

# 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3月31日

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： エグゼクティブサマリ [1/2]

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

- アナログ規制のデジタル化で想定された手法の種類で動画・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
- 上記デジタル化の種類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
  - 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
  - 多くの海外事例ではデータの作成/送信/格納・利用までの機能を実装。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
- 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

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有

- 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
  - 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
- 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
- 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

# 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： エグゼクティブサマリ [2/2]

## ニーズの 分析・ 分類化、 課題の 整理

- 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
    - 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
  - 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データの作成・送信・格納/利用・流通で整理したところ、データ作成時と流通時にトラスト確保のニーズが存在
    - 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
  - 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  
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
- 短期：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
  - 中期：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の構築の実施
  - 長期：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の検討

# 本資料の内容

## ▶ 本プロジェクトの概要

動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

ニーズの分析・分類化、課題整理

トラストにおける脅威/不正の種類とトラスト確保手法の整理

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

トラストに係る社会的影響の調査

ロードマップの検討 (長期・中期・短期)

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

# 背景と実施方針



## これまでの経緯・取組み

### デジタル改革におけるトラストの役割

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

例)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

### トラスト基盤実現に向けたデジタル庁の取組み

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<sup>1</sup>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」<sup>2</sup>は、実態調査の中で挙げ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



## 今回の取組みの目的/実施方針(BCG理解)

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する

具体的には以下の調査研究を実施し、今後のマルチステークホルダーによる対応策検討のインプットとする

- 動画・画像等のデータ証拠力の現状分析
  - 国内外の先行研究及び事例の調査
  - ニーズ等の実態調査
- ニーズ・課題の分析・分類化
- ロードマップ(短期・中期・長期)の検討

1. 『トラストを確保したDX推進サブワーキンググループ報告書』(2022年7月)

2. 『デジタル社会の実現に向けた重点計画』(2022年6月)

## 仕様書の調査内容と本報告書の内容の対応 (1/2)

No	仕様書名称	活動成果	本資料との対応
4.2	動画・画像等のデータ証拠力の現状分析	<ul style="list-style-type: none"><li>デジタル臨調におけるアナログ規制のデジタル化類型を基点とし、動画・画像データの利用余地を整理</li><li>動画・画像データ利用余地のあるデジタル化類型において、海外先行事例の有無を調査<ul style="list-style-type: none"><li>(BCGには特に海外の事例調査に期待しているとお話があり、海外事例の調査を優先的に実施)</li></ul></li><li>海外先行事例調査において関心度の高い事例に対し、データフローを作成し、どのような種類のデータの改ざん・偽造リスクがあるか (=トラストのニーズがありうるか)を抽出</li><li>海外先行事例調査を通して抽出リスクを基に、データフローとリスクを生み出す主体を軸に取りリスクの類型化を実施</li></ul>	<ul style="list-style-type: none"><li>動画・画像等のデータ証拠力の現状分析 (公共・民間分野)<ul style="list-style-type: none"><li>国内外の先行調査/事例の整理・類型化</li><li>事例を基にしたリスクの類型化</li></ul></li></ul>
4.3	ステークホルダーからのニーズ等実態調査	<ul style="list-style-type: none"><li>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<ul style="list-style-type: none"><li>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と連絡を取り、現時点では第三者証明による厳格な証拠力のニーズは未確認であることをヒアリング</li><li>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連絡を取り、実施電子署名・タイムスタンプが動画・画像データへ使用されたケースが未確認であることをヒアリング</li></ul></li><li>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<ul style="list-style-type: none"><li>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</li><li>ユースケースにおいて、動画・画像データの活用余地をトラストのリスクを合わせて初期的に整理</li><li>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、各事業者から潜在的なニーズをヒアリング</li></ul></li></ul>	<ul style="list-style-type: none"><li>ステークホルダーからのニーズ等実態調査<ul style="list-style-type: none"><li>トラストニーズ有識者へのインタビュー</li><li>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掘</li></ul></li></ul>

## 仕様書の調査内容と本報告書の内容の対応 (2/2)

No	仕様書名称	活動成果	本資料との対応
4.4	ニーズの分析・分類化、課題の整理	<ul style="list-style-type: none"><li>海外先行事例調査を基に整理したデータフローと存在するリスクに対し、トラスト確保手法を作成し、単一/複数PFそれぞれに適したトラスト確保手法を検討</li><li>上記で作成したトラスト確保手法の内容を基に、アナログ規制の見直し対象かつ貴チームの手掌範囲である電子署名の実施調査のデジタル化における適切なトラスト確保手法を初期的に抽出</li><li>整理したトラスト確保手法を、想定されるデジタル化手法ごとに詳細化し表にすることで、今後のデジタル化におけるトラスト確保手法の判断に寄与</li><li>社会的影響(引き起こされる問題の影響や損失額)が定量的なものと定性的なものがあることを分析し、それぞれ医療業界における画像の偽造事例と自然災害時におけるデマ画像拡散事例を調査</li></ul>	<ul style="list-style-type: none"><li>ニーズの分析・分類化、課題整理<ul style="list-style-type: none"><li>トラストにおける脅威/不正の種類とトラスト確保手法の整理</li><li>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</li><li>トラストに係る社会的影響の調査</li></ul></li></ul>
4.5	具体的なロードマップの検討(長期・中期・短期)	<ul style="list-style-type: none"><li>アナログ規制への対応(短期)、データ流通(中長期)という2つの観点について、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</li><li>業務の特性からトラストのニーズが有りそうな業界において、動画・画像データのニーズがあるかをヒアリング<ul style="list-style-type: none"><li>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</li><li>ユースケースにおいて、動画・画像データの活用余地をトラストのリスクを合わせて初期的に整理</li><li>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</li></ul></li></ul>	<ul style="list-style-type: none"><li>ロードマップの検討(長期・中期・短期)<ul style="list-style-type: none"><li>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</li><li>ロードマップの策定</li></ul></li></ul>

# 本資料の内容

## 本プロジェクトの概要

### ▶ 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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



# 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

## 調査対象/調査内容に関する議論内容

---

### 調査対象について

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

- デジタル化ニーズ  
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
- トラストニーズ  
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  
⇒ 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? という見立てがある  
⇒ 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

### 調査計画について

- 以下両面で調査を進めていく
  - 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く調査
  - 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



- 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

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

#### ▶ 国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

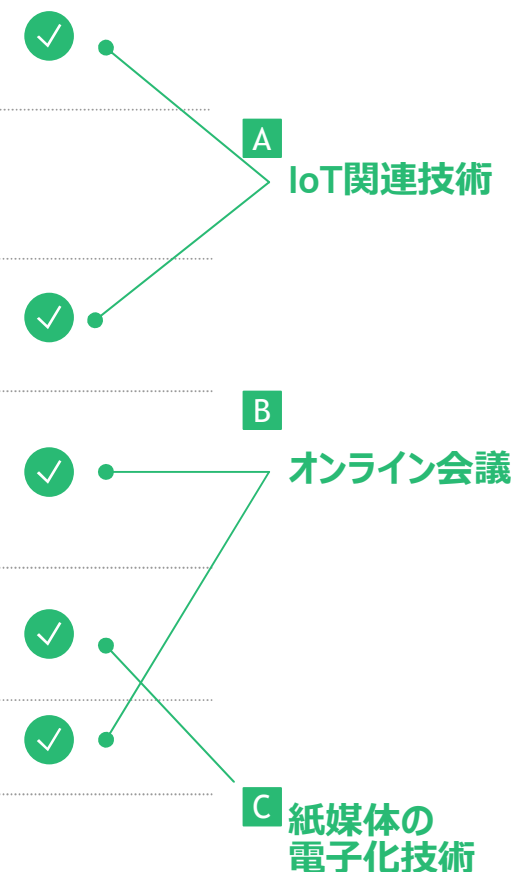
ロードマップの策定

# アナログ規制における動画・画像技術の利用余地は、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

## デジタル監調におけるアナログ規制のデジタル化類型

目的	使用する技術	見直しの概要	具体例
施設・設備等の破損/不備等の確認	ドローン、3D点群データ等を活用した構造物等の検査	 資格者等が現場で実施している検査について、ドローン、3D点群データ等を活用し、従前よりも効率的に不備・劣化に伴う損傷等をリモートで確認・検査を可能にすることで、法定検査等の効率化・省人化を目指す	<ul style="list-style-type: none"> <li>水道施設の目視点検</li> <li>火薬製造施設の完成・保安検査</li> </ul>
	センサー、AI解析等を活用した設備、車両、環境等の定期点検・測定	 資格者等が実施している設備、車両、環境等の定期点検・測定に係る一部の点検・測定項目について、センサーや通信機器等を用いた常時監視・測定により異常を検知可能にすることで、法定点検等の効率化を目指す	<ul style="list-style-type: none"> <li>消火器具、自動火災報知設備等の定期検査</li> <li>自動車の定期点検</li> <li>下水道等の水質の定期検査</li> </ul>
人・モノの動きを監視	監視カメラ、ドローン、画像解析技術、自動通報機能等を活用した人・モノの監視	 見張人等により実施している法定監視行為を監視カメラ、ドローン、画像解析技術、自動通報機能等を活用し、従前よりも網羅的かつ効率的に実施することを可能とすることで、法定監視行為の省人化・効率化を目指す	<ul style="list-style-type: none"> <li>火薬の発破の際の見張り</li> <li>船舶が行う見張り</li> <li>原子力関連施設における見張り</li> </ul>
業務・会計、衛生・安全管理等の状況の確認	オンライン会議システム等を活用した業務・会計等の遠隔検査、常駐・専任業務	 国等が実施している業務・会計に係る検査・調査や、専門職等が常駐し、施設等の衛生・安全管理を行う業務について、オンライン会議システム等を活用し、リモートで情報取得・判断可能にすることで、法定実地検査や常駐・専任業務の効率化を目指す	<ul style="list-style-type: none"> <li>業務・会計の状況、科目の要件合性、診療報酬の請求状況等の実地検査・調査</li> <li>法適合性確認のための立入検査</li> <li>高度管理医療機器等営業所管理者の常駐</li> </ul>
情報の提供	コピー防止、電子透かし技術等を活用したオンラインでの書類縦覧・閲覧	 公的機関等への訪問が必要とされている書面の縦覧・閲覧について、コピー防止、電子透かし技術等を活用し、オンラインで書面の縦覧・閲覧を可能にすることで、縦覧・閲覧業務の効率化を目指す	<ul style="list-style-type: none"> <li>純資産額規制比率 書面の縦覧</li> <li>業者名簿等の閲覧</li> </ul>
技能の習得	講習システム等を活用したオンライン講習	 対面にて実施されている講習について、システム等を活用し、講習申込、講習受講、受講修了証発行のプロセスを、指定場所に訪問することなく、完結することを促進する	<ul style="list-style-type: none"> <li>高圧ガスを扱う施設の災害防止講習</li> </ul>
申請・交付等	クラウド等を活用した申請・交付等の手続、文書の保存	 フロッピーディスク等の記録媒体を用いる行政手続等について、クラウドを利用した申請やクラウド上でのデータの作成・管理などを可能とすることで、行政・事業者双方の事務の効率化を促進する	<ul style="list-style-type: none"> <li>土壌の汚染状況についての報告書等の提出</li> <li>教育委員会における学齢簿の作成・保存</li> </ul>

動画画像  
データ利用余地



# 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

海外における、動画・画像のユースケースの幅出し (1/3)

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) 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)	

# 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

海外における、動画・画像のユースケースの幅出し (2/3)

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 of 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) <span style="float: right;">b</span>
		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) <span style="float: right;">c</span> 製油所・橋・トンネル等インフラ点検 (ドローン)

Source: 各種公開記事

# 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

海外における、動画・画像のユースケースの幅出し (3/3)

デジタル化手法	業界名	国名	事例概要		
オンライン 会議等	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度の仮想体験を通じた遠隔監査 (VRヘッドセット)		
紙媒体の 電子化技術	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)		

## a 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

### シンガポールの建物検査とデジタル化に関する概況

---

#### 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

- 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
- 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
  - HDBが公共住宅、BCAがそれ以外の全ての建物の規制を担当
- 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

#### 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

- 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
- 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



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

## a 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

### 会社概要

会社名	<ul style="list-style-type: none"> <li>Garuda Robotics</li> </ul>
設立年	<ul style="list-style-type: none"> <li>2013年</li> </ul>
事業展開国	<ul style="list-style-type: none"> <li>シンガポール</li> </ul>
事業概要	<ul style="list-style-type: none"> <li>自律型ドローンシステムを活用したデジタル化</li> </ul>
デジタル化領域	<ul style="list-style-type: none"> <li>施設等の点検 (Facilities 4.0)</li> <li>人の監視 (Safe Distance)</li> <li>農作業の効率化 (Plantation 4.0)</li> <li>救急対応 (Garuda Responder)</li> </ul>
対象業界	<ul style="list-style-type: none"> <li>建設業</li> <li>農林水産業</li> <li>エネルギー業</li> <li>情報通信業</li> <li>運輸業、郵便業</li> <li>鉱業、採石業、砂利採取業</li> <li>行政サービス</li> <li>医療、福祉</li> </ul>
提供ソリューション	<ul style="list-style-type: none"> <li>3Dマッピング</li> <li>検査レポート</li> <li>保険調査</li> <li>フレアスタック調査</li> <li>農作物健康状態マッピング</li> <li>タワー検査</li> <li>施設点検</li> <li>ビデオ撮影</li> </ul>

### 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

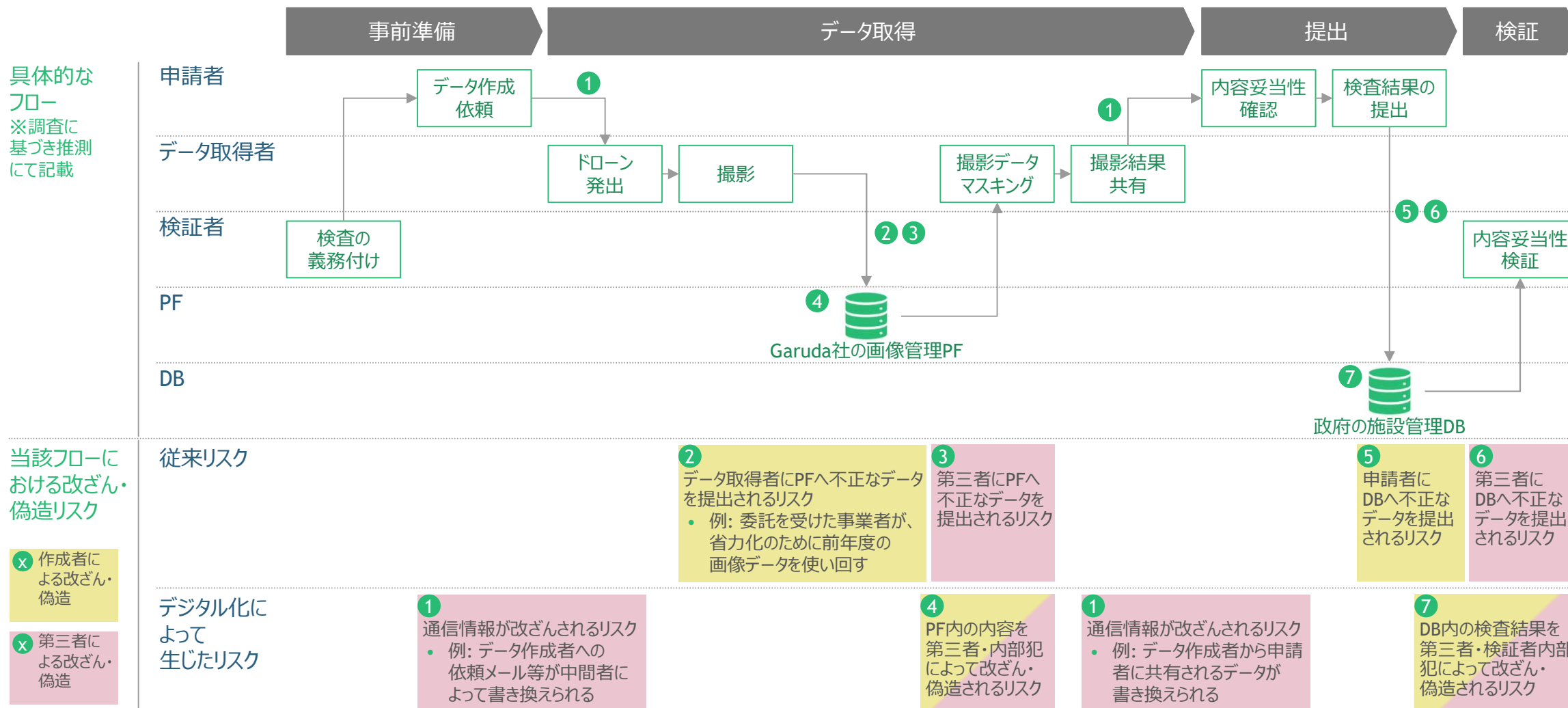
#### 人の監視のデジタル化

- 混雑度合をAIで判断・可視化する "SafeDistance"



## a Garuda Roboticsにおける、ドローンによる施設点検のフロー

前提情報 申請者がデータ取得者 (ドローン業者) にデータ作成業務を委託



# a Garuda Roboticsの事例では、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

発生し得る改ざん・偽造リスク

- ✗ 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

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)

1	通信路で依頼情報が改ざんされるリスク <ul style="list-style-type: none"> <li>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</li> </ul>	✓	<ul style="list-style-type: none"> <li>当局からの対策要請は無し</li> <li>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                             <ul style="list-style-type: none"> <li>- ISO27001の認証取得</li> <li>- ネットワークにおけるVPNの活用</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>従来より不正アクセスへの罰則を規定</li> <li>(当局による内容確認・検証は未実施)</li> </ul>
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 <ul style="list-style-type: none"> <li>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</li> </ul>		<ul style="list-style-type: none"> <li>当局からの対策要請は無し (当局はリスク要素とは認識)                             <ul style="list-style-type: none"> <li>- 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) に対応</li> <li>- 技術的な方法での対策の難易度・導入コストが高い</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>従来より虚偽申請・不正アクセスへの罰則を規定</li> <li>検査資格者が内容確認・検証・最終署名を実施                             <ul style="list-style-type: none"> <li>- 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</li> <li>- 当局は他業務との兼ね合いで、簡単な内容確認のみ実施</li> </ul> </li> </ul>
3	第三者にPFへ不正なデータを提出されるリスク <ul style="list-style-type: none"> <li>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</li> </ul>		<ul style="list-style-type: none"> <li>当局からの対策要請は無し                             <ul style="list-style-type: none"> <li>- 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) に対応</li> </ul> </li> </ul>	
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 <ul style="list-style-type: none"> <li>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</li> </ul>	✓	<ul style="list-style-type: none"> <li>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                             <ul style="list-style-type: none"> <li>- eDelivery/電子署名/タイムスタンプを活用</li> <li>- 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</li> </ul> </li> </ul>	
5	申請者にDBへ不正なデータを提出されるリスク <ul style="list-style-type: none"> <li>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)</li> <li>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</li> </ul>		<ul style="list-style-type: none"> <li>2と同様</li> </ul>	
6	第三者にPFへ不正なデータを提出されるリスク <ul style="list-style-type: none"> <li>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</li> </ul>		<ul style="list-style-type: none"> <li>3と同様</li> </ul>	
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 <ul style="list-style-type: none"> <li>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</li> </ul>	✓	<ul style="list-style-type: none"> <li>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                             <ul style="list-style-type: none"> <li>- タイムスタンプ等を活用</li> <li>- 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</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>従来より第三者の不正アクセスには罰則を規定</li> <li>建物崩壊時に担当した検査資格者への罰則を規定</li> </ul>

## b 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

### インドのATM取引と監視カメラ活用に関する概況

---

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

- 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
- 政府・当局間で対策を議論

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

- 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
- 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



上記のニーズを捉え、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

## b 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

### 会社概要

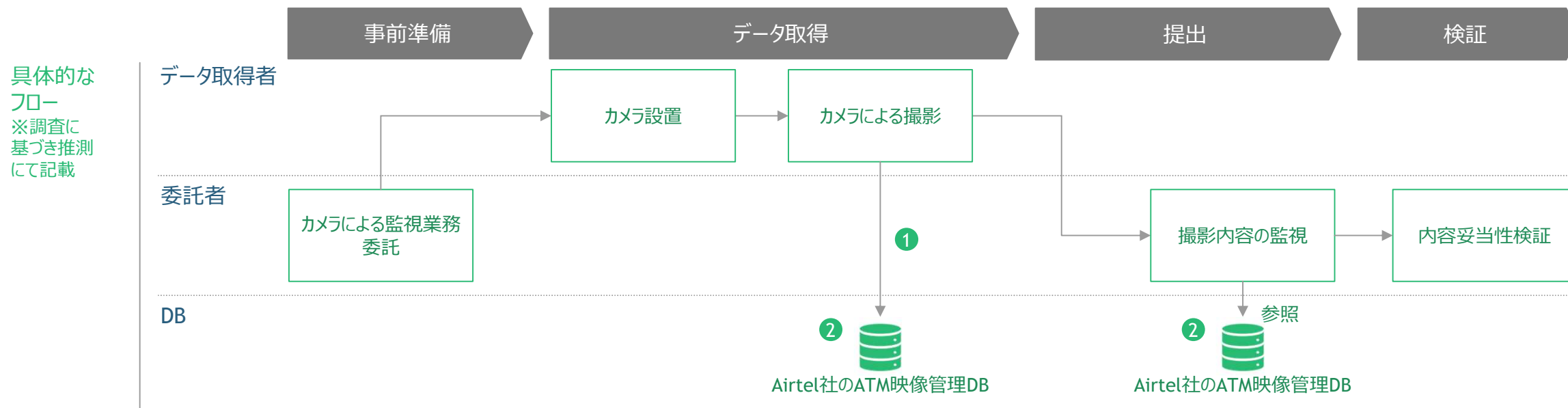
- |       |   |
|-------|---|
| 会社名   | <ul style="list-style-type: none"><li>• Bharti Airtel</li></ul>   |
| 設立年   | <ul style="list-style-type: none"><li>• 1995年</li></ul>   |
| 事業展開国 | <ul style="list-style-type: none"><li>• インド等18か国</li></ul>  |
| 事業概要  | <ul style="list-style-type: none"><li>• 通信ネットワークや多数のIoTソリューションを展開</li><li>• 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</li><li>• 映像管理ソリューションをATMの監視等に活用</li></ul> |

### 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

## b 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

前提情報 委託者 (ATM管理業者) がデータ取得者 (監視カメラ業者) にカメラによる監視業務を委託



当該フローにおける改ざん・偽造リスク

従来リスク

デジタル化によって生じたリスク

✕ 作成者による改ざん・偽造

✕ 第三者による改ざん・偽造

1 通信路で依頼情報が改ざんされるリスク

- 例: カメラからDBへの通信過程で、別の時間での映像等に差し替えられる

2 DB内の動画内容を第三者・内部犯によって改ざん・偽造されるリスク

- 例: 振り込め詐欺等の証拠を隠蔽したいDB内で該当する映像データを別の時間や別のATMの映像に差し替える

## b 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

発生し得る改ざん・偽造リスク

✕ 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

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)

### 1 通信路で依頼情報が改ざんされるリスク

- 例: カメラからDBへの通信過程で、別の時間での映像等に差し替えられる



- 当局からの対策要請は無し
  - 当局から銀行へ基準提示・監査・罰則を規定するが、委託先の詳細な技術手法は各銀行のシステムに依存するとの想定から未関与
- 自助努力としてサイバーセキュリティ強化を実施
  - ネットワークにおけるVPNの使用
  - 多要素認証の実施
- 一方、動画・画像自体のトラストは未確保
  - 動画撮影時に編集不能な形でタイムスタンプや位置情報を付与させる技術は未開発

- 従来より第三者による不正アクセスへは罰則が規定
- 企業間の委託契約書 (Request for proposal)にて、データ取得者の不正への罰則、セキュリティレベルに応じた賞与等を明記
  - 背景として、銀行は当局による罰則規定・監査の対象であり、末端の委託先に対しても睨みを利かせる必要
  - 銀行は当局提示のフレームワークを参照し委託先を選定

### 2 DBの動画内容を第三者・内部犯によって改ざん・偽造されるリスク

- 例: 振り込め詐欺等の証拠を隠ぺいしたい加害者が、DB内で該当する映像データを別の時間や別のATMの映像に差し替える



- 当局からの対策要請は無し
  - 当局から銀行への基準提示・監査・罰則規定は行うが、委託先の詳細な技術手法は各銀行のシステムに依存するとの想定から関与せず
- 自助努力としてサイバーセキュリティ強化を実施し、DB上のトラストは一定確保
  - AIによるDB上の疑惑行動検知・アラート機能を導入
  - DB上の全ての行動に対し、電子署名/タイムスタンプを適用
  - 多要素認証を実装



## c 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

### 循環型経済とGAIA-Xに関する概況

---

循環型経済はSDGsの実現に向けた有効な手段の一つ

- 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
- 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
- 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

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

- 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
- 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



産業別のプロジェクトにより具体構築が進められており、ドイツ主導です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



## c Catena-Xは動画・画像データやIoT機器の活用が見られる情報共有プラットフォーム

### 事例概要

#### 事例概要

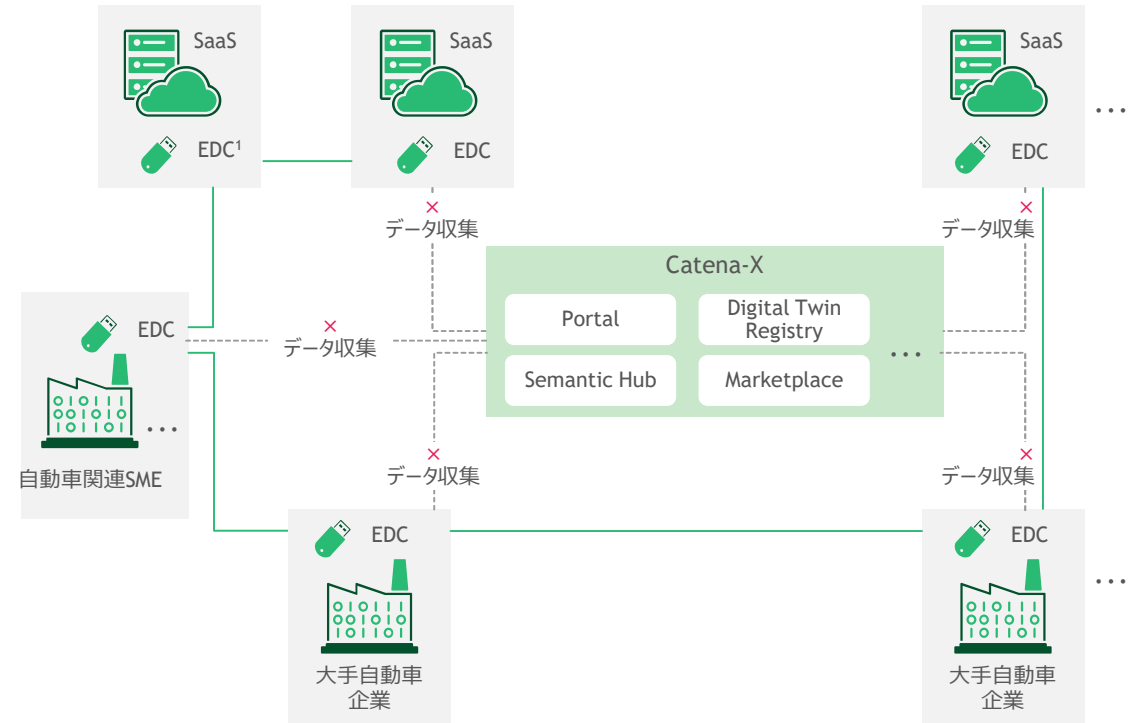
- Catena-Xはドイツ等の自動車業界ステークホルダーによる情報共有プラットフォーム
  - 動画・画像データやIoT機器の活用も見られるプラットフォームであり、一定のトラスト担保を実現
- 自動車メーカー・部品サプライヤ・ソフトウェアプロバイダー・販売業者が参加
  - SAP・シーメンス等のソフトウェアプロバイダーが構築を主導しており、行政の関与は限定的
  - (Catena-XのベースであるGAIA-Xにおいて、行政が法規制・財源面の関与を実施)
  - 現時点での主なデータ入力・活用者は自動車メーカー・部品サプライヤであり、消費者のデータ活用は検討中
- 自動車メーカー・部品サプ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







## c 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

### 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

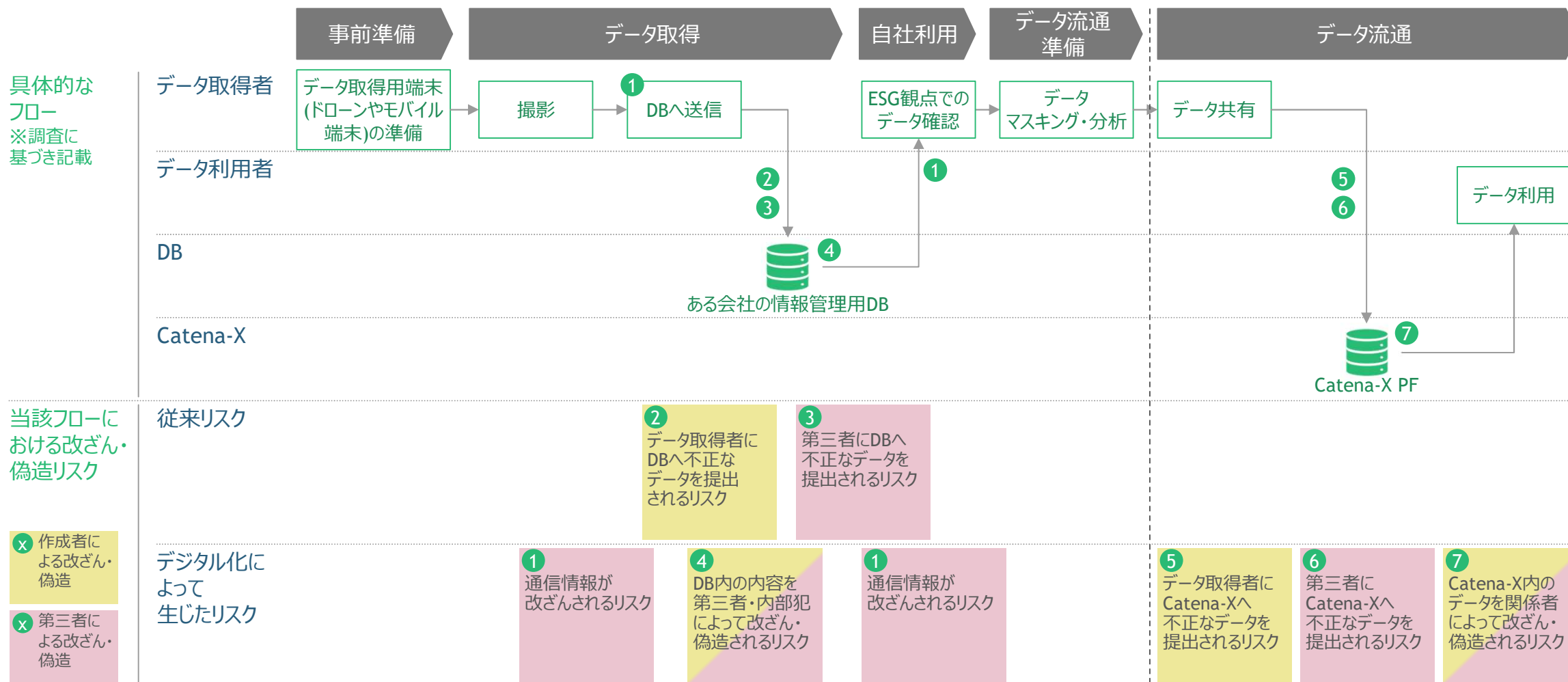
- AIによる動画・画像の異常・偽造検知
  - データ取得者・申請者に不正なデータを提出されるリスク (工場内画像の産業廃棄物排出部分をフォトショップで削除してからデータを提出される等) に対応
- 動画・画像へのタイムスタンプ・電子署名・位置情報の付与
  - データ取得者・申請者に不正なデータを提出されるリスク (児童労働が行われていない類似施設や別の時間のデータを提出される等) に対応

### 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



# c 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





# c 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

## 発生し得る改ざん・偽造リスク

- ✕ 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

## 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)

	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)
データ作成・自社利用	1 通信情報が改ざんされるリスク 例: ドローンからDBへの通信過程で別の時間の映像に改ざんされる	✓	<ul style="list-style-type: none"> <li>通信路へのサイバーセキュリティを強化                             <ul style="list-style-type: none"> <li>HTTPSやSSLを実装し通信路をセキュア化</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>(不正アクセスに関する各国の一般的な刑法で対応と想定)</li> </ul>
	2 データ取得者にDBへ不正なデータを提出されるリスク 例: 確認依頼を受けたサプライヤが、省力化のために前年度の動画データを使いまわす		<ul style="list-style-type: none"> <li>メタデータの真正性担保/動画・画像の偽造検知を実施                             <ul style="list-style-type: none"> <li>DB上でID管理や動作に対するログ管理を実施</li> <li>IoT機器の機能により、一部の動画・画像データに対し、撮影時の電子署名/タイムスタンプ/位置情報を付与</li> <li>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</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>AIが算出したスコアが一定以下の動画・画像を管理者が確認し、改ざん・偽造有無を判断</li> </ul>
	3 第三者にDBへ不正なデータを提出されるリスク 例: サプライヤの児童労働を隠蔽したい第三者が、児童労働が行われていない他サプライヤの工場の動画にすり替える		<ul style="list-style-type: none"> <li>関係者/機器の身元保証を実施                             <ul style="list-style-type: none"> <li>DB登録前に4-8週間にわたる関係者への事前審査実施</li> <li>IoT機器の事前審査も実施し、IDに紐づく電子署名を通して、機器単位・会社単位での身元管理が可能</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>①と同様</li> </ul>
	4 DB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DB内のデータを改ざんする	✓	<ul style="list-style-type: none"> <li>DBへのサイバーセキュリティ強化を実施                             <ul style="list-style-type: none"> <li>DB内でID管理やアクセス制限を実装</li> <li>DB上の行動へのログの取得と監視を実施</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>(虚偽申請に関する各国の一般的な刑法で対応と想定)</li> <li>内部者には、利用規約で改ざん・偽造への処分を明記</li> </ul>
データ流通	5 データ取得者にCatena-Xへ不正なデータを提出されるリスク 例: 省力化のために前年度のデータを使いまわす	✓	<ul style="list-style-type: none"> <li>②、③と同様の内容を実施</li> </ul>	<ul style="list-style-type: none"> <li>②と同様</li> </ul>
	6 第三者にCatena-Xへ不正なデータを提出されるリスク 例: 競合他社が問題のある映像にすり替える	✓		<ul style="list-style-type: none"> <li>①と同様</li> </ul>
	7 Catena-X内のデータを第三者・関係者によって改ざん・偽造されるリスク 例: 自社の工場画像内の廃棄物排出部分を加工する	✓	<ul style="list-style-type: none"> <li>④と同様の内容をより厳格に実施                             <ul style="list-style-type: none"> <li>管理者であってもレポートの閲覧・確認権限以外は付与しない等、厳格なアクセス制限を実施</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>④と同様</li> </ul>

Source: エキスパートインタビュー、BCG分析

# (参考) 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

海外におけるフェイク動画・画像検知手法の幅出し

## 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  
(アルバーニー大)

- 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%

- 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
- 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
  - 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
- 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
- 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

# (参考) 顔写真以外だと、AIが生成した画像の検知は手法を開発済

## フェイク画像検知手法の例

### 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



## d 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

### アメリカの資格試験のオンライン化に関する概況

---

2020年10月~カリフォルニア州を含む18の州で司法試験をリモート開催 (全受験者がリモート受験)

- 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

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

- 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
- 本人以外によるなりすまして受験を防ぐ



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



## d Turnitin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

### 会社概要

会社名	<ul style="list-style-type: none"> <li>Turnitin           <ul style="list-style-type: none"> <li>前述のソリューションを提供するExamSoftを2020年に買収</li> </ul> </li> </ul>
設立年	<ul style="list-style-type: none"> <li>1998年</li> </ul>
事業展開国	<ul style="list-style-type: none"> <li>アメリカ</li> </ul>
事業概要	<ul style="list-style-type: none"> <li>オンライン学術支援ツールの提供</li> </ul>
提供ソリューション	<ul style="list-style-type: none"> <li>試験管理ツール:ExamSOFT</li> <li>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</li> <li>学術研究向け盗用・剽窃チェックツール 等</li> </ul>

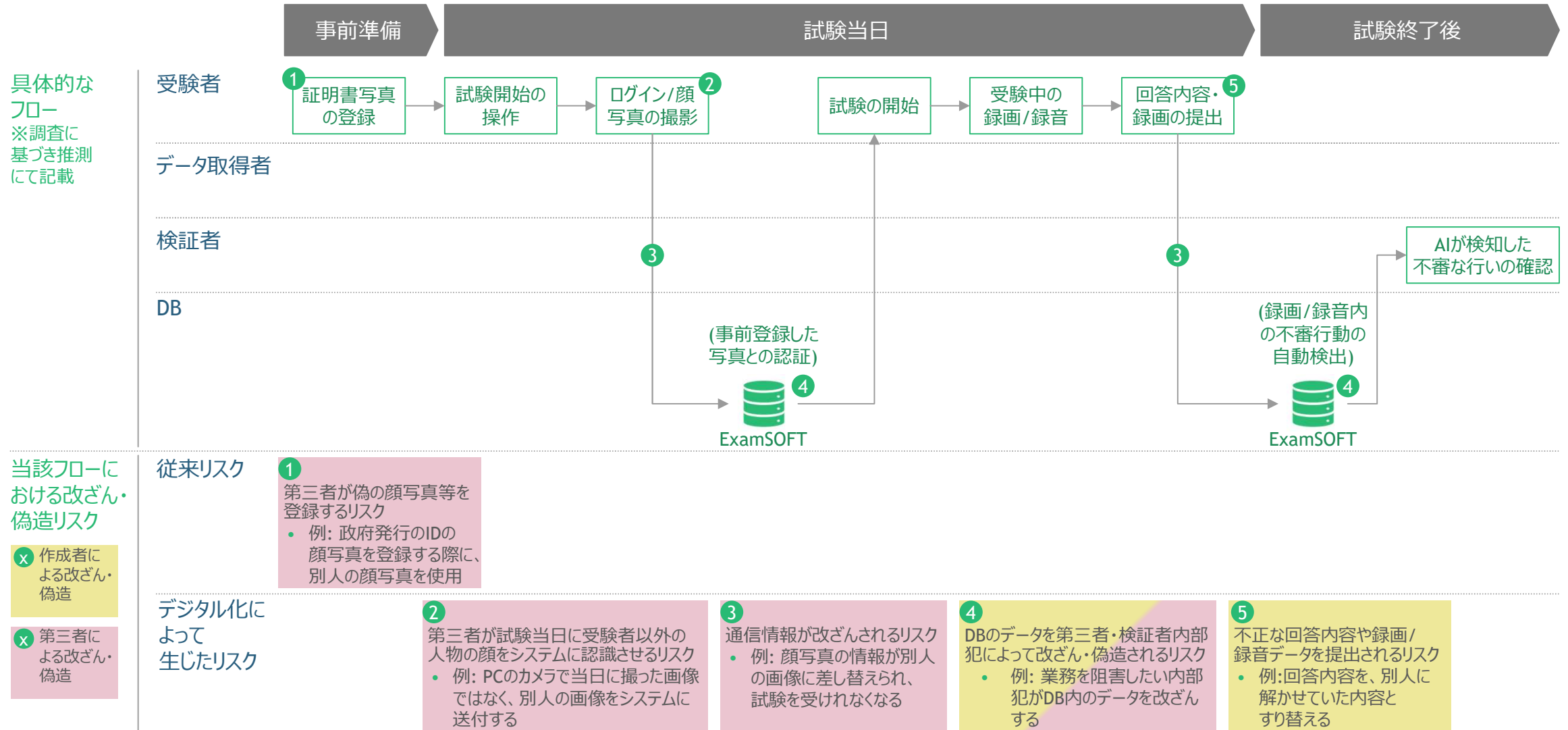
### イメージ

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



## d 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







## d 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

### 発生し得る改ざん・偽造リスク

- ✕ 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

### 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)

<p>1 第三者が偽の顔写真等を登録するリスク</p> <ul style="list-style-type: none"> <li>例: 政府発行のIDの顔写真を登録する際に、別人の顔写真を仕様</li> </ul>		<ul style="list-style-type: none"> <li>顔写真撮影による認証も実施することで二重チェック</li> <li>政府発行のIDの顔写真の登録が必須化</li> </ul>	<ul style="list-style-type: none"> <li>(なりすましに関する一般的な刑法により対応と想定)</li> </ul>
<p>2 第三者が試験当日に受験者以外の人物の顔をシステムに認識させるリスク</p> <ul style="list-style-type: none"> <li>例: PCのカメラで当日に撮った画像ではなく、別人の画像をシステムに送付する</li> </ul>		<ul style="list-style-type: none"> <li>ExamSOFTを立ち上げたPC上のカメラを使って顔認証する際、ExamSOFTの機能として「他のアプリケーションをすべて閉じていること」を確認できるため、改ざんの余地が大きく制限可能</li> </ul>	
<p>3 通信情報が改ざんされるリスク</p> <ul style="list-style-type: none"> <li>例: 顔写真の情報が別人の画像に差し替えられ、試験を受けられなくなる</li> </ul>		<ul style="list-style-type: none"> <li>一般的なサイバーセキュリティ対策を実施                             <ul style="list-style-type: none"> <li>顧客に関わるデータを紛失、誤用、不正アクセス、開示、改ざん、および破壊から保護するために合理的な予防措置を講じることをプライバシーポリシー上に明記</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>(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)</li> </ul>
<p>4 DB内のデータを第三者・検査者内部犯によって改ざん・偽造されるリスク</p> <ul style="list-style-type: none"> <li>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</li> </ul>			
<p>5 回答内容や、録画/録音データを改ざんするリスク</p> <ul style="list-style-type: none"> <li>例: 回答内容を、別人に解かせていた内容とすり替える</li> </ul>		<ul style="list-style-type: none"> <li>試験終了のタイミングで答案ファイルと共にビデオデータをアップロードさせ、改ざんする猶予を削減</li> <li>データの送信完了まで、ExamSOFT以外のアプリケーションの立ち上げ不可のため改ざんの余地が大きく制限</li> <li>ビデオデータについて、水や携帯等の禁止物品持ち込みや、不審な動きをAIを用いて検知しフラグ立て</li> </ul>	<ul style="list-style-type: none"> <li>AIがフラグを立てたビデオに関して委員が録画・録音を確認し、不正があったかを判断</li> </ul>



## e 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

### アメリカの公証人制度とデジタル化に関する概況

---

#### 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

- アメリカでは 印鑑証明という制度がない
- 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
  - 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、容易には浸透せず
  - 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
- 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
- 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



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



## e Notarizeはオンラインビデオを用いたオンラインでの公証を実施

### 会社概要

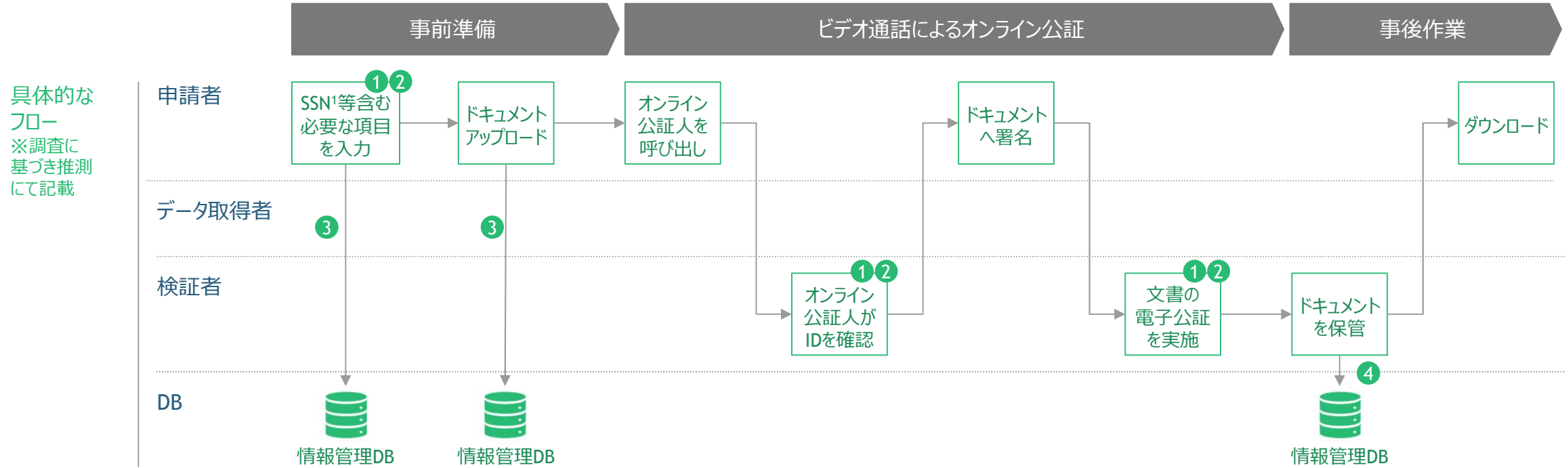
- 会社名
  - Notarize
- 設立年
  - 2015年
- 事業展開国
  - アメリカ
- 事業概要
  - 文書のオンライン公証を提供
  - コロナ禍の需要増加により、2021年春時点では、前年と比較し売上が600%増

### 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



# e Notarizeにおける、オンライン公証のフロー



当該フローにおける改ざん・偽造リスク

- ✕ 作成者による改ざん・偽造
- ✕ 第三者による改ざん・偽造

**従来リスク**

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

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

**デジタル化によって生じたリスク**

3 通信情報が改ざんされるリスク

- 例: 申請者の個人情報や中間者によって書き換えられる

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



## e 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

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	<p>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</p> <ul style="list-style-type: none"> <li>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</li> </ul>		<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>(虚偽申請等に関する一般的な刑法により対応と想定)</li> <li>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</li> </ul>
2	<p>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</p> <ul style="list-style-type: none"> <li>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</li> </ul>		<ul style="list-style-type: none"> <li>公証人の正当性を保証するための電子署名を発行                             <ul style="list-style-type: none"> <li>公証人が身元証明を完了した後に発行</li> <li>すべての公証人の身元が保障</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>
3	<p>通信路で依頼情報が改ざんされるリスク</p> <ul style="list-style-type: none"> <li>例: 申請者の個人情報が中間者によって書き換えられる</li> </ul>	<p>✓</p>	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>(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)</li> </ul>
4	<p>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</p> <ul style="list-style-type: none"> <li>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</li> </ul>	<p>✓</p>	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>③と同様</li> </ul>

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

➤ 事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

# 事例を基としたリスクの種類

## 考え方

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リスクの種類を定義

- 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

## リスク種類

リスク主体	作成	送信	格納・利用	流通
データ作成者を含む内部関係者	データ作成者を含む内部関係者に不正なデータを偽造されるリスク	なし	データ作成者を含む内部関係者にPFやDBの情報を改ざん・偽造されるリスク	関係者及び第三者によって、不正なデータを流通させるリスク (データ流通のフェーズでは関係者が急激に増加するため、関係者と第三者の違いが曖昧になると推測)
第三者	第三者に不正なデータを偽造されるリスク	第三者に通信路の情報を改ざんされるリスク	第三者にPFやDBの情報を改ざん・偽造されるリスク	

ここまで発展しているのは  
Catena-Xの事例のみ

# (参考) これまでのユースケースにおけるリスクのマッピング

事例	リスク	リスクタイプ	リスク主体	作成	送信	格納・利用	流通				
a ドローンによる 施設点検 (シンガポール)	a-1	通信路で依頼情報が改ざんされるリスク	データ 作成者を 含む 内部関 係者	a-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	なし	a-3	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	c-4	Catena-X内のデータを関係者によって改ざん・偽造されるリスク	
	a-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		a-4	申請者にDBへ不正なデータを提出されるリスク		a-5	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			
	a-3	第三者にPFへ不正なデータを提出されるリスク		c-2	データ取得者にDBへ不正なデータを提出されるリスク		b-2	DBの動画内容を第三者・内部犯によって改ざん・偽造されるリスク			
	a-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		c-5	データ取得者にCatena-Xへ不正なデータを提出されるリスク		c-4	DB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			
	a-5	申請者にDBへ不正なデータを提出されるリスク		d-5	回答内容や、録画/録音データを改ざんするリスク		d-4	DB内のデータを第三者・検査者内部犯によって改ざん・偽造されるリスク			
	a-6	第三者にDBへ不正なデータを提出されるリスク		e-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		e-3	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			
	a-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									
b ネットワークカメラによる ATMの監視 (インド)	b-1	通信路で依頼情報が改ざんされるリスク	第三者	a-3	第三者にPFへ不正なデータを提出されるリスク	a-1	通信路で依頼情報が改ざんされるリスク	a-3	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	c-7	Catena-X内のデータを関係者によって改ざん・偽造されるリスク
	b-2	DBの動画内容を第三者・内部犯によって改ざん・偽造されるリスク		a-6	第三者にDBへ不正なデータを提出されるリスク	b-1	通信路で依頼情報が改ざんされるリスク	a-5	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		
	c-1	通信情報が改ざんされるリスク		c-3	第三者にDBへ不正なデータを提出されるリスク	c-1	通信情報が改ざんされるリスク	b-2	DBの動画内容を第三者・内部犯によって改ざん・偽造されるリスク		
	c-2	データ取得者にDBへ不正なデータを提出されるリスク		c-6	第三者にCatena-Xへ不正なデータを提出されるリスク	d-3	通信情報が改ざんされるリスク	c-3	DB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		
	c-3	第三者にDBへ不正なデータを提出されるリスク		d-1	第三者が偽の顔写真等を登録するリスク	e-2	通信路で依頼情報が改ざんされるリスク	d-4	DB内のデータを第三者・検査者内部犯によって改ざん・偽造されるリスク		
	c-4	DB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		d-2	第三者が試験当日に受験者以外の人物の顔をシステムに認識させるリスク			e-3	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		
	c-5	データ取得者にCatena-Xへ不正なデータを提出されるリスク		e-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						
c 自動車産業 向け情報共有 プラットフォーム (EU)	c-1	通信情報が改ざんされるリスク									
	c-2	データ取得者にDBへ不正なデータを提出されるリスク									
	c-3	第三者にDBへ不正なデータを提出されるリスク									
	c-4	DB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									
	c-5	データ取得者にCatena-Xへ不正なデータを提出されるリスク									
	c-6	第三者にCatena-Xへ不正なデータを提出されるリスク									
	c-7	Catena-X内のデータを関係者によって改ざん・偽造されるリスク									
d e-learningによる オンライン司法 試験の替え玉 受験防止 (米国)	d-1	第三者が偽の顔写真等を登録するリスク									
	d-2	第三者が試験当日に受験者以外の人物の顔をシステムに認識させるリスク									
	d-3	通信情報が改ざんされるリスク									
	d-4	DB内のデータを第三者・検査者内部犯によって改ざん・偽造されるリスク									
	d-5	回答内容や、録画/録音データを改ざんするリスク									
e オンライン会議 システムによる オンライン公証 (米国)	e-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									
	e-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									
	e-3	通信路で依頼情報が改ざんされるリスク									
	e-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									



# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ➤ ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

# 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

## 現状分析からわかったこと

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

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



## 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掘する方向で、以下2つの方法でニーズを調査

- 1 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
  - 1-1 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
  - 1-2 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（内容は非公表）
- 2 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
  - 2-1 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
  - 2-2 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
  - 2-3 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（以下主なヒアリング事項）
    - 今後のデジタル化の展望及び動画・画像データの活用余地
    - 上記ユースケースにおける、動画・画像データの証拠力ニーズ
    - 上記ニーズを実現するために行政に求められる役割 等

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

#### ▶ 有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

## 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。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 弁護士エキスパートへのインタビュー結果

- 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い
  - 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
- 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る
  - 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
- 事実認識にデータが必要なユースケース=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
- 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
  - 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
  - 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



トラストニーズに知見のある  
弁護士

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

➤ 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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

# 「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

トラスト確保や、トラスト確保したデジタル化のニーズのある主なユースケース

凡例	BtoB BtoC BtoB/C	BtoG/GtoB GtoC/CtoG GtoB/C	個人の ニーズが 大きいもの	企業の ニーズが 大きいもの	★ 特に動画・画像の活用 余地がありそうなユース ケースと判断し、深掘
----	------------------------	----------------------------------	----------------------	----------------------	---

	関連する人が多く、海外でも先行してトラストが導入された主な業種/分野					その他
	行政	民間	準公共	準公共以外		
		医療・福祉	情報通信	運輸・郵便	金融・保険	
厳格な本人確認 が必要な申請/ 手続等	戸籍の届け出、 住民票の取得、 戸籍謄抄本の取得、 投票、 厚生年金保険の 保険料口座振替 申請	遠隔医療、★ 問診、 PHR	携帯電話/スマホの★ 契約、 レンタル/シェアリング サービス登録/利用、 年齢確認が必要な サービス等の登録/利 用	-	銀行口座の開設、★ 証券口座の開設、 保険の契約、 送金、 国際送金	-
内容の 非改ざん性/ 真正性が 必要な申請/ 交付/情報授受	住民票関連の申請、 運転免許証、 国際運転免許証、 後見登記等の申請、 旅券、 在留カード、 ワクチンパスポート、 自動車保管場所標章	健診/検査結果の 発行、 診断書の発行、 薬の処方、 カルテの作成・保管、★ 医療機関の間での 患者情報の連携、	マーケティングのための 顧客情報連携	通学定期の発行、 モビリティIoT (車両のデータ取得)	保険契約証書の 発行	社内での営業情報の 報告
法的証拠能力が 必要な文書/記録 等の作成・授受・ 保存	税務申告、★ 自動車関連の手続、 補助金等の請求、 年金関連の手続、 健保関連の手続、 労災関連の手続、 労働基準法関連の 届出 (36協定等)	治験データの作成・★ 保存・授受	★ ネット回線の契約、★ 有料放送の契約	国際物流関連の 手続 (通関等)	融資/ローンの契約、 貿易金融、 為替取引	不動産売買/賃貸★ 契約
	社外取引: 経費の精算、受発注書の取り交わし、契約書の取り交わし、請求書の授受、商品等のトレーサビリティ確保 社内記録: 会計帳簿の作成・保存、意思決定記録の作成・保存 (稟議、取締役会決議、株主総会決議等)、稟議・決裁 ... 規制対応: 他の法律等で定められた台帳・帳簿・記録等の作成・保存 (医薬品・医療機器の台帳、外国為替取引の本人確認記録等)					

鉱業、建設業、  
製造業、電気・  
ガス等、卸売・小売、  
宿泊業・飲食業等

Source: 個人向けアンケート調査 (n=4,406、2021/11/19~11/24実施)/企業向けアンケート調査 (n=347、2021/11/24~12/7実施)

## 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初期的に整理

		動画・画像のユースケース	想定されるリスク	
			リスクの種類	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、 <b>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</b>
		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、 <b>脱税を目的に偽造された画像が作成される</b>
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、 <b>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</b>
		製薬等のための治験データの実施	作成時	望ましい <b>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</b>
			格納・利用時	望ましい <b>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</b>
		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	<b>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</b>
	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、 <b>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</b>
		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、 <b>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</b>
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、 <b>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</b>
	金融・保険	保険の申請	作成時	保険金の搾取のため、 <b>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</b>
		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、 <b>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</b>

## 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(1/2)

	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 行政がマイナンバー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は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に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 <ul style="list-style-type: none"> <li>• 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</li> <li>• ExamSoft以外のPCアプリケーションの立ち上げの禁止</li> <li>• 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</li> <li>• 試験中の不審行動のAIでの監視</li> </ul>
	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 <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> </ul> 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 <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> </ul>



## 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(2/2)

	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
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おうが、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、 <b>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</b>
	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	<b>本人確認は基本的に実印の押印で実施されている</b> 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
	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、高額の場合保険業者が現地確認を実施している。 <b>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</b>
	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 <b>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</b>

# (参考)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

## 電子帳簿保存法について

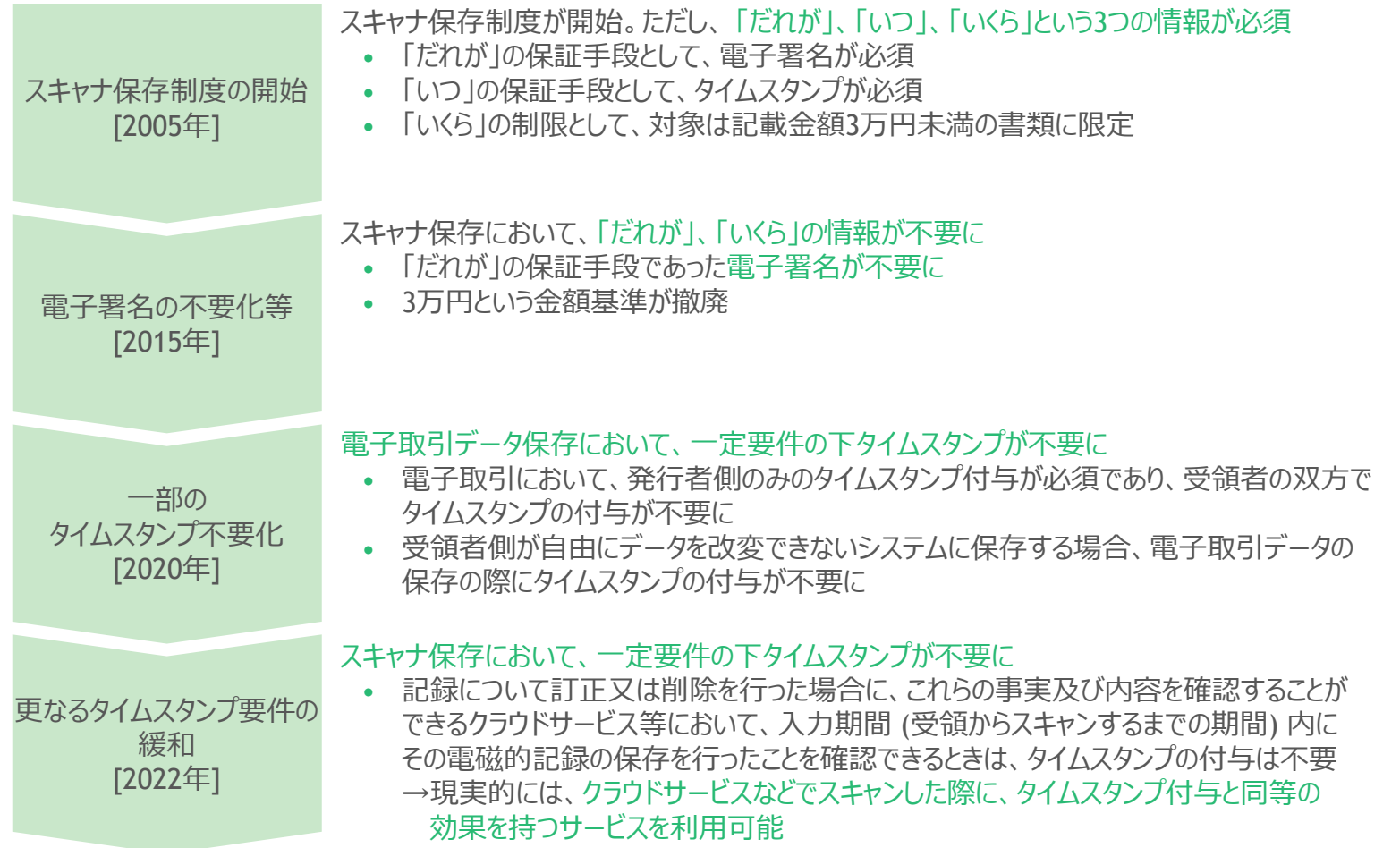
1998年より施行された、帳簿を電子保存できるように定められた法律

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

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

- 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

## 電子帳簿保存法の改正の流れ (電子署名・タイムスタンプに関わるところを中心に記述)



# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ➤ ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

#### ➤ 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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

# トラスト確保手法の類型化の考え方の整理

## 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

## i 事例を基としたリスクの類型

### 考え方

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リスクの類型を定義

- 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

### リスク類型

リスク主体	作成	送信	格納・利用	流通
データ作成者を含む内部関係者	データ作成者を含む内部関係者に不正なデータを偽造されるリスク	なし	データ作成者を含む内部関係者にPFやDBの情報を改ざん・偽造されるリスク	関係者及び第三者によって、不正なデータを流通させるリスク (データ流通のフェーズでは関係者が急激に増加するため、関係者と第三者の違いが曖昧になると推測)
第三者	第三者に不正なデータを偽造されるリスク	第三者に通信路の情報を改ざんされるリスク	第三者にPFやDBの情報を改ざん・偽造されるリスク	

ここまで発展しているのは  
Catena-Xの事例のみ

## ii 類型リスクへのトラスト確保手法の整理

### 考え方

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

- 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

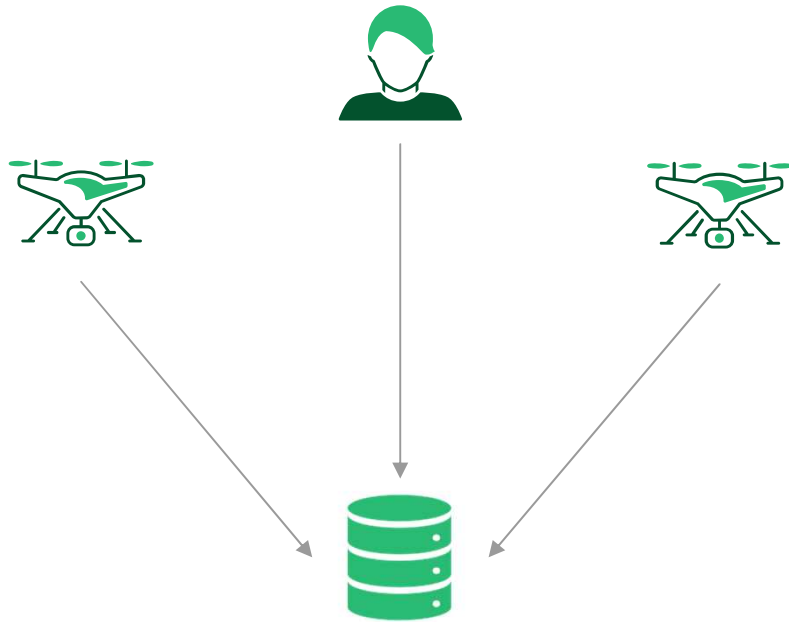
### リスク類型へのトラスト確保手法 ※緑字は狭義のトラスト

リスク主体	作成	送信	格納・利用	流通
データ作成者を含む内部関係者	<ul style="list-style-type: none"> <li>• メタデータの真正性担保による、データ証拠力の担保</li> <li>• 動画・画像データ自体の偽造検知/防止</li> </ul>	<ul style="list-style-type: none"> <li>• なし</li> </ul>	<ul style="list-style-type: none"> <li>• プラットフォーム(PF)/データベース(DB)のセキュリティ強化</li> </ul>	<p>作成時と同様の対策にて確保可能</p> <ul style="list-style-type: none"> <li>• メタデータの真正性担保による、データ証拠力の担保</li> <li>• 身元保証による、提供元の正当性担保</li> <li>• 動画・画像データ自体の偽造検知</li> </ul>
第三者	<ul style="list-style-type: none"> <li>• 身元保証による、提供元の正当性担保</li> </ul>	<ul style="list-style-type: none"> <li>• 通信路のセキュリティ強化</li> </ul>		

● 単一のPFで実現されることが多い領域
 ● 複数のPFで実現されることが多い領域

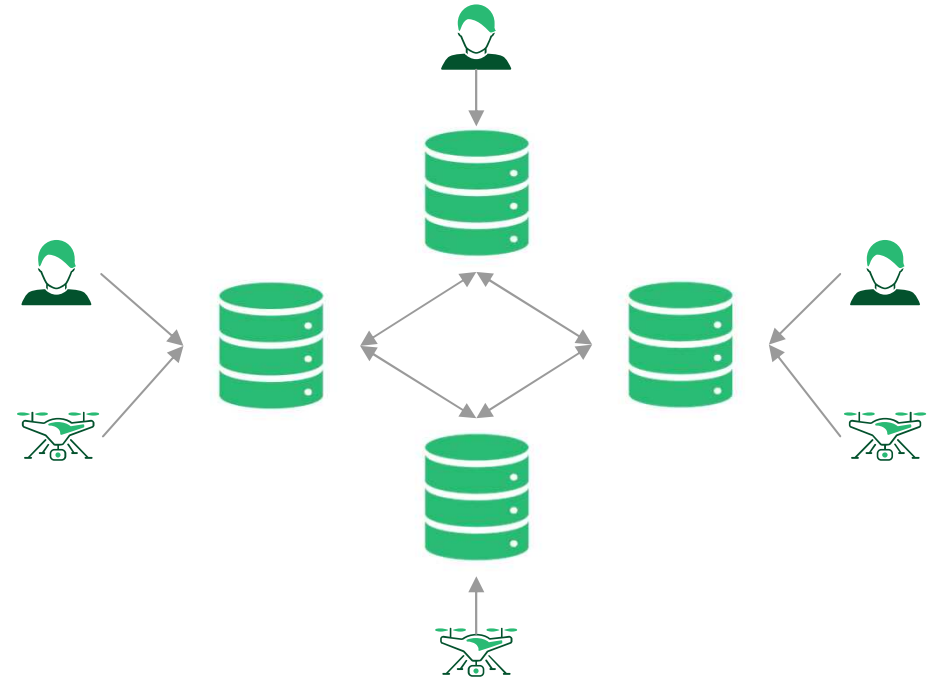
## ii (参考) 単一/複数PFのイメージ

### 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



## ii トラスト確保手法の詳細内容

### 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

メタデータの真正性担保による、  
データ証拠力の担保

#### 技術的な対応

- 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

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除外
- ログの取得と監視の実施 等

#### その他の対応 (含む、法整備)

- 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

## ii デジタル化を実施する際にトラスト可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(1/2)

データ作成時のリスク

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
ドローン等のIoTデバイスを用いた無人確認	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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> </ul>
アナログ規制例 <ul style="list-style-type: none"> <li>水道施設の目視点検</li> <li>火薬製造施設の完成・保安検査</li> </ul>	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偽造される	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>
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	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  オンライン会議に別人が対象者になりすまし出席する	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>Deepfake対策ツールといった偽造を検知するツールの導入</li> </ul>
アナログ規制例 <ul style="list-style-type: none"> <li>業務状況、科目の要件合性等の現地検査・調査</li> <li>法適合性確認のための立入検査</li> </ul>	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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> <li>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</li> </ul>
事前に用意した、動画・画像  アナログ規制例 <ul style="list-style-type: none"> <li>会計の状況、診療報酬の請求状況等の現地検査・調査</li> </ul>	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  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偽造される	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>事前に用意した画像・動画データへ位置・時刻情報を付与</li> <li>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</li> </ul>
	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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>事前に用意した画像・動画データへ作成者情報を付与</li> </ul>

## ii 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(2/2)

	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	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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> </ul>
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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>通信路のセキュリティ対策を実施                             <ul style="list-style-type: none"> <li>- SSL/TLS、HTTPS、VPNによる通信路のセキュア化 等</li> </ul> </li> </ul>
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	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>DB/PFのセキュリティ対策を実施                             <ul style="list-style-type: none"> <li>- ID管理/アクセス制限の実装・ログの取得と監視の実施 等</li> </ul> </li> </ul>
		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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>DB/PFのセキュリティ対策を実施                             <ul style="list-style-type: none"> <li>- 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</li> </ul> </li> </ul>

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

➤ 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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

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

# 電子署名法におけるデジタル化の対象となる業務は、大きく実地調査部分の6項目

電子署名法における、デジタル化手法の洗い出し (1/2)

## 概要と法令内容

### 認定制度の概要

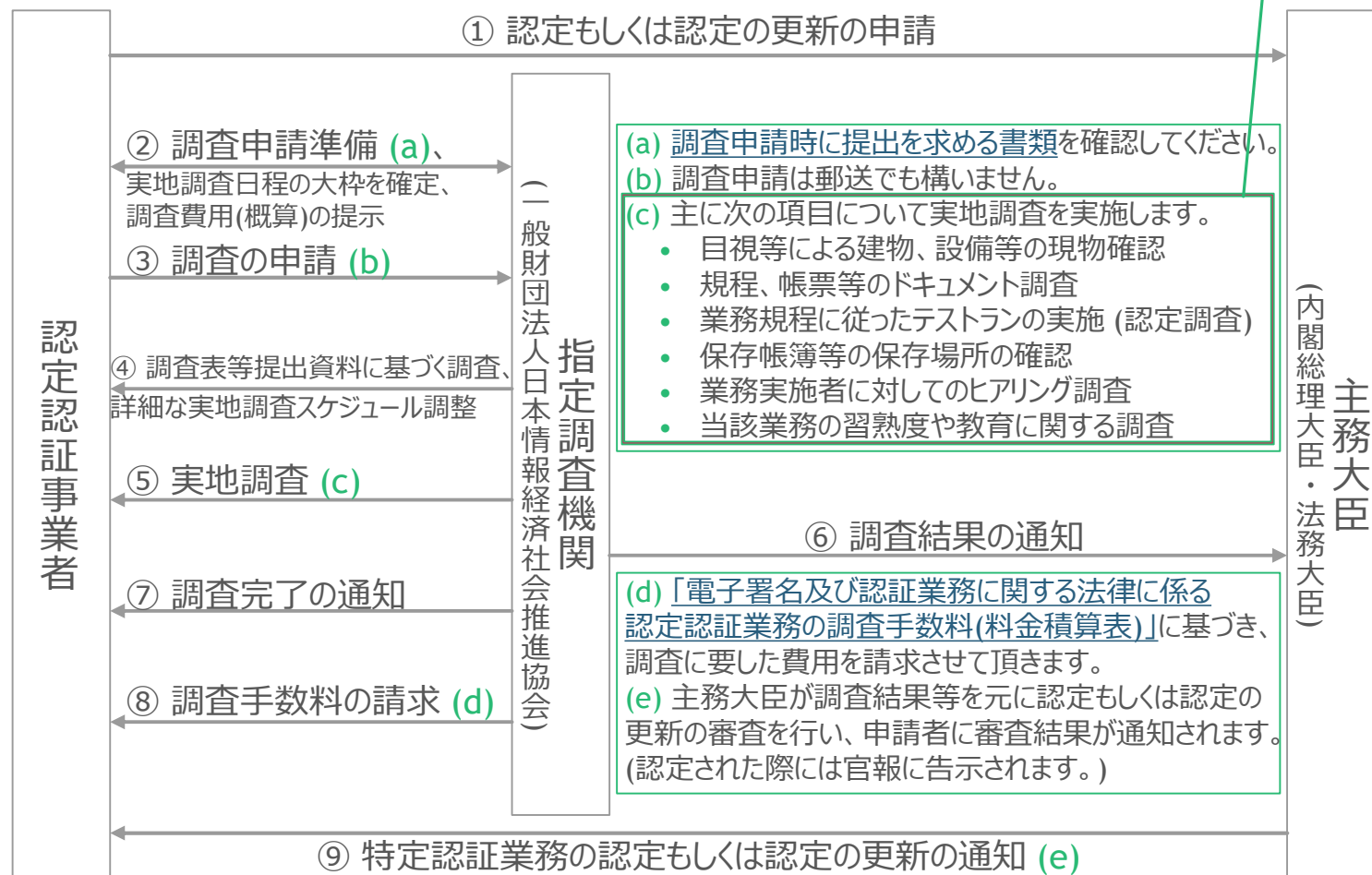
- 電子署名法が平成13年(2001年)4月1日から施行され、電子署名が手書きの署名や押印と同等に通用する法的基盤が整備
- 認証業務のうち一定の基準を満たすものは、国の認定を受けることができる制度が導入

### 当該法令の内容

- 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

## 認定是非の調査手順

デジタル化対象:実地調査部分



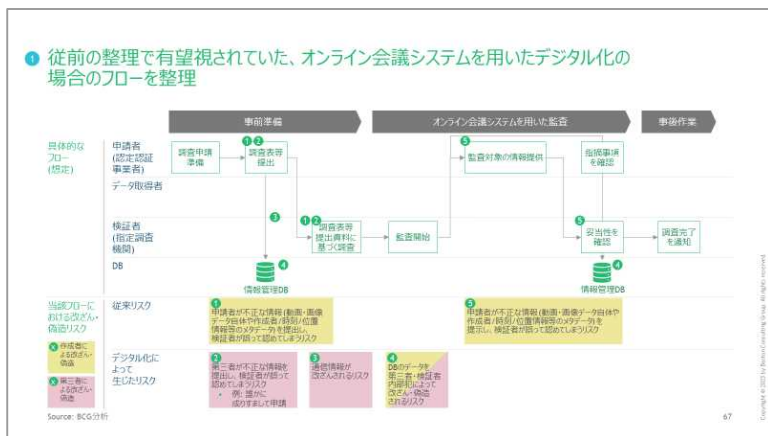
# 前述の現地調査の6項目は、3つのデジタル化の手法に整理

電子署名法における、デジタル化手法の洗い出し (2/2)

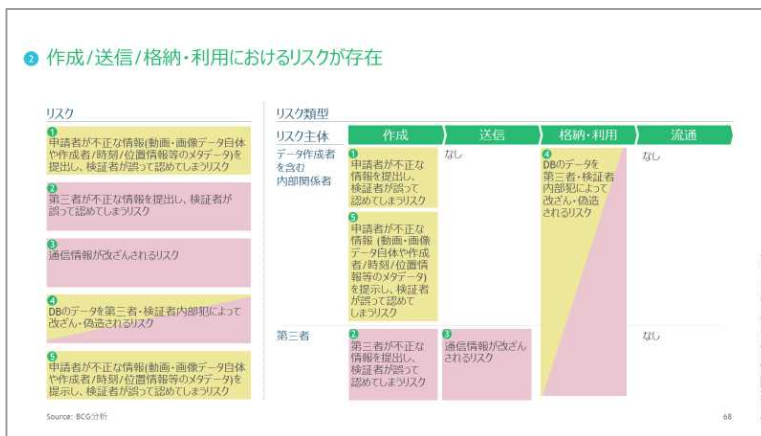
		現地調査の内容						アナログ規制 関連技術 との対応
		目視等による 建物、設備等の 現物確認	規程、帳票等の ドキュメント調査	業務規程に従った テストランの実施 (認定調査時)	保存帳簿等の 保存場所の 確認	業務実施者に 対しての ヒアリング調査	当該業務の 習熟度や教育に 関する調査	
デジタル化の手法と ニーズの達成度、 各業務での適用可否	低 無人	① ドローン等のIoTデバイスを用いた無人確認	✓		✓			A IoT 関連技術
	人の負担	② オンライン会議システムなどを用いた、リアルタイムでの人による確認	✓	✓	✓	✓	✓	B オンライン 会議 システム
	高 非リアルタイムかつ有人	③ 事前に用意した、動画・画像・書類データを提出し、確認	✓	✓		✓	✓	C 紙媒体の 電子化 技術

# 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

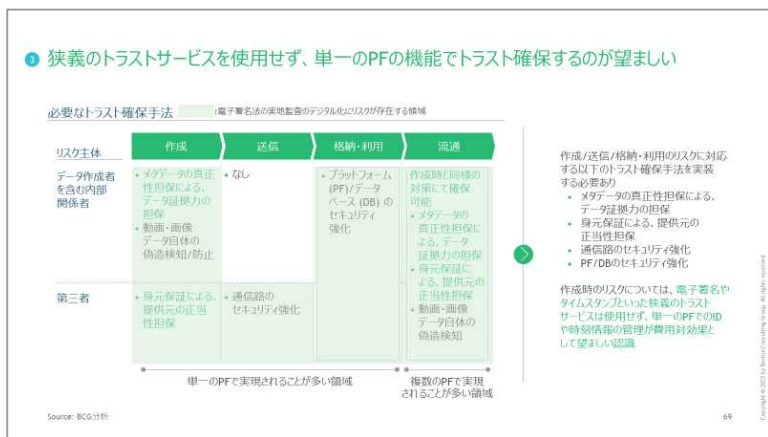
## 1 フローとリスクの整理



## 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



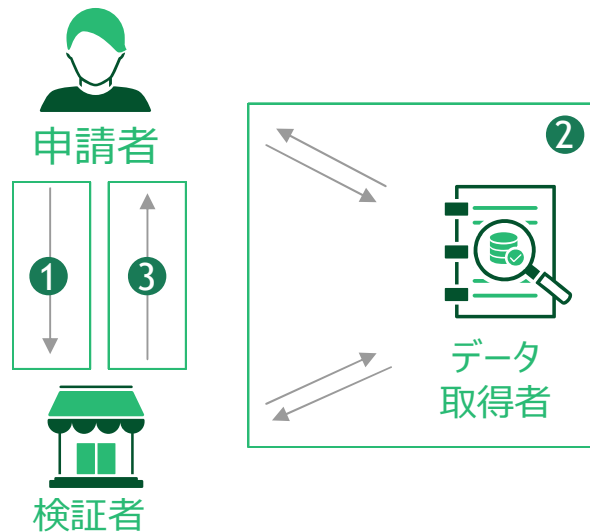
今後アナログ規制等の見直し等のデジタル化を実施する際も、同様の流れで必要なトラスト確保手法を判断できる認識

# 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が必要。申請者、データ取得者、検証者の3パターンに分岐

## 検証対象データの作成者のパターン

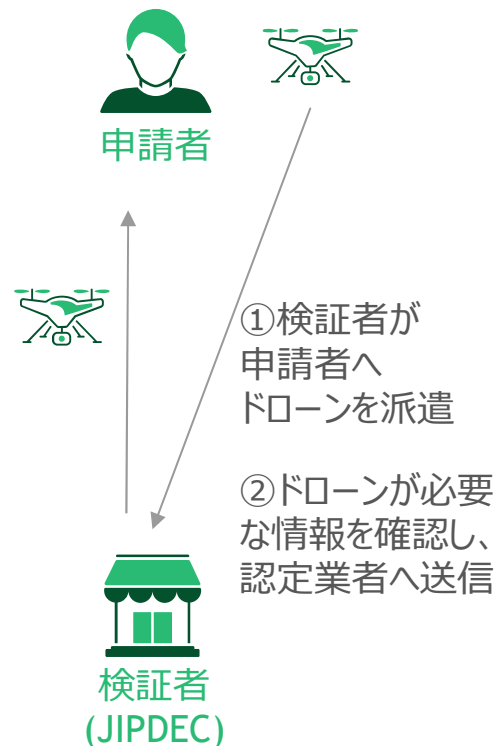
以下3パターンが存在

- ① 申請者が作成
- ② 申請者と検証者の仲介者としてのデータ取得者が別途存在し、データ取得者が作成
- ③ 検証者が作成



## 電子署名法のデジタル化手法における作成者パターン

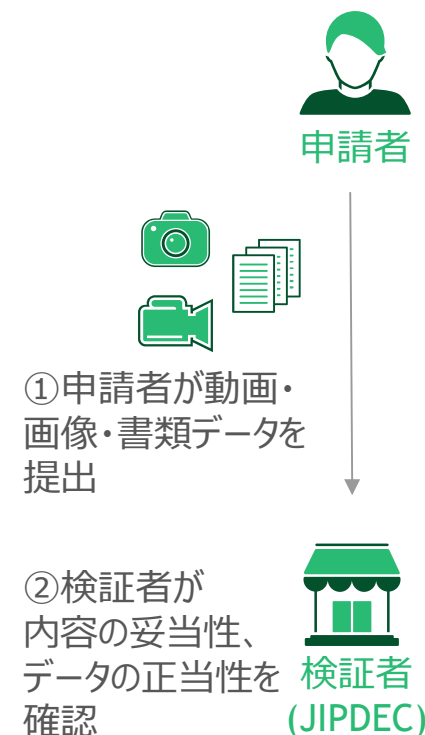
- ① ドローン等のIoTデバイスを用いた無人確認 (③のパターン)



- ② 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 (①のパターン)



- ③ 事前に用意した、動画・画像・書類データを提出し、確認 (①のパターン)

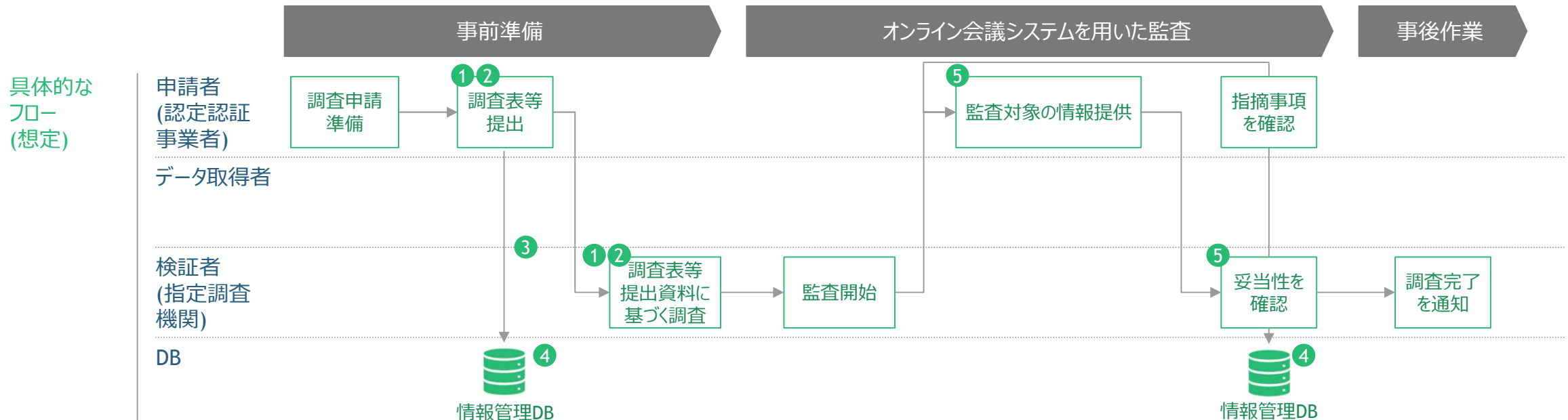




# 電子署名法における改ざん・偽造リスクを性悪説に基づき幅広く捉え、トラスト要否を評価

デジタル化手法	検証対象 データの作成者	改ざん・偽造リスク≒トラスト要否		改ざんされ得るデータ			
		作成者による改ざん・偽造	第三者による改ざん・偽造	動画・画像	メタデータ 作成者	時刻	位置
<b>XX: 電子署名法の事例に該当</b>							
IoT 関連技術 ① ドローン等のIoT デバイスを用いた無人 確認	申請者	無 • データの作成者 = データの検証者である ため	有 • 第三者が偽造した 不正なデータを検証者 に送り、システムを障害 する可能性有 • インターネットを介した 通信を行うため、 中間者攻撃等により、 改ざん・偽造の 可能性有	✓	✓	✓	✓
	データ取得者						
	検証者						
オンライン会議 ② 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	申請者	有 • 申請者に改ざん・ 偽造申告される 可能性有	有 • 第三者が偽造した 不正なデータを検証者 に送り、システムを障害 する可能性有 • インターネットを介した 通信を行うため、 中間者攻撃等により、 改ざん・偽造の 可能性有	✓	✓	(リアル タイムの ため)	✓
	データ取得者						
	検証者						
紙媒体の 電子化技術 ③ 事前に用意した、 動画・画像・書類 データを提出し、確認	申請者	有 • 申請者に改ざん・ 偽造申告される 可能性有	有 • 第三者が偽造した 不正なデータを検証者 に送り、システムを障害 する可能性有 • インターネットを介した 通信を行うため、 中間者攻撃等により、 改ざん・偽造の 可能性有	✓	✓	✓	✓
	データ取得者						
	検証者						

# ① 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整理



当該フローにおける改ざん・偽造リスク

- ✕ 作成者による改ざん・偽造
- ✕ 第三者による改ざん・偽造

従来リスク	①	②	③	④	⑤
デジタル化によって生じたリスク	申請者が不正な情報 (動画・画像データ自体や作成者/時刻/位置情報等のメタデータ) を提出し、検証者が誤って認めてしまうリスク	第三者が不正な情報を提出し、検証者が誤って認めてしまうリスク ・ 例: 誰かに成りすまして申請	通信情報が改ざんされるリスク	DBのデータを第三者・検証者内部犯によって改ざん・偽造されるリスク	申請者が不正な情報 (動画・画像データ自体や作成者/時刻/位置情報等のメタデータ) を提示し、検証者が誤って認めてしまうリスク

## 2 作成/送信/格納・利用におけるリスクが存在

### リスク

1 申請者が不正な情報(動画・画像データ自体や作成者/時刻/位置情報等のメタデータ)を提出し、検証者が誤って認めてしまうリスク

2 第三者が不正な情報を提出し、検証者が誤って認めてしまうリスク

3 通信情報が改ざんされるリスク

4 DBのデータを第三者・検証者内部犯によって改ざん・偽造されるリスク

5 申請者が不正な情報(動画・画像データ自体や作成者/時刻/位置情報等のメタデータ)を提示し、検証者が誤って認めてしまうリスク

### リスク類型

リスク主体	作成	送信	格納・利用	流通
データ作成者を含む 内部関係者	<p>1 申請者が不正な情報を提出し、検証者が誤って認めてしまうリスク</p> <p>5 申請者が不正な情報(動画・画像データ自体や作成者/時刻/位置情報等のメタデータ)を提示し、検証者が誤って認めてしまうリスク</p>	なし	<p>4 DBのデータを第三者・検証者内部犯によって改ざん・偽造されるリスク</p>	なし
第三者	<p>2 第三者が不正な情報を提出し、検証者が誤って認めてしまうリスク</p>	<p>3 通信情報が改ざんされるリスク</p>		なし

### 3 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

必要なトラスト確保手法 :電子署名法の実地調査のデジタル化にリスクが存在する領域

リスク主体	作成	送信	格納・利用	流通
データ作成者を含む内部関係者	<ul style="list-style-type: none"> <li>メタデータの真正性担保による、データ証拠力の担保</li> <li>動画・画像データ自体の偽造検知/防止</li> </ul>	<ul style="list-style-type: none"> <li>なし</li> </ul>	<ul style="list-style-type: none"> <li>プラットフォーム (PF) / データベース (DB) のセキュリティ強化</li> </ul>	作成時と同様の対策にて確保可能 <ul style="list-style-type: none"> <li>メタデータの真正性担保による、データ証拠力の担保</li> <li>身元保証による、提供元の正当性担保</li> </ul>
第三者	<ul style="list-style-type: none"> <li>身元保証による、提供元の正当性担保</li> </ul>	<ul style="list-style-type: none"> <li>通信路のセキュリティ強化</li> </ul>		<ul style="list-style-type: none"> <li>動画・画像データ自体の偽造検知</li> </ul>

●
●

単一のPFで実現されることが多い領域
複数のPFで実現されることが多い領域



作成/送信/格納・利用のリスクに対応する以下のトラスト確保手法を実装する必要あり

- メタデータの真正性担保による、データ証拠力の担保
- 身元保証による、提供元の正当性担保
- 通信路のセキュリティ強化
- PF/DBのセキュリティ強化

作成時のリスクについては、電子署名やタイムスタンプといった狭義のトラストサービスは使用せず、単一のPFでのIDや時刻情報の管理が費用対効果として望ましい認識

## 4 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 (1/2)

：電子署名法の実地調査のデジタル化にリスクが存在する領域

データ作成時のリスク

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
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 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偽造される	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>
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 オンライン会議に別人が対象者になりすまし出席する 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	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> </ul>
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 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偽造される 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	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> <li>事前に用意した画像・動画データへ作成者情報を付与</li> </ul>

## 4 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(2/2)

	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	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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> </ul>
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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> </ul>
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	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> </ul>
		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	<ul style="list-style-type: none"> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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除外・ログの取得と監視の実施 等</li> </ul>

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

### ➤ トラストに係る社会的影響の調査

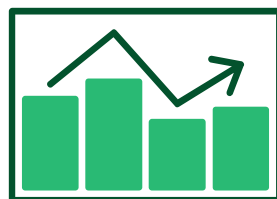
### ロードマップの検討 (長期・中期・短期)

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

# 社会的な影響には定量的なものや定性的なものがある

## 定量的な影響



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

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認識

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

## 定性的な影響



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

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認識**

台風による水害のフェイク画像に関する事例を調査





# 米医療業界で、画像の偽造により行政が数億ドルの損失を被り得る事案が発生

## 動画・画像の改ざん・偽造による社会的損失の事例

### 概要

- 米国医療業界の製薬臨床研究での、作成時の内部者による画像データ偽造に関する事例
  - 米製薬企業のアルツハイマー病薬の臨床実験にて、別実験の画像や同実験の別画像を複製して成果を際立たせた疑い
- 改ざんの有無を巡り、行政・研究誌出版社・製薬企業の三者間で泥沼化
  - 神経科学者が研究誌Science掲載の同研究の画像の異変に気づき、行政・出版社に告発
  - 行政は告発を受けた後の事後的対応に終始。「臨床報告段階における行政側の確認の不備が損失・混乱の原因」との言及有り
  - 出版社/製薬企業は、画像分析家や専門家に調査/弁護を依頼

### 損失額

- 同研究及び派生研究への支援額を合算すると、行政の損失は年間3億ドル以上となる見込み
  - 行政機関であるNIHは、同研究に数千万ドルの資金提供を実施
  - また、同研究はアルツハイマー分野において今世紀最も引用数が多い研究
  - NIHのアルツハイマー分野への年間支援額は2021年時点で2億8700万ドルに到達

## わかったこと・示唆

- 業界によっては、動画・画像の改ざん・偽造により間接的な損失も発生
  - 臨床研究のユースケースでは、当該研究だけでなく派生研究への支援額も社会的損失と解釈可能
- 動画・画像の改ざん・偽造による多額の損失や混乱を防ぐためには、行政側の技術的な対応や法規制対応が有用か
  - 行政が動画・画像の確認不備によって多額の損失を被る可能性が示唆
  - 対応として、AIによる偽造検知や他研究との照合機能等を活用した、確認の仕組み構築は行政で実施可能
  - 行政による厳罰化や、データの真正性を確認できるようなプロセスの策定も検討が必要か

# 台風による水害のフェイク画像により、社会的混乱が発生

## フェイク画像拡大による社会的混乱発生事例

### 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子会社の社員(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

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ➤ ロードマップの検討 (長期・中期・短期)

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

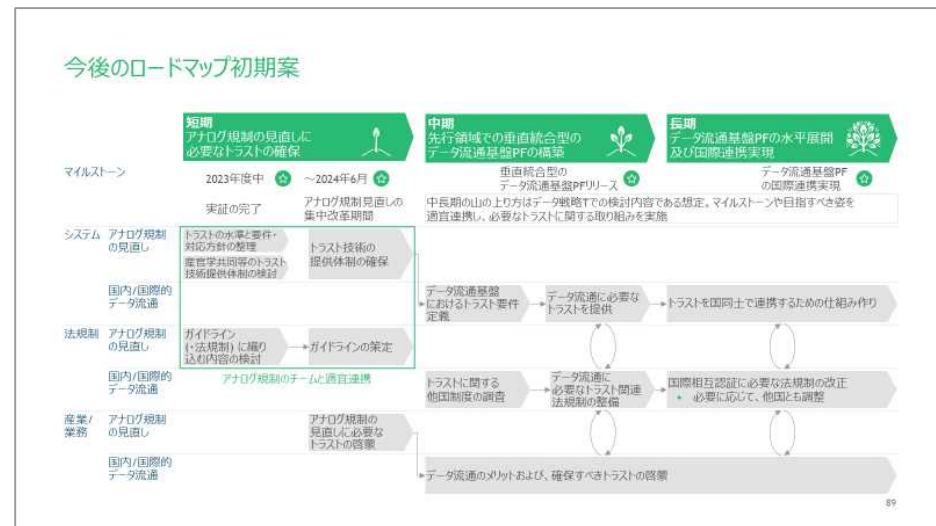
# 目指すべき姿と実現に向けた課題・ネクストアクションを整理したうえで、 目指すべき姿の実現タイミングとアクションの前後関係を踏まえてロードマップを策定

## 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

### 実施イメージ



## ロードマップの策定



### 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

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

### ロードマップの検討 (長期・中期・短期)

➤ 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

# 目指すべき最終形的设计 / 課題 / 必要なアクションの洗い出し(1/2)

## 社会として目指す姿 (BCG理解)

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

## 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

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
法規制	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
	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)

# 目指すべき最終形的设计 / 課題 / 必要なアクションの洗い出し(1/2)

## 社会として目指す姿 (BCG理解)

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

## 課題 (初期的) 緑字:トラスト関連

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

## 必要なアクション (初期的) 緑字:トラスト関連

- (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

システム

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

# 本資料の内容

## 本プロジェクトの概要

### 動画・画像等のデータ証拠力の現状分析 (公共・民間分野)

国内外の先行調査/事例の整理・類型化

事例を基にしたリスクの類型化

### ステークホルダーからのニーズ等実態調査

有識者へのインタビュー

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

### ニーズの分析・分類化、課題整理

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

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

トラストに係る社会的影響の調査

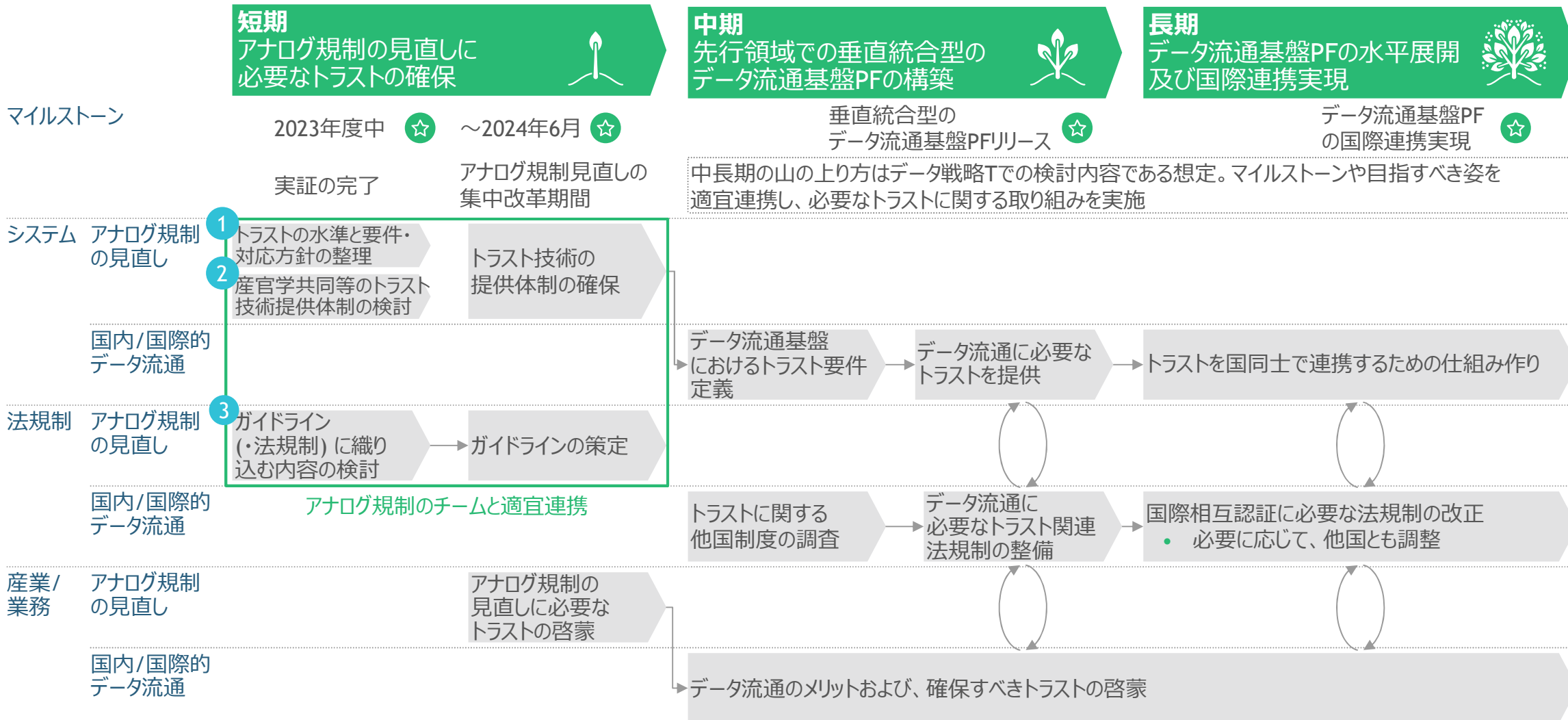
### ロードマップの検討 (長期・中期・短期)

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



# 今後のロードマップ初期案



# デジタル臨調でのアナログ規制の見直しの動きに合わせてトラストの水準と要件・対応方針の整理を実施する

## デジタル臨調でのアナログ規制の見直し

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

2023年4月～2024年3月までの期間にて、以下のような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

- 規制の見直しに必要な実証の実施
- 民間・公共に寄るデジタル導入の際に役立つ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

## 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

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

- デジタル臨調の事務局に対し、トラストに関する考え方／方針をご共有
- 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ご説明
- 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
- 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atalogの掲載要件に落とし込む



## 官民共同規制の在り方の事例 及び 初期案 [SWG議論用たたき台]

トラスト基盤/その他のデジタル基盤に関する官民共同規制の在り方としては、大別して3パターンある

- 政府/行政主導型: 政府や行政が規制やガイドラインを策定し、場合によりシステム開発や運営も行政の下で行う
- ハイブリッド型: 政府や行政が規制を行うが、ガイドライン策定やシステムの開発や運営は民間との協同により行う
- 民間主導型: 政府や行政は規制・監督は行うが、民間がガイドライン策定やシステム開発・運営を行う

上記では、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、立上げにかかる期間、普及推進力にトレードオフがある

- 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

日本におけるトラスト基盤の普及に向けては、上記の特徴も踏まえると、ハイブリッド型が望ましいのでは

- **コントローラビリティ/アジリティの観点:**  
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/ガイドライン作りを目指す。技術変革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
- **政府/行政に必要とされるケイパビリティの観点:**  
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/認定基準等の下位規約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
- **立上げ/普及推進の観点:**  
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

# システムや法規制を行政側がどこまで整備すべきかは、官民共同規制の形に依存する想定

	政府主導型	ハイブリッド型	民間主導型
類型概要	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>規制策定のボードに民間ベンダーの識者を招聘</li> <li>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</li> </ul>	<ul style="list-style-type: none"> <li>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</li> <li>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</li> </ul>
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 <span style="color: green;">民間IDによる政府サービスの電子化</span>
主な事例	<ul style="list-style-type: none"> <li><b>SingPass (シンガポール)</b> <ul style="list-style-type: none"> <li>シンガポールの国民ID及び関連するトラストサービス</li> </ul> </li> <li><b>e-Estonia (エストニア)</b> <ul style="list-style-type: none"> <li>エストニアの国民ID及び関連するトラストサービス</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>eIDAS (EU)</b> <ul style="list-style-type: none"> <li>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</li> </ul> </li> <li><b>GOV.UK Verify (英)</b> <ul style="list-style-type: none"> <li>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</li> </ul> </li> <li><b>ICANN (米) ※設立時</b> <ul style="list-style-type: none"> <li>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</li> <li>2016年に民営化し民間主導の運営体制へ変更</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><b>Digital ID (豪)</b> <ul style="list-style-type: none"> <li>Australia Postが運営するデジタルIDサービス</li> </ul> </li> <li><b>BankID (ノルウェー)</b> <ul style="list-style-type: none"> <li>国内主要銀行が展開するデジタルIDサービス</li> </ul> </li> <li><b>PIV-AV (米)</b> <ul style="list-style-type: none"> <li>航空業界において機材部品やソフトウェアのIDと作業員の個人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</li> </ul> </li> </ul>
※ICANNのみ 非トラスト領域の事例	<p style="color: red;">行政・企業間取引の電子化・トラスト確保</p> <p style="color: orange;">政府IDによるサービス電子化</p>	<ul style="list-style-type: none"> <li><b>Digital Identity Programme (ニュージーランド)</b> <ul style="list-style-type: none"> <li>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</li> </ul> </li> </ul>	

# トラストサービス実現に向けたフレームワーク基準の構成 (初期案)

担当機関	基準内容	デジタルIDに係る詳細内容	トラストサービスに係る詳細内容
<p>ポリシー策定者 (デジタル庁)</p>	<ul style="list-style-type: none"> <li>一般規定</li> <li>トラストサービスの定義</li> <li>アシュアランスレベル</li> <li>下位規則の規定</li> </ul>	<ul style="list-style-type: none"> <li>デジタルIDアシュアランスレベル (IAL/AAL)</li> <li>個人の身元確認/本人認証におけるリスクレベル</li> <li>評価とその保証プロセスの定義</li> </ul>	<ul style="list-style-type: none"> <li>トラストサービスの一覧/定義 eシール、タイムスタンプ、分散台帳 等</li> <li>各トラストサービスに関する下位規定の必要性 および基準策定の期日の定義</li> </ul>
<ul style="list-style-type: none"> <li>政府/民間事業者間の認証連携に関するインターフェース/運営事項の基準(FAL相当)</li> <li>国際相互連携に関するインターフェース/運営事項の基準(トラストアンカー/トラステッドリスト)</li> <li>各担当機関間のサービス連携イメージ、各トラストサービスの活用イメージ</li> </ul>			
<p>基準提供者 (トラスト フレームワーク プロバイダ)</p>	<ul style="list-style-type: none"> <li>各サービス事業者の運営/ 監督基準</li> <li>認定プロセス</li> <li>審査官の資格認定</li> </ul>	<ul style="list-style-type: none"> <li>欧州/シンガポールにおいては各加盟国政府によるIDプロバイダサービス提供が前提となる。 (国が認定/監査だけでなくサービス提供までの責務を負う)</li> <li>本取組においても、行政手続きや公共サービス等国民全体を対象としたサービスのための政府が管理するIDの活用を前提とする</li> <li>具体的なサービスとしては、JPKI/法人ID等マイナンバーと切り離れた仕組みの活用を念頭に、トラストサービス事業者と同等の要件を定義し、政府サービスとしてのトラストな運営を実現する。</li> </ul>	<p>トラストサービス事業者が遵守すべき要件</p> <ul style="list-style-type: none"> <li>設備要件、技術要件</li> <li>鍵管理要件</li> <li>運用要件</li> <li>監査要件</li> </ul> <p style="text-align: right; border: 1px solid black; border-radius: 10px; padding: 5px;">手塚教授ご提示のTAL相当</p>
<p>サービス事業者 (トラストサービス プロバイダ)</p>	<ul style="list-style-type: none"> <li>サービス事業運営の方針</li> <li>個人情報保護方針</li> </ul>		<ul style="list-style-type: none"> <li>上記基準で定められた運営基準に関する詳細各トラストサービスごとに異なる基準への対応詳細をどう吸収するかが論点</li> </ul>
<p>サービス受益者 (各業界団体)</p>	<ul style="list-style-type: none"> <li>業界横断でのトラストサービス活用範囲の定義</li> <li>サービス運営方針、各事業者の義務/受益内容の定義</li> <li>その他レギュレーション</li> <li>共通インターフェース定義</li> </ul>	<p>WIP</p> <ul style="list-style-type: none"> <li>トラストIDプロバイダー (マイナンバー) の活用方針、個人情報の利用目的の定義</li> <li>個人情報の取り扱いに係る基準 (利用許諾等)</li> </ul>	<p>WIP</p> <ul style="list-style-type: none"> <li>各業界で民間事業者で足並みを揃える箇所の定義</li> <li>トラストサービス事業者との役割分担の定義</li> </ul>

## 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

### 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

## (参考) デジタル臨調と、トラスト検討チームの間では「トラスト」という言葉が違う意味で活用 トラストの考え方

	「トラスト」の内容	対応するリスク
デジタル臨調での議論における「トラスト」	テクノロジーマップは規制官庁、規制実施主体、規制対象事業者等による調達や規制見直し等に影響を与えることを念頭に、掲載情報に一定の真正性/真実性 (トラスト) を確保する	技術利用者が、テクノロジーマップ掲載企業を活用した際に顕在化するリスク全般であり、データの取扱いに直結しないものを含む (以下に例示) <ul style="list-style-type: none"><li>技術保有企業から誤った/虚偽の技術情報が申告され、採用企業が想定した効果を得られない</li></ul>
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における「トラスト」	適正なデータ流通やデータ利活用の推進を行うための、データ証拠力を担保する (狭義のトラスト)	デジタル活用をした際に、取り扱うデータの信頼性・証拠力が毀損し、業務の目的が達成できなくなるリスク (以下に例示) <ul style="list-style-type: none"><li>目視等の規制をドローンでの点検で差し替えた際に、画像データが当事者/第三者に差し替えられ、適切な点検結果が得られなくなる</li><li>オンライン講習・試験棟、本人確認を行うプロセスにおいて本人の画像・動画が別人に差し替えられ、なりすましが発生する</li></ul>

臨調側で実証を広くご担当の大迫行政実務研修員からは一部の省庁では「データの改竄をどのように守るか」という検討実績があるが、省庁間でトラストの捉え方には温度差がある旨をヒアリング