Vol.2017-CSEC-79 No.2
2017/12/4

モバイル端末を用いた金融サービスにおけるセキュリティ対策としてのセキュア・エレメントと TEE に関する一考察

宇根正志† 廣川勝久†

概要：スマートフォン等のモバイル端末を活用した金融サービスを安全に提供するうえで，サービス利用者や取引内容の確認，すなわち認証を適切に行うことが重要である．最近，モバイル端末を標的とする各種のマルウェアが報告されており，そうしたマルウェアによってモバイル端末上での認証が正しく行われなくなり，認証や金融取引にかかるデータが盗取されたり，改変されたりするリスクが懸念される．本稿では，こうしたリスクを軽減する手段として注目されているセキュア・エレメントと TEE（Trusted Execution Environment）を取り上げ，これらをどのように活用することができるかについて検討するとともに，今後の研究課題を示す．

キーワード：金融取引，セキュア・エレメント，認証，モバイル端末，TEE

A Study on Secure Elements and TEE as Security Measures for Financial Services with Mobile Devices

MASASHI UNE† KATSUHISA HIROKAWA†

Abstract: In order to provide with secure financial services through mobile devices such as smartphones and tablets, it is crucial to successfully carry out user and transaction authentication. Various types of malware targeting mobile devices have been recently reported. Those malware may cause security risks such as eavesdropping and manipulation of data or results related to authentication. In this paper, we will focus on secure elements and TEE, i.e., Trusted Execution Environment, as countermeasures against these risks and discuss how to adopt these technologies appropriately in financial services. We will also show future research topics regarding secure elements and TEE.

Keywords: authentication, financial transaction, secure element, mobile device, TEE

1. はじめに

近年，スマートフォンやタブレット端末（以下，まとめてモバイル端末という）を通じた金融サービスの提供が一段と活発化している．例えば，モバイル・バンキングに加え，口座情報サービスや決済指図伝達サービス等の新しい金融サービスがモバイル端末を通じて提供されている[1]．また，モバイル端末は，電子マネーや消費者信用の媒体としても活用されている[2]．こうしたなか，モバイル端末を用いたサービス利用者の本人確認や取引内容の確認，すなわち「認証」が，安心安全な金融サービスを実現するうえで一層重要となっている．

その一方，モバイル端末を対象とするマルウェアによる攻撃が，近年，益々高度化している．例えば，マルウェアによって内部のデータの盗取やアプリケーション・ソフトウェアの改変等を試みる攻撃が典型的である[3][4][5][6]．その他，モバイル端末の動作状況を詳細に観察することで，端末内部の暗号用の鍵を効率的に推測することが可能であるとの研究結果も報告されている[7][8][9]．こうしたマルウェアがさらに高度化し，金融サービス用のアプリケーション・ソフトウェアにおける認証処理を攻撃することが可能になれば，サービス利用者が入力する認証用データ（暗証番号や生体情報等）が盗取されたり，金融取引のデータが改ざんされたりするリスクが生ずる．

上記のような攻撃に対抗する方法として，セキュア・エレメント（Secure Element: SE）を活用するアプローチが注目を集めている．SE は，暗号処理等のセキュリティ機能を有するとともに，外部からの物理的な攻撃に対しても高い安全性を有するモジュールの総称であり，ハードウェアとソフトウェアを組み合わせて実現される．モバイル端末上に SE を装備することによって，通常の実行環境である REE（Rich Execution Environment，例えば Android OS）とは物理的かつ論理的に隔離された，より安全な実行環境を実現することができると期待される．また，SE に関連する実行環境であり，主にソフトウェアによって通常の実行環境から分離された安全な実行環境を実現する TEE（Trusted Execution Environment）の開発や実装も進められている．モバイル端末を利用した金融サービスを提供する金融機関等は，マルウェア等による攻撃の高度化に備えて，こうした新しい対策手法の動向をフォローすることが重要である．

本稿では，モバイル端末を用いた金融サービスにおける認証にかかる処理をより安全に実現するための技術として，

† 日本銀行 金融研究所 情報技術研究センター
Center for Information Technology Studies, Institute for Monetary and Economic Studies, Bank of Japan

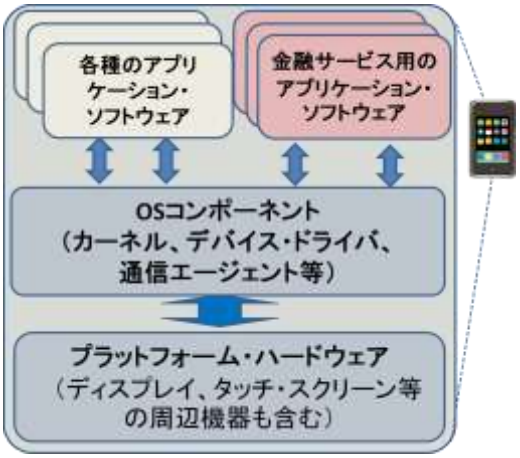

図 1　モバイル端末内部の構成例（概念図）

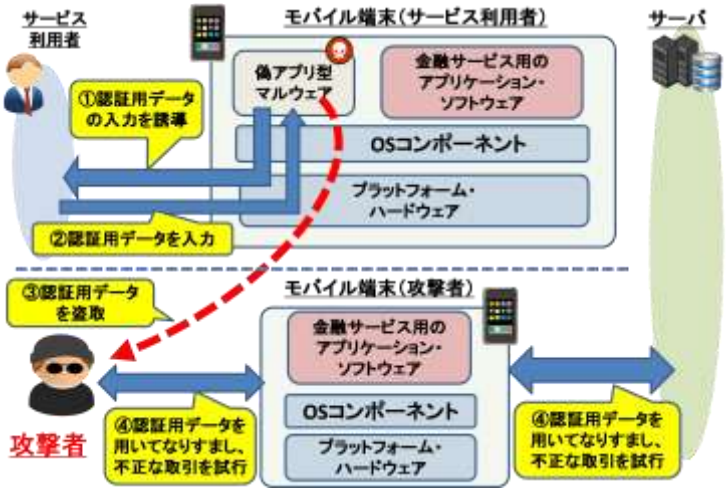

図 2　偽アプリ型のマルウェアによる攻撃の流れ（概念図）

SE および関連する実行環境としての TEE について考察する．本稿は，宇根・廣川が執筆した日本銀行金融研究所ディスカッション・ペーパーに基づいている[10].

まず，2 では，モバイル端末における認証のモデルおよびマルウェアへの対策方針を示す．3 では，SE と TEE の概要を説明し，4 では，それらの実行形態を分類して各形態の留意点を示す．5 では，金融機関等が今後 SE や TEE を活用していく際の主な課題を考察する．

なお，本稿で示されている意見は，すべて著者たち個人に属し，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著者たち個人に属する．

2. モバイル端末を用いた金融サービスと認証

2.1 エンティティと認証

モバイル端末で金融サービスを処理するためのシステムは，主に次の 4 つのエンティティから構成される．すなわち，①当該サービスを提供する金融機関や FinTech 企業（以下，金融機関等），②金融機関等が管理し，サービスの提供にかかる処理を実行するサーバ，③金融機関等が提供するサービスを利用する個人であるサービス利用者，④サービス利用者が有するモバイル端末である．金融サービスにかかるデータの処理や通信は，サーバとモバイル端末間で行われる．

ここでは，サービス利用者の本人確認（利用者認証）と取引内容の確認（取引認証）にフォーカスする．利用者認証では，サーバからの認証要求がモバイル端末のユーザ・インタフェースを通じてサービス利用者に伝えられ，サービス利用者が認証用データ等をモバイル端末に入力する．認証用データがモバイル端末で処理された後，モバイル端末で認証の成否が判定されるケース（以下，端末判定型）と，サーバで判定されるケース（以下，サーバ判定型）が考えられる．端末判定型では，認証用データを検証するためのデータが予めモバイル端末に格納され，判定結果がサーバに送信される．

取引認証では，サーバから取引内容のデータがモバイル端末に送信され，モバイル端末で処理された後，取引内容がディスプレイに表示される．サービス利用者は，表示内容を確認し，承認するか否かを示すデータ（OK や NG を表すデータ等）を入力する．当該データは，モバイル端末で処理された後，サーバに送信される．

モバイル端末は，主に，プラットフォーム・ハードウェア（ディスプレイ，タッチ・スクリーン，CPU，メモリ，通信機器等），OS コンポーネント（カーネル，デバイス・ドライバ，通信エージェント等），アプリケーション・ソフトウェアによって構成される（図 1 を参照）．金融サービス用のアプリケーション・ソフトウェアは，通常，金融機関等によって準備され，サービス利用者によってインストールされる．また，認証処理は，金融サービス用のアプリケーション・ソフトウェアによって実行されている．

2.2 保護対象のデータとマルウェアによるリスク

マルウェアがモバイル端末に侵入した場合，認証用データと取引内容の確認にかかるデータを保護することが最重要の課題となる．これらがさらされるリスクはマルウェアの性質に依存する．ここでは，攻撃形態の観点から，井澤・五味による偽アプリ型と凶悪型の分類を引用し，それぞれのマルウェアによる攻撃とリスクを整理する[11].

2.2.1 偽アプリ型のマルウェア

偽アプリ型のマルウェアは，正規の金融サービス用のアプリケーション・ソフトウェアとは別のアプリケーション・ソフトウェアとしてインストールされ，正規のソフトウェアのデータにはアクセスできないものと定義される．例えば，正規のソフトウェアに不正なコードを埋め込んで再配布したもの（リパッケージング）が挙げられる[11][12].

偽アプリ型のマルウェアは，正規のソフトウェアを装って認証用データの入力をサービス利用者に促し，入力された認証用データを盗取する可能性がある（図 2 を参照）．認

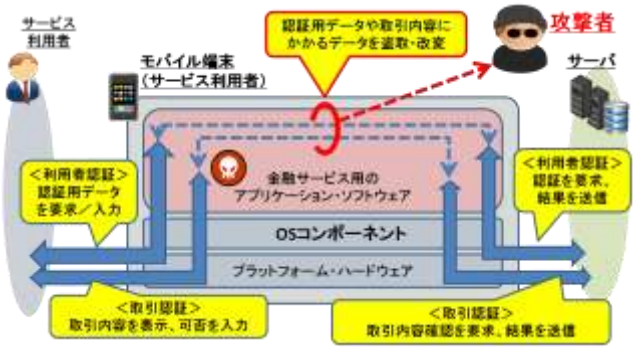

図 3　凶悪型のマルウェアによる攻撃の流れ（概念図）

証用データが盗取されると，利用者認証が適切に機能せず，攻撃者がサービス利用者の端末以外のモバイル端末（金融サービス用のアプリケーション・ソフトウェアがインストールされたもの）に認証用データを入力してなりすましを成功させるおそれがある．

2.2.2 凶悪型のマルウェア

凶悪型のマルウェアは，正規の金融サービス用のアプリケーション・ソフトウェアのデータにアクセスすることが可能であり，当該ソフトウェアで処理されるデータの盗取やプログラムの改変を実行できるものと定義される．これは，正規の金融サービス用のアプリケーション・ソフトウェアを装ってインストールされることもあれば，全く別のソフトウェアとしてインストールされることもある．

凶悪型のマルウェアは，利用者認証にかかる認証用データを盗取する可能性がある（図 3 を参照）．また，サービス利用者が入力した取引内容のデータや，サーバがサービス利用者に向けて送信したデータを改変する可能性もある．取引認証においては，サーバからサービス利用者に送信された取引内容を，モバイル端末のディスプレイへの表示時に改変したり，サービス利用者が入力した取引可否を示すデータを改変したりする可能性が考えられる．

2.3 マルウェアによる攻撃への対策方針

2.3.1 偽アプリ型のマルウェアの場合

偽アプリ型のマルウェアによる認証用データの盗取やなりすましのリスクに対しては，不正なアプリケーション・ソフトウェアのインストールを防ぐこと（対策方針 1）が第 1 に求められる．例えば，アプリケーション・ソフトウェアの作成者情報や当該ソフトウェアに対する不正な改変の有無を検証するために，デジタル署名（コード署名と呼ばれる）等を当該ソフトウェアに付与するなどの対応が考えられる．同時に，コード署名が付与されていないソフトウェアを極力インストールしないようにサービス利用者に促すことも，こうした対応に含まれる．

もっとも，コード署名等による対応がモバイル端末によっては困難なケースもありうるほか，ソフトウェアの不正な改変が検知できずに正規のソフトウェアとして配布されるケースもありうると考えられる．その場合，コード署名の検証は無効となることから，追加的な対応として，モバイル端末とサービス利用者の対応関係を検証する手段を利用すること（対策方針 2）が考えられる．例えば，モバイル端末内部に，当該端末を所有するサービス利用者と対応付けられた鍵を格納しておき，認証時に，認証用データや当該取引に固有のデータ（例えば，取引日時データ）等のデジタル署名を生成し，当該署名とサービス利用者の対応関係をサーバが検証するという方法がありうる．

2.3.2 凶悪型のマルウェアの場合

凶悪型のマルウェアに対しては，正規の金融サービス用のアプリケーション・ソフトウェアと同じパーミッションを有し，認証用データ等にアクセスできることから，上記の対策方針 1, 2 では攻撃によるリスクを十分に軽減できるとはいえない．そのため，当該マルウェアの影響が極力及ばない環境で認証にかかる処理を実行すること（対策方針 3）といった対応が求められる．具体的なアプローチとして，ハードウェアを組み合わせた SE の活用が注目を集めている．このアプローチを採用するには専用のハードウェアが必要となるものの，今後，凶悪型のマルウェアによる攻撃がさらに高度化していく可能性に鑑みると，こうした対応が益々重要になってくると考えられる．

3. セキュア・エレメント等とその活用条件

本節では，SE および関連する実行環境としての TEE の概要を説明する．次に，モバイル端末での活用条件を整理し，凶悪型のマルウェアによる攻撃において活用条件がどう充足されるかを検討する．

3.1 SE

3.1.1 認証処理に関する 3 つの条件

SE の定義は文献によって区々であるが，共通点を抽出すると，「(複数の) アプリケーションをその内部で実行する機能を有するモジュールであり，記録された重要情報の保護と暗号や認証等のセキュリティにかかる処理を実行するとともに，ハードウェアに基づく耐タンパー性によって，外部からの物理的な攻撃に対しても一定の安全性を確保できるもの」と表現することができる[13]. 凶悪型のマルウェアによる影響を排除するために，SE をモバイル端末に搭載し認証処理を実行することが考えられる．

SE による認証処理が有効となるためには，以下の 3 点を満たすことが求められる．

- 条件①：SE 内部で認証にかかる処理を行うアプリケーション・ソフトウェア（以下，SE アプリ）が改変されないこと．
- 条件②：SE アプリとサーバの間の通信データが盗取・改変されないこと，または暗号化等によって保護されること．

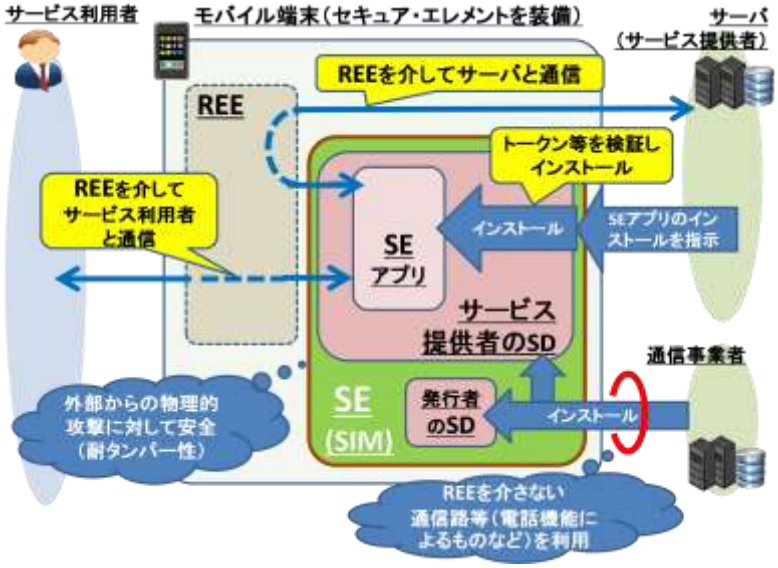

図 4　セキュア・エレメントの機能（概念図）

・条件③ : SE アプリとサービス利用者の間の通信データが盗取・改変されないこと.

これらの条件がモバイル端末の SE においてどのように充足されるかを，モバイル端末における代表的な SE である SIM（Subscriber Identity Module）を前提に説明する.

3.1.2 SIM の構成と管理機能

SIM 内部の SE アプリのインストールや削除等は，同じく内部に組み込まれる管理用ソフトウェアであるセキュリティ・ドメイン（Security Domain: SD）によって制御される（図 4 を参照）. 通信事業者が自身の SD を SIM に導入することに加え, SIM を活用するサービス提供主体(以下，サービス提供者）がサービス用の SD を準備し，通信事業者の承認を得てインストールするケースが想定される[14][15]. 金融サービス用の SD の場合，金融機関等が通信事業者の承認のもとで SIM に導入することが考えられる.

SIM に SE アプリをインストールする際には，サービス提供者のサーバとサービス用の SD が相互認証や鍵共有を行った後，サーバが，当該 SE アプリのインストールを承認した証となるデータ（トークンと呼ばれ，サーバの署名等が付与される）を当該 SD に送信する. SD は，トークンを検証し，検証に成功した場合に SE アプリをインストールする. SE アプリの更新等の処理も同様の流れで行われる.

3.1.3 認証処理に関する 3 つの条件との関係

認証処理に関する 3 条件に鑑みると，SE としての SIM の利用は次のように評価できる.

条件①の SE アプリの改変に関しては，SE アプリをアンインストールして不正なソフトウェアをインストールする，あるいは, SE アプリに不正な変更を加えるなどの攻撃が考えられる. これに対しては，サーバと SD（あるいは SIM）の間の相互認証や暗号通信のプロトコル，デジタル署名等の暗号方式，署名生成鍵の管理等に問題がなければ，SE アプリへの攻撃は成功しないと考えられる.

条件②の SE アプリとサーバの間の通信データの盗取・改変に関しては，SD が相互認証や鍵共有にかかる暗号処理を SE アプリに提供することが想定されており，これを利用したエンド･ツー･エンドでの暗号化によって通信データの盗取・改変は困難になると考えられる[14].

条件③の SE アプリとサービス利用者の間の通信データの盗取・改変に関しては，サービス利用者が SE アプリとエンド・ツー・エンドでの暗号通信を実行することは困難であることから，サービス利用者との通信の安全性をどう確保するかが留意点となる.

3.2 SE に関連する実行環境としての TEE

3.2.1 認証処理に関する 3 つの条件

SE の特徴は, 耐タンパー性を有するハードウェアを利用することで物理的な攻撃に対しても安全性を確保することができるように設計されている点にある. ただし，メモリ等の計算リソースの制約が REE に比べて厳しくなるほか，サービス利用者との通信は REE を介して行う必要がある. こうした問題への対応として TEE を活用するアプローチが注目されている. TEE は REE から隔離された実行環境であり，その実現方法に関する各種の仕様が GlobalPlatform によって策定・公開されている[16][17][18][19][20][21][22].

TEE は，SE と異なり，基本的にソフトウェア・ベースの技術によって実現されると同時に，外部からの物理的な攻撃に対する耐タンパー性は想定されていない（図 5 を参照）. また，TEE を利用するためには，TEE を実装するモバイル端末を準備する必要がある. REE 上の凶悪型のマルウェアに対抗するために，TEE で動作するアプリケーション・ソフトウェア（Trusted Application: TA）で認証処理を実行し，それ以外の処理を，REE 上の金融サービス用のアプリケーション・ソフトウェアで実行することが考えられる.

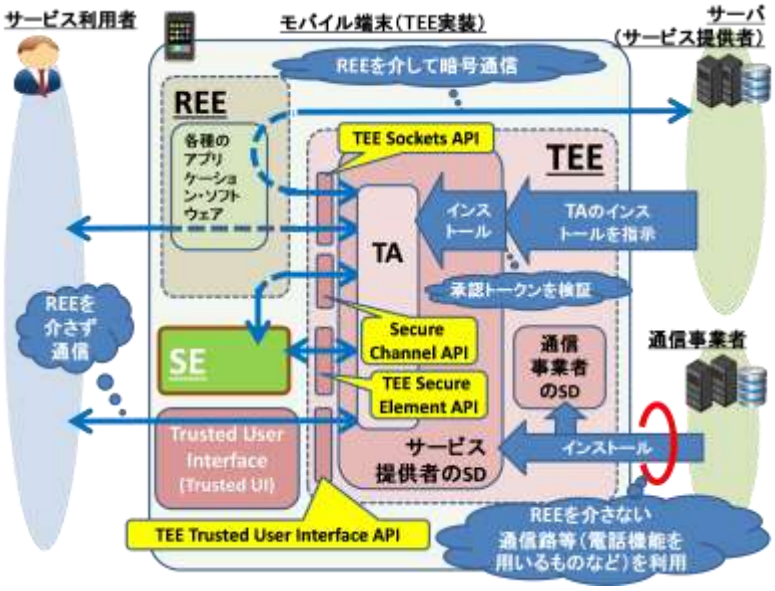

図 5　TEE の機能（概念図）

その際，マルウェアに対する耐性を確保するために，SE の場合と同様に，以下の 3 点を満たすことが求められる．

・条件①：認証にかかる処理を行う TA を改変させないこと．
・条件②：TA とサーバの間の通信データの盗取・改変を防止すること，または暗号化等によって保護すること．
・条件③：TA とサービス利用者の間の通信データの盗取・改変を防止すること．

3.2.2 TEE の構成と管理機能

通常のモバイル端末では，REE 上に単一の OS コンポーネントが存在し（Rich OS，例えば Android OS 等），サービス利用者がアプリケーション・ソフトウェアをインストールして動作させることができる．一方，TEE を利用するケースでは，モバイル端末内部に，Rich OS と，TEE 用の OS コンポーネント（Trusted OS）が存在する．Trusted OS が REE から TEE へのアクセスを制御する．

TA のインストールや変更等の管理機能は，SE の場合と同様に，サーバによる承認の証となるデータ（承認トークン＜authorization token＞）に基づいて，SD によって制御される[20]．承認トークンにはサーバによるデジタル署名が付与されており，SD はその署名を検証することによって承認トークンの正当性を確認する．

3.2.3 認証処理に関する 3 つの条件との関係

認証処理に関する 3 条件に鑑みると，TEE の利用を次のように評価できる．

条件①の TA の改変に関しては，TA を改変するためには，攻撃者がサーバになりすまして当該 SD と相互認証を行った後，承認トークンを偽造して SD に送信しなければならない．したがって，サーバと SD の間の相互認証や暗号通信のプロトコル，承認トークンの生成・検証に用いられるデジタル署名等の暗号方式，署名生成用の鍵の管理等に問題がなければ，攻撃は成功しないと考えられる．

次に，条件②の TA とサーバの間の通信データの盗取・改変に対しては，データをエンド・ツー・エンドで暗号化する，または，マルウェアによる影響が及ばない通信路を利用する（セキュア・チャネル・プロトコル）といった対策が考えられる．例えば，TA が TEE Sockets API 等を利用して外部のエンティティと暗号通信路（TLS 等を利用）を確立することが考えられる[20][21][22]．また，TEE と SE が接続されている場合，TA は SE 経由でサーバと通信することも考えられる．TA が，SE アプリとの間で通信するためのインタフェースである TEE Secure Element API を利用して SE アプリと通信し，続いて，SE アプリとサーバの間の通信路を介して通信するというものである[19]．SE が REE に接続され，TA が REE を介して SE と通信するケースもある．その場合，Secure Channel API を利用して暗号通信路を確立したうえで通信することが想定される．

条件③の TA とサービス利用者の間の通信データの盗取・改変に関しては，サービス利用者が TA と直接暗号通信を実行することは困難であり，REE を介さない通信路を別途準備するなどの対応が必要となる可能性がある．こうした場合でも安全な通信路として，TEE にはオプションとして Trusted UI（Trusted User Interface）があり，そのインタフェースとして TEE Trusted User Interface API が規定されている[16][20]．この API は，TA がモバイル端末のタッチ・スクリーン等を介してサービス利用者とデータを安全に交信するための機能を提供する．TEE Trusted User Interface API を利用するための機能やデバイスを備えたモバイル端末を利用できる場合であれば，Trusted UI による

表 1　認証の実行形態の分類

タイプ名	TEE の有無	SE の有無	認証にかかる処理の実行箇所と実行主体
RS 型	なし	あり（REE に装着）	SE（実行主体：SE アプリ）
RS-T（TA）型	あり	あり（REE に装着）	TEE（実行主体：TA）
RS-T（SE）型			SE（実行主体：SE アプリ）
R-TS（TA）型		あり（TEE に装着）	TEE（実行主体：TA）
R-TS（SE）型			SE（実行主体：SE アプリ）

通信を活用することが考えられる．

4. SE や TEE による認証の実行形態

モバイル端末上での金融サービスにおいて SE 等を活用して認証処理を実行する場合，認証の実行形態として複数のバリエーションが想定される．今後，それらが新しいモバイル端末上で実現され，金融機関等も金融サービスの認証に SE 等を活用できるようになる可能性がある．そうした状況を展望して, SE 等を活用した認証の実行形態を整理し，各実行形態での対策方針や安全性上の留意点を示す．

4.1 実行形態の分類

モバイル端末上での実行環境としては，SE と REE の組合せ, あるいは, SE と REE と TEE の組合せが想定される．SE が REE もしくは TEE に装着されるケースも考えられる．これらを踏まえると, 実行環境として想定されるのは, REE と SE の組合せ（以下，RS 型），「SE が装着された REE」と TEE の組合せ（以下，RS-T 型），REE と「SE が装着された TEE」の組合せ（以下, R-TS 型）の 3 つとなる．なお，SE として SIM を想定する場合，通常のモバイル端末との組合せで実現可能であり，その意味で RS 型の受け皿となる端末は現在広く利用されているといえる．一方，TEE を利用可能なモバイル端末は一部に止まっており，今後の普及が期待される．

RS-T 型と R-TS 型は, 認証にかかる処理を担う主体が TA の場合と SE アプリの場合があり, 2 つのタイプに分類できる．RS-T 型において，認証にかかる処理を TA が担うものを RS-T（TA）型と呼び, SE アプリが担うものを RS-T（SE）型と呼ぶ．また，R-TS 型において，認証にかかる処理を TA が担うものを R-TS（TA）型と呼び，SE アプリが担うものを R-TS（SE）型と呼ぶ．この結果，認証の実行形態は論理的には 5 つに分けられる（表 1 を参照）．

ここで，利用者認証については，①サービス利用者への認証用データ要求の送信，②サービス利用者からの認証用データの受信，③サーバへの認証用データの転送あるいは判定結果の送信を含む．取引認証については，①サーバからの取引認証要求の受信，②サービス利用者への確認要求の送信，③サービス利用者からの確認結果の受信，④サーバへの確認結果の送信を含む．

これらの実行箇所としては，TEE あるいは SE を想定する．TEE で実行する場合には，認証処理用の TA が安全にインストールされていることとする．他方，SE で実行する場合には，認証処理用の SE アプリが安全にインストールされていることとする．

4.2 各実行形態における攻撃への対策方針

凶悪型のマルウェアが金融サービス用のアプリケーション・ソフトウェア（Rich OS Application: RA）として REE 上で動作する場合の対策方針を，各実行形態について検討する．TEE と SE による内部のデータやソフトウェアの保護・管理機能は有効であるとするほか，TEE と SE の内部のデータ（暗号用の秘密鍵等）の盗取・改変や，TA や SE アプリの改変はマルウェアにとって実行困難であるとする．なお, RA は, TA のように, 信頼できるソフトウェアとして確認されるわけではない．

RS 型は，REE に SE が装着され，SE アプリが認証処理を実行するタイプである．サーバとの通信は, SE アプリが, データを暗号化したうえで REE を介して行うことが考えられる．SE アプリがセキュア・チャネル・プロトコルを利用できる場合，それによって，通信事業者等を経由することを含めて，サーバと接続することも考えられる．サービス利用者との通信は，REE を介することとなり，マルウェアによる通信データの盗取・改変に留意する必要がある．

RS-T（TA）型は，REE と TEE が併存し，SE が REE と直接通信するタイプであり，認証処理は TA によって実行される．サーバとの通信は，TA がサーバの公開鍵等を用いてデータを暗号化し，REE を介して行うことが可能である．また，TA が，セキュア・チャネル・プロトコルを利用可能な場合，それによってサーバとの間で通信路を確立することも考えられる．なお，TA が，SE アプリとの間で暗号化等による通信を行うとともに，通信事業者等を経由することを含めて，サーバとの間でセキュア・チャネル・プロトコルを利用することも選択肢となりうる．サービス利用者との通信は，Trusted UI を利用できれば安全に行うことができる. そうでない場合, REE を介して行うため, マルウェアによる通信データの盗取・改変に留意する必要がある．

RS-T（SE）型は，REE と TEE が併存し，SE が REE と直接通信するタイプであり，認証処理は SE アプリによって実行される．サーバとの通信は，SE アプリがサーバの公開鍵等を用いてデータを暗号化し，REE を介して行うことが可能である．また，SE アプリは，サーバや通信事業者等との間でセキュア・チャネル・プロトコルを利用可能な場合，それによって安全な通信路を確立することも考えられ

表 2　各実行形態におけるマルウェアの攻撃への対策方針や留意点

タイプ名	対策方針や留意点	
	サーバとの通信	サービス利用者との通信
RS 型	・通信データを暗号化し REE を介して通信. ・SE あるいは TEE のセキュア・チャネル・プロトコルを利用.	REE を介して通信するため，通信データの盗取・改変に留意.
RS-T（TA）型		Trusted UI を利用．そうでない場合，REE を介して通信するため，通信データの盗取・改変に留意.
RS-T（SE）型		
R-TS（TA）型		
R-TS（SE）型		

る．なお，SE アプリが，TA との間で暗号化等による通信を行うとともに，TA とサーバの間でセキュア・チャネル・プロトコルを利用することが可能な場合，REE および TA を経由してサーバと通信することも選択肢となりうる．サービス利用者との通信は，SE アプリがデータを暗号化して REE 経由で TA に送信した後，Trusted UI を利用できる場合には，それを介して行うことができる．Trusted UI を利用できない場合，REE を介して行うため，マルウェアによる通信データの盗取・改変に留意する必要がある．

R-TS（TA）型は，REE と TEE が併存し，SE が TEE と直接通信するタイプであり，認証処理は TA によって行われる．サーバとの通信は，TA がサーバの公開鍵等を用いてデータを暗号化し，REE を介して行うことが可能である．また，TA がセキュア・チャネル・プロトコルを利用できる場合，サーバとの間で通信路を確立することも考えられる．なお，TA が，SE アプリとの間で暗号化等による通信を行うとともに，通信事業者等を経由することを含めて，サーバとの間でセキュア・チャネル・プロトコルを利用することも選択肢となりうる．サービス利用者との通信は，Trusted UI を利用できる場合，安全に行うことができる．そうでない場合には，REE を介して行うため，マルウェアによる通信データの盗取・改変に留意する必要がある．

R-TS（SE）型は，REE と TEE が併存し，SE が TEE と直接通信するタイプであり，認証処理が SE アプリによって行われる．サーバとの通信は，サーバの公開鍵等を用いてデータを暗号化し，TEE と REE を介して行うことができる．SE アプリが，通信事業者等を経由することを含めて，サーバとの間でセキュア・チャネル・プロトコルを利用することも考えられる．なお，SE アプリが，TA とサーバの間でセキュア・チャネル・プロトコルが利用できる場合，暗号化したデータを TA 経由でサーバに送信することも選択肢となりうる．サービス利用者との通信は，TA を介して Trusted UI を利用できる場合，安全に行うことができる．Trusted UI を利用できない場合，REE を介して行うため，通信データの盗取・改変に留意する必要がある．

4.3 対策方針のまとめ

SE アプリや TA によるサーバとの通信は，いずれも，データを暗号化する，または，可能な場合にはセキュア・チャネル・プロトコルを利用するという対応が考えられる（表 2 を参照）．データの暗号化に関しては，SE アプリや TA にこうした機能が備わっている場合が多いとみられるが，通信相手（サーバ等）の公開鍵や署名検証用の電子証明書等を事前に入手することなどが別途必要であり，これらの管理について留意が求められる．また，セキュア・チャネル・プロトコルを利用するためには，TEE あるいは SE が REE を介さず通信するための通信用デバイスが必要になる場合がある．

SE アプリや TA によるサービス利用者との通信は，エンド・ツー・エンドでの暗号通信が困難であり，REE を経由しない通信路の利用がまず考えられる．RS 型以外のタイプでは，Trusted UI を利用するという選択肢がありうる．もっとも，これはオプションとされている機能であり，専用のデバイス等が必要となる場合もある．

このようにみていくと，SE アプリや TA の実行形態として複数の選択肢が存在するなかで，サーバやサービス利用者との通信の安全性を確保することが重要な課題であり，とりわけ，SE アプリや TA によってサービス利用者との通信をどう実現するかが重要であるといえる．

5. SE 等の活用における今後の課題

4 では SE（SE アプリ）や TEE（TA）による認証処理の実行形態を分類し，対策方針と留意点を示した．これらを踏まえ，金融機関等が SE 等を活用した認証処理を実現するための主な課題について考察する．

まず，金融機関等は，金融サービス用のアプリケーション・ソフトウェアに加えて，認証処理用の SE アプリや TA，これらを管理するための SD 等を用意し，サービス利用者が自分のモバイル端末にインストールするための環境を整備する必要がある．そのためには，SE や TEE を管理する主体である通信事業者やモバイル端末ベンダー等（以下，通信事業者等）と連携して検討を進めることが求められる．その際，①認証処理の実行形態，②モバイル端末への SE アプリ，TA，SD 等の導入方法，③通信事業者等との役割分担が検討項目になると考えられる．

上記①の認証処理の実行形態に関しては，サービス利用者との通信をどう保護するかが課題となる．サービス利用者との通信は，エンド・ツー・エンドでの暗号化が困難である．しかし，Trusted UI を備えたモバイル端末であれば，

それを介して安全に行うことができる(RS 型を除くタイプが該当)．もっとも，現時点では，TEE や Trusted UI を利用可能なモバイル端末は一部に限られ，別の手段で対応せざるを得ない端末も存在する．このため，足許では，Trusted UI を前提としない SIM のみを利用した手法が候補になると考えられる[5][23].

上記②のモバイル端末への SE アプリ等の導入方法については，SE や TEE が製品レベルで期待どおりの機能を有していることをどう確認するかが重要な課題である．SE に関しては，コモン・クライテリア（Common Criteria）に基づく評価・認証や米国連邦政府や日本の暗号モジュールにかかる認証スキーム（CMVP／JCMVP）による認証の有無とその内容がベンチマークになる[24]．こうした認証は，対象の製品が一定の安全性を確保していることを示す証となり，金融機関等がセキュリティ要件の充足度合いを確認するだけでなく，サービス利用者の安心感や信頼感を醸成するうえでも重要である．最近では，Trusted OS コンポーネント等がコモン・クライテリアに基づく評価・認証を取得した事例も知られている[25]．今後，こうした事例が増加することが期待される．

さらに，SE や TEE の安全性に問題がないとしても，SE アプリや TA が期待した動作を行わない場合，モバイル端末上での安全な認証を実現できなくなる可能性がある．したがって，SE や TEE へのインストールが許容される SE アプリや TA の品質の適切性をいかに確保するかが課題となる．モバイル端末上での処理を安全に実行する手段として SE や TEE が一段と注目されるようになれば，金融機関等のサービス提供者だけでなく，さまざまなベンダーが SE アプリ等を開発・提供するようになり，不正な SE アプリ等にかかるリスクが高まっていく可能性がある．そうしたリスクへの対応として，SE アプリや TA を作成するための開発ツールの提供，正規の SE アプリや TA の認証，セキュア・チャネル・プロトコル等による安全な通信路を介したインストール等が検討項目として考えられる．これらについて，金融機関等は，通信事業者等と連携しつつ，役割分担を明確にしながら検討を進めていく必要がある．

SE や TEE の最大の特徴は，金融機関等がサービス利用者のモバイル端末内部に，信頼できる実行環境とアプリケーション・ソフトウェアを実現する仕組みを提供する点にあるといえる．インターネットを介したオンライン・バンキング等では，これまでパソコンによる利用が中心となっているが，残念ながら，サービス利用者のパソコン内部に同様の信頼できる実行環境等を実現するに至っておらず,マルウェアによる脅威にさらされる状況が続いている．金融サービスを利用する媒体としてのモバイル端末の普及と歩調を合わせて SE の活用を検討するとともに，今後の普及が期待される TEE や Trusted UI の活用を検討することは，上記のパソコンにおける状況からの改善や脱却という観点からも重要であると考えられる．

金融サービスにおけるモバイル端末のさらなる活用を展望する金融機関等においては，通信事業者，モバイル端末ベンダー，SE や TEE のベンダー等，関係者と密接に連携しつつ検討を進めていくことを期待したい．

参考文献

[1] 中村啓佑．金融分野の TPPs と API のオープン化：セキュリティ上の留意点．金融研究. 2017, 36 (3), pp. 83-110.
[2] 日本銀行決済機構局．モバイル決済の現状と課題．決済システムレポート別冊シリーズ. 2017.
[3] Marczak, B. and Scott-Railton, J.. The Million Dollar Dissident: NGO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Citizen Lab. August 24, 2016.
[4] Pan, J.. User Beware: Rooting Malware Found in 3rd Party App Stores. TrendLabs Security Intelligence blog. 2016.
[5] 大塚玲ほか. SIM-Sign：実用的な Android 端末向け MitMo 対策技術．コンピュータセキュリティシンポジウム 2016 予稿集. 2016.
[6] Taylor, V. F. and Martinovic, I.. Short Paper: A Longitudinal Study of Financial Apps in the Google Play Store. Proc. of Financial Cryptography and Data Security 2017. 2017.
[7] Lipp, M. et al.. ARMageddon: Cache Attacks on Mobile Devices. Proc. of the 25th USENIX Security Symposium. 2016, pp. 549-564.
[8] Timmers, N. and Spruyt, A.. Bypassing Secure Boot using Fault Injection. Black Hat Europe 2016. 2016.
[9] Irazoqui, G. and Guo, X.. Cache Side Channel Attack: Exploitability and Countermeasures. Black Hat Asia 2017. 2017.
[10] 宇根正志，廣川勝久．モバイル端末による金融サービスの安全性を高めるために：セキュア・エレメント等の活用. IMES Discussion Paper Series. 2017, no. 2017-J-15.
[11] 井澤秀益，五味秀仁．次世代認証技術を金融機関が導入する際の留意点 : FIDO を中心に．金融研究. 2016, 35 (4), pp. 21-54.
[12] European Union Agency for Network and Information Security. Security of Mobile Payments and Digital Wallets. 2016.
[13] Elenkov, N.. Android Security Internals: An In-Depth Guide to Android's Security Architecture. No Starch Press. 2015.
[14] GlobalPlatform. Card Specification version 2.3. Document Reference: GPC_SPE_034. 2015.
[15] GlobalPlatform. The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market. 2015.
[16] GlobalPlatform. Trusted User Interface API version 1.0. 2013
[17] GlobalPlatform. TEE Protection Profile version 1.2. 2014.
[18] GlobalPlatform. TEE Management Framework version 0.0.038, 2016.
[19] GlobalPlatform. TEE Secure Element API version 1.1.1. 2016.
[20] GlobalPlatform. TEE System Architecture version 1.0.0.27. 2016.
[21] GlobalPlatform. Annex C: TLS Specification of TEE Sockets API Specification version 1.0.1. 2017.
[22] GlobalPlatform. TEE Sockets API Specification version 1.0.1. 2017.
[23] 磯原隆将，竹森敬祐，本間輝彰. 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．コンピュータセキュリティシンポジウム 2016 予稿集. 2016.
[24] 田村裕子，宇根正志．情報セキュリティ製品・システムの第三者評価・認証制度について: 金融分野において利用していくために．金融研究. 2008, 27 (1), pp. 53-100.
[25] Trustonic. Trustonic device security platform achieves world's first TEE security certification from Common Criteria. Trustonic Press Releases. March 16, 2017.
[26] GlobalPlatform. GlobalPlatform Launches Developers' Kit to Ease and Expedite Development of Secure Mobile Services. 2017.