ICキャッシュカード取引のセキュリティ強化を実現する「IC基本形認証サーバ」

村上　聡　　安田　弘法

近年，盗難や偽造キャッシュカードを使ったATM（現金自動預け払い機）からの不正引き出しなどの犯罪が増加し社会問題化している。以下に金融庁の調査によるこれまでの被害状況を示す。**図1**，**図2**から，偽造キャッシュカードによる被害が平成15年から急増していることが分かる[1)]。

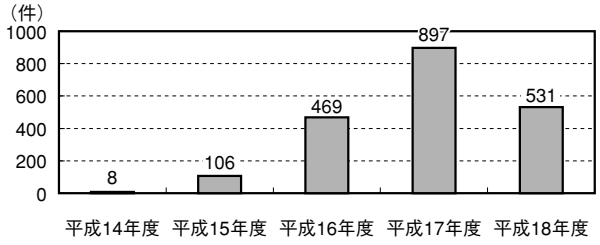

図1　偽造キャッシュカードによる被害件数推移

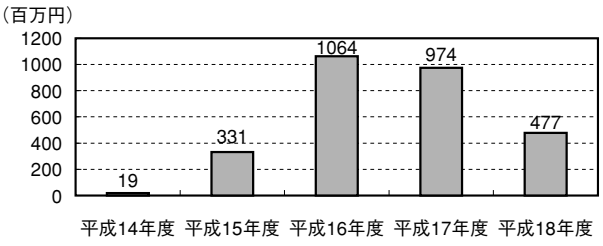

図2　偽造キャッシュカードによる被害金額推移

このため金融業界および利用者のセキュリティに対する関心が高まり，ATM取引に対する安心感や信頼性が強く求められている。

本稿では，偽造キャッシュカード問題に対する金融業界での取り組みについて述べると共に，昨年12月にOKIが発表した「IC基本形認証サーバ」を紹介する。

金融業界での取り組み

偽造キャッシュカード問題に対して，全国銀行協会（略称，全銀協）では以下のような取り組みを行っている[2)]。

- 偽造が極めて困難なICキャッシュカードの標準仕様を制定（平成13年3月「初版」，平成18年3月「第2版」）
- 預金者に対するキャッシュカードや暗証番号の取り扱いに関する注意喚起を実施（平成15年～16年）
- 偽造キャッシュカード被害の補償ルールを決定（平成17年10月）

上記の内，「全銀協ICキャッシュカード標準仕様」では，ICキャッシュカードの正当性確認（カード認証）方式について以下の2つの方式が定義されている（**図3**）[3)]。

① **経過期間**
ATMでオフライン認証する方式

② **基本形**
自金融機関（ホストやサーバ）でオンライン認証する方式

上記「基本形」を実現するには，ホスト，ネットワーク等の改造にかなりの時間を要する。このため経過的にカード認証をATMに判断させる「経過期間」を可能とする段階的移行の規定を図る必要があった。

「全銀協ICキャッシュカード標準仕様（初版）」では，「経過期間」を平成17年度末までとした。その後，平成18年3月に改版された「全銀協ICキャッシュカード標準仕様（第2版）」では，さらに5年間延長し，平成22年度末までとした。その後，平成19年に全銀協から全加盟行に対してアンケート調査を実施した結果，現在はさらに1年間延長し，平成24年頃を目処に「基本形」へ移行することを推進している。

また金融機関側でも，以下のような取り組みを行っている。

- ICキャッシュカードの導入（平成14年～）
- 利用限度額の個別設定サービス（平成14年～）
- 利用限度額の引き下げ
- 生体認証による本人確認（平成16年～）
- ATMでの支払い取引の時間帯，場所を預金者が設定でき

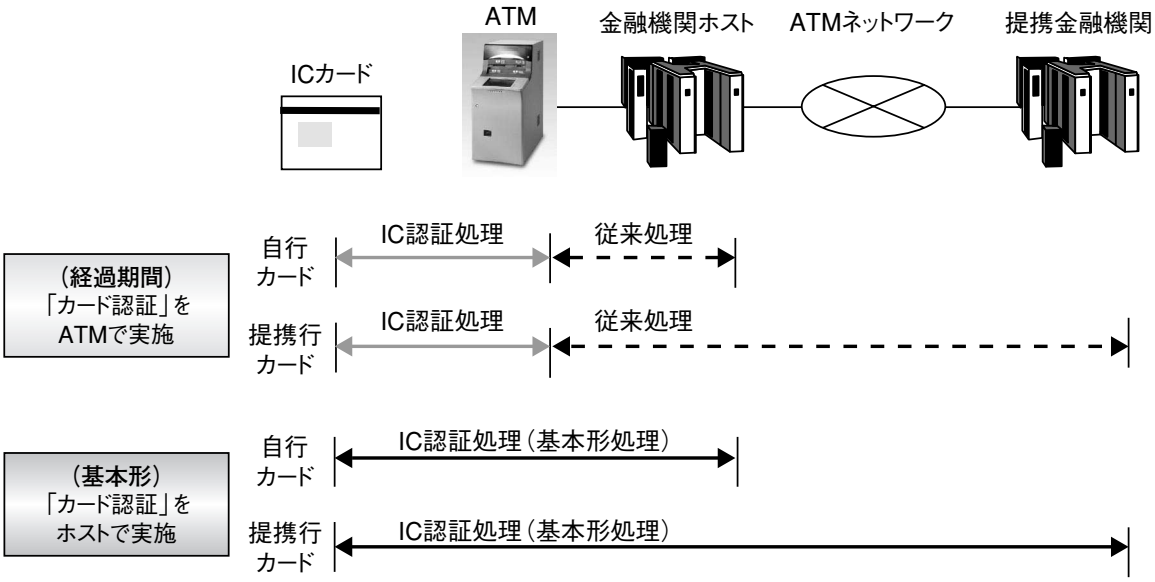

図3　基本形と経過期間における取引の流れ

るサービス（平成17年～）
●異常取引検知システム

金融機関においては，従来の磁気ストライプを使ったキャッシュカードから，より安全なICキャッシュカードへ移行する動きが進んでいる。また，平成24年頃を目処にICキャッシュカードの認証方式を現在の「経過期間」から「基本形」へ移行する方向で取り組みが進んでいる。

OKIの取り組み

「基本形」に移行するためには，ATMと基幹系ホスト両方の対応が必要となるが，基幹系ホストで対応する場合コスト面／リスク面で問題がある。このため，ホストで行うべき基本形処理を，サーバで実現する方式が考えられた。

OKIでは，ICキャッシュカードの標準仕様【第2版】に準拠した「IC基本形認証サーバ」を昨年12月に発表し，販売を開始した。

また，ATMにおいても早くから「全銀協ICキャッシュカード標準仕様」に適合する機種として「ICキャッシュカード認定制度運営協議会」が認定する機器認定を取得している。

IC基本形認証サーバの紹介

「IC基本形認証サーバ」は，「全銀協ICキャッシュカード標準仕様（第2版）」に準拠し，ATMと連携してICキャッシュカードの正当性確認（カード認証）をサーバで実現する製品である。

「IC基本形認証サーバ」は，「経過期間」における従来処理と「基本形」で新たに必要となる処理の違いを本サーバで吸収することにより，既存システムに影響を与えず，低リスクでシームレスに従来の「経過期間」から「基本形」への移行が実現できる。

図4（次ページ）に「IC基本形認証サーバ」を使用した「基本形」移行イメージを示す。**図4**では，以下3つの取引パターンを記載している。

① 自行カードが自行ATMで使用された場合
② 自行カードが提携行ATMで使用された場合
③ 提携行カードが自行ATMで使用された場合

IC基本形認証サーバの主な特長を以下に示す。

① ホスト負荷を軽減

IC基本形認証サーバでは，暗号鍵を使用する複雑な認証処理は本サーバで処理する。また，認証処理に加え，電文中継，電文変換（基本形電文⇔従来電文）処理機能も提供する。そのため，基幹系ホストへの影響（開発および処理負荷など）を最小限に抑えることが可能となる。

② 高い可用性

IC基本形認証サーバの主要コンポーネントは全て冗長構成をとり，高い可用性を実現する。そのため，万が一システムに障害が発生した場合でも，迅速に障害ポイント

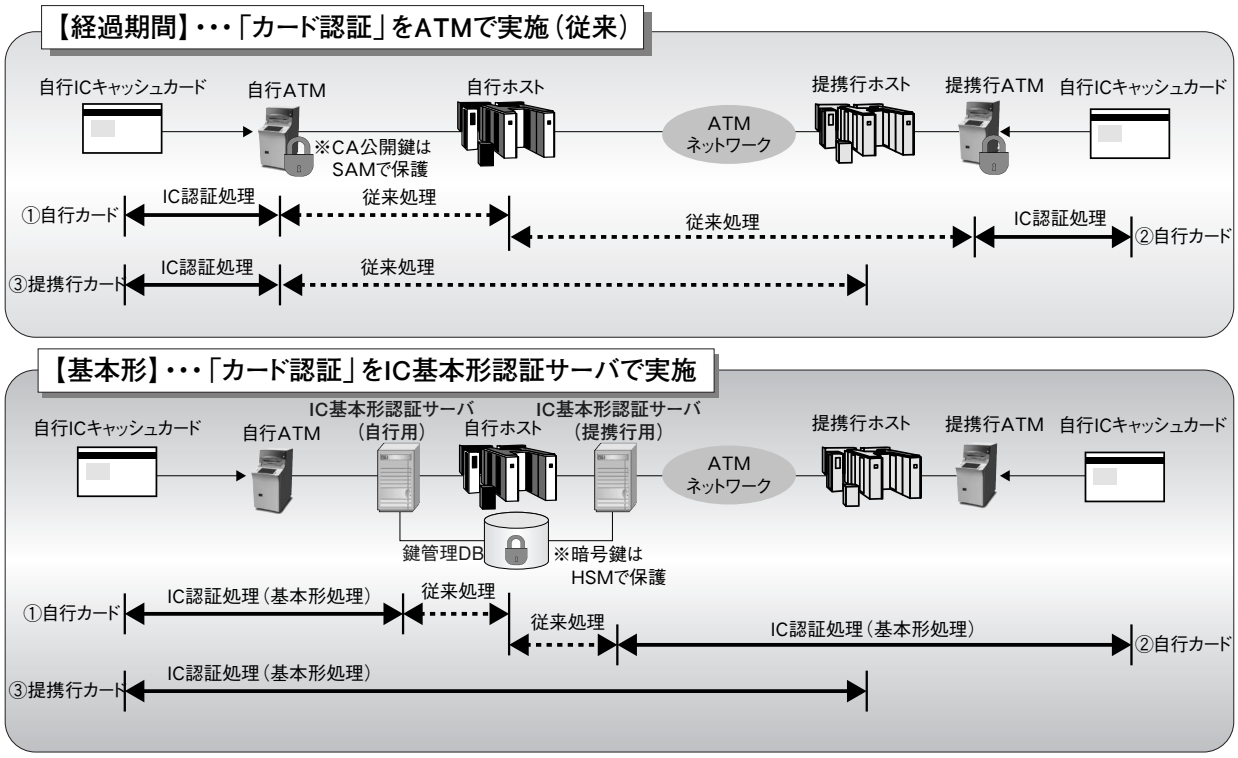

図4　「IC基本形認証サーバ」を使用した「基本形」移行イメージ

を切り離し，運用を継続させることが可能となる。

③ 暗号鍵を安全に保護

基本形認証に必要となる金融機関ごとの暗号鍵の保管・管理は，HSMを採用した安全な仕組みで実現する。これによりFISC安全対策基準や金融庁通達などの各種セキュリティ指針に準拠できる。

④ 柔軟な拡張性

将来の機能拡張や処理能力増強などにも柔軟に対応できる優れた拡張性を提供する。これにより段階的な基本形移行や将来の取引量増加時などにも柔軟に対応可能となる。

＜段階的な基本形移行の例＞

【Step1】自行ATM取引対応

【Step2】提携行ATM取引対応

⑤ 提携行ATM取引対応

IC基本形認証サーバでは，自行取引だけでなく提携行とのATM取引にも対応することが可能となる。

⑥ イシュアスクリプト対応

ICキャッシュカードの正当性確認の機能に加え，セキュリティを確保したICキャッシュカード内容書換え（イシュアスクリプト）にも対応可能である。

あ と が き

本稿では，偽造キャッシュカード問題に対する金融業界での取り組みについて述べると共に，OKIのICキャッシュカード基本形認証ソリューションである「IC基本形認証サーバ」の紹介をした。本製品を導入することにより，既存システムへの影響を最小限に抑え，安全で迅速な「基本形」への移行が可能となる。今後は，ATMトップベンダとして，ATMと共に本サーバを金融市場向けに積極的に販売していく。また，これと並行して「基本形」認証に対するATM側のシステム開発も進めており，安全，確実なシステム移行の実現をサポートする。さらに，要件定義から設計，実装，運用保守といったシステムのライフサイクルに対応するトータルサポートサービスも提供する。 ◆◆

■参考文献

1）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，2007年6月

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最終報告書，金融庁，2005年6月

3）全銀協ICキャッシュカード標準仕様（第2版），全国銀行協会，2006年3月

●筆者紹介

村上聡：Satoshi Murakami. 金融ソリューションカンパニー 金融システム本部 金融ソリューション開発部 開発第一チーム
安田弘法：Hironori Yasuda. 金融ソリューションカンパニー 金融システム本部 金融ソリューション開発部 開発第一チーム

TIPS【基本用語解説】

全銀協ICキャッシュカード標準仕様（第2版）
ICキャッシュカードの金融機関間相互運用性の確保等を目的として2001年（平成13年）3月に全国銀行協会が制定した標準仕様。5年ごとに定期的に見直しがおこなわれ，2006年（平成18年）3月に第2版が制定された。

経過期間
ICキャッシュカードの正当性確認（カード認証）を，ATMが判断する認証方式。「ICキャッシュカードオフライン認証」などと言われることもある。ATMではSAM（Secure Application Module）と呼ばれる認証モジュールを搭載して経過期間認証をおこなう。またCA公開鍵の更新に合わせ5年ごとにSAMの交換が必要である。

基本形
ICキャッシュカードの正当性確認（カード認証）を，自金融機関（ホストやサーバ）が判断する認証方式。「ICキャッシュカードオンライン認証」などと言われることもある。基本形移行により経過期間で必要であったATMへのSAM搭載，および5年ごとのSAM交換が不要となる。

HSM
（Hardware Security Module）
電子署名や暗号化に使用する鍵を，ハードウェア内部で安全に管理し，暗号処理機能を提供するセキュリティモジュール。HSMは耐タンパ性を備えており，鍵を他人に盗まれたり，不正アクセスにより他者が自由に利用できてしまうということはない。

耐タンパ性
データの不正な読出しや使用，改ざん，また故意に誤動作させることに対して，物理的・論理的に防止すること。

FISC
（The Center for Financial Industry Information Systems）
財団法人 金融情報システムセンターのこと。

イシュアスクリプト
ICカード内容書換えを目的にICカードに送るコマンドスクリプトのこと。