民間におけるPIAの取組（企業におけるプライバシー保護の勘所）

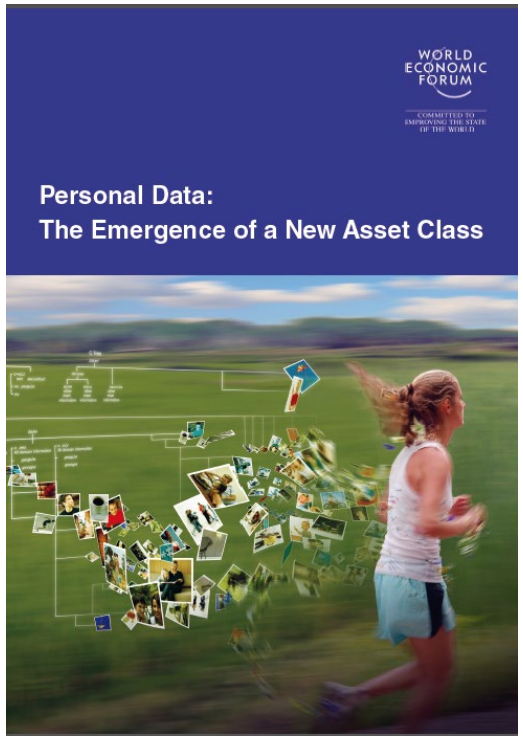
2021年2月25日

株式会社 日立コンサルティング

HITACHI
Inspire the Next

プライバシーガバナンスのためのPIA

プライバシーガバナンスの高まり



匿名加工情報

情報銀行

ニューノーマルへの移行

人の活動そのもののオンライン化デジタル化

個益と公益の両立の難しさ

プライバシーガバナンス

As some put it,
personal data will be the new “oil” – a valuable resource of the 21st century.

出典:World Economic Forum ”Personal Data：The Emergence of a New Asset Class”

プライバシーガバナンスの構成要素

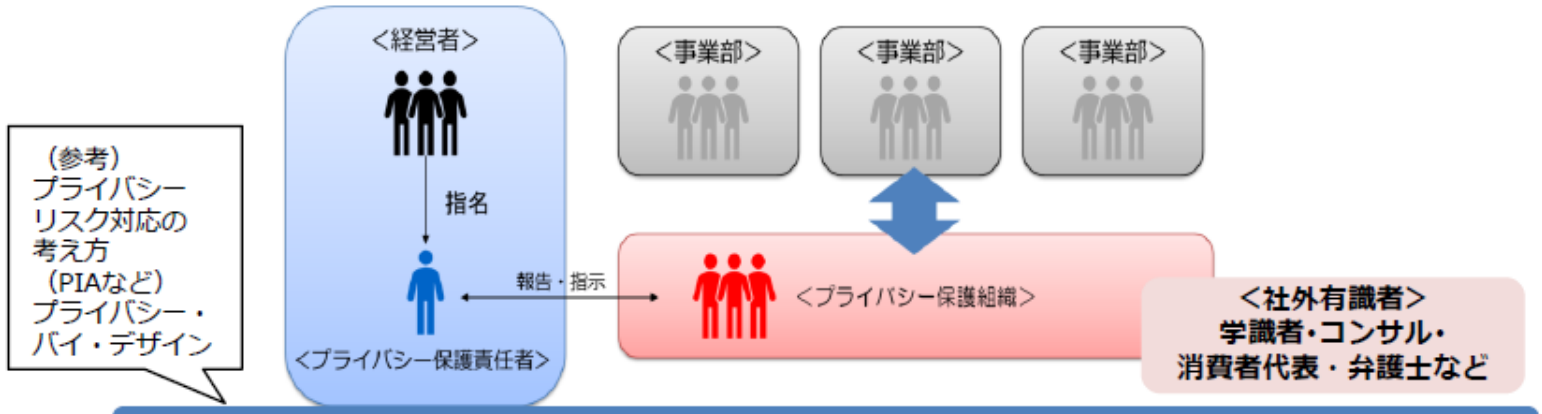
HITACHI
Inspire the Next

経営者が取り組むべき3要件

要件１：プライバシーガバナンスに係る姿勢の明文化
経営戦略上の重要課題として、プライバシーに係る基本的考え方や姿勢を明文化し、組織内外へ知らしめる。経営者には、明文化した内容に基づいた実施についてアカウンタビリティを確保することが求められる。

要件２：プライバシー保護責任者の指名
組織全体のプライバシー問題への対応の責任者を指名し、権限と責任の両方を与える。

要件３：プライバシーへの取組に対するリソースの投入
必要十分な経営資源（ヒト・モノ・カネ）を漸次投入し、体制の構築、人材の配置・育成・確保等を行う。



プライバシーガバナンスの重要項目

1. **体制の構築**（内部統制、プライバシー保護組織の設置、社外有識者との連携）
2. **運用ルールの策定と周知**（運用を徹底するためのルールを策定、組織内への周知）
3. **企業内のプライバシーに係る文化の醸成**（個々の従業員がプライバシー意識を持つよう企業文化を醸成）
4. **消費者とのコミュニケーション**（組織の取組について普及・広報、消費者と継続的にコミュニケーション）
5. **その他のステークホルダーとのコミュニケーション**
（ビジネスパートナー、グループ企業等、投資家・株主、行政機関、業界団体、従業員等とのコミュニケーション）

業務プロセスとしての実践

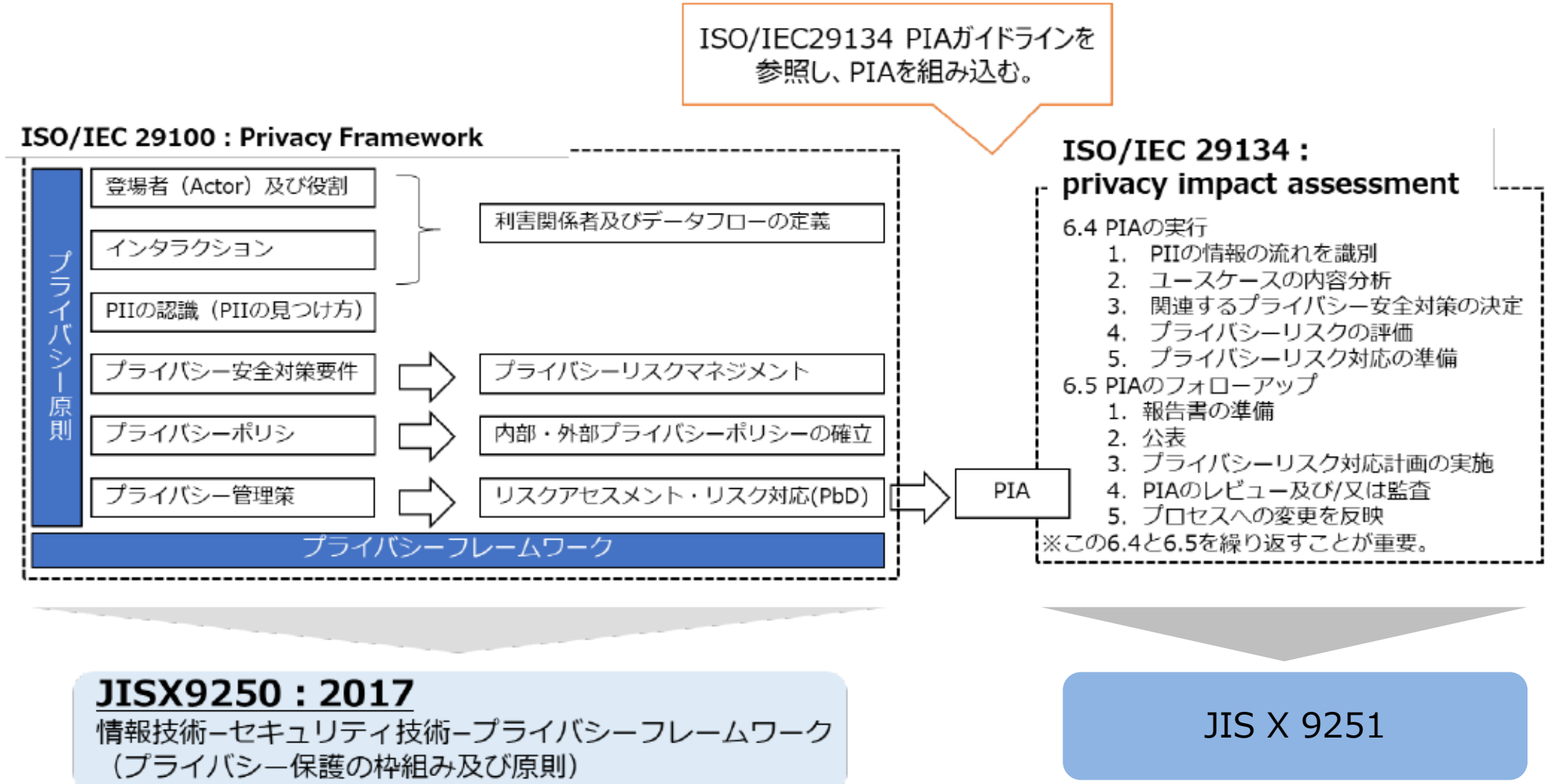
Privacy by Design

PbDの実践手法

Privacy Impact Assessment

出典：総務省、経済産業省「DX企業のプライバシーガバナンスガイドブック」

PIAの国際標準



出典：総務省、経済産業省「DX企業のプライバシーガバナンスガイドブック」

日立におけるプライバシー保護の事例

プライバシー保護　－背景－

HITACHI
Inspire the Next

■ パーソナルデータを利活用する新たな事業機会

✓技術革新(ビッグデータ、IoT、AI、ドローン、ロボティクス・・・)

✓データ量増加、データ多様化、データ分析技術の高度化・・・

×

■ パーソナルデータの利活用における新たな事業リスク

✓国内外の関連法制度に抵触し、法執行を受けるおそれ

✓個人からの反発、ブランド毀損、信頼性の低下

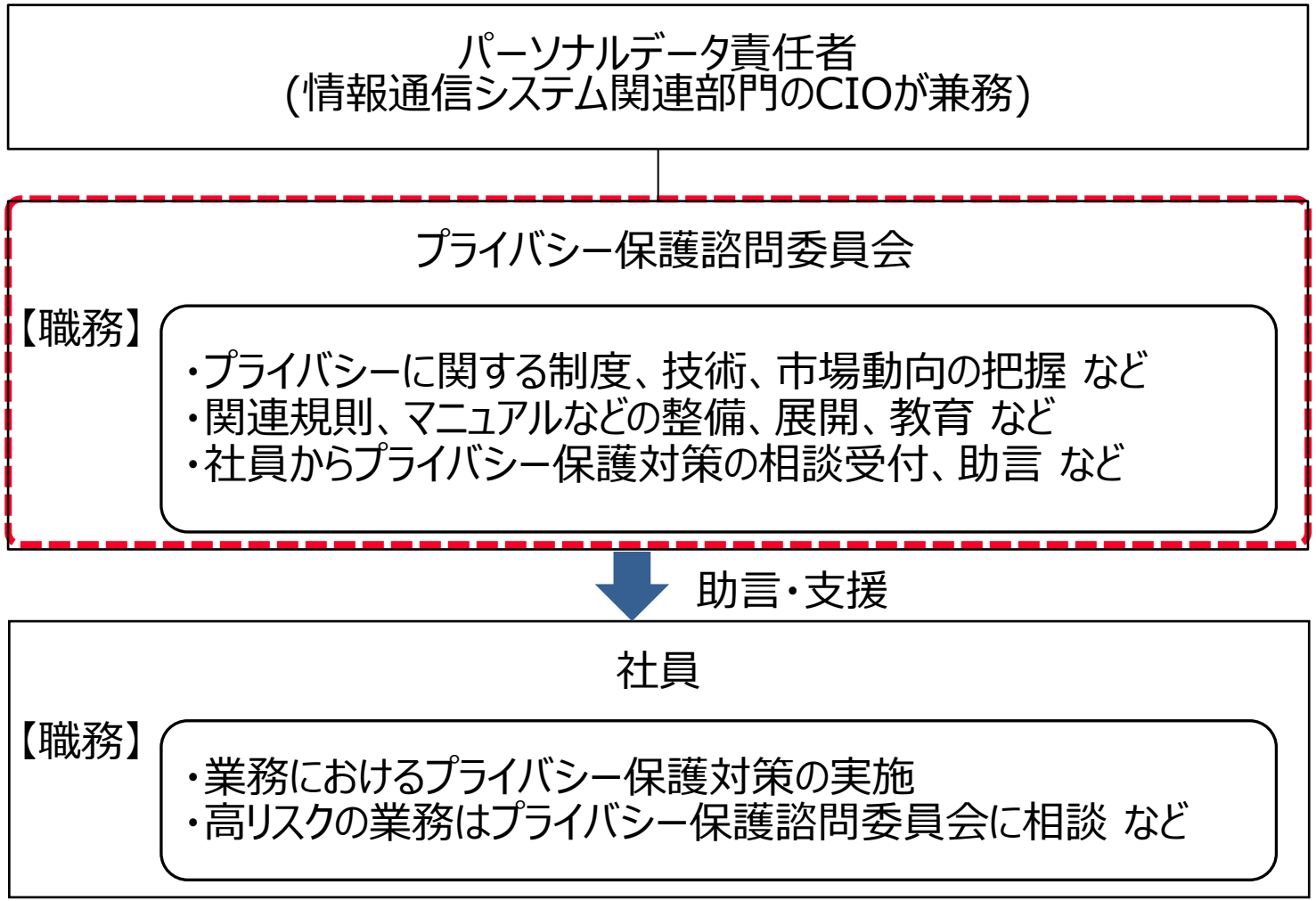
✓協創パートナーからの信頼性低下

パーソナルデータを利活用するビジネスを推進するためには、
個人の懸念を払拭し、プライバシーに関わるリスクを最小化する取り組みが必要

出典：　日立セキュリティフォーラム2019「パーソナルデータの利活用における日立のプライバシー保護の取り組み」

プライバシー保護　－体制－

プライバシー保護の中核となる専門組織としてプライバシー保護諮問委員会を設置

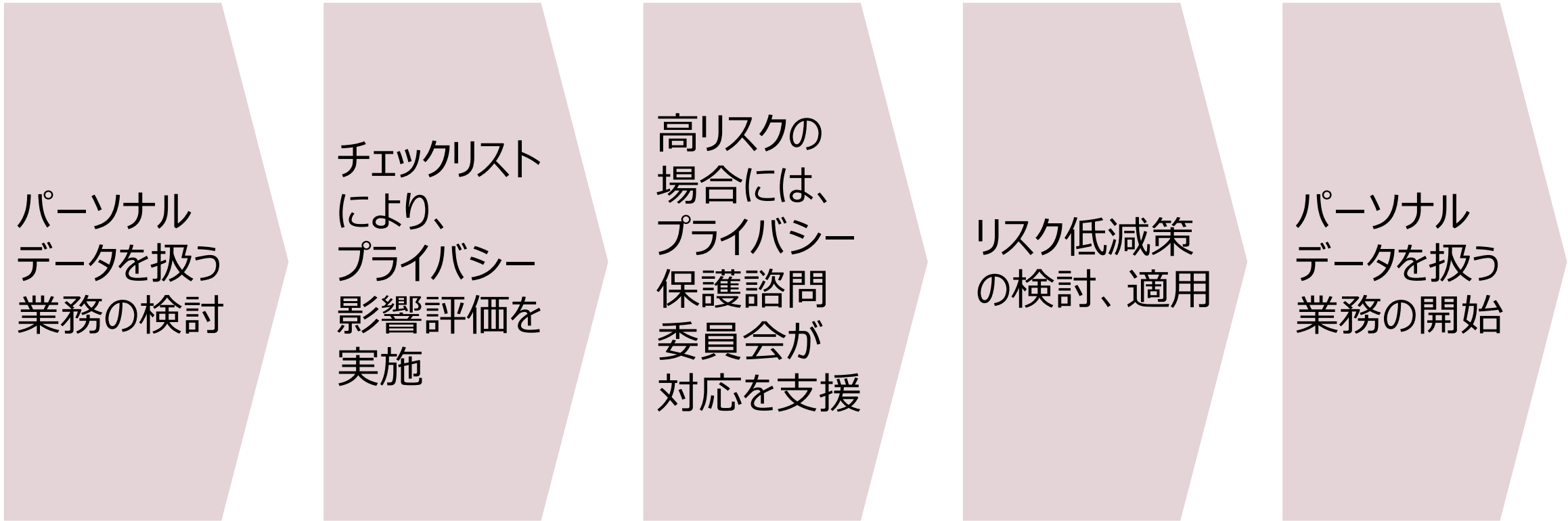


ＣＩＯ：Ｃｈｉｅｆ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｏｆｆｉｃｅｒ

出典：　日立セキュリティフォーラム2019「パーソナルデータの利活用における日立のプライバシー保護の取り組み」

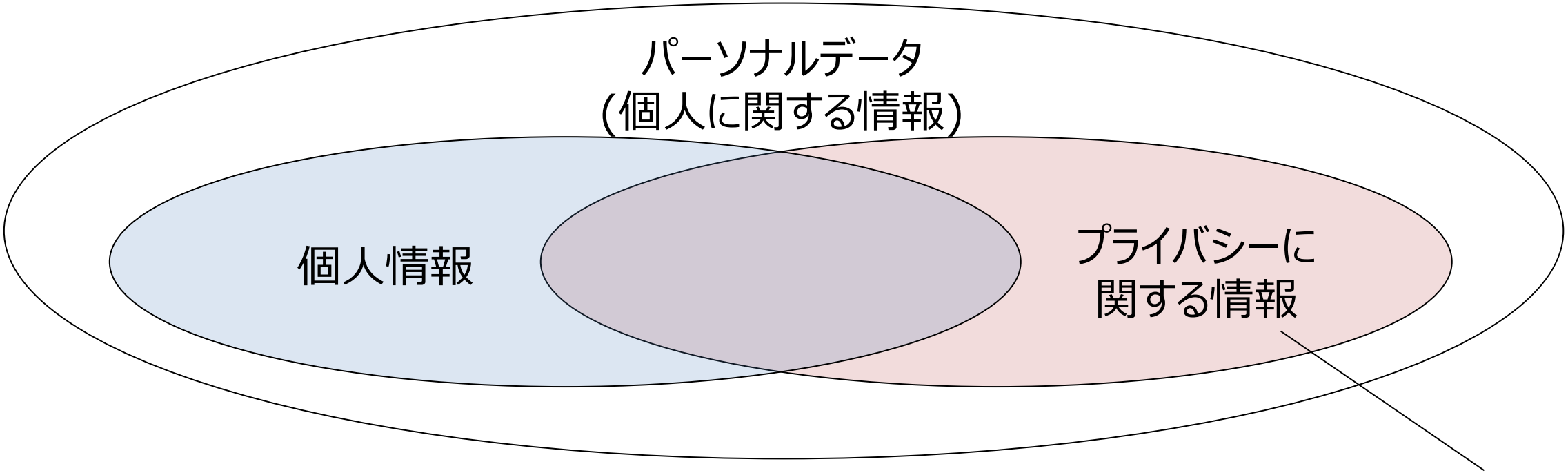
プライバシー保護　－PIA－

パーソナルデータを取り扱うにあたっては、プライバシーへの影響を
事前に評価したうえで、プライバシー保護対策を実施



出典：　日立セキュリティフォーラム2019「パーソナルデータの利活用における日立のプライバシー保護の取り組み」

プライバシー保護　－PIAの対象－



例えば、位置情報、
購買履歴、検索履歴、
バイタルデータ・・・

- 伝統的なプライバシー権を侵害しうる情報
- その取得・利活用・蓄積が個人に不安、違和感などを与えるおそれのある情報

※本取り組みにおける独自定義

出典：　日立セキュリティフォーラム2019「パーソナルデータの利活用における日立のプライバシー保護の取り組み」

ある企業におけるPIAの試行

PIA試行の背景

- 2020年6月5日に個人情報保護法の改正が成立した。
- 法律自体には書き込まれていないが、法改正の考え方を取りまとめた制度改正大綱には以下の記述がある。

> ２．民間の自主的取組の推進
>
> （１）基本的考え方
>
> ○ 個人情報保護法は、認定個人情報保護団体制度を含め、民間事業者の自主的な対応を尊重する制度設計が織り込まれてきている。
>
> ○ 特に、デジタル技術を活用した新たな利用分野では個人情報保護に関する問題が発生しやすいが、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ことが多いことから、法の規定を補完する形で、民間主導で自主ルールが策定、運用されることは望ましく、これらの取組を更に促進していく必要がある。
>
> ○ 具体的には、PIA（Privacy Impact Assessment、個人情報保護評価）の取組、個人データの取扱いに関する責任者の設置、企業の自主的な取組を推奨する仕組みなどについて、その取組を促進していくことが考えられる。

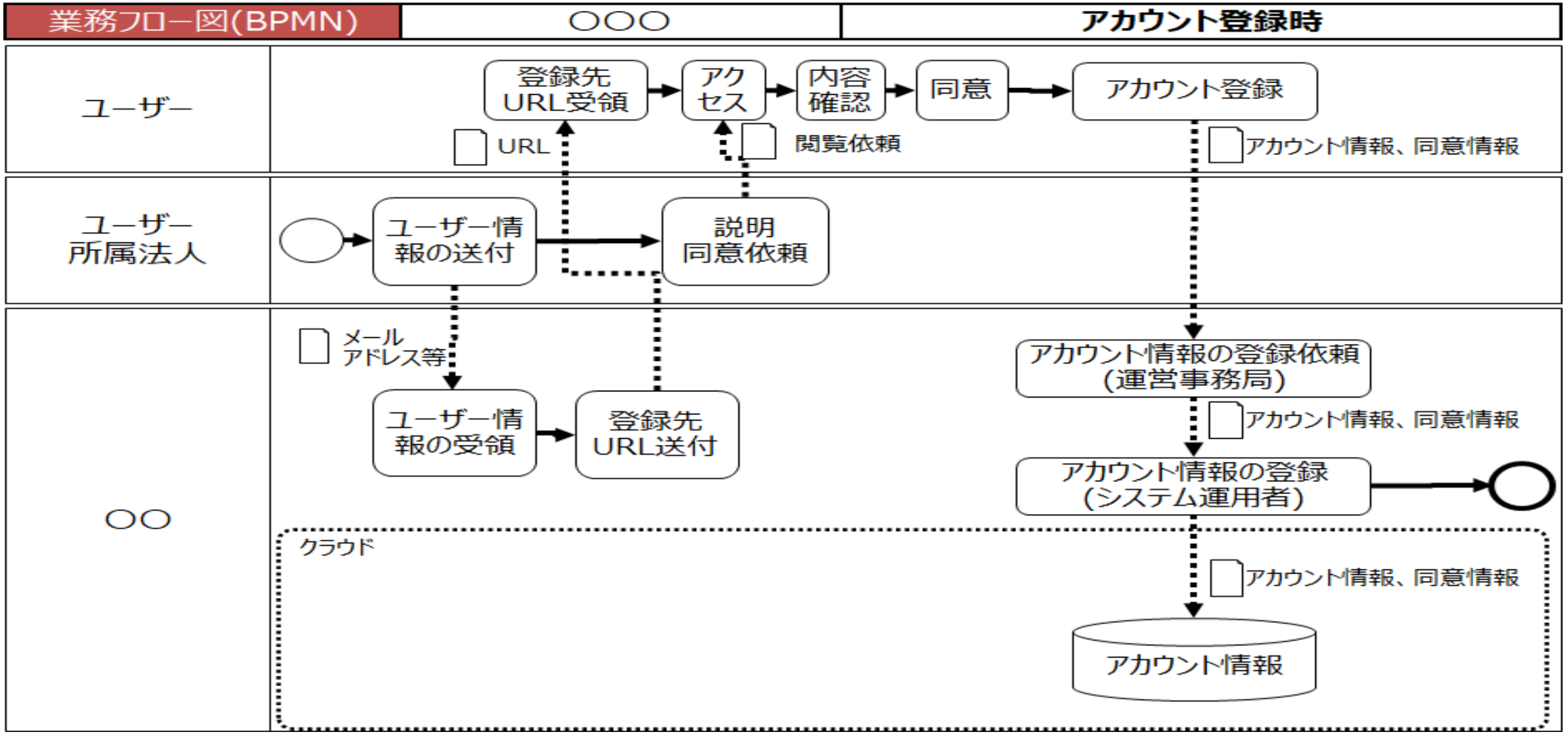
- 個人情報保護委員会では、PIAについて民間の自主的な取組を尊重することとし、PIAの事例集の作成や表彰制度の創設等を検討していく、としている。
- 経済産業省、総務省「DX時代における企業のプライバシーガバナンスガイドブックver1.0」が示され、企業価値向上のためにプライバシー保護の取組が求められている。
- 2021年1月20日には、国際的なPIAの標準規格であるISO/IEC29134をJIS化した「JIS X 9251:2021」が発行された。

PIA試行の実施手順

	作業項目
実施方針の検討	評価対象とする事業の選定
	PIAの実施手法の精査
PIAの対象となる事業の整理	PIAの対象範囲の設定
	対象とする事業に係るビジネスプロセス、情報システム、組織等の整理（取り扱われるパーソナルデータを特定した上で整理）
	評価対象となるビジネスプロセス、情報システム等の詳細化（PIIの収集方法、処理方法、処理目的、利用方法、管理・変更方法、廃棄方法、責任者等）
	ユーザーのユースケースの設定
プライバシーリスクの分析、整理	コンプライアンス要件等の整理
	プライバシーリスクの特定
	プライバシーリスクの分析、評価
	プライバシーリスク対策の検討
	プライバシーリスク管理策の検討
PIA報告書等のとりまとめ	プライバシーリスク対応計画の作成
	PIA報告書の作成

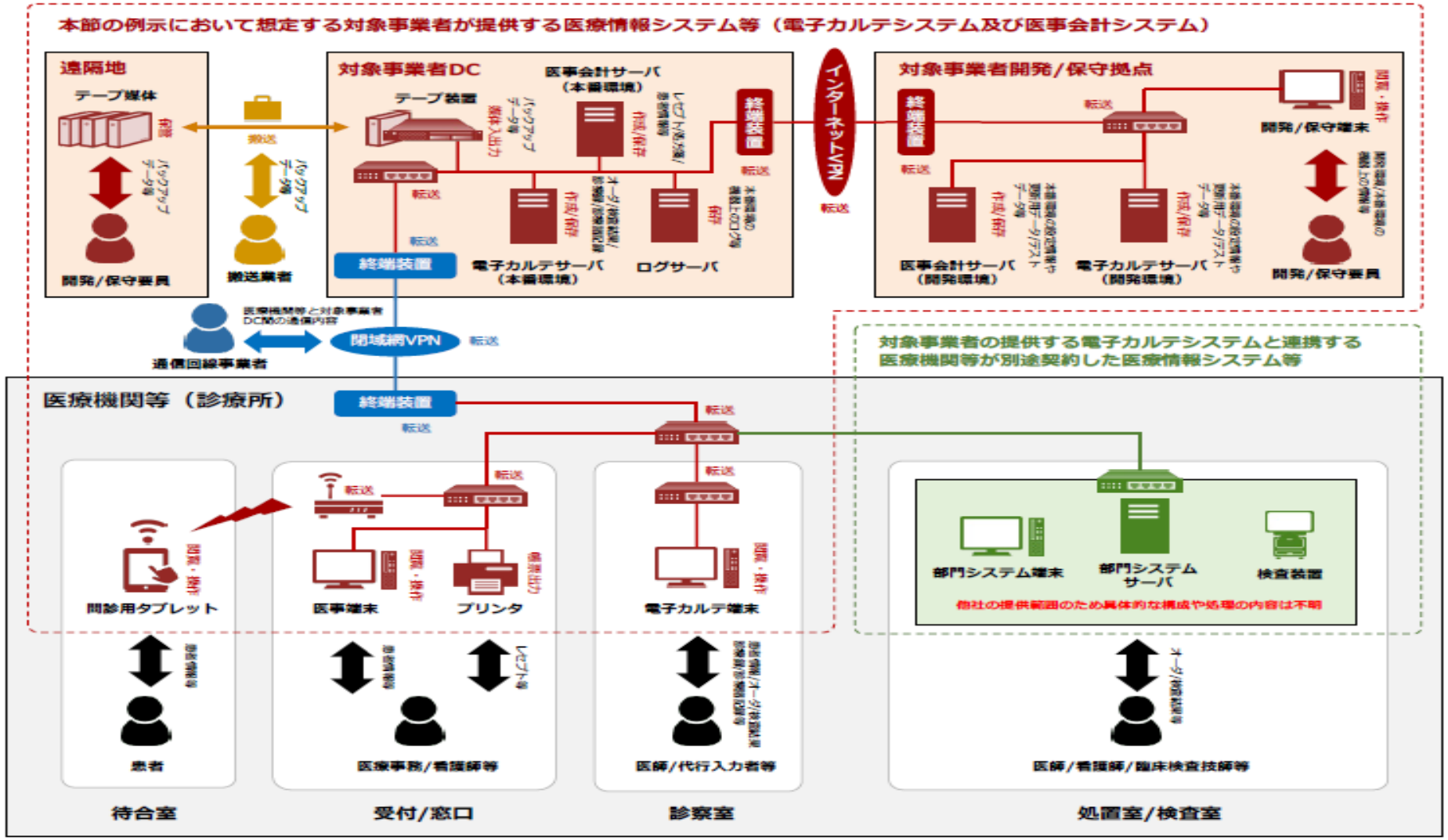
評価対象事業の整理

- BPMN等を使ってプロセスを可視化。



評価対象事業の整理

- ユーザーのデバイス、クラウド等も含めて情報システムの構成等を整理。

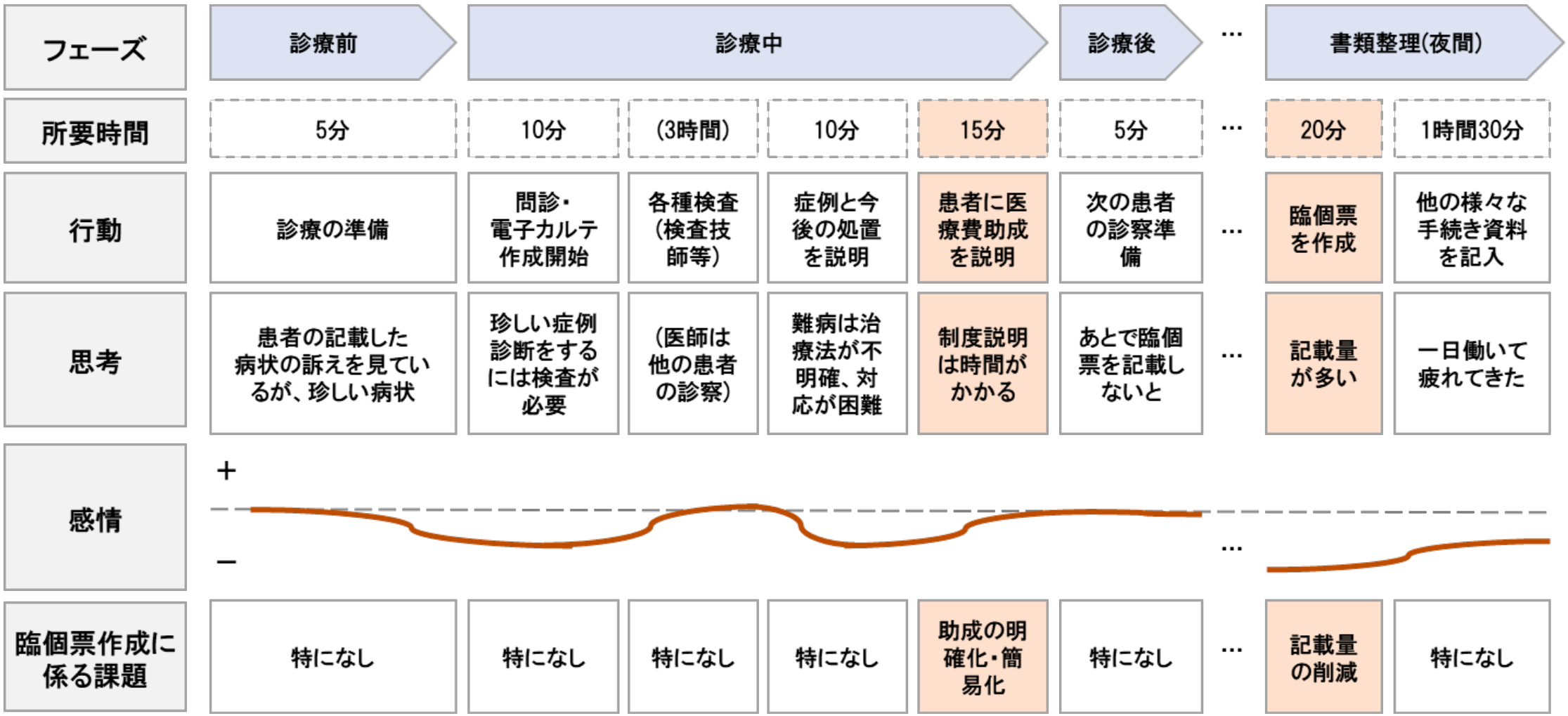


出典：経済産業省、総務省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」

評価対象事業の整理

HITACHI
Inspire the Next

- ジャーニーマップ等の手法で個人目線でユースケースを整理。



コンプライアンス要件等の整理

HITACHI
Inspire the Next

- コンプライアンス要件等を整理する。

名称	発行年月日	発行機関
個人情報の保護に関する法律	2003年5月	ー
ISO/IEC 29134：2017(Information technology - Security techniques - Guidelines for privacy impact assessment)	2017年6月	ISO/IEC
JIS X 9250：2017(Information technology-Security techniques-Privacy framework)	2017年6月	一般財団法人日本規格協会
位置情報プライバシーレポート～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～	2014年7月	総務省
スマートフォン プライバシー イニシアティブⅢ	2017年7月	総務省
人事データ利活用の原則	2020年3月	一般社団法人ピープルアナリティクス&HRテクノロジー協会

プライバシーリスクの特定

HITACHI
Inspire the Next

- コンプライアンス要件以外のプライバシーのチェック項目を踏まえ、プライバシーリスクをチェックする。

プロセス	確認項目
収集	• 個人情報を収集する対象、取得方法、取得する内容、取得する目的 • 本人から収集する際の通知や同意の方法 • 収集する主体がどのようになっているか（個社か共同利用か等）
保管・管理	• 委託先等も含めて個人情報の安全管理 • 個人に対する適切な情報の開示 • 個人からの請求等への対応 • 個人情報に関する記録 • 正確性が担保とID管理
利用	• 個人情報を利用する目的や利用主体 • 加工や分析の内容、方法 • 個人に対してフィードバックする仕組みの有無 • 加工された情報が二次利用される可能性 • 他のデータと結合したり、新たなデータが生成される可能性
移転	• 提供先の第三者の利用範囲や管理 • 加工した個人情報の第三者提供の有無 • 移転先で他の個人情報と結合される、あるいは個人情報に戻る可能性
削除	• 保存期間の設定 • 適切に廃棄・削除

プライバシーリスクの特定

HITACHI
Inspire the Next

- チェックリスト及びコンプライアンス要件等から特定した、情報システム又はビジネスプロセスから生じるプライバシーリスクを整理する。

特定したプライバシーリスク(1/2)

#	チェック項目	特定したプライバシーリスク
1		
2		
3		
4	個人情報を取得する方法が適切でかつ安全か	ユーザーの個人情報を電子メールで取得するため、暗号のかけ忘れ等により、電子メールに含まれるユーザー情報がネットワーク上で漏洩する可能性がある。
5		
6		
7		

プライバシーリスクの特定

HITACHI
Inspire the Next

特定したプライバシーリスク(2/2)

#	チェック項目	特定したプライバシーリスク
8		
9		
10		

#	コンプライアンス要件等	特定したプライバシーリスク
11	利用制限の原則	警察等の国家機関からプロファイリング結果を求められた場合の対応方法を想定しておらず、プライバシーポリシーに除外規定を記述していない
12	アカウンタビリティの原則	
13	苦情相談への対応体制の確保	
14	利用者に対する説明表示	

プライバシーリスクの分析、評価

HITACHI
Inspire the Next

- 適切な対応策、管理策を特定するため、特定したプライバシーリスクのそれぞれの影響の大きさ及び起こりやすさのレベルを推定した。
- また、プライバシーリスクの定量的な評価は技術的に困難であるため、数段階の定性的な評価基準を策定した。

【影響の大きさ】

特定されたプライバシーリスクの影響の大きさは、ユーザーや企業への影響を考慮に入れて推定する。

#	項目	説明
4	甚大	ユーザーに対して精神的あるいは経済的に著しい損失を与える可能性があり、その結果、企業の信用失墜や相当の経済的な損失につながる可能性がある。(心理的または身体的疾患、口座番号・暗証番号の流出 等)
3	重大	ユーザーが一定の不利益を被るものの、甚大ではなく、回復可能であり、企業の信用等に対する影響も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	一部のユーザーにおいて不安感等を創出し、企業におけるリスクは存在するものの、その範囲は限定的である。(サービスへのアクセス拒否、データ利用に関する説明不足 等)
1	無視できる	ユーザーの不利益の可能性はあるものの極めて小さく、企業への影響も無視できるレベルである。(長時間のメンテナンス、煩わしさ 等)

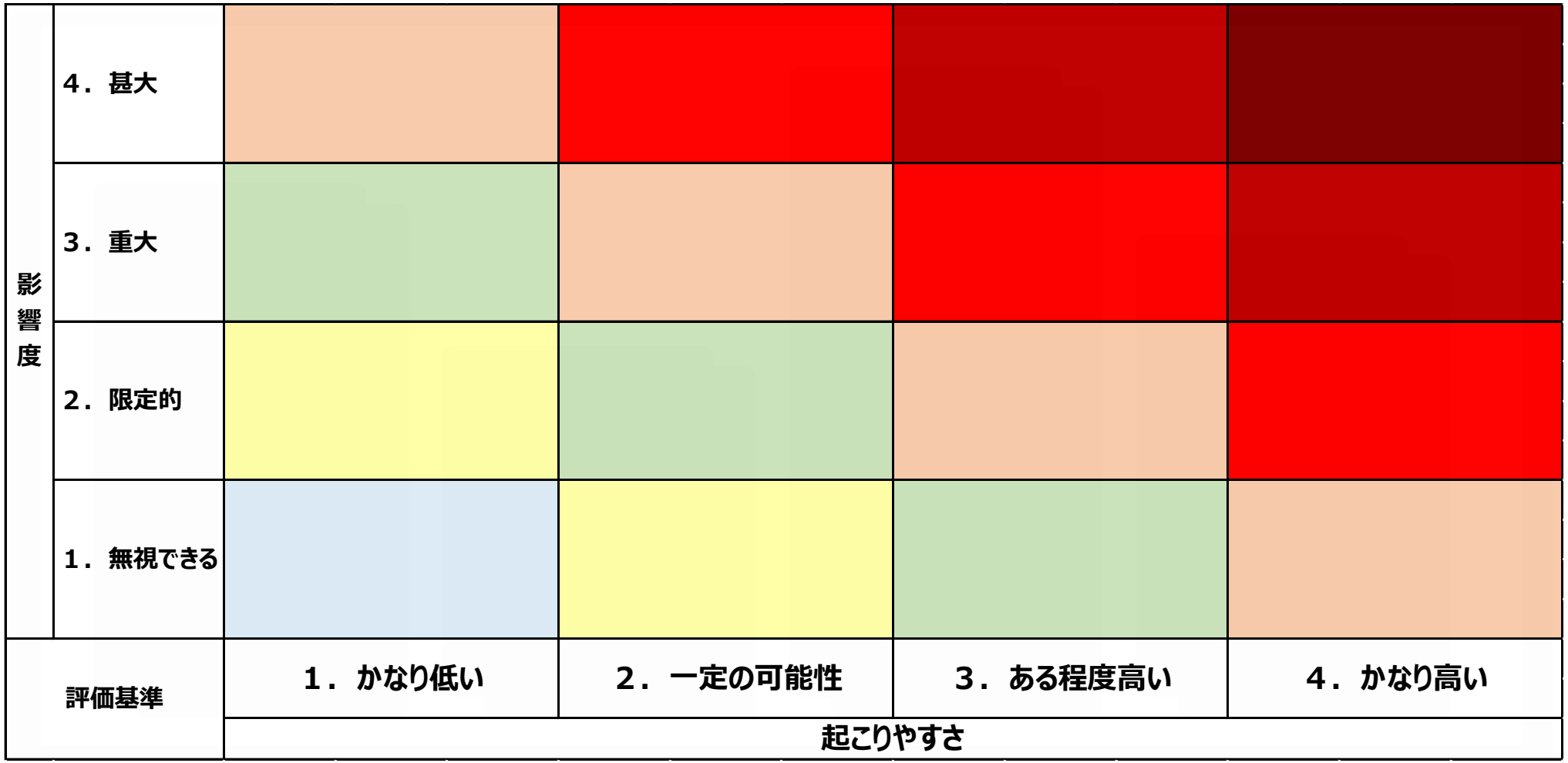
【起こりやすさ】

モチベーション、実施の容易さ等、リスクの特性を考慮してプライバシーリスクの起こりやすさを推定する。

#	項目	説明
4	かなり高い	管理策を用意していない、又は、既存の管理策等に不備があることから、リスクが発生することは容易に想定できる。(セキュリティ対策を施していらず、情報漏洩等が発生する 等)
3	ある程度高い	リスクが発生する可能性があると思われる。(乗車時のPCの置き忘れ、社用携帯の紛失 等)
2	一定の可能性	既存の管理策等の観点から、リスクが発生すること可能性は低い、又は一定の可能性があると思われる。(確認メッセージが表示されるが、メールの誤送信が発生する 等)
1	かなり低い	リスクが起こる可能性はない。また、実施のモチベーション等の観点から限りなく低い可能性である。(入館証読み取り機とアクセスコードで保護された部屋に保管された紙文書の盗難 等)

プライバシーリスクの分析、評価

- プライバシーリスクの影響の大きさ及び起こりやすさの評価結果からプライバシーリスクマップを作成した。
- 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参考となる。



プライバシーリスクの対応策

HITACHI
Inspire the Next

- 特定したプライバシーリスクの対応策を決定する。

プライバシーリスクの対応策(1/4)

#	特定したプライバシーリスク	プライバシリスクの対応策
4	ユーザーの個人情報を電子メールで取得するため、暗号のかけ忘れ等により、電子メールに含まれるユーザー情報がネットワーク上で漏洩する可能性がある。	• ユーザー所属法人が可能であれば、オンラインストレージを活用し適切にアクセス権を設定し、ファイル共有を行う。
5		
6		
7		
8		

プライバシーリスク管理策

- プライバシーリスクの抽出と対応策の検討については、静的なものになる。今後の事業や社会環境の変化も踏まえて、プライバシーリスクが発生する可能性を検討し、管理すべき事項を明確化しておく必要がある。
- ISO/IEC 29100のプライバシーの原則に沿って今後、生じる可能性がある変動要因とそれに伴うリスクを整理し、このリスクへの対応を図るための管理策を整理した。

プライバシーリスク管理策(1/2)

観点	変動要因	リスク	管理策
同意及び選択			
目的の正当性及び明確化	事業内容の変更により、パーソナルデータ収集の目的等が変更になる		
収集制限	事業内容や活用する技術の変化によって収集するパーソナルデータが拡大したり、変更したりする		
データの最小化			

プライバシーリスク管理策

プライバシーリスク管理策(2/2)

観点	変動要因	リスク	管理策
利用，保有，及び開示の制限			
正確性及び品質	技術的な変化によって事業で扱うパーソナルデータの品質が変動する	技術的な変化によって解析の精度等が落ちる	精度の評価を定期的に行うとともに、技術的な変化によるデータ品質の変動についても定期的にモニタリングする
公開性，透明性，及び通知			
個人参加及びアクセス			
責任			
情報セキュリティ	情報システムへの攻撃方法等は常に変化するとともに、脆弱性等も随時、発見される可能性がある		
プライバシーコンプライアンス	個人情報保護に関する法制度、あるいは業界団体のガイドライン等が見直される可能性がある		

プライバシーリスク対応計画

- プライバシーリスクの対応行動を実施するために、プライバシーリスク対応計画、管理計画を策定した。
- 管理責任者は本対応計画、管理計画に基づき、プライバシーリスクを対処する。

#	プライバシーリスク対応策	対応期限
1		

#	管理策	モニタリングのタイミング
1		

プライバシーリスク対応計画

- プライバシーリスクの対応行動を実施するために、プライバシーリスク対応計画、管理計画を策定した。
- 管理責任者は本対応計画、管理計画に基づき、プライバシーリスクを対処する。

#	プライバシーリスク対応策	対応期限
1		

#	管理策	モニタリングのタイミング
1		

プライバシーリスク対応計画

HITACHI
Inspire the Next

- 特定したプライバシーリスクの対応を適切に行うことで、リスク低減することができる。

プライバシーリスク対応策　実施前

影響度					
	4．甚大		①		
	3．重大			②	
	2．限定的			③	
	1．無視できる				
評価基準		1．かなり低い	2．一定の可能性	3．ある程度高い	4．かなり高い
		起こりやすさ			

プライバシーリスク管理策　実施前

影響度					
	4．甚大				
	3．重大		①	②	
	2．限定的			③	
	1．無視できる				
評価基準		1．かなり低い	2．一定の可能性	3．ある程度高い	4．かなり高い
		起こりやすさ			

プライバシーリスク対応策　実施後

影響度					
	4．甚大				
	3．重大	①			
	2．限定的	②			
	1．無視できる	③			
評価基準		1．かなり低い	2．一定の可能性	3．ある程度高い	4．かなり高い
		起こりやすさ			

プライバシーリスク管理策　実施後

影響度					
	4．甚大				
	3．重大				
	2．限定的	①②			
	1．無視できる	③			
評価基準		1．かなり低い	2．一定の可能性	3．ある程度高い	4．かなり高い
		起こりやすさ			

HITACHI
Inspire the Next

まとめ

まとめ

- プライバシーガバナンスのニーズは益々高まると考えられる。
- 日立の情報通信システム関連部門ではプライバシー保護の仕組みを運用しており、その中でPIAも実施している。
- ISO/IEC29134をフルスペックでやることは効果もあるが、それなりの労力を要する。
- すべての案件について実施するのは非現実的であり、対象の選定が鍵となる。

HITACHI

Inspire the Next