

様式第九（第4条関係）

新事業活動に関する規制について規定する法律及び法律に基づく命令の規定に係る照会書

令和4年7月13日

内閣総理大臣 岸田 文雄 殿
財務大臣 鈴木 俊一 殿
総務大臣 金子 恭之 殿
法務大臣 古川 禎久 殿
経済産業大臣 萩生田 光一 殿

川崎市幸区堀川町72番地34
東芝デジタルソリューションズ株式会社
取締役社長 岡田 俊輔

産業競争力強化法第7条第1項の規定に基づき、実施しようとする新事業活動及びこれに関連する事業活動に関する規制について規定する法律及び法律に基づく命令の規定の解釈並びに当該新事業活動及びこれに関連する事業活動に対する当該規定の適用の有無について、確認を求めます。

記

1. 新事業活動及びこれに関連する事業活動の目標

弊社では、これまで培ってきたシステムインテグレーション力をベースに、CPSテクノロジーを活用した新たなサービスや価値の創造に取り組んでいます。国や地方公共団体、民間企業向けにおいて、「やさしく、あたたかなデジタルで社会を豊かにする」とのビジョンのもとに各種ソリューションの提供を行っています。

また、弊社では複数サーバで高信頼なシステムを実現するクラスタ技術を永らく保有しており、そこで培われた技術を基に、高速で可用性・信頼性に優れたブロックチェーンエンジンの開発を行っています。

これらの活動のなかで、弊社が構築するデータを安全かつローコストに管理可能なブロックチェーンを活用し、PDFに限らない電子契約サービスを提供することで、国や地方公共団体における調達事務手続き全般（業者登録、入札、契約、遂行、納品に至る全般の業務）の事務効率化、契約受託者の事務効率化、及び民間企業間における契約事務効率化に貢献することを目指しています。

2. 新事業活動及びこれに関連する事業活動により生産性の向上又は新たな需要の獲得が見込まれる理由

「新たな役務の開発又は提供」に該当します。

国や地方公共団体、民間企業において、電子契約（当事者型、立会人型）が進められていますが、PDFに電子署名する形式になっていることから、契約事務手続で発生する各種書面（各種電子ファイル）を対象にすることが困難であり、事務全般の効率化を求める

ことができません。

弊社が構築するデータを安全かつローコストに管理可能なブロックチェーンのプラットフォームと電子入札業務を実現させる 一般財団法人 日本建設情報総合センター（J A C I C）の電子入札コアシステムを組み合わせ活用することで、契約事務手続き全般の効率化、新型コロナ感染症対策として接触機会低減などを図ることが可能です。g B i z I D等の共通認証システムや、マイナンバーカード等による個人認証と組み合わせることで、電子入札コアシステムを利用しない場合でも、電子契約の締結が可能になります。

また、電子契約の適用範囲を工事などの大型入札案件に留めず、認証基盤発行の I Cカードを利用しない少額の随意契約案件にも広げることで、国及び地方公共団体の契約事務を抜本的に改善するとともに、受託した事業者の事務効率も同時に期待できます。

さらに、電子契約で利用するブロックチェーンのプラットフォームを活用することで、社会のデジタル化を妨げていた信用確保に対するコスト（費用、時間、労力、仕組）を大幅に抑制できることから、マイナンバーカードとの連携や、I Cカードを使わない e K Y C（本人確認）とを組み合わせ、さまざまな社会問題の解決や自治体 D X を推進できます。例えば、行政内のすべての文書を対象にした決裁記録、本人確認が可能な申請届け出などのさまざまな分野へ容易に適用でき、社会全体のデジタル化・スマート化を加速させます。

【電子契約需要獲得見込み】

[Redacted text]

[Redacted text]

3. 新事業活動及びこれに関連する事業活動の内容

(1) 事業実施主体

サービス提供事業者：弊社

サービス利用者：国・地方公共団体、契約受託者

(2) 事業概要

データの改ざんが事実上困難なブロックチェーン技術を利用して、従来紙と印鑑を用いて作成されていた契約の署名を、国又は地方公共団体（甲）と民間事業者（乙）、もしくは複数者（J V や三者契約等）との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）を提供します。

本サービスは、電子入札システムと連携した電子契約サブシステムとなります。（図1の右側部分）

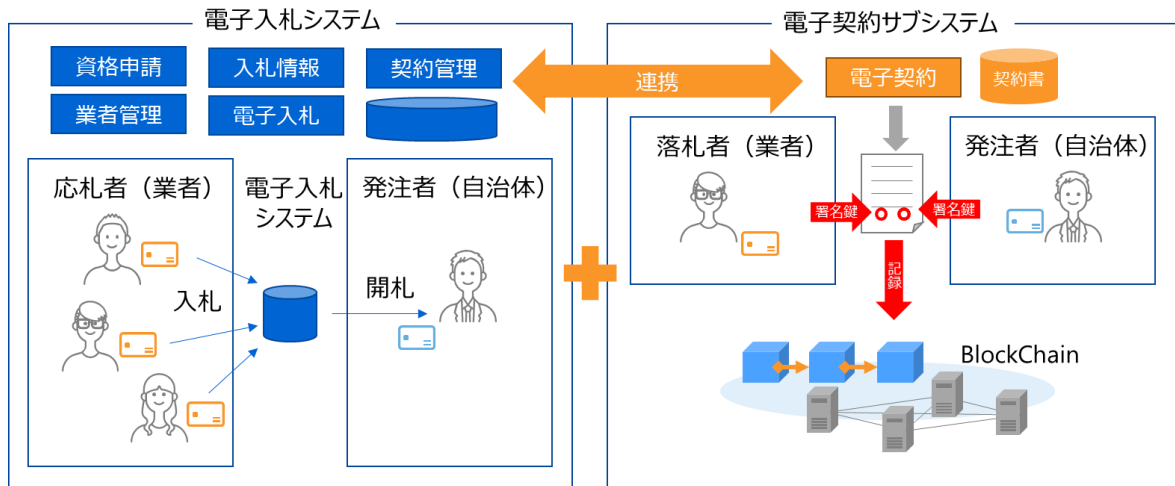


図 1 本サービスの概要図

ブロックチェーンにおいては、ブロックと呼ばれる記録の塊にネットワーク内で発生した取引の記録、1つ前に生成されたブロックの内容を示すブロックハッシュ値及びナンス値の3つを格納し、この3つの値を合成して、ハッシュ関数に入力し、当該ブロックのブロックハッシュ値を計算します。この生成されたブロックが時系列に沿ってチェーンのようにつながっていくことからブロックチェーンと呼ばれるものです。ブロックチェーンにおいては、改ざんが生じた場合、ハッシュ値に変更が生じることから後続するすべてのブロックのハッシュ値も変更しなければならず、事実上、改ざんは困難と考えられています。

ア) 契約手順

ブロックチェーンの技術を利用し、下記手順により契約締結を行います。

- ・国又は地方公共団体（甲）は、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」）を取得します。ICカードが無い場合でも、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と呼ばれるデータを利用することも可能です。
- ・民間事業者（乙）は、地方公共団体へ業者情報の登録を行い、登録番号の発行を受け、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」）を取得します。認証局発行のICカードを保有しない場合は、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と呼ばれるデータを取得します。また、契約当事者（甲乙）は、本サービスを通じて、ICカード又はWalletを用いて、公開鍵から作るブロックチェーン上でWalletを特定するための識別情報としてWalletアドレスを取得します。
- ・ICカードや登録番号を利用しない場合でも、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、Walletを取得できる仕組みの提供も予定しています。
- ・本サービスを利用して電子署名を行う場合、国又は地方公共団体（甲）は、まず、本サービスにログインを行い、上記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します。民間事業者（乙）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、認

証局発行のICカードを保有している場合、保有する証局発行の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します。証局発行のICカードを保有していない場合、民間事業者（乙）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します。

- 次に、契約当事者（甲乙）は、契約書の電子ファイルを、①本サービス上にアップロードする、又は②メールの添付ファイルとして送るといった方法により、受け渡しを行います。
- その後、契約当事者（甲乙）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）します。
- 契約当事者（甲乙）は、証基盤発行のICカード、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）に電子署名を行います。電子署名については、現時点では、RSA2048bitの暗号方式を用います。
- 電子署名を行う手順は、以下のとおりです。まず、電子署名を行う当事者は、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、①秘密鍵の有効化を行います。証基盤発行のICカード、証局発行のICカードを利用する場合には、当該ICカードリーダーによる読み取り後、PINコードを入力することにより秘密鍵の有効化を行います。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後、PINコードを入力し、秘密鍵の有効化を行います。②次に、契約書に合意したとのボタンを押します。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ます。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します。
- 電子署名は、契約当事者（甲乙）双方が行うため、ブロックチェーン上には民間事業者（乙）の電子署名、国又は地方公共団体（甲）の電子署名と2つの合意形成があったことが記録されます。契約当事者が三者となる場合も同様であり、この場合は、3つの合意形成があったことがブロックチェーン上に記録されます。
- ブロックチェーン上に取引記録としてタイムスタンプ情報の記録は行われませんが、時刻の記録は複数の管理ノードにより行われます。一般的には標準時に同期されたものを使い、これと大きくずれたものは排除されることとなります。また、ブロックチェーンの記録については、ブロックチェーンの性質上、ブロックチェーン前後の記録で時間が遡ることはないかとされています。
- 本サービスでは、最終合意をした契約書の電子ファイルを本サービス上に置き、契約当事者（甲乙）が当該契約書の電子ファイルの確認を行うことができることも予定しています。

イ) 検証手順

- 本サービスでは、ブロックチェーン上に記録された電子署名を行った秘密鍵に対応する公開鍵情報、最終合意をした契約書の電子ファイル及び電子署名データをもって、ブロックチェーンの仕組みを利用して検証を行うことが可能です。

- ①ブロックチェーン上には、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。契約当事者（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。
- ②契約当事者（甲乙）は、本サービスを通じて、甲が当該契約書に合意したというトランザクションは契約書の電子ファイルの作成者が甲であるか、すなわち、甲が電子署名をしたものかということ、乙が当該契約書に合意したというトランザクションは契約書の電子ファイルの作成者が乙であるか、すなわち、乙が電子署名をしたものかを確認することが可能です。
- ③契約当事者（甲乙）は、相手方の電子署名が本人のものであるかどうかについては、
（i）ブロックチェーン上に記録された電子署名者のWalletアドレスを取得し、当該Walletアドレスと紐づけられたユーザ情報を取得することにより、確認を行うことが可能です。（ii）認証局発行のICカードにより電子署名が行われている場合、電子証明書の取得及び業者登録情報により確認を行うことが可能です。
- ④上記①ないし③については、ブロックチェーン上に記録された内容と照合することにより確認を行うものです。上記のとおり、ブロックチェーン上の記録は改ざんが困難であり、上記プロセスを経ることにより、最終合意をした契約書の電子ファイルとの整合性、電子署名の整合性の検証が可能です。

さらに、ブロックチェーン上に記録された内容が改ざんされていないかを確認したい場合、本サービスを通じて、ブロックハッシュを生成するブロックに含まれている全部のトランザクションの確認をしていき、再計算してブロックハッシュが合っているかを検証することにより、整合性を確認でき、改ざんがなされていないかを確認することができます。現在は、検証ボタンがあり、それを押すと計算することができることを予定しています。

(3) 新事業活動を実施する場所

日本国内の地方公共団体向けにスタートし、府省、民需に拡大していきます。

4. 新事業活動及びこれに関連する事業活動の実施時期

準備期間 令和4年2月～（数か月程度）

実施期間 令和4年度中

5. 解釈及び適用の有無の確認を求める規制について規定する法律及び法律に基づく命令の規定

○電子署名及び認証業務に関する法律

第二条 この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）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、次の要件のいずれにも該当するものをいう。

一 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。

二 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。

2 この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

3 この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

○契約事務取扱規則

第二十八条 次の各号に掲げる書類等の作成については、次項に規定する方法による法第四十九条の二第一項に規定する財務大臣が定める当該書類等に記載すべき事項を記録した電磁的記録により作成することができる。

一 契約書

二 請書その他これに準ずる書面

三 検査調書

四 第二十三条第一項に規定する書面

五 見積書

2 前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は、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り作成するものとする。

3 第一項第一号の規定により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であつて法第四十九条の二第二項に規定する財務大臣が定める措置は、電子署名（電子署名及び認証業務に関する法律（平成十二年法律第百二号）第二条第一項の電子署名をいう。）とする。

○地方自治法施行規則

第十二条の四の二 地方自治法第二百三十四条第五項の総務省令で定めるものは、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（平成十五年総務省令第四十八号）第二条第二項第一号に規定する電子署名とする。

○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

第二条 この省令において使用する用語は、特段の定めがある場合を除くほか、情報通

信技術活用法において使用する用語の例による。

- 2 この省令において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
- 一 電子署名 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（平成十四年法律第百五十三号）第二条第一項又は電子署名及び認証業務に関する法律（平成十二年法律第百二号）第二条第一項に規定する電子署名をいう。

6. 具体的な確認事項並びに規制について規定する法律及び法律に基づく命令の規定の解釈及び当該規定の適用の有無についての見解

(1) 具体的な確認事項並びに規制について規定する法律

ア) 本サービスで採用した電子署名が電子署名法に定める「電子署名」に該当し、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できるか

本サービスで利用している電子署名の仕組みが、電子署名法第2条1項の「電子署名」に規定する技術的要件を満たしており、本サービスで採用した電子署名が電子署名法に定める「電子署名」に該当し、これを引用する地方自治法施行規則第12条の4の2、および契約事務取扱規則第28条3項で定める「電子署名」であって、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。

イ) 本サービスで採用している仕組みが、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か

本サービスは、電子署名法第2条1項の「電子署名」を引用する契約事務取扱規則第28条2項に規定する「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ことを確認したい。

(2) 法律に基づく命令の規定の解釈及び当該規定の適用の有無についての見解

法律事務所に意見を求めたところ、別添のとおり意見をいただいております。【別添：意見書 東啓綜合法律事務所 2021年9月16日】

ア) 本サービスで採用した電子署名が電子署名法に定める「電子署名」に該当し、契約書が電磁的記録で作成された記名押印に代わるものとして利用できるか

電子署名法第2条第1項では、1) 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、2) 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、3) 改変されていないことが確認できることと述べられています。

本サービスで採用した仕組みは電子署名法第2条第1項に規定される技術的基準の要件を満たしています。

地方自治法施行規則第12条の4の2、および契約事務取扱規則第28条3項で定める「電子署名」は電子署名法第2条第1項を引用しており、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という要件を満たしています。

1) 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

本サービスでは、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（PKCS#1 RSA2048bit）をするものです。

なお、本サービスでは契約書（PDF等）そのものに暗号化措置を行った情報を記録するのではなく、より安全に記録を保持できるブロックチェーンに②電磁的に記録を保持する方式を採用しています。

この方式における①暗号化措置は契約書（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）に行われる措置であることから、電子署名法第2条第1項に規定される「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」である技術的基準の要件を満たしています。

2) 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

本サービスでは、利用者が保有する秘密鍵（ICカードまたはWallet）と、これを利用するための本人しか知りえないPINコードを用いて、契約書（原文となる電子ファイル）のハッシュ値、および公開鍵を示す情報（Walletアドレス）、取引行為（コントラクト）とを一つにまとめた情報に、公開鍵暗号方式による暗号化措置（PKCS#1 RSA2048bit）をするものです。

本サービスの利用者の本人性は、国又は地方公共団体（甲）については、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」）を取得することにより担保されております。

また、民間事業者（乙）についても、地方公共団体へ業者情報の登録を行い、登録番号の発行を受け、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」）を取得することにより担保されております。

認証局発行のICカードを保有しない場合についても、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を取得し、本人性を担保するようにしております。さらに、本サービスを利用して国や地方公共団体で入札・契約を行おうとする事業者（利用者）は、本人を証明するための書類（登記事項証明書、納税証明書、メールアドレス等）を添えて、発注者に応札の申請をします。これらの本人確認及び受注資格に関する書類の審査を経て、入札参加資格有りと判断した事業者について、発注者から業者番号（ログインID）とパスワードが当該事業者に発行されます。当該事業者は、通知された業者番号とパスワードを元に、本サービスにアクセスし後続の各種登録処理を実施します。このため、発注者においても本人性の確認を行った事業者のみが本サービスを利用することができます。

以上のように、本サービスにログインした利用者は業者情報に登録された本人であ

り、利用者が利用する秘密鍵（ICカードもしくはWallet）が特定されています。この秘密鍵を使った電子署名は第三者の意思が介在せず、本人の意思のみで記録されます。これらのことから登録された秘密鍵を用いて暗号化措置行えるものは本人であり、「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」要件を満たしています。

なお、上記ICカードもしくはWallet取得後に、これら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します。このような仕組みにより、電子署名を記録するブロックチェーン上のユーザ情報についても、本人との結びつきが担保されています。

3) 改変されていないことが確認できること

ブロックチェーンを利用した本サービスでは、改変を検知する機能を備えるための技術として、公開鍵暗号方式による電子署名（PKCS#1 RSA2048bit）、および情報の電磁的記録においてブロックとよばれる情報の塊が時系列に沿って暗号化されたチェーンのようにつながっていく仕組みを採用しています。

契約書（原文となる電子ファイル）から求めた①契約書のハッシュ値（SHA256）と、公開鍵を示す情報（②Walletアドレス）、および取引行為（③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、④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を記録していきます。

この暗号文を公開鍵で復号化した④トランザクション要求のハッシュ値は、本来、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ようになっています。

万が一、契約書が変更されていると、トランザクション要求に含まれている①契約書のハッシュ値が変わり、その結果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が変わることから、④トランザクション要求のハッシュ値と合致しないため、改ざんが検知できる仕組みとなっています。また、ブロックチェーン上に記録された①のハッシュ値のみを検証することも可能です。

さらに、情報の記録においては、該当の暗号文を含むトランザクション要求情報と、直前のブロックのハッシュ値を含む情報とを一つにくくりブロックとし、時系列に沿った暗号化されたチェーンのように記録します。これにより、単一の暗号化措置に比べて、さらに強固な改ざん防止を施して記録する仕組みになっています。

これらのことから、契約書が不正に改ざんされた場合、改変の検知が可能であることから、「改変されていないことが確認できる」要件を満たしています。

イ) 本サービスで採用している仕組みが、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きるか

契約事務取扱規則第28条第2項では、同条第2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は、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り作成

するものと規定しています。

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、同意を行うものであることから、「各省各庁の使用に係る電子計算機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」に該当した「電磁的記録の作成」であることから、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要件を満たしています。

7. その他
特になし。