eID 相互利用環境調査委員会(第 5 回)　議事録

■日時　　2021 年 12 月 13 日(月)　　10:00～11:40
■場所　　一般財団法人ニューメディア開発協会　A 会議室
■出席者　[委　　員]　　作田吉弘(東工大) 、土居仁士(東工大)、村松正男(東工大)
　　(Zoom 参加)　小尾高史 委員長(東工大)、久保高志(凸版印刷)、北村祐貴(ＮＴＴデータ)、
　　鈴木茜(日立製作所)
　　[オブザーバ]　　村山博康(NICSS)
　　(Zoom 参加)　細川敬太(総務省)、大山永昭(東工大)、矢部祐一(日本電気)、
　　平良奈緒子(東工大)、山口晃(ＮＴＴコミュニケーションズ)、
　　神力哲夫(大日本印刷)、野村真義(凸版印刷)
　　[事　務　局]　　永松理事長、中嶋、小林、宮井

(敬称略、順不同)

■配布資料

資料 1　　第 5 回委員会　次第
資料 2　　eIDAS 調査に関する進捗報告
資料 3　　eIDAS 調査報告＃ 3
資料 4　　eIDAS messages　　(資料 3 補足資料)
資料 5　　eIDAS 調査報告　課題一覧　(資料 3 補足資料)
資料 6　　eIDAS の Level of Assuarance
追加 1　　ｅＩＤ相互利用環境調査委員会　委員名簿
追加 2　　個人の証明を海外に対して行うためにローマ字表記を使う国の施策例

■議事概要

1. ２０２１年度ｅＩＤ相互利用環境調査委員会の開催に当たって

◆ 永松理事長［事務局］より、2021 年度初回の委員会開催に当たっての挨拶を行った。

本研究会は、ＪＫＡの補助を頂き、昨年度の調査研究事業として予定しておりました。しかし、コロナの影響で調査活動、特に EU の現地調査の実施目処が立たなくなるということで、来年 3 月まで期間を延長して頂けることになり、本日の委員会は、通算で第 5 回目となります。

コロナの方も新種コロナの感染拡大により予断は許さない状況でありますけれども、徐々に回復の兆しが見え始め、経済回復の機運も高まっております。こうした中で、今年の 9 月にデジタル庁が発足し、デジタル社会構築に向けたまさに司令塔として、経産省、総務省など関係省庁を束ねてマイナンバー利用の拡大やマイナンバーカードの普及などといった包括的かつ強力なデジタル戦略を進めて頂けると期待しております。当協会も、これまで 20 年以上に亘り、東工大のご指導を頂きながら、JPKI による IC カード利用システムの開発とか、国の依頼を受けて IC カードリーダライタの互換性検証事業も進めており、デジタル社会基盤としてマイナンバーカードの普及に貢献していければと考えております。本研究会は、我が国の JPKI のカードが海外においても利用可能になるように、また EU の eID カードが我が国においても使うことができるようになる。そのための相互利用環境について調査検討を行う者であり、今後、マイナンバーカードのグローバル社会における活

用の在り方を踏まえて、国としての普及戦略の検討に使って頂ければ大変幸いであると思っております。限られた時間でございますが、本日のご審議をよろしくお願い致します。

2. 事業内容について

◆ 小尾委員長の議事進行に基づき、下記の報告及び審議を行った。

(1) eIDAS 調査に関する進捗報告について

◆ 資料 2「eIDAS 調査に関する進捗報告」を宮井(事務局)より説明した。

昨年の 2020 年度の活動でございますが、この事業の目的は「公的個人認証サービスを用いたデジタルチケットの実用化に向け、eIDAS 規則に基づく EU 加盟国内に eID 連携の仕組みについて、運用環境を含む技術的な調査及び比較検討を行う」ことでした。2020 年度の活動としては、「諸外国における eID 相互利用に関する調査」として、EU に学ぶということで、eIDAS 規則の制定に至るまでの経緯を調べ、eIDAS 規則に基づく EU 加盟国の現状、EU 加盟国における eID 事情を調査しました。

次に「eID 相互利用に係る技術及び運用環境に関する検討」として、EU における eID 相互利用環境構築のための支援活動、Connecting Europe Facility (CEF)の資金援助プログラムについて調べました。昨年度の報告では、58 件でしたが、今年になって 10 件が新規に追加されている状況です。そして、eIDAS 規則他関連規則を紹介し、委員の皆様に eID 相互利用における課題抽出をお願いしました。これらは、表面的なものであり、本質的な技術調査としては不十分であったため、2021 年度は、この技術調査を本格的に行うという流れになっています。

そして、今回の目的で「デジタルチケットの実用化」を掲げておりましたので、EU におけるデジタルチケット事例やデジタルチケット関連事業者に対してヒアリング調査を行いました。3 頁の図は、その結果を踏まえて、購入時における本人情報の登録とか、利用時における権利保有者であることの確認とかを整理し示したものです。

4 頁、本年度の活動ですが、今回、技術調査として、公的個人認証サービスと海外 eID における eID 連携の実現可能性を見極める。そのために、JPKI 仕様を踏まえた技術調査を実施する。これが技術調査の位置付けです。当初のスケジュールでは、第 5 回委員会として 5 月末を想定していましたが、本日（12 月半ば）の開催となってしまいました。この技術調査に関しては、本日オブザーバで参加して頂いている NTT コミュニケーションズ株式会社殿と大日本印刷株式会社殿の協力を得て実施しております。今までの流れとしては、まずは、技術調査の進め方に関する打合せを行い、第 1 回報告会を 8 月 19 日に、第 2 回報告会を 11 月 5 日に行い、海外協力者への質問第 1 弾を 9 月 26 日に、質問第 2 弾を 11 月 26 日に送り、質問第 2 弾の回答は未だ頂いておりません。なお、第 3 回報告会は、本日、この委員会で行う予定です。また、海外協力者とのビデオ会議を 12 月 15 日 18 時から開催する予定になっています。

5 頁、調査方針は、「JPKI を利用する場合のインタフェースを調査し、そのための技術的要件を確認する」です。実際のシーケンスに関しては、ユーザがサービスサイドにアクセスして、認証要求が SP から eIDAS-Connector、eIDAS-Service を経由して、対外国の IdP へと伝搬する。IdP とユーザ間で認証のやり取りが行われ、その結果が SP に戻ってきて、うまく認証が出来れば、サービス利用が可能になるという流れです。

事業を開始した時点では国内イベントをイメージしていましたが、これでは、JPKI との連携が存在しないことになることから、海外の国際イベントに参加するという場面に切り替えて検討することに

しました。

6 頁、調査手順は、Step 1 から Step 5 までの 5 段階です。Step 1 では、調査ターゲットとして「海外の国際イベントへの登録」を仮置きしました。Step 2 では、eIDAS 技術調査やサンプルプログラムの分析を行い、このアウトプットが第 1 回報告会での報告です。Step 3 では、SAML のデータセットを確立するとし、このアウトプットが第 2 回報告会での報告です。今回、多少ずれているかも知れませんが、Step 4 (11 月末までの調査)のアウトプットが本日行われる第 3 回報告会での報告であり、12 月末までに、Step 5 (IdP とマイナンバーカードの連携についての検討)を行います。

7 頁、第 1 回報告会の報告内容ですが、調査の目的は「公開資料から eIDAS に関わる技術仕様を把握し、今後検討すべき技術要件を明確にし、検討を進めるための課題を整理する」ことです。

CEF 下の CEF Digital の中には、8 つの Building blocks が存在し、その中の eID Building block に関連した規則が eIDAS 規則です。調査としては、eID Building block の技術仕様を調査し、動作フローを整理しました。

8 頁、eID Building block の技術仕様ですが、メッセージ仕様は、SAML メッセージのフォーマットを規定したものです。eIDAS 相互運用アーキテクチャは、eIDAS-Connecter/eIDAS-Service 間のインタフェースの定義を中心に規定しており、暗号要件は、「eIDAS 相互運用アーキテクチャ」の中のセキュリティ要件を補足するものです。属性プロファイルは、SAML メッセージに含まれる Attribute の詳細を規定したものです。

9 頁、動作フローは図に示すとおりです。赤い四角で囲んでいる内容は、今後具体化しておかなければならないポイントです。10 頁は、実際のデータのやり取りは、ブラウザでのリダイレクトを通じて通信が行われることを示した図です。この辺の仕組みが事務局側で理解できず、第 1 回報告会から質問第 1 弾を海外協力者に投げるまでに、 1 か月程の時間を要してしまいました。

11 頁、調査を踏まえた 1 番目の疑問点は、「SAML Assertion 中の文字コード」です。その仕様や制限について確認しましたが、「知らない」という回答でした。但し、理論的には、UTF-8 以外のもの、UTF-16 を使用することが可能であるが、既存の CEF eID 基準実装ノードでは、UTF-8 を使用しているとの事でした。日本として、UTF-8 と UTF-16 のいずれを利用すべきであるかを決める必要があります。

12-13 頁、2 番目の疑問点は、「氏名、住所などの英語表記」についてです。日本語文字は表意文字と表音文字が混在しており、人によって読みが異なります。技術仕様書に、日本語文字と、日本語文字をラテン文字に transliteration(翻字/音訳)したものを併記する旨の記載があるため、日本語文字を適用する場合の対処方法について質問しました。質問文の中に、IdP で処理するといった記述をしたため、IdP ではなく、eIDAS-Service で処理を行うなど、本当に知りたい回答が得られなかったため、何度かメールのやり取りを行い、「日本語文字だけを送ることは許されない。日本語文字とラテン文字のペアを送らなければならない」ことが分かりました。では、日本語文字をラテン文字に音訳したものだけを送ることが可能であるのか。これについての質問メールを送りましたが、今のところ、回答が無い状況です。

14 頁、3 番目の疑問点は、「署名検証で利用する証明書の入手方法」です。事前に二国間でルート公開鍵証明書を交換する必要があることから、その方法を確認しました。二国間の交換プロセスを利用して証明者や URL を交換しているという回答でした。

15 頁、第 2 回報告会の報告内容ですが、調査の目的は「eIDAS で利用するメタデータやメッセージのサンプル作成を通じて、eID 連携の理解を深め、JPKI を利用した eID 連携を実現する際の課題を見つける」ことです。調査概要としては、メタデータや SAML メッセージのサンプル作成（16-21 頁、30-36 頁参照）です。この作業を通じて抽出した課題は、優先課題を課題Ａ、実運用までに解決すべき課題を課題Ｂの 2 つに分類しました。課題Ａのみを説明します。

１番目の課題(22 頁)は、JPKI の LoA（Level of Assurance)にについてです。eIDAS-Service の SAML Metadata（17 頁)には、3 つ（High, Substantial, Low）の LoA が記載されています。日本がこの 3 つのいずれまでのレベルをサポート可能であるか、つまり、日本の JPKI はどのレベルに該当するかを見極めて置かなければならないという課題です。なお、LoA の要求レベルを SAML AuthnRequest(34 頁)で指定し、適用される LoA のレベルを SAML Assertion(21 頁)で返すことになります。

2 番目の課題ですが、eIDAS-Service の SAML Metadata（18 頁)には、NameIDFormat として、3 つのパラメータ(Persistent, Transient, Unspecified)が記載されています。このパラメータは、IdP が生成する名前識別子(NameID)のフォーマットとして、永続的な識別子（Persistent Identifier)、一時的な識別子（Transient Identifiier)、指定なし（Unspecified）を示しています。この 3 つをサポートが必要であるのかどうか。JPKI の ID からこれらをどのように生成し、どのような値を設定すればよいのか。この点がよくわからないという課題です。

3 番目の課題ですが、SAML AuthnRequest（34 頁）によって、PersonIdentifier、CurrentFamiltName、CurrentGivenName、DataOfBirth など指定された属性値を SAML Assertion で返すことになりますが、実施にどのような属性値をサポートするかについては、SAML Metadata の中で定義します。日本とし、Mandatory な属性値のみをサポートするか。それ以外の属性値もサポートするか。そのサポート範囲を決定する必要があるという課題です。

4 番目の課題ですが、SAML Assertion の中で、２番目の課題で挙げた NameIDFormat が示す値(20 頁)と PersonIdentifier が示す値(21 頁)が同一です。また、NameIDFormat は、Persistent な値を返していますが、SAML AuthnRequest(34 頁)の NameIDPolicy で指定された形の値を返していると推定されます。この NameIDFormat と PersonIdentifier の関係、NameIDPolicy と NameIDFormat の関係など、SAML Assertion の中で返す Identifier(ID)についての理解を深め、JPKI の処理として、どのような値を返せばよいかを明確にする必要があるという課題です。

５番目の課題は、JPKI には「読み仮名」の情報がないことから、ラテン文字表記の要否を確認する必要があるという課題です。

課題抽出(22 頁)は、これら 5 つの課題を改めた書き直したものです。このうち、1 番目と 3 番目は、国内で検討しなければならない課題であり、5 番目は、既に質問中の課題です。23 頁は、4 番目の課題に関する参考情報です。

24 頁は、２番目と 4 番目の課題を踏まえた質問項目です。なお、回答は未だ頂いておりません。

●小尾委員長

今、事務局から説明を頂いたように、今年度の調査に当たっては、日本の JPKI と eIDAS の eID を技術的な面で接続可能であるかということを主な調査内容として検討してきたということです。今回、色々な課題という形で事務局からお話が合った内容は、仮に eIDAS-Node の一つとして日本を仮定して eIDAS-Node の実装を考えた時に、EU が公開している技術仕様を調査し、どのようなことが不明な点であり、どのようなことを今後検討しなければならないかを整理し、わからない部分について、

ＥＵ側に問合せし、回答を頂く形で進めてきたということです。よろしいでしょうか。

事務局から説明があった内容について、ご意見とかご質問とかがあれば、お願いしたいのですが、如何でしょうか。オンラインで参加されている方は、チャットでも良いので、手を挙げてください。

●作田委員

資料２の５頁目をお願いしたいのですが、技術調査の進め方【調査範囲】の補足的な説明で、外国のサービスを使用する時の認証手段として JPKI を使用する場合に限定するようなことが記載されています。その逆のケースは、最終的な報告書の報告対象にならないと、おっしゃっているのでしょうか。それとも、今回の技術的な調査の対象になっていないだけで、最終的な報告書には、逆のケースについても実現可能性についての結果を記載するというお考えでしょうか。

●事務局(宮井)

事務局としては、このリクエスト／レスポンスのやり取りは、逆のケースでは、リクエストとして受けているものを相手に送り、レスポンスとして返しているものを相手から受け取る。つまり、お互いに逆の関係にあると考えれば、双方向について検討していることになる。ですから、最終的な報告書に、逆のケースについても載せても大丈夫であろうと考えています。

●作田委員

少なくとも「できるか／できないか」について検討した結果が最終的な報告書に記載されるということなのか、それともこの段階で「逆のケースについては検討しない」ということをいっているのかが分かりませんでした。

最終的な報告書に、逆のケース、日本のサービスを外国の方が利用した時の認証として、利用者の自国の IdP を介して認証する場合に、それが可能か否かについて、報告書に記載するのですか／しないのですか。

●事務局(宮井)

調査事業全体としては、当初の計画に逆のケースも含まれていますので、報告書に記載します。

●小尾委員長

その他ご質問、ご意見がありましたらお願いします。

内容が結構、細かい話になっておりますので、一回説明を受けただけでは理解できない部分もあると思いますので、配布資料をご覧頂いて、わからないところや、不明な点があれば、事務局に別途、確認してください。

(2) 第３回技術調査の結果報告について

◆ 資料３「eIDAS 調査報告＃3」及び資料４「eIDAS messages」を神力オブザーバより説明した。

資料３の２頁は、事務局からお話があった、第２回報告会の目的でした。

調査報告＃３の目的は、前回(第２回報告会までに)、解析したメッセージをやり取りするためには、日本国側の eIDAS-Service と IdP/JPKI にどのような機能が必要であるか。どのような機能を使ってメッセージのやり取りをするかについて深堀し、この検討を通じて、JPKI と連携させる上で必要な課題を抽出することです。

調査報告＃３の内容(資料３の３頁)ですが、大きく三つの作業を行っています。

１つ目の作業ですが、SAML AuthnRequest とか、SAML Response とか言っているのが、先月末までの調査で整理した、やり取りするメッセージの名前になりますが、このメッセージのやり取りを行うに当たって、どのような処理が日本国内側に必要であるか、その処理内容を分析し、その中にはいろいろな暗号演算も出てくることから、暗号演算と暗号鍵とがどのように関係しているかということを分析しました。

２つ目の作業として、それを実現する際に、日本国内には、eIDAS-Service と JPKI/IdP の 2 つのエンティティが存在しますので、この間の役割分担を整理しました。

その上で、課題を抽出するのが３つ目の作業であり、この３つのステップで解析を進めました。

ここから具体的な内容に入ります。処理内容の分析ですが、このような形(資料 4 参照)で整理しています。資料 4 の上半分の図が eIDAS-Service、下半分の図が JPKI/IdP になっています。この 2 つのサービスがお互いにやり取りしながら、今回のサービスを提供しています。細かいところは飛ばしますが、基本的には、海外の eIDAS-Connector から受け取るデータもあれば、ユーザが持っているマイナンバーカード若しくはユーザ本人からとってくる情報もありますが、緑色で示すメッセージを外部から受け取って、黄色で示す処理を行い、青色で示すレスポンスを返すというのが全体像です。繰り返しますと、赤色がインプット、黄色が処理、青色がレスポンスと考えてください。

資料 3 の 4 頁は、資料 4 の図を模式化したものです。eIDAS-Connector は、海外にあるサービスであり、黄色で示すところが、日本国内で立ち上げなければならないものであり、海外との Connector との接点となる Service、実際に JPKI を使ったユーザ認証を提供する IdP、そしてマイナンバーカードの３つが、当然ユーザもでてきますが、この３つ＋ユーザが日本国側の関係者になります。

基本的には、eIDAS-Connector と eIDAS-Service との間で、事前にメタデータを交換しておいて、認証のリクエストを受けて、マイナンバーカードと利用者認証をした上で必要な情報（名前、性別等）に変える仕組みになっています。

資料４の図で示すように、緑色で示すものがたくさん出てきます。どのようなところに暗号演算が潜んでいて、どのような鍵を使うのかを分析しています。事前に交換しておかなければならない鍵もあれば、メタデータの中で別途指定される鍵や、実行時に生成する鍵もありますが、これを整理したものが、資料３の 5 頁に示す表です。

ここからが重要なところであると思いますが、今回の技術的な深堀りを通じて、幾つかの課題が出てきましたのでご説明させて頂きます。

一つ目の課題(6 頁)ですが、マイナンバーカードの JPKI アプリケーションの中には、２種類の証明書が入っています。これを実際に、どのように使うかというところの確認になります。今回の eID 連携では、姓、名、性別、誕生日といった情報を返さなければなりませんが、利用者証明の電子証明書には、この情報が入っておりません。署名用電子証明書の中に、これらの情報が入っています。したがって、eID 連携を JPKI で実現しようとすると、利用者証明書の電子証明書の情報だけでは不十分ということになります。

それでは、どのように実現するのかということですが、総務省殿が公開している民間利用のガイドライン(7 頁)によると、まずは、署名用電子証明書を使ってサービスの申込をしてもらい、運用時に利用者証明用電子証明書を使う、二段階の仕組みになっています。今回の eID 連携でも、この仕組みを使うことになるのではないかと考えています。この方針で次回までに、マイナンバーカードをどの

ように組み合わせるかについての技術的な調査を考えていますが、前提が変われば調査内容にも影響することから、署名用電子証明書だけを使ってサービスを組み立てられないかというような意見があればお伺いしたいと思っています。

マイナンバーカードには、8頁に示すように、2つの証明書が格納されており、それぞれ使い方が異なります。この資料に書き損ねてしまいましたが、これに関係した課題として、今回のサービスで使用する4情報が変更された場合に、署名用電子証明書は更新されるが、利用者証明用電子証明書は変更されずに、そのままキープされるように見えることから、4情報が変更されたことに気付けないという課題があるのではないかと考えています。この点に関しては、既存の民間サービスがどのように解決されているかが分かれば、ご教示を頂ければ助かります。

二つ目の課題(9頁)は、Family Name と First Name の分離が JPKI で出来ていないことです。事前登録時に情報をもらうというような想定で良いと考えていますが、もし違うということであれば、おっしゃってください。

三つ目の課題(9頁)は、SAML Service と JPKI/IdP の2つのサービスに分離することから、その間の通信のセキュリティをどうするかということです。

●小尾委員長

ご説明ありがとうございました。ご質問やご意見があれば、お願いしたいと思いますが、如何でしょうか。

(3) 欧州委員会とのビデオ会議について

◆ 資料2「eIDAS 調査に関する進捗報告」(25-28頁)を宮井(事務局)より説明した。

欧州委員会技術チームとのビデオ会議を明後日、12月15日18時(日本時間)より行います。参加のためのアドレスは、画面(25頁)に記載している通りです。皆さんの中で、ご参加を頂ける方がおられれば、別途でも構いませんので、事務局までご連絡をください。

26-27頁は、ビデオ会議の次第案です。

28頁は、今年の6月3日に公開された eIDAS 規則改訂案(Ver 2.0)に関する参考情報です。

もしビデオ会議で、こういうことも確認しておきたいということがあれば、ご意見を頂きたいと思っています。

●小尾委員長

ビデオ会議に参加されたい方がおられましたら、事務局に連絡してください。

事務局へのお願いですが、正式版のアジェンダが出ていないと思います。正式版のアジェンダを先方の参加者にも送ってください。

●事務局(宮井)

特に皆さんから他にご意見がなければ、現状のアジェンダの案を取って、正式版のアジェンダとして先方の参加者に送りたいと思います。

(4) 今後の予定

◆ 資料2「eIDAS 調査に関する進捗報告」(29頁)を宮井(事務局)より説明した。

今後の予定ですが、本日、この委員会において、11月末までに実施した技術調査報告(第3回)を行いました。引き続き、12月末までに技術調査を行い、その報告(第4回)を1月に第6回委員会として

開催したいと考えています。そして、報告書レビューとして第７回委員会を２月に開催したいと考えておりますが、如何でしょうか。

●小尾委員長

進め方に関しては、事務局の考えでよろしいかと思います。

最後の委員会は、報告書レビューとなっていますが、皆さんにご理解を頂くために、必要に応じて早めに資料を送るなり、メールにて質問を受けるなりのスケジュール感をもって、丁寧にケアをして頂ければよいと思います。

●事務局(宮井)

第４回報告会がいつ頃開催できるか、これを睨んで第６回委員会の開催日を決定したいと思いますが、この流れでよろしいでしょうか。

●小尾委員長

第６回委員会、第７回員会については、事務局サイドで検討を頂いて、開催時期が近くなったら、日程調整をして頂ければよいと思います。よろしくお願いします。

他に、何かございますか。

●事務局(宮井)

本日説明していない資料として、資料６があります。eIDAS の LoA を Commission Implementing Regulation (EU) 2015/1502 に基づいて整理したものです。ご覧を頂き、ここは違うのではないかとかのご意見がありましたら、事務局までご連絡をください。

もう一つの資料は、本日送付した「個人の証明を海外に対して行うためにローマ字表記を使う国の施策例」です。これは、新型コロナワクチンの接種証明書で、海外向けの場合には、パスポートを使って名前のローマ字表記を入れるというものです。本委員会での議論とは違いますが、名前のローマ字表記（ラテン文字表記）をどうするかについての参考情報としてご紹介しました。

3. その他(連絡事項)

●事務局(宮井)

先程も申しましたが、次回委員会に関しては、状況を見て、皆様のご予定を確認させて頂き、ご連絡を差し上げます。

●小尾委員長

今後も引き続き、委員会が開催されますので、本日の資料をご覧頂いて、質問等がありましたら、是非お願いしたいと思います。

最後に向けて、良い報告書が仕上がるよう、ご協力を頂ければよいと思いますので、今後ともよろしくお願い致します。

以上で委員会を終了と致します。本日は、ありがとうございました。

以　上

KEIRIN 競輪の補助事業

この事業は競輪の補助を受けて実施しました。
http://jka-cycle.jp