

コンテンツ配信・モバイルコマース用の セキュアマルチメディアカード

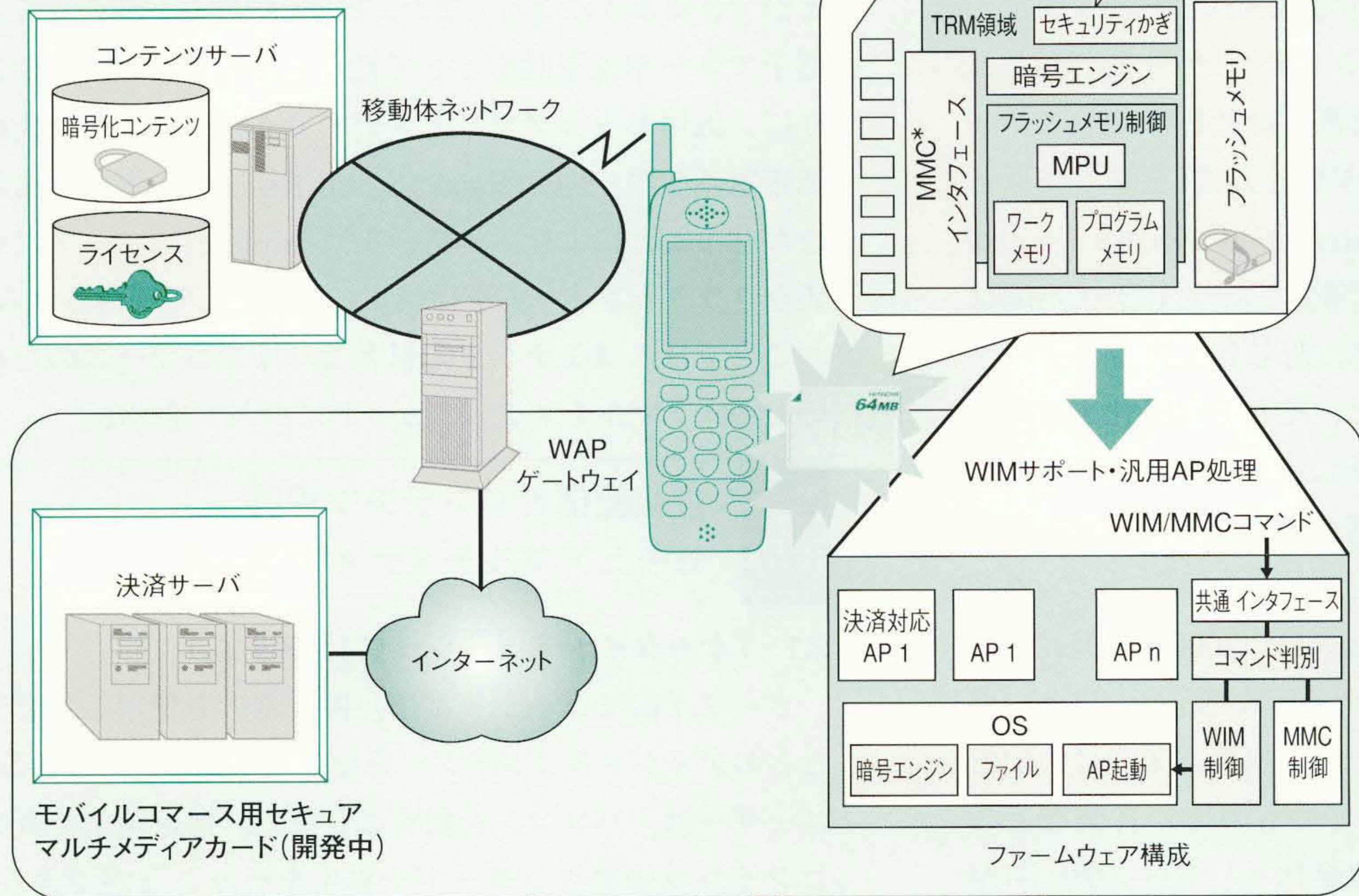
Secure MultiMediaCard for Content Distribution and Mobile Commerce

三宅 順 Jun Miyake

常広隆司 Takashi Tsunehiro

石原晴次 Haruji Ishihara

コンテンツ配信用セキュアマルチメディアカード



注：略語説明ほか

WAP (Wireless Application Protocol)

TRM (Tamper-Resistant Module)

MMC (MultiMediaCard)

MPU (Microprocessing Unit)

WIM (WAP Identity Module)

AP (Application)

OS (Operating System)

*MMC (MultiMediaCard) は、独Infineon Technologies AGの商標である。

モバイル ネットワーク サービスのセキュリティニーズに対応するセキュアマルチメディアカード

インターネットや携帯端末などのネットワークを介したコンテンツ配信をはじめ、モバイルコマースなどさまざまなサービスが展開されていく。セキュアマルチメディアカードは、大容量フラッシュメモリに加え、これらのサービスに不可欠なセキュリティニーズに対応する機能を提供する。

音楽データをはじめとする、ネットワークを介したデジタルコンテンツの配信がすでに始まっている。それに伴い、不正コピーなどを防止するコンテンツ保護技術が重要になってきた。

2000年11月に、世界に先駆けて携帯電話によるデジタル音楽配信サービスがわが国で開始された。このサービスには、「ケータイdeミュージック」のシステムと、日立製作所のコンテンツ保護セキュアマルチメディアカードが採用されている。これは、三洋電機株式会社、富士通株式会社、および日立製作所が共同開発したコンテンツ保護技術に基づくものである。この記録メディアは、大容量フラッシュメモリに加えて、公開かぎ暗号方式に基づいたセキュリティ機能を内蔵している。

さらに現在、モバイルコマースなど汎用に適した次世代のセキュアマルチメディアカードを開発中である。汎用セキュアマルチメディアカードは、WAPフォーラムで定義されているWIM (WAP Identity Module) 機能を内蔵し、ICカードと同様のユーザー認証機能を実現する。ユーザーはこの汎用セキュアマルチメディアカードにデジタルコンテンツをダウンロードするだけでなく、同カードで支払いも済ませることができるようになる。日立製作所のセキュアマルチメディアカードでは、コンテンツ保護からモバイルコマースまで、ネットワークを介したさまざまなサービスに不可欠なセキュリティニーズに対応し、シームレスなソリューションを提供する。

1 はじめに

インターネットや携帯電話の普及により、いつでもどこでも必要なデータを入手することが可能な環境が整いつつある。このような状況下で、ネットワークを介した

デジタルコンテンツの配信事業が、大きな成長分野として期待されている。その中でも特に、音楽配信サービスは、「キラーアプリケーション」として多くの企業が参入を計画している。

一方、ユーザー間の違法コピーソフトウェアが流行す

るなど、著作権保護の面からの合法的なデジタルコンテンツ配信の普及は十分に進んでいなかった。デジタルコンテンツの不正利用を排除する著作権保護のための基本要件を、SDMI(Secure Digital Music Initiative)¹⁾が規定している。これを満たし、合法的な配信ビジネスを成功させるために、著作権を守るためのデジタルコンテンツの保護技術が不可欠である。

日立製作所は、1999年に三洋電機株式会社および富士通株式会社と共同で音楽配信システム「ケータイdeミュージック」を企画し、著作権保護技術としてPKI(Public Key Infrastructure：公開かぎ暗号方式)を基本技術としたUDAC-MB(Universal Distribution Access Control with Media Base)規格を共同開発した²⁾。UDAC-MBは超流通の概念に基づいており³⁾、暗号化した音楽データなどのデジタルコンテンツと、それを復号化するためのかぎであるライセンスを別々に流通させることができる技術である。これにより、著作権保護とユーザーの使いやすさを同時に実現している。「ケータイdeミュージック」規格を採用した音楽配信サービスは、2000年11月にDDIポケット株式会社のPHS向けサービス“Sound Market”として本格的に開始した。これは、携帯端末向けの配信サービスとしては世界で初めてのもので、音楽などのデジタルデータ格納用の記録媒体として日立製作所が開発、製品化したコンテンツ保護機能付きセキュアマルチメディアカードが採用されている(図1参照)。このセキュアマルチメディアカードは、標準のマルチメディアカード⁴⁾に対して上位互換性を持ち、さらに、公開かぎ方式を用いたセキュリティ機能を内蔵したものである。

さらに現在は、EC(Electronic Commerce)やモバイルコマースなど汎用用途に適した次世代のセキュアマルチメ

ディアカードを開発中である。この汎用セキュアマルチメディアカードは、WAPフォーラム⁵⁾で定義されているWIM[WAP(Wireless Application Protocol)Identity Module]の機能を内蔵したもので、ICカードと同様のユーザー認証機能を実現する。したがって、ユーザーは、音楽などのデジタルコンテンツをダウンロードするだけでなく、同カードを使ってその支払いまで済ませることができるようになる。また、Mondexカード^{※1)}のように電子マネーや電子財布として使うこともできる。このように、汎用セキュアマルチメディアカードは、次世代の携帯電話やPDA(Personal Digital Assistant)などと組み合わせることにより、本格的なM(Mobile)コマースに必要なプラットフォームを提供するものとして期待される。

ここでは、コンテンツ配信とモバイルコマースのためのセキュアマルチメディアカードについて述べる。

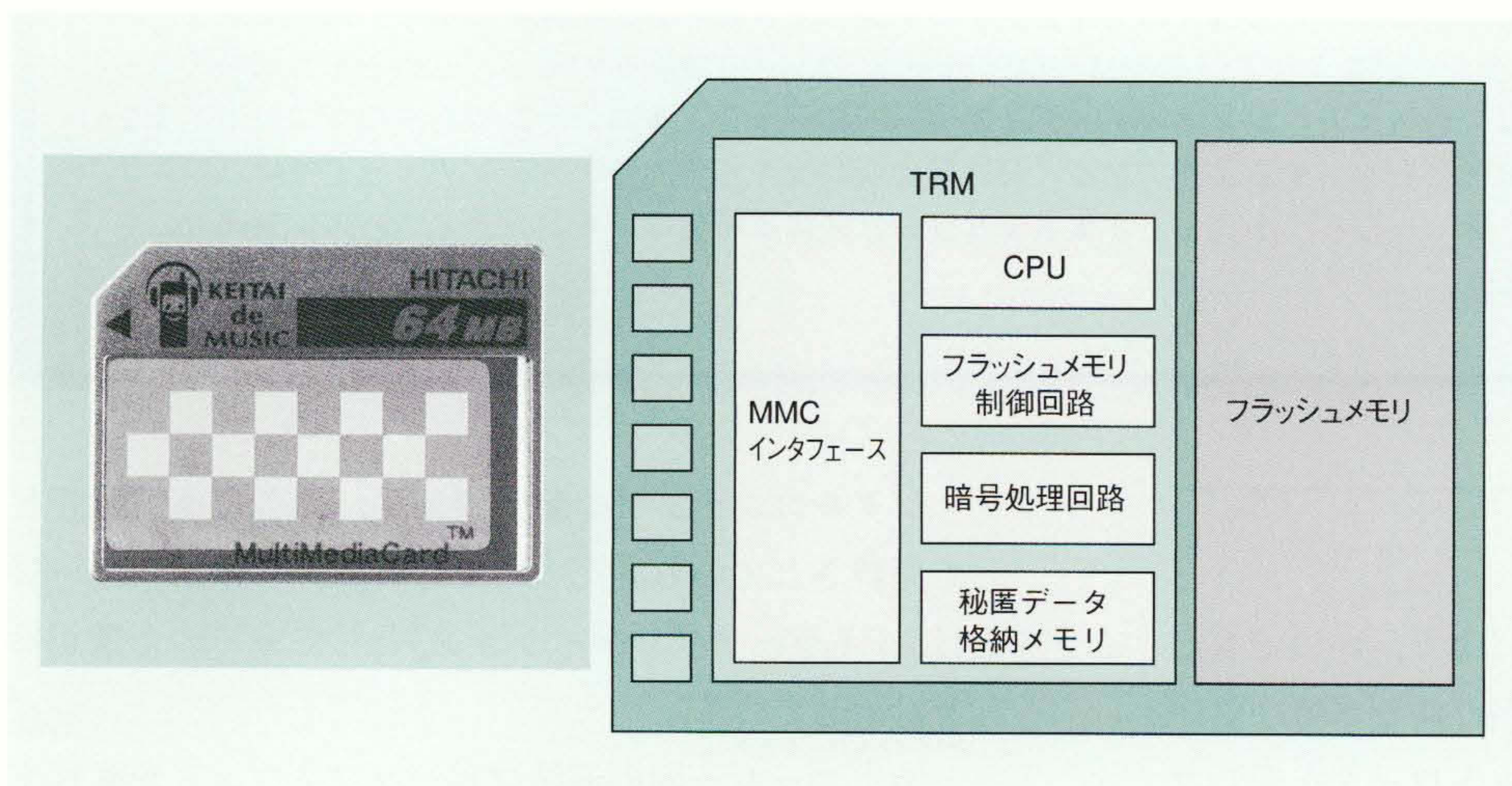
2

音楽配信とコンテンツ保護 セキュアマルチメディアカード

2.1 「ケータイdeミュージック」システム

ケータイdeミュージックは、携帯端末を使用して音楽などのデジタルコンテンツを配信するシステムである。ユーザーは、パソコンを使うことなく、携帯端末で音楽コンテンツのダウンロードや再生を行うことができる。暗号化されたコンテンツとそのライセンス(楽曲の復号のためのかぎ)は、セキュアマルチメディアカードに格納される。暗号化されたコンテンツは通常のファイルとしてフラッシュメモリへ格納され、ライセンスはTRM

※1) Mondexは、Mondex International Limitedの登録商標である。



注：略語説明

TRM(Tamper-Resistant Module)

MMC(MultiMediaCard)

CPU(Central Processing Unit)

図1 セキュアマルチメディアカードの外観(左)と機能ブロック図

セキュアマルチメディアカードは、音楽などコンテンツ配信に使用されている。カード自体に暗号処理機能を内蔵し、かぎなどのセキュリティ関連情報の格納と処理をカード内のTRM領域内で実行することにより、著作権保護などに必要なコンテンツ保護機能を実現している。現在、32 Mバイトと64 Mバイトの容量をラインアップしている。

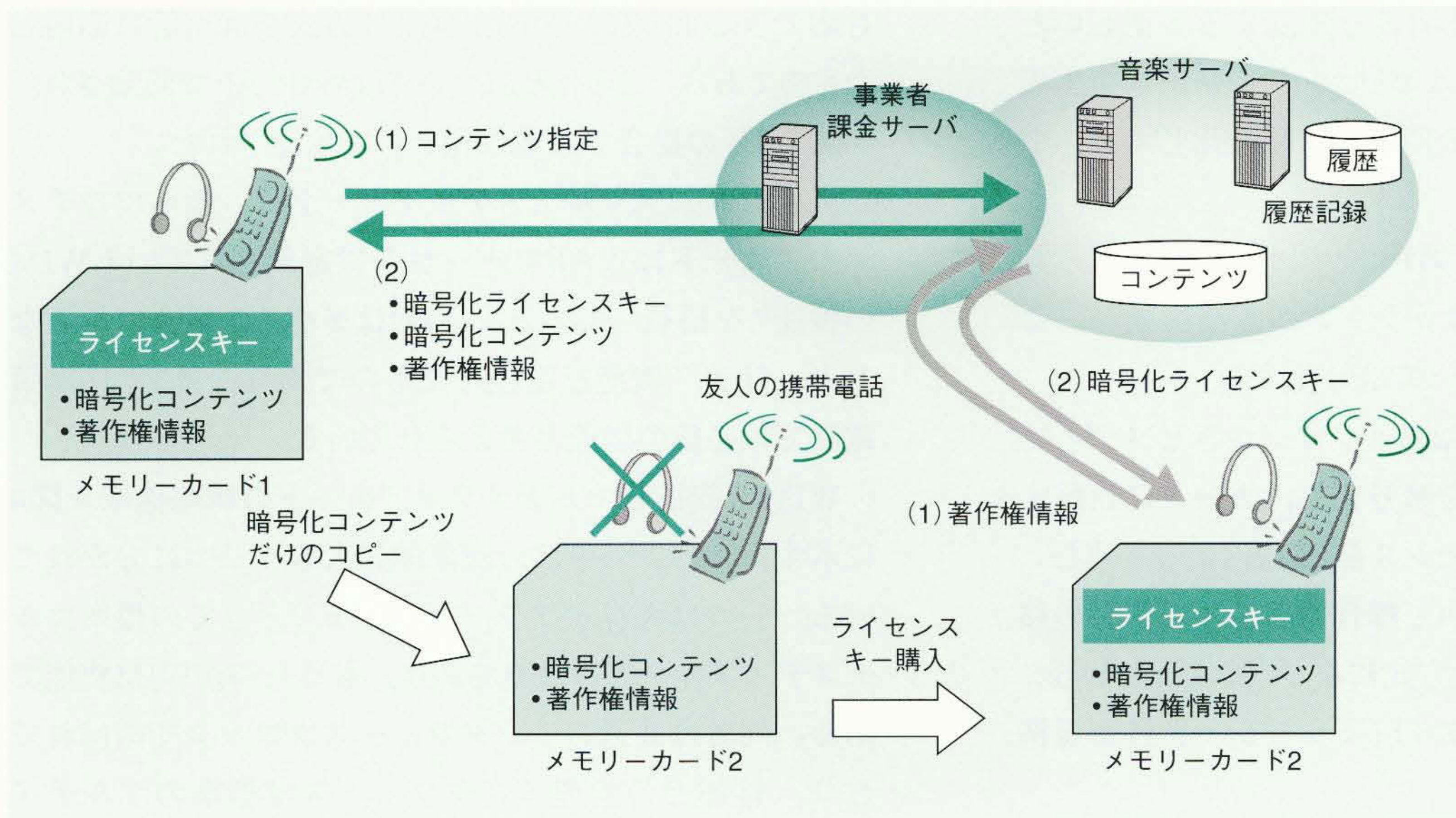


図2 「ケータイdeミュージック」のシステム概要

PKIを基本技術とし、超流通の概念に基づいた技術規格UDAC-MBにより、暗号化コンテンツとそれを復号するかぎを別々に配信することができる。これにより、暗号化コンテンツはカードから別の個人のカードへ合法的にコピーでき、コピーしたカードユーザーは、ライセンスかぎだけを携帯電話で購入することで復号、再生ができる。

(Tamper-Resistant Module) 領域に安全に格納される。これは、超流通理論に基づいた配信方式であり、コンテンツとライセンスを別々に配信することができるものである。暗号化されたコンテンツのコピーは自由であるが、ライセンスのコピーはできず、カードからカードへの移動だけができる。ユーザーは、コピーした暗号化コンテンツのライセンスを別に購入して再生する。ケータイdeミュージックのシステム概要を図2に示す。

2.2 コンテンツ保護セキュアマルチメディアカード

セキュアマルチメディアカードのブロック図を先の図1に示す。セキュアマルチメディアカードには、標準のマルチメディアカードの機能に加えて、公開かぎ暗号方式に基づいたセキュリティ機能が実装されている。こ

のカードには、相手の装置を認証する機能、暗号化・復号化機能、および秘匿データ格納機能を持たせている。これらの機能は、LSI内部の高いセキュリティ機能を持つTRM内に配置されており、外部からの不法なアクセスに対して保護されている。

ライセンスをサーバから取得するプロトコルを図3に示す。カード製造者は、あらかじめ認証局から発行されたカードの、公開かぎに対する証明書をカードに書き込む。かぎ情報とCRL (Certificate Revocation List: 証明書失効リスト) も同様にTRM領域に書き込む。ライセンス取得は、以下のステップで行われる。

(1) ステップ1: メディア(カード)の証明書がサーバに送信される。

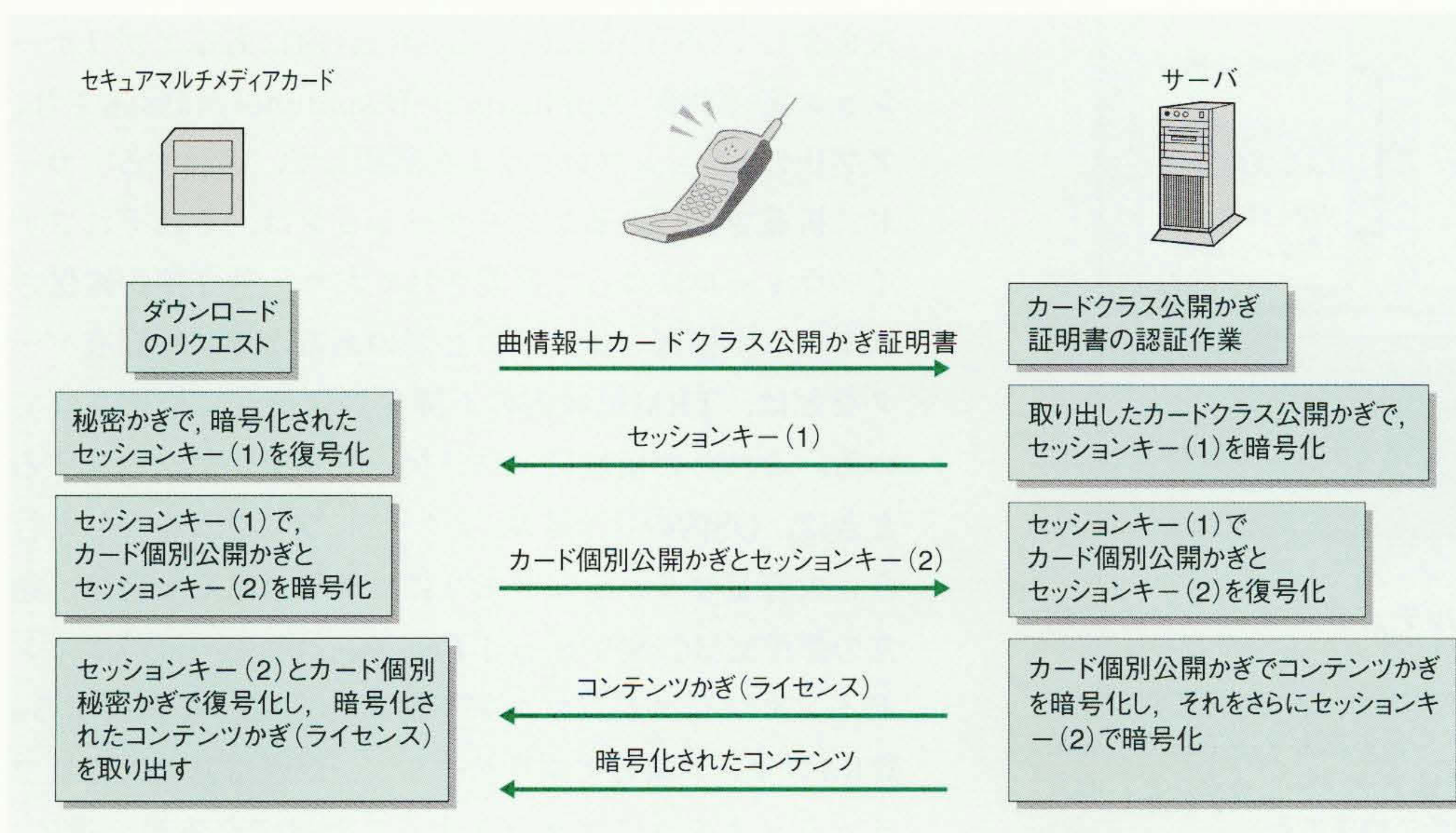


図3 ライセンス取得プロトコルの概要

音楽などの暗号化コンテンツのライセンスかぎをサーバから取得する手順概要を示す。PKI方式に基づいて、配信先の記録メディアとセキュアマルチメディアカードをサーバが認証後、公開かぎ、およびセッションかぎで暗号化されたコンテンツごとの暗号かぎを取得する。

(2) ステップ2：サーバが証明書を確認する。正しいと確認された場合、サーバは第1セッションかぎを生成し、これをメディアクラス公開かぎで暗号化してカードに返信する。

(3) ステップ3：カードは、第1セッションかぎを復号して取り出す。さらに、第2セッションかぎを生成し、これを第1セッションかぎを使って暗号化する。

(4) ステップ4：サーバは第2セッションかぎとメディア固有公開かぎでライセンスを暗号化し、カードに返信する。カードは、取得したライセンスをTRM内に書き込む。

再生時のライセンス読み出し操作時とライセンスの移動時も、同様の公開かぎ暗号方式に基づいて実行される。プロトコルの詳細は、ケータイdeミュージック技術規格書⁶⁾に定義されている。

3

モバイルコマース用の 汎用セキュアマルチメディアカード

3.1 WIM機能搭載マルチメディアカード

コンテンツ保護セキュアマルチメディアカードがコンテンツ保護の用途に最適化したセキュリティ機能を持っているのに対し、汎用セキュアマルチメディアカードの仕様は、モバイルコマースの幅広いアプリケーションに

対応できるように、公開かぎ暗号方式を汎用的に応用したものである。この仕様についてはMMCA⁷⁾で議論され、2001年6月の総会で標準仕様として承認された。

汎用セキュアマルチメディアカードは、標準マルチメディアカードにWAPフォーラムで定義されているWIMの機能⁸⁾を搭載している。WIMはモバイル機器に最適なセキュリティ機能を定義したものであり、第3世代携帯電話では必須の機能と考えられている。

WIM機能搭載マルチメディアカードの概略構成を図4に示す。カードの中は、機能的に大きく二つに分かれている。一つは大容量フラッシュメモリとしての標準マルチメディアカードの機能であり、もう一つがWIM機能である。両者は共通のインタフェースブロックで結ばれており、外部との論理インタフェースは標準のマルチメディアカードと同じ仕様となっている。WIM機能を使用するためのWIMコマンドは、マルチメディアカードの標準コマンドの拡張として定義する。実際のWIMコマンドはISO7816で定義されたコマンド^{9), 10)}であり、これによって実現するのは、ICカードと同等の機能である。したがって、WIM機能を実装した汎用セキュアマルチメディアカードは、現在、銀行決済などに使用されているICカードと同様の使い方が可能である。これを搭載したモバイル機器は、そのままモバイルコマース端末として使用することができる。

3.2 ソフトウェア構造

WIM機能搭載セキュアマルチメディアカードのソフトウェア構造を図5に示す。WIMコマンドも標準マルチメディアカードのコマンドも、共通インタフェースを通してカードに入力される。WIMコマンドは専用インタフェースを介してOS(Operating System)内にあるアプリケーション実行制御(Application Dispatcher)に転送され、アプリケーションプログラムを選択して、起動する。カードに搭載されているアプリケーションは、それぞれファイアウォールによって保護されており、独立性が確保されている。秘密を保持する必要があるかぎ類や固有データなどは、TRM領域内の不揮発性メモリに格納されている。これらの領域にアプリケーションがアクセスするときは、OS内のファイルアクセスシステムを介して行う。大容量フラッシュメモリにアクセスする場合は、通常の標準MMC/SPI(Serial Peripheral Interface)コマンドインタプリタがコマンドを解釈し、実行を制御する。WIMコマンド側のアプリケーションが通常側の大容量フラッシュメモリにアクセスすることはできるが、逆に、

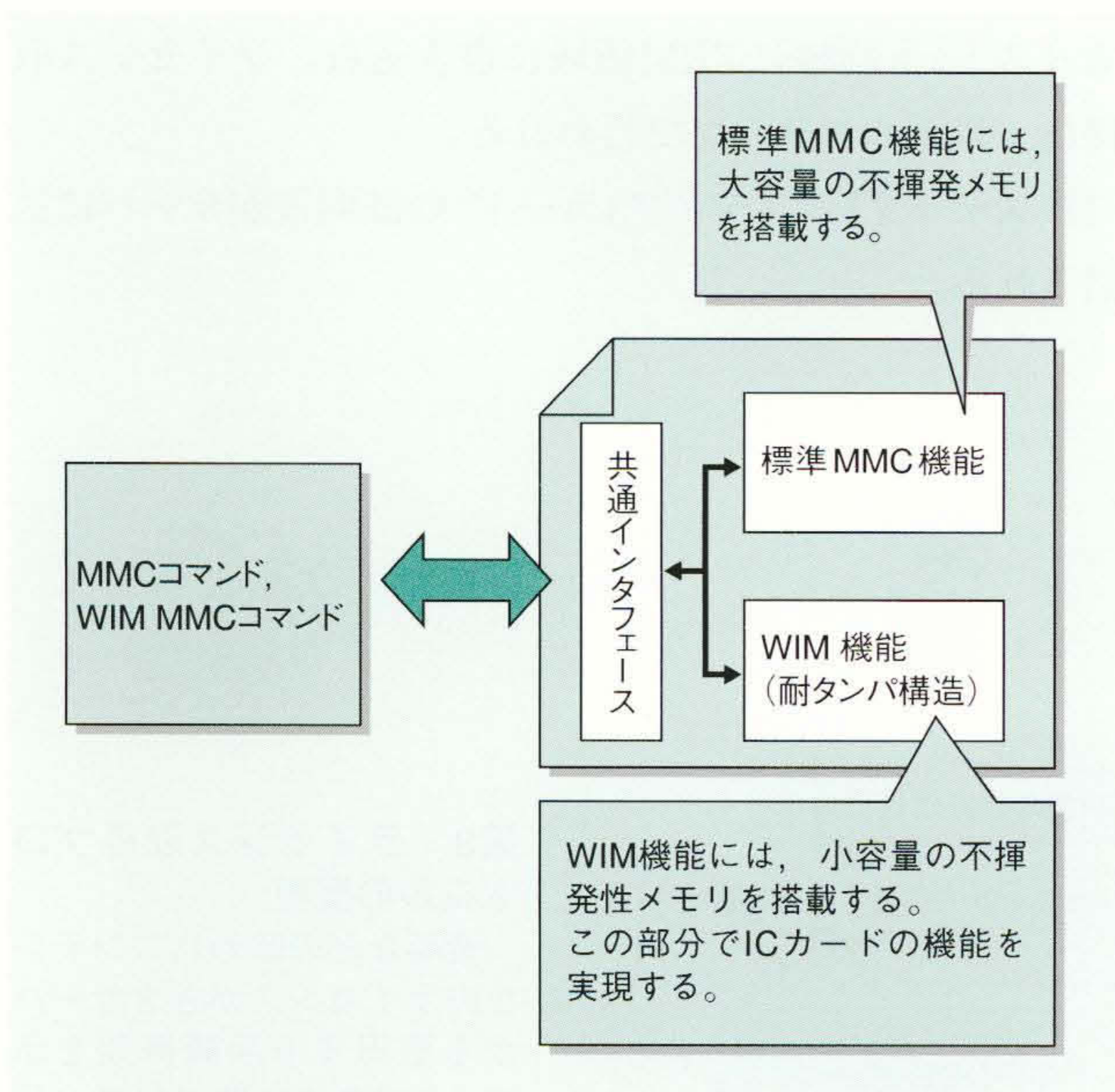
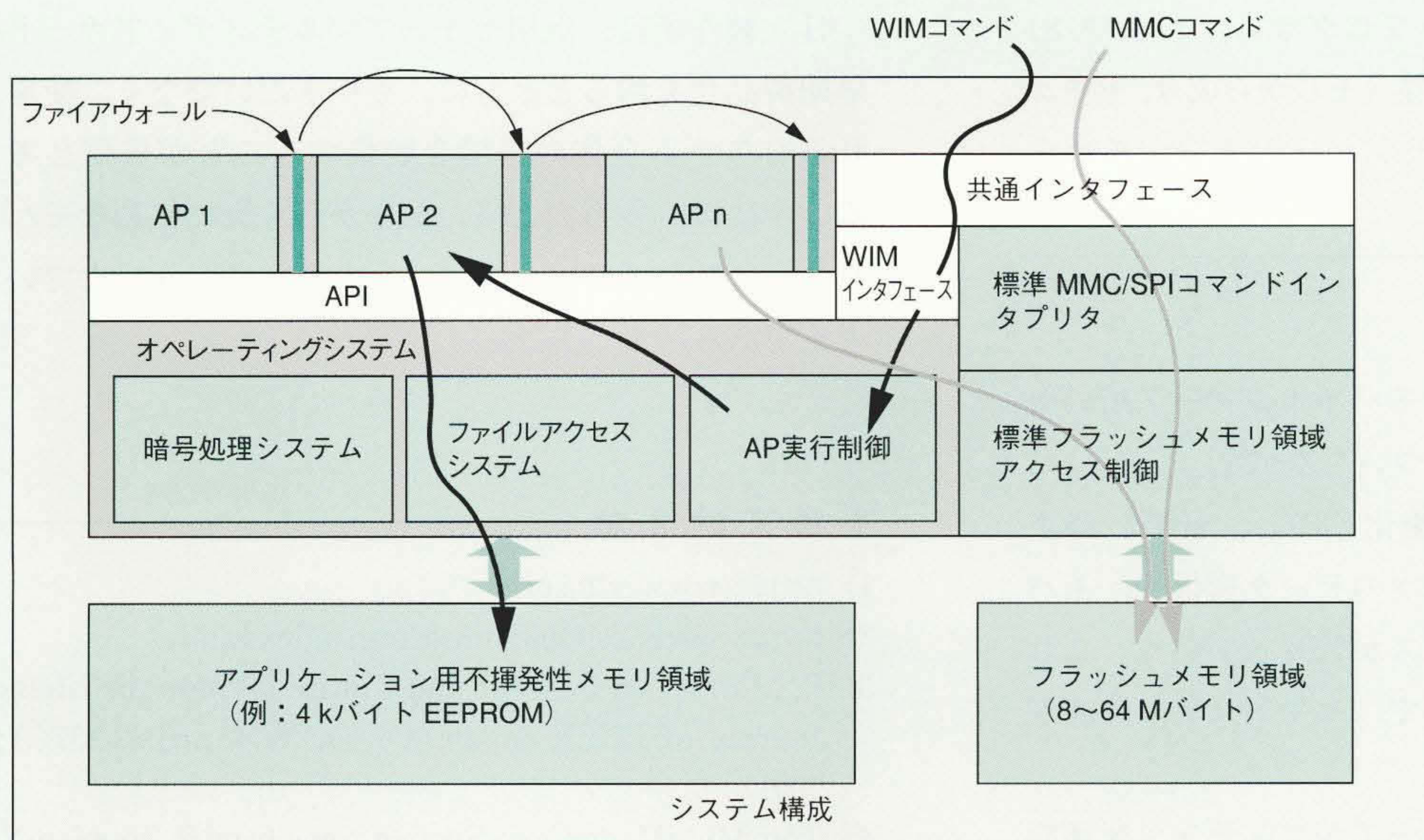


図4 WIM機能搭載セキュアマルチメディアカードの概略構成

モバイルコマースなどの幅広いアプリケーション用にWIM機能を搭載したのが汎用セキュアマルチメディアカードである。従来のマルチメディアカードと同じ大容量フラッシュメモリと、ICカードと同等の機能を実現するWIM機能で構成する。



注：略語説明
 AP (Application)
 API (Application Programming Interface)
 EEPROM (Electrically Erasable Programmable Read-Only Memory)

図5 WIM機能搭載セキュアマルチメディアカードのソフトウェア構造

従来の標準MMCコマンドと新規WIMコマンドの入力に対応する。共通インタフェースを介して入力された後、WIMコマンドは、専用インタフェースを介して、それぞれ対応するアプリケーションを選択し、起動する。標準MMCコマンドは大容量フラッシュメモリにアクセスし、WIMコマンド側のアプリケーションからも大容量フラッシュメモリにアクセスできる。カードには複数のアプリケーションが搭載され、それぞれファイアウォールによって保護され、独立性を確保している。

標準のマルチメディアカードのコマンドがTRM内の不揮発性メモリ内にアクセスすることはできない。OSにMULTOS^{※2)}を採用しMondexアプリケーションを搭載すれば、セキュアマルチメディアカードでMondexの電子マネーを扱うことができる。したがって、カードを搭載した携帯端末で電子財布機能を実現することができる。

※2) MULTOSは、Mondex International Limitedの登録商標である。

3.3 ハードウェア構造

WIM機能搭載セキュアマルチメディアカードの機能ブロックを図6に示す。カードは、コントローラとフラッシュメモリの二つの要素で構成している。フラッシュメモリは非セキュアなデータだけを扱うので、通常のフラッシュメモリをそのまま使うことができる。コスト低減上の効率もよい。

コントローラは、(1) 全体の制御用CPU、(2) 一時記憶用RAM(Random Access Memory)、(3) システムROM(Read-Only Memory)、(4) 暗号処理回路、(5)

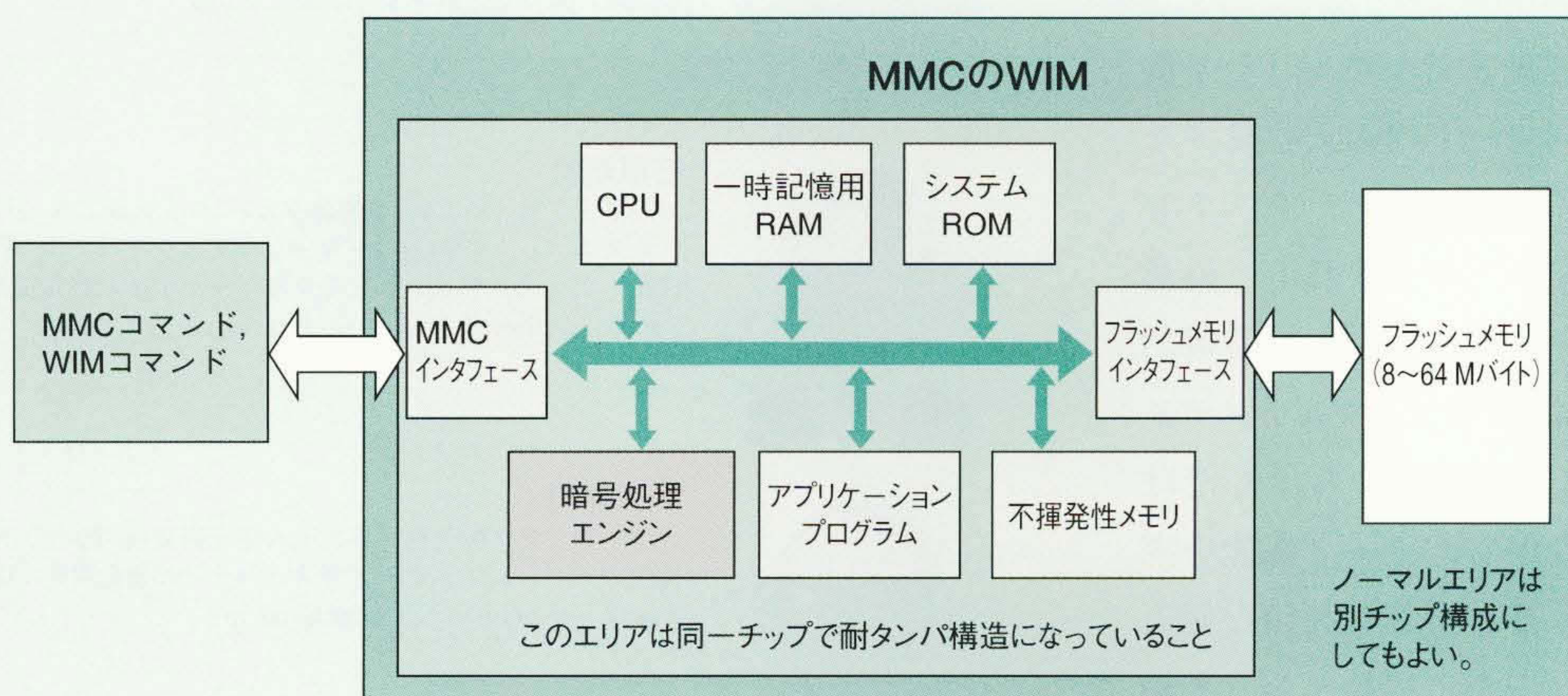


図6 WIM機能搭載セキュアマルチメディアカードの機能ブロック図

WIM機能搭載セキュアマルチメディアカードの基本ハードウェアは、非セキュアデータだけを扱う通常のフラッシュメモリと、耐タンパ構造のコントローラで構成する。

外部とのインタフェース回路，(6)フラッシュメモリ制御回路，(7)アプリケーションプログラム，および(8)秘密情報を記憶しておく不揮発性メモリから成り，セキュリティレベルの高い耐タンパモジュール構造が求められる。

4 おわりに

ここでは，コンテンツ配信とモバイルコマース用のセキュアマルチメディアカードについて述べた。

今後，移動体通信基盤の高速化に伴い，音楽，静止画，動画などの大容量コンテンツのデータ通信や，モバイル環境でのさまざまなサービスが普及していく。これらのサービスのいろいろな局面で，セキュリティ機能がますます不可欠になってくる。

中でも重要なセキュリティニーズがコンテンツ保護であり，この機能を実装したセキュアマルチメディアカードを製品化した。これはすでに，世界に先駆けてスタートした，携帯電話の音楽配信サービスに採用されており，PKI方式を実装した最初のフラッシュメモリカードである。

PKI方式を採用した利点は，高いセキュリティを実現しているという点だけでなく，ユーザーの使い勝手のよさという点にもある。ユーザーは，これにより，通信基盤と既存のリアルな流通の両方を組み合わせた，超流通の柔軟な配信サービスが受けられる。最も手軽な流通は，ユーザー自身による友人どうしでの合法コピーである。これであれば，大容量コンテンツデータを通信コストをかけずに，いわゆる“Peer to Peer”で入手することができる。

次世代の汎用セキュアマルチメディアカードでは，PKI方式によるセキュリティ機能を拡張することにより，ユーザー認証機能を実現する。

コンテンツ保護からユーザー認証までセキュリティ機能をサポートすることにより，同カード内の大容量メモリの用途がさらに広がるとともに，単なるデータストレージにない，付加価値のある使いみちが生まれる。外形寸法もICカードと比べて小さく，小型化の進む携帯電話のスロットに収まる。ユーザーは，セキュアマルチメディアカードをスロットに入れた携帯電話を持ち歩くだけで，そのままネットワークにつながるICカード機能を携帯できることになる。当然，ユーザー自身も大切な個人情報やアドレス帳などをこの中に安全に格納することができ，電話機を買い替えるときもカードを入れ替えるだ

けで済む。

日立製作所は，汎用セキュアマルチメディアカードの早期製品化を図るとともに，カードだけでなく，使用されるシステム全体の環境を整備することが重要と考える。今後は，多方面と協力しながら，真に便利なモバイルサービスとプラットフォームの提案に取り組んでいく考えである。

参考文献ほか

- 1) <http://www.sdmi.org/>
- 2) <http://www.keitaide-music.org/index.html>
- 3) R. Mori : The Concept and Future of Superdistribution, Journal of IEICE Japan, Vol.84, No.4, pp.233-237 (Apr. 2001)
- 4) The MultiMediaCard System Specification Version 2.11 Official Release c June 1999, MMCA Technical Committee
- 5) <http://www.wapforum.org/>
- 6) Keitaide-Music Technical Specification Ver. 1.0, December 2000, Keitaide-Music Consortium
- 7) <http://www.mmca.org/>
- 8) Wireless Application Protocol Identity Module Specification, WAP-198-WIM, Version 18-Feb-2000
- 9) Information Technology - Identification Cards - Integrated Circuit(s) Cards with Contacts, Part 4, Interindustry Commands for Interchange, ISO/IEC 7816-4
- 10) Identification Cards - Integrated Circuit(s) Cards with Contacts, Part 8, Security Related Interindustry Commands, ISO/IEC 7816-8

執筆者紹介



三宅 順

1984年日立製作所入社，半導体グループ システムメモリビジネスユニット プロダクトマーケティングチーム 所属
現在，次世代フラッシュメモリのマーケティングに従事
E-mail : miyake-jun @ sic. hitachi. co. jp



石原晴次

1972年日立製作所入社，半導体グループ システムメモリビジネスユニット プロダクトマーケティングチーム 所属
現在，次世代フラッシュメモリのマーケティングに従事
E-mail : ishihara-haruji @ sic. hitachi. co. jp



常広隆司

1978年日立製作所入社，システム開発研究所 第六部 所属
現在，デジタルメディアセキュリティの研究開発に従事
E-mail : tsunehir @ sdl. hitachi. co. jp