電子チケットの経路非依存配信手法

1H−04

仁野裕一　谷幹也　市山俊治
NECインターネットシステム研究所

1. はじめに

電子チケット(以下、単にチケット)の配信は、安全性の観点からデバイス（特にICカード）に依存したサービスが中心であった。しかし、このサービスは、チケット配信において経路(入出力I/F)が制限される、多様な権利を扱えない等の問題があった。

これらの問題を解決するために、著者らは現在広く普及した携帯電話上のアプリケーション実行環境でアプリケーションとして実装するチケット管理手法を提案する。このアプリケーション実行環境は、経路非依存性が高くて、配信経路の多様性を実現できる。また、多様な権利管理手法に対してそれぞれに応じたアプリケーションを実装することが可能なため、権利の多様性にも柔軟に対応できる。本稿では、本手法の概要とその応用例としてチケットのpush型配信手法について述べる。

2. チケット管理手法

2.1. 携帯電話アプリケーション実行環境

現在多く利用されている携帯電話上のアプリケーション実行環境には、携帯電話上のjava等がある。これらは、チケットのアプリケーション構築に適したいくつかの特徴を有している。

第1に、MULTOS[1]カード等の実行環境と同様に、複数のアプリケーションが実行可能で、アプリケーション内で利用するデータは他のアプリケーションから利用できない仕様になっている。

第2に、HTTPが利用可能なため、ICカードのように特別な書き込みデバイスがなくても、インターネットを介してアプリケーションを提供できる。

第3に、Bluetooth、IrDA、ICカードなどとの入出力I/Fの開発も急速に進んでいる。

したがって、これを利用することで、チケット配信事業者は、将来的に種々の入出力I/Fで授受が可能となるチケット管理APを自由に実装し、簡単にユーザに提供できる。しかも、配信したチケットが他のアプリケーションによって破損される恐れもない。

ところが、この実行環境はこれらの入出力I/Fが内部に組み込まれると、実行環境内のデータが外部に流出する危険性が増す問題がある。したがって、単にこれらの実行環境でチケット管理APを構築するだけでは不十分で、内部のチケットデータを安全に守る枠組みがないと、チケットの改ざん/複製による悪用を防止できない。

2.2. 提案するチケット管理手法

著者らは、上記チケット管理APの安全性を高めるために、本人認証用の証明書と暗号化機能/復号機能を有する2ndチップ[2]と連携する手法を提案する。チケット管理APは、チケット発行/譲渡/利用時に2ndチップ内の証明書を発行元/譲渡者/利用機関に送付し、チケットの暗号化/復号を2ndチップの機能を利用して行う。本手法のシステム図を図1に示す。

本手法では、チケット配信事業者が上記の機能を有するチケット管理APを事前にHTTPで配信する。その後、チケット管理APがチケット発行/譲渡/利用時に本手法特有の処理を行う。ここでは紙面の都合上、チケット利用時の処理のみ図2を利用して説明する。なお、ここで示すのは最低限の処理であり、チケット管理AP独自の処理の追加は可能である。

まず、チケット配信事業者は2ndチップ内の本人認証用の証明書をチケット管理APに要求し、チケッ

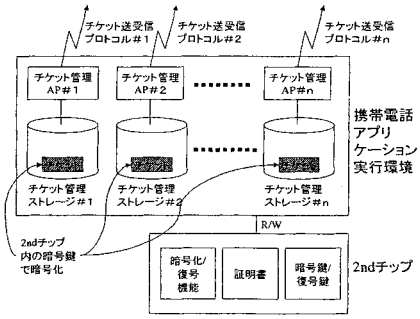

図1 チケット管理システム図

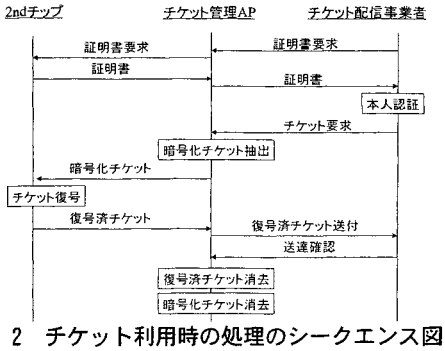

図2 チケット利用時の処理のシークエンス図

An e-Ticket Distribution Method Independent of Distribution Routes
Yuichi Nino, Mikiya Tani and Shunji Ichiyama
Internet Systems Research Laboratories, NEC Corp.

ト管理APは2ndチップにある証明書をチケット配信事業者に送付する。つぎに、チケット配信事業者は本人認証後、チケット管理APにチケットを要求する。チケット管理 AP はストレージ内にある暗号化チケットを 2nd チップに送付し、2nd チップで復号された復号済チケットをチケット配信事業者に送付する。チケット配信事業者はチケットの重複利用はないかチェックし、必要に応じて利用許可/不許可の判断を行い、その結果を送達確認として送信する。最後に、チケット管理APは送達確認の情報に基づき、復号済/暗号化チケットを削除する。

以上の方法により、チケットの改ざん/複製による悪用の防止を実現する。

3. 応用例

本手法は、多様な配信経路をサポートしていることが特徴であるが、これを利用したチケットのpush型配信へ適用する応用について紹介する。push型配信とは、予め譲渡先を指定した上でチケットを発行するものである。現在、種々のチケット流通基盤が提案されている[3]が、譲渡先の事前指定は行えない。

携帯電話では、push型配信を受信する経路として現在メールしか実装されていないが、今後 P2P や Webサーバなど様々な経路がサポートされる可能性がある。表 1ではこれら３つの配信経路が携帯電話に実装された場合における、チケットの push 型配信を実現するための必要機能を示す。

つぎに、図 3に push 型配信への適用例として、チケット購入者と利用者が異なる場合に、購入と同時にチケットを利用者の端末にメールを利用して配信した場合の処理内容の１例を示す。

4. 他の手法との比較

本手法とICカードとの比較を表 2に示す。

まず、本手法は、多種類の入出力 I/F をサポートする実行環境上で動作するので、多様な配信経路を実現できる。一方、IC カードは、独自の入出力 I/F しかサポートしていないので、配信経路が限定的である。また、本手法は、多様なチケット管理 AP を実装することが可能なため、多様な権利を扱える。一方、IC カードは内部に実装できるチケット管理 AP が限定されるので、その管理 AP がサポートした少種類の権利しか扱えない。

ただし、本手法は、チケットの複製を防止できないので、①重複利用を監視するための機能を事業者側が必ず導入することと、②運用上チケットには有効期限を設けることが必要である。また、携帯電話はメモリ障害によるデータ破損が稀に発生するので、③障害時のチケット復旧サービスを事業者側で備えることが必要となる。①②については現在のサービスでも行われておりそれほど問題にならないが、現在③に類したサービスはなく、事業者側の負担の少ない復旧方式を今後検討する必要がある。

表 1 チケットの push 型配信における必要機能

経路	必要機能
メール	送信された情報の Content-Type をもとに、適切な管理 AP を起動し、チケットを格納する機能を持つメーラ
Ｐ２Ｐ	外部から管理 AP を参照、実行する機能
Ｗｅｂ サーバ	送信元の URI から適切な管理 AP を起動し、送受信情報の Content-Type をもとに、管理ストレージの格納を行う機能

表 2 本手法と IC カードとの比較

	IC カード	本手法
配信経路	限定的	多様
扱える権利	少種類	多種類
権利の改ざん防止	可	可
権利の複製防止	可	不可
内部のデータ破損	無	稀に生じる

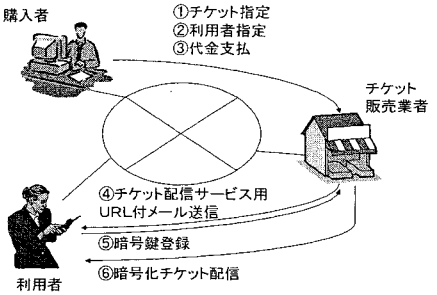

図 3 チケットの push 型配信の処理内容

5. おわりに

IC カードに比べて経路非依存性が高く、多様な権利を扱え、かつ安全性の高いチケット管理手法として、携帯電話アプリケーション実行環境と 2nd チップを利用した管理手法を提案し、それを利用したチケットの push 型配信手法について説明した。今後、携帯電話のメモリ障害時の復旧方式としてエスクローモデルを検討し、本管理手法をコンテンツの利用管理システム[4]に適用していく予定である。

参考文献

[1] 助田他,IC カードを利用したゲームシステムの提案と実装,信学ソ大,D-6-8,1999

[2] ECOM,モバイル EC に関わる決済標準モデルの研究中間報告書,pp.9-15, 2001

[3] 寺田他,電子権利流通基盤のための汎用的な原本性保証方式,情報処理学会論文誌,vol.42,No.8, pp.2017-2029,2001

[4] 中村,他:コンテンツ利用管理システム:モバイル RightsShell,情処全大 63 回, 5V-01,5V-02, 2001.