日本システム監査人協会 近畿支部 第163回定例研究会
ＩＳＡＣＡ 大阪支部 12月度特別講演会

DAIICHI LAW OFFICE, P.C.
弁護士法人 第一法律事務所

「個人情報を巡る最新動向と企業に与える影響」
～改正個人情報保護法の施行に備えて～

弁護士・公認システム監査人
福　本　洋　一

1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 改正の沿革

2005／4	個人情報の保護に関する法律の全面施行
2013／6	パーソナルデータに関する検討会の設置
2014／6	パーソナルデータの利活用に関する制度改正大綱の策定
2015/9	個人情報の保護に関する法律の改正法が成立・公布
2016／1	個人情報の保護に関する法律の改正法の一部施行 （所管が消費者庁から個人情報保護委員会へ）
2016／10	改正個人情報保護法に基づく政令及び委員会規則を公示
2016／11	個人情報の保護に関する法律についてのガイドラインを公表
2017／春	個人情報の保護に関する法律の改正法が全面施行

個人情報保護法（全面施行版）　http://www.ppc.go.jp/files/pdf/personal_law.pdf

2 改正の背景

ビッグデータ事業者、名簿屋・名簿を購入する事業者を除く
一般の中小事業者にとって、今回の新制度の影響は軽微

大手交通系企業のICカードの乗降データ提供

- 個人情報の定義の明確化
- 匿名加工情報

大手教育出版系企業の個人情報大量流出事案

- トレーサビリティの確保
- オプトアウト規定の厳格化
- 個人情報データベース等提供罪

3 主な改正項目

対象範囲	① 個人情報の定義の明確化	2①②
	② 小規模取扱事業者の特例の廃止	2⑤
取得	③ 要配慮個人情報（いわゆる機微情報）	2③,17②
	④ トレーサビリティの確保（受領側）	2⑤
利用	⑤ 利用目的の変更要件の緩和	15②
	⑥ 匿名加工情報に関する加工方法や取扱い	2⑨⑩
提供	④ トレーサビリティの確保（提供側）	25,26
	⑦ 外国にある第三者への個人データの提供制限	24
	⑧ オプトアウト規定の厳格化	23②～④
	⑨ 個人情報データベース等提供罪	83
開示	⑩ 開示等請求権の明確化	28～34
その他	⑪ 個人情報保護委員会の新設及びその権限	40～
	⑫ 国境を越えた適用と外国執行当局への情報提供	75,78

※ 資料内の番号は改正法の全面施行後の条文番号を示す

1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 個人情報の定義の明確化

個人情報

生存する個人に関する情報であって、

⑴ 当該情報に含まれる氏名、生年月日その他の記述等により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でき、それにより特定の個人を識別することができるものを含む）

⑵ 個人識別符号（顔認識データ・指紋認識データ等／旅券番号・免許証番号・基礎年金番号・保険証番号・マイナンバー等）が含まれるもの（※ 容易照合性がなくても該当する点に留意）

個人データ

個人情報データベース等を構成する個人情報

保有個人データ

自らが開示、訂正、削除等の権限を有する個人データ
（６月以内に消去することとなるものを除く。）

2 小規模取扱事業者の特例の廃止

個人情報取扱事業者（２⑤）

・個人情報データベース等を事業の用に供している者のうち、国の機関・地方公共団体等を除いた者

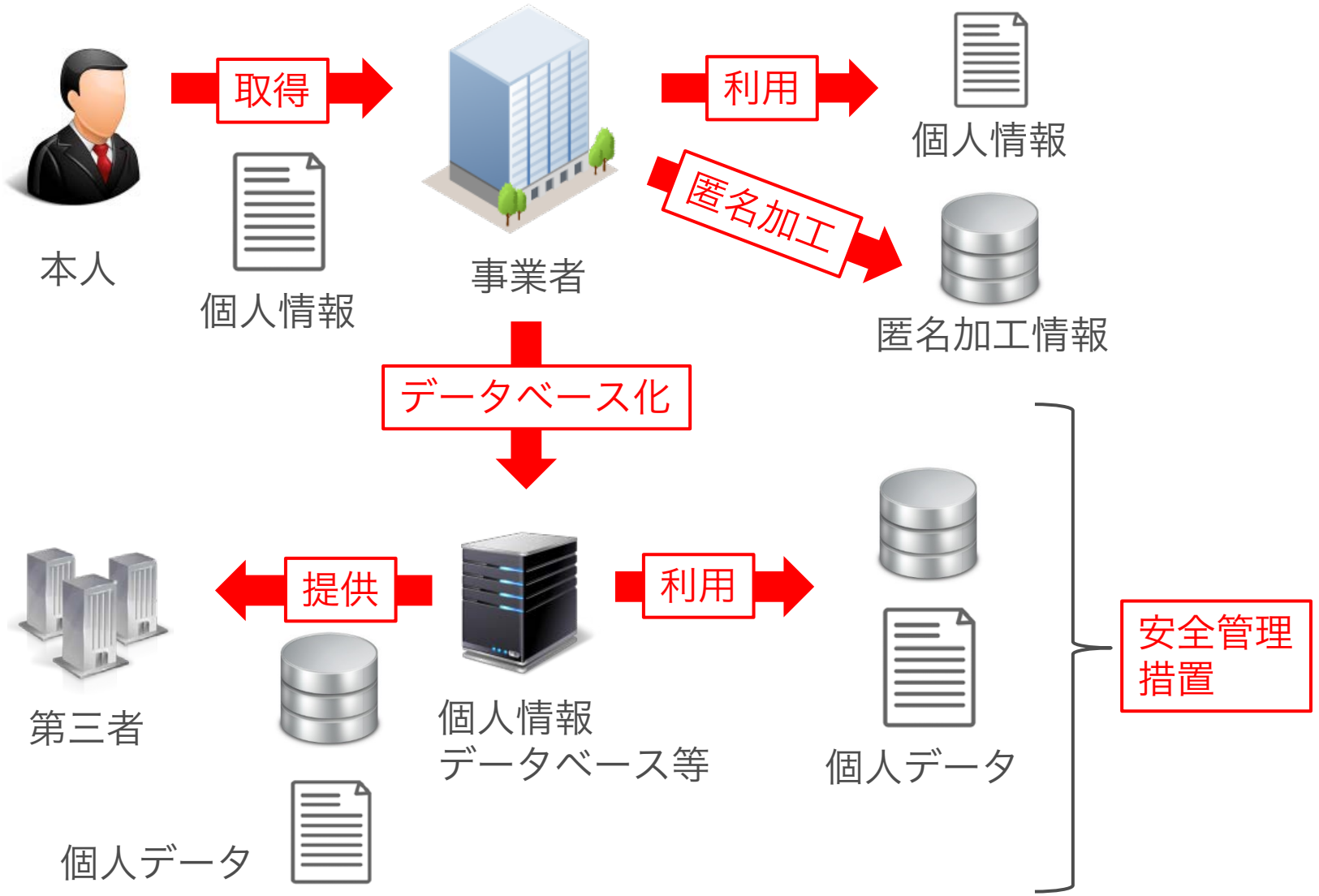
小規模取扱事業者の特例が廃止

・個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６か月以内のいずれの日においても5,000を超えない者

⬇

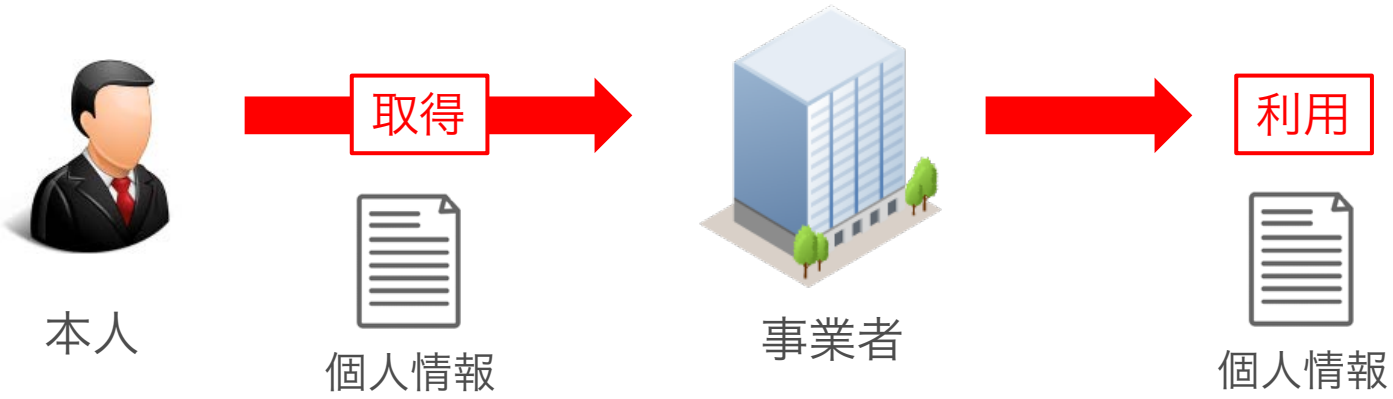
新たに個人情報取扱事業者としての情報管理体制を構築

3 個人情報の管理フロー



1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 取得・利用段階における法規制



❶ 利用目的の特定(15)・利用目的による制限(16)

❷ 適正な取得(17)

・偽りその他不正の手段による取得の禁止

・要配慮個人情報の取得制限(17②)

❸ 取得に際しての利用目的の通知等(18)

❹ トレーサビリティの確保（個人データの受領側）(26)

2 利用目的の変更に対する制限の緩和

・個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と~~相当の~~関連性を有すると合理的に認められる範囲を超えて行ってはならない（15②「相当の」を削除）

・経産分野GL：
変更後の利用目的が変更前の利用目的からみて「社会通念上、本人が想定することが困難でないと認められる範囲内」で変更は可能

・PPCのGL：
「社会通念上、本人が通常予期し得る限度と客観的に認められる範囲内」
＝ 一般人を基準として、当初特定した利用目的とどの程度の関連性を有するかを総合的に勘案して判断

3 要配慮個人情報

要配慮個人情報（2③）

・不当な差別や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次の①から⑪までの記述等が含まれる個人情報（いわゆる機微情報）

① 人種（国籍ではない）

② 信条（思想・信仰も）

③ 社会的身分（職業的地位や学歴は含まない）

④ 病歴（統合失調症等）

⑤ 犯罪の経歴

⑥ 犯罪により害を被った事実

⑦ 心身の機能の障害があること

⑧ 医師等による健康診断等の結果

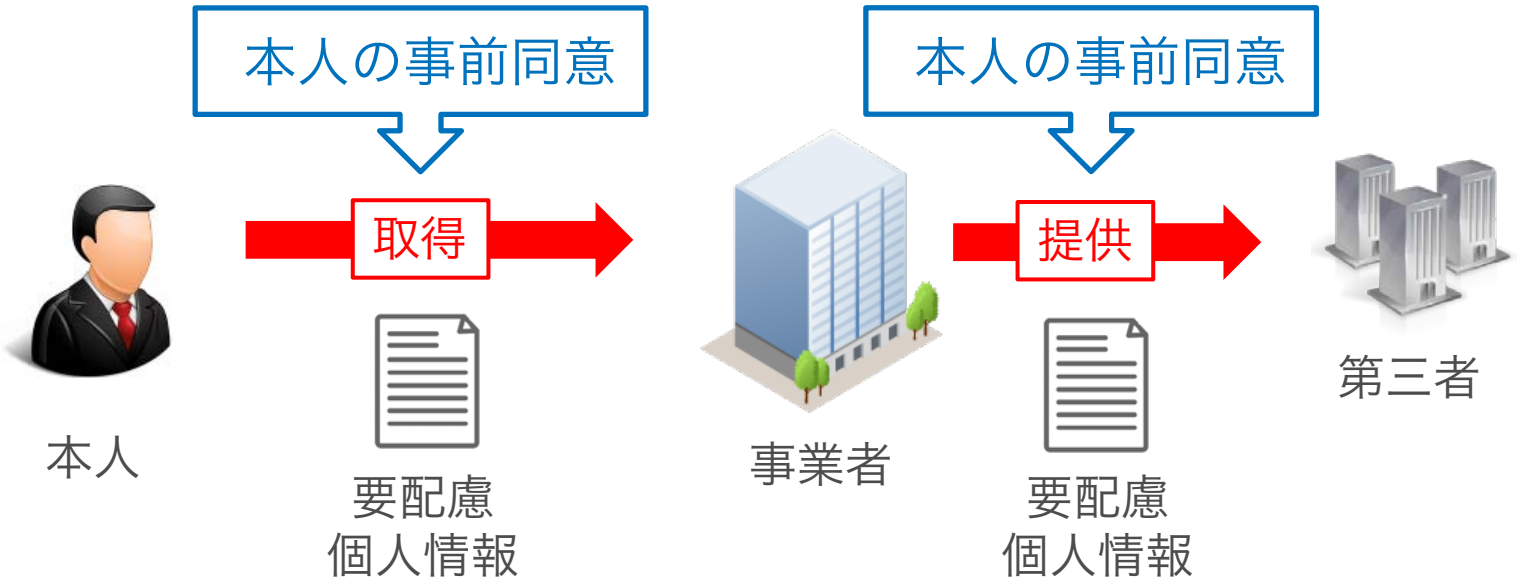
⑨ 医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと

⑩ 逮捕・捜索等の刑事手続に関する手続が行われたこと

⑪ 少年の保護事件に関する手続が行われたこと

3 要配慮個人情報

要配慮個人情報についての規制（17②・23②）



1. 取得・提供に本人の事前同意を要求（17②・23①）
2. オプトアウト手続による第三者提供の制限の例外を排除（23②）

3 要配慮個人情報

取得制限の例外（17②）

1. 目的外利用の例外（16③各号）と同じ
2. 次の者により公開されている場合
   - (1) 本人
   - (2) 国の機関
   - (3) 地方公共団体
   - (4) 報道機関
   - (5) 著述を業として行う者
   - (6) 大学その他の学術研究機関
   - (7) 宗教団体
   - (8) 政治団体
   - (9) 外国の政府、政府機関、地方公共団体又は国際機関
   - (10) 外国において上記のいずれかに該当する者
3. 本人を目視・撮影することで、その外形上明らかな場合
4. 事業承継・共同利用・委託で取得する場合

4 トレーサビリティの確保（受領者側）

大手教育出版系企業の顧客情報漏洩事件（2014）

・システム保守の再委託先の派遣社員が無断で会員情報を持ち出して、名簿業者に会員情報１億7800万件分が売却され、名簿業者から、さらに50社以上に転売され、最終的に複数の名簿業者などを通じて、500社超に流出していたことが判明

・不正な個人情報の流通を抑止するために、必要に応じて個人情報の流通経路を辿ることができることが必要（名簿屋対策）

・オプトアウトによる場合
・第三者提供について本人の同意を得て提供される場合
・私人から提供される場合

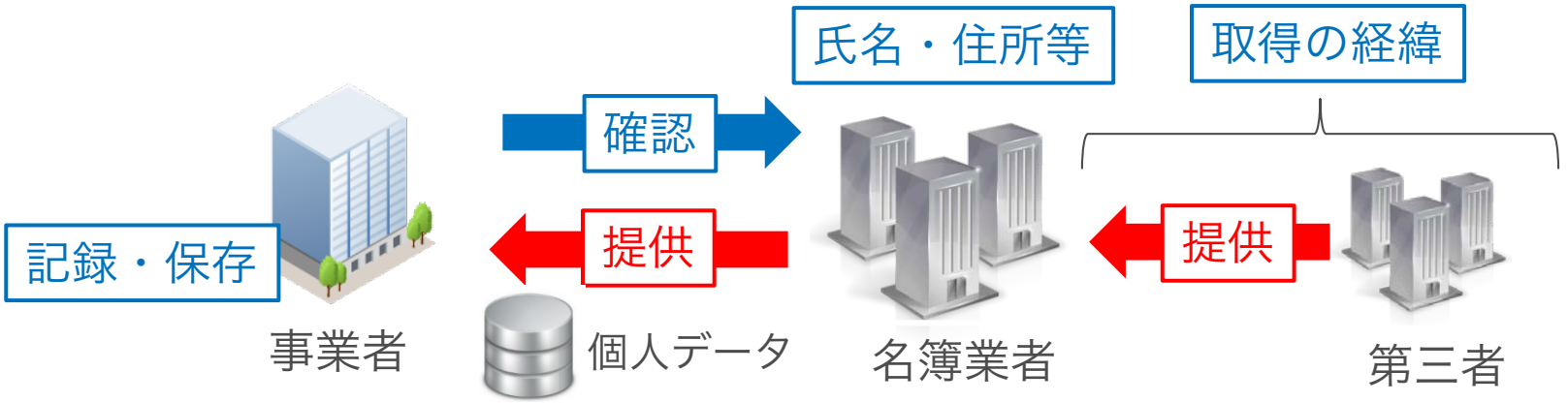
→ ○ 確認記録必要

・委託・事業承継・共同利用に基づいて提供される場合
・法令に基づき第三者に提供される場合等

→ × 確認・記録不要

4 トレーサビリティの確保（受領者側）

第三者提供を受ける側の義務（26）



記録・保存事項	オプトアウト	本人の同意	私人からの提供
提供を受けた年月日	○		
第三者の氏名・名称＋住所等	○	○	○
取得の経緯（直近まで）	○	○	○
本人の氏名・番号・ID等	○	○	○
個人データの項目	○	○	○
委員会により公表されている旨	○		
本人の同意を得ている旨		○	

4 トレーサビリティの確保（受領者側）

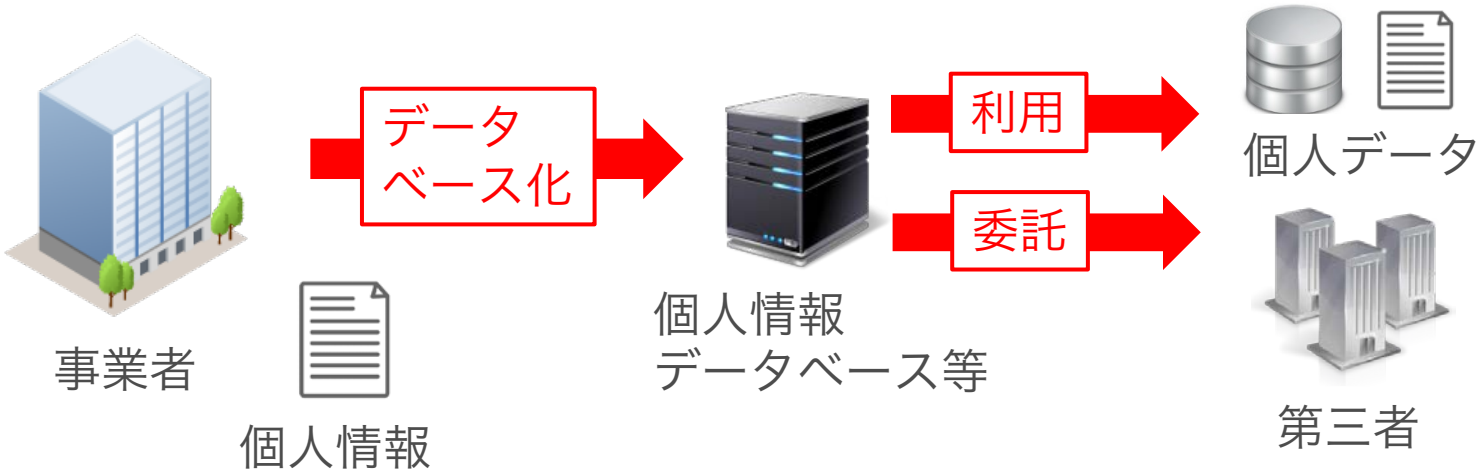
記録の保存期間（提供側・受領側共通）

記録の作成方法の別		保存期間
原則（授受の都度作成）		3年
例外	契約書等の代替手段による方法により記録を作成した場合	最後に当該記録に係る個人データの提供を行った日から起算して1年を経過する日までの間
例外	一括して記録を作成する方法により記録を作成した場合	最後に当該記録に係る個人データの提供を行った日から起算して3年を経過する日までの間

※ オプトアウトの場合は例外なし

1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 安全管理措置における対応事項



1. データ内容の正確性の確保等(19)
   - 遅滞なく消去する努力義務
2. 安全管理措置(20)
3. 従業者の監督(21)
4. 委託先の監督(22)

2 安全管理措置の概要

漏洩等により本人が被る権利利益の侵害の程度

＋

漏洩リスクの評価

- 事業の規模・性質
- 取扱状況（性質・量）
- 記録した媒体の性質

❶ 基本方針の策定

事業者の名称、関係法令・ガイドライン等の遵守、安全管理措置に関する事項、質問及び苦情処理の窓口等

❷ 個人データの取扱いに係る規律の整備

取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定

2 安全管理措置の概要

組織的安全管理措置

① 組織体制の整備
② 個人データの取扱いに係る規律に従った運用
③ 個人データの取扱状況を確認する手段の整備
④ 漏洩等の事案に対応する体制の整備
⑤ 取扱状況の把握及び安全管理措置の見直し

人的安全管理措置

① 従業者の教育
（定期研修・守秘義務）

物理的安全管理措置

① 個人データを取り扱う区域の管理
② 機器及び電子媒体等の盗難等の防止
③ 電子媒体等を持ち運ぶ場合の漏洩等の防止
④ 個人データの削除及び機器、電子媒体等の廃棄

技術的安全管理措置

① アクセス制限
② アクセス者の識別と認証
③ 外部からの不正アクセス等の防止
④ 情報システムの使用に伴う漏洩等の防止

3 情報漏洩の原因

大手教育出版系企業の顧客情報漏洩事件（2014）

（事案の概要）

・グループ企業であるS社へ委託され、システム保守の部分に関しては別業者へ再委託されたところ、再委託先の派遣社員が無断で会員情報を持ち出して、12～13回にわたり、名簿業者に会員情報１億7800万件分を約280万円で売却

・委託先に対する必要かつ適切な監督の懈怠を理由に是正勧告

① 委託先に対して行う定期的な監査において、当該情報システムの対象範囲を監査の対象としていなかった

② 自社の業務の全過程において自社が保有する個人情報の利用・管理に責任を持つ部門の設置を怠っていた

※ 組織的安全管理措置が大規模漏洩の防止のポイント

1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 提供段階における対応事項

1. 第三者提供の制限(23①)
   - オプトアウト規定の厳格化(23②～④)
   - 事業承継・共同利用・委託の例外(23⑤)
2. 外国にある第三者への個人データの提供制限(24)
3. トレーサビリティの確保（提供側）(25)
4. 個人情報データベース等提供罪(83)

2 オプトアウト規定の厳格化

❶ 以下の事項について、本人への通知又は「本人が容易に知り得る状態※」に置く

- 第三者への提供を利用目的とすること
- 第三者に提供される個人データの項目
- 第三者への提供の方法
- 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること
- 本人の求めを受け付ける方法

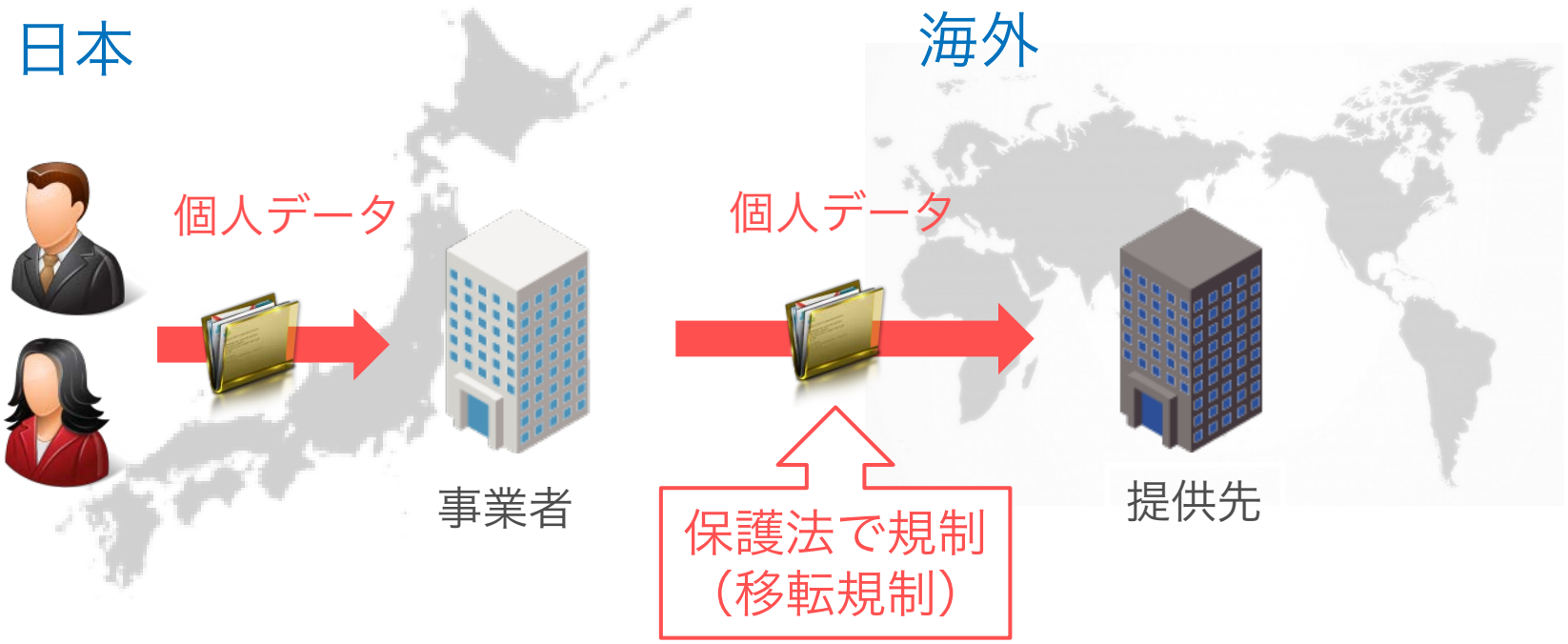
※ 本人が提供の停止を求めるのに必要な予告期間をおいて、事業所の窓口等への書面の掲示・備付けやホームページへの掲載その他の継続的方法による（PPCのGL）

❷ 個人情報保護委員会への届出（23②）

❸ 個人情報保護委員会によるその内容の公表（23④）

3 外国にある第三者への個人データの提供制限

外国にある第三者への個人データの提供（24）



外国への移転については委託・事業譲渡・共同利用は第三者提供の制限の例外にはならず、本人の同意を取得する等の義務あり
（海外のグループ企業や海外の委託先がある事業者に影響）

3 外国にある第三者への個人データの提供制限

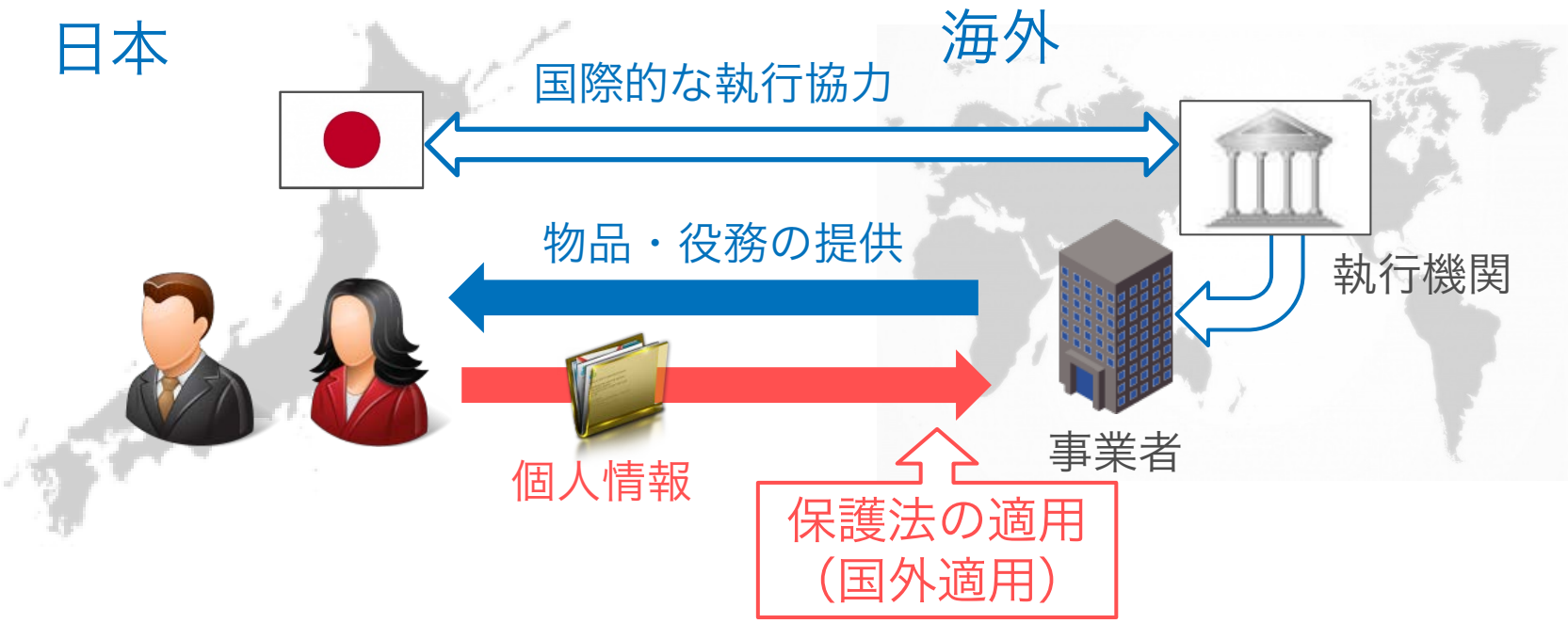
外国にある第三者への提供制限の例外

1. 本人の同意がある場合
2. 我が国と同等の水準にあると認められる個人情報保護の制度を有している外国にある第三者（現時点ではなし）
3. 提供の当事者間で、提供先における個人データの取扱いについて、契約や内規等により、法の規定の趣旨に沿った措置の実施が確保されている第三者、又は

   APECの越境プライバシールール（CBPR)の認証を得ている第三者
4. 第三者提供の制限の例外（23①）の場合

3 外国にある第三者への個人データの提供制限

海外の事業者による日本から海外へのデータ移転規制（75・78）



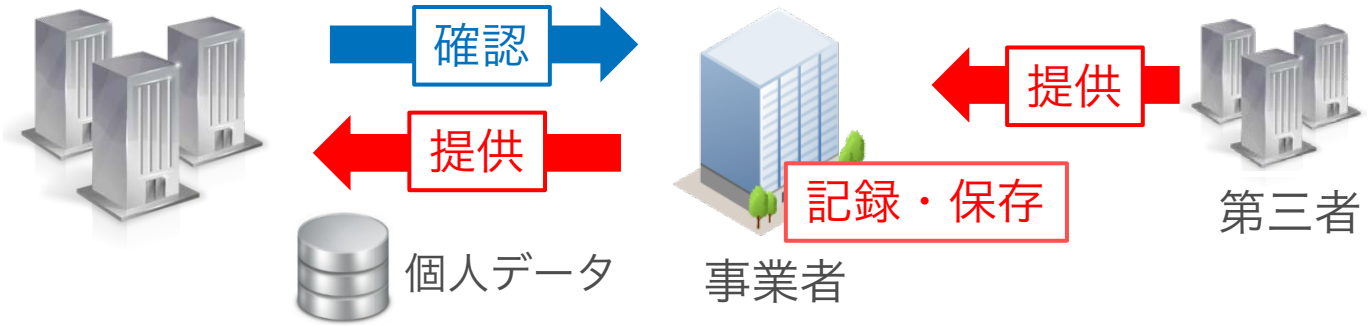
・保護法違反に対しては、指導・助言、是正勧告による対応

・報告・立入検査、命令は、執行管轄の問題があるため適用なし

・刑事罰は、不正な利益を図る目的でのデータベースの提供のみ

4 トレーサビリティの確保（提供側）

第三者提供する側の義務（25）



※ 確認に係る事項を偽ってはならない（26②・88：10万円以下の過料）

記録・保存事項	オプトアウト	本人の同意
提供した年月日	○	
第三者の氏名・名称＋住所等	○	○
本人の氏名・番号・ID等	○	○
個人データの項目	○	○
本人の同意を得ている旨		○

5 個人情報データベース等提供罪

個人情報データベース等提供罪の新設（83）

主体

個人情報取扱事業者（その者が法人*である場合にあっては、その役員、代表者又は管理人）若しくはその従業者又はこれらであった者

* 法人でない団体で代表者又は管理人の定めのあるものを含む。

行為

その業務に関して取り扱った個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）を自己若しくは第三者の不正な利益を図る目的で提供又は盗用

罰則

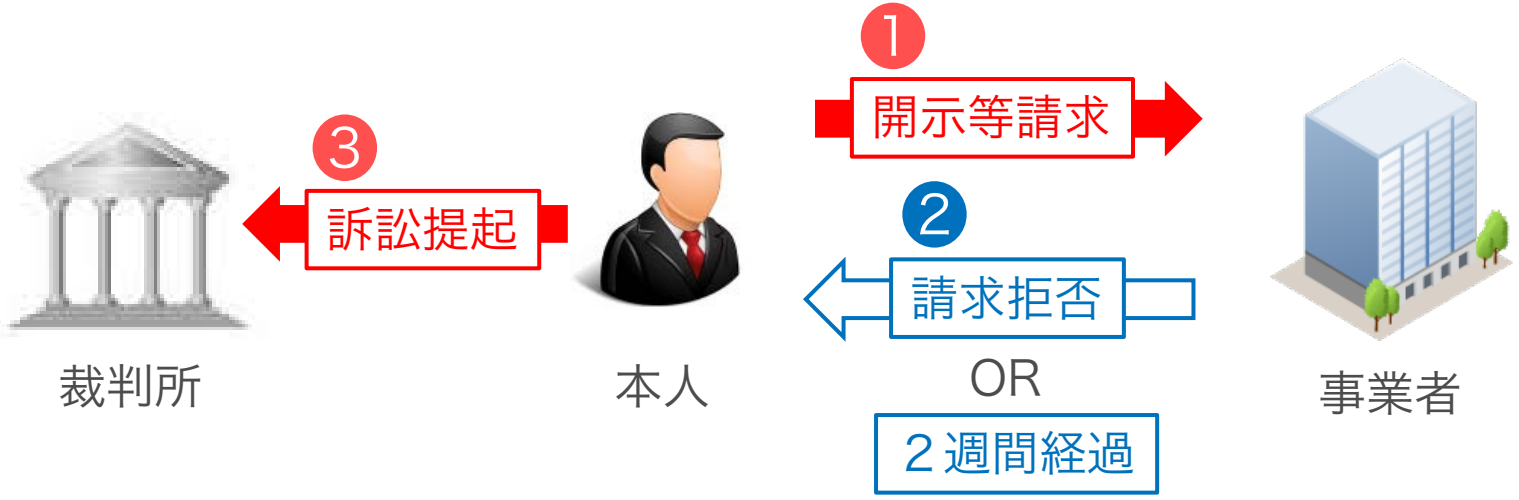
１年以下の懲役又は５０万円以下の罰金

1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1　開示等請求権の明確化

・東京地判平成19年6月27日（判時1978号27頁）は開示等の請求権の権利性を否定（行政処分のみ）

・本人が個人情報取扱事業者に対し、自身の保有個人データの開示、訂正等及び利用停止等の請求を行う権利を有することを明確化（28①、29①、30①③、裁判で実現）



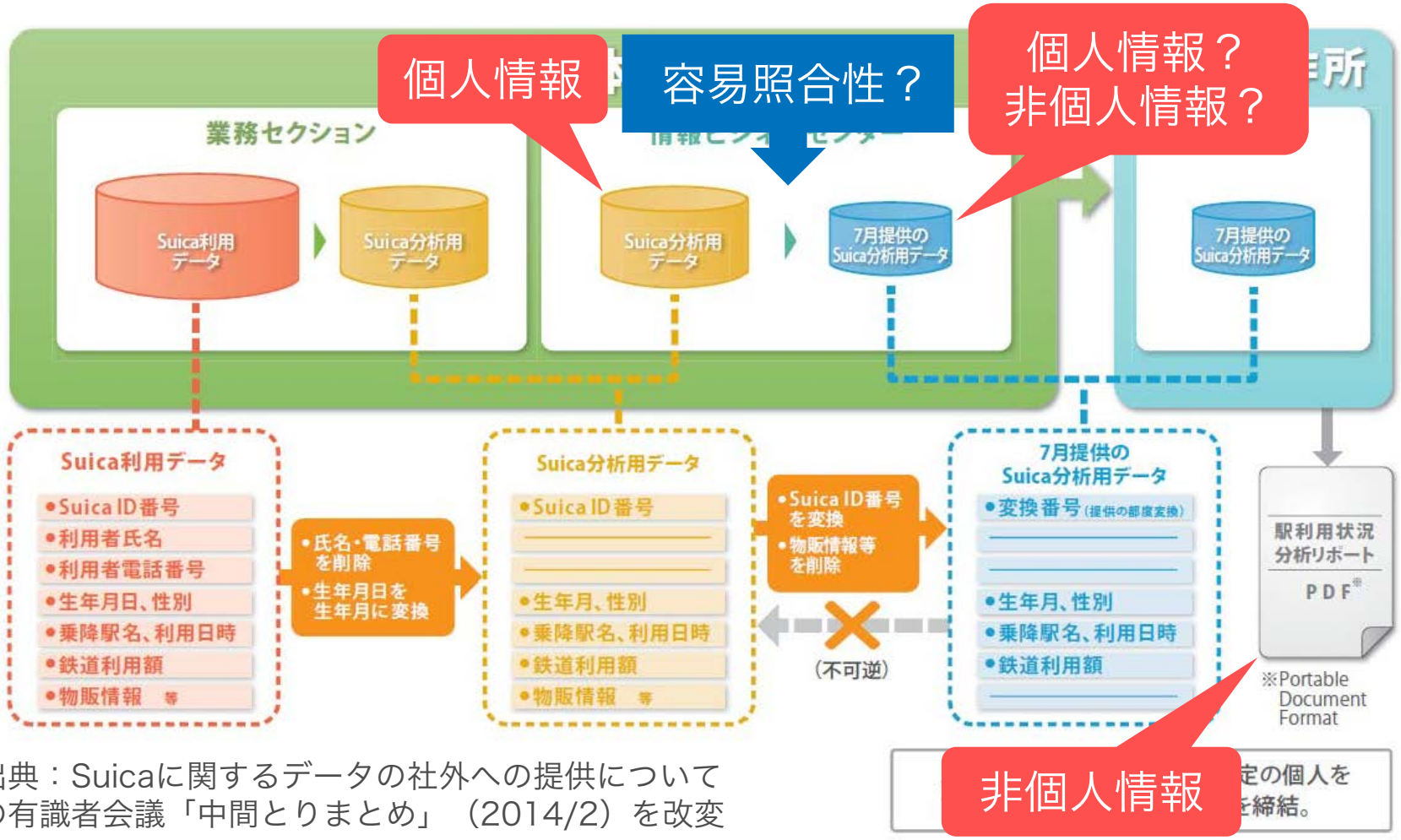
1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 匿名加工情報の位置づけ

個人情報の区分	講じる措置の内容	情報の内容
生存する個人に関する情報であって、当該情報に含まれる記述等により特定の個人を識別することができるもの（２①(1)）	当該個人情報に含まれる記述等の一部を削除すること	・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 ＋ ・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
生存する個人に関する情報であって、個人識別符号が含まれるもの（２①(2)）	当該個人情報に含まれる個人識別符号の全部を削除すること	

1 匿名加工情報の位置づけ

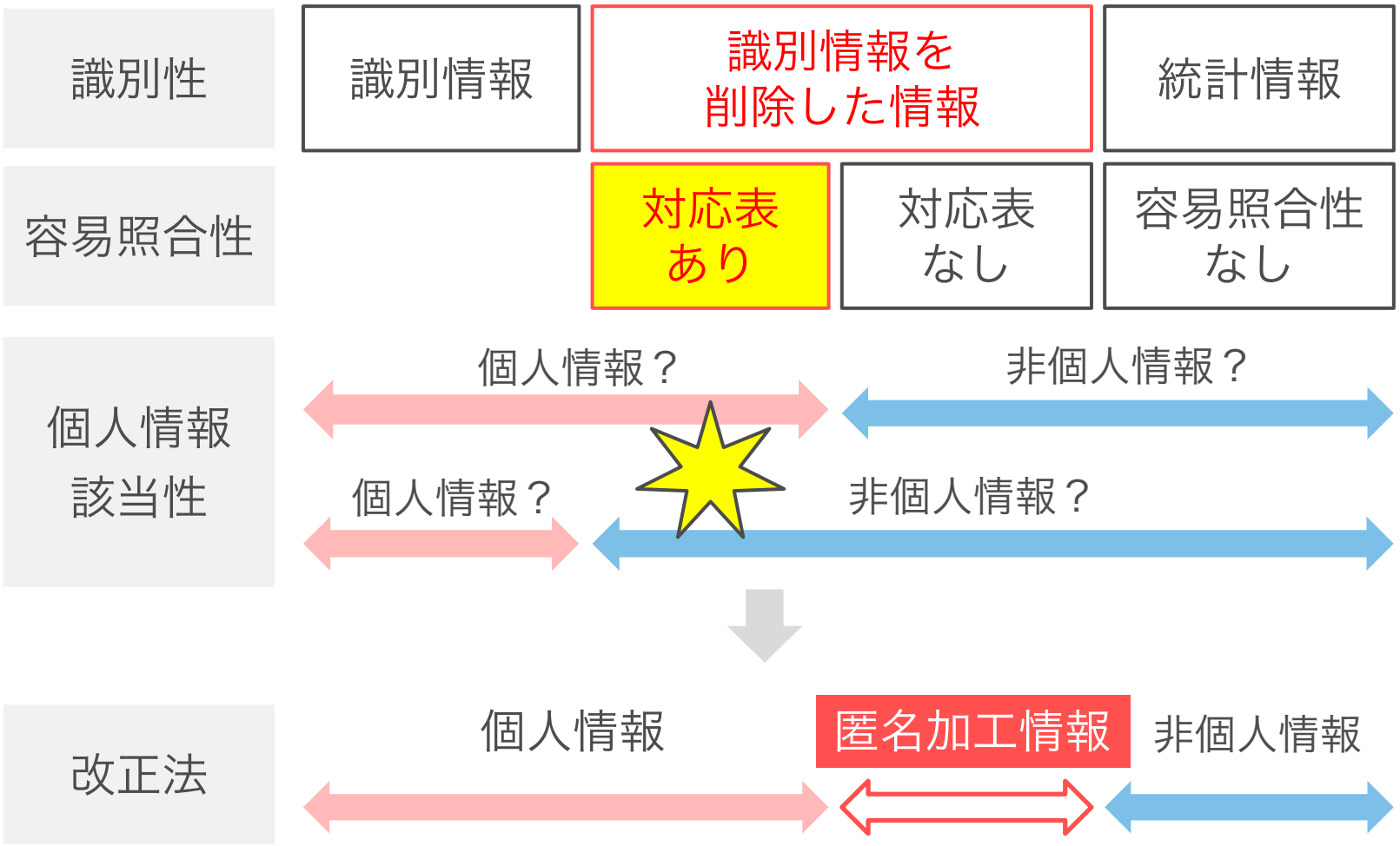
匿名加工情報の利用場面



出典：Suicaに関するデータの社外への提供についての有識者会議「中間とりまとめ」（2014/2）を改変

1 匿名加工情報の位置づけ

匿名加工情報の位置づけ



2 匿名加工情報に関する加工方法や取扱い

匿名加工情報の作成等（36①～③）

① 匿名加工情報の適正な加工

- 特定の個人を識別することができる記述等の削除
- 個人識別符号の削除
- 情報を相互に連結する符号の削除
- 特異な記述等を削除すること
- 個人情報データベース等の性質を踏まえたその他の措置

② 匿名加工情報等の安全管理措置等

- 加工方法等情報の安全管理措置
- 匿名加工情報の安全管理措置等

③ 匿名加工情報に含まれる個人に関する情報の項目を公表

※ 個人情報の安全管理措置の一環として、一部の情報を削除あるいは分割して保存・管理する等の加工をする場合又は個人情報から統計情報を作成するために個人情報を加工する場合等を含まない

2 匿名加工情報に関する加工方法や取扱い

匿名加工情報の第三者提供（36④、37）

1. 提供に当たりあらかじめ、以下の項目を公表
   - 第三者に提供する匿名加工情報に含まれる個人に関する情報の項目
   - 匿名加工情報の提供の方法を公表
2. 提供を受ける第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示

識別行為の禁止（36⑤・38）

1. 自ら作成した匿名加工情報を取り扱う場合
   - 本人を識別するために他の情報と照合してはならない
2. 他者の作成した匿名加工情報を取り扱う場合
   - 受領した匿名加工情報の加工方法等情報を取得してはならない
   - 受領した匿名加工情報を、本人を識別するために他の情報と照合してはならない

1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 既に個人情報取扱事業者である事業者の対応

1. 個人情報保護方針の改訂（個人情報の拡大による利用目的の見直し・開示請求手続）
2. 個人情報取扱規程の改訂（定義・要配慮個人情報の取扱・利用目的の変更・開示請求対応）
3. 要配慮個人情報の取得時の同意書の策定
4. 外国の委託先や関連会社の洗出し（情報管理体制の確認と見直し・グループ会社取扱規程の整備、外国の委託先等との個人情報の取扱に関する契約等の締結・変更）
5. 本人からの外国への提供の同意書の策定
6. 社内における研修教育の実施

2 名簿業者・名簿購入事業者の対応

1. 個人情報保護方針の改訂（オプトアウトの公表事項として本人の求めを受け付ける方法の追加）
2. 個人情報取扱規程の改訂（オプトアウトによる要配慮個人情報の取得禁止・予告期間の設定等）
3. オプトアウトの個人情報保護委員会に対する届出
4. 個人データの第三者提供時・受領時の帳票（確認書・授受の際の記録簿）の策定
5. 社内における研修教育の実施

3 ビッグデータ事業者の対応

1. 個人情報保護方針の改訂（公表事項への対応等）
2. 個人情報取扱規程の改訂（匿名加工情報の作成・管理・提供における取扱手順等・識別行為の禁止）
3. 匿名加工情報の加工方法等の情報の安全管理措置
4. 匿名加工情報の公表用のサイトページの設置
5. 社内における研修教育の実施

1. 個人情報保護法の改正の概要
2. 適用対象・適用範囲の拡大等
3. 取得・利用段階における対応事項
4. 安全管理措置における対応事項
5. 提供段階における対応事項
6. 開示段階における対応事項
7. 匿名加工情報への対応事項
8. 改正保護法に対する主な対応事項
9. システム監査における留意点

1 システムの利用方法による影響

個人データを扱う情報システム

改正法において安全管理措置の内容に変更はない（但し、PPCのGLにおいて要求項目に一部変更あり）

→ 影響なし

個人データの第三者提供を管理する情報システム

オプトアウト・本人同意等によって提供・受領する個人データを取り扱う場合には、確認・記録の義務あり

→ 取得した個人データ毎に16頁と29頁の各項目を記録する仕組み

匿名加工情報を取り扱う情報システム

匿名加工情報については再識別が不能であることが求められる

→ 37頁の①適正な加工方法を実現する仕組み
加工方法等情報に対するアクセス制限の仕組み
元データとの照合等により再識別ができないことを担保する仕組み

2 システムの運営・利用主体による影響

国内の事業者が運営するクラウドシステム

外国に置かれたサーバーを利用したクラウドシステムについては、日本国内の事業者が運営する限りは、外国への移転に本人同意の取得等は不要

→ 影響なし

外国の事業者が運営するクラウドシステム

国内に置かれたサーバーを利用したクラウドシステムであっても、外国の事業者が運営する限りは、外国への移転に本人同意の取得等が必要

→ 外国の事業者との委託契約の見直し

外国のグループ会社と共用するシステム

外国のグループ会社から、システム内の日本で取得した個人データを閲覧可能であれば、共同利用を行っていても、外国への移転に本人同意の取得等が必要

→ 外国のグループ会社との委託契約の締結やグループ規約の見直し

ご質問・ご相談のお問合せ先

☎（06）7669 - 8938（直通）
✉ fukumoto@daiichi-law.jp

弁護士法人第一法律事務所

弁護士・公認システム監査人

福　本　洋　一

東京事務所
東京都千代田区有楽町1丁目7番1号
有楽町電気ビル南館6階
TEL（03）5252 - 7022（代表）

大阪事務所
大阪市北区中之島２丁目２番７号
中之島セントラルタワー２４階
TEL（06）6227 - 1951（代表）