資料１－２

トラストサービスに関する主な検討事項

２０１９年１月３１日

事　　務　　局

トラストサービスの必要性

必要性１　サービスに応じたIDの利用

○　プラットフォーム事業者の発行するIDを利用して、様々なサービス間の連携が進展。当該IDの発行に際して行われる本人確認のレベルは様々であり、必ずしも厳格な本人確認が行われていないものも存在。

○　求められる本人確認のレベルが様々である状況を踏まえると、利用者や利用可能なサービスの多寡を基準にIDを選ぶのではなく、利用するサービスに求められる本人確認のレベルに応じたポリシーに基づいて発行されたIDを選ぶ環境を整えることが必要。

○　これにより、多種様々なオンラインサービスについて、それらの内容・重要度に応じてID情報の信頼度をレベル分けするLoA（Level of Assurance）の考え方に基づいた利用・提供の実現が可能。

トラストサービスの必要性

必要性２　Society5.0を支えるトラストサービス

○　近年のIoTの爆発的な普及等に伴い、サイバー空間と実空間の一体化が加速的に進展しており、実空間での様々な活動がサイバー空間に置き換わる中、その有効性を担保するためには、サイバー空間の安全性や信頼性の確保が重要。

○　センサーを始めとする、様々なモノがネットワークにつながる中、正当でないモノがネットワークにつながったり、誤ったデータや改ざんされたデータが紛れ込まないようにすることが重要。

○　人だけでなく、組織やモノも認証するとともに、データの完全性を確保するためのトラストサービスの実現が必要。

○　Society5.0に向けて、トラストサービスの基盤を活用することが考えられる例として、情報銀行が挙げられる。情報銀行による個人に向けたサービスが適切に行われるには、各関係者の正当性の確認や、データ流通の過程において改ざん等が行われていないかを担保する完全性の確保が重要。

欧州におけるトラストサービスの動向

○ EUは、eIDAS(electronic Identification and Authentication Services)規則を2016年7月に発効。eIDAS規則では、一定の要件を満たすトラストサービスの提供者を適格トラスト・プロバイダーとして規定し、EU各国はトラストリスト(適格トラスト・プロバイダーのリスト)を公開し、維持しなければならない。具体的には、電子署名、タイムスタンプ、ウェブサイト認証、eシール、eデリバリー等の法的枠組みを規定。

電子署名	○ 自然人が電磁的に記録された情報について、その自然人が作成したことを示すもの。
タイムスタンプ	○ 電子データが、ある時刻に存在していたこととその時刻以降に改ざんされていないことを示すもの。
ウェブサイト認証	○ ウェブサイトが真正で正当な主体により管理されていることが保証できることを示すもの。
eシール	○ 文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すもの。
eデリバリー	○ データの送受信の証明も含め、データ送信の取扱いに関する証拠を提供するもの。

○ 他方、我が国には、eIDAS規則に相当するトラストサービスを包括的に規定する法令が存在しない。国際的な相互運用性の確保の観点からも、トラストリストの構築を含め、我が国としてのトラストサービスの在り方について検討が必要。

○ データを国外とやり取りする国民や企業等が、国外での訴訟等においてその真正性や完全性を主張する場合など、国民や企業等が国外での権利実現を図る基盤としても、我が国における法制度に基づくトラストサービスの構築が期待。

トラストサービスの在り方の検討における基本的視点

視点１　ネットワークにつながる人・組織・モノの正当性を確認できる仕組みの確保（Identification / Authentication）

○　金融サービスや企業の重要情報を取り扱う電子契約のような利用にあたって高いレベルの本人確認が求められるオンラインサービスにおいては、プラットフォーム事業者が提供するIDの活用が十分に進んでいない現状。

○　信頼性の高いサービスを実現するためには、人やモノの真正性を適切に確認してIDが発行される（Identification）とともに、誰からの／何からのデータであるかを確認する仕組みとしてPKI（Public Key Infrastructure）等を活用した、よりハイレベルで、より厳格な認証（Authentication）の仕組みが必要。

○　Society5.0の実現に際しては、（１）誰からのデータであるかを保証する利用者認証、（２）組織が発行したデータであることを保証する組織による認証、（３）ネットワークにつながるIoT機器等のモノからのデータであることを保証するモノの認証の在り方についての検討が必要。

○　こうした認証を行うことで、認証された利用者、組織やモノがどのようなデータにアクセス可能か、データへの認可（Authorization）をサービスごとに柔軟に変えることができる仕組みの実現に寄与。

トラストサービスの在り方の検討における基本的視点

視点２　データの完全性の確保（Data Integrity）

○　大量のデータが流通するSociety5.0において、データの利用価値を高めるためには、完全性（Integrity）の観点も重要であり、具体的な仕組みとしてトラストサービスは有効。

○　データの信頼性を保証するためには、データの完全性（改ざんされていないか）を確保することが必要であり、（１）データの存在証明・非改ざん証明の仕組みや、（２）データの完全性と送受信の正当性の確認を組み合わせた仕組みについての検討が必要。

○　トラストサービスが長期的に確保できる検証サービスについての検討も必要。

トラストサービスの実現にあたって配慮すべき事項

○ Society5.0において、サイバー空間におけるサイバーセキュリティの確保は重要であり、トラストサービスの実現にあたっては、サイバーセキュリティの三要素である機密性（Confidentiality）や、データの真正性を含めた完全性（Integrity）とともに、利用者が簡便に利用できるような可用性（Availability）を確保することが必要。

○ トラストサービスの実現にあたっては、技術革新のスピードに鑑み、最新の技術動向を踏まえつつも、特定の技術に依拠することなく、要件志向で検討することが必要。

○ トラストサービスの実現にあたっては、技術的な堅牢さや強度だけを追求するのではなく、利用者にとって使いやすいインターフェースであることが必要。

○ ID登録の際に取得する情報について必要最小限のものに留めるなどプライバシー・バイ・デザインにも配慮が必要。

○ トラストサービスを提供する事業者や利用者にとって過度なコスト負担や不便を強いることが無いよう、検討することが必要。

基本的視点に基づく検討事項

視点１

ネットワークにつながる人・組織・モノの正当性を確認できる仕組みの確保（Identification/Authentication）

- **検討事項１－１** 人の正当性を確認できる仕組み
  - （１）利用者認証
  - （２）リモート署名
- **検討事項１－２** 組織の正当性を確認できる仕組み
  - （１）組織による認証
  - （２）ウェブサイト認証
- **検討事項１－３** モノの正当性を確認できる仕組み

視点２

データの完全性の確保（Data Integrity）

- **検討事項２－１** データの存在証明・非改ざん証明の仕組み
  - タイムスタンプ
- **検討事項２－２** データの完全性と送受信の正当性の確認を組み合わせた仕組み
  - eデリバリー

検討事項１－１　人の正当性を確認できる仕組み

（１）利用者認証

○　プラットフォーム事業者が発行するIDについて、当該事業者が提供するもの以外も含めて、様々なオンラインサービスのログインに利用が拡大。しかしながら、当該IDの発行に際しては、必ずしも厳格な本人確認が行われていない場合もあり、より高いレベルでの本人確認が求められるサービスへの利用については限界。

○　フィンテックなど新たなサービスの創出も見据え、その基盤となる利便性と信頼性を合わせ持った利用者認証のためのトラストサービスが期待。

○　トラストサービスの起点として、PKIベースの電子証明書の活用が有力な方策となり得るが、これについては、

①　公的個人認証制度（※）において、電子署名のための電子証明書に加え、マイナポータルに接続する際の本人確認等に用いる利用者認証のための電子証明書も発行されている一方、

（※）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

②　電子署名のための電子証明書を発行する民間の認証局に係る規律（電子署名法）はあるものの、利用者認証のための電子証明書を発行する民間の認証局については規律されておらず、官民で制度上の非対称が存在。

○　こうした状況を踏まえ、民間の認証局が発行する電子証明書を利用するサービスの具体的なニーズと、当該認証局への規律の必要性について検討。

検討事項１－１　人の正当性を確認できる仕組み

（２）リモート署名

○　クラウドの急速な普及に伴い、様々なオンラインサービスにおいて、データやアプリケーション等をクラウド上に保管し、ネットワークを通じて利用することができるクラウドサービスが進展。

○　現行の電子署名法においては、電子証明書（鍵）をICカード等に収納し、ユーザーが当該カードを用いてパソコン等から電子署名を付すことを前提。

○　電子署名に関しても、クラウドを介して電子証明書（鍵）を利用するリモート署名について、

・　一定のネットワーク環境があれば、端末を選ばずに電子署名を利用できるようになり、利便性が大幅に向上する

・　ICカードの紛失等のリスクが無くなる

といったメリットから、ニーズが見込まれている。

○　こうした状況を踏まえ、リモート署名を実現する上での技術的課題や制度的課題について検討。

検討事項１－２　組織の正当性を確認できる仕組み

（１）組織による認証

○　商業登記に基づく電子認証制度(※1)においては、法人の代表者に対する電子証明書を発行。また、企業による行政への電子申請等、代表者の委任を受けて行う行為については、社員個人に発行された電子証明書を用い、代理権等については電子委任状による確認をすることで一定の措置(※2)。

（※1） 商業登記法 （※2） 電子委任状の普及の促進に関する法律

○　一方、例えば、企業がソフトウェアアップデートプログラムを配布する場合やプレスリリースを行うような場合には、組織として情報やデータを発行するものであり、企業の社員の意思に基づくものではないため、社員個人による署名はなじまず、企業名による署名により発行するニーズが存在。

○　受信者から見ても、組織のなりすましの防止により、安心してさまざまなサービスを利用できる基盤となりうる。

○　EUにおいては、eIDAS規則において、文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示すものとしてeシールが規定。

○　こうした状況を踏まえ、我が国における組織による認証のユースケースの具体化や制度的課題について検討。

検討事項１－２　組織の正当性を確認できる仕組み

（２）ウェブサイト認証

○　ウェブサイト認証のための電子証明書を発行する認証局については、CA／ブラウザフォーラムが定める要件がデファクトスタンダード化されており、当該要件を満たすと認められなくなると、必ずしもセキュリティ上問題がない場合であっても、ウェブブラウザ上、安全ではないサイトと表示されるおそれ。

○　EUでは、eIDAS規則に基づき適格な認証局を公的にリスト化しており、当該認証局については、CA／ブラウザフォーラムにおいても安全なものと認定。

○　こうした状況を踏まえ、現行のデファクトスタンダード化の状況における問題点を具体化した上で、認証局に係る我が国として適切な要件を設定することの必要性を検討。

検討事項１－３　モノの正当性を確認できる仕組み

○　IoT時代において、例えば、各種センサーから送信される環境情報（気温や雨量等）や生体情報（体温や心拍数等）、自動走行する車の部品から送信されるプローブ情報（走行位置や速度等）等を活用する際、モノの正当性を確認することで、データのなりすまし等を防止する仕組みが求められる。

○　また、API（Application Programming Interface）を活用したさまざまなプログラムが機械的にサーバ等と情報を送受するようになり、AI（Artificial Intelligence）の活用が進展する中、モノがサーバ認証を行うケースが増えることが見込まれる。

○　利用者認証や組織認証と同様に、モノの認証においても例えばPKIによる認証の仕組みが考えられるが、センサーなどのIoT機器にPKIの仕組みを導入することには、機能的な制約もある。

○　モノの認証においてどのような認証の在り方があるか、技術的課題や制度的課題について検討。

トラストサービスの在り方の検討事項

検討事項２－１　データの存在証明・非改ざん証明の仕組み

タイムスタンプ

○　現在は、総務省指針「タイムビジネスに係る指針」（2004年11月５日）に基づき、日本データ通信協会による民間の認定スキーム（タイムビジネス信頼・安心認定制度）により、タイムスタンプ事業者がサービスを提供しており、国税関係の帳簿保存への利用をはじめ、着実に利用が拡大。

○　法律上の位置付けがあれば、一層の利用拡大が見込まれることが期待。

○　今後、タイムスタンプを付した電子文書を国際的にやりとりする機会が拡大することが見込まれている。EUにおいては、eIDAS規則に基づき一定の基準を満たすタイムスタンプ事業者が適格なサービス提供者として認められているところ、今後、我が国の事業者が発行するタイムスタンプがEUにおいて有効とみなされない事態や、我が国のタイムスタンプビジネスがEUの事業者に席巻されるような事態を招くおそれ。

○　EUとの政策対話において、タイムスタンプを含むトラストサービスに関して、具体的なユースケースに基づいて相互の制度を比較するマッピングを進めることを合意。その交渉状況を踏まえ、国際的な相互運用性の確保等の観点から、タイムスタンプの制度の在り方について検討。

○　トラストサービスが長期的に確保できる検証サービスについての検討も必要。

検討事項２－２　データの完全性と送受信の正当性の確認を組み合わせた仕組み

eデリバリー

○　送信・受信の正当性や送受信されるデータの完全性の確保を実現するサービスとして、eIDAS規則においてはeデリバリーを規定。

○　例えば、ドイツでは、暗号化されたメッセージの送受信の証拠を保証する「De-Mail」サービスが提供されている。

○　こうした状況を踏まえ、送信・受信の正当性を確認するとともに送受されるデータの完全性の確保を実現するサービスに対するニーズの具体化について検討。