資料１－５

技術WGによる検討作業の前提

日本ヒューレット・パッカード株式会社
佐藤　慶浩

2014年5月13日

技術WGによる検討作業の前提

「（仮称）準個人情報」に何が相当するかについて検討する作業範囲について、次のように想定する。

ただちには

万が一、識別特定された場合に

特定個人を　識別しないが、その取扱いによって　本人に権利利益侵害がもたらされる可能性があるもの

← 侵害リスクA

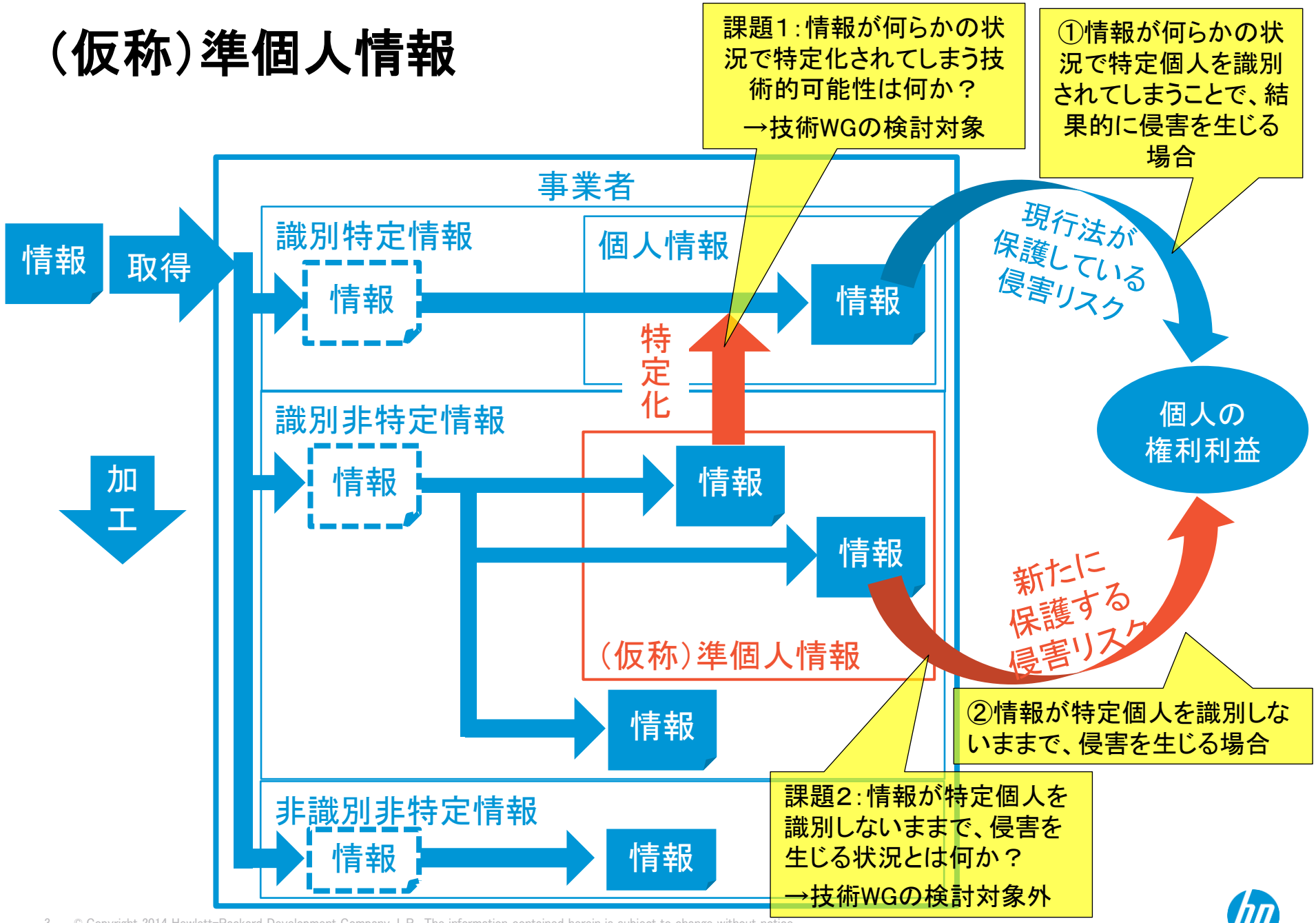
すなわち、以下は、技術WGによる今回の検討範囲外という理解。

識別特定されない状態のままで

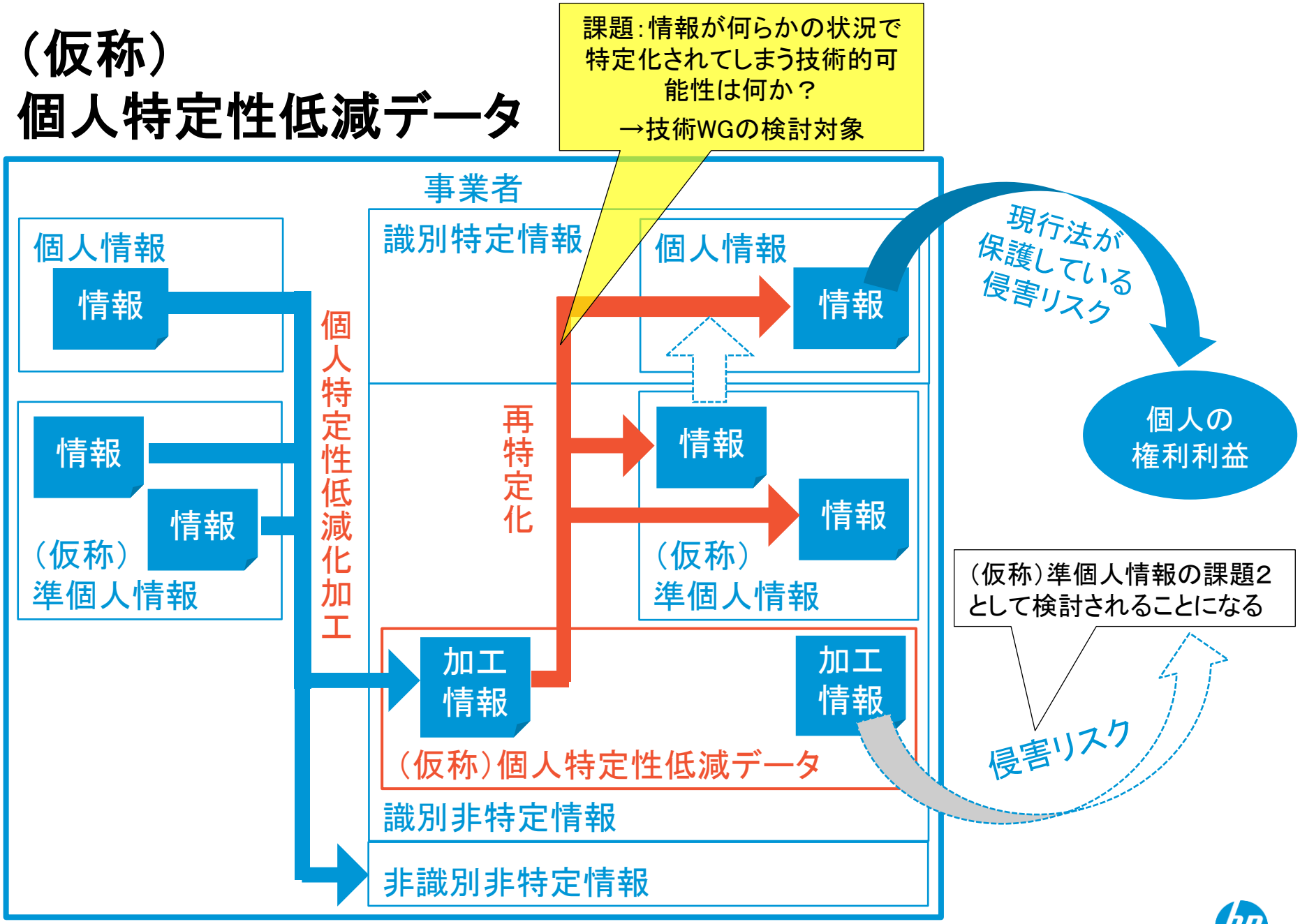
特定個人を　識別しないが、その取扱いによって　本人に権利利益侵害がもたらされる可能性があるもの

← 侵害リスクB

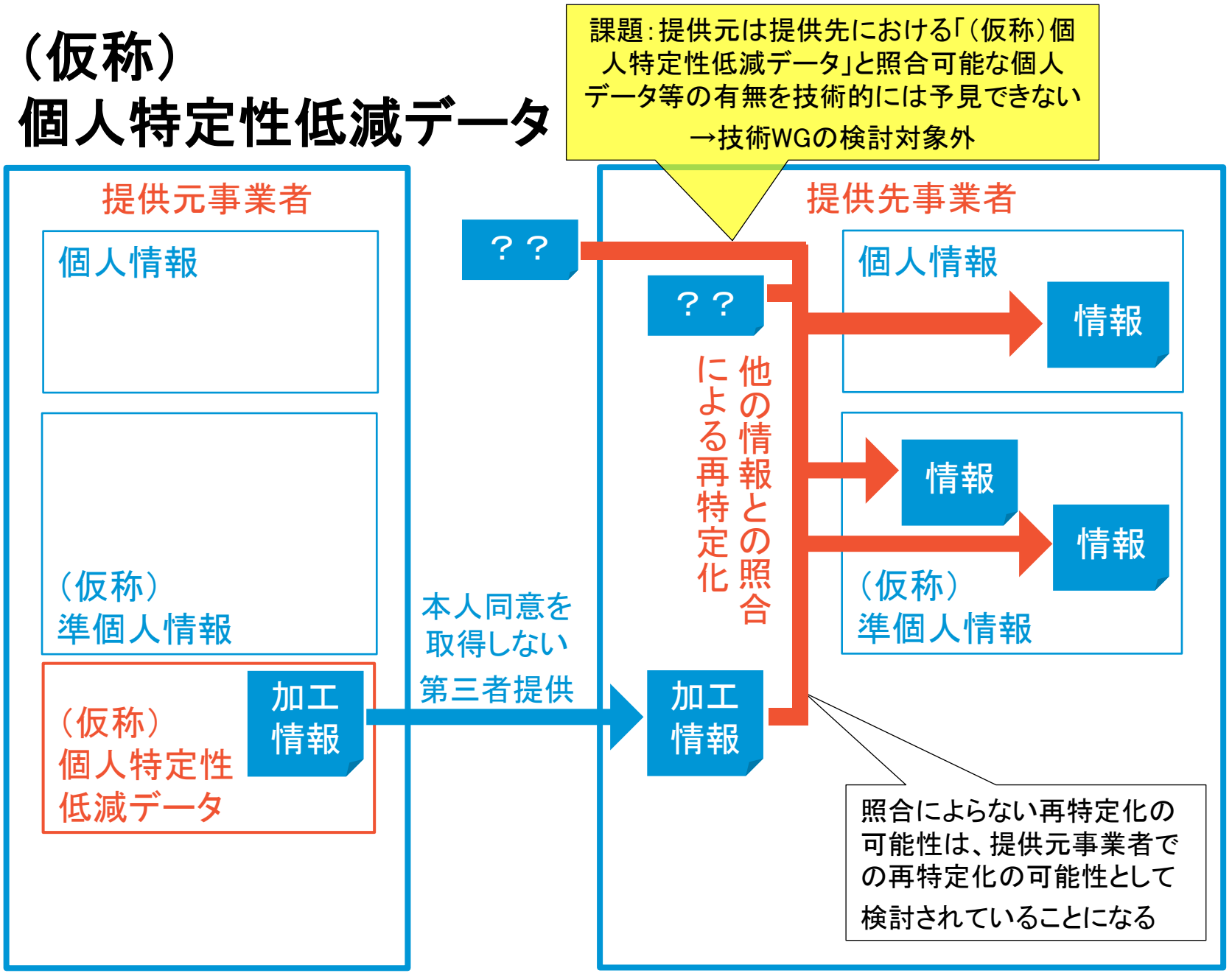
（仮称）準個人情報



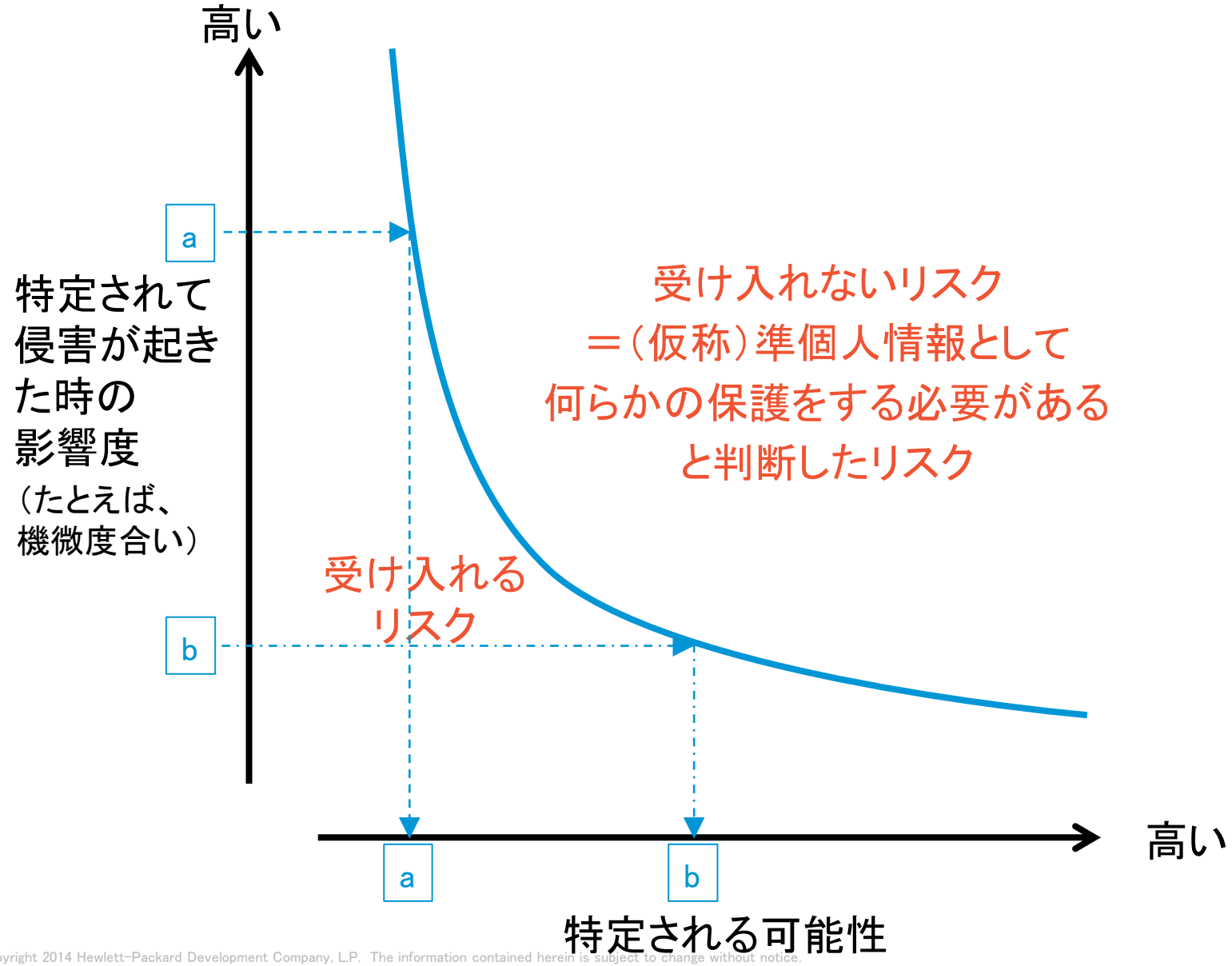
（仮称）
個人特定性低減データ



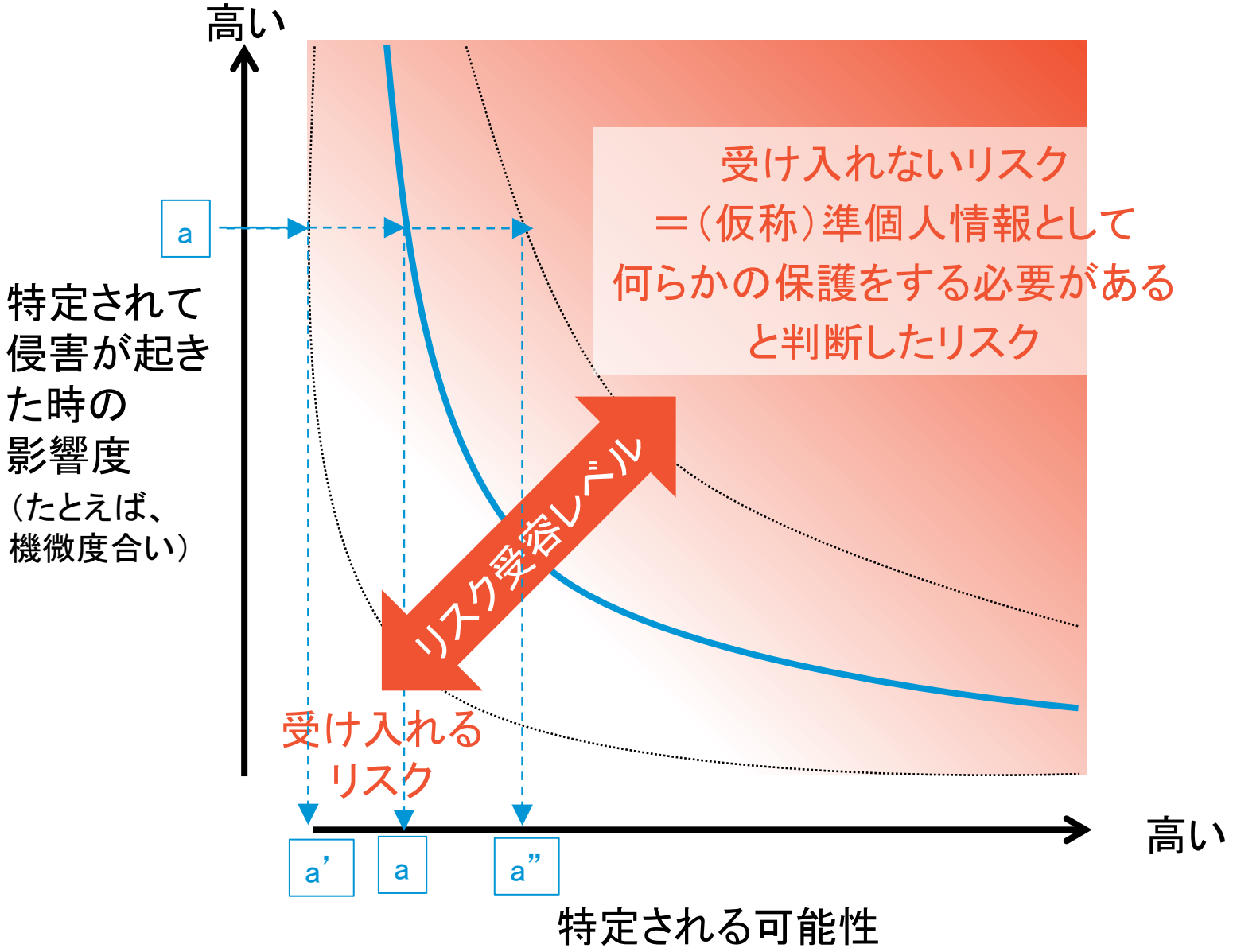
（仮称）
個人特定性低減データ



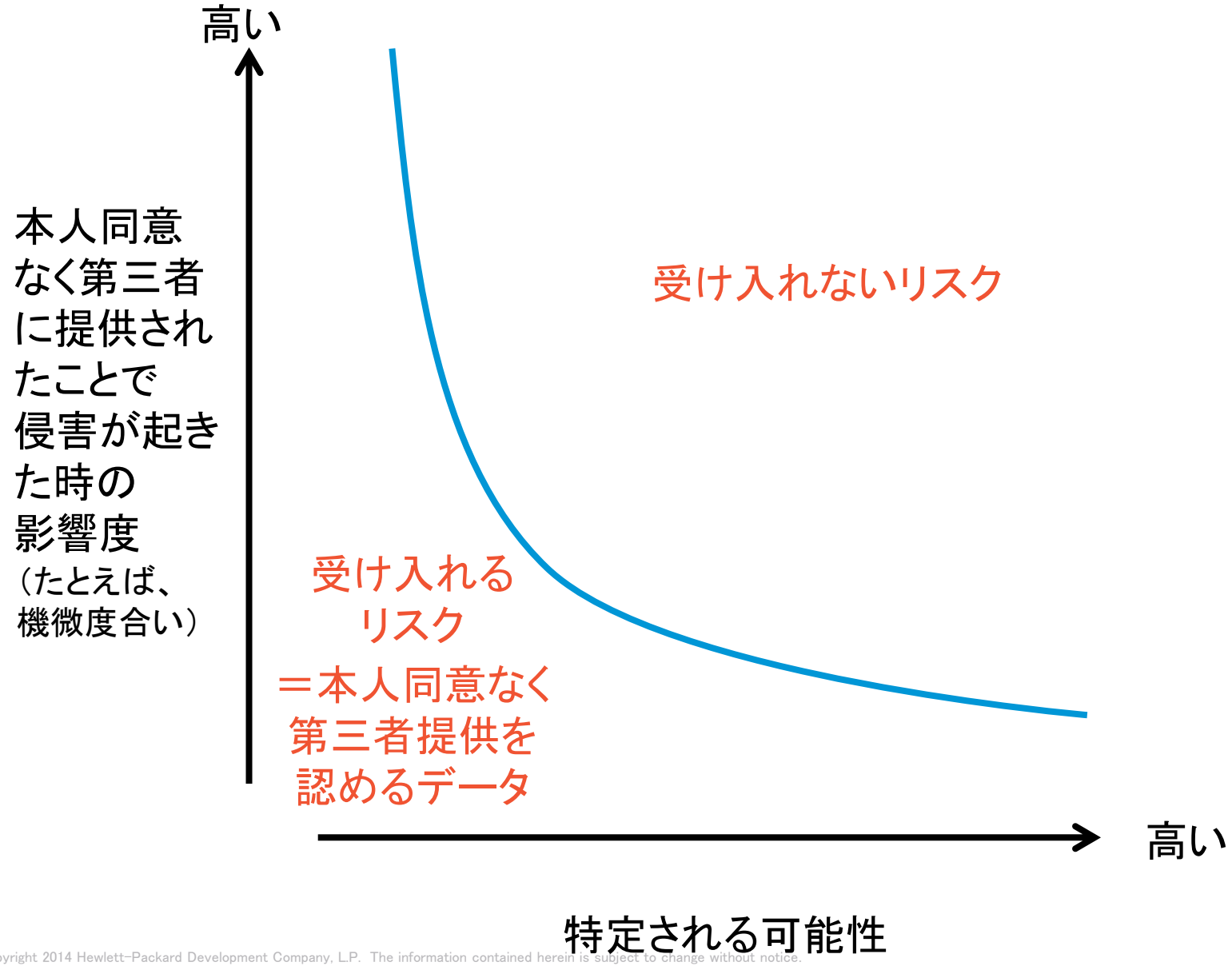
侵害の影響度と特定の可能性とリスクの関係



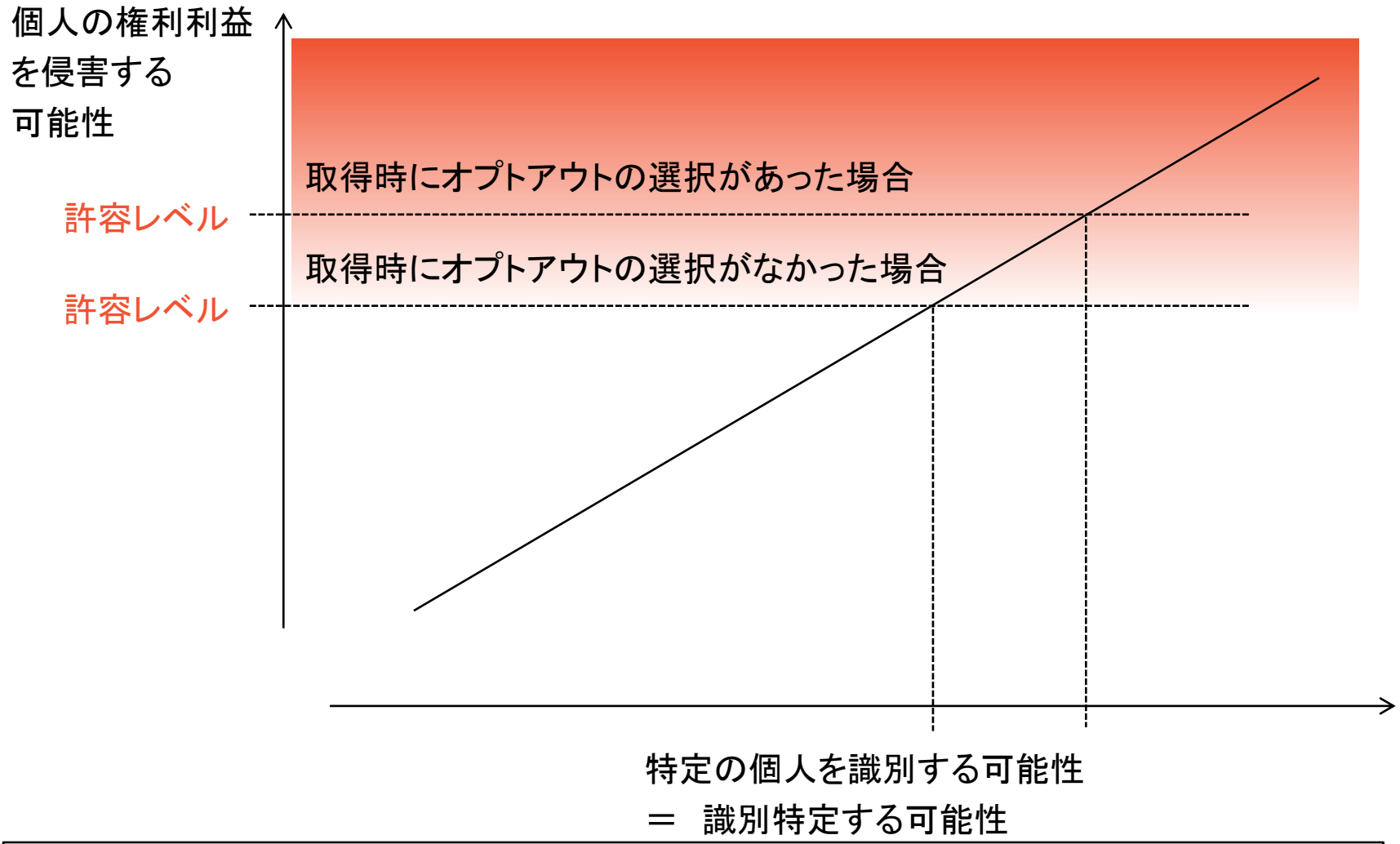
リスクを受けれるか否かと影響度・特定性の関係



侵害の影響度と特定の可能性とリスクの関係

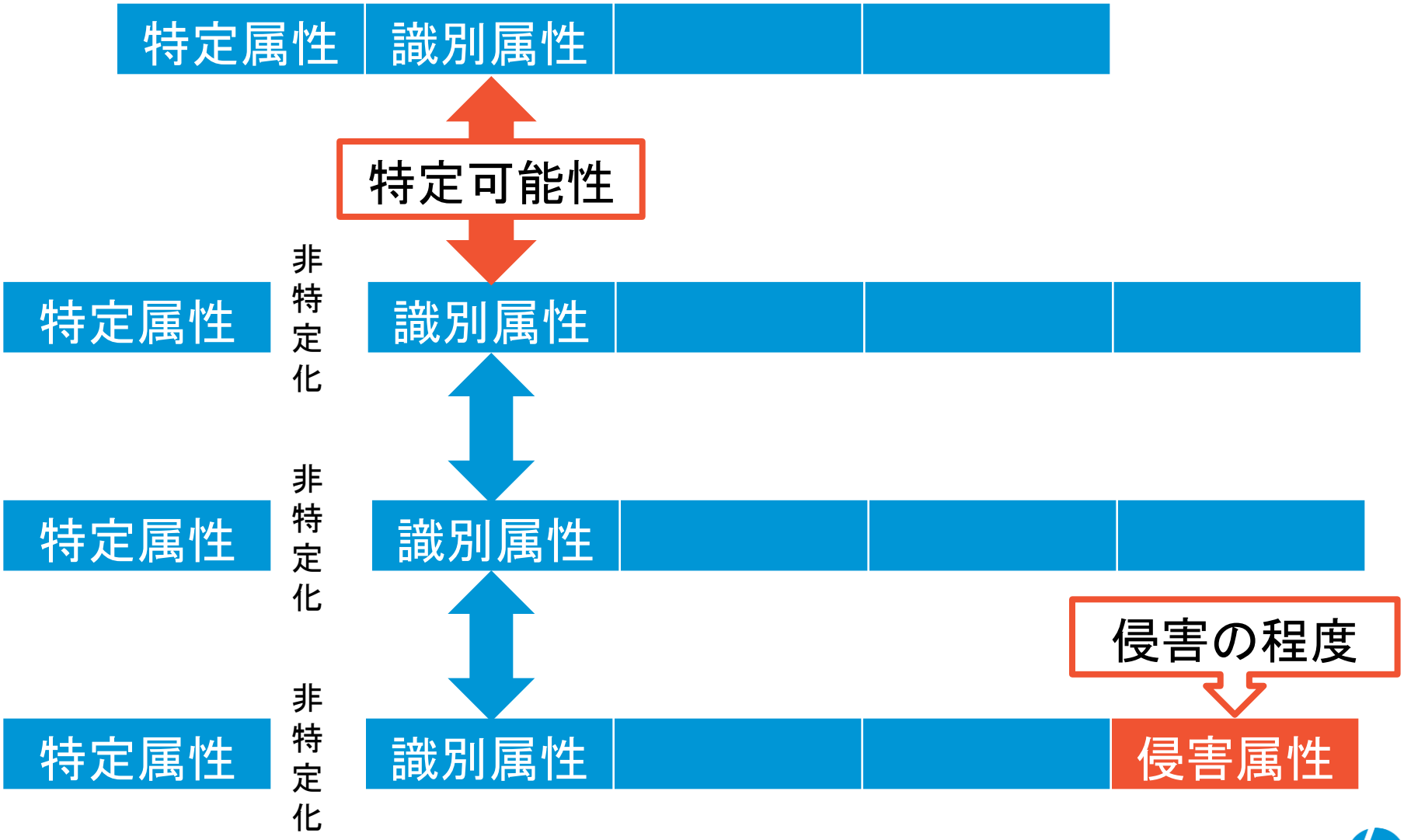


特定可能性と権利利益侵害可能性



特定と侵害の2者間の関係は上図のとおりだが、権利利益侵害の有無の判断においては、特定可能性は、侵害リスクAにおける必要条件であって、何（どの属性情報）が特定されたかにより侵害の程度が決まる。（上図の横軸を識別非特定性にすれば、侵害リスクBも同じ）

特定可能性と権利利益侵害可能性



特定~~可能性~~と権利利益侵害~~可能性~~

リスクマネジメント

リスク受容レベル　＜　一定値　において、

リスク受容レベル　＝　リスク発生時の影響度　×　リスク発生の確率

権利利益侵害リスクマネジメント

リスク受容レベル　＜　一定値　とするなら、

リスク受容レベル　＝　特定による影響度　×　特定の可能性

ただし、リスクマネジメント（JIS TR Q 0008:2003）では、

脅威：システム又は組織に危害を与える事故の潜在的原因

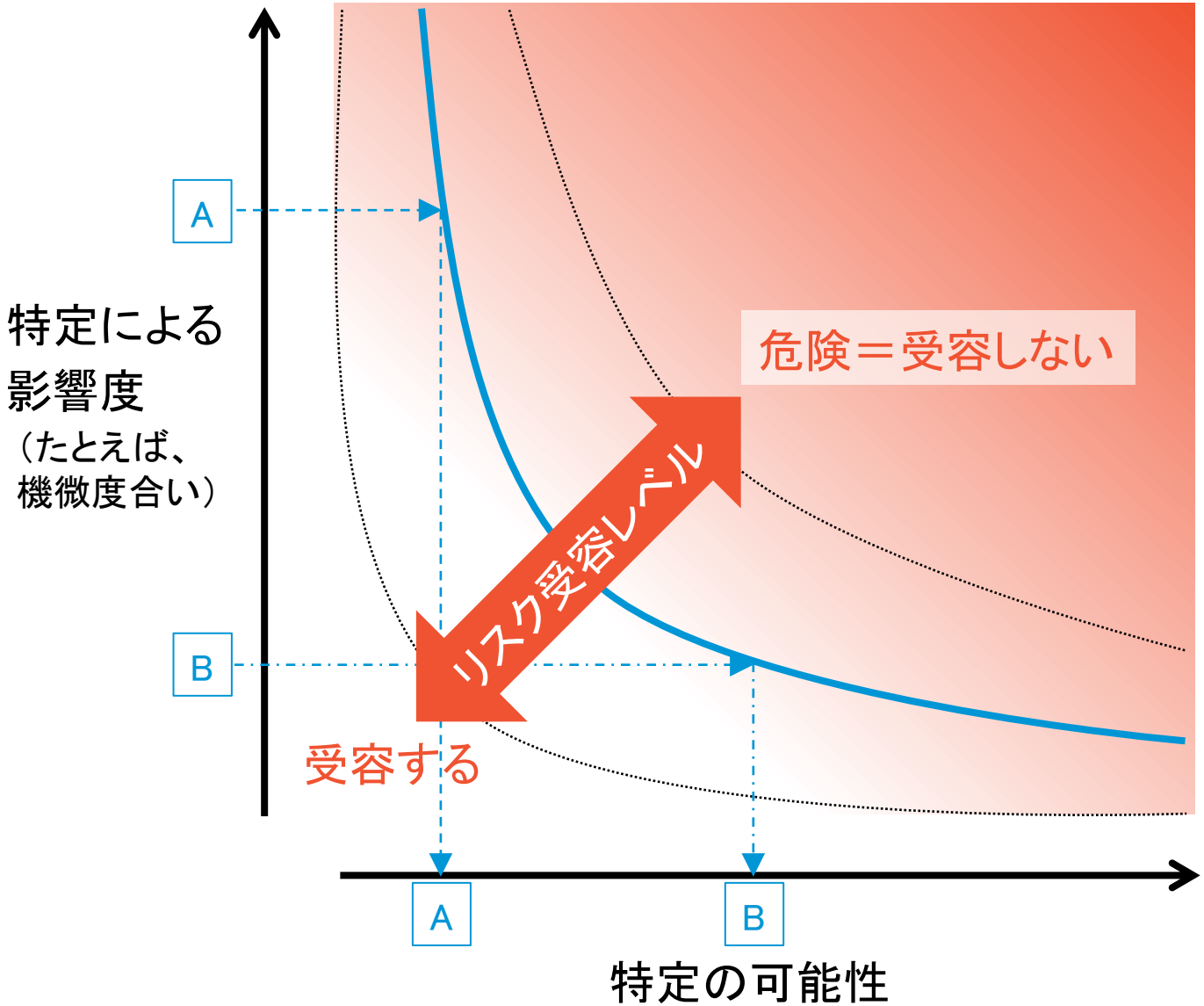
脆弱性：脅威によって影響を受ける内在する弱さ

リスク：ある脅威が脆弱性を利用して損害を与える可能性

リスク因子＝脆弱性　＋　脅威

と定義されており、脅威に対するリスク対策は脆弱性ごとに本来はとられる

特定~~可能性~~と権利利益侵害~~可能性~~



海外事例の概要

EU29条調査委員会（WP29）のAnonymisation Techniques意見書

AnonymisationとPseudonymisationについて方式を複数列記し、それぞれについての注意事項を書いてあるのみ。

結論は以下の言及のみ。

Good anonymisation practices

In general:

– Do not rely on the “release and forget” approach. Given the residual risk of identification, data controllers should:

1. Identify new risks and re-evaluate the residual risk(s) regularly,

2. Assess whether the controls for identified risks suffice and adjust accordingly; AND

3. Monitor and control the risks.

– As part of such residual risks, take into account the identification potential of the non-anonymised portion of a dataset (if any), especially when combined with the anonymised portion, plus of possible correlations between attributes (e.g. between geographical location and wealth level data).

海外事例の概要

ISO/TS 25237 Health information – Pseudonymization

ユースケースに沿っているため網羅性は高い。（公表や再識別化についても言及している。）
しかし、匿名化の加工方法についての具体的な記述はなく、管理体系の整理を主として記述している。

以下の（下線部）は技術WGと同意見である。また、利用目的に言及していることも興味深い。

5.1.4.3 The concept of pseudonymization

The practice and advancement of medicine require that elements of private medical records be released for teaching, research, quality control and other purposes. For both scientific and privacy reasons these record elements need to be modified to conceal the identities of the subjects.

There is no one single de-identification procedure that will meet the diverse needs of all the medical uses while providing identity concealment. Every record release process shall be subject to risk analysis to evaluate:

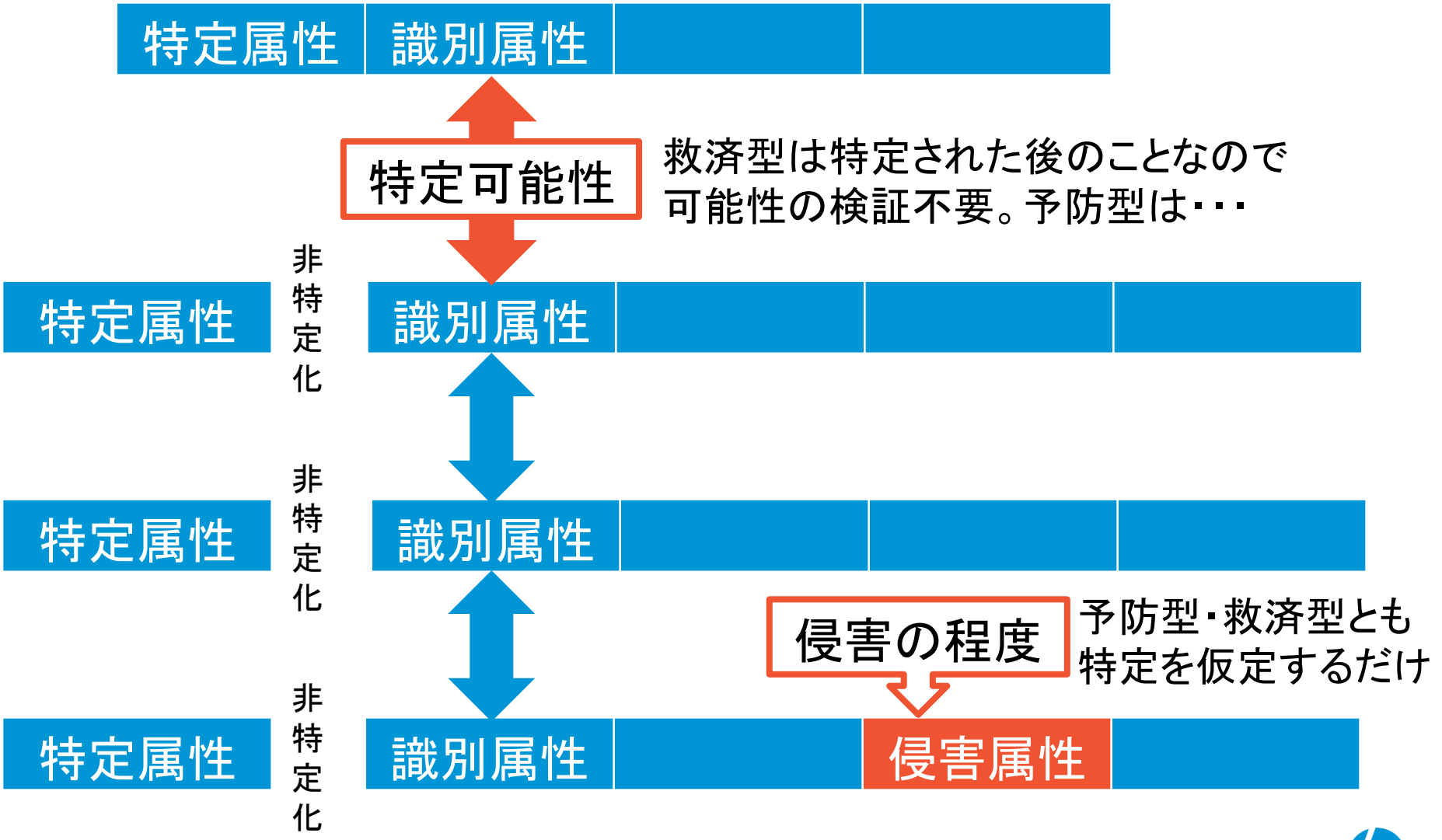
a) the purpose for the data release (e.g. analysis); →WP29意見書の2.2.1冒頭と同じ

b) the minimum information that shall be released to meet that purpose;

c) what the disclosure risks will be (including re-identification);

d) what release strategies are available.

特定可能性と権利利益侵害可能性



参考：第5回 パーソナルデータに関する検討会

今後の検討課題について（親会への依頼事項等）

資料2－2

✓ **新たな類型としての「（仮称）法第23条第1項適用除外情報」について**

- 制度的枠組みにより提供者及び受領者が個人情報及びプライバシーの保護を実現することが前提であるが、現時点では、制度的枠組みが不明確。
- 更なる制度的枠組みを踏まえ、類型の範囲やそのための技術的要件等についての具体的な議論が可能と思料。

✓ **立法措置を前提とした「合理的な技術的匿名化措置」について**

- 親会の依頼をもとに、いわゆる「ＦＴＣ3要件」を念頭にした検討の詳細化。
- 仮に「ＦＴＣ3要件」類似の制度を採用する場合には、提供者の約束や受領者の契約上の義務が実効的に実施される担保的な措置等の技術的な検討が必要。

✓ **ユースケースなどを想定した詳細検討**

- 取り扱う個人情報に含まれる属性情報の種類や利用の目的等を個別に判断することで、個別の事情に見合った合理的な匿名化の措置を行うことは不可能ではないが、詳細は議論できなかった。これは第三者提供される情報の種類や利用の目的等を明確ではなかったためである。今後、これらの情報が明確になった後に詳細な議論が必要であろう。