デジタル・ドキュメント 26－1
（２０００．１１．１７）

行政システムにおける権限認証局ツリーの構築

近藤 徹 （日本IBM）
久村 敏雄　松本 正憲 （NTT東日本）
中森 博 （日本IBM情報ｿﾘｭｰｼｮﾝ）
樋口 洋一　橘 信行 （札幌総合情報ｾﾝﾀｰ）
山本 強 （北海道大学）

インターネット技術に基づいて行政システムを構築するとき、インターネットの公開性故にプライバシーや機密性への配慮が強く求められる。このため考え出されたセキュリティ管理のシステムの中に、個人と行政アプリケーションの関係を一括管理するための権限認証局があるが、利用者数の大規模化にも対応して認証処理を可能とするための工夫が必要となってきている。その解法として、認証局の分散化を検討し、それを権限認証技術と時限認証技術との組み合せにより実現した。

本稿は、通信・放送機構(TAO)における「北海道札幌市マルチメディア・モデル展開事業」の「福祉ネットワーク・システム」において構築し実験を実施した、分散化された認証局モデル“権限認証局ツリー”について報告する。

Tree-structure of Authority Authentication for electronic administrative system

Tohru Kondoh (IBM Japan)
Toshio Kumura, Masanori Matsumoto (NTT East)
Hiroshi Nakamori (IBM Global Services Japan East Solutions)
Yohichi Higuchi, Nobuyuki Tachibana (Sapporo Information Network)
Tsuyoshi Yamamoto (Hokkaido University)

It is strongly requested to keep individual privacy and security in electronic administrative systems, which are constructed using generic internet technologies. Authority authentication was introduced for this purpose. It also plays the role to control the relation between individuals and administrative applications. Now it becomes necessary to consider how to support huge number of users. By establishing tree-structure of Authority authentication, we succeeded in dispersing the workload and finally in generating distributed system. This paper reports how we made the tree-structure in the project of “Multimedia Model Municipal Office at Sapporo City”, sponsored by Telecommunication Advancement Organization of Japan(TAO).

１．はじめに

インターネット技術の普及により、多くの企業でインターネット技術を用いた業務システムの再構築が行われている。公共システムにおいても、インターネット上で行政アプリケーションを構築する動きがある。しかし、インターネットの特徴である公開性のため、セキュリティへの配慮が強く求められる。この要求を満たすべく考え出されたセキュリティ管理のシステムの中にあって、個人と行政アプリケーションの関係を仲介して一括管

理するため、権限認証局が存在する。しかし、利用するユーザー（市民）の数が大規模化してくると、認証局へのアクセスの集中が問題となりうる。従って、円滑な行政サービスを実現するためには、セキュリティの強度を落とすこと無く認証局の分散化を実現することが求められる（大規模分散認証システム構築技術）。当実験では、権限認証局技術と、極めて短期間の有効期限を管理するための時限認証技術とを組合わせて、“権限認証局ツリー”を構築することにより実現した。

なお、本実験は、通信・放送機構(TAO)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「福祉ネットワーク・サービス」の「手話相談システム」において実施した。

2．セキュリティ管理システム

2－1．システム要件

今回提案する権限認証局ツリーは、インターネット技術に基づいて行政アプリケーション・システムを構築する場合、個人のプライバシーや情報の機密性などを保護・管理するために必要となるセキュリティ管理システムを構成するものである。このセキュリティ管理システムが有効に機能するためには、次の要件を満たすことが求められる。

① 強固なセキュリティ機能

多数の市民を対象とすることから、システム上個人のプライバシーや情報の機密性は安全に保護されなければならない。また、ウイルスによる汚染やハッカーによる故意の侵害についても、機密性について十分に堅固であることが求められる。

② 負荷の増加に対する拡張性

行政アプリケーションの増加、あるいは市民数の増加などによるシステム負荷の変動に対応できる拡張性を持つことが必要である。

2－2．権限認証局ツリー

膨大な数の市民と権限とを細かに管理でき、前述のシステム要件を満たすためのシステムとして、権限認証局ツリーを提案する。図2-2-1 に示すとおり、一次からｎ次までの階層からなる権限認証局をツリー状に配置し、それぞれを中心にしたサービス・エリアを展開する。市民は最寄りのサービス・エリア内のｎ次の権限認証局にて操作することにより、容易に円滑なサービスを受けることが出来る。なお、この権限認証局ツリーを実現するためには、権限認証局技術について多くの検討を加える必要がある。これらについて後述する。

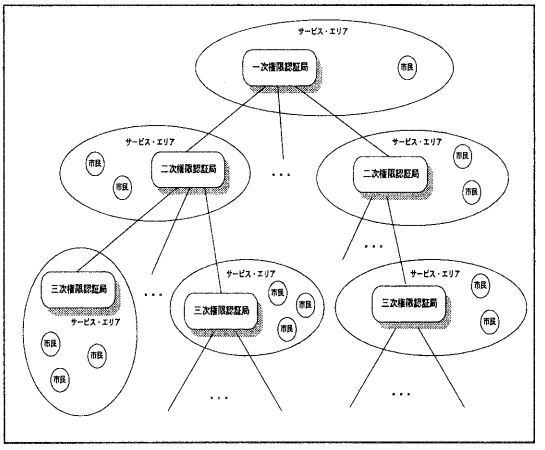

図 2-2-1 権限認証局ツリー(イメージ)

3．権限認証局の課題

3－1．権限認証局技術

最近広く普及しつつある電子商取引などに

おいて、セキュリティを保護・管理するために、認証局技術が使用されている。これは、本人であることを認証したり、書類の正規性を証明するためのデジタル署名等において基になる証明書を発行したり、申請者の公開鍵を証明したりする技術である。

今回提案する“権限認証局ツリー”を構成している権限認証局とは、前述の認証局技術のうち、本人認証部分と本人の行政アプリケーションへのアクセス権限の認証部分（権限認証）とを分離し、後者を実施する局として定義したものである。権限チケットという概念を導入することにより、この権限チケットでアプリケーション実行権限を実現し、またチケット管理サーバーで権限認証局を実現した（チケット権限管理技術）。

この、“権限認証局モデル”(図 3-1-1) については参考文献 [1] (「公共システムにおける権限認証局」) にて発表済みであるので本稿では触れない。

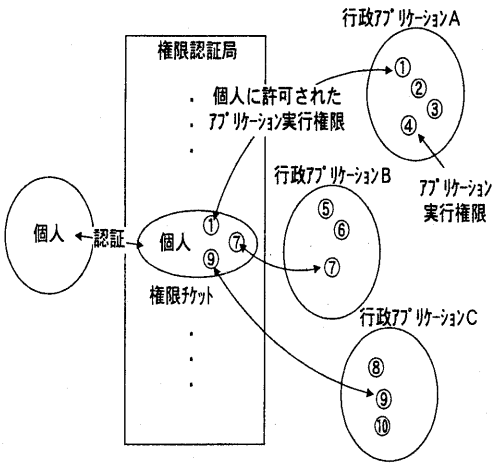

図 3-1-1 権限認証局モデル

3－2．権限認証局の課題

前記の“権限認証局モデル”に基づいて実施された実験により、権限チケットと権限認証局による行政アプリケーションのセキュリティ管理のしくみは、通常の場合においては、有効に機能することが確認されているが、下記のとおり、いくつかの点で検討すべき課題も発見された。

① 権限チケットのセキュリティ

インターネットを舞台にしたウイルスやハッカーの問題が顕在化している。ＰＣ内に存在するすべてのデータは、これらの脅威に晒されている。ＰＣ上の行政アプリケーションに渡される権限チケットも、行政アプリケーションの管理如何によってはウイルスの標的になりうる。

② ユーザビリティの向上

呼出すアプリケーションが変わるたびに、本人認証と権限認証を再度実行するため ICカードの再挿入が求められる点、ユーザビリティ上問題である。これは、前記の実験で、改善要望が強かった点である。

③ 負荷の集中化の回避

市民一人一人と行政アプリケーションの一つ一つをリアルタイムに紐付け管理する権限認証局に、トランザクションが集中する。そのため、アプリケーションや市民の増加の影響が心配される。

以上の課題を解消するため、権限認証局のツリー化と、それを支える時限認証局を導入した。

4．権限認証局のツリー化

4－1．時限認証局と時限チケット

3－2に記述した権限認証局のかかえる課題を解決する方法として、時限チケットおよび時限認証局の考えを導入した。

① 権限チケットのセキュリティ強化

IC カードから行政アプリケーションに渡された後の権限チケットのセキュリティは、行政アプリケーションの管理に委ねられることになるが、権限チケットの安全性を一律確保するために、超短期の有効期限（権限証明書内の有効期限とは別）の要素を追加した。超短期の有効期限の設定により、行政アプリケーションの権限チケット管理方法に左右されず、権限チケットの安全性を一律確保することが可能になるし、ウイルスへの感染の脅威も確実に減少する。また、超短期の有効期限を増減することにより、安全性の強弱の管理も可能となる。

権限チケットに時間管理の要素を付加する方法として、時間に関するチケットを発行する方式（時限チケット方式）を採用した。また、この時限チケットを認証し、且つそれを証明するための認証局として時限認証局を定義した。

時限チケットは、それ自体が証明書となることから、そのフォーマットについては国際標準である X.509 フォーマットに準拠した。

この時限チケットの発行のしくみは、アプリケーション（権限認証局）が時限認証局に対して、希望の有効時間を指定して、証明書の発行を要求することにより、時限認証局により発行される。図 4-1-1 に発行の流れを示した。

この方式により、権限チケットの安全性の大幅な向上が実現できる。

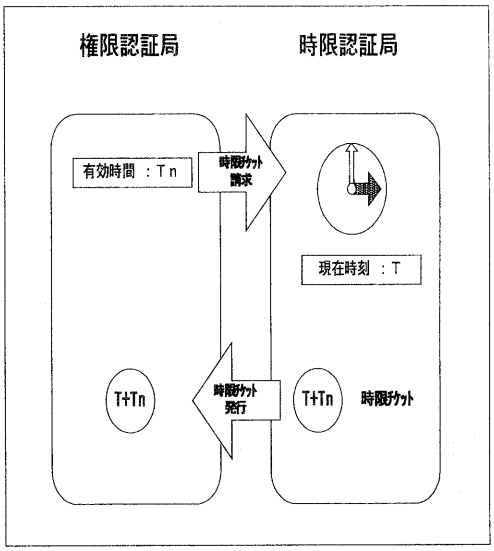

図 4-1-1 時限チケット発行の流れ

ところで、権限認証局は、権限チケットと時限認証局から発行された時限チケットとを、ペアとして保証する必要がある。これを実現するため、二つのチケットに電子割印を押す方法を採用した。

図 4-1-2 にそのイメージを示す。

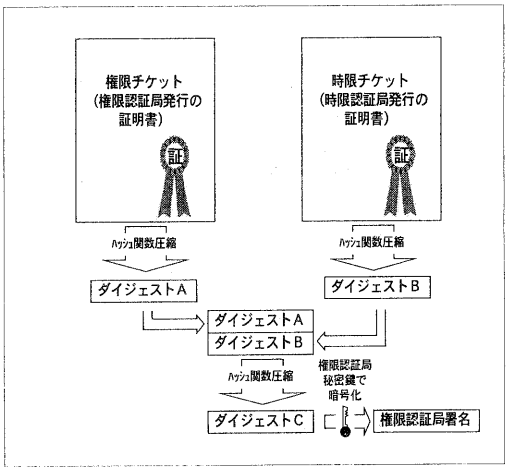

図 4-1-2 時限/権限チケットのペア保証

② ユーザビリティの向上

時限チケットの導入により、権限チケットのセキュリティ強化が実現される。これにより、IC カード挿入中などは、権限チケットを行政アプリケーション側で保管できるようになり、アプリケーションとしては、権限認証局をあまり意識せずにユーザビリティの向上を図ることができる。課題となっていた、アプリケーションの切替えの度に求められる IC カードの再挿入要求の問題は、クライアント側のアプリケーションに IC カードが挿入されていて、なお且つ時限チケットが有効である限りにおいては解決された。

また、端末に権限チケットを一時的に保持することが可能になることにより、アプリケーションによる権限認証局へのアクセス頻度が低減する。さらに権限認証局の負荷低減によるシステム効果で、他のユーザビリティの向上も期待できる。

③ 負荷の集中化の回避

システム内で発生するトランザクションの流れを分析すると、発生元である市民と行政アプリケーションから、すべてのトランザクションが権限認証局へ集中している（図 4-1-3 参照）。さらに、その中身についてみると、アプリケーションから権限認証局へのアクセスは、権限チケットの登録・削除のタイミングのみ発生するのに対して、市民から権限認証局へのアクセスはアプリケーションの使用の度に発生する。

また、アプリケーションの数に比較して、市民の数が圧倒的に多いことから、負荷の集中化の回避を考える時、市民と権限認証局間のトランザクションの分散化を図るのが効果的であると考えられる。図 4-1-4 にトランザクション比較を示す。

以上から判断して、この課題の解決策として、権限認証局の分散を検討した。

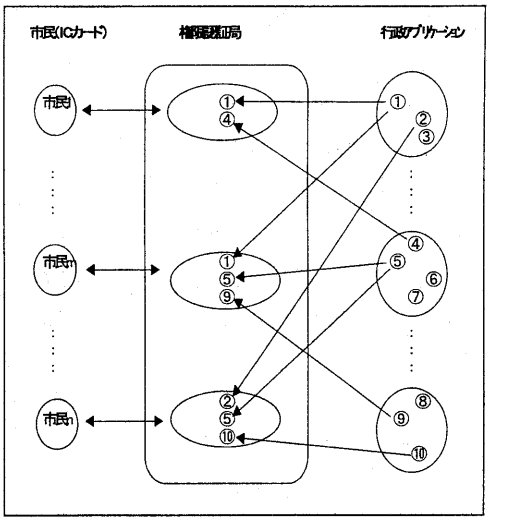

図 4-1-3 トランザクションの集中図

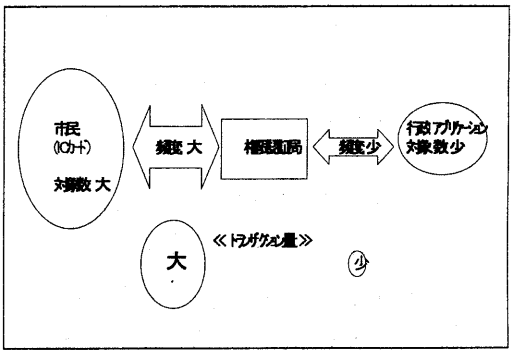

図 4-1-4 トランザクション比較

4－2．権限認証局の分散

権限認証局を分散するにあたり、市民がアプリケーションにアクセスするのに使用する端末に、個人による局所性があることに注目した。また、インターネット技術のなかからキャッシュ技術に注目し、そのキャッシュ技術を用いて二次権限認証局を設計した。キャ

ッシュ技術の利用により、二次権限認証局は直近で実績のある市民の権限チケットと時限チケットのみを管理すればよくなり、資源の有効利用も実現できた。

二次権限認証局での権限チケットのセキュリティ確保のためには、一次権限認証局と同様に時限認証局技術を導入した。これにより、一次権限認証局と二次権限認証局間のタイムラグによるセキュリティの低下を減らすことが可能となった。図 4-2-1 に、分散した権限認証局と、時限認証局の関係を示す。 時限チケットの導入により、二次権限認証局にある権限チケットの安全性を大いに向上することが出来た。

しかしながら、それでも緊急を要する権限の変更、たとえば IC カードの紛失による権限取消しなど、に対しては十分に安全とは言えない。そのため、権限取消技術として古くからあるブラックリスト確認技術 (Certification Revocation List) を導入した。これは、使用不可となった人（IC カード）の情報をブラックリストと呼ぶ共有ファイルに登録し、以後の不適な使用について阻止するものである。すなわち、権限認証局では、一次権限認証局に通知された IC カード紛失などの情報により、その認証局で管理する該当カードの権限チケットを使用不可とするとともに、全ての二次権限認証局にこの情報を通知し、ブラックリストに登録する。従って、全ての認証局において、該当カードは即座に使用不可能となる。これにより、否権限者の使用や侵入を、入り口で阻止・排除することができた。

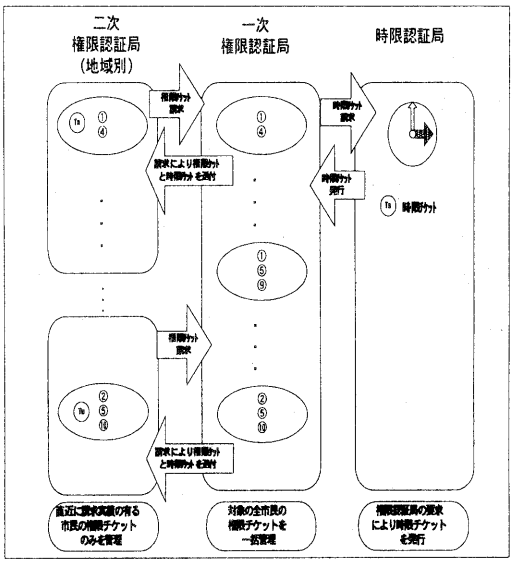

図 4-2-1 権限認証局と時限認証局の関係

4—3．時限認証局の拡張

権限認証局は、時限認証局が発行する時限チケットを基に分散が実施され、信頼される二次権限認証局が構築された。しかし、二次権限認証局においても、一次権限認証局と同様の配慮が必要であり、従って二次権限認証局に対応して二次時限認証局の必要をみた。図 4-3-1 に、拡張した時限認証局を含む分散権限認証局の構造を示す。

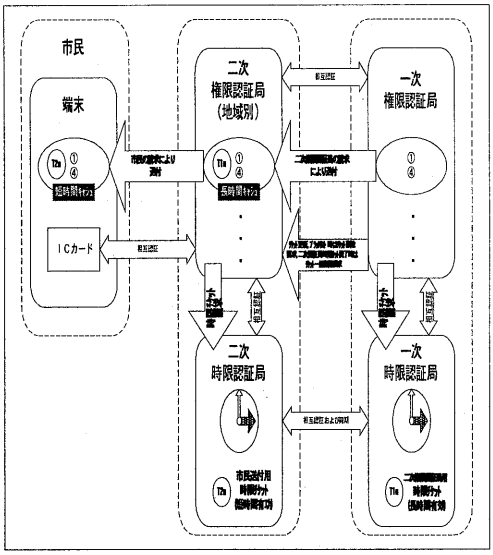

図 4-3-1 時限認証局の拡張

4－4．権限認証局ツリー

前述の時限認証局技術により、権限認証局は一次認証局を基本にした**権限認証局ツリー**を構築することを可能とした。一次権限認証局の下に複数の二次権限認証局を設け、さらに各々の二次権限認証局の下に複数の三次権限認証局を設ける。このように、ツリー構造によりサービス・エリアの細分化を実施することにより、広い範囲の行政エリアへの対応もスムーズに実現できることになる。その結果、権限認証局の利用は分散化され、結果として、莫大な数の市民と権限とを細かに管理する可能性を将来にむけて拡大した。

図 4-4-1 に権限認証局ツリーのイメージを示す。

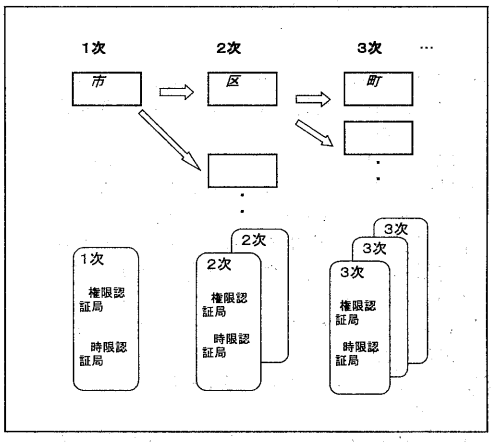

図 4-4-1 権限認証局ツリー

5．おわりに

最近の国をあげてのＩＴ振興政策に後押しされて、電子政府などを含む行政システムのＩＴ化の研究がますます活発に行われている。こんな状況のなか、電子認証についても国の法整備も着々と進んでおり、実用化への動きも加速することが予想される。

一般的に、行政システムは高い機密性を求めると同時に、多くの利用者をかかえる事が多い。したがって、高いセキュリティを維持しながら大規模なユーザーに対応して認証処理が可能な、認証局の分散化の技術が強く求められることになる。

本稿は、権限認証技術と時限認証技術とを組合わせて、“権限認証局ツリー”を構築することによる、「大規模分散認証システム」構築技術について述べた。この技術が、同様のシステムを構築しようとする時参考になることを期待する。

参考文献

[1]山本,樋口,橘,嶺,岩佐,久村："公共システムにおける権限認証局"、情報処理学会研究報告、Vol99, No.25

[2]山本,樋口,橘,近藤,久村："平成 11 年度北海道札幌市ﾏﾙﾁﾒﾃﾞｨｱ・ﾓﾃﾞﾙ市役所展開事業 成果報告書" ,通信・放送, May,2000

[3]松本,岩下："金融業務と認証技術：ｲﾝﾀｰﾈｯﾄ金融取引の安全性に関する考察" ,金融研究 Vol19,Apr.2000

[4]NetworkPro "ｾｷｭﾘﾃｨ ﾊﾟｰﾌｪｸﾄ･ｶﾞｲﾄﾞ"、雑誌,07/2000

[5]ICAT Newslettle, Vol.7,IETF 会議報告, 09/98

[6]TYOUSA 152, "組織間網におけるｱｸｾｽ制御の実態調査 V 章"

[7]Larry J.Hughes, Jr.,長原 宏次 監訳："ｲﾝﾀｰﾈｯﾄｾｷｭﾘﾃｨ"、ｲﾝﾌﾟﾚｽ, 1997

[8]Network Working Group: An approach for Using LDAP as Network Information Service,http://www.cis.ohio-state.edu/htbin/rfc/rfc2307.htm,1998