

ICカード応用のセキュア情報システム

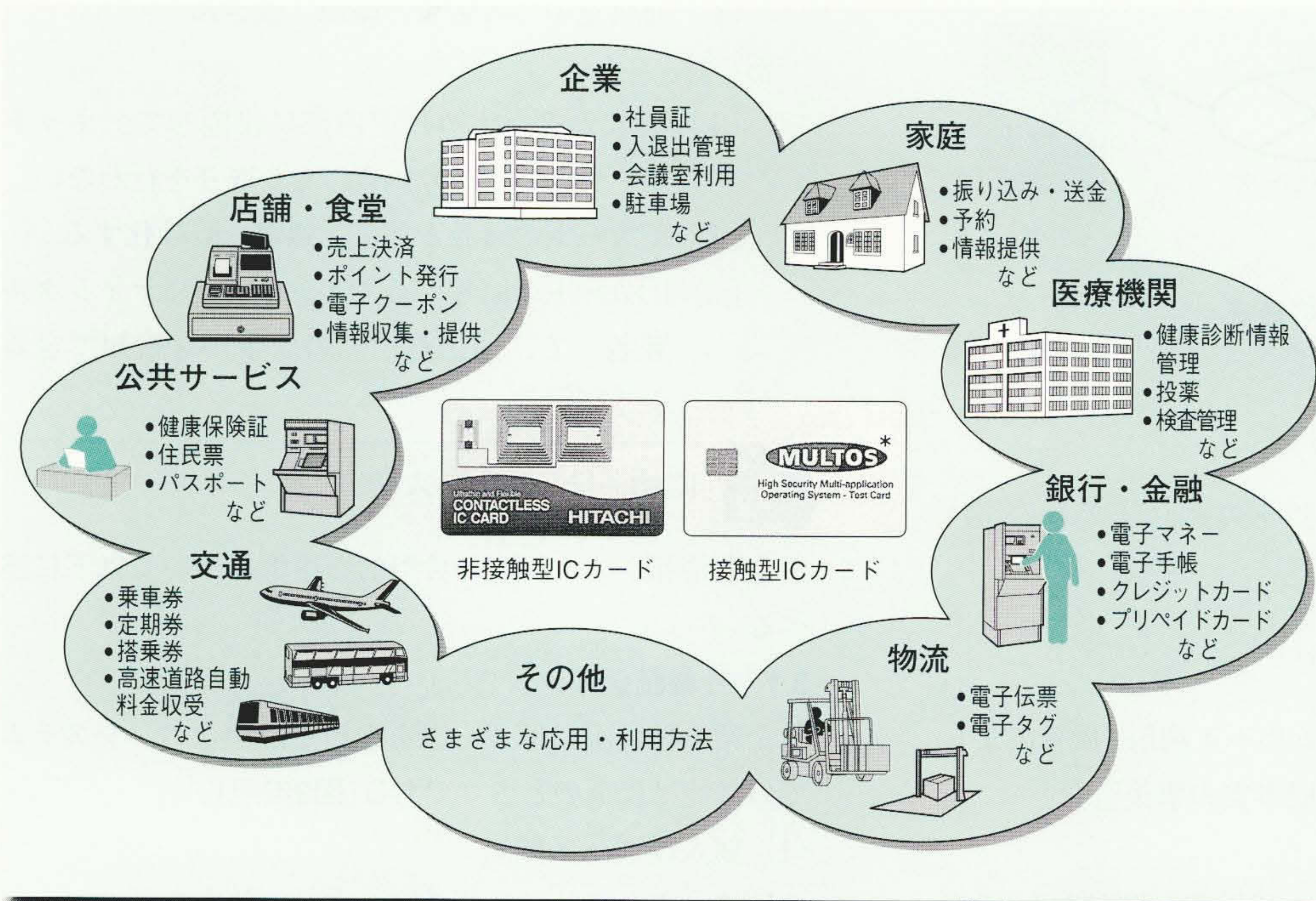
Secure Information Systems Applying IC Cards

船橋義孝 Yoshitaka Funabashi

井上 剛 Tsuyoshi Inoue

戸田幸利 Yukitoshi Toda

全 隆生 Takao Zen



注：* MULTOSは、MAOSCO Limitedの登録商標である。

ICカードシステムのさまざまなアプリケーション

ICカードは、さまざまな分野の応用システムの中で、セキュリティを支える重要なデバイスとして、今後ますます適用が拡大していく。

ICカードは、個人情報や機密情報を安全に格納し、容易に携帯でき、さまざまな分野で利用できる、利便性の高いセキュアなコンポーネントとして急速に注目を集めている。

一方、メーカー各社のICカード関連製品の仕様やセキュリティ(安全性)基準には共通性がないため、システムの普及が遅れている。そこで、わが国でも国家的なプロジェクトが発足し、業種・業界を越えて、ICカードシステムのさまざまな標準化活動が展開されている。

日立製作所は、これらの標準化活動に積極的に参加し、オープンでセキュアなICカードシステムの開発に取り組んでおり、「日立ICカードソリューション」として、社員証システムや入退出管理システムなどの、ICカードを応用したシステムのソリューションビジネスを展開している。

1 はじめに

ICカードは、CPU (Central Processing Unit) を内蔵したセキュリティ(安全性)の高さや、記憶容量の大きさ、価格対性能比の向上などの理由で、世界中でさまざまな応用システムの実証実験が行われ、導入が進んでいる。

ICカードには、以下の特徴がある。

- (1) 暗号のかぎや、かぎの正当な所有者であることを示す証明書¹⁾などの情報を、安全に管理できる(耐タンパリング性)。
- (2) 利用先の端末でも、暗号通信や本人認証などの機能が利用できる(携帯性)。

さらに、非接触型ICカードでは、以下の特徴が加わる。

- (3) かざすだけで、建物や改札などへの出入りができる。

- (4) 水、油、粉じんなどに対する耐環境性が高い。

最近のEC (Electronic Commerce：電子商取引) の普及に伴い、営業機密や個人情報(プライバシー)の管理の面で企業責任が問われる時代となってきた。今やICカードは、セキュリティ対策のコンポーネントとして、急速に重要性が増してきた。

ここでは、ICカード応用のセキュアシステムについて述べる。

2 ICカード利用によるセキュリティ対策

ネットワークを介してサーバにアクセスする場合の、情報システムのセキュリティ上の脅威と、ICカードを応

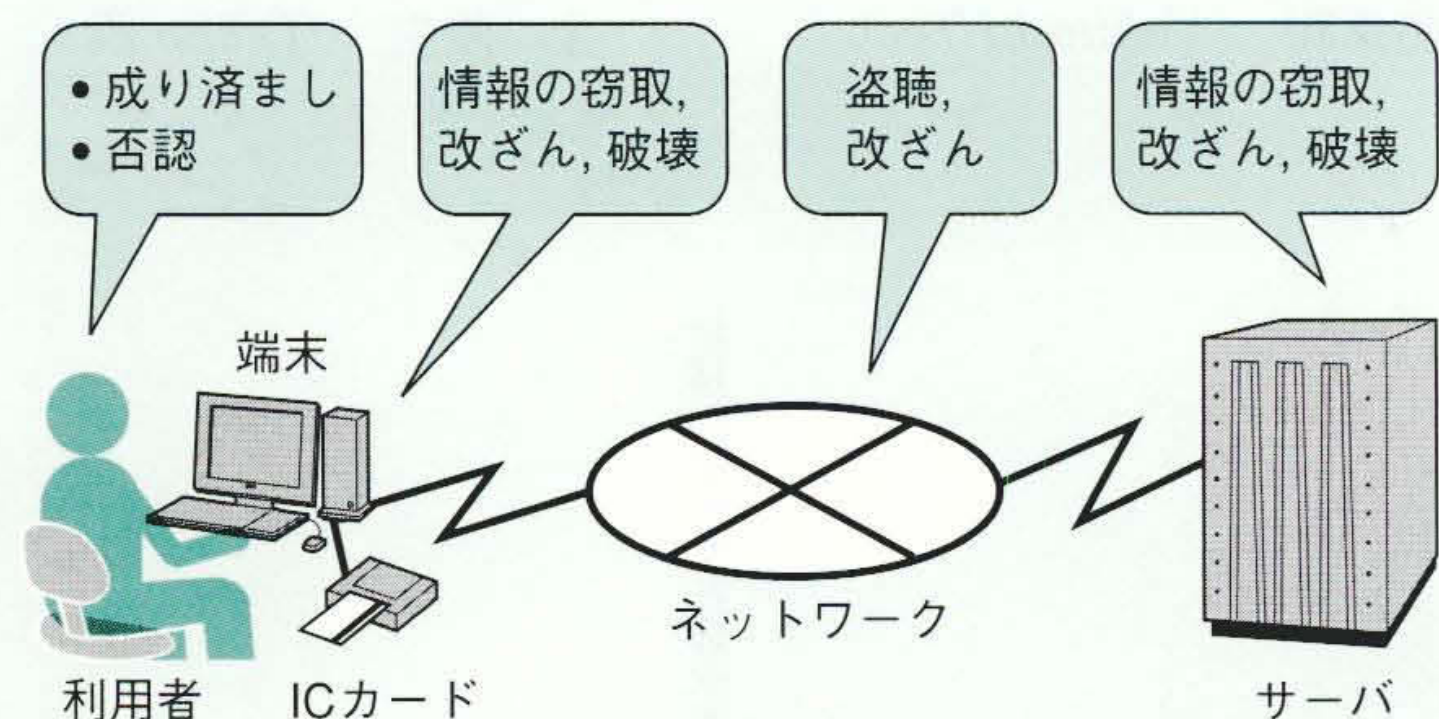


図1 システムのセキュリティ上の脅威

情報システムには、さまざまな「セキュリティ上の脅威」が潜在している。

用した対策の特徴的な点は、以下のとおりである（図1参照）。

(1) 利用者

(a) 脅威

- (i) 第三者によるシステムの不正利用，成り済まし
- (ii) 利用者本人による取引事実の事後否認

(b) 対策

- (i) 所持するICカードで，利用者を識別する（所有物による識別）。
- (ii) 利用者の入力した暗証番号や，指紋などの生体情報と，ICカードに記録した情報を照合し，所有者の正当性を検証する。
- (iii) ICカード内部の暗号かぎを利用した電子的な署名により，取り引きの証拠を残す（デジタル署名¹⁾による処理事実と送信内容の保証）。

(2) 端末，サーバ

(a) 脅威

- (i) 装置で管理している情報の窃取，改ざん，破壊

(b) 対策

- (i) 端末で生成した乱数をICカードに送付し，端末とICカード内部の暗号かぎで乱数をそれぞれ暗号化する。その結果を端末側で照合し，ICカードの正当性を検証する（端末によるICカードの認証）。
- (ii) ICカードで生成した乱数を端末に送付し，端末とICカード内部の暗号かぎで乱数をそれぞれ暗号化する。その結果をICカード側で照合し，端末の正当性を検証する（ICカードによる端末の認証）。
- (iii) ICカードに秘匿した証明書を用いて，利用者の端末やサーバへのアクセス権限をチェックす

る（アクセス制御）。

(3) ネットワーク

(a) 脅威

- (i) 通信途中での情報の盗聴，改ざん

(b) 対策

- (i) 暗号かぎをICカード内部に秘匿して，ネットワーク上での暗号かぎのやり取りを行わない。
- (ii) ICカードの暗号かぎで，通信を暗号化する。
- (iii) ICカードの暗号かぎでメッセージにデジタル署名して，通信途中での改ざんを検知できるようにする。

3 ICカード応用システム

企業情報システムでの典型的な事例について以下に述べる。

3.1 社員証システム

企業の社員証にICカードを応用した場合の，システムでの機能は以下のとおりである（図2参照）。

(1) 個人識別認証機能

ICカード上の社員番号や暗証番号で個人を識別する。

- (a) 社屋や計算機室，資料管理室の入退出管理
- (b) 端末や情報システム，その他の施設を利用する際の識別

(2) 秘密通信機能

ICカード上の社員別暗号かぎや証明書の情報を利用して，通信情報の秘密を守る。

- (a) 暗号通信，暗号メール
- (b) ワークフローでの電子決裁

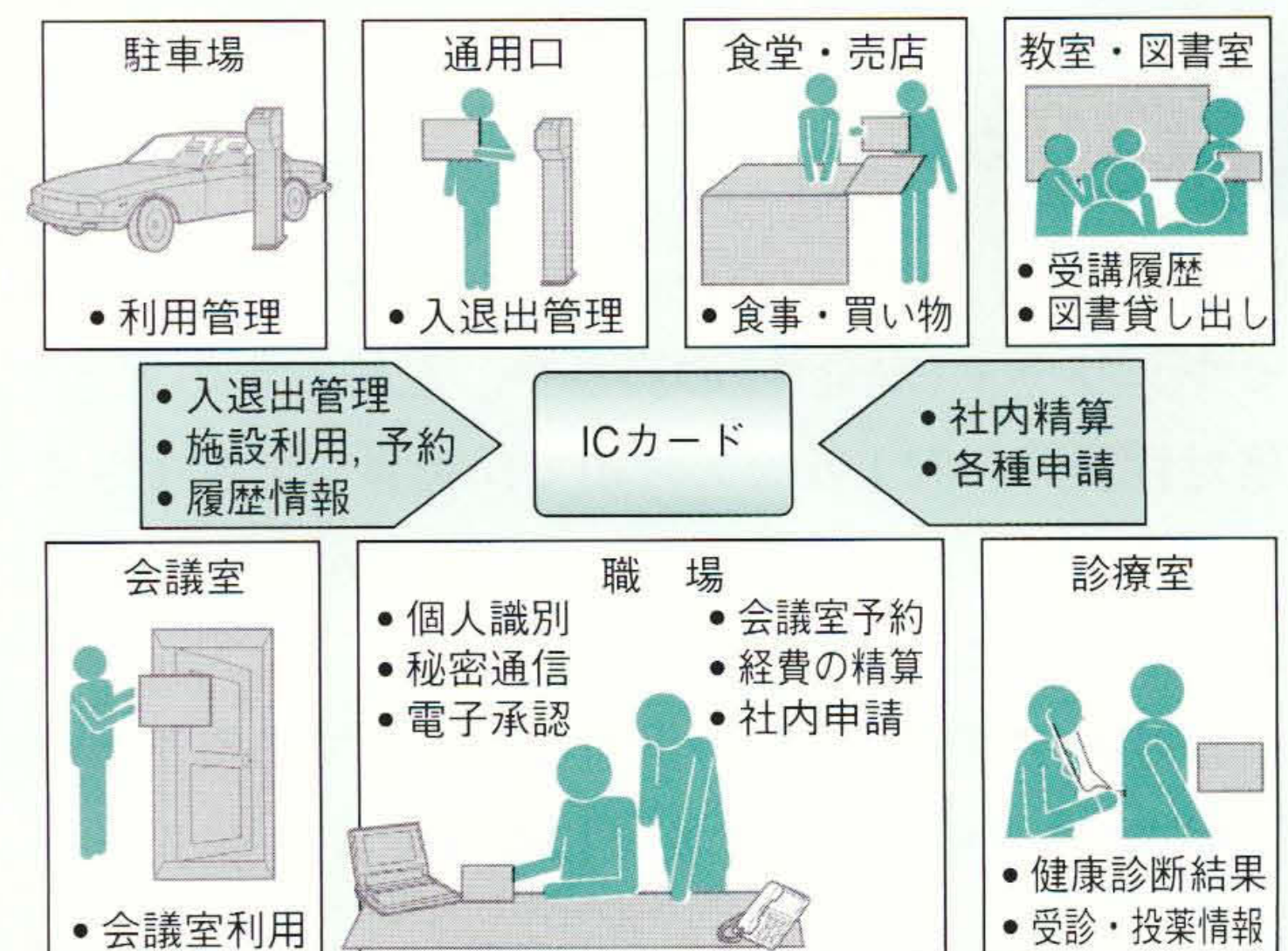


図2 ICカードの応用例

ICカードには，企業内の応用のほかにも，さまざまな用途がある。

(3) 決済機能

ICカード上の社員給与口座番号やクレジットカード番号などの情報を利用して決済する。

(a) 社内の食堂や売店での支払い

(4) 情報蓄積機能

ICカードに社員の履歴情報を記録し、職制変更や異動などに対応する。

(a) 業務、教育、資格、表彰などの履歴

(b) 健康診断結果の履歴、受診や投薬の記録

3.2 入退出管理システム

日立製作所は、非接触型ICカードを応用したセキュアな入退出管理システム“Gatevision[※]”を提案している。

Gatevisionは、以下のような機能を持つ(図3参照)。

(1) 状態監視機能

システムの通信状態を監視したり、ドアを遠隔から操作する。

(2) カード管理機能

発行カードの入退出エリアでの個人別情報や、有効期限切れの無効カードの状態などを管理する。

(3) レポート作成機能

入退出情報の記録やエリア別のディスプレイに表示、レポートの印刷などを行う。

(4) 運用支援機能

平日や休日の設定など、システム全体の運用を容易に

※) Gatevisionは、株式会社日立インフォメーションテクノロジーの登録商標である。Gatevisionは、入退出についての各種管理機能を標準仕様で提供する。

し、管理情報のバックアップなどを確実にする。

またICカードは、固有のかぎ情報を持っており、第三者による偽造を防止するので信頼性が高い。さらに、センサから放出する電磁波を受けて作動することから電池を必要としない。

3.3 決済システム

日立製作所は、多機能ICカードであるMULTOS〔マルチアプリケーション搭載カード用OS(Operating System)〕カードを用いた決済システムを提供している。

MULTOSの高度なOS機能により、本格的な電子マネーシステムの構築が可能なセキュリティと、会員向けポイントサービスやクレジット取り引きに代表される複数のアプリケーションを、必要に応じて追加、削除できる柔軟性を実現する。

MULTOSカードにより、ICカード1枚で多彩なサービスを実現する。利用者にとっては利便性が高く、サービス提供者にとっては安全性が高い決済システムを構築することができる。

4 今後の展開

ICカードシステムの今後の動向について以下に述べる。

(1) ICカードシステムの標準化

日立製作所は、利便性向上などのために、ICカード関連の各種標準化活動に積極的に参画している(表1参照)。

また、セキュリティ面については、国際的な評価基準“CC(Common Criteria)”に基づいて、わが国でもICカードと関連製品の安全基準の策定活動が始まっており、日

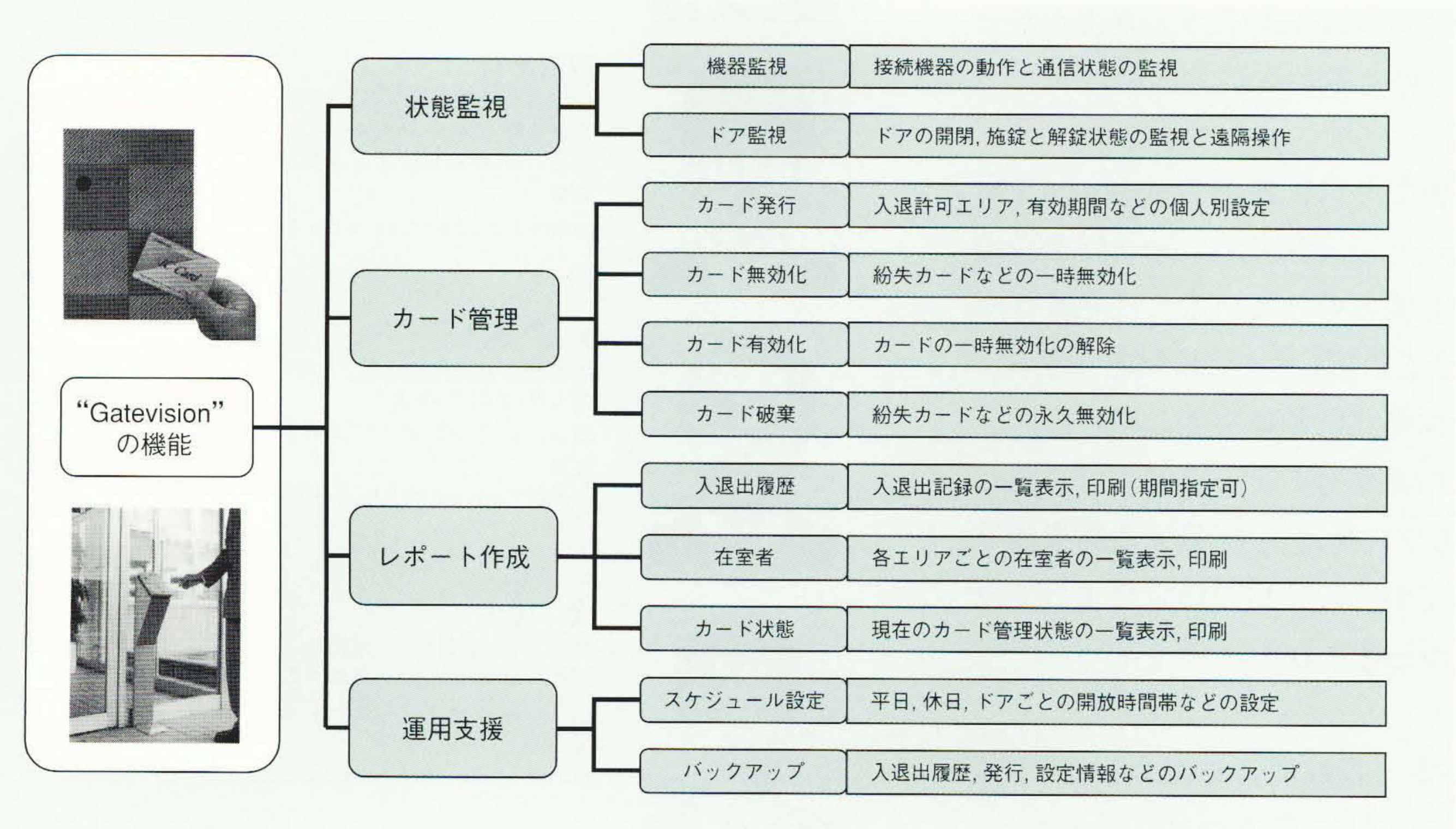


図3 入退出管理システム“Gatevision”の機能概要
Gatevisionは、入退出についての各種管理機能を標準仕様で提供する。

表1 日立製作所の参画する主なICカードシステム標準化推進活動

日立製作所は、ICカードシステムの標準化などに関連する活動を推進する各種組織活動に参画している。

名 称	概 要	研究会などへの参加 企業・団体など
社団法人日本事務機械工業会(JBMA)	国際標準規格の国内審議機関 (ISO/IEC, JTC1/SC17 国内委員会など)	ICカード・端末 関連メーカー
ICカードシステム利用促進協議会(JICSAP)	わが国のICカードシステムの効率的、継続的な普及推進	会員数76社
財団法人ニューメディア開発協会(NMDA)	ニューメディアに関する調査、普及啓発、次世代ICカードシステムの開発	ICカード・端末 関連メーカー
ICカード取引システム研究開発事業組合(ICCS)	EC用非接触ICカード対応の汎用端末用リーダ・ライタ装置の技術開発	会員数48社
電子商取引実証推進協議会(ECOM)	ECを実現するための技術、制度的課題の検討、共通プラットフォームの構築	会員数239社 (団体を含む。)
汎用電子乗車券技術研究組合(TRAMET)	非接触ICカードを使用した自動改札、関連システムの技術開発と実証	会員数55社
次世代ICカードシステム研究会(NICSS)	公共分野の次世代ICカードシステム共通プラットフォームの検討、普及推進	発起企業17社

日立製作所は、これらに参加していく。今後、ICカード関連製品を選定する際には、このCCに準拠するか否かがセキュリティの目安になるものと考ええる。

(2) 多機能端末装置

ICカードの異なる仕様ごとに、異なる仕様のATM (Automated Teller Machine)やPOS(Point-of-Sale)端末、キオスク端末などが必要となっている。日立製作所は、この問題に対し、さまざまなICカードに対応できる、多機能端末装置の仕様の標準化活動に参加している。

この多機能端末では、暗証番号のデータ漏えいを防ぐための「暗証番号入力制御システム」を搭載する高機能リーダ・ライタも検討されており、仕様の確定によってセキュリティが向上するものと考ええる。

(3) 生体認証システム

日立製作所は、ICカードと指紋照合を融合した「生体認証技術」などを研究している³⁾。従来の暗証番号では、

他人に推測されたり、本人が忘れるなどの問題がある。そこで、本人の指紋情報を抽出してICカードに登録し、暗証番号の代わりに用いる。ICカードに登録した情報と利用者の指紋を照合させることにより、他人による成り済ましを防ぐセキュリティを確保することができる。

5 おわりに

ここでは、情報システムのセキュリティ上の脅威と、ICカードシステムによるこの脅威に対する対策、応用システムの事例や今後の展開について述べた。

日立製作所は今後も、進化していくセキュリティ技術と多様な市場のニーズを先取りし、利便性が高くセキュアなICカードシステムの普及のために、応用システムやソリューションを提案していく考えである。

参考文献

- 1) ウォーウィック・フォード，外：デジタル署名と暗号技術，プレントイスホール出版社(1997-12)
- 2) 特集 21世紀のシステムインフラストラクチャー「次世代ICカードシステム」，日立評論，80，4(平10-4)
- 3) 三村，外：指紋によるICカード持ち主認証システムの開発，コンピュータセキュリティシンポジウム'98，情報処理学会シンポジウムシリーズ，Vol.98，No.12，pp.185～188(1998-10)

執筆者紹介



船橋義孝

1963年日立製作所入社，情報・通信グループ 情報システム事業部 ICカードシステムビジネス推進センタ 所属
現在，ICカードソリューションビジネスの推進・拡販に従事
E-mail：funabasi @ system. hitachi. co. jp



戸田幸利

1989年日立製作所入社，情報・通信グループ 情報システム事業部 ICカードシステムビジネス推進センタ 所属
現在，ICカードソリューションビジネスの推進・拡販に従事
E-mail：ma-toda @ system. hitachi. co. jp



井上 剛

1980年日立製作所入社，情報・通信グループ システム開発本部 第四部 所属
現在，決済分野でのICカードアプリケーションの開発に従事
E-mail：t-inoue @ iabs. hitachi. co. jp



全 隆生

1988年株式会社日立情報システムズ入社，ソリューションサービス事業部 テクニカルサービス部 所属
現在，ICカードソリューションビジネスの推進・拡販に従事
E-mail：take-zen @ system. hitachi. co. jp