Vol.2015-CSEC-71 No.11
2015/12/4

セキュア SIM を搭載したスマートフォンを利用したトランザクション署名手法の提案

祢宜知孝[†1]　森拓海[†1]　平野貴人[†1]　小関義博[†1]　松田規[†1]　河内清人[†1]
米田健[†1]

概要：Man-in-the-Browser（MITB）攻撃は，インターネットバンキングユーザのブラウザを乗っ取り，ブラウザから入力された取引内容（送金先口座番号や送金額）を改ざんし，ユーザのブラウザにはユーザが入力したとおりの内容を表示させる．そのため，同攻撃は，ユーザにもインターネットバンキングのサービス提供者にも，攻撃を受けていることに気づかれにくい．既存の MITB 対策としてトランザクション署名などがあるが，専用デバイスを必要とするなどの課題がある．本稿では，取引内容改ざん型 MITB 攻撃への対策として，PC に表示された認証情報を埋め込んだ特殊な文字画像をスマートフォンのカメラで撮影し，セキュア SIM で認証情報を取り出す方法を提案する．更に，提案方式の安全性と利便性について考察する．

キーワード：インターネットバンキング，オンライントランザクション，Man-in-the-Browser 攻撃，セキュア SIM，スマートフォン，トランザクション署名

Approach for the method of transaction signing utilizing smartphone with Secure SIM

TOMONORI NEGI[†1]　TAKUMI MORI[†1]　TAKATO HIRANO[†1]
YOSHIHIRO KOSEKI[†1]　NORI MATSUDA[†1]　KIYOTO KAWAUCHI[†1]
TAKESHI YONEDA[†1]

Abstract: A Man-in-the-Browser (MITB) attack is accomplished by hijacking a browser of a victim, manipulating contents of the transaction, such as a beneficiary account number and an amount of remittance, and having the browser display contents as the user inputs. Therefore both user and service provider of the Internet banking are hard to notice it. Several solutions such as transaction signing exist, but they have problems such as they need a dedicated device. This paper proposes a solution by using a smartphone with a secure SIM. And we solve by photographing a particular characters image displayed on a PC's monitor, which includes authentication information, and extracting information from the image with the secure SIM. This paper also discusses the security and usability of this proposed solution.

Keywords: Internet Banking, Online Transaction, Man-in-the-Browser Attack, Secure SIM, Smartphone, Transaction Signing

1. はじめに

近年，インターネットバンキングにおける不正送金の被害が急増し，社会問題化している．2012 年には，被害件数が 64 件，被害額が 4,800 万円であったのに対し，2014 年には，被害件数が 1,876 件，被害額が 29 億 1,000 万円に及んだ[1]．不正送金には，様々な攻撃手法が存在するが，その中でも特に Man-in-the-Browser（MITB）攻撃と呼ばれる攻撃手法（以下，「MITB 攻撃」）が注目を集めている．

MITB 攻撃には，「ID 盗取型 MITB 攻撃」と「取引内容改ざん型 MITB 攻撃」がある[2]．ID 盗取型 MITB 攻撃は，ユーザの PC に感染したマルウェアが，インターネットバンキングへのユーザログイン時にログイン画面を改ざんし，本来は要求されない認証情報（乱数表の全数字など）の入力を要求する偽の画面を表示し，認証情報を盗む攻撃である．一方，取引内容改ざん型 MITB 攻撃は，ユーザの PC に感染したマルウェアが，ブラウザの通信内容を監視し，インターネットバンキングへのアクセスを検知すると，ブラウザの通信を改ざんし，ユーザに攻撃者が望む銀行取引を行わせる攻撃である．取引内容改ざん型 MITB 攻撃は，ユーザにもインターネットバンキングのサービス提供者にも，攻撃を受けていることに気づかれにくいという特徴がある．MITB への対策としてトランザクション署名などが提案されているが，専用の認証トークンデバイスを必要とするなどの課題がある．

本稿では，MITB 攻撃のうち，取引内容改ざん型 MITB 攻撃への対策手法を提案する．本稿で提案する手法は，PC でインターネットバンキングを利用する際の認証トークンデバイスとしてスマートフォンを利用し，PC に表示された認証情報を埋め込んだ特殊な文字画像をスマートフォンのカメラで撮影して，セキュアエレメントを搭載したセキュア SIM[3]で認証情報を取り出す方法である．

本稿の構成は，次のとおりである．2 章で取引内容改ざん型 MITB 攻撃について述べた後，3 章で従来の MITB 攻

†1 三菱電機（株）
Mitsubishi Electric Co.

撃への対策手法を紹介する．4 章で提案方式を説明した後，5 章で提案方式の考察を行い，最後に 6 章で本稿をまとめ，今後の課題を述べる．

2. インターネットバンキングと MITB 攻撃

2.1 インターネットバンキング取引（送金）手順

インターネットバンキングにおける一般的な取引（以下「送金」）手順を述べる[4]．インターネットバンキングの構成要素は，インターネットバンキングサービスを提供する金融機関のサーバ（以下，「銀行サーバ」），及びブラウザがインストールされ，銀行サーバとインターネットを介して接続されたユーザ PC，インターネットバンキングサービスを利用するユーザである．インターネットバンキングの送金は，ユーザがブラウザからインターネットバンキングサービスにログインし，送金のページに移動した後，以下の手順で実行される（図 1）．

① ユーザは，送金情報（送金先の口座番号や送金額）を PC（ブラウザ）に入力する．
② PC は，送金情報を銀行サーバへ送信する．
③ 銀行サーバは，送金内容を確認するため，確認情報（送金先の口座番号や送金額）を PC へ送信する．
④ PC は確認情報を受信し，画面に表示する．
⑤ ユーザは，PC の画面に表示された確認情報が，送金情報（意図する送金情報）と一致していることを確認する．
⑥ ユーザは，送金情報と確認情報が一致している場合には，確定ボタンをクリックする．両情報が一致していない場合には，ユーザは中止ボタンをクリックする．
⑦ PC は，確定／中止を銀行サーバへ送信する．
⑧ 銀行サーバは，確定を受信した場合には，送金処理を実行する．中止を受信した場合には，銀行サーバは送金処理を中止する．
⑨ 銀行サーバは，送金結果を PC へ送信する．
⑩ PC は，受信した送金結果を PC の画面に表示する．
⑪ ユーザは，PC の画面に表示された送金結果を確認する．

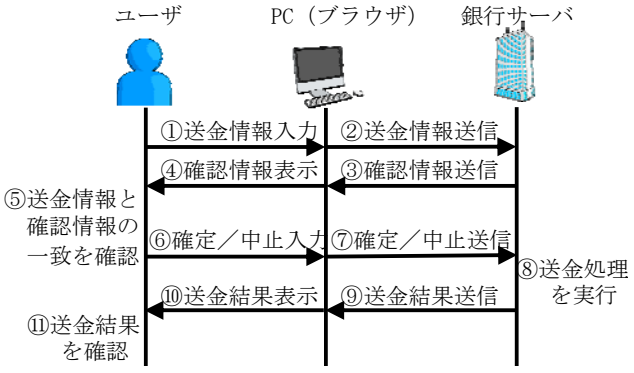

図 1 送金手順

2.2 取引内容改ざん型 MITB 攻撃

取引内容改ざん型 MITB 攻撃は，PC に感染したマルウェアが，ユーザによって入力された送金情報を改ざんすると共に，銀行サーバから送信されてくる確認情報，及び送金結果をユーザによって入力された送金情報に書き換える攻撃である．これにより，ユーザに気づかれることなく，ユーザの意図しない送金が行われる．図 1 に示した送金手順に対する取引内容改ざん型 MITB 攻撃の手順は，以下のようになる（図 2）．

① ユーザは，送金情報（送金先の口座番号や送金額）をマルウェアに感染した PC（ブラウザ）に入力する．
② PC（ブラウザ）に感染したマルウェアは，送金情報を偽の送金情報（以下，「送金情報’」）に書き換え，送金情報’を銀行サーバへ送信する．
③ 銀行サーバは，送金内容を確認するため，確認情報（＝送金情報’）を PC へ送信する．
④ PC は確認情報を受信する．マルウェアは，確認情報をユーザによって入力された送金情報に書き換え，偽の確認情報（以下，「確認情報’」）を画面に表示する（確認情報’＝送金情報）．
⑤ ユーザは，PC の画面に表示された確認情報’が，送金情報（意図する送金情報）と一致していることを確認する．
⑥ ユーザは，送金情報と確認情報’が一致しているため，確定ボタンをクリックする．
⑦ PC は，確定を銀行サーバへ送信する．
⑧ 銀行サーバは，送信情報’に従い送金処理を実行する．
⑨ 銀行サーバは，送金結果を PC へ送信する（送金結果＝送信情報’）．
⑩ PC は，送金結果を受信する．マルウェアは，送金結果をユーザによって入力された送金情報に書き換え，偽の送金結果（以下，「送金結果’」）を PC の画面に表示する（送金結果’＝送金情報）．
⑪ ユーザは，PC の画面に表示された送金結果’を見て，送金情報と同じであることを確認する．

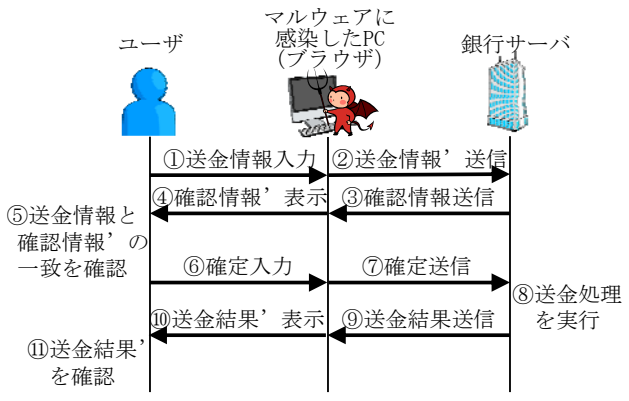

図 2 取引内容改ざん型 MITB 攻撃

3. 従来の MITB 攻撃対策

MITB 攻撃対策として，専用の OCRA(OATH Challenge-Response Algorithm)仕様[5]に準拠したワンタイムパスワード（以下,「OTP」）トークンデバイスを用いて，トランザクション署名を行う方法がある[6][7][8][9]．トランザクション署名とは，送金情報などの処理情報をデジタル署名により暗号化する仕組みである．ユーザは，トークンデバイスに送金情報（送金先の口座番号や送金額）を入力し，トークンデバイスに表示される送金情報の署名を確認情報画面に入力する．トークンデバイスは，専用デバイスであるため，マルウェアに感染することはなく，送金情報の署名が．マルウェアによって偽造されることはない．

しかし，専用のトークンデバイスは，顧客に配布するためのコストが大きい上，送金を行う際に手元に用意し，[9]を除いては送金情報を手入力する必要があり，操作性が悪い．そのため，専用のトークンデバイスの代わりに，導入コストのかからない携帯電話やスマートフォンを用いる方法が提案されている．

桜井[10]は，PC から銀行サーバへ送金情報を送信後，銀行サーバが携帯電話へ暗号鍵を送信する方法を提案している．ユーザは，送金先口座番号を携帯電話へ入力後，送金先口座番号を暗号鍵で暗号化し，暗号化された送金先口座番号を PC の確認画面に入力する．銀行サーバは，暗号化された送金情報を復号し, PC から送信されてきた送金情報と比較することによって，MITB 攻撃を防ぐことができる．ユーザは，送金先口座番号のみを入力するため，送金情報の入力と比べると，操作性は悪くない．

関野ら[11][12]は，PC とスマートフォンなどの端末が同時にマルウェアに感染することを前提に, PC 以外に 2 台以上（n 台）の端末を用い，銀行サーバがn台の端末へ送金確認情報を送信する方法を提案している．ユーザは，n台の端末で送金情報を確認し，マルウェアに感染していない端末から銀行サーバへ送金を指示する．本方式は，n＋1台の内n台の端末がマルウェアに感染しても MITB 攻撃を防ぐことができるが, 複数台の端末を必要とし, 導入コスト（端末購入コスト）がかかる．

半田ら[13]は，送金情報を入力した状態の送金画面を PC でキャプチャし，暗号化したキャプチャ画像を PC からスマートフォンに送ると供に，送金情報を銀行サーバへ送信し，スマートフォンから銀行サーバへ振込情報を問い合わせて，送金情報とキャプチャ画像の内容との一致を確認する方法を提案している．本方式は，送金情報をスマートフォンへ手入力する必要はないが，PC の画面をキャプチャ，暗号化し，送信しなければならず，操作性は良くない．

また，Saisudheer ら[14]は，携帯電話上で公開鍵暗号を用いてユーザが入力した送金情報の電子署名を算出し，算出した電子署名を振込情報と供に銀行サーバへ送信することを提案している．本方式は，送金情報を手入力しなければならず，操作性が悪い．

[11][12]以外の従来の提案は，PC とスマートフォンなどが同時にマルウェアに感染することは無いという前提にたった方式であり，それらが同時にマルウェアに感染し，マルウェアが連携して MITB 攻撃を行うことを想定していない．しかし，近年スマートフォンをターゲットにしたマルウェアが急増し[15]，しかも高度化している[16][17]．したがって，スマートフォンがマルウェアに感染しないという想定は，もはや適当ではない．

従来の提案[10]を例に，携帯電話やスマートフォンがマルウェアに感染し, PC 上のマルウェアと連携した場合には, MITB 攻撃を防ぐことができないことを示す．ユーザによって携帯電話に入力された送金先口座番号が，暗号化される前に，携帯電話に感染したマルウェアによって，PC 上のマルウェアが目的とする不正送金先の口座番号に改ざんされてしまうと，暗号化された送金口座番号は，不正送金先の口座番号となる．そのため，銀行サーバは，暗号化された送金情報を復号し, PC から送信されてきた送金情報と比較すると，両者が一致し，不正送金を実行してしまう．

マルウェアに感染する恐れがないデバイスを用いる方法も提案されている．Weigold[18]らは，USB スティック型のセキュリティデバイス（ZTIC）を用い，ZTIC を SSL/TLS 通信とブラウザの間に介在させることで，通信内容を目視する方法を提案している．本方法では，ユーザは ZTIC を保有し，送金を行う際にわざわざ手元に用意しなければならず，導入コストがかかる．また，高木[19]らは，トランザクション署名を NFC（近距離無線通信）に用いてスマートフォンから電子ペーパへ送信し，送金内容を電子ペーパに表示する方法を提案している．電子ペーパでトランザクション署名を処理するため，MITB 攻撃を防止することが可能である．本方式は，スマートフォンでの送金を想定しており, NFC 機能が普及していない PC には適用できない．

以上のように，従来方式では以下の課題がある．

- OTP トークンデバイスや電子ペーパなど，常に身の回りにないデバイスを用いなければならない．
- マルウェアが携帯電話やスマートフォンに感染し，PC に感染したマルウェアと連携して MITB 攻撃が行われることが考慮されていない．

そこで，本稿では, PC でインターネットバンキングを利用することを前提に，常に身の回りにあるスマートフォンを用いて導入コストを削減し，マルウェアがスマートフォンに感染し，PC に感染したマルウェアと連携しても，利便性を損なわずに MITB 攻撃を防ぐことが可能なトランザクション署名方式を提案する．

4. 提案方式

本稿で提案する方式は，セキュア SIM カードを装着した

スマートフォンを認証トークンデバイスとし, PC の画面に表示された特殊な文字画像をスマートフォンのカメラで撮影して, セキュア SIM カード内で文字画像から認証情報を取り出す方式である．セキュア SIM カードは，耐タンパ性を持ち，データを安全に格納するメモリや，暗号機能などを内蔵したセキュアエレメントを搭載し，セキュアエレメント内で処理を行うことが可能な IC(SIM)カードである．スマートフォン上のアプリケーションは, セキュア SIM カード内の処理に関与できないため，SIM カード内の処理はマルウェアの影響を受けず, 安全に実行することができる．近年のスマートフォンなどには，このセキュア SIM が搭載されている．

図 3 に提案方式における送金の流れを示す．この時，銀行サーバとセキュア SIM カードとの間で, 予め鍵が共有されている．

① ユーザは，送金情報を PC（ブラウザ）に入力する．
② PC は，送金情報を銀行サーバへ送信する．
③ 銀行サーバは，OTP を生成し，送金情報と共に共有鍵で暗号化する．更に，銀行サーバは，暗号化したデータが埋め込まれた，送金情報を表す特殊な文字画像を生成する．特殊な文字画像に関しては，後述する．
④ 銀行サーバは, 特殊な文字画像を確認情報として PC へ送信する．
⑤ PC は確認情報を受信し，特殊な文字画像で示された確認情報を画面に表示する．
⑥ ユーザは，PC の画面に示された確認情報が，意図する送金情報と一致していることを確認し，PC の画面をスマートフォンのカメラで撮影する． PC の画面に表示された確認情報が，意図する送金情報と一致していない場合には, MITB 攻撃よって改ざんされた恐れがあるため，ユーザは中止ボタンをクリックし，⑬以降の流れへ移行する．
⑦ スマートフォンは，撮影画像をセキュア SIM へ転送する．
⑧ セキュア SIM は，撮影画像中の特殊な文字画像を抽出し，文字認識処理により送金情報を取得する．更に，セキュア SIM は，特殊な文字画像に埋め込まれたデータを取り出し，共有鍵で復号して送信情報を取得し，文字認識された送金情報と，復号して取り出された送金情報とを比較する．
⑨ ⑧で比較した結果，両者が一致すれば，復号されたデータから OTP を取得する. 両者が一致しない場合には，MITB 攻撃によって送金情報が改ざんされた恐れがあるため，スマートフォンに認証エラーを表示させて，処理を終了する．認証エラーが表示された場合，ユーザは中止ボタンをクリックし，⑬以降の流れへ移行する．
⑩ セキュア SIM は，OTP をスマートフォンに送信する．
⑪ スマートフォンは，OTP を画面に表示する．
⑫ ユーザは，OTP を PC に入力後，確定ボタンをクリックする．送金を中止する場合には，ユーザは，OTP を入力せずに中止ボタンをクリックする．
⑬ PC は, OTP と確定, 又は中止を銀行サーバへ送信する．
⑭ 銀行サーバは，確定を受信した場合には，送金処理を実行する．中止を受信した場合には，銀行サーバは送金処理を中止する．
⑮ 銀行サーバは，送金結果を PC へ送信する．
⑯ PC は，受信した送金結果を PC の画面に表示する．
⑰ ユーザは, PC の画面に表示された送金結果を確認する．

本提案で特殊な文字画像を用いる理由は，次のとおりである．MITB を防ぐ手段として，従来の対策と同様に 2 端末認証が有効であり，更に認証トークンデバイスには，常に身の回りにあるスマートフォンが適当である．また，2 端末認証を行うためには, 送金先口座番号や送金金額など, 認証を行うための情報を認証トークンデバイスに与える必要があり，ユーザの操作性を良くするために，簡単に操作できるスマートフォンのカメラを用いる．つまり，スマートフォンのカメラで PC の画面から情報を取り込む．スマートフォンに与える情報は，マルウェアが改ざんできず，かつ改ざんされた場合にはユーザと認証トークンデバイスが認識できなければならず，テキストや QR コードは条件を満たさない. QR コードは, 生成ルールが知られており，マルウェアが容易に改ざんできる．しかも，QR コードが改ざんされても, ユーザは QR コードを解釈できないため, 改ざんされていることに気付かない．そこで，ユーザが解釈できる文字画像に秘密のルールで情報を埋め込み，文字画像で送金内容を示すことで，送金内容と埋め込まれた情報を紐付けた．更に，よりセキュリティ強度を高めるために，OTP 方式を採用した上で，文字画像に埋め込む情報は暗号化する．

また，セキュア SIM を用いる理由は，スマートフォン上のアプリケーションの関与を受けずに安全に処理を行う他, 暗号鍵, 及び情報埋め込み規則をセキュア SIM に保存することにより，スマートフォンに感染したマルウェアから守るためである．従来の対策 [10] ～ [14] は，メールや Web(HTTP)の通信や,（ソフト）キーボード入力を必要とするため，スマートフォンの OS やアプリケーションが提供する機能を利用せざるを得ず，スマートフォンに感染したマルウェアの影響を受けてしまう．そのため，従来の対策では，セキュア SIM が有効に機能しない．一方，本提案方式では，カメラ機能もセキュア SIM 上に搭載さえすれば，スマートフォンの OS が提供する機能を使用するのは，画面表示を行う時のみである．スマートフォンに感染したマルウェアが, 画面に表示される OTP を改ざんしても, MITB 攻撃による不正送金を行うことができない．そのため，本提案方式では，セキュア SIM が有効に機能する．

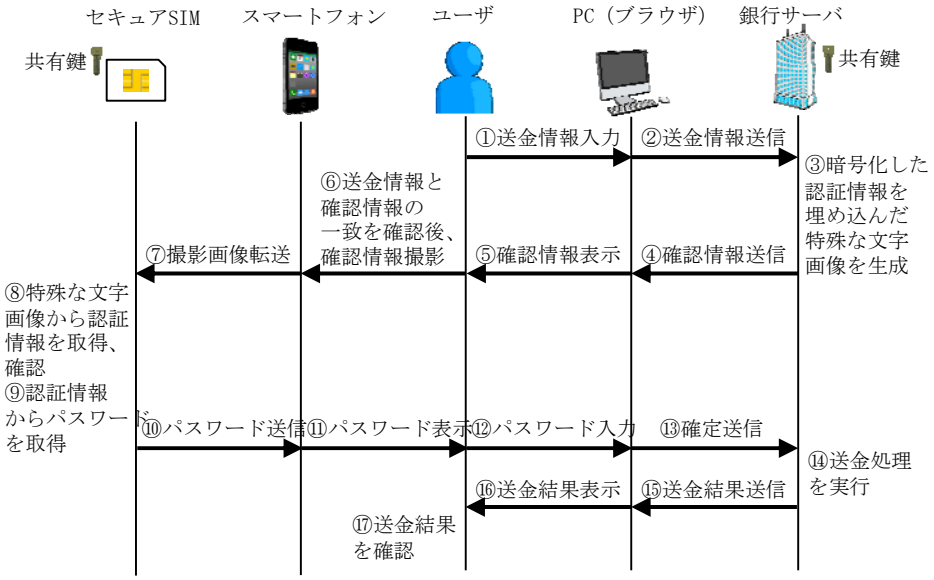

図 3 送金の流れ

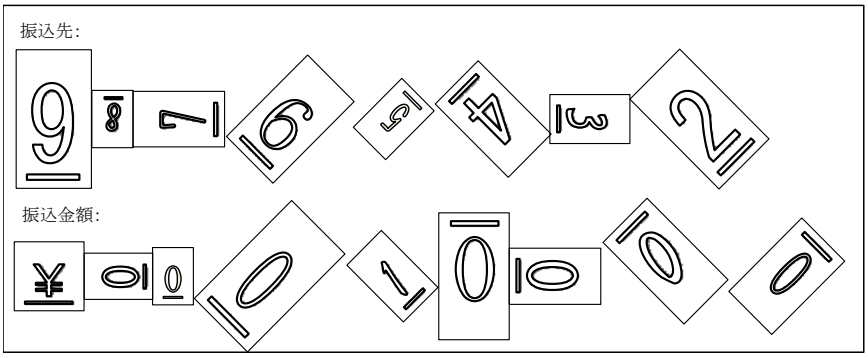

図 4 特殊な文字画像

表 1 情報埋め込み規則

数値	形	値	文字色	値	枠色	値	背景色	値	傾き	値	大きさ	値
0	明朝	00	赤	00	白	00	赤	00	0°	000	0.8 倍	000
	ゴシック	01	青	01	黒	01	青	01	45°	001	1.0 倍	001
	行書	10	緑	10	水色	10	緑	10	90°	010	1.2 倍	010
	教科書	11	黄	11	紫	11	黄	11	135°	011	1.4 倍	011
									180°	100	1.6 倍	100
									225°	101	1.8 倍	101
									270°	110	2.0 倍	110
									315°	111	2.2 倍	111
1	明朝	01	赤	10	白	11	赤	00	0°	001	0.8 倍	111
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

次に，特殊な文字画像（図 4）について説明する．銀行サーバとセキュア SIM カードは，予め表 1 に示すような情報埋め込み規則を共有している．例えば，表 1 において，文字の数値“0”の形（フォント）が明朝体であり，文字の色が赤であり，文字枠の色が白であり，文字の背景色が赤であり，傾きが 0 度であり，大きさが基準とする文字（図 4 の例では“¥”．予め基準とする文字は，決めておく．）の 0.8 倍である場合には，文字画像に埋め込まれている情報は，ビット列“00 00 00 00 000 000”を意味する．この情報埋め込み規則に従い，共有鍵で暗号化された OTP と送金情報のビット列が，文字画像に埋め込まれている．

図 4 の例では，98765432 の口座番号へ 10,000 円を送金する場合を示している．この場合，送金金額（振込金額）の最初の“0”が，形はゴシック体，文字の色は赤，文字枠の色は黒，背景色は黄，傾きは 270 度，大きさは 1.0 倍であれば，同文字画像は，ビット列“01000111110001”を意

味する．銀行サーバは，共有鍵で暗号化された OTP と送金情報のビット列を情報埋め込み規則に従って文字画像中に埋め込み，セキュア SIM が情報埋め込み規則に従ってビット列を文字画像から取り出す．

PC に感染したマルウェアは，情報埋め込み規則を知らないため，特殊な文字画像から情報を取り出すことができない上，文字画像が示す内容と，文字画像に埋め込まれた情報が紐付いているため，意図する文字画像を正しく作り出すこともできない．文字画像が示す内容と，文字画像に埋め込まれた情報が正しく紐付いていない場合，正しく紐付いていないことがセキュア SIM によって検出される．ユーザとセキュア SIM カードを装着したスマートフォンが，送金情報を多重チェックすることにより，MITB 攻撃を防ぐことができる．

5. 考察

提案方式により，PC とスマートフォンの両方にマルウェアが感染し，両マルウェアが連携して MITB 攻撃が行われたとしても，利便性（操作性）を損なわずに不正送金を防ぐことが可能であることを，考察する．セキュア SIM を装着したスマートフォンは，広く普及し，誰もが所有しており，導入コストはかからない．よって，本章では導入コストに関する考察は行わない．

5.1 安全性の考察

本稿では，PC のみがマルウェアに感染した場合と，PC とスマートフォンの両方がマルウェアに感染し，両マルウェアが連携する場合に分け，表 2 を用いてマルウェアにおける情報埋め込み規則と共有鍵に関する知識の有無毎に，安全性を考察する．表 2 は，情報埋め込み規則と共有鍵に関する知識の有無に毎に，マルウェアによる不正操作の可否を示した表である．ここでは，不正送金に成功した場合に，MITB 攻撃が成功したとする．本提案方式では，ユーザがブラウザから入力する情報には，以下がある．

- 送金先口座番号（Ad）
- 送金金額（M）
- OTP（P）

最初に，PC に感染したマルウェアが MITB 攻撃を行い，不正送金を試みる場合を考察する．以下では，$\mathrm{Enc}_K(\mathrm{Ad}, \mathrm{M}, \mathrm{P})$は，Ad と M，P を共有鍵（K）で暗号化した情報を意味する．

いかなる場合においても，マルウェアは，ユーザがブラウザから入力した送金情報（Ad，M）を改ざんし，改ざん後の送金情報（Ad’，M’）を銀行サーバへ送信する（表 2 (1)～(4)）．その後マルウェアは，文字画像に埋め込まれた認証情報（$\mathrm{Enc}_K(\mathrm{Ad'}, \mathrm{M'}, \mathrm{P})$）と，文字画像に示された送金情報（Ad’，M’）を，認証情報（$\mathrm{Enc}_K(\mathrm{Ad}, \mathrm{M}, \mathrm{P})$）に改ざんし，更に同認証情報が組み込まれ，かつユーザの意図する送金情報（Ad，M）を示す文字画像に改ざんする必要がある．

表 2 マルウェアによる情報埋め込み規則・共有鍵の不知/既知と不正操作の可否

情報埋め込み規則		不知		既知	
共有鍵		不知	既知	不知	既知
PC 上のマルウェア	送信情報の改ざん	(1) 可能	(2) 可能	(3) 可能	(4) 可能
	埋め込み情報の取得	(5) 不可能	(6) 不可能	(7) 可能	(8) 可能
	埋め込み情報の復号	(9) 不可能	(10) 不可能	(11) 不可能	(12) 可能
	埋め込み情報の生成	(13) でたらめな情報のみ可能	(14) でたらめな情報のみ可能	(15) でたらめな情報のみ可能	(16) 可能
	埋め込み画像の生成	(17) でたらめな情報のみ可能	(18) でたらめな情報のみ可能	(19) でたらめな情報のみ可能	(20) 可能
スマートフォン上のマルウェア	認証処理への介入	(21) 不可能	(22) 不可能	(23) 不可能	(24) 不要
	OTP の改ざん	(25) 可能	(26) 可能	(27) 可能	(28) 可能

[A] マルウェアが情報埋め込み規則も，共有鍵（K）も知らない場合，PC 上のマルウェアは，情報埋め込み規則も共有鍵も知らないため，文字画像から情報（$\mathrm{Enc}_K(\mathrm{Ad'}, \mathrm{M'}, \mathrm{P})$）を取り出すこともできず（表 2 (5)）埋め込み情報を復号し，OTP（P）を入手することもできない（表 2 (9)）．一方，PC 上のマルウェアは，でたらめな埋め込み情報の生成や，でたらめな埋め込み画像の生成はできる（表 2 (13)，(17)），しかし，セキュア SIM 内での文字認識された送金情報（Ad，M）と，復号して取り出された送金情報との比較で，両者が一致しない．よって，マルウェアによる MITB 攻撃は失敗する．

[B] マルウェアが共有鍵（K）のみを知っている場合，PC 上のマルウェアは情報埋め込み規則を知らないため，文字画像から情報（$\mathrm{Enc}_K(\mathrm{Ad'}, \mathrm{M'}, \mathrm{P})$）を取り出すことができず（表 2 (6)），情報を復号できないため（表 2 (10)），OTP（P）を取り出せない．そのため，PC 上のマルウェアは，でたらめな埋め込み情報しか作成できない（表 2 (14)）．しかも，でたらめな埋め込み画像しか作成できない（表 2 (18)）．したがって，セキュア SIM 内での文字認識された送金情報（Ad，M）と，復号して取り出された送金情報との比較で，両者が一致せず，マルウェアによる MITB 攻撃は失敗する．

[C] マルウェアが情報埋め込み規則のみを知っている場合，

マルウェアは埋め込み情報（$\mathrm{Enc}_K(\mathrm{Ad'}, \mathrm{M'}, \mathrm{P})$）を取得することはできる（表 2 (7)）．しかし，共有鍵を知らないため，埋め込み情報（$\mathrm{Enc}_K(\mathrm{Ad'}, \mathrm{M'}, \mathrm{P})$）を復号できず（表 2 (11)），OTP（P）を取り出せない．そのため，PC 上のマルウェアは，でたらめな埋め込み情報しか作成できず（表 2 (15)），生成する埋め込み画像はでたらめとなる（表 2 (19)）．したがって，セキュア SIM 内での文字認識された送金情報（Ad，M）と，復号して取り出された送金情報との比較で，両者が一致せず，マルウェアによる MITB 攻撃は失敗する．つまり，情報埋め込み規則と共有鍵（K）がマルウェアに知られない限りは，マルウェアによる MITB 攻撃は失敗する．

次に，PC とスマートフォンにマルウェアが感染し，両マルウェアが連携して MITB 攻撃を行い，不正送金を試みる場合を考察する．セキュア SIM は，スマートフォン上のアプリケーションからの関与を受けないため，マルウェアからの関与も受けない．

スマートフォンで撮影された文字画像は，セキュア SIM で処理され，スマートフォンに感染したマルウェアは，PC に感染したマルウェアと連携したとしても，文字画像にアクセスすることができない（表 2 (21)～(23)）．したがって，両マルウェアが連携したとしても，[A]～[C]で考察した状況と変わらず，マルウェアによる MITB 攻撃は失敗する．また，埋め込み規則と共有鍵（K）は，セキュア SIM に格納されているため，スマートフォン上のマルウェアはこれらを入手することもできない．

スマートフォンに感染したマルウェアは，OTP の改ざんは可能であるが（表 2 (25)～(27)），OTP を改ざんしても，正当な送金の妨害をできても，不正送金を行うことはできない. つまり, PC とスマートフォンにマルウェアが感染し，両マルウェアが連携したとしても，情報埋め込み規則と共有鍵（K）がマルウェアに知られない限りは，マルウェアによる MITB 攻撃は失敗する．したがって，PC とスマートフォンが同時にマルウェアに感染した場合には MITB 攻撃が成功してしまう従来の提案に比べ，同時にマルウェアに感染しても MITB 攻撃が成功しない本提案方式は，優れている．

5.2 利便性の考察

文献[20]では，セキュリティの利便性に対する脅威として，行動と判断について以下の 8 項目が提案されている．

【行動】

SUV-A1 : ユーザが，要求されているセキュリティ行動を理解できない

SUV-A2 : ユーザが，正しいセキュリティ行動を行うのに十分な知識を持っていない

SUV-A3 : ユーザが，セキュリティ行動による心理的，又は肉体的な負荷に耐えられない

SUV-A4 : 繰り返しセキュリティ行動を行う場合に，ユーザが心理的，又は肉体的な負荷に耐えられない

【判断】

SUV-C1 : ユーザが，情報に基づく要求されたセキュリティ判断を理解しない

SUV-C2 : システムが，セキュリティ判断に必要とされる十分な情報を提供しない

SUV-C3 : ユーザが，セキュリティ判断を行うことによる精神的な負荷に耐えられない

SUV-C4 : 繰り返しセキュリティ判断を行う場合に，ユーザが精神的な負荷に耐えられない

SUV-A1 と SUV-A2 については，従来の操作に加え，スマートフォンで撮影をし，OTP を入力するのみであり，ユーザがスマートフォンと PC を普通に使用できれば，問題が発生することはない．SUV-A3 と SUV-A4 については，苦労することなく，PC からキーボード入力を行え，スマートフォンで文字画像を撮影できれば，スマートフォンを用意しなければならないという煩わしさは伴うが，問題が発生することはない．

SUV-C1 と SUV-C2 については，入金先口座番号や入金額，OTP が画面表示されるため，問題が発生することはない. PC の画面に表示される入金先口座番号や入金額を示す文字列が特殊な文字画像であるため，判別のしづらさがあるが，判別は可能である．入金元口座番号や入金先口座名を表示すれば，更に問題が発生することがなくなる．

SUV-C3 と SUV-C4 については，文字画像を認識し，入金先口座番号や入金額が一致しているかの確認が，精神的な負荷になるか否かが焦点となる．文字の色や大きさなどが異なるうえ，文字が回転しているため文字判別しづらいが，CAPTCHA のような歪んだ複雑怪奇な文字ですら認識できる人間の文字認識能力を持ってすれば，精神的な負担は小さいと考える．更に，セキュア SIM 内で機械的に情報の一致を確認するため，ユーザは確認に神経質になる必要がなく，精神的な負担は小さい．したがって，本操作を繰り返し行っても, 問題が発生することはないと考えられる．

以上のように，本提案方式は，利便性に対する脅威は小さい．本提案方式は，図 1 示した既存の手順に，スマートフォンを用意し，文字画像をスマートフォンのカメラで撮影し，OTP を入力する手順が増えたのみである．したがって，本提案方式の利便性は，専用デバイスやスマートフォン，携帯電話を用意し，送金情報や OTP などを手入力しなければならない従来の提案方式の多くと比べ, 勝っている．

5.3 埋め込み可能な情報量の考察

振込先銀行番号，振込先店番号，振込先口座番号，振込金額から 256bit のハッシュ値を算出し，このハッシュ値と 8 文字の OTP（64bit）を AES で暗号化することを考える．ハッシュ値と OTP を合わせた 320bit の認証情報をブロック・鍵長 128bit で AES 暗号化すると，384bit の暗号化データが，暗号化された認証情報として生成される．384bit の

暗号化された認証情報を，表 1 に示した情報埋め込み規則に従って文字画像に埋め込むためには，28 文字必要となる．

国内では，通常，銀行番号は 4 桁，店番号は 3 桁，口座番号は 7 桁であり，振込元と振込先それぞれの銀行番号，店番号，口座番号を表すだけで 28 桁となる．したがって，振込元と振込先それぞれの銀行番号，店番号，口座番号だけで，384bit の暗号化された認証情報を埋め込むことができる．そのため，振込金額表示を 8 桁に固定すると，表 1 に示した情報埋め込み規則に従う場合，504bit(63Byte)の情報を文字画像に埋め込むことが可能である．

6. まとめ

本稿では, 取引内容改ざん型 MITB 攻撃への対策として，PC に表示された認証情報を埋め込んだ特殊な文字画像をスマートフォンのカメラで撮影し，セキュア SIM で認証情報を取り出す方法を提案し，安全性と利便性について考察した．表 3 に示すとおり，本提案方式は，導入コストをかけずに, PC とスマートフォンが同時にマルウェアに感染した場合においても，利便性を損なわずに安全性を保つことができる．表 3 は，従来対策と提案方式をマルウェアへの感染対策の有無（○：有，△：不十分，×：無），利便性（操作性）（○：高，△：中，×：低），導入コスト（○：低，△：中，×：高）の視点から比較した結果を示したものである．

表 3 従来対策と提案方式の比較

	マルウェアへの感染対策の有無		利便性(操作性)	導入コスト
	PC	スマートフォン		
提案方式	○	○	○	○
[6][7][8]	○	—	×	×
[9]	○	—	○	×
[10]	○	×	△	○
[11][12]	○	△	×	△
[13]	○	×	△	○
[14]	○	×	×	○
[18]	○	—	○	×
[19]	—	○	○	×

今後の課題としては，セキュア SIM 内に提案方式の処理を行うセキュアエレメントを搭載させることが可能であるかを，検証する必要がある．また，提案方式の利便性に関して，実証実験を行う必要がある．

参考文献

1) 警察庁: 平成 26 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，広報資料
https://www.npa.go.jp/cyber/pdf/H260904_banking.pdf
2) 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，日本銀行金融研究所 金融研究，第 32 巻第 3 号， pp.51-76, 2013
3) Smart Card Alliance: NFC Frequently Asked Questions
http://www.smartcardalliance.org/publications-nfc-frequently-asked-questions/#7
4) 土屋貴史，藤田真浩，高橋健太，加藤岳久，間形文彦，勅使河原可海，佐々木良一，西垣正勝: Man In The Browser 攻撃対策を実現する人間・サーバ間のセキュア通信プロトコル，情報処理学会研究報告 CSEC, Vol. 2015, No. 22, pp. 1-9, 2015
5) OCRA: OATH Challenge-Response Algorithm RFC 6287: Internet Engineering Task Force (IETF) https://datatracker.ietf.org/doc/rfc6287/
6) VASCO Data Security: VASCO Strong Two Factor Authentication – E-signature DIGIPASS Devices
https://www.vasco.com/products/client_products/esignature_digipass/esign.aspx
7) VASCO Data Security: みずほ銀行が，VASCO のトランザクション署名機能を導入しました
http://www.vasco.co.jp/Press/Mizuho_Retail_DP275TS_PR.pdf
8) 飛天ジャパン: MITB 対策 不正送金対策 トランザクション署名 OCRA 仕様 OTP トークン OATH 準拠,
http://www.ftsafe.co.jp/solutions/ocra_mitb
9) SafeNet: eToken 3500 - オンライン詐欺を防止する OTP（ワンタイムパスワード）バンキングトークン
http://www.safenet-inc.jp/multi-factor-authentication/authenticators/one-time-password-otp/etoken-3500-banking-token/
10) 桜井鐘治: 取引認証の改良と安全性・利便性についての考察, 情報処理学会研究報告 CSEC, Vol. 2009, No. 20, pp. 217-222, 2009
11) 関野智啓，古原和邦，今井秀樹: 複数の独立した端末と認証方式を使ったボットウィルス対策，コンピュータセキュリティシンポジウム（CSS2008）, Vol. 2008, No. 8, pp. 863-868 (2008)
12) 関野智啓，古原和邦，今井秀樹: 複数の独立した端末と認証方式を使ったマルウェアに強い命令（電子商取引）方式, 2009 年暗号と情報セキュリティシンポジウム（SCIS2009）, 2009
13) 半田富己男，矢野義博: Man-in-the-Browser 攻撃を検出可能なトランザクション認証手法の提案, 2015 年暗号と情報セキュリティシンポジウム（SCIS2015）, 2015
14) A.Saisudheer and M.Tech: Smart Phone as Software Token for Generating Digital Signature Code for Signing In Online Banking Transaction, International Journal of Computer Engineering Science (IJCES), Vol. 2013, No. 3(12), 2013
15) McAfee: スマートフォンで急増するマルウェアの脅威 - マカフィーセキュリティニュース,
http://www.mcafee.com/japan/home/security/news/027.html
16) Paul Roberts: Zeus Banking Trojan Comes to Android Phones
https://threatpost.com/zeus-banking-trojan-comes-android-phones-071211/75420
17) Symantec Security Response: iBanking: Exploiting the Full Potential of Android Malware
http://www.symantec.com/connect/blogs/ibanking-exploiting-full-potential-android-malware
18) Thomas Weigold, Thorsten Kramp, Reto Hermann, Frank Höring, Peter Buhler, and Michael Baentsch: The Zurich Trusted Information Channel - An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks, Trusted Computing-Challenges and Applications, pp. 75-91 (2008)
19) 高木 浩光，渡辺 創: Man-in-the-Browser の脅威と根本的な解決策，産業技術総合研究所 第 2 回セキュアシンポジウム
https://www.risec.aist.go.jp/files/events/2014/0313-ja/risec-sympo2014-takagi.pdf
20) Audun Jøsang, Bander AlFayyadh, Tyrone Grandison, Mohammed AlZomai, and Judith McNamara: Security Usability Principles for Vulnerability Analysis and Risk Assessment, 23rd Annual Computer Security Applications Conference (ACSAC2007), pp. 269-278 (2007)