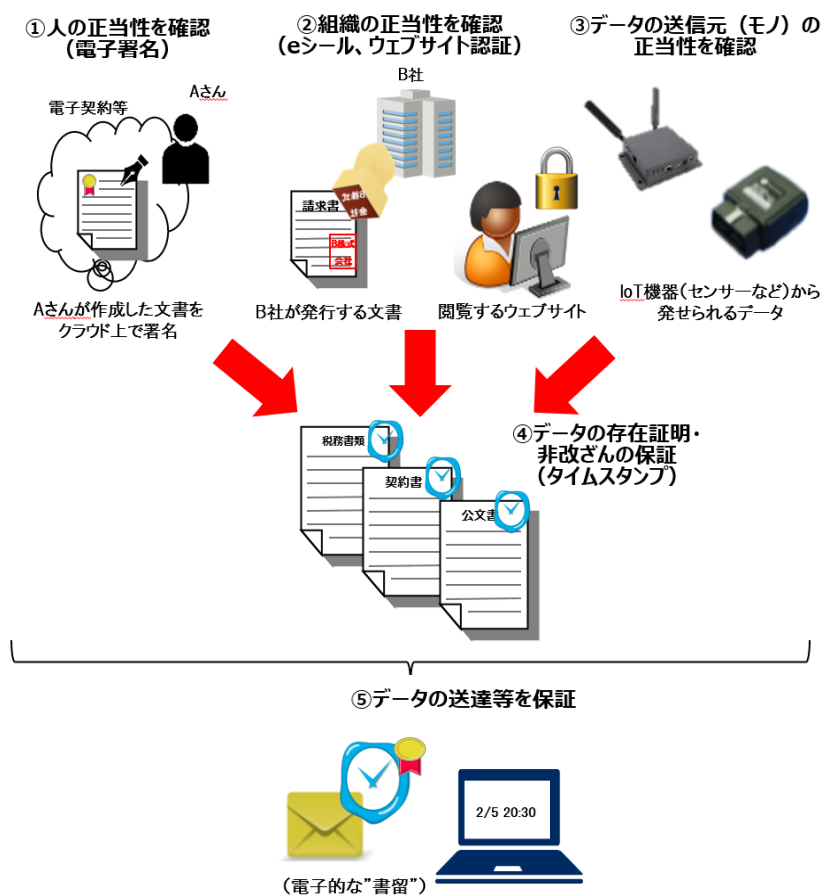


トラストサービスがもたらすビジネス改革

令和元年6月17日
総務省
サイバーセキュリティ統括官室

- Society5.0の実現に向けて、サイバー空間と実空間の一体化が加速的に進展し、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の基盤として、ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスが必要。

トラストサービスのイメージ



- ① 電子データを作成した本人として、**人の正当性**を確認できる仕組み(電子署名)
- ② 電子データを発行した法人として、**組織の正当性**を確認できる仕組み(組織を対象とする認証、ウェブサイト認証)
- ③ IoT時代における各種センサーから送信されるデータのなりすまし防止等のため、**モノの正当性**を確認できる仕組み
- ④ 電子データがある時刻に存在し、その時刻以降に当該**データが改ざんされていないことを証明**する仕組み(タイムスタンプ)
- ⑤ **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**する仕組み

① リアル空間→サイバー空間へ

社会経済活動全体において、紙のデータの電子化が十分に進んでいない。民間のデジタル化の推進のためには、作成された文書等の真正性やデータの完全性の確保が必要。

(参考:e文書法制定時の経団連の試算(2004年)では、税務書類の紙による保存コストは年間約3,000億円)

(事例) 日本公認会計士協会が発出している通達において、監査法人が上場企業の監査を行う際は原本で確認することが規定されており、監査が終了するまでは原本の破棄はできないという現状がある。その根本的な原因として、電子的に長期保存されたデータの信頼性が担保されていないということが考えられる。

② Society5.0に対応した組織やモノを認証する仕組みの構築

電子署名法は、ヒトに対して電子証明書を発行する仕組みであるところ、Society5.0においては、ネットワークにつながる組織や機器から大量のデータが送信される中で、組織やモノの正当性、また、それらから発信される情報の完全性を確認できる仕組みの構築が必要。

データの信頼性確保のための基盤構築の必要性

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やデータの完全性の確保等を実現するためのトラストサービスについて、EUにおけるeIDAS規則の制定等の動きも踏まえつつ、国際的なサービスの進展を視野に入れた相互運用性の確保の観点からも、我が国としての在り方について検討が必要。

- 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。

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や、国民や企業等の国外での権利実現を図るための基盤構築の観点からも、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。

検討事項

- (1) 我が国のトラストサービスに係る現状と課題
- (2) 上記(1)の課題を解決するための方策

プラットフォームサービス
に関する研究会

トラストサービス検討
ワーキンググループ

- ・ プラットフォーム事業者による利用者情報の適切な取扱いの確保の在り方等を検討
- ・ 総合通信基盤局長とサイバーセキュリティ統括官が共同で開催
- ・ 我が国におけるトラストサービスの在り方について、国際的な動向も踏まえつつ検討
- ・ 第1回 1/31、第2回 2/15、第3回 2/28、第4回 3/19、第5回 4/15、第6回 5/13、第7回 5/31

構成員等

(構成員)

- | | |
|-------------|--|
| 手塚 悟 (主査) | 慶應義塾大学大学院 政策・メディア研究科 特任教授 |
| 宮内 宏 (主査代理) | 宮内・水町IT法律事務所 弁護士 |
| 新井 聡 | 株式会社エヌ・ティ・ティ ネオメイト ITビジネス本部 プラットフォームサービス推進部電子認証サービス担当 主査 |
| 小笠原 弘貴 | 株式会社エヌ・ティ・ティ・データ セキュリティ技術部 サイバーセキュリティ統括部 ソリューション担当 課長 |
| 小川 博久 | 日本トラストテクノロジー協議会 運営委員長 |
| 楠 俊樹 | 株式会社三井住友銀行 事務統括部 上席推進役 |
| 繁戸 和幸 | 株式会社安井建築設計事務所 ICT本部 本部長 |
| 柴田 孝一 | セイコーソリューションズ株式会社 DXソリューション統括部 部長 |
| 袖山 喜久造 | SKJ総合税理士事務所 所長 |
| 谷 幹也 | 日本電気株式会社 セキュリティ研究所 所長 |
| 西山 晃 | セコムトラストシステムズ株式会社 プロフェッショナルサポート1部 担当部長 |
| 古屋 昌彦 | 株式会社日立製作所 公共システム事業部 公共ソリューション推進第二部 担当部長 |
| 宮崎 一哉 | トラストサービス推進フォーラム 副会長 |

(オブザーバー)

内閣官房情報通信技術 (I T) 総合戦略室、法務省、経済産業省、一般財団法人日本情報経済社会推進協会 (JIPDEC)

スケジュール

2019年1月	2月	3月	4月	5月	6月	7月	...	12月	
総務省 トラストサービス検討ワーキンググループ									
1月～4月 関係者ヒアリング				5月～7月 論点整理			▲ 中間 取りまとめ		▲ 最終 取りまとめ

検討事項1 人の正当性を確認できる仕組み(電子署名)

電子署名については、電子署名法が整備されているものの、クラウドを活用したリモート署名など最新の技術に制度が十分に対応しきれていない部分があるため、検討が必要。

検討事項2 組織の正当性を確認できる仕組み

・組織を対象とする認証(eシール)

請求書、領収書等の企業が発行する文書等に対し、電子的にその企業が発行したことを簡便に保証する仕組みがないことから、その在り方について検討が必要。

・ウェブサイト認証

CA/ブラウザフォーラムの定める基準がデファクトスタンダード化していることにより生じている課題への対応について、検討が必要。

検討事項3 IoT機器等のモノの正当性を確認できる仕組み

IoT化がますます進展する中、モノのなりすましやデータの改ざん等を防止するため、モノの正当性について検討が必要。

検討事項4 データの存在証明・非改ざんの保証の仕組み(タイムスタンプ)

日本データ通信協会による民間の認定スキームが存在する中、今後、タイムスタンプの更なる利用拡大に向けて、検討が必要。

検討事項5 データの送達等を保証する仕組み

EUのeデリバリーに相当するような、トラストサービスを利用した新たなサービス創出に向けて、検討が必要。

現状

- リモート署名については、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ができるようになることに加え、ICカードの紛失等のリスクが無くなる等のメリットから、利便性が大幅に向上し、利用拡大が期待されている。
- 電子契約において、契約者が署名をする場合、現状では主にICカードを用いており、ICカードや端末がある場所でないとう電子署名が行えない状態となっている。
- EUでは、安全なリモート署名に関する規格や評価制度等も含めて規定され、リモート署名が広く利用されている。

課題1: 制度的な位置づけが明確ではない

- クラウドを介するリモート署名が本人によるものであることが技術的に担保される場合において、電子署名法第3条に基づく「本人による電子署名」であると言えるか、制度的な位置づけが明確ではない。

課題2: 技術的な要件が整理されていない

- リモート署名サーバの中に格納した本人の秘密鍵にログインする際のアクセス方法について、どのような要件を満たせば本人によるアクセスとされるのか、技術的な基準が整理されていない。
- 我が国においてリモート署名のシステムを実装するに当たっては、
 - ・ 重要な鍵ペアの安全な管理・利用シーン
 - ・ 保証レベルの考え方を踏まえた本人確認の仕組みなど、セキュリティ確保の観点から、顧客に安全性を納得してもらえるレベルの基準策定が必要。

現状

- 法人が行う契約や申請において、法人代表者や法人代表者から委任された担当者が意思表示をする場合には、実空間では代表印（丸印）や個人印の押印、電子的には電子署名を利用しており、後者については、電子署名法や電子委任状法といった法制度が整備済。
- 他方、法人が発行する請求書や領収書等の書類については、実空間では社印（角印）で済ませているところ、電子的には組織を対象として認証する仕組みがない。
- EUでは、eIDAS規則に基づき、eシールを電子データの完全性と起源を保証するものとして法的な効力が認められている。

課題1：組織が行う実空間でのやりとりが、サイバー空間では簡便に実現できていない

- 法人の真正性を電子的に担保する法的枠組みがないため、法人が発行する請求書や領収書等の書類についても、法人代表者又は法人代表者から委任された担当者の電子署名で処理している場合が多い。このため、
 - ・ 受取側にとっては、発行側の担当者の異動、退職後に請求書等の有効性の確認に手間が生じる
 - ・ 発行側にとっては、担当者の異動、退職時に電子署名の電子証明書を改めて発行する必要がある
 - ・ 書類ごとに自然人による意思表示を示す電子署名は、機械的な大量処理に向かないといった課題が存在する。

課題2: 業務の効率化が十分に進んでいない

- 法人が発行した請求書や領収書等については、機械発行したものに対して自動的にeシールを付す処理が効率的であるが、我が国においては、紙で発行された請求書や領収書等をスキャナ等により電子化し、保存する形態にとどまっており、電子化のメリットが十分に発揮できていない。
- 他方、EUでは、エストニアにおいて電子処方箋や従業員登記などのサービスを中心にeシールの利用が拡大しているほか、EU全体としても、決済サービス指令(PSD2)において、金融機関等の決済サービス業者が提供するサービスの決済データを対象に、eシールの利用が義務化されていることから、利用が拡大している。
- 我が国でも、2023年10月に、軽減税率導入に伴う「適格請求書等保存方式」(インボイス制度)の導入が予定されており、事業者側の手間が増えることが想定されている。eシールを活用することで、インボイスの真正性を確保しつつ、突合、検索、計算などが自動処理可能となり、デジタル化による負担軽減や大幅なコスト削減が期待。

課題3: Society5.0に向けた対応が求められる

- 現行パソコンやスマートフォンのアップデートプログラムにコード署名が付されている場合は、OSやブラウザにより検証が実施されているが、Society5.0時代においては、様々な機器がインターネットに接続されるIoT化が進展することとなり、これら機器のプログラムをアップデートする場合、コード署名について一般的なOSやブラウザによらない検証が増加すると予測されていることから、その際の検証方法について検討が必要である。
- また、プログラムをアップデートする際、真正性を確認するに当たっては、自然人の電子証明書を利用した場合、担当者ごとに電子証明書を管理する必要があり、管理コストが高くなることから、組織・法人を対象とする電子証明書を発行するニーズが高まっている。

- 2023年の消費税に係るインボイス制度の導入に伴い、**仕入税額の控除に当たっては、税務署に登録された適格請求書等発行事業者が発行した請求書等を保存**することが要件。
- 仕入先が多岐にわたる場合、適格請求書等発行事業者の発行した請求書等を**個別に確認する事務作業が膨大に発生**。
- インボイスの電子化により、事務負担の軽減が期待されるが、上記の適格請求書等発行事業者を**効率的に確認する仕組みがない**。

期待される効果

- **法人に対する認証の仕組み(eシール)を制度化し、適格請求書発行事業者であるかを属性として記載することで、電子インボイスによる効率的で正確な納税手続を実現**。

(参考) 消費税に係るインボイス制度

- 消費税法改正（2016年4月）により消費税の軽減税率制度が2019年10月から開始されるころ、複数税率（標準税率10%、軽減税率8%）の下で適正な課税を確保する仕組み（仕入れ税額控除の方式）として、2023年10月から適格請求書等保存方式（いわゆるインボイス制度）が実施される。
- 適格請求書とは「売手が買手に対し正確な適用税率や消費税額等を伝えるための手段」であり、一定の事項（取引年月日、消費税率、軽減税率の対象品目である旨等）が記載された書類のこと。

適格請求書のイメージ

(株)〇〇御中 請求書 ××年11月分			
11月1日	牛肉	※	5,400円
11月2日	小麦粉	※	2,160円
・	・	・	・
・	・	・	・
・	・	・	・
11月30日	ビール		6,600円
※	軽減税率対象	合計	87,200円
		うち消費税	7,200円
(10%対象)	40,000円	消費税4,000円	
(8%対象)	40,000円	消費税3,200円	
登録番号 T1234567890123			



現状

- 利用者がウェブサイトを開覧する際、ウェブブラウザでサーバ証明書を確認することにより、そのウェブサイトが正当な企業等により開設されたものであるかどうかを確認することができるウェブサイト認証という仕組みが利用されている。
- その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求められる基準については、認証局事業者と米国のウェブブラウザベンダ等からなる団体である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、必ずしも直ちに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がある。
- EUでは、eIDAS規則に基づき、一定の要件を満たした適格な認証局を公的にリスト化し、当該認証局については米国ブラウザベンダに対して安全なものとして認めてもらえるよう、CA／ブラウザフォーラムに積極的に働きかけを行っている。
- 中国では、独自ブラウザや独自トラストリストを開発し、米国のウェブブラウザベンダに依存しない体制を構築中。

課題：CA／ブラウザフォーラムへの関与について検討が必要

- CA／ブラウザフォーラムのガイドラインを踏まえ、ブラウザベンダは認証局に対して、セキュリティの確保の観点から、
 - ・ポリシーの変更等への迅速な対応
 - ・認証局の運用体制等の透明性の確保
 - ・なりすまし防止等のための証明書発行における確認事項の厳格性の確保
- などを要求しており、認証局は一方向的に求められるそれらの要求に随時対応しなければならず、利用者にとっても短期間で証明書を切り替える必要があるなど、各種コストを要している。
- 法人名の日本語表記は海外の人には読めない、登記簿には英字表記は存在しないなど、日本独自の仕様がCA／ブラウザフォーラムに認められないことがある。そのため、日本の特殊な事情を表明していくことが求められる。
- CA／ブラウザフォーラムの運営に積極的に参画しているEUの活動を参考にしつつ、我が国としてもトラストリスト策定に関する検討や、CA／ブラウザフォーラムのガバナンスに戦略的に関与していくことが必要。

現状

- IoT機器の稼働状況などから大量のデータ(ビッグデータ)が蓄積され、AIによるデータ解析を活用することで、より高密度のデータの収集・蓄積・解析を通じて社会課題の解決につなげていくSociety5.0においては、その基盤としてモノから発信されるデータの正当性を確保することは極めて重要。
- 特に、重要IoT機器については、Society5.0を実現する上で、デバイスの製造段階からソフトウェアの更新、廃棄までの一連のライフサイクルにおいて「安全」であることが重要であり、PKI等による認証の仕組みを導入することが考えられる。

課題1:実装に当たって、機能的制約やコスト面の課題がある

- センサーなどの小さなIoT機器(チップ)にPKIの仕組みを導入することには機能的な制約がある。
- PKIの仕組みをIoT機器に導入するに当たって、費用対効果の観点から、そのコストについても考慮が必要。

課題2:認証単位等について更なる検討が必要

- モノの認証については、人や組織の認証と違い、様々な単位(機器ごとか、製造ロットごとか等)で行うことが考えられ、それぞれの利用実態に応じて柔軟に対応できる仕組みが必要である。
- また、IoT機器の廃棄に関して、データの出所を後で追跡や検証する際には検証用の鍵が必要となるため、廃棄の際の鍵の扱いなどについても検討が必要である。

現状

- 現在は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など一部の分野において、利用が進んでいる。
- 他方、タイムスタンプの有効性に関する制度的な裏付けがないため、民間の認定スキームでは企業の法務部門等で使用を躊躇するケースが存在するなど、上記以外の分野では十分に利用が広がっているとは言えない。
- また、電子帳簿保存法では、国税関係書類をスキャナ保存する場合にタイムスタンプの使用が義務付けられているが、e文書法においては、建築や医療など特定の分野におけるガイドラインにおいて記載されているのみなど、規定のレベルや有無が分野によってバラバラであり、結果として、タイムスタンプの利用の程度もまちまちである。

【主な使用例】

- ・ 国税関係書類：電子帳簿保存法施行規則において、日本データ通信協会が認定する事業者のタイムスタンプを規定
→ タイムスタンプの利用が一定程度普及
 - ・ 建築設計業務の設計図書：公益社団法人におけるガイドラインにおいて、日本データ通信協会が認定する事業者のタイムスタンプを規定
→ 中小の設計事務所に普及進まず
- ※ その他、多くの分野では具体的な規定なし

課題1:電子化の推進には、長期署名への対応が必要

- 電子署名の電子証明書の有効期間は5年間であり、電子署名のみでは長期的に真正性を検証できない。
- 長期にわたって保存が求められる文書、例えば、民間の契約書(住宅ローン最長35年)や建築士法に基づく設計図書の保存(15年)等について、タイムスタンプを用いた長期署名の枠組みが法的に整備されることで、利用者にとってより安心・安全なサービスの提供につながることを期待される。
- 日本公認会計士協会が発出している通達において、監査法人が上場企業の監査を行う際は原本で確認することが規定されており、監査が終了するまでは原本の破棄はできないという現状がある。その根本的な原因として、電子的に長期保存されたデータの信頼性が担保されていないということが考えられる。

課題2:廃業の際の対応策が未整備

- 現行の民間の認定スキームにおいては、タイムスタンプ事業者やタイムスタンプ事業者に電子証明書を発行している認証局の廃局・廃業時の対応策について、具体的な規定が存在しない。

課題3:国際的な相互承認のための公的枠組みが必要

- 民間による認定スキームのままでは、海外において日本のタイムスタンプの有効性を争う訴訟が起きた際、証拠として採用されにくくなるおそれがある。
- 日本のタイムスタンプが、国際的な枠組みにおいて信用のあるものだと認められれば、第三国において訴訟を行う場合でも、証拠として示しやすくなるため、EUを始め、各国と枠組みを構築することが求められる。

- 建築士法において、建築士の業務として作成した設計図書は、15年間保存しなければならない旨を規定。
 - e-文書法により、当該設計図書を電子保存することが可能となっているが、
 - ① 電子データの真正性を保存期間内にわたって保証する仕組みであるタイムスタンプについて法的な位置づけがない
 - ② タイムスタンプの利用について、民間団体のガイドラインで推奨されるにとどまっている
- 等の要因により、タイムスタンプの導入を躊躇し、電子化が十分に進んでいない。
- 中小の多くの設計事務所は電子的に作成した図面を紙で出力して保存している状況。



期待される効果

- タイムスタンプの制度化により、図面の作成から保存まで、安心して一貫したデジタル化が可能となり、業務の効率化と文書の保存コスト削減が実現。

現状

- eデリバリーは、送受信者の識別とデータの送受信日時の正確性、送受信データの完全性を保証するものであり、例えば、ドイツでは「De-Mail」サービスが提供されている(※)。「De-Mail」のユースケースとして、B2Cでは保険契約事項に関する連絡や株主総会に関する連絡等、B2Gでは不動産事業者の認可申請や商業登記申請等、C2Gでは住宅給付申請や税額の査定申請等が挙げられる。

(※) 2019年3月現在、1916組織及び約100万アカウントがeデリバリーを利用している。

- また、受信者・送信者個人が特定されるので、フィッシング詐欺やマルウェア配布を防止することにもつながると考えられる。

課題

- eデリバリーについては、国内においてそのニーズが顕在化していない。

検討事項1 人の正当性を確認できる仕組み(電子署名)

- リモート署名の電子署名法上の扱いについて、主務省庁において整理した上で、特定認証業務と認定認証業務に係る基準の具体化を進める。

検討事項2 組織の正当性を確認できる仕組み

- どのような枠組みでeシールに係るサービスが提供されれば、利用者が安心して利用できるか、制度化も視野に入れて検討を深めていく。
- ウェブサイト認証については、CA/ブラウザフォーラムのガバナンスに戦略的に関与していくことが必要。

検討事項3 IoT機器等のモノの正当性を確認できる仕組み

- コストや機能上の制約を踏まえ、どのような分野への適用が適当かを整理した上で、引き続き、仕組みの具体化について検討を進めていく。

検討事項4 データの存在証明・非改ざんの保証の仕組み(タイムスタンプ)

- タイムスタンプの普及が一部の分野を除き進んでいない原因を分析した上で、タイムスタンプの利用を社会全体に広げるための制度の在り方について、検討を深める。

検討事項5 データの送達等を保証する仕組み

- 現時点ではeデリバリーのニーズがなく、今後の我が国におけるトラストサービスの進展を踏まえつつ、引き続き検討を進める。

「未来投資戦略2019」(案) (令和元年6月5日「未来投資会議」資料)

- I. Society5.0の実現 1. デジタル市場のルール整備 (1)KPIの主な進捗状況 ii) データ流通の促進 ③ サイバーセキュリティの確保
- サイバー空間での自由で安心・安全なデータ流通を支える基盤として、データの改ざんや送信元のなりすまし等を防止する仕組み(トラストサービス)の在り方について、国際的な相互運用性の観点も踏まえ、**本年中を目途に結論を得て、速やかに制度化を目指す。**

「デジタル時代の新たなIT政策大綱」

(令和元年6月7日「高度情報通信ネットワーク社会推進戦略本部(第76回)・官民データ活用推進戦略会議(第7回) 合同会議」決定)

第2章. デジタル時代の新たなIT政策 2つめの柱 官民のデジタル化の推進 ②民間部門のデジタル化時代への対応の促進
～デジタル・トランスフォーメーションの推進による競争力強化～

- 71. デジタル手続法により官民の手続きについてデジタル化を徹底していく中で、民間における文書保存等についても一層のデジタル化が期待されている。安心・安全なデータ流通を支える基盤となる**トラストサービス**(データの存在証明・非改ざん性の確認を可能とするタイムスタンプや、企業や組織を対象とする認証の仕組みなど)**の活用のための制度の在り方を含め**、関係省庁間で連携し、法令に基づき民間企業等が行う文書保存等の一層のデジタル化に向けた取組について検討を行い、**令和元年度内に結論を得る。**

「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画」(令和元年6月14日 閣議決定)

第1部 世界最先端デジタル国家創造宣言 IV.国民生活で便益を実感できるデータ利活用 2信頼性向上のためのデータ流通ルール整備
(5)プラットフォームサービスの在り方を巡る議論

- 電子データの安全な長期保存を可能とするタイムスタンプをはじめ、インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する**トラストサービスについても**、EU等の動向も踏まえつつ**制度の在り方について検討を進める。**

- 信頼のある自由なデータ流通(Data Free Flow with Trust)は、これからの成長のエンジン。
- デジタル手続法により、行政手続のデジタル化が徹底。今後、**民間も含め社会全体として「紙からデジタルへ」を実現するためには**、データの信頼性を確保し、安心・安全なデータ流通を支える基盤が不可欠。具体的には、**送信元のなりすましやデータの改ざん等を防止する仕組み＝“トラストサービス”が必要**。
- さらに、**Society5.0においては、ヒトだけでなく、組織**(企業が発行する文書等)**やモノ**(IoT機器からのセンサー情報の発信等)**の正当性も確認できる包括的な仕組みが求められる**。
- トラストサービスの制度化により、様々な経済・社会活動のデジタル化が加速し、生産性の向上をもたらすことが期待される。

社会全体のデジタル化に向けて、トラストサービスの普及を推進

