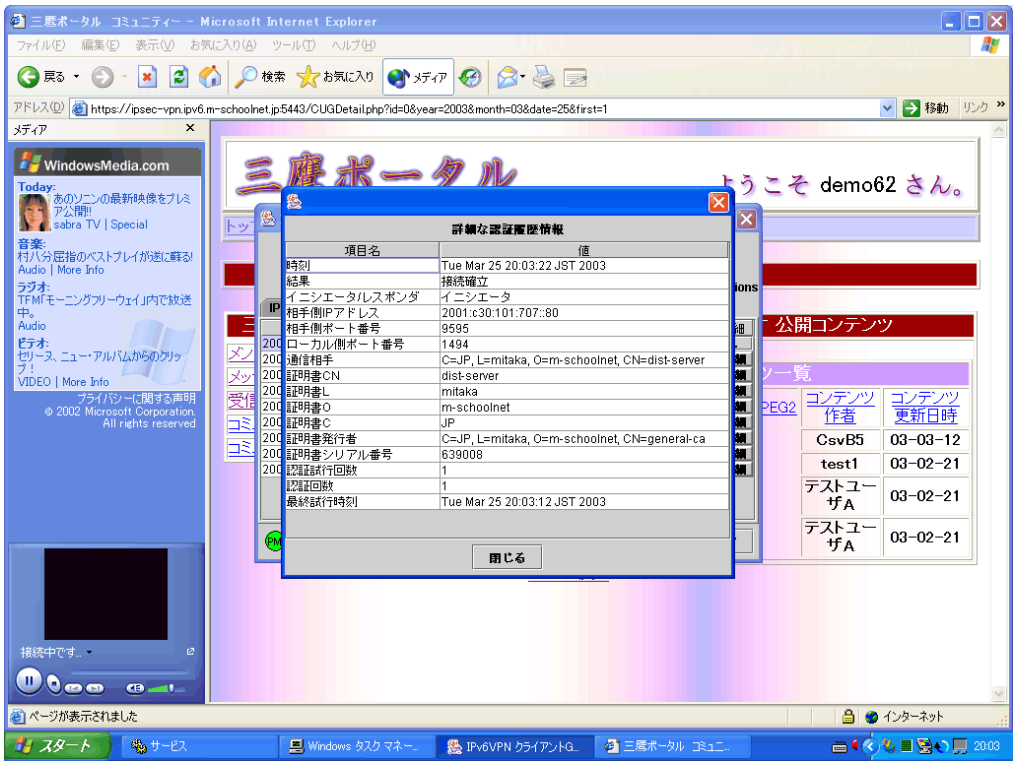


図 3.1.70 クライアントの証明書の設定内容

(3) 結論・考察

クライアントの通信ログから、IPsec による暗号化を実行していることが確認できた。ア）の結果とあわせ、クライアント及び、ネットワークを流れるパケットが一致していることが分かる。

3.1.11.5.3. 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 産業プラザでクライアント端末を接続する。

② クライアント端末から「三鷹ポータル」にログインする。

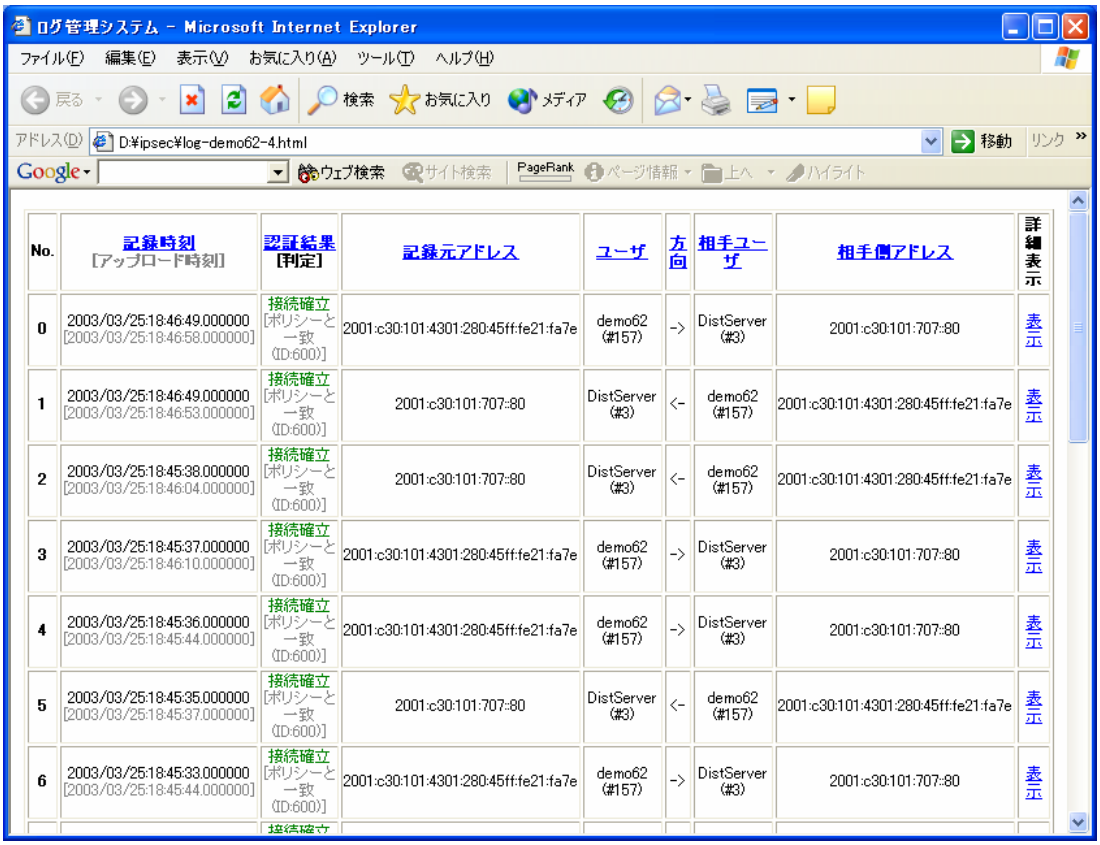
③ コンテンツを視聴する。

④ 「三鷹ポータル」からログアウトする。

⑤ IPsec ポリシーサーバの通信ログで、接続確立のログが記録されていることを確認する。

(2) 検証結果

以下に示すように、IPsec ポリシーサーバの通信ログ上で、接続が確立されていることを確認できた。



No.	記録時刻 [アップロード時刻]	認証結果 [判定]	記録元アドレス	ユーザ	方向	相手ユーザ	相手側アドレス	詳細表示
0	2003/03/25:18:46:49.000000 [2003/03/25:18:46:58.000000]	接続確立 [ポリシーと一致 (ID:600)]	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62 (#157)	->	DistServer (#3)	2001:c30:101:707::80	表示
1	2003/03/25:18:46:49.000000 [2003/03/25:18:46:53.000000]	接続確立 [ポリシーと一致 (ID:600)]	2001:c30:101:707::80	DistServer (#3)	<-	demo62 (#157)	2001:c30:101:4301:280:45ff:fe21:fa7e	表示
2	2003/03/25:18:45:38.000000 [2003/03/25:18:46:04.000000]	接続確立 [ポリシーと一致 (ID:600)]	2001:c30:101:707::80	DistServer (#3)	<-	demo62 (#157)	2001:c30:101:4301:280:45ff:fe21:fa7e	表示
3	2003/03/25:18:45:37.000000 [2003/03/25:18:46:10.000000]	接続確立 [ポリシーと一致 (ID:600)]	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62 (#157)	->	DistServer (#3)	2001:c30:101:707::80	表示
4	2003/03/25:18:45:36.000000 [2003/03/25:18:45:44.000000]	接続確立 [ポリシーと一致 (ID:600)]	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62 (#157)	->	DistServer (#3)	2001:c30:101:707::80	表示
5	2003/03/25:18:45:35.000000 [2003/03/25:18:45:37.000000]	接続確立 [ポリシーと一致 (ID:600)]	2001:c30:101:707::80	DistServer (#3)	<-	demo62 (#157)	2001:c30:101:4301:280:45ff:fe21:fa7e	表示
6	2003/03/25:18:45:33.000000 [2003/03/25:18:45:44.000000]	接続確立 [ポリシーと一致 (ID:600)]	2001:c30:101:4301:280:45ff:fe21:fa7e	demo62 (#157)	->	DistServer (#3)	2001:c30:101:707::80	表示

図 3.1.71 ログ管理システム

(3) 結論・考察

ウ）の結果とア）及び、イ）のそれぞれ結果から、IPsec 通信が正しく行われていることを確認できた。それぞれが一致することにより、意図する通信が行われていることがわかる。

3.1.11.6. まとめ

表 3.1.37　検証内容と検証結果のまとめ

項目	検証内容	結果
ア）	アナライザ等を使って IP パケットをモニタリング	通信が暗号化されていることが確認できた。
イ）	IPsec クライアントにおける通信ログを監視	正しく暗号化されていることを確認した。
ウ）	IPsec ポリシーサーバにおける通信ログの確認	正しく暗号化されていることを確認した。

本検証で、実際にパケットが暗号化されていることが確認された。また、意図しているように暗号化されていることをクライアント、及び、サーバのログからも確認できた。

今回のプロジェクトにより、大規模な IPv6 ネットワークと、セキュリティを考慮したアプリケーションが構築され、実際にセキュリティが保たれている。インフラからアプリケーション、実際のユーザの利用状況まで確認できた意義は大きい。

3.1.12. IPsec 管理システムを用いた利用者認証技術の検証

3.1.12.1.検証概要

IPsec ポリシーサーバと CA サーバを連携させて、証明書発行を行い、その証明書に基づき IPsec 管理システムを用いた利用者認証技術の検証

3.1.12.2.検証目的

IPsec とともにセキュリティを確保する重要な役割として、IKE（Internet Key Exchange）がある。IKE は、鍵交換を行う仕組みを提供する。IPsec で用いられる認証のための情報は SA（Security Association）と呼ばれる。SA には、以下のような情報がある。

① セキュリティプロトコル
ESP（Encapsulating Security Protocol）あるいは、AH（Authentication Header）のいずれか

② カプセル化モード
トンネルモードかトランスポートモード

③ Security Parameters INDEX（SPI）
SA を識別する ID

④ 暗号化や認証（完全性保証）アルゴリズム
暗号化や認証に使用する具体的なアルゴリズム

⑤ セレクタ
SA を適用するパケットのフィルタ

⑥ 秘密対称鍵
暗号化を行うための鍵

本検証では、上記の通信により、認証が正常に行われていることを、証明書発行と証明書による認証の動作により確認する。さらにサーバとクライアントのログが一致することも確認する。

3.1.12.3.検証項目

表 3.1.38　検証 11 の検証内容と評価基準

項目	検証内容	評価基準
ア）	クライアントが持っている証明書は、CA サーバが発行した正しい証明書であることをクライアントのログで確認する。	通信が正常に行われて、その結果がクライアントや IPsec ポリシーサーバの通信ログに記録されているか。
イ）	証明書を用いて、クライアントにあらかじめ登録されたポリシーに従って通信が確立されているかクライアントのログで確認する。	非 IPsec クライアントからの接続要求を拒否している通信ログが IPsec ポリシーサーバに残っているか。

3.1.12.4. 検証環境

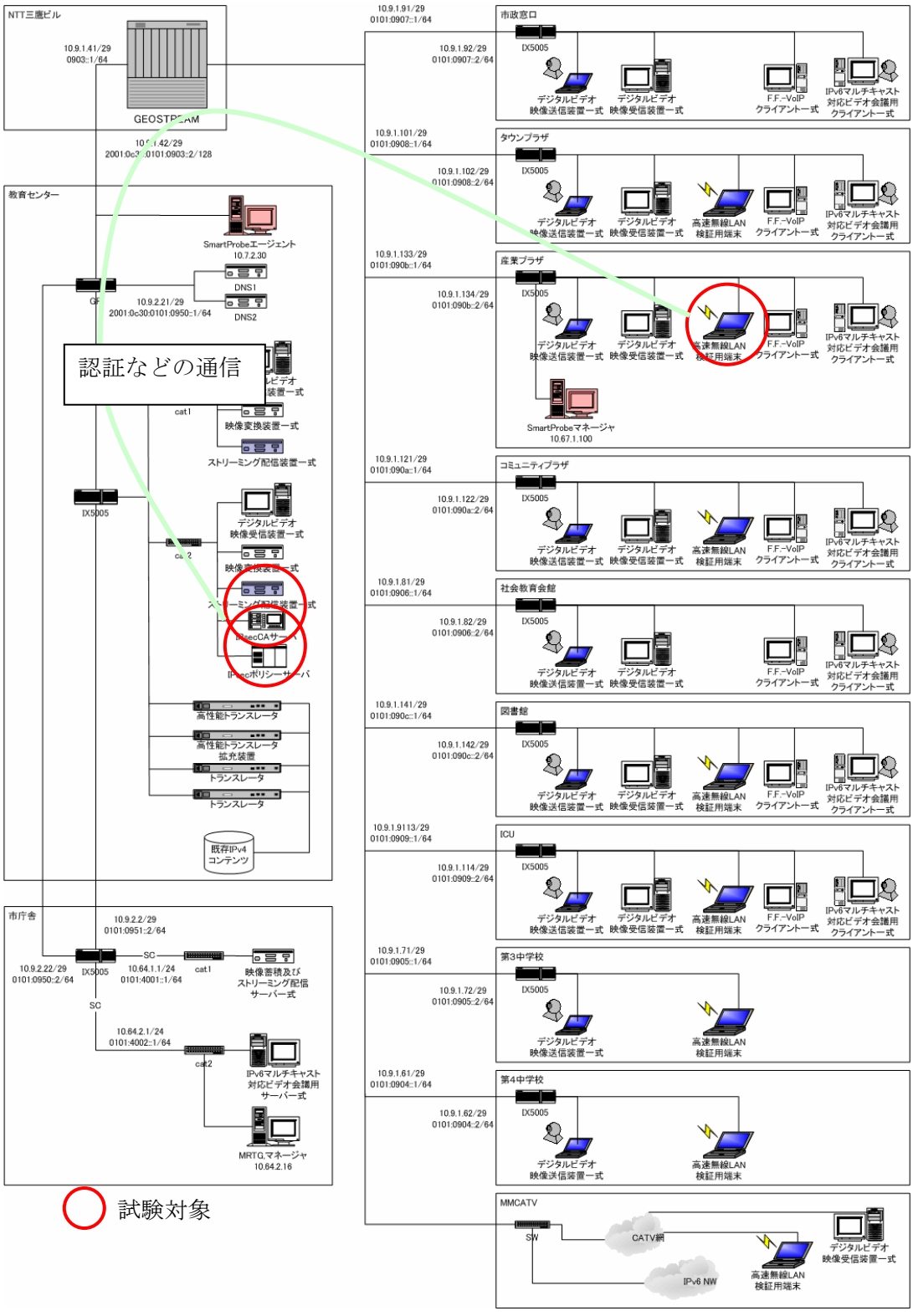


図 3.1.72　試験対象と検証で使用する測定器

3.1.12.5.検証方法と結果

3.1.12.5.1.　ア）クライアントが持っている証明書は、CA サーバが発行した正しい証明書であることをクライアントのログで確認する。

(1)　検証方法

本検証では CA サーバから HTTPS 経由で証明書の取得を行う。その証明書が意図する証明書であることをクライアント側で確認する。

① IPsecCA サーバにより証明書の登録を行う。
② クライアントから「三鷹ポータル」に HTTPS でサーバポート番号 5443 にアクセスし、証明書発行のページを開く。
③ 証明書をダウンロードする。
④ クライアントに証明書を保存する。
⑤ Internet エクスプローラに証明書の設定を行う。
⑥ VPN クライアントに証明書の設定を行う
⑦ 「三鷹ポータル」にログインする。
⑧ クライアントのログを確認する。

(2) 検証結果

クライアントの通信ログに設定した証明書を使って認証を行っていることが出力された。

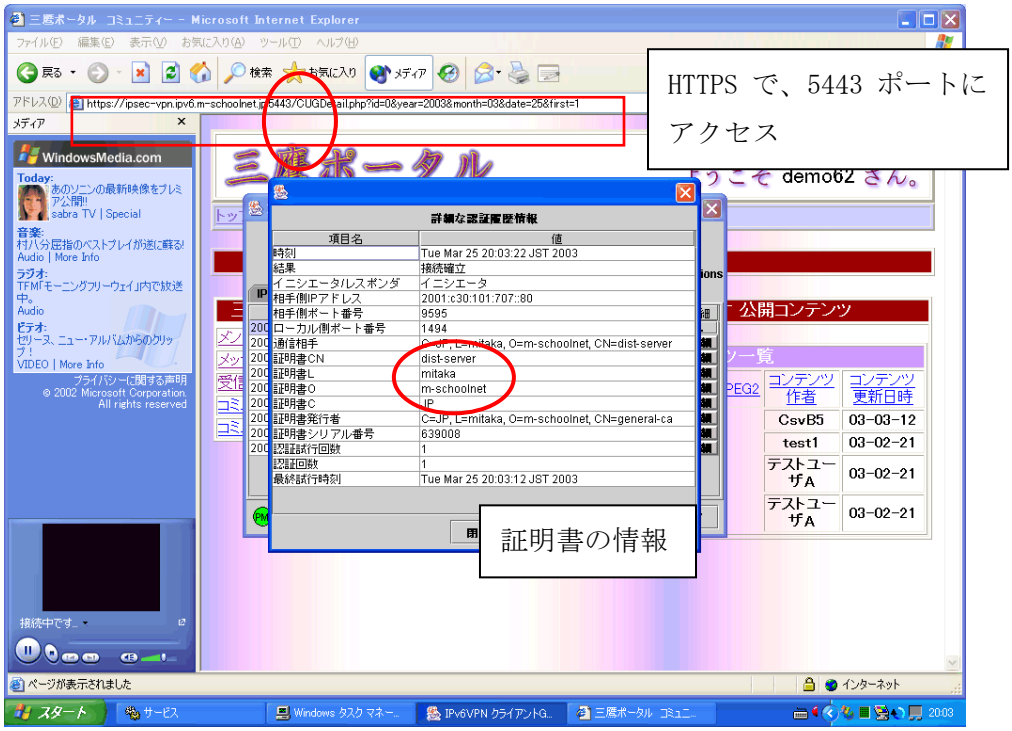


図 3.1.73 クライアントの証明書の設定内容

(3) 結論・考察

クライアントの VPN クライアント・アプリケーションのログに CA サーバの名前が載っていることから、意図した正しい証明書が認証に使われていることを確認。

3.1.12.5.2. イ）証明書を用いて、クライアントにあらかじめ登録されたポリシーに従って通信が確立されているかクライアントのログで確認する。

(1) 検証方法

① クライアントでポリシーを設定する。

② クライアントから「三鷹ポータル」にログインする。

③ コンテンツを視聴する。

④ クライアントのログを確認する。

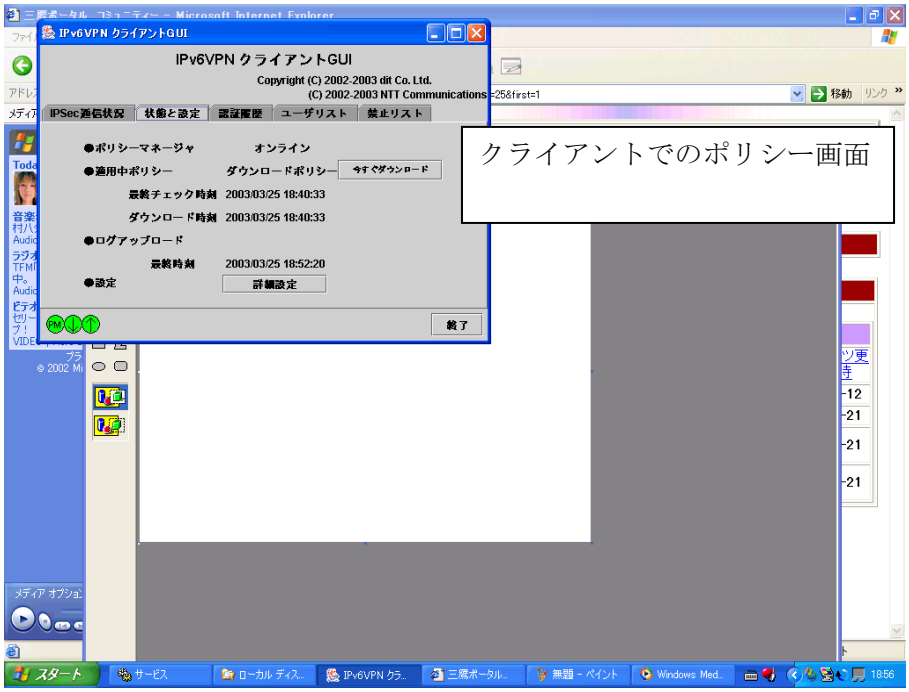


図 3.1.74　IPv6VPN クライアント GUI

(2)　検証結果

クライアントのポリシーで設定画面に設定されたようにコンテンツを視聴することが出来た。またその結果が、下記のように通信ログに出力されている。

図 3.1.75　「三鷹ポータル」映像コンテンツ再生の様子

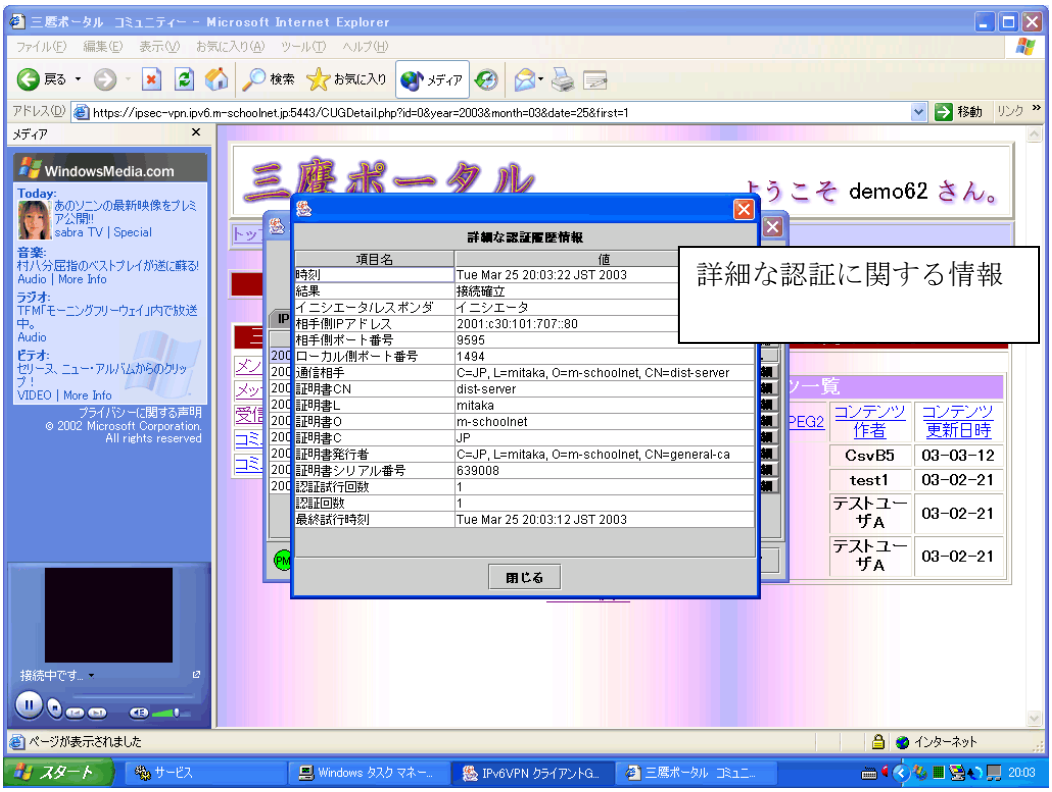


図 3.1.76　クライアントの証明書の設定内容

(3)　結論・考察

証明書を用いて、クライアントに登録されたポリシーのとおりに通信が確立されたことを確認できた。

3.1.12.6.まとめ

表 3.1.39　検証内容と検証結果のまとめ

項目	検証内容	結果
ア）	クライアントが持っている証明書は、CA サーバが発行した正しい証明書であることをクライアントのログで確認する。	正しい証明書であることを確認できた。
イ）	証明書を用いて、クライアントにあらかじめ登録されたポリシーに従って通信が確立されているかクライアントのログで確認する。	あらかじめ登録されたポリシーどおりに通信が確立されていることを確認した。

本検証では、CA サーバから発行された正しい証明書を用いていることを確認した。これは不正なサイトがユーザに偽の証明書を発行して、ユーザが被害を受けるのを防ぐことができることを意味する。

しかし、現状では証明書を発行する際に、ユーザ及び、端末が正しいことを確認できず、成りすましなどの被害が出来ることが想定される。今後、IC チップや指紋による特定を行うなど、クライアントを識別する手段が必要になる。

3.1.13. スケーラブルな環境に実証フィールドを移行した場合の性能限界の検証と検討

3.1.13.1.検証概要

ネットワーク規模を順次拡大させ IPsec 管理システムの性能限界を含めた評価を行い、ネットワーク規模と準備すべきサーバ群の性能限界を検証、評価し、今後のネットワーク設計時の基礎データに役立てる。

3.1.13.2.検証目的

IPsec による暗号化は通常の通信に比べ、ユーザデータを暗号化・復号化する際に、サーバ及び、クライアントの演算処理を増やし、ネットワークにも負荷をかける。また、セッションごとに認証を行うため、通信量もさらに増える。

本検証では、市民 e モニタなどユーザ数が順次拡大していく中で、負荷がどのように影響を与えるのか、また IPsec 管理システムの性能限界について確認を行う。

3.1.13.3.検証項目

表 3.1.40　検証 12 の検証内容と評価基準

項目	検証内容	評価基準
ア)	負荷集中時のレスポンスタイムの測定及び、サーバの CPU 負荷率の測定	サーバの負荷により、クライアントの通信に影響がでるか。
イ)	過負荷時のサーバ及び、クライアントの動作状況	サーバの負荷により、通信に影響があった場合は、どの程度影響するのか。
ウ)	フェーズ毎のクライアント数やアクセス数と、サーバ処理能力の測定	クライアント数やアクセス数とサーバの処理能力の因果関係は何か。

3.1.13.4. 検証環境

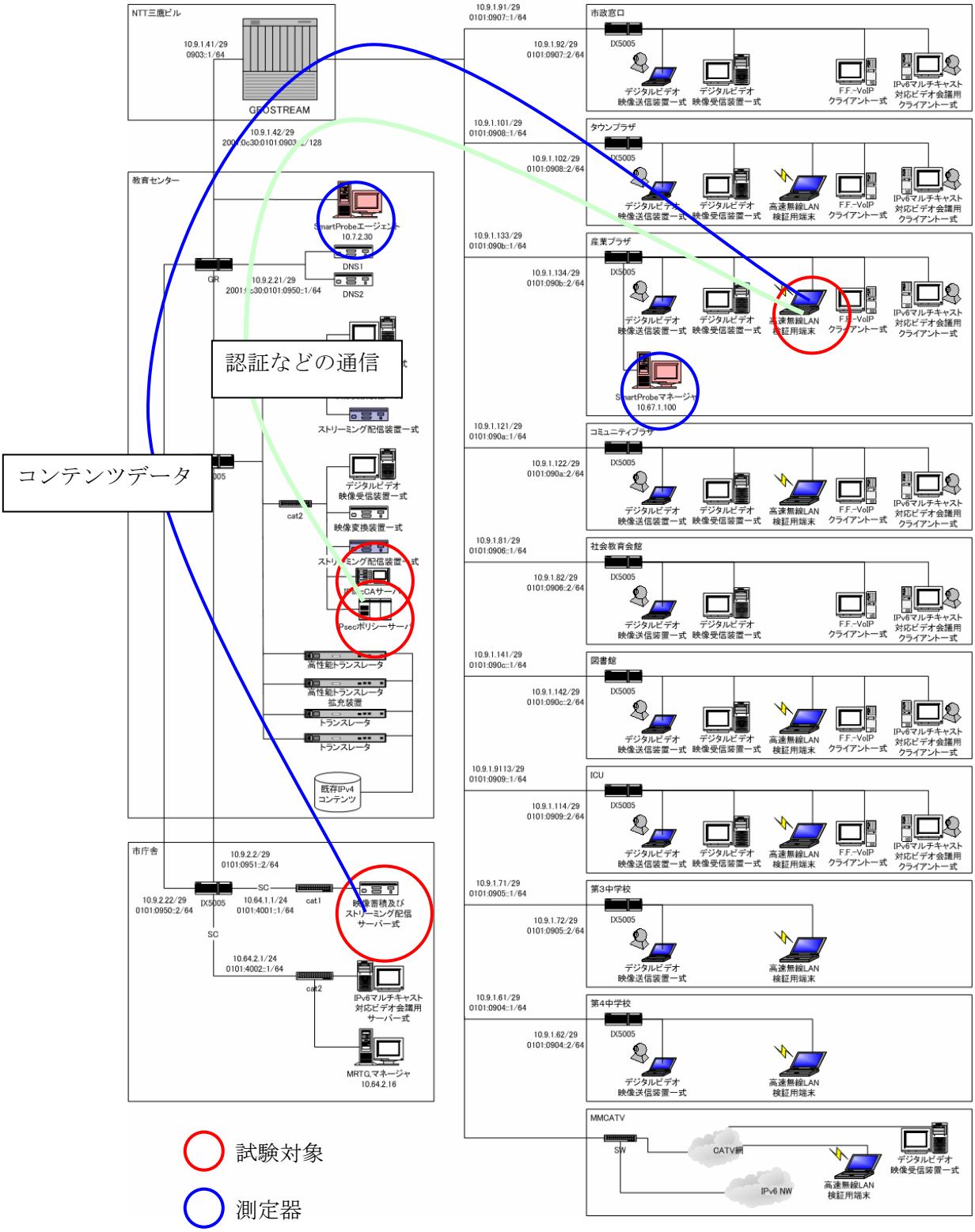


図 3.1.77　試験対象と検証で使用する測定器

3.1.13.4.1. ア）負荷集中時のレスポンスタイムの測定及び、サーバの CPU 負荷率の測定

(1) 検証方法

サーバの CPU 使用率を測定するために、TOP コマンドを使用した。TOP コマンドは、Linux や FreeBSD でリソースを管理するのに一般的なコマンドで、キャラクタベースで表示される。

また、サーバやネットワークのレスポンスタイムを測定するために PING を用いた。PING は、ICMP と呼ばれるプロトコルを用いて、ネットワーク層で機器の生死や到達範囲を確認するコマンドである。

① IPsecCA サーバ及び、IPsec ポリシーサーバの CPU 使用率をロギングするように設定する。
② IPsecCA サーバ及び、IPsec ポリシーサーバへ、継続的に PING をうち、ロギングするように設定する。
③ クライアント端末を 5 台用意する。
④ 1 台クライアント端末から、同時に「三鷹ポータル」にログインする。
⑤ 2 台クライアント端末から、同時に「三鷹ポータル」にログインする。
⑥ 5 台クライアント端末から、同時に「三鷹ポータル」にログインする。
⑦ 4.のときの CPU 使用率、PING の応答時間を集計する。

(2) 検証結果

CPU 使用率、レスポンスタイムは以下のようになった。

- 1 台　：　使用率　0.1%　　応答時間 1msec
- 2 台　：　使用率　0.0%　　応答時間 1msec
- 5 台　：　使用率　0.0%　　応答時間 1msec

(3) 結論・考察

問題となるようなエラーや、処理遅延は発生しなかった。上記結果から、ポリシーサーバは性能的に非常に余裕があり、クライアント数が多少増えても、想定できる範囲では問題にならないことが予想される。

3.1.13.4.2.　イ）過負荷時のサーバ及び、クライアントの動作状況

(1)　検証方法

① IPsecCA サーバ及び、IPsec ポリシーサーバの CPU 使用率をロギングするように設定する。

② IPsecCA サーバ及び、IPsec ポリシーサーバへ、継続的に PING をうち、ロギングするように設定する。

③ クライアント端末を 6 台用意する。

④ 5 台クライアント端末から、同時に「三鷹ポータル」にログインする。

⑤ クライアントが異常な動作をしないか確認する。

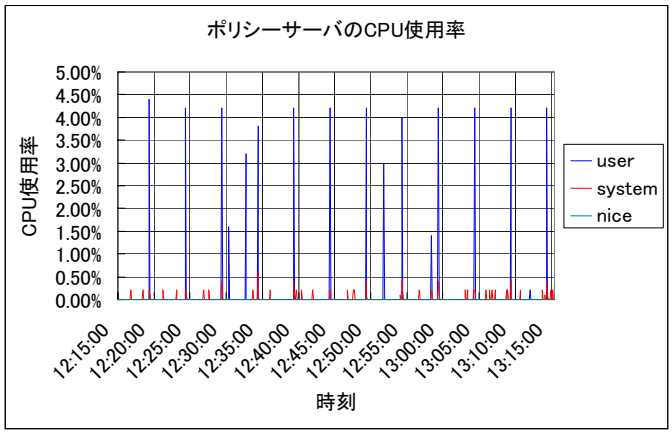
⑥ 4.、5. を 5 分おきに 10 回繰り返す。

⑦ 残り 1 台のクライアント端末から、「三鷹ポータル」にログインする。

⑧ 負荷のかかった後、特に異常がないことを確認する。

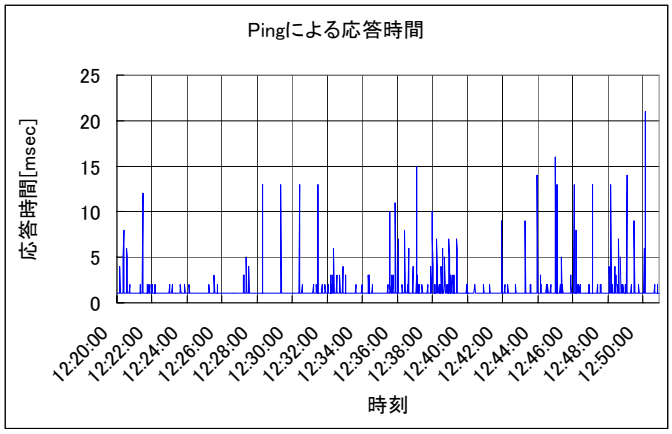
(2)　検証結果

同時にログインを行った 5 台のクライアントとも、正常にログインできた。また、10 回繰り返しても正常にログインできた。さらに、10 回繰り返しの後、残り 1 台のクライアントからログインを行っても、正常に動作した。



CPU の使用率は、10 分周期ごとに定期的に 4%前後まで上がっている。これは、アクセスによるものではなく、バックグラウンドプロセス（デーモンなど）による CPU 負荷だと考えられる。

図 3.1.78　ポリシーサーバの CPU 使用率



Ping の応答時間は 20msec 以下で、特に問題にならない程度である。

図 3.1.79　Ping による応答時間

(3)　結論・考察

本検証では、サーバ及び、クライアントは正常に動作した。しかし、同時に認証を多く発生させることは、現在の環境では難しい。今後、ユーザの利用が増えていく中で、長期的に安定して動作するかを、運用を通して検証していく必要がある。

3.1.13.4.3.　ウ）フェーズ毎のクライアント数やアクセス数と、サーバ処理能力の測定

(1)　検証方法

① トラフィック測定システム「SmartProbe」で IPsecCA サーバ、IPsec ポリシーサーバのクライアント接続数を測定しておく。

② 順次接続数が増えていく中で、サーバの処理能力がどのように変化していくかを確認する。

(2)　検証結果

クライアント接続数の推移を以下に示す。

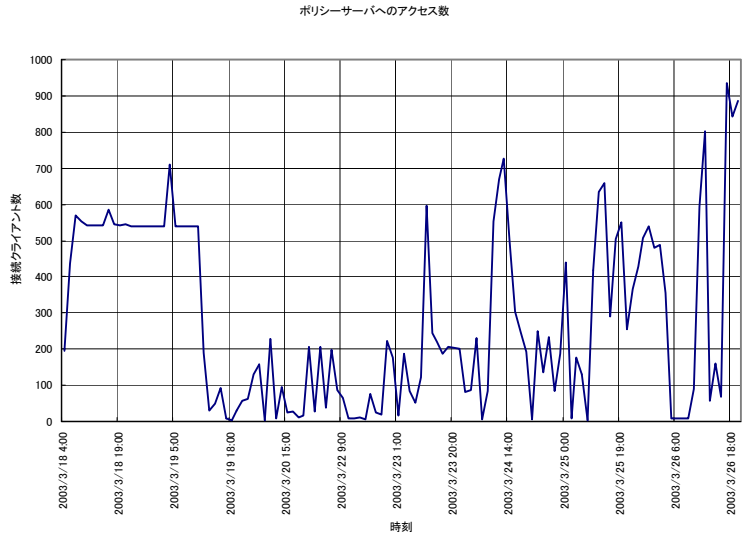


図 3.1.80　ポリシーサーバへのアクセス数

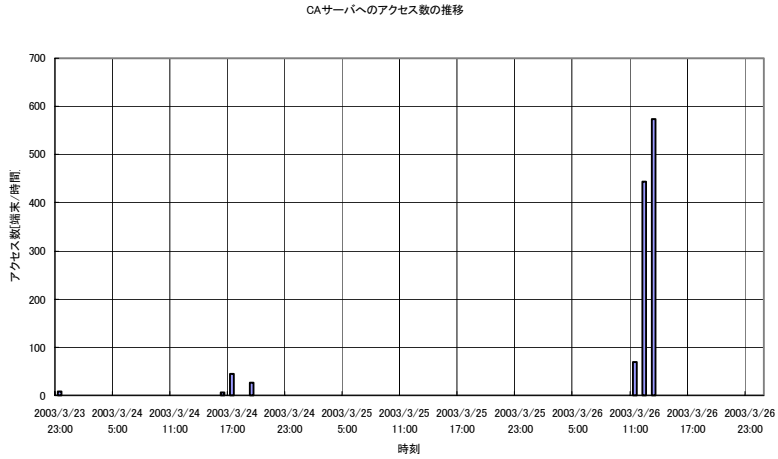


図 3.1.81　CA サーバへのアクセス数の推移

このデータは、1 分あたりの接続クライアント数を 1 時間分足したものである。このように、現段階ではまだユーザの利用が非常に少ない。3 月 26 日に多くのアクセスがあったが、同一クライアントとの通信によるためで、実際には数十端末程度のアクセスである。3 月 26 日の PING の応答時間を以下に示す。

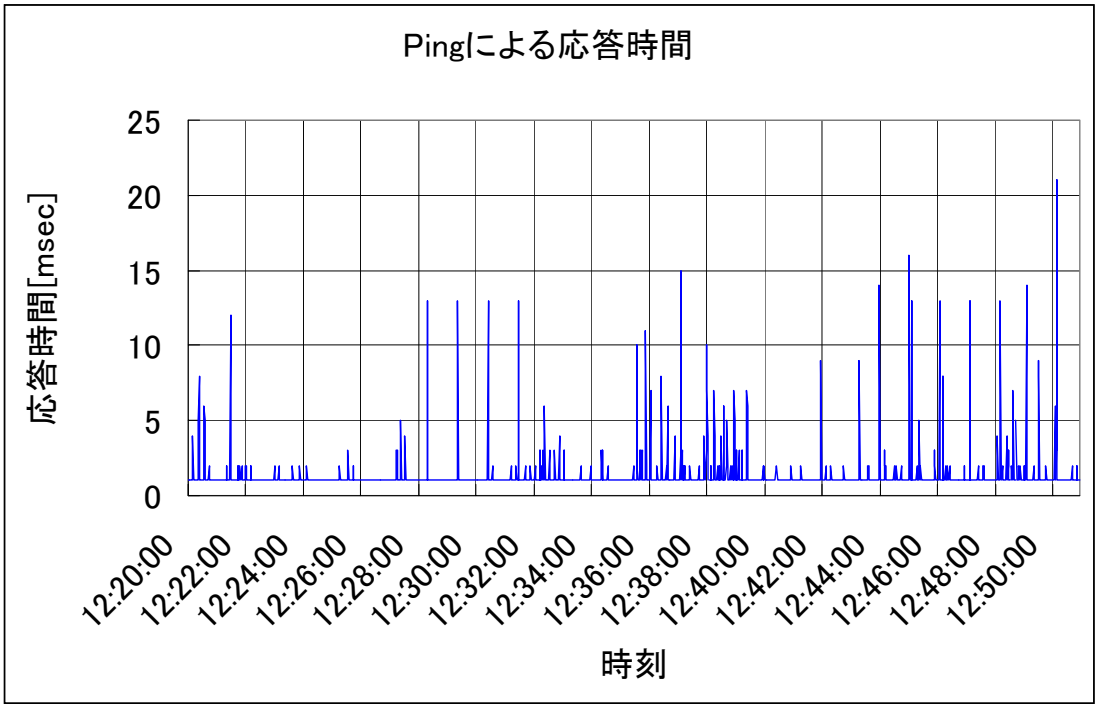


図 3.1.82　Ping による応答時間

Ping の応答時間は 20msec 以下で、特に問題にならない程度である。

(3)　結論・考察

現状のクライアント数であれば、サーバの性能には影響を与えない。ただし、クライアントの同時アクセス数が、数百・数千台となると指数的に負荷が上がる可能性がある。長期的に継続して推移を監視する必要がある。

3.1.13.5.まとめ

表 3.1.41　検証内容と検証結果のまとめ

項目	検証内容	結果
ア)	負荷集中時のレスポンスタイムの測定及び、サーバの CPU 負荷率の測定	レスポンスタイムや CPU 負荷率は、それほど高くならず問題にならない。
イ)	過負荷時のサーバ及び、クライアントの動作状況	過負荷状態でも、サーバ及び、クライアントは安定して動作する。
ウ)	フェーズ毎のクライアント数やアクセス数と、サーバ処理能力の測定	現段階では、処理能力は問題ない。長期にわたる継続的な監視が必要。

本検証では、CPU やネットワークの過負荷時の性能に関する検証を行った。実際に多くの負荷をかけることが難しく、傾向からの推定による検証が多い。同時に数百台や数千台からの要求があったときに耐えうる検証をすることは、非常に困難な検証である。

現在一般的に行われているシステムのさまざまな検証では、アプリケーションレベルまでレイヤの上がった負荷試験を行うことが難しい。ソフト開発なでは、特別な負荷発生装置を開発して負荷試験をすることが多いのが現状である。

一方、ネットワーク・インタフェース・カードの高機能化により、IPsec 機能がハードウェアにより処理できるようになってきた。これは、サーバやクライアントの CPU 負荷を下げる効果がある。また、ネットワークは高速化が著しく、10GbitEthernet もサービスが開始されている。今後の運用状況を監視しておく必要はあるが、将来的に IPsec によるセキュリティ確保しても、性能を維持できると推測される。

長期的なアプリケーションレベルの性能監視には、サーバ内部やネットワークに挿入するパフォーマンス監視ツールを利用すると、容易に傾向を把握できる。

3.1.14. デジタルビデオ映像等を WMT 形式等に容易に変換するための技術検討

3.1.14.1.検討概要

エンドユーザが実際にデジタルビデオコンテンツを公開する際に必要であったメディア変換、サーバへのアップロード、番組サーバへの登録などの煩雑な作業をなくし、特別な知識が無くても簡単な操作で前述の作業を一括して行う技術を開発し、ユーザがコンテンツを提供しやすい環境は、いったい何かを検討し、IPv6 マルチキャストを使った映像コンテンツ配信ビジネスに向けた検討を行う。

3.1.14.2.検討目的

現状、一般のユーザがデジタルビデオコンテンツを公開するのは多くの煩雑な手順を踏まなくてはならない。また、そのためにいくつかの知識が必要となり、容易に利用することが困難な状況になっている。以下にその手順を示す。

① DV 機器で録画を行う。
② 録画した画像をパソコンに読み込みファイルに保存する。(このときファイル形式は、AVI や MPEG2 が一般的)
③ 録画した画像を配信用にフォーマット変換しファイルに保存する。(ここで Windows Media Video に変換する)
④ 配信サーバにファイルをアップロードする。
⑤ 配信する番組表や Web ページを作成する。

上記作業には、高スペックのパソコンや高機能な編集ソフトが必要になる場合が多い。また、各作業にはある程度の知識が必要になるため、一般ユーザにはなかなか使いにくいものである。

本検討では上記の作業を自動化するシステムを開発するとともに、ユーザに使いやすいものであるか、今後の改良の方向性などを探る。

3.1.14.3.検討項目

表 3.1.42　検討内容

項目	検討内容
ア)	アプリケーションの開発と単体動作検証
イ)	サーバ類の構築とフィールドでの結合試験、総合動作試験
ウ)	ユーザへのアプリケーション開放
エ)	ユーザの要望をアンケート等により収集
オ)	要望内容のとりまとめ
カ)	開発へのフィードバック
キ)	フィールド検証
ク)	IPv6 マルチキャストを使った映像コンテンツ配信ビジネスに向けた検討

3.1.14.4. 検討環境

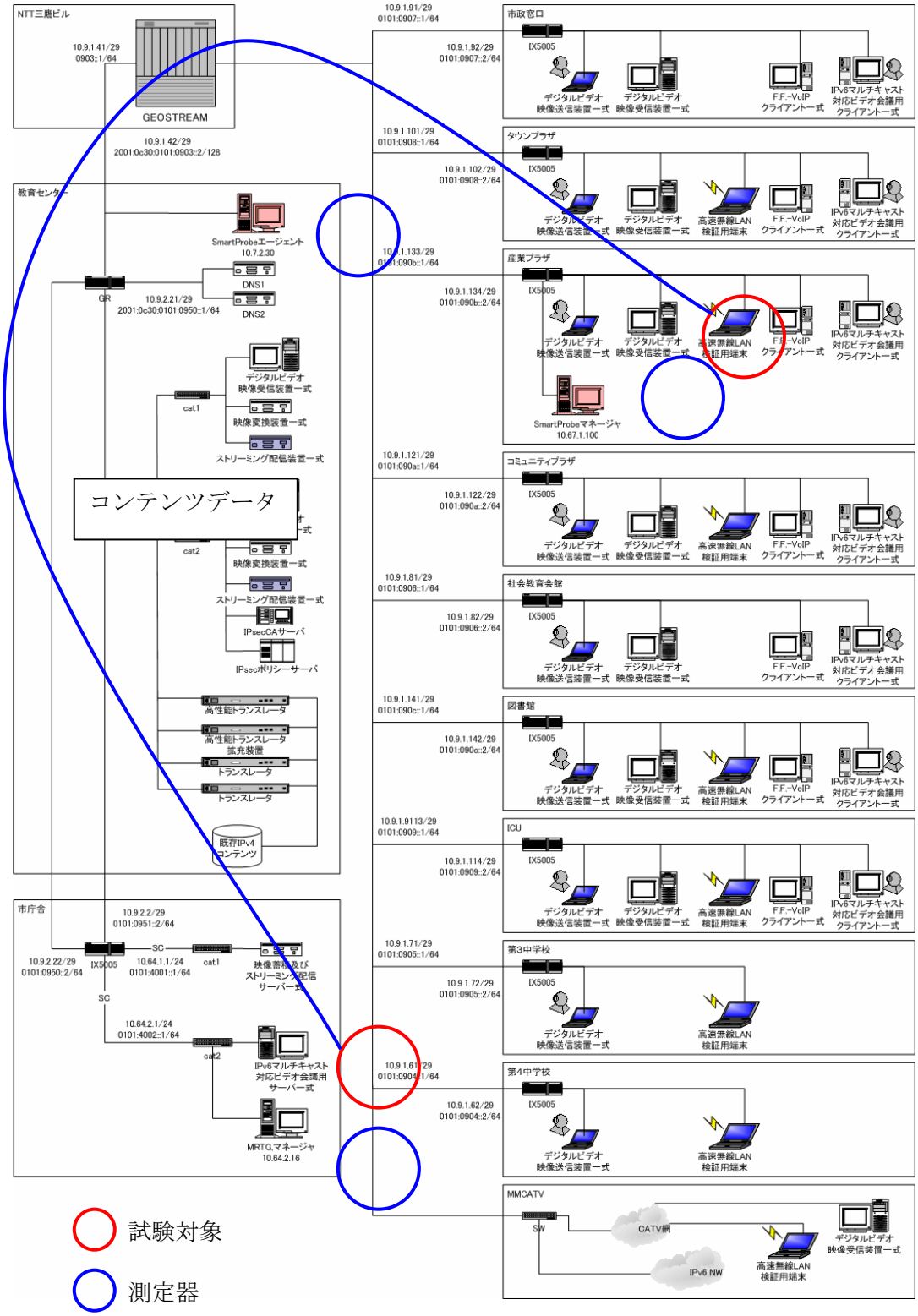


図 3.1.83　試験対象と検討で使用する測定器

3.1.14.5.検討方法と結果

3.1.14.5.1.　ア）アプリケーションの開発と単体動作検証

(1)　検討方法

アプリケーションの開発を行う。

(2)　検討結果

主な機能は以下のとおりである。

① ネットワーク経由でのコンテンツアップロード機能
② 映像変換機能
③ WMT による映像配信機能
④ コンテンツ管理機能

以下に開発したアプリケーションの画面を載せる。また、「映像管理ソフトに関する仕様書」を付録として添付する。

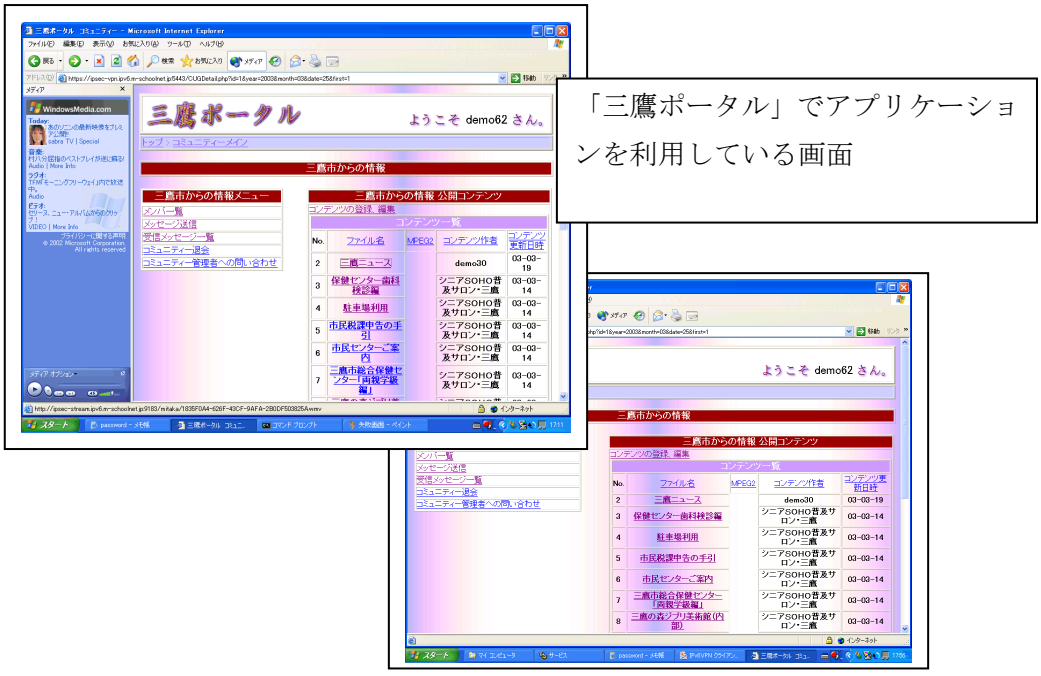


図 3.1.84　「三鷹ポータル」でアプリケーションを利用している画面

(3) 結論・考察

アプリケーションの開発及び、単体検証は、無事終了した。

3.1.14.5.2. イ）サーバ類の構築とフィールドでの結合試験、総合動作試験

(1) 検討方法

① コンテンツ蓄積配信サーバを市庁舎に構築する。

② クライアントからアップロード及び、ダウンロードが出来ることを確認する。

(2) 検討結果

図 3.1.85 に示す画面から、コンテンツのアップロードを行い、正常に再生できることを確認した。

検証した際の検査結果を表 3.1.46 に載せる。

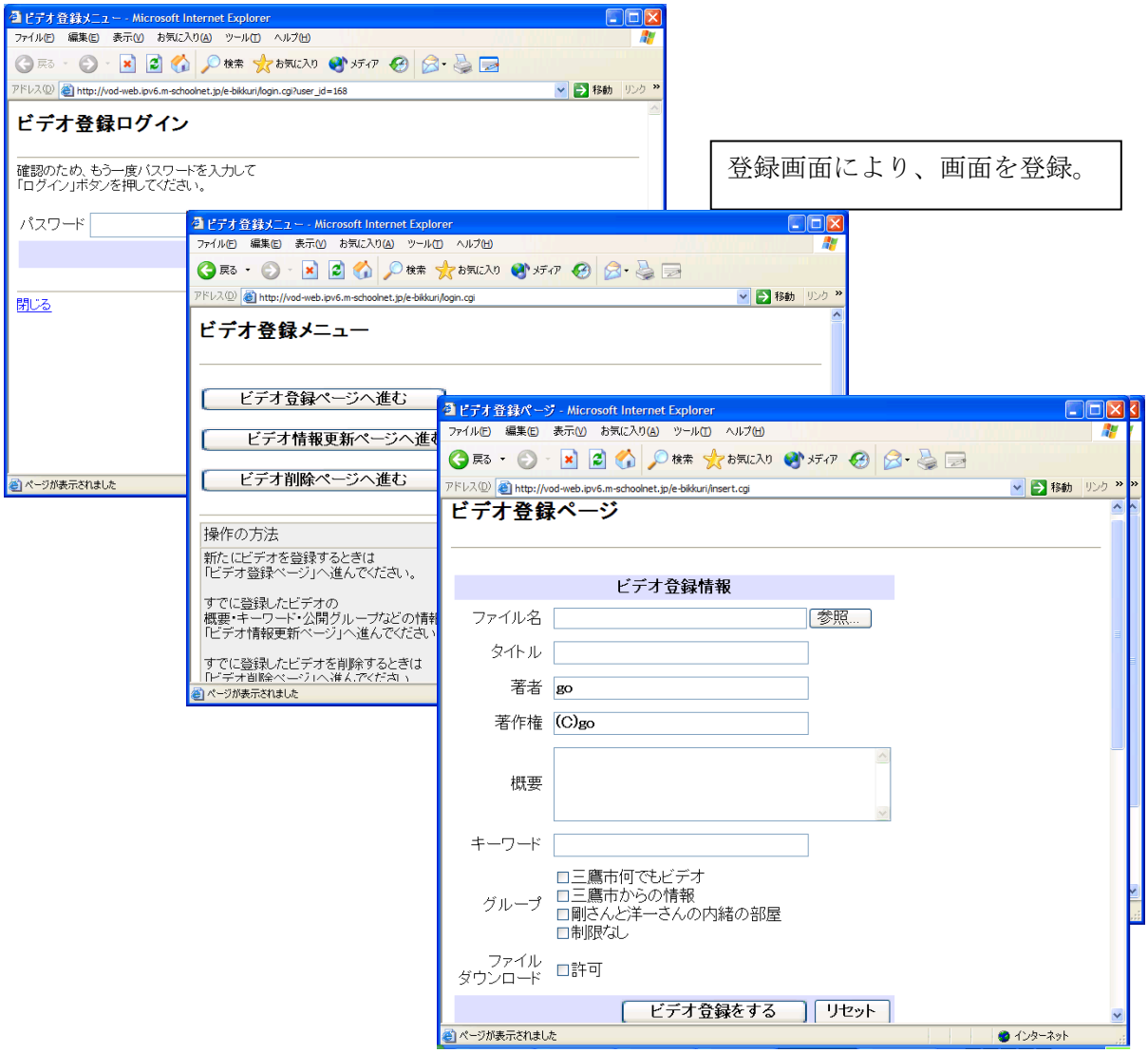


図 3.1.85　コンテンツのアップロード画面

(3)　結論・考察

総合試験では表 3.1.46 の試験結果の通り動作を確認した。サーバ類の構築後、フィールドでコンテンツのアップロード及び、ダウンロードを行ったが、動作確認が出来るようになるまで、非常に時間がかかった。アップロードあるいは登録の機能に関して、うまくいかないときがあった。

3.1.14.5.3.　ウ）ユーザへのアプリケーション開放

(1) 検討方法

① 市民ｅモニタにアプリケーションを開放する。
② 市民ｅモニタにアカウントを配布する
③ 市民ｅモニタにアクセス方法を説明する。
④ コールセンタを設置し、市民ｅモニタからの問い合わせに答える。

(2) 検討結果

2 月 24 日「e!School 三鷹モデル」キックオフセレモニーから、市民ｅモニタにアプリケーションを開放した。運用サポート面ではコールセンタを開設し、問い合わせに対し対応している。

また、3 月 8 日にはモニタ集会を開き、実験の目的や「三鷹ポータル」の利用方法をモニタの方に説明した。

(3) 結論・考察

ユーザへのアプリケーションの開放は無事完了した。

今後、市民 e モニタの数が増えていくに従い、さまざまな発展が考えられる。インフラとしてのネットワークやアプリケーションの検討ではなく、地域文化、特に教育方面への応用が大いに期待される。

生徒のコンテンツ作成で「課題を創造」し、自由度の大きい教育が考えられる。また、先生のコンテンツ作成で「生徒への教材の作成」、「家庭への情報の提供・問題の共有」などの可能性もある。さらに、保護者間のコンテンツ作成･閲覧により、「保護者間、地域の交流」が盛んになることも期待できる。上記コンテンツのうち、運動会や遠足の様子を未就学児に公開などさまざまな利用形態が考えられる。

3.1.14.5.4.　エ）ユーザの要望をアンケート等により収集

(1)　検討方法

① アンケートを作成する。
　利用歴、年齢などの利用者の背景となる知識から質問する。
② 市民ｅモニタにアンケートを配布する。
③ アンケートを収集する。

(2)　検討結果

ユーザからのアンケート結果を以下に記す。

- 利用歴：7 年以上（85%）、4～6 年（15%）
- 年代：40 代（58%）、30 代（28%）、50 代（14%）

- 三鷹ポータル：

① 画像ファイルのアップロードが出来ないことがある。
② デザインがよくない。殺風景。
③ マニュアルやヘルプがほしい。
④ うまくいかないことが多い。
⑤ 「戻る」ボタンを押すとおかしくなる。「戻る」のリンク場所が押しにくい。
⑥ フレームを使ったりして、使いやすくしてほしい。
⑦ リンクが少なく使いにくい。
⑧ 動画の感想を掲示板に書けるようにしてほしい。
⑨ 市民ｅモニタの紹介画面がほしい。

- コンテンツ：

① 絵がきれい。
② 図書館の利用方法を見ることが出来てためになった。
③ ジブリのコンテンツが楽しい。
④ 画像品質、音声品質がよい。

(3) 結論・考察

アンケートの結果では、ユーザはなかなか利用できていないようである。DV 機器を持っているユーザが少ないことや、期間が短いことなどが原因として考えられる。VHS からアップロードできる機材が市の施設にあると、更にユーザがコンテンツを作りやすいかと思われる。

3.1.14.5.5. オ）要望内容のとりまとめ

(1) 検討方法

① e モニタから収集したアンケートを集計する。
② 要望を機能、性能、品質などにわけ整理する。

(2) 検討結果

アンケートの結果を以下に示す。

- 機能に関して：

① 12 ビットの音声だけでなく、16 ビットの音声にも対応してほしい。
② 簡単に登録できるので、作業がわずらわしくなく使いやすい。
③ サポートしている画像ファイルのフォーマットを増やして欲しい。
④ コンテンツの配信ビットレートを自由に設定させて欲しい。
⑤ ファイルが多くなってくると、使いにくくなるかもしれない。

- 性能に関して：

① 特に問題ない。
② 思っていたより早い。

- 品質に関して：

① 画面の見栄えがよくない。
② うまくアップロードできないことがあった。

(3) 結論・考察

ユーザは概ね使えているようだが、今後、改良していく余地がある。さらに何度か更新を続けるとともに、多くのユーザに利用してもらい、意見をフィードバックしていくとよい。

3.1.14.5.6.　カ）開発へのフィードバック

(1) 検討方法

アンケートからの要望を開発の要求事項としてまとめる。

(2) 検討結果

「12 ビットの音声だけでなく、16 ビットの音声にも対応してほしい。」という要望に対し、実際に機能追加を行った。

DV の音声に関して、16 ビット 48kHz サンプリング、12 ビット 32kHz サンプリングの 2 通りある。通常一般的な目的では、12 ビットのサンプリングを用いることが多い。しかし、より高音質を求められる場合、16 ビットのサンプリングでの録音をすることもある。

このようなコンテンツを利用したいという要望に対し、16 ビットサンプリングにも対応させる開発を行った。

(3) 結論・考察

今後、さらに利便性を高める必要がある。以下に要求事項をあげる。

① GUI を改善し、より使いやすく見栄えのよいものを作る。
② ＤＶから直接アップロードできる仕様を検討する。
③ クライアントにアップロードソフトをインストールする構成を検討する。
④ 圧縮やバッチ処理などにより、高速・手間のかからないアップロード方式を検討する。
⑤ 設定内容を豊富にしたり、対応フォーマットを増やしていく。

上記を踏まえ、さらによいアプリケーションを開発していくとよい。

3.1.14.5.7.　キ）フィールド検討

(1) 検討方法

アプリケーションをフィールドで確認する。

(2)　検討結果

実際にフィールドで動作している様子を以下に載せる。

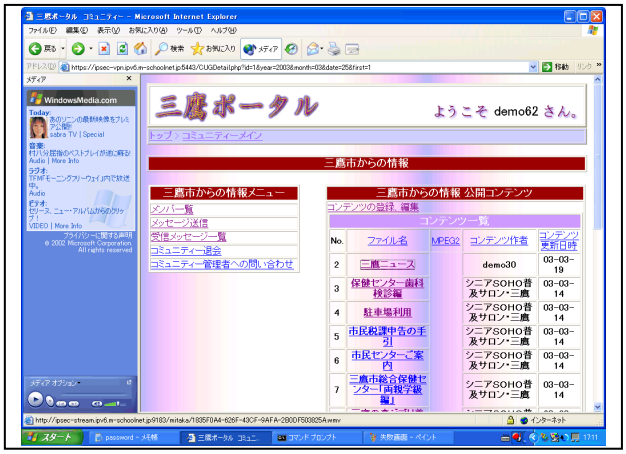


図 3.1.86　「三鷹ポータル」画面

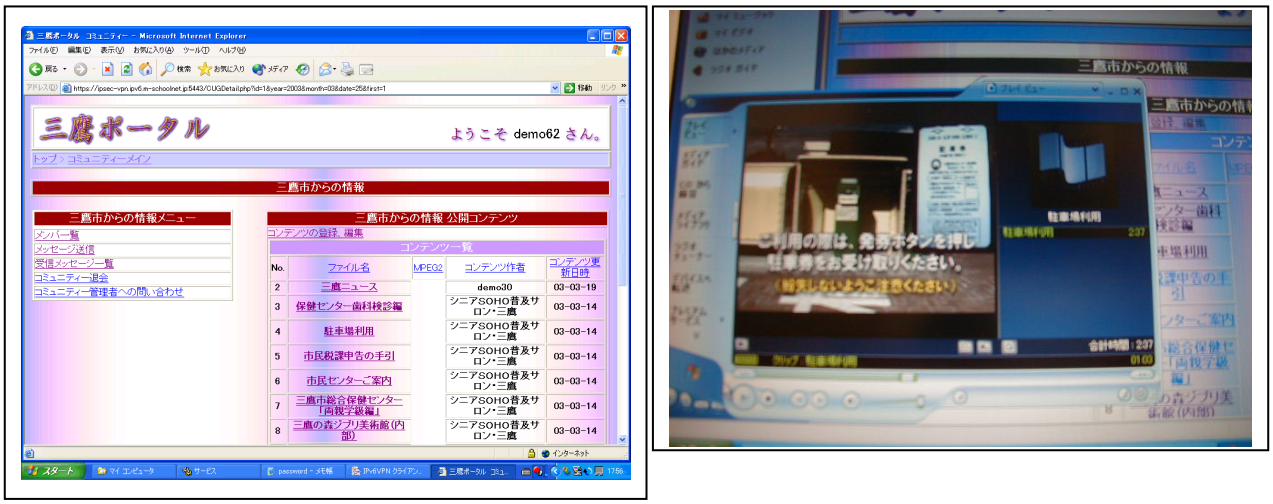


図 3.1.87　「三鷹ポータル」映像コンテンツ再生の様子

(3)　結論・考察

本アプリケーションは IPv6 の IPsec、DV アップロード及び WMT に自動変換しダウンロードすることが出来る最先端のシステムである。正常に動作しているが、うまくいかないときがあるようである。しかし、アップロードされているコンテンツが少ない、閲覧するユーザが少ないなど、もうしばらく時間が経過し利用者が増えるのを待ってから、安定性を検討する必要がある。

3.1.14.5.8.　ク）IPv6 マルチキャストを使った映像コンテンツ配信ビジネスに向けた検討

(1)　検討結果

世界でもトップレベルの普及率となったブロードバンドネットワークの利用目的として、映像コンテンツ配信は中心となるアプリケーションである。映像コンテンツ配信ビジネスを支えるために、ネットワークに要求される条件・課題は、以下のようなものがある。

① 大きな帯域の通信に耐えられる性能、品質
② 多くの顧客、広いエリアをサポートできるスケーラビリティ
③ 課金方式と不正アクセスの防止

IPv6 マルチキャストは、広帯域の通信を非常に効率よく送受信する機能を持つ。特に膨大な数のユーザが同時に同じコンテンツを視聴するライブ配信などを行うことが可能である。また、帯域を大幅に節約することにより、インフラのコストを低減することが可能である。

IPv6 プロトコルは広大なアドレス空間を持ち､IPv4 アドレスの枯渇の問題がない。また、サーバがなくても、自分自身のアドレスを生成する機能を持ち、簡単にネットワークへ接続することが出来る。

ユーザがそれぞれグローバルで一意なアドレスを持つため、課金に関する情報を扱いやすい。また、同じ理由で不正アクセスを防止することが可能である。

(2)　結論・考察

映像コンテンツ配信は IPv6 マルチキャストを用いることにより、効率的に多数のユーザにセキュアな環境を得ることが出来る。各家庭にブロードバンド環境が整ってきている現在の情況から、今後は、インフラ及びアプリケーションの IPv6 対応が進めば、コンテンツホルダが容易にコンテンツ配信ビジネスへ参入できるものとなる。

3.1.14.6.まとめ

表 3.1.43　検討内容と検討結果のまとめ

項目	検討内容	結果
ア)	アプリケーションの開発と単体動作検証	完了
イ)	サーバ類の構築とフィールドでの結合試験、総合動作試験	完了
ウ)	ユーザへのアプリケーション開放	完了
エ)	ユーザの要望をアンケート等により収集	今後、ユーザが順次増えていくにしたがって、ユーザの要望を集め、さらに使いやすいアプリケーションにするとよい。
オ)	要望内容のとりまとめ	
カ)	開発へのフィードバック	
キ)	フィールド検証	
ク)	IPv6 マルチキャストを使った映像コンテンツ配信ビジネスに向けた検討	本文参照

3.1.15. 上記ネットワーク設備の運用管理技術の確立とその評価

3.1.15.1.検討概要

検証 1 から 3.1.13 検証 13 の技術検証を通して、最低限必要なネットワーク設備の運用について、MMCATV や既存の学校インターネットを運用している部署と協力し、IPv6 ネットワークの運用管理技術を確立し、評価する。

3.1.15.2.検討目的と進め方

本検討では、IPv6 マルチキャスト及び、IPsec による高性能かつ機密性の高いネットワークが、学校教育や地域社会にどのように貢献できるのか、構築に際しての経験と問題点、今後の発展性を検討する。

(1) 実証ネットワークの設計段階から、運用を意識したネットワーク設計を行い、MMCATV や既存学校インターネットの運用担当と密に連絡を取る。
(2) 構築フェーズでも、お互いの責任分担を明確にし、既存の商用サービスや研究設備に影響が無いように十分留意し、より効率的な検討が行えるようなネットワークを構築する。
(3) IPv6 の特徴の１つであるセキュリティ面を十分考慮したネットワークを構築する。
(4) 問題点が発生した場合は、プロジェクト管理手法等、的確な手法を用いて、解決する。
(5) ネットワーク監視装置の責任範囲については、既存サービスを十分考慮し、お互いの協力により、構築する。
(6) 管理対象や監視周期等の監視パラメータ、トラフィック管理、故障管理、IP アドレス等の構成管理パラメータ等についても、お互いの立場を理解し、相互に協力し合う。

3.1.15.3.検討項目

表 3.1.44　検討 14 の検討内容

項目	検討内容
ア）	設計段階からの問題点等を整理し、より効率的な設計が行えたか
イ）	既存の商用サービスや研究設備に影響がない構築が行えたか
ウ）	セキュリティ面を十分考慮したネットワークが構築できたか
エ）	問題点が発生した場合は、プロジェクト管理手法により、迅速に解決が行えたか
オ）	ネットワーク監視方法について、十分な議論が行われ、効率的な監視体制で運用できたか
カ）	性能管理や構成管理、故障管理等の管理方法について、効率的な管理ができたか
キ）	IPv6 に対応したネットワーク管理手法を確立できたか

3.1.15.4.検討方法と結果

3.1.15.4.1.　ア）設計段階からの問題点等を整理し、より効率的な設計が行えたか

(1) 検討方法

構築結果に関する考察を行う。

(2) 検討結果

IPv6 固有の問題点として、以下のような問題点が予想された。

① ルータやスイッチ、OS の安定性

製品が新しく、まだ不具合が残っている可能性がある。

② 各ベンダの機器間の相性

製品が新しく、接続した実績が少ない。

③ 障害時の切り分け

障害時に切り分けを行うノウハウや、信頼性の優劣、回避方法が確立されていない。

④ ネットワーク管理ツール

NMS や性能監視ツールなどの IPv6 への対応が完全ではない。

上記を踏まえ、設計のポイントとして以下のような思想で検討を行った。

① トポロジを出来るだけシンプルにする。

② 各機器の役割を明確にする。

③ 構築及び、障害原因の切り分けが容易なように、各拠点が同一の構成になるようにする。

(3) 結論・考察

3.1.15.4.2. イ）既存の商用サービスや研究設備に影響がない構築が行えたか

(1) 検討結果

技術面については、以下のことで協力して作業を進めた。CATV サービスでは独自の IPv4 プライベートアドレスを用いており、DHCP によりアドレスを管理し、割り振りを行っている。このアドレスは商用サービスとしてのエンドユーザが接続する端末に加えて CATV 網の終端装置であるケーブルモデムにも管理用として設定される。一方、「e!School ネットワーク」では、DNS 通信用として IPv4 プライベートアドレスを使用しており、ネットワーク間を移動する端末の IPv4 アドレスを自動で設定するために DHCP で管理する必要がある。その為に今回の学区内アクセスポイント接続用セグメントには同じネットワーク上に「CATV 管理用 IPv4 アドレス」と「e!School ネットワーク用 IPv4 アドレス」を共存させ、これら 2 つのアドレス体系を付与する為の 2 つの DHCP サーバを設置する必要があり、「e!School ネットワーク」端末を CATV 網経由で「e!School ネットワーク」に接続する場合、「e!School ネットワーク」端末には「e!School ネットワーク」の IPv4 アドレスを、ケーブルモデムには CATV 網の IPv4 アドレスを割り振る必要がある。

検証を行なった結果、２つの DHCP が共存した状態で CATV 網に端末もしくはケーブルモデムを接続すると CATV 網の IPv4 アドレスを取得することが判明し CATV 網の DHCP サーバが「e!School ネットワーク」の DHCP サーバと比べてレスポンスが早いこと判明したので、CATV 網の DHCP 機能に「e!School ネットワーク」で使用する端末の MAC アドレスを全て登録しこれらのアドレスを無視する設定を行なった。この

対処を行なうことで「e!School ネットワーク」端末には「e!School ネットワーク」の IPv4 アドレスを、ケーブルモデムには CATV 網の IPv4 アドレスを割り振る事ができた。

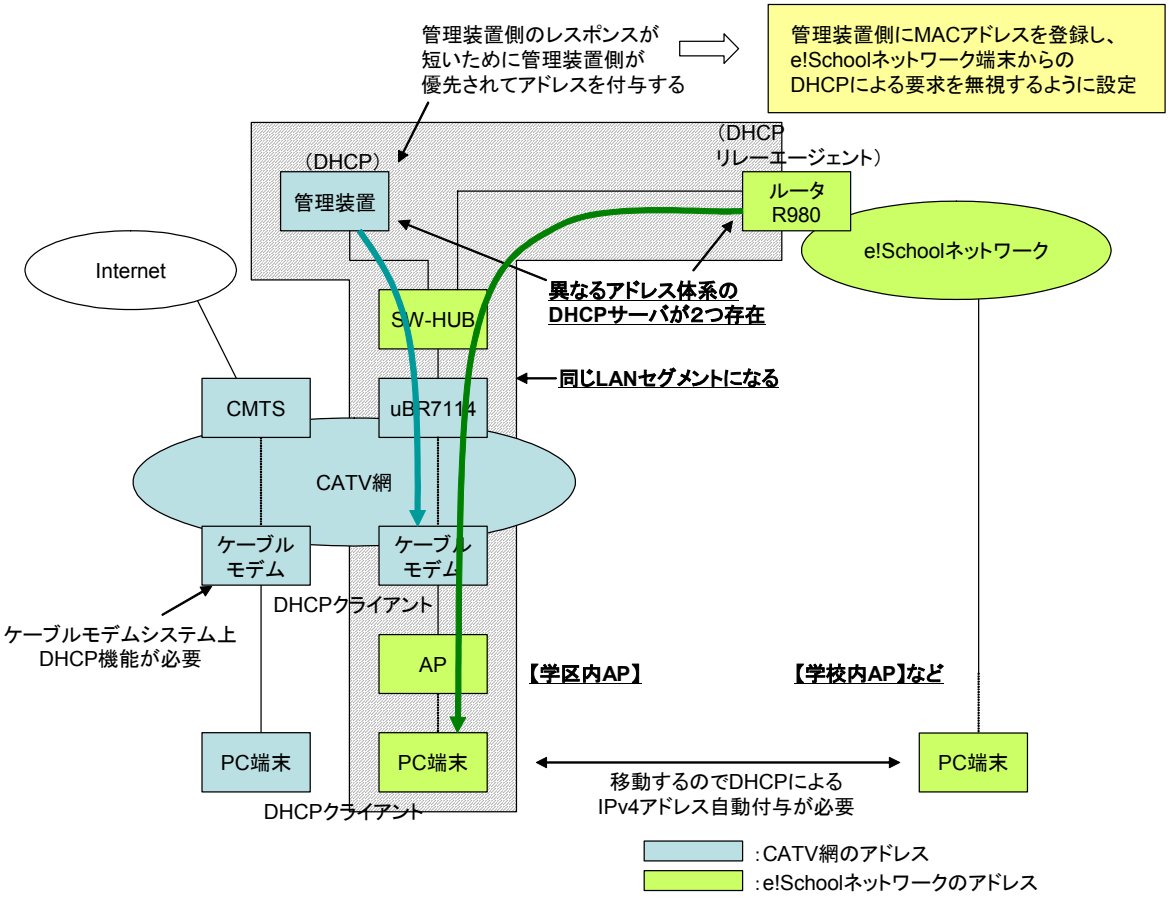


図 3.1.88　「e!School ネットワーク」と CATV 網の DHCP 構成図

(2)　結論・考察

三鷹市及び、MMCATV と連携し、既存の商用サービスや研究設備に影響がない構築を行うことが出来た。

3.1.15.4.3.ウ）セキュリティ面を十分考慮したネットワークが構築できたか

(1)　検討結果

相互接続のネットワークであるインターネットでは、不特定多数の利用者が互い

のネットワークにアクセスする。そのような環境では、悪意を持ったユーザに、個人情報が盗聴されたり、機器が攻撃を受けたりするような事態が発生する。インターネットの普及に伴い、攻撃から防御するためにセキュリティ対策が重要な課題となっている。悪意を持ったユーザからの被害の一例としては以下のようなものがある。

- 攻撃によるサービスの停止（DoS 攻撃、ウィルスメールなど）
- 企業・個人情報の盗聴
- 著作権の侵害

攻撃に対し、セキュリティを守る手段としては、認証・暗号化がある。

一方、「e!School ネットワーク」では、各アプリケーションの多くは通信の際に IPsec 機能を利用している。また、IPsec 通信を行わないアプリケーションも、IPsec 用のアダプタを接続することにより、ネットワークを流れるパケットは暗号化されている。

(2) セキュリティなどに関する三鷹市との打ち合わせ内容

セキュリティに関しては、三鷹市と何度も打ち合わせを重ねた。

①三鷹市庁内ネットワークとの接続

- 内容

  三鷹市より生涯学習用の端末として三鷹市庁舎の端末を利用するための庁内ネットワークと e!School ネットワークを接続いたいとの要望があった。また、配線の負担を減らすために三鷹市庁舎内に設置する F.F-VoIP 端末について庁内ネットワーク経由で接続することが望ましかった。

- 問題点

  設計・構築時点に IPv6 でのファイアーウォールが製品化されておらす、接続を行なった場合に庁内ネットワークの端末から e!School ネットワーク側のみならず e!School ネットワーク側の端末から市庁舎内の端末にアクセスが可能となってしまう。

- 結論

  市民のデータ流出などは絶対あってはならないので庁内ネットワークとの IP レベルでの接続は行なわない事とした。但し、庁内ネットワークに e!School ネットワーク用の VLAN を追加し、この VLAN と e!School ネットワークとの接続を行うことで庁内ネットワークを経由して F.F.-VoIP 端末を接続した。これにより、セキュ

リティを保つのと同時に配線工事を最小限にし、端末移動時にも庁内ネットワークの VLAN 設定を変更することで簡単に対応できるようにした。

②学校インターネットとの接続

- 内容

  既存の学校インターネット上のサーバおよび IPv4 インターネットと接続するために e!School ネットワーク及び既存学校インターネットを接続する必要がある。

- 問題点

  学校インターネットは外部インターネット接続する際にファイアウォールを使用してセキュリティを保っている。しかし、e!School ネットワーク側は IPv6 でインターネットと接続を行なうがファイアウォール製品が無いので高度なセキュリティ設定を行なうことができない。また、Windows XP はアドレスを自動設定する際に MAC アドレスをベースとする IPv6 アドレス（Public）とアドレスの一部（下位 64bit）をランダムに生成する IPv6 アドレス（Anonymous）の２つを生成して、通常通信を行なう場合には Anonymous アドレスを使用するため、サーバなどで通信ログを記録してもだれがアクセスしたか解析できない可能性がある。

- 結論：

  IPv6 インターネットとの接続点となる GeoStream にて学校インターネットと接続を行なうためのトランスレータ装置群と通信できる範囲を今回構築したネットワーク及び生涯学習市民 e モニタとして登録されたネットワークのみに制限した。また、IPv6 アドレスに関しては Anonymous 方式の IPv6 アドレスの使用を禁止する設定を行いかならず Public 方式のアドレスを使用させることで IPv6 アドレスから MAC アドレスを計算し端末を割り出せるようにした。

なお、当初予定していた授業風景の配信など、学校や地域と連携して進めていく課題については、様々な問題で十分な検証ができなかったので来年度以降に充実を図る予定である。

(3) 結論・考察

セキュリティに関して、三鷹市と多くの議論を行い、十分な検討が出来た。

IPv6 の IPsec 機能を用い、暗号化や認証を使った通信を行うネットワークを構築した。また、監視や特定の用途のためにプライベートの IPv4 アドレスを割り振った。IPv4 のプライベートアドレスには、外からアクセスすることは出来ない。上記によ

り、セキュリティ面では十分な考慮を行えた。

3.1.15.4.4. エ）問題点が発生した場合は、プロジェクト管理手法により、迅速に解決が行えたか

(1) 検討方法

プロジェクト管理に関する考察を行う。

(2) 検討結果

多種多様化したネットワークの構築において、プロジェクト管理は必須の事項である。ISO9000 や PMBOK などプロジェクト管理手法には、さまざまなものがある。プロジェクト管理手法では、一般的に以下のステップをスパイラルに行うことが謳われている。

① Plan(計画)

・プロジェクト目標の設定
・リソースの確保
・スケジュールを立てる
・目標品質の設定
・リスクの洗い出し

② Do（実行）

以下を考慮しながら計画を実行する。

・工数（費用）
・スケジュール
・資源

③ Check（評価）

計画と実行結果を見比べ評価を行う。

④ Action（見直し）

計画通りに行かないものについて見直しを行う。

これらに基づき、本プロジェクトでも独自の管理手法に基づき、構築を行った。
具体的にはほぼ定期的に進捗会議・連絡会議を行った。

(3) 結論・考察

構築では切り分けと問題点の整理を行うとともに、各ベンダと調整して迅速な解

決を行うことが出来た。しかし、問題点が発生した場合に、非常に複雑で高度な技術が必要である。運用に際しては高いレベルの技術者が必要で、今後の課題である。

3.1.15.4.5. オ）ネットワーク監視方法について、十分な議論が行われ、効率的な監視体制で運用できたか

(1) 検討結果

ネットワークに求められる信頼性により、さまざまな監視形態がある。ネットワークシステムのダウンが、すぐに企業の損失を招く場合、24 時間体制の監視と早急な復旧が必要になる。そのためには、監視体制だけでなくさまざまなツールの導入が必要である。これらのツールのうち、代表的なものを以下にあげる。

① 障害監視ツール（NMS ネットワーク・マネジメント・システム）
- PING によるサーバ及び、ネットワーク機器の死活監視

② パフォーマンス監視ツール（SNMP 系のツール）
- トラフィック量の監視
- サーバのリソース（メモリ、ディスク、CPU など）の監視

③ サービス監視ツール（アプリケーションレベルの監視）
- サーバアプリケーションの応答時間、リソース使用量の監視

④ セキュリティ監視ツール（Firewall、IDS）
- 侵入監視
- 攻撃の防御
- メールのウィルスチェックなど

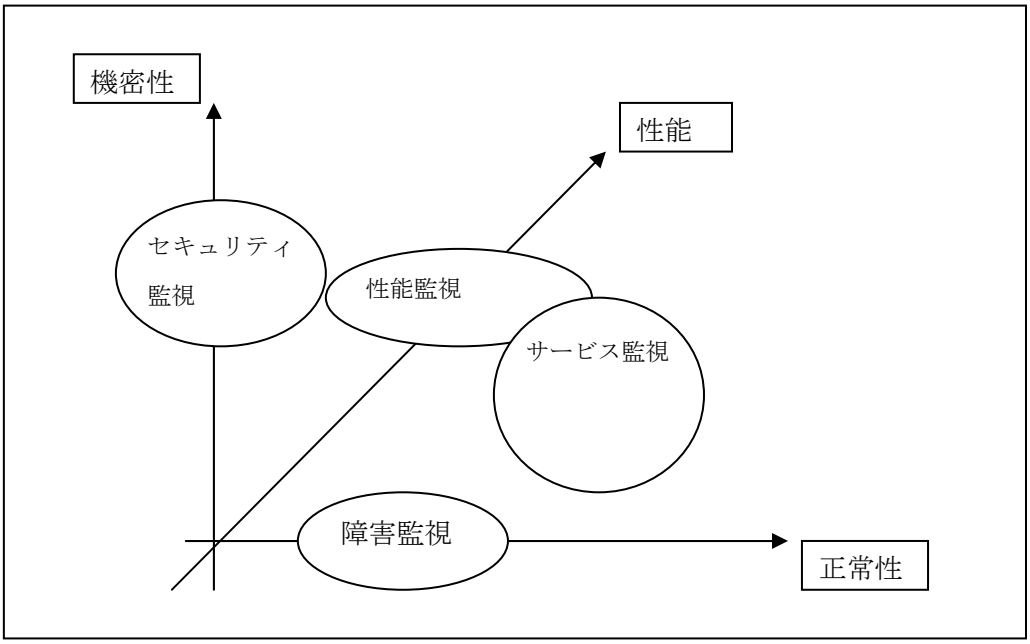


図 3.1.89　各ネットワーク監視項目の相関

上記のような監視を行うのは、エンドユーザや ISP（インターネット・サービス・プロバイダ）の他に MSP（マネージメント・サービス・プロバイダ）サービスなどのような、アウトソーシングを行う企業のサービスとして提供されている。そのサービスの形態としては、常駐・遠隔監視・定期巡回・オンサイト（呼び出しによる駆けつけ)、ヘルプデスク（問い合わせに対するメールや電話での対応）などがある。

これらの中で、「e!School ネットワーク」では、遠隔監視を行っている。

(2)　結論・考察

ネットワーク監視は、大手町からの遠隔監視が可能となっている。このため、各拠点のルータ・スイッチだけでなくサーバのメンテナンスも行えるようにし、効率的な監視・運用体制が整えられている。

今後の課題としては、ユーザが増加しトラフィックが増えてきたときの、ネットワーク性能と品質の確保が重要である。障害・性能を監視するだけでなく、ネットワーク構成の再設計やトラフィック予測など、状況に応じた運用・管理とネットワークの見直しを行っていく必要がある。

3.1.15.4.6. カ）性能管理や構成管理、故障管理等の管理方法について、効率的な管理ができたか

(1) 検討結果

ネットワークに管理の 5 大要素は障害管理・構成管理・性能管理・機密管理・課金管理といわれている。それぞれにさまざまなツールが開発されている。その中の、障害管理や構成管理には、NMS が一般的に広く用いられている。また、性能管理に関しては幅が広く、回線のスループット・アプリケーションの応答時間・サーバのプロセッサ使用率など多岐にわたる。中でも RMON に代表されるリモートモニタは、性能管理の中心的な存在である。

「e!School ネットワーク」の実証実験ネットワークでは、24 時間の完全な管理は本ネットワークの主旨を考慮し、行っていない。構成管理、及び、障害管理に関しては、遠隔からメンテナンスが出来るような構成で監視を行うことにより、効率のよい管理方法をとっている。

また、トラフィック監視には、SmartProbe と MRTG のトラフィックモニタシステムを導入している。MRTG では各ルータの MIB 情報を収集して、入出力データ量の大まかな量を測定している。MRTG によりネットワーク全体のトラフィック状況を把握できるようになっている。教育センタと NTT 三鷹ビルを結ぶ回線では、主要なサーバの通信があるため、SmartProbe を用いてより詳細で高度な監視を行っている。

(2) 結論・考察

障害管理・構成管理については、簡易な管理を行っている。性能管理については、高速ネットワークであるため、ある程度しっかりした管理をしている。これらは、「e!School ネットワーク」に適応した効率的な管理といえる。

3.1.15.4.7. キ）IPv6 に対応したネットワーク管理手法を確立できたか

(1) 検討結果

IPv6 ネットワークを管理する際に、IPv4 と異なる点を以下にあげる。

- IPv4 が通信できていても IPv6 が通信できるとは限らない。
- IPv6 が通信できていても IPv4 が通信できるとは限らない。
- ユニキャストだけでなく、マルチキャストが通信できるかを監視しなくてはならない。
- アドレスを割り振るのは DHCP サーバでなく、ルータからの広告によるもので

ある。

- IPv6 は IPv4 に比べ、ネットワーク監視ツールが少なく、まだ実績が少ない。

上記を踏まえ、IPv4 と IPv6 の両方を用いた管理を行っている。

(2) 結論・考察

現段階では、IPv6 に対応したネットワーク管理ツールが出揃っていないのが現状である。そのため、既存の IPv4 と組み合わせることにより、柔軟で効率的なネットワーク管理を行うことが出来た。

しかし、IPv6 に特化したネットワーク管理手法の確立までにはいたっていない。確立に向けた課題としては、複雑で多岐にわたる障害に対し、非常に高いレベルの技術者が必要であることがあげられる。これは、機器やアプリケーションの IPv4 に比べると安定性が低いことと、マルチキャストや IPsec など高度で新しい技術に追従していくのが困難なためである。今後は、運用を重ねてノウハウを得るとともに、より運用しやすい手法を模索していく必要がある。

3.1.15.5.まとめ

表 3.1.45　検討内容と検討結果のまとめ

項目	検討内容	結果
ア)	設計段階からの問題点等を整理し、より効率的な設計が行えたか	効率的な設計が行えた。
イ)	既存の商用サービスや研究設備に影響がない構築が行えたか	影響の少ない構築が行えた。
ウ)	セキュリティ面を十分考慮したネットワークが構築できたか	セキュリティを考慮したネットワークを構築できた。
エ)	問題点が発生した場合は、プロジェクト管理手法により、迅速に解決が行えたか	迅速な解決が行えた。
オ)	ネットワーク監視方法について、十分な議論が行われ、効率的な監視体制で運用できたか	効率的な監視体制で運用が出来た。
カ)	性能管理や構成管理、故障管理等の管理方法について、効率的な管理ができたか	効率的な管理が出来た。
キ)	IPv6 に対応したネットワーク管理手法を確立できたか	IPv4 と共存させることにより、よりよい管理手法を確立した。

本検討を通したまとめを述べる。

① IPv6 マルチキャスト・IPsec を用いた高機能、高性能なネットワークをマルチベンダ構成で構築し、検討

② 世界的にも最先端の試みなので、構築・保守・運用に高いスキルが必要

③ 今回の検討では、ユーザの利用量がまだ少なく、引き続き検討を行う必要がある

④ 学校教育や地域に広く利用が期待できるが、成果を生かしていくためには、著作権、肖像権など制度面の課題がある

3.1.16. 付録

表 3.1.46　映像配信サーバ総合試験表

番号	項目	内容	合否
A-1	Web サーバ	IPv6 クライアント(Windows XP + SP1、以下同様)の Web ブラウザに GUI インタフェースを提供することが可能であること	良
A-2		GUI インタフェースは十分にわかりやすいこと	良
A-3		指定の IPv6 クライアントで快適に動作可能であること	良
A-4		クライアントと IPv6 にて通信を行っていること	良
A-5		番組管理サーバからのリンク時にユーザ情報を受け取ることができること	良
A-6		IPsec クライアントを搭載し IPsec 管理システムと連携した IPsec 通信が問題なく動作すること	良
A-7		一度に複数ユーザからのアクセスを許可すること	良
A-8		ユーザからアップロードされた MPEG2 ファイルを受信しエンコーダへ送信する機能を持つこと	良
A-9		情報管理 DB サーバに必要な情報を参照･登録・変更・削除することができること	良
A-10		ユーザによりファイルダウンロード型映像配信を指定されたコンテンツを保存し、コンテンツ毎に利用を許可されたユーザから配信要求があった場合に IPv6 クライアントに対して映像ファイルを送信できること	良
A-11		指定された Web サーバ上で問題なく動作すること	良
B-1	アップロードクライアント	Windows2000 もしくは XP 上で動作するアプリケーションであること	良
B-2		ユーザログイン時に情報管理 DB のユーザ情報を基にした認証を行うことができること	良
B-3		GUI インタフェースは十分にわかりやすくなっていること	良
B-4		ユーザが登録する MPEG2 ファイルを DVD/CD 等のメディアから読み出しエンコーダへ送信することが可能であること	良

B-5		DV 端子経由で接続された DV デッキを制御しユーザが登録する映像情報を DV テープ等のメディアから直接エンコーダへ送信する事が可能であること	良
B-6		情報管理 DB サーバに必要な情報を参照･登録・変更・削除することができること	良
B-7		指定されたアップロードクライアントで問題なく動作すること	良
C-1	エンコーダ	Web サーバ及び、アップロードクライアントから送信された映像ファイルを受信できること	良
C-2		登録時にユーザが入力した映像情報及び、システム管理情報を映像管理 DB サーバへ登録できること	良
C-3		受信した映像ファイルを Windows Media Encoder を制御する事により WMT 形式のファイルへ変換できること	良
C-4		映像変換処理が終了後に WMT 形式のファイルを映像配信サーバの指定されたディレクトリへ転送し、コンテンツ情報及び、映像変換処理結果を情報管理 DB へ登録できること	良
C-5		複数の変換要求があった場合でもキューイングによりスムーズな変換処理が可能であること	良
C-6		エンコード時にコマ落ち等が発生しないこと	良
C-7		品質などのエンコードパラメータを設定ファイル等により簡易に変更できること	良
D-1	映像配信サーバ	Microsoft Windows Media Service もしくは同等品を用いて WMT 形式のストリーミング動画配信が可能であること	良
D-2		ストリーミング動画配信を IPsec サーバからの要求により開始し IPv4 プロトコルによって IPsec サーバへ配信すること	良
D-3		複数の配信要求があった場合でも正常に動作し問題なく配信できること	良
E-1	情報管理データベース	コンテンツ情報を保存するためのテーブルを備えていること	良

F-1	結合試験	番組管理サーバで認証されたユーザ ID を番組管理サーバから受け取り情報管理 DB のユーザ情報によりアクセス制限を行っていること	良
F-2		番組管理サーバが認証を行った IPv6 クライアントとのみ IPsec を使用した通信を行うこと	良
F-3		IPv6 クライアントから Web ブラウザによるコンテンツの登録操作が可能であること	良
F-4		上記操作においてユーザが所属するユーザグループへのコンテンツ登録が可能であること	良
F-5		上記操作においてユーザが所属しないユーザグループへのコンテンツ登録が拒否されること	良
F-6		IPv6 クライアントから Web ブラウザによるコンテンツ付加情報変更操作が可能であること	良
F-7		上記操作においてユーザが登録したコンテンツへの操作が可能であること	良
F-8		上記操作においてユーザが登録していないコンテンツへの操作が拒否されること	良
F-9		IPv6 クライアントから Web ブラウザによるコンテンツの削除操作が可能であること	良
F-10		上記操作においてユーザが登録したコンテンツの削除操作が可能であること	良
F-11		上記操作においてユーザが登録していないコンテンツの削除操作が拒否されること	良
F-12		IPsec システムと連携して IPv6 クライアントへのストリーミング型コンテンツの配信が可能であること	良
F-13		上記操作においてユーザが所属するユーザグループのコンテンツを受信可能であること	良
F-14		上記操作においてユーザが所属しないユーザグループのコンテンツの受信を拒否されること	良
F-15		IPv6 クライアントへ Web ブラウザによるファイルダウンロード型コンテンツの配信が可能であること	良
F-16		上記操作においてユーザが所属するユーザグループのコンテンツを受信可能であること	良
F-17		上記操作においてユーザが所属しないユーザグループのコンテ	良

		ンツの受信を拒否されること	
F-18		アップロードクライアントのアップロードアプリケーションからのコンテンツの登録操作が可能であること	良
F-19		上記操作においてユーザが所属するユーザグループへのコンテンツ登録が可能であること	良
F-20		上記操作においてユーザが所属しないユーザグループへのコンテンツ登録が拒否されること	良
F-21		アップロードクライアントのアップロードアプリケーションからのコンテンツ付加情報変更操作が可能であること	良
F-22		上記操作においてユーザが登録したコンテンツへの操作が可能であること	良
F-23		上記操作においてユーザが登録していないコンテンツへの操作が拒否されること	良
F-24		アップロードクライアントのアップロードアプリケーションからのコンテンツの削除操作が可能であること	良
F-25		上記操作においてユーザが登録したコンテンツの削除操作が可能であること	良
F-26		上記操作においてユーザが登録していないコンテンツの削除操作が拒否されること	良