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２回）議事概要

１　日　時

平成２７年１２月１日（火）１３：００～１４：４５

２　場　所

中央合同庁舎２号館８階　第１特別会議室

３　出席者

（１）構成員

手塚主査、阿部構成員、新井構成員、小尾構成員、鴨志田構成員、川関構成員、
橘井構成員（大道構成員代理）、木村構成員（熊木構成員代理）、斉藤構成員、白戸構成員、
高橋構成員、田村構成員（佐藤構成員代理）、蔦田構成員（米沢構成員代理）、庭野構成員、
野田構成員（四十谷構成員代理）、林構成員、松田構成員、宮野構成員、
村上構成員（田中構成員代理）、吉本構成員、進藤説明者

（２）総務省

山田情報通信国際戦略局長、小笠原情報通信政策課長、上仮屋住民制度課企画官、
奥田行政情報システム企画課管理官、望月個人番号企画室長、
飯村情報通信政策課課長補佐、大澤事業政策課課長補佐

４　議事

(1)　ＮＦＣスマートフォンを活用した民間事例
(2)　実現方法及び課題について
(3)　意見交換

５　議事概要

(1)ＮＦＣスマートフォンを活用した民間事例

【田村構成員（佐藤構成員代理）】

○　本日、当社から説明する民間事例「モバイルＮＦＣサービス」は、ソフトバンク、ＫＤＤＩともに基本的には３者共通の仕組みとご認識いただきたい。一連のやり方、フローに関して本ＳＷＧでの議論にご参考にしていただければと思う。

【進藤説明者】

○　説明する前提として、「ＵＩアプリ」はスマートフォンでユーザーインターフェースアプリをいうが、「アプレット」は利用者証明用機能をＳＩＭに入れるための箱のようなイメージであると考えていただきたい。

○　機能分担について説明したい。モバイルキャリア（ＭＮＯ）は、各サービスプロバイダ（ＳＰ）に対してモバイルＮＦＣサービスのプラットフォーム、つまり、ＮＦＣ対応の携帯電話、ＳＩＭなどのいわゆるシステム環境を提供する。その上で、ＳＰが対応サービス、例えば、電子マネー、クレジットカード、ポイントカード、社員証、交通機関の乗車券等を提供する。今回、利用者証明機能をＳＩＭの中に格納することになるのであれば、ＳＰの立ち位置にＪ－ＬＩＳが入るような想定になる。

○　手順については、例えば、モバイルキャリアは、ＭＮＯ－ＴＳＭというサーバを運用し、ＳＩＭの中に領域を確保、つまりアプレットを格納する作業を実施し、ＳＰは、ＳＰ－ＴＳＭというサーバの開発～運用、アプレットの開発、ＵＩアプリの開発、鍵や証明書などのＳＰデータを準備し、ＳＰ－ＴＳＭ経由でＳＩＭのＳＰ領域へ格納する。

○　現在、商用サービスを提供している「オリエントコーポレーション」のモバイルＮＦＣサービスにおける利用者の申込み、鍵や証明書の格納、クレジット決済までの一連のフローをご紹介。利用者は、オリコのウェブサイトでＮＦＣサービス「payWave」の新規申込みを行うと、アクセスコードとパスワードが本人限定受取郵便で送付される。利用者は、ＮＦＣ対応のAndroidスマートフォンと対応のＳＩＭカードを用意し、Google Playから、対象のＵＩアプリをスマートフォン上へダウンロードし、ＵＩアプリを用いて初期設定を行う。もちろん、事前準備として、ＳＰはGoogle Play上にＵＩアプリをアップロードしておく必要がある。利用者は、アプリ上で各種同意を行ってから郵送されたアクセスコードとパスワードを入力。その間利用者のスマートフォンにはステータスバーが進捗している状態になるが、バックグラウンドでは、ＭＮＯ－ＴＳＭ、ＳＰ－ＴＳＭのサーバが順次処理を行い、アクセスコードとパスワードをもとに利用申し込みされた情報などを連携させＳＩＭの中に書き込みが行われている。以降、利用者はpayWave対応の加盟店でスマートフォンをかざすとクレジット決済が実現。

○　クレジット決済の利用申込みについては、犯罪収益移転防止法等において取引時の本人確認義務があるため、本人限定受取郵便でアクセスコードとパスワードを送付する手段を採用。

○　この一連の利用者からの申込み、ＳＩＭへの登録から利用に至るまで、既に商用サービスで確立したフレームワークがあり、公的個人認証サービスの利用者証明機能の格納にあたっても、活用できるフレームワークだと思う。是非参考にご活用をご検討いただきたい。

【鴨志田構成員】

○　既に、決済分野でセキュリティ環境を確保して運用していること、モバイルキャリア、ＳＰの役割や責任範囲も一定の基準の中で運用が開始されている。今後、ＳＩＭへのダウンロードの実現に向けて、いろいろな課題解決の参考になればと思う。モバイルキャリア３社とも前向きに考えて行きたい。

【橘井構成員代理（大道構成員代理)】

○　個人番号カードをスマートフォンで活用するにあたっては、ユーザがいかに簡単に、安心して使えるフローを立てられるかが肝要。このワーキングの中でしっかり議論して、より幅広い方に活用していただけるものとしていきたい。

【手塚主査】

○　モバイルキャリア３社からの非常に前向きなご発言に感謝。技術的にも、サービスとしても既に確立された仕組みがあり、今後の議論にとって非常に有意義なモデル。

○　公的個人認証サービスの電子証明書のスマートフォンへのダウンロード方法をＳＷＧで決めていく中で、その必要な条件整理、課題の精査にあたっては、是非この仕組みを活用し、検討を進めてまいりたい。

【蔦田構成員（米沢構成員代理)】

○　海外では、モバイル、特にＳＩＭカードを使ったモバイルでの認証サービスが既に商用で開始されており、これらの国でどういった仕組みでサービスを提供し、どのようにユーザに受け入れられているかという点をご紹介したい。

○　携帯電話事業者が加入しているＧＳＭＡ（GSM Association）では、「mobile・connect」という名称でモバイルを使った認証サービスの標準化などに取り組む。我々は、ＳＩＭカードベンダーとしての立場のほか、モバイルＩＤのソリューションベンダーとして参加。

○　当社は計１８カ国でモバイルＩＤのプロジェクトを実施。ヨーロッパでは早くからモバイルを使った認証サービスが始まっており、本日はフィンランド、ノルウェー、アイスランドについてご紹介。ＧＳＭＡの準拠ということで、ドイツ、ポーランド、ルーマニア、スウェーデンなどでも、今後、モバイルを使った認証を広めていくという動きが出ている。

○　ＧＳＭＡではセキュリティを４レベルで定義。ＬＥＶＥＬ１は、通常のＩＤ・パスワードでのログイン、ＬＥＶＥＬ２は、何かの認証デバイスを使った本人確認、二要素認証しないようなパターン、ＬＥＶＥＬ３は、二要素認証としてＰＩＮなどを使うパターン、ＬＥＶＥＬ４は、

二要素認証を使うとともに、ＰＫＩを使うことによる最高レベルのセキュリティ。ＬＥＶＥＬ２はウエブのクラウドのサービスなど、ＬＥＶＥＬ３は銀行あるいは企業のシステム、ＬＥＶＥＬ４は公共のサービス、行政サービスで使用。

○　サービス利用時は大画面を使うことがよくあるため、「サービス利用デバイス」としてパソコン、タブレット、スマートフォンがあるが、このほか、認証デバイスもある。利用デバイスからのサービス利用時、サービスプロバイダのウェブサイトで利用者認証を行う際、「モバイルＩＤプラットフォーム」にその要求を投げる。モバイルＩＤプラットフォームは、基本的には通信事業者、携帯電話事業者が提供するケースが多く、携帯電話網を使って認証デバイスに対して認証要求を送信、認証デバイスではＳＩＭカードに入っている認証用の鍵を使って認証、その結果をモバイルＩＤプラットフォーム経由でサービスプロバイダに返すという仕組み。

○　モバイルＩＤプラットフォームでは、認証局が別であっても同じプラットフォームを使える仕組みを提供。携帯電話の方では、ＳＩＭカードの中でＰＫＩの鍵を生成・保持し、サーバに証明書をアップロードする仕組みを採用。ＳＩＭカードに通信する仕組みとしては２パターン、ＵＩアプリを使うパターンとＳＴＫ（SIM TOOL KIT）がある。ＳＴＫではテキストベースでの表示を行うことによってAndroidやiPhone、さまざまなデバイスで利用可能。

○　フィンランドでは、１９９９年からeIDカードを導入したが、カードリーダが負担となって利用が進まなかったが、モバイルの浸透が進み、２０１１年からモバイルＩＤを開始。１５万人以上が２２０のオンラインサービス、公共サービス、保険、ヘルスケア、メディア、オンラインバンキングなどで利用。

○　サービスプロバイダが全てのモバイルキャリアと個々に接続すると負担が大きくなることから、大手３キャリア間でシグネチャー・ローミングという形で電子署名のローミングを実現。これによりユーザがどこの携帯電話事業者のユーザであってもモバイル認証ができる仕組み。フィンランドのFiComが中心となって仕様を策定。

○　ノルウェーでは、従来、オンラインバンキングなどでハードウエアＯＴＰトークンが使われていたが、２００９年からハードウエア、ＳＩＭカードを使ったモバイルＩＤサービスを開始。２０１５年11月現在、７２万ユーザ、実際にオンラインバンキングを使える人口の約２７％。特徴的なのは、ユーザ当たりの月の利用回数が１４回、ハードウエアトークンによる取引の約２倍という数字。通信事業者は５社あるが、銀行間で設立されたプラットフォーム「バンクＩＤ」が公共サービスを含む様々サービスに対してモバイルキャリアとの接続を提供。２００９年のサービス開始以来、対応するキャリアも増え、ユーザ数も増加。

○　ノルウェーのユースケースの場合、海外にいる場合でもモバイルＩＤを利用できる環境を実現。また、住居申請の例として、紙の手続では１０日から１４日の処理日数がバンクＩＤを使

うことによって処理日数が３日程度となる結果。

○　アイスランドでは、２０１３年から既存の電子ＩＣカードに加えてモバイルでのサービスを提供。２０１４年にMobile・World Congressという展示会において大臣がモバイルＩＤ利用のデモとして議事録に署名するというデモンストレーションを実施。対象となるユーザの２５％がモバイルＩＤを使用。

○　ナイジェリアでは、モバイルＩＤプロジェクトが２０１５年から開始。最初のユースケースはモバイルによる出生届。ＧＳＭＡの「mobile・connect」準拠した形での最初の大規模なサービスとして、モバイルオペレーターが主導してプロジェクトを開始。

○　スペインでは、２０１５年末からモバイルＩＤサービスを開始予定。ヨーロッパのｅＩＤの規制、ｅＩＤＡＳの規制に合わせて、今後、クロスボーダー認証も対応予定。その最初のパイロットとして、今後、ボーダフォンのスペインとフィンランドとの間でのクロスボーダー認証を開始する予定。

【小尾構成員】

○　３点質問がある。１点目は、ＳＩＭの中にアプレットを入れた場合、例えば、機種変更した場合でもそのまま使えるのか。２点目は、ＵＩアプリからの要求でＳＩＭにアプレットを登録するとあるが、特定のＵＩアプリからのみアプレット登録の要求を送ることができるのか。３点目は、ＪＰＫＩの利用者認証用の電子証明書の利用を実現するに当たって、ＳＩＭがこれからパーソナライズする人の契約の下で発行されているのかについて確認したい場合、ＳＰ側がパーソナライズするＳＩＭに対して、アプレットに対してパーソナライズをするという段になってＳＩＭが誰のものかを確認する術はあるのか。

【進藤説明者】

○　１点目の機種変更については、現状使える状況。具体的には、古いスマートフォンでＵＩアプリをダウンロードして、インストールして利用までしていたお客様がいた場合、新しいスマートフォンを購入後、新しいスマートフォンにＵＩアプリをダウンロードすればＳＩＭを差しかえるだけで使える状況になる。基本的に、これに関しては、ドコモ契約者の方はドコモのＳＩＭ、ドコモのスマートフォンといった組み合わせに関しては使えるという状況。

○　２点目のアプレットに対する制限は、ＭＮＯ側において明示的にこのＵＩアプリを使う点についての審査、申請を行う運用フローとなっている。そういった縛りがあるアプリケーションからしかＳＩＭアプレットの新規登録はできない仕組み。

【小尾構成員】

○　ＵＩアプリが正規のものであれば、例えば、パーソナライズをしないで、アプレットだけダウンロードすることも可能になるのか。

【進藤説明者】

○　アプレットだけダウンロードはできる。また、３点目のモバイルキャリアにおけるＳＩＭの契約者確認について、パーソナライズ時においては現状のモバイルＮＦＣサービスにおいてはそのような行為は行っていない。そこに関しての課題があるかどうかは即答できないが、実態としてはやられていない。

【鴨志田構成員】

○　我々も運用も同じ。

【橘井構成員（大道構成員代理)】

○　我々も運用も同じ。

【小尾構成員】

○　仮定の話として、携帯電話ショップのような店頭おいてＳＩＭの本人確認はできるのか。

【進藤説明者】

○　各キャリア同じだと思うが、一義的に決めづらい部分もあるが、ショップの運営上、またオペレーション上の一定の課題があると認識。

【吉本構成員】

○　その他の国では具体的どのような中身なのか。米国などの先進国はプロジェクトの予定国、パイロット実施国になっているが、これは本当にグローバルに普及していくとみているのか。

【蔦田構成員（米沢構成員代理)】

○　その他の国になっている中国かインドなどは、まず公共サービスが軸となるほか、オンラインバンキングがその次のサービスとして使われている。

○　パイロットプロジェクト実施国における今後の動向について、モバイルでの認証という意味では拡大するものと推察するが、ＳＩＭカードを使うかどうかに関しては、パイロットの段階

でまだ決まっていないところが存在。モバイルを使う認証には様々な技術があり、モバイルキャリアのＩＤの認証などもその一つ。セキュリティについて考えた場合、ＳＩＭカードは非常にセキュリティの高いデバイスになっており、ＳＩＭカードの有効活用という意味でＳＩＭカードベースのものも今後広がっていく可能性がある。

【吉本構成員】

○　米国は、こういうことに対してどういう動きをされているのか。やはり一番キーになるのはアメリカだと思う。

【蔦田構成員（米沢構成員代理）】

○　現状では、パイロットの段階のため、最終的にどうなるか見えていないという状況。

○　通信事業者が提供するネットワークベースの認証サービスが既にある中で、セキュリティの高いものに対するニーズがあると見ており、ＳＩＭカードを使ったものを議論。

【川関構成員】

○　通信事業者が準備するものとサービスプロバイダが用意するものとがあるが、ＮＦＣチップやＴＳＭプロキシエージェントというのは、誰がどういう形で準備されるものなのか。

【進藤説明者】

○　モバイル端末のＮＦＣチップはハードウエアになるため、発売前に端末の中にプリセット、そもそも組み込まないといけないという類いのもの。ＴＳＭプロキシエージェントは、Androidスマートフォンでいうと、出荷前にメーカープリセットされたミドルウエア。いずれも基本的には２つともダウンロードするものでなく、出荷前にプリセットされているものとご理解いただきたい。

【川関構成員】

○　それは３キャリア共通で準備されているものなのか、端末ベンダーで準備されているものなのか。

【進藤説明者】

○　仕様については、基本的には３キャリア個別に端末メーカとやっているが、主要部分の足並みを揃えるべきところは統一させている。実際にどうやってプリセットして出していくかとい

うところは、ほぼ一緒だと思うが、各キャリアマター。

【望月個人番号室長】

○　アプレットをＳＩＭカードのチップに入れる際に、キャリアごとに別のアプレットを作らなければいけなのか、同じものを入れることができるのか。

【進藤説明者】

○　ほぼ同様のものでいける、基本的な部分は統一的にできると思うが、キャリアごとにＳＩＭにも特性があるので､大なり小なりカスタマイズしなければならない部分があるかもしれない。

【鴨志田構成員】

○　サービスプロバイダの考え方にもよるが、想像するに、基本的に仕様としてはそんな変わらないが、おそらく作り分けられているのではないかと思う。

【橘井構成員（大道構成員代理)】

○　同じ認識。基本ベースの部分は、おそらく３社共通だと思うが、ＳＩＭの構造で若干違う部分があるのではないかと思う。カスタマイズ範囲ということで、サービスプロバイダによっては作り分けされているところもあると思う。

【蔦田構成員（米沢構成員代理)】

○　特にクレジットカードの場合、国際ブランドが非常に大きな役割を示しており、ブランドの方からアプレットをサービスプロバイダに提供しているケースもある。

【小尾構成員】

○　諸外国の説明においてＳＩＭで鍵ペアを生成するという点について、現在、日本のモバイルキャリアのＳＩＭカードでも同じように実現可能なのか。公的個人認証サービスのアプリケーションのパーソナライズ手順を決める際の重要なファクターになる。つまり、公的個人認証サービスでも鍵ペアを生成しなければならないが、ＳＩＭの中で鍵ペアを生成できるかどうか、そもそも対応できないというのであれば外から入れるしかないが、できるのであれば、いろいろな課題はあるにしても、その方向で考えるというのも一つの手になる。

【橘井構成員（大道構成員代理)】

○　答えとして、できる可能性はある。ただしＳＩＭのセキュアエレメントの中にアプレットを仕込んでおくことが必要になる。その場合は、今のＳＩＭと全く異なる仕様になってしまうため、マイナンバー対応の専用ＳＩＭという形でのご準備させていただくことになると思う。

【進藤説明者】

○　概ね認識は同じで現行ＳＩＭでできる可能性はあると思う。ただし実際にＳＩＭのパフォーマンスとして性能を満たせるかと言った点では技術検証が必要であること、プリセットしないと内部生成できないとなればオペレーション自体が変わることなど、できるか否かは技術検証を通じて確認する必要がある認識。

【鴨志田構成員】

○　概ね認識は同じ。

【手塚主査】

○　このサブワーキンググループでは、本日ご説明いただいた民間活用における実現方法を参考に公的個人認証サービスの利用者証明機能を格納させることについての議論をまとめていく。

○　次回以降、ベンダーの皆様において、スマートフォンのＳＩＭカードに格納された電子証明書を使ったユースケースのご提案を是非お願いしたい。

⑵実現方法及び課題について

【小笠原情報通信政策課長】

○　今回事務局からご提案する実現方法は、ただいまご紹介のあった、ＳＩＭカードの中で鍵ペアが生成されるという方法を取らず、本日モバイルキャリアからご紹介のあった、現実で稼働しているサービスをベースに整理したもの。これに決めているというものではなく、今後、技術検証を行うとすれば、仮にこうしたシステムを前提にしてはどうかという提案。

○　先ほど、手塚主査よりモバイルキャリア三社とも非常に前向きであったことへのコメントがあったように、事務局としても、２枚目の電子証明書をＳＩＭにダウンロードすることに関するモバイルキャリアのスタンスについて改めて認識し直した。つまり、論点は、現実にサービスとして、運用ルールとしても動いているものがあり、それを個人番号カード、２枚目の電子証明書に適用していけるかどうかであるという点であることを再認識した。

○　これで決めるというものでなく、あくまで例であって、実証すべきシステムを考えていく際

のたたき台としてお考えいただきたい。秘密鍵の生成にあたっては利用者からの申込みが必要になるが、利用者証明用電子証明書の発行申請を電子署名かつオンラインで行うこと、Ｊ－ＬＩＳで生成された秘密鍵はネットワークを経由して書き込むことを前提としている。特に後者についてはご議論があったわけだが、既にご提供されている方式を前提にすれば、ネットワークから秘密鍵をＳＩＭに書き込むという方法となる。

○　課題についても事務局で整理したが、制度面の課題を除けば、現実のサービスで既に運用されているのを前提にし、公的個人認証サービスの利用者証明機能にあてはめた時、どのように適用するのか、あるいはデフォルメできるのか、技術的課題と運用面での課題についてどういった方向性が出てくるのか、関係者にどういったコストと作業が発生するのか、新たにプレーヤーとなるＪ－ＬＩＳをはじめとする方の既存システムへの影響について検証していく必要がある。手がかりという面からは既に動いているシステムやルールがあるので随分明確。制度面の課題については、もう一枚の利用者証明用電子証明書を発行することになるため、制度的措置が必要になるが、当然ながらユースケースとニーズ、コストや手続が関係者の受任の範囲にあるかどうかとの関係から制度措置ができるか決まる。また、先ほどモバイルキャリアからの紹介では、本人限定受取郵便を使って本人確認を実施しているとのことだったが、３ページ目以降、申請方法や本人確認方法、格納方法についてそれぞれのメリットとデメリットを整理。

○　事務局からの提案として様々課題はあるが、現実に運用されているシステムやルールを個人番号カードの利用者証明機能に適用する場合、今あるシステムやルールをそのまま適用できるのかというスタンスから考えてはどうか。このようなスタンスであれば、可能ならば２０１９年をもう少し早めることも視野に入れることが期待できるのではないかと思う。

○　手塚主査からお話のあったとおり、ユーザから見て、スマートフォンの中にある個人番号カードの利用者証明用電子証明書でどのような使い方ができるのか具体化されていくことも必要。実証に進に当たっては、実際のユースケースについても皆様のお知恵をいただきたい。

(3)　意見交換

【田村構成員（佐藤構成員代理)】

○　事務局からご説明のあったとおり、今動いている仕組みをご理解いただいた上、前向きに検討していただければと思う。その上で重要になるのが、ユースケースや利便性を考慮した運用面の課題をクリアすることであり、これらが整理されると実証も進めやすくなる。

○　本人確認をどうするかは本人確認のポリシーの問題。オンラインの場合、善意の代行を許容することにもなるが、善意の代行を許容するということは悪意の場合も想定しなければならない。今回、スマートフォンを個人番号カードに活用するにあたって、ポリシーとあわせて本人

確認をどうしていくのか検討していければと思う。

【鴨志田構成員】

○　繰り返しになるが、既に商業提供されている方式をうまくご活用することで、国民に対していち早くサービス提供できる素地が整う。是非前向きに取り組んで参りたい。

【橘井構成員（大道構成員代理）】

○　今日ご紹介させていただいたとおり、技術的には既に本サービスとして運用しているものであり、その枠内であれば基本的にすぐにでも提供できるサービスである。利用者である国民の皆様が便利に使えるユースケースを踏まえた上で、利便性、安全という外堀をうめていく形で議論を進んでいければと思う。

【川関構成員】

○　近年、ＭＶＮＯが提供するサービスのユーザも増加。ＳＩＭや端末はユーザが購入する形態。そういうケースも含めて利用者が利用できる仕組みを考えて行けたらいいと思う。

【宮野構成員】

○　我々は、国内中心に、決済、会員証等の機能をサービス提供者に代わってダウンロードするサービスを、古くはおサイフケータイ、最近では、スマートフォン向けの仕組みとして運用。

○　アプレット等をどう作成するか、ネットワークをどのように構成し、セキュリティを確保するのかについて、クレジットの場合、どのように認定し運用しているのか、モバイルキャリア、サービス提供者等の提供している仕組みを参考にしていただき、今回の公的個人認証サービスのダウンロード実現に向けて、我々からも知見を提供していきたい。

【林構成員】

○　Ｊ－ＬＩＳは、ここで表現されたパーツのいくつかを自ら作成する役割を担うことになると思う。先ほどＭＮＯ－ＴＳＭを使ったＳＩＭへのダウンロードの仕組みは既にあるというご説明をいただいたが、是非今後、議論するに当たって、検討材料としてそのサービスの内容、仕様をご提供いただき、検討を深めたい。

【小尾構成員】

○　今後、公的個人認証サービスを実際にＳＩＭカードに入れて、どのような形で使っていくか

というところまで踏み込んで検討していくことが必要。

○　日本では、国民の半分くらいがiPhoneという特殊な事情があるが、例えば、ＮＦＣについては、iPhoneは開放されてないため使えないが、今後もやはりアップルが情報開示してくれないと難しいという状況なのか。

【進藤説明者】

○　基本的に、iPhoneは今現在、モバイルＮＦＣサービス事例で紹介したようなＯＴＡでのＳＩＭへの情報書き込みを許容していないと認識している。iPhoneはアップル社提供の製品であるため、アップル社のプロダクト戦略の中で先方が検討されるか否かということになる。仮に本件が日本国内での公的個人認証サービスのいい事例として認識され、アップルのプロダクト戦略にそぐうようなことがあれば、アップル社としても一考する余地があるかもしれないが、今現在、そのような予定はないのではないかと認識している。

【小尾構成員】

○　最初はAndroidだけになってしまうかもしれないが、Androidで是非成功させていい事例としてもらいたい。

【村上構成員（田中構成員代理)】

○　ＳＩＭへの格納、ダウンロードにいたるまでには、申請があって、本人確認があって、それぞれ複数のパターンがある。例えば、格納のところではオンラインなのか窓口なのか、ＳＩＭカードでの鍵生成を検討するのか、個人番号カードの署名用電子証明書を使って電子申請する場合にはリーダが必要になるなど、その組み合わせによりパターンごとメリット・デメリットがあって絞れていくと思う。

○　それぞれ、利用者視点から、組み合わせのパターン、申請と本人確認、格納のパターン化と課題の深掘りに向けて協力していきたい。

【松田構成員】

○　ベンダーの立場としても、今後、ユースケースの検討を進めてまいりたい。

○　モバイル端末を使うメリットは２つ。1つ目は、個人番号カードを持ち歩くのが難しいというときスマートフォンのようなデバイスが最適であること、２つ目は利用者の認証という点で様々なケースが考えられること。

【野田構成員（四十谷代理）】

○　先ほど、ＳＩＭの中で鍵の生成のお話があったが、鍵を外に出さない点で圧倒的に安全ではあるが、ＳＩＭカードそのものの耐タンパー性の議論も必要となり、公的個人認証サービスの証明書の発行スキームを考えると、センター側で鍵ペアを生成し、ダウンロードする方がなじむのではないかと思う。

○　また、スマートフォンをなくした場合、通常、キャリアショップで即座に全て利用停止が可能となるが、今回の利用者証明機能のダウンロードを考えた場合、その利用停止の即時性はＩＣカードにない利便性であり、大いに強調できると思う。

○　一方、法的な失効ということで考えると、ＣＲＬ、失効リストに載せる、オンラインでＯＣＳＰ提供するといったところが中心になるが、そちらでの対応がなされないと失効したとは言えない。そうなると、スマートフォンを紛失した場合は、モバイルキャリアの窓口での手続、市町村窓口での失効申請を行わなくてはならなくなる。利用者の利便性を考えれば、どちらか一方にいけば両方とも解決するということも手続きの方法として整理していく必要がある。

○　ＩＴベンダーとして、利用ユースケースをまとめ、機会があればご紹介させていただきたい。

【木村構成員（熊木構成員代理）】

○　今後、ユースケースの検討について、ＩＴベンダーの立場でご協力させていただきたい。

○　ＳＩＭカードへの利用者証明機能のダウンロードの実現にあたって、運用レベルに引き上げるには検証が必要。一方、運用面での責任分界については、例えばＳＩＭカード自体がモバイルキャリアの所有になるので、ＭＶＮＯ事業者が増加している中、責任範囲を明確にしていく必要がある。我々も技術的観点含め協力したい。

【高橋構成員】

○　公的個人認証サービスに関わる実証に参加する立場から、様々な利用シーン、ユースケースを検討。本サブワーキンググループの議論では、Ｂ to Ｃに向けたサービスという視点が結構多かったが、Ｂ to Ｂという社内、社間も含めて、少し幅広くどういう利用シーンがあるのか、検討していきたい。

【吉本構成員】

○　運用の仕方によって、これが使いやすいかどうかというのが実際のビジネス上は非常に重要。技術的にはどういう方法がよいのかは合意できるところを選べばいいと思うが、実際、海外では、例えばタクシーの配車サービスの米Uber（ウーバー）のようにビジネスが先行し、あっと

いう間に全米で普及したものがある。新たなサービスを考える際、単に技術面だけではなく、運用面で使いやすい仕組みになっているのかどうかよく見ていく必要がある。

○　本日海外の商用サービスの事例の御紹介があったが、金融機関としては本人確認するのは一番重い本人確認でいいとは思うが、それ以外のビジネスの面ではもう少し軽めの方法もあると思う。ビジネス面でやりやすい決め方をしていくような議論をしていく必要がある。例えば、Uber（ウーバー）のようなサービスが実際どのように使われているのかについて、皆さんと情報共有して見極めていくのも重要。

【手塚主査】

○　本日の議論により、既に実サービスとして提供されているＳＩＭカードを使ったクレジット決済の例を参考にすれば、公的個人認証サービスの電子証明書をどのように格納すればいいのか、その仕組み、システムがだいぶ明らかになってきた。

○　本日のモバイルキャリアからのご説明においても、ＳＩＭカードの空き領域を活用して、公的個人認証サービスの利用者証明用電子証明書を格納することを新たなサービスとして歓迎いただいており、これを参考に進めることについて、本サブワーキンググループでも共通の認識。

○　次回以降、このクレジットの例を公的個人認証サービスに当てはめた場合、どのような課題が生じるのかを早急に明らかにし、次年度以降、実証を行い、課題解決を図っていくこととしたい。

○　構成員の皆様においては、本日事務局から提案のあったＳＩＭカードへのダウンロードする仕組みやシステム、実現に向けた課題について、妥当性、課題の詳細化や解決策、ユースケースのご提案をお願いしたい。期限としては１２月１１日に一旦ご提出いただき、最終的には年内目途ということで、１２月２５日までに事務局宛てに提出いただきたい。

○　また、スマートフォンの利活用の拡大、市場の拡大という観点から、現在、ＡＲＩＢで検討を進めているスマートフォンでの個人番号カードの読み取り（方式１、方式２）の実現についても、重要な視点。チップ性能も技術の日進月歩に伴い向上している現状からも、引き続きよろしくお願いしたい。

○　１２月中旬、本サブワーキンググループの親会にあたる「公的個人認証サービス等を活用したＩＣＴ利活用ワーキンググループ」開催。本サブワーキンググループの議論の状況については、私から報告させていただきたくが、報告内容については、本日の資料をベースとし、本日いただいた意見を盛り込んだ形とする予定。別途、事務局から照会させていただくが、最終的には主査である私にご一任いただく形をとらせていただきたい（異議なし）。

○　引き続き皆様の積極的な議論をお願いしたい。

【小笠原情報通信政策課長】

○　今月中に、「公的個人認証サービス等を活用したＩＣＴ利活用ワーキンググループ」、「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」を開催する予定。本日手塚主査がご発言された内容に沿って、ワーキンググループでは手塚主査から、懇談会では大山主査からご報告をいただくよう進めてまいりたい。基本的には、モバイルキャリアのご協力の下、ＳＩＭへのダウンロードの実現に向けて、現実に提供されているサービスを下敷きに検討できるという点から大きな前進があったという点をご報告することとしたい。

○　課題の詳細化、ユースケースのご提案などのご提出を１２月２５日とさせていただき、これらを参考に検証内容案を作成し、２月を目途に第３回を開催したい。

【手塚主査】

○　それでは、以上で第２回会合を終了する。

以上