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７年１１月１３日

２．回答を行った年月日
令和７年１２月５日

３．新事業活動に係る事業の概要
照会者は、ブロックチェーン電子契約（以下「本サービス」という。）を国や地方公共団体等の契約書の署名に用いることを想定し、提供を予定している。具体的には、以下手順により契約締結を行う。

【契約締結までの流れ】
本サービスは、利用者の指示に基づき照会者が提供する署名鍵（秘密鍵）により暗号化を行う事業者署名型の電子契約サービスである。署名依頼者は本サービスアカウントが必要であり、契約相手は本サービスアカウントがなくても電子署名を行い、契約を締結することができる。
具体的な手順に関しては以下のとおりである。

① 担当者間（送信元担当者・送信先担当者）で契約内容を協議し合意する。まず対面、オンライン、メールやり取りなどで相互に、本人に加え関係者や代表者のメールアドレス、氏名や所属、役職、さらにはメール以外の本人への連絡手段（スマートフォンの番号やメールアドレス等）の確認を行う。その後契約内容に沿った契約書を双方が共同で作成する。
② 送信元担当者が本サービスの Web アプリケーションに、予め登録したログイン ID とパスワードを用いてログインする。
③ 契約書（PDF ファイル）と組織間の承認フロー（送信元・送信先の関係者や代表者、承認順序などの情報）をシステムへ登録する。システムは契約書ファイルのハッシュ値を求め、この契約に対応するブロックチェーンの先頭ブロックに求めたハッシュ値を登録する。なお、本サービスによる契約１件目では、先頭ブロックはジェネシスブロックとなり、２件目の契約では１件目契約の最終ブロックの次に２件目契約の先頭ブロックが追加される。３件目以降もこれを繰り返す。
④ 送信元担当者は承認フローを開始する。送信元関係者、送信元代表者は、それぞれ自身の PC 等の電子計算機を使用して、システムから受け取った承認依頼のメールに記載された URL にアクセスする。URL が示す本サービスに自身の ID・パスワードを使ってログインし、あらかじめアクセス権が付与されている契約書ファイルの内容と、それまでの承認履歴を確認する。URL はワンタイムでありランダムに生成された文字列を含むもので、第三者が推察することはほぼ不可能であり、メールを受け取った人以外はアクセスできない。また、本サービスにログインする ID・パスワードは、送信元関係者や代表者が URL にアクセスした際に、メールによる URL 送付とは別の手段（スマートフォンのメッセージやメールなど）でシステムが本人宛てに送付する（二段階認証に相当）。内容に異議なければ Web アプリケーション画面上の承認ボタンをクリックすることで承認処理を行う。それを指示としてシステムは承認者の情報（所属、役職、氏名、メールアドレス）と承認履歴（承認ボタンをクリックした記録）のハッシュ値をブロックチェーンに登録する。同時にそのブロック生成に対するタイムスタンプがシステムに登録される。送信元代表者が承認処理をした場合には、その指示に基づきシステムにより文書に電子署名が付与される。電子署名の形式は、ECDSA（楕円曲線デジタル署名アルゴリズム、P-256）による公開鍵方式の電子署名で

ある。また、視覚的にわかりやすくするため印鑑画像が文書に貼り付けられる。送信元代表者の承認により、直前のブロック全体のハッシュ値、送信元代表者のユーザー情報および承認履歴、電子署名のハッシュ値に加えて新たな印鑑画像が貼り付けられた文書のハッシュ値がブロックチェーンに登録される。なお、承認フローが開始された後、ユーザーが出来る作業は「承認」「閲覧」となる。契約内容を承認できない、あるいは誤記などがあった場合、契約書を差し替えて承認フローを修正する。この際には①の手順から再度実行する必要がある。

⑤ システムが送信先関係者及び送信先代表者に承認依頼をメールにて通知する。

⑥ メールを受領した送信先関係者及び送信先代表者は、メールに記載されている URL から本サービスの Web アプリケーションへログインする。本サービスのログインに必要な ID・パスワードは、送信先関係者や代表者が URL にアクセスした際に、メールによる URL 送付とは別の手段（スマートフォンのメッセージやメールなど）でシステムが本人あてに送付する。ログインした送信先関係者及び送信先代表者は契約書を順次閲覧し承認操作を行う。
この承認操作により④の手順と同じく、システムが承認したユーザーの情報と承認履歴（ハッシュ値）をブロックチェーンに登録し、送信先代表者が承認処理をした場合には文書に電子署名が付与され、直前のブロック全体のハッシュ値、送信元代表者の情報および承認履歴のハッシュ値に加えて新たな印鑑画像が付与された文書のハッシュ値とともにブロックに登録される。なお、④と⑥の手順でシステムに登録されるタイムスタンプは、ブロックチェーン（Hyperledger Fabric）システムが登録する情報となるため、管理者も含めてユーザーの手による改変は確認することが可能である。以上の処理は送信先、および送信元の関係者、代表者の意思でシステムが実施するもので、サービス提供事業者の意思が介在する余地はない。
ここまでの操作でブロックチェーンに記録された契約書の情報（ハッシュ値）と全ユーザーの承認履歴（ハッシュ値、タイムスタンプ）の記録を、本サービスにおける電子署名の内容と各ユーザーによる承認の証跡として利用する。送信元、および送信先の関係者、代表者の氏名や、誰がいつ承認処理を行ったかの情報は、Web アプリケーションの画面上で確認できる。さらに、最終結果として契約元と契約先の代表者の印鑑画像が貼り付けられた契約文書も画面上で確認できる。対象となる契約書と、誰がいつ承認したかという全ユーザーの承認履歴はブロックチェーンに記録されており、そこに第三者、あるいはシステム管理者などによる不正なアクセスがあり改変されると、ブロックの情報が変更されチェーンの連続性（事前のブロックのハッシュ値を受け継いでいる）が損なわれ、Hyperledger Fabric の機能としてシステムが正常動作しなくなる。すなわち、改変された後にはユーザーはシステムにアクセスはできても承認処理が行えない（承認のボタンを押しても反応しない）、契約完了後に契約文書を閲覧できない、という事象が発生する。Web アプリケーションによる承認処理や文書確認が問題なく行われるということにより、各ユーザーによる承認の真正性が確認でき、改変されていないことが検証できる。
また、システム管理者によるブロックチェーン全体の差替え等の行為は、以下の仕組みで防ぐことが出来る。本サービスを実現するクラウドには、たとえシステム管理者でも改変できない操作ログ（誰がいつ何をしたか）を記録する仕組み（台帳型のデータベース）が実装されている。操作ログは複数の人間に随時システムから報告されるので、ブロックチェーン全体の差替えなどの行為は必ず発覚することが社内に周知されている。

■契約締結後の流れ（署名データの検証手順）

⑦ 組織間で締結された契約書は全て Web アプリケーションに登録されており、契約締結を契機に登録された全ての関係者に対してメールで契約の締結を通知する。通知を受けたユーザーには ID 及び認証情報が発行される。ID 及び認証情報が発行されたユーザーは本サービスへアクセスし、発行された ID 及び認証情報を利用して本人確認を行う。本人確認が取れたユーザーに対しては、システムはアクセス権限の範囲内で契約書へのアクセスを許可し、契約書情報を表示する。契約書を閲覧しているユーザーは契約書のダウンロード操

作を行う事が出来る。なおこのアクセス権限は恒久的なものではなく、一時認証が可能なID 及び認証情報を発行することで一時的なアクセスを可能にする。また、ID 及び認証情報は契約の関係者以外の第三者（あらかじめ登録された者）にも発行することができ、これを用いることで一時的なアクセスと閲覧が可能になる。

４．確認の求めの内容

（１）従来の紙面と印鑑を用いて作成していた契約業務をデータの改ざんが困難なブロックチェーン技術を用いた本サービスのWebアプリケーションで行うという仕組みが、契約事務取扱規則（昭和３７年大蔵省令第５２号）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、契約書類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①」という。）。

（２）本サービスのWebアプリケーション上で、契約文書の登録・承認（署名）する事が出来る仕組みが、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項に定める電子署名に該当し、これを引用する契約事務取扱規則第２８条第３項に基づき、国の契約書について利用可能であること。また、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（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についても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

従来の紙面と印鑑を用いて作成していた契約業務をデータの改ざんが困難なブロックチェーン技術を用いた本サービスのWebアプリケーションで行うという仕組みは、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、契約書類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。

この点について本サービスは、送信元担当者がPC等の電子計算機から「契約書類の電子ファイルを電気通信回線で接続されたシステムに登録し、送信元担当者および送信先担当者を通じて双方の組織の関係者、代表者が電気通信回線を介して本サービスにアクセスして契約締結を行う仕組み」（照会書９ページ参照）であることから、同条第２項の方法に該当するものと認められる。

（２）本照会②についての回答

ア　結論

本サービスによる電子署名は、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、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。また、地方自治法施行規則第１２条の４の２に定め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についても利用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、同法第２条第１項に規定されているとおり、（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であって（同項柱書）、（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

本サービスは、「契約書等の電子ファイル（ハッシュ値）とそれを承認した送信元、および、送信先の代表者のユーザー情報や承認履歴（ハッシュ値）および、タイムスタンプの情報が、本システム（サービス事業者（注：照会者））の署名鍵により暗号化（電子署名）されブロックチェーンやシステム（電磁的記録）へ記録する」（照会書１０ページ参照）仕組みであることを前提とすれば、「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であること」との要件を満たすことになると考える。

（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

本サービスでは、契約内容が記録された契約書ファイル（PDF形式）をシステムへ登録した際に、当該契約書ファイルのハッシュ値を算出し、ブロックチェーンの先頭ブロックに保存する。その後、契約当事者双方がそれぞれ画面上で同意し、契約締結業務を実施する仕組みとなっている。この場合、契約当事者双方の当該操作の後に、サービス提供者である照会者により契約当事者の情報と承認履歴のハッシュ値が次々とブロックに登録されるサービスであるため、電子署名法第２条第１項第１号の「当該措置を行った者」が利用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た「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、以下の解釈が示されている。

- 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。

本サービスは、「利用者の指示に基づき本サービス提供事業者の署名鍵を利用して署名を行う」（照会書３ページ参照）事業者署名型の電子契約サービスであり、具体的に

は、まず「送信元担当者が本サービスのWebアプリケーションに、予め登録したログインIDとパスワードを用いてログイン」し、「契約書（PDFファイル）と組織間の承認フロー（送信元・送信先の関係者や代表者、承認順序などの情報）をシステムへ登録」。その際に「システムは契約書ファイルのハッシュ値を求め、この契約に対応するブロックチェーンの先頭ブロックに求めたハッシュ値を登録する」（照会書４ページ参照）とのことである。

送信元担当者が承認フローを開始すると、「送信元関係者、送信元代表者は、それぞれ自身のPC等の電子計算機を使用して、システムから受け取った承認依頼のメールに記載されたURLにアクセスする。URLが示す本サービスに自身のID・パスワードを使ってログインし、あらかじめアクセス権が付与されている契約書ファイルの内容と、それまでの承認履歴を確認」し、「内容に異議なければWebアプリケーション画面上の承認ボタンをクリックすることで承認処理を行」い、「それを指示としてシステムは承認者の情報（所属、役職、氏名、メールアドレス）と承認履歴（承認ボタンをクリックした記録）のハッシュ値をブロックチェーンに登録」するとのことである。なお、送信元代表者が「承認ボタン」をクリックすると、「その指示に基づきシステムにより文書に電子署名が付与される」とともに、「直前のブロック全体のハッシュ値、送信元代表者のユーザー情報および承認履歴、電子署名のハッシュ値に加えて新たな印鑑画像が貼り付けられた文書のハッシュ値がブロックチェーンに登録され」、「システムが送信先関係者及び送信元関係者に承認依頼をメールにて通知する」（照会書４～５ページ参照）とのことである。

その後、「メールを受領した送信先関係者及び送信先代表者は、メールに記載されているURLから本サービスのWebアプリケーションへログイン」し、「契約書を順次閲覧し承認操作を行う」とのことである。送信先代表者が「承認ボタン」をクリックすると、「文書に電子署名が付与され、直前のブロック全体のハッシュ値、送信元代表者の情報および承認履歴のハッシュ値に加えて新たな印鑑画像が付与された文書のハッシュ値とともにブロックに登録される」（照会書５ページ参照）とのことである。

なお、「対象となる契約書と、誰がいつ承認したかという全ユーザーの承認履歴はブロックチェーンに記録されており、そこに第三者、あるいはシステム管理者などによる不正なアクセスがあり改変されると、ブロックの情報が変更されチェーンの連続性（事前のブロックのハッシュ値を受け継いでいる）が損なわれ、Hyperledger Fabricの機能としてシステムが正常動作しなくなる。すなわち、改変された後にはユーザーはシステムにアクセスはできても承認処理が行えない（承認のボタンを押しても反応しない）、契約完了後に契約文書を閲覧できない、という事象が発生する」（照会書５ページ参照）とのことである。

さらに、「送信元、および送信先の関係者、代表者の氏名や、誰がいつ承認処理を行ったかの情報は、Webアプリケーションの画面上で確認できる」（照会書５ページ参照）とのことである。

以上より、本サービスが適用する電子署名は、利用者の指示に基づき、照会者や第三者の意思が介入する余地なく機械的に、サービス提供事業者である照会者の署名鍵により暗号化処理が実行される仕組みであり、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」ことが認められる。

以上のことを前提とすれば、「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」との要件を満たすことになると考える。

（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、本サービスの電子署名にはECDSA（楕円曲線デジタル署名アルゴリズム、P-256）が使用され、取引履歴としてブロックチェーンに記録されており、「そ

こに不正アクセスによりブロックチェーンの登録情報が改変されると、チェーンの連続性（事前のブロックのハッシュ値を受け継いでいる）が損なわれ、Hyperledger Fabricの機能としてシステムが正常動作しなく」なることから、「Webアプリケーションによる承認処理や文書確認が問題なく行われるということにより、改変が行われていないことにより、各ユーザーによる承認の真正性が確認でき、改変されていないことが検証できる」（照会書５ページ参照）とのことから、「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。そのため、同項を引用する契約事務取扱規則第２８条第３項に基づき国の契約書についても利用可能であると考えられる。

また、地方自治法施行規則第１２条の４の２に定め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についても利用可能であると考える。

（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。また、電子署名サービスの安全性を担保するものではない。