デジタル・ドキュメント 17－4
（1999. 3. 12）

公共システムにおける権限認証局

山本強(1) 樋口洋一(2) 橘信行(2) 嶺典史(3)
岩佐博(4) 久村敏雄(5)

公共性の高い行政システムが，一般的に使われているインターネット技術を基に再構築さるのは，時代の流れであり，今後増加するものと考えられる。インターネット技術を用いた行政イントラネットでは，内容開示に伴う情報の公開性とともに市民および企業・団体等のプライベート情報の機密性が併せて要求される。これら一見矛盾した情報コントロールを実現するため，利用者の本人確認に加え，各々の行政アプリケーションについて，その本人のアクセス権限の有無を判断する必要がある。

本報告は，「行政の電子化における権限認証モデル」を提案し，通信・放送機構が実施する「北海道札幌市マルチメディア・モデル市役所展開事業」における「見積もり合わせ実験」でその有効性を検証したので報告する。

A model of authority authentication for electronic administrative system

Tsuyoshi Yamamoto, Yohichi Higuchi, Nobuyuki Tachibana, Norifumi Mine
Hiroshi Iwasa, Toshio Kumura

It is a general trend for administrative information systems to be reconstructed using generic internet technologies. In administrative intranet system using internet technology, openness as public information system and security control for private information of individual citizen or corporate are required at the same time. To realize these opposite demands, it is necessary for administrative application to authenticate not only user's personal identification but also access level control of each users.

In this paper, we propose a model of authority authentication for electronic administrative system. The model was implemented and applied to "estimate matching experiment" in "Multimedia Model Municipal Office at Sapporo City" sponsored by Telecommunications Advancement Organization of Japan(TAO).

（1） 北海道大学，通信・放送機構 委託研究員
（2） 札幌総合情報センター（株），通信・放送機構
（3） 札幌総合情報センター（株）
（4） 通信・放送機構 共同研究者
（5） 通信・放送機構 共同研究者

1. まえがき

行政システムには，その公共性の高さから相反する二つの側面が要求される。つまり公開性と機密性である。その公開性という性格から，今後のシステムは，インターネット技術を基に再構築されるのが時代の流れであり，今後増加するものと考えられる。同様に，機密性の要求も，インターネット技術を採用した機密保護を必要とすることが多くなると思われる。

しかし，これまでのインターネット技術の発展は，個人対個人（電子メール），個人対サーバー（World Wide Web）という具合に，おもに個人を対象とした形で展開している。公開鍵証明書インフラストラクチャ（Public Key Infrastructure，以下 PKI と略す）技術に代表されるインターネットのセキュリティー技術も個人を念頭に展開し応用されており，組織的運用に代表される機密の共有，権限の動的な変更等に十分に対応したものとは言えない。

本報告では，行政アプリケーションの特徴について考察し，アクセス権限および暗号化を組織の立場から管理可能な技術要求と捉え，公共システムに適した権限認証方式を考案し，「行政の電子化における権限認証モデル」として提案する。更に，これを導入することにより，本人認証情報を変更することなく，権限を臨機に付与および削除することが可能になったことを，実験アプリケーションである区役所での「見積もり合わせ業務」[1]を通して検証したので報告する。

2. 認証技術

コンピュータシステムのセキュリティの基本的な要件としては，下記の項目があげられる[2]。

- ユーザーの認証
- アクセス制御
- 同一性
- 機密性

通信を行う両端においては，データの漏洩がなく，データが破壊・改竄されることがなく，そのデータが送り出されたことと相手に届いたことを確認できる必要がある。これらを満たすための要件には，「ユーザを識別してその正当性を判定する機能（認証）」と，「ユーザがアクセスしようとするデータやサービスに対する許可があるかどうかを判定する機能（アクセス制御）」が少なくとも必要となる。一般にセキュリティ技術のなかでは，認証が全ての基本にあり，認証が可能であって始めて，その人宛ての暗号化が可能になる。

2.1. 従来の認証方式

一般に，人を特定する方法としては，次の３つの要素があげられる[2]。

① What you know(記憶情報)
ユーザーＩＤ，パスワード等に代表される個人が記憶した機密情報による認証。

② What you have(所持情報)
鍵，クレジット・カード，ＩＣカード等に代表される所持情報による認証。

③ What you are(身体情報)
指紋，網膜，声紋などに代表される個人特有の身体情報による認証。

これら三つの要素を① ② ③と進むに従って固有情報の複製が困難になり，これらを複合して用いる事により，セキュリティの強度を上げることができる。

2.1.1. パスワード照合による認証

コンピュータ・システムにおいてユーザを認証する手段としてもっとも広く用いられているのは，ユーザＩＤとパスワードによる照合である。この方法は，記憶情報の固有性に基づくもので記憶情報の管理を確実に行なえば，これほど簡易かつ柔軟性に富む方法もない。しかし，当然ながら固有情報の漏洩は，常に問題になる。また，この方法のみで認証を行なう場合は，ユーザの入力したユーザＩＤとパスワードがネットワーク上を流れ漏洩の要因になるという問題も見逃すわけにはいかない[2]。

2.1.2. 公開鍵暗号方式による認証

現在インターネットのセキュリティ機能として広く使用されている方式で，ユーザ認証とデータの暗号化の機能を合わせ持っている。この方式は，ＩＣカード等に秘密鍵を入れることにより前記②の所持情報の固有性に基づくもので，自分しか持っていない秘密鍵を所持することを証明することで認証を行なう。この認証方式の特徴は，固有の所持情報である秘密鍵をどこにも知らせることなく（漏洩せず）この情報（秘密鍵）を所有していることを証明できる点にある。パスワード方式と違い本人を証明する相手方と固有情報を共有する必要がない。従って，認証手段としては，非常に強固であることが期待でき，インターネットの主要な認証技術である。

2.2. 公開鍵認証方式の一般的特徴

認証技術のセキュリティ上の強固性ゆえに，行政システムにおける認証方式においても，公開鍵暗号方式に基づく認証方式が中心になると考えられる。そこで，公共システムに適用した場合の課題点を検証するため，公開鍵暗合方式の他の側面について概観する[3]。

① 秘密鍵は，アイデンティティと同一視され，個人を証明するものとして扱われる。（鍵の貸し借りを認めない）

② この認証の方式を採用するためには，暗号鍵と，「公開鍵証明書」の他に，この「公開鍵証明書」に根拠を与える中立・公正な第三者機関である認証局が必要である。

③ 秘密鍵は，その鍵の保管と本人を結び付ける関連付けが必要である。

④ 現在のX.509 V3「公開鍵証明書」[4]では，証明書内の情報の選択的開示を認めない。

3. 行政の電子化における認証の課題

インターネットセキュリティ技術を行政システムに適用した場合に，いかなる課題があるのかを検討整理するため，行政システムの一例として「見積もり合わせシステム」を概観し整理する。

3.1. 見積もり合わせシステム

見積もり合わせ業務の流れは，おおよそ以下の通りである。

① 市側：見積もり要項を公開
- 市もしくは区の担当職員は，発注のタイミングで見積もり品目の要項を入力して指名通知を行なう。
- 指名業者に対して見積もり要項を公開する。

② 業者：見積もりデータの入力・提出
- 業者は，見積もりデータを入力し，確認メッセージ（受領書）の応答を受け取る。
- 業者からの見積もりデータの入力に際しては，デジタル署名を行なう。
- 公募期間終了後は，業者からの見積もり提出を不可とする。

③ 市側：見積もりデータの受付
- 入力されたデータは，センターの見積もりデータベースに公募期間中保管される。但し一度入力したデータへの照会および変更は不可とする。
- 公募期間中は，送付された見積もりデータへの市・区の職員のアクセスを不可とする。
- 締め切り日時の変更は，不可とする。
- 公募期間終了後は，業者からの見積もり提出を不可とする。

④ 市側：見積もりデータの開札・業者決定
- 公募期間終了後，市・区の担当職員は，見積もりデータを開札し，落札業者を選定し，２次伺い承認を受ける。
- 承認権限者は，承認・非承認を担当職員に通知し，落札業者を決定する。

⑤ 市側：決定・発注通知
- 業者決定後，落札業者に対して見積もり品の発注通知を行なう。

⑥ 業者側：受注確認
- 発注通知の受注確認を行なう。

3.2. 一般的インターネットとの違い

２章で確認したインターネットのセキュリティ技術を行政システムの一つである見積もり合わせに適用してみると次のことが分かる。

ユーザーの本人認証のための仕組みとしては，特に課題はない。しかし，一般にインターネットが対象とするアプリケーションは，電子メールに代表されるように個人対個人のものである。それに対し，前述の様な行政アプリケーションは，法人・組織・グループ・業務がその主体であり，個人はそれを担当する者，もしくは代表する者でしかない。これに対して，PKI 技術は，これを特に考慮した作りになっているとは言えない。

従って，この法人・組織・グループ・業務をどう扱うか，また監査等をどう扱うかが課題となると考えられる[5]。

この課題を見積もり合わせシステムに対して考察した結果を示す。

1）市側：見積もり要項の公開に際して，デジタル署名によって内容を証明する必要があり，担当者本人の秘密鍵による署名と組織の署名の両方でされるべきである。

2）業者からの見積もり送付に際しては，市側の公開鍵による暗号化を行なう必要がある。この際の暗号化は市担当者宛てなのか，見積もり合わせを受け付ける組織宛てなのかが問題となる。実際には，組織移動等を考慮して市担当者宛てではなく組織宛てとなる。これは，業務単位（権限単位）に秘密鍵が必要であることを意味する。

3）市側：見積もりデータの開札にあたっては，担当者といえども開札時刻まで見ることができない仕組みが必要となる。これは，担当者がある時刻までは秘密鍵を所持できないことを意味する。逆にある時刻になればダイナミックに秘密鍵を手に入れられる仕組みが必要となる。

4）担当者の異動・緊急時の対応について：組織間・グループ間の業務では，秘密鍵の所有者が異動等によって組織を離れたり，ＩＣカードの紛失等で秘密鍵を失ってしまった場合を考慮し，その対応が必要となる。

3.3. 課題の整理

行政システムでは，一般のインターネットアプリケーションと違い，担当者個人の本人認証におけるセキュリティの他にグループ・組織・法人・業務単位を「秘密鍵を持つ存在」として認定し，これを併用して認証・暗号化・署名を行なう必要がある。また，このグループ・組織・法人・業務単位の「秘密鍵」は，ダイナミックに付与及び剥奪することが可能でなければならないことが分かった。

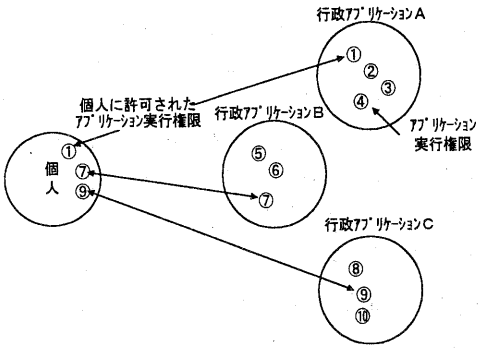

図1 個人とアプリケーション実行権限関係

すなわち，アプリケーション実行権限とは，「業務」を本人とみなした時の秘密鍵と認証書を手に入れることであると考えられる。さらに，将来に向けて行政システムは，市民に向けて開かれて行くと推定されることから，多くの個人（市民および職員）と多数の行政アプリケーションが認証の対象になると考えられる。これに伴い，個人と個人に許可された行政アプリケーションとの関係は，複雑に絡み合ったものになると考えられ，図1のように，多数の鍵を使い分ける要求が増えてくると思われる。

4. 行政の電子化における権限認証モデル

4.1. 権限チケット

第3章で述べたように，行政システムにおいてセキュリティを保つためには，個人の本人認証の他にアプリケーション実行権限として，業務の「秘密鍵」とその「認証書」が必要であった。

この2つを統合したものを，ここでは「アプリ

ケーション・チケット」もしくは「権限チケット」と呼ぶことにする。 この権限チケットは，個人を認証する場合の公開鍵暗合方式の「公開鍵と秘密鍵」と「証明書」とで構成されるのと同様に，「証明書と公開鍵」を含む X.509 フォーマットの証明書と「秘密鍵」との組み合わせで構成する。それにより図２に示すように，権限チケットが本人認証されかつ実行権限のある個人と紐付けることが可能となる。

この権限チケット技術をどのように安全に管理・配布・剥奪・無効化するかという議論で第３章で示した課題への解答が得られる。

4.2. 権限チケットの発行手順

業務の権限チケットが利用可能になるまでの手順の概略を，順を追って説明する。

① 行政アプリケーションの管理者は，業務をユーザーID として公開鍵暗号アルゴリズム用の鍵の対（秘密鍵と公開鍵）を作成する。

② 作成した鍵のうち，公開鍵のみを認証局に送付し，公開鍵証明書の発行を依頼する。

③ 認証局は，業務の公開鍵に業務の名前などの付加情報を加え，そして認証局の秘密鍵で電子署名を行う。

④ 認証局は，完成した公開鍵証明書を業務権限者に返送する。業務権限者は，鍵の対と受け取った証明書を手元の権限チケットとして必要なユーザー分を各ユーザーの公開鍵で暗号化してチケット管理サーバーへ格納する。

⑤ チケット管理サーバーは，自身のデータベースで権限チケットを管理し業務選択サービスを通して権限をもつユーザーにのみチケットを配布する。

4.3. 権限チケットと情報ライフタイム

権限チケットをどのように管理し，また配布するかは，様々な方法が考えられる。その尺度は，他のセキュリティ要件と同様に，要求される安全性（機密の強度）とコストの問題である。別の言葉で言いかえれば，ライフタイムの長い情報ほどコストをかけてもより安全に管理する必要がある。従って，ライフタイムの長く変更のない権限チケットについては，ＩＣカードに格納して配布することも考えられる。逆にライフタイムが短く，情報変更が頻繁な権限チケットの場合は，情報更新の度にＩＣカード再発行を行なうのは合理的とはいえない。特に情報変更の即時性が要求される場合は，殆どコストが見合わないことになる。そこでなんらかの権限チケットの発行・管理・配布・剥奪・無効化の手段が必要となる。

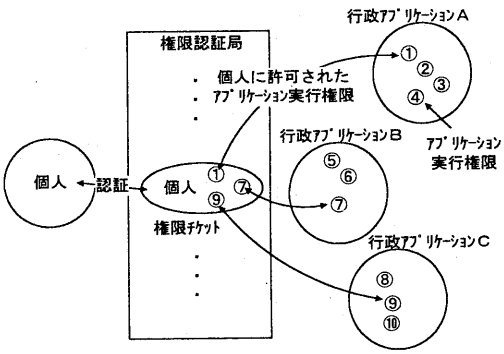

図２ 権限と個人の紐付け

4.4. チケット管理サーバー

「見積もり合わせシステム」においては，第２章の要件にもある様に，権限チケットをダイナミックに付与したり，剥奪する必要がある。つまり組織の構成員の異動による権限の付与と剥奪，業務を担当することによる権限の付与，開札業務の様に特定時刻になると初めて付与される権限の扱いが該当する。

本実験では，各個人と各行政アプリケーションとの関係を仲介して権限チケットを一括管理（管理・配布・剥奪・無効化）する権限認証局の考え方を採用した。 本見積もり合わせシステムでは，権限認証局をチケット管理サーバで実現し，アプリケーション実行権限を権限チケットで実現した。

これにより，個々人は，認証サーバにより本人認証されたうえで行政アプリケーションとの関係をチケット管理サーバで一括管理される。見積もり合わせシステムの認証関連を図３に示す。

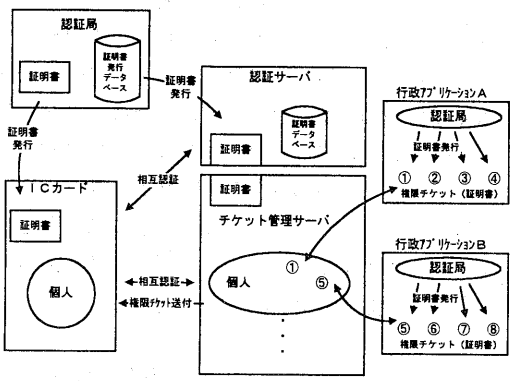

図３ 見積もり合わせシステムの認証関連図

4.5. 権限チケットの暗号化

チケット管理サーバが端末へ送付する権限チケットは，最も重要な機密情報の一つであり，強固なセキュリティを必要とする。

本見積もり合わせシステムでは，このセキュリティにデジタル封筒技術を用いた暗号化方式を採用している。この暗号化イメージを図４に示す。なお，暗号化はＲＳＡ公開鍵暗号化方式とＲＣ２共通鍵方式を用いた。

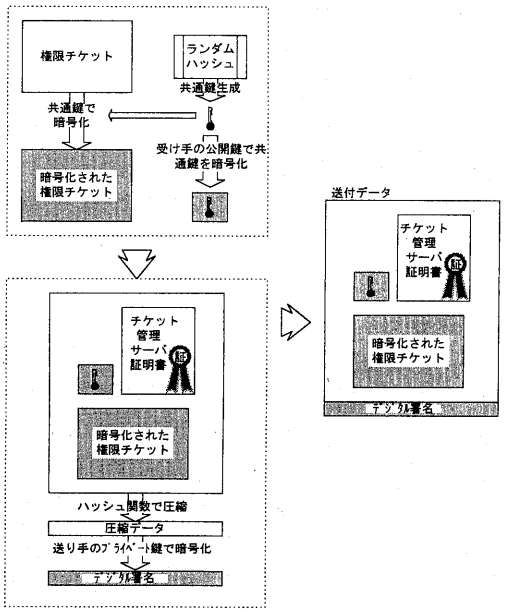

図４ 権限チケットの暗号化イメージ

4.6. 行政の電子化における権限認証モデル

行政システムの一つである「見積もり合わせシステム」で展開した権限認証の考え方は，下記に示す一般モデルで表現することができる。

ここで，「行政の電子化における権限認証モデル」を提案する。

１）前提

ユーザーＡの公開鍵：UserAPub

ユーザーＡの秘密鍵：UserAPri

共通鍵：s1，s2，s3

業務Ｂの権限チケット：Tb

権限チケットの中で

業務Ｂ用の公開鍵 ： ApBPub

業務Ｂ用の秘密鍵 ： ApBPri

送付先の業務Ｘ用の公開鍵： ApXPub

鍵Ｋでデータ Ｍを暗号化することを

Ｅ[K](M)

鍵Ｋでデータ Ｎを復号化することを

Ｄ[K](N)

とする。

２）権限チケットの保管

ユーザーＡが業務Ｂを行なう権限があればチケット管理サーバーに業務Ｂ用のチケットＴｂが

Ｅ[s1](Tb) ＋ Ｅ[UserAPub](s1)

の形で保管されている。

かつ，チケット管理サーバーは，独自の形式で（今回の実験ではＲＤＢの表形式）各ユーザーが各業務の実行権限があるかどうかを管理し，権限の有効時間の管理も行なっている。

３）権限チケットの要求

チケット管理サーバーがユーザーＡから業務Ｂの権限チケットの要求があった場合。チケット管理サーバーはユーザーＡ用の業務Ｂのチケットを保管していて，かつ他の有効要件を満たす場合はチケットを送付する。

他の有効要件とは，見積もり合わせシステムで言うところの「すでに開札時刻を経過してい

る」等の条件である。もちろん，この際のユーザーAとチケット管理サーバーは，個人の本人認証を行なう。

4）権限チケットの復号化

権限チケットは，ユーザーAが受信した後，ユーザA所持の秘密鍵で以下の様に復号化される。

D[UserAPri](s1)

D[s1](Tb)

これにより，ユーザーAは権限チケットの中の

業務B用の公開鍵 ： ApBPub

業務B用の秘密鍵 ： ApBPri

を入手できたことになる。

5）業務Bデータの復号化

この業務Bが開札業務だとした場合，見積もり合わせデータMは，業者によって業務B用の公開鍵を使用して暗号化されている。(公開鍵ApBPubは，すでに公開されている)

その様な業務BデータMの復号化は，

D[ApBPri](s2)

D[s2](M)

となる。

6）業務Bデータの署名の確認

手に入れたデータが信頼できるものかどうかは，データMの２つのデジタル署名で確認できる。すなわち，業務権限者としての署名と本人個人の署名である。

7）デジタル署名の添付

ユーザーA が業務 B においてデジタル署名を添付する場合は

業務B用の秘密鍵 ： ApBPri

ユーザーAの秘密鍵：UserAPri

の２つの署名を添付することになる。(UserAPriの署名を添付したデータを ApBPri で署名する)

こうすることによって個人の責任を明らかにすることができる。

8）送付データの暗号化

最後に送付データの暗号化であるが，これは，公開されている業務・グループ等の公開鍵ApXPubを使用し暗号化することになる。

E[s3](Data)

E[ApXPub](s3)

と言う結果になる。

5. 見積もり合わせシステムの実際

前述の権限チケットの機能を見積り合わせシステムに適用した場合の取引書類のセキュリティについて説明する。 対象となる書類は，大きく分けて①指名通知書②見積書③第２次伺書④決定・発注通知書があり，各々の書類はデジタル署名により本人署名され，内容の改竄を防止している。 見積り合わせ書類の暗号化イメージを図５に示す。

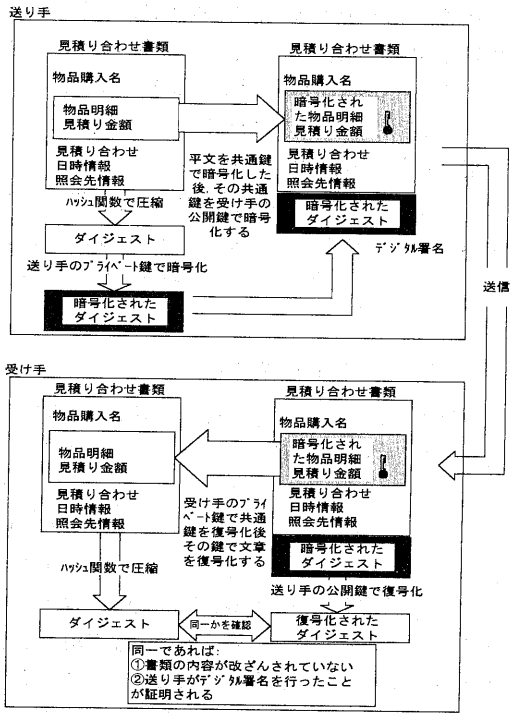

図５ 見積り合わせ書類の暗号化イメージ

また，物品明細及び見積り金額は共通鍵で部分暗号化された後，その鍵を受け手の公開鍵で更に暗号化され，暗号化された共通鍵と共に受け手へ送付される。これにより，この情報は受け手の秘密鍵でのみ平文に復号可能となる。よって，何者かがこのデータを入手できたとしても，物品明細及び見積り金額を読み取ることはできない。

また，このような部分暗号化のもう一つの目的

は，業者の投封状況などの管理情報をシステムが非暗号化データ部分から読取り，運用管理を可能にする事にある。また，取引書類のセキュリティで用いられる秘密鍵は，権限チケットに含まれるものを使用する。この権限チケットに含まれる秘密鍵は，組織上の権限鍵を意味しており，これを使用する事により担当者の人事移動等による書類の解読不可能な状況を回避した。また，権限チケットは，見積もり合わせの発注番号単位に別チケットとし見積もり合せ箱の管理を容易にした。

5.1. 緊急時の権限の付替え

見積もり合わせに限らず，担当者の何らかの事故等で権限の付替えが必要になる時がある。従来のシステムであれば，本人以外に暗号化されたデータを復号化することはできないのが基本であり，可能な場合もある程度の時間を要した。その点，今回の権限チケット機能を使用すると，業務上の権限付与者がチケット管理サーバーに要求を出すことによって，権限チケットを容易に付与することができた。

5.2. 監査及び鍵回復機能

業務用権限チケットを予め監査用及び鍵回復用のユーザーID で暗号化してチケットとしてチケット管理サーバーに登録しておくことによって可能である。このチケットは，鍵回復権限者や監査権限者といえどもチケット管理サーバーの配送許可がなければ使用できない点に意味があると考える。チケット管理サーバー自身は自分の秘密鍵ではチケットを復号化することが出来ないために，権限のチェックアンドバランスを取ることが可能になる。

5.3. 見積り合わせ箱密閉機能

見積合せ箱は，業者投封から区役所の開封までの期間において，業者及び区役所の双方から見積情報を密閉にする必要がある。今回は，チケット管理サーバーを公正機関[6]としたチケット配布制限機能により実現することができた。

6. むすび

インターネットのセキュリティ技術である本人認証の秘密鍵・公開鍵の他に，その応用として権限における秘密鍵・公開鍵（権限チケット）を導入することによりセキュリティを保ったまま行政システムの特徴であるグループでの作業が可能となった。特に，業務の担当者の異動・変更に対して柔軟に対応することが可能となった。この行政システムに適した権限認証モデルを「行政の電子化における権限認証モデル」として提案した。

今後は，多くの市民の利用を前提とするチケット管理の在り方(分散システム等)に研究課題が残される。また昨今，チケットなどを汎用的に管理するインターネット標準も（LDAP 等）実用化され始めている[7]。これらについても注目して行きたい。

参考文献

[1] 樋口, 橘, 山本, 山田, 岩佐, 久村:"平成９年度 北海道札幌市マルチメディア・モデル市役所展開事業 成果報告書", 通信・放送機構, 1998

[2] Larry J. Hughes, Jr., 長原 宏治 監訳: “インターネットセキュリティ”, インプレス, 1997

[3] Simson Garfinkle Gene Spafford: “Web セキュリティ&コマース”, 6 章, O' REILLY, 1998

[4] ITU-T Recommendation X.509(1997) | ISO/IEC 9594-8:1997, Information technology – Open Systems Interconnection – The Directory: Authentication framework

[5] 道明誠一, 梅木久志, 他: “商用目的に適した鍵回復システムの開発”, 情報処理学会第56回全国大会, 6F5, PP. 3-398 - 3-399, 1998

[6] 工藤道治: “インターネットにおける電子入札システム”, 情報処理学会第56回全国大会, 6F5, PP. 3-426 - 3-427, 1998

[7] Network Working Group: An Approach for Using LDAP as a Network Information Service, http://www.cis.ohio-state.edu/htbin/rfc/rfc2307.html, 1998