■11 群（社会情報システム）－ 7 編（金融情報システム）

7 章 電子マネー・システムにおけるセキュリティ対策

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

■概要■

現在，利用可能な店舗の拡大などを背景に国内外で電子マネー・サービスが普及しつつある．2006 年度に 2 兆 6 千億円であったプリペイド型の電子マネー発行額が，2010 年度には 4 兆 5 千億円に拡大するとの予測もある [1]．電子マネー・サービスによる恩恵を享受できるようになった反面，こうしたサービスにおける電子マネーの偽造や不正なチャージなどの不正行為が懸念されている．電子マネー・サービスの形態に応じて，技術面と運用面の双方から十分な対策を実施し，適切なリスク管理を行っていくことが一層重要となってきている．

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，中山ら [2]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ほか，最近では，リスク管理まで含めた検討が鈴木ら [3, 4]によって行われている．中山ら [2]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などを踏まえると，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との問題意識から，鈴木ら [3, 4]は，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っている．

本章では，鈴木ら [3, 4] を基に電子マネー・システムにおけるセキュリティ対策とリスク管理についてみていく．まず，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．更に，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．

【本章の構成】

本章では，7-1 節で検討対象とする電子マネー・システム及びシステムへの攻撃を示すとともに，電子マネー・システムの分類を行う．7-2 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．7-3 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述べる．

■11 群 － 7 編 － 7 章

7-1 電子マネー・システムのモデルと検討対象

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

7-1-1 検討対象とする電子マネー・システム

本章では，図 7･1 のプリペイド型の電子マネー・システムを検討対象とする．電子マネー・システムにおいて取引可能な金額の根拠となる情報を価値情報と呼ぶ．まず，利用者は価値情報を電子マネーとして発行してもらうために，発行額に応じた金額を入金し，その情報（入金情報）を発行者に送り，発行者から電子マネーの発行に関する情報（発行情報）を自身のデバイス（IC カードなど）に受け取る．商品やサービスを提供する受取者から利用者がそれらを購入する際，利用者は，取引の金額，時刻，受取者などの情報（取引情報）を受取者のデバイスから受け取り，価値情報を基に代金を支払うことを示す情報（支払情報）を渡す．受取者は，各取引処理での支払情報から集計した売上に関する情報（売上情報）を発行者に送り，売上情報に応じた資金を受け取るとともに，その資金に関する情報（資金入金情報）を受け取る．発行者は，電子マネーの発行と取引の承認などを行うシステム（センター）を利用する．

図 7・1　検討対象とする電子マネー・システム

電子マネー・システムには，**図 7･1** の三つのエンティティ以外にもエンティティが存在するケースもある．本章では，支払情報の偽造攻撃への耐性を議論の主たる対象とし，分析結果をより明確にするために，支払情報をやり取りする利用者と受取者に焦点を当てて簡略化したシステムを想定した．また，発行者はセンターを安全に管理・運営していると仮定し，センターは物理的な攻撃やネットワーク経由の侵入などに対して安全であり，センターで管理される秘密情報は漏えいしないと仮定する．

7-1-2 想定する攻撃法

電子マネー・システムに対する攻撃では，システムでやり取りされる情報（発行情報，支払情報など）が盗聴・偽造の対象となりうる．中山ら [2)]は，発行情報，売上情報，支払情報を対象として分析している．本章において注目する支払情報の偽造は，不特定多数の利用者に攻撃者が紛れ込みやすく，攻撃の阻止や攻撃者の特定が相対的に困難であり，対策の検討が必須と考えられる．偽造対象の支払情報として，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ほか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を想定する．これらの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ぶ．

7-1-3 電子マネー・システムの分類

(1) 先行研究における分類

電子マネーに関連する研究分野では，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おり，各性質の分析も行われている [5]．そうした性質のうち，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への耐性は，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，宮崎ら [5]と中山ら [2]の研究事例がある．宮崎ら [5]は，発行者の不正行為を分析対象としており，支払情報の偽造という観点ではなく，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．一方，中山ら [2]は，支払情報の生成にかか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・システムを分類しており，支払情報の偽造の成否に関連した分類となっている．本章では，こうした点を踏まえて中山ら [2]の分類方法を採用する．

(2) 想定する電子マネー・システムのタイプ

中山ら [2]は，次の 4 種類の技術的特徴に基づいて電子マネー・システムを分類している．

- 価値情報の形態 : 価値情報として電子マネーの残高全体を表す情報を利用し，チャージや取引時に残高を増減する残高管理型があるほか，一つのデータに電子マネーの価値を割り当てたうえで，それらのデータの集合を価値情報として利用する電子証書型がある．電子証書型において，電子マネーの価値が割り当てられたデータは当該価値を示す金額の情報と識別番号などから構成されるケースが多く，「電子証書」と呼ばれる．
- 転々流通性 : 発行者のセンターを介さず利用者のデバイスから別の利用者のデバイスに直接価値情報を譲渡するオープン・ループ型と譲渡しないクローズド・ループ型がある．
- センター接続 : 取引時に発行者のセンターに接続し，取引の承認を行うオンライン型と，事後的に承認を行うオフライン型がある．インターネット上の取引であっても，取引時にセンターが承認を行わない場合はオフライン型となる．
- 価値情報の管理場所 : 利用者のデバイス（ローカル管理型），発行者のセンター（センター管理型），デバイスとセンターの両方（併用管理型）が想定される．

中山ら [2]は，これらを組み合わせて電子マネー・システムを型 1～9 に分類している（**表 7・1**）．現在クローズド・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が多いと推測される．また，電子証書型は，発行者が電子証書をどの利用者に発行したかを把握できないようにすることで匿名性の実現を可能にするというコンセプトのもとに提案されている（中山ら [2]）．今後，利用者のデバイスやネットワークの性能向上などによってこれらの型の実用化が容易になれば，それらの安全性についても検討することが有用と考えられるため，本章では型 1～9 を検討対象とする．

表 7・1 電子マネー・システムのモデルの分類

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		L	LC	C	L	LC	C	L	LC	C	L	LC	C
価値情報の形態	残高管理型	型 1	型 2	×	型 3	型 4	型 5	型 6	×	×	×	×	×
	電子証書型	型 7	×	×	型 8	×	×	型 9	×	×	×	×	×

（備考）本表は中山ら [2]を基に作成．L はローカル管理型，C はセンター管理型，LC は併用管理型を表す．

■11 群 － 7 編 － 7 章

7-2 電子マネー・システムにおけるセキュリティ評価

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

本小節では，型 1～9 の電子マネー・システムの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・システムにおける支払情報の処理の流れ（取引プロトコル）を説明し，電子マネー・システムの安全性にかかわる要素技術の条件（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が成功するか否かを分析する．

7-2-1 取引プロトコルの設定

商品購入の際，利用者のデバイスが支払情報を生成し，これを発行者のセンターまたは受取者のデバイスが検証して問題がなければ当該取引を成立させるという処理フローが一般的と考えられる．

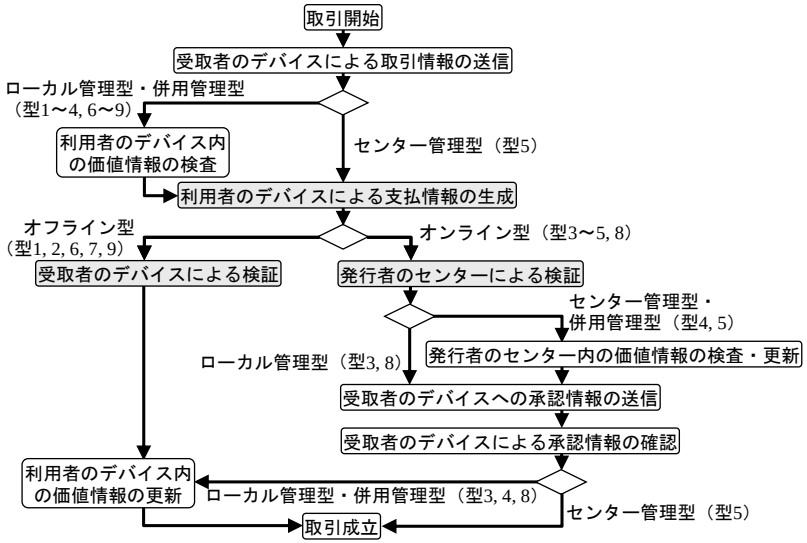

図 7・2　一般的とみられる取引の処理フロー

(1)　取引の処理フローのタイプごとの差異

具体的な取引の処理フローは，価値情報の管理場所とセンター接続の有無によって異なる（**図 7・2**）．価値情報が利用者のデバイス内で管理される場合（ローカル管理型と併用管理型）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利用者のデバイスにおいて検査され，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センター内で管理される場合（センター管理型と併用管理型）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センター内で検査され，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，受取者のデバイスが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，発行者のセンター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（承認情報）を受取者のデバイスへ送信する．受取者のデバイスは，承認情報を確認したうえで取引を成立させる．

(2) 暗号アルゴリズムによる取引プロトコルの差異

(a) 六つの方式

中山ら [2]は，取引プロトコルにおいてデバイスと通信路上での攻撃を想定している．そのうえで，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）を達成するために暗号アルゴリズム（共通鍵暗号方式や電子署名方式）を利用する 6 種類の取引プロトコルの方式を例示している．本章は，残高管理型である型 1～6 に対して M1～M3 方式を採用するとともに，電子証書型である型 7～9 に対しては三つの方式（M4～M6 方式）を中山ら [2] の具体例をベースに新たに定義する（**表 7･2**）．次に，各方式における支払情報の生成と検証の具体的な処理を説明する．

表 7・2　利用する暗号アルゴリズムのセキュリティ機能と各方式の対応

セキュリティ機能		残高管理型 (型 1～6)	電子証書型 (型 7～9)
利用者のデバイスの真正性確認	通信データの保護		
共通鍵暗号方式		M1 方式	M4 方式
共通鍵暗号方式（守秘）	電子署名方式（一貫性確保）	M2 方式	M5 方式
電子署名方式（真正性確認のみ）		M3 方式	M6 方式

(b) 記号の定義

M1～M6 方式で使用する記号を**表 7･3** のとおり定義する．

表 7・3　記号の定義

記号	定義
ID_U, $ID_{U'}$, ID_{U*}	利用者 U, ほかの実在する利用者 U', 架空の利用者 U*のそれぞれの識別情報.
B_U, N_U, V_U	利用者 U の残高（B_U），電子証書の識別番号（N_U）と金額情報（V_U）.
(PK_U, SK_U), ($PK_{U'}$, $SK_{U'}$), (PK_{U*}, SK_{U*})	利用者 U，U'，U*のそれぞれ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．システム共通の鍵.
$E_X(Y)$	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（取引対象の商品等の金額，時刻，受取者等の情報を含む）.
DB(ID), DB(PK)	正規の利用者の識別情報（ID，公開鍵）を管理するデータベース.
DB(ID, B), DB(PK, B)	正規の利用者の残高を管理するデータベース.
DB(N, V)	有効な電子証書の識別番号と対応する金額情報に関するデータベース.

(c) 各エンティティが管理する情報

型 1～9 の各特徴と M1～M6 方式が利用するセキュリティ機能から，各エンティティが管理する情報を整理すると**表 7･4** のとおりである．価値情報の管理場所に応じて，各型において利用者のデバイスとセンターが価値情報（残高あるいは電子証書）を管理するか否かが決まる．センター接続の有無に応じ，各型において受取者のデバイスが検証に必要な鍵を管理するか否かが決まる．ただし，型によらずセンターはすべての鍵を管理しているとする．例

えば，型 6 は，ローカル管理型であり利用者のデバイスのみで残高が管理されるほか，オフライン型であり受取者のデバイスで検証用の鍵が管理される．

表 7・4　各エンティティが管理する情報

<table>
<tr><th></th><th>利用者のデバイス</th><th>受取者のデバイス</th><th>発行者のセンター</th></tr>
<tr><td>型2</td><td rowspan="3">M1方式：K, ID_U, B_U
M2方式：K, $S_I(ID_U)$, B_U
M3方式：SK_U, $S_I(PK_U)$, B_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), DB(ID, B)
M2方式：K, SK_I, PK_I, DB(ID), DB(ID, B)
M3方式：SK_I, PK_I, DB(PK), DB(PK, B)</td></tr>
<tr><td>型1, 6</td><td>M1方式：K, DB(ID)
M2方式：K, SK_I, PK_I, DB(ID)
M3方式：SK_I, PK_I, DB(PK)</td></tr>
<tr><td>型3
型4</td><td rowspan="2">M1～M3方式：なし</td><td rowspan="2">M1方式：K, DB(ID), DB(ID, B)
M2方式：K, SK_I, PK_I, DB(ID), DB(ID, B)
M3方式：SK_I, PK_I, DB(PK), DB(PK, B)</td></tr>
<tr><td>型5</td><td>M1方式：K, ID_U
M2方式：K, $S_I(ID_U)$
M3方式：SK_U, $S_I(PK_U)$</td></tr>
<tr><td>型7, 9</td><td rowspan="2">M4方式：K, ID_U, N_U, V_U
M5方式：K, $S_I(ID_U)$, $S_I(S_I(ID_U), N_U, V_U)$
M6方式：SK_U, $S_I(PK_U)$, $S_I(S_I(PK_U), N_U, V_U)$</td><td>M4方式：K
M5方式：K, PK_I
M6方式：PK_I</td><td rowspan="2">M4方式：K, DB(ID), DB(N, V)
M5方式：K, SK_I, PK_I, DB(ID), DB(N, V)
M6方式：SK_I, PK_I, DB(PK), DB(N, V)</td></tr>
<tr><td>型8</td><td>M4～M6方式：なし</td></tr>
</table>

(d)　支払情報の生成・検証

各方式が利用するセキュリティ機能に応じて，支払情報の形式が異なる．M1, M2, M4, M5 方式は，通信データの守秘のために共通鍵暗号方式を利用し，取引情報と利用者の識別情報を暗号化・伝送する．M4, M5 方式では，これらに加え電子証書も暗号化・伝送の対象とする．電子証書は，M4 方式では(N_U, V_U)となり，M5, M6 方式では $S_I(S_I(PK_U), N_U, V_U)$となる．M3 方式は，取引情報に利用者が署名を施し伝送するほか，M6 方式では，これらに加え電子証書も伝送する．以上により，M1 方式では $E_K(ID_U, DT)$，M2 方式では $E_K(S_I(ID_U), DT)$，M3 方式では $S_U(DT)$, $S_I(PK_U)$, M4 方式では $E_K(ID_U, N_U, V_U, DT)$, M5 方式では $E_K(S_I(S_I(ID_U), N_U, V_U), S_I(ID_U), DT)$，M6 方式では $S_U(DT)$, $S_I(PK_U)$, $S_I(S_I(PK_U), N_U, V_U)$がそれぞれ支払情報となる．

表 7・5　受取者のデバイスによる支払情報とその検証（型 1, 2, 6, 7, 9）

方式	検証処理
M1方式	①支払情報 $E_K(ID, DT)$を復号し，DT を抽出．②DT が当該取引のものか否かを検査.
M2方式	①支払情報 $E_K(S_I(ID_U), DT)$を復号し，$S_I(ID_U)$と DT を抽出．②PK_I を用いて $S_I(ID_U)$を検査．③DT が当該取引のものか否かを検査.
M3方式	支払情報は $S_U(DT)$, $S_I(PK_U)$である．①PK_I を用いて $S_I(PK_U)$を検査し，PK_U を抽出．②PK_U を用いて $S_U(DT)$を検査．③DT が当該取引のものか否かを検査.
M4方式	①支払情報 $E_K(ID_U, N_U, V_U, DT)$を復号し，V_U, DT を抽出．②DT が当該取引のものか否かを検査．③DT を用いて V_U の不足を検査.
M5方式	①支払情報$E_K(S_I(S_I(ID_U), N_U, V_U), S_I(ID_U), DT)$を復号し，$S_I(S_I(ID_U), N_U, V_U)$, $S_I(ID_U)$, DT を抽出．②PK_I を用いて $S_I(S_I(ID_U), N_U, V_U)$の真正性を検査し，V_U を抽出．③PK_I を用いて $S_I(ID_U)$を検査．④DT が当該取引のものか否かを検査．⑤DT を用いて V_U の不足を検査.
M6方式	支払情報は $S_U(DT)$, $S_I(PK_U)$, $S_I(S_I(PK_U), N_U, V_U)$である．①PK_I を用いて $S_I(S_I(PK_U), N_U, V_U)$を検査し，$S_I(PK_U)$, V_U を抽出．②PK_I を用いて $S_I(PK_U)$を検査し，PK_U を抽出．③PK_U を用いて $S_U(DT)$の真正性を検査し，DT を抽出．④DT が当該取引のものか否かを検査．⑤DT を用いて V_U の不足を検査.

受取者のデバイスで支払情報の検証を行う場合（型 1, 2, 6, 7, 9）は，支払情報に含まれる取引情報が当該取引のものか否かが検査される．これに加え，M4～M6 方式では電子証書の真正性と価値情報の不足が検査される（**表 7･5**）．

センターで支払情報の検証を行う場合（型 3～5, 8）は，支払情報に含まれる利用者の識別情報が正規の利用者のものか否かが検査される．これに加え，M4～M6 方式では，電子証書の識別番号の有効性（登録の有無，二重使用など）が検査される（**表 7･6**）．

表 7・6　発行者のセンターによる支払情報の検証（型 3～5, 8）

方式	検証処理
M1 方式	①支払情報 $E_K(ID_U, DT)$を復号し，ID_U を抽出．②DB(ID)に ID_U が登録されているか否かを検査.
M2 方式	①支払情報 $E_K(S_I(ID_U), DT)$を復号し，$S_I(ID_U)$を抽出．②PK_I を用いて $S_I(ID_U)$を検査．③DB(ID)に ID_U が登録されているか否かを検査.
M3 方式	①PK_I を用いて $S_I(PK_U)$を検査し，PK_U を抽出．②DB(PK)に PK_U が登録されているか否かを検査．③PK_U を用いて $S_U(DT)$を検査.
M4 方式	①支払情報 $E_K(ID_U, N_U, V_U, DT)$を復号し，ID_U, N_U, V_U, DT を抽出．②DB(ID)に ID_U が登録されているか否かを検査．③DB(N, V)を用いて，N_U の登録の有無，N_U の二重使用，N_U と V_U の対応を検査．④DT を用いて V_U の不足を検査.
M5 方式	①支払情報 $E_K(S_I(S_I(ID_U), N_U, V_U), S_I(ID_U), DT)$を復号し，$S_I(S_I(ID_U), N_U, V_U)$, $S_I(ID_U)$, DT を抽出．②PK_I を用いて $S_I(S_I(ID_U), N_U, V_U)$の真正性を検査し，N_U, V_U を抽出．③PK_I を用いて $S_I(ID_U)$を検査．④DB(ID)に ID_U が登録されているか否かを検査．⑤DB(N, V)を用いて，N_U の登録の有無，N_U の二重使用，N_U と V_U の対応を検査．⑥DT を用いて V_U の不足を検査.
M6 方式	①PK_I を用いて $S_I(S_I(PK_U), N_U, V_U)$を検査し，$S_I(PK_U)$, N_U, V_U を抽出．②PK_I を用いて $S_I(PK_U)$を検査し，PK_U を抽出．③DB(PK)に PK_U が登録されているか否かを検査．④PK_U を用いて $S_U(DT)$の真正性を検査し，DT を抽出．⑤DB(N, V)を用いて，N_U の登録の有無，N_U の二重使用，N_U と V_U の対応を検査．⑥DT を用いて V_U の不足を検査.

7-2-2 環境条件

電子マネー・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などの暗号処理用のデバイスと共通鍵暗号や公開鍵暗号などの暗号アルゴリズムに焦点を当てる．

(1)　暗号処理用のデバイスの安全性

中山ら[2]は，暗号処理用のデバイスに物理的損傷を与えて回路内部を観察するという破壊攻撃と，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などの情報を用いて暗号鍵を推定するという非破壊攻撃を取り上げ，検討時点ではこれらの攻撃に対する安全性を客観的に評価困難であると指摘し，デバイスが危殆化した状況のみを想定している．最近では，攻撃法や対策の研究が進展し，暗号モジュールの試験・認証制度 JCMVP[7]が運用されているほか，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・認証の枠組みとして，EMVCo の枠組み[8]も整備されている．これらを活用することで一定の安全性を有するデバイスが利用可能になっている．ただし，試験対象でない攻撃法や新たに提案され対策が確立していない攻撃法を前提とすれば，デバイスが危殆化するおそれは否定できない．そこで，本章では，デバイスが安全な場合と危殆化した場合の両方を想定し，デバイス内に格納されている暗号鍵などの秘密情報が読出困難な状況を「デバイスが安全である」，読出可能な状況を「デバイスが危殆化している」とそれぞれ呼ぶ．

攻撃者が攻撃実行時にアクセスするデバイスごとに攻撃者が得られる情報は次のとおりで

ある．

- 利用者のデバイスにアクセスする場合，非破壊攻撃などによって内部の鍵などを読み出す．
- 受取者のデバイスにアクセスする場合，①受取者のデバイス内部の鍵などを読み出すことに加え，同デバイスに不正な加工を施し，利用者のデバイスの内部の鍵などを読み出すケースと，②ネットワーク上での取引において受取者のデバイスからのみ非破壊攻撃によって暗号鍵などを読み出すケースがある．

これらの分析を踏まえ，（攻撃者本人が所持する）利用者のデバイスの鍵などを入手するケース（ケース 1），受取者のデバイスの鍵などを入手するケース（ケース 2），受取者のデバイスの鍵などに加え，同デバイスを経由して（複数の）利用者のデバイスの鍵なども入手するケース（ケース 3）を想定する．

(2) 暗号アルゴリズムの安全性

中山ら[2]は，暗号アルゴリズムのセキュリティ評価手法の成熟などを根拠に，暗号アルゴリズムが安全である状況を想定している．現状をみると，国内外において，公的機関による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，我が国では，電子政府推奨暗号リスト[9]が 2003 年に公表されている．一方，システム修正のコストやほかのシステムとの互換性の維持といった運用上の制約から，安全性の低下が著しい暗号アルゴリズムが利用され続けているケースもあり，暗号アルゴリズムが危殆化しないとは言い切れないとの指摘もある[10]．そこで，本章では，暗号文の解読や署名の偽造などが困難な状況を「暗号アルゴリズムが安全である」，暗号鍵や秘密鍵を現実的な時間内に探索可能であるという状況を「暗号アルゴリズムが危殆化している」とし，両方の状況を想定する．その際，暗号アルゴリズムの危殆化によりデバイス内に格納されている暗号鍵などを入手可能な場合は，デバイスの危殆化には含めない扱いとする．また，発行者が利用者の識別情報に対して署名を施すために利用する電子署名方式（発行者用署名方式）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（利用者用署名方式）よりも安全性が高いと仮定する．また，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．

7-2-3 危殆化により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は以下の情報を入手する．

- 攻撃者は，共通鍵暗号方式が危殆化した場合，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た場合，利用者本人の秘密鍵 SK_U とほかの利用者の秘密鍵 $SK_{U'}$ を入手する．
- 攻撃者は，発行者用署名方式が危殆化した場合，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た場合，ケース 1～3 に応じた鍵をそれぞれ入手する．

これらを基に，各方式において攻撃者が入手する鍵をまとめると**表 7･7** のとおりである．表 7･7 をみると，デバイスが危殆化し共通鍵暗号が安全な状況では，攻撃者が暗号鍵 K を入手できる場合（型 1, 2, 6, 7, 9 のケース 1～3 と型 3～5, 8 のケース 1, 3）とできない場合（型 3～5, 8）がある．これは，オンライン型のタイプ（型 3～5, 8 のケース 2）では，受取者のデバイスが支払情報を検証しないため暗号鍵 K を格納しておらず，当該状況において攻撃者が本

デバイスにアクセスしても（ケース 2），この鍵を入手できないためである．

表 7・7　各環境条件のもとで攻撃者が入手する鍵

(1)　M1, M4 方式について

		M1方式 (型1, 2, 6)	M4方式 (型7, 9)	M1方式 (型3～5)	M4方式 (型8)
・デバイスが危殆化 ・共通鍵暗号方式は安全	ケース1, 3	K			
	ケース2	K		なし	
・共通鍵暗号方式が危殆化 （デバイスの状態に依存しない）	ケース1～3	K			

(2)　M2, M5 方式について

		M2方式 (型1, 2, 6)	M5方式 (型7, 9)	M2方式 (型3～5)	M5方式 (型8)
・デバイスが危殆化 ・共通鍵暗号方式は安全 ・発行者用署名方式は安全	ケース1, 3	K			
	ケース2	K		なし	
・デバイスが危殆化 ・共通鍵暗号方式は安全 ・発行者用署名方式は危殆化	ケース1, 3	K, SK_I			
	ケース2	K, SK_I		SK_I	
・デバイスは安全 ・共通鍵暗号方式は安全 ・発行者用署名方式が危殆化	ケース1～3	SK_I			
・共通鍵暗号方式が危殆化 ・発行者用署名方式は安全 （デバイスの状態に依存しない）	ケース1～3	K			
・共通鍵暗号方式が危殆化 ・発行者用署名方式が危殆化 （デバイスの状態に依存しない）	ケース1～3	K, SK_I			

(3)　M3, M6 方式について

		M3方式(型1～6)	M6方式(型1～9)
・デバイスが危殆化 ・利用者用署名方式は安全 ・発行者用署名方式は安全	ケース1	SK_U	
	ケース2	なし	
	ケース3	SK_U, $SK_{U'}$	
・利用者用署名方式が危殆化 ・発行者用署名方式は安全 （デバイスの状態に依存しない）	ケース1～3	SK_U, $SK_{U'}$	
・利用者用署名方式が危殆化 ・発行者用署名方式が危殆化 （デバイスの状態に依存しない）	ケース1～3	SK_U, $SK_{U'}$, SK_I	

7-2-4 支払情報の偽造の成功のレベル

表 7･7 より，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）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，受取者のデバイスあるいは発行者のセンターが当該支払情報の偽造を検知困難な状況を意味するものとする．偽造の成功のレベルは，①成功しない，②特定の条件のもとでのみ成功する，③成功するという 3 段階が考えられ，以下では各段階にそれぞれ 0, 1, 2 という数字を割り当てる．数字が小さいほど偽造の成功のレベルは低く，偽造への耐性が高いといえる．本分析の結果は**表 7･8** のとおりである．同表では，三つの数字を連結し，例えば「0-1-0」のように表記している．各数字は左から順に，本人支払情報偽造，他人支払情報偽造，架空利用

者支払情報偽造の成功のレベルをそれぞれ示す．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」ことを意味する．

表 7・8　支払情報偽造の成功レベル

(1) 型 1〜6（M1〜M3 方式）について

	利用可能な鍵	型1, 2, 6	型3	型4, 5
M1方式	K	2-2-2	2-2-0	$0\text{-}1^{A}\text{-}0$
M2方式	K	2-2-0		$0\text{-}1^{A}\text{-}0$
	SK_I	0-0-0		
	K, SK_I	2-2-2	2-2-0	$0\text{-}1^{A}\text{-}0$
M3方式	SK_U	2-0-0		0-0-0
	SK_U, $SK_{U'}$	2-2-0		$0\text{-}1^{A}\text{-}0$
	SK_U, $SK_{U'}$, SK_I	2-2-2	2-2-0	$0\text{-}1^{A}\text{-}0$

(2) 型 7〜9（M4〜M6 方式）について

	利用可能な鍵	型7, 9	型8
M4方式	K	2-2-2	$1^{BC}\text{-}1^{BC}\text{-}0$
M5方式	K	2-2-0	$0\text{-}1^{B}\text{-}0$
	SK_I	0-0-0	
	K, SK_I	2-2-2	$1^{BC}\text{-}1^{BC}\text{-}0$
M6方式	SK_U	2-0-0	0-0-0
	SK_U, $SK_{U'}$	2-2-0	$0\text{-}1^{B}\text{-}0$
	SK_U, $SK_{U'}$, SK_I	2-2-2	$1^{BC}\text{-}1^{BC}\text{-}0$

（備考）評価結果「1」の右上の記号（A〜C）は，攻撃成功の条件であり，いずれかを満たせば不正な取引が成立する．A は「偽造した支払情報に対応する利用者を U'とすると，センターで管理されている U'の価値情報が取引金額に対して足りている」，B は「ほかの利用者が取引時に送信した電子証書を盗取し，当該利用者の取引より先にセンターによる検証を受け有効と判断される」，C は「推測した電子証書の識別番号を基に偽造した電子証書がセンターに有効であると判断される」を意味する．

(1)　方式間の比較

同一の型において各方式の支払情報偽造の成功のレベルを比較する．攻撃者が利用可能な鍵のバリエーションは方式ごとに異なる．まず，攻撃者が利用可能な鍵が同一のケースに注目すると，攻撃者が利用する鍵が同一となるのは，M1, M2, M4, M5 方式において「攻撃者が秘密鍵 K を利用するケース」のみである．このケースでは，M1 方式と M2 方式（型 1〜6），M4 方式と M5 方式（型 7〜9）をそれぞれ比較できる．型 3〜5 では，M1 方式と M2 方式の偽造の成功のレベルは 2-2-0 または $0\text{-}1^{A}\text{-}0$ であって同一である．型 1, 2, 6 では，M2 方式（2-2-0）が M1 方式（2-2-2）よりも偽造の成功のレベルが低く，偽造への耐性が相対的に高いといえる．また，型 7〜9 では，M5 方式（2-2-0 または $0\text{-}1^{B}\text{-}0$）が M4 方式（2-2-2 または $1^{BC}\text{-}1^{BC}\text{-}0$）に比べて偽造の成功のレベルが低く，偽造への耐性が高いといえる．

次に，攻撃者が利用可能な鍵が最も多いケースに注目し，M1〜M3 方式（型 1〜6），M4〜M6 方式（型 7〜9）を比較する．M1〜M6 方式の偽造の成功のレベルは，方式ではなく型に応じて，2-2-2（型 1, 2, 6, 7, 9），2-2-0（型 3），$1^{BC}\text{-}1^{BC}\text{-}0$（型 8），$0\text{-}1^{A}\text{-}0$（型 4, 5）のいずれかになる．本ケースでは，同一の型における各方式の偽造への耐性は等しいといえる．

(2)　電子証書型と残高管理型の比較

電子証書型と残高管理型を，センター接続，転々流通性，価値情報の管理場所に関するそれぞれの特徴が同一となるシステム同士で比較する．電子証書型の型 7〜9 には，残高管理型の型 1, 3, 6 がそれぞれ対応することから，これらを比較する．型 1, 6, 7, 9 については，支払情報偽造の成功のレベルが 2-2-2 であり同一となっている．型 8（$1^{BC}\text{-}1^{BC}\text{-}0$）については，型 3（2-2-0）に比べて支払情報偽造の成功のレベルが低い．これは，型 8 が，センターで管理している電子証書の識別番号などを検証に利用できるという点で，型 3 よりも多くの検証手段を備えていることによる．以上より，価値情報の形態以外の特徴が同一の場合，支払情報の偽造に対しては，電子証書型がより安全といえる．

(3) 支払情報偽造に影響を与える特徴

電子マネー・システムにおける四つの特徴（センター接続，転々流通性，価値情報の形態，価値情報の管理場所）のなかで支払情報偽造の成否に最も影響を与える特徴はどれかを分析する．各特徴に注目して型 1〜9 を分けるとともに，各型に対応する支払情報偽造の成功のレベルを整理する（**表 7･9**）．ここでは，各型において攻撃者が利用可能な情報が最も多いときの偽造成功のレベルを用いる．各レベルは，2-2-2, 2-2-0, 1^{BC}-1^{BC}-0, 0-1^{A}-0 のいずれかになる．

センター接続に注目した場合，オフライン型（2-2-2）よりもオンライン型（2-2-0, 1^{BC}-1^{BC}-0, 0-1^{A}-0）が成功のレベルが低い．そのほかの特徴に着目すると，いずれも偽造成功のレベルに明確な差異はみられない．

以上の分析より，オンライン型かオフライン型かによって，支払情報偽造の成功のレベルに明確な差異が生じ，偽造成功のレベルの上限が定まることがわかる．したがって，オンライン型かオフライン型かが攻撃の成否に有意な影響を与えているといえる．

表 7・9　各特徴で分類した場合の偽造成功のレベル

(1) センター接続に注目した場合

オンライン型 (型3〜5, 8)	オフライン型 (型1, 2, 6, 7, 9)
2-2-0, 1^{BC}-1^{BC}-0, 0-1^{A}-0	2-2-2

(2) 転々流通性に注目した場合

クローズド・ループ型 (型1〜5, 7, 8)	オープン・ループ型 (型6, 9)
2-2-2, 2-2-0, 1^{BC}-1^{BC}-0, 0-1^{A}-0	2-2-2

(3) 価値情報の形態に注目した場合

残高管理型 (型1〜6)	電子証書型 (型7〜9)
2-2-2, 2-2-0, 0-1^{A}-0	2-2-2, 1^{BC}-1^{BC}-0

(4) 価値情報の管理場所に注目した場合

ローカル管理型 (型1, 3, 6〜9)	併用管理型 (型2, 4)	センター管理型 (型5)
2-2-2, 2-2-0, 1^{BC}-1^{BC}-0	2-2-2, 0-1^{A}-0	0-1^{A}-0

■11 群 － 7 編 － 7 章

7-3 電子マネー・システムにおけるリスク管理

（執筆者：鈴木雅貴）［2009 年 3 月 受領］

7-3-1 リスク管理の重要性

支払情報の偽造による攻撃が行われた場合，電子マネーの発行者などに金銭的な損害が発生する可能性があるほか，電子マネー・サービスに対するレピュテーションが大きく低下する可能性もある．そのため，リスクを許容レベル以下に抑えるよう適切にリスク管理を行う必要がある．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ことから，これらの要素を制御してリスク管理を行うという方法が考えられる．その際には，利用者の利便性や費用などを考慮してリスク分析を適切に行う必要がある．

7-3-2 被害発生時の損失の軽減

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 日当たりの取引金額を低く設定するという方法や，1 回あるいは 1 日当たりのチャージ金額や価値情報の上限を低くするという方法が考えられる．現行の電子マネー・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（**表 7･10**）．

表 7・10　1 回の取引金額における利用可能限度額の例

Suica, PASMO, QUICPay	Smartplus	WAON	nanaco	Edy	OneTouch	Octopus
2 万円	3 万円	5 万円	149,995 円 (5 枚併用時)	25 万円 (5 枚併用時)	10GBP =約 1,414 円	1,035HKD =約 13,579 円

（備考）本表は，各電子マネー・サービスのウェブサイトやヒアリングを基に作成した．OneTouch と Octopus に関しては，それぞれ 1GBP=141.43JPY，1HKD=13.12JPY（2009 年 3 月 16 日 10:31，三菱東京 UFJ 銀行の対顧客電信売相場）として換算した．

7-3-3 発生頻度の抑制

発生頻度の抑制には，まず，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が考えられる．具体的には，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，EMV 仕様では，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ほか，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，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．

また，危殆化を想定し，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運用上の対策の採用もありうる．そうした対策としては，目的に応じて，不正な取引の成立の阻止（目的 1），不正な取引の検知（目的 2），検知した不正取引による被害の拡大防止（目的 3）という 3 種類が考えられる．電子マネー・システムのタイプ，及び目的に応じて，適応可能

となりうる対策が異なる．例えば，次の対策が考えられる（表 7・11）．

対策 A：取引時やデバイスの始動時等に本人確認を実施する．
対策 B：正規の利用者の識別情報に関するリスト（ホワイトリスト）を利用する．
対策 C：正規の電子証書識別番号に関するリスト（ホワイトリスト）を利用する．
対策 D：不正な利用者の識別情報に関するリスト（ブラックリスト）を利用する．
対策 E：不正な電子証書識別番号に関するリスト（ブラックリスト）を利用する．
対策 F：取引時に，本人の購入パターンか否かを検査する．
対策 G：取引後に，本人の購入パターンか否かを検査する．
対策 H：利用者のデバイスで管理されている価値情報と発行者のセンターで管理されている価値情報を突合することで，価値情報を検査する．
対策 I：利用者が，発行者に自身の価値情報を照会する．
対策 J：電子証書の有効性を検査する．

表 7・11　各型において候補となりうる運用面からの対策例

<table>
<tr><th colspan="2"></th><th>本人支払情報偽造</th><th>他人支払情報偽造</th><th>架空利用者支払情報偽造</th></tr>
<tr><td rowspan="3">型 1, 2</td><td>目的 1</td><td>攻撃の検知・阻止は困難．</td><td>対策 A</td><td>対策 A, B</td></tr>
<tr><td>目的 2</td><td colspan="2">対策 G（型 2 では対策 H も候補）</td><td>対策 B</td></tr>
<tr><td>目的 3</td><td colspan="2">対策 D</td><td>上記対策が機能しない場合には対策困難．</td></tr>
<tr><td rowspan="3">型 3, 8</td><td>目的 1</td><td>対策 F</td><td>対策 A, F</td><td rowspan="3">不正な取引を阻止できるか否かはタイプに依存．</td></tr>
<tr><td>目的 2</td><td colspan="2">上記対策が機能しない場合には対策困難．</td></tr>
<tr><td>目的 3</td><td colspan="2">対策 D（型 8 では対策 E も候補）</td></tr>
<tr><td rowspan="3">型 4, 5</td><td>目的 1</td><td rowspan="3">不正な取引を阻止できるか否かはタイプに依存．</td><td>対策 A, F</td><td rowspan="3">不正な取引を阻止できるか否かはタイプに依存．</td></tr>
<tr><td>目的 2</td><td>対策 H（型 4 の場合）
対策 I（型 5 の場合）</td></tr>
<tr><td>目的 3</td><td>対策 D</td></tr>
<tr><td rowspan="3">型 6</td><td>目的 1</td><td>攻撃の検知・阻止は困難．</td><td>対策 A</td><td>対策 A, B</td></tr>
<tr><td>目的 2</td><td colspan="2">対策 G</td><td>対策 B</td></tr>
<tr><td>目的 3</td><td colspan="2">対策 D</td><td>上記対策が機能しない場合には対策困難．</td></tr>
<tr><td rowspan="3">型 7, 9</td><td>目的 1</td><td>対策 C</td><td>対策 A, C</td><td>対策 A, B, C</td></tr>
<tr><td>目的 2</td><td colspan="2">対策 G, J</td><td>対策 B（型 7 では対策 J も候補）</td></tr>
<tr><td>目的 3</td><td colspan="2">対策 D, E</td><td>対策 E</td></tr>
</table>

こうした対策には，以下のとおり，解決すべき課題があるものや一定の条件のもとでのみ効果を発揮するものがある点には留意が必要である．

- ホワイトリストやブラックリストを用いる対策（B～E）では，リストのサイズが膨大な場合，受取者のデバイスに格納させるといった運用が困難になり，実現可能性が低下する可能性がある．
- ブラックリストを用いる対策（D, E）では，不正な利用者の識別情報や電子証書識別番号をリストに反映させるまでは効果が期待できない．
- 購入パターンを用いる対策（F, G）では，どのようなパターンを不正な取引と判定するかを明確にする必要があり，不正取引の誤検知や検知の失敗が発生する可能性がある．

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，こうした点を十分に考慮する必要がある．

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技術が期待どおりの効果を発揮しているか否かをつねに確認していくとともに，適切なリスク管理のもとで，デバイスなど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

1) 矢野経済研究所，“プリペイド決済市場に関する調査結果，”リサーチエクスプレス，8th Jan. 2008.
2) 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，vol.18，no.s2，pp.57-114，日本銀行金融研究所，1999.
3) 鈴木雅貴・廣川勝久・宇根正志，“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，”金融研究，vol.27，no.s1，pp.39-78，日本銀行金融研究所，2008.
4) 鈴木雅貴・宇根正志，“暗号アルゴリズムとデバイスの危殆化を想定した電子マネー・システムのセキュリティ分析，”信学技報，ISEC2008，pp.39-46，電子情報通信学会，2008.
5) E. Chida, M. Manbo and H. Shizuya, “Digital Money – A Survey”, Interdisciplinary Information Sciences, vol.7, no.2, Tohoku University, pp.135-165, 2001.
6) 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，pp.67-74，電子情報通信学会，1998.
7) 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)（http://www.ipa.go.jp/security/jcmvp/）
8) EMVCo, “EMV Integrated Circuit Card Specification for Payment Systems (EMV 4.2): Book 2 – Security and Key Management,” EMVCo, 2008.
9) 総務省・経済産業省，“電子政府推奨暗号リスト，”（http://www.cryptrec.jp/images/cryptrec_01.pdf），総務省・経済産業省，2003.
10) 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，vol.26，no.s1，pp.31-51，日本銀行金融研究所，2007.