SIM を活用したモバイルバンキングのセキュリティ向上に関する検討

磯原 隆将[†1]　竹森 敬祐[†2]　本間 輝彰[†1]

概要：オンラインバンキングの普及に伴い，取引に用いる端末を乗っ取ることで，不正送金等を行う，Man-in-the-Browser（MITB）攻撃の脅威が増している．本研究では，スマートフォンを用いるモバイルバンキングに着目して，MITB 攻撃への対策を考慮した，セキュリティ向上に関する提案を行う．具体的には，スマートフォンが備える，SIM（Subscriber Identity Module）に実装するアプレットを活用して，ログイン認証の強化と取引認証を実現するシステムを提案する．提案方式の実装と評価および考察を行い，有効性の検証を行う．

キーワード：SIM, セキュアエレメント, MitB 攻撃, 取引認証, FinTech

SIM-based security enhancement of mobile banking against Man-in-the-Browser attacks

Takamasa Isohara[†1]　Keisuke Takemori[†2]　Teruaki Honma[†1]

Abstract: Man-in-the-Browser (MitB) attacks is one of the most serious threat on a mobile banking services. To against this kind of threat, we propose a Subscriber Identity Module (SIM) based security enhancement for mobile banking services. Our scheme uses a Java applet which runs on the SIM to achieve a client authentication and a transaction authentication. We have implemented our proposed architecture and discuss an effectiveness for security on the mobile banking services.

Keywords: SIM, Secure Element, MitB attack, Transaction Authentication, FinTech

1. はじめに

昨今, PC やスマートフォン等の携帯電話を用いた銀行取引である，オンラインバンキングの普及が進んでいる．

オンラインバンキングの普及にともなって，不正送金や不正な住所変更等といった，金融犯罪の脅威が増している [1].

こうした金融犯罪は，財産に対する直接的な被害を及ぼすことから，深刻な社会問題として認識されている．

従来，オンラインバンキングおける主な脅威は，オンラインバンキングの利用者のフィッシングサイトへ誘導や，サービスを利用する端末やアプリを，スパイウェアやウイルスに感染させることで，ID やパスワード，乱数表などの認証に関する情報を不正に入手して，悪用するものであった．しかし，近年，オンラインバンキングに用いるブラウザやアプリケーションに不正なプログラムを組み込むことで，こうした脅威は Man-in-the-Browser 攻撃（MitB 攻撃）と呼ばれている. MitB 攻撃による取引内容の改ざんへの対策として，ソフトウェアやハードウェアが分離された 2 つ以上の経路を用いて，取引内容の承認をユーザに求める，取引認証が用いられている．

オンラインバンキングに用いられる携帯電話には，耐タンパ性を持ち，演算機能とアプリ実行環境を備えた SIM が実装されている．

そこで本論文では，取引認証のために必要な分離された経路の実現にあたって，SIM を活用する方式を検討する．具体的には，SIM 上に，取引認証のためのアプリケーションを実装し，取引認証を実現するものである．また，SIM がアプリ実行環境を持つことと，通信事業者による本人確認を伴って発行されていることに着目して，中間認証局として機能するアプレットを用いて，利用者の PC に対して公開鍵証明書を発行し, PC を用いたオンラインバンキングの利用時に，二要素による端末認証を実現する仕組みについても提案する．

以降，2 章でオンラインバンキングにおける攻撃とその対策について整理し，3 章で，SIM と，携帯電話に実装される SIM とのインタフェースである USAT について説明する．4 章で，SIM を活用したオンラインバンキングの安全性向上の提案を，携帯電話単体でオンラインバンキングを利用するモデルと, PC と携帯電話路あわせて利用するモデルのそれぞれについて述べる. さいごに, 5 章でまとめる．

†1KDDI 株式会社
KDDI Corporation
†2 KDDI 研究所
KDDI R&D Laboratories

2. オンラインバンキングにおける攻撃と対策

本節では，はじめに，提案方式の前提となるオンラインバンキングに関して，モデルと処理の流れを述べる．続いて,オンラインバンキングに対する攻撃について説明する．その上で，攻撃に対する対策を整理する．

2.1 オンラインバンキングのモデル

オンラインバンキングは，サービスの利用者であるユーザが，PC やスマートフォン等を用いて，インターネット等のネットワークを通じて，金融機関のサーバが提供する金融サービスを利用するものである．

本論文では，オンラインバンキングを，ユーザ，クライアント端末，金融機関サーバから構成されるモデルと定義する．図 1 に，これら構成要素とモデルを示し，以下，各要素について説明する．

ユーザは，金融機関が提供するオンラインバンキングのサービスを利用するためのアカウントを有している．サービスを利用する際は，クライアント端末を用いて，金融機関サーバにアクセスを行う．

クライアント端末は，PC やスマートフォン等の，金融機関サーバにアクセスを行うための端末である．クライアント端末では，サービスを利用するためのソフトウェアが実行される．一般的に，PC の場合は Web ブラウザが用いられ，スマートフォンの場合は，オンラインバンキング用の専用アプリケーションが利用される．

金融機関サーバは，オンラインバンキングサービスを提供する金融機関のサーバである．

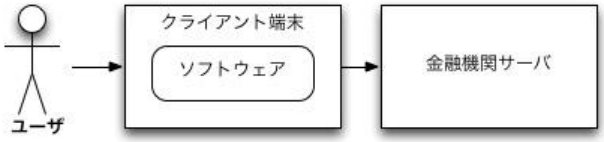

図 1 オンラインバンキングのモデル

2.2 オンラインバンキングの処理の流れ

クライアント端末と金融機関サーバの間で実行される，オンラインバンキングにおける処理を図 2 に示し，以下に詳細を述べる．

オンラインバンキングを利用する場合，ユーザは，はじめに，クライアント端末を用いて，アカウント情報を金融機関サーバに対してアカウント情報を送信し，金融機関サーバにおける認証を経て，ログインを行う．以降，本論文では，これをログイン処理と定義する．

認証に成功してログインを完了した場合，ユーザは，自身の口座の残高照会や，振込み，住所変更等の，オンラインバンキングにおいて提供されるサービスを利用する．これを，取引処理と定義する．取引処理においては，振込みや住所変更など,金銭的な被害に影響を及ぼすと考えられ，高いセキュリティを求められる重要な取引については，取引を実行するにあたって，その認証が行われる．取引に対する認証は，事前に乱数表などを共有して，これを利用する方法や，ハードウェアやソフトウェア的なトークンを利用してワンタイムパスワードを生成･送信する方法がある．

通常，一度のログイン処理でセッションを構築した後，そのセッション内で,複数の取引処理の実行が可能である．

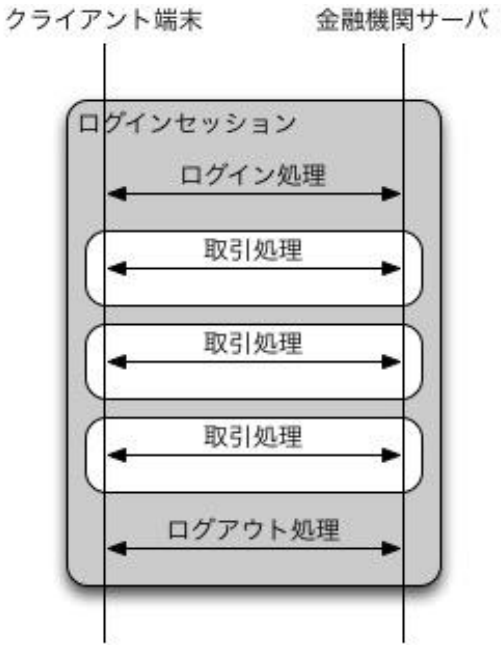

図 2 オンラインバンキングの処理の流れ

2.3 オンラインバンキングにおける脅威

本論文では，オンラインバンキングの処理が，ログイン処理と取引処理に大別できることに基づき，それぞれの処理における脅威として，なりすましと取引内容の改ざんに着目する．

2.3.1 なりすまし

なりすましは，攻撃者が，正規ユーザのアカウント情報や認証情報を不正に入手して悪用する脅威である．

ユーザの ID やパスワードといったアカウント情報，および取引認証に用いる乱数表などの認証情報が，攻撃者の手に渡ることで，成りすましの脅威が発生する．

2.3.2 取引内容の改ざん

取引の改ざんは，攻撃者が，クライアント端末と金融機関サーバの間で行われる取引処理に対して攻撃を行い，正規ユーザが意図しない取引内容に変更を行う脅威である．

2.4 脅威の原因となる攻撃

なりすましと取引内容の改ざんの要因となる攻撃について整理する．

2.4.1 フィッシング・スパイウェア・ウイルス感染

攻撃者がアカウント情報や認証情報を不正に取得する方法は，サーバ側で行われるモデルと，クライアント端末

側で行われるモデルに分類される．

前者については，フィッシングサイトと呼ばれる偽のウェブサイトを構築して，ここに利用者を誘導することで，情報を盗み出す方法がある．

後者については，クライアント端末をウイルスに感染させる方法や，スパイウェアと呼ばれる悪意のアプリケーションを作成して，これを利用者の PC やスマートフォンにインストールさせる方法により，情報を盗み出す方法がある．

2.4.2 Man-in-the-Browser **攻撃**

Man-in-the-Browser 攻撃（以下，MitB 攻撃）は，オンラインバンキングを利用するクライアント端末上のソフトウェアに感染した不正なプログラムが，ソフトウェアに対する入力や取引の内容を，盗聴・改竄する攻撃である．

図 3 に示すように，オンラインバンキングを行うクライアント端末上のソフトウェアに攻撃者が存在するモデルであり，PC のブラウザに不正プログラムが感染するものを，Man-in-the-Browser 攻撃（以下，MitB 攻撃）と称し，スマートフォンのアプリケーションに感染するものを，Man-in-the-Application 攻撃（MitA 攻撃）と称する．以下，本論文では，MitB 攻撃と MitA 攻撃をあわせて，MitB 攻撃と称する．

MiB 攻撃は，ユーザによる正規の操作中にアカウント情報の窃盗や取引内容の改ざんを行うことが可能であるため，ユーザが攻撃に気づきにくいという特徴がある．

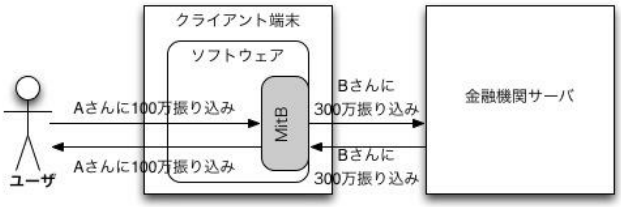

図 3 MitB 攻撃のモデル

2.5 脅威と攻撃への対策の考察

オンラインバンキングにおける，成りすましと取引内容の改ざんの脅威，および，これら脅威の原因となるフィッシング・スパイウェア・ウイルス感染と，MitB 攻撃への対策を考察する．

2.5.1 クライアント端末におけるセキュリティ対策

スパイウェアや MitB 攻撃は，クライアント端末やそこで稼動するブラウザおよびアプリケーションがスパイウェアやウイルスに感染することが脅威の原因となっている．

したがって，これらを防止する手段として，OS やアプリケーションのセキュリティパッチを適切に適用すること，ウイルス対策ソフトを導入することがあげられる．

ウイルス対策ソフトの中には，フィッシング等の悪性 Web サイトへの接続を未然に防止する機能を持つものもある．

2.5.2 SSL 証明書を用いたサーバおよびクライアントの端末認証の強化

SSL 証明書を用いた端末認証は，サーバを認証する対策と，クライアント端末を認証する対策の双方に用いることが可能である．

サーバの認証に用いる場合，ユーザがフィッシングサイトへ接続して，アカウント情報や認証情報を攻撃者に渡してしまうことの防止に効果が見込まれる．

クライアント端末の認証に用いる場合，二要素認証による端末認証を実現することとなり，攻撃者にアカウント情報が渡った場合でも，なりすましによる，不正な端末からのログインを防止することに効果が見込まれる．

2.5.3 MitB 攻撃対策のための取引認証

MitB 攻撃は，ブラウザやアプリケーションがウイルスに感染することで成立する攻撃であることから，ウイルス対策の確実な実施が有効である．

しかし，ウイルス感染等を完全に防止することは困難であることから，ブラウザやアプリケーションがウイルスに感染していることを前提として，オンラインバンキングを行うクライアント端末やソフトウェアとは別の環境を組み合わせて，取引処理を実施する対策が採られている．こうした対策を取引認証といい，ユーザが実行しようとする取引内容を，別の経路を通じて認証する対策となる．

[2]では，MitB 攻撃対策としての取引認証の安全性を評価するに当たって，MitB 攻撃の種類，想定する対策システムの構成，および取引認証に用いる TAN（Transaction Authentication Number）について考察を行っている．以下，それぞれの観点について要約する．

まず，MitB 攻撃を，「ID 盗取型」と「取引内容改ざん型」に分類して，MitB 攻撃に求められる取引認証の用件を整理しており，いずれの攻撃に対しても，「取引時にリアルタイムで得る情報を利用した取引認証」が有効であると考察している．

つぎに，MitB 攻撃対策のシステムは，オンラインバンキングに用いるクライアント端末上のブラウザやアプリケーションが攻撃者にのっとられていることを前提として，同一端末上の別のソフトウェアやハードウェアの要素を組み合わせて取引を行うモデルを採用する．ここで，組み合わされる要素を「モジュール」と定義しており，処理の煩雑性と利便性の観点から，図 4 に示す，2 つのモジュールを併用してオンラインバンキングの処理を行うシステムを想定している．

最後に，取引認証において，ユーザが取引内容を認証するための使い捨て番号である「Trans- action Authentication Number」(以下，「TAN」)について，ユーザが入手するタイミングと生成場所，および，TAN の生成に用いる情報に注目し，表 1 のような整理を行っている．

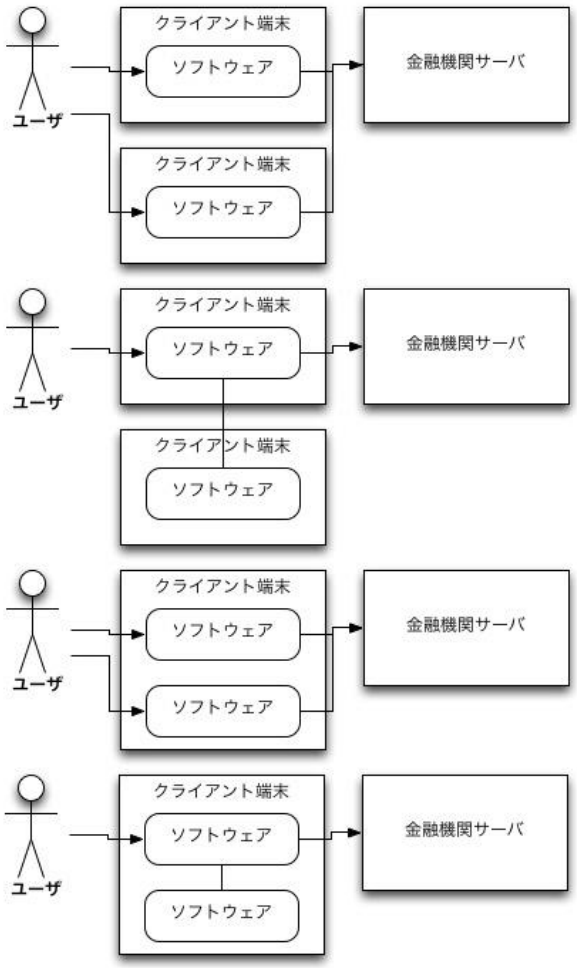

図 4 MitB 対策のモデルの分類

表 1 TAN の分類

入手タイミング	生成場所	具体例
事前配布		乱数表など
リアルタイム	サーバ	SMS や電子メールで通知
	クライアント	取引内容と独立した TAN 生成
		取引内容を利用した TAN 生成

3. SIM/USAT

従来，オンラインバンキングの利用形態として，クライアント端末に，PC を用いるものが主流であった．しかし昨今，スマートフォンなどの携帯電話をクライアント端末として用いる利用形態が増えている．

PC と携帯電話を，モジュールの構成に着目して比較した場合，携帯電話には，SIM（Subscriber Identity Module）（以下，SIM）と呼ばれる IC モジュールが搭載されているという特徴がある．

SIM は，耐タンパ性を有するセキュアエレメントであること，演算機能およびアプリ実行環境を持つことが特徴である．また，SIM で実行されるアプリは，携帯電話に実装されるインタフェースである USAT（User Subscriber identity module Application Toolkit）機能を通じて，ユーザとの情報のやり取りが可能である．

以下，SIM と USAT について整理する．

3.1 SIM

SIM は，携帯電話の加入者の識別や認証に用いる情報を記録するモジュールを搭載した，IC カードである．

SIM に記録される情報には，SIM を一意に識別する情報である ICCID（IC Card Identifier）や，加入者を一意に識別する情報である IMSI（International Mobile Subscriber Identity），加入者がネットワークに接続する際の認証処理に用いる認証鍵などがある．

また，SIM には，演算を行う機能が備わっており，ネットワーク接続時の認証等に必要な処理を，SIM が持つアプリ実行環境上で実行されるカードアプリケーションとして実装することが可能である．SIM カードにおけるカードアプリケーションの実行のプラットフォームの代表的なものに，Java Card があり[3]，ここで実行されるアプリケーションを Java アプレットと称する．

具体的には，携帯電話の音声・データ通信サービスのために，加入者識別や認証を行うカードアプリケーションである USIM（Universal Subscriber Identity Module）[4]や ISIM（IP Multimedia Services Identity Module）[5]と呼ばれる NAA（Network Access Application）や，クレジットカードの決済サービスを提供するアプリケーションなどがある[6][7].

SIM に記録される情報やアプリケーションは，不正な読み込みや改ざんによって悪用された場合，成りすましや不正課金の被害を生じるおそれがある．そのため，SIM は，ハードウェアに対する物理的な攻撃と，ソフトウェアに対する電子的な攻撃から情報を保護可能な，耐タンパ性を備えたセキュアデバイスとなっている．

たとえば，認証に用いる鍵情報は，直接読みだすことは不可能であり，認証に際しては，鍵を用いた演算結果のみを戻す．これにより，クローン作成の防止と認証デバイスとしての機能の両立を果たしている．

SIM カード上の Java アプレットは，単一のカード上で複数のアプレットを実行することが可能である．このとき，セキュアデバイスである SIM カードに対して，複数のアプレットを搭載・管理するための，コンテンツ・マネジメント技術が必要となる．コンテンツ・マネジメント技術を標準化する組織に，GlobalPlatform がある[8]．GlobalPlatform が策定する規格により，Java アプレットを提供するサービス・プロバイダは，安全な通信路を用いた SIM カード上のアプレット実行領域への Java アプレットのインストールと，インストール後の Java アプレットのカスタマイズ等を

実現する．ここで，アプレットはOTAでコントロールすることが可能であるまた，Javaアプレットを SIMカードに導入する際の安全な通信路は，GlobalPlatformの規定するセキュアチャネルと呼ばれる通信方式を利用する必要があるが，インストール後のアプレットは，HTTPS等の任意のプロトコルを利用することが可能である．

以上より，SIMカードは，加入者の識別や認証に必要な情報が記録された，演算の機能によってJavaアプレットの実行が可能なICカードであるといえる．SIMカードに格納される情報やプログラムは，機密性・完全性・可用性を高いレベルで求められることから，SIMカードは，耐タンパ性を有するセキュアデバイスとなっている．また，GlobalPlatformが策定するコンテンツ･マネジメント技術に関する規格に則り，単一のSIMカード上で，複数のJavaアプレットを実行する環境を安全に実現することが可能である．

3.2 USAT

通常，SIMカードは受動的なデバイスであり，携帯電話等の移動機からの命令（コマンド）を受けて，命令に対する応答（レスポンス）を返す．これに対して，USATでは，SIMカードに実装されるUSATアプリケーションが，プロアクティブコマンドと呼ばれる命令を能動的に発することで，携帯電話などの端末の機能を作動させたり，ネットワークを通じて外部のWebサーバと通信を行ったりすることが可能となる．この仕組みにより，SIM上で実行されるアプリケーションを活用した，様々なサービスの実現を可能としている．

USATアプリケーションを構成する技術として，SIMに実装されるプロアクティブコマンドと，端末に実装されるUSATコマンドがある．プロアクティブコマンドは3GPP TS31.111で標準化されており[9]，USATコマンドは，ETSI（European Telecommunications Standards Institute） TS 102.221で標準化されている[10].

プロアクティブコマンドは，多くのコマンドが規定されているが，ここでは，代表的なものとして，GET INKEYとOPEN CHANNEL/CLOSE CHANNEL，RECEIVE DATA/SEND DATAについて，以下に説明する．

- GET INKEY：携帯電話のディスプレイを通じて，ユーザにメッセージを通知するとともに，Yes/Noなどの入力を要求する．入力結果は，TERMINAL RESPONSEによって返される．本コマンドの実行結果の例を図 5に示す．
- OPEN CHANNELおよびCLOSE CHANNEL：SIMアプレットが外部のサーバと接続する仕組みであるBIP（Bearer Independent Protocol）の経路のOPEN/CLOSEの要求を行う場合に用いられる．

図 5 GET INKEYコマンドによる画面表示の例

- RECEIVE DATA：SIMカードに対してデータを送信したい場合に用いる．送信するデータはTERMINAL RESPONSEによって入力される．SEND DATAは，SIMカードから送信されたデータを端末に通知する場合に用いる．

USATコマンドは，TERMINAL PROFILE，ENVELOPE，FETCH, TERMINAL RESPONSEの4つが規定されている．

- TERMINAL PROFILE：端末がSIMカードに対して，対応するUSAT機能を通知するために用いられる．
- ENVELOPE：端末からSIMカードに対して，USATに関連する情報を伝達するために用いられる．
- FETCH：SIMカードから端末に対して，プロアクティブコマンドを発行するために用いられる．
- TERMINAL RESPONSE：そのコマンドが発行されるより以前にFETCHによってSIMカードから端末に発行されたプロアクティブコマンドの実行結果を，端末からSIMカードに通知するために用いられる．

4. SIMを活用したオンラインバンキングの安全性向上に関する提案

オンラインバンキングの安全性を確保する対策として，ウイルス対策，SSL証明書を用いた端末認証，MitB攻撃を想定した取引認証が有効であることを示した．このうち，クライアント端末で実施可能な対策は，ウイルス対策，クライアント証明書を用いた端末認証，および，MitB攻撃対策のための取引認証となる．

また，オンラインバンキングにおいて，クライアント端末として用いられる携帯電話に備えられたSIMに着目し，SIMが耐タンパ性を有するセキュアデバイスであること，演算機能とアプリ実行環境を持つことを示した．

取引認証の対策を実現する場合には，同一端末上で動作する別のソフトウェアや，別のハードウェアを用いる方式

が有効であると示されている．この要件を満たすものとして，オンラインバンキングの安全性向上に寄与するモジュールとして，SIM を利用することが可能と考える．

そこで本節では，SIM を活用して，オンラインバンキングの安全性を向上する方式の提案を行う．以下，オンラインバンキングのモデルを，利用形態に応じて，スマートフォン等の携帯電話単体でオンラインバンキングを行う「モバイルバンキング」と，PC を用いたオンラインバンキングに携帯電話を併用する「インターネットバンキング」と定義し，モバイルバンキングとインターネットバンキングのそれぞれについて，SIM を活用した提案方式について説明する．

4.1 モバイルバンキング向け安全性向上策

4.1.1 モバイルバンキング向け安全性向上策のシステム構成

提案方式のシステム構成を図 6 に示す．

提案システムは，図に示したオンラインバンキングのモデルにおいて，クライアント端末に，スマートフォン等の携帯電話を用いる構成である．

携帯電話には，オンラインバンキングを行うためのバンキングアプリがインストールされている．このアプリは携帯電話の OS のプラットフォーム向けに作成されたものである．ユーザは，バンキングアプリを利用して，取引を行う．

また，携帯電話には，SIM カードが備わっており，SIM カードには，以下に述べるアプレットが搭載されている．

- 音声･データ通信のために必要となる，USIM や ISIM 等の，NAA
- 取引認証を実現するための，取引認証アプレット

取引認証アプレットは，USAT 機能を用いて，ユーザへの情報の通知・表示や，ユーザからの入力の受け取りを行うことが可能である．

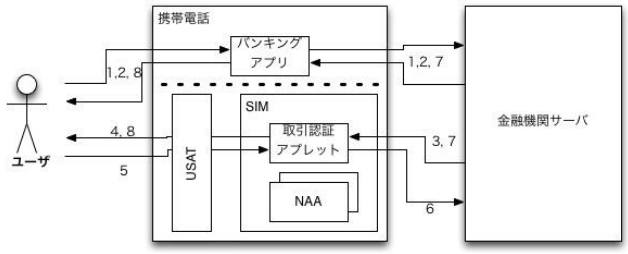

図 6 モバイルバンキング向け安全性向上策の構成

4.1.2 モバイルバンキング向け安全性向上策の処理フロー

提案方式における処理の流れを図 7 に示し，詳細を以下に説明する．

1. ユーザは，クライアントアプリにアカウント情報を入力して，金融機関サーバにログインする．
2. ログインに成功した場合，クライアントアプリに取引内容を入力する．取引内容は，クライアントアプリを通じて，金融機関サーバに送信される．
3. 金融機関サーバは，ユーザによる取引認証を行うため，受信した取引内容を，SIM の取引認証アプレットに送信する．取引内容の送信には，SMS などを用いる．
4. 取引認証アプレットは，受信した内容を，USAT 機能の GET INKEY コマンドを用いて，ユーザに表示する．（TAN の取り扱いが入る）
5. ユーザは，取引認証アプレットが GET INKEY コマンドを用いて表示した取引内容を確認し，表示されている内容が意図するものであれば，取引を続行する旨を入力する．表示内容が意図したものでなければ，取引を中止する旨を入力する．
6. 取引認証アプレットは，ユーザが入力した内容を，金融機関サーバに通知する．取引認証アプレットから金融機関サーバへの情報の送信は，BIP により構築される安全な通信経路を用いて行われる．
7. 金融機関サーバは，受信した内容に応じて，取引の続行や中止を処理し，処理が完了した場合，それを，UI アプリや取引認証アプレットに通知する．
8. UI アプリや取引認証アプレットは，金融機関サーバから受信した取引処理の結果を通知して，処理を終える．

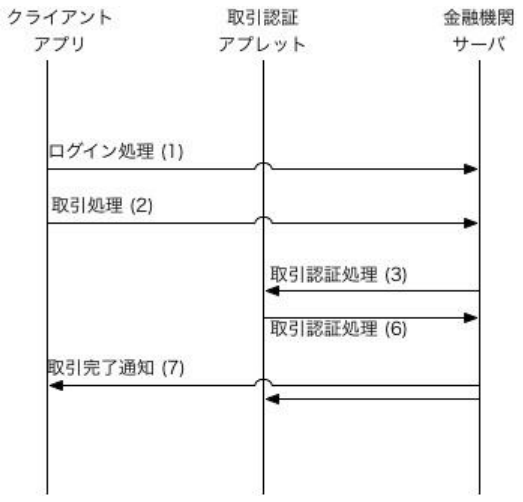

図 7 モバイルバンキング向け安全性向上策の処理フロー

4.2 インターネットバンキング向け安全性向上策

4.2.1 インターネットバンキング向け安全性向上策のシステム構成

提案方式のシステム構成を図 8 に示す．

提案システムは，図 1 に示したオンラインバンキングのモデルにおいて，クライアント端末に，PC とスマートフォン等の携帯電話を用いる構成である．

PC には, オンラインバンキングを行うためのブラウザ等のアプリがインストールされている．ユーザは，このアプリを利用して，取引を行う．

携帯電話には，SIM カードが備わっており，SIM カードには，先に述べた NAA，取引認証アプレットに加えて，PC に対するクライアント証明書を発行する中間認証局アプレットを搭載する．

SIM は，発行を行う通信事業者が情報を管理しており，携帯電話の契約時に，免許証やパスポート，健康保険証等の証明書類の確認を伴う本人確認を経て，SIM に記録される情報と契約者情報の関連付けが行われる．したがって，公的な証明書類を用いた本人確認が行われていることを担保できるセキュアデバイスであるといえる．

そこで，Java アプレットを用いて公開鍵証明書の発行機能を持つ認証局を実装することで, SIM や SIM が実装された携帯電話の所有者が，公開鍵証明書の発行を行える環境を実現する．

ここで発行された公開鍵証明書は，通信事業者などに Root 認証局を設置している場合，証明書の検証を行うことができる．

し, SIM 内パーソナル認証局が発行する証明書を用いて，二要素認証を実現する方式を説明する．

4.2.2 インターネットバンキング向け安全性向上策の処理フロー

提案方式における処理の流れを図 9 に示し，詳細を以下に説明する．

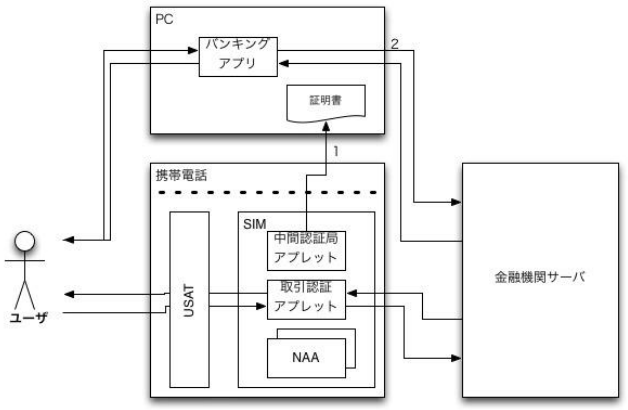

図 8 インターネットバンキング向け安全性向上策の構成

1. ユーザは, PC とスマートフォンの中間認証局アプリを用いて，PC に対するクライアント証明書の生成を行う．具体的には，PC で秘密鍵と公開鍵のペアを生成し，公開鍵をスマートフォンに送付する．続けて，スマートフォンの中間認証局アプリで，公開鍵証明書を作成し，PC に送信する．PC とスマートフォンの鍵や証明書の授受は，QR コードや Bluetooth などを用いることが考えられる．
2. ユーザは，クライアントアプリにアカウント情報を入力して，金融機関サーバにログインする．このとき，アカウント情報に基づくログイン認証とあわせて，Step で生成したクライアント証明書を用いた，端末認証も行う．
3. ログインに成功した場合, 以降の手順は, に順ずる．

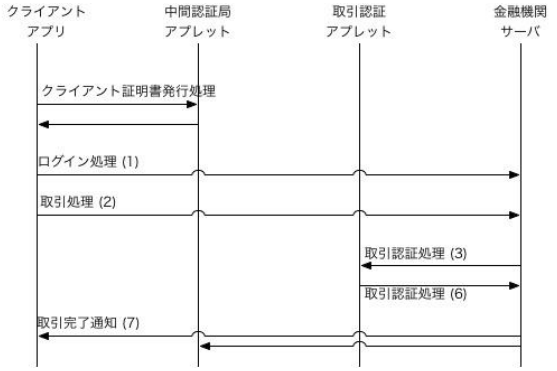

図 9 インターネットバンキング向け安全性向上策の処理フロー

5. おわりに

本論文では, PC や携帯電話から利用されるオンラインバンキングにおける，成りすましや取引改ざんの脅威に着目して，その安全性を向上する提案を行った．

オンラインバンキングにおいては，クライアント端末上で実行するソフトウェアがウイルスなどに感染することによって，正規のユーザによる正規の取引の裏側で，アカウント情報や認証情報の窃盗や，取引内容の改ざんが行われる，MitB 攻撃の脅威があることを整理した．MitB 攻撃への対策として，オンラインバンキングに用いるクライアント端末において，ハードウェアやソフトウェアを 2 つ以上に分ける，取引認証が有効であることに着目し，取引認証を実現するモジュールとして，携帯電話に備えられた SIM に着目した．

携帯電話単体でオンラインバンキングを行うモデルと，PC と携帯電話をあわせて使用するモデルのそれぞれについて，SIM で実行されるアプレットを用いた，取引認証や端末認証のためのクライアント証明書の発行の仕組みを提案した．

提案方式は，携帯電話に搭載される形で広く普及している SIM を用いる方式であることから，専用のハードウェアの導入などを伴わずに，低コストで実現できることが特徴となる．

今後は，PC や携帯電話のソフトウェアおよび OS への各種の攻撃を想定して，提案方式の安全性について，より仔細な検討と評価を行ってゆく．

参考文献

[1] “インターネット・バンキングにおける預金等の不正な払戻しについて”. http://www.zenginkyo.or.jp/topic/detail/nid/6389/,(参照 2016-08-12).

[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. 金融研究. 2013.7. p.51-76

[3] “Java Card Technology”. http://www.oracle.com/technetwork/java/embedded/javacard/overview/index.html, (参照 2016-08-12).

[4] 3GPP TS 31.102 v13.4.0 “Characteristics of the Universal Subscriber Identity Module (USIM) application”. 2016-06

[5] 3GPP TS 31.103 v13.1.0 “Characteristics of the IP Multimedia Services Identity Module (ISIM) application”. 2016-06

[6] “VISA payWave”. http://www.visa-news.jp/paywave/, (参照 2016-08-12).

[7] “MasterCardContactless”. http://www.mastercard.com/contactless/, (参照 2016-08-12).

[8] “GlobalPlatform”. https://www.globalplatform.org, (参照 2016-08-12).

[9] 3GPP TS 31.111 v13.4.0 “Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)”. 2016-06

[10] ETSI TS 102 221 v13.1.0 “Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)”. 2016-05