5R-01

携帯情報機器を用いた権利流通方式

千綿 伸之　花舘 蔵之　寺田 雅之
NTT 情報流通プラットフォーム研究所
{chiwata, hanadate, te}@isl.ntt.co.jp

1. はじめに

現在、権利は主に紙を媒体として、証券やチケットなどの形で流通されている。これらの権利を印刷された紙ではなく電子的な権利情報“電子チケット”として流通させることにより、Internet を介したチケットの購入や、発行および改札コストの低減などを可能にし、利便性を向上させる試みが提案されている[1]。電子チケットには以下の要件が必要とされる。

(1) 多様性への対応：多様な権利を様々な発行者が発行できる。

(2) 安全性の確保：権利が偽造・改竄・複製されない。また、流通事実の否認ができない。利用者の匿名性が確保される。

(3) 実用性の確保：負荷が集中するようなサーバを排除できる。オフラインで権利の流通を行える。発行や利用のための経済的・時間的コストが十分に低い。

このような電子チケット流通基盤実現のために、IC カードを用いて上記の要件を満たす原本性保証方式［2］とその方式に基いた電子チケットシステム FlexTicket［3］の提案がなされている。電子チケットシステム FlexTicket では、利用者は IC カードを持ち歩き、電子チケットの購入・譲渡・消費・内容確認の際には利用者の自宅あるいは街頭に設置された IC カードリーダ・ライタ付きの PC を利用する。

しかし、上記利用形態では、利便性・安全性の面で問題がある。まず、電子チケットを利用できる場所が IC カードリーダライタ付き PC の設置された場所に限られることから、電子チケットの内容確認や流通を行う際に、不便な場合がありうる。

また、IC カードそのものには表示・操作系が存在しないため、完全に安全とは言いきれない[6]という安全性の問題も存在する。

本稿ではそのような電子チケットの利便性・安全性の問題を解決するために、携帯情報機器に電子チケットを格納・流通させることを提案し、携帯情報機器をもちいた電子チケットの流通処理が実用的な性能でおこなえることを示す。

2. 電子チケット流通に必要な機能

電子チケット流通に必要な機能を示す。

表 1. 電子チケット流通に必要な機能

機能名	機能概要
格納	所持している電子チケットを保持する。
表示	所持している電子チケットの内容を表示する。
操作	電子チケットの流通、管理などの操作を受け付ける。
通信	通信を行い、電子チケットを流通させる。
暗号	電子チケット流通処理内で行われる暗号処理（電子署名、署名検証など）を行う。

上記機能のうち格納・表示・操作・通信機能については、携帯情報機器のペン操作機能、赤外線通信機能などを用いることにより、容易に実現可能である。

しかし、暗号機能については、鍵管理・処理速度の点で問題がある。

まず、FlexTicket における署名鍵は、利用者本人からも秘匿されなければならないが、携帯情報機器にはそのような秘匿手段がない。

また、携帯情報機器の演算速度が一般的な PC の 1/10～1/500 程度であるため、計算量の多い

電子署名および検証処理は性能上のボトルネックになることが予測される。

そこで携帯情報機器で利用可能な暗号処理LSIの開発が進んでいる［4］［5］[6]ことに着目し、これを暗号処理で用いることを前提に評価を行った。

3. 評価および結果

携帯情報機器をもちいた電子チケットの流通処理が実用的な性能でおこなえることを示す。評価は、2 台の暗号処理用 LSI を搭載した携帯情報機器を想定し、それらが赤外線通信路を介して電子チケットの流通を行った場合の性能値を計算する事で行った。格納・表示・操作・通信の各処理の性能は、携帯情報機器上にテストプログラムを構築することにより性能値を収集した。また暗号処理については参考文献[6]の値を用いた。この評価では、携帯情報機器として3Com 社の PalmIII を想定した。

評価の結果、電子チケットの流通処理にかかる時間は約 3 秒程度であることがわかり、携帯情報機器を用いた電子チケットの流通処理は、実用的な処理時間を実現可能であるとの結論を得た。

ただし、上記性能値は、FlexTicket の流通処理を単純に携帯情報機器に実装した場合を想定して算出した。そのため、この評価には、性能向上のための実装上の工夫（通信時のデータの圧縮など）は考慮されていないため、実際にはさらに性能向上できる余地があると考えられる。

4. まとめ

本稿では、電子チケットを利用する上で求められる利便性の要件を挙げ、その要件を満たす方式として携帯情報機器を用いて電子チケットを流通させることを提案した。また、携帯情報機器を用いた電子チケットの流通処理が 3 秒程度という実用的な性能を実現可能であることを検証した。

今後は、処理の更なる高速化を目指すと共に、携帯情報機器で電子チケットを扱うために不可欠な安全性の問題について検討をすすめる予定である。

5. 参考文献

［1］ K. Fujimura, and Y. Nakajima, “General-purpose Digital Ticket Framework,” *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*(1998).

［2］ 寺田雅之、久野浩、花舘蔵之、”権利流通基盤のための原本性保証方式”、コンピュータセキュリティシンポジウム’99 予稿集（1999）.

［3］ 水野康尚、千綿伸之、大嶋嘉人、松山一雄、”権利流通基盤のための汎用デジタルチケットシステム”、コンピュータセキュリティシンポジウム’99 予稿集（1999）.

［4］ 櫛間 英樹、新島 秀人、丸山 宏, “RSA チッ プによる SSL の高速化実験,” 情報処理学会第 56 回全国大会 （1998）.

［5］ A. Satoh, Y. Kobayashi, H. Niijima, N. Ooba, S. Munetoh and S. Sone, "A High-Speed Small RSA Encryption LSI with Low-Power Dissipation," Information Security Workshop（1997）.

［6］ 神谷 耕史、丸山 宏、”一時的なデジタル証明書による権限委譲”、コンピュータセキュリティシンポジウム’98（1998）