偽造キャッシュカード問題に関する
スタディグループ最終報告書

～偽造・盗難キャッシュカード被害発生の予防策・
被害拡大の抑止策を中心として～

平成１７年６月２４日

偽造キャッシュカード問題に関するスタディグループ

目　次

平成１７年６月２４日

偽造キャッシュカード問題に関するスタディグループ最終報告書

～偽造・盗難キャッシュカード被害発生の予防策・被害拡大の抑止策を中心として～

Ⅰ．これまでの検討の経過

昨年以降、偽造キャッシュカードを使用した犯罪による被害が急増したことを受け、本年２月２２日、金融庁において「偽造キャッシュカードに関する金融庁の対応について」が公表された。その中では、偽造キャッシュカード被害に関する実態調査の結果が公表されるとともに、その結果を踏まえ、金融機関等に対し、より実効性のある犯罪防止策及び犯罪発生後の対応に関する速やかな検討の要請が行われた。更に、①犯罪防止策、②犯罪発生後の対応のあり方、③被害が発生した場合の預金者への補償のあり方、について検討を行うため、監督局において、法律やシステムの専門家からなる「偽造キャッシュカード問題に関するスタディグループ」（座長：岩原紳作東京大学大学院法学政治学研究科教授）を開催することとされた（注１）。

これを受け、当スタディグループは、２月２２日の第１回会合以降１９回に亘り会合を開催し、検討を行ってきた(注２)。当初の会合においては、まず、喫緊の課題である偽造キャッシュカード被害への補償のあり方について議論を行い、３月３１日に「偽造キャッシュカード問題に関するスタディグループ中間取りまとめ～偽造キャッシュカード被害に対する補償を中心として～」（以下、「第一次中間取りまとめ」）を公表した。盗難キャッシュカードの問題については、第一次中間取りまとめにおいて「（それまでの）議論も踏まえ、更なる検討が必要ではないか。」と位置付けられていたところ、4 月 15 日に改めて金融庁より当スタディグループの検討項目に加えるよう要請を受けるに至った。この要請に対し、当スタディグループでは、集中的な議論を行い、５月１３日に「偽造キャッシュカード問題に関するスタディグループ第二次中間取りまとめ～盗難キャッシュカード被害に対する補償を中心として～」を公表した（注３）。

更に、当スタディグループでは、犯罪防止策、犯罪発生後の対応のあり方等について議論を重ね、検討を行ってきた。本最終報告は、犯罪防止策等を被害発生の予防策・被害拡大の抑止策として整理しつつ、これまで当スタディグループにおいて行われてきた検討の結果を取りまとめたものである。

（注１）偽造キャッシュカード問題に関するスタディグループのメンバーについては、

別添１参照。

（注２）偽造キャッシュカード問題に関するスタディグループの開催実績については、別添２参照。

（注３）「偽造キャッシュカード問題に関するスタディグループ中間取りまとめ～偽造キャッシュカード被害に対する補償を中心として～」（３月３１日公表）については、別添３参照。「偽造キャッシュカード問題に関するスタディグループ第二次中間取りまとめ～盗難キャッシュカード被害に対する補償を中心として～」（５月１３日公表）については、別添４参照。

Ⅱ．我が国におけるＡＴＭシステム及び被害発生の予防策等の現状

（1）我が国ＡＴＭシステムの発展の歴史

昭和 40 年代半ばからＣＤ（現金自動支払機）の運用が開始され、その後、入金や通帳記入が可能なＡＴＭ（現金自動預入支払機）が導入され、平成 16 年 3 月末時点においては、全国の民間金融機関の保有するＣＤ／ＡＴＭ機は、約 11 万台、キャッシュカードの発行枚数（郵便局を除く）は約 3 億 3 千万枚となるに至っている。

ＣＤ／ＡＴＭのオンライン提携については、昭和 50 年代半ばから業態間オンライン提携が開始され、平成 2 年には全国キャッシュサービス（ＭＩＣＳ）を通じて都銀キャッシュサービス（ＢＡＮＣＳ）及び地銀ＣＤ全国ネットサービス（ＡＣＳ）の接続が開始され、平成 3 年にはＭＩＣＳで７業態（都市銀行、地方銀行、第二地方銀行、信用金庫、信用組合、労働金庫、農協系統）相互間の接続が開始された。このようにＡＴＭネットワークは、まずは業態内、次に業態間のネットワークを接続することにより拡張されてきたが、平成 16 年 1 月に、次期システムとして統合ＡＴＭスイッチングサービスが導入され、信用金庫等一部業態を除き、各金融機関が業態センターを介さずに統合ＡＴＭに直接接続する方式が採用された。なお、本年 5 月には統合ＡＴＭの新機能拡充を行ったところであり、今後、ＡＴＭサービスの利便性の向上が期待されているところである。

（2）ＡＴＭシステムに関しこれまでに採られたセキュリティ対策

金融業界においては、ＡＴＭシステムに関するセキュリティ対策として、平成 16 年までに以下のような対策が講じられてきた。本年に入ってからは、偽造キャッシュカード問題が社会問題化する中、1 月に全国銀行協会で申し合わせがなされるなど、全国銀行協会等の金融関係団体や

各金融機関におけるＡＴＭシステムに関するセキュリティ対策は、加速している状況にある。

〔全国銀行協会〕

① カード及び暗証番号の取扱いに関する統一ポスターの作成や暗証番号についての注意喚起等、カードの安全対策の徹底を示達（昭和 61 年）
② カード上の磁気ストライプのゼロ暗証化、暗証番号のホスト照合の申し合わせ（昭和 62 年）
③ 「全銀協ＩＣカード標準仕様」を策定（昭和 63 年）（以降、随時改定）
④ ＩＣキャッシュカード認定制度運営協議会設立（平成 13 年）、認証局開局（平成 14 年）
⑤ 防犯チラシの配布等による顧客に対するキャッシュカードや暗証番号の取扱いに関する注意喚起を実施（平成 15～16 年）
⑥ 偽造キャッシュカードの被害届の提出ルールに関する申し合わせ（平成 16 年）

〔個別金融機関における対応等〕

一部金融機関において以下のサービスを開始。

(ア)ＩＣキャッシュカード（平成 14 年～）
(イ)利用限度額の個別設定サービス（平成 14 年～）
(ウ)生体認証による本人確認（平成 16 年～）
(エ)利用限度額の設定・引下げ
(オ)異常取引検知システム

なお、金融庁は、本年 2 月に偽造キャッシュカードに関する実態調査結果を公表するとともに、金融関係団体に対して、偽造キャッシュカード問題に関する事前予防策及び被害発生後の対応を要請した。その後、当該要請において示された各項目についての金融機関の対応状況に関して、銀行法第 24 条等の規定に基づき、「偽造キャッシュカード犯罪緊急対応方針」が各金融機関から金融庁に提出されたところである（注）。

（注）17 年 4 月末時点における各金融機関のＡＴＭシステムに係るセキュリティ対策の状況については、別添５参照

（3）ＡＴＭシステムに係る基準・標準等

現在、ＡＴＭシステムに関するセキュリティ対策に関して、国内外に様々

な基準・標準等が存在している。国内基準としては、金融情報システムセンター（以下、「ＦＩＳＣ」）、全国銀行協会など金融関係団体が中心となって作成したものやＪＩＳ規格等があり、他方、国際基準としては、ＩＳＯ規格や国際クレジットカードブランドが定める仕様が中心的な役割を果たしている。

なお、我が国の金融分野における標準化の特徴として、ＩＣカード仕様等を除き、国際標準に準拠していないとの指摘がなされた。その理由としては、我が国において、磁気ストライプ等が海外に先駆けて導入され、国際標準への採用を働きかけたものの、不成功に終わった経緯などが挙げられるが、他方で、言語・慣習等の違いから、海外と整合させるために国際標準に準拠するという必要性が希薄だったため、ＩＣカード仕様等を除き、国際標準を意識することが少なかったとの指摘があった。

〔国内の基準〕

① 金融機関等コンピュータシステムの安全対策基準（以下、「安全対策基準」）（ＦＩＳＣ）
② 全国銀行協会ＩＣキャッシュカード標準仕様（全国銀行協会）
③ 金融機関の防犯基準（警察庁）
④ ＪＩＳ　Ｘ６３０１（識別カード）

〔国際的な基準〕

ＩＳＯ（国際標準化機構）規格
（例）ＩＳＯ９５６４（暗証番号管理とセキュリティ）（ＴＣ６８）
ＩＳＯ/ＩＥＣ７８１３（金融取引カード）（ＪＴＣ1/ＳＣ１７）
ＩＳＯ/ＩＥＣ７８１６（端子付きＩＣカード）（同上）

このうち、ＦＩＳＣ安全対策基準は、1985 年に初版が公表され、その後、継続的に見直しを行っている。金融庁の検査マニュアルにより、システムリスク管理態勢の確認検査において、管理態勢に問題が見られ、さらに深く業務の具体的検証をすることが必要と認められる場合には、検査官は、安全対策基準に基づきこれを行うものとされていることから、安全対策基準には一定の規範性が付与されている。なお、安全対策基準はＦＩＳＣ内に設置された、学識経験者、預金取扱金融機関、保険会社、証券会社、クレジットカード会社及びコンピュータメーカー等の専門的知識を有する者から構成される安全対策専門委員会、及びその下部組織である検討部会において審議・作成されている。

また、金融サービスに利用される情報セキュリティ技術に関するＩＳＯの

各種国際標準については、ＩＳＯ/ＴＣ６８（金融専門委員会）において検討されている。その審議は、同委員会のメンバー国の民間金融機関、中央銀行、銀行協会などが参加して行われており、日本国内における国内審議は、日本銀行が事務局を務めるＩＳＯ/ＴＣ６８国内委員会が担当している。

Ⅲ．海外の状況

（1）諸外国におけるペイメントカード（キャッシュカードも含む）の不正利用の現状

① 諸外国でペイメントカードの不正利用の原因・形態として認識されているものには、カードの偽造・紛失・盗難・ＣＮＰ(Card Not Present：電話取引などカードが提示されない取引において行われるＩＤや口座番号の不正利用)などがある。欧州全体では、ペイメントカード全体の不正利用率は、利用限度額の設定や、データの暗号化、ＩＣカード化など、様々な方策が各金融機関により採られてきたこともあり、全体として年々減少する傾向にある。

しかし、インフラの共通化の進行によりカードの外国での利用が可能となったことにより、特に外国において盗難・偽造されたカードをデビットカードとして利用する犯罪が増加してきている。被害総額はむしろ上昇傾向にあり、現在、ＥＵ全体として、この数年の内にＩＣカード化を進めようとしているところである。

② また、イギリス等ＩＣカード化の途上にある地域や、米国等ＩＣカード化がなされていない地域においても、引出限度額の引下げや口座のモニタリング等の効果により、キャッシュカード関連の被害は全体として減少傾向にある。他方、電子商取引の拡大との関連で、フィッシング詐欺やＩＤ窃盗による被害が増えてきており、諸外国において問題になってきている。

（2）諸外国の金融機関等が採っている予防策

① 欧米の主要な金融機関では、事前予防策を考える上で、基本的に、①金融機関としての円滑な取引を顧客に保証するのが金融機関の役割であり、②そのサービスを提供するにあたって、リスクが存在する場合、利用者へのリスクの説明や責任分担ルールの開示を行うことで、金融機関として対応可能な限界と顧客がなすべき対策を理解してもらう、という共通した考え方が存在する。

② 具体的な方策としては、リスクに関する利用者教育や口座限度額の

引下げ（注１）などがあるが、他に、利用者向けの 24 時間オープンの電話窓口の設置、カード交換・有効期限の設定、ＩＣカードの導入、スキミング防止のためのＡＴＭの改良、異常取引検知システムの導入(もしくは高度化)などがあげられる。また、ステートメント方式（毎月の利用明細書を送付する方式）を採用していることが、結果として被害の早期発見に役立っているとも考えられる。なお、業務・規模により程度の差はあるが、ＩＳＯ等様々な国際基準に準拠できるよう、ＡＴＭ関連だけではなく、情報セキュリティ全体の第三者による監査が行なわれ、システムの安全性レベルの維持が図られている。

③ また、主要先進国では、暗証番号をデータ送信する際には、３ＤＥＳ暗号（注２）が広く利用され、欧米における実質的な標準暗号となっている。さらに、各金融機関の情報セキュリティマネジメントの安全性維持と信頼性の高い技術の普及のためにＩＳＯ/ＴＣ６８が策定した様々な国際標準が各金融機関で尊重されており、キャッシュカード取引をはじめ、その他の金融取引においても広く活用されている。（また、広く情報セキュリティマネジメントシステムの実施基準と仕様を規定したＩＳＯ/ＩＥＣ規格（例えば、ＩＳＯ/ＩＥＣ１７７９９）やＢＳ７７９９、ＩＳＭＳなどもシステム構築に活用されている。）

（注１）もともと欧米諸国におけるＡＴＭ利用限度額は、我が国に比べて低額である。（1 日あたりの利用限度額:金融機関によりまちまちであるが､米 1000 ドル程度、英 400～500 ポンド、独・仏 500 ユーロ程度、日 200～500 万円といった例が見受けられる。）

（注２）3DES：共通鍵型の暗号方式である「DES」(Data Encryption Standard：1977 年に米国商務省標準局(National Bureau of Standards(NBS))（現米国商務省標準技術局(National Institute of Standards and Technology (NIST))）によって連邦情報処理基準（Federal Information Processing Standards (FIPS)）に採用された共通鍵暗号化アルゴリズム。暗号の強度が低下したとの認識から、2005 年 5 月に標準暗号としての認定を廃止。）を三重に適用するようにした方式のこと（1998 年に米国内で標準暗号に認定。）。コンピュータの性能向上に伴って DES 暗号を解読される危険性が高まったため、異なる暗号鍵を用いて同じ方式を三重にかけることにより、強度を高めた。

Ⅳ．被害発生の予防策等に関する基本的な考え方

（預金者保護）

○ 金融機関に期待されるサービスの最たるものは、預金者の財産を安全に管理すること。ＡＴＭシステムの運用にあたっては、預金者保護のため、一定レベル以上のセキュリティが確保されるべきである。

○ システム・セキュリティ対策は金融機関に一方的に求めるものではなく、預金者のカード等の管理意識の向上、モラルハザード防止の観点も踏まえ、検討されるべきである。なお、預金者の意識向上を求めるにあたっては、ＡＴＭや金融ネットワークの仕組みについて、消費者教育を行い、金融取引リテラシーの向上を図ることが必要である。

（金融機関の被害への対応）

○ 偽造・盗難キャッシュカード被害の預金者への補償がルール化されたことにより、金融機関が一定の損失負担を行うこととなるが、そのことにより、金融機関は、被害を極小化しようとするインセンティブを持つこととなる。

○ 金融機関が行う被害極小化の方策には、様々なものがあるが、その中には利用者利便とのトレードオフの関係となる方策も含まれるため、利用者サイドでの安全性、利便性の選好が重要になる。

○ 安全性と利用者利便のトレードオフに関して、安全性を重視し被害を最小限に食い止める観点からは、顧客利便性や金融機関のコスト削減に重きを置きがちであったこれまでのビジネスモデルの変更が求められるのではないか。新たなビジネスモデルにおける安全性と利便性のバランスをどのように図るかについては、預金者側の理解・協力を十分に得つつ、広く社会的費用を最小化するとの観点から検討する必要がある。

○ 金融機関内においても、システム関係以外の職員等は、システム・セキュリティに関する知識が十分とはいえないのではないか。預金者の金融取引リテラシーの向上を求める以上、金融機関の職員等についても、システム・セキュリティに関する知識の底上げを図るべきである。

○ なお、システム・セキュリティ対策を講ずるにあたっては、個人情報保護の観点からの配慮も必要である。

（金融ビジネス）

○ 金融機関は巨大な情報システムを管理する装置産業として、技術進歩に伴うシステム・レベルの高度化とセキュリティ・レベルの向上を絶えず行っていく責務がある。

○ その際、本人認証を含むシステム・セキュリティ対策のレベルは、一律に高いものを求めるのではなく、取引のリスクに応じたものであるべきである。仮に現在のシステム・セキュリティ対策が不十分との評価であれば、取引限度額を引き下げる等により取引のリスクを下げるべきであり、他方、高リスクの高額取引をＡＴＭネットワーク上行うのであれば、それに見合ったシステム・セキュリティ対策を講ずるべきである。
○ 金融機関はセキュリティ・レベル向上等の責務を前提にしても成り立ちうるビジネスモデルを模索していく必要がある。
○ 同時に、そうした金融機関の対応が、銀行法等により金融機関に対して求められる「業務の健全かつ適切な運営」として、行政上の評価に耐えうる必要がある。

（システム・セキュリティ・レベルを向上・維持するための環境整備）
○ 預金者の信頼を確保し金融システムの安定に資するため、システム・セキュリティ・レベルを向上させ、一定のレベルを維持するための環境整備を図るべきである。具体的には、システム全般から個々の機能や技術に亘る仕様等の標準・評価基準を整備確立し、そうした標準等に基づいて、システム機器が開発・製造・調達されているか、システムが適正に実装・運用されているかについて、監査し評価する仕組みを作るべきである。
○ 金融機関は、そうした標準等を利用して、適切なセキュリティ対策を採っていることを公開可能な範囲で対外的に明らかにすべきである。
○ 更に、システム全体のセキュリティを統括し、責任をもって対応できる主体を構築すべきである。また、システムの新たな問題点が発見された場合に、その情報を共有する枠組みを構築すべきである。
○ 技術的に新たな対策を導入する場合には、十分な安全性等の評価が必要である。また、既存の技術も含め将来新たな問題点が顕在化した場合に対応できる態勢整備を図るべきである。
○ 新技術に完全に移行するまでは、旧技術との併存状態が続く。その間、一定のセキュリティ水準を維持しつつ、混乱なく新技術に転換していく道筋を確保していくことが必要である。
○ なお、ドイツにおいては、金融業界が信頼性の高いシステム・セキュリティ対策を講じたことが、裁判実務に影響を与えている。我が国においても、金融業界が高いシステム・セキュリティを維持することにより、少なくとも補償ルールの適用における金融機関の無過失の立証がより容易になるなどの効果もあるのではないか。

（システム・ネットワーク保護）

○ 各金融機関のＡＴＭシステムは、統合ＡＴＭ等を通じて相互に接続することで、社会インフラとしての役割も担っている。仮に脆弱なＡＴＭシステムを放置する金融機関が存在した場合、システム・ネットワーク及び他の金融機関に影響を及ぼすことが懸念される。したがって、各金融機関がＡＴＭネットワークに参加するためには、一定レベルのセキュリティ確保が求められる。

（犯罪対応の徹底）

○ 最も悪いのは犯罪者。犯罪予防の徹底とともに犯人の早期検挙が強く求められる。そのため、金融機関による防犯基準の誠実な履行とともに、（被害の偽装ケースも含む）犯人検挙のため、捜査機関のイニシアティブの下、預金者、金融機関、金融監督当局と捜査機関との徹底した協力体制が構築されるべきである。その際には、いかにすれば、信頼性があり、捜査価値の高い資料を集積できるかについても検討されるべきである。

Ⅴ．具体的な被害発生の予防策等

（１）顧客サービスに直結する事項

〔所持認証　―　キャッシュカード〕

○ 現在多くの金融機関は、ＩＣカードの導入（及びＩＣカード対応ＡＴＭの拡充）を実施ないし検討している。これについては、キャッシュカードのセキュリティ・レベルを引き上げ、偽造を防止する観点から、基本的に望ましい方向であると考えられる。特に、金融機関の経営判断により、ＡＴＭシステムにおいてリスクの高い高額取引を行っていくのであれば、ＩＣカード化は必須である。また、ＩＣカードの導入を決定した場合には、利用者利便の確保の観点から、ＩＣカード対応ＡＴＭの出来るだけ早期の普及に努めることが望ましい。

○ 金融機関によっては、その経営判断において、ＩＣカードへの切換えを行わず磁気カードを継続するところもありうると考えられる。また、ＩＣカードへの転換を段階的に進める場合、カード上に磁気ストライプを併存させることが多いと考えられる。こうした場合には、以下の事項を参考に、各金融機関のＩＣカード化への切換戦略に応じて、磁気カードの脆弱性（スキミングの可能性）を補強する何らかの方策を実施することが必要である。

・ カードへの有効期限の設定。それにより、期限ごとのセキュリティのグ

レードアップやカード送付の際の本人確認が可能となる（有効期限経過後のカード保有者を窓口に誘導することとすれば、住所が不明な顧客についても本人確認が可能）。

・ キャッシュカード交付の際、カード保持にかかるリスク（特にスキミングのリスク）や預金者としての注意義務を、（事例等を交えて）より具体的・明示的に説明。

・ 磁気ストライプ内の情報保存状況についての再点検（ゼロ暗証化していないカードの探索等）。

・ 磁気ストライプに記録する偽造判別用コードの強度を引き上げることを検討。

・ 少なくともホワイトカードについては、ＡＴＭへのカード挿入時に判別、排除できる機能の導入。

○ なお、現在、全国銀行協会において、ＩＣキャッシュカードの仕様を制定・管理しているが、磁気カードについても、そのセキュリティのレベルを確保するために、いずれかの主体が中心となって、脆弱性を補強するための方策に関する情報交換を行うことが望ましい。

〔記憶認証　―　暗証〕

○ 金融機関側からの暗証の漏洩がないことを担保する暗証管理体制の更なる徹底を図ることが必要である（例えば、暗証を書類に記入せずに直接ホストコンピュータに登録し、その後も金融機関従業員等の関係者は一切アクセスできない仕組みとすることやデータベース等における暗証の暗号化を徹底する等）。

○ 金融機関領域内の覗き見、盗撮の完全排除を徹底することが必要である（例えば、間仕切りの再点検、整理列の再点検、覗き見防止フィルム、手元覆いカバー、後方確認用ミラーの装填等）。

○ 顧客領域で暗証が盗取されないよう、具体的・明示的な預金者への働きかけを徹底する必要がある（例えば、発生事件などを個別メールで知らせる等）。

○ ４桁番号に付加した第二の記憶認証（例えば、数字以外に「英字」、「かな」、「カナ」の使用）の導入・検討は、暗証機能の強化を図る観点から、基本的に望ましいと考えられる。また、ＩＣカード導入に伴い、ＩＣカードを利用可能状態にするための暗証を（ＡＴＭからの引出し用の暗証とは別に）導入するなど、第二の記憶認証のあり方について幅広い検討が可能ではないか。なお、第二の記憶認証を導入する場合、金融機関ごとに異なる方式の暗証を導入すれば、利用者利便が損なわれることとなるため、互換性確保の観点からの検討が必要と考えられる。

○　ただし、記憶の容易さ、高齢者等への配慮を勘案すれば、4 桁の暗証を記憶認証として維持することは経営判断としてありうると考えられる。その際、現行の 4 桁の暗証番号を数字以外の「かな」等に置き換えることは、金融システム及びネットワークの抜本的な改変となることから、当面の方策としては困難ではないか。4 桁の暗証番号を維持した場合には、顧客の対応可能性も考慮しつつ、例えば、以下のような方策を併せ検討すべきである。

・ テンキーシャッフル機能の導入。
・ 生年月日等を入力した場合にカードを受け付けない機能の導入。
・ カードに有効期限を付し、切換えの際に、以前と同じ暗証番号を受け付けない機能の導入。（但し、この点については、預金者、特に高齢者にとっては様々な暗証番号を記憶することが困難な面があることに留意する必要があるとの意見があった。）
・ 生年月日等他人が容易に類推可能な番号を暗証に使うことのリスクを、状況によっては預金者側の過失が認定されうることも含めてより具体的・明示的に預金者に説明。

〔生体認証〕

○　生体認証は第三の認証の仕組みとして、偽造及び盗難キャッシュカード被害ならびに被害偽装を防止する上で注目すべき。

○　ただ、生体認証は、センシティブ情報の保護、一部の疾患の患者には利用が困難であるといった基本的な問題があることに加え、技術として成熟途上にあり、認証精度の評価、装置のセキュリティ評価、運用基準等に関する検討が更に必要である。

○　生体認証対応のキャッシュカードは、生体認証技術、ＩＣカード技術、暗号技術の組み合わせであり、その標準化と互換性の確保についてはある程度の時間が必要と考えられ、監督官庁は、技術の開発、進展を注意深く見守るべきものではないか。なお、生体認証が幅広く利用されるほどに、生体認証情報の偽造や、不正な詐取を行なおうとする犯罪者の動機付けも高くなる。こうしたことも十分配慮の上で生体認証に関するセキュリティ基準等を検討する必要がある。

〔利用限度額の引下げ〕

○　1 日あたりのＡＴＭ引出限度額又は振込限度額が、依然、無制限である場合には、少なくとも個人顧客については、速やかに一定額まで限度額を引き下げる必要がある。また、既に 1 日あたりの利用限度額が設定されている場合でも、被害の拡大抑止の必要性と利用者ニーズ等を総合的に勘案して、妥当と考えられる水準まで引下げを行うことが望ましい。

○　利用限度額の設定は、基本的には金融機関相互の競争の中で各金融機関が経営判断により決定すべき問題であり、一律に決まるものではないが、自らのシステム・セキュリティ・レベルに応じたものにすべきと考えられる。仮に顧客利便性を抑えて、安全性に重きを置いた場合、以下の点を踏まえると、一応の参考値として一日あたり 50 万円という水準がありうるのではないか。

・ 複数の金融機関からの聞き取りによれば、一日の利用額について、顧客の 9 割以上は 50 万円以下であった。

・ 一部金融機関において、磁気カードを用いた取引について 1 日あたり 50 万円に引き下げる予定。

○　1 日あたりの利用限度額に加え、例えば、一週間、一ヶ月あたりの利用限度額も設定することが望ましい。

○　利用限度額の引下げに加え、利用可能なＡＴＭの制限、機能の制限（例えば、預金担保借入機能の制限）など、カードの利便性全般について、顧客が選択できるようにすることが望ましい。

〔顧客対応〕

○　少なくともＡＴＭ稼働時間中は有人の顧客対応窓口を設けることとし、その旨を顧客に対して周知すべき。約款において、顧客に対して速やかな届出を求めるのであれば、仮に有人窓口が稼動していない時間帯においても、何らかの方法により顧客の届出を受け付け、ＡＴＭ稼動開始前までに口座の利用を停止するなどの措置が必要である。更に顧客のパニックを防ぐ観点からは、24 時間の有人対応が望ましい。

○　偽造カードによる被害が発生した際の金融機関の初期対応の悪さが指摘されていることに鑑み、金融機関の窓口対応の再教育が必要である。

○　スキミングの可能性、暗証及びカードの盗取の危険性、類推されやすい暗証の使用の危険性、被害拡大の可能性（ＡＴＭ利用限度額等）、不必要に多くのカードを保有することによる管理上の問題など、キャッシュカード利用に伴うリスクに関し、定期的なお知らせやダイレクトメール、電子メールの活用等により、これまで以上に具体的、個別的、継続的な説明を行うことが必要である。なお、ダイレクトメール等による説明があれば、それにより、仮にカードの利用期間中に新機能が導入された場合に、預金者の当該機能の利用意思を確認することがより容易になるのではないか。

　また、現時点においてリスクが想定されていない場合であっても、将来にわたって完全な技術というものが存在しない以上、一定の注意を預金者に対して呼びかけることが望ましい。

○　定期的な残高確認を行うよう、預金者に対して働きかけることに加え、例

えば、長期間、通帳に記帳せずに利用している場合、ＡＴＭでの取引を一時停止して、預金者を窓口に誘導するなどの方策をとれば、預金者は、自己の口座の取引の推移について、明確に認識するよう努めるのではないか。

○　自己の口座からの引出しについて、預金者が明確に認識するためには、通帳方式よりステートメント方式のほうが望ましいとの考え方もあり、預金者の選択によりステートメント方式に移行することも考えられるのではないか。仮にステートメント方式に移行した場合、顧客への通知が定期的に行えることから、上述の顧客への個別的な説明がより容易になるとの効果もあると考えられる。

○　金融機関は、システム・セキュリティに関する情報を十分に公開するとともに、本問題に関する現実の被害状況や問題点の所在について、積極的に情報開示すべきである。こうした情報公開に基づき、顧客対応窓口等に対して、金融機関利用者側から意見が寄せられた場合には、関係機関は、そのような声を踏まえて、安全対策基準やシステム・セキュリティ対策を検討することが求められる。

○　システム・セキュリティ・レベルを高度化するためにはコストがかかるが、預金を安全に管理するための金融機関の責任を明らかにし、顧客への十分な説明を行った上で、顧客に一定の負担を求めることは許容されるのではないか。

（２）主として金融機関サイドで取り組む事項

〔システム・セキュリティ対策に係る枠組み〕

○　現状において、金融機関が自らのシステム・セキュリティ・レベルを対外的に明らかにするためには、ＦＩＳＣの安全対策基準や第三者の評価を経た暗号技術等を基に、第三者によるシステム監査を行うことなどが考えられる。

○　システム・セキュリティ対策について、標準・評価基準を整備し、システム全般から個々の機能や技術に亘る仕様等が当該標準等を満たしているか、システムが適正に運用されているか等について、監査・評価する仕組みのあり方を検討すべきである。その場合、ＦＩＳＣの安全対策基準を中心に金融業界内外で既に行われている取組みも踏まえた検討を行い、必要に応じて標準等を整備していくことが必要ではないか。そのための検討の場として、金融関係団体、ＦＩＳＣ、統合ＡＴＭ利用者組織、金融庁、日本銀行などからなる検討会を設置すべきである。なお、同検討会においては、本スタディグループにおける指摘事項も含め、金融機関におけるシステム・セキュリティ対策全般についてのフォローアップもあわせて行うべきではないか。

○　現在、ＦＩＳＣにおいて、事故・犯罪発生状況の把握及び分析がなされている。例えば、このようなノウハウも活用し、システムの新たな問題点が発見された場合に、行政当局も含め、関係者がその情報を共有し、システム・セキュリティ・レベルの補強を図る必要がある。

○　金融業界におけるシステム・セキュリティ対策に関するノウハウの蓄積を図り、セキュリティ・レベルの向上を図るため、金融機関間における情報交換の場を設けることが望ましい。このことは、システム・セキュリティ対策に強い人材の育成にも資するのではないか。

○　クレジットカード業界においては、警察庁などの関係省庁との連携の場である全国クレジットカード犯罪対策連絡協議会が設置され、カード犯罪対策を推進している。キャッシュカード犯罪についても、警察庁と金融関係団体等との定期的な情報交換や対策の検討、対策の取組状況の点検を行うための場を設ける必要がある。

〔防犯基準・防犯対策等〕

○　現行の「防犯基準」は、主として銀行強盗を念頭において作成されているが、社会情勢の変化に合わせて、上述のＩＣカード化、利用限度額の見直し等の金融業界における取組みの進捗も考慮しつつ、以下のような項目も含め、偽造・盗難キャッシュカード犯罪やそれに伴う被害の偽装にも対応できるようにすべきである。

- 覗き見や盗撮等による暗証漏洩を防止するための措置
- 防犯ビデオの設置方法、保存期間、画質等
- ジャーナルの方式、保存期間等
- スキミング装置の設置を防止するための措置

○　コンビニＡＴＭにおける防犯対策に関し、例えば、不正引出しが疑われる場合にコンビニエンスストアの店員が警報を発する仕組みを導入するなど、設置金融機関とコンビニエンスストア側とのＡＴＭの管理委託契約を見直すことが必要である。

○　無人店舗ＡＴＭが破壊された際の取引記録情報の保護対策を含め、店舗外ＡＴＭにおけるセキュリティ対策について見直すことが必要である。

○　ＦＩＳＣの安全対策基準は、金融庁検査において規範性を有していることにも鑑み、環境変化や技術進歩等に対応し、随時見直されているところであり、今後、本スタディグループにおいて示された観点等も踏まえ、十分な事項が盛り込まれているかについて、見直す必要がある。

○　真正でないカードをＡＴＭで利用した場合は、カードをＡＴＭに取り込む機能を導入するなど、ＡＴＭの防犯機能の向上を図ることが望ましい。

〔被害の早期発見〕

○　異常取引を検知できるオペレーション上の仕組みを早期に確立し、被害額を抑制することが求められる。これについては、商品購入との関連付けが可能なクレジットカードに比べ、キャッシュカードシステムにおける異常取引検知は難しいとの意見はあるものの、特に高額取引を引き続き行うのであれば、必要なノウハウの集積を図った上で、リアルタイムの検知システムの導入が必須と考えるべき。

○　オンラインの異常取引検知機能により、異常取引と疑われる取引が検知された場合には、当該取引を一時停止した上で、本人確認を行うことにより、不正取引の排除を目指すことが望ましい。

○　預金者による被害の早期発見を可能とする仕組み（電子メールによる個別取引の通知など）を検討することが望ましい。

〔暗号化〕

○　個人情報保護法の関連で、金融機関は、伝送データの漏洩防止を含む、個人データの保護策を講ずることとされており、これを受け、ＦＩＳＣの安全対策基準においても、個人データを伝送する場合には、暗号化等の対策が必要とされている。個人情報保護の観点に加え、偽造・盗難キャッシュカード問題の観点からも、各金融機関においては、ＡＴＭとホストコンピュータ間の電文の暗号化に関する検討を進めるべきである。

○　ＡＴＭ、ホストコンピュータを結ぶ専用線の使用に加え、暗号化が必要ではないか。少なくとも国際的に活動する金融機関や高額取引を引き続きＡＴＭシステムにおいて行う金融機関については、一定のセキュリティ評価を行った上で、暗号分野の国際標準を踏まえた安全対策（周辺機器、運用基準等を含む）を行うことが望ましい。現状においても、第三者による客観的な評価を受けている暗号方式を用いることにより、一定の強度を有する暗号化を行っている旨を対外的に明らかにすることができるのではないか。

○　国際的な業務展開を行っている金融機関については、国際的なセキュリティトレンドに沿った対策を講ずるように努めることが望ましい。

〔被害の偽装対策〕

○　被害の偽装を防止するため、

・　偽造・盗難補償の実績について、金融機関間で情報交換する仕組みを、個人情報保護の観点に留意しつつ、構築することが必要であると考えられる。その際、保険における不正請求等防止制度が参考になるのではないか。

・ 被害の偽装を疑う合理的な根拠がある場合、預金者による警察への被害届の内容について、金融機関が警察に照会できる仕組みを構築するなど、被害偽装防止策について、警察・金融機関間の具体的協力関係の速やかな検討を進める必要がある。

○ 利用限度額の引上げを顧客が選択した上で偽装犯罪が行われることも考えられることから、そうした場合については、被害に至った原因・状況、取引の過去の履歴等について、金融機関による調査は厳格に行われることが望ましい。

○ 真正カード券面に細工をして、偽造カードに見せかけるといった操作も今後考えられうることを念頭に、金融機関は被害の状況について慎重な調査を行うことが望ましい。

（３）監督サイドで取り組む事項

○ 金融機関におけるシステム・セキュリティ対策については、監督指針において明確に位置付けるべきである。

○ 統合ＡＴＭや共同システムなど、金融機関外に存在するシステムで、現在直接に金融庁の検査・監督権限が及んでいないものについて、今後、どのように対応していくべきか、検討する必要がある。

○ カードや暗証の管理について、ホームページを利用するなどにより、金融庁・警察庁は共同で直接の呼びかけを行うべきである。

Ⅵ. 終わりに

金融機関のシステムやネットワークを巡っては、その技術が日進月歩である一方で、犯罪技術についても常に巧妙化が進んでいる状況にある。このような中で、金融機関は、随時、技術の動向を注視し、必要なシステム・セキュリティ対策を講じていく必要がある。

そのためには、まずは各金融機関において、ＡＴＭシステム全般のセキュリティ対策を最優先の経営課題の一つとして位置付け、真剣に取り組む態勢の整備が必要となる。金融業界全体としても、標準・評価基準の整備、各種仕様やシステムの運用について、監査・評価する仕組みを検討し、構築していくことにより、個別の金融機関がより効果的、効率的な対策を講じやすくする環境整備を行うことが望まれる。また、システム・セキュリティ対策は金融機関に一方的に求めるものではなく、預金者のカード等の管理意識の向上等も重要な課題であることは言うまでもない。より安全なＡＴＭシステム

を実現するためには、金融機関、金融関係団体、預金者、行政当局が相互に協力して対応することが望まれる。

なお、本スタディグループは、ＡＴＭシステムに関わる問題を中心に検討してきたが、窓口における預金取引（盗難通帳の問題を含む）、インターネットバンキング、デビットカードの諸問題についても注視していく必要があるとの意見が出された。その際、

① 窓口における預金取引については、現行の本人確認の方式は、印鑑による認証を基本とする我が国の商慣習にも関わる重大な問題であり、その検討にあたっては窓口での本人確認手続き等の実務の対応及び利用者利便への影響を考慮する必要があること

② インターネットバンキングについては、利用される端末が金融機関の管理下にないこと、また、電子商取引一般との整合性について考慮する必要があること

③ デビットカードについては、暗証番号とカードの所持によりオンラインで認証、取引の決済を行っており、キャッシュカード取引に類似するが、他方、商品購入を行う必要上、利用限度額がキャッシュカードの場合に比べて高額となる可能性もあること

など、今後の預金取引、ひいては今後の金融業務のあるべき姿に関連する幅広い観点からの慎重な検討が必要であるとの指摘があった。更には、金融取引一般に関する統一的な法整備の問題についても、今後考えていくべきとの意見もあった。

これらについては、将来的に各方面で議論されることが期待されるが、その場合、金融関係団体及び各金融機関によって主体的かつリーダーシップをとった検討がなされることが期待されるものである。

（以上）

（別添１）

偽造キャッシュカード問題に関するスタディグループ　メンバー

座　　長	岩原　紳作	東京大学大学院法学政治学研究科教授
メンバー	川地　宏行	専修大学法学部教授
	中尾　誠	㈱三井住友銀行執行役員事務統括部長 （第 1 回～第 9 回）
	平田　淳	㈱みずほ銀行事務統括部長 （第 10 回～第 19 回）
	姫野　和弘	警察庁生活安全局生活安全企画課都市防犯対策官
	日和佐 信子	雪印乳業㈱社外取締役、前全国消費者団体連絡会事務局長
	松本　貞夫	明治大学法科大学院教授
	松本　勉	横浜国立大学大学院環境情報研究院教授
	松本　恒雄	一橋大学大学院法学研究科教授
	松本　泰	セコム㈱ＩＳ研究所主席研究員
オブザーバー	米谷　達哉	日本銀行金融市場局決済・市場インフラ企画担当総括参事役 （第 1 回～第 6 回、第 11 回～第 14 回、第 19 回）
	岩下　直行	日本銀行金融研究所情報技術研究センター長 （第 7 回～第 10 回、第 15 回～第 18 回）
	吉田　徹	法務省民事局参事官（第 1 回～第 6 回）
	筒井　健夫	法務省民事局参事官（第 7 回～第 19 回）
	郡山　信	(財)金融情報システムセンター監査安全部長 （第 1 回、第 2 回）
	久木田 弘好	(財)金融情報システムセンター監査安全部主任研究員 （第 3 回～第 19 回）
	喜入　博	金融庁情報化統括責任者（ＣＩＯ）補佐官
	杉浦　宣彦	金融庁金融研究研修センター研究官
事 務 局	金融庁監督局	

（別添2）

偽造キャッシュカード問題に関するスタディグループ　開催実績

第1回　平成17年
2月22日(火)
・岩原座長より、検討項目（座長メモ）について説明
・金融庁より、「偽造キャッシュカードに関する金融庁の対応について」（平成17年2月22日公表）について説明

第2回　2月25日(金)
・柳田邦男氏より、偽造キャッシュカード犯罪及び被害の問題点について説明
・中尾委員より、全銀協の偽造キャッシュカード問題への取組みについて説明

第3回　3月4日(金)
・川地委員より、キャッシュカードの不正使用をめぐるドイツの法状況について説明
・岩原座長より、偽造その他無権限キャッシュカード等取引に関する英米仏等の法制について説明
・金融庁より、民法第478条とATM引出しの適用事例等について説明

第4回　3月11日(金)
・三井住友カード㈱より、クレジットカード業界における偽造被害への取組みについて説明
・松本貞夫委員より、「カード規定試案」の制定経緯等について説明
・金融庁より、金融制度調査会エレクトロバンキング専門委員会における議論について説明

第5回　3月18日(金)
・杉浦ｵﾌﾞｻﾞｰﾊﾞｰより、海外調査報告（預金者への補償のあり方と偽造予防策）について説明
・中間取りまとめに向けた討議

第6回　3月25日(金)
・中間取りまとめに向けた討議

（ 3月31日(木)　中間取りまとめ公表 ）

第7回　4月1日(金)
・全銀協より、キャッシュカード取引について説明
・各金融関係団体（地銀協、全信協等）より、偽造キャッシュカード問題への取組みについて説明

第8回　4月8日(金)
・中尾委員より、「カード規定試案」の改定案について説明
・姫野委員より、金融機関の防犯基準について説明

第9回　4月15日(金)
・岩下ｵﾌﾞｻﾞｰﾊﾞｰより、偽造キャッシュカード問題の現状とその対策について説明
・松本勉委員より、金融取引における生体認証について説明
・松本泰委員より、偽造キャッシュカード問題と認証システムの考察について説明

第10回　４月２２日(金)　・（財）金融情報システムセンターより、偽造キャッシュカード対策強化のための「金融機関等コンピュータシステムの安全対策基準」の改訂について説明
・金融庁より、盗難キャッシュカードの問題に関する論点メモ等について説明

第11回　４月２６日(火)　・姫野委員より、カードの窃盗被害の状況とカード使用犯罪について説明
・平田委員より、盗難キャッシュカード被害の状況等について説明
・金融庁より、盗難キャッシュカード等に係る判例の概要について説明

第12回　４月２８日(木)　・金融庁より、損害保険におけるモラルハザードの防止例について説明
・金融庁より、過失相殺が認められた判例の概要について説明
・盗難キャッシュカード被害に対する補償のあり方について討議

第13回　５月１０日(火)　・第二次中間取りまとめに向けた討議

第14回　５月１１日(水)　・第二次中間取りまとめに向けた討議

（ ５月１３日(金)　第二次中間取りまとめ公表 ）

第15回　５月１９日（木）・（社）電子情報技術産業協会金融端末専門委員会より、ATMにおけるセキュリティ対策について説明
・被害の予防策・被害拡大の抑止策について自由討議

第16回　５月２６日（木）・シティバンク、エヌ･エイより、シティバンクのフロード防止策について説明
・杉浦ｵﾌﾞｻﾞｰﾊﾞｰより、海外調査報告（偽造・盗難等に対する事前予防策）について説明

第17回　６月１日（水）　・被害の予防策・被害拡大の抑止策に関する基本的な考え方について討議
・㈱アイワイバンク銀行より、アイワイバンク銀行における偽造カード対応について説明

第18回　６月１０日（金）・岩下ｵﾌﾞｻﾞｰﾊﾞｰより、金融業務における情報セキュリティ技術の国際標準化について説明
・最終取りまとめに向けた討議

第19回　６月１６日（木）・最終取りまとめに向けた討議

（ ６月２４日(金)　最終報告書公表 ）

（別添３）

平成17年3月31日

偽造キャッシュカード問題に関するスタディグループ中間取りまとめ
～偽造キャッシュカード被害に対する補償を中心として～

１．偽造キャッシュカード被害に関する補償の現状及び問題点

（1） 現行約款の運用

- 金融機関は、ATMの操作の際に、「電磁的記録によって・・・カードを当行が交付したものとして処理」し、「入力された暗証と届出の暗証との一致を確認」して預金の払戻しをすれば免責（全国銀行協会カード規定［試案］第10条第2項本文）。
- 金融機関は、払戻しが偽造キャッシュカードによるものであり、「カードおよび暗証の管理について預金者の責に帰すべき事由がなかったことを確認できた場合」には「このかぎりではない」としている（全国銀行協会カード規定［試案］第10条第2項但書）が、その確認が困難であるため、実際には預金者が補償を受けられないケースが多いとの批判。

（2） これまでの判例・学説

- 偽造キャッシュカードに関する判例は現在のところ見あたらないが、以下の最高裁判決が議論の手がかり。

<u>最高裁平成5年7月19日第二小法廷判決</u>

（真正なカードを利用してCD機から預金が引き出されたケース）

- 真正なキャッシュカードが使用され、正しい暗証番号が入力されていた場合は、銀行による暗証番号の管理が不十分等の特段の事情がない限り、約款上の免責は有効。
- （暗証番号の）解読には相応の知識と技術が必要であり、また、本件支払いがされた当時（昭和56年）は、そのような解読技術はそれほど知られていなかったことから、CD機による支払いシステムが免責約款の効力を否定しなければならないほど安全性を欠くものとはいえない。

<u>最高裁平成15年4月8日第三小法廷判決</u>

（盗取した預金通帳を使用してATMから預金が引き出されたケース）

- 本件についても、民法478条の適用があるものと解すべきであり、非対面のものであることをもって同条の適用を否定すべきではない。
- 銀行が無過失であるためには、単に払戻しの際に機械が正しく作動したことだけでなく、銀行が、機械払システムの設置管理の全体について、可能な限度で無権限者による払戻しを排除しうるよう注意義務を尽くしていたことを要する。

・（通帳機械払のシステムを採用していたにもかかわらず、その旨をカード規定等に規定せず、預金者に対する明示を怠った銀行は、）通帳機械払のシステムについて無権限者による払戻しを排除しうるよう注意義務を尽くしていたということはできず、本件払戻しについて過失があったというべき。

- これらの判決を偽造キャッシュカードにおいて具体的にどう考えるか。

  磁気キャッシュカードの偽造が容易にできることが広く周知されてきたことに加え、ICカード等より安全なシステムが技術的に可能となっていることにかんがみれば、現在のシステム及びその管理態勢について何らの措置も行わない場合には、将来的には、免責約款の効力が否定される、もしくは金融機関に過失ありとして弁済が無効と判断されることもありうるのではないかとの意見があった。

- 電子的方法による預金払戻しについては、民法第478条の適用を認めるのが通説・判例であるが、偽造キャッシュカードの損失補償について、特別法規や約款が存する場合には、民法第478条に優先することとなる。但し、約款が民法第478条に比べて預金者に不当に不利益を与えている場合には、消費者契約法第10条により無効とされるおそれがあることに配慮が必要。

2. 海外の制度等と我が国の特殊性

（1） 海外における補償制度

① 法令等か自主規制ルールか

法令等により対応している国（米国、フランス、オーストラリア）もあれば、約款等の自主規制ルールにより対応している国（英国、カナダ）もある。ドイツでは、民法の規定を前提に、実際の責任分担ルールをカード約款で規定している。

② 紛失、盗難、偽造の区別

紛失、盗難、偽造を区別せず同じ扱いをすることとしている国（米国、カナダ、オーストラリア）もあれば、紛失・盗難と偽造を区別して扱いを変えることとしている国（英国、ドイツ、フランス）(注) もある。後者の国では、偽造の場合、預金者の負担はないこととしている。

（注）但し、英国、ドイツでは、偽造について明示的な規定が置かれているわけではない。

③ 預金者の（重）過失の有無と負担額の設定

預金者の（重）過失の有無を考慮に入れて預金者の負担額を決めている国がほとんどであり、これらの国では、（重）過失がある場合は負担額の制限はないこととしている(注1)。

一方、預金者の（重）過失がない場合、預金者に全く負担を求めないこととしている国（カナダ、オーストラリア）もあれば、紛失・盗難の場合においてであるが、預金者に一定の負担を求めることとしている国（英国、フランス）[注２]もある。ドイツでは、紛失・盗難の場合において、軽過失がある場合は被害額の 10%を負担することとしている[注３]。
米国では、預金者の過失の有無は責任の範囲に影響しないが[注４]、預金者の通知遅延による損失を考慮に入れている。

（注１）但し、負担の上限を口座の取引限度額や口座残高の範囲に限定していることが多い。

（注２）（注３）なお、前述のとおり、英国、フランス、ドイツでは、偽造の場合、顧客の負担はないこととしている。

（注４）例えば、カードに暗証番号を記載していても、カード等の紛失・盗難を知った後２営業日以内に通知すれば、負担は 50 ドルまでとなる。

④ 立証責任

預金者の過失の立証の責任は金融機関側が負うこととしている国がほとんどである[注]（なお、米国では、預金者の通知遅延による損失の立証の責任を銀行側が負う）。英国では、金融機関側の立証を容易にするため、預金者が金融機関及び警察の調査に協力しない場合、金融オンブズマン又は裁判所がその点を考慮する可能性がある旨を約款の運用指針として公表している。

（注）但し、ドイツでは、最近の最高裁判決において、98 年に導入された暗証番号システムは事実上解読不可能であることを前提に、預金者が不正使用であることを反証しない限り、預金者の重過失である可能性が高いと判示している。

⑤ 実際の補償状況

以上のような制度整備は行われているが、諸外国の金融機関では、金融取引の円滑性や金融機関のレピュテーショナルリスクにかんがみて、実際には、一定の条件のもとに全額補償をするところが大半である。これは、第一に、顧客や金融機関が、発生した被害につき、偽造・盗難等のいずれによるものか、直ちに証明することが極めて難しい場合があることや、第二に、我が国のような現金主義ではないことを反映して、ATMによる現金引出額が比較的低い金額に設定されていることにより、被害額が限定され、金融機関として負担できる範囲に収まるケースが大半であることが背景にあると考えられる。

（2） クレジットカード

- 偽造カードによる被害については、商品購入、キャッシングともに、カード会社において事実関係を調査し、会員が暗証番号管理を含む善管注意義務を尽く

していると判断される場合には、カード会社において負担。

- 盗難・紛失については、会員規約（会員保障制度等）に従い、会員の損害をてん補。
- 但し、クレジットカードについては、キャッシュカードと異なり、利用限度額や年会費がある。
- クレジットカード会社においては、被害を押さえるために不正使用検知システムを整備。

（3） 我が国の特殊性

- 我が国は先進国の中でも突出した現金主義社会。小切手やカード利用が中心の欧米諸国と対照的。
- 我が国におけるATMでの払戻し限度額は、欧米諸国に比べ高額。

（1日あたりの払戻し限度額 ： 金融機関によりまちまちではあるが、米 1000ドル程度、英 400～500 ポンド、独・仏 500 ユーロ程度、日 200 万～500 万円といった例が見受けられる。）

3．我が国における損失負担ルールの考え方

（1） 損失負担ルール

① 本中間取りまとめにおける検討対象

偽造キャッシュカードを使用した預金の払戻しに限らず、振込及び預金担保借入も対象とする。

② 損失負担ルール検討にあたり考慮すべきポイント

- 損失負担ルールを考えるにあたっては、金融機関に、偽造キャッシュカードによる被害を予防する措置を講ずるインセンティブが働くよう配慮すべき。
- 他方、暗証番号やカードの管理に関する預金者のモラルハザードを招かない配慮も必要。

③ 損失負担ルールの前提となる考え方

- 偽造キャッシュカードによる払戻し、振込、預金担保借入は、無権限者への預金の払戻し、無権限者の指図による振込、無権限者による借入であり、本来、有効な行為ではないということを前提とすべき。
- 現在のキャッシュカードシステムは、カードの所持と暗証番号との二つの認証により成り立っているが、偽造キャッシュカードが作られる状況とは、カードの所持による認証が機能していないことに他ならず、（完璧なシステムがありうるのかという議論はあるものの、）現行のキャッシュカードシステム自体には、何らかの改善・補強を行うべき欠陥があるといえるのではないか。

- 金融機関と預金者では、一般的に立証能力等に差があり、債務者の動態的取引の保護に重きを置いた民法第４７８条的な発想では、偽造キャッシュカードの場合には、債権者（預金者）側に酷な場合が多いのではないか。
- もちろん、カード及び暗証番号の管理について預金者に全く注意義務を求めないのは適切ではない。偽造されるリスクをあらかじめ説明したうえで、預金者にも注意義務を尽くすことを求めるべき。

④ 新しい損失負担ルール

- 以上を勘案すると、原則的な偽造キャッシュカードによる損失補償のあり方としては、次のような考え方が望ましいのではないか。

○ 偽造キャッシュカードが使用されたことによる損害は、原則として金融機関が負担。 ○ 但し、預金者の責に帰すべき重大な事由がある場合には、預金者が負担。 ○ 預金者の帰責事由については、金融機関に立証責任。

- 預金者の責に帰すべき重大な事由とは、キャッシュカードの偽造またはその使用につき預金者に故意がある場合、及びキャッシュカードまたは暗証番号の管理につき預金者に重過失がある場合をいう。なお、預金者の重過失については、（偽造キャッシュカードの場合、スキミングと預金引出しとの間で時間的余裕を犯罪者側が持ちうることにもかんがみ、）キャッシュカード及び暗証番号の両方の管理につき過失が認められる場合に初めて認定すべきとの意見もあった。
- 負担の割合については、過失相殺等により事案に応じて勘案することも考えられる。

⑤ 実施上の留意点

- この案によった場合、個別の事案につき帰責事由の有無や過失割合等が考慮されるため、金融機関による対応に差が出るおそれがある。これを防止するために、なんらかの目安（ガイドライン）を作ることが必要であることから、具体的にいかなる場合に預金者が損失を負担するのかを、ルール上明示すべき。
- 以上が原則的な損失負担ルールの考え方であるが、各金融機関が、預金者の選択により、当該ルールに基本的に沿った特別なルールを組み込んだ商品を提供することを否定するものではない。例えば、預金者への早期補償実現の観点から、下記のように預金者の過失の程度により、預金者、金融機関

が損失を負担すべき割合をあらかじめ約款において定めておき、過失相殺を考慮せず損失を補償する方法も考えられる。なお、このように原則的な損失負担ルールに沿った特別なルールを採用する商品を提供するにあたっては、預金者にその内容を事前に周知徹底することが必要なことは言うまでもない。

（例） 預金者が無過失の場合　預金者　0%・金融機関100%
預金者が軽過失の場合　預金者10%・金融機関90%
預金者が重過失の場合　預金者100%・金融機関0%

（2） 預金者の重大な責に帰すべき事由

預金者が損失を負担すべき重大な帰責事由について検討する。

① 考え方

偽造キャッシュカードに関する損失は、原則として金融機関が負担すべきとする前記（1）④の考え方にたてば、預金者が損失を負担することとなる事由は限定的に考えるべき。

② 具体的な例についての検討

イ 預金者にキャッシュカードの偽造またはその使用につき故意がある場合

- キャッシュカードの偽造またはその使用につき預金者に故意がある場合には、預金者が損失を負担すべきである。
- 但し、一般的には、金融機関といえども預金者の故意を立証することは困難な場合が多いと考えられることから、故意が推認される合理的な理由がある場合には、金融機関が損失負担に応じないこととする仕組みを採ることが必要ではないか。

  具体的には、
  - 家族、同居人、使用人による不正利用に起因する場合
  - 金融機関による調査に協力しない場合
  - 被害状況の届出等に虚偽があった場合

  には、金融機関が免責されると考えられないか。
- もっとも、こうした内容を金融機関の免責事由として法律や約款に記載し、その効果として預金者が金融機関に対して補償を求める権利を喪失させるには、如何なる場合に補償を受けられないのかを極めて詳細に記述することが必要になると考えられる。そのため、免責事由として列挙するのではなく、実務上の運用指針とするほうが望ましいとの意見があった。

ロ　預金者の重過失が問題となる場合

（暗証番号の管理に関して）

- 預金者の重過失が認められる場合
  - i　他人に暗証番号を知らせた場合
  - ii　暗証番号をカード上に書き記した場合

- 周辺事情を総合的に勘案して、重過失を認定する際の一要素となりうる場合

  以下のような場合の指摘があった。
  - iii　暗証番号のメモ（または、暗証番号を推測させる書類等）をカードと一緒に保管あるいは携帯した場合
  - iv　預金者自身の生年月日、預金者の自宅や勤務先の電話番号・住所など外部から容易に推察されうる番号を暗証番号として使用していた場合
  - v　暗証番号と同じ番号を金融機関以外の第三者との取引で使用していた場合

・ iii、iv、vについては、それぞれの項目に該当したというだけで、直ちに重過失に該当するとは考えられない。実際にも、口座ごとにキャッシュカードが交付され、また、個人が多種・多数のカードを保有している現在においては、暗証番号の記憶、管理が困難となっており、これらの事由のみで直ちに預金者に損失を負担させるのは酷なものと考えられる。

・ もっとも、iii、iv、vについても、周辺事情を総合的に勘案して、預金者の重過失を認定できる場合もあるのではないか。

・ iiiについては、暗証番号を記載したメモをカードにクリップ止めした場合など、前記②ロii「暗証番号をカード上に書き記した場合」と同視できるような場合には重過失が認められるが、暗証番号を記載した手帳をカードと同じ鞄に入れていた場合など、直ちに重過失が認定できない場合もあり、周辺事情を総合的に勘案したうえで、重過失といえるか否か、慎重に判断すべきである。

・ ivについても、重過失を認定する要素としては慎重に考えられるべきである。但し、過去に類推されやすい番号を、第三者との取引における暗証番号として使用し、不正取引の被害にあったにもかかわらず、その後継続して同じ暗証番号を使用している場合などには、重過失に該当しうるといえる場合があるのではないか。また、ivとあわせて、（iiiにあるように）暗証番号を推測させる書類等をカードと一緒に保管あるい

は携帯したといった場合には、重過失を認定しうる場合があるのではないか。

- ｖについては、周辺事情を総合的に勘案しても、預金者の重過失を認定できる場合は極めて少ないのではないかとの意見があった。
- ただし、今後、金融機関から、預金者に対し、ⅲ、ⅳ、ｖに記載されているような行為を行わないよう、暗証番号管理の必要性等が周知徹底された場合には、これらをそれぞれ重過失に該当する事由と考えることも可能となってくるとの意見もあった。

（カードの管理に関して）

ⅰ　預金者自ら、カードの占有を安易に第三者に移転した場合（ただし、デビットカード取引のように、カードの本来の使用目的として、預金者の監視の下に、キャッシャーにカードを手交する場合などは除く。）

ⅱ　カードの占有を第三者に容易に奪われる状況においた場合（施錠可能なセーフティボックス等に保管した場合は、該当しない。）

（金融機関への通知、口座の管理に関して）

ⅰ　第三者による出金を知ってから金融機関に対して通知するまでに一定時間を経過した場合

- 金融機関において、２４時間通知を受けうる態勢と預金者が容易に通知先を知りうる態勢を作ることが前提。
- 上記のような態勢が整っているにもかかわらず、通知が遅れたことにより増加した損失については、預金者が原則負担か。

ⅱ　第三者による出金があったがこれに気づかないまま一定期間を経過した場合

- 長期間の経過により証拠が消滅するなどして金融機関による立証ができなくなる場合にまで、金融機関の補償を原則とするのは適切ではないとの意見があった。
- 現在の預金通帳への記帳による口座管理を前提にした場合にこれを重過失と考えることは困難であるが、金融機関から、定期的にステートメントを送付することを前提とした場合には、数度ステートメントを受け取ったにもかかわらず、これを放置した場合を問題とすることが可能ではないか。

（バスケット条項を記載することに関して）

帰責事由を網羅的に記述することは困難であるため、具体的な責に帰すべき重大な事由を列挙したうえで、「その他預金者に故意または重大な

過失があると推認しうる合理的な根拠が認められる場合」といったバスケット条項を記載することはやむをえないのではないか。

なお、バスケット条項の運用実態にかんがみ、将来的な条項の見直しを検討すべきではないかとの意見があった。

4. 損失負担ルールの前提としての環境整備

（1） 補償の悪用（被害の偽装など）対策

例えば、補償の検討にあたっては、金融機関は預金者本人及び警察に対して、当該預金者があらかじめ警察に対して申告をしたか調査するなど。

（2） 被害を早期に発見するための態勢

① 異常な取引を察知するシステム（例：深夜に一定額以上の出金がある場合に取引を停止した上で、本人に連絡して確認）
② 預金者に対する通知
③ 預金者からの通知を24時間受けうる態勢と連絡先の周知
④ 預金者の側にも通知義務を課し、通知してもらえるような工夫

（3） 損失負担への対策

① 払戻し限度額の設定

預金者の利便性に配慮しつつ、被害額の抑制を図るため、原則として限度額を低く設定したうえで、預金者の判断による限度額の引上げを可能とすべき。

② 口座維持手数料
③ 保険

まずは、既存の商品に加え、これらを組み込んだ個別商品等を開発し、預金者の選択の幅を広げることが必要。

（4） 預金者が補償を受けられないケース、及びその前提となる注意義務の内容の周知

① 約款等への記載

重過失の例示とともに、預金者が最低限尽くすべき注意義務も明記すべきか。

② 説明態勢の整備

預金者にキャッシュカードの交付を受けるか否かの判断を求める際には、金融機関は、あらかじめ預金者に対し、キャッシュカードの交付を受け、これを所持することのリスク（例えば、偽造キャッシュカードによる損失を被った場合に、必ずしも全額が補償されるわけではないこと）及び、預金者として尽くすべき注意義務の内容（例えば、暗証番号を他人に教えてはならない等）

を説明することが必要。

（5） 金融機関による預金者への過剰なサービスの自粛と、自己の管理可能な範囲でサービスを享受するという預金者側の意識の喚起

例えば、定期預金担保借入付の普通預金を顧客に対して勧める場合には、併せて定期預金担保借入が付されていない商品もあることを説明することとするなど。

5．今後の対応

（1） 緊急の対応

偽造キャッシュカードに関する損失補償の緊急性にかんがみ、偽造キャッシュカード問題について検討を集中してきたところ。立法による対応も視野に入れつつ、まずは約款の改正で対応すべき。その際には、その実効性を担保するための行政上の対応が必要である。

（2） 新たな損失補償ルールが適用される以前の損失について

約款を改正した場合には、新しいルールが実施される以前の偽造キャッシュカードの被害者に対しても、新しいルール下での補償のあり方と平仄を図るべく、誠意を持って対応すべき。

（3） 立法による対応に関する検討

- 立法による対応を検討する場合には、預金取引のみについて法規制を行うことの法技術上の問題のほか、表見代理（民法第109条、110条、112条）、金融機関の善管注意義務違反を内容とする債務不履行（民法第415条）、債務不履行等を前提とした過失相殺（民法第418条）など、議論すべき論点が多い。また、無権限者による振込や総合口座における定期預金担保借入等、ATMを利用した他の取引に関する補償のあり方との整合性も検討する必要がある。
- 補償の悪用（被害の偽装など）防止に関する刑事法分野における対応も要検討か。この点については、偽造キャッシュカードによる損失につき、預金者が捜査機関に対し、窃盗罪（刑法第235条）や、支払用カード電磁的記録不正作出準備罪（刑法第163条の4）の被害者として、被害届が提出できるよう、立法上、実務上の対応が必要との意見があった。

（4） 当スタディグループにおける検討の範囲

- 偽造キャッシュカードに関する損失補償の対応を踏まえ、盗難キャッシュカードに関する損失補償への対応をいかに考えるべきか。偽造キャッシュカー

ドと盗難キャッシュカードとでは損失補償の考え方を異にすべきか。
この点につき、偽造キャッシュカードの問題は、キャッシュカードシステム自体の欠陥の問題であり、当該システムに瑕疵がないことを前提とした盗難キャッシュカードの問題とはあくまで区別して考えるべきとの意見があった。他方、盗難キャッシュカードと偽造キャッシュカードとは、真正のキャッシュカードの占有を奪った後、そのカード自体を不正使用するか、スキミングをした上で真正のキャッシュカードを返却し、これをもとに作出した偽造キャッシュカードを使用するかの違いに過ぎず、両者に関する補償のあり方を区別する必要はないのではないかとの意見もあった。
盗難キャッシュカードの問題については、以上のような議論も踏まえ、更なる検討が必要ではないか。

- 消費者保護の観点からすれば、偽造キャッシュカードに加え、盗難キャッシュカード、更に、預金通帳を利用した不正取引も含め、銀行取引に関する消費者被害全般を視野に入れて検討すべきとの意見があった。
これに対しては、預金通帳と印影を使用した窓口での不正取引は、相対の場面であり、ATMといった機械を利用した不正取引とは態様が違うのではないかとの意見があった。
また、盗難キャッシュカード、預金通帳を利用した不正取引についてまで議論を広げることになれば、印鑑照合を含む金融機関における預金払戻しシステムそのものを大きく見直すことが必要になるのではないかとの意見があった。

（以上）

（別添４）

平成１７年５月１３日

偽造キャッシュカード問題に関するスタディグループ第二次中間取りまとめ
～盗難キャッシュカード被害に対する補償を中心として～

盗難キャッシュカードの問題については、3 月 31 日の「偽造キャッシュカード問題に関するスタディグループ中間取りまとめ～偽造キャッシュカード被害に対する補償を中心として～」（以下、「第一次中間取りまとめ」という。）において、「（それまでの）議論も踏まえ、更なる検討が必要ではないか。」と位置付けたところである。その後、4 月 15 日に、金融庁より、盗難キャッシュカードの問題についてもスタディグループの検討項目とするよう要請が行われた。これを受け、当スタディグループにおいて、集中的な議論を行い、以下のとおり第二次中間取りまとめとして盗難キャッシュカードに関する議論の集約を行った。

（注）本取りまとめにおいて、盗難キャッシュカード被害とは、本人の意思によらずにその占有が失われた（盗難に加え、強盗や脅迫等による場合を含む。）真正キャッシュカードが無権限者により ATM（現金自動預入支払機）（CD（現金自動支払機）を含む。）において使用され、不正に現金引出し等が行われることをいう。

１．盗難キャッシュカード被害に関する補償の現状等

（１）盗難キャッシュカード被害の状況等

- 警察庁の資料によれば、平成 16 年（1～11 月）におけるキャッシュカード盗難の認知件数は 14 万 2443 件であり、犯罪類型別に見ると、車上ねらい 4 万 7596 件（33.4%）、置引き 2 万 5049 件（17.6%）、ひったくり 1 万 5915 件（11.2%）、住宅対象侵入窃盗 1 万 2138 件（8.5%）となっている（なお、同期間の各種窃盗被害総数は約 183 万件）。
- また、同時期における盗難及び偽造キャッシュカードによる ATM からの不正な現金引出しの認知件数は 3114 件（キャッシュカードの窃盗被害認知件数の約 2%）で、キャッシュカードの窃盗被害認知件数に占める割合は低いが、この理由としては、例えば、犯人側が暗証番号を推知できなかったこと、預金者から金融機関への通知により不正な引出しを止めることができたことなどが考えられる。なお、現金被害総額は約 21 億円、1 件平均は約 69 万円となっている。
- 盗難キャッシュカードによる被害については、各金融機関において網羅的な把握がなされていないため、全国銀行協会等による統計は存在しない。そのような中で、一部金融機関における調査によると、

  ①キャッシュカードの利用停止の申出は、盗難のほか、紛失による場

合も含まれると考えられるが、一月当たり数万件程度、

②サンプリング調査によれば、不正払出しから預金者による金融機関への届出までの時間は、1 時間以内が 3 割程度、6 時間以内が 6 割程度、24 時間以内が 8 割弱、48 時間以内が 8 割強、

③キャッシュカードの盗難類型は様々であり、空き巣、車上荒らし、ロッカー等からの盗難、すり、置引き、ひったくり、強盗、脅迫等が見られる。また、暗証番号の不正取得の態様も、運転免許証等の生年月日等からの類推、覗き見、警察官等を装った聞き出し、脅迫による聞き出し等、様々である（なお、暗証番号を推知された理由が預金者に不明な場合も存在する。）。

（２）現行約款の運用

- 金融機関は、ATM の操作の際に、「電磁的記録によって･･･カードを当行が交付したものとして処理し、入力された暗証と届出の暗証との一致を確認して預金の払戻し」（全国銀行協会カード規定[試案]第 10 条第 2 項本文）を行えば免責される。
- 偽造キャッシュカードの場合と異なり、現行約款においては預金者に帰責事由がない場合のただし書き規定が存在せず、盗難キャッシュカードのほとんどのケースで預金者は補償を受けられないとの批判がある。

（３）盗難キャッシュカード等に関する判例上の扱い

- 約款上は、上記のように、カードとその暗証番号の一致を確認すれば金融機関は免責されることになっているが、判例においては、民法第 478 条を踏まえ、金融機関が免責されるためには、金融機関の善意無過失が必要（最高裁昭和 42 年 4 月 15 日第二小法廷判決ほか）。

  金融機関の注意義務の内容としては、銀行の過失が認められた最高裁平成 15 年 4 月 8 日第三小法廷判決が参考となる。

  銀行側の注意義務に関する記述：

  「銀行が無過失であるというためには、…暗証番号の確認が機械的に正しく行われたというだけでなく、銀行において、預金者による暗証番号等の管理に遺漏がないようにさせるため当該機械払の方法により預金の払戻しが受けられる旨を預金者に明示すること等を含め、機械払システムが全体として、可能な限度で無権限者による払戻しを排除しうるよう組み立てられ、運営されるものであることを要するというべきである。」

- また、約款上は、金融機関の免責に当たり、預金者（ないしカード契約者）側の過失の有無は考慮されていないが、判例においては、

  ①いかなる場合においても預金者（もしくはカード契約者）が不正使用の危険を負担しなければならないと解するのは、銀行と契約者との間に存する諸々の格差を考慮すれば、妥当とは言い難く、預金者（もしくはカード

契約者)に帰責事由がなければ、約款の適用ができないとして預金者(もしくはカード契約者)側の過失を要するとしたもの(福岡高裁平成 11 年 9 月 22 日判決ほか)、

②銀行の関与の及ばないカード契約者側の事情により銀行の免責が左右されるのは相当でないとしてカード契約者側の過失は不要としたもの(東京地裁平成 15 年 4 月 25 日判決ほか)、

に分かれている状況。

- なお、銀行と預金者の双方に過失が認められる場合には、損害の負担割合につき過失相殺を認めた判例が存在する。

〔参考〕さいたま地裁平成 16 年 6 月 25 日判決

銀行が無過失でない限り、民法第 478 条の適用はなく、その弁済は無効だが、預金者に重大な過失がある場合には、公平の観点から民法第 418 条を類推適用して、その過失を斟酌し、過失相殺することができる(本事案では、双方の事情を総合的に勘案し、預金者の過失割合を 3 割とした。)。

２．盗難キャッシュカードと偽造キャッシュカードに関する整理

(１) 盗難キャッシュカードと偽造キャッシュカードの共通点

- いずれも、本人に関する情報を搭載したカードの所持(所持認証)及び暗証番号(記憶認証)の二重の認証機能により本人確定を行う現行の ATM／キャッシュカードシステムを用いた非対面取引。
- 二重の認証機能のうち、特に記憶認証がハードルとして機能しない場合に被害が発生するという点が両者に共通する。

(２) 盗難キャッシュカードと偽造キャッシュカードの相違点

- 偽造キャッシュカードによる払出しは所持認証機能が失われたいわばシステムエラーともいうべき問題。盗難キャッシュカードによる払出しは、システムは正常に機能していることが前提。
- 盗難キャッシュカードの場合においても、カードの盗難により所持認証機能は失われるが、偽造キャッシュカードと異なり、一般的には、喪失に気が付いた正当な権利者の早期対応が可能。
- 偽造キャッシュカードの場合、システム提供者たる金融機関の責任が重く、それゆえ預金者の帰責は限定的(故意・重過失)に解すべきとされた。他方、盗難キャッシュカードの場合は、窃盗の一類型としての側面があり、その態様は広く(例:空き巣、車上荒らし、ロッカー等からの盗難、すり、置引き、ひったくり、強盗、脅迫等)、偽造キャッシュカードによる不正取引に類似した預金者の帰責性が低いと考えられるものから、専ら預金者に過失が認められるものまであり、預金者の帰責の程度も区々である(判例の認定も様々。)。

３．損害保険におけるモラルハザード対策

- 盗難キャッシュカード被害への補償を考えるに当たっては、預金者のモラルハザードや被害の偽装に対する対応策が重要となる。この点については、損害保険においてこれまで蓄積されてきた対応策が参考になるとの指摘があった。
- 具体的には、参考となる方策として、一般の損害保険における以下のものがあげられる。

  ① 保険商品設計段階の方策

  保険金額の上限や免責額を設定することや、損害額の一定割合について自己負担することを求める。

  ② 保険事故発生時の方策

  一定の補償対象期間を設定するなど、補償対象を制限。また、盗難について警察への届出や損害保険会社の損害調査に協力する義務を課す。

  ③ 同様の事故が繰り返された場合の方策

  再発防止策の実施の要請や契約更新時の保険料の引上げ、補償範囲の厳格化といった対応。

- 現在、金融機関が加入しているキャッシュカード盗難保険においては、金融機関が保険料を負担するのを基本とするが、そうした保険においては、以下のような対応がなされている。

  ①保険金額に 100～300 万円の上限を設ける。

  ②盗難について警察への届出や損害保険会社の損害調査に協力する義務を課す。

  ③被害通知の 10 日前以後を補償対象期間とする。

  ④再発防止策の実施の要請や契約更新時の保険料の引上げを行う。

４．海外における補償制度

海外における補償制度については、第一次中間取りまとめで整理したとおりであるが、盗難キャッシュカードに関して、留意する必要があると考えられる点は以下のとおり。

- 諸外国においては、実務上、原則として、偽造・盗難の区別なく補償を行っている場合がほとんどであるが、これは、国外で引き出されたり、デビットカードとして使われてしまうケースが多くあることや、偽造・盗難の区別をするための調査が容易でない場合が多いことに加え、ATM の引出限度額が低く設定されていることに伴い、損害額が低くなっていることなどによる。なお、最低限の補償ルールが以下の例のように法令等（米国、フランス、オーストラリア）や約款（英国、カナダ）で決められており（ドイツでは民法を前提に約款で規定）、各金融機関は、それらを基本にしつつ実務上の補償内容をより上乗せした形のものにしている。

- 預金者による通知の時点により、補償の金額に差異を設けている例がある。例えば、米国では、①盗難・紛失に気付いた後、2 営業日以内に通知した場合は 50 ドル、②2 営業日終了後、期間計算書交付から 60 日以内は 500 ドル、③60 日終了後は全損失、を預金者が負担する。フランスでは、一定の期間（2 営業日以上で金融機関が定める期間）以内に通知しない場合は、預金者が損失の全額を負担する旨を金融機関が約款で定めることも可能としている。
- 預金者に対して一定の負担を求めている例がある。例えば、米国では、通知の時点によって 50 ドル又は 500 ドルを負担する。また、英国では 50 ポンド、フランスでは 150 ユーロを負担する。
- 預金者側の過失の軽重等により、預金者の負担を加減している例がある。例えば、ドイツでは、軽過失の場合は 10%、重過失の場合は全損失を負担する。英国では、預金者が相当な注意を払わなかった場合、全損失を負担する。
- 立証の困難性に配慮した例がある。例えば、オーストラリアでは、預金者が無過失であれば負担なし、過失があれば全損失を負担する。また、過失の有無が不明な場合は、預金者は損失額のうち 150 豪ドルまで負担する。

５．盗難キャッシュカード被害に関する損失負担ルールの考え方

（１）損失負担ルールの適用を検討する対象

- 盗難された真正なキャッシュカードを無権限者が ATM において不正に使用した、預金の払戻し、振込み及び借入れを対象とする。
- 紛失も盗難と同様に扱うこととする。なお、紛失の場合は、盗難と比べても、本人の帰責性が高いと一般的に考えられ、盗難とは一線を画すのが適当との意見もあった。

（２）損失負担ルールの検討に当たり考慮すべきポイント

損失負担ルールを検討するに当たっては、偽造キャッシュカードの場合と同様に、金融機関において、盗難キャッシュカードによる被害予防のインセンティブが働くよう配慮すべきであるし、預金者の暗証番号やカードの管理に関するモラルハザードを招かない配慮も必要と考えられる。

（３）損失負担ルールの前提となる考え方

(基本的考え方)

- 盗難キャッシュカードによる払戻し等は、無権限者による行為であり、本来、有効な行為ではないということを前提とすべき。
- 預金者が金融機関に求めるサービスの最たるものは、自己の財産を安全に管理してもらうこと。こうした金融機関への預金の安全性に対する預金者の信頼を尊重する観点からは、金融機関の過失のみに着目し金融機関が

善意無過失の場合に免責される民法第 478 条的な考え方ではなく、特に、預金者が通常求められる注意義務を果たしている場合には、預金者が保護されて然るべきではないか。

（預金者の責任）

- 盗難キャッシュカードは窃盗犯罪の一類型であり、一旦カードが発行された後は預金者側のカード及び暗証番号管理における注意義務が問題になる。実際、盗難の発生は、預金者のカード及び暗証番号管理の程度に深く関連しており、金融機関にとっては、盗難発生の真偽さえ知り得ない場合がほとんどであり、かつ、盗難発生に関する過失は極めて限定的ではないか。
- 現在の ATM／キャッシュカードシステムを前提とする場合、預金者には、カードや暗証番号の管理について、一般人として通常求められる程度の注意義務を果たすことが期待されているほか、仮に盗難された場合は、カードが喪失していることから、速やかに金融機関に届け出ることが求められていると考えられる。

（金融機関の責任）

- 他方、金融機関においても、システム提供者の責務として、可能な限り無権限者による払戻し等を排除し得るよう注意義務を尽くすことを要する（最高裁平成 15 年 4 月 8 日判決参照）と考えられるのではないか。これについては、コスト面、技術面での制約はあったにしても、被害の拡大を抑止するための引出限度額の設定に関する工夫や、認証システムとしての暗証番号の改善、異常取引の検知と排除のためのシステム開発等について、金融機関としてより踏み込んだ検討がこれまでも可能だったのではないかとの意見があった。

（特に留意すべき点）

- キャッシュカードの盗難件数は、偽造キャッシュカードと異なり、大量であるため、ルールの検討に当たっては、理論的な詰めだけではなく、実務上の実行可能性について配慮する必要がある。その際、保険実務などを参考に、外形的な基準による選り分けを行うことは一定の合理性があるのではないか。
- 過大な補償を求めるなど、金融機関に極端な負担を強いる場合には、金融機関のビジネスモデルとして成り立たなくなり、その場合、口座維持手数料を一律に課したり、引出限度額を極端に引き下げたりする事態が想定され、結果的に預金者の利便性が損なわれるといった副作用が生じ得ることにも配慮する必要がある。
- 偽造キャッシュカードと比べて、被害の偽装がより容易であることから偽装の防止が必要である。その際、盗難キャッシュカードでは、預金者が

警察に被害届を出すのが通常であり、当該届の提出を金融機関に補償を求めるための一つの条件とすることで一定の被害の偽装防止策となり得るのではないか。

６．盗難キャッシュカード被害に関する補償のルール案

- 上記の前提となる考え方を踏まえると、理論的には以下のようなルール案が考えられる。

  ①警察への被害届等を補償を求めるための前提とする。

  ②金融機関に故意又は過失がない場合であっても、（現行約款等の考え方を改め、）預金者に故意又は過失がない場合は、金融機関が損害を補償することとする。

  ③立証責任については、キャッシュカードが盗難されて現金が引き出されるに至った事情については預金者にしか分からず、また、システム提供者としての責任を果たしていたかは金融機関にしか分からないため、前者の立証責任は預金者に、後者の立証責任は金融機関に課す。

  しかしながら、こうしたルール案の場合、特に、預金者にとっては、盗難されたことについての帰責事由がないことの立証は実際には困難であることが多いため、一般人としての通常の注意義務を果たしていた場合であっても、補償されない事態が想定される。また、全ての盗難被害について、個々のケースごとに立証を行うことは預金者、金融機関双方にとって実務上の負担が極めて大きいことが懸念される。

- したがって、損失負担のルール案の策定に当たっては、上記「前提となる考え方」でも述べたように、理論的な妥当性のみならず、実行可能性についても配慮することが必要であると考えられ、その観点から以下のような点を満たすルール案が適当ではないか。

  ①過失責任の原則をベースとしつつも、預金者・金融機関の公平性に十分配慮しつつ、大量の事故を処理する観点から、基本となる対応方針を定めた上で、さらに当事者の過失が明らかな場合については、それに応じた負担を求めることとする。

  ②そのために、可能な限り外形基準による認定を行い、負担が大きい個別の過失認定を行う場合を限定していくこととする。

  ③モラルハザード回避の観点から、両当事者に犯罪予防に対する適切なインセンティブを与える仕組みとする。

➢　以上の検討を踏まえれば、原則的な盗難キャッシュカードによる損失負担のあり方としては、以下のようなルールが適当ではないかと考えられる。

○ 盗難キャッシュカードが使用されたことによる損害は、金融機関に過失がない場合であっても、盗難に関する金融機関への速やかな届出、警察署への被害届、金融機関による調査への全面的な協力（注 1）及び以下のイ）～　ハ）（注 2）に該当しないことを条件に、

イ）預金者の家族、同居人、使用人によって使用された場合
ロ）被害状況の届出等に虚偽があった場合
ハ）戦争、暴動等著しい社会秩序の混乱に乗じ又は付随してなされた場合

盗難の届出の一定期間前以後に発生した損害を補償対象とすることとし、それについて、
①原則として、預金者と金融機関が 50%ずつ負担（注 3）、
②ただし、預金者が無過失の場合、金融機関が全額負担（預金者側に疎明を行う責任）、
③また、預金者が重過失の場合、預金者が全額負担（金融機関側に立証責任）、
とする。

○ 金融機関に過失がある場合、原則として金融機関が負担。ただし、預金者の過失に起因する損害があれば預金者も一定の負担か。

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">預金者の過失</td></tr>
<tr><td>重過失</td><td>標準的なケース
（重過失が立証不能・無過失の疎明が不十分な場合を含む）</td><td>なし</td></tr>
<tr><td rowspan="3">金融機関の過失</td><td>あり</td><td colspan="2">原則として金融機関が負担。
但し、預金者の過失に起因する損害があれば預金者も一定の負担か。</td><td>金融機関が負担</td></tr>
<tr><td>⇩（金融機関が立証）
なし</td><td>預金者が負担</td><td>金融機関　５０％
預金者　　５０％</td><td>金融機関が負担</td></tr>
<tr><td colspan="2">⇦（金融機関が立証）</td><td colspan="2">⇨（預金者が疎明）</td></tr>
</table>

（注）預金者に重過失がありその立証を金融機関が行った場合は、預金者が被害額を負担することになる点は、偽造キャッシュカードの場合と同じ。ただし、偽造キャッシュカードの場合は、立証不能の場合、金融機関の全額負担となり、より重い責任を金融機関に負わせることとなる。

- 補償対象期間については、盗難の届出の一定期間前以後とすることが適当と考えられるが、それについては、以下のような 2 つの意見があった。
  ①一部金融機関による実態調査からすると、不正払出から預金者による金融機関への届出までの時間は、48 時間以内が 8 割強となっていることに鑑み、届出時の 48 時間前以後の損害を対象としてはどうか。ただし、預金者が金融機関に通知する機会を持ち得ない状態にあるなど、特別な事情がある場合には、個別の事情に配慮する必要があるのではないか。
  ②キャッシュカード盗難保険の例に鑑み、届出日の 10 日前以後の損害を対象としてはどうか。その際、盗難に気が付きながら、直ちに届出を行わない場合は、預金者の重過失と考えられるのではないか。
- 預金者にとって無過失の立証は極めて困難であることに鑑み、預金者は自己の盗難の状況等について可能な限り合理的な説明を金融機関に対して行い（疎明を行う責任）、金融機関がそれを一応確からしいと推測を得た場合（いわゆる疎明の状態）には、預金者の無過失を認定することを基本とするべきではないか。そのために、金融機関において預金者対応を専門的に行う窓口を作ることが必要か。
- 本ルールの導入に当たっては、預金者に対して被害にあった場合の連絡先を含めルールの内容について十分な説明を行うとともに、カードの常時携帯、不要なカードの整理、定期的なカードのチェックなどの被害防止のための方策について注意喚起することが必要。また、金融機関のみならず警察における受付体制も整備することが必要か。
- 預金者の重過失とは、第一次中間取りまとめの議論と同様、以下のような場合が考えられる。
  - 本人が他人に暗証番号を知らせた場合
  - 本人が暗証番号をカード上に書き記した場合
  - 本人が自らの意思で、盗難される危険性が高いと一般的に考えられる状況下にカードをおいた場合
  - 本人が通常求められる程度の注意を払っていなかったり、防犯措置を講じていなかった場合
  - その他預金者に故意又は重大な過失があると推認し得る合理的な根拠が認められる場合
- 金融機関の無過失については以下の点を満たす必要がある。
  - 暗証番号の漏洩に故意過失がないこと
  - ATM 及びつい立ての設置状況や顧客行列の適切な誘導等、覗き見を防止するための措置に十分な注意を払っていること
  - 異常な取引を認知し排除しなかったことについて故意過失がないこと
  - その他可能な限度で無権限者による払戻しを排除し得るよう注意義務を尽くしていること

（注 1）金融機関に対する当初手続きとしては、金融機関に対する速やかな届出を行い、その届出後 1 週間以内に、盗難に至った状況やその後の対応、警察への被害届の記載内容及び受理番号等を書面に記載し、所轄警察官署の証明書等を付して、金融機関に提出するといった扱いが考えられるか。

（注 2）イ）～　ハ）の条件については盗難キャッシュカード保険にも同様のものがある。

（注 3）預金者には、カードが盗難されたことについて何らかの過失があると推認されること、他方、金融機関には、システム提供者として預金の安全性への信頼を守る責務があると考えられることなどから、原則として損失を折半することとしたもの。

７．その他

第一次中間取りまとめにおいて指摘された事項に加えて、金融機関や業界団体に求められる対応としてあげられた事項は以下のとおり。

（１）保険の活用等による多様な預金商品の提供

- 本中間取りまとめにおいて示された損失負担ルールは、いわば最低限のルールであり、各金融機関において、預金者のニーズを踏まえ、それぞれの金融機関の創意工夫により多様な預金商品を提供することが望ましい。
- 例えば、

①預金者が、損失負担ルールにより預金者が負担することになる部分について、より高い安全性と補償を求める場合は、預金者の選択として、口座維持手数料の徴収、盗難キャッシュカード保険の付保等を組み込んだ新たな個別商品の開発、

②損失を極小化するため、ATM における引出限度額を引き下げる一方で、多額の現金決済を必要とする預金者に対しては、引出限度額を引き上げる（預金者の選択により引き上げた引出限度額部分が被害にあっても補償の対象としないこととする場合には、その旨を預金者に対して事前に周知徹底することが必須。）、

などの対応が考えられる。

（２）被害の偽装防止のための対応

- 保険の活用による副次的な効果として、自動車保険や火災保険等における不正請求等防止制度と同様の制度を導入することにより、不正請求者に係る情報を交換することで、被害の偽装を防止することはできないかとの意見があった。
- 盗難キャッシュカード被害の偽装防止策については、警察との緊密な協力の下、金融関係団体において、更なる検討が必要である。例えば、被害

の偽装を疑う合理的な根拠がある場合、預金者による警察への被害届の内容について、金融機関が警察に照会できる仕組みを構築するなど、被害偽装防止策について警察・金融機関間の具体的協力関係を検討し、何らかの取決めを締結すべきではないかとの意見があった。

（以上）

（別添５）

各金融機関におけるＡＴＭシステムに関するセキュリティ対策の概要

銀行法第 24 条により提出を求めた「偽造キャッシュカード犯罪緊急対応方針」等及びその後のフォローアップにより、各金融機関におけるＡＴＭシステムに関するセキュリティ対策を取りまとめたところ、状況は以下のとおり。

（注１）　キャッシュカードを発行している全民間金融機関約 1,800（民間金融機関とは、銀行、信用金庫、信用組合、労働金庫、農水系統金融機関。このうちＡＴＭを保有している民間金融機関は約 1,600）を対象に調査を実施。

（注２）　計数は全民間金融機関合計（カッコ内は銀行合計）

① 利用限度額の引下げ

- 引出し限度額の一律引下げ（予定を含む）　　９１％（９０％）
  銀行のうち、対応済みのものをみれば、引下げ後の利用限度額は 100 万円超 200 万円以下が全体の８割。
- 個別利用限度額の設定可能（同上）　　６８％（９４％）
  なお、銀行について、対応済みのものをみれば、設定可能上限額は 500 万円超が全体の４割、100 万円超 200 万円以下が全体の３割。

② ＩＣキャッシュカード化

- ＩＣキャッシュカードの導入（予定を含む）　８％（３９％）
  なお、主要行（都市銀行、長期信用銀行、信託銀行、外国銀行等）及び地方銀行に限れば４８％が対応済み又は対応予定。
- ＩＣキャッシュカード対応ＡＴＭ（対応予定として回答のあった予定台数を含む）　１５％（１９％）
  なお、主要行に限れば、２６％が対応済み。

③ 生体認証

- 生体認証の導入（予定を含む）　　５％（１７％）
- 方式（同上）　手のひら静脈４８％、指静脈３０％、未定２２％

④ ＡＴＭ稼働時間中の出金停止

- ＡＴＭ稼働時間中の出金停止（予定を含む）　９３％（９９％）
- ２４時間受付体制　８％（３０％）

⑤ 類推されやすい暗証番号の使用防止

- 啓発ステッカー等の貼付（予定を含む）　９３％（９３％）
- ＡＴＭ画面での啓発（同上）　３２％（７４％）
- ＡＴＭでの暗証番号変更機能の搭載（同上）　８６％（９５％）

⑥ ＡＴＭ画面覗き見防止策

- 覗き見防止フィルムの貼付（予定を含む）　６４％（９５％）

⑦ 異常取引検知システムの導入（予定を含む）　３３％（６１％）

⑧ 預金者への対応の徹底

- 被害者への対応マニュアル策定（予定を含む）　９％（５１％）

（以上）