2021年12月9日

一般社団法人コンパクトスマートシティプラットフォーム協議会
会員様向け　個人情報保護法勉強会

スマートシティと個人情報保護法
～法令の概要と体制整備の進め方～

ＴＭＩ総合法律事務所　パートナー
弁護士・情報処理安全確保支援士
寺門　峻佑

講師紹介

寺門峻佑（てらかど　しゅんすけ）

TMI総合法律事務所　パートナー弁護士（日本・NY州）
情報処理安全確保支援士
情報セキュリティ監査人補

URL：http://www.tmi.gr.jp/staff/s_terakado.html

- TMIプライバシー＆セキュリティコンサルティング株式会社取締役、内閣サイバーセキュリティセンタータスクフォース構成員、防衛省陸上自衛隊通信学校非常勤講師、経済産業省大臣官房臨時専門アドバイザー、滋賀大学データサイエンス学部インダストリアルアドバイザー、情報処理安全確保支援士会理事を歴任。
- データ利活用における個人情報保護法・各国データ保護法対応、情報セキュリティインシデント対応・情報セキュリティ管理体制構築を中心としたデータ・プライバシー・サイバーセキュリティ領域、システム/アプリ開発・ライセンスビジネスを中心としたIT法務・紛争、フォレンジックを含む不正調査案件を主に取扱う。
- ロサンゼルスのQuinn Emanuel Urquhart & Sullivan, LLPにおける国際紛争案件、サンフランシスコのWikimedia Foundation, Inc.法務部における各国データ保護法・各国著作権法・ドメイン保護案件、エストニアのLaw Firm SORAINENテクノロジーセクターにおけるeコマース・Fintech関連案件の経験も有する。

アジェンダ

1．スマートシティと個人情報保護法

2．個人情報保護法の概要

3．データガバナンス体制整備の進め方

4．令和２年改正個人情報保護法の概要

１．スマートシティと個人情報保護法

スマートシティとデータ連携

住民が参画し、住民目線で、2030年頃に実現される未来社会を先行実現することを目指す。

【ポイント】

①**生活全般にまたがる複数分野の先端的サービスの提供**
AIやビッグデータなど先端技術を活用し、行政手続、移動、医療、教育など幅広い分野で利便性を向上。

②**複数分野間でのデータ連携**
複数分野の先端的サービス実現のため、「データ連携基盤」を通じて、様々なデータを連携・共有。

③**大胆な規制改革**
先端的サービスを実現するための規制改革を同時・一体的・包括的に推進。

出典：内閣府地方創生推進事務局「『スーパーシティ』構想について」（令和3年4月）4頁より抜粋

スマートシティと個人情報保護法

個人情報保護法：規制の概要

個人情報該当性	Cookie, IDFA, POSデータと個人情報 容易照合性の議論
取得フェーズ	利用目的の通知公表（適切なプラポリ） 要配慮個人情報（本人の同意取得）
管理フェーズ	安全管理措置 委託先の監督 権利行使への対応
提供フェーズ	第三者提供の同意と確認記録義務 委託・共同利用の枠組み 外国にある第三者への提供

スマートシティと個人情報保護法：令和2年改正

改正法案の内容

1．個人の権利の在り方

- **利用停止・消去等の個人の請求権**について、不正取得等の一部の法違反の場合に加えて、**個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和**する。
- **保有個人データの開示方法**（※）について、**電磁的記録の提供を含め、本人が指示できる**ようにする。

  （※）現行は、原則として、書面の交付による方法とされている。
- 個人データの授受に関する**第三者提供記録**について、**本人が開示請求できる**ようにする。
- ６ヶ月以内に消去する**短期保存データ**について、保有個人データに含めることとし、**開示、利用停止等の対象**とする。
- オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、**①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外**とする。

  （※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

2．事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、**委員会への報告及び本人への通知を義務化**する。

  （※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。
- **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

3．事業者による自主的な取組を促す仕組みの在り方

- 認定団体制度について、現行制度（※）に加え、**企業の特定分野(部門)を対象とする団体を認定できるようにする。**

  （※）現行の認定団体は、対象事業者のすべての分野(部門)を対象とする。

4．データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した**「仮名加工情報」を創設**し、内部分析に限定する等を条件に、**開示・利用停止請求への対応等の義務を緩和**する。
- 提供元では個人データに該当しないものの、**提供先において個人データとなることが想定される情報の第三者提供**について、**本人同意が得られていること等の確認を義務**付ける。

5．ペナルティの在り方

- 委員会による命令違反・委員会に対する虚偽報告等の**法定刑を引き上げる**。

  （※）命令違反：6月以下の懲役又は30万円以下の罰金
  → **1年以下の懲役又は100万円以下の罰金**

  虚偽報告等：30万円以下の罰金 → **50万円以下の罰金**
- データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、**法人に対しては行為者よりも罰金刑の最高額を引き上げる**（法人重科）。

  （※）個人と同額の罰金（50万円又は30万円以下の罰金） → **1億円以下の罰金**

6．法の域外適用・越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、**罰則によって担保された報告徴収・命令の対象**とする。
- 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

※　その他、本改正に伴い、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

出典：個人情報保護委員会「個人の保護に関する法律等の一部を改正する法律案（概要）」（令和２年３月10日）参照　https://www.ppc.go.jp/files/pdf/200310_gaiyou.pdf

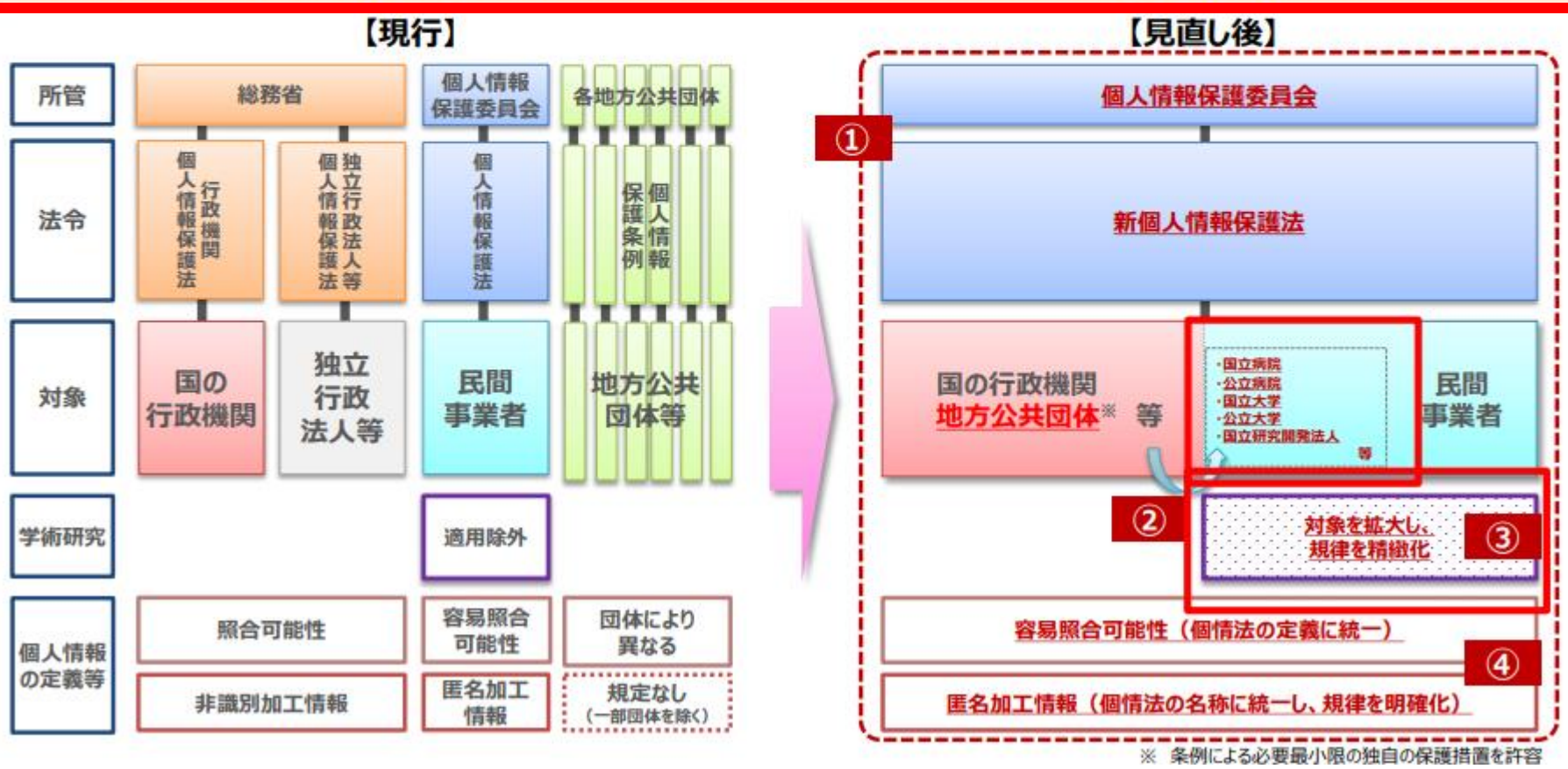
スマートシティと個人情報保護法：令和3年改正

① 個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の**3本の法律を1本の法律に統合**するとともに、**地方公共団体の個人情報保護制度**についても**統合後の法律において全国的な共通ルールを規定**し、**全体の所管を個人情報保護委員会に一元化。**

② 医療分野・学術分野の規制を統一するため、**国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用。**

③ 学術研究分野を含めたGDPRの十分性認定への対応を目指し、**学術研究に係る適用除外規定**について、一律の適用除外ではなく、**義務ごとの例外規定として精緻化。**

④ **個人情報の定義等を国・民間・地方で統一**するとともに、行政機関等での**匿名加工情報の取扱いに関する規律を明確化。**



出典：個人情報保護委員会「デジタル社会の形成を図るための関係法律の整備に関する法律」の「概要資料」1頁より抜粋 https://www.ppc.go.jp/files/pdf/seibihou_gaiyou.pdf

２．個人情報保護法の概要

①個人情報該当性

個情法：個人情報の定義（2条1項）

- 特定の個人を識別することができるものであり、他の情報により特定の個人を識別することができるものを含む

典型例

- ✓ 氏名・生年月日・連絡先の情報など特定の個人が識別できる情報
- ✓ カメラ画像など本人が判別できる映像情報

個人識別符号

- ✓ 身体の一部の特徴を変換した符号

  ＤＮＡ、顔、虹彩、声紋、歩行態様、手指の静脈、指紋等

- ✓ サービス利用や書類にて対象者ごとに割り振られる符号

  旅券番号、基礎年金番号、免許証番号、住民票コード、保険証等

①個人情報該当性

個情法：個人情報の定義（2条1項）

- 特定の個人を識別することができるものであり、他の情報により特定の個人を識別することができるものを含む

Cookie, IDFA, POSデータは個人情報と認定されるのか？
単体では特定の個人を識別できないので、原則として、個人情報に該当しない　　※GDPR等ではcookieも個人情報

Cookie, IDFA, POSデータが個人情報に該当する場合は？
他の情報と容易に照合することで個人識別性がある場合
例：会員情報・アカウント登録情報などとの連携
例：共通IDが付された個人識別性のある情報が法人内にある

なお、個人関連情報の提供先の個人データ化に関する法改正

②取得フェーズ

個情法（取得フェーズ）：利用目的の通知・公表

- 利用目的はできる限り特定して公表する必要がある
- 利用目的の大幅な変更は本人同意が必要となる

推奨されないプライバシーポリシーの記載

「マーケティング」「情報提供」

推奨されるプライバシーポリシーの記載

「お客様の当社ウェブサイト・アプリの利用状況の解析」

「お客様の趣味・趣向に合った広告配信」

※取得した個人情報は特定した利用目的の範囲内で利用する

②取得フェーズ

個情法（取得フェーズ）：要配慮個人情報

- 要配慮個人情報を取得する時は本人の同意が必要

要配慮個人情報とは

- 人種、信条、社会的身分、病歴、前科、犯罪被害情報
- その他政令で定めるもの（本人に対する不当な差別、偏見が生じないように特に配慮を要するもの）
  - ✓ 身体障害・知的障害・精神障害等があること
  - ✓ 健康診断その他の検査の結果
  - ✓ 保健指導、診療・調剤情報
  - ✓ 逮捕等の刑事手続が行われたこと
  - ✓ 保護処分等の少年の保護事件に関する手続が行われたこと

③提供フェーズ

個情法（提供フェーズ）：第三者提供

- 個人データの第三者提供には本人同意が必要
- 委託・共同利用の枠組みの場合には本人同意は不要

委託提供

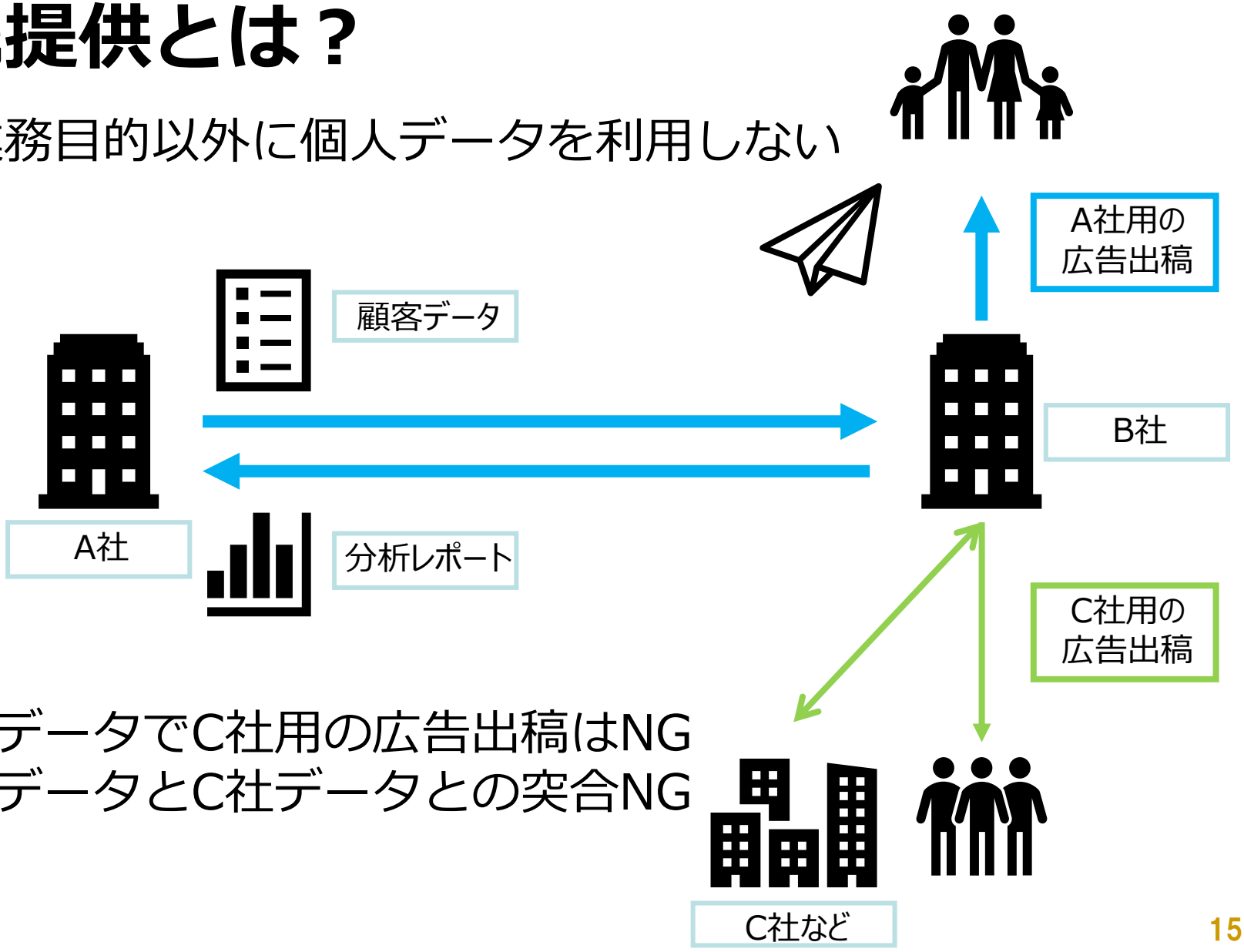
- 適切な委託先の選定
- 委託契約の締結
  - ① 目的外利用の禁止
  - ② 監査条項
- 委託先における個人データの取扱状況の把握

共同利用

- プライバシーポリシーにおける共同利用枠組み
  - ① 共同利用する旨
  - ② 個人データの項目
  - ③ 共同利用者の範囲
  - ④ 共同利用目的
  - ⑤ 管理責任者

委託提供とは？

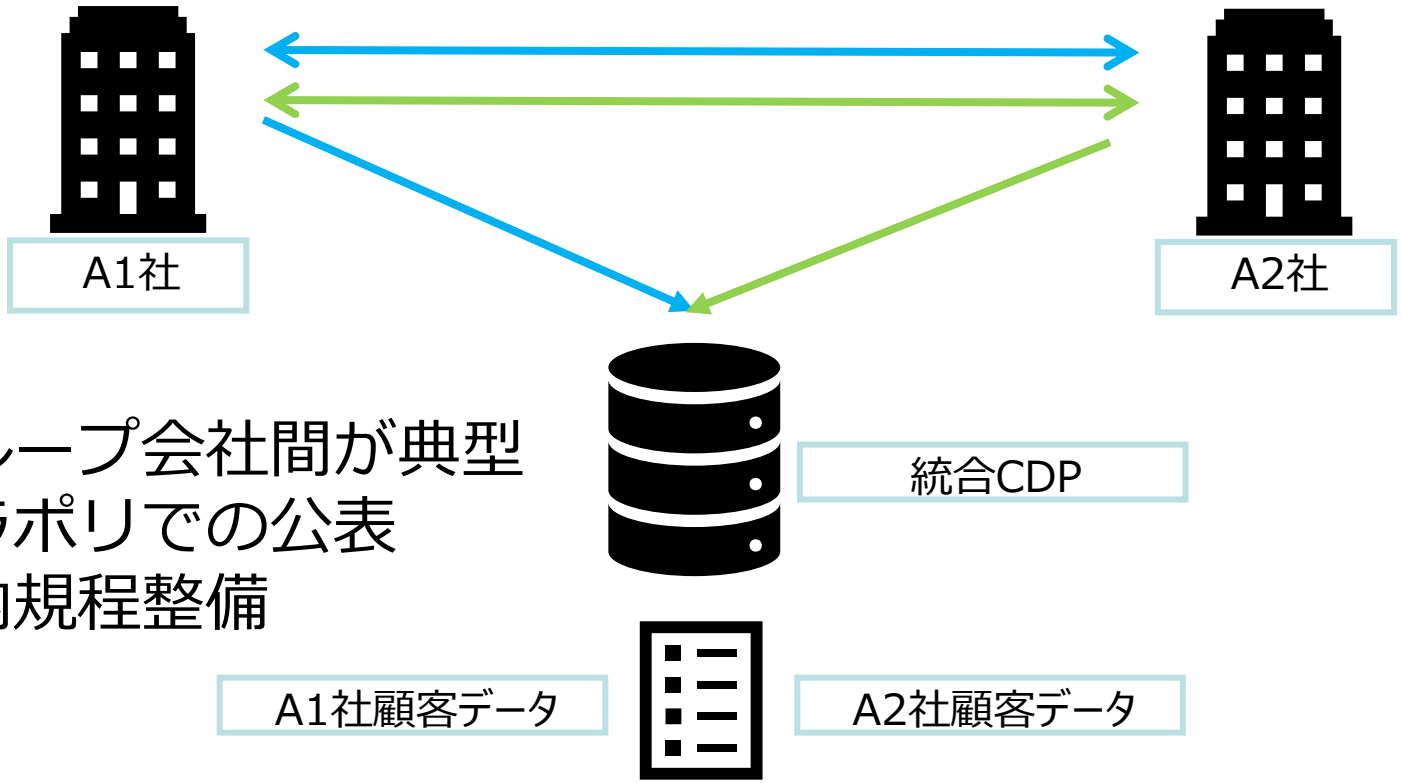
委託業務目的以外に個人データを利用しない



※A社データでC社用の広告出稿はNG
※A社データとC社データとの突合NG

共同利用とは？

社会通念上、共同利用者の範囲や利用目的等が、本人が通常予期し得ると客観的に認められる範囲内でのデータ共有

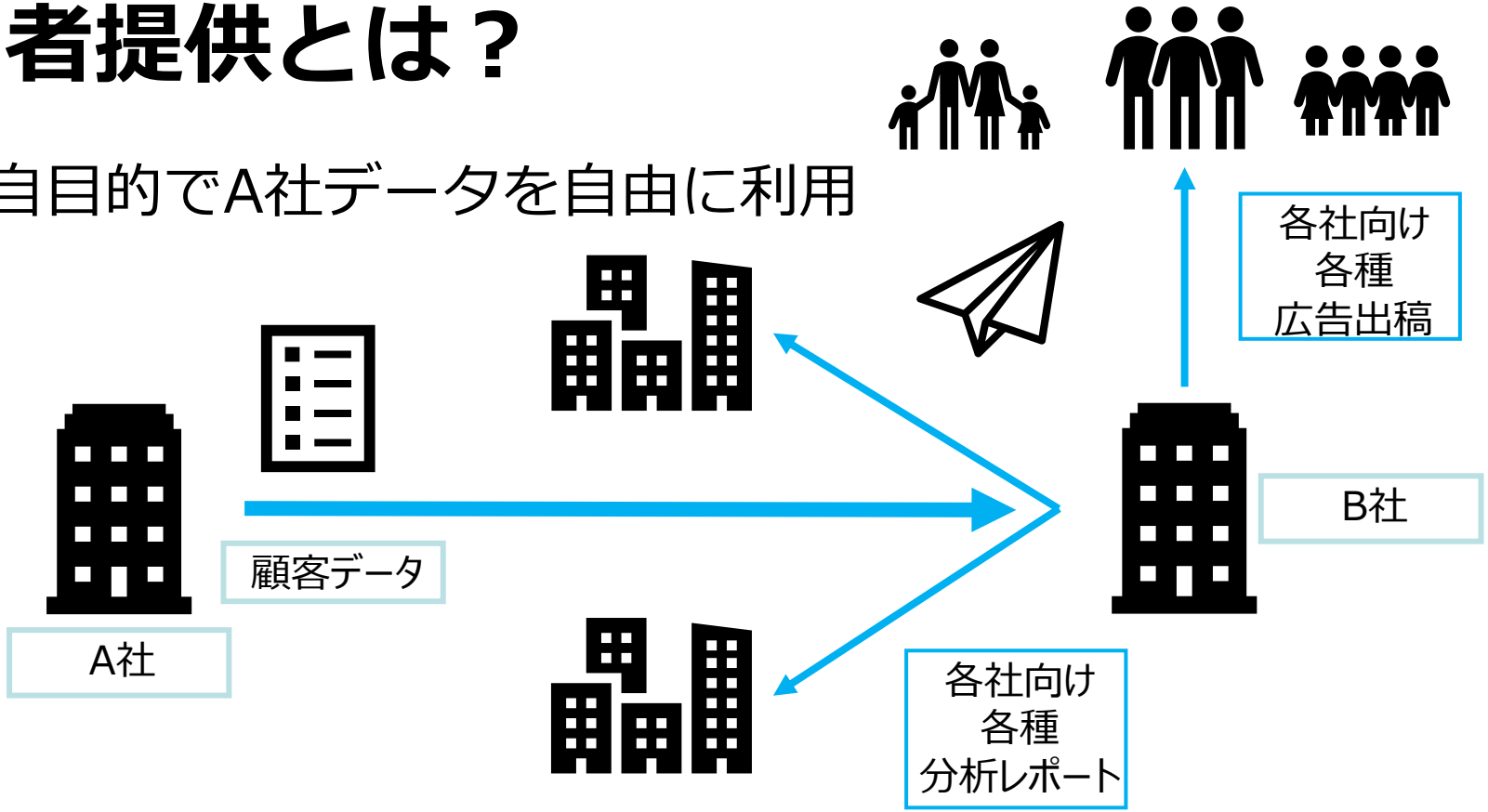


※グループ会社間が典型
※プラポリでの公表
※社内規程整備

③提供フェーズ

第三者提供とは？

B社独自目的でA社データを自由に利用



※提供元で個人を特定できる場合＝個人データの第三者提供

データ提供側	**顧客ID**	**氏名**	**メアド**	**住所**	**POS**	**IDFA**
データ受領側				**顧客ID**	**POS**	**IDFA**

③提供フェーズ

個情法：第三者提供確認記録義務（25条及び26条）

- 個人データの第三者提供にあたっては、提供元・提供先、それぞれが以下の事項を記録する必要がある

※提供側：提供年月日、受領者の特定事項、個人データ項目、本人の特定事項、本人の同意を得ている旨

※受領側：提供年月日、提供者の特定事項、個人データ項目、取得経緯、本人の同意を得ている旨

具体的にどのように行う？

契約における記載＋ログの保存

※なお、第三者提供確認記録の開示対象化の法改正に留意

③提供フェーズ

問題となり得るケース

- 個人データに該当するcookie, IDFA, POSデータを非個人情報と判断し、本人同意を得ることなく第三者提供を行った
- 委託先の独自利用が想定されるのに、本人同意を得ることなく第三者提供を行った

⇒法令違反

・プライバシーポリシーの内容は適切か？
・本人同意取得できているか？
・第三者提供の確認記録義務への対応は？

③提供フェーズ

個情法（提供フェーズ）：外国にある第三者への提供

- 個人データの外国第三者への提供には、①本人同意取得、②提供先国が日本と同水準であると個情委が定めている、③提供先が個情委が定める基準に適合する体制を整備済、のいずれかが必要（委託・共同利用の枠組みの場合含む）

問題となり得るケース

委託先の海外クラウドベンダが、個情委が定める基準に適合する体制を整備していないのに、本人同意を得ることなく、委託に基づき個人データ提供を行った

解決策：データフロー精査・委託先海外ベンダの体制レビュー

「外国第三者提供時の情報提供等」に関する個情法改正

④管理フェーズ

個情法（管理フェーズ）：安全管理措置・委託先の監督

- データセキュリティの確保（漏洩・滅失・き損の防止など）
- 委託先や従業員に対する必要かつ適切な監督

問題となり得るケース

- データセキュリティを確保していないベンダに委託し、委託先から情報漏えいインシデントが発生した
- 委託先ベンダに、委託した業務の遂行に必要な範囲を超えて個人データへのアクセス権限を与えていた

解決策：委託先選定時のアセスメント・委託先管理の見直し

「漏えい等の報告義務の法定」に関する個情法改正

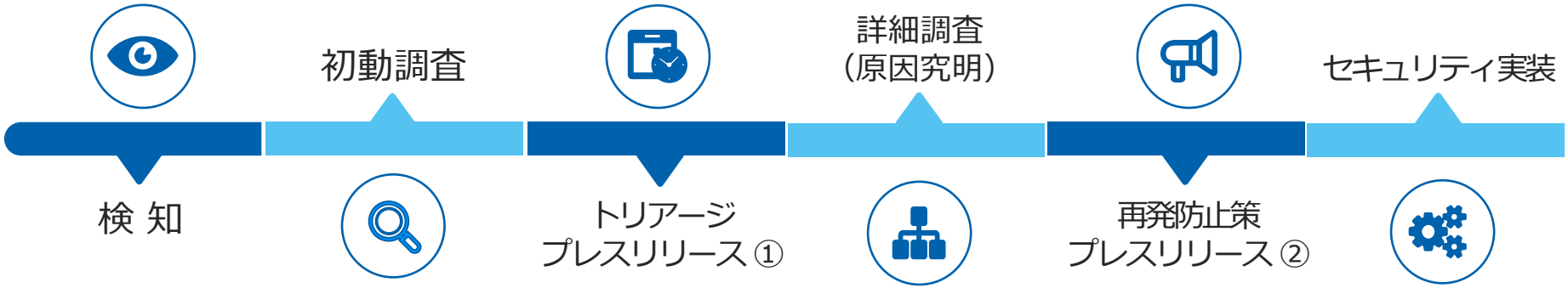
（参考）インシデント発生時の報告・通知・対応

- 個人情報保護委員会等への報告
- 漏えい事案が発覚した場合に講ずべき措置
  - 事業者内部における報告及び被害拡大防止
  - 事実関係の調査及び原因の究明
  - 影響範囲の特定
  - 再発防止策の検討及び実施
  - 影響を受ける可能性のある本人への連絡等
  - 事実関係及び再発防止策等の公表

（参照）個人データの漏えい等の事案が発生した場合等の対応について（平成29年個人情報保護委員会告示第1号）
https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

2022年4月1日以降、法的義務になるので注意

セキュリティ・インシデント対応



初動調査支援

- 初動対応アドバイス

トリアージ、被害拡大防止支援

- トリアージアドバイス
- フォレンジック業者選定
- フォレンジック調査のスコープ決定・ディレクション
- 第三者委員会組成
- 詳細調査実施

再発防止策策定支援

- 組織再編プラン
- セキュリティシステムプラン

セキュリティ実装支援

- 規程類見直し
- インシデント対応フロー見直し
- セキュリティシステム導入

IR・広報お客様対応支援

- 1次プレスリリース(初動版)作成
- 本人通知作成(メール・郵便)
- 記者会見セット・リハ
- 適時開示
- コールセンタのセット
- お客様対応アドバイス(クレーム処理方針)
- 2次プレスリリース(フル版)作成
- 本人通知作成
- 記者会見セット・リハ
- 適時開示

当局対応支援

- 1次報告
  個人情報保護委員会
- IPA・JP-CERT
- サイバー犯罪対策課
- 当局対応
- 2次報告

被害補償対応支援／被害回復支援

- 被害補償対応
- ベンダへの請求
- 刑事告訴

④管理フェーズ

個情法（管理フェーズ）：個人の権利行使対応

「保有個人データ」に関する個人の権利行使への対応が必要

- 保有個人データの利用目的等の公表
- 開示請求
- 訂正・追加・削除請求　※データの内容が事実でない場合
- 利用停止・消去請求　※目的外利用又は不正取得の場合
- 第三者提供の停止請求　※第三者提供規制違反の場合

「利用停止・消去・第三者提供停止請求の拡大」
「開示請求の拡大」に関する個情法改正

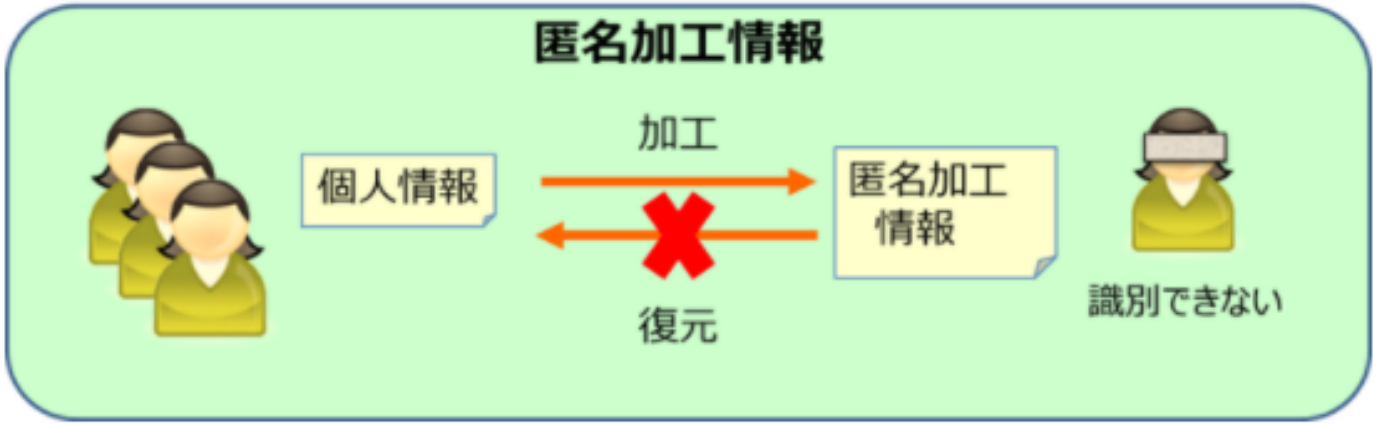
＋公表事項の充実（安全管理措置の内容）

⑤匿名加工情報の活用

匿名加工情報（2条9項, 36条以下）

匿名加工情報とは、特定個人を識別できないように個人情報を加工し、

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



匿名加工情報≠個人情報・統計情報

- 利用目的制限や第三者提供の本人同意等が不要
- 匿名加工情報の作成者・受領者が遵守すべき義務あり

出典：個人情報保護委員会ウェブページ「匿名加工情報制度について」より抜粋
https://www.ppc.go.jp/personalinfo/tokumeikakouInfo/

⑤匿名加工情報の活用

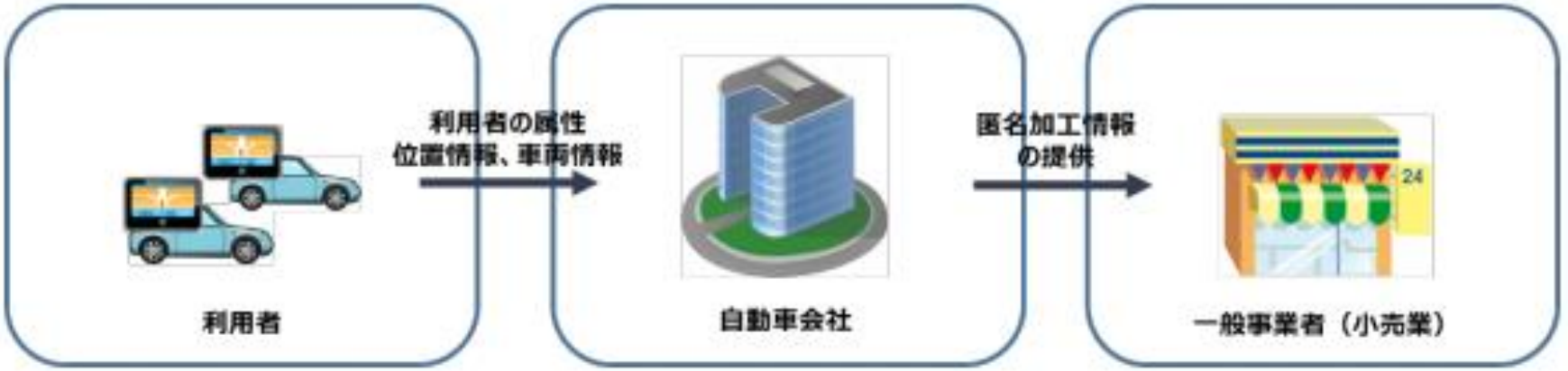
匿名加工情報の活用の実際

7.2.2 移動履歴の事例

1）ユースケース

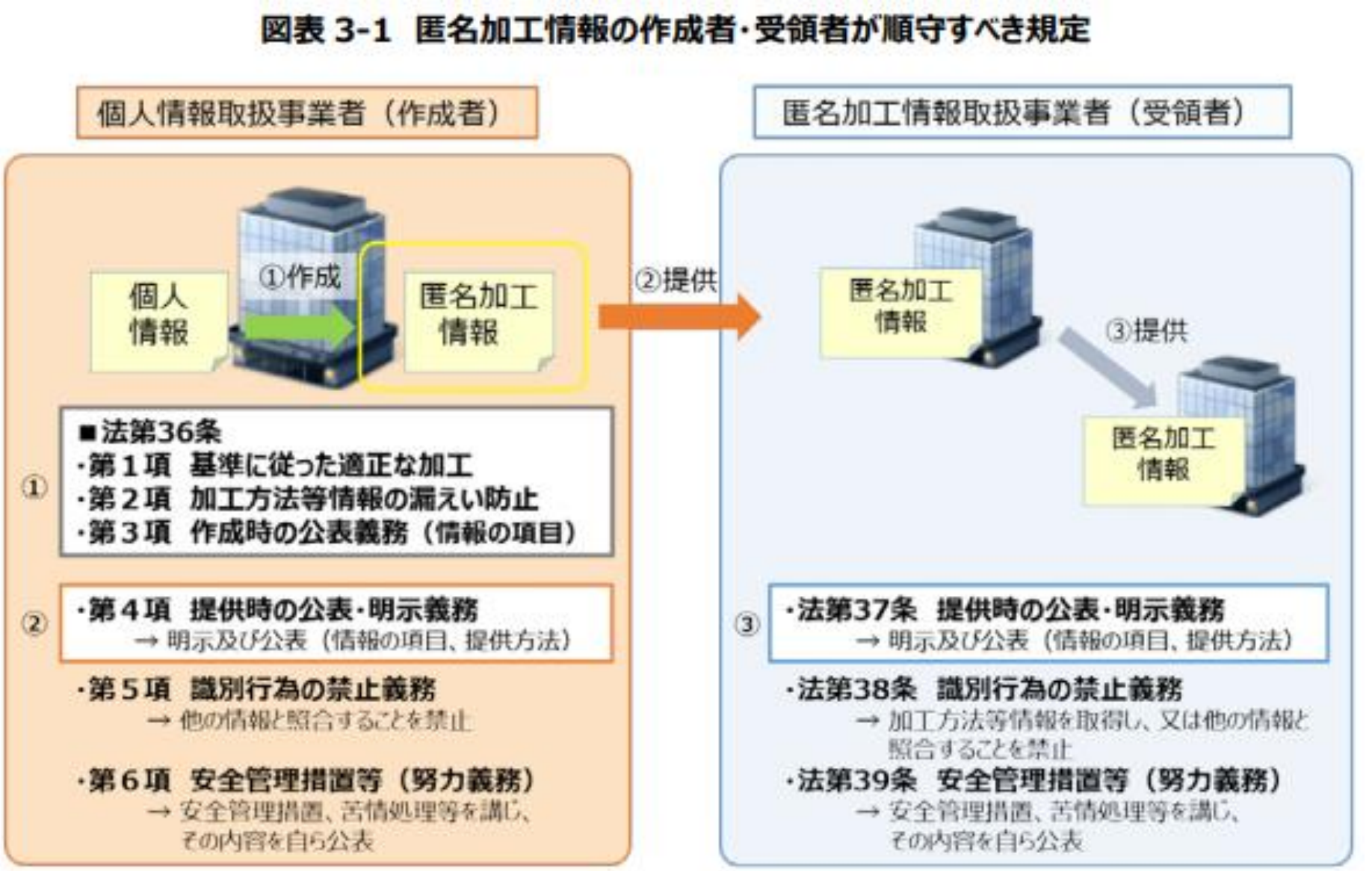
本ユースケースは、自動車会社が保有する移動履歴情報について、匿名加工を行ったうえで、匿名加工情報の枠組みを活用して、一般事業者（小売業）に提供するというものである。一般事業者においては、自動車の移動履歴とその所有者の年代や性別等の基本属性に基づいて、店舗における商品ラインナップの検討や新しい店舗の出店計画に活用することが想定される。

図表 7-16 自動車会社が保有する移動履歴情報を第三者に提供するユースケースのイメージ



出典：「匿名加工情報　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」（個人情報保護委員会事務局、2017年2月）58頁より抜粋 https://www.ppc.go.jp/files/pdf/report_office.pdf

⑤匿名加工情報の活用

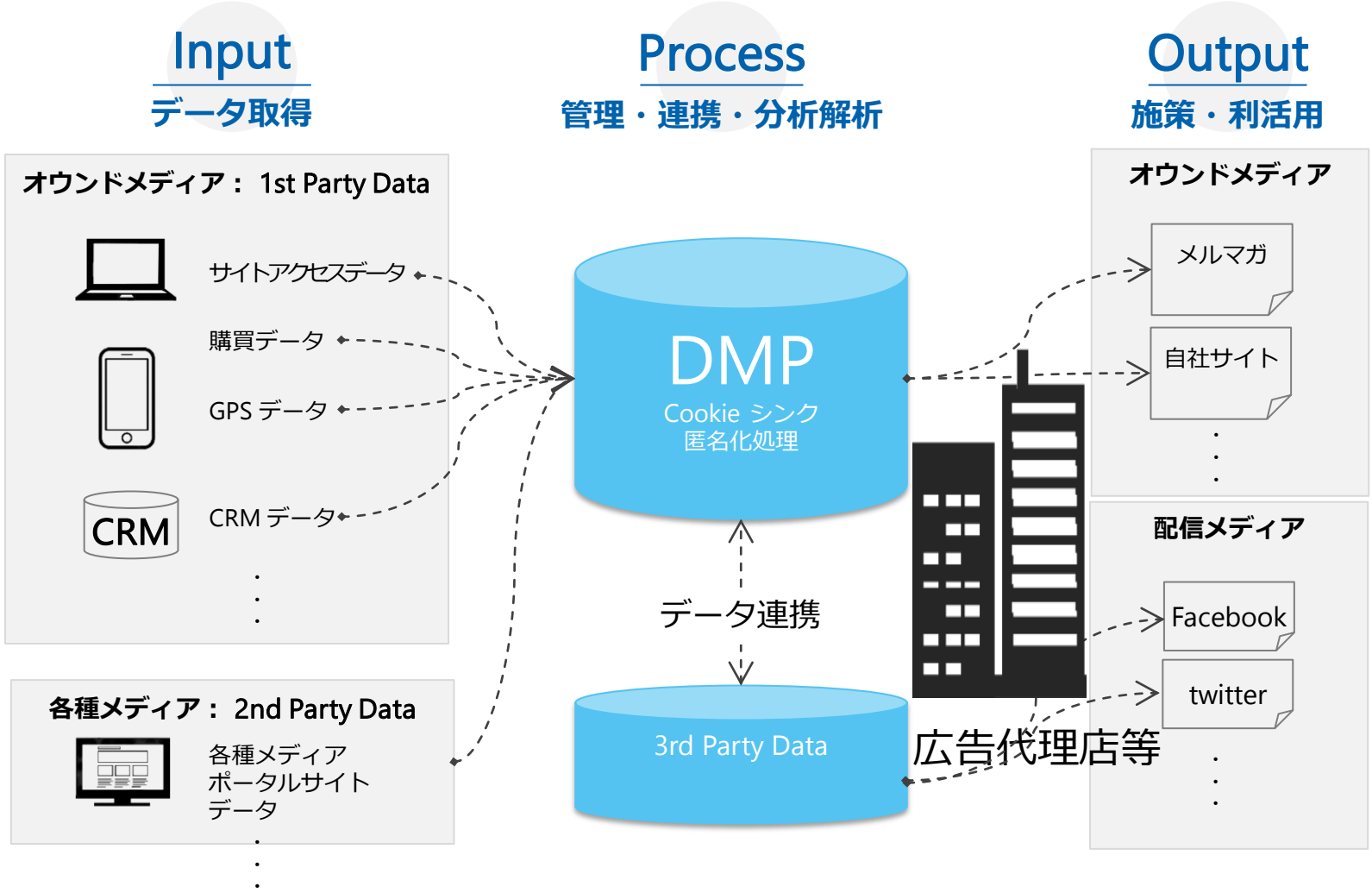


出典：「匿名加工情報　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」（個人情報保護委員会事務局、2017年2月）13頁より抜粋 https://www.ppc.go.jp/files/pdf/report_office.pdf

３．データガバナンス体制整備の進め方

CDP/DMP導入によるデータ利活用

データの取得・管理・利用/提供の３つのフェーズ



CDP/DMP導入の実務課題の整理と対応方法

課題

- データ利用目的・データ提供先を踏まえて、データ取得フェーズにおいて予め適切な対応を行う必要がある
- 個人情報保護法の規制を越えた、プライバシーへの配慮の取り組みが必要である

Todo

- **データの取得・管理・利用・提供の各フェーズを一気通貫でレビューする**
- **法規制・自主ルールの遵守対応を行う**
- **ユーザーの不安感除去のための施策を行う**

データDDの流れ：現状把握とリスクアセスメント

現状把握 データマッピング	● 商流把握 ● 取扱いデータの棚卸し
各規制の洗い出し	● 個人情報保護法及びプライバシー保護規制 ● 海外データ保護規制 ● 監督官庁等のガイドライン
Fit & Gap	● 各規制の要求事項と現状の体制を比較 ● あるべき姿と現状のGapを洗い出し
リスクアセスメント	● Gap事項のリスク評価 ● セキュリティリスクアセスメント

データDDの流れ：改善計画と実装・運用

クリアランス計画	● Fit & Gap分析をベースにGap事項への対応方法を策定 ● 同意取得方法の見直し ● サービス設計の見直し
実装プロセス	● プライバシーポリシーやクッキーポリシーの整備 ● 社内規程・マニュアルの整備 ● データ提供・連携契約の見直し ● システム実装
運用	● 教育 ● 定期監査 ● 法改正対応等の見直し

４．令和２年改正個人情報保護法の概要

令和２年改正個人情報保護法の全体像

① 個人関連情報の第三者提供時の確認記録義務

② 個人の権利の拡大

③ 個人データの漏えい等の報告・通知義務の法定

④ 個人データの越境移転規制の強化

⑤ 不適正利用禁止の明文化

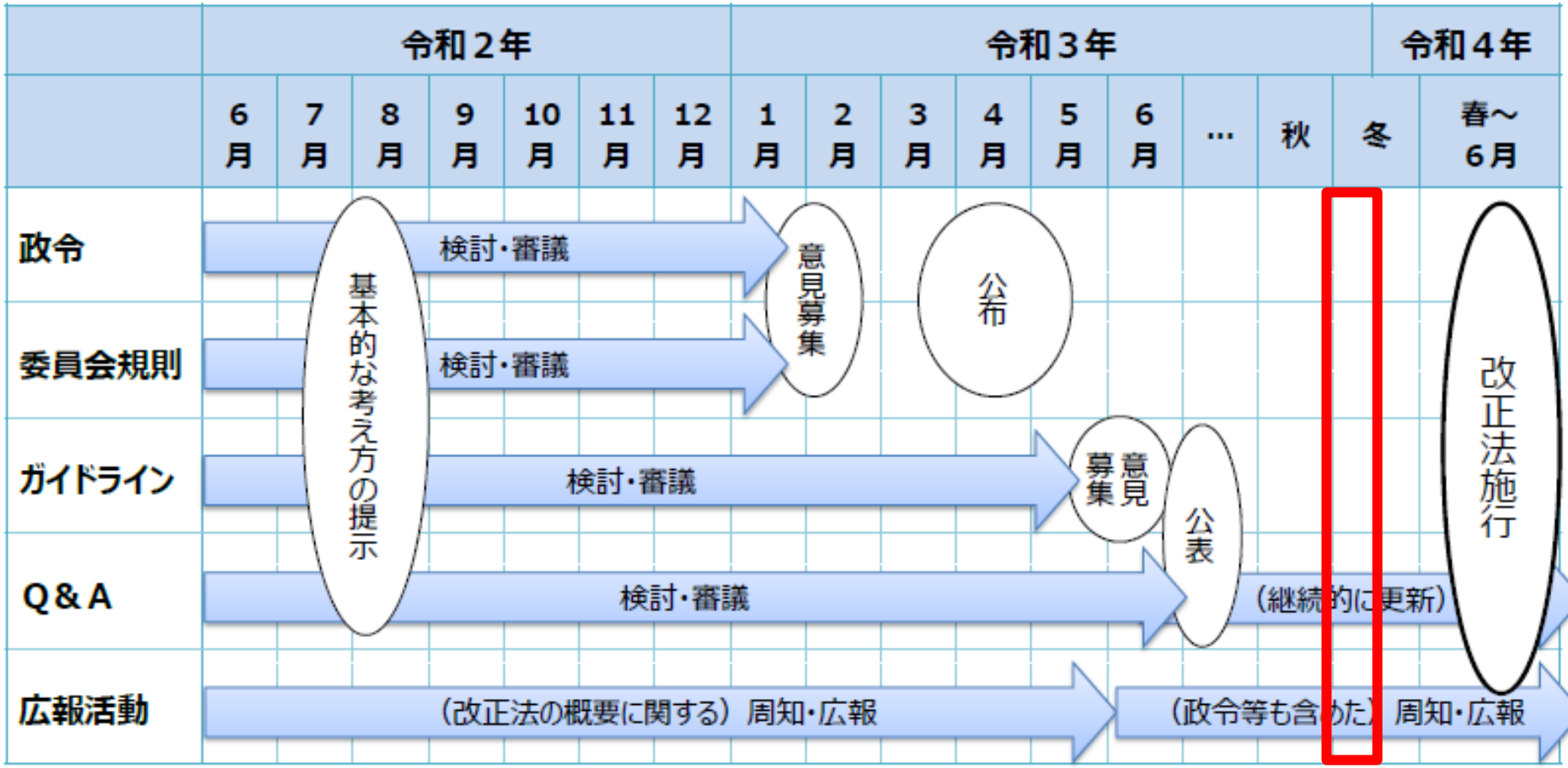
⑥ 仮名加工情報創設とデータ利活用促進

⑦ オプトアウト規制強化

⑧ ペナルティ強化

＋公表事項の充実 (安全管理措置の内容)

令和２年改正個人情報保護法の対応タイムライン



※このほか、個人情報の保護に関する基本方針、認定個人情報保護団体の認定等に関する指針等についての改正も予定。
※上記の表は現時点での大まかな見込みであり、今後の状況によって変わり得る。

出典：個人情報保護委員会「個人情報の保護に関する法律等の一部を改正する法律の成立を受けた個人情報保護委員会の今後の取組（案）について」（令和２年６月１５日）参照
https://www.ppc.go.jp/files/pdf/200615_shiryou1.pdf

令和２年改正個人情報保護法の対応タイムライン

改正法対応として、何時までに、何をやるか？

①2021年3月24日：政令・委員会規則公布

②2021年8月2日：ガイドライン公表

③2021年9月10日：Q&A公表

④2022年4月1日：改正法施行

改正法施行のタイミングで対応できていれば良い

しかし、改正法対応にすぐにでも着手すべきタイミング

TMIのデータ利活用支援メニュー

データの収集

- データマッピング作成
  （散在するデータを収集・集約）
- デジタルトランス
  フォーメーション（DX）支援
  （データ化されていないデータを発掘）
- 個人情報取扱規程など社内規程の整備
- プライバシーポリシーの整備
- クッキーポリシーの整備

データ管理体制

- セキュリティアセスメント
- インシデント対応体制構築支援

データ匿名化処理

- 匿名化処理などリスク
  低減化プラン策定
- 再識別化リスクアセスメント

データの第三者との連携

- データ連携・提供契約の締結
- API 連携ポリシーの策定

データの利用

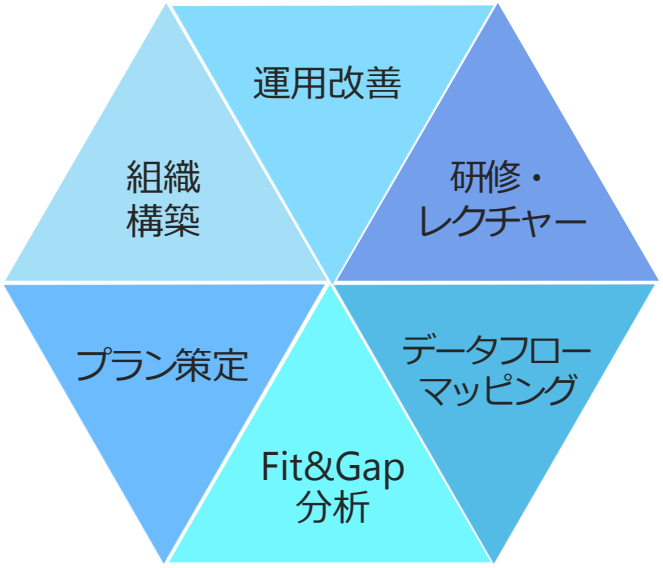
- ターゲティング広告
- セキュアなCRM 施策の検討
- データの第三者への販売支援

メディアの選別

- ブランド（レピュテーション）
  コントロール
  - 不適切なメディアへの掲載を防止
  - ブランドセーフティ
  - アドベリフィケーション
- アドフラウド（広告不正）
  防止対策

TMIのセキュリティ体制構築と支援メニュー

経営責任 / 説明責任



組織構築

- 各種規程の改定
- セキュリティ管理委員会組成
- セキュリティ施策実装
- サイバー保険の導入支援

成果物例：
・各種ポリシー
・各種規程・マニュアル

運用改善

- セキュリティ管理委員会運用
- インシデント発生時の有事対応

成果物例：
セキュリティ管理委員会参加

研修・レクチャー

- プロジェクト当初における経営層レクチャー
- プロジェクト最終における事業部レクチャー

成果物例：レクチャー資料

データフローマッピング

- ビジネスフローマッピング
- データフローマッピング

成果物例：
・ビジネスフローシート
・データマッピングシート

Fit&Gap 分析

- セキュリティアセスメント
- プライバシーインパクトアセスメント

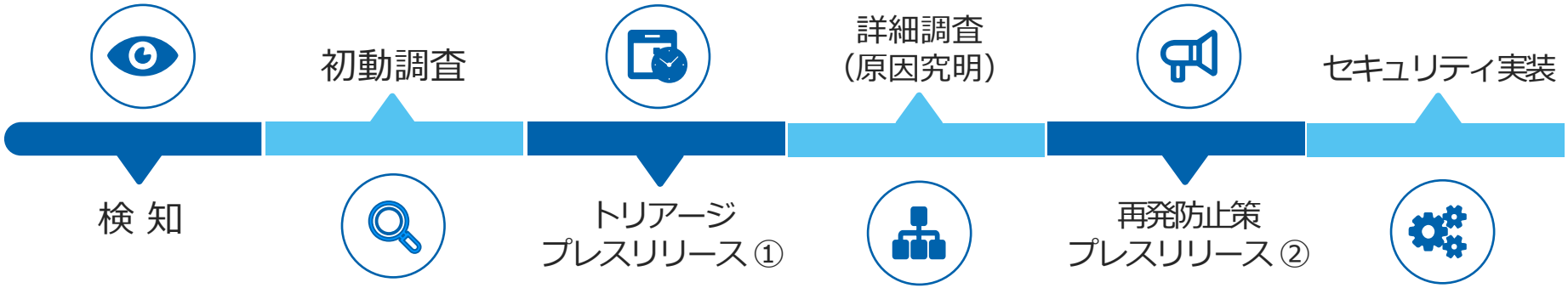
成果物例：Fit&Gap シート

プラン策定

- GAP 事項のクリアランス計画策定

成果物例：
クリアランス計画書

TMIのセキュリティインシデント対応支援メニュー



初動調査支援

- 初動対応アドバイス

トリアージ、被害拡大防止支援

- トリアージアドバイス
- フォレンジック業者選定
- フォレンジック調査のスコープ決定・ディレクション
- 第三者委員会組成
- 詳細調査実施

再発防止策策定支援

- 組織再編プラン
- セキュリティシステムプラン

セキュリティ実装支援

- 規程類見直し
- インシデント対応フロー見直し
- セキュリティシステム導入

IR・広報お客様対応支援

- 1次プレスリリース(初動版)作成
- 本人通知作成(メール・郵便)
- 記者会見セット・リハ
- 適時開示
- コールセンタのセット
- お客様対応アドバイス(クレーム処理方針)
- 2次プレスリリース(フル版)作成
- 本人通知作成
- 記者会見セット・リハ
- 適時開示

当局対応支援

- 1次報告
  個人情報保護委員会
- IPA・JP-CERT
- サイバー犯罪対策課
- 当局対応
- 2次報告

被害補償対応支援／被害回復支援

- 被害補償対応
- ベンダへの請求
- 刑事告訴

ご清聴ありがとうございました