6G-03: モバイルキャッシュ・セキュリティシステム (1)

中溝 孝則　加藤 岳久　宮崎 真悟　倉富 修　才所 敏明
(株) 東芝 SI 技術開発センター

1 はじめに

現在、多くの電子マネーによる電子決済の実証実験が行われているが、多くはスマートカードなどを利用した対面販売、または PC によるインターネットを介した販売を前提にしたものである。

また、PC やスマートカードによる電子決済を携帯電話で行う方法として、フィンランドでは Mobail Pay と呼ばれる携帯電話を利用した、自動販売機の商品を購入するシステムの実用化に向けた実験が行われている

しかし、それらは、クレジット決済をベースにしたものであり、利用者が商品を購入する際の通信コスト負担が大きいこと、支払までの期間が長いこと、手数料が発生するといった問題点がある。

本論文では、商品購入時の利用者の負担を軽減するため、商品購入時に携帯端末と自動販売機間だけで決済が行え、かつ携帯端末と自動販売機の物理的接触が不要な無線を用いる商品購入システムを提案する。

2 既存の方式とその問題点

本節では、現在提案されている、携帯電話を用いた自動販売機での商品購入システムについての概略を説明し、それらの問題点を挙げる。

Mobail Pay

自動販売機に明記された番号に電話をかけることで、センターが電話の持ち主の口座を確認し商品をだす。

MMS

携帯端末から決済用のサーバにアクセスし、携帯電話番号、自動販売機の識別番号、利用金額を入力。サーバから自動販売機に送り返された電話番号と、自動販売機のコネクタに接続した携帯電話の電話番号が一致した場合、商品を購入できる。

これらのシステムには以下のような問題点が存在する。

- 携帯端末と自動販売機との物理的接触が必要。
- 商品を購入する際、自動販売機以外と通信する必要があり、通信料がかかる。
- 商品を購入するまでに、携帯端末で多くの操作を行う必要があり、利用者の負担が大きい。

3 提案システムの特徴

前節で述べた問題点を解消するため、次のような特徴をもつシステムを提案する。

プリペイド方式

あらかじめ、利用者の携帯電話にバリューを格納することで、携帯端末および自動販売機間だけで決済が行えるプリペイド方式を採用した。これにより商品購入時にセンターと通信する必要が無くなり通信料を削減することができる。

Bluetooth の利用

携帯端末と自動販売機の間の通信は無線で行い、消費電力が少なく携帯端末にも組み込むことができる Bluetooth を利用

楕円曲線暗号方式を利用

メモリー容量の少ない携帯端末での利用を考え、RSA 暗号に比べ鍵長を短くできる楕円曲線暗号を採用

不正防止

プロトコルの各段階で、署名をつけることにより不正を防止するとともに、データの真正性、証拠性を確保する。

再充填可能なバリュー

携帯端末に格納されているバリューの残高が少なくなった場合バリューの再充填を可能とした。

Security for Mobilecash System (1)
Takanori Nakamizo, Takehisa Kato, Shingo Miyazaki, Osamu Kuratomi, and Toshiaki Saisho
System Integration Technology Center, Toshiba Corporation

4　システムの概要

4.1　システムの構成

本システムは、下図に示すようにバリュー発行機関、携帯端末、自動販売機、証明書発行機関の４つの部分により構成されている。

以下ではそれぞれの機能について概要を述べる。

証明書発行機関

バリュー発行機関、携帯端末、自動販売機で使用する秘密鍵、公開鍵および、公開鍵証明書を生成する。証明書発行機関は、ネットワークに接続せず単独で動作する。

バリュー発行機関

バリュー発行機関は、携帯端末を認証し、新規バリューの発行/バリューの再充填を行う。

また、バリュー発行機関は、証明書発行機関検証鍵、バリュー発行機関署名鍵・検証鍵を保持している。

携帯端末

携帯端末は、バリューの購入、商品購入の２つの機能をもつ。バリュー購入時には、購入したバリューの正当性を確認し、携帯端末内の残高カウンターを増額する。

商品購入時には、代金を支払ったことを示す支払証明書を発行し、残高カウンターを減額する。

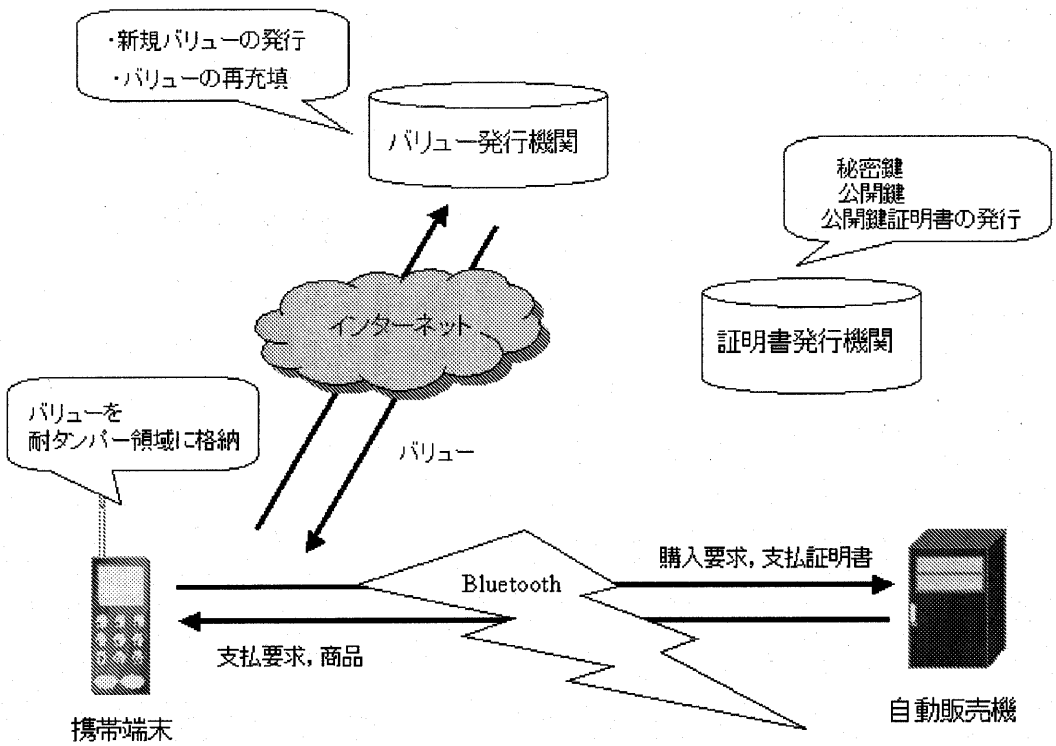
携帯端末には、工場出荷時に携帯端末の署名鍵・検証鍵・公開鍵証明書、バリュー発行機関検証鍵、証明書発行機関検証鍵が格納される。

また、携帯端末には耐タンパー領域が存在し、バリュー残高の管理をそこで行う。

自動販売機

自動販売機は携帯端末から送られてくるバリューの正当性を確認し、携帯端末のバリュー残高が購入金額分減額されたのを確かめ、商品を排出する。

自動販売機には、工場出荷時にバリュー発行機関検証鍵、自動販売機署名鍵・検証鍵・公開鍵証明書が格納される。



5 プロトコル概要

本システムは、大きく以下の 3 つの部分に分けられる。

- 利用者は携帯端末からインターネットでバリュー発行機関に接続し、バリューを購入し携帯端末に格納する、バリュー購入。
- Bluetooth を用いて自動販売機と接続し、購入金額分のバリューを支払い商品を受け取る、商品購入。
- 携帯端末に格納してあるバリュー残高が少なくなった場合に、バリュー発行機関に接続し、バリューを再充填する、バリュー再充填。

本節では、バリュー購入、商品購入、バリュー再充填がどのように行われるかその詳しい手順を示す。プロトコルの詳細については [1] を参照

5.1 バリュー購入手順

1. 携帯端末は、端末検証鍵および公開鍵証明書を発行機関に送る。
2. 発行機関は、端末検証鍵の検証を行い、発行メニューを携帯端末に送る。
3. 携帯端末は、利用者の入力したバリューの購入を希望するベンダー名と購入金額、端末 ID のハッシュ値を計算しそれに端末の署名をつけたバリュー発行要求を発行機関に送る。
4. 発行機関は、バリュー発行要求の検証をおこない、ベンダー名、購入金額、バリュー通し番号のハッシュ値を求め、それへの署名（バリュー）を計算し携帯端末に送る。
5. 携帯端末はバリューの検証を行い、耐タンパー領域にあるカウンターを購入金額分増やす。その後、格納通知とバリュー通し番号のハッシュ値の署名を計算し、発行機関に送る。
6. 発行機関は完了通知を生成し、携帯端末に送る。

バリュー購入の流れを図 1 に示す。

5.2 商品購入手順

1. 携帯端末と自動販売機との Bluetooth セッションを確立する。
2. 携帯端末は、乱数を生成し自動販売機に送る。
3. 自動販売機は乱数に対し署名を行い、署名、自動販売機で扱っているベンダー名（複数）、公開鍵、公開鍵証明書を携帯端末に送る。
4. 携帯端末は、乱数及び自動販売機検証鍵の検証を行い、送られたベンダー名のうち、携帯端末に格納されているベンダーのバリューと残高を自動販売機に送る。
5. 自動販売機は、バリューの検証を行い、残高が商品金額より多い場合商品ボタンを点灯する。
6. 利用者は、商品を選択する。
7. 自動販売機は、選択された商品のベンダー名、商品価格から支払要求を作成し携帯端末に送る。
8. 携帯端末は、支払要求分の金額をカウンターから減額し、減額したことを示す支払証明書を自動販売機に送る。
9. 自動販売機は支払証明書の検証を行い検証結果が正しければ、商品を排出する。

商品購入の流れを図 2 に示す。

5.3 バリュー再充填手順

バリュー再充填の手順は、携帯端末が格納しているバリュー残高を初期化したことを示す残高初期化証明書の作成および検証の手順が加わる以外、バリュー購入手順と同じである。

1. 携帯端末は、端末検証鍵および公開鍵証明書を発行機関に送る。
2. 発行機関は、端末検証鍵の検証を行い、発行メニューを携帯端末に送る。
3. 携帯端末は、利用者の入力したバリュー再充填を希望するベンダー名のバリュー残高を初期化した後、初期化したことを示す残高初期化証明書を生成しそれに署名をつけて、バリュー発行要求とともにバリュー発行機関に送る。
4. 発行機関は、バリュー発行要求および残高初期化証明書の検証をおこない、ベンダー名、購入金額、バリュー通し番号のハッシュ値を求め、それへの署名（バリュー）を計算し携帯端末に送る。
5. 携帯端末はバリューの検証を行い、耐タンパー領域にあるカウンターを購入金額分増やす。その後、格納通知とバリュー通し番号のハッシュ値の署名を計算し、発行機関に送る。
6. 発行機関は完了通知を生成し、携帯端末に送る。

バリュー再充填の流れを図 6 に示す。

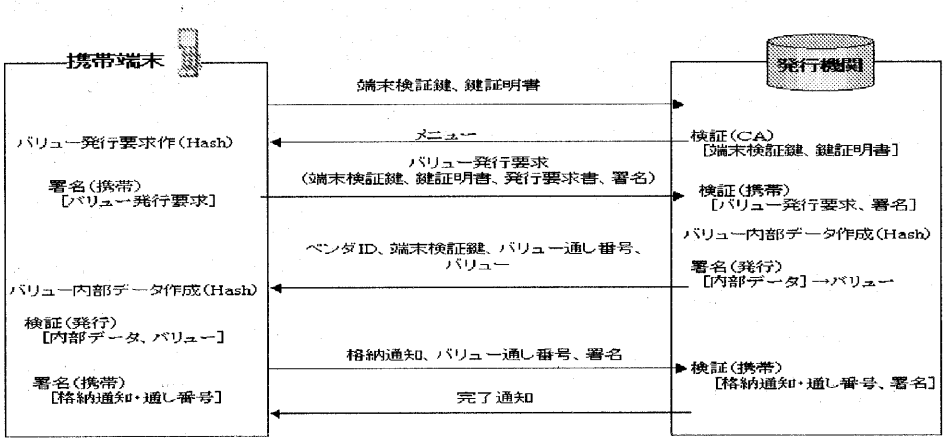


図 1: バリュー購入の流れ

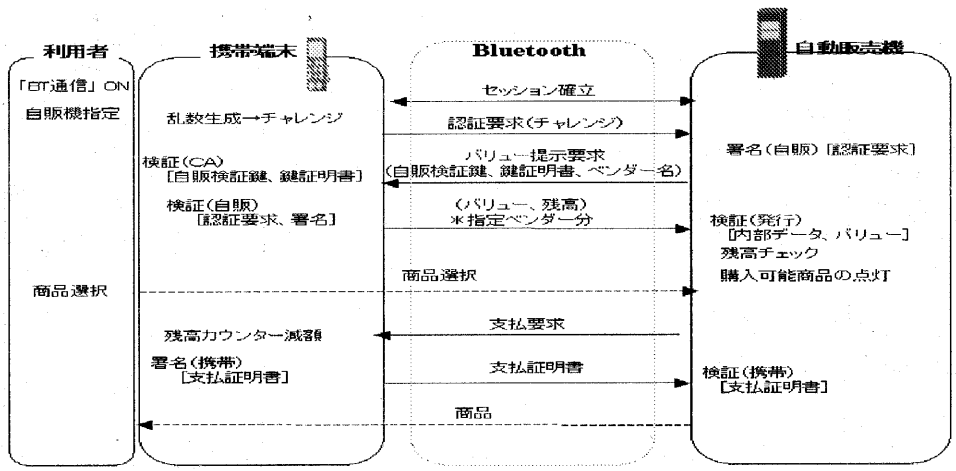


図 2: 商品購入の流れ

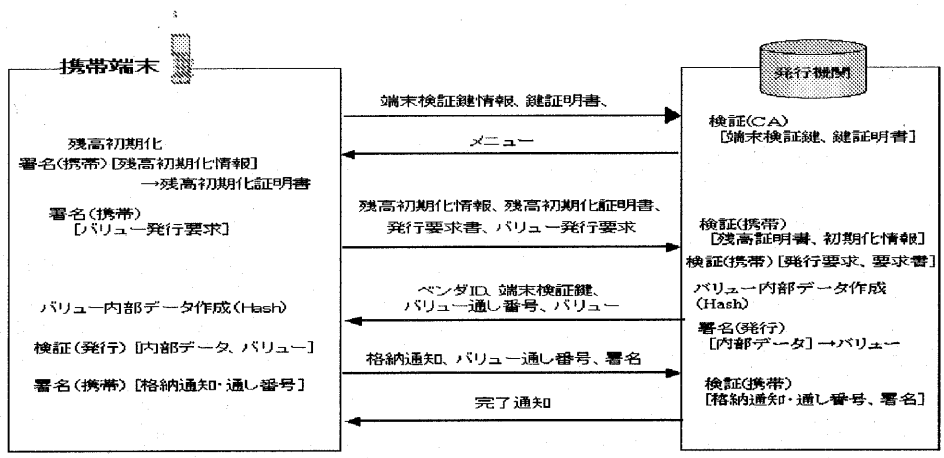


図 3: バリュー再充填の流れ

6　システムの実装

本文で示した機能を実装したバリュー発行機関、携帯端末、自動販売機、証明書発行機関を試作した。

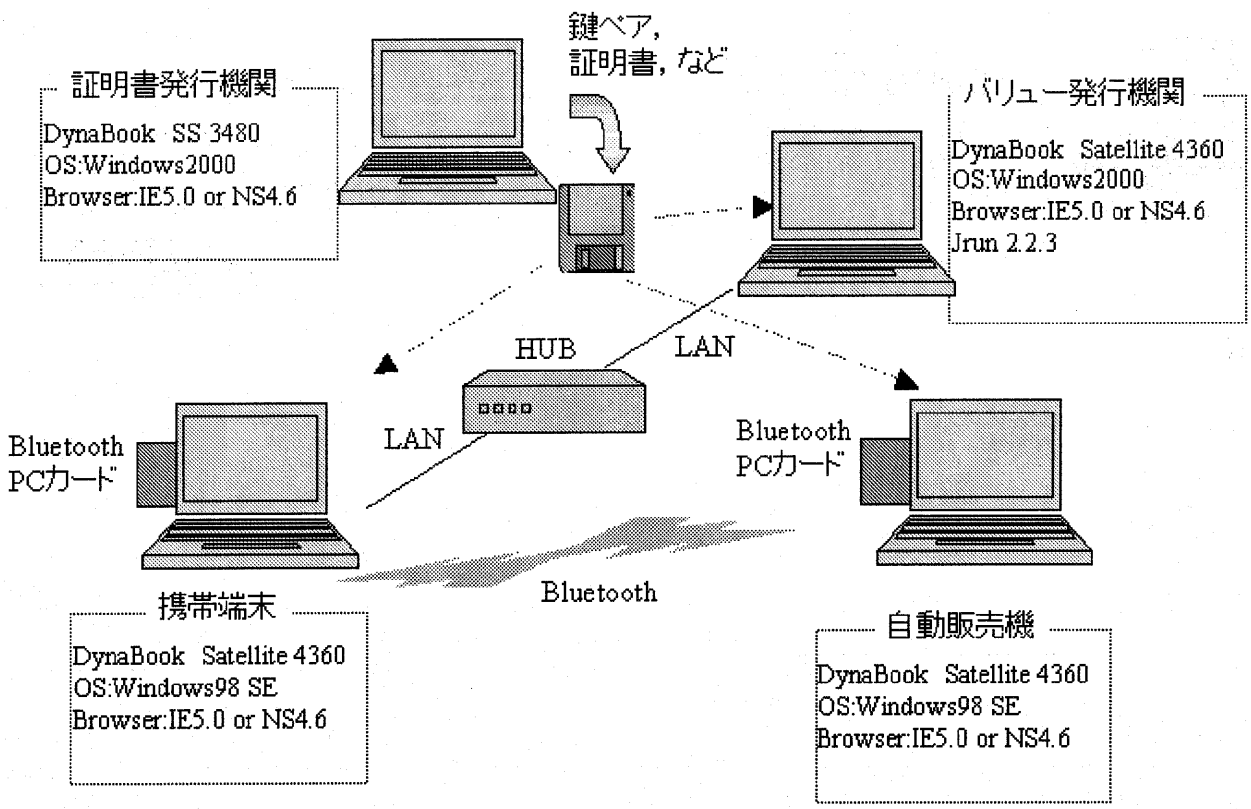
ただし、携帯端末、自動販売機についてはPCで代用した。また、携帯端末と自動販売機との間でBluetoothのセッションを確立する際に、Bluetooth　PCカード付属のデジアンサー社製のツールを利用している。

実装システムの構成および各端末のスペックは下図のとおりである。

- バリュー発行機関と携帯端末の間はLANで接続し、携帯端末と自動販売機の間はBluetoothを用い無線で通信を行う。
- デジタル署名に用いる楕円暗号モジュールはC言語で実装した。
- デジタル署名にはEC-DSA署名方式を用い、鍵長は160bitとした。
- バリュー発行機関は、Servlet Engine と Web Server をもつ。
- 携帯端末のバリュー購入画面は、バリュー発行機関においてServletを使って生成し、携帯端末のブラウザで表示している。
- 携帯端末の商品購入部分、自動販売機、証明書発行機関はJavaで実装した。

7　まとめ

本論文では、商品購入時の利用者の負担を軽減するため、商品購入時に携帯端末と自動販売機間だけで決済が行え、かつ携帯端末と自動販売機の物理的接触が不要な無線を用いる商品購入システムとして、プリペイド型のバリューおよびBlue toothを用いたモバイルキャッシュシステムを提案し、それらの実装を行った。



8　今後の課題

今後の課題としては、今回の実装では、携帯端末と自動販売機とのBluetoothセッションを確立するために、Bluetoothカードに付属しているデジアンサー社のツールを用いているが、そのようなツールを用いない実装の検討があげられる。

謝辞

本発表は，情報処理振興事業協会が実施する「先端的情報化推進基盤整備事業」の一環として委託を受け，当社が開発したシステムに関するものである．関係各位のご支援に感謝する．

参考文献

[1] 宮崎 真悟, 加藤 岳久, 中溝 孝則
倉富 修, 才所 敏明
モバイルキャッシュ・セキュリティシステム (2)

[2] 宮津和弘 Bluetooth ガイドブック日刊工業新聞社