スマートフォンへの利用者証明機能ダウンロード検討サブワーキンググループ（第５回）

議事概要

１　日　時

平成２８年１０月２５日（火）１０：００～１１：３０

２　場　所

中央合同庁舎第２号館１０階　共用１０階会議室

３　出席者

（１）構成員

手塚主査、新井構成員、小尾構成員、金山構成員（八島代理）、川関構成員、橘井構成員、木村構成員、斉藤構成員、高橋構成員、田村構成員（太口代理）、蔦田構成員（米沢代理）、庭野構成員、野田構成員、林構成員、松田構成員、宮野構成員、村上構成員（田中代理）、吉本構成員、長島説明者

（２）総務省

吉田情報通信国際戦略局参事官、小笠原情報通信政策課長、渡邉住民制度課企画官、下仲個人番号企画室長、岸情報通信政策課課長補佐、廣田情報システム企画課調査係長

４　議事

（１）今後の進め方について

（２）意見交換

５　議事概要

（１）今後の進め方について

【村上構成員（田中代理）】

○　資料５－１に従って総務省の実証事業について当社が提案した実証方法を説明。検証内容は大きく４つ。このうち、本サブワーキンググループで関係の深いものとして、Ａ

ｎｄｒｏｉｄ搭載端末のＳＩＭカードへの利用者証明機能の書き込みと、ｉＯＳ搭載端末におけるダウンロードの検討について説明。

○　５ページのとおり、１つ目のポイントは、モバイル通信事業者３社（ＮＴＴドコモ、ＫＤＤＩ、ソフトバンク）のスマートフォン、ＳＩＭカード、プラットフォームを用いて検証を行うこと。

○　２つ目のポイントは、モバイル通信事業者が提供するモバイルＮＦＣサービスプラットフォームを活用すること。

○　３つ目のポイントは、先行事例であるクレジット決済の実績に基づいたセキュリティ対策を検討すること。

○　４つ目のポイントは、ＳＩＭカードの中にアプレット、鍵、証明書を格納したスマートフォンをチケットレスサービスにおけるイベント会場での入場時にリーダにタッチするという形で活用すること。

○　６ページは、前回までの本サブワーキンググループで議論されたＳＩＭカードへのダウンロードに係る一連のフローを示している。今回の検証では、ダウンロードの評価にフォーカスし、⑫ＪＰＫＩデータの書込要求から始め、アプレットのダウンロードと利用者証明用秘密鍵・利用者証明用電子証明書のＳＩＭカードへのモバイル回線を使った書き込みについて、システム構築し検証する。

○　７ページは６ページの流れを詳しく示したもの。スマートフォンに搭載するアプリ（ＪＰＫＩ－ＵＩアプリ）、ダウンロードサーバ（ＳＰ－ＴＳＭ）及びＪＰＫＩアプレットを開発し、ＳＩＭカードにダウンロードする。

○　手順については、最初にＪＰＫＩ－ＵＩアプリ側でアクセスコード、パスワードを入力するとＴＳＭプロキシエージェントを介してＳＰ－ＴＳＭに送られる。ＳＰ－ＴＳＭでアクセスコード、パスワードの照合を行い、ユーザー認証されるとＴＳＭプロキシエージェントからＭＮＯ－ＴＳＭにアプレットのダウンロード要求が送られる。ＳＩＭカードへのアプレットのダウンロードが終わると、ＴＳＭプロキシエージェントからＳＰ－ＴＳＭに、発行データの書き込み要求が送られ、ＳＰ－ＴＳＭから利用者証明用秘密鍵と利用者証明用電子証明書がＳＩＭカードに書き込まれる。

○　８ページでは、セキュリティ対策の調査検討し、評価会で安全性を評価する項目を示している。ＳＰ領域の安全性については、ＳＰ領域の生成権限は誰にあるのか、どのような認証をすればその権限が得られるのか、ＳＰ領域の独立性はどのように担保される

のか等。

○　アプレット配送の安全性については、アプレット登録は誰の権限で行われて、その権限を得るためにはどのような認証をするか、モバイル回線を使ってアプレットを配送する際の暗号化の方式は何か、鍵はどのように共有するのか等。

○　秘密鍵配送の安全性については、鍵がＳＰ－ＴＳＭからＳＩＭカードに送られる際の権限を得るのはどういうやり方か、暗号化や鍵の共有はどういう方式で行うのか等。

○　評価体制は評価会と検討会の２段階で考えている。評価会は有識者、Ｊ－ＬＩＳで構成。具体的な有識者は主管課と協議の上決定する。説明者として当社のほか受託関係者として、アプレットを担当するＮＴＴコミュニケーションズ㈱、ＳＰ－ＴＳＭを担当する大日本印刷㈱が参加。また、プラットフォームを提供するモバイル通信事業者３社、総務省関係課についてはオブザーバとして協力いただく。

○　検討会で資料をまとめ、評価会に付議し、評価をいただく形で進める。

○　評価会は３回程度開催予定。第１回（１１月）、第２回（１月）のテーマは鍵配送、アプレット配送の安全性などを想定。第３回目（３月）については、運用面として、例えば、スマートフォン特有の業務として機種変更や譲渡、紛失、解約などについて、電子証明書に関する業務として、発行や更新、ＰＩＮロックの解除、ＰＩＮの変更などの課題を検討することを考えている。

○　ＭＶＮＯによる利用者証明機能ダウンロードにおける課題についても検討したい。技術面については、ＭＶＮＯによって様々なＳＩＭカード、スマートフォンが使われているため、その組み合わせの調査から始め、実現可能な組み合わせについて明らかにする。加えて、既存のＭＶＮＯのプラットフォームへの影響を整理し、具体的な実現方式を検討する。さらに、ビジネス面でも、ＭＶＮＯ数社にヒアリングやニーズ調査をすることを想定している。

○　ｉＯＳ搭載スマートフォンへの利用者証明機能のダウンロードの検討について、実現方式は２通り考えられる。１つ目がＡｎｄｒｏｉｄ搭載端末で検証する方式と同様にＪＰＫＩ側で鍵と証明書を生成してダウンロードする方式。２つ目がｉＰｈｏｎｅ側で鍵ペアを生成して、ＪＰＫＩシステム側で生成した証明書をｉＰｈｏｎｅ側に返す方式。この２つの方式のうち、後者の方式での検討を考えている。

【長島説明者】

○　資料５－２に基づき、ｉＯＳ搭載スマートフォンへの利用者証明機能のダウンロードの詳細について、実証事業の請負事業者であるＮＴＴデータの下で検討を行う立場として説明する。Ａｎｄｒｏｉｄ搭載スマートフォンのＳＩＭカードへの利用者証明用秘密鍵と利用者証明用電子証明書のダウンロードの仕組みと同様に、ＳＩＭカードに利用者証明機能をダウンロードできれば問題ないが、ｉＰｈｏｎｅではＳＩＭカードに何かを書き込んだり、領域をつくったりするＰｕｂｌｉｃ　ＡＰＩは公開されていない。

○　それを図示したものが３ページ。ＪＰＫＩ－ＵＩアプリとＴＳＭプロキシエージェントをｉＰｈｏｎｅに入れることは可能と思われるが、Ａｐｐ　Ｓｔｏｒｅへ登録できるアプリケーションに制約があるため、ＳＩＭカード内にＳＰ領域をつくり、アプレットをダウンロードし、利用者証明用秘密鍵や利用者証明用電子証明書を格納することはできない。そのため、別の方法によりＳＩＭカードと同様のセキュリティを担保できるのではないかと考えられる仕組みを説明する。

○　まずはｉＰｈｏｎｅのセキュリティの仕組みについて説明する。今回、格納の対象としている利用者証明用秘密鍵や利用者証明用電子証明書は、最終的にｉＯＳデバイスの上ではファイルという形で保管され、基本的には、ｉＯＳデバイス上の全てのファイルは一つ一つが別の鍵で暗号化される。これらの鍵は、ハードウェアのＳｅｃｕｒｅ　Ｅｎｃｌａｖｅという別のＯＳで動いているコプロセッサ内のＵＩＤ（ＡＥＳの２５６ビットの鍵）から作られ、その鍵でファイルを暗号化する。つまり、ｉＰｈｏｎｅの場合、ＵＩＤが漏洩しないということが安全性の非常に重要な担保になっている。このＵＩＤは、製造時にＳｅｃｕｒｅ　Ｅｎｃｌａｖｅ一つ一つに焼きつけられるもので、ＣＰＵチップメーカーもＡｐｐｌｅ社もこのＵＩＤを管理していない。すなわち、誰もこのＵＩＤが分からないので、最終的にここから派生する鍵も分からないというセキュリティの仕組みをとっている。

○　なお、ｉＰｈｏｎｅにはＳｅｃｕｒｅ　Ｅｌｅｍｅｎｔ　ｆｏｒ　Ａｐｐｌｅ　Ｐａｙというハードウェア領域もあり、当初はこの領域を使うことを検討していたが、今のところＡｐｐｌｅ　Ｐａｙ以外では使わないということなので、ＡＰＩは公開されていない。

○　ファイルをセキュアに保管する流れは、始めにＳｅｃｕｒｅ　ＥｎｃｌａｖｅにあるＵＩＤがハードウェアキーを生成する。その鍵は、ファイルメタデータを暗号化するファイルシステムキーの暗号鍵になる。さらに一つ一つのファイルはファイルキーで暗号

化される。そのファイルキーは、端末に持ち主が設定するパスコードキーでさらに暗号化されて、四重にＫｅｙ　Ｅｎｃｒｙｐｔｉｏｎ　Ｋｅｙ（ＫＥＫ）の状態をつくることで、安全性を実現している。これだけの暗号化複合はソフトウェアでは重い処理になるので、これらを処理するハードウェアのエンジンもｉＯＳデバイスの中にチップとして組まれている。

○　普通のファイルはこのようにｉＯＳデバイスの中に格納されるが、証明書や鍵のような特殊なファイルを格納する場合、Ｋｅｙｃｈａｉｎという仕組みも利用する。前記のＫＥＫに加え、Ｋｅｙｃｈａｉｎデータ保護サービスを経由して、鍵の処理を行う仕組みにより、高いセキュリティを実現している。この仕組みはＡｎｄｒｏｉｄ搭載端末で検討されていることと同様なことを実現できるのか、安全性は同等か、また同等でなければどのような工夫をすれば同等になるのかについて検討したいと考えており、検討方法は２通り考えられる。

○　５ページは、Ａｎｄｒｏｉｄ搭載端末で検討されている方法にｉＰｈｏｎｅの場合を当てはめてみた図。アプリケーションにより格納する仕組みにおけるＳＰ－ＴＳＭ等は使えず、ＳＩＭカードに相当する部分がＫｅｙｃｈａｉｎデータ保護サービスになり、その中にＫｅｙｃｈａｉｎをＳＰ領域相当のものと想定し、検討を行う方法。利用者証明用秘密鍵をネットワークで配送する方法を説明している。Ａｐｐ　Ｓｔｏｒｅからｉ ＯＳ端末にＪＰＫＩ－ＵＩアプリをダウンロードし、ＪＰＫＩシステム側で鍵ペアと利用者証明用電子証明書を生成し、ネットワークでｉＯＳ端末に配送する。

○　Ａｎｄｒｏｉｄ搭載端末と同様の仕組みは実現可能なため、今回は６ページのとおり、Ｋｅｙｃｈａｉｎ内で鍵ペアを生成し、利用者証明用公開鍵をもとに利用者証明用証明書作成リクエストを送り、ＪＰＫＩシステムで利用者証明用電子証明書を生成して、証明書をＫｅｙｃｈａｉｎにダウンロードする仕組みを検討する。この仕組みはネットワークを通さずに利用者証明用秘密鍵を処理ができるという利点がある。鍵ペア生成処理が実用に耐えるのか、証明書のセキュアな伝送等について検討したい。

【手塚主査】

○　「ＮＦＣスマートフォンによるマイナンバーカードの読み取り」について、電波産業会（ＡＲＩＢ）アドホック会合での検討状況を説明する。

○　アドホック会合は２０１４年１０月から開催。メンバーは携帯電話事業者３社（ＮＴ

Ｔドコモ、ＫＤＤＩ、ソフトバンク）、携帯電話メーカー６社（ＬＧ、京セラ、サムスン、シャープ、ソニー、富士通）で構成。

○　１０月１９日開催の第６回アドホック会合で、Ｊ－ＬＩＳから「ＮＦＣスマートフォンに関するマイナンバーカード対応基準」が提示され、当該基準について、メンバーで検討レビューした。その結果、当該基準で問題ないということになり、今後の公表に向けてＪ－ＬＩＳで最終調整をしているところ。読み取り対応スマートフォンについては、携帯電話事業者及びメーカーにおいて従前から検討が行われていたことから、今後、各キャリア、メーカーによる積極的な対応に期待したい。

【小笠原情報通信政策課長】

○　資料５－３に基づき、次回ワーキンググループに向けた報告案について説明する。まず、スマートフォンへの利用者証明機能の搭載について、本年６月の個人番号カード・公的個人認証サービス等の利活用推進の在り方に関する懇談会において取りまとめられた当面の目標の進捗状況として、本年１０月、Ａｎｄｒｏｉｄ搭載スマートフォンのＳＩＭカードへの利用者証明機能のセキュアなダウンロード実現に向けた実証を開始することに加え、ｉＯＳ搭載スマートフォンへの利用者証明機能の搭載の検討についても着手することを明記。

○　本年度中に、利用者証明機能を搭載したスマートフォンがどのように使えるのかという具体的な姿を見せるため、イベント会場でのチケットレス入場の実証実験を実施。

○　Ａｎｄｒｏｉｄの場合は鍵を安全に配送する方法の検証、ｉＯＳの場合はＫｅｙｃｈａｉｎ領域で安全に鍵を生成・格納する方法の検討を踏まえ、２枚目の利用者証明用電子証明書を発行するための制度整備等を実施する。

（２）意見交換

【田村構成員（太口代理）】

○　ＳＩＭカードへの利用者証明機能のダウンロードを含めた検証については、速やかに開始し、さまざまな課題をしっかり深堀りしながら、最終的に世の中にしっかり出せるものが実現できる取組になるように、しっかり対応したい。

○　ｉＯＳへの対応については、ＡｐｐｌｅあるいはＩＢＭの協力が不可欠。何かお手伝いできることがあれば、積極的に対応する。

【金山構成員（八島代理）】

○　実証実験について全面的に協力したい。特に、チケットレスという具体的なサービスを実験できることは、民間事業者にとっても非常に有意義。

【橘井構成員】

○　ＮＦＣサービスで既に提供しているプラットフォームを活用して、セキュアなＳＩＭカードへのダウンロードを実現していきたい。

○　実証実験に関しては、当社のプラットフォームやＳＩＭカード、端末を有効活用し成功させたい。

【川関構成員】

○　利用者証明機能ダウンロードは、携帯キャリアだけでなく、ＭＶＮＯも広く利用できるような形で実現してほしい。

【庭野構成員】

○　ＳＩＭカード、ｉＰｈｏｎｅのいずれも安全性をきちんと評価した上で、課題等をあぶり出して次のステップへつなげ、多くの人が使えるようなサービスを実現するということを念頭に検討いただきたい。

【斉藤構成員】

○　手塚主査から説明があったとおり、電波産業会において、スマートフォンをリーダライタの代わりとして、マイナンバーカードを読み取ることについて検討している。スマートフォンのスペック上、非常に難しいが、できる可能性があるということで、一生懸命頑張って実現しようとしているメーカもいる。

【宮野構成員】

○　モバイルＮＦＣサービスでＳＰ－ＴＳＭのサービスを実際に提供している立場から実証実験に協力する。今回の実証で安全性について問題なしと評価されて、安全・安心・便利な機能がスマートフォンに搭載されるよう検証されていけばよい。我々も積極的に

協力させていただく。

【蔦田構成員（米沢代理）】

○　高いセキュリティを持ったＳＩＭカードを使ったサービスが実証に向けて動き出したということで、ＳＩＭカードソリューションベンダとして期待している。セキュリティ全体の観点で何かサポートできることがあれば、積極的に参加していきたい。

【木村構成員】

○　ＭＶＮＯという立場と、企業グループとしての端末ベンダという立場から、今回の実証実験が成功することを願いながら、活用できるサービスを並行して考えていきたい。

【高橋構成員】

○　最近、サービスの軸足をスマートフォンに移している企業が非常に多いと感じている。本サブワーキンググループでの検討と実証実験を通じて、ビジネスにいかに早くつなげていけるかということに関心を持って検討を進めていきたい。

【野田構成員】

○　ｉＯＳのＫｅｙｃｈａｉｎ、要は、ソフトウェアで耐タンパ相当のセキュリティを実現しようという試みは、ＩＡサーバ等にも生かされると思っているので、今後の活動に非常に期待している。

【松田構成員】

○　スマートフォンをリーダライタとして使うことに加え、ｉＯＳにも対応するということで、スマートフォン単独で利用できるさまざまなユースケースが出てくることを期待している。ユースケースをいろいろ考え、ひいては、地方創生や経済活性化の観点でも力になれればと考えている。

【吉本構成員】

○　スマートフォンによる公的個人認証サービスの利用を日本で普及させるには、やはりｉＰｈｏｎｅの存在は欠かせない。スマートフォンで利用できるようにしないとサービ

ス自体が広まらないと思われるので、今回のｉＰｈｏｎｅでの検討開始は非常に良い話。特に東京オリンピックを考えた場合には、テロ対策も含めてチケットレスサービスでの活用は非常に有効だと考えるので、期待している。

【新井構成員】

○　地方の現場でマイナンバーカードや公的個人認証サービスを活用しようとすると、リーダライタが必ず課題になってくる。ｉＰｈｏｎｅの検討を含め、スマートフォンの対応には非常に希望を持って期待している。

【林構成員】

○　ＪＰＫＩの安全性を担保したままスマートフォンに搭載していくことに大いに期待しているので、積極的にセキュリティの検討をお願いしたい。

【小尾構成員】

○　技術的な方向性はある程度示されたと思うので、今後はこの提案内容に従って着々と進めてもらいたい。その一方で、安全性等に関する懸念は最後まで残るので、しっかり検証していただきたい。

○　検証の範囲はＳＩＭカードとＳＰ－ＴＳM間の安全性やＳＩＭカードに安全に鍵や証明書が格納できるかということ。また今後、Ｊ－ＬＩＳがこの仕組みを運用することを考えた場合、実証実験においても大日本印刷が開発することから鑑みてもＳＰ－ＴＳＭ自体をＪ－ＬＩＳが持つということはないとすると、ＳＰ－ＴＳＭとＪ－ＬＩＳで責任をどのように分担するのか、さらに、現在のＪＰＫＩのＣＰ／ＣＰＳをそのまま維持して、その中でこの仕組みを組み入れていくのか、それとも、違う形で、違う方針のもとに運用していくのかということに関しても、ぜひ検討いただきたい。

【手塚主査】

○　本日の請負事業者からの報告内容は、これまで本サブワーキンググループにおいて整理してきた方向性に概ね合致するものであり、この方向で着実に実証実験を進めていただきたい。

○　ＳＩＭカードへの利用者証明機能のダウンロードの実現に向けては、技術面もさるこ

となが ら、法律などの制度面やビジネスモデルなどの運用面での課題もまだ多くあると考えている。これらの課題について確実に解決を図っていくためには、総務省、Ｊ－ＬＩＳ、そして、キャリアの協力は不可欠と考えているので、引き続きご協力をお願いしたい。

○　ｉＯＳへの対応についても、利用者証明機能が利用可能な端末の幅が広がることは、国民の利便性向上の観点から非常に望ましいことであり、大いに歓迎したい。特に、ＳＩＭカードとの比較で、秘密鍵をＯＳ内部で生成する点についての検討結果には、特に注目したい。

○　技術面や制度面での検討と並行して、ＳＩＭカードの利用料の負担の在り方などビジネスモデルの確立に向けた検討も、今年度の実証事業において意欲的に取り組んでいただき、速やかに社会実装ができることを期待。

○　利用者証明機能を搭載したスマートフォンを使ってチケットレス入場を実証する等、近い将来、スマートフォンがマイナンバーカードと同様に使える可能性があることを目に見える形で世間にアピールしていくことは、公的個人認証サービスの利活用促進のために極めて重要。

○　先述のとおりＡＲＩＢの検討グループで、スマートフォンを「マイナンバーカード対応」として公表するために、Ｊ－ＬＩＳの作成した基準が示され、公表に向け調整を行っている。公的個人認証サービスの利活用の拡大という観点から、スマートフォンでのマイナンバーカードの読み取りの実現も重要であると考えているので、キャリアやメーカーの積極的な対応を大いに期待する。

【小笠原情報通信政策課長】

○　本サブワーキンググループの検討状況については１１月９日のワーキンググループで手塚主査から報告をいただき、その後１１月１４日の親会でワーキンググループの大山主査から報告いただく。

以上