JEITA

IS－14－技標－ 1

情報セキュリティ調査報告書

2014年3月

一般社団法人 電子情報技術産業協会
情報セキュリティ調査専門委員会

はじめに

近年、ビジネス利用を目的としたビッグデータ活用が盛んになり、スマートフォン、タブレットやPC等、多様な端末を通じて得られる個人に付随する情報の、収集・保存・活用が拡大している。

一方で、ビッグデータ活用事案間で発生するデータ連携により個人が特定され、その結果として個人が知られたくない情報が流通してしまう等、プライバシーに関わる新たなリスクの発生が指摘されている。

このような状況を背景に、各国においては、プライバシー保護に関わる様々な規程やガイドライン、法制度等が整備されつつあるため、グローバルビジネスを展開する企業は、海外でのプライバシー情報利用時にこれらの動向に留意する必要がある。日本においても法改正の動きがあり、施行されれば国内で活動する企業にも対応が求められる。

本報告書は、情報セキュリティ調査専門委員会が、ビッグデータの活用に際して、企業が取り組むべき課題を提示し、対応する施策を提言するものである。報告書作成の過程では、企業によるビッグデータ活用事例、プライバシーデータ保護技術、プライバシーデータの取り扱いに関するユーザ意識、国内・国外のプライバシー保護に関する法制度化への取り組みを調査・分析し、課題の抽出及び施策検討を行った。

プライバシーデータの取り扱いに関するユーザの意識調査は、急速に変化する意識動向の把握に利用され、法制度化に向けた動きの解説は、リスクマネジメント計画策定時に参照されることを目的とした。また、取り組むべき課題と施策には、先進的な会員企業のノウハウを反映し、ビッグデータ活用計画策定時の参考になることを意図した。

本調査においてご協力いただいた企業の皆様、多くの情報と示唆をご提供いただいた有識者の方々、そして本委員会の関係者の皆様に深く感謝するとともに、本報告書が我が国産業界の競争力強化と事業拡大の一助となれば幸いである。

2014年3月

情報セキュリティ調査専門委員会
委員長　池田政弘

情報セキュリティ調査専門委員会名簿

（敬称略・順不同）

委員長	池田政弘	富士ゼロックス㈱
副委員長	白石節男	富士通㈱
委員	福島孝文	東芝テック㈱
〃	水島九十九	日本電気㈱
〃	武本敏	㈱日立製作所
〃	池田恵一	富士通㈱
〃	米田健	三菱電機㈱
〃	坂上勉	三菱電機㈱
〃	畠山有子	三菱電機㈱
〃	櫻井朝彦	三菱電機㈱
〃	濱田剛	三菱電機インフォメーションテクノロジー㈱
〃	平木博史	㈱リコー
〃	佐藤淳	㈱リコー
オブザーバ	川口修司	㈱三菱総合研究所
〃	江連三香	㈱三菱総合研究所
〃	阪口瀬理奈	㈱三菱総合研究所
事務局	稲垣宏	（社）電子情報技術産業協会
	志村昌宏	（社）電子情報技術産業協会

目次

第1章　現状認識

1.1 プライバシー情報をとりまく環境

携帯電話やスマートフォンで情報を調べ買い物し、さらに日常を写真とともにネットワーク上に記録し公開する昨今、企業はそれらの行動や記録から得られる様々な情報をマーケティング活動に活用するようになっている。一方でこのような企業活動が、プライバシーを侵害しているとの問題意識からトラブルに発展するケースも発生し、プライバシー情報をめぐる議論が活発になっている。

1.1.1 ビックデータのビジネス活用

情報通信技術の進展により多種多様のデータ（ビックデータ）が生み出されており、これらのデータを活用することにより業務運営の効率化や新たなサービス、新たな産業の創出が期待されている。総務省の調査によれば、ビッグデータ流通量は 7 年間で 5.5 倍と高い伸びを示し[1]、労働生産性の伸び率との間にプラスの相関関係があり、ビッグデータを活用することにより、業務効率化・付加価値向上など高い効果を発現する、としている。

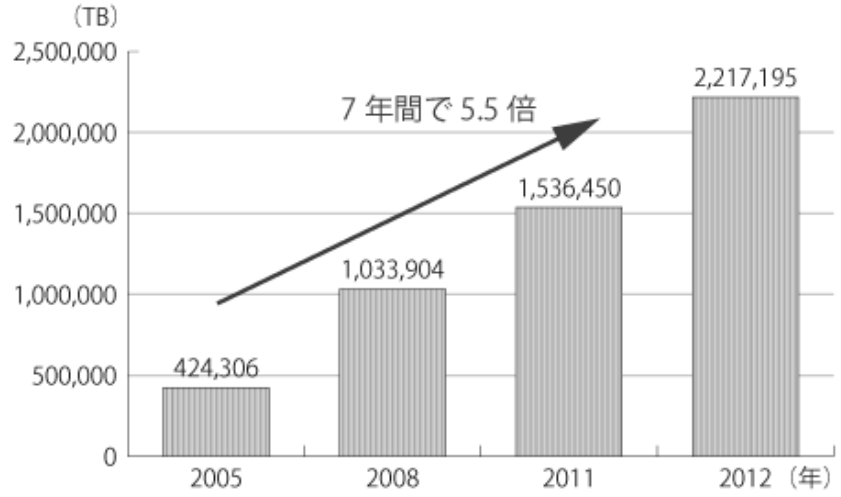


図 1.1-1 ビッグデータの国内流通量の推移 [1]

ビックデータに関わる情報として[2]多岐にわたる情報があるが、その中のソーシャルメディアデータ、マルチメディアデータ、ウェブサイトデータ、カスタマーデータ、センサーデータ、ログデータなどがプライバシー情報に該当する。利用者自身や社会のためになることに対しては、ネットワークを介してサービスを受けるのにいろいろなデータを登録し

[1] 平成 25 年度版　情報通信白書 http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/na000000.html
[2] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P.6

ているが、条件として自身で自身の情報を把握・管理できることを重視する意見が多い。サービス以外へのデータの利用に対しては、利用者は不安や抵抗を感じている。特に、肖像（写真）や（携帯電話やスマートフォンによる）位置情報、クレジットカードの使用履歴、Web サイトの検索履歴、ソーシャルメディアへの書き込みなど、活用が期待されるデータの 2 次利用に強い抵抗感を示している。

国際情勢としては、米国の消費者プライバシー権利章典の公開や EU の「データ保護規制案」採択（予定）、個人情報保護法制定の背景になっている OECD プライバシーガイドラインの 13 年ぶりの改正など、ここ数年プライバシーに関わる大きな動きがいくつもあった。

国内でも経済産業省の「IT 融合フォーラム　パーソナルデータワーキンググループ」の報告書の他いくつかの調査報告等が発表された。平成 25 年 12 月 20 日に政府、高度情報通信ネットワーク社会推進戦略本部で決定された「パーソナルデータの利活用に関する制度見直し方針」では、『個人情報及びプライバシーの保護を前提としつつ、パーソナルデータの利活用により民間の力を最大限引き出し、新ビジネスや新サービスの創出、既存産業の活性化を促進するとともに公益利用にも資する環境を整備する。さらに、事業者の負担を配慮しつつ、国際的に見て遜色のないパーソナルデータの利活用ルールの明確化と制度の見直しを早急に進める』としており、個人情報保護法改定等の制度の見直しが進められている。

1.1.2 トラブル事例

プライバシー情報を活用したビジネスはすでに数多く始まっており、プライバシーに関わるトラブルも少なからず発生している。トラブルとなる原因として主なものを 3 つ取り上げた。

① 第三者への閲覧可能性（権限）や譲渡が原因
② データを取得する際の説明不足
③ セキュリティ技術の問題

またこれらの原因が同時に複数発生していることもある。それぞれについて少し詳しく説明する。

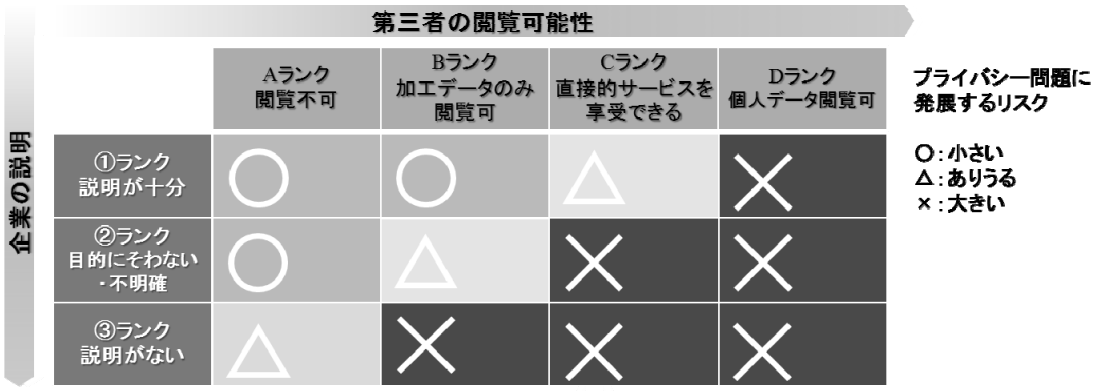
第三者への閲覧可能性（権限）や譲渡が原因となった例では、利用者の履歴を参照できるサービスで履歴情報を本人以外でも比較的容易に閲覧可能となっていた。オプトアウトはできたものの、プライバシー侵害の可能性が問題となり、発覚した後サービスは停止となった。

データを取得する際の説明不足による例として、ユーザのプロフィール等の個人情報が公開され、さらに利用履歴の閲覧の可能性もあったため批判が起きた。プライバシー設定の問題も含め、利用規約の概要等の不備があったという点が問題となったケースである。

セキュリティ技術の問題が原因の例として、利用者の想定対象外の個人情報を全てサーバで収集し、スパイウェアや情報漏えいプログラムのようであり、不正指令電磁的記録供用罪にあたる可能性を有する事例があった。さらに、通常セキュア通信で扱うような情報を平文で送っているなどセキュリティ上の問題があった。この例ではサービスを一時停止していたが、対策を施しサービスを再開している。

第三者の閲覧可能性と企業による説明の適切さがそれぞれの利用者のプライバシーに関する問題意識の強弱に影響する。2 つが組み合わされた時のリスクについて分類したものを表 1.1-1 に示した。

表 1.1-1　プライバシー問題のリスク[3]



第三者の閲覧可能性が高くなり、合わせて目的に沿った説明が不十分であるとトラブルになる可能性が高くなる。匿名化データや統計データでも第三者への閲覧可能性があり目的に沿った説明が不十分であることでトラブルとなっている。トラブルに発展した事例は、インターネットで話題が拡散し、情報が爆発的に増加「炎上」したケースがあり、一度「炎上」するとその後の対応が難しい。

[3] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P.18

1.2 消費者のプライバシーに対する意識

ビジネスのスピードが速く環境の変化も予測しづらい現状において、消費者のプライバシーに対する意識に応じながら、プライバシー保護に配慮した情報活用を行い、高い付加価値を生み出すビジネスを展開することが重要である。情報を活用したビジネスを展開するための方策について検討するためにも、情報の保護に対する消費者の意識を知るために、一般消費者に対してアンケート調査を実施し、プライバシー情報の保護やプライバシー情報を利用したサービスに対する意識の調査結果を示す。

1.2.1 プライバシー情報の利活用に対する意識

プライバシー情報に対する消費者の意識を調査するために、一般消費者に対して、日本全国の 20～60 代男女 500 名に対して Web によるアンケート調査を実施した[4]。

アンケート結果を単純集計してまずわかるのは、取り扱うプライバシー情報の種類により消費者の抵抗感が変化する点である。消費者のプライバイシー情報に対する抵抗感をまとめたのが図 1.2-1 である。プライバシー情報の種類として、①個人のステータス情報（例：保有資産、病歴・医薬品）、②個人の行動情報やプロフィール情報（例：会員カード、購買履歴、自身で編集可であるプロフィール）、③個人に関するが間接的な情報（例：GPS、ログ、音声・動画、温度）と分類して集計すると、取り扱うデータの種類により、消費者の抵抗感が変化することがわかる。プライバシー情報として何らかの保護を必要と考えている割合は、個人のステータスなどの機微な情報に対して 83.4%以上だが、個人に関するが間接的な情報であれば 75.0%未満である。直接的に個人を特定できない情報ほどプライバシー情報として強い保護を必要と考える割合は少なく、こうした情報を利用したサービスの利用意向も比較的に高い数値を示している。また、機微な情報、個人を特定できる情報ほどプライバシー情報として保護を必要と考える割合は多く、ビジネス利用への抵抗感も比較的強い[5]。

[4] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P.46
[5] 同上 P.49-51

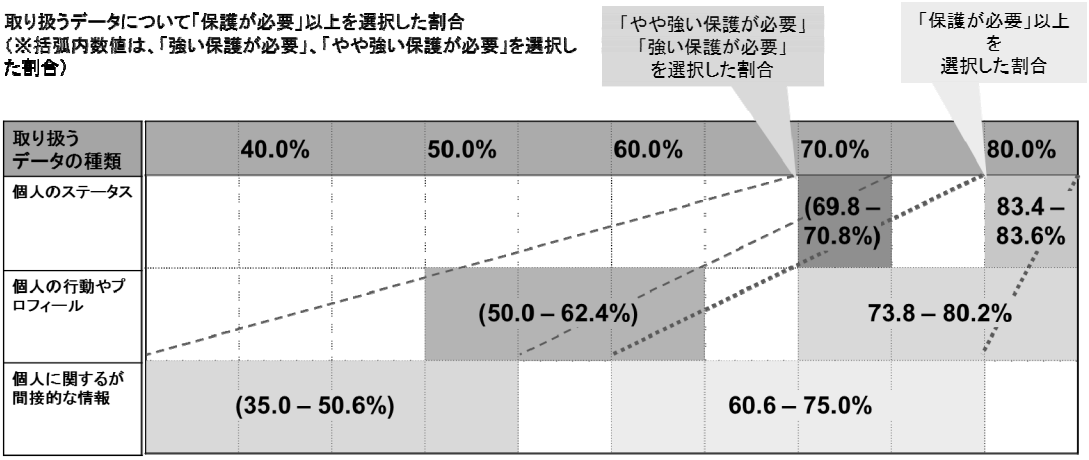


図 1.2-1 プライバシー情報としての保護の意向[5]

また、取り扱うプライバシー情報の種類によりその共有利用範囲についても、消費者の意向は差異を示した。図 1.2-2 にまとめているが、プライバシー情報の共有利用範囲の意向について、他組織提供型でもよいと考える割合はデータの種類によらず 30.6%未満で、中でも個人のステータスなどの機微な情報では 21.3%未満と抵抗感はより強い。プライバシー情報の共有利用範囲については、消費者がプライバシー情報を提供した組織が、その情報をさらに他組織へ提供する他組織提供型に消費者の抵抗感が強い。一方、消費者のプライバシー情報を提供する際、そのプライバシー情報を提供した組織のみで利用する自組織活用型については、抵抗感が比較的低い傾向がある。また、他組織提供型のビジネスモデルにおける利用条件については、個人を特定されないことを条件とする割合は高い[6]。実際に、プライバシー情報を用いたサービスで不快な経験があるという回答もあった。具体的には、求めていないサービスが勝手に提供された経験や、提供を意図していなかった情報が企業に送られていた経験である[7]。

[6] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P.54-56
[7] 同上　P.57

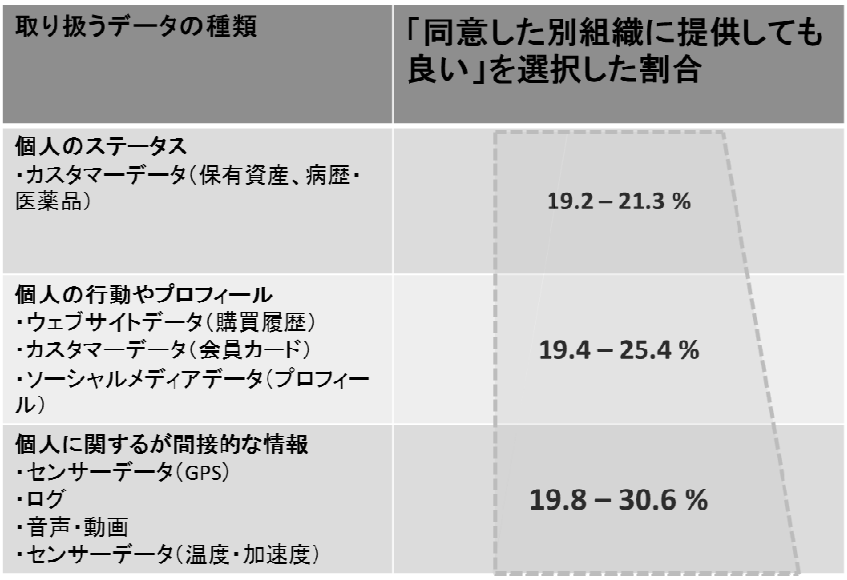


図 1.2-2　プライバシー情報の共有利用範囲の意向[8]

1.2.2 リスク情報の認知に基づく特徴

消費者のプライバシーに対する意識として、消費者の認知度が高いリスクは、企業のプライバシー情報管理体制に起因するものが多い。具体的には、消費者の 60%以上が下記のリスクを認知している。

・「プライバシー情報が、悪意のある第三者によって漏えいする」
・「プライバシー情報が、企業の不注意等によって漏えい・消失・紛失する」
・「自身の購買履歴や閲覧履歴等を用いて、企業から製品やサービスの勧誘がなされる」

こうしたプライバシー情報のリスクを知っていると答えたアンケート回答者は、いくつかの特徴がある。その特徴は、プライバシー情報に対して保護の意識が高いが、プライバシー情報を活用したサービスの利用意向も高いことである[9]。また、比較的インターネットの利用時間も長く、特にオンラインショッピングやオンラインバンキング・株取引を利用している割合も多い[10]。プライバシー情報の取り扱いに注意している人が多いことも特徴である。例えば、位置情報や写真等の情報を不用意にインターネット上にアップしないとか、サービス提供に不必要と思われる情報は企業に提供しないなど、情報の取り扱いに注意している人が多い[11]。

消費者がプライバシー情報を用いるサービスを利用する場合の企業に対する要望も強く、

[8] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P.51 に基づく
[9] 同上　P.60-66
[10] 同上　P.67
[11] 同上　P.68

中でも下記項目については 30%以上の割合が条件としている[12]。

・「情報の取り扱いについて、プライバシーポリシー等できちんと説明されている場合」

・「プライバシーマークや ISMS 等、第三者認証を得ている場合」

プライバシー情報を守る技術・対策の関心も高く、下記の技術・対策については 60%以上の割合が要望している[13]。

・「自身のインターネット上での行動履歴を追われない技術・対策」

・「インターネット上から自身のプライバシー情報を削除できる技術・対策」

[12] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P.70

[13] 同上　P.71

1.3 国内外の法制度について

到来しつつあるビックデータ社会に対応するため、「個人情報」から「プライバシー」の保護へと対応が必要となっている。欧米を始め諸外国では、プライバシー情報に関する議論が積極的に行われ、パーソナルデータの利活用が新産業創出など重要な役割を果たすと考えられており、関連法制度の見直しが加速している。アジアの国々でも個人情報保護についての関心が高まっており、個人情報保護法の制定が続いている。特にマーケティング目的で電話やファックスを送ることを規制したシンガポールの個人情報保護制度についても記載する。

1.3.1 EU データ保護指令の改訂について

2012 年 1 月、欧州連合の法案提出権を持つ欧州委員会は、欧州議会及び EU 理事会に新たなデータ保護規則の法案を正式に提出した。現 EU 指令の採択から 16 年以上が経ち、インターネットを初めとする急速な ICT 技術の進歩やグローバル化の進展により、新たな課題が浮かび上がっている。新たな法的枠組みの刷新が必要となり、また現在の法執行が 28 ヶ国の国内法により実施されていることで各国法の不整合により多大なコストが発生している。さらに、EU の憲法とも言えるリスボン条約に基本的人権として「プライバシー権」が独立した項目で記載されたため対応が必要と考えられている。

それらに対処するため、今回の EU データ保護規則案では、EU 域内の事業者に対する義務の追加、EU 域外の事業者に対する義務の新設、個人に対する権利などの新たな規制強化が盛り込まれている。また、EU 加盟国が各国内法にて対応する指令（directive）から、強制力を持ち EU 加盟国へ直接適用する EU 共通の法律である規則（regulation）に格上げされ、採択を目指して協議が進められている。

新たな EU データ保護規則案では、EU の域内・域外を問わず、EU に居住する個人のデータを取り扱う企業はこの規則の対象となる。情報サービスを提供する情報システム関係企業のみならず、EU に居住する個人に商品やサービスを提供する日系企業全般に影響が及び、日本企業の事業環境に与える影響は少なくないと想定される。

この法改正案により、日本企業特にクラウドサービスを手がける IT 関連企業や EU にサービスを提供する企業において、ビジネス上の制約やコスト負担が増えることが懸念されている。産業界にとっての大きな課題は下記 3 点である。

① データ移転制限によるグローバルな事業活動が制約を受ける
　→グローバル人材活用のための従業員データに関して日本本社への移転が困難に
② 事業活動の抑制や萎縮により、革新的なサービスの提供の妨げとなる
　→クラウドビジネス、データセンター運営、Web サービス等
③ EU 域内事業拠点を含め、強化規則対応のために多大な負荷が生じる

→例外規定対応への多大なコスト負担　等

2014 年 3 月時点で、EU データ保護規則案の審議状況は下記のとおりとなっている。大方の見込みでは 5 月の欧州議会選挙前の採択は難しく、2014 年末の採択を目指して作業が進められている模様である（適用はさらに 2 年後）。

- 欧州議会の LIBE 委員会の修正案が検討され 2013 年 10 月に投票が行われた。これにより欧州議会の合意形成がほぼ終了し、2014 年 3 月に議会本会議としての投票が行われた。
- 合わせて欧州議会と EU 理事会にて第一読会を行うことが予定されていたが、EU 理事会での規則案の修正案検討作業が遅延しており、3 月には完了しない見込み。法案化するために時間をかけて詳細検討しているようで、また 5 月の欧州議会選挙に影響を受けずに作業が進められている模様。特に、EU 理事会の議長国であるギリシャは任期である 2014 年 6 月には検討作業を終えたい意向のようであるが、やはり実際には作業は完了しない見込み。
- 欧州議会は 5 月に解散するため、それ以前に第一読会ができない場合には、継続審議ができず、欧州委員会が新法案ドラフトの作成までさかのぼる可能性が高い。
- また、2014 年 7 月からは欧州連合理事国の議長国がイタリアになり、7 月からは欧州議会、欧州理事会、欧州委員会との修正案を摺り合わせるための非公式な 3 極会議（Trilogue Meeting）[14]が行われる予定。

3 極会議を経て、イタリア議長国の任期である年末までには決着させ、2015 年 2 月には、28 ヶ国の言語に翻訳した正式文書として公表したい考えのようである。

[14] 欧州委員会、欧州議会、EU 理事会における水面下の非公式な修正案を巡る三者交渉。法案の行く末を左右する最も重要な会議。

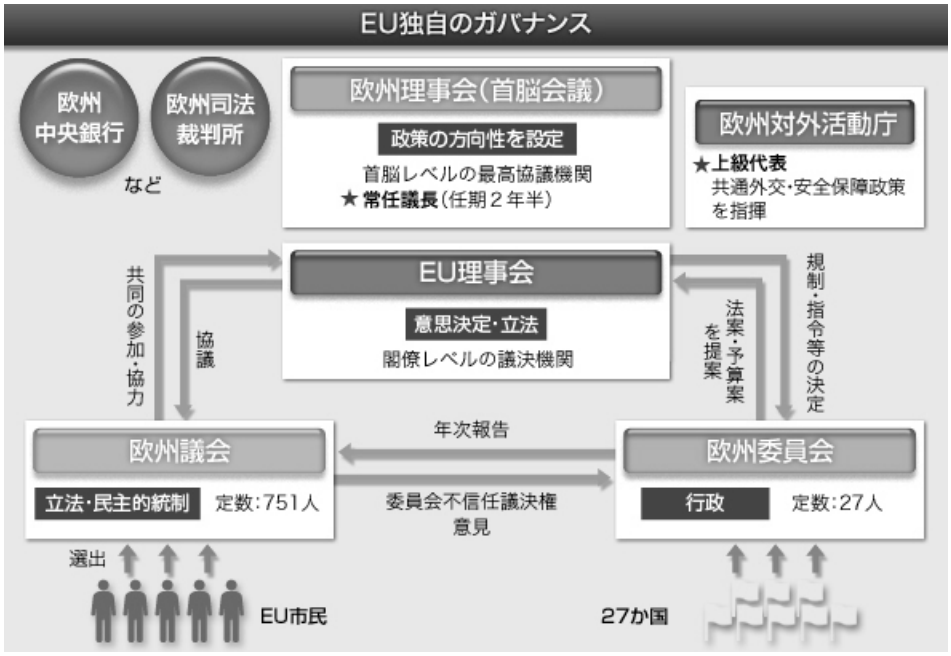


図 1.3-1　（参考）EU ガバナンス体制[15]

1.3.2 OECD プライバシーガイドラインの改正

1980 年 9 月に OECD で採択された「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」が、30 年後の 2013 年 7 月に改正され、2013 年 9 月に公開された。2008 年にソウルで開かれた閣僚会議で提起され、2010 年から作業がスタートし、昨年改定された。経済協力開発機構（OECD）「プライバシー保護と個人データの流通についてのガイドラインに関する理事会勧告（OECD プライバシーガイドライン）」は、OECD 理事会勧告として採択され、OECD は、先進 34 ヶ国（EU21 ヶ国＋域外 13 ヶ国）で構成され、ガイドラインは OECD 加盟国の指針となるものである。

OECD プライバシーガイドラインの「OECD8 原則」は以下の 8 つであり、この原則は、個人情報保護制度を整備するにあたって事実上の世界標準となっている。

① 収集制限の原則（適法かつ公正な手段によって個人への通知または同意を得て収集）
② データ内容の原則（データ内容の正確性、完全性、最新性を確保すること）
③ 目的明確化の原則（利用目的を明確にすること）
④ 利用制限の原則（その目的以外で利用は行わないこと）
⑤ 安全保護の原則（紛失や破壊、使用、改ざん、漏えいなどから保護すること）
⑥ 公開の原則（データの存在、利用目的や管理者等に関する情報を明示すること）

[15] 外務省　http://www.mofa.go.jp/mofaj/press/pr/wakaru/topics/vol53/

⑦　個人参加の原則(データ所在や内容確認ができ、異議を申し立てることを保証する)
⑧　責任の原則（個人データの管理者は、諸原則を実施する上での責任を有する）

今回の主な改正ポイントとしては、ICT 技術が高度化することで個人情報の取り扱いに変化が生じたため、その状況への対応が主な内容である。OECD プライバシーガイドラインは、個人情報の取り扱い及びプライバシー保護に必要な基本的事項を定めたガイドラインであり、プライバシーや個人情報保護、情報セキュリティ関係のガイドラインのベースになるものである。ガイドラインの対象範囲に従来と同様に、公的部門及び民間部門の双方に適用される。ただし、民間部門については全てのステークホルダが対象になっている。

また、ガイドラインに新たに追加された項目は以下のとおりである。OECD ガイドラインに、プライバシー・マネジメント・プログラムが明記され、その目的は、8 原則のうちの「責任の原則」を達成する上で必要な取り組みとして示されたものであり、マネジメントシステムに基づいて実施している民間事業者のみならず、官民を問わず全ての関係者における取り組みが要求されている。

■データ管理者の義務

・企業によるプライバシー・マネジメント・プログラムの導入
・セキュリティ違反時の通知

■加盟国の義務

・十分な権限を持ったプライバシー執行機関（DPA）の設置
・国家プライバシー戦略の開発
・教育と普及啓発の実施
・データ管理者以外の個人等の役割考慮
・国際的な取り決めの開発促進（米セーフハーバー、欧州の BCR、CBPR 等）
・国際比較可能な統計手続の開発促進

1.3.3 プライバシーに関する米国の動向

米国の個人情報保護法制は、業種や分野別に個別法を定める「セクター形式」を取っており、日本の個人情報保護法に相当する一般法はない。一般法がないことから、対応する個別法がない分野では、個人情報やプライバシー保護が事業者の裁量に委ねられている。個人に関する情報の利用は比較的自由な環境にある。特に、企業のデータ利用により個人が実際に不利益を被ることがなければ問題がない。また安全保障や経済発展などが、米国の国益にかなう要素があれば、プライバシーやデータ保護より優先されるという考え方である。

しかしながら、個人に関する情報を活用するビジネスが拡大する一方で、消費者のプライバシーを侵害する事件が増え、規制強化を要請する機運が高まってきた。オバマ大統領は 2012 年 2 月に「消費者プライバシー権利章典」(A Consumer Privacy Bill of Rights)を取りまとめた。消費者のプライバシー権を従来以上に明確化し、事業者の自主規制を促すこととした。同章典では消費者の権利を 7 つ定めている。①個人による管理、②透明性、③経緯の尊重、④セキュリティ、⑤アクセス及び正確性、⑥対象を絞った収集、⑦説明責任である。特に、①の自己情報コントロール権、③の消費者が意図した脈絡（コンテキスト）で、事業者による個人データやプライバシーに関わる情報の取り扱いがなされることを期待する権利などが特徴となっている。

米国連邦取引委員会（FTC：Federal Trade Commission）は 2012 年に「急速に変化する時代における消費者プライバシー保護」と題する報告書を作成した。これはプライバシー保護のための新しいフレームワークを提唱することを意味している。特に、①プライバシー・バイ・デザイン（Privacy by Design）、②消費者への簡潔な選択肢の提供（Simplified Choice）、③透明性の確保（Transparency）が主な内容となっている。また、そのフレームワークの適用対象を、特定の消費者、コンピュータ、その他のデバイスに合理的に結び付けられる消費者データを収集または利用する全ての事業者としている。ただし、例外的に年間 5000 名未満の消費者から機微でないデータを収集し、第三者と共有しない事業者は対象外としている。

また、そのフレームワークにおいて FTC3 要件と呼ばれる重要な保護措置を定義しており、その全てを実施している状況であれば保護対象外とするものである。つまり、特定の消費者またはデバイスに合理的に結び付けられることにはならないという解釈である。

■FTC3 要件

① 事業者はそのデータの非識別化を確保するために合理的な措置を講ずるべきである。

② 事業者は、そのデータを非識別化された形態で保有及び利用し、そのデータの再識別化を試みないことを、公に約束すべきである。

③ 非識別化されたデータを事業者が他の事業者に提供する場合には、その事業者がデータの再識別化を試みることを契約で禁止すべきである。

しかしながら、この FTC3 要件は米国内においても法令やガイドライン等で縛られていないため十分に機能している訳でもない。FTC の強力な権限執行に基づく考え方がそのベースとなっているが、現時点では単なる FTC の提案に留まっている。ちなみに日本においても、「日本版 FTC3 要件」なるものも検討されているが、②③だけでも法整備が必須であり、その実行においては課題が山積している状況である。

1.3.4 プライバシーに関する APEC の動向

APEC では、2004 年に APEC プライバシー原則を定め、これに基づく国内個人情報保護制度の策定を APEC 参加国・地域（エコノミー）に勧奨してきた。また一方で、ビジネスのグローバル化に伴い、個人情報が頻繁に国境を越えて移動する状況において、越境個人情報の保護が問題視されるようになってきた。APEC では、個人情報が国境を越えても APEC プライバシー原則に基づき保護されるよう、APEC 越境プライバシールールシステム（CBPR システム：Cross Border Privacy Rules system)CBPR システムを構築した。

2006 年から APEC の ECSG(電子商取引運営グループ)において検討が開始された。2007 年に閣僚会議の承認によって設置された「APEC データプライバシー・パスファインダー」において開発が進められた。2011 年 11 月の APEC 閣僚会合及び首脳会議において取りまとめられ公表された。

この制度は、企業等の越境個人情報保護に関する取り組みに対して APEC プライバシー原則への適合性を認証するものである。申請企業等は、自社の越境個人情報保護に関するルール、体制等に関し自己審査を行い、その内容について中立的な認証機関から認証審査を受け、APEC プライバシー原則を遵守していると認められた場合、認証を受けることができる。これにより、認定機関の認証を受けた企業等は自社の個人情報の取り扱いが APEC プライバシー原則に適合しているものであることを示すことが可能となる。ポリシーに対するコミットメントに違反した企業に対しては、各国のプライバイシー執行機関（DPA 等）が法執行を行う。このプライバシー執行機関は CBPR の要件と整合的な国内法令の下で法執行を行う能力が必要となる。また、参加国のプライバシー執行機関の少なくとも 1 つは「APEC 越境プライバシー執行のための協力取り決め（CPEA：APEC Cross-border Privacy Enforcement. Arrangement)」に参加していることが必要条件となる。

1.3.5 シンガポールの個人情報保護制度

シンガポールの個人情報保護法（PDPA: Personal Data Protection Act）は、事業者の個人情報の取得方法（収集、利用及び開示等）を規制する法律で、主な規定は 2014 年 7 月に発効された。個人情報を守るという個人の権利と個人情報の利活用のバランスが考慮されている。特に情報保護に関して、2014 年 7 月に 8 つの情報保護原則(The Data Protection Principles)が発効される。8 原則は、①同意、②目的、③アクセス権、④修正権、⑤正確性、⑥保護、⑦保持、⑧国外移転となっている。

また、2013 年 1 月に個人情報保護委員会（PDPC: Personal Data Protection Commission）が設置された。情報保護原則に違反した場合には、刑事または民事の処分が科せられ、個人情報保護委員会は最大 100 万シンガポールドルまでの罰金を科すことができる。

さらに、電話勧誘拒否登録制度（Do Not Call Registry）に関する規定も 2014 年 1 月に発効されている。

■電話勧誘拒否登録制度（DNC 登録：Do Not Call Registry）

シンガポールの民間事業者は下記 3 つの義務を遵守しなければならない。

① 登録確認として、事業者はシンガポールの電話番号にマーケティングメッセージを送付する際には事前に DNC に登録する必要がある。

② 連絡先の通知として、マーケティングメッセージには、送り主の明確かつ正確な連絡先の記載が必要である。

③ 電話番号非通知設定については、マーケティングメッセージは非通知で送ってはいけない。

1.3.6 日本の個人情報保護法等の改正について

2013 年 6 月に IT 戦略「世界最先端 IT 国家創造宣言」が閣議決定された。それを受けて、グローバルな競争を勝ち抜くために、新たな付加価値を創造するサービスや革新的な新産業・サービスの源泉とも言える「パーソナルデータ」の利活用に期待が高まっている。その戦略的な利活用により、全産業の成長を促進する社会の実現を目指すものである。

現在、IT 総合戦略本部の下に新たな検討組織が設置され、個人情報やプライバシー保護に配慮した「パーソナルデータの保護と利用」に関する検討が進められている。パーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し、同意取得手続の標準化等に取り組んでいる。新たな検討組織が、第三者機関の設置を含む、新たな法的措置も視野に入れた制度見直し方針が策定した。高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）は、2013 年 9 月より、「パーソナルデータに関する検討会」を 5 回開催し、匿名化の基準や独立した第三者機関の設置に向けた検討を行った。2013 年 11 月には、個人情報保護法制度の見直しに向けた提案がなされ、「パーソナルデータの利活用に関する制度見直し方針」が公表された。

また、パーソナルデータの利活用に関する制度見直しの方向性は、個人情報及びプライバシーを保護しつつ、パーソナルデータの利活用を躊躇する要因となっているルールの曖昧さの解消等を目指すものである。具体的には下記の 3 つがその見直し方針となっている。

■パーソナルデータ利活用に関する制度見直し方針

- ビッグデータ時代におけるパーソナルデータ利活用に向けた見直し
- プライバシー保護に対する個人の期待に応える見直し
- グローバル化に対応する見直し

さらに、パーソナルデータの利活用に関する制度見直し事項は下記のとおりである。

■パーソナルデータ利活用に関する制度見直し事項

- 第三者機関（プライバシー・コミッショナー）の設置
  独立した第三者機関を設置し、パーソナルデータの保護と利活用をバランスよく推進する観点から、分野横断的な対応を迅速かつ適切にできる体制を整備する。
- 個人が特定される可能性を低減した個人データの個人情報及びプライバシー保護
  個人情報及びプライバシー保護に配慮したパーソナルデータの利用・流通を促進する
- 国際的な調和を図るために必要な対応
  欧米のパーソナルデータ保護の法制度に追従するために下記内容の対応を検討する。
  ①諸外国の制度との調和、②他国への越境移転の制限、③開示、削除等の在り方、④パーソナルデータ利活用のルール遵守の仕組みの構築、⑤取り扱う個人情報の規模が小さい事業者の取り扱い、⑥行政機関、独立行政法人等及び地方公共団体が保有する個人情報の取り扱い 等

プライバシー保護等に配慮した情報の利用・流通のために実現すべき事項として、①パーソナルデータの保護の目的の明確化、②保護されるパーソナルデータの範囲の明確化、③プライバシーに配慮したパーソナルデータの適正利用・流通のための手続等の在り方、を検討することとなった。

2014 年 3 月末時点で、個人情報保護法等の改訂に向けた法案化の状況は下記のとおりとなっている。

- 2014 年 6 月の大綱決定・公開に向けて、内閣官房内に「パーソナルデータ関連制度担当室」が設置され、内閣法制局とも連携しドラフト作成を進めている。
- 2014 年 3 月から再び、パーソナルデータに関する検討会が開催され、有識者によって課題に対する技量や法案内容の審議が行われる見込み。
- 大綱決定後にはパブリックコメントが募集され、その後法案作成され 2015 年 1 月の通常国会に法案提出されるのが最短スケジュールとなっている。

表 **1.3-1**　全世界的なデータ保護制度見直しの動き[16]

EU	・1995 年　EU データ保護指令　採択 ・2012 年 1 月　EU データ保護規則案　公表 ・2013 年 10 月　欧州議会 LIBE(司法委員会)の修正案　採択 ・2014 年 3 月　欧州議会の本会議にて投票実施
OECD	・1980 年　プライバシーガイドライン　採択 ・2013 年 7 月　プライバシーガイドライン　改定
米国	・1974 年　プライバシー法（連邦行政機関を対象）　制定 ・1998 年　児童オンラインプライバシー保護法　成立 ・2012 年 2 月　消費者プライバシー権利章典　公表 ・2012 年 3 月　FTC のプライバシー・フレームワーク　公表
カナダ	・1978 年　カナダ人権法　制定 ・1982 年　プライバシー法　制定 ・2000 年　個人情報保護及び電子文書法　制定
APEC	・2004 年　APEC プライバシー・フレームワーク　採択 ・2011 年　越境プライバシールール（CBPR）　採択 ・2013 年 6 月　CBPR に日本が参加申請
シンガポール	・2013 年 1 月　個人情報保護委員会　設置 ・2014 年 1 月 電話勧誘拒否登録制度（Do Not Call Registry）　発効 ・2014 年 7 月 個人情報保護法（PDPA: Personal Data Protection Act）発効予定
日本	・2003 年　個人情報保護法　制定 ・2013 年 6 月　「世界最先端 IT 国家創造」宣言 ・2013 年 12 月　「パーソナルデータの利活用に関する制度見直し方針」

[16] 国際社会経済研究所「個人データ保護の国内外動向とデータ利活用に向けた取り組み」(2013/10/03) (http://www.i-ise.com/jp/study/pdf/20131003.pdf)の表をもとに作成

1.4 技術動向

積極的にインターネットを利活用するに当たって、利用者はプライバシーが守られないのではないかと、脅威を感じている。本節においては、プライバシー保護等に配慮した情報の利活用のために必要とされる基礎技術、及び応用技術をまとめる。

1.4.1 基礎技術

プライバシー保護に関わる基礎技術としては、(1)アクセス制御、(2)暗号化、(3)匿名化、(4)秘密分散などが挙げられる。

(1)アクセス制御技術

アクセス制御技術は、データを参照する権限をある特定の人に制限する技術であり、現在広く使用されている技術である。管理者などアクセス権限を持つ人にデータの内容が見えてしまう課題がある。

(2)暗号化技術

暗号化技術は、データを鍵で変換し、第三者に対してデータの内容を秘匿するための技術である。歴史的にも戦時下などにおいて、機密性の高い通信を用いる場面で利用されてきた。暗号化･復号には鍵が必要であり、その鍵の管理の方法で、共通鍵暗号方式と公開鍵暗号方式に分けられる。前者の方式は性能的に優れているが、共通鍵を持っていないと対象データを復号することができないので、データを共有する分野には不向きである。一方公開鍵暗号方式においては、性能は共通鍵方式に劣るものの、データを共有という観点では優位性がある。公開鍵暗号の一種として ID ベース暗号がある。ID ベース暗号は、利用者の識別可能な一意な情報（例えばメールアドレス）を元に、利用者の公開鍵を生成するものである。本方式では、利用者の公開鍵の管理や配布をしなくてよいメリットがある。

(3)匿名化技術

匿名化技術は、個人情報における「個人を特定しにくくする加工を行う」技術である。加工方法には大きく分けて、氏名等の個人識別情報を削除した仮名化、氏名等の個人識別情報を削除し元の情報と対応できないようにした無名化がある。さらに、k-匿名化のように、特定の個人を識別することが困難にする加工を行う高度な匿名化技術がある。これらの技術はプライバシー保護を進めながらも、データの利活用を進めたいニーズに基づき研究されてきた。

なお、匿名化については、IT 総合戦略本部が進めるパーソナルデータに関する検討会に

おいて、以下のように整理されている[17]。

① どのような個人情報に対しても、「一人ひとり識別されるが個人が特定されない状態」、または、「一人ひとりが識別されない状態」となるような汎用的な匿名化を行う加工方法はない。

② 汎用的な匿名化を行う加工方法はないが、個人情報の種類･特性と適用する加工方法を選択することで、匿名化に近づける加工は可能である。

③ インターネット等の発展により、異なる情報源からの情報を組み合わせることにより、個人情報を識別できる可能性は高まっている。

(4)秘密分散技術

秘密分散技術は、情報をいくつかの分散情報に分け、格納する仕組みである。格納された情報は個別では意味を持たないため、プライバシー保護の観点から有用な技術として応用されてきた。

1.4.2 応用技術

一般的にデータの機密性を確保するためには暗号化や秘密分散等を用いるが、データ処理の際には元に戻さなければならず、そのタイミングを狙った不正アクセスが発生している[18]。プライバシーデータの処理にクラウド・コンピューティングのように他者が介在するリソースの活用を考える場合には、特に注意しなければならない。そこで、暗号技術を応用して、データを秘匿したままデータ処理を行う技術が研究開発されている。

(1)検索可能暗号化

検索可能暗号技術は、DB 上のデータを暗号化したまま検索可能とする技術である。

共通鍵暗号を使用した検索可能暗号化技術として、日立製作所は 2012 年 3 月に「クラウド上での情報漏えい防止に貢献する検索可能暗号化技術」[19]を発表した。

同技術は、共通鍵暗号方式をベースにすることにより、平文でのデータベースでの検索とほぼ変わらない高速処理を実現している。

また、同一の内容を持つデータを暗号化した場合に暗号文が一意となってしまう場合には、頻度分析などのリスクが高まり、安全性に不安があった。しかし、同技術では毎回異なる乱数を用いることにより、同一の内容を持つデータであっても異なる暗号文になるようにランダム性を高め、準同型暗号技術を応用して異なる暗号文の比較を実現することにより、安全性を確保している。

---

[17] 第 5 回パーソナルデータに関する検討会資料 2-1　http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf
[18] IT Pro 日経コンピュータ　http://itpro.nikkeibp.co.jp/article/COLUMN/20101119/354336/
[19] 日立製作所　http://www.hitachi.co.jp/rd/portal/news/y/2012/0312.html

公開鍵暗号を使用した検索可能暗号化技術として、富士通は 2014 年 1 月に「暗号化したままデータ分析を行う秘匿分析技術」[20]を発表した。同技術は、全ての文字列を暗号化した状態で検索する技術である。暗号化したまま統計処理などの演算が行える準同型暗号の技術をベースに、1 回の処理で暗号演算を同時に行えるように改良した。これにより、文字列全体に含まれる検索キーワードの一致判定を一括して行え、暗号化したまま、16,000 字を 1 秒以内で検索を可能とした。

(2) 秘匿計算

秘匿計算とは、利用者が秘密に保持している情報を、他の実行者に見せずに情報の処理や、分析を可能とする方式を言う。

本技術の応用として、NEC は 2013 年 11 月に「データベースの情報を暗号化したまま処理できる秘匿計算技術」[21]を発表した。同技術においては、広く普及しているリレーショナルデータベースに適用でき、データベース側でデータが復号化されることを防ぐ秘匿計算技術を実現した。

また、日立製作所は 2014 年 1 月に「暗号化したままデータ分析が可能な秘匿分析技術」[22]を発表した。同技術においては、暗号化されたデータを復号することなく、頻度集計、相関ルール分析が可能にしている。これにより、10 万件規模の暗号化されたデータに対して約 10 分間で相関ルール分析を可能としており実用的な高速性を有している。2014 年中に医療分野での実証実験を行い、2015 年度中の実用化を目指している。

(3) 秘密分散

秘密分散を使用した実証実験について、日本成人白血病治療共同研究グループと NTT は 2012 年 2 月に「医療統計処理における秘密計算技術を世界で初めて実証」[23]を発表した。秘密分散でデータを保管することで、データの機密性を担保したシステムを構築した。

1.4.3 応用例

(1) マイナンバー

「行政手続き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」(番号法)で導入される番号制度は、納税者の「公平・透明・納得」を目指し、正しい所得把握体制を築くために必要不可欠とされている。税の徴収や社会保障の給付に有効であるものの、国民一人ひとりに一意の番号を付与するため、番号によって個人の情報が名寄せされる恐

[20] 富士通　http://pr.fujitsu.com/jp/news/2014/01/15.html
[21] 日本電気　http://jpn.nec.com/press/201311/20131106_01.html
[22] 日立製作所　http://www.hitachi.co.jp/New/cnews/month/2014/01/0121b.html
[23] NTT　http://www.ntt.co.jp/news2012/1202/120214a.html

れがあり、個人情報保護の観点からは番号は注意深く取り扱う必要がある。2010 年 5 月に内閣官房 高度情報通信ネットワーク社会推進戦略本部がまとめた「新たな情報通信技術戦略」[24]では「社会保障・税の共通番号の検討と整合性を図りつつ、個人情報保護を確保し府省・地方自治体間のデータ連携を可能とする電子行政の共通基盤として、2013 年までに国民 ID 制度を導入する。」とされており、番号制度導入にあたって個人情報保護に配慮することが明記されている。

内閣官房　社会保障改革担当室が 2013 年 11 月に公開した「情報提供ネットワークシステム等の設計・開発等業務　調達仕様書（案）」では、番号の付番を行うコアシステムや、番号を使って情報連携を行うためのインタフェースシステムなどの仕様が記載されているが、個人情報を保護するため以下を定めている。

- 保護すべき情報に対してアクセス制御を行うことに加えて、保存された情報を暗号化すること。
- マルウェア対策や不正アクセス、侵入検知・通知を行う機能を有すること。
- 個人情報を一元的に管理することができる機関または主体が存在しないことを担保するため、情報提供ネットワークシステムの中で個人を特定するために使用する機関別符号は、情報照会・提供機関毎に異なるものとし、情報提供ネットワークシステムにおいて発行・管理する。
- 機関別符号は住民票コードを基に、複数機関の機関別符号間、また同一機関の複数者の機関別符号間が容易には推測できない手段で生成されること。
- 機関別符号の生成過程の中間符号等から住民票コードへの変換ができないこと。

調達仕様書（案）に記載されたスケジュールでは、2015 年 10 月に国民に個人番号を通知し、2016 年 1 月から制度を開始。2017 年 1 月から情報照会・提供機関間の連携を開始することとしている。

(2) 情報銀行

情報銀行とは、個人が自分の活動情報を「銀行口座」に蓄積・管理し、プライバシーを守りながら自分や社会・産業のために高次利用することを可能とする社会的な仕組みである。個人が全ての情報にアクセス可能な唯一の主体であることに着目し、本人の管理の下で様々な事業者に散在する活動情報を統合（名寄せ）し、本人の承認を通じて様々に利活用する仕組みを提供する。

[24] 新たな情報通信技術戦略：http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf

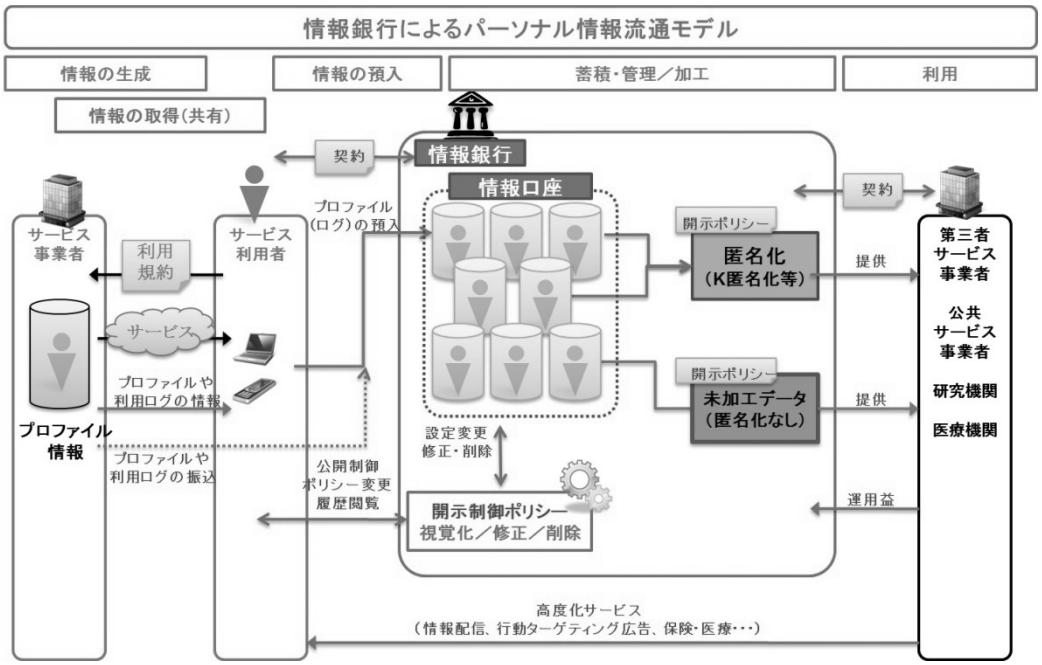


図 1.4-1　情報銀行の概念図[25]

1.4.4 プライバシー保護技術の方向性

プライバシー保護技術について、現在盛んに研究・開発が進められているのは、暗号化技術・匿名化技術の分野である。特に近年、検索可能暗号や秘匿計算の様に暗号化した状態のままデータ処理を行う技術の実用化が近くなっており、プライバシー保護への活用が期待されている。しかし、現在の検索可能暗号では範囲検索や大小比較、あいまい検索など、通常の検索であれば当たり前に利用できる検索ができないなどの制約や、秘匿計算においては演算のバリエーションや演算可能回数に制約がある。さらに、検索可能暗号と秘匿計算に共通する問題として演算性能やデータ量増加の課題があり、適用範囲が広がらない要因になっている。今後は、暗号化したまま処理する技術について、より柔軟に、より高速に行える方向に研究が進むものと思われる。

暗号化技術などが進歩する一方で、ほとんどの利用者は、データの利活用にリスクを感じ続けている。これは利用者個人が、自己の情報自体をコントロールできていないことに起因しており、アンケート結果[26]を踏まえ、ニーズに応える技術開発が期待される。例えば現在、情報銀行という考え方も出てきており、今後利活用の基盤となる可能性もある。

[25] 東京大学　柴崎研究室　http://shiba.iis.u-tokyo.ac.jp/research/contextaware/pdf/infobank.pdf
[26] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P58

第2章 ビッグデータ活用における課題

2.1 ビッグデータ活用計画策定時

ビッグデータ活用計画策定時の不備により、サービスの中止に追い込まれたり、企業が倒産したりする事例が発生している。このような事例が多発すると、ビッグデータ活用ビジネスの萎縮やデータアナリスト育成の阻害要因となり得る。

そこで本節では、実事例をベースに、ビッグデータ活用計画策定時に何が課題になり得るのかを示す。なお、実際のトラブル事例については、別紙を参照されたい。

2.1.1 運用に関する課題

(1) リスクコミュニケーション[27]不足

ビッグデータ活用ビジネスの実運用に際して、ステークホルダへの説明が不十分であったり、誤りであったりしたことから社会問題化し、サービスの中止や中断に至った事例がある。特に、データの第三者提供がある場合や、ステークホルダの人数が多い場合に、問題が顕在化する傾向にある。

現行の法制度上の遵法性には問題がない場合であっても、事業者による説明が不足したことから、ステークホルダの「気持ち悪さ」を誘発してしまう事例がある。これは、ビッグデータ活用ビジネスに限らずに発生する課題である。その解決策として、例えば、事故発生時に環境に大きな影響を与える様な大規模な公共事業を行う際には、環境影響評価を含む環境アセスメントの手続が法制度化されているが、IT 関連の事業について同様の制度は存在しないため、評価手続の制度化といった方法も考えられる。

(2) 体制の不備

ビッグデータ活用ビジネス検討の際に、事業者内に有識者等により構成される独立した第三者機関が存在しなかったことにより、プライバシー保護に関する検討が必要十分でなかったり、対外的な対応を見誤ったりして、サービスの中止や中断に至った事例がある。

ビッグデータ活用ビジネスは、まだ発展途上であるため成功事例・失敗事例が少なく、有識者も社内・社外を含めて、必要十分には存在しないのが現状である。今後のビッグデータ活用ビジネス進展のためには、社会全体としての有識者の育成が急務である。

---

[27] リスクコミュニケーションには様々な定義があるが、ここでは当該ビッグデータ活用ビジネスのリスクに関する正確な情報を、公的機関、有識者、企業、一般市民などのステークホルダで共有し、相互に意思疎通を図ることをいう。

(3) コンプライアンス・企業モラルと世論の違い

ビッグデータ活用ビジネス検討の際に、現行の国内法制度への遵守のみを検討したことにより、結果として世論の反感を買い、サービスの中止や中断に至った事例がある。これは、現行の法制度が世論に追いついていないことも 1 つの原因である。

また、国内外の現行法制度等に照らし合わせた場合に、取り扱いが難しく社会問題化した事案もある。このような場合に迅速に見解を示す公的機関がないことも課題である。特に、近年の IT を活用したビジネスでは、データ越境が問題になる場合があり、慎重な判断が求められる。

2.1.2 技術適用に関する課題

プライバシー情報を含むビッグデータ活用ビジネスを提供する際の技術適用の不備により、社会問題化し、サービスの中止や中断に至った事例がある。これには、大きく分けて 2 種類ある。1 つは、初歩的な暗号化やデータ開示範囲に関する設計ミスにより、プライバシー情報の開示範囲が意図とは異なる実装となっていた場合である。もう 1 つは、企業が考えるプライバシー保護対策と、世論の考えが異なっていた場合である。

これは、ビッグデータ活用ビジネスへのセキュリティ技術の適用に関する考え方が整理されていないことに問題がある。適用される可能性のある技術の整理や、ビッグデータ活用ビジネスの類型化[28]がないことから、混乱が生じているのではないかと考えられる。

また、国内外の業界団体や標準化団体による大きな動きがないことも、課題となっている可能性がある。例えば、クラウド・コンピューティングの黎明期や、スマートフォンの普及期には、それぞれのセキュリティを検討する団体・組織が複数設立され、検討の主導権を握っていたが、ビッグデータ活用ビジネスにはその主導する組織が存在しない。

[28] クラウド・コンピューティングの黎明期には「SaaS」「PaaS」「IaaS」の 3 類型が示され、様々な検討が進められた。現在ではこの類型に当てはまらない多種多様なクラウド・コンピューティングサービスが提供されているが、この類型化はセキュリティ検討には十分に役に立ったのではないかと考えられる。

2.2 ビッグデータ活用時

情報通信技術により、膨大なプライバシーデータを収集し、容易にビジネス活用できるようになった。ビッグデータ活用ビジネスでは、業務データ他に大量の個人データを収集・活用し、ビジネスの将来予測やそれに基づいた業務運用の効率化、新規領域のビジネスへの展開につなげている。大量の個人データには、住所・氏名などの情報の他に、人の行動や社会活動などプライバシーに関する情報も含まれており、従来以上に取り扱いに注意しなければならない。

本節では、ビッグデータを活用する時に発生する課題について示す。

2.2.1 ビッグデータの活用時の課題

ビッグデータの中には取引データや顧客管理データなど直接ビジネス活動により得られるオペレーションデータの他に、人の行動や活動に関するプライバシー情報が含まれている。プライバシー情報は、ソーシャルメディアデータ、マルチメディアデータ、ウェブサイトデータ、カスタマーデータ、センサーデータ等から得られる。

個人情報は、個人情報保護法により定義されている[29]が、プライバシー情報に関しては法的には定義されていない。判例等によるとプライバシーは「他人にみだりに知られたくない情報」とされている。また、「他人にみだりに知られたくない」という抵抗感に対する基準は個人個人により大きく異なることが多い。一般的に、情報提供者が情報提供にあたって抵抗感や不安感を与える情報はその人にとってのプライバシー情報と考えて取り扱うべきである。

ビッグデータを円滑に活用するためには、情報提供者に対して抵抗感や不安感を与えず、データを提供してもらうことが重要である。このためには、データの収集方法がプライバシーの侵害を発生させないように実施されていることと、データ管理が適切に実施されていることを「見える化」する必要がある。

このような環境であれば、データアナリストが収集された様々なデータを活用して、新しい価値を見出し、新しいビジネス創造に結び付けられると考えられる。

2.2.2 事業者内の体制に関する課題

ビッグデータ活用ビジネスでは、「データの収集・取得」、「データの利用・管理」、「サー

[29] 個人情報保護法　第二条による定義
http://www.caa.go.jp/seikatsu/kojin/houritsu/index.html
第二条　この法律において「個人情報」とは、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。）をいう。

ビス事業者へのデータ提供」のフェーズがある。これらの各フェーズでプライバシーに関連した情報の提供への抵抗感や不安感を減少させ、信頼感や安心感を持ってもらうことで、より多くのデータを提供してもらえる。これらの各フェーズで法的に要求されている事項は表 2.2-1 のとおりである。

表 2.2-1 プライバシー情報保護のための法的要求[30]

収集・取得	利用・管理	提供
・実名でログインしている場合、識別性の要件を満たすため、**閲覧履歴等の端末情報は個人情報に該当し**、個人情報保護上は、**利用目的の特定、明示が必要**。（許諾は不要） ・他人に知られたくない情報の、**無断取得、提供行為等は差し止め・損害賠償**の対象。（プライバシー権の保護） ・個人識別性を満たさなくても、**端末識別性がある場合**（他の情報を結び付くことで個人識別性を持つ可能性）に注意。	・個人情報保護上、**利用目的の達成に必要な限度に限られる**。個人データ利用目的の範囲内で**正確・最新の内容**に保つように努め、**安全管理のために必要・適切な措置を講じ、従業員及び委託先を監督**する義務を負う。 ・安全管理を怠って情報漏えいを起こした場合には、**個人情報保護法による命令対象**となるほか、**プライバシー権の侵害として本人に対し損害賠償責任**を負う。 ・データ利用過程で匿名化してしまえば、個人情報は適用されないが、**他の情報と容易に照合して識別可能な形で匿名化するだけでは足りず、完全匿名化**しなければならない。プライバシーとの関係でも同様。	・個人情報保護法上、提供について事前に本人の同意を**取得**するか、提供に先立って**匿名化**しておく必要がある。

ビッグデータ活用事業者は、プライバシー侵害のリスク回避のために、表 2.2-1 の法的要求を満足させる必要がある。

2.2.3 対策基準に関する課題

プライバシー侵害のリスクを回避するために必要な、法的要求は表 2.2-1 のとおりであるが、これらを一律に満足する具体的な基準は存在していない。データ取得者元（収集・取得）、ビッグデータ保有者（利用・管理）、サービス提供者（提供）の各プレイヤー間の利害関係が複雑に絡まり合っていることと、同じプライバシー情報を取得するにしても様々な入手方法（流通経路）があり対応は複雑となるなどのことから、一意に基準が決めらない。このため、案件毎に必要な基準が得られるような方策が必要である。そして、その基準に従ってシステムやビジネスが運用されていることを常にチェック（監査）することが必要となってくる。

近年、プライバシー保護を検討するための概念としてプライバシー・バイ・デザイン(PbD ：Privacy by Design)[31]が注目されている。PbD には 7 つの基本原則があるが、対策としてどのようなものを入れるのか、何を考えればよいのかを提示するに留まり、具体的な基準は提供されていない。

[30] 三菱総合研究所「企業におけるプライバシー情報活用と情報セキュリティ対策に関する調査報告書」P.13

[31] Privacy by Design http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-japanese.pdf

2.3 トラブル発生時

政府の「パーソナルデータに関する検討会」でも議論されていたように、現行の個人情報保護法では、制度上の曖昧さがあり、「1.1.2 トラブル事例」にもあるとおり、法律上の義務を遵守したとしても、事業者がプライバシーに係る批判を受けるケースが見受けられる。

このようなトラブル発生により、企業イメージの毀損、信用失墜、ビジネス機会の損失など、ビジネスに悪影響を与えることが懸念される。従って、ビッグデータ活用ビジネスの推進にあたっては、何らかのトラブル発生を想定し、事前に対策を講じておくことが課題となってくる。

本節では、ビッグデータ活用ビジネス推進時のトラブル対応にあたっての課題について示すものである。

2.3.1 トラブル対応に向けた課題

ビッグデータ活用ビジネス推進時に発生し得るトラブルへの対応にあたっては、以下のような項目が課題となってくる。

① ビッグデータ活用ビジネスを推進するにあたってのリスクの把握
実施しているビジネスにおいて、どのようなリスクが存在するかを事前に把握しておく必要がある。

② トラブル対応のための体制の整備
トラブルの早期検知、早期収束のために必要な組織（人材）、連絡ルール（タイミング）／ルート等を整備しておく必要がある。

③ トラブル対応のためのルール策定
整備した体制で円滑なトラブル対応ができるようルールを策定する必要がある。

④ トラブル早期検知の仕組みの構築
トラブルの早期収束のために、トラブルを検知する仕組みを構築する必要がある。

⑤ トラブル拡大防止
トラブルの影響拡大を防ぐために、顧客への情報発信の仕組みや相談窓口を整備する必要がある。

⑥ トラブル再発防止に向けた取り組み
トラブル再発防止のため、発生したトラブルについて分析し、サービス提供にあたっての課題を明確にする必要がある。

⑦ トラブル事例の共有
効果的な対策実施のため、発生したトラブルを事業者間で共有する仕組みの構築が必要となる。

これら課題に対する具体的な対策については、「3.3 トラブル発生時」に記載する。

第3章　提言

3.1 ビッグデータ活用計画策定時

ビッグデータ活用計画策定時には、セキュリティ・バイ・デザインやプライバシー・バイ・デザインの考え方が欠かせない。費用対効果の高い計画策定のためには、セキュリティ運用と技術適用がバランスよく設計されていること、それらが全てのステークホルダに対して透明性を持っていることが重要である。

そこで本節では、運用設計・技術適用に関する、JEITA 会員企業及び国や公的機関に対する提言を行う。

3.1.1 運用設計に関する提言

(1) リスクコミュニケーション

プライバシー情報を含むビッグデータ活用計画の策定には、「データ発信者」「データ収集者」「データ分析者」「分析結果利活用者」「有識者」「国や公的機関」等のステークホルダの同意が重要となる。特に 1 章で述べたとおり、取り扱うデータの種類や、各ステークホルダへのメリットの大小により、その抵抗感が変化することがわかっており、ビッグデータ活用者（受益者）による適切な説明と同意が鍵となっている。

この同意のためには、特に「データ発信者」へのメリットが小さい場合には、以下のような項目を実施することが重要である。

・類似事例調査[32]・市場動向調査[33]
・プライバシー影響評価（Privacy Impact Analysis）、影響低減施策の検討
・各ステークホルダとの同意（アセスメント）
・有識者へのヒアリング調査、コンシューマ向けアンケート調査、その他

これらの項目における作業を軽減させる方法として、サービスに関するプライバシーポリシーの公開[34]や、情報セキュリティ報告書などの活用が考えられる。特に企業内のセキュリティ対策やプライバシー保護の取り組みを公開することは、本節冒頭に述べた透明性の確保の重要な支援となる。また、2.1.1 節でも述べたとおり、環境アセスメントの手法やノウハウは参考になり得ると考える。

---

[32] 例えば、HIPPA プライバシー保護、カナダ・オーストラリア等における健康・医療分野のパーソナルデータ保護制度等における手順や考え方が参考になると考えられる。

[33] 例えば以下の先進事例がある。
日立と博報堂、「ビッグデータで取り扱う生活者情報に関する意識調査」を実施：
http://www.hitachi.co.jp/New/cnews/month/2013/05/0527.html

[34] 例えば以下の先進事例がある。
ビッグデータ利活用事業におけるプライバシー保護のための取り組みを強化：
http://www.hitachi.co.jp/New/cnews/month/2013/05/0531.html

さらに、1 章に述べたとおり、プライバシー保護に関する各国法制度が異なるため、国際的なビッグデータ分析を行う場合には、専門家を含めた検討が重要である。

ただし、これらの手順を全てのビッグデータ活用計画者が実施することは非効率であり、場合によっては結論を誤る可能性がある。そこで、国や業界団体による、実証実験やフィージビリティスタディ等を経た、ガイドライン作成やビッグデータ活用に向けた各ステークホルダ間の共通意識の醸成、世界規模でのプライバシールールの整合性確保等が求められる。

(2) 独立した社内組織の設置や公的な第三者機関の活用

(1)に示したリスクコミュニケーションや、ビッグデータ分析事業を円滑に進めるためには、事業とは独立した部門の設置が望ましい場合がある。これは、「事業者における対外的な窓口」と「事業者内の責任・判断をする部門、監査部門等」の設置を含む。特に、事業の透明性の確保が重要となる場面[35]では重要な位置づけとなる。ただし、このような組織は、経験の積み上げにより次第に正確な対応が可能となるものであり、必要に応じて急速に立ち上げることは困難である。

その一方で、政府や公的機関による信頼できる第三者機関の設置も望ましい。この第三者機関には「判断」と「監査」の機能が要求される。つまり、当該サービス事業のプライバシー対策が必要十分であるかをステークホルダに代わって判断すること、当該サービス事業の透明性を全てのステークホルダに代わって確認することが主な役割となる。特に、事業の特性により、全てのステークホルダに情報開示できない場合などには、第三者機関が特に有効となる。

(3) データの第三者提供時の要件（匿名化等）とデータ破棄時の要件の明確化

1 章に示したとおり、プライバシー情報を含むビッグデータ活用計画を自社内のみで完結して実施する場合には大きな問題とはならないが、当該データを第三者が分析する場合には、プライバシー侵害に十分な留意が必要である。そのプライバシー保護のための技術は多種多様であり、通常は、元の個人情報の種類・特性や分析したい内容を考慮して、これらの技術を単独でまたは複数組み合わせて利用されるべきであり、あらゆる情報について汎用的にプライバシー保護を実現する技術・手法が存在しないことは、「技術検討ワーキンググループ 報告書（2013 年 12 月 10 日 第 5 回 パーソナルデータに関する検討会 資料 2-1）[36]」に記載のとおりである。そこで、ユースケースを想定した詳細検討（運用設計と技術適用の組み合わせ等）や、実証実験・新たな技術開発等を行った上で、第三者提供に関するコンセンサスを得ること、場合によっては法制度化することも重要である。

[35] 特に「データ発信者」へのメリットが小さい場合等
[36] http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf

また、法制度化されるまでの当面の間は、2014 年 6 月に政府より公表が計画されている大綱やそれに対するパブリックコメントなどを含め、法改正の動き・各種検討会等の動きを注視する必要があるだろう。

3.1.2 技術適用に関する提言

汎用的にプライバシー保護を実現する技術・手法が存在しないため、運用と技術の組み合わせによってプライバシー保護を実現する必要がある。そのため、従来考えられていた暗号技術や匿名化技術を応用したプライバシー保護技術（PETs）に加え、運用の透明性確保のための技術（TETs）の適用が必要となる。これらの技術を大別すると以下のとおりとなる。

① 匿名化・仮名化に関する技術
- ・不要データ削除・抽象化・一般化、摂動化・ランダマイズ、交換
- ・選択開示型暗号技術
- ・匿名化・仮名化の安全性評価

② 秘匿分析に関する技術
- ・プライバシー保護データマイニング、秘密分散、検索可能暗号、準同型暗号技術

③ 透明性確保に関する技術
- ・高機能署名技術、他

これらの技術は、産学でそれぞれの仮定や要件に応じた研究開発が進められており、その安全性の検証や、実用化にはまだまだ課題が山積していると考えられる。それぞれの事業に応じた技術開発は個々の事業体において行う必要がある。その一方で、その根本となる考え方や安全性検証方法については､暗号における CRYPTREC[37]や暗号プロトコル評価技術コンソーシアム[38]等のように、国や業界団体等より提供されることが望まれる。

[37] http://www.cryptrec.go.jp/
[38] https://www.cellos-consortium.org

3.2 ビッグデータ活用時の課題への対応

プライバシー情報を含んだビッグデータを安全に活用するためには、予め検討し実施する施策がいくつかある。本節では、プライバシーの侵害を防ぐために事業者が実施することが望ましい施策と、施策がシステムとして問題なく動作していることをモニタリングする箇所について述べている。

3.2.1 ビッグデータの活用時

ビッグデータを活用した事業を提供するには、プライバシー情報の提供者に信頼感と安心感を持ってもらうことが必要である。そのためには、事業者が収集するデータの種類と取得の方法、取得したデータの利用と管理の方法と保護施策、データの二次利用や提供の有無とその方法、などを情報提供者に開示することが望ましい。いくつかのビッグデータを取り扱う事業者は信頼感と安心感を得るために、自主的取り組みとして、プライバシー保護体制や施策についてドキュメントとして公開している。

例えば、日立製作所では「ビッグデータビジネスにおける日立のプライバシー保護の取り組み」[39]といったホワイトペーパーを公開している。このホワイトペーパーでは、プライバシー保護に対する基本的な考え方、プライバシー影響評価(PIA：Privacy Impact Assessment)、プライバシー保護体制、データ活用の各フェーズでの対策、プライバシー保護のために技術的対策と人的対策などを策定し開示することで、社会的責任を果たし、事業に対する信頼感や安心感を得ている。

PIA はプライバシー情報を取り扱う事業者が「システム、事業、サービス等において、プライバシーへの影響を事前に評価し、プライバシーの侵害を防ぐために運用面、技術面での対策を講じる一連のプロセス」とされ、諸外国では PIA の実施を義務づけている国もある。ただし、各国共通の PIA ガイドラインは存在せず、各国の行政機関やプライバシーに関する独立した第三者機関(プライバシーコミッショナーなど)が、各国事情に応じたガイドラインを公表していた。その後、2008 年に PIA の要求事項が ISO22307(Financial services -- Privacy impact assessment)として国際標準として策定された。ISO22307 は金融サービスをターゲットとしたものであるが、他分野でも活用できる。日本で PIA を実施するには、ISO22307 を要求事項としたガイドラインの整備が必要である。なお、日立製作所のホワイトペーパーでは、PIA 実施にあたって、ビックデータ特有のプライバシー侵害に関するリスクを評価する項目を追加し、PIA チェックリストを作成して運用している。

[39] 日立製作所「ビッグデータビジネスにおける日立のプライバシー保護の取り組み」
http://www.hitachi.co.jp/products/it/bigdata/approach/wp_privacy.pdf

しかし、一事業者毎に情報を開示していても、その開示している内容がプライバシーを適切に保護しているのか、不足はないのか、実際にそのとおり運用されているのかなどについて情報提供者は容易に理解し確認することはできない。このため、PIA の実施を公的に明確にするための仕組みと PIA の結果を情報提供者の立場に立って、その内容を中立的・専門的にコミットメントする組織が必要である。

PIA の実施を明確にする公的組織ができるまでの間、ビッグデータ活用の各フェーズ「データ収集・取得」、「データの利用・管理」、「データ提供」において、それぞれの分野・業界団体で必要と考えられる PIA チェックシートを作成し、その内容をコミットメントすることも効果があると思われる。ビッグデータは標準化されて流通することで、新たなビジネスが創造できるので、各フェーズ間で取り扱うデータを規定するのも、情報提供者に取ってわかりやすいと考える。

3.2.2 事業者内の体制

ビッグデータを活用するビジネスを提供する場合には、含まれるプライバシーデータによりプライバシー侵害が発生することを抑止する必要がある。その 1 つが、前節で説明した PIA である。PIA 実施のためにガイドラインを作成し、それに準拠した運用が実施されているのかを確認する PIA チェックシートが必要である。

プライバシー保護責任者主導で PIA を実施する。そこで使用する PIA チェックシートの作成においては、業務委託企業とも連携し、責任を明確にすることも必要である。また、プライバシーデータが関係者の間を過不足なく、安全に流通するかを確認することも重要である。プライバシー保護対策としては運用と技術の両方があるが、データの送り手と受け手が同じ技術や設定、運用方法を採用しないと脆弱な箇所が作られる可能性があるので注意しなければならない。

プライバシー保護責任者は PIA チェックシートを定期的に確認する。基本的には PIA チェックシートの定期的チェック以外でも、毎日の運用において、プライバシー保護の状況を日常業務で常にチェックできるようにすることが望ましい。ビジネスシステムが期待通りの動作をしていることを確認するのである。また、これに合わせて、セキュリティ意識の向上のために、セキュリティ教育も定期的に実施することが望まれる。

3.2.3 対策基準

プライバシーデータの保護については、人が関わらないでも済むように、技術的対策で実施することが望ましい。PIA の実施結果に基づき、プライバシー保護強化技術（PETs ： Privacy Enhancing Technologies）を導入し、データの利活用とプライバシー保護の両立を図るようにする。PET の適用によりプライバシー対策とセキュリティ対策の両方を達成

することができ、システムの信頼性（安全性）とユーザの安心感を高めることができる。PET は暗号技術と認証技術、匿名化技術等の複合的に利用したものの総称で、プライバシー保護に特化するものである。

PETs も様々なものがあるが、大きく 3 つに分類される[40]。「代替的 PET（Substitute PET）」、「プライバシー保護のために活用しやすい補完的 PET(Complementary Privacy-Friendly PET)」、「プライバシー保護目的のための補完的 PET (Complementary Privacy-Preserving PET)」である。

「代替的 PET」の目的は、トラッキング及びプロファイリングを防止し、個人情報を取得しないまたは取得させないことで、具体的なものは、匿名プロキシサーバや Tor（The Onion Router）がある。

「プライバシー保護のために活用しやすい補完的 PET」の目的は、ユーザによるオンライン広告のコントロールをすることで、具体的なものは、広告設定及びクッキー管理、追跡拒否ツールがある。

「プライバシー保護目的のための補完的 PET」の目的は、個人情報を第三者に提供することなくトラッキング及びプロファイリングを許可することで、具体的なものは Adnostic（プライバシーを保護したターゲット広告）がある。

「代替的 PET」はプライバシー情報を利用することができなくなるので、ビッグデータを活用するためには補完的 PET を利用することが必要である。最近では、「プライバシー保護目的のための補完的 PET」が利用される傾向がある。これに使用される技術が暗号化と匿名化である。

いずれにしても、ビッグデータ活用ビジネスには一定の具体的な対策基準は存在しない。ビジネスやシステムについて個別に対策基準を策定する必要があるので、その対策基準を策定するためのルールを定める必要がある。そして、このルールが守られていることをモニタリングする体制を作ることが必要である。

3.2.4 運用の透明化

ビッグデータ活用ビジネスにおいてはプライバシー保護のルール作りと、プライバシー情報管理サイクルにわたってモニタリングする体制が重要である。情報セキュリティに関連する事象の多くは様々な要素が複雑に絡み合うため、何をモニタリングすればよいのか判断するのは難しいが、適切なモニタリングを行うことで、運用の透明化が実現できるようになる。（図 3.2-1 参照）

[40] Ira S. Rubinstein, Regulating Privacy by Design,26 Berkeley Technology Law Journal 1409 http://btlj.org/data/articles/26_3/1409-1456_Rubinstein_WEB%20031012.pdf

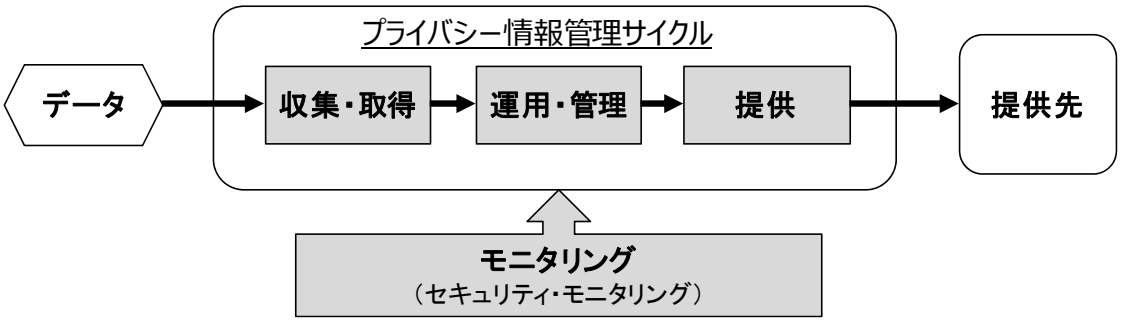


図 3.2-1　プライバシー情報管理サイクルとモニタリング

モニタリングの中心となるのがログ解析である。ログには、セキュリティ機能が正しく予期したとおりに動作しているのか、データ収集は正しく行われたのか、データにアクセスした者は誰なのか、データ処理は正しく行われたか、提供（送信）されたデータはどのような情報が含まれているのか、運用システムの脆弱性はないかなど多くのものがある。

プライバシー情報管理サイクルにおけるモニタリングの内容は表 3.2-1 のとおりである。

表 3.2-1　プライバシー情報管理サイクルとモニタリング内容

プライバシー情報管理サイクル	モニタリング内容の例
収集・取得	・データ取得ポリシーの提示と同意 ・データ収集経路の確認 ・データの正確性 ・データ収集システムの真正性 ・データのアクセス制御（人、サービス、プログラムなど） ・セキュリティ機能の動作 ・出力データの適正性 ・ウイルス対策 ・システムの脆弱性
運用・管理	・運用システムの操作権限管理 ・入力データの適正性 ・データ処理システムの真正性 ・データ処理の自動化 ・データのアクセス制御（人、サービス、プログラムなど） ・出力データの適正性 ・セキュリティ機能の動作 ・データの適切な削除（廃棄） ・ウイルス対策 ・脆弱性管理
提供	・データ提供ポリシーの提示と同意 ・提供データの適正性 ・提供手段の安全性 ・データの適切な削除（廃棄）

しかし、これら多くのログをその都度分析するのは効率が悪く、日常的なモニタリングは不可能と言える。モニタリングは日常的に実施することが望ましいので、効率のよいモ

ニタリング手法が必要となる。このために、多くのログを集約して、システム全体にわたって横断的な検索と分析ができるようにし、特定のセキュリティ侵害やエラーが検出されたら管理者にアラート通知することを自動的に行われるようなログ分析システムを構築することが必要となる。特に、プライバシー情報に関わるデータに関しては、人的なアクセスを極力無くし、情報の漏えいや改ざんする機会を防ぐことも考慮する。

これらのモニタリングの結果は、できる限りリアルタイムで相互に関連づけを行いながらセキュリティ侵害などの異常を検出できるようにし、アラートも確実に管理者に通知されるようにすることが望ましい。また、システムの操作者が対処しなければならない事柄がある場合には、操作者にも適切な通知がされるようにしなければならない。また、アラート通知を受けた場合の対応手順などを予め定めておく必要がある。また、異常の検出パターンやその検出頻度やレベルがどの程度であればセキュリティ侵害であるのかを事前に決定しておかなければならない。しかしながら、これらを全て技術的対策で実施することは非常にコストがかかる。従って、事業者は取り扱っているプライバシー情報の影響を PIA により評価するとともに、技術施策と運用施策のコストバランスを取りながらモニタリング機能を実装していくことが必要である。特に運用コストについては事業を実施したら永続的に必要になるので十分な検討が必要である。

このように、プライバシー情報管理サイクルにわたるモニタリングは重要であり、事前に異常検出のルールとその報告及び対応手順、日常的にチェックできる方法の実装、異常時に策定したルール通りに動作するための教育や訓練なども実施する必要もある。

3.3 トラブル発生時

本項は、2.3 項のトラブル発生時の課題を解決する対策を記載する。

プライバシー侵害の成立要件は、①公開された内容が私生活の事実またはそれらしく受けとられる恐れのある事柄であること、②一般人の感受性を基準にして当該私人の立場に立った場合、公開を欲しないであろうと認められること、③一般の人々にまだ知られない事柄であること、であり、個人の立場（社会的地位）によって異なる。

ついては、トラブル発生時の対策も今までの個人情報保護対策に加え、個人を意識した対策が必要となる。具体的な対策を以下に示す。

3.3.1 想定されるリスクの把握

まずは、自社のビッグデータ活用ビジネスの推進にあたって、どのようなリスクが存在しているかを分析し、把握しておくことが重要となる。取り扱っているパーソナルデータの内容や暗号化・匿名化などのデータ処理の状況、データを取り扱う関係者の洗い出しなどを行い、自社のビッグデータ活用ビジネスの特徴を踏まえ、実施する対策を検討していくことが望ましい。

3.3.2 体制の整備

想定されるリスクが把握できたら、トラブル対応のための体制を整備する。トラブル発生の早期検知と組織内の迅速な情報伝達、トラブル対応にあたってのノウハウの蓄積と共有につなげられるような体制の整備が必要である。また、一口にビッグデータ活用ビジネスにおけるトラブルと言っても、1.1.2 で述べられているとおり、起こりうるトラブルは様々である。発生するトラブルに柔軟に対処できる体制が求められる。

トラブル対応にあたり中心的組織となる部署、後述するトラブル発生状況をモニタリングする担当者、実施する対策を決定する意志決定者、トラブル発生時における顧客からの問い合わせを受け付ける相談窓口などを予め決定しておく。また、弁護士などの有識者との関係を構築しておくことも必要である。

体制の整備に際して、組織内に CSIRT（Computer Security Incident Response Team）や個人情報保護担当部署が存在している場合は、一から組織を立ち上げるのではなく、既存の組織の機能強化・拡張で対応できないか検討すべきである。

3.3.3 対応ルールの策定

整備した体制の運営にあたっては、トラブル発生時に迅速な対応が可能となるよう、事

前に、運用ルールの明確化、意思決定フローの確立などの対応マニュアル整備が必要となる。作成したマニュアルについては、定期的に見直しを行い、机上訓練を行うことも有効である。策定したルールに関し、経営層の合意を得ておくことも重要である。

3.3.4 早期検知の仕組み構築

発生するトラブルに適切に対処するためには、トラブルの発生を早期に検知することが必要である。整備した体制に、インターネットなどをモニタリングする担当者を設置することが必要となる。ただし、人手でのモニタリングには限界があるため、ネット上の風評情報を分析するサービス[41]を利用することも考慮すべきである。

3.3.5 早期鎮静化・問い合わせ対応など拡大防止策

発生したトラブルの影響拡大を防ぐためには、顧客を納得させることのできる対処方針を明示し、問い合わせに対し、適切な回答を行うことが必要である。適切な情報発信を行うためには、発信する方法を事前に検討しておき、迅速に発信できる仕組みを構築しておくこと、また、発信内容の妥当性を確保するため、弁護士など有識者との関係を構築し、裏付けを持った情報を発信していくことが必要である。

設置した相談窓口で、きちんとした受け答えができるよう、事前に発生するトラブルを想定した問答集などを準備し、担当者に対する教育を行っておくことも重要である。

3.3.6 再発防止に向けた取り組み

トラブルの再発防止のためには、発生したトラブルについて、その原因や実施した対処について検証し、課題や対策の不十分な点を明らかにする必要がある。そして、それら検証結果に基づき、体制の見直し、マニュアルの再整備やシステムの改善につなげていくことが求められる。

3.3.7 トラブル事例の共有

サイバーセキュリティの分野においては、政府主導で、インシデント情報を共有する仕組みの構築が進んでいる[42]。このような取り組みと同様に、トラブルの未然防止及び発生時の効率的な対応のためにも、ビッグデータ活用の分野でもトラブル事例を共有する仕組

[41] 風評速報サービス ウワサーチ　http://jp.fujitsu.com/solutions/cloud/saas/application/uwasearch/
ネット風評被害バスターズ http://www.dentsu-pr.co.jp/servicemenu/busters.html
[42] サイバー情報共有イニシアティブ　http://www.ipa.go.jp/security/J-CSIP/

みの構築が求められる。共有すべき内容としては、トラブルの経緯、エスカレーションのタイミング、公に発表した情報などが考えられる。

3.3.8 サービスの活用

これまで述べてきたような体制の整備・対策の実施を行うためには、様々なノウハウが必要となるため、自社だけでは対応できないことも考えられる。適切なトラブル対応の実現のための、ビッグデータ活用時のリスク分析や対策支援のサービス[43]も提供されており、それらを活用することも有用である。

[43] プライバシー保護対策支援コンサルティング
http://www.hitachiconsulting.co.jp/solution/big_data/privacy/index.html

おわりに

近年、IT を活用した社会経済活動において、企業が競争力を強化し、成長し続けるために、様々な方法でビッグデータを活用する傾向が拡大している。このことは、活用事例の増加からも明らかであり、その有効性については共通認識となりつつある。

一方で、プライバシーデータを含むビッグデータの活用に際しては、利用者の意識及び法規制を遵守することが求められており、これは利用者を中心とした社会の要請と捉えることができる。

情報セキュリティ調査専門委員会では、「企業が社会的なニーズを満たしながら、経済的な成長を継続する」ためにはどうしたらよいのかをテーマに議論を継続してきた。本報告書では、委員会で参照した情報を整理し、調査・分析した結果を提言としてまとめている。

今後の我が国における、IT の活用を通じた産業界の発展と国際競争力強化のために、本書が活用されることを期待する。

情報セキュリティ調査報告書

発　行　日　　平成26年３月
編集・発行　　一般社団法人　電子情報技術産業協会
　　インダストリ・システム部
　　情報システムグループ
　　〒100-0004　東京都千代田区大手町1-1-3
　　大手センタービル
　　TEL　(03)5218-1057
印　　刷　　三 協 印 刷 株 式 会 社