

共通セキュリティ関連技術 WG 中間報告書

平成 9 年 5 月

電子商取引実証推進協議会 (ECOM)

目 次

1	はじめに	1
2	共通セキュリティ関連技術WGの目標と研究内容	1
	2.1 目 標	1
	2.2 研究内容と成果.....	1

1 はじめに

EC協議会（略称ECOM）の中の共通セキュリティ関連技術WGとして、会員会社の各委員の方のご協力を頂き、過去1年間研究を行なってきた。

ECシステムのセキュリティ機能について成果を公表するのは、本年9月を予定しているが、平成8年度の活動報告書として今回、中間報告をまとめた。

今回の主な報告内容は

第1部 ICカード型電子マネーシステムセキュリティガイドライン

第2部 インターネット利用クレジット決済システムのセキュリティ機能である。

WGの研究内容、本年9月予定の成果物については次章を参照して頂きたい。

クレジット決済のためのセキュア・プロトコルとしてはいくつかの方式があるが、多くの実証実験プロジェクトでSET（Secure Electronic Transaction）準拠のプロトコルを採用している。

このため第2部の参考資料として、SET概説を添付した。

2 共通セキュリティ関連技術WGの目標と研究内容

2.1 目 標

実証実験プロジェクトをはじめとして、各種のECシステムが、運用を開始し、今後も、銀行決済など、新しい形のシステムが開発されようとしている。

ECシステムでは、セキュリティ機能の重要性が、必ず指摘されるが、具体的な機能となると、表現方法すら一定ではなく、個々の表現に委ねられているのが現状である。

今後、システムの開発あるいは、運用にあたってセキュリティ機能の評価、比較が容易な統一された表示方法があれば、大変便利であり、ECの発展に役立つ。

この目標に従って、以下、サブWGに分れて研究中である。

2.2 研究内容と成果

(1) ICカード使用の電子マネー サブWG

各国で、様々な技術開発および実験が行なわれ、特にMomdex、Visa、Master Cardのストアードバリューカードは広い範囲で実験が行なわれている。

実証実験プロジェクトでも、4プロジェクトでサポート予定である。

当サブWGではチップの設計・製造、カードメーカーの一次発行、運搬、金融機関の二次発行、バリューの移転、バリューの回収、カードの廃棄の各フェーズについて必須、推奨、選択に分けて、セキュリティ機能要件を研究している。

研究手順、報告内容を図2-1に示す。

今回はステップ3までの成果（ 版）の報告でありステップ5までの成果を 版として本年9月に公表する予定である。

(2) インターネット上のクレジット決済 サブWG

実証実験プロジェクトのうち、10 のプロジェクトで、この業務がサポートされる。

(表 2 - 1 参照)

実証実験以外にも、既に多くのシステムが使用開始され、また開発中である。

セキュリティ機能の充実はコスト上昇につながるものであり、システムの対象(消費者の規模、取扱商品、限度額)によって、セキュリティ機能も選択される。

当サブWGでは、システムのセキュリティ設計の責任者が、多様な角度から見たセキュリティ機能と機能レベルについて自己評価できる仕掛を研究する。(評価リスト、評価の手引書)

システム事業者とシステムインテグレータとの間で、セキュリティ機能の確認を行なう際に、比較/評価に役立つ。

研究手順、報告内容を図 2 - 2 に示す。

ステップ4の成果を 版とし、ステップ6までの成果を 版として本年9月に公表する予定である。

(3) 暗号タスクフォース

システム事業者、システムインテグレータが必要とする暗号知識(暗号方式と鍵長、鍵管理、米国の輸出問題など)の解説書を、クレジット、ICカードの 版に合せ、本年9月に公表すべく研究中である。

表 2 - 1

プロジェクト名	中心となる会社名	電子商取引の内容	実験開始	セキュア°モデル
商施設プロデュース(まちこ)	NTTデータ通信(株)	3次元モール運営、クレジット決済	H9.4	SSL
エレクトロニック・マーケット・プレイス	日本IBM(株)	モール運営、ICカード認証クレジット決済、電子マネー	H9.4	iKP+EMV
ジャパン・ネット	三菱商事(株)	企業間電子商取引、モールでの電子通販・電子出版 (銀行決済) (クレジット決済)	H9.1	SET他
スマート・カラー・クラブ	(株)三菱総研	モール運営、クレジット決済、仮想銀行決済	H9.1	SET他
サイバーネット・クラブ	UCカード(株)	モール運営、クレジット決済	H8.6	SECE
サイバー・コマース・シティ	(株)関西情報センター	マルチメディア利用モール運営、クレジット決済	H9.1	SET
メディアポート名古屋	(株)名鉄コンピュータサービス	モール運営(取引代行)、クレジット決済	H9.4	SECE
スマートコマースジャパン	(株)東芝	モール運営、ICカード認証クレジット決済、電子マネー	H9.4	SET+EMV
バーチャル・シティ	日本電気(株)	モール運営、パブリックスペースでのキオスク端末、クレジット決済	H9.5	SET
カードレス・カード・システム	(株)野村総研	モール運営、認証書によるクレジット決済 (カードレス)	H8.10	SECE

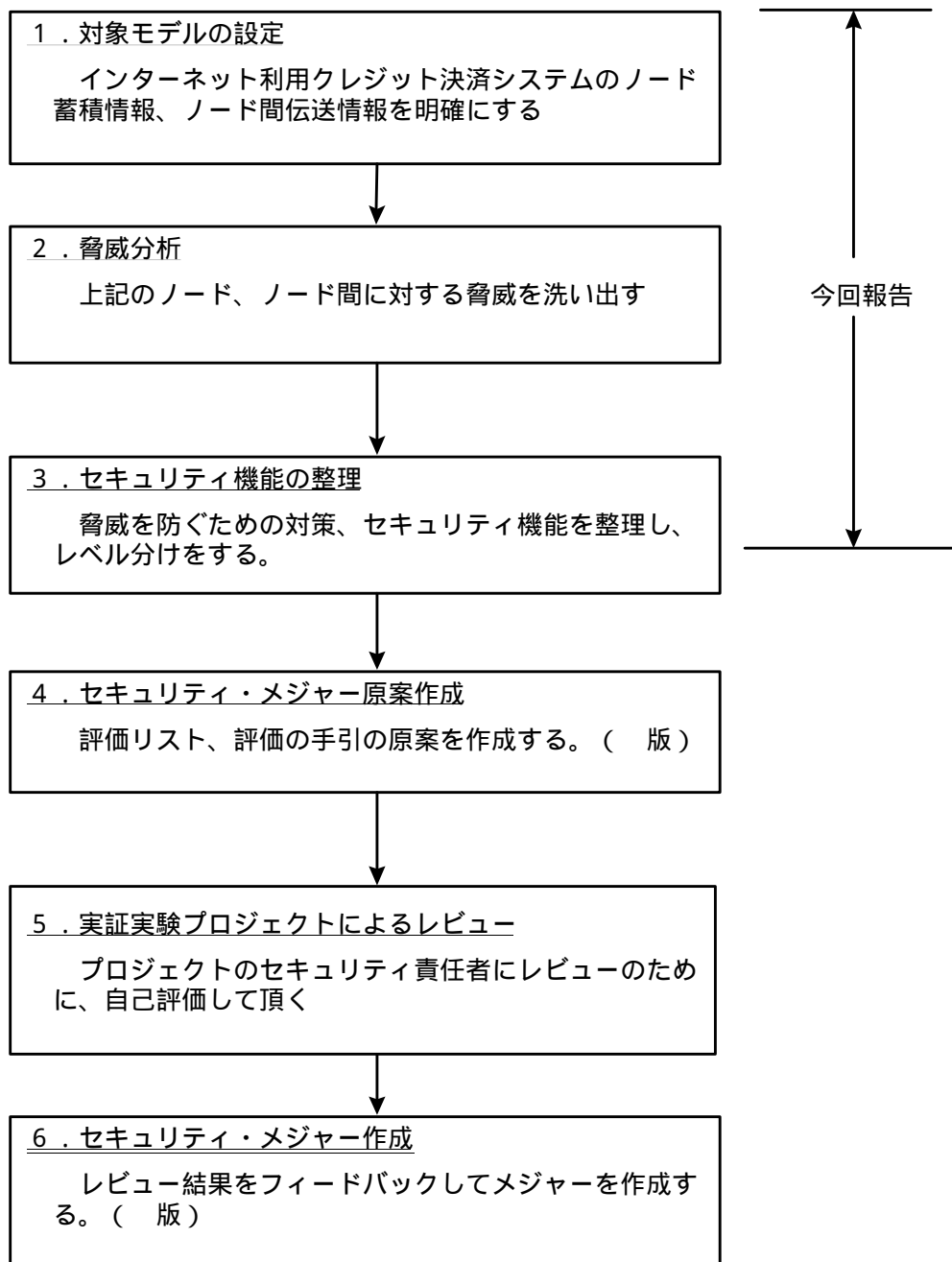


図 2 - 1

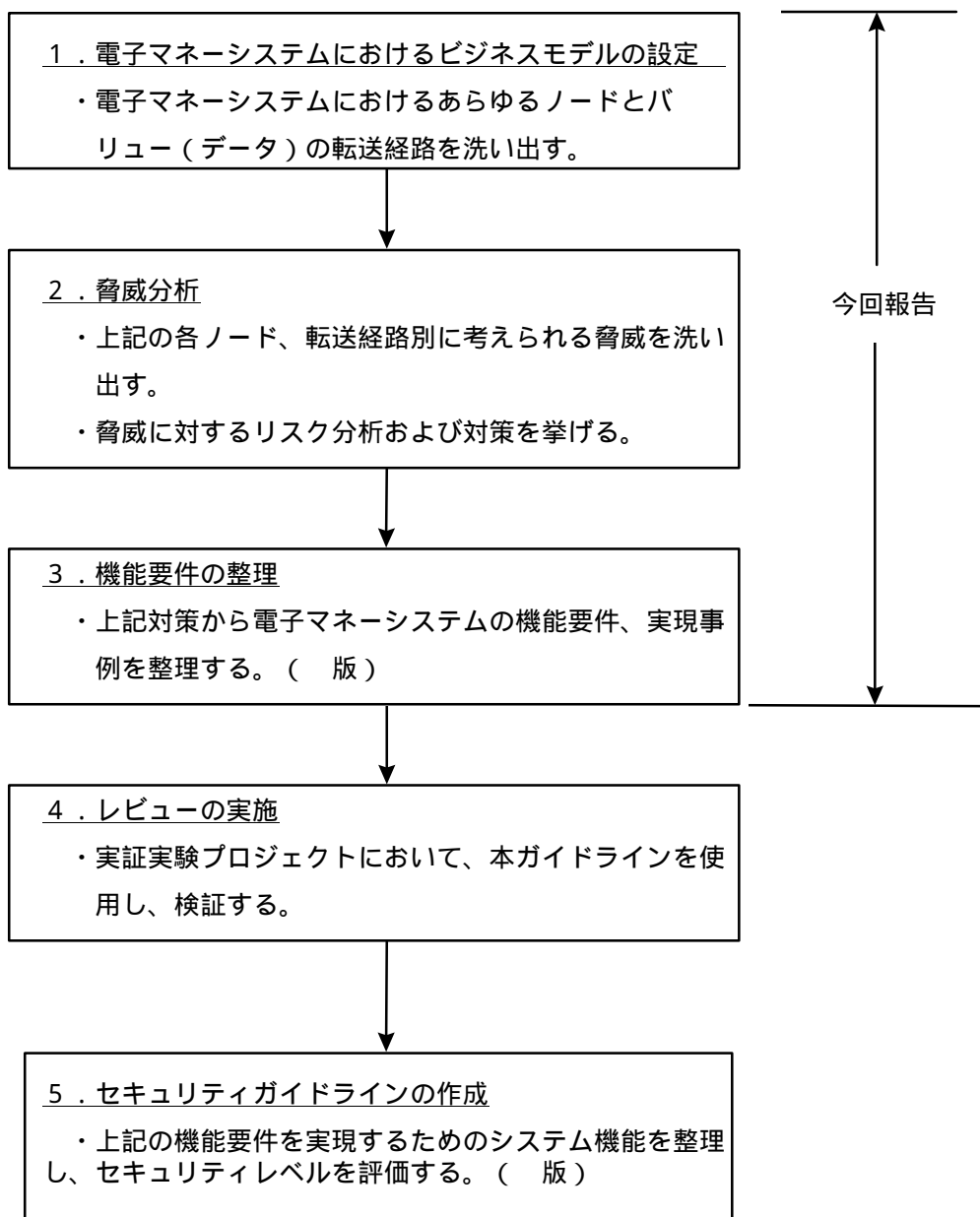


図 2 - 2

第 1 部

ICカード型電子マネーシステムセキュリティ ガイドライン

平成 9 年 5 月

共通セキュリティ関連技術WG

目 次

1	はじめに（ＩＣカード型電子マネーシステムのセキュリティについて）.....	1
2	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.....	1
3	セキュリティ対策の進め方.....	8
4	ＩＣカード型電子マネーのノード分析事例.....	9
5	ＩＣカード型電子マネーの脅威分析のまとめ.....	11
6	ＩＣカード型電子マネーのセキュリティ機能要件について.....	14
6.1	電子マネーとしてのＩＣカードのセキュリティ機能の要件.....	14
6.2	ＩＣチップ、ＩＣカードに対するセキュリティ要件.....	15
6.2.1	ＩＣチップ、ＩＣカードの製造過程における要件（不正流出の防止）....	15
6.2.2	ＩＣチップの不正解析（電子顕微鏡による解析）の防止.....	16
6.2.3	ＩＣチップ不正アクセス手段の解析.....	16
6.2.4	ＩＣチップ誤動作による不正解析（熱、圧力、etc.）.....	16
6.2.5	ＩＣカードの流通過程における要件（盗難対策）.....	17
6.2.6	ＩＣカードの廃棄における要件.....	17
6.3	各種端末機器のセキュリティ機能要件.....	18
6.3.1	端末機器の設計／製造工程での不正防止.....	18
6.3.2	端末機器の正当性の証明.....	18
6.3.3	端末機器のソフトウェア、機密データの保護.....	19
6.3.4	端末機器の流通過程における要件.....	20
6.4	発行機関におけるＩＣカードの運用と要件.....	21
6.4.1	ＩＣカードの発行過程における要件（不正発行の防止）.....	21
6.4.2	電子マネーの貯蔵機能における要件.....	22
6.4.3	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.....	23
6.4.4	電子マネーにおける上限金額の設定.....	23
6.5	電子マネーの価値移転時のセキュリティ機能要件.....	1
6.5.1	不正な電子マネー引き出しの防止.....	24
6.5.2	電子マネーの転送経路のセキュリティ機能要件.....	25
6.5.3	電子マネーの価値移転時のエラー.....	26
6.5.4	価値移転後の否認防止.....	26
6.5.5	価値移転時の機器障害時のセキュリティ機能要件.....	26
6.5.6	電子マネーの金融機関システムへの転送時のセキュリティ機能要件.....	27
6.5.7	加盟店での決済時点におけるセキュリティ機能要件.....	27
6.5.8	加盟店での運用上におけるセキュリティ機能要件.....	28
6.6	消費者保護について.....	28
6.6.1	消費者のプライバシー対策（匿名性について）.....	28
6.6.2	ＩＣカードの盗難・紛失対策.....	29
7	ＩＣカード型電子マネー検討メンバー（敬称略、順不同）.....	30

1 はじめに(ICカード型電子マネーシステムのセキュリティについて)

我が国の消費社会における決済の仕組は、現金、クレジットカード、手形、銀行振込、プリペイドカード等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、Mondexの実証実験、Visa, Master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おり、その内容は、いずれもオフラインによるICカード型の即時決済系が中心である。

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。又、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い出し、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カードの相互認証、デジタル署名通信に応用可能である。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。

又、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ー保護が必要である。

本報告書はICカードの電子マネーシステムに発生しうるあらゆる脅威を洗い出し、電子マネーシステムの機能要件をまとめたものである。更に本報告書は、電子マネーシステム構築時にセキュリティ機能の実現にあたってのガイドラインとなることを目的とする。又、本報告書は今回は中間報告書であり、今後レビュー後9月に完成版を出版する予定である。

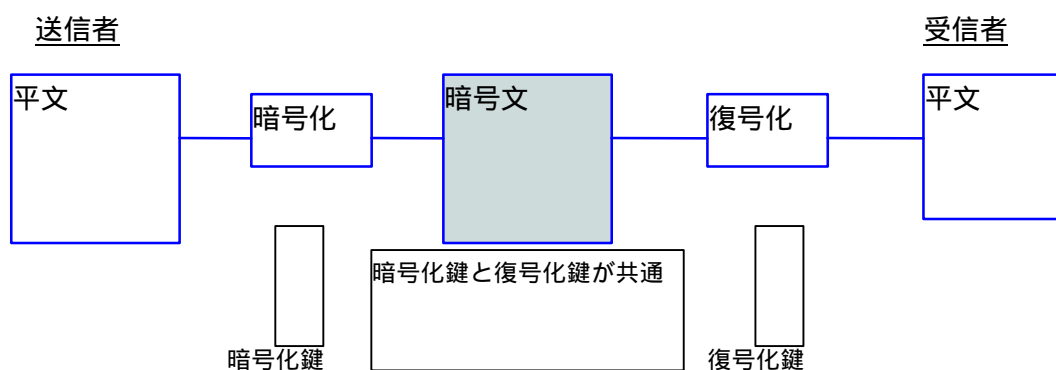
2 ICカード型電子マネーシステムとセキュリティ技術について

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、第5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竄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、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)、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、改竄、否認等の防止)、メッセージの秘匿等が必要である。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。以下にICカード型電子マネーにおいて一般的に使用されている暗号処理技術について述べる。

(1) 共通鍵暗号方式

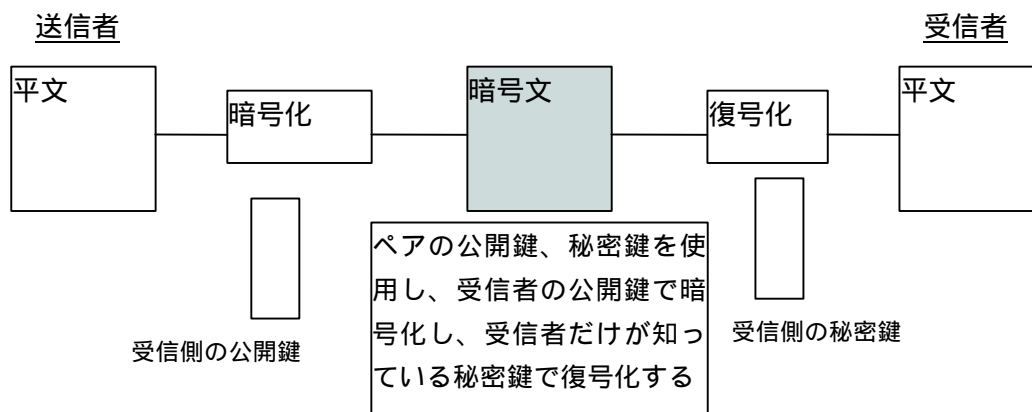
共通鍵暗号方式は、対称型暗号方式とも呼ばれ、メッセージの暗号化と復号化で同じ鍵を使う方式。従って、メッセージの送り手と受け手は秘密の鍵を共用することになる。本方式は高速な演算処理が可能であるが、全利用者ICカードに共通の鍵を書込んでおくことになり、共通鍵が解かれた場合の被害が甚大となる。又、通信相手毎に共通鍵を変えることはICカード型電子マネーの場合は現実的でない。共通鍵暗号方式の代表的なものにDES方式がある。



(2) 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。ICカード型電子マネーに应用する場合は、すべてのICカードに公開鍵、秘密鍵を事前に書込んでおき、公開鍵は通信相手に都度転送することになる。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。上記のようにICカード型電子マネーにおいては、ICカード発行時に鍵の書込みが必要となるため、ICカード発行システムにおけるセキュリティも重要なポイントである。特に鍵の生成にあたり、発行機関から正規に発行されたものであることを保証するため公開鍵、秘密鍵に加え、公開鍵証明書を添付する。

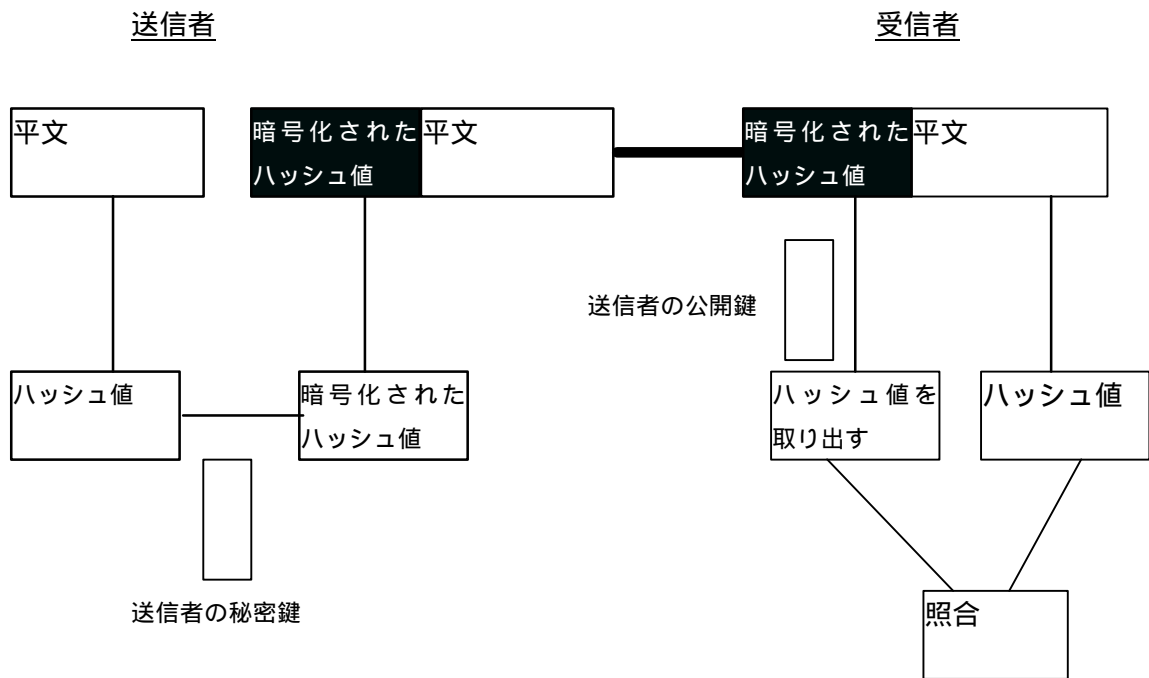
更に、昨今ICカードにおいてRSAの公開鍵暗号処理を可能とするため、RSAを高速で実行するための専用のプロセッサを持ったICカードがあり、RSA方式採用の場合は必須となろう。



	共通鍵方式	公開鍵方式
処理時間	短い	長い (I C カード内で実現するためには専用のプロセッサが必要)
鍵の個数	一般的には通信相手の数だけ鍵が必要 (I C カードの場合は同じ鍵を事前に書込むことになる)	利用者ごとに一組の公開鍵、秘密鍵が必要 (通信相手ごとには必要ない)
鍵の配送	通信相手への配信が必要 (I C カードの場合は事前に書込むことが必要)	一般的には通信相手への配信は不要 (I C カードが通信する場合は通信相手に公開鍵を転送することになる)
具体例	D E S / トリプル D E S F E A L、Clipper 等	R S A、エルガマル、楕円曲線暗号等

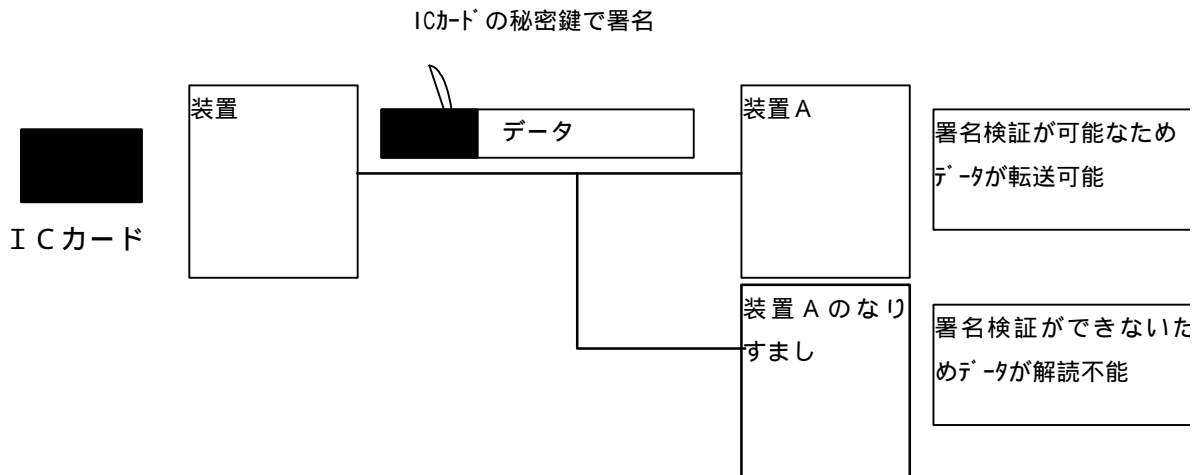
(3) デジタル署名

I C カードから I C カードへ電子マネーを転送する場合、なりすまし、改竄、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、下図のとうり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 I C 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とり、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。



なりすましの防止について

電子マネーの価値移転時、ネットワーク上で転送相手の装置へのなりすましを防止するため、価値データに対してデジタル署名通信を行うことで通信相手の特定、改竄の防止が可能となる。



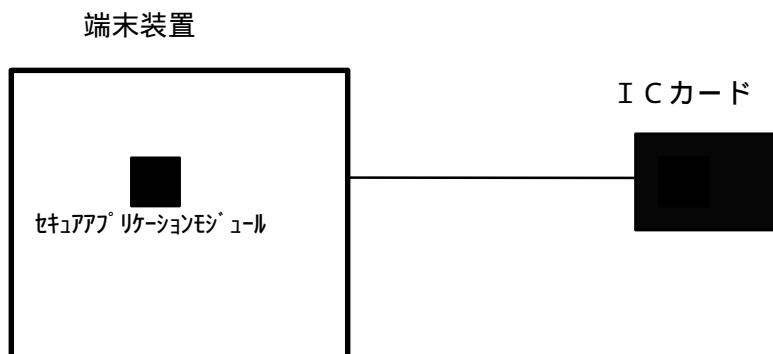
(4) 相互認証

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。以下に公開鍵暗号方式の場合の相互認証の事例を示す。本方式はICカードの発行機関に加え、第三者の証明機関が存在する場合の方式である。

(a) 相互認証の方式

イ. 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。

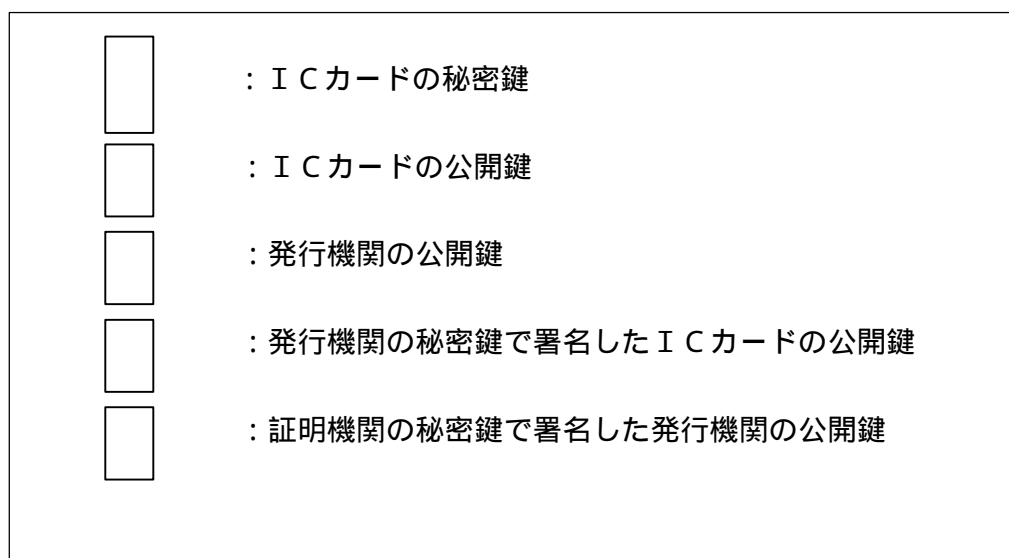


ロ. ICカード主導方式

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) 保有する鍵の種類（例）

公開鍵方式の場合、ICカードの発行機関に加え、証明機関を設定する場合の鍵の種類は以下のようになっていると考えられる。（ICカード内に保有する鍵）



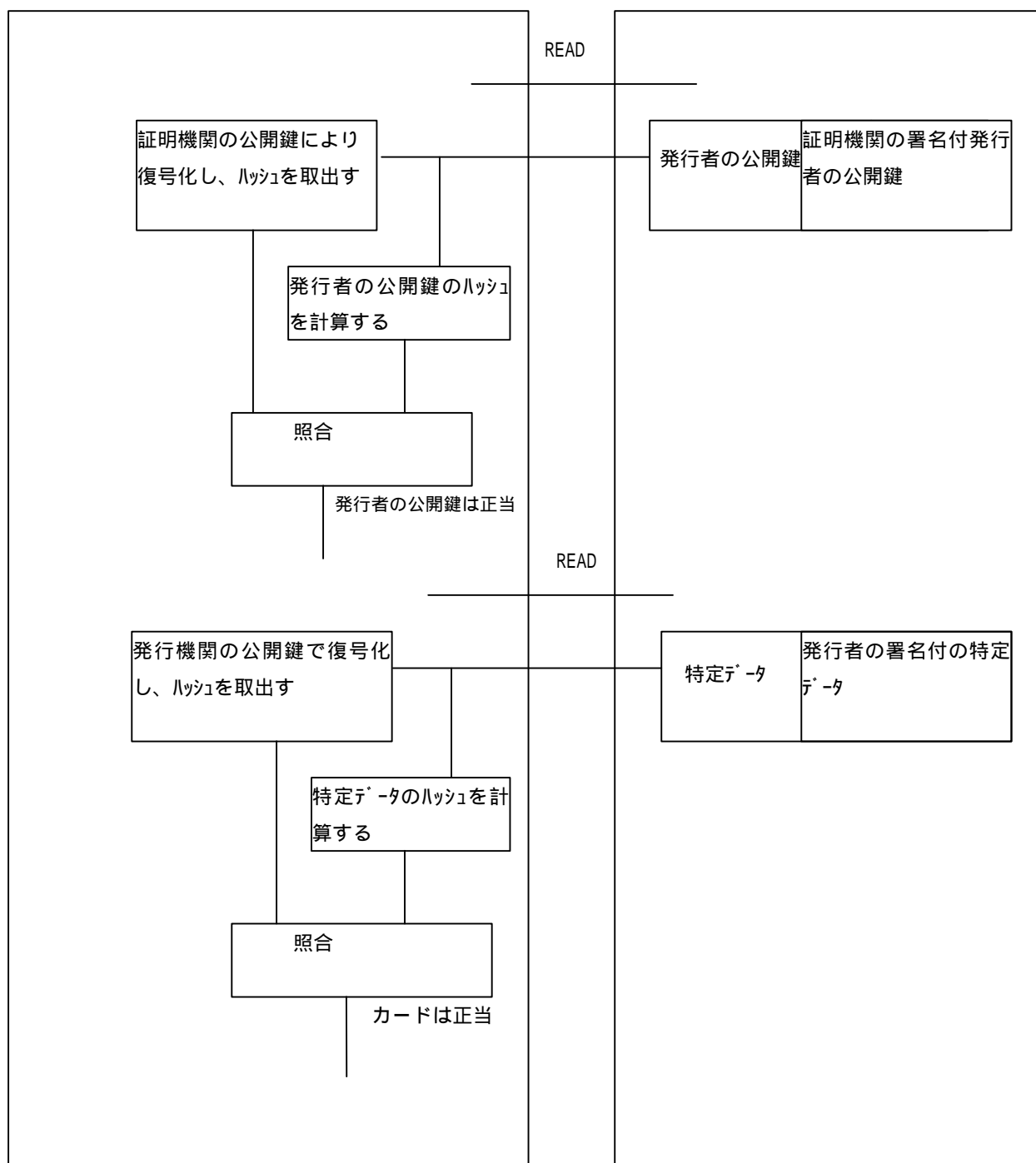
(c)相互認証ロジック例

端末主導のケースについて述べる。

イ. 静的認証方式

端末装置

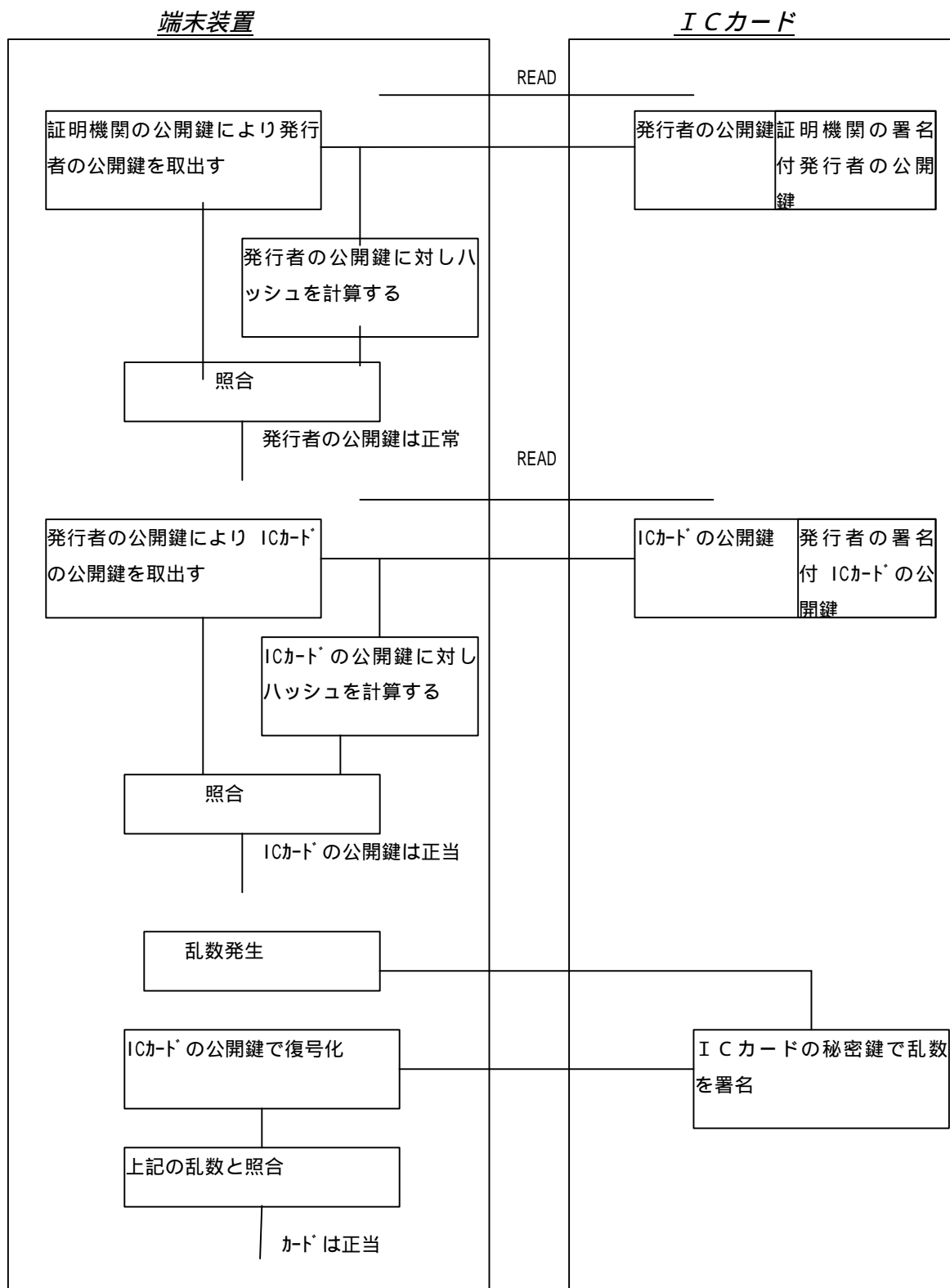
ICカード



不一致の場合は端末が認識し、認証エラーの表示を行う。

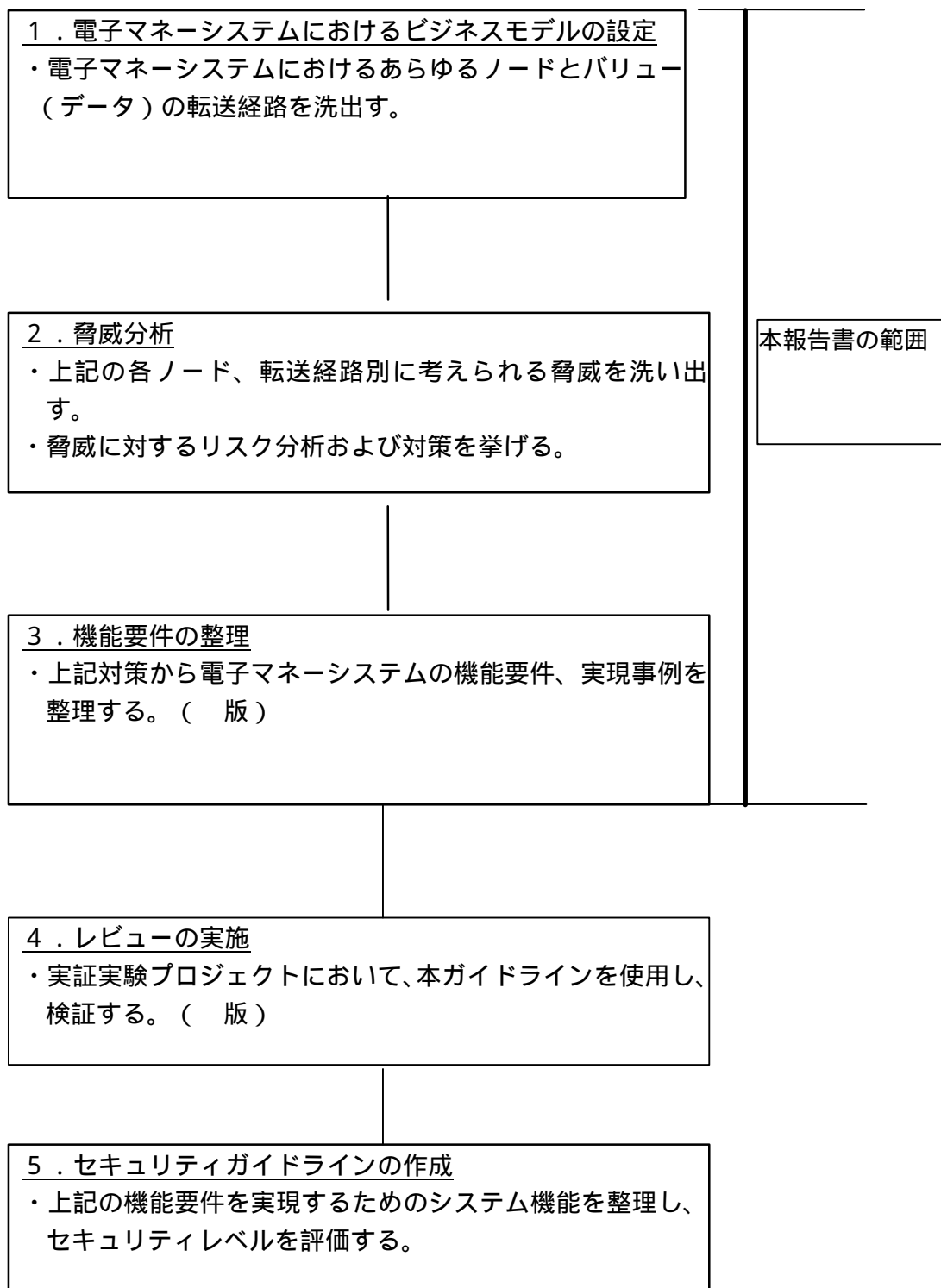
ロ. 動的認証

動的認証の場合は下図のように上記の認証に加え、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。

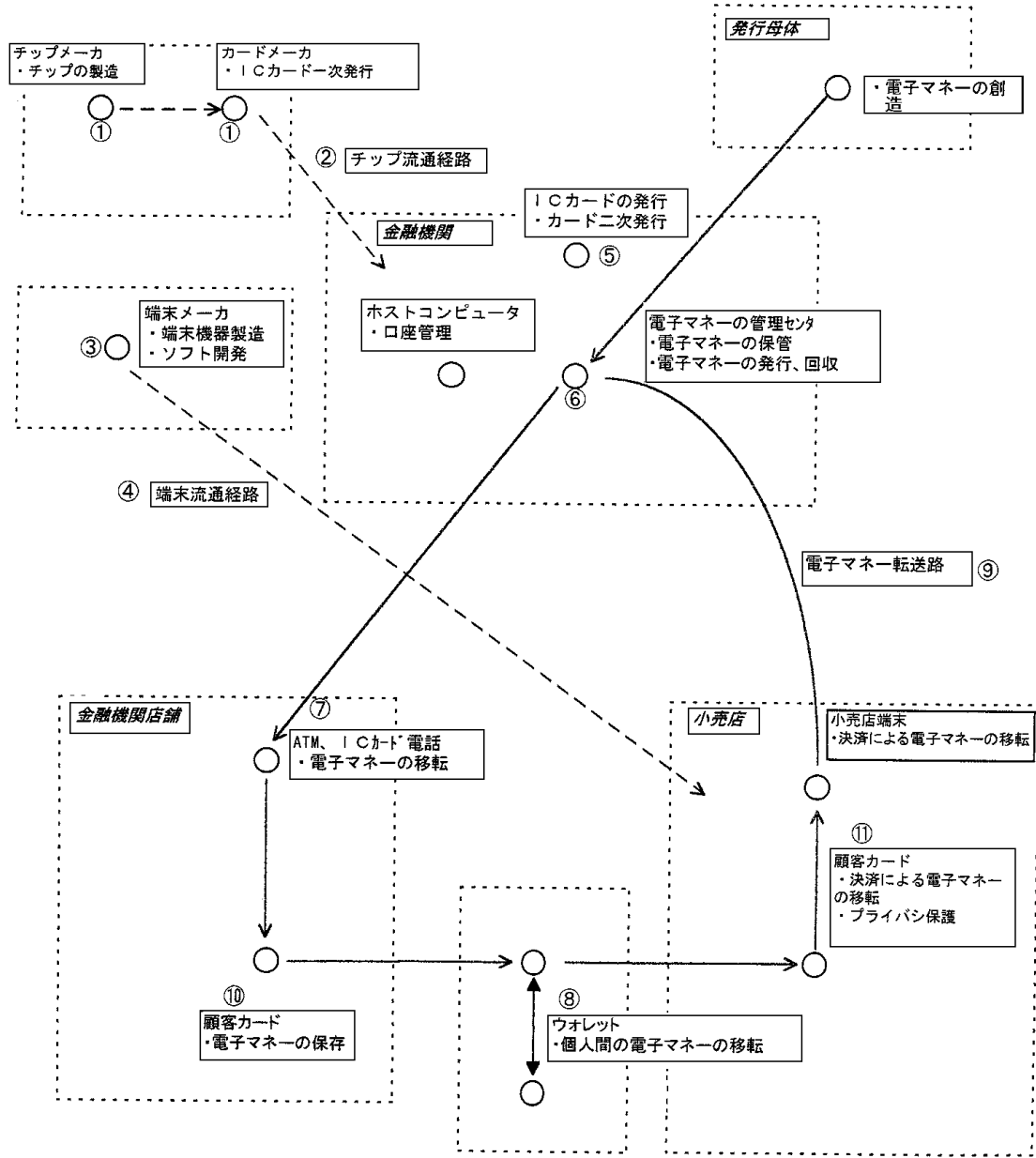


3 セキュリティ対策の進め方

ICカード型電子マネーシステムにおける安全対策基準作成にあたり以下の手順で分析した。



4 ICカード型電子マネーのノード分析事例



(注)

————→ 電子マネーの価値移転経路

-----> ICカード、機器等の運搬経路

5 ICカード型電子マネーの脅威分析のまとめ

脅威の内容			脅威の具体的内容						発生の可能性 (難易度)
NO	ノード	内容	誰が	いつ	どこで	何を	目的	方法	
	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	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盗団との共謀により可能
	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 る者で相当な研究設備 有する者(電子顕微鏡 する等)
	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カードのパリ 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 る者で相当な研究設備 有する者
	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カードのパリ 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 る者で相当な研究設備 有する者
	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カードメーカーが)	金融機関への輸送途中	金融機関への輸送途中	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により可能
	端末機器製造業者	端末機器のソフトの改竄による不正使用	端末設計者	いつでも	端末製造メーカー	端末内のパリュ ュー	端末内のパリュ ューを不正に増やす	ICカードのアクセス方法を解析して	端末ソフト開発経験者
	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	小売店への輸送途中	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により可能

脅威の内容			脅威の具体的内容						発生の可能性 (難易度)
NO	ノード	内容	誰が	いつ	どこで	何を	目的	方法	
	ICカードの発行	ICカードの不正発行	ICカード発行事務のオペレータ	発行手続き中	銀行の事務センター	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	カードの申し込み用紙を盗む	内部犯行(オペレータと管理者と共同で犯行が可能)
	ICカードの	鍵情報の漏洩	ICカード発行事務のオペレータ	発行手続き中	銀行の事務センター	鍵情報の書かかれているフ	偽造カードを作目的	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)

	発行		タ			ファイルを盗む		て	
	ICカードの発行	ICカードの発行管理資料を捏造して不正に発行する	システムの開発者と内部の者が共謀して	発行手続き中	銀行の事務センター	ICカードを不正に発行	偽造カードを作目的で	ICカード発行管理資料を捏造して発行の履歴を抹消する	システム開発者と内部のペレータの共謀
	バリュー管理センター	電子金庫からICカードを盗難	金融機関の内部の者	管理者のいない時	バリュー管理センターの設置してある建物内	電子金庫からICカードを盗み出して	電子マネーを盗むために	電子金庫の開け方をぬすんで(パスワード等)	バリュー管理センターへ入ることが許される者に限定
	バリュー管理センター	電子金庫内のICカードを別のICカードにすりかえる	金融機関の内部の者	管理者のいない時	バリュー管理センターの設置してある建物内	電子金庫のICカードを別のICカードに交換して	電子マネーを盗むために	電子金庫の開け方をぬすんで(パスワード等)	バリュー管理センターへ入ることが許される者に限定
	バリュー管理センター	電子金庫のバリューを自分のICカードに移転する	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	バリュー管理センターの設置してある建物内		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ペレータとの共謀(テストシステム等の使用により可

脅威の内容			脅威の具体的内容						発生の可能性 (難易度)
NO	ノード	内容	誰が	いつ	どこで	何を	目的	方法	
	バリュー転送	金融機関内部での不正なバリューの移転	バリューセンターの開発経験者	人のいない所	特別に開発した端末でバリュー引き出し時	不正にバリューを自分のICカードに移転し	バリューを増やすことを目的に	バリューセンター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共謀することで可能
	バリューの転送経路(銀行ATM.電話端末間)	金融機関のバリューセンターからATM、電話端末等により不正にバリューを取得する	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正にバリューを転送する	バリューを不当に取得することを目的に	端末ソフトを改竄して	本システムにおける端末衣鉢経験者
	バリューの転送経路(銀行と端末間)	バリューの伝送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	バリュー転送時に	バリュー転送経路に	バリューを自分のICカードに不当に取得する	バリューを不当に取得することを目的に	電話網に他のICカードを分岐接続になりすまして	カードとカードの転送方をモニタすることでなりましを行えば可能
	バリュー転送経路(ウォレット)	ウォレットで価格移転時、オペレーションで指定した金額を途中で改竄して移転する	システム内部に精通した者	ウォレット使用時	ウォレット使用時	指定した金額を途中で改竄して転送する	バリューを不当に取得することを目的に	ウォレット内ソフトを改竄して	ウォレット内部のソフト設計者が設計資料を入手すれば可能

	内部)								
	バリュー転送経路(ウォレット内部)	ウォレットで価格移転時、電池切れの事故	ICカードホルダが	ウォレット使用時	ウォレット使用時	使用中電池が切れてバリューが消滅する		電池切れ	電池の寿命により発生
	バリューの転送経路(小売店銀行間)	バリュー管理センターになりすまして小売店端末からのバリューを取得する	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	バリューを自分のICカードに不当に取得する	不当にバリューを取得することを目的に	バリュー管理センターに成りすますサーバを開発して	バリュー管理センターのしみを熟知した者に限定される

脅威の内容			脅威の具体的内容						発生の可能性 (難易度)
NO	ノード	内容	誰が	いつ	どこで	何を	目的	方法	
	顧客ICカード(消費者)	バリュー移転の否認	ICカード保有者が	引出し時	ATM、ICカード電話により	バリューを引出し後、引出した事実を否認して	バリュ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
	顧客ICカード(消費者)	プライバシーの侵害(消費者保護)	金融機関のセンターが	買い物時	金融機関のセンターシステムにおいて	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は可能
	加盟店端末	買物代金以上のバリュ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	買物代金以外のオペレーションにより余分のバリューを引出す	不当にバリュ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発者と共謀して特殊なオペレーションを組みこめば可能

6 ICカード型電子マネーのセキュリティ機能要件について

本章では、5.によりノード毎の各脅威内容に対して、対策（機能要件）を記載したが、その機能要件毎に、実際のシステムでの実現事例を挙げた。

又、各実現事例に対して、以下のようなレベル表現をした。

ア.システムに組み込みが必須なもの。-----

イ.システムに組み込むことが望ましいもの。-----

ウ.システムに組み込むかどうかセキュリティレベルに応じて選択すべきもの。---

6.1 電子マネーとしてのICカードのセキュリティ機能の要件

(1) 脅威と機能要件

ICカード型電子マネーにおいて最大の脅威はICカードの偽造であり、電子マネーの発行母体に甚大な被害が発生する。従って、ICカード内部の機能として暗号処理機能を活用した相互認証機能の実現等は必須である。

(2) ICカードの機能要件

(ア) 暗号機能

ICカードの機能として暗号処理機能を保有していることは必須である。

なお、暗号方式は以下の例があるが、ICカード内部での実現性と目的に応じて選択すべきである。

共通鍵暗号機能例

- ・DES / トリプルDES暗号処理
- ・FEAL
- ・Clipper
- ・IDEA、RC2, RC4等

公開鍵暗号機能の保有（コプロセッサ付きICカードが必要となる）

- ・RSAの公開鍵暗号方式

(イ) 相互認証機能の保有

暗号処理による相互認証機能は必須である。方式はICカードの条件と目的に応じて選択する。

共通鍵方式による静的認証方式

共通鍵方式による動的認証方式

公開鍵方式による静的認証方式

公開鍵方式による動的認証方式

6.2 ICチップ、ICカードに対するセキュリティ要件

6.2.1 ICチップ、ICカードの製造過程における要件(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工場内の取り扱い管理及び保管管理時の不正流出防止を保証する必要がある。

ICチップ、ICカードの厳密な数量及び製造番号の管理、また保管室のセキュリティや製造ラインへの入退室管理などの工場全体のセキュリティ確保について保証することが必要である。

(2) 機能要件

(ア) ICチップの設計時における管理

設計ブロックごとに分け、複数者に分担する。

設計図及び仕様書等の情報管理を厳密に行う。(データの焼却、消去、etc.)

ROMデータの情報管理を厳密に行う。(ROMデータ作成時における独自プログラム言語の使用、etc.)

(イ) ICカードの製造時における管理

工場入庫時におけるICチップ、ICカードの受入チェックを行うこと。(入庫形態、品番、数量、入庫場所、担当者、管理番号、etc.)

加工作業前に使用するICチップ、ICカードのチェックを行うこと。(品番、数量、管理番号、取り扱い担当者、etc.)

加工作業後に作業時に発生したICチップ、ICカードの損失及び製品の管理を行うこと。(損失品、製品、予備品、各々のICチップ、ICカードの数量及び管理番号の付与、取り扱い担当者、etc.)

(ウ) 保管管理

ICチップ、ICカード、設計書等を保管する場所のゲートにおける入室管理を行うこと。

保管場所における保管庫の施錠を義務づけ及び鍵の管理を行うこと。

(エ) 工場のセキュリティ確保

作業員の身元確認を行うこと。

作業員の入退管理、行動制限を行うこと。

工場全体の保安を確保すること。(警備会社との提携、etc.)

ICチップ、ICカード発送時における受け渡しする際、工場の人間と運送業者が直接に接触できないようにバッファの部屋を用意するなどの工夫をすること。

(オ) 残損処理管理

製造時に発生した予備品及び損失品を物理的に破壊し処分すること。(ICチップの電氣的破壊、パンチングによる物理的破壊、etc.)

(カ) ソフト上のガード

初期化されたカードは最初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工夫する。オンラインで接続することにより、事

前登録の PIN 番号を要求し、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

6.2.2 ICチップの不正解析(電子顕微鏡による解析)の防止

(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は、ROMに焼き付けられているOSを知る必要があり、このROMを解析されることを防止する必要がある。

(2) 機能要件

(ア) ICチップ内のROMエリアをを工夫を行うこと。(ICチップの一番下の層に形成する、etc.)

(イ) ROMデータ作成の工夫を行うこと。(独自の専用開発ツールを使用する、etc.)

(ウ) ROM層の上にダミーの前面電極を挿入して電子顕微鏡での解析を困難にする。

(エ) IC設計の際にできるだけ小さいマイクロルールを使用して物理的に解析を困難にする。

(オ) 適宜にダミーを入れて電子顕微鏡での解析を妨害する。

6.2.3 ICチップ不正アクセス手段の解析

(1) 脅威とセキュリティ機能

ICチップの不正アクセス手段による解析に対して防止する必要がある。

(2) 機能要件

(ア) ICチップの自己診断機能の保有すること。

端末との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を保有していること。(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.)

(イ) 特定のデータに対して、ある一定回数以上のアクセスを検知した場合、カードをブロックする機能を保有していること。(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.)

6.2.4 ICチップ誤動作による不正解析(熱、圧力、etc.)

(1) 脅威とセキュリティ機能

ICチップに対して物理的な攻撃を加えることによって、ICチップ内のデータを解析されることを防止する必要がある。

(2) 機能要件

(ア) 電氣的攻撃に対する対策

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

(イ) 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。

6.2.5 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カードの解析及び運用を防止する必要がある。

(2) 機能要件

(ア) ICカードへのトランスファープロテクトを付加すること

初回使用時に指定する鍵(パスワード、etc.)を入力されないと、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。

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竄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.)

(イ) 専用運送会社を確保すること。

(ウ) 出荷納品時に当事者、警備員が立会うこと。

(エ) 管理コードによるプロテクト

製造者管理コードとシリアル番号により、不当な流出があった場合、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。

6.2.6 ICカードの廃棄における要件

(1) 脅威とセキュリティ機能

回収廃棄したICチップ、ICカードの解析や不正使用に対して防止する必要がある。

(2) 機能要件

(ア) ICチップの破壊

ICチップに物理的攻撃を加え、ICチップそのものがしようできないようにすること。

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。

(イ) 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を経過すると運用システム無情で使用できないようにする。

(ウ) 回収廃棄業者の管理

業者の身元確認、及び廃棄の管理を行うこと。(廃棄時に当事者が立ち会う。etc.)

6.3 各種端末機器のセキュリティ機能要件

6.3.1 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
- ・ 機密データ（暗号鍵、各種ID等）の漏洩
- ・ 機器設計者によるセキュリティホールの組み込み
- ・ 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

(ア) 設計者 / 評価者 / 製造者の選択

たとえば、社内的に設計資格 / 評価資格 / 製造資格等の規定を設け、これらの適合者を選択する。特に外部に設計 / 評価または製造を委託する場合は注意のこと。

(イ) 設計場所 / 評価場所 / 製造場所の隔離

設計場所 / 評価場所 / 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。

(ウ) ドキュメント / 機密データ等の管理

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 / 機密データ等の管理を行うこと。（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。

(エ) 設計時の端末機能の検証

端末設計者が、端末機器へセキュリティホールを組み込み、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なうこと。また、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。

(オ) 設計 / 評価時の試作品の管理

試作品の台数管理を確実にしなうこと。また、廃棄は破砕処理後に行なうこと。

(カ) 製造時の機密データの登録方法

端末への機密データ登録は、機密データが直接製造者に見えないようにすること。

(キ) 在庫品等の管理

製造過程での在庫管理を確実にしなうこと。

6.3.2 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）などのため、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。ここでの

端末機器とは、店舗等に設置される電子マネーの決済端末を想定している。

(2) 機能要件

(ア) 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。

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。端末機器の設置時や購入時、特殊な保守操作により端末機器が活性化されない限り、その端末機器はシステム内において正常動作しないような仕組みが必要である。以下に実現例を示す。

- ・システム運用に必須なデータを端末内にダウンロードする。データが機密データの場合は、データ保護（暗号化等）が必要であり、活性化操作者にもデータ内容が見えない方法が望ましい。
- ・認証情報の照合を行う。認証情報とは、あらかじめ端末内に内蔵されかつ活性化操作者のみが知りうるものとする。

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等を端末機器に貼付する方法もある。

(イ) 端末機器の相互認証機能

端末機器の「なりすまし」防止のため、端末機器とその端末機器にアクセスする機器との間で、暗号を用いた相互認証機能が必要となる場合がある。

端末機器 - ICカード

端末機器 - オンラインホスト（インターネット等のオープンネットワークの場合）

端末機器 - オンラインホスト（公衆回線等のクローズドネットワークの場合）

端末機器 - 周辺機器等

6.3.3 端末機器のソフトウェア、機密データの保護

(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では、ICカードとのアクセスや上位機器（オンラインセンタ等）とのアクセス時に、暗号処理やセキュアプロトコル等のセキュリティ技術を使用している。端末機器内には、セキュリティ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）が内蔵されており、これらを悪意の第三者から保護する必要がある。

ここでは端末機器が具備すべきであるタンパープルーフ機能（不正使用されないための仕組み）について述べる。

(2) 機能要件

(ア) プログラム（または機能）のLSI化

ここでは、セキュリティ技術を実現するプログラム（または機能）をハード的に封印（LSI化）し、悪意の第三者からのアクセスを防止することを目的としている。

プログラムのマスク化

1チップCPUの内蔵ROM部にプログラムをマスク化する方法がある。マスク化対象プログラムの優先順位は以下の通り。

- 1)暗号部、ICカードアクセスプロトコル部などのセキュリティ機能部
- 2)OS（リアルタイムモニタ）部
- 3)ハードウェア制御用デバイスドライバ
- 4)端末アプリケーション部

特に、1)については、外部プログラムとの直接的な入出力インタフェースは持たないこと。

プログラムのマスク化（スクランブル機能付き）

上記にプログラム読み出し防止機能が付加されたものを使用する方法がある。

専用LSIの使用

暗号部、ICカードアクセスプロトコル部などのセキュリティ機能部を組み込んだ専用LSIを使用する方法がある。

(イ) 筐体不正開放時の自爆機能

ここでは、筐体の不正開放に対する端末機器の動作例について述べる。

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り、これを検出することによりプログラムや機密データの漏洩を防止する。

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、次項との組み合わせが効果的となる。

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、以降の正常動作を不可能とさせる方法がある。前項との組み合わせが効果的となる。

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。前項との組み合わせが効果的となる。

(ウ) 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。

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。

必須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。

6.3.4 端末機器の流通過程における要件

(1) 脅威とセキュリティの機能

端末機器偽造集団と端末機器製造業者の結託によるICカード型電子マネー端末機器の横流し、機器流通途中での盗難、物理的破壊等が考えられる。

上の脅威に対する対策として、内部の人間の管理、端末に番号を付けることが考えられる。

(2) 機能要件

(ア) 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、牽制機関を設置しなければならない。

(イ) 端末固有番号（製造番号）の管理

仮に、端末が流通途中で横流しにあった場合に、犯罪者を追跡したり、端末輸送前・輸送後の数量チェックをするのに、番号の管理をしなければならない。

(ウ) 輸送手段のセキュリティの確保

輸送ルートに、国道・県道等普段マイカーが通る道を選ばないことも考えられる。

(エ) 端末の不正解放防止機構

端末内のROM等に格納されているプログラムが、不正解放時にストールする機構になっている、あるいは警報が鳴る機構になっているのが望ましい。

(オ) 廃棄端末の厳重な処理

廃棄された端末は、不正利用を防ぐ為にも、内部チップを取り外せる機構になっている必要がある。

(カ) 端末設置場所内に入退室する人間のチェック

端末設置場所入り口に、電気錠・バイOMETRICS本人確認手段（指紋・アイリス・音声等）を設置する必要がある。

(キ) 運搬作業後の作業報告の作成

出発時間・搬入時間、どのルートを通りを通った等、運搬業者は製造業者に対して作業経過を報告することも考えられる。

6.4 発行機関におけるICカードの運用と要件

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。

6.4.1 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おこな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。又、鍵情報の漏洩が行われないうための配慮が必要である。

(2) 機能要件

(ア) ICカード発行体制

本発行手続きを行なう場所、組織体制について以下のような考慮が必要である。

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等。

ICカード発行システムにおけるパソコンの操作予定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なうこと。

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。

ICカード発行部門に対する内部監査を行なえる組織体制とすること。(発行

部門と監査部門の分離)

(イ) 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。

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。)又、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。

各種集計表を作成可能なこと。(日別/月別/店別等)

申込用紙の枚数とのチェックを行ない、余分に発行されていないかの検証を行なう。

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なう等の方法もある。

(ウ) 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。

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。

生成された鍵情報ファイルに対する不正コピーの防止。

----外部への持ち出しを不可能とするためのコピー等の操作に対して、消滅させる等の機能が必要である。

6.4.2 電子マネーの貯蔵機能における要件

(1) 脅威とセキュリティ機能

ICカード上に電子マネーを蓄積する方式のシステムの場合、高額の電子マネーを多数保管することが必要なため、ICカードの盗難、すりかえ等の脅威がある。従って、ICカードの保管にあたっては、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。(本機能はMONDEX等の電子マネーをICカード内に常に保管するシステムの場合に適用される。)

(2) 機能要件

(ア) 金庫による保管(電子金庫の保有)

ICカードの盗難に対処するため、多数のICカードをセットしたものを、金庫内に保管し、施錠管理を行なう。鍵の開閉は厳重なアクセス権限の管理が必要である。

(イ) 電子金庫の保管場所、管理体制等

電子金庫の保管場所は、充分に入退室が管理された場所とし、あらかじめ登録された者のみが可能となるようにする。又、管理責任者は複数の部門による相互牽制が行われることが必要である。

(ウ) 電子金庫内の各ICカードの状態監視機能

電子金庫内にセットされたすべてのICカードの状態をシステムで監視し、本来あるべきICカードかどうかを常に認識できる機能をもつ必要がある。

(エ) 電子マネーの発行量の把握

電子金庫のすべてのICカードの発行、回収の履歴を管理することが必要である。

(オ) 各ＩＣカードの相互認証機能

不当なアクセスを防止するため、本ＩＣカードと外部のノードとの相互認証機能を保有することが必要である。

(カ) 金庫用ＩＣカード盗難対策

金庫用カードを盗んでも一般のカードとして使用できないように金庫用としてのＩＤを保有し、一般の決済時には使用不可能とすることが必要である。

6.4.3 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。又、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

(ア) 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内に期限情報を設定することが考えられる)

(イ) 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望ましい。

(ウ) 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等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。)

(エ) 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。

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カードのリーダー・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。)

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ます。

6.4.4 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望ましい。

(2) 機能要件

(ア) 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。

(イ) 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)

(ウ) 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カード発行時点で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を設定をもつことも考えられる。

6.5 電子マネーの価値移転時のセキュリティ機能要件

6.5.1 不正な電子マネー引き出しの防止

(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、顧客口座から電子マネーを補充する時点において次のような脅威がある。

- 不正(盗難、変造、偽造)ICカードによる電子マネー引き出し
- 不正(盗難、変造、偽造)端末による電子マネー引き出し
- 不正に顧客口座情報やPIN等を取得することによる電子マネー引き出し

これらの脅威に対して、顧客口座の本人確認機能や、ICカードと端末およびホストのそれぞれの間での相互認証機能、並びに、ICカードや端末の盗難、変造、偽造対策、また、取り引きログ採取等の責任追及対策を考慮する等の対策が必要である。

(2) 機能要件

(ア) 顧客口座の本人確認機能

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確認機能を持たなければならない。

- PIN(暗証番号)による本人確認
 - バイオメトリック情報(指紋、虹彩、声紋等の生体情報)による本人確認
- 不正な本人確認入力を制限するために、失敗入力ロギング機能や回数制限等を行うことが望ましい。

(イ) ICカード、端末、ホストそれぞれの間での相互認証機能

それぞれの機器自体や処理の真正性を確認するために、相互認証を行うことが望ましい。

不正な相互認証処理を制限するために認証失敗などのロギング機能や回数制限を行うことが望ましい。

(ウ) 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、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り引きの都度参照して不正な IC カードの使用を防ぐことが望ましい。

(エ) 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が望ましい。

端末持ち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
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

(オ) 責任追及のための証拠機能

不正な処理が行われた、あるいは正常に処理が完結したことを検証するために
処理ログ等の取引証拠を IC カード、端末機器、ホストのそれぞれに格納する
ことが望ましい。

ログ自体の改ざんなどを防ぐためデジタル署名等を行う方法もある。

6.5.2 電子マネーの転送経路のセキュリティ機能要件

(1) 脅威とセキュリティ機能

電子マネー転送時において転送路に侵入・分岐するなどの次のような脅威がある。

- 転送路への侵入・分岐や転送路分岐先でのモニタリング
- モニタリングによるセンシティブデータ（暗号鍵、PIN など）分析やコマンド / レスポンス分析、フロー分析、プロトコル分析等
- 転送路分岐先でのデータ改ざんや転送路分岐先でのなりすまし

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
- 転送セッション・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

(ア) 転送路の機密性・完全性の確保

転送路の機密性や完全性を確保するために次のような対策を行う方法がある。

- 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

(イ) 転送データやセッションの真正性の確保

データの改ざんや成りすまし等を防ぐため、データにメッセージ認証子やデジタル署名の付加を行う方法がある。

セッションの改ざんや成りすまし等を防ぐため、データにメッセージ認証子やデジタル署名の付加を行う方法がある。

(ウ) 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了したことを検証するためにログなどの取り引き証拠をICカードや端末機器、ホストのそれぞれに格納することが望ましい。

ログ自体の改ざんなどを防ぐためデジタル署名などを行う方法がある。

6.5.3 電子マネーの価値移転時のエラー

(1) 脅威とセキュリティ機能

電子マネーの価値移転時のエラーによる取り引き中断・回復処理の不整合を利用した不当な請求や加盟店・顧客への不利益等の脅威に対し次の対策を行うことが必要である。

- 処理の可用性 (Availability) 確保
- 処理中断・回復状態の完全性

(2) 機能要件

(ア) 処理の可用性確保

取り引き中断を可能な限り回避するためには、次のような対策が望ましい。

- 転送路の二重化 (専用線の場合)
- 処理・バッファの二重化
- 処理・進行状態チェックと回復処理
- 未決済ログ、回復ログ等

(イ) 処理中断・回復状態の完全性

取り引き途中での中断からの回復処理のために取り引き状態を示す情報を相互で保持することが望ましい。

取り引き中断・回復状態の情報に対する改ざんなどを防ぐためにデータへの認証子やデジタル署名の付加等の方法がある。

6.5.4 価値移転後の否認防止

(1) 脅威とセキュリティ機能

価値移転後のその事実の否認に対する脅威に対し、取り引きの完全性を確保し、その取り引き証拠を保存することにより取り引きの事実を追跡・証明できることが必要である。

(2) 機能要件

(ア) 責任追及のための証拠保存

取り引き事実の追跡・証明等の責任追及性を確保するために処理ログの採取と保管を行う方法がある。

さらにログデータに対しデジタル署名を付加するなどの方法がある。

6.5.5 価値移転時の機器障害時のセキュリティ機能要件

(1) 脅威とセキュリティ機能

価値移転時に機器障害を起こし、不当な請求を行う、または、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り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

(ア) 機器の可用性の確保

機器障害を最小限にとどめるために、障害検出機能が必要である。

障害検出後リカバリー稼動またはリカバリーのためのデータを保存する等の方法がある。

障害からの復旧に際し、障害事前状態への回復と回復したことを示すログを保存する等の方法がある。

(イ) 取り引き正当性確認手段の確保

取り引きの中断や完了状態を機器相互間で保持、さらにその状態データに対しメッセージ認証子やデジタル署名を付加することにより取り引きの成立・不成立の正当性を確保する等の方法がある。

6.5.6 電子マネーの金融機関システムへの転送時のセキュリティ機能要件

(1) 脅威とセキュリティ機能

金融機関ホストへのなりすましによる加盟店からの不当な価値回収等の脅威に対して、成りすまし防止等の対策が必要である。

(2) 機能要件

(ア) ホストへのなりすまし防止

ホストに成りすますことで正当な加盟店から不当に価値を回収することを防ぐために次のような対策がある。

接続時の相手相互確認

転送チャネルの暗号化・認証

(イ) 価値回収の使用権の制御

不正なホストで不当に回収された価値が、転用・再使用できないように加盟店からの価値回収時点において端末機器で再使用できないように価値情報を加工した後ホストに送信する等の方法がある。例えば、価値回収時点で、使用済み情報と加盟店署名を合わせてメッセージ認証子あるいはデジタル署名を付加する等。

6.5.7 加盟店での決済時点におけるセキュリティ機能要件

(1) 脅威とセキュリティ機能

加盟店での決済時点においては、次のような脅威がある。

- 不正なカードによる決済
- 不正な端末による不当な電子マネーの搾取
- 電子的に価値移転が行われることにより目視確認ができないために起こる当事者の故意や過失による誤った決済

これらの脅威に対して次のような対策を行う必要がある。

- ICカードや端末の真正性や有効性の確認
- 決済金額の確認

(2) 機能要件

(ア) ICカードや端末の真正性や有効性の確認

ICカードや端末の真正性の確認

ICカードと端末間、または、ICカードとホスト間による相互認証を行うことによりICカードの真正性を確認することが望ましい。

ICカードや端末の有効性の確認

ICカードや端末の有効性を確認するため、ブラックリスト若しくはホワイトリストを端末（対ICカード）またはホスト（対ICカード及び端末）に持ち、決済の都度参照して無効カードの使用を防ぐ方法がある。

(イ) 決済金額の確認

電子マネーを支払う側及受け取り側の双方において取り引き金額を目視確認できる仕組みとするべきである。

取り引き後に電子マネーを支払う側が電子マネーを受け取る側の見ている前で支払前と支払後の残高を残高表示器で確認する方法がある。

6.5.8 加盟店での運用上におけるセキュリティ機能要件

(1) 脅威とセキュリティ機能

加盟店での運用において、店員による不正（横領など）に対する脅威がある。

この脅威に対し電子マネー保管機等の管理を行うなどの不正対策が必要である。

(2) 機能要件

(ア) 電子マネー保管機材の物理的隔離

加盟店端末の近傍など店員が容易に取り扱えるところに電子マネー保管機材を置かないなど、物理的に隔離することで売上金（電子マネー）を管理する方法がある。

(イ) 加盟店ICカードの操作制限

加盟店端末用のICカードに尾員PIN（暗証番号）などを設け、特定者のみが電子マネーの管理が行えるようにする方法がある。

加盟店端末用のICカードのか価値移転先を、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。

6.6 消費者保護について

6.6.1 消費者のプライバシー対策（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、誰がいつどこ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、金融機関などに不当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に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。

(2) 機能要件

(ア) 取引履歴情報の最少化

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。

保管期限などについても規定を設けることが望ましい。

(イ) 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とが望ましい。

(ウ) 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。

通信路においても同様とする。

これにより、上記(イ)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できる。

6.6.2 ICカードの盗難・紛失対策

(1) 脅威とセキュリティ機能

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) 機能要件

(ア) ロック機能

消費者にICカードに加えウォレット等の機器を配布し、ICカードにロックをかける機能を提供することが考えられる。

(イ) 小売店におけるパスワードチェック機能

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。

(ウ) 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。

(エ) 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。

事故届けのあったカードの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。

7 ICカード型電子マネー検討メンバー(敬称略、順不同)

五味 俊夫 (主査)	電子商取引実証推進協議会
辻 秀一 (副主査)	電子商取引実証推進協議会
菅 知之 (副主査)	電子商取引実証推進協議会
米倉 昭利 (副主査)	電子商取引実証推進協議会
中山 要治郎 (リーダー)	沖電気工業(株)
甲斐 貴章 (サブリーダー)	日本電気(株)
須賀 秀徳 (サブリーダー)	松下電器産業(株)
勝田 進	アンリツ(株)
相川 博治	(株)コンテック
山口 卓	シーメンス(株)
井阪 智	昌栄印刷(株)
和泉 豪信	(財)情報処理相互運用技術協会
有吉 一彦	(株)住友クレジットサービス
谷 一郎	(株)ゼクセルインテリジェンス
鬼頭 俊貴	総合警備保障(株)
村谷 博文	(株)デザイン・ビジョン・ラボラトリーズ
五十嵐 善之	(株)デンソー
河合 泰彦	(株)東芝
青島 賢明	(株)土木情報サービス
大沼 武彦	三菱商事(株)

第 2 部

インターネット利用クレジット決済システムのセキュリティ機能

平成 9 年 5 月

共通セキュリティ関連技術WG

目 次

1 研究の目的	1
---------------	---

2 既存のセキュリティ基準との関係	2
2.1 既存のセキュリティ基準	2
2.2 セキュリティ・メジャー（仮称）	2
3 メジャーの研究手順	3
4 対象モデルの設定	4
5 脅威とセキュリティ機能	6
6 インターネット利用クレジット決済検討メンバー（敬称略、順不同）	14
参考資料 SET 概説	

1 研究の目的

電子商取引の中で、インターネット利用のクレジット決済システムが電子マネーと並んで、日米で最も早く実用化されようとしている。企業 - 消費者間 EC の通産実証実験において実システムを構築する 14 のプロジェクトのうち 10 プロジェクトが、インターネットを利用したクレジット決済を行なう予定である。

しかし、インターネットを利用してクレジット決済を行なうことについてはセキュリティ面で、問題がないか、必ず論議の焦点となる。

従来のセキュアプロトコルに加え本年 5 月には、SET (Secure Electronic Transaction Protocol) の正式な Version 1 が制定されようとしているが、セキュリティ機能の実実は、当然コストの上昇につながるものであり、システムの対象とする消費者の規模、取扱商品、取引額の上限 (1 回毎、月毎の限度額) によって、各種のセキュリティ機能が選択されていくと予想される。

ECOM として、論議を尽くした上で、次の目的で、インターネット利用クレジット決済システムのセキュリティメジャー (仮称) を研究することになった。

セキュリティメジャー (仮称) の内容と目的

システムのセキュリティ設計の責任者が、多様な角度から見たセキュリティ機能と、機能レベルについて、自己評価できる仕掛けを作る。

評価リストと評価手引き書によって、責任者が自己評価すれば第三者が客観的にシステムの機能評価ができるようにする。この様な仕掛けがないと、責任者にセキュリティ機能の表示を求めた時、表示すべき機能の有無や、レベルが表現されなかったり、機能表示ではなくて、機能を実現する為の詳細な仕様説明になったりして不便である。

セキュリティメジャー (仮称) の適用例

システム事業者とシステムインテグレータとの間でセキュリティ機能の確認を行なう際に、インテグレータ側が、このメジャーに基づく評価結果を提示すれば、事業者から見てシステムの評価あるいは複数のインテグレータの比較が容易となる。

今後、多くのシステムの建設が行なわれる中で、この様なメジャーがあれば、活用される機会が多いと予想される。

2

既存のセキュリティ基準との関係

2.1 既存のセキュリティ基準

セキュリティ基準は図2 - 1に示す課程を経て制定されてきたオレンジブックとして知られているTCSEC (Trusted Computer Security Evaluation Criteria) が米国の国防総省で作成されたのが初めである。

現在も連邦政府の調達条件の一つに用いられている。

FC (Federal Criteria - IT Security) は政府非軍事部門や民間商用システムでのニーズに対応して制定されるものである。

ヨーロッパやカナダの同様な Criteria との統合、標準化が政府協議に基づいて進められCC (Common Criteria) が制定された。この調整結果が、ISOのWGに入力され、正式なISOの基準となる。

これらのCriteriaは主としてスタンドアロンのシステムを対象としたセキュリティ基準である。

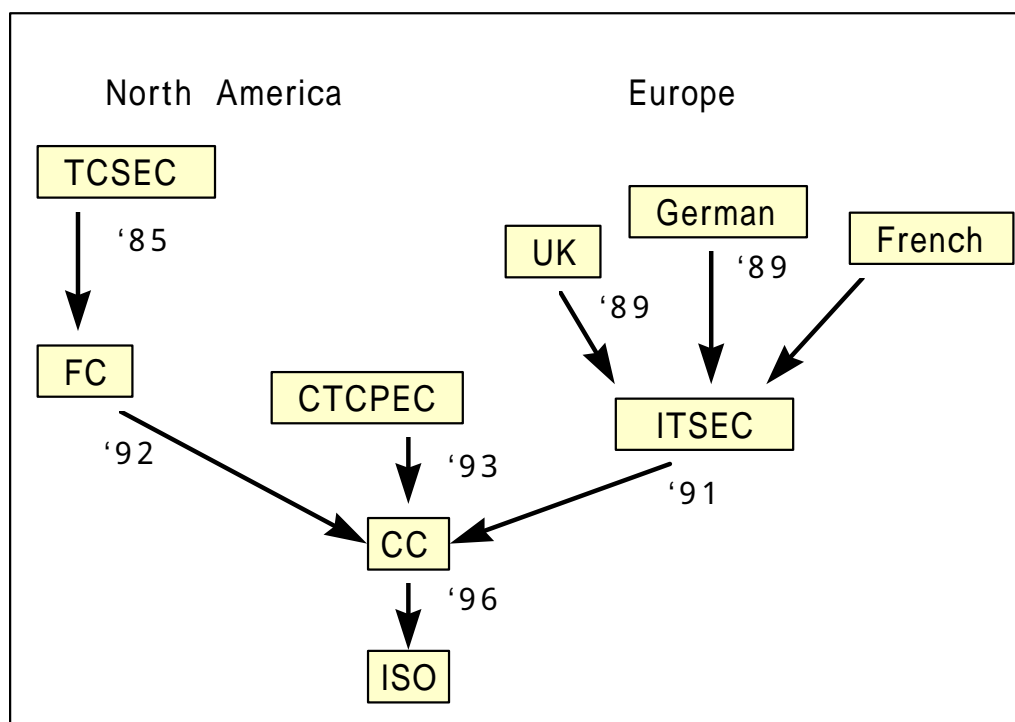


図2 - 1 Historical View of Evaluation Criteria

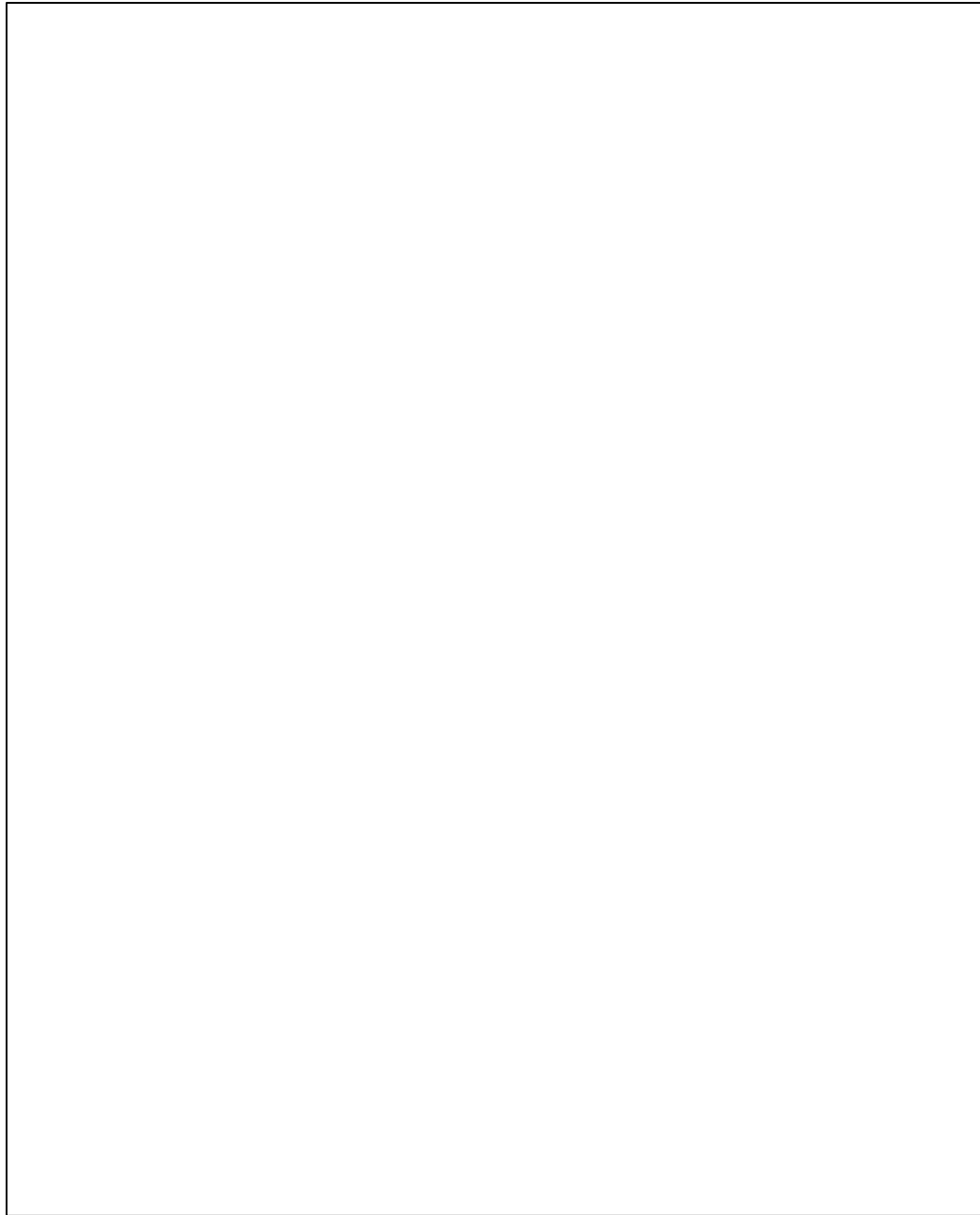
2.2 セキュリティ・メジャー（仮称）

対象モデルのノードとしては、カード会社の運営するノードも含まれるが、センターとしてのセキュリティ・メジャーは2.1の既存のCriteriaで規定されている。

ここではインターネット上のプロセスを中心としたセキュリティ機能についてメジャーの研究を行なう。

3 メジャーの研究手順

以下の手順でメジャー研究を行なっている。



現在ステップ3のセキュリティ機能の整理の段階であり、セキュリティ機能レベルを明確にして、メジャー原案を作成する。実証実験のうち10プロジェクトでクレジット決済を行なう為、セキュリティ責任者にメジャーを適用した自己評価を試みて頂き、このレビュー結果をフィードバックしてセキュリティ・メジャーを作成する。本年9月に正式なセキュリティ・メジャーを公表する予定である。

4 対象モデルの設定

研究対象とするインターネット上のクレジット決済のモデルを設定し、ノード間伝送情報、ノード内に蓄積される情報を明確にした。

モデルはSETに基づいているが、セキュリティ機能の整理とレベル分けの段階で他のセキュアプロトコルや、パスワード・ユーザID使用システムなども視野に入れて検討を行ない、適用範囲の広いメジャーを研究する。

インターネット上のクレジット決済は図 4-1 のようになる。

ノード間の情報、ノードに蓄積される情報を明確にすると図 4-2 のようになる。

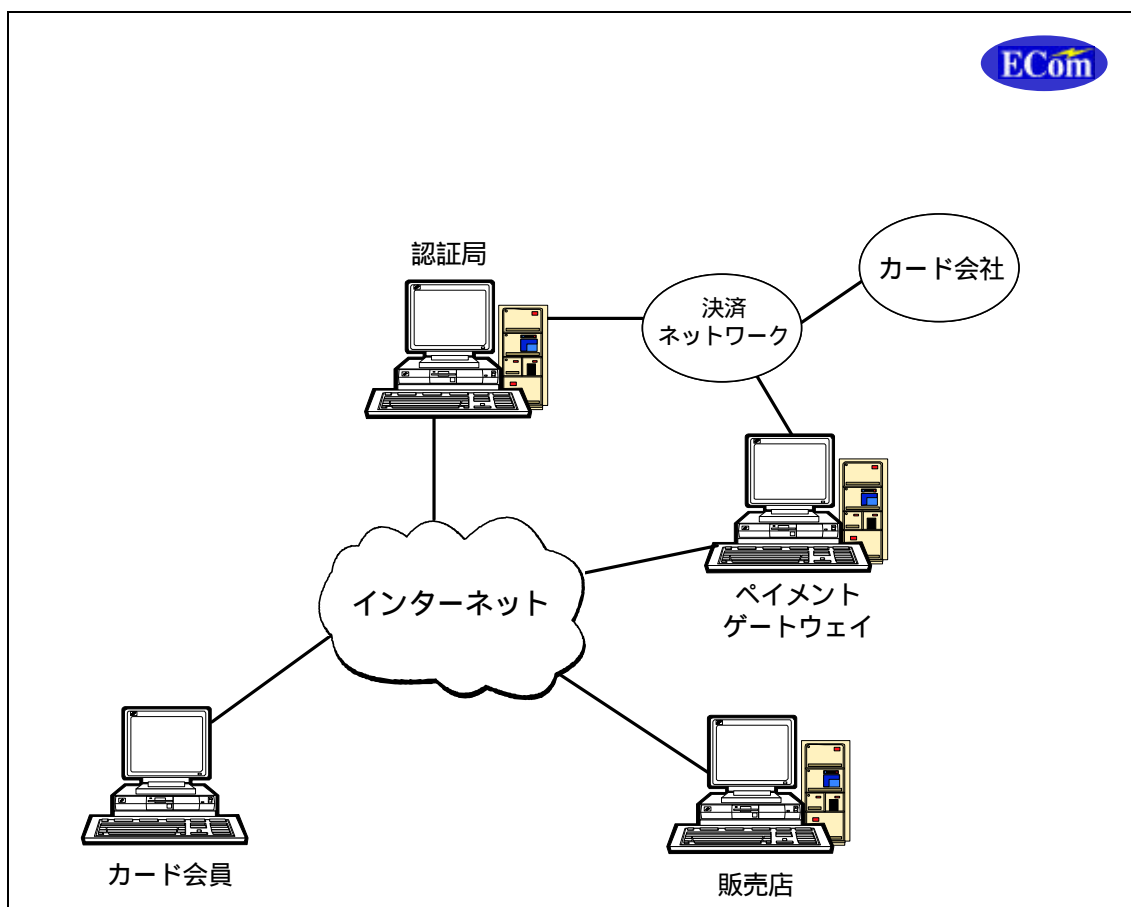
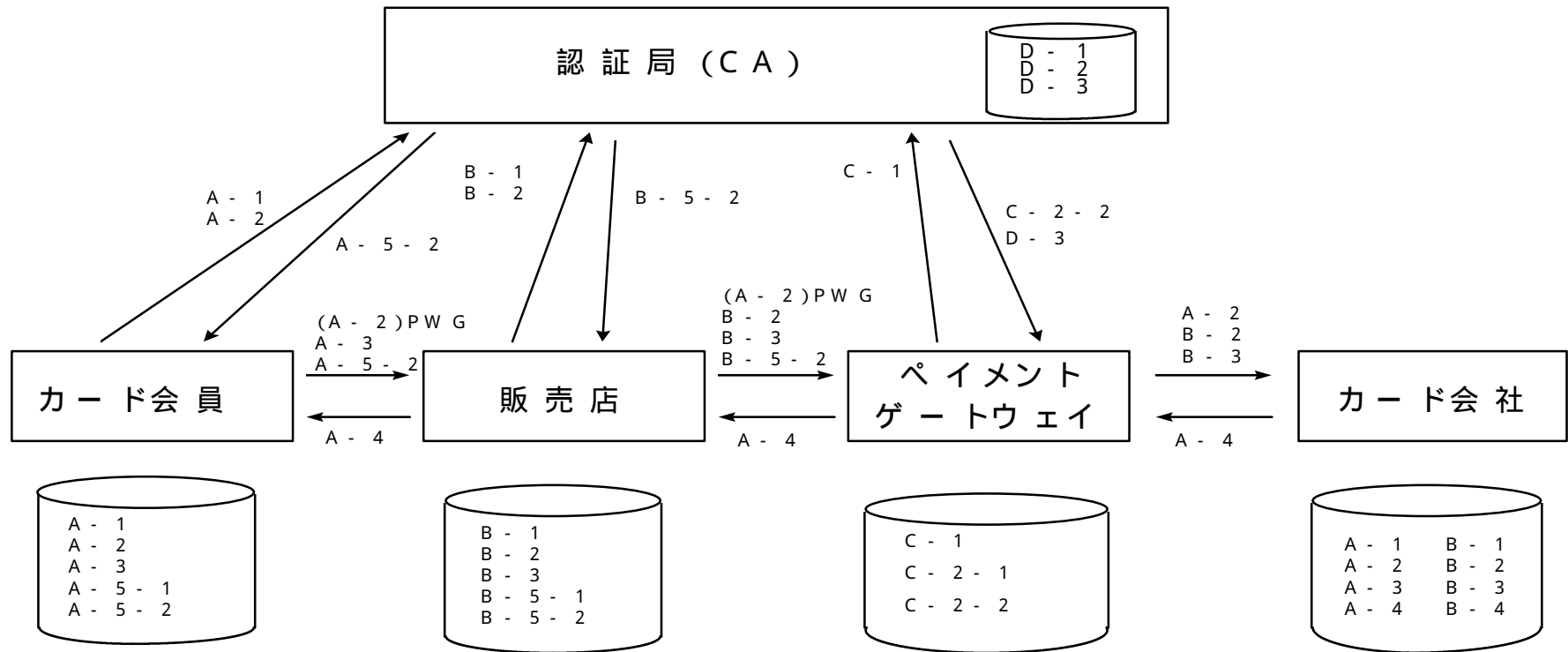


図 4-1 インターネット利用のクレジット決済



- | | |
|--|--|
| <p>A . 個人情報</p> <ol style="list-style-type: none"> 1. 属性情報 (氏名、家族構成、生年月日、住所、TEL、職業、資産 (年収持家)、性別、国籍) 2. クレジット (、有効期限、限度額) 3. 購入情報 (品名、店、金額) 4. 支払情報 (引落とし状況) : クレジット会社が持つ情報 B / W) 5. KEY (秘密鍵、個人証明書) <p>B . 加盟情報</p> <ol style="list-style-type: none"> 6. 属性情報 (住所、TEL、資本金...) 7. 加盟店番号 8. 販売情報 (品名、客、金額) 9. 決済情報 (事故履歴) 10. KEY (秘密鍵、証明書) | <p>C . PG / W の情報</p> <ol style="list-style-type: none"> 1. 属性 (IPアドレス、機種、管理者名...) 2. KEY (秘密鍵、自分の証明書) <p>D . CA 情報</p> <ol style="list-style-type: none"> 3. 属性 (CA の階層レベル...) 4. KEY (秘密鍵、自分の証明書) 5. 証明証情報 (発行履歴)、事故情報 CRL (CA Revocation List。盗難届が出たときに、PG / W に伝える) |
|--|--|

5 脅威とセキュリティ機能

ノードとノード間に発生する可能性のある脅威の洗い出しと整理を行なった。

脅威は、誰が、なにを目的に行動するのか具体的に記述することとした。

ここでは、インターネット上の取引のために発生する脅威のみに絞っておりインターネットでなくても発生する脅威は除いてある。(例えば、他人名義のカードを申請し、そのカードでインターネット登録し、物品を購入するケースなど)

次に脅威を防ぐための技術的なセキュリティ機能の洗い出しを行なった。

結果を表 5-1～7 に示す。

ハード、ソフトの機能ではなく、管理、運用面での対策が必要と考えられるものは、備考に記した。

今回は中間報告であり、3章の研究手順のステップ3として今後、次の検討を行なう予定である。

1. SSL、パスワード方式など、SET以外の対称モデルを明確にし、セキュリティ機能を詰める。
2. 秘密鍵が盗まれた場合、影響が大きいのので別に取り上げて検討する。
3. デジタル商品のケースは、配送証明がないので配慮が必要であり、別に取り上げる。
4. 販売店とカード会員が結託したケースを検討する。

ステップ6までの研究成果を、本年9月に公表する予定である。

表5 - 1

攻撃対象	概要	who (誰が)	when (いつ)	where (どこで)	what (何を)	why (なぜ)	how (どんな方法で)	セキュリティ向上の為の機能	備考
カード会員	端末(PC)からの個人情報の漏洩	悪意の第三者	-	カード会員宅	個人情報	入手した情報を利用するため	無許可での端末操作、盗難された端末内のデータ解析	端末の不正使用防止機能 個人情報の保護機能(暗号化、端末との分離、不正使用によるデータの破壊、等)	ユーザ教育
カード会員	キーボード操作からパスワード推測	悪意の第三者	キー操作中	カード会員宅	個人情報	入手した情報を利用するため	キー操作中に背後またはキーインの音で推測	パスワードの複雑化(予測不可にする) パスワードの強制変更機能、ICカード化	ユーザ教育
カード会員	会員端末から情報を搾取	悪意の第三者	-	カード会員宅	会員端末に保存している情報	入手した情報を利用するため	端末修理時。 ネットワーク経由で侵入	端末の不正使用防止機能 個人情報の保護機能(暗号化、端末との分離)	
カード会員	代金の詐取	悪意の販売店	取引成立後	-	-	代金の詐取	デジタル商品を送らない	検討中	デジタル商品再送の義務付け
カード会員	情報悪用	悪意の販売店	-	-	個人情報	個人情報の悪用	-	購入情報と支払情報の分離	
カード会員	代金の詐取	悪意の販売店	-	-	-	代金の詐取	請求額の水増し	購入情報と支払情報の分離 支払情報への会員のデジタル署名	
カード会員	偽ソフトの使用による情報の漏洩	悪意の第三者	取引等の通信時	-	-	個人情報の悪用	偽の通信ソフトの使用により、盗難される。(アクセス先を変更等)	ダウンロード元の確認 個人情報の保護機能(暗号化、端末との分離)FD郵送	ユーザ教育
カード会員	実在する販売店へのなりすましによる個人情報取得	悪意の第三者	取引等の通信時	-	-	個人情報の取得により物品を詐取	実在する販売店の類似モール作成	CAによる販売店証明機能	カード会員への啓もう
カード会員	CAへのなりすましによる個人情報取得	悪意の第三者	取引等の通信時	-	-	個人情報の取得により物品を詐取	類似webの作成	上位CAによるCA証明機能 CAアドレス等の公表	カード会員への啓もう
カード会員	トラブル等によりデジタルが届かないのに支払の請求	善意の販売店	送信時	-	-	-	通信時のトラブル	再送機能 販売店の送信ログ管理	

表5 - 2

	攻撃対象	概要	who (誰が)	when (いつ)	where (どこで)	what (何を)	why (なぜ)	how (どんな方法で)	セキュリティ向上の為の機能	備考
	販売店	コンテンツ改ざん	悪意の第三者	-	販売店のサーバー	商店の保持している売上データ	いたずら(業務妨害)	発信情報(コンテンツ)を改ざんすることによって	アクセス制御機能	
	販売店	情報の不正取得	悪意の第三者	-	販売店のサーバー	商店の保持している売上データ	顧客情報を盗むため	ファイアウォールを破って	アクセス制御機能	
	販売店	支払を拒否	悪意の第三者	支払時	-	-	物品を搾取するため	物品を受け取ったのに受け取っていないと支払を拒否	否認防止機能(購入意思確認、ログ所得、個人認証、契約書、等) (デジタル商品は解約不能?)	
	販売店	ハイトラフィック攻撃	悪意の第三者	-	-	-	取引の妨害	ハイトラフィック攻撃	検討中	
	販売店	実在する会員へのなりすまし	悪意の第三者	-	-	-	品物の詐取	リトライによるカード会員番号の取得	CAによる会員証明機能	

表5 - 3

	攻撃対象	概要	who (誰が)	when (いつ)	where (どこで)	what (何を)	why (なぜ)	how (どんな方法で)	セキュリティ向上の為の機能	備考
	カード会員～ 販売店	盗聴	ネットワーク 上の悪意の第 3者	取引等の 通信中	ユーザネット ワーク、プロ バイダ内	ネットワー ク上を伝送 される取引 データ	個人情報、取引データ の入手	中継機器でのタッピング、中継 機器への盗聴機能組み	暗号化機能	
	カード会員～ 販売店	盗聴データを改ざ んし取引内容を変 更	ネットワーク 上の悪意の第 3者	データ伝 送中	ユーザネット ワーク、プロ バイダ内	カード番 号、個人情 報、購入品 目等	いやがらせ	ネットワーク上をアナライザ 等でモニタ	暗号化機能(デジタル署名)	
	カード会員～ 販売店	リピート攻撃	ネットワーク 上の悪意の第 3者	取引等の 通信中	ユーザネット ワーク、プロ バイダ内	ネットワー ク上を伝送 される取引 データ	商店に対しリピート 攻撃を行うため	盗聴した取引データをそのま まりピート送信することによ り	通番管理、タイムスタンプ	
	カード会員～ 販売店	データ廃棄	ネットワーク 上の悪意の第 3者	取引等の 通信中	ユーザネット ワーク、プロ バイダ内	ネットワー ク上を伝送 される取引 データ	取引の妨害	データ廃棄	暗号化機能 再送機能	

表5 - 4

	攻撃対象	概要	who (誰が)	when (いつ)	where (どこで)	what (何を)	why (なぜ)	how (どんな方法で)	セキュリティ向上の為の機能	備考
	P G / W	情報の不正取得	悪意の第三者	-	P G / W	-	情報の不正取得	ファイアウォールをやぶって	アクセス制御機能	
	P G / W	情報の改ざん	悪意の第三者	-	P G / W	-	情報の改ざん	侵入後不正アクセスと改ざん	アクセス制御機能	
	P G / W	通信上のトラブル	-	-	-	-	-	通信時のトラブルによる	再送機能	
	P G / W	ハイトラフィック攻撃	悪意の第三者	-	-	-	取引の妨害	ハイトラフィック攻撃	検討中	

表5 - 5

	攻撃対象	概要	who (誰が)	when (いつ)	where (どこで)	what (何を)	why (なぜ)	how (どんな方法で)	セキュリティ向上の為の機能	備考
	C A	情報の不正取得	悪意の第三者	-	C A	-	情報の不正取得	ファイアウォールをやぶって	アクセス制御機能	
	C A	情報の改ざん	悪意の第三者	-	C A	-	情報の改ざん	侵入後不正アクセスと改ざん	アクセス制御機能	
	C A	通信上のトラブル	-	-	-	-	-	通信時のトラブルによる	再送機能	
	C A	ハイトラフィック攻撃	悪意の第三者	-	-	-	取引の妨害	ハイトラフィック攻撃	検討中	

表5 - 6

	攻撃対象	概要	who (誰が)	when (いつ)	where (どこで)	what (何を)	why (なぜ)	how (どんな方法で)	セキュリティ向上の為の機能	備考
	カード会員～ C A	盗聴	ネットワーク上の悪意の第三者	取引等の通信中	ユーザネットワーク、プロバイダ内	カード番号、個人情報、証明書等	個人情報、取引データの入手	中継機器でのタッピング、中継機器への盗聴機能組込み	暗号化機能	
	カード会員～ C A	盗聴データを改ざんし内容を変更	ネットワーク上の悪意の第三者	データ伝送中	ユーザネットワーク、プロバイダ内	カード番号、個人情報、証明書等	いやがらせ	ネットワーク上をアナライザ等でモニタ	暗号化機能(デジタル署名)	
	カード会員～ C A	リポート攻撃	ネットワーク上の悪意の第三者	取引等の通信中	ユーザネットワーク、プロバイダ内	ネットワーク上を伝送される取引データ	C Aに対しリポート攻撃を行うため	盗聴した取引データをそのままリポート送信することにより	通信管理、タイムスタンプ	
	カード会員～ C A	データ廃棄	ネットワーク上の悪意の第三者	取引等の通信中	ユーザネットワーク、プロバイダ内	ネットワーク上を伝送される取引データ	登録の妨害	データ廃棄	暗号化機能 再送機能	

表5 - 7

	攻撃対象	概要	who (誰が)	when (いつ)	where (どこで)	what (何を)	why (なぜ)	how (どんな方法で)	セキュリティ向上の為の機能	備考
	販売店～ C A	盗聴	ネットワーク上の悪意の第三者	取引等の通信中	ユーザネットワーク、プロバイダ内	販売店情報、証明書	販売店情報、取引データの入手	中継機器でのタッピング、中継機器への盗聴機能組込みに	暗号化機能	
	販売店～ C A	盗聴データを改ざんし取引内容を変更	ネットワーク上の悪意の第三者	データ伝送中	ユーザネットワーク、プロバイダ内	販売店情報、証明書	いやがらせ	ネットワーク上をアナライザ等でモニタ	暗号化機能(デジタル署名)	
	販売店～ C A	リピート攻撃	ネットワーク上の悪意の第三者	取引等の通信中	ユーザネットワーク、プロバイダ内	ネットワーク上を伝送される取引データ	C A / 販売店に対しリピート攻撃を行うため	盗聴した取引データをそのままリピート送信することにより	通信管理、タイムスタンプ	
	販売店～ C A	データ廃棄	ネットワーク上の悪意の第三者	取引等の通信中	ユーザネットワーク、プロバイダ内	ネットワーク上を伝送される取引データ	登録の妨害	データ廃棄	暗号化機能 再送機能	

6 インターネット利用クレジット決済検討メンバー(敬称略、順不同)

五味俊夫	(主査)	電子商取引実証推進協議会
辻秀一	(副主査)	電子商取引実証推進協議会
菅知之	(副主査)	電子商取引実証推進協議会
米倉昭利	(副主査)	電子商取引実証推進協議会
堀越繁明	(リーダー)	日本ユニシス(株)
中村逸一	(サブリーダー)	NTTデータ通信(株)
天野大緑	(サブリーダー)	富士通(株)
佐藤哲朗		(株)アドバンス
石井大輔		(株)オリエントコーポレーション
春本昌宏		共同印刷(株)
岡田健司		東京海上火災保険(株)
三ツ堀啓		東電ソフトウェア(株)
橋本仁		(株)東洋情報システム
濱谷卓美		凸版印刷(株)
沼尾雅之		日本アイ・ビー・エム(株)
中沢均		富士通エフ・アイ・ピー(株)
吉川義幸		マスターカード・インターナショナル・ジャパン・インク
新保尚二		(株)名鉄コンピュータサービス

参考資料

SET概説

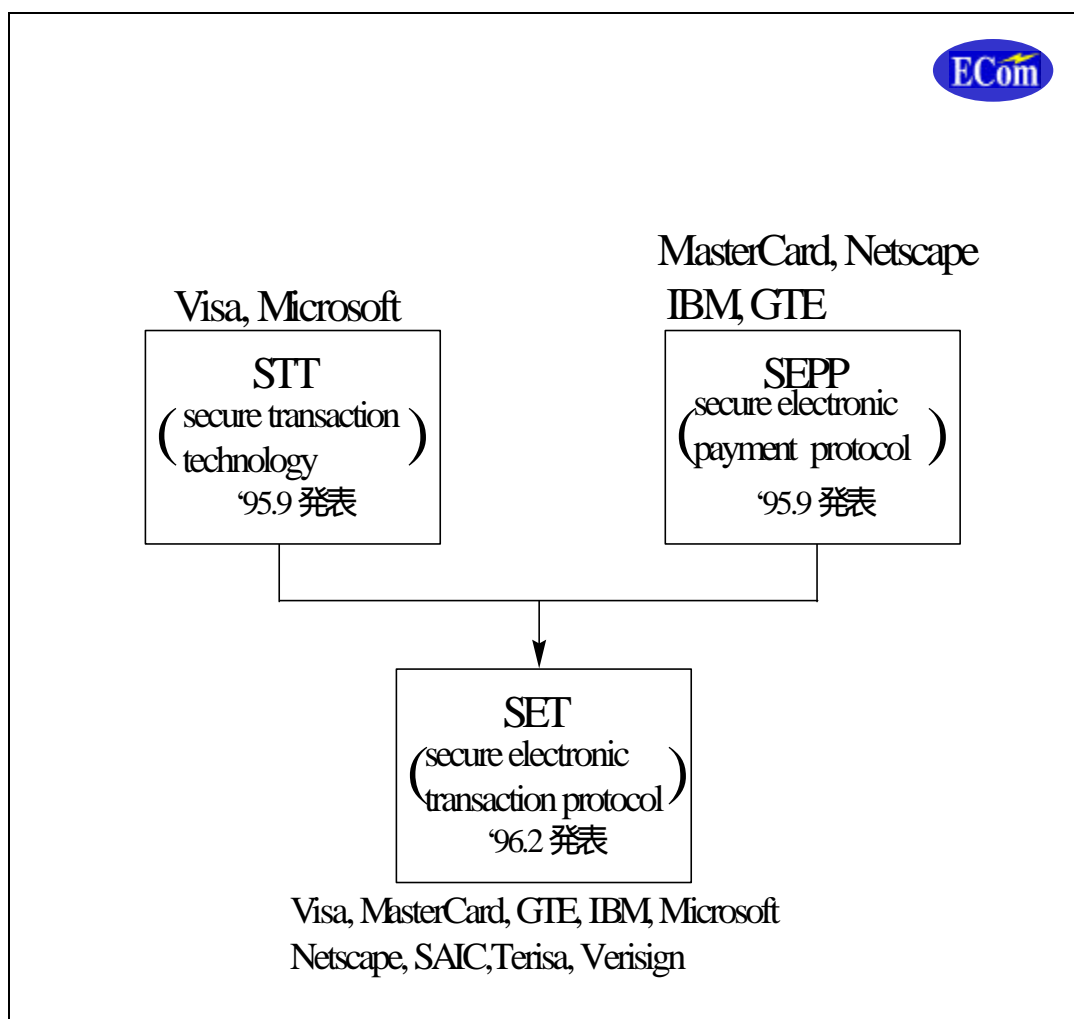


図-1 クレジット決済プロトコル(SET開発の経緯)

1. クレジット決済プロトコル(SET開発の経緯) 図-1 参照

SETのプロトコルは、大きくシェアを持っているVisaカードとMasterCardが、95年の初めから共同で仕様をつくらないと普及しないということで合意していたが、いろいろ経緯があって、9月にそれぞれがセキュアなプロトコルを発表した。しかし、やはり原点に戻らなければいけないということで、1996年の2月に、双方が合意の上でVisa、MasterCardが中心となり、VeriSign、GTEといった認証局ビジネスをやっている企業、IBMなどのコンピュータメーカーと協力して、クレジット決済するための安全なプロトコルの試案を発表し、この後、6月に改定されている。1997年5月に正式なバージョンが公表される。セキュア・プロトコルというのはSETだけではなく、世の中に多くある

が、実証プロジェクトが多く使用しているため、我々の研究の中心になっている。

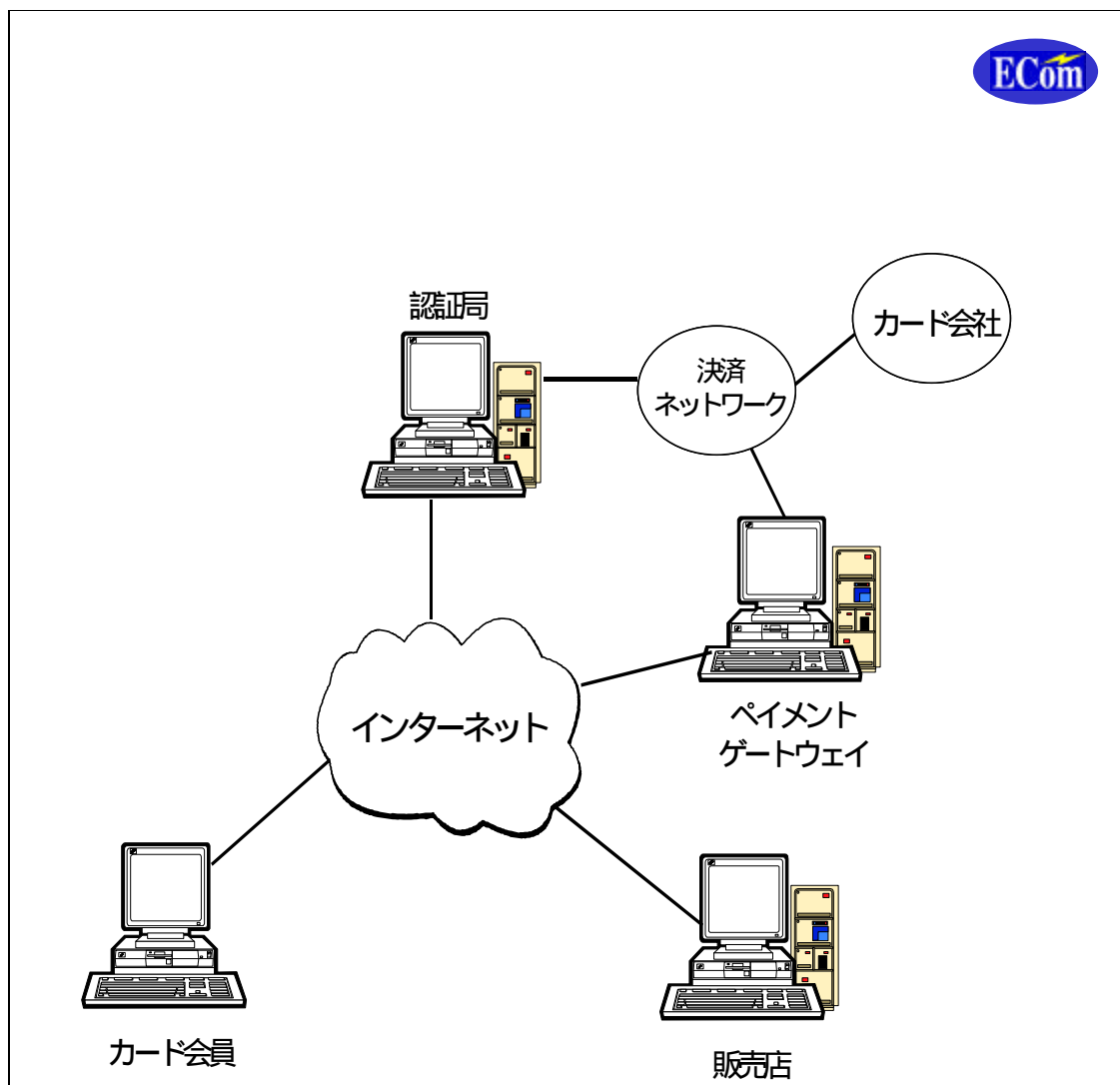


図-2 インターネット利用のクレジット決済

2. インターネット利用のクレジット決済 図-2 参照

オープンなネットワークというのがポイントであり、オープンだからこそ誰でもこれに加入すればアクセスできるかわりに、この中にはいろいろなゲートウェイを経由していくため、自分が見られるかわりに他人も見ることができる。情報の盗聴、改竄などの可能性がある。便利な反面、そういう性質のあるインターネットというものの上に、これに加入したカード会員が販売店の品物を見て、見るだけではセキュリティとは関係ないが、購入を決意して、かつ、インターネット上でクレジットカードで決済したい、支払い指示を出したいということが一番の課題になる。一般にクレジット決済の場合、カード会員、販売店双方を認証する認証局、カード会社とつながった決済ネットワークに接続するための支払いゲートウェイというものが使われる。

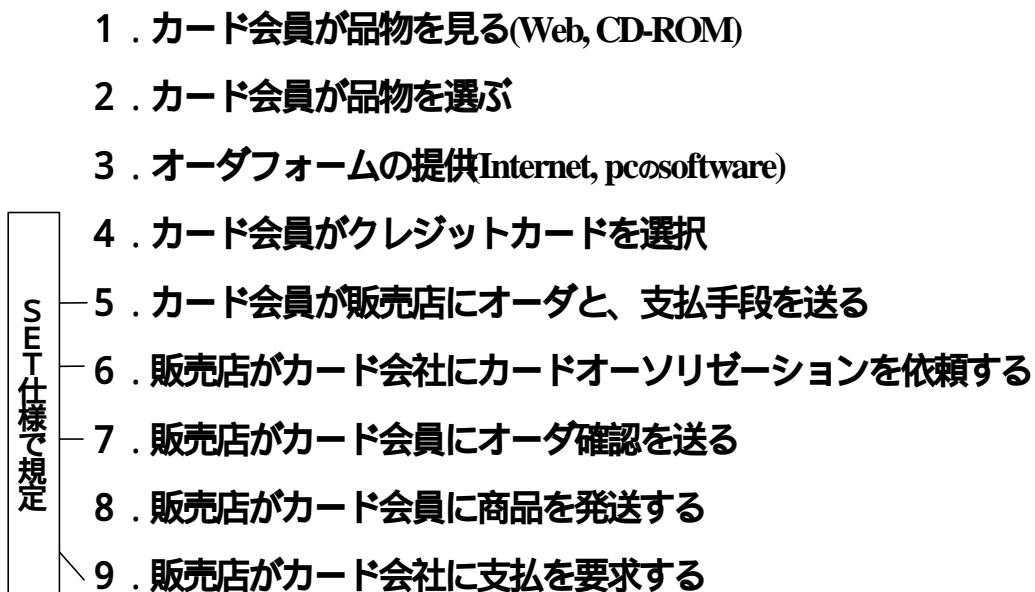
- 
- 1 . カード会員が品物を見る(Web, CD-ROM)
 - 2 . カード会員が品物を選ぶ
 - 3 . オーダーフォームの提供(Internet, pcのsoftware)
 - 4 . カード会員がクレジットカードを選択
 - 5 . カード会員が販売店にオーダーと、支払手段を送る
 - 6 . 販売店がカード会社にカードオーソリゼーションを依頼する
 - 7 . 販売店がカード会員にオーダー確認を送る
 - 8 . 販売店がカード会員に商品を発送する
 - 9 . 販売店がカード会社に支払を要求する

図 - 3 S E Tの対象範囲

3. S E Tの対象範囲 図-3 参照

インターネット上でどのような手順で一般的に取引が行われるかということになると、販売店の Web を見るというやり方がある。この場合スピードの問題とかいろいろあるのであらかじめ販売店から郵送されたCD-ROMで見るというやり方もある。品物を選んで、販売店からオーダーフォームを提供される。これもインターネット上でもらうケースもあるし、先ほどのソフトウェアに組み込みまれている場合もある。このオーダーフォームを見た後、問題は、オーダーする、それからクレジットの支払い指示をするということからセキュリティを必要とする領域に入ってくる。

カード会員がクレジットカードを選択し、販売店に最終的に注文するということを知らせる。それから、クレジットカードの支払い手段を送る。そうすると、販売店は、今の店でもやっているように、オーソリゼーションという行為が必要になる。カード会員の信用確認である。これが済むと、カード会員に承認したということを送る。ここで取引が成立する。商品を発送し、この商品もリアル商品の場合もあるし、デジタル商品、あるいはサービスのもの入ってくる。この後で、販売店は支払いのための要求を行う。

5番、6番、7番、9番に対してSET仕様では標準のセキュアな手順を規定している。

それ以外については自由にやれるということになる。

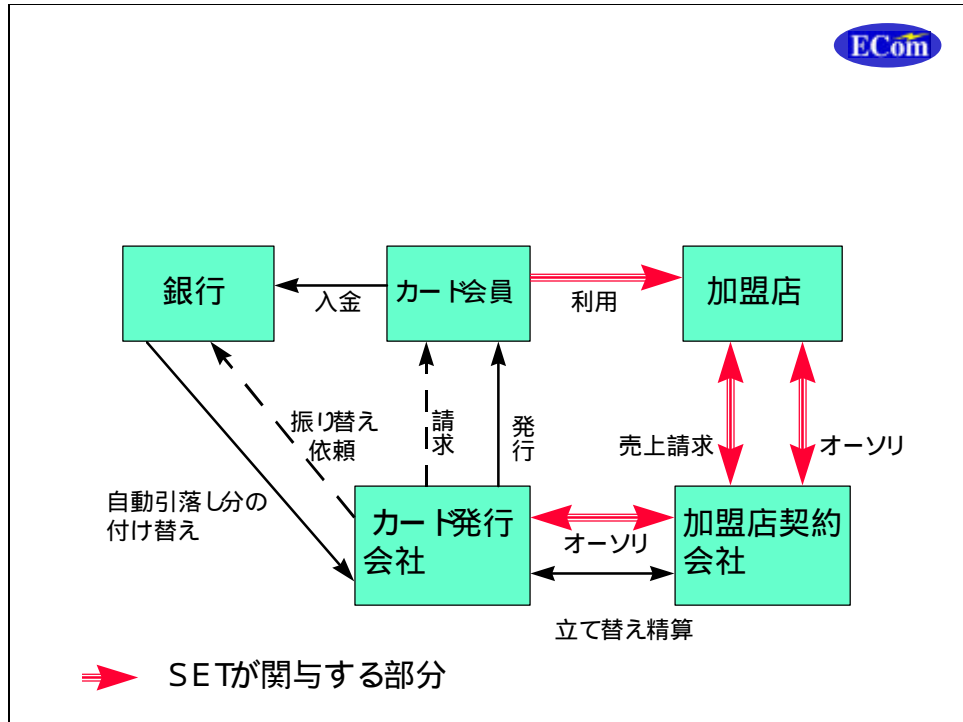


図-4 クレジットカード処理の流れ

4. クレジットカード処理の流れ 図-4 参照

これを一般的なクレジット処理の流れで考えると、カード会員がカード会社からカードを発行してもらって、カードを利用して支払い指示をするという部分に該当する。加盟店がオーソリをかけて、最終的にカード会員に発行したカード会社、つまりイシュアに確認して、販売店がオーケーを出すということで取引が成立する。その後で販売店は売上げを請求する。ここら辺は月の何日締めとか、カードの加盟契約があるので、タイミングとしては少しずれるが、いずれにせよ売上げを請求をし、アクワイアラがイシュアと立て替え精算し、カード会社が請求して、個人が払うということで、二重の線の部分がSETの関与する部分ということになる。

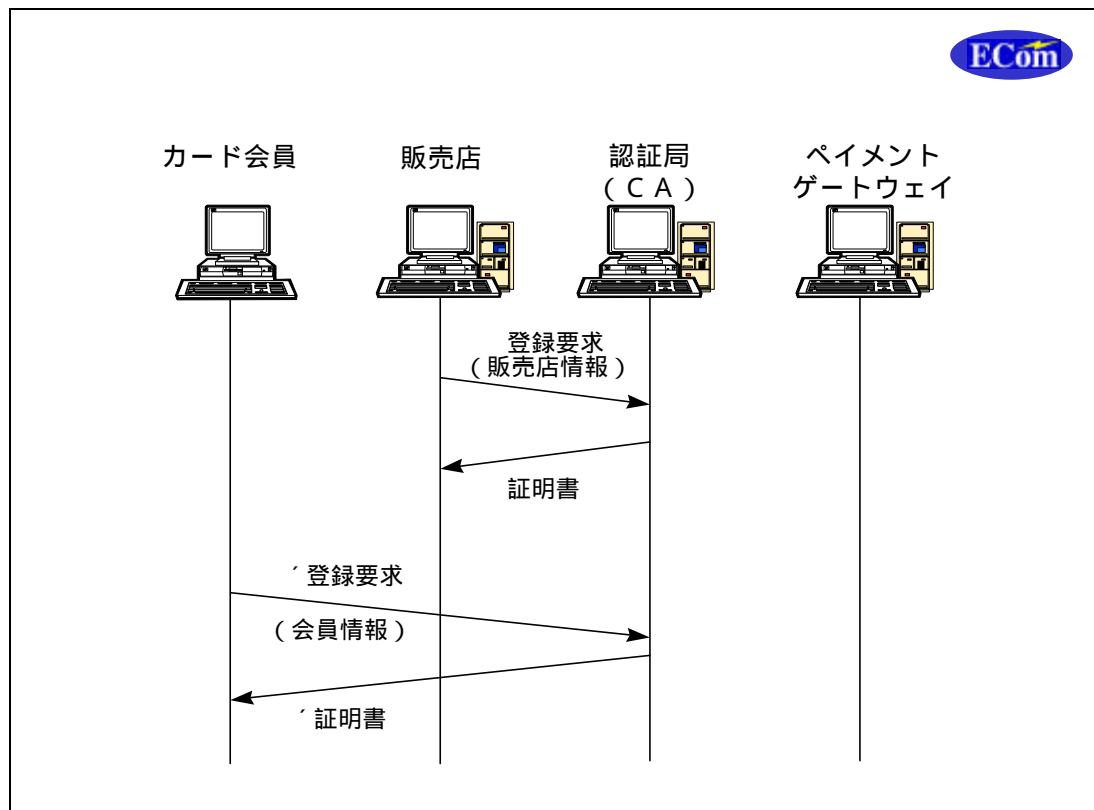


図-5 クレジット決済(登録)

5. クレジット決済(登録) 図-5 参照

これがコンピュータ処理の流れである。先ほどのような取引は、あくまでも事前に登録するということが前提となっている。カード会員はカードを発行してもらっているし、販売店は加盟店契約をしているが、インターネット上のSET仕様では新たに登録ということが必要になる。販売店はSETが定める認証局に登録要求をし、証明書をもらわなければならない。この電子的な証明書が後の決済取引で非常に重要な役割を果たすわけである。このときに、確かに加盟店契約をした正しい販売店であるかを確認するためにいろいろな情報を送ることになる。同様に、カード会員もここで会員情報を詳しく送ることになる。なぜならば、CAは情報をもらおうとイシューなりアクワイアラに、確かにあなたが許可した本人ですかということを尋ねて、その回答をもらうわけであるから、ここでは余り簡単な情報だと他人になりすましてしまうという危険がある。

SETでは、本人確認に、イシューとかアクワイアラがどのくらいの情報を必要とするかということは、それぞれのイシュー、アクワイアラに任せることになっていて、どのくらい詳しい情報が必要になるかというのはカード会社の政策、本人認証という一番大事な行為であるから、それぞれの政策にかかわる部分になる。ここは非常に大事な情報で、これが他人に漏らされると一番怖い、なりすましということが起きる可能性がでてくる。そのため暗号化と復号ということが必要になってくる。

この証明書について、CAの電子的なサインが必要になる。CAしかサインできないよ

うなことが必要になる。

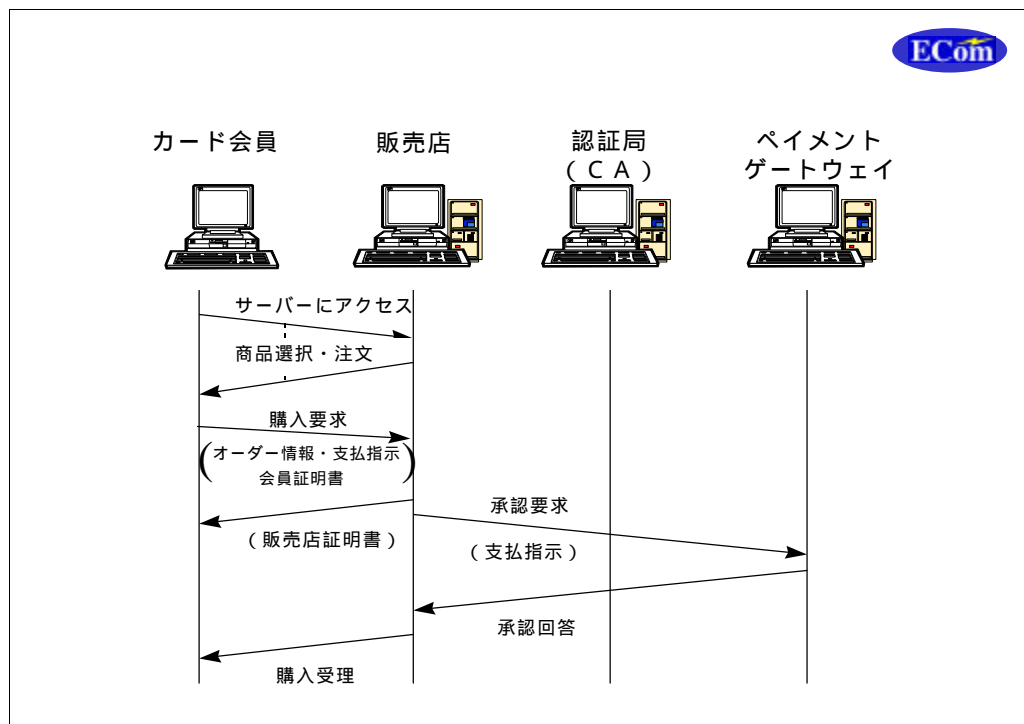


図 -6 クレジット決済(購入、承認)

6. クレジット決済(購入、承認) 図-6 参照

さきほどの登録という重要な行為が済まされているからこそ、購入要求をし、オーソリをかけて、取引が成立する。この段階で、カード会員から販売店には会員の証明書、販売店の方も、正しい加盟店であるという証明書の交換をすることになる。この証明書にはCAのサインがある。こういった流れのため、秘密送信とお互いの認証ということがどうしても必須になる。

- secureでないネットワークを利用する非対面取引でのクレジットカードによる安全な決済を行うためのプロトコル
- EC (ネットワーク利用)に係わる部分だけをカバー (従来からのクレジットカードの仕組みを前提として利用する)
- 「相手の認証」と「重要通信の秘密化」

図 -7 S E T (Secure Electronic Transaction)とは

7. S E T (Secure Electronic Transaction)とは 図-7 参照

一番のポイントは顔を見合わせていないということである。それで、かつ、安全にしなければいけないということで、相手の認証と通信の秘密化ということが必要になる。クレジットの仕組みを、現在のものを前提として、その決済部分をカバーするのがS E Tである。

秘密鍵暗号

(対称型暗号：Symmetric cryptography)

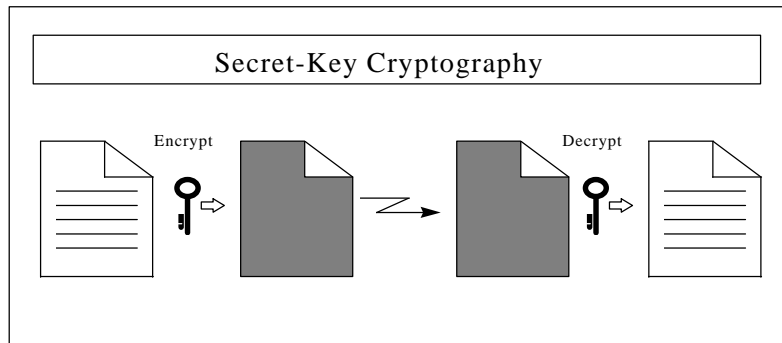


図 -8 秘密鍵暗号

8. 秘密鍵暗号 図-8 参照

秘密鍵暗号（対称鍵暗号）の方が歴史が古い。この方式では暗号化ということになると、同じキーをお互いが秘密に持っていて、他人に漏らさないようにして送るという方式を従来からとっていた。しかしインターネット上で、この方式だけでやろうとすると明らかに無理がある。つまり販売店にしてみると、インターネット上でその販売店が対象とするお客さんというのは数万人から数十万人、多ければ多いほどいい。そうすると、他人になりすまされないできちんと送るためには、10万人を相手にしようと思えば10万個のキーを販売店は管理しなければいけない。かつ、そのキーをどうやってお互いが安全に持つかという問題もある。実際にはこういうやり方で行うというのは、規模が大きくなると不可能になる。

ただ、いわゆる秘密鍵、お互いに同じキーで暗号化、復号するというやり方、これは Secret Key Cryptography、または同じ鍵を使うので対称型、Symmetric Cryptography と呼ばれているが、この方式の方が暗号化とか復号のスピードが速い。従って、実際には S E T の中でもこのやり方を利用しているが、この方式だけでやるのは先ほどのような理由で実際には無理ということになる。

公開鍵暗号

(非対称型暗号：asymmetric cryptography)

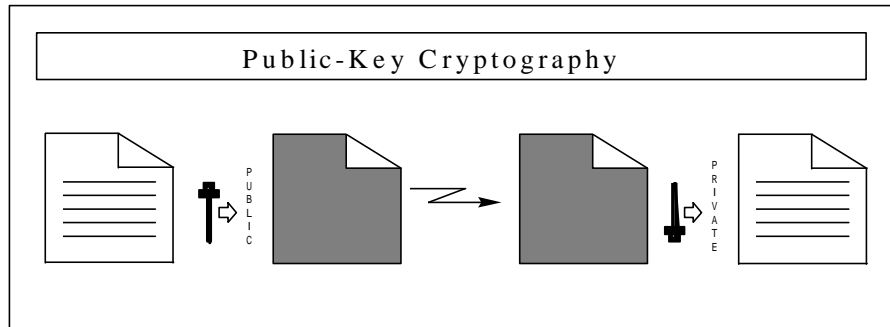


図 -9 公開鍵暗号

9. 公開鍵暗号 図-9 参照

そこで考え出されたのが公開鍵暗号であり、この方式があるからこそインターネット上での取引が可能になる。数学的にある関係を持つ違うキーを使って、パブリック・キーというもので暗号化して、復号はプライベート・キーで行う。これはパブリック・キーがポイントなので、Public Key Cryptographyと呼ばれている。また鍵が同じキーではないので、非対称、asymmetric Cryptographyとも呼ばれている。

なぜこれが優れているかというと、販売店は自分の公開鍵を公表できるわけである。このパブリック・キーでカード会員が暗号化したものは、販売店が持っている自分の秘密鍵でしか復号できない。この鍵ペアはそういう関係になっている。従って、販売店は、自分の公開鍵を証明書つきでばらまいてもカード会員は安全に送れる、販売店がプライベート・キーを漏らさない限り会員は安全に送れるということになるわけである。10万であろうが、100万であろうが販売店は取引をしたいというお客さんに自分の公開鍵の証明書を配れば、それで暗号化してくれればいい、ここが一番のポイントになっている。

もう一つのポイントは、逆に販売店が自分しか知らないプライベート・キーで暗号化すると、パブリック・キーでしか復号できない、これも一つの利点である。あるメッセージをプライベートで暗号化すると、みんなが知っているパブリック・キーで復号できるが、その復号結果が正しければ、間違いなく販売店が暗号化したものであるということの確認ができる。販売店でしかできない署名をしたということになる。つまり、Public Privateの方向でやると秘密送信になるが、逆にPrivateで暗号化して、Publicで復号すると販売店の署名を認めることになる。そういう非常に優れた利点がある。この公開鍵の優れた利点によってクレジット決済が可能になる。



図 -10 公開鍵暗号の2組の鍵

10. 公開鍵暗号の2組の鍵 図-10 参照

先ほども述べたように、秘密送信をするときにもこのパブリック、プライベートを使うし、署名のときにも使うが、安全のために鍵のペアを別に行っている。図においてこれは両方とも販売店が秘密鍵を持つ鍵ペアなのでマーチャントと書いてある。従って、販売店に秘密送信をするときに使うわけである。鍵交換、秘密送信であるというのがこの鍵のマークである。これは販売店が秘密鍵を持つペアである。プライベートとパブリックというのは両方「P」になるのでややこしいが、公開の方が「パブ」のパブリックだと覚えるとわかりやすい。

次に、販売店が間違いなく自分が署名したものだよということで秘密鍵を管理する、署名のときの確認に使う公開と秘密のペアを signature pair と呼んでいる。販売店が秘密鍵を持って署名を行う。販売店から受け取った方は公開鍵によって、署名を確認する。署名に使うためにデジタル署名の菱形のマークが入っている。従って、販売店は必ず二つの鍵対を持つことになる。つまり自分に対して秘密送信をしてもらう必要があるし、自分が署名して相手に送る必要が必ずあるので、この2つの鍵ペアは必須になる。後でこれを使った説明が出てくるので、図-10 に戻って、参照のために再確認するとわかりやすい。

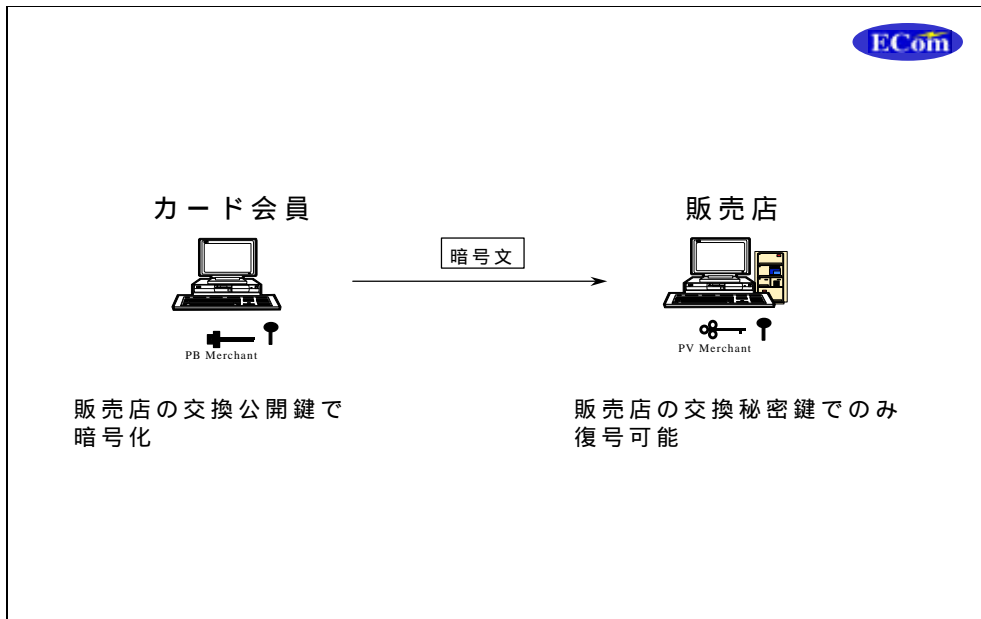


図 -11 情報の秘密送信

11. 情報の秘密送信 図-11 参照

カード会員が販売店に送る場合には、販売店の公開鍵、パブリックで送信すると、販売店しか持っていない秘密鍵でしか復号できないので、販売店は他人に知られずに、自分が不注意で秘密鍵をとられない限り、秘密通信できたということになる。

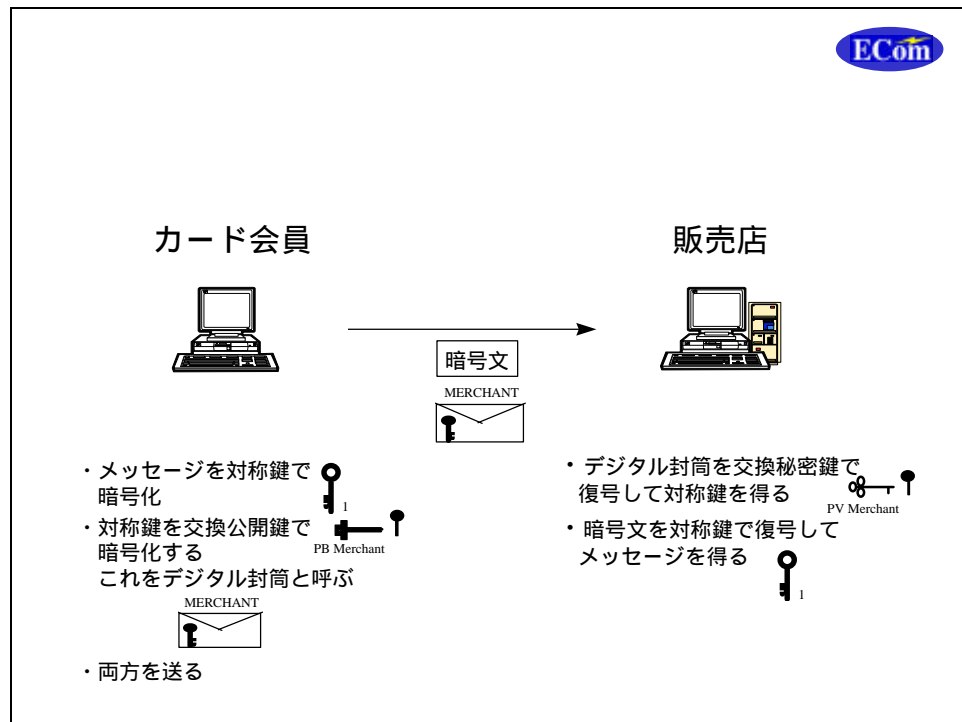


図-12 対称鍵方式の応用とデジタル封筒

12. 対称鍵方式の応用とデジタル封筒 図-12 参照

ただ、問題は先ほどのべたように、対称鍵の方が暗号化、復号のスピードが早い。メッセージを全部公開鍵方式でやると非常に時間がかかるので、実際には対称鍵を組み合わせたやり方を使っている。つまり長いメッセージの暗号化、復号には対称鍵の方が速いので、ランダムジェネレーションで、カード会員は対称鍵をジェネレートし、ジェネレートした他対称鍵で暗号化する。あとは、この対称鍵を安全に販売店に秘密のうちに送ればいいわけであるから、そこで今の秘密送信を使う。従って、長いメッセージは対称鍵で暗号化して、鍵交換の販売店の公開鍵で一番大事な対称鍵を暗号化して、それを販売店しか持っていない秘密鍵で復号して、対称鍵を手に入れて復号するという2段構えでやるわけである。工夫が行き届いていて、処理スピードも速いし、安全に対称鍵を送ることができる。SETでは、対称鍵を販売店の公開鍵で暗号化したときに、封筒の記号を使う。これをデジタル・エンベロップと呼んでいる。図ではこの中に対称鍵が入っている。販売店の公開鍵で暗号化したデジタル封筒である、つまり販売店の秘密鍵でしかあけることはできないということを示している。

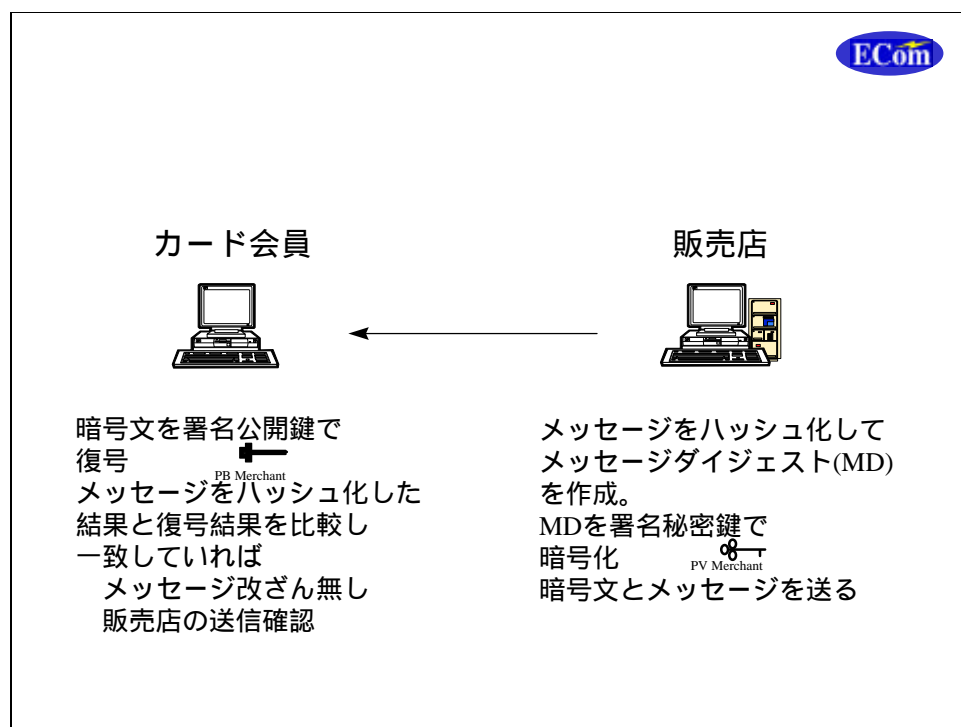


図 -13 デジタル署名

13. デジタル署名 図-13 参照

次に、デジタル署名であるが、今度は署名鍵のペアを使う。販売店が自分しかできないという署名をする場合であるが、もとのメッセージを160ビットにハッシュ化する。これは圧縮関数であるが、160ビットに圧縮したものをメッセージダイジェストと呼んでいる。このメッセージダイジェストを販売店しか持たない署名用の秘密鍵で暗号化して送ると、こちらではもらったメッセージをハッシュ化して、デジタルサインを販売店の公開鍵で復

号する。そうすると、販売店からもらったもとのメッセージからハッシュ化したものと、ハッシュ化したものを秘密鍵で暗号化したものを復号して、両方を比較するという動作をする。

一致していればメッセージは改竄されていない、かつ、販売店しか知らない秘密鍵で署名されているという二つのことが確認できる。このハッシュ関数もよくできていて、1ビットでも直すと平均して160ビットのメッセージダイジェストの半分ぐらいが入れ変わるような関数になっているから、メッセージが変更されていないということが、このハッシュを比較することによって確認できる。

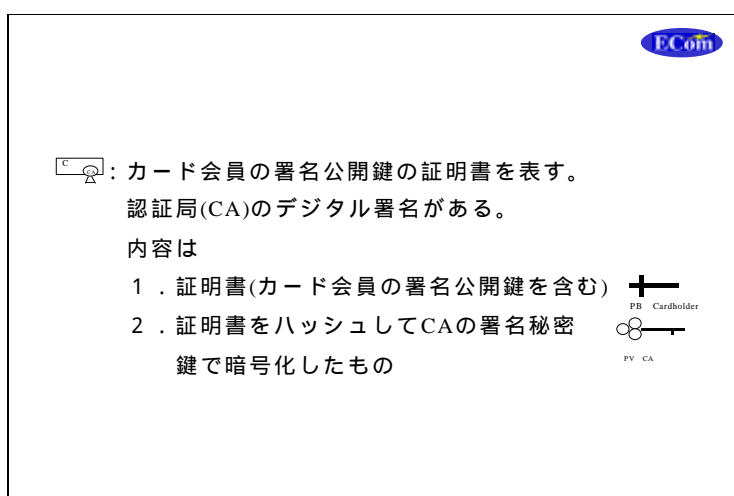


図 -14 証明書

14. 証明書 図-14 参照

これが私の公開鍵ですよという証明書をお互いにやりとりするのであるが、証明書自身がいいかげんなものであったら、信用できない。そのためお互いの証明書に対してはCA = 認証局の、認証局しかできないデジタル署名がある。図においてカード会員の署名公開鍵の証明書には署名のマークがある。Cというカード会員の頭文字がある。それから、CAのシールが貼ってある。CAの署名入りの証明書であるということになる。

この中の内容は、カード会員が販売店に知らせるための署名公開鍵を含んでいなければならない。また、証明書をハッシュ化してCAが署名したものであるから、もらった方はCAの証明書が別にあるのであるが、そこからCAの署名用の公開鍵を知ることができ、それで署名を復号して、証明書のハッシュと比べて、これが一致したということになると、これは間違いなくCAがサインしたものである。

これは署名の公開鍵の証明書であるが、販売店の場合、鍵交換の公開鍵の証明書もある。販売店はペアを二つ持つから、公開鍵についても2種類の証明書をCAに出してもらって持っていれば身元証明ができるということになる。

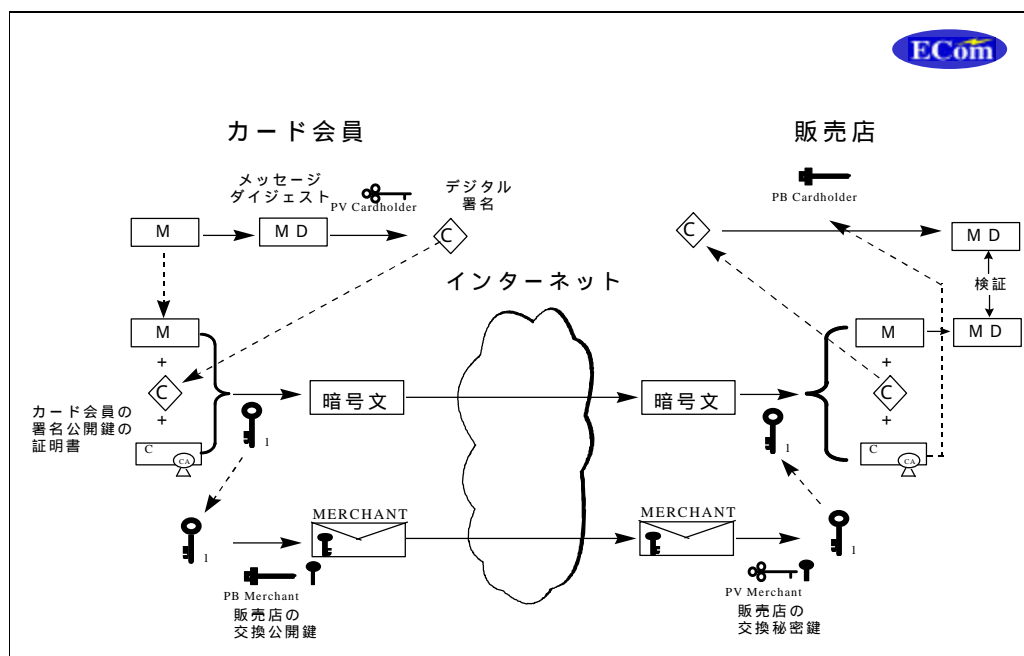


図 -15 秘密通信と認証

15. 秘密通信と認証 図-15 参照

今まで述べた方式を使って、カード会員が販売店にメッセージを秘密に送信し、かつ、自分の身元も証明するという流れがこの図である。まず、カード会員はメッセージを送るのであるが、正しく自分が送ったものだと、自分が作成したメッセージだということを証明するためにデジタルサインをする。そのためにメッセージからハッシュで160ビットのメッセージダイジェストをつかって、それを自分の秘密の署名鍵で暗号化する。デジタルサインと呼ばれるものである。これをメッセージにつける。もとのメッセージをハッシュ化して、復号した結果と比べて正しいかどうかチェックするわけであるから、もとのメッセージが必要である。

次に、デジタルサインを販売店に知らしめるためには、自分の署名公開鍵を教えなければならぬ。従って、前の図で説明したカードホルダーの署名用の公開鍵とCAのシールがついた証明書を送る必要がある。これを公開鍵方式で全部暗号化すると時間がかかり過ぎるので、先ほど述べたように、ジェネレートした対称鍵を使って暗号化する。これを販売店の鍵交換で公開している交換用の公開鍵で暗号化してやると、販売店は安全に対称鍵を取り出すことができる。自分しか知らない交換用の秘密鍵を使えばいいわけである。この暗号文が三つとも平文に戻るわけである。

戻ったら、ハッシュをカード会員しか知らない秘密鍵で暗号化したものであるから、この証明書から取り出した署名の公開鍵で復号する。それで、メッセージダイジェストを取り出す。それから、今もらったメッセージを自分でハッシュして、この二つをコンペアする。これが一致していれば、それは正しくカード会員がつくったメッセージであり、メッセージは変更されてない。カード会員しか知らない秘密鍵で署名されている。かつ、自分しか知らない秘密鍵で復号したものであるから、メッセージの秘密送信も確認される。公

開鍵方式とか署名というのは大体こういうパターンで使われている。

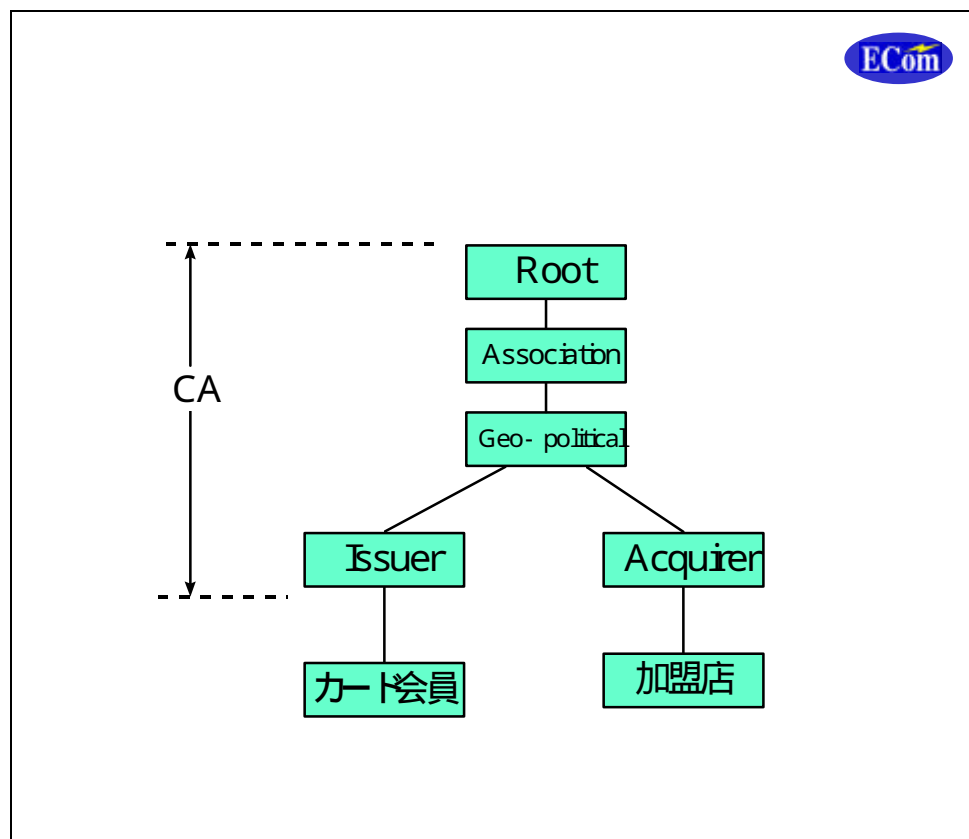


図 -16 CAのTree 構造(Hierarchy of Trust)

16. CAの木構造(Hierarchy of Trust) 図-16 参照

疑いの世界では、おまえは確かか、実はCAの証明書がある。ではそのCAはどうなんだということになる。先ほど、カード発行するイシュア、加盟店を契約するアクワイアラとCAというのを別々に書いたが、実際には、それらがCAそのものを運営するケースが多いだろうとSETも予想している。

CAになっているイシュア、CAになっているアクワイアラ、こういったものはサインをして、カード会員とか加盟店に公開鍵の証明書を出すわけであるが、自分自身はもう少し上の、例えば Visa、Master Card でいうと、地域とか国が中心になるような組織の証明書もらう。それに対しては、Visa とか Master Card の本社のアソシエーションの証明書を出すわけである。従って、確かめたければ、証明書の証明書を要求して、また証明書を要求して、それぞれの組織のデジタルサインを確認することによってCAの信用を確認することができる。

今はここまでであるが、その上の、公的な国の中央の組織、その証明書は Visa、Master Card がもらおうという動きをしている。これがルートキーで、ここから上はないということになる。つまりルートキーの組織は自分で自分自身を証明するしかないということに

なる。こういうことによって単に一重構造のC Aになりすますことを防止するやり方をとっている。

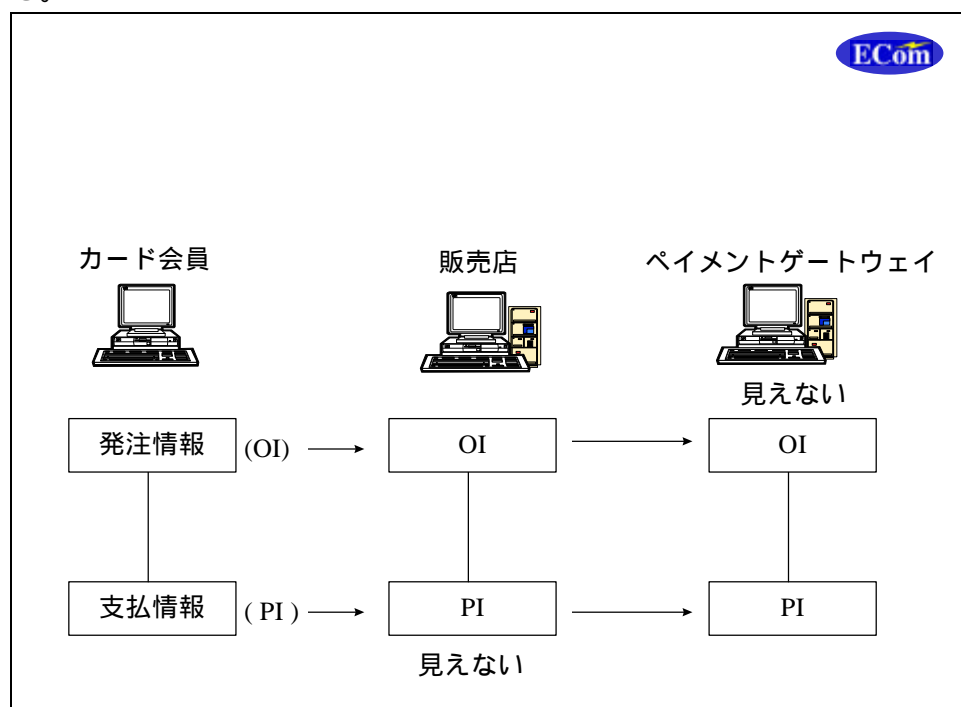


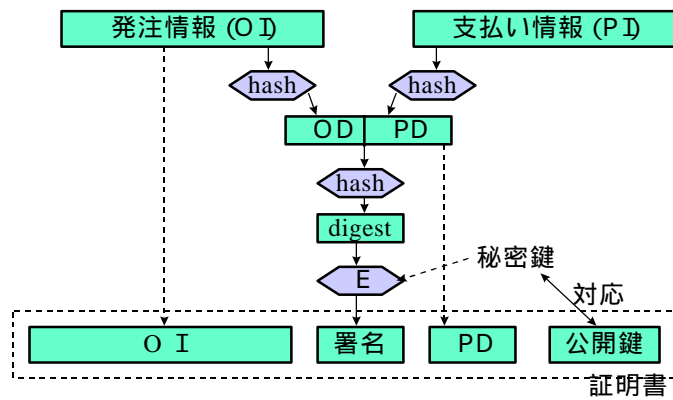
図-17 注文とカード情報(二重署名の必要性)

17. 注文とカード情報(二重署名の必要性) 図-17 参照

このほかにSETでクレジット決済を行う際に、少し込み入った問題が発生する。カード会員はどのようなカードを使う、それから、どのようなものを注文するという二つの情報を、販売店には注文を送らなければいけないし、ペイメントゲートウェイ、またその先のイシューに対しては支払い関係の情報を伝えなければいけない。

その際、カード会員にしてみると、カード関係の細かい情報は販売店に見られたくないし、また見せる必要もない。それから、カード会社にはどんなものを買っているかということは別に知らせる必要はない。販売店にはどのようなものを注文しなければいけない、カード会社には幾らの支払いをしてくれということだけを知らせればよい。こういうものをつくった方がよりカード会員としてはありがたいし、見せる必要のないものは極力見せないというのがプライバシー保護の鉄則である。そのかわりこの二つは同じ品物の注文に絡む話なので関係がある。

2つの情報に併せて署名する技術



加盟店への発注情報 (支払情報は見えない)

図-18 二重署名(Dual Signature)

18. 二重署名(Dual signature) 図-18 参照

このような機能を実現するために、同じ署名でも Dual Signature という方式をとっている。先程の発注情報と支払情報、この両方のハッシュをとる。このハッシュを連結してもう一回ハッシュをかける。この二重ハッシュに対して、例えば加盟店に送る場合には、自分しか知らない秘密鍵で暗号化して署名するわけである。あと、販売店に必要な情報は発注情報、これは当然なければいけない。支払情報は見せる必要はないので、片一方のハッシュだけを入れてやるわけである。自分の公開鍵の証明書も当然送るということになる。

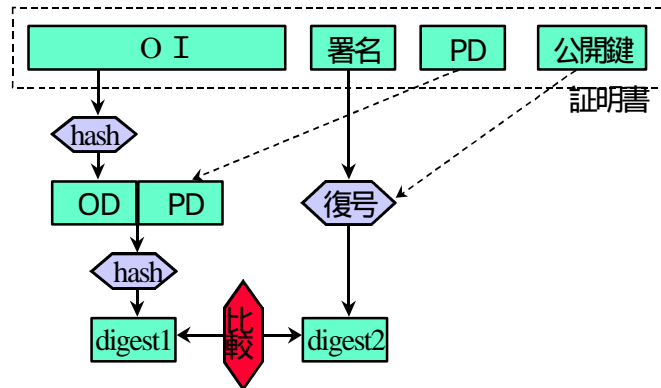


図-19 二重署名の検証

19. 二重署名の検証 図-19 参照

これを送ると、販売店の方では、オーダー情報は自分が知らなければいけないのであるが、オーダー情報のハッシュをとる。このハッシュというのはもとの情報はわからないようになっているので、それだからこそ支払情報はわからないのであるが、そのハッシュと連結して二重ハッシュをつくる。先ほどの署名したものを会員の公開鍵で復号して、それと比べる。つまり支払情報は見れないかわりに、そのハッシュをもらってお互いの関係を確認し、カード会員の身元も証明する。かつ、オーダー情報とかハッシュが変更されていないことも確認できるという方式をとっている。

これと裏返しのやり方をすれば、支払いゲートウェイには片一方のハッシュしか見せない。つまり支払いゲートウェイにはオーダー情報のハッシュしか送らないということで、支払いゲートウェイに送るときには、支払いゲートウェイの鍵交換用の公開鍵で暗号化するから、この情報というのは販売店は見れない。販売店が見れるのは今送ってもらった情報だけということになるから、支払情報とオーダー情報のハッシュを支払いゲートウェイの公開鍵で暗号化して送ってやれば、支払いゲートウェイは支払情報とオーダー情報のハッシュしか見れない。同じように二つの関係が確認できるということになる。

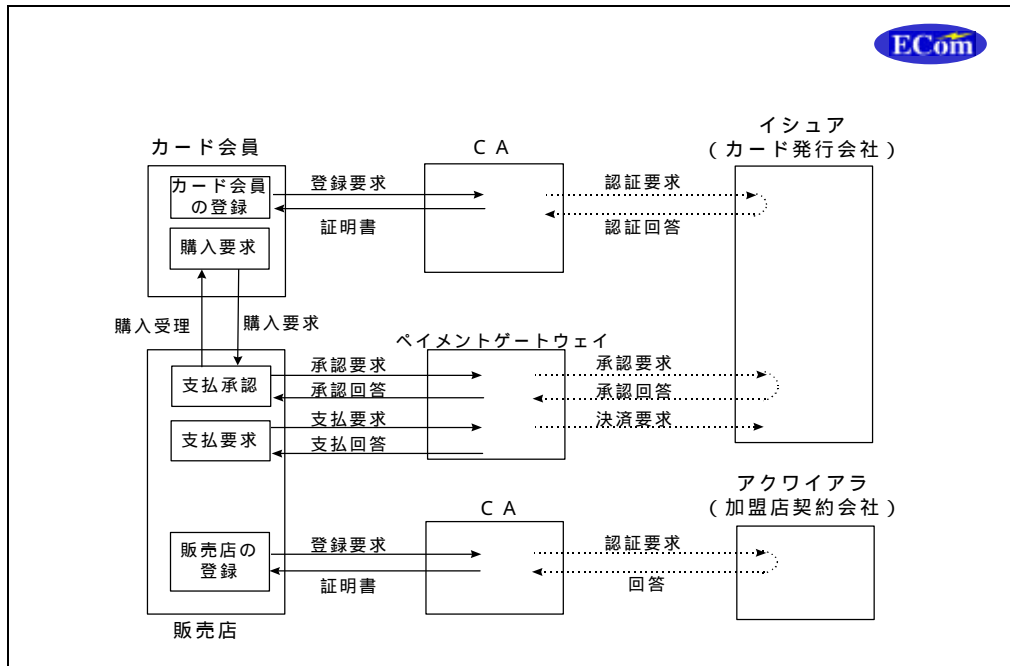


図 -20 S E Tの代表的トランザクション

20. S E Tの代表的なトランザクション 図-20 参照

S E Tで、代表的なトランザクションと呼ばれているものを図-20 に表わす。カード会員がC Aに登録し、証明書をもらう。販売店が登録し、証明書をもらう。購入を決意すると、購入要求を出して、オーソリを掛けて回答をもらう。取引が成立すると、後ほど販売店は支払要求を出す。実線部分はS E Tで細かく規定されている。点線部分はS E Tの中でこういうことをやるという示唆はされているが、実際のやり方はそれぞれのシステムに任されている。

イシューアとC A、アクワイアラとC Aというのは同じカード会社が運営することが多いが、理解の都合上、取引としては、S E Tの中では分けて記述されている。ただし、これは恐らくは同じ会社だろうということはS E Tの中でも述べられている。

身元確認をどうやるかというのは、いわゆる本人認証の一番ポイントのところであるが、それはそれぞれのカード会社に任されている。S E Tで規定する問題ではないと述べている。

- Book1 : Business Description
業務要件、暗号と認証、代表的取引フロー
- Book2 : Programmer's Guide
取引と処理の詳細
- Book3 : Formal Protocol Specification
メッセージ内容の規定

図 -21 Specification

21. Specification 図-21 参照

S E Tのスペックには、図にあるように、Book 1、2、3とあって、Book 2、Book 3はソフトウェアベンダーでないと必要ないぐらいの細かい情報になっている。今まで述べたような情報をより詳細に理解するには Book 1が一番適当ではないかと思われる。大体 80 ページのものである。ただ、Visa、Master Card が中心になってまとめているので、クレジット関係の知識については余り丁寧に書いていない。ネットワーク上のコンピュータ処理に関するプロセスの方は細かく書いてある。

そういう意味で、これを英文のまま読みくださるのはなかなか大変である。E C O Mの方ではカード会社出身の主査とコンピュータメーカー出身の主査と入り交じっていて、協力して、Book 1の解説書をつくった。内容を理解して日本語化しているのも、厳密な翻訳よりはわかりやすい日本語化というものに努めている。

また、クレジット処理について、いわゆる S E Tの範囲だけではなく、クレジット処理全般について解説をつけた。クレジット処理全体の中の位置づけや、暗号化及び署名、鍵の問題のわかりやすい解説、ノードと取引の関係、などの解説も追加している。Master Card と Visa の日本支社の方にも内容をチェックしていただいた。

この解説書は E C O Mに申し込んで頂ければ、入手できる。