多目的なＩＣカードを共通的に利用するためのミドルウェア(2)
～Javaカード利用ミドルウェアの試作～

2G－9

麻野間　利行，石原　達也，青木　恵，才所　敏明
株式会社　東芝　ＳＩ技術開発センター

1．はじめに

情報インフラが整備されたオープンなネットワーク上で，今後は，電子商取引，行政，医療，金融，教育などのさまざまなサービスが提供されていくことが予想される．それらのサービスにおいてセキュリティの確保は必須の課題であり，ＩＣカードの利用，さらには1枚のカードでいろいろなサービスを受けることができるようになることが期待されている．しかし，各アプリが個別にカードにアクセスしていたのでは，そのような共通化は困難で，また，カードとの通信自体が煩雑であるという問題がある．そこで，カードを共通的にかつ簡便に利用できるミドルウエアを提案する．

多目的なＩＣカードを利用したアプリケーションの開発には共通ミドルウエアを構築することがアプリケーションの生産性向上につながり，さらには利用者にとっての利便性を確保することにもなる．そこで，多目的なＩＣカードとしてJavaカードを選択し，標準的なWebブラウザ上のJavaアプレットから，Javaカードの利用を可能にするミドルウエアを開発するとともにその有効性を検証することとした．

2．特徴

ミドルウエアの開発にあたっては，ネットワークでの利用を想定して，より効果が期待できる設計を行い，ＩＣカードさえ受け取れば個別の機能モジュールをインストールせずに，ネットワーク上から動的にダウンロードし，すぐに利用できる環境を実現できるアーキテクチャを検討した．

ミドルウェアの機能として，アプリケーションの処理を簡略化できるように，Javaカードをアクセスする煩雑な手続きや基本機能を持たせ，さらに，公開鍵方式ベースの認証インフラで高度ＩＣカードを利用可能とする目的で，公開鍵証明書の処理を付加した．

3．機能要件

ミドルウェアの機能として以下の4点があげられる．

1）アクセス手続きの隠蔽，簡略化

カードとの低レベル通信プロトコルの知識が不要で，カード／ドライバの種類の違いを意識せずに済むような簡便カードアクセスを実現するために，カード／ドライバのインタフェースを共通／簡便化し，個々の違いを個別追加モジュールによって吸収できるようにする．

2）基本機能を利用する共通インタフェースの提供

カードの主な利用目的である本人確認や暗号処理を共通的に行えるようにするために，鍵の保存管理，暗号／署名処理，公開鍵証明書保存管理，などの共通インタフェースを定義し，対応する（下記3）における）カードサービスと，それと対をなすカードアプレットを開発する．

3）個別機能の利用を支援する枠組みの提供

上位アプリケーションでカードの個別機能（カードアプレット）を利用するためには，カードアプレット固有のカードコマンドを利用した低レベル通信が必要で簡便利用性が損なわれるという課題に対し，カードサービスというカードアプレットを簡便に利用するためコンポーネントを追加／管理可能にすることにより，Ｊａｖａカード個別機能の簡便利用を実現する．

4）公開鍵証明書の分解，検査，管理機能

X.509の証明書は可変長データが折り重なった複雑な構成であり，カード内での汎用的処理が困難であるが，カード外の証明書ライブラリとカード内証明書をシームレスに連携させることにより，

The Middleware for Common Use of Multipurpose Smart Cards(2) : A Prototype of The Middleware for Accessing Java Cards
Toshiyuki Asanoma,Tatsuya Ishihara,
Megumi Aoki,Toshiaki saisho
System Integration Technology Center,
TOSHIBA CORPORATION

カード証明書の簡便利用を実現する．

4．設計，試作

別途検討した基本的なアーキテクチャ[1]にこれらを考慮し，ミドルウェアのアーキテクチャ（図1）および機能ブロック（図2）を設計し，試作を行った．

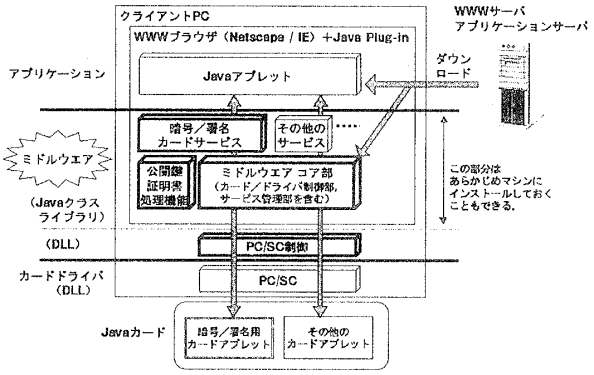

図1　ミドルウェアのアーキテクチャ

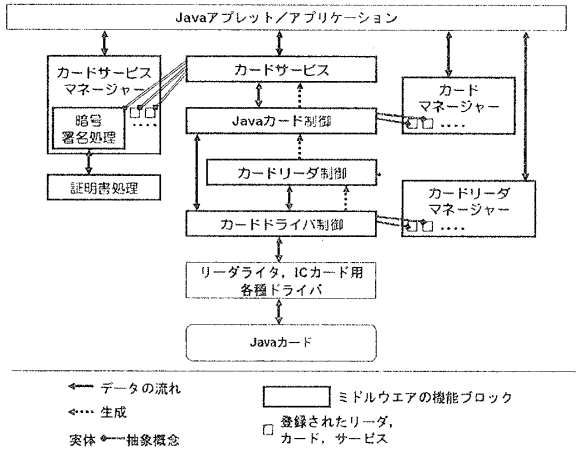

図2　ミドルウェアの機能ブロック図

また，Javaカードと Webサーバ／ブラウザを用いた簡単な認証システムを含んだＥＣデモシステムの設計，試作を行った．

5．結果

今回のミドルウエアの設計／開発を通じて，ミドルウエアのフレームワークの部分では，様々な種類のカードドライバ，Java カード，カードアプレットに対応できるような拡張性を持たせることができた．そして，実際に Java アプレットから PC/SC を経由して，様々な Java カード上の，様々なサンプルカードサービスにアクセスすることができた．

また，暗号／署名カードサービスでは，Java カードに共通鍵や公開鍵ペアを複数個格納して，その鍵を使って暗号や署名を行うことが，鍵の種類によらず共通的なインタフェースで簡単にできるような設計／開発を行うことができた．さらに，公開鍵証明書ライブラリと連携させることで，公開鍵暗号を利用した様々なシステムに，Java カードを組み込む一つの方法を確立できた．

また，ＥＣデモシステムによりミドルウェアの有用性を確認した．具体的には，ミドルウエアの各機能が予定通り動作すること，カードの詳細な知識なしにプログラム開発できること，複数の Java カードに対応可能であること，を検証し，さらにミドルウエアを利用しない場合とした場合の生産性の比較を行った結果，開発ステップ数で約5分の1となることを確認した．

6．おわりに

Java カードを利用するアプリケーションの開発に，ここで紹介した方法を使用することにより，アプリケーション開発者による，電子商取引，医療，教育，公共サービス等，高度かつセキュリティ機能が必須な次世代のアプリケーションの開発促進が期待される．そして最終的には，利用者はこれらのさまざまなサービスを1枚（もしくは目的，重要度別の数枚）のカードで受けることができるようになる．

7．謝辞

本研究は，通信・放送機構の委託研究「マルチメディアネットワーク共通化技術の研究開発」によるものである．

関係各位のご支援に感謝する．

参考文献

[1]石原他：多目的なＩＣカードを共通的に利用するためのミドルウェア(1)～課題の抽出と，対策およびアーキテクチャの検討～，第59回情報処理学会全国大会 2G-08,1999.