IMES DISCUSSION PAPER SERIES

EMVカードシステムへの新攻撃手法を踏まえた、インターネット・バンキングにおける「取引認証」実施時の留意事項

井澤秀益（いざわひでみつ）・中山靖司（なかやまやすし）

Discussion Paper No. 2015-J-11

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-11

2015 年 7 月

EMV カードシステムへの新攻撃手法を踏まえた、インターネット・バンキングにおける「取引認証」実施時の留意事項

井澤秀益（いざわひでみつ）*・中山靖司（なかやまやすし）**

要　旨

近年、金融機関のリテール取引チャネルの一つとしてインターネット・バンキングによる重要性が増している。一方で、インターネット・バンキングを利用した不正送金による被害は増加し社会問題化している。このような不正送金への対策の一つとして「取引認証」が考えられ、国内の金融機関において導入に向けた動きがみられる。この「取引認証」は IC カードを利用した取引においては一般的に行われているもので、その業界標準である EMV 仕様の中で「取引認証」の仕組みが規定されている。

しかしながら近年、EMV 仕様の「取引認証」への攻撃手法が発表されており、同攻撃手法は、インターネット・バンキングへの「取引認証」にも適用できると考えられる。

そこで本稿では、EMV 仕様の「取引認証」への攻撃手法を踏まえ、インターネット・バンキングにおける「取引認証」への攻撃手法を検討するとともに、その対策・留意点について考察する。考察にあたっては、システム構築上の留意点だけではなく、ユーザ教育・啓蒙活動の観点での留意点についても言及する。

キーワード : インターネット・バンキング、取引認証、MitB 攻撃、Pre-play attack、ユーザ教育・啓蒙活動

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企画役（現総務人事局、E-mail: yasushi.nakayama@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、金融機関のリテール取引チャネルの一つとしてインターネット・バンキングの契約口座数が増加し（FISC [2013,2012,2011,2010]）、金融機関にとって必要不可欠な決済インフラとなっている。一方で、同バンキングの不正送金による被害は増加傾向にあり（全国銀行協会[2015]）社会問題化している。このような不正送金は、フィッシング等の認証情報窃取による預金者への成りすましやパソコンのマルウェア[1]感染による自動送金等の手法によるものと考えられる。また海外においては、マルウェアが預金者の行った取引指図の内容を秘密裏に改ざんする Man-in-the-Browser 攻撃（MitB 攻撃）も確認されており、今後、国内の金融機関に対して同攻撃が行われる可能性が考えられる。MitB 攻撃への対策手法はいくつか考えられるが、その一つとして「取引認証[2]」があり（鈴木・中山・古原[2013]）、国内金融機関においても一部で導入に向けた動きがみられる。

一方、キャッシュカード等で使われる IC カードにおいては、その業界標準である EMV 仕様[3]において、「取引認証」の仕組みが仕様に規定されている（EMVCo [2011a,b,c,d]）。しかし近年、英国ケンブリッジ大学の研究グループから、EMV 仕様における「取引認証」に対して、特定の条件のもとで攻撃が成立しうることが発表された（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について、本攻撃手法が使われた可能性を指摘している。この Pre-play attack の基本的な考え方は、EMV カードシステムの「取引認証」に限らず、近年導入に向けた動きがあるインターネット・バンキングの「取引認証」にも適用可能であると考えられる。

そこで、本稿では、第 2 章で前提知識として、インターネット・バンキングの「取引認証」について触れた後、第 3 章で IC カードシステムにおける Pre-play attack の手法を解説する。次に、第 4 章でインターネット・バンキングの「取引認証」に対して Pre-play attack を適用した場合の攻撃手法およびその対策を検討し、「取引認証」実施時における留意点等について考察する。最後に第 5 章でまとめる。

---

[1] 本稿では、「コンピュータの利用者に対し、何らかの形で有害な機能を持ったプログラム等」について、コンピュータウィルスを含め「マルウェア」と呼ぶことにする（土居ほか[2003]）。

[2] ログイン時の本人認証とは別に、本人の意思に基づいた取引指図（振込先、金額等）であることを金融機関が確認すること。

[3] 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. インターネット・バンキングにおける「取引認証」

本章では、インターネット・バンキングにおける不正送金の手口やその対策としての「取引認証」について、解説する。

(1) インターネット・バンキングにおける不正送金の手口

インターネット・バンキングにおける不正送金の被害件数・被害額は、年々増加しており（全国銀行協会[2015]）、不正送金の手口も、以下の通り徐々に巧妙化している（大日向[2015]）。

偽メールによる情報搾取：攻撃者が顧客に対して偽メール（フィッシングメール）を送付し、顧客をフィッシングサイトに誘導した上で、偽画面を表示し、顧客の ID、パスワードや乱数表情報を不正に取得する手法。【2011 年頃から現在に至るまで継続的にみられる】

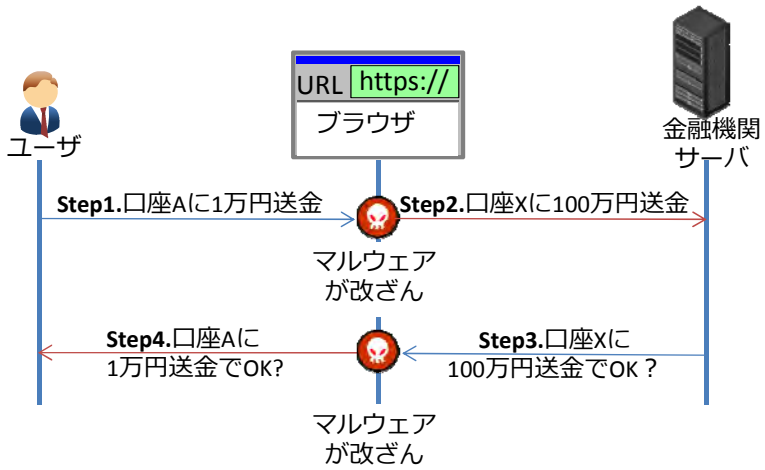
マルウェアによる情報搾取：攻撃者が顧客の PC をマルウェアに感染させ、顧客がインターネット・バンキングに接続すると、マルウェアがブラウザに表示される画面を書き換え、乱数表等の認証用情報の入力要求を表示し、攻撃者が当該情報を不正に取得する手法。【2012 年 10 月頃から現在も時々見られる手口】

マルウェアによる自動送金：攻撃者が顧客の PC をマルウェアに感染させ、顧客がインターネット・バンキングに接続すると、マルウェアが、画面上は「ダウンロード中」等の偽画面を表示しつつも、裏では攻撃者への振込操作を自動実施（その後の乱数表等認証用情報の入力を顧客に求める）するという手法。【2013 年 9 月頃から現在も続いている手口】

さらに、海外においては以下のような Man-in-the-Browser 攻撃（以下、「MitB 攻撃」）と呼ばれる、さらに高度な攻撃手法が出てきており、今後国内においても出現する可能性が指摘されている。

マルウェアによる取引改ざん：攻撃者が顧客の PC をマルウェアに感染させ、顧客がインターネット・バンキングに接続し、取引のタイミングになったところで、マルウェアが活動を開始し、表示画面や送信内容を改ざんする。例えば、「口座 A に 1 万円送金」との送金指示が、マルウェアによって「口座 X に 100

万円送金」と改ざんされ、金融機関サーバに送信される。金融機関からの確認画面も改ざんされ、元の指示である「口座 A に 1 万円送金」と表示される。不自然な画面が表示されること等が一切無いため、ユーザが気づくことは難しい（図表 1）。



図表 1. マルウェアによる取引内容改ざん（MitB 攻撃）

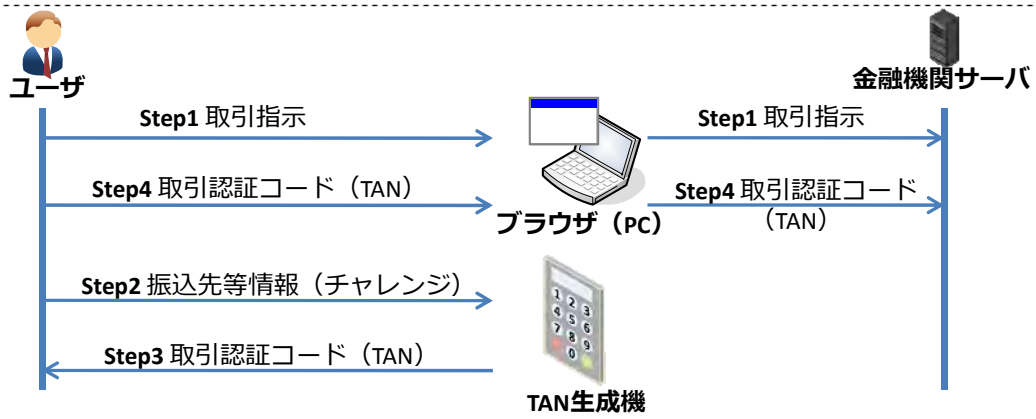
このようなマルウェアによる自動送金の手口やマルウェアによる取引改ざんの手口（MitB 攻撃）は、正規の本人による認証が終わった後に行われるものであることから 2 要素認証等による本人認証の強化を行っていたとしても対策とはならず、本人認証強化による対策には限界がある。

(2) 不正送金対策としての「取引認証」

マルウェアによる自動送金や取引改ざんの手口への対策は色々考えられるが、その一つとして、「取引認証」が挙げられる（鈴木・中山・古原[2013]）。「取引認証」を行うことにより、マルウェアによる自動送金が行われても、金融機関は本人の取引意思に基づくものなのかを確認することが出来るほか、マルウェアによる取引の改ざんが行われても、それを検知することが可能となる。

「取引認証」の具体例について、鈴木・中山・古原[2013]で述べられた 3 形態について以下で解説する。これらの形態は、PC がマルウェア感染したとしても、第 2 要素認証機器（以下で述べる、TAN 生成機、携帯電話、ページャー）がマルウェア感染しなければ、「取引認証」を行うことが出来るものとなる。

イ．TAN 生成機使用フロー



図表 2．TAN 生成機を使用する取引フロー

Step1．ユーザは、金融機関サーバに対して、振込先口座番号および金額の入力といった取引指示を、PC のブラウザを介して行う。

Step2．ユーザは、TAN 生成機に対して、振込先等の情報（振込先口座番号や振込金額等。以降、「チャレンジ」と呼ぶ）を入力する。

Step3．TAN 生成機は、チャレンジ、タイムスタンプ、カウンタ、および鍵[4]等をもとに、取引認証コード（TAN: Transaction Authentication Number）を生成[5]する。

Step4．ユーザは、Step3 で得られた TAN を PC のブラウザを介して金融機関のサーバに対して送信する。金融機関は、Step1 の取引指示を基に TAN を生成し、受信した TAN と一致するかどうかを検証[6]することによって、取引内容が改ざんされていないことを確認した上で、振込を実施する。

本取引フローでは、PC がマルウェア感染し、取引指示が改ざんされたとしても、マルウェアは正しい TAN を生成できないため（TAN 改ざんのためには鍵が必要）、MitB 攻撃に耐性を持つ取引フローであると言える。

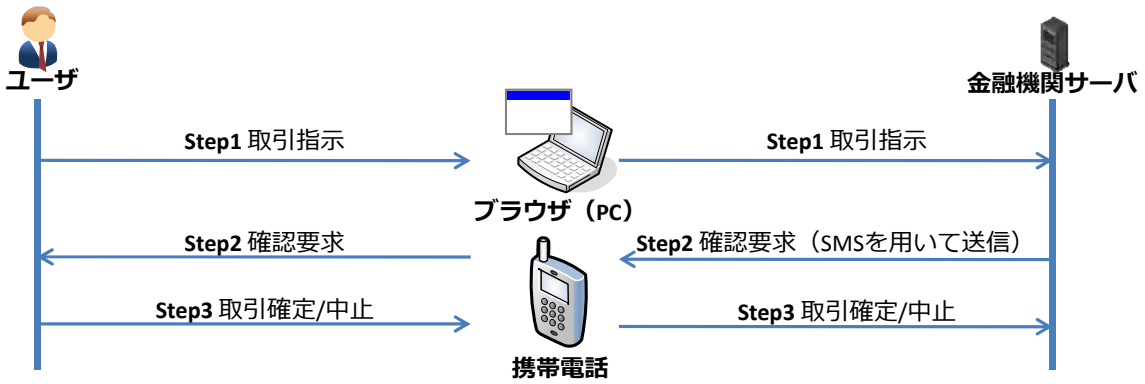
---

[4] 鍵は、TAN 生成機と金融機関で事前に共有しているとする。

[5] TAN 生成方法として例えば、RFC6287（M'Raihi *et al.*[2011]）において OCRA（OATH Challenge-Response Algorithm）が規定されている。OCRA では、チャレンジ、タイムスタンプおよびカウンタ等に対して、HMAC（メッセージと鍵に対してハッシュ関数を演算する方法）を利用する方法が規定されている。

[6] 金融機関は一度受け入れた（振込を実施した）TAN と同じものは拒絶する仕組みを持っていると仮定する。仮に、拒絶できなければ、攻撃者が TAN を盗聴し、それを再送する攻撃（Replay Attack：リプレイ攻撃）が成功してしまうことになる。

ロ．携帯電話使用フロー



図表 3. 携帯電話を使用する取引フロー

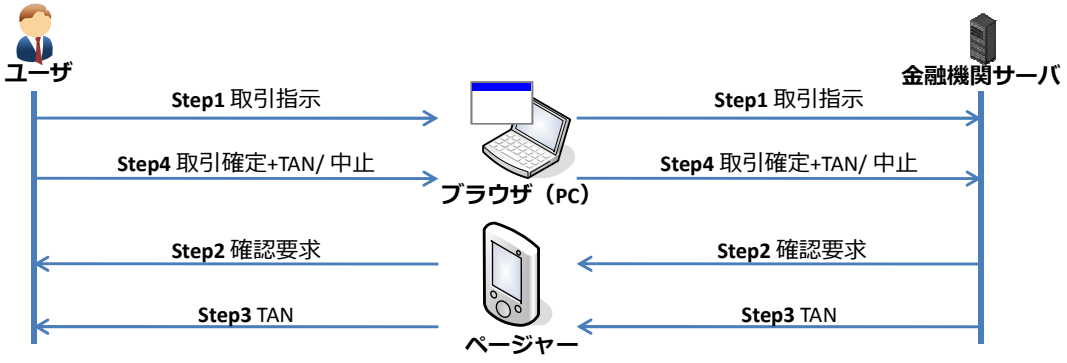
Step1. ユーザは、金融機関サーバに対して、振込先口座番号、金額といった取引内容の指示を、PC のブラウザを介して行う。

Step2. 金融機関は、振込相手先や金額情報を記した取引内容の確認要求を、ユーザの携帯電話に SMS 等を用いて送信する。

Step3. ユーザは、Step2 で受けた取引内容を確認した上で、取引を確定させるか中止するかの判断を行い、携帯電話を介して金融機関に指示を行う。金融機関は、確定指示を受けた場合、Step1 の取引指示に基づき振込を実施する。

本取引フローでは、PC がマルウェア感染して取引指示が改ざんされたとしても、別経路（携帯電話）で確認要求が来ることにより、ユーザは取引内容の改ざんに気づくことが出来るため、MitB 攻撃に耐性を持つ取引フローであると言える。

ハ．ページャー使用フロー



図表 4. ページャーを使用する取引フロー

Step1. ユーザは、金融機関サーバに対して、振込先口座番号、金額といった取引

内容の指示を、PC のブラウザを介して行う。

Step2．金融機関は、振込相手先や金額情報を記した取引内容の確認要求をユーザのページャー[7]（ポケットベル）に送信する。

Step3．金融機関は、取引内容を元に生成した TAN をユーザのページャーに送信する。

Step4．ユーザは、Step2 で受けた取引内容を確認した上で、取引を確定させるか中止させるかの判断を行い、①確定させる場合にはその旨と Step3 で受信した TAN を、②取引中止する場合にはその旨のみを、PC のブラウザを介して金融機関に送信する。金融機関は、確定指示を受けた場合、受信した TAN が Step3 でページャーに送った TAN と一致する場合は、取引が改ざんされていないものとして振込を実施する。

本取引フローでは、PC がマルウェア感染して取引指示が改ざんされたとしても、別経路（ページャー）で確認要求が来ることにより、ユーザは取引内容の改ざんに気づくことが出来るため、MitB 攻撃に耐性を持つ取引フローであると言える。

3. IC カード利用システムにおける Pre-play attack の手法

本章では、EMV 仕様に準拠した IC カード利用システムにおける Pre-play attack の手法の解説を簡単に行う。

(1) EMV 仕様のセキュリティ対策

EMV 仕様[8]における主なセキュリティ対策としては、①「カード認証」、②「本人認証」、③「取引認証」の 3 種類が仕様に規定されている（EMVCo[2011a,b,c,d]）。①の「カード認証」は、端末が、IC カードの真正性を確認することを目的としており、IC カード固有のデータに対するデジタル署名を端末で検証すること等によって実現している。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おり、ユーザが入力した PIN（暗証番号）をホストシステム内に登録されている PIN や IC カード内に登録されている PIN と照合すること等によって実現している。③の「取引認証」は、ホストシステムが、IC カードを利用した取引の内容の真正性および当該取引が正規の IC カードからのもので

[7] ここでは、金融機関サーバからの確認要求の受信および表示機能を備える機器としてページャーを挙げているが、同機能を満たす携帯電話（スマートフォン）を用いても構わない。

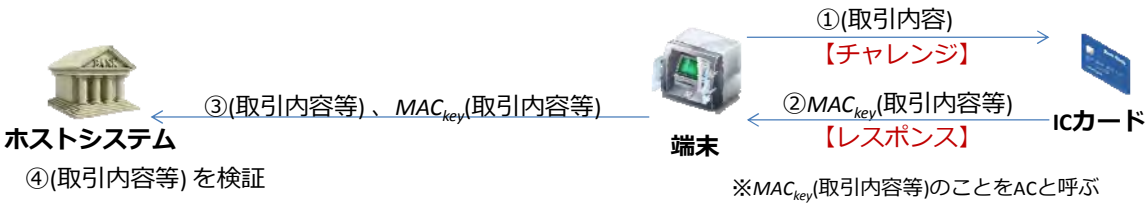
[8] EMV 仕様に準拠した IC カードを使った取引においては、ホストシステム、端末、IC カードおよびユーザからシステムが構成される。

あることを確認することを目的としており、実現方法については次節で述べる。

(2) EMV 仕様の「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[9]である。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 IC カードとで共有している鍵（「セッション鍵」）を意味する。

「AC の生成・検証」の流れとしては、図表 5 に示す通り、①端末が取引内容を IC カードに送付し、②IC カードが取引内容をはじめとする項目に対してメッセージ認証子を付与（AC 生成）したうえで端末に返信する。次に、③端末は、IC カードから受け取った AC とともに取引内容等をホストシステムに送付し、④ホストシステムは受信した情報を使って AC を検証（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に対して、セッション鍵を用いて自らも 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有無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 5. EMV 仕様における「取引認証」のポイント

EMV 仕様における「取引認証」のもう一つのポイントは、図表 5 における「取引内容」に、UN（Unpredictable Number）と呼ばれる乱数などの「予測不可能な数」を加えるという点である。UN は、チャレンジ・レスポンス認証におけるチャレンジの役割を果たし、AC はレスポンスの役割を果たす。UN は、同一端末で続けて同一金額の取引を行ったとしても、異なる AC を生成させる目的で用いられる。

---

[9] 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) Pre-play attack の攻撃手法・原因・対策

Pre-play attack は、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 カードを作成する攻撃手法である。

Pre-play attack では、攻撃を行うための情報収集の手法として 2 種類の手法が提案されており（Bond *et al.* [2014]）、その内容を図表 6 にまとめる。Pre-play attack の詳細については（井澤・廣川[2015]）を参照されたい。

	攻撃手法 1	攻撃手法 2
主な攻撃前提	・攻撃者が用意した端末（ATM や POS）に対して、被害者が自身の IC ｶｰﾄﾞを挿入し、PIN を入力する。	
	・端末のﾁｬﾚﾝｼﾞ（UN）生成方法について、EMV 仕様上は「予測不可能な数」を生成するべきところを、実装の不備等でﾁｬﾚﾝｼﾞ（UN）が攻撃者に類推可能である場合。	・端末がﾏﾙｳｪｱ感染しており、攻撃者が端末でやり取りされる情報を自由に操作できる場合。
攻撃手法の概要	・攻撃者が類推したﾁｬﾚﾝｼﾞ（UN）とそれに対するﾚｽﾎﾟﾝｽ（AC）のﾍﾟｱを正規 IC ｶｰﾄﾞを使って収集しておき、端末が送信するﾁｬﾚﾝｼﾞ（UN）が当該ﾍﾟｱの中に発見できれば、対応するﾚｽﾎﾟﾝｽ（AC）を端末に送付し AC 検証を突破する。	・攻撃者がﾁｬﾚﾝｼﾞ（UN）とﾚｽﾎﾟﾝｽ（AC）のﾍﾟｱを正規 IC ｶｰﾄﾞを使って収集しておき、端末上のﾏﾙｳｪｱがﾁｬﾚﾝｼﾞおよびﾚｽﾎﾟﾝｽを当該ﾍﾟｱにすり替えて AC 検証を突破する。
主な原因	・端末の乱数生成方法に問題がある（【原因Ａ】と呼ぶ)。	・EMV 仕様ではﾁｬﾚﾝｼﾞ（取引内容）がすり替えられても、それに対するﾚｽﾎﾟﾝｽの検証者（ﾎｽﾄｼｽﾃﾑ）は、すり替えを知ることが出来ない[10]（【原因Ｂ】と呼ぶ)。
主な対策 [井澤・廣川 2015]	・端末の UN に乱数等の「予測不可能な数」を使用する。 ・ﾎｽﾄｼｽﾃﾑにて UN が単なるｶｳﾝﾀになっていないか確認する。	・端末のﾏﾙｳｪｱ感染とﾎｽﾄｼｽﾃﾑ・端末間通信の保護を実施する。 ・ﾎｽﾄｼｽﾃﾑにおいて取引承認の AC（TC）を確認する。

図表 6. Pre-play attack の攻撃手法・原因・対策のまとめ

[10] EMV 仕様においてはオフライン処理も想定しているため、チャレンジ生成者とレスポンス検証者が異なることを前提としているプロトコル設計となっている。

4. Pre-play attack の手法をインターネット・バンキングの「取引認証」に適用した場合の、攻撃手法と対策

本章では、3.で説明した IC カード利用システムにおける「取引認証」への攻撃手法（Pre-play attack）を、インターネット・バンキングの「取引認証」に適用した場合の攻撃手法およびその対策・留意事項について考察する。まず、考察の前提事項について(1)で述べた上で、Pre-play attack の適用に関する考え方を(2)で述べる。(3)、(4)において、具体的な攻撃手法および対策・留意点について述べる。

(1) 前提とするインターネット・バンキングおよび攻撃者

イ．ユーザの前提

想定するインターネット・バンキングのユーザとして、以下の想定を置く。

- ユーザの PC はマルウェア感染しているとする。

また本前提に伴い、マルウェアは、PC のブラウザ画面上に様々な指示を出すことにより、ユーザを騙そうとする（攻撃者にとって好ましいと思う動作をユーザに指示する）事が出来ると仮定する。ユーザがマルウェアの出した指示に騙されるか否かによって、以下の 2 通りのユーザの前提を考える。

「ユーザの前提」2 種類

- 【Ⅰマルウェアに騙されないユーザ】: マルウェア（攻撃者）が出した指示に騙されないユーザ。すなわち、金融機関が意図する動作を行うユーザ。
- 【Ⅱマルウェアに騙されるユーザ】: マルウェア（攻撃者）が出した指示に騙されてしまうユーザ。すなわち、金融機関が意図する動作から逸脱してしまうユーザ。

ロ．取引フローにおける前提

想定するインターネット・バンキングにおける「取引認証」のフローとして、2.(2)で述べた 3 通りの前提を考える。

「取引フローの前提」3 種類

- 【①TAN 生成機使用フロー】（図表 2）
- 【②携帯電話使用フロー】（図表 3）
- 【③ページャー使用フロー】（図表 4）

ハ.【①TAN 生成機使用フロー】におけるチャレンジフォーマットの前提

【①TAN 生成機使用フロー】の図表 2 の Step2 におけるチャレンジのフォーマットに関して、振込先口座番号の下3桁のみか一般的な口座番号の桁数である7桁か、また、送金金額を含めるか否か、によって以下の 4 形態を考える。

【①TAN 生成機使用フロー】におけるチャレンジフォーマットの前提

- 【チャレンジフォーマット１】: 振込先口座番号の下 3 桁のみ
- 【チャレンジフォーマット２】: 振込先口座番号の下 3 桁＋送金金額
- 【チャレンジフォーマット３】: 振込先口座番号 7 桁のみ
- 【チャレンジフォーマット４】: 振込先口座番号 7 桁＋送金金額

ニ. 攻撃者の前提

攻撃者の前提を以下の通りとして考察を行う。

- 攻撃者は、ユーザの PC をマルウェア感染させることが出来、遠隔地から当該 PC を自由に操ることが出来る。ただし、第 2 要素認証機器（TAN 生成機、携帯電話、ページャー）についてはマルウェア感染させることが出来ない。
- 攻撃者にとって、攻撃の成功とは、「攻撃者の口座に対して、ターゲットの口座の資金を送金させること」とする。なお金融機関は、顧客から受け付けた送金指示等の取引については、「取引認証」にて確認出来れば、正当な取引であると認識し、送金を実施するものとする。

(2) Pre-play attack のインターネット・バンキングへの適用

本稿では、EMV 仕様における（「取引認証」への攻撃である）Pre-play attack を、インターネット・バンキング（の「取引認証」）に適用することを考える。ただし、EMV 仕様とインターネット・バンキングとでは取引認証の具体的なプロトコルが大きく異なるため、Pre-play attack の手法をインターネット・バンキングにそのまま適用することは困難である。そこで本稿では、「Pre-play attack のアイデアや攻撃が起こる原因を、インターネット・バンキングの取引に当てはめる」というアプローチをとる。

前章 3.(3)では、Pre-play attack が起こる原因について、以下の通り 2 種類を指摘した。

Pre-play attack が起こる原因　2 種類

原因 A：乱数生成方法の問題（本来は予測不可能な乱数を生成するべきところを、乱数生成器に問題があり、予測が可能となってしまうという問題）

原因 B：プロトコル設計の問題（チャレンジが改ざんされても、検証者はそれを知ることが出来ないという問題）

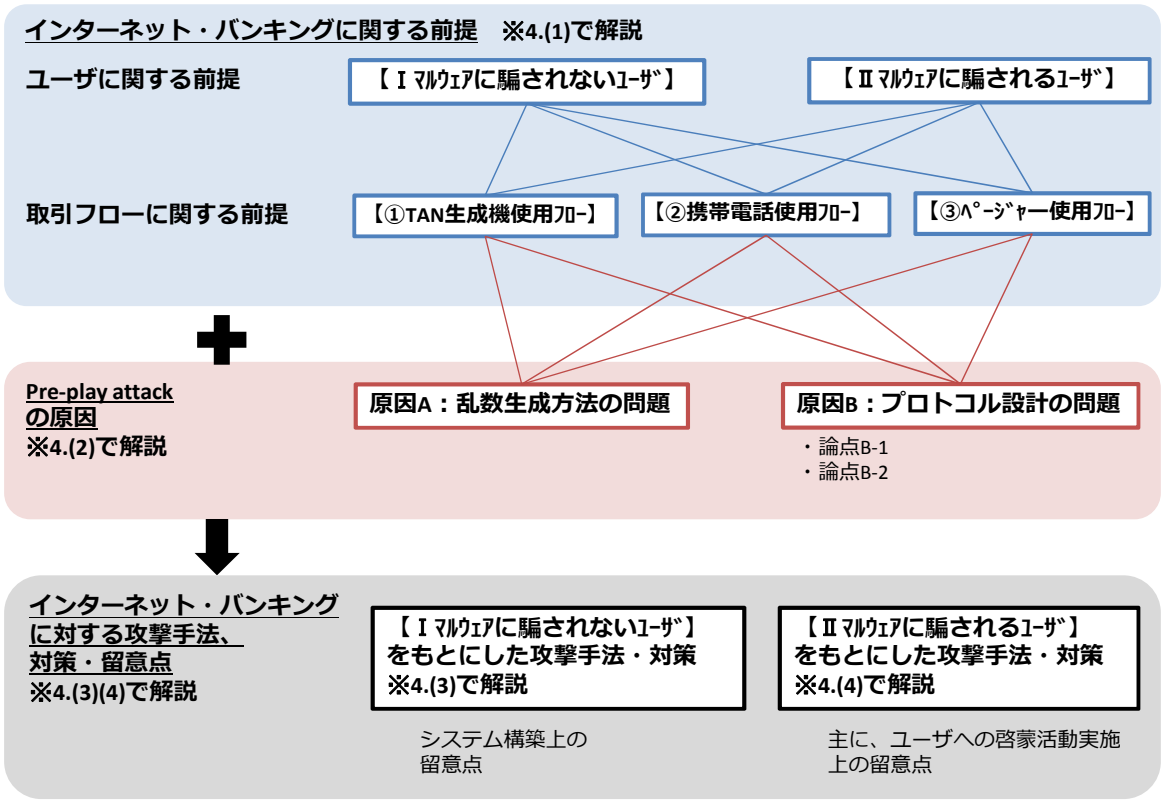
ここで原因 B については、さらにその内容を分解して以下の論点で検討を行う。

原因 B における論点

論点 B-1：攻撃者がチャレンジを改ざんでき（以降、「状況 i：チャレンジ改ざん可能性」と呼ぶ）、かつ、検証者がその改ざんを確認出来ない状況（以降、「状況 ii：確認不能性」と呼ぶ）、は起こり得るか。

論点 B-2：チャレンジの改ざんを行わなくても攻撃が成功する状況が起こり得るか。

インターネット・バンキングにおける前提条件は 4.(1)で述べたように大きく分けて、ユーザ前提 2 個×取引フロー前提 3 個＝6 通り存在する。6 通りそれぞれについて、Pre-play attack が起こる原因 2 種類（原因 A および原因 B）の検討を行う。検討としては、インターネット・バンキングのシステム（6 通り）に対して、Pre-play attack が起こる原因（2 種類）を当てはめ、具体的な攻撃手法を想定して考察するとともに、それに対応した対策を示す（図表 7）。



図表 7. 本章における説明の概念図

なお、【Ⅰマルウェアに騙されないユーザ】をもとにした攻撃手法は、ユーザが十分気をつけていたとしても成立する攻撃である。このため、本前提を基にした攻撃・対策に関する考察は、「システム構築上の留意点」と読み替えることが出来る。

また、【Ⅱマルウェアに騙されるユーザ】をもとにした攻撃手法は、マルウェアに騙されるユーザを前提とした攻撃である。対策としては、「マルウェアに騙されないようにユーザへの啓蒙活動を実施する」ということが中心となる。具体的な騙し方の手口を例示しながら、どのような点に気を付けるようユーザへの啓蒙活動を実施すればよいか、ということを意識しつつ検討を行う。このため、本前提を基にした攻撃・対策に関する考察は、主として「ユーザへの啓蒙活動実施上の留意点」と読み替えることが出来る。

(3) インターネット・バンキングへの Pre-play attack の適用に関する考察（【Ⅰマルウェアに騙されないユーザ】の場合）

本節では、【Ⅰマルウェアに騙されないユーザ】における攻撃手法およびその対策を検討する。なお、本前提は、次節で述べる【Ⅱマルウェアに騙されるユーザ】よりも攻撃者にとって不利な前提となる。このため、本節で成功した攻撃は、次節でも成功することとなる。

イ.【①TAN 生成機使用フロー】を前提とした考察

（原因 A：乱数生成方法の問題について）

原因 A で指摘した、「乱数生成方法の問題」について、本取引フローでは、乱数を使用する場面は見当たらない[11]。従って、原因 A をもとに攻撃が成立することは有り得ない。

（原因 B：プロトコル設計の問題について）

原因 B で指摘した、「チャレンジ自体が改ざんされても、検証者はそれを知ることが出来ない点」を検証するにあたり、4.(2)で述べた 2 つの論点（論点 B-1、論点 B-2）で検討を行う。

≪論点 B-1 について≫

（状況 i：チャレンジ改ざん可能性）に関して、攻撃者がチャレンジを改ざんするためには、ユーザが入力する口座番号や振込先情報等を改ざんする必要があり、【Ⅰマルウェアに騙されないユーザ】の場合には、これは難しい。このため、論点 B-1 の観点では、攻撃が成立することは難しいといえる。

≪論点 B-2 について≫

チャレンジのフォーマットによっては、チャレンジの改ざんを行わなくても各種の攻撃が想定できる。具体的な攻撃手法を、チャレンジフォーマット毎に図表 8 に例示する。

[11] 通信プロトコルの各種レイヤー（例えば、SSL）において乱数生成が行われる可能性があるものの、本稿では通信プロトコルレイヤーの安全性については検討対象外とする（以下同様）。

		チャレンジフォーマットに送金金額情報が	
		なしの場合	ありの場合
口座番号情報が	口座番号下3桁の場合	（チャレンジフォーマット１） **攻撃手法** ①マルウェアが取引指示内容を改ざんした結果、「正規振込先の口座番号」と、「攻撃者の口座番号の下 3 桁」が偶然一致してしまうと攻撃が成功する[12]。 ②ターゲットが攻撃者の口座に対して「正規の手続き[13]」として少額送金の指示を行った場合、マルウェアが送金金額を改ざんしても正当な取引として受理されてしまい攻撃が成功する。	（チャレンジフォーマット２） **攻撃手法** ③左記①同様、正規振込先と攻撃者の口座番号下 3 桁が偶然一致してしまうと、攻撃が成功する。 ④チャレンジフォーマットに送金金額情報が入っており、送金金額の改ざんが出来ないため、左記②と同様の攻撃は成功しない。
	口座番号7桁の場合	（チャレンジフォーマット３） **攻撃手法** ⑤チャレンジフォーマットに口座番号 7 桁が入っており、口座番号を改ざん出来ないため、上記①と同様の攻撃は成功しない。 ⑥上記②同様、ターゲットが攻撃者の口座に対して「正規の手続き」として少額送金の指示を行った場合、マルウェアが送金金額を改ざんしても正当な取引として受理されてしまい攻撃が成功する。	（チャレンジフォーマット４） **攻撃手法** ⑦チャレンジフォーマットに口座番号 7 桁が入っており、口座番号を改ざん出来ないため、①と同様の攻撃は成功しない。 ⑧ チャレンジフォーマットに送金金額が入っており、送金金額の改ざんが出来ないため、②と同様の攻撃は成功しない。

図表 8. チャレンジフォーマット毎の攻撃手法

対策・留意点

- 金融機関はチャレンジのフォーマットに、「振込先口座番号 7 桁＋送金金額」（チャレンジフォーマット４）を利用することが望ましいと考えられる。

[12] 口座番号が偶然一致しなくても、攻撃者の口座が 1,000 口座程度存在すれば、成功する可能性を飛躍的に高めることが出来る。これは、（チャレンジフォーマット２）においても同様。

[13] 例えば、①攻撃者が格安の EC サイトを立ち上げ、ターゲットが商品の代金を支払うために、あくまで「正規の」手続きとしてターゲットが攻撃者に対する送金手続きを行うことや、②攻撃者がターゲットに少額のお金を振込み、ターゲットに対して「間違えて振込んでしまったため、お金を返してほしい」と言って、あくまで「正規の」手続きとしてターゲットが攻撃者に対する送金手続きを行うこと、が考えられる。

ロ.【②携帯電話使用フロー】を前提とした考察

（原因 A：乱数生成方法の問題について）

原因 A で指摘した、「乱数生成方法の問題」について、本取引フローでは、乱数を使用する場面は見当たらない。従って、原因 A をもとに攻撃が成立することは有り得ない。

（原因 B：プロトコル設計の問題について）

原因 B で指摘した点について、イ．と同様に、4.(2)で述べた 2 つの論点（論点 B-1、論点 B-2）で検討を行う。

≪論点 B-1 について≫

本取引フローは、チャレンジ・レスポンス方式ではないが、図表 3 における Step1（取引指示）をチャレンジ、Step2（確認要求）をレスポンスと対応付けた上で、考察を行う。（状況 i：チャレンジ改ざん可能性）に関して、攻撃者は、PC 上のマルウェアを使ってチャレンジを改ざんすることが可能である。ただし、（状況 ii：確認不能性）に関して、チャレンジの生成者とレスポンスの検証者が同一主体であるため（図表 9）、「Step2 がマルウェアにより改ざんされない」という前提のもとでは、ユーザはチャレンジの改ざんを確認できる[14]。このため、本論点では、攻撃が成立することは難しいといえる。

チャレンジ		レスポンス	
内容	生成者	内容	検証者
Step1 の取引指示	ユーザ	Step2 の確認要求	ユーザ

図表 9.【②携帯電話使用フロー】におけるチャレンジとレスポンスの内容

≪論点 B-2 について≫

本取引フローは、チャレンジ改ざんを行わなくても攻撃が成功する方法は見当たらない。このため、本論点では、攻撃が成立することは難しいといえる。

[14] 本稿では検討の対象外とするものの、海外においては、「携帯電話を紛失した」と虚偽の届け出を行うことで、攻撃者がターゲットの携帯電話を入手する攻撃手法（Robertson [2013]）が存在する。このように、インターネット・バンキングのシステム全体のセキュリティレベルが、携帯電話やそれを運営している通信事業者のセキュリティレベルに依存する点は、国内の金融機関においても留意が必要な事項である。また、攻撃者が携帯電話の番号の変更を容易に行えるような環境であっても攻撃が可能となるため、留意が必要である。

ハ.【③ページャー使用フロー】を前提とした考察

（原因 A：乱数生成方法の問題について）

原因 A で指摘した、「乱数生成方法の問題」について、本取引フローにおいては、図表 4 における Step3 の TAN として（サーバで生成した）乱数が使われる場合が考えられる。仮に、サーバでの乱数生成器に問題があり、攻撃者が TAN を予測できる場合には、以下のように攻撃が成功する可能性がある。

攻撃手法

- マルウェア（攻撃者）は、図表 4 の Step1 の取引内容の改ざんを行う。ユーザは、Step2 にて不正な取引であると認識し、Step4 にて取引中止指示をサーバに送信する。しかし、マルウェアはそれを改ざんし、取引確定をサーバに送信する。加えて、マルウェアは Step4 として、予測した TAN をサーバに送信する。TAN に関する予測が当たれば、サーバは Step4 を正当な取引とみなし、攻撃が成功する。

対策・留意点

- TAN を生成する際には、乱数等の、攻撃者の予測が不可能な数字・文字列を用いなければならない。

（原因 B：プロトコル設計の問題について）

原因 B で指摘した点について、イ．と同様に、4.(2)で述べた 2 つの論点（論点 B-1、論点 B-2）で検討を行う。

≪論点 B-1 について≫

本取引フローにおいては、チャレンジ・レスポンス方式ではないが、図表 4 における Step1（取引指示）をチャレンジ、Step2（確認要求）と Step3（TAN）をレスポンスと対応付けた上で、考察を行う。（状況 i：チャレンジ改ざん可能性）に関して、攻撃者は、PC 上のマルウェアを使ってチャレンジを改ざんすることが可能である。（状況 ii：確認不能性）に関して、チャレンジの生成者とレスポンスの検証者が同一主体であるため（図表 10）、「Step2 や Step3 の経路がマルウェアにより改ざんされない」という前提のもとでは、検証者であるユーザはチャレンジの改ざんを確認できる。このため、攻撃が成立することは難しいといえる。

チャレンジ		レスポンス	
内容	生成者	内容	検証者
Step1 の取引指示	ユーザ	Step2,3 の確認要求/TAN	ユーザ

図表 10.【③ページャー使用フロー】におけるチャレンジとレスポンスの内容

≪論点 B-2 について≫

本取引フローにおいては､チャレンジ改ざんを行わなくても攻撃が成功する方法は見当たらない。このため、本論点では、攻撃が成立することは難しいといえる。

(4) インターネット・バンキングへの Pre-play attack の適用に関する考察（【Ⅱマルウェアに騙されるユーザ】の場合）

本節では、【Ⅱマルウェアに騙されるユーザ】における考察を行う。本ユーザ前提では、「マルウェア（攻撃者）が出した指示に騙されてしまうユーザ」を想定しており、攻撃者にとって非常に有利であるため、どのような技術的な対策を施したとしても攻撃が成功する。これは、例えば以下の攻撃手口のように、マルウェアが PC のポップアップ等でユーザに指示を出し、ユーザがその通りに行動すれば、どのような技術的な対策も無効になってしまうからである。

攻撃手法

- 攻撃者が、自口座への送金指示をユーザに行い、ユーザが当該指示に従えば、攻撃が成功する。攻撃者による送金指示の方法としては、例えば、①攻撃者が金融機関になりすまし「振込操作習熟のための練習」と称して自口座への送金指示を出す方法[15] 、②攻撃者が EC サイトに記載されている振込先口座情報を自口座のものに改ざんし、当該 EC サイトで商品を購入したユーザに振込ませる方法、③攻撃者が請求書の内容を改ざんし、請求書を受領したユーザが本来送金する口座とは異なる口座（攻撃者の口座）に送金させられる方法、等が考えられる。

対策・留意点

- 金融機関は、ユーザに対して「他人の指示により振込操作を決して行わない」旨、良く意識してもらう必要がある。

[15] そのような手口は IBM[2014]においても報告されている。

- 金融機関は、ユーザに対して「振込操作を実施するときに振込先の情報に不審な点がないかどうか確認する」旨、良く意識してもらう必要がある。

イ.【①TAN 生成機使用フロー】を前提とした考察

（原因 A：乱数生成方法の問題について）

原因 A で指摘した、「乱数生成方法の問題」について、前節で述べたとおり、本取引フローにおいては、乱数を使用する場面は見当たらない 。従って、原因 A をもとに攻撃が成立することは有り得ない。

（原因 B：プロトコル設計の問題について）

原因 B で指摘した点について、前節と同様に、4.(2)で述べた 2 つの論点（論点 B-1、論点 B-2）で検討を行う。

≪論点 B-1 について≫

（状況 i：チャレンジ改ざん可能性）に関しては、攻撃者（マルウェア）は、PC のポップアップ等を通じて、ユーザに指示を与えることにより、チャレンジ（図表 2 の Step2）の改ざんを行うことが可能である。また（状況 ii：確認不能性）については、図表 11 の通り、チャレンジ生成者とレスポンス検証者が異なるため、レスポンス検証者である金融機関はチャレンジの改ざんを見抜くことができない。

チャレンジ		レスポンス	
内容	生成者	内容	検証者
Step2 の振込先口座番号や振込金額等	ユーザ	Step3、Step4 の TAN（取引認証コード）	金融機関

図表 11.【①TAN 生成機使用フロー】におけるチャレンジとレスポンスの内容

このように（状況 i：チャレンジ改ざん可能性）および（状況 ii：確認不能性）を考慮すると、本論点に関して以下のような攻撃手法[16]が考えられる。

[16] また本稿では検討の対象外とするが、攻撃者が、ユーザの TAN 生成機を一時的に借用したり、盗むなどして、ユーザの TAN 生成機を一時的でも入手できれば、攻撃が成功する。このため「TAN 生成機は、セキュリティ上重要な機器であるため、紛失したら直ぐに届け出るほか、他人に貸したりしない」ということを金融機関はユーザに意識してもらう必要がある。

攻撃手法

- 攻撃者（マルウェア）は、インターネット・バンキングの画面を改ざんすることにより、ユーザに対して「攻撃者に都合の良い TAN」を生成させるように誘導することができ、ユーザがそれに従えば攻撃が成功する[17]。

対策・留意点

- 金融機関はユーザに対して、「TAN 生成機に入力するのは、PC の画面に表示された数字ではなく、自分が意図する振込先の口座番号、金額の情報である」ということを良く意識してもらう必要がある。
- また金融機関におけるシステム構築上の留意点として、画面に表示された数字（振込金額や振込先口座番号）をトークンに入力させるような作りは、上述攻撃を誘発することになりかねないため、避けるべきである。TAN 生成機に「（PC の画面に表示された数字ではなく）自分が意図する振込先の口座番号、金額の情報を入力してください」と表示しておくことも有効な手段の一つである。

≪論点 B-2 について≫

攻撃者は、以下のような手法により、チャレンジの改ざんを行わなくても攻撃を行うことが出来る可能性がある。

攻撃手法

- 攻撃者は、自口座に送金を行うための手続きをユーザに「正規に」実施[18]させた後、同じ送金取引を「不正に」複数回繰り返させる。すなわち、「チャレンジ自体の改ざんは行わないものの、チャレンジ・レスポンスを繰り返させることによって、結果的に送金金額を試行回数倍に引き上げる」、という攻撃手法である。攻撃者が取引を「不正に」複数回繰り返させる手法として例えば次のような方法が考えられる。ユーザは、攻撃者の口座に対してあくまで「正規」取引として図表 2 の Step1～Step4 を実行する。その後マルウェ

[17] 例えば、「画面に表示された数字（実際には攻撃者の口座番号と金額）をトークンに入力してください」とマルウェアがユーザに指示を出し、ユーザがそれに従ってしまえば、攻撃が成功する（高木[2014]においても同様のことが述べられている）。また攻撃者が振込確認画面を改ざんすることにより、ユーザに不信感を与えなくすることも可能となる。

[18] 脚注 13 参照。

アは「先ほどの取引にエラーが発生したため、再度 Step2～Step4 を実行して下さい」とのメッセージを（金融機関からのメッセージと称して）ユーザに出す。ユーザが当該指示に従えば攻撃が成功する。

対策・留意点

- 金融機関はユーザに対して、「TAN の送信（Step4）は細心の注意を持って行う」ということを良く意識してもらう必要がある。
- また金融機関におけるシステム構築上の留意点として、短時間の間にユーザから同内容（金額・口座）の取引要求を受けたら、特に注意を要する（取引を停止する、もしくは、電話等の別手段にて当該取引の正当性を確認する等）必要がある。

ロ.【②携帯電話使用フロー】を前提とした考察

（原因 A：乱数生成方法の問題について）

原因 A で指摘した、「乱数生成方法の問題」について、前節で述べたとおり、本取引フローにおいては、乱数を使用する場面は見当たらない 。従って、原因 A をもとに攻撃が成立することは有り得ない。

（原因 B：プロトコル設計の問題について）

原因 B で指摘した点について、前節と同様に、4.(2)で述べた 2 つの論点（論点 B-1、論点 B-2）で検討を行う。

≪論点 B-1 について≫

本取引フローは、チャレンジ・レスポンス方式ではないが、前節と同様、図表 3 における Step1（取引指示）をチャレンジ、Step2（確認要求）をレスポンスと対応付けた上で、考察を行う。（状況 i：チャレンジ改ざん可能性）に関して、攻撃者（マルウェア）は、チャレンジ（図表 3 の Step1）の改ざんを行うことが可能である。（状況 ii：確認不能性）に関して、図表 9 の通り、チャレンジ生成者とレスポンス

検証者が同一であるものの、以下の攻撃手法[19]により Step2（確認要求）の内容を無効化することが出来る可能性がある。

攻撃手法

- 攻撃者（マルウェア）は、取引指示の内容を改ざんした上で、PC のポップアップ等を通じてユーザに「携帯電話に表示される確認要求の内容（図表 3 の Step2）は間違っています。PC 上の画面に正しい確認要求が表示されましたら、取引確定（Step3）を実行して下さい」といったようなメッセージを出す。ユーザがこの内容を鵜呑みにして、取引確定（Step3）を実行してしまうと、攻撃が成功する。

対策・留意点

- 金融機関はユーザに対して、「PC がマルウェア感染して取引指示が改ざんされたとしても、別経路（Step2）で確認要求が来るため、改ざんが検知できる」という、仕組みを伝えた上で、「別経路（Step2）での確認要求の内容を確認することなく取引確定してはならない」ということを良く意識してもらう必要がある。

≪論点 B-2 について≫

本取引フローにおいても、前項(4)イ．≪論点 B-2≫で議論したものと同様の手法により攻撃が成功する可能性がある。

攻撃手法　対策・留意点

- 前項(4)イ．≪論点 B-2≫と同様の手法および対策[20]。

[19] また、本稿では検討の対象外とするが、攻撃者がユーザの携帯電話を一時的に借用したり、盗むなどして、ユーザの携帯電話を入手できれば、攻撃者は、ブラウザ（PC）と携帯電話の両方の経路を掌握出来るため攻撃が成功する。したがって、「携帯電話は、インターネット・バンキングにおいて重要な機器であるため、紛失したら直ぐに届け出るほか、他人に貸したりしない」ということを金融機関はユーザに意識してもらう必要がある。ここで示した例のほかにも、攻撃者が（金融機関を模した）フィッシングサイトにユーザを誘導し、バンキングアプリと称した Android アプリをインストールさせることにより、携帯電話（スマートフォン）を乗っ取る手口が海外で報告されている（Sancho, Hacquebord, and Link [2014]）。

[20] (4)イ．における「図表 2 の Step1～Step4」、「Step2～Step4」、「TAN の送信（Step4）」を、ここではそれぞれ、「図表 3 の Step1～Step3」、「Step2～Step3」、「取引確定の送信（Step3）」と読み替える。

ハ.【③ページャー使用フロー】を前提とした考察

（原因 A：乱数生成方法の問題について）

原因 A については、前節の(3)ハ．で検討した内容と同様の手法で攻撃が成功する可能性がある。

（原因 B：プロトコル設計の問題について）

原因 B で指摘した点について、前節と同様に、4.(2)で述べた 2 つの論点（論点 B-1、論点 B-2）で検討を行う。

≪論点 B-1 について≫

本取引フローにおいては、(3)ハ．で述べたとおり、チャレンジ・レスポンス方式ではないが、図表 4 における Step1（取引指示）をチャレンジ、Step2（確認要求）と Step3（TAN）をレスポンスと対応付けた上で、考察を行う。（状況 i：チャレンジ改ざん可能性）に関して、攻撃者（マルウェア）は、チャレンジ（図表 4 の Step1）の改ざんを行うことが可能である。（状況 ii：確認不能性）に関して、チャレンジの生成者とレスポンスの検証者が同一主体であるものの、(4)ロ．の≪論点 B-1 について≫で議論したものと同様の攻撃手法により Step2（確認要求）の内容を無効化することが出来る可能性がある。

攻撃手法	対策・留意点
● 前項(4)ロ．≪論点 B-1≫と同様の手法および対策[21]。	

≪論点 B-2 について≫

本取引フローにおいても、前項(4)イ．≪論点 B-2≫で議論したものと同様の手法により攻撃が成功する可能性がある。

攻撃手法	対策・留意点
● 前項(4)イ．≪論点 B-2≫と同様の手法および対策[22]。	

また、以下のような手法によっても攻撃が成功する可能性がある。

---

[21] (4)ロ．における「携帯電話」、「図表 3 の Step2」、「取引確定（Step3）」を、ここではそれぞれ、「ページャー」、「図表 4 の Step2」、「取引確定（Step4）」と読み替える。

[22] (4)イ．における「図表 2 の Step1～Step4」、「TAN の送信（Step4）」を、ここではそれぞれ、「図表 4 の Step1～Step4」、「取引確定の送信（Step4）」と読み替える。

攻撃手法

- マルウェア（攻撃者）は、取引指示の内容を改ざんした上で、PC のポップアップ等を通じてユーザに「ページャーで受信する TAN（図表 4 の Step3）を PC に入力してください」といったようなメッセージを出す。ユーザがこの内容を鵜呑みにして、TAN を PC に入力してしまうと、たとえユーザが取引中止の指示（Step4）をしたとしても、マルウェアはそれを書き換え、TAN とともに送信し、攻撃が成功する。

対策・留意点

- 金融機関はユーザに対して、「TAN（Step3）は取引を確定するときのみに PC に入力する」ということを良く意識してもらう必要がある。

5. おわりに

本稿では、インターネット・バンキングにおける「取引認証」への攻撃手法を示し、その対策手法を検討することにより、インターネット・バンキングの「取引認証」実施時の留意点を示した。

具体的には、IC カード利用システムにおける「取引認証」への新攻撃手法（Pre-play attack）の基本的な考え方を、インターネット・バンキングの「取引認証」に適用することを試みた。攻撃手法を検討するにあたり、ユーザがマルウェアに騙されないという前提をもとにした攻撃手法から、インターネット・バンキングのシステム構築の際に留意すべき事項が明確になった。また、ユーザがマルウェアに騙されるという前提をもとにした攻撃手法から、金融機関がユーザに対して実施する啓蒙活動の留意点等が明確になった。各前提における攻撃手法および対策・留意点は、付録に改めて整理する。

本稿ではインターネット・バンキングにおける「取引認証」の留意点に関して、「セキュリティレベル向上」の観点から技術的視点やユーザへの啓蒙活動の視点で検討を行った。もっとも、金融機関においては「ユーザの利便性」や「コスト」の観点も大きな要素である。例えば、技術的な対策を突き詰めていくと、結果としてユーザの利便性低下につながったり、システム構築のコストが嵩んでしまう、といったことが往々にして考えられる。このため、今後の研究課題としては、「ユーザの利便性」や「コストの観点」も含めた、総合的な観点での検討を行うことが望ましいと考えられる。具体的には、ユーザの利便性を考えると、全ての振込取引に関して「取引認証」を行うのではなく新規先に振込むときや、リスクベース認証に

おいて高リスクと判断された場合にのみ、「取引認証」を実施するという形態も考えられる。また、利便性に配慮し「取引認証」を一部分においてのみ使用するという形態における安全性評価が今後必要であろう。

さらに、持続的なインターネット・バンキングの安全性向上を考えれば、「ユーザの利便性」や「コスト」のみならず、「制度面」、「組織体制面」等、幅広い視野での検討が必要であり、それらの状況の変化にも適切に対応していかなければならない。例えば、「制度面」においては、「携帯電話における SIM ロック解除が原則義務化される」という制度面での状況変化（総務省[2014]）が、結果的に（携帯電話を利用した）インターネット・バンキングのセキュリティレベル低下につながる可能性も考えられる。これは SIM ロック解除義務付けに伴い、ユーザは通信キャリアに依らずスマートフォン端末を自由に選べるようになるということである。それに伴い、今よりもスマートフォン端末の中古市場が活性化する可能性があるが、その際に、OS が改ざんされたり、マルウェアが仕組まれたりした端末が中古市場に流通してしまう可能性が今よりも増加する可能性があり、（当該端末を認証要素として使用する）インターネット・バンキングのセキュリティレベルが結果として現在よりも低下することが懸念される。

ほかの例では、インターネット・バンキングにおける不正の手口が日々高度化している状況下、金融 ISAC[23]等の金融機関同士で不正手口等に関する情報を共有する枠組みや、組織内の CSIRT（Computer Security Incident Response Team）の重要性が一層高まると考えられ、「組織体制面」においても必要に応じて見直しを行うことが重要である。

インターネット・バンキングにおける不正事件の手口は日々巧妙化している。このような状況下、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

[23] Information Sharing and Analysis Center。金融機関によるサイバーセキュリティに関する情報の共有および分析を行い、金融システムの安全性の向上を推進することにより、利用者の安心・安全を継続的に確保することを目的として設立された組織。

付録　本稿で述べた攻撃手法および対策・留意点のまとめ

第 4 章で述べたインターネット・バンキングの「取引認証」について、前提毎の攻撃手法および対策手法をまとめると以下の通りとなる。

項番	ｲﾝﾀｰﾈｯﾄ・ﾊﾞﾝｷﾝｸﾞの前提事項		Pre-play attack の原因	攻撃手法	対策・留意点
	ﾕｰｻﾞ前提	取引ﾌﾛｰ前提	原因		
1	1	1	B	TAN 生成機に入力するチャレンジのフォーマットが、振込先口座番号下 3 桁のみの場合： マルウェアが取引指示内容を改ざんした結果、「正規振込先の口座番号」と、「攻撃者の口座番号の下 3 桁」が偶然一致してしまうと攻撃が成功する。	TAN 生成機に入力するチャレンジのフォーマットに、「振込先口座番号 7 桁＋送金金額」を使用する。
2	1	1	B	TAN 生成機に入力するチャレンジのフォーマットが、振込先口座番号下 3 桁のみの場合： ターゲットが攻撃者の口座に対して「正規の手続き」として少額送金の指示を行った場合、マルウェアが送金金額を改ざんしても正当な取引として受理されてしまい、攻撃が成功する。	
3	1	1	B	TAN 生成機に入力するチャレンジのフォーマットが、振込先口座番号下 3 桁＋送金金額の場合： 項番 1 同様、正規振込先と攻撃者の口座番号下 3 桁が偶然一致してしまうと、攻撃が成功する。	
4	1	1	B	TAN 生成機に入力するチャレンジのフォーマットが、振込先口座番号 7 桁のみの場合： 項番 2 同様、ターゲットが攻撃者の口座に対して「正規の手続き」として少額送金の指示を行った場合、マルウェアが送金金額を改ざんしても正当な取引として受理されてしまい攻撃が成功する。	
5	1	3	A	マルウェア（攻撃者）は、図表 4 の Step1 の取引内容の改ざんを行う。ユーザは、Step2 にて不正な取引であると認識し、Step4 にて取引中止指示をサーバに送信する。しかし、マルウェアはそれを改ざんし、取引確定をサーバに送信する。加えて、マルウェアは Step4 として、予測した TAN をサーバに送信する。TAN に関する予測が当たれば、サーバは Step4 を正当な取引とみなし、攻撃が成功する。	TAN を生成する際には、乱数等の、攻撃者の予測が不可能な数字・文字列を用いなければならない。
6	2	-	-	攻撃者が、自口座への送金指示をユーザに行い、ユーザが当該指示に従えば、攻	金融機関は、ユーザに対して「他人の指示により振込操作

項番	ｲﾝﾀｰﾈｯﾄ・ﾊﾞﾝｷﾝｸﾞの前提事項		Pre-play attack の原因	攻撃手法	対策・留意点
	ﾕｰｻﾞ前提	取引ﾌﾛｰ前提	原因		
				撃が成功する。攻撃者による送金指示の方法としては、例えば、①攻撃者が金融機関になりすまし「振込操作習熟のための練習」と称して自口座への送金指示を出す方法、②攻撃者が EC サイトに記載されている振込先口座情報を自口座のものに改ざんし、当該 EC サイトで商品を購入したユーザに振込ませる方法、③攻撃者が請求書の内容を改ざんし、請求書を受領したユーザが本来送金する口座とは異なる口座（攻撃者の口座）に送金させられる方法、等が考えられる。	を決して行わない」旨、良く意識してもらう必要がある。 金融機関は、ユーザに対して「振込操作を実施するときに振込先の情報に不審な点がないかどうか確認する」旨、良く意識してもらう必要がある。
7	2	1	B	攻撃者（マルウェア）は、インターネット・バンキングの画面を改ざんすることにより、ユーザに対して「攻撃者に都合の良い TAN」を生成させるように誘導することができ、ユーザがそれに従えば攻撃が成功する。	金融機関はユーザに対して、「TAN 生成機に入力するのは、PC の画面に表示された数字ではなく、自分が意図する振込先の口座番号、金額の情報である」ということを良く意識してもらう必要がある。 また金融機関におけるシステム構築上の留意点として、画面に表示された数字（振込金額や振込先口座番号）をトークンに入力させるような作りは、攻撃を誘発することになりかねないため、避けるべきである。 TAN 生成機に「（PC の画面に表示された数字ではなく）自分が意図する振込先の口座番号、金額の情報を入力してください」と表示しておくことも有効な手段の一つである。
8	2	1	B	攻撃者は、自口座に送金を行うための手続きをユーザに「正規に」実施させた後、同じ送金取引を「不正に」複数回繰り返させる（すなわち、「チャレンジ自体の改ざんは行わないものの、チャレンジ・レスポンスを繰り返させることによって、結果的に送金金額を試行回数倍に引き上げる」、という攻撃手法）。攻撃者が取引を「不正に」複数回繰り返させる手法として例えば次のような方法が考えられる。ユーザは、攻撃者の口座に対してあくまで「正規」取引として図表 2 の Step1～Step4 を実行する。その後マルウェアは「先ほどの取引にエラーが発生したため、再度 Step2～Step4 を実行して下さい」とのメッセージを（金融機関からのメッ	金融機関はユーザに対して、「TAN の送信（Step4）は細心の注意を持って行う」ということを良く意識してもらう必要がある。 また金融機関におけるシステム構築上の留意点として、短時間の間にユーザから同内容（金額・口座）の取引要求を受けたら、特に注意を要する（取引を停止する、もしくは、電話等の別手段にて当該取引の正当性を確認する等）必要がある。

項番	ｲﾝﾀｰﾈｯﾄ・ﾊﾞﾝｷﾝｸﾞの前提事項		Pre-play attackの原因	攻撃手法	対策・留意点
	ﾕｰｻﾞ前提	取引ﾌﾛｰ前提	原因		
				セージと称して）ユーザに出す。ユーザが当該指示に従えば攻撃が成功する。	
9	2	2	B	攻撃者（マルウェア）は、取引指示の内容を改ざんした上で、PC のポップアップ等を通じてユーザに「携帯電話に表示される確認要求の内容（図表 3 の Step2）は間違っています。PC 上の画面に正しい確認要求が表示されましたら、取引確定（Step3）を実行して下さい」といったようなメッセージを出す。ユーザがこの内容を鵜呑みにして、取引確定（Step3）を実行してしまうと、攻撃が成功する。	金融機関はユーザに対して、「PC がマルウェア感染して取引指示が改ざんされたとしても、別経路（Step2）で確認要求が来るため、改ざんが検知できる」という、仕組みを伝えた上で、「別経路（Step2）での確認要求の内容を確認することなく取引確定してはならない」ということを良く意識してもらう必要がある。
10	2	2	B	項番 8 と同様。	項番 8 と同様。
11	2	3	A	項番 5 と同様。	項番 5 と同様。
12	2	3	B	項番 8,9 と同様。	項番 8,9 と同様。
13	2	3	B	マルウェア（攻撃者）は、取引指示の内容を改ざんした上で、PC のポップアップ等を通じてユーザに「ページャーで受信する TAN（図表 4 の Step3）を PC に入力してください」といったようなメッセージを出す。ユーザがこの内容を鵜呑みにして、TAN を PC に入力してしまうと、たとえユーザが取引中止の指示（Step4）をしたとしても、マルウェアはそれを書き換え、TAN とともに送信し、攻撃が成功する。	金融機関はユーザに対して、「TAN（Step3）は取引を確定するときのみに PC に入力する」ということを良く意識してもらう必要がある。

※　ユーザ前提１：【Ⅰマルウェアに騙されないユーザ】
ユーザ前提２：【Ⅱマルウェアに騙されるユーザ】
取引フロー前提１：【①TAN 生成機使用フロー】
取引フロー前提２：【②携帯電話使用フロー】
取引フロー前提３：【③ページャー使用フロー】
原因 A：乱数生成方法の問題（本来は予測不可能な乱数を生成するべきところを、乱数生成器に問題があり、予測が可能となってしまうという問題）
原因 B：プロトコル設計の問題（チャレンジが改ざんされても、検証者はそれを知ることが出来ないという問題）

参考文献

井澤秀益・廣川勝久、「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」、IMES Discussion Paper Series、2015 年

大日向隆之、「オンラインバンキング不正送金の手口と対策」、日本銀行金融研究所第 16 回情報セキュリティ・シンポジウム　講演資料、2015 年（http://www.imes.boj.or.jp/citecs/symp/16/ref4_oohinata.pdf）

金融情報システムセンター（FISC）、『平成 26 年版金融情報システム白書』、FISC、2013 年

―――、『平成 25 年版金融情報システム白書』、FISC、2012 年

―――、『平成 24 年版金融情報システム白書』、FISC、2011 年

―――、『平成 23 年版金融情報システム白書』、FISC、2010 年

鈴木雅貴・中山靖司・古原和邦、「インターネット・バンキングに対する Man-in-the-Browser 攻撃への対策『取引認証』の安全性評価」、『金融研究』第 32 巻第 3 号、2013 年、51～76 頁

全国銀行協会、「『インターネット・バンキングによる預金等の不正払戻し』等に関するアンケート結果（平成 17～25 年度）」、全国銀行協会、2015 年 3 月 3 日（http://www.zenginkyo.or.jp/abstract/news/detail/nid/4542/）

総務省、「SIM ロック解除に関するガイドライン」、総務省、2014 年 12 月改正（http://direct.bk.mufg.jp/clouddirect/setsumei.html）

高木浩光、「インターネットバンキング不正送金被害の根本的対策と監督当局の関わり方（金融庁　金曜ランチョン）」、2014 年 9 月 19 日

土居範久・佐々木良一・内田勝也・岡本栄司・菊池浩明・寺田真敏・村山優子、「情報セキュリティ事典」、共立出版、2003 年

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.

IBM, “No silver bullet: Eight ways malware defeats strong security controls,” Thought Leadership White Paper, IBM Software Group, 2014.

M’Raihi, D, J.Rydell, S.Bajaj, S.Machani, and D.Naccache, “OCRA : OATH Challenge-Response Algorithm,” IETF, RFC 6287, 2011.

Robertson, Jordan, “SIM-Card Hackers' Phone Fraud Is Costing Mobile Carriers a Fortune, ” Bloomberg Business, Bloomberg, 2013. (http://www.bloomberg.com/bw/articles/2013-10-17/sim-card-hackers-phone-fraud-is-costing-mobile-carriers-a-fortune)

Sancho, David, Feike Hacquebord, and Rainer Link, “Finding Holes Operation Emmental,” A Trend Micro Research Paper, Trend Micro, 2014.