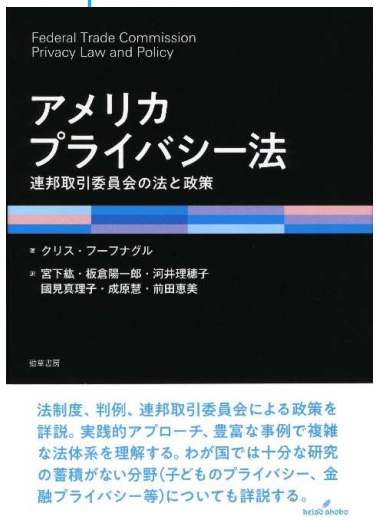
ひかり総合法律事務所 パートナー弁護士
板倉陽一郎

プライバシー保護技術の国内法制度における位置づけ

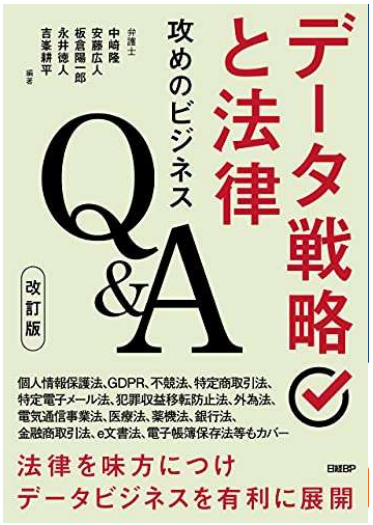
自己紹介

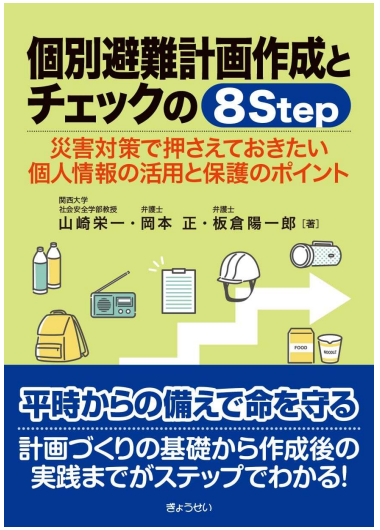
- 2002年慶應義塾大学総合政策学部卒，2004年京都大学大学院情報学研究科社会情報学専攻修士課程修了，2007年慶應義塾大学法務研究科（法科大学院）修了。2008年弁護士（ひかり総合法律事務所）。2016年4月よりパートナー弁護士。
- 2010年4月より2012年12月まで消費者庁に出向（消費者制度課個人情報保護推進室（現・個人情報保護委員会事務局）政策企画専門官）。
- 2017年4月より理化学研究所革新知能統合研究センター社会における人工知能研究グループ客員主管研究員，2018年5月より国立情報学研究所客員教授，2020年5月より大阪大学社会技術共創研究センター招へい教授，2021年4月より国立がん研究センター研究所医療AI研究開発分野客員研究員，2023年9月より早稲田大学次世代ロボット研究機構AIロボット研究所客員上級研究員（研究院客員教授）。
- 政府委員等として，法務省・民事判決情報データベース化検討会委員，内閣府消費者委員会デジタル化に伴う消費者問題ワーキング・グループオブザーバ等。
- 法とコンピュータ学会理事、日本メディカルAI学会監事等。

近著


Federal Trade Commission
Privacy Law and Policy
アメリカ
プライバシー法
連邦取引委員会の法と政策
クリス・フーフナグル
宮下紘・板倉陽一郎・河井理穂子
國見真理子・成原慧・前田恵美
法制度、判例、連邦取引委員会による政策を詳説。実践的アプローチ、豊富な事例で複雑な法体系を理解する。わが国では十分な研究の蓄積がない分野(子どものプライバシー、金融プライバシー等)についても詳説する。

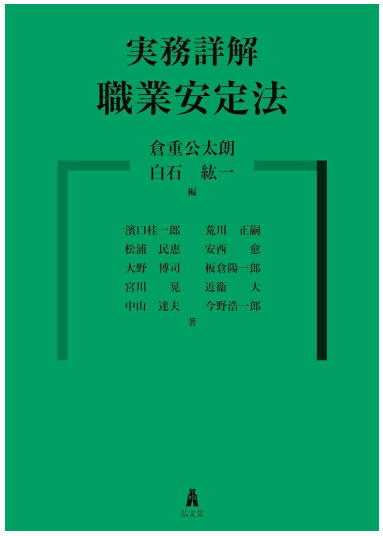

HRテクノロジーの
法・理論・実務
人事データ活用の新たな可能性
労務行政研究所[編]　弁護士 倉重公太朗[編集代表]
今野浩一郎
岩本 隆
宇野禎晃
酒井雄平
丸吉香織
伊達洋駆
小島武仁
今村謙三
小田原悠朗
江夏幾多郎
藤本 真
白石紘一
板倉陽一郎
リコージャパン
LINE
NEC
労務行政

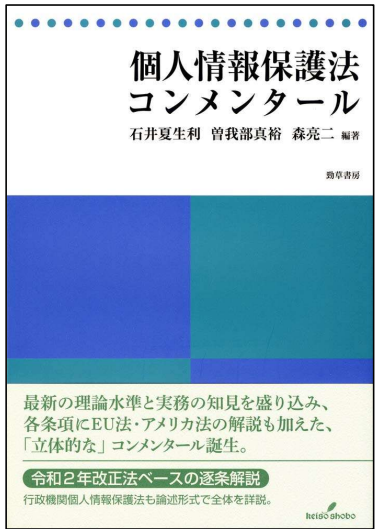

弁護士
中崎 隆
安藤広人
板倉陽一郎
永井徳人
吉峯耕平
編著
データ戦略と法律
攻めのビジネス
Q&A
改訂版
個人情報保護法、GDPR、不競法、特定商取引法、
特定電子メール法、犯罪収益移転防止法、外為法、
電気通信事業法、医療法、薬機法、銀行法、
金融商取引法、e文書法、電子帳簿保存法等もカバー
法律を味方につけ
データビジネスを有利に展開
BNBP


個別避難計画作成と
チェックの8Step
災害対策で押さえておきたい
個人情報の活用と保護のポイント
関西大学
社会安全学部教授
山崎栄一・岡本 正・弁護士
井護士
板倉陽一郎[著]
平時からの備えで命を守る
計画づくりの基礎から作成後の
実践までがステップでわかる!
ぎょうせい

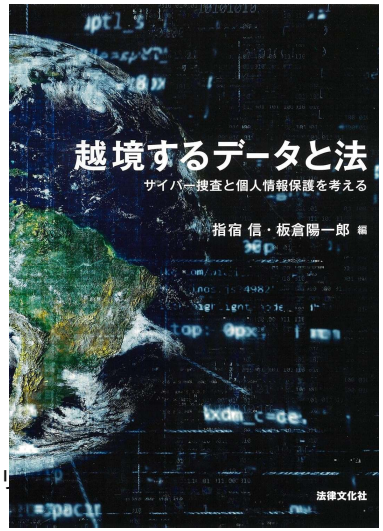

金融機関の
個人情報保護の
実務
板倉陽一郎
斉藤 邦史 著
令和3年改正個人情報保護法、
金融分野ガイドライン等にもとづいて
金融機関に求められる
最新の実務対応を具体的に解説!
巻末に金融分野ガイドライン、金融機関における個人情報Q&Aを収録
経済法令研究会


これだけで
わかる!
医療
AI
井川房夫
藤田広志
AI知らずに大丈夫!?
AIは既に、医療者誰しもが無視できないツールです。
医療現場に必要なAIの基本的知識から実際の活用方法まで、やさしく解説しました。
何から手をつけていいかわからない人、まずは本書を開いてみてください。
このまま知らないと2024/12/15できますか?
中外医学社


実務詳解
職業安定法
倉重公太朗
白石 紘一
編
濱口桂一郎　荒川 正嗣
松浦 民恵　安西 愈
大野 博司　板倉陽一郎
宮川 晃　近衛 大
中山 達夫　今野浩一郎
著


個人情報保護法
コンメンタール
石井夏生利　曽我部真裕　森亮二 編著
勁草書房
最新の理論水準と実務の知見を盛り込み、
各条項にEU法・アメリカ法の解説も加えた、
「立体的な」コンメンタール誕生。
令和2年改正法ベースの逐条解説
行政機関個人情報保護法も論述形式で全体を詳説。


Basic Lecture of Consumer Law
中田邦博+鹿野菜穂子 編
基本講義 消費者法
[第5版]
基礎から応用までを理解するための
消費者法テキストの決定版
法律文化社


越境するデータと法
サイバー捜査と個人情報保護を考える
指宿 信・板倉陽一郎 編

アジェンダ

1. プライバシー保護技術と個人情報保護法制
1.1. 個人情報保護法制全体の概観
1.2. プライバシー保護技術への個人情報保護法制の態度
1.3. 個人情報該当性
1.4. 安全管理措置（セキュリティ）
1.5. 監督官庁への通知義務の免除
1.6. 利用目的規制・第三者提供規制との関係
2. 秘密計算と不正競争防止法
3. 今後の展望

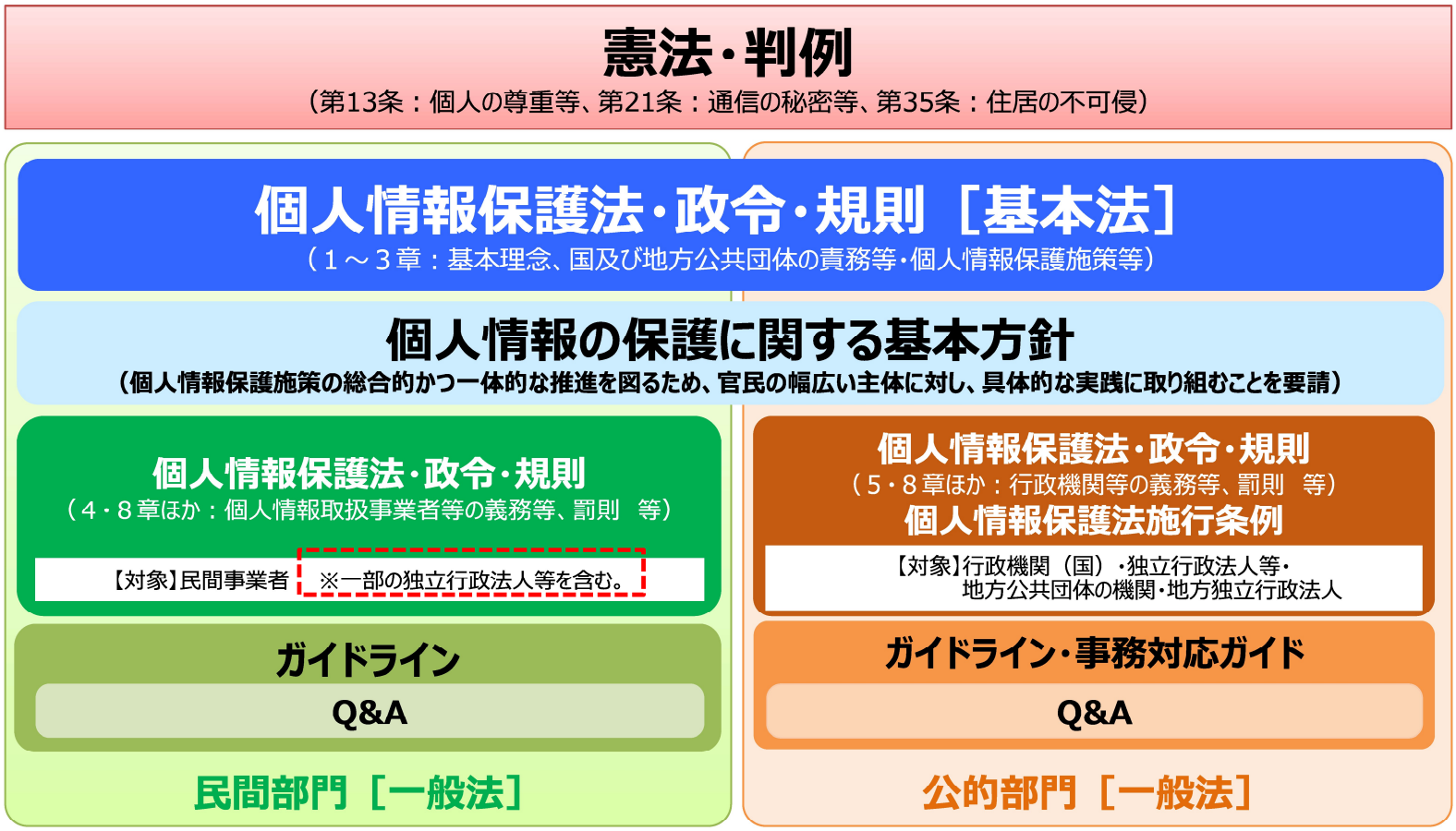
1. プライバシー保護技術と個人情報保護法制
1.1. 個人情報保護法制全体の概観

個人情報保護法制は極端な縦割り構造であったが，2021年改正により相当程度一元化された。

プライバシー保護技術の適用分野として，大学・病院・研究機関が設立母体に拘わらず概ね個人情報取扱事業者（民間部門）の規律に統一されたことが重要。

個人情報保護委員会「個人情報保護法の基本」（令和5年9月）

1-7. 個人情報保護法の全体像



注１　個人番号（マイナンバー）や医療分野等においては、上記一般法に優先して適用される特別法も遵守する必要。
注２　金融関連分野、医療関連分野や情報通信分野等の特定分野においては、上記ガイドライン等のほか、当該分野ごとのガイドライン等も遵守する必要。
注３　独立行政法人等、地方公共団体の機関及び地方独立行政法人の一部である国公立の病院・大学等の法人又は業務については、基本的には民間部門の規律が適用されるが、個人情報ファイル、開示等及び匿名加工情報に関する規律については、公的部門の規律が適用。
注４　民間部門においては、対象事業者に対する苦情処理、情報提供や指導等を行う認定個人情報保護団体に対し、対象事業者における個人情報等の適正な取扱いに関する自主的なルール（個人情報保護指針）を作成する努力義務があり、対象事業者は当該指針も遵守する必要。
注５　EU及び英国域内から十分性認定により移転を受けた個人データについては、上記法令及びガイドライン等のほか、補完的ルールも遵守する必要。

個人情報保護制度見直しの全体像

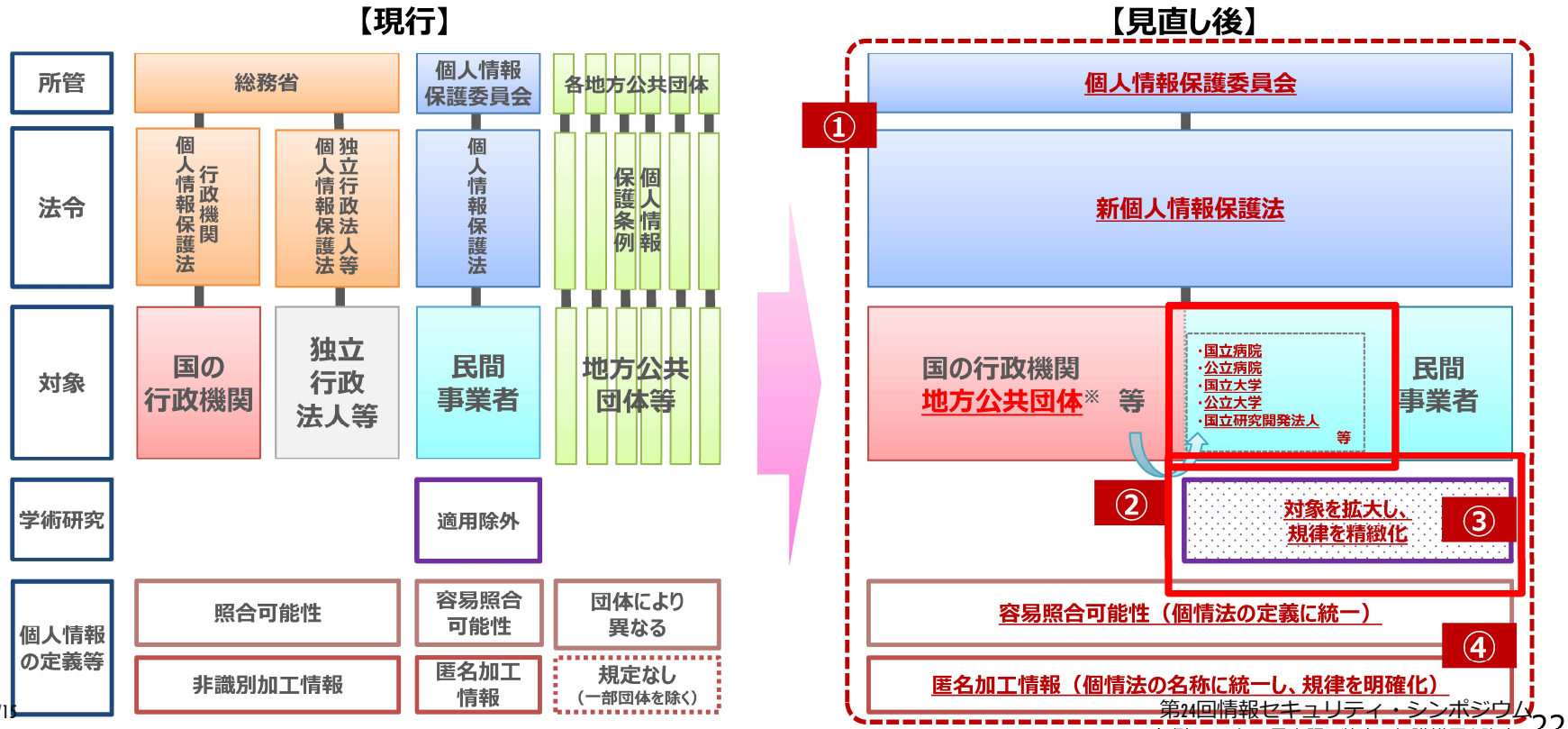
第１回　生命科学・医学系研究等における個人情報の取扱い等に関する合同会議
令和３（2021）年５月７日
資料３－２

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。**

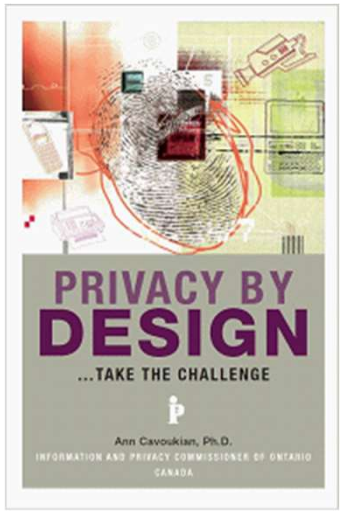


※　条例による必要最小限の独自の保護措置を許容

1.2.　プライバシー保護技術への個人情報保護法制の態度

「従来は，プライバシー強化技術(PETs)を利用することが，解決策であると考えられてきた」

(Ann Cavoukian)



2023年に報告書の公表が相次いだ

挙げられている技術

①データ難読化ツール（匿名化／仮名化，合成データ，差分プライバシー，ゼロ知識証明）
②暗号化データ処理ツール（準同形暗号，マルチパーティ計算(Multi-Party Computation), TEE (Trusted ExecutionEnvironment)）
③統合・分散アナリティクス（連合学習(FederatedLearning), Distributed analytics)
④データ透明化ツール（透明化されたシステム，閾値秘密分散，個人データ保管／個人情報マネジメントシステム）

挙げられている技術

準同形暗号
ゼロ知識証明
連合学習
合成データ
TEE
差分プライバシー

1.3. 個人情報該当性

個人情報保護法が対象としているのは「個人情報」であり（2条1項），個人情報でなくなれば個人情報保護法の対象ではなくなる。

「個人情報」と「個人に関する情報」

「個人情報」

- 生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
  - ①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個人識別符号が含まれるもの

「個人に関する情報」であることが要件の一つであることから，**「個人に関する情報」でない**といえるところまで加工されれば，それはもはや個人情報に該当せず，個人情報保護法の規制下におかれない，ということになる

暗号化によって個人情報ではなくなるのではないか？→委員会は明確に否定

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（通則編）（平成28年11月（令和4年9月一部改正））

2-1「『個人に関する情報』とは、氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、**暗号化等によって秘匿化されているかどうかを問わない**。」

準同型暗号を用いた秘密計算との関係でも，個人情報該当性が失われないことが確認されている（後述）

1.4. 安全管理措置（セキュリティ）

個人情報保護法23条

- 「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」
- セキュリティについての措置を講じなければならない，という包括的な規定

GL通則編による詳細

- 「10（別添）講ずべき安全管理措置の内容」
- 「10-6 技術的安全管理措置」
- 「（4）情報システムの使用に伴う漏えい等の防止」
- 「個人データを含む通信の経路又は内容を暗号化する」との手法が例示

秘密計算と安全管理措置

秘密計算は，暗号化を伴うものとは限らないが，漏えい等を防止し，又は，漏えいした場合の影響を最小限にするための技術であることは疑いがなく，適切に用いられていることを前提に，技術的安全管理措置の一部を構成すると考えてよい。

自由民主党『「経済構造改革戦略：Target 4」＝経済構造改革に関する特命委員会 最終報告＝』（平成30年4月27 日）

- 「個人情報保護の観点から開発を進めている**秘密計算技術**をはじめ、最新のセキュリティ技術の研究開発を推進する」（18頁）

自由民主党政務調査会デジタル社会推進特別委員会『デジタル・ニッポン2020』（令和2年6月11日）

- 「巧妙化するサイバー犯罪や量子コンピュータの実用化により従来型の暗号化やパスワードによる運用の限界がみられており、新たな技術として、データを断片化して暗号化自体を不必要にする**秘密分散技術**や、断片化したまま、あるいは複数の暗号化したままのデータの高速処理が可能な**秘密/秘匿計算技術等**が注目を集め始めている。これらの技術はデジタル田園都市国家で地方分散が進んだ際にも有効であり、また日本企業に強みがあるため、国としても導入を推進すべき。」（100頁）

政府・デジタル田園都市国家構想実現会議（第4回）（令和4年2月24日）【資料7】経済産業省「デジタル田園都市国家構想実現のための「デジタル日本改造ロードマップ」の検討の方向性について」

- 「データを暗号化したまま計算することができる秘密計算技術の実用化に向けた研究開発を加速し、データ分析の高度化とプライバシー保護の両立を図る。」（10頁）

秘密計算と安全管理措置（続）

内閣官房内閣情報セキュリティセンター（NISC）『政府機関等の対策基準策定のためのガイドライン（令和５年度版）』（令和５年７月４日）

- □基本対策事項3.1.1(6)-2 b)・基本対策事項3.1.1(6)-3 c)「複数の情報に分割し」について
- 「暗号技術の一種である秘密分散技術を用いて、秘匿すべき情報を複数のデータに分割することで、そのうちの一つを窃取しても元の情報を一切復元できないようにすることができる。この分割されたデータのそれぞれを異なる経路で運搬・送信する（例えば、片方を電子メールで送信し、もう片方を DVD や USB メモリ等の外部電磁的記録媒体で郵送するなど）ことにより、情報漏えいを防止することができる。なお、秘密分散技術自体が暗号技術の一種であるので、これにより分割されたデータをさらに暗号化する必要はなく、暗号鍵も必要ない」（119頁）

1.5. 監督官庁への通知義務の免除

個人情報保護法26条（民間），68条（公的）※68条の条文は若干違う

- 第1項「個人情報取扱事業者は、**その取り扱う個人データの漏えい、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個人の権利利益を害するおそれが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、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない**。ただし、（略）。」
- 第2項「前項に規定する場合には、個人情報取扱事業者（同項ただし書の規定による通知をした者を除く。）は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。ただし、（略）。」

個人情報保護法施行規則8条

- 法第26条第1項本文の個人の権利利益を害するおそれが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。
  - 一　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
  - 二　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
  - 三　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
  - 四　個人データに係る本人の数が千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

「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」とは

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（通則編）（平成28年11月（令和4年9月一部改正））

- 「3-5-3-1 報告対象となる事態」「なお、漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、「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」が講じられている場合については、報告を要しない。」

「個人情報の保護に関する法律についてのガイドライン（通則編）の一部を改正する告示案」に関する意見募集（2020年改正時）結果

- 169番「「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」については、**Q＆Aでお示しする**ことを検討してまいります。また、**秘密分散については、技術の進展や社会実装の動向も踏まえつつ、引き続き検討してまいります**。」

Q&Aの記載

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（令和5年5月25日）

- 6-16「報告を要しない「漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、漏えい等が発生し、又は発生したおそれがある個人データについて、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。
- 第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置としては、**適切な評価機関等により安全性が確認されている電子政府推奨暗号リストや ISO/IEC18033 等に掲載されている暗号技術が用いられ、それが適切に実装されていることが考えられます**。
- また、暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、
  - ①暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止する適切な措置を講じていること、
  - ②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は
  - ③第三者が復号鍵を行使できないように設計されていること
- のいずれかの要件を満たすことが必要と解されます。」

ISO/IEC 19592-2:2017と「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」

現時点では秘密分散を含む秘密計算技術が「「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」に該当するかについては，GLに特段の記述がなく，QAにもまだ掲載されていない。

電子政府推奨暗号リストにも登載されていないが，CRYPTREC 暗号技術調査ワーキンググループ（高機能暗号）「CRYPTREC 暗号技術ガイドライン（高機能暗号）」（2023年3月）では中心的に取り上げられている。

秘密分散についてはISO/IEC 19592-2:2017が平成29年10月に技術標準として発行しており，秘密分散による秘密計算については，少なくともISOに認められた方式が存在し，（現行QAにおける）「第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置」に該当すると考えてよいのではないか

1.6. 利用目的規制・第三者提供規制との関係

秘密計算は，「複数の組織が，各組織の持つデータを他組織に知られることなく，全組織のデータを結合した計算結果を得る手続き」とされる

複数の組織（法人等）のデータが，お互いに開示されることなく，計算結果だけが導き出されるということを最大限評価するのであれば，個人情報・個人データに関して，本人の同意なしに計算結果の導出ができないか，ということが検討され得る

利用目的規制と秘密計算

個人情報保護法上，個人情報取扱事業者は、個人情報を取り扱うに当たって、利用目的をできる限り特定し（17条1項），個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない（21条1項）

「計算結果」を導出することが利用目的に該当するか

- 「個人情報を統計処理して特定の個人を識別することができない態様で利用する場合についても、利用目的として特定する必要がありますか。」（Q2-5）
- 「**利用目的の特定は「個人情報」が対象であるため、個人情報に該当しない統計データは対象となりません。また、統計データへの加工を行うこと自体を利用目的とする必要はありません**。」（A2-5）

「計算結果」の導出自体は利用目的規制の対象とならないと解し得る

第三者提供規制と秘密計算

秘密計算の過程で「各組織の持つデータ」が「結合」される点については，個人データの第三者提供に該当し，本人の同意なしには許されないのではないか（個人情報保護法27条1項柱書）。

一般財団法人情報法制研究所（JILIS）個人情報保護法タスクフォースによる，個人情報保護法のガイドライン策定時のパブリックコメント（秘密計算技術と第三者提供規制の関係についての意見）

「暗号化によって秘匿されていても個人情報であるとされるが、準同型暗号を用いたプライバシー保護データマイニングによるデータ交換は、個人情報の提供に当たらないとみなすべき」

- 「法2 条1 項のガイドラインで、「個人に関する情報とは……であり、……暗号化等によって秘匿化されているかどうかを問わない。」とされている。確かに、個人情報を暗号化したデータが個人情報に該当するかというとき、復号鍵を誰が利用できる状態にあるかといった条件にかかわらず、暗号化された個人情報も個人情報であるとする法解釈が多数説となっていた。これにはクラウドと委託の関係等、様々な論点が関連し、議論の残るところと考えるが、少なくとも、**準同型暗号を用いたプライバシー保護データマイニング（*Privacy-Preserving Data Mining*、*PPDM*）におけるデータ交換は個人情報（個人データ）の提供に当たらないと解釈されるべく、法律上の位置づけの再整理をお願いしたい。この技術を用いれば、暗号化する事業者と復号する事業者のどちらも、どの情報がどの元情報に対応しているか知り得ることなく、集計などの統計情報を得ることができると期待されている**。」

個人情報保護委員会の回答

- 「**暗号化については、安全管理措置の一つとして考慮されるべき要素であり、個人情報該当性に影響するものではないと考え、本ガイドライン（通則編）案*2-1* において、「暗号化等によって秘匿化されているかどうかを問わない」と記載しております。なお、本ガイドライン（通則編）案*4* にあるとおり、漏えい等の事案が発生した場合の対応については、別に定めることとしております。**」（「個人情報の保護に関する法律についてのガイドライン（通則編）（案）」に関する意見募集（2015年改正時）結果27番）。

個人情報保護委員会の回答の解釈

個人情報保護委員会は，「個人情報該当性に影響するものではない」として，第三者提供規制の解釈上の例外であることは認めなかった。

タスクフォースのコメントは，「**個人情報（個人データ）の提供に当たらない**」との解釈を提案したものであって，個人情報に該当しないことを理由にはしていなかったので，個人情報保護委員会の回答はタスクフォースの意見に正面からは答えていない。

それでも，秘密計算を用いて計算結果を導出するための個人データの結合は，第三者提供に該当しないとはいえないとの見解はピン止めされている。

仮名加工情報＋共同利用？

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（仮名加工情報・匿名加工情報編））」（平成28年11月（令和4年9月一部改正））

- 「2-2-3-3　第三者提供の禁止等（法第41条第6項関係）」
  - (3)共同利用（法第41条第6項、第27条第5項第3号関係）
    - 「仮名加工情報は、加工によりそれ自体では特定の個人を識別できないものとなっており、また、本人を識別する目的での利用や本人に連絡等をする目的での利用が禁止されていること（法第41条第7項及び第8項）等を踏まえ、利用目的の柔軟な変更が許容されている（法第41条第9項）。そのため、仮名加工情報である個人データの共同利用における利用する者の範囲や利用目的等は、作成の元となった個人情報の取得の時点において通知又は公表されていた利用目的の内容や取得の経緯等にかかわらず、設定可能である。」

- 個人情報保護委員会事務局レポート：仮名加工情報・匿名加工情報信頼ある個人情報の利活用に向けて―制度編―（2022 年 5 月更新）注66
  - なお、**削除情報等の安全管理措置義務が適用されるのは「仮名加工情報を作成したとき」であるから、仮名加工情報の作成前の段階で、仮ＩＤの作成方法に関する情報を他の事業者と共有することが、直ちに同項違反となるわけではない**が、同項の趣旨に鑑み、仮名加工情報の作成前の段階であっても、**これを共有しないことが望ましい**。仮に、仮名加工情報の作成前の段階で、仮 ID の作成方法に関する情報を他の事業者と共有することがあったとしても、**仮名加工情報の作成後は削除情報等を他の事業者が有している状態となるため、共有している全ての事業者において、直ちに当該作成方法に関する情報を削除する等の措置を講じなければならない**。

仮名加工情報の共同利用

共同利用

民間病院（個人情報取扱事業者）

法41条6項・27条5項3号

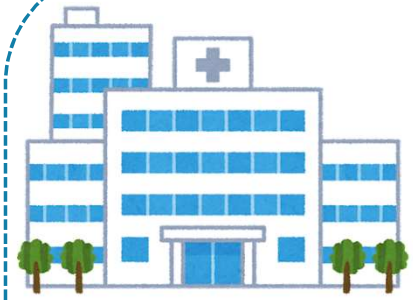
①共同して利用される個人データの項目
②共同して利用する者の範囲
③利用する者の利用目的
④管理について責任を有する者の氏名又は名称及び住所
⑤責任者の代表者の氏名　　公表

メーカー（個人情報取扱事業者）

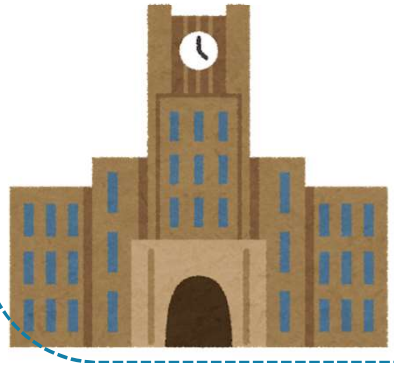
※仮名加工情報なので元の個人情報との識別行為は禁止

名寄せして共同利用

国立大学（規律移行法人）



民間病院（個人情報取扱事業者）



法41条6項・27条5項3号

①共同して利用される個人データの項目
②共同して利用する者の範囲
③利用する者の利用目的
④管理について責任を有する者の氏名又は名称及び住所
⑤責任者の代表者の氏名

製薬会社（個人情報取扱事業者）

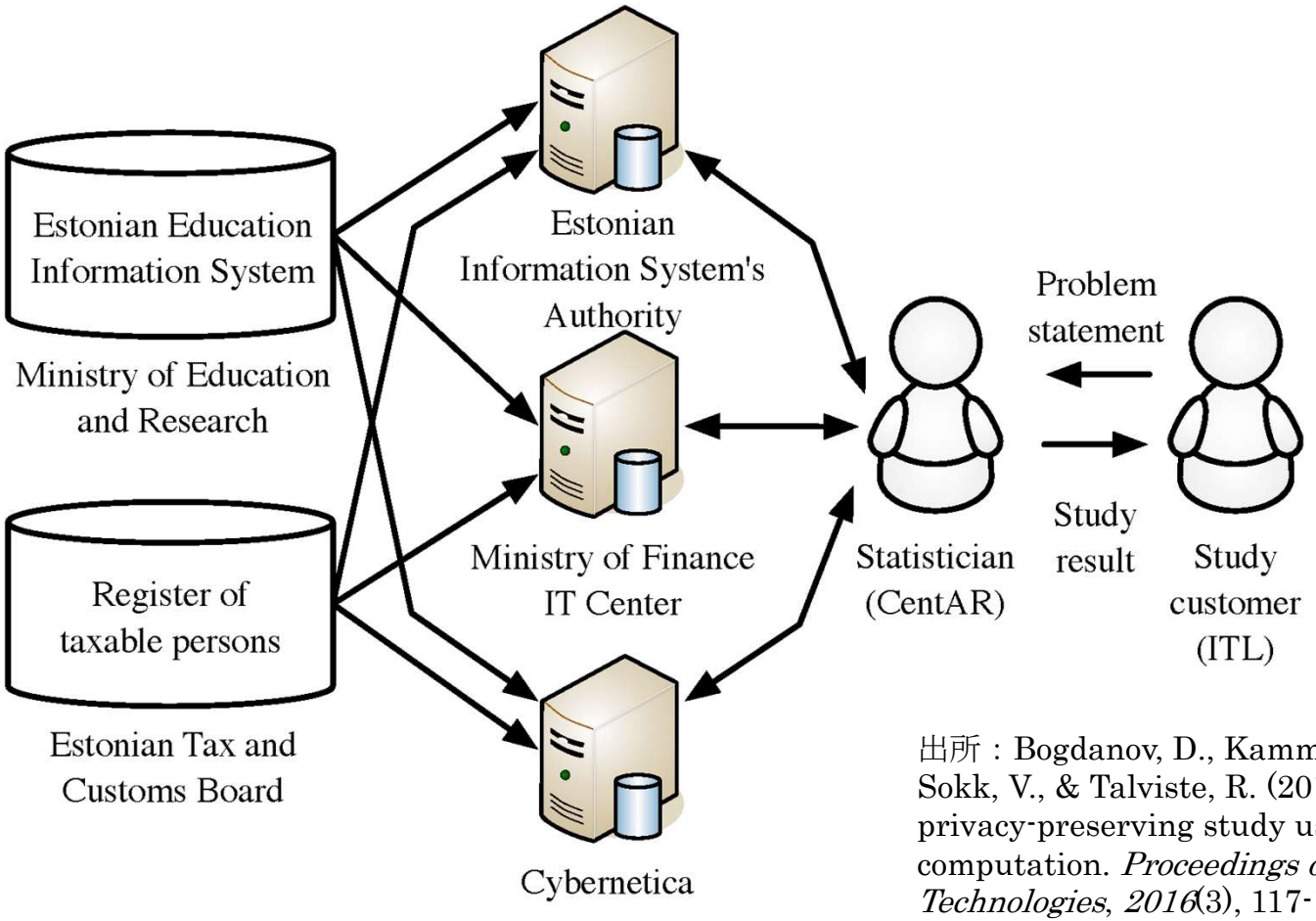
海外の事例①：平成26（2014）年1月27日付のエストニアデータ保護機関の見解

エストニア個人データ保護法（GDPR以前）においては，センシティブデータの処理に関して，事前にデータ保護機関の許諾が必要であった。

秘密計算を用いた処理は個人データの処理に該当しないとして，データ保護機関の事前許諾は不要とした 。

政府関係機関等が保有する税情報と教育情報を結合し，大学生の留年と仕事量（アルバイト等）の相関関係たる計算結果を導出する処理に秘密計算を用いたものであった 。ただし，個人データの処理に該当しない前提として，以下が挙げられている。

- ①研究目的
- ②導出されるのが統計データ
- ③秘密計算のソースコードについて事前のレビューがなされ，PIA（プライバシー影響評価）が実施
- ④秘密分散による秘密計算を行う組織間での結託を防止する契約が締結されていたこと



出所：Bogdanov, D., Kamm, L., Kubo, B., Rebane, R., Sokk, V., & Talviste, R. (2016). Students and taxes: a privacy-preserving study using secure computation. *Proceedings on Privacy Enhancing Technologies*, *2016*(3), 117-135.

Fig. 1. Stakeholders of the privacy-preserving statistical study

エストニア法の解釈の日本法への解釈への影響

日本と欧州は相互にデータ保護制度を認証している（欧州からの十分性認定，日本からの同等性の決定，2019年1月23日。Review2023年４月４日）

そうすると，一般データ保護規則（GDPR）の解釈についても，間接的に日本法の解釈に影響が与えられるということであり，GDPR以前のEUデータ保護指令及びエストニアデータ保護法に基づくデータ保護機関の判断であっても，現在も有効なものとして維持されている以上，日本法の解釈にあたっても参考になる。

海外の事例②：“RECOMMENDATIONS 01/2020”
前提：欧米間の（過去の）十分性認定

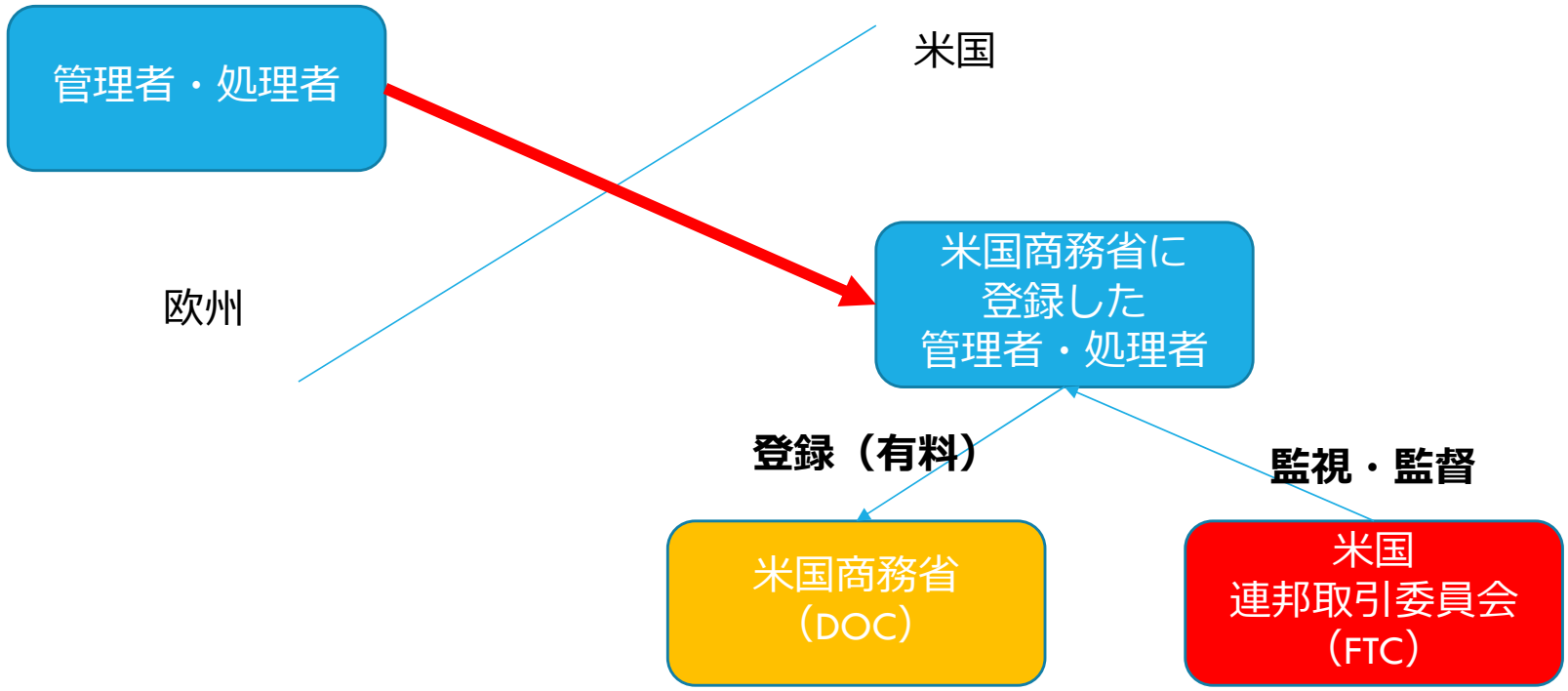
データが最も行き来しているであろう米国との間はどうなっているのか．米国には，包括的な連邦レベルでのデータ保護法も，公的機関を含む監視監督を行うデータ保護機関も存在していないため，**欧米で合意したデータ保護の枠組みに従うこととした個別の企業が，米国商務省に登録し，これに違反した場合には，不公正・欺瞞的な行為又は慣行に該当するとして，米国連邦取引委員会が連邦取引委員会法5条を用いて執行を行っていた**.

この，「欧米で合意したデータ保護の枠組み」が，欧米プライバシーシールドであり，欧州側の手続としては，十分性について決定が下されている。

- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) C/2016/4176.

欧米プライバシーシールドの十分性認定

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) C/2016/4176



MAXIMILLIAN SCHREMS V DATA PROTECTION COMMISSIONER(C-362/14) （SCHREMSI）

(interpretation of Directive Art.25-26)

…**in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union**

…the term **'adequate level of protection' must be** understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, **a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.**

THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 7

Respect for private and family life

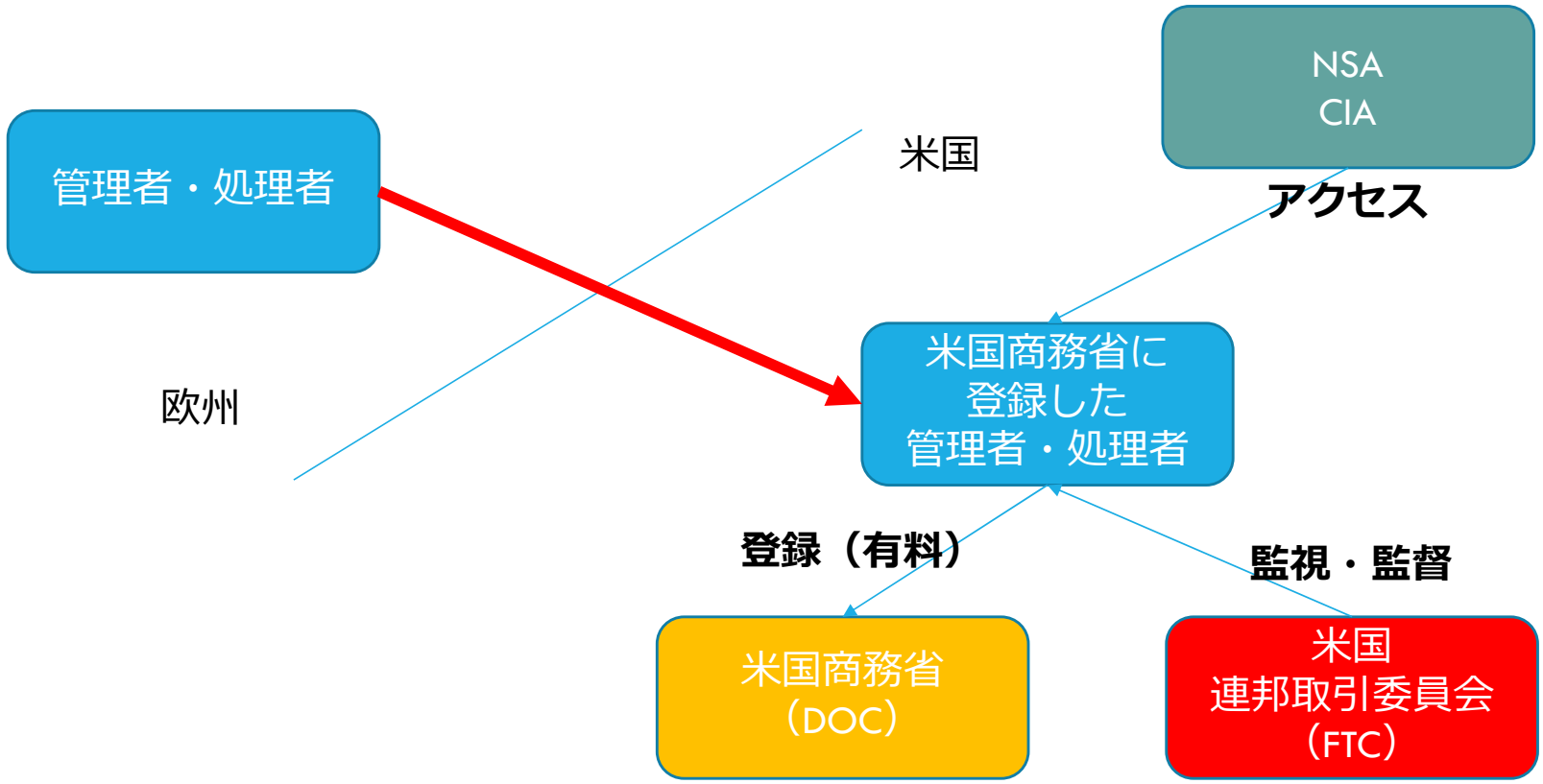
- Everyone has **the right to respect for his or her private** and family life, home and communications.

Article 8

Protection of personal data

- 1. Everyone has **the right to the protection of personal data concerning him or her.**
- 2. Such data must be processed fairly for specified purposes and on the basis of the consent of theperson concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- 3. Compliance with these rules shall be subject to control by an independent authori

個人データへの公的機関のアクセス



SCHREMSII決定

SchremsII決定では，”Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid.”，つまり，欧米プライバシーシールドについての十分性決定が無効とされた.

その主たる理由は，移転先である米国におけるパブリック・アクセス，就中，**米国が安全保障のために執行している諜報法分野における措置が，欧州連合基本権憲章が求める権利の保障のレベルに達していない**ということにある.

特に問題である点として，

- ①**米国の諜報法体系の下で，非米国人である（欧州市民を含む）データ主体が，米国当局に対して訴訟可能な権利を与えられていない**こと，
- ②**米国の諜報機関を拘束するための権限を有するはずのオンブズパーソンの独立性が確保されていない**こと

133 It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.

133 GDPR46 条(2)(c)に基づいて欧州委員会が採択した標準的なデータ保護約款は，EU に設立された管理者及び処理者に対して，すべての第三国で一律に適用される契約上の保証を提供することのみを目的としており，その結果，各第三国で保証されている保護レベルとは無関係である．これらの標準的なデータ保護条項は，その性質上，EU 法の下で要求される保護レベルへの準拠を保証するための契約上の義務を超える保証を提供することができない限りにおいて，特定の第三国の実勢に応じて，その保護レベルへの準拠を保証するために，管理者が追加的な措置を採用することを要求する場合がある．

「追加的な措置」の必要性

Schrems II決定は，プライバシーシールドについての十分性認定を無効であるとし，その主たる理由は，米国の諜報法分野におけるデータ主体の保護の薄弱さであった．ここで問題となっているのは移転先国たる米国における個人データの保護のレベルなのであるから，標準データ保護条項ないし標準契約約款（Standard Contractual Clauses）に基づく移転もできなくなるのではないかというのが，産業界の当然の懸念．

欧州連合司法裁判所は，「追加的な措置」が必要な場合があるとし，他方で，当該措置が必要な場合があることを前提に，標準データ保護約款による移転すべてを無効とはしなかった．

この「追加的な措置」は，SchremsII決定が初出ではなく，一般データ保護規則（GDPR）前文109においても「追加的な保護措置」（additional safeguards）という語は現れていた．しかしながら，文脈的には，SDPCないしSCCを契約や約款の一部とすることは許され，より強い保護は奨励される，というものであり，追加的な措置が必要的な場合があるということを読み取ることは困難であった．

GDPR前文(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. **Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses**.

(109) 欧州委員会又は監督機関によって採択された標準データ保護約款を管理者又は処理者が利用することができるということは，欧州委員会又は監督機関によって採択された標準契約条項と直接又は間接に矛盾せず，かつ，データ主体の基本的な権利及び自由を妨げるものではない限り，管理者又は処理者が，処理者と別の処理者との間の契約のような，より広範囲の契約の中に標準データ保護条項を含めることを妨げるものではなく，また，その約款の中に別の条項や保護措置を追加することを妨げるものでもない．**管理者及び処理者は，標準データ保護条項を補完する契約上の約定を介して，追加的な保護措置を提供することが奨励されなければならない**.

追加的措置についての動き

EDPB（欧州データ保護ボード）

- 2020年11月11日には，"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"（EUの個人データ保護のレベルの遵守を確実にするための移転ツールに追加する措置に関する勧告，「追加的措置勧告」）を公表し，2020年12月21日までパブリックコメントに付した
- 2021年6月18日“Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0”（EUの個人データ保護のレベルの遵守を確実にするための移転ツールに追加する措置に関する勧告第2版）として公表

EDPB及びEDPS（欧州データ保護観察官）

- 新SCC案に2021年1月14日に合同で意見を述べている
  - EDPB - EDPS Joint Opinion 1/2021 on the European Commission’s Implementing Decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725.

“RECOMMENDATIONS 01/2020 ON MEASURES THAT SUPPLEMENT TRANSFER TOOLS TO ENSURE COMPLIANCE WITH THE EU LEVEL OF PROTECTION OF PERSONAL DATA VERSION 2.0”（EUの個人データ保護のレベルの遵守を確実にするための移転ツールに追加する措置に関する勧告第2版）

ステップ1　移転の認知

ステップ2　移転ツール（越境移転に関する適法化事由）の特定

ステップ3　移転ツールの有効性

ステップ4　追加的な措置の採用

ステップ5　有効な追加的な措置を確認した場合の手続

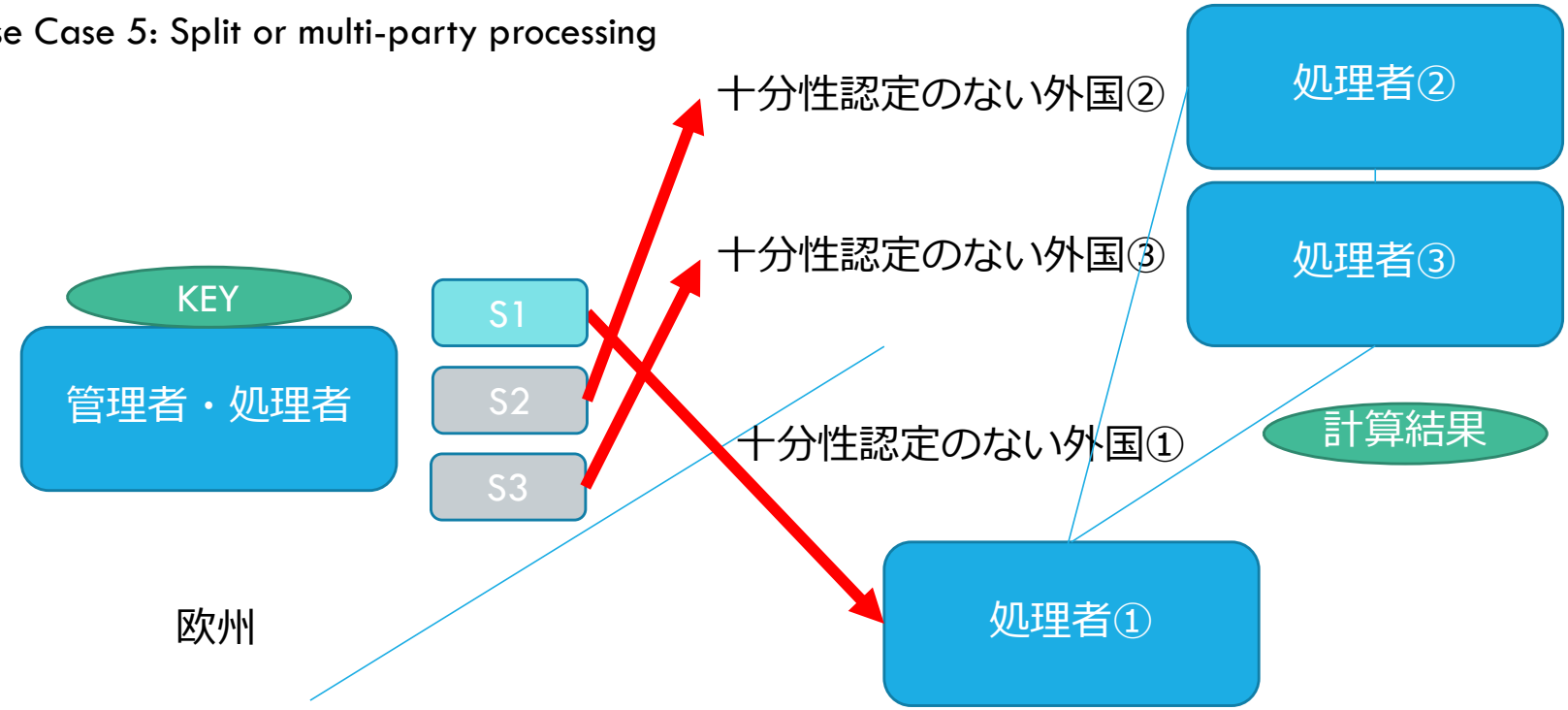
ステップ6　再評価

追加的措置

技術的な追加的な措置

- 有効なユースケースと無効なユースケースを列挙している．有効なユースケースとしては，
  - ①強力な暗号化がなされている場合の第三国におけるバックアップ，
  - ②適切な仮名化がなされている場合の移転，
  - ③エンドツーエンド暗号化がなされている場合の，第三国の通過，
  - ④暗号化がなされている場合の，特に保護された輸入者への移転，
  - ⑤**秘密計算の利用**が挙げられている．
- 他方，無効なユースケースとして，
  - ⑥クラウドサービスを利用した場合，当該サービスにパブリックアクセスが行われる場合，
  - ⑦ビジネス目的でリモートアクセスを行うが，パブリックアクセスが行われる場合，が挙げられている．
- いずれも詳細には要件が挙げられており，あくまで例示ではあるが，クラウドサービスを利用した場合のパブリックアクセスについては（米国を意識してか）特に厳しい見解ではないかと思われる．

Use Case 5: Split or multi-party processing



1. a data exporter processes personal data **in such a manner that it is split into two or more parts each of which can no longer be interpreted or attributed to a specific data subject without the use of additional information**,
2. **each of the pieces is transferred to a separate processor located in a different jurisdiction**,
3. the processors optionally process the data jointly, e.g. using secure multi-party computation, in a way that no information is revealed to any of them that they do not possess prior to the computation,
4. the algorithm used for the shared computation is secure against active adversaries,
5. **there is no evidence of collaboration between the public authorities located in the respective jurisdictions where each of the processors are located**, which would allow them access to all sets of personal data held by the processors and enable them to reconstitute and exploit the content of the personal data in a clear form in circumstances where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects. Similarly, public authorities of either country should not have the authority to access personal data held by processors in all jurisdictions concerned.
6. the controller has established by means of a thorough analysis of the data in question, taking into account any information that the public authorities of the recipient countries may possess, that the pieces of personal data it transmits to the processors cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

海外の事例③：PROMOTING DIGITAL PRIVACY TECHNOLOGIES BILL(117TH CONGRESS (2021-2022))

SEC. 2. DEFINITIONS.

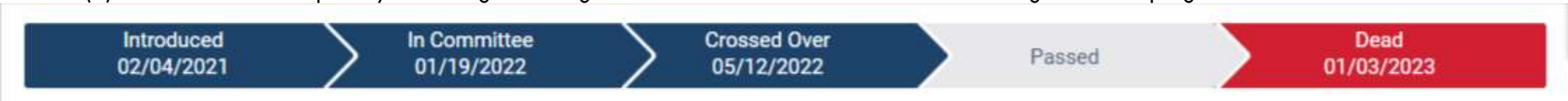
In this Act:

- (1) PERSONAL DATA.—The term “personal data” means information that identifies, is linked to, or is reasonably linkable to, an individual or a consumer device, including derived data.
- (2) PRIVACY ENHANCING TECHNOLOGY.—The term “privacy enhancing technology”—
  - (A) means any software solution, technical processes, or other technological means of enhancing the privacy and confidentiality of an individual’s personal data in data or sets of data; and
  - (B) includes anonymization and pseudonymization techniques, filtering tools, anti-tracking technology, differential privacy tools, synthetic data, and **secure multi-party computation**.

SEC. 3. NATIONAL SCIENCE FOUNDATION SUPPORT OF RESEARCH ON PRIVACY ENHANCING TECHNOLOGY.

The Director of the National Science Foundation, in consultation with other relevant Federal agencies (as determined by the Director), shall support merit-reviewed and competitively awarded research on privacy enhancing technologies, which may include—

- (1) fundamental research on technologies for de-identification, pseudonymization, anonymization, or obfuscation of personal data in data sets while maintaining fairness, accuracy, and efficiency;
- (2) fundamental research on algorithms and other similar mathematical tools used to protect individual privacy when collecting, storing, sharing, or aggregating data;
- (3) fundamental research on technologies that promote data minimization principles in data collection, sharing, and analytics; and
- (4) research awards on privacy enhancing technologies coordinated with other relevant Federal agencies and programs.



https://www.billtrack50.com/billdetail/1303148

海外の事例④：SECURING AMERICAN RESEARCH FROM CYBER THEFT ACT(117TH CONGRESS (2021-2022))

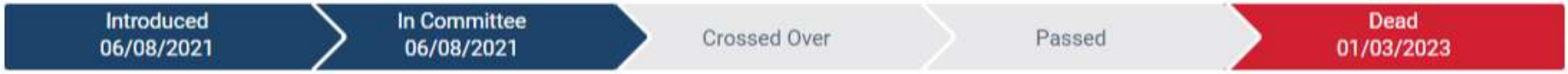
SEC. 2. PURPOSE.

The purposes of this Act are to help institutions of higher education protect federally funded research from cyber theft and interference by—

- (1) directing the Networking and Information Technology Research and Development Program to provide for support and guidance on improving the security of academic computing and networking systems that process, store, and transmit federally funded research; and
- (2) establishing a pilot program to support regional secure computing enclaves for academia to provide researchers with secure data storage and adequately protect Federal Government data.

SEC. 4. COMPUTING ENCLAVE PILOT PROGRAM.

- (d) Program Elements.—The Director shall work with institutions of higher education selected pursuant to subsection (b) to—
  - (1) develop an approved design blueprint for compliance with Federal data protection protocols;
  - (2) develop a comprehensive and confidential list, or a bill of materials, of each binary component of the software, firmware, or product that is required to deploy additional secure computing enclaves;
  - (3) develop templates for all policies and procedures required to operate the secure computing enclave in a research setting;
  - (4) develop a system security plan template; and
  - (5) develop a process for managing a plan of action and milestones for the secure computing enclave.



https://www.billtrack50.com/billdetail/1379770

2. 秘密計算と不正競争防止法

産業データの活用の観点からは，不正競争防止法（平成5年法律第47号）における営業秘密について，秘密計算技術を用いて互いに提供し，計算結果を得た場合であっても営業秘密の秘密管理性が失われないかという論点が存する。

限定提供データの技術的管理性についても同様に問題になりうる（なお2023年改正）。

秘密管理性は規範的な要件であり，秘密計算技術を用いて互いに提供する両当事者間において秘密保持契約等の契約上の措置が取られていたことで肯定されることがある。

秘密計算技術による相互の提供について，契約上の措置も加味すれば，秘密管理性が失われないという解釈は十分に可能であろう。

3. 今後の展望

プライバシー技術のうち，特に秘密計算や秘密分散について，総論では展開していこうという流れ（自民党，政府ともか）。

現時点では安全管理措置の一環でしかなく，「高度な暗号化」としてQ&Aや電子政府推奨暗号リストにも記載されていないが，「CRYPTREC 暗号技術ガイドライン（高機能暗号）」（2023年3月）には記載。

目的外利用や第三者提供の例外にはならない。壁は厚い。仮名加工情報＋共同利用が可能であれば，そこで利用すればよいが，ニュアンスは微妙。

OECDやICOの比較的新しい文書で再整理が試みられている。個人情報保護法の第二次3年ごと見直しでどう受け止めるか。