**様式第十三**（第４条関係）

新事業活動に関する確認の求めに対する回答の内容の公表

１．確認の求めを行った年月日
令和４年７月１３日

２．回答を行った年月日
令和４年７月２９日

３．新事業活動に係る事業の概要
照会者は、国若しくは地方公共団体と民間事業者(以下、まとめて「**契約当事者**」という。)との間で又は三者間で電子ファイルによって行うことを可能とするサービス（以下「**本サービス**」という。）を提供することにより、国の契約書、請書その他これに準ずる書面、検査調書等への押印を代替する用途として提供する新規事業を検討している。
本サービスは、本サービス上にアップロードされた契約書の電子ファイルに政府認証基盤（ＧＰＫＩ）又は地方公共団体における組織認証基盤(ＬＧＰＫＩ）から発行される電子証明書及び秘密鍵情報が含まれたＩＣカード（以下「**認証基盤発行のＩＣカード**」という。）、電子入札コアシステム対応認証局又は商業登記認証局より公開鍵の所有者を証明する電子入札用電子証明書及び秘密鍵情報が含まれたＩＣカード（以下「**認証局発行のＩＣカード**」という。）又はＷａｌｌｅｔ（本サービスによって生成される秘密鍵情報及びその対となる公開鍵情報を含むＷａｌｌｅｔと呼ばれるデータ）に格納されている自らの秘密鍵を用いて当該ハッシュ値、自らのＷａｌｌｅｔアドレス及び取引行為（コントラクト）に電子署名を行うサービスである。
なお、契約当事者の間で本サービスを利用して電子契約を締結する場合は、以下手順により契約締結を行う。
① 契約当事者はそれぞれ本サービス上で以下のログイン等を行う。
(ア)国又は地方公共団体は、本サービスにログインを行い、認証基盤発行のＩＣカード又はＷａｌｌｅｔに格納された秘密鍵を用い、Ｗａｌｌｅｔアドレスと本サービスのブロックチェーンのユーザ情報との紐づけを行い、当該情報をブロックチェーン上に記録する。
(イ)一方で、民間事業者は、電子申請（入札参加資格登録申請）時に国又は地方公共団体から付与された電子入札システムと連携された業者番号（ＩＤ）とパスワードを用いて、本サービスにログインを行い、(ⅰ)認証局発行のＩＣカードを保有している場合、保有する認証局発行のＩＣカード内の秘密鍵を用いて、Ｗａｌｌｅｔアドレスと本サービスのブロックチェーンのユーザ情報（自治体への業者登録を行っている登録番号及び本サービスのブロックチェーンに登録しているユーザ情報。以下同じ。）との紐づけを行い、当該情報をブロックチェーン上に記録する。(ⅱ)認証局発行のＩＣカードを保有していない場合、民間事業者は、上記と同様の方法によりログイン後、本サービスによって生成されたＷａｌｌｅｔ内の秘密鍵を用いて、Ｗａｌｌｅｔアドレスと本サービスのブロックチェーンのユーザ情報との紐づけを行い、当該情報をブロックチェーン上に記録する。
② 契約当事者は、契約書の電子ファイルを、（ⅰ）本サービス上にアップロードする、又は（ⅱ）メールの添付ファイルとして送るといった方法により、受け渡しを行う。
③ 契約当事者は、それぞれ、契約書の電子ファイルの最終版（契約内容について合意をし、署名を行う前の段階のもの）を本サービス上にアップロードし、ハッシュ関数を用いてハッシュ値化（現時点では、ＳＨＡ－２５６の計算方法で、任意の長さ

の元データを２５６ｂｉｔに要約した値）する。

④　契約当事者は、認証基盤発行のＩＣカード、認証局発行のＩＣカード又はＷａｌｌｅｔに格納されている自らの秘密鍵を用いて、サービス事業者等の第三者の介在なしに当該ハッシュ値、自らのＷａｌｌｅｔアドレス及び取引行為（コントラクト）に電子署名を行う。

なお、電子署名を行う手順は、次のとおりである。

(ア)電子署名を行う契約当事者は、本サービス上に契約書の電子ファイルをアップロード後、秘密鍵の有効化を行う。（ｉ）認証基盤発行のＩＣカード又は認証局発行のＩＣカードを利用する場合には、当該ＩＣカードリーダによる読み取り後、ＰＩＮコードを入力することにより秘密鍵の有効化を行う。（ⅱ）Ｗａｌｌｅｔを利用する場合には、パソコン上に保管された電子ファイルを読み込み後、ＰＩＮコードを入力し、秘密鍵の有効化を行う。

(イ)契約当事者は契約書に合意したとのボタンを押す。これにより、契約書の電子ファイルのハッシュ値、Ｗａｌｌｅｔアドレス及び取引行為（コントラクト）の内容に対する電子署名が行われ、この電子署名データ（電子署名を行った秘密鍵に対応する公開鍵情報を含む。）は、ブロックチェーン上に記録され、１つ前のブロックのハッシュ値及びナンス値と共に格納される。本ブロックチェーン上に、契約当事者の電子署名が記録されることにより、本サービスによる電子署名のプロセスが完了する。

⑤　電子署名は、契約当事者双方が行うため、ブロックチェーン上には民間事業者の電子署名及び国又は地方公共団体の電子署名と各契約当事者による合意があったことが記録される。

４．確認の求めの内容

（１）照会者が提供する本サービスによる署名が、電子署名及び認証業務に関する法律（平成１２年法律第１０２号。以下「電子署名法」という。）第２条第１項に規定する電子署名の要件を充足し、地方自治法施行規則（昭和２２年内務省令第２９号）第１２条の４の２及び総務省関係法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則（平成１５年総務省令第４８号）第２条第２項第１号に基づき、地方公共団体の契約書が電磁的記録で作成されている場合の記名押印に代わるものとして利用が可能であること及び契約事務取扱規則（昭和３７年大蔵省令第５２号）第２８条第３項に基づき、国の契約書が電磁的記録で作成されている場合の記名押印に代わるものとして利用可能であることを確認したい（以下「**本照会①**」という。）。

（２）照会者が提供する本サービスの仕組みが契約事務取扱規則第２８条第２項に規定する方法による「電磁的記録の作成」に該当し、契約書の作成に代わる電磁的記録の作成として、利用可能であることを確認したい（以下「**本照会②**」という。）。

５．確認の求めに対する回答の内容

（１）本照会①についての回答

ア　結論

本サービスを用いた電子署名は、電子署名法第２条第１項に規定する電子署名に該当すると認められる。したがって、これを引用する地方自治法施行規則第１２条の４の２に規定する総務省関係法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則第２条第２項第１号に基づき地方公共団体の契約書が電磁的記録で作成されている場合の記名押印に代わるものとして、利用が可能であり、また、契約事務取扱規則第２８条第３項に基づき、国の契約書が電磁的記録で作成されている場合の記名押印に代わるものとして、利用が可能であると考える。

イ　理由

電子署名法における「電子署名」とは、電子署名法第２条第１項に規定されているとおり、(ア）デジタル情報（電磁的記録に記録することができる情報）について行われる措置であって、(イ）当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること（同項第１号）及び（ウ）当該情報について改変が行われていないかどうかを確認することができるものであること（同項第２号）のいずれにも該当するものである。

（ア）電磁的記録に記録することができる情報について行われる措置の該当性

本サービスについては、「契約書（原文となる電子ファイル）から求めた契約書のハッシュ値（ＳＨＡ２５６）と、公開鍵を示す情報（Ｗａｌｌｅｔアドレス)、および取引行為（コントラクト）とを一つにまとめた情報（トランザクション要求）に、ＩＣカードもしくはＷａｌｌｅｔの秘密鍵を用いて公開鍵暗号方式による①暗号化措置をするもの」である（照会書８ページ）とのことであり、この記載を前提とすれば、「電磁的記録に記録することができる情報について行われる措置」の要件を満たすことになるものと考える。

（イ）当該情報が当該措置を行った者の作成に係るものであることを示すためのものであることの該当性

本サービスは、契約当事者が、契約当事者において内容が確定した契約書の電子ファイルを本サービス上にアップロードし、その後、（ｉ）「認証基盤発行のＩＣカード、認証局発行のＩＣカードを利用する場合には、当該ＩＣカードリーダによる読み取り後、ＰＩＮコードを入力することにより秘密鍵の有効化」（以下「**ＩＣカードによる措置**」という。）又は（ⅱ）「Ｗａｌｌｅｔを利用する場合には、パソコン上に保管されたファイルを読込後、ＰＩＮコードを入力し、秘密鍵の有効化」（以下「**Ｗａｌｌｅｔによる措置**」という。）を行った上で、契約書に合意したとのボタンを押すことにより、「契約書の電子ファイルのハッシュ値、Ｗａｌｌｅｔアドレス及び取引行為の内容に対する電子署名が行われ」ることが予定されている（照会書４ページ）。

まず（ｉ）ＩＣカードによる措置については、契約書の作成者である契約当事者がそれぞれ物理的に管理する秘密鍵によって行う措置であることから、「当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること」に該当すると考える。

次に（ⅱ）Ｗａｌｌｅｔによる措置については、「本サービスを利用して契約当事者の操作で生成される秘密鍵情報及びその対となる公開鍵情報を含むＷａｌｌｅｔ」内の「自らの秘密鍵を用いて、サービス事業者など第三者の介在なしに当該ハッシュ値、自らのＷａｌｌｅｔアドレス、及び取引行為（コントラクト）に電子署名を行う」（照会書３ページ及び４ページ）とのことであり、いわゆる「リモート署名」の類に該当すると考える。すなわち、本サービスは、契約当事者の指示に基づき、契約当事者の署名鍵により暗号化等を行うサービスとのことであるため、電子署名法第２条第１項第１号の「当該措置を行った者」が契約当事者であると評価し得るかどうかが問題となる。

この点、令和２年７月１７日に総務省、法務省及び経済産業省において公表している「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するＱ＆Ａ」（以下「Ｑ＆Ａ」という。）では、下記の解釈が示されているところである。

・　電子署名法第２条第１項第１号の「当該措置を行った者」に該当するためには、必ずしも物理的に当該措置を自ら行うことが必要となるわけではなく、例えば、物理的にはＡが当該措置を行った場合であっても、Ｂの意思のみに基づき、Ａの意思が介在すること

なく当該措置が行われたものと認められる場合であれば、「当該措置を行った者」はＢであると評価することができるものと考えられる。

- このため、利用者が作成した電子文書について、サービス提供事業者自身の署名鍵により暗号化を行うこと等によって当該文書の成立の真正性及びその後の非改変性を担保しようとするサービスであっても、技術的・機能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されていると認められる場合であれば、「当該措置を行った者」はサービス提供事業者ではなく、その利用者であると評価し得るものと考えられる。
- そして、上記サービスにおいて、例えば、サービス提供事業者に対して電子文書の送信を行った利用者やその日時等の情報を付随情報として確認することができるものになっているなど、当該電子文書に付された当該情報を含めての全体を１つの措置と捉え直すことによって、電子文書について行われた当該措置が利用者の意思に基づいていることが明らかになる場合には、これらを全体として１つの措置と捉え直すことにより、「当該措置を行った者（＝当該利用者）の作成に係るものであることを示すためのものであること」という要件（電子署名法第２条第１項第１号）を満たすことになるものと考えられる。

照会書の記載によれば、本サービスは、いわゆるリモート署名型によるものであり、本サービスでは、照会者（サービス提供事業者）自身の署名鍵ではなく、契約当事者（利用者）の署名鍵を用いるため、上記Ｑ＆Ａの直接の適用はないものの、上記Ｑ＆Ａの考え方は、「当該措置を行った者」（電子署名法第２条第１項第１号）の該当性を判断する上で参考になるものと考える。

以上を踏まえて本件について検討すると、Ｗａｌｌｅｔによる措置を行うに当たっては、本サービスの利用のために契約当事者はそれぞれ所定のログイン手続を行う必要があることに加えて、将来的には「甲乙の本人確認を外部で認証されたｇＢｉｚＩＤやマイナンバーカード、各種の二要素認証やｅＫＹＣを組み合わせて、Ｗａｌｌｅｔを取得できる仕組みの提供も予定」しているように（照会書３ページ）、本サービスでは、上記の所定のログインの手続を通じて契約当事者の本人確認がなされたことを前提に、契約当事者が合意したとのボタンを押すことにより、契約当事者の署名鍵により「契約書の電子ファイルのハッシュ値、Ｗａｌｌｅｔアドレス及び取引行為の内容に対する電子署名が行われ」ること（照会書４ページ）、また、契約当事者の名義を取引行為（トランザクション）情報として確認することが可能であること（照会書５ページ）等を踏まえると、サービス提供事業者の意思が介在することなく、契約当事者本人の意思に基づき署名することができる仕組みと認められる。そのため、本サービスは、「技術的・機能的に見て、サービス提供事業者の意思が介在する余地がなく、利用者の意思のみに基づいて機械的に暗号化されたものであることが担保されている」ことが認められ、これを前提にすれば「当該措置を行った者」は照会者（サービス提供事業者）ではなく、契約当事者（利用者）であると評価し得るものと考えられる。よって、「当該措置を行った者」は契約当事者であると評価することができ、電子署名法第２条第１項第１号の「当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること」の要件を満たすことになるものと考えられる。

（ウ）当該情報について改変が行われていないかどうかを確認することができるものであることの該当性

照会書によれば「契約書（原文となる電子ファイル）から求めたハッシュ値（ＳＨＡ２５６）と、公開鍵を示す情報（Ｗａｌｌｅｔアドレス)、および取引行為（コントラクト）とを一つにまとめた情報（トランザクション要求）に、公開鍵暗号方式による暗号化措置（ＰＫＣＳ＃１　ＲＳＡ２０４８ｂｉｔ）による暗号文、すなわち、トランザクション要求のハッシュ値を秘密鍵で処理した暗号文が記録されています。契約当事甲乙）

は、この暗号文を公開鍵で復号化したハッシュ情報と、トランザクション要求を再度ハッシュ関数でハッシュ値にしたものと合致するかどうかを照合することにより、改ざんがなされていないことを確認することができます」（照会書５ページ）とのことであるから、この記載を前提とすれば、「当該情報について改変が行われていないかどうかを確認することができるものであること」の要件を満たすことになるものと考えられる。

以上から、照会者の提供する本サービスを用いた電子署名は、電子署名法第２条第１項における「電子署名」に該当すると考えられる。したがって、本サービスは、地方自治法施行規則第１２条の４の２及び総務省関係法令に係る情報通信技術を活用した行政の推進等に関する法律施行規則第２条第２項第１号に基づき、地方公共団体の契約書が電磁的記録で作成されている場合の記名押印に代わるものとして、利用が可能であり、また、契約事務取扱規則第２８条第３項に基づき、国の契約書が電磁的記録で作成されている場合の記名押印に代わるものとして、利用が可能であると考える。

（２）本照会②についての回答

ア　結論

照会者が提供する本サービスにおいて、利用者が契約書の電子ファイルを本サービス上にアップロードし、当該電子ファイルを確認・同意を行うことが可能である等の仕組みは、契約事務取扱規則第２８条第２項に規定する方法による「電磁的記録の作成」に該当し、契約書等の作成に代わる電磁的記録の作成として、利用可能であると考える。

イ　理由

契約事務取扱規則第２８条第２項は、同条第１項各号に掲げる書類等の作成に代わる電磁的記録の作成について、「各省各庁の使用に係る電子計算機（入出力装置を含む。以下同じ。）と契約の相手方の使用に係る電子計算機とを電気通信回線で接続した電子情報処理組織を使用して当該書類等に記載すべき事項を記録する方法」によることを規定している。

本サービスは、「契約当事者がそれぞれの電子計算機からインターネット等の電気通信回線で接続して利用するサービスです。契約当事者は、当該電気通信回線で接続した本サービス上において、契約に必要な各種書類を確認し、同意を行う」（照会書１０ページ）とのことであり、同項各号に掲げる書類等に記載すべき事項を記録する方法により電磁的記録を作成するものであれば、これに該当するものと認められる。

（注）

本回答は、確認を求める対象となる法令（条項）を所管する立場から、照会者から提示された照会書の記載内容のみを前提として、現時点における見解を示したものであり、もとより、捜査機関の判断や罰則の適用を含めた司法判断を拘束するものではない。