

第3章 安全対策の現状と課題（別添資料2）

1 利用者と真正なクレジットカード会員の同定～本人認証

（1）サインの照合

サインの照合は、クレジットカード利用の基本的な原則であるが、サインになじんでいない日本的慣習もあり、必ずしも履行率が高いとはいえない状況である。現在までに、クレジットカード裏面の署名欄のサインの履行については、日本クレジット産業協会を中心としてクレジットカード会社によるサイン照合徹底キャンペーン等も継続して行われている。IC (Integrated Circuit) カード化以降においても、暗証番号によらない取引については重要な意味を持つことから、関係機関の努力により、更なる徹底が期待される。

（2）無効カードのチェック

加盟店において、クレジットカード会社の保持している無効（盗難・遺失）カードのデータベースシステムとのチェック方法としては、

- ・クレジットカード会社からデータベースを加盟店に配信し、加盟店でチェックする。
- ・加盟店からカード情報をクレジットカード会社に送信し、クレジットカード会社においてデータベースでチェックする。

という2つの方法がある。

前者の方式では、今後は後者の方式に移行していくことが望ましいが、クレジットカードの利用頻度、照会時間の制約等により、前者の方式を採用している業界では、紛失・盗難発生時から即時に不正使用されるという犯罪の態様に鑑み、適宜の情報登録が可能な対応が重要である。また、加盟店で保有するデータベースの量も十分に確保される必要がある。

ただし、データベースに登録されていなければ、チェックを行うことができないので、クレジットカード会社への届け出の受付と届け出がなされた時点で速やかにデータベースに登録する仕組みが必須である。

オンライン化については相当数進んできているが、オンラインシステムが導入されていない加盟店について、オンライン化を進めて、全件オンラインオーソリを実現することが望まれる。

（3）写真入りカードについて

写真入りカードの採用は、紛失・窃取事案に関しては、目視による本人確認が容易になり、不正使用者に対する牽制効果を有しており、不正防止にかなりの効果があるものと考えられる。

また、偽造に関しても、写真があることで偽造自体に対する牽制効果はあり、また電話照会時にも写真の有無のみで容易に偽造カードか否かが判別できる利点もあることから、ある程度の効果は有するものと思われる。

写真入りカードについては、必ずしも利用者が望まないといった点や海外で発行されたカードについて限界を有すること、一部のカードだけの採用ではその効果が十分に発揮できないこと、コストがかかること、作成手続きに若干の手間がかかることといった点はあるものの、上記のような不正防止効果を考えると、今後、消費者ニーズを勘案の上、普及促進について検討されることを期待する。

(4) その他

ア 売上票に印刷されたカード番号とカードに打刻された番号の照合

偽造カードでは、磁気データはスキミングを行ったものをそのまま利用しているため、真正なカード番号となっているが、クレジットカード券面に打刻された番号については、そのスキミングデータを解析した番号を打刻する必要があり、打刻ミスなどにより、それらの番号の相違したままの偽造カードも用いられている。従って、加盟店において、売上票に印刷されたカード番号（磁気データの番号）とクレジットカードに打刻された番号の照合を行うことによって、これらの偽造カードの利用を未然に防ぐことができる。

イ クレジットカード会社への電話連絡（ボイスオーソリ）の活用

加盟店からのオーソリは、機械で行う場合と、機械が設置されていない加盟店の場合や機械で行った結果としてクレジットカード発行会社に連絡する旨の表示が出た場合などに加盟店の店員が電話で連絡（ボイスオーソリ）を行うことがある。この電話でのオーソリを積極的に活用することで不審な利用を発見するきっかけとなるものと期待される。

ウ 氏名記載書類、特に写真入り I D (Identification) の活用による本人確認

クレジットカード利用時に、真正な利用者であることをチェックする仕組みとして、氏名記載書類、特に写真入り I D の提示を求めることは、盗難・遺失

によるクレジットカードの利用を抑制することができるだけでなく、偽造カードの利用も買い子のIDをも偽造する手間がかかることとなり、抑止効果が期待できる。ただし、加盟店でのチェックであるので、加盟店の協力体制と利用者の理解を得るための広報が重要である。

2 カード自体のセキュリティの確保～偽造防止対策

(1) カードの物理仕様上の対策

クレジットカード発行会社では、クレジットカードに対して以下のような偽造防止対策を施してきており、一定の効果は上げてきている。ただし、最近の偽造技術の高度化により一見して見分けることの難しい偽造カードが出てきていることから、その他の対策と合わせることで、総合的にセキュリティを高めていかなければならない。

ア 特殊エンボス文字の刻印

クレジットカード会社ごとのマークなどの特別の活字体の凸版の文字を刻印する。

イ ホログラムの貼付

クレジットカード会社ごとの立体写真印刷技術（ホログラム）の用紙を貼付する。

ウ 特殊素材を用いた署名欄

張り替えることが困難で、一旦記入した署名は消すことができない欄にする。

エ マイクロ文字の印刷

カラーコピーなどでは複写できない、作成には高度の印刷技術を必要とする文字を印刷する。

オ 偽造しにくい蛍光印刷

紫外線を照射すると浮かび上がる模様などを蛍光塗料で印刷する。

カ 偽造防止コード

クレジットカード発行時に、会員番号等から暗号演算によって算出した数字を磁気部分に追加することで、架空の会員番号を用いての偽造を困難とさせるものであるが、スキミングでは、この数字も複写されるため効果がなくなっている。

(2) ICカード化

ICカード化については、導入時期も含め関係各方面での議論が進展してきていることから、次章において、記述する。

3 磁気に係る偽造カードをターゲットとした対策

(1) カード券面への偽造に係る不正使用防止のための固有コードの印字

クレジットカード発行時に、会員番号等から暗号演算によって算出した数字を券面に印刷しておくもの。磁気部分を写し取るスキミングによってはこの数字がわからないのでこのコードを照合することにより偽造による不正使用が困難になる。このコードを本格的に活用するためには、システム面での整備がなされることが必要であり、現状ではボイスオーソリ時、インターネットでの利用時等に主に利用されるにとどまっている。

(2) 端末に係る対策

加盟店に設置されている端末からの情報窃取により偽造カードが作成される事案への対応のため、開封検出ラベルの上下ケースの合わせ目への貼付等の対策が講じられてきている。これに対して、巧妙にはがす或いは偽造シールを作成するなどによる犯行が生じ、これに対応するため、開封検出機構の導入やケースの強化が図られている。クレジットカード業界では、端末メーカーと、さらに耐タンパ性を向上させるための検討を行っている。

また、近時は携帯スキマーを利用した犯行も見られており、これらに関する情報の提供も含め、加盟店のスキミングに対する認識を高めるための施策の一層の推進と、端末の管理強化等がなされることが求められる。

(3) 利用パターン等の分析による不正利用防止策

利用パターン等の特徴を捉えて不正使用を早期に発見し、被害及び被害の拡大を防止するシステムが導入されつつある。

このシステムを有効活用するためには、情報の速やかなクレジットカード発行会社への集約のための全件オンラインオーソリ化の推進とリアルタイムでの取引管理の重要性が指摘されている。

このようなシステムの一層の普及と積極的な運用が期待される。

(4) その他

その他の施策として、磁気ストライプの磁気パターン解析システムとも言うべきものがある。これは、カード磁気部分の磁気粒子の並び方が、粒子レベルで見ると固有の並び方をしていることから、その並び方を解析し正当なカードとの同一性を判定するシステムである。現行の磁気カードを変更する必要はないが、端末装置に磁気粒子を読み取るヘッドを追加する点とカード発行会社で並び方のデータベースを持つ必要があり、海外で試行が行われている段階である。

4 クレジットカード業界による対策

急増するクレジットカード犯罪に対応するため、日本クレジット産業協会が平成12年7月に「業界における今後のクレジットカード不正使用の防止対策について」をとりまとめた。(別添資料3)

これは、次の4点を柱とするもので、関係業界・関係機関と連携しつつ対策を推進することとしており、こうした取り組みの成果が期待される。

- 1 安全性の高いクレジットカードの開発
- 2 ICカード化までの不正使用防止対策
- 3 カード会員に対する啓発活動
- 4 取締り当局への協力体制の確立

5 加盟店による対策

加盟店による対策に係る動向に関して、特に注目に値するのは日本百貨店協会の取り組みである。

日本百貨店協会においては、クレジットカードに係る問題について、従来からも「クレジット問題研究会」を中心に検討を進めていた。

平成12年には、これを発展的に改組し、「カードビジネス専門委員会」を常設の検討機関として設置し、「百貨店をカード犯罪の場にさせない」をスローガンに、問題に対応するための活動を積極的に進めていくこととした。

第1回のカードビジネス専門委員会は、平成12年6月30日に開催され、特に「カード不正使用問題」について最優先課題とし、百貨店として実施すべき具体的な防止策の立案に取り組むこととされた。

この成果として、9月には「百貨店におけるクレジットカード不正使用防止対策

ガイドライン～百貨店をカード犯罪の場にさせないために～」がとりまとめられ、日本百貨店協会の正式な自主基準として決定された。（別添資料４）

この「ガイドライン」では、次の３つの原則を掲げ、不正使用に対する強い姿勢を内外に示している。

- 一．百貨店は、サイン照合等クレジットカードの正しい取り扱いルールを徹底するとともに、これらに対する顧客への理解促進に努める。
- 二．百貨店は、カード会社の不正使用防止対策と連動し、全件オンラインオーソリ化の推進、信用照会端末の管理強化等、クレジット決済に関するセキュリティレベルの向上に努める。
- 三．百貨店は、社会的責務として、取締り当局等関係諸機関との連携を強化し、実効性ある不正使用防止体制の確立に努める。

そして、これに続き、制定の趣旨等を明らかにした後、

- １．店頭手続等に関するガイドライン
- ２．システムに関するガイドライン
- ３．非対面決済に関するガイドライン
- ４．連携・協力等に関するガイドライン

を掲げ、さらに具体的対応についても記述している。

日本百貨店協会では、これに加え、顧客に対しても協力を求めるための店頭掲示用の告知板・ステッカーの作成・掲示等の対策も行っている。

先に見たように、百貨店においては、全体の不正被害が増加し、百貨店における売り上げも特に大きく減少していない状況下で、不正被害の減少をみているところであるが、これはこうした積極的な取り組みが成果を上げているものと考えられる。

6 不正利用防止のための広報・啓発

利用者に関しても、これまでの関係者の啓発活動により徐々に意識の高まりは見られるものの、依然として、家族・友人間で相互利用したり、クレジットカード裏面への署名欄への署名をしないなどのケースが見られる。こうした点に関し、利用者に対しては、上記のような例をはじめとする自らのセキュリティ管理の甘さに起因するリスク等について一層の理解を深めるような広報啓発活動を進めていく必要があると考えられる。

クレジットカード業界においても、利用者に対し、店頭において本人確認のための待ち時間等について理解を得るための「本人確認徹底のためのキャンペーン」を実施することとしている。また、類推しにくい暗証暗号の設定・変更の促進、カード犯罪情報の提供、クレジットカード管理上の義務等の広報を内容とするクレジットカードセキュリティ確保のための継続的な啓発活動を実施することとしている。

これに加え、関係業界、関係省庁、関係団体等による啓発・広報活動の推進も期待される。

7 その他

- その他の被害の防止対策として、C P P（Common Purchase Point：クレジットカード情報が窃取された可能性のある場所）で利用等されたクレジットカードの監視強化、早期の切り替え等の対応がある。また、こうした情報の活用のための一層の取り組みが期待される。

また、平成12年7月に日本クレジット産業協会がとりまとめた不正使用防止対策の前文においては、加盟店契約会社に対し、不正使用の防止依頼を行っても対応が不十分で継続的に不正使用が発生する加盟店に対して毅然とした対応をとることを求めている。こうした対応は、クレジットカードの不正使用を防止する上で大きな重要性を持つものと考えられ、これが推進され、効果をあげることを期待したい。

- なお、今後 I C カード化の推進等に伴い、クレジットカードにおいても P I N（Personal Identification Number）の入力等が必要となる。従って、P I N の管理が重要となるが、これに係る安全対策について、現在デビットカードにおいてとられている対策が参考になると考えられる。（別添資料5）

8 インターネット取引に係るクレジットカード利用の安全対策

インターネットでの消費者と販売店の決済手段としてクレジットカードは広範に利用されている。特に、インターネットの世界は匿名性が高いこともあり、一種の I D 的な機能をクレジットカードに係る情報が果たしている面もある。

一方、いうまでもなくインターネットはオープンネットワークであり、それだけにインターネット上での商取引についてはその安全性に関して高い水準が求められる。

インターネット上でのクレジットカードの利用に関しては、販売を行おうとする加

盟店とクレジットカード会社間の契約において、

- ・申し込み内容及び取引の許諾の加盟店からクレジットカード会社への通知
- ・通信の安全化対策
- ・暗号による取引要領の盗聴防止
- ・ファイアーウォールによる不正アクセスの防止
- ・取引自体の記録の保管

等を定め、その安全確保を図っている。

インターネット上のなりすまし等によるクレジットカード不正利用について、日本国内では今まで顕在化しているものはない。警察による検挙もこれまでのところ例はない。しかしながら、海外においては、

○利用者による不正として、カード情報を不正に入手してこれを悪用した例（他人のカード番号を不正に入手し、インターネットで商品購入や有料サイトの料金を支払うもの）

○事業者による不正として、偽加盟店による不正売り上げの例（偽の有料サイトを設置し、閲覧申込のあったクレジットカード会員に対して売り上げを上げるもの）が報告されている。

以下の表は、リスク源と防止対策及びクレジットカード会社による取り組みをまとめたものであるが、今後とも安全なネット上の商取引の確保のため、関係者が連携の上、認証システムの普及・迅速な被害拡大防止等不正事案への早期対応のための体制の整備等を図っていくことが重要と考えられる。

リスク源に対する防止対策とクレジットカード会社の取り組み

リスク源	防 止 対 策	カード会社の取り組み
情報の改竄、盗聴	・暗号化措置 ・ファイアーウォール ・加盟店従業員のアクセス管理	・加盟店管理、指導 ・会員啓発
なりすまし、取引否認	・認証機関による会員、加盟店認証	・認証システムの普及 ・全件オーソリ ・売上モニタリング