デビットカードサービスの仕組みと現状

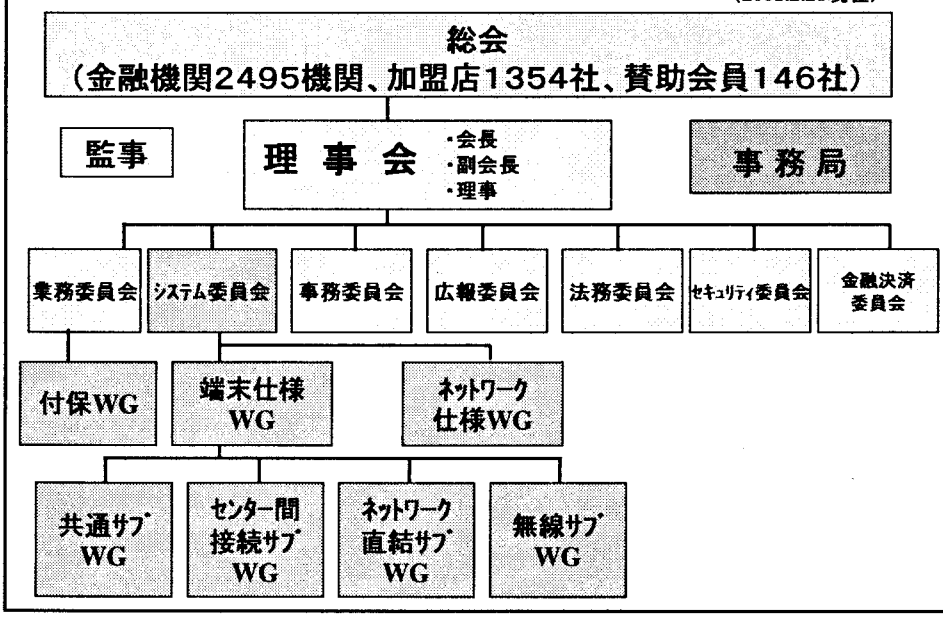
J-Debit

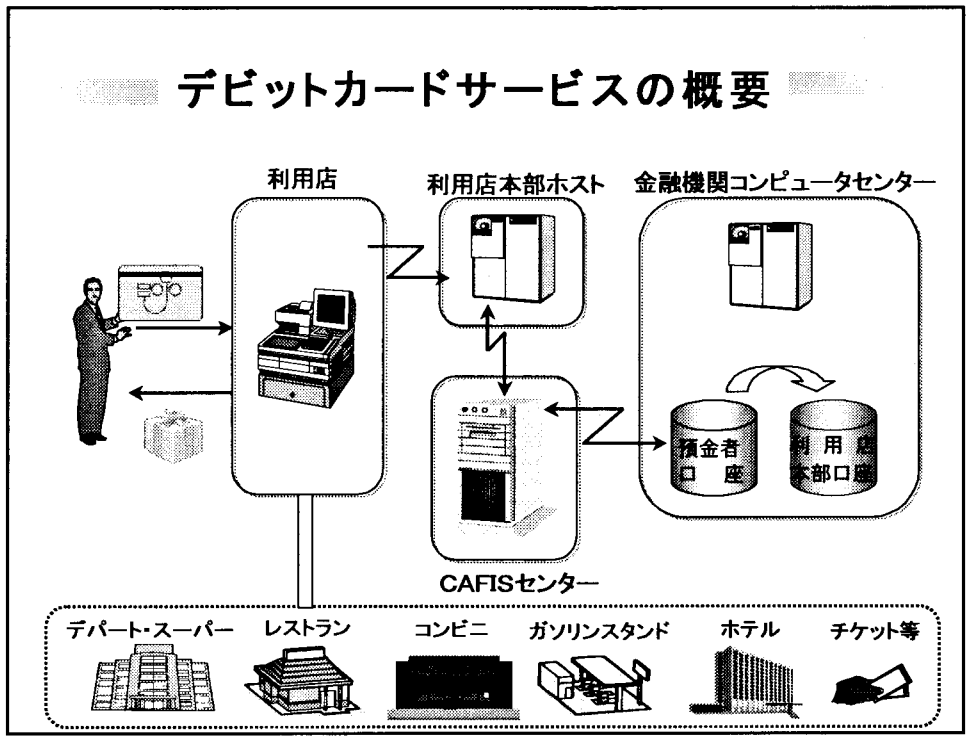
日本デビットカード推進協議会

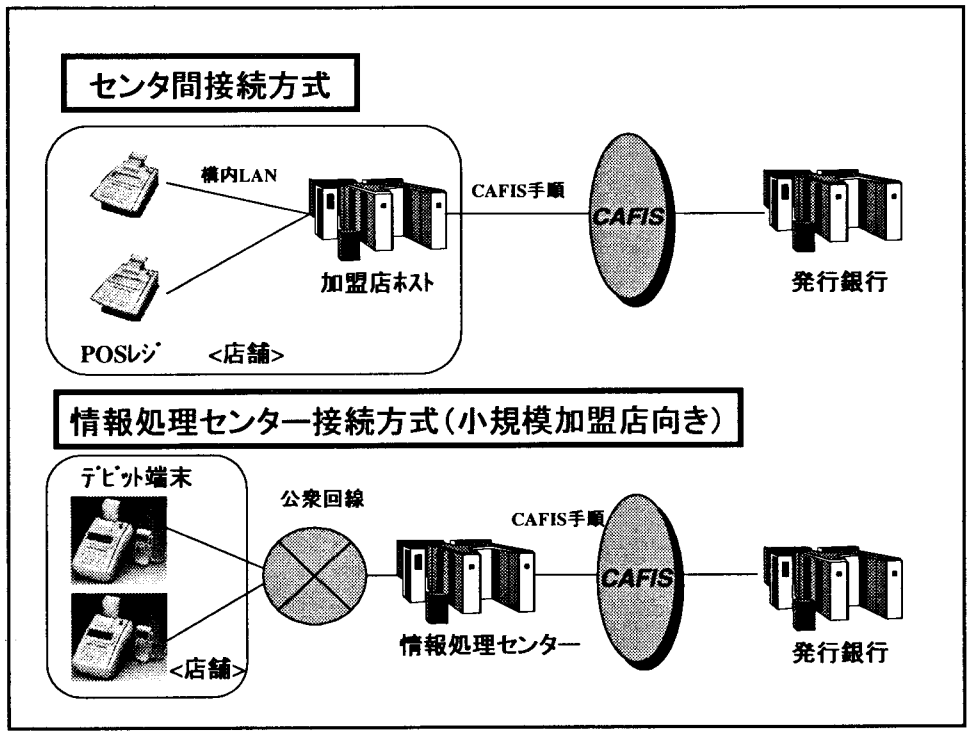
Ver 2k1.3.19a

協議会の組織図

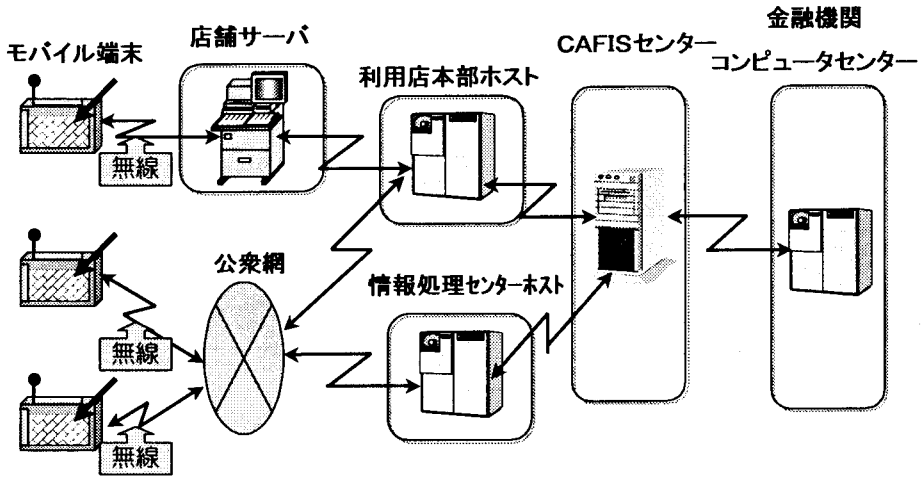
（2001.2.28現在）



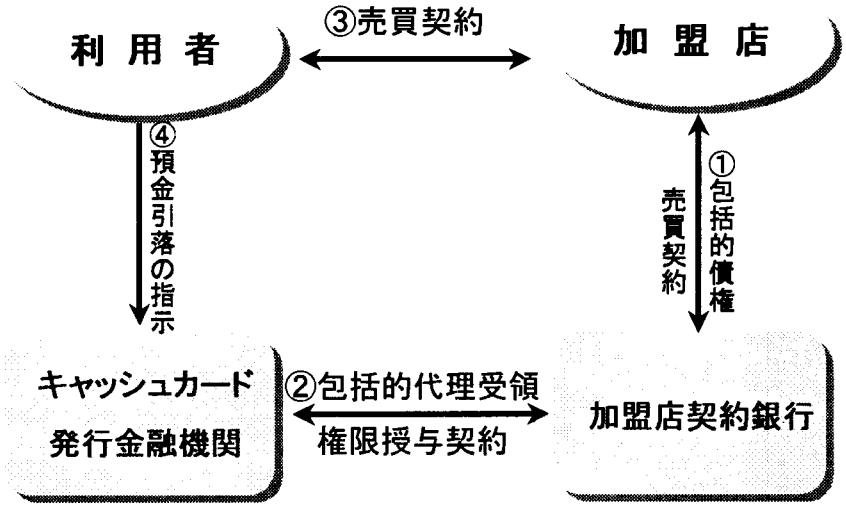

デビットカードサービスの概要
利用店
利用店本部ホスト
金融機関コンピュータセンター
預金者口座
利用店本部口座
CAFISセンター
デパート・スーパー
レストラン
コンビニ
ガソリンスタンド
ホテル
チケット等


センタ間接続方式
構内LAN
加盟店ホスト
CAFIS手順
CAFIS
発行銀行
POSレジ
<店舗>
情報処理センター接続方式(小規模加盟店向き)
デビット端末
公衆回線
CAFIS手順
CAFIS
情報処理センター
発行銀行
<店舗>

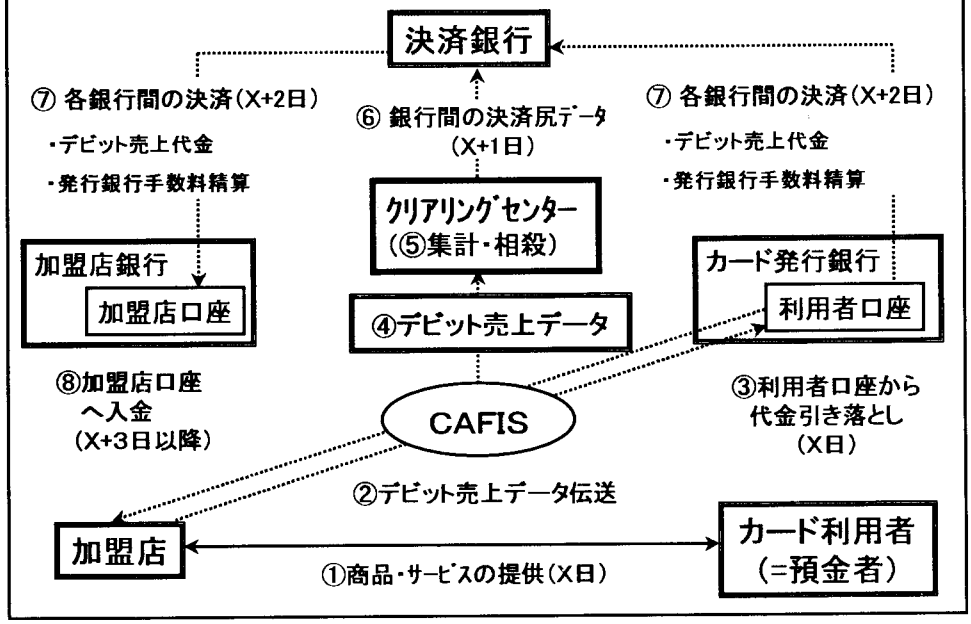
モバイル端末のシステム構成例



デビットカードの法律構成



決済スキーム



本格サービス後の状況

	1999年12月期実績		2000年12月期実績
件数	：4万4500件	→	50万 900件
金額	：14億5100万円	→	244億5500万円
平均単価	：3万2600円	→	4万8800円

	1999年末時点		2001年1月時点
金融機関	：9金融機関	→	1468金融機関
キャッシュカード	：1億1200万枚	→	約3億2500万枚
加盟店	：19加盟店	→	712＋間接加盟店
利用場所	：1万7000ヶ所	→	15万ヶ所以上
情報処理センター	：9社	→	92社

サービス中 金融機関（2001年1月時点）

1468金融機関　3億2500万枚

- ■ 郵便貯金
- ■ 都市銀行(8行)
- ■ 信託銀行(3行)
- ■ 地方銀行(64行)
- ■ 第二地方銀行(52行)
- ■ 外国銀行(1行)
- ■ 信用金庫(370庫)
- ■ 信用組合(113組)
- ■ 労働金庫(39庫)
- ■ 31都府県の817農協

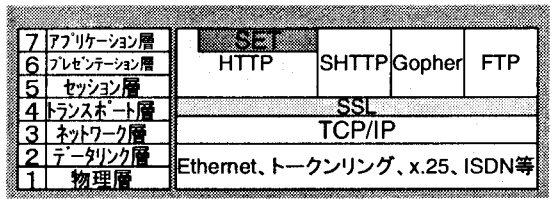
日本デビットカード推進協議会における セキュリティの取組み

平成13年3月19日
日本ﾃﾞﾋﾞｯﾄｶｰﾄﾞ推進協議会

目次

1－1. J-Debitのセキュリティとは（その1）

- オープンネットワーク（インターネットに相当）のセキュリティ（対比）
  - 想定される脅威は、盗聴・改ざん・なりすましであり、それぞれ暗号化・デジタル署名・認証技術で防止するのが一般的である。
  - エンド・トゥ・エンドのプロトコルが一様であるためセキュリティ対策についても標準化しやすい。
  - 例）SSL、SET



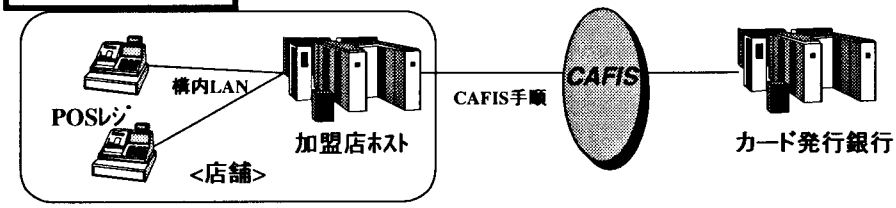
1－2. J-Debitのセキュリティとは（その2）

- クローズドネットワーク（J-Debitに相当）のセキュリティ
  - J-DebitはCAFISを中継ネットワークとして独自手順をベースに実現している。加盟店システムや情報処理センターについては既存のしくみが多様に展開していることから、J-Debitのセキュリティについては、ネットワークだけでなく、加盟店、情報処理センター、金融機関が一丸となって維持していくべきものである。
  - 例）加盟店等における多様なシステム
    - デパート等のPOSレジ接続型
    - 小売店・飲食店に設置されるデビット専用端末（情報処理センタ設置端末）
    - ガソリンスタンドのセルフ給油機
    - コンビニエンスストア等に設置されるマルチメディア端末
    - 無線携帯端末　etc.

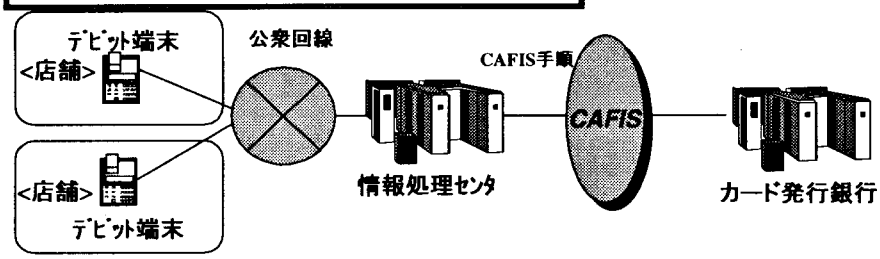
1－3. J-Debitのセキュリティとは（その3）

J-Debitでは、セキュリティについてCAFISに加え、加盟店、情報処理センター、金融機関それぞれの主体が遵守すべき事項を明定している。

センタ間接続方式



情報処理センタ接続方式（小規模加盟店向き）



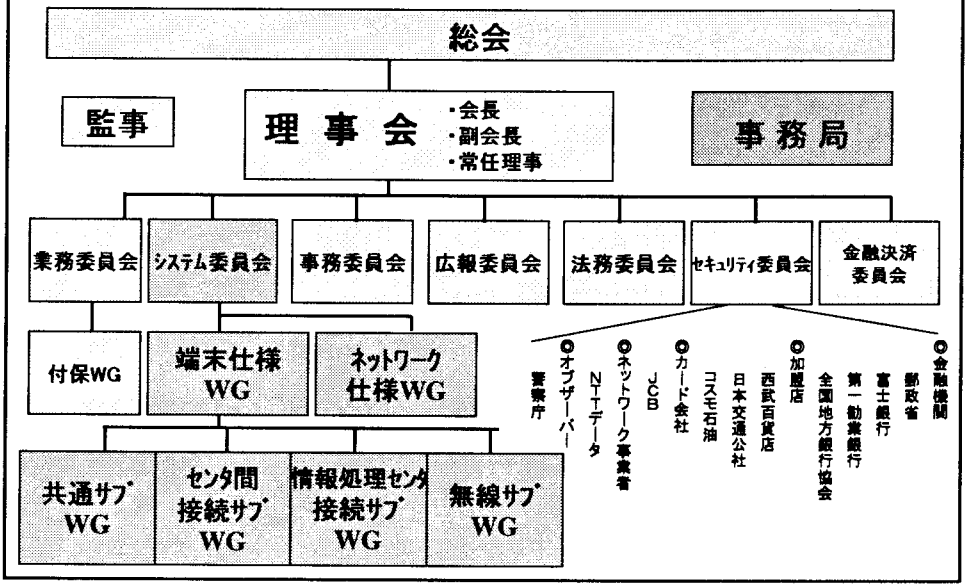
2－1. セキュリティ維持のための組織構成

日本デビットカード推進協議会は、J-Debitに関するセキュリティ対策に関し、設立と同時に検討してきたが、99年2月より専門に検討する部署としてセキュリティ委員会を新たに発足させ、更なる安全性の向上に向け、日々努力している。

- これまでの歩み（詳細は後記）
  - ・98年
    - ・業務部会（現：業務委員会）：決済スキーム構築における安全性の確保
    - ・システム部会（現：システム委員会）：ネットワークシステムにおける安全性の確保
    - ・端末WG：端末仕様における安全性の確保
    - ・広報部会（現：広報委員会）：セキュリティに関する加盟店、利用者への啓蒙活動
  - ・99年
    - ・セキュリティ委員会：セキュリティを専門的に検討する委員会の立ち上げ
    - ・法務委員会（現：法務委員会）：安全性確保実現のための条項を加盟店規約、デビットカード取引規定等に反映

2－2. セキュリティ委員会

- 平成11年3月にセキュリティ委員会を創設



3. 具体的取組み概要

主な取り組み	概要	責任部署
端末セキュリティ	J-Debit端末より不正に情報を入手する事を避けるために、端末に具備するべき機能の策定	端末WG（端末ベンダ）
ネットワークセキュリティ	J-Debitに関わるネットワーク全域において、情報の盗聴・改ざんを防止するための手段の策定（電文の暗号二重化）	システム委員会
セキュリティガイドライン策定	J-Debitサービスの安全性保持のため、金融機関・加盟店・情報処理センターが遵守すべき事項を策定（全45項目）	セキュリティ委員会
セキュリティ監査の実施	セキュリティガイドラインの遵守状況を把握し、不良加盟店を排除し純化していくため、加盟店向監査を定期実施	セキュリティ委員会
セキュリティ広報の実施	カード利用者、店舗要員等にセキュリティに対する注意喚起を実施	広報委員会
その他	利用限度額の検討、不正利用検知システムの導入、等の課題を鋭意検討中。	全委員会

4－1. 具体的取組み（端末セキュリティ）

- 暗証番号盗み見防止（端末かざしの装着）
  - 暗証番号入力時の盗み見予防措置として据え置き型暗証キーパッドについて「かざし」装着を「端末仕様ガイドライン」にて義務化する。
- 端末改造防止（耐タンパー機能設定）
  - 端末／暗証キーパッドの耐タンパー機能の作り込みを「端末仕様ガイドライン」にて義務化する。
  - 耐タンパーとは、暗号化鍵、暗号アルゴリズム、暗証番号が外部へ漏洩しないよう開けられない構造、または開いた場合前記情報が消去される機構。
- 端末仕様ガイドラインリファレンスの作成
  - 端末仕様ガイドラインの内容に加え、「暗証キーパッドでのセキュリティ」「カード情報盗用に関するセキュリティ」「接続に関するセキュリティ」を追記し、端末タイプ毎にセキュリティ実現方法を詳細化した。
- 端末設備認定
  - 端末は協議会による認定が必須（基準は上記諸項目）。認定不合格の端末は使用不可。（端末製造は協議会賛助会員メーカーにのみ限定許可）。

4－2. 具体的取組み（ネットワークセキュリティ）

- ネットワークの暗号化
  - 暗証番号については協議会指定の暗号化を必須としている。
  - 暗証キーパッド～銀行間における途中ノードでは一切暗証番号が平文化 されない。
- 暗号の二重化
  - 暗証キーパッド～加盟店・情報処理センタホスト間はさらにDESにより重複して暗号化する。
- CAFIS手順規程の暗号化
  - 加盟店・情報処理センタ～CAFIS間は一部CAFIS手順で規定された方式により重複して暗号化を実施する。
- セキュリティ情報の不保持
  - 暗証番号については一切端末、加盟店・情報処理センタホスト等で保持しない。

4－3. 具体的取組み
（セキュリティガイドラインの策定）

- セキュリティガイドラインとは
  - J-Debitサービスの安全性維持・不正利用防止を目的として作成
  - 加盟店・情報処理センター・金融機関における遵守事項を記載
  - 本ガイドラインを遵守しない場合、規約違反となり登録抹消
  - 運用実態に合わせ年1回の定期改訂を実施
  - 緊急対策が必要な事象が発生した場合は臨時改訂を行う

- 加盟店および情報処理センタにおける遵守事項
  - 加盟店販売員への周知徹底
  - 加盟店店舗環境および端末設置環境上での対策
  - システム管理、運用上の対策

- 金融機関における遵守事項
  - キャッシュカード発行時点での利用者への周知徹底
  - システム管理、運用上の対策
  - その他セキュリティ対策

4－4. 具体的取組み
（セキュリティ監査の実施）

- セキュリティ監査とは
  - 加盟店を被監査者、協議会を監査者とし、セキュリティガイドラインの遵守状況を確認する。
  - 明らかに遵守していないと判定された加盟店は、協議会規約に従いサービスの停止、加盟店登録抹消を実施する。
  - 毎年6月を目途に定期監査を実施
  - 必要に応じ臨時監査を実施（ｾｷｭﾘﾃｨｶﾞｲﾄﾞﾗｲﾝ臨時改定時等）

- 監査内容
  - ホストコンピューターを所有する加盟店、及び情報処理センターについてはシステム運用、端末管理、及び店舗運用の観点から監査を実施する。
  - ホストコンピューターを所有しない加盟店については、主に店舗運営面より監査を実施する。

4－5. 具体的取組み
（セキュリティ広報の実施）

- 正規加盟店の判別
  - ロゴマークの制定、店頭呈示の義務づけ
- 協議会から会員を通じて実施するセキュリティ広報活動
  - 利用者に対し暗証番号の管理に留意してもらうため、協議会作成のセキュリティポスター（イメージキャラクターとしてヒロコグレース氏を起用）を金融機関、加盟店に無料で配布し、金融機関ATM、加盟店店舗等全店にて掲示を義務付けている。
- 協議会から媒体を通じて実施するセキュリティ広報活動
  - 協議会より、新聞・雑誌の記事・広告に注意喚起のメッセージを記載している。
  - 協議会作成のパンフレット・チラシに注意喚起のメッセージを記載している。
- 協議会会員からの実施するセキュリティ広報活動
  - 協議会会員が利用者に向けて利用するJ-Debitのプロモーションビデオ・ポスター・ステッカー・POPの一部は協議会が販売しており、その中に注意喚起メッセージを記載している。

4－6. 具体的取組み
（その他取組状況）

- 一日（一回）利用限度額のレベル吟味
  - 協議会において、利用金額レベルにあった利用者毎の限度額設定が可能なシステムの導入を金融機関に推奨している。（一部金融機関ではすでに実施済）
- 不正利用検知システムの導入
  - CAFISセンターに不正利用検知を導入する事により、不正利用が自動的に検知可能なしくみを構築、本情報を基に金融機関と不正利用の未然防止の機構を検討する。
- 金融機関での利用停止措置
  - 不正利用と疑われた場合、又は利用者から緊急停止の要望があった場合に、金融機関が利用者口座を凍結する仕組み。そのためのシステム実現方法をモデル化。
- 暗証番号変更手続きの運用システム
  - 利用者が暗証番号を変更する際の一般的な手続きの流れ、即時変更の可能性、システム的な変更手順（ATMによる変更）等をモデル化。（一部金融機関ではすでに実施済）

4－6. 具体的取組み
（その他取組状況）

- 加盟店端末管理強化策
  - 加盟店における端末管理のあり方を強化すべく加盟店、金融機関、情報処理センターが連携して以下の6項目の施策を実施中。
    - セキュリティガイドライン改訂
      セキュリティガイドラインに端末管理に関する規定を追加
    - セキュリティ監査
      新規定の遵守を目的とした監査の実施
    - セキュリティチェックシート
      加盟店にて毎営業日、端末管理状況をチェックするしくみの導入
    - セキュリティシール
      端末が不正に開けられた場合、目で検知可能とするしくみの導入
    - アンケート（初期導入端末のみ）
      加盟店に対し端末管理状況について実態調査を実施
    - 実地検査（初期導入端末のみ）
      アンケート実施加盟店のうち、さらに一部については現地に赴き端末の管理状況を実地点検

カード犯罪総合対策検討委員会報告書

発　行　　平成13年3月

編　集　　社団法人　日本防犯設備協会
　　海外規格調査委員会

発　行　　社団法人　日本防犯設備協会
　　〒105-0012　東京都港区芝大門1丁目6番11号
　　芝大衛ビル2F
　　TEL　03－3431－7301
　　FAX　03－3431－7304

印刷　㈱小日向商事