IMES DISCUSSION PAPER SERIES

ICカード利用システムにおいて
新たに顕現化した中間者攻撃とその対策

鈴木雅貴(すずきまさたか)・廣川勝久(ひろかわかつひさ)・古原和邦(こばらかずくに)

Discussion Paper No. 2011-J-16

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2011-J-16
2011 年 10 月

IC カード利用システムにおいて新たに顕現化した中間者攻撃とその対策

鈴木雅貴*・廣川勝久**・古原和邦***

要　旨

クレジットカード等の金融取引用 IC カードとこれに利用される端末の仕様を定めた業界標準「EMV 仕様」が日本を含め国際的に利用されている。EMV 仕様に準拠した IC カードと端末を利用する「IC カード利用システム」は、端末やホストシステムおよびそれらを繋ぐ通信路等から全体システムが構成されており、端末やホストシステム自体あるいは端末とホストシステム間の通信路における様々な脅威について対策が講じられてきた。しかし、IC カードと端末間を流れるデータの盗聴・改ざんを行うタイプの「中間者攻撃」については、これまで必ずしも現実的な脅威として認識されてこなかった。こうしたなか、近年、実際の運用環境と同等の実験環境において、IC カードと端末間への中間者攻撃により本人になりすました不正な取引が成立し得ることが示された。

そこで、本稿では、EMV 仕様において規定されている最低限の要件のみを満たす IC カード利用システムを検討対象とし、各攻撃への対策および対策の実装のために追加的に求められる要件について検討する。また、対策の導入コストの問題や利便性の低下等により、技術的には対策可能であっても適用が困難な状況が想定される場合には、運用面での対策が一層重要になることを指摘する。

キーワード：EMV 仕様、中間者攻撃、IC カード、本人確認、クレジットカード、キャッシュカード、ビジネスリスク管理

JEL classification: L86、L96、Z00

*　日本銀行金融研究所（E-mail: masataka.suzuki@boj.or.jp）
**　日本銀行金融研究所（E-mail: katsuhisa.hirokawa@boj.or.jp）
***　独立行政法人産業技術総合研究所（E-mail: k-kobara@aist.go.jp）

本稿の作成に当たっては、東芝ソリューション株式会社の山田朝彦氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行あるいは独立行政法人産業技術総合研究所の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

目　次

1. はじめに 1
2. **EMV** 仕様のセキュリティ機能と取引の流れ 3
　2.1　**IC** カード利用システムの全体像 3
　2.2　想定する **IC** カード利用システム 4
　2.3　**EMV** 仕様のセキュリティ機能 4
3. 想定する中間者攻撃 10
　3.1　想定する中間者攻撃のタイプと共通の前提条件 10
　3.2　任意 **PIN** 利用型攻撃 11
　3.3　**Barisani *et al*.[2011]**による盗取 **PIN** 利用型攻撃 14
　3.4　**Adida *et al*.[2006]**による盗取 **PIN** 利用型攻撃 17
4. 想定する中間者攻撃への対策 19
　4.1　共通の対策 19
　4.2　任意 **PIN** 利用型攻撃への対策 21
　4.3　**Barisani *et al*.[2011]**による盗取 **PIN** 利用型攻撃への対策 24
　4.4　**Adida *et al*.[2006]**による盗取 **PIN** 利用型攻撃への対策 27
5. 考察 29
6. おわりに 33
参考文献 34

1. はじめに

クレジットカード等の金融取引用 IC カードとこれに利用される端末の仕様を定めた業界標準「EMV 仕様[1]」が国際的に利用されている。EMV 仕様の策定・管理を行っている EMVCo によれば、全世界で利用されている金融取引用カードのうち IC カードは約 36%（約 10 億枚）、全世界の加盟店に設置された端末のうち IC カードに対応した端末は約 65%（約 1,540 万台）である（2009 年 9 月 1 日現在）[2]。特に、欧州では、SEPA（Single Euro Payments Area）加盟国における IC カードと IC カード対応端末の普及率が高い[3]。わが国でも、EMV 仕様に準拠したキャッシュカードやクレジットカードが発行されている[4]。

EMV 仕様に準拠した IC カードと端末を利用したシステム（以下、「IC カード利用システム」）は、IC カード、端末、発行者のホストシステムといったエンティティとそれらを繋ぐ通信路等から全体システムが構成されており、各装置が安全であったとしても、通信路上のデータを盗聴・改ざんする攻撃（「中間者攻撃（Man-in-the-Middle Attack）」と呼ばれる）の脅威が存在する。IC カード利用システムでは、端末とホストシステム間の通信路に対する中間者攻撃に対して技術面または運用面からの対策が講じられてきた。しかし、IC カードと端末間への中間者攻撃については、必ずしも現実的な脅威として認識されてこなかった。こうしたなか、2007 年に IC カード利用システムにおいて、IC カードと端末間への中間者攻撃により不正な取引が成立し得ることが実験により示された（Adida *et al*.[2006]、Drimer and Murdoch[2007]）。さらに、2010 年と 2011 年にも、そうした中間者攻撃に分類される別の攻撃により不正な取引が成立し得ることが実験により示された（Murdoch *et al*.[2010]、Rosa[2010]、Barisani *et al*.[2011]）。

こうした中間者攻撃に対して EMVCo は、現行の EMV 仕様のままでも影響を限定的なものに止める対応は可能であるとの声明を公表しており、想定されるリスクを十分に評価したうえで IC カード利用システムを適切に構築・運用する

---

[1] 現行の EMV 仕様（4.2 版）は、4 分冊（Book 1～4）の構成である（EMVCo[2008abcd]）。本稿では、EMV 仕様の特定の箇所を参照する場合には、例えば「Book 1, 1 節」と表記する。

[2] 本統計データは、EMVCo の認定を取得したカードと端末について、EMVCo が、American Express、JCB、MasterCard、Visa の統計データを集約・公表したものである（EMVCo[2011a]）。

[3] SEPA 加盟国における IC カードと IC カード対応端末の普及率（2010 年末現在）は、カードが 81%、POS 端末および ATM が 96%である（European Payments Council[2011]）。

[4] わが国では、全キャッシュカード 4.7 億枚のうち約 12%（約 5,600 万枚）が IC カードであるほか、全 ATM 14.5 万台のうち約 79%（約 11.4 万台）が IC カード対応 ATM である（2010 年 3 月末現在、金融情報システムセンター[2010]）。また、日本クレジットカード協会によるアンケート（2010 年 7～8 月に実施、有効回答 1,963 人）によれば、クレジットカードを所持しているユーザのうち 65.5%が IC クレジットカードを所持している（日本クレジットカード協会[2010]）。

ことが重要である[5]。上述したように実際の運用環境と同等の実験環境において攻撃が成功したことが指摘されていることから、各攻撃が成功する条件や想定される対応について把握し、新規に構築するシステムあるいは運用中のシステムへの影響を評価し、必要に応じて問題発生時に備えた対応方針を検討しておくことが求められる。

本稿では、EMV 仕様において規定されている最低限の要件のみを満たす IC カード利用システムを検討対象とし、各攻撃による影響を分析する。最低限の要件のみを考慮することで、各攻撃に耐性をもたせるために追加的に求められる要件等を明らかにする。検討にあたっては、上記の中間者攻撃を 2 つに分けて扱う。1 つは、任意の暗証番号（以下、「PIN＜Personal Identification Number＞」）を用いて不正な取引を試みる攻撃（以下、「任意 PIN 利用型攻撃」）である。本攻撃は、本人確認時にどの方法が用いられたかをカードと端末がお互いに確認しない状況を利用している。そのため、本人確認に関するログをカードと端末が突合させることが対策となる。こうした対策には、取引時にリアルタイムで発行者のホストシステムが実施するタイプのものと、端末が実施するタイプのものが存在する。ただし、端末が実施するタイプの対策の場合、カードやホストシステムと異なり端末には発行者の管理が直接及ばないことから、端末の対策への対応をどのように進めていくかが課題となる。また、もう 1 つの中間者攻撃は、正規のユーザが行う取引において正しい PIN を盗取したうえで、攻撃者がその PIN を用いて不正な取引を試みる攻撃（以下、「盗取 PIN 利用型攻撃」）である。本攻撃（具体的には、Adida *et al*.[2006]による攻撃）による ATM を用いたシステムへの影響を検討した結果、ユーザが偽 ATM を利用し、かつ、正規の ATM が偽カードを受け入れてしまう場合には、不正な取引が成立する可能性を否定できないことが明らかとなった。本攻撃への技術的な対策は存在するが、導入コストの問題や利便性の低下等によりそうした対策の適用が困難な状況が想定される場合には、運用面での対策が一層重要になる。

以下、本稿では、2 節において、任意 PIN 利用型攻撃および盗取 PIN 利用型攻撃を理解するうえで必要となる EMV 仕様に係るセキュリティ機能を概説し、3 節において各攻撃を説明する。4 節において各攻撃への対策について検討し、その結果を踏まえた金融機関としての留意点を 5 節において考察する。

[5] Murdoch *et al*.[2010]が指摘する攻撃に対して EMVCo は、取引データの検査、不正な取引パターンに基づく検査、ログ解析等の対策を挙げつつ、本攻撃による経済的な影響は限定的であるとの声明を公表している（EMVCo[2010]）。また、Barisani *et al*.[2011]が指摘する攻撃に対して EMVCo は、本攻撃が盗取した IC カードを利用することから、盗取したカードを用いた不正な取引に対する既存の対策が利用可能であるとの声明を公表している（EMVCo[2011b]）。

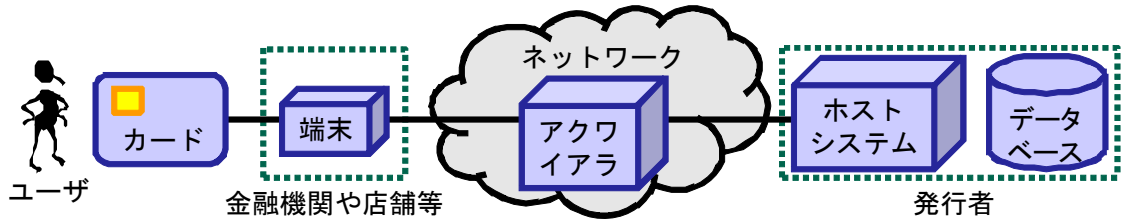
2. EMV 仕様のセキュリティ機能と取引の流れ

本節では、EMV 仕様に対する中間者攻撃を理解するうえで必要となる知識として、EMV 仕様が想定する IC カード利用システムや取引時に利用される EMV 仕様の各セキュリティ機能等について説明する。

2.1 IC カード利用システムの全体像

EMV 仕様は、IC カード利用システムにおける IC カードと端末の技術的な要件や通信プロトコル等を定めた業界標準であり、国際的に広く利用されている。EMV 仕様は、最低限の要件やオプションを規定しているに過ぎず、IC カード利用システムを構築するためには、EMV 仕様をベースとして追加の仕様を決定する必要がある。例えば、VISA、MasterCard、JCB 等の国際ブランドは、こうした追加仕様（「ブランド仕様」と呼ばれる）を策定している[6]。また、わが国では、こうした追加仕様として、銀行系カード会社で構成される日本クレジットカード協会が「IC カード対応端末機能仕様書」を策定しているほか、全国銀行協会が「全銀協 IC キャッシュカード標準仕様」を策定している。

本稿では、EMV 仕様が想定する IC カード利用システムを以下の要素からなるモデルとして扱う（図表 1 参照）。



図表 **1**. IC カード利用システムの全体像

カード：アカウントに対して発行者が発行する IC カード。IC カードには、アカウント番号、ユーザ名、有効期限等のカードに固有のデータ（以下、「カード固有データ」）が発行時に記録される。カード固有データ全体に対する発行者のデジタル署名も IC カードに記録される。

ユーザ：発行者からカードの発行を受けた利用者。「カード所持者」とも呼ばれる。

端末：リーダ・ライタを介してカードと通信するほか、アクワイアラと通信する装置。また、端末は、PIN を入力する装置（「PIN パッド」と呼ばれる）

[6] 例えば、VISA は、ブランド仕様として「Visa Integrated Circuit Card Specification （VIS）」を策定している（Visa International [2001ab]）。

を備える。こうした端末としては、ATM や CAT[7]が挙げられる。

アクワイアラ：端末およびホストシステムと通信を行うエンティティ。アクワイアラは、各店舗の端末に対してリスク管理上の設定を行う。本稿では、明示的にアクワイアラとホストシステムを区別する必要がある場合を除いて、アクワイアラを省略して議論する。

ホストシステム：カードの発行や取引の承認を行う発行者のサーバ。ホストシステムは、各カードのカード固有データをデータベースで管理している。

2.2 想定する IC カード利用システム

本稿が検討対象とする中間者攻撃については、EMV 仕様において規定されている最低限の要件のみでは防ぐことが困難なケースがあると考えられるが、実際に運用されている IC カード利用システムでは、追加仕様の中でそうした攻撃への対策を規定している場合もある。そこで、本稿では、中間者攻撃に備えるためには EMV 仕様の最低限の要件以外にどのような要件等が必要となるか、を明らかにするために検討を行う。具体的には、EMV 仕様の中で最低限規定されている要件だけを考慮した IC カード利用システムを想定し、中間者攻撃による同システムへの影響を整理したうえで対策を検討する。こうした検討結果の活用方法としては、追加仕様に反映させる、あるいは、今後 EMV 仕様が改訂される際に反映させるという選択肢が考えられる。

2.3 EMV 仕様のセキュリティ機能

EMV 仕様は、取引におけるリスクを管理するために様々なセキュリティ機能を用意している。代表的な機能として、カード認証（Card Authentication）、本人確認（Cardholder Verification[8]）、取引照会用の暗号情報（AC＜Application Cryptogram＞）の生成（AC generation。以下、「AC 生成」）が挙げられる。これらの機能を取引の流れに沿って説明すれば以下のとおりである。

ユーザが端末にカードを挿入すると、まず、端末により当該カードが真正であることを確認するために「カード認証」が行われる。次に、カードを提示したユーザが本人であることを「本人確認」によって確認する。これらの結果や取引の金額や日時といった当該取引に関するデータ（以下、「取引データ」）を基に当該取引を承認するか否かが決定される。この際、取引データの真正性や当該取引にカードが利用されたことを保証するために「AC 生成」が行われる。

---

[7] Credit Authorization Terminal（信用照会端末）の略。クレジットカードの信用照会を行う端末。POS（Point-Of-Sale）端末と一体化されているケースもある。

[8] 直訳すれば「カード所持者確認」であるが、本稿では読み易さの観点から「本人確認」と表記する。

なお、この処理手順は一例であり、カード認証の前に本人確認を行うケースや本人確認を省略するケースも EMV 仕様を実装した IC カード利用システムとして存在しうる。

これらのセキュリティ機能の中には、複数の処理方法が想定されているものがある。その場合は、カードおよび端末に設定された条件[9]と当該取引のリスクに応じて処理方法が選択される。各セキュリティ機能の具体的な内容は以下のとおりである。

2.3.1 カード認証

EMV 仕様では、カード認証を行う方法として、静的データ認証、動的データ認証、動的データ認証と AC 生成を組み合わせた方式の 3 つのカード認証方法が用意されている[10]。

静的データ認証（SDA＜Static Data Authentication＞）：カードが送信したカード固有データおよび対応するデジタル署名を用いて、端末がカード固有データの真正性を検証する処理。

動的データ認証（DDA＜Dynamic Data Authentication＞）：静的データ認証と同様にカード固有データの真正性の検証を行い、そのうえで動的なデータの真正性の検証を行う処理。動的なデータの検証は、端末が送信する乱数やカードが生成した乱数等に対するデジタル署名をカードが生成し、これを端末が検証するという手順で行われる。動的データ認証をサポートするカードには、発行時に当該カード用の公開鍵と秘密鍵のペアが格納される。

動的データ認証と AC 生成を組み合わせた方式（以下、「CDA＜Combined DDA/Application Cryptogram generation＞」）：動的データ認証と後述する AC 生成を組み合わせた処理。組み合わせることで、カードと端末間の通信回数の軽減が図られている。また、カードが AC を生成したうえでデジタル署名を付与するため、端末はカードと端末間の通信路上で AC が改ざんされたか否かを検証できる。ただし、AC を生成・検証するための鍵は、カードとホストシステム間でのみ共有されるため、端末は、AC が取引データに基づき正しく生成されているか否かを検証することができない。

---

[9] カード側の条件は、発行者のリスク管理の方針に基づき決定される。端末側の条件は、アクワイアラのリスク管理の方針に基づき決定される。これらの条件は、発行者やアクワイアラのビジネス判断に委ねられており、EMV 仕様には記述されていない。

[10] EMV 仕様では、カード認証方法を選択する方法を規定している（Book 3, 10.3 節）。具体的には、カードと端末が共通にサポートするカード認証方法のうち、最もセキュリティ・レベルの高い方法が選択される。

EMV 仕様では、取引に関する端末用のログファイルとして、「TSI（Transaction Status Information）」と「TVR（Terminal Verification Results）」が用意されている。TSI にはカード認証を実行したことが記録され、TVR にはカード認証によりデータの改ざんを検知した場合にその旨が記録される。

2.3.2 本人確認

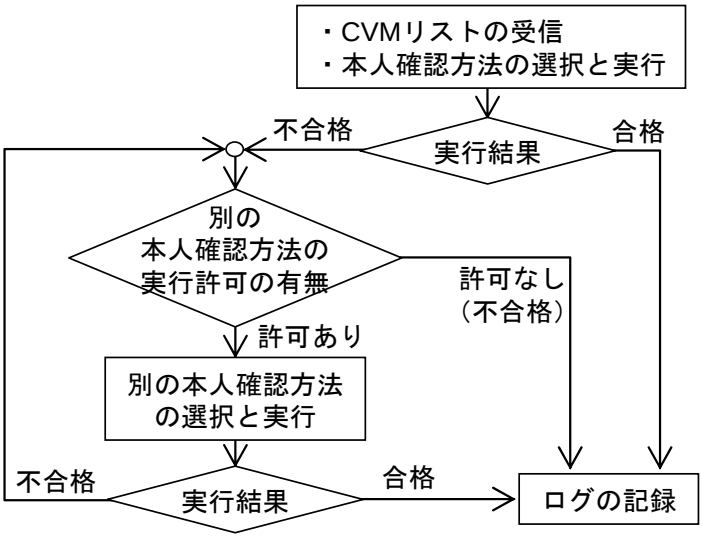
EMV 仕様では、リスクに応じて本人確認方法を使い分けることを可能とする仕組みを導入しているため、カードや端末がそれぞれ複数の本人確認方法をサポートしているケースがある。そのため、本人確認処理は、本人確認方法の選択と実行という 2 段階で構成される。

本人確認方法の選択では、まず、カードから端末に本人確認方法（CVM＜Cardholder Verification Method＞）のリスト（以下、「CVM リスト」）が送信される（図表 2 参照）。CVM リストは、カードがサポートする本人確認方法を優先度順にリスト化したデータであり、本人確認方法毎に当該方法を選択する際の条件（例えば、取引金額が x 円以上等）が付与されている。端末は、優先度の高いものから順に、条件を満足するか否か、端末が当該方法をサポートしているか否かを確認したうえで実行する本人確認方法を決定する。

また、ある本人確認方法が実行され、その結果が不合格となった場合、別の本人確認方法の実行を認めるケースと認めないケースがある（図表 3 参照）。認めるか否かに関する情報も CVM リストに含まれる。なお、CVM リストは、カード固有データの 1 つである。

優先度	本人確認方法	選択する際の条件
1	オフライン PIN 認証	3,000 円以下
2	手書き署名	3,000 円以下
3	オンライン PIN 認証	3,000 円以上

図表 **2**. CVM リストの例



図表 **3**. 本人確認の処理フロー

実行される本人確認方法について EMV 仕様では、オフライン PIN 認証、オンライン PIN 認証、手書き署名を用意している[11]。各本人確認方法の具体的な内容は次のとおりである。

オフライン PIN 認証：ユーザが端末に入力した PIN がカードに送信され、内部の参照用 PIN との照合をカードが行う処理。端末が PIN を送信する際、カードの公開鍵で暗号化するケース（以下、「オフライン PIN 認証（暗号文）」）と暗号化しないケース[12]（以下、「オフライン PIN 認証（平文）」）がある。また、繰り返し PIN の照合を行うことで正しい PIN を探索する攻撃（いわゆる、PIN の全数探索）を防ぐために、カードには「PIN Try Counter」と呼ばれるカウンタが用意されている。カウンタの値は、PIN の照合が不合格になるたびに減少し[13]、ゼロになるとそれ以降の PIN の照合を実行することができなくなり、その結果、取引を行うことができなくなる（以下、この状態を「PIN ブロック状態」と呼ぶ）。

オンライン PIN 認証：ユーザが入力した PIN を端末が暗号化したうえでホストシステムに送信し、ホストシステム内で照合する処理。オフライン PIN 認証に用いる PIN（以下、「PIN（オフライン）」）とオンライン PIN

[11] オフライン PIN 認証と手書き署名を同時に実行するといった複数の本人確認方法の併用が可能であるほか、現行の EMV 仕様では触れられていない本人確認方法（例えば、生体認証等）を追加することも可能である。

[12] 例えば、公開鍵暗号をサポートしていないカードを用いた取引において、端末とカード間の通信路の安全性が確保されていることを前提に選択されることが考えられる。

[13] 通常、PIN Try Counter は、照合結果が合格となった際に初期値にリセットされる。

認証に用いる PIN（以下、「PIN（オンライン）」）は、それぞれ別の値を設定可能である。

手書き署名：ユーザが手書きした署名を店舗等のスタッフが目視で確認する処理。

端末は、本人確認に関するログを前述の TSI と TVR に記録するほか、「CVMR（CVM Results）」にも記録する（図表 4 参照）。一方、カードには、「IAD（Issuer Application Data）」と呼ばれるログファイルが用意されているが、EMV 仕様では、同ファイルに記録されるログ項目やそのフォーマットは発行者が決定する扱いとしており、本人確認に関するログの記録については明示的に求められていない（Book 3, Annex A1）。

ログファイル	記録場所	記録される内容	
		実行に関するログ	結果に関するログ
TSI	端末	実行した旨を記録	記録しない
TVR	端末	記録しない	不合格になった旨を記録
CVMR	端末	実行した本人確認方法を記録	結果（合格・不合格・不明(注)）を記録

（注）本人確認の結果が不明として扱われるケースとしては、例えば、手書き署名の確認を店舗等のスタッフが行った際に、その確認結果を端末に入力せずに取引処理を続ける状況が想定される。

図表 **4**. 本人確認に関するログ

2.3.3 AC 生成とその利用

AC を生成・検証するメカニズムについて概説したうえで、取引のリスクに応じて AC を検証するタイミングを選択するという EMV 仕様のリスク管理について説明する。

① AC の生成と検証

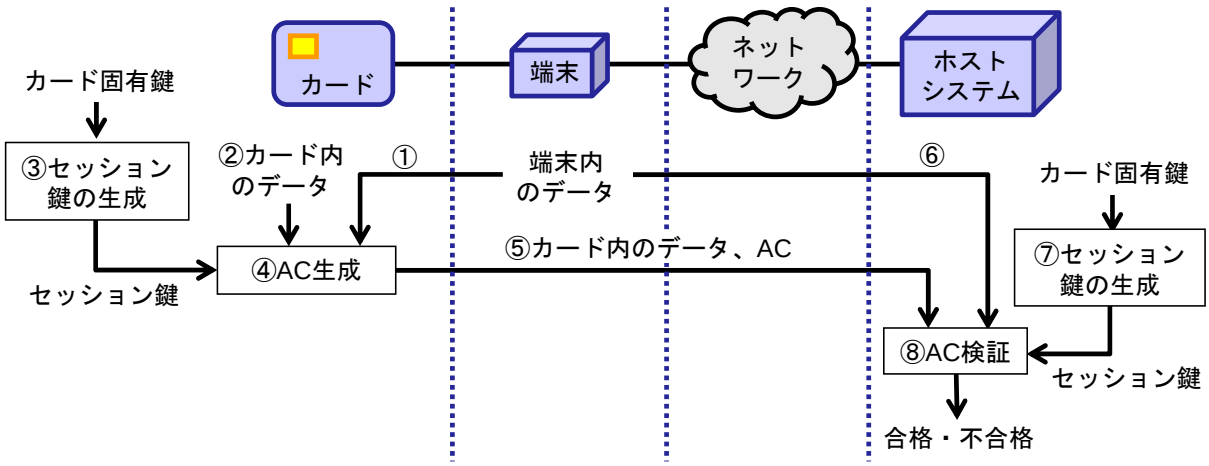
端末はカードに AC の生成を指示する前に、カード認証および本人確認の結果や、取引データ（金額、日付等）を基に当該取引の扱いの案を端末サイドで定める。取引の扱いには、「オフラインで拒否する」、「オフラインで承認する」、「ホストシステムに取引を承認するか否かを照会する」という 3 つの候補がある。

次に、端末はカードに当該取引の扱いに関する案を提示するとともに、AC の生成を指示する。端末から AC 生成の指示を受けてカードは、端末による当該取引の扱いの案に対し、取引データと発行者が予め設定した条件に基づき当該取

引の扱いをカードサイドで判断する。その際、参照した取引データの真正性と当該取引へのカードの関与を保証するために、取引データに対する AC を生成する（図表 5 参照）。当該取引の扱いに関するカードの判断内容は、「CID（Cryptogram Information Data）」と呼ばれるデータに記録され、端末に送信される。端末は、受信した CID を踏まえて当該取引の扱いを最終決定する[14]。

AC は、取引データに付与されるメッセージ認証子であり、デジタル署名と同じくデータの真正性の確認と認証に利用することができる。デジタル署名では生成と検証にそれぞれ秘密鍵と公開鍵を用いるのに対し、メッセージ認証子では生成と検証に同一の暗号鍵を用いる点が異なる。EMV 仕様では、カードが AC を生成し、それをホストシステムが検証することを想定している。ホストシステムは、カード発行時に「カード固有鍵」をカードに格納しておき、ホストシステムとカードがこの固有鍵から取引毎に異なる値の鍵（以下、「セッション鍵」）を生成・共有できるようにしている。そのため、取引データが改ざんされた場合、ホストシステムはセッション鍵を用いて AC を検証することで改ざんを検知できるが、端末は AC を検証できないため必ずしも取引データの改ざんを検知できるとは限らない[15]。

また、どの取引データを基に AC を生成するかは個々の発行者のビジネス判断に委ねられている。EMV 仕様では、AC 生成時に利用する取引データについて TVR を含む必要最低限の項目を示しているものの、TSI、CVMR については触れていない（Book 2, 8.1.1 節）。



（備考）AC の生成・検証は、例えば、図表中の①～⑧の順に実行される。

図表 **5**. AC の生成と検証（概念図）

[14] 例えば、端末からカードに「当該取引をオフラインで承認する」という案を提示したとしても、カードが「当該取引をオフラインで拒否する」と判断した場合には、当該取引はホストシステムに照会されることなく拒否される。

[15] カード認証により取引データの改ざんを検知できるケースもある。

② AC を検証するタイミングによるリスク管理

EMV 仕様は、取引金額や利用環境等の取引のリスクに応じたリスク管理を可能とする仕組みを用意している。具体的には、カードの発行者がホストシステムを用いて当該取引を成立させるか否かを即時に検証する「オンライン取引照会」と、店舗等の端末に設定された取引条件に従って当該取引を成立させるか否かを決定する「オフライン取引照会」の双方に対応可能な仕組みが用意されている。リスクが高いと判断された取引では、オンライン取引照会が選択される。オフライン取引照会では、取引時のホストシステムへの照会を省略することで処理時間や通信コストの軽減等を図っているほか、取引後に当該取引に対する端末の決定が適切か否かをホストシステムが検証することによりリスク管理を可能としている。

AC を検証するタイミングと端末が最終決定する当該取引の扱いの関係について整理すると、オンライン取引照会の場合には「ホストシステムに取引を承認するか否かを照会する」が選択され、オフライン取引照会の場合には「オフラインで拒否する」と「オフラインで承認する」のいずれかが選択される。また、AC を検証するタイミングとホストシステムに接続するタイプの本人確認（具体的には、オンライン PIN 認証）について補足すると、EMV 仕様では、本人確認の際に接続するか否かと AC 生成の際に接続するか否かは論理的には独立している。例えば、オンライン PIN 認証が実施された場合でもオフライン取引照会が選択される可能性がある。

3. 想定する中間者攻撃

本節では、EMV 仕様に対して指摘されている中間者攻撃を 2 つに分けたうえで、各攻撃の前提条件や処理手順を説明する。

3.1 想定する中間者攻撃のタイプと共通の前提条件

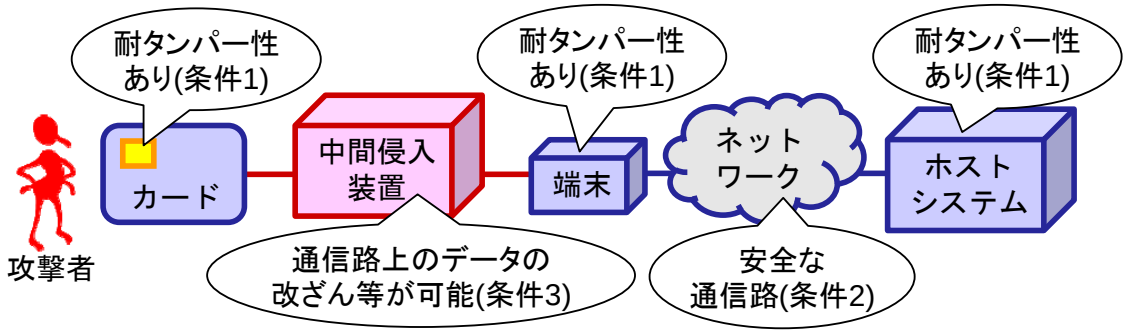
EMV 仕様に対して指摘されている中間者攻撃（Adida *et al*.[2006]、Murdoch *et al*.[2010]、Barisani *et al*.[2011]等）は、不正な取引を成立させるために、カードと端末の間に攻撃用の装置（以下、「中間侵入装置」）を挿入している。本稿では、「不正な取引が成立する」とは、取引時に端末あるいはホストシステムがデータの改ざん等の異常をリアルタイムに検知できない状況を意味するものとする。これらの攻撃について正しい PIN を利用するか否かという観点から、正しい PIN を利用しなくてもよい「任意 PIN 利用型攻撃」（Murdoch *et al*.[2010]）と正しい PIN を必要とする「盗取 PIN 利用型攻撃」（Barisani *et al*.[2011]、Adida *et al*.[2006]）に分けて検討する。

各攻撃について、共通する前提条件は以下のとおりである（図表 6 参照）。

条件 1：攻撃者は、カード、端末、ホストシステムを解析し、内部のデータを直接改ざん・抽出したり、内部機能を改変したりすることはできない。つまり、カード、端末、ホストシステムは耐タンパー性[16]を有する。

条件 2：端末とホストシステム間の通信は、物理的あるいは暗号技術により保護されており、攻撃者は、この通信路上のデータを盗聴・改ざん・遮断することができない。

条件 3：攻撃者は、カードと端末の間に中間侵入装置を挿入し、カードと端末間の通信を盗聴・改ざん・遮断可能である。



図表 **6**. 各タイプの攻撃に共通の前提条件

次に、任意 PIN 利用型攻撃（3.2 節）、Barisani *et al.*[2011]による盗取 PIN 利用型攻撃（3.3 節）、Adida *et al.*[2006]による盗取 PIN 利用型攻撃（「リレー攻撃」とも呼ばれる。3.4 節）についてそれぞれ説明する。

3.2 任意 PIN 利用型攻撃

Murdoch *et al.*[2010]が指摘する任意 PIN 利用型攻撃は、盗取したカードと中間侵入装置を用いる。本人確認については、本人確認方法としてオフライン PIN 認証を想定しており、本来カードが生成するはずの認証結果を中間侵入装置が偽造することで、端末に対して本人確認に合格したように見せ掛けている。実際にカードが PIN の照合を行わないため、任意の PIN を用いてなりすましを行うことができる。また、カード認証と AC 生成の各処理については、盗取したカードに処理を行わせている。

本攻撃の前提条件と手順は、それぞれ以下のとおりである。

[16] 耐タンパー性は、デバイスを解析して内部のデータを盗取したり、機能を改変したりする攻撃への耐性のこと。

3.2.1 任意 PIN 利用型攻撃の前提条件

任意 PIN 利用型攻撃では、3.1 節で示した共通の前提条件（条件 1～3）に加えて、以下の前提条件を想定している。

条件 4：攻撃者は、正規のユーザのカードを盗取できる。
条件 5：本人確認方法として、オフライン PIN 認証（平文）またはオフライン PIN 認証（暗号文）が選択される。
条件 6：カードは、本人確認に関する端末のログファイル CVMR を用いて、実際に実行された本人確認方法の確認を行わない。
条件 7：ホストシステムは、カードと端末のログファイル（IAD と CVMR）を用いて、実際に実行された本人確認方法の確認を行わない。

上記の条件 6 と条件 7 については、EMV 仕様で次のように扱われている。まず、CVMR がカードおよびホストシステムに送信されるか否かをみる。CVMR は、カード認証および AC 生成の各処理において、カードが端末に要求した場合に端末からカードに送信されるものの、EMV 仕様はこれを必須とはしていない。また、EMV 仕様は、CVMR のアクワイアラへの送信について規定しているものの、アクワイアラからホストシステムへの送信については EMV 仕様の範囲外のため言及していない（Book 4, 12.1.1 節、同 12.1.2 節）。次に、IAD がホストシステムに送信されるか否かをみる。EMV 仕様は、AC 生成の処理において AC とともに IAD を端末に送信することをオプションとして規定しているが、必須とはしていない（Book 2, 6.6.1 節）。また、端末が IAD を受信した場合にはアクワイアラに送信することを規定しているが、アクワイアラからホストシステムへの IAD の送信については EMV 仕様の範囲外のため言及していない（Book 4, 12.1.1 節、同 12.1.2 節）。

3.2.2 任意 PIN 利用型攻撃の手順

任意 PIN 利用型攻撃は、以下の手順で実行される（図表 7 参照）。

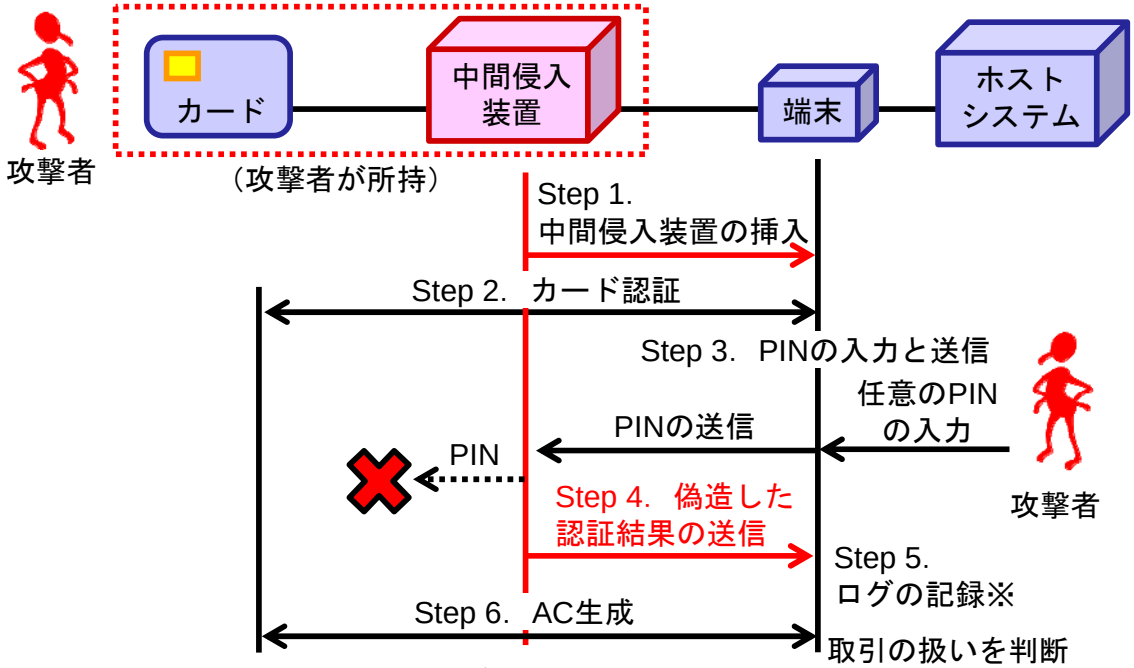
Step 1. 攻撃者が、盗取したカードをセットした中間侵入装置を正規の端末に挿入する。
Step 2. 中間侵入装置を介して、カードと端末間でカード認証が実行される。
Step 3. 本人確認では、前提条件によりオフライン PIN 認証が選択され、攻撃者が任意の PIN を入力する。端末は、入力された PIN をカードに向けて送信する。
Step 4. 攻撃者は、中間侵入装置を用いて端末から PIN を受信したうえで、合格

という認証結果を偽造し端末に返信する。オフライン PIN 認証の結果は、暗号化されていないため容易に偽造可能である。なお、攻撃者は端末から受信した PIN をカードに転送しない。

Step 5. 端末は、合格の認証結果を受信し、TSI に本人確認を実行した旨を記録するほか、オフライン PIN 認証を実行し、その結果が合格である旨を CVMR に記録する。なお、カードは、PIN を受信していないため、オフライン PIN 認証を実行したというログは発生しない。

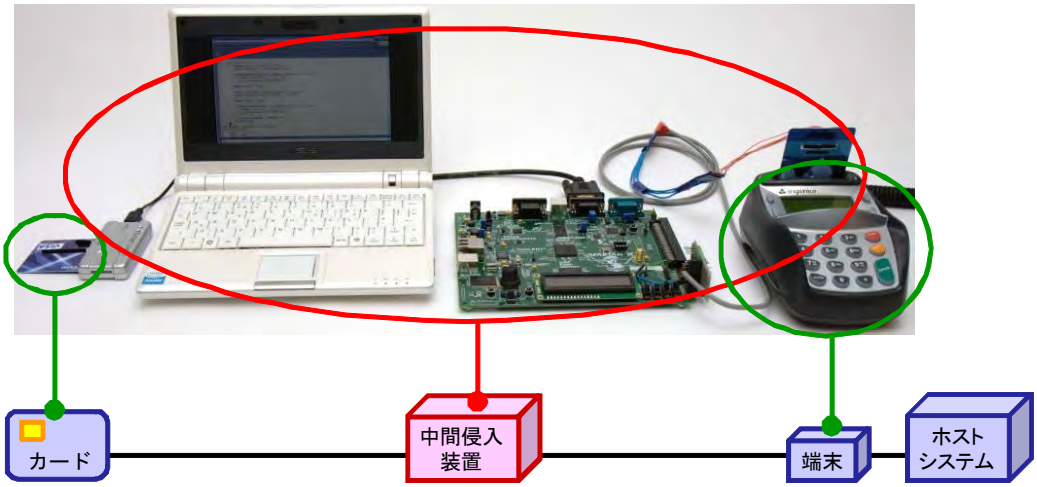
Step 6. 中間侵入装置を介して、カードと端末間で AC 生成が実行される。

この攻撃を実際の運用環境と同様の実験環境において試行し、複数のカードで不正な取引が成立しうることが報告されている（Murdoch *et al.*[2010]、Rosa[2010]）。特に、Murdoch *et al.*[2010]では、オンライン取引照会のケースでも不正な取引が成立しうることが示されている。Murdoch *et al.*[2010]における実験で利用された装置は図表 8 のとおりである[17]。



図表 7. 任意 PIN 利用型攻撃の手順

[17] 実験の様子を撮影した動画は、BBC[2010]において閲覧可能である。



（備考）Murdoch *et al*.[2010]の Figure 4 に説明用情報を追加。

図表 **8**. 任意 PIN 利用型攻撃の実験装置

3.2.3 任意 PIN 利用型攻撃の拡張

Murdoch *et al*.[2010]の中間者攻撃をベースに、他の取引データも改ざんすることで攻撃の適用範囲を拡張できる可能性がある。

Rosa[2010]では、盗取したカードが PIN ブロック状態であっても上記の攻撃を適用可能にする方法が指摘されている。具体的には、PIN ブロック状態のカードを用いた場合、オフライン PIN 認証においてカードから PIN Try Counter の値としてゼロが送信される。この値を中間侵入装置においてゼロでない値（例えば、3）に改ざんすることで、端末に当該カードが PIN ブロック状態ではないと認識させることができる。実際の運用環境と同様の実験環境において、PIN ブロック状態のカードでも不正な取引が成立しうることが報告されている（Rosa[2010]）。

このほか、カードから端末に送信される CID（当該取引の扱いに関するカードの判断を表すデータ）を改ざんすることも考えられる。例えば、カードが「オフラインで拒否」として CID を生成・送信したとしても、これを「オフラインで承認」と攻撃者が改ざんした場合には、不正な取引が成立する可能性がある。

3.3 Barisani *et al*.[2011]による盗取 PIN 利用型攻撃

Barisani *et al*.[2011]が指摘する盗取 PIN 利用型攻撃は、PIN（オフライン）の盗取を試みるフェーズ（フェーズ 1）と、盗取した PIN（オフライン）を用いて不正な取引を試みるフェーズ（フェーズ 2）から構成される。フェーズ 1 では、予め端末に中間侵入装置を取り付けておき、正規のユーザが自分のカードを用いて取引を行う際に入力する PIN（オフライン）の盗取を試みる。フェーズ 2 では、当該ユーザから盗取したカードとフェーズ 1 で盗取した PIN（オフライン）を用いて攻撃者が不正な取引を試みるため、中間侵入装置は不要であり、取引

時にオフライン PIN 認証が選択された場合に不正な取引が成立する可能性がある。当該ユーザの PIN（オフライン）と PIN（オンライン）が同じ値の場合には、オンライン PIN 認証が選択された場合でも不正な取引が成立する可能性がある。

なお、本攻撃で用いる中間侵入装置は、データの盗取のみを目的とする従来のスキミング装置とは異なり、盗取のほかにデータの改ざんや遮断を行う機能も有している。フェーズ 1 では、カードと端末間でやり取りされるデータを改ざんするため、当該ユーザの取引が成立しなくなる可能性がある。

本攻撃の前提条件と手順は、それぞれ以下のとおりである。

3.3.1 Barisani *et al*.[2011]による盗取 PIN 利用型攻撃の前提条件

盗取 PIN 利用型攻撃では、3.1 節で示した共通の前提条件（条件 1～3）に加えて、以下の前提条件を想定している。

条件 4：攻撃者は、正規のユーザのカードを盗取できる。
条件 8：中間侵入装置は、正規の端末に取り付けられている。
条件 9：端末は、オフライン PIN 認証（平文）をサポートしている。
条件 10：当該ユーザの PIN（オフライン）と PIN（オンライン）が異なる場合には、フェーズ 2 では、本人確認方法としてオフライン PIN 認証（平文）またはオフライン PIN 認証（暗号文）が選択される。

3.3.2 Barisani *et al*.[2011]による盗取 PIN 利用型攻撃の手順

盗取 PIN 利用型攻撃のフェーズ 2 は正規のユーザが行う取引の手順と同様であることから、フェーズ 1 に焦点を当てる。フェーズ 1 の手順は以下のとおりである（図表 9 参照）。

Step 1. 正規のユーザが、中間侵入装置を取り付けられた端末に正規のカードを挿入する。
Step 2. カードから CVM リストを含むカード固有データが送信される。その際、攻撃者は、中間侵入装置を用いて CVM リストをオフライン PIN 認証（平文）が選択されるように改ざんする。
—— なお、CVM リストがそもそもオフライン PIN 認証（平文）を優先する設定となっている場合には、攻撃者は改ざんを行わない。この場合、後述の Step 3 におけるカード認証の結果が合格となるが、以下では、CVM リストを改ざんするケースで説明する。
Step 3. 端末は、受信したカード固有データを基にカード認証を行う。CVM リストが改ざんされているため、カード認証の結果は不合格となる。

Step 4. 端末は、受信した（改ざんされた）CVM リストに基づき、本人確認方法としてオフライン PIN 認証（平文）を選択する。次に端末は、ユーザが入力した PIN（オフライン）を平文の状態でカードに向けて送信する。その際、攻撃者は、中間侵入装置を用いて PIN（オフライン）を盗取する。

Step 4 において、PIN（オフライン）の盗取というフェーズ 1 における目的は達成される。Barisani *et al.*[2011]では、実際に運用されている環境と同様の実験環境を構築し、Step 4 において PIN（オフライン）を盗取できることが報告されている。なお、この後の手順は、カードがオフライン PIN 認証（平文）をサポートしているか否かに応じて[18]、次の 2 つのケースが考えられる。

ケース 1. カードがオフライン PIN 認証（平文）をサポート

攻撃者は、中間侵入装置を用いて PIN（オフライン）をカードに転送する。その結果、カードが PIN（オフライン）の照合を行ったうえで合格の認証結果を返信すると考えられる。その後、中間侵入装置を介して、カードと端末間で AC 生成が実行される。

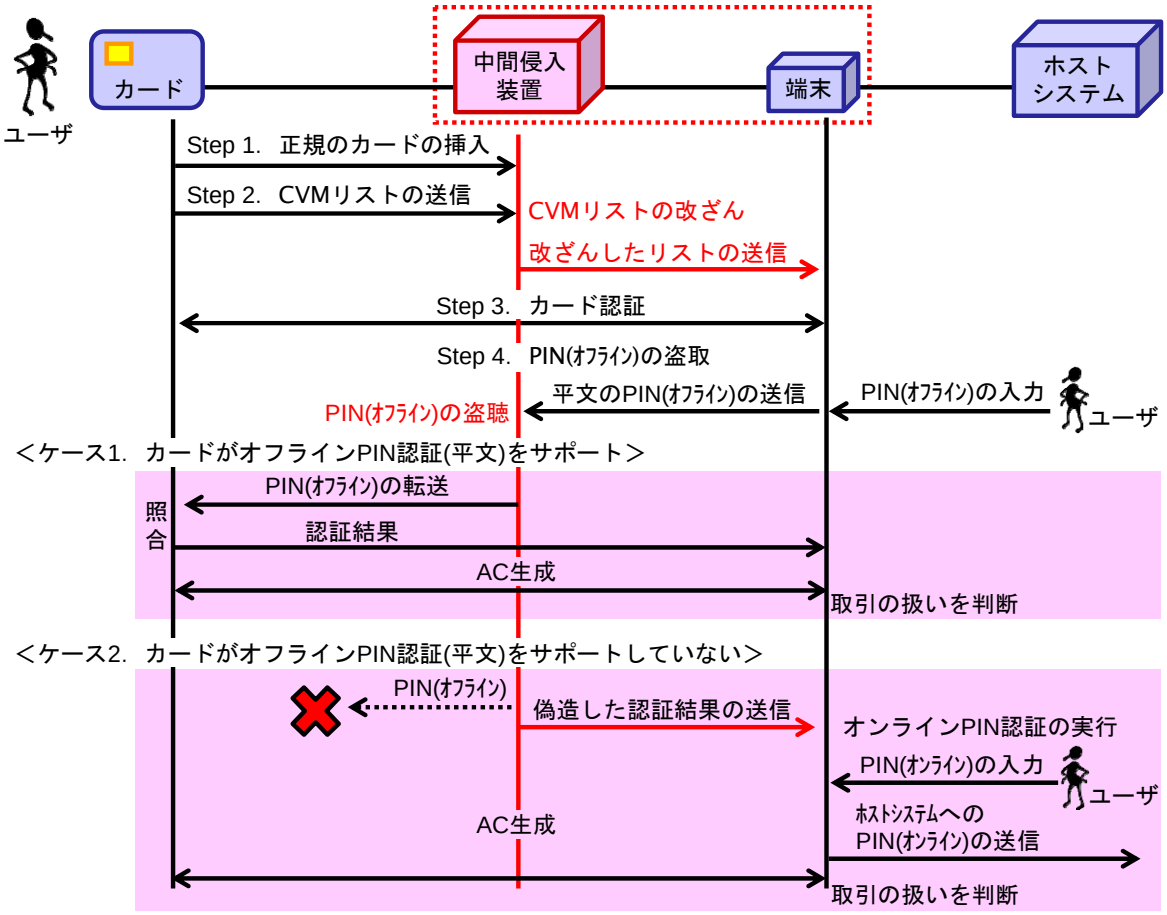
ケース 2. カードがオフライン PIN 認証（平文）をサポートしていない

攻撃者は、予め Step 2 において「最初にオフライン PIN 認証（平文）が選択され、本認証方法の結果が不合格の場合にはオンライン PIN 認証が選択される」ように中間侵入装置を用いて CVM リストを改ざんしておく。攻撃者は、カードに PIN（オフライン）を転送せず、中間侵入装置を用いて失敗の認証結果を偽造したうえで端末に返す。次に端末は、改ざんされた CVM リストに従いオンライン PIN 認証を選択し、ユーザが入力した PIN（オンライン）を暗号化したうえでホストシステムに送信する。その後、中間侵入装置を介して、カードと端末間で AC 生成が実行される。

このケースでは、ユーザに PIN の入力を 2 回要求することになるものの、最終的に実行される本人確認方法（オンライン PIN 認証）のログのみが記録されるため、オフライン PIN 認証（平文）の結果が不合格となったログは残らない[19]。また、端末がオンライン PIN 認証をサポートしていることが前提となる。

[18] 中間侵入装置は、CVM リストを盗聴することで、当該カードがオフライン PIN 認証（平文）をサポートしているか否かを確認できる。

[19] なお、オンライン PIN 認証用の PIN（オンライン）は、端末からカードを経由することなく直接ホストシステムに送信されるため、中間者装置で盗取することはできない。



図表 **9**. Barisani *et al*.[2011]による盗取 PIN 利用型攻撃の手順（フェーズ 1）

3.4 Adida *et al*.[2006]による盗取 PIN 利用型攻撃

Adida *et al*.[2006]による盗取 PIN 利用型攻撃では、ある店舗で取引を行おうとしているユーザのカードを、別の店舗の端末と密かに通信させることで、当該ユーザが意図しない不正な取引を試みる。攻撃者は、まず、正規のカードと通信可能な偽端末とこの偽端末と無線で通信する偽カードを用意し、協力者がいる店舗 1 に偽端末を設置したうえで、自分は偽カードを所持して店舗 2 で待機する。そして、正規のユーザが自分のカードを店舗 1 の偽端末に挿入したタイミングで攻撃者は偽カードを店舗 2 の正規の端末に挿入し、この偽端末と偽カードを介して、当該ユーザに本人が意図しない（店舗 2 における）取引を行わせるよう試行する。なお、前提条件 1 により正規の端末は耐タンパー性を有すると仮定していることから、偽端末は攻撃者が自作したものを想定する[20]。この偽端末と偽カードがセットで本攻撃における中間侵入装置となる。

本攻撃ではユーザが偽端末を利用すれば PIN の盗取が容易に行えると考えら

[20] この偽端末は、アクワイアラと通信する機能を有する必要はないため、EMV 仕様の知識があれば自作可能であると考えられる。

れることに加えて、盗取した PIN を利用することで本人確認方法としてオフライン PIN 認証およびオンライン PIN 認証のいずれが選択されても攻撃が成功しうるという点で強力な攻撃といえる[21]。本攻撃の前提条件と手順は、それぞれ以下のとおりである。

3.4.1 Adida *et al*.[2006]による盗取 PIN 利用型撃の前提条件

Adida *et al*.[2006]による盗取 PIN 利用型攻撃では、3.1 節で示した共通の前提条件（条件 1～3）に加えて、以下の前提条件を想定している。

条件 11：ユーザが偽端末を利用する。
条件 12：本人確認方法として、オフライン PIN 認証またはオンライン PIN 認証が選択される。

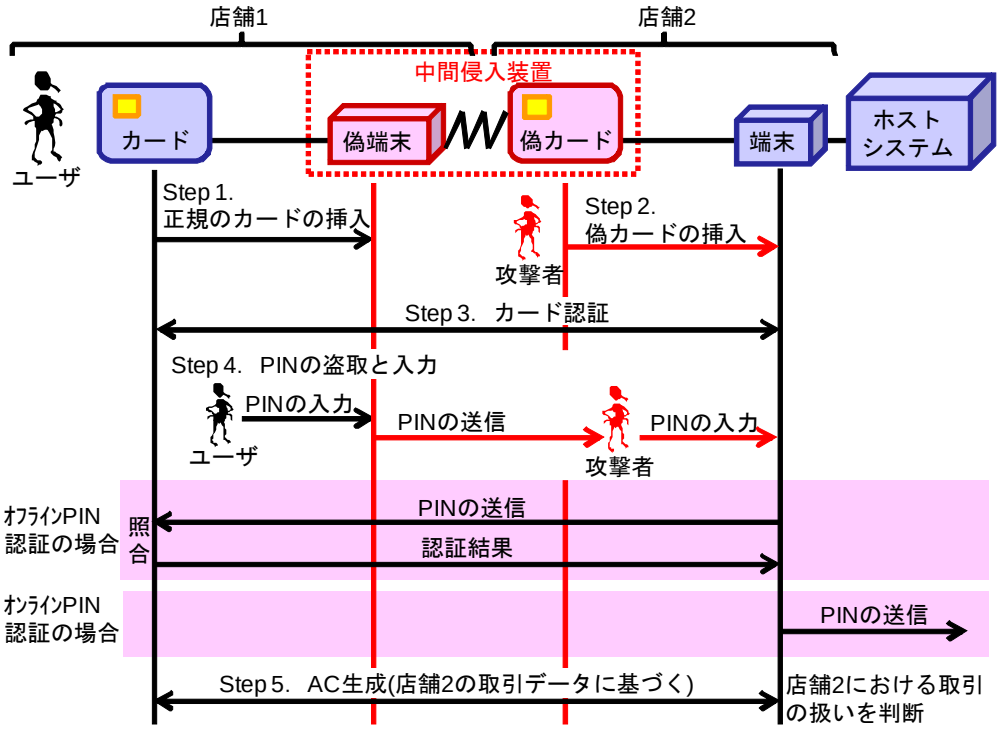
3.4.2 Adida *et al*.[2006]による盗取 PIN 利用型攻撃の手順

Adida *et al*.[2006]による盗取 PIN 利用型攻撃は、以下の手順で実行される（図表 10 参照）。

Step 1. 正規のユーザは､店舗 1 に設置された偽端末に正規のカードを挿入する。
Step 2. 偽端末に正規のカードが挿入されたことを確認したうえで[22]、店舗 2 に居る攻撃者は、偽カードを店舗 2 の正規の端末に挿入する。
Step 3. 偽端末と偽カードを介して、正規のカードと店舗 2 の端末間でカード認証が実行される。
Step 4. ユーザは、偽端末に PIN を入力する。攻撃者は、偽端末を利用して当該 PIN を盗取したうえで、店舗 2 の端末に入力する。入力された PIN は、選択された本人確認方法がオフライン PIN 認証かオンライン PIN 認証かに応じて、それぞれ次のように処理される。
（オフライン PIN 認証が選択された場合）攻撃者は、店舗 2 の端末が送信した PIN を、偽カードと偽端末を介して正規のカードに転送する。正規のカード内で PIN の照合が行われた後、攻撃者は、その結果を偽端末と偽カードを介して店舗 2 の端末に返信する。
（オンライン PIN 認証が選択された場合）店舗 2 の端末は、入力された PIN をホストシステムに送信する。

[21] 本攻撃と Murdoch *et al*.[2010]による任意 PIN 利用型攻撃を組み合わせれば、本人確認方法としてオフライン PIN 認証が選択されることが条件（前提条件 5）となるものの、正規のカードを盗取しない（前提条件 4 を想定しない）タイプの任意 PIN 利用型攻撃となる。
[22] 店舗 1 に居る協力者から別途連絡を受けるなどの方法が考えられる。

Step 5. 偽端末と偽カードを介して、正規のカードと店舗 2 の端末間で AC 生成が実行される。



図表 **10**. Adida *et al.*[2006]による盗取 PIN 利用型攻撃の手順

この攻撃を実際の運用環境と同様の実験環境において試行し、不正な取引が成立しうることが報告されている（Drimer and Murdoch[2007]）。

4. 想定する中間者攻撃への対策

前節で説明した各中間者攻撃が可能となる原因として、任意 PIN 利用型攻撃についてはコマンドに対するレスポンスを攻撃者が偽造可能である点、Barisani *et al.*[2011]による盗取 PIN 利用型攻撃についてはデータの改ざんを検知した後の処理が適切に行われないケースがある点、Adida *et al.*[2006]による攻撃による盗取 PIN 利用型攻撃についてはユーザが端末や取引データを確認する手段が提供されていない点がそれぞれ考えられる。本節では、こうした点を踏まえて各攻撃への対策について検討する。

4.1 共通の対策

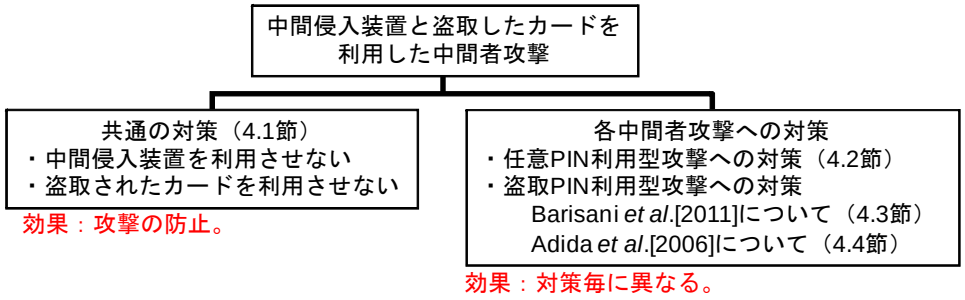
不正な取引を試みる攻撃に対しては、「攻撃を防止するための対策」と、防止できない場合に備えた「攻撃が実施されたことを事後に検知するための対策」および「攻撃が繰り返し実施されることによる被害の拡大を防止するための対

策」という 3 段階の対策が考えられる。

攻撃を防止するという観点から任意 PIN 利用型攻撃と盗取 PIN 利用型攻撃に共通の対策を考えると、いずれの攻撃も中間侵入装置の利用が前提となっていることから、中間侵入装置を利用させないことが対策となる。例えば、任意 PIN 利用型攻撃および Adida *et al*.[2006]による盗取 PIN 利用型攻撃では、攻撃者が正規のカードの代わりに中間侵入装置（偽カードを含む）を端末に挿入しようと試みるため、(a)店舗等のスタッフが端末の側にいる場合にはユーザが正規のカードを提示しているか否かをスタッフが目視等で確認すること、(b)端末に中間侵入装置を挿入させないようにすること[23]、(c)中間侵入装置が端末に挿入されたとしても動作しないようにすること[24]が考えられる。また、Barisani *et al*.[2011]による盗取 PIN 利用型攻撃では、攻撃者が正規の端末に中間侵入装置を取り付けるため、端末に中間侵入装置が取り付けられていないことをスタッフが目視等で定期的に確認することが考えられる。

このほか、任意 PIN 利用型攻撃や Barisani *et al*.[2011]による盗取 PIN 利用型攻撃では、盗取したカードを用いることから、攻撃を防止するために従来から行われている「ユーザがカードの紛失・盗難に気付いた時点で速やかに発行者に連絡することを徹底すること」も対策の 1 つになりえる（図表 11 参照）。

以下では、こうした対策が効果を発揮せず、攻撃者が中間侵入装置や盗取したカードを利用できるという条件のもとで有効な対策を各中間者攻撃について検討する。



図表 **11**. 中間者攻撃への対策の全体像

[23] 図表 8 で紹介した中間侵入装置は、正規のカードを読み取るリーダ部分、計算処理を行う本体、正規の端末に挿入する部分から構成され、各部分と本体がそれぞれケーブルで接続されているという実装形態となっている。この場合、ケーブルが付いたカードを挿入させないように、カード挿入後に端末のカード挿入口を物理的に閉じるという対策が考えられる。

[24] 図表 8 で紹介した実装形態のほかに、ケーブルではなく無線通信で中間侵入装置の本体と端末への挿入部分が通信するものも考えられる。この場合、カード挿入後にカードが外部と無線通信を行えないように端末側で電磁波シールドを施すなどの対策が考えられる。このほか、正規のカードの券面に偽造防止技術（例えば、ホログラム等。宇根・田村・松本[2009]に詳しい）を施しておき、この偽造防止技術を利用して端末が挿入されたカードが正規のカードか否かを検査するという対策も考えられる。

4.2 任意 PIN 利用型攻撃への対策

任意 PIN 利用型攻撃への対策については、本攻撃を指摘したケンブリッジ大学の研究グループによって提案されている（Murdoch[2009]、Murdoch *et al*.[2010]）。具体的には、動的データ認証、CDA、AC 生成を利用した対策が提案されている。本節では、同研究グループの研究成果を踏まえて、EMV 仕様の各セキュリティ機能を利用した場合に、任意 PIN 利用型攻撃に対してどの程度効果のある対策を講じることができるかを整理する。

任意 PIN 利用型攻撃における本人確認の処理をみると、カードはオフライン PIN 認証が実行されたとは認識していないのに対し、端末はオフライン PIN 認証が実行されたと認識しており、両者の認識に不整合が生じている。そのため、取引時にこうした不整合が生じているか否かを確認することが本攻撃への対策となる。具体的には、実行された本人確認方法に関するログをカードおよび端末がそれぞれ記録しておき、両者のログを突合させるという対策である。

EMV 仕様では、端末については、こうしたログを CVMR に記録するよう規定している。一方、カードについては、こうしたログの記録に関して規定していない（2.3.2 節参照）。そこで、本節では、カードは、IAD に「オフライン PIN 認証を実行したか否か」と「（同認証方法を実行した場合には）その結果」を記録すると仮定したうえで検討を行う[25]。なお、EMV 仕様は、IAD の仕様やフォーマットを発行者が決定する扱いとしており、IAD と CVMR の突合が可能なのは、カードおよびホストシステムに限られる。端末は、通常、IAD のフォーマットに関する情報を有しておらず IAD を解釈できないため、IAD を入手したとしても突合を行うことは困難であると考えられる。

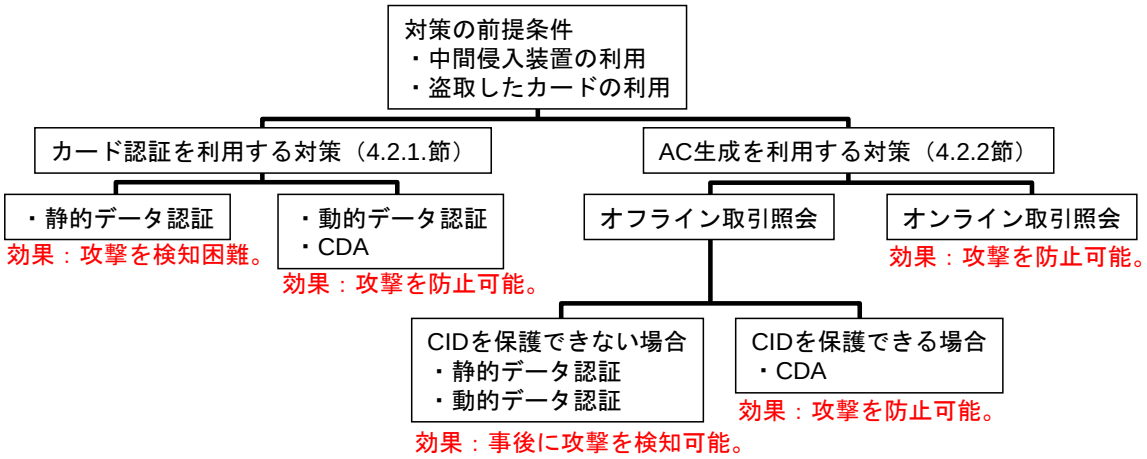
端末が CVMR をカードに送信する際、あるいは、ホストシステムに IAD を送るためにカードが IAD を端末に送信する際、攻撃者が中間侵入装置を用いてログが整合的になるように改ざんする可能性があるため、これらのログファイルを保護する必要がある。取引データを保護するために、カード認証および AC 生成を活用することができる。以下では、カード認証および AC 生成を利用した対策の可能性についてそれぞれ検討する（図表 12 参照）。

---

[25] こうしたログの項目を設定しているケースがある。例えば、VISA のブランド仕様 VIS（Visa International[2001a]の Appendix A.1）や CCD（Common Core Definition、Book 3, Annex C7.3）*が挙げられる**。

* CCD は、EMV 仕様中のオプションとしてのミニマム要件のセットであり、複数の国際決済ブランドによる共通利用が可能な追加仕様とともに利用される（EMVCo[2008abcd]）。EMV 仕様およびこのオプションを前提に「CPA（Common Payment Application）仕様」が策定・公表されている（EMVCo[2005]）。

** 厳密には、VIS も CCD 仕様も、IAD の一部として「CVR（Cardholder Verification Results）」を定義し、CVR にこれらのログを記録する扱いとしている。



図表 **12**. 任意 PIN 利用型攻撃への対策とその効果

4.2.1 カード認証を利用する対策

カード認証の各方法について保護対象となるデータを踏まえて対策に利用できるか否かを検討する。

① 静的データ認証の利用の可能性

保護対象は、発行者がカードに格納する静的なデータであり CVMR が含まれないため、静的データ認証を対策に利用できない。

② 動的データ認証の利用の可能性

保護対象は、カード内部のデータと端末から受信したデータであり CVMR を保護対象に含めることができるため、動的データ認証を対策に利用できる。具体的には、カードは、IAD と端末から受信した CVMR[26]の突合を行い、さらに CVMR と突合結果に対するデジタル署名を生成して端末に返信するという方法が考えられる。端末からカードに CVMR が送信される際に改ざんされた場合、あるいは、カードから端末に送信される突合結果が改ざんされた場合、端末がデジタル署名を検証した結果が不合格になるため検知できる[27]。

ログの突合により不整合が確認された場合の取引処理の流れについては、EMV 仕様では触れられていない。そこで、そうした取引処理の流れについて考えると、例えば、(a)実施した本人確認方法に関するログが整合的でないと判断

[26] 動的データ認証では、端末からカードに送信されるデータをカードが指定する。カードによる指定は、指定するデータ名を記録したリスト「DDOL（Dynamic Data Authentication Data Object List）」を端末に送信することで行われる。動的データ認証において、カードが端末から CVMR を受信するためには、DDOL の中で CVMR を指定すればよい。

[27] CVMR は、もともと端末に格納されているデータであり、カードから端末には送信されないため、カードから端末に返される CVMR を攻撃者が偽造するという状況を想定する必要はない。

した旨をカードや端末のログファイルに記録するという処理や、(b)本人確認の結果を不合格に変更するという処理等が想定される。なお、この対策では、本人確認に関するログファイルである CVMR を用いるため、カード認証の前に本人確認を実施しておく必要がある。

③ CDA の利用の可能性

CDA は、動的データ認証と AC 生成を組み合わせた処理であるため、動的データ認証と同様の対策が可能であるほか、AC 生成を活用した対策も可能である。AC 生成を活用した対策については、4.2.2 節で説明する。

4.2.2 AC 生成を利用する対策

保護対象は、カード内部のデータと端末から受信したデータであり IAD と CVMR を含めることができるため、AC 生成を対策に利用できる。具体的には次に示す方法が考えられる。まず、カードは、IAD と端末から受信した CVMR[28]の突合を行い、その結果等を基に当該取引の扱いを判断したうえでその判断内容を CID に記録する。例えば、ログの突合により不整合が確認された場合には、CID には、「当該取引をオフラインで拒否する」旨が記録される。次に、カードは、IAD、CVMR を含む取引データに対する AC を生成し、IAD、CID、AC 等のデータを端末に返信する [27]。

この対策の効果について、オンライン取引照会とオフライン取引照会の観点から考察する。オンライン取引照会では、ホストシステムが端末から即時に IAD、CVMR、AC 等のデータを受信し、IAD と CVMR の突合や AC の検証を実施可能であり、不正な取引の成立を防止できると考えられる。

オフライン取引照会では、ホストシステムが AC の検証や IAD と CVMR の突合を即時に実施できない。しかし、オフライン取引照会であっても、端末が改ざんの有無を検証したうえで CID を参照することができれば、不正な取引を防止可能である。カード認証方法の 1 つである CDA では、カードが CID に対するデジタル署名を生成することが EMV 仕様で規定されていることから、CDA が選択されている場合には不正な取引を防止可能であると考えられる。一方、静的データ認証や動的データ認証は、AC 生成を実施する前に処理を完了させておくことが EMV 仕様で規定されており、CID を保護することができない。この場合、不正な取引が成立した後に、ホストシステムがそれを検知することになる

[28] AC 生成または CDA では、動的データ認証と同様に、端末からカードに送信されるデータをカードが指定する。ここで用いられるリストは、「CDOL（Card Risk Management Data Object List）」と呼ばれており、AC 生成または CDA において、カードが端末から CVMR を受信するためには、CDOL の中で CVMR を指定すればよい。

と考えられる。

4.2.3 任意 PIN 利用型攻撃への対策のまとめ

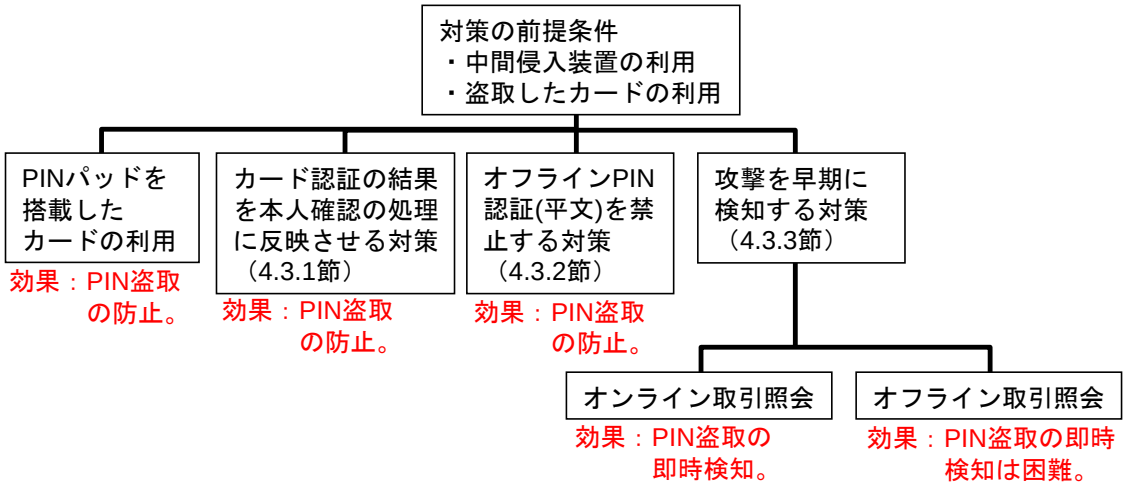
カード認証またはAC生成を利用した対策について整理すると(図表13参照)、オンライン取引照会を想定できる場合には、AC 生成を利用した対策により不正な取引を防止可能であることがわかる。オフライン取引照会を想定する場合には、動的データ認証または CDA を実行可能なカードを用いることで不正な取引を防止可能であることがわかる。また、カード認証として静的データ認証を想定する場合には、オフライン取引照会では不正な取引を即時に検知することが困難であることがわかる。

利用する機能	保護対象データ（想定条件）	検証するｴﾝﾃｨﾃｨ		端末やﾎｽﾄｼｽﾃﾑの対応例
		突合	改ざんの検知	
静的ﾃﾞｰﾀ認証	—	—	—	—
動的ﾃﾞｰﾀ認証	CVMR、突合結果	ｶｰﾄﾞ	端末	AC 生成の際に端末がｵﾌﾗｲﾝで取引拒否を判断する
CDA				
AC 生成	IAD、CVMR（ｵﾝﾗｲﾝ取引照会）	ﾎｽﾄｼｽﾃﾑ	ﾎｽﾄｼｽﾃﾑ	ﾎｽﾄｼｽﾃﾑが取引拒否を判断し、端末に伝える
	IAD、CVMR、CID（ｵﾌﾗｲﾝ取引照会、CDA）	ｶｰﾄﾞ	端末	AC 生成の際に端末がｵﾌﾗｲﾝで取引拒否を判断する
	IAD、CVMR（ｵﾌﾗｲﾝ取引照会、静的ﾃﾞｰﾀ認証または動的ﾃﾞｰﾀ認証）	ﾎｽﾄｼｽﾃﾑ	ﾎｽﾄｼｽﾃﾑ	取引成立後にﾎｽﾄｼｽﾃﾑが不正を検知する

図表 **13**. カード認証または AC 生成を利用した対策

4.3 Barisani *et al*.[2011]による盗取 PIN 利用型攻撃への対策

Barisani *et al*.[2011]による盗取 PIN 利用型攻撃への対策には、PIN の盗取を防止するものや、盗取された PIN を PIN の更新により無効化するものが考えられる。Barisani *et al*.[2011]では、PIN の盗取を防止するために、カードに PIN パッドを搭載することで通信路上で PIN を盗聴させないという対策を提案している。本節では、この対策以外の対策の可能性について検討する（図表 14 参照）。



図表 **14**. Barisani *et al.*[2011]による盗取 PIN 利用型攻撃への対策とその効果

4.3.1 カード認証の結果を本人確認の処理に反映させる対策

本攻撃では、改ざんされた CVM リストに基づいて本人確認方法が選択される点を利用している。そのため、PIN の盗取を防止するためには、本人確認処理の前にカード認証を実施し、その結果を本人確認処理に反映させるという対策が考えられる。具体的には、カード認証においてデータの改ざんを検知した場合、(a)本人確認処理を実施せずに、改ざんがあった旨を当該取引の扱いに反映させるという方法や、(b)本人確認処理を実施せずに直ちに当該取引を終了するという方法、(c)本人確認処理においてオフライン PIN 認証（平文）以外の本人確認方法を選択・実施するという方法が考えられる。なお、カード認証の結果を本人確認処理に反映させるために、本人確認処理の際に TVR を参照するという方法が考えられる。

EMV 仕様では、カード認証を実施してから本人確認を実施するという手順もその逆の手順も認めているものの、上記対策(a)～(c)を講じるためには、先にカード認証を実施することが求められる。また、EMV 仕様では、本人確認処理の際に TVR を参照することについては言及していないが（Book 3, 10.5 節）、上記対策(c)を講じるためには TVR の参照が必要となる。

4.3.2 オフライン PIN 認証（平文）を禁止する対策

上記の対策のほかに、PIN の盗取を防止するためには、端末がオフライン PIN 認証（平文）をサポートしないように予め設定しておくという対策が挙げられる[29]。この対策により端末からカードに平文のまま PIN が送信されることはなくなるため、中間侵入装置を用いた盗聴への耐性をもたせることができる。

[29] 端末がサポートする本人確認方法を設定するファイルとして、端末には「Terminal Capabilities」が格納されている（Book 4, Annex A2）。

ただし、例えば、正規のカードが本人確認方法としてオフライン PIN 認証（平文）のみを候補として挙げていた場合、本人確認を実施することができなくなるため、店舗にとっては取引機会の喪失につながりうる。また、選択可能な本人確認方法の種類が減少するため、利便性が低下することになる。

4.3.3 攻撃を早期に検知する対策

端末においてオフライン PIN 認証（平文）の利用を禁止しない場合、攻撃者が中間侵入装置により PIN を盗取する可能性があるため、本攻撃を早期に検知しユーザに PIN の更新を促すという対策が考えられる[30]。本攻撃の検知については、単にデータの真正性を検証するだけでは不十分である。任意 PIN 利用型攻撃であれば、異常を検知し当該取引を不成立にすればよい。しかし、Barisani *et al.*[2011]による盗取 PIN 利用型攻撃では、取引が不成立となっても PIN の盗取というフェーズ 1 における目的は達成されてしまうため、異常を検知した際にその異常が本攻撃に基づくものか否かを見極めることが重要となる。

本攻撃の特徴は、本人確認方法としてオフライン PIN 認証（平文）が選択されるように CVM リストを改ざんする点であり、この特徴を本攻撃の見極めに利用できる。カード認証では、カード固有データ全体に対するデジタル署名が付与されているため、端末は検証結果が不合格であれば改ざんされたデータが含まれていることはわかるものの、改ざんされたデータを特定することはできない。他方、発行者は、自分が発行したカードにどのようなデータを格納したかをすべて把握しているため、端末がカードから受信したカード固有データをホストシステムにそのまま送信することで、どのデータがどのように改ざんされているかを確認することができる[31]。そこで、カード認証の結果が不合格となった場合には、カード認証に用いたデータ[32]を発行者に送信するという対策が考えられる。

この対策をオンライン取引照会とオフライン取引照会の観点からみた場合、オンライン取引照会の場合には本攻撃を即時に検知できると考えられる。他方、オフライン取引照会の場合、改ざんされたデータが発行者に即時には送信されないため、本攻撃の検知に一定の時間を要し、その間にカードが盗取され、不

[30] 実際に PIN を更新する際には、何らかの方法でユーザの本人確認を行う必要がある。なお、EMV 仕様では、リモートで安全に PIN を更新するために、Issuer Script Processing と呼ばれる通信手順と PIN Change/Unblock コマンドを用意している。

[31] 例えば、オフライン PIN 認証（平文）をサポートしていないカードとの取引において、端末に読み出された CVM リストがオフライン PIN 認証（平文）を含んでいる場合には、盗取 PIN 利用型攻撃が行われた可能性があると推測できる。

[32] カード認証に用いたすべてのデータを送信することでカード発行者がカード認証を追試可能となる。通信量の制約によりこれらのデータをすべて送信することが困難な場合には、少なくとも CVM リストを送信することが望ましい。

正な取引に利用されるおそれがある。

4.3.4 Barisani *et al*.[2011]による盗取 PIN 利用型攻撃への対策のまとめ

以上を整理すると、カード認証の結果を本人確認の処理に反映させる、あるいは、オフライン PIN 認証（平文）を禁止にすることで、PIN の盗取を防止できることがわかる。また、オフライン PIN 認証（平文）の利用を禁止しない場合、オンライン取引照会では本攻撃をリアルタイムに検知できるものの、オフライン取引照会では検知までにタイムラグが発生することがわかる。

4.4 Adida *et al*.[2006]による盗取 PIN 利用型攻撃への対策

Adida *et al*.[2006]による盗取 PIN 利用型攻撃に対しては、本攻撃を指摘したケンブリッジ大学の研究グループがいくつかの対策（下記の対策①②④）を提案している。本節では、それらの対策および他の対策（下記の対策③）について説明する。

本攻撃は、店舗 1 に居るユーザのカードと店舗 2 の正規の端末の通信を攻撃者が中間侵入装置を用いて中継しており、カードと端末間では正常な取引として処理が行われてしまう可能性がある。そのため、意図した処理が行われているか否かをユーザあるいは店舗等のスタッフが確認することが攻撃を防止するための対策となりうる（下記の対策①～③）。このほか、データの中継により発生する遅延に着目した対策（下記の対策④）も考えられる。各対策は次のとおりである。

① カード券面とレシートに記載されたアカウント番号を突合する対策

通常、カード券面にはアカウント番号が印字されているほか、取引時に発行されるレシートには使用されたカードのアカウント番号が一部マスクされた状態で印字される。本攻撃では、ターゲットとなる正規のカードのアカウント番号を攻撃前に攻撃者が入手していない可能性があり、その場合は、カード券面およびレシートのアカウント番号が整合的でないと考えられる。そこで、店舗等のスタッフが端末のそばに居る場合には、取引終了後にカード券面のアカウント番号とレシートのアカウント番号のマスクされていない部分を突合し、整合的でなければ当該取引を不正な取引とみなすという対策が考えられる。本対策は、Drimer and Murdoch[2007]において提案されている。

② 取引データをユーザが直接確認する対策

攻撃時に正規のカードが処理する取引データは、ユーザが意図している店舗 1 における取引のものではない。Adida *et al*.[2006]による盗取 PIN 利用型攻撃のよ

うな攻撃を想定すれば端末が信頼できるとは限らないため、カードが処理する取引データ（主に、金額）を信頼できる装置のディスプレイに表示したうえで、ユーザが直接確認するという対策（「Man-in-the-Middle Defense」と呼ばれる）が考えられる。具体的には、ユーザが、正規のカードと端末の間に取引データの表示と取引処理の管理を行うための装置を挿入し、意図した取引データであることを確認した場合にのみ、同装置に対して取引処理の継続の指示を行うという方法である。本対策は、Anderson and Bond[2006]、Drimer and Murdoch[2007]、Choudary[2010]において提案・検討されている。

③ 端末の認証を行う対策

本攻撃では、ユーザが偽端末を利用しているため、ユーザが自分のカードを用いて端末を認証するという対策が考えられる。この対策には、認証結果を表示するためのインタフェース[33]を搭載したカードが必要となる。本対策を適用した取引の手順は、例えば、次のとおりである。ユーザが端末にカードを挿入した後、カードは端末の認証を行い、その結果を表示する。ユーザは、端末認証の結果を確認したうえで、当該取引の処理を継続するか否かを判断する。なお、カードが端末を認証する方法としては、例えば、ユーザの PC（カードに相当）がインターネット上のサーバ（端末に相当）と暗号通信を開始する前に行う「サーバ認証[34]」を参考にすることが考えられる。

④ 遅延を検知する対策

本攻撃には、店舗 1 に設置された偽端末と店舗 2 で利用される偽カード間の通信が必要となる分、正常な取引よりも時間を要するという特徴がある。そこで、店舗 2 の端末は、カードからのレスポンスが一定時間以上遅れた場合には、当該取引を中止するという対策が考えられる。ただし、カードからのレスポンスの遅延が当該カードの計算性能に依存するため、利用されるカードの計算性能がまちまちである場合には、どの程度の遅延までを許容するかという課題が生じる。本対策は、Drimer and Murdoch[2007]において提案されている。

---

[33] 例えば、カードに LED 等を搭載しておき、端末認証の結果が合格の場合にのみ点灯するよう設定しておくことが考えられる。

[34] サーバ認証は、ユーザが PC を用いてアクセスしたサーバが、ユーザが意図した正当なサーバであることを確認するために行われる。具体的な手順は次のとおりである。認証局がサーバのドメイン名とサーバの公開鍵の対応を保証するデジタル署名（「公開鍵証明書」と呼ばれる）を生成し、予めサーバにこの証明書を付与しておく。サーバは、アクセスしてきた PC にこの証明書を送信し、PC はこの証明書を検証することで、当該サーバが正当なサーバか否かを判断する。

以上を整理すると、端末のそばにスタッフが居る運用形態であれば対策①が可能になるほか、追加の装置やディスプレイ付きカードの利用を仮定すれば、上記の対策②や③が可能になる。スタッフの存在やディスプレイ等を搭載したカードの利用を仮定しない場合の対策としては対策④が考えられるが、レスポンスの遅延をどこまで許容するかという課題が残る。

5. 考察

本節では、4 節の検討結果を踏まえて、金融機関が対策を講じる際の留意点として、①攻撃と対策に関する理解の重要性、②ATM を用いたシステムへの影響、③カードの機能と各攻撃への耐性、④対策に対応していない端末の存在、⑤改ざんされたデータに基づく不適切なリスク管理、⑥運用による対策の重要性について考察する。

① 攻撃と対策に関する理解の重要性

オンライン取引照会では、オフライン取引照会よりも厳格な検証が実施可能である。その理由としては、(a)ホストシステムが各カードのカード固有データを管理していること、(b)カードが生成したデータについて、ホストシステムは端末より多くのデータを検証できること、(c)ホストシステムが与信枠を管理していることなどが挙げられる。ただし、取引の処理をオンライン取引照会にしたとしても、当該攻撃を防ぐことができるとは限らない。各攻撃やそれらの前提条件を理解したうえで、適切な対策を講じることが重要である（図表 15 参照）。

前提条件		説明	任意 PIN 利用型攻撃	盗取 PIN 利用型攻撃	
分類	番号			Barisani *et al*.[2011]	Adida *et al*.[2006]
カード、端末、ホストシステム等の安全性に関する条件	1	カード、端末、ホストシステムは、耐タンパー性を有する。	○	○	○
	2	端末とホストシステム間の通信は安全である。	○	○	○
	3	攻撃者は、カードと端末間の通信を盗聴・改ざん・遮断可能である。	○	○	○
	4	攻撃者は、正規のユーザのカードを盗取できる。	○	○	×
	8	中間侵入装置は、正規の端末に取り付けられている。	×	○	×
	11	偽端末が利用される。	×	×	○
ログに関する条件	6	カードは、CVMR を用いて実際に実行された本人確認方法の確認を行わない。	○	×	×
	7	ホストシステムは、IAD と CVMR を用いて、実際に実行された本人確認方法の確認を行わない。	○	×	×
本人確認方法に関する条件	5	本人確認方法として、オフライン PIN 認証が選択される。	○	×	×
	9	PIN（オフライン）盗取を行う際（フェーズ 1）には、オフライン PIN 認証（平文）が実行可能な端末を想定する。	×	○	×
	10	PIN（オフライン）とカードを盗取後に不正な取引を試行する際（フェーズ 2）には、本人確認方法としてオフライン PIN 認証が選択される。	×	○*	×
	12	本人確認方法として、オフライン PIN 認証またはオンライン PIN 認証が選択される。	×	×	○

（備考）「○」は当該条件を想定することを、「×」は想定しないことをそれぞれ表す。また、「○*」は当該ユーザの PIN（オフライン）と PIN（オンライン）が異なる場合に想定することを表す。

図表 **15**. 各中間者攻撃の前提条件

② ATM を用いたシステムへの影響

端末として ATM を想定した場合に、本稿が想定する各中間者攻撃の影響について考察する。ATM では、本人確認方法としてオンライン PIN 認証のみが想定されている。そのため、条件 5, 9, 10 が成立せず、任意 PIN 利用型攻撃と Barisani *et al*.[2011]による盗取 PIN 利用型攻撃への耐性を有していると考えられる。一方、Adida *et al*.[2006]による盗取 PIN 利用型攻撃については、ユーザが偽端末に自分のキャッシュカードを挿入してしまう場合には（条件 11 に対応）、本攻撃が成立する可能性は否定できないと考えられる。

③ カードの機能と各攻撃への耐性

カードの機能が向上すれば攻撃への耐性が向上するケースがある一方で、カードの機能が攻撃への耐性に影響を与えないケースもある。発行者が効率的に対策の導入に投資を行うためには、カードの機能と各攻撃への耐性を把握しておくことが重要となる。そこで、カードの機能として、実行可能なカード認証方法とカードが搭載するユーザ・インタフェースに着目して、対策への耐性を整理すると図表 16 のとおりである。

任意 PIN 利用型攻撃に対しては、動的データ認証や CDA が可能なカードを採用することが望ましい。Barisani *et al*.[2011]による盗取 PIN 利用型攻撃に対しては、カードの機能の違いが攻撃への耐性に影響を与えないことがわかる。また、Adida *et al*.[2011]による盗取 PIN 利用型攻撃に対しては、ディスプレイ等を備えたカードか否かが耐性の違いに表れる。

<table>
<tr><th colspan="2" rowspan="2">カードの機能</th><th rowspan="2">任意 PIN
利用型攻撃</th><th colspan="2">盗取 PIN 利用型攻撃</th></tr>
<tr><th>Barisani et al.[2011]</th><th>Adida et al.[2006]</th></tr>
<tr><td rowspan="3">カード
認証</td><td>静的データ認証</td><td>・オンライン取引照会の場合：防止可能
・オフライン取引照会の場合：取引後に検知可能</td><td rowspan="3">—</td><td rowspan="3">—</td></tr>
<tr><td>動的データ認証</td><td rowspan="2">防止可能</td></tr>
<tr><td>CDA</td></tr>
<tr><td>ユーザ・
インタ
フェース</td><td>ディスプレイ等</td><td>—</td><td>—</td><td>防止可能</td></tr>
</table>

（備考）「—」は、当該機能が対策を実施するうえで影響を与えないことを表す。

図表 **16**. カードの機能と攻撃への耐性

④　対策に対応していない端末の存在

4 節で検討した対策の中には、オフライン取引照会の場合でも攻撃を防止可能なものがある。オフライン取引照会を想定できるのであれば、店舗は、取引に要する処理時間の短縮や通信コストの削減等の恩恵を享受できる。ただし、オフライン取引照会を前提とする対策を実施するためには、カードと端末を対応させる必要がある点には留意が必要である。カードについては、発行者が管理しており、カードの更新に合わせて対策を施した新しいカードに切り替えるなどの方法により移行を進めることができると考えられる。他方、端末への対策の導入については発行者の管理下にないため、発行者は対策が施されていない端末において自社のカードが利用される状況を想定する必要がある。

⑤　改ざんされたデータに基づく不適切なリスク管理

EMV 仕様では、AC 生成だけでなく、カード認証や本人確認においてもリスク管理が行われる。本人確認においては、カードが提示した CVM リスト、端末がサポートする本人確認方法、取引金額等に基づき、本人確認方法を選択するというリスク管理が行われる[35]。Barisani *et al*.[2011]による盗取 PIN 利用型攻撃では、改ざんされた CVM リストを基に本人確認方法が選択されてしまうことを利用しているといえるが、現行の EMV 仕様では、リスク管理（例えば、本人確認方法の選択）に用いるデータ（例えば、CVM リスト）が改ざんされている場合の処理について明確にされていないケースがある[36]。IC カード利用システムを構築・運用する際には、こうした点にも留意することが望ましい。

⑥　運用による対策の重要性

技術的な対策を直ぐに講じることができない場合には、運用による対策が一層重要になる。例えば、Barisani *et al*.[2011]による盗取 PIN 利用型攻撃においては、オフライン PIN 認証（平文）をサポートした端末を想定すると、攻撃者が PIN を盗取することを防げない。この場合、攻撃者に中間侵入装置や盗取カードを利用させないようにするために、端末の管理の厳格化を促すことやカードの盗難・紛失時の早期届け出を行うように啓蒙することが考えられる。このほか、発行者がユーザに対して、自分のカードの利用履歴の確認や、PIN 更新の環境を整備したうえで定期的な PIN の更新を行うよう啓蒙することも考えられる。

---

[35] カード認証においては、カードと端末間で、両者がサポートする方法の中で最も安全性の高い方法（CDA が最も安全性が高い）を選択するというリスク管理が行われる。AC 生成においては、カード認証や本人確認の結果、その他の取引データに基づき当該取引の最終的な扱いを決定するというリスク管理が行われる。

[36] ただし、CVM リストのフォーマットの異常については、EMV 仕様は、端末が当該取引を中止するように規定している（Book 3, 10.5 節）。

6. おわりに

本稿では、これまで必ずしも現実的な脅威として認識されてこなかった IC カードと端末間への 3 つの中間者攻撃を紹介し、各攻撃への対策の検討や金融機関が対策を講じる際の留意点について考察を行った。

これら 3 つの攻撃は、実際の運用環境と同等の実験環境において成功することが報告されており、各攻撃の前提条件が成立し得る IC カード利用システムが攻撃対象とされた場合には、不正な取引が成立する可能性がある。また、Murdoch *et al.*[2010]では、上記以外にも EMV 仕様にはセキュリティの観点から脆弱な処理やデータが複数存在し、これらを中間者攻撃に利用できる可能性があると指摘している。

そのため、金融機関には、少なくとも本稿で紹介した 3 つの攻撃に対して、新規に構築するシステムあるいは運用中のシステムが耐性を有するか否かを評価することが求められる。

今後も金融機関が利用する情報システムに対する中間者攻撃やそれ以外の攻撃が指摘されると予測されるが、金融機関は、そうした情報を国内外の学界や関連する業界等から広く収集し、自社のシステムへの影響を分析するという取組みを継続することが重要である。また、何らかの対策が必要であると判断した場合には、技術的な対策だけでなく運用による対策も含めて各対策の効果や実施するための条件を明確にしたうえで、ビジネス要件を考慮しながら安全性と利便性のバランスを図っていくことが求められる。

参考文献

宇根正志・田村裕子・松本 勉、「偽造防止技術のなかの人工物メトリクス：セキュリティ研究開発の動向と課題」、『金融研究第』28 巻第 2 号、2009 年、143～181 頁

金融情報システムセンター、「平成 21 年度 金融機関等のコンピュータシステムに関する安全対策実施状況調査報告書」、『金融情報システム』増刊 70 号、No.310、2010 年

日本クレジットカード協会、「IC クレジットカードに関する調査 結果報告書」、2010 年

Adida, Ben, Mike Bond, Jolyon Clulow, Amerson Lin, Steven Murdoch, and Ron Rivest, "Phish and Chips (Traditional and New Recipes for Attacking EMV)," Cambridge Security Protocols Workshop, 2006.

Anderson, Ross and Mike Bond, "The Man-in-the-Middle Defence," Cambridge Security Protocols Workshop, 2006.

Barisani, Andrea, Daniele Bianco, Adam Laurie, and Zac Franken, "Chip & PIN is definitely broken," CanSecWest, 2011.

BBC, "Flaws in chip and pin bank card security identified," 11 February 2010. http://news.bbc.co.uk/2/hi/science/nature/8511710.stm

Choudary, Omar S., "The Smart Card Detective: a hand-held EMV interceptor," Master Thesis, University of Cambridge, 2010.

Drimer, Saar and Steven J. Murdoch, "Keep your enemies close: distance bounding against smartcard relay attacks," USENIX Security Symposium, 2007.

EMVCo, "A Guide to EMV," 2011a.

———, "Book 1 Application Independent ICC to Terminal Interface Requirements," *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.2, EMVCo, 2008a.

———, "Book 2 Security and Key Management," *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.2, EMVCo, 2008b.

———, "Book 3 Application Specification," *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.2, EMVCo, 2008c.

———, "Book 4 Cardholder, Attendant, and Acquirer Interface Requirements," *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.2, EMVCo, 2008d.

———, "Common Payment Application Specification," *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 1.0, 2005.

———, "Response from EMVCo to the Cambridge University Report on Chip and PIN

vulnerabilities," 2010.

———, "Response from EMVCo to the Inverse Path Paper 'Chip and PIN is Definitely Broken – March 2011'," 2011b.

European Payments Council, "SEPA for cards: tracking EMV roll-out," *EPC Newsletter*, Issue 10, 2011.

Murdoch, Steven J., "Defending against wedge attacks in Chip and PIN," Light Blue Touchpaper, August 25th 2009. http://www.lightbluetouchpaper.org/2009/08/25/defending-against-wedge-attacks/

———, Saar Drimer, Ross Anderson, and Mike Bond, "Chip and PIN is Broken," 2010 IEEE Symposium on Security and Privacy, 2010.

Rosa, Tomas, "On the 'Chip & PIN Brocken' Attack Experience Gained in Raiffeisenbank," 2010.

Visa International, "Visa Integrated Circuit Card Specification (VIS) – Card Specification version 1.4.0," Visa Public, 2001a.

———, "Visa Integrated Circuit Card Specification (VIS) – Terminal Specification version 1.4.0," Visa Public, 2001b.

以　上