IWATA GODO
Established 1902

「個人情報保護評価（PIA）の意義と実施手順について」

2022年12月15日
（DPO協会第6回個人情報保護セミナー）

岩田合同法律事務所
弁護士　松田 章良

Ⅰ 本日のトピック

1 イントロダクション

2 PIA実施に当たっての基本的な考え方

3 PIAの一般的なプロセス・実施手順

4 PIAの実務例

Ⅱ　イントロダクション

PIA＝Privacy Impact Assessment（プライバシー・インパクト・アセスメント）

個人データの利活用を伴う事業について、適正な利活用を確保するための事業者側の自発的な取り組み

Privacy by Design：事業計画全体を通じて、計画的にプライバシー保護の仕組みを導入することにより、違反時・漏えいのリスクを軽減し、かかる事案の発生に伴うコスト発生を防止

3年ごとの見直し・制度改正大綱では義務化も検討されたが、2022年施行の改正法では義務化は見送られた。事業の規模・性質、取り扱う個人データの性質に応じて「推奨」されている。

「PIAの取組の促進について」（個人情報保護委員会、2021年6月30日）

「個人情報保護に関する民間の自主的取組の在り方に関する調査報告書」（2022年3月）

Ⅲ　PIA実施に当たっての基本的考え方①

PIAを実施することによるメリット

当該事業における個人データ取扱状況の透明化

消費者をはじめとする利害関係者からの信頼の獲得

- 事故発生のリスクを軽減
- 事故が発生した場合においても、事業者にて適切な対応を取っていたことの証明手段となる（透明性の向上）

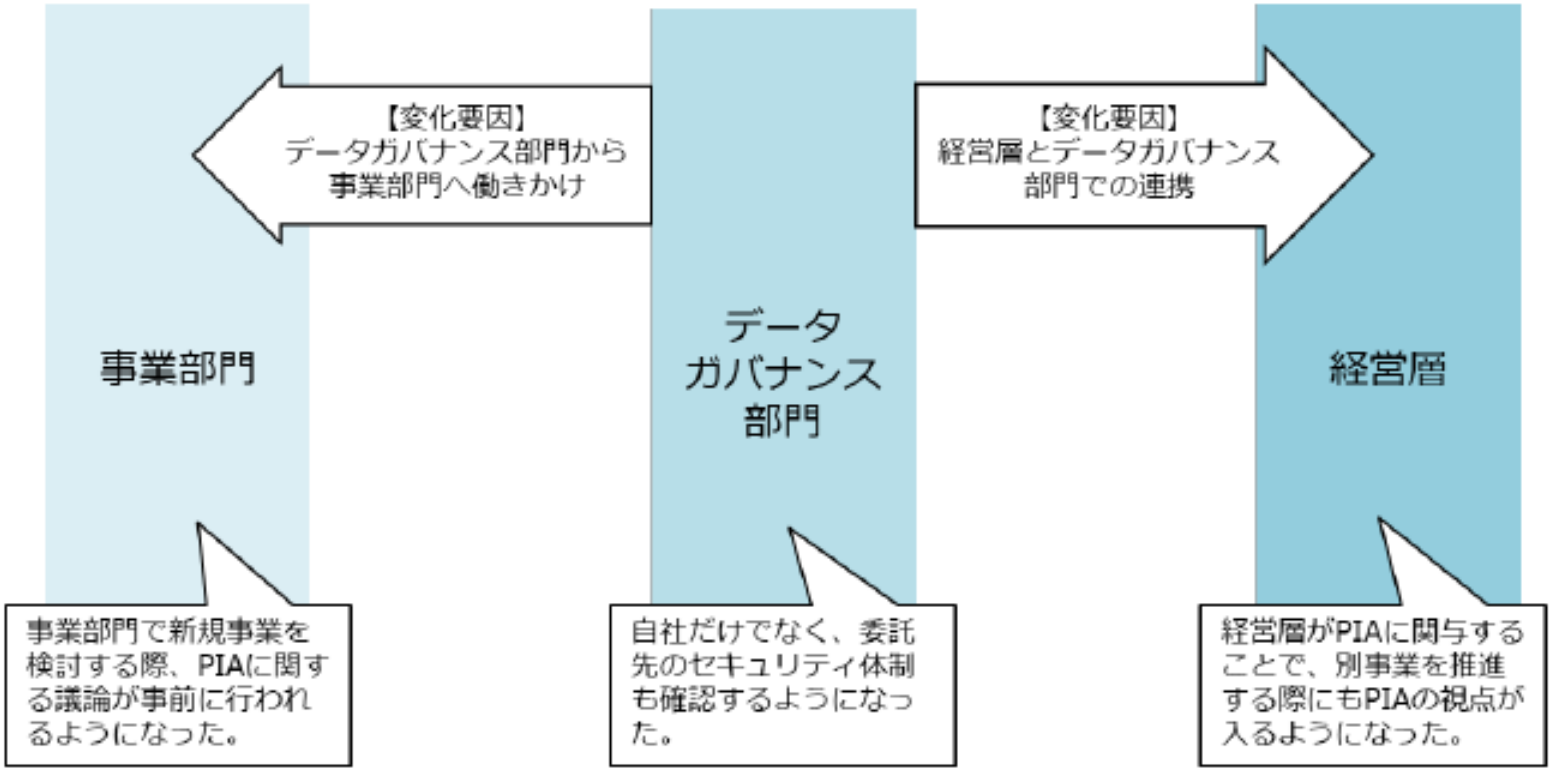
事業のトータルコストの削減

- 事業の中止、多額のコストをかけた改修対応、消費者への補償などの防止

従業者の教育を含む、事業者の個人データの取扱いに係るガバナンスの向上

- 経営層を含め、自社における個人データの取扱い状況及びそれに伴うリスクを把握することが可能に

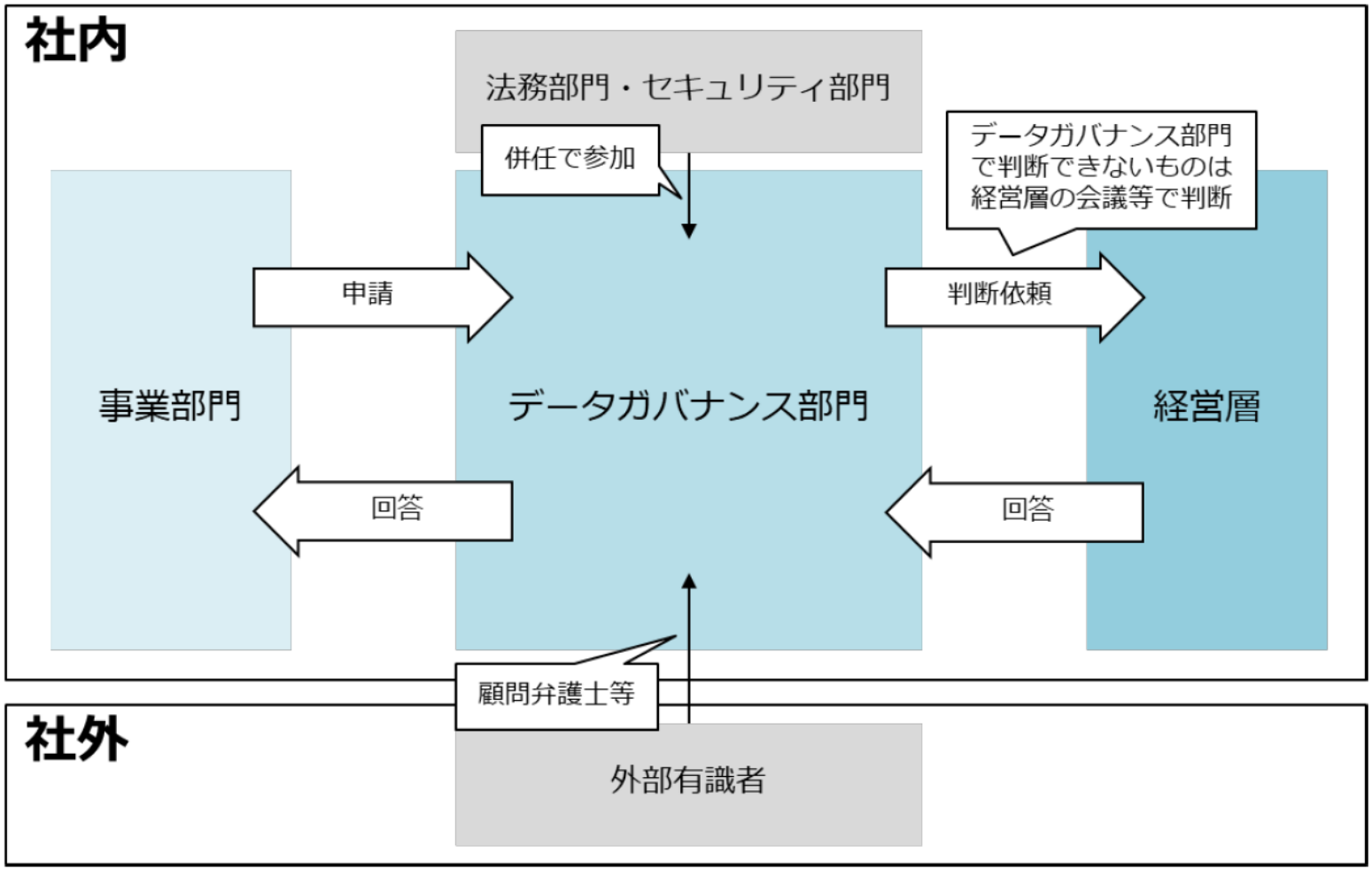
Ⅲ　PIA実施に当たっての基本的考え方②：効果の例



「個人情報保護に関する民間の自主的取組の在り方に関する調査報告書」（2022年3月）（図表14）

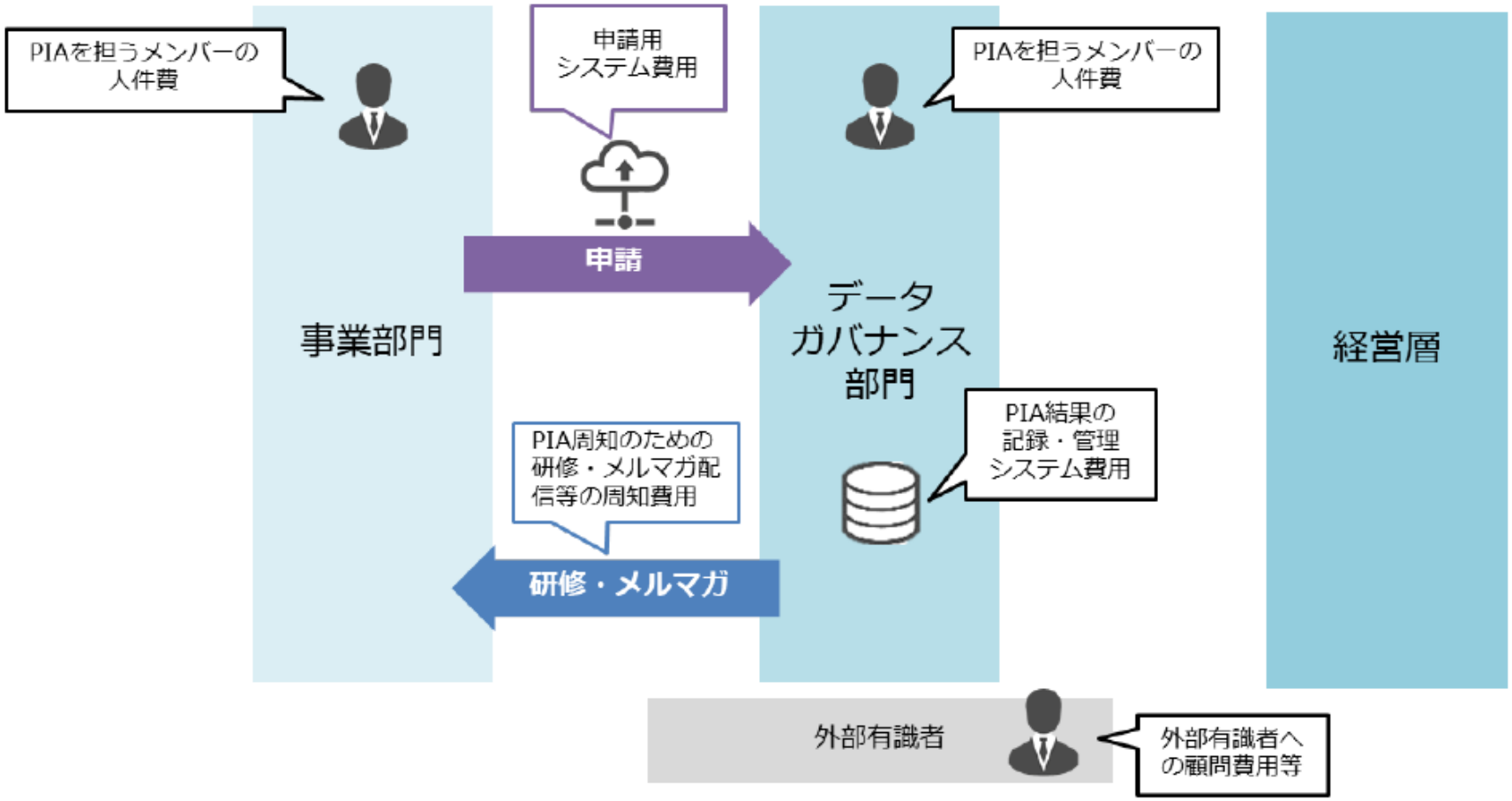
- 例1：販売店舗への顧客システムについて、販売店の全てで顧客情報を閲覧可能であったことから、アクセス制限を導入
- 例2：外国のクラウドサービス事業者（GDPRベース）：管理者としてのPIA+処理者としてのPIA

Ⅲ　PIA実施の基本的考え方③：実施体制のイメージ



「個人情報保護に関する民間の自主的取組の在り方に関する調査報告書」（2022年3月）（図表10）

Ⅲ　PIA実施の基本的考え方④:コスト



「個人情報保護に関する民間の自主的取組の在り方に関する調査報告書」(2022年3月)(図表13)

Ⅳ　PIAの一般的なプロセス・実施手順

準備

1.PIA実施要否の検討
2.体制の整備
3.個人情報等のフローの整理
4.関係法令等の整理

リスクの特定・評価

- 個人情報等のフローにより、事業内容に応じた評価項目を設定し、リスク要因を特定した上、影響度や発生可能性の観点から評価を行う

リスクの低減

- 対応方針の決定
- PIA報告書の作成（必要に応じて、有識者を含む第三者機関によるチェック）

Ⅳ　準備段階：PIA実施要否の判断①

PIA実施に当たっての考慮要素

時期

- 原則→事業の企画・設計段階
- ただし→事業の進行段階で必要性を認識した場合に、実行することも意義がある（個人の権利・利益の侵害が生じる前に是正をすることが可能であるため）

対象範囲

- 事業の規模・性質、個人データの性質・分量、利用期間、利用目的等に応じて、個別的に判断する必要
- 重要な視点は、「消費者本人の個人情報の保護を含む権利利益の保護にどの程度資するか」
- 委託先などを含め、事業に係る関係者の全体について検討することが望ましい

対象法令

- 個人情報保護法
- 法令以上の対応を取ることが望ましい場合もある（例：①個人関連情報について、個人の権利利益保護のための方策、AIの利用）

Ⅳ　準備段階：PIA実施要否の検討②

PIA実施要否の検討

- PIA実施の必要性が高いと考えられる事例
  1）要配慮個人情報・生体認証データ等の利用を行う場合
  2）いわゆるプロファイリング（取得したデータから本人の行動・関心等の分析を行う場合）
  3）委託・共同利用などにより、他の事業者とともに個人データを用いる場合
  4）個人データに係る業務フローの変更、事業の買収・拡大

- 参考：GDPRにおけるDPIA（Data Protection Impact Assessment）
  ・「特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合」（GDPR35条）
  ・ガイドライン（「高いリスク」の判断について）
  1)プロファイリングを含め、自動的な取扱いに基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価の場合
  2)第9条第１項に規定する特別な種類のデータ又は第10 条に規定する有罪判決及び犯罪行為と関連する個人データの大規模な取扱いの場合
  3)公衆がアクセス可能な場所の、システムによる監視が大規模に行われる場合

Ⅳ　準備段階：体制の整備

体制の整備：必要なリソースの投入（経営陣の理解が必要）

①　実施責任者の任命

- PIAの業務プロセスについて十分に理解しており、権限を有することが必要

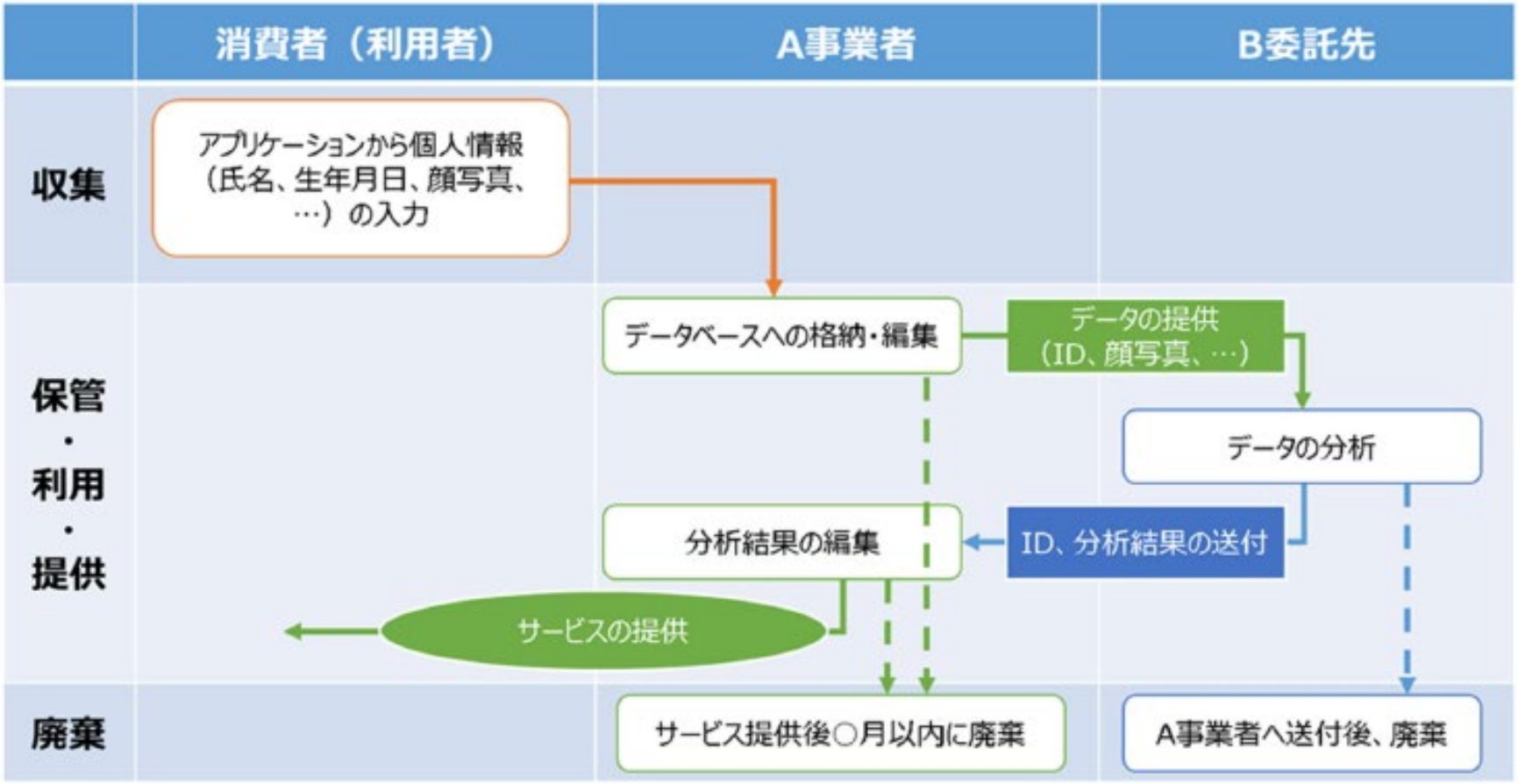
②　投入人員数などのリソース計画

- 部門を横断するのが通常（事業の実施部門、IT・システム部門、法務部門、コンプライアンス部門、（もしあれば）データガバナンス部門）
- 外部有識者（顧問弁護士、消費者団体の代表など）

③　スケジュールの策定

- 1/2週間～数か月（複雑な事案、外部の関与事業者との調整・交渉を要する場合）

Ⅳ　準備段階：個人情報等のフローの整理



「PIAの取組の促進について」（個人情報保護委員会、2021年6月30日）（図表3）

Ⅳ　準備段階：関係法令等の整理

評価の根拠・要件の洗い出し（既存事業との平仄も重要）

個人情報保護法、（適用がある場合）業法規制

- 法令上義務とされている項目に加え、ガイドライン等において、「望ましい」とされている事項に対応するかの検討
- クロスボーダー案件の場合、海外法令の基準に合わせる場合も

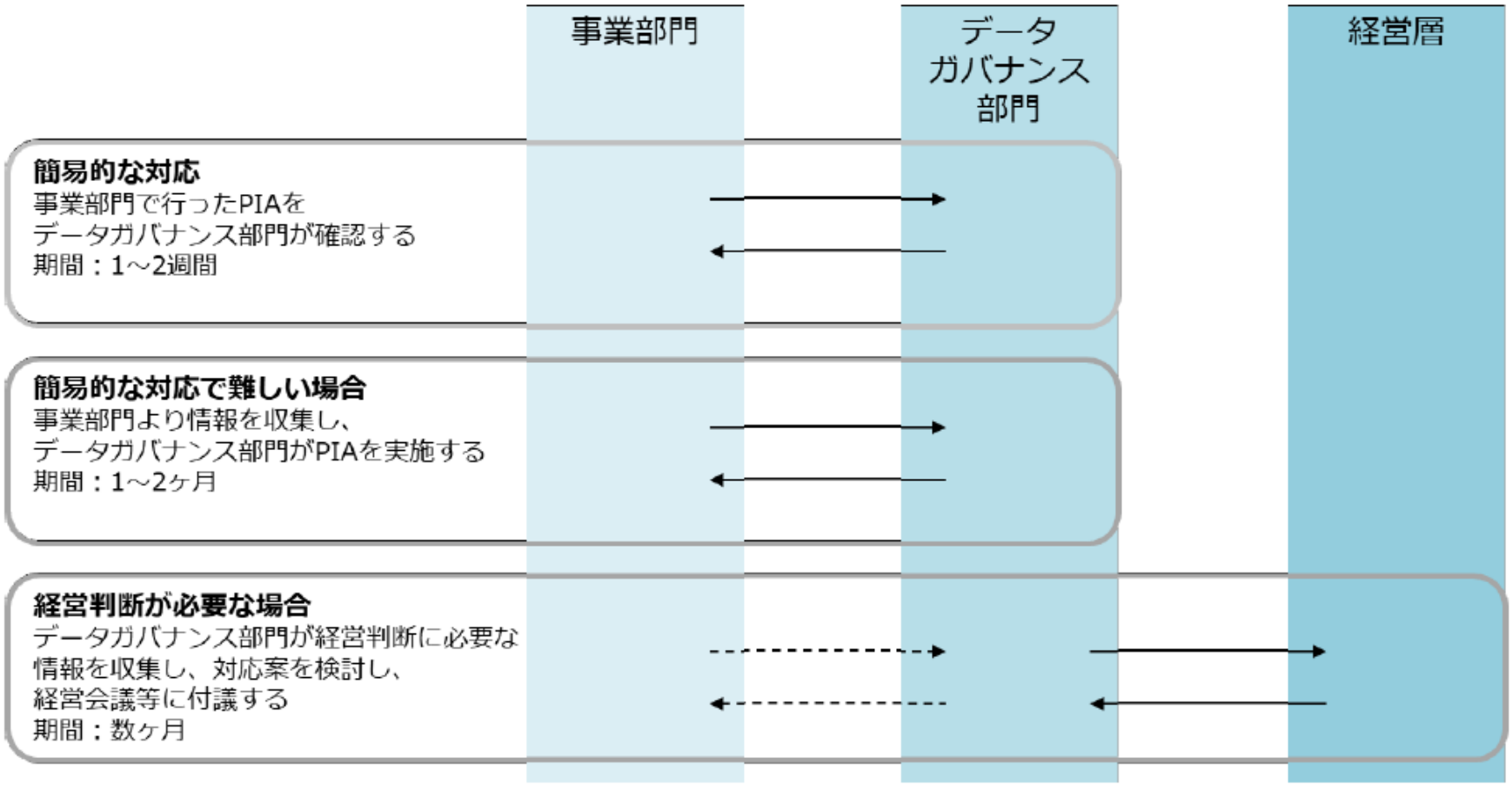
監督官庁の指針、業界団体の指針など

- 法令上の義務とはされていない事項も多いが、ベストプラクティスとして従うことを検討

社内規程・契約・セキュリティルールなど

- 特に、契約に留意（ベンダーとの契約、事業関係者との間の契約については、PIAと同時並行で契約交渉を行うべき場合も多い）

Ⅳ　リスクの特定・評価：実施方法



「個人情報保護に関する民間の自主的取組の在り方に関する調査報告書」（2022年3月）（図表12）

Ⅳ　リスクの特定・評価：リスクの特定

事業者側のリスク

- 利用目的の通知や同意の取得が本人に分かりやすい形で行われるか。
- 本人が、自らの個人情報等がどのように取り扱われることとなるか、利用目的から合理的に予測・想定できるか。
- 個人情報等が過剰に収集される可能性がないか。
- 本人からの各種請求への対応は滞りなく行われるか。
- 権限のない者が個人情報等に不正にアクセスする可能性がないか。
- 個人情報等の紛失、盗難又は不正に持ち出される可能性がないか。
- 不適正な個人情報等の編集、紐づけ、分析等の利用が行われる可能性がないか。
- 不必要に保有し続ける情報がないか。

消費者側のリスク

- 事業者側で想定している利用方法として意図していた行動とは異なる行動（デバイスの誤操作・誤設定、機器の紛失等）があり得ることも踏まえて、リスクを特定

Ⅳ　リスクの特定・評価：リスク整理表のイメージ

	個人情報保護法	○○事業ガイドブック	その他
収集	・利用目的が通知・公表されているか ・不正な取得がなされていないか …	・同意の取得や通知が本人に分かりやすい形で行われているか。 …	・事業に不要な情報まで収集していないか …
保管	・内容の正確性が確保されているか ・必要かつ適切な安全管理措置が講じられているか …	・示されているセキュリティ対策がなされているか。 …	・各種請求対応は円滑に行われるか。 ・消費者による機器の紛失等の際の処理が適切になされるか。 …
利用	・目的外の利用がないか ・不適正な利用がなされていないか …	・推奨されている手順に沿って利用がなされているか …	・処理のログが取られているか ・不適切な編集・分析が行われる可能性はないか …
提供	・第三者提供時にあたり同意を取得することとされているか …	移転先が本人に明示されているか …	・移転する情報は必要かつ最小限なものとなっているか …
廃棄	・必要ない情報は廃棄されているか …	・保存期間が設定されているか …	・廃棄時に複数人で確認されるか …

「PIAの取組の促進について」（個人情報保護委員会、2021年6月30日）（図表4）

Ⅳ　リスクの特定・評価：リスクの評価基準（例）

（影響度）

レベル		基準
4	甚大	・利用者に回復不可能な多大な不利益が生じ、これに伴い、企業の信用失墜や経済的損失が生じる （心理的・身体的疾患、口座番号、暗証番号の流出等）
3	重大	・利用者に一定の不利益が生じるものの、回復可能であり、企業の信用等への影響は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	・一部の利用者に不安感を与え、企業の信頼等に影響が及ぶ可能性があるが、その範囲は限定的 （サービスへのアクセス拒否、利用方法に関する説明不足等）
1	無視可	・利用者への不利益の程度は極めて小さく、企業への影響は無視できるレベル （同意取得時にアプリケーション上にチェックを入れる煩わしさ等）

（発生可能性）

頻度		基準
4	非常に高い	・安全管理等に不備があるため、リスク発生が容易に想定される （セキュリティ対策の不備で情報漏えい等が発生する等）
3	ある程度高い	・安全管理の一部に不備があるため、リスク発生の可能性がある （ノートPCや携帯電話などのモバイルの紛失等）
2	一定の可能性	・安全管理措置により、リスク発生の可能性は低い （注意喚起のメッセージが表示される中でのメール誤送信等）
1	非常に低い	・リスク発生の可能性は極めて低い （入館証読取機でセキュリティ対応の採られた室内の書類の紛失等）

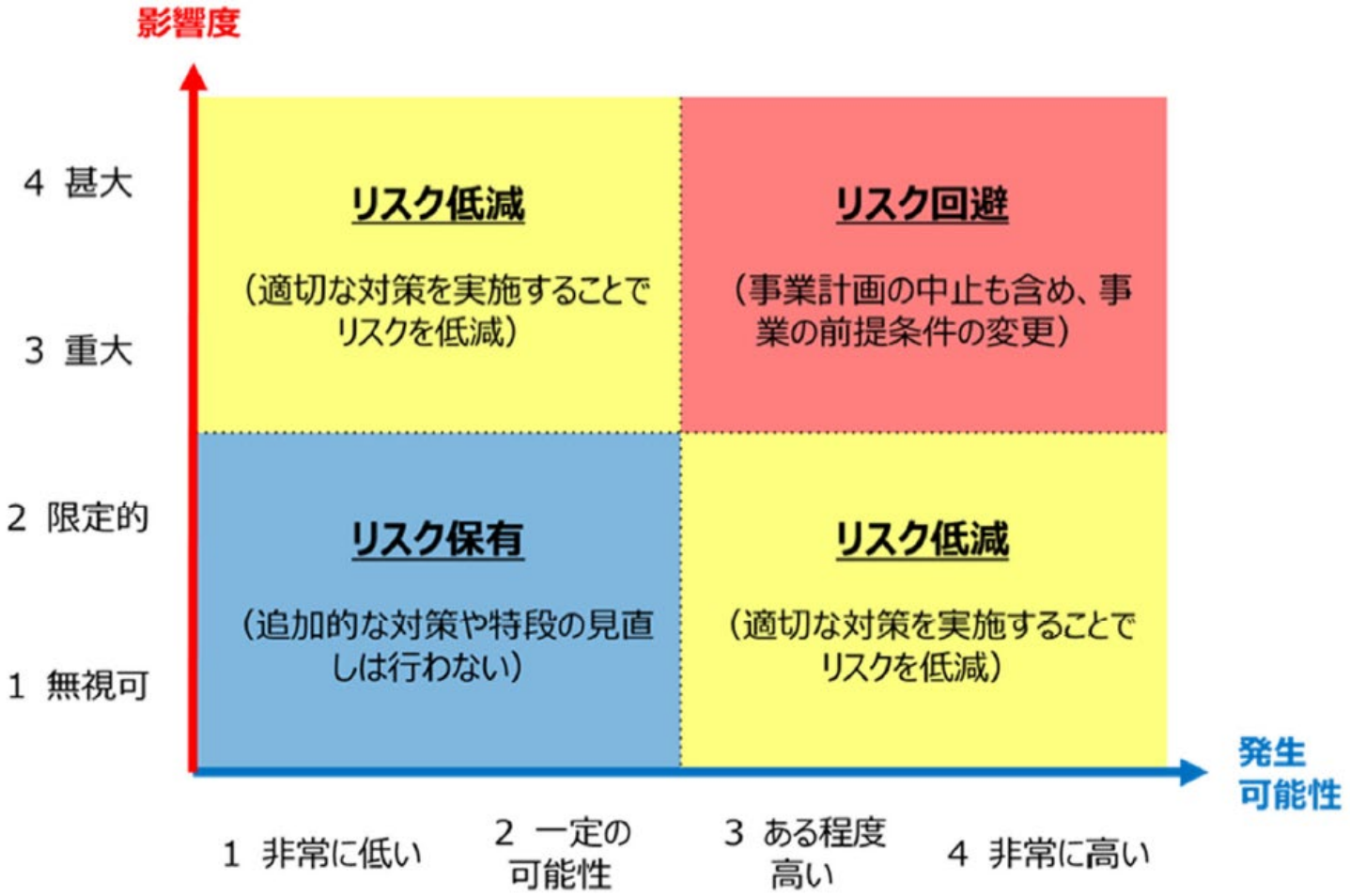
「PIAの取組の促進について」（個人情報保護委員会、2021年6月30日）（図表5）

Ⅳ　リスクの特定・評価：リスクの評価表

	特定したリスク	取扱状況、措置等	影響度	発生可能性
収集	①利用目的の通知や同意の取得が本人に分かりやすい形で行われるか	図も含めてアプリケーション上に内容を表示し、チェックを入れる設計となっている	1	1
	②事業に不要な情報まで収集されていないか	一部、利用目的と関連のない情報を取得する設計となっている	2	1
	…	…	…	…
保管	⑤○○事業ガイドブックに示されているセキュリティ対策がなされているか	一部、実施できていないセキュリティ対策がある	3	4
	…	…	…	…
利用	⑨処理のログが取られているか	ログは取るようにしているが、容易に編集・削除できるようになっている	3	2
	…	…	…	…
…	…	…	…	…
廃棄	㉒必要ない情報は廃棄されているか	サービス提供後、○月以内に廃棄されることとしている	1	1
	…	…	…	…

「PIAの取組の促進について」（個人情報保護委員会、2021年6月30日）（図表6）

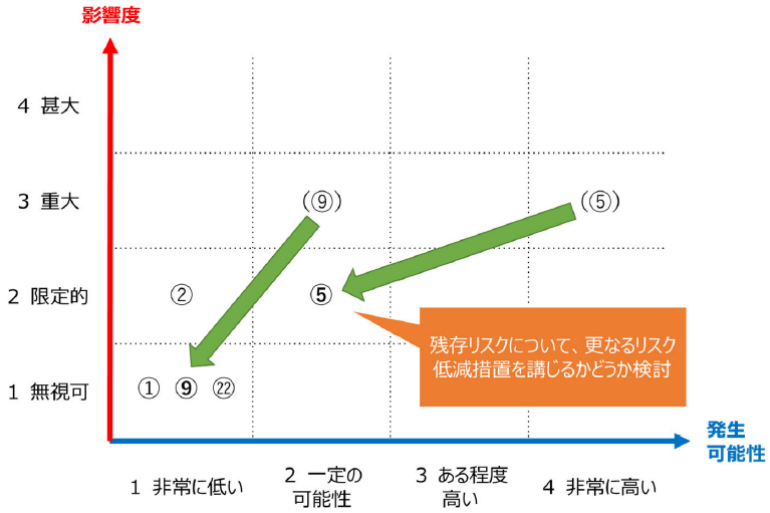
Ⅳ　リスクの低減：対応方針（例）



「PIAの取組の促進について」（個人情報保護委員会、2021年6月30日）（図表8）

Ⅳ　リスクの低減：対応策・対応後のリスクマップ

特定したリスク	想定していた 取扱状況、措置等	対応策
…	…	…
⑤○○事業ガイドブックに示されているセキュリティ対策がなされているか。	一部、実施できていないセキュリティ対策がある	・推奨されているセキュリティ対策を実施 ・ …
…	…	…
⑨処理のログが取られているか	ログは取るようにしているが、容易に編集・削除できるようになっている	・ログにアクセスできる者を限定し、また監査部門がシステム監査を行う ・ …
…	…	…



「PIAの取組の促進について」（個人情報保護委員会、2021年6月30日）（図表9、10）

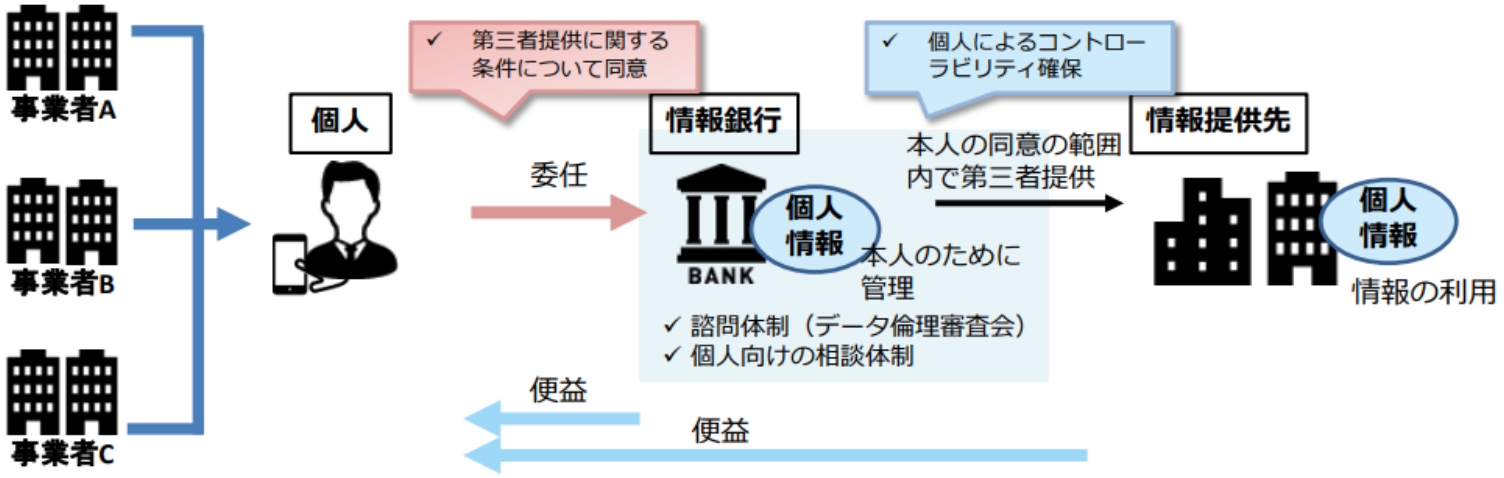
Ⅴ　PIAの実例

情報銀行の事業ストラクチャー

「情報銀行」は、実効的な本人関与（コントローラビリティ）を高めて、パーソナルデータの流通・活用を促進するという目的の下、本人が同意した一定の範囲において、本人が、信頼できる主体に個人情報の第三者提供を委任するというもの。

【機能】
- 「情報銀行」の機能は、個人からの委任を受けて、当該個人に関する個人情報を含むデータを管理するとともに、当該データを第三者（データを利活用する事業者）に提供することであり、個人は直接的又は間接的な便益を受け取る。
- 本人の同意は、使いやすいユーザインタフェースを用いて、情報銀行から提案された第三者提供の可否を個別に判断する、又は、情報銀行から事前に示された第三者提供の条件を個別に／包括的に選択する、方法により行う。

【個人との関係】
- 情報銀行が個人に提供するサービス内容（情報銀行が扱うデータの種類、提供先第三者となる事業者の条件、提供先における利用条件）については、情報銀行が個人に対して適切に提示し、個人が同意するとともに、契約等により当該サービス内容について情報銀行の責任を担保する。



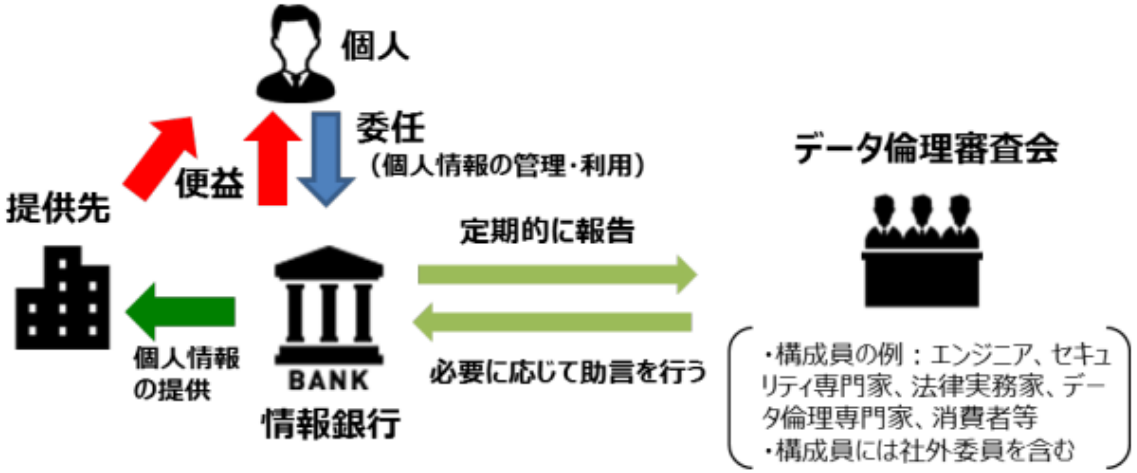
「情報信託機能の認定に係る指針Ver2.1」別紙3、3頁（情報信託機能の認定スキームの在り方に関する検討会（総務省他、2021年8月））

Ⅴ　PIAの実例

情報銀行におけるデータ倫理審査会

■ データ倫理審査会における審議の考え方
- 情報銀行は、個人の代理として、個人が安心して自らに関する情報を預けられる存在であることが期待される。このため、利用者たる個人の視点に立ち、適切な運営が確保される必要がある。
- このため、データ倫理審査会は、情報銀行の事業内容が個人の利益に反していないかという観点から審議を行う。

（例）・個人によるコントローラビリティを確保するための機能が誤解のないUIで提供されているか
・個人の同意している提供先の条件について、個人の予測できる範囲内で解釈されて運用されているか
・個人にとって不利益となる利用がされていないか／個人に対し個人情報の利用によるリスクが伝えられているか
・個人にとって高いリスクを発生させる恐れがある場合には、GDPRで義務づけられているDPIA（データ保護影響評価）を参考にすることも考えられる



●情報銀行事業について、以下の事項についてその適切性を審議し、必要に応じて助言を行う
- ・個人と情報銀行の間の契約の内容
- ・情報銀行の委任した個人情報の利用目的
- ・個人による情報銀行に委任した個人情報の第三者提供に係る条件の指定及び変更の方法（UI）
- ・提供先第三者の選定方法
- ・委任を受けた個人情報の提供の判断

●運営方法
- ・構成員及び（必要な範囲の）議事録は公開する
- ・必要に応じ情報銀行に調査・報告を求めることができる

「情報信託機能の認定に係る指針Ver2.1」別紙3、13頁（情報信託機能の認定スキームの在り方に関する検討会（総務省他、2021年8月））

講師プロフィール　弁護士　松田章良　(AKIRA MATSUDA)

岩田合同法律事務所パートナー弁護士(2008年弁護士登録)。2006年東京大学法学部卒業、2008年9月長島・大野・常松法律事務所入所。2015年コロンビア・ロースクール(LL.M.)卒業(Harlan Fiske Stone賞)、同年NY州司法試験合格。2015年9月岩田合同法律事務所入所。同年11月より2021年9月までシンガポールのDREW & NAPIER法律事務所にても勤務。2019年NY州弁護士登録。

シンガポール・日本の両方を拠点に、クロスボーダーの企業取引、紛争及び調査案件を主に取り扱っているほか、東南アジア地域を中心として、日本企業の海外進出・展開に係る案件を多く担当している。また、日本・シンガポール・EUにおけるデータプロテクション(個人情報保護)に係る案件を多数取り扱うほか、AIやフィンテック分野を含む先進的なデータの利活用に係る案件を専門とする。

≪最近の著作≫
Data Protection 2nd Edition Country Comparative Guide (Legal 500)
Global Data Review- Handbook 2020 (Law Business Research)
Data Privacy & Transfer in Investigations (Global Investigations Review (Law Business Research))
Global Legal Insights to: AI, Machine Learning & Big Data 2020 (Global Legal Group)
Why AI is the future of Cyber Security (ICLG Cybersecurity 2020) (Global Legal Group)
Corporate Investigation (Japan) (ICLG Corporate Investigations 2020) (Global Legal Group)
GTDT- Cloud Computing 2021 (Law Business Research)

≪連絡先≫
岩田合同法律事務所
TEL: +81 3 3214 6282　　E-MAIL: amatsuda@iwatagodo.com