IMES DISCUSSION PAPER SERIES

電子マネーを構成する情報セキュリティ技術と安全性評価

中山 靖司　太田 和夫　松本 勉

Discussion Paper No. 98-J-26

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所

〒100-8630 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 98-J-26
1998年11月

電子マネーを構成する情報セキュリティ技術と安全性評価

中山 靖司[*1]　太田 和夫[*2]　松本 勉[*3]

要　旨

電子マネーのセキュリティ対策については、既に様々な理論的・実証的研究が行なわれているが、電子マネーの安全性を確保するためには、発生し得る不正のリスクを十分考慮の上、これに見合った効果的なセキュリティ対策を施していく必要がある。そのためには、発生し得る不正のリスクの種類、程度を十分把握するとともに、使用しているICカードが実際に必要なセキュリティレベルに達しているか、使用している暗号アルゴリズムやその鍵長の設定が適当か、鍵管理等が適切に行なわれているか、等を総合的に評価していくことが必要となる。

本稿では、まず、電子マネーを構成する様々な情報セキュリティ技術のうち、特に代表的な要素技術として暗号技術と耐タンパー技術を取り上げ、こうした要素技術は一定の条件のもとでの安全性を保証するものに過ぎず、絶対的な安全性を持つものではないことを指摘する。次に、これらの情報セキュリティ技術のうち、IC カード等の耐タンパー性に頼ることなく電子マネーを構成した場合に、その論理的な構成方法の違いによって、電子マネーの安全性にどのような差が出てくるのかを、発生し得る不正のリスクの種類、程度、範囲を分析することにより評価する。このような評価結果は、各電子マネー実現方式間の優劣関係を示すとともに、それぞれの電子マネー実現方式が総合的な安全性を確保するためには、さらにどのような要素技術（耐タンパー装置等）を追加する必要があるかを検討する材料として利用しうる。なお、分析の対象とする電子マネー実現方式は、電子マネーを機能および技術的観点から整理・類型化し、全ての電子マネーを包含しうるモデルを作成したうえで、それぞれに対し典型的な暗号技術を適用することによって導びかれたものである。このようにモデルを用いたアプローチは同時に電子マネーの安全性を評価するためのひとつの考え方を提案しているといえる。

今後は、こうした提案を参考にして、個々の電子マネー実現方式について、複数の情報セキュリティ技術を用いて総合的な安全性を確保する方法を検討していくことが必要と思われる。

キーワード：　電子マネー、電子現金、暗号、耐タンパー性、セキュリティ、安全性、IC カード
JEL classification: E49, L86, Z00

*1 日本銀行金融研究所研究第2課（E-mail: yasushi.nakayama@boj.or.jp）
*2 日本電信電話(株)情報通信研究所（E-mail: ohta@sucaba.isl.ntt.co.jp）
*3 横浜国立大学大学院工学研究科人工環境システム学専攻（E-mail: tsutomu@mlab.dnj.ynu.ac.jp）

本論文は、1998年11月4日に日本銀行で開催された「金融分野における情報セキュリティ技術に関するシンポジウム」への提出論文に加筆・修正を加えたものである。

目　　次

頁

Ⅰ.はじめに

電子マネーのセキュリティ対策については、既に様々な理論的・実証的研究が行なわれているが、現実に使用される電子マネーの安全性を適切に評価するにあたっては、その実装までを視野に入れた分析が必要である。すなわち、電子マネーという決済手段を実用化する際の採算性を考えながら実装を行なうときには、セキュリティ対策にかけられる費用に制約があるため、発生し得る不正のリスクと、それを防止するのにかかるコストのバランスを十分考慮の上、効果的なセキュリティ対策を施すことが重要となってくる。そのためには、個々のセキュリティ対策がどのような種類、程度のリスクに備えたものかを十分把握した上で、これに見合ったレベルの安全性を実現することが必要である。また、実装には様々な技術的あるいは運用的制約が伴うため、必ずしも理論通りの理想的な仮定が成り立たないことも多く、開発者が当初想定していた安全性のレベルが達成できていない可能性もある。例えば、IC カード型の電子マネーの多くは、IC カード内部の情報を不正に読み出すことが困難なことを安全性の拠り所としているが、IC カードの種類によって耐タンパー性の強度は異なるため、実際に必要なセキュリティレベルに達している適切な IC カードを採用しているということは重要なことである。また、使用している暗号アルゴリズムの選択、その鍵長の設定、鍵管理等が適切に行なわれていることも、安全性のレベルに直接影響する事項である。

本稿では、まず、第Ⅱ章で電子マネーを構成する様々な情報セキュリティ技術のうち特に基本的なものとして、暗号技術と耐タンパー技術を取り上げ、こうした要素技術は絶対的な安全性を持つものではなく、一定の条件のもとでの安全性を保証するものに過ぎないことを指摘する。次に、第Ⅲ章でこれらの情報セキュリティ技術のうち IC カードの耐タンパー性に頼ることなく電子マネーを構成した場合に、その論理的な構成方法の違いによって、電子マネーの安全性にどのような差が出てくるのかを、発生し得る不正のリスクの種類、程度、範囲を分析することにより評価する。このような評価結果は、各電子マネー実現方式間の優劣関係を示すとともに、それぞれの電子マネー実現方式が総合的な安全性を確保するためには、さらにどのような要素技術（耐タンパー装置等）を追加する必要があるかを検討する材料として利用しうる。なお、分析の対象とする電子マネー実現方式は、電子マネーを機能および技術的観点から整理・類型化し、全ての電子マネーを包含しうるモデルを作成したうえで、それぞれに対し典型的な暗号技術を適用することによって導かれたものである。最後に第Ⅳ章でまとめを行なう[1]。

[1] 本稿は、「1998 年 暗号と情報セキュリティシンポジウム（SCIS’98）」で発表した研究内容（中山・太田・松本[1998]）を、その根拠とともに詳細に示すとともに、さらに研究対象のスコープを広げ発展・拡充させたものである。

Ⅱ.電子マネーを構成する情報セキュリティ技術

安全で効率的な電子マネーを実現するためには、暗号技術、耐タンパー技術といった要素技術を複雑に組み合わせて電子マネー実現方式の検討を行う必要がある。また、実際に電子マネーを稼働させるためには、その他の実装技術、運用技術等についても注意を払わなければならない。電子マネーの安全性を評価するためには、組み合わせられた技術ひとつひとつの安全性を評価すると同時に、全体としての電子マネーのシステムに欠陥がないかを確認することも必要である。

本稿では、このうち、電子マネーの実現方式に焦点を当てて分析を行う。まず、本章において、安全で効率的な電子マネーを設計するために必要な、暗号技術及び耐タンパー技術に代表される要素技術の安全性についての現状を把握し、その上で、第Ⅲ章で、こうした要素技術を使った電子マネーの実現方式の違いによって、電子マネーのシステム全体の安全性がどのように変化するかを分析する。

（電子マネーを実現するために必要な技術）

- 電子マネー実現方式　（Ⅲ章で分析）
  - 電子マネープロトコル等
- 暗号技術　（Ⅱ．１．で分析）
  - 公開鍵暗号、共通鍵暗号、ディジタル署名方式等
- 実装技術
  - 耐タンパー技術　（Ⅱ．２．で分析）
    - IC カード、暗号デバイス装置、PCMCIA 等
- 運用技術　（今回の分析対象外）

1. 暗号技術

(1)電子マネーで利用される暗号技術の機能

電子マネーを構成するためには、以下のような暗号技術の持つ様々な機能／特徴等が利用されている。

メッセージ守秘…電子マネーの発行や支払等の取引を行なう際に、盗聴によって取引で受け渡される情報や電子マネーが第 3 者に入手され、取引者個人のプライバシー情報が漏洩したり、電子マネーを不正にコピーされて使用されることを防ぐ。DES 等の共通鍵暗号のほか、RSA 等の公開鍵暗号が使われる。

ディジタル署名…電子マネーが真正な発行機関によって発行されたものであること、正しく譲渡されたものであること、あるいは改竄されていないこと等を保証する。RSA 等のディジタル署名方式のほか、必要によってはブラインド署名方式も使われる。

相手認証…電子マネーの発行や支払等の取引を行なう際に、相手が正当な取引相手かどうかあるいは支払いを受けるために提示された電子マネーの正しい保有者かどうか等を確認する。ゼロ知識証明やディジタル署名を使ったチャレンジ･レスポンス等が使われる。

メッセージのハッシュ化…電子マネーを構成する情報等を一方向性関数で圧縮することによって、情報量の削減を図るほか、予めハッシュ値を公表しておき、必要なときにだけ元のメッセージを公表しこれが改竄されていないことを証明する等に使われる。MD5 や SHA-1 等の方式がある。

(2)暗号技術と安全性

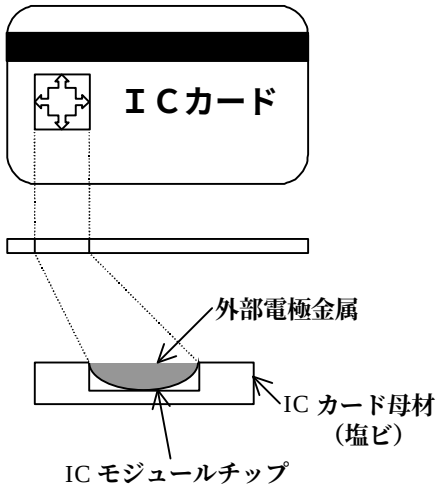
電子マネーは、公開鍵暗号、共通鍵暗号、ディジタル署名方式、ブラインド署名方式、ハッシュ関数、鍵配送／共有方式などの暗号技術が必要に応じて組み合わされて実現されており、これらの暗号技術のもつ強度がそのまま電子マネーの安全性のレベルに影響する。また、コンピュータのコストパフォーマンス向上等の技術進歩や新しい攻撃法の出現により、従来安全と考えられていた暗号についても、その安全性が低下する可能性もある。従って、信頼できる安全な暗号技術を使って電子マネーを構成することが必要なのはもちろんであるが、常に最新の技術動向を睨みつつ、安全性を見込んだ適切な暗号鍵の鍵長や有効期限の設定等を行う必要がある。なお、各暗号方式の強度については、宇根・岡本[1998]、宇根・太田[1998]のほか、多くの文献が論じているので参照されたい。

2.耐タンパー技術

(1)耐タンパー技術と IC カード

耐タンパー技術とは、外部からの不正な手続き等により、秘密の情報を観測･改変することや、本来の設計意図とは異なる不正な動作を行なわせること等を困難にするための物理的･論理的技術であり、ハードウェアによって実現されるものとソフトウェアによって実現されるものがある。このような耐タンパー技術を使って実現されたものとしては、CPU (Central Processor Unit) を内蔵した IC カード（スマートカード）が代表的である[2]。IC カードは、内部の情報にアクセスするためには正規の手順を踏むことが必要であり、外部から直接メモリにアクセスして情報を読み出すことが困難な仕組みになっている。IC カードには、外部端子付きの接触型 IC カードと、外部端子のない非接触型 IC カードがあるが、現在電子商取引プロジェクト等で使用されているものは接触型 IC カードが中心であるため、以下では接触型 IC カードを例に説明する。

（図 1）IC カードの構造



接触型 IC カードの基本構造は塩化ビニル等の IC カード母材で作られたカード基板に、IC モジュールチップを埋め込んだ構造となっている（図 1 参照）。このうち IC モジュールチップは CPU、メモリ[3]（RAM、ROM、 EEPROM 等）、メモリアクセス制御回路、セキュリティ回路などから構成されているほか、さらに高性能なカードでは、公開鍵暗号等を高速に処理できるコプロセッサ[4]

---

[2] 他にも、暗号デバイス装置、PCMCIA カード等に耐タンパー技術を適用したものがある。

[3] IC カードで使用されるメモリは、その特性により、通常以下の３つに区別される。

RAM (Random Access Memory)：任意のアドレスを指定して自由に読み書きすることが可能な半導体メモリであり、ほとんどのものは電源が供給されないとデータを保持できない揮発性の記憶デバイスである。なお、最近では、電源が供給されなくてもデータを保持できる不揮発性の FRAM (FLASH RAM) 等もある。

ROM (Read Only Memory)：読み出し専用の半導体メモリであり、RAM と違って電源が供給されなくてもデータを保持できる不揮発性の記憶デバイスである。ROM にはチップの製造時にマスクパターンとしてハードウェア的に作成され、いかなる状況下でも変更ができないマスク ROM のほか、特別な条件下ではデータの消去および再書き込みが可能となる PROM (Programmable Read Only Memory)がある。IC チップモジュールにおいて単に ROM といえば、一般的にはマスク ROM を指す。

PROM (Programmable Read Only Memory)：特別な条件下ではデータの消去および再書き込みが可能な ROM のことであり、マスク ROM 同様、電源が供給されなくてもデータを保持できる不揮発性の記憶デバイスである。主要なものとしては EPROM (Erasable Programmable Read Only Memory) と EEPROM (Electrically Erasable Programmable Read Only Memory ）があるが、その書き込み速度は RAM に比べて遅い。

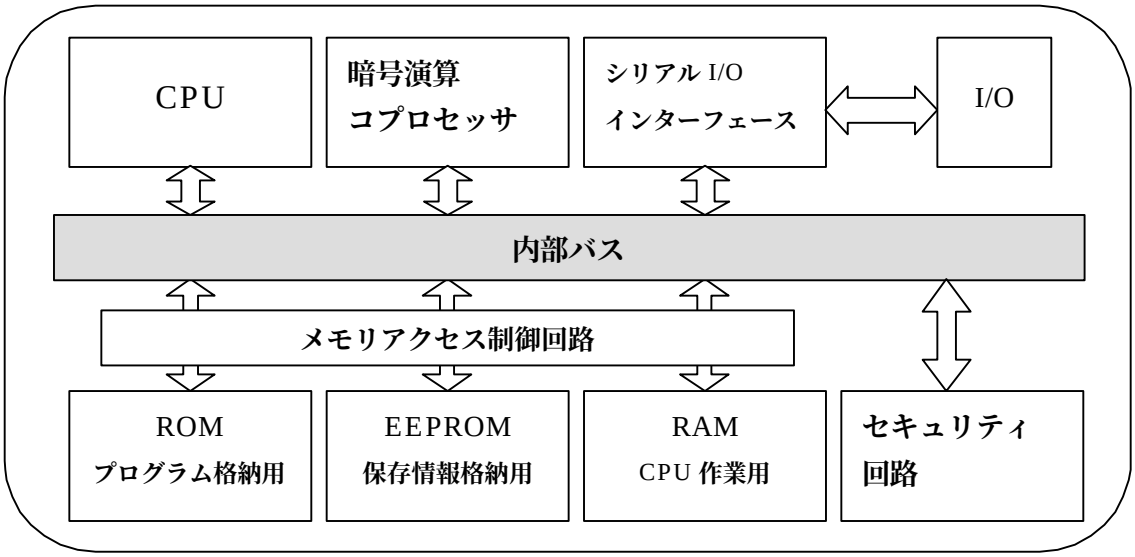
EPROM は一般的にはデータの消去に紫外線を使う UV-EPROM を指す。EPROM にデータを書き込むときには、電源電圧（5V）よりも高い電圧（6V や 12.5V）をかける必要があるほか、データを消去するためにはチップ表面に紫外線を照射する必要がある。

EEPROM は電気的に一括消去や書き換えができる ROM である。データの消去には 5V よりも高い電圧が必要であるが、最近の EEPROM では内部で電源電圧の 5V を昇圧しているため、基盤に実装したままデータを消去して書き換えることが容易になっている。ただし、数十万～百万回までしか、消去／書き換えができないという欠点がある。

IC モジュールチップに実装される PROM としては、実装したままデータを消去して書き換えることができることから EEPROM が一般的である。

[4] コプロセッサ（Co-Processor Unit）：浮動小数点演算処理、マルチメディア処理、暗号計算処理等を高速に処理するために専用に設計された演算処理装置で、中央処理演算処理と協調して

（図 2）IC カードのアーキテクチャ



や乱数発生装置を搭載したものもある（図 2 参照）。

セキュリティ回路は耐タンパー性を実現するために重要なものであり、紫外線を検知したり周波数や電圧の異常を検知した場合等に、CPU を停止させる回路である。また、メモリアクセス制御回路は、許可されない不正なメモリへのアクセスを防ぐための制御回路である。この回路によって、アプリケーションプログラムは他のアプリケーションプログラムか OS のインターフェースしか呼び出せない仕組みになっており、暗号ライブラリを直接呼び出したり、暗号パラメータにアクセスすることによって秘密情報が漏洩することを防いでいる。

(2) IC カードで使われている耐タンパー技術

IC カードで使われている耐タンパー技術は、①物理レベル、②論理レベル、③構造レベル、④運用レベル、の 4 つの階層から論じることができる[5]。以下にそれぞれの階層に属する対策の具体例を示すが、実際には IC カードにかけられるコスト制約のもとで、こうした技術を組み合わせることにより、より高い耐タンパー性を実現することとなる。

(a)物理レベルの対策

IC チップの取出し／露出、回路／メモリの物理的解読や EEPROM のデータの物理的破壊等に対する防止対策であり、主に物理的構造解析等の攻撃に対する安全対策となる。

- **チップの表面をアルミ等でカバー**
- **構成要素をチップ上に分散**
- **配線を２つ以上の層に分散**

処理を行なう。

[5] **国際標準** ISO 13491-1 (Banking – Secure cryptographic devices (retail) – part1: Concepts, requirements and evaluation methods) **では、安全な暗号デバイスは、攻撃を防ぐ耐タンパー性**（tamper resistance）**のほか、攻撃されたときにこれを感知して反応動作を行なうタンパー反応性**（tamper responsive）**、攻撃されたときにその証跡を記録するタンパー証拠性**（tamper evident）**等の特徴を持つことが必要とされている。本稿ではこれらを総称して耐タンパー性として扱っている。**

・ダミー配線を織り交ぜる
・ROM の上にダミーの全面電極を配置
・できるだけ細かいデザインルールを使用して設計
・酸化しやすい材質でチップを構成し、表面を不活性ガスで封入
　――不活性ガスの覆いが無くなると腐食が進み、回路が破損
・ホイートストンブリッジ
　――チップ上にホイートストンブリッジ回路を組み込むことによって、回路に物理的な変更が加えられたときにこれを感知し、データを電気的に消去
・特別な材質の保護層により紫外線、X 線、電磁波による改竄を防止
・EEPROM に格納されているデータに対するハッシュ値を保存
　――EEPROM の内容が改竄され、保存されているハッシュ値と合わない場合は動作停止

(b)論理レベルの対策

不適切な電気信号や電源電圧印加による IC 動作の制御、探針による電気信号読み取り、等に対する防止技術。

・低周波検知回路
・温度センサ
・電圧電流のモニタ回路
・紫外線検出回路
・メモリのパリティチェック機能
・二度同じ計算を行ない計算結果をチェック
・計算処理する際に、計算前に乱数による撹乱処理、計算後に撹乱解除処理を行なうなどにより、タイミング･アタック、電力差分アタックを防ぐ（ブラインド署名の手順を応用）。

(c)構造レベル

プロセッサ、コプロセッサ、メモリアクセス制御回路などの機能およびその構成の解読に対する防止技術。

・OS や開発ツールを独自化
・チップ／CPU 等の専用化

(d)運用レベル

カードの詳細情報の守秘管理やカード発行管理、カードの有効期限設定、旧カードの回収／無効化などの IC カードのライフサイクル管理や運用面から施した安全対策。

・IC カードの短期更新
・リトライの回数制限
・上限金額の設定や、取引相手や用途等の利用制限
・取引の追跡監視、取引履歴を使用したシャドウバランスチェック

(3)耐タンパー技術の安全性

IC カードの耐タンパー性を攻撃するための解析技術は、半導体製造・検査技術と密接な関係にあり、多額のコストをかけて半導体製造・検査を行う最新の装置を用意する等を行えば、攻撃が可能となるとの見方が多い。

IC カードの攻撃方法は、主に(1)物理的構造解析と(2)論理的データ解析にわけられる。物理的構造解析は IC チップの構造やそこに記憶されているデータを、外部から回路等を直接観察することによって解析する方法である。観察するためには通常、チップの表面を露出させる等の物理的に手を加えることが必要となる。一方、論理的データ解析とは、正常時／異常時等の IC 回路の動作状態の変化を観察する等によって、内部の情報を推測する解析方法である。意識的に故障を起こしたときの状態の変化や、実装することによって初めて表れてくる暗号処理の特徴等を利用して秘密情報を抽出する方法などがある。

(a)物理的構造解析

①静的解析

チップを取出した後、表面あるいは裏面を研磨したのち、HNO_3 を数滴たらし、エポキシ樹脂が溶け出してきたところをアセトンで洗浄という処理を繰り返すことによってチップ表面を露出し、光学顕微鏡等によって、回路がどのようになっているかを調べるもの。実際には、これだけでは回路のおおよそのパターンを読み取る程度のことしかできない。

②動的解析

実際にチップを動作させ、電子顕微鏡やマニュアル・プローバ（探針）等により、データバス上の電流の流れや ROM、EEPROM 等のメモリ等の各ビットの電位を測定する方法。また、半導体メーカーがチップ製造時の不良品検査を容易化するために組み込まれた試験回路を使用して解析を行なう方法も存在する。なお、この試験回路は通常は耐タンパー性を高めるために切り離されているが、これも FIB (Focussed Ion Beam）等を使ったリペア技術によって復活させることは可能。

(b)論理的データ解析

①しらみつぶし

IC カードにアクセスするための暗証番号等のすべての組み合わせについて、しらみつぶしに施行を試みることによって、秘密情報等を入手する方法。

②故障利用攻撃（Differential Fault Analysis あるいは Fault Based Attack）

IC カードの動作中に、放射線／高電圧／高周波等の物理的影響を故意に与えることにより、意識的に故障を起こすことによって誤動作を生じさせ、誤った計算結果と正しい計算結果からデバイス内に格納されている秘密情報を推定する方法。この攻撃のアイディアは、最初、Boneh[1996]らによって発表され、続いて多くの暗号研究者が意図的に起こした様々な故障を前提に、秘密鍵等の情報を導出することができることを論文発表している。誤動作としては紫外線や電気的刺激により IC・メモリやレジスターの特定のビットを書換／消

去／反転する方法[6]、クロック周波数を操作することにより命令コードを一つづつ実行したり、特定のコードをスキップしたり、処理を不完全に終了する方法、などがあり、実際に誤動作を起こすこと自体は難しいことではないと考えられるが、意図した誤動作を生じさせるようにどの程度コントロールできるかについては議論のあるところである。

③タイミング・アタック（Timing Attack）

使用する秘密鍵によって計算時間が異なることに着目し、計算処理時間を観察･分析することによって秘密情報を抽出する方法。Kocher[1995]によって発表された。暗号の種類やプログラミングの組み方などのシステムのデザインや実装の仕方に依存した攻撃法であり、後述の電力差分攻撃の基礎となった考え方でもある。RSA を実装した IC カードの中の秘密鍵を推測する場合を例に、その攻撃法の考え方を以下に示す。

（アタックの前提）

・攻撃者は攻撃目標のシステムのデザインに関する知識を持つ（タイミング情報を観察・分析することによって推測できる場合もある）。
・平文、公開情報、計算時間等の攻撃に必要な情報は、盗聴によって得られる。
・比較分析用の任意の鍵で処理する場合のタイミングの計測サンプルは、シミュレーション等により得られる。

[6] IC メモリの種類による書き換えの容易さの違いは以下のとおり。

メモリの種類		特徴	格納データ	不正な書き換えの容易さ
RAM		読み書き可能、揮発性	実行時のワーキングエリア等。	電気的に書換可能
ROM (マスク ROM)		読取専用、不揮発性	変更することのないプログラムコードや固定データ。すべての IC カード共通の固定鍵等。	非常に困難。
PROM	EPROM	通常は読取専用だが、特殊な書込動作により消去・書き換えも可能、不揮発性	プログラムコードやデータ。変更可能な鍵。個々の IC カード固有の秘密鍵等。	紫外線により消去可能
	EEPROM			電気的に書換可能

（タイミング・アタック＜対 RSA＞の手順の例）

RSA の計算式、$R = y^x \bmod n$（ただし、x：秘密鍵、y：平文、R：暗号文、n：公開情報＜公開鍵の一部＞）を、実際に IC カードに実装するプログラミング方法にはいくつかあるが、代表的なものとして剰余乗算の繰り返し[7]によって行なう場合を例に説明する。計算処理フローは以下のとおりになる。

Let $S_0 = 1$.
For $k = 0$ *upto* $w-1$: ：ビット長（w）回数繰り返す
  If (bit k of x) is 1 *then*
    Let $R_k = (S_k \cdot y) \bmod n$. ：秘密鍵 x の第 b ビットが 1 の場合の処理
  Else
    Let $R_k = S_k$. ：秘密鍵 x の第 b ビットが 0 の場合の処理
  Let $S_{k+1} = R_k^2 \bmod n$.
EndFor （ただし、w はビット長）
Return (R_{w-1}).

つまり、この計算処理ルーチンでは、秘密鍵 x の第 b ビットが 1 の場合は $R_b = (S_b \cdot y) \bmod n$ が計算され、反対に 0 の場合は $R_b = S_b$ と値が代入されるので、$(S_b \cdot y) \bmod n$ が時間のかかる計算であれば、処理にかかる時間を計測することにより、秘密鍵 x の第 b ビットの値を知ることができるというもの。

実際には、鍵のビットを 0 と推測した場合と 1 と推測した場合の 2 通りについて、推測した鍵で計算した複数のサンプルと、盗聴等によって収集したデータの計測時間の差の分散を比較し、分散の小さい方の推測したビットが正しいとみなすことを、鍵のすべてのビットに対して繰り返し行なうことにより、鍵の全ビットを導き出す。なお、RSA の計算式を IC カードに実装する際に使用する計算アルゴリズムによっては、さらに効率的な攻撃方法が存在する場合もある。

④電力差分攻撃（Differential Power Analysis）

使用する秘密鍵の値によって生じる計算の種類や処理量の違いにより、消費電力が異なることに着目し、消費電力や発生する電磁波を観察・分析することによって秘密情報を抽出する方法。アイデア自体は以前より半導体メーカー等の関係者の間で認識されていたものであるが、1998 年に Kocher によって具体的な攻撃方法として発表されたことから、一般にも知られるところとなった。タイミング・アタック同様、暗号の種類やプログラミングの方法などのシステムのデザインや実装の仕方に依存した攻撃法である。さらに、複数の計測手段を用いた観察結果を利用した分析を行なう HO-DPA（High-Order Differential Power Analysis）も提案されている。以下に DES を実装した IC カードを例に、暗号鍵を推測する考え方を示す。

[7] $R = y^x \bmod n$ は以下のように、剰余乗算の繰り返しに展開可能。
$= y \wedge (x_0 \cdot 2^{w-1} + x_1 \cdot 2^{w-2} \cdot \cdots \cdot x_{w-2} \cdot 2^1 + x_{w-1} \cdot 2^0) \bmod n$
$= (y \wedge x_0 \wedge 2^{w-1})(y \wedge x_1 \wedge 2^{w-2}) \cdot \cdots \cdot (y \wedge x_{w-2} \wedge 2)(y \wedge x_{w-1} \wedge 2^0) \bmod n$
$= ((\cdots(((y \wedge x_0 \bmod n)^2 \cdot y \wedge x_1 \bmod n)^2 \cdot y \wedge x_2 \bmod n)^2 \cdot \cdots \cdot \bmod n)^2 \cdot y \wedge x_{w-2} \bmod n)^2 \cdot y \wedge x_{w-1} \bmod n$
（ただし、w はビット長、x_k は x の第 k ビットの値）

（アタックの前提）

・攻撃者は攻撃目標のシステムのデザインに関する知識を持つ（実際には消費電力等の情報を観察・分析することによって推測することが可能と考えられる）。

・暗号文、消費電力等の攻撃に必要な情報は、手元で実際に IC カードに処理を行なわせ、これを計測することによって得られる。

（電力差分攻撃＜対 DES＞の手順の例）

攻撃は①データ収集と②データ解析の２フェーズにわけられる。

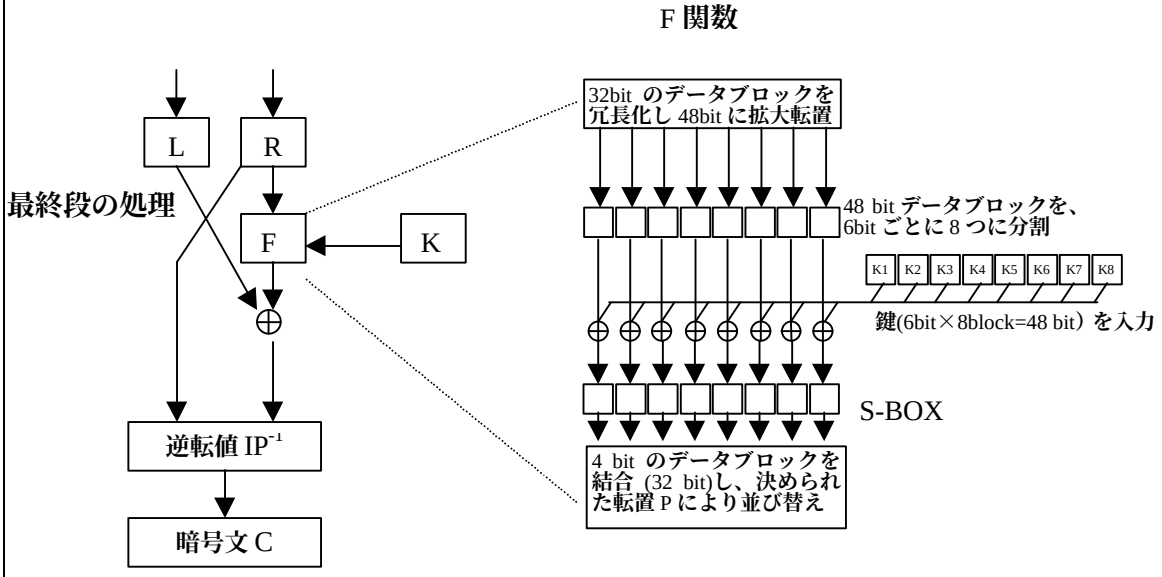
①データ収集

最後の数段の計算について 10 万ヶ所の時系列の計測点を設け、1 千回の暗号処理サンプルについて電力消費量の計測値を収集。

②データ分析

DES による暗号化処理における最終段の 6 ビットのサブキーKi を統計的処理を使った分析により推測し、これを 8 回繰り返すことで 48 ビットの最終段の鍵 K を導出。鍵スケジュールを逆に辿ることにより鍵の 48 ビット分を復元できるほか、さらに前の段について同様の処理を行なうか、残りの 8 ビットをしらみつぶしに探索することで暗号鍵を導出。

分析は、F 関数の出力と L の排他的論理和演算に着目。排他的論理和演算の結果のうちサブキーKi の影響を受けるビットが、これに対応する L のビットと同じ値である場合に、電力消費量に区別可能な差が生じることを利用。具体的には差分平均を求め、該当する部分のビットにバイアスが表れている場合の Ki が正しい値と推測される（正しくない Ki の値の場合、差分平均は 0 となる）。



Ⅲ.電子マネーの安全性評価

1.安全性評価の対象とその方法

電子マネーは暗号技術や耐タンパー技術等の様々な要素技術を組み合わせて構成することによって、その安全性を実現している。しかしながら、第Ⅱ章でも述べたとおり、これらの要素技術は絶対的な安全性を持っているとは限らない。従って、実際に実用に耐える電子マネーを構築するためには、こうした個々の要素技術の安全性が期待された通りでない場合でも、全体としては必要な安全性を保つことができ、システム崩壊に繋がらないように工夫を施しておくことが必要である。

個々の要素技術のうち暗号技術については、多くの場合そのアルゴリズムが公開され、オープンな場で多くの研究者による安全性に関する議論が行なわれている。この議論の過程で何らかの問題があるとされる暗号は淘汰されていったのに対し、多くの研究者による研究対象となったにも関わらず、現在もさほど大きな問題が見つかっていない暗号は、多くの信頼を得て安全と考えられるようになっていることから、適当なアルゴリズムを選択し、十分な鍵長を設け、安全を見込んで鍵の有効期間を設定する等、適切な運用等を行なっていれば必要なレベルの安全性を確保することは可能と考えられる[8]。これに対し、IC カードの耐タンパー性については、現状では、メーカー等の技術情報開示がほとんどなく、オープンな場で安全性に関する議論が尽くされているとは言い難い。従って、その安全性を客観的に評価することが困難であり、予めどの程度のリスクを見積もっておくべきか判断することが困難である。

そこで、個々の要素技術のうち、IC カードの耐タンパー性に頼ることなく電子マネーを構成した場合、その論理的な構成方法の違いによって、電子マネーの安全性にどのような差が出てくるのかを、発生し得るリスクの種類、程度、範囲の分析を行なうことによって評価する。このような評価結果は、逆に、耐タンパー装置がどのような場合に必要となるか、また、その耐タンパー装置に要求される安全性の強度はどの程度か等、電子マネーの総合的な安全性のレベルを上げるために追加的に組み合わせるべき手段の検討に利用できるものである。なお、ここで評価の対象とするのは、特に「価値を不正に手に入れる行為」に対する安全性であり、決済を妨害したり電子マネーのシステム自体を破壊しようとする行為などに対する安全性は対象としない[9]。また、「価値を不正に手に入れる行為」であっても、電子マネーの入った IC カード自体を盗んで使用するといった類の不正行為については、通常のお金と同じ物理的な盗難に対する安全対策の問題であり、電子マネー固有の事情ではないため、直接の検討対象外とする[10]。

評価は、具体的には、電子マネーをいくつかのモデルタイプに分け、例えば、利用者のもと

---

[8] 暗号技術については、そのリスクを見積もった上で、鍵長を長くしたり、鍵の有効期限を短くする等の運用を行なえば、必要なレベルの安全性を確保することができると考えられる。

[9] 電子マネーが広く普及し、決済手段として重要な位置付けとなった場合には、サービスが停止することは、経済活動にとって大きな混乱を招くことになる。そのため、サイバー・テロリズム等のシステムを破壊しようとする行為に対する安全対策も重要な問題であるが、これについては、情報セキュリティ技術のみならず、本稿とは異なる観点からの検討も必要となるため今回は検討の対象外とした。

[10] IC カード盗難に対する対策としては、IC カードにパスワードを設定しておき、第 3 者による使用を防止する方法や、電子マネー受入れ端末に盗難 IC カード番号のリストを配布しておき、使用時にチェックする方法などが考えられている。

に存在する情報を使ってどのような不正を行なうことができるのか（防止）、それはシステムを管理するものにとって検知できるものなのか（検知）、不正を検知したときに被害をとどめるための対策はあるのか（抑制）、といった観点[11]から発生し得るリスクの種類、程度、範囲を分析することによって行なう。評価の結果は、利用者のもとに存在するデータを不正には利用できないようにICカード等の耐タンパー機器に閉じ込める必要があるかどうか、また、その強度はどれくらいかを判断する材料とすることができるため、その分析例等も示す。

電子マネーをいくつかのモデルに分類しその安全性を評価するにあたっては、必ずしも具体的な電子マネープロジェクトや論文は想定せず、一般的な電子マネー全てに対して適応可能な結論を導出することを目的とする。そのため、電子マネーのセキュリティに影響を与える主要な技術的特徴や機能について、考えられる選択肢の全ての組み合わせを候補として挙げ、その中で現実的に有り得るものを評価の対象モデルとすることにする。

2.電子マネーの技術的特徴とモデルの形成

電子マネーの技術的特徴の主なものとしては、(a)電子マネーの価値の形態、(b)転々流通性の有無、(c)価値情報の管理場所、(d)センター接続の有無、(e)使用する暗号技術、などが考えられる。ここでは(a)～(d)の項目の組み合わせをもとに考え得るモデルを示し、それぞれについて(e)の使用する暗号技術の選択の仕方によって、安全性がどのように変化するかを評価することにする。

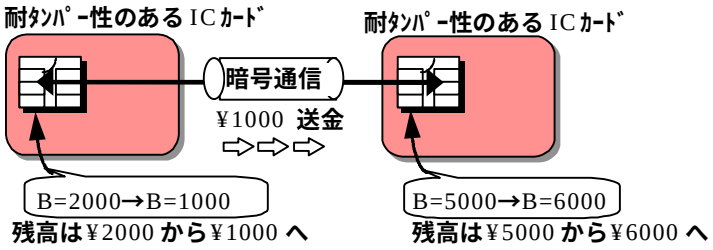
(1)モデル形成に使用する電子マネーの技術的特徴

(a)電子マネーの価値の形態

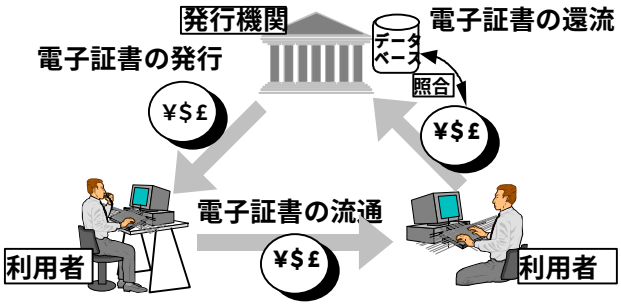
残高管理型：電子財布等に充填されている残高金額を管理（度数管理）する方法で、取引の都度、この残高情報の更新により、支払いや受取りを処理（図3参照）。

電子証書型：個々の電子マネーが額面金額、識別番号等の情報を持ち、それぞれを区別することができるもので、これを受け渡すことによって支払いや受け取りを処理（図4参照）。

（図3）残高管理型の価値移転方法の一例



（図4）電子証書型の価値移転方法の一例

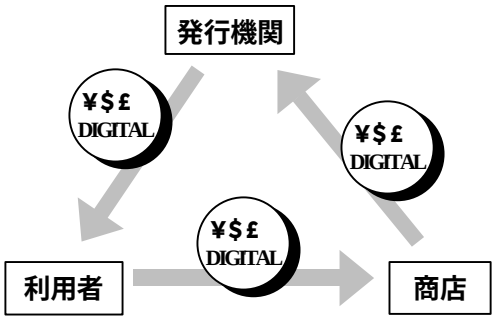


[11] BIS[1996]では、電子マネーのセキュリティ対策は「不正を未然に防ぐこと」（防止）、「不正の発生の検出、あるいは不正の特定ないし追跡」（検知）、「不正が確認されたときに、これ以上被害が広がらないように二次的な対策を講じること」（抑制）に分けられるとしている。

(b)転々流通性の有無

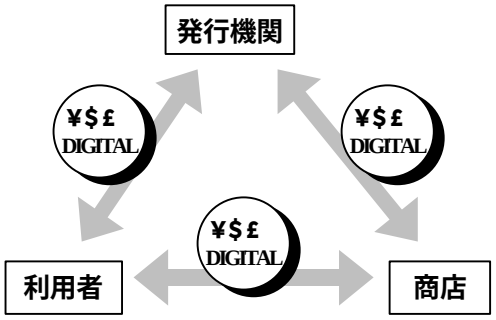
利用者から利用者へセンターを介在することなく、電子マネーの譲渡が可能かどうかによってオープンループ型とクローズドループ型に分類（図 5，6 参照）。

（図 5）closed-loop 型



※ closed-loop 型では、電子マネーの流れは一方向で、利用者と商店は機能的に異なる。

（図 6）open-loop 型



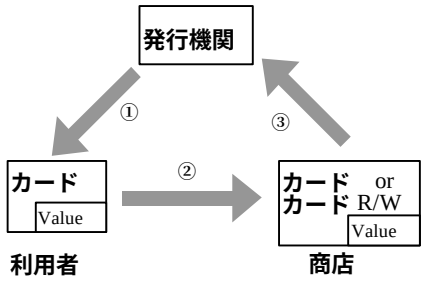
※ open-loop 型では一般の利用者と商店の間には機能的な差はほとんどなく、商店も利用者の一つ。電子現金が利用者間を延々と流通し続け、なかなか発行機関に還流しないことが有り得る。

(c)価値情報の管理場所

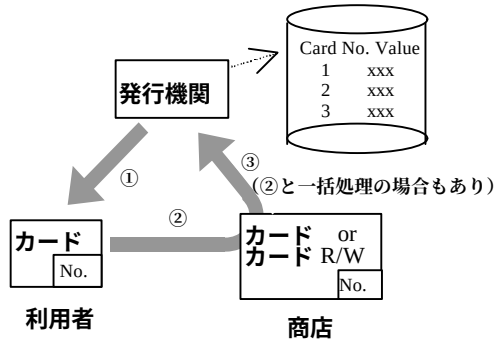
電子財布内（ローカル）で価値を管理する方法、センター（例えば電子マネーの発行機関）において価値を管理する方法、あるいはそれらの双方を併用するタイプに分類（図 7，8 参照）。

(d)センター接続の有無

（図 7）ローカル管理＜残高管理型＞の例



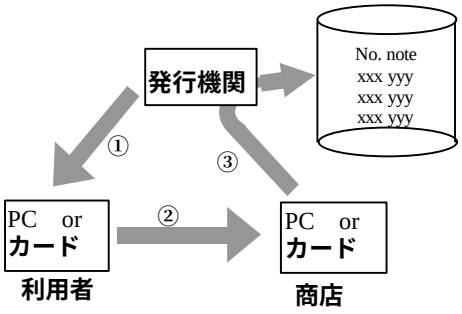
（図 8）センター管理＜残高管理型＞の例



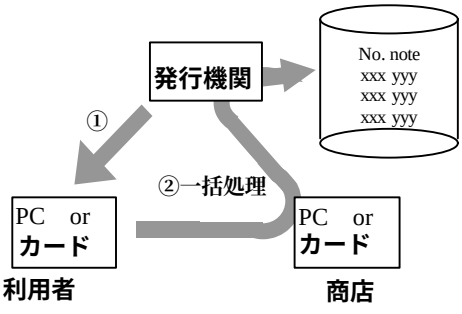
取引をオフラインで行なうことができるか、あるいは必ずオンラインでセンターに問合せを行なう必要があるかによって分類（図 9，10 参照）。

(2)**電子マネーモデルの形成**

（図 9）オフライン＜電子証書型事後検証＞の例



（図 10）オンライン＜電子証書型即時検証＞の例



こうした技術的特徴をもとに全ての組合わせについて、その安全性を検討するわけであるが、センターで価値を管理するためにはセンター接続が必須の条件になるとか、電子証書型では価値管理場所がローカルしかありえないなど、現実的には矛盾あるいは無意味な組み合わせもあり、必ずしも全ての電子マネーが存在するわけではない。各組み合わせにおける電子マネーの有無を示したものが表 1-1、1-2 であり、実際には残高管理型 6 種類、電子証書型 3 種類が実現可能なモデルとして残る（以下、それぞれのモデルを表 1-1,1-2 に示す通り、型Ⅰ～Ⅶ、Ⅰ'、Ⅲ'と呼ぶことにする）。なお、現在、各地で実証実験／実用化が進められている電子マネーの中には、セキュリティ仕様を明らかにしていないものも多いが、それらも上記のモデルのいずれかに該当すると推定できる。

（表 1-1）電子マネーのモデル類型＜残高管理型＞

流通形態	クローズドループ						オープンループ					
価値管理場所	ローカル		併用		センター		ローカル		併用		センター	
センター接続	Off	On	Off	On	Off	On	Off	On	Off	On	Off	On
モデル有無	○ 型Ⅰ	○ 型Ⅰ'	○ 型Ⅱ	○ 型Ⅲ'	× (※1)	○ 型Ⅲ	○ 型Ⅳ	× (※2)	× (※1)	× (※2)	× (※1)	× (※2)

（表 1-2）電子マネーのモデル類型＜電子証書型＞

流通形態	クローズドループ						オープンループ					
価値管理場所	ローカル		併用		センター		ローカル		併用		センター	
センター接続	Off (事後)	On (即時)	Off	On	Off	On	Off (事後)	On (即時)	Off	On	Off	On
モデル有無	○ 型Ⅴ	○ 型Ⅵ	× (※3)	× (※3)	× (※3)	× (※3)	○ 型Ⅶ	× (※2)	× (※3)	× (※3)	× (※3)	× (※3)

※1 センターにオンライン接続せずにセンターで残高を管理することは不可能。

※2 オープンループ型は「利用者から利用者にセンターを介在せずに価値を移転することができるもの」であり、この意味で取引の都度、センターに接続し情報のやり取りがあるものはオープンループとはいえない。

※3 電子証書型は、データ自体が価値を持つとのコンセプトで作られている方法であるため、価値管理場所はローカルしかあり得ない。

(3)各電子マネーモデルに適用される暗号技術の選択肢

各電子マネーモデルで利用される暗号技術としては、大きくわけると共通鍵暗号を利用したもの、公開鍵暗号（ないしディジタル署名方式）を利用したもの、その中間的なものの３種類が考えられる。本稿では (2)で検討した実現可能な電子マネーモデルに対し、これらの暗号技術を利用した取引手順の典型的なものを前提に、安全性を評価することにする。なお、残高管理型と電子証書型では実現方式の違いにより暗号技術の利用の仕方が異なるため、選択肢の内容は以下のようにそれぞれ異なる。

（残高管理型）

共通鍵型：本人確認およびデータ送受信に共通鍵暗号を使用する方式。

共通鍵型＜静的認証あり＞：データ送受信に共通鍵暗号を使用するが、本人確認はセンターの秘密鍵によってディジタル署名された証明書の提示による方式。

公開鍵型＜動的認証あり＞：本人確認を公開鍵暗号を利用した動的認証（支払時にチャレンジ＜店名、金額、時刻等＞に対するディジタル署名を生成）によって行なう方式。さらに、データ送受信にも暗号を使うこともある。

（電子証書型）

共通鍵型：本人確認およびデータ送受信に共通鍵暗号を使用し、発行機関が割り当てた識別番号等を含む電子証書（ディジタル署名なし）を送信することによって、価値を移転する方法。

公開鍵型＜静的認証あり＞：本人確認をセンターの秘密鍵によってディジタル署名された証明書の提示によって行なう方法。なお、電子証書自体もセンターの秘密鍵によってディジタル署名される（ブラインド署名を使用することを仮定）。

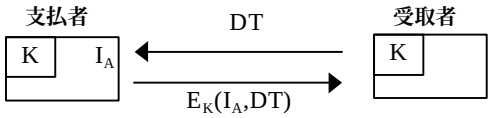
公開鍵型＜動的認証あり＞：本人確認を公開鍵暗号を利用した動的認証（支払時にチャレンジ＜店名、金額、時刻等＞に対するディジタル署名を生成）によって行なう方式。なお、電子証書自体はセンターの秘密鍵によってディジタル署名される（ブラインド署名を使用することを仮定）。

本稿で検討する前提となる、利用する暗号技術の選択肢ごとの取引手順を図 11、12 に示す。なお、こうした暗号技術等により、電子マネーは原則、誰に発行した電子マネーがどのような経路で流通して、還流してきたのかを追跡することが不可能なように匿名性を実現[12]している。

[12] 残高管理型の電子マネーは、受け渡される価値はすべて残高情報として一括管理され、どこから受け取った価値か区別がつかないため完全な匿名性を持つ（電子財布自体には区別するための識別番号があるが、必ずしもセンターは誰にどの電子財布を発行したかを管理する必要はない）。一方、電子証書型の電子マネーは個々が区別できる個性を持つものであるが、発行処理の際に公開鍵暗号を使ったブラインド署名を使用することによって、発行機関が誰に発行した電子マネーかを認識できないようにすることによって匿名性を実現するともに、同時に二重使用が行なわれた場合にのみ電子マネーに含まれている利用者を識別する情報が露見する仕組みを実現可能。なお、電子証書型電子マネーのうち共通鍵型については、本稿で想定した方法だけでは、このような仕組みを実現することができないため、匿名性を実現していない。

（図 11）残高管理型の暗号技術の選択肢と取引手順

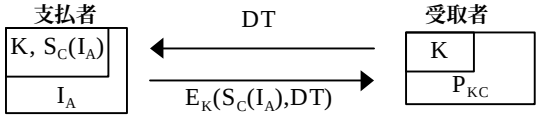
共通鍵型



発行機関＜センター＞保有情報）
K :共通秘密鍵

①受取者は、要求金額および現在時刻等 DT をチャレンジとして支払者に送信。
②支払者は、共通秘密鍵 K を用いて識別子 I_A, 要求金額および現在時刻等 DT を暗号化することによって支払情報 $E_K(I_A,DT)$を作成し、受取者に送信するとともに、保有残高を減額。
③受取者は、受け取った支払情報を共通秘密鍵 K を使って復号し、予め送付した DT が含まれることを確認した後、保有残高を増額。

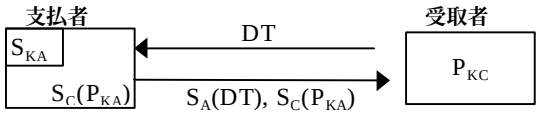
共通鍵型＜静的認証あり＞



発行機関＜センター＞保有情報）
K :共通秘密鍵
$S_{KC,}$ P_{KC}:**センターC の秘密鍵、公開鍵**

①受取者は、要求金額および現在時刻等 DT をチャレンジとして支払者に送信。
②支払者は、共通秘密鍵 K を用いて、センターの証明書 $S_C(I_A)$, 要求金額および現在時刻等 DT を暗号化することによって支払情報 $E_K(S_C(I_A),DT)$を作成し、受取者に送信するとともに、保有残高を減額。
③受取者は、受け取った支払情報を共通秘密鍵 K を使って復号し、センターの証明書をセンターの公開鍵 P_{KC} を使って検証するとともに、予め送付した DT が含まれることを確認した後、保有残高を増額。

公開鍵型＜動的認証あり＞



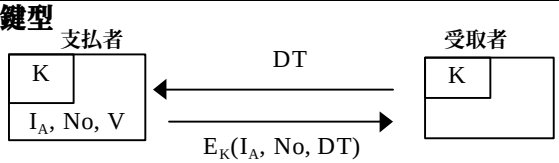
発行機関＜センター＞保有情報）
$S_{KC,}$ P_{KC}:**センターC の秘密鍵、公開鍵**

①受取者は、要求金額および現在時刻等 DT をチャレンジとして支払者に送信。
②支払者は、秘密鍵 S_{KA} を用いて要求金額および現在時刻等 DT を署名することによって支払情報 $S_A(DT)$を作成し、公開鍵証明書 $S_C(P_{KA})$とともに受取者に送信すると同時に、保有残高を減額。
③受取者は、受け取った支払情報を、センターの公開鍵 P_{KC} を使って公開鍵証明書から取り出した支払者の検証鍵 P_{KA} によって検証し、保有残高を増額。

K：共通秘密鍵（システムで一意）
$E_K(X)$：データ X を鍵 K で暗号化
I_A：利用者 A の匿名の識別子
P_{KA}, P_{KB}：利用者 A,B の公開鍵
S_{KA}, S_{KB}：利用者 A,B の秘密鍵
$S_C(X)$：センターC によるデータ X への署名
$S_A(X)$：利用者 A によるデータ X への署名
P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
DT：店名、金額、時刻等

（図 12）電子証書型の暗号技術の選択肢と取引手順

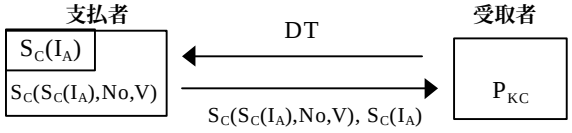
共通鍵型



発行機関＜センター＞保有情報）
K :共通秘密鍵

①受取者は、要求金額および現在時刻等 DT をチャレンジとして支払者に送信。
②支払者は、共通秘密鍵 K を用いて、支払いに使用する（＝要求金額が額面金額 V に一致する）電子証書識別番号 No, 利用者の識別子 I_A, 要求金額および現在時刻等 DT を署名することによって支払情報 $E_K(I_A, No, DT)$を作成し、受取者に送信。
③受取者は、受け取った支払情報を共通秘密鍵 K を使って検証。

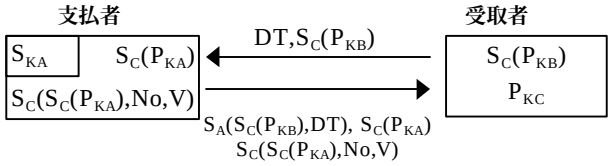
公開鍵型＜静的認証あり＞



発行機関＜センター＞保有情報）
S_{KC}, P_{KC}:**センターC の秘密鍵、公開鍵**

①受取者は、要求金額等 DT を支払者に送信。
②支払者は、支払いに使用する（＝要求金額が額面金額 V に一致する）電子証書 $S_C(S_C(I_A), No, V)$を選択し、センターの証明書 $S_C(I_A)$とともに受取者に送信。
③受取者は、受け取った電子証書およびセンターの証明書を公開鍵 P_{KC} を使って検証。

公開鍵型＜動的認証あり＞



発行機関＜センター＞保有情報）
S_{KC}, P_{KC}:**センターC の秘密鍵、公開鍵**

①受取者は、要求金額および現在時刻等 DT および受取者の公開鍵証明書 $S_C(P_{KB})$をチャレンジとして支払者に送信。
②支払者は、支払いに使用する（＝要求金額が額面金額 V に一致する）電子証書 $S_C(S_C(P_{KA}), No, V)$を選択し、さらに受取者の公開鍵証明書 $S_C(P_{KB})$、現在時刻等 DT に署名して作成した譲渡証 $S_A(S_C(P_{KB}),DT)$とともに、受取者に送信。
③受取者は、受け取った電子証書と譲渡証を公開鍵 P_{KC} を使って検証。

K：共通秘密鍵（システムで一意）
$E_K(X)$：データ X を鍵 K で暗号化
I_A：利用者 A の匿名の識別子
P_{KA}, P_{KB}：利用者 A,B の公開鍵
S_{KA}, S_{KB}：利用者 A,B の秘密鍵
$S_C(X)$：センターC によるデータ X への署名
$S_A(X)$：利用者 A によるデータ X への署名
P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
DT：店名、金額、時刻等
V：額面金額

3．電子マネーの安全性評価の前提条件と評価項目

電子マネーの安全性評価を行なうにあたっては、不特定多数の利用者が不特定多数の商店で電子マネーを用いて支払う状況を想定する。そして、各利用者、商店が、自ら保有する IC カード（耐タンパー性なし）やコンピュータの記憶装置の中にある電子マネーに関する情報を読み出して、これを利用することによって、どのような不正行為を行なうことができるのかを分析する。また、発行機関（含む登録機関）のセキュリティ対策が不十分であったり、内部者による犯行が可能であるとの仮定のもと、保有する秘密鍵等の情報が外部に漏れた場合、それによってどのような不正が行なえるのかについても分析する。

安全性の評価は、本章で整理した実現可能なモデルに対し、それぞれ 3 通りの暗号技術を適用した電子マネー実現方式を想定し、考えうる不正の種類（偽造、変造、複製、搾取等）、不正検知の可否（不正が生じている事実の検出、不正の発生箇所を特定）、さらに検知できた場合には不正行為を抑制するための対応策の有無を分析することによって行なう。特に、利用者が支払情報を偽造する場合については、他人に成りすますかたちでの不正ができるかどうかという観点からも安全性のレベルを区別するほか、商店が還流情報を偽造できないと判断された場合についても、他の利用者と結託することによって不正が可能になるのかについて評価する。なお、使用する共通鍵暗号、公開鍵暗号、ディジタル署名方式は、適切なアルゴリズムを利用し、十分な鍵長を設定しているため安全であり、解読や署名の偽造はないものと仮定する。

安全性の分析を行なう項目およびその内容は以下のとおり。

①支払情報の偽造（利用者が保有する情報を利用した不正行為）

利用者が自ら保有する秘密情報を利用することにより、支払情報を偽造して商店に受け渡す不正行為。偽造された支払情報が本来の利用者本人としてのものか（**支払情報の偽造１＜本人＞**）、ある特定の利用者としての支払情報を偽造したものなのか（**支払情報の偽造２＜特定＞**）、任意の利用者（実在しなくてもよい）としての支払情報を偽造したものなのか（**支払情報の偽造３＜不特定＞**）によって、不正行為の追跡が可能かどうかの差が生じるため、これを特に区別する。

②還流情報の偽造（商店の保有する情報を利用した不正行為）

商店が利用者から受け取った売上げ（受取情報）を偽造して、銀行に還流させることにより、価値を入手する不正行為（**還流情報の偽造<結託なし>**）。商店と銀行の間の取引は匿名性がない状態で行なわれるため、商店はやり逃げタイプの不正を行なうことは不可能。なお、商店が特定の利用者と結託し、利用者の保有する秘密情報も利用することによって、初めて実行可能になる不正行為（**還流情報の偽造<結託あり>**）についても分析する。

③発行機関＜含む登録機関＞の情報を利用した偽造（発行機関の情報を入手した不正行為）

不正行為者が、発行機関＜含む登録機関＞の保有する秘密情報を不正に手に入れ、これを利用して発行情報ないし支払情報を偽造することによって、価値を手に入れる不正行為。発行機関による秘密鍵等の情報管理が脆弱であったり、内部者による不正行為が可能な場合に想定される偽造である。

4．評価結果

各電子マネーモデルに対して、(1)支払情報の偽造、(2)還流情報の偽造、(3)発行機関の情報を使った偽造について分析・評価した。

以下は、残高管理型４種類（残高管理型・ローカル管理・クローズドループ、残高管理型・センター管理ローカル管理併用・クローズドループ、残高管理型・センター管理・クローズドループ、残高管理型・ローカル管理・オープンループ）、電子証書型３種類（電子証書型・事後検証・クローズドループ、電子証書型・即時検証・クローズドループ、電子証書型・事後検証・オープンループ）について、分析･評価を行った結果である。

なお、型Ⅰ’（残高管理型、ローカル管理、クローズドループでセンター接続するもの）、については、本稿の検討の範囲で安全性を評価する観点からは、センター接続する必然性が認められず、型Ⅰと同様の結果となったため、そちらを参照されたい。

また、型Ⅲ’（残高管理型、センター管理・ローカル管理併用、クローズドループでセンター接続するもの）については、技術的には型Ⅱ（残高管理型、センター管理・ローカル管理併用、クローズドループでセンター接続しないもの）と型Ⅲ（残高管理型、センター管理、クローズドループでセンター接続するもの）を合わせた複合タイプであると考えられる（実装にかかるコスト等は増大）。しかしながら、型Ⅲ’を分析・評価したところ、センター以外にローカルでも冗長に価値を管理することによって特に安全性のレベルが向上しているわけではなく（不正行為者が攻撃を行う手間は増加するものの安全性のレベルは変化しない）、型Ⅲと同様の結果となったため、そちらを参照されたい。

(1)**支払情報の偽造**

(a)**型Ⅰ（残高管理型、ローカル管理、クローズドループ）　――支払情報の偽造――**

【共通鍵型】IC カード等[13]の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額、任意の識別 ID（架空の ID も可能）を含む、支払情報 $E_K(I_A^*,DT')$を偽造することが可能。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

――― 偽造が大規模に行なわれれば、発行額、還流額の統計的な傾向を監視することにより、不正の疑いを持つことは可能ながら、確証を得ることは不可。

【共通鍵型＜静的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K、証明書 $S_C(I_A)$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、利用者の識別 ID にセンターの署名をつけた証明書については、攻撃者が任意の利用者 A*としての証明書 $S_C(I_A^*)$を作ることは困難（センター署名 S_C の安全性は高い）なため、本人の証明書を使うか、共通秘密鍵 K を使って盗聴等により入手した他人 A'の証明書 $S_C(I_A')$を使って成りすますことのみ可能であり、任意の利用者に成りすまして不正を働くことは困難。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

【公開鍵型＜動的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、電子財布固有の秘密鍵 S_{KA}、公開鍵に対するセンター署名 $S_C(P_{KA})$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、任意の利用者 A*としての支払情報を偽造しようとして、P_{KA}^* ,S_{KA}^*を予め決めてから公開鍵に対するセンター署名 $S_C(P_{KA}^*)$を作ることは、センター署名 S_C の安全性が高いため困難。また、特定の利用者 A'としての支払いを目的に、盗聴等により A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、利用者 A'の支払情報 $S_A'(DT')$を作ることができないため、成りすましは困難。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

（評価結果で使用している記号の意味）

A：攻撃対象の電子財布の利用者	P_{KA}, S_{KA}：利用者 A の公開鍵, 秘密鍵
A'：他の特定の利用者（実在）	Sc(X)：センターC によるデータ X への署名
A^*：任意の利用者（架空でも可）	P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
K：秘密鍵（システムで一意）	DT：店名、金額、時刻等
$E_K(X)$：データ X を鍵 K で暗号化	DT'：任意に指定した店名、金額、時刻等
I_A：利用者 A の識別子	

[13] 電子財布は IC カードのほか、パソコン上で実現されていても構わない。

(b)**型Ⅱ（残高管理型、センター管理・ローカル管理併用、クローズドループ）――支払情報の偽造――**

【共通鍵型】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額、任意の識別 ID（架空の ID も可能）を含む、支払情報 $E_K(I_A^*,DT')$を偽造することが可能。

ただし、各電子財布の残高情報はセンターでも管理されているため、商店から銀行に電子マネーが預けられ、還流情報がセンターに戻ってきた後に、正規の残高以上に不正に支払いを行なった結果、残高がマイナスになっている電子財布を発見することが可能（識別 ID も特定）。さらに、商店の受取端末がホットリストを持ち、これに登録されている不正な識別 ID の電子財布との取引を拒否する仕組みにすれば、被害を抑えることが可能。

【共通鍵型＜静的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K、証明書 $S_C(I_A)$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、利用者の識別 ID にセンターの署名をつけた証明書については、攻撃者が任意の利用者 A*としての証明書 $S_C(I_A^*)$を作ることは困難（センター署名 S_C の安全性は高い）なため、本人の証明書を使うか、共通秘密鍵 K を使って盗聴等により入手した他人 A'の証明書 $S_C(I_A')$を使って成りすますことのみ可能であり、任意の利用者に成りすまして不正を働くことは困難。

ただし、各電子財布の残高情報はセンターでも管理されているため、商店から銀行に電子マネーが預けられ、還流情報がセンターに戻ってきた後に、正規の残高以上に不正に支払いを行なった結果、残高がマイナスになっている電子財布を発見することが可能（識別 ID も特定）。さらに、商店の受取端末がホットリストを持ち、これに登録されている不正な識別 ID の電子財布との取引を拒否する仕組みにすれば、被害を抑えることが可能。

【公開鍵型＜動的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、電子財布固有の秘密鍵 S_{KA}、公開鍵に対するセンター署名 $S_C(P_{KA})$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、任意の利用者 A*としての支払情報を偽造しようとして、P_{KA}^* ,S_{KA}^*を予め決めてから公開鍵に対するセンター署名 $S_C(P_{KA}^*)$を作ることは、センター署名 S_C の安全性が高いため困難。また、特定の利用者 A'としての支払いを目的に、盗聴等により公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、A'の支払情報 $S_A'(DT')$を作ることができないため、成りすましは困難。

ただし、各電子財布の残高情報はセンターでも管理されているため、商店から銀行に電子マネーが預けられ、還流情報がセンターに戻ってきた後に、正規の残高以上に不正に支払いを行なった結果、残高がマイナスになっている電子財布を発見することが可能（識別 ID も特定）。さらに、商店の受取端末がホットリストを持ち、これに登録されている不正な識別 ID の電子財布との取引を拒否する仕組みにすれば、被害を抑えることが可能。

(c)型Ⅲ（残高管理型、センター管理、クローズドループ）――支払情報の偽造――

【共通鍵型】各電子財布の残高情報はセンターで管理され、取引の都度オンラインでチェックされるため、電子財布の正規の残高以上に不正に支払いを行なうことは不可能。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 $I_{A'}$を使ったり、任意に選んだ I_{A}*が存在すれば、その残高を上限に横取りすることが可能。残高を横取りされた利用者の申し出により、不正は発覚するものの、不正行為者の特定は不可能であり、再度同じ利用者が被害を受けるのを防止することができる程度。

なお、支払時にセンター側でパスワードチェックを行なう等の対策を併用すれば、横取りはより難しくなる。

【共通鍵型＜静的認証あり＞】各電子財布の残高情報はセンターで管理され、取引の都度オンラインでチェックされるため、電子財布の正規の残高以上に不正に支払いを行なうことは不可能であるが、共通秘密鍵を使って盗聴した他の利用者 A'の電子財布の証明書 $S_C(I_{A'})$を使うことにより、その残高を上限に横取りすることは可能。なお、攻撃者が任意の利用者 A*としての証明書 $S_C(I_A*)$を作ることは困難なため、不特定の利用者の残高を横取りすることは困難。

残高を横取りされた利用者の申し出により、事後、不正は発覚するものの、不正行為者の特定は不可能であり、再度同じ利用者が被害を受けるのを防止することができる程度。

なお、支払時にセンター側でパスワードチェックを行なう等の対策を併用すれば、横取りはより難しくなる。

【公開鍵型＜動的認証あり＞】各電子財布の残高情報はセンターで管理され、取引の都度オンラインでチェックされるため、電子財布の正規の残高以上に不正に支払いを行なうことは不可能。なお、任意の利用者 A*に成りすまそうと、P_{KA}* ,S_{KA}*を予め決めてから、公開鍵に対するセンター署名 $S_C(P_{KA}*)$を作ることは、センター署名 S_C の安全性が高いため困難。また、特定の利用者 A'に成りすまそうと、A'の公開鍵に対するセンター署名 $S_C(P_{KA'})$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA'})$に対応した秘密鍵 $S_{KA'}$を求めることはできず（公開鍵の安全性は高い）、利用者 A'の支払情報 $S_{A'}(DT')$を作ることができないため攻撃は不成功。

(d)型Ⅳ（残高管理型、ローカル管理、オープンループ）――支払情報の偽造――

【共通鍵型】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額、任意の識別 ID（架空の ID も可能）を含む、支払情報 $E_K(I_A^*,DT')$を偽造することが可能。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

――― 偽造が大規模に行なわれれば、発行額、還流額の統計的な傾向を監視することにより、不正の疑いを持つことは可能ながら、確証を得ることは不可。

【共通鍵型＜静的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K、証明書 $S_C(I_A)$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、利用者の識別 ID にセンターの署名をつけた証明書については、攻撃者が任意の利用者 A*としての証明書 $S_C(I_A^*)$を作ることは困難（センター署名 S_C の安全性は高い）なため、本人の証明書を使うか、共通秘密鍵 K を使って盗聴等により入手した他人 A'の証明書 $S_C(I_A')$を使って成りすますことのみ可能であり、任意の利用者に成りすまして不正を働くことは困難。もっとも、このタイプの電子マネーは転々流通性を持つことから、第３者の電子財布を介在することによって、実質的には偽造価値の使用時の匿名性を保つことが可能であり、不特定な利用者としての攻撃が成功したのと同様の効果。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

【公開鍵型＜動的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、電子財布固有の秘密鍵 S_{KA}、公開鍵に対するセンター署名 $S_C(P_{KA})$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、任意の利用者 A*としての支払情報を偽造しようとして、P_{KA}^* ,S_{KA}^*を予め決めてから $S_C(P_{KA}^*)$を作ることは、センター署名 S_C の安全性が高いため困難。また、特定の利用者 A'としての支払いを目的に、A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、利用者 A'の支払情報 $S_A'(DT')$を作ることができないため、成りすましは困難。もっとも、このタイプの電子マネーは転々流通性を持つことから、第３者の電子財布を介在することによって、実質的には偽造価値の使用時の匿名性を保つことが可能であり、不特定な利用者としての攻撃が成功したのと同様の効果。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

(e)**型Ⅴ（電子証書型、事後検証、クローズドループ）――支払情報の偽造――**

【共通鍵型】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額、任意の識別 ID（盗聴で得た特定の ID の他、架空の ID も可能）を含む、支払情報 $E_K(I_A^*, No, DT')$を偽造することが可能。

なお、支払情報は事後的にセンターに送られてチェックされ、支払情報がデータベースに登録されていない不正なものであることが判明する。ただし、架空の識別 ID 等を使われた場合、この不正行為者を追跡し、被害を抑えることは不可能。

【公開鍵型＜静的認証＞】電子証書を偽造・変造するためにはセンターの秘密鍵による署名が必要であるが、センター署名 S_C の安全性は高く困難。唯一可能な不正は、電子証書を複製し、これを複数回使用するというもの。本人が保有する電子証書を複製して使用した場合は、事後的にセンターでチェックされた結果、不正行為者の識別 ID が判明するので、被害は限定される。他人の電子証書を盗聴（使用時）して、これを使用した場合は、事後的にセンターでチェックされ不正が検知されても、盗聴された利用者の実名が判明するだけで、不正行為者の追跡ができず、被害はとどめることは不可能。

【公開鍵型＜動的認証＞】電子証書を偽造・変造するためにはセンターの秘密鍵による署名が必要であるが、センター署名 S_C の安全性は高く困難。唯一可能な不正は、電子証書を複製し、これを複数回使用するというもの。本人が保有する電子証書を複製して使用した場合は、事後的にセンターでチェックされた結果、不正行為者の識別 ID（公開鍵 P_{KA} と一意に対応）が判明するので、被害は限定される。なお、他人 A'の電子証書および公開鍵に対するセンター署名 $S_C(P_{KA}')$を盗聴により入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、利用者 A'の譲渡証 $S_A'(S_C(P_{KB}'),DT')$を作ることができないため、成りすましは困難。

（評価結果で使用している記号の意味）

A：攻撃対象の電子財布の利用者	$S_C(X)$：センターC によるデータ X への署名
A'：他の特定の利用者（実在）	P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
A^*：任意の利用者（架空でも可）	DT：店名、金額、時刻等
K：秘密鍵（システムで一意）	DT'：任意に指定した店名、金額、時刻等
$E_K(X)$：データ X を鍵 K で暗号化	No：電子証書の識別番号
I_A：利用者 A の識別子	V：電子証書の額面金額
P_{KA}, S_{KA}：利用者 A の公開鍵，秘密鍵	V'：任意に指定した電子証書の額面金額
P_{KB}, S_{KB}：利用者 B(譲渡先)の公開鍵，秘密鍵	

(f)**型VI（電子証書型、即時検証、クローズドループ）――支払情報の偽造――**

【共通鍵型】IC カード等の電子財布中の情報が読み出され、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額、任意の識別 ID（盗聴で得た特定の ID の他、架空の ID も可能）を含む、支払情報 $E_K(I_A^*, No, DT')$を偽造したとしても、オンラインでセンターのデータベースに登録されているかがチェックされるため、不正は不可能。なお、他の利用者が電子マネーを発行してもらう際の情報を盗聴し、センターに登録してある電子証書の登録番号、利用者の識別子、金額等を手に入れ、これを先に使用すれば、横取りすることが可能。後に、正規の持ち主が、この電子証書が使用できないことを知り、不正が発覚するが、この不正を防ぐ根本的な手段はない。

【公開鍵型＜静的認証＞】電子証書を偽造・変造するためにはセンターの秘密鍵による署名が必要であるが、センター署名 S_C の安全性は高く困難。一方、電子証書を複製し、これを複数回使用するという不正についても、センターでオンラインチェックが行われるため不可能。

唯一、他人が使用しようとして送信した電子証書を途中で傍受、即座に使用する一方、正規の支払処理を妨害すること等によって先にオンラインチェックを終えることができれば、横取りが可能と考えられなくもないが、現実的には困難。

――― このタイプの電子証書は発行にはブラインド署名を行なっており、発行時の盗聴によって電子証書を入手することは困難。

【公開鍵型＜動的認証＞】電子証書を偽造・変造するためにはセンターの秘密鍵による署名が必要であるが、センター署名 S_C の安全性は高く困難。また、電子証書を複製し、これを複数回使用しようとしても、センターでオンラインチェックされるため、不正は不可能（この場合、不正が失敗する上、不正未遂者の識別 ID＜P_{KA} と一意に対応＞が発覚）。なお、他人 A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を盗聴により入手し、先に使用しようとしても、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、利用者 A'の譲渡証 $S_A'(S_C(P_{KB}'),DT')$を作ることができないため、成りすましは困難。

(g)型Ⅶ（電子証書型、事後検証、オープンループ）――支払情報の偽造――

【共通鍵型】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額、任意の識別 ID（盗聴で得た特定の ID の他、架空の ID も可能）を含む、支払情報 $E_K(I_A^*, No, DT')$を偽造することが可能。

なお、支払情報は事後的にセンターに送られてチェックされ、支払情報がデータベースに登録されていない不正なものであることが判明する。ただし、架空の識別 ID 等を使われた場合、この不正行為者を追跡し、被害を抑えることは不可能。

【公開鍵型＜静的認証＞】電子証書を偽造・変造するためにはセンターの秘密鍵による署名が必要であるが、センター署名 S_C の安全性は高く困難。唯一可能な不正は、電子証書を複製し、これを複数回使用するというもの。本人が保有する電子証書を複製して使用した場合は、事後的にセンターでチェックされた結果、不正行為者の識別 ID が判明するので、被害は限定される。他人の電子証書を盗聴（使用時）して、これを使用した場合は、事後的にセンターでチェックされ不正が検知されても、盗聴された利用者の識別 ID が判明するだけで、不正行為者の追跡ができず、被害を抑えることは不可能。

【公開鍵型＜動的認証＞】電子証書を偽造・変造するためにはセンターの秘密鍵による署名が必要であるが、センター署名 S_C の安全性は高く困難。唯一可能な不正は、電子証書を複製し、これを複数回使用するというもの。本人が保有する電子証書を複製して使用した場合は、事後的にセンターでチェックされた結果、不正行為者の識別 ID（P_{KA} と一意に対応）が判明するので、被害は限定される。なお、他人 A'の電子証書および証明書 $S_C(P_{KA}')$を盗聴により入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、利用者 A'の譲渡証 $S_A'(S_C(P_{KB}'),DT')$を作ることができないため、成りすましは困難。

(2)**還流情報の偽造**

(a)**型Ⅰ（残高管理型、ローカル管理、クローズドループ）――還流情報の偽造――**

【共通鍵型】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額の還流情報 $E_K(I_A,DT')$を偽造することが可能。また、この偽造した価値は正規の価値と区別できないため、後にこれを検知することは不可能。

【共通鍵型＜静的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K、証明書 $S_C(I_A)$を使うことによって、扱える上限金額内での自由な金額の還流情報を偽造することが可能。また、還流させる価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

【公開鍵型＜動的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、電子財布固有の秘密鍵 S_{KA}、公開鍵に対するセンター署名 $S_C(P_{KA})$を使うことによって、扱える上限金額内での自由な金額の還流情報を偽造することが可能。また、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。なお、電子マネーを受取る際の動的認証のログをセンターに送ってチェックすることにより、還流情報の偽造は困難になるが、利用者との結託攻撃には対応できない。

（評価結果で使用している記号の意味）

A：攻撃対象の電子財布の利用者	$S_C(X)$：センターC によるデータ X への署名
A'：他の特定の利用者（実在）	P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
A^*：任意の利用者（架空でも可）	DT：店名、金額、時刻等
K：秘密鍵（システムで一意）	DT'：任意に指定した店名、金額、時刻等
$E_K(X)$：データ X を鍵 K で暗号化	No：電子証書の識別番号
I_A：利用者 A の識別子	V：電子証書の額面金額
P_{KA}, S_{KA}：利用者 A の公開鍵，秘密鍵	V'：任意に指定した電子証書の額面金額

(b)**型Ⅱ（残高管理型、センター管理・ローカル管理併用、クローズドループ）――還流情報の偽造――**

【共通鍵型】各電子財布の残高情報はセンターで管理されており、還流時にすべてオンラインでチェックされるため、電子財布の正規の残高以上に還流を行なうことは困難。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 $ID_{A'}$を使ったり、任意に選んだ識別 I_{A}*が存在すれば、その残高を上限に横取りすることが可能。もっとも、残高を横取りされた利用者の申し出により、不正の事実および不正行為を行った者の口座が発覚するため、「やり逃げ」しかできない。

なお、他の利用者と結託した攻撃方法も特に存在しない。

【共通鍵型＜静的認証あり＞】各電子財布の残高情報はセンターで管理されており、還流時にすべてオンラインでチェックされるため、電子財布の正規の残高以上に還流させることは困難。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 $I_{A'}$を使ったり、任意に選んだ識別 I_{A}*が存在すれば、その残高を上限に横取りすることが可能。もっとも、残高を横取りされた利用者の申し出により、不正の事実および不正行為を行った者の口座が発覚するため、「やり逃げ」しかできない。

なお、他の利用者と結託した攻撃方法も特に存在しない。

【公開鍵型＜動的認証あり＞】各電子財布の残高情報はセンターで管理されており、還流時にすべてオンラインでチェックされるため、電子財布の正規の残高以上に還流を行なうことは困難。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 $I_{A'}$を使ったり、任意に選んだ識別 I_{A}*が存在すれば、その残高を上限に横取りすることが可能。もっとも、残高を横取りされた利用者の申し出により、不正の事実および不正行為を行った者の口座が発覚するため、「やり逃げ」しかできない。

なお、電子マネーを受取る際の動的認証のログをセンターに送ってチェックすることにより、還流情報の偽造は困難になり、他の利用者との結託攻撃に対しても安全。

(c)**型Ⅲ（残高管理型、センター管理、クローズドループ）――還流情報の偽造――**

【共通鍵型】各電子財布の残高情報はセンターで管理されており、還流時にすべてオンラインでチェックされるため、電子財布の正規の残高以上に還流金額を増やすことは困難。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 I_A'を使ったり、任意に選んだ識別 I_A^*が存在すれば、その残高を上限に横取りすることが可能。もっとも、残高を横取りされた利用者の申し出により、不正の事実および不正行為を行った者の口座が発覚するため、「やり逃げ」しかできない。

なお、他の利用者と結託した攻撃方法も特に存在しない。

【共通鍵型＜静的認証あり＞】各電子財布の残高情報はセンターで管理されており、還流時にすべてオンラインでチェックされるため、電子財布の正規の残高以上に還流金額を増やすことは困難。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 I_A'を使ったり、任意に選んだ識別 I_A^*が存在すれば、その残高を上限に横取りすることが可能。もっとも、残高を横取りされた利用者の申し出により、不正の事実および不正行為を行った者の口座が発覚するため、「やり逃げ」しかできない。

なお、他の利用者と結託した攻撃方法も特に存在しない。

【公開鍵型＜動的認証あり＞】各電子財布の残高情報はセンターで管理されており、還流時にすべてオンラインでチェックされるため、電子財布の正規の残高以上に還流金額を増やすことは困難。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 I_A'を使ったり、任意に選んだ識別 I_A^*が存在すれば、その残高を上限に横取りすることが可能。もっとも、残高を横取りされた利用者の申し出により、不正の事実および不正行為を行った者の口座が発覚するため、「やり逃げ」しかできない。

なお、電子マネーを受取る際の動的認証のログをセンターに送ってチェックすることにより、還流情報の偽造は困難になり、他の利用者との結託攻撃に対しても安全。

(d)**型Ⅳ（残高管理型、ローカル管理、オープンループ）――還流情報の偽造――**

【共通鍵型】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額の還流情報を偽造することが可能。なお、還流させる価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

【共通鍵型＜静的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額の還流情報を偽造することが可能。なお、還流させる価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

【公開鍵型＜動的認証あり＞】IC カード等の電子財布中の情報が読み出された場合、共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額の還流情報を偽造することが可能。還流させる価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することも不可能。

なお、電子マネーを受取る際の動的認証のログをセンターに送ってチェックすることにより、還流情報の偽造は困難になるが、他の利用者との結託があれば攻撃可能である。

(e)**型Ⅴ（電子証書型、事後検証、クローズドループ）――還流情報の偽造――**

【共通鍵型】還流後、センターチェックが終了するまでのわずかの間に、還流見合の額を資金開放する場合は一時的に二重使用による「やり逃げ」が可能となるが、センターチェック後に資金開放を行なう運用にすれば「証書・即時・クローズド」と同じレベルで安全。

【公開鍵型＜静的認証＞】 同上

【公開鍵型＜動的認証＞】 同上

(f)**型Ⅵ（電子証書型、即時検証、クローズドループ）――還流情報の偽造――**

【共通鍵型】還流時に、オンラインでチェックされるため安全。

【公開鍵型＜静的認証＞】 同上

【公開鍵型＜動的認証＞】 同上

(g)**型Ⅶ（電子証書型、事後検証、オープンループ）――還流情報の偽造――**

【共通鍵型】還流後、センターチェックが終了するまでのわずかの間に、還流見合の額を資金開放する場合は一時的に二重使用による「やり逃げ」が可能となるが、センターチェック後に資金開放を行なう運用にすれば「証書・即時・クローズド」と同じレベルで安全。

【公開鍵型＜静的認証＞】 同上

【公開鍵型＜動的認証＞】 同上

（評価結果で使用している記号の意味）

A：攻撃対象の電子財布の利用者	$S_C(X)$：センターC によるデータ X への署名
A'：他の特定の利用者（実在）	P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
A^*：任意の利用者（架空でも可）	DT：店名、金額、時刻等
K：秘密鍵（システムで一意）	DT'：任意に指定した店名、金額、時刻等
$E_K(X)$：データ X を鍵 K で暗号化	No：電子証書の識別番号
I_A：利用者 A の識別子	V：電子証書の額面金額
P_{KA}, S_{KA}：利用者 A の公開鍵，秘密鍵	V'：任意に指定した電子証書の額面金額
P_{KB}, S_{KB}：利用者 B(譲渡先)の公開鍵，秘密鍵	

(3)**発行機関（登録機関を含む）の情報を使った偽造**

(a)**型Ⅰ（残高管理型、ローカル管理、クローズドループ）――発行機関の情報を使った偽造――**

【共通鍵型】共通秘密鍵 K によって、任意の利用者に成りすまして支払情報を作成することが可能なほか、価値を不正に発行することも可能となる。ただし、共通秘密鍵は利用者の IC カードからも得られるものであり、敢えて発行機関の情報を入手する必要には乏しい。

【共通鍵型＜静的認証＞】センター秘密鍵 S_{KC} によって、任意（架空を含む）の利用者の証明書 $S_C(I_A^*)$を作成可能。従って、共通秘密鍵 K のほか、自らの電子財布中の $S_C(I_A)$、盗聴によって得られた特定の利用者 A'の証明書 $S_C(I_A')$、偽造した証明書 $S_C(I_A^*)$ のいずれかを用いることによって、本来の利用者本人としての支払情報の他、特定の利用者ないし任意の利用者に成りすました上での支払情報を作成することが可能。

【公開鍵型＜動的認証＞】P_{KA}^* ,S_{KA}^*を任意に選び、センター秘密鍵 S_{KC} によって、この公開鍵に対するセンター署名 $S_C(P_{KA}^*)$を作成することが可能。従って、本来の利用者本人としてはもちろんのこと、任意の利用者に成りすまして秘密鍵 S_{KA}^*、公開鍵に対するセンター署名 $S_C(P_{KA}^*)$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、特定の利用者 A'に成りすますために、盗聴等により A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、利用者 A'の支払情報 $S_A'(DT')$を作ることができないため攻撃は不成功。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

（評価結果で使用している記号の意味）

A：攻撃対象の電子財布の利用者	$S_C(X)$：センターC によるデータ X への署名
A'：他の特定の利用者（実在）	P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
A^*：任意の利用者（架空でも可）	DT：店名、金額、時刻等
K：秘密鍵（システムで一意）	DT'：任意に指定した店名、金額、時刻等
$E_K(X)$：データ X を鍵 K で暗号化	No：電子証書の識別番号
I_A：利用者 A の識別子	V：電子証書の額面金額
P_{KA}, S_{KA}：利用者 A の公開鍵，秘密鍵	V'：任意に指定した電子証書の額面金額

(b)**型Ⅱ（残高管理型、センター管理・ローカル管理併用、クローズドループ）――発行機関の情報を使った偽造――**

【共通鍵型】共通秘密鍵 K によって、任意の利用者に価値を不正に発行することが可能。

ただし、各電子財布の残高情報はセンターでも管理されているため、商店から銀行に電子マネーが預けられ還流情報がセンターに戻ってきた後に、正規の残高以上に不正に支払いを行なった結果残高がマイナスになっている電子財布を発見することが可能（識別 ID も特定）。さらに、商店の受取端末がホットリストを持ち、これに登録されている不正な識別 ID の電子財布との取引を拒否する仕組みにすれば、被害を抑えることが可能。

【共通鍵型＜静的認証＞】センター秘密鍵 S_{KC} によって、任意（架空を含む）の利用者の証明書 $S_C(I_A^*)$を作成可能。従って、共通秘密鍵 K のほか、自らの電子財布中の $S_C(I_A)$、盗聴によって得られた特定の利用者 A'の証明書 $S_C(I_A')$、偽造した証明書 $S_C(I_A^*)$ のいずれかを用いることによって、本来の利用者本人としての支払情報の他、特定の利用者ないし任意の利用者に成りすました上での支払情報を作成することが可能。

ただし、各電子財布の残高情報はセンターでも管理されているため、商店から銀行に電子マネーが預けられ、還流情報がセンターに戻ってきた後に、正規の残高以上に不正に支払いを行なった結果残高がマイナスになっている電子財布を発見することが可能（識別 ID も特定）。さらに、商店の受取端末がホットリストを持ち、これに登録されている不正な識別 ID の電子財布との取引を拒否する仕組みにすれば、被害を抑えることが可能。

【公開鍵型＜動的認証＞】P_{KA}* ,S_{KA}*を任意に選び、センター秘密鍵 S_{KC} によって、この公開鍵に対するセンター署名 $S_C(P_{KA}*)$を作成することが可能。従って、本来の利用者本人としてはもちろんのこと、任意の利用者に成りすまして秘密鍵 S_{KA}^*、公開鍵に対するセンター署名 $S_C(P_{KA}^*)$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。

ただし、各電子財布の残高情報はセンターでも管理されているため、商店から銀行に電子マネーが預けられ還流情報がセンターに戻ってきた後に、正規の残高以上に不正に支払いを行なった結果残高がマイナスになっている電子財布を発見することが可能（識別 ID も特定）。さらに、商店の受取端末がホットリストを持ち、これに登録されている不正な識別 ID の電子財布との取引を拒否する仕組みにすれば、被害を抑えることが可能。

なお、特定の利用者 A'としての支払いを目的に、盗聴等により A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできないため、成りすましは困難。

(c)型Ⅲ（残高管理型、センター管理、クローズドループ）――発行機関の情報を使った偽造――

【共通鍵型】各電子財布の残高情報はセンターで管理され、取引の都度オンラインでチェックされるため、電子財布の正規の残高以上に不正に支払いを行なうことは不可能。ただし、共通秘密鍵を使って盗聴した他の利用者の電子財布の識別 $I_{A'}$を使ったり、任意に選んだ I_{A}*が存在すれば、その残高を上限に横取りすることが可能。残高を横取りされた利用者の申し出により、不正は発覚するものの、不正行為者の特定は不可能であり、再度同じ利用者が被害を受けるのを防止することができる程度。

なお、支払時にセンター側でパスワードチェックを行なう等の対策を併用すれば、横取りはより難しくなる。

【共通鍵型＜静的認証あり＞】各電子財布の残高情報はセンターで管理され、取引の都度オンラインでチェックされるため、電子財布の正規の残高以上に不正に支払いを行なうことは不可能であるが、共通秘密鍵を使って盗聴した他の利用者 A'の電子財布の証明書 $S_C(I_{A'})$を使うことにより、その残高を上限に横取りすることは可能。なお、任意に選んだ I_{A}*が存在すれば、センターの秘密鍵 S_{KC} を使って、任意の利用者 A*としての証明書 $S_C(I_{A}*)$を作ることにより、その残高を上限に横取りすることが可能。

残高を横取りされた利用者の申し出により、事後、不正は発覚するものの、不正行為者の特定は不可能であり、再度同じ利用者が被害を受けるのを防止することができる程度。

なお、支払時にセンター側でパスワードチェックを行なう等の対策を併用すれば、横取りはより難しくなる。

【公開鍵型＜動的認証あり＞】各電子財布の残高情報はセンターで管理され、取引の都度オンラインでチェックされるため、電子財布の正規の残高以上に不正に支払いを行なうことは不可能。また、特定の利用者 A'に成りすまそうと、A'の公開鍵に対するセンター署名 $S_C(P_{KA'})$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA'})$に対応した秘密鍵 $S_{KA'}$を求めることはできず（公開鍵の安全性は高い）、利用者 A'の支払情報 $S_{A'}(DT')$を作ることができないため攻撃は不成功。なお、任意の利用者 A*に成りすまそうと、任意の P_{KA}* ,S_{KA}*を予め決めてから、入手したセンター秘密鍵 S_{KC} を使って公開鍵に対するセンター署名 $S_C(P_{KA}*)$を作ることは可能であるため、この任意に作成した P_{KA}* ,S_{KA}*が実際に使用されていれば（確率は低い）、その残高を上限に横取りは可能。

(d)**型Ⅳ（残高管理型、ローカル管理、オープンループ）――発行機関の情報を使った偽造――**

【共通鍵型】共通秘密鍵 K によって、任意の利用者に成りすまして支払情報を偽造することが可能なほか、価値を不正に発行することも可能となる。ただし、共通秘密鍵は利用者の IC カードからも得られるものであり、敢えて発行機関の情報を入手する必要には乏しい。

【共通鍵型＜静的認証＞】センター秘密鍵 S_{KC} によって、任意（架空を含む）の利用者の証明書 $S_C(I_A^*)$を作成可能。従って、共通秘密鍵 K のほか、自らの電子財布中の $S_C(I_A)$、盗聴によって得られた特定の利用者 A'の証明書 $S_C(I_A')$、偽造した証明書 $S_C(I_A^*)$ のいずれかを用いることによって、本来の利用者本人としての支払情報の他、特定の利用者ないし任意の利用者に成りすました上での支払情報を作成することが可能。

【公開鍵型＜動的認証＞】P_{KA}* ,S_{KA}*を任意に選び、センター秘密鍵 S_{KC} によって、この公開鍵に対するセンター署名 $S_C(P_{KA}*)$を作成することが可能。従って、本来の利用者本人としてはもちろんのこと、任意の利用者に成りすまして秘密鍵 S_{KA}^*、公開鍵に対するセンター署名 $S_C(P_{KA}^*)$を使うことによって、扱える上限金額内での自由な金額の支払情報を偽造することが可能。ただし、特定の利用者 A'に成りすますために、盗聴等により A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、攻撃者はこれだけでは $S_C(P_{KA}')$に対応した秘密鍵 S_{KA}'を求めることはできず（公開鍵の安全性は高い）、利用者 A'の支払情報 $S_A'(DT')$を作ることができないため攻撃は不成功。

なお、支払われた価値はもともと受取者が保有する他の価値と合算され区別なく管理されるため、後にこれを検知することは不可能。

(e)**型Ⅴ（電子証書型、事後検証、クローズドループ）――発行機関の情報を使った偽造――**

【共通鍵型】共通秘密鍵 K を使うことによって、本来の利用者としての支払情報の偽造はもちろん、特定ないし任意の利用者に成りすまして支払情報を偽造すること、さらには、価値を不正に発行することも可能となる。なお、支払情報は事後的にセンターに送られてチェックされ、支払情報がデータベースに登録されていない不正なものであることが判明する。ただし、架空の識別 ID 等を使われた場合、この不正行為者を追跡し、被害を抑えることは不可能。

【公開鍵型＜静的認証＞】センターの秘密鍵 S_{KC} を使うことによって、任意の I_{A^*}、電子証書の識別番号 No、額面金額 V の電子証書 $S_C(S_C(I_{A^*}), No, V)$を偽造することが可能（ID は盗聴により入手した特定の $I_{A'}$のほか、任意の架空の I_A*を使用することが可）。また、事後的に行なわれるセンターチェックでも不正を検知することは不可能[14]。

【公開鍵型＜動的認証＞】センター秘密鍵 S_{KC} によって、任意のセンター署名 $S_C(P_{KA}*)$、識別番号 No、額面金額 V を含む電子証書 $S_C(S_C(P_{KA}*),\ No,\ V)$ を偽造することが可能。また $P_{KA}*$, $S_{KA}*$を任意に選び、センター秘密鍵 S_{KC} によって、この公開鍵に対するセンター署名 $S_C(P_{KA}*)$を作成するとともに、$S_{KA}*$によって任意の利用者 A*の譲渡証 $S_{A^*}(S_C(P_{KB'}),DT')$を作成することも可能。従って、任意の利用者に成りすまして、偽造した電子証書を使用することができる（事後的に行なわれるセンターチェックでも不正を検知することは不可能）。ただし、特定の利用者 A'に成りすます攻撃については、盗聴等により A'の公開鍵に対するセンター署名 $S_C(P_{KA'})$を入手することは可能であるが、これだけでは $S_C(P_{KA'})$に対応した秘密鍵 $S_{KA'}$を求めることはできず（公開鍵の安全性は高い）、利用者 A'の譲渡証 $S_{A'}(S_C(P_{KB'}),DT')$を作ることができないため成立しない。

（評価結果で使用している記号の意味）

A：攻撃対象の電子財布の利用者	$S_C(X)$：センターC によるデータ X への署名
A'：他の特定の利用者（実在）	P_{KC}, S_{KC}：センターC の公開鍵、秘密鍵
A^*：任意の利用者（架空でも可）	DT：店名、金額、時刻等
K：秘密鍵（システムで一意）	DT'：任意に指定した店名、金額、時刻等
$E_K(X)$：データ X を鍵 K で暗号化	No：電子証書の識別番号
I_A：利用者 A の識別子	V：電子証書の額面金額
P_{KA}, S_{KA}：利用者 A の公開鍵，秘密鍵	V'：任意に指定した電子証書の額面金額
P_{KB}, S_{KB}：利用者 B(譲渡先)の公開鍵，秘密鍵	

[14] 電子証書の事後センターチェックには、以下の２通りの方法が存在（今回評価した電子マネーモデルは共通鍵型は①の方式であるのに対し、公開鍵型はブラインド署名を使った発行処理を仮定しているため②の方式）。

①発行時に電子証書の識別番号を記録しておき、還流時にこの番号の消し込みを行なう。もし、還流された電子証書の識別番号が記録になければ、これを不正なものと判断する。

②ブラインド署名を使った電子証書発行では、発行時に電子証書の識別番号を記録することができないため、還流時に電子証書の識別番号の記録。もし、還流された電子証書の識別番号が既に記録にあるものは二重使用されたものと判断する。

②は二重使用された電子証書をチェックするだけなのに対し、①は偽造された電子証書をチェックすることもできる。

(f)**型VI（電子証書型、即時検証、クローズドループ）――発行機関の情報を使った偽造――**

【共通鍵型】共通秘密鍵 K を使うことによって、扱える上限金額内での自由な金額、任意の識別 ID（盗聴によって得た特定の ID の他、架空の ID も可能）を含む、支払情報 $E_K(I_A^*, No, DT')$を偽造したとしても、即時にセンターのデータベースに登録されているかどうかがチェックされるため、不正は不可能。なお、他の利用者が電子マネーを発行してもらう際の情報を盗聴し、センターに登録してある電子証書の登録番号、利用者の識別子、金額等を手に入れ、これを先に使用すれば、横取りすることが可能。後に、正規の持ち主が、この電子証書が使用できないことを知り、不正が発覚するが、この不正を防ぐ根本的な手段はない。

【公開鍵型＜静的認証＞】センターの秘密鍵 S_{KC} を使うことによって、任意の I_{A^*}、電子証書の識別番号 No、額面金額 V の電子証書 $S_C(S_C(I_{A^*}), No, V)$を偽造することが可能（ID は盗聴により入手した特定の I_A'のほか、任意の架空の I_A^*を使用することも可）。なお、即時に行なわれるセンターチェックでも不正を検知することは不可能。

【公開鍵型＜動的認証＞】センター秘密鍵 S_{KC} によって、任意のセンター署名 $S_C(P_{KA}^*)$、識別番号 No、額面金額 V を含む電子証書 $S_C(S_C(P_{KA}^*), No, V)$ を偽造することが可能。また P_{KA}^* , S_{KA}^*を任意に選び、センター秘密鍵 S_{KC} によって、この公開鍵に対するセンター署名 $S_C(P_{KA}^*)$を作成するとともに、S_{KA}^*によって任意の利用者 A*の譲渡証 $S_{A^*}(S_C(P_{KB}'),DT')$を作成することも可能。従って、任意の利用者に成りすまして、偽造した電子証書を使用することができる（即時に行なわれるセンターチェックでも不正を検知することは不可能）。ただし、特定の利用者 A'に成りすます攻撃については、盗聴等により A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、これだけでは $S_C(P_{KA}')$に対応した秘密鍵 $S_{KA'}$を求めることはできず（公開鍵の安全性は高い）、利用者 A'の譲渡証 $S_A'(S_C(P_{KB}'),DT')$を作ることができないため成立しない。

(g)**型Ⅶ（電子証書型、事後検証、オープンループ）――発行機関の情報を使った偽造――**

【共通鍵型】共通秘密鍵 K を使うことによって、本来の利用者としての支払情報の偽造はもちろん、特定ないし任意の利用者に成りすまして支払情報を偽造すること、さらには、価値を不正に発行することも可能となる。なお、支払情報は事後的にセンターに送られてチェックされ、支払情報がデータベースに登録されていない不正なものであることが判明する。ただし、架空の識別 ID 等を使われた場合、この不正行為者を追跡し、被害を抑えることは不可能。

【公開鍵型＜静的認証＞】センターの秘密鍵 S_{KC} を使うことによって、任意の I_{A*}、電子証書の識別番号 No、額面金額 V の電子証書 $S_C(S_C(I_{A*}), No, V)$を偽造することが可能（ID は盗聴により入手した特定の I_A'のほか、任意の架空の I_A*を使用することも可）。また、事後的に行なわれるセンターチェックでも不正を検知することは不可能。

【公開鍵型＜動的認証＞】センター秘密鍵 S_{KC} によって、任意のセンター署名 $S_C(P_{KA}*)$、識別番号 No、額面金額 V を含む電子証書 $S_C(S_C(P_{KA}*), No, V)$ を偽造することが可能。また $P_{KA}*$, $S_{KA}*$を任意に選び、センター秘密鍵 S_{KC} によって、この公開鍵に対するセンター署名 $S_C(P_{KA}*)$ を作成するとともに、$S_{KA}*$によって任意の利用者 A*の譲渡証 $S_{A*}(S_C(P_{KB}'),DT')$を作成することも可能。従って、任意の利用者に成りすまして、偽造した電子証書を使用することができる（事後的に行なわれるセンターチェックでも不正を検知することは不可能）。ただし、特定の利用者 A'に成りすます攻撃については、盗聴等により A'の公開鍵に対するセンター署名 $S_C(P_{KA}')$を入手することは可能であるが、これだけでは $S_C(P_{KA}')$に対応した秘密鍵 $S_{KA'}$を求めることはできず（公開鍵の安全性は高い）、利用者 A'の譲渡証 $S_A'(S_C(P_{KB}'),DT')$を作ることができないため成立しない。

(4)評価結果の整理

各電子マネーについて、支払情報の偽造による被害の状況について整理したものを表 2-1, 2-2 に、還流情報の偽造による被害の状況について整理したものを表 3-1, 3-2 に、発行機関の情報を利用した偽造による被害の状況を整理したものを表 4-1, 4-2 に示す。

なお、表は、各評価の欄の上段は攻撃による不正の可否、中段は攻撃が成功したときの検知の可否、下段はさらに検知が可能なときにこれを抑制する対応策の有無について、安全性が高いものを記号「○」、以降、安全性が低くなるに従い「□」「△」「×」で示したものである。

（評価表で使用している記号の意味）

【攻撃による不正の可否】

○ … 攻撃を未然に防止でき、安全。
□ … 適切な運用を怠らない限り攻撃を未然に防止でき、安全。
△ … 他の利用者の価値の横取りや価値をコピーする二重使用攻撃が成立する等。
× … 価値を自由に創出する攻撃が成立。
― … 他の方法により、もっと簡単に攻撃が成立するため、不正の可否を論じることが無意味。

【攻撃が成功したときの検知の可否】

○ … センターあるいは被害者の申告によって、攻撃が成立し被害を受けたことを検知可能。
× … 攻撃が成立し被害を受けても、検知不可能。
― … 攻撃が成立しないため検知の可否は問題にならない。

【検知が可能なときにこれを抑制する対応策の有無】

○ … 事後的に不正行為者を特定することが可能等。
△ … 不正行為者を特定することはできないが、不正行為に使用した電子財布等を使用停止にすることは可能等。
× … 攻撃が成立した不正を抑制する対応策なし。
― … 攻撃が成立しないため検知の可否は問題にならない、あるいは攻撃が成立し被害を受けたことを検知することすらできないため、対応策を講じようがない。

（表 2-1）支払情報の偽造に対する安全性　――　残高管理型電子マネー　――

安全性低い←×△□○→安全性高

残高管理型		**型 I**	**型II**	**型III**	**型IV**
流通形態		**クローズドループ**			**オープンループ**
価値管理場所		**ローカル**	**併用**	**センター**	**ローカル**
＼センター接続 暗号技術と偽造の種類		Off-line	Off-line	On-line	Off-line
共通鍵型	偽造１ (本人)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △一部対応策あり(※2)	○安全 ― ―	×攻撃成立 ×検知不可 ―
	偽造２ (特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △一部対応策あり(※2)	△(※3) ○検知可能(※4) △一部対応策あり(※5)	×攻撃成立 ×検知不可 ―
	偽造３ (不特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △一部対応策あり(※2)	△(※6) ○検知可能(※4) △一部対応策あり(※5)	×攻撃成立 ×検知不可 ―
共通鍵型 <静的認証あり>	偽造１ (本人)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △一部対応策あり(※2)	○安全 ― ―	×攻撃成立 ×検知不可 ―
	偽造２ (特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △一部対応策あり(※2)	△(※3) ○検知可能(※4) △一部対応策あり(※5)	×(※7) × ―
	偽造３ (不特定)	○安全 ― ―	○安全 ― ―	○安全 ― ―	×(※7) × ―
公開鍵型 <動的認証あり>	偽造１ (本人)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △一部対応策あり(※2)	○安全 ― ―	×攻撃成立 ×検知不可 ―
	偽造２ (特定)	○安全 ― ―	○安全 ― ―	○安全 ― ―	×(※7) × ―
	偽造３ (不特定)	○安全 ― ―	○安全 ― ―	○安全 ― ―	×(※7) × ―

(※1)事後的なセンターチェックにより検知、不正行為の行なわれた電子財布の特定も可能。

(※2)商店がホットリストをもとにチェックし、不正な電子財布を受けつけなくすれば対応可能。

(※3)盗聴によって I_A'を手にいれた A'の残高を横取り可能。

(※4)横取りされた A'（A*）が自らの残高が減少していることに気付き、不正が発覚。また、センターのログにより、A'（A*）からどの電子財布に対して不正な資金移動があったかを把握することは可能。

(※5)不正行為の行なわれた電子財布を取引停止することによって、被害は限定。

(※6)任意に選んだ識別 I_A*が実在すれば、A*の残高を横取り可能。

(※7) **完全な匿名性があるため、偽造 1 を第 3 者を介在して行うことで実質的に攻撃成功と同様の効果。**

（表 2-2）支払情報の偽造に対する安全性　　―― 電子証書型電子マネー ――

安全性低い←×△□○→安全性高

電子証書型 流通形態 価値管理場所 ＼センター接続 暗号技術と偽造の種類		**型Ⅴ**	**型Ⅵ**	**型Ⅶ**
		クローズドループ		**オープンループ**
		ローカル		
		Off-line（**事後検証**）	On-line（**即時検証**）	Off-line（**事後検証**）
共通鍵型	偽造１ (本人)	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	○安全 － －	×攻撃成立 ○検知可能(※1) △対応策あり(※2)
	偽造２ (特定)	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	△(※4) ○検知可能（※1） ×対応策なし	×攻撃成立 ○検知可能(※1) △対応策あり(※2)
	偽造３ (不特定)	×攻撃成立 ○検知可能(※1) ×対応策なし	○安全 － －	×攻撃成立 ○検知可能(※1) ×対応策なし
公開鍵型 <静的認証あり>	偽造１ (本人)	△重複使用攻撃のみ可能 ○検知可能(※1) ○対応策あり(※3)	○安全 － －	△重複使用攻撃のみ可能 ○検知可能(※1) ○対応策あり(※3)
	偽造２ (特定)	△盗聴したA'の証書を不正使用可能 ○検知可能(※1) ×対応策なし	○(※5) － －	△盗聴した A'の証書を不正使用可能 ○検知可能(※1) ×対応策なし
	偽造３ (不特定)	○安全 － －	○安全 － －	○安全 － －
公開鍵型 <動的認証あり>	偽造１ (本人)	△重複使用攻撃のみ可能 ○検知可能(※1) ○対応策あり(※3)	○安全 － －	△重複使用攻撃のみ可能 ○検知可能(※1) ○対応策あり(※3)
	偽造２ (特定)	○安全 － －	○安全 － －	○安全 － －
	偽造３ (不特定)	○安全 － －	○安全 － －	○安全 － －

(※1)事後的なセンターチェックにより検知。不正行為者ないし被害者の特定可。
(※2)商店がホットリストを持つことができればチェック可能。
(※3)露見した不正行為者を特定する情報をもとに不正行為者を追跡。
(※4)盗聴（特に発行時）したA'の証書を先に使用できれば攻撃可能。
(※5)盗聴したA'の証書を先に使用できれば攻撃可能。なお、証書は発行時は暗号化されているため盗聴困難であり、盗聴可能なのは使用時に限られるため、攻撃が成功する可能性はかなり低いとみられる。

（表 3-1）還流情報の偽造に対する安全性　――　残高管理型電子マネー　――

安全性低い←×△□○→安全性高

残高管理型 流通形態 価値管理場所 ＼センター接続 暗号技術と偽造の種類		**型 I**	**型II**	**型III**	**型IV**
		クローズドループ			**オープンループ**
		ローカル	**併用**	**センター**	**ローカル**
		Off-line	Off-line	On-line	Off-line
共通鍵型	結託なし	×攻撃成立 ×検知不可 ―	△(※1) ○検知可能(※2) ○対応策あり(※3)	△(※1) ○検知可能(※2) ○対応策あり(※3)	×攻撃成立 ×検知不可 ―
	結託あり	― ― ―	○安全 ― ―	○安全 ― ―	― ― ―
共通鍵型 <静的認証あり>	結託なし	×攻撃成立 ×検知不可 ―	△(※1) ○検知可能(※2) ○対応策あり(※3)	△(※1) ○検知可能(※2) ○対応策あり(※3)	×攻撃成立 ×検知不可 ―
	結託あり	― ― ―	○安全(※4) ― ―	○安全(※4) ― ―	― ― ―
公開鍵型 <動的認証あり>	結託なし	×攻撃成立 ×検知不可 ―	△(※1) ○検知可能(※2) ○対応策あり(※3)	△(※1) ○検知可能(※2) ○対応策あり(※3)	×攻撃成立 ×検知不可 ―
	結託あり	― ― ―	○安全(※4) ― ―	○安全(※4) ― ―	― ― ―
動的認証のログも転送する場合	結託なし	○安全 ― ―	○安全 ― ―	○安全 ― ―	○安全 ― ―
	結託あり	×攻撃成立 ×検知不可 ―	○安全(※4) ― ―	○安全(※4) ― ―	×攻撃成立 ×検知不可 ―

(※1)既に取引があり識別 I_A がわかっている A の残高を横取り可能。

(※2)事後的に、A が自らの残高が減少していることに気付き、不正が発覚。センターのログによって A からどの電子マネー出納口座に対して不正な資金移動があったかを把握可能。

(※3)不正行為者の電子マネー出納口座を封鎖し、取引停止。

(※4)残高はセンターで管理されているため、商店と結託者の情報では両者間の価値移動しか行なえない（価値を偽造することはできない）。

（表 3-2）還流情報の偽造に対する安全性　――　電子証書型電子マネー　――

安全性低い←×△□○→安全性高

電子証書型 流通形態 価値管理場所 センター接続		**型Ⅴ**	**型Ⅵ**	**型Ⅶ**
		クローズドループ		**オープンループ**
		ローカル		
		Off-line（**事後検証**）	On-line（**即時検証**）	Off-line（**事後検証**）
共通鍵型	結託なし	□安全(※1) ― ―	○安全(※2) ― ―	□安全(※1) ― ―
	結託あり	□安全(※1) ― ―	○安全(※2) ― ―	□安全(※1) ― ―
公開鍵型＜静的認証あり＞	結託なし	□安全(※1) ― ―	○安全(※2) ― ―	□安全(※1) ― ―
	結託あり	□安全(※1) ― ―	○安全(※2) ― ―	□安全(※1) ― ―
公開鍵型＜動的認証あり＞	結託なし	□安全(※1) ― ―	○安全(※2) ― ―	□安全(※1) ― ―
(証書型は動的認証ログも転送)	結託あり	□安全(※1) ― ―	○安全(※2) ― ―	□安全(※1) ― ―

(※1)還流後、センターチェックが終了するまでのわずかの間に、還流見合の額を資金開放する場合は一時的に二重使用による「やり逃げ」が可能となるが、実際には還流は匿名取引ではないため、不正が特定されるのを恐れることによる抑制効果が働くほか、センターチェック後に資金開放を行なう運用にすれば「証書・即時・ｸﾛｰｽﾞﾄﾞ」と同じレベルで安全となる。

(※2)特定の商店あるいは不特定の利用者による二重使用未遂を検知。

（表 4-1）発行機関の情報を利用した偽造に対する安全性　――　残高管理型電子マネー　――

安全性低い←×△□○→安全性高

残高管理型 流通形態 価値管理場所 ＼センター接続 暗号技術と偽造の種類		**型 I**	**型II**	**型III**	**型IV**
		クローズドループ			**オープンループ**
		ローカル	**併用**	**センター**	**ローカル**
		Off-line	Off-line	On-line	Off-line
共通鍵型	偽造１ (本人)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	○安全 ― ―	×攻撃成立 ×検知不可 ―
	偽造２ (特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	△(※3) ○検知可能(※4) △一部対応策あり(※5)	×攻撃成立 ×検知不可 ―
	偽造３ (不特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	□(※6) ○検知可能(※4) □一部対応策あり(※5)	×攻撃成立 ×検知不可 ―
共通鍵型 <静的認証あり>	偽造１ (本人)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	○安全 ― ―	×攻撃成立 ×検知不可 ―
	偽造２ (特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	△(※3) ○検知可能(※4) △一部対応策あり(※5)	×攻撃成立 ×検知不可 ―
	偽造３ (不特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	□安全(※6) ○検知可能(※4) □一部対応策あり(※5)	×攻撃成立 ×検知不可 ―
公開鍵型 <動的認証あり>	偽造１ (本人)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	○安全 ― ―	×攻撃成立 ×検知不可 ―
	偽造２ (特定)	○安全 ― ―	○安全 ― ―	○安全 ― ―	×(※8) × ―
	偽造３ (不特定)	×攻撃成立 ×検知不可 ―	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	□安全(※7) ○検知可能(※4) □一部対応策あり(※5)	×攻撃成立 ×検知不可 ―

(※1)事後的なセンターチェックにより検知、不正行為の行なわれた電子財布の特定も可能。

(※2)商店がホットリストをもとにチェックし、不正な電子財布を受け付けなくすれば対応可能。

(※3)盗聴によって $I_{A'}$を手にいれた A'の残高を横取り可能。

(※4)横取りされた A'（A*）が自らの残高が減少していることに気付き、不正が発覚。また、センターのログにより、A'（A*）からどの電子財布に対して不正な資金移動があったかを把握することは可能。

(※5)不正行為の行なわれた電子財布を取引停止することによって、被害は限定。

(※6)任意に選んだ識別 I_A*が実在すれば、A*の残高を横取り可能。

(※7)任**意に作成した** P_{KA}* ,S_{KA}*が実在すれば、A*の残高を横取り可能。

(※8)**完全な匿名性があるため、偽造 1 を第 3 者を介在して行うことで実質的に攻撃成功と同様の効果**。

（表 4-2）発行機関の情報を利用した偽造に対する安全性　――　電子証書型電子マネー ――

安全性低い←×△□○→安全性高

電子証書型 流通形態 価値管理場所 ＼センター接続 暗号技術と偽造の種類		**型Ⅴ**	**型Ⅵ**	**型Ⅶ**
		クローズドループ		**オープンループ**
		ローカル		
		Off-line（**事後検証**）	On-line（**即時検証**）	Off-line（**事後検証**）
共通鍵型	偽造１ (本人)	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	○安全 － －	×攻撃成立 ○検知可能(※1) △対応策あり(※2)
	偽造２ (特定)	×攻撃成立 ○検知可能(※1) △対応策あり(※2)	△(※4) ○検知可能（※1） ×対応策なし	×攻撃成立 ○検知可能(※1) △対応策あり(※2)
	偽造３ (不特定)	×攻撃成立 ○検知可能(※1) ×対応策なし	○安全 － －	×攻撃成立 ○検知可能(※1) ×対応策なし
公開鍵型 <静的認証あり>	偽造１ (本人)	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －
	偽造２ (特定)	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －
	偽造３ (不特定)	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －
公開鍵型 <動的認証あり>	偽造１ (本人)	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －
	偽造２ (特定)	○安全 － －	○安全 － －	○安全 － －
	偽造３ (不特定)	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －	×攻撃成立 ×検知不可 －

(※1)事後的なセンターチェックにより検知。不正行為者ないし被害者の特定可。
(※2)商店がホットリストを持つことができればチェック可能。
(※3)露見した不正行為者を特定する情報をもとに不正行為者を追跡。
(※4)盗聴（特に発行時）した A'の証書を先に使用できれば攻撃可能。
(※5)盗聴した A'の証書を先に使用できれば攻撃可能。なお、証書は発行時は暗号化されているため盗聴困難であり、盗聴可能なのは使用時に限られるため、攻撃が成功する可能性はかなり低いとみられる。

5.考察

(1)支払情報の偽造に対する安全性と耐タンパー装置の必要性

利用者が自ら保有する秘密情報をもとに、支払情報の偽造等を行なうことによって価値を不正に入手する攻撃が成功し、かつその事実を検知できないタイプの電子マネー（安全性レベル A）や、検知は可能であっても、この偽造等による被害を抑制する対応策を何も講じることができないタイプの電子マネー（安全性レベル B）は、これだけでは必要な安全性を確保できていないということであり、IC カード等の耐タンパー性を利用することによって、利用者が自ら保有する秘密情報に不正にアクセスできなくすることが必要となる。一方、価値を不正に入手する攻撃が成功する可能性があったとしても、事後的に不正行為者を特定できる等、これを検知しかつ抑止する効果的な対応策が存在するタイプの電子マネー（安全性レベル C）は、「やり逃げ」ができない等の限られた運用環境下では、ある程度は安全といえるが[15]、耐タンパー性のある機器を組み合わせることによって、さらに安全性を高めることができる。なお、支払情報の偽造等の価値を不正に入手する攻撃が成功しないタイプの電子マネーは、そのままでも必要な安全性を確保しており、IC カード等の耐タンパー性のある機器を必ずしも必要としない（安全性レベル D）[16]。電子マネーを設計する際には、一定のコスト制約のもとで、必要な機能や利便性を実現しつつ、こうした安全性のレベルを極力高めることが必要である。

（表 5）電子マネーの安全性のレベルと耐タンパー性の必要性

安全性レベル	不正の未然防止	不正の検知	不正を抑制する対応策	安全性の判断	耐タンパー性の必要性
レベル A	×攻撃成功	×検知不可	――	危険	必須
レベル B	×攻撃成功	○検知可能	×対応策なし	危険	必須
レベル C	×攻撃成功	○検知可能	○対応策あり	必要最低限の安全性を確保	望ましい
レベル D	○安全	――	――	安全	必要なし

※上表は、価値を不正に手に入れる行為に対する安全性のレベルを整理したものであり、必要とされるコストや実現される機能､利便性の観点からの優劣について考慮しているものではない。

各電子マネーモデルについての支払情報の偽造に関する評価結果（表 2-1, 2-2）をもとに、耐タンパー機器の必要性について整理したものが表 6 である。これによると、残高管理型では、

[15] 利用者の情報が他人に盗まれ、「やり逃げ」される場合は抑止効果が弱いため、このリスクまで考慮すれば耐タンパー機器は必要。

[16] レベル D を実現するには、後述の通り、暗号技術として公開鍵暗号を利用するとともに、センターとのオンラインで通信を行うことが必要となるが、こうした方式は、比較的コストがかかると考えられるほか、利用者にとって必要な利便性を必ずしも実現していないことが多く、本稿でこの表におけるレベル D が一番優れていると主張しているものではない。

本稿で訴えたいことは、耐タンパー性のある装置を始め、様々な情報セキュリティ技術を組合せ、複数の安全対策を施す等によって、利用者の利便性等の要求を満たしつつ、安価に総合的な安全性を確保した電子マネーを実現することが大事だということである。

ローカルで価値を管理（センター併用を含む）するオフライン型の電子マネーは、基本的には価値の不正な創出が自由に行えるため、さらに耐タンパー性を持った IC カード等の付加的な安全対策を講じる必要がある。センターで価値を管理するオンライン型の電子マネーでは、価値が不正に創出される危険はないが、本人認証の安全性が確保されない場合には、他人の価値が搾取される危険がある。この点、暗号方式として共通鍵暗号や公開鍵暗号による静的認証を使うタイプの電子マネーは、盗聴により本人認証のための情報等が盗まれると成りすましが容易に行えるため、攻撃される危険性がある。従って、残高管理型の電子マネーで耐タンパー装置に頼らなくても安全なものは、センターで価値を管理するクローズドループ型の電子マネーで暗号技術として公開鍵暗号を使った動的認証を用いるタイプのみということになる。なお、耐タンパー装置が必須と判断される他のタイプの電子マネーについても、その攻撃による被害が価値の創出なのか、他人の価値の搾取なのかといった電子マネーシステムに与えるインパクトの大きさに応じて、必要とされる耐タンパー装置の強度レベルは異なる。

一方、電子証書型の電子マネーでは、暗号技術として公開鍵暗号を使ったタイプであれば、基本的に偽造を行なうことができない。ここで問題となるのは、利用者本人が保有する電子マネーの二重使用や、盗聴等により手に入れた他の利用者が保有する電子マネーの不正使用であるが、これらについてはオンラインで即時検証を行なうことにより防ぐことができる。なお、オンラインで即時検証を行なわなくても、暗号方式として公開鍵暗号の動的認証を使用するタイプであれば、盗聴等により手に入れた他の利用者の電子マネーが不正使用されることを防ぐことは可能である。この場合でも、利用者本人の保有する電子マネーを二重使用することは可能であるが、暗号技術により不正行為者が事後的に特定される仕組みを設けることはできるため、「やり逃げ」ができないような運用環境下では安全といえる。耐タンパー機器等の付加的な安全対策を組み合わせれば、さらに「やり逃げ」まで防止することも可能である。

残高・ローカル・オープン型の電子マネーは、採用している暗号技術に関わらず攻撃が成功し、その安全性は変わらない。つまり、必要最低限の暗号技術が使用されていれば、それがどのような方法であるかは電子マネーの安全性レベルにはあまり影響しないことから、暗号方式の強化にコストをかけるよりは、耐タンパー性の強化にコストをかけることの方が意味のあることになる。

（表 6～10 における記号の見方）

表 6～10 は、表 2-1, 2-2, 3-1, 3-2, 4-1, 4-2 の分析結果から安全性の高さを表す記号のみを整理したもの。各欄の記号は、表 6,7,8, 10 では、上段が**偽造 1**、中段が**偽造 2**、下段が**偽造 3** に、表 9 では上段が**結託なし**、下段が**結託あり**に対応し、それぞれについて、1 列目が不正の未然防止可否、2 列目が不正発生時の検知可否、3 列目が不正を検知したときの対応策有無を示す。

（表 6）支払情報の偽造に対する安全性と耐タンパー装置の必要性

安全性低←×△□○→安全性高

残高管理型	型Ⅰ	型Ⅱ	型Ⅲ	型Ⅳ
流通形態	クローズドループ			オープンループ
価値管理場所	ローカル	併用	センター	ローカル
＼センター接続 暗号技術と偽造の種類	Off-line	Off-line	On-line	Off-line
共通鍵型	××ー ××ー ××ー	×○△ ×○△ ×○△	○ーー △○△ △○△	××ー ××ー ××ー
共通鍵型 <静的認証あり>	××ー ××ー ○ーー	×○△ ×○△ ○ーー	○ーー △○△ ○ーー	××ー ××ー ××ー
公開鍵型 <動的認証あり>	××ー ○ーー ○ーー	×○△ ○ーー ○ーー	○ーー ○ーー ○ーー	××ー ××ー ××ー

電子証書型	型Ⅴ	型Ⅵ	型Ⅶ
流通形態	クローズドループ		オープンループ
価値管理場所	ローカル		
センター接続	Off-line （事後検証）	On-line （即時検証）	Off-line （事後検証）
共通鍵型	×○△ ×○△ ×○×	○ーー △○× ○ーー	×○△ ×○△ ×○×
公開鍵型 <静的認証あり>	△○○ △○× ○ーー	○ーー ○ーー ○ーー	△○○ △○× ○ーー
公開鍵型 <動的認証あり>	△○○ ○ーー ○ーー	○ーー ○ーー ○ーー	△○○ ○ーー ○ーー

耐タンパー機器が必須
耐タンパー機器があるとさらに安全性が向
耐タンパー機器は必ずしも必要ない

（各欄中の記号の見方）

	不正の未然防止可否	不正の検知可否	不正を抑制する対応策有無
偽造 1	ーー	ーー	ーー
偽造 2	ーー	ーー	ーー
偽造 3	ーー	ーー	ーー

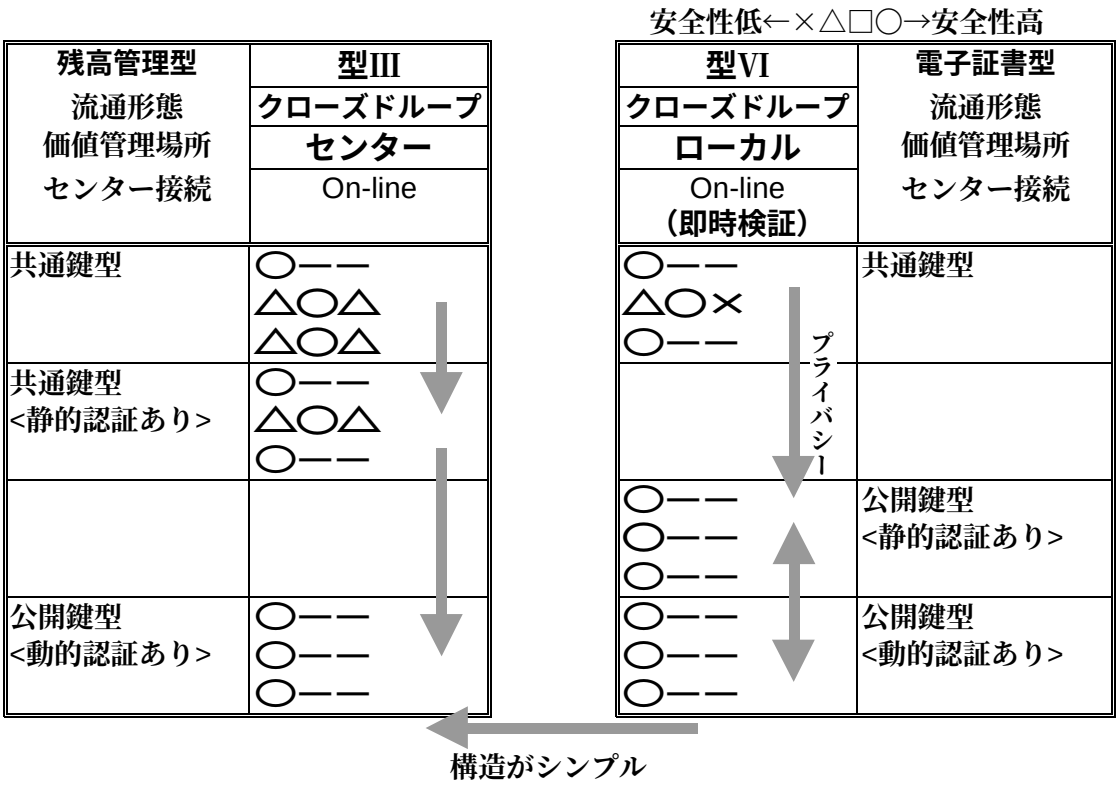
(2)支払情報の偽造に対する安全性からみたオンライン型電子マネーの比較

支払情報の偽造という観点からみると、オンライン型の電子マネーは、暗号技術として公開鍵暗号を利用したものは残高管理型、電子証書型とも同レベルで安全である（表 7 参照）。ただし、実際にインプリメントすることまで考慮すると、構造がシンプルなために、処理に必要な資源等が少なくて済む分、残高管理型が優位といえる。

一方、暗号技術として共通鍵暗号を利用したものは、新たに価値を創出する種類の不正は不可能であるが、盗聴によって得た情報を利用することにより、他人の価値を盗むことは可能である。残高管理型は一度盗聴されると、盗聴された利用者の取引を停止する等の対策を講じない限り、センターで管理されている残高が将来に渡ってすべて横取りの危険にさらされるのに対して、電子証書型は盗聴された電子証書の価値のみが横取りの対象となり、攻撃者は不正を行なう度に盗聴する必要が生じる。

なお、個々の電子マネーが個性を持って区別できる電子証書型の場合、共通鍵型ではどの電子マネーを誰に発行したかが発行機関にわかってしまうのに対し、公開鍵型ではブラインド署名等を使用することによりこれをわからなくし、匿名性を持たせることもできる。

（表 7）オンライン型電子マネーの比較



※　矢印の方向は安全性が高くなること、あるいは他の理由により優れている事を示す。

(3)支払情報の偽造に対する安全性からみたオフライン型電子マネーの比較

支払情報の偽造という観点からみると、オフライン型電子マネーは耐タンパー性のある装置なくしては、何らかの攻撃による被害を受ける可能性がある。しかしながら、電子証書型で暗号技術として公開鍵暗号（静的認証）を使用するタイプは、被害を受けたときに不正行為者の特定を行なうことが可能であるなど、その攻撃に対する対応策を持っている点で優れており、運用環境に配慮すれば必要最低限の安全性を有しているといえる。

残高管理型の電子マネーではオープンループ型はクローズドループ型に比べ安全性が低いのに対し、電子証書型では両者の安全性は同じであり、処理する情報量の増大を気にする必要がなければ、電子証書型の場合はオープンループ型にして利便性を高める方が合理的となる（表８参照）。

なお、残高管理型の電子マネーにおいては、型Ⅱ（残高・併用・クローズド型）は使用する暗号技術の種類に関わらず、型Ⅰ（残高・ローカル・クローズド型）より安全性の面で優れており、センター側でも価値を管理するというさほど大きくない仕様変更によって、価値を創出するタイプの偽造を防ぐことができることがわかる。これは、実際に世の中で実験されている残高管理型のクローズドループ型電子マネーの多くが、型Ⅱであるという事実に適合している。

（表８）オフライン型電子マネーの比較

安全性低←×△□○→安全性高

残高管理型	型Ⅰ	型Ⅱ	型Ⅳ	型Ⅴ	型Ⅶ	電子証書型
流通形態	クローズドループ		オープンループ	クローズドループ	オープンループ	流通形態
価値管理場所	ローカル	併用	ローカル	ローカル		価値管理場所
センター接続	Off-line	Off-line	Off-line	Off-line (事後検証)	Off-line (事後検証)	センター接続
共通鍵型	××－ ××－ ××－	×○△ ×○△ ×○△	××－ ××－ ××－	×○△ ×○△ ×○×	×○△ ×○△ ×○×	共通鍵型
共通鍵型 <静的認証あり>	××－ ××－ ○－－	×○△ ×○△ ○－－	××－ ××－ ××－			
				△○□ △○× ○－－	△○□ △○× ○－－	公開鍵型 <静的認証あり>
公開鍵型 <動的認証あり>	×× ○－－ ○－－	×○△ ○－－ ○－－	××－ ××－ ××－	△○□ ○－－ ○－－	△○□ ○－－ ○－－	公開鍵型 <動的認証あり>

※　矢印の方向は安全性が高くなること、あるいは他の理由により優れている事を示す。

(4)還流情報の偽造からみた電子マネーの安全性と耐タンパー装置の必要性

還流情報の偽造という観点からみると、電子証書型の電子マネーは、還流時はいずれのタイプも結果的にオンラインチェックとなるため安全である（耐タンパー装置は不要）。

一方、残高管理型の電子マネーは、センターで残高を管理していない場合（ローカルのみで残高を管理している場合）は、価値を不正に創出するタイプの攻撃が可能である（耐タンパー装置が必要）。もっとも、この場合、価値受取り時のログ（取引の履歴）も発行機関に対して還流させることにすれば安全となるが、それでも商店が他の利用者と結託した場合には攻撃されうることがわかる。また、センターで残高を管理する場合は、商店が一時的に他人の価値を横取りすることは可能であるが、横取りされた利用者の申し出により不正の事実が発覚するほか、センターのログを確認することによって横取りされた価値がどの商店の電子マネー出納口座に入金されたかを把握可能なため、不正が行なわれた電子マネー出納口座を凍結したり、口座の持ち主を捕まえることによって被害は限定される（耐タンパー性があるとさらに安全性が向上）。なお、価値受取り時のログ（取引の履歴）も発行機関に対して還流させることにすれば、結託者以外の利用者から受け取った電子マネーの還流情報を偽造することはできないためさらに安全となる（耐タンパー装置は不要）。

表９は、還流情報の偽造からみた耐タンパー装置の必要性を整理したものである。

（表９）還流情報の偽造に対する安全性と耐タンパー装置の必要性

安全性低←×△□○→安全性高

残高管理型 流通形態 価値管理場所 ＼センター接続 暗号技術と偽造の種類	**型Ⅰ**	**型Ⅱ**	**型Ⅲ**	**型Ⅳ**
	クローズドループ			**オープンループ**
	ローカル	**併用**	**センター**	**ローカル**
	Off-line	Off-line	On-line	Off-line
共通鍵型	××－ －－－	△○○ ○－－	△○○ ○－－	××－ －－－
共通鍵型 <静的認証あり>	××－ －－－	△○○ ○－－	△○○ ○－－	××－ －－－
公開鍵型 <動的認証あり>	××－ －－－	△○○ ○－－	△○○ ○－－	××－ －－－
動的認証のログも転送する場合	○－－ ××－	○－－ ○－－	○－－ ○－－	○－－ ××－

電子証書型 流通形態 価値管理場所 センター接続	**型Ⅴ**	**型Ⅵ**	**型Ⅶ**
	クローズドループ		**オープンループ**
	ローカル		
	Off-line（**事後検証**）	On-line（**即時検証**）	Off-line（**事後検証**）
共通鍵型	□－－ □－－	○－－ ○－－	□－－ □－－
公開鍵型＜静的認証あり＞	□－－ □－－	○－－ ○－－	□－－ □－－
公開鍵型＜動的認証あり＞ (証書型は動的認証ログも転送)	□－－ □－－	○－－ ○－－	□－－ □－－

■ 耐タンパー機器が必須
■ 耐タンパー機器があるとさらに安全性が向
□ 耐タンパー機器は必ずしも必要ない

（各欄中の記号の見方）

	不正未然防止可否	不正の検知可否	対応策有無
結託なし	－－	－－	－－
結託あり	－－	－－	－－

(5)発行機関の情報を利用した偽造からみた電子マネーの安全性

発行機関の情報を利用した偽造という観点からみると、残高管理型の電子マネーの場合、センターにオンラインで接続して取引処理が行われるタイプ（「残高・センター・クローズド」型）では、他人の残高を横取りする種類の偽造しかあり得ず（公開鍵暗号を利用した動的認証によって本人確認をすればこれも防止）、しかも、事後的に不正を行った電子財布を特定することができるため、相対的に安全性は高い。これに対して、センターとはオフラインのまま取引処理が行われるタイプは基本的にすべて、暗号技術の選択の方法等に関わらず、価値を創出する種類の偽造が可能となる（表 10 参照）。

一方、電子証書型の場合は、発行機関の情報を利用することによって、任意の電子証書、譲渡証を作成することが可能。ただし、還流時の発行機関による二重使用チェックの方法によっては、これを発見し、不正使用を防止することができる。電子マネー発行にブラインド署名を使うことにより匿名性を実現しているタイプの電子マネーでは、発行時に電子証書識別番号を登録することができないことから、通常、還流時に登録を行ない、もし、既に登録済みであれば二重使用された電子マネーとみなしている。このため、発行機関の秘密鍵を使って新たに偽造された電子証書は正規のものと区別できずに受け入れてしまう。これに対し、電子マネー発行時に電子証書識別番号を登録することができる電子マネーでは、還流時にこの消し込み処理を行ない、もし、消し込むべき識別番号が存在しなければ不正な電子マネーと判断しているため、いくら正当な発行機関の秘密鍵を使った電子証書であっても、これが偽造であると判断することができるため、安全性が高い。なお、中山・森畠・阿部・藤崎[1997]などは、登録機関を新たに設けることによって、コントロールされた匿名性を保ちつつ、この後者の方法を実現することに成功している。

（表 10）発行機関の情報を利用した偽造

安全性低←×△□○→安全性高

残高管理型	**型 I**	**型II**	**型III**	**型IV**
流通形態	**クローズドループ**			**オープンループ**
価値管理場所	**ローカル**	**併用**	**センター**	**ローカル**
＼センター接続 暗号技術と偽造の種類	Off-line	Off-line	On-line	Off-line
共通鍵型	××ー ××ー ××ー	×○△ ×○△ ×○△	○ーー △○△ □○□	××ー ××ー ××ー
共通鍵型 <静的認証あり>	××ー ××ー ××ー	×○△ ×○△ ×○△	○ーー △○△ □○□	××ー ××ー ××ー
公開鍵型 <動的認証あり>	××ー ○ーー ××ー	×○△ ○ーー ×○△	○ーー ○ーー □○□	××ー ××ー ××ー

電子証書型	**型 V**	**型VI**	**型VII**
流通形態	**クローズドループ**		**オープンループ**
価値管理場所	**ローカル**		
＼センター接続 暗号技術と偽造の種類	Off-line **（事後検証）**	On-line **（即時検証）**	Off-line **（事後検証）**
共通鍵型	×○△ ×○△ ×○×	○ーー △○× ○ーー	×○△ ×○△ ×○×
公開鍵型 <静的認証あり>	××ー ××ー ××ー	××ー ××ー ××ー	××ー ××ー ××ー
公開鍵型 <動的認証あり>	××ー ○ーー ××ー	××ー ○ーー ××ー	××ー ○ーー ××ー

Ⅳ．おわりに

本稿では、電子マネーで使用される情報セキュリティ技術のうち主要な要素技術について紹介するとともに、これらの要素技術自体は絶対的な安全性を持つとは限らないことを示した。次に、耐タンパー性を利用せずに電子マネーを構成した場合に、各電子マネー実現方式の違いによって、発生し得るリスクの種類、程度、範囲にどのような違いがあるのかを分析した。こうした分析結果は、電子マネーの機能や技術的特徴の違いが、各電子マネー実現方式の安全性に大きな影響を与えることを示すとともに、安全性を高めるためには他にどのような要素技術（耐タンパー装置等）を追加する必要があるかを検討する材料として利用しうる。

電子マネーは、様々な情報セキュリティ技術を組み合わせることによって成り立つ総合技術である。特定の情報セキュリティ技術に過度に頼ることなく、仮に利用している要素技術の安全性が期待された通りでなかったとしても、他の要素技術がこれを補完して全体としては必要な安全性が保たれるように、複数の情報セキュリティ技術をバランス良く組み合わせることによって、「総合的な安全性」を高めることが重要であろう。

今後は、本稿で得られた結論を利用して、個々の電子マネー実現方式について、複数の情報セキュリティ技術を用いて総合的な安全性を確保する方法を検討していくことが課題である。

以　上

【参考文献】

（電子マネー関連）

太田和夫・岡本龍明・川原洋人、「電子現金の実用化動向とその課題」、『1997 年電子情報通信学会総合大会講演論文集』、基礎・境界 TA-4-2, pp.578-579, **電子情報通信学会、**1997 **年**

岡本龍明・太田和夫、「理想的電子現金方式の一方法」、『電子情報通信学会論文誌』、J76-D-I**、**No.6**、**pp.315-323**、電子情報通信学会、**1993 **年**

中山靖司、「実現せまる電子マネーの現状」、『Dr. Dobb's JOURNAL JAPAN**』、**1998 **年** 2 **月号**、**pp.70-81**、翔泳社、**1998 **年**

――――、「電子決済について」、『ITU **ジャーナル』、**Vol26**、**No.7**、**pp.54-62**、新日本** ITU **協会、**1996 **年**

――――・太田和夫・松本 勉、「電子マネーの安全性評価について」、『1998 **年 暗号と情報セキュリティシンポジウム』、**SCIS'98-3.1.A**、**1998 **年**

――――・森畠秀実・阿部正幸・藤崎英一郎、「電子マネーの一実現方式について――安全性、利便性に配慮した新しい電子マネー実現方式の提案――」、『金融研究』、第 16 **巻第** 2 **号、日本銀行金融研究所、**1997 **年** 6 **月号**

――――・森畠秀実・阿部正幸・藤崎英一郎、「電子現金の一実現方式について」、『ディスカッションペーパーシリーズ』、97-J-5**、日本銀行金融研究所、**1997 **年**

藤崎英一郎・岡本龍明、「エスクロー電子現金」、『電子情報通信学会論文誌』、IT95-51**、**ISEC95-46**、**SST95-112**、**pp.7-12**、電子情報通信学会、**1996 **年**

森畠秀実・阿部正幸・藤崎英一郎・中山靖司、「電子現金方式」、『1997 **年 暗号と情報セキュリティシンポジウム』、**SCIS'97-3C**、**1997 **年**

BIS, "Security of Electronic Money," Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, Aug 1996.**（日本銀行電算情報局訳、『電子マネーのセキュリティ』、ときわ総合サービス、**1997 **年）**

Brands, S., "Untraceable Off-line Cash in Wallet with Observers," Advances in Cryptology-CRYPTO'91, LNCS 773, pp.302-318, Springer-Verlag, 1993.

Chaum, D., "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM, Vol.28 NO.10, pp.1030-1044, 1985.

――――, A. Fiat and M. Naor, "Untraceable Electronic Cash (Extended Abstract)," Advances in Cryptology-CRYPTO'88, LNCS, No.403, pp.328-335, Springer-Verlag, 1989.

Eng, T. and Okamoto, T., "Single-Term Divisible Electronic Coins," Proc. of EUROCRYPT '94, LNCS 950, pp. 306-319, Springer-Verlag, 1995.

Even, S., Goldreich, O., Yacobi, Y. "Electronic Wallet," Proc. of CRYPTO'83, A later version appeared in Proc. of 1984 International Zurich Seminar on Digital Communications, pp.199-201, IEEE cat No.84CH1998-4.

Matsumoto, T., "An Electronic Retail Payment System with Distributed Control - A Conceptual Design -," IEICE Trans. Fundamentals, Vol.E78-A, No.1, 1995.

Nakayama, Y., Moribatake, H., Abe, M. and Fujisaki, E., "An Electronic Money Scheme -- A Proposal for a New Electronic Money Scheme which is both Secure and Convenient," Discussion paper series, 97-E-4, Institute for Monetary and Economic Studies, Bank Of Japan, 1997.

Okamoto, T. and Ohta, K., "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility," Advances in Cryptology-EUROCRYPT'89, LNCS 434, pp.134-149, Springer-Verlag, 1989.

――――, and ――――, "Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash," Proc. of CRYPTO '89, LNCS 435, pp.481-496, Springer-Verlag, 1990.

————, and ————, “Universal Electronic Cash,” Advances in Cryptology-CRYPTO’91, LNCS 576, pp.324-337, Springer-Verlag, 1991.

（暗号技術関連）

岩下直行、「金融分野における情報セキュリティ技術の国際標準化動向」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

宇根正志・太田和夫、「共通鍵暗号を取り巻く現状と課題―DES から AES へ―」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

――――・岡本龍明、「公開鍵暗号の理論研究における最近の動向」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

楠田 浩二・櫻井 幸一、「公開鍵暗号方式の安全性評価に関する現状と課題」、『ディスカッションペーパーシリーズ』、97-J-11、日本銀行金融研究所、1997 年

松本 勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

Kusuda, K. and Matsumoto, T, “A Strength Evaluation of the Data Encryption Standard,” Discussion paper series, 97-E-5, Institute for Monetary and Economic Studies, Bank Of Japan, 1997.

National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication (FIPS PUB) 140-1, January 11,1994.

（IC カード等耐タンパー技術関連）

「IC カードのセキュリティ要素技術」、『月刊カードウェーブ』、8 月号、pp.55-57、シーメディア、1998 年

「IC カードのセキュリティ要素技術－その 2－」、『月刊カードウェーブ』、9 月号、pp.54-56、シーメディア、1998 年

五味俊夫・辻秀一、「IC カードのセキュリティをどう守るか？」、『エレクトロニクス』、9 月号、pp.68-72、オーム社、1998 年

竹田忠雄、「IC カードの第四の性能指標：耐タンパー」、『1997 年電子情報通信学会基礎・境界ソサイエティ大会講演論文集』、TA-3-2、pp. 298-299、電子情報通信学会、1997 年

電子商取引実証推進協議会共通セキュリティ関連技術検討 WG、「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」、電子商取引実証推進協議会、1998 年

電子商取引実証推進協議会 IC カード WG、「IC カード利用ガイドライン（接触／非接触）」、電子商取引実証推進協議会、1998 年

Boneh, D., Demillo, R. A., and Lipton, R. J., “A New Breed of Crypto Attack on ‘Tamperproof’ Tokens Cracks Even the Strongest RSA Code”, 25 Sep. 1996.
available at http://www.belllcore.com/PRESS/ADVSRY96/smrtcrd.html
and http://www.belllcore.com/PRESS/ADVSRY96/medadv.html

“Common Criteria for IT Security Evaluation Protection Profile,” Registered at the French Certification Body under the number PP/9704, Oct 1997.

ISO/TC68/SC6, ISO 13491-1 “Banking – Secure cryptographic devices (retail) – Part1: Concepts, requirements and evaluation methods,” 1996.

Paul C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” “URL: http://www.cryptography.com/timingattack/paper.html”, 1995.

――――――――, “Differential Power Analysis,”
”URL: http://www.cryptography.com/dpa/technical/Index.html”

（電子マネープロジェクト等の Home Page）

インターネットキャッシュ, “URL: http://www.icash.gr.jp/”

ミリセント, “URL: http://www.millicent.kcom.ne.jp/”

Danmønt, “URL: http://www.danmoent.dk/”

ecash, “URL: http://www.digicash.com/”

Geldkarte, “URL: http://www.celectronic.de/die.htm”

Mondex, “URL: http://www.mondex.com/”

Net-U, “URL: http://www.u-card.co.jp/”

Proton, “URL: http://www.proton.be/”

Visa Cash, “URL: http://www.visa.com/cgi-bin/vee/nt/cash/main.html”

Webmoney, “URL: http://www.webmoney.ne.jp/”

(電子マネー関連特許)

「電子現金実施方法およびその装置」、日本電信電話(株) 、特公平 7-52460

「電子小口決済システム」、日本銀行、特開平 7-85171

「電子小口決済システムにおける取引方法」、日本銀行、特開平 7-85172

「番号登録式電子現金方法およびその利用者装置」、日本電信電話(株)・日本銀行、特開平 10-091696

「発行機関分離型番号登録式電子現金方法およびその利用者装置」、日本銀行・日本電信電話(株) 、特開平 10-091697

“Electronic monetary system,” CitiBank US Patent Number, 5,453,601

“Electronic monetary system”, CitiBank, US Patent Number 5,455,407

“One-show blind signature systems,” Chaum, David., U.S. Patent No. 4,914,698

“Value Transfer System,” Jonhig Ltd., EPC/EP0479982B1