電子マネーの安全性評価について
An evaluation of security of e-money

中山　靖司
Yasushi NAKAYAMA

Email:yasushi.nakayama@boj.or.jp

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

Institute for Monetary and Economic Studies
Bank of Japan

2-1-1, Hongoku-Cho Nihonbashi,
Chuo-Ku Tokyo, 103-8660 Japan
(URL:http://www.imes.boj.or.jp/)

太田　和夫
Kazuo OHTA

Email:ohta@sucaba.isl.ntt.co.jp

日本電信電話株式会社
情報通信研究所

〒239-0847 横須賀市光の丘 1-1
NTT 情報通信研究所 Y-609A

NTT Information and Communication Systems Laboratories
Nippon Telegraph and Telephone Corporation

1-1, Hikarinooka Yokosuka-Shi,
Kanagawa 239-0847 Japan

松本　勉
Tsutomu MATSUMOTO

Email: tsutomu@mlab.dnj.ynu.ac.jp

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

〒240-8501 横浜市保土ヶ谷区
常盤台 79-5 電子情報工学棟

Division of Artificial Environment and Systems
Yokohama National University

Elec. and Comp. Bldg. 79-5, Tokiwadai,
? □ 言
hama, 240-8501 Japan

あらまし

電子マネーのセキュリティ対策については、既に様々な学術的・技術的研究が行なわれているが、それらの評価を行なうに当たっては、発生し得るリスクと、それを防止するためのコストに関する比較考察が必要である。本稿では、様々な電子マネー実現方式を機能およびセキュリティの観点から整理・類型化し、このモデルを前提に、発生し得るリスクの程度・範囲を分析することにより、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示す。

Abstract

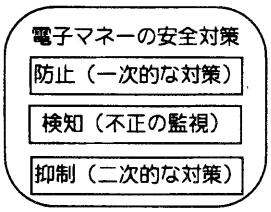
To evaluate security of electronic money from the practical viewpoint, it is essential to consider risk and cost of various combinations of security measures in all aspects. In this paper, we examined all possible combinations of functions and security technologies of e-money and proposed a method to evaluate security of e-money.

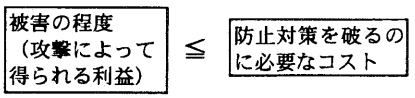
出典

SCIS'98 The 1998 Symposium on Cryptography and Information Security
Hamanako, Japan, January 28-31, 1998
The Institute of Electronics, Information and Communication Engineers

1.はじめに

電子マネーのセキュリティは、「不正を未然に防ぐこと」（防止）、「不正の発生の検出、あるいはさらに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）の３つの観点から論じることができる。本稿では防止については直接検討の対象とせず、防止対策が破られたときにどのような影響が出るかを分析することによって、各電子マネーを安全性の面から比較するとともに、防止対策に必要な強度を検討するひとつの材料を提供する。





2.モデル化

本稿では、具体的な電子マネープロジェクトを想定するのではなく、電子マネー一般に対して適応可能な結論を導出することを目的とする。その方法としては、電子マネーのセキュリティに影響を与える技術的な特徴について、考えられる選択肢の全ての組合せを評価の対象とすることにする。

電子マネーの技術的な特徴としては、１）電子マネーの価値の形態、２）転々流通性の有無、３）価値情報の管理場所、４）センター接続の有無、５）使用する暗号技術、などが考えられる。ここでは１）～４）の項目をもとに考え得るモデルを示し、それぞれについて５）の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。

2.1 モデル化

１）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。

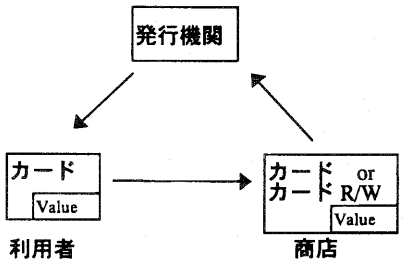
電子証書型：個々の電子マネーが額面金額、識別番号等の情報を持った、それぞれを区別することができる方法で、これを受け渡すことによって支払や受け取りを処理。

２）転々流通性の有無

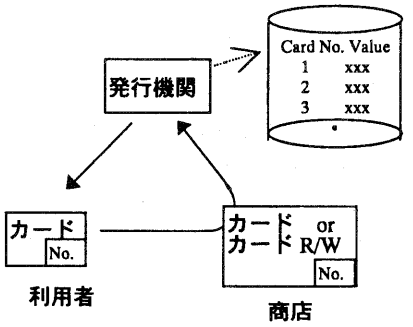
利用者から利用者への電子マネーの譲渡が可能かどうかによってopen-loop型とclosed-loop型に分類。

３）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かセンター（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１，２参照）。



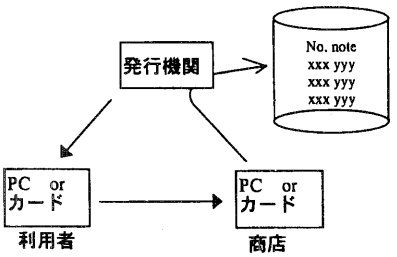
（図１）残高管理型＜ローカル＞の例



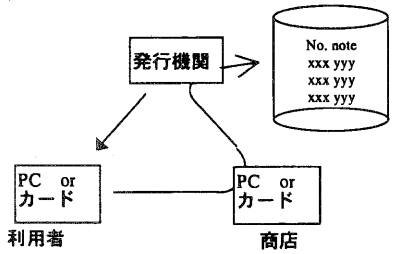
（図２）残高管理型＜センター＞の例

４）センター接続の有無

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３，４参照）。



（図３）証書型＜事後＞の例



（図４）証書型＜即時＞の例

こうしたモデル化から全ての組合わせ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合せもあり、全てについて電子マネーが存在するわけではない。各組合せにおける電子マネーの有無を示したものが表１であり、実際には残高管理型４種類（残高ローカルクローズド、残高併用クローズド、残高センタークローズド、残高ローカルオープン）、電子証書型３種類（証書事後クローズド、証書即時クローズド、証書事後オープン）が実現可能なモデルとして残る。なお、現在、各地で実際にプロジェクトとして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。

2.2 暗号技術の選択肢

前提とする価値移転のための暗号技術としては、以下のものについて検討する。

（残高管理型）

共通鍵型：本人確認およびデータ送受信に秘密鍵暗号を使用する方式。

共通鍵型＜静的認証あり＞：データ送受信に秘密鍵暗号を使用するが、本人の所持するカードの認証はセンターの秘密鍵によって署名された証明書による方式。

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＞に対する署名を生成）によって行なう方式。さらに、データ送受信に暗号を使うこともある。

（電子証書型）

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

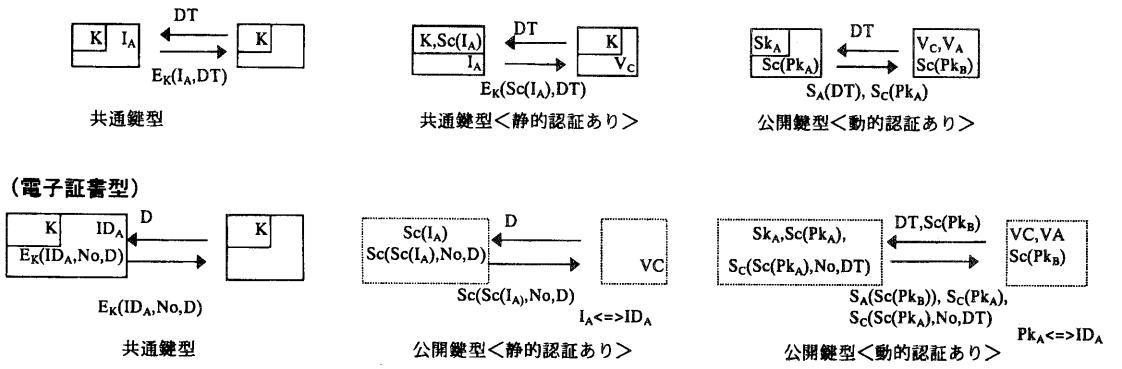
公開鍵型＜静的認証あり＞：本人確認をセンターの秘密鍵によって署名された証明書によって行なう方法。なお、電子証書自体もセンターの秘密鍵によって署名。

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＞に対する署名を生成）

価値管理方法	残高管理型										電子証書型			
流通形態	closed-loop						open-loop				closed-loop		open-loop	
価値管理場所	ローカル		併用		センター		ローカル		センター		ローカル（電子証書型の特徴）			
センター接続	off	on	off	on	off	on	off	on	off	on	off (事後)	on (即時)	off (事後)	on (即時)
モデル有無	○	× (※1)	○	× (※1)	× (※2)	○	○	× (※3)	× (※2)	× (※3)	○	○	○	× (※3)

※１センターに on-line 接続する場合、ローカルに価値を持つこと自体が無意味。
※２センターに on-line 接続せずにセンターで残高を管理することは不可能。
※３open-loop 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 open-loop とはいえない。

（表１）電子マネーのモデル類型



記号　K：秘密鍵
$E_K(X)$：データ X を鍵 K で暗号化
I_A：利用者 A の匿名の識別子
ID_A：利用者 A の実名の識別子
Pk_A,Pk_B：利用者 A,B の公開鍵
Sk_A,Sk_B：利用者 A,B の秘密鍵

Sc(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
V_C,V_A：センターC,利用者 A による署名を検証する関数
DT：店名、金額、時刻等
D：金額

（図５）セキュリティ技術毎の支払シーケンス例

によって行なう方式。なお、電子証書自体もセンターの秘密鍵によって署名。

―― なお、電子証書型において共通鍵型は匿名性がないのに対し、公開鍵型は両者ともブラインド署名を使うことにより匿名性を持ち、不正が行なわれた場合のみ実名が露見する仕組みのものとする。

３．前提条件と評価項目

3.1 前提条件

不特定多数の利用者が不特定多数の商店で電子現金を用いて支払う状況において、１次的な不正防止対策が破られる等により、IC カード等の耐タンパー機器の中の情報が読み出されたり、PC 上の記憶装置の情報が不正に利用されることによって、どのような被害が想定されるのかを分析する。

なお、使用する秘密鍵暗号、公開鍵暗号、署名暗号は、適切なアルゴリズムを利用し、十分な鍵長をとっ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。

3.2 評価項目

セキュリティのレベルを、偽造の種類、検知（不正が生じていることの検出、不正の発生箇所を特定）、および検知されたときの対応策の有無の観点から評価する。なお、偽造の種類については以下のように分類する。

支払情報の偽造１（本人）：本来の利用者としての支払情報を偽造して、商店、銀行を欺く。
―― 不正を検知され、特定される場合は「やり逃げ」のみ可能。

支払情報の偽造２（特定）：特定の利用者としての支払情報を偽造して、商店、銀行を欺く。
―― 盗聴等により得た特定の利用者の情報等を利用。

支払情報の偽造３（不特定）：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て、商店、銀行を欺く。

還流情報の偽造＜結託なし＞：商店が売上げ（受取情報）を偽造して、銀行を欺く。
―― 商店は匿名性がない状態で不正を実施。

還流情報の偽造＜結託あり＞：商店が特定の利用者の情報も読み出して利用した上で、売上げ（受取情報）を偽造して、銀行を欺く。

４．考察

4.1 評価結果

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まとめたものを表２に、還流情報の偽造による被害の状況についてまとめたものを表３に示す。

4.2 耐タンパー装置の必要性

攻撃が成功し、かつ対応策も打てないタイプの電子マネーは耐タンパー性のある装置に閉じ込めることが必須である。一方、攻撃の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により、「やり逃げ」しか出来ないタイプの電子マネーは、これが抑止効果となるため、ある程度は安全といえるが、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、そのままでほぼ安全な電子マネーは、耐タンパー性のある機器を必ずしも必要としない。各電子マネーモデルについて耐タンパー機器の必要性についてまとめたものを表4に示す。

なお、特に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らず、すべて想定される被害の程度は同じ（攻撃は成功）であり、暗号技術よりは、耐タンパー性の強化に力を注ぐ方が意味のあることがわかる。

4.3 支払情報の偽造からみた電子マネーの安全性

オンライン型の電子マネーは、暗号技術として公開鍵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。ただし、実際にインプリメントする際は構造がシンプルな分、残高管理型が優位といえる。一方、共通鍵を利用したものは、新たに価値を無尽蔵に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組み合わせることにより、他人の価値を盗むことのみ可能である。なお、電子証書型の場合、共通鍵型と公開鍵型では安全性が高いのはもちろん、匿名性を持たせることができる分、公開鍵型が優れている（表5参照）。

オフライン型の電子マネーは、耐タンパー性のある機器が破られた場合は、程度の差はあれ攻撃が成功する。ただし、電子証書型は不正行為の追跡が可能な分、優れている。また、残高管理型はオープンループにすると安全性が低下するのに対し、電子証書型は安全性自体は変わらず、情報量の増大を気にする必要がなければ、転々流通性を持たせることが合理的となる（表6参照）。なお、残高管理型の電子マネーにおいては、残高ローカルクローズド型は残高併用クローズド型とした方が追加コストのわりに安全性は飛躍的に高まることがわかる。

4.4 還流情報の偽造からみた電子マネーの安全性

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。残高管理型の電子マネーではセンターで残高を管理する場合、一時的に他人の価値を横取りすることが可能であるが、還流時は実名口座を使っているため、結果的に犯人は捕まるので被害は限定される。一方、センターで残高を管理していない場合は攻撃が成功する。この場合、ログ（取引の履歴）も還流させれば安全となるが、それでも他の利用者との結託には弱いことがわかる。

5．おわりに

本稿では、電子マネーの機能とセキュリティ対策に関する様々なバリエーションを悉皆的に評価、検討することによって、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示した。今後は、本稿で得られた結論を利用して、安全な電子マネーを実現するためのセキュリティ対策を検討していくことが課題である。

【参考文献】

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, 1997

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.

中山靖司・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

（残高管理型）　　安全性低い←●△□○→安全性高

暗号技術と偽造の種類		残高=ﾛｰｶﾙ=ｸﾛｰｽﾞﾄﾞ off-line	残高=併用=ｸﾛｰｽﾞﾄﾞ off-line	残高=ｾﾝﾀｰ=ｸﾛｰｽﾞﾄﾞ on-line	残高=ﾛｰｶﾙ-=ｵｰﾌﾟﾝ 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)	●(※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) △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ICカードの特定も可能。(※2)商店がホットリストを持ってチェックし、不正なICカードを受け付けないようにできれば可能。(※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。不正行為者の特定は不可。(※5)センターでA'を取引停止にすることによって、A'の被害は止まる。(※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)第3者を介在することで実質的に攻撃成功と同様の効果。

（電子証書型）　　安全性低い←●△□○→安全性高

暗号技術と偽造の種類		証書=事後=ｸﾛｰｽﾞﾄﾞ	証書=即時=ｸﾛｰｽﾞﾄﾞ	証書=事後=ｵｰﾌﾟﾝ
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。不正行為者あるいは被害者の特定は可。(※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)露見した実名をもとに不正者を追跡。(※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おり盗聴困難であり、盗聴可能なのは使用時のみのため、攻撃が成功する可能性はかなり低いとみられる。

（表2）各方式における安全性－支払情報の偽造（利用者が偽造）

（残高管理型）　　安全性低い←●△□○→安全性高

暗号技術と偽造の種類		残高=ﾛｰｶﾙ=ｸﾛｰｽﾞﾄﾞ off-line	残高=併用=ｸﾛｰｽﾞﾄﾞ off-line	残高=ｾﾝﾀｰ=ｸﾛｰｽﾞﾄﾞ on-line	残高=ﾛｰｶﾙ=ｵｰﾌﾟﾝ 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	－結託の必要なし－	○安全	○安全	－結託の必要なし－
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	－結託の必要なし－	－結託による新たな攻撃方法なし－(※4)	－結託による新たな攻撃方法なし－(※4)	－結託の必要なし－
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	－結託の必要なし－	－結託による新たな攻撃方法なし－(※4)	－結託による新たな攻撃方法なし－(※4)	－結託の必要なし－
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	－結託による新たな攻撃方法なし－(※4)	－結託による新たな攻撃方法なし－(※4)	●攻撃成立 ●検知不可

(※1)すでに取引があり識別 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。還流は実名取引のため、センターのログによって A から誰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）。

（電子証書型）　　安全性低い←●△□○→安全性高

		証書=事後=ｸﾛｰｽﾞﾄﾞ	証書=即時=ｸﾛｰｽﾞﾄﾞ	証書=事後=ｵｰﾌﾟﾝ
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、実際には還流は自口座を利用した実名取引のため、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。
(※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３）各方式における安全性－還流情報の偽造（商店＜実名＞が偽造）

	オフライン	オフライン	オンライン	オフライン
	残高=ﾛｰｶﾙ=ｸﾛｰｽﾞﾄﾞ	残高=併用=ｸﾛｰｽﾞﾄﾞ	残高=ｾﾝﾀｰ=ｸﾛｰｽﾞﾄﾞ	残高=ﾛｰｶﾙ=ｵｰﾌﾟﾝ
共通鍵型	●● ●● ●●	●○△ ●○△ ●○△	○ △○△ △○△	●● ●● ●●
共通鍵型 ＜静的認証あり＞	●● ●● ○	●○△ ●○△ ○	○ △○△ ○	●● ●● ●●
公開鍵型 ＜動的認証あり＞	●● ○ ○	●○△ ○ ○	○ ○ ○	●● ●● ●●

	オフライン	オンライン	オフライン
	証書=事後=ｸﾛｰｽﾞﾄﾞ	証書=即時=ｸﾛｰｽﾞﾄﾞ	証書=事後=ｵｰﾌﾟﾝ
共通鍵型	●○△ ●○△ ●○●	○ △○● ○	●○△ ●○△ ●○●
公開鍵型 ＜静的認証あり＞	△○○ △○● ○	○ ○ ○	△○○ △○● ○
公開鍵型 ＜動的認証あり＞	△○○ ○ ○	○ ○ ○	△○○ ○ ○

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上
耐タンパー機器は必ずしも必要ない

（表４）各方式における耐タンパー機器の必要性

（表の見方）

	被害	検知	抑制
偽造１	○	○	○
偽造２	○	○	○
偽造３	○	○	○

安全性低←●△□○→安全性高

※　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。

	残高=ｾﾝﾀｰ=ｸﾛｰｽﾞﾄﾞ	証書=即時=ｸﾛｰｽﾞﾄﾞ	
共通鍵型	○ △○△ △○△	○ △○● ○	共通鍵型
共通鍵型 ＜静的認証あり＞	○ △○△ ○	プライバシー	
		○ ○ ○	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＞

構造がシンプル

（表５）オンライン型の電子マネー間の安全性の比較

（残高管理型）

	残高=ﾛｰｶﾙ=ｸﾛｰｽﾞﾄﾞ	残高=併用=ｸﾛｰｽﾞﾄﾞ	残高=ﾛｰｶﾙ=ｵｰﾌﾟﾝ
共通鍵型	●● ●● ●●	●○△ ●○△ ●○△	●● ●● ●●
共通鍵型 ＜静的認証あり＞	●● ●● ○	●○△ ●○△ ○	●● ●● ●●
公開鍵型 ＜動的認証あり＞	●● ○ ○	●○△ ○ ○	●● ●● ●●

（電子証書型）

	証書=事後=ｸﾛｰｽﾞﾄﾞ	証書=事後=ｵｰﾌﾟﾝ
共通鍵型	●○△ ●○△ ●○●	●○△ ●○△ ●○●
公開鍵型 ＜静的認証あり＞	△○○ △○● ○	△○○ △○● ○
公開鍵型 ＜動的認証あり＞	△○○ ○ ○	△○○ ○ ○

（表６）オフライン型の電子マネー間の安全性の比較