1. 証明書所有者の鍵ペア生成処理の記録
2. 証明書の発行・失効処理の記録
3. CRL 発行処理の記録
4. CA の設定に関わる情報の記録
5. CA のアクセス記録の記録　等

4.5.2 監査の頻度

監査用記録の監査は、月に 1 回以上の頻度で行うものとする。

4.5.3. 監査用記録の保管期間

監査用記録の保管期間は、 1 年間とする。

4.5.4. 監査用記録の保護

監査用記録は別途定められた標準に従い、流出、改竄、削除からの保護措置を講ずるものとする。

4.5.5. 監査の報告

記録に対する監査を行った後には、監査結果をポリシ委員会に報告する。なお、記録の監査により、問題を発見した場合には、監査ログ検査者は直ちに CA サービス運用責任者に報告する。CA サービス運用責任者は、定められた手順に従い、それを是正するための処置を行うものとする。

4.6. 記録の保管

4.6.1. 記録の種類

1. 利用者からの申請書と添付書類の一式
2. CA の証明書
3. CA が発行したエンドエンティティ証明書
4. CRL の申請書

4.6.2. 保管期間

記録は最低 10 年間保管される。

4.6.3. 保管方法

記録は、外部媒体へ格納され、安全な場所に保管される。

4.7. 鍵の切替え

証明書所有者が公開鍵を別の公開鍵に円滑に切り替えることができるように、本 CA は、切替日の 30 日前に新しい証明書を発行して、その日以降は新しい証明書を使用する必要がある日付を証明書所有者に明確に知らせなければならない。

4.8. 危殆化と業務の継続性の保証

CA 私有鍵の危殆化の場合及び災害等により CA の業務が停止した場合には、最低限、次の手順を実行し、安全な環境を修復する。
CA が発行したすべての証明書の失効手続きを行う。
CA 停止状況を証明書所有者や検証者に報告する。

4.9. CA の終了

本 CA が運営を停止する場合には、運営の終了時に直ちに証明書所有者に通知し、CA の鍵と情報の継続的な保管を手配するものとする。また、ルート認証局及び関連している組織のすべてに対しても通知するものとする。CA の運営がより低い保証レベルで運営されている別の CA に譲渡される場合には、運営が譲渡される CA によって発行された証明書は、譲渡に先立ち、その CA によって署名された CRL を通じて失効されるものとする。CA が終了する場合には、その CA の記録の安全な保管または廃棄を確実にするための取り決めを行うものとする。

5. 建物・関連設備、運用、要員のセキュリティ管理

これらは、ISO 17799-1：2000と同等以上の規格、又は認可された認定あるいは免許基準に従うものとする。これは、セクション5に適用され、次の項目をカバーする。

5.1. 建物及び関連設備管理

5.1.1. 施設の位置と建物構造

隔壁により他の設備からは隔てられている。

5.1.2. 入退管理

CA設置サーバルームに対する入退出の状況はＴＶカメラで監視しており、常時警備員が警戒している。ＴＶカメラの画像は長期間の保存に耐える媒体を使用するものとする。また、入退出時にはICカードと生体認証の組み合わせが必要である。

入退出者の本人確認方法を定められた方法により確実に行い、かつ入退出の記録を残す。個人情報管理室及びサーバ室への立入りは、複数の者により行われるものとする。

設備の保守その他の業務の運営上必要な事情により、やむを得ず、立入りに係る権限を有しない者を個人情報管理室及びサーバ室へ立ち入らせることが必要である場合においては、立入りに係る権限を有する複数の者が同行する。

5.1.3. 電源及び空調設備

CA 設置サーバルームの電源は UPS・自家発電設備により瞬停、及び停電から保護される仕組みとし、電源断の確認後自動的に自家発電設備が起動する仕組みとする。また、空調設備を用意し、機器類の動作環境及び要員の作業環境を適切に維持する。さらに、電源設備、空調設備等の運転状態を監視し、必要な措置（異常警報を発して記録し、操作を行う等）を行うものとする。

5.1.4. 水害及び地震対策

漏水の恐れのある場所に漏水検知器等を設置し、水漏れ防止措置を講ずるものとする。建物は耐震構造とし、CA設置サーバルームは、転倒防止策を講じるものとする。また、感震器を設置し、異常を監視、検知できるものとする。

5.1.5 防火設備

建物は耐火構造とする。認証設備室は防火区画とし、火災報知器、消火設備及び耐火金庫を備えるものとする。

5.1.6. 記録媒体

アーカイブデータ、バックアップデータ、入退室情報（監視カメラの情報を含む）を含む媒体は、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、所定の手続に基づき適切に搬入出管理を行う。また、指定された重要度の高い媒体は耐火金庫にて保管されるものとする。

5.1.7. 廃棄物の処理

機密扱いとする情報を含む文書・記録媒体は、完全な初期化を行うか物理的に破壊を行い、紙面･文書等の紙ベースのものはシュレッダーにかけ廃棄を行う。

証明書所有者が所有するICカードは、使用期間が終了したときには回収し、確実に廃棄を行う。個人での廃棄は認めない。

5.1.8. オフサイト・バックアップ

現状において、オフサイド・バックアップ対応はしていない。XXX の建物内において十分に距離をおいた上、耐火金庫等安全な場所2箇所に分散保管するものとする。

5.2. 手続的管理

以下のポリシーに従いCAの安全な運用を保障するものとする。

1. 要員の職務権限を分離し、相互牽制をはかる。
2. 要員単独で運用することによるシステムの悪用を牽制するため、CA 運用業務の遂行は原則複数人の管理下で行うものとする。
3. セキュリティ上問題が無いと判断された場合は、一人の要員が複数の運用業務を担当するものとする。

5.3. 要員管理

5.3.1. 採用と契約

1. 要員を採用する段階でセキュリティの責任を言及し、それを雇用条件に盛り込む。
2. CA 運用業務を担当する全ての要員に対し、機密保持（守秘義務）契約書への署名を求める。
3. CA 業務に係わる要員は必ず XXX 職員でなければならない。(アルバイトや派遣、外注は認めない)

5.3.2. 教育

本 CA の運用管理に携わるもの全員に対して、セキュリティに関する教育を 1 年に 1 回以上行う。

5.3.3. 罰則

内容の軽重にかかわらずセキュリティ違反に対する罰則事項を定め、違反者は厳格に処分する。また、罰則には故意、過失を問わない。

6. 技術的なセキュリティ管理

6.1. 鍵ペアの生成と実装

6.1.1. 鍵ペアの生成

証明書所有者の公開鍵／私有鍵のペアは、CA によってのみ生成されるものとする。
CA の署名鍵生成及び管理は、サーバ室内で複数の者によって専用の端末を用いて行われること。

6.1.2. 所有者への私有鍵の送付

証明書所有者の私有鍵は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、または同様に安全な方法によって、証明書所有者に引き渡されるものとする。CA はオリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことの証明ができるものとする。

6.1.3. CA への公開鍵の送付

証明書所有者の公開鍵は CA が生成するため、証明書所有者が公開鍵を CA に送付することはない。

6.1.4. 証明書所有者への CA 公開鍵の配付

公開鍵は証明書に結合されるので、公開鍵は、作成後直ちに証明書とともに証明書所有者に送られるものとする。公開鍵の引渡しには、証明書の引渡しと同じ手続きが適用されるものとする。

6.1.5. 鍵のサイズ

本 CA の署名用の鍵は、ハッシュアルゴリズムとして SHA-1 を用いた RSA 方式であり、鍵長は 2048 ビットとする。証明書所有者の署名用の鍵は、ハッシュアルゴリズムとして SHA-1 を用いた RSA 方式であり、鍵長は 1024 ビットとする。

6.1.6. 公開鍵パラメータの生成

なし

6.1.7. パラメータ品質の検査

なし

6.1.8. ハードウェア又はソフトウェアによる鍵ペア生成

鍵の生成は、安全な方法で行われるものとする。

CA の公開鍵／私有鍵ペアの生成は、FIPS140-1 Level3 相当以上のタイタンパー性が確保された HSM 上で行う。

6.1.9. 鍵の使用目的

認証鍵及びデジタル署名鍵は、身元確認及び/または否認防止目的のためだけに使用されるものとする。データの暗号化目的には別個の鍵ペアがあるものとする。

6.2. 私有鍵の保護

本 CPS では２つの鍵ペアが存在する。１つは、本人認証またはデジタル署名鍵であり、この鍵は CA でバックアップしない。もう１つは、暗号のためのペアであり原則として CA ではバックアップしないが、XXX 内サーバの暗号用鍵ペアについてのみバックアップするものとする。

6.2.1. 暗号モジュールに関する標準

CA 署名鍵は、US FIPS 140-2 レベル２と同等以上の規格に準拠するものとする。ただし、電子署名法に適応させる場合は、CA 署名鍵は、US FIPS 140-2 レベル 3 と同等以上の規格に準拠するものとする。他の証明書は、US FIPS 140-2 レベル 1 と同等以上の規格に準拠するものとする。

6.2.2. 複数人による私有鍵の管理

証明書所有者の私有鍵は所有者の管理とし、複数人の管理は認めない。

6.2.3. 私有鍵のエスクロウ

認証またはデジタル署名のために使用される私有鍵は、法律によって必要とされる場合を除き、エスクロウされないものとする。ただし、XXX 内サーバの暗号用鍵ペアについてはエスクロウするものとする。

6.2.4. 私有鍵のバックアップ

デジタル署名鍵は、証明書所有者の IC カード内に格納されているが、証明書所有者がこれをバックアップすることはない。

6.2.5. 私有鍵のアーカイブ

CA は XXX 内サーバの暗号用鍵私有鍵についてのみバックアップする。この私有鍵は XXX の安全な場所に、CA の証明書用鍵と同等の扱いで厳格に保管するものとする。

6.2.6. 暗号モジュールへの私有鍵の格納

本 CA ではエンティティの暗号モジュールで生成することはないので、IETF RF2510「証明書管理プロトコル」に従って、また同様に安全な方法で、モジュールに入力されるものとする。

6.2.7. 私有鍵の活性化方法

ヘルスケア PKI においては、証明書所有者だけが自身の私有鍵を活性化することができる。証明書所有者は、私有鍵の活性化の前に、私有鍵を保護している暗号モジュール又はアプリケーションに認証されるものとする。この認証には、指紋認証及びパスワードを用いる。非活性化された私有鍵は、アクセス制御されたハードウェア又は／及び暗号化された形式で保管されるものとする。

6.2.8. 私有鍵の非活性化方法

鍵が非活性化されアクセス制御されないメモリに格納されている場合は、メモリが割当て解除される前に、鍵がメモリから消去されるものとする。鍵が格納されていたディスク領域は、その領域がオペレーティングシステムに解放される前に上書きされるものとする。

暗号モジュールは、事前設定された非活動期間の後に自動的に私有鍵を非活性化するものとする。

6.2.9. 私有鍵の破棄方法

私有鍵の使用の終了時には、複数のものによりコンピュータメモリ及び共有ディスク領域内の私有鍵および全てのコピーは、複数回上書きすることによって確実に破壊するものとする。この破棄処理はCA操作員二人以上の複数人で処理されるものとする。私有鍵破棄手続きは、CPSまたは公的に入手可能な文書で記述するものとする。

6.3. 鍵ペア管理に関するその他の面

6.3.1. 公開鍵の保管

公開鍵は、後日の署名の検証を可能にするために、信頼できる第三者によって保管される必要がある。CAは、公開鍵が保管されたことを保証する責任があるものとする。

6.3.2. 私有鍵と公開鍵の有効期間

CA以外の公開鍵と私有鍵の使用は3年とし、その後に新しい鍵ペアが発行されるものとする。また、本CAの公開鍵と私有鍵の使用は、10年とし、その後に新しい鍵ペアが発行されるものとする。

6.4. 活性化用データ

活性化データは、一意で予想不能なものとし、証明書所有者に安全に伝えられるものとする。

6.5. コンピュータのセキュリティ管理

本CAは、ISO17799-1:2000に則ったコンピュータのセキュリティ管理基準に従っており、別途セキュリティポリシーを定めている。

6.6. ライフサイクルの技術的管理

本 CA は、ISO17799-1:2000 に則ったライフサイクルの技術管理に従っており、別途セキュリティポリシーを定めている。

6.7. ネットワークのセキュリティ管理

本 CA は、ISO17799-1:2000 に則ったネットワークのセキュリティ管理基準に従っており、別途セキュリティポリシーを定めている。

6.8. 暗号モジュールの技術管理

本 CA は、ISO17799-1:2000 に則った暗号モジュールの技術管理に従っており、別途セキュリティポリシーを定めている。

7. 証明書と失効リストのプロファイル

7.1. 証明書のプロファイル

MEDIS『ヘルスケア PKI 認証局証明書ポリシ』の証明書プロファイル仕様に準じるものとし、本 CA 特有の部分のみ以下にコメントする。

対象	フィールド	識別情報
version	Version	2
serialNumber	CertificateSerialNumber	CA 側で一意になる番号を指定し、再使用しない
signature	Signature	1.2.840.113549.1.1.5(sha1WithRSAEncryption)
Issuer（発行者）	CountryName	C=JP
	LocalityName	使用しない
	OrganizationName	O=XXX
	OrganizationUnitName	使用しない
	CommonName	Cn=MD-HPKI-01-YYYYY
Subject（発行申請者）	Country	C=JP
	LocalityName	使用しない
	Organization	組織名をアルファベットで記入
	OrganizationUnit	使用しない
	CommonName	Cn=姓名をアルファベットで記入 ＋ シリアル NO
	surName	使用しない
	givenName	使用しない
	E-mail	使用しない
extensions	AuthorityKeyIdentifier	keyIdentifire だけを使用し、IA の公開鍵を SHA-1 ハッシュした値
	SubjectKeyIdentifier	所有者公開鍵を SHA-1 ハッシュした値
	KeyUsage	NonRepudation のみ ON
	certificatePolicies	本 CPS の OID を格納
	subjectDirectoryAtXXXbutes	ISO TS 17090 に準拠した hcRole atXXXbute を記述する。HcRole 以外の atXXXbute を使用しない
	basicConstraints	CA の場合：True、CA で無い場合：false

	CRLDiaXXXbutionPoints	DirectryName にて、CRL/ARL の配布点を指定

7.2. 証明書失効リストのプロファイル

MEDIS『ヘルスケア PKI 認証局証明書ポリシ』の失効リストプロファイル仕様に準じるものとし、本 CA 特有の部分のみ以下にコメントする。

フィールド	識別情報
Version	2
Signature	CA 証明書の signature に同じ
Issure	CA 証明書の issure に同じ
ThisUpdate	当該失効リストの発行日時(UTCTime)
NextUpdate	次回の発行予定日時(UTCTime)
RevockedCertificates	無効になった証明書の情報(n個記述できる)
UserCertificates	証明書のシリアル番号
RevocationDate	破棄時刻(失効日)
CrlentryExtentions	拡張項目
ReasonCode	認証局証明書の場合、子認証局作成の制限
invalidityDate	証明書無効日(オプション)
CRLExtentions	—
AuthorityKeyIdentifier	CRL に署名した認証局の鍵を区別するための ID 証明書の AuthorityKeyIdentifier に同じ
KeyIdentifier	
cRLNumber	CRL の番号

8. 本 CPS の管理

8.1. 改定手続

ポリシ委員会は、本 CPS を、証明書所有者、検証者に事前に了解を得ることなく改定する事ができる。

本 CPS 改定の際は、ポリシ委員会において改定内容を検討し、その妥当性が確認され、ポリシ委員会の承認を得なければならない。その後、CPS 改定をルート CA のポリシ委員会の承認を得る必要がある。

8.2. 公表と通知の手続

本 CA の CPS は公表しない。

8.3. CPS 承認と通知の手続

本 CPS は、CA サービスの実装と鍵ライフサイクル管理の手続きを正確に詳述する。それは CP より詳細であり、CA のセキュリティを確保するために秘密に保たれる情報が含まれている。CPS は、ポリシ委員会によって承認されるものとする。

厚生労働科学研究費補助金（医療技術評価総合研究事業）
分担研究報告書

保健医療分野におけるICカードの利用に関する研究

主任研究者　坂本　憲広　神戸大学医学部附属病院　教授

研究要旨

平成13年度では、処方箋や診療情報提供書など、保健医療施設間で頻繁に交換される保健医療文書を対象として、それに電子署名を付加するための情報モデルおよびプロトコルを研究開発した。本年度（平成14年度）は平成13年度の成果を活用し、医療施設間で実際に電子署名付きデータを交換する実証実験を行った。その中で、電子署名を大規模な保健医療機関や広域環境で利用する場合には、証明書利用者の管理、認証局の管理、私有鍵の管理など、運用上の問題が様々あることが明らかになった。そこで、個人がそれぞれの私有鍵を保管する方法として最も有効であるICカードについて調査を行った。

ICカードはこのインターネット社会において、個人を認証し、情報セキュリティを担保する有力な手段である。住民基本台帳カードや公的個人認証基盤などの整備が始まりICカードが急激に普及し始めていることが分かった。また、保健医療における活用事例も既に十分であり、ICカードの実用性の高さが明確となった。従って、今後は本研究においても、ICカードを用いた電子署名について研究していくのが妥当であると考える。

分担研究者：
山本隆一
　東京大学大学院情報学環　助教授
下川俊彦
　九州産業大学情報科学部　助教授

A. 研究目的

本研究の目的は、電子署名を保健医療分野において実用化するためにICカードの実用性を調査、検討しようとするものである。われわれが身近に目にするカードには大きく分けて、プラスチックカード、磁気カード、ICカードの3種類がある。また、やや特殊ではあるが、保健医療分野で使われることが多いものとして、光カードがある。これらのカードの形状には様々なものが存在するが、最もよく目にするものは**ISOサイズ**と呼ばれる85.6×54.0×0.76mmの形状のカードであろう。

プラスチックカードは最も単純なカードである。これには券面に様々な情報が印刷されており、エンボッサーを用いて、所有者のID番号や名前などが刻印されていたり、

あるいは手書きで書き込まれたりしている。プラスチックカードは医院や診療所などの診察券に用いられることが多い。

磁気カードは、プラスチックカードに磁気ストライプを付加したカードで、カード上の文字情報に加え、磁気ストライプにも情報を格納することができる。現在、区役所などが発行する印鑑登録証はこの磁気カードである。また、病院などで発行している診察券もこの磁気カードが殆どであり、磁気ストライプに患者番号などが書き込まれており、診察の受付の際などには磁気カードリーダーでその情報を読み取っている。ただ、磁気ストライプに書き込める情報は高々200 文字程度であり、非常に限られているため、診察券としてしようする場合には、患者番号だけしか書き込まれていない場合も多く、A 病院のシステムに誤って B 病院の磁気カードを挿入した場合にその患者番号だけを読み込んでシステムが誤動作する危険性もある。

IC カードはプラスチックカードに IC（Integrated Circuit: 集積回路）を組み込んだカードである。磁気カードと比較すると、IC チップの中のメモリに 16K バイトから64Kバイト程度の大容量の情報を記憶させることができると同時に、セキュリティ性能が大幅に向上しているため、偽造や複製が困難になっている。ＩＣカードでは、例えば、チップ表面を薄く削って直接メモリ回路に電極を繋いでメモリの内容を読み取られるリスクなど、IC カードに対する外部からの物理的侵入に対する防御、すなわち**耐タンパ性**が高いというセキュリティ特性がある。そのため、これまで磁気カードが主流であったクレジットカードなどが、最近では IC カードに移行しつつある。医療現場においても、IC カードを利用した診察券も見られるようになってきており、また、健康保険証の IC カード化への動きもある。そこで本研究では、IC カードの最近の動向と、保健医療分野における応用について調査する。

B．研究方法

本研究では、保健医療分野における IC カードの活用について、文献を主体として、調査、研究する。

また、実用例として、我々がこれまで関わったプロジェクトや神戸大学病院の事例を詳細に検討する。

C．研究結果

IC カードの種類

IC チップの情報処理性能から見ると、IC カードは、IC チップの中にメモリ（記憶装置）だけを内蔵したものと、メモリに加えて CPU（中央演算処理装置）も内蔵したものの 2 種類に分類できる。後者は言わば小型のコンピュータ本体と同じ構成であり、この種類の IC カードをメモリ機能だけの IC カードと区別して、特に「スマートカード(Smart Card)」と呼ぶ。また、IC チップのデータの読み書き方式から見ると、データを読み書きする際に、リーダライタ（IC カードのデータ読み書きの装置）と IC カードを接触させる必要のある、接触型 IC カードと、IC カードをリーダライタに近づけるだけでデータの読み書きが可能な非接触型 IC カードに分類できる。（図 1）非接触型

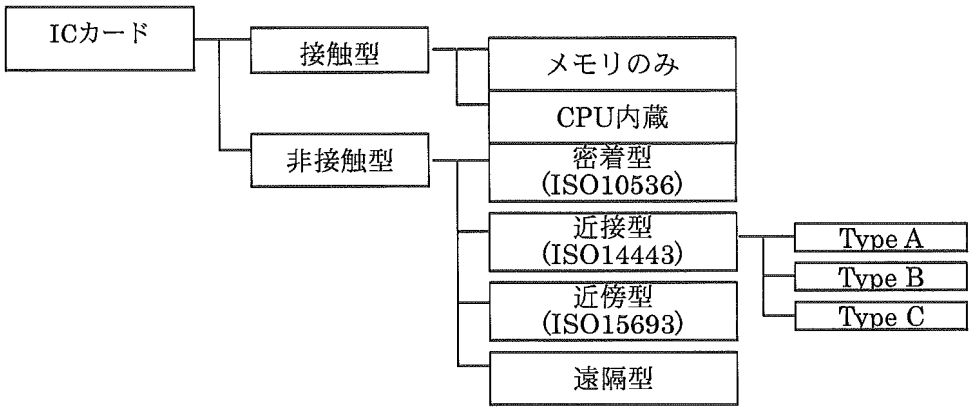

図1. ICカードの分類

IC カードは、IC チップの周りをアンテナがコイル状に取り巻いている。この内蔵アンテナコイルはデータを送受信するだけではなく、リーダライタからの電波から微弱な電力を発生し、IC チップに電力を供給している。そのため、リーダライタとの接触も不要であり、また、電池などの電源も不要である。

接触型 IC カードは、非接触型 IC カードに比べ、データの読み書きが安定しているというメリットがあるが、接触面の磨耗や腐食などのデメリットがある。そこで接触式 IC カードでは、接触面を金メッキしている。接触式 IC カードはキャッシュカードやクレジットカードに採用されている。また、ドイツやフランスなどでは、健康保険証が接触式 IC カード化されて、全国民に普及している。一方、非接触型 IC カードは、IC カードリーダライタに IC カードを近づけるだけで、データの読み書きが可能であるため、使用が非常に容易である。また、IC カードリーダライタに装着する必要がなく、IC カードの接点の物理的劣化や動作不良の可能性少なく、耐久性が高いという利点がある

非接触型 IC カードは、リーダライタとの通信距離（電波の届く距離）によって、さらに、「密着型」(ISO/IEC10536)、「近接型」(ISO/IEC 14443)、「近傍型」(ISO/IEC 15693)、「遠隔型」に細かく分類される。密着型 IC カードはデータ伝送距離が約 2mm 以下であり、接触型 IC カードのようにリーダライタに IC カードを挿入するか、あるいはリーダライタに軽く触れるくらいまで近づけて使うため、使いやすさは接触型 IC カードと余り変わらないが、接触面の磨耗などの心配がなく、耐久性に優れている。近接型 IC カードはデータ伝送距離が約 20cm 以下であり、近傍型 IC カードは約 1m 以下、遠隔型 IC カードは数 m 程度のデータ伝送が可能である。しかしながら、伝送距離を長くするためには、その分電波の強度も強くする必要があるため、医療現場においては医療機器への影響の可能性もあり、

使用環境や使用方法などを考慮した上で、最適なICカードを選ぶ必要がある。

電波法が改正されたこともあり、最近では、非接触型ICカード、特に近接型ICカードの利用が増えてきている。この近接型ICカードは、符号化方式や通信速度によって「Type A」「Type B」「Type C」の3種類がある。Type A、Type BはISO/IEC 14443に適合しており、Type Bは、住民基本台帳カードに使用される予定である。一方、Type CはソニーとドイツInfenion Technologies社が開発した非接触ICカード技術であり、FeliCa方式とも呼ばれる。現在日本がISOに提案中であるが、データの高速処理が可能であり、電子マネーや交通機関のプリペイドカード、定期券に向いているため、JR東日本の運賃決済用非接触型ICカード「SuiCa」カードなどに使用されており、大量に普及し始めている。

ICカードにはさらに、ハイブリッドカード(Hybrid Card)とコンビネーションカード(Combination Card)の2種がある。ハイブリッドカードは、非接触型ＩＣチップと接触型ＩＣチップの両方を一枚のプラスチックカードの中にそれぞれ埋め込んだものである。既存システムとして接触型ICカードリーダを利用したシステムがあり、さらに別の新しいシステムが非接触型ICカードを利用するような事例で使用されている。コンビネーションカードは、さらに進んだ方式であり、非接触型ICチップと接触型ICチップを一つのチップとしたものである。CPUやメモリを共有することが可能なため、ハイブリッドカードと比較すると、コストを低く抑えることができると同時に、アプリケーションでの応用も広くなる。

ICカードの利用方法

ICカードの利用方法は、大きく2つに分けられる。1つは主としてICカードのデータ記憶容量の大きさに注目した利用であり、ICカードの所有者の様々な個人データをICカードに保存しようとするものである。特に医療分野では、個人の検査データや処方データをICカードに書き込んで、異なる医療機関で情報を共有する試みがなされている。2番目の利用方法は、主としてICカードのセキュリティ特性に注目した利用であり、個人識別番号などの個人情報に繋がるキーとなるデータだけをICカードに格納し、ICカードを個人の認証のために利用する方法である。ICカードで利用して処理したい情報の増加、ネットワークの普及に伴い、後者の利用方法が主流となってきている。

最近では、1枚のICカードを1つの特定の目的、あるいは特定のアプリケーションだけで使うのではなく、複数のアプリケーションで共有して利用する方法も増えてきている。すなわち、ICカードのメモリ内を分割して、そのICカード発行主体とは異なる他のアプリケーションに対し開放し、1枚のカードで複数の機能を実現するマルチアプリケーションカードも普及し始めている。例えば、電子政府や電子社会を支える基盤技術の1つである、公開鍵基盤(PKI)の整備が始まり、その秘密鍵をICカードに格納することも行われ始めており、印鑑にも使用目的によって、実印、銀行印、認印など何種類もの使い分けをするように、1枚のICカードに複数の秘密鍵を格納しておき、用途によって使用方法を変えるような利用方法も行われ始めている。また、e-Japan 重

点計画では、行政機関が発行するICカードに関しては、国民の利便性の向上、行政コストの削減を図るため、複数の情報を相乗りさせることを検討している。

ICカードの利用例

IC カードの利用例は、JR 東日本の SuiCa や、経済産業省による平成 12 年度「IC カードの普及等による IT 装備都市研究事業」などをきっかけに利用が急速に拡大しつつある。さらに 2003 年 8 月には住民基本台帳カード(略して住基カード)がスタートする予定である。

住民基本台帳カードは、平成 11 年 8 月に住民基本台帳法案が成立し、2003 年 8 月 25 日から全国の市町村で希望者に交付することに決定している。この住民基本台帳カードは公的な身分証明書代わりに用いることができ、このカードを用いれば、転出、転入の行政手続きを始めとする様々な行政サービスを受けることができる。

経済産業省は「IC カードの普及等による IT 装備都市研究事業」は、172 億円を計上し、住民基本台帳カードや健康保険証、介護保険証等、複数の行政系カードと、診察券、プリペイドカードなどの民間発行のカードを1枚のマルチアプリケーションICカードとする「連携 IC カード」を実装して、来るべき電子社会の都市像を研究している。全国の 21 地域、54 の地方公共団体で様々な「連携 IC カード」の実証実験が行われ、約 120 万枚の非接触マルチアプリケーション対応ICカードと約 9000 台のリーダライタが配布され、延べ 100 種類の住民サービスが提供されている。

保健医療分野におけるICカードの利用

保健医療分野における IC カードの利用方法としては、先に述べたとおり、1)病歴、薬歴、検査結果、血液型、感染症、アレルギー情報などの主要な診療情報を記録し、異なる医療機関での情報共有を可能にするための可搬型記憶媒体、2)健康保健、介護保険などの被保険者番号、医療機関の患者番号、などの情報を記録し、本人確認を可能にするための ID カード、の 2 通りがある。光カードは 1-2M バイトの記憶容量を有するため、可搬型記憶媒体としてよく用いられているが、IC カードは高々64K バイト程度であるため、可搬型記憶媒体としての有用性に劣る。また大容量の光カードであっても画像や波形データを考慮すると不十分であり、ネットワーク化が進むにつれて、セキュリティの高い ID カードとしての利用が主流となりつつある。

兵庫県津名郡（淡路島）五色町では、1989 年に保健医療情報を IC カード化した。これが国内で最初の例であり、人口約 11,000 人で約 4,800 枚の IC カードを配布している。その後、全国各地で保健医療情報の IC カード化が試みられているが、小規模なものが多い。しかしながら、1991 年には兵庫県加古川市、稲美町、播磨町の 3 地区が合同で「地域保健医療情報システム」を構築し、地域住民に5万枚以上のICカードを配布し、住民検診などに活用している。また、愛媛県西条市でも、1994 年から、65 歳以上の高齢者と乳幼児に対して、保健、医療、福祉サービスを利用するための IC カードを発行している。これらの IC カードはいずれも患者の診療情報を記録した可搬型記憶媒体としての利用が主である。

IC カードを利用した保健医療情報ネットワークの実例

保健医療情報システム検討会による「保健医療分野の情報化に向けてのグランドデザイン最終提言」において求められている「医療施設のネットワーク化」に向けて「情報セキュリティの確保」、「個人情報の保護対策」が適切に行われることがシステム構築の重要な要件となっているため、特に保健医療分野においては e-Japan 重点計画に記載された施策に加えて特殊性を配慮して対策を立てる必要がある。このことから、「電子認証システムの構築」、「IC カード等の医療分野での活用」を推進することが求められている。そのため、IC カードをセキュリティの高い ID カードとして活用する事例は今後増えてくるもと思われる。われわれは、これまで接触型 IC カードを用いて、医師や患者の認証を行うシステムを構築してきたので、その事例を詳細に調査した。

福岡市医師会プロジェクト

われわれは平成 13 年に、経済産業省「先進的 IT 技術を活用した地域医療ネットワーク公募事業」の 1 事業として、福岡市医師会と九州大学病院を中心とした、「公開鍵基盤を利用した広域分散型糖尿病電子カルテネットワーク開発事業」を行った。この電子カルテは、国民病といわれるほど罹患率が高く、生涯にわたるコントロールが必要で、かつチーム医療が望まれる、糖尿病をターゲットとした電子カルテである。この電子カルテネットワークでは医療従事者、患者がともに接触型 IC カードを所有し、公開鍵基盤（PKI）と呼ばれる最新のセキュリティ技術を利用し、ネットワークで共有される患者情報の保護を完全にしている。（図 2）この糖尿病電子カルテネットワークには大学病院をはじめとし、地域の中核病院、糖尿病専門病院、眼科病院、透析病院などの医療機関だけではなく、調剤薬局、フィットネスクラブ、保健所など、福岡市

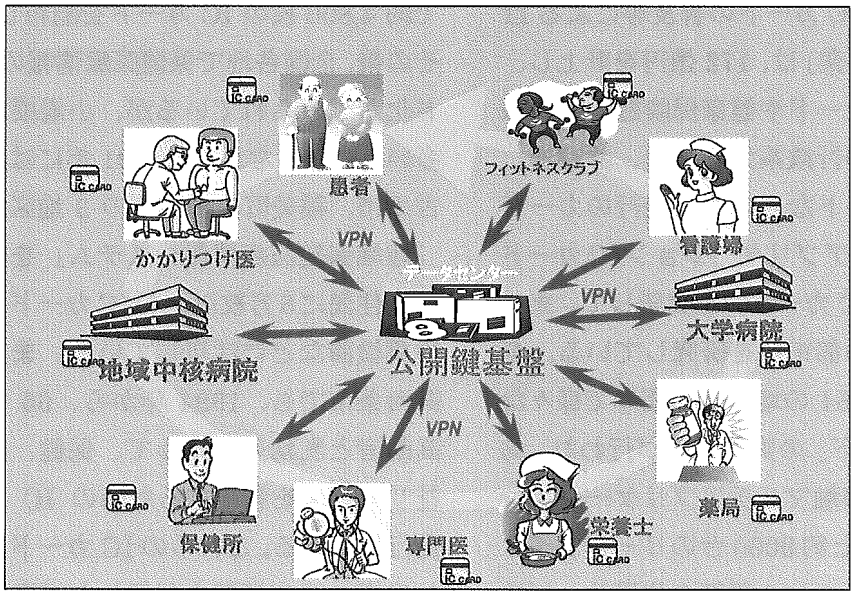

図2. 福岡市医師会プロジェクト