IMES DISCUSSION PAPER SERIES

電子マネー・システムにおけるセキュリティ対策
—リスク管理に焦点を当てて—

鈴木雅貴（すずきまさたか）・廣川勝久（ひろかわかつひさ）・宇根正志（うねまさし）

Discussion Paper No. 2008-J-3

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2008-J-3
2008 年 2 月

電子マネー・システムにおけるセキュリティ対策
―リスク管理に焦点を当てて―

鈴木雅貴(すずきまさたか)*・廣川勝久(ひろかわかつひさ)**・宇根正志(うねまさし)***

要　旨

近年、電子マネー・サービスが、利用可能な店舗の拡大等を背景に普及しつつある。そうしたなか、一部のサービスにおいては電子マネーを不正に使用する事件等が発生しており、電子マネー・システムの安全性の確保が重要な課題となっている。電子マネー・サービスを安全に運営し提供していくためには、想定される脅威やリスクを分析し、技術と運用の双方から適切なセキュリティ対策を講じる必要がある。

本論文では、こうした問題意識から、中山・太田・松本［1999］をベースに電子マネー・システムのセキュリティ評価を行う。同システムの安全性を考える際に重要な要素技術である IC カード等のデバイスや暗号アルゴリズムの危殆化を想定し、電子マネーによる支払いに関する情報を偽造するという攻撃の成否を検討するほか、運用上の主な対策の効果や課題を検討する。その結果として、デバイスと暗号アルゴリズムが危殆化すると、一部のタイプの電子マネー・システムにおいては攻撃の検知・防止が困難となり、運用面からの対策も必要となることを示す。

こうした検討結果を踏まえると、電子マネー・システムの安全性を確保していくためには、デバイスや暗号アルゴリズムの安全性に常に注意を払い、これらの危殆化を未然に防ぐことがまず必要であるといえる。そのうえで、同システムのリスク管理として、デバイスや暗号アルゴリズムの危殆化に備えて運用面からの対応についても十分に検討しておくことが重要である。

キーワード：電子マネー、セキュリティ評価、リスク管理、暗号アルゴリズム、IC カード、危殆化

JEL classification: L86、L96、Z00

* 日本銀行金融研究所（E-mail: masataka.suzuki@boj.or.jp）

** 日本銀行金融研究所（E-mail: hirokawa@imes.boj.or.jp）

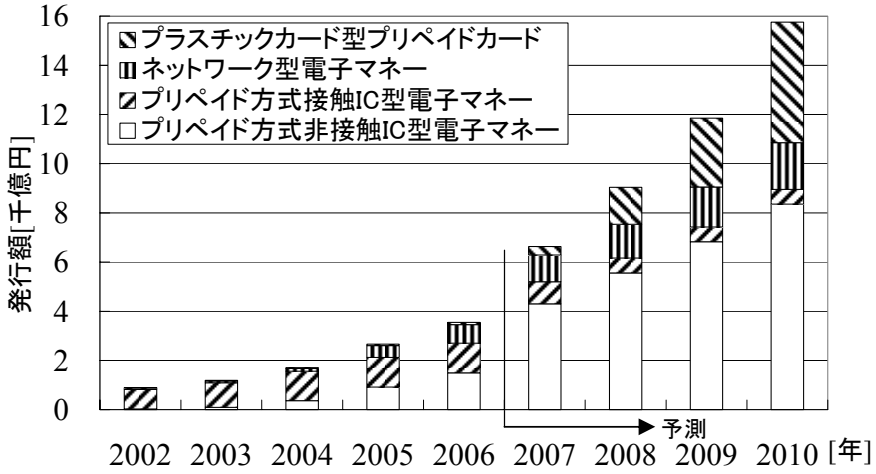
*** 日本銀行金融研究所企画役（E-mail: une@imes.boj.or.jp）

本稿は、2008 年 2 月 5 日に日本銀行で開催された「第 10 回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

目　次

1. はじめに

電子マネー・サービスは、1990 年代に盛んに実証実験が行われ、現在では、利用可能な店舗の拡大等を背景に国内外で実際のサービスとして普及しつつある。矢野経済研究所［2007］によれば、プリペイド方式の電子マネー・サービスにおける電子マネー発行額ベースの市場規模は年々拡大しており、今後も普及の一途をたどると予想されるとのことである（図表 1 参照）。



図表 1：プリペイド方式の電子マネー・サービスの市場規模[1]

こうした電子マネー・サービスによって、店舗等における小額の支払がスムーズになる等の恩恵を享受することができる。しかし、電子マネー・サービスの普及が進むなかで、同サービスを実現するシステム（以下、電子マネー・システムと呼ぶ）に関わるエンティティ（発行者、加盟店、利用者等）が増加するとともに、例えば以下のような不正行為の発生が懸念されている。

- 利用者が電子マネーを偽造し不正に使用する。
- 加盟店が電子マネーによる売上げを水増しして発行者に請求する。
- 加盟店が電子マネーを IC カードに不正にチャージしたり偽造したりする[2]。
- 電子マネーのチャージの際、利用者が入金に関する情報を改ざんする[3]。

---

[1] 矢野経済研究所［2007］を基に作成。本図表のデータは、2006 年までが実績に基づく数値であり、2007 年以降が予測に基づいた数値である。

[2] 電子マネー・サービス「Edy」において、コンビニエンスストアの元オーナーらが客から入金があったように見せかけて Edy カード（IC カード）に不正にチャージを行い、それを使用したという事件が報道されている（2007 年 2 月 22 日、産経新聞東京朝刊）。また、電子マネー自体の偽造の事例ではないが、電子マネー・サービスとしても利用されている共通 IC カード乗車券「Pasmo」のサービスにおいては、東京都交通局の元職員が磁気定期券の金銭データを別の IC カードに不正にコピーし、当該金銭データを払戻ししたという事件も報道されている（2008 年 1 月 23 日、日本経済新聞夕刊）。

また、電子マネーの利用について安全性の観点から不安を感じている利用者も少なくないことを示す調査結果もあり[4]、こうした不安を解消していくことが電子マネー・サービスの円滑な普及のために必要であろう。

電子マネー・システムにおける不正行為を防止するためには、利用する技術や運用方法等を考慮し、システム全体として十分な安全性を確保することが求められる。そうした検討を行う際には、まず、電子マネー・システムにおいてどのような脅威が存在し、どのようなリスクが想定されるかを分析することが必要である。既存の電子マネー・システムを想定した場合、情報セキュリティ上の脅威やリスクを分析するうえで重要な要素技術として、IC カードや加盟店端末等の暗号処理用のデバイスと共通鍵暗号や公開鍵暗号等の暗号アルゴリズムが挙げられる[5]。電子マネー・システムに採用されているこれらの要素技術の安全性にまず着目することが求められる。

デバイスの安全性については、近年、攻撃手法の高度化とともにそれらへの対策も洗練されてきているものの、セキュリティ評価については定量的な評価手法の確立には至っていないのが実情である。そのため、既知の攻撃に対しては相応の対策を講じることは可能であるが、それだけで十分か否かは明確とはいえない。新たな攻撃手法によってデバイスが危殆化し内部の暗号鍵等の秘密情報が露呈してしまうケースも想定しておく必要がある。

また、暗号アルゴリズムの安全性については、近年評価手法がほぼ確立されており、NIST や CRYPTREC[6]等の公的機関によって推奨暗号アルゴリズムの選定や監視作業等が行われている。しかし、危殆化が懸念されている暗号アルゴリズムが運用上の制約等から使用され続けているケースがあるとの指摘もあり（Une and Kanda［2007］、鈴木・神田［2007］）、電子マネー・システムにおいても暗号アルゴリズムが危殆化することを視野に入れた対応を検討することが必

---

[3] 携帯電話を利用した「モバイル Suica」において、不正に入手したカード情報を用いてなりすまし、不正に電子マネーを使用したという事件が報道されている（2007 年 11 月 10 日、産経新聞東京朝刊）。また、インターネットで使用する電子マネー・サービス「WebMoney」においては、振込金額を改ざんするという方法で不正なチャージを行ったという事件が 2007 年 12 月 3 日に報道されている（株式会社ウェブマネーのサイト : http://www.webmoney.jp/news/20071203_1.html）。

[4] 民間調査会社マクロミルが 2007 年 12 月に 20 歳以上約千人を対象にインターネット上で行った調査によれば、電子マネー・システムの安全性に不安を感じている人（「どちらかといえば」を含め「不安」と回答した人）が 64%に上ったと報じられている（2008 年 1 月 14 日、日本経済新聞朝刊）。

[5] 例えば、中山・太田・松本［1999］においても、電子マネー・システムのセキュリティ評価における要素として、デバイスと暗号アルゴリズムを取り上げている。

[6] CRYPTREC（Cryptography Research and Evaluation Committees）：電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクト。暗号研究者をはじめとする専門家がメンバーとなっている暗号技術検討会、暗号技術監視委員会、暗号モジュール委員会で構成されており、総務省と経済産業省が事務局を務めている。

要である。

電子マネー・システムの安全性に関する既存の研究をみると、中山・太田・松本［1999］によって約 10 年前に体系的なセキュリティ評価が行われている。この研究では、デバイスの安全性を客観的に評価することが困難であるとの理由からデバイスが危殆化した状況を想定し、暗号アルゴリズムについては適切に管理されていて安全な状況を想定して分析している。しかし、暗号アルゴリズムの危殆化に関する前述の指摘等を踏まえると、デバイスだけでなく暗号アルゴリズムが危殆化した状況についても想定した評価が必要である。

こうしたことから、本論文では、中山・太田・松本［1999］をベースに、デバイスと暗号アルゴリズムが安全な場合と危殆化している場合の両方を想定し、プリペイド方式の電子マネー・システムにおけるセキュリティ評価を行う。想定する攻撃として、攻撃の発生頻度が相対的に高く、攻撃の阻止や攻撃者の特定が相対的に難しいと考えられる「利用者が加盟店に送る（電子マネーによる）支払いに関する情報」の偽造による不正取引を取り上げ、電子マネー・システムのモデルをいくつかのタイプに類型化し、各タイプにおいて不正取引が成立するか否かを分析する。さらに、デバイスや暗号アルゴリズムが危殆化してしまうという状況のもとでリスクを軽減するための運用上の主な対策を説明し、その効果と課題を整理する。

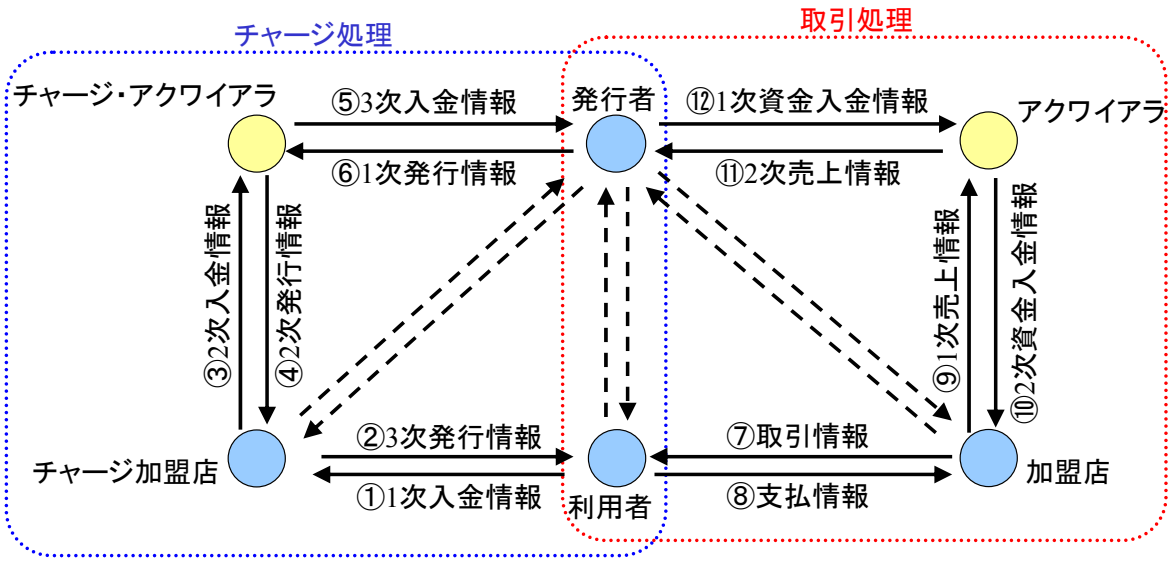
本検討の結果として、デバイスや暗号アルゴリズムの危殆化を想定すると、個々の利用者のデバイス内部で電子マネーの情報を管理する形態やオフラインで取引を行う形態のシステムにおいては、利用者による不正取引を検知することが困難であることが示される。また、不正取引に対する運用上の主な対策については、一定の効果は見込まれるものの、適切に活用するためにはいくつかの課題をクリアすることが必要であることが示される。

本論文の構成は以下のとおりである。2 節では、電子マネー・システムをモデル化したうえでいくつかのタイプに分類し、本論文の検討対象とする電子マネー・システムを特定する。3 節では、各タイプにおける取引の手順と、デバイスや暗号アルゴリズムの危殆化に基づく評価の条件を示したうえで、電子マネーによる支払いに関する情報の偽造による不正取引の成否を分析する。4 節では、電子マネー・システムにおけるリスク管理について説明したうえで、運用上の主な対策の効果と課題を整理する。

2. 電子マネー・システムのモデルと検討対象

(1) 電子マネー・システムのモデル

本論文で検討の対象とするプリペイド方式の電子マネー・システムのモデルは、一般に、図表 2 のように抽象的に表すことができる。



図表 2：プリペイド方式の電子マネー・システムのモデル

イ．エンティティ

電子マネー・システムに関わるエンティティとして以下が挙げられる。

- 発行者：電子マネー・サービスの運営主体であり、電子マネーを発行し、同発行額に相当する資金をチャージ加盟店から得るとともに、電子マネー使用額に対応する資金を加盟店に支払うエンティティ。発行者は電子マネーの取引に関連する情報の処理や管理のためのサーバを安全に運営していると仮定し、物理的な攻撃やネットワーク経由の侵入等に対して安全であり、サーバ内の秘密情報は漏洩しないと仮定する。
- 利用者：電子マネーを発行してもらい、電子マネーを使用して商品やサービスを購入するエンティティ。
- チャージ加盟店：電子マネーをチャージするデバイスを管理し、利用者と発行者間の間に立って電子マネーの発行処理を支援するエンティティ。
- 加盟店：利用者に商品やサービスを販売し、電子マネーによる取引で得られた情報を基に資金を発行者から得るエンティティ。

・ アクワイアラ：電子マネー・システムに参加する新たな加盟店を開拓する業務を発行者に代わって行うエンティティ。また、アクワイアラが複数の加盟店を統括し、発行者のサーバにおける負荷の軽減や加盟店のデバイスとハ行者のサーバ間のネットワークにおける輻輳の解消に貢献する。
・ チャージ・アクワイアラ：アクワイアラと同様に、新たなチャージ加盟店の開拓業務を代行するエンティティ。複数のチャージ加盟店を統括する。

ロ．チャージ処理の流れ

チャージ処理は、利用者が発行者から電子マネーを発行してもらうことに伴って発生する一連の処理であり、ここでは次の手順で実行されるものとする。

・ 利用者は、電子マネー・サービスにおいて取引可能な金額の根拠となる情報（以下、価値情報と呼ぶ）を電子マネーとして発行してもらうために、チャージ加盟店に発行額に対応する金額を入金し、入金に関する情報（以下、1 次入金情報と呼ぶ）をチャージ加盟店のデバイスに送る（図表 2 の①）。
・ 電子マネーの発行に関する情報（以下、3 次発行情報と呼ぶ）は、チャージ加盟店のデバイスから利用者のデバイスに送られる（図表 2 の②）。
・ チャージ加盟店は、チャージ・アクワイアラに対して、チャージ処理で受け取った 1 次入金情報を基に入金を行うとともに、この入金に関する情報（以下、2 次入金情報と呼ぶ）をチャージ加盟店のデバイスからチャージ・アクワイアラのデバイスに送る（図表 2 の③）。
・ 2 次入金情報に対応する電子マネーの発行に関する情報（以下、2 次発行情報と呼ぶ）は、チャージ・アクワイアラのデバイスからチャージ加盟店のデバイスに送られる（図表 2 の④）。
・ チャージ・アクワイアラは、電子マネー・システムの提供者である発行者に対して、チャージ加盟店から受け取った 2 次支払情報を基に入金を行うとともに、この入金に関する情報（以下、3 次入金情報と呼ぶ）をチャージ・アクワイアラのデバイスから発行者のサーバに送る（図表 2 の⑤）。
・ 3 次入金情報に対応する電子マネーの発行に関する情報（以下、1 次発行情報と呼ぶ）は、発行者のサーバからチャージ・アクワイアラのデバイスに送られる（図表 2 の⑥）。

ハ．取引処理の流れ

取引処理は、利用者が電子マネーで加盟店から商品等を購入することに伴って発生する一連の処理であり、ここでは次の手順で実行されるものとする。

・ 利用者は、加盟店から商品やサービスを購入する際、金額、取引時刻、加盟店等の情報（以下、取引情報と呼ぶ）を加盟店のデバイスから受け取る（図表 2 の⑦）。
・ 価値情報を基に代金を支払うことを示す情報（以下、支払情報と呼ぶ）が利用者のデバイスで生成され、加盟店のデバイスに送られる（図表 2 の⑧）。
・ 加盟店のデバイスは、アクワイアラのデバイスに対して、取引処理で受け取った支払情報から集計した売上に関する情報（以下、1 次売上情報と呼ぶ）を送る（図表 2 の⑨）。
・ 加盟店は、アクワイアラから 1 次売上情報に対応する資金を受け取るとともに、その資金に関する情報（以下、2 次資金入金情報と呼ぶ）をアクワイアラのデバイスから受け取る（図表 2 の⑩）。
・ アクワイアラのデバイスは、発行者のサーバに対して、加盟店から受け取った 1 次売上情報から生成した売上情報（以下、2 次売上情報と呼ぶ）を送る（図表 2 の⑪）。
・ アクワイアラは、発行者から 2 次売上情報に対応する資金を受け取るとともに、受け取った資金に関する情報（以下、1 次資金入金情報と呼ぶ）を発行者のサーバから受け取る（図表 2 の⑫）。

なお、電子マネー・システムが単一の組織で運用されている場合や小規模である場合には、発行者が、チャージ加盟店や加盟店を直接統括したり、利用者と直接やり取りをしたりすることが考えられる(図表 2 の破線のケースに相当)。

ニ．ポストペイ方式の電子マネー・システム

図表 2 に示したモデルにおいて、1 次入金情報と 3 次発行情報のやり取りが取引情報と支払情報のやり取りの後に発生するというかたちで取引の順序を変えると、ポストペイ方式の電子マネー・システムのモデルとなる。ただし、プリペイド方式とポストペイ方式では、利用者からの入金のタイミングが異なるため、想定されるリスクも異なる。したがって、ポストペイ方式の電子マネー・システムのセキュリティ評価やリスク管理について検討を行う場合には、本論文において以下で行う検討とは別に、ポストペイ方式を前提とした検討を行うことが必要である。

(2) デバイス、暗号アルゴリズム、攻撃手法に関する想定

電子マネー・システムの安全性を検討するうえで、まず、本システムの安全性を大きく左右する要素技術として、IC カードや加盟店端末等の暗号処理用のデバイスと共通鍵暗号や公開鍵暗号等の暗号アルゴリズムに焦点を当てる。

イ．暗号処理用のデバイスの安全性

暗号処理用のデバイスの安全性に関する研究動向をみると、90 年代後半、デバイスの消費電力等を測定することによってデバイス内の暗号鍵を推定するサイドチャネル攻撃が提案されたほか（Kocher［1996］、Kocher, et al.［1999］）、故意にデバイスに異常な処理を行わせることで得られた情報を暗号鍵の推定に利用する故障利用攻撃等の新しい攻撃手法も提案された。また、近年では、サイドチャネル攻撃と故障利用攻撃を組み合わせた攻撃手法等が提案されており、攻撃手法が高度化してきている。こうした新しい攻撃手法への対策に関する研究も盛んになってきているものの、そうした対策の定量的なセキュリティ評価手法については確立されているとは言いがたいのが現状である。

暗号処理用のデバイスの安全性を評価する枠組みについては、90 年代には、一定のセキュリティ要件を満足しているか否かの試験を行いその結果を認証する制度が整備されている。例えば、米国とカナダの政府によって暗号モジュールの試験・認証制度 CMVP（Cryptographic Module Validation Program）の運用が 1995 年から開始されているほか、わが国では同様の制度として JCMVP（Japan Cryptographic Module Validation Program, IPA［2007］）が 2007 年 4 月から開始されている。また、クレジットカード取引向けの IC カードと端末を対象とする試験・認証として、EMVCo の枠組み（EMVCo［2006］）が知られている[7]。

こうした認証を得たデバイスを利用することで、試験・認証の際に考慮された攻撃手法に対しては相応の安全性を確保できると考えられる。ただし、試験・認証の対象となっていない、あるいは、新しく提案されたばかりであり対策が確立されていない攻撃手法を前提とすれば、上記の制度による評価・認証を得たデバイスであったとしても危殆化するおそれは否定できない。

ロ．暗号アルゴリズムの安全性

暗号アルゴリズムの安全性に関する研究動向をみると、近年、共通鍵暗号や公開鍵暗号の安全性の概念等に関する研究が進展しており、セキュリティ評価手法が成熟してきているといえる。こうした評価手法に基づいて公的機関によって暗号アルゴリズムの評価・選定が行われ、その推奨期間とともに公表されている。例えば、欧州では暗号アルゴリズムの評価プロジェクト NESSIE（New European Schemes for Signatures, Integrity, and Encryption）による推奨暗号の公募・選定が行われたほか（NESSIE consortium［2003］）、わが国では CRYPTREC による電子政府推奨暗号リストの作成が行われた（総務省・経済産業省［2003］）。米国においても、連邦政府内の情報システムにおいて利用される暗号アルゴリ

[7] これらの暗号モジュールの試験・認証制度については、田村・宇根［2008］を参照されたい。

ズムとその鍵長に関するガイドライン（NIST［2005］）等が策定されている。電子マネー・システムにおいても、こうした第三者による評価を得た暗号アルゴリズムを選択することが望まれる。

ただし、システム修正のコストや他のシステムとの互換性の維持等の運用上の制約から、安全性の低下が著しい暗号アルゴリズムを使い続けてしまい、暗号アルゴリズムの危殆化が情報システム自体の安全性低下につながる可能性が懸念される事例が指摘されている（Une and Kanda［2007］、鈴木・神田［2007］）。現行の電子マネー・システムの中には、利用者のデバイスとして採用されているICカードに有効期限が設定されていないものがある。この場合、新しい暗号アルゴリズムへの移行や鍵長の伸長が必要となったとしても古いカードが使われ続ける可能性があり、古いカードの暗号アルゴリズムが危殆化して内部の暗号鍵が漏洩し、当該カードの偽造につながるおそれがある[8]。

ハ．デバイスと暗号アルゴリズムについての想定

電子マネー・システムのセキュリティ評価に関する検討は、約10年前に先行研究として中山・太田・松本［1999］によって行われている。中山・太田・松本［1999］は、デバイスに対する攻撃として、デバイスに物理的損傷を与えて回路内部を観察する破壊解析と、デバイスに物理的損傷を与えずにその動作時に得られる消費電力等の情報を用いて暗号鍵を推定する非破壊解析を挙げている。ただし、これらの攻撃について、「オープンな場でデバイスの安全性に関する議論が尽くされているとは言いがたく、安全性を客観的に評価することが困難である」と指摘し、デバイスが危殆化した場合のみを想定して分析を行っている。また、暗号アルゴリズムについては、暗号アルゴリズムと鍵長が適切に管理されると想定し、暗号アルゴリズムが安全である場合のみを想定している。

本論文では、上記のイ．とロ．の整理を踏まえ、デバイスと暗号アルゴリズムが安全である場合と危殆化している場合の両方を想定して分析を行うこととする。これらの安全性に関する条件（以下、環境条件と呼ぶ）に関して、中山・太田・松本［1999］と本論文の差異は図表3のとおりである。

---

[8] こうした事例の1つとして、フランス銀行カード協会（Cartes Bancaires）の仕様に準拠したICカードの偽造事件が挙げられる（松本・岩下［2001］）。フランスでは1989年にRSA署名方式（鍵長200ビット程度）を実装した金融取引用ICカードが発行されたが、その後も古いICカードが使い続けられ、1999年から2000年にかけてそれらのICカードが偽造されたという事例がある。

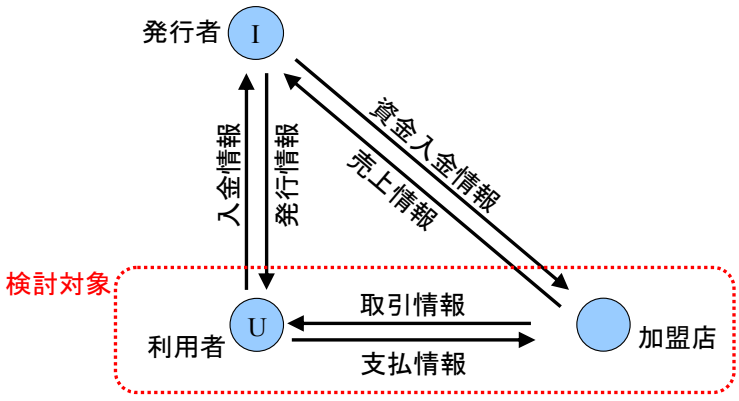
	中山・太田・松本[1999]	本論文
デバイス	危殆化している状況を想定。	安全である状況と危殆化している状況の両方を想定。
暗号アルゴリズム	安全である状況を想定。	安全である状況と危殆化している状況の両方を想定。

図表 3：環境条件の比較

ニ．検討対象とする攻撃手法

仮にデバイスや暗号アルゴリズムが危殆化した場合、電子マネー・システムにおいて処理される各情報（入金情報、発行情報、取引情報、支払情報、売上情報、資金入金情報）は盗聴されたり偽造されたりするおそれがある。これらのうち、本論文では、支払情報の偽造に着目し、「偽造された支払情報を用いて商品やサービスを不正に購入する」という攻撃を検討対象とする。支払情報は、システムのエンティティ間でやり取りされる頻度が相対的に多く、不特定多数の利用者に攻撃者が紛れ込み、攻撃の阻止や攻撃者の特定が相対的に困難とみられることから、最初に攻撃の標的となりやすいと考えられる[9]。

支払情報の偽造を検討対象とする場合、支払情報をやり取りする利用者と加盟店に焦点を当てた 3 エンティティ（発行者・利用者・加盟店）のモデルに簡略化して検討することが可能であり、図表 4 に示すモデルを検討対象とする。ただし、アクワイアラは不正を行わないことを仮定する[10]。



図表 4：　検討対象とする 3 エンティティのモデル

[9] 電子マネー・システムで処理されるその他の情報についても、デバイスや暗号アルゴリズムの危殆化によって安全性に何らかの影響が及ぶ可能性がある。これらの情報の偽造の可否を分析する際は、支払情報の偽造に関する分析が参考になると考えられる。また、本論文では直接検討対象としないが、デバイスと暗号アルゴリズムが安全であっても運用上の不備を突いた攻撃が想定される。そうした攻撃についても適切な対策を講じる必要がある。

[10] アクワイアラの不正を想定する場合、アクワイアラを含めたモデルを用いて、アクワイアラの処理を考慮したうえで分析する必要がある。

偽造の対象となる支払情報に関しては、①攻撃者本人の支払情報（攻撃者が正規の利用者として電子マネー・システムに登録している場合）、②電子マネー・システムに登録している他の利用者の支払情報、③登録していない架空の利用者の支払情報という 3 つのバリエーションが想定される。これらの偽造による攻撃をそれぞれ本人支払情報偽造、他人支払情報偽造、架空利用者支払情報偽造と呼び、検討の対象とする。

(3) 電子マネー・システムの分類

電子マネー・システムはこれまで様々な方式が提案されている。ここでは、電子マネー・システムのモデルを分類し、検討対象を特定する。

イ．先行研究における分類

電子マネーの研究については、方式の提案以外にも、電子マネー・システムに関する情報セキュリティ上の性質が多数提案されている。例えば、匿名性[11]や否認防止等の性質がよく知られており、Chida, et al.［2001］にまとめられている。本論文では支払情報を偽造し商品やサービスを不正に購入する攻撃を検討対象としているが、こうした攻撃への耐性は Chida, et al.［2001］における耐偽造性（unforgeability）に対応すると考えられる。

耐偽造性を検討する際の分類方法としては、宮崎・櫻井［1998］が挙げられる。宮崎・櫻井［1998］は、発行者の不正行為を分析の対象としており、発行者に登録する利用者の暗号鍵の形態によって電子マネー・システムを分類している。ただし、宮崎・櫻井［1998］では支払情報の偽造という観点からの分類が行われておらず、本論文では採用しないこととする。

これに対して、中山・太田・松本［1999］では、支払情報の生成に関わる価値情報の管理場所や支払情報を処理するエンティティといった観点から電子マネー・システムが分類されており、支払情報の偽造の成否に関連している。そこで、本論文では中山・太田・松本［1999］の分類方法を用いることとする。

ロ．中山・太田・松本［1999］における分類の観点

中山・太田・松本［1999］における電子マネー・システムの分類方法を説明する。中山・太田・松本［1999］は、（イ）電子マネーの価値の形態、（ロ）転々流通性の有無、（ハ）センター接続の有無、（ニ）価値情報の管理場所に注目して分類を行っている。

---

[11] 匿名性とは、発行者や加盟店が、どの利用者が購入したのかわからない、あるいは、監視している利用者が何を購入したのかわからないといった性質を指す。

（イ）電子マネーの価値の形態

電子マネー・システムはその価値の形態という観点から残高管理型と電子証書型に分類される。残高管理型では、チャージや取引時に価値情報を増減することで発行や支払の処理を行う。電子証書型では、個々の価値情報が額面金額や識別番号等の情報を有し、価値情報を識別可能である。

（ロ）転々流通性の有無

転々流通性は、発行者のサーバを介在することなく利用者のデバイスから別の利用者のデバイスに価値情報を譲渡できるという性質である。この性質を満たすものをオープンループ型、満たさないものをクローズドループ型と呼ぶ。

（ハ）センター接続の有無

利用者と加盟店間の取引におけるセンター（発行者のサーバ）への接続の必要性という観点から分類される。取引毎に必ず発行者のサーバに接続して問い合わせる必要があるオンライン型と、発行者のサーバに問い合わせる必要がないオフライン型が存在する。

（ニ）価値情報の管理場所

価値情報の管理場所としては、ローカル（利用者のデバイス)、センター（発行者のサーバ)、あるいは両者の併用が想定される。それぞれ、ローカル管理、センター管理、併用管理と呼ぶ。

ハ．検討対象とする電子マネー・システムのタイプ

中山・太田・松本［1999］は、これらの特徴を組み合わせて、電子マネー・システムのモデルを複数のタイプに分類している（図表 5 参照)。ただし、上記の（イ）～（ニ）には次の関係 1～3 が存在し、すべてのタイプが実現されるわけではないとされている。

- 【関係 1】発行者のサーバに接続せず発行者のサーバで利用者の価値情報を管理することは不可能である。
- 【関係 2】オープンループ型は「発行者のサーバを介在せずに利用者のデバイスから別の利用者のデバイスに価値情報を譲渡することができるもの」であり、取引毎に発行者のサーバに接続し情報のやり取りが必要なタイプは、オープンループ型とはいえない。
- 【関係 3】電子証書型はデータ自体が価値を持つとの考え方で設計されてお

り、管理場所はローカル（利用者のデバイス）しかあり得ない。

転々流通性	クローズドループ型						オープンループ型					
センター接続	オフライン型			オンライン型			オフライン型			オンライン型		
価値情報の管理場所	ローカル	併用	センター	ローカル	併用	センター	ローカル	併用	センター	ローカル	併用	センター
タイプ	○ 型1	○ 型2	× ※1	○ 型3	○ 型4	○ 型5	○ 型6	× ※1	× ※1	× ※2	× ※2	× ※2

(1) 残高管理型の電子マネー・システムの各タイプ

転々流通性	クローズドループ型						オープンループ型					
センター接続	オフライン型			オンライン型			オフライン型			オンライン型		
価値情報の管理場所	ローカル	併用	センター	ローカル	併用	センター	ローカル	併用	センター	ローカル	併用	センター
タイプ	○ 型7	× ※3	× ※3	○ 型8	× ※3	× ※3	○ 型9	× ※3	× ※3	× ※2	× ※3	× ※3

(2) 電子証書型の電子マネー・システムの各タイプ

図表 5：電子マネー・システムのモデルの分類[12]

このように 9 個のタイプ（型 1～9）が想定されるが、現行の電子マネー・システムをみると、クローズドループ型のシステムが主流のようであるほか、電子マネー・システムを設計する際、電子証書型のシステムよりも暗号処理や通信の負荷が相対的に軽く実装しやすい残高管理型のシステムが多いと推測される[13]。こうしたことから、残高管理型でクローズドループ型の 5 個のタイプ（型 1～5）を検討対象とする（図表 6 参照）。

	型1	型2	型3	型4	型5
価値の形態	残高管理型				
転々流通性	クローズドループ型				
センター接続	オフライン型		オンライン型		
価値情報の管理場所	ローカル管理	併用管理	ローカル管理	併用管理	センター管理

図表 6：検討対象とする電子マネー・システムのタイプ

[12] 本図表は中山・太田・松本［1999］を基に作成した。図表中の「○」は実現可能なモデル、「×」は実現不可能なモデルを意味し、「ローカル」はローカル管理型、「併用」は併用管理型、「センター」はセンター管理型を意味する。「※1」～「※3」は該当するモデルが存在しない理由（【関係 1】～【関係 3】）にそれぞれ対応する。

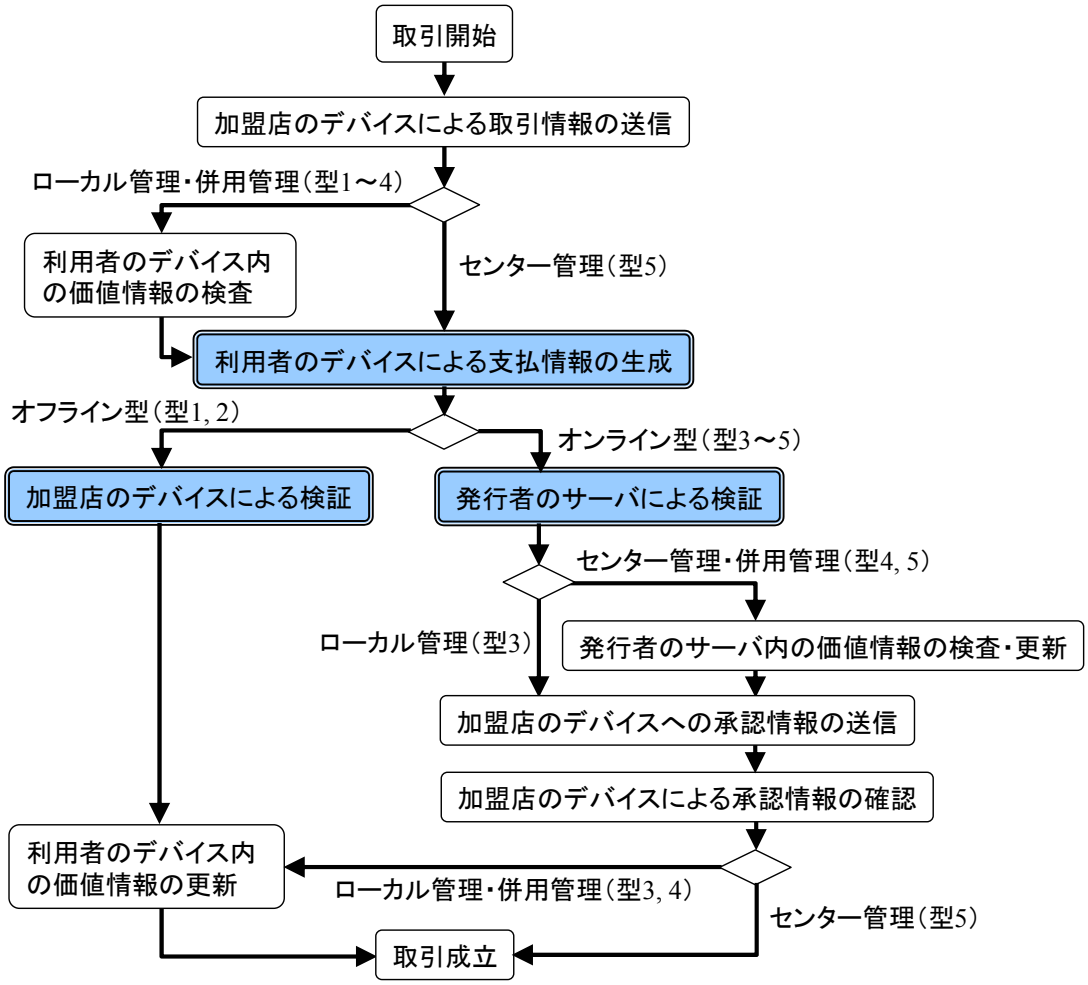
[13] 例えば、利用者のデバイスとして非接触型 IC カードを採用し、1 秒に満たない時間で（利用可能な金額以内で）任意の金額の取引を実現しているシステムが存在する。本システムを電子証書型で実現するためには、公開鍵暗号系の処理を高速に処理する IC チップが必要となり、利用者に配付する IC カードが高額になると予想される。こうした事情を勘案すると、本システムでは、残高管理型を採用しているとみられる。

3. 電子マネー・システムのセキュリティ評価

本節では、電子マネー・システムの 5 つのタイプ（型 1～5）において、デバイスと暗号アルゴリズムの安全性を考慮したセキュリティ評価を行う。まず、検討の前提とする電子マネー・システムにおける典型的な取引プロトコルを説明し、想定する環境条件を定義する。次に、各環境条件において攻撃者が利用可能となる情報を整理し、これらの情報を利用した支払情報の偽造による不正な取引が成立するか否かを分析する。

(1) 取引プロトコルの設定

支払情報を用いた取引プロトコルを図表 7 に示す。取引プロトコルは、価値情報の管理場所やセンター接続の有無によって差異が生じる。



図表 7：検討の際に前提とする取引プロトコルの処理フロー

イ．各型による取引プロトコルの差異

価値情報が利用者のデバイス内で管理される場合（ローカル管理と併用管理）には、支払情報の生成前に、取引金額に対して価値情報が足りているか否かが検査され、支払情報の検証後に、取引金額に応じて価値情報が更新される。一方、価値情報が発行者のサーバ内で管理される場合（センター管理と併用管理）には、取引金額に対して価値情報が足りているか否かが発行者のサーバ内で検査され、足りている場合には取引金額に応じて価値情報が更新される。

オフライン型では、加盟店のデバイスは支払情報を検証し問題がなければ取引を成立させる。オンライン型では、発行者のサーバが支払情報を検証し、問題がなければ取引を承認する情報（以下、承認情報と呼ぶ）を加盟店のデバイスへ送信する。加盟店のデバイスは、承認情報を確認したうえで取引を成立させる。なお、オンライン型における取引では、発行者のサーバが価値情報を管理している場合（センター管理と併用管理）にのみ、発行者のサーバによる利用者の価値情報の検査と更新が行われる。

ロ．利用する暗号アルゴリズムによる取引プロトコルの差異

中山・太田・松本［1999］は、攻撃場所としてデバイスと通信路を選択し、利用者のデバイスの真正性確認と通信データ保護（真正性確保や守秘）に注目して取引プロトコルを 3 つに大別している（図表 8 参照）。①デバイスの真正性確認と通信データ保護に共通鍵暗号方式を用いる方式（以下、M1 方式と呼ぶ）、②デバイスの真正性確認と通信データ保護にそれぞれ電子署名方式と共通鍵暗号方式を用いる方式（以下、M2 方式と呼ぶ）、③デバイスの真正性確認と通信データ保護に電子署名方式を用いる方式（以下、M3 方式と呼ぶ）である。本論文においても、これらの方式について検討することとする。

方式	利用者のデバイスの真正性確認	通信データ保護
M1方式	共通鍵暗号方式	
M2方式	電子署名方式	共通鍵暗号方式
M3方式	電子署名方式	

図表 8：M1～M3 方式で利用される暗号アルゴリズム

図表 7 における「利用者のデバイスによる支払情報の生成」、「加盟店のデバイスによる検証」、「発行者のサーバによる検証」の内容は、M1～M3 方式によって変わってくる。次に、これら 3 つの処理についてそれぞれ説明する。

（イ）記号の定義

まず、本論文で使用する記号を以下のとおり定義する。

記号	定義
ID_U, $ID_{U'}$	利用者 U および他の実在する利用者 U'の識別情報。
ID_{U*}	攻撃者が生成する実在しない利用者 U*[14]の識別情報。
V_U	利用者 U の価値情報。
PK_U, SK_U	利用者 U の公開鍵と秘密鍵のペア。
$PK_{U'}$, $SK_{U'}$	利用者 U'の公開鍵と秘密鍵のペア。
PK_{U*}, SK_{U*}	攻撃者が生成する利用者 U*の公開鍵と秘密鍵のペア。
PK_I, SK_I	発行者の公開鍵と秘密鍵のペア。
K	共通鍵暗号方式の暗号鍵。
$E_X(Y)$	暗号鍵 X で平文 Y を暗号化した暗号文。X を用いて復号可能。
$S_X(Y)$	エンティティ X がメッセージ Y に対して施した署名。
DT	取引情報（取引対象の商品の金額、時刻、加盟店等の情報を含む）。
DB(ID)	正規の利用者の ID に関するデータベース。
DB(PK)	正規の利用者の公開鍵に関するデータベース。
DB(V)	正規の利用者の価値情報に関するデータベース。

（ロ）各エンティティが管理する情報

型 1～5 の各特徴と M1～M3 方式において利用される暗号アルゴリズムの種類から、各エンティティが管理する情報を検討すると図表 9 のとおりになる。

<table>
<tr><th>型</th><th>利用者のデバイス</th><th>加盟店のデバイス</th><th>発行者のサーバ</th></tr>
<tr><td>型1</td><td rowspan="4">M1方式：K, ID_U, V_U
M2方式：K, $S_I(ID_U)$, V_U
M3方式：SK_U, $S_I(PK_U)$, V_U</td><td rowspan="2">M1方式：K
M2方式：K, PK_I
M3方式：PK_I</td><td>M1方式：K, DB(ID)
M2方式：K, PK_I, SK_I, DB(ID)
M3方式：PK_I, SK_I, DB(PK)</td></tr>
<tr><td>型2</td><td>M1方式：K, DB(ID), DB(V)
M2方式：K, PK_I, SK_I, DB(ID), DB(V)
M3方式：PK_I, SK_I, DB(PK), DB(V)</td></tr>
<tr><td>型3</td><td rowspan="2">M1～M3方式：なし</td><td>M1方式：K, DB(ID)
M2方式：K, PK_I, SK_I, DB(ID)
M3方式：PK_I, SK_I, DB(PK)</td></tr>
<tr><td>型4</td><td rowspan="2">M1方式：K, ID_U
M2方式：K, $S_I(ID_U)$
M3方式：SK_U, $S_I(PK_U)$</td><td>M1方式：K, DB(ID), DB(V)
M2方式：K, PK_I, SK_I, DB(ID), DB(V)
M3方式：PK_I, SK_I, DB(PK), DB(V)</td></tr>
<tr><td>型5</td></tr>
</table>

図表 9：各エンティティが管理する情報

[14] 本論文では、「U*」を「実在しない利用者」を表す記号として用いているが、中山・太田・松本［1999］では、「実在しない利用者および実在する利用者をあわせた任意の利用者」を表す記号として用いている。

（ハ）利用者のデバイスによる支払情報の生成

利用者のデバイスによる支払情報の生成は、すべての型において行われる。

M1 方式では、暗号鍵 K を用いて利用者の識別情報 ID_U と取引情報 DT が暗号化され、支払情報 $E_K(ID_U, DT)$が生成される。M2 方式では、暗号鍵 K を用いて発行者の署名付き識別情報 $S_I(ID_U)$と取引情報 DT が暗号化され、支払情報 $E_K(S_I(ID_U), DT)$が生成される。M3 方式では、利用者の秘密鍵 SK_U を用いて取引情報 DT に署名が施され、支払情報 $S_U(DT)$が生成される。

（ニ）加盟店のデバイスによる検証

加盟店のデバイスによる支払情報の検証は、型 1, 2 において実施される。

M1 方式では、暗号鍵 K を用いて支払情報 $E_K(ID_U, DT)$を復号し、当該取引に対する取引情報 DT が含まれているか否かを確認する。M2 方式では、暗号鍵 K を用いて支払情報 $E_K(S_I(ID_U), DT)$を復号し、発行者の公開鍵 PK_I を用いて $S_I(ID_U)$を検証するとともに、当該取引の取引情報 DT が含まれているか否かを確認する。M3 方式では、発行者の公開鍵 PK_I を用いて公開鍵証明書 $S_I(PK_U)$を検証し、利用者の公開鍵 PK_U を取り出す。PK_U を用いて支払情報 $S_U(DT)$を検証し、当該取引の取引情報 DT が含まれているか否かを確認する。

（ホ）発行者のサーバによる検証

発行者のサーバによる支払情報の検証は、型 3〜5 において実施される。

M1 方式では、暗号鍵 K を用いて支払情報 $E_K(ID_U, DT)$を復号し、ID_U の登録の有無を確認する。M2 方式では、暗号鍵 K を用いて支払情報 $E_K(S_I(ID_U), DT)$を復号し、発行者の公開鍵 PK_I を用いて $S_I(ID_U)$を検証するとともに、ID_U の登録の有無を確認する。M3 方式では、発行者の公開鍵 PK_I を用いて公開鍵証明書 $S_I(PK_U)$を検証し、利用者の公開鍵 PK_U を取り出す。PK_U が正規の利用者の公開鍵であるか否かを確認したうえで、支払情報 $S_U(DT)$を検証する。なお、発行者のサーバが当該利用者の価値情報を管理している場合（型 4, 5）には、当該利用者の価値情報の検査と更新が行われる。

(2) 環境条件

2 節で述べたように、本論文では、デバイスと暗号アルゴリズムが安全であるという状況と危殆化している状況の両方を想定する。

イ．デバイスの安全性

「デバイスが安全である」とは、破壊解析や非破壊解析によってデバイス内に格納されている暗号鍵等の秘密情報が読出困難な状況を意味するものとする。また、「デバイスが危殆化している」とは、破壊解析等によってデバイス内の暗号鍵等が読出可能な状況を意味するものとする。利用者と加盟店の両者のデバイスが安全であるという状況を「D0」、両者のデバイスが危殆化しているという状況を「D1」と呼ぶ。

ロ．暗号アルゴリズムの安全性

「暗号アルゴリズムが安全である」とは、解読や署名の偽造等が困難な状況を意味し、「暗号アルゴリズムが危殆化している」とは、該当暗号鍵や秘密鍵を現実的な時間内に求めることが可能であるという状況を意味するものとする。暗号アルゴリズムの危殆化によってデバイス内に格納されている暗号鍵等を入手可能な場合は、デバイスの危殆化には含めないこととする。

また、発行者が利用者の識別情報（ID や公開鍵等）に対して署名を施すために利用する電子署名方式（以下、発行者用署名方式と呼ぶ）は、利用者が支払情報を生成するために利用する電子署名方式（以下、利用者用署名方式と呼ぶ）よりも安全性が高く設定されていることが一般的であり[15]、本論文においても発行者用署名方式の方が安全性が高いと仮定する。以下では、暗号アルゴリズムとして共通鍵暗号方式、利用者用署名方式、発行者用署名方式を想定し、各暗号アルゴリズムが安全である状況をそれぞれ「S0」、「A_U0」、「A_I0」と呼び、危殆化している状況をそれぞれ「S1」、「A_U1」、「A_I1」と呼ぶ。

ハ．想定する環境条件

環境条件は各方式で利用される暗号アルゴリズムに依存する。M1～M3 方式において想定される環境条件のバリエーションを図表 10 に示す。ただし、M3 方式においては、発行者用署名方式が危殆化した場合、利用者用署名方式も危殆化するという状況を想定する。図表 10 中の環境条件の標記について説明すると、例えば、M1 方式における「D0-S0」は「デバイスと共通鍵暗号方式がどちらも安全である」という状況を示しているほか、M2 方式における「D0-S1-A_I0」は、「デバイスと発行者用署名方式は安全であるが、共通鍵暗号方式は危殆化している」という状況を示している。

なお、攻撃者は、共通鍵暗号方式、利用者用署名方式、発行者用署名方式と

[15] 利用者用署名方式より発行者用署名方式の公開鍵の鍵長が長いケース等が挙げられる。

してどのようなアルゴリズムが採用されているかを知っていると仮定する。

方式	表記	環境条件			
		デバイス	暗号アルゴリズム		
			共通鍵暗号方式	利用者用署名方式	発行者用署名方式
M1方式	D0-S0	安全D0	安全S0		
	D0-S1		危殆化S1		
	D1-S0	危殆化D1	安全S0		
	D1-S1		危殆化S1		
M2方式	D0-S0-A_I0	安全D0	安全S0		安全A_I0
	D0-S1-A_I0		危殆化S1		安全A_I0
	D0-S0-A_I1		安全S0		危殆化A_I1
	D0-S1-A_I1		危殆化S1		危殆化A_I1
	D1-S0-A_I0	危殆化D1	安全S0		安全A_I0
	D1-S1-A_I0		危殆化S1		安全A_I0
	D1-S0-A_I1		安全S0		危殆化A_I1
	D1-S1-A_I1		危殆化S1		危殆化A_I1
M3方式	D0-A_U0-A_I0	安全D0		安全A_U0	安全A_I0
	D0-A_U1-A_I0			危殆化A_U1	安全A_I0
	D0-A_U1-A_I1			危殆化A_U1	危殆化A_I1
	D1-A_U0-A_I0	危殆化D1		安全A_U0	安全A_I0
	D1-A_U1-A_I0			危殆化A_U1	安全A_I0
	D1-A_U1-A_I1			危殆化A_U1	危殆化A_I1

図表 10：M1～M3 方式における環境条件のバリエーション

(3) 攻撃者がアクセスするデバイス

攻撃者が攻撃実行時にアクセスするデバイスとしては、利用者と加盟店のデバイスが想定される。

攻撃者が利用者のデバイスにアクセスする場合には、利用者のデバイスに対して直接破壊解析や非破壊解析を行い、内部の暗号鍵や秘密鍵を読み出すという状況が考えられる。

攻撃者が加盟店のデバイスにアクセスする場合、実際の店舗における取引では、利用者のデバイス（IC カード等）を加盟店のデバイス（カード・リーダ等）に提示・挿入させる状況が一般的であることから、加盟店のデバイス内部の暗号鍵や秘密鍵に加え、同デバイスを経由して利用者のデバイスに対して非破壊解析を行い、その内部の暗号鍵等を読み出す状況も考えられる。一方、ネットワーク上の店舗での取引においては、利用者のデバイス（PC 等）と加盟店のデバイス（PC 等）はネットワーク経由で通信することから、取引時に利用者のデバイスに非破壊解析を適用して暗号鍵等を読み出すことは現時点では困難と考えられる。

こうしたことから、①（攻撃者本人が所持する）利用者のデバイスの暗号鍵

等を入手するケース、②加盟店のデバイスの暗号鍵等を入手するケース、③加盟店のデバイスの暗号鍵等に加え、同デバイスを経由して（複数の）利用者のデバイスの暗号鍵等も入手するケースの 3 つが考えられる。

(4) デバイス等の危殆化時に攻撃者が入手する情報

暗号アルゴリズムやデバイスが危殆化した際に攻撃者が入手する情報は、以下のとおりとなる。

- 攻撃者は、共通鍵暗号方式が危殆化している状況（S1）のもとで、暗号鍵 K を入手する。
- 攻撃者は、利用者用署名方式が危殆化している状況（A_U1）のもとで、利用者本人の秘密鍵 SK_U と他の利用者の秘密鍵 $SK_{U'}$を入手する。
- 攻撃者は、発行者用署名方式が危殆化している状況（A_I1）のもとで、発行者の秘密鍵 SK_I を入手する。
- 攻撃者は、デバイスが危殆化している状況（D1）のもとで、当該デバイスの種類に応じて、①（攻撃者本人が所持する）利用者のデバイスの暗号鍵等を入手するケース、②加盟店のデバイスの暗号鍵等を入手するケース、③加盟店のデバイスの暗号鍵等、および、同デバイスと交信する（複数の）利用者のデバイスの暗号鍵等の両方を入手するケースがある。

これらをもとに、各方式において攻撃者が入手する情報をまとめると図表 11 のとおりである。

M1 方式においては、攻撃者は、暗号鍵 K を入手する場合と入手しない場合があることがわかる。M2 方式においては、攻撃者は、暗号鍵 K を入手する場合、発行者の秘密鍵 SK_I を入手する場合、これら両方を入手する場合、いずれの鍵も入手しない場合の 4 通りがあることがわかる。M3 方式では、攻撃者は、攻撃者本人の秘密鍵 SK_U を入手する場合、SK_U と他の実在する利用者の秘密鍵 $SK_{U'}$を入手する場合、SK_U と $SK_{U'}$と発行者の秘密鍵 SK_I の 3 つを入手する場合、いずれの鍵も入手しない場合の 4 通りがあることがわかる。

攻撃者はこれらの情報を用いて支払情報の偽造を試みることとなる。

方式	環境条件	攻撃者がアクセスするデバイス	型1	型2	型3	型4	型5
M1方式	D0-S0	利用者のデバイス	なし				
		加盟店のデバイス					
		両者のデバイス					
	D0-S1	利用者のデバイス	K				
		加盟店のデバイス					
		両者のデバイス					
	D1-S0	利用者のデバイス	K				
		加盟店のデバイス	K		なし		
		両者のデバイス	K				
	D1-S1	利用者のデバイス	K				
		加盟店のデバイス					
		両者のデバイス					
M2方式	D0-S0-A_I0	利用者のデバイス	なし				
		加盟店のデバイス					
		両者のデバイス					
	D0-S1-A_I0	利用者のデバイス	K				
		加盟店のデバイス					
		両者のデバイス					
	D0-S0-A_I1	利用者のデバイス	SK_I				
		加盟店のデバイス					
		両者のデバイス					
	D0-S1-A_I1	利用者のデバイス	K, SK_I				
		加盟店のデバイス					
		両者のデバイス					
	D1-S0-A_I0	利用者のデバイス	K				
		加盟店のデバイス	K		なし		
		両者のデバイス	K				
	D1-S1-A_I0	利用者のデバイス	K				
		加盟店のデバイス					
		両者のデバイス					
	D1-S0-A_I1	利用者のデバイス	K, SK_I				
		加盟店のデバイス	K, SK_I		SK_I		
		両者のデバイス	K, SK_I				
	D1-S1-A_I1	利用者のデバイス	K, SK_I				
		加盟店のデバイス					
		両者のデバイス					
M3方式	D0-A_U0-A_I0	利用者のデバイス	なし				
		加盟店のデバイス					
		両者のデバイス					
	D0-A_U1-A_I0	利用者のデバイス	SK_U, $SK_{U'}$				
		加盟店のデバイス					
		両者のデバイス					
	D0-A_U1-A_I1	利用者のデバイス	SK_U, $SK_{U'}$, SK_I				
		加盟店のデバイス					
		両者のデバイス					
	D1-A_U0-A_I0	利用者のデバイス	SK_U				
		加盟店のデバイス	なし				
		両者のデバイス	SK_U, $SK_{U'}$				
	D1-A_U1-A_I0	利用者のデバイス	SK_U, $SK_{U'}$				
		加盟店のデバイス					
		両者のデバイス					
	D1-A_U1-A_I1	利用者のデバイス	SK_U, $SK_{U'}$, SK_I				
		加盟店のデバイス					
		両者のデバイス					

図表 11：各環境条件のもとで攻撃者が入手する情報

(5) 支払情報の偽造の成否

図表 11 の結果を用いて、3 種類の支払情報の偽造（本人支払情報偽造、他人支払情報偽造、架空利用者支払情報偽造）がそれぞれ成功するか否かを分析する。ここで、「支払情報の偽造が成功する」とは、加盟店あるいは発行者が当該支払情報の偽造を検知できない状況を意味するものとする。偽造がどの程度成功するかに関しては、①成功しない、②特定の条件のもとでのみ成功する、③成立するという 3 段階に分類することができるが、以下ではこれらの各段階をそれぞれ「0」、「1」、「2」という数字を割り当てて説明する。

本分析の結果は図表 12 のとおりである[16]。同図表では、「0-1-0」といったように 3 つの数字を連結して表示している。これは、左から 1 番目の数字が本人支払情報偽造の成否のレベル、2 番目が他人支払情報偽造の成否のレベル、3 番目が架空利用者支払情報偽造の成否のレベルを示している。例えば、「0-1-0」は、「本人支払情報偽造と架空利用者支払情報偽造は成功しないものの、他人支払情報偽造は条件付きで成功する」という状況を意味する。

方式	攻撃者が利用する情報	各型における偽造の成否				
		型1	型2	型3	型4	型5
M1方式	なし	0-0-0				
	K	2-2-2		2-2-0	0-1-0	
M2方式	なし	0-0-0				
	K	2-2-0			0-1-0	
	SK_I	0-0-0				
	K, SK_I	2-2-2		2-2-0	0-1-0	
M3方式	なし	0-0-0				
	SK_U	2-0-0			0-0-0	
	SK_U, $SK_{U'}$	2-2-0			0-1-0	
	SK_U, $SK_{U'}$, SK_I	2-2-2		2-2-0	0-1-0	

図表 12：支払情報の偽造の成否

方式間の比較を試みると、攻撃者が利用する情報に関して同一の条件となっているのは、M1 方式と M2 方式において「攻撃者が秘密鍵 K を利用するケース」のみとなっている。本ケースについてみると、型 1, 2 に関しては、M2 方式において架空利用者支払情報偽造が成功しない（2-2-0）のに対し、M1 方式においては成功する（2-2-2）という結果となっていることがわかる。また、型 3～5 に関しては、M1 方式と M2 方式の両方とも偽造の成否のレベルは同一となっていることがわかる。このように、上記のケースに関しては、M2 方式は M1 方式に比べて相対的に安全性が高いといえる。

16 詳細な分析内容は補論に記述し、ここでは分析結果を説明することとする。

次に、攻撃者が利用する情報の種類が最も多い場合[17]において型同士を比較する。この場合、いずれの方式であっても各偽造の成否のレベルは同一となる。

まず型 1, 2 においては、オフライン型であり加盟店のデバイスで支払情報を処理するため、支払情報の偽造を検知できず不正な取引が成立してしまう。

型 3 においては、オンライン型であるが価値情報を利用者のデバイスで管理しており、攻撃者本人あるいは他の実在する利用者の支払情報が偽造された場合には、発行者のサーバは当該利用者の価値情報が取引金額に対して不足しているか否かを検査することができず、支払情報の偽造を検知できない。ただし、実在しない利用者の支払情報が偽造された場合、当該利用者が正規の利用者か否かを検査することで攻撃を検知できるため、不正な取引の成立を阻止することができる。

型 4, 5 においては、オンライン型であり、かつ、価値情報を発行者のサーバで管理しているため、利用者本人や実在しない利用者の支払情報が偽造された場合、サーバがその本人の価値情報が取引金額に対して不足しているか否かを確認することで偽造を検知することができる。ただし、他の実在する利用者の支払情報が偽造された場合、当該利用者の価値情報が取引金額に対して不足しているか否かを検査としても、足りている場合には偽造を検知できない。

このように、攻撃者が利用する情報の種類が最も多い場合において型の比較を行うと、オンライン型で価値情報を発行者のサーバで管理する型 4，5 が、その他の型に比べて相対的に安全性が高いといえる。

[17] 具体的には、M1 方式では暗号鍵 K、M2 方式では暗号鍵 K と秘密鍵 SK_I、M3 方式では秘密鍵 SK_U と秘密鍵 $SK_{U'}$ と秘密鍵 SK_I がそれぞれ利用可能な場合である。

4. 電子マネー・システムにおけるリスク管理

(1) リスク管理の重要性

3 節において検討した支払情報の偽造による攻撃が仮に成功したとすれば、不正に荷担していない利用者、加盟店、発行者が金銭的な損害を直接被る可能性があるほか、電子マネー・サービス自体の信頼性がレピュテーションの低下によって損なわれる可能性もある。電子マネー・システムの安全性を確保していくためには、同システムのリスク管理を適切に行い、想定されるリスクを許容できるレベル以下に抑えることが必要である。

一般に、想定されるリスクは、被害発生時の損失と当該被害の発生頻度の積で見積もられる。したがって、被害発生時の損失を抑える、あるいは、被害の発生頻度を抑えることによってリスクを制御するという方法が考えられる。こうした方法を発行者が検討するにあたっては、利用者の利便性や費用等も考慮しつつ、リスク分析を適切に行う必要がある。

発生時の損失や発生頻度を抑制するための主な対策を順に検討する。

(2) 被害発生時の損失の軽減のための対策

被害発生時の損失を軽減する方法として、1 回の攻撃で被る損失を低くするという方法が考えられる。具体的には、1 回あるいは 1 日あたりの取引限度額を低く設定する方法や、プリペイド方式の電子マネー・システムであれば 1 回あるいは 1 日あたりのチャージ金額や価値情報の上限を低くする方法が考えられる。現行のプリペイド方式およびポストペイ方式の電子マネー・システムでは、どの程度の金額が設定されているのかを参考までに紹介する（図表 13 参照[18]）。

---

[18] 図表 13 の情報は各運営団体のウェブサイト等から入手した。特に、「1 回の取引における利用可能限度額」については以下の情報を参考にした。

- Suica では、「２枚以上の Suica を使用してのお支払いはできません」との記述がある（http://www.jreast.co.jp/suica/faq/faq05.html#10）。
- PASMO では、「1 回の電子マネー取引につき 2 枚以上の PASMO を同時に使用することはできない」との記述がある（http://www.pasmo.co.jp/stipulation/e_money.html）。
- Edy では、「(am/pm では) 1 回のお取引に最大 5 枚までご使用になれます」との記述がある（http://www.ampm.jp/service/edy/）。
- nanaco では、「セブン-イレブンでは、1 回の精算で最大 5 つの nanaco（カード・モバイル）をご利用いただけます」との記述がある（http://www.nanaco-net.jp/faq/faq_shopping.html）。
- WAON では、「複数枚の WAON カードでのお支払いはできません」との記述がある（http://www.waon.com/guide/index.html）。
- Octopus では、「If the remaining value on an Octopus is positive (e.g. HK$0.1 or above) but insufficient to cover the payment of a particular transaction, then the Octopus can still be used

	Suica	PASMO	Edy	nanaco	WAON	Octopus
1回の取引における利用可能限度額	20,000円	20,000円	250,000円 (5枚併用時)	149,995円 (5枚併用時)	50,000円	1,035 HKD = 約14,914円
カード1枚あたりの価値情報の上限	20,000円	20,000円	50,000円	29,999円	50,000円	1,000 HKD = 14,410円
電子マネー発行元	東日本旅客鉄道	パスモ	ビットワレット	アイワイ・カード・サービス	イオン、イオン銀行	Octopus Cards Limited

(1) プリペイド方式の電子マネー・システムにおける金額設定

	QUICPay	iD	Smartplus	OneTouch (Barclaycard)
1回の取引における利用可能限度額	20,000円	クレジットカード会社等により異なる	30,000円	10 GBP = 約2,192円
1アカウントあたりの価値情報の上限	クレジットカードの上限金額	クレジットカードの上限金額	クレジットカードの上限金額	クレジットカードの上限金額
発行元	JCB等	DCMX等	三菱UFJニコス	Barclaycard

(備考) QUICPay、iD、Smartplus については本人確認を行わずに購入できる金額を示した。本人確認を行う場合にはより高額な取引が可能となっている。

(2) ポストペイ方式の電子マネー・システムにおける金額設定

図表 13：各電子マネー・システムにおける金額設定

(3) 発生頻度の低下のための対策

イ．対策の方針とそのバリエーション

発生頻度を低下させるという方法は、電子マネー・システムで利用しているデバイスや暗号アルゴリズムを危殆化させないという方針（方針 1）と、仮に危殆化してしまったとしても、システムを破綻させないためにデバイスや暗号アルゴリズムに頼らずに発生頻度を抑えるという方針（方針 2）に分けられる。

---

provided the resulting negative value does not exceed HK$35.」との記述がある（http://www.octopuscards.com/consumer/help/faq/en/index.jsp）。

- QUICPay では、「一回のお買い物にご利用いただける上限額は 2 万円です」との記述がある（http://www.quicpay.jp/faq/index.html#q4）。
- OneTouch では、「OneTouch payment is a new cashless way to pay for low value purchases of £10 and under more quickly and conveniently.」との記述がある（http://www.barclaycard-onepulse.co.uk/onePulseFaq.html?set=set6）。
- iD については DoCoMo インフォメーションセンターと三井住友カードから、Smartplus については三菱 UFJ ニコスから得た情報による。

また、Octopus と OneTouch に関しては、それぞれ 1 HKD = 14.41 JPY、1 GBP = 219.26 JPY（2008 年 1 月 9 日、三菱東京 UFJ 銀行の対顧客電信売相場）として換算した。

（イ）方針 1：デバイスや暗号アルゴリズムの危殆化防止に向けた対応

方針 1 における対策としては、デバイスや暗号アルゴリズムの安全性を定期的に評価し、危殆化の兆候が現れた際には、より高度な技術にスムーズに移行する仕掛けをシステムに取り入れておくという方法が考えられる。

例えば、クレジットカード取引における IC カードと端末のやり取りを規定している業界標準である EMV 仕様（EMVCo［2004］）では、公開鍵暗号系として利用している RSA の鍵長の見直しを毎年行っている[19]。また、EMV 仕様では、インデックス番号によって暗号アルゴリズムを指定する方法を採用しており、新たな暗号アルゴリズムには未使用の番号を割り当てることで、新しい暗号アルゴリズムの追加を容易にしている。このほか、カードに有効期限を設けて定期的にカードを更新し、鍵の更新、新しい暗号アルゴリズムへの移行、より安全性の高いデバイスへの移行を可能としている。

（ロ）方針 2：デバイスや暗号アルゴリズム以外の手段による対応

方針 2 における対策をその目的に基づいて細分化すると次の 3 つに分けられる。すなわち、①偽造された支払情報による不正な取引の成立を阻止すること（以下、「不正取引の阻止」と呼ぶ）、②仮に不正な取引が成立してしまった場合に、それを検知すること（以下、「攻撃の検知」と呼ぶ）、③不正取引を検知できた場合に、同様の攻撃の繰り返しによる被害の拡大を防ぐこと（以下、「被害拡大の防止」と呼ぶ）である。

以下では、3 種類の攻撃（本人支払情報偽造、他人支払情報偽造、架空利用者支払情報偽造）を前提としたときに、上記の対策目的（不正取引の阻止、攻撃の検知、被害拡大の防止）の達成に資するとみられる主な対策を取り上げ、それらの有効性や限界について検討する[20]。

---

[19] EMVCo では発行者の RSA の鍵長を毎年見直しており、下記の URL に掲載されている。
http://www.emvco.com/bulletins.asp?show=14

[20] 被害拡大の防止のための対策としては、攻撃者を追跡しやすくすることで攻撃を行う際の抑止力を高める方法が考えられる。例えば、物理的に存在する店舗であれば監視カメラによって利用者を撮影する、あるいは、ネットワーク上の店舗であれば IP アドレスの記録等を行っておき、何らかの証拠を基に攻撃の事実が明らかになった際に、攻撃者を特定できるようにしておくといった方法が挙げられる。こうした方法は、いずれの型においても有効な対策となりうる。

		想定する攻撃		
		本人支払 情報偽造	他人支払 情報偽造	架空利用者 支払情報偽造
対策目的	不正取引の 阻止	検討する型： 型 1～3	検討する型： 型 1～5	検討する型： 型 1 と型 2
	攻撃の 検知	検討する型： 型 1～3	検討する対象： 型 1～5	検討する対象： 型 1 と型 2
	被害拡大の 防止	検討する型： 型 1～3	検討対象： 型 1～5	検討対象： 型 1 と型 2

図表 14：攻撃・対策目的の組合せと本節で詳細に検討する型

図表 14 のとおり、攻撃と対策目的の組合せは 9 通りとなるが、型 1～5 のすべてにおいて 9 通りの組合せを適用して検討するわけではない。オンライン型であり、かつ、発行者が利用者の価値情報を管理するタイプの型 4, 5 については、その検証のタイミングで本人支払情報偽造と架空利用者支払偽造を検知し不正取引を阻止可能である。そのため、型 4, 5 に関しては、本人支払情報偽造と架空利用者支払情報偽造に関する検討を以下で改めて行わず、他人支払情報偽造のみを扱うこととする。

また、オンライン型であるものの、発行者が利用者の価値情報自体の管理を行っていないタイプである型 3 に関しては、利用者が事前に登録されているか否かの検証によって架空利用者支払情報偽造を検知することができるものの、その他の攻撃については検知困難と考えられる。そのため、型 3 については、架空利用者支払情報偽造以外の攻撃に関する検討を以下で行うこととする。

ロ．購入パターンを利用した検査

不正取引の阻止や攻撃の検知を目的とする対策の 1 つとして、支払情報を購入パターンの観点から検査して不正な取引か否かを検知するという方法が考えられる。例えば、支払情報が当該利用者の過去の購入パターンから逸脱しているか否か、不正な購入パターン（換金率のよい商品を短期間に買い回る等）に類似しているか否か等を検査する。これらの検査の効果は電子マネー・システムが【ロ-1】オンライン型か【ロ-2】オフライン型かによって異なる。

【ロ-1】オンライン型の場合（型 3～5 が対象）

オンライン型の電子マネー・システム（型 3～5）を想定した場合、発行者のサーバが受信した支払情報を検査することで、不正な取引の成立を阻止するという方法が考えられる。本検査は、取引の際に即時に行われることから「購入パターン即時検査」と呼ぶ。本検査は、オンライン型の電子マネー・システ

ムに対する本人支払情報偽造（型 3 が対象）と他人支払情報偽造（型 3～5 が対象）への対策となりうる。

ただし、支払情報の偽造による取引が通常の購入パターンからどの程度逸脱していれば不正な取引と判断するかを見極めることが容易でないという課題がある。

【ロ-2】オフライン型の場合（型 1, 2 が対象）

オフライン型の電子マネー・システム（型 1, 2）を想定した場合、個々の加盟店のデバイスにおいて各利用者の購入パターンのデータベースを管理することは現実的とはいえず、加盟店のデバイスが受理した支払情報を発行者のサーバにおいて検査するという方法が考えられる。この検査では、不正取引の阻止を目的とするのではなく、事後的な攻撃の検知が目的となる。この検査は取引後に行われることから、「購入パターン事後検査」と呼ぶ。購入パターン事後検査は、オフライン型の電子マネー・システムに対する本人支払情報偽造と他人支払情報偽造への対策となりうる。

ただし、購入パターン即時検査と同様の課題が存在するほか、加盟店のデバイスから送信された支払情報を発行者のサーバが受信していることが前提となるため、発行者のサーバが偽造された支払情報を受信するまでの間は不正取引を検知できないという限界がある。

ハ. 価値情報を利用した検査

次に、利用者の価値情報を用いて不正な取引か否かを検査するという方法が考えられる。ただし、ここでの議論の前提となっている「デバイスや暗号アルゴリズムが危殆化している」という状況のもとでは、利用者のデバイスで管理されている価値情報を信頼することが困難であり、本検査に利用することができないと考えられる。したがって、本検査に利用できる価値情報は発行者によって管理されているものに限定されることとなる。そこで、以下では、【ハ-1】発行者のサーバで管理されている価値情報だけを用いる場合と、【ハ-2】発行者のサーバと利用者のデバイスの両者で管理されている価値情報を用いる場合に分けて検討する。

【ハ-1】発行者のサーバで管理されている価値情報だけを用いる場合

この場合は、発行者のサーバにおいて価値情報が管理されている型 2, 4, 5 が対象となる。具体的な対策の方法は、発行者のサーバへのセンター接続の

形態によって異なる。

【ハ-1-1】オンライン型の場合（型 4, 5 が対象）

発行者のサーバは、取引の際に即時に当該利用者の価値情報を検査するという方法によって不正取引の阻止が可能である。

また、価値情報を発行者のサーバのみで管理している電子マネー・システム（型 5）においては、利用者側[21]が発行者に価値情報を問い合わせ、予期せぬ価値情報になっていた場合、その旨を発行者に通報するという方法（以下、「利用者側による価値情報の照会」と呼ぶ）も考えられる。これは、攻撃の検知を目的とするものであり、他人支払情報偽造への対策となりうる。ただし、利用者の主張を裏付ける情報が必要になる等の問題がある。

【ハ-1-2】オフライン型の場合（型 2 が対象）

発行者のサーバにおいて、利用者の価値情報が取引金額に対して不足しているか否かを検査するという方法（以下、「価値情報の不足検査」と呼ぶ）が考えられる。本検査の実施は、加盟店のデバイスが支払情報を受理し取引が成立した後となる。本検査によって、不正取引の阻止は困難であるものの、攻撃の検知は可能である。本検査は本人支払情報偽造と他人支払情報偽造への対策となりうる。

ただし、利用者のチャージ情報が発行者のサーバに送信される前に、発行者のサーバが当該利用者の支払情報を受信した場合には、価値情報が不足しているか否かを判断することが困難であるという問題がある[22]。

【ハ-2】両者で管理されている価値情報を用いた場合（型 2, 4 が対象）

価値情報が併用管理の電子マネー･システム（型 2, 4）においては、双方で管理されている価値情報を突き合わせて検査するという方法（以下、「価値情報の突合検査」と呼ぶ）が考えられる。具体的には、利用者の価値情報を支払情報に含め、発行者のサーバに送信して双方の価値情報を突き合わせるという方法と、利用者側が発行者のサーバに対して価値情報の照会を要求し、

[21] 利用者が直接問い合わせる場合やデバイスを利用する場合等がありうる。

[22] この問題を解決するために、発行者のサーバは各支払情報に対して価値情報が不足するか否かを検査するのではなく、チャージの情報が遅れて発行者に届くことを見越して、一定金額までの不足、つまりマイナスの価値情報を許容する運用方法が考えられる。ただし、この方法では、不正な取引が行われていたとしても、この一定金額を下回らない限り検知できない。

利用者側で価値情報を突き合わせるという方法が考えられる。これらの検査はいずれも攻撃の検知を目的とするものであり[23]、他人支払情報偽造への対策となりうる。

ただし、価値情報の突合検査には価値情報の不足検査と同様の問題がある。

ニ．ブラックリストを用いた検査

被害拡大の防止を目的とする場合、不正な取引に関わった利用者に電子マネー・システムを以後利用させないようにするという方法が考えられる。不正な利用者の識別情報（ID や公開鍵等）を登録したリスト（以下、ブラックリストと呼ぶ）を作成したうえで、取引の際に利用者の識別情報がブラックリストに登録されているか否かを検査し、登録されている場合には取引を中止するという方法（以下、「ブラックリスト方式」と呼ぶ）である。本方式の効果は、【ニ-1】オンライン型か【ニ-2】オフライン型かに依存する。

【ニ-1】オンライン型の場合（型 3〜5 が対象）

オンライン型の場合には、ブラックリストを発行者のサーバにおいて作成し、同サーバ上でブラックリストの検査を行うという方法が考えられる。これは、本人支払情報偽造（型 3）と他人支払情報偽造（型 3〜5）への対策となりうる。

ただし、他の実在する利用者の識別情報を容易に入手できる場合、攻撃者は、他人支払情報偽造を行う際に、偽造対象の利用者の識別情報を再利用せず毎回変えることが想定される。このケースでは、ブラックリスト方式によって被害拡大の防止を達成することはできない。ブラックリスト方式を有効に機能させるためには、攻撃者が他の実在する利用者の識別情報を容易に入手・推測できないようにする必要がある。

【ニ-2】オフライン型の場合（型 1, 2 が対象）

オフライン型の場合には、加盟店のデバイスにブラックリストを配布して同デバイス上でブラックリスト方式を実施するという方法が考えられる。これは、本人支払情報偽造と他人支払情報偽造への対策となりうる。

ただし、発行者のサーバにおけるブラックリスト方式と同様の問題が存在するほか、不正な利用者が検知されたとしても、加盟店のデバイスに格納されて

[23] 不正取引の発生は検知できるが、どの取引が不正取引かを特定するためにはさらに別の対策を講じる必要がある。

いるブラックリストが更新されるまでは攻撃の繰返しを阻止することが困難である。また、ブラックリストに登録された利用者が多い場合には、取引処理に時間がかかる、ブラックリストのサイズが加盟店のデバイスの記憶容量を超えてしまう可能性がある。

ホ．ホワイトリストを用いた検査

発行者のサーバが正規の利用者の識別情報を登録したリスト（以下、ホワイトリストと呼ぶ）を作成し、支払情報から抽出した利用者の識別情報がこのリストに登録されているか否かを確認するという方法（以下、「ホワイトリスト方式」と呼ぶ）が考えられる。発行者のサーバが管理する利用者の識別情報等のデータベースがホワイトリストに対応する。ホワイトリスト方式は、架空利用者支払情報偽造への対策となりうる。

オンライン型の電子マネー・システム（型 3～5）の場合、通常の取引処理においてホワイトリスト方式を実施しているといえる。オフライン型（型 1, 2）の場合、ホワイトリスト方式を実施するエンティティに依存して効果が異なると考えられることから、【ホ-1】加盟店のデバイスにおいて実施する場合と、【ホ-2】発行者のサーバにおいて実施する場合に分けて検討する。

【ホ-1】加盟店のデバイスで実施する場合（型 1, 2 が対象）

加盟店のデバイスにホワイトリストを格納し、取引の際に即時にホワイトリスト方式を実施することで、架空利用者支払情報偽造による不正取引の阻止を目的とする対策となりうる。

ただし、取引処理の時間が長くなる、あるいは、加盟店のデバイスの記憶容量の制約からホワイトリストをデバイスに格納できないといった問題が考えられる。また、加盟店のデバイスが危殆化している状況を想定した場合には、ホワイトリストが改ざんされてしまっているという問題も考えられる。

【ホ-2】発行者のサーバで実施する場合（型 1, 2 が対象）

発行者のデバイスにおいてホワイトリストによる確認を行う場合、その確認は取引が成立した後で実行されることとなる。そのため、発行者のデバイスによるホワイトリスト方式は、架空利用者支払情報偽造の検知を目的とする対策になりうる。

へ．本人確認（型 1～5 が対象）

電子マネー・システムにおける利用者の利便性を重視する場合、本人確認をあえて行わないことも想定される。しかし、本人確認を導入することによってなりすましを困難にし、不正取引を阻止する効果が期待できる。本人確認の形態としては次のようなものが考えられる。

① 利用者のデバイスを発行する際に本人確認を行い、その後は、利用者本人が当該デバイスを適切に管理する。
② 取引可能な状態と取引不可能な状態に切替え可能な利用者のデバイスを用意する。取引可能な状態に切り替える際に本人確認を行う。取引時には、当該デバイスが取引可能な状態か否かを検査する。
③ 一定の条件に基づいて本人確認を行うか否かを個々の取引で判断する。一定の条件としては、取引金額が一定額を超えているか否か、本人確認を行わない取引が連続して何回続いているか等が考えられる。
④ 取引前に、パスワード等の本人であることを示す情報（以下、本人確認情報と呼ぶ）を利用者のデバイスに入力し、その状態を維持しておく。取引時には、本人確認情報を入力するのではなく、当該デバイスに本人確認情報が設定されているか否かを検査する。
⑤ 取引金額等の条件に関係なく、取引毎に本人確認情報を入力し本人確認を行う。

これらは、攻撃対象が利用者本人以外、つまり、他人支払情報偽造と架空利用者支払情報偽造への対策となりうる。もっとも、型 3～5 については、発行者のサーバにおける利用者の識別情報の検査によって架空利用者支払情報偽造を検知可能であり、本人確認を別途実施する必要はない。

ただし、取引時に利用者が本人確認情報を追加的に提示することが必要となるほか、取引にかかる時間が増加すると想定され、利用者の利便性が損なわれる可能性がある。また、本人確認を実現する方式の中には、デバイスや暗号アルゴリズムの安全性を前提とするものが多く、それらが危殆化する可能性を考慮した場合、本人確認を実現する方式自体が有効でなくなる可能性がある。

ト．検討のまとめ

以上の検討結果を整理すると図表 15 のとおりである。本節において検討した対策には課題や限界が存在するものが多く、デバイスや暗号アルゴリズムの危殆化を想定して別途対策の採用を検討する際には、これらの点を十分に考慮する必要がある。

		想定する攻撃		
		本人支払 情報偽造	他人支払 情報偽造	架空利用者支払 情報偽造
対策目的	（型 1）不正取引の阻止	（加盟店のデバイスによる阻止は困難）	・本人確認	・本人確認 ・加盟店のデバイスにおける WL 方式
	（型 1）攻撃の検知	・購入パターン事後検査		・発行者のサーバにおける WL 方式
	（型 1）被害拡大の防止	・加盟店のデバイスにおける BL 方式		（本人確認と WL 方式が機能しない場合、対策の実施は困難）
	（型 2）不正取引の阻止	（加盟店のデバイスによる阻止は困難）	・本人確認	・本人確認 ・加盟店のデバイスにおける WL 方式
	（型 2）攻撃の検知	・購入パターン事後検査 ・価値情報の不足検査	・購入パターン事後検査 ・価値情報の不足検査 ・価値情報の突合検査	・発行者のサーバにおける WL 方式
	（型 2）被害拡大の防止	・加盟店のデバイスにおける BL 方式		（本人確認と WL 方式が機能しない場合、対策の実施は困難）
	（型 3）不正取引の阻止	・購入パターン即時検査	・本人確認 ・購入パターン即時検査	
	（型 3）攻撃の検知	（購入パターン即時検査や本人確認が機能しない場合、偽造の検知は困難）		
	（型 3）被害拡大の防止	・発行者のサーバにおける BL 方式		
	（型 4）不正取引の阻止		・本人確認 ・購入パターン即時検査	
	（型 4）攻撃の検知		・価値情報の突合検査	
	（型 4）被害拡大の防止		・発行者のサーバにおける BL 方式	
	（型 5）不正取引の阻止		・本人確認 ・購入パターン即時検査	
	（型 5）攻撃の検知		・利用者側による価値情報の照会	
	（型 5）被害拡大の防止		・発行者のサーバにおける BL 方式	

（備考）図表中の WL と BL はそれぞれホワイトリスト、ブラックリストを意味する。

図表 15：各型において想定される対策の例

型ごとに各対策をみると、まずオフライン型の電子マネー・システム（型 1, 2）に関しては、デバイスや暗号アルゴリズムが危殆化している状況のもとでは、正規の利用者となっている攻撃者が自分の支払情報を偽造する場合（本人支払情報偽造）、加盟店のデバイスにおいて不正取引を阻止することは困難である。そうしたなかで攻撃の検知や被害拡大の防止を行うためには、何らかの方法で発行者のサーバの支援を仰ぐ必要があり、加盟店の端末と発行者のサーバとの

間でホワイトリストやブラックリストの配信や支払情報に基づく購入パターンの検査等を機動的に実施することが求められる。また、架空利用者支払情報偽造については、本人確認やホワイトリスト方式が有効に機能しない場合には、被害拡大の防止のための有効な対策を講じることは困難とみられる。

オンライン型であり利用者のデバイスのみで価値情報を管理する電子マネー・システム（型 3）に関しては、発行者のサーバにおける取引時の支払情報の検査によって架空利用者支払情報偽造を阻止することができる。ただし、その他の支払情報の偽造を阻止するためには、本人確認や購入パターンの検査といった対策を利用することが必要となる。

オンライン型であり発行者のサーバで価値情報を管理する電子マネー・システム（型 4, 5）に関しては、発行者のサーバで管理される価値情報を利用することによって、本人支払情報偽造や架空利用者支払情報偽造を阻止することができる。他人支払情報偽造に対しては、型 3 と同様に、本人確認、購入パターンの検査、ブラックリストの検査といった追加的な対策の採用が求められる。

このように、デバイスや暗号アルゴリズムの安全性に頼らないという方針を採用する場合、型 4, 5 のようにオンライン型で発行者のサーバにおいて価値情報を管理するタイプのシステムが、相対的に運用面からの対策を実施しやすいといえる。ただし、こうしたタイプのシステムには、オフライン型のシステムに比べて、通常の取引において加盟店と発行者間でデータ交信を実施する等の負担が増すという問題がある。通常の取引におけるコストや利便性も踏まえつつ、どのような対策を選択することが望ましいかに関しては、リスク分析の結果を踏まえつつ、電子マネー・システム全体のリスク管理の文脈の中で十分に検討することが必要である。

5. まとめ

近年、電子マネー・サービスが小額決済の分野において拡大しつつあるなかで、電子マネーを不正に使用する事件等が散見されている。安心して利用することができる電子マネー・サービスを実現していくうえで、技術面と運用面の双方から十分な対策を実施し、不正取引等によるリスクを適切に管理することが一層重要となっている。

本論文では、こうした問題意識を背景に、電子マネー・サービスの利用者が加盟店に提示する支払いに関する情報を偽造するというタイプの攻撃に焦点を当てて、電子マネー・システムに用いられるデバイスや暗号アルゴリズムの危殆化が同システムの安全性にどのような影響を与えるかについて検討した。約10 年前に発表された先行研究である中山・太田・松本［1999］においては、安全でない（危殆化した）デバイスと安全な暗号アルゴリズムを前提として分析を行っているが、本論文では、これらが安全であるケースと危殆化したケースの両方を考慮して分析した。また、本論文では、デバイスや暗号アルゴリズムの危殆化のもとで想定されるリスクを軽減する運用上の対策についても分析し、その効果と課題について整理した。

本論文における分析の結果、デバイスや暗号アルゴリズムが危殆化した場合、個々の利用者のデバイス内部で電子マネーの情報を管理するタイプ、あるいは、オフラインで取引を行うタイプの電子マネー・システムにおいては、電子マネーによる支払いに関する情報を偽造して不正な取引を行うという攻撃を検知し防止することが困難であることがわかった。また、デバイス等の危殆化に対応するための運用面からの対策に関しては、取引時における利用者の本人確認や商品・サービスの購入パターンの検査といったさまざまな対策が想定され、一定の効果が見込まれるものの、実際に導入するうえでクリアすべき課題が少なくないことがわかった。

今後、電子マネー・システムが一層普及していく状況を想定した場合、デバイスや暗号アルゴリズムを含め、同システムに採用される情報セキュリティ対策技術が期待通りの効果を発揮しているか否かを常に確認していくとともに、適切なリスク管理のもとで、デバイス等の危殆化を想定した運用面からの対策の必要性についても検討することが求められる。今後、安全な電子マネー・システムが普及し、使い勝手のよい小額決済手段として広く活用されるようになることが望まれる。

【参考文献】

鈴木雅貴・神田雅透、「IC カードに利用される暗号アルゴリズムの安全性について：EMV 仕様の実装上の問題点を中心に」、『金融研究』第 26 巻別冊第 1 号、日本銀行金融研究所、2007 年

総務省・経済産業省、『電子政府推奨暗号リスト』、総務省・経済産業省、2003 年（http://www.cryptrec.jp/images/cryptrec_01.pdf）

田村裕子・宇根正志、「情報セキュリティ製品・システムの第三者評価・認証制度について―金融分野において活用していくために―」、*IMES Discussion Paper Series*、no.2008-J-4、日本銀行金融研究所、2008 年

独立行政法人情報処理推進機構セキュリティセンター（IPA）、『暗号モジュール試験及び認証制度』、IPA、2007 年（http://www.ipa.go.jp/security/jcmvp/）

中山靖司・太田和夫・松本 勉、「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」、『金融研究』第 18 巻第 2 号、日本銀行金融研究所、1999 年、57～114 頁

松本勉・岩下直行、「情報セキュリティ技術の信頼性を確保するために」、『金融研究』第 20 巻第 2 号、日本銀行金融研究所、2001 年、21～32 頁

宮崎真悟・櫻井幸一、「オフライン型電子現金システムの分類と安全性評価」、『信学技報』、ISEC98-45、電子情報通信学会、1998 年

矢野経済研究所、『プリペイド式電子マネー市場に関する調査結果』、リサーチエクスプレス、2007 年 12 月 10 日（http://www.yano.co.jp/press/pdf/314.pdf）

Chida, E., M. Manbo and H. Shizuya, “Digital Money – A Survey,” *Interdisciplinary Information Sciences*, vol.7, no.2, Tohoku University, pp.135-165, 2001.

EMVCo, *EMV Integrated Circuit Card Specification for Payment Systems (EMV 4.1): Book 2 – Security and Key Management*, EMVCo, 2004.

————, *EMV Security Guidelines: EMVCo Security Evaluation Process*, v1.0, EMVCo, 2006.

Kocher, P. “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems,” *Proc. of CRYPTO'96*, Springer-Verlag, 1996, pp.104-113.

————, Joshua J. and Benjamin J., “Differential Power Analysis,” *Proc. of CRYPTO'99*, Springer-Verlag, pp.388-397, 1999.

National Institute of Standards and Technology (NIST), *Recommendation on Key Management, SP800-57*, NIST, 2005. (http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf)

New European Schemes for Signatures, Integrity, and Encryption (NESSIE) consortium, *Portfolio of recommended cryptographic primitives*, NESSIE, 2003. (https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf)

Une, M. and M. Kanda, “Year 2010 Issues on Cryptographic Algorithms,” *Monetary and Economic Studies*, vol.25, no.1, Institute for Monetary and Economic Studies, Bank of Japan, pp. 129-164, 2007.

補論　支払情報の偽造に関する分析

支払情報の偽造による攻撃の成否について、攻撃者が入手する情報に応じて分析を行う。以下では、本人支払情報偽造、他人支払情報偽造、架空利用者支払情報偽造における攻撃の成否に関する分析結果をそれぞれ記述する。

(1)　型 1～5 の M1 方式に関する分析

型 1～5 の M1 方式に対する本人支払情報偽造、他人支払情報偽造、架空利用者支払情報偽造では、攻撃者は、それぞれ支払情報 $E_K(ID_U, DT)$、$E_K(ID_{U'}, DT)$、$E_K(ID_{U*}, DT)$を偽造し、不正な取引の成立を試みる。M1 方式では、①攻撃者が暗号鍵 K を利用する場合と②暗号鍵 K を利用しない場合があり、それぞれの場合について分析すると、以下のとおりである。

①暗号鍵 K を利用する場合

<table>
<tr><th></th><th>型1</th><th>型2</th><th>型3</th><th>型4</th><th>型5</th></tr>
<tr><td>本人支払情報偽造</td><td colspan="3">暗号鍵Kを用いて偽造した支払情報を加盟店のデバイスに受理させ、不正な取引を成立させることができる。</td><td colspan="2">支払情報の偽造自体は可能であるが、オンライン型であるため、発行者のサーバは、利用者Uの価値情報が取引金額に対して不足していることを確認することで、不正な取引を阻止することができる。なお、価値情報が足りている場合には、利用者Uの価値情報から支払うことになるため、不正な取引にはあたらない。</td></tr>
<tr><td>他人支払情報偽造</td><td colspan="3">暗号鍵Kと盗聴等により入手した$ID_{U'}$を用いて偽造した支払情報を、加盟店のデバイスに受理させ、不正な取引を成立させることができる。</td><td colspan="2">支払情報の偽造自体は可能であるが、発行者のサーバが価値情報を管理するオンライン型であるため、当該利用者$ID_{U'}$の価値情報が取引金額に対して足りている場合のみ不正な取引が成立する。逆に、不足している場合には不正な取引を阻止することができる。</td></tr>
<tr><td>架空利用者支払情報偽造</td><td colspan="2">実在しないID_{U*}と暗号鍵Kを用いて偽造した支払情報を、加盟店のデバイスに受理させ、不正な取引を成立させることができる。</td><td colspan="3">支払情報の偽造自体は可能であるが、オンライン型のため、発行者のサーバは、支払情報の利用者ID_{U*}が正規利用者のデータベースDB(ID)に登録されていないことを確認することで、不正な取引を阻止できる。</td></tr>
</table>

②暗号鍵 K を利用しない場合

<table>
<tr><th></th><th>型1</th><th>型2</th><th>型3</th><th>型4</th><th>型5</th></tr>
<tr><td>本人支払情報偽造</td><td colspan="5" rowspan="3">暗号鍵Kを利用できないため、支払情報を偽造することができない。</td></tr>
<tr><td>他人支払情報偽造</td></tr>
<tr><td>架空利用者支払情報偽造</td></tr>
</table>

(2)　型 1～5 の M2 方式に関する分析

型 1～5 の M2 方式に対する本人支払情報偽造、他人支払情報偽造、架空利用者支払情報偽造では、攻撃者は、それぞれ支払情報 $E_K(S_I(ID_U), DT)$、$E_K(S_I(ID_{U'}), DT)$、$E_K(S_I(ID_{U*}), DT)$を偽造し、不正な取引の成立を試みる。M2 方式では、①攻撃者が暗号鍵 K を利用する場合、②発行者の秘密鍵 SK_I を利用する場合、③K と SK_I を利用する場合、④これらの情報を利用しない場合の 4 通りが想定され、それぞれの場合について分析すると以下のとおりである。

①暗号鍵 K を利用する場合

	型1	型2	型3	型4	型5
本人支払情報偽造	暗号鍵Kを用いて偽造した支払情報を加盟店のデバイスに受理させ、不正な取引を成立させることができる。			支払情報の偽造自体は可能であるが、オンライン型のため、発行者のサーバは、利用者Uの価値情報が取引金額に対して不足していることを確認することで、不正な取引を阻止することができる。なお、価値情報が足りている場合には、利用者Uの価値情報から支払うことになるため、不正な取引にはあたらない。	
他人支払情報偽造	盗聴等により入手した$S_I(ID_{U'})$と暗号鍵Kを用いて偽造した支払情報を、加盟店のデバイスに受理させ、不正な取引を成立させることができる。			支払情報の偽造自体は可能であるが、オンライン型であり、かつ、発行者のサーバが価値情報を管理するため、当該利用者$ID_{U'}$の価値情報が取引金額に対して足りている場合のみ不正な取引が成立する。逆に、不足している場合には不正な取引を阻止することができる。	
架空利用者支払情報偽造	秘密鍵SK_Iを利用できないため$S_I(ID_{U*})$を偽造できず、支払情報を偽造できない。				

②秘密鍵 SK_I が利用する場合

	型1	型2	型3	型4	型5
本人支払情報偽造	盗聴やSK_Iを用いた署名の偽造等により$S_I(ID_U)$、$S_I(ID_{U'})$、$S_I(ID_{U*})$を入手あるいは生成できるが、暗号鍵Kを利用できないため、支払情報を偽造できない。				
他人支払情報偽造					
架空利用者支払情報偽造					

③暗号鍵 K と秘密鍵 SK_I が利用する場合

	型1	型2	型3	型4	型5
本人支払情報偽造	暗号鍵Kを利用できる場合の型1～3のM2方式の結果と同じ結果となる。			暗号鍵Kを利用できる場合の型4, 5のM2方式の結果と同じ結果となる。	
他人支払情報偽造					
架空利用者支払情報偽造	秘密鍵SK_Iを用いて存在しないID_{U*}に対する発行者の署名$S_I(ID_{U*})$を偽造できるため、$S_I(ID_{U*})$と暗号鍵Kを用いて支払情報が偽造可能であり、この支払情報を加盟店のデバイスに受理させ、不正な取引を成立させることができる。			支払情報の偽造自体は可能であるが、オンライン型であるため、発行者のサーバは、支払情報の利用者ID_{U*}が正規利用者のデータベースDB(ID)に登録されていないことを確認することで、不正な取引を阻止できる。	

④暗号鍵や秘密鍵を利用しない場合

	型1	型2	型3	型4	型5
本人支払情報偽造	暗号鍵Kと秘密鍵SK_Iを利用できないため、支払情報を偽造することができない。				
他人支払情報偽造					
架空利用者支払情報偽造					

(3)　型 1～5 の M3 方式に関する分析

型 1～5 の M3 方式に対する本人支払情報偽造、他人支払情報偽造、架空利用者支払情報偽造では、攻撃者は、支払情報と公開鍵証明書のペア $S_U(DT)$, $S_I(PK_U)$、$S_{U'}(DT)$, $S_I(PK_{U'})$、$S_{U*}(DT)$, $S_I(PK_{U*})$をそれぞれ偽造し、不正な取引の成立を試みる。M3 方式では、①攻撃者が攻撃者本人の秘密鍵 SK_U を利用する場合、②SK_U と他の実在する利用者の秘密鍵 $SK_{U'}$を利用する場合、③SK_U と $SK_{U'}$と発行者の秘密鍵 SK_I を利用する場合、④これらの情報を利用しない場合の 4 通りが想定され、それぞれの場合について分析すると以下のとおりである。

①秘密鍵 SK_U を利用する場合

	型1	型2	型3	型4	型5
本人支払情報偽造	秘密鍵SK_Uを用いて偽造した支払情報を加盟店のデバイスに受理させ、不正な取引を成立させることができる。			支払情報の偽造自体は可能であるが、オンライン型であるため、発行者のサーバは、利用者Uの価値情報が取引金額に対して不足していることを確認することで、不正な取引を阻止することができる。なお、価値情報が足りている場合には、利用者Uの価値情報から支払うことになるため、不正な取引にはあたらない。	
他人支払情報偽造	秘密鍵$SK_{U'}$を利用できないため、支払情報を偽造できない。				
架空利用者支払情報偽造	支払情報$S_{U*}(DT)$を偽造できるものの、秘密鍵SK_Iを利用できないため、公開鍵証明書$S_I(PK_{U*})$を偽造できず、不正な取引を行うことができない。				

②秘密鍵 SK_U と $SK_{U'}$を利用する場合

	型1	型2	型3	型4	型5
本人支払情報偽造	秘密鍵SK_Uを利用できる場合の型1～3のM3方式の結果と同じ結果となる。			秘密鍵SK_Uを利用できる場合の型4, 5のM3方式の結果と同じ結果となる。	
他人支払情報偽造	秘密鍵$SK_{U'}$と盗聴等により入手した$S_I(PK_{U'})$を用いて偽造した支払情報を、加盟店のデバイスに受理させ、不正な取引を成立させることができる。			支払情報の偽造自体は可能であるが、オンライン型であり、かつ、発行者のサーバが価値情報を管理するあるため、当該利用者$ID_{U'}$の価値情報が取引金額に対して足りている場合のみ不正な取引が成立する。逆に、不足している場合には不正な取引を阻止することができる。	
架空利用者支払情報偽造	秘密鍵SK_Iを利用できない場合の型1～5のM3方式の結果と同じ結果となる。				

③秘密鍵 SK_U と $SK_{U'}$と SK_I を利用する場合

	型1	型2	型3	型4	型5
本人支払情報偽造	秘密鍵SK_Uと秘密鍵$SK_{U'}$を利用できる場合の型1～3のM3方式の結果と同じ結果となる。			秘密鍵SK_Uと秘密鍵$SK_{U'}$を利用できる場合の型4, 5のM3方式の結果と同じ結果となる。	
他人支払情報偽造					
架空利用者支払情報偽造	秘密鍵SK_Iを用いて、任意に生成した公開鍵PK_{U*}に対する発行者の署名$S_I(ID_{U*})$を偽造できるため、PK_{U*}に対応する秘密鍵SK_{U*}を用いて支払情報が偽造可能である。この支払情報と公開鍵証明書のペアを加盟店のデバイスに受理させ、不正な取引を成立させることができる。			支払情報の偽造自体は可能であるが、オンライン型であるため、発行者のサーバは、支払情報に使用された公開鍵PK_{U*}が正規利用者の公開鍵のデータベースDB(PK)に登録されていないことを確認することで、不正な取引を阻止できる。	

④いずれの秘密鍵も利用しない場合

	型1	型2	型3	型4	型5
本人支払情報偽造	秘密鍵SK_Uと秘密鍵$SK_{U'}$を利用できないため、支払情報を偽造できない。				
他人支払情報偽造					
架空利用者支払情報偽造	支払情報$S_{U*}(DT)$を偽造できるものの、秘密鍵SK_Iを利用できないため、公開鍵証明書$S_I(PK_{U*})$を偽造できず、不正な取引を行うことができない。				

以　　上