携帯電話を用いた権限委譲方式の提案とセキュリティ検証

山越 公洋† 山本 英朗† 森田 哲之† 菅沼 毅†

†日本電信電話株式会社 NTTセキュアプラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11
E-mail: †{yamakoshi.kimihiro, yamamoto.hideaki, morita.t, suganuma.takeshi}@lab.ntt.co.jp

あらまし IC カードに登録された本人証明書を活用して、スマートフォンなどを用いて認証サービスを安全に実現可能な方式を提案する。提案方式では、トークン発行局が IC カードの本人証明書を元にスマートフォンで利用可能な認証権限(トークン)を発行、管理する。トークンを発行する際に、PKI の連鎖署名を利用した権限委譲をおこなう。利用者が所有するスマートフォンに対してトークンを発行したことを保証するために、IC カードに対してスマートフォンの署名が付いた自己署名型のチャレンジレスポンス認証を用いる。これにより、IC カードにスマートフォンの公開鍵証明書の発行元認証局の公開鍵を事前にインストールすることを必要とせず、所有者のスマートフォンに認証権限を安全に発行することが可能となる。スマートフォンで認証サービスを利用する際は、トークンを認証サーバに送信するとともにチャレンジレスポンス認証をおこなうことにより、トークンのコピーを利用したなりすましを回避する。提案方式の Android OS 搭載スマートフォンへの実装を前提に、CC 認証のスキームに従い脅威と前提条件を定義してセキュリティ検証を実施した。

A proposal and security verification for authority transfer with smart-phone

Kimihiro Yamakoshi† Hideaki Yamamoto† Tetsushi Morita† Takeshi Suganuma†

†NTT Secure Platform Laboratories
9-11, Midori-Cho 3-Chome Musashino-Shi, Tokyo 180-8585, Japan
E-mail: †{yamakoshi.kimihiro, yamamoto.hideaki, morita.t, suganuma.takeshi}@lab.ntt.co.jp

Abstract We propose an authentication method for personal identification using a smart-phone utilizing a personal identification public key certificate issued to IC-card. Token-issuer issues and manages a token for a smart-phone from a public key certificate in IC-card. Token is issued by similar way as PKI based signature-chain mechanism. Self-signature by smart-phone is used for challenge to IC-card to guarantee that a token is issued to an owner's smart-phone from an owner's IC-card. This makes it possible to realize safe token-issue from an IC-card to a smart-phone without installing a public key of CA for smart-phones to IC-card in advance. PKI based challenge-response also avoids replay attack with used token. We made security verification based on CC authentication defining threat and presumption for the system in the case of adopting our method to smart-phones with Android OS.

1 はじめに

PKI 認証に必要な本人情報を IC カードに登録し、IC カードを用いた本人証明やポータルサイトへのログイン、電子申請などを可能とするサービスが自治体により実現されている[1]。これらのサービスでは、IC カード毎に認証局から発行された公開鍵証明書と秘密鍵のペアがセキ

ュリティ実現の要となる。公開鍵証明書の属性情報として、公的に保証された本人情報が登録され、秘密鍵により署名生成が可能である。

Android OS 搭載スマートフォンでは、NFC（近距離無線通信）[2]機能を搭載しており IC カードとの通信が可能である。IC カードに対して発行された認証権限を利用者の意志でスマートフォンに安全に委譲できれば、図 1 に示すようにスマートフォンだけで店舗などでのオフライン認証に加えネットワーク経由でのオンライン認証が可能となり利便性の向上が期待できる。

個人認証サービスでは、本人であることを確認した上で本人情報を発行する手続きが最も重要かつ手間のかかる作業であるため、保証済の本人情報を個人のスマートフォンなどにそのまま安全に格納できれば、従来郵送や窓口で身分証明が必要であった銀行口座開設などのサービスをオンラインでおこなうことが可能となる。

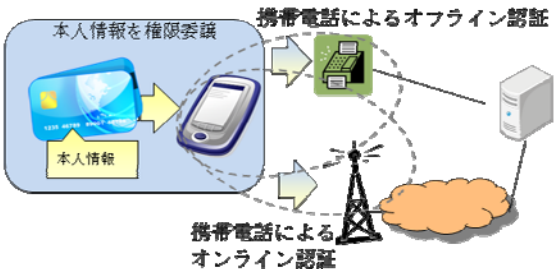

図 1 スマートフォンへの権限委譲

本稿では、まず IC カードなどに発行された認証権限を他の端末などに活用する際の従来の権限委譲方式の課題を示すとともに、IC カードに携帯電話などの認証局の公開鍵を事前に格納することなく、認証権限を携帯電話などの端末に安全に委譲する方法を提案する。提案方式をセキュリティ上の課題が指摘されることの多い NFC 機能付き Android OS 搭載スマートフォンに実装するケースを例題として、CC 認証のスキームに従い脅威と前提条件を定義しセキュリティ検証を実施した結果を示す。

2 スマートフォンの前提条件

Android OS を搭載したスマートフォンは NFC 機能を搭載するなど従来の携帯電話とは異なり、ユーザの意志で様々なアプリケーションを自由にインストールすることができるなど利便性が高い半面、不正なアプリケーションをユーザが意識せずにインストールしてしまうリスクが無視できない。この結果、ユーザ情報が外部に流出するといった事象も報告されている[3],[4]。文献[5],[6]では、Android OS を搭載した携帯電話に関するセキュリティ上の脅威を解説している。

一般的な Android OS を搭載したスマートフォンの構成を図 2 に示す。ここで、本提案方式を実装したアプリケーションソフトを “認証アプリ” とした。

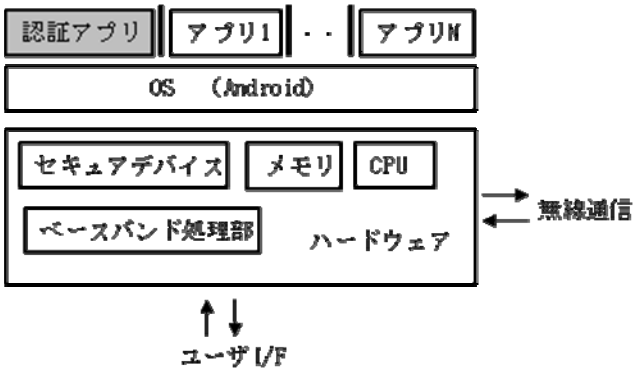

図 2 Android OS 搭載スマートフォンの構成

Android OS 搭載スマートフォンの前提条件として以下を想定する。

- 耐タンパ性を備えたセキュアデバイス領域を備え、署名生成、暗号化、復号などの演算を安全におこなうことができ、秘密鍵、公開鍵証明書、PIN 情報などのセキュア情報を格納し物理攻撃から保護するとともに、アクセス制御機能を搭載し許可された条件でのみデータアクセスが可能。
- NFC 機能により IC カードやスマートフォンとの通信が可能。
- 認証アプリ本体は正しく動作し、他のアプリ

の動作と干渉することがない。
- 認証アプリの署名生成に必要な PIN などの本人照合情報は所有者本人以外知らない。
- 非セキュア領域に存在するメモリ上に置かれた認証情報の読み出しや改竄の脅威が存在する。
- セキュア領域と外部装置間の通信経路において、認証情報の読み出しや改竄の脅威が存在する。

3　従来方式

3.1　従来の権限委譲方式

著者らは文献[7]で、IC カードからスマートフォンへ認証権限を移す際に、電話番号と紐付けた認証情報(トークン)を用いる方式を提案した。方式の装置構成を図 3 に示す。IC カード内に格納された公開鍵証明書(証明書 A とする)の発行主体である認証局 A、スマートフォンの公開鍵証明書(証明書 B とする)の発行主体である認証局 B、および IC カードから取得した公開鍵証明書の本人情報を元にスマートフォンで利用可能な認証トークンを発行するトークン発行局から構成される。スマートフォンへのトークンの発行主体であるトークン発行局が、認証局 A および認証局 B を信頼するモデルである。IC カードの認証権限をスマートフォンに格納する際に、スマートフォンの NFC 機能を利用する。認証サーバはトークン発行局と認証局 B を信頼してスマートフォンに対して認証サービスを提供する。

IC カードの認証権限を委譲する際にスマートフォンが IC カードに対して電話番号を通知する。IC カード側では証明書 A の本人情報と電話番号に対して IC カードの署名を生成し権限委譲先を保証することによりなりすましを防止している。

3.2　従来方式の課題

スマートフォンから IC カードへ電話番号を通知する際に、スマートフォンの署名付きで電話番号を通知する方法を用いることにより電話番号の正しさを保証しているが、IC カード側で電話番号の検証に証明書 B が必要となる。さらに証明書 B の検証のために、証明書 B の発行元である認証局 B の公開鍵を IC カードに事前にインストールしておく必要があるが、発行済み IC カードに新たに認証局 B の公開鍵をインストールすることは、サービスをおこなう上で障壁となる。

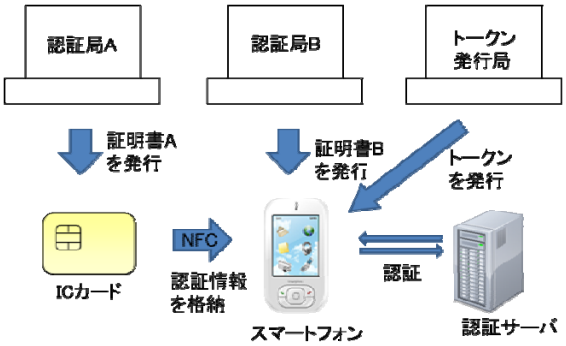

図 3　権限委譲方式の構成

4　提案方式

上に述べた課題に対して、トークン発行局のチャレンジに対するスマートフォンの署名を IC カードへのチャレンジとして利用する方式を提案した[8] 。スマートフォンを用いた認証サービスのライフサイクルとして、(1)IC カードおよびスマートフォンの公開鍵証明書を発行する初期登録フェーズ、(2)IC カードの認証権限をスマートフォンへ格納する認証権限格納フェーズ、(3)スマートフォンにより認証サービスを利用するサービス利用フェーズ、(4)認証権限を失効して認証サービスを停止する失効フェーズ、の4つのフェーズがある。図 6 に失効を除く3つのフェーズの手順を示す。次節ではこれらのフェーズについて述べる。

4.1　初期登録

(1)証明書 A の発行

証明書 A の発行は、認証サービスの要であるため、発行窓口などで直接本人であることを確実に確認したうえで発行するのが望ましい。

公的個人認証の例では、生成した鍵ペアから X.509 形式に準拠した公開鍵証明書が発行される[9]。証明書 A の属性情報として、氏名、住所、生年月日、性別などの本人情報が登録される（図 4）。

社員証や学生証などのケースでは、本人を特定するための ID も属性情報として含まれる。また、属性情報として、ID 情報のみが登録されるケースも考えられる。

属性情報 (ID,本人情報)	IC カード 公開鍵	認証局 A の署名

図 4 IC カードの公開鍵証明書（証明書 A）

（2）証明書 B の発行

スマートフォンを購入する際に、PKI サービスを利用するために必要な公開鍵証明書を販売店頭などで発行する。公開鍵ペアをスマートフォンのセキュアデバイス内で生成し、電話番号などの端末識別番号を属性情報とする端末公開鍵証明書（図 5, 証明書 B）を認証局 B が発行しスマートフォンのセキュア領域に格納する。

端末識別番号 （電話番号など）	スマートフォン公開鍵	認証局 B の署名

図 5 端末公開鍵証明書（証明書 B）

既に利用中のスマートフォンに対して証明書 B を発行する場合、セキュアデバイス内で鍵ペアを生成し認証局 B に対してオンラインで証明書 B の発行依頼をおこない取得する方法も可能である。

IC カード、スマートフォンのいずれにおいても、署名生成時に PIN 認証や生体認証などの本人照合を要求することによりセキュリティを高めることができる。

4.2 認証権限のスマートフォンへの格納

証明書 A の本人情報とスマートフォンの端末識別番号とを紐付けトークン発行局の署名付きでスマートフォンに発行するために、PKI クライアント認証と類似のチャレンジレスポンス方式を用いる。IC カードの認証権限を特定のスマートフォンに対して発行したことをトークン発行局が保証するために以下の処理をおこなう。

1. トークン発行局は、トークン発行要求を受けてチャレンジ（乱数 P）を生成する。
2. スマートフォンは P に対してスマートフォンの秘密鍵で署名 Q を生成し、Q と証明書 B をトークン発行局に送信するとともに Q（自己署名チャレンジ）を IC カードに送信する。
3. トークン発行局は、証明書 A および証明書 B が有効であること（失効していないこと）を認証局 A および認証局 B の公開鍵により確認した上で、証明書 B により P に対する Q の検証を、また証明書 A により Q に対する R の検証をおこなう。
4. トークン発行局は、3. の署名検証結果が正しいことが確認された場合、証明書 A の属性情報（IC カードの本人情報）と証明書 B の属性情報（電話番号などの端末識別番号）に対してトークン発行局の秘密鍵による署名値を付与したトークンを発行し、スマートフォンに送信する。
5. スマートフォンは、トークンをセキュアデバイス領域に格納する。

本方式では、所有者の IC カードの本人情報から所有者のスマートフォンに対してトークンを発行したことを保証するために、トークン発行局からスマートフォンを経由して IC カードに至る2段階の連鎖署名を用いている点に特徴がある。P に対する Q,R の検証が正しくない限りトークンが発行されないため、トークンの発行要求元スマートフォンと IC カードの権限委譲先スマートフォンの同一性を確実に保証できる。P の生成から Q および R の取得までの時間にタイムアウトを設けることにより安全性をさらに向上できる。

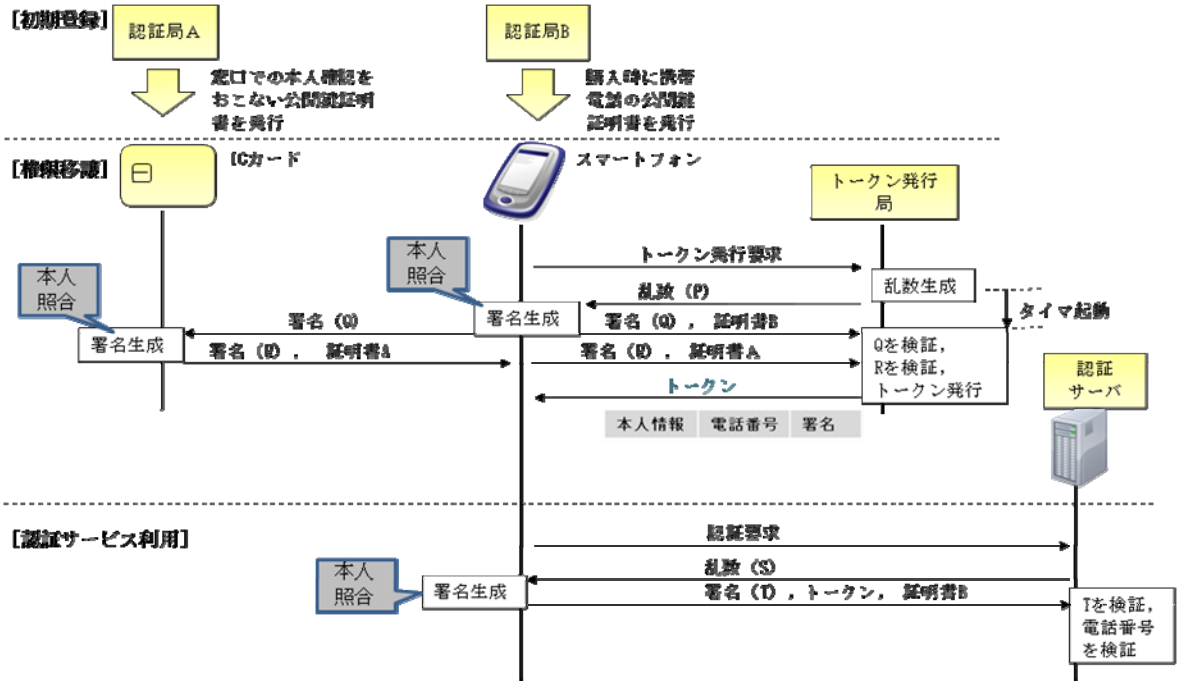

図 6　初期登録、権限委譲、認証サービス利用の動作

権限委譲の鍵となる動作である署名生成演算で、IC カードおよびスマートフォンに対して PIN や生体認証などの本人照合を必要とすることにより、本人以外の人物による権限委譲を防止できる。

いったんトークンをスマートフォンに格納できれば、**4.3** に述べる認証サービスの利用が可能であるが、トークン発行時に証明書 A,B と同程度またはそれ以下の有効期限を設けることが望ましい。

なお、[7]で示したようにトークンの発行において、生年月日のみや市町村以下を省略した住所のように、開示する本人情報にバリエーションを持たせることができる。

4.3　認証サービスの利用

スマートフォンによる認証サービスは、下記に示すようにトークンを併用したチャレンジレスポンス認証を用いる。

1. 認証サーバは、認証要求に対して、乱数 S を生成する。
2. S に対して、スマートフォンの秘密鍵で署名 T を生成し、T、トークン、証明書 B を認証サーバに送信する。
3. 証明書 B およびトークンの署名値を認証局 B およびトークン発行局の公開鍵により検証した後、証明書 B の公開鍵により T の署名を検証するとともに、証明書 B の端末識別番号とトークンの端末識別番号の照合をおこなう。

3. において、T の署名検証が正しければ、証明書 B の属性情報、すなわち認証サービスを要求してきたスマートフォン（の端末識別番号）を特定できる。同時に、証明書 B とトークンの端末識別番号が一致すれば、認証サービスを要求してきたスマートフォンと IC カードが権限委譲したスマートフォンとが同一であることが保証される。これらの検証を経て、トークンに登録された本人情報の正しさを確認できる。また、チャレンジレスポンス認証を併用しているため、トークンの有効性を 1 回に限定でき、トークンのコピーを利用した不正な認証（リプレイ攻撃）を回避できる。

証明書 A の属性情報に応じて、認証サービス

を使い分けることができる。例えば本人情報を属性情報としてトークンを発行した場合、スマートフォンを用いた本人証明を署名付きでおこなうことが可能である。また、トークン発行局を認証局 A が兼ね、ID を証明書 A の属性情報として発行した場合、IC カードの ID によるポータルサイトなどへのログイン認証と同等の機能をスマートフォンにより実現可能である。

4.4 認証権限の失効

トークンの有効期限内に証明書 A または証明書 B が失効した場合、対応するトークンも無効化する必要がある。このため、トークン発行局は認証局 A および認証局 B の失効リストを定期的にチェックし、トークンの有効状態リストに反映する処理をおこなう。

5 セキュリティ分析

本節では、Android OS 搭載スマートフォンに TOE（認証アプリ）を実装することを想定し、CC（Common Criteria）認証の方法に従い PP（Protection Profile）を定義し、TOE に対する総合的なセキュリティ検証をおこない、追加すべき機能を明らかにした。本 PP では[10],[11],[12]への適合を主張し、保護すべき情報資産、前提条件、脅威、セキュリティ対策方針を次のように定義した。

（1）保護資産

証明書A、証明書B、トークン、署名用秘密鍵、認証時にサービス提供装置とやり取りされる認証情報、本人照合用 PIN、認証局の公開鍵、TOE の動作に必要な設定データなどがある。

（2）前提条件

IC カードや端末、装置類の一般的な利用環境を考慮して、以下の前提条件を定めた。

・**A.SecureDevice** 耐タンパ性を持つセキュアデバイスによりデータを保護するとともに、セキュアデバイスはアクセス制御機能を持つ。

・**A.AuthData** 端末利用者は本人照合に用いる PINを安全に管理する。

・**A.Operation** 利用者が端末操作時に、画面に表示された情報を第三者に盗み見られることはない。

・**A.CertIssuer** 端末認証局やトークン発行局は、信頼できる組織により運営される、正しい時刻によりシステムが管理される、証明書や鍵が HSM（Hardware Security Module）などで適切に管理される、証明書の失効状態を適切に管理する、等の手段を備える。

・**A.Terminal** 認証サービスの提供装置は社会的に信頼できる組織により運営されるとともに安全な場所に設置され、利用者の電子証明書やトークンの個人情報を適切に管理する。また認証やログインの際に認証データの再利用を防止する手段を備える。

・**A.Environment** スマートフォンの動作環境として、不正なアプリが任意のメモリ領域のデータを任意のタイミングでの読み取りをおこなうことはできないとする。（ただし、特定領域のメモリのダンプやモジュール間を移動するデータの読み取りの可能性は許容する）

・**A.Application** スマートフォンにインストールした TOE は、改変されていない状態で起動できる。

（3）脅威：

現実的な脅威として以下を想定した。

・**T.Lost** スマートフォンの紛失や盗難により第三者の不正利用により本人になりすます。

・**T.FileRead** Android OS 上の他のアプリが情報資産に不正にアクセスする。

・**T.FileChange** Android OS 上の他のアプリが情報資産を不正に書き換える。

・**T.Deny** 利用者がトークンを利用したことを否認する。

・**T.CommRead** TOE と外部装置間の通信データが第三者によって読み取られる。

・**T.CommChange** TOE と外部装置間の通信データが第三者によって書き換えられる。

・**T.CipherKey** セキュアチャネルの暗号化鍵が

第三者に漏洩する。
・T.Memory　メモリ残存するデータや外部装置との通信データに含まれる情報資産が漏洩する。
・T.Input　スマートフォンから入力した情報資産が残存していることにより漏洩する。
・T.Display　画面表示した情報資産が残存していることにより漏洩する。
・T.Defect　動作環境の不具合により、セキュリティ機能の迂回や干渉、非活性化などの影響を受ける。
・T.Privilege　不正なアプリが root 権限で起動し、特定のメモリ領域データのダンプや、モジュール間を移動するデータの読み出しがおこなわれる。
・T.PhysicalAttack　物理的な攻撃によりスマートフォンに格納された情報資産の不正読み出しや書き換えがおこなわれる。

(4)TOEによる対策
　上述の脅威は、以下の「TOE による対策」により回避する。各脅威は、単独もしくは複数の TOE 対策により回避される。
・O.Authentication　セキュアデバイス内に格納されたデータとの照合により利用者を認証する。→ T.Lost を回避。
・O.DataAccess　セキュアデバイスに格納されたデータに対して、O.Authentication の認証証結果に基づきアクセス制御を実施する。→ T.Lost を回避。
・O.Cipher　メモリやファイルにデータを暗号化して格納する。 → T.FileRead を回避。
・O.CipherKey　データの暗号化用鍵はセキュアデバイス内に格納する。 → T.FileRead を回避。
・O.DataCheck　改変検知情報を付加してデータをメモリやファイルに格納する。→ T.FileChange を回避。
・O.Signature　格端末利用者がトークンを使用した証跡としてセキュアデバイス内に格納された秘密鍵により署名生成する。→ T.Deny を回避。
・O.KeyDelivery　セキュアデバイス内に格納された秘密鍵を使用して、外部の IT 装置から配送された秘匿通信用暗号化鍵を受け取る。→ T.CommRead を回避。
・O.ClearKey　暗号化処理で使用された鍵は使用後クリアされる。→ T.CipherKey を回避。
・O.ClearSecret　表示されたデータや入力データは使用後クリアされる。→ T.Memory, T.Input, T.Display を回避。
・O.SecureChannel　端末利用者の指示に基づき、外部 IT 装置との間に秘匿通信路を確立し、通信データの秘匿と改変チェックをした状態で個人情報を含む電子証明書やトークンを IT 装置へ送信する。→ T.CommRead, T.CommChange を回避。
・O.InternalData　モジュール間でやり取りされる内部データが読み取られないように保護する。→ T.Privilege を回避。

(5) セキュリティ方針
・P.Replay　サービス提供装置での認証において、認証データが再利用できない方式を採用する。
・P.Validation　証明書やトークンに対して有効期限と失効の管理をおこなう。
・P.SingleUse　1 台のスマートフォンの固有番号に対して 1 人の個人情報の権限委譲を許可する。
・P.MultiToken　個人情報から情報開示レベルに応じた情報を部分的に抽出して複数トークンを発行できる。
　これらのトークン発行や認証データ利用に関するセキュリティ方針は、前提条件 A.CertIssuer により実現される。提案方式では、端末認証局やトークン発行局と IC カード、スマートフォンの連携による署名チェーンを利用した権限委譲動作により、上に述べたセキュリティ方針を満たすトークンの発行が可能となる。

(6) 考察
　耐タンパ性を持つセキュアデバイスを備えたスマートフォンと HSM 機能を持った信頼できる

認証局およびトークン発行局を前提とした構成において、前節で述べたように提案方式はリプレイ攻撃やトークンの失効管理などのセキュリティ方針に対して有効な方式といえる。PIN 照合を利用したアクセス制御等の基本対策に加え、O.Cipher, O.CipherKey, O.DataCheck, O.InternalData 等のスマートフォン内部でのデータ保護対策が必要である。また、外部装置との通信においては、O.KeyDelivery による O.SecureChannel や、データ処理完了後の O.ClearKey, O.ClearSecret 等の対策が必要となる。

前提条件で述べた、A.Environment は、現時点ではスマートフォンが root 権限を取得されたとしてもデバイス内の任意のデータを取得される可能性は低いが、将来的により強力な攻撃法が現れた場合の対策として、OS 上に安全な動作環境を実現する TEE（Trusted Execution Environment）[13]などの技術仕様が GP（Global Platform）にて議論されており、Android OS 搭載スマートフォンへの実装の検討が進められている。同様に、A.Application も現時点ではアプリが改竄される可能性は低いが、TCG（Trusted Computing Group） [14]において OS やアプリの改竄をチェックするための仕組みが提案されており、今後想定されるより強力な攻撃法への対策として、将来的にはこれらの技術の併用を考慮した端末設計が有効になると考えられる。

6 まとめ

発行済みの IC カードからスマートフォンなどに PKI の認証権限を安全に委譲する方式を提案した。提案方式を例題として CC 認証のスキームに準じて PP を定義し、セキュリティ検証を実施した。システムとして必要なセキュリティの脅威を定義して、不足するセキュリティ機能を明らかにした。また運用の前提条件を定義し、妥当性について考察した。

提案方式はなりすましやリプレイ攻撃への基本対策を備えているが、これに加えてデバイス内や外部装置とのデータ処理をおこなう際の対策が必要である。

またスマートフォンの安全な動作環境として、将来的にはセキュリティ要件に応じたより強固な対策を施していく必要があると考えられる。

参考文献

[1] 公的個人認証サービス. http://www.jpki.go.jp.

[2] NFC Forum. http://www.nfc-forum.org/home.

[3] 公式 Android マーケットでマルウェア発見、広がるセキュリティ脅威. http://news.mynavi.jp/news/2011/03/05/005/index.html.

[4] Android マーケットにウィルス混入アプリ、50 種類以上が公開. http://itpro.nikkeibp.co.jp/article/NEWS/20110307/358014/.

[5] スマートフォンセキュリティ集中講義 ＜脅威編＞ ～iPhone/Android の違いとそのメカニズムを学ぶ. http://businessnetwork.jp/tabid/65/artid/1639/page/1/Default.aspx.

[6] Android セキュリティ・バイブル 2012, 日経 BP.

[7] 山越, 山本, 森田, 菅沼、”携帯端末を用いた個人認証システムの提案“, 信学技, vol. 111, no. 204, ISEC2011-29, p. 17-24, 2011.

[8] 山越, 山本, 森田, 菅沼、”携帯電話を用いた権限移譲方式の提案“, 信学技, vol. 111, no. 470, LOIS2011-100, p. 165-170, 2012.

[9] 公的個人認証サービス プロファイル仕様書 第 1.0 版. www.lascom.or.jp/jinfo/jpkiapv1/profile.pdf

[10]「セキュリティ評価のためのコモンクライテリア パート 1：概説と一般モデル」, 2009 年 7 月, Ver.3.1, CCMB-2009-07-001.

[11]「セキュリティ評価のためのコモンクライテリア パート 2：セキュリティ機能コンポーネント」, 2009 年 7 月, Ver.3.1, CCMB-2009-07-002.

[12]「セキュリティ評価のためのコモンクライテリア パート 3：セキュリティ保障コンポーネント」, 2009 年 7 月, Ver.3.1, CCMB-2009-07-003.

[13] TEE(Trusted Execution Environment) Device Committee. http://www.globalplatform.org/aboutuscommitteesdevice.asp.

[14] TCG（Trusted Computing Group）. http://www.trustedcomputinggroup.org.