IMES DISCUSSION PAPER SERIES

オンライン・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

鈴木雅貴・中山靖司・古原和邦

Discussion Paper No. 2013-J-4

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 2013-J-4
2013 年 3 月

オンライン・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

鈴木雅貴*・中山靖司**・古原和邦***

要　旨

国内のインターネットバンキングにおいて、ログイン後に乱数表のすべての情報等の入力を求める「偽画面」を表示するフィッシング詐欺が昨年後半より発生している。こうした攻撃は、ユーザ PC 内のウイルスが通信内容を盗取・改ざんすることで可能となっており、「Man-in-the-Browser 攻撃」と呼ばれている。同攻撃への対策としては、取引の内容を本人が認証する「取引認証」が海外の一部の金融機関において導入され始めているが、情報セキュリティ研究者の間で取引認証方式の安全性を統一的に評価する枠組みが確立されていないのが実情である。そこで、本稿では、取引認証を用いたインターネットバンキングにおける「Man-in-the-Browser 攻撃」への対策について検討した。具体的には、インターネットバンキングに用いるブラウザとは異なるソフトウエアや端末・ハードウエア（IC カード、携帯電話、USB デバイス等）を用いた取引認証方式についての安全性の考え方を整理・評価し、金融機関が取引認証を導入する際の留意点について分析した。その結果、取引処理の観点からは TAN（Transaction Authentication Number）を利用することにより対策の選択肢・自由度が増えること、システム構成の観点からはインターネットバンキングのブラウザが対策に用いられるソフトウエアや端末・ハードウエアと電気信号的に分離していることが重要であること等がわかった。

キーワード：インターネットバンキング、Man-in-the-Browser 攻撃、取引認証、多端末認証、多重認証、乗っ取り、重要インフラ
JEL classification: L86、L96、Z00

* 日本銀行金融研究所主査（E-mail: masataka.suzuki@boj.or.jp）
** 日本銀行金融研究所企画役（E-mail: yasushi.nakayama@boj.or.jp）
*** 独立行政法人産業技術総合研究所研究グループ長（E-mail: kobara_conf@m.aist.go.jp）

本稿の作成に当たっては、横浜国立大学の吉岡克成准教授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

金融機関は、インターネットバンキングにおける不正な資金移動等の犯罪を防止するため、様々な対策を講じてきた。例えば、偽の金融機関サイトを立ち上げてユーザのアクセスを誘い、ID／パスワード等の認証情報を入力させる、いわゆるフィッシングサイトに対しては、①サーバの正当性の確認を厳格化するための対策として、EV SSL 証明書[1]の導入や、インターネットをパトロールし、発見したフィッシングサイトを速やかに閉鎖させるサービスの利用等を進めてきた。また、フィッシングやキーロガー等のウイルスにより盗取された認証情報（ID／パスワード等）を用いたなりすましに対しては、②インターネットバンキングへのログイン時の本人認証を強化するための対策として二要素認証[2]（乱数表、One-Time-Password 等）の導入をおこなってきた。しかし、最近、こうした対策では防止困難な新たな攻撃が発生している[3]。具体的な攻撃手口はいくつか知られているが、例えば、予め標的型メール等によって密かに PC に感染していたウイルスが通信の状態をモニターし、ユーザがインターネットバンキングを始めたことを検知すると通信に割り込んで、資金移動指図等の通信内容を盗取したり改ざんしたりする攻撃がある。こうした攻撃は PC の Web ブラウザ（以下、単に「ブラウザ」と呼ぶ）の中で人が悪さをしているかのように見えるため「Man-in-the-Browser 攻撃」（以下、「MitB 攻撃」）と総称されている[4]。

こうした MitB 攻撃は、ウイルスの利用を前提としていることから、PC やブラウザをウイルスに感染させないための基本的な対策（ウイルス対策ソフトの利用、OS やブラウザ等へのセキュリティパッチの適用等）は欠かせないが、ウイルス対策ソフトを適切に利用していないユーザの存在や新種のウイルスの存

---

[1] Extended Validation Secure Socket Layer 証明書。企業等の存在確認など、厳格な審査を行ったうえで認証局から発行されため、通常のサーバ証明書よりも信頼性が高いとされる。

[2] 本人認証に用いる要素は、知識（パスワード等）、所持物（IC カード、使い捨てパスワード生成トークン等）、生体（指紋、虹彩等）の 3 種類に大別できる。このうちの 2 種類を併用する場合に二要素認証と呼ばれる。最近ではさらに多くの要素を併用した「多要素認証」という言葉も使われている。

[3] 昨年末の同攻撃による国内での被害は、不正送金が 5 つの金融機関において総額約 1,900 万円（計 14 件）、うち総額約 1,200 万円については不正引出されたことが明らかとなっている（2013 年 1 月 31 日現在、産経新聞[2013]）。もっとも、海外では 72 億円規模の被害も報告されており、今後、国内での被害が拡大していく可能性が高い（McAfee[2012]、警察庁[2012]）。

[4] 典型的には、MitB 攻撃として、資金移動指図をリアルタイムで改ざん・偽造するタイプを指すが、最近では、ブラウザの表示内容を改ざんすることでパスワード等を盗取するタイプ（2.2 節参照）も MitB 攻撃の 1 つとして扱われている。本稿では、両者のタイプを検討対象とする。なお、MitB 攻撃の可能性は、2006 年頃から指摘されている（中山[2006]、Gühring[2007]）。

在を考慮すればウイルス感染を完全に防ぐことはもはや困難であり、このためウイルス感染していても不正取引を防止できる対策が重要になる。

ウイルス感染した PC の利用を前提とした対策としては、ログイン時の本人認証とは別に、取引指図の内容（送金先、金額）を本人が認証するという対策（「取引認証」と呼ばれる）が知られており、研究レベルや製品レベルで多種多様な方式が提案されている。英国の一部の金融機関では既に同対策を導入しており[5]、MitB 攻撃の被害の広がりを鑑みると今後普及していくと見込まれる。しかし、取引認証方式の安全性を統一的に評価する枠組みが確立されていないのが実情である。そこで、本稿では、取引認証の安全性の考え方を整理・評価し、金融機関が導入する際に留意すべき事項について考察する。

以下、本稿では、2 節において MitB 攻撃の概要を述べる。3 節において取引認証方式の分類方法を検討し、4 節において分類された各形態の安全性評価を行う。5 節において金融機関が取引認証を導入する際の留意点について考察する。

2. Man-in-the-Browser（MitB）攻撃と対策

本節では、まず、分析の前提となるインターネットバンキング・サービスのモデルを示す。次に、複数想定される MitB 攻撃のシナリオのうち、不正取引に直接つながる典型的な 2 つのシナリオ（それぞれ「ID 盗取型 MitB 攻撃」、「取引内容改ざん型 MitB 攻撃」と呼ぶ）[6]を説明する。そのうえで、検討対象とする対策について考察する。

2.1 インターネットバンキング・サービスのモデル

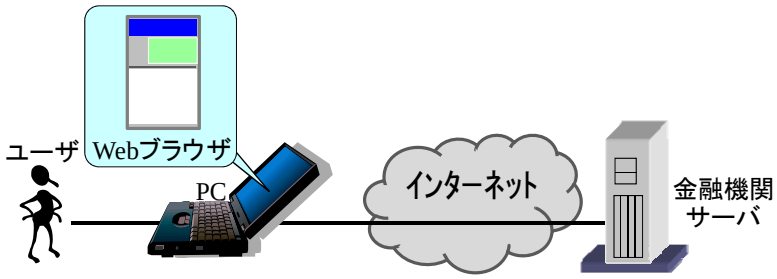
本稿では、インターネットバンキング・サービスを以下の要素からなるモデルとして扱う（図表 1 参照）。

---

[5] 英 Barclays の対策については Barclays[2007, 2012]を、英 NatWest の対策については下記 URL を参照。

http://www.natwest.com/personal/online-banking/g1/banking-safely-online/card-reader.ashx

[6] MitB 攻撃にも様々な形態があり、この他にも、インターネットバンキングにログインする際に偽画面を表示して、取引に必要な認証情報まで入力させた後、ユーザの取引指示の有無にかかわらず裏で不正な取引指図を勝手に行う「取引偽造型 MitB 攻撃」も考えられる。同攻撃に対しては、取引内容改ざん型 MitB 攻撃への対策が有効であることから、本稿では別途議論しない。



図表 1. インターネットバンキング・サービスのモデル

金融機関サーバ：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、「サーバ」と呼ぶ。本稿では、サーバが適切に管理されており、サーバ内のデータが攻撃者に漏洩したり、サーバ内のデータや処理が改ざんされたりすることはないと仮定する。

ユーザ：当該金融機関に口座を保有し、インターネットバンキング・サービスを利用する顧客。同サービスを利用して金融取引を行う際は、PC を用いてサーバにアクセスし、「取引内容」を伝える。本稿では、取引内容とは、「送金先」と「(送金) 金額」を指すこととする。

PC：キーボード、ディスプレイ、インターネット接続機能を有するほか、ブラウザがインストールされている端末。ユーザは、キーボードやディスプレイに表示されたブラウザを通じてサーバとやり取りを行う。

2.2 ID 盗取型 MitB 攻撃

ID 盗取型 MitB 攻撃は、ユーザのログイン時に、ウイルスがなりすまし等の不正取引に必要となる情報を盗取する攻撃である。同攻撃は、国内では 2012 年 10 月下旬から発生が確認されており、「偽画面」や「ポップアップ型フィッシング詐欺」と報道されている（日本経済新聞[2012]）。従来から知られているキーロガー[7]と比較すると、キーロガーは金融機関が要求する情報（ID、パスワード、乱数表の一部の情報等）のみを盗取の対象にできるのに対し、上記の攻撃は金融機関が本来要求しない情報（乱数表のすべての情報等）も盗取の対象にできる点が異なる。同攻撃の典型的な手順は以下のとおりである（図表 2 参照）。

Step 1. 攻撃者は、ユーザの PC にウイルスを感染させる。その後、ウイルスは、ユーザの通信を常時監視する。

Step 2. ユーザは、ブラウザを通じてインターネットバンキングの正規のログインページにアクセスする。

Step 3. ウイルスは、ユーザによる同ページへのアクセスを検知し、ログインペー

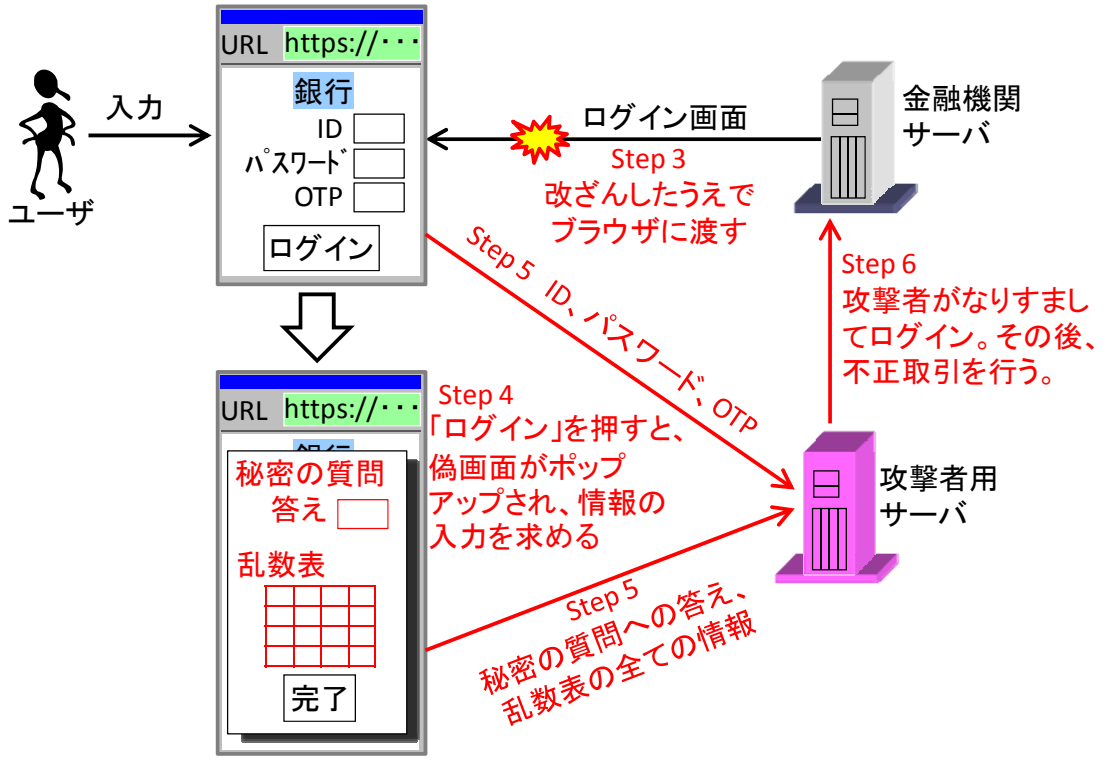
[7] キーボード経由で入力された情報（パスワード等）を盗取し、外部に漏洩するウイルス。

ジのボタンを押した後の動作として、「乱数表のすべての情報や秘密の質問への答えを求めるページ（偽画面）」が表示されるような命令を追加する改ざんを行ったうえで、ブラウザに渡す。

Step 4. ユーザは、ID やパスワードを入力したうえで、同ページにある「ログイン」ボタンを押す。すると、乱数表のすべての情報や秘密の質問への答えの入力を求めるページ（偽画面）が表示されるため、これらの情報も入力する。

Step 5. ウイルスは、Step 4 でユーザが入力した情報を盗取し、外部の攻撃者に送信する。

Step 6. 攻撃者は、Step 5 で盗取した情報を利用してなりすましてログインし、不正取引を行う。



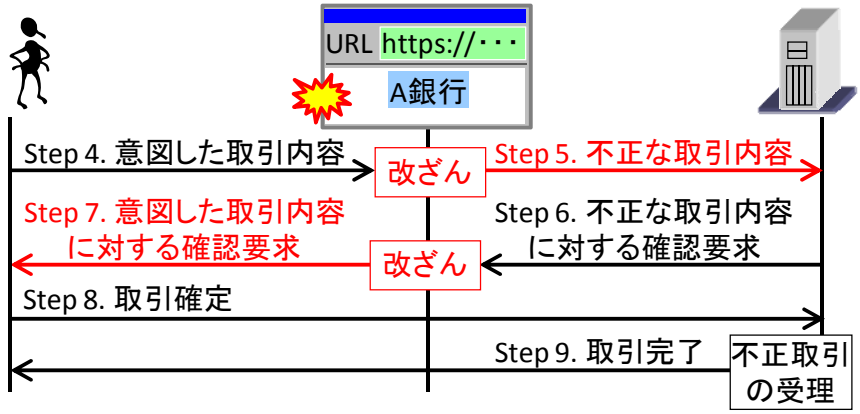
図表 2. ID 盗取型 MitB 攻撃の概要（Step 3~6）

2.3 取引内容改ざん型 MitB 攻撃

取引内容改ざん型 MitB 攻撃は、ウイルスが取引内容（送金先、金額）をユーザの PC 内でリアルタイムに改ざんする攻撃であり、既に海外では発生が確認されている（McAfee[2012]）。同攻撃では、金融機関サーバは改ざんされた取引内容を受理しているにも関わらず、ブラウザにはユーザが入力した取引内容が表示されるため、ユーザは自分が意図する取引が受理されていると誤認する可能

性がある[8]。また、攻撃実施のハードルの観点から 2 つの MitB 攻撃を比較すると、ID 盗取型 MitB 攻撃はサーバから受信する通信内容の改ざんを行っているが、取引内容改ざん型 MitB 攻撃は送受信される通信内容の改ざんを行っており、より高度な攻撃であるといえる。同攻撃の典型的な手順は以下のとおりである（図表 3 参照）。

Step 1, 2.　ID 盗取型 MitB 攻撃の Step 1, 2 と同様。
Step 3. ユーザは、正規ログインページに ID 等を入力し、ログインする。
Step 4. ユーザは、キーボードを用いて取引内容（振込先、金額）を入力する。
Step 5. ウイルスは、入力された取引内容をリアルタイムで改ざんし、サーバに送信する。
Step 6. サーバは、取引内容の確認のために、受信した取引内容を PC に送信する。
Step 7. ウイルスは、サーバから受信した取引内容を改ざんして、ユーザがもともと入力した内容に戻してブラウザに渡す。
Step 8. ユーザは、ブラウザに表示された取引内容が意図したとおりの内容であることを確認し、「取引確定」ボタンを押す。「取引確定」がサーバに送信される。
Step 9. サーバは、「取引確定」を受信し、Step 5 で受信した（改ざんされた）取引内容を受理し、「取引完了」を PC に送信する。「取引完了」がブラウザに表示され、取引処理が終了する。



図表 3.　取引内容改ざん型 MitB 攻撃（Step 4~9）

[8] 本稿では分析対象とはしていないが、インターネットバンキングにおいて、ユーザが取引履歴を閲覧する際、不正取引の発覚を遅らせるために、改ざんがなかったように取引履歴を書き換えて表示する攻撃も MitB 攻撃の 1 つとして指摘されている。

2.4　検討対象とする対策

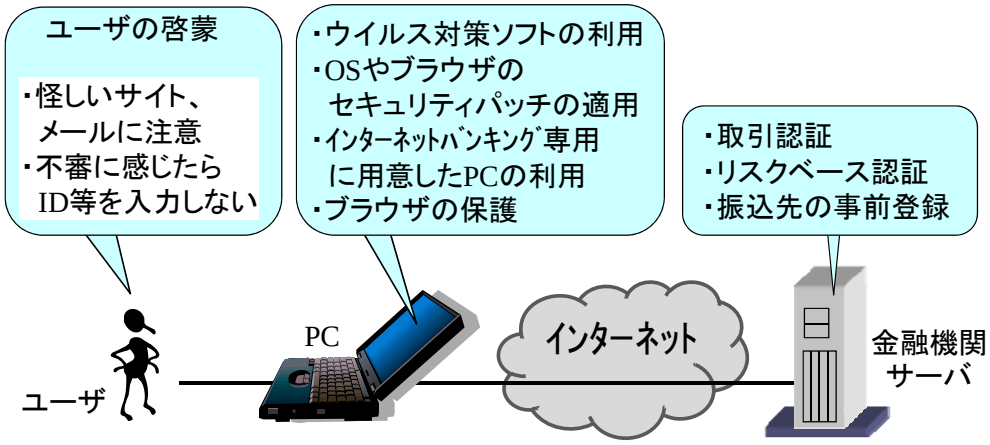
MitB 攻撃はウイルスが活動することを前提としていることから、ウイルスに感染させない対策が有効である。具体的には、①ウイルス対策ソフトの適切な利用、②OS やブラウザ等へのセキュリティパッチの適用、③インターネットバンキング専用として用意した PC の利用、④不審なメールやサイトに関する注意喚起の実施等が挙げられる。しかし、ウイルス対策ソフトやセキュリティパッチを適切に利用していないユーザの存在や新種のウイルスの存在を考慮すると、ウイルスに感染した PC は一定数存在すると考えられることから、本稿ではウイルスに感染していても不正取引を防止可能な対策に注目する。

こうした対策としては、①取引認証、②リスクベース認証、③ブラウザの保護、④送金先の事前登録等が挙げられる。「取引認証」は、サーバが受信した取引内容（送金先、金額）を本人が認証するという対策である。「リスクベース認証」は、サーバが当該取引のパターンを過去蓄積された不正取引のパターンと比較・分析等することで不正取引の可能性（リスク）を数値化し、リスクに応じて認証や取引の扱いを変更する対策である[9]。例えば、(a)リスクが低い場合には取引処理を継続する、(b)リスクがある程度高い場合には追加の認証（改めて本人認証を行う、取引認証を行う等）をユーザに求める、(c)リスクがさらに高い場合には直ちに取引を中止するといった対応が考えられる。「ブラウザの保護」は、PC がウイルスに感染している状況において、インターネットバンキングに関するブラウザの処理を保護することを目的とした技術であり、例えば、同処理を安全な環境に隔離して実行するなどの方法が採られる（フォティーンフォティ技術研究所[2012]）。「送金先の事前登録」は、金融機関窓口や郵送等により予め登録した送金先以外には送金を許可しないというルールに基づく運用である。本稿では、これらの対策のうち（図表 4 参照）、対策の詳細が公開されているものが多くオープンに議論しやすい取引認証を検討対象とする。

ID 盗取型および取引内容改ざん型の MitB 攻撃に求められる取引認証についてみると、まず、ID 盗取型 MitB 攻撃では、いったん盗取した情報を事後的に利用して不正取引を試行しているため、取引時にユーザ本人であってもリアルタイムでしか得られない情報を利用することが対策になる。また、取引内容改ざん型 MitB 攻撃については、本人のログイン後に PC 側でインターネットバンキングの処理を乗っ取ったうえで不正取引を試行しているため、ログイン時の本人認証とは別に、「サーバが受信した当該取引が意図したとおりの取引であることをユーザ本人が認証すること（取引認証）」が対策になる。そこで、本稿では、

[9] リスクの算出に当たっては、本人の普段の取引のパターンと当該取引のパターンの乖離度や、送金先の口座が過去に不正取引に利用されたことがあるか否か等の情報を参考にすることが考えられる。

両攻撃への有効な対策であると考えられる「取引時にリアルタイムで得る情報を利用した取引認証」を検討対象とする。



図表 4. MitB 攻撃に対する様々な対策[10]

3. 取引認証方式の分類方法

本節では、既存の取引認証方式を踏まえ、取引認証方式の分類方法を検討する。

3.1 想定するシステム

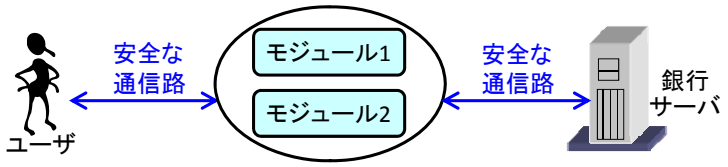
学界で議論されたり、製品として販売されていたりする既存の取引認証方式をみると[11]、ウイルスがブラウザを乗っ取っている状況等を想定し、同一端末上の別のソフトウエアや別の端末・ハードウエア（IC カード、携帯電話、USB デバイス等）といったシステムの構成要素を同ブラウザと併用して取引を行うという形態になっている。ブラウザやこうした構成要素を「モジュール」と呼ぶことにすると、既存方式のアイデアは、複数のモジュールを併用し、少なくとも 1 つのモジュールがウイルスに乗っ取られていなければ不正取引を防止できるというものである。既存方式が利用するモジュールの数は、2 つのものから N 個のものまであるが、モジュールの数が増加するほど処理が複雑になるほか利便性の観点から現実的ではなくなるため、相対的に処理が単純であり実現性が高いと考えられる 2 つのモジュール（それぞれ「モジュール 1, 2」と呼ぶ）を併

[10] 本稿では、MitB 攻撃への対策を、ウイルスに感染させない対策か、ウイルスに感染していても不正取引を防止可能な対策かによって分類したが、対策を導入する際のハードルや利便性の観点からの分類も知られている。具体的には、取引時にユーザに追加の操作を求めるタイプ（「Active 型」と呼ばれる。例：取引認証）と、求めないタイプ（「Passive 型」と呼ばれる。例：ウイルス対策ソフトの利用）である（桜井[2009]、Entrust[2010]）。

[11] 例えば、学会レベルでは Li *at el*.[2011]、Weigold *et al*.[2008]、関野・古原・今井[2008, 2009]、桜井[2009]等が存在するほか、製品レベルでは CA Technologies[2011]、RSA[2010]、石井[2012]等が存在する。

用してサーバと取引処理を行うシステムを想定する（図表 5 参照）。

なお、本稿では、ウイルスがブラウザを乗っ取るという状況に焦点をあてるため、ユーザとモジュール間、モジュールとサーバ間の通信路は盗聴・改ざんされないほか、ユーザやサーバは信頼できると仮定する。



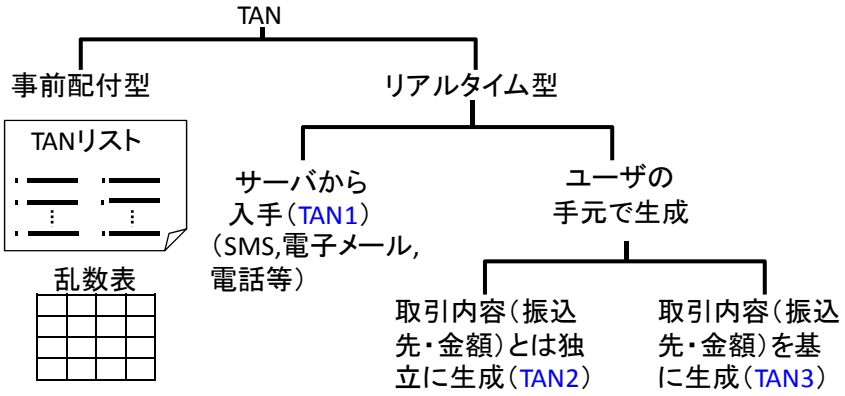
図表 5. 想定するシステム（2 つのモジュールの併用）

3.2 Transaction Authentication Number（TAN）

既存の取引認証方式では、ユーザが各取引を認証するために使い捨て番号「Transaction Authentication Number」（以下、「TAN」）を利用するケースがある。TAN は、取引認証方式の分類方法を検討するうえで重要な概念であり、既存方式では 6~8 桁の数字等として示される。TAN をユーザが入手するタイミングに基づいて整理すると、ユーザがインターネットバンキングを利用するより前に配付されるタイプ（以下、「事前配付型 TAN」）と取引時にリアルタイムで入手するタイプ（以下、「リアルタイム型 TAN」）に大別できる。事前配付型 TAN には、例えば、多数の TAN を印字した紙や乱数表等が含まれる。リアルタイム型 TAN は、サーバが生成したものをモジュールを用いて SMS（Short Message Service）、電子メール、電話等で入手するタイプ（以下、「TAN 1」）と、ユーザの手元にあるモジュールで生成するタイプに分類できる。さらに、手元にあるモジュールで TAN を生成するタイプは、取引内容（振込先、金額）に関係なく独立して生成するタイプ（以下、「TAN 2」）と取引内容に紐づいて生成するタイプ[12]（以下、「TAN 3」）に分類できる（図表 6 参照）。

本稿では、図表 5 に示した 2 つのモジュールを利用するシステムをベースにしつつ、TAN を利用しない方式と利用する方式の双方を検討対象とする。なお、事前配付型 TAN は、偽サイトや ID 盗取型 MitB 攻撃等で盗取された場合にそのまま不正取引に利用されるリスクがあるため検討の対象とはせず、TAN を利用する方式ではリアルタイム型 TAN（TAN 1~3）を取り上げる。

[12] 例えば、取引内容に対するメッセージ認証子やデジタル署名を利用して実現する方法が考えられる。



図表 6. TAN の分類

3.3 想定する取引処理の流れ

インターネットバンキングで金融取引を行うためには、まず、サーバにログインする必要があるが、本稿では、議論を単純化するために、ユーザが正規サーバにログインした後の状況を想定する。本稿で想定する取引処理の流れは以下のとおりである（図表 7 参照）。なお、各ステップにおいてモジュール 1, 2 の一方を使用するが、どちらを利用するかは後述する。

Step 1. ユーザは、モジュールに取引内容（振込先、金額）を入力する。同モジュールは、取引内容をサーバに送信する。

Step 2. サーバは、ユーザに取引内容を確認させるために、受信した取引内容をモジュールに送信する。同モジュールは、取引内容をユーザに表示する。

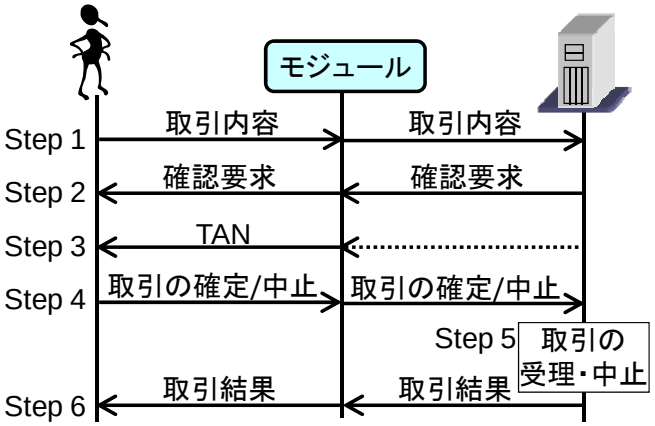
Step 3. TAN 1 を利用する方式の場合、サーバからモジュールに TAN が送信され、ユーザは同モジュールの画面等から TAN を入手する。TAN 2, 3 を利用する方式の場合、ユーザはモジュールのボタン等を使って TAN の生成を指示し、生成された TAN を同モジュールの画面等から入手する。なお、TAN を利用しない方式では、Step 3 を省略する。

Step 4. ユーザは、Step 2 において表示された取引内容を確認し、意図した内容であれば「取引確定＋TAN」をモジュールに入力する。意図した内容でなければ「取引中止」を入力する。同モジュールは、入力された情報をサーバに送信する。なお、TAN を利用しない方式では「取引確定＋TAN」の代わりに「取引確定」を入力・送信する。

Step 5. サーバは、「取引確定＋TAN」を受信した場合には、TAN の検証を行う。TAN の検証結果が合格の場合には、当該取引を受理し、「取引受理」をモジュールに送信する。TAN の検証結果が不合格の場合、または、「取引中止」を受信した場合には、当該取引を中止し、「取引中止」をモジュールに送信する。なお、TAN を利用しない方式では TAN の検証は行わず、「取

引確定」を受信した場合には、当該取引を受理する。

Step 6. モジュールは、受信した取引結果（取引受理、または、取引中止）をユーザに表示し、取引処理を終了する。



図表 7. 想定する取引処理の流れ

3.4 取引認証方式の分類

想定するシステム（図表 5 参照）における取引認証方式は、TAN の利用の有無や取引処理の各ステップにおいて使用するモジュールによって分類可能である（以下、「取引処理に基づく分類」）。また、システム構成の観点からも分類可能である（以下、「システム構成に基づく分類」）。以下では、それぞれの分類方法について説明する。

3.4.1 取引処理に基づく分類

取引認証方式は、取引処理において TAN を利用するか否かにより分類可能である。まず、TAN を利用しない方式については、取引処理の Step 1, 2, 4, 6 のそれぞれにおいてモジュール 1, 2 のどちらを利用するかにより分類可能である。簡単のために Step 1 はモジュール 1 を利用すると定めると、図表 8 (a)に示す 8 個の形態（A1~8）に分類される。一方、TAN を利用する方式についても、取引処理の Step 1~4, 6 のそれぞれにおいてモジュールのどちらを利用するかにより分類可能であり、TAN を利用しない方式と同様に考えれば、まず、図表 8 (b)に示す 16 個の形態（B1~16）に分類される。さらに、利用する TAN のタイプ（TAN 1~3）により、48 個の形態に細分化できる。

	形態							
	A1	A2	A3	A4	A5	A6	A7	A8
Step 1	1	1	1	1	1	1	1	1
Step 2	2	1	2	2	1	1	2	1
Step 4	2	2	1	2	1	2	1	1
Step 6	2	2	2	1	2	1	1	1

(a) TAN を利用しない方式の形態

	形態															
	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
Step 1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Step 2	2	1	2	2	2	1	1	2	1	2	2	1	1	1	2	1
Step 3	2	2	1	2	2	1	2	1	2	1	2	1	1	2	1	1
Step 4	2	2	2	1	2	2	1	1	2	2	1	1	2	1	1	1
Step 6	2	2	2	2	1	2	2	2	1	1	1	2	1	1	1	1

(b) TAN を利用する方式の形態

（備考）セル内の数字（「1」または「2」）は、各ステップにおいて使用されるモジュール（1 または 2）を表す。

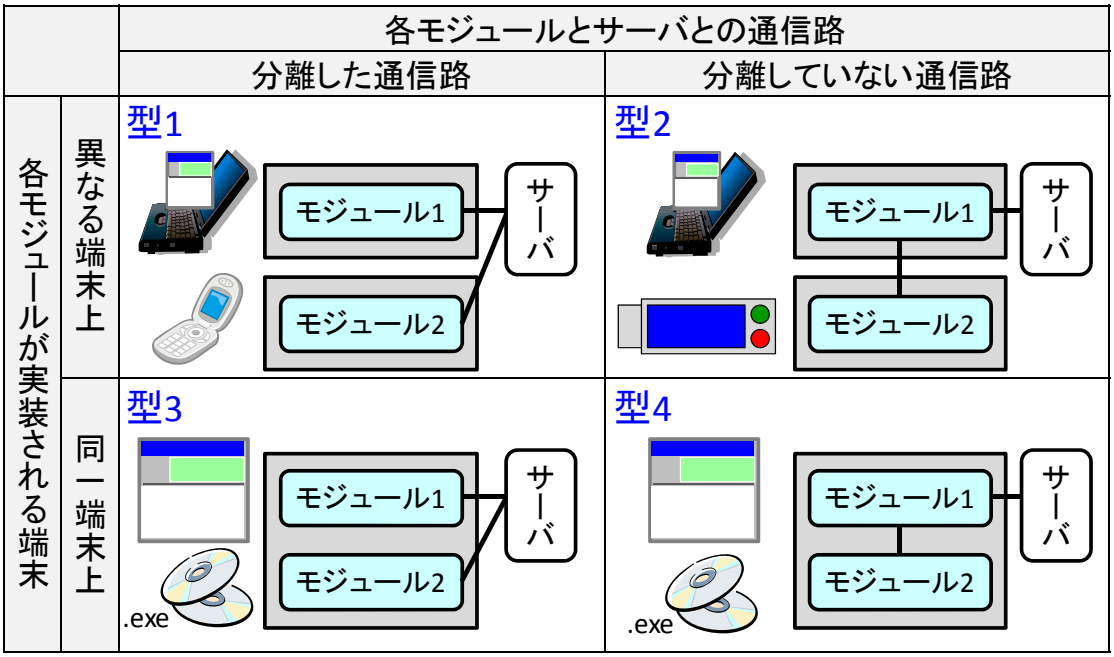
図表 8. 取引処理に基づく分類

3.4.2 システム構成に基づく分類

既存の取引認証方式をみると、1 台の PC 内にブラウザと別の専用ソフトウエアを用意しこれらを併用するタイプと、PC（のブラウザ）と別の端末（同 PC に接続された USB デバイス、携帯電話、IC カード等）を併用するタイプが存在する。こうした事例を踏まえると、システム構成として、2 つのモジュールが同一の端末上に実装されているか否かにより分類可能である。

また、①PC と携帯電話を併用するタイプと、②PC と同 PC に接続された USB デバイスを併用するタイプを、利用する通信路の独立性の観点から比較すると、①では各モジュールとサーバとの通信路が分離しているのに対し、②では一方のモジュール（PC）を経由しなければ他方のモジュール（USB デバイス）がサーバと通信できず通信路が分離していないという差異があることがわかる。これを踏まえると、各モジュールとサーバとの通信路が分離しているか否かによっても分類可能である。

これらの 2 つの観点から、取引認証方式は図表 9 に示す 4 個の形態（型 1~4）に分類できる。



（備考）図表中のブラウザ、携帯電話、USB デバイス等のイラストは、各モジュールの例示である。

図表 9. システム構成に基づく分類

3.4.3 取引認証方式の分類の全体像

取引処理に基づく分類とシステム構成に基づく分類を組み合わせることで、取引認証方式は図表 10 のように分類できることがわかる。

		取引処理に基づく分類			
		TANなし	TAN利用		
			TAN 1	TAN 2	TAN 3
		A1~8	B1~16	B1~16	B1~16
システム構成に基づく分類	型1				
	型2		全224通り		
	型3				
	型4				

図表 10. 取引認証方式の分類の全体像

4. 取引認証方式の安全性評価

本節では、取引認証方式の安全性評価の現状を述べたうえで、取引処理に基づいて分類された各形態とシステム構成に基づいて分類された各形態についてそれぞれ安全性評価（それぞれ「評価 1, 2」と呼ぶ）を行う。

4.1　取引認証方式の安全性評価の現状

取引認証方式の安全性評価についての研究動向をみると、MitB 攻撃を明確に定義しないまま、ウイルス対策ソフトの利用や取引認証等のさまざまな対策を取り上げたうえで、各対策の効果の有無を示している文献はあるが（Entrust [2010]）、複数の方式を同じ枠組みにより統一的に整理・評価している研究等の文献はほとんどないのが実情である。

4.2　評価 1：取引処理に基づいて分類された形態の安全性評価

取引処理に基づいて分類された各形態について、MitB 攻撃による不正取引が成立するか否かを評価する。まず、攻撃者の能力や攻撃方法を定め、そのうえで攻撃の成否を示す。

4.2.1　想定する攻撃者

本評価では、不正取引により不正な利益を得ることを目的とする攻撃者を想定する。同攻撃者は、以下の 2 つの能力を有すると仮定する。

能力 1: ウイルスにより、モジュール 1 またはモジュール 2 のいずれかを乗っ取ることが可能（一方のみを乗っ取ることを想定）。

能力 2 : ウイルスを用いて、乗っ取ったモジュールが扱う情報を盗取・改ざんすることが可能。

情報の盗取・改ざんについて補足すると、モジュールは、ユーザやサーバと安全な通信路を用いて通信するため、攻撃者は通信路上では盗聴・改ざんはできないとする。ただし、能力 2 では、攻撃者がモジュールを乗っ取った場合には、当該モジュール内で処理される情報を盗聴・改ざんできることを想定している。

次に、攻撃成功の条件について考察する。ユーザが取引中または取引後に不正取引を検知し、送金先の口座の凍結を金融機関に依頼するケースが考えられる。しかし、口座の凍結前に攻撃者が振込先の口座から現金を引き出すことができれば、攻撃者の目的は達成されたといえる。そこで、本稿では、ユーザが不正取引を検知したか否かに関わらず、取引処理の流れの Step 5 においてサーバが不正取引を受理した場合に攻撃成功とする。

4.2.2　攻撃の手順

攻撃者は、Step 1~4, 6 で利用される各モジュールを乗っ取った場合に（以下では「ステップを乗っ取る」と表現する）、以下の操作を行う（図表 11 参照）。

Step 1 を乗っ取った場合 : ユーザが入力した取引内容を、ウイルスは不正な内容に改ざんし、サーバに送信する。なお、Step 1 を乗っ取ることができない場

合には、攻撃が成功しないことは自明であるため、ウイルスは攻撃を中止する。以下では、Step 1 の乗っ取りを前提とする。

Step 2 を乗っ取った場合：ウイルスは、サーバから受信した取引内容をユーザが入力した内容に改ざんしたうえでユーザに表示する。なお、Step 2 が乗っ取られていない場合には、ユーザは攻撃を検知可能である。

Step 3 を乗っ取った場合：ウイルスは、サーバからの TAN を不正に入手する（TAN 1 の場合）、または、TAN を不正に生成する（TAN 2, 3 の場合）。なお、TAN 3 の場合には、ウイルスは不正な取引内容（振込先、金額）に対応した TAN を生成する。

Step 4 を乗っ取った場合：

（TAN を利用しない形態のケース）ユーザの入力が「取引確定」の場合、ウイルスはそのままサーバに転送する。ユーザの入力が「取引中止」の場合、ウイルスは「取引確定」に改ざんしたうえでサーバに送信する。

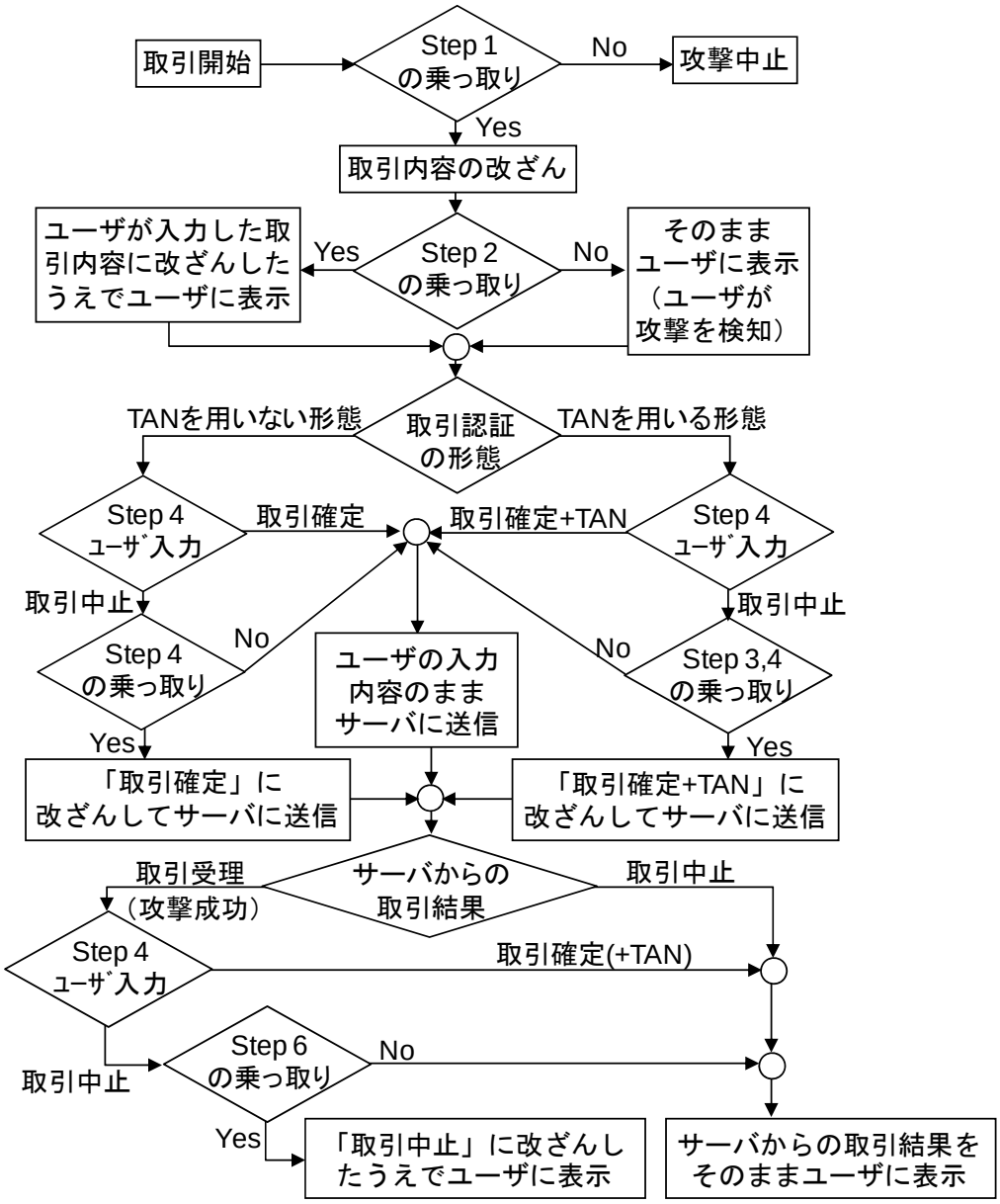
（TAN を利用する形態のケース）ユーザの入力が「取引確定+TAN」の場合、ウイルスはそのままサーバに転送する。ユーザの入力が「取引中止」の場合、Step 3 で TAN を不正に入手・生成していれば、ウイルスは「取引確定+TAN」に改ざんし、サーバに送信する。TAN を入手・生成していなければ、ウイルスは TAN を偽造できないため「取引中止」のままサーバに転送する[13]。

Step 6 を乗っ取った場合：

（サーバからの取引結果が「取引受理」のケース）攻撃は成功しているが、ユーザにその事実を気付かせ難くするために、次の処理を行う。Step 4 におけるユーザの入力が「取引確定」の場合、ウイルスは「取引受理」のままユーザに表示する。この場合、不正取引が受理されているにも関わらず、ユーザは自分が意図する取引が受理されたと誤認する。Step 4 におけるユーザの入力が「取引中止」の場合、ウイルスは「取引中止」に改ざんしたうえで表示する。この場合、不正取引が受理されているにも関わらず、ユーザは意図しない取引が無事に中止されたと誤認する。

（サーバからの取引結果が「取引中止」のケース）Step 4 におけるユーザの入力に関わらず、ウイルスは「取引中止」のまま表示する。

[13] Step 3 で TAN を入手していない場合は、ランダムに生成した TAN'を利用する方法も考えられる。通常、TAN は 6~8 桁の数字であるため、この場合に TAN の検証に合格する確率は 10^{-8}~10^{-6} 程度と考えられる。



図表 11. 攻撃の手順

4.2.3 攻撃の成否

Step 1 が乗っ取られているという前提のもと、Step 5 において、サーバが不正取引を受理するか否かについて分析する。Step 5 においてサーバが受信するメッセージは、「取引確定+TAN」「取引確定」「取引中止」の 3 種類である。各メッセージを受信した場合の取引結果は、それぞれ次のとおりである。

（「取引確定+TAN」を受信した場合） TAN の検証結果が合格となれば、不正取引が受理される。TAN の検証結果を TAN 1~3 について個別にみていく。

- TAN 1 は、サーバが不正な取引内容を受信し、同内容に対して発行した TAN である。そのため、TAN の検証結果が合格となり、不正取引は受理される。
- TAN 2 は、取引内容（振込先、金額）とは独立にユーザの手元で生成された TAN であり、取引内容が改ざんされても有効な TAN となる。そのため、TAN の検証結果が合格となり、不正取引は受理される。
- TAN 3 は、取引内容に基づきユーザの手元で生成された TAN である。Step 3 が乗っ取られていない場合、ユーザが意図する取引内容に基づき TAN が生成される。そのため、Step 4 においてユーザが自ら TAN を入力したとしても、不正な取引内容に対して有効な TAN とはならず、TAN の検証結果が不合格となり、不正取引は中止される。逆に、Step 3 が乗っ取られている場合には、不正な取引内容に対して有効な TAN が生成されるため、TAN の検証結果が合格となり、不正取引は受理される。

（「取引確定」を受信した場合）　不正取引は受理される。

（「取引中止」を受信した場合）　不正取引は中止される。

4.2.4　評価結果

取引処理に基づき分類された各形態（A1~8、B1~16＜TAN 1~3＞）について安全性評価を行った結果、MitB 攻撃による不正取引を防止可能な形態は 24 個となった（評価の詳細については**補論**を参照）。その内訳をみると、TAN を利用しない場合は 2 形態、TAN 1 を利用する場合は 6 形態、TAN 2 を利用する場合は 6 形態、TAN 3 を利用する場合は 10 形態となっており、TAN を利用する方が不正取引を防止可能な形態が多く、特に、TAN 3 を利用した場合が最も多い。

また、システム設計上の観点からは、モジュール 2 に求める機能が少ないほど、モジュール 2 が安価になる、あるいは、相対的に簡単に実装できるなどのメリットがあると考えられる。そこで、各形態のモジュール 2 に求める機能として、入力インタフェース（ボタン等）、出力インタフェース（画面等）、モジュール外部への送信機能、モジュール外部からの受信機能、TAN 生成機能について整理すると図表 12 のとおりである。同図表から、出力インタフェースについてはすべての形態において求められており重要な機能であるほか、TAN を利用することにより、モジュール 2 に求められる機能が TAN を利用しない場合に比べ軽減できるケースが多いことがわかる。

形態	MitB 攻撃を防止可能な形態	モジュール 2 に求められる機能					利便性に関する備考
		ユーザインタフェース		送信	受信	TAN 生成	
		入力	出力				
TAN を利用しない形態	A1, 4	要	要	要	要	—	TAN 生成指示や TAN の入力が不要
TAN 1 を利用する形態	B1, 3, 5, 10	要	要	要	要	—	TAN の入力が必要
	B4, 11	—	要	—	要	—	
TAN 2 を利用する形態	B3, 10	要	要	要	要	—	TAN 生成指示が必要※ TAN の入力が必要
	B1, 5	要	要	要	要	要	
	B4, 11	要※	要	—	要	要	
TAN 3 を利用する形態	B3, 10	要	要	要	要	—	TAN 生成指示が必要 TAN の入力が必要
	B1, 2, 5	要	要	要	要	要	
	B4, 7, 11	要	要	—	要	要	
	B9	要	要	要	—	要	
	B14	要	要	—	—	要	

※ 1 分等の短い間隔で更新される TAN をモジュール 2 に常に表示させるという実装や、取引の確認要求（取引手順 Step 2）をトリガーにモジュール 2 が TAN 生成を開始するという実装の場合には、ユーザが TAN 生成の指示をモジュール 2 に与える必要がないため、入力インタフェースは不要となる。

図表 12. 取引処理に基づき分類された各形態の安全性

4.3 評価 2：システム構成に基づいて分類された形態の安全性評価

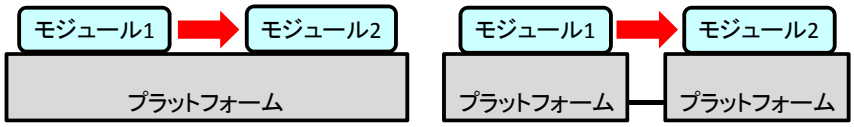
想定するシステムでは 2 つのモジュールを併用しており、両モジュールを乗っ取られた場合には MitB 攻撃による不正取引を防止することが困難である。そこで、システム構成に基づいて分類された各形態（型 1~4、前掲図表 9 参照）について、一方（モジュール 1 とする）を乗っ取ったウイルスが他方（モジュール 2 とする）も乗っ取ることの困難さについて安全性評価を行う。以下では、ウイルスの感染能力について定義したうえで、両モジュールが乗っ取られる困難さを評価する。なお、モジュール 1 とモジュール 2 の立場を入れ替えても同様の議論が可能である。

4.3.1 ウイルスの感染能力

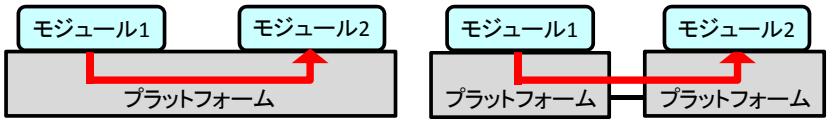
ウイルスがソフトウエアを乗っ取る方法として、まず、同ソフトの脆弱性を突く方法が挙げられる。仮に、そうした脆弱性が利用できないとしても、同ソフトが実装されているプラットフォーム（OS 等）の同ソフトに対する書込み権限

を利用する方法が挙げられる。これらを踏まえると、モジュール 1 を乗っ取っているウイルスがモジュール 2 を乗っ取る方法は、モジュール 2 の脆弱性を突いて乗っ取る方法（以下、「感染方法 1」）と、モジュール 2 が実装されているプラットフォームである OS に感染したうえで乗っ取る方法（以下、「感染方法 2」）が考えられる（図表 13 参照）。

なお、いずれの感染方法についても、モジュール 2 を乗っ取るためには、モジュール 1 を乗っ取ったウイルスがモジュール 2 に信号を送信可能になっている状態が前提となる。本稿では、こうした状態をモジュール 1 とモジュール 2 が「電気信号的に接続されている」と表現する。



(a) 感染方法 1



(b) 感染方法 2

図表 13. モジュール 2 を乗っ取る方法（イメージ図）

4.3.2 ウイルス感染への耐性

ウイルスの感染能力は、感染方法 1, 2 が可能であることをそれぞれ仮定するか否かにより 4 つに分類できる。取引認証方式の 4 つの形態（型 1~4）について、各感染方法のウイルスを想定した場合に、モジュール 2 が乗っ取られるか否かを分析する（図表 14 参照）。

感染方法 1	感染方法 2	型 1		型 2		型 3	型 4
		電気信号的に分離	電気信号的に接続	電気信号的に分離	電気信号的に接続	電気信号的に接続	
仮定する	仮定する	乗っ取られない	乗っ取られる	乗っ取られない	乗っ取られる	乗っ取られる	
仮定する	仮定しない						
仮定しない	仮定する						
仮定しない	仮定しない						

図表 14. 型 1~4 のウイルス感染への耐性

まず、感染方法 1, 2 のどちらも仮定しない場合、いずれの形態においてもモジュール 2 が乗っ取られないことは自明であるため、感染方法 1, 2 の一方または両方を仮定するケースについてみていく。

型 1 については 2 つの端末（モジュール 1, 2）がネットワーク等で繋がっている場合（同一のネットワーク機器の利用等）、両モジュール 1 が電気信号的に接

続されていれば、モジュール 2 が乗っ取られ、逆にこうした電気信号的な接続がなければ、モジュール 2 が乗っ取られないことがわかる。

型 2 については、2 つの端末（モジュール 1, 2）が接続されている場合（PC への USB デバイスの挿入等）、両モジュールが電気信号的に接続されており、モジュール 2 が乗っ取られることがわかる。逆に、2 つの端末間のやり取りを人手で行う場合には、両モジュールが電気信号的に接続されているとはいえず、モジュール 2 が乗っ取られないことがわかる（Barclays[2007, 2012]等）。

型 3, 4 については、同一プラットフォーム上に 2 つのソフトウエア（ブラウザと別アプリ）が実装され電気信号的に接続されているため、モジュール 2 が乗っ取られることがわかる。

この結果を踏まえると、型 1 や型 2 の電気信号的に分離されているケースの方が、その他のケースよりもウイルス感染への耐性が高いといえる。

5. 考察

本節では、TAN の効果、本研究の安全性評価の限界、運用上の留意点について、それぞれ考察する。

5.1 TAN の効果

取引処理に基づき分類された形態の安全性評価の結果（前掲図表 12 参照）をみると、TAN を用いなくとも MitB 攻撃を防止可能な形態（2 個）は存在するが、TAN を用いることでシステムを設計するうえで選択可能な形態の数（6～10 個）が増えることから、設計の自由度が高まるといえる。

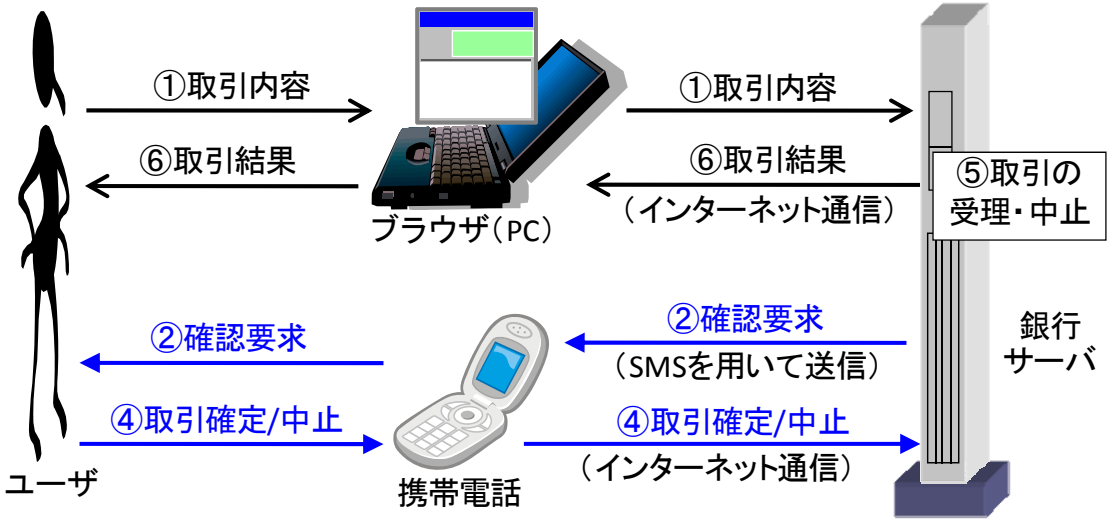
次に、モジュール 2 に求める機能の差異から、TAN の効果を考察する。TAN を利用しない形態（A1, 4）をみると、モジュール 2 に入出力インタフェースが必要となるほか、サーバとモジュール 2 がデータをやり取りする必要がある。図表 15 は、ブラウザ（PC）と携帯電話を併用する形態の具体例である。

これに対して、TAN を利用する場合、次の形態も選択可能になるという利点がある。1 つは、TAN 1 を利用する形態（B4, 11）である。同形態では、モジュール 1 に TAN を入力する手間が発生するものの、モジュール 2 には入力インタフェースとモジュール外への送信機能が不要となる。図表 16 は、ブラウザ（PC）とページャーを併用する形態の具体例である。

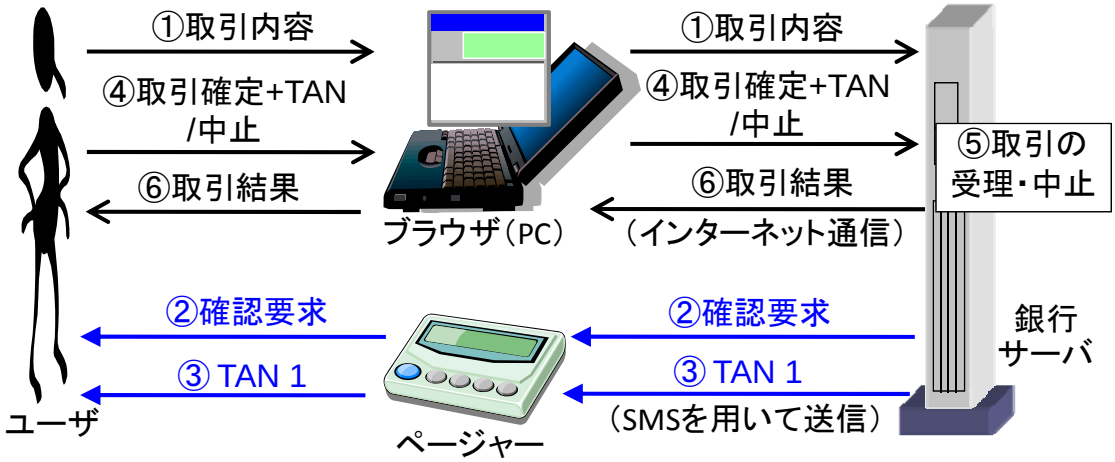
もう 1 つは、TAN 3 を利用する形態（B14）である。同形態では、TAN 生成をモジュール 2 に指示する手間とモジュール 1 に TAN を入力する手間が発生するものの、モジュール 2 は外部と通信する必要がないスタンドアローンで実現可能となる。同形態の具体例として英 Barclays の実装例をみると、モジュール 1

として PC のブラウザを利用する一方、モジュール 2 としては IC カードリーダを有する専用の TAN 生成装置ないし専用の TAN 生成アプリケーションを搭載したスマートフォンを利用している（図表 17 参照、Barclays [2007, 2012]）。

したがって、モジュール 2 に求める機能に注目すると、各金融機関が導入している既存の対策との親和性やビジネス要件、コスト等の観点から、①入力インタフェースをもたないモジュール 2 を前提とする必要がある場合には TAN 1 を利用する形態（B4, 11）を、②スタンドアローンのモジュール 2 を前提とする必要がある場合には TAN 3 を利用する形態（B14）を、③入出力インタフェースと外部との送受信機能を有するモジュール 2 を前提とする必要がある場合には TAN を利用しない形態（A1, 4）をそれぞれ選択することが考えられる。



図表 15. TAN を用いない形態（A4）の具体例



図表 16. TAN 1 を用いる形態（B11）の具体例

(a)IC カードリーダを有する専用の TAN 生成装置　(b) 専用の TAN 生成アプリケーションを搭載したスマートフォン

（備考）英 Barclays では、送金先が新規の場合に TAN を利用する。

図表 17.　英 Barclays が利用するモジュール 2

5.2　本研究の安全性評価の限界

本研究の 2 つの安全性評価（評価 1, 2）では、具体的な実装方法に立ち入らずにモジュールがウイルスに乗っ取られるという前提のもとで議論した。しかし、実装された具体的な取引認証方式の安全性評価を行うためには、これらの前提が成立する可能性についても評価することが求められる。このため、本研究の安全性評価の結果だけを参照して、個別の取引認証方式の安全性を比較することは適切ではない。

5.3　運用上の留意点

MitB 対策として取引認証を導入していくに当たっては、次に挙げる事項についても十分検討を行う等、留意することが必要である。

- 取引認証方式を導入するために、事前作業として端末やメールアドレス等の登録やアプリケーションのインストール等の作業が必要となるケースが想定される。また、ユーザの PC がウイルスに既に感染している状況も想定されるため、そうした PC を前提にしても適切に取引認証方式を導入可能な方法を検討することが望ましい。例えば、登録やインストール時に PC のウイルススキャンを行うツールを提供する方法や PC 以外の安全性を確保できる他の手段（郵便、電話等）を利用して登録作業を行う方法等が考えられる。
- 取引認証方式を適切に導入できたとしても、ユーザが同方式を適切に活用で

きなければ期待した効果が得られない。例えば、海外では、TAN をスマートフォンで受信する取引認証方式に対して、ユーザを騙し、「TAN を盗取する不正アプリケーション（「Man-in-the-Mobile」と呼ばれる）をスマートフォンにインストールさせる手口」が報告されているほか（Roberts[2011]）、「新しいセキュリティ機能に慣れるための練習と称して、不正取引を本人に実施させる手口」も報告されている（Trusteer[2011]）。こうした手口にも対応できるようにユーザに継続的な啓蒙を行うことも重要である。

・ 本研究では、MitB 攻撃を防止する対策として取引認証に焦点を当てたが、同攻撃を事後的に検知可能な対策についても検討することが望ましい。例えば、取引処理の流れの Step 6（前掲図表 7 参照）においてサーバからユーザに取引結果を伝える際に、具体的な取引内容（振込先、金額）を含めるという方法が考えられる。

6. おわりに

本稿では、MitB 攻撃への対策の 1 つである取引認証に焦点を当てて、安全性の考え方の整理や評価を行った。具体的には、取引認証方式を取引処理およびシステム構成の観点からそれぞれ分類可能であることを示した。そのうえで、取引処理の観点からは、モジュール 2 に求める機能に注目した場合に有力となる 3 つの対策形態を示すとともに、TAN を用いることでシステムを設計するうえで選択可能な対策形態の数が増加し、設計の自由度が高まることを示した。システム構成の観点からは、ブラウザ（PC）とスタンドアローンの TAN 生成装置の組合せのように 2 つのモジュールが電気信号的に分離しているほど 2 つのモジュールが共にウイルス感染しにくいことを示した。

比較的導入し易い取引認証方式としては、一部の金融機関が既に導入している「取引時に One-Time-Password（TAN 1 に相当）をユーザの携帯電話に送信する」という形態を MitB 攻撃に耐性をもつように改良する案が考えられる。具体的には、携帯電話に TAN 1 を送信する際に、取引内容（送金先、金額）も併せて送信するように修正することが考えられる（サーバにおける TAN の検証も必要）。こうした形態（前掲図表 16 参照）であれば、追加のコストを抑えられるほか、利便性の低下も軽減できると考えられる。

なお、本研究では取引内容を改ざんから保護する対策に焦点を当てたが、今後の検討課題としては、インターネットバンキングで利用されるその他の情報を保護する必要があるかについても検討を加えることが望ましい。例えば、登録されている個人情報（メールアドレス等）や送金限度額等の情報がウイルスによって改ざんされた場合、不正取引やその被害額の増加につながる可能性があ

るか評価し、そうした情報の変更時には必要に応じてユーザによる追加認証を行うという対策が考えられる。

インターネットバンキング関係の不正事件は日々複雑かつ巧妙になっており、内外の不正事件や学界の動向をフォローしつつ、ユーザが安心してサービスを利用できるよう安全性を確保していくための努力を今後も継続することが望まれる。

補論．評価 1 の評価結果の詳細

取引処理に基づいて分類された形態の安全性評価の詳細を示す。まず、モジュール 1, 2 の一方が乗っ取られたときに、Step 1~4, 6 の各ステップが乗っ取られるか否かを図表 18 に示す。また、その場合に不正取引が成立するか否かも図表 18 に示す。分析結果から、一方のモジュールが乗っ取られても不正取引を防止可能な形態は、TAN を利用しない形態については 2 個（A1, 4）、TAN 1, 2 を利用する形態については 6 個（B1, 3~5, 10, 11）、TAN 3 を利用する形態については 10 個（B1~5, 7, 9~11, 14）となる。

形態	A1		A2		A3		A4		A5		A6		A7		A8	
ケース	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2
Step 1	○	×	○	×	○	×	○	×	○	×	○	×	○	×	○	×
Step 2	×	○	○	×	×	○	×	○	○	×	○	×	×	○	○	×
Step 4	×	○	×	○	○	×	×	○	○	×	×	○	○	×	○	×
Step 6	×	○	×	○	×	○	○	×	×	○	○	×	○	×	○	×
不正取引	○	○	○	×	○	×	○	○	○	×	○	×	○	×	○	×

(a) TAN を利用しない形態

形態	B1		B2		B3		B4		B5		B6		B7		B8	
ケース	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2
Step 1	○	×	○	×	○	×	○	×	○	×	○	×	○	×	○	×
Step 2	×	○	○	×	×	○	×	○	×	○	○	×	○	×	×	○
Step 3	×	○	×	○	○	×	×	○	×	○	○	×	×	○	○	×
Step 4	×	○	×	○	×	○	○	×	×	○	×	○	○	×	○	×
Step 6	×	○	×	○	×	○	×	○	○	×	×	○	×	○	×	○
不正取引	○	○	○	×	○	○	○	○	○	○	○	×	○	×	○	×

形態	B9		B10		B11		B12		B13		B14		B15		B16	
ケース	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2
Step 1	○	×	○	×	○	×	○	×	○	×	○	×	○	×	○	×
Step 2	○	×	×	○	×	○	○	×	○	×	○	×	×	○	○	×
Step 3	×	○	○	×	×	○	○	×	○	×	×	○	○	×	○	×
Step 4	×	○	×	○	○	×	○	×	×	○	○	×	○	×	○	×
Step 6	○	×	○	×	○	×	×	○	○	×	○	×	○	×	○	×
不正取引	○	×	○	○	○	○	○	×	○	×	○	×	○	×	○	×

(b) TAN を利用する形態（TAN 1, 2）

形態	B1		B2		B3		B4		B5		B6		B7		B8	
ケース	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2
Step 1	○	×	○	×	○	×	○	×	○	×	○	×	○	×	○	×
Step 2	×	○	○	×	×	○	×	○	×	○	○	×	○	×	×	○
Step 3	×	○	×	○	○	×	×	○	×	○	○	×	×	○	○	×
Step 4	×	○	×	○	×	○	○	×	×	○	○	×	○	×	○	×
Step 6	×	○	×	○	×	○	×	○	○	×	×	○	×	○	×	○
不正取引	○	○	○	○	○	○	○	○	○	○	○	×	○	○	○	×

形態	B9		B10		B11		B12		B13		B14		B15		B16	
ケース	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2	C1	C2
Step 1	○	×	○	×	○	×	○	×	○	×	○	×	○	×	○	×
Step 2	○	×	×	○	×	○	○	×	○	×	○	×	×	○	○	×
Step 3	×	○	○	×	×	○	○	×	○	×	×	○	○	×	○	×
Step 4	×	○	×	○	○	×	○	×	×	○	○	×	○	×	○	×
Step 6	○	×	○	×	○	×	×	○	○	×	○	×	○	×	○	×
不正取引	○	○	○	○	○	○	○	×	○	×	○	○	○	×	○	×

(c) TAN を利用する形態（TAN 3）

（備考）モジュール 2 のみが乗っ取られている状況をケース「C1」、モジュール 1 のみが乗っ取られている状況をケース「C2」と表記した。各ステップについては、乗っ取られていない場合には「○」、乗っ取られている場合には「×」と表記した。不正取引については、防止できる場合には「○」、防止できない場合には「×」と表記した。

図表 18. 評価 1 の評価結果

参考文献

Barclays, “PINsentry User Guide,” 2007.

———, “Mobile PINsentry,” 2012.（http://www.barclays.co.uk/BarclaysMobile Banking/MobilePINsentry/P1242616134119）

CA Technologies, 「Man-in-the-Browser および Man-in- the-Middle 攻撃からオンライン顧客を保護」、2011 年

Entrust, “Defeating Man-in-the-Browser Malware,” 2010.

Gühring, Philipp, “Concepts against Man-in-the-Browser Attacks,” 2007.

Li, Shujun, Ahmad-Reza Sadeghi, Sören Heisrath, Roland Schmitz and Junaid Jameel Ahmad, “hPIN/hTAN: A Lightweight and Low-Cost e-Banking Solution against Untrusted Computers?,” Financial Cryptography, 2011.

McAfee、「分析：Operation High Roller」、ホワイトペーパー、2012 年

Roberts, Paul, “Zeus Banking Trojan Comes to Android Phones,” Threatpost, 12th July 2011.（http://threatpost.com/en_us/blogs/zeus-banking-trojan-comes- android-phones-071211）

RSA、「金融機関における脅威の分析と緩和：Man-In-The-Browser 型トロイの木馬について」、RSA White Paper、2010 年

Trusteer, “No Silver Bullet: 8 Ways Malware Defeats Strong Security Controls,” White paper, 2011.

Weigold, Thomas, Thorsten Kramp, Reto Hermann, Frank Höring, Peter Buhler, Michael Baentsch, “The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks,” TRUST 2008, LNCS vol.4968, pp.75-91, 2008.

石井晋也、「インターネットバンキングで必要となる本人認証とは？　～真のユーザ保護のために、今すべきこと～」、ベリサイン金融機関向けセミナー、2012 年 11 月 22 日

警察庁、「インターネットバンキング利用者の金融情報を狙った新たな犯行手口の発生について」、広報資料、2012 年 10 月 26 日（http://www.npa.go.jp/cyber/warning/h24/121026.pdf）

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」、CSEC 研究会、2009 年

産経新聞、「ネット不正送金、三菱東京 UFJ でも被害」、2013 年 1 月 26 日

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法を使ったボットウイルス対策」、コンピュータセキュリティシンポジウム（CSS）、2008 年

———・———・———、「複数の独立した端末と認証方法を使ったマルウェア

に強い命令（電子商取引）方式」、暗号と情報セキュリティシンポジウム、2009 年
中山靖司、「インターネット・バンキングの安全性を巡る現状と課題」、『日銀レビュー』2006-J-14、2006 年
日本経済新聞、「ネットバンキングなど狙う「ポップアップ型フィッシング詐欺」が多発」、日本経済新聞 電子版、2012 年 11 月 5 日 23:00
フォティーンフォティ技術研究所、「11 月 20 日、Web Browser Protection「FFRI Limosa（エフエフアールアイ リモザ）」をリリース」、プレスリリース、2012 年 11 月 16 日（http://www.fourteenforty.jp/news/release_20121116.htm）

※ 各 URL は、2013.1.9 に確認

以　上