

2023年2月21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～

T M I 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

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



- RIZAPグループ株式会社社外取締役監査等委員、株式会社インティメートマージャー社外取締役、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、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等を歴任。
- 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、グローバル内部通報制度の構築やフォレンジックを含む不正調査対応を含めた、コンプライアンス・ガバナンス領域、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、を主に取扱う。
- ロサンゼルス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。

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. 改正個人情報保護法の改正ポイントまとめ
4. データガバナンス体制整備の進め方

1. スマートシティと個人情報保護法

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。



個人情報保護法：規制の概要

個人情報該当性

取扱いデータが個人情報に該当するのか
要配慮個人情報該当性

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・従業員／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／委託・共同利用の枠組
外国にある第三者への提供

※なお、2022年4月1日に改正個人情報保護法が施行

※個人関連情報の第三者提供時の確認記録義務にも注意

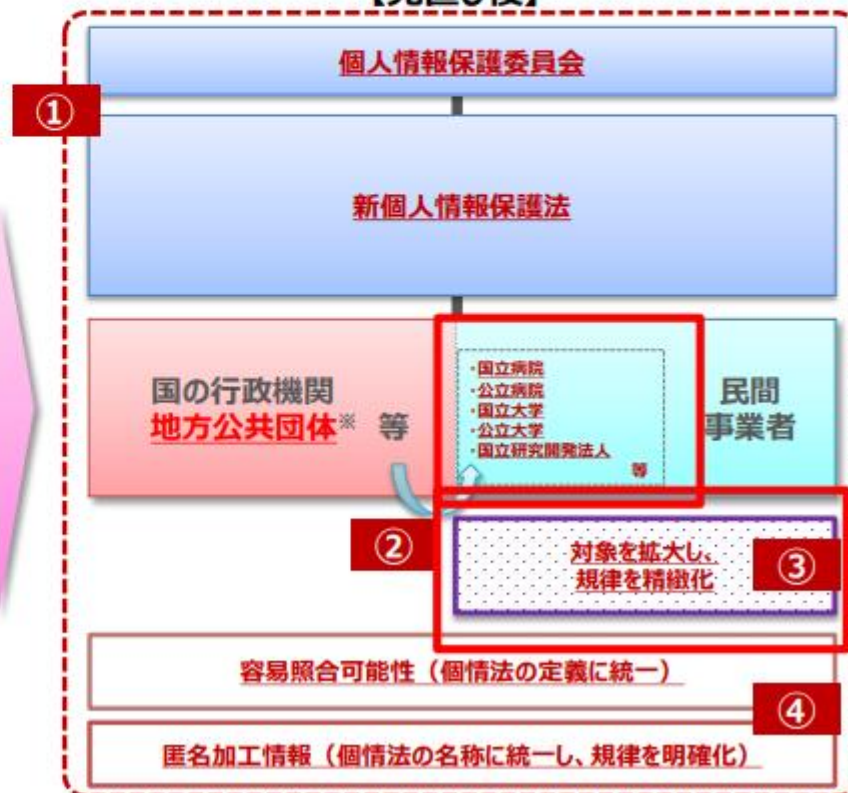
スマートシティと個人情報保護法：令和3年改正

- 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。

【現行】



【見直し後】



2. 個人情報保護法の概要

個情法：個人情報の定義（2条1項及び2項）

生存する個人に関する情報であって、

- ① 特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
- ② 個人識別符号
 - 身体の一部の特徴を変換した符号
 - サービス利用や書類にて対象者毎に割り振られる符号

Cookieは個人情報と認定されるのか？

原則として、単体では個人情報に該当しないが、**会員情報やアカウント登録情報等との連携により個人情報に該当し得る**

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

「特定の個人を識別することができるもの」とは？

- ✓ 氏名が典型例だが、メールアドレスもこれに該当する場合あり
- ✓ 他情報との容易照合性により特定個人が識別なものを含むので、「氏名などと結びつく一切の情報」がこれにあたる

例）：従業員や取引先担当者の氏名とともに取得している一切の情報、どの従業員が使用しているPCであるか一覧表で管理されている場合のPCのネットワークログなど

「個人識別符号」とは？⇒医療業界では生体データに留意

- ✓ 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、マイナンバー、各種保険証等

①個人情報該当性

個人情報法：要配慮個人情報の定義（2条3項）

- 人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報

⇒要配慮個人情報を取得するときは本人の同意が必要

ヘルスケアデータと要配慮個人情報

- 病歴
- 身体障害・知的障害・精神障害等があること
- 健康診断等の検査の結果
- 医師等による指導又は診療・調剤が行われたこと

⇒医療機関のカルテ、保険薬局の処方箋、健保のレセプト等

※ウェアラブルデバイスによって収集したバイタルデータは含まない。

②取得フェーズ

個人情報（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」

※取得した個人情報と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

個人情報法（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

例外

- ① 法令に基づく場合
- ② 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
- ③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
- ④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- ⑤ 当該情報が、本人、国の機関、地方公共団体、第76条第1項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合
- ⑥ **目視又は撮影により、その外形上明らかな要配慮個人情報を取得する場合**
- ⑦ **法第23条第5項各号に掲げる場合において、個人データである要配慮個人情報の提供を受けるとき**

個人情報（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

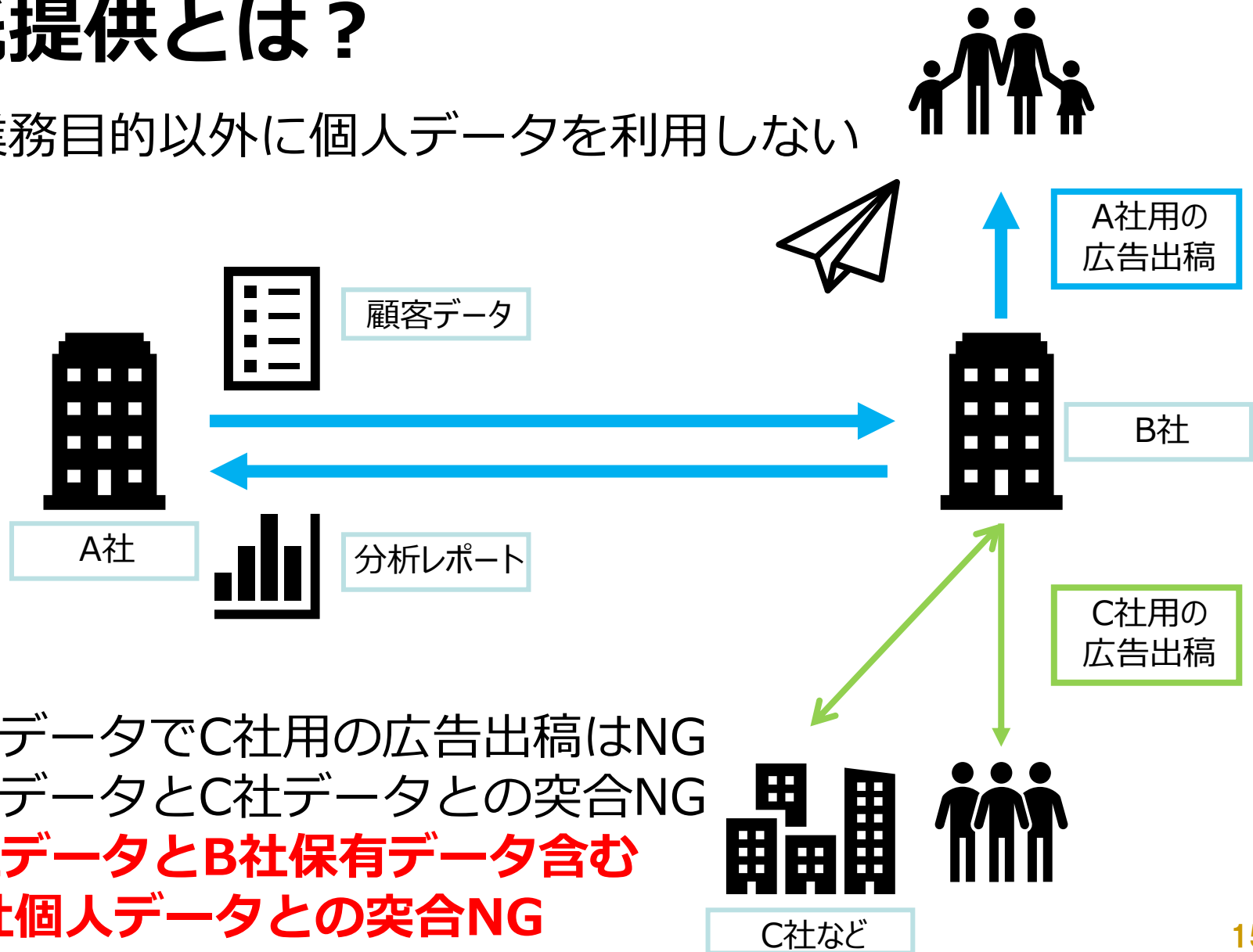
- 適切な委託先の選定
- 委託契約の締結
 - ① 目的外利用の禁止
 - ② 監査条項
- 委託先における個人データの取扱状況の把握

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



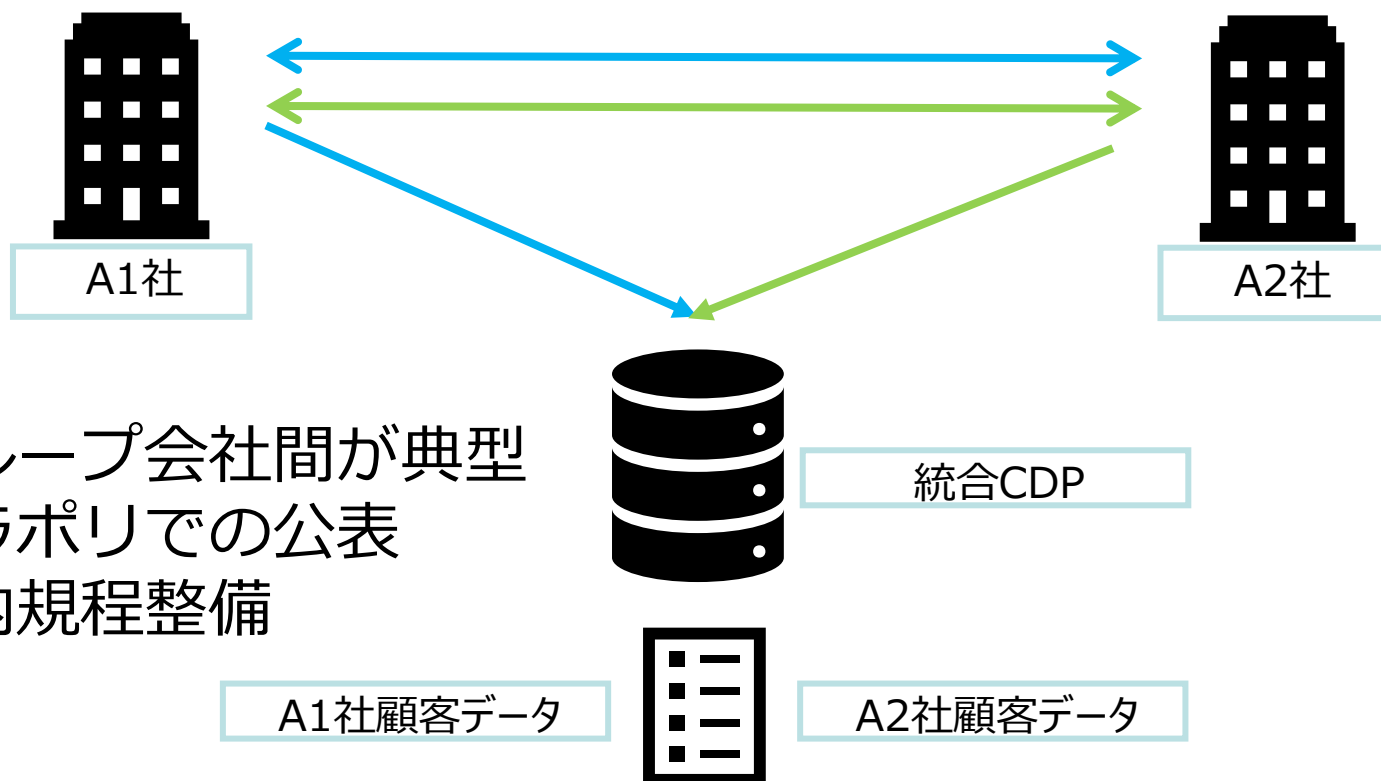
※ A社データでC社用の広告出稿はNG

※ A社データとC社データとの突合NG

※ **A社データとB社保有データ含む
他社個人データとの突合NG**

共同利用とは？

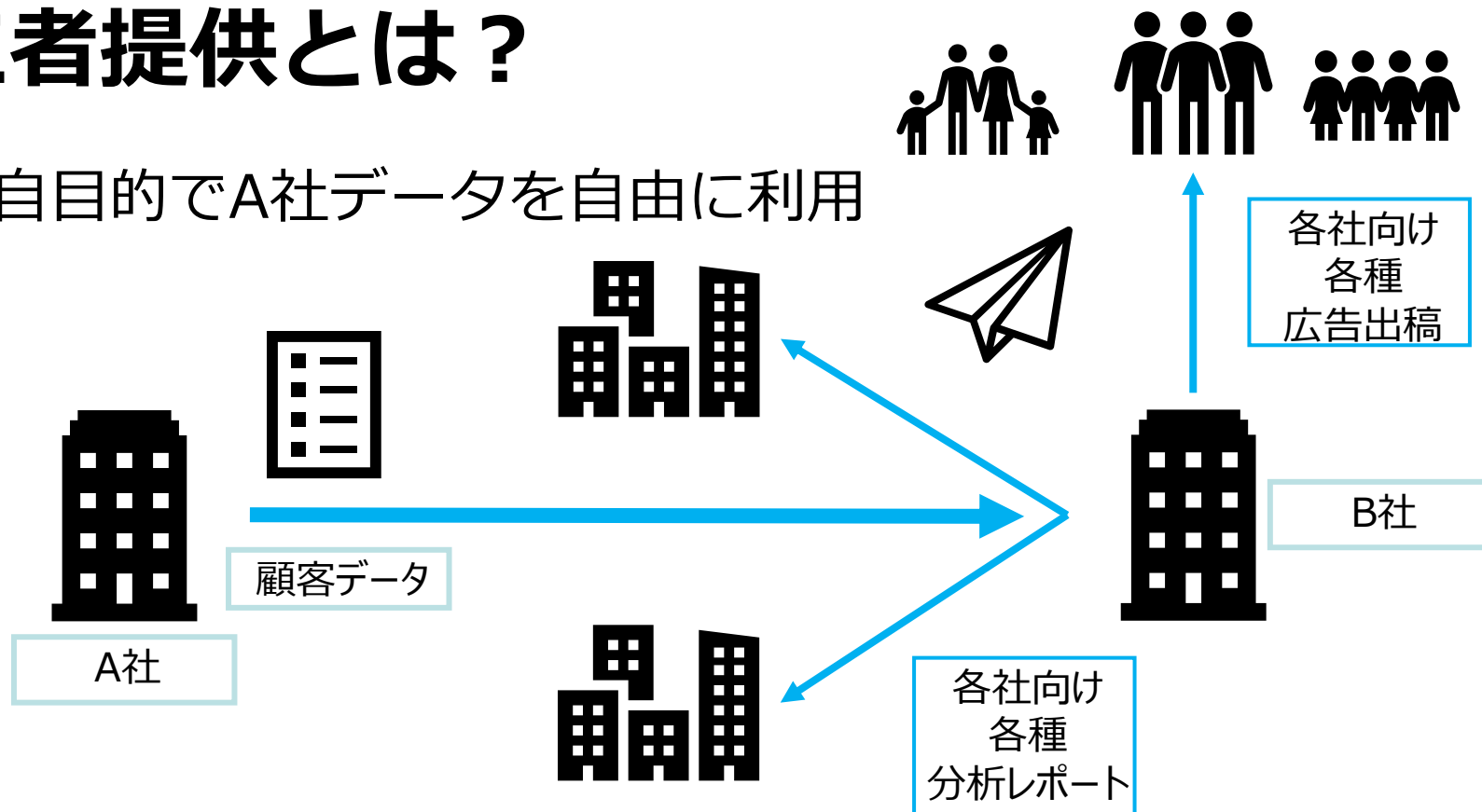
社会通念上、共同利用者の範囲や利用目的等が、本人が通常
予期し得ると客観的に認められる範囲内でのデータ共有



- ※ グループ会社間が典型
- ※ プラポリでの公表
- ※ 社内規程整備

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
------	-----	------

個人情報：第三者提供確認記録義務

- 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

問題となり得るケース

- 個人データに該当する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？

個人情報法（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人情報委が定めている、③提供先が個人情報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、個人情報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」に関する個人情報改正

個人情報法（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」に関する個人情報改正

個人情報法（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」に関する個人情報改正

個人情報（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」

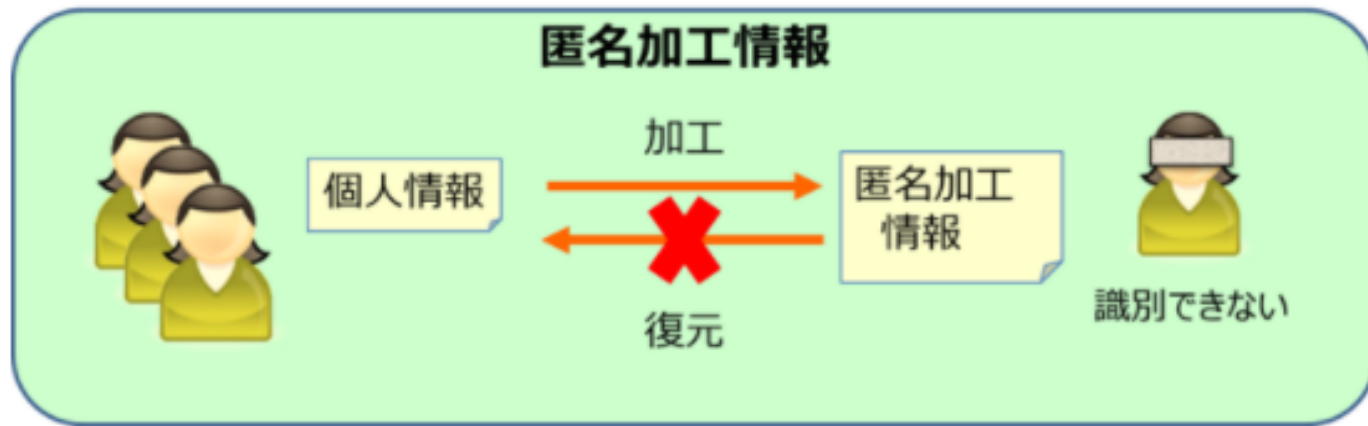
「開示請求の拡大」に関する個人情報改正

+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

Q15-2 統計情報と匿名加工情報の違いは何ですか。

統計情報は、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計等して得られる情報であり、一般に、特定の個人との対応関係が排斥されているため、「個人情報」に該当しないものです。他方、**匿名加工情報**は、法第43条第1項に基づき、施行規則第34条各号で定める基準に従い加工したものであり、**例えば、ある一人の人物の購買履歴や移動履歴等の情報など、個人単位の「個人に関する情報」を含むもの**です。

→適切に匿名化されていても個人単位の情報であれば匿名加工情報

Q15-6 個人情報を、安全管理措置の一環等のためにマスキング等によって匿名化した場合、匿名加工情報として取り扱う必要がありますか。

匿名加工情報を作成するためには、匿名加工情報作成の意図を持って、法第43条第1項に基づき、施行規則第34条各号で定める基準に従い加工する必要があります。したがって、**匿名加工情報の加工基準に基づかずに、個人情報を安全管理措置の一環等としてマスキング等によって匿名化した場合には、匿名加工情報としては扱われません**。また、客観的に匿名加工情報の加工基準に沿った加工がなされている場合であっても、**引き続き個人情報の取扱いに係る規律が適用されるものとして取り扱う意図で加工された個人に関する情報については、匿名加工情報の取扱いに係る規律は適用されません**。

→個人単位の情報適切に匿名化されていない場合には個人情報

出典：個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン に関するQ & A」より抜粋

https://www.ppc.go.jp/personalinfo/faq/APPI_QA/

⑤ 匿名加工情報の活用

Q14-1 匿名加工情報と仮名加工情報の違いは何ですか。

匿名加工情報は、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**（法第2条第6項）です。

「個人情報」（法第2条第1項）に該当せず、本人の同意を得ずに第三者に提供することが可能です（匿名加工情報の取扱いに係る義務等については、ガイドライン（仮名加工情報・匿名加工情報編）3-2参照）。

これに対し、仮名加工情報は、**他の情報と照合しない限り特定の個人を識別できないように加工した個人に関する情報**（法第2条第5項）であり、**仮名加工情報を作成した個人情報取扱事業者においては、通常、当該仮名加工情報の作成の元となった個人情報や当該仮名加工情報に係る削除情報等を保有していると考えられることから、原則として「個人情報」（法第2条第1項）に該当するものです。**

変更前の利用目的と関連性を有すると合理的に認められる範囲を超える利用目的の変更が可能です（法第41条第9項）、**原則として第三者への提供が禁止されています**（法第41条第6項）（仮名加工情報の取扱いに係る義務等については、ガイドライン（仮名加工情報・匿名加工情報編）2-2参照）。

→復元可能性の有無が異なる（復元することができない＝匿名加工情報）

活用例

- 医療機関が保有する医療情報を活用した創薬・臨床分野の発展
- カーナビ等から収集される走行位置履歴等のプローブ情報を活用したより精緻な渋滞予測や天候情報の提供等

【例】医療情報の例



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/>

3. 改正個人情報保護法の 改正ポイントまとめ

- ① 個人関連情報の第三者提供時の確認記録義務
- ② 個人データの越境移転規制の強化
- ③ 個人データの漏えい等の報告・通知義務
- ④ 個人の権利の拡大
- ⑤ 個人データの安全管理措置に係る公表
- ⑥ 不適正利用禁止の明文化
- ⑦ 仮名加工情報創設とデータ利活用促進
- ⑧ オプトアウト規制強化
- ⑨ ペナルティ強化

個人関連情報とは？（改正法第2条第7項）

生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの

<個人関連情報に該当する事例>

- Cookie 等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴
- メールアドレスに結び付いた、ある個人の年齢・性別・家族構成等
- ある個人の商品購買履歴・サービス利用履歴
- ある個人の位置情報
- ある個人の興味・関心を示す情報

⇒現状、非個人情報と取扱っているもののうち、統計情報ではないものが該当する。

新設

個人関連情報

個人関連情報とは、生存する個人に関する情報で、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの。

個人関連情報の第三者提供規制

例えば*...

- Cookie等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴
 - ある個人の商品購買履歴やサービス利用履歴
 - ある個人の位置情報
- *特定の個人を識別できる蓄積された位置情報等は個人関連情報ではなく、個人情報に該当。

提供元

A社

- A社では、誰の個人データかわからない

提供

B社

提供先

- B社では、A社とID等を共有
- B社では、ID等に基づいて個人データを保有

B社において個人データとすることが想定される場合は原則本人の同意が必要

A社から提供されたデータをID等を使って自社内の個人データと結合

個人データ

氏名	年齢	ID等
山田 郎	55歳	1
佐藤次郎	29歳	2
伊藤三郎	45歳	3

個人データ

氏名	年齢	ID等	購買履歴
山田 郎	55歳	1	ミルクティ、おにぎり
佐藤次郎	29歳	2	紅茶、サンドイッチ
伊藤三郎	45歳	3	スツ、ネクタイ

個人関連情報

ID等	購買履歴
1	ミルクティ、おにぎり
2	紅茶、サンドイッチ
3	スツ、ネクタイ

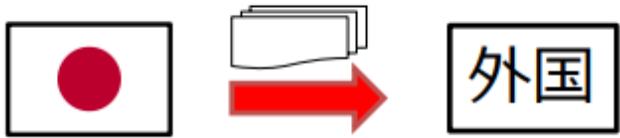
MEMO

個人関連情報を第三者に提供する場合、提供先(B社)において個人データとして取得することが想定されるときは、提供元(A社)に第三者提供に関して本人同意が得られていることの確認を義務付け。

※本人同意を得るのは、基本的に提供先(B社)

②個人データの越境移転規制の強化

- 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取扱いに関する本人への情報提供の充実等を求める。

改正前	改正後
 <p>外国にある第三者に個人データを提供できる要件</p> <ul style="list-style-type: none">本人の同意基準に適合する体制を整備した事業者我が国と同等の水準国（EU、英国）	<p>各要件に基づく移転時、それぞれ以下を義務付け</p> <div><p>本人からの<u>同意取得時</u>に、以下の情報を提供（§28②）</p><ul style="list-style-type: none">・ 移転先の<u>所在国の名称</u>・ 当該<u>外国における個人情報の保護に関する制度</u>・ 移転先が講ずる<u>個人情報の保護のための措置</u></div> <div><p>① 移転元に対し以下の必要な措置を求める</p><ul style="list-style-type: none">・ 移転先における<u>適正な取扱いの実施状況等の定期的な確認</u>・ 移転先における適正な取扱いに<u>問題が生じた場合の対応</u><p>+</p><p>② <u>本人の求めに応じて</u>必要な措置等に関する情報を提供（§28③）</p></div>

出典：個人情報保護委員会「令和2年改正個人情報保護法について」令和4年3月

<https://www.ppc.go.jp/files/pdf/r2kaiseihou.pdf>

③個人データの漏えい等の報告・通知義務

漏えい・滅失・毀損等の報告及び本人通知の義務化

旧法 努力義務（ただし金融分野では義務規定）

改正法 法律上の義務（改正法第26条）

個人情報保護委員会への報告（改正法第26条第1項）

- ①漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって
- ②個人の権利利益を害するおそれ大きいものとして
個人情報保護委員会規則で定めるものが生じたときは、
- ③**個人情報保護委員会規則で定めるところにより、報告**

本人への通知（改正法第26条第2項）

報告対象となる場合、本人に通知しなければならない

③個人データの漏えい等の報告・通知義務

①個人情報報告の対象

規則第7条（個人の権利利益を害するおそれ大きいもの）

法第26条第1項本文の個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

- ① 要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第一項において同じ。）の漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態
例）従業員の健康診断等の結果の漏えい
- ② 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
例）クレジットカード情報、決済サービスのLogin ID/パスワードの漏えい
- ③ 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
例）不正アクセス、ランサムウェアによる暗号化、内部不正による情報盗取
- ④ 個人データに係る本人の数が1000人を超える漏えい等が発生し、又は発生したおそれがある事態
例）システムの設定ミス等により個人データが閲覧可能な状態になった

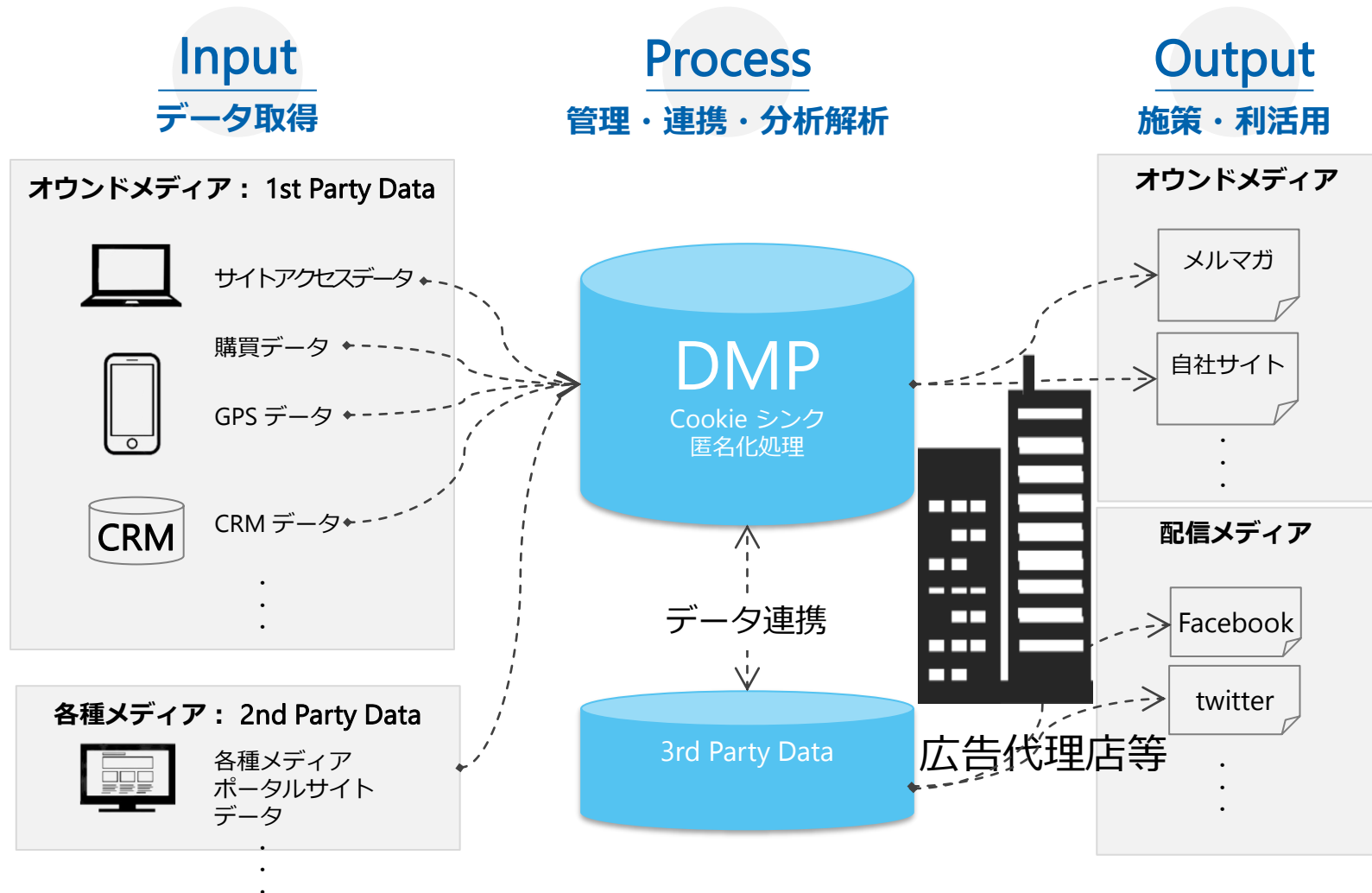
個人データの漏えい事故が起こったら？

- 個人情報保護委員会への速報（3日～5日以内）
- 個人情報保護委員会への確報（30日or60日以内）
- 本人通知（事態の状況に応じて速やかに）

⇒事案検知後、直ちに法務相談が必要

4. データガバナンス体制整備の進め方

データの取得・管理・利用/提供の3つのフェーズ



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
- 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



To do

- **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**

プライバシーガバナンス体制の構築プロセス

チーム 組成

- 企画
- メンバ
選定
- PJ
計画

データ マッピング

- 商流把握
- 取扱いデータの
棚卸
- データフローの
可視化

アセスメント

- 各規制の洗い出し
 - 遵守すべき規
制その他要求
事項の整理
- Fit & Gap
 - 現状体制とあ
るべき姿との
Gapを洗い出
し
- リスクへの対応
計画
 - Gapへの対応
策を議論・決
定

実装プロセス

- 各種規程類の整備
 - ポリシー
 - 規程
 - マニュアル
 - チェックリス
ト
 - 契約等
- 情報漏えいインシ
デント対応体制の
整備
 - 対応フロー化
- 自社の取組の
公表等
 - 対外説明ド
キュメント

継続 運用

- 教育
- 定期
監査
- 法改正
対応

ご清聴ありがとうございました



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

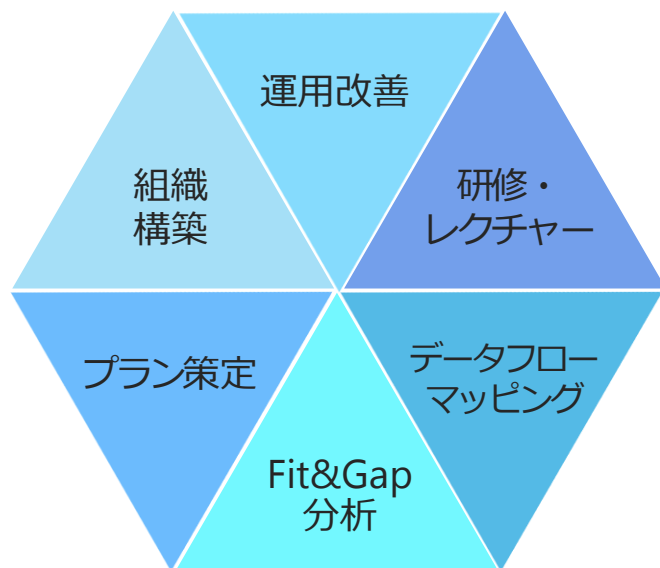


- ✓ ターゲティング広告
- ✓ セキュアなCRM 施策の検討
- ✓ データの第三者への販売支援

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

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

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

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

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

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

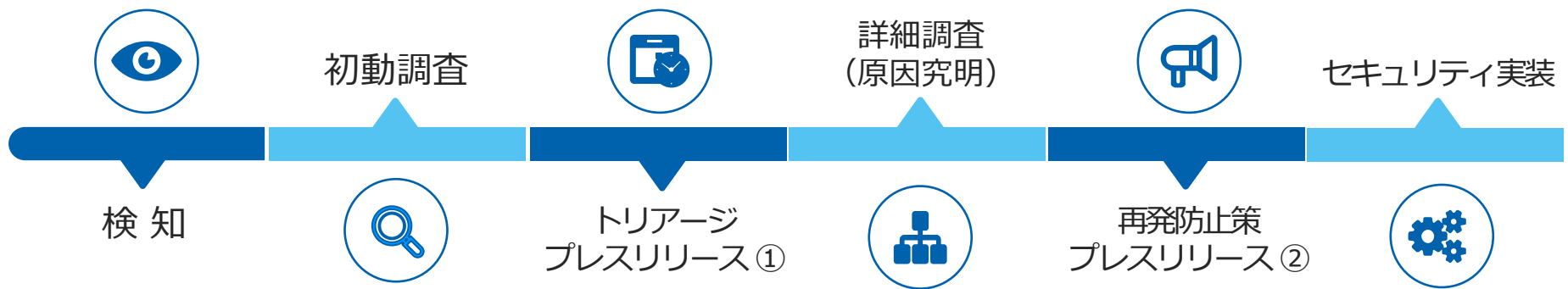
プラン策定

- ✓ 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 トリアージ、被害拡大防止支援 再発防止策策定支援 セキュリティ実装支援

初動対応アドバイス

- ✓ 初動対応アドバイス

- ✓ 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

- ✓ 組織再編プラン
- ✓ セキュリティシステムプラン

- ✓ 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