PIA（プライバシー影響評価）の進め方

2021年2月25日

電子情報利活用研究部

はじめに

- 令和元年12月13日**「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱」**では、特に、デジタル技術を活用した新たな利用分野において個人情報保護に関する問題が発生しやすい。また、このような分野ではビジネスモデルの変革や技術革新等も著しいため、法の規定を補完する形で、民間主導で自主ルールが策定、運用されることが望ましい。これらの取組を更に促進していく必要があり、具体的には**PIA（Privacy Impact Assessment、個人情報保護評価）の取組などを促進**していくとしている。

- ISOにおいて2017年PIAのガイドラインである「ISO／IEC　29134」の国際標準が制定され、それに基づき**2021年1月20日、日本産業規格JIS X9251として発行**された。

目次

PIAとは何か

プライバシー影響評価とは、

■ 環境影響評価（環境アセスメント）

- 環境に大きな影響を及ぼすおそれのある事業を実施する事業者が、その事業の実施に伴って生ずる環境への**影響について事前に調査・予測・評価**するとともに環境保全措置の検討を行い、**住民や行政機関などの意見も踏まえた上で、事業実施の際に環境の保全への適正な配慮を行う**ための仕組み。
  - 実際に、受け取った意見をもとに事業計画を調整、変更することも多い。
  - 環境影響評価法に定められ、①自然の良好な状態の維持ができるか、②人と自然のふれあいが維持できるか、③環境への負荷はどれくらいかについて、調査・予測・評価をしなくてはならない。

（出典：環境影響評価準備書の審査書、2015年12月）

■ プライバシー影響評価（PIA）

- プライバシー影響評価（以下、PIAという。）は、個人識別可能情報（以下、PIIという。）を処理するプロセス、情報システム、プログラム、ソフトモジュール、デバイス、その他の取組におけるプライバシーに対する**潜在的な影響をアセスメントするための手段**である。**取組の可能な限り早い段階から始まるプロセス**であり、取り組みの結果に影響を及ぼす機会がまだあることから、**プライバシーバイデザインを確実にするもの**である。

（出典：JIS X9251、2021年1月）

PIIの見つけ方

- プライバシー問題を起こさないようにリスクアセスメントする際には、取り組みで扱われる**情報**を把握しなければならない。
- ここでいう**情報**は、個人情報保護法の個人情報よりも広く個人に関連する情報について対象にしなければならない。
- JIS X9251が引用しているJIS X9250プライバシーフレームワーク（ISO/IEC29100）では、**個人識別可能情報（PII）の定義と、PIIの見つけ方**を示している。

◆ 個人識別可能情報，PII
（personally identifiable information）

a) その情報に関連するPII主体を識別するために利用され得る情報，又は
b) PII主体に直接若しくは間接にひも（紐）付けられるか又はその可能性がある情報。

注記 PII主体が識別可能か否かを判断するには，その個人を識別するためにそのデータを保有するプライバシー利害関係者（2.22），又は他の者が合理的に利用することができる，全ての手段を考慮するのがよい。

個人情報ではなく、PIIを捉える。
データではなく、人が相手だと認識する。

◆ PIIの認識（PIIの見つけ方）

個人を識別可能であるか否かを判断するには、複数の要因を考慮する。

- 識別子
  - ✓ マイナンバー等の識別子、及び識別子と紐付けられた情報
- 区別に役立つ他の特徴
  - ✓ 他人と本人とを区別する性質を持つ情報（基本4情報、生体情報、行動履歴等）
- 本人に紐づく、紐づく可能性のある情報
  - ✓ たとえ個人を識別できなくても（k > 1）、その情報が自然人について何かを表している場合、個人情報として取り扱うべき
- 仮名データ
- メタデータ
  - ✓ 写真のEXIF（日付、位置情報）など
- 意図せず取得したPII
  - ✓ 匿名フォームに入力された個人情報など
- 機微PII

プライバシー影響評価（以下、「PIA」）

■ 定義

- JIS本文3.7　個人識別可能情報（以下、PIIという。）の処理に関する**潜在的な**プライバシー影響の、**特定、分析、評価、協議、伝達及び対応の計画を立てるための全体的なプロセス**であって、組織のより広範なリスクマネジメントの枠組みに組み込まれたもの

■ 実施対象

- PIIを処理するプロセス，プログラム，ソフトウェア，モジュール，デバイス又はその他の取組み。

必要最低限の個人情報を取得し、考えられるリスクを最大まで軽減する運用とセキュリティ対策が施されるのであれば、「秘密」（プライバシー）は守られるという考え方

目的と効果

■ 目的

目的	解説
個人のプライバシー等の権利権益の侵害の未然防止	●**個人のプライバシー等の権利権益が一旦侵害されると、その回復は容易ではない**。 ●個人のプライバシー等の権利権益の保護のために、事前にPIIの取り扱いに伴うPIIの漏えいその他の事態を発生させるリスクを分析し、それらを軽減するための措置を講じておくことが必要。
利害関係者の信頼の確保	●入手するPIIの種類、使用目的・方法、安全管理措置等について利害関係者（提供するものによって正又は負の効果が与えられる者）に分かり易く説明し、その透明性を確保することが必要。 ●PIIの取り扱いにおいて個人のプライバシー等の権利権益の保護に取り組んでいることを自ら宣言し、どのような措置を講じているか具体的に説明することによって、利害関係者の信頼を得る。（例：契約上の義務を遵守している証拠の提供）

■ 効果

- ➢ 企業経営の観点
  - 課題を早期に特定し対策することで、管理上の時間・法的経費・社会懸念に対する対応コストが削減できる。
  - プライバシーリスクを管理する意識を高めることで、答責性が確立できる。
  - 自社のサービス等のブランド効果を高めることができる、など。

JIS X9251におけるベースとなる考え方

JIPDEC

■ プライバシーバイデザイン（Privacy by Design）

- PIIを処理するプロセス，プログラム，ソフトウェア、モジュール，デバイス又はその他の取組みにおいて**初期段階で実施**する。

■ 利害関係者のエンゲージメント（stakeholder engagement）

- PIAの準備段階で**利害関係者をエンゲージメント**（合意形成を図りその結果を約束）することで、実施するPIAのリスクを多角的に特定する。
- 評価結果については利害関係者に対し、**公表する**ことが推奨されている。

■ デューデリジェンス（Due diligence）

- ある行為者の行為結果責任を、行為者が法的に負うべきかを否かを決定する前に、行為に**先んじて払ってしかるべき正当な注意義務及び努力**。

個人情報を取り扱うシステムにおいて、構築、運用前に、利害関係者に影響を与えるプライバシーリスクに対し、利害関係者とアセスメント及び協議するといった事前にリスクを明確にする行為が、その結果責任に対し法的に負うべきか否かを決定するときの判断指標となる。

引用：JIS X9251解説　3 d)　デューデリジェンス

実施のタイミング（参考）

■ 推奨

- PIIを処理するプロセス，プログラム，ソフトウェア、モジュール，デバイス又はその他の取組み（新規開発または改変）を**開始する前**。
  - 要件定義（企画）、基本・詳細設計（設計）、開発（準備）など、どのフェーズからでも実施できるが、後工程で実施するほど、リスクを低減させる必要が発生した場合に、手戻り（コストや工数など）が大きくなる。

■ システムやサービスを改変等する場合の目安となる考え方の例

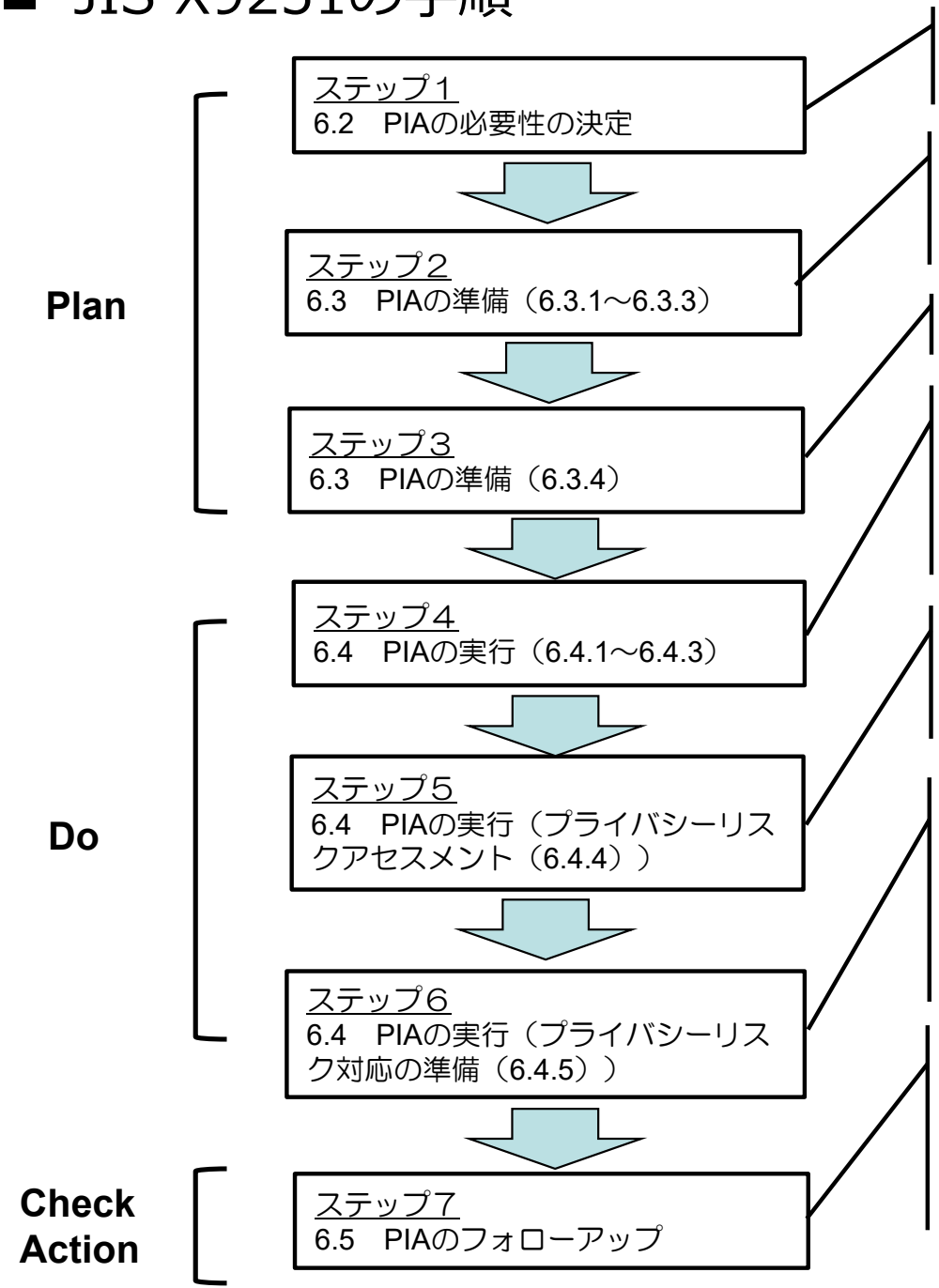
	確認する観点
1	PIIを新たに取得・保有・利用・提供し、従来のPIIの**範囲を拡大**するか。
2	PIIの**取得方法を変更**するか。
3	PIIを取得・保有・利用・提供・廃棄する既存の**業務手順に大きな変更**があるか。
4	PIIの取得・保有・利用・提供・廃棄の処理手順が変更されることによって、**想定外のPIIが利用または廃棄されたり、PIIを繰り返し取得する必要性**が発生するか。
5	**第三者からPIIを提供**され、又は当該データベースを**第三者と連携して利用**する事があるか。
6	取得されたPIIが、**目的外で利用**される事があるか。

	確認する観点
7	システムを利用する過程で生成した情報が、**保有しているPIIと結合して、プライバシーに影響する情報を生成**するか。
8	システムの新規構築又は変更において、PIIが格納されるデータベースの**アクセス制御、及び管理のためのセキュリティ対策に大きな変更**が発生するか。
9	従来のPII管理システムに、**特定技術等を適用**することにより、PIIが本人識別のできる形に変換されるなどプライバシー侵害が予期されるか。
10	構築予定のシステムが、**位置情報・生体情報など個人識別符号等を取得**し、サービスを提供する場合、プライバシー侵害が予期されるか。

PIAの進め方

PIAのプロセス　（6 PIA実施プロセスのガイダンス）

■ JIS X9251の手順



＜期待されるアウトプット＞

- しきい値分析の結果(6.2)
- PIAの実施要項及び範囲の判断

- 実施責任者の任命、リスク基準（6.3.1）
- PIAの実施計画、リソース計画（6.3.2）
- 評価対象のビジネスプロセス、情報システムの説明（6.3.3）

- **利害関係者のエンゲージメント（6.3.4）**

- PII情報フロー（収集、保管、移転、利用、廃棄）（6.4.1）
- ビジネスプロセス内の利用者のユースケースに関する調査結果の概要（6.4.2）
- プライバシー安全対策要件のリスト（6.4.3）

- プライバシーリスクの特定（6.4.4.1）
- プライバシーリスクの分析結果（6.4.4.2）
- プライバシーリスクマップ(6.4.4.3)

- プライバシーリスクに対する対応措置のリスト（6.4.5.1）
- 管理策のリスト、ISMSの枠組みにおける適用宣言書（6.4.5.1）
- プライバシー対応計画、管理計画、リスク管理責任者の承認、受容ステートメント（6.4.5.3）
- 対応措置の実装

- 公表する要素の意思決定、公表のためのPIA報告書（6.5.1）
- PIAパブリックサマリ、公表するPIA報告書（6.5.2）
- プライバシー対応計画の実装（6.5.3）
- レビュー報告書（6.5.4）
- PIAの再実施の意思決定（6.5.5）

PIAの準備
（評価計画を作成するまで）

ステップ1　– 6.2　PIA必要性の決定（しきい値分析）

- PIAが必要かどうかを判断する。
- 「実施のタイミング」以外に、参考になる考え方を以下に示す。

例	説明
特定個人情報保護評価	①対象人数（本人数）は何人か、②特定個人情報を取り扱う職員・外部委託先の人数は500人以上か、③過去一年以内に、特定個人情報の漏えい等に関する重大事故を発生させたかによって、基礎・重点・全項目評価を選択して実施する。（参考：https://www.ppc.go.jp/files/pdf/260114siryo3-6.pdf）
GDPR（一般データ保護規則）	・第35条において、DPIA（Data Protection Impact Assessment）として規定。 ・以下のケースの場合に実施する事が求められている。 – （a）**プロファイリングを含む自動的された処理**に基づいて自然人に関する個人的側面を体系的かつ広範囲に**評価**され、当該評価に基づいて決定がなされ、その決定が自然人に関して法的効果を発生させまたは類似の重大な影響を与える場合 – （b）第 9 条第 1 項で定める**特別なカテゴリーのデータ**、または第 10 条13 で定める有罪判決及び犯罪に関する個人データを大規模に取扱う場合。 – (c)**一般の人々がアクセスできる場所において大規模な体系的監視を行う場合。**
ある民間企業	・**プロファイリングの結果**を用いるサービス ・**センシティブ情報**を推測するサービス ・**オプトアウト方式、又は共同利用による提供を伴うサービス**

海外の例（2）

■ 英国Cygnet Health Careの例

- 以下のスクリーニングの質問を通して、潜在的なプライバシーの問題を浮き彫りにする。いずれかに「はい」と答えると、リスクを特定、評価、及び軽減するためにさらに分析する必要がある。

Q1.プロジェクト／プロセスには、**個人情報や機密情報の処理が含まれます**か？

Q2.プロジェクトでは、**個人に関する新たな情報を収集する**ことになりますか？

Q3.プロジェクトは、**個人に自分の情報を提供することを強制**しますか？

Q4.個人に関する情報は、**これまで日常的に情報にアクセスすることができなかった組織や人々に開示**されますか？

Q5.個人に関する情報を、**現在利用していない目的や方法で利用**しますか？

Q6.プロジェクトには、**生体情報や顔認証**など、プライバシーを侵害すると認識される可能性のある新技術の使用が含まれていますか？

Q7.このプロジェクトの結果、個人に大きな影響を与えるような方法で、あなたが個人に対して決断を下したり、行動を起こしたりすることになりますか？

Q8.個人に関する情報は、プライバシーに関する懸念や期待を抱かせる可能性があるか？例えば、健康記録、犯罪歴、またはその他の情報で、人々が私的なものと考える可能性が高いものはありますか？

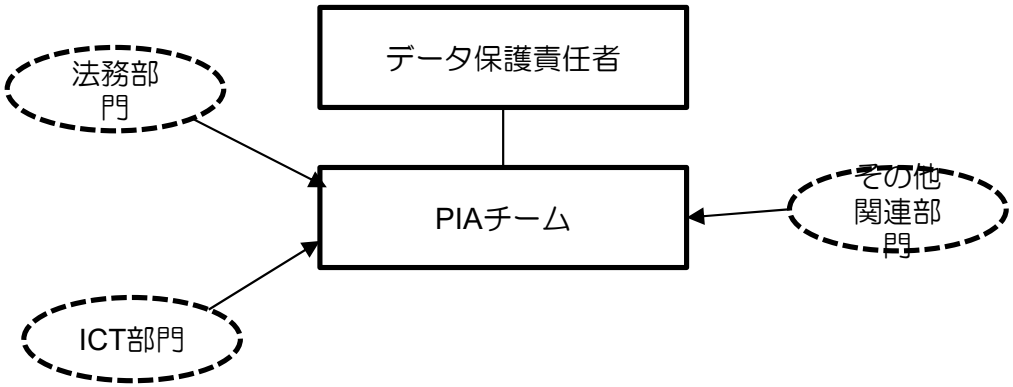
Q9.このプロジェクトでは、彼らが侵襲性が高いと感じるような方法で個人と接触することが必要になりますか？

Q10.このプロジェクト/プロセスは、PIAを実施せずにパイロットとして既に開始されているか？

ステップ2　-6.3.1　PIAチームの設置及び指示

■ 実行チームの編成：責任者や担当者を決める。

- ある民間企業の例
  - 責任者（法務担当執行役員）
  - メンバー
    - サービス企画部署（部長、課長）
    - 個人情報取扱責任者
    - セキュリティ管理者など。



■ リスク基準を定義する

- 利用情報のプライバシー性
- プライバシー影響度
- リスクの起こりやすさ

リスク基準の参照先
⇒JIS X9251の付属書A

※リスク基準は、組織が別々に定義してもよいが、上級管理職が必ず承認していること。

影響のレベルを測る　-　JIS X9251附属書A.2

■ 利用するPIIが利用者へ与える影響レベルの例

影響レベル	PIIの性質	例
1	一般的にアクセス可能なPII	電話帳、住所録など
2	アクセス制御が必要であり、且つ正当な利益を提供するPII	限定公開ファイル、配布リストなど
3	不正な開示が利用者の評判に影響を及ぼすPII	所得、財産、社会福祉給付など
4	不正な開示・変更・滅失・棄損が利用者の存在・健康・自由・生命に影響を及ぼすPII	誓約、刑罰、人事評価、健康データ、利用不能の債務など

リスクの起こりやすさを推定　- JIS X9251附属書A.3

■ リスクの起こりやすさを推定するレベルの例

レベル	説明	例
リスク小（実施を見合わせるレベルではない）	情報の特性を利用して、脅威が起きる可能性は無い。 （発生しても、速やかにトレーサビリティできる。）	入退出管理システムで保護された部屋に、アクセスコードで保護されたキャビネの中に保管された文書の盗難
リスク中（一定のリスクがあり、必要性とのバランスで判断する）	情報の特性を利用して、脅威がおきることは難しい。	入退出管理システムで保護された部屋に保管された文書の盗難
リスク中～大（きわめて慎重に判断する）	情報の特性を利用して、脅威が起きる可能性がある。	受付で入館手続きしなければアクセスできないオフィスに保管された紙文書の盗難
リスク大（実施すべきではない）	情報の特性を利用して、脅威を起こす事が容易である。	入退室自由なオフィスに放置された紙文書の盗難

参考　– 利用者への配慮を分析

■ 利用者への配慮を分析するための基準例

項目	説明		
プライバシー影響度	利用する情報のプライバシー性	基本情報、趣味趣向、取引履歴、利用履歴、財産情報、センシティブ情報、特定個人が識別できる画像等、身体・容姿に関する情報、位置情報	「使われたい」、「使われたくない」と利用者が感じる度合い
	利用目的のプライバシー影響度	顧客管理などの必要な業務、サービス提供、技術開発、マーケティング（自社・他社）、情報販売	
	利用時の加工状態におけるプライバシー影響度	生データ、統計、匿名加工、仮名、プロファイル	
利用者の予測可能性	データの取得時のプロセスを踏まえ、定められた目的で利用されることを利用者が予測できるか。		
利用者の受益	利用者がデータを利用されることによって、メリットを感じる度合い、又はそれを認識・実感する機会があるか。		
オプトアウト手段の提供の有無	オプトアウト手段の提供の有無（オプトアウト手段の認識度・簡便さ）、提供を拒否した場合の不利益の程度など。		
利用者への説明	提供する説明によって、利用者が理解できるか。		

参考　- 利用者への影響度の参考例

■ プライバシーリスクの影響度など測る指標の例

レベル	説明	例
リスク小（実施を見合わせるレベルではない）	１．利用者は影響を受けない。 ２．不都合（情報の再入力に要する時間、煩わしさ、いら立ち等）を体験する可能性がある。	入力項目が多いサービス
リスク中（一定のリスクがあり、必要性とのバランスで判断する）	１．利用者は対処が可能な重大な不都合（余分なコスト、アクセス拒否、不安、理解の欠如、ストレスなど）を体験する可能性がある。	スマホから入力ができないサービス
リスク中～大（きわめて慎重に判断する）	１．利用者は深刻な問題、対処が可能な重大な結果（資金横領、ブラックリストへの掲載、物的損害、失業、健康状態の悪化など）を招く可能性がある。	ネットバンクのID、パスワードを平文で入力するサービス
リスク大（実施すべきではない）	１．利用者は自ら克服することができない重大な、又は取り返しがつかない結果（返済不能債務などの財産的苦痛、就業不能、長期にわたる心理的身体的疾患など）を招く必要がある。	個人名と共に内定辞退率を提供するサービス

PIA実施計画書の作成　-6.3.2 PIA計画の作成リソースの決定

■ PIAを実施するにあたり、組織内で合意形成（決裁など）を行うために、実施計画書を作成する。

項目	内容
評価項目	PIA実施の必要性や背景を記述。
評価対象	評価対象となる個人識別可能情報（以下，PIIという。）を処理するプロセス，プログラム，ソフトウェア、モジュール，デバイス又はその他の取組み。
評価主体	評価チームの構成
評価機関	–
評価手法	例：「JISX9251を参照して実施する」など。
主要評価項目	重点的に評価をする事項
評価基準、評価項目	要求される評価項目、該当事業で特定技術の有無など。
資料収集、分析計画	PIA実施時に分析する必要がある関連参考資料を列記。
評価結果の整理	報告書の章立てなど。

ステップ３　-6.3.4 利害関係者のエンゲージメント

■ PIAの準備において、対象の製品、サービスに関わる多様な利害関係者（ステークホルダー）を特定し、エンゲージメントすることが大事。

- エンゲージメント（合意形成を図りその結果を約束、巻き込む）

■ 利害関係者の特定

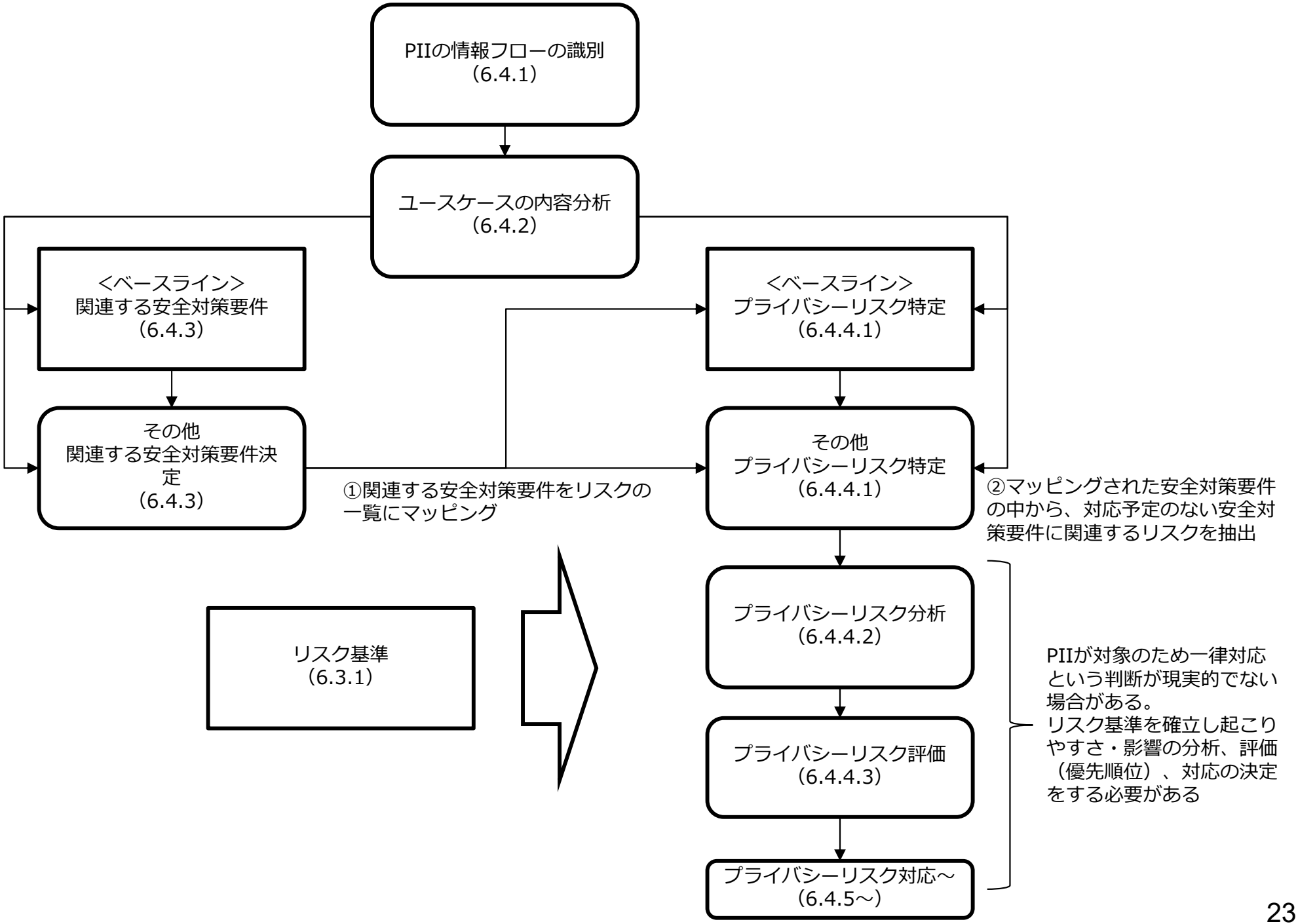
- 従業者（人事、法務、情報セキュリティ、事業運営部門など）
- PII主体などPIIの処理によって影響を受ける可能性のある個人
- 労働者及び消費者の代表者
- ビジネスパートナー、下請け業者
- アプリケーション及びデータベース管理者・作業者
- コンピュータ又はネットワーク管理者・作業者
- 保守要員など

■ 利害関係者との協議

- 組織は、利害関係者の視点を理解する。
- 利害関係者からのフィードバックなどはPIA報告書に記載されるとよい。

PIAの実行

PIAの実施プロセス概要　-6.4 PIAの実行



PIAの実施概観

■ サービス全体の説明の作成

- 「利用者が」見てわかる絵を描く事。
- 「利用者が」読んでわかる文章を作成する事。
- PIIについて「誰のPIIが、何のために、誰にどのように使われるか」を記載。

■ PIIのフローの作成

- 利用するPIIの取得・保有・利用・提供・廃棄のフローを作成する。
- 本当に必要なPIIであるかを精査する。
- 保有や廃棄の期間を確認する。

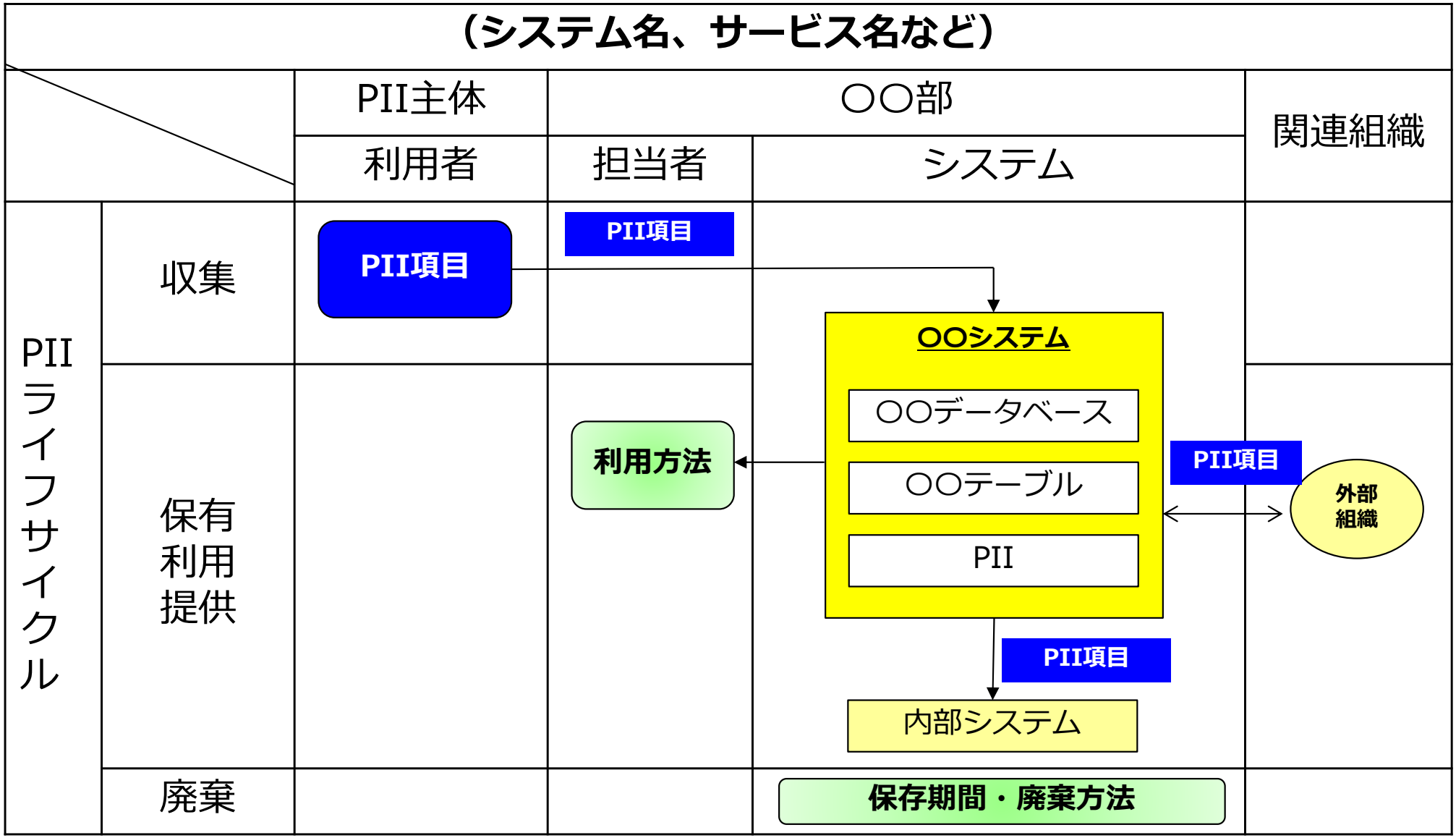
■ リスク項目の洗い出し

- 組織のリスクと、サービス等提供するもののリスクを分けて考えること。

■ 対策の洗い出しと選定

- ヒト・モノ・カネの観点から、ベストエフォート（できる最大限）の選択を行うこと。

■ フロー図は、PII処理業務別にPIIの収集・保有・利用・提供・廃棄の改定を俯瞰して把握できるように作成する。



＜記載例＞

評価用資料の収集　-6.4.3　関連するプライバシー安全対策要件の決定

項目	なぜ収集するのか	資料の例
事業説明資料	評価対象を通じて取得されるPIIの量と範囲が当該事業実施のために適切かを見るため。	・実施計画書など。
	外部連携の有無を確認するため。	・システム等の連携に関する計画書 ・委託計画など
内部資料	組織内の個人情報保護体系、規定などの分析のため。	・個人情報保護規定 ・セキュリティ規定 ・内部統制関連資料など。
	個人情報取扱者（情報システム運営者など）、委託事業者に対する規定、管理・教育体系、権限などを確認するため。	・アクセス権限などの内部規定 ・委託業者に関する管理規定 ・教育計画など。
	情報システムの構造と連携したPII保護技術を把握するため。	・セキュリティシステムの構成図など。
外部資料	個人情報保護に関するコンプライアンスの確認をするため。	・個人情報保護法。関連ガイドラインなど。
	政策環境文書	・PIAに関する政府機関発行文書など。

参考

- 個人情報保護管理者、セキュリティ実施責任者がいる企業の場合、既存でリスク分析をしているところが多い。その場合は、既存のリスク分析を利用して実施している事も多い。

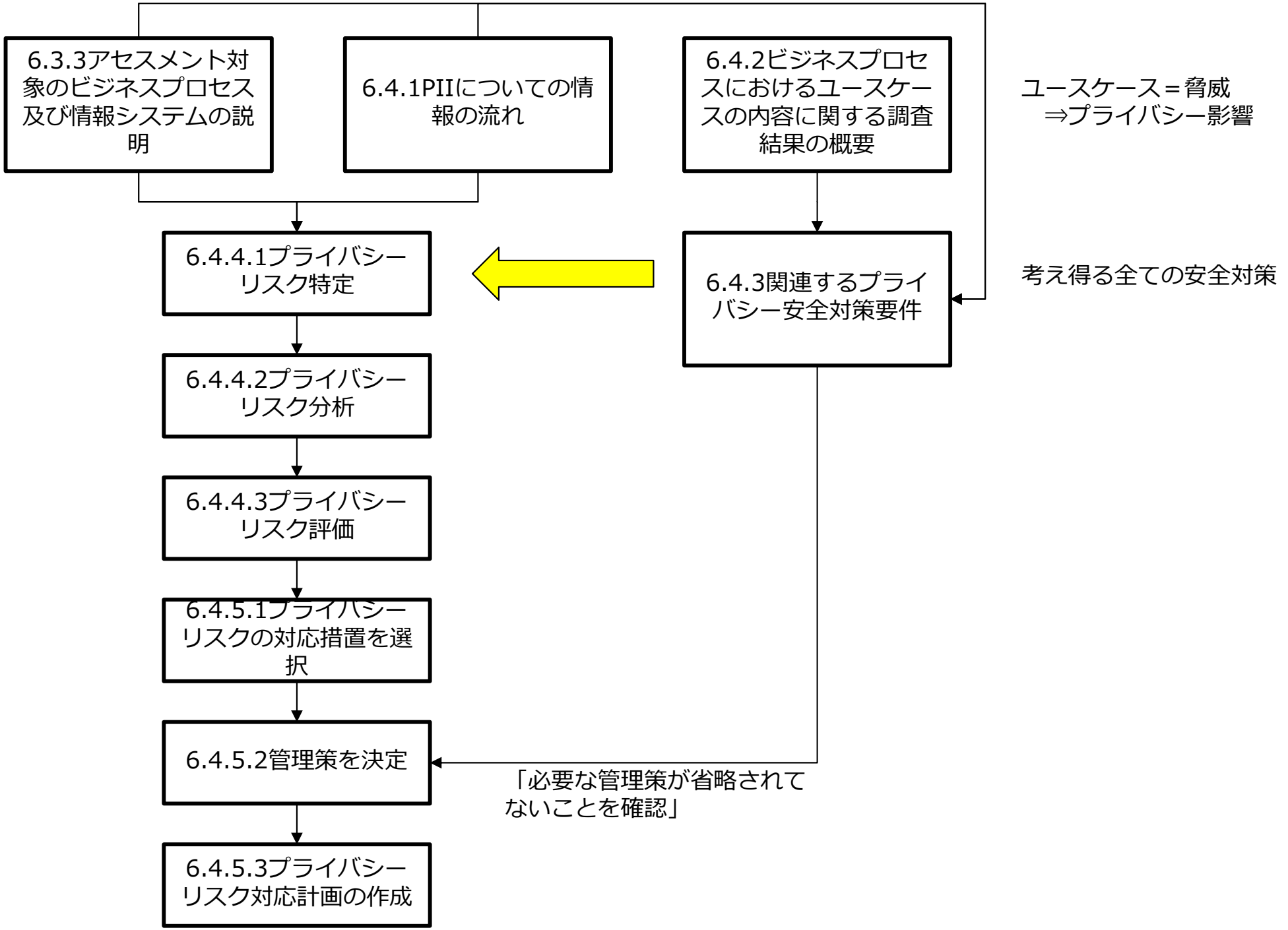
リスク分析の考え方

考え方

■ プライバシーリスクを
- PII主体の観点に基づくプライバシーリスク
- 組織の観点に基づくプライバシーリスク

に分けて検討する。

安全対策の要件をリスクアセスメントに反映



ステップ５　- 6.4.4.1 プライバシーリスク特定

■ 前提：利用者の基本的権利が守られているか。

■ その上で、以下を確認する。

- PIIへの認可されていないアクセスがあるか。（機密性の喪失）
- PIIへの認可されていない変更がされているか。（完全性の喪失）
- PIIの紛失・盗難、又は認可されていない持ち出しがあるか。（可用性の喪失）
- PIIが目的の達成に必要以上の取得をしていないか。（運用管理の喪失）
- PIIの認められていない・不適切な紐づけがされていないか。
- PIIの処理目的に関する情報が不十分でないか。（透明性の欠如）
- 利用者の権利（開示請求など）への考慮が欠如していないか。（アクセス権の喪失など）
- 利用者の認識又は同意無しにPIIを処理することはないか。
- 利用者の同意無しに、目的を変更することはないか。
- 不必要にPIIを長期間保有することはないか。

プライバシーリスクの分析　- JISX9251附属書A.2、A.3

JIPDEC

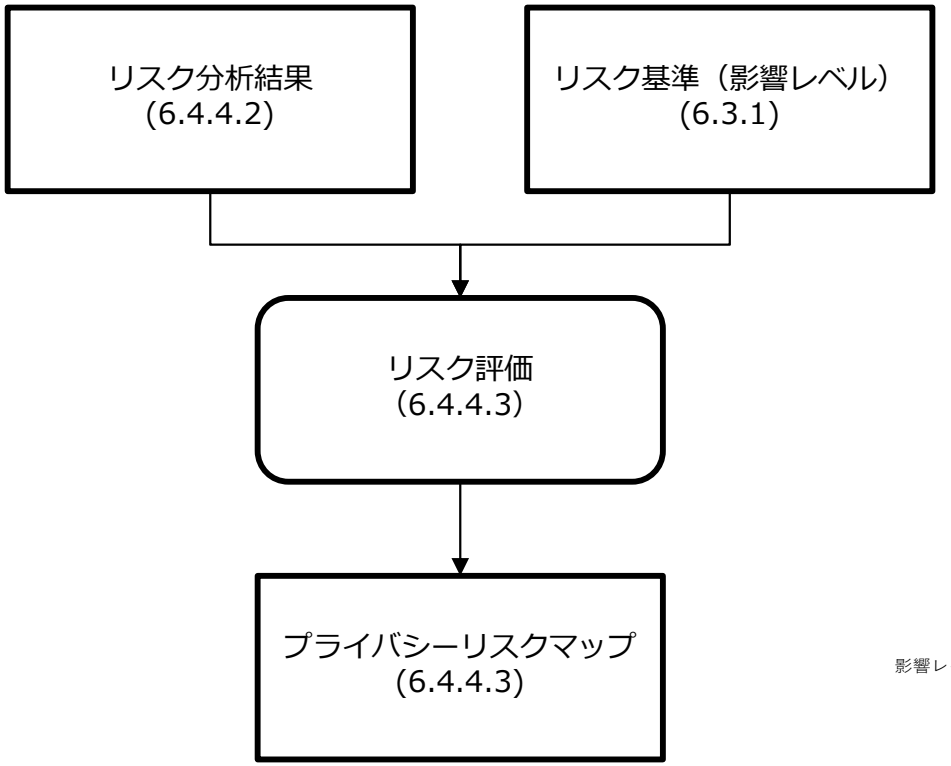
■ 利用するPIIが利用者へ与える影響レベルの例 - JIS X9251附属書A.2

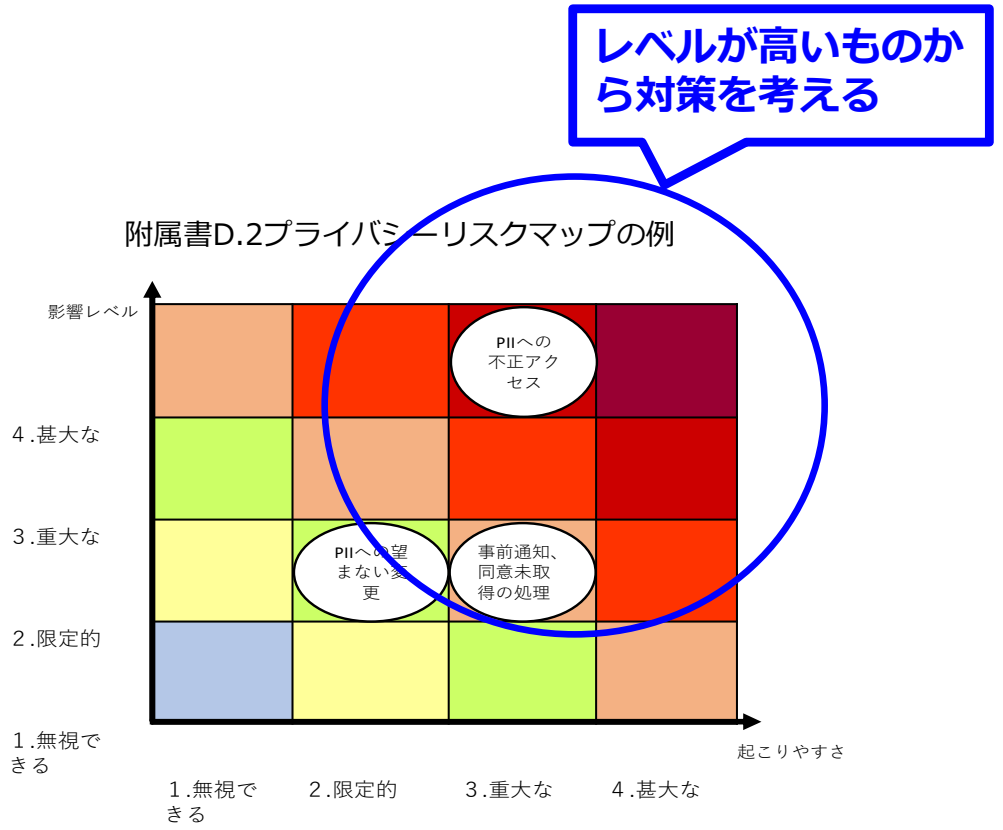
影響レベル	PIIの性質	例
1	一般的にアクセス可能なPII	電話帳、住所録など
2	アクセス制御が必要であり、且つ正当な利益を提供するPII	限定公開ファイル、配布リストなど
3	不正な開示が利用者の評判に影響を及ぼすPII	所得、財産、社会福祉給付など
4	不正な開示・変更・滅失・棄損が利用者の存在・健康・自由・生命に影響を及ぼすPII	誓約、刑罰、人事評価、健康データ、利用不能の債務など

■ リスクの発生のしやすさを推定するレベルの例　– JIS X9251附属書A.3

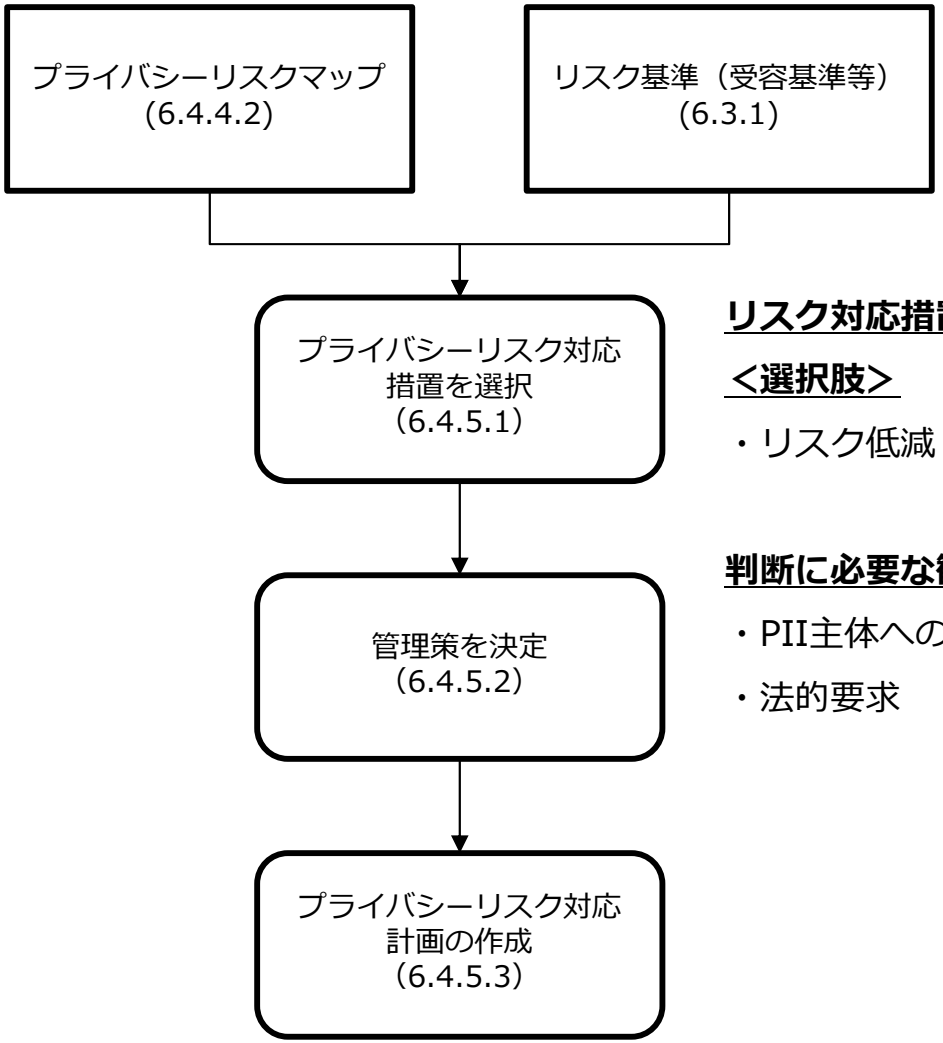
レベル	説明	例
リスク小（実施を見合わせるレベルではない）	情報の特性を利用して、脅威が起きる可能性は無い。（発生しても、速やかにトレーサビリティできる。）	入退出管理システムで保護された部屋に、アクセスコードで保護されたキャビネの中に保管された文書の盗難
リスク中（一定のリスクがあり、必要性とのバランスで判断する）	情報の特性を利用して、脅威がおきることは難しい。	入退出管理システムで保護された部屋に保管された文書の盗難
リスク中～大（きわめて慎重に判断する）	情報の特性を利用して、脅威が起きる可能性がある。	受付で入館手続きしなければアクセスできないオフィスに保管された紙文書の盗難
リスク大（実施すべきではない）	情報の特性を利用して、脅威を起こす事が容易である。	入退室自由なオフィスに放置された紙文書の盗難

プライバシーリスクの評価　-6.4.4.3 プライバシーリスク評価





リスク対応　-6.4.5 プライバシーリスク対応の準備



リスク対応措置を選択

＜選択肢＞

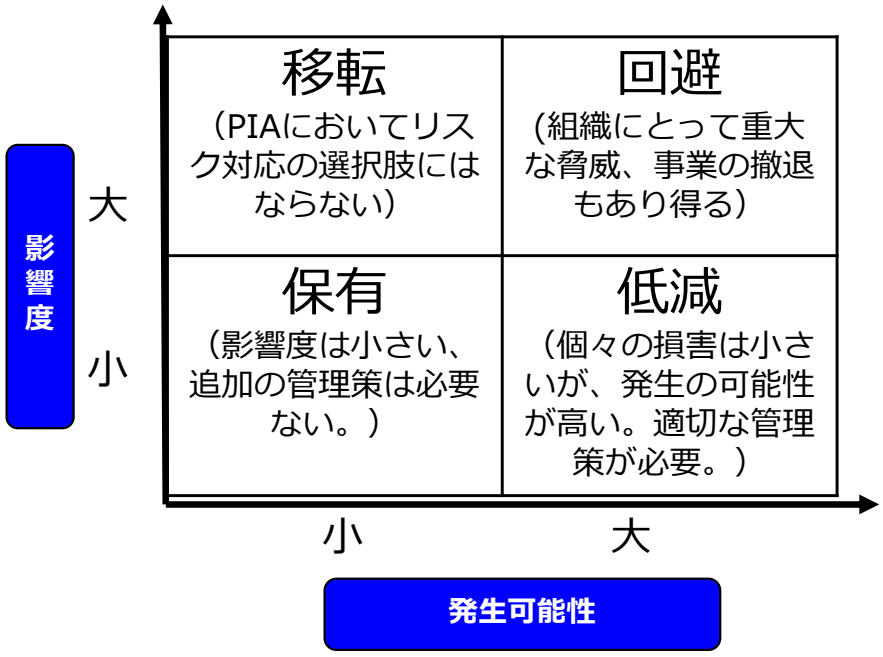
・リスク低減・リスク保有・リスク回避・リスク移転

判断に必要な観点

・PII主体への影響

・法的要求

ある企業におけるリスクマップの例



ステップ６　-6.4.5.1プライバシーリスクの対応措置を選択

■ リスク対応措置の選択肢

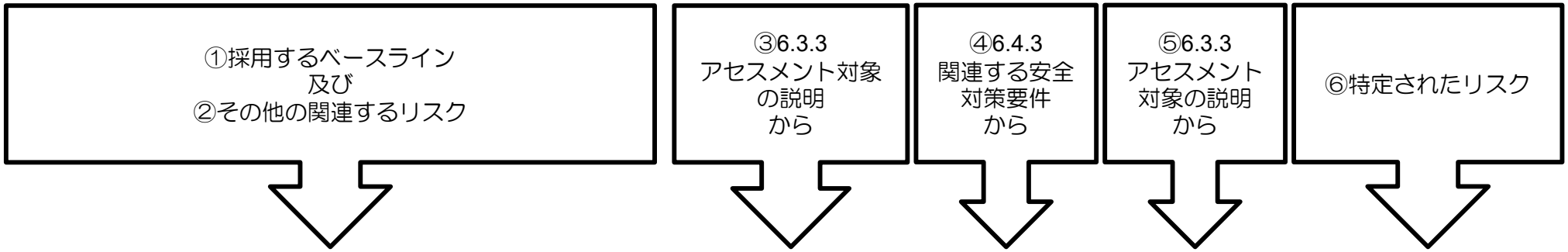
対応措置	説明
リスク低減	適切な管理策を選択することで達成できる。残留リスクが残っている場合は、受容できるかどうかを決定し、追加の管理策で対処する。 - 処理対象のPIIの種類を変更する - 組織構造、方針、処理手順の変更 - 従業者資格の変更（許可、研修、認定など）
リスク保有	リスクの影響レベルがリスク基準を満たしている場合は、追加の管理策を実施することなくリスクを保有することができる。
リスク回避	リスクが高すぎるとみなされる場合、組織はその事業から撤退する、あるいは活動条件を変更するなどによって回避する。
リスク移転	特定のリスクを外部委託するなどで移転することができる。ただし、リスク移転は、新しいリスクを生み出す可能性があり、それまで特定したリスクを変更が余儀なくされることはあり、その対応が必要になる場合がある。 また、リスク管理の責任を移転したとしても、影響の責任を移転することはできない。ステークホルダーは通常、悪影響の責任は当該組織にあるとみなす。

■ リスク管理策の洗い出し

- JIS Q 27001/2014附属書A
- ISO/IEC 29151の管理策
- 公認機関によって発行された管理策
- 自社で新たに開発し追加する管理策　など

リスク分析・管理策　-6.4.5.2 管理策の決定

■ どれくらいのダメージがあるのか、結果・計画又は、実施される管理策を考慮して推定する。

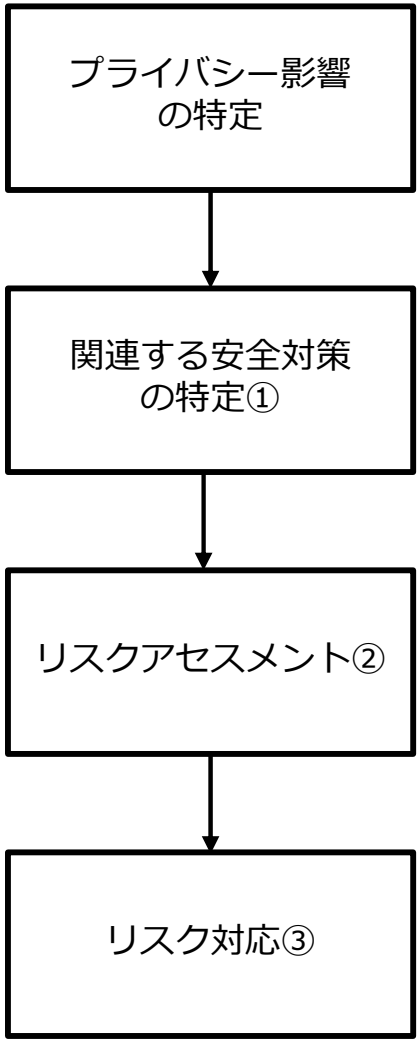


No	サポートする資産	アクション	プライバシーリスク	脅威の例	関連するユースケース システム	関連する安全対策	採用済み（計画済み）安全対策	特定リスク（脆弱性）	脆弱性 No
1	ハードウェア	異常使用	PIIの消失	個人ファイルの保管：個人利用	全般 指定場所以外のファイル保存等	**C.8.2.3**	・情報管理規定（業務外使用の禁止。ファイル管理のルール）	規定違反による保存（ファイルの保存に制限がない）	1-1
2	ハードウェア	異常使用	PIIへの不正アクセス	機微情報を取り扱う用途としては不適切なUSBフラッシュドライブ，メモリの使用，又は個人的な理由により実施する機微情報を含んだハードウェアの運搬	システムからのファイル出力	**C.8.3.1**	・情報管理規程（ファイルの持ち出し禁止） ・USBメモリーの使用制限 ・媒体使用ログの保管	-	2-1
									2-2

安全対策の要件をリスクアセスメントに反映

■ 安全対策の引き算で脆弱性を洗い出し

（考え得る全ての安全対策　－　想定（計画）済みの安全対策　＝　脆弱性）



ユースケース＝脅威の特定

考え得る全ての安全対策の洗い出し

特定：想定済みの安全対策と①の
ギャップを抽出
①－②＝脆弱性 の関係
分析：影響と起こりやすさの分析
評価：対応の優先順位を決定

リスク対応
受容の決定（残留リスク含む）
①＝②の想定済み安全管理策＋③

PIA報告書

ステップ７　－　6.5 PIAのフォローアップ

■ PIA報告書で示す内容

- システム要件情報：対象となる情報システムの処理の目的、機能要件リスト等
- システム設計情報：アーキテクチャの概要、データフロー図、PIIのライフサイクル
- 運用計画及び手順に関する情報
- リスク基準：影響レベル、起こりやすさの基準、リスク受容の基準
- 関連するリソース：チーム構成、PIA実施計画、予算
- 利害関係者協議：利害関係者の一覧、協議の方式、内容
- プライバシー要件：プライバシー安全対策要件のリスト
- リスクアセスメント
  - リスク源：特定したプライバシーリスク源の一覧
  - 脅威及びその起こりやすさ：脅威及び起こりやすさの一覧
  - 分析結果及びその影響レベル：特定された各リスクの影響レベル
  - リスク評価：リスクの影響レベルと起こりやすさを示すプライバシーリスクマップ
  - コンプライアンス分析：アセスメント対象の処理がプライバシー安全対策にどの程度従っているかの記載
- リスク対応計画
- 結論及び意思決定

報告書のフォーマット

■ 報告書のフォーマットは存在しない。

- 日本の場合には、特定個人情報保護評価の形式を利用するなどの方法が考えられる。
  - 但し、特定個人情報保護評価は、マイナンバーを使う事務単位評価になっているため、フォーマットを見直す必要がある。

- 民間で活用できるフォーマットの必要性は、**個人情報保護委員会とも共有しています。**

公表

■ PIAの結果を利害関係者に通知する。

- PIA報告書

- PIAパブリックサマリ
  - PIA報告書のうち、事業者の商業的に機微性の高い情報を削除し、PII主体に関連する重要な側面にとどめる。
    - プログラム、情報システム又はプロセスの便益
    - 処理及び収集されるPIIの種類
    - コンプライアンス分析の概要
    - 組織が実施したプライバシーリスク対応措置の概要
    - PII主体に推奨されるあらゆる措置
    - 責任を負うPII管理者の所属部署、連絡先
    - 利用者の対応窓口

以上。
ご清聴ありがとうございました。