■11 群（社会情報システム）－ 7 編（金融情報システム）

1 章 金融情報システムの概要

（執筆者：岩下直行）［2009 年 3 月 受領］

■概要■

一般に，「金融業務」とか「銀行業務」というと，堅苦しく古めかしい伝票と帳簿のイメージが強い．しかし，近年の情報技術革新の影響を受けて，金融業務と金融機関は大きく変化してきており，従来のイメージでとらえることは正確ではなくなってきている．実際，現在の金融機関における金融取引の実務は，各種の金融情報システムによって支えられている．

金融情報システムとは，金融機関及びその関連組織が開発し，あるいは利用している，金融取引を行うための各種の情報通信システムのことである．一般の人々にも身近な小口の金融情報システムとしては，銀行の現金自動預入支払機（ATM：Automated Teller Machine），商店の店頭に置かれた電子マネーやクレジットカード決済用の端末装置，あるいはインターネットや携帯電話を通じた銀行取引や証券取引のためのシステムなどがある．

これに対し，金融機関の内部には，本支店間や同業他社の金融機関との間を接続する様々なコンピュータ・ネットワークが張り巡らされ，そこに様々な業務システムが接続されている．世界的な情報通信ネットワークが発達し，国内と海外の金融市場の統合化が進んだ結果，国際的な金融取引がリアルタイムで行われるようになった．今や，大口の金融取引も，マーケット情報の収集，注文，成約，決済といったすべての段階において，金融情報システムに全面的に依存するようになっている．

こうした金融情報システムは，ほかの情報システムに比べて，機密性，完全性，可用性などの情報セキュリティ確保に対する要請が強い．従来，金融情報システムでは，巨大なコンピュータ・センターや専用回線を用いてシステムを外部から隔離することによりセキュリティを高める戦略が主流であった．しかし，最近では，インターネットが普及し，通信ネットワークがオープンなものとなってきたため，暗号技術，IC カード，バイオメトリクス認証など，最新の情報セキュリティ技術を活用することで，セキュリティ確保の要請に応える方針に変わりつつある．金融機関にとって，優れた情報セキュリティ技術を選択し，それを適切に使いこなしていくことが，極めて重要な時代となってきているのである．

本章では，金融情報システムの概要を説明するとともに，金融情報システムにおける情報セキュリティの重要性について述べる．

【本章の構成】

本章では，1-1 節で，本編で検討の対象となる金融情報システムについて概説する．1-2 節では，金融機関における情報セキュリティ対策の現状について分析する．1-3 節では，金融情報システムの情報セキュリティを考えるための導入として，社会問題化した偽造キャッシュカード問題とその後の対応について述べる．

■11 群 － 7 編 － 1 章

1-1 金融機関の情報システムの現状

1-1-1 金融情報システムの分類

金融情報システムは，金融機関の業務に使用されるシステムであり，いくつかの視点から分類することができる．

まず，金融業という産業は，制度上，いくつかの細分化された業種によって構成されている．主要な業種としては，銀行業，金融商品取引業，保険業，貸金業などがあげられる．金融業は，顧客の財産を預かって運用したり，資金を貸し出したり，投資の助言を行ったりする業務を行っている関係で，その業務の健全性に対する要請が強い．このため，各業種における業務内容は法律によって規制されており，兼業を制限されていることも多い．金融情報システムも，こうした規制の影響を受ける．例えば，銀行業，金融商品取引業，保険業における情報システムは，各々別のものと理解されており，業務上，相互に接続されることもほとんどない．この結果，金融情報システムは，銀行の情報システム，証券会社の情報システム，保険会社の情報システム等々に区分されることになる．

ただし，情報システムの技術的な分析を行う観点からは，こうした金融制度に基づく区分はそれほど重要なものではない．各情報システムの担い手は異なるものの，利用している技術の多くは共通だからである．以下の記述は，主として銀行の情報システムが中心となるが，これは様々な金融情報システムの代表として取り上げるもので，証券会社や保険会社など，銀行以外の業態の情報システムにおいてもほぼ共通の特徴があるものと理解されたい．

これとは別の視点の分類としては，取引の相手先として誰を想定するか，に着目する方法がある．金融業界の主要企業の多くは，銀行であれ，証券会社であれ，保険会社であれ，大口顧客から小口顧客まで幅広いレンジを取引先としている．同一の金融機関であっても，個人を取引相手とする業務と，大手企業や同業者を取引相手とする業務は，その形態がかなり異なる．このため，情報システムも，想定している取引相手先によって異なることになる．

例えば，銀行の情報システムについてみると，小口顧客を取引対象とするリテール・バンキングと呼ばれる銀行業務には，キャッシュカードによる ATM 取引，クレジットカード，デビットカード，電子マネー，インターネット・バンキングといったものが含まれる．一方，大口顧客や同業者を取引対象とするホールセール・バンキングと呼ばれる銀行業務には，短期金融市場，株式・債券市場，外国為替市場での取引や，国際的な金融取引が含まれる．各々の業務において利用される情報システムも異なる．なお，こうした対外取引のほかに，金融機関の社内に閉じた業務で利用される情報システムも存在するが，それらの多くはほかの一般企業の社内向けシステムと大きく変わることはないため，以下では特に言及しない．

リテール・バンキングは，大量の小口顧客との間で効率的な取引を行うために，カードや ATM など，金融業に独特な情報システムを利用している．こうしたリテール・バンキング用システムは，人々の生活の場でも広く利用されており，その特殊な形態から，典型的な金融情報システムとして広く認識されている．これに比べ，ホールセール・バンキングは限られたプロ同士の取引であり，外部からはみえない，隔離された情報システムとして運用されていることが多い．

1-1-2 銀行の資金決済系システム

それでは，具体的な金融情報システムの事例をみてみよう．金融機関は，業界内の企業・組織との間で，資金決済や証券決済に関するデータの授受を行うことによってその業務を進めているが，その際に金融機関間の情報ネットワーク・システムが極めて重要な役割を果たす．そこで，以下では，金融機関相互を接続する伝統的な金融情報システムの典型として，銀行の資金決済系システムを取り上げる．

図 1･1 は，我が国の銀行における資金決済系システムの情報ネットワーク・システムの構造を示したイメージ図である．ここには，①日銀ネット，②全銀システム，③統合 ATM という異なる三つの金融情報システムが描かれている．

日銀ネットは，日本銀行とその取引先金融機関との間の資金や国債の決済をオンライン処理することを目的として構築されたネットワークであり，我が国金融取引の決済における中核的な役割を果たしている [1),2)]．

全銀システムは，個人や企業が金融機関に振込みを依頼した場合に，金融機関同士が決済を行うための仕組みである．同センターでは，金融機関における個々の支払指図を送受信するほか，これらを集計して金融機関ごとに受払差額を計算し，その結果を日本銀行にオンラインで送信する．この送信結果に基づき，各金融機関が日銀ネットで最終的な決済を行う [3)]．

統合 ATM は，金融機関の ATM 取引における相互乗り入れを可能とするためのシステムである．都市銀行，地方銀行などは，直接，統合 ATM センターに接続し，信用金庫などは業態別センター経由で接続している．各金融機関の ATM に入力された提携カードによる預金引出しなどの取引電文は，統合 ATM センターを経由して送受信される．同センターでは，受払差額を計算し，全銀システムを通じて請求され，日銀ネットで最終的に決済される [3)]．

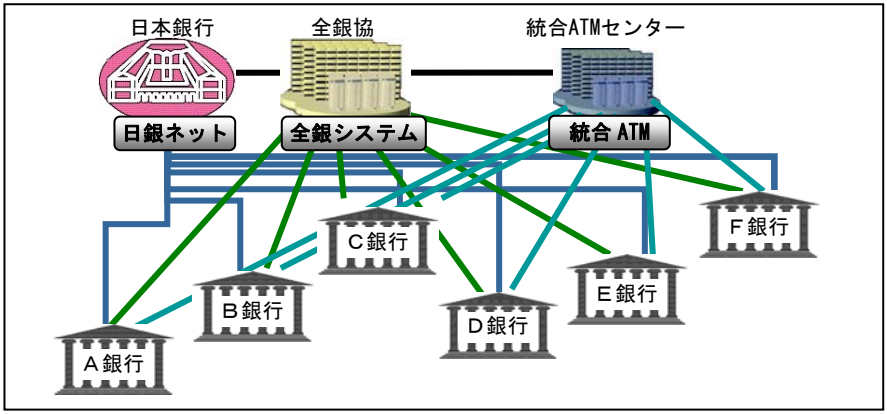

図 1・1　我が国の金融機関間のネットワーク構造（銀行の資金決済系システムの例）

このイメージ図に描かれているように，各銀行は各システムのセンターとデータを送受信するために，物理的に異なる通信回線を利用して接続するようになっている．これは，各々の金融情報システムが固有のセキュリティ･ドメインをもっているため，それに対応してネットワークを閉域に保つことにより，セキュリティを確保しようという考え方だからである．

■11 群 － 7 編 － 1 章

1-2 金融機関における情報セキュリティ対策

1-2-1 金融機関と情報セキュリティ

金融業界は，コンピュータによるネットワーク・システムを最も早い時期に整備した業種の一つであった．1970 年代に開発が進められた第二次オンライン・システムは，金融機関内部の事務を飛躍的に合理化し，現在の金融機関による決済サービスの原型を形作った．前節で紹介した銀行における資金決済系システムは，その流れを受け継ぐものである．現在利用されているキャッシュカードの磁気ストライプの形状や，CD/ATM の基本構造は，この第二次オンライン以来，30 年間以上にわたって維持されてきたものである．

1990 年代にインターネットが普及する前は，コンピュータ・ネットワークといえば真っ先に金融機関のオンライン・システムがあげられる存在であり，その頑健性，安全性に疑いが差し挟まれることはほとんどなかった．金融機関は，頑丈な建物や金庫によって守られるその物理的なセキュリティと同様に，情報システムのセキュリティについても，十分な安全性が確保されていると信じられてきた．

しかし，インターネットが普及し，一般の人々も情報通信ネットワークを様々に活用する時代になると，従来型の金融情報システムを墨守していくことが最適な戦略とは限らなくなってくる．実際，2003 年から 2004 年にかけて，偽造キャッシュカードで不正に預金が引き出される事件が急増すると，大きな社会問題となった．その後も，スパイ・ウェアやフィッシング詐欺メールなど，金融機関とその利用者を脅かす新手の金融ハイテク犯罪の手口が次々に出現し，利用者が実害を被る事例も相次いでいる．

こうした環境変化を受けて，今日では，金融機関が利用者にサービスを提供する際には，情報システムを活用することが不可欠となっている．そうした状況下において利用者からの信頼を維持するためには，無権限者による不正取引や個人情報漏えいが発生しないように情報セキュリティを適切に管理し，それを積極的にアピールしていくことが必要とされている．既に，多くの金融機関が，インターネットのホームページに，自行の情報セキュリティが万全であることをアピールする説明文を掲載している．情報セキュリティの管理体制について，第三者機関から評価・認定を受ける金融機関も増えてきている．

1-2-2 安全対策から情報セキュリティへ

金融機関のシステム開発・運用の現場において「情報セキュリティ」というカタカナ語が普及したのは，比較的最近のことである．もちろん，それ以前から，金融機関にとって不正防止や個人情報保護が重要でなかったわけではないが，かつては「安全対策」という用語が一般的であった．例えば，1984 年には，大蔵省銀行局長による最初の機械化通達（昭和 59 年蔵銀 1234 号）が出状されたが，その事務連絡のなかで，「安全対策については，コンピュータシステムの事故防止，取引者のプライバシー保護対策等に万全を期するための諸措置を講じさせる」ことが要請されている．1985 年には，金融情報システムセンター（FISC）の「金融機関等コンピュータシステムの安全対策基準」の初版が発行されている．そのような公式な日本語表現が用いられていたにもかかわらず，その後，カタカナ語が主流となったのはな

ぜだったのだろうか.

辞書的な説明になるが,「安全」を意味する代表的な英単語には,セキュリティとセイフティの 2 種類がある.セキュリティという単語は,警備員を指し示す場合にも用いられるように,単に安全な状態を意味するだけではなく,外敵からの攻撃を防御する手段という意味ももつ.これに対し，セイフティという単語は，自動車のシート・ベルトをセイフティ・ベルトと呼ぶように，不慮の事故や不注意による被害を予防するための手段という意味ももつ．日本語で「安全対策」,「安全装置」といった表現を用いた場合は，どちらかというとセイフティの意味合いが強く出るようである.

かつての金融情報システムは，企業内，業界内に閉じたクローズドなネットワーク・システムであった．巨大なコンピュータ・センターに大型汎用機を並べ，支店，ATM との間を専用回線でつなぐことによりシステムを外部から物理的に隔離すれば，システム全体を安全に保つことが可能と考えられていた．リテール・バンキングにおける顧客の認証も，磁気ストライプカードと 4 桁暗証番号の照合のみという素朴な認証方式が主流であった．暗号，電子認証，IC カードなどの情報セキュリティ技術はほとんど利用されていなかったが，特に先端技術を導入しなくても一定の安全性が期待できる環境にあり，利用者が金融ハイテク犯罪の被害者となることはほとんどなかった.

そのような状況においては，金融機関の情報システムが抱える主要なリスクは，システム開発時の人為的なミスなどに起因するサービスの停止や,不注意による情報漏えいであった.金融機関に求められていたのは，システム開発と運用を確実に管理するとともに，機器類の物理的な保護を行うことであった．そういう対応について,「安全対策」という用語が用いられたことは自然であっただろう.

こうした「安全対策」が「情報セキュリティ」へと変わったのは，1990 年代後半におけるインターネットの普及と電子マネーへの関心の高まりによるものであった．それまで情報システムの閉鎖性を安全のよりどころとしてきた金融機関においても，利用者の利便性と金融機関の効率化のために，新しいオープンな通信インフラを利用する動きが出始めた．金融情報ネットワークのオープン化が進められると，従来と同じ素朴な認証方式のままでは安全性が確保できない．物理的に外部とつながった環境においては，外部からの不正な侵入者・攻撃者を，暗号，電子認証，IC カードなどの情報セキュリティ技術によって迎え撃つ必要がある．インターネット・バンキングにおいては，暗号通信プロトコルによって暗証番号や取引内容の機密を保護する必要が生ずる．電子マネーを実現するためにも，暗号や IC カードの技術は必須である.

このようにインターネット上での金融サービスの提供が進むにつれて,金融機関の対応は,不慮の事故を防ぐことを主眼とした「安全対策」から，外敵からの防御を主眼とした，より高度な対策として,「情報セキュリティ」に変化した．つまり，金融情報システムのオープン化に伴い，目的も手段も変化したために，よりふさわしい名称として,「情報セキュリティ」というカタカナ語が主流となり，それが現在も続いているのである.

■11 群 － 7 編 － 1 章

1-3 偽造キャッシュカード問題とその後の対応

1-3-1 偽造キャッシュカード問題の発生

我が国の金融機関における情報セキュリティの位置づけを考えるうえで, 2004 年から 2005 年にかけて発生し，社会問題化した「偽造キャッシュカード問題」を避けて通ることはできない.

2002 年以前はほとんど発生していなかった偽造キャッシュカードによる不正預金引出の被害は，2003 年度から急増し，2004 年度には 10 億円に達した．2005 年 1 月に，ゴルフ場の貴重品ロッカーからキャッシュカードを盗み出してスキミングする手口で不正に預金を引き出していたグループが逮捕され，その手口が大きな扱いで報道されると，テレビの報道番組や雑誌記事が相次いで被害の深刻さを伝え，金融機関の対応を批判する声が相次いだ．この問題を受けて, 2005 年 8 月に預金者保護法が成立し, 2006 年 2 月から施行された. この結果，偽造・盗難カードによる不正預金引出に伴う被害については，原則として金融機関が被害者に補償を行うこととなった.

偽造キャッシュカードによる不正な預金引出の急増は，金融機関が長年培ってきた業務面の信頼を大きく損なうものであった．とはいえ，偽造キャッシュカードの被害額は最高でも年間十億円程度であった．偽造クレジットカードの被害額がピーク時（2002 年）に年間 165 億円に達していたことや，過去に発生した何種類かのプリペイドカードの偽造犯罪の被害額が各々数百億円に及ぶと推定されているのに対して，特に規模の大きいものとはいえない．しかし，クレジットカードやプリペイドカードの偽造事件では，主としてカード発行業者，システム運営者が損失を被り，消費者に被害が及ばなかったのに対し，偽造キャッシュカード事件では，不正に預金が引き出された預金者個人にまず損失が発生し，被害補償も後手に回ってしまった．このため，預金者の誰もが被害者になり得ると受け止められ，一般の人々も不安を募らせることとなった.

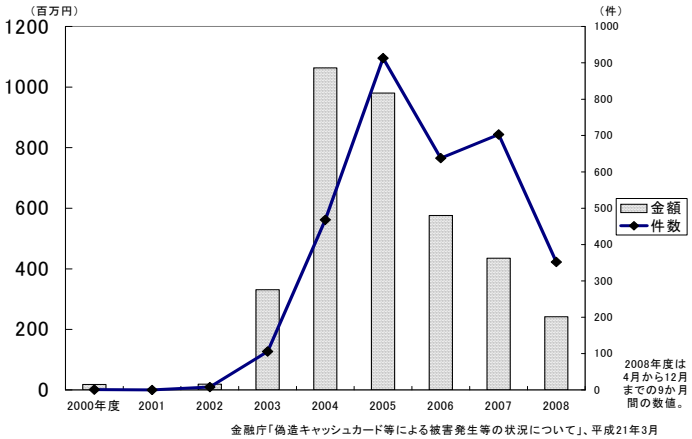

図 1・2　偽造キャッシュカードによる預金等払戻しの被害金額・件数の推移

1-3-2 偽造カード問題の被害沈静化の原因と今後の対応

その後，偽造キャッシュカードの被害は，2006 年度には件数，金額とも大幅に減少し，2007 年度以降も被害額は低水準で推移している．偽造キャッシュカードによる不正預金引出の被害額が減少したのは，金融機関が講じてきた様々なセキュリティ対策が奏効したものと考えられるが，それらのなかのどの対策が有効だったのだろうか[4]．

最も有効だったと考えられるのは，2004 年頃から各金融機関が進めてきた，キャッシュカードの利用限度額の引下げである．この対策は，業態を問わず，ほぼすべての金融機関で実施されてきた．偽造キャッシュカードが問題となる以前は，1 日当たりの限度額は数百万円に設定されていたが，現在では，IC カードや生体認証を利用した取引を除けば，1 日当たり 50 万円程度とすることが一般的となっている．この対策が直接的に，1 件当たりの平均被害額の低下に寄与し，被害金額を引き下げていることは明らかであろう．また，犯罪者の立場からみたとき，ATM で偽造キャッシュカードを使って預金不正引出を行うという，最もリスクの高い行為の「実入り」が，最大でも 50 万円程度に下がり，カード偽造自体が「割に合わないビジネス」となった．このことが被害件数を減少させ，相乗効果で被害が沈静化したものと考えられる．

更に，報道などを通じて利用者の間で偽造カード被害に関する認知度が上がったことや，金融機関が利用者に積極的に警告を発した効果により，利用者がカードや暗証番号を慎重に取り扱うようになったことも有効であったと思われる．

これに対し，IC カードや生体認証などの予防対策が被害の減少に大きく寄与したとは考えにくい．2008 年 3 月末時点の調査では，IC キャッシュカードはすべてのキャッシュカード発行枚数の 5.6%（うち，生体認証対応は 3.1%）しか普及していないからである[5]．

生体認証対応の IC カードを利用していても，不正預金引出の被害に遭わないで済むとは限らない．現段階で発行されている IC キャッシュカードのほとんどは，提携先 ATM での利用を可能とするために，IC カードに磁気ストライプが貼付された併用カードとなっている．多くの提携先 ATM では，生体認証機能も IC による認証もない通常の磁気ストライプカードとして認識されるため，磁気ストライプ部分のみを偽造して不正に利用することが可能なのである．

磁気ストライプカードと 4 桁暗証番号という脆弱な個人認証メカニズムを利用している限り，偽造カード犯罪の根が絶たれたわけではなく，新しい犯罪の手口を常に警戒していなければならない．全面的な IC カードへの移行など，より抜本的なセキュリティ対策の検討を進める必要性が高まっているように思われる．

1-3-3 これからの金融情報システムのセキュリティ対策のありかた

銀行の実務に利用されているシステムのなかには，かつてセキュリティに対する意識があまり高くなかった時代に導入されたシステムがそのまま残ってしまっていることがある．磁気ストライプカードと 4 桁暗証番号による預金引出，カード番号と氏名を SSL 入力するだけのクレジットカード取引など，今日的な情報セキュリティの水準を満たさないシステムが広く普及してしまっている．かといって，これらをすべて再構築するわけにもいかない．さし当たっては，運用面も含めた対策により不正取引の防止に努め，もし不正取引が発生してしまったら，その被害を限定することに努めていくしかない．

しかし，こうした古いシステムは，時代の流れとともに，いずれは新しいシステムに置き換えられていくはずである．次世代のシステムに移行したときに，そのシステムのセキュリティのレベルが低いままとなってしまうことは，是非避けなければならない．この観点からは，次世代のシステムのセキュリティについて，最新のセキュリティ技術に関する知見に基づく理論的な警告についても対応を検討していかなければならない．

実際，偽造キャッシュカード問題については，現在の段階では，偽造による不正預金引出のリスクが相対的に高い磁気ストライプカードと 4 桁の暗証番号が主流であるから，そのセキュリティのレベルがどの程度であっても，IC カードや生体認証を導入しさえすれば改善といえる．IC カードや生体認証のなかにも，耐偽造性やなりすまし攻撃への対策が進んでいるものとそうでないものがあるが，そのなかからどれを選んだとしても，さしあたっては，現在の磁気ストライプよりは改善となるからである．しかし，だからといって，セキュリティに問題のある IC カードや破られやすい生体認証の実装技術を選択してしまった場合，新旧の技術が共存する期間が過ぎて次世代の技術が主流となったときに，問題点が顕現化してしまう．特に，金融業界が一斉にある新技術を導入する場合においては，将来を見据えた選択が可能となるように，セキュリティにかかる十分な検討を行っておく必要があるだろう．

情報セキュリティ対策というのは，過去に発生した問題について後追い的に対応するだけでは駄目で，ある程度先を読んだうえで検討していくことがどうしても必要になる．世間の常識と同じレベルのことをやっていたのでは，対応が遅いといわれてしまうし，問題が生じてから対策を講じるまでのタイムラグを考えても，ある程度，将来発生する問題を予測しながら対策を講じていくことが必要となる．そのような予測を的確に行うためには，アカデミックな最新の研究成果を意識し，その情報を活用していくことが重要であろう．

情報セキュリティに対する関心の高まりは，金融情報システムのオープン化の帰結であった．こうしたシステム技術面の変化が更に続いていった場合，金融機関はどのような影響を受けるのだろうか．

かつて，金融機関がレガシー系の技術で等質の情報システムを維持していた時代には，「金融機関のシステムであれば，どれも安全で信頼できる」という意味で，業界全体としてのブランド化が達成されていた．オープン系の安価な技術を導入せず，高価なレガシー系システムを使い続けることにより，そうした「業界ブランド」が維持できてきたと考えられる．

現在，インターネット・バンキングのセキュリティ向上や IC カード，生体認証などへの投資を行っているのは，個別企業として，安全性，信頼性のブランドを向上させたいと希望する金融機関のようである．他方，そうした個別ブランド化を志向しない金融機関は，情報セキュリティ対策に，人的，システム的な投資を多くは振り向けていない．当面の間は，そのような投資判断でも特段の問題は発生しない．むしろ，過去からの慣性として，金融機関であればどこでも安全で信頼できるという「業界ブランド」が維持されている状況であれば，新しい技術にチャレンジせず，現状維持としていた方が短期的には効率的かもしれない．

しかし，今後，金融情報システムのオープン化が更に進むなかで，金融機関の一部がシステムの現状維持を選択してしまうと，安全性，信頼性の観点から，業界全体のブランドが維持できなくなるおそれがある．金融機関のシステムは相互に連携して機能するものであるため，個別企業のシステムだけが優れていても，全体としては利用者の安全を守ることはできないからである．

こうした観点から考えれば，現在進められているセキュリティの高度化は，広く業界全体が対応していかなければならない課題と受け止めるべきであろう．今後，金融情報システムの情報セキュリティを高度化していくためには，専門性をもった人材の育成と業界内での適切な情報共有が必要であり，金融業界全体としての積極的な取組みが求められているのである．

■参考文献

1) 日本銀行金融研究所，“新しい日本銀行―その機能と業務（増補版），”有斐閣，2004.
2) 日本銀行，“決済システムレポート 2007－2008，”日本銀行，2008.
3) 金融情報システムセンター，“平成 21 年版金融情報システム白書，”金融情報システムセンター，2008.
4) 金融庁，“偽造キャッシュカード等による被害発生等の状況について，”金融庁，2009.
5) 金融庁，“偽造キャッシュカード問題等に対する対応状況（平成 20 年 3 月末），”金融庁，2008.