



GlobalPlatformにおける標準化動向

にわの えいかず ごろうまる ひでき

庭野 栄一 / 五郎丸 秀樹

NTTサービスインテグレーション基盤研究所

現在、多様な分野においてICカードの導入が進められており、ここ数年、1枚のカード上に複数のICカードアプリケーションを搭載・管理するための技術が注目を集めてきました。ここでは、このようなマルチアプリケーションICカード管理技術の標準においてもっとも有力な標準化組織の1つであるGlobalPlatformに関する標準化動向を紹介します。

ICカード管理技術

ICカードは1970年代前半に日本とフランスでほぼ同時期に発明され、1990年代終わりには単機能型・単目的利用型から多目的利用型へと技術開発が進展してきました。この多目的利用を実現するための技術がマルチアプリケーションICカード管理技術です。これはアプリケーションや鍵の搭載などのICカードの発行から、ICカード発行後にアプリケーションを追加するための仕組みを提供するものです。この技術を利用すると住民基本台帳カード、Suicaなどの交通系カード、金融におけるキャッシュ・クレジットカード、そしてモバイル通信におけるFOMAカードなど多様なICカードアプリケーションを1枚のカード上に搭載することができるようになります。

GlobalPlatformとは

GlobalPlatform⁽¹⁾はVISAを中心に開発されたOpen Platform (OP)

技術をベースに1999年に設立された、マルチアプリケーションICカード管理システムに関する業界標準化組織です。現在、MasterCardを中心に設立されたMAOSCO⁽²⁾などとともに世界でもっとも有力なICカード標準化組織の1つとなっています。

参加企業をみてみますとGlobalPlatformにはVisa International, MasterCard, JCBなどのクレジット会社, Gemplus, Axalto, 大日本印刷などのカードベンダ, DataCardなどのカード発行機ベンダ, そしてIBMなどのソリューション企業をはじめ、フランステレコム, NTTなどの通信事業者など、多様な業界から世界で約50の企業・機関が会員となっています。

GlobalPlatformは「マルチアプリケーション」を標榜していることもあり、業界中立的な立場で多様な分野に対して標準書の実装・展開を推進しています。特にGlobalPlatformで規定されたカード仕様は、携帯電話に組み込まれている加入者認証用チップSIM/UICC (Subscriber Identity Module/Universal Integrated Circuit Card) に対するアプリケーション管理の標準として、電気通信関連の標準化組織であるETSI/3GPP (European Telecommunication Standards Institute/3rd Generation Partnership Project) に採用されており (ETSI & GSM 03.48, TS 23.048, ETSI & 3GPP SCP TS 102.225/102.226), モバイル通信系ICカードアプリケー

ション管理の業界標準となっています。

またICカードのマルチアプリケーション管理の仕様策定作業が進行しているISO (International Organization for Standardization) 7816-13においても、国内行政系の業界標準策定組織であるNICSS⁽³⁾ (Next generation IC Card System Study group) のフレームワークやMultos仕様⁽²⁾ (前記MAOSCOが仕様規定。現在ライセンスはStepNexus社に移管) とともに、GlobalPlatformのカード仕様が代表的な方式としてAnnexに記載されるに至っています。

GlobalPlatformの組織

GlobalPlatformの組織構成を図1に示します。GlobalPlatformの意志決定機関は理事会 (Board of Directors) ですが、技術統括や戦略マーケティングを統括するためのDirectorがアサインされているのが特徴です。理事会には、選挙で選任されたElected Directors 11名, Strategic Directors 3名, 前述の戦略・マーケティングを統括するExecutive Director 1名, 技術を統括するTechnical Director 1名が存在します。国内からは、Elected DirectorsとしてNTT, 日立 (Treasurer), JCBの3社, Strategic Directorsとして東芝が務めており、またNTT以外の通信事業者としてフランステレコムがElected Director



となっています。

また技術標準の策定組織としてはカードの仕様を規定するカード委員会、カードアクセプタンスデバイス（カードを挿入する端末）仕様を規定するデバイス委員会、カード発行者やアプリケーション提供者（サービス提供者）などサーバ側および全体のアーキテクチャや要件などを定義するシステム委員会があります。

なお最近では、GlobalPlatformユーザの声を反映し、実装や展開を促進していくための組織として、この委員会と理事会の間にAdvisory Councilが設立されました。この組織は委員会と理事会をつなぐための役割も持っており、今後GlobalPlatformにおいて非常に重要な位置付けをなすものと考えられます。

カード委員会

カード委員会はGlobalPlatformにおいてもっとも影響力が強かつ仕様の普及や実装が進んでいる委員会です。本委員会が規定する範囲は、①一般のカード管理コマンド（カード情報取得コマンドや鍵管理コマンドなど）、②カードアプリケーション管理*コマンド、③カードとカード以外のエンティティ間の認証と暗号路を確立するためのセキュアチャネルプロトコル、④カードアプリケーション用のAPI（Application Programming Interface）です。

* カードアプリケーション管理：カード上のアプリケーションのロード、インストールなどライフサイクルを管理する。

カード委員会は2003年3月にカード仕様V2.1.1を策定し、本年3月終わりに3年かけてカード仕様V2.2をリリースしました。カード仕様V2.1.1の特徴は、カードとカード外部のエンティティ（サーバなど）間の共通鍵ベースセキュアチャネルプロトコル（SCP: Secure Channel Protocol）、JavaCardを利用する場合のAPI、SCPに基づくカードアプリケーション管理コマンド、そして、ICカード発行者だけではなくサービス提供者がICカード発行者からの許可を得てICカードアプリケーションをICカード上にダウンロードするためのトークン（許可証）や実行結果であるレシートの形式などを規定していることです。カード仕様V2.2はこの機能に加え、モバイル網およびPKI（Public Key Infrastructure）ベースのSCP、PKIに基づくトークン、レシート、およびカードアプリケーション管理コマンド、そしてMultosのランタイム環境などを追加しています。このようにカード仕様V2.2はPKI認証をベースとしたNICSS方式さらにMultos方式を取り込み、現状では世界でもっとも有力な方式をカバーした仕様となっています。

カード委員会には次の3つのワーキンググループ（WG）があります。

- ① マルチアプリケーションカードに対するカードとアプリケーション管理に関して技術中立な標準の策定を行っているCard Specification WG（Working Group）
- ② カード仕様に対するコンプライアンスを保証するためのガイドラインやプロセス・ツールの定義を行っているCompliance WG
- ③ GlobalPlatformカードのセキュリティ要件の定義やCommon Criteria手法に基づく

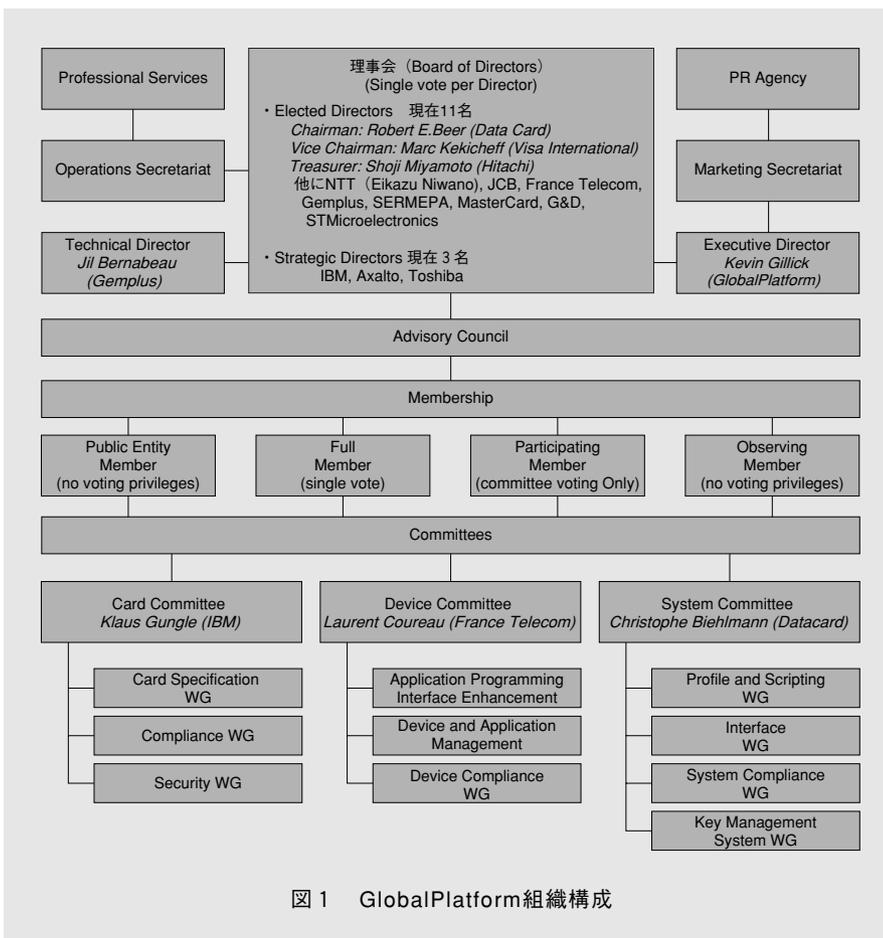


図1 GlobalPlatform組織構成



GlobalPlatform Protection Profileの開発・維持を行っているSecurity WG

デバイス委員会

デバイス委員会では、マルチアプリケーションカードを挿入するPOS端末などのカードアクセプタンスデバイス上のアプリケーション (Stipletと呼ばれる) 開発のためのオープンなアーキテクチャとAPIを定義し、カードアクセプタンスデバイス上のアプリケーション開発と配布を容易にしています。

このための仕組みを実現するプラットフォームとして提供されているものがSTIP (Small Terminal Interoperability Platform) であり、これは共通機能を持つSTIP Core Framework Technologyと、ある特定のカードアクセプタンスデバイスに特有の機能を持つSTIP Profileに分けられます。STIP Core Framework Technologyは、すべてのカードアクセプタンスデバイス (POSなどのリーダ機能を持つ端末) に対する共通のAPIとして、OS利用に関するアクセス制御やカード保有者認証などを提供します。STIP Profileは、特有のカード挿入用デバイスを利用する場合のAPIを規定する仕組みで、現在、携帯電話、EFT-POS端末、FINREAD (欧州の金融系RW (Reader Writer)) 端末用のProfileが規定されています。現在、GlobalPlatform Device/STIP Specifications V2.2が最新版の仕様となっています。

本委員会は1999年にJavaCard ForumのSCAD (Smart Card Accepting Devices) で共通APIとポリシー管理を行うために設立されたSTIPコンソーシアムの技術を基本として設立されたものでしたが、近年STIP

コンソーシアムが本デバイス委員会に統合されて現在に至っています。本仕様の適用分野としては、EFT-POS terminals(STIP EFT-POS Profile)、ATM、交通系端末、自動販売機、携帯電話、PDA、セットトップボックス、ホームバンキング端末、カードリーダ付PCなどが挙げられます。

デバイス委員会には次の3つの組織があります。

- ① グローバル・プラットフォーム・メンバのビジネス要件と機能要件を満たしたAPIの改良を行っているApplication Programming Interface (API) Enhancement WG
- ② デバイスとアプリケーション管理のためのフレームワークの確立を行っている Device and Application Management WG
- ③ 要求された相互運用性レベルを実現するためのGLOBALPLATFORM仕様に準拠したガイドライン、プロセス、およびツールの提供を行っている Device Compliance WG

システム委員会

システム委員会はICカードのバックオフィスのインフラストラクチャに対する機能要件や技術仕様、ガイドを作成すること、そしてコンプライアンステストのためのフレームワークを作成することにあります。そのためにマルチアプリケーションICカードのインフラストラクチャにかかわるすべてのアクタ (カード発行者やアプリケーション提供者などのプレイヤー) に関する役割や責任モデルを規定するとともに、アクタ間のメッセージング・データ交換にかかわる参照仕様、鍵管理に対する要件、ICカードのパーソナリゼーションに対

するガイドを規定しています。

システム委員会には次の4つのWGがあります。

- ① ICカードのカスタマイズのためのオープンな標準の策定 (特にXMLとECMAScriptを使ったデザインを含む) を行っている Profile and Scripting WG
- ② カードとカード内部のライフサイクルを含む全般的なシステムアーキテクチャの定義を行っている Interface WG
- ③ 主として相互運用性に基づくシステム・コンプライアンス・プログラムの定義を行っている Systems Compliance WG
- ④ 鍵管理システム間のインタフェースと鍵を共有しているシステム間の相互運用性を定義している Key Management System WG

他ICカード関連組織との協調

GlobalPlatformはICカード業界にかかわる多くの世界中の標準化関連機関との協調を行っています (図2)。例えば、行政系の連携に関してAICF (Asia IC Card Forum、日・韓・中・シンガポールの機関で構成) やGCF (Global Collaboration Forum、日・欧・米の機関で構成)、NICSS、NIST (National Institute of Standards and Technology)、そしてモバイル系についてはOMTP (Open Mobile Terminal Platform) やETSI、その他Java Card Forum、Smart Card Allianceなどです。

導入事例

GlobalPlatformのスマートカードの導入は2004年末には7000万枚に

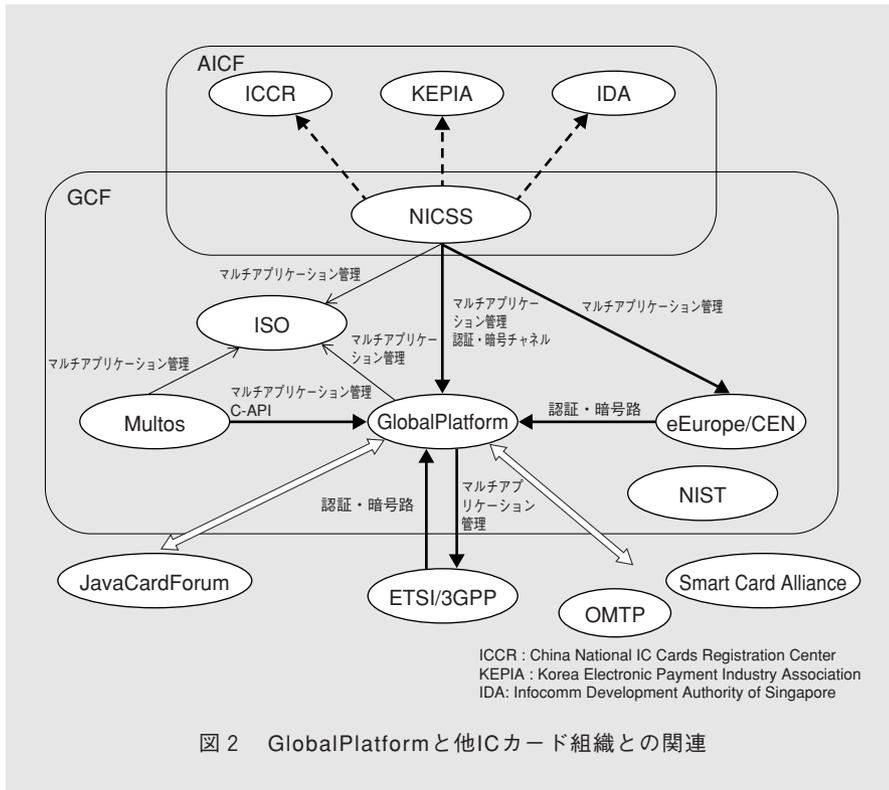


図2 GlobalPlatformと他ICカード組織との関連

NICSSコラボレーションEG (Expert Group) の主査 (現在双方とも庭野が担当) としてGlobalPlatformとの協調を図ってきました。その結果としてこのフレームワークはGlobalPlatformカード仕様V2.2に採用され⁽⁴⁾、⁽⁵⁾、共通鍵ベースのGlobalPlatform方式 (カード仕様V2.1.1)、Multos方式とともに世界の主要方式の1つとして認知されるに至っています。

そこで我々は、今後もこのようなICカード標準化組織とのPKI認証に基づくマルチアプリケーション管理によるオープン・ダイナミックかつセキュアなICカード管理の推進と協調を通じて、誰もがいつでもどこでも簡単に安全な情報通信サービスが受けられるような電子社会を実現していきたいと考えています。またこの実現に向けて国内のe-Japan (新IT改革戦略) やu-Japanの構想、および世界中のICカードシステムの相互接続・連携に対して貢献を図っていきたく考えています。

■参考文献

- (1) <http://www.GlobalPlatform.org/>
- (2) <http://www.multos.com/>
- (3) <http://www.nicss.or.jp/>
- (4) <http://www.globalplatform.org/pressreleaseview.asp?id=357>
- (5) <http://www.globalplatform.org/pressreleaseview.asp?id=380>

達し、GSMカードに至っては6億5000万枚が発行されています。例えば、シティバンクや三井住友カード、韓国のテレコム企業であるSKテレコム・KTコーポレーション、モスクワソーシャルカード、米国国防総省の公務員カードなど金融・医療・ID (行政)・通信など他分野にわたって世界的に導入が進んでいます。

業界標準の1つでもあります。このようにPKI認証をサポートしたことにより、国民IDカード・市民カードなどのID系や電子行政系においても今後有力な標準となっていくと考えられます。最近電気通信分野において次世代通信網 (NGN: Next Generation Network) の議論が盛んですが、同標準化作業においてはSIM仕様の適用が議論されていますので、将来は従来のモバイル網だけではなく固定網への適用が進んでいくかもしれません。さらにデバイス委員会で規定した仕様の実装が開始されており、今後の展開が期待されます。

このような流れの中、NTTはNICSSにおいてPKIベースのマルチアプリケーション管理フレームワークの規定に中心的な貢献をし、GlobalPlatform設立当初よりGlobalPlatformの理事 (Board of Directors)、および2002年からはNICSSにおけるGlobalPlatform -

今後の動きとNTTの取り組み

現在GlobalPlatformはカード仕様V2.2に関するコンプライアンステスト仕様作成や電子行政系向けのユーザガイドの作成と並行して、IDや行政系市場への展開を図ろうとしています。このために、Advisory Council内にシステムインテグレータと行政のタスクフォースを設立しています。GlobalPlatformはすでにモバイル通信における業界標準であり、またVOPの流れを汲む将来的に金融系でもっとも有力な