デジタル庁

デジタル改革に伴う

新分野のトラスト確保に向けたデータ証拠力の調査研究

最終報告書

2023 年 03 月 31 日

目次

エグゼクティブサマリ 2
1. 動画・画像等のデータ証拠力の現状分析 (公共・民間分野) 4
1.1 国内外の先行調査/事例の整理・類型化 4
1.2 事例を基にしたリスクの類型化 18
2. ステークホルダーからのニーズ等実態調査 20
2.1 有識者へのインタビュー 20
2.2 過去トラスト案件で整理した、トラストニーズのある業界からの深堀 22
3. ニーズの分析・分類化、課題整理 25
3.1 トラストにおける脅威/不正の類型とトラスト確保手法の整理 25
3.2 電子署名法の実地調査のデジタル化を想定した、フレームワークの検証 28
3.3 トラストに係る社会的影響の調査 34
4. ロードマップの検討 (長期・中期・短期) 36
4.1 目指すべき姿と実現に向けた課題・ネクストアクションの整理 37
4.2 ロードマップの策定 38

エグゼクティブサマリ

調査研究の背景と実施内容

わが国では、画像生成 AI で作成された災害に係る真実でない画像(いわゆる「フェイク画像」)が新たな社会課題となる等、データによるデジタル改革において、適切なデータ流通やデータ利活用を担保するトラスト基盤の必要性が高まっている。デジタル庁 (トラストを確保した DX 推進 SWG) では、トラスト確保に対するニーズ等の実態調査を行い、トラスト確保に必要な取組や課題について検討整理を進めてきた。SWG 報告書では、トピック別に検討をすすめることが提起され、「動画・画像データ、機器、時間等のトラストに係るニーズや課題」については、情報収集・調査検討から開始すべきとされた。加えて、「デジタル社会の実現に向けた重点計画」は、実態調査の中で挙がった課題等の対処法について、「使いやすいサービス」とするために、マルチステークホルダーでの議論を推奨している。

そのような中、本調査研究では国内外のドローン・カメラや赤外線センサーによる動画・画像、重要な IoT 機器、時刻、位置のデータ証拠力(以下、「動画・画像等のデータ証拠力」という)について、国内外の先行調査研究や具体的な対応事例の現状分析を行い、その結果明らかとなった脅威や不正等の可能性に係る課題を各種の社会的ニーズを中心に深掘りすることで、その考察から今後の論点やトラスト確保に資する具体的な施策等の在り方を整理した。具体的には、動画・画像等のデータ証拠力の現状分析(公共・民間分野)、ステークホルダーからのニーズ等実態調査、ニーズの分析・分類化、課題の整理、ロードマップの検討(短期・中期・長期)を実施した。本エグゼクティブサマリでは、それぞれの要約を記載する。

動画・画像等のデータ証拠力の現状分析(公共・民間分野)

動画・画像データを用いたデジタル化における証拠力確保の手法はプラットフォームによる作成者情報や時刻情報の管理が主要であり、第三者証明による厳格な証拠力の管理はデータ流通の事例で一部確認した。

アナログ規制のデジタル化で想定された手法の類型で動画・画像データの活用余地があるのは IoT 関連技術・オンライン会議・紙媒体の電子化技術の 3 種類である。

上記デジタル化の類型に近い海外事例でも動画・画像データを用いたものはあるが、証拠力の担保のためには、データ作成・更新時の ID 管理やメタデータの管理といった一般的な PF の機能で実装した事例が多数であった。それぞれの海外事例におけるデータフローとリスクを整理したところ、大きくデータの作成/送信/格納・利用/流通の 4 段階で整理でき、それぞれに改ざん・偽造リスクが存在したことを確認した。

多くの海外事例ではデータの作成/送信/格納・利用までの機能実装。これらのケースでは、単一 PF 上では、データ作成・更新時の ID やメタデータの管理や一般的なサイバーセキュリティによって、改ざん・偽造リスクを抑制していた。一方、データ流通までを見越した Catena-X の事例では電子署名やタイムスタンプを用いた証拠力担保が実装されているが、すべてのデータへの適用義務は未実施であった。

ステークホルダーからのニーズ等実態調査

専門家の視点から見ても、動画・画像データの証拠力として第三者証明による厳格な証拠力のニーズは現時点では未確認であるが、今後事業者側のニーズが高まる可能性があることを、ヒアリングを通して確認した。

弁護士のエキスパート曰く、動画・画像データを用いたデジタル化でトラストが求められるケースは訴訟での活用等。訴訟のケースでも第三者証明による厳格な証拠力のニーズは現時点では未確認であった。動画・画像データ

を利用したデジタル化でのトラスト確保のニーズを探すよりも、トラストが必要なデジタル化において、動画・画像データの利活用余地がないかのニーズを探す方が、筋が良いとの示唆もいただいた。

トラストサービス事業者曰く、電子署名・タイムスタンプが動画・画像データへ使用されたケースは、現時点では未確認であった。今後動画・画像の証拠力が重要になるユースケースが顕在化する可能性はあり、電子署名・タイムスタンプ・位置情報の実装も有り得る。その場合には、第三者機関による認証の仕組みが必須であるとのこと。

ニーズの分析・分類化、課題の整理

デジタル化におけるデータの改ざん・偽造リスクとリスクに対するトラスト確保手法を、今後も利用可能な形で整理した。特に、データの作成時と流通時にトラストニーズがあり、それぞれの領域で効率的なトラスト確保手法の違いを明確にした。今回の整理を用いることで、今後の行政主導でのデジタル化において、トラスト確保の要否と確保のための手法を判断可能な見立てである。送信・格納/利用にも改ざん・偽造のリスクは存在するが、通信路とデータベース・プラットフォームへのセキュリティを担保することで対応可能であることを明確にした。また、単一 PF と複数 PF では ID 管理や統一的なトラスト・セキュリティの適用の容易性に差が存在することがわかった。単一 PF では PF 上での ID・メタデータの管理でトラストを確保できる一方、複数 PF では電子署名やタイムスタンプといったトラストサービスの利用が推奨されうる見立てである。

ロードマップの検討(長期・中期・短期)

アナログ規制のデジタル化と国内/国際的データ流通という目指すべき姿に向け、大きく 3 ステップのロードマップでの推進を想定している。

短期的には、アナログ規制のデジタル化に向けた、トラスト確保の要件定義及び産官学共同等を含むトラスト技術提供体制の検討、及びアナログ規制見直しとのチーム連携を実施する必要がある認識である。

中期的には、国内でのデータ流通に向けた特定の業界での垂直統合的 PF や省庁内での統一的な PF の構築を行うべきだと考えている。

長期的には、国際的データ連携を視野に入れた、トラスト確保 / プライバシー・データ主権保護手法、他国制度を踏まえた法制度を検討するべきだと考えている。

1. 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

動画・画像等のデータ証拠力の現状分析 (公共・民間分野)の取り組みアプローチ

本調査研究では、調査対象について貴庁とディスカッションしつつスコープを定めた。まず、動画・画像へのトラスト活用は、デジタル臨調に関わるアナログ規制の見直しに関わるデジタル化の優先度が高いことをヒアリングした。デジタル化ニーズ、トラストニーズそれぞれが存在し、デジタル化ニーズは「各事業者の認可を実施する上で必要となっているアナログな現地調査業務に関して、動画や画像を使ったデジタルな手法で簡略化したい(※デジタル臨調にてデジタル化の対象となる具体的な現地調査業務が選定される)」という内容であり、トラストニーズは「現地調査作業のデジタル化はリモートが主体となり、データ真正性担保の観点でトラスト技術の導入が見込まれる」という内容であった。また、ヒトが現地確認していた部分を、トラストが確保された動画・画像による確認手法で置き換えられないか? という見立てがあったことから、データ取得担当者の ID 確認とは別に、実際に取得された動画や画像の真正性をトラストで別途担保する必要があるという認識で調査をする方針であった。

調査の計画として、各産業における動画・画像を使ったデータ活用&トラスト活用のユースケースを幅広に調査以下両面で調査を進めていくことと、今回の主眼である「人による確認作業を動画・画像で代替しているもの」について、トラストの利活用方法について深掘りを両面で進めていくことを合意した。具体的には、以下の 4 つの方針で本項目の調査を実施した。

- 調査対象を動画・画像のトラスト確保に絞り、デジタル臨調テーマを優先的にニーズの深掘りを進める
- 幅広調査は臨調テーマを類型化し、類型別に類似ユースケースはないか? を補足的にリストアップ
- 関心度の高い事例についてデータフローと改ざん・偽造リスクを整理し、トラストの対象を明確化
- 調査した事例より、トラストに係るリスク（脅威や不正内容）を類型化

1.1 国内外の先行調査/事例の整理・類型化

アナログ規制における動画・画像技術の利用余地

デジタル臨調テーマである、アナログ規制のデジタル化においては 7 つのデジタル化類型が存在するが、その中での動画・画像データの利用余地は、IoT 関連技術、オンライン会議システム、紙媒体の電子化技術の大きく 3 つに集約されると分析した。そのため、これら 3 つの類型において海外の先行事例がないかどうかを調査した。

関連する海外先行事例の調査

海外では IoT 関連技術による動画・画像データの活用が進展していることが分かった。特に関心度の高い事例として、建設業におけるシンガポールの事例で、建物のひび割れや腐食などの欠陥を自動で特定するシステム (ドローン・AI)が事例や、金融業、保険業におけるインドの事例で、ATM 取引の監視をネットワークカメラを用いて実施している事例、製造業における EU の事例で、自動車産業ステークホルダー間の情報共有プラットフォームの構築 (ドローン・センサー)の事例も確認した。後段にて、これらの事例について、深堀調査・データフローと改ざん・偽造リスクを分析した結果を示す。

デジタル化手法	業界名	国名	事例概要
IoT 関連技術 A	建設業	シンガポール	建物のひび割れや腐食などの欠陥を自動で特定するシステム (ドローン・AI) a
			プレキャスト部材の状況確認や設計図の展開 (3Dモデリング技術)
		インド	送電線・鉄塔点検 (ドローン・AI)
			工場での品質検査の自動化 (AI・5G遠隔ロボット)
		スコットランド	没入型3D環境での建設現場の監視・点検 (モバイル技術・AI)
		ドイツ	未知の建物探索やモニタリング (ドローン・3D点群データ)
		スペイン	危険地域における建設物・インフラ保全点検 (カメラ・センサー・3D点群データ)
		イタリア	産業プラントやクレーン等構造物の点検(ドロ ーン)
		英国	遺産として保全されている構造物の検査・近接点検 (ドローン・センサー)
		米国	建物の外観の定期点検 (ドローン)
	エネルギー業 (電気、ガス、水道 等)	シンガポール	ソーラーパネル使用時期の最適化と点検の自動化 (BIM・AIソフトウェア)
		英国	電力用鉄塔点検 (ドローン・センサー・AI)
		エストニア	配電線点検 (ドローン・AI)
		米国	アナリティクス、センサー、運用データを組み合わせ、発電所の故障時期を予測するサービスの提供 (センサー)
	エネルギー業 (電気、ガス、水道 等) 農林水産業	シンガポール	農林水産業やエネルギー業向けの土地調査・環境管理プラットフォーム (ドローン)
	農林水産業	シンガポール	農業研究に向けたデータ収集を自動化するシステム (ドローン・センサー)
			作物への栄養投与や保管・収穫など農作業の自動化ツール (AI)
		米国	空中マッピングや肥料・農薬散布の自動化による農作業の効率化 (ドローン)
			作物と土壌の健康状態の監視 (ドローン)

デジタル化手法	業界名	国名	事例概要	
IoT関連技術 A	行政サービス	シンガポール	貯水池での違法な水上活動 (ドローン・アルゴリズム)	
			公共イベント監視 (ドローン)	
			国有施設点検 (ドローン・AI)	
			交通監視のためのビデオ分析	
		インド	鉄道の橋梁・線路点検 (ドローン)	
			受刑者監視 (AI)	
		オーストラリア	橋の鉄鋼と塗装点検 (ロボット・AI)	
			淡水及び沿岸地域の水質点検 (センサー)	
			駅・線路点検 (ドローン)	
		英国	交通事故の検知 (AI)	
			運転中の携帯等違反検知 (AI)	
		エストニア	警察の巡回の配置 (AI)	
			違法駐車の検知 (AI)	
		UAE	交通違反の検知、巡回配置 (AI)	
			トンネル点検 (ドローン・AI)	
	業界横断	オーストラリア	作業員の手袋未着用等のチェック (AI)	
		英国	コロナ禍のマスク着用等のチェック (AI)	
	鉱業、採石業、砂利採取業	EU	ヨーロッパ全土の鉱山現場の監視と分析のために鉱山の高解像度データを収集するAIプラットフォーム (衛星・ドローン・現場センサー)	
	金融業、保険業	インド	ATM取引の監視 (ネットワークカメラ)	b
	製造業	シンガポール	ビデオと画像を用いたリモート産業機械検査	
		EU	自動車産業ステークホルダー間の情報共有プラットフォームの構築 (ドローン・センサー)	c
			製油所・橋・トンネル等インフラ点検 (ドローン)	

オンライン会議や紙の電子化技術によって動画・画像データを活用する事例も存在する。特に関心度の高い事例として、行政サービスにおける米国の事例で、オンライン司法試験実施時の替え玉受験の防止 (e-learning)事例や、業界横断で使用されるサービスにおける米国の事例で、オンライン公証(オンライン会議)の事例を確認した。後段にて、これらの事例について、深堀調査・データフローと改ざん・偽造リスクを分析した結果を示す。

デジタル化手法	業界名	国名	事例概要	
オンライン会議等 B	医療・福祉	シンガポール	遠隔医療 (オンライン会議)	
		インド	遠隔医療 (オンライン会議)	
		オーストラリア	遠隔医療 (オンライン会議)	
		エストニア	遠隔医療 (オンライン会議)	
		UAE	遠隔医療 (オンライン会議)	
		バーレーン	遠隔医療 (オンライン会議)	
		英国	遠隔服薬サポート (オンライン会議)	
		EU	製薬企業や病院向け倫理規定監査の遠隔化 (VR)	
	行政サービス	インド	労働者の技能訓練 (e-learning)	
		バーレーン	警官訓練 (e-learning)	
		英国	仮想現場による警官訓練 (VR)	
		米国	オンライン司法試験実施時の替え玉受験の防止 (e-learning)	d
	業界横断	スペイン	オンライン公証 (オンライン会議)	
		米国	オンライン公証 (オンライン会議)	e
	卸売業、小売業	米国	360度の仮想体験を通した遠隔監査 (VRヘッドセット)	
紙媒体の電子化技術 C	行政サービス	台湾	税務申告における領収書の偽造検知 (深層学習モデル)	

シンガポールにおけるドローン活用事例

シンガポールでは、「施設等の破損/不備の確認」にて、ドローンを活用したデジタル化が進展している。シンガポールの建物検査とデジタル化に関しての概況としては、シンガポールでは過去 5 年で建物検査に関する規制を厳格化している。災害発生の可能性が低く、インフラや住宅等、建物の老朽化がかねてより進行していた。そのような背景の中、2018 年以降、政府機関である HDB(住宅開発庁)と BCA(建築建設庁)が建物検査に関する規制を段階的に執行した。なお、HDB が公共住宅、BCA がそれ以外の全ての建物の規制を担当している。2022 年から PFI 制度(定期的な外観検査制度)が施行され、築 20 年以上・高さ 13m 以上の建物は、7 年ごとに全ての外観の検査を要求している。

また、安全かつ効率的に全ての外観の検査を実現すべく、政府主導でドローン活用によるデジタル化を推進している。2017 年に HDB と BCA が共同で、ドローン検査システムを開発する企業向けにオープンイノベーションの取組を開始した。また、2020 年に官民共同で建物検査でのドローン活用に関するガイドラインを策定。検査報告書のテンプレートとドローン業者の資格基準を公表した。

上記のデジタル化ニーズを捉え、Garuda Robotics は施設等の点検を起点に、ドローン等を活用したデジタル化を主導している。Garuda Robotics はドローン等を活用し、施設等の点検を中心にデジタル化を推進している。

会社概要

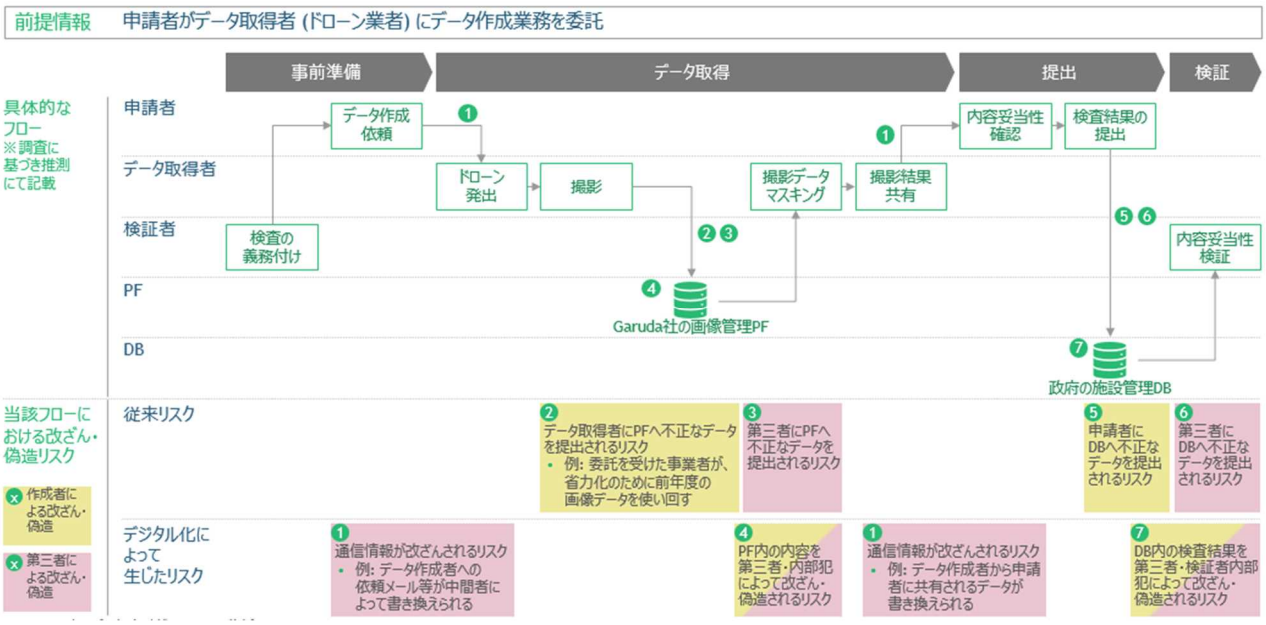
会社名	• Garuda Robotics
設立年	• 2013年
事業展開国	• シンガポール
事業概要	• 自律型ドローンシステムを活用したデジタル化
デジタル化領域	• 施設等の点検 (Facilities 4.0) • 人の監視 (Safe Distance) • 農作業の効率化 (Plantation 4.0) • 救急対応 (Garuda Responder)
対象業界	• 建設業 • 農林水産業 • エネルギー業 • 情報通信業 • 運輸業、郵便業 • 鉱業、採石業、砂利採取業 • 行政サービス • 医療、福祉
提供ソリューション	• 3Dマッピング • 検査レポート • 保険調査 • フレアスタック調査 • 農作物健康状態マッピング • タワー検査 • 施設点検 • ビデオ撮影

イメージ

施設等の点検のデジタル化
- AIを活用した自社プラットフォーム"Facilities 4.0"
- ドローンに、ひびの自動検知機能"FaultFinder AI"を搭載

人の監視のデジタル化
- 混雑度合をAIで判断・可視化する "SafeDistance"

Garuda Robotics における、ドローンによる施設点検のフローを、フローにおける改ざん・偽造リスクとともに以下のように整理した。



Garuda Robotics の事例では、基本的なセキュリティ対策は実施されているものの、当局主導の対応を含め、動画・画像にユニークなトラスト確保手法は未実施であることを確認した。

発生し得る改ざん・偽造リスク		データ証拠力の担保手法	
✕作成者による改ざん・偽造 ✕第三者による改ざん・偽造	デジタル化に特有のリスク	技術的な対応 (含む、トラストサービス)	その他の対応 (含む、法整備)
① 通信路で依頼情報が改ざんされるリスク • 例: データ作成者への依頼メール等が中間者によって書き換えられる	✓	• 当局からの対策要請は無し • Garuda Roboticsでは自助努力としてのサイバーセキュリティ強化を実施 - ISO27001の認証取得 - ネットワークにおけるVPNの活用	• 従来より不正アクセスへの罰則を規定 • (当局による内容確認・検証は未実施)
② データ取得者にPFへ不正なデータを提出されるリスク • 例: 委託を受けた事業者が、省力化のために前年度の画像データを使いまわす		• 当局からの対策要請は無し (当局はリスク要素とは認識) - あくまで従来から存在するリスクであり、従来より法整備 (虚偽申請への処罰等) で対応 - 技術的な方法での対策の難易度・導入コストが高い	• 従来より虚偽申請・不正アクセスへの罰則を規定 • 検査資格者が内容確認・検証・最終署名を実施 - 当局から委託された検査資格者が、内容の妥当性に対する最終責任を負う - 当局は他業務との兼ね合いで、簡単な内容確認のみ実施
③ 第三者にPFへ不正なデータを提出されるリスク • 例: 業務を阻害したい他のドローン業者が、委託業者になりすまして別の画像データにすり替える		• 当局からの対策要請は無し - あくまで従来から存在するリスクであり、従来より法整備 (なりすましへの処罰等) で対応	
④ PF内の内容を第三者・内部犯によって改ざん・偽造されるリスク • 例: 業務を阻害したい内部犯がPF内のデータを改ざんする	✓	• 当局として気にしている内部犯によるリスクに対し、サイバーセキュリティを強化することでDB上のトラストを一定確保 - eDelivery/電子署名/タイムスタンプを活用 - 外部からのDBへのアクセスや改ざんは非常に困難と想定	
⑤ 申請者にDBへ不正なデータを提出されるリスク • 例: 画像データを修正した上でアップロード (設備のヒビ等を画像修正する 等) • 例: 類似施設で取得した、検査を通過できる画像データに差し替える		• ② と同様	
⑥ 第三者にPFへ不正なデータを提出されるリスク • 例: 競合他社が申請者になりすまして、問題のある画像データにすり替える		• ③ と同様	
⑦ DB内の検査結果を第三者・検査者内部犯によって改ざん・偽造されるリスク • 例: 業務を阻害したい内部犯がDB内のデータを改ざんする	✓	• 当局として気にしている内部犯によるリスクに対し、サイバーセキュリティを強化することでDB上のトラストを一定確保 - タイムスタンプ等を活用 - 当局規制により外部からのDBへのアクセスや改ざんは非常に困難と想定	• 従来より第三者の不正アクセスには罰則を規定 • 建物崩壊時に担当した検査資格者への罰則を規定

インドにおける監視カメラ活用事例

インドでは、ATM 取引へのセキュリティ対応として政府主導で監視カメラの活用を推進している。インドの ATM 取引と監視カメラ活用に関する概況としては、インドでは 15 年前に ATM が普及して以降、ATM 絡みのセキュリティ問題が顕在化した。例えば、ATM 上で暗証番号を盗撮・スキミングする技術が存在し、カードがハッキングされる事案が多発した事例である。

こういった概況を踏まえ、政府・当局間で対策を議論したところ、ATM のセキュリティ問題に対処すべく、政府主導で監視カメラを活用した取組を推進する方針とした。政府から銀行へ、ATM への監視カメラ設置を含むメカニズムの導入を義務付け、セキュリティ対策の不備に対しては罰則を規定政府主導で銀行・ATM 管理事業者・監視カメラ業者・通信事業者からなるエコシステムを構築し、補助金付与により参入を促進した。また、エンドユーザーである顧客に対して、ATM のセキュリティ対策やメカニズムについての教育を展開した。

上記のデジタル化ニーズを捉え、Airtel は ATM 取引の監視においてネットワークカメラを活用した映像管理ソリューションを提供した。Airtel はネットワークカメラを用いた映像管理ソリューションを提供している。

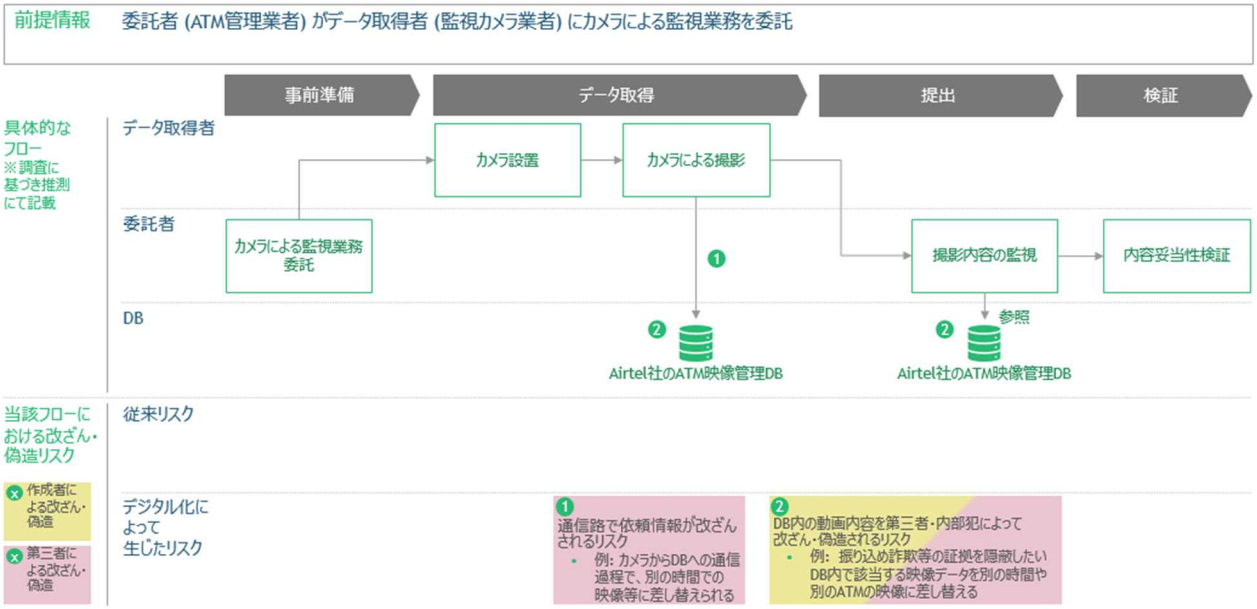
会社概要

会社名	• Bharti Airtel
設立年	• 1995年
事業展開国	• インド等18か国
事業概要	• 通信ネットワークや多数のIoTソリューションを展開 • ネットワークカメラを用いた映像管理ソリューションを提供しており、セキュリティ文脈で進展しているユースケースに該当 • 映像管理ソリューションをATMの監視等に活用

イメージ

- ネットワークカメラで撮影された映像がクラウド上にアップロード
- 利用者は管理DBから映像を確認

Airtel における、ネットワークカメラによる ATM 取引監視のフローを、フローにおける改ざん・偽造リスクとともに以下のように整理した。



Airtel の事例でも、当局からの技術的な対応要請はなく、動画・画像にユニークなトラスト確保手法は未実施であることを確認した。

EU における Catena-X によるデータ流通・利活用事例

EU では SDGs の実現のためのデータ共有/利活用による循環型経済を形成する動きが進展している。循環型経済と GAIA-X に関する概況としては、循環型経済は SDGs の実現に向けた有効な手段の一つとして捉えられている。それは、資源枯渇や環境破壊が経済活動の脅威となりつつある現在において、資源を消費して使わなくなったものを廃棄するだけの経済は成立しないということと、今後の生産・消費活動、国や企業の成長戦略の中には、資源や廃棄物の再利用、再活用を組み込む必要があることと、循環型経済はこれまで環境問題の課題解決策だったリサイクルやリユースを、経済発展や産業拡大に活かした経済の形であるということに起因している。

また、EU 規模でのデータ共有/利活用のためのインフラ構築の構想として GAIA-X があり、循環型経済へ貢献することが狙いである。2019 年、EU 規模でのデータ共有やデータ利活用を支援するインフラ構築構想として GAIA-X がドイツ・フランス主導で発表されたが、これは製品サービスシステムのライフサイクル全体でのトレーサビリティを確保することにより循環経済へ貢献することや、ユーザーから発生するさまざまなデータを産業機構全体で共有し、運用・保守サービス水準の向上を図ることなどが狙いである。

そのため産業別の各プロジェクトでより具体構築が進められており、ドイツ主導ですすめられている自動車産業のプロジェクト Catena-X が、現時点で最も大きなイニシアティブである。Catena-X は動画・画像データや IoT 機器の活用が見られる先進的な情報共有プラットフォームとして注目を集めている。

事例概要

事例概要

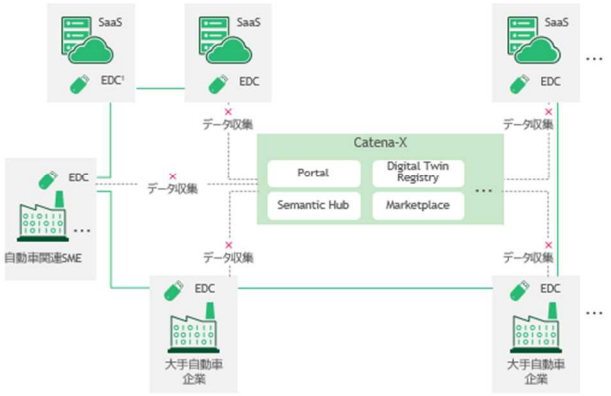
- Catena-Xはドイツ等の自動車業界ステークホルダーによる情報共有プラットフォーム
  - 動画・画像データやIoT機器の活用も見られるプラットフォームであり、一定のトラスト担保を実現
- 自動車メーカー・部品サプライヤ・ソフトウェアプロバイダー・販売業者が参加
  - SAP・シーメンス等のソフトウェアプロバイダーが構築を主導しており、行政の関与は限定的
  - (Catena-Xのベースである GAIA-Xにおいて、行政が法規制・財源面の関与を実施)
  - 現時点での主なデータ入力・活用者は自動車メーカー・部品サプライヤであり、消費者のデータ活用は検討中
- 自動車メーカー・部品サプライヤ・ソフトウェアプロバイダーが投資・運営を実施
- 2023年末の実用化に向け現在テスト中の段階

提唱している代表的なユースケース

- Traceability 以降で詳述
- Circular Economy
- CO2/ESG Monitoring
- Demand/Capacity management
- Online control/Simulation
- MaaS
- Modular Production
- Live Quality Loops
- Behavior Digital Twin
- Business Partner Management

イメージ

- Catena-XはGAIA-Xに準拠したオープンプラットフォームで、自動車業界のステークホルダーに対しバリューチェーン全体に関するデータを提供・流通



Source: 各種公開記事、エキスパートインタビュー
1. Eclipse Dataspace Connectorの略。IDS (International Data Spaces)のデータスペース標準やGAIA-Xのインフラストラクチャに基づいたテクノロジーの実装プロジェクト及びその実装形態

23

Catena-X では、ESG 調達文脈で活用が進む動画・画像データと IoT 機器に対し、一定のトラストを担保している。

動画・画像データの活用が見られるユースケース

- Traceability (トレーサビリティ)
  - ドローンやモバイル端末で撮影およびリモート監査時にオンライン会議システムで投影した採掘現場や工場内の動画・画像データを活用
  - 原料の採掘から製品のリサイクルに至るまで一連のサプライチェーンにおける、原材料の使用状況や労働環境を追跡してプラットフォーム上に可視化し、ESG観点での確認を実施
    - 採掘の進度や産業廃棄物の排出状況、リサイクル用電池の保管方法等、環境面でのチェックを実施
    - 児童労働の有無や労働環境の安全性等、社会・倫理面でのチェックも実施
    - その他として、現場に不要な機材が設置されていないかのチェックも実施

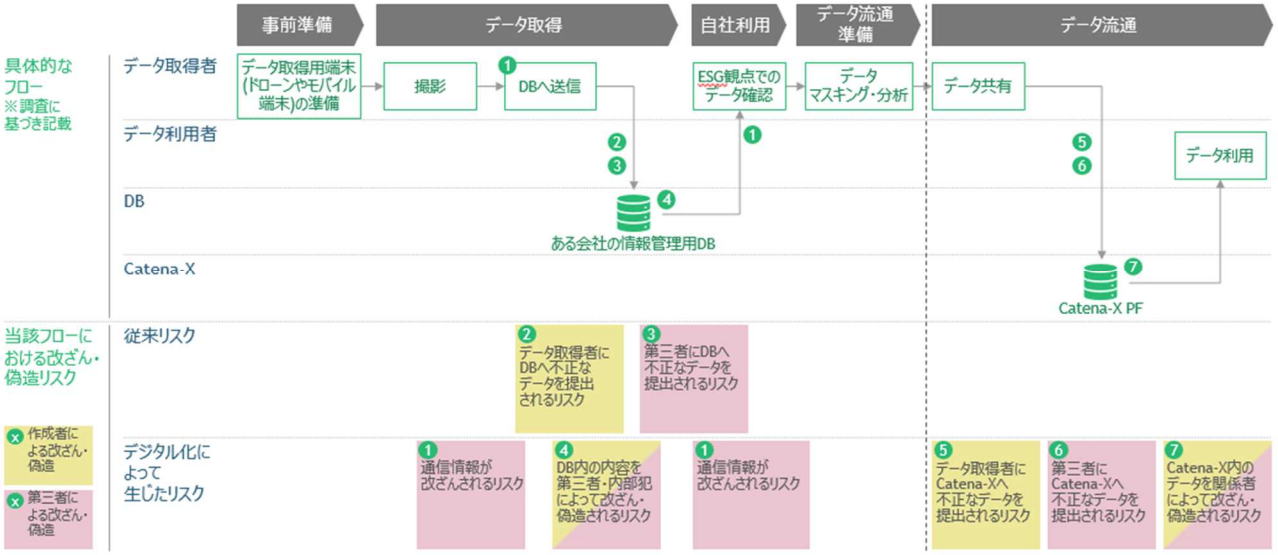
動画・画像データに対するトラスト担保の仕組み

- AIによる動画・画像の異常・偽造検知
  - データ取得者・申請者に不正なデータを提出されるリスク (工場内画像の産業廃棄物排出部分をフォトショップで削除してからデータを提出される等) に対応
- 動画・画像へのタイムスタンプ・電子署名・位置情報の付与
  - データ取得者・申請者に不正なデータを提出されるリスク (児童労働が行われていない類似施設や別の時間のデータを提出される等) に対応

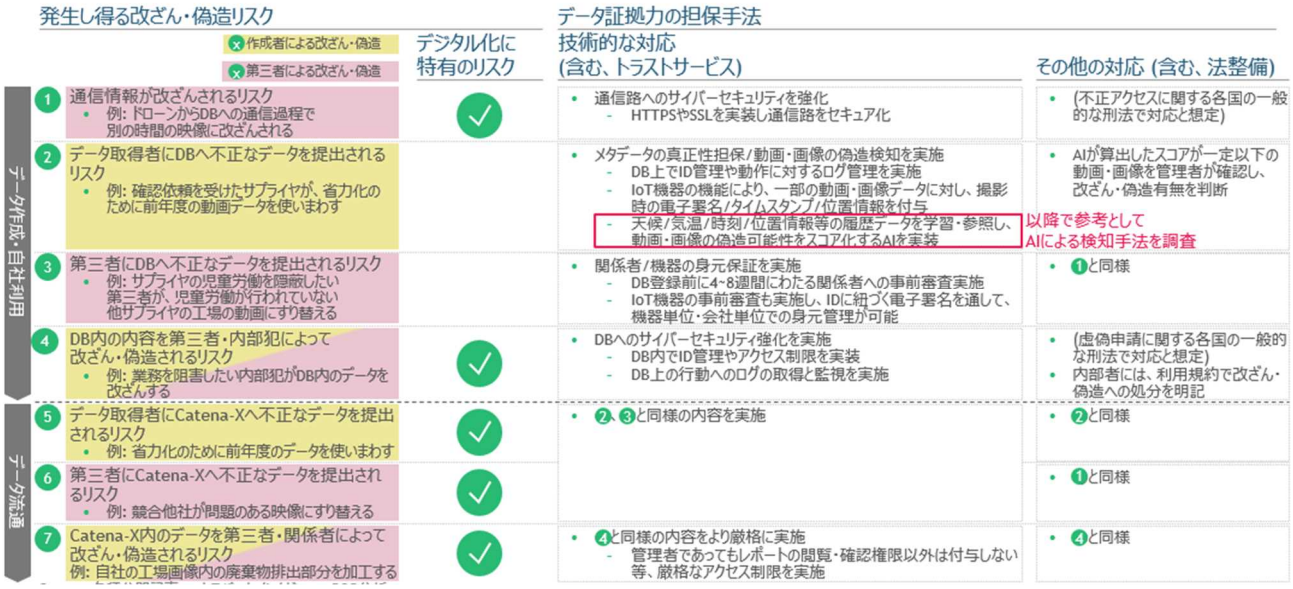
IoT機器のID管理の仕組み

- 事前登録時に機器ごとにIDが与えられ、IDに紐づく形で電子署名が付与
  - 身元不明の機器から不正な情報が提出されるリスクに対応
- IDの中に保有元を示す数字が含まれ、機器を保有している会社の特定でき、会社単位での管理も可能

Catena-X における、ESG 観点でのデータ確認及びデータ流通のフローを、フローにおける改ざん・偽造リスクとともに以下のように整理した。Catena-X の事例ではデータの 2 次・3 次利用に向けたデータ流通を実施しており、そこが他の事例との大きな差分である認識である。



データ流通段階のリスクは流通前と大きく変わらず、流通前と同様の対応を一部より厳格に実施することでトラストを担保していることを確認した。



また、Catena-X の事例では、不正な動画・画像データ自体への対応として、天候/気温/時刻/位置情報等の履歴データを学習・参照し、動画・画像の偽造可能性をスコア化する AI を実装していた。

参考までだが、海外では人の顔の動きに着目したフェイク動画・画像検知手法の開発が進展しており、いくつかの技術が研究・開発されている。我々でもいくつかの手法についての概要とその制度を調査したので、以下に記載する。

手法名 (開発者例)	手法概要	精度
色彩の境界線検知 (マイクロソフト)	• ディープフェイクで発生する、人の目では判読不能なレベルの顔の色あせ・グレースケールの境界線を検出し、動画・画像の信頼度スコアをリアルタイムで算出 • アメリカ大統領選挙演説動画の政治的印象操作の有無を見抜く用途等で活用	不明
心拍信号検知 (インテル)	• 顔から発する心拍の生体信号 (PPG 信号) や心拍による肌の色の微妙な違いを抽出し、時間的・空間的整合性を調査 • 人の顔・感情表現に関する複数の 3D データベースを学習させ、フェイクの可能性を判断 • 映画における映像加工や政治家演説の印象操作を見抜く用途等で活用	97.3%
発声における音素・視覚の不一致検知 (スタンフォード大)	• 発声時の口の形状と発声された音素の不一致を検出 • 音声トラックから自動的に音素を生成できる API ツールや、発声時の口の形状や音素を抽出したデータベースを活用 • 音声のトランスクリプトを入力するだけで顔の動きを含めて映像編集が可能な、リップシンク技術を用いた高度なディープフェイクツールの悪用防止策として開発	~93.4%
顔の動作・表情解析 (ケンブリッジ大)	• 動画中の表情・顔・頭の動きを追跡し、顔のランドマーク検出・頭の姿勢や視線の推定・顔の動きの認識をリアルタイムで実施 • 各個人の特定の行動の存在と強さを抽出して学習	不明
目の動作検知 (アルバニー大)	• 開眼時と閉眼時の目の動き・瞬き等の生理的信号を検出し、データセットと照合 • 再帰的ニューラルネットワーク (RNN) と畳み込みニューラルネットワーク (CNN) という 2 つの深層学習モデルを活用し、特徴量の抽出と時間的シーケンス分析を実施	~97.0%

これらの調査からわかったことは、現在主流のフェイク動画・画像対策手法は人の顔の動きに着目しているため、本人確認を行うケース (例:フェイク画像を使ったオンライン試験でのなりすましの抑止) 等には使える可能性があることである。また、今回の文脈とは離れるが、政治家等の発言の偽装を見抜くケースでは活用可能な見立てである。一方、ドローンによる建物検査等対象が人以外のケースや、画像を用いているケースには使えない見込みであり、こうしたケースでは、動画・画像の真正性を見抜くのではなく、身元保証等別の方法でのトラスト確保が必要な認識である。

また、顔写真以外だと、AI が生成した画像への検知手法を開発済であり、我々の調査でもいくつか確認した。

AIが生成した画像の検知

- 画像生成AI「Stable Diffusion」によって生成された画像であれば検知が容易であり、フェイクである可能性を算出可能
- 人の顔以外 (災害現場等) の生成画像の検知も可能

生成・偽造された顔写真の検知

- 顔写真の検知に関しては、フェイク画像の特徴量を深層学習させる手法の他に、独自に生成した疑似フェイク画像を学習させる、より高精度な手法も存在
- 更に、人物の画像と同一人物の色・周波数・サイズをわずかに変更した画像とブレンドした画像を疑似フェイク画像として活用することで、最高精度の検出性能を実現

アメリカにおける e-learning 活用事例

アメリカでは、 e-learning を活用した「資格試験のオンラインでの実施」が普及している。アメリカの資格試験のオンライン化に関しての概況としては、2020 年 10 月にカリフォルニア州を含む 18 の州で司法試験をリモートで開催した (全受験者がリモート受験)。これは、コロナ禍において、受験生/監視官等の健康を守り、安全に試験を実施するための措置であったが、各受験生が自宅から受験を行う環境下においても不正が行われないようなオペレーションが必要となった。そこで、PC で試験内容に関する調べ物や、外部とのコミュニケーションを行うことを防ぐ仕組みや本人以外によるなりすまして受験を防ぐ仕組みを導入した。

上記のデジタル化ニーズを捉え、ExamSOFT by Turnitin は高度な不正対策を備えたオンライン試験を実現している。Turnitin では e-learning を活用し、試験管理ツール「ExamSOFT」により資格試験のリモート化を推進している。

会社概要

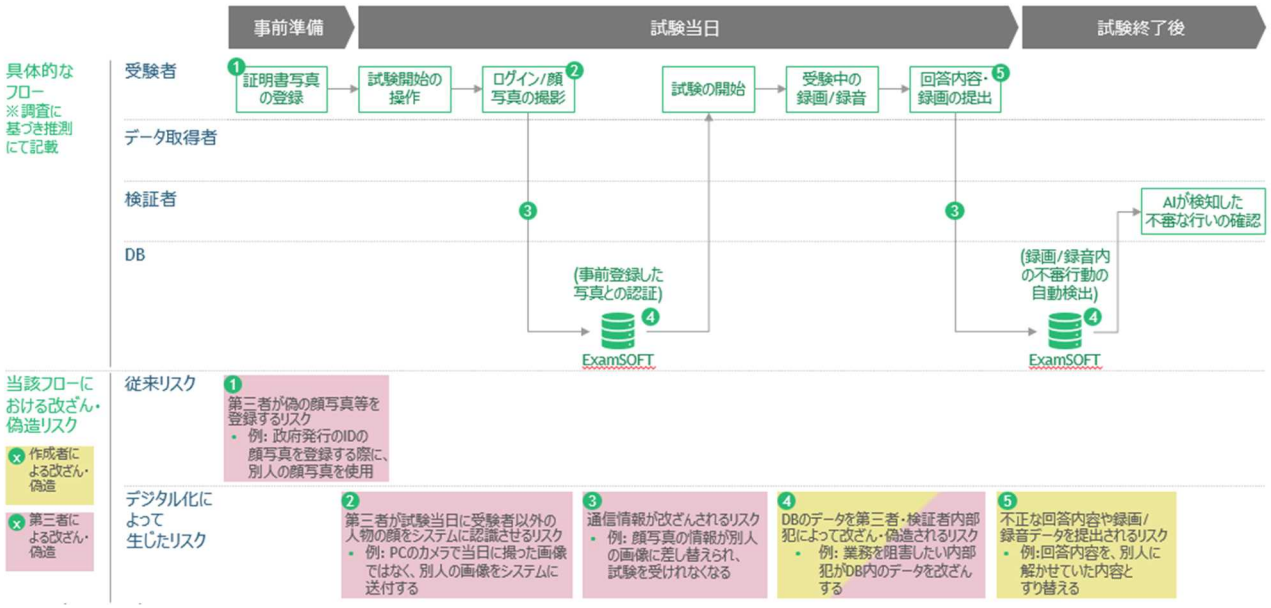
会社名	• Turnitin - 前述のソリューションを提供するExamSoftを2020年に買収
設立年	• 1998年
事業展開国	• アメリカ
事業概要	• オンライン学術支援ツールの提供
提供ソリューション	• 試験管理ツール:ExamSOFT • 学生のレポートの類似性チェック・ライティング指導ツール • 学術研究向け盗用・剽窃チェックツール　等

イメージ

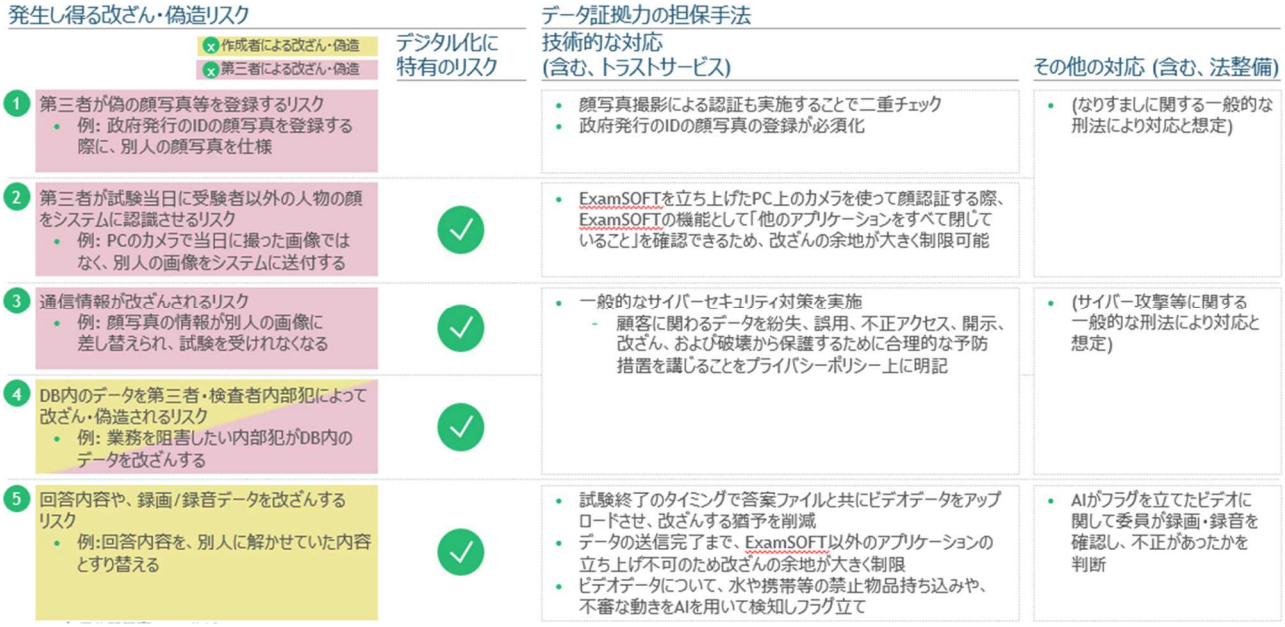
以下のような手法で不正を防ぐ形での試験のオンライン化

- 事前に登録した身分証の写真と、試験時にPCの前に座る受験者の顔の一致をAIで確認
- ExamSoft以外のPCアプリケーションの立ち上げの禁止
- 試験中の受験者の様子の録画/録音および試験官への送信
- 試験中の不審行動のAIでの監視

ExamSOFT by Turnitin における、e-learning システムを用いたオンライン試験のフローを、フローにおける改ざん・偽造リスクとともに以下のように整理した。



ExamSOFT by Turnitin の事例では、AI を用いてビデオデータ内の不審な動きを検知していることを確認した。



アメリカにおけるオンライン会議システム活用事例

アメリカでは、新型コロナの影響でオンライン公証が急速に普及した。アメリカの公証人制度とデジタル化に関しての概況としては、アメリカでは　印鑑証明という制度がないという背景から、不動産取引など重要な書類を作成する際に、公証人が文書の認証を実施しているという背景がある。（州から任命された公証人が、サインした人の身元と、脅迫といった状況でないことを確認）

オンライン公証は 2012 年にバージニア州議会が承認して以来、全米で徐々に採択されていたが、オンライン公証の推進派がデジタル処理の利便性や書類ミスの防止効果を強調する一方、従来の公証ビジネスの仕事を奪い、詐欺やハッキングを招くと懸念する声もあり、容易には浸透しなかった。一方、新型コロナウイルスによる感染が

拡大するにつれ、緊急法案や州知事命令などの手立てを用いてオンライン公証を臨時的に合法化する州が続出し、合法化する州が増えていくにつれ、オンライン公証サービスのニーズも増加した。

上記のデジタル化ニーズを捉え、Notarize はオンライン会議システムを活用したオンライン公証サービスを提供した。Notarize はオンラインビデオを用いたオンラインでの公証サービスを提供している。

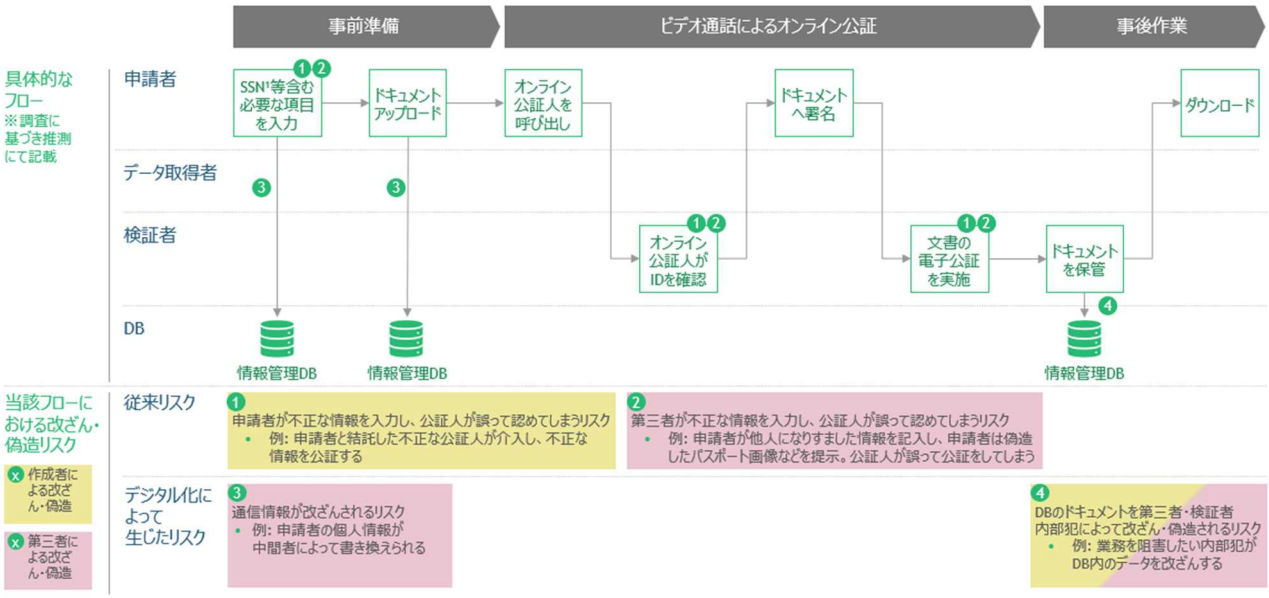
会社概要

会社名	• Notarize
設立年	• 2015年
事業展開国	• アメリカ
事業概要	• 文書のオンライン公証を提供 • コロナ禍の需要増加により、2021年春時点では、前年と比較し売上が600%増

イメージ

- PC、タブレット、スマートフォンで利用可能
- オンラインビデオを介して公証人と接続
- 公証人が確認し、ユーザが自分の署名と押印をデジタルで追加したのちに、完全に公証された文書をダウンロード可能

Notarize における、オンライン公証のフローを、フローにおける改ざん・偽造リスクとともに以下のように整理した。



Source: 各種公開記事、BCG分析
1. ソーシャルセキュリティナンバーの略であり、アメリカ合衆国における社会保障番号

35

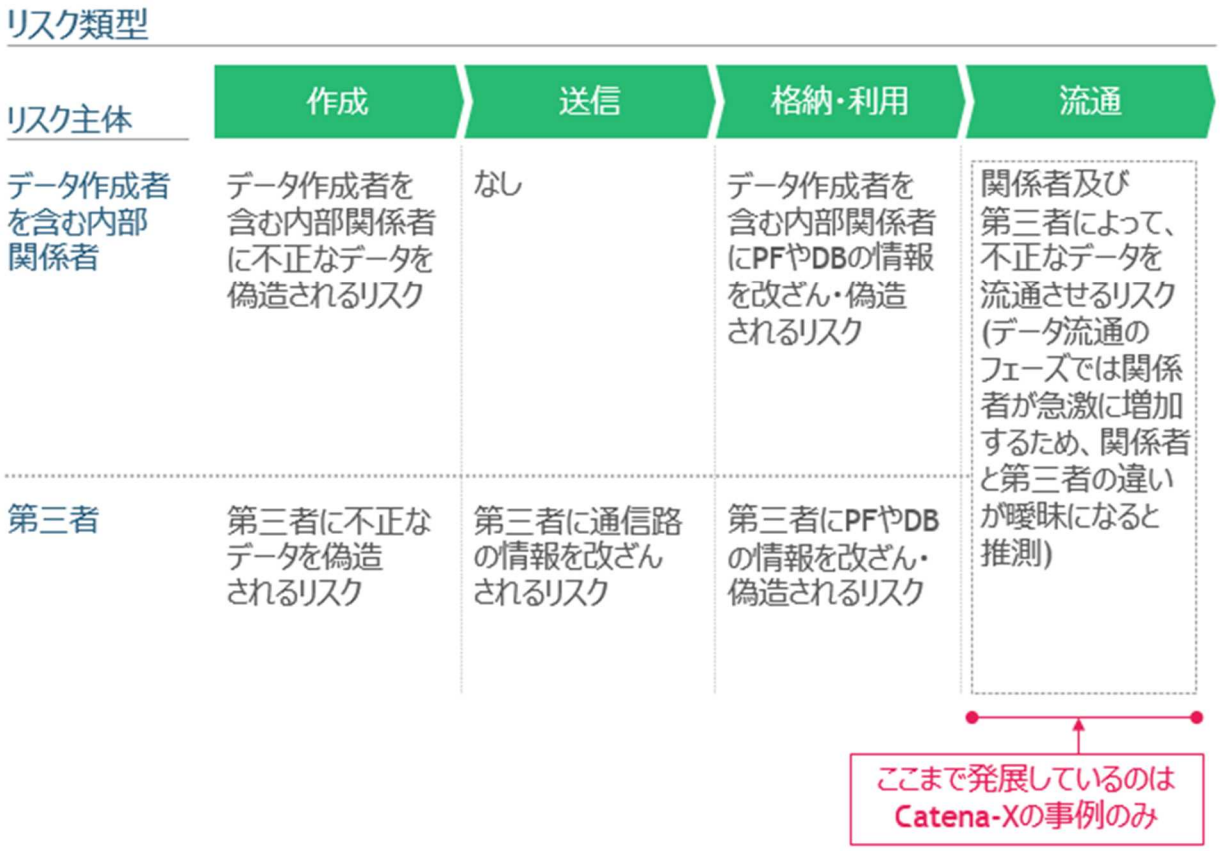
Notarize の事例では、申請内容の正当性確認のためにビデオ通話を用いているが、動画・画像にユニークなトラスト確保手法は未実施であったことを確認した。

発生し得る改ざん・偽造リスク	デジタル化に特有のリスク	データ証拠力の担保手法 技術的な対応 (含む、トラストサービス)	その他の対応 (含む、法整備)
		作成者による改ざん・偽造 第三者による改ざん・偽造	
1 申請者が不正な情報を入力し、公証人が誤って認めてしまうリスク • 例: 申請者と結託した不正な公証人が介入し、不正な情報を公証する		• 公証人は、申請内容の正当性確認のため、ビデオ通話の中で個人情報から生成された一連の質問とSSN等の政府発行のIDの自動分析を実施	• (虚偽申請等に関する一般的な刑法により対応と想定) • 内容確認に正当な公証人を当たらせることで対応と想定
2 第三者が不正な情報を入力し、公証人が誤って認めてしまうリスク • 例: 申請者が他人になりすました情報を記入し、申請者は偽造したパスポート画像などを提示。公証人が誤って公証をしてしまう		• 公証人の正当性を保証するための電子署名を発行 - 公証人が身元証明を完了した後に発行 - すべての公証人の身元が保障	• テキサス州の法律では、オンラインの公証人は、電子署名作成に使用された登録済み端末が最新で、端末の発行または登録機関によって取消や終了がされていないことを確認するための措置を講じる旨が規定 • テキサス州の法律では、オンライン公証人の電子記録、電子署名、または電子印鑑の他者による使用を許可しない旨が規定
3 通信路で依頼情報が改ざんされるリスク • 例: 申請者の個人情報が中間者によって書き換えられる	✓	• AES-256 ビット暗号を使用した転送中および保存中のすべてのデータの暗号化と保護、すべてのアプリケーションアクセスの追跡など、個人情報のセキュリティとプライバシーを確保するためにさまざまな手段を採用していることがサイト上に明記	• (サイバー攻撃等に関する一般的な刑法により対応と想定)
4 DBのドキュメントを第三者・検証者内部犯によって改ざん・偽造されるリスク • 例: 業務を阻害したい内部犯がDB内のデータを改ざんする	✓	• プライバシーポリシーに、システムが外部からの侵入、マルウェア、およびランサムウェアを防止し、回復力を持つように構築されていることが明記されており、一定レベルの対策が実施されていると推測	• 3 と同様

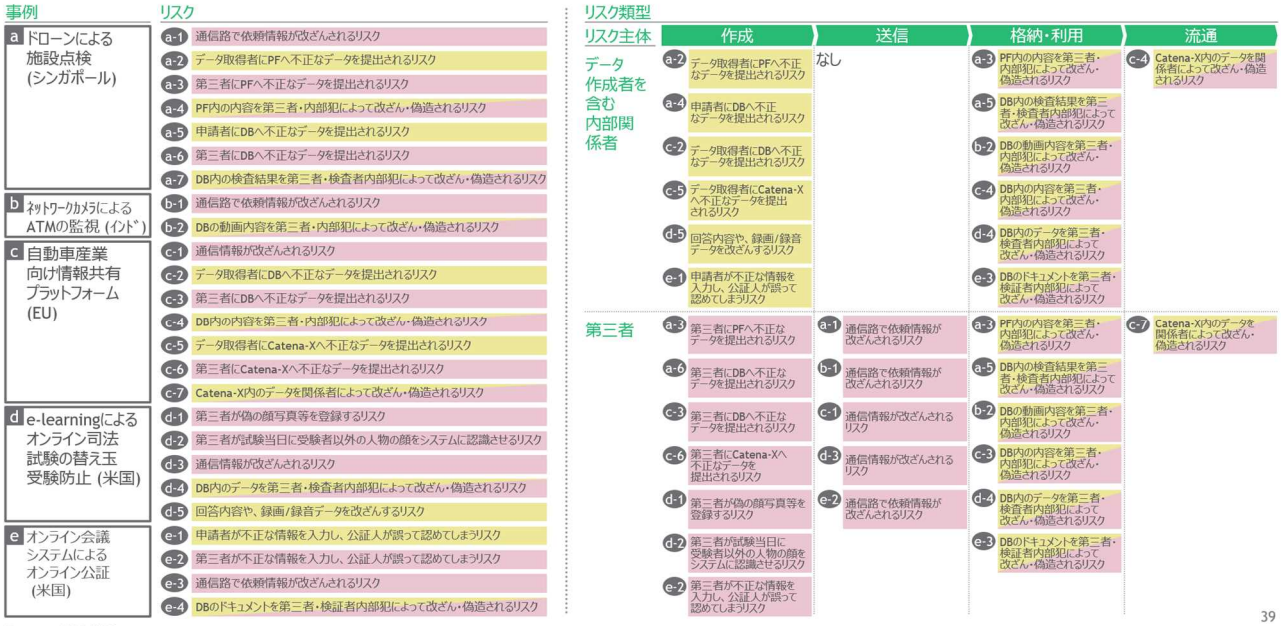
1.2 事例を基にしたリスクの類型化

事例を基としたリスクの類型

事例から抽出されたリスクを基に、データフローとリスクの作成主体からリスクの類型を定義した。これは、データの作成/送信/格納・利用/流通というフローそれぞれにリスクが存在することと、本案件で分析したどのユースケースにおいても、データを作成し、送信し、格納・利用するという流れは共通であるということからこのような定義とした。一方で、DFFT の理念や Catena-X の事例でもあるように、異なるプレイヤー間でのデータ流通が今後期待されることから、流通というフローも追加した。また、リスクを生み出す主体としてデータ作成者を含む内部関係者 (性悪説) と第三者が存在することからこれらをリスク主体の軸として採用した。



参考までだが、前述の各事例で抽出したリスクを上記で定義した類型にマッピングした結果を以下に記す。全てのリスクがマッピングできたことを確認した。



Source: BCG分析

2. ステークホルダーからのニーズ等実態調査

「1.動画・画像等のデータ証拠力の現状分析 (公共・民間分野)」から、海外の先進事例においても厳格なデータ証拠力の担保を意識的に実施している事例は Catena-X のデータ流通の事例のみであることがわかった。そのため、日本の動画・画像を用いたデジタル化において、いずれの業界でもニーズが現時点で顕在化していないと推察される。

本章では、上記仮説が正しいのかを検証するため、トラストに関するエキスパートへのヒアリングと、トラストが求められるユースケースに関わる事業者へのヒアリングから、動画・画像データの証拠力ニーズを調査した。

ニーズ調査の方向性

トラストニーズを第一に置いた上で、その中でどの程度現状・将来的な動画・画像の利用シーンがあるか、その中でトラストニーズがあるかを深堀する方向で、以下 2 つの方法でニーズを調査した。

- トラストのニーズに詳しいと想定される、弁護士・トラストサービス事業者へヒアリングを実施した。
  - 動画・画像データの証拠力が求められるケースが実例でどの程度あるのか、将来必要になるのかを把握するべく、弁護士へヒアリングを実施した。
  - 動画・画像データに対し、狭義のトラストサービスである電子署名・タイムスタンプが使われているケースがあるのかを把握するべく、トラストサービス事業者へヒアリングを実施した。（内容は非公表）
- 業務の特性からトラストのニーズが有り得る業界において、動画・画像データのニーズがあるかをヒアリングした。
  - トラストニーズ全体像から、特に動画・画像ニーズの強い見込みのあるユースケースを抽出した。
  - ユースケースにおいて、動画・画像データの活用余地とリスクを初期的に整理した。
  - 将来のデジタル化可能性も考慮しつつ、動画・画像データの活用余地がないか、各事業者へヒアリングを実施した。

2.1 有識者へのインタビュー

弁護士へのヒアリング結果

弁護士エキスパートへインタビューしたところ、動画・画像データを用いたデジタル化でトラストが求められるケースは、現時点では裁判の証拠等限定的であるとのことであった。位置情報についても同様にトラストのニーズは現時点では低いと想定されるとのことであった。

現状、真正性を担保する仕組みが動画・画像データに対して求められるケースはあまりなく、裁判の検証手続きなどで製造業の製品の品質をチェックするための撮影のように、動画データが何かの判断の材料になるケースでは改ざんされていないことが求められるとのことであった。

一方、トラストが求められるのは、事実認識に必要なデータの場合であり、不動産売買契約時に求められる書面や、アナログの図面をデジタル化し内容の真正性保証、あるデータを 2 次 3 次利用した際の大本のデータの真正性保証が例として挙げられるとのことであった。

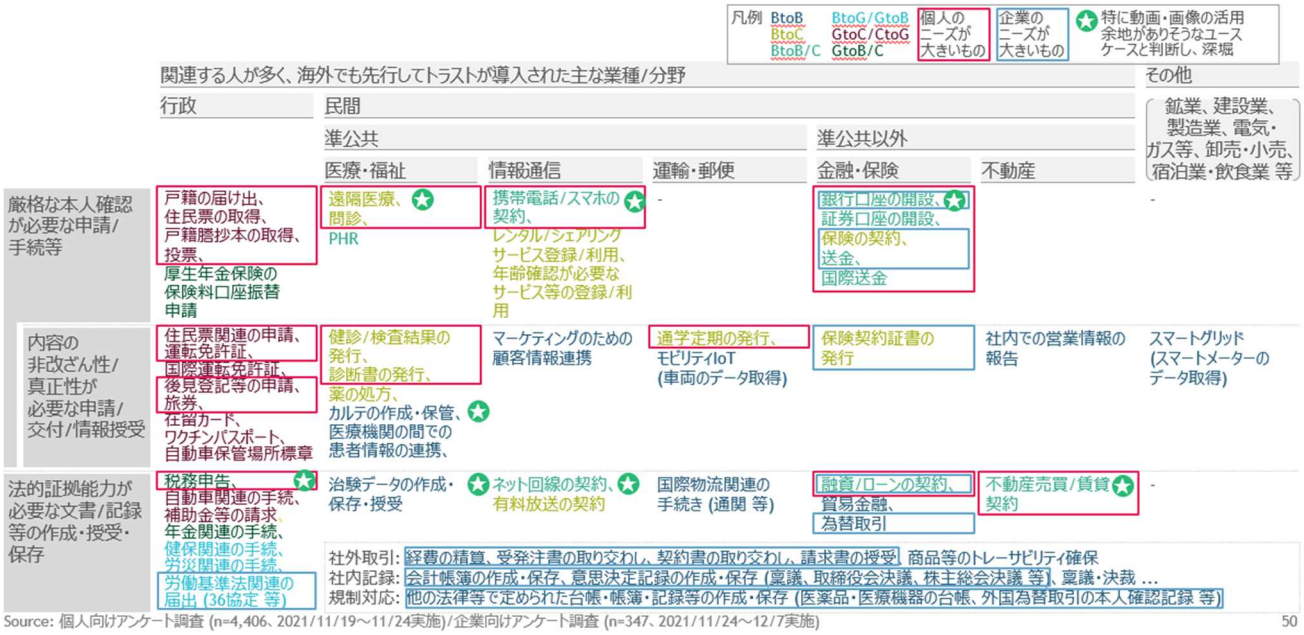
そのため、動画・画像データを用いたデジタル化においてトラストニーズがあるかを調査するよりも、事実認識にデータが必要なユースケース、すなわちトラストが求められるユースケースにおいて、動画・画像データを使用するケースを探し評価する方が、筋が良いと考えられるとのことであった。

デジタル化が進む中で動画・画像データに紐ついた位置情報にもトラストが求められる可能性はある一方、現時点でのニーズは低いと想定されるとのことであった。デジタル化された手続きで使用された動画・画像データを事実認識に用いた場合、作成者に加え位置情報の正当性が求められるケースは考えられる。一方、現状の監査法人のリモート監査で場所を確認する際は、そこまでの厳密な確認はしておらず追加質問や周辺の動画を取ることでカバーしているとのことであった。また、位置情報については、コストパフォーマンスによるが、現状位置情報の厳密性を求められているケースは少ないためニーズは低いと想定されるとのことであった。

2.2 過去トラスト案件で整理した、トラストニーズのある業界からの深堀

動画・画像データのニーズが強いユースケース抽出

「行政」および民間準公共の「医療・福祉」、準公共以外の「金融・保険」分野のデジタル化において、トラストニーズと動画・画像の活用余地があり得るユースケースを抽出した。



ユースケースにおける動画・画像データの活用余地とリスク

動画・画像データの活用余地のある業界のユースケースとリスクを下記図のように整理した。

		動画・画像のユースケース	想定されるリスク	
			リスクの類型	具体のリスク
行政		行政手続き時の本人確認	作成時	オンラインでの行政手続き時に運転免許証等での本人確認を実施する場合、偽造された運転免許証画像によりなりすましによる手続きが行われる
		リモート試験の実施	作成時	受験者本人ではない人が変わりに試験を実施する(替え玉受験)
		税務申告のための証憑データの添付	作成時	事業経費等の証憑の画像提出時に、脱税を目的に偽造された画像が作成される
民間(準公共)	医療・福祉	画像データを用いた遠隔医療/問診の実施	作成時	遠隔医療/問診の際に、虚偽の疾病に基づく不当な処方や保険金搾取等を目的とし、虚偽の画像が用いられる
		製薬等のための治験データの実施	作成時	望ましい治験データを捏造するために、虚偽の診療画像データが作成される
			格納・利用時	望ましい治験データを捏造するために、保存された診療画像データが改ざんされる
		複数医療機関を横断する医療の提供のための治療データの作成・保存・授受	流通	虚偽の疾病に基づく不当な処方や保険金搾取等を目的とし、虚偽の画像が用いられる
	情報通信	回線や、レンタルサービス等の新規契約・利用時の本人確認	作成時	新規契約・利用時に運転免許証等での本人確認を実施する場合、偽造された運転免許証画像によりなりすましによる手続きが行われる
		回線や、レンタルサービス等の新規契約・利用時の重要事項説明	作成時	新規契約・利用時に運転免許証等での本人確認を実施する場合、偽造された運転免許証画像によりなりすましによる手続きが行われる
	運輸・郵便	(現時点で明示的なニーズは見えず)	–	–
民間(それ以外)	不動産	不動産売買/賃貸契約時の本人確認	作成時	不動産売買・賃貸契約時に運転免許証等での本人確認を実施する場合、偽造された運転免許証画像によりなりすましによる手続きが行われる
	金融・保険	保険の申請	作成時	保険金の搾取のため、虚偽の損害画像 (例: 破損した自動車/家 等) を用いて保険金の申請が行われる
		新規口座開設/新規契約時の本人確認	作成時	新規口座開設/新規契約時に運転免許証等での本人確認を実施する場合、偽造された運転免許証画像によりなりすましによる手続きが行われる

各事業者へのヒアリングなどによるニーズ調査結果

各業界の事業者へ、対策と動画・画像データの証拠力担保のニーズをヒアリングした結果を以下に示す。

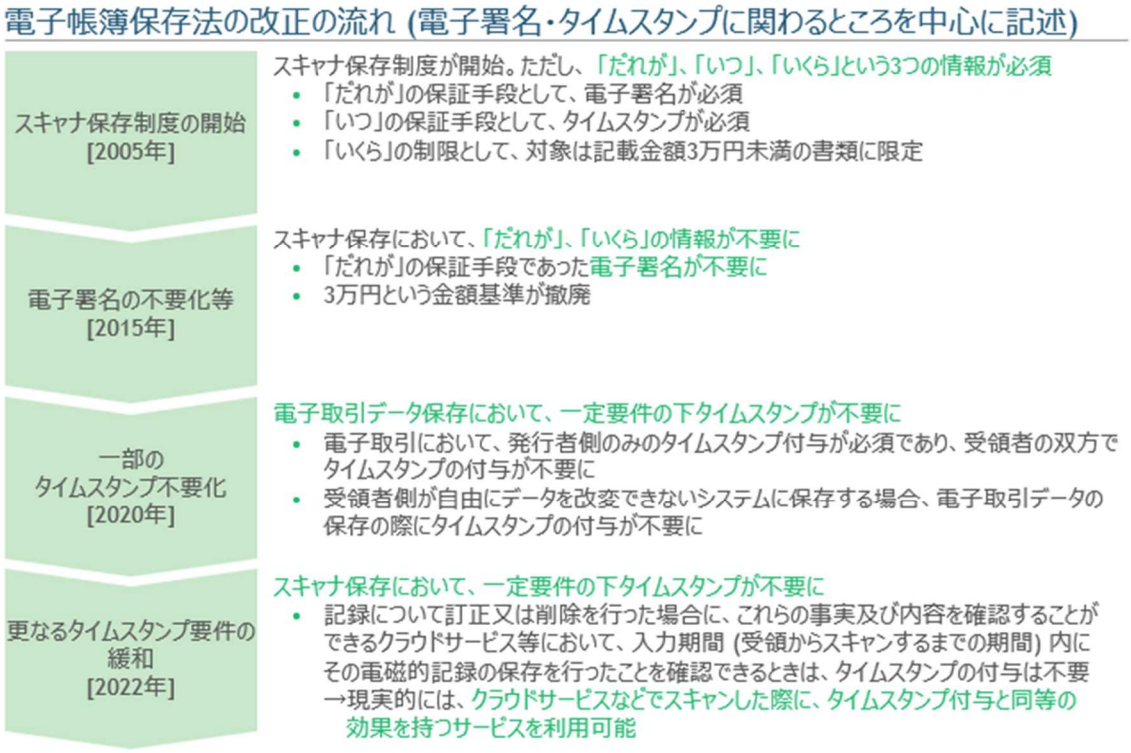
		動画・画像のユースケース	事業者からのコメント/ Webでの調査結果
行政		行政手続き時の本人確認	行政系の本人確認は、今後マイナンバーカードを利用することで、改ざん・偽造リスクを軽減 行政がマイナンバカードを用いた認証システムのAPIを開放すれば事業者に有益であるとの声有り
		リモート試験の実施	マイナンバーカードの認証のみでは他人が別の人のなりすまされてしまう可能性があり、追加の対策を実施する想定。アメリカの事例では、以下のような手法で不正を防止 • 事前に登録した身分証の写真と、試験時にPCの前に座る受験者の顔の一致をAIで確認 • ExamSoft以外のPCアプリケーションの立ち上げの禁止 • 試験中の受験者の様子の録画/録音および試験官への送信 • 試験中の不審行動のAIでの監視
		税務申告のための証憑データの添付	電子帳簿保存における電子署名/タイムスタンプ付与が必要なケースが、緩和傾向にある
民間 (準公共)	医療・福祉	画像データを用いた遠隔医療／問診の実施	遠隔画像診断にて、CT・X線・MR画像データなどが利用されている。また、医療に関わる画像データはDICOMという国際規格が使用され、ユニークなIDが振り分けられ、作成者や時刻情報といったメタデータがタグとして付与される DICOMは世界的な規格であり、IDが重なってはいけないという共通認識があるが、日本ではシステム設定不備などにより、年間数件程度衝突が発生。ただしシステムの修正で運用が回っている
		製薬等のための治験データの実施	
		複数医療機関を横断する医療の提供のための治療データの作成・保存・授受	データ証拠力が担保されたデータ集約・利活用のための基盤へのニーズは高い • 証拠力が担保された動画・画像データの収集・利活用は、最新システム承認の加速化によるマーケットの活性化や運用負荷軽減の可能性 • AIを用いた医療系システムが開発されているが、PMDAの承認のハードルが高くマーケットで利用されている事例は少ない データ集約を戦略的に実施している海外事例はあるが、データ証拠力への関心は低く、データ集約・利活用を先行して実施 • 台湾では、データ集約を第一目的とした医療クラウドにデータを集約しており、医療機関間の情報連携による再検査コストの削減を実現 • ICチップによる本人確認をしなければ医者は当該患者のデータが見れないようにするといった認証機能は実施している一方、データ自体の証拠力は特にケアされていないとのこと
民間 (準公共)	情報通信	回線や、レンタルサービス等の新規契約・利用時の本人確認	申し込みの際に、運転免許証や保険証といった本人が確認できるものを提示してもらうが、裏表のコピーのを提示しているため、改ざん・偽造が可能な認識 一方、ドコモショップにおけるなりすましによる不正契約といった事例もあり、画像データに対する証拠力のニーズが高まっている
		回線や、レンタルサービス等の新規契約・利用時の重要事項説明	昨今オンライン会議システムを用いて実施するようになった。説明実施を否認されるリスクを避けるため、説明後署名や押印を貰っているが、動画自体に証拠力を持たせることができるのであれば、署名や押印を不要にできる可能性がある
	運輸・郵便	(現時点で明示的なニーズは見えず)	
	不動産	不動産売買／賃貸契約時の本人確認	本人確認は基本的に実印の押印で実施されている 新築物件かつローンによる購入の場合、法務局、司法書士、銀行、不動産業者との契約などステークホルダーがたくさんいて一括のデジタル化が難しい。特に、法務局の押印文化がハードルとなっている印象があり、ここが緩和されない限りデジタル化は難しい印象 重要事項説明など、一部オンライン会議システムを用いたデジタル化は進んでいるが、最終的な同意は実印の押印で実施
民間 (それ以外)	金融・保険	保険の申請	自動車保険や火災保険の申請の妥当性検証のため、自動車の事故箇所や火災現場の画像データを用いている。ただし、金額の上限があり、高額の保険料の場合保険業者が現地確認を実施している。画像データの証拠力が担保されれば、高額の保険においても画像データや動画データを用いたリモートでの妥当性検証ができるようになり、人件費削減のニーズがある
		新規口座開設／新規契約時の本人確認	申し込みの際に、運転免許証や保険証といった本人が確認できるものを提示してもらっている。それに加え本人の写真撮影や証明証の厚みの確認を実施することで、改ざん・偽造防止を実施

Source: エキスパートインタビュー、各種公開記事

参考までだが、電子帳簿保存における電子署名/タイムスタンプ付与が必要なケースは緩和の傾向にあることが調査からわかった。電子帳簿保存法とは、1998 年より施行された、帳簿を電子保存できるよう定められた法律である。電子帳簿が対象とするのは、国税関係帳簿/国税関係書類/電子取引の 3 種類であり、対象データの保存形態は電子帳簿等保存/スキャナ保存/電子取引データ保存の 3 種類ある。それぞれの内容を以下に記す。

- 電子帳簿等保存: 電子的に作成した帳簿・書類をデータのまま保存。
  電子署名、タイムスタンプの付与は不要
- スキャナ保存: 紙で受領・作成した書類を画像データで保存。
  電子署名は不要、タイムスタンプは一部必要
- 電子取引データ保存: 電子的に授受した取引情報をデータで保存。
  電子署名は不要、タイムスタンプは一部必要

電子子帳簿保存法が改正され、電子署名・タイムスタンプが緩和傾向にある流れを以下に記す。



3. ニーズの分析・分類化、課題整理

3.1 トラストにおける脅威/不正の類型とトラスト確保手法の整理

トラスト確保手法の類型化の考え方

①事例を基としたリスクの類型と②類型リスクへのトラスト確保手法の整理の 2 段階で、トラスト確保手法の類型化した。なお①の内容は 1.2「事例を基にしたリスクの類型化」の内容と同様になるのでそちらを参照いただきたい。

ⅰ 事例を基としたリスクの類型

事例から抽出されたリスクをデータフローとリスクの作成主体から類型を整理

- データの作成/送信/格納・利用/流通というフローそれぞれにリスクが存在
  - 本案件で分析したどのユースケースにおいても、データを作成し、送信し、格納・利用するという流れは共通
  - 一方、DFFTの理念やCatena-Xの事例でもあるように、異なるプレイヤー間でのデータ流通が今後期待される
  - 今までの整理から、データフローそれぞれのフェーズにリスクが存在することを確認
- リスクを生み出す主体としてデータ作成者を含む内部関係者(性悪説)と第三者が存在

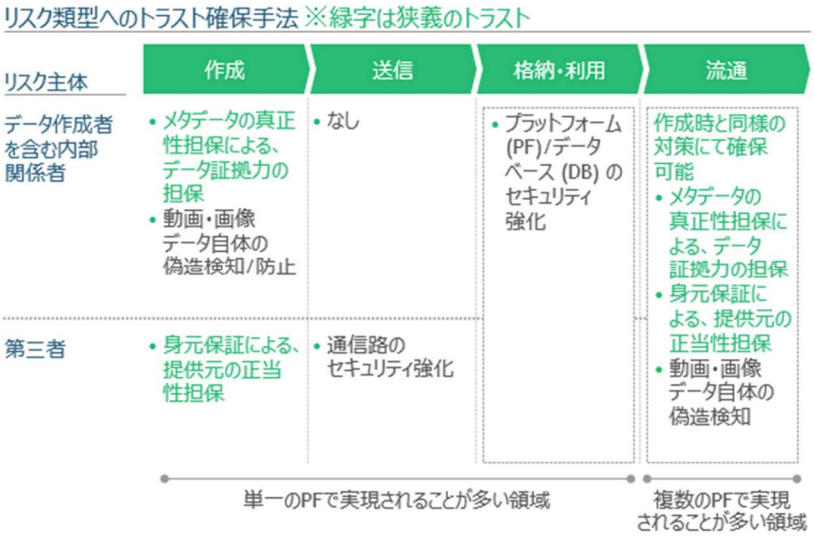
ⅱ 類型リスクへのトラスト確保手法の整理

ⅰで整理された類型リスクに対し、トラストを確保するための手法を整理

- 本案件で分析したユースケースの中では、トラスト確保の手法として、データ証拠力担保のための仕組みやサイバーセキュリティの強化、加工された画像のAI検知などが存在
- 類型化されたリスクをケアするために必要なトラスト確保の手法をマッピング
- 本フェーズで整理した内容を活用することで、今後デジタル化を実施する際に、対象ユースケースをフローと紐づくリスクを整理するとトラストの要否と確保手法が評価可能になる見立て
- アナログ規制の見直しなどのデジタル化を実施する際にトラスト要否を容易に判断できるよう、デジタル化の類型における改ざん・偽造リスクとトラスト確保手法を、具体例と併せて整理

類型リスクへのトラスト確保手法の整理

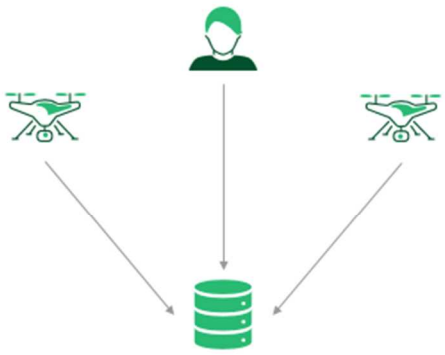
①で整理された類型リスクに対し、トラストを確保するための手法を整理した。整理するうえで注目した点としては、本案件で分析したユースケースの中では、トラスト確保の手法として、データ証拠力担保のための仕組みやサイバーセキュリティの強化、加工された画像の AI 検知などが存在したことである。これを踏まえ、以下の図のように類型化されたリスクをケアするために必要なトラスト確保の手法をマッピングした。



本フェーズで整理した内容を活用することで、今後デジタル化を実施する際に、対象ユースケースをフローと紐づくリスクを整理するとトラストの要否と確保手法が評価可能になる見立てである。

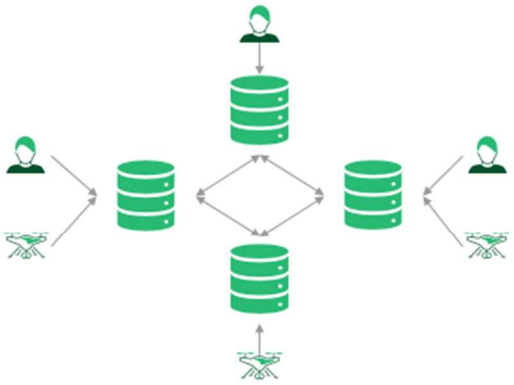
参考までに単一/複数 PF のイメージを以下に記す。

単一のPF



情報のやり取りが一つのPFに集約される
そのため、PF上でのID管理や統一的なトラスト・セキュリティの適用が容易に可能
例: 通常のサービスPF

複数のPF



情報のやり取りが複数のPF間で実施される
そのため、互換性のあるID管理や統一的なトラスト・セキュリティの適用が困難
例: エストニアの情報連携の仕組み (X-tee) で
公共・民間セクターの様々な情報システムを連携

各リスク類型へのトラスト確保手法の詳細内容は以下である。

リスク類型へのトラスト確保手法 ※緑字は狭義のトラスト	技術的な対応	その他の対応 (含む、法整備)
メタデータの真正性担保による、 データ証拠力の担保	• 複数PFの場合: 電子署名/eシール/タイムスタンプといったトラストサービス (位置情報を担保するサービスは現状存在せず) • 単一PFの場合: PF上でID管理や時刻、位置情報を管理する機能、データを作成した瞬間にトラストサービスを付与する/送信する等のデジタル的な仕組みを実装	• 不正に対する厳罰化 • 複数のデータの照らし合わせ等により、内容を検証 - 例: 画像データと、撮られた時刻における天候などを照らし合わせ、矛盾しないかを確認
身元保証による、 提供元の正当性担保	• PF上の登録時/情報提供時の身元確認 - 人の場合: 身分証明書の提示 等 - IoT機器の場合: 正当な業者からの提供であるかの確認	
動画・画像データ自体の偽造検知/防止	• DeepFake対策ツールの導入 等 • データ作成時にトラスト付与する技術的な仕組みの導入 等	
通信路のセキュリティ強化	• SSL/TLS、HTTPS、VPNによる通信路のセキュア化 等	
PF/DBのセキュリティ強化	• ID管理/アクセス制限の実装 • 不必要なサービスとポートの停止 • SCMやシャドーITの撲滅によるセキュリティホールの除外 • ログの取得と監視の実施 等	

デジタル化を実施する際にトラスト要否を容易に判断できるよう、デジタル化の類型における改ざん・偽造リスクとトラスト確保手法を、具体例と併せて整理した。

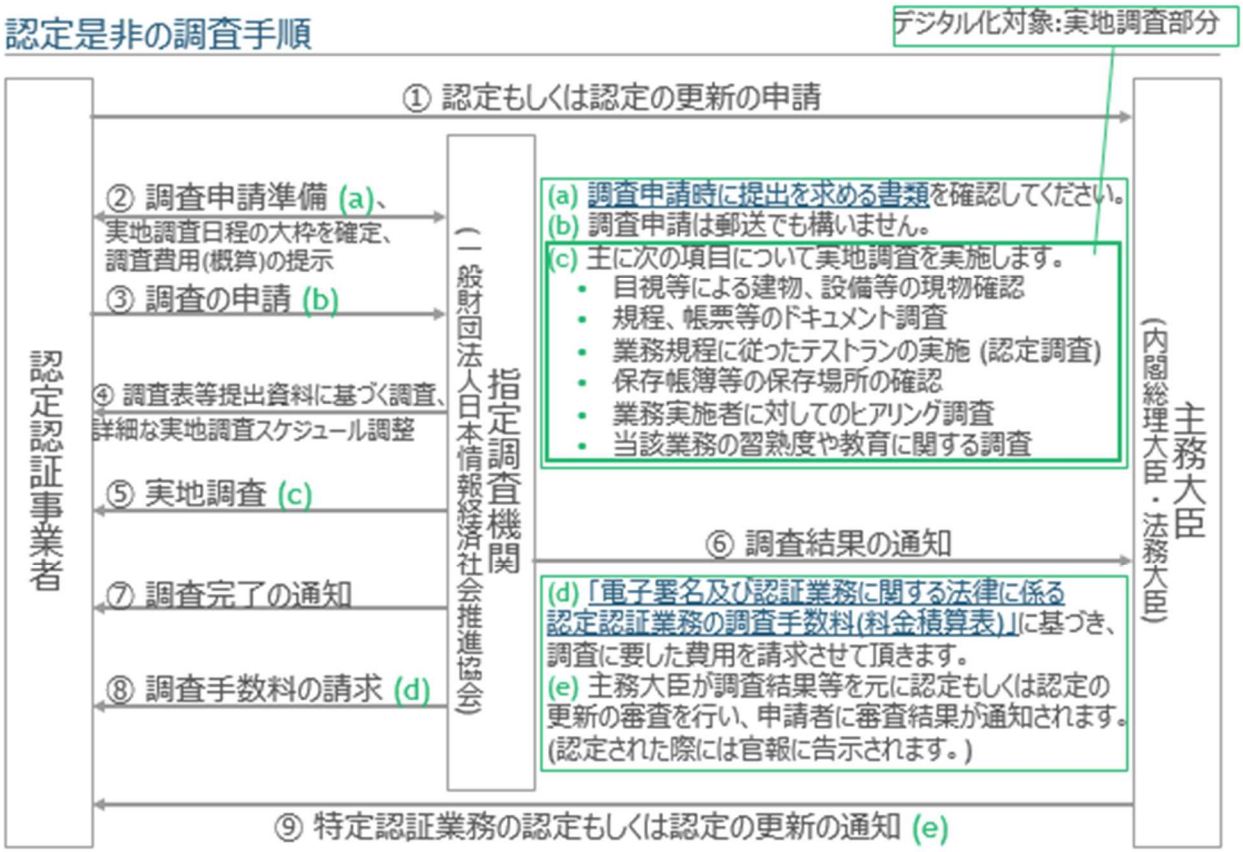
	デジタル化の手法	ありうる偽造・改ざん・否認のパターン	左記パターンが発生する具体例	左記に該当する場合に必要なトラスト手法
データ作成時のリスク	ドローン等のIoTデバイスを用いた無人確認 アナログ規制例 ・水道施設の目視点検 ・火薬製造施設の完成・保安検査	IoTデバイスで撮影した画像・動画データ自体が内部関係者によってDeepFakeツール等を用いて偽造される	・設備の傷や老朽化といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース	・Deepfake対策ツールの導入や、データを作成した瞬間に送信してしまうといった、動画・画像データ自体の偽造検知/防止機能を実装
		IoTデバイスで撮影した画像・動画データの位置・時刻情報が、内部関係者によってに偽造される	・複数の類似の施設がある際に、1つの施設の設備を最新化し、その施設への点検画像・動画データを他の施設の点検に流用することで設備の瑕疵を隠したいなど、負担軽減のインセンティブが働くケース	・IoTデバイスで撮影した画像・動画データへ位置・時刻情報を付与 ・より内部関係者による偽造・改ざんリスクを下げたい場合は、データを作成した瞬間に送信するといった機能を実装することで、内部関係者が偽造・改ざんする余地を出来るだけ削減
	オンライン会議システム等を用いた、リアルタイムでの人による確認 アナログ規制例 ・業務状況、科目の要件合性等の実地検査・調査 ・法適合性確認のための立入検査	オンライン会議中に提示している動画の提示対象をリアルタイムで加工する	・設備の傷や老朽化といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース	・加工防止機能を備えた専用ツールでのオンライン会議の実施 ・Deepfake対策ツールといった偽造を検知するツールの導入
		オンライン会議に別人が対象者になりすまし出席する	・有資格者の担当者が不在といった瑕疵を隠すために、なりすましによる負担軽減のインセンティブが働くケース	・オンライン会議中に運転免許証や保険証といった本人が確認できるものを提示してもらう ・上記に加え、本人の写真撮影や証明証の厚みの確認を実施することで、証明証自体の偽造・改ざんを防止
		オンライン会議中に内部関係者が示した位置情報が偽造されている	・複数の類似の施設がある際に、1つの施設の設備を最新化し、他の施設へのリアルタイムでの点検を最新化した施設で行うことで、設備の瑕疵を隠したいなど、負担軽減のインセンティブが働くケース	・位置情報を取得できかつ改ざん防止機能を備えた専用ツールでのオンライン会議の実施 ・スマートフォン等GPS機能の持つデバイスによる位置情報の提示
	事前に用意した、動画・画像 アナログ規制例 ・会計の状況、診療報酬の請求状況等の実地検査・ 調査	事前に用意した画像・動画データ自体が内部関係者によってDeepFakeツール等を用いて偽造される	・書類の不備といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース ・財務状況を良好に見せるために財務報告書を偽造するなど、金銭的なインセンティブが働くケース	・Deepfake対策ツールの導入や、データを作成した瞬間に送信してしまうといった、動画・画像データ自体の偽造検知/防止機能を実装
		事前に用意した画像・動画データの位置・時刻情報が、内部関係者によってに偽造される	・過去データを流用することで、負担軽減のインセンティブが働くケース	・事前に用意した画像・動画データへ位置・時刻情報を付与 ・より内部関係者による偽造・改ざんリスクを下げたい場合は、データを作成した瞬間に送信するといった機能を実装することで、内部関係者が偽造・改ざんする余地を出来るだけ削減
		不正が発覚した後に、証跡としてデータを出した際に作成者から否認される	・不正を起こしたことが監査などによって発覚した際に、責任逃れのために否認してしまうケース	・事前に用意した画像・動画データへ作成者情報を付与
データ作成時のリスク	共通	第三者が不審なデータを正当なデータ見せかけ偽造する	・ある会社が競合他社のサービスを混乱させることで自社を有利にさせるなど、金銭的なインセンティブが働くケース	・データ作成者の身元を検証するための、ID管理機能およびデータ検証機能の実装
データ送信時のリスク	共通	作成した画像・動画データを第三者が通信路上で偽造・改ざんする	・ある会社が競合他社のサービスを混乱させることで自社を有利にさせるなど、金銭的なインセンティブが働くケース	・通信路のセキュリティ対策を実施 -SSL/TLS、HTTPS、VPNによる通信路のセキュア化 等
データ格納・利用時のリスク	共通	DB/PF上に格納された画像・動画データを内部関係者が偽造・改ざんされる	・書類の不備といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース ・財務状況を良好に見せるために財務報告書を偽造するなど、金銭的なインセンティブが働くケース	・DB/PFのセキュリティ対策を実施 -ID管理/アクセス制限の実装・ログの取得と監視の実施 等
		DB/PF上に格納された画像・動画データを第三者が偽造・改ざんする	・ある会社が競合他社のサービスを混乱させることで自社を有利にさせるなど、金銭的なインセンティブが働くケース	・DB/PFのセキュリティ対策を実施 -ID管理/アクセス制限の実装・不必要なサービスとポートの停止・SCMやシャドーITの撲滅によるセキュリティホールの除外・ログの取得と監視の実施 等

3.2 電子署名法の実地調査のデジタル化を想定した、フレームワークの検証

電子署名法における、デジタル化手法の洗い出し

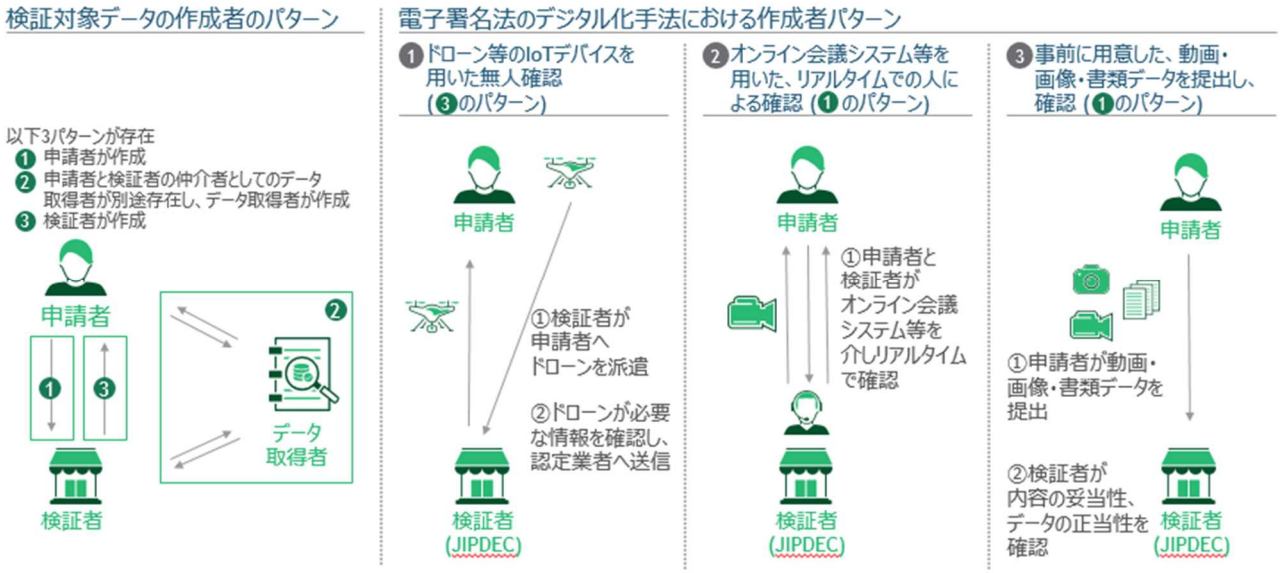
電子署名法というのは、平成 13 年（2001 年）4 月 1 日から施行された法律であり、電子署名が手書きの署名や押印と同等に通用する法的基盤が整備された。認証業務のうち一定の基準を満たすものは、国の認定を受けることができる制度が導入された。2023 年 3 月現在、デジタル庁でデジタル臨調におけるアナログ規制の見直しが進められているが、電子署名法の実地調査も見直しの対象となっている。当該法令の内容を以下に記す。

- 主務大臣は、第四条第一項の認定のための審査に当たっては、主務省令で定めるところにより、申請に係る業務の実施に係る体制について実地の調査を行うものとする

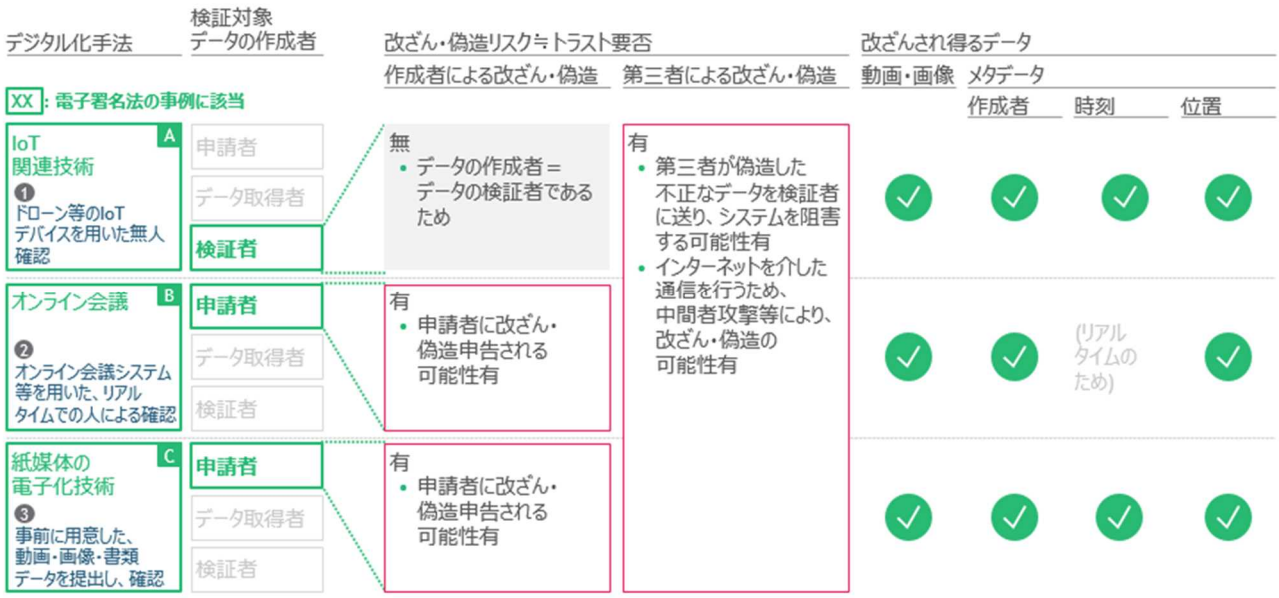


前述の実地調査の 6 項目は、3 つのデジタル化の手法に整理される。

また、各デジタル化手法の技術的なトラスト要否の評価にあたり、検証対象データの作成者の分類を実施した。検証対象データの作成者のパターンとして、申請者、データ取得者、検証者の 3 パターンに分類される。



電子署名法における改ざん・偽造リスクを、性悪説に基づき幅広に捉え、トラスト要否を以下のように評価した。

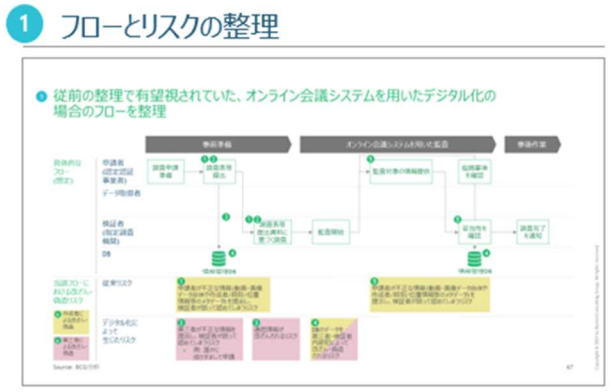


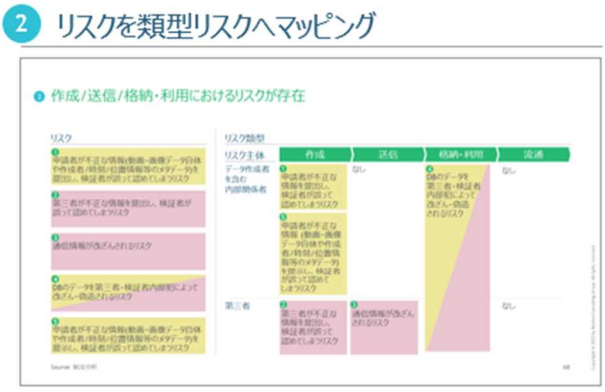
電子署名法の実地調査のデジタル化におけるトラスト確保手法の評価

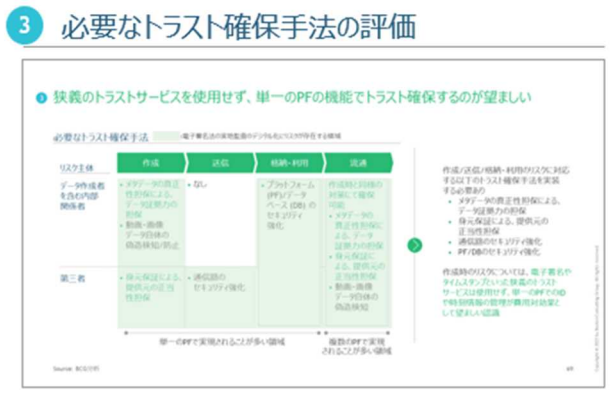
本調査研究で整理した流れに沿って、以下の４フェーズにて電子署名法の実地調査のデジタル化におけるトラスト確保手法の評価を実施した。

① フローとリスクの整理
② リスクを類型リスクへマッピング
③ 必要なトラスト確保手法の評価
④ 手法に適した詳細なトラスト確保手法の評価

なお今回は、デジタル化手法の中で最も有望であったオンライン会議システムを用いたデジタル化を想定しつつ評価した。結果としては、オンライン会議システムを用いた電子署名法の実地確認のデジタル化は作成・送信・格納/利用のリスクが存在し、PF を利用したトラスト確保手法が望ましいと考えられる。

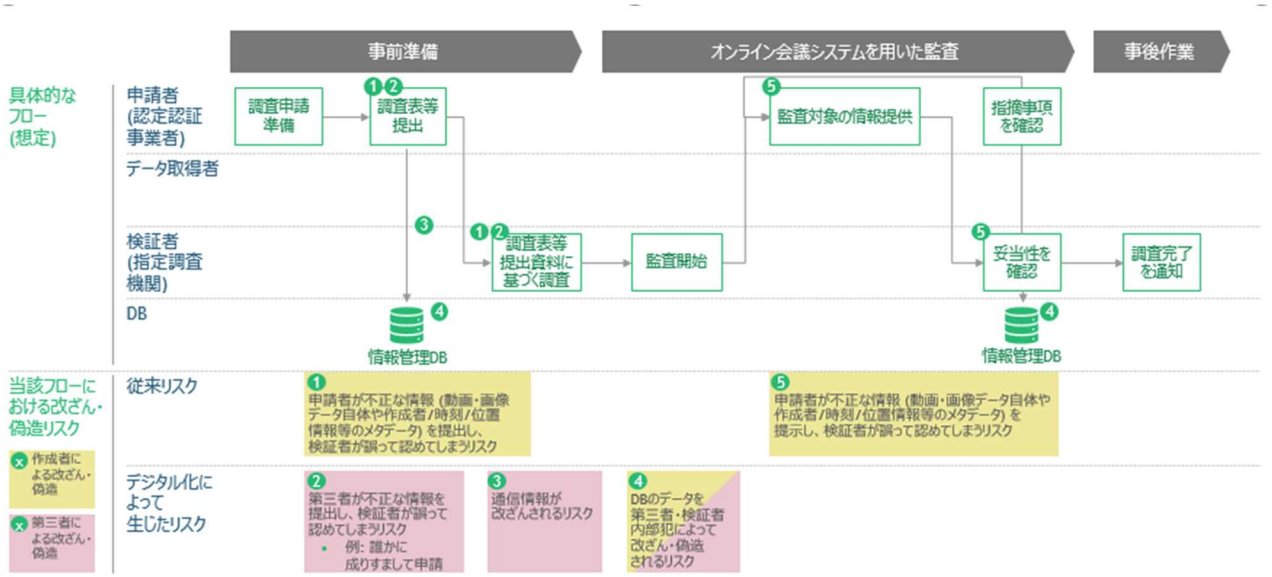




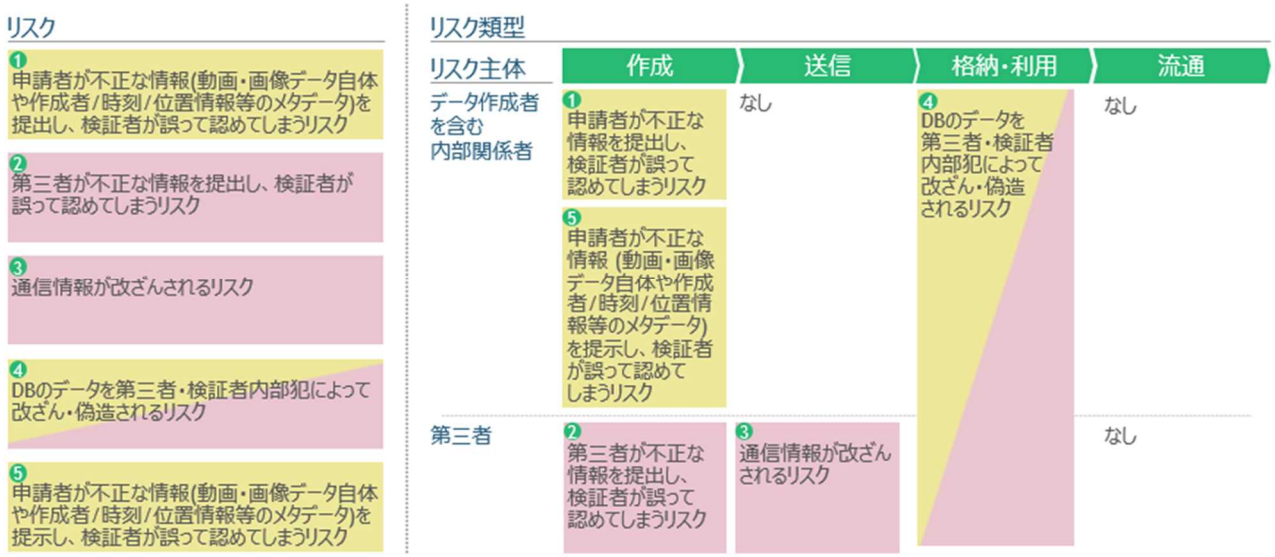


なお、今後アナログ規制等の見直し等のデジタル化を実施する際も、同様の流れで必要なトラスト確保手法を判断できる認識である。

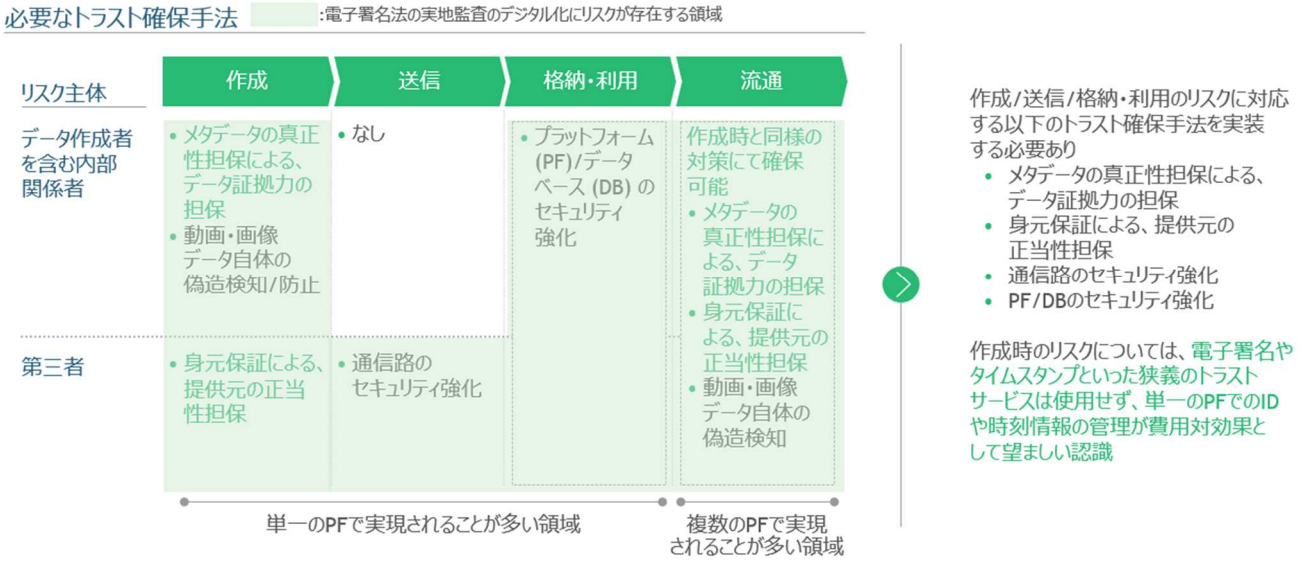
①フローとリスクの整理の内容について記載する。従前の整理で有望視されていた、オンライン会議システムを用いたデジタル化の場合のフローを以下のように整理した。



②リスクを類型リスクへマッピングした結果を以下に記す。作成/送信/格納・利用におけるリスクが存在することがわかった。



③必要なトラスト確保手法の評価の結果を以下に記す。上段でも示した通り、電子署名法の実地調査のデジタル化においては、狭義のトラストサービスを使用せず、単一の PF の機能でトラスト確保するのが望ましい。



④手法に適した詳細なトラスト確保手法の評価の結果を以下に記す。オンライン会議システムを利用する場合、位置情報の改ざんリスクがあるため、専用ツールやスマートフォン等 GPS 機能の持つデバイスの提示が必要となる想定である。

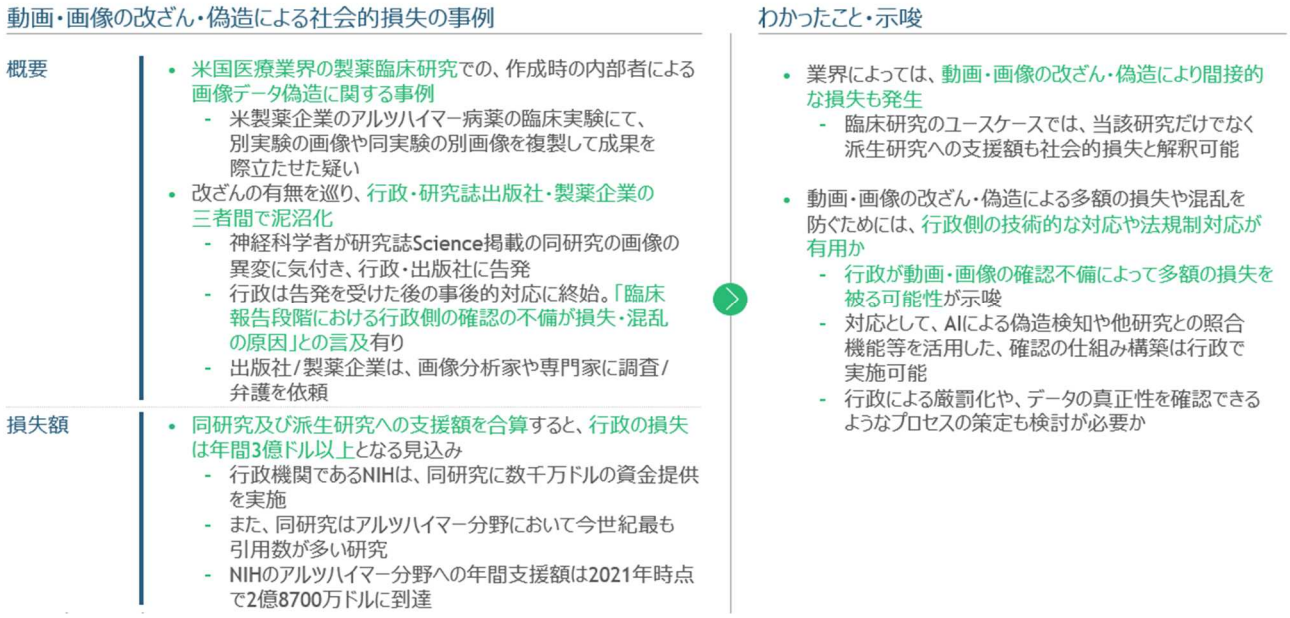
:電子署名法の実地監査のデジタル化にリスクが存在する領域

	デジタル化の手法	ありうる偽造・改ざん・否認のパターン	左記パターンが発生する具体例	左記に該当する場合に必要なトラスト手法
データ作成時のリスク	ドローン等のIoTデバイスを用いた無人確認 アナログ規制例 •水道施設の目視点検 •火薬製造施設の完成・保安検査	IoTデバイスで撮影した画像・動画データ自体が内部関係者によってDeepFakeツール等を用いて偽造される	•設備の傷や老朽化といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース	•Deepfake対策ツールの導入や、データを作成した瞬間に送信してしまうといった、動画・画像データ自体の偽造検知/防止機能を実装
		IoTデバイスで撮影した画像・動画データの位置・時刻情報が、内部関係者によってに偽造される	•複数の類似の施設がある際に、1つの施設の設備を最新化し、その施設への点検画像・動画データを他の施設の点検に流用することで設備の瑕疵を隠したいなど、負担軽減のインセンティブが働くケース	•IoTデバイスで撮影した画像・動画データへ位置・時刻情報を付与 •より内部関係者による偽造・改ざんリスクを下げたい場合は、データを作成した瞬間に送信するといった機能を実装することで、内部関係者が偽造・改ざんする余地を出来るだけ削減
	オンライン会議システム等を用いた、リアルタイムでの人による確認 アナログ規制例 •業務状況、科目の要件合性等の実地検査・調査 •法適合性確認のための立入検査	オンライン会議中に提示している動画の提示対象をリアルタイムで加工する	•設備の傷や老朽化といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース	•加工防止機能を備えた専用ツールでのオンライン会議の実施 •Deepfake対策ツールといった偽造を検知するツールの導入
		オンライン会議に別人が対象者になりすまし出席する	•有資格者の担当者が不在といった瑕疵を隠すために、なりすましによる負担軽減のインセンティブが働くケース	•オンライン会議中に運転免許証や保険証といった本人が確認できるものを提示してもらう •上記に加え、本人の写真撮影や証明証の厚みの確認を実施することで、証明証自体の偽造・改ざんを防止
		オンライン会議中に内部関係者が示した位置情報が偽造されている	•複数の類似の施設がある際に、1つの施設の設備を最新化し、他の施設へのリアルタイムでの点検を最新化した施設で行うことで、設備の瑕疵を隠したいなど、負担軽減のインセンティブが働くケース	•位置情報を取得できかつ改ざん防止機能を備えた専用ツールでのオンライン会議の実施 •スマートフォン等GPS機能の持つデバイスによる位置情報の提示
	事前に用意した、動画・画像 アナログ規制例 •会計の状況、診療報酬の請求状況等の実地検査・調査	事前に用意した画像・動画データ自体が内部関係者によってDeepFakeツール等を用いて偽造される	•書類の不備といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース •財務状況を良好に見せるために財務報告書を偽造するなど、金銭的なインセンティブが働くケース	•Deepfake対策ツールの導入や、データを作成した瞬間に送信してしまうといった、動画・画像データ自体の偽造検知/防止機能を実装
		事前に用意した画像・動画データの位置・時刻情報が、内部関係者によってに偽造される	•過去データを流用することで、負担軽減のインセンティブが働くケース	•事前に用意した画像・動画データへ位置・時刻情報を付与 •より内部関係者による偽造・改ざんリスクを下げたい場合は、データを作成した瞬間に送信するといった機能を実装することで、内部関係者が偽造・改ざんする余地を出来るだけ削減
		不正が発覚した後に、証跡としてデータを出した際に作成者から否認される	•不正を起こしたことが監査などによって発覚した際に、責任逃れのために否認してしまうケース	•事前に用意した画像・動画データへ作成者情報を付与
データ作成時のリスク	共通	第三者が不審なデータを正当なデータ見せかけ偽造する	•ある会社が競合他社のサービスを混乱させることで自社を有利にさせるなど、金銭的なインセンティブが働くケース	•データ作成者の身元を検証するための、ID管理機能およびデータ検証機能の実装
データ送信時のリスク	共通	作成した画像・動画データを第三者が通信路上で偽造・改ざんする	•ある会社が競合他社のサービスを混乱させることで自社を有利にさせるなど、金銭的なインセンティブが働くケース	•通信路のセキュリティ対策を実施 -SSL/TLS、HTTPS、VPNによる通信路のセキュア化 等
データ格納・利用時のリスク	共通	DB/PF上に格納された画像・動画データを内部関係者が偽造・改ざんされる	•書類の不備といった瑕疵を隠すために画像・動画データを偽造するなど、負担軽減のインセンティブが働くケース •財務状況を良好に見せるために財務報告書を偽造するなど、金銭的なインセンティブが働くケース	•DB/PFのセキュリティ対策を実施 -ID管理/アクセス制限の実装・ログの取得と監視の実施 等
		DB/PF上に格納された画像・動画データを第三者が偽造・改ざんする	•ある会社が競合他社のサービスを混乱させることで自社を有利にさせるなど、金銭的なインセンティブが働くケース	•DB/PFのセキュリティ対策を実施 -ID管理/アクセス制限の実装・不必要なサービスとポートの停止・SCMやシャドーITの撲滅によるセキュリティホールの除外・ログの取得と監視の実施 等

3.3 トラストに係る社会的影響の調査

本節では、トラストに係る社会的影響を調査したが、社会的な影響には定量的なものと定性的なものが存在すると整理した。

定量的な影響とは、動画・画像データの不正な改ざん・偽造によって、損害金額といった被害が現れるものである。被害の大小は、不正された動画・画像データの利用規模や対象のサービス・システムの大小によって変化すると考えられる。定量的な影響が出た事例として、米医療業界における画像の偽造によって行政が数億ドルの損失を被り得る事例を調査したため、その結果を以下に記す。この事例は、画像の偽造により行政が数億ドルの損失を被り得るものであった。



定性的な影響とは、動画・画像データの不正な改ざん・偽造によって、社会的な信頼の失墜や社会の混乱といった被害が現れるものである。被害の大小は、不正された動画・画像データの利用規模や対象のサービス・システム

の大小によって変化するが、定量的な評価が難しいと考えられる。定性的な影響が出た事例として、台風による水害のフェイク画像によって社会的混乱が発生した事例を調査したため、その結果を以下に記す。

フェイク画像拡大よる社会的混乱発生の事例

概要

- 台風15号による水害被害が発生している静岡県を巡って、フェイク画像が拡散
  - 2022年9月16日に投稿者は「ドローンで撮影された静岡県の水害」と称し、Twitter上で画像を投稿
  - 上空から俯瞰した視点で建物や土地が水没している様子が写っているが、濁流の流れや建物に不自然な部分があり、投稿に対して「画像生成AIが作成した偽物ではないか？」など疑問の声が浮上
  - 投稿者は問題の画像がフェイクだと認め、謝罪文を投稿。画像生成AI「Stable Diffusion」を使い、作成したことを明かした
  - 後日、熊本県警はデマツイートを投稿した神奈川県の会社員の男(20)を偽計業務妨害の疑いで逮捕

社会的影響

- 松野官房長官は、「被災地の住民等の適切な判断と行動を助ける上で、流言飛語等による社会的混乱を防止することは重要であると認識している」とコメント
- ジャーナリストの佐々木俊尚氏は、当該フェイク画像をテレビや新聞に掲載されることによる混乱拡大の可能性を言及

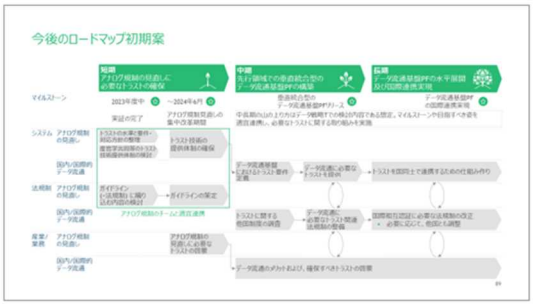
わかったこと・示唆

- AIを用いたツールを使用することで、誰でもフェイク画像を作成することができ、改ざん・偽造リスクの増加に繋がる可能性あり
  - 「Stable Diffusion」はWebサービスとしても使用可能なオープンなツールである
  - そのようなツールを用いて大半の人が騙されてしまうような精度のフェイク画像が作成可能
  - 今後普及が進むと、人をだますモチベーションでフェイク画像を作成する人が増加し、改ざん・偽造リスクの増加に繋がり得る
- テレビや新聞といった周囲からの信頼を得ている提供主体は、公開情報の証拠力の担保が重要になる認識
  - 従前よりテレビや新聞は公開情報を使用している認識だが、今後フェイク画像の増加によりデマ情報を流布してしまうリスクが高まる可能性有り
  - 検証するコストの兼ね合いもあるが、周囲からの信頼を得ている提供主体は持つ影響力の大きさを考慮した、利用する公開情報が正当なものなのかの検証が重要になる認識

4. ロードマップの検討 (長期・中期・短期)

本章の実施内容概要

本章では、今後デジタル庁がトラストの普及に向け短期・中期・長期で実施すべき内容をロードマップという形でまとめた。目指すべき姿と実現に向けた課題・ネクストアクションを整理したうえで、目指すべき姿の実現タイミングとアクションの前後関係を踏まえてロードマップを策定した。

	目指すべき姿と実現に向けた課題・ネクストアクションの整理	ロードマップの策定
実施イメージ		
実施内容	デジタル庁の大方針として、デジタル臨調関係とDFFT関係がある理解。 それぞれの目指すべき姿を定義し、実現に向けて解決すべき課題をトラスト関係のものを含み整理し、ネクストアクションを検討	左記で抽出した、目指すべき姿・課題・ネクストアクションについて、実現すべきタイミングと実行の前後関係を整理し、短期・中期・長期でのロードマップを策定

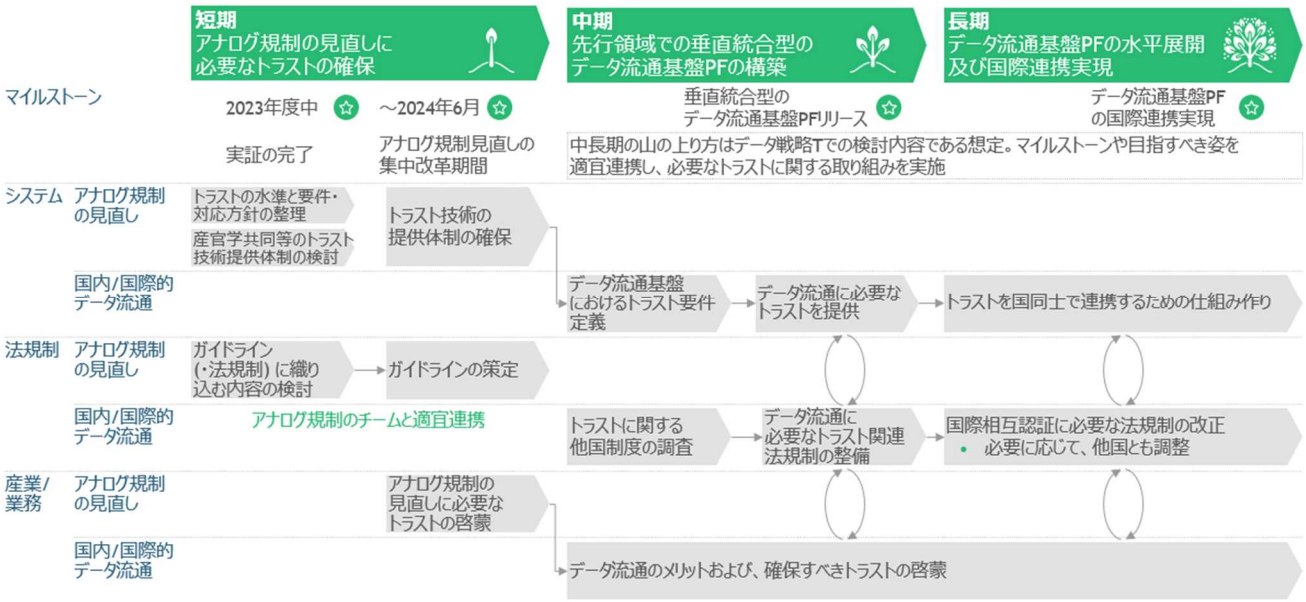
4.1 目指すべき姿と実現に向けた課題・ネクストアクションの整理

今後デジタル庁が実現している社会の目指す姿として、「アナログ規制から各企業から解放され、実際に各企業で業務のデジタル化が進捗」と、「規制に関わらない領域でも、”自由貿易主義に基づく”数十億 ID レベルのデータ流通・データ利活用による産業イノベーション推進」の 2 つがある認識である。それぞれの目指す姿に向けた初期的な課題と、必要なアクションを下記のようにまとめた。

社会として目指す姿 (BCG理解)		課題 (初期的) 緑字:トラスト関連	必要なアクション (初期的) 緑字:トラスト関連
アナログ規制から各企業から解放され、実際に各企業で業務のデジタル化が進捗 • 例: 従来、目視で行っていた業務がドローンによる監視、センサー等で実施される • 例: 従来、オフラインで実施されていた法定資格の試験が、オンラインで実施される	システム	アナログ規制の見直しに必要なPFやサービスが現時点で決まっていない	アナログ規制についての技術実証を行った上で、あるべき規定を実現
		上記に付随し、業務をデジタル化した際に発生するデータのやり取りについて、トラスト上のリスクを抑制するトラストの仕組みが明らかでない	トラスト上のリスクを整理の上、アナログ規制の見直しを実施するチームと連携し、トラストの仕組みを構築
		業務の変更に向けて組むべきテクノロジー企業が探索 / 選定できない	各企業がテクノロジー企業を探索できるPFの整備
		上記に付随し、業務の変更に伴い必要なトラスト技術を提供する主体が明らかになっていない	各企業が必要なトラスト及びトラスト確保の提供主体を検索できるPFの整備
	法規制	アナログ規制の見直し後、どのような法制度の改正になるかが定まっていない	アナログ規制の見直しによる法制度の改正内容を整理し、各所管省庁へ連携
		上記に付随し、業務をデジタル化した際に発生するデータのやり取りについて、トラスト上のリスクを抑制するトラストの法制度が明らかでない	トラスト上のリスクを整理の上、アナログ規制の見直しを実施するチームと連携し、システムでカバーできない範囲/法的な証拠能力が必要な領域を適宜法制度に織り込み
	産業 / 業務	アナログ規制の見直しがされても企業に周知されない	業界団体/メディアなどと連携し、アナログ規制についての周知を実現
		アナログ規制が見直されても、各企業はコスト等を理由に従来の業務手法を維持する	業務の見直しにあたってのハードルを理解し、それぞれへの対策を行う (補助金・税制優遇等のインセンティブ/ディスインセンティブ設計)
規制に関わらない領域でも、”自由貿易主義に基づく”数十億IDレベルのデータ流通・データ利活用による産業イノベーション推進	システム	データの流通にあたって、利便性 / 低コスト / トラストを含むセキュリティが確保された共通的な仕組みがない	(1) 特定の業界での垂直統合的PFの構築 • 構築を通じ、機能・その他要件を洗い出し (業界選定にあたってはデジタル臨調の動きも横にらみ) (2) 水平展開の実施 (特に (1) で整理した共通的な要件を踏まえ) (3) 国際標準への対応方針
	法規制	データの流通について法やガイドラインが未整備。また特に他国との法制度のすり合わせが必要(トラストの確保 / プライバシー・データ主権の保護等の観点を踏まえ)	データ流通におけるリスク (特にトラスト等) を精査の上、事業者ニーズ / 他国制度も踏まえ、法制度を実現 • トラスト確保 / プライバシー・データ主権の保護等
	産業 / 業務	国内において、企業が事業に関する情報をデジタル化し、流通させることや、流通している情報を活用することに積極的でない	いずれかの業界で、垂直統合的に変革を実現。データ流通の前例を創出の上、他業界にも周知 業界団体 / メディア当友連携し、アナログ規制についての周知を実現
		データを国際的に連携するニーズが見えておらず、システムが実現したとしても国際的なデータ流通が進まない	国際的なデータを活かした利活用事例を発掘し、国際的な周知を実施

4.2 ロードマップの策定

前節で整理した目指すべき姿と実現に向けた課題・ネクストアクションを踏まえて、以下のようにロードマップを策定した。



アナログ規制のデジタル化と国内/国際的データ流通という目指すべき姿に向け、大きく 3 ステップのロードマップでの推進を想定している。

短期的には、アナログ規制のデジタル化に向けた、トラスト確保の要件定義及び産官学共同等を含むトラスト技術提供体制の検討、及びアナログ規制見直しとのチーム連携を実施する必要がある認識である。

中期的には、国内でのデータ流通に向けた特定の業界での垂直統合的 PF や省庁内での統一的な PF の構築を行うべきだと考えている。

長期的には、国際的データ連携を視野に入れた、トラスト確保 / プライバシー・データ主権保護手法、他国制度を踏まえた法制度を検討するべきだと考えている。

トラストの水準と要件・対応方針の整理

デジタル臨調でのアナログ規制の見直しでは、デジタル化を妨げるアナログ規制を可及的速やかに一掃するため、各種見直しを 2024 年 6 月までを目途に実施することとして加速化されることが見込まれる。

2023 年 4 月～2024 年 3 月までの期間にて、規制の見直しに必要な実証の実施や、民間・公共に寄るデジタル導入の際に役立ちうる技術保有企業を掲載したカタログの運営、各種ガイドラインの取りまとめ等といったアナログ規制の見直し・デジタル導入促進のための事業が実施される見込みである。

それに対し、トラストの水準と要件・対応方針の整理のために必要なアクションとしては、デジタル臨調の事務局と連携して、規制の見直しにトラストの観点を織り込むことが考えられる。そのためには、デジタル臨調の事務局に対し、トラストに関する考え方／方針を共有することや、デジタル臨調事務局より、ありうるデジタル化のパターンをヒアリングの上、それぞれのリスクと取りうる対策を説明すること、各規制について、所管省庁にて許容しうるリスク／しえないリスクを峻別すること、許容し得ないリスクへの対応に必要なトラストの施策については、実証の対象にする / カタログの掲載要件に落とし込むことが重要である。

産官学共同等のトラスト技術提供体制の検討

上記ロードマップにおける「産官学共同等のトラスト技術提供体制の検討」では、2022 年 3 月弊社からデジタル庁に報告させて頂いた、「日本におけるトラスト基盤の整備に係る調査研究最終報告書」の「7.3 官民共同規制の在り方 (案)」が参考になる見立てである。参考までに当該内容を以下に記載する。

日本におけるトラスト基盤の整備に係る調査研究最終報告書の 7.3 官民共同規制の在り方 (案)のサマリ

トラスト基盤の構築を推進するにあたって、官庁だけでなく民間の協力を得ることも必要であり、すでに世界各国で先進的にトラスト基盤を導入している国では、官民共同規制の在り方に関して、グローバルには①政府/行政主導型、②ハイブリッド型、③民間主導型の 3 パターンが存在する。この 3 パターンの官民共同規制の在り方は、互いに規制のコントローラビリティ/アジリティ、政府/行政の内製化が必要なケイパビリティ、立ち上げに係る期間、普及推進力にトレードオフがある。①政府/行政主導型は、普及速度やフェデレーション等を含め、コントローラビリティやアジリティは高い一方、政府/行政に必要とされるケイパビリティは大きく、立ち上げまでにかかる期間は長い。民間主導型は、政府/行政に必要とされるケイパビリティは限定的で、立ち上げにかかる期間は早い一方、普及は限定的になる可能性があり、コントローラビリティやアジリティも低くなる。ハイブリッド型はいずれも中程度である。

日本におけるトラスト基盤の普及に向けては、これらの特徴を踏まえるとハイブリッド型が望ましいと考える。我が国におけるハイブリッド型の官民共同規制として望ましいと思われるものをコントローラビリティ/アジリティ、政府/行政に必要とされるケイパビリティ、立ち上げ/普及推進の 3 つの観点から説明する。まずコントローラビリティ/アジリティの観点では、行政/各業界のユースケースを踏まえ、行政トップダウンではなくトラストニーズの優先度を加味した規制/ガイドライン作成を目指すことが望ましいと考える。技術革新や社会ニーズの変化に対しては、情勢に対して規制/ガイドラインを一定程度機動的に更新していく。次に政府/行政に必要とされるケイパビリティの観点では、サービスの設計・開発。運営について、行政内だけで賄う/取り込むことはハードルが高く、運営ガイドライン/認定基準等の会期薬の必要性を示した上で、政府からの委託ではなく民間主導での事業運営を目指すことが望ましいと考える。最後に立ち上げ/普及促進の観点では、トラストに関する認知向上や管轄省庁とタイアップした初期ニーズを満たすサービス実現等、トラストサービス市場形成のための一定の推進力を確保し、早期の普及実現を目指すことが望ましい。

官民共同規制の在り方の類型化

官民共同規制の在り方として、グローバルには①政府/行政主導型、②ハイブリッド型、③民間主導型の 3 パターンが存在する。それぞれに規制のコントローラビリティ/アジリティ、政府/行政の内製化が必要なケイパビリティ、立ち上げに係る期間、普及推進力にトレードオフが存在し、すでに世界各国で先進的にトラスト基盤を導入している国ではそれぞれのニーズに合わせてどの類型を採用するか決定している。

政府主導型は主にシンガポールやエストニアで採用されている類型であり、政府/政府機関が規制策定および eTS 認証基盤の整備・運用を担当する累計である、民間ベンダーは基板の実装支援または市場展開を部分的に担当する等、トラスト基盤の大部分を政府が担当する。民間主導型は、主にオーストラリアやノルウェー、アメリカで採用されている類型であり、特定民間企業・業界にて既に運用されているデジタル ID/eTS 基盤を活用する方式を採る。政府はサービス普及推進のための法整備やガイドラインを担当するに留まる。また、ハイブリッド型は EU やイギリス、トラストサービス導入初期のアメリカで採用されていた類型であり、政府/政府機関はガイドライン策定や

監査を主に担当する。基板の実装・運用は各ベンダーおよび地方政府が担当する形式で分業を行う。また政府の法規制策定のボードには民間ベンダーの識者を招聘し、早い段階から民間の巻き込みを実施する。

これら 3 類型を比較すると、政府主導型はアジリティ高く推進できる一方、内製を行うためのケイパビリティを獲得する難易度が高い。具体的には、組織・人材の育成/獲得が必須となる。一方、民間主導は早期実装が可能である者の独自規格化のリスクをはらんでいる。両者ともに大きなハードルがある形になるため、ハイブリッド型を基本として官民が持つケイパビリティ、国内のサービス環境等の条件を複合的に考慮し、官民共同の在り方を模索していく必要がある。

	政府主導型	ハイブリッド型	民間主導型
類型概要	• 政府/政府機関が規制策定及びeTS認証基盤の整備・運用を担当 • 民間ベンダーは基盤の実装支援または市場展開を部分的に担当	• 規制策定のボードに民間ベンダーの識者を招聘 • 政府/政府機関はガイドライン策定及び監査を主に担当、基盤の実装・運用は各ベンダー及び地方政府が担当	• 特定民間企業・業界にて既に運用されているデジタルID/eTS基盤の活用 • 政府はサービス普及推進のための法整備、ガイドライン整備を担当
法規制の作成主体	政府	政府	政府
ガイドライン作成主体	政府	官民共同	民間
基盤運営主体	官民共同/民間委託	官民共同/民間委託	民間
主な事例 ※ICANNのみ非トラスト領域の事例	• SingPass (シンガポール) - シンガポールの国民ID及び関連するトラストサービス • e-Estonia (エストニア) - エストニアの国民ID及び関連するトラストサービス	• eIDAS (EU) - EU加盟国共通でeID及びトラストサービスの法的効力を認める規則 • GOV.UK Verify (英) - 国内の民間デジタルID提供企業と連携しトラストサービスを提供 • ICANN (米) ※設立時 - インターネット上の識別子管理及びDNSルートサーバシステムの運用 - 2016年に民営化し民間主導の運営体制へ変更	• Digital iD (豪) - Australia Postが運営するデジタルIDサービス • BankID (ノルウェー) - 国内主要銀行が展開するデジタルIDサービス • PIV-AV (米) - 航空業界において機材部品やソフトウェアのIDと作業者の個人IDを紐づけた認証管理により業務コスト削減・セキュリティ向上
	行政・企業間取引の電子化・トラスト確保 政府IDによるサービス電子化	• Digital Identity Programme (ニュージーランド) - 政府自ら電子ID基盤を運営しつつ、民間基盤との相互運用に向けた法整備、およびガイドライン作りを推進	民間IDによる政府サービスの電子化

Source: BCG分析

156

ガイドライン (・法規制) に織り込む内容の検討

上記ロードマップにおける「ガイドライン (・法規制) に織り込む内容の検討」の参考として、主要な論点を以下のように整理した。ガイドラインの内容に当たるトラストに関するユースケース/リスク/要件/運用体制の定義や、トラスト概念の普及の方法の検討が肝要である認識である。

主要な論点	検討事項	初期仮説
トラストの概念を普及するための方法は？	• トラストの概念の定義 • トラストが必要な理由の明瞭な説明 • ガイドライン策定後の周知方法	• トラストはあらゆる信頼を表す概念のため、ガイドラインの対象となるトラストの定義が必要。本検討対象のガイドラインでは、改ざん・偽造防止のためのデータ証拠力の担保が対象 • 事実確認や作成元保証のため、トラスト確保が肝要 • デジタル臨調におけるデジタル化ガイドラインと併せて周知が良いか
想定するユースケースとリスクは何か？	• 特にトラストが求められる業界の提示 • トラストが求められるユースケースの例示 • ユースケースにおけるリスクの提示	• トラストニーズが高い業界と動画・画像データを利用しかつトラストが求められるユースケース、ユースケースにおけるリスクを**P49**にて整理
トラスト確保のために必要な要件は？	• トラスト確保手法の提示 • 必要なトラスト確保手法を選択するための資料の作成 • 手法実施のための詳細な要件の定義	• トラスト確保の手法及び選択のための表を作成**(P55~61)** • 電子署名法の実地調査のデジタル化を想定した、フレームワークの検証時に、フレームワークを使用する際の流れを整理**(P65)** • 手法実施のための詳細な要件は、デジタル化手法の詳細化と併せて今後検討する方針
トラスト提供のための運用体制は？	• 官民共同規制の形の定義 - 行政側の提供範囲の定義 - 事業者側の提供範囲の定義	• コントローラビリティ/アジリティの観点、政府/行政に必要とされるケイパビリティの観点、立上げ/普及推進の観点から官民協同規制のパターンの中でもハイブリット型を取るのが望ましいか - 政府/政府機関はガイドライン策定及び監査を主に担当、基盤の実装・運用は各ベンダー及び地方政府が担当