HITACHI
Inspire the Next

匿名化に関する制度の国際動向

2018/2/22

株式会社 日立コンサルティング
美馬 正司

1. 匿名化に関する法制度(1)

HITACHI
Inspire the Next

制度的な取組は2000年まで遡る

国/地域	法規制	概要
米国	HIPAA(1996)	・HIPAAの中でプライバシールールとセキュリティルールを制定(2000年) ・プライバシールールでは、医療情報(PHI)を匿名化データをとして扱うために、専門家による方法と、セーフハーバーに基づく18属性の匿名化、という二つの方法を提示 ・2012年に匿名化の適切な実施を推進するためガイドライン策定
EU	データ保護指令(1995)	・「データ保護の原則は、匿名で提供されたことによりデータ主体を特定できなくなったデータに対しては適用されるべきではない」ことを提示
	データ保護規則(2018)	・「データ保護の原則は、匿名の情報、すなわち、識別された、または識別可能な自然人に関係しない情報、またはデータ主体が識別できない、またはもはや識別できないような形で匿名化された個人データには適用されない」ことを提示(前文) ・追加情報の利用なくして、特定のデータ主体に結び付ける(attribute)ことができない個人データを仮名データ(pseudonymous data)として定義
英国	Anonymisation : managing data protection risk code of practice(2012)	・英国におけるオープンデータの推進、データ保護指令が匿名化データを対象としていないこと等を背景として、データの適切な活用を推進するために作成されたガイドライン ・Data Protection Act(DPA)では完全なリスク無しの匿名化を要求していない。適切に匿名化するための考え方やケースを提示 ・匿名化の手法や技術については、代表的なものを付属資料として示しているが、詳細は記述していない

2. 匿名化に関する法制度(2)

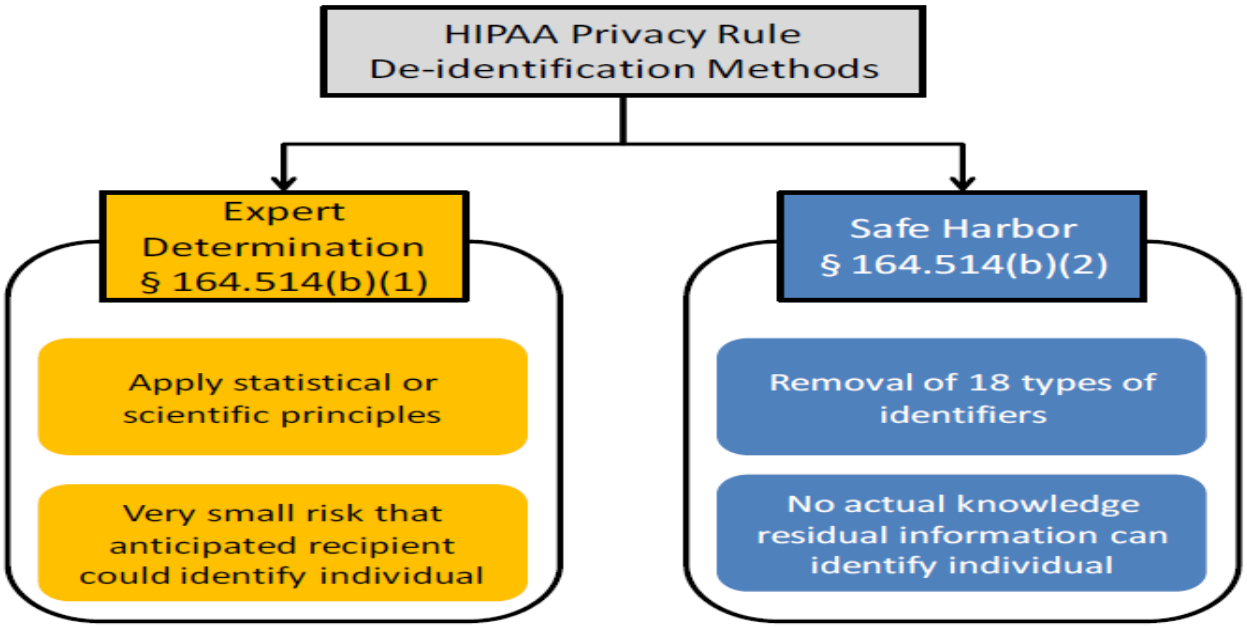
HITACHI
Inspire the Next

国/地域	法規制	概要
日本	個人情報保護法改正(2015)	・個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものを「匿名加工情報」と定義 ・匿名加工情報は個人情報保護委員会規則で定める基準に従い、加工、安全管理措置、情報の公表等を行うことが必要
韓国	匿名化のガイドライン(2016)	・国務調整室　行政自治部　放送通信委員会　金融委員会　未来創造科学部　保健福祉部という省庁横断的なガイドラインとして定められた。 ・第三者機関によって、匿名化したデータの名寄せを可能にしている。
豪州	De-identification Decision-Making Framework (2017)	・これは匿名化のプロセスに対する独立したガイドであり、データ状況を評価し、その状況におけるリスクを管理するための適切な環境やデータを基礎としたコントロールを選択するための原則的な方法を提供する、 ・このフレームワークは10のコンポーネント(実施項目)から構成されており、「データ状況の監査」、「リスク評価とコントロール」、「影響管理」の三つにグルーピングされている。
中国	情報セキュリティ技術　個人情報非識別化ガイドライン(2017)	・中国は、国家標準「情報セキュリティ技術　個人情報非識別化ガイドライン」に関する意見募集(パブリックコメント)を2017年8月に実施した。 ・パブリックコメントは10月までであったが、その結果を踏まえた正式版は2018年1月時点で公開されていない。
英国	Data Protection Bill (2017)	・英国では、EUから離脱、GDPR対応等を踏まえて、データ保護法の改定が検討されており、2017年9月にData Protection Bill(新データ保護法案)が議会に提出された。 ・同法案では、第6章の「執行」の部分において匿名化に関する事項が盛り込まれている。

3. 米国HIPAAの事例

HITACHI
Inspire the Next

- ✓Health Insurance Portability and Accountability Act(HIPAA)（医療保険の携行性と責任に関する法律）は、医療情報の使用、開示、および保護に関する要件を策定する法律であり、1996年に成立した。
- ✓その後、2000年にプライバシールールとセキュリティルールが定められ、前者において匿名化したデータの活用が示されている。
- ✓HIPAAのプライバシールールに基づき医療情報の匿名化が適切に行われるために、2012年11月、HHSが”Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule”を策定。
- ✓策定にあたっては、市民権局(the Office for Civil Rights:OCR)の協力を得て、匿名化に係る技術、実用、政策に係る経験を持つ人達によるワークショップを開催。
- ✓医療情報(PHI)を匿名化データをとして扱うためには、専門家による方法と、セーフハーバーに基づく18属性の匿名化、という二つの方法を提示。



4. 韓国の事例(1)

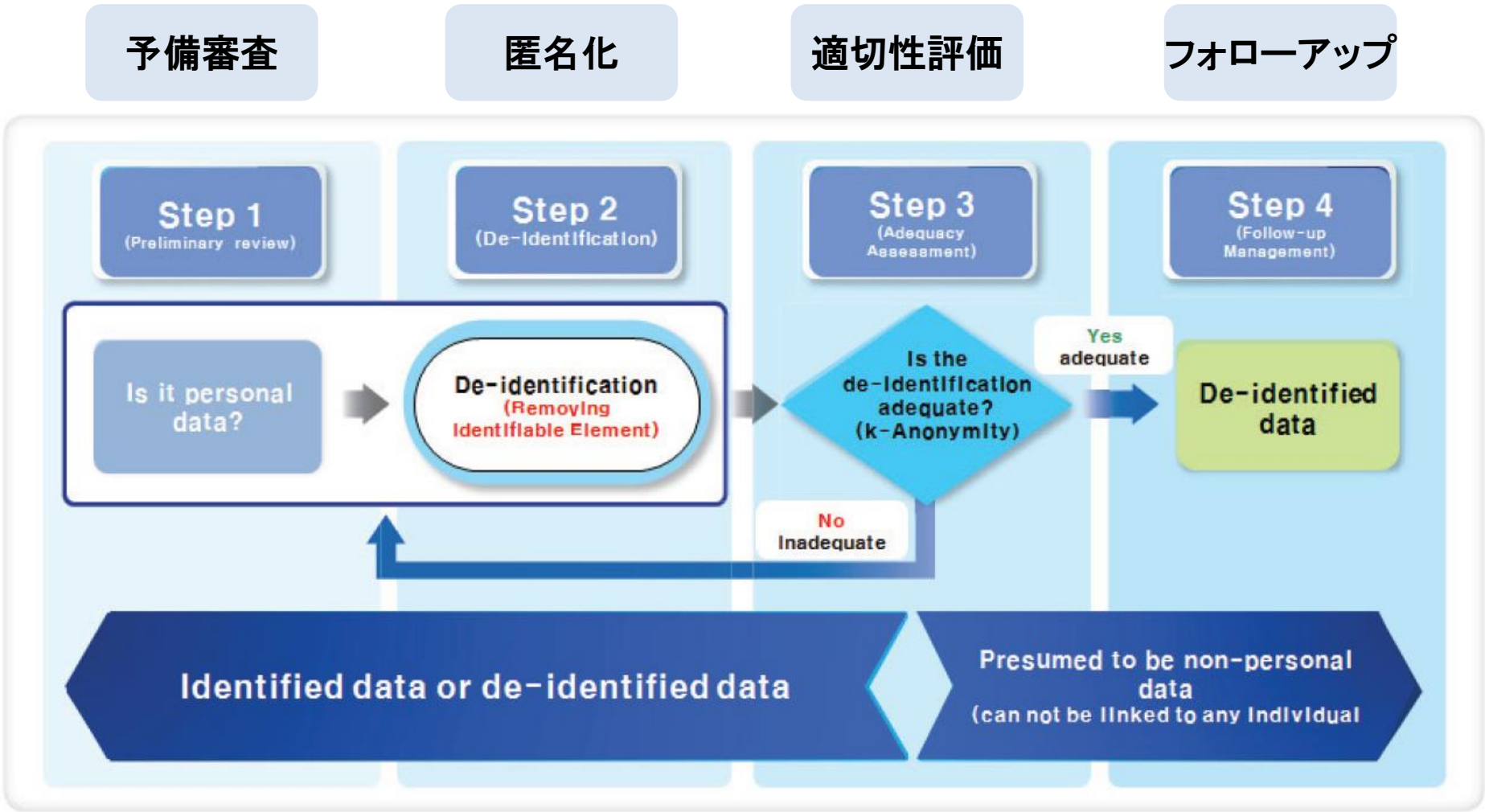
HITACHI
Inspire the Next

- ✓韓国では「個人情報保護法 」が2011年3月に公布され、同年9月に施行されている。
- ✓匿名化技術に関連した法制度としては、「個人情報保護法」の補足として「ビッグデータのプライバシーガイドライン 」が2014年12月に放送通信委員会において策定されている。
- ✓同ガイドラインでは、匿名化を行い、それについて公表すれば、第三者提供等も可能であることが示されている。ただし、機微な情報の推定等は禁止されている。

条項	内容
収集時から個人情報の徹底した匿名化（非特定化）措置	個人情報が含まれている公開された情報と利用履歴情報は、匿名化（非特定化）処理を行った後、収集･保存･組み合わせ･分析及び第三者の提供等が可能
ビッグデータ処理の事実･目的等の公開を通じた透明性の確保	匿名化（非特定化）措置後、ビッグデータ処理の事実･目的･収集源と情報活用拒否権行使の方法等を利用者にプライバシーポリシーを介して公開
個人情報の再特定時における即時破棄及び再匿名化（非特定化）措置	ビッグデータ処理によって生成された情報（分析結果や2次生成物）から個人情報が再特定された場合、すぐに破棄し、追加の匿名化（非特定化）措置するようにする
情報通信の秘密の収集･利用･分析等を禁止	・特定の個人の思想･信条、政治的見解等機微な情報の推定を目的とする情報の収集･利用･保存･組み合わせ･分析等の処理を禁止 ・電子メール、テキストメッセージ等の通信内容の収集･利用･保存･組み合わせ･分析等の処理を禁止
収集された情報の保存･管理時に「技術的･管理的保護措置」の施行	・匿名化（非特定化）措置がとられた情報を保存･管理している情報処理システムの技術的･管理的保護措置の適用

- ✓「ビッグデータのプライバシーガイドライン」において匿名化データについて第三者提供等が可能になることが示されたものの、引き続き具体的な匿名化の在り方が政策的な課題になっていたと推察される。
- ✓欧米のデータ活用促進、国内のデータ漏えい事件を背景に、個人データ保護の現在の法的境界内でビッグデータの安全な利用のため、匿名化データの活用に必要な個人データの匿名化の標準や範囲について明らかにすることを目的として「個人データの匿名化のためのガイドライン 」を2016年6月30日に国務調整室、行政自治部、放送通信委員会、金融委員会、未来創造科学部、保健福祉部等韓国政府の共同の取組として公表した。
- ✓同ガイドラインでは、匿名化の具体的な手順等である「匿名化の標準」と、その具体的な導入を推進するための「サポートと管理のシステム」が示されている。以下、その具体的な内容について整理する。

5. 韓国の事例(2)



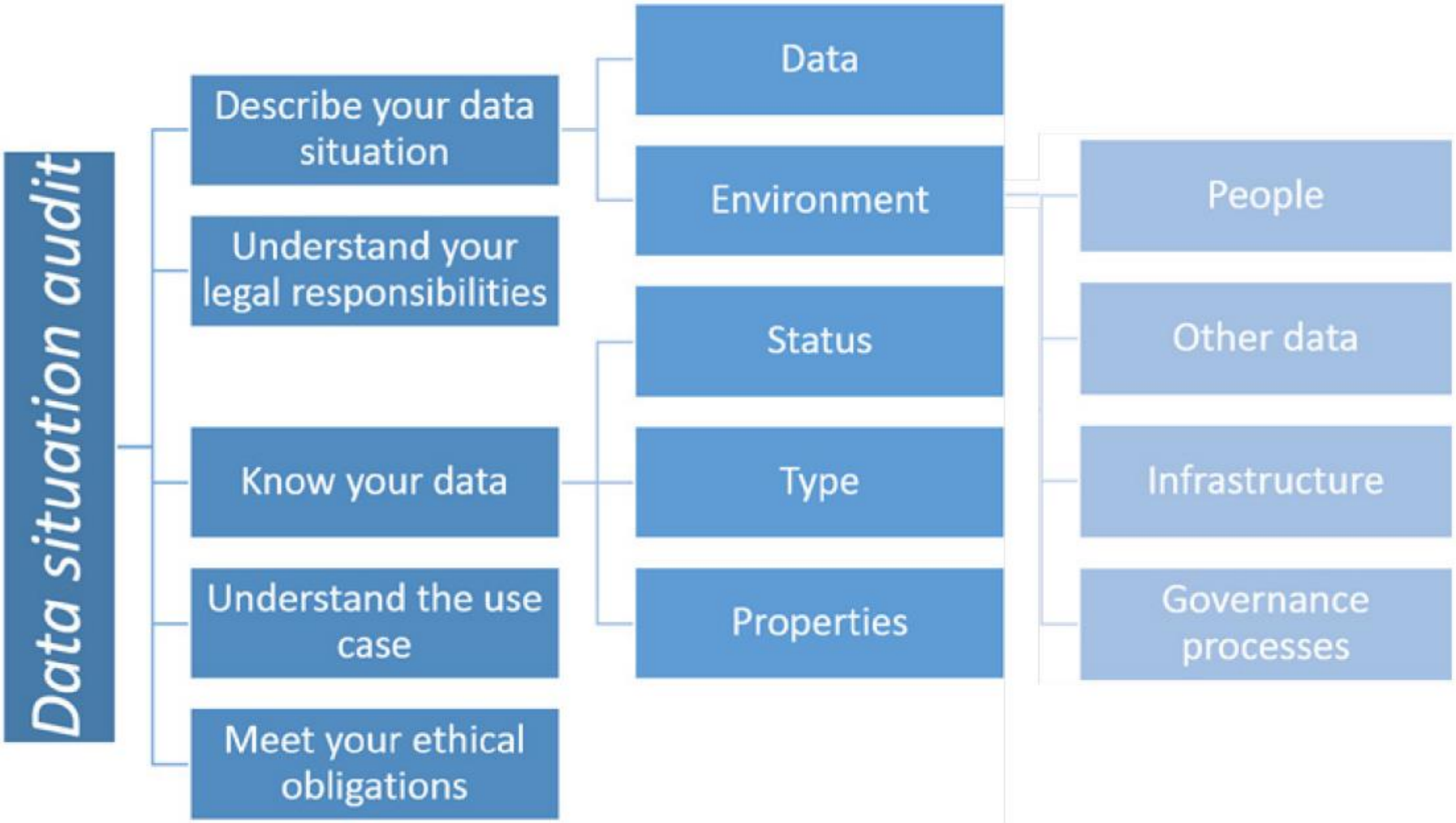
6. 豪州の事例

HITACHI
Inspire the Next

- ✓ 2017年9月にオーストラリア連邦政府の情報コミッショナーオフィスから匿名化の実用的なガイドとして”The De-Identification Decision-Making Framework”が発表された。
- ✓ これは匿名化のプロセスに対する独立したガイドであり、データ状況を評価し、その状況におけるリスクを管理するための適切な環境やデータを基礎としたコントロールを選択するための原則的な方法を提供する、
- ✓ このフレームワークは10のコンポーネント(実施項目)から構成されており、「データ状況の監査」、「リスク評価とコントロール」、「影響管理」の三つにグルーピングされている。
- ✓ フレームワークの5つの原則として以下が示されている。
  - データを単独で見ることで、データの共有/公開が安全かどうかを判断することは不可能。
  - しかし、データを見ることは依然として不可欠
  - 匿名化は安全なデータを生成するプロセスであるが、安全かつ有用なデータが作成された場合にのみ意味がある
  - 有用なデータを作成する上でゼロリスクは現実的には不可能
  - リスクを管理するための措置は、リスクとその影響に比例する必要がある
- ✓ プライバシー法に準拠するだけでなく、倫理的な検討を求めていることも特徴である。
- ✓ リスクを整理するために”Five Safes”というフレームワークが示されている。
  - Safe projects:データが適切に使われているか
  - Safe people:研究者は適切なマナーで利用することが信頼できるか
  - Safe data:データ自体の暴露リスクはないか
  - Safe settings::権限の無い利用を制限するアクセス制御があるか
  - Safe outputs:統計的は結果は非開示か
- ✓ 匿名化したデータの流通としては以下の4類型が示されている。
  - Open access:Web掲載等の一般公開
  - Delivered access:認めた相手に特定の環境での提供
  - On-site safe settings:認められた安全な環境でデータのアクセスを許可
  - Secure virtual access:セキュアなリンクによる認められたデータへのアクセス

6. 豪州の事例(2)

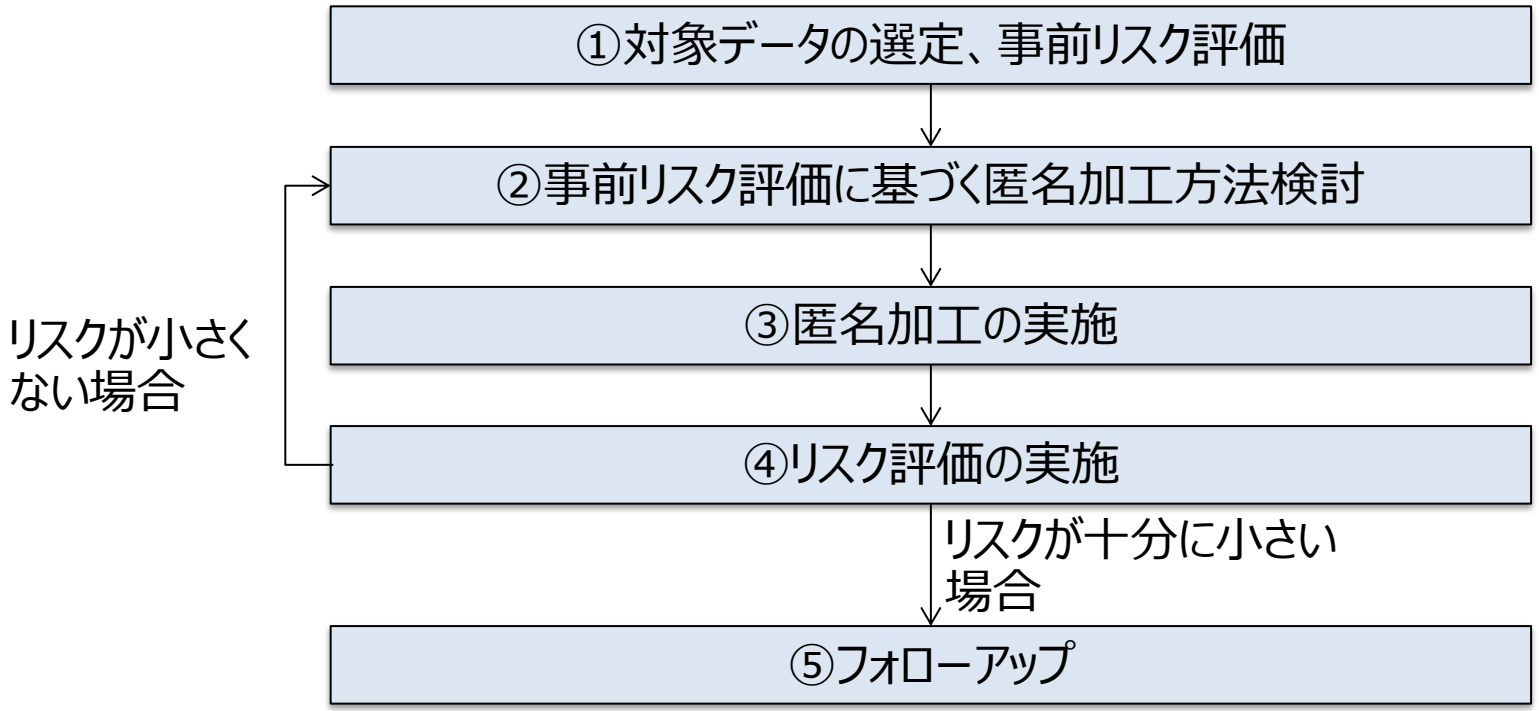
HITACHI
Inspire the Next



7. まとめ

HITACHI
Inspire the Next

- ✓リスクベースの考え方が一般的。
- ✓評価を法律で正当化する動きも。
- ✓フォローアップも重要。契約、再特定時対応、技術変化等。
- ✓名寄せを考慮した制度設計も重要。



HITACHI

Inspire the Next