IC カード型電子マネーセキュリティ

平成 10 年 3 月

電子商取引実証推進協議会（ECOM）

1 はじめに

我が国の消費社会における決済の仕組みは、現金、クレジットカード、手形、銀行振込、プリペイドカードなどの各種形態があるが、小口決済は現金によるものが圧倒的に多く、ＩＣカードを活用した小口決済の電子化が望まれている。昨今、ＥＣ分野におけるＩＣカードを取り巻く環境が一変し、各国で様々な技術開発および実証実験が行われている。特に MasterCard/Mondex, Visa, GeltKarte, PROTON のストアードバリューカードは広い範囲で実験が行われている。

ＩＣカードによる電子マネーシステムにおいては、ＩＣカードの偽造等の犯罪が考えられる。また、実際に偽造したＩＣカードが出回れば被害は甚大である。そのためあらゆる脅威を洗出し、暗号、認証等の技術あるいは管理技術により十分な対策を講じる必要がある。

近年ＩＣカードにおいて電子マネー等に活用されることを考慮し、ＲＳＡの公開鍵暗号処理を高速で実行するための専用プロセッサ付きのチップもあり、ＩＣカードの認証、ディジタル署名に応用可能である。従って、ＩＣカード内の電子マネーをＩＣカードと端末間あるいはネットワークを介して金融機関システムと安全に転送する仕組みが可能となった。

また、一方においては消費者保護のための安全対策も必要であり、電子マネーという価値移転時の正当性の保証あるいはプライバシ保護が必要である。

本報告書はＩＣカードの電子マネーシステムに対して発生する可能性のある脅威を洗出し、電子マネーシステムのセキュリティ機能要件をまとめたものである。

本報告書は、電子マネーシステムを構築するＳＥ（システムエンジニア）などを対象にまとめたものであり以下のような利用方法を想定している。

- 電子マネーシステムを構築するＳＥが、対象とするシステムのノード分析により発生しうる脅威を認識する。
- 電子マネーシステムを構築するＳＥが、要求されるセキュリティのレベルに応じて実現すべきセキュリティ機能を明確にする際のガイドラインを提供する。

国内において、今年から各種の電子マネー実験が本格化しようとしている。これにさきだって取りまとめたところに本ガイドラインの意義があると考える。

ＥＣＯＭセキュリティワーキンググループ委員の中で議論しまとめたものであり、脅威の対策としてのセキュリティ機能、機能の必要度（必須、推奨、選択）、必要度の評価の理由、を明記している。ご意見を頂いて、今後より一層の充実をはかっていきたい。

2　本ガイドラインの対象とするシステム

現在ＩＣカード型電子マネーあるいはプリペイドマネーシステムは参考資料1の例にあるように世界中でトライアルが行われているが、電子マネーに対する信頼性から発行母体はいずれも金融機関であることが多い。現在日本においては、地域を限定して特定の商店街、ビルの内部で使用されており、発行母体は共同組合となっているが今年から金融機関を母体とするトライアルが本格化しようとしている。

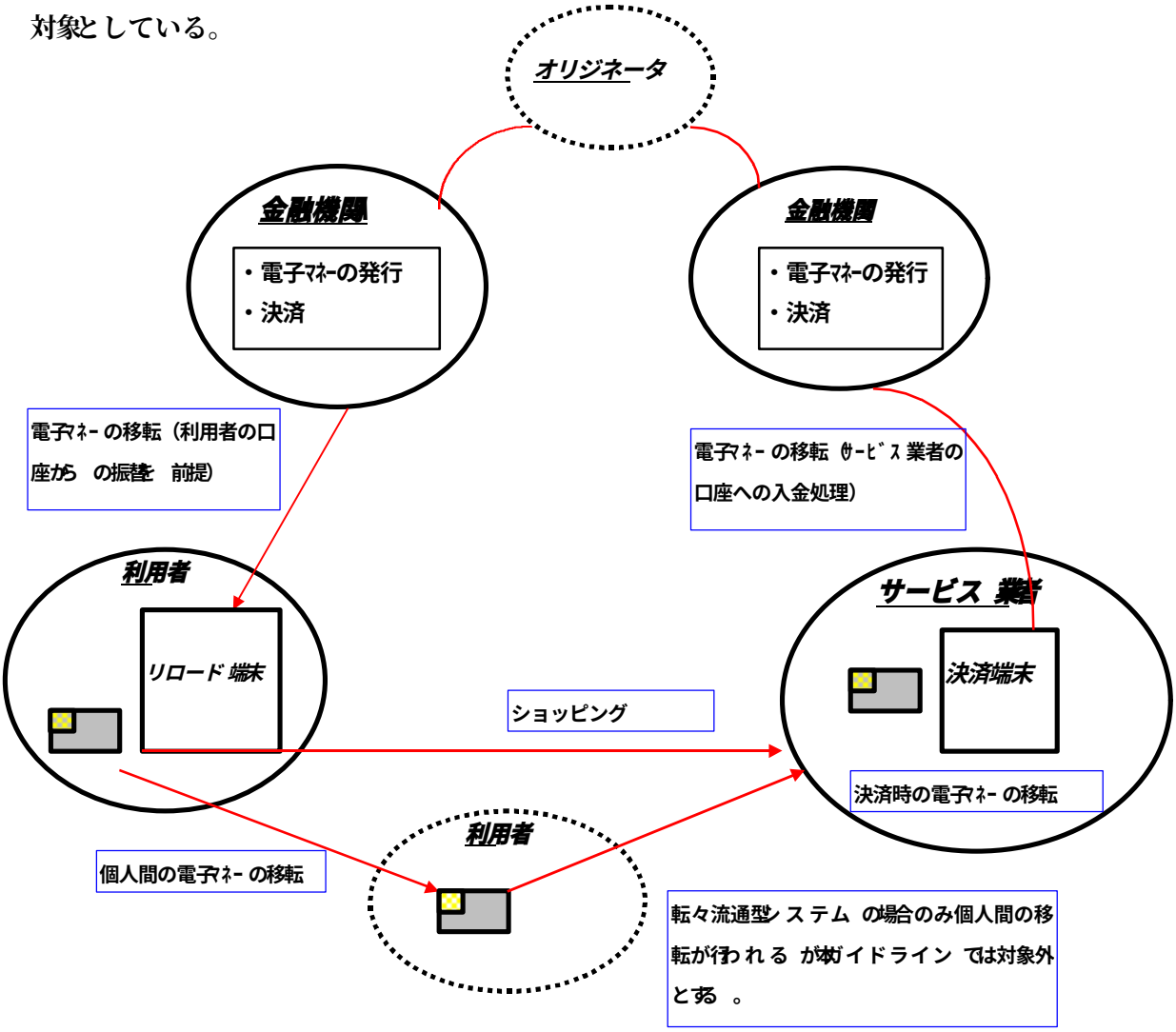
また、参考資料1にあるようにグローバルに展開されているトライアルの例ではいずれも安全性に対する配慮があり、昨今はＩＣカード内部における暗号処理機能を利用し、相互認証等を行っているケースが多い。

本ガイドラインの対象とするシステムは、このような状況をふまえて

○　金融機関（銀行、クレジットカード会社等）が発行母体

○　地域を限定せずグローバルな展開が可能なシステム。

の2条件を前提とし、セキュリティ技術を使用し、安全性の確保が要求されるシステムを対象としている。



3 ＩＣカード型電子マネーシステムとセキュリティ技術について

ＩＣカード型電子マネーの普及を図るためにはセキュリティの確保が最重要課題である。電子マネーシステムの脅威については、６章にまとめてあるが、各ノード毎にいろいろな脅威が考えられ、各脅威毎に対策を立てる必要がある。特にＩＣカードの偽造あるいは端末ソフトウェアの改ざん等により不正にマネーが創造された場合、被害が甚大となる。ＩＣカード型電子マネーにおいて決済時の安全性を保証するためには、

① 端末とＩＣカードの相互認証機能（偽造されたＩＣカードあるいは端末機を排斥する機能）

② 通信相手の真正性を常に確認しながら通信する機能（なりすまし、改ざん、否認等の防止）

③ メッセージの秘匿

などが必要である。これらの脅威に対する技術として最も有効なのが暗号技術である。

(1) 一般的に使用されている暗号処理技術

(a) 共通鍵暗号方式

共通鍵暗号方式は、対称型暗号方式とも呼ばれ、メッセージの暗号化と復号化で同じ鍵を使う方式である。従って、メーセージの送り手と受け手は秘密の鍵を共用することになる。本方式は高速な演算処理が可能であるが、全利用者ＩＣカードに共通の鍵を書込んでおくことになり、共通鍵が解かれた場合の被害が甚大となる。ＩＣカード毎に共通鍵を変える方式については、参考資料2 (7)を参照されたい。

共通鍵暗号方式の代表的なものにＤＥＳ方式がある。

(b) 公開鍵暗号方式

公開鍵暗号方式は、非対称型暗号方式とも呼ばれ、メッセージを暗号化する鍵（公開鍵）と復号化する鍵（秘密鍵）の２つの鍵を使用する。２つの鍵には数学的な関係があり、２つの鍵の内の一方の鍵で暗号化したデータを復号化できるのはもう一方の鍵を使用した場合に限られる。また、公開鍵から秘密鍵を解くことが困難であることが数学的に証明されている。暗号通信時は相手の公開鍵で暗号化して、他方が自分の秘密鍵で復号化し、デジタル署名時は秘密鍵で暗号化して、公開鍵で復号化する。公開鍵暗号方式においては、秘密鍵が別の者に開示されなければ、保証される。よく知られた公開鍵暗号方式としてＲＳＡがある。

昨今ＩＣカードにおいてＲＳＡの公開鍵暗号処理を可能とするため、ＲＳＡを高速で実行するための専用のプロセッサを持ったＩＣカードがある。

(c) デジタル署名

ＩＣカードからＩＣカードへ電子マネーを転送する場合、上記②のなりすまし、改ざん、否認防止等通信相手、データの真正性を常に保証するため、デジタル署名技術が有効である。すなわち、平文を転送する場合、平文のハッシュに対し、自分の秘密鍵で暗号化して平文と共に転送し、相手側のＩＣカードは、送り手の公開鍵で復号化し、更にデータ部のハッシュを取り、送られてきたハッシュと照合を取って、真正性の保証を行なう。

(2) 相互認証機能

ＩＣカードが偽造されたカードでないことを証明するため端末－ＩＣカード間で相互認証を行うことが有効である。ＲＳＡ方式の場合の相互認証機能には一般的に以下のような方式がある。

(a) 端末主導／ＩＣカード主導方式

① 端末主導方式

相互認証機能を端末のソフトウェアで実現する方式。ただし、鍵情報は端末内のＩＣチップ（セキュアアプリケーションモジュール）内に保有する方式が一般的である。

② ＩＣカード主導方式

相互認証をＩＣカード内のファームウェアで実現する方式。従って、上記と同様端末内にＩＣカード（あるいはＩＣチップ）を保有し、端末内ＩＣカードとＩＣカード間で相互認証を行う（端末のソフトウェアは各ＩＣカードに対して処理を仲介する機能のみとする）。

(b) 相互認証のアルゴリズム（静的認証／動的認証）

① 静的認証

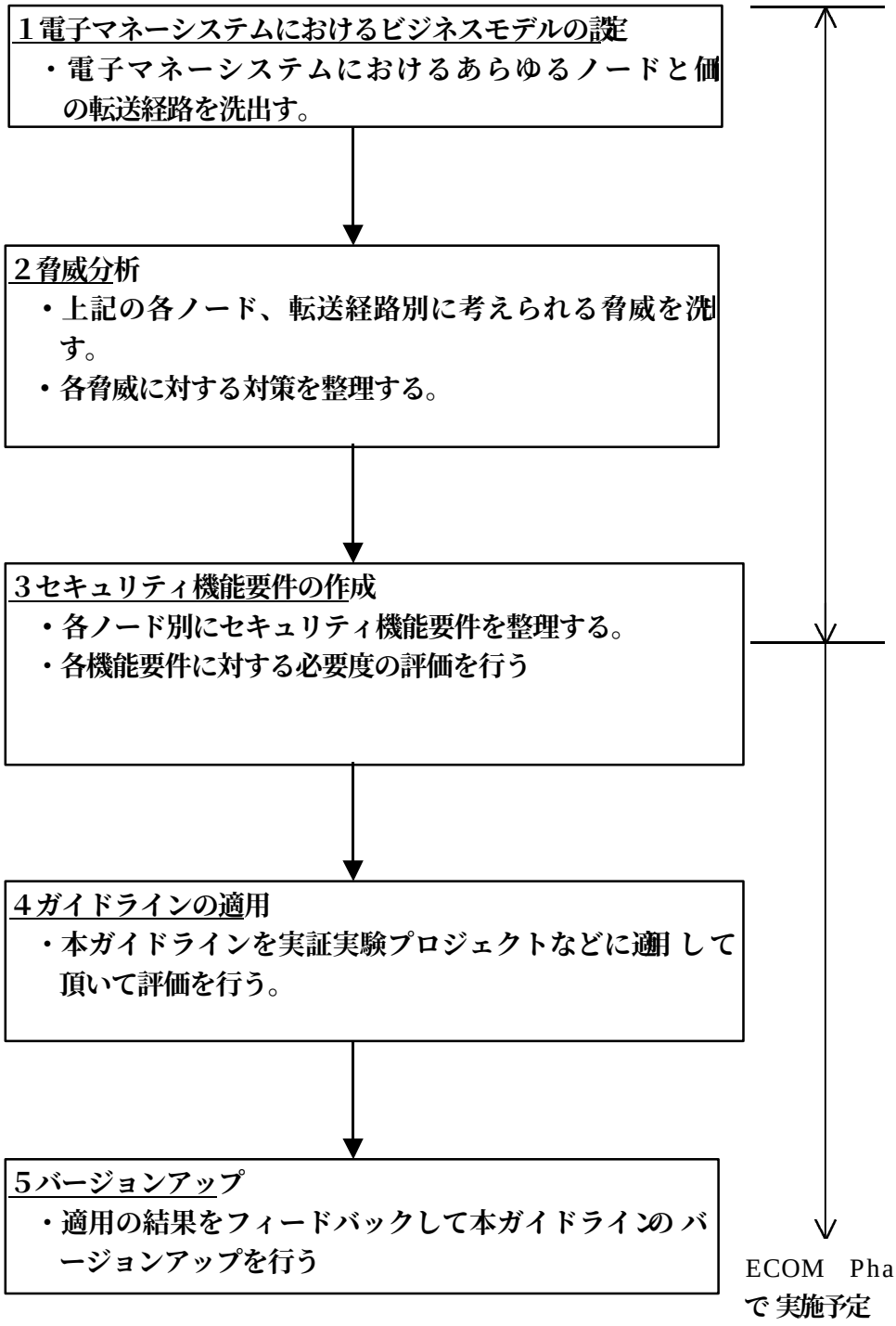
あらかじめ書込まれた公開鍵証明書を互いに交換し、証明検証することで正規のカードかどうかを判定する。

② 動的認証

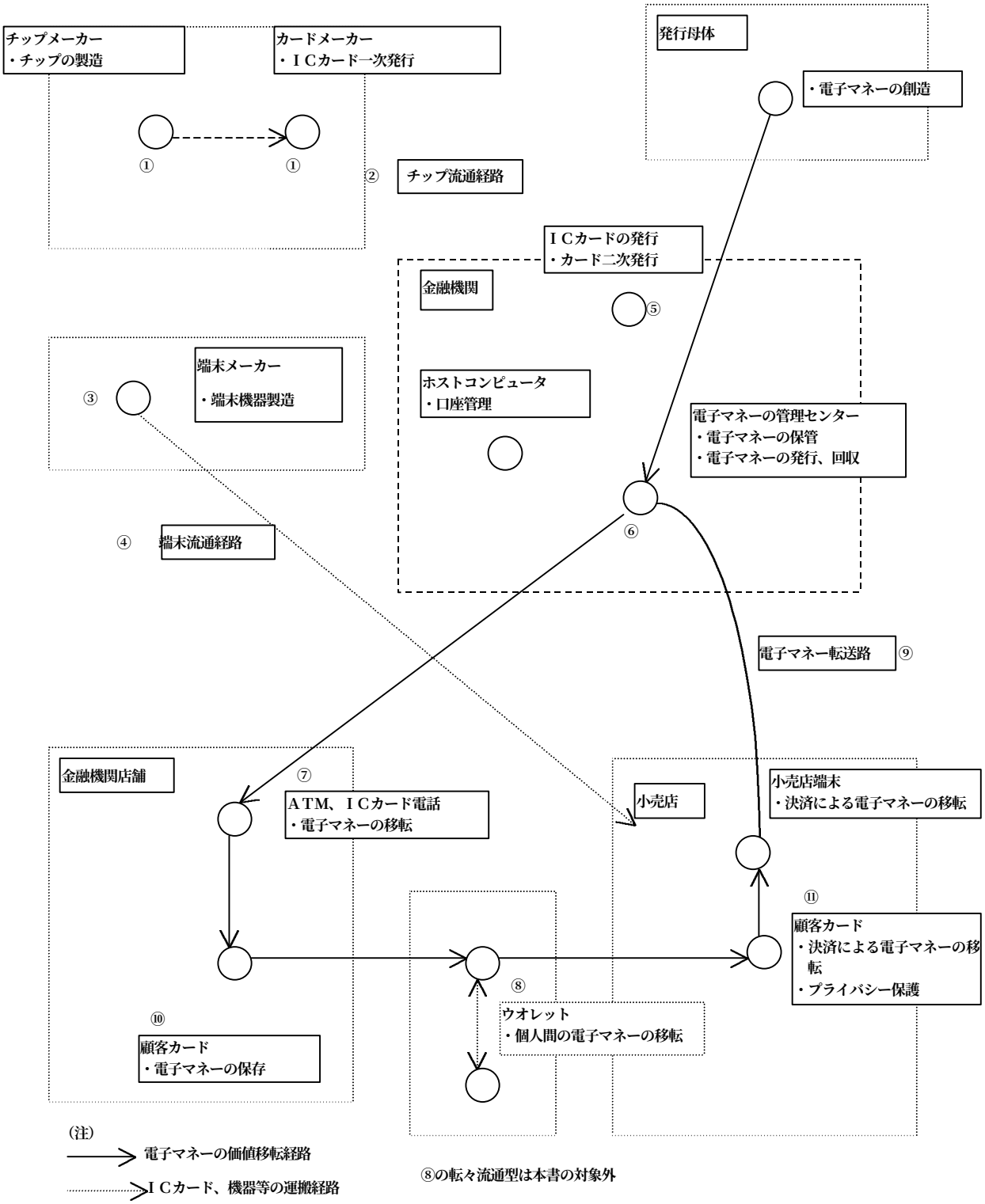
動的認証の場合は上記の認証に加え、端末で発生させた乱数をもとに、ＩＣカード内でＩＣカードの秘密鍵で署名し、端末に送り、署名を検証するフェーズを追加したものである（ＩＣカード電子マネーの認証技術については、参考資料2を参照のこと）。

4 ガイドラインの作成手順

ＩＣカード型電子マネーシステムにおけるガイドライン作成にあたり、①システムのモデル化 ②当該モデルにおける脅威分析 ③各ノード別のセキュリティ機能要件の整理 ④セキュリティ機能必要度の評価の順で作業を行った。



5 ＩＣカード型電子マネーのノード分析劃



6 ＩＣカード型電子マネーの脅威分析のまとめ

（注）№は前章5.ノード分析事例の各ノード番号である。

脅威の内容			脅威の具体的内容						発生の可能性	対策（機能要件）
NO	ノード	内容	誰が	いつ	どこで	何を	目的	方法		
①	ＩＣカード、チップの製造	カード、チップの流出	製造業者の従業員	人のいない時	製造工場内で	出荷前のカード、チップを	第三者に売却するために	カード、チップを盗んで	製造工場の従業員と犯罪集団との共謀により可能	①厳密な数量管理 ②施錠のあるロッカで保管する ③製造番号を付ける
①	ＩＣカード、チップの製造	チップの不正解析	チップの開発経験者	いつでも	研究室で	ＩＣカードのチップを盗んで	ＩＣカードの偽造のため	設計資料を盗んでチップを解析して	チップの開発・研究に従事する者で相当な研究設備を保有する者（電子顕微鏡で解析するなど）	①ROMエリアの格納場所について工夫する（電子顕微鏡での解析を防ぐため）
①	ＩＣカード、チップの製造	チップへの不正アクセス手段の開発	チップの開発経験者	いつでも	研究室で	ＩＣカードのチップを	自分のＩＣカードのﾊﾞﾘｭｰを増やすため	設計資料を盗んでチップのＲＯＭ内容を解析して	チップの開発・研究に従事する者で相当な研究設備を保有する者	①自己診断機能の保有
①	ＩＣカード、チップの製造	チップを故意に誤動作させる（ストレス、熱等による）	チップの開発経験者	いつでも	研究室で	ＩＣカードのチップに対して	自分のＩＣカードのﾊﾞﾘｭｰを増やすため	誤動作内容を解析して	チップの開発・研究に従事する者で相当な研究設備を保有する者	①自己診断機能の保有
②	ＩＣカードの流通経路	ＩＣカード、チップの盗難 廃棄されたＩＣカードの不正利用	運搬業者が（ＩＣカードメーカが）	金融機関への輸送途中に	金融機関への輸送途中に	ＩＣカードを犯罪者に横流しする	偽造集団にＩＣカードを売って利益を得る	ＩＣカードを犯罪者に横流しする	運送業者と偽造集団の共謀により可能	①チップに対して鍵をかけ相手に極秘にを渡す ②ＩＣカードのアクセス方式（コマンド仕様）を漏洩しない ③ＩＣカードの廃棄処理の徹底
③	端末機器製造業者	端末機器のソフトの改ざんによる不正使用	端末設計者	いつでも	端末製造メーカ	端末内の電子ﾏﾈｰ	端末内の電子ﾏﾈｰを不正に増やす	ICｶｰﾄﾞのアクセス方法を解析して	端末ソフト開発経験者	①ＩＣｶｰﾄﾞｱｸｾｽﾃﾞｰﾀを暗号処理する ②ＩＣｶｰﾄﾞｱｸｾｽﾌﾟﾛｸﾞﾗﾑのマスク化 ③暗号処理のＬＳＩ化 ④筐体の不正開放によりソフトウェアを消滅させる

脅威の内容			脅威の具体的内容						発生の可能性	対策（機能要件）
NO	ノード	内容	誰が	いつ	どこで	何を	目的	方法		
④	端末機器流通経路	端末機器の盗難廃棄された端末機器の不正な利用	運搬業者が	小売店への輸送途中に	小売店への輸送途中に	端末機器を犯罪者に横流しする	偽造集団に端末機器を売って利益を得る	輸送中に犯罪者に横流しする	運送業者と偽造集団の共謀により可能	①内部管理の徹底 ②製造番号（端末固有番号）による管理 ③出荷段階では運用不可能とする
⑤	ＩＣカードの発行	ＩＣカードの不正発行	ICｶｰﾄﾞ発行事務のオペレータ	発行手続き中	銀行の事務センタ	申込用紙の内容を盗んで不正にカードを作成	偽造カードを作目的で	カードの申し込用紙を盗む	内部犯行（オペレータと管理者と共同で犯行が可能）	①発行履歴の管理資料を作成する。 ②内部監査の実施 ③発行作業場所への入退室管理の徹底
⑤	ＩＣカードの発行	鍵情報の漏洩	ICｶｰﾄﾞ発行事務のオペレータ	発行手続き中	銀行の事務センタ	鍵情報の書かかれているファイルを盗む	偽造カードを作目的で	鍵情報ファイルの場所を開発者から聞いて	システム開発者の犯行（鍵情報の格納ﾌｧｲﾙを知っている者だけが可能）	①鍵情報ファイルへの不当アクセスの防止。 ②発行済み鍵情報ファイルの厳重な管理。 ③鍵生成オペレーションの権限管理機能
⑥	電子マネーの管理センタ	電子マネー管理センタ内の電子マネーを不当に取得	システムの開発者と内部の者が共謀して	管理者のいない時	電子マネーの管理センタの設置してある建物内	電子マネーを不当に取得する	電子マネーを盗むために	テストシステムを使用して	システム開発者と内部のオペレータとの共謀(テストシステム等の使用により可能)	①金融機関システムの口座からの引落しを前提とすれば不可能だが、システム開発者のテストシステム等の使用により可能となるため本番システムから削除する。
⑦	電子マネーの転送経路	不当な利用者による電子マネーの不正引き出し	紛失・盗難・偽造カードの取得者	電子マネーの引き出し時	端末の設置場所	自分のICカードに価値移転	電子マネーを不正に増やすこと	不正な端末操作	不正カードを犯罪者、或いは、犯罪組織から入手することで発生する可能性がある。	①金融機関ホストでの本人認証（本人確認） ②ICカード認証 ③取引きの追跡と管理
⑦⑨	電子マネーの転送経路	不正なICカード、または、不正な端末機器による電子マネーの移転	システム内部精通者や犯罪組織	電子マネーの移転時	端末機器設置場所	不正なICカード、あるいは、端末機器で不正に電子マネーを移転	電子マネーを不正に取得する	盗難または変造、あるいは、偽造したICカードや端末機器を用いる	開発者や開発経験者、或いは保守員等の内部精通者と窃盗・変造・偽造組織との結託により発生する可能性がある。	①取引き相手認証と認証失敗回制限とロギング ②IC カードの有効性の確認 ③端末機器の変造・複製の防止 ④取引き証拠の保存と管理
⑦⑨	電子マネーの転送経路	金融機関内部での不正な電子マネーの転送	電子マネーの管理センタの開発経験者	人のいない所	特別に開発した端末で電子マネー引出し時	不正に電子マネーを自分のＩＣカードに移転し	電子マネーを不当に増やすことを目的に	電子マネーの管理センタへの不正なアクセス方法を開発して	システム開発者と犯罪者が共謀することで可能	①相手認証による顧客カードや端末機器のなりすまし防止 ②金融機関ｼｽﾃﾑによる認証(本人確認) ③取引ログの取得 ④端末機の不当アクセス防止と改ざん検出
⑦⑨	電子マネーの転送経路（銀行ATM,電話端末間）	金融機関の電子マネーの管理センタからＡＴＭ,電話端末等により不当に電子マネーを取得する	端末開発経験者	改造した端末機を使用して	改造した端末機を使用して	改造した端末により不当に電子マネーを転送する	電子マネーを不当に取得することを目的に	端末のソフトを改竄して	本システムにおける端末開発経験者	①相手認証による顧客カードや端末機器のなりすまし防　止 ②金融機関ｼｽﾃﾑによる認証(本人確認)

脅威の内容			脅威の具体的内容						発生の可能性	対策（機能要件）
NO	ノード	内容	誰が	いつ	どこで	何を	目的	方法		
⑦⑨	電子マネーの転送経路（銀行と端末間）	電子マネーの移転経路を分岐させ他のカードに価値を移転させる	システム内部に精通した者が	電子マネー転送時に	電子マネー転送経路に	電子マネーを自分のＩＣカードに不当に取得する	電子マネーを不当に取得することを目的に	電話網に他のＩＣカードを分岐接続してなりすまして	カードとカードの転送方式をモニタすることでなりすましを行えば可能	①相手認証による顧客カードや端末機器のなりすまし防止 ②金融機関ｼｽﾃﾑによる認証(本人確認) ③取引ログの取得 ④端末機の不当アクセス防止と改ざん検出
⑨	電子マネーの移転経路（小売店銀行間）	電子マネーの管理センタになりすまして小売店端末からのバリューを所得する	通信業者等が	小売店端末から銀行にバリュー転送時	転送経路上で	電子マネーを自分のＩＣカードに不当に取得する	不当に電子マネーを取得することを目的に	電子マネー管理センタになりすますサーバを開発して	電子マネーの管理センタの仕組みを熟知した者に限定される	①端末による顧客カードの認証 ②ﾃﾞｼﾞﾀﾙ署名によるなりすまし防止 ③金融機関ｼｽﾃﾑによる認証(本人確認) ④取引ログの取得
⑩	顧客ＩＣカード(消費者)	紛失・盗難	ＩＣカード保有者が	いつでも	どこでも	ＩＣカードを	他人のＩＣｶｰﾄﾞを利用して電子ﾏﾈｰを引出すことを目的に	他人の財布を盗んで	常に盗難の可能性がある	①ＩＣカードのロック機能 ②リロード時のパスワードチェック機能 ③紛失時の事故設定機能 ④紛失時の残高保証機能
⑩	顧客ＩＣカード(消費者)	電子マネー移転の否認	ＩＣカード保有者が	引出し時	ATM、ＩＣカード電話により	電子マネーを引出し後、引出した事実を否認して	電子マネーを不当に増やすことを目的に	引出した事実を金融機関に対して否認する	常に否認されるの可能性がある	①ﾃﾞｼﾞﾀﾙ署名による認証の実施 ②カード内の取引ログの取得と証明
⑩	顧客ＩＣカード(消費者)	プライバシの侵害（消費者保護）	金融機関のセンタが	買い物時	金融機関のセンタシステムにおいて	消費者の取引履歴をすべて取得して	消費者動向をつかむ目的で	小売店の取引明細データをすべて吸上げて	金融機関システムの運用者は可能	①取引履歴取得時の情報を最小限とする ②情報の保管資格者を特定する ③取引ログの暗号化
⑪	加盟店端末	買物代金以上の電子マネーを顧客から引出す	小売店の店員が	買物代金決済時	小売店で	買物代金以外のｵﾍﾟﾚｰｼｮﾝにより余分の電子マネーを引出す	不当に電子マネーを取得することを目的に	不正なオペレーションを行って	小売店の店員がシステム開発者と共謀して別の方法でセンターへのファイル伝送を可能とすれば	①端末機の不当アクセス防止と改ざん検出 ②取引ログの取得
⑪	加盟店端末	加盟店端末内の売上データの改竄（端末の盗難）	小売店の店員が	管理者のいない時	小売店で	端末内に蓄積した売上情報を	売上情報を改ざんして別の口座に入金する目的で	売上情報を別の方法でセンタにファイル伝送することで	小売店の店員が金融機関システム関係者と共謀して特殊なオペレーションを組みこめば可能	①売上げ情報に対し、ディジタル署名を付加 ②売上げ情報受信時の署名検証の実施

7 ＩＣカード型電子マネーシステムのセキュリティ機能

7.1 セキュリティ機能のまとめ方について

前述の脅威分析においてはノード別に脅威と対策をまとめたが、セキュリティ機能要件を記述するにあたり、共通要素をもとに以下の分類でまとめた。

・ＩＣチップ、ＩＣカードに対するセキュリティ機能要件
・各端末機器のセキュリティ機能要件
・電子マネーの発行機関における運用とセキュリティ機能要件
・電子マネーの価値移転時のセキュリティ機能要件
・消費者保護についての要件

また、各機能要件に対して、以下のような必要度の評価とその理由を記した。

A．システムへの組込みが必須なもの。- ----- ◎

B．システムに組込むことが望ましいもの。- ----- ○

C．組込むかどうかシステムの特性を考慮して選択すべきもの。- ---△

更に各節の終わりに必要度評価の根拠について補足解説として記述した。

7.2 ＩＣチップ、ＩＣカードに対するセキュリティ要件

7.2.1 ＩＣチップ、ＩＣカードの製造過程における機能要件（不正流出の防止）

(1) 脅威とセキュリティ機能

ＩＣチップ、ＩＣカードの製造過程において、製造工場からＩＣチップのハードウェア構成図やＲＯＭに格納されるＯＳなどの情報、または製品そのもの等の不正な流出により、偽造カードが作成され運用される可能性がある。よって、製造工場内での取扱い管理や保管管理時の不正流出を防止するとともに、製造工場全体ののセキュリティを確保する必要がある。

(2) 機能要件

(a) ＩＣチップの開発／設計時における管理

ＩＣチップの設計段階における情報や設計図そのもの流出により、偽造カードの作成等行われる可能性がある。よって、ＩＣチップ設計時における工場の管理体制によってセキュリティを確保する。

① 複数設計者による開発／設計

開発／設計時に情報が漏洩した場合、開発／設計ブロック毎に担当者を分けることで情報全体の流出を防ぐ。 ◎

② 開発／設計者の管理

設計図や仕様書等の情報を部署内または工場から持ち出せないよう入退室管 ◎

理や作業者のチェックを厳密に行うことで情報の流出を防止する。

③　設計図および仕様書等の情報管理

不要になった設計に関わる書類、データまたはサンプル製品等の処分については、焼却、消去、破壊等により情報の流出を防止する。

④　ROMデータの情報管理

ROMデータ作成時において、一般で使用されていない独自のプログラム言語の使用することで、情報の流出を防止する。

(b)　ＩＣカード製造時における管理

ＩＣカードを製造する工場から製品が流出した場合、不当にＩＣカードを運用される可能性がある。工場の管理体制によってセキュリティを確保する。

①　工場入庫時におけるＩＣチップ、ＩＣカードの受入管理

受け入れ時に入庫形態、品番、数量、入庫場所、担当者、管理番号等のチェックを行うことで、ＩＣチップやＩＣカードの流出を防止する。

②　加工作業前の管理

加工作業前に使用するＩＣチップ、ＩＣカードの品番、数量、管理番号、取扱い担当者等チェックを行うことで工場からの不当な流出を防ぐ。

③　加工作業後の管理

加工作業後に、作業時に発生したＩＣチップ、ＩＣカードの損失品、製品、予備品、各々のＩＣチップ、ＩＣカードの数量および管理番号の付与、取扱い担当者等のチェックを行うことで、工場からの不当な流出を防止する。

(c)　保管管理

ＩＣチップ、ＩＣカードを保管する場合、保管場所からの持出し等による不当な流出を防ぐために厳密な管理を行うことでセキュリティを確保する。

①　保管室の入退室管理

ＩＣチップ、ＩＣカード、設計書等を保管する場所の入室管理を行うことで、不当な流出を防止する。

②　保管場所／保管庫の施錠義務

保管場所のゲートや保管庫に施錠を義務づけ、鍵の管理を行うことで不当な流出を防止する。

③　ソフト上のガード

工場でＩＣカードを保管する際、不当に流出した場合、ＩＣカードが運用システムの端末機器で使用できないようにソフト上でガードをかけておくことで、セキュリティを確保する。

④　運用システムによるガード

カードをシステムで運用する際に、オンラインで接続されて認証を受けてから初めて使えるようにソフト上でガードをかける。また、オンラインで接続することにより、事前登録のＫｅｙを要求し、更にＩＣカード内の管理番号のチェックや不正カードのチェックができるようにすることでセキュリティを確保できる。

(d)　工場内の作業員の管理

◎
△
◎
◎
◎
◎
◎
◎
◎

工場からの不当な流出は人為的要因が大きく考えられる。よって、工場内での作業員の管理を行うことでセキュリティを確保する。

① 作業員の身元確認行うこと。 ◎

作業員の身元を確認することで、情報の漏洩時における作業者のトレースを行うことで二次的被害を防止する。

② 作業員の入退管理、行動制限を行うこと。 ◎

許可された場所以外で作業を行わないように管理することで、セキュリティを確保する。

③ 工場全体の保安を確保 ◎

警備会社との提携する事で常時、不当な進入者を防止することでセキュリティを確保する。

④ 工場出荷／受入れ時におけるセキュリティの確保 ◎

ＩＣチップ、ＩＣカード発送または受入れする際、工場の人間と運送業者が直接に接触できないように間接的な部屋を用意するなどの工夫することで作業者の安全とセキュリティを確保する。

(e) 残存処理管理

製造時に発生した不良品や予備材料等廃棄処分する際に、不当に流出することを防止することでセキュリティを確保する。

① 物理的破壊 ◎

製造時に発生した予備品および損失品を物理的（ＩＣチップの電気的破壊、パンチングによる破壊etc．）に破壊し処分することでセキュリティを確保する。

―補足解説―

本文での機能要件のレベル分けは、記述内容の全てがセキュリティを確保する上で必要条件であると考え、「◎」としている。ただし、工場内での各々の取り扱いについては、各工場の造りや工程システムなどのセキュリティを含めた管理体制によって、選択できるものと考えられる。

7.2.2 ＩＣチップの不正解析の防止対策（電子顕微鏡による解析）

(1) 脅威とセキュリティ機能

ＩＣチップ自体のセキュリティを破るために、ROM に格納されているＯＳを解析される可能性がある。よって、ROMの解析を防止する工夫を必要とする。

(2) 機能要件

(a) ＩＣチップの設計の工夫

ＩＣチップのハードウェア構成を工夫することで、解析を防止する。

① ＩＣチップの一番下の層にROMエリアを形成 ○

ROMエリアを最下層に形成することで、電子顕微鏡の解析を困難にする。

② ダミーの回路を形成 ○

ROM層の上にダミーの全面電極等を挿入し、電子顕微鏡での解析を妨害する。

③　ミクロンルールの使用

ＩＣ設計の際にできるだけ小さなミクロンルールを使用して物理的に解析を困難にする。

④　アドレスの工夫

物理アドレスと論理アドレスのスクランブルをかけ外部からアクセスするアドレスが物理アドレスと合致しないようにして外部からの解析を防ぐ。

(b)　ROMデータ作成の工夫

ROMに格納するＯＳの開発ツールを工夫することで解析を防止する。

①　独自の専用開発ツールを使用

○

○

△

―補足解説―

本文の機能要件の区分分けは、記述内容が必要度が比較的高い条件であると考え、「○」としている。また、（イ）の①については、より高いセキュリティを追求する場合とし、「△」としている。

7.2.3　ＩＣチップへの不正アクセスの防止対策

(1)　脅威とセキュリティ機能

ＩＣチップへ不当にアクセスを行うことでデータを収集することで、ＩＣチップの解析を行う手段に対して、解析を防止する必要がある。

(2)　実現すべき機能要件

(a)　ＩＣチップの自己診断機能の保有

①　相互認証

ＩＣチップにアクセスする端末（上位コンピュータ）または対象者が正当であるかどうかを認証する機能（ＰＩＮやパスワードによる照合、静的データ認証、動的データ認証、ｅｔｃ．）を保有することでセキュリティを確保する。

②　アクセス回数の制限機能

特定のデータに対して、ある一定回数以上のアクセス（ＰＩＮ入力回数の制限、データアクセス回数のカウンタによる制限、ｅｔｃ．）を検知した場合、カードをブロックする機能を保有することでセキュリテを確保する。

○

○

―補足解説―

本文の機能要件のレベル分けは、記述内容が最低限必要な条件であると考えられるが、「○」としている。これは、ＩＣチップによる自己診断機能は、ＩＣチップのROMに格納されるＯＳ機能によって、セキュリティの強度が決定されるものと考えるためである。

7.2.4　ＩＣチップの誤動作による不正解析の防止対策（熱、圧力、etc.）

(1)　脅威とセキュリティ機能

ＩＣチップは、物理的な攻撃を加えられることによって、誤動作する可能性があり、その誤動作により、ＩＣチップ内のデータを解析される可能性がある。よって、

誤動作しないように工夫することでセキュリティを確保する。

(2) 実現すべき機能要件

(a) 電気的攻撃に対する対策

設定された周波数帯以外の周波数や電圧を検知した場合、ＩＣカードが動作しないように工夫をすること。

(b) 熱攻撃に対する対策

正常動作を保証する熱量以外の熱量が付加されるとＩＣチップが破壊されるようにすること。

○

○

－補足解説－

ＩＣカードの耐タンパー性については、まだまだ技術的に実現が難しく、本文に記述している内容レベルでもかなり難しいと考えられる。よって、機能要件のレベル分けでは、「○」としている。

7.2.5 ＩＣカードの流通過程における要件（盗難対策）

(1) 脅威とセキュリティ機能

ＩＣカードを工場から出荷、納品時において盗難等による不当な流出によるＩＣカードの解析および運用を防止する必要がある。

(2) 実現すべき機能要件

(a) ＩＣカードへのトランスファープロテクトの付加

工場出荷や初回運用までに、ＩＣカードが運用できないように、ＩＣカードに機能プロテクトを付加することで、盗難／紛失に対するセキュリティを確保する。

① 機能プロテクト解除の鍵の保有

使用時に指定する鍵（パスワード,ｅｔｃ．）を入力させないと、ＩＣチップ内のデータにアクセスが一切できないようにすること。

② データ改ざんチェック機能の保有

運用システムで初回使用される場合に、ＩＣカード内部のデータが改ざんされていないかどうかをチェックすること（ＩＣカードに格納データを秘密エリアに圧縮格納し、端末側で格納されている平文データを圧縮計算し、ＩＣカード内部の圧縮データと比較照合する,ｅｔｃ．）。

(b) 専用運送会社を確保

専用の運送会社を確保することで、盗難や紛失に対するトレース機能を確保することが可能となる。

(c) 出荷／納品時における当事者、警備員の立会い

出荷／納品時に警備員や当事者が立会うことで、盗難・紛失に対する責任の所在を明確にすることで、セキュリティの確保を促す。

(d) 管理コードによるプロテクト

管理コードを設けることにより、正当なメーカーで製造されたＩＣチップ／ＩＣカードかどうかをチェックすることで、不当なＩＣカードの運用を防止する。

① 運用システムによる管理

◎

◎

○

○

◎

製造者管理コードとシリアル番号により、システム運用上で受け入れられないようにするため、出荷したＩＣチップのデータ管理を行うこと。

－補足解説－

機能要件のレベル分けについては、(ａ)～(ｄ)の内容を必須とすることで、最低限のセキュリティを確保できるものと考える。また、(ｂ)～(ｅ)の内容について選択とする。

7.2.6　廃棄ＩＣカードの悪用に対するセキュリティ要件

(1)　脅威とセキュリティ機能

回収廃棄したＩＣチップ／ＩＣカード盗難や紛失による、ＩＣチップの解析やＩＣカードの不正使用を防止する必要がある。

(2)　実現すべき機能要件

(a) ＩＣチップの破壊	
回収したＩＣカードのＩＣチップを破壊することで、廃棄時における盗難／紛失の防止を行う。	
①　ソフトによる破壊	○
ＩＣチップにカードブロックするコマンドを送信し、ＩＣチップを使用できなくする。	
②　物理的破壊	◎
ＩＣチップに物理的攻撃を加え、ＩＣチップそのものが使用できないようにすること。	
(b) 発行ＩＣカードと回収ＩＣカードとチェック	
ＩＣカード発行時に、発行カードの管理リストを作成し、回収時に管理リストをチェックし、未回収カードに関してはある一定期間が経過すると運用システム上で使用できないようにする。	○
(c) 回収廃棄業者の管理	
回収廃棄業者の身元確認、および廃棄管理（廃棄時に当事者が立会う。etc.）を行うことで、ＩＣカードの盗難／紛失を防止する。	○

－補足解説－

本文の機能レベル分けについては、(ａ)②のＩＣチップを物理的に破壊することでほぼセキュリティを確保できるものと考えられる。よって、(ａ)②を「◎」とし、その他を推奨ということで「○」とした。ソフトによる破壊を行えばより効果的である。

7.3　端末機器のセキュリティ機能要件

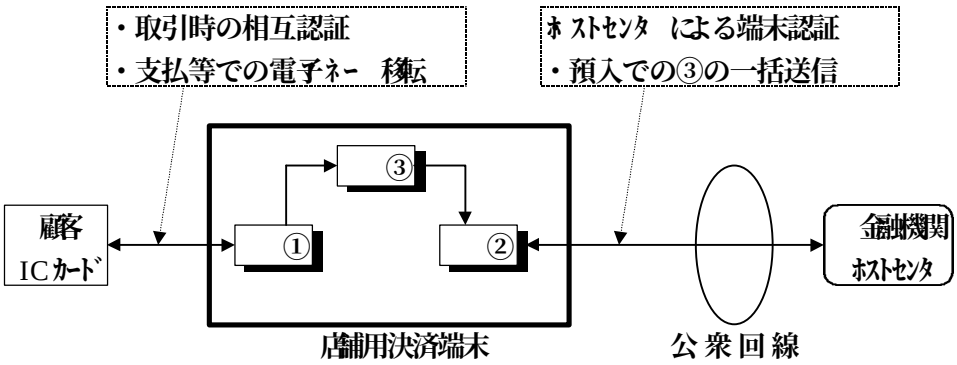
本項では、ＩＣカード型電子マネーシステムで必要となるセキュリティ技術（３章、参考資料２を参照）を内蔵する端末機器を対象に、これらのセキュリティ技術を悪意の第３者から保護し、またシステム内で正当な運用を行うために必要な機能要件について記述する。

ここでは、セキュリティ技術を内蔵する端末機器とは、店舗等に設置され、電子マ

ネーにより決済（支払／預入）を行う決済端末を例にその内容と構成を示す。

下図はオフライン取引型の決済端末の例である。取引時は①で相互認証を行い、支払された電子マネーは③に蓄積され、定期的に一括で金融機関へ預入を行う。（預入はオンラインで行う場合と媒体でのデータ渡しの場合がある。下図はオンラインでの預入を示す。）

なお、下図は一例であり、システムに応じて必要なセキュリティ技術を適用する。例えば、端末機器の不正防止機能でその正当性を保証されていると判断するシステムでは、②のホストセンタによるオンライン端末認証は適用しない場合がある。



①端末機器と顧客ＩＣカード間のセキュリティ技術
　相互認証、デジタル署名、電文暗号化、各種暗号鍵の保持／管理
②端末機器とホストセンタ間のセキュリティ技術
　オンライン端末認証、デジタル署名、電文暗号化、各種暗号鍵の保持／管理
③電子マネー、取引ログの蓄積（必要に応じて暗号化して蓄積）

図中［　　］は各機能ブロックを示す。個々にまたは統合してセキュアアプリケーションモジュール化（3.1(2)(a)項参照）することが望ましい。

―補足説明―

リロード専用端末や家庭用ＰＣ＋Ｒ／ＷなどはＩＣカード⇔センタ間で、またウォレットなどはＩＣカード相互間で直接セキュリティ技術を実現する場合がある。この場合の端末機器は、電文通信路の確保、ＩＣカードの物理的アクセス制御、標準伝送プロトコル制御等、セキュリティ処理の仲介を行うだけとなる。このような端末機器に以降の各項目を適用するか否かは、該当機器に要求されるセキュリティレベル（暗号強度との兼ね合い等）や、設置環境（有人／無人、店舗内／外等）を考慮し、システム毎に判断すること。

7.3.1　端末機器の不正解析/改造防止機能（ソフトウェア、各種データの保護）

(1)　脅威とセキュリティ機能

ＩＣカード型電子マネーにおける端末機器には、様々な機能動作を実現するソフトウェアや各種データが内蔵されており、悪意の第三者による不正な解析／改造から、これらを保護する必要がある。特にセキュリテ技術を実現するソフトウェアや、それに関連する機密データ（暗号鍵、各種ＩＤ等）の保護は重要である。

ここでは、端末機器が有するソフトウェアや各種データの保護のために必要な不正防止機能の実現手段について述べる。

(2) 機能要件

(a) セキュアアプリケーションモジュールの実現手段

セキュアアプリケーションモジュールとは、セキュリティ機能を実現するためのデバイス（ＣＰＵ、メモリーなど）を集約しモジュール化したものであり、一般的には端末機器の内部に組込まれて使用される。このセキュアアプリケーションモジュールに十分な不正防止機能を盛り込むことにより、端末機器としてのセキュリティを確保することができる。ここではその実現手段について述べる。

① マスクROM化

市販の１チップＣＰＵ内のマスクＲＯＭ部に、セキュリティ関連要素を封印する方法がある。この場合、内部メモリーデータの読出し防止機能の付加や、解析ツールの接続が不可能な実装方法等を考慮する必要がある。 △

② 専用ＬＳＩの使用

セキュリティ関連要素を組込んだ専用ＬＳＩを開発、使用する方法がある。各機能のハードウェア集積化、独自アーキテクチャ、言語等の組込み等により解析を困難とさせる。 △

③ ＩＣチップ化

ＩＣカードに使用されるＩＣチップを使用する方法がある。セキュリティ関連要素をＩＣチップ内に組込む。この場合、ＩＣチップの耐タンパー性がそのまま利用できる（7.2 項の機能要件も参照のこと。）。 △

④ 物理的なモジュール化

構成部品（ＣＰＵ、メモリーなど）をケースなどに封印し、物理的にモジュール化する方法がある。この場合、以降での「端末機器」を「セキュアアプリケーションモジュール」と読替え、セキュリティ要件を確保すること。 △

(b) 端末機器への物理的攻撃に対する不正防止機能

ここでは、端末機器への物理的攻撃（筐体の不正開放、破壊等）に対する不正防止機能（耐攻撃性、攻撃の痕跡検知等）について記述する。なお、筐体の不正開放とは、正当なメンテナンス手順に従わずに端末機器の筐体を開放することである。

① 筐体をシールなどで封印する方法がある。

② 筐体の不正開放後は、正常に閉まらなくなるような筐体構造とする方法がある。 △

③ 筐体の不正開放に対して、聴覚的（アラーム音の鳴動等）、視覚的（アラームランプの点灯等）な警報を行う方法がある。 △

④ 筐体を一般では開放できない構造とする方法がある。特殊ネジの使用、筐体の一体化（接着剤等での封印、モールド一体化）等が考えられる。 △

⑤ 次項の自爆機能を具備する方法もある。 △

(c) 端末機器の筐体不正開放時の自爆機能

ここでは、端末機器の筐体不正開放に対する端末機器の自爆機能の動作例について述べる。筐体の不正開放を検出し、端末機器の動作を制限することにより、不正な内部解析を防止する。 △

① プログラムの停止

不正開放検出により、プログラムが停止し、以降の操作を不可能とさせる方法がある。不正開放検出の仕組みを解析／対策された場合は、効果がなくなるため、次項②③との組合わせが効果的となる。 △

② 機密データの消失

不正開放検出により、端末動作に必須な機密データを消失させ、機密データの漏洩を防止し、かつ以降の正常動作を不可能とさせる方法がある。 △

③ プログラムの消失

不正開放検出により、端末内のプログラムを消失させ以降の正常動作を不可能とさせる方法がある。 △

(d) プログラム解析に対する防御

端末機器の盗難等によるプログラム解析に対し、以下の防御方法が考えられる。

① プログラムの暗号化を行うことにより防御する方法がある。

不揮発性メモリーに暗号化されたプログラムを保存しておき、端末動作時は、当該プログラムを揮発性メモリーに復号展開し、揮発性メモリー側でプログラム動作を行う。揮発性メモリーの内容（平文プログラム）は、(Ｃ)③項により保護することが望ましい。 △

② プログラムを端末稼動前にダウンロードする方法がある。

端末起動毎にオンラインで接続されたセンタから必要プログラムをダウンロードする。 △

(e) セキュリティに関連する操作の保護

機密データの登録／変更、(Ｃ)項の自爆機能の解除（復旧等）などセキュリティに関する操作は、正当な保守者以外の第３者がアクセスできないようにする必要がある。またこれらの操作中に機密データなどが漏洩しないようにする必要がある。

① パスワードなどの照合により認証を行う方法がある。

パスワードは、あらかじめ端末内に内蔵され、十分秘匿されていること。パスワードの入力回数、入力処理時間には上限を設けること。 △

② 保守専用のツールを用いる方法がある。

・保守者専用ＩＣカードでの相互認証による操作の許可 △

・保守者のみがもつ専用治具による操作

－補足解説１－

本文での機能要件のレベル分けは、記述内容が全て実現手段であるため、端末機器の種別毎に任意に選択できるよう、全て「△：選択」とした。

ただし、物理的な保護手段である機能要件の(ａ)～(ｄ)については、いずれかの方法（または、組合わせ）により、セキュリティ関連要素を秘匿することが必須と考えられる。よってシステム内で端末機器が要求されるセキュリティレベルによって、適宜各機能要件を適用すること。

例えばセキュアアプリケーションモジュールを採用している端末機器であれば、(ｂ)～(ｄ)は選択的な項目となり得るし、セキュアアプリケーションモジュールを採用し

なければb）（d）のいずれかは必須となると考えられる。
端末機器またはセキュアアプリケーションモジュールに対し、セキュリティに関する操作を行う場合は、機能要件e）は必須である（実現手段は選択）。

◎

－補足解説２－

端末機器の筐体以外の構造的な条件として、以下が考えられる。 ◎

・ＩＣカードの接続部分は、最も容易な外部から攻撃部分である。不正アクセスのための異物の挿入防止／検出のため、挿入口、挿入口シャッタ、検出センサ（カード有無、形状チェック）、端子接点機構等の構造を考慮する必要がある。取引中のＩＣカードの引抜き防止が必要な場合、引抜き防止機構（ＩＣカードを端末機器内に取込む方式（モータ搬送）等を検討する必要がある。この場合、故障時等の対応のため、強制排出機構も考慮する。 ◎

外部機器との試験用端子は、外部から容易にアクセスできないようにする。または設けない。 ◎

7.3.2 端末機器の設計／製造工程での不正防止

(1) 脅威とセキュリティ機能

端末機器メーカーでの設計／製造工程での脅威として以下のような例が考えられる。 ◎

・設計用ドキュメント等の漏洩
・ソフトウェア、各種データ（特に暗号鍵等の機密データ）の漏洩
・機器設計者によるセキュリティホールの組込み ◎
・端末機器の横流し

これら脅威への対策は、端末機器メーカーの設計／製造の管理体制に言及される。ここでは、これらの管理体制に対するガイドラインを述べる。 ◎

(2) 機能要件

(a) 設計／評価工程での機能要件

① 設計者／評価者の選択

例えば、設計資格／評価資格等の規定を設け、これの適合者を選択する。 ◎
特に外部に設計／評価を委託する場合は注意のこと。

② 設計場所／評価場所の隔離

設計場所／評価場所に、無関係な人間が入れないように管理／隔離すること。 ◎

③ ドキュメント／ソフトウェアなどの管理

部外者による「ごみ箱あさり」、また盗難等されないようにドキュメント／ソフトウェアなどの管理を行うこと（複製の制限、未使用時の金庫管理、使用時の管理強化等）。またパソコンやサーバ上にデータが保存してある場合、アクセス制限等の対策を行うこと。 ◎

④ 端末機能の検証

端末設計者が、端末機器へセキュリティホールを組込み、不正に利用することが考えられる。 ◎

これを防止するため、複数の設計者／評価者により機能検証を行うこと。

⑤　評価用機能の削除

セキュリティに関する評価用の特殊機能は、出荷製品からは削除すること。

⑥　試作品の管理

試作品の台数管理を確実に行うこと。また、廃棄は破砕処理後に行うこと。

(b) 製造工程での機能要件

①　製造者の選択

例えば、製造資格等の規定を設け、これらの適合者を選択する。特に外部に製造を委託する場合は注意のこと。

②　製造場所の隔離

製造場所に、無関係な人間が入れないように管理／隔離すること。

③　ドキュメント／ソフトウェア等の管理

製造図面、検査仕様等のドキュメント、また端末機器組込み用のソフトウェア、各種データなどがコピー、盗難等されないよう管理を行うこと（複製の制限、未使用時の金庫管理、使用時の管理強化等）。

④　組立／検査治具の管理

端末機器の組立／検査に使用する治具、製造装置等がセキュリティに関係する場合、筐体組み立て用特殊工具、データ登録装置等、これらが盗難、紛失また許可無き人間が操作できないよう管理を行うこと。

⑤　ソフトウェアのインストール

端末機器へソフトウェアのインストールを行う場合、それらの秘密が守られるような環境のもと、信頼できる製造者により実行されること。

⑥　端末機器の初期化

端末機器に各種のデータ登録を行うことにより、端末機器の初期化を行う場合、それらの秘密が守られるような環境のもと、信頼できる製造者により実行されること。

⑦　不良品の管理／廃棄

製造工程で発生した不良品が、外部に流出しないよう管理すること。また廃棄する場合は、セキュリティに関する部分は破砕処理を行うこと。

⑧在庫品等の管理

在庫品の管理を確実に行うこと。

－補足解説１－

本項は、ＩＣカード型電子マネーシステムに限らず広くは電子決済システムのリスク対策の基本要素として端末機器メーカが十分整備すべき内容であり、全ての項目を必須事項とした。

システム提供者の端末機器メーカの選択時等に参考となる。

－補足解説２－

(b) ⑥項の端末機器の初期化での各種データ登録には暗号鍵等の機密データも含まれ

るが、これらの登録は漏洩防止のため、端末機器メーカーではなくシステム提供者が管理／登録を行う場合も考えられる。
また、機密データに関する操作を行う場合は、7.3.1(e)項に従うこと。

－補足解説３－
システムによっては、セキュアアプリケーションモジュールと端末機器の設計／製造工程のメーカーが異なる場合がある。端末機器メーカーでは、システム提供者から支給されるセキュアアプリケーションモジュールを端末機器に組み込み、端末機器を完成させる。この場合でも端末機器メーカでの管理体制は本項に準じる必要がある。
また、セキュアアプリケーションモジュールの設計製造メーカーにおいても本項と同様な管理体制が必要となる。この場合は本項の端末機器をセキュアアプリケーションモジュールに読替える必要がある。

7.3.3 端末機器の正当性の証明

(1) 脅威とセキュリティ機能

ＩＣカード型電子マネーシステムにおいて、端末機器の「なりすまし」防止、端末機器の管理（盗難等のトラブル時の保証）等のため、使用する端末機器がそのシステム内において認定されかつ正当なものであることを証明する必要がある。

(2) 機能要件

(a) 端末機器の活性化

端末機器は、特殊な保守操作、運用データの登録等により活性化されない限り、取引き等の運用を開始することができないような仕組みが必要である。 ◎

端末機器の活性化を正しい保守者が正しい設置場所で行うことにより、端末機器のシステム内での正当性を確保することができる（端末機器製造メーカや端末機器輸送中の盗難、横流し対策に効果的となる。）。

(b) 運用機関からの端末の証明

端末機器はそのシステム内において正常な運用を行うため、運用管理機関から認定を受けたものでなければならない。

① 運用管理機関が一元的に管理する端末機器ＩＤを付番する。ＩＤはシステム内においてユニークであり、一般ユーザの操作では確認、変更ができないこと。

運用機関に端末機器ＩＤを登録／管理しておくことにより、端末機器の偽造の検知、盗難端末の使用の抑制等が容易となる。 ◎

② 認定シール等の端末機器への貼付

システムの運用管理機関が発行した認定シールなどを端末機器に貼付する方法もある。 △

(c) 端末機器の認証

端末機器の「なりすまし」防止、また端末機器の正当性の証明のため、端末機器の認証が必要である。具体的な内容については、９章、参考資料２を参照のこと。 ◎

－補足解説１－

機能要件(a) の端末機器の活性化について、7.3.2(2)(b)⑥ 項の端末機器の初期化がされていない限り活性化できず、活性化されていない限り取引等の運用を開始することができないような仕組みが望ましい。これにより低位フェーズ（製造、輸送等）での脅威を低減することができる。

また、端末機器は活性化操作のみでなく非活性化操作も行える事が望ましい。システムの一時中断等で端末機器が放置される場合、端末機器を非活性化し、システム再開で再活性化を行うことができる。

なお、活性化または非活性化操作は、7.3.1(e) 項に従い、保守者以外が行うことが出来ないようにすること。

◎

－補足解説２－

本項は、セキュアアプリケーションモジュール単独の機能要件としても適用できる。この場合は、本項の端末機器をセキュアアプリケーションモジュールに読み替えること。

7.3.4 端末機器の流通過程における要件（機器の横流し、盗難等に対する対策）

(1) 脅威とセキュリティの機能

脅威として、端末機器偽造集団と端末機器製造業者の結託による端末機器の横流し、盗難、物理的破壊等が考えられる。

脅威の対策として、廃棄端末の厳重な処理、端末に保管すること等が考えられる。

(2) 機能要件

(a) 端末機器製造業者の内部情報管理の徹底

端末製造業者の内部犯行を防ぐため、重要な情報は鍵のかかるところに保管しなければならない。

◎

(b) 端末固有番号（製造番号等）の管理

製造番号の項目は複数でなければならない。例えば、項目として製造年月日、地域コードなどが考えられる。

(c) 輸送手段のセキュリティの確保

運搬車を防犯の為に特殊加工をすることも考えられる

(d) 端末の不正解放防止機構

筐体内のＲＯＭなどに格納されているプログラムが、運搬時の不正開放で以降の操作を不可能にするような機構にするか、アラームが鳴る機構になっているのが望ましい。

◎

(e) 廃棄端末の厳重な処理

廃棄後の筐体から、使用済みのセキュアアプリケーションモジュールが取り出せるようになっていて廃棄できるのが望ましい。

△

(f) 配送時の保管場所内に入退室する人間のチェック

複数のセキュリティ手段にする必要はないが、少なくとも電気錠・バイオメトリックス本人確認手段（指紋・アイリス・音声等）のどちらかを設置する必要が

◎

ある。 △

(g) 作業報告書の作成

出発時間・搬入搬出時間・どのルートを通ったかなど 運搬業者は依頼者に対して報告しなければならない。 ◎

－補足解説－

本機能要件は他要件と重複しているところもあり、技術面はあまり詳しく記していない。主に内部の数量チェックや作業報告書の提出等管理面」に重点をおいて記している。

各要件のレベル付けの理由を述べる。まず必須であるが ◎

・内部の事情通の犯罪だと被害額が大きくなる。

・既存のインフラで既に実施済みであると思われる場合。

・万が一盗難・横流しにあった場合でも追跡が容易になる ◎

という理由から必須にした。

次に、選択・推奨であるが △

・他の要件と重なっている場合

・要件によっては、各社の裁量に委ねるのが適当（作業報告書の様式等）という理由から選択・推奨にした。

7.4 発行機関におけるＩＣカードの運用とセキュリティ機能要件 ◎

本章では、ＩＣカードの二次発行機関がもつべき機能要件について述べる。 ◎

7.4.1 ＩＣカードの発行過程における要件（不正発行の防止）

(1) 脅威とセキュリティ機能

ＩＣカード型電子マネーにおいては、二次発行時に個人化情報に加え、暗号処理に必要な鍵情報の書込みが必要となるが、鍵情報の漏洩はＩＣカードの偽造を可能とすることになる。従って、ＩＣカードの発行過程においては、内部の者による不正な発行が行われないよう厳重な管理体制、第三者による監査機能のもとに行なう必要がある。また、鍵情報の漏洩が行われないためのシステム上の配慮が必要である。

(2) 機能要件

(a) ＩＣカード発行体制

本発行手続きを行う場所、組織体制について以下のような考慮が必要である。

① コンピュータによる入退室管理を行なうこと。

---- あらかじめ登録された者の個人認証を確認した上で入退室を許可するなど。

② ＩＣカード発行システムにおけるパソコンの操作者をあらかじめ管理者により登録し、スケジュール管理を行うこと。 ◎

③ ＩＣカード発行オペレータに対する管理責任者を明確にすること。 ○

④ ＩＣカード発行部門に対する内部監査を行える組織体制とすること（発行部門と監査部門の分離等）。 ◎

⑤　ＩＣカードの郵送事務の自動化

作成されたＩＣカードは通常顧客に郵送されるが、事故防止のため、ＩＣカードの作成と同時に住所ラベルが自動的に出力され、スタッカからＩＣカードが放出する順番に住所ラベルが作成され、誤りなく本人のもとに届けられる体制を整備すること。 ◎

(b)　ＩＣカード発行システムにおける管理機能について ○

上記の内部監査を可能とするための各種管理資料を作成する機能が必要である。

①　発行履歴管理表を作成可能なこと（機械別／オペレータ別に発行したカードの一覧表を作成できること）。また、申し込用紙との突合わせにより正しく発行されていることが検証可能なこと。 ◎

②　各種集計表を作成可能なこと（日別／月別／店舗別）。 ◎

申込用紙の枚数とのチェックを行い、余分に発行されていないかの検証を行う。

③　オペレータに対する操作モニタリング---管理者のパソコンにてオペレータに対する監視を行うなどの方法もある。 ◎

(c)　ＩＣカード発行システムにおける鍵情報の管理

鍵情報の漏洩を防止するため、ＩＣカード発行システムにおいて鍵情報生成の過程において以下の保証が必要である。 ◎

①　鍵の生成処理は特別なアクセス権限を保有する者のみ操作可能とすること。

②　生成された鍵情報ファイルに対する不正コピーの防止。 ◎

----外部への持出しを不可能とするためのコピーなどの操作に対して、消滅させるなどの機能が必要である。

―補足解説― ○

ＩＣカード型電子マネーシステムにおいてＩＣカードの発行時の体制を整備することは大変重要事項であり、当然必須事項である。また郵送時の事故防止のための住所ラベルの自動作成と放出されるＩＣカードとの突合せが容易にしておくことは必須である。 ○

また、ＩＣカード発行システムについても内部犯行を牽制、防止するための監査機能を保有することは必須であり、(ｂ)の①、②のような発行管理履歴を出力し、事後の精査を可能としておくことは必須である。ただし、オペレータの操作をモニタするなどはシステム上の特別な仕組みを要するため選択とした。更に鍵情報ファイルに対するアクセス権の管理および漏洩を防ぐための仕組みは重要事項である。

7.4.2　電子マネーの発行・回収の管理

(1)　脅威とセキュリティ機能

電子マネーシステムにおいては金融機関の既存システムに加え電子マネーの発行・回収の管理を行うマネー管理サーバが存在することが多いが、本サーバシステムの管理にあたっては充分な管理体制、システムによる監査により安全性の保証が必要である。

(2)　機能要件

(a) マネー管理サーバの管理体制等

① マネー管理サーバの保管室に対する入退室管理
あらかじめ登録された者のみが可能となるようにする

② 固体認識機能による入退室管理
保管室の入退室にあたり特定の個人のみを許可するための固体認識機能の保有。

(b) マネー管理サーバの発行管理機能

① マネー管理サーバにおける電子マネーの発行を常時監視し、電子マネーの発行履歴、発行量の管理を行う機能。

② 電子マネーの発行は勘定系システムと連動して行われ、勘定系元帳の残高から引落とした上で、同一価値の電子マネーの発行を行うため勘定系システムとの間で精査を行うことが必要である。

③ 電子マネーの発行が正常に終了しなかった時のリカバリ機能も必須となる（電子マネーの価値移転時の要件については 7.5 参照）。

(c) 電子マネーの回収管理機能

① マネー管理サーバは加盟店からの電子マネーにおける売上げ情報の回収を行い、加盟店毎の電子マネー回収履歴、回収量の管理が必要となる。

② 本データにより金融機関の勘定系における加盟店口座への入金処理を行う。

(d) 発行・回収の整合性の検証機能

発行した電子マネーの改ざんあるいは複製等に対処するため、発行した電子マネーと回収した電子マネーの照合等の機能があることが望ましい。

① 統計的手法による分析
発行量に比較して回収量の分析を行い、不当な複製等の検証を行う。

② 発行した電子マネーの追跡管理機能の保有
発行した電子マネー毎にＩＤを付加し、電子マネーの使用履歴をすべてとらえ、発行した電子マネーと回収した電子マネーを常に照合する。

―補足解説―

・本サーバシステムは電子マネーシステムの中核であり、コンピュータシステムに対する充分な安全対策が必要である（コンピュータシステムの安全対策基準についてはここでは省くこととする）。また、電子マネーの発行・回収における充分な管理・精査機能が必須となる。発行・回収の整合性の検証機能についてはセキュリティレベルに依っては望ましい機能と考える。

7.4.3 電子マネーにおける有効期限の設定と期限到来時の手続き

(1) 脅威とセキュリティ機能

ＩＣカード内で暗号処理等を行なう場合、ＩＣカード内の鍵情報の漏洩は偽造につながることになる。従って、同一の鍵情報で長期間運用すると漏洩の可能性が高くなるため、有効期限を設定することが望ましい。また、期限到来時、電子マネーとしての運用が即時停止すると、ＩＣカード内に残存している電子マネーを失うことになるため、期限到来時のルールを取決めておくことが必要である。

(2)　機能要件

(a)　ＩＣカード発行時の有効期限の書込み

ＩＣカード発行システムにおいて、有効期限情報の書込み機能が必要である（ＲＳＡの公開鍵方式の場合は、発行機関の公開鍵証明書に期限情報を設定することが考えられる）。　◎

(b)　端末における有効期限のチェック

各種ＩＣカード端末は、顧客ＩＣカード内の有効期限のチェックを行い、期限到来時の表示機能を保有することが必要である。　◎

(c)　鍵の世代管理機能

ＩＣカードにあらかじめ複数の鍵情報を書込み、期限到来により自動的に別の鍵に切替えるなどの機能をもつ方式もある（切替えのタイミングは端末より指示が必要となる。）。　△

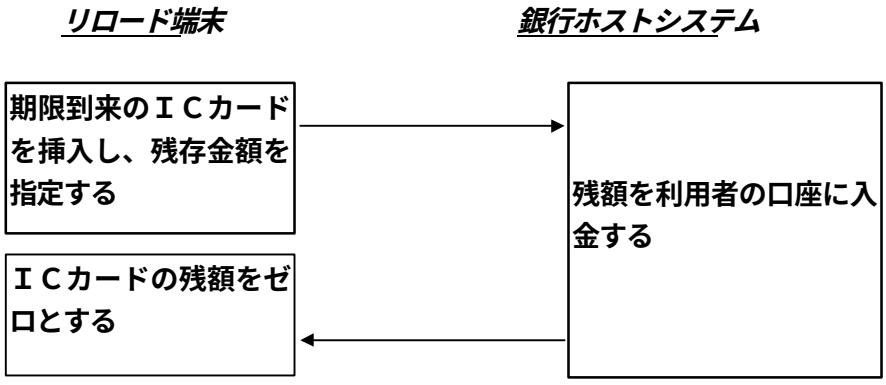
(d)　期限到来時の扱い

期限到来時、電子マネーとして運用している場合は、ＩＣカード内に電子マネーが残存しているケースがあるので、混乱なく再発行を行なうための手続きを検討することが必要である。

①　期限到来により使用不可能とする。ただし、残存している電子マネーは再発行手続きにより新ＩＣカードに引き継ぐことを可能とすること。

このためには再発行受付け窓口にてＩＣカードのリーダ・ライタの設置および再発行時に当該金額の電子マネーの書込み機能が必要となる（受付け窓口とＩＣカード発行部門との情報の正確な伝達が必要である）。　△

②　期限到来により使用不可能とする。ただし、残存している電子マネーは、金融機関の窓口により利用者の預金口座へ入金処理を行うことも考えられる。　○



―補足解説―

ＩＣカード型電子マネーとしては、長期間運用する鍵情報の漏洩の可能性がでてくる点とＩＣカードには物理的にアクセス回数に制限があり、期限はおのずから限界があり、期限の設定は必須となる。ただし、期限到来時、残額がある場合の事務手続きは大変複雑となるため、充分に検討しておくことが必要である。(ｄ)の②のケースは事務手続きが簡単であるが、換金に応じることと同じであり、金融機関発行型であれば問

題がないが、その他の場合は当局への確認が必要である。

7.4.4　電子マネーにおける上限金額の設定

(1)　脅威とセキュリティ機能

ＩＣカード型電子マネーの本来の目的は小額取引が対象であり、紛失、盗難等に対する消費者保護の立場からも書込み可能な電子マネーの金額に上限を設定することが必要である。

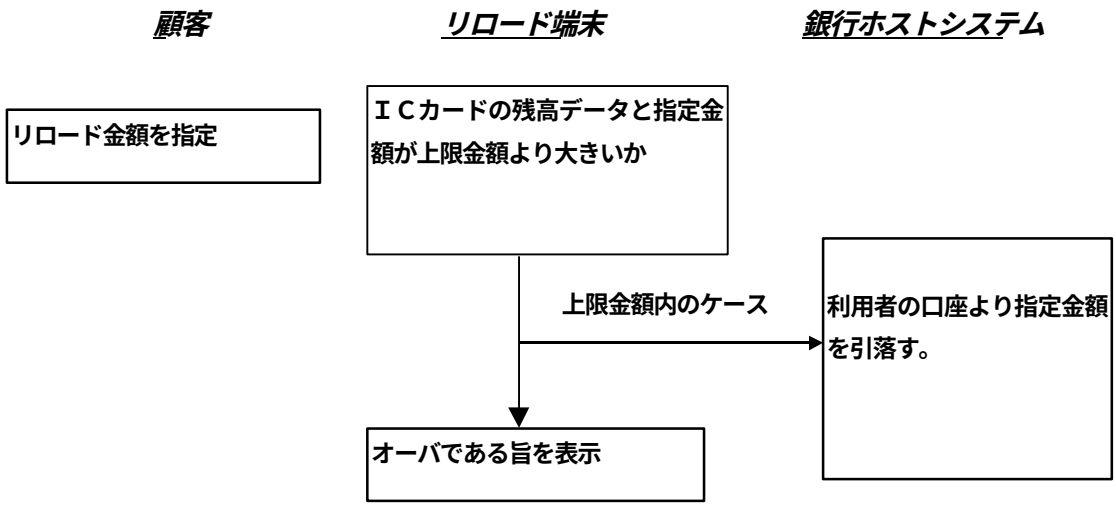
(2)　機能要件

(a)　ＩＣカードへの上限設定機能

ＩＣカードへの電子マネーの書込み時、書込み可能な上限金額を設定する機能をもつこと。 ◎

(b)　ＩＣカードの上限金額チェック機能

ＩＣカードに電子マネー書込み時はＩＣカードの機能として上限金額をチェックし、上限金額を越えた金額の書込みはエラーとする（ＩＣカードから当該エラー情報を返し、端末は上限を越えた旨のエラーメッセージを表示することが必要）。 ◎



(c)　ＩＣカードの種類に応じた上限金額の設定機能

ＩＣカードとしては一般的な利用者のＩＣカードの場合と、端末の内蔵カードの場合等で上限金額が異なるため、ＩＣカード発行時にＩＣカードの種類に応じた上限金額の設定ができることが必要である。 ○

利用者の中でも一般利用者と子供用のＩＣカード等の何種類かの上限金額設定をもつことも考えられる。

―補足解説―

上限金額を設定することは消費者保護の観点から望ましい機能といえる。また上限金額は消費者向けカード、小売店カードなど利用者に応じた設定が必要である。

7.4.5　取引きの追跡と監視（シャドウバランスの把握）

(1)　脅威とセキュリティ機能

電子マネー取引きについては、不正取引の監視あるいは ＩＣカード紛失時残高の保証等の観点から、極力取引一件一件の追跡機能を持つことが考えられる。またセンタ側で発行の履歴と回収の履歴を保有することで各ＩＣカードの残高の推定値（シャドウバランス）を算定することも可能となり紛失時でも残高の保証をすることも考えられる。また電子マネー取引が小売業者の各機器でフライ決済されるため各機器からセンタが回収するまでの時間によって、どの程度リアルタイムに把握できるかが異なることになる。転々流通性を可能とすると完全な追跡が不可能となるため、本機能要件はクローズドループ型のシステムに限定される。

(2)　機能要件

(a) 顧客別（ＩＣカード別）取引履歴ファイル（残高ファイル）の保有

センタシステムにおいてＩＣカード別の残高ファイルを保有する。

(b) 電子マネーの発行履歴の把握

電子マネーのリチャージは通常センタシステムから行われるため、センタシステム（電子マネーの発行管理を行うサーバシステム）において、発行の都度履歴をサーバに転送してリアルタイムに把握する。

(c) オフラインにおける決済取引の履歴管理

小売店においてオフライン決済時は、取引履歴をログし、業後まとめて金融機関の管理サーバに転送することで、顧客別ＩＣカード残高ファイルを更新することで、最終残高を予測することができる。

(d) 取引履歴の改ざん防止

取引ログをサーバに転送し、ＩＣカード残高を把握する場合は、取引ログの信憑性が問題であり、以下の対処が必要。

① 取引ログの二重送信、送信モレがないように送信時に通番管理を行う。

② 取引ログの改ざんを防止するため、ディジタル署名を付加する。

(e) 取引履歴の照会機能に対する制限（プライバシーの保護）

取引履歴に対する照会は、プライバシー保護の観点から誰でも可能とはせず、特別な権限を有するものに限定することが必要である また権限チェック等の機能をもつことが必須となる。

○
○
○
○
○

―補足解説―

取引の追跡によりＩＣカード上の残高を推定する機能は、ＩＣカードの紛失あるいはＩＣカードが読めないケースに対処するため保有することが好ましいが、プライバシー保護の観点で、取引履歴情報の取扱いには充分な配慮が必要である。

7.5　電子マネーの価値移転時の要件

ＩＣカード型電子マネーの価値移転は、金融機関からの価値の引出し、小売店への価

値の支払い、金融機関による価値の回収の大きく３つの ケースに分類整理できる。これ らの価値移転時のセキュリティ要件としては、①正当な利 用者であることの確認　②不正な ＩＣカード、不正な端末機器間の電子マネー移転防止 ③電子マネーの改ざん、複製の防 止　④異常処理への対応　⑤システムの不正な運用の防 止　の５点に留意する必要がある。

7.5.1　正当な利用者であることの確認

(1)　脅威とセキュリティ機能

金融機関からの価値の引出し時において、正当な電子マ ネーの所有者以外の者に電子マネーを利用される脅威がある。これらの脅威に対 して、電子マネーの所有者の本人確認や顧客口座等の所有者の本人確認が必要とな る。

(2)　機能要件

(a) 金融機関からの価値の引出し時には、顧客口座の本人認 証機能が必要である。

①　顧客口座の正当な所有者であることを確認するた めの本人認証機能を持つこと。この本人認証要求は、金融機関ホストで処理・認証さ れなければならない。

②　不正な本人認証情報提示を防止するために、失敗回 数ロギング機能や回数制限等を行うことが必要である。

(b) 電子マネーをＩＣカードに移転する際には、発行機関が 発行した正当なＩＣカードであることの確認として、ＩＣカード認証が必要とな る。ＩＣカード認証については、“参考資料２　ＩＣカードのセキュリティ機能” を参照のこと。

―補足解説―

・価値引出しの元本となる顧客口座の取引きについては 、既存のホストシステムの運用上、ホスト側の顧客口座に対する本人認証となるた め必須とした。なお、本人認証の方式には、ＰＩＮ（暗証番号）認証を用いるのが 一般的であるが、将来的にはバイオメトリックス情報（指紋、虹彩、声紋等の生体情 報）による認証方式も導入される可能性がある。これらの本人認証技術については 、ＷＧ６本人認証技術検討ＷＧの報告書等の解説が参考となる。

・ＩＣカード型電子マネーの価値自体の移転は、プリペ イドカード等と 同様の利便性をもたせることからもＰＩＮ入力等の手間を省き、ＩＣ カードそのものを所有していることを権利の証とするのが一般的である。また盗 難・紛失時の対策として所有者の持つワレットなどの機器でＩＣカードをロックす る機能を提供すること等がある。これらの詳細については .6.2　のＩＣカード盗 難・紛失対策を参照のこと。

7.5.2　不正なＩＣカード、不正な端末機器間の電子マネー移転防止

(1)　脅威とセキュリティ機能

盗難、変造、偽造による不正なＩＣカードまたは不正な 端末機器を用いた電子マネーの移転は、電子マネーの不正利用（偽造、複製、搾 取等）につながる危険性が高い。これらの脅威に対して、ＩＣカードと端末機器お よびホストのそれぞれの間での認証機能、ならびにＩＣカードや端末の盗難、変造 偽造対策、また取引ログ採取等を行い責任追及ができることが必要である。

(2) 機能要件

(a) 相手認証機能

① 各取引きにおいてカードや端末機器の真正性を確認するために、相手認証を行うこと。

② 不正な相手認証を制限するために認証失敗などのログ ギング機能や回数制限を行うこと。 ◎

(b) ＩＣカードの有効性の確認

カードの有効性を確認するために端末、または、ホスト にブラックリスト、若しくは、ホワイトリストを持ち取引きの都度参照して不 正なＩＣカードの使用を防止することが望ましい。 ◎ ◎

(c) 端末機器の変造・複製の防止

端末機器の変造や複製を防止するために次の対策を行う こと。

① 端末持込み時の端末真正性の確認や端末持ち出し時 の端末使用権剥奪

② 保守点検時のアクセス制限や保守点検後の端末真正 性の確認

(d) 責任追及のための証拠機能

① 不正な処理が行われた、あるいは正常に処理が終結 したことを検証するために処理結果等の取引き証拠をＩＣカード、端末機器、ホスト のいずれかに格納すること。また、取引き証拠の格納が完了しなければ処理 が完結しないプロトコルとすること。 ◎ ◎ ◎

② 処理結果の改ざん等を防ぐため署名を付加する方法 がある。

―補足解説―

相手認証は、ＩＣカードや端末機器のなりすましを防止 するために必須の機能とした。また失敗回数制限も全数検索法による攻撃を防止する機 能として必須とした。なお、相手認証については、“参考資料２ ＩＣカード型電子 マネーのセキュリティ機能について”を参照のこと。また、機器間の相手認証が有効 となる前提として、認証される側において物理的、電気的に盗聴や変造、偽造が困難 であること、すなわち、ＩＣカード、端末機器のＳＡＭ（セキュア・アプリケーション・モジュール）の耐タンパー性が要求される。耐タンパー性についての要件は“7.3 各種端末機器のセキュリティ機能要件”および“ＩＳＯ13491-1:1996 Banking - Secure cryptographic devices”などを参照されること。

ブラックリストなどによるＩＣ カードの有効性チェック は、リスト量によっては端末機器側で行うには記憶容量、処理速度の面から見て現実 的でない場合があり任意とした。 ◎

7.5.3 電子マネーの転送路における改ざん、複製の防止

(1) 脅威とセキュリティ機能

ＩＣカードと端末機器、端末機器とホスト間等の転送路 に侵入・分岐しデータを

盗聴および分析するなどして価値移転時の電子マネーの改ざん、複製するなどを行われる脅威がある。これらの脅威に対し次のような対策を行うことが必要である。

・転送路の機密性・完全性の確保 ◎
・転送データの真正性の確保 ◎
・責任追及のための証拠保存 △

(2) 機能要件

(a) 転送路の機密性・完全性の確保 ◎

価値移転が行われる転走路の機密性や完全性を確保する必要がある。具体的対策には以下のような対策があるが、各システムの通信路種別（専用線、公衆回線等）のセキュリティ特性に基づき任意に選択対策することが必要である。

・コールバック等による接続先確認 △
・相手認証による接続先確認
・論理チャネルの認証・暗号化

(b) 転送データの真正性の確保 △

データの改ざんやなりすましなどを防ぐため、データに署名の付加を行う方法がある。この署名には、セッション鍵（共通鍵）を用いたＭＡＣ（メッセージ認証子）や公開鍵を用いたデジタル署名の方法がある。

・ＭＡＣ（Message Authentication Code ）はANSI X 9.9A【NSI】やISO9797を参照のこと。一般的には、メッセージをCBC-DES モードによって暗号化し、最後出力の上位32 ビットを認証子としてメッセージに添付して送信する。MAC の場合には送信側、受信側で共通鍵を共有することが前提となる。

(c) 責任追及のための証拠保存 ○

不正なデータ転送や処理が行われた、あるいは、正常にデータ転送や処理が完結したことを検証するために取引き結果等を取引き証拠としてＩＣカードや端末機器、ホストのいずれかに格納することが必要である

(d) 取引き証拠の改ざんを防ぐため署名を行う方法がある

―補足解説―

価値移転が行われる転送路上は、盗聴によるデータ分析や改ざん等の攻撃を受けやすいため、これを防止することは必須とした。 △

7.5.4 異常処理への対応

(1) 脅威とセキュリティ機能

電子マネーの転送が何らかの要因で正常に行われなかった場合、原因を特定し、電子マネーの所在を確定し正式な価値移転を復旧完了させる必要がある。また、故意または過失で価値移転時に機器障害を起こし、不当な請求を行ったり、加盟店・顧客へ不利益を与える脅威に対し、機器の可用性の確保や取引き正当性の確認手段を確保すること必要である。

(2) 機能要件

(a) 機器の可用性の確保

① 機器障害を最小限にとどめるために、システム障害検出機能が必要である。
② 障害検出後リカバリー処理のためのデータ格納、およびリカバリー処理を行うこと。
③ 転送路、転送処理、バッファなどの二重化を図る方法もある。

(b) 否認の防止、異常処理の事実関係を究明するための証拠保存
① 取引き事実の追跡・証明等の責任追及手段を確保するために取引きの中断や完了状態を保持すること。
② 取引き処理の中断状態や完了状態の取引き証拠データの改ざんを防止するため署名を付加する方法がある。

―補足解説―

異常処理への対応は、システムの信頼性確保のため必須であり、特にシステムの障害検出機能やリカバリー処理、および、取引き証拠の保存は不可欠な要素であり必須とした。

7.5.5 システムの不正な運用の防止

(1) 脅威とセキュリティ機能

店舗の従業員による不正（横領等）や利用者不正な運用の防止対策を行うことが必要である。

(2) 機能要件

(a) 決済金額の目視による確認①

電子マネーを支払側と受取り側の双方において取引き金額を目視確認できる仕組みとすること。

(b) 決済金額の目視による確認② △

取引き後に電子マネーを支払う側が電子マネーを受取る側の見ている前で支払前と支払後の残高を確認する方法がある。

(c) オフライン運用時の店舗管理 △

自動販売機等一部オフライン運用となる場合があるシステムにおいては、従業員や店員が容易に取り扱えるところにカードを置かないなど、物理的な隔離や、保管場所に監視カメラを設置するなどの対策を行う方法がある。 △

(d) 店舗用端末の操作制限

店舗よりマニュアル操作で金融機関に価値移転するなど店舗端末の管理業務の操作者識別が必要なシステムの場合、店舗端末用の操作者を識別するためのＰＩＮ（暗証番号）認証機能等を設け、正当な管理者のみが電子マネーの管理を行えるようにする方法がある。また、不正な操作を抑制するために、加盟店端末用の電子マネー移転先を特定先（金融機関の販売店口座）のみに限定するなどの方法がある。 △

―補足解説―

・施設自体を管理できる金融機関ホストシステムと違い、店舗や個人保有の端末では、その管理は非常に困難となる。このため、運用面よりシステム面で不正防止を図る

ことが必要であり、運用面での対策のほとんどは選択 なる。但し、決済金額の目視による確認は当事者が取引きの結果を確認できる唯 の方法となるため必須とした。なお、金融機関における運用については"7.4 電子マネーの発行機関におけるＩＣカードの運用とセキュリティ機能要件"を参照 ること。

7.6 消費者保護について

7.6.1 消費者のプライバシ対策（匿名性について）

(1) 脅威とセキュリティ機能

ＩＣカード型電子マネーの使用に際して、誰がいつど で何をいくらで買い残高がいくらかなどの消費行動の履歴が、金融機関等に否 に蓄積され悪用される危険性がある。これらのプライバシーに関わる情報が不正 利用されないためのシステム面、および、運用面での対策が必要である。

ＥＣＯＭではプライバシー問題検討ＷＧがあるが、通 セキュリティ関連技術ＷＧでも主として技術面からプライバシー保護の問題を検 討している。ＩＣカード型電子マネーの実現のために、システムの各所で各種の情 報が利用・蓄積される。転々流通性、匿名性等の実装のためのブラインド署名等の技 術面での開発も盛んではあるが、システムの機能が高くなるほど、個人の情報が濫 用される、また、統計情報から個人のデータが推論されるなどの危険性がゼロにな ることはないであろう。

システムを構築する側、システムの運用者、また、シス テムの利用者も含めて、プライバシーに配慮する必要がある。

(2) 機能要件

(a) 取引履歴情報の最少化

① システムの運用に不可欠な情報のみを履歴として残 し、不要な情報を残すことによる悪用を避けなければならない。

② 保管期限等についても規定を設けることが望ましい 。

(b) 履歴情報管理者の限定 ◎

履歴情報の保管、利用に関するアクセス制御を厳密に実 施し、資格の無い者による不正アクセスを防止する必要がある。 ○

利用に関し、誰が何の目的で使用したかを記録するこ が望ましい。 ◎

(c) 第３者による履歴情報管理

システムの運用者とは異なる第３者（たとえばオリジネ ータ）が履歴情報を管理できるような形態のシステムの技術・運用面での検討 も行うことも 考えられる。

(d) 履歴情報の暗号化 ○

履歴情報を暗号化して格納しておくことが望ましい。

これにより、上記b） のアクセス制御が突破された場合 にも、履歴データが暗号化されていることにより、実質的な情報の漏れが防止 きる。 ○

通信路においても同様に暗号化が望ましい。

―補足解説―

取引履歴情報の最少化について、余分な情報を残さない ことは必須であり、保管規定等の規定は望ましい。
履歴情報管理者の限定については、アクセス制御が無い と、不法アクセスの可能性大のため必須とする。利用記録は望ましいが、必須とまで は考えず、○とする 。
第３者による管理は情報の集中の弊害を避けるというメ リットがあるが、現段階では種々の困難も予想されるので、△とする。
履歴情報の暗号化について、履歴情報が正しく管理され ていれば、暗号化は必須ではない。ただ、万一の場合に備えて暗号化しておくことは 望ましい。通信路においても格納時の暗号化と同様○である。

◎
△

7.6.2 ＩＣカードの盗難・紛失対策

(1) 脅威と機能要件

ＩＣカードの盗難・紛失時、他人に使用され損害を被る ことを防止するための対策も考慮することが必要である。

(2) 実現すべき機能事例

(a) ＩＣカードにおけるロック機能の保有

他人によるＩＣカードの不正使用を防止するため消費者 が保有する機器を利用し、ＩＣカードにロックをかける機能を提供することが 望ましい。

(b) 小売店におけるパスワードチェック機能（ＰＩＮ認識機 能）

小売店端末使用時は、パスワード入力の手間がかかるた め、一般的には使用しない。ただし、高額商品時の代金決済時、テンキーパッ ドより入力できる機能を提供することが考えられる。

(c) リロード時のパスワードチェック機能

金融機関で設置してある端末でリロードを行う場合は 通常暗証入力により銀行の元帳上の暗証とのチェックを行うためＩＣカード内 でのパスワードチェック機能は必須ではない。

(d) ＩＣカードの再発行時の残高保証機能

ＩＣカードの盗難・紛失により再発行を行なう場合、紛 失したＩＣカードの残高を保証すべきかどうかの選択があるが、保証する場合 は、ＩＣカードの残高を把握するシステムを構築する必要がある。従って、電子 マネーの書込みならびにすべての電子マネーにおける代金決済の記録を電子通貨 管理サーバに吸上げ、消費者のＩＣカード毎に残高を把握するシステムを構築 することが必要となる。

(e) 事故カードのチェック機能

電子マネー発行機関は、利用者からのＩＣカードの紛失 ・盗難等の連絡があった場合、本システムに事故届けの登録を行なう機能をも つことが望ましい。

なお、本機能により届けられたカードが使用されること を防ぐため以下の機能をもつことが必要である。

① リロード時に事故届けのあったカードであることを 判別できるシステムとする。
② 情報を事前に小売店端末に転送し、端末内でチェッ クを行い、使用不可とする。

○
△
△
△
○

―補足解説―

ＩＣカードのロック機能は、紛失時の他人による不正使用を防止するため保有することが好ましい。ただし、小売店での支払い時あるいはリロード時にパスワード チェックを行うことは、オペレーション時間が長くなるため必須ではない。

また事故カードの使用を小売店でチェックすることは困難であり必須ではない。

（参考資料１）　ＩＣカード型電子マネーシステムの動向

36

37

（参考資料２）　ICカードの証

不正なＩＣカードの使用を防止するため、端末装置（電子マネー用小売店端末）は、ＩＣカードの正当性を確認する必要がある。

この認証については、メーカーに主として依存するICチップの設計製造段階でのセキュリティと異なり、システム事業者が、メーカーの協力を得て、自身のシステムのセキュリティ保持のため、どのような認証方式を採用するのか、決定する必要がある部分である。

認証には、暗号の利用が必要となる。

1)　共通鍵暗号

図－１では、秘密鍵暗号を表している。方式としては古くから用いられているものであり、同一の鍵で暗号化し、復号を行う。このため共通鍵暗号とも呼ばれる。メッセージの送り手と受け手の双方がこの鍵を知っていなくてはならないし、またそれ以外の人に知らせてはならない。

このため、どうやって双方が、秘密のうちに鍵を知るかが課題となる。

暗号化／復号の処理時間は次の公開鍵暗号に比べて短い。

ＩBM社のＤＥＳ（Data Encryption Standard）が代表的であり、鍵長が64ビットあれば安全といわれている。

2)　公開鍵暗号

図－２は、公開鍵暗号を表している。公開鍵（Public Key）を広く公開し、秘密鍵（Private Key）は秘密に保持する。公開鍵と秘密鍵は一対であり、数学的な関係がある。公開鍵で暗号化されたメッセージは秘密鍵でのみ復号できる。異なった鍵で、暗号化／復号がなされるため非対称暗号とも呼ばれる。

鍵対を生成し、公開鍵を相手に渡すことになるが、秘密鍵を自分が保持していれば、公開鍵は広く知られてもよいため、鍵の受渡しが容易である。

暗号化／復号の処理時間が、共通鍵に比べて長い。

ＲＳＡ社のＲＳＡ暗号（発明者３人の頭文字をとってつけられた）が代表的であり1,024ビット以上あれば安全といわれている。N＝P×Q（P、Qは素数）で、P、Qが大きな数のとき、NからP、Qを見つけるのは、大変な計算量が必要となる事を利用している。Nを含んだ公開鍵で暗号化しP、Qを含んだ秘密鍵で復号される。

公開鍵暗号には、もうひとつ大きな特長があり、秘密鍵（Private Key）で暗号化されたメッセージは公開鍵（Public Key）で復号される。図－３では逆の方向の暗号化／復号も可能となる。この特長が電子的な署名に生かされる。

3)　暗号の利用

最近、暗号の方式とか、鍵とかが、一般の新聞でも取り上げられている。暗号の利用といった、従来では軍事機密や、一部の金融ネットワークでのみ適用されていた技術が、脚光を浴びているのは次の理由による。

コンピュータネットワークのネットワークと呼ばれるように、インターネットでは、複数のゲートウエイを経由して通信が行なわれるために情報の盗聴や改ざんの

可能性がある。従ってインターネット上で、クレジット カードにより商品を購入する場合には、暗号を利用した秘密通信が必須となる。クレジットカード番号が盗聴される事は大変に危険である。

また、インターネット上で上記のような商取引をする場合、実在する店に行ってカードを見せて署名をする対面取引と異り、非対面取引となる。正しい販売店、正しいカード会員であることの確認はどうすればよいのだろうか。

認証には公開鍵暗号を使って以下の方法がとられる。

① Aさんがデータを自分の秘密鍵（Private Key）を使って暗号化する。

② Aさんは暗号化した暗号文ともとのデータの2つをBさんに送る。

③ Bさんは公けにされているAさんの公開鍵を使って暗号文を復号し、もとのデータと照合する。

④ 一致していればBさんは次の事が確認できる。まちがいなくAさんの作成したデータである。データは改ざんされていない。

Aさんが自分の秘密鍵（Private Key）を他にもらさないかぎり、これはAさんの署名と同じ効果を持つ。

従って上の①～④の行為を電子的な署名の一種と考え デジタル署名（Digital Signature）と呼んでいる。

このデジタル署名がＩＣカードの正当性の確認に使われる。

4)(端末装置によるＩＣカードの認証（ＥＭＶ）

Europay, Master Card, Visa によって制定された業界標準として、3者の頭文字をとったEMVがある。これは金融分野に用いられるＩＣカードの標準であるが、ＩＣカード仕様全てを規定するものではなく端末装置とＩＣカードのインターフェースを中心に制定された標準であり最新版の「EMV'96」（ver.3.0）が９６年6月に公開された。

EMVでは2つの認証方法がきめられている。

5)(EMVの静的認証

図－3は静的認証（Static Data Authentication）を表したものである。公開鍵暗号を利用している。

ここではカードの発行者の他に、公開鍵が正しい鍵である事を記明する証明機関（認証局）が必要となる。

図でdS(ca,i)とあるのは、カード発行者の公開鍵を証明機関の秘密鍵（Private Key）で暗号化したもの、すなわち証明機関の署名を表わしている。

端末からのEMVコマンドによってＩＣカードからレスポンスを返し、端末側でカードの正当性をチェックしている。

① 端末からのコマンドに従ってＩＣカードは、カード発行者の公開鍵（Pi）と公開鍵を証明機関の秘密鍵で暗号化したもの（証明機関の署名）dS(ca,Pi）を端末に送る。

② 端末は署名を証明機関の公開鍵で復号しPiと比較して一致していればPiを正しい発行者の公開鍵と認める。

③ 次にＩＣカードは端末からのコマンドに従いカードの個有データと個有データを

カード発行者の秘密鍵で暗号化したもの（発行者の署名）ｄｓ(ｉ、M）を端末に送る。

④　端末は先程正当と認めた発行者の公開鍵P(ｉ　)署名を復号し、Mと一致すれば、カードが正しく、発行者によって発行されたものと認める。

証明機関とカード発行者の秘密鍵が秘密に保持されている限り、上記のロジックは保たれる。

しかし、インターネット上と異り、ＩＣカードから端末に送られるデータは全体が暗号化されずに送られているため、このデータが傍受される可能性は0ではない。また、あるＩＣカードについていえば送られるデータは毎回、同一である。

このことから、送出されるデータをそっくりコピーして偽造カードが作成されるのを防ぐため、EMVでは次のような認証方式も決められている。

6)(　EMVの動的認証

図－４は動的認証D(ynamic Data Authentication)を表したものである。やはり公開鍵暗号を利用している。

ここでは、カード発行者、証明機関のほかに、ＩＣカード毎に個有の公開鍵P(ublic Key)、秘密鍵P(rivate Key)が使われている。

①　始めのカード発行者の公開鍵の真正性のチェックは静的認証と同じである。

②　次にＩＣカードは、端末からのコマンドに従いこのＩＣカードの公開鍵と、公開鍵をカード発行者の秘密鍵で暗号化したもの（カード発行者の署名）を端末に送る。

③　端末は署名をカード発行者の公開鍵で復号しＰｉｃと比較して一致すればＰｉｃを正しいＩＣカードの公開鍵と認める。

④　次に端末は、ある乱数Rを生成し、ＩＣカードに送る。

⑤　ＩＣカードは、秘密に保持しているこのＩＣカードの秘密鍵でＳｉｃ乱数を暗号化し端末に送る（ＩＣカードによる署名）。

⑥　端末は、ＩＣカードの公開鍵で復号しさきほどの乱数Rを比較し、一致すればこのＩＣカードにより署名されたことを確認できる。

この動的認証では、毎回異なる乱数が生成され、またＩＣカードの秘密鍵は、外部に送られることはないので、さきほどのような送出データのコピーによる偽造はありえない。

7)(　端末装置とＩＣカード間の認証

このほかにも、端末装置とＩＣカード間の認証を行う手順がある。EMVのコマンドが使われるが、静的、動的認証のように処理内容全般がEMVで規定されているわけではない。その手順を表したものが図－５である。

①　ＩＣカードが端末装置の正当性を確認する手順

(a) 端末装置が正当性確認をＩＣカードに指示する（GET　CHALLENGE コマンド）

(b) ＩＣカードは乱数を発生させ端末装置に送る。

(c) 端末装置は、乱数を定められた方法で暗号化し結果をＩＣカードに送り、認証を要求する。（EXTERNAL　AUTHENTICATE　コマンド）

(d) ＩＣカードは端末と同じ方法で乱数を暗号化し、結果が一致しているか確認する。

(e) 端末処理の正当性認証の結果（ＯＫ／ＮＧ）を端末装置に送る。

② 端末装置がＩＣカードの正当性を確認する手順

(a) 端末装置は乱数を発生させＩＣカードに送って暗号化を指示する（ＩＮＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ　コマンド）。

(b) ＩＣカードは定められた方法で乱数を暗号化し、結果を端末装置に送る。

(c) 端末装置はＩＣカードと同じ方法で乱数を暗号化し結果を比較して正当性認証を行なう。（ＯＫ／ＮＧ）

③ 暗号化の方法

①、②では、端末装置とＩＣカードで同じ方法で乱数を発生させ、結果を比較して認証を行う。

この方法としては、共通鍵暗号の利用が可能である。しかし共通鍵暗号では、端末装置とＩＣカードが、秘密裡に共通の鍵を保持する必要がある。ひとつの方法としては、端末側で秘密に保持しているマスター鍵でＩＣカード番号を暗号化したものを共通鍵とする方法がある。この方法をとれば端末装置は認証に必要な共通鍵を手に入れることができる。ＩＣカードには、予めマスター鍵でカード番号から生成した共通鍵を秘密裡に記録しておけばよい。

8)　端末からのＩＣカードの認証

ＩＣカードの認証としては、(６)で説明したEMVの動的認証がセキュリティ面で優れている。この方式では、処理の負荷の大きい公開鍵暗号による乱数の暗号化とＩＣカードで実行させるため、世界の有数のＩＣチップベンダーは、短時間に暗号化可能なコ・プロセッサ付ＩＣチップの開発に力を注いでいる。今年から来年にかけて、市場に製品がでていくものと推測される。

このほかに、従来からある方式としてEMVの静的認証と(７)－②を組合わせた方式がある。(７)－②では１回毎に新たに生成した乱数を用いるため静的認証で同一のＩＣカードが毎回同一のデータを端末装置に送る弱点をカバーできる。共通鍵暗号は処理の負荷が大きくないのでコ・プロセッサは必要ない。

9)　端末装置の認証

① オンライン処理の場合

ＩＣカード－端末装置－ホストコンピュータの間で毎回オンライン処理が行なわれる場合、端末装置によるＩＣカードの正当性の確認は必要であるが、端末装置の正当性確認はＩＣカードからでなく、ホストコンピュータから行なうことが可能であり、(７)－①の手順は必ずしも必要ではない。

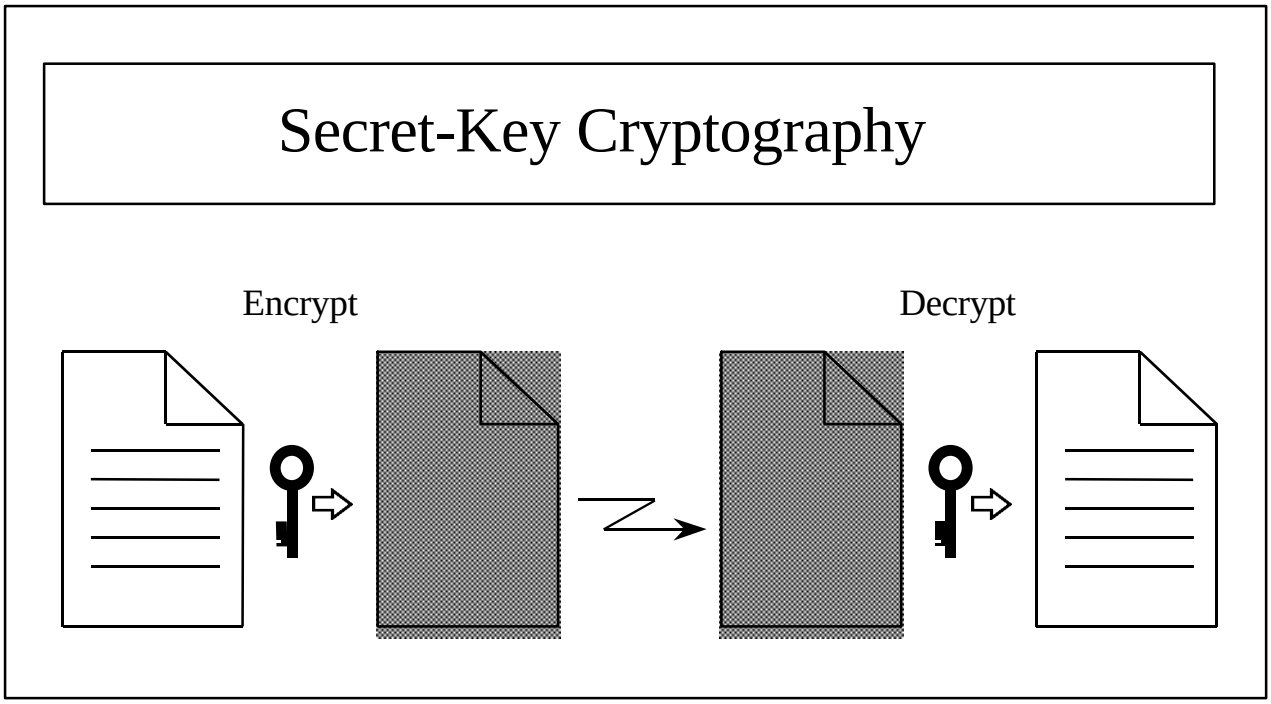
② オフライン処理の場合

端末装置－ホストコンピュータ間では毎回オンライン処理を行なわずＩＣカード－端末装置間の処理のみが行なわれるケースがある。この場合、端末装置－ホストコンピュータ間ではたとえば一日分の取引をまとめて処理することになる。

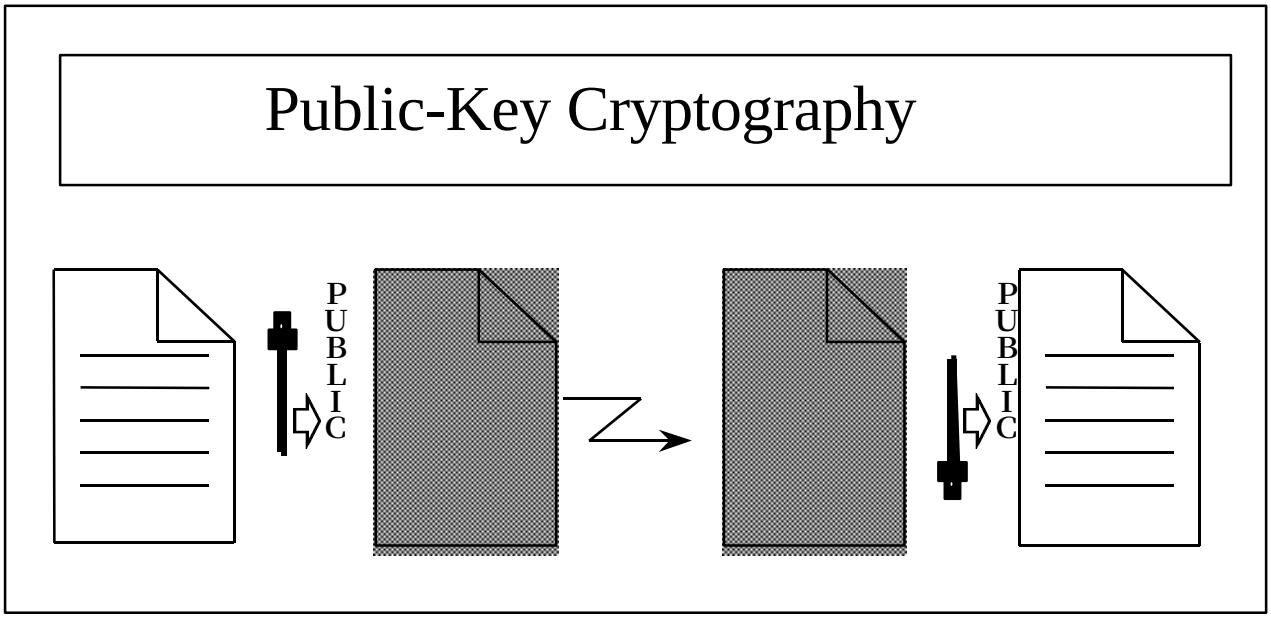
この場合、ＩＣカード側としては、ホストコンピュータによる端末装置の認証がオンラインで行なわれる訳ではないので、(７)－②の手順により、端末装置の認

証を行なう。

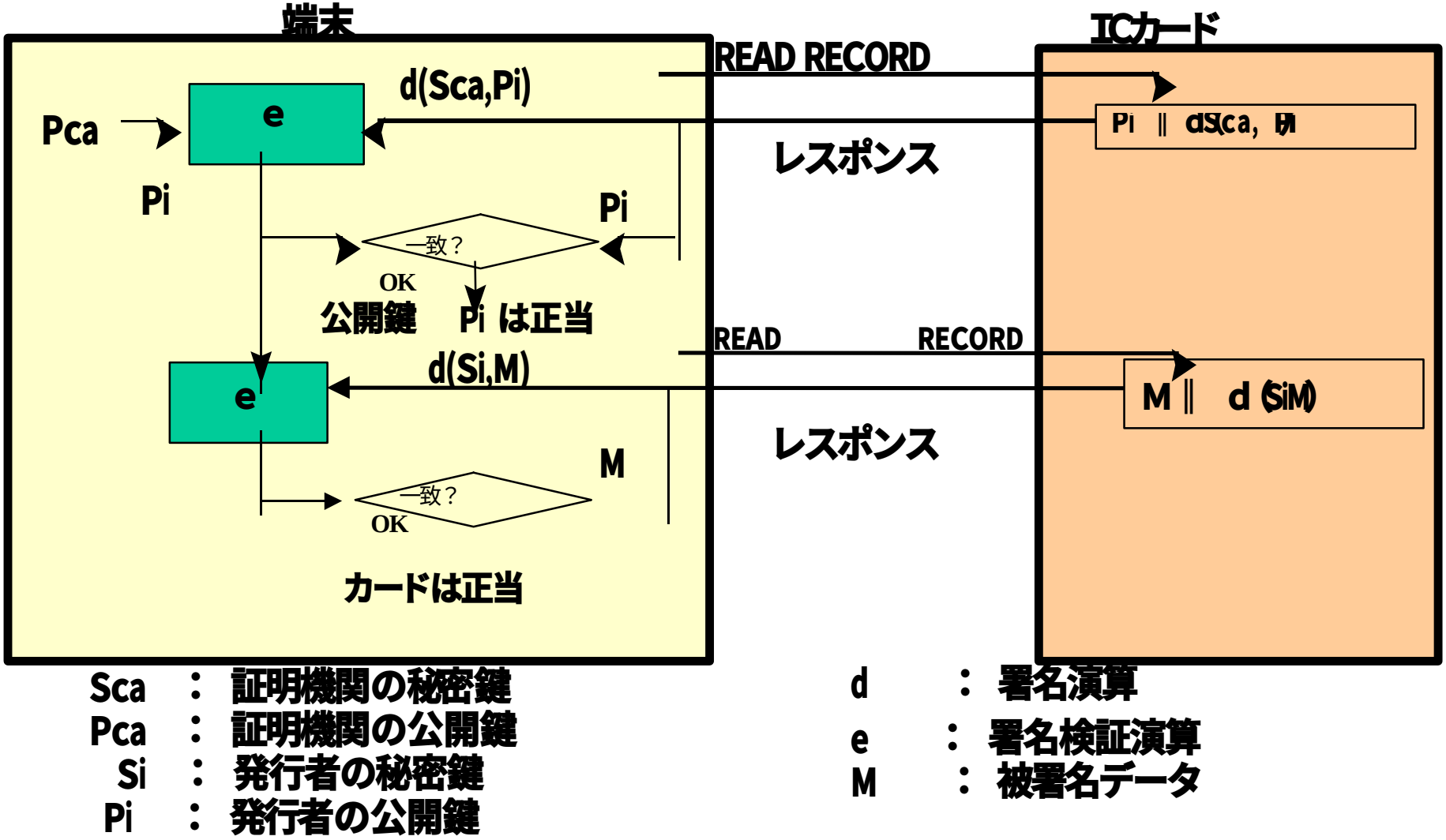
端末装置のソフトウエアは、ＩＣチップよりはるか複雑であり、端末装置がTamper-proof　改ざんが不可能な構造）になっている場合、端末装置の偽造、改ざんはありえないとの立場から、端末装置の認証を行わないシステムもある。



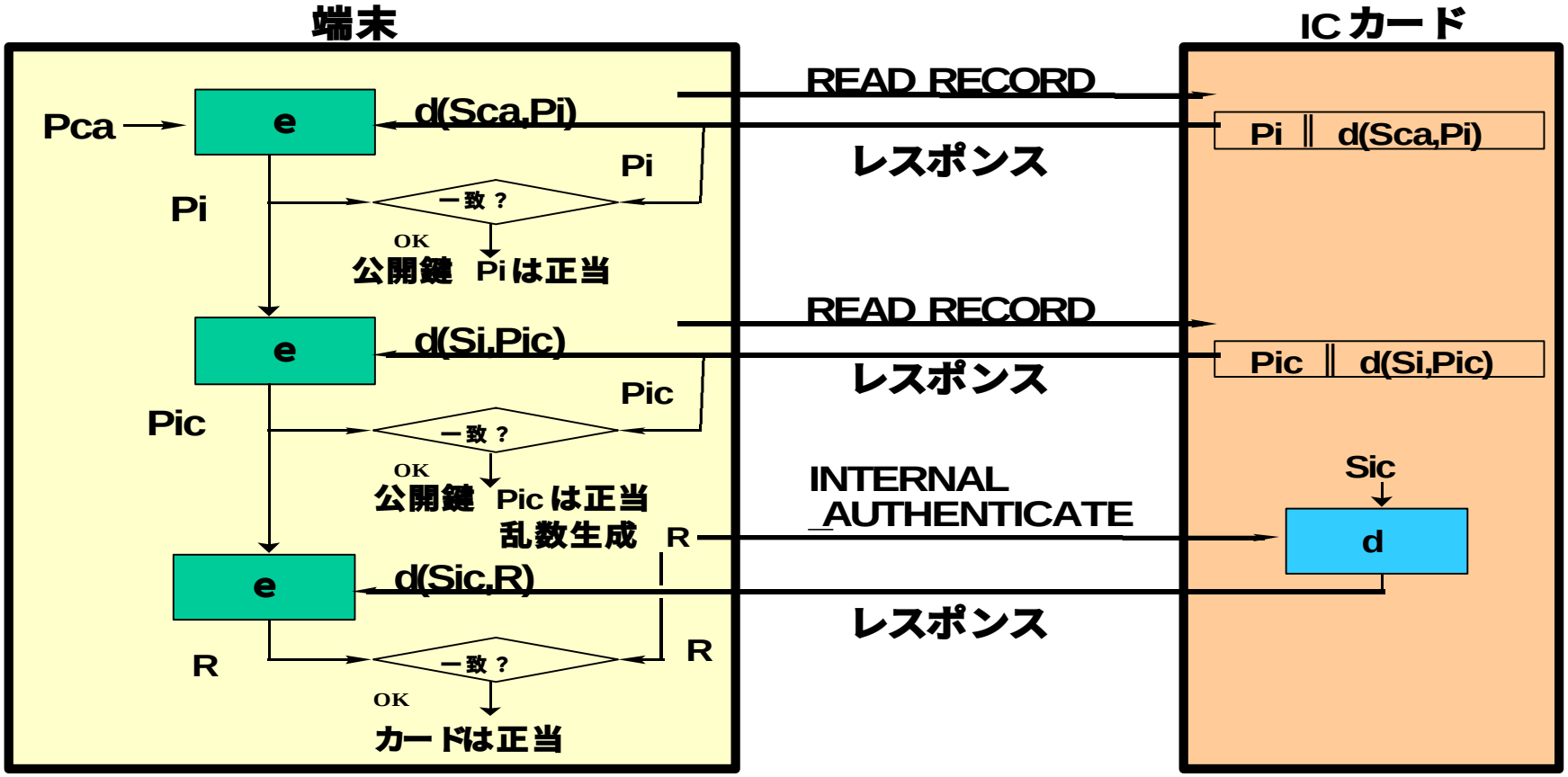
図－１　秘密鍵暗号（共通鍵暗号）



図－２公開鍵暗号

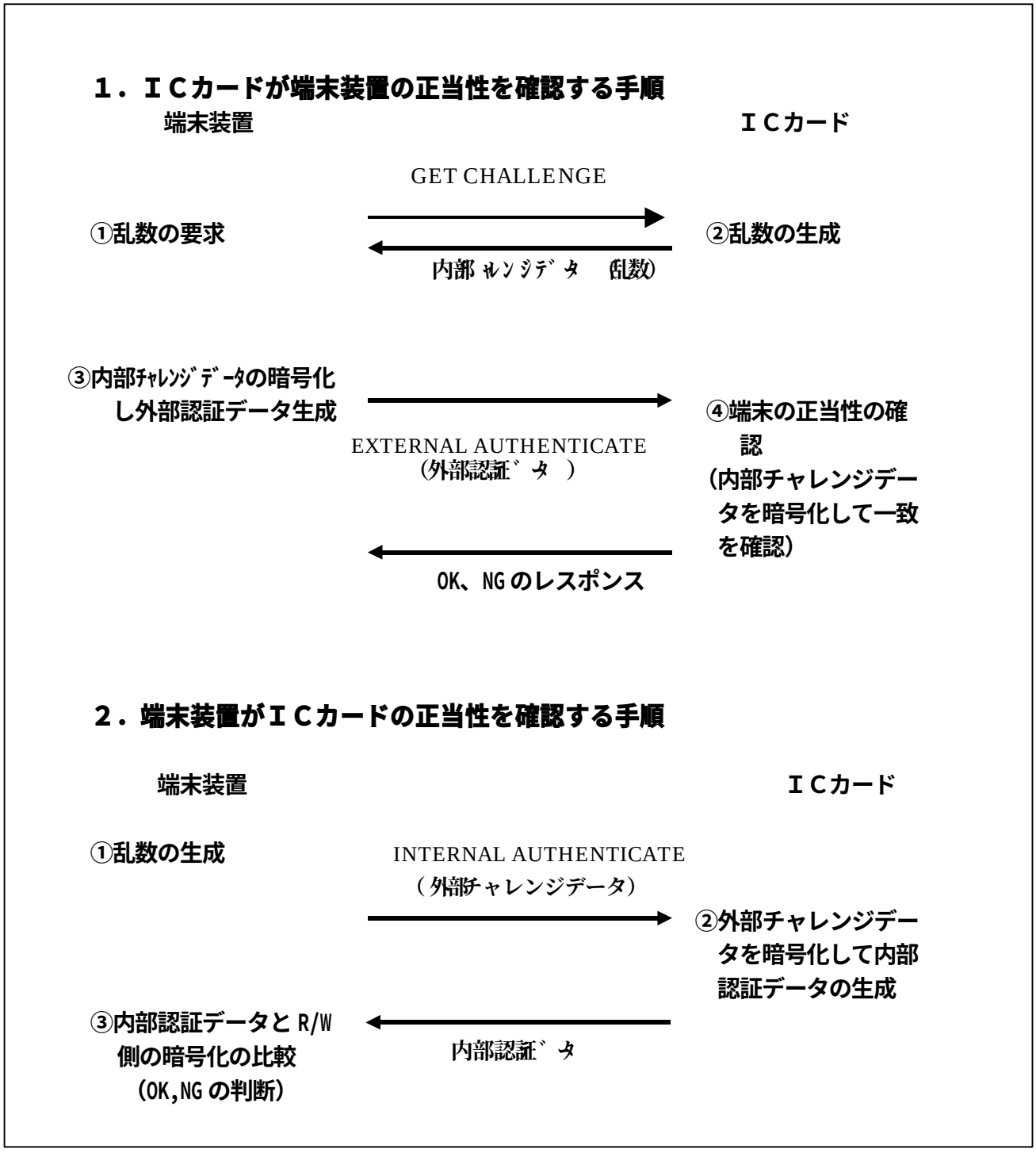


図－３　ＩＣカードの静的認証



Sca ： 証明機関の秘密鍵
Pca ： 証明機関の公開鍵
Si ： 発行者の秘密鍵
Pi ： 発行者の公開鍵
Sic ： ICカードの秘密鍵
Pic ： ICカードの公開鍵
d ： 署名演算
e ： 署名演算の逆演算
R ： 乱数

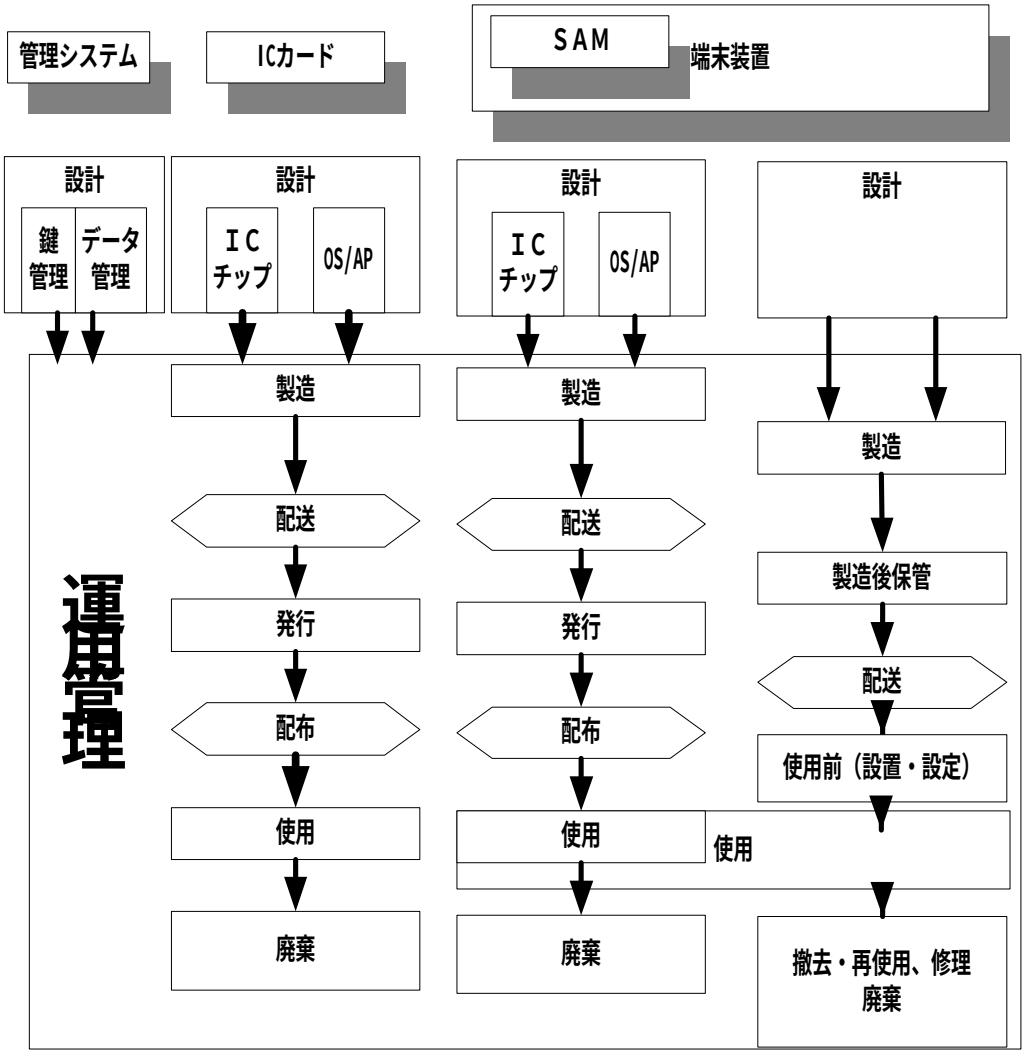
図－4 ＩCカードの動的認証



図－５　端末装置とＩＣカード間の認証

（参考資料３）ＩＣカード型電子マネーシステムにおけるライフサイクルとセキュリティ管理

一般にＩＣカードシステムにおいては、使用するＩＣカードの設計・製造、発行から使用、廃棄までのライフサイクルの各フェーズでセキュリティ管理に留意する必要がある。ＩＣカード型電子マネーシステムにおいては、ＩＣカードに加え、価値情報や取引き結果および暗号鍵等の秘密情報を保持・蓄積している端末装置、あるいは、端末装置内のＳＡＭ（セキュア・アプリケーション・モジュール）を含めたシステム全体でのライフサイクル管理を行う必要がある。



＜ ライフサイクル・フロー＞

上図のように、システムのライフサイクルを通じ、それぞれのフェーズにおいてセキュリティ管理が必要となる。ＩＣカード型電子マネーシステムにおいては、次のものが管理対象となる。

(1)　ＩＣカード（顧客カード）

(2)　発行機や店舗端末等の管理用ＳＡＭ（セキュア・アプリケーション・モジュール）

(3)　端末装置

これらのＩＣカードや端末装置等のライフサイクルに関連する規格としては、以下のものがある。

ISO10102-1:1991-Financial transaction cards-Security architecture of financial transaction systems using integrated circuit cards-Part 1:Card Life Cycle

ISO/DIS 13491-1:1996–Banking–Secure cryptographic devices(retail) Part1: Concepts, requirements and evaluation methods

(1) ICカード、(2) SAMについてはISO10102-1、4などで規定されているカードライフサイクル

ＳＡＭライフサイクルに関する記述が参考となる。また、(3)端末装置については、ISO13491-1などで規定されるセキュアな暗号装置に関する記述が参考となる。

また、鍵管理に関しては、“暗号利用技術ハンドブック”の鍵管理の章が参考となる。

なお、具体的な運用に当たっては、各電子マネーシステム毎でのライフサイクル管理規定を設ける必要があり、さらには、これらの管理規定において、カード発行者、および、サービス提供者それぞれの管理範囲を明確にすることが必要となる。