普通論文

セキュリティ国際規格認定暗証番号入力機器

後藤 雅生・菊池 重寿
鉾田 祐也・森田 誠

要　旨

これまでクレジット決済システムはIT技術を駆使し重要な社会インフラの1つとして発展、確立されてきました。昨今の技術革新、社会の構造変化、情報価値、および個人情報に対する社会認識の変化などにより、このクレジット決済システムにおいてもさらに高度な情報セキュリティ技術を保持することが必要となる時代となってきました。

このたび、セキュリティ国際規格であるPCI 規格（Payment Card Industry）を国内で初めて取得した、暗証番号入力機器（PINPAD）を開発しましたので、紹介します。

キーワード

●クレジット決済 ●セキュリティ機器 ●PCI規格 ●PINPAD ●PIN ●PCIPED ●ICカード

1. はじめに

国内においてこの10年間に発行されたクレジット決済用カード枚数は1.25倍、また与信金額も1.86倍に伸びています。こうした普及拡大のなか、悪用の手口も多様化、高度化してきており、それに伴い、クレジット業界でも、2003年から本格的にICカード化を推進し、クレジット決済のセキュリティを高めてきました。

このため、ICカードクレジット決済では、暗証番号入力機器（PINPAD）による暗証番号（PIN）の保護が非常に重要となってきています。今回、国内で初めて、ICカードクレジットPINPADのセキュリティ国際規格であるPCI規格（Payment Card Industry）を取得し、クレジット会社の認定を受けた高セキュリティPINPADを開発しましたので報告します。[*1]

2. PCI規格の背景

PCI規格とは、ICカードクレジット決済で必要なPINを入力する機器に対する、物理的、論理的なセキュリティ要件を規定した規格になります。

本規格確立までの簡単な経緯は、2000年にPINPADに対する独自規格が立案され、2004年に国際規格として、PCI規格となりました。2005年秋口には国内ブランドも参画し、日本でもPCI規格取得要求が本格的になってきました。

また、国際ブランド5社からキーメンバーが参加する評議会である　PCI SSC （PCI　Security Standard Council）が設立され、2008年、その1つに、PINPADのセキュリティ要件として、PIN Entry Devices Programが盛り込まれ、PCI PED（PIN Entry Devices）規格として運用されています。

本機器は、外部からの攻撃に対して、安全に使用でき、重要な情報が盗まれないなどのPCI規格を満たすために、最新の技術や独自の工夫を盛り込み実現したものです。

3. PCI規格の要件概要

PINPADのセキュリティ要件は、以下の4つのカテゴリで分類されます。

(1) Physical Security Core Requirements
PINPADのハードウェアのセキュリティ要件
（物理的攻撃に対する防御と検知に関すること）

(2) Logical Security Core Requirements
ファームウェアのセキュリティ要件
（ハッキングや改ざん行為に対する、PINやPINブロックの防御に関すること）

[*1] セキュリティ機器であるため、一部公開できない情報や記述できない部分があることをご了承願います。

(3) Online Requirements
オンラインPIN入力のセキュリティ要件
(4) Offline Requirements
オフラインPIN入力のセキュリティ要件

4. 商品仕様

今回開発したPINPADの商品仕様を **表** に示します。

なお、PINPADの外観図について、磁気カードリーダが無いモデルと、搭載したモデルを、それぞれ **写真1** 、 **写真2** に示します。

表　PINPADの仕様

項目		仕様
表示部	デバイス	液晶ディスプレイ(コマンドによるバックライト制御)
	表示文字数	全角8文字×4行(128×64ドット)
	表示文字	JIS第一水準
	ディスプレイサイズ(mm)	表示エリア 約41(W)×約24(H)
キーボード	配列	電話機配列
	テンキー	数値キー:10個(0～9)、ﾌｧﾝｸｼｮﾝｷｰ:4個 確定キー:1個、取消キー:1個
	電源キー	無し
ブザー音		キー入力音、アラーム音
ICカードリーダ		ISO/IEC7816準拠　EMV4.0認定取得
磁気カードリーダ		JIS1(ISO第1,2トラック)、JIS2
セキュリティ		日本ﾃﾞﾋﾞｯﾄｶｰﾄﾞ推進協議会端末ｶﾞｲﾄﾞﾗｲﾝ準拠 日本ﾏﾙﾁﾍﾟｲﾒﾝﾄﾈｯﾄﾜｰｸ推進協議会ｶﾞｲﾄﾞﾗｲﾝ準拠、 PCI規格認定取得(バージョン1.3A)
設定		コントラスト(5段階)、ブザー音量(3段階)、音程(固定)、 鳴動時間(可変)
インタフェース		RS232、USB
ケーブル長		RS232およびUSB　標準　2m
設置		ハンディ式(手に持つタイプ)
外形(mm)		約190(W)×約70(D)×約30(H) (磁気カードリーダ付き:かざし含まず)

写真1　磁気カードリーダ無モデル（かざし未装着時）

写真2　磁気カードリーダ搭載モデル（かざし装着時）

5. 具体的適用技術と特徴

5.1 物理的対応技術と特徴

物理的要件として求められるものは、攻撃を受けにくくかつ攻撃を受けたことを検知する機能を設けることになります。

(1) 攻撃を検知する技術

攻撃を検知する方法として、スイッチやセンサを複数設け、その1つでも動作すれば、機微情報（PIN、暗号鍵など）が即座に消去できる仕組みが必要となります（**図**）。

本機器には、ケースを開ける、基板をはずす、基板を削るなどの物理的攻撃に対し、様々な方法で検知する機能を有しています。また、環境攻撃手法として、メモリに対する低温攻撃の存在が知られており、これに対しては、温度センサICを使用することで攻撃に対する検知を実現しました。

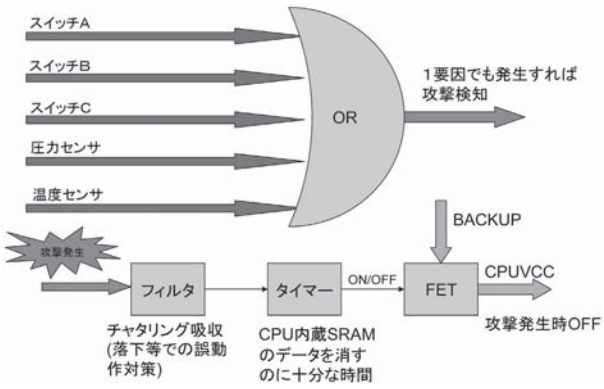

図　攻撃を検知する方法

(2) 攻撃を受けにくくする技術

攻撃を受けにくくするために、本機器は、極力不要な隙間、不要な空間を設けないような構造になっています（**写真3**、**写真4**、**写真5**）。　これは、ICカード挿入口にカードの厚み以上の隙間がある場合、攻撃者がカードとケースの間にスキミング装置を差し込み、ICカードの情報を盗み出す可能性を排除するために実施したものです。

さらに、攻撃された痕跡が残るような構造にもしています。本機器では、ケースかみ合わせ部を直線ではなく曲線にしました。これは、かみ合わせ部分から、カッターなどで切

写真3　ICカードを2枚挿入できなくしている

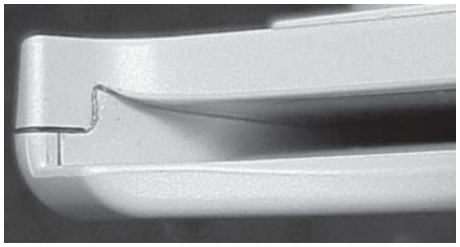

写真4　内部にスキミング装置の入る空間をなくしている

写真5　カード挿入口が見えるためスキミング装置がある場合一目でわかる

写真6　シールドケースで、内部を保護、またシールドケースに攻撃を加えると検知する

断しケースを開ける場合、かみ合わせ部が曲線なため、開けにくく、かつ、開けた痕跡が残りやすくなるためです。

また、回路設計上での注意点としては、メモリを直接攻撃され、内部機微情報を不正取得されることのないように、機微情報の保存部分（メモリ）を保護するという点です。本機器では、メモリを含むメイン回路を、攻撃検知回路内蔵のシールドケースで覆いました（**写真6**）。

5.2 論理的対応技術と特徴

論理的要件として求められるものは以下の項目となります。

1) PINを知られない、また推測されないこと。

2) PINPADは想定外の通信データを受信しても暴走しないこと（暴走させることにより予期せぬ動作を引き起こさせる）。

3) 第三者が悪意あるプログラムをPINPADに挿入できないこと。

4) 攻撃検知時に機微情報を削除すること。

上記要件に対する本機器での対応技術と特徴を以下に述べます。

(1) PINを知られない、また推測されないこと

利用者が入力したPINを、PINPADの外に出さないようにしています。

また、キー入力ごとにデータを暗号化して、機微情報として保持し、不要になった時点（ICカードにPINを出力した時点など）、および、キー入力開始からのタイムアウト時に、暗号化データを削除しています。

この動作により、PINを極力PINPADに保持せず、また保持する場合でも暗号化し、攻撃によりPINが盗まれるリスクを低減しています。

さらに、PIN入力時のキー入力音が単一であり、表示部には

意味のないキャラクタ（アスタリスク）を表示させることで、キー入力音や表示部から、PINを推測させません。

(2) PINPADは想定外の通信データを受信しても暴走しないこと

仕様書に定義されるコマンドデータ以外のデータをまったく無意味なデータとして扱うような特殊な防御プログラムを組み込むことにより、大量のデータや想定外データの送信などによるプログラムを暴走させる攻撃を防ぎます。

(3) 第三者が悪意あるプログラムをPINPADに挿入できないこと

ファームウェアの書き換えに必要な暗号鍵情報を、各PINPAD固有にし、さらにファームウェア情報にハッシュ値を持たせることで第三者によるファームウェア改ざんを防止しています。

(4) 攻撃検知時に機微情報を削除すること

攻撃検知時に機微情報を削除しています。また、機微情報が含まれるデータは、使用後には即座に消去し、メモリ上に残さないようにします。機微情報が含まれるデータは、攻撃検知回路内蔵のシールドケースで保護されていない外部メモリ上では、使用しません。

さらに、定期的に、機微情報の確認を行い、情報に変化があった場合には、攻撃を受けたと判断し、即座に機微情報を削除します。

6. まとめ

本稿は、国内初のPCI規格取得 PINPADとして、機器開発を行った内容を報告しました。

PCI認定機器として市場でも優位性が評価され、これまで、大手量販店でのPOS接続ICカードクレジット決済システム向けや大手メーカへのOEM供給など、約5万台の出荷をしています。

技術革新が進むなか、攻撃の手法も年々高度化しており、求められるセキュリティレベルは変化しています。実際、2008年4月1日よりPCI規格も、バージョン1.3Aからバージョン2.0にアップし、より高度なセキュリティレベルの取得が製品化の要求となりました。

今回の機器開発で培ったノウハウを基に、より高いセキュリティ要求をクリアできるよう技術の向上に努め市場でのさらなる拡大をめざしていきます。

参考文献

1) 社団法人　日本クレジット協会　統計資料
2) “Payment Card Industry (PCI) PIN Entry Device (PED) Testing and Approval Program Guide,” Version 1.0, December 2007
3) PCI POS PED Security Requirements v1.3
4) PCI POS PED DTRs v1.3
5) EMV Integrated Circuit Card Specifications for Payment Systems (c)1994-2004 EMVCo, LLC (“EMVCo”). All rights reserved.
6) ANS X9.24-2004 Retail Financial Services Symmetric Key Management (c)2004 Accredited Standards Committee X9, Inc. All rights reserved.

執筆者プロフィール

後藤 雅生
NECインフロンティア
iアプライアンス事業部
第3商品開発グループ
エキスパート

菊池 重寿
NECインフロンティア
iアプライアンス事業部
第3商品開発グループ
マネージャー

鉾田 祐也
NECインフロンティア
iアプライアンス事業部
第3商品開発グループ

森田 誠
NECインフロンティア
iアプライアンス事業部
第3商品開発グループ