プライバシー影響評価（Privacy Impact Assessment）

～ISO/IEC29134:2017 の JIS 化について～

目次

1. はじめに 2
2. PIA の概要 2
   2.1. PIA 実施の意義 2
   2.2. PIA 報告の目的 3
3. PIA の実施手順 4
   3.1. ステップ 1　PIA の必要性の決定 5
   3.2. ステップ 2　PIA の事前準備 5
   3.3. ステップ 3　アセスメント（評価）対象の説明 7
   3.4. ステップ 4　ステークホルダーのエンゲージメント（信頼構築） 8
   3.5. ステップ 5　プライバシー安全対策の決定 8
   3.6. ステップ 6　プライバシーリスクのアセスメント（評価） 9
   3.7. ステップ 7　プライバシーリスク対応の準備 10
   3.8. ステップ 8　PIA のフォローアップ 11
4. おわりに 12

1. はじめに

令和２年６月に成立した個人情報保護法（施行は、令和４年春の見込み。）には、プライバシー影響評価（Privacy Impact Assessment。以下、PIA という。）の実施を事業者に求めるという要件は含まれていない。しかし、令和元年 12 月の制度改正大綱において、民間の自主的取組の推進として、PIA の実施が推奨されている。このような動きに伴い DX を推進する組織は、個人識別可能情報[1]（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、ソフトウェアモジュール、デバイス又はその他の取組において、今まで以上にプライバシーに対するデューデリジェンス（善管注意義務）及びプライバシーバイデザイン（Privacy by Design[2]）の達成が求められることとなった。PIA は、潜在的なプライバシーへの影響を事前にアセスメント（評価）するための手段であり、ステークホルダーと協議してプライバシーリスクに対応するために必要な行動を起こすための手段である。PIA を実施することは、プライバシーバイデザインを達成することである。

当協会では、昨年度 PIA ガイドラインの国際標準である「ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment」を 10 名の有識者の協力の下で、JIS 原案（情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン）の策定を行った（令和３年２月頃に JIS 規格として発行される見込みである）。

このレポートは、個人情報保護法の改正を前に、これから PIA を実施しようと考えている組織のプライバシー保護担当者に、PIA の概要及び実施の概要について、JIS 原案の作成を通じて得られた知見をもとに取り纏めたものである。

2. PIA の概要

2.1. PIA 実施の意義

PIA が組織にもたらす効果と便益は、次のようなものがある。

① 計画的なプライバシー対策の達成と相対的なコスト削減

PIA は、対象のプロセス、情報システム等の計画段階など早期に実施し、PII 処理に起因する潜在的なプライバシーリスクを検出する方法を組織に提供する。そのため組織が多額の投資をする前に、予防策を講じてリスクに合わせた安全対策を構築することができるようになる。計画段階で対象のプロセス等を修正するコストは、後で修正が発生するコストに

---

[1] JIS X 9250 では、「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。」と定義されている。

[2] https://www.jipdec.or.jp/library/publications/pbd_book.html

比べれば少額である。またアセスメントによって受容できないプライバシーへの影響が認められた場合は、プロジェクトを中止することで大きな被害を未然に防ぐという決定もなされることもある。

② ステークホルダーとの信頼の構築

PIA 報告書は、プライバシーリスク又はプライバシー侵害が発生した場合、組織がその発生を防止しようと適切に行動したという証拠を提供することができる。これによって、組織へのあらゆる負債、レピュテーションリスク（負の評判及び信頼の喪失）を緩和あるいは排除することにも役立つ。適切な PIA を実施する組織は、そうでない組織に比べ顧客又は市民の信頼を得られる可能性がより高い。

③ PII におけるデューデリジェンス（善管注意義務）の達成

PIA は、オープンなコミュニケーションによって、ステークホルダーとの共通の理解及び透明性を促進するものである。また、PIA は組織の従業者及び契約事業者に対して、プライバシーに関する教育や、損害を与えるプライバシーの問題に注意を払うよう喚起する方法の一つでもある。組織は、PIA の実施をデューデリジェンスの証左とすることができる。

この規格で規定されていることは、

- **PIA のプロセス**
- **PIA 報告書の構成及び内容**

である。PII を処理するデータ処理システム及びサービスを運営する当事者及びプロジェクトの設計又は実装に係る組織（公開、非公開を問わず様々な企業、政府機関及び非営利団体）に適用することができる。

2.2. PIA 報告の目的

PIA 報告（公表）の目的は、組織の PII 処理が適正に PII を管理していることをステークホルダーへ伝えることとし、PIA 報告書あるいは PIA パブリックサマリによってステークホルダーへ報告（あるいは公表）することが推奨されている。

各局面における PIA への期待を、図表 1 に示す。

局面	PIA への期待
PII 主体（本人）	PIA によって、PII 主体のプライバシーが組織によって適切に保護されていることを保証する。
組織のマネジメント	PIA によって、プライバシーリスクを適切に管理し、組織内の意識を高め、責任が確立される。組織内の PII 処理を可視性のあるものにし、プライバシーリスク及び影響を可視化することで、事業又は製品の戦略構築へインプット情報を提供する。PIA をプロジェクトの初期段階に組み込むことで、製品又はサービス設計の変更など早い段階で再設

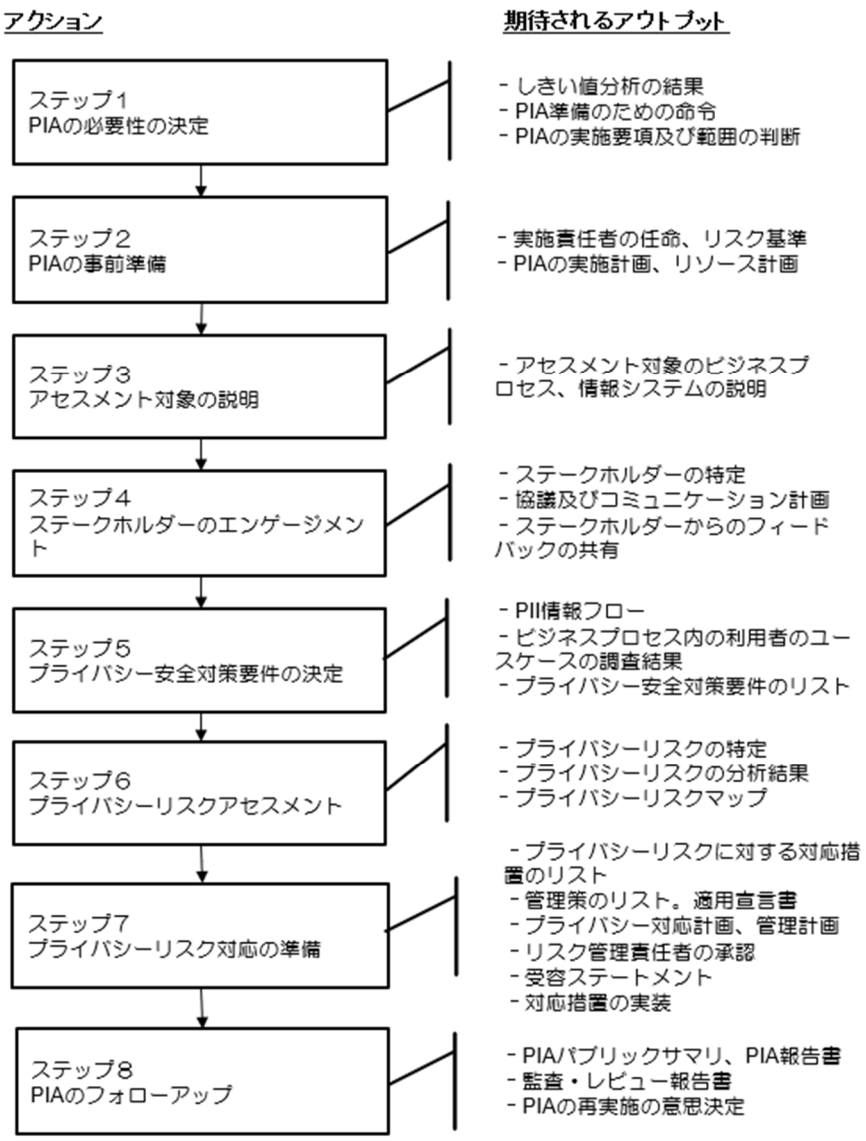
	計などの判断を行うことができる。
規制当局	違反、不遵守の疑い、消費者からの苦情などが発生した場合に、組織が実施した善管注意義務（デューデリジェンス）としての証拠とすることができる。
顧客	PIA は、PII をどのように扱っているかの評価手段であるので、組織が契約上の義務を果たしていることの証拠とすることができる。

図表 1　PIA への期待

3.　PIA の実施手順

PIA の範囲、対象、及びどのように実施されるかについては、組織の規模、国・地域の法域に合わせて行う。我が国においては、PIA を法的に実施する要件はないが、冒頭に記載したように、事業者の自主的取組として PIA が推奨される。また、PIA の対象となる特定のプログラム、情報システム又はプロセスごとに決定する必要がある。したがって、事業者が PIA を実施する際は、国際標準である ISO/IEC29134:2017 を参考に、自社に適した形で PIA の実施方法を策定することでもよいし、中小企業などにおいては、業界団体などが提供するガイドラインを参考にすることでもよい。

次に、ISO/IEC29134:2017 で示されたガイダンスを PIA 実施のステップに分けて解説する。図表 2 は、PIA の準備から実施、フォローアップまでの作業の流れと各ステップで期待されるアウトプットをまとめたものである。



図表 2　PIA 実施のステップ

3.1.　ステップ 1　PIA の必要性の決定

PIA の実施は、PII を処理するプログラム、情報システム又はプロセスをしきい値による分析を行い、その結果で PIA の実施が必要かどうかを決定する。実施する PIA は新規に行うものだけではなく、以前 PIA を行ったものの更新も対象となる。新規の PIA 又は PIA の更新が求められる場合、組織のマネジメントは PIA 評価者とともに実施要項を定義し、PIA の範囲を決めるための境界及び適用の可能性を決定する。

3.2.　ステップ 2　PIA の事前準備

- PIA 実施の責任者の任命、実施チームの立ち上げ

組織は、PIA 実施の責任者及び PIA 報告書を承認する責任者を任命する。PIA の実施は、組織内に専門チームを設置して実施してもよいが、PIA 実施の結果に信頼性と透明性を持たせるために専門的な知見を有する独立した第三者に委託してもよい。前者の組織内のチームが PIA を実施する場合には、実施した PIA の妥当性を検証するために独立した監査人に監査を要請することで、PIA の品質を保つことができる。また、PIA が確実に行われるようにするためには、組織のマネジメントによる強力で継続したサポートが必要である。PIA を確実に実施するという責任（アカウンタビリティ）と PIA 結果に対する責任（アカウンタビリティ）は、PII 管理者のトップマネジメントにある。

- リスク基準の定義

PIA の実施責任者は、リスクの重大性を評価するために使用するリスク基準を定義し、リスク受容のための基準を特定する。これらの基準は組織の上級管理職の承認を確実にしておく。

リスク基準は、ISO/IEC29134:2017（あるいは、これに対応する JIS 規格）の付属書 A に基づいて定義する。あるいはそれらを参考に組織の事情に合わせ個別に定義をすることでもよい。

プライバシーリスクの重大性を評価するために重要なことは、プライバシーリスクを PII 主体の観点と組織の観点に分けてリスク基準の定義を検討することである。

リスク基準の定義は、次のようなことを考慮する。

— 製品、サービス又はシステムは、利用者に対しどのような危害を与えるのか、とくに PII におけるプライバシーリスクの影響は、様々な種類のプライバシーを考慮する。
— 法的及び規制的要件、並びに個別の契約上の義務を考慮する。
— ステークホルダーの期待及び認識、並びに信用及び評判に対する否定的な結果を考慮する。
— PII 処理の運用上の可用性、機密性及び完全性の重要度を考慮する。
— 情報処理の戦略的価値を考慮する。
— 情報処理によってもたらされる現在の価値及び将来の機会といった戦略的価値を考慮する。

PIA の実施を第三者機関が行う場合は、組織の戦略的価値について言及することは難しいことから一般的な説明にとどまる可能性があるため、組織が補う必要がある。

- PIA の規模の決定

PIA の規模は、想定される影響がどの程度重大なものかによって決まる。例えば、会社の従業者だけの PII 処理プロセスであれば PIA は比較的小規模になるが、行政が市民を対象とした新しいシステムを導入するなどの場合は、ステークホルダーが広範囲になるため、非

常に大規模な PIA を実施する必要がある。

PIA の規模の決定は、一人当たりの PII の量／粒度、機微度、PII 主体の数、その PII にアクセスできる人数などが重要な要素となる。

- 実施要項の策定

PIA 実施の責任者は、リスク基準と PIA の規模を決定し、PIA の実施要項及び範囲を組織に提案する。

実施要項では、ステークホルダーへ意見聴取を実施するかどうか、PIA 報告書を誰に提示するのか、PIA の名目予算と期間、PIA 報告書又は概要を公表するのかについて明確にする。

- PIA 実施計画の作成

PIA 実施要項及び範囲を基に PIA 実施計画を作成し、PIA 実施のための人的リソース及び予算の割当を行う。計画は実施されるアセスメントの範囲に大規模なリソースが含まれているなど複雑性が高い場合は、PIA の繰り返しの実施を考慮に入れておく。

また、計画は、PIA のタスク、PIA チームの各人の役割分担、スケジュールを決め、特にステークホルダーと協議する場合は、協議が必要な理由、協議相手、協議方法など詳細に説明する。

この計画に基づいて、時間（工数）及びリソース等を見積り、必要な予算とリソースを組織のマネジメントへ要請し、組織のマネジメントは適切な予算とリソースを割り当てることを保証する。

3.3. ステップ 3 アセスメント（評価）対象の説明

アセスメント対象のプログラム、プロセス又は情報システムを説明するために、評価者は、システム要件情報、システム設計情報、運用計画及び手順に関する情報、並びに外部要因及び内部要因の状況から、ビジネスプロセス及び情報システムを説明する。具体的には、以下の問いについて明確にする。

— 処理される PII は何か
— 処理の目的は何か
— PII の処理によってもたらされる便益は何か
— PII 受領者はだれで、受領者は PII をどのように扱うのか
— PII の処理が実行されるビジネスプロセスは何か
— PII の処理によって影響を受ける PII 主体はだれか
— プライバシープロセスはどのように実行されるか
— PII 主体は組織からどのように通知され、同意を求められるのか
— デバイスやハードウェア、ソフトウェアなどのサポートする資産は何か

組織は、各 PII 処理について、使用する予定あるいは使用中のサポートする資産（利用者のものを含むハードウェア及びソフトウェア、通信ネットワーク、紙資料など）の場所などを特定する。この特定された情報システムやこれらのサポートする資産について、評価者は、運用の計画及び手順についての ID 管理及び利用者管理の方法、運用がどこで行われるのか、従業者あるいは委託事業者の PII へのアクセスの程度、バックアップ及びリカバリ方法、データの保有、削除及び廃棄の方法、システムの廃止などを協議する。

これらを明確にすることは、PIA を実施する評価者へのインプット、PIA 報告書への記載、及びステークホルダーのためのサマリー文書として使用することができる。

3.4. ステップ 4 ステークホルダーのエンゲージメント（信頼構築）

ステークホルダーの例としては、組織の従業者、PII 主体、消費者、ビジネスパートナー、ICT に関連する管理者、作業者などがある。組織は、PII を処理する可能性のある個人、又は PII の処理によって影響を受ける可能性のある個人など PII 主体を含む全てのステークホルダーの代表的な個人を特定する。

PIA 実施の責任者は、PIA 実施要項でステークホルダーとの協議が必要とされた場合、信頼関係を築くため協議計画を策定する。この協議計画には、ステークホルダーと協力して、プライバシーリスクを特定しアセスメント、あるいは PIA 報告書のドラフト版のレビューを通じてステークホルダーの関心を適切に把握しているかどうかを確認する。

これらの協議は、組織がステークホルダーの視点を理解することで、協議の結果を類似した他のプロジェクトに再利用できるなど、潜在的で重大な影響を最小限に抑えることができるという側面がある。

3.5. ステップ 5 プライバシー安全対策の決定

- PII の情報フロー

PIA 実施の責任者は、アセスメント中の PII 情報の流れをフロー図などで視覚化し、PII の取得方法と情報源、PII 処理の目的と方法、PII の保有と廃棄ポリシー、PII の管理と責任者、などについて明確にする。

- 潜在的な利用者のユースケースの分析

PII 主体によるデジタルデバイスの使用などの潜在的な利用者の利用行動は、しばしば意図しないプライバシーリスクをもたらす。このような利用者の行動の例として、

－ デバイスの OS のセキュリティ設定を不適切に変更
－ モバイルデバイスやスマートカードの紛失
— デバイスの誤操作やアプリの間違った設定
— マルウェアを埋め込んだメールや悪意のあるリンク先へのアクセスなど

などがある。

組織はこれらのビジネスプロセス内の利用者の行動がもたらすプライバシーリスクを特定する。

- プライバシー安全対策要件の決定

アセスメント中のプログラム、情報システム又はプロセスの目的に関連するプライバシー安全対策要件を決定するために情報フロー、ビジネスプロセスにおけるユースケースの調査結果からプライバシー安全対策要件のリストを作成する。

組織が、プライバシーリスク管理の枠組みを実装するためにプライバシー要件を特定し、計画されている又は既存の管理策並びに過去のプロジェクトの関連情報を洗い出すことで、評価者は考え得る全ての安全対策を考慮する。

3.6. ステップ 6 プライバシーリスクのアセスメント（評価）

- プライバシーリスクの特定

組織は、アセスメント中のプログラム、情報システム又はプロセスから生じるステークホルダーのリスクを特定し、分析し、評価する。プライバシーリスクには、

— PII への不正な
　アクセス（機密性の喪失）
　修正（完全性の喪失）
— PII の
　紛失、盗難又は無許可での持出（可用性の喪失）
　過剰な収集（運用管理の喪失）
　無許可又は不適切なリンク
　処理目的の情報が不十分（透明性の欠如）
　不必要な長期保有
— PII 主体の認識又は同意なしでの
　PII 主体の権利への配慮の欠如（例：アクセス権の喪失）
　PII を処理する（関連する法令又は規則で処理が想定される場合を除く）
　第三者と PII を共有又は異なる目的での利用

がある。何が起こるかを特定し、その結果どのようになるかの全てのシナリオを考慮するためには、技術的又は環境的な障害を含むシナリオも含まれる。したがって、プライバシーリスクを特定するには、関連性のある最新の情報、特定するための適切な知識を持つ人員の関与が必要である。

- プライバシーリスクの分析

評価者は、特定されたプライバシーリスクの潜在的な影響や脅威を分析し、それぞれの影響の度合や起こりやすさを推定し、原因となる要素が何かを特定する。

リスク分析は、危険にさらされる可能性がある PII 及び PII へアクセスする PC、スマートフォンなどのデバイスやネットワーク等の脆弱性を攻撃する外部の脅威、それに対する既存の管理策も対象とする。PII 主体に影響があるリスク源は、組織の管理の内外を問わず、可能な限り包括的なプライバシーリスクのリストにまとめる。

評価者は、リスクがもたらす結果及び起こりやすさに影響を及ぼす要因を特定し、既存の管理策の有効性について評価する。プライバシーリスクの影響度や発生の可能性が非常に高いと評価された場合は、リスクの要因を分解し、それぞれについて影響度や起こりやすさを分析することで、より適切な管理策を特定することができる。

次に分析したリスクの影響レベルをリスク基準により決定された尺度を用いてランク付けをする。リスクの推定は、その潜在的な結果（影響レベル）及び脅威（起こりやすさ）を数値で表現すると分かりやすい。リスク分析は、主要なリスクを明らかにするために一般的な指標による定性分析がよく使用されるが、必要に応じて、より具体的にするため定量的な分析を組み合わせて実施することでもよい。

- プライバシーリスクの評価

評価者は、PII 主体に対するプライバシーリスクの影響及び起こりやすさのレベルの評価結果からプライバシーリスクマップを作成する。プライバシーリスクの相対的な優先順位付けを行うことは、組織が限られたリソースをプライバシーリスクの対応のために配分する際に役立つ。

ISO/IEC29134:2017 には、付属書 D にプライバシーリスクマップの例示があるので参考にすると良いだろう。

3.7. ステップ 7 プライバシーリスク対応の準備

- 対応措置を選択

アセスメントされたプライバシーリスクごとに最も適切な対応措置を決定しリストを作成する。どの対応措置にするかの選択は、組織が PII 主体のプライバシーを保護するという義務と対応措置を実装するコスト及び対応工数とのバランスをとることを考慮し決定する。組織の対応策の意思決定は、組織のリスクの選好度又はリスクに対する態度、及びすでに確立されているリスク基準に影響を受ける可能性があるので注意する。それらを防ぐため、組織や評価者は対応策の選択において、必要に応じてステークホルダーから意見を求めるとよい。

対応策を実施するリソースは、通常、限られているため、リスク対応計画は、実施するリスクの優先順位を明確にする。また、プライバシーリスク対応後の残留リスクについては、意思決定者及びステークホルダーがリスクの性質及び度合を共通の認識としていることが望ましい。意思決定者は、残留リスクをモニタリングし、レビューし、必要であればさらに対応することとなる。

プライバシーリスクの対応措置には、リスク低減、リスク保有、リスク回避、リスク移転の４つの選択肢がある。

対応措置	内容
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。
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か、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者などへ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、又は特定したリスクが移転によって新たにリスク対応することが必要な場合がある。リスク移転により、リスクの管理責任を移転した場合でも、リスクの悪影響が出た場合、ステークホルダーは移転させた組織の過失であるとみなす。

図表 3　プライバシーリスクの対応措置

- 管理策の決定

選択されたリスク対応措置のための適切な管理策及び法的に求められる管理策を全て特定し、プライバシーリスクと選択された管理策を組み合わせた新たなリストを作成する。

管理策は、既存及び計画されている管理策に加え、必要に応じて国際規格又は公認機関によって発行された管理策から選択、あるいは組織が新たに開発し追加するなど考え得る全ての管理策を洗い出す。これらの管理策によって、リスクが受け入れ可能なレベルに修正されることの判断をもってリスクに対する処理は完了する。これらの選択された管理策の実施後の残留リスクについては、影響レベル及び起こりやすさを再確定し、プライバシーマップへ再配置する。

- プライバシーリスク対応計画の作成と実施

管理策のリストからプライバシーリスク対応計画、管理計画、各管理策を実施するコストの見積を策定し、リスク管理責任者の承認、及び残留リスクの受容ステートメントの承認を行う。

組織は、リスク管理責任者が承認したプライバシーリスク計画の対応策を実装し、実施経過をモニタリングする。

3.8.　ステップ８　PIA のフォローアップ

- PIA 報告書の作成と公表

報告書は、前述のステップ１～６から得られたアウトプットの結果を記載し、包括的な報

告書のどの要素を公表し、どの要素を適切なステークホルダーに通知するかを決定する。報告の要素によっては、組織の機密事項が含まれることがあるため、ステークホルダーへは、パブリックサマリで公表することでよい。

- PIA の見直しと監査

組織は、レビュー又は監査のポリシーを確立し、見直しのトリガーとなる重大性のしきい値を設定する。第三者によるレビュー又は監査は、PIA 報告書の信頼性を高め、透明性を向上させ、第三者の経験から学ぶことができ、PIA 実践の質を高めることにもなる。だが、もし、PIA が第三者によって実施されたものであれば、レビュー又は監査は同じ人物は避けた方がよい。

- プロセスへの変更の反映

組織は、ステークホルダーに提示した PII 処理に影響を与えるプロセス又は情報システム内の重大な変更があった場合、PIA を再実施するかどうかの意思決定をする。また、PIA 実施から一定の期間で PIA を更新するメカニズムを持つと良い。

4. おわりに

特定個人情報保護指針では、「特定個人情報保護評価は、諸外国で採用されているプライバシー影響評価（PIA）に相当するものである。」とされているが、プライバシー影響評価（PIA）と特定個人情報保護評価では、その対象と目的が明らかに違う。以下に相違点を示す。

- 根拠及び実施の主体

  プライバシー影響評価（PIA）は、ISO/IEC29134:2017 及び対応する JIS（JIS Q 9251 情報技術－セキュリティ技術－プライバシー影響評価のためのガイドライン）を根拠とするもので、実施後は国際規格に準じたものとして有効になる可能性がある。実施の主体も公的機関、民間を問わずプライバシー情報を扱う組織である。

  特定個人情報保護評価は、国内法である番号法第 27 条に基づくもので、公的な行政機関、地方自治体、特定個人情報を扱う民間の団体の健康保険組合などが対象である。

- 評価の独立性

  プライバシー影響評価（PIA）では、中立性、専門性を持つ第三者機関あるいは、組織の部門による実施の場合でも中立性、専門性が求められる。評価の妥当性は実施者と異なる第三者による監査によって保証される。

  特定個人情報保護評価は、行政機関などのシステム構築・運用する組織の自己評価である。

- 評価の対象

プライバシー影響評価（PIA）は、個人情報を扱うプログラム、情報システム又はプロセスについて実施する。

特定個人情報保護評価は、情報システムやサーバ単独で評価するものではなく、個人番号を含む個人情報保護ファイルなど特定個人情報を扱う（運用する）事務が対象である。

- 実施の時期

  プライバシー影響評価（PIA）は、情報システムの構築前に実施し、システムが内外の環境変化などで改修されるなどした場合は、必要に応じて再実施することを推奨している。

  特的個人情報保護評価もシステム構築前に実施するが、情報システムの運用・事務が対象となることから 5 年ごとの再実施が義務付けられている。

- 報告書

  プライバシー影響評価（PIA）は、根拠となる国際標準、ガイドライン等に則り、中立的な専門家が必要な評価事項を検討し、評価結果をまとめる。

  特定個人情報保護評価では、特定個人情報保護委員会が定める評価指針に則り、記述する。

- 報告書の公表

  プライバシー影響評価（PIA）は、公表は義務付けられるものではなく組織の判断に任されている。しかしながら、要約版などを用いてステークホルダーに通知することは組織にとってもメリットのあることとして推奨されている。

  特定個人情報保護評価では、公示することが義務付けられている。

- 実施の目的と動機付け

  プライバシー影響評価（PIA）は、計画的なプライバシー対策の実践と想定的なシステム構築前の実施による想定的なコスト削減、ステークホルダーとの信頼構築、組織のデューデリジェンスによってリピュテーションリスクの回避などがある。

  特定個人情報保護評価は、評価の実施により個人のプライバシー等の権利利益の影響を未然に防止し、国民の信頼を確保する。

特定個人情報保護評価と PIA では、上記のように違いがあって、特定個人情報保護評価＝PIA ではないことに注意が必要である。特定個人情報保護評価は、公的機関、自治体等を対象としているなど限定的で PII 処理の運用プロセスの評価のため民間事業者にとって取組にくいものである。それに比べて PIA は、新しい PII 処理システムに対して PII 主体の観点と組織の経営的な観点の双方からリスク基準を定義するなど、経営戦略に沿ったリスクマネジメントを形成することができる。また、すでに ISMS 適合性評価制度やプライバシーマーク制度を実施している事業者であれば、PIA を組み込むことで、より一層プライバシー保護への対応を強化することとなる。そのようなことから、PIA は事業者が取組やすいも

のであるといえる。

個人情報保護法の改正により、昨年 12 月に個人情報保護委員会が公表した個人情報保護法改正大綱では、個人情報を扱う民間事業者の自主ルールの策定、運用をさらに促進するよう求めており、PIA がその有用な取組として明記され推奨されている。また、現時点において、評価項目や手法等を規定し義務化するのではなく、民間の自主的な取組を促すことが望ましいとされている。当協会が進めている国際規格（ISO/IEC29134:2017）の JIS 化もそのような取組を一層促進するための取組である。近年、自治体をはじめ民間企業、団体等から PIA に関する問い合わせが増えている。ISO/IEC29134:2017 の JIS が制定された後も、ガイドブックや解説本など、自治体や事業者がプライバシー影響評価（PIA）を実施しやすい環境づくりを進めていくこととしたい。