資料２－１

PIAの取組の促進について

―PIAの意義と実施手順に沿った留意点―

（概要）

（案）

令和３年６月30日

Ⅰ．PIAの意義　①

- PIA　（Privacy Impact Assessment、個人情報保護評価）は、個人情報等の収集を伴う事業の開始や変更の際に、個人の権利利益の侵害**リスクを低減・回避するために、事前に影響を評価**するリスク管理手法（←事業の企画・設計段階から個人情報等の保護の観点を考慮するプロセスを事業のライフサイクルに組み込む）。

- PIAの対象範囲は、事業の規模や性質等によっても異なるが、最終的に消費者本人の個人情報等の保護を含む権利利益の保護にどれだけ資するかが重要。したがって、**個人情報等の取扱いにより影響を受ける消費者等の個人との関係を整理し、場面ごとにリスクを適切に評価することが不可欠**。また、委託先等の事業に関わる**利害関係者を含めて実施**することが望ましい。

- 消費者の不安や懸念を払拭するために、**個人情報保護法の遵守にとどまらない範囲も含めて対応することが重要**。

- PIAの実施範囲や取り組む視点は、事業分野毎に共通している部分もあると考えられ、**認定個人情報保護団体をはじめとした業界団体等が**、その事業分野における**PIAを実施するための基準や対象範囲、評価項目等を整理して、必要に応じてその構成員に共有していくことは有効**。また、事業者が実施したPIAの**妥当性を第三者の立場から評価することは、PIAの信頼性を高める上で有効**。

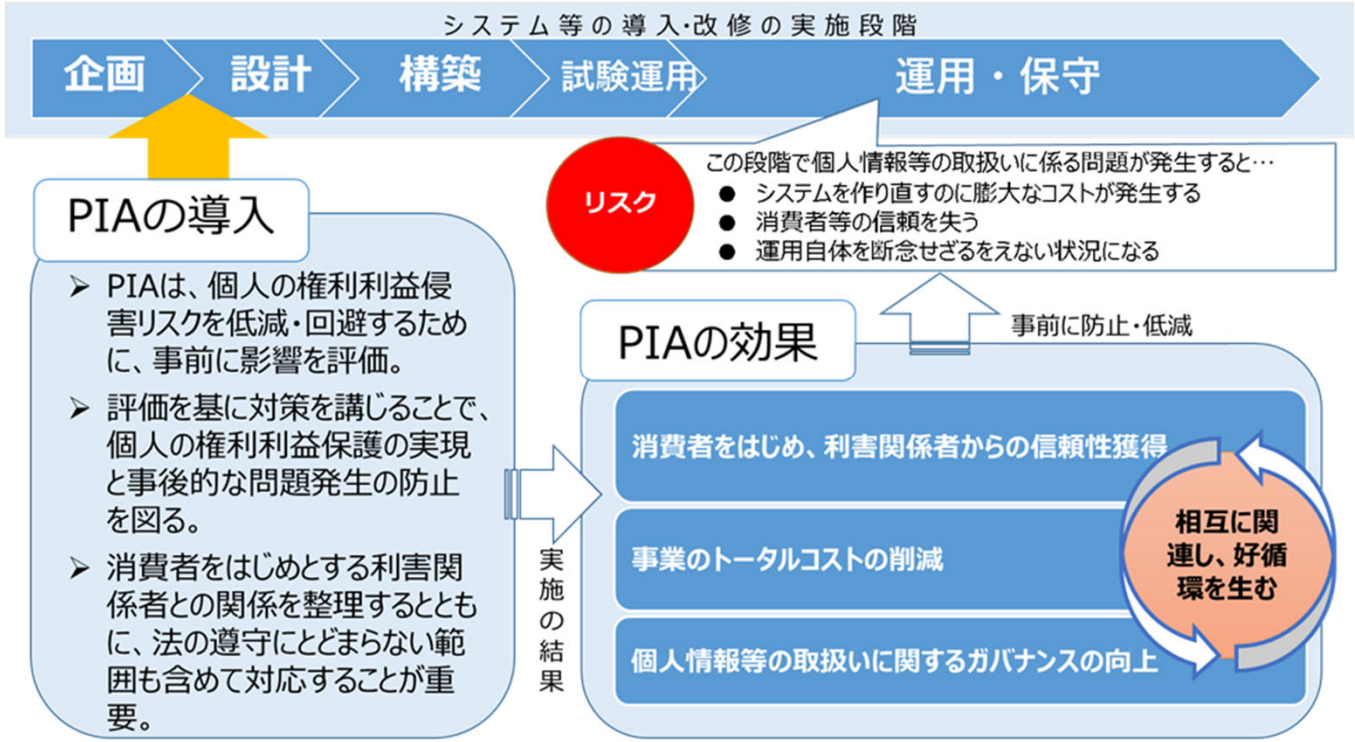
Ⅰ．PIAの意義　②

- PIAを実施する主な効果（これらは相互に関連）

① **<u>消費者をはじめとする利害関係者からの信頼性の獲得</u>** → 法令遵守やリスクを低減するために適切な対応を実施した旨の証明となり、社会的な信用を得ることに資する。また、結果の公表等により、説明責任を果たし透明性を高め、消費者・事業者間の情報の非対称性の解消にも資する。

② **<u>事業のトータルコストの削減</u>** → 多額のシステム投資や事業の中止を決定する前に、必要な対応が可能。結果として、事業のトータルでのコスト負担抑制。

③ **<u>従業者の教育を含む事業者のガバナンスの向上</u>** → 従業者が自覚を持つとともに、経営層も個人情報等の取扱状況等を把握することで、ガバナンス向上。



Ⅱ． PIAの実施手順に沿った留意点

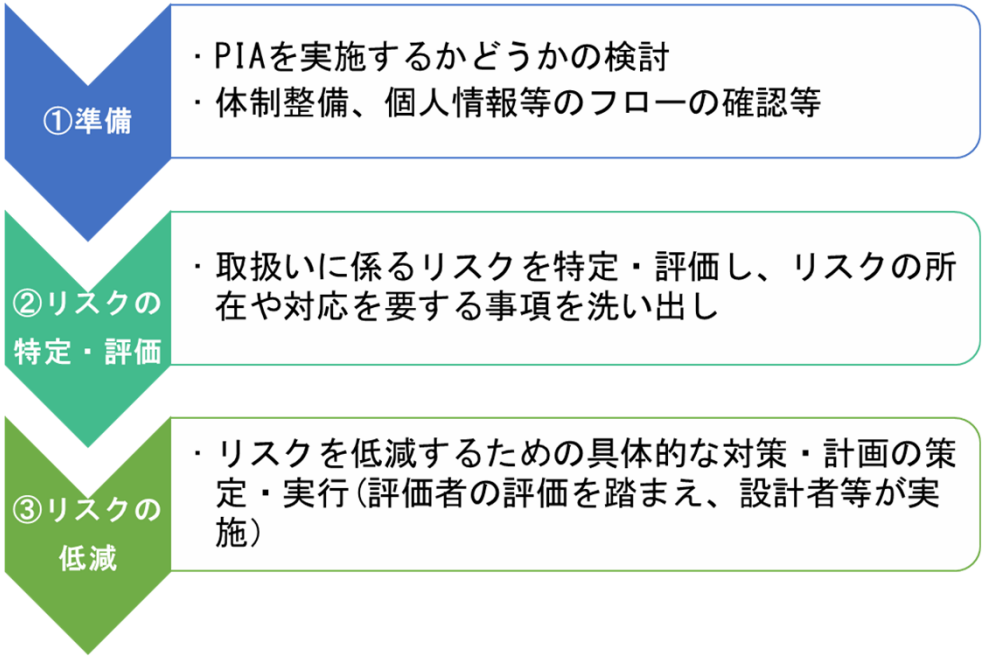
●プロセスの一例は以下のとおり。ただし、実施手法は**事業の規模、性質や個人情報等の内容等によって様々であり、事業者自身において、最適な手法を考慮していくことが重要**。

① **準備** → PIAを実施するかどうかの検討後、体制整備や個人情報等のフローの確認等の多角的かつ幅広い情報収集・整理を行う。

② **リスクの特定・評価** → ①の準備をもとに、評価者が個人情報等の取扱いに係るリスクを具体的に特定・評価し、重大なリスクや対応を要する事項を洗い出す。

③ **リスクの低減** → ②で評価者が特定・評価したリスクを低減するための具体的な対策・計画を設計者等が策定し、実効する。

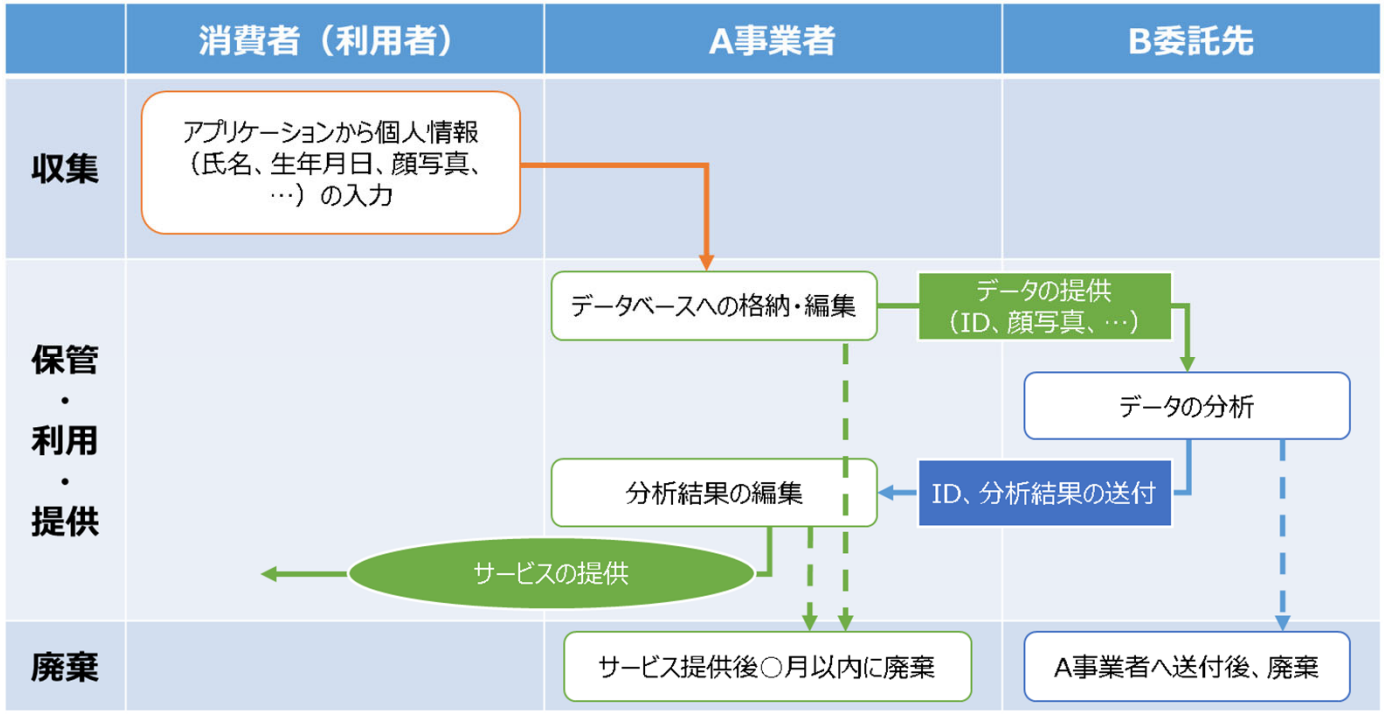
【一般的なPIAのプロセス】



Ⅱ． PIAの実施手順に沿った留意点（１．要否の検討、２．準備）

- 個人情報等を取り扱う業務の実施もしくは見直し等に際して、幅広く、PIAを実施する必要があるのか否かを検討。
- PIAを実施することを決定した場合は、**実施責任者の任命、投入人員数などリソース計画、スケジュールの策定など、実施のための体制整備が必要**。準備にあたり、**経営層がPIAの必要性を理解・認識した上で、必要なリソースを割り当てることについてコミットすることが重要**。
- 前提として、収集・保管・移転・利用・廃棄等の**プロセスごとに、個人情報等のフローを整理**しておく必要。また、**消費者や委託先等の利害関係者を関係主体として組み込むことが重要**。

【個人情報のフローの整理】



Ⅱ．PIAの実施手順に沿った留意点（３．リスクの特定）

- 整理したフローの段階ごとに、**事業者側のオペレーションなどに伴い想定されるリスク要因**、**消費者・利用者側の利用方法などに伴うリスク要因なども踏まえて、リスクを洗い出し**、整理することが求められる。
- リスク整理表を作成することが有効であり、個人情報保護法等の法令により求められること、公的機関の指針や業界ルールにより求められること、それ以外に事業の性質上求めることが望ましいこと等の区別を明確にしていくことが望ましい。

【リスク特定の着眼点の例】

- 利用目的の通知や同意の取得が本人に分かりやすい形で行われるか。
- 本人が、自らの個人情報等がどのように取り扱われることとなるか、利用目的から合理的に予測・想定できるか。
- 個人情報等が過剰に収集される可能性がないか。
- 本人からの各種請求への対応は滞りなく行われるか。
- 権限のない者が個人情報等に不正にアクセスする可能性がないか。
- 個人情報等の紛失、盗難又は不正に持ち出される可能性がないか。
- 不適正な個人情報等の編集、紐づけ、分析等の利用が行われる可能性がないか。
- 不必要に保有し続ける情報がないか。

【リスク整理表のイメージ】

	個人情報保護法	○○事業ガイドブック	その他
収集	・利用目的が通知・公表されているか ・不正な取得がなされていないか …	・利用目的の通知や同意の取得が本人に分かりやすい形で行われるか。 …	・事業に不要な情報まで収集していないか …
保管	・内容の正確性が確保されているか ・必要かつ適切な安全管理措置が講じられているか …	・示されているセキュリティ対策がなされているか。 …	・各種請求対応は円滑に行われるか。 ・消費者による機器の紛失等の際の処理が適切になされるか。 …
利用	・目的外の利用がないか ・不適正な利用がなされていないか …	・推奨されている手順に沿って利用がなされているか …	・処理のログが取られているか ・不適切な編集・分析が行われる可能性はないか …
提供	・第三者提供時にあたり同意を取得することとされているか …	移転先が本人に明示されているか …	・移転する情報は必要かつ最小限なものとなっているか …
廃棄	・必要ない情報は廃棄されているか …	・保存期間が設定されているか …	・廃棄時に複数人で確認されるか …

Ⅱ． PIAの実施手順に沿った留意点（４．リスクの評価①）

- 特定したリスクについて、**「影響度」及び「発生可能性」の観点**で評価を実施。
- リスク評価の基準は、数段階（無視できる、限定的、重大、甚大等）の基準を設定することが考えられる。

【評価基準の例】

（影響度）

レベル		基準
4	甚大	・利用者に回復不可能な多大な不利益が生じ、これに伴い、企業の信用失墜や経済的損失が生じる （心理的・身体的疾患、口座番号、暗証番号の流出等）
3	重大	・利用者に一定の不利益が生じるものの、回復可能であり、企業の信用等への影響はそれほど大きくない （迷惑メールの受信、アカウントの乗っ取り等）
2	限定的	・一部の利用者に不安感を与え、企業の信頼等に影響が及ぶ可能性があるが、その範囲は限定的 （サービスへのアクセス拒否、利用方法に関する説明不足等）
1	無視可	・利用者への不利益の程度は極めて小さく、企業への影響は無視できるレベル （同意取得時にアプリケーション上にチェックを入れる煩わしさ等）

（発生可能性）

頻度		基準
4	非常に高い	・安全管理等に不備があるため、リスク発生が容易に想定される （セキュリティ対策の不備で情報漏えい等が発生する等）
3	ある程度高い	・安全管理の一部に不備があるため、リスク発生の可能性がある （ノートPCや携帯電話などのモバイルの紛失等）
2	一定の可能性	・安全管理措置により、リスク発生の可能性は低い （注意喚起のメッセージが表示される中でのメール誤送信等）
1	非常に低い	・リスク発生の可能性は極めて低い （入館証読取機でセキュリティ対応の採られた室内の書類の紛失等）

Ⅱ． PIAの実施手順に沿った留意点（４．リスクの評価②）

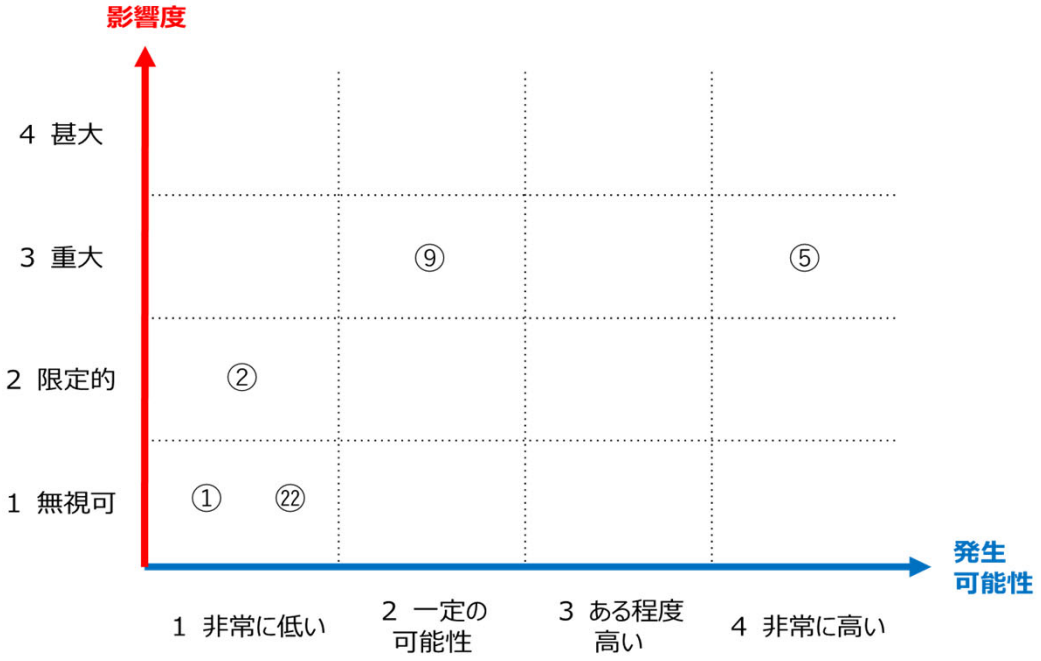
- 設定した基準に従い、特定した各リスクについて、**想定されている個人情報の取扱内容等に照らし、影響度及び発生可能性を評価**。

- 評価後、各リスクの分布を総覧的に把握し、対策を講じる優先度等の検討を行いやすくするため、影響度と発生可能性の二軸のリスクマップを作成することが考えられる。

【評価表のイメージ】

	特定したリスク	取扱状況、措置等	影響度	発生可能性
収集	①利用目的の通知や同意の取得が本人に分かりやすい形で行われるか	図も含めてアプリケーション上に内容を表示し、チェックを入れる設計となっている	1	1
	②事業に不要な情報まで収集されていないか	一部、利用目的と関連のない情報を取得する設計となっている	2	1
	…	…	…	…
保管	⑤○○事業ガイドブックに示されているセキュリティ対策がなされているか	一部、実施できていないセキュリティ対策がある	3	4
	…	…	…	…
利用	⑨処理のログが取られているか	ログは取るようにしているが、容易に編集・削除できるようになっている	3	2
	…	…	…	…
…	…	…	…	…
廃棄	㉒必要ない情報は廃棄されているか	サービス提供後、○月以内に廃棄されることとしている	1	1
	…	…	…	…

【リスクマップのイメージ】

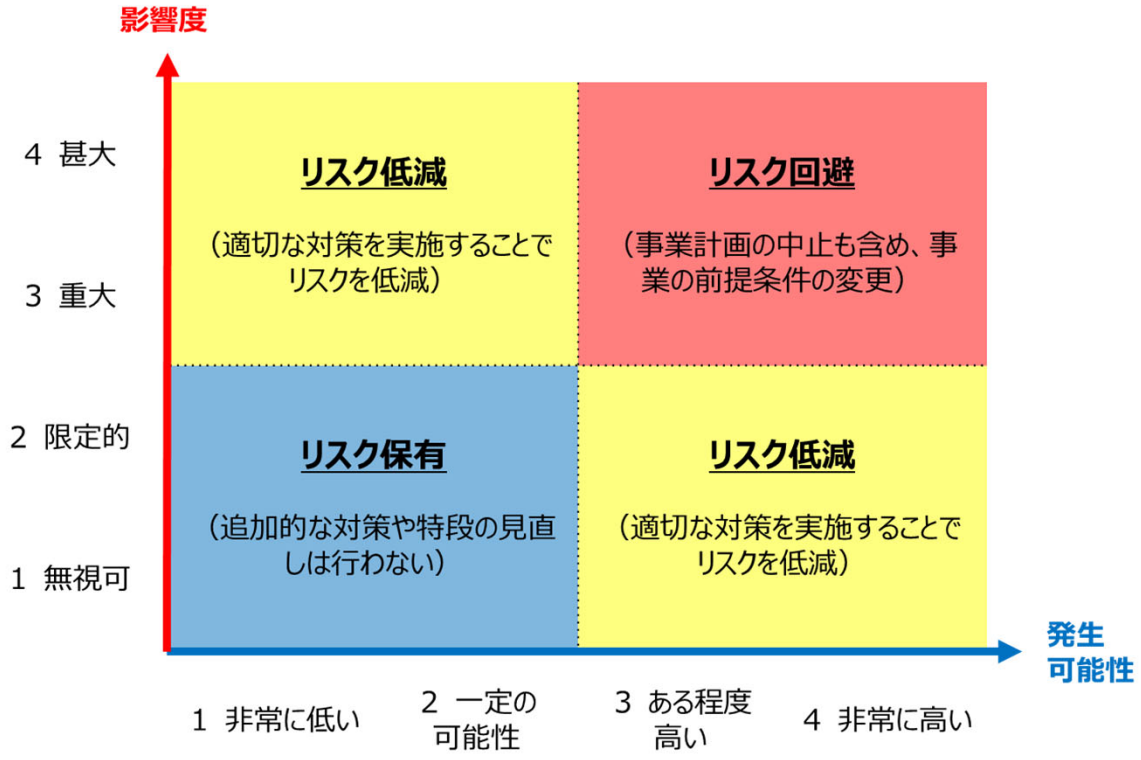


Ⅱ．PIAの実施手順に沿った留意点（５．リスクへの対応①）

●評価者が評価したリスクについて、例えば、以下のように設計者等が対応方針を決定。

- **影響度が高く、発生可能性も高い場合**は、事業の前提条件の変更など**リスクを回避**。
- **影響度は低いものの、発生可能性が高い場合、もしくは影響度は高いものの、発生可能性が低い場合**は、適切な対策を実施することで**リスクを低減**。
- **影響度が低く、発生可能性も低い場合**は、追加的な対策や特段の見直しは行わず、そのまま**リスクを保有**。

【対応方針の例】



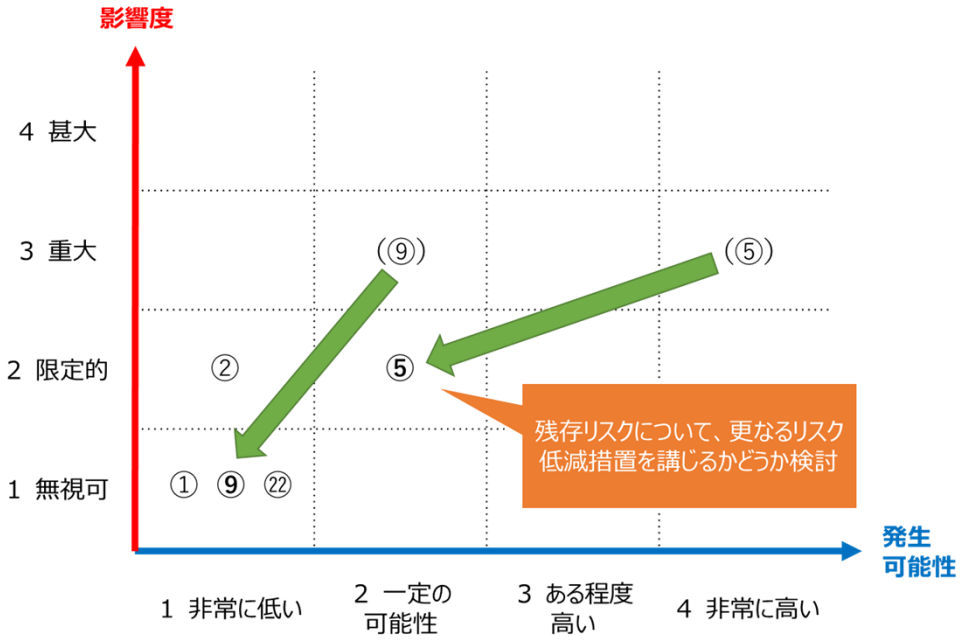
Ⅱ．PIAの実施手順に沿った留意点（５．リスクへの対応②）

- 対応方針を踏まえ、設計者等は具体的な対応策を検討。
- 対応策を踏まえて、影響度、発生可能性を再評価した上でマップを修正し、残存リスクについて、さらに低減等する必要があると判断した場合は、更なる対応策を検討することも考えられる。

【対応策の例】

特定したリスク	想定していた 取扱状況、措置等	対応策
…	…	…
⑤○○事業ガイドブックに示されているセキュリティ対策がなされているか。	一部、実施できていないセキュリティ対策がある	・推奨されているセキュリティ対策を実施 ・ …
…	…	…
⑨処理のログが取られているか	ログは取るようにしているが、容易に編集・削除できるようになっている	・ログにアクセスできる者を限定し、また監査部門がシステム監査を行う ・ …
…	…	…

【修正後のリスクマップのイメージ】



Ⅱ．PIAの実施手順に沿った留意点（６．PIA報告書のとりまとめ等）

- PIAの実施結果等について、**報告書としてとりまとめ、事業者の経営層への報告を行うことにとどまらず、対外公表することは、消費者をはじめとするステークホルダーへの説明責任と透明性の観点から有効**。

- もっとも、対外公表に際して、実施結果等の詳細まで提供する必要性は乏しく、むしろ、報告書の**サマリーを作成し、簡潔でより分かりやすい形で公表することが有効**。

- 報告書には、個人情報等の取扱いのフロー、当該フローのうちPIAの実施範囲、実施方法、特定したリスク、当該リスクの評価結果、対応策等について記載することが考えられる。

- 事案に応じて、報告書の内容について、**第三者機関のチェックを経て、信頼性を高めることも有効**。その際、特に消費者団体などの**消費者を代表する立場にある者からの確認を得る**ことが重要。