“モバイルキャッシュ”を実現するセキュリティ技術

Security Technology for “Mobile Cash”

加藤　岳久　KATO Takehisa
宮崎　真悟　MIYAZAKI Shingo
才所　敏明　SAISHO Toshiaki

携帯電話を用いてインターネットへアクセスするユーザーの数が急速に伸び，携帯電話とインターネットとを用いたモバイルコマースの実験やサービスが行われている。

当社は，携帯電話を電子財布として機能させ，自動販売機とBluetooth™(注1)無線技術で接続して決済をする“モバイルキャッシュ”を提案し，そのセキュリティ技術を検証するためのシステムを試作している。このシステムは，楕円（だえん）曲線暗号を用いた電子署名をベースとした簡便でセキュリティの高いシステムである。

The number of people who access the Internet using cellular phones is increasing rapidly. As a result, several organizations have conducted experiments and introduced services for mobile commerce using cellular phones.

Toshiba has proposed the“Mobile Cash”system in which a cellular phone is used as an electronic wallet, connected to a vending machine with Bluetooth™ wireless technology. This system was prototyped to confirm its security functionality. The elliptic curve digital signature algorithm was used in the system to attain simple and highly secure transactions.

1 まえがき

携帯電話の急速な普及に伴い，携帯電話とPHSの加入者数は6,500万を超え，インターネット接続契約者数も3,300万を超えた(1)。また，これまで多くの電子マネーが提案され，かつ実証実験が行われている。最近では，携帯電話とインターネットを用いたモバイルコマースも提案され，実用化が進められている。

当社は，携帯電話と自動販売機とをBluetooth™無線技術で接続して，商品購入にかかわる代金を決済する“モバイルキャッシュ”を提案している。そして，楕円曲線暗号によるPKI（Public Key Infrastructure）をベースとしたモバイルキャッシュのためのセキュリティシステムを試作した。

ここでは，まず携帯電話を用いた代表的な商品購入システムを述べる。それから，モバイルキャッシュの特徴と概要について説明し，開発したセキュリティ技術を紹介する。

2 携帯電話を用いた電子決済

現在，国内外において，携帯電話を用いた自動販売機の商品購入システムが提案，試行されている。代表的なシステムについて，商品購入時の決済方法という点で分類すると，次のとおりとなる。

(1) ローカル型　利用者があらかじめバリュー（価値のある電子データ）を購入しておくプリペイド方式が多い。購入したバリューを格納した携帯電話やスマートカードなどを用いて自動販売機とやり取りし，商品を購入する。使用されたバリューに関するデータをバリュー発行機関などへ戻す還流が発生することが多い。

モバイルキャッシュや保護データ内蔵型電子バリュー交換方式(2)が，これに当たる。

(2) センターアクセス型　利用者は，自動販売機に明記されている番号へ電話を掛ける。センターは，利用者の口座をチェックし，残高が足りていれば自動販売機を販売可能にする。利用者が選択して購入した商品の金額分が口座から引かれる。このため，還流はない。

フィンランドで運用されているMobile Pay(3)やモバイルマネー システムユニット（MMS/U：Mobile Money System /Unit)(4)が，これに当たる。

3 モバイルキャッシュの概要

モバイルキャッシュは，携帯電話を財布代わりに，という目的で開発されたシステムである。

モバイルキャッシュの全体システムを図1に示す。

バリュー発行機関とベンダーとは，バリューの発行契約を行い，バリュー発行機関が発行可能なバリュー金額を設定する。利用者は，インターネットへ接続可能な携帯電話からバリュー発行機関にアクセスし，バリューを購入する。購入したバリューの金額分だけ，残高カウンタがセットされる。

バリューを購入した利用者は，自動販売機とBluetooth™無線技術により接続し，商品を購入する。なお，商品を購入

（注1） Bluetoothは，その商標権者が所有しており，当社はライセンスに基づき使用している。

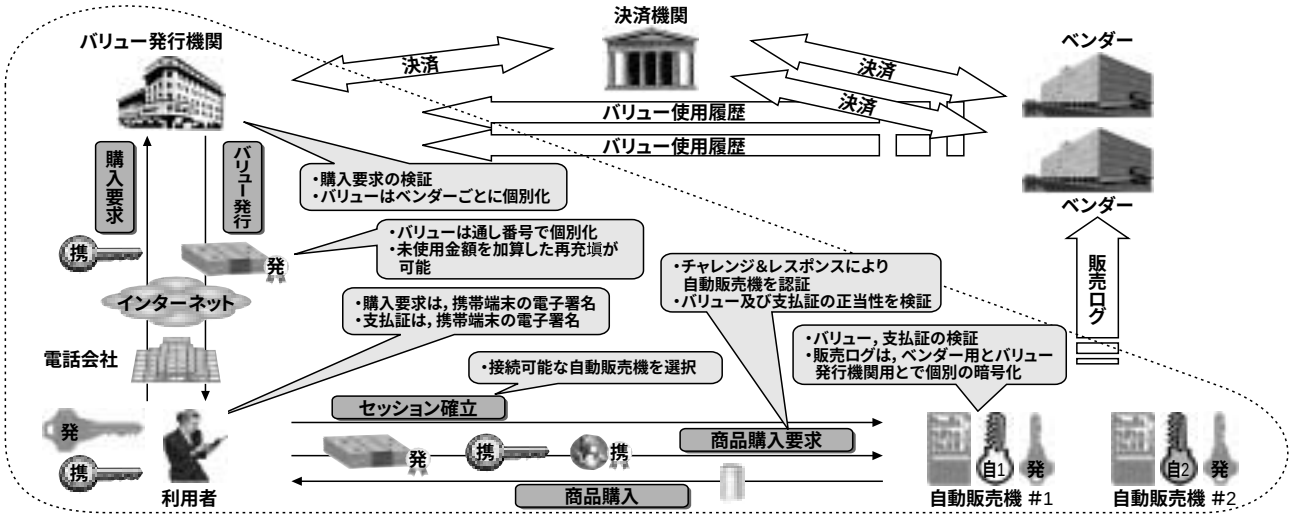

図1．電子署名をベースとしたモバイルキャッシュシステム　電子署名を用いることにより，流通するデータの真正性，証拠性を確保し，偽造などの不正を困難にしている。

“Mobile Cash”system based on digital signature

する際，利用者は購入可能な商品を，従来と同様，選択ボタンを押して選択する。これは，自動販売機の改良などのコストを抑えるためである。商品選択後に，残高カウンタは購入金額分だけ減額され，商品が排出される。

モバイルキャッシュの主な特徴は，次のとおりである。

⑴　プリペイド方式　　商品購入時における決済手数料をなくし，かつ利用者の利便性を考慮し，ローカル型の決済方式を採用した。これにより，商品購入時におけるセンターとの通信をなくし，利用者の通信コストも削減できる。

⑵　商品を提供するベンダーごとに異なるバリュー

モバイルキャッシュで用いるバリューは，商品を提供するベンダーごとに異なる。利用者は，購入する商品のベンダーのバリューを，あらかじめ購入しておく必要がある。

⑶　Bluetooth™無線技術による接続　　商品を購入するとき，携帯端末と自動販売機とはBluetooth™無線技術により接続する。Bluetooth™無線技術は10～100 mの範囲で接続が可能なため，利用者がストレスを感じることなく，自動販売機との接続が可能である。

自動販売機と携帯電話とをコネクタにより接続すれば，“なりすまし”といった不正に対する耐性は高まる。しかし，利用者の利便性を考慮すると，無線通信のほうが望ましいと思われる。

赤外線通信の場合，自動販売機と携帯電話とをかなり近づけないとデータのやり取りができない欠点がある。

3.1　モバイルキャッシュのセキュリティ

開発したセキュリティシステムは，図1の破線で囲んだバリュー発行機関，携帯端末，自動販売機の三者間のやり取りに関する部分である。インターネットを経由して携帯電話でバリューを購入し，自動販売機と無線通信を行い，商品を購入する。

そこで，モバイルキャッシュのセキュリティ要件として，以下を考えた。

⑴　バリュー購入時に，第三者になりすまし，不正にバリューを購入し，購入代金を支払わないことを防止する。

⑵　第三者が，バリューを購入するときにやり取りされるデータを盗聴し，取得したバリューなどの情報を不正使用することを防止する。

⑶　バリューを購入するときに，異なる携帯端末にバリューを格納することを防止する。

⑷　バリューをコピーし，複数の携帯端末で商品を購入することを防止する。

⑸　バリューの残高を偽り，自動販売機にアクセスして商品を購入することを防止する。

⑹　バリューのデータを不正に生成し，商品を購入することを防止する。

⑺　自動販売機になりすまし，他人のバリュー残高を減額させることを防止する。

3.2　セキュリティの基本方針

PKIをベースに，モバイルキャッシュでのデータの真正性，証拠性，利用者認証を実現し，高いセキュリティを確保した。そこで，セキュリティシステムでは，下記を前提とした。

⑴　携帯端末と自動販売機は，CA（Certification Authority）から，それぞれあらかじめ公開鍵（かぎ）ペア，及び公開鍵証明書が配布されている。

⑵　携帯端末には，公開鍵証明書を検証するためのCAの公開鍵，バリュー発行機関の公開鍵があらかじめ格

納され，自動販売機には，バリュー発行機関の公開鍵があらかじめ格納されている。

(3) 電子署名のための秘密鍵，及びバリューの残高カウンタは，携帯端末の持ち主ですら操作不可能な耐タンパ性メモリに格納されている。

3.3 バリューの新規購入

バリューの新規購入[5]における手順を図2に示す。

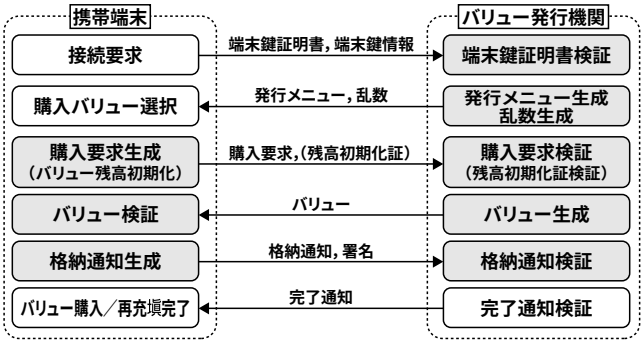

図2．バリュー購入手順　網掛け部が暗号処理の部分である。再充塡の際は，バリュー残高を初期化して新規にバリューが発行される。
Value purchase procedure

利用者はバリューを新規購入する際，端末鍵証明書を送信し，バリュー発行機関はこれを検証する。利用者は，バリュー発行機関からチャレンジ(乱数)を受け取り，購入するバリューに関する情報とチャレンジに電子署名を施した購入要求を送信する。

バリュー発行機関は，購入要求の正当性が確認できた場合だけバリューを生成する。利用者は，受け取ったバリューを検証して格納すると，格納通知を送信する。最後に完了通知を受け取り，バリューの新規購入が完了する。

バリュー購入におけるセキュリティのポイントを次に示す。

(1) 購入要求は，バリュー発行機関が送信したチャレンジを含んだ携帯端末の電子署名となっているため，正当な公開鍵ペアを所有する携帯端末以外から正当な購入要求を送れない。

(2) バリューはバリュー発行機関の電子署名であるので，偽造は困難である。また，バリューには端末公開鍵情報が埋め込まれている。

(3) 格納通知は，携帯端末の電子署名とし，購入要求を出した携帯端末と，バリューを受け取った携帯端末とが異なるような不正は困難である。

(4) データの欠落などでバリューが正しく受け取れない場合，再送要求を受け付ける。再送要求は携帯端末の電子署名とし，一度格納通知を送った携帯端末へは再送はしないことで，バリューの二重取得を防止している。

3.4 商品の購入

商品の購入における手順を図3に示す。

携帯端末からBluetooth™無線技術で自動販売機と接続し，自動販売機からのチャレンジに携帯端末のレスポンス(乱数に対する電子署名)を返すことで，自動販売機の相手認証を行う。

自動販売機が扱う商品の情報を携帯端末へ送信し，利用者が保有するバリューの情報，残高を自動販売機に送信する。検証の結果，商品の購入が可能なボタンが点灯し，利用者はボタンを押して商品を選択する。選択した商品の金額分の支払要求を自動販売機から受け取り，携帯端末はバリュー残高を減額して支払証を生成し，自動販売機へ送信する。自動販売機は，支払証の正当性を確認し，商品を排出し，受領証を生成して携帯端末へ送信する。

商品の購入におけるセキュリティのポイントを次に示す。

(1) 利用者は，自動販売機鍵証明書によるCAの承認，及びチャレンジ&レスポンスによる相手認証により，自動販売機の“なりすまし”は困難である。

(2) バリューには端末公開鍵の情報が埋め込まれているため，バリューの検証により端末公開鍵の正当性が検証できる。不正者は，正当な支払証が生成できないため商品は排出されない。したがって，携帯端末の“なりすまし”は困難である。

(3) 第三者がコピーしたバリューで商品を購入する場合，バリューに埋め込まれた端末公開鍵の情報から，支払証の検証で不正が検出できる。したがって，バリューのコピーによる不正は困難である。

(4) 商品が排出されなかった場合，自動販売機に支払証を，携帯端末に受領証を送信しておくことで証拠性を高めている。

(5) 個人の購入情報が1か所に集まると，個人の趣向を

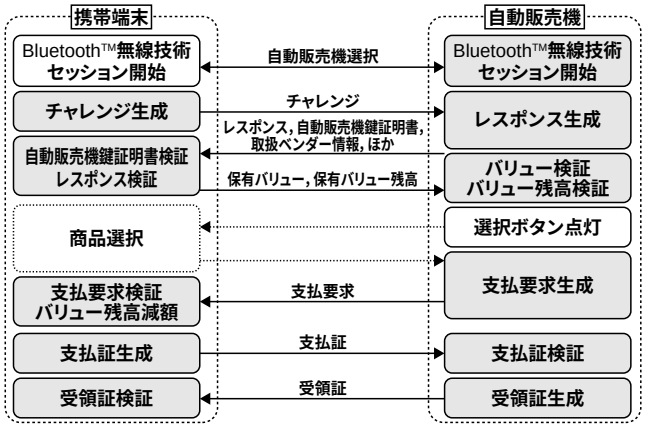

図3．商品購入手順　網掛け部が暗号処理の部分である。チャレンジ&レスポンスを用いた相手認証と，電子署名による偽造防止により安全性を確保した。
Goods purchase procedure

ベンダーなどが知ることが可能となり，プライバシーの問題が発生する。そこで，ベンダーには個人を特定可能な情報を販売ログとして含ませず，バリュー発行機関へ送信するバリューの使用履歴には商品を特定できる情報は含ませない。また，それぞれのデータは異なる鍵で暗号化して，安全性を高めた。

3.5 バリューの再充塡（じゅうてん）

残高が少なくなったベンダーのバリューを増額する場合，新規に購入して複数保持する方法が考えられる。しかし，携帯電話への適用を考慮すると，同じベンダーのバリューを複数保持することは，メモリが必要となるだけでなく，制御も複雑となる。そこで，残高が少なくなったバリューは，残高カウンタをいったん初期化し，バリュー発行機関へ初期化する前のバリュー残高を通知して，バリューを新規発行する(6)。

例えば，バリューの残高が50円で，1,000円のバリューを再充塡する場合，50円を0円にして，新しく1,000円のバリューを受け取り，支払う金額は950円となる。

したがって，バリューの再充塡では，携帯端末が購入要求を送信するときに，残高を初期化したことを証明するための残高初期化証も送信される（図2）。この残高初期化証は，携帯端末の電子署名である。バリューの再充塡におけるセキュリティのポイントを次に示す。

(1) 再充塡要求は，バリュー発行機関が送信したチャレンジを含んだ携帯端末の電子署名となっているため，正当な公開鍵ペアを所有する携帯端末以外から正当な再充塡要求は送れない。

(2) 残高初期化証は，携帯端末の電子署名となっているため，バリューの二重購入などは困難である。

4 技術検証システムの特徴

モバイルキャッシュにおけるバリューの購入，商品の購入，バリューの再充塡でのセキュリティ技術を検証するシステムを，パソコン（PC）で構築した(7)。構築したシステムの主な特徴は，次のとおりである。

(1) バリュー発行機関と携帯端末とはLAN接続とし，携帯端末と自動販売機とは当社製Bluetooth™無線技術PCカードを用いた。

(2) 公開鍵暗号は鍵長が160ビットの楕円曲線暗号を用いた。

(3) バリュー発行機関はServlet Engine(注2)とWebサーバとから成り，バリュー購入時の画面はServletを使って生成し携帯端末画面上に表示する。

(4) Bluetooth™無線技術で用いるプロファイルとして，Serial Port ProfileとLAN Access Profileとを検討した。1対1通信ということを考慮し，Serial Port Profileを用いた。

5 あとがき

携帯端末と自動販売機とをBluetooth™無線技術で接続し，商品購入における決済可能なモバイルキャッシュのセキュリティ技術を構築した。

このセキュリティシステムは，耐タンパ性メモリを用いることを前提とした。しかし，DoPa(注3)やPHSのネットワークを用いて，バリューの使用状況をバリュー発行機関へリアルタイムに伝えるシステムもある。これを利用し，耐タンパ性が破られた場合でも不正を検出する仕組みを追加することができる。また，ベンダーごとに異なるバリューを想定したが，すべてのベンダーに共通なバリューにすることも可能である。

謝　辞

このシステムは，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。ここに，関係各位のご支援に謝意を表します。

文　献

(1) TCA，2月末現在の携帯・PHS加入者数速報：http://k-tai.impress.co.jp/news/2001/03/07/tca.htm
(2) 保護データ内蔵型電子バリュー交換方式を開発：http://www.matsushita.co.jp/corp/news/official.data/data.dir/jn990917-1/jn990917-1.html
(3) http://www.sonera.com/
(4) http://www.lil.co.jp/~protect/
(5) 宮崎真悟，ほか．“モバイルキャッシュ・セキュリティシステム（2）”．第62回情報処理学会全国大会特別トラック（3）講演論文集．2001-03，p.135−140.
(6) 加藤岳久，ほか．“電子申請に適用可能な電子印紙システム”．コンピュータセキュリティシンポジウム1999論文集．1999，p.87−92.
(7) 中溝孝則，ほか．“モバイルキャッシュ・セキュリティシステム（1）”．第62回情報処理学会全国大会特別トラック（3）講演論文集．2001-03，p.129−134.

（注2） Webサーバー上で実行されるモジュール化されたJavaプログラムで，サーブレットの追加により，Webサーバの機能を拡張することができる。Javaは，米国SunMicrosystems社の商標。
（注3） （株）エヌ・ティ・ティ・ドコモによる800 MHz帯のデジタル携帯電話を使用するパケット通信サービス。

加藤　岳久　KATO Takehisa
e-ソリューション社 SI技術開発センター SI技術担当主務。情報及びネットワークセキュリティの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Systems Integration Technology Center

宮崎　真悟　MIYAZAKI Shingo
e-ソリューション社 SI技術開発センター SI技術担当。暗号及び情報セキュリティの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Systems Integration Technology Center

才所　敏明　SAISHO Toshiaki
e-ソリューション社 SI技術開発センター 戦略企画担当参事。暗号及び情報セキュリティの研究・開発に従事。情報処理学会，CSI，ACM，IEEE会員。
Systems Integration Technology Center