

「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則の一部を改正する命令案」に係る意見募集の結果について

令和6年6月12日

デジタル庁デジタル社会共通機能グループ

「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則の一部を改正する命令案」について、令和6年1月26日から同年2月29日まで御意見の募集を行ったところ、29件の御意見をいただきました。

いただいた御意見の概要及びそれに対するデジタル庁の考え方について、以下のとおりまとめました。なお、とりまとめの都合上、内容により適宜集約させていただいております。

貴重な御意見をお寄せいただき、厚く御礼申し上げます。

御意見の概要	御意見に対する考え方
<p>弊社では、Firebase を用いた ID 基盤を構築しており、Google ログインやメールアドレス認証を利用しています。しかし、弊社ドメイン特性上、マイナンバーカード認証との相性が非常に良いものがあります。</p> <p>そこで、マイナンバーカード認証について、既存事業者が実装しやすいような、Firebase Authentication、Auth0、Amazon Cognito に準拠した実装がしやすい仕様である必要性があると考えます。</p> <p>理由</p> <p>マイナンバーカード認証は、本人確認の強度が高く、利便性にも優れていることから、今後ますます普及していくことが予想されます。しかし、マイナンバーカード認証の仕様が既存の認証サービスと異なる場合、既存事業者がマイナンバーカード認証を導入する際に、実装コストや開発期間が増える可能性があります。</p> <p>そのため、マイナンバーカード認証の仕様は、既存の認証サービスとできるだけ共通化することが望ましいと考えます。これによ</p>	<p>デジタル認証アプリは、OpenID connect 等の標準的な仕様を採用しています。</p> <p>民間事業者の IDaaS システムとも連携しやすいものと理解しておりますが、認証機能を含む既存の民間サービスについてもご活用いただければ幸いです。</p>

り、既存事業者は、マイナンバーカード認証を導入する際に、新たな認証サービスを導入するよりも、既存の認証サービスにマイナンバーカード認証機能を追加する方が、実装コストや開発期間を抑えられるようになります。

具体的な提案

具体的には、Firebase Authentication、Auth0、Amazon Cognito の各サービスで、マイナンバーカード認証に対応する API を提供するとともに、それらの API のインターフェースを共通化する提案をします。これにより、既存事業者は、どの認証サービスを利用する場合でも、マイナンバーカード認証を実装するために必要なコードを、ほとんど変更することなく再利用できるようになります。

結論

マイナンバーカード認証の普及を促進するためには、既存事業者がマイナンバーカード認証を容易に導入できるようにすることが重要です。そのためには、マイナンバーカード認証の仕様を既存の認証サービスと共通化する必要があると考えます。

以上、ご検討のほどよろしくお願ひ申し上げます。

認証のためには、同等以上の暗号強度と現実的な耐タンパー性があるパスキーで代替可能であるから、ログインのためのユースケースが十分に活用されるとは思えない。事業者サイドで有効性確認サービスを提供しないので、犯罪収益移転防止法や古物営業法における本人確認の用に供することができず、法令で求められる本人確認のためのユースケースが十分に活用されるとは思えない。

OIDC で解放するとしても、OIDC の利用のためには Client ID の発行を受ける必要があるが、発行のための審査が依然事業者の負担となる。同様の事例として、マイナポータル API は、情報公開をすすめてはいるものの、主に審査のハードルの高さによって普及していない。従って、審査に関する大幅な飛躍がない限り、こちらも普及するとは思えない。

また、他の事業者が同様の取り組みを行っており、本アプリは他事業者に対するダンピングに相当するものにほかならない。

したがって、本アプリの導入はするメリットがない、またはすべきではない。ゆえに、これに付随する本施行規則改正もすべきでない。

マイナンバーカードによる認証を負担なく迅速に利用できる基盤を構築する観点から、デジタル認証アプリも活用し、官民のサービスのオンライン化の推進・発展に取り組むことで、安全で利便性の高いデジタル社会を構築してまいります。

・利用者証明用電子証明書の民間での利活用が進んでいない原因として、コストが挙げられており、原因の1つではあると思いますが、課題は他にもあると考えています。

中でも民間事業者目線で大きな課題と考えられるのは、都度物理カードを手元に用意してスマホに読み取らせなくてはならないUXの悪さです。

活用例としてECサイトが挙げられていますが、ECサイトへのユーザ登録時であれ購入時であれ、マイナンバーカードの読み取りを必要とさせることはユーザのドロップに繋がるのが明らかで、本人確認をしたくても、APIが無料で使用できても、活用することは到底できません。

(iOSとAndroid両方で解決される必要があります。)

・デジ庁がOIDCのOPとなる構成かと思いますが、ユーザがどのようなサービスを利用しているのかがデジ庁に丸わかりというのをプライバシーの面で嫌がるユーザもいると思われます。

・民間事業者向けの署名検証・有効性確認サービスは提供しないとありますが、これは既存のPF事業者を守ることを意図してのものでしょうか。

使い勝手の良いAPIとなるのか疑問です。既存のPF事業者のサービスから移行できる利用者は無料のAPIに移行してしまうと考えられます。

既存の事業者のAPIとのジレンマで微妙な立場のAPIになると思われます。

・上記の課題への対応策として考えられるのは、デジ庁がマイナンバーカードのVerifiable Credentialを発行するIssuerを構築することです。

デジタル認証アプリは、将来的にはスマホ用電子証明書にも対応していく予定です。対応できた場合は、カードをかざすことなく利用することができます。

デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報の保護に関する法律(以下「個人情報保護法」といいます。)に基づき適切に取り扱います。マイナンバーカードの電子証明書の発行の番号(以下「シリアル番号」といいます。)をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。

国民の皆様に対しても、安心して利用いただけるよう、デジタル認証アプリのメリットや安全性について、分かりやすい説明に努めてまいります。

<p>有効期限を設けた VC を発行し、都度の物理カードの読み込みは不要なものとする ことで、普及さえすれば EC サイトなどのサービス側も耐えうる UX になると考えられます。 デジ庁が Issuer のみの役割を担えば (Issuer のみとして使うことをユーザが選べれば) デジ庁に監視されるという問題もありません。 マイナカードの VC を発行できるのは政府のみであり、民間がどう頑張っても実現できないものですので、デジ庁が対応することに非常に価値があります。</p> <p>・ Holder や Verifier は民間でも構築できるものですので、まず Issuer 構築と regulation の整備 (Google, Apple が独占しないようなルールも必要) に力を割いていただくのが良いと考えています。</p>	
<p>デジタル化は促進すべきでない地震大国であるこの国は災害でインフラが使い物にならなくなった時アナログが大きな意味を持つプライバシーの観点からもデジタル化は促進すべきでない。</p>	<p>いただいた御意見は、今後のデジタル政策を検討する上で参考とさせていただきます。</p>
<p>マイナンバーカード (以下、MNC) から個人情報を読み取るという機微な領域において、民間のサードパーティアプリではなく政府機関公式アプリで実現することで、利用者における心理的抵抗の軽減と、サービスプロバイダーにおける経済的負担の軽減が期待できるので、積極的に利用したい思いである。一方、広く世の中に本アプリを普及させるためには、利用を希望する事業者が簡単に (手続きが容易で、スピーディーに) 利用できることが必要と考える。また、準公共サービスと民間ビジネスアプリで本アプリの利用可否と利用できる機能の範囲 (署名 / 認証) が変わるとのことなので、利用可否承認プロセスや、審査にあたってエントリすべき情報は何か、審査リードタイムはどの程度か、準公共サービス</p>	<p>本案についての賛同の御意見として承ります。 いただいた御意見は、今後の検討に当たって参考にさせていただきます。</p>

と民間サービスの線引きはどのような基準といった情報が明確であると有難い。なぜなら、リジエクトリスクを考慮・軽減するべくそれらを踏まえた上でプロジェクト計画を立案する必要がある為である。また技術面についても、ニッチで特殊なテクノロジーの理解を必要とせず、事業会社であっても（SIerのようなテクノロジー会社でなくとも）技術面でのアセスメントが可能であり、且つ技術者の調達が容易であることが望ましい。

そして、持続可能なサービスであるためには、サービスプロバイダーをサポートする問い合わせ窓口など開設されるのが望ましく、また経済面でも長期的に無償で利用し続けられることを期待したい。

さらに、本アプリのバージョンアップや仕様変更、バージョン間の互換性、あるいはメンテナンスの予定など、本アプリを利用した施策を展開する事業者が、前広にそれらの情報を知り得る仕組みが必要との認識である。バージョンアップについて欲を言えば、例えばMNCがじきにスマートフォン内部へ格納されることに併せて、スマホ内部に格納されたMNCから読み取ることができるライブラリを提供するなど、MNCを取り巻くまわりのデジタル施策に合わせて機能拡張されることを期待している。

いずれにせよ、当方はリアルの良さとデジタルの組み合わせで顧客体験を大きく高め、「一人ひとりにやさしく便利で豊かな世界」を実現するべく、官民一体となり本アプリの利活用を推進し、デジタルネイティブの加速化へ一助を担いたいという思いである

国の個人データの取扱いと同様に、民間企業における個人データの取扱いに信用がおけない場面がこれまでもありました。そのため、民間だけでなく、国による認証サービスを利用できるという選択肢が生まれるということは、全体としてバランスが取れた健全な方向性だと考え、趣旨に賛同します。

特に、国・行政が国民に提供する公共性の高いサービスについては、可能な限り安価に実現・提供されるべきであり、国が認証業務を行うことでそれが実現できるのであれば、国民にとってそれに越したことはありません。

民業圧迫という意見が出てくるかもしれませんが、その場合は、国が無料でサービス提供できる範囲について一部制限を設ける事で問題は解消できるため、本命令案に強く賛同します。

デジタル認証アプリは、今後の公的個人認証（以下、「JPKI」という）発展において、現時点アプリをお持ちでないWebサービスを主とするお客様においても、マイナンバーカードの読み取りと公的個人認証を可能にするツールとして活用いただけるものと考えております。一方で、デジタル認証アプリの台頭により既存のPF事業者、SP事業者のビジネスへ影響を及ぼすことが危惧される点もあり、これら不安を払拭していくことで、官民がより一丸となってJPKI拡大に取り組めるものと期待しております。

P3

デジタル認証アプリを用いて利用者証明用証明書を利用した本人認証を実現する経路を用意されることは、利用を促す取り組みとして有用であると思われま

本案についての賛同の御意見として承ります。

いただいた御意見は、今後の検討に当たって参考にさせていただきます。

いただいた御要望は、今後の検討に当たって参考にさせていただきます。

がら、デジタル認証アプリを「マイナンバーカードの読み取りと公的個人認証を可能にするツール」として活用できるよう、署名機能と同様に、認証機能においても利用者証明用電子証明書を利用した署名だけが行える（署名検証、有効性確認はSP/PF事業者が行う）経路を用意いただきたいと考えております。

事業者が自己のビジネスモデルに基づき、デジタル認証アプリで本人認証を完結させるか、サービストータルの魅力を鑑みデジタル認証アプリでは読み取りのみを行い署名検証や有効性確認はSP/PF事業者のサービスで行うかを比較検討できるようになることが望ましいと存じます。

P7

準公共サービスのエリアにおいてはデジタル認証アプリの署名利用も想定されている図となっておりますが、準公共サービスが示す範囲を資料上に例示いただくことをご検討ください。

例えば、自治体の地域通貨発行における本人確認は準公共の範囲か、自治体が管理する施設利用時の本人確認はどうかなど、いくつか例示いただくことで、官民協調領域を検討する一助になるものと考えております。

P8

スマホ用電子証明書について、民間アプリのみでスマホ用電子証明書へのアクセスを可能とできる方法もご検討ください。

現時点、スマホ用電子証明書へのアクセスはマイナポータルアプリを経由することが必須となっておりますが、利用者の操作性向上がサービスの重要指標となる昨今、複

<p>数アプリを行き来するのは実装を躊躇わせる一因であり、事業者のアプリ単独で操作を完結させるニーズが根強く存在します。</p>	
<p>公的個人認証（JPKI）については、マイナンバーカードを読み取り、国民の本人確認を行うという点において、政府が一元的に管理されるべき事柄であると考えております。</p> <p>現状におきましては、民間団体・地方公共団体のそれぞれのユースケースにおいて、マイナンバーカードの読取りアプリケーションが乱立しており、国民等利用者は対象団体に合わせて、スマートフォンにアプリケーションをインストールするという事象が起きています。</p> <p>マイナンバーカードの利活用・公的個人認証（JPKI）の本格的、かつ、安定した運用においては、やはり政府（官公庁）から提示される仕組みを利用すべきと考えており、この度のデジタル認証アプリの展開について、弊社としては大きく賛同しています。</p> <p>マイナンバーカードの利活用において、多くの国民等利用者にマイナンバーカード、ならびに公的個人認証の有効性が伝わっていない現状があると思われ、デジタル認証アプリを提供されることで、本格的な利用推進に繋がるのではないかと考えております。</p>	<p>本案についての賛同の御意見として承ります。</p> <p>いただいた御意見は、今後の検討に当たって参考にさせていただきます。</p>
<p>「命令案」第二十九条の電子署名等確認業務受託者に内閣総理大臣を加える改正、並びに関連資料「デジタル認証アプリについて」の6ページ目のシステム連携想定イメージ、7ページ目のサービス提供領域を鑑みると以下のプライバシー上の懸念がある。</p> <ul style="list-style-type: none"> 電子署名等確認業務受託者に内閣総理大 	<p>デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。国民の皆様に対しても、安心して利用いただけるよう、デジタル認証アプリのメリッ</p>

<p>臣を加えることにより、行政府が電子署名等確認業務全般を遂行可能になることが可能になる</p> <ul style="list-style-type: none"> ・その結果としてデジタル庁がデジタル認証サーバを持ち電子署名等確認業務を遂行することが可能となる ・上記と並んでサービス提供領域が準公共・民間となることを鑑みると、結果的として行政府が利用者が個人番号カード用利用者証明用電子証明書を行使する対象システムについての把握を行うことが可能となる <p>上記懸念より、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律に対して以下の条項を追加することが望ましいと考える。</p> <ul style="list-style-type: none"> ・利用者証明認証業務の第二三条について、現状の「利用者証明利用者符号」に加えて「電磁的な記録（ログ等）を含む利用者証明認証行為の行使先に関する記録」についても適切な管理対象とする 	<p>トや安全性について、分かりやすい説明に努めてまいります。</p>
<p>JPKI サーバ、デジタル認証サーバに残る情報はどの程度か明確でない、マイナンバーカードの認証情報が蓄積されるなら、個人を特定できるのでそれは個人情報ではないでしょうか匿名化のプロセスを明示してほしいです</p> <p>便利になります、国がチェックするから安心でしょ、は説明になりません</p> <ul style="list-style-type: none"> ・民間の認証を政府が確認するというのは政府の介入があるというように見えます ・政府の認証を総理大臣が確認する場合も同様です ・民間から仕事を奪うことにもつながるのでは？ ・カルト宗教や偏った一部の団体が政府に接近した結果として擬態した企業に情報が 	<p>デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。国民の皆様に対しても、安心して利用いただけるよう、デジタル認証アプリのメリットや安全性について、分かりやすい説明に努めてまいります。</p>

<p>流れることは無いのか いずれも情報の利用の仕方が明確でないから不安で、情報はすべて適時に開示されるべきです</p> <p>ことを決めてしまってから「丁寧に説明する」のではなく、ことを始める前に議論を尽くし、一つずつの論点について回答を示していただきたい</p>	
<p>公的個人認証サービスポータルサイト >制度に対応した法令等一覧 >認証業務及びこれに附帯する業務の実施に関する技術的基準 を見る限り、JLISでのログ保存は問題ない。(否認防止用) しかし、デジタル庁のデジタル認証アプリサーバは問題なので、アプリサーバーで保存する障害調査用のログは、毎日更新される秘密鍵を使って、暗号化して保存し、一定期間経過後に秘密鍵を捨てる手があるかもしれない。(暗号的削除)</p> <p>第三十一条 第三号 電子署名等確認業務以外の業務において、署名用電子証明書の発行の番号又は利用者証明用電子証明書の発行の番号（以下この号において「署名用電子証明書の発行の番号等」という。）を、個人を識別し管理するための 符号として直接に使用せず、署名用電子証明書の発行の番号等に対応し、署名用電子証明書の発行の番号等に代わる番号、記号</p>	<p>デジタル認証アプリのリリースに当たっては、各種法令を遵守した上で、厳格なアクセス制御、暗号化などのセキュリティ対策を講じてまいります。</p>

その他の符号を使用すること。また、署名用電子証明書の発行の番号等を外部に提供しないこと

(電子署名等確認業務の実施のために必要な場合を除く。)

https://www.jpki.go.jp/jpkiguide/lawindex_pdf/jpki_guide_law18.pdf

デジタル認証アプリについては、個人が官民の各種サービスを利用した履歴が一元管理され、不当な個人のプロファイリングや、関連性のないデータによる個人の選別・差別、国家による個人の監視などの個人の権利利益の侵害や個人の人格権侵害のリスクがあります(マイナンバー法1条、個人情報保護法1条、3条、憲法13条、「マイナカード利用「認証アプリ」、個人の利用状況を国が一元管理のプライバシーリスク」2024年2月26日付日経クロステック参照)。そのため、「法律による行政の原則」(憲法41条、65条、76条)の観点から、公的個人認証法の施行規則の一部改正だけではなく、マイナンバー法そのものを一部改正し、根拠条文を設置し、利用目的や目的外利用の禁止、安全管理措置等を規定し、違法・不当な利用に歯止めをかけるべきと考えます。

また、デジタル認証アプリで収集された個人情報(「連続的に蓄積」されたサービス利用履歴等も含む。個人情報ガイドライン(通則編)2-8(※)参照。)についても、

デジタル認証アプリにおいては、個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱い対応します。シリアル電子証明書の発行番号をもとに、氏名等の4情報を照会することは、目的外利用に当たると見なされ、行うことができません。

また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。

なお、デジタル庁を含む署名検証者については、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律(以下「公的個人認証法」といいます。)第52条及び第53条において、シリアル番号を含む、地方公共団体情報システム機構から受領した電子証明書失効情報等について確認以外の目的での利用・提供が禁止されています。

<p>利用目的の制限、第三者提供等の制限、安全管理措置、保存期間の設定、データ最小限の原則、開示・訂正請求など本人関与の仕組みの策定、情報公開・透明性の仕組みの確保、不適正利用・プロファイリングの禁止などの法規制がなされるべきと考えます。</p> <p>さらに、マイナンバーカードの電子証明書の発行番号（シリアル番号）についても、マイナンバー（個人番号）に準じたものとして扱うように法規制し、利用目的の厳格化、目的外利用の禁止、第三者提供の制限、厳格な安全管理措置などの法規制を、マイナンバー法を改正するなどして盛り込むべきだと考えます。（同様に、マイナンバーカードやマイナポータルなどについてもマイナンバー法に根拠条文が非常に少ないため、これらについても「法律による行政の原則」の観点から、政令や施行規則・通達等の整備ではなく法規制を実施すべきだと思われまます。）</p>	
<p>マイナンバーカードに格納される電子証明書は、個人番号に紐づけられている一意の番号であるから、個人番号と同等の取り扱いが必要であると考えられます。</p> <p>したがって、使用用途も個人番号と同様となり、目的外の利用、例えば認証を行ったサービスの横断的な統計処理、電子証明書番号から逆算したサービスの利用状況の取得については禁止とすべきです。</p>	<p>デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。</p> <p>なお、デジタル庁を含む署名検証者については、公的個人認証法第52条及び第53条において、シリアル番号を含む、地方公共団体情報システム機構から受領した電子証明書失効情報等について確認以外の目的での利用・提供が禁止されております。</p>
<p>< 認証業務に関する官民役割に関して ></p> <ul style="list-style-type: none"> ・国際的にも様々な技術が今後も現れ、政 	<p>御指摘いただいた事項に関しては、今後官民連携して運営する協議会において検討する予定です。</p>

策課題・国際協調課題を継続的に進化させなければいけない本分野に国が責任をもって関与し、資金を投じていただけることは大変喜ばしいことであり、諸外国の動きに伍していくのみならず、日本の国際的なプレゼンスにふさわしい活動を展開いただけるものと期待します。

・行政関係の様々な認証がこのような統一的な活動となっていく中で、民間も呼応する必要があると考えております。民間の理解を促進し、民間がこれを利用してビジネスを拡大していくために、情報・戦略の共有、民間から新たなサービス、産業が生まれるような機会を醸成すべく、官民が情報共有するような協議会、団体等の活動を活性化すべきではないかと思えます。

・つきましては、下記の事項に関して、官としての対応はいかにお考えでしょうか。

1 デジタル認証アプリの適用範囲に関して、関連資料『デジタル認証アプリについて』に『民間事業者向けの署名検証・有効性確認サービスは、提供しません。』とありますが、具体的な適用範囲を官民で協議する体制整備。

2 デジタル認証アプリの運用に関して、現状のPF事業者の役割も含め適切な体制の整備はいかにあるべきかの検討。

3 多段フェデレーションによる適用範囲の不当な拡大を防ぐ方策についての検討

4 次世代自己主権型アイデンティティの社会実装に向けた官民協働の取組

<プライバシー課題への対応に関して>

1 電子署名等確認業務受託者に内閣総理大臣を加え、国が直接利用者証明サービスを提供することとすると、どのサービス事業者を介して誰の認証が求められたかという情報を国が把握することとなります。しかも、このサービスをナショナルインフラとして提供する場合、国が把握する情報の範囲は極めて広いものになる可能性があります。これにより国民のプライバシーが侵害される懸念があるのではないのでしょうか。

上記の懸念を払拭するために国民が納得できる仕組みが構築されるかどうか、以下の各観点からどう考えますか。

(1) 国民のプライバシーを侵害しないための法律上の仕組み

(2) 国民のプライバシーを侵害しないための技術的な仕組み

(3) 国がナショナルサービスとして認証基盤を統合していくことに対する国民の理解

2 今般の改正案では、PF事業者とは異なり、電子署名等確認業務受託者としての内閣総理大臣には特段の監督機関が設けられていません。個人情報保護法上の監督機関としては個人情報保護委員会がありますが、電子署名等確認業務受託者を担うデジタル庁も個人情報保護委員会も内閣総理大臣の直下の組織であり、デジタル大臣は個人情報保護委員会の担当大臣を兼ねています。電子署名等確認業務受託者を担う内閣総理大臣ないしデジタル庁を監督する機関及びガバナンス体制の構築についてはどう考えますか。

デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。なお、個人情報の取扱いに関しては、独立性の高い、いわゆる3条委員会の個人情報保護委員会の監視、監督を受けることとなります。

<p>内閣総理大臣をデジタル庁が権限者として設けているが セキュリティの基本からすると余りに紐付けが大雑把すぎるのではないか？ そもそもであるがデジタル庁が署名業務を取り扱える格として別途制限された権限が必要なのではないか。 また、認証時に保持する連携先サービスや認証を実施した時刻ログ等の情報の取り扱いに付いても特段の理念的規定がないためその気になればタスポであった様に警察による個人の追跡等、国民の行動追跡を行政ができてしまう濫用の可能性をはらみ、要らぬ疑念を呼び起こすことから普及の大きな妨げになっていると愚考する。</p>	<p>デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。</p>
<p>番号制度においては「今後の法案策定作業を念頭に政府・与党として方向性を示すもの」として社会保障・税番号大綱が策定されており、認証アプリにおいてもこの大綱に沿った法案策定や設計を行われるべきである。</p> <p>認証アプリにおいては、マイナンバーカードに格納される電子証明書のシリアル番号を用いて個人を識別することになるが、シリアル番号は高い悉皆性と唯一無二性、10年間という長い有効期間を持つ番号であり、行政機関にとっては本人を特定できる識別子となる。</p> <p>さらに、自治体においては電子証明書のシリアル番号と住民情報を紐づけるDBを持っていること、また今後デジタル庁は自治体を利用するシステムをSaaSとして提供する方針を示していることから、デジタル庁は証明書のシリアル番号とSaaSとして自治体から預かった各種個人情報、そして認証アプリを通じて連携しているサービスの情報を照合することができる機関となり得る。従って、認証アプリを通じてシリアル番号を用いて集約される利用サービスの情報は</p>	<p>デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に対応します。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。</p> <p>なお、デジタル庁を含む署名検証者については、公的個人認証法第52条及び第53条において、シリアル番号を含む、地方公共団体情報システム機構から受領した電子証明書失効情報等について確認以外の目的での利用・提供が禁止されております。</p>

<p>プライバシーインパクトの大きい情報であり、その取扱いには慎重な設計が求められる。</p> <p>社会保障・税番号大綱では「1 国家管理への懸念」「2 個人情報の追跡・突合に対する懸念」「3 財産その他の被害への懸念」という3つの懸念に対処するための各種の制度上およびシステム上の保護措置の措置を講じることとしており、特に1 国家管理への懸念、2 個人情報の追跡・突合に対する懸念については、認証アプリにおいてもこれが起き得ないような仕組みと透明性が求められる。</p> <p>そのため、認証アプリのサービス開始に先立って、特に「第三者機関による監視」「自己情報へのアクセス記録の確認」「法令上の規制等措置」「罰則強化」「アクセス制御」「個人情報及び通信の暗号化」について実効性のある対策が取られるべきである。</p> <p>具体的には、個人情報保護委員会の監視・監督を受けること、認証アプリを通じて管理される利用サービスの情報についても個人情報であるとみなし、法令上の規制を行い不当なアクセスについては罰則を設けること求める。</p> <p>また、各個人が利用したサービスの情報へのアクセスの記録やアクセス制御、個人情報及び通信の暗号化を行う技術的な仕組みについて公開してプライバシーに関する有識者の意見を求め、十分に個人情報を保護できていることを確認するべきである。</p>	
<p>カード持ち歩きに繋がり 情報漏洩のリスク上がります やめてください</p>	<p>今回のサービスに関しては、個人情報保護法も踏まえ、厳格なアクセス制御、暗号化などのセキュリティ対策を講じてまいります。</p>

・デジタル認証アプリは、OpenID Connectの仕組みを利用してサービス事業者提供される。民間ビジネスアプリが、デジタル認証アプリを利用する場合、「サービス事業者」は「みなし署名検証者」または「みなし利用者証明検証者」の位置付けとなりますか？

・既に民間ビジネスアプリが民間のプラットフォーム事業者による署名検証者から「みなし署名検証者」としてJPKIに署名用電子証明書を利用した本人確認（犯収法施行規則のワ方式）を利用している場合、併用してデジタル認証アプリを利用することは可能ですか？

・デジタル認証アプリは、活用例にネットバンキングのオンライン本人確認の記載がありますが、犯収法施行規則へ方式の場合、容貌の撮影して券面の顔画像と一致させる必要があり、券面入力補助APに加え券面APによる券面の顔写真の画像の取得が必要になるため、券面APも必要ではないでしょうか？

内閣総理大臣が受託可能な電子署名等確認業務の範囲を利用者証明用電子証明書に限定したうえでの施行を希望いたします。今回の改正案施行により、内閣総理大臣は電子証明書の種類を問わず民間事業者における電子署名等確認業務を受託可能となると解釈しております。デジタル庁様交付資料「デジタル認証アプリについて（2023年12月14日付）」記載の「民間事業者における利用者証明用電子証明書の利用促進を目的としてデジタル認証アプリの機能を提供する」という趣旨に則り、受託可能業務の範囲を限定していただきたいと考えます。

デジタル庁様および総務省様にて策定され

デジタル認証アプリを利用するサービス事業者の位置付けについてはご理解のとおりです。

既にプラットフォーム事業者に電子署名等確認業務の全部を委託している事業者であってもデジタル認証アプリを利用することはできますが、デジタル認証アプリは、民間事業者向けの署名検証・有効性確認サービスは提供しない点にご留意願います。御提案いただいた機能を含め、リリース後も必要な機能の提供に努めてまいります。

貴重な御意見として今後の参考にさせていただきます。

ております「公的個人認証サービス利用のための民間事業者向けガイドライン第1.3版」P.28にて、PF事業者の提供するシステムをSP事業者が共同利用することでコストの低廉化が実現できるとの記載がございます。

「デジタル認証アプリについて（2023年12月14日付）」3スライド：「デジタル認証アプリプロジェクト概要」記載内容を踏まえると、本法改正は電子署名等確認業務のコスト低廉化を目的として全部受託者に内閣総理大臣を追加するものと理解しております。コストの低廉化を図るこれらの両施策が競合するものと推察しております。

また、地方公共団体をはじめとする行政機関におかれましても、PF事業者と接続した民間のITサービスを共同利用し業務効率化するケースも多く存在していると認識しています。これらのケースもPF事業者にとっては従前より「割り勘効果」を発揮するための大切な顧客領域であり、PF事業者とデジタル認証アプリとの競合が生じないよう対処いただきたいと考えます。

加えて、既に複数の民間事業者にて「マイナンバーカードICチップからの電子証明書読出および署名値生成」に必要なスマートフォン用アプリが提供されていると認識しております。このようなアプリ提供事業者のサービスと今回の認証アプリのサービス提供範囲が重複し、場合によっては民間事業者にて検討・提供されている既存サービスに影響を及ぼすと思料しております。

本法改正案による民間事業者の既存事業への影響が想定されるため、冒頭記載の通り、デジタル庁様より「デジタル認証アプリについて（2023年12月14日付）」にて記載いただいた趣旨に則り内閣総理大臣の

<p>受託可能業務を限定した内容での法改正を希望します。</p>	
<p>本件は、マイナンバーカードの利用者証明用電子証明書 AP と券面事項入力補助 AP を利用した IdP をデジタル庁が運営し、民間を含めた各種事業体に市民の属性を提供可能とするものである。このことは、「デジタル認証アプリについて」より読み取ることができる。しかしながら、このような機能を民間であるプラットフォーム事業者ではなく政府自体が提供するにあたって必要と思われる以下の規律が設けられていない。</p>	<p>貴重な御意見として今後の参考にさせていただきます。 なお、デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第 29 条第 2 項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。</p>
<p>【市民のサービス利用先情報の政府への蓄積に関する規律の必要性】 IdP サービスを政府が提供すると、市民がどのサービスにいつログインしようとしたか、どのようなデータを提供したかという情報が政府が取得できてしまう。そのような情報が政府によって無制約に取得されてしまうと、プライバシー侵害の問題や国民の行動監視の問題を生じることになる。本命令案では、このような取得されるデータの利用目的制限、利用制限、データの保管期限制限に関する規律が設けられていないが、政府が直接サービス提供するということを鑑みると、規律が設けられるべきである。</p>	
<p>【提供されるデータの利用目的の適正性およびデータ最小化のための規律の必要性】 本命令が施行されると、政府から多数の民間サービスに対して券面情報および利用者証明情報が流布される。また、マイナポータルアプリと統合されることを鑑みると、将来的にこれ以外の情報も提供される可能性も考えられる。シンガポールの事例によれば、こうしたデータ取得要求に関して、利用目的の適正性および取得データが最小</p>	

化されているかの審議をクライアントサービスごとに行うといった規律が設けられている。これは、事業者と市民間の情報及び能力の非対称性を鑑みると妥当であると考えられる。日本においても同様の規律が設けられるべきである。

【提供にあたっての同意取得の方法に関する規律の必要性】

政府による情報の取得と政府から民間サービスへの情報提供のいずれについても、利用者の同意に基づいて行われることが適切である。利用者が情報の提供に「同意」する場合に、何が何のために提供されるのか、十分わかりやすい方法で利用者に提示される必要がある。本命令案には、そうした同意取得の方法やユーザーインターフェイスに関する規律を追加すべきである。

以上

【意見1】

今後のデジタル認証アプリの拡張において、一定のセキュリティ/制度要件を満たした民間の認証事業者が発行する電子証明書と連携する機能の搭載について検討いただきたい。デジタル認証アプリは、デジタル田園都市国家構想においても活用されていくことが想定されますが、マイナンバーカードとの連携のみならず、民間の認証事業者が発行するや電子証明書と連携することでデータ連携基盤におけるデータ連携の活性化や基盤の横展開を促進できると思われる。

【意見2】

デジタル認証アプリにおいて、署名検証及び有効性確認機能が搭載されていない理由についてご教示いただきたい。署名検証及び有効性確認は、犯罪収益移転防止法や携帯電話不正利用防止法の本人確認において

デジタル認証アプリは、民間事業者において利用が進まない利用者証明用電子証明書の利活用推進を主目的としているので、民間事業者向けの署名検証・有効性確認サービスは提供しないこととしています。また、デジタル認証アプリは、将来的にはスマホ用電子証明書にも対応していく予定です。対応できた場合は、カードをかざすことなく利用することができます。

極めてニーズの高い機能です。また FinTech サービスや通信サービスを提供するスタートアップ企業等においては、公的個人認証法のプラットフォーム事業者サービスの導入コスト・運用コストの負荷が高いため、プラットフォーム事業者を介さずに利用できる認証アプリに署名検証及び有効性確認機能が搭載されることで、スタートアップ企業等がよりマイナンバーカードを活用しやすくなると思料します。

【意見 3】

本デジタル認証アプリを利用してオンラインサービス等で認証を実施する際、毎回マイナンバーカードをスマートフォンにかざす必要があるのかご教示いただきたい。

【意見 4】

認証アプリの普及には、ID/パスワードによる認証の限界や脆弱性を広く認知することが必要であると考えられるが、そのためにどのような施策を考えているのかご教示いただきたい。

本デジタル認証アプリは、利用者証明用電子証明書を用いた ID/パスワードより格段にセキュリティレベルの高い認証方法を搭載したものであり、ID/パスワードの様な、なりすましや認証情報の漏洩リスクが少ないことが特徴ですが、そのセキュリティについて理解している事業者/利用者が少ないことから、国内 IT サービスの殆は未だに ID/パスワード認証で提供されており、この問題を解決しない限り、認証アプリも促進しないと思われる。

・民間事業者との競合について

これまで、民間サービスに係る署名検証業務は、主務大臣による認定を受けた民間事業者に限って認められていたところ、デジタル庁の長となる内閣総理大臣を電子署名等確認業務受託者に追加し、国が税金により署名検証業務を広くナショナルインフラとして無償で提供することは、当該領域においてすでに投資をし、事業を営んでいる民間事業者の民業を圧迫する。さらに、技術の進歩が速いデジタル ID 分野において、国が民間事業者を排除しつつサービスを提供することは、結果的に業界全体のイノベーションを阻害する懸念がある。

マイナンバーカードの民間利活用を推進するのであれば、本来は当該分野に対して果敢に投資を行うスタートアップ企業等の民間事業者を後押しするような施策を国として実施すべきところ、そのような事業者の事業を圧迫し、市場におけるマイナンバーカード利活用ソリューションにおける自由競争を阻害してまで、国家がこれに介入すべき経済的外部性があるとすれば、それは何かお伺いしたい。

・手数料の無償化ではなく国が直接サービスを無償提供する必要性

すでに、民間でのマイナンバーカードの利活用を促進する政策として、J-LIS の手数料が 2023 年 1 月から当面 3 年間は無償化され、サービスプロバイダ事業者の認定社数も順調に増加し、民間での利活用は拡大している。その政策の成果分析を持って、J-LIS 手数料無償化に加え、デジタル庁が直接利用者証明サービスを無償で提供する必要性を認めたのであれば、その根拠は何かお伺いしたい。

関係事業者の皆様に対しては、今回御指摘いただいた御意見も踏まえ、丁寧に御意見を伺った上で説明を尽くしてまいります。

・市場調査の実施について

マイナンバーカードの民間利活用は、署名用電子証明書による身元確認を中心に進んでおり、当人認証を目的とした利用者証明用電子証明書の活用は現状少ない。ただし、これは単純にランニングコストのみが要因となっているのではなく、既存システムとの連携、UI/UX、ブランディングやマーケティング等様々な要因が絡んでおり、またデバイス認証や生体認証等、マイナンバーカード以外に存在する様々な認証技術のなかから、ユースケースや経済性等によって最適最善な手法が選択されている結果でもある。デジタル庁が利用者証明サービスを提供することによって満たされるニーズが存在するのかについて、市場調査は行われたのか、また行われたのであればその結果は公表されているのかお伺いしたい。

電子署名等確認業務受託者の対象に内閣総理大臣を加えることに反対します。理由は、電子証明書の発行番号のデータを厳格に管理する法律が十分に整備されていない状態で受託者の対象を増やすことは、国民のプライバシーが侵害されるリスクが増すと考えるからです。法律施行規則の一部を改正する命令案の前に、まずは、マイナンバーカードの電子証明書の発行番号（シリアル番号）についても、マイナンバー（個人番号）に準じたものとして厳格に取扱うよう、法整備をお願いします。参考サイト：

<https://www.naka2656-b.site/archives/39935795.html>

デジタル認証アプリにおいては、個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱い対応します。シリアル電子証明書の発行番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。

また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。

なお、デジタル庁を含む署名検証者については、公的個人認証法第52条及び第53条において、シリアル番号を含む、地方公共団体情報システム機構から受領した電子証明書失効情報等について確認以外の目的での利用・提供が禁止されております。

デジタル認証アプリは、個人が官民の各種サービスを利用した履歴が蓄積し、一元管理されてしまいます。

そして個人のプロファイリングや、データによる個人の選別・差別、個人の監視などの人権侵害のリスクがあります。

デジタル庁・国であっても、個人情報を経営者に渡すのは良くないです。

違法で、不当な利用にあたると思います。

このようなマイナンバーカードの法規制は改正する必要があります。

元々、「デジタル社会の実現に向けた重点計画」（令和5年6月9日閣議決定。）

は、個人情報保護についての認識が薄く、人権保障より、個人情報の利活用が優先されています。

これが、根本的に間違っていると思います。

このパブコメでの提起に、反対します。

デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。

以下の理由により、改正案による改正は反対である。

1. デジタル庁（内閣総理大臣）に、以下の情報が蓄積される可能性があるが、その情報の取り扱いについて定めていない、

また、今回の意見募集において提示されておらず、今回の省令案において告示等の下位の規程への委任もされていない。

- ・国民の個人がマイナンバーカードを利用した日時

- ・国民の個人がマイナンバーカードを利用した官民のサービス名

- ・国民の個人がマイナンバーカードを利用した官民のサービスの内容・目的（ログイン・署名）

2. デジタル庁が当該サービスを運営するにあたり行うべきセキュリティ等の内容等が定められていない、

また、今回の意見募集において提示されておらず、今回の省令案において告示等の下位の規程への委任もされていない。

地方公共団体情報システム機構については、法律レベルで、規定しているのに、

デジタル庁の当該サービスについて、そのような規定が存在しない

（同様の民間サービスであれば、「団体署名検証者」として、規定がある。）

3. 民間では、同様のサービスを行っている業者が存在し、

デジタル庁の当該サービスは、今後、民業圧迫となる可能性がある。

4. デジタル庁の当該サービスを利用する民間サービスに対して、「結果を連携」しているが、

この連携を受け取った民間サービスが、その認証の結果をどのように扱うのか扱いについて、今回の省令上は規制されない。

5. 4に記載の民間サービスが受取った「認証の結果」について、民間サービスが

デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。

また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。

なお、デジタル認証アプリは、民間事業者において利用が進まない利用者証明用電子証明書の利活用推進を主目的としているので、民間事業者向けの署名検証・有効性確認サービスは提供しないこととしています。

個人情報法上は、本人から取得した同意に基づき、扱う必要があると理解しているが、

その同意をどこにおいて取得するか具体的に記載がなく、

国民に不安を与える若しくは、自身の情報の扱いへの無関心さを助長する結果となる疑念がある。

6. 署名作成機能を利用する民間サービスよりの依頼に基づき、

個人番号カードを読み込み作成された署名に対して、

民間サービスが、署名検証者でない場合、その署名の取り扱いに関して規制がないのではないかと

現在は、署名検証者のみが、地方公共団体情報システム機構より、

個人番号カードの読み出しの詳細情報にアクセスすることを規制をしていると理解しています。

公的個人認証を認証基盤にすることは賛成ですが、方法には賛成できません。

マイナンバーカードの「デジタル認証アプリ」について。

「デジタル認証アプリ」は、行政や民間企業のサービスのログインなどで使われるとのことですが、個人の各種サービスの利用状況がデジタル庁のサーバーに蓄積され、個人についての広範囲な情報を国が一元管理することとなります。

こうした情報を一元的に把握することに対しては、利用者個人への不当なプロファイリングなどのプライバシーリスクがあるように思います。

また、電子証明書のシリアル番号は、新旧シリアル番号の紐付けサービスをJ-LISが行っており、実質的には失効することなく、追跡が可能となっていることも同様です。

デジタル認証アプリにおいては、個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱い対応します。シリアル電子証明書の発行番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるとため行うことができません。

また、デジタル庁がデジタル認証アプリを提供する際には、改正案の第29条第2項に基づき、セキュリティに関してプラットフォーム事業者と同等の基準を遵守する必要があります。

なお、デジタル庁を含む署名検証者については、公的個人認証法第52条及び第53条において、シリアル番号を含む、地方公共団体情報システム機構から受領した電子証明書失効情報等について確認以外の目的での利用・提供が禁止されております。

マイナンバーについては、マイナンバー法が利用目的・管理・罰則などを明確にしていますが、シリアル番号については、利用目的の制限がなく、発行番号は特定個人情報にも該当しない、厳格な安全管理措置もない、というのは、国民の個人情報保護やプライバシー保護を軽視し、あまりにも利便性のみを追求しているように思えます。官民のサービス履歴が一元化され、関連性のないデータであっても、利用者個人の不当なプロファイリングや人格権侵害のリスクが生じるように思います。

「デジタル認証アプリ」が、本人確認の認証を確保するものである、というのであれば、マイナンバー法そのものを改正し、根拠条文を設置し、利用目的や目的外利用の禁止、安全管理措置等を規定し、違法・不当な利用に対し厳格な対応をすることが本来望まれていることなのではないでしょうか。

また、電子証明書のシリアル番号についても、マイナンバーに準じたものとして法規制されるべきと思います。

「法律による行政の原則」により運用されますようお願い申し上げます。

プラットフォーム事業者は、公的個人認証がどのサービスで使われたのかを国家権力に準ずる J-LIS がトラッキングできないようにする役割があると認識しております。今回の改正案は、公的個人認証がどのサービスで使われたのかを国家権力であるデジタル庁がトラッキング可能にしてしまいます。これはプラットフォーム事業者が設けられた趣旨に沿わないものであり、プライバシー保護の観点で問題のある内容

デジタル認証アプリにおいて個人情報を取り扱う場合、個人情報保護法に基づき適切に取り扱います。シリアル番号をもとに、氏名等の4情報を照会することは、目的外利用に当たるため行うことができません。

マイナポータルについては カードを作ったが 目的や内容を知らずにポイント目当てで登録してしまった国民が多い。政府が国民にきちんとした説明もなしに 保険証を無くしますという周知の仕方で 当然ながら大混乱が起きてしまった。既に企業が 利用している電子署名があるわけで、今回も良く分からず登録してしまった国民に またもや説明もなくデジタル庁に繋がるポータルを推進することをすれば、国民を一方的に一元管理する人権的に最悪の政策となります。

電子証明書のシリアル番号で個人を追跡することが可能になり、マイナンバーカードが、分散管理で安全と言っていたのに、デジタル庁が一元管理する形になっているのは、「だまし討ち」のようです。一元化されて蓄積された個人情報により、不当なプロファイリングや個人の「選別」、国による監視が行われ、プライバシーが著しく侵害されます。特に 自衛隊の近辺の住民は、大きな不安を持ちます。

今回いただいた御意見も踏まえ、国民の皆様に対しても、安心して利用いただけるよう、デジタル認証アプリのメリットや安全性について、分かりやすい説明に努めてまいります。