4　映像対話型電子申請・交付システムの調査、検証

映像対話型電子申請・交付システムに必要とされるセキュリティ機能、個人認証、印刷文書の真正証明機能の検証を行うとともに、電子申請交付システムを利用したときの効率、利便性についての利用調査を行った。

映像対話型電子申請・交付システムの概要を以下に示す。

4.1 映像対話型電子申請・交付システムの概要

電子申請・交付システムにおける交付書類については、福祉系申請、納税系申請ともに基本的には即時発行できるものを、申請時に申請者側のプリンタに印刷し、映像を通して印刷結果確認を行うこととした。

また、納税系の申請については、運用面を考慮し、明細が必要なもの、記載内容の補筆及び税額の修正が必要なものについては対象から除外した。

システム化の対象とする申請を表 4-1に示す。

表 4-1 システム化の対象とする申請

申請	受付	申請者	システム交付書類
身体障害者手帳再交付申請	各福祉事務所	本人	無し
補装具の交付・修理申請	各福祉事務所	本人	判定通知書
障害証明交付申請	各福祉事務所	本人	障害証明書
老人医療受給者証再交付申請	各福祉事務所	本人	無し
市県民税(所得・課税)証明交付申請	本庁市民税課	本人	市県民税(所得・課税)証明書
	本庁市民税課	本人	市県民税(所得・課税・控除)証明書
	本庁市民税課	本人	所得証明書(児童手当用)
固定資産{評価・公課}証明交付申請	本庁市民税課	本人	固定資産評価証明書
	本庁市民税課	本人	固定資産公課証明書
	本庁市民税課	本人	固定資産(償却資産)評価証明書
納税証明交付申請　※２	本庁市民税課	本人	納税証明書(法人以外)
	本庁市民税課	本人、代理人	軽自動車税納税証明書(継続検査用)

※１　身体障害者更生相談所以外の医療機関等で判定を受ける場合の必要様式も申請者端末に取得、印刷することが可能。
※２　法人からの申請は軽自動車納税証明（継続検査用）のみとする。
※３　手数料が必要な書類については、領収書も同時に発行する。

申請を行うにあたってユーザ ID、パスワードによる個人認証、SSL によるサー

バ認証とセッションの暗号化、申請内容の正当性を証明するための送信データに対するデジタル署名等のセキュリティ対策を行う。図 4-1、図 4-2にそれぞれ電子申請の処理フロー、電子交付の処理フローを示す。

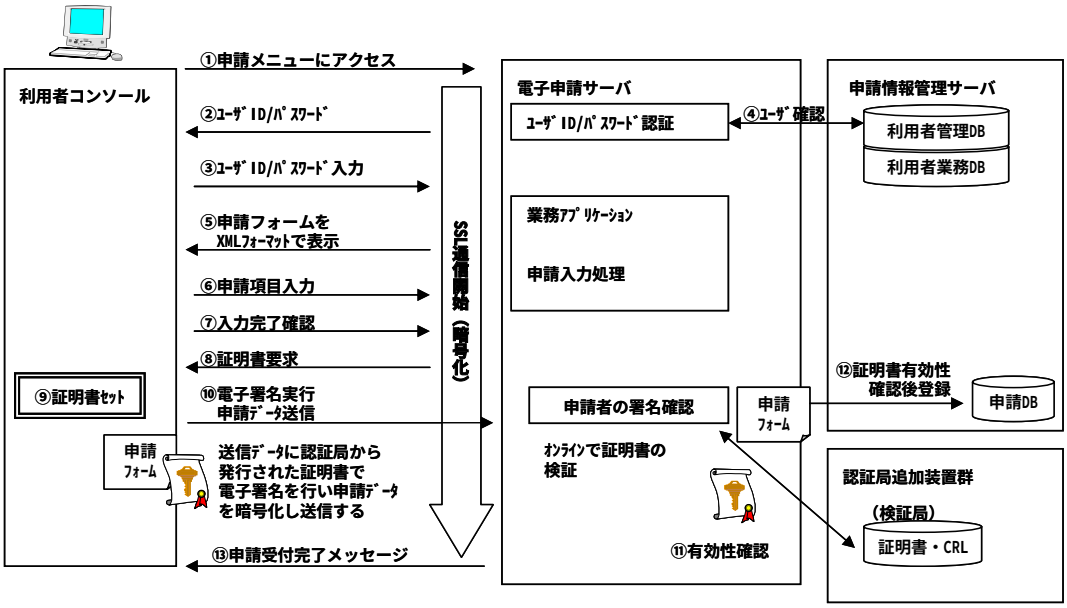


図 4-1 電子申請の処理フロー

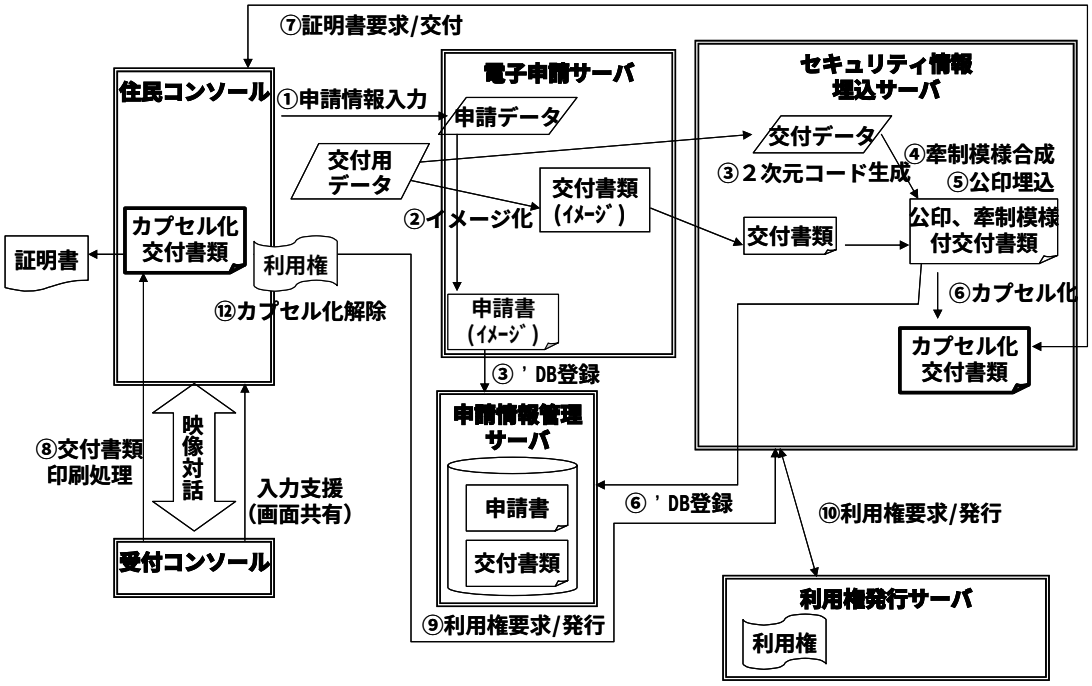


図 4-2 電子交付の処理フロー

電子交付についてはダウンロードしたファイルに利用権を設定し、申請者の端末以外からファイルを印刷できないような対策を施した。また、印刷した交付文書の真正を保証ための技術を適用した。

実際の申請・交付業務との差異を少なくするため及び業務の合理化のために以下のようにした。

(1) 窓口職員による交付書類の印刷

実際の窓口での交付は窓口職員から手渡しで行われる。そのため、交付文書の印刷開始は職員側が遠隔で実施することとした。尚、交付文書の到達時期は印刷完了時とした。

(2) 写真の撮影

身体障害者手帳の再交付申請は申請時に手帳に貼り付けるための証明写真が必要になる。これを映像対話の画面を職員側で印刷することで証明写真に代用することとした。このことにより、写真を提出する必要がなくなり電子申請がより合理化される。

尚、写真の作成については窓口側画面（相手の映像全画面表示）をデジタルカメラで撮影し取り込むこととした。

(3) 手数料の納付

手数料の納付については、インターネットバンキングシステムを利用して行うこととした。インターネットバンキングに市役所の口座を設け、その口座への振り込み確認後交付処理を開始することとした。手数料支払フローを図 4-3に示す。この方法の場合、口座への入金を行うと即座に反映される。

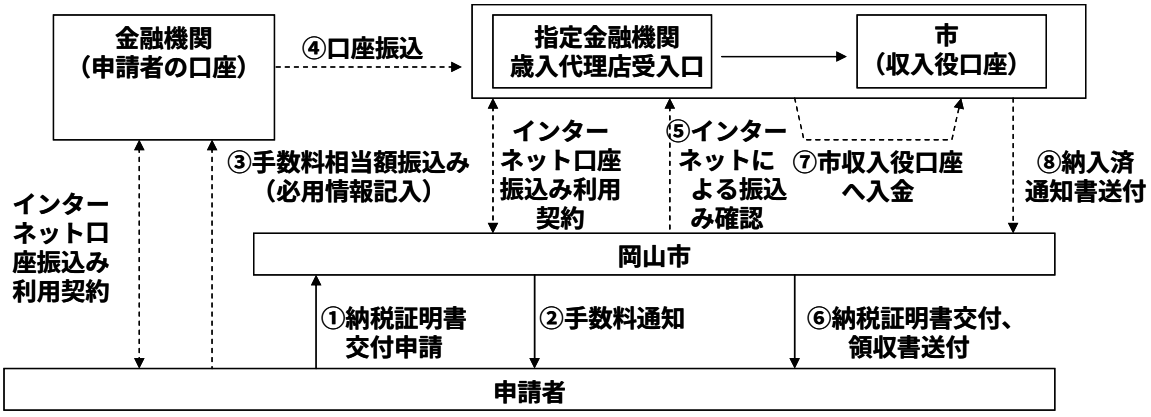


図 4-3 手数料支払フロー

①申請者は、自端末からネットワークを通じて市役所に対し申請を行う。
②受付者は申請を受付し、申請にかかった手数料を映像対話で申請者に通知する。
③申請者はインターネットバンキングにより必用情報を入力し手数料を振り込む。
④申請者から振り込まれた料金が指定された口座に入金される。
⑤申請者から手数料が実際に振り込まれたかどうかインターネットバンキングの明細確認等で確認する。
⑥受付者は申請者に対し書類の交付を行う。
⑦受け入れ窓口口座から払戻し市収入役口座へ入金する。
⑧金融機関より納入済通知書を受領する。
注）インターネットバンキングの場合当日扱いの処理については「8:00 から 15:00 の受付に限る」等の時間制限がある。

(4) 原本の管理

交付した文書の真正証明実験で比較を行うため、交付済書類のイメージデータも保存しておくこととした。

(5) 文書の様式

申請書及び交付文書については現行の様式と同様なものとした。

4.2 IPsec 技術によるセキュリティ耐性の調査、検証

インターネットを利用した電子申請や行政相談ではインターネット上で個人情報がやりとりされるためプライバシーの保護が非常に重要になる。IP レイヤでセキュリティ機能を実現する IPsec では IP を利用したアプリケーションであれば TCP、UDP にかかわれず包括的に改竄、盗聴、成りすましの防止ができるため、映像対話や遠隔制御などのインターネットを利用した複合的な行政サービスのセキュリティ保護のために有効であると考えられる。ここでは映像対話型電子申請・交付システムにおける IPsec 技術の適用についての有効性評価を行う。

4.2.1 IPsec の概要

インターネットでは様々なセキュリティプロトコルが利用される。表 4-2に暗号化と認証機能を持つプロトコルを示す。

表 4-2 暗号化と認証機能を持つプロトコル

OSI 参照モデル	セキュリティプロトコル
アプリケーション層	S/MIME、PGP、SSH etc.
セッション層	SSL、TLS、SOCKSv5
ネットワーク層	IPsec
データリンク層	PPTP、L2F、L2TP

IPsec はインターネットのような公開ネットワーク上でプライベートな通信を安全に行えるように開発されたプロトコルである。他のセキュリティプロトコルと IPsec の最も大きな違いは実装レイヤがネットワーク層ということである。インターネットを利用する場合の最も低いレイヤでの実装であり、パケット単位での暗号化や認証が可能である。IPsec は、現在の IPv4 ではオプションとして利用できたが、IPv6 では標準の機能とされている。IPsec の概要について述べる。

ネットワークでのセキュリティへの脅威には、大きく以下の 3 種類が存在する。

(1) 盗聴

インターネット上の情報を不正に取得することによって、第三者への機密情報が流出したり、あるいは、悪意を持った人間に公開サーバに不正侵入され情報の内容を盗み見られてしまったりする可能性がある。

(2) 改竄

重要な情報をインターネットでやり取りする場合、その内容を悪意のある第三者によって書き変えられてしまう恐れがある。

(3) 成りすまし

悪意を持った第三者が正当な人物に成りすまして、意図しない情報をやり取りされてしまう恐れがある。

IPsec では、これらの脅威への対策としてそれぞれ次のセキュリティ技術が適用される。

(1) 盗聴に対する対策

ネットワークに流れる情報を暗号化することによって機密性を確保する。送信時の暗号化と受信時の復号化には、送信側と受信側のみが知っている暗号化鍵（＝復号化鍵）が使用される。この鍵は定期的に安全な方法（鍵交換アルゴリズム）で変更される。仮にある時点で暗号が破られたとしても、他の鍵で暗号化された情報の内容まで解読されることはないため、情報全体としては安全性が高いといえる。この暗号化には、主に DES やトリプル DES、IDEA、RC5 などの共通鍵暗号方式が使われる。

この機能は、IPsec では暗号ペイロードで実現される。

(2) 改竄に対する対策

ネットワークに流れる情報に送信側と受信側のみが知っている秘密の認証鍵を加えて一方向性関数（ハッシュ関数）などで認証データを計算し、その認証データをもとの情報に付与して送る。受信側は、同じように受け取った情報の認証データを計算し、それを送信側が付与した認証データと比較することによって、メッセージが改竄されていないかどうかを確認することができる（これをメッセージ認証という）。この認証データを計算するための関数として、MD5 や SHA1 などの一方向性関数（ハッシュ関数）が使用される。この認証鍵も、前述の「盗聴に対する対策」で説明した暗号化鍵の場合と同じ鍵交換アルゴリズムによって定期的に変更される。

この機能は、IPsec では「認証ヘッダ（Authentication Header : AH）（RFC1826）」で実現される。

(3) 成りすましに対する対策

送信側と受信側の暗号化鍵（復号化鍵）又は認証鍵が一致しないとデータの復号化やメッセージ認証に失敗するため、送られてきた情報を受け取らないような仕組みにしている。このため、これらの鍵を所持しない第三者が正当な人物になりすますことはできない。しかし、これらの鍵は定期的に自動で交換される。その際に、交換する相手が正当な相手かどうかの確認が必要

となる。多くの場合、RSA の公開鍵と秘密鍵のペアを利用するなどして、本当に鍵を交換すべき相手なのかどうかを事前に確認し合う仕組みを設けることで第三者がこれらの鍵を入手することはできないようにしている。

この機能が、鍵管理アルゴリズムによって実現される。IPsec では、IKE（Internet Key Exchange）などのプロトコルが利用される。

4.2.2 IPsec の構成

IPsec の構成要素を表 4-3に示す。

表 4-3 IPsec の構成要素

IPsec の構成要素	利用されるアルゴリズム等
AH	Keyed-MD5、HMAC-MD5、HMAC
ESP	DES-CBC
鍵交換	DOI、IKE、SKIP

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

4.2.3 セキュリティポリシー（SP）

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

①パケットを破棄する
②IPsec を適用せずに通常の処理を行う
③IPsec を適用する

これらは、通信パケット内の送信元 IP アドレス、宛先 IP アドレス、プロトコル、宛先ポート番号によって判断される。このような、通信パケットを選択する項目を総称してセレクタと呼ぶ。セレクタの考え方は、ルータにおけるアクセ

スリストに近い。

このセレクタと実際に適用する処理の内容を含んだものをセキュリティポリシー（SP）と呼ぶ。SP 内では IPsec を適用する場合の IPsec プロトコル(AH、ESP、IPComp)やモード(トランスポート、トンネル)等も指定する。

4.2.4 セキュリティ・アソシエーション(SA)と SPI

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

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

SA には、使用する暗号化アルゴリズムの種類、暗号化アルゴリズムのモード、暗号化アルゴリズムで使用する初期ベクトル（IV）の長さ、認証アルゴリズムの種類、認証アルゴリズムのモード、暗号化鍵、認証鍵などの情報が保持される。この SA はそれぞれの機器で保持され、IPsec パケットを送り出す場合には、相手側の保持する SA の中から利用できるものを送信側が選択し、その SA に付けられているセキュリティ・パラメータ・インデックス（SPI）の値をそのパケットの認証ヘッダや暗号ペイロードのフィールドに含めて送る。受信側は、認証ヘッダや暗号ペイロードのヘッダ中の SPI 値によってどの SA が使用されているのかを識別する。この SPI の値は受信側が付与する（0～255 は予約されているので、その他の値が使用される）。

この SA は単方向であり、端末 A と端末 B が通信する場合、端末 A から端末 B へのパケットと、端末 B から端末 A へのパケットには異なる SA が使用される。よって、行きのパケットは DES で暗号化し、帰りのパケットはトリプル DES で暗号化するといったような、その方向によって使用するアルゴリズムを変えることができる。

また、認証ヘッダと暗号ペイロードはそれぞれに SPI フィールドを持っており、それぞれ独立して別の SA を選択することができる。

4.2.5 トンネルモードとトランスポートモード

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

(1) トンネルモード

トンネルモードと呼ばれるモードでは、IP パケット全体を暗号化し、それ

を新しいIPパケットにカプセル化（包み込む）する。こうすることで、データだけではなく、IP ヘッダも暗号化されるので、送信元アドレスや宛先アドレス、使用しているプロトコル（アプリケーション）などの情報を隠すことができる。

このモードの長所と短所は以下の通りである。

（i） 長所

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

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

（ii） 短所

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

(2) トランスポートモード

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

（i） 長所

トンネルモードのようにパケットのサイズが大きくならずに済む。

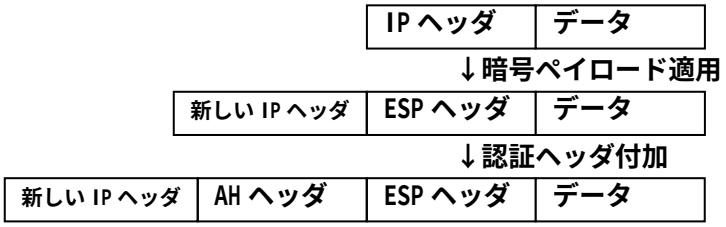
（ii） 短所

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

IPヘッダは暗号化されない。

図 4-4にIPパケットにIPsecが適応される場合の変化を示す。 以下の図は、暗号ペイロード（ESP）の処理と認証ヘッダ（AH）の処理の両方がされているが、どちらかが単独で使用されても構わない。

①トンネルモード



②トランスポートモード

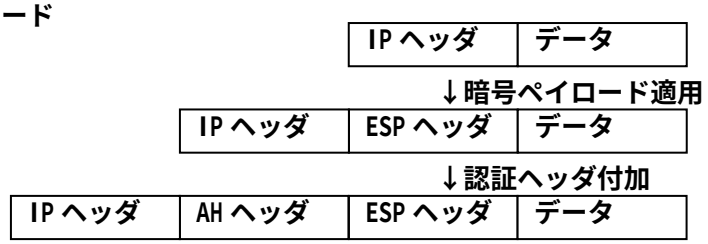


図 4-4 IP パケットに IPsec が適応される場合の変化

4.2.6 認証ヘッダ

認証ヘッダ（AH: Authentication Header RFC1826）は、IP パケット全体のインテグリティを保証するための仕組みである。認証ヘッダでは、MD5 や SHA-1 のような一方向性ハッシュ関数をパケット全体に対して適用し、その結果を認証データとしてそのパケットと一緒に送る。この時、送信側と受信側しか知らない秘密の認証鍵を認証計算に含めることで、第三者がパケットの内容を改竄した後で認証データを再び計算し直すことができないようにしている。

ここで重要なのは、認証ヘッダは IP のデータのみではなく、IP ヘッダを含んだパケット全体に対して認証データを計算するということである。こうすることで、例えば、IP ヘッダの送信元アドレスなどの情報も配送中に改竄されることはなくなる。すなわち、そのパケットの送信元アドレスのホストが確かに送り出したパケットであることが保証されることになり、身元証明を必要とするアプリケーションに利用することができる。

しかし、IP ヘッダの内容には、IPv4 ヘッダの TTL やヘッダチェックサム、そして IPv6 ヘッダの中継限界数フィールドのように、配送中に内容が変更されるフィールドを含んでいる。これらのフィールドを認証計算に含めると、受信側での認証の確認の際には内容が変更されているため、認証に失敗することになる。このため、これらのフィールドは、認証の計算の際に値が "0" であるとして計算される。

特に、データ部分のインテグリティは、データ部を暗号化する暗号ペイロー

ドによってある程度保証されており（特に現在議論中の改訂版の仕様では、暗号ペイロードの機能として、ハッシュ関数を利用したデータ部のインテグリティチェックの機能が含まれる予定)、認証ヘッダは、IP ヘッダの情報を改竄から守るものとして利用される。

認証ヘッダで使用されるアルゴリズムは、認証ヘッダ自体の仕様では決められていないが、必須のアルゴリズムとして、Keyed-MD5（RFC1828）と HMAC-MD5（RFC2085）を実装することとなっている。その他のアルゴリズムとしては、Keyed-SHA1（RFC1852）などがある。

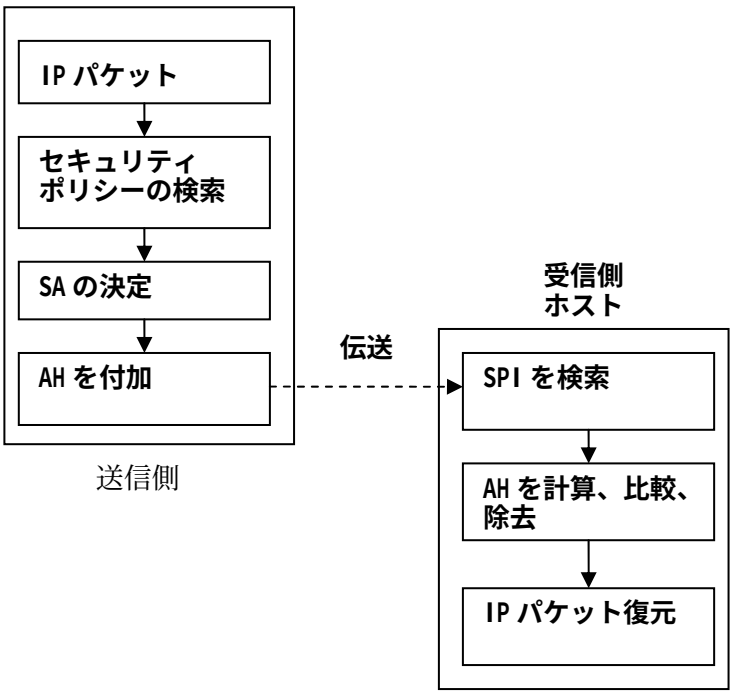


図 4-5 ESP の処理フロー

(1) 送信側での処理の流れ

①通信相手のアドレスや通信プロトコル等を SP に照らし合わせる。

②AH で使用するセキュリティ・アソシエーションを決定する。

③セキュリティ・アソシエーションで指定する認証アルゴリズム、認証鍵を使用してパケット全体に渡って認証データを計算する。この時、配送中に中間のルータなどによって変更される可能性のあるフィールドは、すべて "0" で満たされているとして計算する。このフィールドは、IPv4 の場合は、「TTL」、「ヘッダチェックサ

ム」(「TOS」、「フラグ」、「断片オフセット」も "0" にされることも多い)、IPv6 の場合は、「中継限界数」フィールドである。この時は認証ヘッダが挿入された状態のパケットに対して認証データが計算されるが、その「認証データ」フィールドも、"0" で満たされているとみなされる。

④認証ヘッダの次ヘッダ・フィールド、長さフィールド、SPI フィールドに適切な値を入れ、先ほど計算された認証データを認証データ・フィールドに挿入し、パケットを組み立てる。この時、IP ヘッダの全パケット長・フィールドが適切な値に調整される。

⑤組み立てたパケットがネットワーク上に送られる。

(2) 受信側での処理の流れ

①受信されたパケットのプロトコル・フィールド（IPv4 の場合)、次ヘッダ・フィールド（IPv6 の場合）に IP プロトコル番号 51 が含まれているので､認証ヘッダが使用されていることが判断される。

②認証ヘッダの SPI フィールドの値から、使用されているセキュリティ・アソシエーションを検索する。

③そのセキュリティ・アソシエーションから、使用されている認証アルゴリズム、認証鍵を判断し、パケット全体に渡って認証データを計算する。この時、IPv4 ヘッダの「TTL」や「ヘッダチェックサム」、IPv6 ヘッダの「中継限界数」フィールド、そして認証ヘッダの「認証データ」フィールドは送信側と時と同様に "0" であるとみなされる。

④ここで計算された認証データと、認証データ・フィールドに入っていた値とを比較し、同一のものであれば認証処理が成功したことになる。

⑤認証処理が成功すれば、認証ヘッダが外されて、もとの状態でネットワーク上に送られる。この時、IP ヘッダの全パケット長フィールドが適切な値に調整される。

4.2.7 暗号ペイロード

暗号ペイロード（ESP: Encapsulating Security Payload、RFC1827）は IP パケットを暗号化することによって､IP パケットの機密性を保証する仕組みである。

暗号ペイロードはトンネルモードとトランスポートモードの２つのモードを実現する仕組みを持っている。しかし、その暗号化のアルゴリズムについては、暗号ペイロードの仕様では決められていない。これは、将来新しい安全なアルゴ

リズムを使用したい場合に、この暗号ペイロードの仕様を変更することなく使用できるようにするためである。 暗号ペイロードには、IP プロトコル番号として 50 番が割り当てられている。この暗号ペイロードは、通常、IP ヘッダや認証ヘッダなどの後に挿入されるので、例えば認証ヘッダと一緒に使用されれば、IP ヘッダのプロトコル・フィールドには 51 番が含まれ、他のヘッダが利用されなければ、50 番が含まれることになる。

ESP の処理は以下のようなフローで動作する。

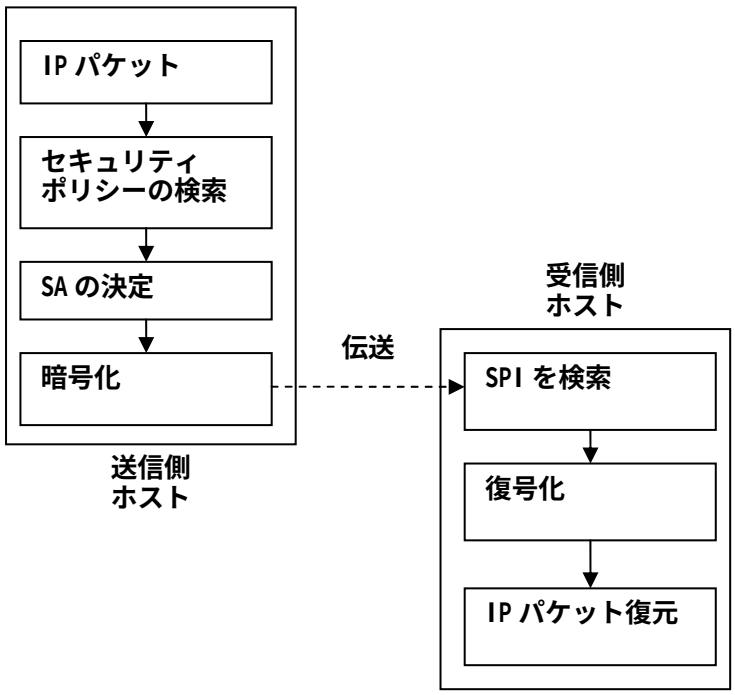


図 4-6 ESP の処理フロー

(1) 送信側での処理の流れ

①通信相手のアドレスや通信プロトコル等を SP に照らし合わせる。

②ESP で使用するセキュリティ・アソシエーションを決定する。

③トンネルモードの場合は、IP パケット全体をセキュリティ・アソシエーションで指定する。

④初期ベクトルの長さ、暗号化アルゴリズム、暗号化鍵を使用して暗号化する。トランスポートモードの場合は、IP パケット中のデータ部のみ（TCP、UDP、ICMP）をセキュリティ・アソシエーションで指定する初期ベクトルの長さ、暗号化アルゴリズム、暗号化鍵を使用して暗号化する。この時、暗号化される前のデータの最後

には、パディング、パディング長・フィールド、次ヘッダ・フィールドが付加される。この暗号ペイロードの次ヘッダ・フィールドには、トンネルモードであれば、IP-in-IP で指定されている IP プロトコル番号の 4 番、トランスポートモードであれば、暗号化したトランスポート層プロトコルの IP プロトコル番号が含まれる（TCP であれば 6 番、UDP であれば 17 番となる）。

⑤使用したセキュリティ・アソシエーションを示す SPI 値と、もし使用されていれば暗号化アルゴリズムの初期ベクトル、そして先ほど暗号化されたペイロードデータを使って暗号ペイロードを組み立てる。

⑥トンネルモードであれば、送信元アドレスが暗号ペイロードの処理を施した機器のアドレス、宛先アドレスが相手側の（復号化する）機器のアドレスを含んだ IP ヘッダが付加される。トランスポートモードであれば、もともとの IP ヘッダが付与される。この時、その IP ヘッダのプロトコル・フィールド（IPv4）、次ヘッダ・フィールド（IPv6）には、暗号ペイロードの IP プロトコル番号である 50 番が含まれる。また、この時、全パケット長フィールドの値も調整される。

⑦組み立てられたパケットがネットワーク上に送られる。

(2) 受信側での処理の流れ

①受信されたパケットのプロトコル・フィールド（IPv4）、次ヘッダ・フィールド（IPv6）に 50 番が含まれているので、暗号ペイロードが使用されていることが判断される。

②暗号ペイロードの SPI フィールドの値から使用されているセキュリティ・アソシエーションを検索する。

③そのセキュリティ・アソシエーションから、初期ベクトルの長さや使用されている暗号化アルゴリズムの種類、復号化鍵を判断し、それらを利用して復号化処理をする。

④復号化された暗号ペイロードの次ヘッダ・フィールドの値から、トンネルモードとトランスポートモードのどちらが使用されているのかが判断される。

⑤復号化されたパディング長・フィールドで指定された長さのパディングが取り除かれる。 トンネルモードの場合は、復号化されたパケットがそのままネットワーク上に送り出される。トランスポートモードの場合は復号化されたデータにもとの IP ヘッダが付与

され、ネットワーク上に送り出される。この時、IP ヘッダのプロトコル・フィールド（IPv4)、次ヘッダ・フィールド（IPv6）と、全パケット長・フィールドの内容が適切な値に調整される。

映像対話に IPsec を適用する場合、IPsec 映像対話コンソール相互間ではなく、映像対話コンソールと経路制御装置間で終端される。このため、経路制御装置で一旦 ESP は復号化されることに注意が必要である。

4.2.8 鍵管理

IPsec の仕組みである認証ヘッダと暗号ペイロードは、IP パケットに強力なセキュリティを提供する。しかし、このセキュリティは、使用する暗号化鍵や認証鍵が第三者に知られないことが前提とされている。つまり、これらの鍵が知られてしまえば IPsec の仕組みはセキュリティのないものとなってしまう。

暗号の解読の基本的な方法に鍵の総当たりが使用ある。鍵の長さはなるべく長いものを利用して、鍵の総当たりにかかる時間をなるべく長くするべきであるが、結局時間を費やせば解かれてしまうし、暗号技術の輸出規制などにより、十分に長い鍵長のものを利用できないという現実がある。

そこで、その暗号化鍵や認証鍵を定期的に短い間隔で変更することが必要となる。

(1) 手動鍵管理

鍵の一番簡単な交換方法は、手動鍵管理（マニュアル鍵管理）である。この手動鍵管理は、IPsec の仕様では必須とされている。

手動鍵管理では、文字通り、管理者が送信側と受信側の各システムで鍵を手動で設定する。しかし、定期的に鍵を手動で変更するのはとても現実的な方法ではない。そこで、後述する自動で鍵を交換する仕組みが求められる。

(2) 既存の鍵交換方式

自動で鍵交換を行う仕組みには、大きく分けて二つの方式が存在する。

一つは、RSA などの公開鍵暗号方式を利用する方式がある。これは、データ自体は高速な DES などの共通鍵暗号方式で暗号化するが、そこで使われる秘密の暗号化鍵を、RSA などの公開鍵暗号方式で暗号化して相手側に送るというものである。

もう一つは、Diffie-Hellman 法である。この方式では、鍵を交換する[A]と[B]には、あらかじめ素数[p]と原始根[g]を知らせておく。この[p]と[g]は第三者に知られても構わない。そして、[A]と[B]はそれぞれ秘密の乱数値[x]と[y]を生成する。そしてその秘密の値と、先程の[p]と[g]からある計算式に

よって、それぞれ[n]と[m]という値を生成する。この[n]と[m]をお互いに交換し（この値は第三者に知られても構わない)、交換された値と自分の持っている秘密の値、そして素数[p]からある計算式によって、[A]と[B]の両者は全く同じ[K]という値を得ることができる。この値[K]を[A]と[B]で共有する秘密鍵として使用する。

(3) 鍵管理プロトコル

鍵交換の基本的な方式としては、上記のような方式が使用されるが、RSA や Diffie-Hellman 法では、鍵交換の仕組みをプロトコルレベルで規定しているわけではないので、各社独自に実装することになる。それでは相互接続性を保つことができない。これをプロトコルレベルで規定したものが、IKE（Internet Key Exchange）や SKIP（Simple Key-management for Internet Protocol）である。これらの鍵管理プロトコルは、基本的には Diffie-Hellman 法を使用するものだが、鍵の交換だけではなく、暗号化アルゴリズムの種類などのセキュリティ・アソシエーションのパラメータを取り決める機能も持っている。

IPsec では、必須の鍵管理プロトコルとして IKE を指定している。IKE は以前 ISAKMP（Internet Security Association and Key Management Protocol）/Oakley と呼ばれていた鍵管理プロトコルである。このプロトコルは、UDP のポート 500 番を使用し､実際のデータパケットとは別のパケットを使用する。

また、その他の鍵管理プロトコルとしては、SKIP が存在する。こちらも RFC としては出されていないが、IPsec ではオプションとして使用することが決定されている。しかし、比較的早くから実装が進められているため、SKIP を採用している VPN 機器間では、既にある程度の相互接続ができているもようである。こちらは IP のオプションヘッダとして規定されており、実際のデータパケットのヘッダという形で挿入される。すなわち、別のパケットが発生することはないが、パケット自体のサイズは大きくなる。SKIP には、IP プロトコル番号として 57 番が割り当てられている。

ISAKMP/Oakley に SKEME と呼ばれる鍵交換方式を取り込んだものが、最終的に IPsec の鍵交換プロトコルの標準として定まった。 IKE の通信そのものは、UDP で扱われる。ポート番号は 500 である。 デーモンとして実装できるので、定期的に鍵を変更することなどが簡単になる。

IKE の通信には IPsec は使わない。

IKE での SA の確立は次の通りとなる。

<phase 1> IKE 自身が安全に情報の交換を行うための SA を確立する。鍵交

換にはDiffie-Hellmanが使用される。

<phase 2>phaseで確立したSAを使って、IPsecの通信で使用される認証や暗号化のパラメータが交換される。

鍵管理プロトコルによってSAのパラメータが動的に交換される場合は、それに先立ってお互いの正当性の認証を行う必要がある。

IKEではこの認証の方式として、以下の３つの方式が定められている。

(i)　既知共有鍵（pre-shared key)
(ii)　電子署名(Digital Signature)
(iii)公開鍵暗号(Public Key Encryption)

これらの鍵管理プロトコルにより、IPsecの通信に用いられる暗号鍵のパラメータが毎回、あるいは一定の通信ごとに変更される。

より強力な認証が必要な場合は、例えばX.509の規格にそった電子証明書による認証をIKEのもとで利用することが可能である。X.509による認証は、公開鍵インフラストラクチャ(PKI)のもとでの利用が可能になれば、インターネットでの通信に簡単で確実な手段を提供するようになる可能性がある。

4.2.9　システム構成

IPv6セキュアサーバにてSP、SAの集中管理を行い、IPsecの評価、検証を行うためのシステムを開発した。システム構成図を図 4-7に示す。

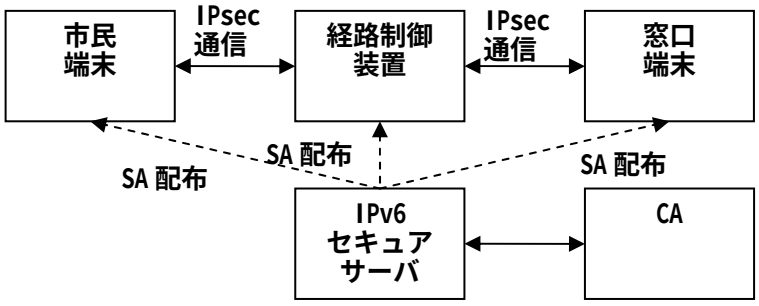


図 4-7　システム構成図

IPv6セキュアサーバ機能一覧を

表 4-4に示す。

表 4-4 IPv6 セキュアサーバ機能一覧

項番	機能名	内容
1	セキュリティポリシー管理機能	IPsec 用セキュリティポリシー（SA；セキュリティアソシエーションを含む）の作成、維持管理機能。
2	セキュリティポリシー配布機能	IPsec 用セキュリティポリシー（SA；セキュリティアソシエーションを含む）を経路制御装置等に配布する機能。
3	セキュリティポリシー状態管理機能	IPsec 用セキュリティポリシー（SA；セキュリティアソシエーションを含む）をどのサイトに配布して実行中であるか等の状態管理を行う機能。
4	セキュリティドメインメンバ登録・管理機能	住民端末、受付端末、経路制御装置等をセキュリティドメインメンバーとして登録・管理・削除ができる機能。
5	セキュリティドメインメンバ認証機能	PKI と連携し、セキュリティドメインメンバーの認証ができる機能。

以下に個々の機能について述べる

(1) セキュリティポリシー管理機能

セキュリティポリシー及びセキュリティアソシエーションについて、作成、修正、削除、一覧表示、詳細表示する機能である。

(i) セキュリティポリシー

セキュリティポリシーを表 4-5に示す。

表 4-5 セキュリティ・ポリシー

送信元アドレス〔ポート番号〕		
宛先アドレス〔ポート番号〕		
上位層プロトコル	tcp / udp / icmpv6 / any	
ポリシー	方向	in / out
	方針	discard / none / ipsec
IPsec の場合	セキュリティプロトコル	ah / esp
	モード	transport / tunnel
	トンネルモードの場合	トンネルエンドポイント
	レベル	default / use / require / unique

(ii) 4.1.2 セキュリティアソシエーション

セキュリティアソシエーションを

表 4-6に示す。

表 4-6 セキュリティ・アソシエーション

送信元アドレス	
宛先アドレス	
セキュリティプロトコル	ah / esp
SPI (security parameter index)	
モード	transport / tunnel / any
リプレイ攻撃防止用ウインドウサイズ	
シーケンス番号サイクリック使用の可否	
パディングの指定	zero-pad / random-pad / seq-pad
unique 指定時の ID	
ハード有効期限	
ソフト有効期限	
認証アルゴリズム	hmac-sha1 / hmac-md5
暗号アルゴリズム	3des-cbc / des-cbc / aes
暗号鍵	
認証鍵	

(iii) その他管理機能

上記のセキュリティポリシー及び SA を Web 画面によって作成、修正、削除、一覧、詳細な内容を表示できる機能。

(2) セキュリティポリシー配布機能

セキュリティポリシー及び SA をセキュリティドメインメンバの各サイトに配布する機能である。 配布のプロトコルは SPP に準拠する。

(3) セキュリティポリシー状態管理機能

セキュリティポリシー及び SA をどのサイトに配布して実行中であるか等を管理する機能である。

以下の４とおりの表示が可能である。

(i) セキュリティポリシー又は SA を指定して、その配布先を表示する

(ii) IP アドレスを指定して、配布されているセキュリティポリシー及び SA を表示する

(iii) すべてのセキュリティポリシー又は SA と、配布先との対応一覧を表示する

(iv) すべての IP アドレスと、セキュリティポリシー及び SA との対応一

覧を表示する

(4) セキュリティドメインメンバ登録・管理機能

住民端末、受付端末、経路制御装置等をセキュリティドメインメンバとして登録、削除、一覧表示する機能である。

(i)　登録機能

住民端末、受付端末、経路制御装置等をセキュリティドメインメンバとして登録する機能である。このとき、当該メンバの証明書も登録する。

(ii) 削除機能

特定のＩＰアドレスをセキュリティドメインメンバから削除する機能である。

(iii) 一覧表示機能

セキュリティドメインメンバの一覧を表示する機能である。

(5) セキュリティドメインメンバ認証機能

PKI と連携してセキュリティドメインメンバの認証ができる機能。セキュリティドメインメンバに対してＣＡが発行した証明書を格納し、要求に応じてメンバに配布する機能である。処理シーケンスを以下に示す。

①メンバが他のメンバに対する証明書を要求する。

②メンバ登録の有無をチェックする。ＮＧの場合、ＮＧ応答を返す。

③証明書の有効性をチェックする。この場合、ＣＡと連携して、ＣＲＬをチェックする。ＮＧの場合、ＮＧ応答を返す。

④名所を付けてＯＫ応答を返す。

4.2.10 検証内容

担当窓口と IPv6 セキュアサーバが IPsec 通信を行うことにより、実験を行った。

ESP を適応したトランスポート、トンネルモードの両方で評価、検証を実施することとした。

尚、認証アルゴリズムとして hmac-md5、暗号アルゴリズムとして 3DES-CBC を使用し、アルゴリズムの違いにおける通信性能等の比較は実施しない。

CA の発行する証明書は X.509 証明書形式 V3、CRL は X.509 CRL 形式 V2 に準拠とする。CA の署名アルゴリズムとして、ハッシュ関数は MD5、鍵長 2048 ビット RSA を使用した。また信頼モデルとしては、単独 CA モデルとした。

尚、評価項目は以下に挙げる 3 項目である。

①漏洩耐性
②改竄耐性
③リプレイ攻撃耐性

実験に先立ってFreeBSD、WindowsXPといったIPv6に対応したOSのIPsec機能の確認を行った[資料18-21]。

4.2.11 漏洩耐性の評価

(1) 測定方法

IPsec機能の一つとして、通信内容の暗号化による機密性確保がある。ここでは通信内容が漏洩しているか、いないかの評価、検証を行った。

以下に漏洩耐性の評価基準、評価方法、評価環境を示す。

評価基準：通信経路の途中で傍受を行っても、通信内容が漏洩しないこと。

評価方法:IPsecを使用する､しない場合とでFTPによるファイル転送を行い、Snifferを用いて、パケットデータの観察を行った。

評価環境：漏洩耐性評価環境を図 4-8に示す。

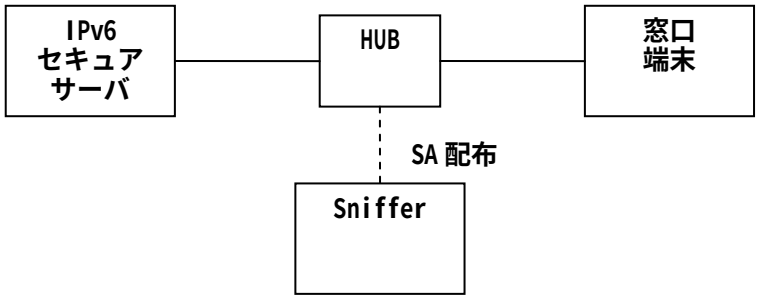


図 4-8　漏洩耐性評価環境

(2) 測定結果

(i)　IPsecを使用しない場合

Sniffer等のLANアナライザを用いることにより、容易に通信内容の傍受ができた[資料22]。

(ii) ESPのトランスポートモードの場合

FTPによるファイル転送を行っていることが分からなかった｡これはIPsecにおけるESPの暗号化機能により､パケットが暗号化されているからである。

全てのパケットのデータが暗号化されており、ログイン ID、ログインパスワード、ファイル名、ファイルの内容は解読できなかった。つまり、機密性が保たれていることが分かる[資料 23]。

(iii) ESP のトンネルモード

上記の結果と同様にデータの解読はできなかった。機密性が保たれていることが分かる[資料 24]。

4.2.12 改竄耐性の評価

(1) 測定方法

IPsec 機能の一つとして、通信データの完全性の保証がある。これは通信データが送信元と宛先の間で改竄されていないことを保証するものである。

以下に改竄耐性の評価基準、評価方法、評価環境を示す。

評価基準：IPsec を使用した状態でデータ改竄を行った場合、その改竄が検知できること。

評価方法：IPsec を使用する場合、しない場合とでパケットの送受信を行う。

Sniffer を用いて、キャプチャしたパケットに改竄を施し、もとの NW 上に送信する。

評価環境：耐改竄性評価環境は図 4-9になる。

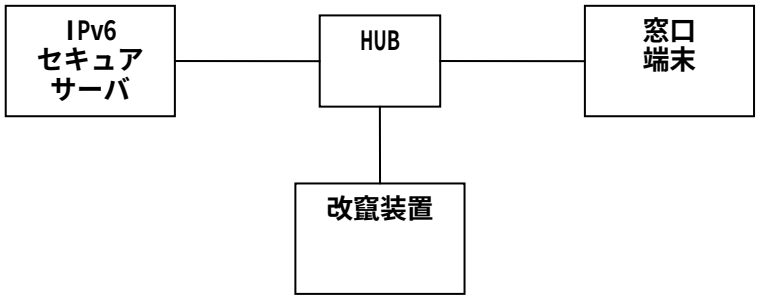


図 4-9　耐改竄性評価環境

改竄装置は担当窓口端末から IPv6 セキュアサーバに送信されたパケットを横取りしてそれを改竄し、担当窓口端末に成りすまして IPv6 セキュアサーバに再送信する機能を持つ。

(2) 測定結果

(i)　IPsec を使用しない場合

改竄されたパケットを受信していること及び改竄されたパケットに対し

て返信していることが確認できた。IPsec を使用しない場合は改竄されたデータに対して受信、返信を行うことが分かる[資料 25]。

(ii) ESP のトランスポートモード

IPv6 レベルでは改竄されたパケットを受信していることが確認できたが IPsec レベルではパケットを正しく受信していない。そのため、送られてきたパケットに対して返信していないことが確認できた。このことから ESP のトランスポートモードでは改竄されたデータを検知していることがいえる[資料 26]。

(iii) ESP のトンネルモード

ESP のトンネルモードでは IPv6 レベルでは改竄されたパケットを受信していることが確認できたが、IPsec レベルでは、パケットを正しく受信していないことが確認できた。このため、送られてきたパケットに対して返信していない。このことから、ESP のトンネルモードでは改竄されたデータを検知することがいえる[資料 27]。

(iv) AH のトランスポートモード

AH のトランスポートモードでは、IPv6 レベルでは改竄されたパケットを受信していることが確認でき、IPsec レベルでは改竄されたパケットを検知して、破棄していることが確認できた。このことから送られてきたパケットに対して返信していないことが確認できた。AH のトランスポートモードは、改竄攻撃を検知しているといえる[資料 28]。

4.2.13 リプレイ攻撃耐性の評価

(1) 測定方法

第三者があるトランザクションのログをとっておき、あとでそのログと同じことを繰り返してそのトランザクションの結果を得ようとすることを、リプレイ攻撃という。IPsec 機能の一つとして、リプレイ攻撃の防御がある。

以下にリプレイ攻撃耐性の評価基準、評価方法、評価環境を示す。

評価基準：IPsec を使用した状態でリプレイ攻撃を行った場合、リプレイが検知できること。

評価方法：Sniffer にて ping6 の実行結果のキャプチャを行い、キャプチャしたパケットの一つを再び送信する。

評価環境：リプレイ攻撃耐性評価環境は図 4-10になる。

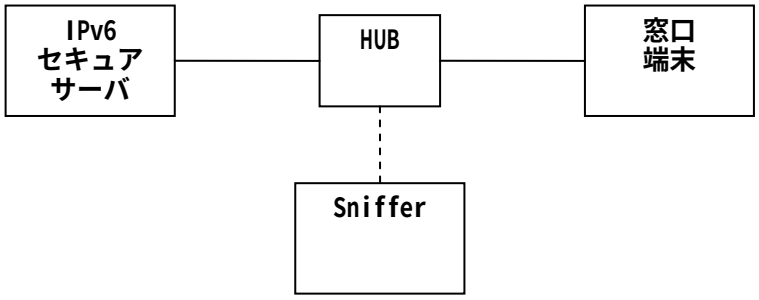


図 4-10　リプレイ耐性評価環境

(2) 測定結果

表 4-7に、パラメータの組合せにおけるリプレイ攻撃防御機能の有無を示す。リプレイ攻撃耐性の評価、検証から得られた結果をまとめると以下のようなる[資料 29-35]。

表 4-7　リプレイ攻撃防御機能の有無

IPsec のモード	ウィンドウサイズ	認証機能あり	認証機能なし
トランスポートモード	ウィンドウサイズ指定	○	×
	ウィンドウサイズなし	×	×
トンネルモード	ウィンドウサイズ指定	○	×
	ウィンドウサイズなし	×	×

リプレイ攻撃防御機能有効：○
リプレイ攻撃防御機能無効：×

表 4-7 より、ウィンドウサイズの指定、認証機能を有効にした場合にのみ、リプレイ防御機能が有効となることが分かる。

ウィンドウサイズが指定されていても、認証機能がなかった場合、次のようなことが起こりうる。

リプレイ攻撃を行う者が、再送するパケットのシーケンス番号を相手がまだ受信していないシーケンス番号に改竄した場合、受信側がリプレイ防御機能を有効にしていても、受信してしまう可能性がある。特に、攻撃者が非常に大きなシーケンス番号をもった IPsec パケットを送信した場合にはそのパケットを受信してしまうばかりでなく、そのシーケンス番号に合わせて、リプレイ防御ウィンドウが大きくスライドしてしまうため、その後に送られてくる正規の IPsec パケットを破棄してしまう。

シーケンス番号が改竄されないために、ヘッダを保護する必要があるため、

手動で SP、SA の設定を行った場合、リプレイウィンドウサイズの他に認証機能が必須となってくる。

4.2.14 IKE を利用した場合のリプレイ攻撃耐性の評価

(1) 測定方法

IKE にて SA の生成、管理を行い、IPsec の評価、検証を行った。

ESP を適用したトランスポートモード、トンネルモードの両方で評価、検証を行うこととする。また ESP では認証機能を有効にする。(リプレイ防御機能を有効にするため。)

IKE における認証方式としては電子証明書認証方式を採用する。(KAME の開発している IKE デーモン Racoon はパッケージ又は ports を利用する。)

各々の端末用に電子証明書とその証明書を発行したルート CA(1 階層)の証明書を準備する。発行する電子証明書は EC1 保有の CA にて発行されたものであり、X.509 証明書形式に準拠。CA の署名アルゴリズムとして、ハッシュ関数は MD5、鍵長 2048 ビット RSA を使用する。

IKE のフェーズ 1 において、通信モードとしてはアグレッシブモード、暗号アルゴリズムとしては 3des、ハッシュアルゴリズムとしては sha1 を指定することとする。IKE のフェーズ 2 において、暗号アルゴリズムとしては 3des、ハッシュアルゴリズムとしては hmac_md5、また圧縮アルゴリズムでは deflate を指定することとする。

以下に IKE を利用した場合のリプレイ攻撃耐性の評価基準、評価方法、評価環境を示す。

評価基準：IPsec を使用した状態でリプレイ攻撃を行った場合、リプレイが検知できること。

評価方法：Sniffer にて ping6 の実行結果のキャプチャを行い、キャプチャしたパケットの一つを再び送信する。

評価環境：リプレイ攻撃耐性評価環境は図 4-11になる。

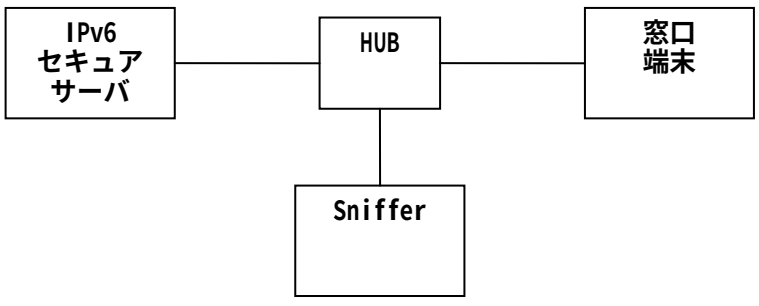


図 4-11　リプレイ攻撃耐性評価環境

(2) 測定結果

ESP のトランスポートモードでは IPsec パケットを受信しておらず、リプレイチェック値がリプレイ攻撃前より増加している。再送したパケットに対して、相手側からの応答がないリプレイ攻撃を検知していることがいえる[資料 36]。

4.2.15 まとめ

(1) 今回構築した IPv6 セキュリアサーバにより WindowsXP 相互間、WindowsXP 及び FreeBSD における IPsec 相互接続が確認できた。

(2) FreeBSD 相互間における IPsec 機能の確認を行い、漏洩耐性、改竄耐性、リプレイ攻撃耐性に関して調査を行った。各々の調査に関して、IPsec を使用した場合、しなかった場合で差異があり、IPsec を使用した場合はデータの保護、リプレイ攻撃に対する防御がなされていることが確認できた。

(3) これらの結果から、IPv6 の IPsec 機能により行政サービスで利用されるアプリケーションプロトコルに依存することなく、改竄、盗聴、成りすましから防止できることが確認できた。

4.2.16 課題

(1) 操作性、利便性

各種 OS での IPsec のサポートは、現状でも不十分であり設定が複雑で IPv6 のサポートが完全でない。今後、利用者が IPsec の細かな設定を意識せず簡単に安全に利用できるために OS やツール等への IPsec の実装の仕方に改善の必要がある。

(2) 通信相手の確認

IPsec 通信を行うためには、予め通信相手のセキュリティポリシーを知っておかなければならない。不特定多数の市民を相手にするような行政サービスにおいては、通信を開始する前段に相手を認証し相手のセキュリティポリシーに合わせて自分のセキュリティポリシーを構成するといった仕組みが必要になる。

(3) マルチキャスト対応

IKE は 2 者間での鍵交換プロトコルであるので、複数のホストとの間で利用することができない。多地点での相談をマルチキャストを用いてセキュア

に実施するなどの応用のためには IPsec のマルチキャスト対応の検討が必要である[4]。

(4) DoS 攻撃に対する耐力

DoS 攻撃（Denial of Service attack）などの攻撃は、傍受や改竄ではなくサービスを不能にしてしまうことを目的としているためその防止が困難である。IPsec は特に高負荷な処理であるため、他のサービスに比べ攻撃を受けたときの影響も大きい。IPsec 以外の実装で DoS 攻撃等に対する配慮も必要になる。

(5) 通信の存在

IPsec では IP ヘッダは暗号化されていない。そのためネットワーク上のトラフィックを統計的に調べることで、どことどこ（誰と誰）がいつ通信を行ったかという通信の存在やその量は知られてしまう。そのため通信の存在自体を解析される脅威は依然として残る。

(6) 規制などに関する問題

暗号技術は、アメリカなどのように国家安全保障上の理由からある一定以上の強度の輸出を禁じている国が多数存在する。特にアメリカには IPsec の技術開発で中心的な企業が多数存在しているため、IPsec で利用できないアルゴリズムも存在する。今後各国の規制が緩和されないと IPsec の普及は進展しない。

4.3 個人認証技術の調査、検証

PKI を利用した個人認証において、通信プロトコルが IPv6、IPv4 に係りなく同様に行える必要がある。そこで今回構築したシステムにおいて IPv6 を利用して IPv4 と同様な個人認証が可能であることの検証を行った。

4.3.1 PKI 概要

公開鍵暗号方式の通信を開始するために、使用する公開鍵が本当に相手のものであるかを確認する必要がある。公開鍵の所有者を正しく確認するために信頼できる第三者機関 (TTP： Trusted Third Party)に公開鍵の所有者を保証してもらう。TTP は、公開鍵の所有者の本人性をなんらかの方法で確認し、公開鍵とその所有者を保証する証明書(Certificate)を発行する。証明書には、公開鍵とその所有者を証明する情報が記載され、改竄を防ぐために TTP による署名が付与される。

証明書を発行する認証局（CA）は、「認証局運用規定 (CPS: Certificate Practice Statement)」 と呼ばれる文書を公開して、セキュリティポリシーを定めることになっている。

4.3.2 構成要素

PKI 構成要素は表 4-8のとおりである。

表 4-8　PKI 構成要素

認証局 (CA：Certification Authority)	証明書所有者(Certificate Holder)に証明書を発行する。 エンドエンティティ(End Entity) [35] に対して、公開鍵と対応する秘密鍵の所有者を結びつける証明書（公開鍵証明書）を発行する。 発行した証明書の信頼性が失われた場合は、その証明書を失効させ、証明書失効リスト（CRL)を発行する。 証明書利用者が取得できるように、証明書と CRL をリポジトリに公開する
登録局 (RA: Registration Authority)	PKI を大規模で運用する際に、発行権限の分散管理を可能にして運用コストを削減する。 PKI ユーザからの証明書申請が発生した場合に、本人性の確認を行う。 CA に対して証明書の発行や失効を要求する。
リポジトリ (Repository)	証明書及び CRL を格納し、PKI ユーザへ公開します。CA が発行した証明書や CRL を格納する。 証明書や CRL を証明書利用者が検索して取得をできるようにする。
アーカイブ (Archive)	証明書の長期保存や秘密鍵のバックアップを行う。 電子署名の長期保存に適用するため、有効期限が切れた証明書や CRL を保持する。 暗号目的で利用される秘密鍵のバックアップを行う。
証明書所有者 (Certificate Holder)	証明書を発行される人（エンティティ）のこと。加入者 (Subscriber) とも言う。 証明書及び対応する秘密鍵を用いて、電子文書へのデジタル署名や暗号文の復号を行う。 RA へ証明書の申請を行う。 証明書に対応する秘密鍵を安全に保持し、デジタル署名や暗号文の復号に使用する。
証明書利用者 (Relying Party)	証明書所有者の証明書を入手し、デジタル署名の検証や文書の暗号化を行う。信頼できる CA （トラストポイント） の一覧を安全に管理する。 リポジトリから証明書や CRL を取得し、それらの有効性を検証する。 取得した証明書を使い、署名検証や文書の暗号化を行う。

ディレクトリについては資料 37-39 を参照のこと。

4.3.3　X.509 電子証明書

X.509 証明書は、用途によって以下の種類があり、一般に「証明書」という場合は、「公開鍵証明書」のことを指す。証明書の種類を

表 4-9に示す。証明書のフォーマットについては資料 40 参照のこと。

表 4-9 証明書の種類

公開鍵証明書 (Public Key Certificate)	CA 証明書	CA に対して発行する証明書。
	エンドエンティティ証明書	PKI ユーザに対して発行する証明書。
属性証明書 (Attribute Certificate)		公開鍵証明書で証明された人に対して、その人が所有する権限や役割を証明する。
特定証明書 (Qualified Certificate)		人（自然人）に対して発行することを目的とした証明書。

4.3.4 PKI アプリケーション

電子申請で利用される PKI アプリケーションには TLS/SSL やデジタル署名がある。以下それらの概要について述べる。

(1) TLS/SSL

TLS /SSL(Transport Layer Security) は、クライアント/サーバー間通信をセキュアに保つプロトコルである。TLS/SSL は 、TCP/IP レイヤの上で動作し、HTTP、LDAP、FTP、TELNET 等のアプリケーションで利用できる。TLS/SSL を利用するには、サーバーとクライアントに証明書が必要になるが、クライアントを認証しない場合はクライアント側の証明書は必要ない。TLS/SSL は、以下のセキュリティ機能を持つ。

(i) 認証 (Authentication)

X.509 証明書を利用することで、サーバー及びクライアントの認証を行い、第三者による成りすましを防止する。

(ii) 守秘性 (Confidentiality)

サーバーとクライアント間の通信を暗号化することで、第三者への情報の漏洩を防止する。暗号化は共通鍵によって行い、共通鍵をサーバーとクライアント間で交換するために X.509 証明書の公開鍵を用いる。

(iii) 完全性 (Integrity)

サーバーとクライアント間で交換されるデータの完全性を確認し、情報の改竄を防止する。完全性の確認には MAC (Message Authentication Code)を用いる。

電子申請アプリケーションでは通信相手の認証と通信内容の漏洩防止の目的で TLS/SSL を利用する。利用者が行政機関の電子申請サーバにアクセスする際に電子申請サーバに格納された公開鍵証明書（CA 証明書）により通信相手が行政機関のサーバであるかどうかを検証することができる、同様に電子申請サーバ側では利用者にあらかじめ配布しておいた公開鍵証明書（エンドエンティティ証明書）によりアクセスしてきた利用者が登録を受けているものであるかどうかを検証することができる。両者によりお互いが認証された後は共通鍵をセキュアに交換し、共通鍵による暗号化通信が開始される。

(2) XML 署名の概要

XML は拡張可能なマークアップ言語であり、テキストファイルでありながら構造化された情報を柔軟に扱うことが可能である。XML 文書に対する改竄、成りすましを防止するためのデジタル署名を付与するための規格として、W3C (World Wide Web Consortium) において「XML 署名(XML Signature)」の標準化が進められている。XML の署名要件(RFC2807)、XML 署名構文と処理(RFC3075)、XML の正規化 (RFC3076) が RFC として公表されている。XML 署名の中の署名データは XML 形式で表現される。XML 署名の主な特徴を以下に示す。

(i) 署名を XML で表現するため、従来のバイナリ形式の署名に比べて可読性や再利用性が向上する。
(ii) XML 以外の文書にも署名可能である。
(iii) 文書の一部分への署名、複数の XML 文書への一括した署名、複数人による署名が可能である。

XML 署名は、次のセキュリティ機能を提供する。

(i) 完全性 (Integrity)
署名対象のデータの改竄を検出する。
(ii) 認証 (Authentication)
署名に付与する署名者の証明書により、署名者を認証する。
(iii) 否認防止 (Non Repudiation)
XML 文書に対する否認を防止する。

電子申請アプリケーションではダウンロードした申請フォームに申請フォー

ムの発行機関の署名を付加することで真に行政機関で発行されたものであるかどうか、及び、フォームの内容が途中経路で改竄されていないことを利用者側で検証することができる。また、利用者が必要事項を記入した申請フォームを行政機関に返送する際にそのフォームに署名をつけて送り返すことで、記入内容が利用者自身によるものであること、及び、その内容が途中経路で改竄されていないことを保証することができる。

4.3.5 検証内容

実験に利用したシステム構成を図 4-12に示す。

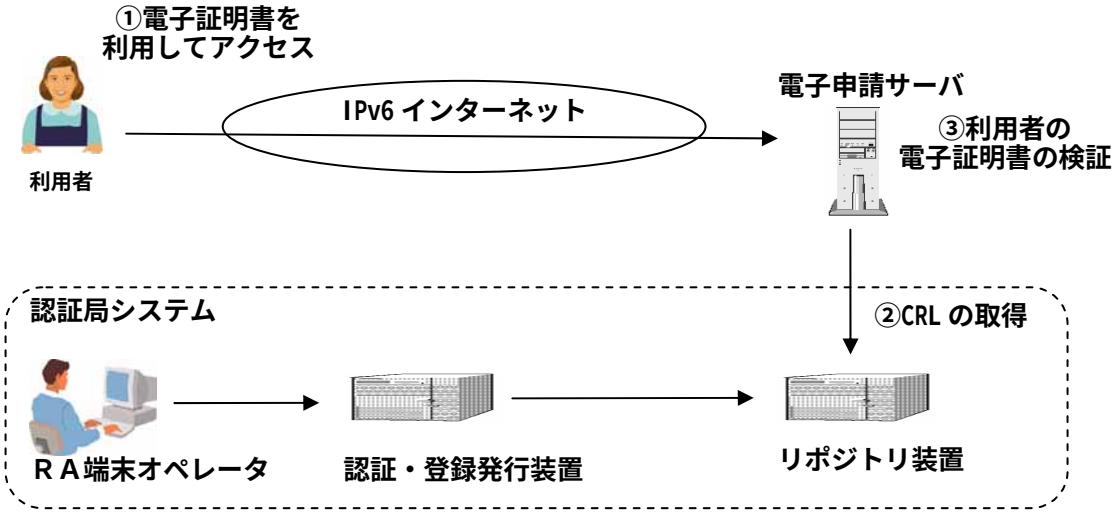


図 4-12 システム構成

下記の手順で利用者の個人認証が行われる。

①利用者が電子証明書を利用して電子申請サーバにアクセスする。

②電子申請サーバは利用者の電子証明書を確認して岡山市認証局から発行された登録ユーザのものかどうかを確認する。

③登録ユーザのものであることが確認されると、何らかの理由でそれが失効していないかどうかをリポジトリ装置から CRL[資料 41-43]を取得し確認する。

④有効であることが確認されると要求を受付、電子申請の手続が始まる。電子証明書が正しいものではなかったり、失効していたりすると要求を受け付けない。

この電子証明書を用いた個人認証システムにおいて、以下の項目について検証を行う。

①電子証明書の真正性認証動作の検証

②電子証明書の有効性認証の検証

4.3.6　電子証明書の真正性確認の検証

(1) 検証内容

岡山市認証局の電子証明書（認証局自体の電子証明書）を信頼されたルート証明機関として電子申請サーバへ登録しておく。その他の認証局の電子証明書は電子申請サーバへ登録しない。

次に岡山市認証局から発行された電子証明書及び、その他の認証局から発行された電子証明書を利用者の端末にインストールし、各々の電子証明書を利用して電子申請サーバへアクセスする。岡山市認証局から発行された電子証明書はアクセスを受付、その他の認証局から発行された電子証明書はアクセスを受け付けられない事を確認する。図 4-13に岡山市認証局から発行された電子証明書を示す。

以上の確認を IPv6 ネットワークで実施し IPv4 と同様に動作することを確認する。

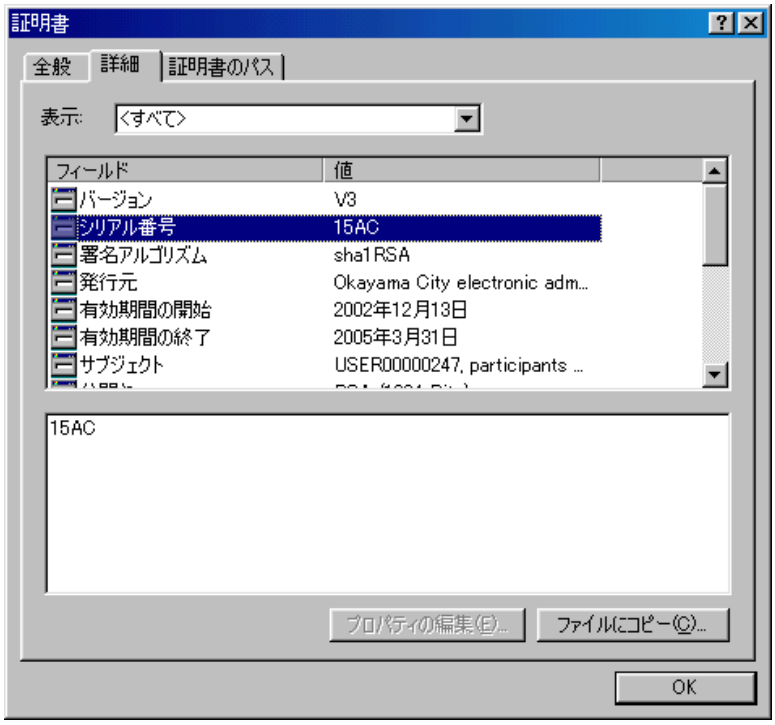


図 4-13 岡山市認証局から発行された電子証明書

(2) 検証結果

IPv6 及び IPv4 のそれぞれのプロトコルに対し、岡山市認証局から発行された電子証明書を選択すると署名処理が正常に受け付けられたが、岡山市以外の認証局で発行された電子証明書では受け付けてもらうことができなかった。したがって、問題なくアクセス制御されることを確認できた[資料 44]。

4.3.7 電子証明書の有効性確認の検証

(1) 検証内容

岡山市認証局から２枚の電子証明書を発行し、一方を失効する。失効した電子証明書を確認する為に CRL の発行、及び、登録を行う。

２枚の電子証明書を利用者の端末へインストールし、各々の電子証明書を利用して電子申請サーバへアクセスする。失効していない（有効な）電子証明書はアクセスを受付、失効した電子証明書はアクセスを受け付けられない事が予測される。図 4-14にCRL の内容を示す。

以上の確認を IPv6 ネットワーク、及び、IPv4 ネットワークを利用して実施し同様に動作することを確認する。

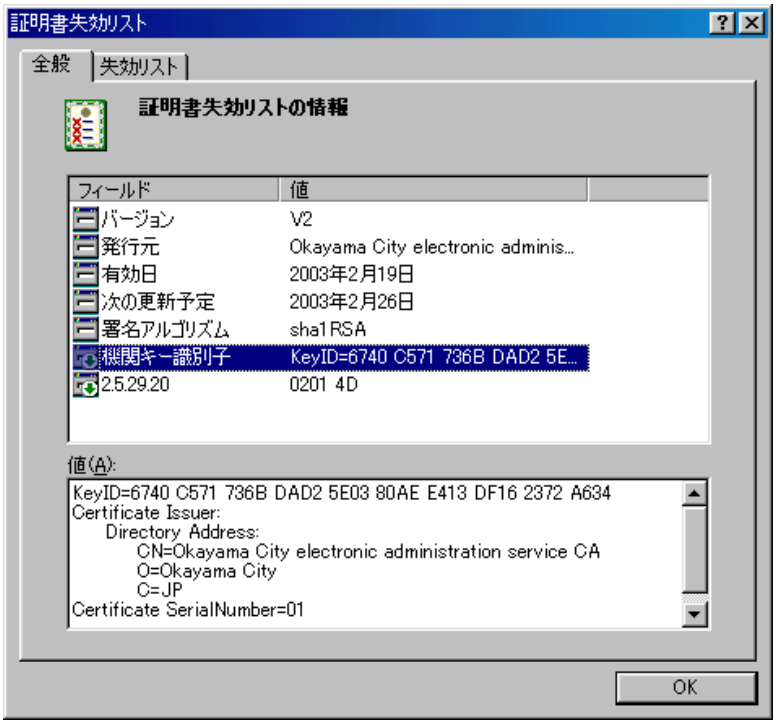


図 4-14 CRL の内容

(2) 検証結果

IPv6 及び IPv4 のそれぞれのプロトコルに対し、電子証明書選択画面で失

効していない（有効な）電子証明書を選択すると署名処理が正常に受け付けられたが、失効した電子証明書による署名では受理されなかった。

したがって、問題なくアクセス制御されることを確認できた[資料 45]。

4.3.8 まとめ

(1) IPv4、IPv6 の両方のプロトコルで、正しく発行された電子証明書、及び他の機関により発行された電子証明書による署名において、ただしく発行されたものを用いたときは受理され、他の機関で発行されたものを用いたときは受理されないのを確認した。

(2) IPv4、IPv6 の両方のプロトコルで有効な電子証明書による署名は受理され、失効しているものを用いたときは受理されないのを確認した。

(3) これらの結果から、IPv6 でも IPv4 と同様に行政アプリケーションでの個人認証が可能であることが確認できた。

4.4 真正証明技術の調査、検証

4.4.1　背景と目的

近年、電子自治体推進に向けて多くの自治体で法人市民税の申告など一部の手続について、インターネットを活用した「電子申請」の試験運用が実施されているところである。しかし、証明書などの交付文書においては市役所窓口に出向いていくか、郵送に頼らざるを得ないのが現状である。

今回の実証実験では、申請後の証明書交付までを市役所窓口に出向くことなく申請場所（自宅又は、公民館等）において完結することを目指し、映像対話などのアプリケーションとともに、自宅などのプリンタで証明書などの交付を実現する映像対話型電子申請・交付システムを構築することにより、効率的かつ利便性の高い電子的行政サービスに向けた実証実験を行った。

電子申請の後に交付される交付文書などを取得し自宅などのプリンタから出力されるまでのプロセスにおいて複製や改竄など様々な危険やリスクを伴うことが予測される。

通常窓口で発行される交付文書には公印が押されているが、交付文書の紙自体に透かしや牽制文字といった特殊な印刷が施されており利用者はその紙自体から本物であることを即座に認識できる。しかしながら、家庭で印刷される交付文書は家庭用のパーソナルプリンタや普通紙とで作成されるため上記の特殊な印刷を施した紙を利用することができない。家庭での交付文書発行を実現するためにはなんらかのセキュリティ対策を施さなければならない。

本実証実験においては、紙ベースでセキュリティ対策を講じる技術を利用して、申請後の証明書交付までを市役所窓口に出向くことなく申請場所において完結するためのきセキュリティ対策について検討するとともに、この実現に向けて必要とされるシステムの構築とその有効性について調査、検証を行った。

4.4.2　交付文書の真正証明モデル

紙文書の真正を証明するために紙文書自体にデジタルのデータを埋め込み、そのデータを検証することで真正を証明するモデルを考案した。本モデルは以下の要件を満たしていなければならないこととした。

(i)　紙文書にデジタルデータを埋め込んで印刷することができること。
(ii) 印刷された紙文書に埋め込まれたデジタルデータを読み込み、その真正証明ができること。
(iii) 埋め込まれたデジタルデータが容易に複製、解読、改竄されないこと。

4.4.3 多値画像による二次元コード技術（MIG コード技術）

交付文書の真正証明モデルの要件①、②について、交付文書に印刷される公印に、多値画像によって形成される特殊な二次元コード技術（以下、MIG コード技術）を使用する方法で実現することとした。

文書の「余白部分」にコード情報を埋め込む方式としては、1 次元コード（バーコード)、2 次元コードが一般的に普及しており、バーコードは商品識別や図書館の貸出しなどの幅広い分野で､2 次元コードは有価証券などで利用されている。一方､文書の内容(画像/テスト文書等)にコード情報を埋め込む方式としては“透かし”（デジタル画像に情報を埋め込む電子透かしを印刷に応用したもの）と呼ばれる方式が採用されている。1 次元や 2 次元コードの特徴としては、情報量は多い反面、紙面上の「余白部分」にしか情報を付与することが出来ない。

透かし技術は、写真などの画像部分にも画質を劣化させずに情報を埋め込むことが可能である反面、埋め込み可能な情報量は少なく、画像等の状態（白/黒部分が多い等）によっては埋め込み可能な情報量が不安定であり、デコード性能に影響を及ぼすという短所があるため広く普及するまでは至っていない。

MIG コード技術は 1 次元、2 次元コードと透かしの優位性を併せ持った微細な画像形成コード技術であり次のような特徴を持つ。

(1) 情報量

2 次元コードには多少劣るが、“透かし”よりも多くの情報を埋め込むことが可能であり一定かつ安定的な情報量（約 30～50Byte/ｃ㎡）を確実に埋め込めることができる。

(2) 対象ドキュメントの柔軟性

画像/テキスト文書等に対して情報を埋め込むことが可能であり（“透かし”と同様)、濃度変調レベルを制御することにより偽造困難度や真偽判定度が極めて高い。

(3) デザイン性

コードの生成は単純な矩形ではなく、現在の押印などに変わるものとして

シンボリックにデザインをすることも可能である。

(4) 画質

“透かし”と比較すると多少画質は劣化する。

本システムでは、既存の交付文書の様式に極力手を加えずそのまま利用することを前提としているために、紙面の余白を利用することなく文書中の画像に情報を埋め込める MIG コード技術を採用した。

4.4.4 牽制画像フォーマット技術

交付文書の真正証明モデルの要件③を実現するために、牽制画像フォーマット技術を利用した。

紙文書は、複写機の普及により極めて容易に複製することが可能になった。こうした不正利用を防止するため、複写したときに牽制文字を浮かび上がる画像フォーマットを新に構築することにした。現在、行政サービスにおいて交付文書への不正利用を牽制するために、プレ印刷された専用紙が広く利用されている。

しかしながら、証明書交付までを申請場所（自宅又は、公民館）で完結するためには、自宅などに普及したパーソナル型のプリンタと普通紙などによって牽制文字の印刷が実現されなければならない。

牽制画像フォーマット技術は、複写機の再現性を利用したプリンタの印字ドットの重畳パターンにより、普通紙などに隠し文字を埋め込むことを可能とする。これにより、一般的に普及しているパーソナル型プリンタと普通紙などによって、不正利用に対する視覚的な牽制を実現する。

牽制画像フォーマットの特徴は以下のとおりである。

(1) パーソナル型プリンタと普通紙などで実現（専用紙の必要がない）
(2) 複写したときに「禁複写」「無効」などの隠し文字が浮かび上がる
(3) 印字情報を損なわない

4.4.5 システム構成

MIG コード技術及び牽制画像フォーマット技術を用いて交付文書の真正を証明可能なシステムを構築した。図 4-15に交付文書の申請証明を行うシステムを示す。

申請情報管理サーバから取得される交付文書イメージデータ（TIFF 形式）に対して、MIG コードや牽制画像フォーマットの合成を可能とする。

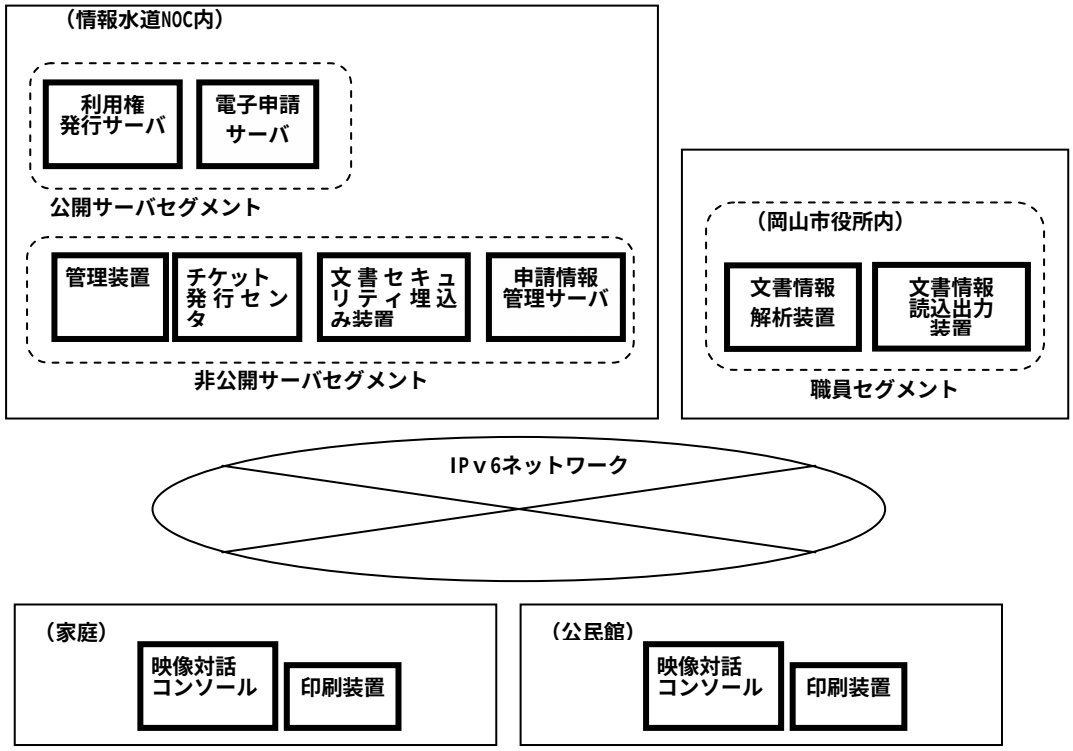


図 4-15 交付文書の申請証明を行うシステム

このシステムの持つ機能を以下に示す。

(1) セキュリティ埋込み機能

(i) MIG コード

交付文書の一意を特定する情報を抽出し、MIG エンコーダモジュールを使用して公印画像ファイルを形成する機能を提供した。形成された公印画像ファイルは、牽制画像フォーマットとともに交付文書ファイルに合成される。

(ii) 牽制画像

牽制画像フォーマットとこれを交付文書イメージデータ（TIFF）に合成する機能を提供した。

本システムにおいては、牽制画像フォーマットに「複製」「無効」の 2 種

類の隠し文字を埋め込むことにした。

(2) 交付文書印刷機能

交付される交付文書の自宅などにおける印刷においては設置環境等を考慮し、以下の仕様によるパーソナル型のプリンタを使用した。

表 4-10 プリンタ

製　造	富士ゼロックス株式会社
製品名	JetWindB70

(3) 文書解析機能

文書解析機能においては交付文書を管理するサーバからネットワーク経由で一意を特定する比較対象データを取得し、公印画像部を切り出した後、MIG デコードモジュールを使用して埋め込まれた特定情報を取得する機能を提供した。

4.4.6　検証内容

(1) 実験仕様

以下の仕様で交付した文書の真正証明、複製防止等について検証を行った。

(i)　交付文書の真正を識別する情報は、600dpi の解像度で多値画像(MIG コード）化された市長印などの公印に埋め込むことにする。

(ii) 公印画像に埋め込む識別情報は申請情報管理サーバから CSV 形式で取得することにする。

また、CSV ファイルに記述する識別情報は以下の項目とした。

表 4-11図 4-16 CSV ファイルに記述する識別情報

No.	項目	バイト数	No.	項目	バイト数
1	担当窓口番号	1	5	証明書種類	3
2	証明書連番	10	6	見本判定	1
3	時間	6	7	日付	6
4	利用者 ID	8	8	連番頭	1

(2) 測定手順

①真正証明技術を利用した交付システムから提供された交付文書は映像対話コンソールに接続された印刷装置から出力する。

②出力した交付文書は、文書情報読込出力装置のスキャナ部を用いて読み取る。

③文書情報読込出力装置を経由して得られた公印画像の情報読取、解析は、文書情報解析装置において実施する。

④公印画像の解析から得られる結果をもとに申請情報管理サーバに保管される一意を特定する比較対象データとネットワーク経由で照合する。

⑤また、このとき一意を特定した識別情報の一部を画面に表示する。

⑥交付文書イメージデータは TIFF 形式で申請情報管理サーバから取得することにする。

⑦交付文書イメージデータ（TIFF）には、複製などの不正利用を視覚的に牽制するための画像フォーマットを合成する。

⑧交付の対象となる証明書と公印種類を表 4-12に示す。

表 4-12 証明書と公印種類

申請業務	証明書名	公印
市県民税（所得・課税）証明	市県民税（所得・課税）証明書	市　長
	市県民税（所得・課税・控除）証明書	市　長
	市県民税（所得・課税・控除）証明書 特別児童扶養手当・児童扶養手当用	市　長
	所得証明書（児童手当用）	市　長
固定資産（評価・公課）証明	固定資産評価証明書	市　長
	固定資産評価証明書(評価なし)	市　長
	固定資産公課証明書	市　長
納税証明	納税証明書	市　長
	軽自動車税納税証明書	市　長
補装具（交付・修理）申請及び判定通知書交付	判定通知書	福祉事務所長
障害証明書申請及び障害証明書交付	証明書	福祉事務所長

(3) 評価項目

真正証明技術の評価、検証を行う。以下に信頼性評価のための評価項目・

評価基準、評価方法を示す。

信頼性に関する評価項目は以下の４項目とする。

①エンコード耐性
②デコード耐性
③真正性
④世代耐性

4.4.7　エンコード耐性の検証

(1) 評価基準

20%以上のエラー修正率を与えた交付文書の公印画像に対する識別情報のエンコード率が 90%以上確保されることとした。

(2) 評価方法

エンコード耐性の評価環境を図 4-17に示す。

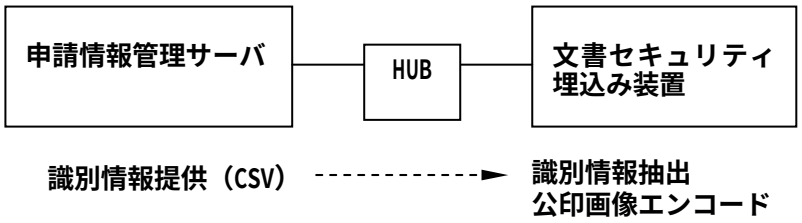


図 4-17 エンコード耐性の評価環境

エンコード耐性は、申請情報管理サーバから受信した CSV ファイルの識別情報を公印画像へ埋め込む際のエラー数を文書セキュリティ埋込み装置において確認することで行う。実施手順を以下に示す。

①文書セキュリティ埋込み装置の実行ログファイルデータを採取する。
②文書セキュリティ埋込み装置の実行ログファイルからエラー数を検出する。
③エラー数をもとにエンコード率を算定する。

(3) 検証結果

平成 15 年 2 月 7 日～2 月 25 日の期間において実施された公印画像作成 55

件について評価を行った。表 4-13にエンコード率を示す。

この期間において、エラーログ検出数は 0 件であり、エンコード率が 100%確保されていることが確認された。

表 4-13 エンコード率

期　間	実行件数	エラー数	エンコード率
2 月 7 日～2 月 14 日	29	0	100%
2 月 17 日～2 月 21 日	16	0	100%
2 月 24 日～2 月 25 日	10	0	100%
合　計	55	0	100%

4.4.8　デコード耐性の検証

(1) 評価基準

正常に印刷された交付文書の公印画像に対する識別情報のデコード率が 90%以上確保されることとした。

(2) 評価方法

文書情報解析装置において公印画像からの情報読取、解析する際のエラー数により確認を行った。デコード耐性の評価環境を図 4-18に示す。

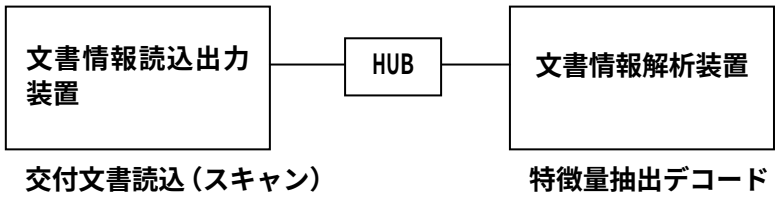


図 4-18 デコード耐性の評価環境

実施手順について以下に示す。

①文書情報解析装置の実行ログファイルデータを採取する。

②文書情報解析装置の実行ログファイルからエラー数を検出する。

③エラー数をもとにデコード率を算定する。

(3) 検証結果

平成 15 年 2 月 7 日～2 月 25 日の検証期間において、文書情報解析装置の

実行が 5 件あり、その中にエラーログが 1 件検出された。このことよりデコード成功率は 80%となり、90%以上を満足することができなかった。デコード率を表 4-14に示す。

表 4-14 デコード率

期　間	実行件数	エラー数	デコード率
2 月 7 日～2 月 14 日	3	1	67%
2 月 17 日～2 月 21 日	2	0	100%
2 月 24 日～2 月 25 日	0	0	―
合　計	5	1	80%

4.4.9　真正性確認の検証

(1) 評価基準

印刷された交付文書から得られる情報をもとに特定の自治体が発行したという真正性と改竄などの不正利用を判別できることとした。

(2) 評価方法

真正性の評価環境は図 4-19になる。

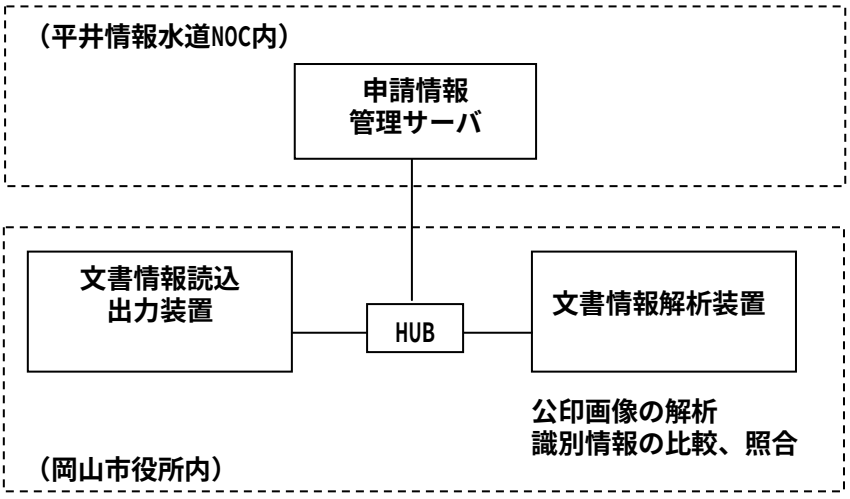


図 4-19 真正性の評価環境

識別情報をエンコードした公印画像を伴って印刷された交付文書から、その解析よって得られる結果をもとに原本など一意を特定する比較対象データと一致することによって判定した。

また、このとき一致した識別情報の画面表示によって、交付文書の記述と

比較を可能にすることで改竄などの不正行為を確認できることとした。
実施手順について以下に示す。

①交付文書の解析実行画面に ID、パスワードとともにログインする。
図 4-21に解析実行のログイン画面イメージを示す。

図 4-20 解析実行のログイン画面イメージ

②文書情報読込出力装置のスキャン部を利用して印刷された交付文書を読み込む。図 4-21に文書情報読込装置の操作イメージを示す。

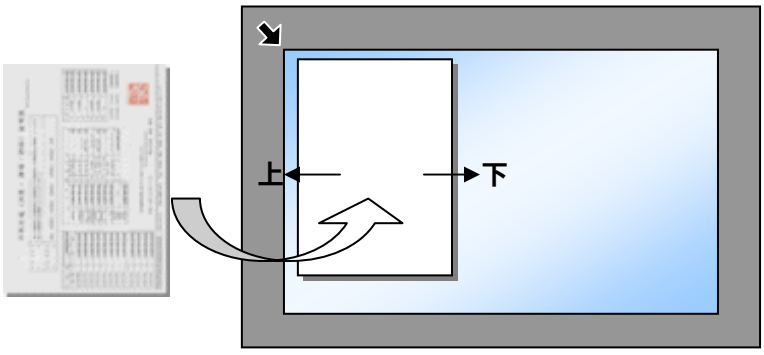


図 4-21 文書情報読込装置の操作イメージ

③文書情報読込出力装置で読み込まれたスキャン画像は、ネットワーク経由で文書情報解析装置に転送する。図 4-21に受信フォルダー転送完了イメージを示す。スキャン画像が文書情報解析装置の受信フォルダー内に転送されたことを確認する。

図 4-22 受信フォルダー転送完了イメージ

④証明書認証画面の「表示」ボタンを押して解析を実行する。

図 4-23　実行画面イメージ

⑤交付文書の解析の結果をもとに原本などの一意を特定する比較対象データと照合する。このとき、一致した識別情報の証明書名、氏名、文書 ID、日付の項目が正常に画面表示されることを確認する。

(3) 検証結果

(i)　真正性については、印刷された交付文書から得られる結果をもとに一意を特定する比較対象データとの一致を確認した。また、このとき一意を特定した識別情報として画面表示される証明書名、文書ＩＤ、氏名、日付情報と交付文書の記述を目視で比較することにより、偽造や改竄などの不正行為がないことを確認した。

(ii) 次に正常に真正が確認できた交付文書をコピー機で複製し、複製した文書について同様な検証を行った。複製物の場合は、エラーとなり真正を証明することはできなかった。

4.4.10 世代耐性の検証

(1) 評価基準

印刷された交付文書を複写することにより、複写牽制機能を施した隠し文字の画像フォーマットが２世代に渡り出力確保されることにした。

(2) 評価方法

世代耐性の評価環境を図 4-24に示す。

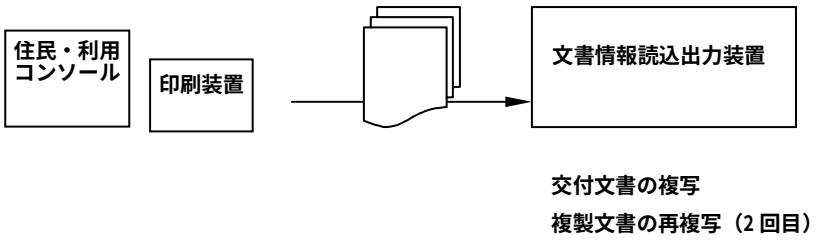


図 4-24 世代耐性の評価環境

交付文書を複写した際、牽制画像フォーマットに埋め込まれた隠し文字が浮かび上がることを確認する。また、一度複写した複製文書を、再度複写することで 2 世代目の複製文書にも隠し文字が浮かび上がることを確認する。

実施手順について以下に示す。

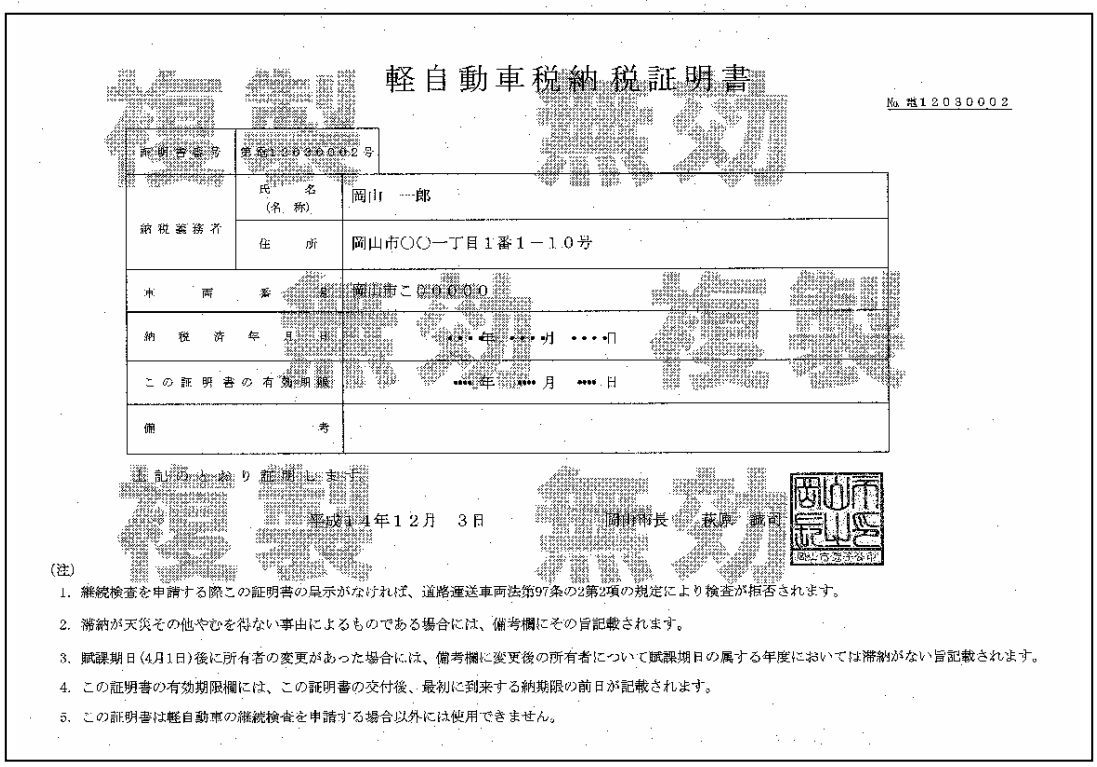
①印刷された交付文書を文書情報読込出力装置で複写する。
②牽制画像フォーマットに埋め込まれた隠し文字が、複写された複製文書に浮き上がっていることを確認する。
③一度、複写された複製文書を再度文書情報読込出力装置で複写する。
④再度、牽制画像フォーマットに埋め込まれた隠し文字が、複製文書に浮き上がっていることを確認する。

(3) 評価結果

世代耐性については、交付文書を複写（コピー）したとき牽制画像フォーマットに埋め込まれた隠し文字が浮かび上がることを確認した。

また、一度複写した複製文書を再度複写することで 2 世代目の複製文書にも隠し文字が浮かび上がることを確認した。図 4-25に交付文書の複写サンプルを示す。

しかしながら、複写機の機種などや濃度によっては隠し文字が明確に浮かび上がらないこともあったが、これはプレ印刷された牽制専用用紙においても同様の課題があることが分かった。



軽自動車税納税証明書

No. 地12030002

証明書番号	第No.12030002号	
納税義務者	氏名（名称）	岡山 一郎
	住所	岡山市〇〇一丁目１番１－１０号
車両番号		岡山市こ00-00
納税済年月日		****年 ***月 ***日
この証明書の有効期限		****年 ****月 ****日
備考		

上記のとおり証明します。

平成14年12月 3日　　岡山市長 萩原 誠司

（注）
1. 継続検査を申請する際この証明書の呈示がなければ、道路運送車両法第97条の2第2項の規定により検査が拒否されます。
2. 滞納が天災その他やむを得ない事由によるものである場合には、備考欄にその旨記載されます。
3. 賦課期日（4月1日）後に所有者の変更があった場合には、備考欄に変更後の所有者について賦課期日の属する年度においては滞納がない旨記載されます。
4. この証明書の有効期限欄には、この証明書の交付後、最初に到来する納期限の前日が記載されます。
5. この証明書は軽自動車の継続検査を申請する場合以外には使用できません。

図 4-25　交付文書の複写サンプル

4.4.11 まとめ

(1) 真正証明技術の信頼性については、交付文書の公印に対する識別情報のエンコード耐性、デコード耐性とその結果から得られる真正性を検証した。

(2) 同時に、複写行為を視覚的に牽制するための画像フォーマットの世代耐性についても検証を行った。

(3) エンコード耐性については、特にエラーなどの問題を確認することなく概ね高い成功率を確保することができた。

(4) デコード耐性についてはエラー数こそ 1 回認められたが、実行総数が低調であったため評価基準の 90%以上を確保することができなかった。

(5) 真正性については高い確率で識別情報の一致が認められ、複製物では真正の確認ができなかった。レスポンスについては今後の検討が必要な結果となった。

(6) 世代耐性については、概ね良好な結果となったが複写機の機種や複写濃度などに依存することが分かった。

(7) これらの結果から、今回考案した家庭のプリンタに印刷する交付システムにおいて、印刷物の真正の証明が十分に可能であり、複製を検出可能であることが確認できた。

4.4.12 課題

(1) 解析処理の信頼性

情報読取、解析精度（デコード率）を改善する必要がある。公印画像の特徴量抽出方法に関する訂正及び追加機能について検討が必要がある。

(2) 真正証明モデル

交付文書の真正強化、識別情報に対するセキュリティ対策強化が必要である。真正及びセキュリティ対策強化に関する訂正及び追加機能について検討する必要がある。

(3) 牽制画像フォーマットの隠し文字

複写機の機種や濃度などによっては隠し文字が浮かび上がらないことがある。対応案として、実証実験の取扱いとして『この証明書はカラー印刷で、すかし等の「複写偽造防止」処理を施してあります』を交付文書に表示したが、根本的解決が必要である。

(4) インターネットを利用した真正確認

真正の確認をセンタに問い合わせるのではなく、利用者がどこからでも容易に検証できる方法の検討が必要がある。

4.5 映像対話型電子申請・交付システムによる業務の効率化

4.5.1 背景

市役所などの多くの地方行政機関において、業務の効率化と市民サービスの向上を目指し、申請・交付の電子化へ向けた取り組みを進めている。しかしながら、インターネットを通じて申請登録を行っている国や県などに比べて、多くの市役所等は申請書様式のダウンロードを提供しているにすぎない。これは、国や県などが「行政」や「企業」がその対象であるのに対して、「市民」という１個人が対象であり、形式審査だけでなく、十分な本人性と本人の意思とを確認しなければ受付できない、ということに起因している。また、証明書の交付については、郵送による受取といった施策しかなかった。

本実証実験では、映像対話を通して本人性の確認や意思確認を行い家庭にいながらにして申請ができる映像対話型の電子申請システムを実現し、MIG コードの埋め込みや牽制模様により偽造・複製を防止する電子交付システムにより自宅のプリンタから証明書を取り出すことを可能にした。

本実証実験で申請、交付が可能な手続きは次の 9 種類であり、岡山市では、これらを併せて年間 250,000 件の申請が行われている。

(1) 市県民税（所得・課税）証明書
(2) 所得証明書（児童手当用）
(3) 固定資産（評価・公課）証明書
(4) 納税証明書
(5) 軽自動車納税証明書（継続検査用）
(6) 身体障害者手帳の再交付
(7) 補装具交付・修理申請及び判定通知書の交付
(8) 障害証明書交付申請及び交付
(9) 老人医療受給者証再交付申請

4.5.2 目的

本実験では、映像対話型電子申請・交付サービスを試験運用することにより、本サービスが現在の業務に対する費用対効果を調査することにより、業務効率化の効果を考察することを目的とする。

4.5.3 実験環境

自宅モニタ用端末 100 台及び公民館用端末に１台ずつ、計 112 台のプリンタ

を設置した。また、231 人のモニタ全てに岡山市認証局電子証明書の取得をしていただいた。さらに実験用の見本証明書ではなく、本物の証明書を取得したい人には、地元の銀行のインターネットバンキングへの登録をしていただき、市役所への発行手数料の振り込みが行えるようにした。

4.5.4 方法

現行の窓口での受付業務と映像対話型電子申請・交付システムを利用して行った場合の申請、交付 1 件あたりにかかる諸費用を算出する。さらに、当該システムを導入することによる費用対効果を考察する。また、他申請・交付に関する考察も併せて行う。

4.5.5 結果

現行業務と映像対話型電子申請・交付とを比較する際に考慮する要件としては、環境を作り出す「固定費」部分と手続 1 件あたりで変動する「変動費」の部分とがある。「固定費」部分については、手続件数によって変動し、かつその数が多ければ 1 件あたりが軽微になることから、今回はその要件からははずすこととした。「変動費」部分における要件には、大きく「人件費」、と「牽制用紙代」とがある。（この他にも、インク代やカートリッジ等が必要であることが分かったが、1 件あたりの費用が余りに軽微であるので、省略する。）人件費は、一連の作業にかかわった時間によって増減する。牽制用紙代は映像対話型電子申請・交付にとって費用減の部分となる。

職員へのインタビューの結果、現行業務の申請交付 1 件あたりにかかる時間は、約 3 分ということが分かった。また、映像対話型電子申請・交付システムでの申請・交付には 30 分かかるという実験結果が出た（4.6.3で記述）。人件費については、岡山市の場合、職員給与は、年間平均で 736 万円（平成 13 年度）であることから、年間 2000 時間で除すと、1 時間あたりの人件費は、3,680 円となる。よって、申請・交付 1 件あたりにかかる人件費は、3 分間だと、184 円、30 分だと 1840 円ということになる。

映像対話型電子申請・交付システム導入により、人件費が 1 件あたり 1,656 円増加する結果となった。

牽制用紙は 1 枚あたり 10 円程度であるから、映像対話型電子申請・交付システム導入により、用紙代が 1 件あたり 10 円削減される結果となった。

以上から、映像対話型電子申請・交付システム導入により、1 件あたり 1,600 円程度のコスト高という結果となった。したがって、業務効率を単純に上げるためには、少なくとも 1 件あたりにかかる時間を 3 分程度で完結してしまわなければならないことが分かった。ここで、そのための工夫としては、

(1) 申請の登録までは市民が実施する。
(2) 映像対話は本人確認を行う手段として交付の直前のみ実施する。
(3) 本人確認ができたら職員側は交付文書を送信する。
(4) 交付（プリンタへの打ち出し）は市民側で行うこととする。

が考えられる。このように運用フローを合理化することで職員に要する時間を 3 分程度に圧縮できると思われる。

しかし一方で、映像対話型電子申請交付サービスを取り入れることによる効用は市役所業務の効率化よりは市民側でのメリットのほうがはるかに大きい。

(1) 市民と職員とのコミュニケーションの場がひろがること
(2) 市民側の利便性の向上
(3) 市民側の取得コスト の削減

である。

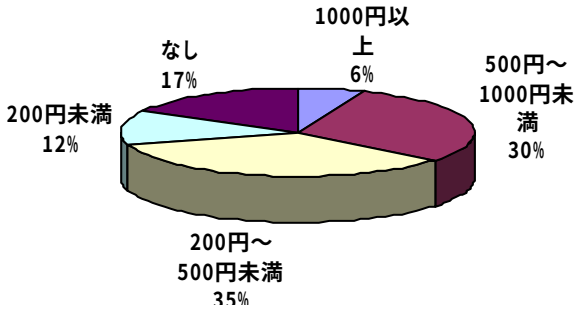


図 4-26 市役所までの交通費について

市民と市役所とのコミュニケーションの場が広がるというのは、市民アンケートによって、その 38%の人が、映像対話によって「親近感がわく」という回答をしていることから裏付けられている。利便性の向上については4.6で述べる。

市民コストについては、市役所窓口で申請・交付を行った場合に比べて、自宅で申請交付を行った場合に短縮できる時間についてのアンケートをとったところ、「かえって手間取った」という人はわずか３%であり、59%の人は、「往復１時間以上の短縮」という結果となった。この１時間短縮というのは、人件費換算（国民所得を平均勤労時間で除した場合）で 1,300 円相当にあたる数字である。

また、同様に、移動のための交通費についてアンケートをとったところ、平均で約 500 円が必要ということが分かった。このように。市民コストは映像対話型電子申請・交付システム導入により、大きく削減できることが分かった。

次に、今回対応していない、他の申請・交付の項目について考察してみる。アンケートの本実証実験に関する感想・意見欄の中に申請書の種類に関する意見がいくつか記入されている。

「住民票等がとれるようになれば利用も広がっていくと思う」（30 代男性）
「今回の申請書は必要のないものばかりであった」（60 代男性）
「業として代理受取の検討をして欲しい。本人受取でも必要な種類が少ない」（70 代男性、行政書士）

今回対象とした申請交付書類の岡山市での年間の申請件数（平成 12 年度岡山市取り扱い件数）は、

- **市県民税(所得・課税)証明書　111,585 件／年**
- **固定資産（評価・公課）証明書　71,243 件／年**
- **納税証明書　63,239 件／年**

市で取り扱っている他の申請・交付で多い順に列記すると、（平成 12 年度岡山市取扱い件数）

- **住民票の写し申請　400,000 件／年**
- **印鑑登録証明書　337,000 件／年**
- **戸籍抄本等の交付　148,000 件／年**

である。

4.5.6　まとめ

映像対話型電子申請・交付サービスを導入することで市役所業務の効率化に対する効果を考察した。

考察の結果、今回実験を行った運用方法では直接市役所業務の効率化には結びつきにくいという結論に至った。一方で、市民側のメリットが大きいことが分かった。

今後は、運用面を含めて市役所側の負担を低減するような工夫が課題である。また、アンケートから住民票、印鑑登録証明書、戸籍抄本等の交付といった、より市民に身近な申請交付を望む声があった。これらの申請に対応させるために各基幹システムとの連携、法律や条令の確認、本人確認の運用方法について検討する必要がある。

4.6 映像対話型電子申請・交付サービスの有効性

4.6.1 目的

本実験では、映像対話型電子申請・交付サービスが、従来の窓口での申請・交付サービスと同様又は、それ以上に利用しやすくなっているかどうかを検証することにより、その有効性を評価することを目的とする。

4.6.2 方法

(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。

(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。

4.6.3 結果

(1) 映像対話型電子申請交付サービスの利便性

アンケート回収方法やアンケート回答者の属性については、4.5と同じである。

Q．市役所の窓口で行う申請・交付サービスに対して、パソコンやプリンタを利用して自宅から申請や交付サービスがうけられる映像対話型電子申請交付サービスはいかがでしたか。

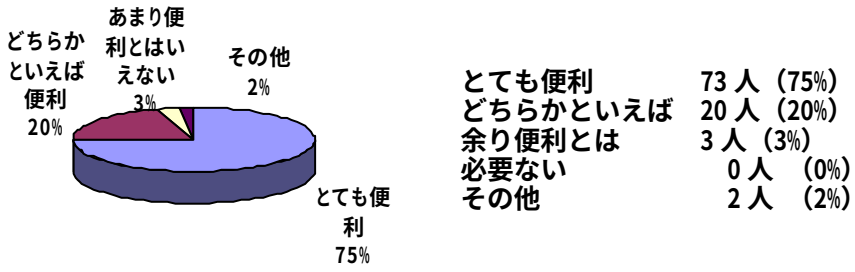


図 4-27 映像対話型電子申請について

「とても便利だった」と「どちらかといえば便利であった」との回答を合わせると、回答者全体の 95%の人が映像対話型の総合案内サービスに対して、便利なサービスだと感じたことが分かった。一方、「余り便利とはいえない」という回答が 3 人（5%）、「その他」という回答が 2 人（2%）あり、「必要ない」

という回答はなかった。年代別にみても全ての年代で、「とても便利だった」という回答が多数をしめた。

今回、電子申請交付サービスの実施に際し、十分な本人性の確認のため、いくつかのステップを踏まないと、サービスを受けられないような仕組みになっている。

①あらかじめ岡山市の認証局から発行された電子証明書を端末にインストールしておき、②その電子証明書のパスワードを投入しないと電子申請システムのページへアクセスできない、③電子申請システムのページにもログイン用のＩＤとパスワードを投入しなければならない。さらに、④市役所職員との映像対話でのやり取りの中でも、従来の窓口と同様に免許証などの本人を確認できるものをカメラの前での提示する運用にしている。

次のグラフはこのようなセキュリティ対策についてのアンケートの回答結果である。

Q．電子申請・交付サービスをうけるには、セキュリティと本人性の確認のため、あらかじめ、岡山市認証局が発行する電子証明書を取得（市役所窓口で申請し交付を受ける）し、端末にインストールをしていただきました。また、電子申請・交付サービスの実施時には、パスワードの投入が必要です。このことについていかが思われますか。

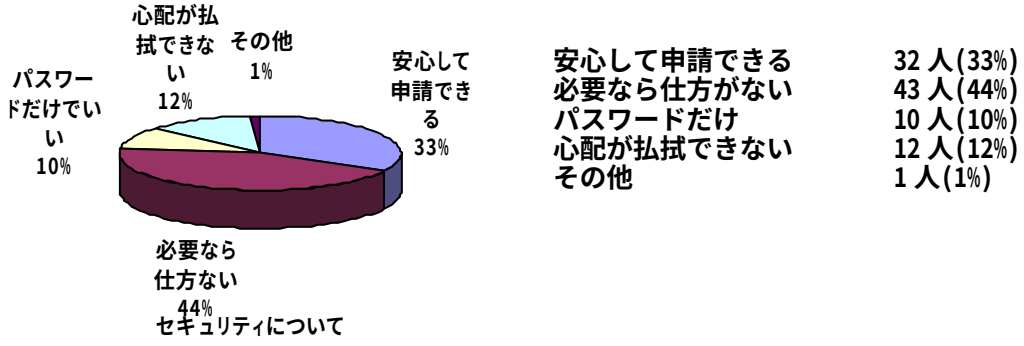


図 4-28 セキュリティについて

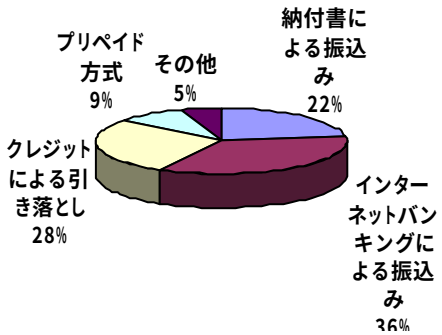
アンケートの結果、「必要ならば仕方がない」(44%)という回答が最も多かった。次に「安心して申請できる」(33%)が続いた。

さらに、これを年代ごとの割合で示したものが次のグラフである。これをみると、15～29 歳や 50 代の人に「必要なら仕方がない」と感じている人が多く、逆に「安心して申請できる」とした人が他の年代に比べて少なくなっている。また、「心配が払拭できない」という回答の割合が比較的に多かったの

は、15～29 歳や 30 代の若い年代であった。

次に、手数料の支払についてのアンケート結果を示す。市役所による証明書などの交付に際しては、発行手数料を市役所に支払う必要がある。本実証実験においても税に関する証明書の発行には、手数料が必要であり、今回は、この手数料の収納のために、地元の銀行が提供しているインターネットバンキングを利用した。こうした市役所への手数料の支払方法に関するアンケートの結果が次のグラフである。

Q．証明書の発行手数料に支払にはどんな方法がよいと思いますか。



納付（請求）書	22 人
インターネットバンキング	35 人
クレジット	27 人
プリペイド方式	9 人
その他	5 人

図 4-29 手数料の収納方法について

最も多かったのが「インターネットバンキングによる振り込み」（36%）で、次に「クレジットによる引き落とし」（28%）と続いた。また、「納付（請求書」による振り込み」（22%）を望まれる人も多かった。

年代別では、30 代の人に「クレジットでの引き落とし」の人気があり、逆に 60 歳以上の人は、極端に少なかった。また、50 代では「プリペイド方式」に人気があった。

(2) 映像対話型電子申請交付の利用特性

次のグラフは、実験開始（2 月 6 日）から 5 週間分のモニタから市民税課へアクセスされた日ごとのアクセス数の推移である。

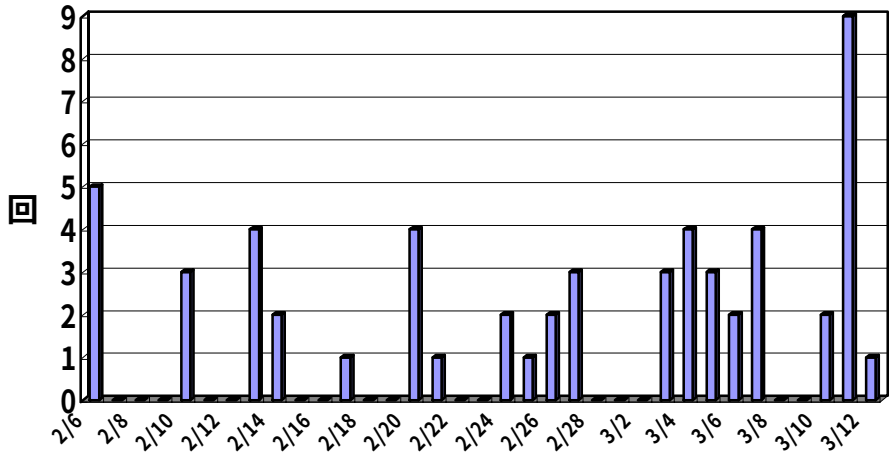
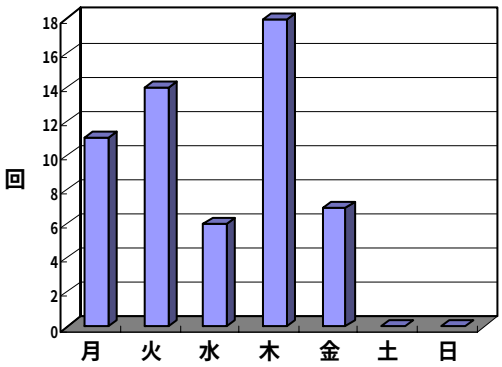


図 4-30 市民税課への日別アクセス数

全部で 56 回のアクセスがあり、うち 54 回対応している。第 1 週目が 8 回、第 2 週目が 7 回、第 3 週目が 10 回、第 4 週目が 12 回、第 5 週目が 17 回であり、徐々に増えている。

総合窓口案内を経由してつながったものが 22 回で、直接アクセスされたものが 32 回であった。

次のグラフは、実験開始から 5 週間分の市民税課への曜日別アクセス数の合計である。



月曜日　10 回
火曜日　14 回
水曜日　 6 回
木曜日　18 回
金曜日　 7 回

図 4-31 市民税課への曜日別アクセス数

最も多いのが木曜日で、水曜日が一番少なかった。ただし、日別のアクセス数を見ても分かるが、週によってその傾向は変わっており、必ずしも曜日によって特性があるとはいえない。

次のグラフは時間別にアクセスを見たものである。

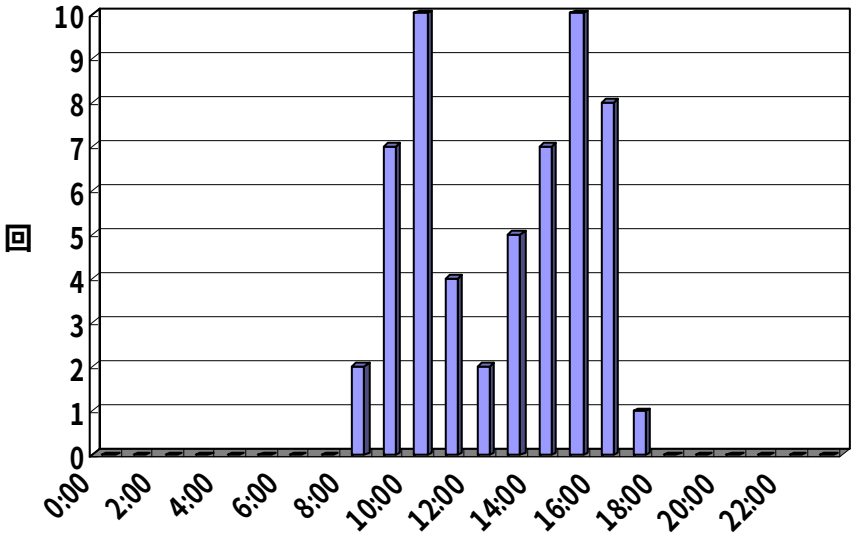


図 4-32 市民税課への時間別アクセス数

11：00 と 16：00 の 2 度ピークがあり、お昼の 12：00 台よりもむしろ 13：00 台がその谷になっている。

次に 1 回あたりの申請・交付に係る時間を示す。3 月分のデータのみ(26 回)を集計したものである。

以下の図は 26 件のアクセスを申請・交付時間の長さの短いものから順に並べたものである。

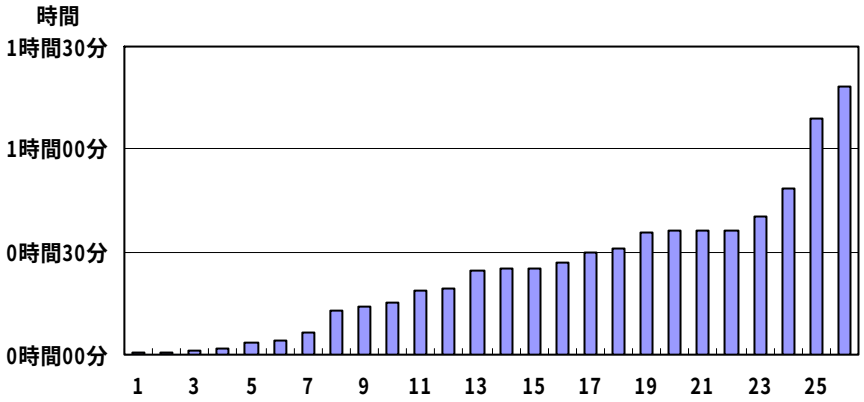


図 4-33 市民税課へのアクセス時間

申請から交付に係る時間は通常で約 15 分程度必要であるため、15 分以下のものについては、申請・交付を最後まで行っていないものと思われる。申請・交付にかかる時間は 30 分前後のものが多く、中には、1 時間を越えるものもあった。

4.6.4 まとめ

(1) 映像対話型電子申請・交付サービスの利便性

全体の約 9 割の人が便利だと感じており、映像対話型電子申請交付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。

手数料の支払い方法として最も人気が高かったのはインターネットバンキングサービスであるが、市民側にとって申請手続きから支払い手続に移る際の連続性がない。シームレスに支払い処理を行うことができる方法の考案が必要である。

(2) 映像対話型電子申請・交付サービスの利用特性

申請・交付サービスの利用は実験を開始してから徐々に増えている。

曜日では火曜日と木曜日のアクセスが多かったが必ずしも曜日に特性があると判断できない。11：00 と 16：00 の時間帯がピークとなる。逆に少ない時間帯は、13：00 であった。

申請・交付に係る時間は平均的には 30 分程度であった。

4.7 証明書等交付におけるセーフティネット

4.7.1　家庭での交付文書発行に係る脅威

交付サービスの実施においては、その様々な危険性に対して十分なセキュリティ対策を講じる必要がある。申請から交付文書の印刷に至るまでのプロセスにおいては、予測される様々な脅威やリスクに対して回避できることが望まれる。また、完全に回避できない場合においては、その回避方法についての考察を行う。さらに、他の申請・交付手続において脅威に対する影響について考察を併せて行うことにした。

遠隔のプリンタで交付文書を発行するフローは以下のようになる。

①利用者が交付文書ファイルをダウンロードする。
②ビューアで交付文書ファイルを開き印刷する。
③印刷された文書を交付文書とする。

交付文書ファイルが紙として出力されてしまえば、4.4で述べた真正証明技術によりその真正は証明が可能で複製防止の措置が講じられているが、その前段において以下のような脅威が考えられる。

(1) 他人が成りすまして交付文書ファイルをダウンロードする。
(2) ダウンロードしたファイルが改竄される。
(3) ダウンロードしたファイルが複製される。
(4) ダウンロードしたファイルが何度でも印刷される。
(5) 印刷が失敗して交付文書が無効となる。

遠隔での交付を実現するためには、これらの脅威に対する対策が施されていなければならない。

4.7.2　アクセスチケットシステムの概要

交付証明書の安全性を確保するために利用権発行サーバ、チケット発行センタにより構築されるアクセスチケットシステムを用いることにした。

アクセスチケットシステムは以下の特徴をもつ。

(1) 特定利用者への識別鍵取得機能
(2) 対象ファイルの暗号化機能
(3) 暗号化されたファイルの利用権（管理属性）の設定機能
(4) 特定利用者への利用権を許諾するチケット発行機能
(5) データの暗号化や処理は公開された標準的な公開鍵暗号アルゴリズム（RSA 暗号、DSA 署名、楕円曲線暗号、零知識証明など）

アクセスチケットシステムは、独自開発したデジタル情報の利用権制御技術により、文書ファイルなどの閲覧や印刷、編集、期間などを特定利用者ごとに利用条件を設定することが可能である。

こうした機能により、文書ファイルや動画コンテンツ、HTML などに対する不正コピーや偽造、改竄などの不正利用を不可能にするとともに、CD-R、FDD、MD などの記録メディアやネットワーク配信を安全に実現する基盤技術として極めて有効である。図 4-34にアクセスチケットのイメージを示す。

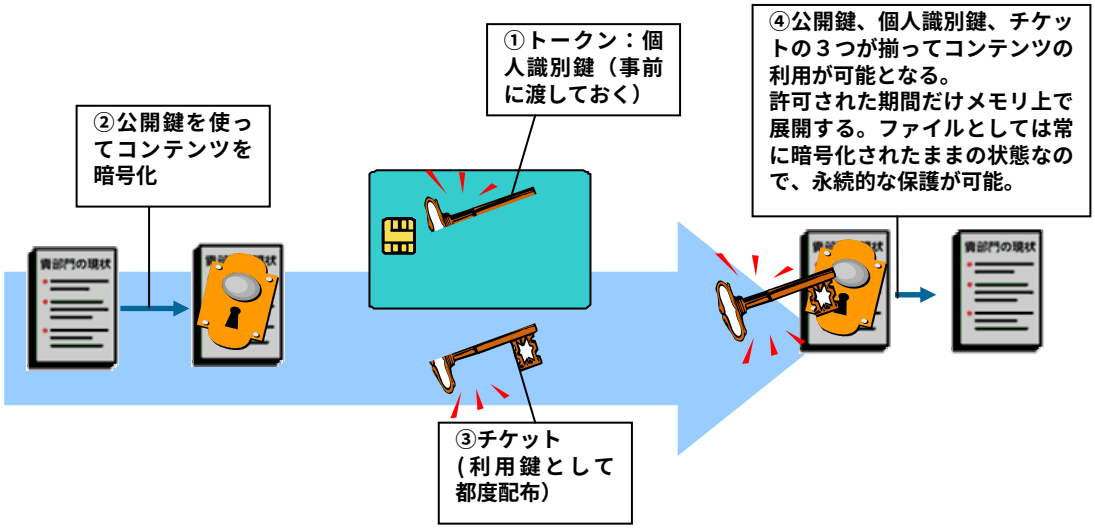


図 4-34 アクセスチケットのイメージ

ユーザーに対し、端末上若しくは IC カード上に個人識別用の鍵データ（トークン）を配布する。コンテンツは公開鍵で暗号化してあり、利用権（チケット）は、公開鍵とトークンに合わせて作られユーザに配布される。公開鍵はコンテンツごとに異なり、個人識別鍵はユーザーごとに異なるので、チケットは、特定のユーザーかつ特定のコンテンツだけの利用権になり、他への横流しや偽造はでき

ない。
また、コンテンツは利用できる期間だけメモリ上で展開され、生ファイルは生成されないため、永続的に保護される。

このようにチケットにコンテンツを復号する鍵だけでなく、コンテンツの利用者や利用時間、編集制限などを合わせて持たせることで柔軟で多様な利用権の発行を実現している。

今回、家庭で印刷された交付文書ファイルの安全性を確保するためにアクセスチケットを以下のように構成した。

(1) 交付文書ファイルに利用権の制御を加えた暗号化の処理を施す。
(2) 暗号化された交付文書ファイルを利用する為に必要なチケットを都度申請者本人に発行する。
(3) 発行されるチケットは、交付文書ファイルの閲覧及び印刷の利用権を各々1回ずつしか許諾しないことにする。
(4) チケットが発行されない状態においては、閲覧及び印刷ができない暗号化された状態とする。
(5) チケットは取得した申請者本人だけが使用でき、他の申請者等が交付文書ファイルを入手しても利用できないことにする。

アクセスチケットシステムをこのように構成することで先に述べた脅威に対し、以下の通り対処する。

(1) 成りすましによるダウンロード
ダウンロードはそもそも https や IPsec 通信の中で行われる。それゆえにセッション開始に先立って認証が行われ他人は成りすましてダウンロードすることができない。

(2) ダウンロードしたファイルの複製
ダウンロードしたファイルは複製が可能であるが、チケットがないとファイルを開くことができない。それゆえに複製しても内容が分からない。チケットを取得できたとしてもトークンがなければ同様に復号することができない。

(3) ダウンロードしたファイルの改竄
チケット、トークンが一致しないとファイル編集ができなくいため他人は

改竄はおろかファイルを閲覧することさえできない。発行を受けた本人が改竄しようとしたとしてもチケットに利用権が明示されているのでその利用権を超える操作はできない。また、チケット自体の改竄はそれがファイルを復号する鍵という性質も併せて持っていることから極めて困難である。

(4) ダウンロードしたファイルの多数の印刷

上記と同様にチケットにより制限されているため印刷できない。

(5) 印刷が失敗して交付文書が無効となる。

プリンタの障害や不慮の停電等により印刷の失敗が発生しうる。そのため、交付文書の印刷は窓口職員が遠隔で実施することとし、職員は必ず印刷された証明書を映像対話で確認することとした。

4.7.3 システム構成

本システムでは、交付文書ファイルの取得から印刷に至るまでのプロセスにおけるセキュリティ対策として、暗号化された交付文書が利用権を許諾するチケットを取得できる申請者本人によってのみ、閲覧、印刷などの利用を可能とするシステムを構築した。

これによりネットワーク上の安全性を確保するとともに、交付される証明書の覧及び印刷時の安全をも確保する制御を行った。

(1) 利用権発行サーバ

利用権発行サーバにおいては、セキュリティ埋込み機能によって作成された交付文書ファイルに対する暗号機能とともに、閲覧や印刷などの利用権の設定機能を提供した。

(2) チケット発行センタ

チケット発行センタにおいては、暗号化された交付文書ファイルの利用権を許諾するチケットを、特定の申請者本人に対して都度発行する機能を提供した。

本システムが対象とするオペレーティングシステム名及び各アプリケーションのバージョンを表 4-15に示す。

表 4-15 オペレーティングシステム名及び各アプリケーションのバージョン

カテゴリ	ソフトウエア	バージョン
サーバ OS	Windows2000 Server	V5.0　SP2 以上
クライアント OS	Windows　XP	V2002 以上
文書フォーマット	DocuWorks	V5.0 以上
公印画像埋込	MIG（Micro Gradation）	VOkayama1.0
リポジトリ管理	DocuShare	V2.3J for Win BASIC
印刷履歴	DocuHouse for LAN	V1.5 以上
スキャンデータ転送	CentreWare Scan Service	R4.7 以上
利用権発行	ATS Enterprise Center	V2.1
	ATS Server Toolkit	V2.1
暗号化	ATS DocuWorks EnCapsulator	V2.1
利用権認証	ATS Client	V2.1
	ATS DocuWors Plug-in	V2.1

ATS：アクセスチケットシステム

4.7.4　検証内容

交付文書におけるセーフティネットの調査、検証を行う。評価環境を図 4-35 に示す。交付文書ファイルに対する利用権制御を加えた暗号化を可能にするシステムを構築し、交付文書ファイルに対する成りすましや盗聴、改竄などの擬似的な不正行為を行う。

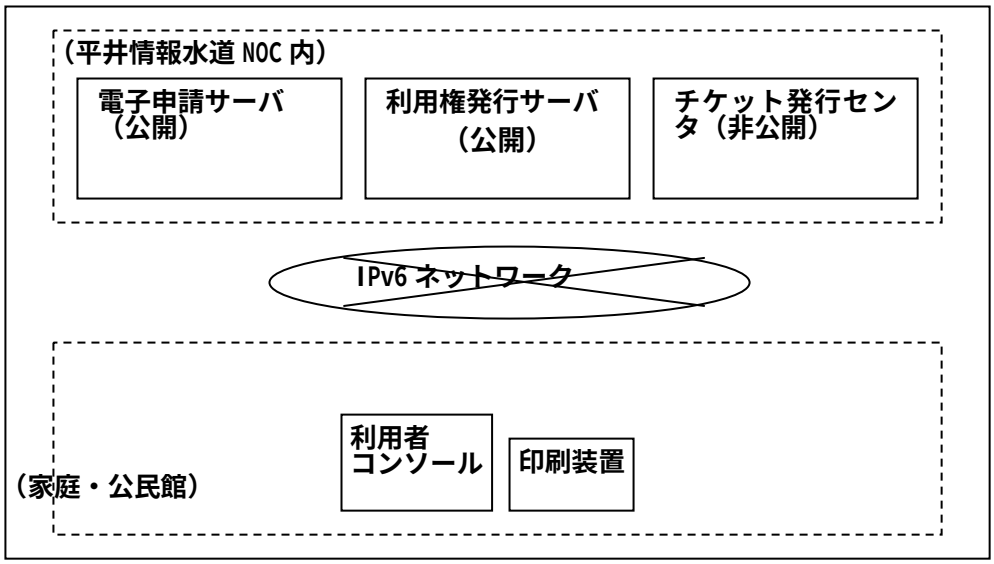


図 4-35 評価環境

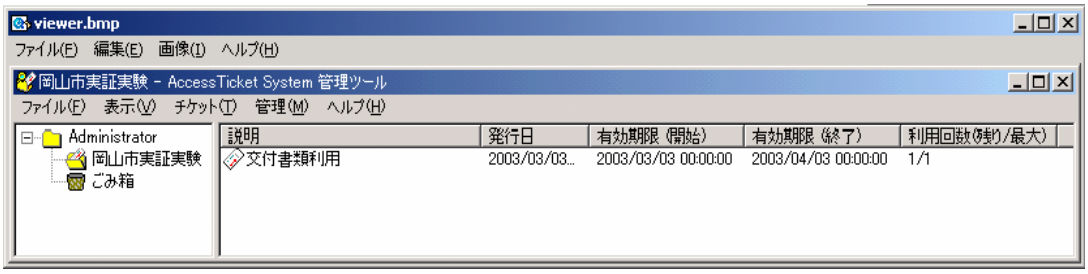


図 4-36 チケット管理ツール画面サンプル

検証項目を以下に示す。

①アクセスチケットシステムの基本機能

・暗号化機能の確認

・チケット適正発行の確認

②複製防止の検証

③改竄・多数の印刷防止の検証

4.7.5 基本機能の検証

(1) 暗号化機能の確認

(i) 評価基準

交付文書ファイルの取得時において、暗号化によって安全に交付され、暗号化された交付文書ファイルは盗聴、改竄などが行われにくいこと。

(ii) 評価方法

利用権発行サーバからの交付文書ファイルの取得に際して、交付文書ファイルが間違いなく暗号化されていることを確認する。また、チケット取得前にはいずれの機能も利用ができないことを確認する。

①実施手順は以下のとおり。

②交付画面から交付文書ファイルをダウンロードする。

③ダウンロードした交付文書ファイルを利用する為に必要なチケットの発行を中止する。

④交付文書ファイルを利用するために必要なチケットが取得されていない状況で閲覧などを実行する。

(iii) 評価結果

利用権を許諾するチケットが発行されていない状態では、暗号化された交付文書ファイルの閲覧や印刷などの利用が全くできないことを確認した。

(2) チケットの適正発行の確認

(i)　評価基準

交付文書ファイルの交付において、申請者本人に対する適正なチケットが発行さることとした。

(ii) 評価方法

申請者が暗号化された交付文書ファイルを取得した際、利用権を許諾するために必要なチケットが、申請者本人に対して正常に発行されていることを確認する。実施手順は以下の通りとする。

①交付画面から交付文書ファイルをダウンロードする。
②ダウンロードされた交付文書ファイルを利用する為に必要なチケットを取得する。
③チケット管理ツールを利用して、チケットが特定の申請者本人に対して正常に発行されていることを確認する。

(iii) 評価結果

交付文書ファイルの利用権を許諾するチケットが、申請者本人に対して正常に発行されていることを確認した。

4.7.6　複製防止の検証

(1) 実験内容

申請者本人が安全に利用することを可能にするとともに、申請者本人以外の第三者によって複製されたファイルが無意味であることを確認する。

(2) 評価方法

暗号化された交付文書ファイルを申請者本人以外の第三者に受け渡した際、その交付文書ファイルの利用ができないこと確認する。

実施手順は以下の通りである。

①交付画面から交付文書ファイルをダウンロードする。
②ダウンロードされた交付文書ファイルを利用する為に必要なチケットを取得する。
③ダウンロードされた交付文書ファイルが、申請者本人に許諾された閲覧や印刷が可能な状態にあることを確認する。
④この交付文書ファイルを申請者以外の第三者に受渡し、閲覧や印刷

などを実行する。

(3) 評価結果

暗号化された交付文書ファイルを本人が開いた時点でチケットが消費され、申請者以外の第三者に受け渡した際、その交付文書ファイルが全く利用できないため盗聴、改竄ができないことを確認した。

4.7.7 改竄・多数の印刷防止の検証

(1) 評価基準

暗号化された交付文書ファイルが、チケットによって許諾された閲覧や印刷以外の利用が不可能な状態であることとした。

(2) 評価方法

暗号化された交付文書ファイルが、取得したチケットによって許諾された閲覧及び印刷を各々１回ずつしか利用できないこと、また 2 回目以降はすべての利用が行えないことを確認する。実施手順は以下の通りとした。

①交付画面から交付文書ファイルをダウンロードする。

②ダウンロードされた交付文書ファイルを利用する為に必要なチケットを取得する。

③申請者本人にのみ許諾された交付文書ファイルの利用条件である閲覧、印刷が各々1 回ずつ実行する。

④同じ交付文書ファイルに対して、再度閲覧、印刷を実行する。

(3) 評価結果

暗号化された交付文書ファイルが、申請者本人へのチケットの発行によって許諾された閲覧、印刷（各々1 回づつ）以外の利用が不可能であることを確認した。

4.7.8 まとめ

セーフティネットについては、交付文書ファイルの取得から印刷に至るまでに予測される成りすまし、盗聴、改竄などの不正利用を防止するためのセキュリティ対策について考察を行った。

(1) 交付文書ファイルに対する利用権の制御を加えたカプセル（暗号）機能により、取得から閲覧、印刷に至るまでのプロセスにおいてはいずれの不正利用も行えないことを確認することができた。

(2) また、カプセル（暗号）化によって設定された交付文書ファイルの利用条件が適正に機能していることを確認することができた。

(3) これらの結果から、交付文書の印刷において取得、閲覧、印刷時に不正な複製を行うことができず、交付文書として十分利用できることを確認した。

4.7.9 課題

本実証実験の評価、検証を基に課題について述べる。

(1) 交付文書の印刷環境に関する課題

今回は特定のプリンタにおいての利用に限定したが、今後対応プリンタのメーカ、機種拡充、公的施設利用による印刷環境の整備が必要である。また、交付文書の印刷技術の標準化や、利用者の利便性を考慮したプリント環境整備に関する検討が必要である。

(2) 解析機能の汎用性

交付文書の汎用的な真正証明（解析）環境の整備が必要であり、セキュリティや通信回線環境を充分に考慮しつつ汎用的な解析環境の整備に関する検討が必要である。