デジタル化に伴う
トラスト確保の方策に関する考察

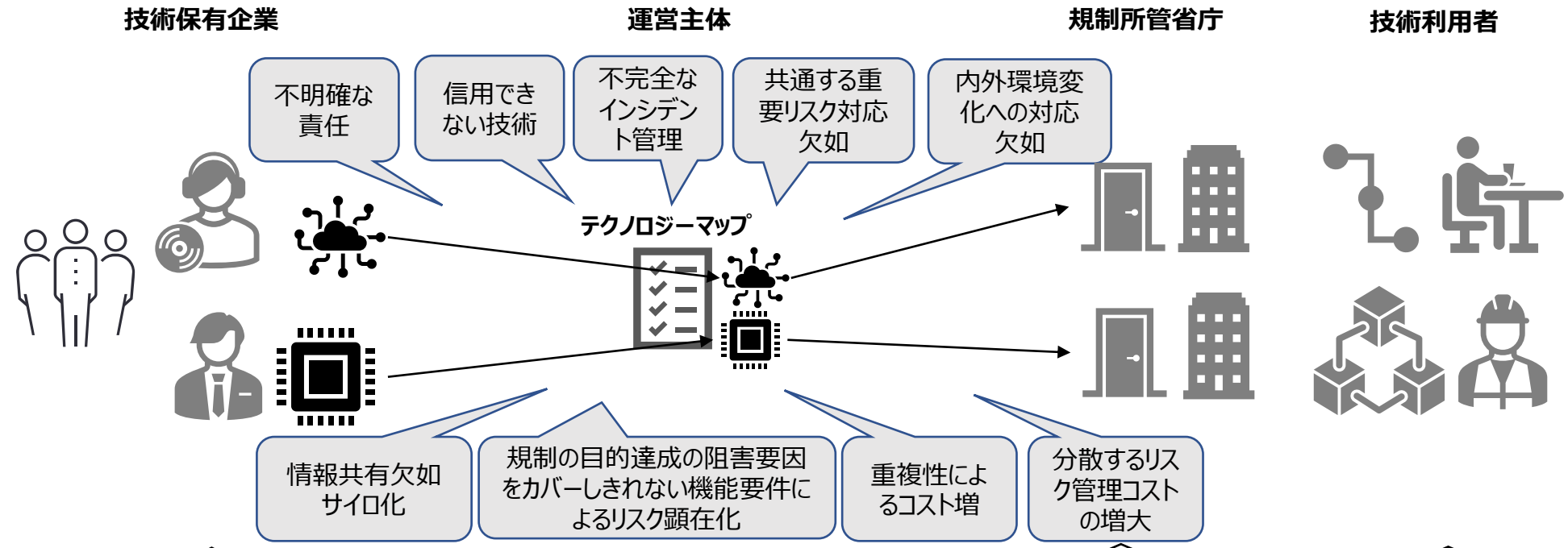
2023年2月9日

EYストラテジー・アンド・コンサルティング
公認会計士　小川恵子

1 トラスト確保に対する説明責任

テクノロジーマップの社会実装のため必須となるトラスト確保

■ トラストな仕組みがなければ各ステークホルダー、敷いては社会全体からの賛同が得られず、社会実装は困難



1

トラストな仕組みがなければ・・・
参加企業に対し社会的信頼がえられず、結果として参加する意義が棄損する

技術保有企業

2

トラストな仕組みがなければ・・・
規制所管省庁が積極的に利用できないデジタル化へのブレーキになる

規制所管省庁

3

トラストな仕組みがなければ・・・
安心して利用ができない

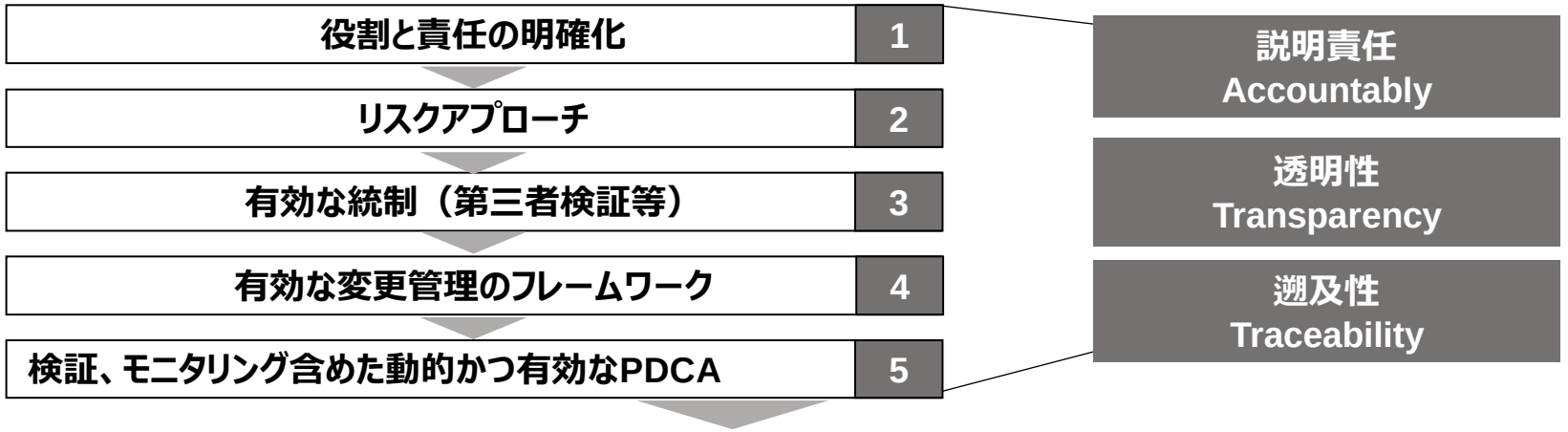
技術利用者

トラスト確保に対する説明責任

- １００%リスクがないと保証することはコストのみならず最新技術の進化のスピード、複雑化、専門性の限界から容易ではない
- 透明性、遡及性、説明責任を果たすことができるトラスト確保のため説明責任を果たせる枠組の構築が求められる

内外環境が非常に複雑で急速に変化しており第三者による時点の検証のみで継続的トラスト確保は限界

1	誰がどの様に役割と責任を負い、Trustedであるとの説明責任を果たすかが極めて重要
2	完全にリスクをゼロとすることができない前提で一定のリスクをテイクする枠組が必要
3	識別し評価したリスクに有効な統制が必要
4	リスクが顕在化した場合の最速の対応の枠組を併せて整備することが必要
5	デジタル技術は急速に進化しており、動的にTrustedであることを担保することが必要



0　トラストを確保する継続的で有効な仕組みをいかに構築するか

トラストの確保の枠組みは、変化のスピードへの対応が鍵

■ テクノロジーマップの社会実装のためのトラストを確保する仕組みは、一時点のものではなく動的（ダイナミック）に継続的に有効に機能しているが必要。

1 責任と役割

テクノロジー自身が原因で生じた問題の責任はだれが負うのか

2 継続的リスク管理

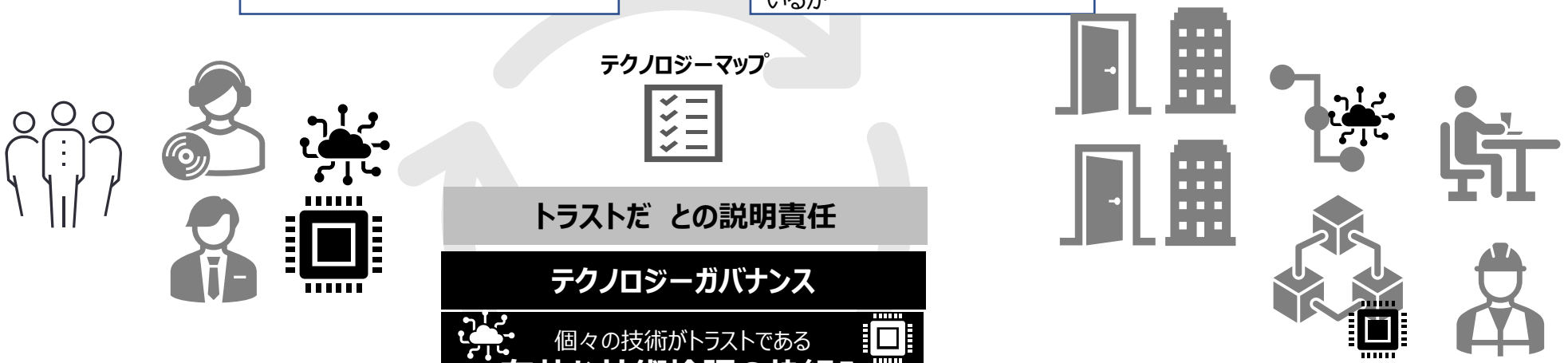
変化するな内外環境を鑑み、規制の目的の達成を阻害するリスクを機能要件がカバーしているか

技術保有企業

運営主体

規制所管省庁

技術利用者



テクノロジーマップ

トラストだ　との説明責任

テクノロジーガバナンス

個々の技術がトラストである

有効な技術検証の枠組み

3 技術検証

進化する技術の検証をいかに行うか

4 変更管理

変更事象が適宜反映される仕組みができているか

5 課題管理

課題は常時評価され適切な対応だなされているか

2 データ・テクノロジーガバナンスの潮流

昨今の　トラストに関するコンプライアンスの潮流

■ 昨今、内外事象が非常に複雑に急速に変化する状況下で、目的に照らしたトラストの確保は、従来の第三者による　監査、検証のみでは限界があり、企業自らの有効で一貫した透明性が高いガバナンスの構築責任が問われている

民間企業参考例：データガバナンスを事例にトラスト確保の枠組に関する動向

データガバナンスへの要請が高まる制度の変遷

1976	ロッキード事件を発端に1977海外不正支払防止法（FCPA） 1985年米国トレッドウェイ委員会「不正な財務報告」等公表
1992	COSOフレームワーク
2001	エンロン事件等受外部監査人監査の限界が露呈。 財務データに係る経営者宣誓責任を課す米国SOX法施行
2006	日本でも会社法改正、日本版SOX
2008	世界金融危機によりドッド･フランク法、ボルカールール施行 銀行の自己取引に係る経営者宣誓責任を課す
2013	BCBS239（リスクに係るデータガバナンス）、IIA 三つの防衛線（その後四つの防衛線）、改訂COSOフレームワーク
2014	米国OCC: Heightened Standard（データ管理含むリスク管理･ガバナンス･内部統制）“Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches”
	金融庁「主要行等向けの総合的な監督指針」にてメガバンクは2016年までにBCBS239対応要請
2017	AMLデータに係るデータガバナンス、経営者宣誓責任を求めるNYDFS 504
2019	COBIT 2019 Managed Data (APO14) 新規追加
	金融庁：AMLに関するガイドライン　⇒　AMLデータに係るデータガバナンス

■ 第三者検証の限界を補うため、有効な統制の整備運用を実現するガバナンスが重要視
■ コンプライアンスの世界では、経営者自身がガバナンス体制について重たい説明責任を負わされるケースが増えてきている

■ 財務諸表作成に関して有効な統制を整備運用していることに対し、経営者自ら宣誓責任を負わせるSOXコンプライアンスでは、経営者に刑事責任をも負わせている。
■ ボルカールール、AML関連ルール、FATCA含めて同様に、トラストであることを担保する有効な統制整備運用に関し経営者自ら重い説明責任を負わせている。
■ 昨今、米国OCCは、ガバナンスの枠組の脆弱性に対し某米銀に対し膨大な制裁金を課し始めている。

米通貨監督庁（OCC）

包括的なガバナンスの枠組、運用モデル、管理監督体制を最低でも整備すること。（OCC, V.(2)(b)）
■リスク管理機能に対する明確な役割、責任、説明責任を確立する。
■一貫性のある包括的な方針、手順、基準を確立し、その遵守を確実にする。

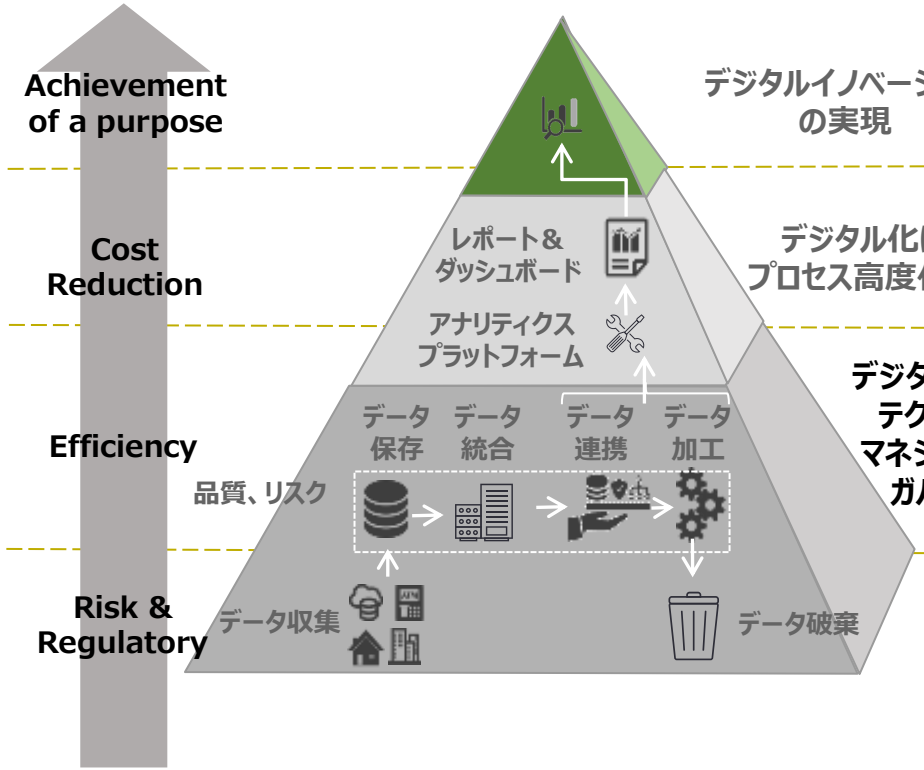
4億ドルの制裁金

トラスト確保のための方策が有効に機能している、という説明責任を、組織全体で果たすことが肝要

アナログからデジタル化を推進するガバナンス基盤

- 昨今、企業においても、IT依然することなく業務部門から自ら業務のデジタル化を実現するためにローコード・ノーコードツールを活用し、社員に広くDX案を募る「市民開発」といった枠組み検討されている。
- こうした企業のDX推進において、あらたなデジタル実装によるリスクをコントロールするためのガバナンス構築は、企業のデジタルトランスフォーメーションの上の鍵となってきている

キードライバー



Key Questions

攻め
- 目的は最適に実現しているか？
- 新たな価値を創造しているか？

- AS-ISからTO-BEが実現されているか？
- コスト削減、効率性は実現されているか？
- 課題は最も適切な方向に解決されているか？

- イノベーションを実現するための役割責任は明確か？
- 最適なテクノロジーを選択する枠組があるか？
- 動的に目的を達成し進化するためのPDCAがあるか？

守り
- 明確に目的を識別しているか？
- 目的達成のための良質で確実なデータを識別しているか？
- リスクが網羅的に識別されコントロールされているか？
- データ保持期間、証跡、非改ざん性は担保されているか？

3 データ・テクノロジーガバナンス

テクノロジーガバナンスの設計

- トラスト確保のための方策としては、明文化され周知された方針、手続きが必要
- トラスト確保のためのガバナンス体制は、内外に対し、透明性をもって説明責任を果たすことで、信頼を獲得する

ガバナンスフレームワーク例

COSO
INTERNAL CONTROL
– INTEGRATED FRAMEWORK

ISO 8000
Data Quality and
Enterprise Master Data

DAMA-DMBOK:
Data Management
Body of Knowledge

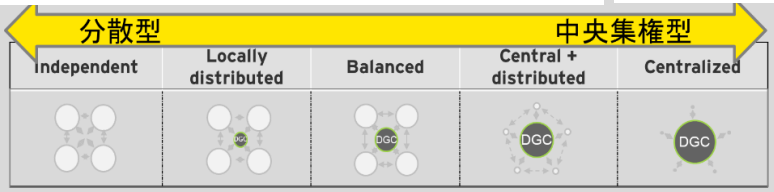
Technology Governance Rule		
	Governance Structure	▸ トラスト確保に関する説明責任体制
	Ownership	▸ トラスト確保のための役割と責任を明確化
	Data Dictionary and Meta Data Definition	▸ データ戦略に基づき必要なデータの特定と定義、データフォーマット等への対応方針、データの抽出性、再現性等に関するルールを整備
Risk Control & Quality	**Risk contorol**	▸ 各種基準や規制目的を逸脱するリスクを識別、分析し、対応するリスク管理基本手続き ▸ リスクをカバーする機能要件（例：完全性、正確性、適時性等）決定基本方針の整備 ▸ 第三者検証、官民ハッカソンを利用した検証など、技術検証に関する基本方針を整備
	Measure and Monitor	▸ セルフチェック、第三者検証、POC等モニタリング方針の整備 ▸ データの遡及性、抽出可能性を担保し、証跡の格納（期間、場所等）方針の整備 ▸ 課題が検出された場合直ちに対応を講じ、同時に情報を還元、共有する枠組を整備 ▸ 顕在化した問題の重要性に鑑みコンティンジェンシーを適時発動する枠組整備
	Change Management	▸ 変更事象を把握し目的の達成の毀損を適宜予防する変更管理のフレームワークを整備 ▸ 常時重複を排除し効率化を実現する枠組を整備

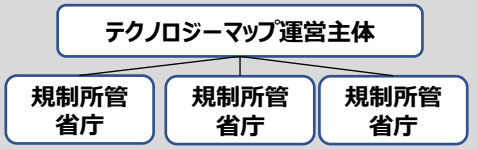
役割と責任の明確化とサードパーティリスク

- 一貫したトラスト確保の体制を構築するために、役割と責任の明確化が鍵
- トラストを語るには、だれがどのリスクを識別、評価、統制するのか、透明性を持たせることが求められる
- 外部で開発したテクノロジーのリスクはサードパーティリスクとよばれ、委託者、システム使用者の一義的リスクとして昨今トピック

（イメージ）

デジタル化に向けたDX推進主体となり新たな技術活用において トラストの確保の枠組を構築し適正な運営を組織横断的に担う者	技術リスク管理体制不備責任を負う	**テクノロジーマップ運営主体**
アナログ業務からデジタルによる自動化へ業務変革を促進し、 定められたトラスト方針に従い各規制の目的の達成責任を負う者	一義的に規制逸脱の責任を負う	**規制所管省庁**





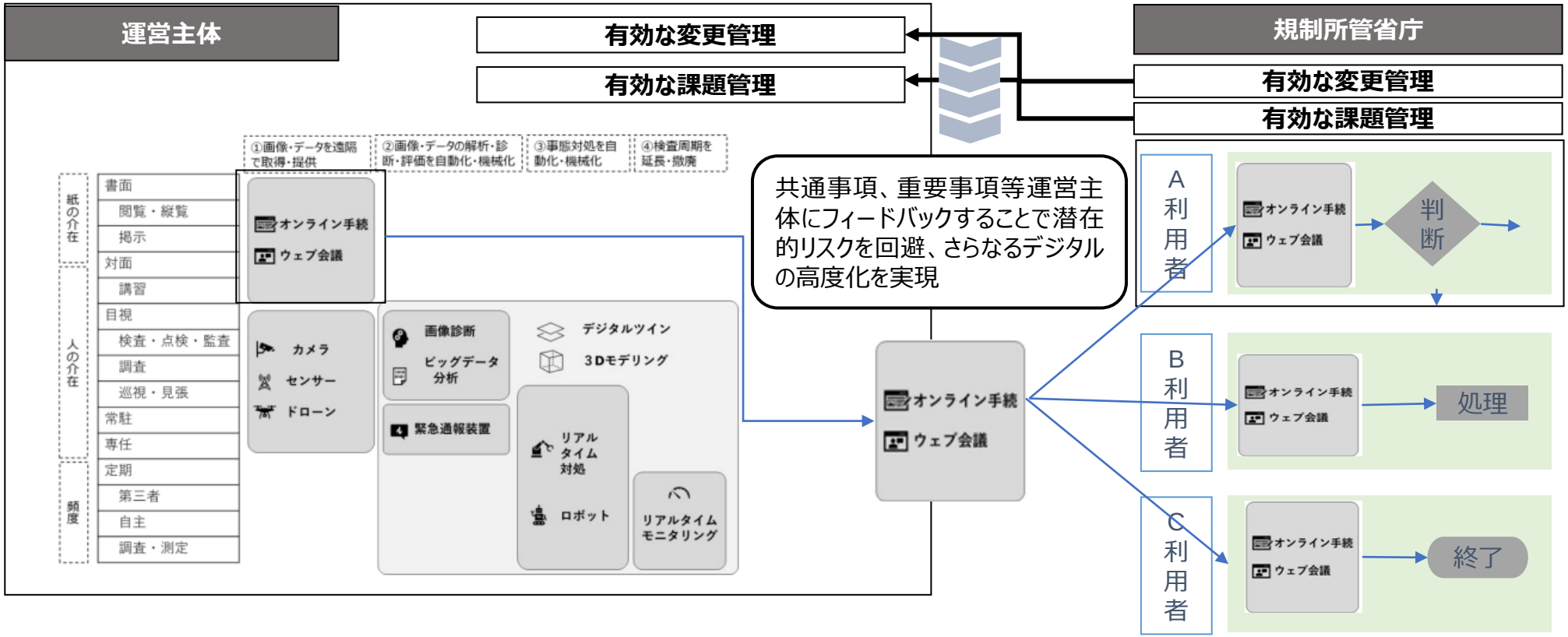
サードパーティリスク

要求される機能要件に従い トラストなテクノロジーを提供する者	技術不備の責任を負う	**技術保有企業** **テクノロジーマップ掲載者**

テクノロジーを利用する者	**技術利用者** **規制対象事業者等**

動的にトラストの確保を実現するための動的な変更管理の整備

- 一度検証した技術についても内外環境の変化に伴い各種機能要件の追加が求められる
- 充分有効な変更管理を実施しない場合、大きなリスクが顕在化する可能性がある
- 各レイヤー（運営主体、規制所管省庁）ごとに、管理すべき必要な変更事象を定義づけて、変更事象対応方針を整備する

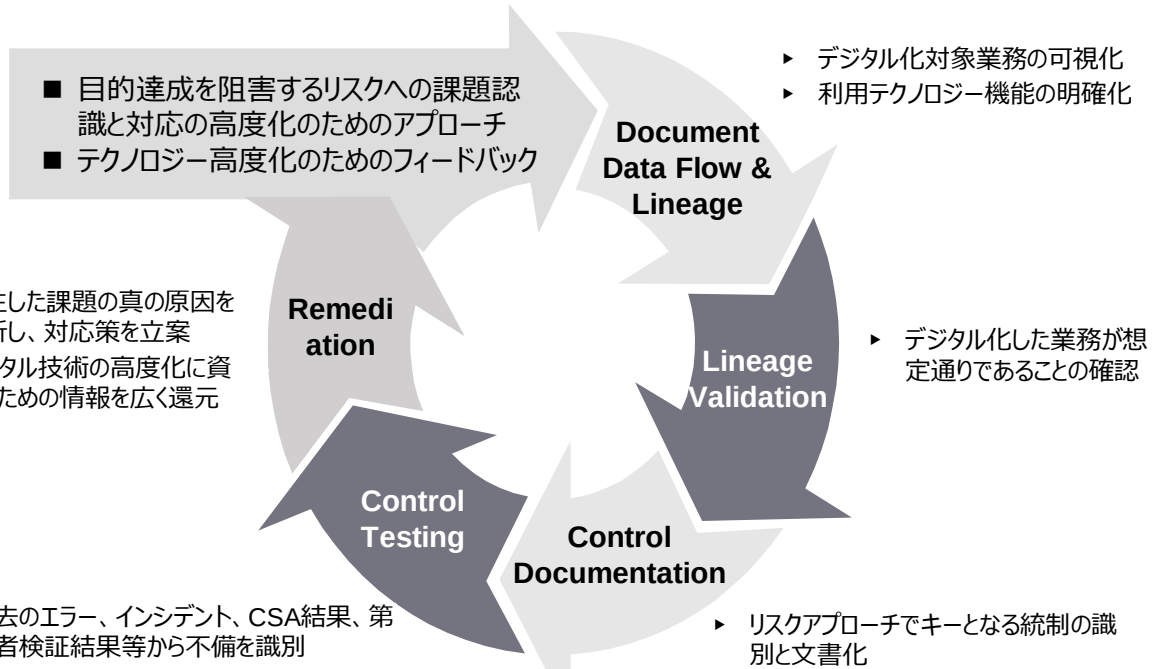


課題管理とフィードバックのフレームワークの整備

- 最新テクノロジーに伴うデジタル化における課題管理（PDCAサイクル）は極めて重要
- 各レイヤー（運営主体、規制所管所長）ごとに実施すべき課題管理手続きを整備
- 運営主体において、組織横断的に、新たに認められた課題に関する情報を適宜収集し今後のために還元する枠組を整備することで、リスクを軽減するのみならず、さらなるテクノロジーの高度化を推進する

品質要件例

- 完全性 (Completeness)
- 一貫性 (Consistency)
- 適時性 (Timeliness)
- 正確性 (Accuracy)
- 明確性 (Clarity)
- 一意性 (Uniqueness)
- 真実性 (Credibility)



- デジタル化対象業務の可視化
- 利用テクノロジー機能の明確化

- デジタル化した業務が想定通りであることの確認

- リスクアプローチでキーとなる統制の識別と文書化
- リスクと統制機能要件の文書化
- テスト方法の文書化

- 過去のエラー、インシデント、CSA結果、第三者検証結果等から不備を識別
- 同様の不備についても潜在性リスクを評価

- 発生した課題の真の原因を分析し、対応策を立案
- デジタル技術の高度化に資するための情報を広く還元

4 リスクアプローチと統制設計

リスクアプローチ

- リスクはゼロにならないことを理解し目的達成を阻害するリスクの重要性に鑑みリスクコントロールすることが重要
- リスクの識別、評価、対応までの一連のプロセスを明確にすることが肝要

リスクアプローチの一般的プロセス

目的の明確化	デジタル化業務の可視化	目的達成の阻害リスクの識別	リスク分析	リスク対応
▸ 規制の背景、趣旨含めて明確にすることが極めて重要 ▸ 対象業務を前提にせず、AS-IsからTo-Beを促す	▸ デジタル化するデータフローを明確にする ▸ 前後のデータフロー、業務フローを含めた可視化により、網羅的なあらたなリスクが識別できる	▸ 目的の達成を阻害しうるリスクを洗い出す ▸ リスクの識別にあたっては、一定の主張（例：アサーション）などを定義づけて説明責任を果たす	▸ リスクが顕在化した場合のリスクの重要性を評価 ▸ 評価には発生確率、発生した場合の影響度合いを考慮 ▸ 従来許容していたリスクも考慮し過度を回避する	▸ リスクを回避する ▸ リスクを移転する ▸ リスクを検証等低減する ▸ リスクを許容する ▸ 方針決定しテクノロジーの機能要件を決定する ▸ コストベネフィットを十分考慮する ▸ デジタル技術導入に合わせて追加的に必要となる統制を設計する

リスク分析の結果デジタル化することは妥当ではないとの決定もしうるプロセスの明確化

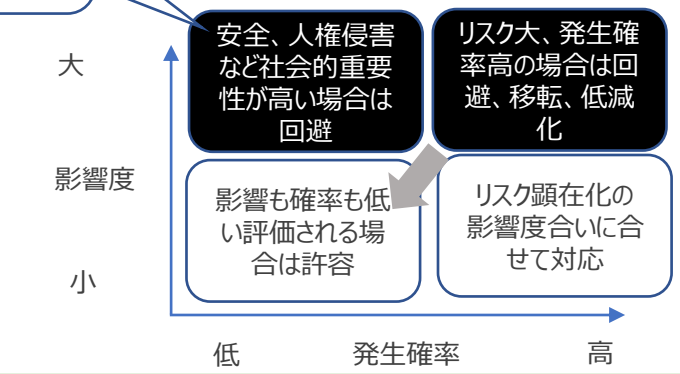
デジタル化に伴うリスク評価

- 過度に保守的になる場合、デジタル化を阻害するため十分な留意が必要
- 逆に、顕在化するリスクが社会全体に及ぼす影響が非常に大き場合、回避をする明確な評価プロセスの透明化が肝要
- デジタル化に伴うリスクには大きく２つのリスクがある

テクノロジーを採用する側のリスク認識評価が欠如することにより要件が十分ではないことに伴うリスク

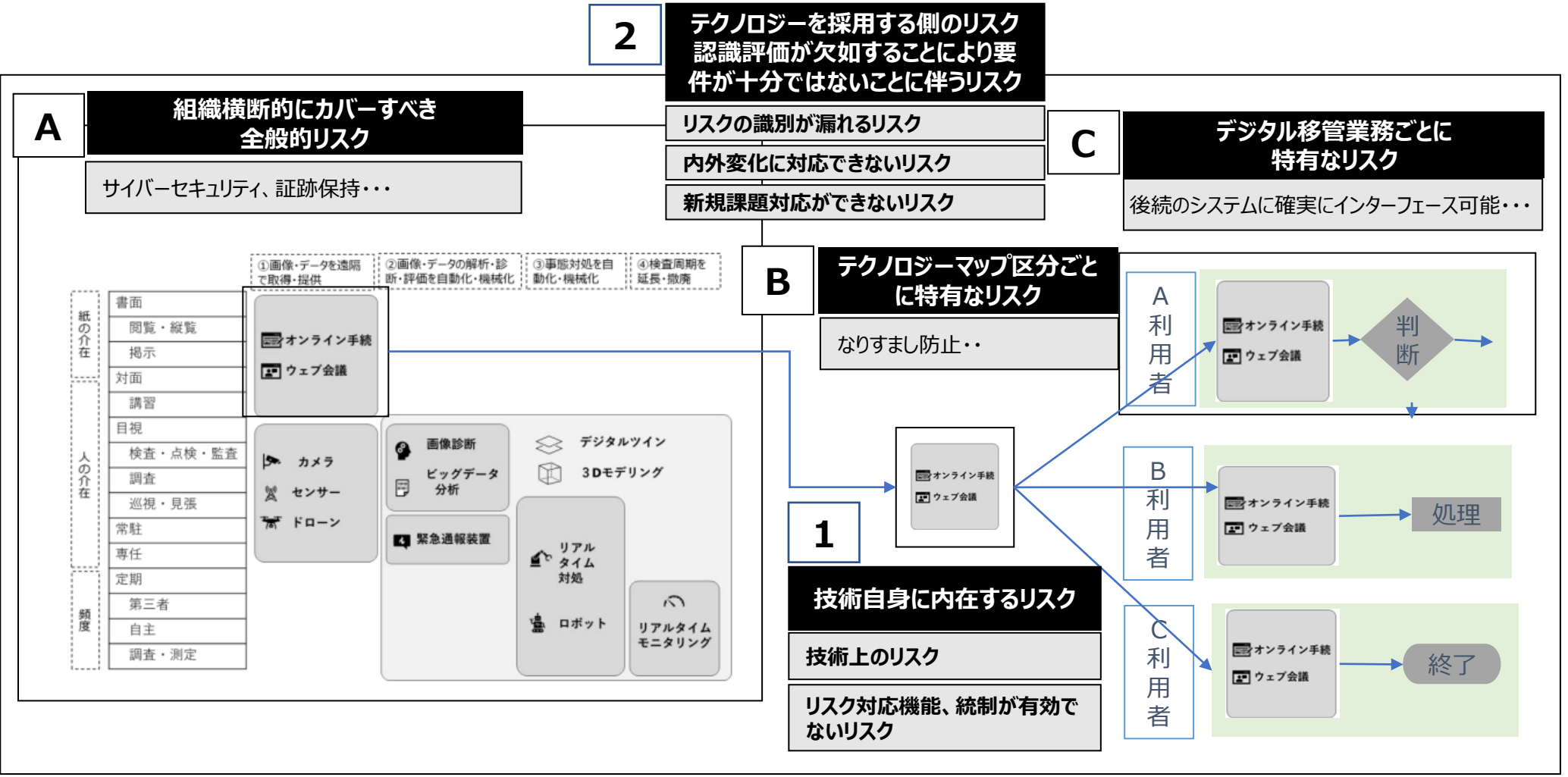
技術自身に内在するリスク（サードパーティリスク）

リスク分析



求められる一貫した動的なリスクコントロールの仕組み

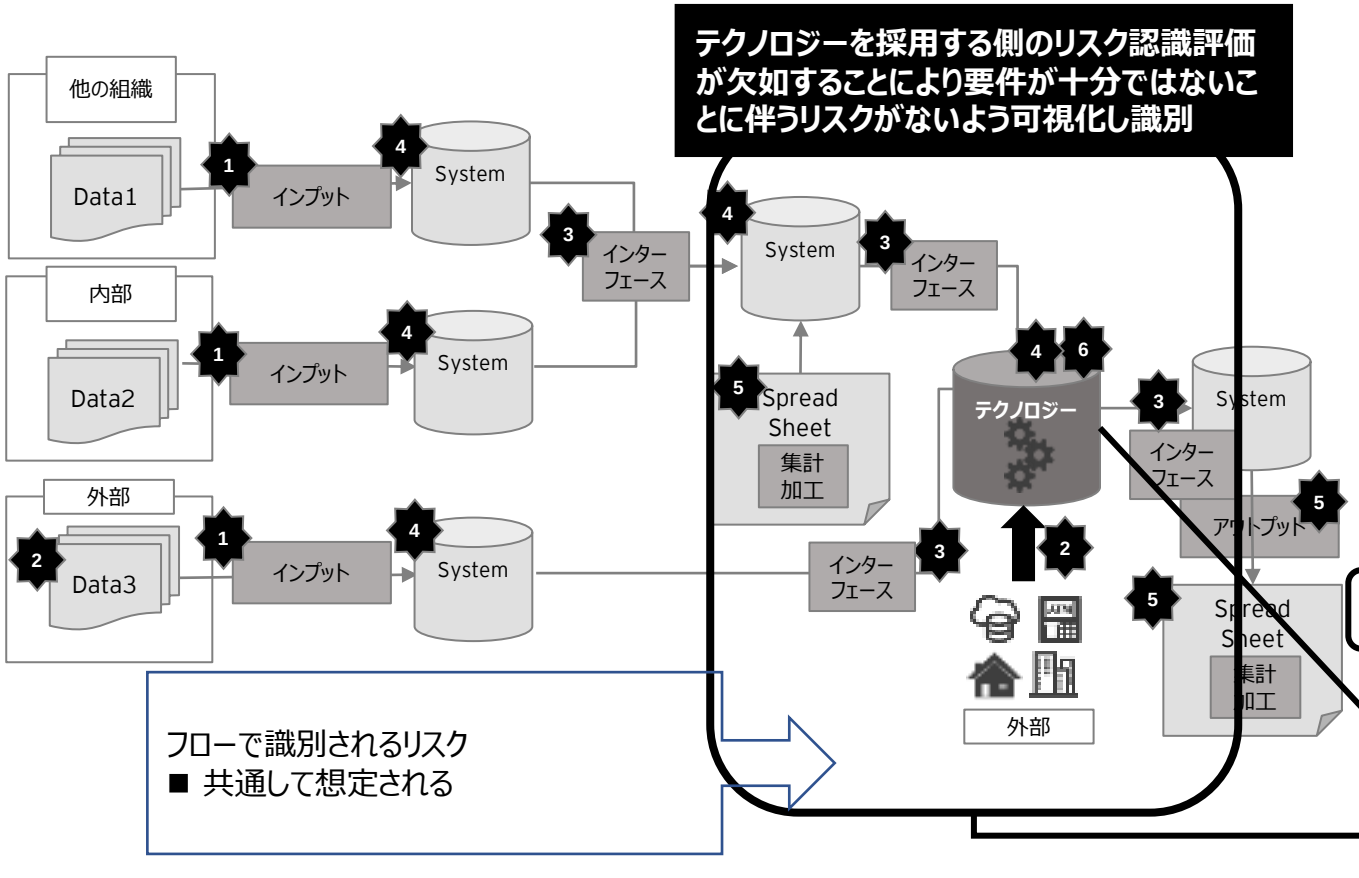
- 例えば技術が機能要件通りであったとしても、機能要件自身が、規制の目的を達成するに十分でなければ、真の意味でテクノロジーマップのトラストを確保できない
- 規制の目的達成を阻害すると想定される全てのリスクに対して、一貫した動的なリスク管理体制の構築が必要と思料



アナログからデジタルに移行するデータ/業務フローとリスクの識別

- 業務フローをすべて最新のテクノロジーに代替することは困難な場合が多い
- デジタル化に移行する新たなプロセス全体の業務、データフローを可視化し、リスクを網羅的に識別することが重要
- こうした一連のリスクアプローチの導入と可視化を組織横断的に推進するガバナンスがトラストの枠組として肝要

デジタル化による新プロセスについてフローチャートによるリスク識別の可視化



統制機能イメージ

No	内部統制におけるリスクアセスメント
1	フロント部署におけるデータインプットの正確性・網羅性を逸脱するリスク
2	外部から入手するデータの正確性・網羅性を逸脱するリスク
3	システム間のインターフェース（自動転送）の正確性・網羅性を逸脱するリスク
4	システムへのアクセスコントロール、SOD（Segregation of Duties：職務分掌）が不適切
5	システムからのデータアウトプットの正確性・網羅性を逸脱するリスク
5	スプレッドシートへのアクセスコントロール、変更管理が不十分なリスク
6	採用するテクノロジーが十分機能しないリスク

技術検証

統制機能要件

リスクコントロールマトリックスと統制機能要件の決定

- 本来の規制の目的に照らし、当該目的達成を逸脱するリスクを識別し、リスクの影響度合いを分析
- 識別評価されたリスクについては、有効な統制機能として、機能要件に含める

リスクコントロールマトリックスによる統制機能要件の決定プロセスの可視化（一部事例）

トラストであることに対する主張（仮定）

デジタル化することで規制の目的達成を阻害、逸脱するリスクを識別

識別されたリスクの顕在化を低減/阻止するため採用するテクノロジー上の機能要件あるいはアナログ統制の整備

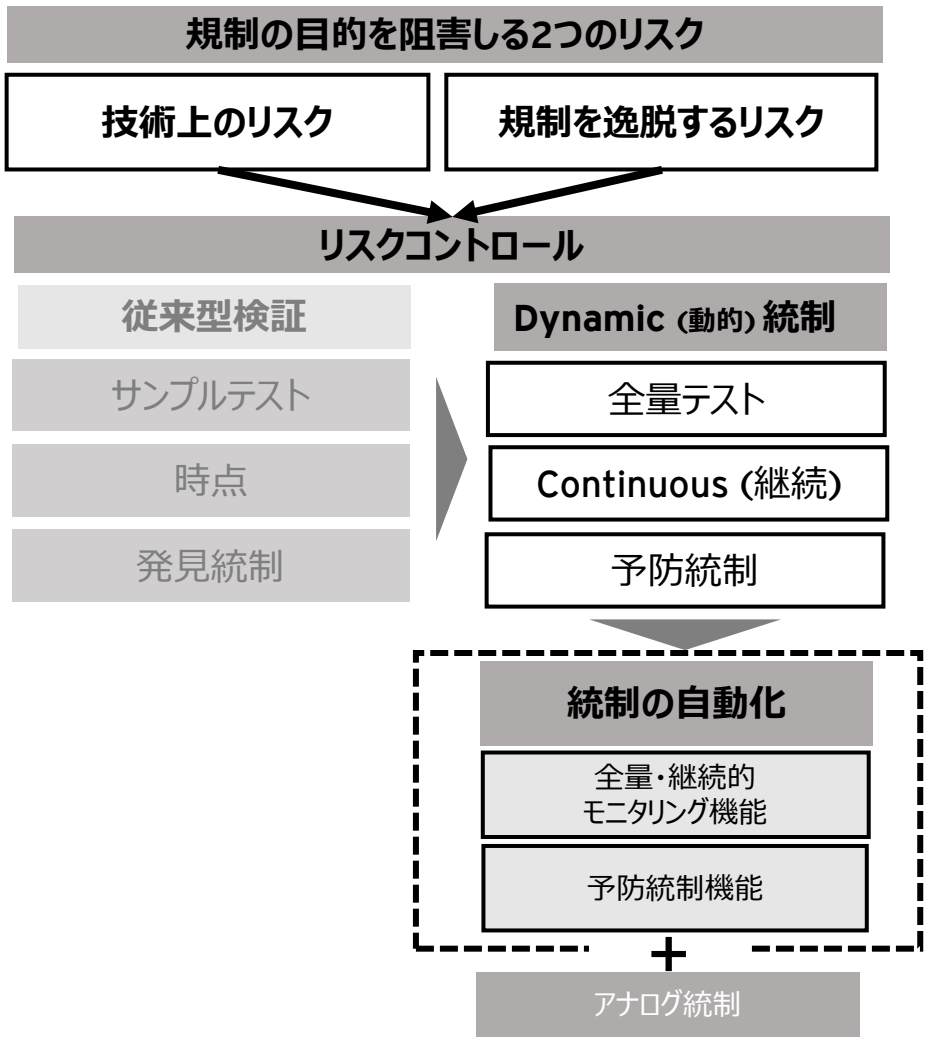
整備された統制活動がきちっと運用されているかのモニタリングテストを設計

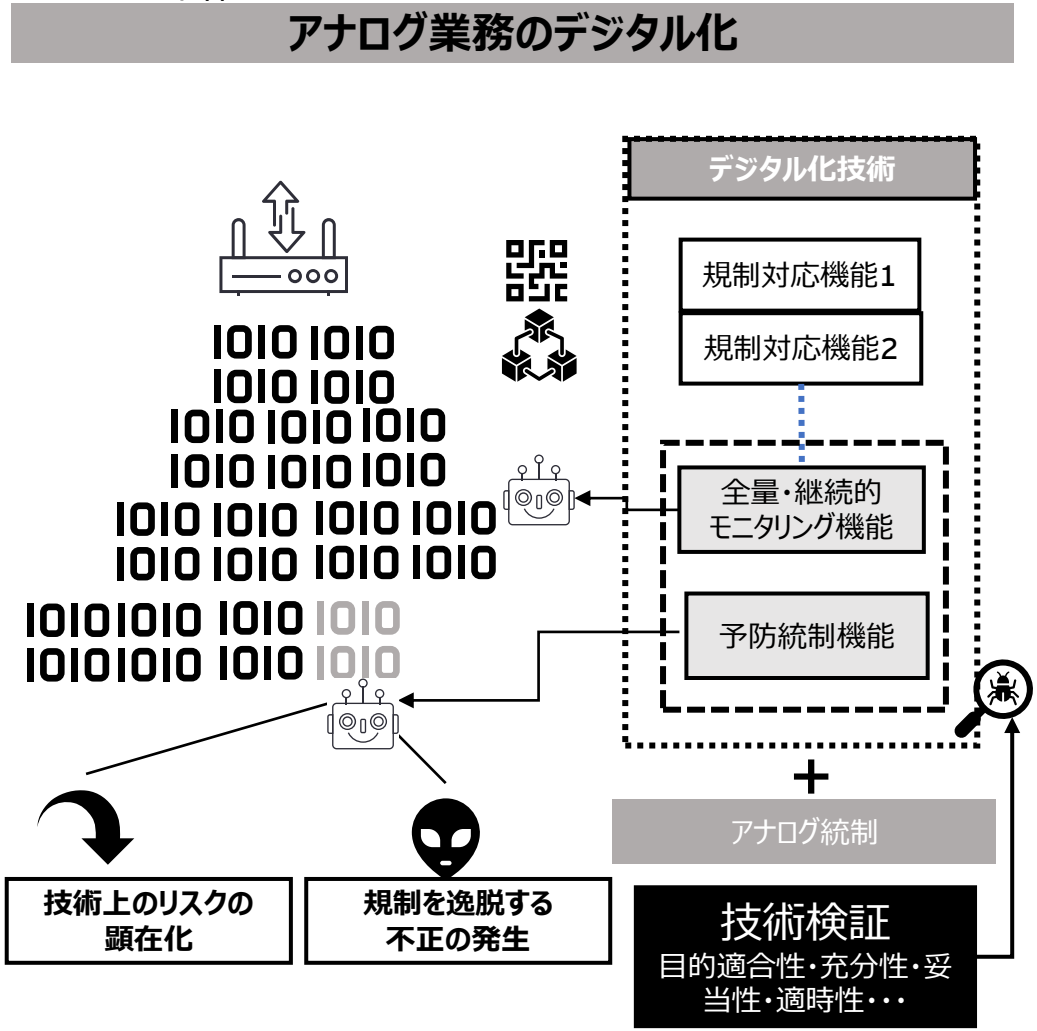
モニタリングテストの運用証跡を格納

アサーション	リスク	統制機能要件	運用テスト機能要件	証跡機能要件
研修内容を理解している	理解していない	▸ 動画の終わりに理解度テストを実施する ▸ レポートや課題を提出させる	テスト結果確認 レポート、課題確認	テスト結果 レポート、課題
不正回答はしていない	テストの回答を不正に入手する	▸ 理解度テストのパターンを増やす ▸ レポートや課題を提出させる	テスト結果確認 レポート、課題確認	テスト結果 レポート、課題
動画をすべて見る	動画を早回しで再生する	▸ 視聴ログ管理を行う ▸ 早送り禁止機能	再生ログ確認	ログデータ
動画をすべて見る	動画を飛ばし見る	▸ スキップ禁止機能	再生ログ確認	ログデータ
本人が見ている	替え玉受験を行う	▸ 動画再生時に本人確認を行う ▸ 生体認証（指紋・虹彩・顔　等）	認証ログ確認	ログデータ
動画だけを見て他のことをしていない	複数の端末で異なる動画を同時に見る	▸ 動画を配信するサーバーに同一のIDで複数の端末でアクセスできないようにする	アクセスログ確認	ログデータ
動画だけを見て他のことをしていない	動画再生中に別のウインドウで作業する	▸ 動画再生中に別ウインドウを開いた場合動画再生が停止される	再生ログ確認	ログデータ
動画だけを見て他のことをしていない	動画再生中に別の作業を行う	▸ 一定時間毎に指定された文字の入力を行わないと次に進まない ▸ Webカメラで受講態度を確認	文字入力ログ確認 Webカメラ映像分析結果確認	ログデータ AI映像分析結果

Dynamic（動的）かつContinuous（継続的） Control

- 内外環境の変化は激しく、リスクの拡散スピードが速く、かつ社会的影響度が大きい
- Regulation Technology（Supervisory technology）は、Dynamic（動的）、Continuous Control が潮流
- 規制対応エリアは、継続的、全量モニタリング、予防統制機能が組み込まれた、最新技術に期待が寄せられている
- リスクは次の２つに整理でき、それぞれともにコントロールすることでトラストを確保する





進化する技術に内在する新たなリスク

■ 最新技術には、従来にない、新たなリスクが認められてきている

例1

RPAノラロボリスク
AIのバイアスデータブラックボックス化によるリスク

- RPA（Robotic process automation）、AI（Artificial Intelligence）の利用は今後さらに進むと想定されるが、そこで生成されるデータの確からしさに対し十分な統制整備が求められる。

RPA Case study

ガバナンス・集中管理
・開発・品質管理

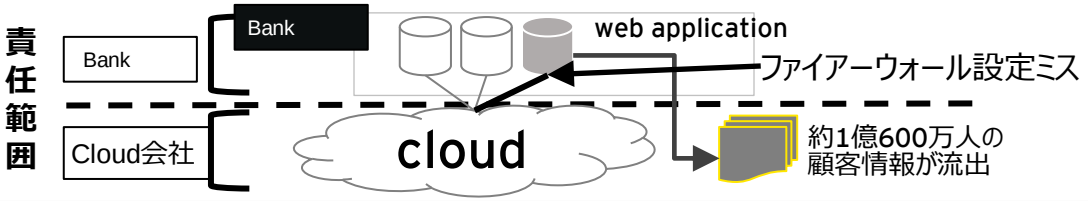
- 処理の監視・品質向上
  - 監査ログ監視
  - 運用管理
  - 不正アクセス
  - 権限管理
  - キャパシティのコントロール

AI Case study

- RPAに加え、さらにモデル、およびバイアスデータの有無等評価軸を検討。一定の管理ルールを導入
  - リスク評価：AI管理チームにより実施
  - 集中管理：AIの一元管理、リスク管理状況の把握
  - 年次評価：リスクの変化及び状況を確認

例2

- 社内業務の一部を外部委託する傾向が強まる昨今、委託会社が責任を有する領域で実施されるべき内部統制（委託会社の相補的な内部統制）の領域で情報漏洩等が発生。外部へ業務委託する際、委託会社自らが責任を有する領域を把握し、適切な内部統制を構築・運用することが重要である。



クラウドカバー範囲との境目のリスク

内外環境の急激な変化により常に変化するリスク

- コロナによる在宅勤務、安全保障問題など、今後も内外環境は複雑に急速にテクノロジーに影響を与えている
- 未曾有なリスクをよりプロアクティブに識別しコントロール可能な体制構築が非常に重要

ペーパーレスに伴う新たなリスク

- 監査上のデジタル証跡に求められる統制の十分性や、税務上の電子帳簿保存法などの要件を満たすことが求められる。新たな統制要件を充足するためのタイムスタンプを伴うワークフローシステムによるデジタル承認や、税務要件を満たすデジタル証跡のストレージなどの対応が重要となる。こうした動きは今後さらに進むと想定される。

例3

＜日本＞監基報 500　A31項：「～略～原本以外の文書の信頼性は、**その作成と管理に関する内部統制に依存する**ことがあるとされている。」
＜米国＞AS 1105: Audit Evidence (As Amended for FYE 12/15/2020 and After) 第8項：「 ～略～**信頼性は、それらの文書の変換と維持に関する管理に依存する**。」

例4

- 次々に新たなテクノロジーが規制エリアに参入
- 不正技術も急速に進化
- 内外環境も急速に変化
- 顕在化した場合のリスクの拡散のスピードが速い
- また重要度が増している

- AML対応で急速にAIなどを活用したRegTechが進化
- 規制対応コストは増大するなか、あらたな規制対応テクノロジーが生まれている
- コードによるガバナンス整備など動的かつ分散型のコントロールが注目されている

デジタル化特有のリスクは常に動的に変化

5 技術検証手法

トラスト確保のための様々な技術検証手法

■ リスク分析結果を踏まえ、有効な検証手法を選択する仕組みを作る

技術保有企業自身の自己評価

- 特許・論文・公表された実証実験実績
- データ再利用等　禁止事項への著名責任
- 各種認証
- **事例１** 経営者のトラストに対する宣誓

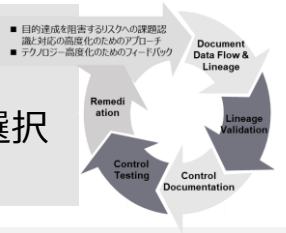
■ 客観性の欠如
■ 技術保有企業のコスト負担
■ 資金力での優劣によりス中小・タートアップ企業の劣後性

第三者評価

- **事例2** サイバーセキュリティ第三者評価
- **事例3** ゼロトラスト評価
- **事例4** 第三者SOCレポート　他

■ １件ずつ実証するには膨大なコストがかかる
■ 時間もかかる
■ 最新技術に対する客観的第三者評価手法の限界
■ 最新技術に対する評価可能実施者の限界

■ 客観的リスク評価を実施し、リスクに応じた有効な技術検証手法を選択するプロセスが重要
■ 新技術については、デファクトスタンダードといった明確な評価基準がない可能性が高い
■ 特許、論文、認証、実証実績なども検証対象としながら、類似する技術の基準を読み替え、有効な検証手法を選択
■ 各種技術専門研究機関と評価の専門家が一体となり、より透明性をもって、トラストだという説明責任を果たす



より動的オープンなトラスト検証

- **事例5** 実証内容及び結果の検証
- **事例6** 規制のサンドボックス
- **事例7** 官主催テクノロジーベースのハッカソン
- **事例8** より多くの目による検証

■ 技術提供会社の実証内容を官（第三者）が検証
■ 申請後実証しプルーフを有識者会議で検証後認証
■ 官主導によるハッカソン
■ ホワイトハッカーの活用
■ 広く公開し幅広く評価に関する意見聴取

EY | Building a better working world

EYは、「Building a better working world ～より良い社会の構築を目指して」をパーパス（存在意義）としています。クライアント、人々、そして社会のために長期的価値を創出し、資本市場における信頼の構築に貢献します。

150カ国以上に展開するEYのチームは、データとテクノロジーの実現により信頼を提供し、クライアントの成長、変革および事業を支援します。

アシュアランス、コンサルティング、法務、ストラテジー、税務およびトランザクションの全サービスを通して、世界が直面する複雑な問題に対し優れた課題提起（better question）をすることで、新たな解決策を導きます。

EYのコンサルティングサービスについて

EYのコンサルティングサービスは、人、テクノロジー、イノベーションの力でビジネスを変革し、より良い社会を構築していきます。私たちは、変革、すなわちトランスフォーメーションの領域で世界トップクラスのコンサルタントになることを目指しています。7万人を超えるEYのコンサルタントは、その多様性とスキルを生かして、人を中心に据え（humans@center）、迅速にテクノロジーを実用化し（technology@speed）、大規模にイノベーションを推進し（innovation@scale）、クライアントのトランスフォーメーションを支援します。これらの変革を推進することにより、人、クライアント、社会にとっての長期的価値を創造していきます。詳しくはey.com/ja_jp/consultingをご覧ください。

ED None

ey.com/ja_jp