二経路認証環境下における オンラインバンキングに対し想定される攻撃と対策の提案

栗原浩介[1]　佐々木良一[1]

概要：近年，オンラインバンキングの利用者を狙った不正送金の被害が急増している．急増している理由として Man in the browser 攻撃（以下 MITB 攻撃とする）が挙げられる．MITB 攻撃はオンラインバンキングの利用者のログインを監視し，ログインした後の画面を改ざんする．その後，利用者には巧みに改ざんした画面を表示しながら，裏では不正な振り込みを行う．そのため従来の防御手法では防ぐことが困難である．そこで防御手法として二経路認証というものがある．二経路認証とはパソコンとスマートフォンといった複数の端末を用い，二つの経路で認証を行う方法である．しかしマルウェアの進化に伴い，二経路認証が安全ではない可能性が出てきた．そこで本研究では MITB を基にした二経路認証に対する攻撃手法を検討する．加えてその攻撃手法に対する防御手法を述べ，MITB に対する対策との比較を行う．

Estimated attacks and proposed measures for online banking under two route authentication environment

KOSUKE KURIHARA[1]　RYOICHI SASAKI[1]

1. はじめに

近年，オンラインバンキング利用者を狙った不正送金の被害が急増している．従来の不正送金の手法としては，メールによって偽のWebサイトへ誘導するフィッシングメールや, 通信内容の改ざんを行うMan in the Middle攻撃が挙げられる．これらの攻撃に対して，オンラインバンキングはワンタイムパスワードや二要素認証などの対策を講じてきた. しかし, 2012年後半にMan in the Browser攻撃（以下MITB攻撃とする）が登場したことにより, 不正送金の被害は2012年から2015年にかけて64件・約4800万円から1495件・約30億7300万円[1]まで増加した.

MITB 攻撃とは，ユーザのパソコンに侵入したマルウェアが Web ブラウザを乗っ取り, ブラウザ上の画面を書き換えることで，不正な取引内容をユーザから隠し，不正送金を行う攻撃である. ユーザがアクセスしている Web サイトは正規の Web サイトであることや，ログイン後の Web ブラウザを乗っ取るといった性質のため，ワンタイムパスワードや電子証明書, ID/パスワードなどの従来の方法では対策が不可能である．そこで MITB 攻撃の対策として二経路認証が挙げられる．二経路認証はパソコンとスマホが，同時にマルウェアに感染していないということを前提として安全性を確立している．しかし，スマホを対象としたマルウェアの増加[2]などにより，二経路認証の安全性に問題が出てきた.

本研究では，パソコンとスマホの二端末がマルウェアに感染した場合に，想定される攻撃手法を検討する．加えて二端末が感染した場合に不正送金を，ダミーの情報を利用して検知する方法を述べる.

1 東京電機大学
Tokyo Denki University

2. 二経路認証

二経路認証とは，パソコンとスマートフォン（以下スマホとする）といった複数の端末を用い，パソコンで入力した取引内容と，スマホアプリで表示される取引内容の合致をユーザが確認するといった手順で認証を行う.
以下2.1項, 2.2項, 2.3項にて二経路認証の流れを説明する.

2.1 二経路認証①

本節ではパソコンとスマホがどちらもマルウェアに感染していない場合の二経路認証の流れを以下に説明する.

① ユーザはパソコンに意図した振り込み先口座番号・意図した金額を入力.
② パソコンは意図した振込先口座番号・意図した金額をオンラインバンキングサーバーに振り込み要求を送信.
③ オンラインバンキングサーバーはスマホに取引内容確認を送信.
④ スマホは意図した振込先口座番号・意図した金額を表示.
⑤ ユーザは入力した内容とスマホに表示された内容が合致していたら確認.
⑥ スマホはオンラインバンキングサーバーに振込先口座番号・意図した金額で通信を実行.
⑦ オンラインバンキングサーバーはパソコンに意図した振込先口座・意図した金額で送信
⑧ パソコンは振込先口座番号・意図した金額を表示.

⑨ ユーザは入力した内容とパソコンに表示された内容が合致しているかを確認.

以上が，パソコンとスマホがどちらもマルウェアに感染していない場合の二経路認証の流れとなる.

2.2 二経路認証②

本節ではパソコンがマルウェアに感染し，スマホがマルウェアに感染していない場合の二経路認証の流れを以下に説明する.

① ユーザはパソコンに意図した振り込み先口座番号・意図した金額を入力.
② パソコンに侵入したマルウェアは意図した振り込み先口座番号・意図した金額を不正な振り込み先口座番号・不正な金額に書き換え.
③ パソコンは不正な振込先口座番号・不正な金額をオンラインバンキングサーバーに振り込み要求を送信.
④ オンラインバンキングサーバーはスマホに取引内容確認を送信.
⑤ スマホは不正な口座番号・不正な金額を表示.
⑥ ユーザは入力した内容とスマホに表示された内容が合致していたら確認.
⑦ ユーザは振込要求を中止.

以上が，パソコンがマルウェアに感染し，スマホがマルウェアに感染していない場合の二経路認証の流れとなる.

2.3 二経路認証③

本節ではパソコンがマルウェアに感染していなく，スマホがマルウェアに感染している場合の二経路認証の流れを以下に説明する.

① ユーザはパソコンに意図した振り込み先口座番号・意図した金額を入力.
② パソコンは意図した振込先口座番号・意図した金額をオンラインバンキングサーバーに振り込み要求を送信.
③ オンラインバンキングサーバーはスマホに取引内容確認を送信.
④ スマホに侵入したマルウェアは意図した振り込み先口座番号・意図した金額を不正な振り込み先口座番号・不正な金額に書き換え.
⑤ スマホは不正な振込先口座番号・不正な金額を表示.

以上が，パソコンがマルウェアに感染していなく，スマホがマルウェアに感染している場合の二経路認証の流れとなる.

3. 二経路認証の危険性

二経路認証ではパソコンとスマホが，同時にマルウェアに感染していないということを前提として安全性を確立している. しかし, スマホを対象としたマルウェアの増加や, 2011 年の Zeus in the mobile[3]や 2013 年のペルケレ Lite for Android[4]などの二端末に感染するマルウェアも登場したことにより，二経路認証の安全性に問題が出てきた．これらのマルウェアの特徴としてスマホの SMS を監視することや, 銀行から送られてくる認証用 SMS コードを攻撃者に転送するといったものがある.

3.1 Zeus in the mobile

本節では二端末に感染するマルウェアの一つであるZeus in the mobileの攻撃について説明する.

ユーザのパソコンに何らかの形で侵入したマルウェアは攻撃者のパソコンに,「口座にアクセスするために必要な個人情報」や「口座の所有者の携帯電話番号」を送信する.

攻撃者は先程，窃取した情報を用い，スマホにセキュリティ証明・必要なソフトウェアの更新ファイルをインストールするように仕向ける偽のテキストメッセージとモバイル用Zeusに感染させるリンクをユーザのスマホに送信する.

そこでユーザが騙されて，モバイル用Zeusに接続させるリンクにアクセスすると感染してしまう.

ユーザのスマホがモバイル用Zeusに感染したのを確認した攻撃者は, 攻撃者のパソコンからID・パスワードを用い, ユーザのオンラインバンキング口座にログインを行う.

そして攻撃者は口座番号と金額を入力し振り込み要求を行う．オンラインバンキングはユーザのスマホに口座番号・振り込み金額・ワンタイムパスワードから構成される認証コードを送信するが，ユーザのスマホはモバイル用Zeusに感染しており，認証コードを攻撃者のスマホに送信する．攻撃者は攻撃のスマホに送られてきた認証コードを見て，攻撃者パソコンに認証コードを入力し，振り込みを完了する.

3.2 想定される二端末への侵入経路

PCとスマホにマルウェアが侵入する手段として本研究では以下の侵入経路を検討している.

① ファイル共有アプリを使用.
  I. マルウェアに感染したパソコンからファイルを介してスマホに侵入.
  II. マルウェアに感染したスマホからファイルを介してパソコンに侵入.
② USBケーブルを介してパソコンとスマホを接続.
  I. マルウェアに感染したパソコンからUSBケーブルを介してスマホに侵入.
  II. マルウェアに感染したスマホからUSBケーブルを介してパソコンに侵入.
③ 同一ネットワーク内で侵入.
  I. マルウェアに感染したパソコンからネットワークを介してスマホに侵入.
  II. マルウェアに感染したスマホからネットワークを介してパソコンに侵入.

3.3 目的

想定される二端末への侵入経路と二端末に侵入した過去の攻撃事例から，パソコンとスマホがマルウェアに感染し攻撃に利用される危険性があることが分かる．本研究では，パソコンとスマホの二端末がマルウェアに感染した場合に，想定される攻撃手法を述べるとともに，二端末が感染した場合にも不正送金を検知可能な方式を提案する.

4. 想定される攻撃

4.1 取引内容改ざん型 MITB 攻撃

本研究では, MITB攻撃の手法の一つである取引内容改ざん型MITB攻撃を対象とする.

取引内容改ざん型MITB攻撃とは, ユーザのパソコンに侵入したマルウェアが，ユーザのオンラインバンキングへのログインを察知することで動作する．ログインを察知したマルウェアは，ユーザに偽のオンラインバンキング画面を表示する．マルウェアは，ユーザにリアルタイムで画面を変化させながら必要な情報を入力させ，裏でユーザの入力した振り込み情報を改ざんし，振り込み処理を行う.

4.2 想定される攻撃

本研究で扱う銀行のシステムは取引時に二経路認証を要求するシステムとする．また，パソコンとスマホの二端末には既に協調するマルウェアが侵入しているものとする．想定される攻撃は取引内容改ざん型MITB攻撃を基にし, 二経路認証環境下で実行する攻撃である．攻撃の流れを以下に記す.

① ユーザはパソコンに意図した振り込み先口座番号・意図した金額を入力.

② パソコンに侵入したマルウェアは意図した振込先口座番号・意図した金額を，不正な振り込み先口座番号・不正な金額に書き換え，オンラインバンキングサーバーに振り込み要求を送信.

③ パソコンに侵入したマルウェアは意図した振り込み先口座番号・意図した金額をスマホに侵入したマルウェアに送信.

④ オンラインバンキングサーバーはスマホに取引内容確認を送信.

⑤ マルウェアはスマホ画面に意図した振り込み先口座番号・意図した金額を表示.

⑥ ユーザはスマホ画面に意図した振り込み先口座番号・意図した金額が表示されたので確認を実行.

⑦ スマホはオンラインバンキングサーバーに取引内容確認を送信.

⑧ オンラインバンキングサーバーはパソコンに取引内容完了を送信.

⑨ マルウェアは意図した振り込み先口座番号・意図した金額をパソコン画面に表示.

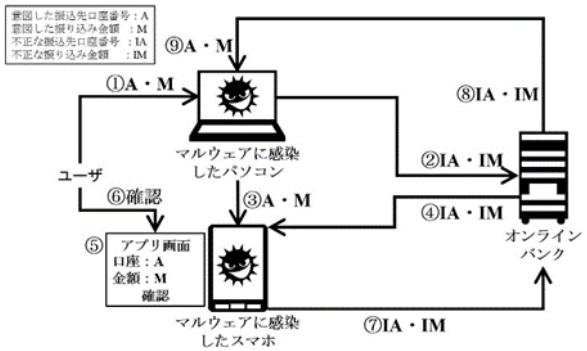

図 1　二端末感染時に想定される攻撃

5. 提案対策手法

5.1 提案対策手法

本研究では，パソコンとスマホがマルウェアに感染した際のマルウェアの取引内容情報の書き換え動作に着目した．ダミー情報を使用しマルウェアの不正書き換え動作を誘引する手法を提案する.

この対策手法を用いた振り込みの流れを説明する。ユーザがダミー情報を使用し，パソコンとスマホにマルウェアが感染していないことをユーザが確認．その後，ユーザが意図した振り込みを実行する.

5.2 ダミー情報の検討

マルウェアの不正書き換え動作を誘引するために必要であるダミー情報として使用可能な情報の検討を行う．ダミー情報として使用可能なものとして条件が2つ挙げられる.

条件1：ユーザと銀行だけが知りえ，マルウェアに知りえない情報.

条件2：銀行に送信される際，マルウェアによる書き換えが行われる情報.

以上，2つの条件を満たすものとして，本研究ではダミー口座番号を使用する.

ダミー口座番号は，実際には存在しない口座番号とし，銀行からユーザに手紙で通知する．ユーザがダミー口座番号で振り込みを行った場合のおおまかな流れを図 2 にて示す．また 5.3 項，5.4 項，5.5 項にて正常な場合，パソコンのみ感染した場合，パソコンとスマホが感染した場合の 3 パターンついて記す.

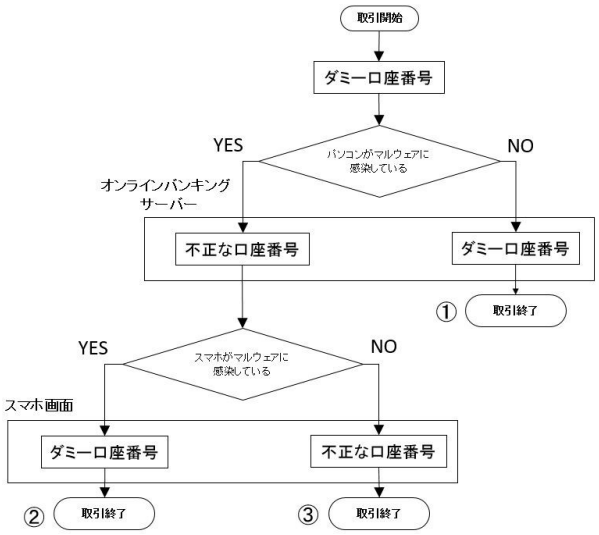

図 2　提案対策手法の流れ

5.3 正常な場合

ユーザが，パソコンとスマホがどちらもマルウェアに感染していない状態で，ダミー口座を使用した場合の動作について以下に記す.

① ユーザはパソコンにダミー口座番号・意図した金額を入力.

② パソコンはオンラインバンキングサーバーに振り込み要求を送信.

③ オンラインバンキングサーバーはパソコンに振込完了を送信.
④ ユーザはスマホには取引内容確認が届かずに，パソコンに振込完了通信が届いたのでパソコンとスマホがどちらも感染していないことに気づく.

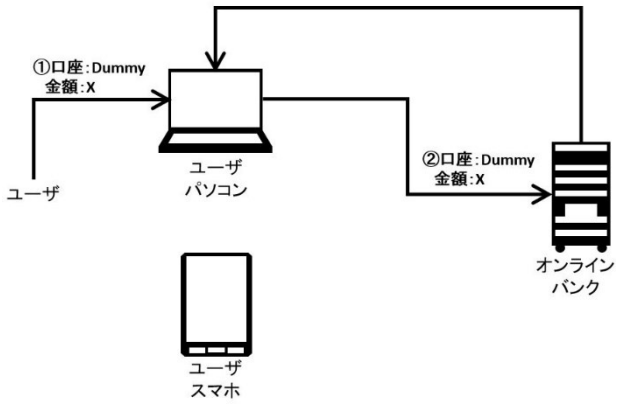

図 3　正常な場合

5.4 パソコンのみ感染した場合

ユーザがパソコンのみがマルウェアに感染した状態で，ダミー口座を使用した場合の動作について以下に記す.

① ユーザはパソコンにダミー口座番号・意図した金額を入力.
② パソコンに侵入したマルウェアは不正な振込先口座番号・不正な金額に書き換え，オンラインバンキングサーバーに送信.
③ オンラインバンキングサーバーはスマホに取引内容確認を送信.
④ スマホに侵入したマルウェアはスマホの画面に不正な振込先口座番号・不正な金額を表示
⑤ ユーザはパソコンがマルウェアに感染していることに気づく.

ユーザはダミー口座を入力したため④が起きないことを認知している．そのためユーザは④が発生した時点で，パソコンがマルウェアに感染していることに気づくことが可能である.

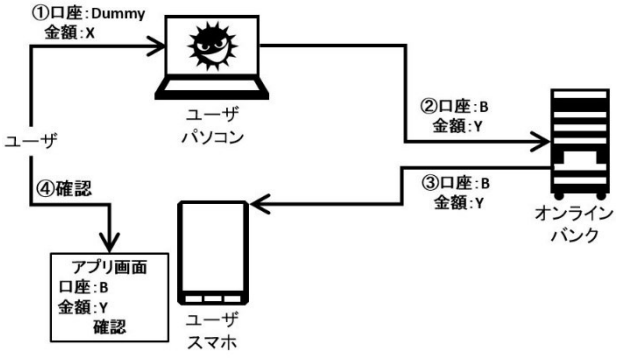

図 4　パソコンのみ感染した場合

5.5 パソコンとスマホが感染した場合

ユーザが，パソコンとスマホがマルウェアに感染した状態で，ダミー口座番号を使用した場合の動作について以下に記す.

① ユーザはパソコンにダミー口座番号・意図した金額を入力.
② パソコンに侵入したマルウェアは不正な振り込み先口座番号・不正な金額に書き換え，オンラインバンキングサーバーに送信.
③ オンラインバンキングサーバーはスマホに取引内容確認を送信.
④ スマホに侵入したマルウェアはスマホ画面にダミー口座番号・意図した金額を表示.
⑤ ユーザはスマホ画面にダミー口座番号・意図した金額表示されたためパソコンとスマホがマルウェアに感染していることに気づく.

オンラインバンキングサーバーはダミー口座番号でない口座番号を受信したので③を実行する.

ユーザはダミー口座番号を入力したため④が起きないことを知っている．そのためユーザはパソコンがマルウェアに感染していることに気づく．加えてスマホ画面にダミー口座番号・意図した金額が表示されているため，スマホがマルウェアに感染していることに気づくことが可能である．なおパソコンのみマルウェアに感染した場合はスマホ画面に不正な振り込み先口座番号・不正な金額が表示される.

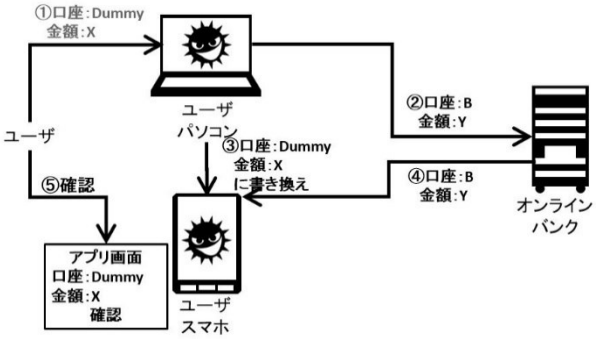

図 5　パソコンとスマホが感染した場合

6. 比較

MITB攻撃に対する防御手法との検討を行う.

① MITB攻撃を防ぐことが可能な既存製品
② パソコンの画面をキャプチャし，スマホに送信することでMITB攻撃を防ぐ事が可能な研究[5]

6.1 関連研究

関連研究として比較項目②で挙げた，パソコンの画面をキャプチャし，スマホに送信することで取引内容を確認しMITB攻撃を防ぐことが可能な研究について記す．これはSCIS2015年に半田富己男と矢野義博がMan in the Bowser攻撃を検出可能なトランザクション手法として発表したものである.

① ユーザはパソコンに意図した振り込み先口座番号・意図した金額を入力.
② パソコンは意図した振り込み先口座番号・意図した金額が入力された画面をキャプチャしてスマホに送信.

③　パソコンは意図した振込先口座番号・意図した金額をオンラインバンキングサーバーに振り込み要求を送信.
④ オンラインバンキングサーバーはスマホに取引内容確認を送信.
⑤ スマホは②で送られたキャプチャと④で送られた取引内容確認の内容が合致しているか確認.
⑥ スマホは合致していたら意図した振込先口座番号・意図した金額を表示.
⑦ ユーザはスマホ画面に意図した振り込み先口座番号・意図した金額が表示されたので確認を実行.
⑧　スマホはオンラインバンキングサーバーに振込先口座番号・意図した金額で通信を実行.
⑨　オンラインバンキングサーバーはパソコンに意図した振込先口座・意図した金額で送信.
⑩　パソコンは振込先口座番号・意図した金額を表示.
ユーザは入力した内容とパソコンに表示された内容が合致しているかを確認.

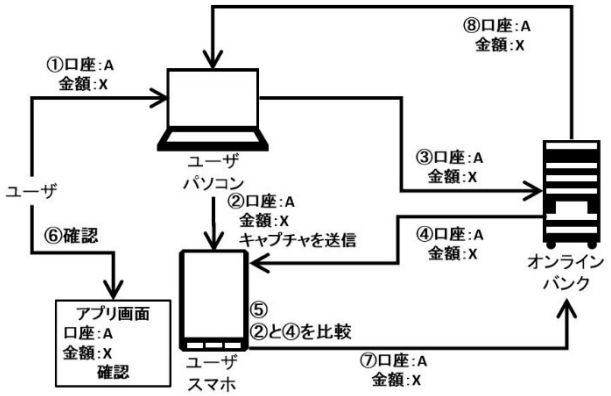

図 6　関連研究

6.2 検討①

想定される攻撃手法を行った場合に，攻撃が成功するのに必要な条件（防御に失敗する事象）を挙げ，それらの事象が発生する確率について考慮を行う．攻撃が成功する確率の上昇に伴い安全性が低下すると考えられる．以下の表1，表2，表3に各項目に対しての検討結果を示す.

表 1　検討結果①

項目	提案対策手法
失敗事象	攻撃者がダミー口座番号を認知に成功
失敗確率	ダミー口座番号を変更する期間や使用頻度に伴い変化
安全性	低～高

表 2　検討結果②

項目	MITB対策ソフト
失敗事象	攻撃者が検知ソフトに検知されず，パソコンの画面を改ざんに成功
失敗確率	マルウェアの進化や検知ソフトのアップデートに伴い変化
安全性	中～高

表 3　検討結果③

項目	関連研究
失敗事象	攻撃者がスマホアプリの画面の改ざんに成功
失敗確率	スマホがマルウェアに感染している→高
安全性	低

6.3 トランザクション認証

スマホ以外の端末を用いる，別の方法としてトランザクション認証[6]というものがある．トランザクション認証とは，計算機端末に口座番号と金額を入力し署名を作成し，パソコンに口座番号と金額,署名を入力するというものだ．本章ではトランザクション認証の流れを以下に記す.
① ユーザが電卓のような機器であるOCRA仕様OTP Tokenに口座番号と金額を入力すると署名が作成される.
② ユーザはパソコンに口座番号と金額，先ほど生成された署名を入力する.
③ パソコンはオンラインバンキングサーバーに口座番号と金額，署名を送信.
④ オンラインバンキングサーバーはOCRA対応OTP認証サーバーに口座番号と金額,ユーザに対応したTokenを送信.
⑤ OCRA対応OTP認証サーバーは口座番号と金額，Tokenに対応した乱数から署名を生成.
⑥ OCRA対応OTP認証サーバーは署名をオンラインバンキングに送信.
⑦ オンラインバンキングサーバーは③で送られた署名と⑥で送られた署名を検証.
⑧ オンラインバンキングサーバーはパソコンに振り込み完了通知を送信.

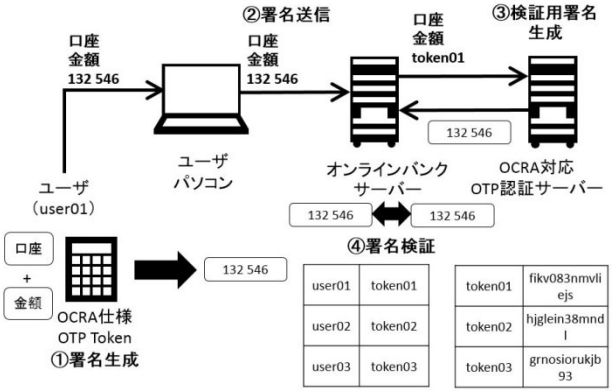

図 7　トランザクション認証

6.4 検討②

トランザクション認証に必要な計算機端末に，ダミー口座番号を生成する機能をつけることで，ダミー口座番号を変更する期間や使用頻度の問題を解決することが可能と考える．これにより提案対策手法の安全性は「低～高」から「中～高」になると考える.

既存製品では，取引内容を改ざんするための前段階である画面の改ざんを防止することでMITB攻撃を防いでいる．しかし，提案対策手法と関連研究では，銀行に対する攻撃

の本質である取引内容の改ざんを防止することでMITB攻撃を防ぐことにより，銀行に対する未知の不正送金の攻撃を防ぐことが可能であると考える.以下の表4に比較結果を示す.

表 4　比較結果

項目	安全性	MITB以外の攻撃
提案対策手法	中～高	○
既存製品	中～高	×
関連研究	低	○

7. おわりに

本研究では，パソコンとスマホの二端末がマルウェアに感染した場合に想定されうる攻撃を述べ，そのような攻撃手法に対する対策手法の提案を行った．今回の比較は銀行で最も重要な項目である安全性のみに対して行ったが，今後はユーザの負担や銀行の導入コストも検討していきたいと考えている

また上記以外にも，スマホ以外の端末を用いず容易にダミー情報を作成する方法や，複数の防御手法を組み合わせる方法，二経路認証以外での方法を検討していくことを課題としたい.

参考文献

[1] 警視庁: 平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について, 警視庁(オンライン) , 入手先<http://www.yomiuri.co.jp/it/security/goshinjyutsu/20150605-OYT8T50305.html>

[2] 総務省: 平成26年版　情報通信白書　最近の情報セキュリティに係る脅威の動向，総務省(オンライン), 入手先<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc143210.html>

[3] KASPERSKY: バンキング型トロイの木馬:モバイルを狙う最大のサイバー脅威，KASPERSKY(オンライン)，入手先<https://blog.kaspersky.co.jp/android-banking-trojans/8915/l>

[4] 読売新聞（YOMIURI ONLINE）：スマホの脅威：モバイル銀行乗っ取りと贋作アプリ，読売新聞(オンライン)，入手先<http://www.yomiuri.co.jp/it/security/goshinjyutsu/20130712-OYT8T00996.html>

[5] 半田富己男, 矢野義博: Man in the Bowser 攻撃を検出可能なトランザクション手法，SCIS2015

[6] 飛天ジャパン株式会社: 不正送金対策～OCRA 仕様 OTP トークンを利用し，MITB による不正送金リスクを低減～，飛天ジャパン株式会社(オンライン)，入手先<http://www.ftsafe.co.jp/solutions/ocra_mitb>