経済産業省　御中

令和６年度経済産業省デジタルプラットフォーム構築事業
（次期ｇＢｉｚＩＮＦＯのリリースに向けた運用ルールの整理）

報告書

Dec 20, 2024

弁護士法人 W Partners法律事務所

資料構成

1. プロジェクト概要

2. リスクアセスメントフェーズ

    1. リーガル観点のアセスメント
    2. データ観点のアセスメント

3. 整理・策定フェーズ

    1. データポリシーの検討
    2. 策定すべき運用方針書、及び反映観点の一覧
    3. システム機能要求事項

1. プロジェクト概要

概要

- 次期gBizINFO構築にあたり、適法性等の観点より、のリスクアセスメントを実施し、対応すべき観点、リスクの抽出を実施
- アセスメント結果に基づき、検討すべきドキュメントの策定を実施

実施内容（実施スコープ）

リスクアセスメント

1：リスク抽出・特定

2：リスク分析

3：リスク評価

4：対応すべき観点/方針の整理

×

リーガル観点の内部/外部リスク

データガバナンス観点のリスク

整理・策定

運用ﾄﾞｷｭﾒﾝﾄの作成・反映

1：データポリシーの整理

2：利用規約の改訂

3：運用ルールの整理

4：次期gBizINFO機能に反映すべき内容の整理

5：リスクコミュニケーション

2. リスクアセスメントフェーズ
2-1. リーガル観点のアセスメント：アプローチ

- 次期gBizINFOで提供するサービスは適法であれば良いだけではなく、レピュテーションリスクやその他のリスクを踏まえて実施の有無や内容を検討する必要があると考えられる。したがって、適法性だけではなく、もう少し広い範囲でのリスク調査・分析を実施することが必要であると考えた。
- そこで、内部・外部のリスクを幅広く分析・評価するために、以下のフレームワークを用いてリスクアセスメントを実施し、本報告書に取りまとめた。

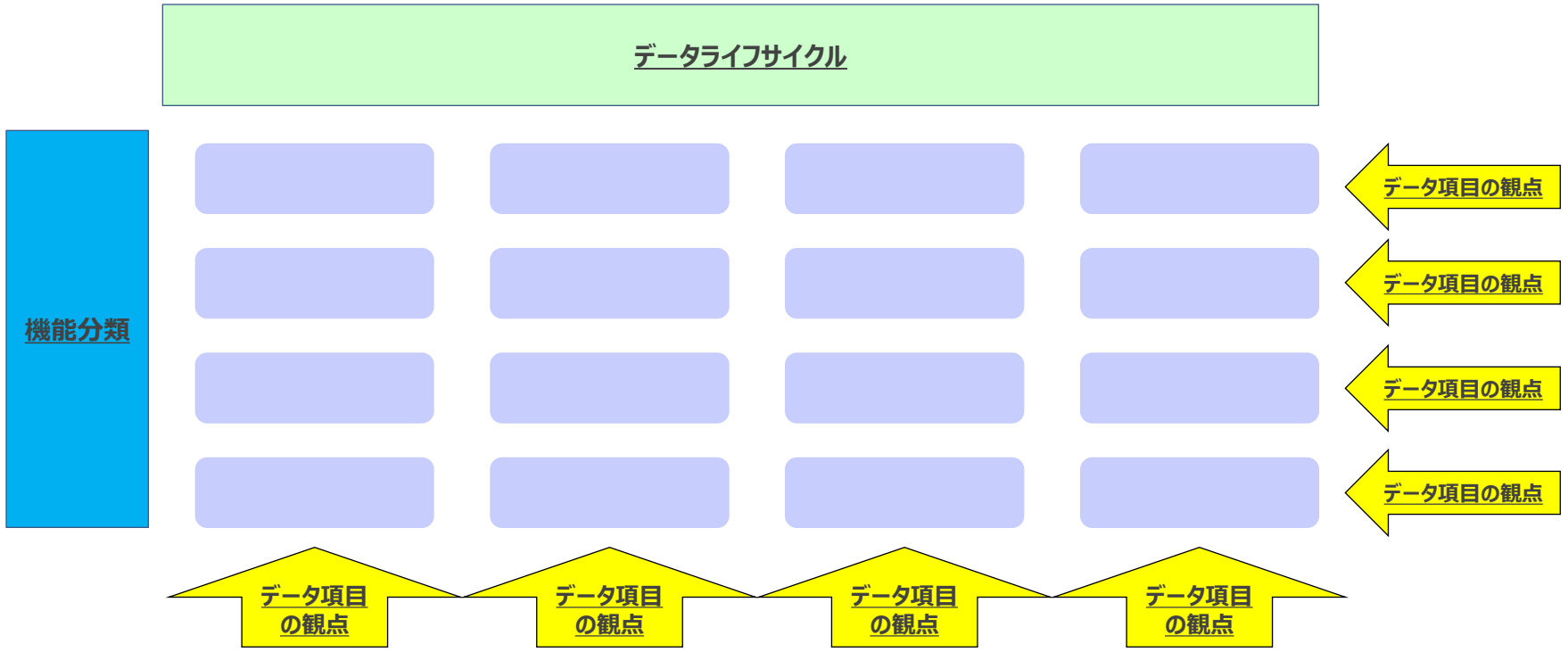
内部リスク	外部リスク
①サービス内容の適法性	⑤ステークホルダー分析
②サービス実施の遵法性	
③リスクコミュニケーション	⑥規制環境
④リスク評価・管理	

2. リスクアセスメントフェーズ
2-1. リーガル観点のアセスメント：論点の洗い出し

- リーガル観点についての検討については、
  (1)次期gBizINFOのデータ項目に基づく分析
  (2)データライフサイクルと次期gBizINFOの機能をベースにしたマトリックス分析
  を併用して、複数方面からの分析を実施

↓

- データ項目のみからのアプローチによる適用法令・適用規制の「見逃し」を補完
- マトリックス分析のみによる個人情報等の「見逃し」を補完



2. リスクアセスメントフェーズ
2-1. リーガル観点のアセスメント：論点一覧

内部リスク／外部リスク	法令等項目	論点
①サービス内容の適法性／②サービス実施の遵法性	1．個人情報保護法	(1) 個人情報の取得の有無／個人情報として取り扱っている範囲
		(2) 利用目的の特定
		(3)-I 個人データの保管・管理／安全管理措置
		(3)-II データの正確性
		(4)-I 第三者提供規制（情報取得時）
		(4)-II 第三者提供規制（公表時）
	2．3rd Party Cookieの問題	(1) 個人関連情報の提供規制にあたらないか
		(2) ポップアップが必要ではないか
	4．不正アクセス禁止法	(1) アクセス管理者の義務
	8．著作権法	(1) 著作物性
	9．経産省「電子商取引及び情報財取引等に関する準則	(1) 該当性
	10．特定商品取引法	(1) 特定商品取引法の適用があるか
	11．消費者契約法	(1) アカウント作成につき消費者契約法の適用があるか
③リスクコミュニケーション	1．個人情報保護法	(5) 本人等からの開示等請求に対する対応
	5．プライバシーポリシーの問題	(2) 情報開示／同意取得
④リスク評価・管理	3．商業登記法（代表取締役等住所非表示措置）／プライバシー権	(1) 非表示への対応
		(2) プリファレンス項目の設定
		(3) 検索項目の設定
	5．プライバシーポリシーの問題	(1) 本システムに則したポリシー
	6．利用規約の問題	(1) データの最新性非保証、責任範囲限定等
		(2) プライバシー侵害への配慮
	7．掲載期間の問題	(1) 正確性の担保
⑤ステークホルダー分析	12．ステークホルダーとの関係	(1) 提供元との関係性等
⑥規制環境	1．個人情報保護法	(6) 今後の法令改正が見込まれるか
	3．商業登記法	(4) 今後の法令改正が見込まれるか

2. リスクアセスメントフェーズ
2-2. データ観点のアセスメント：アプローチ（1/4）

- 「セキュリティリスクの観点」「データガバナンスの観点」の2つの観点からアプローチを実施
- IPA（＋ガバメントクラウド）、DMBOKをフレームワークとして活用をし、アセスメントを実施

セキュリティリスクの観点

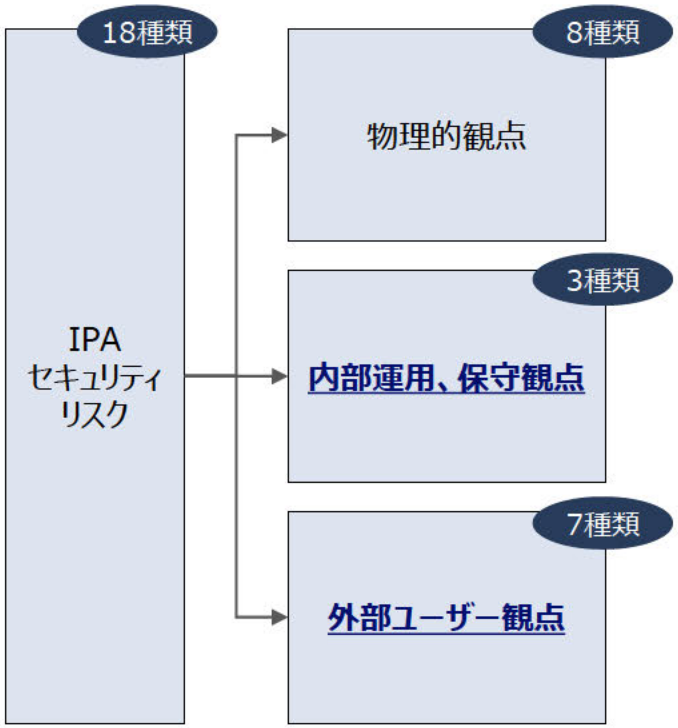
IPA セキュリティガイド	• IPA分析ガイドを参照し、「内部運用、保守観点」「外部ユーザー観点」の計9種類を活用 • 加えて、ガバメントクラウドも参照し、観点の補完を実施
×	
業務プロセス	• gBizINFOで想定される業務プロセス、利用機能に着目し、セキュリティリスクを網羅的に抽出

データガバナンスの観点

DMBOK	• DMBOKにて定義されるデータガバナンスフレームを活用し、データ品質や鮮度、運用体制 等に関するアセスメント観点を整理 • データセキュリティの観点は、左記IPAで包含されるため割愛
×	
データライフサイクル／処理ブロック	• データライフサイクル、データ処理ブロックに着目し、アセスメント項目を網羅的に抽出

2. リスクアセスメントフェーズ
2-2. データ観点のアセスメント：アプローチ（2/4）

- IPAで定義されるリスク観点18種類のうち、本検討に際しては、**「内部運用、保守観点」「外部ユーザー観点」で計9種類を活用**した検討を実施。



リスクシナリオの検討における考え方

- 主にサーバー本体、サーバールーム内で想定されるリスク
- 施錠、デバイス制御、入退館管理　等の物理的な対策が有効となるリスクであり、本PJの検討スコープからは除外

- 主に、システムにおけるプログラムの設定値、設定情報の改ざん、不正利用　等のリスク
- 権限管理、重要操作の承認プロセス導入　等の対策が有効
- 「運用・管理者」「システム保守担当者」の業務にて、想定されるリスクとして検討

- 主に、外部からのアクセスから引き起こされるリスク（高負荷攻撃、ウィルスプログラム　等）
- ファイアーウォール、アクセス制御、パッチ適用　等の対策が有効
- 「Web利用者」「API利用者」の業務において、想定されるリスクとして検討

参照先URL	https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

2. リスクアセスメントフェーズ
2-2. データ観点のアセスメント：アプローチ（3/4）

- ガバメントクラウド（AWS：セキュリティ）のガイドより、下記観点を抽出し、リスクアセスメントに活用

ガバメントクラウドに関するセキュリティの観点

多要素認証	• 認証時の多要素認証の設定 • 本番環境相当へのアクセスは強固な認証方式が推奨	**ログの取得と分析**	• システムログの取得、分析ツールの導入
アクセス制御	• IDの種類に応じた権限の設定 • スイッチロール時の接続元IPアドレス制限の設定	**構成変更の記録と自動検知**	• リソース変更の検知ツールの導入
通信の限定と暗号化	• HTTPSプロトコルによる通信の設定 • 暗号化Keyを活用したデータ格納（データの暗号化）	**脆弱性対策**	• 脆弱性対策の導入（脆弱性の評価、対策の実施）
FireWall	• FireWallの設定による不正アクセスの防止	**CI/CD**	• CI/CDを活用した開発資源の変更、リリース（検討対象外）
DDoS対策	• DDoS対策の導入（リソースの保護、攻撃の検知、攻撃内容の把握）	**対応体制**	• セキュリティ事案発生時の検知から対策までの運営体制の確立
マルウェア対策	• マルウェア対策の導入（対策ソフトの導入　等）		

参照先URL	https://guide.gcas.cloud.go.jp/aws/security-tech/

2. リスクアセスメントフェーズ
2-2. データ観点のアセスメント：アプローチ（4/4）

- DMBOKのフレームワークより、下記5つの観点をリスク検討にて活用
- このうち、データセキュリティの観点は、リーガル観点のアプローチ、IPAのセキュリティリスクの観点で包含

データガバナンスの観点

データ ガバナンス	● データマネジメントが適切に実施されるよう、**データにまつわる意思決定権の体系（戦略、組織、ルール）を規定し、統制**する
データ セキュリティ	● 保有データに対するリスクを明確にし、脅威・脆弱性への対策を実施する。 ● データのプライバシーと機密性を保ち、データを侵害から守り、適切なアクセスを確保する
ドキュメント& コンテンツ管理	● 法令や規制に準拠するために必要な文書など、そこに含まれる**データや情報のライフサイクルを管理するための文書・ルールを管理**する（特に個人情報関連）
データ管理 （メタデータ）	● **高品質で統合されたメタデータ**へアクセス可能にするための計画、実装、統制を行う。
データクオリティ	● 利用されるデータの適性を測定・評価し、改善するための**品質管理技術の計画と遂行を通じて、データクオリティの充足**を図る

- 参照元：データマネジメント知識体系ガイド 第二版（日経BP社）

2. リスクアセスメントフェーズ
2-2. データ観点のアセスメント：アセスメントの観点（1/2）

- 新規開発機能に関連する業務におけるセキュリティリスク、及びリスクアセスメント実施にあたり、以下の観点を実施

			リスクアセスメントの観点
Web利用者	ユーザーIDの登録・管理	1.不正アクセス 6.プロセス不正実行	• ID管理、権限管理、操作の承認プロセス • ウィルス、脆弱性 等の対策 • DDoS対策　等の対策　　等
	自社データの更新対応	1.不正アクセス 11.高負荷攻撃 7.マルウェア感染 15.通信輻輳	
運用管理者	Web利用者IDの発行・管理	4.操作過失 8.情報窃取・改竄・破壊 6.プロセス不正実行 9.不正送信	• ID管理、権限管理、操作の承認プロセス • 操作ログの保管、解析 • ロールバック 等のバックアップ • 異常検知のシステム、体制　　等
	個社データの管理	4.操作過失 8.情報窃取・改竄・破壊	
	利用状況・FBの分析	4.操作過失 8.情報窃取・改竄・破壊	

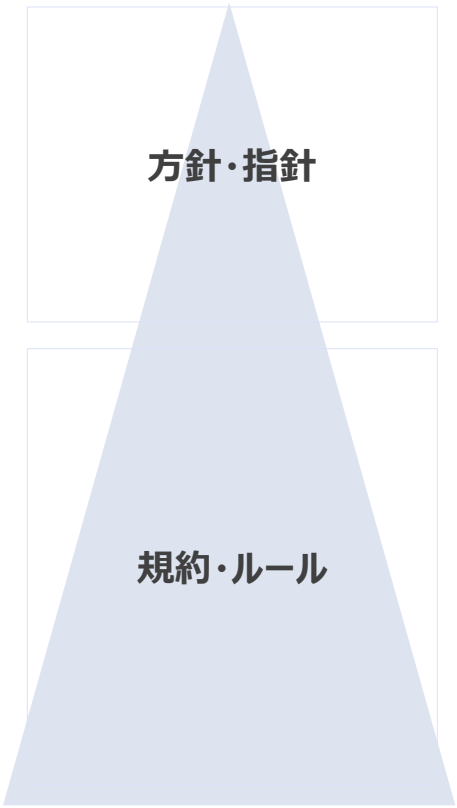
2. リスクアセスメントフェーズ
2-2. データ観点のアセスメント：アセスメントの観点（2/2）

- データガバナンス観点でのアセスメント実施にあたり、以下の観点を実施観点を整理

		アセスメントの観点
データ ガバナンス	● データガバナンス全体を統制するデータポリシー、及び利用規約の定義、開示	• 現行ポリシーの有無、修正要否　等
ドキュメント& コンテンツ管理	● 個人情報保護法観点での安全管理措置に関する運用手順 ● データの授受に関連する運用手順 ● ユーザーからの取得データに関連する運用手順	• 運用手順の網羅性、修正要否　等
データ管理 （メタデータ）	● データ信憑性を担保するメタデータの付与/維持 ● データ信憑性を担保するメタデータの適切な提示 ● 分析、活用を想定したメタデータの定義、付与	• メタデータの付与方法、担保方法 • ユーザー取得項目の充足度　等
データクオリティ	● 不正データの入力、更新の防止 ● 不正データのチェックの実装 ● データの誤登録の防止（加工、補正、変換　等） ● 外部システムからの適切な更新頻度の担保	• 不正データの検知、補正　等のチェック運用、機能 • 外部システムからの連携頻度、方法　等

3. 整理・策定フェーズ
3-1. 検討対象と作成アプローチ

- リスクアセスメント結果を踏まえ、データポリシーの整理、利用規約、運用ルール等の作成を実施
- 検討、作成した資料の内、①データポリシー、④運用方針書、⑤システム機能要求事項を、以降に掲載



	実施プロセス	想定成果物
方針・指針	● 新規機能で取り扱われるデータに関する方針・指針を整理 ● 個人情報等に関する、同意取得、開示請求対応等の指針を作成 ● 掲載情報に関する、保管/削除期間の設定や、セキュリティ等の運用指針を作成	① データポリシー ② プライバシーポリシー
規約・ルール	● 利用ユーザーに要求する責任範囲の明確化、及び同意事項の整理 ● 同意取得を行う際の運用ルールを作成	③ 利用規約（サイト／API） ④ 運用方針書
	● 上記の規約・運用ルールを踏まえ、次期gBizINFO機能に反映すべき内容を抽出	⑤ システム機能要求事項（対象がある場合）
	● 同意取得等を利用ユーザーへ周知を行う際の実施方針を作成	⑥ リスクコミュニケーション方針書

3. 整理・策定フェーズ
3-2. データポリシーの検討：策定の必要性

- 組織にデータマネジメントを導入するためには、その考え方や方針を表明する文書を作成し、組織内に公開・周知する必要があります
- データポリシーがないと、様々な判断を属人的に行われ、組織として恒常的なデータマネジメント運営ができなくなります

データポリシーとは	データと情報を生成・取得し、健全性を保ち、セキュリティを守り、品質を維持し、利用するといった様々な活動を、統制する**基本的なルール**と、それらに共通する**原則と管理意図**を盛り込んだ指示文書である。 （DMBOK2「第3章データガバナンス」より）
①原則・管理意図	「プリンシプル」とも呼ばれ、組織としてのありたい姿を表したものをいいます （例） • 欲しいデータを欲しいタイミングで利用できる環境をつくる • 地域や事業に偏らず全社的視点で統制されたデータを生み出す • 経営が正しい意思決定するために常に正しいデータを提供する
②基本ルール	遵守すべき行為や判断基準を表し、これを基に「標準（スタンダード）」や「運用手続（プロシージャ）」へと具体化されます （例） • 複数領域で利用されるデータは必ずデータ統合基盤に連携する • 顧客、品目マスタは全社視点で標準化されたものを利用する • 経営に影響を及ぼすデータは定期的に監視し品質を維持する

3. 整理・策定フェーズ
3-2. データポリシーの検討：策定ガイドライン（例）

- 公的資金により得られた研究データの機関における管理・利活用を図るためデータポリシーの策定が求められています
- その中でデータポリシーで定める項目として、以下が挙げられています

ポリシー策定の目的	機関のビジョン、ミッション等を踏まえ、ポリシーを策定した背景と研究データ利活用の目的について記述する。（**①原則・管理意図に相当**）
データの定義、制限事項	• 機関のミッションに従い、ポリシーが対象とする「データ」の定義・範囲を明確にし、利活用が想定されるデータ、将来的に利用の可能性が考えられるデータなど、データの種別・内容等について記述する。 • データの利活用に関する機関の方針や基本的な考え方を踏まえ、非公開、共有等の対象となるデータや公開・共有における制限事項について記述する
データの保存・管理・運用・セキュリティ	• データの特性に応じたデータの保管、運用方針について記述する
データに対するメタデータ、識別子の付与、フォーマット	• データに対するメタデータ及び識別子付与についての方針を記述する。また、データの特性に応じた標準的なフォーマットが存在する場合は、それも併せて記述する
データの帰属、知的財産の取り扱い	• データの帰属及び知的財産の取り扱いについて、データの利活用の方針に応じて記述する
データの公開、非公開及び猶予期間並びに引用	• データの公開について、機関のデータの利活用の方針に応じてデータ公開までの猶予期間を適切に設定し、それに基づく公開時期について記述する • 公開データの利用に際しては、利用者に対して適切な引用を求める。その際、識別子を用いた引用情報の記載ルールを設けるなど、他のユーザーが引用元のデータを参照できるよう配慮する

※「国立研究開発法人における データポリシー策定のためのガイドライン」H30. 6.29 国際的動向を踏まえたオープンサイエンスの推進に関する検討会 参照

3. 整理・策定フェーズ
3-2. データポリシーの検討：データポリシーのサンプル（1/2）

作成方針／アプローチ	• 別途受領した、gBizINFOのプロジェクト計画書を活用 • 計画書における、「第2章 政策の目的」を参照し、今後のgBizINFOのあり方を踏まえ、データポリシーにおける「原則・管理意図」のDraftを作成

記載内容（案）	• 「Gビズインフォ」の開発・運営にあたっては、オープンデータ基本指針等に基づき、諸課題の解決、経済活性化、行政の高度化・効率化、透明性・信頼の向上を図るべく、以下の観点でのデータの収集、管理、提供を行っていく
	  • 各省庁が保有するデータを収集し、一元的にデータ整形し、保管する
	  • APIによるデータ取得を進めることによりデータ収集作業の効率化を図る
	  • 一元化されたデータをアクセスしやすい形で公開する
	  • 品質・透明性の高い形でのデータ提供を追求する

3. 整理・策定フェーズ
3-2. データポリシーの検討：データポリシーのサンプル（2/2）

作成方針／アプローチ		• デジタル庁により公表されている「オープンデータ基本指針」を参照し、データポリシーにて定める基本ルールのDraftを作成 • 基本ルールは**「①データの定義・制限事項」「②データの帰属、知的財産の取り扱い」「③データの保存・管理・運用・セキュリティ」「④公開データの形式等」**の4項目にて構成
記載内容（案）	❶ データの定義・制限事項	• 全府省庁が保有する企業の資格、調達、補助金、特許情報などの行政が保有する法人活動情報 • データは、原則オープンデータとして公開
	❷ データの帰属、知的財産の取り扱い	• データの二次利用に関しては、原則として公共データ利用規約を適用する。
	❸ データの保存・管理・運用・セキュリティ	• 「各府省庁にしか提供できないデータ」、「様々な分野での基礎資料となり得る信頼性の高いデータ 」、または「リアルタイム性を有するデータ 」等の有用なデータについては社会的ニーズが高いと想定されるため、積極的な公開を図る
	❹ 公開データの形式等	• 構造化しやすいデータは機械判読に適した構造及びデータ形式で掲載することを原則とする • 構造化が困難なデータを含む全ての公開データは検索やAPI利用が容易になるよう、標準的なメタ情報を付加するとともに、データカタログサイトの利用等、メタ情報公開に向けた環境の整備に努める

- 参照元：オープンデータ基本指針（令和6年7月5日デジタル社会推進会議幹事会決定）

3. 整理・策定フェーズ
3-3. 策定すべき運用方針書、及び反映観点の一覧

- リスクアセスメントの結果に応じて、整備、検討が必要な方針書として、下記の3点を導出

#	対象となる運用方針書	記載・整理すべき観点	アセスメント区分
1	個人情報の安全管理措置　等	・個人情報の管理ファイルの定義（種別、保有件数、履歴　等） ・管理ファイルの運用体制の構築 ・個人情報保護委員会への届け出	リーガル観点
2	本人等からの開示等請求への対応	・開示請求の受付窓口の設置 ・問い合わせフォームの作成 ・開示情報の抽出作業の手順化 ・抽出データの承認プロセスの策定 ・開示データの受け渡し運用の整備（利用プラットフォーム） ・開示請求対応履歴の管理簿の作成	リーガル観点
3	データ取得・授受に関連する管理方針	・取得データ管理台帳の整備（保有件数、取得方法、廃棄運用　等） ・情報を閲覧／操作可能な権限の付与者の一覧化 ・重要データに関する操作の承認運用プロセスの定義 ・データの廃棄に関する手順、エビデンスの定義 ・業務委託先との情報取扱いに関する契約締結（守秘義務、監督者の設置、インシデント発生時の報告フロー　等） ・インシデント発生時の責任者の設置、対応フローの整備	データ観点

3. 整理・策定フェーズ
3-4. システム機能要求事項

- リスクアセスメントの結果より、以下の検討項目、対象画面を導出

	検討項目	対象画面
セキュリティ対策	**ユーザー認証基盤の構築**	事業者ユーザーログイン画面（新規開発）
	アクセス制御の設定	（無し）
ユーザー向け機能	**データ更新状況の画面表示機能の実装**	法人プロフィール（一般ユーザー向け）
	不正確データの更新防止機能の実装	事業者データ更新画面（新規開発）

	検討項目	対象画面
プライバシー・規約関連	**プライバシーポリシー・利用規約の確認ステップ**	詳細検索画面（一般ユーザー向け）
		事業者データ更新画面（新規開発）
		利用申請画面（既存）
	問合せ窓口情報の掲示	トップ画面／利用規約