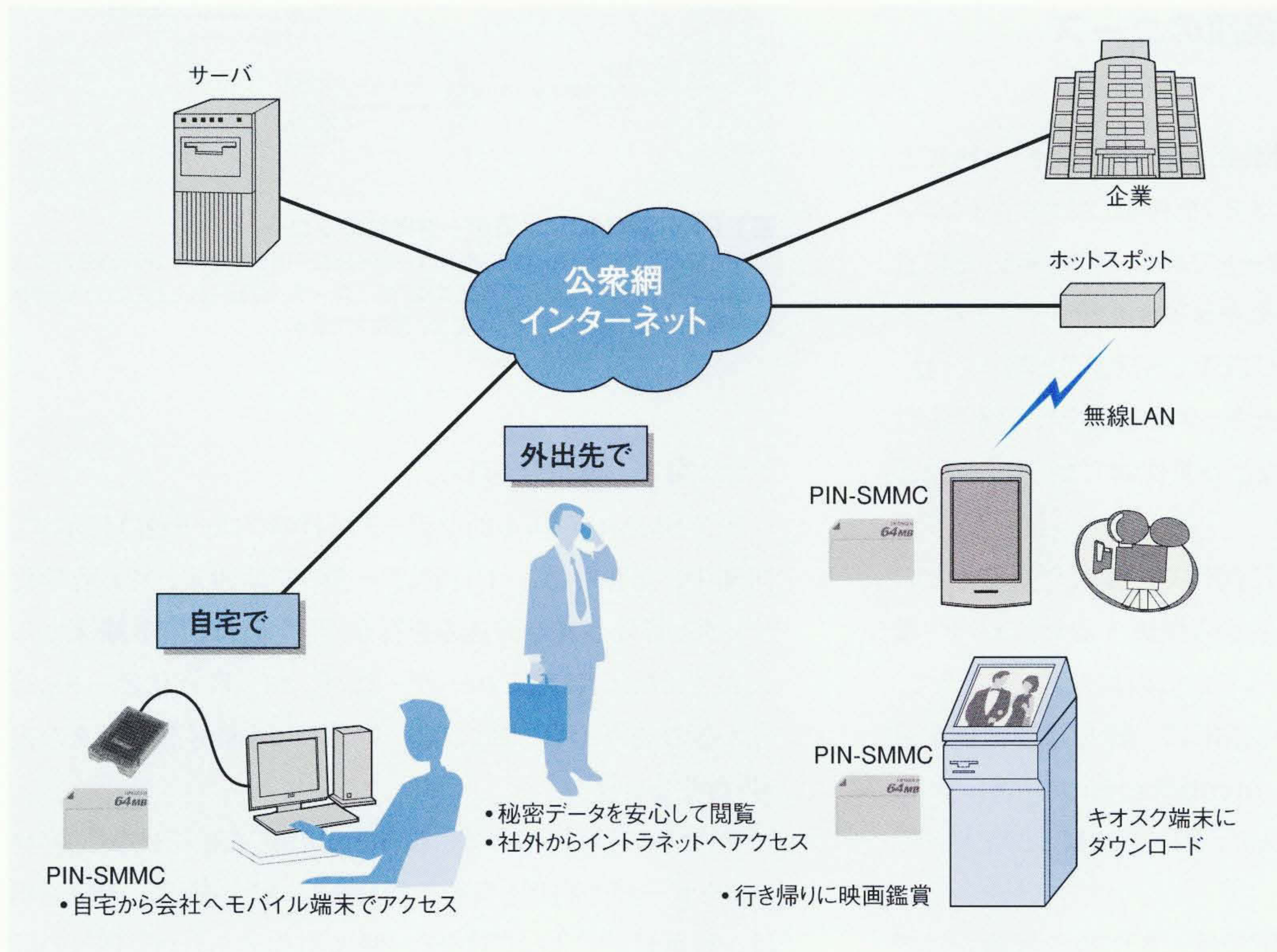


ユビキタス情報社会のセキュリティを支える「PINセキュアマルチメディアカード」

PIN Secure MultiMediaCard to Support the Secure Ubiquitous Information Society

兼平 晃 Akira Kanehira 三宅 順 Jun Miyake 戸塚 隆 Takashi Totsuka



「PINセキュアマルチメディアカード」の利用イメージ

自宅からでも外出先からでも容易に会社の必要なデータにアクセスでき、行き帰りにPDA (Personal Digital Assistant) で映画の鑑賞もできる時代が来る。

注：略語説明

PIN-SMMC (Personal Identification Number—Secure MultiMediaCard)

ユビキタス情報時代のキーワードは「セキュリティ」である。日立製作所は、配信されるコンテンツの著作権を守り、さらに、ユーザーの個人情報や企業の情報を第三者から守る新しいフラッシュメモリカード「PINセキュアマルチメディアカード」を製品化した。

PINセキュアマルチメディアカードでは、セキュアマルチメディアカードと同様に、公開かぎ暗号方式を採用し、コンテンツを保護するとともに、PIN (Personal Identification Number) 認証に成功しないとデータ

が読み出せない機能を実装したことで、第三者の不正アクセス防止と紛失時のデータ保護を可能にする。

このカードをPDAなどのモバイル情報端末のスロットに装着することにより、外交営業員がモバイル環境下で、いつでも、どこでも必要な顧客情報や製品情報にアクセスできるSFA (Sales Force Automation) 用途に威力を発揮する。また、かぎ管理はシステムごとに任されるため、さまざまなセキュリティレベルのシステムに対応することができる。

1 はじめに

ユビキタス情報時代では、いつでもどこでもネットワークにアクセスし、必要な情報を得ることができる。しかし、その便利さと引き換えに、個人や企業の情報が第三者からも容易にアクセスできるという危険性がある。さらに、ネットワークのブロー

ドバンド化やワイヤレス化に伴い、この危険性はますます増大する。

ユビキタス情報時代は、「セキュリティ」ということばが人類有史以来最も重要となる時代であると考えられる。真のセキュリティ環境を実現するためには、ネットワークサーバ、ネットワークライン、情報端末、ストレージカードなどでそれぞれのセキュリティの整備が必要である。しかし、それぞれに厳重なセキュ

リティシステムを実装したのでは、コストや汎用性の観点からユーザーが使いにくくなってしまいます。そのため、情報を得る端末側では、汎用端末を使い、ストレージカードにセキュリティ機能を持たせるシステムが一般的である。

ここでは、コンテンツ保護と個人認証機能を持った新しいフラッシュメモリカード「PINセキュアマルチメディアカード」の概要と、その応用例について述べる。

2 個人・企業データ保護のニーズ

マルチメディアカード(MultiMediaCard[※]：以下、MMCと略す。)は、大容量のフラッシュメモリを利用してさまざまなコンテンツを格納できるストレージカードである。2000年11月に日立製作所が量産を開始したセキュアマルチメディアカード(Secure MultiMediaCard：以下、SMMCと略す。)は、MMCにサーバとデコーダ間でセキュアな通信を行う機能を付与することにより、音楽や画像などの著作物(コンテンツ)保護を可能にしたカードである。

きたるユビキタス情報社会に向けて、個人や企業などのユーザー自身のデータを第三者から保護するセキュリティ機能の要求が、非常に高くなっている。このニーズにこたえて、コンテンツ保護機能を備えたSMMCに、個人認証機能を追加したものが「PIN(Personal Identification Number)セキュアマルチメディアカード」(以下、PIN-SMMCと略す。)である。

この機能により、PIN-SMMCでは、著作物の保護だけでなく、ユーザーが自分自身のデータを暗号化してSMMCに格納できるので、万一カードを紛失した場合にも第三者がデータを取り出すことはできず、カード内の情報を安全に守ることができる。

3 PIN-SMMCの概要と機能

3.1 PIN-SMMCによるデータ保護の流れ

PIN-SMMCでも、SMMCと同様に、PKI(Public Key Infrastructure：公開鍵暗号方式)を採用している。コンテンツは暗号かぎによって暗号化され、SMMCのフラッシュメモリ領域に格納し、このとき用いた暗号かぎを付随情報とともにライセンス形式でSMMCのTRM(Tamper-Resistant Module)領域に保持することにより、コンテンツデータを保護する。PIN-SMMCでは、これに加えて、ライセンスをSMMCから読み出すときに、PIN認証に成功しないと読み出せない機能を実装した。ライセンスの読み出しに成功すると、コンテ

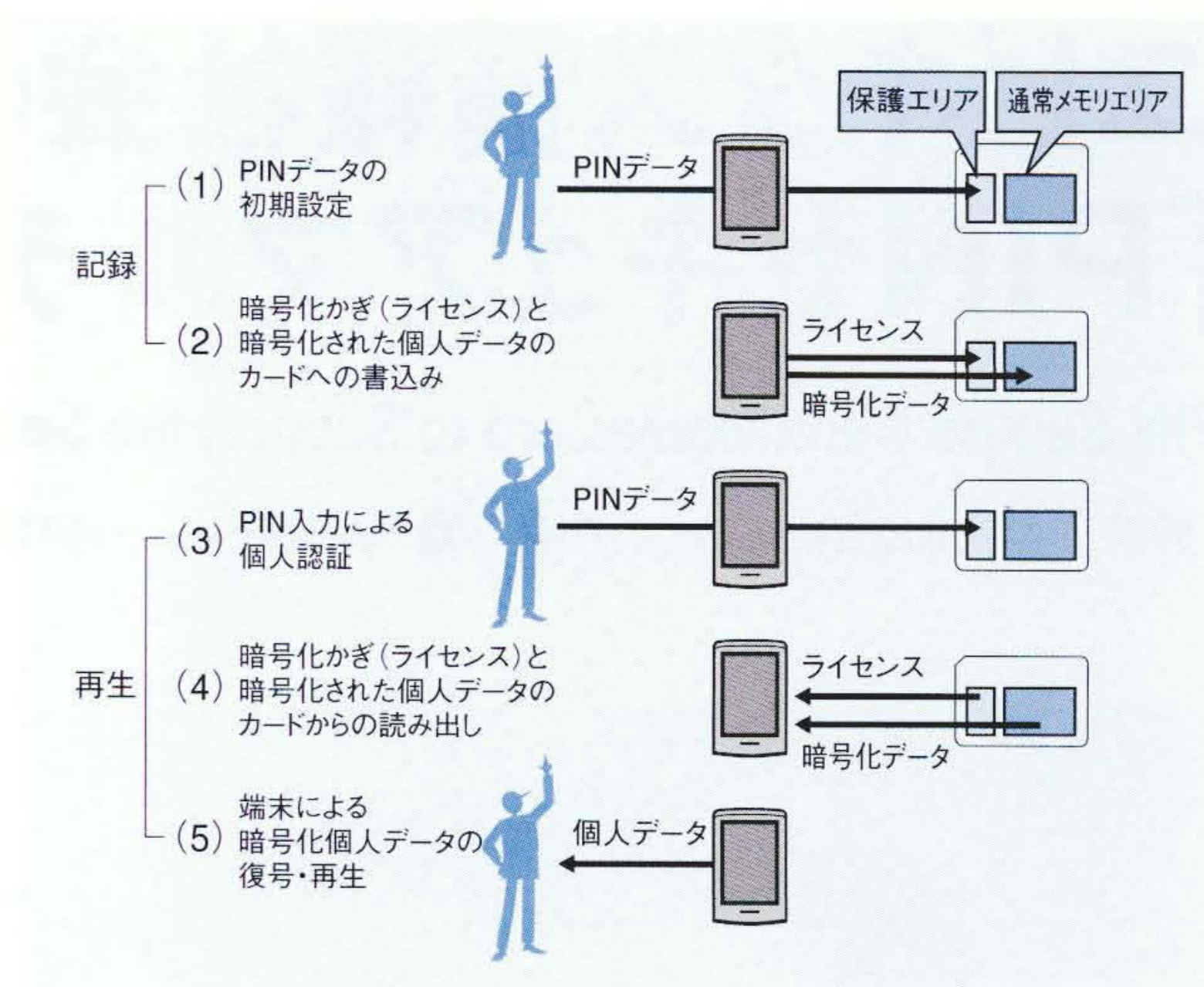


図1 PIN-SMMCによるデータ保護のフロー

PIN-SMMCでは、データ記録時にユーザー認証PINを設定し、これを再生時に入力されるPINと照合する。この検証に成功し、ユーザー認証されたときだけ、暗号化かぎの読み出し、端末でのデータ復号、再生ができる。

ンツは端末上で復号される。

PIN-SMMCの基本的なデータ保護のフローを図1に示す。同図中、記録時は、(1) PINデータの初期設定、(2) 暗号化データと暗号かぎの書き込みを行う。再生時は、(3) 端末から入力されたPINによるユーザー認証、(4) 暗号化データと暗号かぎの読み出し、および(5) 端末による暗号化データの復号・再生を行う。

ライセンスとコンテンツを、端末とSMMCだけではなく、パソコンやサーバの利用も含めて管理を行いたい場合、その運用は、利用目的によって異なる。個人用途であれば、PINの設定と暗号かぎのライセンス管理は個人で行う。一方、企業用途であれば、一般的にライセンスは企業の管理者によって管理され、サーバとパソコンなどのネットワークシステムを使って運営される。社員は、あらかじめ社員の各個人用に管理者がPINを初期設定して支給するPIN-SMMCによってライセンスを受け取る。社員は、そのライセンスを利用して、個人ファイルの暗号化・復号化と自分の属するグループの共有ファイルの暗号化・復号化を行う。これにより、外出先などでも、暗号かぎのライセンスとコンテンツを格納したPIN-SMMCでこれらのファイルを閲覧したり利用することができる。

3.2 PIN-SMMCの構成

PIN-SMMCのブロック図を図2に示す。PIN-SMMCは、(1) MMCの基本構成である「フラッシュメモリ」、(2) ホスト機器からのMMCコマンドに基づいてフラッシュメモリを操作するCPU、(3) フラッシュメモリ制御回路とホスト機器へのMMCインタフェースの各構成部分に対してカードの秘密かぎ・共通かぎなどを格納した「秘匿データ格納メモリ」、および

※) MultiMediaCardは、独Infineon Technologies AGの商標であり、MMCA(MultiMediaCard Association)にライセンスされている。

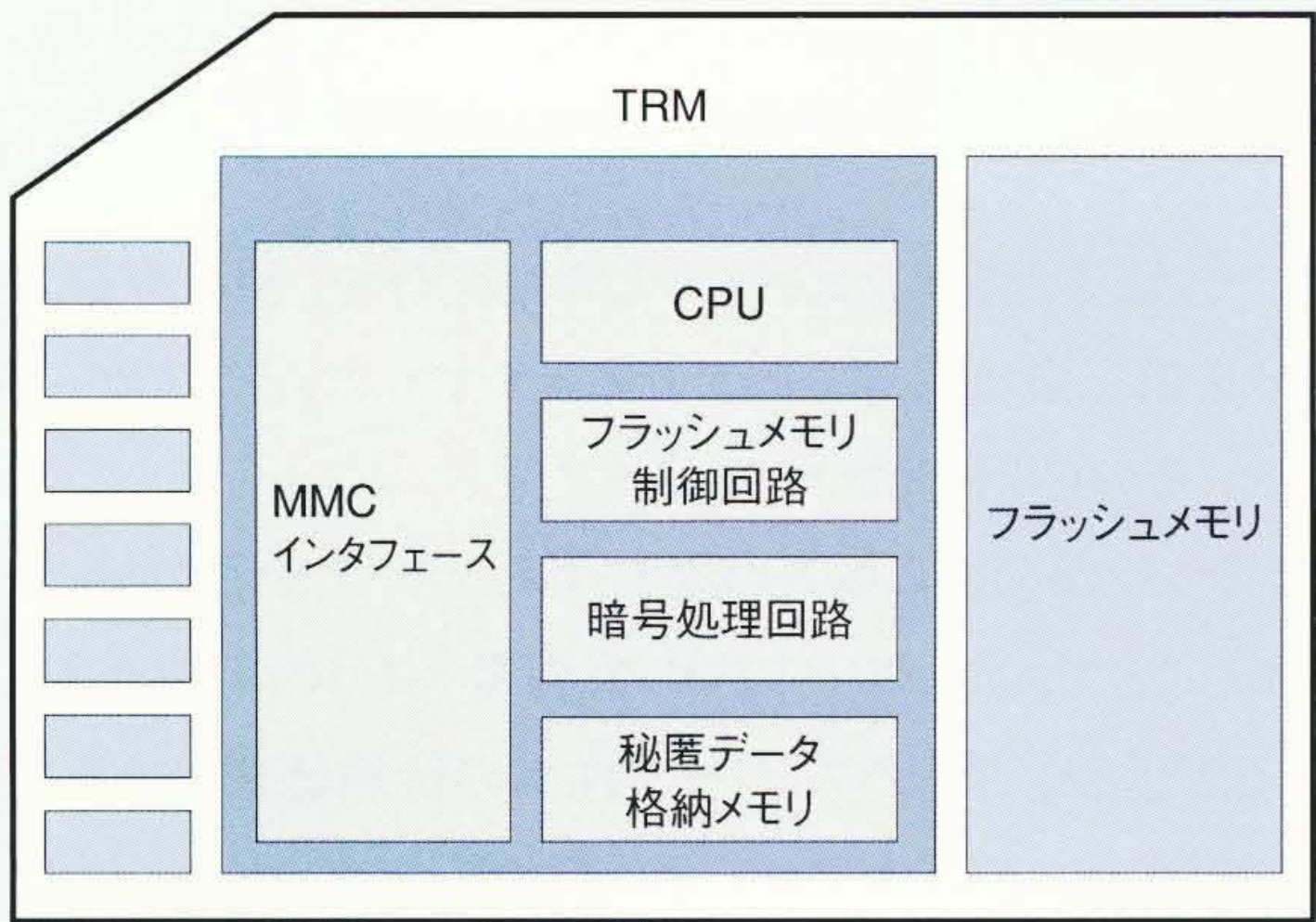


図2 PIN-SMMCの機能ブロック構成
外部からの解析に対して耐性を持つTRM領域の中でPIN検証によるユーザー認証を行うので、ホスト端末上での認証よりも高い安全性を実現している。

(4) ホスト機器からのセキュリティ処理命令に基づいてセキュリティ処理を施す「暗号処理回路」を追加した構成としている。また、フラッシュメモリ制御部は、外部からの解析に対して耐性を持つTRM領域に格納される。PIN-SMMCでは、PIN検証もこのTRMの中で行うので、ホスト機器上での認証操作よりも高い安全性を持たせることができる。

3.3 個人認証機能

PIN-SMMCの個人認証機能は、TRMに格納されているライセンスデータを、PIN入力による認証を通じて端末に読み込むものである。PIN-SMMCでは、個人認証機能として表1に示す五つの機能を実装している。

3.4 認証モードとライセンスアクセス制御

PIN-SMMCでは、従来のSMMCの著作物配信の保護用ライセンス領域とは独立に、一般ユーザーが使用できる拡張

表1 PIN-SMMCの個人認証機能
PIN-SMMCに実装している個人認証機能を示す。これらの機能を使ってユーザーのライセンス領域へのアクセス管理を制御する。

機能	概要
PIN検証	ユーザーが暗証番号によってライセンスの読み出し許可を得る機能である。照合に失敗するとリトライカウンタが一つずつ加算され、検証回数制限値に達すると、ライセンス・PIN初期化を除く個人認証機能が停止する。
PIN更新	ユーザーがTRM内部に設定されたPINを更新する機能である。更新するためには、更新前のPINの照合に成功する必要がある。
検証回数制限値更新	ユーザーがTRM内に設定されたPIN認証検証回数制限値を変更する機能である。更新するためには、PINの照合に成功する必要がある。
ライセンス領域の初期化	ユーザーが指定されたライセンス領域のライセンスをすべて破棄し、新しい参照PIN、リトライカウンタのリセットPINを設定する機能である。
リトライカウンタリセット	指定されたライセンス領域のPIN検証を行い、リトライカウンタを初期値に戻す。同時に、リトライカウンタのリセットPINの更新を行う。

ライセンス領域を新たに追加した。この拡張ライセンス領域のライセンスを読み出す際の認証条件として、前述した「PIN検証」のほか、読み出す機器を特定の機器に限定する、機器の「証明書検証」を条件として組み合わせることが可能である。これは、システムのセキュリティ要件に応じて、あらかじめライセンス領域とアクセス条件を管理者が設定することによって選択することができる。これらの認証機能により、個人から企業や官公庁などのデータベース管理システムまで、さまざまなセキュリティ要件に柔軟に対応できるデータ保護の仕組みを確立した。

4 PIN-SMMCを用いた応用システム

4.1 システムの特徴

PIN-SMMCを用いたシステムの大きな特徴は、かぎ管理がそのシステムごとに任されている点にある。したがって、そのシステム独自の認証局(CA:Certification Authority)を設け、カードと端末の証明書を発行して運営することも、システム簡略化のためにCAを設けずに運営することも可能である。また、かぎと暗号化データを別々に流通させることができる。これにより、だれでもアクセスできるシステムから暗号化データをダウンロードし、かぎを別に配布する形態が可能になる。あるいは、かぎだけあらかじめカードに書き込んだ状態で使用者に配布する形態も考えられる。さらに、かぎにデータのアクセスコントロールを付加することができ、映像や音楽などのデータに再生制限を付けることもできる。

4.2 応用例(I)

PIN-SMMCとPDA(Personal Digital Assistant)とを組み合わせた例について以下に述べる。PDAはモバイル端末として広く普及しつつあり、PIN-SMMCと組み合わせたシステムは業務用途として有効である。顧客データや建築現場のCADデータなどを暗号化して社内のサーバに格納しておき、社員はイントラネットを通して自由にデータをダウンロードする。管理者はデータのカテゴリーごと、あるいは社員の役職に応じて、その社員が見てもよいデータに対応したかぎを別途配布する。これにより、データが入ったカードを無くしても、PINを知らない第三者はカード内の暗号化されたデータを見ることはできず、社員でも、かぎを付与されていないデータは見られないというセキュアなシステムを実現することができる。

4.3 応用例(II)

PDAの性能向上により、動画再生もスムーズに行えるようになったため、通勤や通学途中に映像を楽しむことも可能に

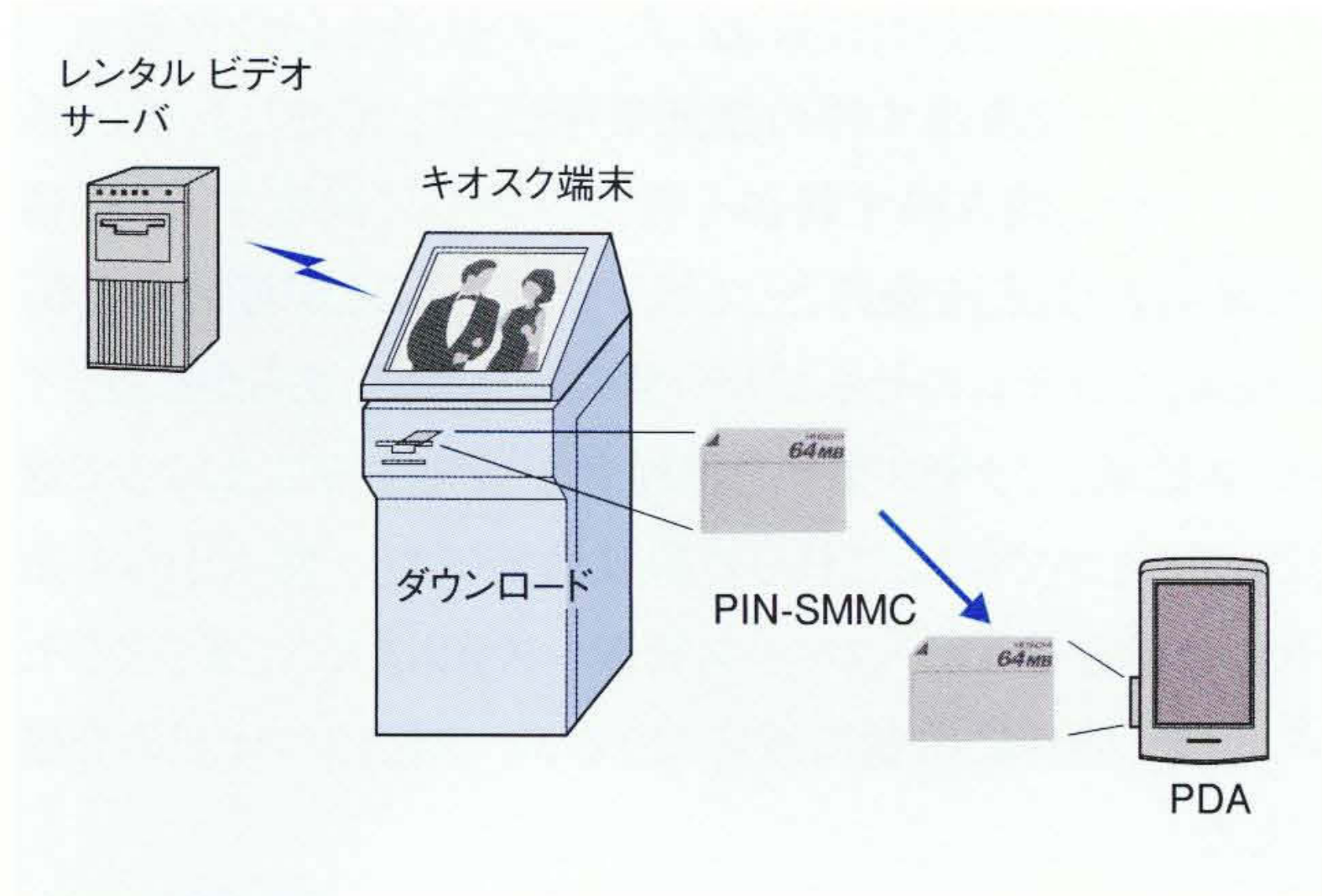


図3 PDAを用いたレンタルビデオシステム

コンビニエンスストアなどのキオスク端末で、PDAにコンテンツをダウンロードすることができる。再生回数を制限することにより、コンテンツを返却する必要のないレンタルシステムが構築できる。

なる。例えば、現在のレンタルビデオの仕組みを変え、映画やドラマなどのコンテンツを暗号化してキオスク端末のようなものでカードにダウンロードできるようにする。そして、このダウンロードした、暗号化されたコンテンツに対応するかぎを、同じキオスク端末で購入したり、携帯電話からダウンロードして購入することで、コンテンツをPDA上で再生する。このかぎに再生制限を付けることにより、コンテンツを返す必要のない、新たなレンタルビデオシステムを構築することができる(図3参照)。

4.4 NetPDAを用いた実システム

日立製作所が2002年6月に発売を開始した、PIN-SMMCと携帯情報端末“NPD-10JWL”を組み合わせた、小売店での顧客対面サポートシステムについて以下に述べる。

NPD-10JWLの特徴の一つは、無線LANを標準搭載していることである。システムの目的は、店員を勘定台に集中させずに各売り場に配置できるようにすることであり、そのために、顧客のデータ(買い物金額に応じて付与するポイント、顧客の連絡先など)、商品の価格、在庫情報などのデータを店員に持ち歩かせ、PDAでこの情報を見られるようにする。このようなデータはセキュリティを必要とするため、店員に持たせる際にPIN-SMMCを利用する。

まず、上記データを本社のサーバで暗号化する。このとき用いるかぎは、各店員のID(Identification)を利用したものとし、各店員に割り当てる。すなわち、PIN-SMMCにあらかじめ書き込み、店員に配布する。データは、本社のサーバから各店舗、各階のサーバに送られ、PDAを持った店員は無線LANで暗号化データをカードに逐次ダウンロードする。このようなシステムを利用することにより、店員は常にアップデートされたデータを手もとに持つことができ、また、そのデータの入ったカード、あるいはカードの入ったPDAごと無くしても、データを第三者に見られることがなく、安全にシステムを運用することができる。

5 おわりに

ここでは、きたるべきユビキタス情報社会で、個人や企業のデータを第三者から守るPINセキュアマルチメディアカードの概要と、その応用例について述べた。

コンテンツ保護から個人認証に至るセキュリティ機能をサポートすることで、同一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、単なるストレージ以上の付加価値のある使い道が生まれる。PINセキュアマルチメディアカードは、外形寸法もICカードに比べて小さく、小型化の進むモバイル端末機器、特に携帯電話のスロットにも収まる。ユーザーは、大切な個人データやアドレス帳などをこの中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。

2002年7月に日立製作所、Ingentix GmbH & Co./Ltd., 松下電器産業株式会社、サンディスクコーポレーション、および株式会社東芝の5社で共同発表したモバイルコマース拡張規格に準拠したモバイルコマース用カードの開発も視野に入れ、今後も、フラッシュメモリカードをさらに進化させ、ユビキタス情報時代のキーデバイスとして提案していく考えである。

参考文献

- 1) MMCA Technical Committee: The MultiMediaCard System Specification Version 2.11, Official Release c (June 1999)

執筆者紹介



兼平 晃

1987年日立製作所入社、半導体グループ メモリビジネスユニット 応用システム部 所属
現在、次世代フラッシュカードのシステム開発に従事
映像情報メディア学会会員
E-mail: kanehira-akira @ sic. hitachi. co. jp



三宅 順

1984年日立製作所入社、半導体グループ メモリビジネスユニット 応用システム部 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



戸塚 隆

1980年日立製作所入社、半導体グループ メモリビジネスユニット 応用システム部 所属
現在、フラッシュカードの次世代応用開拓に従事
E-mail: totsuka-takashi @ sic. hitachi. co. jp