2005 年 4 月 22 日

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

（財）金融情報システムセンター

１．（財）金融情報システムセンター（ＦＩＳＣ）とは

FISC（The Center for Financial Industry Information Systems）は大蔵省（当時）の許可を得て、1984 年 11 月、金融機関、保険会社、証券会社、コンピュータメーカー、情報処理会社等の出捐によって設立された財団である。

金融情報システムに関連する諸問題につき、関係者相互の協力の下に、総合的な調査研究を行うとともに、金融情報システムに係る安全性確保のための施策を推進し、併せてこれらに関連する事業を営むことにより、民間活力発揮のための環境整備を通じて、我が国経済及び金融情報システムの円滑な発展に寄与することを目的としている。

その主要業務として、金融情報システムに係る安全基準の策定等による安全対策の推進がある。

２．ＦＩＳＣが刊行する情報セキュリティ関連のガイドライン等

ＦＩＳＣが刊行する自主ガイドライン等は、金融機関の情報セキュリティの業界標準として広く用いられている。

（１）金融機関等コンピュータシステムの安全対策基準
（初版 1985.12　第６版 2003.10　追補 2005.3）

（２）金融機関等のシステム監査指針　（初版 1987.7　第 2 版 2000.07）

（３）金融機関等におけるセキュリティポリシー策定のための手引書　（初版 1999.01）

（４）金融機関等におけるコンティンジェンシープラン策定のための手引書
（初版 1999.01　第２版 2001.10）

３.「金融機関等コンピュータシステムの安全対策基準（以下ＦＩＳＣ安全対策基準）」の概要

（１）制定の経緯

金融機関のコンピュータシステムは高い公共性および広汎性を有しており、業界の標準となるべき安全対策基準の必要性が認識されたことから、会員金融機関が取り入れるべきコンピュータシステムの安全基準をＦＩＳＣがとりまとめ、会員の代表者による審議を経て 1985 年 12 月に初版を発刊した。

各金融機関はＦＩＳＣ安全対策基準を参照しつつ、自社のコンピュータシステムの安全対策を実施することが期待された。

その後継続的に見直しを行い 2003 年 10 月に第６版を発刊し、2005 年 3 月に個人情報保護法の全面施行に対応して一部基準を見直して第６版追補とした。

なお、金融庁の検査マニュアルにおいても、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、ＦＩＳＣ安全対策基準等に基づき行うものとされている。

（２）対象領域

①. 金融機関の以下のコンピュータシステムについて設備面、運用面および技術面から安全対策について記述

・顧客にオンラインサービスを提供するコンピュータシステム
・他の金融機関等との決済業務に使用するコンピュータシステム
・顧客データを扱うコンピュータシステム　等

②. すなわち銀行、信用金庫、信用組合や生命保険、損害保険、証券会社等の金融機関がサービスを提供するのに必要なコンピュータシステム全般が対象

③. なお、コンピュータメーカや情報処理会社等も金融機関に情報システムを提供するのに本基準を参照している。

（３）ＦＩＳＣ安全対策基準の適用状況

ＦＩＳＣでは金融機関におけるコンピュータシステムの安全対策実施状況の調査をＦＩＳＣ安全対策基準に照らし合わせて隔年で実施している。

調査はアンケート形式で実施され、毎回約６００の有効回答を得てその結果は金融機関等への啓蒙や安全対策基準の改訂に活用されている。　【図表１-1,2 参照】

【参考】安全対策基準の実施状況

	90%以上	90～80%	80～50%	50%未満	合計
必須項目	１６１	４６	２８	0	２３５
推奨項目	１８	１６	２５	5	６４

（2003 年 3 月 31 日現在）

（４）これまでの改訂状況

ＦＩＳＣ安全対策基準は制度変更や技術革新を反映し随時改訂されている。

【改訂履歴と最近の主な改訂内容】

初版策定　　１９８５年１２月

第２版　　１９９１年２月

第３版　　１９９８年７月

第４版　　２０００年７月

第５版　　２００１年９月

第６版　　２００３年 10 月

・情報セキュリティに関する経営層の関与のあり方

・業務継続計画

・アウトソーシングの進展に対応したマネジメント

第６版追補　　２００５年３月発刊

・個人情報保護法に対応した情報管理

・生体認証情報の管理

（５）改訂のための委員会構成

安全対策専門委員会とその実務組織としての安全対策基準検討部会とで審議

①. 安全対策専門委員会

安全対策の推進を目的とした常設委員会で、金融機関等のコンピュータシステムの安全確保に係る諸問題の審議、承認を実施

メンバーは、金融機関やメーカ等会員の代表者および学識経験者から構成

②. 安全対策基準検討部会

専門委員会の下部組織で、実務者を中心に構成

安全対策専門委員会で承認された改訂方針に則り、改訂項目、内容の具体的検討を実施

メンバーは、金融機関やメーカ等会員の実務担当者および学識経験者から構成

４．偽造キャッシュカード対策に関連した現行安全対策基準の主な記載内容

（１）カードの管理体制を明確にすること。

金融機関によるカードの発行や回収業務の安全性を確保するため、カードの発行・保管・交付・廃棄・暗証番号変更について記述

また、顧客への注意喚起についても記述

【記述例：抜粋】

○　カード発行依頼書に暗証番号が記入されている場合は、役席者が厳重に当該依頼書を管理することが必要である。

○　カードの発行

(1) カード発行時に暗証番号の登録が必要な場合は、暗証番号の漏洩防止に万全の措置を講ずることが必要である。

(2) 発行依頼書に基づき作成する場合の確認事項としては､以下のようなものが考えられる。

1)　発行カードの正当性(エンコード、エンボス内容)の確認

2)　発行カード枚数とカード発行依頼枚数の一致確認

○　カードの保管管理（省略）

○　カードの交付方法

顧客へのカードの送付は、原則として書留等受領の記録が残る郵便物により行い、発送管理簿等に記録を残しておくことが必要である。なお、やむを得ず営業店外で作成したカードを営業店で顧客に対し交付する際は、カード作成部署から社内書留等重要物件送付方法によりカードの送付を受け、十分な本人確認を行い、授受の明確化(受領書等の徴求)を行った後に交付することが必要である。

○　郵送返却カードの取扱い

書留等で郵送したカードが返送されてきた場合、役席者が保管管理簿等を用いて厳重に管理するなど、定められた方法で管理することが必要である。

なお、返却理由が「居所不明」のものは、原則として廃棄処分することが必要である。

○　廃棄方法（省略）

○　暗証番号の変更

顧客本人が暗証番号を安全かつ容易に変更できる方法を顧客に明示することが必要である。

暗証番号の変更の方法としては、以下のようなものがある。(以下省略)

○ 顧客への注意喚起

顧客からカードの発行依頼があった場合、他人に判り難い暗証番号を選定するように勧めることが必要である。また、カードを送付する際は、顧客に対し、カードの暗証番号等を安易に他人に教えないなどのカード管理、暗証番号管理の重要性の注意喚起を明示した文書を添付することが必要である。

（２）ＡＴＭ機器室の防犯措置を講ずること。

犯罪の未然防止と発生した場合の記録に役立てるため、防犯カメラやビデオの設置について記述

【記述例：抜粋】

○　自動機器室は一般に営業室から離れた場所に設置される場合が多いので、適切な防犯措置を講ずる必要がある。防犯措置としては、防犯ビデオ等自動機器室に対する防犯設備、および筐体強化用品等自動機器本体に対する防犯措置等を適切に組み合わせ、総合的に行う必要がある。

また、これら防犯措置により、端末機器の破壊、カードの不正使用、強盗等の犯罪の未然防止と、発生した場合の記録に役立てる必要がある。

○．自動機器室の防犯設備としては、以下のような例がある。

(1) 防犯カメラおよび防犯ビデオ

1) 図 1 のように、防犯ビデオにより出入口、自動機器室、および機械室の状況を撮影し、ビデオ装置で記録する。

2) 防犯カメラにより、出入口、自動機器室の状況を撮影、記録する。

3) 静止画像電送装置を設置し、閉店時の残留者確認等を管理センター等で行う。

なお、カラー画像の静止画像電送装置は細部まで監視でき、認識性を高めることができる。

4) 監視および録画ができ、少なくとも利用者の上半身の撮影を可能とする。異常発報時には自動的に高解像モードに切り替わるものが望ましい。デジタル方式の採用等解像度に配慮する。

（３）ＡＴＭ等無人化店舗の監視体制を明確にすること。

無人化店舗の異常状態を発見するため、管理センターでの監視や定期的巡回について記述

（４）コンビニＡＴＭの防犯措置を講ずること。

暗証番号等を覗かれにくくする対策について記述

【記述例：抜粋】

○　コンビニ ATM 利用時に後方や周りから暗証番号等を覗かれにくい設備としては、以下のようなものがある。

(1) コンビニ ATM の設置場所を、雑誌販売コーナー等の長居ができる場所の近くに設置しない。

(2) コンビニ ATM を雑誌販売コーナー等の長居ができる場所の近くに設置する場合は覗かれにくい設備とする。

○　コンビニ ATM 利用時に後方や周りから暗証番号等を覗かれにくい対策としては、以下のようなものがある。

(1) 間仕切り

(2) 画面の表示(視野角制限、表示画面の角度、フォントの大きさ、表示内容)

(3) 入力操作を隠す設備

（５）伝送データの漏洩防止

個人データを伝送する場合は暗号化等により盗聴されてもデータの内容が分からなくする措置を講ずること

【記述例：抜粋】

○ データ伝送時に盗聴された場合にもデータの内容が分からないようにするため、重要なデータについては、暗号化することが望ましい。特に個人データを伝送する場合には、暗号化・パスワード設定等データ伝送時に盗聴された場合にもデータの内容がわからないようにするための対策を講ずることが必要である。

また、個人データを伝送する場合には、上記以外の対策として、以下の条件を満たしセキュアな環境とすることで、光ファイバーの専用線を用いることも有効である。

(1) 建物内に不正な機器が接続されていないことの確認

(2) 切断検知時の報告の徴求およびその分析

○　オープンネットワークや無線を利用して重要なデータを伝送する場合は、通信事業者と協力するなど暗号化対策を図り、十分な漏洩防止対策を講じておくことが必要である。開発時のドキュメント、ソースコード等もその重要性に配慮した伝送方式を考えること。

○　なお、構内 LAN においては、ネットワーク構成機器への未承認機器の論理的・物理的な接続を不可能とする仕組みも有効である。

（６）カードの偽造防止対策を講ずること

カード犯罪を防止し､カードを利用したサービスを安全に提供するためのカードの偽造防止対策について記述

【記述例：抜粋】

○　カードの偽造防止対策としては、以下のようなものがある。

(1) 偽造を判別するためのコードの磁気ストライプへの記録

(2) 顔写真、ホログラム等の券面への印刷

(3) IC カード化等の高セキュリティ技術の導入

(4) カードへの有効期限設定やカードの更新等による高セキュリティ技術の対応

（７）不正アクセスの監視機能を設けること

CD・ATM 等カード取引においては、暗証番号を規定回数誤入力した場合、以後のカード取引を禁止

（８）事故口座の管理を行うこと。

顧客に提供したカード等の紛失、盗難時の受付体制について記述

【記述例：抜粋】

○　事故による不正使用を防止するため、顧客に提供した機器やカード等の紛失、盗難時の受付体制を整備し、すみやかに対応することが必要である。

事故届のあった口座の管理は定められた方法により行うことが必要である。

○　夜間、休日においても CD・ATM 等のサービス提供時間帯においては、例えば管理センター等において顧客からの紛失・盗難届けを受け付け、即時に支払停止等の処置を行う必要がある。

５．偽造キャッシュカードに対応した安全対策基準の改訂状況

（１）金融機関や協会等の対応状況収集

①．預金受入金融機関の協会へのヒアリング

②．有識者へのヒアリング

（２）偽造キャッシュカードの被害を防止するための対策とその網羅性の分析【図表２参照】

①．カード情報や暗証番号漏えいから被害発生までのシナリオを分析

②．上記場面毎に有効な対策を列挙

（３）現状の安全対策基準の見直しと対策を強化すべき事項の検討

①．暗証番号の覗き見防止策

ＡＴＭの設置場所の多様化に対応して、取引時の暗証番号覗き見防止策について検討する。

なお、覗き見防止策としては以下のものがある。

・間仕切り
・入力操作を隠す設備（手元覆いカバー等の装着）
・後方確認用ミラーの装着
・画面の視野角制限（覗き見防止フィルム等）
・画面の表示に工夫（表示画面の角度、文字の大きさ、文字の色合い等）
・画面上のテンキーの利用者に応じた配列方式

②．ＡＴＭの周囲に設置された不正機器の検知

カードの不正読取装置や隠しカメラによって、カード情報や暗証番号の詐取が懸念されることから、遠隔監視や巡回等によりこれらの不正機器の設置を阻止するよう検討する。

③．異常取引の検知

高額な引き出しが一定期間に引き続いて実施された場合等の異常取引の検知機能について検討する。

なお、異常取引の具体例としては以下のものがある。

・顧客の一般的な取引パターンから通常使用されない場所や時間帯での取引を検知
・一定時間内で急激に増加した取引を検知

また、異常取引検知時の顧客への通知方法等について検討する。

④．顧客から異常取引の届出があった場合の対応

従来の窓口対応ではカード紛失や盗難の届出があった場合に支払停止等の措置をとっていたが、顧客から口座残高異常等の届出があった場合についても状況によっては支払停止等の措置対象とするよう検討する。

また、朝のＡＴＭサービス開始直後の時間帯に偽造キャッシュカードによる引出しが集中していることから、ＡＴＭのサービス時間帯以外、特にサービス開始時間以前にも受付時間を拡大することについて検討する。

等

６．今後の対応

（１）安全対策基準を改訂し必要な対応策を普及・啓蒙する。

（２）安全対策上で継続調査が必要な箇所があれば引き続き調査していく。