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 Pre-play attackとその対策

井澤秀益（いざわひでみつ）・廣川勝久（ひろかわかつひさ）

Discussion Paper No. 2015-J-10

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 2015-J-10

2015 年 7 月

IC カード利用システムにおいて新たに顕現化した Pre-play attack とその対策

井澤秀益（いざわひでみつ）*・廣川勝久（ひろかわかつひさ）**

要　旨

近年、キャッシュカードやクレジットカードの偽造・不正使用に対する耐性を高めるため IC カード化が進められている。こうした金融分野における IC カードを用いたカード取引のための IC カードと端末に関する仕様を定めたデファクト標準としては「EMV 仕様」があり、日本を含め国際的に利用されている。EMV 仕様においては、そのセキュリティ機能の一つとして、取引データが改ざんされていないことや、当該取引のために IC カードが利用されていることを保証する「取引認証」の仕組みがある。

ただ近年、英国ケンブリッジ大学の研究グループが、この「取引認証」に対して、ある条件のもとで攻撃が成立し、実質的に正規 IC カードが行う取引と同等の取引が攻撃者作成のカードで可能となることを発表した。本攻撃を発表したグループは当該攻撃手法を「Pre-play attack（プリプレイ攻撃）」と名付けており、欧州において実際に起こった ATM からの不正現金引き出し事例について、本攻撃手法が使われた可能性を指摘している。

そこで本稿では、Pre-play attack の手法や攻撃が成立する条件等について解説するとともに、Pre-play attack への対策手法を検討する。

キーワード：IC カード、EMV 仕様、取引認証、Pre-play attack

JEL classification: L86、L96、Z00

*　日本銀行金融研究所企画役補佐（E-mail: hidemitsu.izawa@boj.or.jp）

**　日本銀行金融研究所テクニカル・アドバイザー
（E-mail: katsuhisa.hirokawa@boj.or.jp）

本稿の作成に当たっては、国立研究開発法人産業技術総合研究所情報・人間工学領域研究戦略部の古原和邦研究連携主幹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

近年、クレジットカードやキャッシュカードの磁気記録情報を読み出して偽造カードを作成し、不正使用を行う「スキミング」と呼ばれる犯罪行為が社会問題化した。このため、クレジットカード発行会社や金融機関では、クレジットカードやキャッシュカードの偽造・不正使用に対する耐性を高めるため、IC カード化が進められている。既に世界的には 34 億枚以上の IC カードが発行されているほか（EMVCo[2015]）、国内においても 1 億枚超の IC キャッシュカードが発行されているとみられる（金融庁[2014]）。

こうした金融分野における IC カードを用いたカード取引のための、IC カードと端末に関する仕様を定めたデファクト標準としては「EMV 仕様[1]」があり、日本を含め国際的に利用されている。EMV 仕様は、IC カード、端末、ホストシステムおよびそれらをつなぐ通信路等から構成される「IC カード利用システム」の技術的要件やプロトコル等を定めているが、その中で、偽造や不正使用を防止するため、暗号技術を応用した高度なセキュリティ機能についても規定されている。そのセキュリティ機能の一つとして、取引データが改ざんされていないことや、当該取引のために IC カードが利用されていることを保証する仕組み（以降、「取引認証」と呼ぶ）がある。これは、IC カードが取引毎に生成するメッセージ認証子[2]により取引内容が改ざんされても検知できる仕組みである。

ただ近年、英国ケンブリッジ大学の研究グループが、この「取引認証」に対して、ある条件のもとで攻撃が成立し、実質的に正規 IC カードが行う取引と同等の取引が攻撃者作成のカードで可能となることを発表した（Bond *et al.*[2014]）。本攻撃を発表したグループは当該攻撃手法を「Pre-play attack（プリプレイ攻撃）」と名付けており、欧州において実際に起こった ATM からの不正現金引き出し事例[3]について、本攻撃手法が使われた可能性を指摘している。

「Pre-play attack」は海外においては数々のメディアで既に取り上げられおり（BBC[2012]）、海外の IC カード関係者は本事象を認識する機会が多いものの、国内においてはほとんど報道されていないように見受けられる。それに加えて本件は、

---

[1] EuroPay International、Matercard International、および Visa International の間で合意した IC カードの統一規格で、三社の頭文字を取って名付けられた。

[2] Message Authentication Code で、データの真正性の確認と認証を行う仕組み。同様の仕組みにデジタル署名があるが、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。

[3] マルタ共和国の某金融機関の顧客が、自分の IC カードに対応する口座から、不正な引き出しが行われていたため、金融機関に対して取引の取り消しを求めたものの、金融機関はそれを拒否。金融機関は、スペインのマヨルカ島で 2011 年 6 月 29 に、顧客の IC カードを使って行われた取引であると判断した。

磁気カードに比べてセキュリティレベルが高い IC カードであっても、それを利用しているだけで安全であるとは言い切れないことを示す事例として認識しておく必要がある。

そこで、本稿では、IC カード関係者に Pre-play attack を広く情報提供するとともに、何が問題であったのか検討を加え、対策手法や実装時の留意点について考察することを企図し、次の順序で説明する。第 2 章で前提知識となる EMV 仕様を取り上げ、第 3 章で Pre-play attack の具体的な攻撃手法を解説する。次に、第 4 章で攻撃への対策手法や実装時の留意点について考察し、第 5 章で本稿をまとめる。なお、本稿に出てくる EMV 仕様関係の用語について、参考として付録に用語集を添付した。

2. EMV 仕様における「取引認証」の仕組みについて

本章では、IC カード利用システムにおける EMV 仕様の概要や、その中における「取引認証」の仕組みについて、EMVCo[2011a,b,c,d]および鈴木・廣川・古原[2012]を参考に解説する。

(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。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）。

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（口座）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が発行時に記録される。

ユーザ：発行者からカードの発行を受けた利用者。カード所有者とも呼ばれる。

端　末：カードリーダ／ライタを介して、カードと通信する他、ホストシステム

と通信する装置。端末は、PIN[4]を入力する装置（「PIN パッド」と呼ばれる）を備える。こうした端末としては、ATM や CAT[5]が挙げられる。

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。

なお、EMV 仕様においては、最低限の要件やオプションを規定しているが、実際に 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仕様を決定する必要がある。例えば、全国銀行協会においては「全銀協 IC キャッシュカード標準仕様」を策定している。

(2) EMV 仕様におけるセキュリティ機能の概要

EMV 仕様におけるセキュリティ機能として主なものは、実際の取引の流れ順に、①「カード認証」、②「本人認証」、③「取引認証」の 3 種類が挙げられる。

①の「カード認証」は、端末が、カードの真正性を確認することを目的としている。その方法として、静的データ認証（SDA: Static Data Authentication）、動的データ認証（DDA: Dynamic Data Authentication）、動的データ認証と AC 生成（後述）を組み合わせた方式（CDA: Combined DDA/Application Cryptogram Generation）、の 3 種類が EMV 仕様では用意されている。例えば、静的データ認証（SDA）では、カードから読み出され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ことにより、「カード認証」を実施する。

②の「本人認証」は、端末やホストシステムが、ユーザの真正性を確認することを目的としている。その方法として現在は、オフライン PIN 認証、オンライン PIN 認証、手書き署名、の 3 種類の方法が用意されている。例えば、オフライン PIN 認証では、ユーザが入力した PIN を端末がカードに送信[6]し、カード内で登録されている PIN との照合[7]を行うことにより「本人認証」を実施する。また、オンライン PIN 認証では、ユーザが入力した PIN を端末（PIN パッド）が暗号化したうえでホストシステムに送信し、ホストシステム内に登録されている PIN と照合する。

③の「取引認証」は、ホストシステムが、カードを利用した取引の内容の真正性

---

[4] 暗証番号のこと。Personal Identification Number の略。

[5] 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。

[6] 端末が PIN を送信する際、カードの公開鍵で暗号化する場合と暗号化しない場合がある。

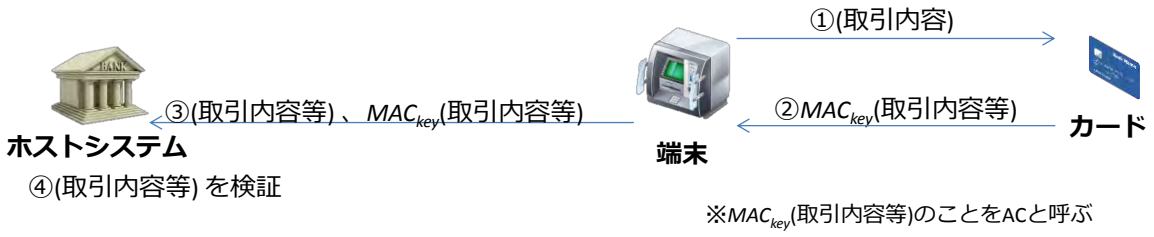
[7] 繰り返し PIN の照合を行うことで正しい PIN を探索する攻撃を防ぐために、カードには「PIN Try Counter」と呼ばれるカウンタが用意されている。カウンタの値は PIN の照合が不合格になるたびに減少し、ゼロになるとそれ以降の PIN の照合を実行することが出来なくなる。

および当該取引が正規のカードからのものであることを確認することを目的としている。その仕組みについては、次節にて詳しく説明する。

(3) EMV 仕様における「取引認証」の概要

EMV 仕様における「取引認証」のポイントは、「AC の生成・検証」と呼ばれる方法により取引内容等の改ざん検知が出来る点である。AC（Application Cryptogram）とは、取引内容等に対するメッセージ認証子である。EMV 仕様では、Triple DES や AES といった共通鍵暗号を用いて AC を生成する方法が規定されている。本稿では、AC を特に「取引内容等」に対するメッセージ認証子であることを示す場合に「MAC_{key}（取引内容等）」と表記する。なお、*key* は、ホストシステムとカードとで共有している鍵（「セッション鍵」[8]）を意味する。

「AC の生成・検証」のポイントは図表 2 に示す通りとなる（詳細は(4)参照）。①端末が取引内容をカードに送付し、②カードが取引内容をはじめとする項目（取引内容等）に対してメッセージ認証子を付与（AC 生成）し、AC（MAC_{key}（取引内容等））を端末に送付する。③端末が、AC とともに取引内容等をホストシステムに送付し、④ホストシステムが取引内容等について AC を使って検証（改ざん検知）する。検証にあたってホストシステムは、受信した取引内容等と、予め共有しているセッション鍵を用いて独自に AC を生成し、受信した AC と照合することにより、取引内容等の改ざんを検知することが出来る。なお、端末はセッション鍵を所有しないため、AC の検証を行うことは出来ない。攻撃者が取引内容等の改ざんを行うためには、「改ざんした取引内容等」に対する AC を生成しなければならないが、そのためにはセッション鍵が必要になるため、（セッション鍵が漏れなければ）攻撃者は取引内容等の改ざんが行えない仕組みとなっている。

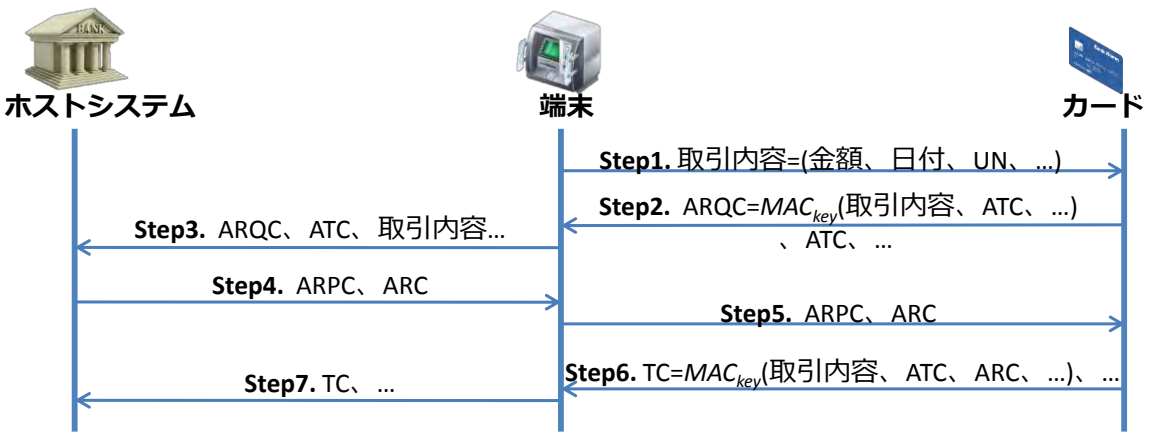


図表 2. EMV 仕様における「取引認証」のポイント

[8] EMV 仕様において暗号化を施す際に使用する鍵については、ホストシステムとカードとの間で、カード発行時にカード固有鍵（マスタ鍵）を共有しておき、実際の取引の際には、ホストシステムとカードがこの固有鍵（マスタ鍵）から取引毎に異なる値の鍵（セッション鍵）を生成・共有できるようにしている。

(4) EMV 仕様における「取引認証」の具体例

EMV 仕様における「取引認証」のフローの具体例[9]は（図表 3）の様になる。なお、以降ではホストシステムが常に端末と通信可能な「オンライン取引」を想定して説明する。



図表 3. EMV 仕様における取引認証のフローの具体例

Step1. 端末は、カードに対して、取引金額、日付等の情報と端末が生成する「予測不可能な数」UN（Unpredictable Number）等を送信する（両者を合わせて、以降「取引内容」と呼ぶ）。UN には乱数等が使われ、同一端末で続けて同一金額の取引を行った場合等であったとしても、Step2 で異なる AC を生成させる目的で用いられる。

Step2. カードは、当該取引を実施することが適当であると判断した場合に、端末から受け取った取引内容と、カード内に保存されている取引カウンタ ATC（Application Transaction Counter）をもとに AC を生成する。この AC を取引承認要求 ARQC（Authorisation Request Cryptogram）として、ATC とともに端末に返信する。なお ATC は、取引毎にカード内で自動的にカウントアップされる。

Step3. 端末は、カードから受け取った ARQC と ATC に取引内容を付加したうえでホストシステムに送信する。

Step4. ホストシステムは、受信した ARQC を検証[10]した上で、当該取引の承認の

[9] EMV 仕様の中から本稿に関係のある項目を中心に説明している。端末とホストシステムにおける通信内容は一例であり、個別の金融機関における実装により変わりうる。

[10] 検証の方法は EMV 仕様の範囲外であるが、例えば検証の方法として、ホストシステムは、「受信した取引内容に対してセッション鍵で暗号化を施すことにより ARQC を自ら生成」し、それと「受信した ARQC」との照合を行う、といった方法が考えられる。

適否を判断[11]し、その結果を表すコードを ARC（Authorisation Response Code）として端末に返信する。なおこの時、①ARC が（カードが送信した正しい）ARQC 等に対応するものであり、②正当なホストシステムから改ざんされることなく返信されていること、を確認するために、暗号化が施された ARPC（Application Response Cryptogram）が生成され一緒に送られる。

Step5. 端末は、ホストシステムから受信した ARPC と ARC をカードに送信する。

Step6. カードは、端末から受信した ARPC を検証[12]した上で、当該取引を実施することが適当であると判断した場合に、端末に対して取引成立確認を示す TC（Transaction Certificate）を送信する。TC は、AC の一種であり、取引内容および ATC 等にホストシステムからの承認結果である ARC を加えたものに対するメッセージ認証子である。

Step7. 端末が TC を受信した時点で当該取引は成立する。その後端末はホストシステムに TC を送信する。

上記 EMV 仕様における「取引認証」のフローをセキュリティの観点から眺めると、取引が正当であることを示すための AC 生成以外に特徴的な点としては、チャレンジ･レスポンス認証と類似の処理が行われていることが挙げられる（図表 4）。

EMV 仕様では、①ホストシステムと常に通信可能ではないオフライン取引（端末とカードのみの取引）にも対応できるよう考えられていること、②このため、クライアントとサーバといった２者間ではなく、ホストシステム･端末･カードといった３者間の通信であること、が特徴として挙げられる。

これら①②に対応するため、図表 4 に示すように、EMV 仕様における「取引認証」のフローは、一般的なチャレンジ・レスポンス認証とは一部異なる方式となっている。一般的なチャレンジ・レスポンス認証においては、サーバがクライアントに、乱数をチャレンジとして送信するが、EMV 仕様においては、端末がカードに、UN に加えて取引金額等をチャレンジとして送信する（以降、チャレンジとしての UN を強調するときには「チャレンジ（UN）」と記載する）。また、一般的なチャレンジ・レスポンス認証においては、クライアントがサーバに対して、チャレンジに対するメッセージ認証子をレスポンスとして送信するが、EMV 仕様においては、カードが端末経由でホストシステムに対して、チャレンジに ATC 等を加えたもの

[11] ホストシステムにおける判断の方法は EMV 仕様の対象外であり、個別の金融機関におけるビジネス管理上の判断に応じて行われる実装に依存する。

[12] 例えば検証の方法として、カードは、「Step2 で送信した ARQC と受信した ARC から、自ら ARPC を生成」し、それと「受信した ARPC」との照合を行う、といった方法が考えられる。

に対するメッセージ認証子（ARQC）をレスポンスとして送信する（以降、レスポンスとしての ARQC を強調するときには「レスポンス（ARQC）と記載する」）。

図表 4. 一般的なチャレンジ・レスポンス認証と EMV 仕様

なお、EMV 仕様では、端末あるいはネットワークを流れる AC を盗聴・保存し、取引が終了したのち、続けざまに当該 AC を使って同内容の取引を行おうとする攻撃（Replay attack：リプレイ攻撃）[13]への対策も意識されている。すなわち、AC 生成を行う際に、（カード内で取引毎にカウントアップされて違う値になる）ATC をメッセージ認証の対象にしていることは、続けて同内容の取引であっても AC が異なる値になることであり、保存しておいた AC を再利用して不正な取引を行うことが出来ないようになっている。

3. Pre-play attack による攻撃手法

本章では、EMV 仕様の IC カードシステムの「取引認証」に対する新たなアイデアに基づく攻撃手法について、Bond *et al.*[2014]を参考に説明する。Bond *et al.*[2014]では当該攻撃手法を Pre-play attack と呼んでいる。

Pre-play attack は、攻撃者が端末・カード間の通信であるチャレンジとレスポンスを不正に収集しておくことにより、ある前提を満たす状況において、正規カードを所有していないにもかかわらず、ターゲット（被害者）のカードを模倣した振舞いを行える不正なカードを作成することが出来る攻撃手法である。類似する攻撃手法に Replay attack がある。Replay attack は攻撃者が「実際に認証に使用されたデータ」を保存しておき、後ほど攻撃者が当該データをターゲットに再送する攻撃手法であるのに対して、Pre-play attack では攻撃者が「実際にはまだ使用されていないデータ」を情報収集しそれを利用する、という点が異なる。

[13] 攻撃者が、ターゲットの認証に使われた情報を収集しておき、当該情報を認証サーバに送ることで認証を突破しようとする攻撃。EMV 仕様においては、攻撃者が、認証に使用された ARQC を保存しておき、それをホストシステムに送るという攻撃手法が考えられる。

(1) Pre-play attack の種類と攻撃前提

（攻撃の種類）

情報収集の方法およびその使い方の違いによって、Bond *et al*.[2014]では以下の 2 種類の攻撃手法が提案されている。

攻撃①：Random number attack　（Defective random number generators や poor UN generation を利用した攻撃）

攻撃②：Protocol flaw attack

（攻撃の目的）

両攻撃手法ともに、その目的は、「攻撃者が、カード内の鍵を盗むこと無く、ターゲットのカードの代わりに取引が行えるカードを作成すること」である。作成したカードをもとに、攻撃者は「ターゲットの口座から預金を引き出す」（キャッシュカードの場合）といった不正行為を行うことが可能となる。

（攻撃の前提事項）

両攻撃手法で共通する前提事項は以下の通りである。

1. 攻撃者は、端末との間で、攻撃者が予め意図した通りに情報のやりとりを行ったり情報を保存したりできるカードを用意する必要がある（以下、このカードのことを「細工カード」と呼ぶ)。ただし、IC カードの耐タンパー性を破った細工を行う必要はなく、Bond *et al*.[2014]でも、実際に作成に成功している。
2. 攻撃者は、端末に細工する等により、カードに対して任意の情報を送信したり、カードから受信した情報やユーザが入力した PIN を保存することが出来る端末を用意する必要がある（以下、この端末のことを「細工端末」と呼ぶ)。Bond *et al*.[2014]でも、実際に作成に成功している。
3. 攻撃者は、ターゲットのカードを入手する必要まではないが、細工端末にターゲットのカードを挿入させる必要がある。
4. 攻撃者は、何らかの方法で、「カード認証」を突破する必要がある。「カード認証」として、端末が静的データ認証（SDA）を利用している場合には、攻撃者は、細工端末を使ってターゲットのカード固有データおよび対応するデジタル署名を保存しそれを細工カードで使用することにより、認証を突破することが出来る可能性がある。
5. 攻撃者は、PIN を入手すること等によって「本人認証」を突破する必要がある。細工端末にターゲットのカードを挿入させたときには、通常の取引を装う等により正しい PIN をターゲットに入力させ、これを保存しておくことで入手可能である。

前提 4,5 により、2.(2)で述べたセキュリティ対策である「カード認証」「本人認

証」「取引認証」のうち、「カード認証」および「本人認証」を攻撃者は突破出来る場合を想定する。残る「取引認証」に対する攻撃を次節で述べる。

(2) Random number attack（攻撃①）による攻撃の仕組み

本節では Random number attack（攻撃①）固有の前提事項および、攻撃の仕組みについて述べる。

（攻撃①固有の前提事項）

- ターゲットとなる端末（以下、「ターゲット端末」と呼ぶ）が生成する UN が、予測可能である必要がある。EMV 仕様において、UN は本来、予測不可能な 32bit の数字であることが規定されているが、端末の実装上の問題等により、（UN の乱数空間が狭いため）同じ数字が比較的短時間のうちに繰り返し出現してしまう場合や、UN が（時刻とともに増加する等の）単なるカウンタになっている場合等が本前提事項に該当する。

（攻撃①の概要）

- 攻撃者は、未使用のチャレンジ（UN）とレスポンス（ARQC）のペアを複数収集した上で、端末が実際に送付するチャレンジ（UN）をペアの中から発見できれば（上述、攻撃①固有の前提事項により発見できる可能性が出てくる）、それに対応するレスポンス（ARQC）を送付することにより攻撃が成功する。

（攻撃①の詳細）

「取引認証」に対する攻撃①の具体的な攻撃手法は以下の通り（図表 5）。

Step1．攻撃者は、ターゲット端末に対して、細工カードを挿入し、予め設定した当該カードの PIN を入力した上で、残高照会操作等の取引を実施する。

Step2．細工カードは、ターゲット端末から送信される取引内容（含む UN）を収集する。攻撃者は、Step1 および Step2 を繰り返すことにより、取引内容に関する情報を複数個収集し、ターゲット端末のチャレンジ（UN）生成に関する特徴（時刻とともに増加する等）を把握する。

Step3．攻撃者は、ターゲットに対して正規カードを細工端末に挿入させ、PIN や引き出し金額を入力させる。

Step4．細工端末は、正規カードに対してチャレンジ（UN）を含む取引内容を送信し、正規カードから返ってくる ARQC や ATC 等を受信する。ここでカードに送られるチャレンジ（UN）は、Step2 において情報収集した内容をもとに、将来生成されるであろうと予想される値とする。

Step5．細工端末は、Step4 の動作を様々なチャレンジ（UN）に対して繰り返し、送

信したチャレンジ（UN）とそれに対応するレスポンス（ARQC）のペアをリストに保存する。一方、ターゲットには「端末故障中」など、取引が正常に行えない旨の通知を行う。Step3 からの一連の流れを情報収集フェーズと呼ぶ。

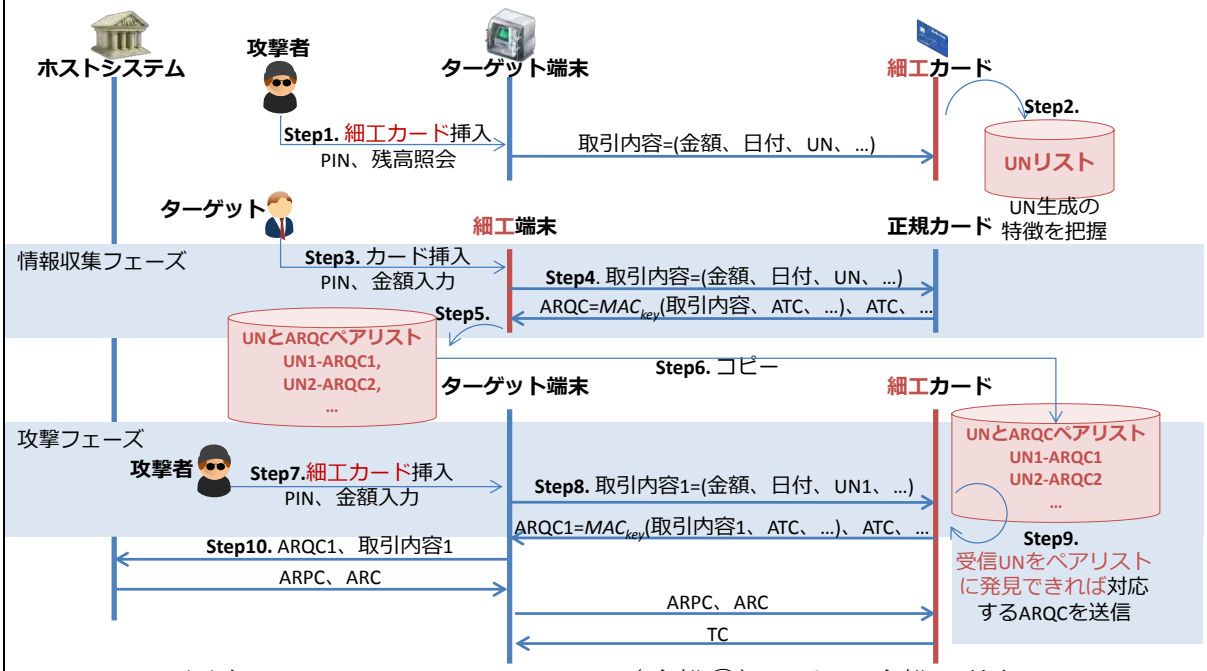
Step6. 攻撃者は、細工端末で収集した「UN と ARQC のペアのリスト」を細工カードにコピーする。

Step7. 攻撃者は、ターゲット端末に対して細工カードを挿入し、予め設定した当該カードの PIN を入力した上で、Step4 と同じ引き出し金額を入力する。

Step8. ターゲット端末は、当該取引に関する取引内容（含む UN）を生成し細工カードに送信する（ここでは取引内容、UN を、それぞれ取引内容 1、UN1 とする）。これと Step9 を攻撃フェーズと呼ぶ。

Step9. 細工カードは、受信した UN1 を、「UN と ARQC のペアリスト」の中に発見出来れば、受信したチャレンジ（UN1）に対応するレスポンスの ARQC（ここでは ARQC1）をターゲット端末に返信する。このようにして送信した ARQC1 は、正規のカードから生成された ARQC1 と見分けがつかない。

Step10. ターゲット端末は、カードから受信した ARQC1 と取引内容 1 をホストシステムに送信し、ホストシステムは ARPC と ARC をターゲット端末に返信する。ターゲット端末は、当該情報を細工カードに送信する。細工カードは TC を端末に送信することにより、端末は現金を攻撃者に払い出し、攻撃が成功する。



図表 5. Random number attack（攻撃①）による攻撃の仕組み

(3) Protocol flaw attack（攻撃②）による攻撃の仕組み

本節では Protocol flaw attack（攻撃②）固有の前提事項および、攻撃の仕組みについて述べる。

（攻撃②固有の前提事項）

- 攻撃者は、ターゲット端末をマルウェアに感染させること等により、端末とホストシステムとの間の通信を自由に改変することが出来る状態になっている必要がある。

（攻撃②の概要）

- 攻撃者は、未使用のチャレンジ（UN）とレスポンス（ARQC）を収集した上で、カードとホストシステム間の正規の通信を、予め収集しておいた情報にすり替えることにより（上述、攻撃②固有の前提事項により可能）攻撃が成功する。

（攻撃②の詳細）

「取引認証」に対する攻撃②の具体的な攻撃手法は以下の通り（図表 6）。

Step1．攻撃者は、ターゲットに対して正規カードを細工端末に挿入させ、PIN や引き出し金額を入力させる。

Step2．細工端末は、任意のチャレンジ（UN）を含む取引内容（ここでは、UN1、取引内容 1 とする）をカードに対して送信する。

Step3．正規カードは、受信した取引内容 1 に対して ARQC を生成し、細工端末に返信する（ここでは ARQC1 とする）。

Step4．細工端末は、送信した取引内容 1 と、受信した ARQC1 のペアを保存する。一方、ターゲットには「端末故障中」など、取引が正常に行えない旨の通知を行う。Step1 からの一連の流れを、情報収集フェーズと呼ぶ。

Step5．攻撃者は、ターゲット端末に対して、細工カードを挿入し、予め設定した当該カードの PIN および引き出し金額を入力する。

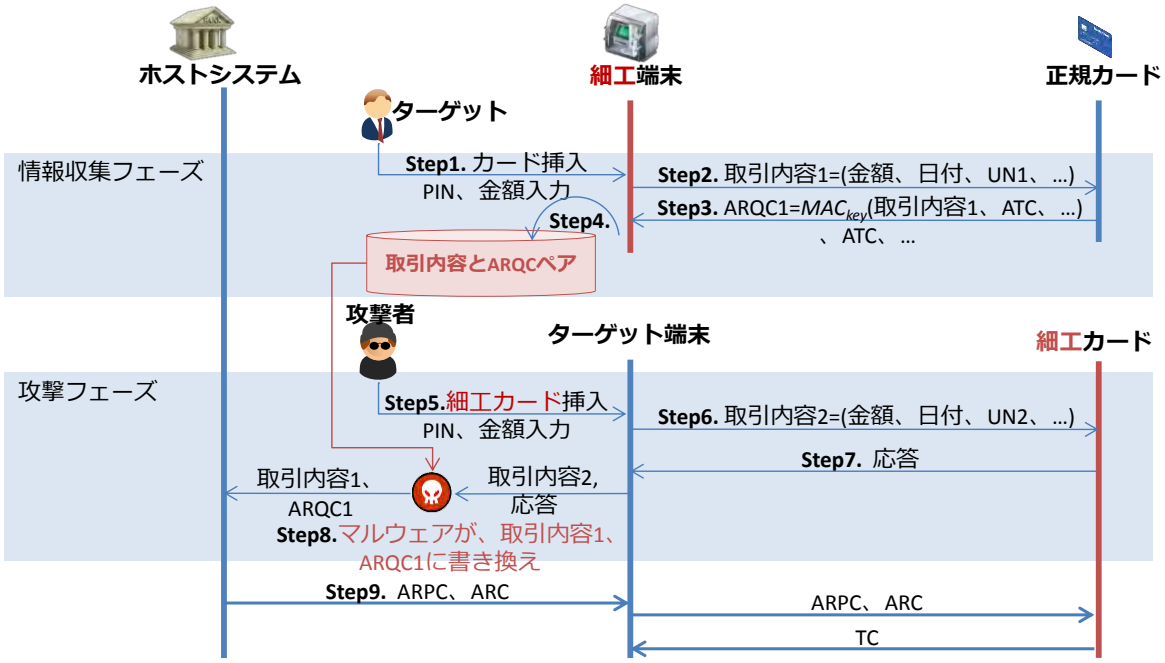
Step6．ターゲット端末は、入力された情報をもとに、取引内容を生成し（ここでは、取引内容 2 とする）細工カードに対して送信する。

Step7．細工カードは、Step6 に対する応答をターゲット端末に送信する。ターゲット端末は、取引内容 2 と Step6 に対する応答をホストシステムに送信しようとする。

Step8．ターゲット端末に感染したマルウェアが、ホストシステムに送信しようとした取引内容 2 と Step6 に対する応答を、それぞれ、Step4 で保存した取引内容 1

と ARQC1 にすり替え、ホストシステムに送信する。そのようにして送信された取引内容と ARQC は正規のカードから生成されたものと見分けがつかない。Step5.からの一連の流れを攻撃フェーズと呼ぶ。

Step9. ホストシステムは、ARPC と ARC を生成し、ターゲット端末に返信する。ターゲット端末は、それを細工カードに送信する。細工カードは TC を端末に送信することにより、端末は現金を攻撃者に払い出し、攻撃が成功する。



図表 6. Protocol flaw attack（攻撃②）による攻撃の仕組み

4. Pre-play attack が起こる原因および対策

本章では、Pre-play attack が起こる原因および対策について考察する。

(1) Pre-play attack が起こる原因の考察

攻撃①および攻撃②が起こる原因について考察する。

イ. 端末のチャレンジ（UN）生成方法の問題（原因Ａ）

攻撃①については、端末のチャレンジ（UN）生成方法に実装上の問題がある場合に攻撃が成功する。攻撃者は、チャレンジ（UN）が単なるカウンタになっている等、予測可能であるという前提により、それに対応するレスポンス（ARQC）を予め収集しておいたリストの中から返信可能となっている（図表 5 の Step9）。そうした ARQC は、端末のチャレンジに対する（正規カードのセッション鍵で生成された）メッセージ認証子であることが検証できるため、ホストシステムからする

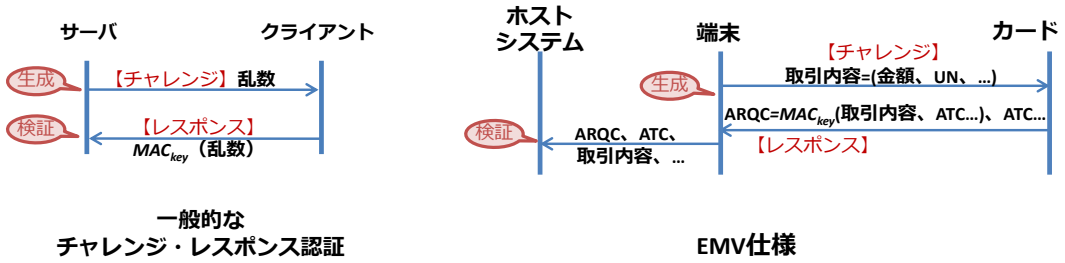
と正規のレスポンス（ARQC）にしか見えず、攻撃が成功する。

ロ．プロトコル仕様（原因Ｂ）

攻撃②については、EMV 仕様に基づいた「取引認証」のプロトコルの特徴を利用しており、端末が攻撃者の意図に従って動作する前提であるため攻撃が成功すると考えられる。EMV 仕様における「取引認証」は、図表 4 で説明したようにチャレンジ・レスポンス認証の方式と類似しており、両者を比較すると図表 7 のようになる。

一般的なチャレンジ・レスポンス認証においては、チャレンジ生成者とレスポンス検証者は同一主体である。一方、EMV 仕様に基づいた「取引認証」では、端末とカードのやり取りのみで行うオフライン取引にも対応できるようにする必要から、チャレンジ生成者とレスポンス検証者が異なるという特徴がある。このため、EMV 仕様に基づいた「取引認証」においては、チャレンジである取引内容が改ざんされても、検証者であるホストシステムでは、改ざんを知ることが出来ないという側面がある。

この点に関して EMV 仕様では、認定を受けた信頼できる端末を使用することが必須の前提となっている。攻撃②においては、端末のマルウェア感染により、この前提に反する環境になっているため、攻撃が成功する。



	一般的な チャレンジ・レスポンス認証	EMV 仕様に基づいた 「取引認証」
チャレンジ	サーバからクライアントに 送信される乱数	端末からカードに 送信される取引内容（含む UN）
レスポンス	クライアントからサーバに 送信される、乱数に対するメッセージ認証子	カードから端末経由でホストシステムに送信される ARQC
チャレンジ生成者	サーバ	端末
レスポンス検証者	サーバ	ホストシステム

図表 7．チャレンジ・レスポンス認証と EMV 仕様の「取引認証」の比較

(2) Pre-play attack への対策

上述した Pre-play attack が起こる原因（原因 A および原因 B）を踏まえた上で、どのような対策により、当該攻撃を防ぎ得るのかについて考察する。まず、Bond *et al.*[2014]において指摘されている対策を紹介する。

イ．チャレンジ（UN）に乱数を使用する

原因 A を解決するために、チャレンジ（UN）生成に予測不可能な乱数を使うことにより攻撃を防止出来る（攻撃①に有効）。なお、EMVCo[2014]においては、チャレンジ（UN）生成時に、専用の乱数生成ハードウェアを使用する方法や、ハッシュ関数（SHA-256）を使う方法が例として挙げられている。

ロ．ホストシステムにおいて取引カウンタ（ATC）を確認する

ホストシステムが、レスポンス（ARQC）を受信時に、カード毎の取引カウンタ（ATC）を確認することにより、（情報収集フェーズによって）不正に情報収集が行われたことを検知出来る可能性がある（攻撃①に有効）。ATC は取引毎にカウントアップされるものであり数字が減ることはありえない。そのためホストシステムは、「ARQC とともに受信した ATC」が「前回の取引で使われた ATC の値」以下であれば、情報収集フェーズにおいて取得された ARQC が使用された可能性があり、不正の可能性を検知出来る。また本対策は、ホストシステムにおける ATC のチェック機構を導入するという形で実現可能である。

ただし、受信した ATC が前回の取引で使われた ATC の値よりも大きいからといって、「不正が行われていない」ことを保証するものではないため、本対策で完全に不正を検知出来るわけではない。

ハ．ホストシステムにおいて取引承認（TC）を確認する

ホストシステムが、取引承認（TC）を端末から受信するたび毎に、その内容を検証することにより、攻撃を事後的に検知出来る可能性がある（攻撃①および攻撃②に有効）。図表 3 において、ホストシステムは、Step3 でレスポンス（ARQC）と取引内容を受信し、Step7 で TC を受信する。これらを用いて、ホストシステムは、TC の検証作業[14]を行うことにより、正規のカードが送信した TC か否かを確認できる。攻撃①および②においては、細工カードが TC を生成する（図表 5 における Step10 や、図表 6 における Step9）ため、この検証が失敗する可能性があり、ホストシステムは不正が行われたと検知できる。また本対策は、ホストシステムにおける TC のチェック機構を導入するという形で実現可能である。

[14] 例えば、ホストシステムにおいて「Step3 で受信した ARQC をもとに自らが生成した TC の内容」と、「受信した TC の内容」とが一致するか否かを確認する方法が考えられる。

ただし、IC カードシステムの実装によっては、ホストシステムで TC を受信する頃には、端末において現金を引き出す操作等が既に行われている可能性がある。そのような実装の場合には、本対策は不正を事後的に検知出来るに留まる。

ニ．端末のマルウェア感染対策とホストシステム・端末間通信の保護を実施する

攻撃②の前提条件となっている「端末のマルウェア感染」を防ぐことにより、攻撃を未然に防ぐことが出来る可能性がある（攻撃②に有効）。マルウェア感染を防ぐことにより、端末において通信内容を書き換えられることは出来なくなり、攻撃②を防ぐ事が可能となると考えられる。ただし、端末のマルウェア感染を防いだとしても、端末とホストシステム間の通信内容を（マルウェア感染とは別の方法で）攻撃者に書き換えられれば、攻撃②と同様の攻撃が成功する。このため、ホストシステム・端末間の通信路の保護も必要となる。

次に、Bond *et al*.[2014]では述べられていない対策について考察する。

ホ．ホストシステムにおいてチャレンジ（UN）を確認する

ホストシステムにおいて受信するチャレンジ（UN）の内容を確認し、原因 A で指摘したように、単なるカウンタになっている等、予想可能かどうか確認することにより、攻撃を未然に防ぐことが出来る可能性がある（攻撃①に有効）。端末の UN の生成方法を改善するというイ．で述べた対策は、攻撃①の根本的解決策として有効であるが、ホストシステムにおいても、UN の内容を図表 3 の Step3 にてチェックし、適切に生成されているかどうか確認することが出来る可能性がある。もしも、ホストシステムにて受信した UN が単なるカウンタ等、予測可能になっている場合には、当該端末に対して原因 A を排除する必要がある。また本対策は、ホストシステムにおける UN のチェック機構を導入するという形で実現可能である。

ヘ．タイムスタンプを用意し、レスポンス（ARQC）の生成に利用する

カードがレスポンス（ARQC）の生成の際に、時刻情報（タイムスタンプ）を含めることにより、ホストシステムは、受信した ARQC が情報収集フェーズによって過去に不正に情報収集されたものか否か確認出来る可能性がある（攻撃①および攻撃②に有効）。EMV 仕様においては、ARQC 生成の際には、日付をはじめとした情報に対して、メッセージ認証子を生成すること（MAC_{key}(金額、日付、UN…)）が最小要件として規定されている。このため、攻撃①および②において攻撃者は、ARQC に記載の日付と攻撃フェーズの日付が同日になるようにしなければ攻撃が成功しないことになる。そこで、カードが ARQC の生成を行う際に、時刻情報（hh 時 mm 分 ss 秒）も含めてメッセージ認証子生成を行う（メッセージ認証子は、

MAC_{key}(金額、日付、UN、時刻情報、…)となる）とともに、当該時刻情報自身を端末・ホストシステムに送信する。このようにすることで、ホストシステムは、ARQCが生成された時刻まで確認することが出来る。ホストシステムは、受信時刻から大きくずれた時刻に生成された ARQC を受信した場合には、不正な取引の可能性が高いと判断できる。本方式は、RFC6238（M'Raihi *et al.* [2011]）で規定されている時刻同期型ワンタイムパスワード（TOTP: Time-Based One-Time Password Algorithm）に類似した方式である。

ただし、攻撃者が情報収集フェーズの直後に攻撃フェーズを行う場合には、時刻のずれがあまり生じない。このため、本対策は攻撃検知の判断材料の一つとはなるものの、本対策だけで攻撃①②を完全に検知することは難しい。また、本対策は、EMV 仕様において送受信しているデータに新たな項目を追加して処理するという対応がホストシステム・カードの両者で必要となるほか、細工端末による時刻情報偽造への対策を考慮すると、「カード内で時刻を管理する」という機能を追加する必要があるため、既に展開しているカードの交換など、対応負担が大きくなると考えられる。

ト．カードとホストシステムで同期可能なカウンタを用意し、レスポンス（ARQC）の生成に利用する

カードとホストシステム間で同期可能なカウンタを新たに用意[15]し、カードがレスポンス（ARQC）生成の際に、当該カウンタを含めることにより、ホストシステムは、受信した ARQC が情報収集フェーズによって不正に情報収集されたものか否か確認できる可能性がある（攻撃①に有効）。カードが ARQC の生成を行う際にカウントアップするカウンタを新たに用意する（「オンライン専用カウンタ」と呼ぶ）。カードが ARQC の生成を行う際に、当該カウンタを含めてメッセージ認証子生成を行うほか、当該カウンタ自身を端末・ホストシステムに送信する（すなわち、カードからホストシステムに送信される電文は次のようになる。取引内容、ATC、オンライン専用カウンタ、MAC_{key}(取引内容、ATC、オンライン専用カウンタ、…)…)）ものと定義する。ホストシステムにおいても当該カウンタ情報を保有し、カードから ARQC を受信するたびに当該カウンタの内容を検証[16]する。攻撃①において

---

[15] EMV 仕様で規定されているカウンタに ATC があるが、ATC は①カードが取引を拒否する場合（カードが AAC と呼ばれる AC を生成する場合）においても ATC がカウントアップされるほか、②クレジットカード取引で起こりうるオフライン認証（ホストシステムが介さない「取引認証」）の場合にも ATC がカウントアップされるように EMV 仕様で規定されている。このため、ホストシステムのあずかり知らないところで ATC がカウントアップされることもあり得る。このようなことから、ATC を、ホストシステムとカードとで同期可能なカウンタとして使用することは難しい。

[16] 「受信した ARQC に含まれるオンライン専用カウンタ」＝「ホストシステムにおいて保持し

は、攻撃者が情報収集フェーズにて ARQC の生成（同時に、オンライン専用カウンタのカウントアップ）を複数回行う必要があるため、当該カウンタの検証に失敗する可能性がある。本方式は RFC4226（M'Raihi *et al.* [2005]）で規定されているカウンタを利用したワンタイムパスワード（HOTP: An HMAC-Based One-Time Password Algorithm）に類似した方式である。

ただし、攻撃者が次回生成される UN の内容を確実に予測することにより、情報収集フェーズで ARQC を一つだけ収集し、それを攻撃フェーズで使用されてしまえば、攻撃を受けたとしてもオンライン専用カウンタに不整合が生じない。このため、本対策も完全に攻撃を防げるわけではない。また、攻撃が行われていないにもかかわらず、何らかの理由でホストシステム側のオンライン専用カウンタとカード側の同カウンタの値がずれてしまった場合においても、オンライン専用カウンタの検証が失敗することになる。このため、本対策は攻撃検知の判断材料の一つとはなるものの、本対策だけで攻撃①を完全に検知することは難しい。また、本対策は、EMV 仕様において送受信しているデータに新たな項目を追加して処理するという対応がホストシステム・カードの両者で必要となる。

チ．前回取引時の取引カウンタを用意し、レスポンス（ARQC）の生成に利用する

カードがレスポンス（ARQC）生成の際に、「（EMV 仕様で規定されている）今回の取引カウンタ（ATC）」だけではなく、「前回取引時の取引カウンタ（ATC'とする）」も含めることにより、ホストシステムは、受信した ARQC が情報収集フェーズによって不正に情報収集されたものか否か確認できる可能性がある（攻撃①に有効）。カードが ARQC の生成を行う際に、ATC'を含めてメッセージ認証子生成を行うほか、ATC'自身を端末・ホストシステムに送信する（すなわち、カードからホストシステムに送信される電文は次のようになる。取引内容、ATC、ATC'、MAC_{key}(取引内容、ATC、ATC'、…)…）ものと定義する。ホストシステムにおいては、受信した ATC と ATC'との差が大きくなっていないか検証する。攻撃①においては、攻撃者が情報収集フェーズにて ARQC の生成（同時に、ATC のカウントアップ）を複数回行う必要があるため、ATC と ATC'の差が大きくなる。

ATC'については、①EMV 仕様で既に定められている「Last Online ATC Register」の値（直近にホストシステムに対して送信した ATC の値）を使用する方法と、②EMV 仕様には定められていない新たなカウンタ値（前回正常に取引した時の ATC 値を取得するために、図表 3 の Step6 における ATC の値）を使用する方法が考えられる。①の方法では、攻撃における情報収集フェーズにて ATC'と ATC がともに

ていたオンライン専用カウンタ」＋１、となっているか確認する、という方法が考えられる。

カウントアップされてしまうため、本対策には不適当であると考えられる。②の方法では、攻撃における情報収集フェーズにて ATC'はカウントアップされない一方で、ATC はカウントアップされるため、両者に差が生じることになり、攻撃検知として使用可能である。

本対策は、ロ．やト．とは異なり、ホストシステムにおいてカード毎の ATC やオンライン専用カウンタ情報を保持しておく必要はなく、通信ごとに受信した ARQC から取り出した ATC と ATC'を比較するだけで良いため、ホストシステムにおけるリソースの節約になる。

ただし、ATC と ATC'との間に差が生じる場合としては、攻撃①が行われた場合以外にも、「直近取引においてカードが取引を拒否した場合（カードが AAC と呼ばれる AC を生成した場合）」も考えられる。この場合、ATC'の値に、AAC が生成された回数を加えたものが今回の ATC の値になる。このため、本対策は攻撃検知の判断材料の一つとはなるものの、本対策だけで攻撃①を完全に検知することは難しい。また、本対策は、EMV 仕様において送受信しているデータに新たな項目を追加して処理するという対応がホストシステム・カードの両者で必要となる。

リ．ホストシステムにおいてチャレンジ（UN）を生成する

原因 B を踏まえた対策として、チャレンジ（UN）の生成を、（端末ではなく）ホストシステムが行うようにすることにより、取引内容（含む UN）の改ざんをホストシステムにて検知することが出来る可能性がある（攻撃②に有効）。このようにフローを変更することにより、ホストシステムが自らチャレンジ（UN）を生成し、それに対するレスポンス（ARQC）の検証を自身で行うことが可能となり、ARQC を受信した際に、それが不正に収集されたものか否かを判断出来る可能性がある。

ただし、本対策は、EMV 仕様の「取引認証」におけるフローに対して「ホストシステムから端末への UN 送信」といった新たなフロー追加することになり、それに伴う大きな仕様変更が必要であり、大幅なシステム改修が必要になる可能性がある。また、（攻撃②の前提となっている）端末のマルウェア感染を考えると、情報収集フェーズにおいて、ホストシステムから受け取ったチャレンジ（UN）とそこから生成した ARQC のペアをマルウェアによって攻撃フェーズで使用されてしまうという手法も考えられるため、完全に攻撃を防げるわけではない。

ヌ．対策のまとめ

上記イ～リ．で対策手法を考察してきたが、それらの対策をまとめると図表 8 のようになる。

対策手法	攻撃①への有効性	攻撃②への有効性	実現の容易性
イ．チャレンジ（UN）に乱数を使用する	◎	×	○
ロ．ホストシステムにおいて取引カウンタ（ATC）を確認する	○	×	○
ハ．ホストシステムにおいて取引承認（TC）を確認する	○	○	○
ニ．端末のマルウェア感染対策とホストシステム・端末間通信の保護を実施する	×	◎	○
ホ．ホストシステムにおいてチャレンジ（UN）を確認する	○	×	○
ヘ．タイムスタンプを用意し、レスポンス（ARQC）の生成に利用する	○	○	△
ト．カードとホストシステムで同期可能なカウンタを用意し、レスポンス（ARQC）の生成に利用する	○	×	△
チ．前回取引時の取引カウンタを用意し、レスポンス（ARQC）の生成に利用する	○	×	△
リ．ホストシステムにおいてチャレンジ（UN）を生成する[17]	×	○	×

有効性について　◎：有効性が高い対策、○：完全ではない対策、×：有効でない対策
実現容易性について　○：EMV 仕様の変更が不要な対策や EMV 仕様が本来求めている対策、
△：EMV 仕様に大きな変更は不要であるものの、ホストシステム・カードの両者に修正が必要な対策、×：EMV 仕様に大きな変更が必要な対策

図表 8．Pre-play attack への対策手法のまとめ

攻撃①への対策としては、「イ．チャレンジ（UN）に乱数を使用する」が最も有効性が高く、現実的な対応であると考えられる。また、それに加えて、ロ．、ハ．およびホ．の対策を実施することにより、EMV 仕様に大きな変更を加えることなくセキュリティレベルを向上させることが出来ると考えられる。

攻撃②への対策としては、「ニ．端末のマルウェア感染対策とホストシステム端末間通信の保護を実施する」が最も有効性が高く、現実的な対応であると考えられる。また、それに加えてハ．の対策を実施することにより、EMV 仕様に大きな変更を加えることなくセキュリティレベルを向上させることが出来ると考えられる。

[17] ただし、ホストシステムにおいて対策イ．が実施されていない場合。

5. おわりに

本稿では、EMV 仕様の IC カード利用システムを取り上げ、当該システムにおける「取引認証」への新しい攻撃手法の例として「Pre-play attack」について解説を行った。当該攻撃手法である Random number attack と Protocol flaw attack の 2 種類を紹介し、いずれの手法も、「攻撃者が端末・IC カード間の通信であるチャレンジとレスポンスを不正に収集しておくことにより、ある前提を満たす状況において、正規 IC カードを所有していないにもかかわらず、ターゲット（被害者）の IC カードを模倣した振舞いを行える不正な IC カードを作成することが出来る」可能性を示した。当該攻撃が起こる原因について、端末の UN 生成方法の問題と、プロトコル仕様について言及した上で、当該攻撃への対策手法に関する考察をした。対策手法については、Pre-play attack に関する論文（Bond *et al*.[2014]）では触れられていない様々なアイデアについても範囲を広げて検討し、他の対策手法についての提案も行った。対策をまとめると、攻撃成立の前提を崩すために、①端末のチャレンジ（UN）の生成に乱数を用いることや、②端末のマルウェア感染を防き、ホストシステム・端末間の通信を保護する、といった対策が現実的であるほか、③ホストシステムにおいて取引カウンタ（ATC）を確認する、④ホストシステムにおいて取引承認（TC）の内容を確認する、⑤ホストシステムにおいてチャレンジ（UN）がカウンタ等になっていないか確認する、ということも有効であり、IC カード利用システムにおいてこれらの点に留意すべきであると考えられる。

なお本稿においては、EMV 仕様に基づく理論的な考察を中心に行った。今後の研究課題としては、各対策技術について、運用面を含め既存システムへの適用の可能性とその課題について更なる検討を実施することが望ましいと考えられる。

IC カード利用システムにおける不正事件の手口は日々巧妙化している。例えば、Bond *et al*.[2014]においては、インターネット・オークションで中古の ATM を購入し、ATM のハードウェアやソフトウェアの解析を行っている。研究者が ATM の解析が出来るということは、犯罪者（攻撃者）も同様のことが出来ると考えるべきであり、本稿で述べたものよりも、より巧妙な手口が将来出てくる可能性がある。したがって、国内外の不正事件や学界の動向を注視しつつ、セキュリティ向上のための努力を今後も継続することが重要である。

以　上

付録　本稿で述べた EMV 仕様関係の用語集

用語	説明
EMV 仕様	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。EuroPay International、Mastercard International および Visa International の間で合意した規格であるため、三社の頭文字をとって名付けられた。
PIN	Personal Identification Number 本人認証のために必要となる暗証番号
SDA	Static Data Authentication 静的データ認証。カード認証を実施する際に、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こと。
AC	Application Cryptogram 取引内容等に対するメッセージ認証子（本稿では MAC_{key}（取引内容等）と記す）。取引内容等に対して鍵（ホストシステムとカードが共有するセッション鍵）を使って暗号化を施すことにより計算する。 ホストシステムは、平文の取引内容等と、AC（MAC_{key}（取引内容等））を同時に受信することにより、取引内容等の改ざんを検知することが出来る。 EMV 仕様においては、AC として ARQC（Authorisation Request Cryptogram）、AAC（Application Authentication Cryptogram）、TC（Transaction Certificate）の 3 種類が規定されている。
ARQC	Authorisation Request Cryptogram オンライン取引承認要求を意味する AC。取引内容や ATC 等に対するメッセージ認証子。ARQC=MAC_{key}（取引内容、ATC、…）となる。
TC	Transaction Certificate 取引承認を意味する AC。取引内容や ATC、ARC 等に対するメッセージ認証子。TC= MAC_{key}（取引内容、ATC、ARC、…）となる。
UN	Unpredictable Number 端末が生成する 32bit の「予測不可能な数」。UN は、EMV 仕様における「取引認証」においてチャレンジとしての役割を果たす。UN は、同一端末で続けて同一金額の取引を行った場合であっても、異なる AC を生成して区別できるようにすることを目的としている。ATC も同様の目的であるが、ATC はカードにおいて生成されるのに対して、UN は端末において生成される。仮に、カードにおいて ATC が正しく実装されていなかったとしても、端末が生成する UN により当該目的を実現することが可能となる。

ATC	Application Transaction Counter カード内に保存されている取引カウンタ。取引開始毎に 1 ずつカウントアップされる。ATC は、取引カウンタとしての目的の他に、UN と同様に、同一端末で続けて同一金額の取引を行った場合でも、異なる AC を生成して区別できるようにすることを目的としている。仮に、端末において UN が正しく実装されていなかったとしても、カードが生成する ATC により当該目的を実現することが可能となる。
ARC	Authorisation Response Code 当該取引をホストシステムが実施することが適当であるか否かが記載されているコード。
ARPC	Application Response Cryptogram ホストシステムにて生成される暗号。カードがホストシステムに送信した ARQC に対する返信が、改ざんされることなく、正当なホストシステムから来たことを、カードが確認するために使用される。ホストシステムにおける生成に関しては、ARQC と ARC に対して XOR 演算を施したものに対して、Triple DES や AES で暗号化を施す方法等が規定されている。

参考文献

金融庁、「偽造キャッシュカード問題等に対する対応状況（平成 26 年 3 月末）について」、2014 年 8 月 27 日（http://www.fsa.go.jp/news/26/ginkou/20140827-5.html）

鈴木雅貴・廣川勝久・古原和邦、「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」、『金融研究』第 31 巻第 3 号、2012 年、107～140 頁

BBC, “Chip and pin ‘weakness’ exposed by Cambridge researchers,” BBC News technology, 2012. (http://www.bbc.com/news/technology-19559124)

Bond, Mike, Omar Choudary, Steven J. Murdoch, Sergei Skorobogatov, and Ross Anderson, “Chip and Skim: cloning EMV cards with the pre-play attack,” IEEE Symposium on Security and Privacy, pp.49-64, 2014.

EMVCo, “Book 1 Application Independent ICC to Terminal Interface Requirements,” EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, EMVCo, 2011 a.

———, “Book 2 Security and Key Management,” EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, EMVCo, 2011 b.

———, “Book 3 Application Specification,” EMV Integrated Circuit Card Specifications

for Payment Systems, Version 4.3, EMVCo, 2011 c.

———, “Book 4 Cardholder, Attendant, and Acquirer Interface Requirements,” EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.3, EMVCo, 2011 d.

———, “SB-144: Terminal Unpredictable Number generation (Spec Change),” Specification Bulletin 1st Edition, EMVCo, 2014.

———, “Worldwide EMV Chip Card Deployment and Adoption,” Worldwide EMV Deployment Statistics, EMVCo, 2015.

(https://www.emvco.com/documents/EMVCo_EMV_Deployment_Stats.pdf)

M’Raihi, D, S.Machani, M.Pei, and J.Rydell, “TOTP: Time-Based One-Time Password Algorithm,” IETF, RFC 6238, 2011.

———, M.Bellare, F.Hoornaert, D.Naccache, and O.Ranen, “HOTP: An HMAC-Based One-Time Password Algorithm,” IETF, RFC 4226, 2005.