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 6 月 23 日

経済産業大臣　萩生田光一　殿
国土交通大臣　斉藤鉄夫　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（ＪＡＣ

ＩＣ）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。ｇＢｉｚＩＤ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ＩＣ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、ＩＣカードを使わないｅＫＹＣ（本人確認）とを組み合わせて、さまざまな社会問題の解決や自治体ＤＸ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]

３．新事業活動及びこれに関連する事業活動の内容

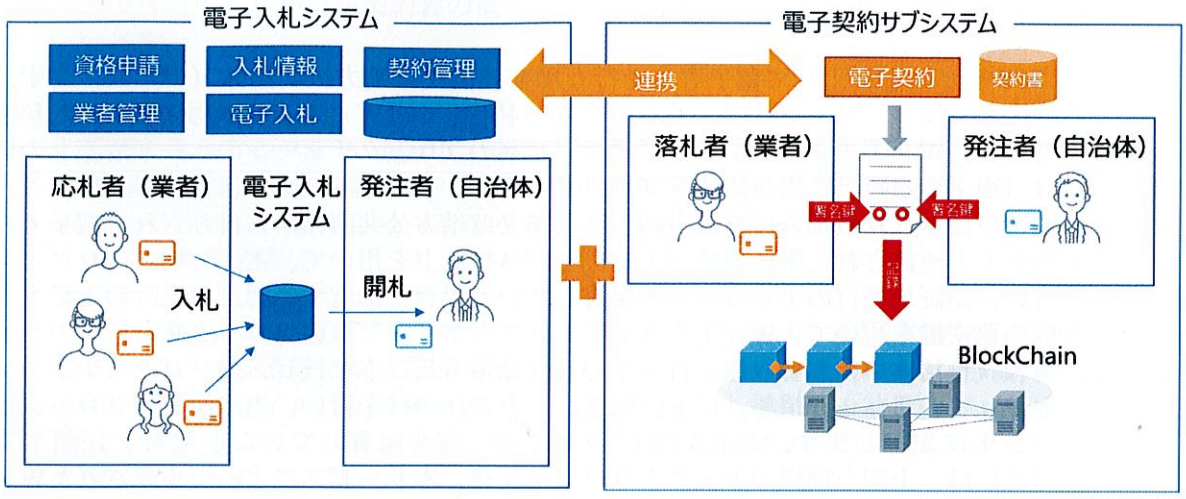
(1) 事業実施主体

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（ＪＶや三者契約等）との間で電子文書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。

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を組み合わせて、Ｗａｌｌｅｔを取得できる仕組みの提供も予定しています。

（予定している認証方法）

認証方法	①ＩＣカード	②ユーザＩＤ	③マイナンバー	④ｇＢｉｚＩＤ	⑤ｅＫＹＣ
本人確認方法	ＩＣカード＋ＰＩＮ	ＩＤ＋パスワード	マイナンバーカード（自己情報取得ＡＰＩ）	ｇＢｉｚＩＤログイン	各種二要素認証
秘密鍵の媒体	ＩＣカード	Ｗａｌｌｅｔ	Ｗａｌｌｅｔ	Ｗａｌｌｅｔ	Ｗａｌｌｅｔ
紐づけ情報	業者登録情報	業者登録情報	業者登録情報	業者登録情報	業者登録情報

※ＩＣカードは、外部Ｗａｌｌｅｔと呼ばれます。

※サービス開始時は①および②を実装し、今後の拡張として③以降を計画しています。

・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カードもしくは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（※１）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します。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（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、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。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ファイルを読込後、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します。
・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。

※1 紐づけ処理

電子入札コアシステム（JACIC）対応した弊社の電子入札システムの業務フローでは、民間事業者は、地方公共団体へ業者情報の登録をする一連の処理のなかで、ICカードを利用するために、登録番号（及びパスワード）を指定して登録します。ICカードを保有しない民間事業者については、発行されたユーザ情報（ID）/パスワードでアクセスし登録をします。

電子入札システムと電子契約サブシステムは連携しており、利用者情報登録機能と同じ仕組みで、登録番号に対して利用しているICカードもしくは生成されたWallet（秘密鍵が含まれるファイル）からWalletアドレスを生成します。その結果をブロックチェーン上に記録することで、業者情報、Walletアドレス、ブロックチェーンのユーザ情報の紐づけを行います。

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（原文となる電子文書）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を、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、上記のほかに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

○建設業法施行規則

第十三条の四　法第十九条第三項の国土交通省令で定める措置は、次に掲げる措置とする。

２　前項に掲げる措置は、次に掲げる技術的基準に適合するものでなければならない。

一　当該契約の相手方がファイルへの記録を出力することによる書面を作成することができるものであること。

二　ファイルに記録された契約事項等について、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措置を講じていること。

三　当該契約の相手方が本人であることを確認することができる措置を講じていること。

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

ブロックチェーンを利用した電子契約である本サービスが、建設業法施行規則第１３条の４第２項に規定する技術的基準を満たしているか。

(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

ア）当該契約の相手方がファイルへの記録を出力することによる書面を作成することができるものにあたるか。（見読性）

本サービスが提供するサーバで保管する電子ファイルをダウンロード、もしくは個々に保管している電子ファイルを、一般的なオフィスソフトなどを利用して閲覧することや、印刷することができます。

このことから、建設業法施行規則第１３条の４第２項第１号「当該契約の相手方がファイルへの記録を出力することによる書面を作成することができるものであること。」の要件を満たすと判断しています。

イ）ファイルに記録された契約事項等について、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措置を講じているといえるか。（原本性）

本サービスが提供するサーバで保管する電子ファイルをダウンロード、もしくは個々に保管している電子ファイルを、ブロックチェーンにそのハッシュ値を問い合わせることで、契約当事者が契約へ合意した事実を確認することができます。

本サービスでは、秘密鍵（ＩＣカード又はＷａｌｌｅｔ）を用いて電子文書のハッシュ値等に電子署名してブロックチェーンに記録しますので、電子文書が改ざんされた場合にはハッシュ値が変わることから、改ざんされた電子文書の契約事実はブロックチェーンに記録されておらず、契約事実が確認できません。

また、電子文書が「ある時刻に存在していたこと」及び「その時刻以降に当該電子データが改ざんされていないこと」を証明するため、ブロックチェーンでは、標準時に同期された複数の管理ノードが時刻の整合性を確認して記録します。また記録された情報はデータが連結し時系列に記録されていることなど、ブロックチェーンの仕組みから改ざんすることは事実上困難な状態です。

これらのことから、建設業法施行規則第１３条の４第２項第２号の「ファイルに記録された契約事項等について、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措置を講じていること。」に該当すると判断しています。

ウ）当該契約の相手方が本人であることを確認することができる措置を講じているといえるか。（本人性）

本サービスでは、認証局が発行したＩＣカード、もしくは入札参加資格登録申請で取得したユーザID/パスワード、ｇＢｉｚＩＤ、ｅＫＹＣ等の認証を経て、本サービスにログインすることで、本サービスを利用するものが国または地方自治体に登録されているユーザとして認識されます。
本サービスにログイン後に、そのユーザに紐づけられているＩＣカードやＷａｌｌｅｔを、本人しか知りえないＰＩＮコードを用いて復号化するなどして利用できる状態にし、ＩＣカードやＷａｌｌｅｔの秘密鍵を用いて、電子文書のハッシュ値や契約合意事実などに電子署名し、ブロックチェーンに記録する仕組みです。この２段階の認証にて「本人性」を特定しています。

これらのことから、建設業法施行規則第１３条の４第２項第３号の「当該契約の相手方が本人であることを確認することができる措置を講じていること。」の要件を満たすと判断しています。

７．その他

照会書に記載した専門用語の説明を記載します。

用語	説明
GPKI	GPKI とは、Government Public Key Infrastructure の略称で、政府認証基盤です。
LGPKI	LGPKI とは、Local Government Public Key Infrastructure の略称で、地方公共団体が利用している地方公共団体組織認証基盤です。
電子証明書	信頼できる第三者（認証局）が間違いなく本人であること

	を電子的に証明することや、改ざんされていないことを確認できるものです。
電子入札コアシステム	電子入札コアシステムとは、日本建設情報総合センター（JACIC）が提供する電子入札システムの中心となるソフトウェアです。
電子入札コアシステム対応認証局	電子入札コアシステムで利用できる IC カードを発行する認証局です。
商業登記認証局	商業登記に基づく電子認証制度の電子証明書を発行する認証局です。
Wallet	ブロックチェーンで利用する秘密鍵を含む情報です。通常は電子ファイルに格納されますが、Wallet として IC カードに格納された秘密鍵を利用することもできます。
Wallet アドレス	Wallet アドレスとは、Wallet がもつ秘密鍵とペアになる公開鍵の情報を元に計算されるアドレス形式の情報です。Wallet アドレスは十分な長さを持つため、Wallet アドレスによって Wallet を一意に特定できます。
gBizID	一つの ID・パスワードで複数の行政サービスにアクセスできる、法人・個人事業主向け認証システムのことです。
eKYC	スマホや PC を使用して、オンライン上で本人確認を完結できる仕組みのことです。
SHA-256	SHA-256 とは、Secure Hash Algorithm 256-bit のことで、任意の長さの原文から固定長の特徴的な値（原文に不可逆な値、ハッシュ値）を算出する計算手順の一つです。256-bit の固定長を計算するものが SHA-256 ですが、384bit や 512bit を計算するものもあります。
RSA2048bit	RSA とは、公開鍵暗号アルゴリズムの一つで、暗号化とデジタル署名が同時にできる仕組みです。鍵長が 2048bit のものを、RSA2048bit と呼びます。 暗号化するための鍵を秘密鍵といい、複合化するための鍵を公開鍵と呼びます。
ハッシュ値	元になるデータから一定の計算手順により求められた固定長の値のことです。電子ファイルからは一つのハッシュ値が計算されますが、電子ファイルの内容が変化（改ざん）するとハッシュ値が異なります。
ナンス値	ブロックチェーン上でデータのブロックをつなぐための値の一つで、Number Used Once の略称です。
管理ノード	ブロックチェーンのデータは複数に分散されたコンピュータで管理されていますが、その管理しているコンピュータを管理ノード（もしくはピア）と呼びます。
トランザクション	ブロックチェーンにおけるトランザクションとは、契約行為や電子マネーの授受などの行為を表すデジタル情報を指します。トランザクションに署名するとは、そのデジタル情報にデジタル署名を行うことを意味します。トランザクションを記録するとは、そのデジタル情報を複数の管理ノード内に格納することを意味します。
ブロックハッシュ	ブロックチェーンでは、１つまたは複数のトランザクションを含めて記録しているまとまったデータの単位をブロックといい、そのブロックの内容全体のハッシュ値を計算し

	た値をブロックハッシュと呼びます。ブロックの内容には、一つ前のブロックのブロックハッシュが含まれ、全体としてチェーン構造を形成しています。