資料６－２

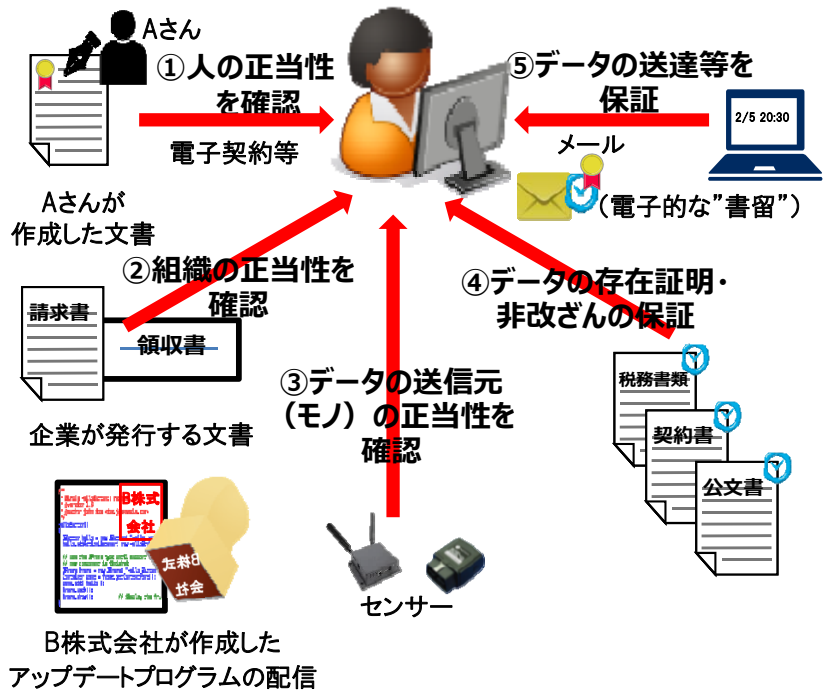
これまでのヒアリング等で示された課題

令和元年５月13日

トラストサービスに関する検討事項

- データの自由な流通(Data Free Flow with Trust)は、これからの成長のエンジン。
- デジタル手続法案により、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。

トラストサービスのイメージ



➤ 次のようなトラストサービスに関する**現状や制度的課題について、**EUにおけるeIDAS規則の制定等の動きもある中、**国際的な調和に配慮しつつ検討**

検討事項1 **人の正当性**を確認できる仕組み(リモート署名)

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、ウェブサイト認証)

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

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)

検討事項5 **データの送達等を保証**する仕組み(eデリバリー)

検討事項1　リモート署名について

検討事項

○　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を実現する上で、技術的・制度的な観点から、どのような課題が存在するか。

現状・課題

■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。

○　欧州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。

（※）電子署名法第3条：電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

検討事項1　リモート署名について

■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。

検討事項2－1　eシールについて

検討事項

○　我が国における組織を対象とする認証（eシール）について、どのようなユースケースが考えられ、制度的な観点から、どのような課題が存在するか。

現状・課題

■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。

(※)電子署名法では、自然人を対象として電子証明書の発行する認証業務を規定。

○　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法的枠組み（eシール）がない。

○　EUでは、eIDAS規則において、法人向け電子証明書が電子署名相当のものとして法的な効力が認められている。

検討事項2－1　eシールについて

■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（現時点における課題）

○　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。

（※）請求書や領収書等は、機械発行したものに対して自動的にeシールが付される運用が望まれるため、自然人による署名は馴染まない。法人を対象とした電子証明書は法人の確認だけで済むため、簡単に審査ができコストも低下することから、安く電子証明書を発行することが可能。

○　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（決済口座にある資金を用いた決済取引等）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、デジタル化による負担軽減や大幅なコスト削減が期待される。

検討事項２－１　eシールについて

■課題２：Society5.0に向けた対応が求められる（今後の課題）

○　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。

（※）コード署名を行うことで、正規のプログラムであること（悪意のある第三者が配布したプログラムではないこと）が確認できる。

○　例えば、自動車におけるOTA（Over The Air）によるアップデートが行われる際のコード署名の検証方法などが考えられる。

○　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すると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。

検討事項2－2　ウェブサイト認証について

検討事項

○　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、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いるが、我が国としてどのような対応を行うべきか。

現状・課題

■現状

○　利用者がウェブサイトを閲覧する際、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。

検討事項2－2　ウェブサイト認証について

■課題：CA／ブラウザフォーラムと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　モノの認証について

検討事項

○　IoT時代において、モノの認証について、どのようなユースケースが考えられ、技術的・制度的な観点から、どのような課題が存在するか。

現状・課題

■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する必要がある。

検討事項3　モノの認証について

■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（機器単位か、システム単位か、工場単位かなど）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。

検討事項4　タイムスタンプについて

検討事項

○　国際的な相互運用性やトラストサービスを長期的に確保する観点から、我が国におけるタイムスタンプの制度の在り方を検討する上で、どのような課題が存在するか。

現状・課題

■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、利用が拡大している。

○　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、電子契約の促進の妨げになっている。

■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）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が期待される。

○　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。

検討事項4　タイムスタンプについて

■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。

（参考事例）タイムスタンプのユースケースの例＜設計図書の保存＞

○　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。

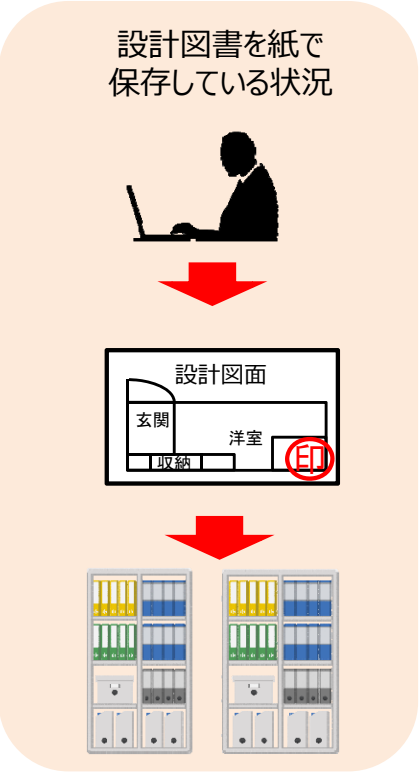
○　e-文書法により、当該設計図書を電子保存することが可能となっているが、

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。

検討事項5　eデリバリーについて

検討事項

○　我が国において、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（eデリバリー）に対するニーズは具体的にどのようなものが考えられ、どのような課題が存在するか。

現状・課題

■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。

■課題

○　eデリバリーは、電子署名、eシール、タイムスタンプの仕組みを組み合わせたものであることから、それらの個々のトラストサービスの進展に応じて、ユースケースの具体化が必要と考えられる。