JEITA

IS－13－技標－１

情報セキュリティ調査報告書

２０１３年３月

一般社団法人 電子情報技術産業協会

はじめに

本報告書は、情報セキュリティ調査専門委員会が、近年の国内外のプライバシーを取り巻く法制度や IT を活用した社会経済活動の変化を調査・分析し、日本国及び JEITA 会員企業が何をすべきかを提言するものである。

本活動は、「2012 年 1 月 25 日に公表された EU データ保護指令の改定案に係る JEITA 会員企業へのインパクト」、「近年のクラウドコンピューティングやビックデータに代表されるサービス提供側の技術の進展」、「スマートフォンやタブレット PC 等のサービス利用側のコモディティ化」を整理し、セキュリティ技術による対応を検討するために開始した。

EU データ保護指令改定案は、情報技術の急速な進展と社会経済活動のグローバル化に伴う現行のデータ保護制度に対する不備を是正するために検討が進められており、2013 年夏～2014 年頃に発効する見込みである。本改訂案では、EU 域外への規制強化が検討されている一方で、EU 域内での規制緩和が検討されている。また、EU 域外でのプライバシー保護に関する法制度も整備されてきており、それらへの対応の遅れからも、IT を活用したグローバルなサービスの提供における日本企業の競争力低下を招いている。

その一方で、日本国内では、事業者の認識不足やセキュリティ対策が不十分なことによるプライバシー侵害事件が発生しており、日本国内企業へのプライバシー保護の底上げが必要である。

これらの国内外における課題に対して、日本国内サービス提供者の国際競争力の強化及び損失の低減、日本国内のサービス利用者の更なる保護を実現するために、日本国内の関係者が何をすべきかを検討した。

本調査・分析にあたり、ご協力いただいた企業や有識者の方々、そして本委員会の関係の皆様に深く感謝の意を表すとともに、本報告書が関係の方々に活用され、今後の我が国企業のビジネスの更なる進展に寄与できれば幸いである。

2013 年 3 月

情報セキュリティ調査専門委員会
委員長　武本　敏

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	武本　敏	㈱日立製作所
副委員長	池田政弘	富士ゼロックス㈱
委員	福島孝文	東芝テック㈱
〃	白石節男	富士通㈱
〃	池田恵一	富士通㈱
〃	米田　健	三菱電機㈱
〃	畠山有子	三菱電機㈱
〃	遠藤　淳	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
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

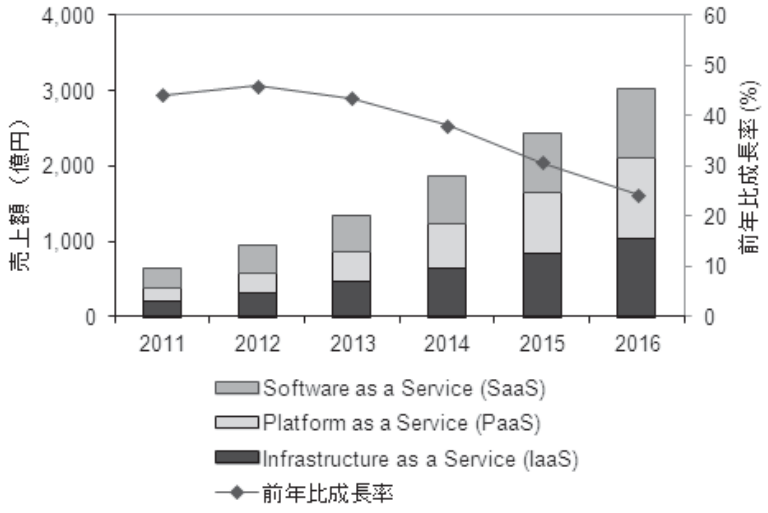
第1章　プライバシー保護を取り巻く環境の変化

1.1 IT の進展（と社会経済の変化）

急速な発展を遂げた情報システムとネットワークは、今や重要な社会基盤として、国民の経済活動や生活を支えている。近年、IT 分野で進展・発展が顕著なトピックを、以下に概観する。

1.1.1 クラウドコンピューティング

日本国内における 2012 年のパブリッククラウドサービス市場は、前年比 46%増の 941 億円、2016 年には 3027 億円に達すると予測され、ベンダーサービスの拡充とユーザの増加から、順調に拡大している[1]。Amazon、Salesforce.com、IBM などのグローバルパブリッククラウドサービスベンダーを始め、富士通、IIJ、NTT コミュニケーションなど日系ベンダにおいても、北米、欧州、アジアといった複数の拠点を開設している。（図 1.1-2 参照）ネットワークの遅延対策、システムの信頼性向上、法規制対応などの理由により、複数拠点によるサービス提供が重要となっている。コンシューマ市場においては、ソーシャルネットワーキングサービスなどクラウドを利用したサービスの利用が一般化されてきている。



Notes:
- システム／アプリケーション開発、導入支援サービスなどのITサービスは含まれていない。
- SaaSには、アプリケーションやシステムインフラストラクチャソフトウェア（システム／デバイス運用管理、セキュリティ、アドバンスドストレージ）が含まれる。

図 1.1-1　国内パブリッククラウドサービス市場 セグメント別売上額予測[1]

[1] IDC Japan プレスリリース, http://www.idcjapan.co.jp/Press/Current/20121105Apr.html

図 1.1-2　Amazon Web Services グローバルインフラストラクチャ[2]

1.1.2 スマートデバイスの普及と BYOD

日本国内の 2012 年第 3 四半期のスマートフォン出荷台数は、前年同期比 50.2%増の 797 万台となり、国内全携帯電話端末出荷に占めるスマートフォン端末の出荷比率は、72.1%まで上昇している。タブレット端末市場も大幅なプラス成長を記録しており、前年同期比 106.8%増の 101 万台まで拡大している。ワールドワイドでもこの傾向は顕著であり、2012 年 10 月～12 月のタブレット端末の出荷台数は 5250 万台と前年比 75.3%増、7 月～9 月比 74.3%増で、同時期のパソコンの出荷台数 8980 万台の 6 割近くにあたる。パソコンの出荷台数は前年比 6.4%減という状況であり、タブレット端末の台数がパソコンを上回るのも時間の問題と見られている[3]。

このようなスマートフォンやタブレット端末などの普及を背景として、労働時間や就業場所にとらわれないフレキシビリティの高い働き方を実現するというようなワークスタイルの変化の一つとして注目されているのが、社員の私物の端末を業務に活用するという BYOD（Bring Your Own Device）である。企業側からすると個別に端末を用意する必要がなくなり、端末の費用、通信費用、端末の管理費用などのコスト削減が期待でき、利用する社員からしても、持ち運ぶ端末を 1 台に集約でき、日常使い慣れた端末を利用できるという効果が考えられる。

---

[2] Amazon Web Services グローバルインフラストラクチャ
http://aws.amazon.com/jp/about-aws/globalinfrastructure/

[3] IDC Press Release http://www.idc.com/getdoc.jsp?containerId=prUS23926713#.UQtLUaWTLYG

1.1.3 ソーシャルメディアサービス

グローバルでの利用者数が、10 億人を超えた Facebook を代表とするソーシャルネットワークサービス（SNS）を始め、Twitter やブログなどのソーシャルメディアサービスは、拡大を続けている。国内における市場規模は、2012 年度で、前年度比 107.5%の 691 億円と見込まれ、2015 年度には、883 億円へ拡大すると予測されている[4]。

SNS やブログは、写真や動画、位置情報などの様々なサービスと連携し、複合的な利用が拡大している。また、スマートフォンに特化したサービスなども現れている[5]。主なソーシャルメディアサービスを、図 1.1-3 に示す。

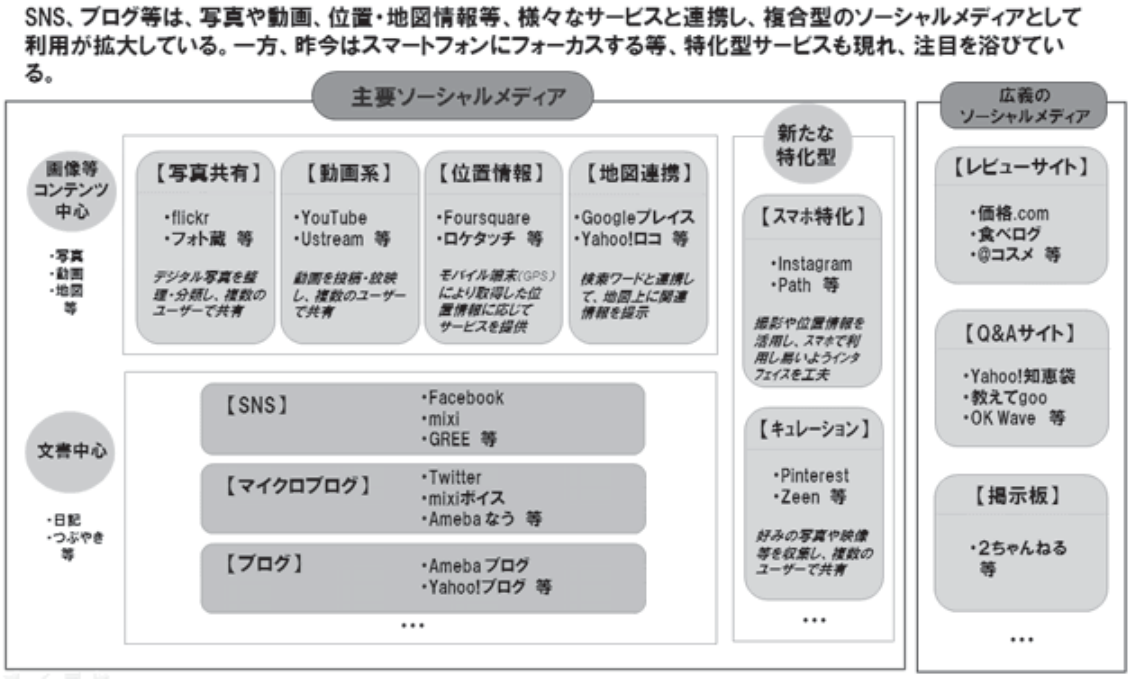


図 1.1-3　ソーシャルメディアサービス全体像[6]

1.1.4 ビッグデータ

スマートフォンやタブレット端末など IT 端末の多様化、ワイヤレス通信の普及やブロードバンド化の進展、クラウドサービスやソーシャルメディアの普及などに伴い、多種多量のデータの生成・収集・蓄積等が容易になってきている。収集された、膨大で多種多様なデータは「ビッグデータ」という総称で呼ばれるようになり、新ビジネスの創出、ユー

[4] ミック経済研究所ソーシャルメディアの市場展望と事業戦略 2012 年度版
http://www.mic-r.co.jp/mr/00620/index.html
[5] NTT データ経営研究所ソーシャルメディアマーケティングの推進
http://www.keieiken.co.jp/monthly/2012/0709/
[6] 総務省スマートフォン時代における安心・安全な利用環境の在り方に関する WG 資料
http://www.soumu.go.jp/main_content/000199207.pdf

ザの利便性向上などへの活用が期待されている。日本国内における 2012 年のビッグデータ関連市場は、前年比 38.2%増の 197 億円、2016 年には 765 億円に達すると予測されている[7]。事業者におけるビッグデータ活用への期待例を図 1.1-4 に示す。

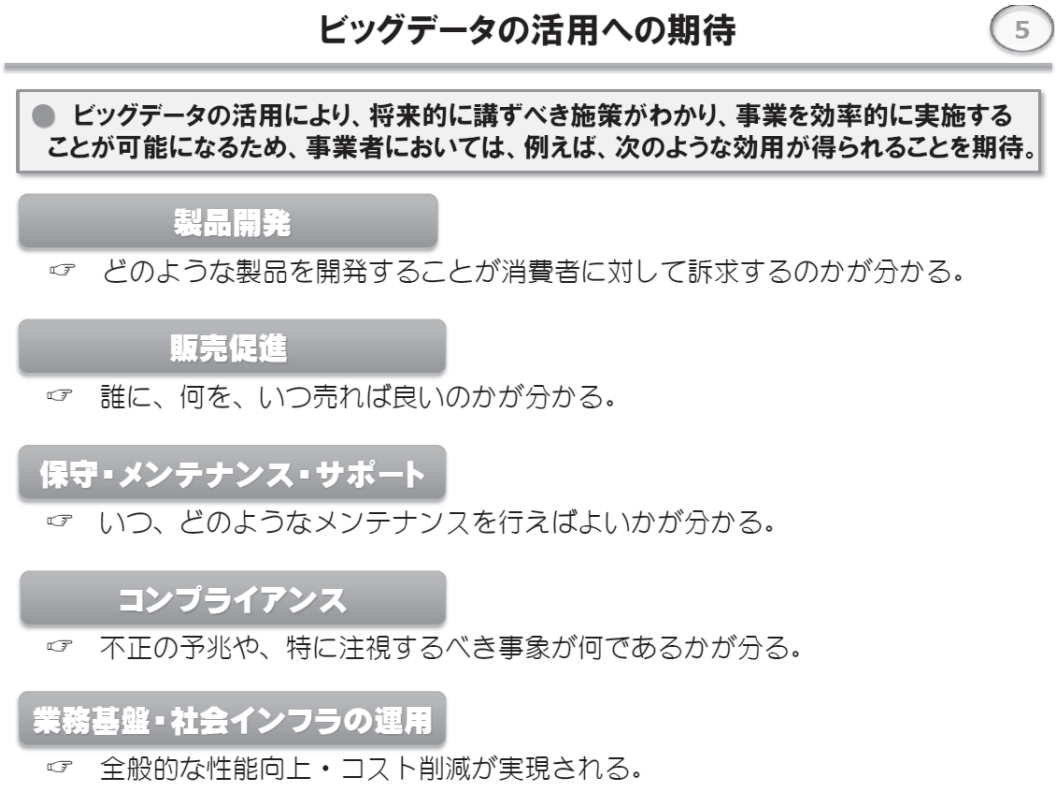


図 1.1-4　ビッグデータの活用への期待[8]

7　IDC Japan プレスリリース, http://www.idcjapan.co.jp/Press/Current/20121003Apr.html

8　「ビッグデータの活用の在り方について」情報通信審議会 ICT 基本戦略ボード ビッグデータの活用に関するアドホックグループ, http://www.soumu.go.jp/main_content/000160628.pdf

1.2 プライバシー情報を活用したグローバルビジネスの拡大

本項においては、パーソナル情報を活用した国内外のビジネス例を紹介する。

1.2.1 プライバシーと個人情報

プライバシーについては、概念の内容や憲法上の根拠等について、様々な見解がある。個人情報とプライバシーの関係についての整理した例を図 1.2-1 に示す。

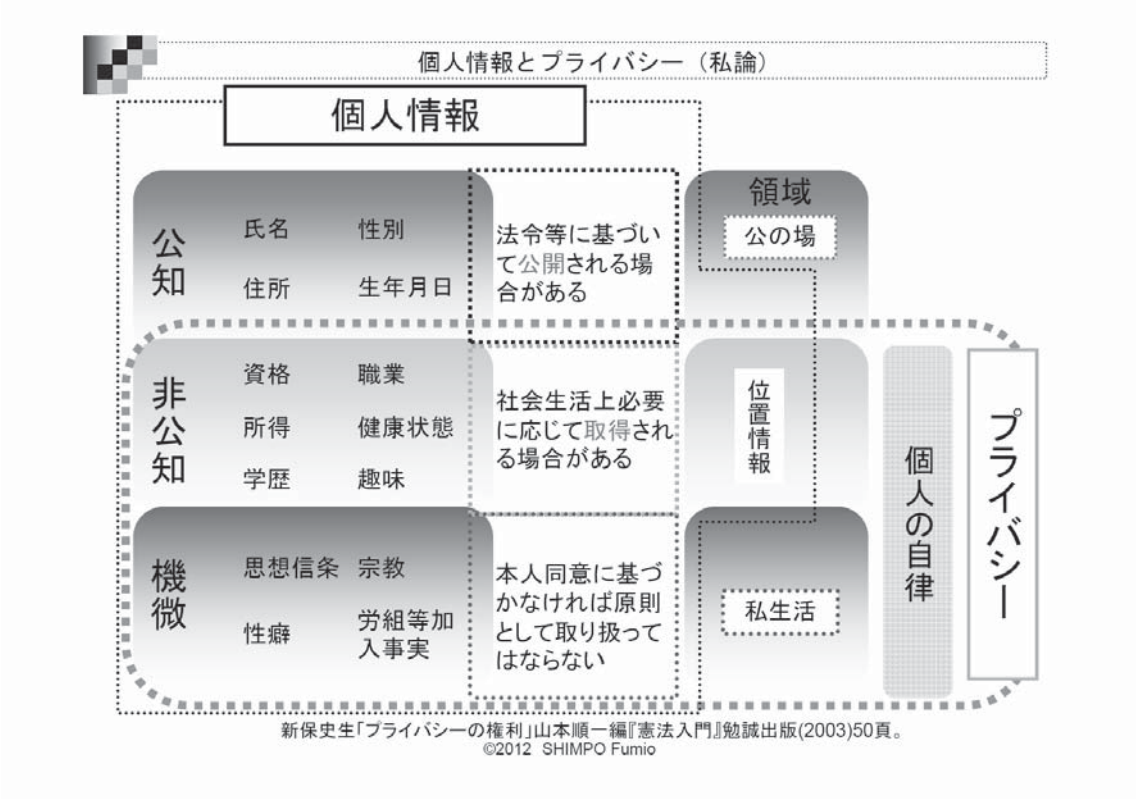


図 1.2-1　個人情報とプライバシー[9]

1.2.2 海外におけるプライバシー情報を活用したビジネス事例

1.1 にて概観したような IT の進展を受け、アメリカを始めとして、海外ではパーソナル情報を集積し 2 次利用するビジネスが広がっている。プライバシー情報を活用したビジネス例を表 1.2-1、表 1.2-2 に示す。

9 総務省パーソナルデータの利用・流通に関する研究会資料
http://www.soumu.go.jp/main_content/000190686.pdf

表 1.2-1　米国における個人情報保護・利活用サービス例[10]

サービス種別	概要	代表的な事業者名
個人情報アグリゲーション・ブローカーサービス	SNS、コンテンツ共有サイト、コミュニティサイト、その他公開情報など、一般公開されている個人情報を収集し、有料で検索できるようにしたり、広告主など第三者に販売するサービスを提供。一般的に、各個人に対する報酬や対価は無し。多くの事業者はデータ削除要求に応じるが、申請方法が複雑な場合、削除費用を課金する場合などもある。	・Intelius ・BeenVerified ・Spokeo ・Anywho ・Scopeo ・White Pages ・ZoomInfo ・MediConnect Global
個人情報価値評価サービス	Twitter や Facebook といった SNS 上アカウントの金銭価値を評価するサービス。フォロワー数、友人数、投稿コンテンツ共有数などといった指標をベースに、各アカウントの価値を算出する。	Klout
公開個人情報の削除代行サービス	個人情報アグリゲーションサービスやブローカーサービス事業者に対して、データ削除申請を消費者に代わって行うサービス。	・Reputation.com ・Abine
個人情報不正使用のモニタリングサービス	第 3 者による個人情報の不正使用（なりすまし、身元詐称など）を防止するため、消費者に代わってウェブ上での個人情報使用状況を監視するサービス	・CSIdentify ・LifeLock ・Intelius ・Reputation.com
データロッカーサービス	消費者の任意入力による各種個人情報を保存し、特定の目的において個人情報が必要とされる場合に、必要な種類の個人情報のみを抽出し、要求者に対して共有するサービス。共有時に消費者に対して、対価を支払うことを想定する動きもある。	・Singly ・Connect.me ・Personal.com ・The Locker Project

[10] JETRO/IPA NY だより 2012 年 6 月号 http://www.ipa.go.jp/about/NYreport/201206.pdf

表 1.2-2　パーソナルデータに関するビジネスの国際動向[11]

Infochimps（http://www.infochimps.com/）	
事業概要	集積データのマーケットプレイスを提供（現在登録されているデータは 14000 件。内 2400 件が有料データ） 販売時の手数料（平均 30%）が収益
パーソナルデータの取扱い状況	・イリノイ州内 400 万人の電話番号リスト（200USD） ・カナダの弁護士 7 万人のリスト（125USD） ・米国のアラブ研究者が、自著“What Arabs Think”で用いたアンケートのデータ
調査結果	・公開が認められていないデータの一つとして、「当該個人から未承諾である個人を特定するデータが指定されている。 ・データの品質を保持するために、一件ずつスタッフが人力による確認を行っている。 ・複製制限については「規約による制限」となっている ・価格設定については「それぞれのユーザに一任」など
Demdex（http://www.demdex.com/）※2011 年 1 月 Adobe 社が買収	
事業概要	行動ターゲッティング広告などに用いるための、ユーザ動態データの提供・流通事業者
パーソナルデータの取扱い状況	・収集するデータは基本的に個人を特定するデータは含まないとしている。中心は、オンラインでのサイト閲覧履歴等に関するデータ
調査結果	・顧客 1 人につき保管するデータ量に応じて月額料金を徴収している ・金額は概ね訪問者 1 人／月あたり 1 セント程度であった。それぞれのユーザについては 40 種類程度の行動変数が取得されていた。
Bluekai（http://www.bluekai.com/）	
事業概要	匿名データの取引を中心とするデータ売買の取次事業（北米では毎月約 300 万の利用者）
調査結果	・サービスは 2 種類 ① Data Exchange パートナー企業から提供を受けているデータを顧客が購入できるシステム（主にアドバイズに利用されている）データ

[11] 経済産業省 パーソナルデータワーキンググループ資料
http://www.meti.go.jp/committee/kenkyukai/shoujo/it_yugo_forum_data_wg2/pdf/001_04_00.pdf

	更新は頻繁 ② Data Management Platform データ解析サービス。顧客のウェブサイト解析（どのページにアクセスされているか、どのページで訪問者が閉じているかや、何のデバイスで見られているかなど）が中心であるが、最近は事業者がデータ持ち込んで解析を依頼されるケースも増えている。 ・プライバシーに関わる部分が残されているデータは取引等を行わない。 ① 名前、住所などは勿論のこと、1 個人の医療記録や金銭面に関するもの ② Minor（18 歳以下、日本における未成年者）のものと思われるデータが発見された場合は、収集及び分析対象から除外。 ・全てのデータは独自のアルゴリズムを用いたツールによる審査を受けてから売買の対象になる。
Allow（http://i-allow.com/）	
事業概要	個人情報を販売し、情報を提供した個人には売上の 70%を手数料として支払っている。
パーソナルデータの取り扱い状況	「個人情報の積極的換金を支援する」方針を明確に打ち出している。
調査結果	・サービス登録はイギリス国民に限定されている ・「保険」「携帯電話」「クレジットカード」に関する問いの価値が高い。
Personal.inc（http://www.personal.com）	
事業概要	個人に関する情報を、保管・共有するサービスを無料で提供する
調査結果	・提供するサービス ①保管（自身の情報を保管する） ②共有（家族、友人などと情報を共有する） ③販売（自身の情報を販売する） ・利用者が預けたデータから利益を得ることを選んだ場合は、Personal 社はデータ販売を行い、手数料として 10%以下を徴収し、利用者へ支払うというビジネスモデル。

1.2.3 国内のプライバシー情報を活用したビジネス事例

日本国内における、プライバシー情報を活用したライフログ市場規模は、2011 年度で約 10 億円と見込まれているが、サービス自体はまだ浸透しておらず、有料サービスを提供する一部事業者の売上に占められているのが実態である[12]。

提供形態としては、消費者から取得したライフログを使って、提供元の消費者に対して、何らかのサービスを行う形態やライフログプラットフォーム事業者が消費者から取得したライフログを第三者の事業者に提供し、その事業者が消費者にサービスの提供を行う形態が考えられる [12]。主なビジネスの事例を表 1.2-3 に示す。

表 1.2-3　国内における個人情報保護・利活用サービス例[13]

サービスの分類	事例	サービス事業者
レコメンド／コンテンツ配信	i コンシェル	NTT ドコモ
Web マーケティング	インターネット視聴率調査	ネットレイティングス
オンライン広告	Google Adwords	Google
販売促進／マーケティング支援	おすすめ商品	Amazon.com
販売促進／マーケティング支援	T ポイントサービス	カルチュアコンビニエンスクラブ
SNS 広告	スポンサー広告	Facebook
O2O	Edy｜au	KDDI、楽天
PHR （Personal Healthcare Record）	ポケットカルテ	日本サスティナブルコミュニティセンター

1.2.4 プライバシー情報を活用したビジネスにおける問題

このように、プライバシー情報をビジネスに活用する仕組みが広がりを見せる一方で、プライバシーを侵害する事例も発生している。

国内で発生した事例としては、T ポイントツールバーの問題がある。T ポイントツールバーは、Internet Explorer 向けのツールバーで、検索窓から検索することで、T-Point を付与する仕組みであったが、利用規約にない情報（MAC アドレス、アクセス URL（T 会員番号と一対一対応した ID で個人を識別））を送信したり、SSL 通信を含むユーザの Web 閲覧履歴を平文で送信（盗聴のリスク）しているなどの問題点が指摘され、最終的には提供停止となっている。

12 矢野経済研究所 ライフログ市場に関する調査結果 http://www.yano.co.jp/press/pdf/879.pdf

13 IPA パーソナル情報保護と IT 技術の調査より抜粋
http://www.ipa.go.jp/security/fy23/reports/pdata/documents/pdata_report.pdf

その他、国内外で問題となった事例を、表 1.2-4 に示す。

表 1.2-4　ネットビジネスで生じたプライバシー侵害事件[14]

	日本			米国	
	ビューン（ビューン社）	AppLog／App.tv（ミログ社）	カレログ（ﾏﾆｭｽｸﾘﾌﾟﾄ社）	Google Buzz（Google 社）	Facebook（Facebook 社）
問題点	ユーザのページ閲覧履歴を無断で収集し、サーバに送信	同意取得をしていない、または取得時の説明が不十分であったテント、送信される情報がユーザにとって不透明である点	アプリのアイコン名が「GPS Connection」になっており、アプリがインストールされていることが端末保有者に分かりにくい点。	ユーザの事前同意を取得せずに、Gmail の情報を Google Buzz の初期設定時のユーザ名等に利用したこと。	ユーザに通知することなく、非公開に設定していた情報の公開設定を変更した点。
問題の類型	事業者の認識不足やセキュリティ対策が不十分だったことによる問題			事業者による意図的な法制度の規範が曖昧な領域への挑戦による問題	

14 野村総合研究所「ソーシャルメディア時代のプライバシー」（モバイル&ソーシャル WEEK2012）

1.3 増大するプライバシーのリスク

1.3.1 クラウドサービス利用におけるリスク

1.2.3 でも述べたように、プライバシーを活用したビジネスが広がりを見せる一方で、プライバシーを侵害するような事例も発生している。特にクラウドサービスについては、データセンターが国外にあったり、サービス事業者が国外の事業者であったりボーダレスな特徴を有している。データセンターの所在する国の法執行機関によって、データの捜索や差し押さえられたり、データの移転が制限されたりすることが考えられる。

例えば、アメリカでは、米国愛国者法（Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001）が制定されている。2001 年 9 月 11 日の同時多発テロを受け、テロ対策を目的として制定された。捜査機関が、裁判所の命令なしに通信を傍受できるなどの権限拡充が行われており、実際 2009 年 4 月に FBI が米国内のデータセンターを捜索して、サーバ等の設備を押収している。結果、このデータセンターを利用していた約 50 社がサービスを利用できなくなる事態に陥った。

また、EU では EU データ保護指令が発効されている（1.4 にて後述）。EU 域外の国にプライバシー情報を含むデータを移転する場合には、移転しようとする国が、EU データ保護指令が要求するプライバシー情報の保護措置を確保している必要がある。2012 年 3 月時点でデータ保護措置の十分性が認定されている国は、スイス・カナダ・アルゼンチンなど 9 カ国で日本は含まれていない。例えば、EU 域内のデータセンターに、そこにクラウドサービスを通じてプライバシー情報が保管されている場合、十分なデータ保護措置を取っていると見なされていない日本に対してのデータ移転が制限される可能性がある。(図 1.3-1)

グローバルに展開されているクラウドサービスの利用にあたっては、準拠法や裁判管轄に関しても留意する必要がある。契約内容によっては、クラウドサービス事業者が存在する国で裁判を起こさざるを得なかったり、判決内容を執行できないことも考えられる。

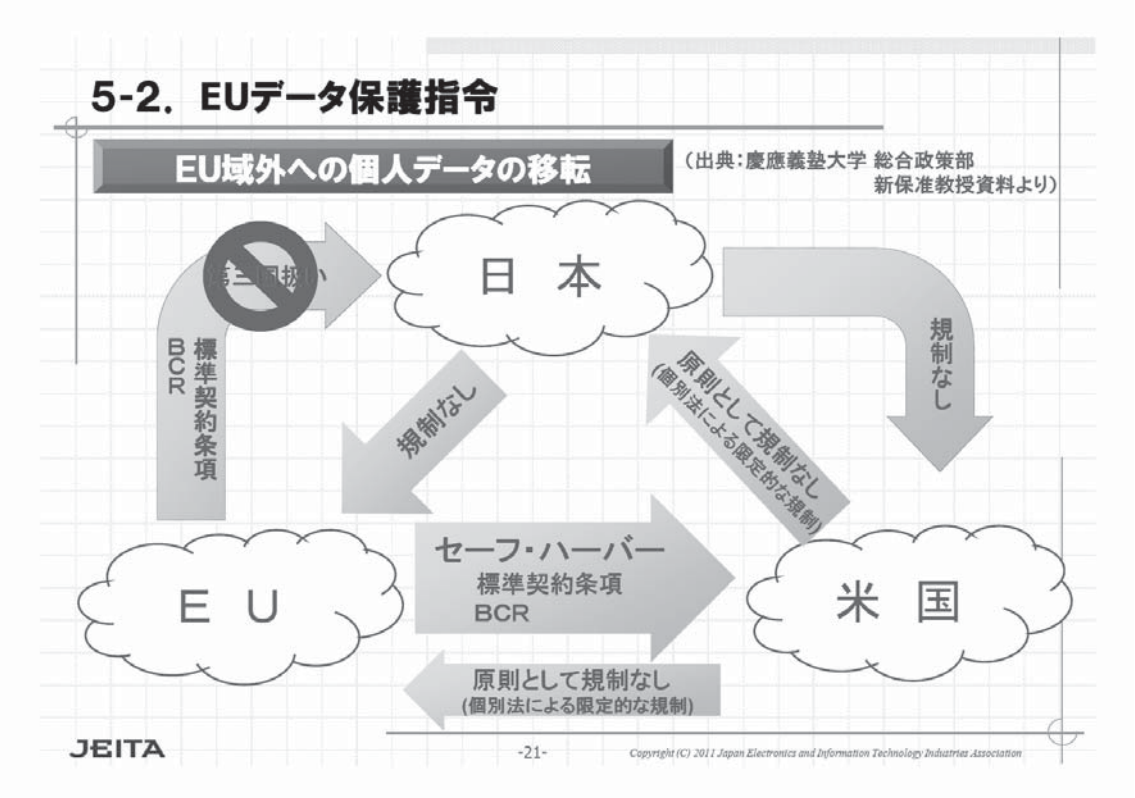


図 1.3-1　EU 域外への個人データの移転[15]

1.3.2 スマートフォン利用におけるリスク

スマートフォンには、電話番号やアドレス帳で管理されているデータの他にも、GPS による高精度の位置情報など､行動履歴や通信履歴等の様々な利用者情報が蓄積されている。それら蓄積された情報に対し、アプリケーションがアクセスし、外部へ送信する場合がある。サービスの提供・向上や利用者の趣向に応じた広告の表示等を目的とされているが、実際どのように活用されているか不明瞭な場合もあり、また利用者に対し、十分な説明がないまま取得するアプリも多く、利用者の不安が高まっている。（図 1.3-2, 1.3-3）

[15] JEITA クラウドサービスと個人情報保護
http://home.jeita.or.jp/upload_file/20111116144904_nBg4ANJmyM.pdf

スマートフォンにおける主な利用者情報

3

■ 常に電源を入れてネットワークに接続した状態で持ち歩くスマートフォンは、PCに比べて利用者との結びつきが強く、利用者の行動履歴や通信履歴等の多種多様な情報を取得・蓄積することが可能。

- 電話番号及びアドレス帳で管理されるデータ、GPS等による高精度の位置情報

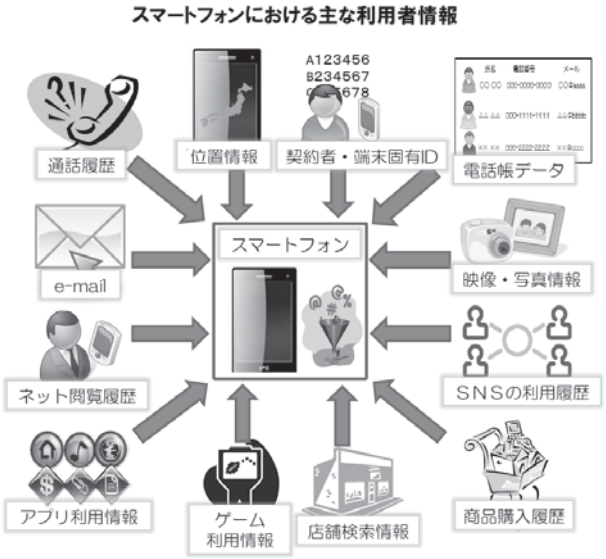


図 1.3-2　スマートフォンにおける主な利用者情報[16]

アプリケーションによる情報収集の実態と収集目的

5

スマートフォンによる利用者情報の収集目的は、一般にサービスの提供・向上や利用者の趣向に応じた広告の表示等とされているが、実際にどのように活用されているか必ずしも明確ではない。

アプリケーションによる情報収集の実態

【 KDDI研究所による調査】

- 2011年8月に選定した980個のアプリについての分析
  - 558（56.9%）のアプリに、情報収集モジュール※が存在
    （※）スマートフォンに蓄積された情報を収集する機能を持つ一連のプログラム。広告配信事業者等が提供し、アプリ作成者がアプリに組み込む。
  - アンドロイドの利用許諾については、端末ID等に係るものが57.9%、位置情報（GPS）に係るものが26.4%に存在。
- 2011年12月-1月に400個のアプリの挙動解析を実施
  - 181個のアプリについて、契約者・端末固有IDや位置情報を外部送信
  - うち、167個についてはアプリにおける利用許諾がなく、情報の外部送信について説明が不十分

利用者情報の収集目的と活用状況

■ **アプリによる利用者情報の活用方法については、大きく分けて①～④のようなものが想定される。**

① アプリがそれ自体のサービス提供のために用いる場合（利用者が情報を入力等しなくとも既存の情報を活用してすぐに利便性の高いサービスを利用することが可能となる場合も多い）

② アプリ提供者が、アプリの利用状況等を把握することにより、今後のサービス開発や市場調査のために用いる場合

③ スマートフォンの位置情報あるいは契約者・端末固有ID等の利用者情報を情報収集事業者等が取得し、広告サービス等に活用する場合又はその他の市場調査等の情報分析等に活用する場合

④ 現段階では目的が明確ではないが、将来的な利用可能性等を見込んで利用者情報を取得する場合

図 1.3-3　アプリケーションによる情報収集の実態と収集目的[16]

16 総務省利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会 資料
http://www.soumu.go.jp/main_content/000167252.pdf

1.3.3 ライフログ活用サービスにおけるリスク

1.2 でも述べているように、ライフログ活用サービスは、利用者の性別や年齢などの属性情報、購買履歴や位置情報などの行動情報、スケジュールや写真などの記録情報などに基づいて、何らかのサービスを提供するビジネスである。利用者にとっては、このような個人情報が流出・悪用されたり、プライバシーの侵害につながったり、犯罪につながったりすることなどが懸念される。プライバシー情報の活用における課題例を図 1.3-4 に示す。

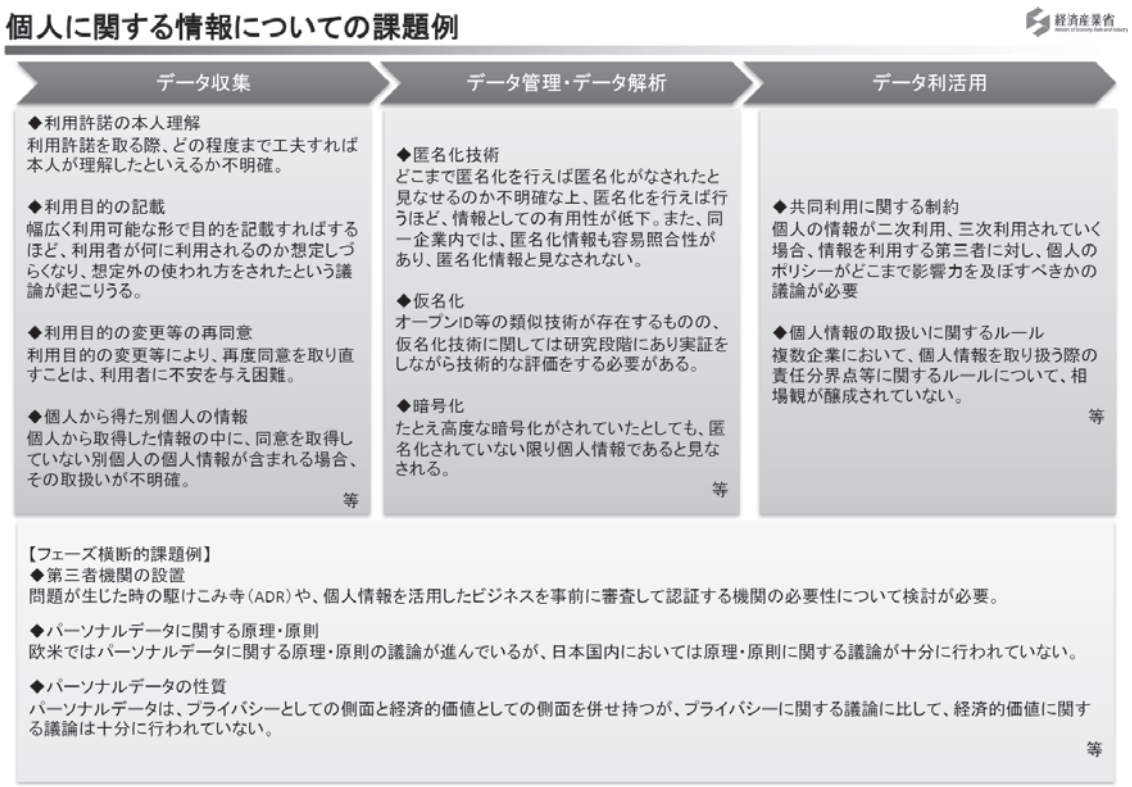


図 1.3-4　個人に関する情報についての課題例[17]

[17] 経済産業省 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資料
http://www.meti.go.jp/committee/kenkyukai/shoujo/it_yugo_forum_data_wg2/pdf/001_03_00.pdf

1.4 重要性を増す各国の法制度

1.4.1 諸外国のプライバシー情報関連制度

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ており、プライバシー情報の活用が、新産業創出など重要な役割を果たすという認識の下、関連法制度の見直しが進められている。

1.4.2 EU データ保護指令

EU データ保護指令は、個人情報の保護に関する指令で、1995 年採択、1998 年に発効となった。EU 加盟国及び EEA（ヨーロッパ経済圏）加盟国の 30 カ国に対し、同指令に基づく個人情報保護に関する国内法規を要求している。主な内容は以下の通りである[18]。

(1) データ内容に関する原則（特定された明示的かつ適法な目的のための取り扱い等）
(2) データ取扱いの正当性の基準（データ主体の明確な同意等）
(3) センシティブデータ※の取扱い
※人種または民族、政治的見解、宗教的または思想的信条、労働組合への加入、健康または性生活に関するデータ
(4) データ主体のデータへのアクセス権
(5) 取扱いの機密性及び安全性
(6) 第三国への個人データ移転に関する規律 （第三国が十分なレベルの保護措置を確保していることを条件とする等）
(7) 独立した監督機関

データ保護指令の採択から 15 年以上が経過し、急速な IT の進歩とグローバル化の進展による以下のようなリスクの拡大が懸念されている。

・クラウドに代表されるグローバルなデータの流通
・Facebook や Twitter を始めとする SNS 利用者の爆発的増大に伴うプライバシー情報の公開・共有の拡大、
・プライバシー情報を活用したビジネスの広がり

このような課題に対処するために、データ保護指令の改定が進められている。

2012 年 1 月に改定案が公表され、2013 年夏～2014 年にかけて採択される予定で、採択から 2 年後に発効される見込である。主な改正の内容は以下の通りである [18]。

---

[18] 総務省パーソナルデータの利用・流通に関する研究会資料より抜粋
http://www.soumu.go.jp/main_content/000197631.pdf

① EU 域内における規制の単一化・簡素化

・国内法制化の不要な「規則」に変更

・一国から承認を得れば、他国の当局からの承認は不要

・データ保護当局間の調査協力のメカニズム

② より強固な個人データ保護ルールの整備

[事業者]

・プライバシー・バイ・デザインの原則

- 新サービスの導入時、データ保護への考慮を義務付けの導入
- 個人の権利や自由に対するリスクを伴う個人データの取扱いを行うにあたって、当該取扱いが個人データの保護に対して与える影響度の評価（PIA:Privacy Impact Assessment プライバシー影響評価）を実施する必要がある旨の規定

・「データ保護職員」の任命義務（250 人以上の従業員の雇用などの要件を満たす事業者が対象）

・個人データ漏えい時の通知義務

- データ保護当局に対しては可能な場合 24 時間以内に、個人に対しては当該個人プライバシー等に悪影響を及ぼす可能性がある際には遅滞なく通知

[個人]

・忘れてもらう権利

データ削除に関する現行法令における個人の権利をより明確化するとともに、データ管理者は、ネット上での個人データへのリンクやコピー・複製された個人データについて、当該個人から削除要求があった場合、当該要求を（それらデータを扱う）第三者に対して通知するなど、あらゆる合理的手段を講ずる義務がある旨規定

・データポータビリティの権利

共通化されたフォーマットで電子的に自らのデータのコピーをデータ管理者から取得できるとともに、自らのデータをあるアプリケーションから別のアプリケーションに移転させることができる権利について規定

・同意の明示（オプトイン原則）

個人データの取得にあたって必要な同意は明示的な（explicit）ものであることを要する旨の規定

③ データ保護に関するグローバルな課題への対応（図 1.4-1）

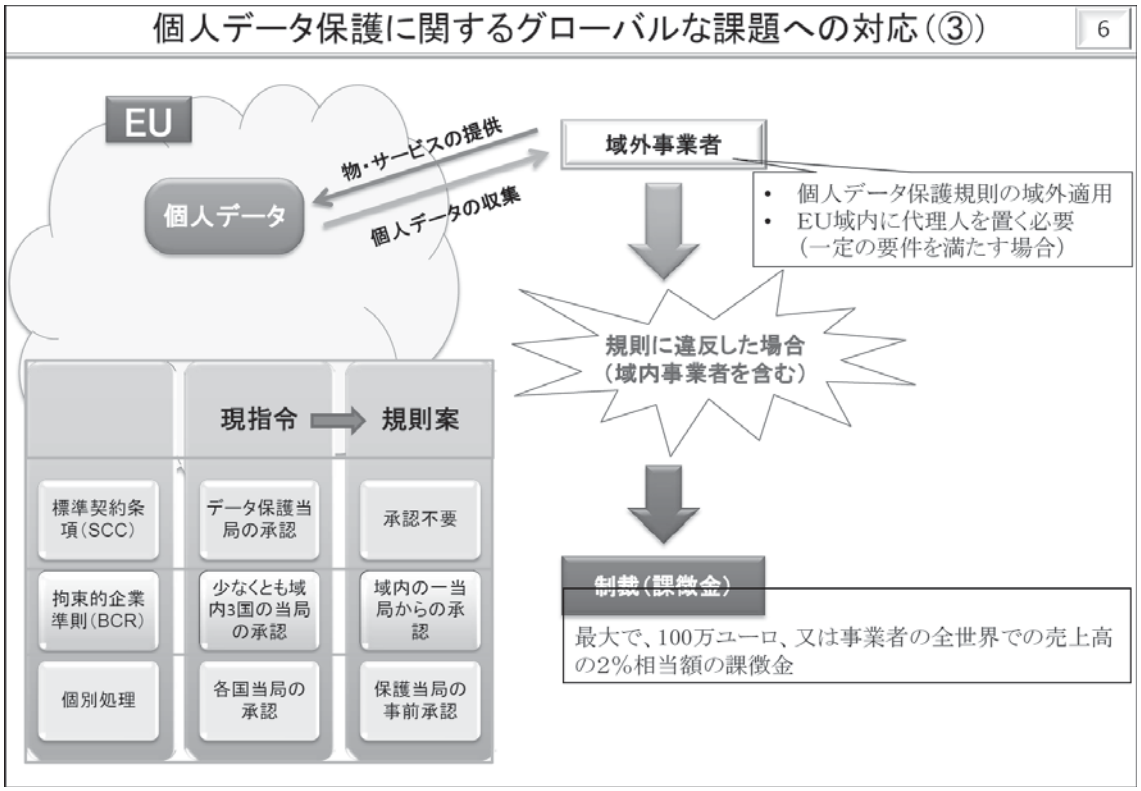


図 1.4-1　個人データ保護に関するグローバルな課題への対応 [18]

EU において、個人データ保護の権利は、「欧州連合基本権憲章」第 8 条や「欧州連合の機能に関する条約」第 16 条で認められた基本的人権の 1 つとして考えられている一方、今回の改定は、Google や Facebook のような全世界からプライバシー情報を収集する多国籍企業や Patriot 法を持つアメリカ、データ保護に関する法律が整備されていないにも関わらず欧州企業からのデータ処理の委託を受けている中国など新興国に対する非関税障壁にもなっているとの指摘もある。

1.4.3 プライバシーに関するアメリカの動向

(1) 個人情報保護制度

アメリカでは、公的部門と民間部門の双方を対象とする包括的な個人情報保護法は存在していない。公的部門については、1974 年に連邦政府の保有する個人情報の取扱いについて、プライバシー法が制定されている。また、民間部門については、信用情報や医療情報など機密性の高い情報を扱う分野において、分野毎に個別法が制定されている。主な法律を以下に示す。

・金融：金融サービス近代化法（GLBA:Gramm-Leach-Bliley Act）

・医療：医療保険の相互運用性及び説明責任に関する法律
（HIPAA:Health Insurance Portability and Accountability Act）

・通信：電子通信プライバシー法（ECPA:Electronic Communications Privacy Act）
・信用情報:公正信用報告法（FCRA: the Fair Credit Reporting Act）

(2) 消費者プライバシー権利章典

アメリカにおいては、(1)で述べたように個々の法制度はあるものの、どちらかと言えば、業界・企業のビジネス上の取り組みが先行し、個人が実際に不利益を被ることがなければ良い、問題が生じた場合には業界の自主規制や損害賠償による解決を計るという流れが主となっていた。

しかし、1.4.2 で述べたように IT の進展に伴い、プライバシーが侵害されるリスクは増大している。このようなネットワーク化された社会における消費者のデータ・プライバシー保護を目的として、2012 年 2 月、ホワイトハウスが大統領名で、「消費者プライバシー権利章典（A Consumer Privacy Bill of Rights」の草案を公開した。（図 1.4-2）

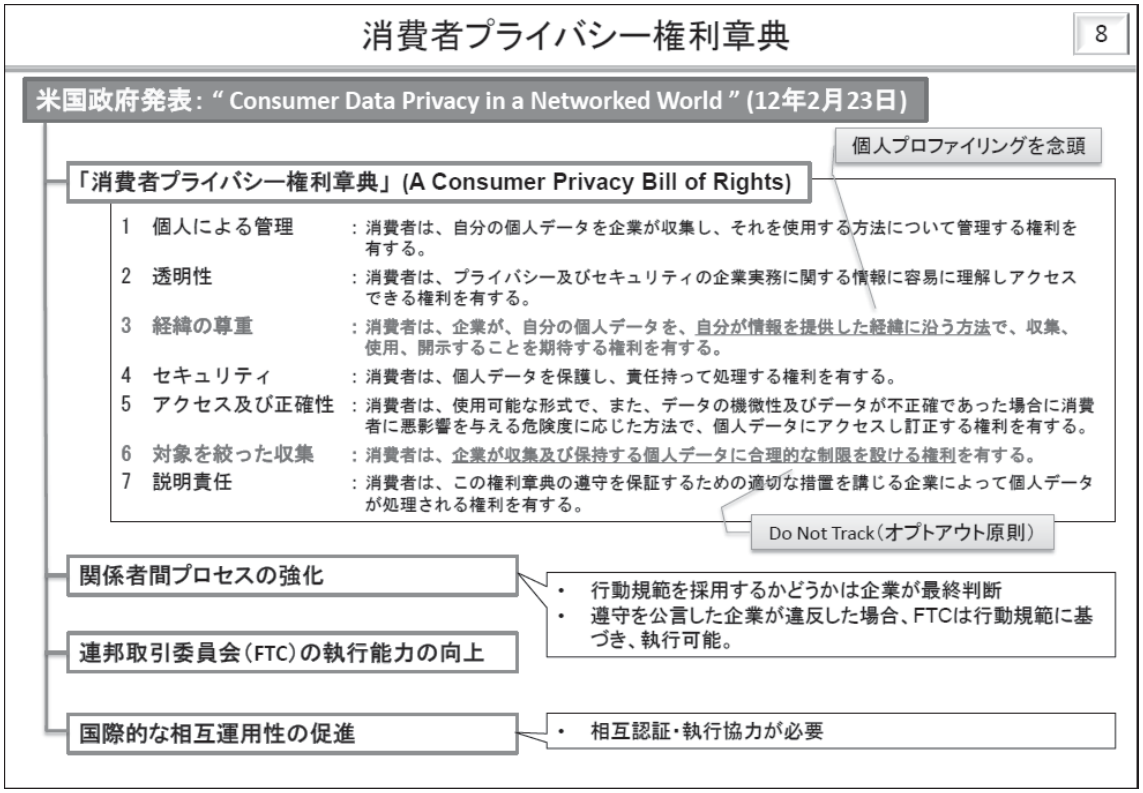


図 1.4-2　消費者プライバシー権利章典 [18]

(3) EU との関係

1.4.2 で述べたように、EU データ保護指令では、適切なレベルの保護措置を取っていない第三国へのプライバシー情報の移転を認めていない。包括的な個人情報保護法を持たないアメリカへのデータの移転を可能とするために、セーフハーバーの枠組みを作り、データの移転を可能としている。（図 1.4-3）

1.4.2 で述べた通り、EU データ保護指令の見直しが進んでいるが、2012 年 3 月 19 日に公表された米国ブライソン商務長官と EU レディング欧州委員会副会長の共同声明において、引続き本枠組みを活用して行くことが謳われている。

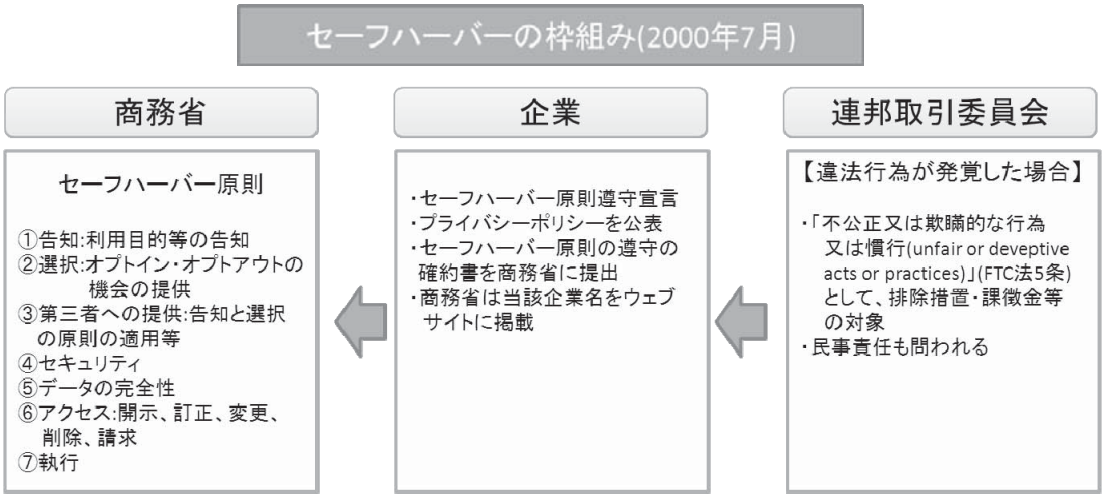


図 1.4-3　セーフハーバーの枠組み [18]

1.4.4 カナダの個人情報保護制度

カナダでは、アメリカと同様に部門に包括的な法律は制定されていない。公的部門に対しては、連邦の公的部門に係る連邦プライバシー法が、民間部門に対しては、個人情報保護及び電子文書法（PIPEDA : Personal Information Protection and Electronic Documents Act）が制定されている。

プライバシー法では、情報の収集への同意、同意を得た目的以外の利用の禁止、個人情報の開示請求等の規制を定めている。プライバシー法に基づき、Office of Privacy Commissioner を連邦議会より、プライバシー権を監督・擁護する権限を与えられている。

PIPEDA では、商業活動の過程で個人情報を収集・利用または提供するあらゆる組織に適用される。

2001 年 12 月には、セグメント方式[19]としては、初めて個人データの移転先国として、保護措置の十分性が EU から認定された。

1.4.5 プライバシーに関する APEC の動向

APEC 加盟エコノミーにおける整合性のある個人情報保護への取り組みを促進し、情報

19 個人データないしプライバシーを保護することを目的とする法律の法的対応の方式の考え方の一つ。公的部門と民間部門とをそれぞれ別の法律で対象とする方式。他に、公的部門と民間部門双方を対象とするオムニバス方式、それぞれの部門について、特定の分野で保護措置を講じるセクトラル方式がある。

流通に対する不要な障害を取り除くことを目的として、2004 年 10 月に APEC プライバシーフレームワークが採択された。以下の 9 原則から成り、APEC 加盟の 21 エコノミーを対象としている。

①損害の回避 ②通知 ③収集の制限 ④個人情報の利用 ⑤選択の機会提供

⑥個人情報の正確性確保 ⑦安全管理措置 ⑧開示・訂正 ⑨説明責任

また、APEC 内で、企業・組織が国境を越えて個人データを移転するために定められたのが、越境プライバシー・ルール（CBPR：Cross Border Privacy Rules）である。個人データを越境移転しようとする企業などは、APEC プライバシーフレームワーク 9 原則に基づく行動規範を開発し、責任団体による第三者認証を受ける必要がある。責任団体は、公的機関でも民間団体でも良いが、APEC による認定が必要となる。2012 年 7 月、アメリカが最初の CBPR 制度の正式参加者となった。

1.4.6 シンガポールの個人情報保護制度

これまで、シンガポールでは、包括的な個人情報保護法は制定されていなかったが、2012 年 10 月、PDPA（Personal Data Protection Act）が国会で可決された。2013 年 1 月に発行となったが、1 年半の適用猶予期間が設けられている。

PDPA では、企業等は、個人情報の取得、使用または開示に対して、その個人からの同意を得ること、また、同意の取得方法については特にこと細かく明示されてはいないが、同意の取得前に、個人情報の取得、使用または開示の目的を当該個人に伝えることが求められている。個人情報が当初と異なる目的で使用される場合には、改めて当該個人から同意を取得することが求められている。さらに、商品やサービスの提供を行うために合理的とされる範囲を超えて、商品やサービス提供の条件として個人情報の収集、使用または開示に対する同意を求めることは、禁止されている。同意をした後も、個人は、同意を撤回する権利を有し、その場合には、企業等は、撤回を受けた個人情報の使用等が禁止される。

個人情報の国外への移転について、原則的に国外への移転は認められていないが、移転先が PDPA に相当する個人情報保護が行われていることが保証される場合、移転することができる。

第2章　日本にとってのプライバシー保護の課題

2.1 産業競争力の低下

インターネットやスマートフォンが普及し、クラウドによる大量のデータの蓄積・分析を活用したサービスが活況を呈する中で、日本の IT 競争力は低下傾向にある。プライバシー情報への取り組みの遅れは、今後 IT 市場の中でも成長が期待されるいわゆるビッグデータ市場への参入の遅れを招き、競争力の低下に拍車をかけると予想される。

2.1.1 世界の時価総額上位 100 社における日本の IT 企業の順位の低下

2003 年から 2012 年の世界の時価総額上位 100 社において、Apple や Google 等の米国 IT 企業が躍進し、アジアでも韓国の Samsung 電子が順位を上げた。一方、日本の IT 企業の順位が大幅に下落した。

（2003年）

順位	社名	国・地域	分類	株式時価総額（100万ドル）
1	Microsoft	米国	ソフトウェア・コンピューターサービス	300,628.6
7	Intel	米国	情報通信機器	179,155.1
8	Intl.Business Machines	米国	ソフトウェア・コンピューターサービス	152,826.8
14	Cisco Systems	米国	情報通信機器	136,108.4
15	Vodafone	英国	通信	135,905.4
17	NTTドコモ	日本	通信	122,625.6
27	Verizon Communications	米国	通信	89,413.8
30	Dell	米国	情報通信機器	85,843.6
37	SBC Communications	米国	通信	73,949.7
38	Nokia	フィンランド	情報通信機器	73,649.8
39	NTT	日本	通信	72,577.8
43	Comcast	米国	メディア	68,023.3
44	Viacom	米国	メディア	67,237.7
48	Aol Time Warner	米国	メディア	65,601.5
51	Deutsche Telekom	ドイツ	通信	60,373.2
52	Telefonica	スペイン	通信	59,716.5
53	Hewlett-Packard	米国	情報通信機器	59,031.3
54	Oracle	米国	ソフトウェア・コンピューターサービス	58,799.7
62	China Mobile (HK)	香港	通信	51,822.3
63	Samsung Electronics	韓国	電子・電気機器	51,393.8
64	France Telecom	フランス	通信	51,329.5
68	Orange	フランス	通信	49,060.1
76	Bellsouth	米国	通信	43,745.4
78	キヤノン	日本	電子・電気機器	43,068.6
82	Telstra Corporation	オーストラリア	通信	41,279.6
83	Walt Disney	米国	メディア	41,230.4
87	Taiwan Semiconductor Manufacturing	台湾	情報通信機器	39,920.9
90	Telecom Italia Mobile	イタリア	通信	39,781.4
92	Texas Instruments	米国	情報通信機器	39,472.5
93	News Corp.	オーストラリア	メディア	38,991.7
95	SAP	ドイツ	ソフトウェア・コンピューターサービス	38,609.1

（2007年）

順位	社名	国・地域	分類	株式時価総額（100万ドル）
3	Microsoft	米国	ソフトウェア・コンピューターサービス	272,911.7
5	AT&T	米国	固定通信	246,206.3
16	China Mobile Hong Kong	香港	移動体通信	181,798.6
28	Cisco Systems	米国	電子機器・部品	154,202.0
31	IBM	米国	ソフトウェア・コンピューターサービス	141,911.1
32	Vodafone	英国	移動体通信	140,429.3
45	Verizon Communications	米国	固定通信	110,343.0
46	Intel Corporation	米国	電子機器・部品	110,322.6
47	Telefonica	スペイン	固定通信	108,088.9
48	Hewlett-Packard	米国	電子機器・部品	107,432.5
51	Google	米国	ソフトウェア・コンピューターサービス	105,421.1
56	Samsung Electronics	韓国	電子機器・部品	98,908.4
62	Nokia	フィンランド	電子機器・部品	93,923.8
65	Oracle Corporation	米国	ソフトウェア・コンピューターサービス	93,203.7
77	NTTドコモ	日本	移動体通信	84,707.4
81	NTT	日本	固定通信	83,054.3
84	Comcast	米国	メディア	80,801.4
85	Apple	米国	電子機器・部品	80,076.8
93	Time Warner	米国	メディア	75,242.9
94	News Corporation	米国	メディア	74,635.4
96	Deutsche Telekom	ドイツ	固定通信	72,844.9
100	キヤノン	日本	電子機器・部品	71,485.9

（2012年）

順位	社名	国・地域	分類	株式時価総額（100万ドル）
1	Apple	米国	電子機器・部品	559,002.1
4	Microsoft	米国	ソフトウェア・コンピューターサービス	270,644.1
5	IBM	米国	ソフトウェア・コンピューターサービス	241,754.6
8	China Mobile	香港	移動体通信	220,978.9
15	AT&T	米国	固定通信	185,154.8
17	Samsung Electronics	韓国	電子機器・部品	181,774.0
25	Google	米国	ソフトウェア・コンピューターサービス	165,414.5
32	Oracle	米国	ソフトウェア・コンピューターサービス	145,074.0
33	Intel	米国	電子機器・部品	140,462.4
36	Vodafone Group	英国	移動体通信	136,591.9
43	Qualcomm	米国	電子機器・部品	115,117.9
44	Cisco Systems	米国	電子機器・部品	113,912.5
46	Verizon Communications	米国	固定通信	108,401.9
60	Amazon.com	米国	小売	92,155.8
66	SAP	ドイツ	ソフトウェア・コンピューターサービス	85,605.0
71	Comcast	米国	メディア	81,264.5
74	Walt Disney	米国	メディア	78,469.5
81	Telefonica	スペイン	固定通信	74,663.5
82	Taiwan Semiconductor Manufacturing	台湾	電子機器・部品	74,554.7
85	NTTドコモ	日本	移動体通信	72,678.1
94	AMX	メキシコ	移動体通信	66,045.1
100	キヤノン	日本	電子機器・部品	63,369.7

図 2.1-1　世界の時価総額上位 100 社（2003 年から 2012 年）[20]

2.1.2 レコメンド機能を活用して事業を拡大するアマゾン

アマゾンの日本における 2012 年の年間の売上は 78 億ドル（7,300 億円）で、国内ネット通販では楽天の 4,434 億円を超えて首位となった。国内小売業全体でも家電量販店のエ

[20] 総務省「情報通信産業・サービスの動向・国際比較に関する調査研究」（平成 24 年）

ディオンを上回り 10 位前後に位置する[21]。

顧客の購買データを活用し、お勧め商品を紹介する「レコメンド」機能はアマゾンの大きな武器の一つとなっており、利用者が増え、購買数が増えるほど、「誰が」「何を買ったか」という情報の分析に基づくレコメンドは、精度が上がって行く。アマゾンで扱う商品は、本から、家電、衣料、食品へと拡大しており、日本の小売業に対する脅威となってきている。

2.1.3 国際市場で存在感が薄くなる日本メーカーの携帯電話・スマートフォン

市場が急拡大している携帯電話は、2010 年から 2012 年にかけて、7.7%から 1.9%へとシェアを失った。

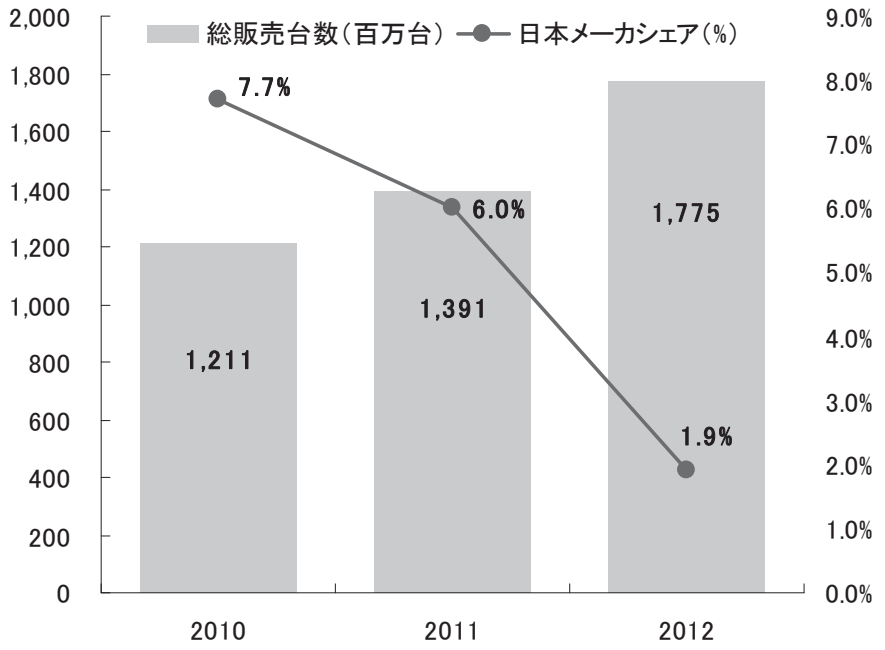


図 2.1-2　携帯電話の総販売数と日本メーカーのシェア[22]

また、伸張著しいスマートフォンも 2010 年から 2012 年にかけて、10.2%から 3.7%へシェアが低下した。

---

[21] 日経新聞 2013 年 2 月 19 日 http://www.nikkei.com/article/DGKDASGF1808Q_Y3A210C1EA2000/

[22] 総務省 「ICT 国際競争力指標」（平成 22 年、23 年、24 年）

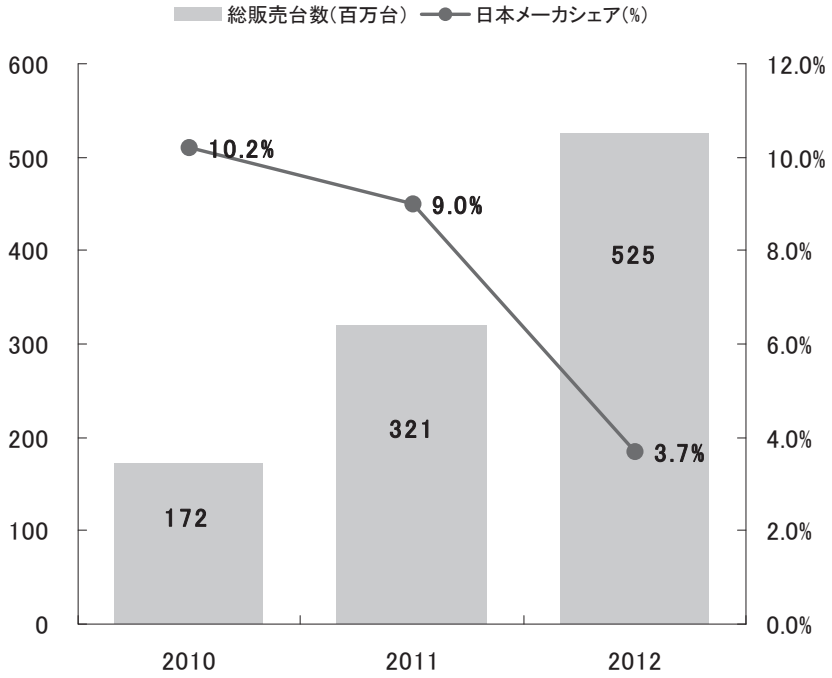


図 2.1-3　スマートフォンの総販売数と日本メーカーのシェア[23]

一方、日本企業の得意な「摺り合わせ型」で競争力を維持していたデジタルカメラ市場においても、徐々に販売台数が減少している。

スマートフォンは、高性能カメラを搭載しており、インターネットにも常時接続可能である。スマートフォンを持っていれば、好きな時に写真を撮り、その場で Facebook 等の SNS にアップロードすることができる。このような付加価値を利用者に提供するスマートフォンの台頭が、競争力あるデジカメの地位を脅かしてきている。

[23] 総務省　「ICT 国際競争力指標」（平成 22 年、23 年、24 年）

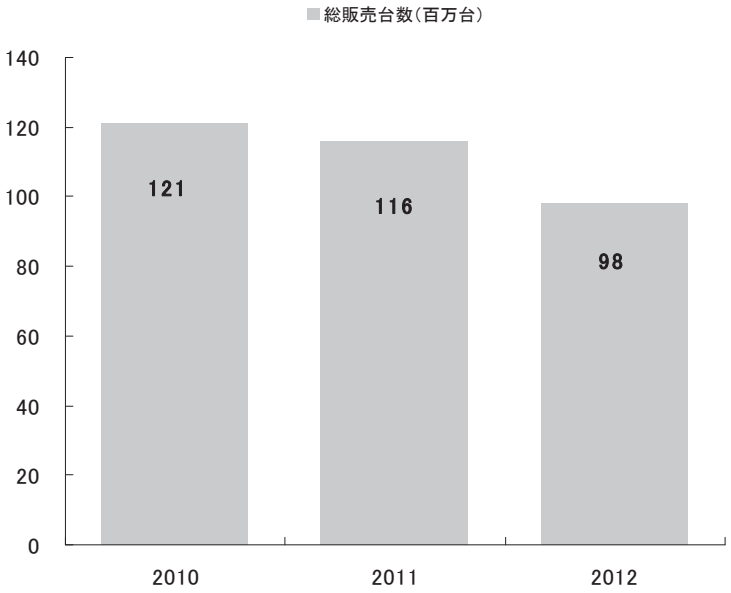


図 2.1-4　国内企業のデジカメ総販売台数[24]

スマートフォンやタブレットの OS は、Google と Apple の寡占状態となった。IDC の調査によると、Google のモバイル OS「Android」を搭載した端末と Apple の「iOS」端末（iPhone）を合わせた出荷台数のシェアは 2012 年第 4 四半期 91.1%となっている。

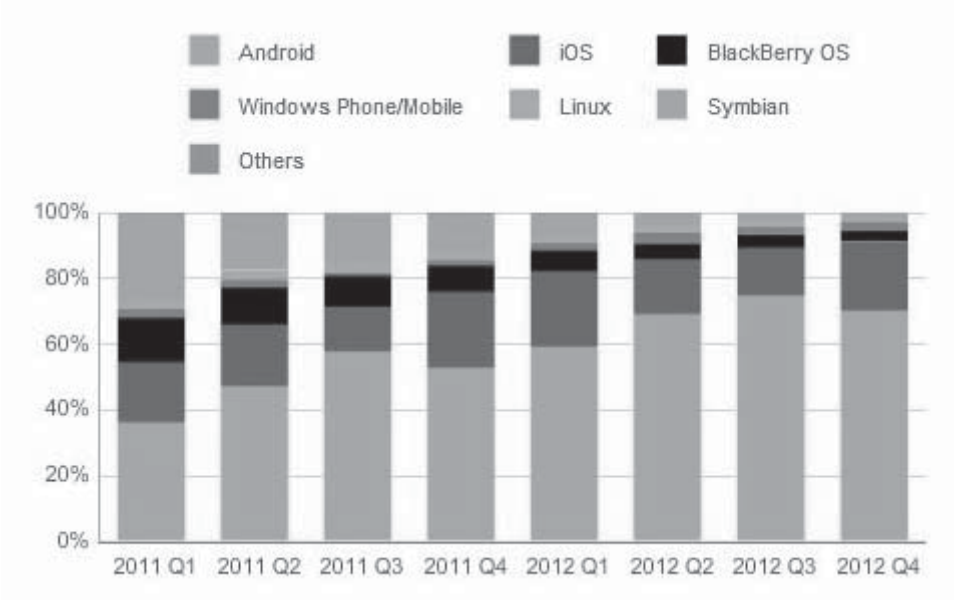


図 2.1-5　OS 別世界スマートフォンシェア推移[25]

24　一般社団法人カメラ映像機器工業会（CIPA）　「デジタルカメラの生産・出荷データ」
http://www.cipa.jp/data/dizital.html

25　IDC Press Release 14 Feb 2013
http://www.idc.com/getdoc.jsp?containerId=prUS23946013#.USXvwx2-3To

2.1.4 伸びるビックデータ市場へのグローバル戦略の見えない日本

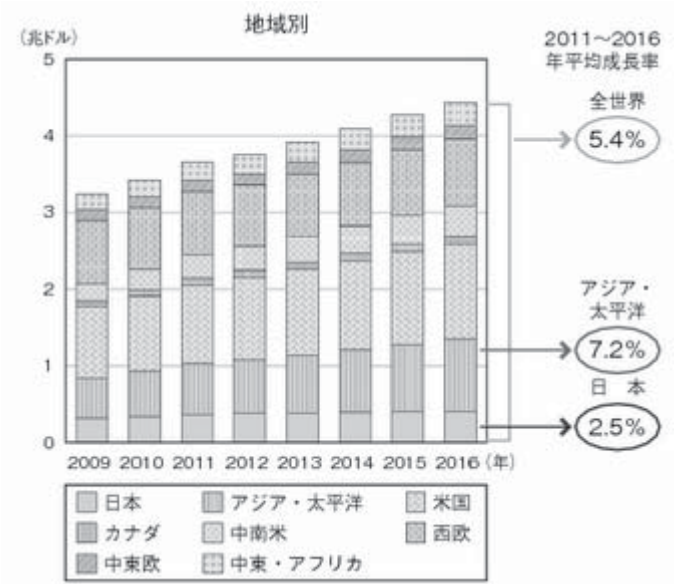


図 2.1-6　世界の IT 投資規模[26]

世界の IT の投資規模は、2011 年は 3.4 兆ドルで、2016 年には 4.44 兆ドルに伸長し、2011 年から 2016 年の年平均増加率は 5.4%となることが予想されている。

一方、近年注目が集まるビックデータの市場は、2011 年 45 億ドルで、2015 年には 168 億ドルに伸張し、年平均増加率は 39.4%となる。

特に、アジア・太平洋地域では、2011 年 2.6 億ドル、2015 年 12 億ドルで、年平均増加率は 46.8%となる。

[26] 総務省「平成 24 年版情報通信白書」
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/html/nc112220.html

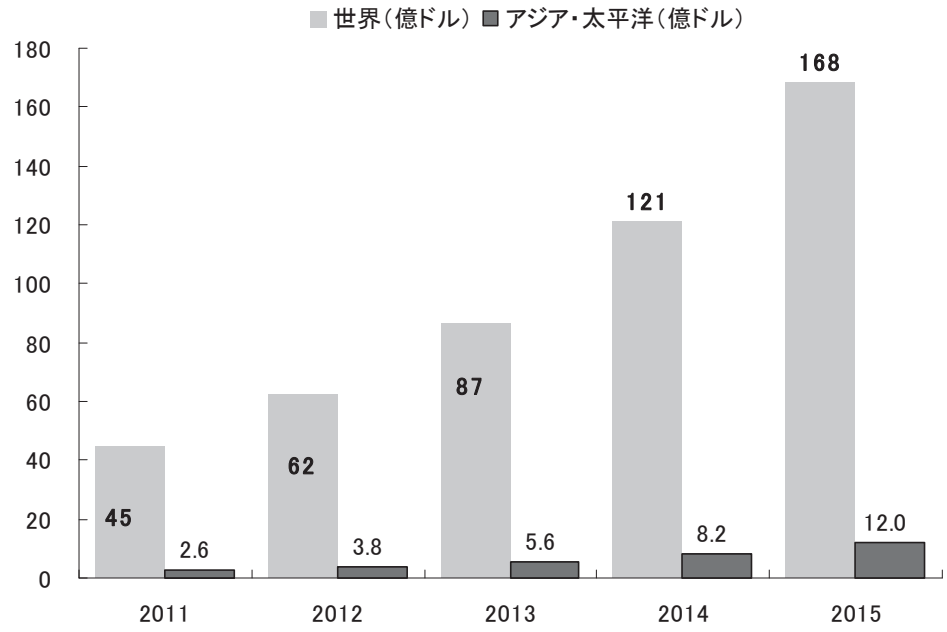


図 2.1-7　IT 投資規模[27,28]

ビックデータの分野では、情報の入出力デバイスであるスマートフォン、情報を蓄積・分析するクラウドが大きな役割を演じることが想定されている。しかし、スマートフォン・クラウドの日本の競争力は決して高いとは言えない。産官学の戦略的な取り組みを実施しないと、グローバルな IT 市場、特にこれから拡大の期待されるアジア・太平洋地域での競争力を失いかねない。

ビッグデータの分野で活路を見出すためには、機器や人の情報を収集・蓄積・分析して付加価値をもたらす事業に、積極・果敢に取り組むことが求められる。

人や機器の情報の収集・蓄積・分析サービスは、インターネットを経由で世界中にボーダレスに提供される。扱う情報は、各国の法律で規制される傾向にある。法制度整備の遅れ、プライバシー情報を使いこなす活用の遅れ、プライバシー情報の管理コスト増大、プライバシー情報に対する利用者（企業、エンドユーザ）の理解不足といった課題の解決が強く求められる。次節以降ではこれらの課題について述べる。

27 IDC Worldwide Big Data Technology and Services 2012-2015 Forecast
http://cdn.idc.com/prodserv/4pillars/download/IDC_Pillar_Promo_BigDataExcerpt.pdf

28 IDC　Big Data Emerging at a Rapid Pace Across Asia Pacific, IDC Reports 30 Oct 2012
http://www.idc.com/getdoc.jsp?containerId=prSG23762712#.USYHkx2-3Tp

2.2 法制度整備の遅れ

2.2.1 個人情報保護に関する各国法整備の状況

1970 年代から欧米諸国では個人情報保護に関する法の整備が進んだ。1980 年代には、各国の規制の内容の調和を図る観点から経済協力開発機構（OECD）理事会勧告において「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」が発行され、以降、各国で急速に個人情報保護法の整備が進められた。OECD 加盟国の大多数が公的部門と民間部門の双方を対象にした個人情報保護法を制定している。

日本でも 1989 年に「行政機関の保有する電子計算処理に係る個人情報保護に関する法律」が施行されたが、法令名が示す通り、公的部門のみが対象であった。EU データ保護指令の第三国条項や国内での個人情報に関する事件の多発に対応するため、民間企業を対象とする個人情報に関する法律の策定が急務となった。日本政府は、情報通信技術（IT）戦略本部に個人情報保護法制化専門委員会を設立し、2000 年に「個人情報保護基本法制に関する大綱」発表。本大綱をベースに法令制定作業を進め、公的部門・民間部門を対象とする「個人情報の保護に関する法律」がようやく 2003 年に施行された。

表 2.2-1　世界各国の個人情報関連法律[29]

制定年	国名	適用部門(公/民	法律名
1970	アメリカ	民	公正信用報告法
1973	スウェーデン	公民	データ法(1998年に新法)
1974	アメリカ	公	プライバシー法
1977	ドイツ	公民	データ処理における個人データの濫用防止に関する法律(データ保護法)
1978	デンマーク	公	公的機関におけるデータファイルに関する法律
〃	〃	民	民間機関におけるデータファイルに関する法律
〃	ノルウェー	公民	個人データファイルに関する法律
〃	フランス	公民	データ処理・データファイル及び個人の自由に関する法律
〃	オーストリア	公民	個人データの保護に関する連邦法律
1979	ルクセンブルク	公民	電子計算処理に係る個人データ利用規制法
1981	アイスランド	公民	個人データファイルに関する法律
1982	カナダ	公	プライバシー法(2000年に新法)
1984	アメリカ	民	ケーブル通信政策法
〃	イギリス	公民	データ保護法(1998年に新法)
1986	アメリカ	民	電子通信プライバシー法
1987	フィンランド	公民	個人データファイル法
1988	オランダ	公民	個人データ保護法
〃	アメリカ	民	コンピュータ・マッチング及びプライバシー保護法
〃	〃	民	ビデオプライバシー保護法
〃	アイルランド	公民	データ保護法
〃	オーストラリア	公	プライバシー法(1990年に改正で信用報告に適用)(2000年に新法)
〃	日本	公	行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律
1991	ポルトガル	公民	個人データ保護法(1998年に新法)
1992	ベルギー	公民	個人データの処理に係るプライバシーの保護に関する法律(1999年に新法)
〃	チェコ	公民	情報システムにおける個人データ保護法
〃	ハンガリー	公民	個人データ保護及び公共データ公開に関する法律
〃	スイス	公民	データ保護法
〃	スペイン	公民	個人データの自動処理の規制に関する法律
1993	ニュージーランド	公民	プライバシー法
1994	韓国	公	公共機関における個人情報保護に関する法律
1995	〃	民	信用情報の利用及び保護に関する法律
1996	イタリア	公民	個人データ処理に係る個人及び法人の保護に関する法律
1997	ギリシャ	公民	個人データ処理に係る個人の保護に関する法律
2000	カナダ	民	個人情報保護及び電子文書法
2003	日本	公民	個人情報の保護に関する法律

日本が公的部門・民間部門に対応するはじめての個人情報保護法の制定作業を進めている間に、諸外国は、1995 年に制定された EU データ保護指令への対応を進めた。

EU データ保護指令では、個人データの第三国への移転は、原則として「当該第三国が十分なレベルの保護措置（以下、十分性）を確保している場合に限って、行うことができる」と定められていた。

EU データ保護指令に関する日本の現状を以下に述べる。

2.2.2 十分性に関する日本の現状

1 章で述べたように、世界で準備が進められている一方、日本はいまだに十分性の認定手続を申請しておらず、十分性を認められていない。

EU からの公式な指摘は得られていないが、現在の日本の個人情報保護法は以下の点が

[29] 堀部政男「個人情報保護法の考え方」
http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu1/006/shiryo/04080202/003.htm

十分性の認定基準を満たしていないと思われる。

表 2.2-2　現状の日本の個人情報保護法における十分性を満たしていない事項[30]

十分性を満たしていない事項	EU データ保護指令	日本の個人情報保護法
開示請求	開示請求が個人情報の主体の権利（アクセス権）として規定	主体の権利としては規定されておらず、個人情報取扱事業者の義務としてのみ規定
監督機関	監督機関の設置を規定	監督機関に該当する概念はない
特別カテゴリーのデータの処理	人種、民族、政治的見解、宗教、思想、信条、労働組合への加盟、健康、性生活等の特別なカテゴリーのデータの処理を原則として禁止	処理を禁止する特別なカテゴリーは存在しない
適用対象事業者	個人情報を保有する事業者は、その件数の多少によらず指令の適用対象	保有する個人情報が 5000 件以下の事業者は、適用対象から外れる
第三国への情報の移転の制限	保護レベルの不十分な国への個人情報の移転を制限	個人情報保護法では、そのような制限の規定なし

30 髙野一彦「わが国におけるプライバシー・個人情報保護の現代的課題」
http://www.kansai-u.ac.jp/Keiseiken/books/sousho155/155_05.pdf

2.3 プライバシー情報活用の遅れ

クラウドコンピューティングやスマートフォンが普及し、そして SNS（social networking service）と呼ばれるソーシャルメディアやオンライン販売のサービスを通しても普及と共に、コメント投稿、閲覧・購買履歴、位置情報などの個人に関するプライバシー情報が日々大量に作られ、インターネット上に多く蓄積されるようになった。これらの情報はビッグデータと呼ばれておりビジネスへの活用が期待されている。ビッグデータの活用により、事業者は個人を対象として木目細やかなサービスやビジネスが提供されている。その一方、消費者の個人情報やプライバシー情報が予期しない形で利用、公開、共有が行われ、悪意を持った第三者に情報が渡った場合には情報の悪用（不正利用）やプライバシー侵害などの問題が発生する恐れがある。プライバシー侵害行為の様態には次の 4 つがある（プロッサーの 4 類型[31]）。

・一人で他人から隔絶されて送っている私的な生活状態への侵入
・知られたくない私的な事実の公開
・一般の人に誤った印象を与えるような事実の公表
・氏名または肖像を、己の利益のために盗用すること

2.3.1 プライバシー情報とビジネス

個人情報とプライバシー情報は概念が異なっている。個人情報は「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」である。個人情報はセンシティブ情報である必要は全くなく、名前や電話帳に載っているような電話番号や、店舗などの監視カメラの画像でも顔が識別できれば個人情報となる。また、顧客番号などであっても、顧客リストと台帳などと容易に照合できることで識別できる場合は個人情報に含まれる。

一方、プライバシー情報は「個人や家庭内の私事・私生活の情報（私事性）」、「一般の人々には知られていない情報（非公知性）」、「一般人の感受性を基準にすれば、当事者が公開を望まないであろう個人の秘密情報」といった情報である。

最近では、より広い概念として、個人の行動の監視、個人の会話の盗聴、私的領域に対する干渉などプライバシー侵害から保護するといった観点から、個人のいる場所や環境、行動に関する情報もプライバシー情報として取り扱うようになってきている。例えば、クレジットカード番号は単なる個人情報（データ）であるが、カードを利用した場所・店、購入したものや数量などの購買情報、利用頻度などはプライバシー情報となる。また、場所や環境、行動のセン

[31] 1990 年に、ウィリアム・L・プロッサー（William. L. Prosser）が「California Law Review　Vol.48 No.3」において、不法行為法上のプライバシーの侵害行為の態様を 4 つの分類に整理している。
William L.Prosser, Privacy,48,California Law Review, p383
http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf

シングするデバイスとして個人が持つスマートフォンの他、カメラ付きの自動販売機やデジタルサイネージ、街頭監視カメラからの情報もプライバシー情報とも言える。

プライバシー情報には、個人の考え方・心情、行動履歴、購買履歴、嗜好、SNS 情報など多くの情報が詰まっており、それらを分析し活用することで、OneToOne マーケティングのように個々に向けた新たなビジネスを創造することができるので期待されている。プライバシー情報を蓄積したものはライフログとも言われており、ライフログの収集と分析はビジネス上の大きな価値を生む。また、プライバシー情報はそのものだけでも売買の対象ともなるので、情報の収集や利用にあたって適切な取扱いが必要である。

2.3.2 プライバシー情報の適切な取扱いと監査

プライバシー情報の内容や公開範囲は、個人個人の考え方や判断、仕事や地域の環境、文化など様々な要因で変化する。従って、保護したいプライバシー情報が一般に同じとは言えない。プライバシー情報の保有者が自主的にプライバシーを公開した場合にはプライバシーとしての保護を受ける範囲がその分狭くなる。プライバシー情報の保有者が自主的にプライバシー情報をビジネスに利用しても良いとの同意を得た場合には、同意を得た範囲で、プライバシー情報をビジネスに活用して良いことになる。このため、利用者にプライバシー情報利用にあたって事前に許可を取る「オプトイン（Opt-In）」の方式を採用する必要がある。また、オプトインを適切に実施して許可を得たという記録を保存しておくことも必要である。反面、プライバシー情報の保有者がプライバシー情報の利用を禁止した場合には、直ちにプライバシー情報の利用を停止しなければならないことも考慮する必要がある。

欧米諸国では「EU データ保護指令（1995 年 EU）、EU データ保護規則（2014 年予定）」や「消費者プライバシー権利章典（2012 年米国）などのプライバシー情報の取扱いを定めた法規制があり欧米の企業はこれに従いビジネスにプライバシー情報を活用している。

日本には、個人情報を保護することを目的とした「個人情報保護法（2005 年成立、2007 年施行）」しかなく、プライバシー情報を適切に取り扱うための法規制は存在していない。このため、プライバシー情報を利用したビジネスを構築しにくい状況になっている。また、ビジネスが構築されたとしても安全性が担保されなければ、利用者が不安になりプライバシー情報を提供しないことも考えられ、ビジネスが成長しないことも予測できる。

Google や Facebook などの米国の企業は、ビジネスの拡大のために、プライバシー情報を積極的に収集し活用している。しかし、いくつかの問題も発生している（表 1.2-4）。米国連邦取引委員会（FTC）は、Google、Facebook への是正措置として、20 年間に渡る第三者監査を義務付けている。第三者監査はプライバシー情報の利用規制をするのではなく、利用者のプライバシー情報が適切に保護されているか否か、そして利用者のデータ収集に関して利用者の同意を取っているのか否かを監査することを目的としている。

このように、政府が企業に対して、プライバシー情報を適切に取り扱っているか否かを

監査する機能を持つことも健全なビジネス発展のために必要である。

2.3.3 プライバシー情報を活用する海外企業と日本企業の違い

Google や Facebook のプライバシーポリシーを見ると EU と米国間では、米国の民間部門の自主的取り組みをベースにした「セーフハーバー原則」に従うとしており、国内外において個人情報やプライバシー情報が適正に保護されて流通するような仕組みを導入している。特に、個人情報やプライバシー情報を利用する処理機能を利用するためには利用者の同意を得るようにしており、情報のコントロールができるようになっている。

例えば、米国 Facebook の SNS サービス「Facebook」と、日本のミクシィの SNS サービス「mixi」の違いは、プライバシーポリシーや利用規約を見るだけでもよく分かる。

Facebook プライバシーポリシーでは、利用者のプライバシー情報や行動を収集していることと、それを適切に利用することを明示するとともに、利用者に留意点を具体的に記載している。また、第三者の WEB アプリケーションとの連携についても明記している（収集対象情報の明記）。一方の mixi にはプライバシー取扱いに関しての記述はなく、ミクシィが個人情報保護法に従ってデータを管理することが利用規約に書かれており、プライバシーポリシーでは利用がやってはいけない一般ルールが規定されているだけで、どのような情報を収集し、どのように利用されるのかは明記されていない。

コンテンツの閲覧行動情報もプライバシー情報と考えられる。mixi では訪問先に閲覧情報が自動的につく「足あと機能」があった。しかし、「足あと」がつくことでコンテンツを閲覧したことが公開されてしまい、行動を把握されプライバシーが侵害されるとの判断で、2011 年 6 月に「足あと機能」を停止するに至った。これにより、利用者の興味のある広告を表示することができなくなり、ビジネスとしても損失を被った。利用者も自己防衛として、個人が特定できないような利用者アカウントの作成や、コンテンツ毎に異なるアカウント利用などの対策をするようになる。このような結果、不正や誹謗中傷、犯罪の温床となり健全性が損なわれて、退会する利用者が増加してビジネス価値が低下して行く。事実、調査会社ニールセンの調べによると、mixi の 2012 年 8 月の国内月間訪問者数は約 567 万人で減少傾向にあり、同じ条件での Facebook の訪問者数約 1673 万人に大差をつけられている。ミクシィ発表でも、2011 年 5 月の約 1547 万人をピークに横ばいか減少傾向が続いている。「足あと」など Facebook にはない mixi 独自の機能が次々と廃止・変更されたことで利用者の支持が離れたことも一因と見られる。mixi の例では、SNS での振る舞いや行動を取得する「足あと機能」の有効化／無効化をオプトインとして利用者にコントロールさせていれば問題がなかったものと考える[32]。プライバシー保護を考えるのであれば、

[32] 現在、2013 年 1 月末より「足あと機能」に代わる機能として「リアルタイム訪問者機能」の試験リリースが開始されているが、プライバシー保護機能については何も明示されていない。

自分で個人に関わる情報の記録、閲覧、更新、削除、公開範囲の制限ができる「自己情報コントロール機能」が必須である。

Facebook の基本機能には「足あと機能」は存在しない。Facebook にはグループメンバーのみが、グループ内のコンテンツ（投稿）についてのみ、いつ確認したか分かる機能がある。これはグループ内だけに公開範囲であるので、不特定多数にプライバシーを公開することはない。ただし、Facebook では認定された多くのアップリケーションがアクセス解析アプリを提供している。利用規約や提供するデータについての同意を求めてくるので、同意しなければ勝手に動作することがないようになっている。

また、米国では Do Not Track 機能と言われる、利用者によりウェブトラッキング遮断する仕組みが検討されている。Do Not Track 機能は、消費者プライバシー権利章典の中で、消費者による自己情報のコントロールを及ぼすべき事例として明示的に規定されており、今後、民間レベルでの自主規制ガイドラインという形を含め、採用が強化されて行くものと考えられる。

米国と日本のプライバシー情報保護に関する状況を SNS の Facebook と mixi について記述したが、このように欧米と日本ではプライバシーポリシーの扱いに大きな差がある。これは、欧米ではセーフハーバー原則に従ったプライバシー情報の取扱いに関した法規則やガイドラインといったルールがあるが、日本にはこれらが存在していないことが原因となっていると思われる。ルールが無くやって良いことが明確でないので、安心してプライバシー情報が使えない。このため、ビジネスにプライバシー情報を活用することに対して躊躇することにもなる。SNS やオンライン販売の利用者からプライバシー情報を適切な方法で収集して安心して利用できるようになれば新たなビジネスやサービスが生まれてくると思われる。米国では既に表 1.2-1 に示すような新たなサービスが登場している。日本政府でも、総務省及び経済産業省では個人情報やプライバシー情報といった「パーソナルデータ」を安全に取り扱うための研究会を開催している[33,34]。早期にプライバシー保護と取扱いに関してルールを定めることがプライバシー情報を活用したビジネスの創造と発展に不可欠である。

利用者は、SNS やショッピングサイトなどでプライバシー情報を提供することで便利な機能やポイントがつくなどのメリットがあるが、安易に情報を提供するのではなく、どのような情報を提供するのか、そして提供された情報がどのように利用されるのか、そして、その情報が漏えいした場合にはどのような影響があるのかを見極める必要がある。目先の損得や利便性だけでプライバシー情報を提供してはならない。

---

[33] 経済産業省：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
http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#it_yugo_forum_data_wg2

[34] 総務省：パーソナルデータの利用・流通に関する研究会
http://www.soumu.go.jp/main_sosiki/kenkyu/parsonaldata/index.html

2.4 プライバシー情報の管理コスト増大

プライバシー情報を適切に収集して安全に利用することがビジネスを提供する企業には望まれている。このプライバシー情報の管理コスト」にも目を向けなければならない。

まず、プライバシー情報を管理するために何が必要なのかを検討する。

2.4.1 プライバシー情報の保護機能と課題

プライバシー情報を収集して安全に管理するために、利用シーン毎に管理すべき内容は次の通りである（表 2.4-1）。

表 2.4-1　プライバシー情報の利用シーンと管理内容

シーン	管理内容
データ収集	・利用者の特定（本人の識別） ・利用目的の記載と適切な利用許諾 ・利用目的の変更時の利用者への再承諾 ・利用者から得た別個人の情報への利用承諾
データ保管、分析	・データの安全な保管（匿名化、暗号化） ・利用者による自己情報コントロール機能（確認、訂正、削除、移動・公開制限）
データ利活用	・データの共同利用の制御 ・データの取扱いに関するルールの共通化

このような管理内容を実装することで､プライバシー情報が適切に収集できるとともに、プライバシー情報を保護することができる。

データの収集時には、収集する相手がプライバシー情報の保有者本人なのかを確認することが望ましい。その後、利用目的を説明してプライバシー情報取得の承諾を得る必要がある。また、利用目的を変更した場合にもそれを提示して承諾を得る必要がある。必要であれば、利用者から得た別個人の情報をどのように使うのかを明示して承諾を得なければならない。例えば、利用者のアドレス帳などに記載されている知人のデータなどがこれにあたる。この場合に、利用者のメリット／デメリットだけでなく、別個人のメリット／デメリットを明確にして、利用承諾を得ることが望ましい。

データの保管、分析時には、データをサーバなどに匿名化技術や暗号化技術を用いて安全に保管して、改ざん、漏えいなどが発生しないようにする必要がある。また、海外のプライバシーに関わる法制度に対応するために、使用者に対して「自己情報コントロール機

能」が必要になってくる。自己情報コントロール機能の構成要素は、個人の権利としての「アクセス（確認）」、「訂正」、「削除」、「利用停止」、「データポータビリティ」と、事業者の義務としての「収集制限」、「保有条件（データの正確性の維持）」、「利用制限」、「事業者情報の公開」と分かれる（表 2.4-2）。

データの利活用時には、他のサービスでプライバシー情報を利用するにあたって、利用者にデータの共同利用の承諾と、共同利用や移転して良いデータ項目を選択できる制御機能があることが望ましい。また、データを共同利用する場合の、取扱いルールを共通に策定する必要がある。

表 2.4-2　自己情報コントロール機能と内容[35]

構成要素	自己情報コントロール機能	自己情報コントロール機能の内容
アクセス・確認	自己情報へのアクセス	自己情報へのアクセス（自己情報の登録や確認等）が可能
	履歴の表示	自らが過去に当該サービスに対して行った行為の履歴の閲覧が可能
	他者による自己情報の参照履歴の表示	他者が自己情報を参照した場合の履歴の確認が可能
	情報伝達経路の追跡	確認時、自己情報の伝達経路を追跡可能（情報伝達経路の追跡技術）
訂正	自己情報の訂正	自己情報の訂正、更新が可能
	複数サービスで連動した自己情報の訂正	複数サービスのいずれででも自己情報の訂正と同期が可能
	情報伝達経路の追跡	訂正時、自己情報の伝達経路を追跡可能（情報伝達経路の追跡技術）
削除	自己情報の削除	自己情報の削除が可能
	履歴の削除	自らが特定の情報を参照した場合の履歴削除が可能
	情報伝達経路の追跡	削除時、自己情報の伝達経路を追跡可能（情報伝達経路の追跡技術）
利用停止	自己情報の利用停止	自己情報の利用停止が可能

[35] 独立行政法人情報処理推進機構「『パーソナル情報保護と IT 技術の調査』報告書」
http://www.ipa.go.jp/security/fy23/reports/pdata/index.html

データポータビリティ	自己情報の規定フォームへのコピー	当該サービスに登録している自己情報の、規定のフォームへのコピー・印刷、保存が可能
	自己情報の共有、移動	自己情報を複数のサービス間で共有、移動することが可能
	自己情報の携帯	自己情報を一元管理でき、その情報を別の事業者へ提示することが可能
収集制限	Do Not Track 機能	Web サイト上での自らの行動が追跡されることを禁止するように通知可能
	オプトアウトツール	Cookie の置き換えにより、行動ターゲティング広告を停止可能
保有条件	保有条件	データの正確性の維持
利用制限	公開する自己情報の選択	どの自己情報を外部に公開するか設定可能
	公開範囲の制御	自己情報の公開範囲を制御可能

このように、プライバシー情報を適切に取り扱うためには、それぞれのプライバシー情報の利用シーンで考慮しなければならないことが多くある。これらの機能の実装は、人的ミスによる事故の発生を防ぐために、できるだけ自動的に実施するのが望ましい。

MRI 報告書・第 4 章に「プライバシー保護に関わる技術」があるが、これらのプライバシー情報を保護する技術はまだ一部のシステムでの利用あるいは開発中にとどまっており、確立していないのが実情である。現状では、どのようなプライバシー情報保護技術を、どの程度、あるいはどの範囲まで実装して対処すれば良いのかが明確ではない。安全のために脆弱さを無くすことを目的として多くの技術を実装しようとすると技術の導入や運用に費用が掛かりコスト高となる。反対に、コストを優先するあまりにプライバシー情報の保護に脆弱な箇所を作ってしまうと、プライバシー情報の改ざんや漏えいなどの事故を起こし多額の賠償金を支払う可能性もある。また、プライバシー情報はそれを保管しているだけでも安全に保護しなければならないのでコストが発生する。従って、ビジネスと導入技術とコストのバランスが必要であるが、これらは業界や扱うプライバシー情報によって異なるので、業界毎にプライバシー保護に関するガイドラインが必要である。

ガイドラインでは、プライバシー情報の活用で実施して良いことをルールとして明確にすることで、不正に取り扱うビジネスや事業者に抜け道を作らないようにすることも重要である。

2.4.2 各国法制度への対応

欧米諸国では「EU データ保護指令（1995 年 EU）、EU データ保護規則（2014 年予定）」や「消費者プライバシー権利章典（2012 年米国）などのプライバシー関連の法規制がある。

近年の IT ビジネスではクラウド・ネットワーク活用したビジネスが主流となってきている。クラウド環境では、データが世界各国を移動する可能性が高く、データ保有国の法制度に従う必要がある。特に欧州では、プライバシーは基本的人権と捉えられており、個人の自由から分離することはできない。EU が強い権限を持って、プラシバシー保護に関わる法制度の整備を進めているのである。このため、プライバシー情報を含むデータを EU から第三国に転送する場合、第三国の個人情報保護制度が十分なレベルの保護基準に適合しない場合、データ転送が制限されてしまう。データ制限を受けずにビジネスを展開する場合には、企業が採用しているセキュリティ対策と実行プロセスが規則に準じていることを証明する必要がある。

米国では、米国商務省とデータ保護に関する欧州委員会との間でセーフハーバー原則に基づく協定を 2000 年に締結しており、米国内の企業・組織が個人を特定しうる情報を EU から米国に転送する際に、EU が要求する法的条件を満たすための指針が提供されている。また、企業はセーフハーバー原則に遵守していることを証明するために、米国商務省が定めた「セーフハーバープログラム[36]」の認証を取得るだけで良い。

現在の日本は、セキュリティ先進国にくらべて大幅な体制整備が遅れており、各国と政府間で取り決めたデータ保護を目的とした条約はない。日本国内では日本情報経済社会推進協会（JIPDEC）により付与さえる「プライバシーマーク制度（P マーク制度）[37]」はあるが、その内容は EU データ保護指令の要求を満たしておらず、EU からは認められていない。従って、EU 諸国からデータ転送を望む日本企業は各国と個別に契約を締結する必要がある。これには、各々の企業がデータの保護基準に達していることを EU に対して証明する必要があり、莫大なコストが必要になる。また、EU データ保護指令に準拠するために実施すべきことや導入施策の基準が明確でないので対策コストがかかる可能性が大きい。

---

[36] セーフハーバー原則では、プライバシー保護方針において、通知、選択、転送、セキュリティ、データ統合、アクセス、施行などについて遵守すべき基本原則が定められている。
Safe Harbor Home：http://export.gov/safeharbor/index.asp

[37] 本情報経済社会推進協会（JIPDEC）プライバシーマーク制度　http://privacymark.jp/

2.5 利用者のプライバシー情報に対する理解不足

エンドユーザが正しいプライバシー情報の提供の仕方､利用の仕方を身に付けることは、プライバシー情報を活用するサービスの発展に不可欠である。しかし、現状はエンドユーザのプライバシー情報に対する理解は十分ではない。

2.5.1 エンドユーザのプライバシー情報に対する理解不足

(1) プライバシー情報に関するリスクの認識が低い

表 2.5-1 に示したように日本のインターネット利用者は、EU と比較してプライバシー情報に関するリスクの認識が低い。

表 2.5-1　プライバシー情報に関するリスク認知[38]

リスク	懸念している	
	EU	日本
1.企業は、私について、プライバシだと思う情報を保有している	61%	54%
2.私の個人情報が、私の知らないところで使われている	82%	65%
3.私の個人情報が私の合意なしで第三者間で共有されている	81%	64%
4.いろいろなところから個人情報を用いて、私がどんな人であるかという情報が形成されている	75%	43%
5.オンラインでは、個人情報によって、私の考えていることや行っていることがゆがめて伝わる場合がある	69%	42%
6.オンラインでは、個人情報によって、私は、評判が悪くなっているかもしれない	62%	33%
7.オンラインでは、第三者が私になりすます危険にさらされている	74%	47%

(2) プライバシー情報を自分で管理・コントロールする意識が低い

表 2.5-2 に示すように、日本のインターネット利用者は、サイトの安全性を確認してプライバシー情報を入力するといった基本的な確認は実施している。しかし、プライバシーポリシーを読むといった一歩踏み込んだ確認は、明らかに EU のインターネット利用者よりも実施していない。

[38] 独立行政法人情報処理推進機構セキュリティセンター
「eID に対するセキュリティとプライバシーに関するリスク認知と受容の調査報告」（2010 年 8 月）

表 2.5-2　プライバシー情報の自己防衛のために積極的に実施するデータ管理策[39]

自己防衛のためのデータ管理策	EU	日本
ウェブサイトのプライバシーポリシーを読む	69%	33%
自分を特定されないように偽の電子メール・アカウントを使用する	84%	16%
クッキーを消去する	56%	23%
重要な個人情報を入力する前に、取引が保護されている、あるいは、サイトが安全であるという表示を持っていることを確認する	28%	40%
プライバシを確保するためにブラウザーのセキュリティ設定を変える	64%	24%

これらの結果は、相手を性善説で信用する傾向がある日本の文化的な背景にも一因があると思われるが、プライバシー情報が悪用される事件等の具体例によってリスクを示し、そのような事件に巻き込まれないためにどのような対策を具体的に示すといった啓発活動の必要性を示している。

(3)「プライバシー情報の管理は企業任せ」という意識

インターネットのサービスを提供する企業は、特にプライバシーポリシーを開示している企業は、適切にプライバシー情報を管理している、という意識がある。

プライバシーポリシーをよく読むと、想定を超えるプライバシー情報が取得されていたり、想定を超える目的に利用されたりしている場合がある。

プライバシーポリシーで取り扱う情報とその利用目的を明示すれば、どのような処理をしてもよい、という企業が存在することを理解していない。扱うプライバシー情報とその利用目的を確認するという最低限の習慣は身に付けるべきであろう。

(4) プライバシー情報のネットへの記載の影響が想像しきれない

インターネットにおける情報の検索力と拡散力の強さに対する理解不足がある。そのために、身内でのみ共有すると想定していたプライベートな情報がネットで拡散し話題となり、謝罪、退学、解雇に至るといったケースが見られる。

例えば以下のようなケースがありえる。

「19 歳の大学生が個人のブログに「飲酒をした」といった証拠となる写真付きで記載した。それをネットで見つけた人が、ツイッターで記事を紹介し、あっという間にネットに拡散した。当人は、退学となった。」

上記のような状況は、インターネットの検索力、話題性のある情報のネットでの拡散力が非常に強力であることを理解せず、情報が身内でしか共有されないという思い込みに起因する。

---

[39] 独立行政法人情報処理推進機構セキュリティセンター
「eID に対するセキュリティとプライバシーに関するリスク認知と受容の調査報告」（2010 年 8 月）

自分のプライバシー情報が、想定を超えた膨大な範囲の第三者に容易に共有されうるリスクを理解していれば、情報の共有範囲を限定する設定をしたり、プライベートな情報は記載しないといった情報の管理の意識も高まるだろう。

(5) 収集・開示されるプライバシー情報に関する知識が低く利便性を優先してしまう

スマートフォンはいつでもどこでもインターネットにアクセスでき、アプリをダウンロードして利用することでソーシャルメディア等の人気のサービスを簡単な操作で利用できる。しかし、一方、スマートフォンは位置情報等プライバシー情報を継続的に計測・収集しており、アプリの利用の仕方次第では、行動した経路が継続的に開示される等のリスクがある。スマートフォンのアプリは利用者の行動・活動を継続的に把握可能となってきているという認識を持ち、収集されるプライバシー情報、公開される可能性のある行動・活動には常に注意を払うべきである。

第3章　提言

本報告書では、プライバシー保護を取り巻く IT 環境の変化として、クラウドコンピューティング、スマートデバイスと BYOD、ソーシャルメディアサービスの普及を取り上げた。また、クラウド側に集約された膨大な情報すなわちビッグデータの分析結果に基づくマーケティングが進化して注目を集めている一方、その取扱いにおいてプライバシーに対する配慮が不可欠であることを示してきた。

また、クラウド側に移動している情報がどの国に集約しているかに着目した場合、米国企業の保有するサービスへの集中化が顕著であり、他の国々にしてみると情報の輸出超過が顕在化していることを示した。情報の輸出超過は、その利活用機会の減少を招きかねないため、EU 指令などはプライバシー保護と同時に情報の国外流出に歯止めをかけるための施策としても機能しているという見方が指摘されている。

このような環境下では、プライバシー保護施策には、IT 産業の振興を加速する効果が期待される。日本にとってのプライバシー保護の課題は、2 章で述べたように下記のように整理されるが、それぞれの課題に対して、国、業界団体、会員企業が IT 産業振興のために実施すべき施策を提言する。

表 3.1　プライバシー保護の課題とリスク

プライバシー保護の課題	放置によるリスク
産業競争力の低下	アメリカの優位拡大
法制度整備の遅れ	他国の産業保護政策による非関税障壁
プライバシー情報活用の遅れ	ビッグデータ活用機会の損失
プライバシー情報の管理コスト増大	利益圧迫に伴う事業収益悪化
利用者の理解不足	本人特定・公開等のプライバシー侵害

3.1 国

3.1.1 産業競争力の低下を改善するための施策

ビッグデータの活用とプライバシー保護において、日本企業の振興を支援するために有効な施策として、国による税制優遇措置を挙げることができる。日本企業が競争力を強化するために実施するビッグデータ活用のための投資活動を対象に税制優遇することにより、これがインセンティブとなって取り組みが加速され、企業のグローバルなビジネス展開が活発化されることが期待される。

優遇対象とするビッグデータ利用の具体的な例としては、1.2.2 で示したライフログ活用サービス等を挙げることができる。国や地方自治体が保有するライフログに対して、その

匿名性を保証しつつ、医療や教育等への活用を奨励するものである。

企業の活用を支援するためには、活用可能なビッグデータアクセス機構を構築するとともに、国や地方自治体が保有するライフログの活用におけるプロセス定義や活用条件の設定等、産業振興を目的として設定してゆくことが望まれる。

ユーザ保護の観点では、オプトインやオプトアウトの規約を整備し、活用フォームを制定して積極的に活用している企業活動についても優遇措置の対象とすることが、併せて有効であると考えられる。

3.1.2 法制度整備の遅れを解消するための施策

企業のグローバルなビジネス展開を通じた産業活性化のためには、税制優遇措置などのインセンティブに加えて、海外のプライバシー保護法制と比肩しうる日本国の法制度の整備が不可欠である。海外の事例を調査しても、プライバシー保護に関する制度制定の目的として各国の産業拡大政策と密接な関係を持っていることが明らかとなっている。

国は、日本の産業振興を促進する法令を制定して国際標準としてゆくことで、利用者のプライバシーを保護すると同時に産業活性化を促進することが期待される。国際標準化の過程では、外国企業の国内展開に対する許認可制を強化することによって、他国の牽制と協調を擁護することも望まれる。

日本企業にとって実施可能で、諸外国の動きを牽制でき、プライバシー保護の潮流に逆行しないプライバシー保護施策の一例として、国内で浸透しているPマークの活用が考えられる。活用に向けた活動は、Pマークと諸外国の保護ポリシーの違いを確認し、必要最小限の改定を行って、外国企業への義務付けと国内企業への適用を促進するものとなる。

整備された法律の適用に際して、どの国の動きと協調してゆくかは、IT産業の振興に影響をもたらすため戦略的な選択が必要となる。協調の枠組みとしては、大別してEU連携、米国追従、及びAPEC協調といった、3つの選択肢がある。

EU連携では、日本においてもプライバシー保護を目的とした法令を制定し、日本人の個人情報を取り扱う企業に対して遵守を義務付ける。これにより、主として米国の情報収集力を牽制すると同時に、日本企業がEUと同等のプライバシー保護を進めていることを持って、EUとの間の障壁を緩和する効果が期待される。

米国追従の場合、セーフハーバーに相当する法律を制定し、この遵守を企業に求めることとなる。情報の輸出超過に対する効果は期待できないが、EUとの間の障壁緩和には一定の効果を期待することができる。

APEC協調路線を選択する際には、APECエコノミーで事業を行うために越境プライバシー・ルールを適用して参入する米国企業に対する内部ビジネスルール開発や、遵守情報を把握するための方法に関する提案等に関与する事が望ましい。このことにより、APECを中心とした経済圏における日本の主導的立場を強固にすることが期待できる。

上記選択肢は排他的なものではないため、情報流出状況を把握しつつ、並行して進めてゆくことが望ましい。

3.1.3 プライバシー情報活用の遅れを挽回するための施策

主に利用者のライフログを収集して構成されるビッグデータは、プライバシー情報を含む一方でその分析結果をマーケティングに活用することによるビジネス貢献可能性を保有している。総じて国内での利活用が遅れているが、その要因の一つに、ビッグデータを活用するための専門家の不足を上げることができる。

(1) ビジネス部門のデータ活用企画

マーケティングにおけるビッグデータ分析結果活用は、従来のビジネスプロセスにおいては一般的ではないため、これらの発想ができるマーケッターやプランナーの獲得が重要となる。各企業の要請を受けて、国の指定する専門家による教育・トレーニングの場を設け、専門家を育成する事が望まれる。

(2) 開発部門のデータ保管・処理システム開発

ビッグデータを収集して分析可能な状態に管理するシステムを構築するためには、NotOnly SQL、超並列データベース、データマイニング、グリッド、エンタープライズサーチなどの技術を活用してシステムを設計する専門能力が必要となる。技術革新の激しい領域であり、個別企業がキャッチアップするには困難が伴うため、国による専門家育成プログラムの設立と企業技術者の受け入れなどの支援を行うことで企業が専門家獲得を支援する事が有効である。

(3) 蓄積されるビッグデータの分析モデル設計及び分析処理

ビッグデータの分析とその結果からの意味の取り出しを行うスキルは、マーケッターやシステム開発者とは異なる専門性を要求される。マーケティングの目的を理解しつつ、システムが保持しているデータを分析する役割は、アナライザやデータサイエンティストと呼ばれ、人材の確保、育成課題の一つとなっている。この分野の専門技術者の育成はビッグデータ活用に不可欠であり、企業毎の取り組みが困難になっているのが現状である。ここでも、国の支援による育成が必要である。

3.1.4 プライバシー情報の管理コスト増大を抑止するための施策

プライバシー管理に必要な技術については、セキュリティ技術、暗号化技術、検索技術、マイニング技術、配信技術等、多岐に渡って関与することが明らかとなっている。このよ

うな状況下では、技術を開発する側も技術を活用してプライバシーを管理する側も、投資対効果に関する分析と技術選択を進めることが難しい状況にある。

そのため、これら一連のプライバシー保護に有効な技術の体系づけを行い、既存技術の明確化と不足技術の特定を進めることが望まれる。さらに、不足技術に関しては、開発支援事業による開発促進と活用しやすいライセンス体系整備による利用振興を進めることによって、プライバシーを活用して企業競争力を進めようとする企業の管理・運用コスト削減に寄与することが期待される。

3.1.5 利用者の理解不足を解消する施策

ライフログが利用者の知らないうちに収集され利用された場合、利用者が同意した利用規約の内容が重要になってくるが、利用時に提示される規約に関して十分な配慮を行うよう啓発して行くことが大切になる。

利用者が個人の場合には、公共広告等を通じて、ライフログを取り扱うアプリケーションやサービスを利用する際に、該当する利用規約を確認して、意図しない収集や利用が行われないことを確認することの重要性を知らしめることが有効であろう。また、オプトアウトを活用して利用を見直すことの有効性を説くこと等も、国や公共機関でなくてはできない啓発活動である。

企業における利用者に対しては、企業向けに注意を喚起する目的の利用ガイドラインを提供することは有効であろう。特に、企業内利用者が個々に利用規約への同意を判断するような状況は、企業のポリシーの徹底を阻害する要因になりかねない。

これらの施策について、既にいくつかの公共団体による取り組みが行われているが、国のリーダシップによって活動の歩調を揃えることにより、より大きな効果を期待することができる。

また、利用者の教育には限界があるため、国が有料アプリケーションを識別ための審査を遂行したり、適合性が確認されたアプリケーションを記載したホワイトリストの管理を行うことにより、利用者の選択・判断を支援することも有効であると考えられる。

3.2 業界団体

3.2.1 産業競争力の低下を改善するための施策

ビッグデータを活用して企業競争力を高めるために、業界団体が支援できることして、業界が保有するビッグデータの利用を促進するために利用に関するコンセンサスの形成、利用を促進するビッグデータの業界プラットフォーム化、及び適用事例の共有促進が考えられる。

利用に関するコンセンサスの形成とは、各企業が単独で実施するには躊躇する利用内容に関して、業界団体としてリスクアセスメントを行い、プライバシー保護に必要な施策とセットで実施に関する合意を会員企業と結ぶことである。このことは各企業の積極的なビッグデータ活用を促進すると同時に、各企業で実施したのでは不十分になりがちなプライバシー保護施策についても網羅的に対処することができると思われる。

ビッグデータの業界プラットフォーム化とは、国が解放するライフログに業界団体が保有する情報を加え、企業毎に縦割りになりがちなデータを業界として水平型プラットフォーム化し、利用を促すことを想定している。利用に関する規約の制定や会員企業の利用に際しての様々な審査なども含めて、業界団体としての推進が望まれる。

一方で企業におけるビッグデータの活用に際して、プライバシー保護への配慮があり、積極的な利用に躊躇していることも要因の一つとなっている。適用事例の共有促進とは、いわゆるベストプラクティスを業界内で共有することにより、活用の効果を確認し、ビッグデータの積極的な活用を促すものである。

3.2.2 法制度整備の遅れを解消するための施策

国がPマークを中心としたプライバシー保護政策を展開する場合、会員企業がこれに対応するための支援が必要となる。既に取得済企業では新たな変更への対処が必要となり、未取得企業への、その取得の奨励と取得に向けた支援活動が有効となる

また、ビッグデータの活用に必須のプライバシー保護施策において、利用規約は非常に重要な役割を持つ。これに関しても、ビッグデータの活用側面同様、個々の会員企業が個別に検討を重ねるよりも、業界団体が多角的に検討した結果としての雛形を会員企業に提供し、適用結果のフィードバックを得ながら改定してゆくことは業界内の一貫したポリシーを保つために有効である。利用規約は利用者に利活用の目的範囲を示すと同時に、企業活動を守るためにも環境の変化に適合させてゆく必要がある。

利用規約は国毎の法令の影響を受けるケースが多いが、米国企業の一部ではサイト毎に利用規約を提示し、ワールドワイドでこれを統一して行く動きが見られるという情報がある。同時に、オプト・アプトを有効に活用して、利用者の保護と企業の活動が両立できるように移行しているとのことである。グローバルな活動を行う業界団体では、これらの展開を視野に入れた規約の検討が求められる。

3.2.3 プライバシー情報活用の遅れを挽回するための施策

ライフログを収集して構成されるビッグデータの利活用が遅れている要因に専門家の不在を指摘したが、国等が提供する育成機構を積極的に活用して人材を育成するよう会員企業に働きかけるのは、業界団体の重要な役目と思われる。

ビッグデータの活用は、複数の専門家すなわち、「ビジネス部門のデータ活用企画担当者」、「開発部門のデータ保管・処理システム開発担当者」、「蓄積されるビッグデータの分析モデル設計及び分析処理担当者」がそれぞれの専門性を生かしてゆくことで効果を発揮する。業界内での専門家の認知を進めるとともに、専門家同士の情報交換やノウハウ共有の場を提供することも業界団体の重要な役割となろう。

一方で、専門家におけるノウハウそのものは個人のスキルであり、企業にとっては競争力であるため、その開示に関しては困難が伴う。しかし、プライバシー保護のための施策や対処経験に関する情報交換については、企業の枠組みを超えて共有することで利用者と企業双方のメリットにつながるため、この点に関しては業界団体の積極的な推進が望まれる。

3.2.4 プライバシー情報の管理コスト増大を抑止するための施策

プライバシー情報を管理する場合、会員企業が単独で取り組む際には、必要となるコストが増大する傾向にある。しかも、これらは直接利益を生み出すための費用でないためにどうしても抑制傾向にあり、結果としてリスクを許容することになりかねない。

そのため、業界団体としては個々の企業の取り組みでは限界のあるプライバシー管理に必要な活動すなわち、ベンチマーク、ガイドラインの制定、技術選択、システム構築、システム運用について支援することが望まれる。

プライバシー管理に関するシステム構築や運用費用に関するベンチマークは、システムの要件定義の参考や投資規模の判断の際に有効となる。これを会員企業毎に実施することは困難なので、業界団体が調査と情報展開を推進することで、企業の負担を軽減することができる。

プライバシー保護ガイドラインの策定と展開は、業界のポリシーや保有するライフログの特性等を考慮して制定し、会員企業に準拠を促すことにより、利用者に対する安心を提供すると同時に保護の水準を業界で設定することができる。

技術選択を支援するため、国の支援によって開発されるプライバシー保護技術及び業界団体に所属する企業が保有する技術のカタログ化を行い、保有するプライバシー情報の特性に応じて技術選択しやすい環境を提供することは会員企業にとって有効である。

システム構築に関しては、技術選択の結果個別システムとして開発するケースや既存システムのプライバシー情報保護をアウトソースサービスとして依頼するケースなど、多様な実施例に関する情報を会員企業間で共有できるような枠組みを作ることは会員企業がシステム構築もしくはサービス利用を検討する際の貴重な情報源となる。

セキュリティ保護に関するサービスを利用する際には対象外となるが、独自にシステムを構築してこれを運用する場合、システム運用を継続的に実施する必要がある。その運用に必要な技術や費用についても、人材育成、運用改善事例紹介、等によって会員企業の運用設計や運用管理を支援することが望まれる。

3.2.5 利用者の理解不足を解消する施策

業界団体には、業界毎にライフログを提供している利用者に対しての教育・啓発活動を実施することが望まれる。具体的には、ライフログが利用されることでどのようなメリットを享受できるのか、ライフログがどのように安全に管理されているか、利用者として注意してほしいことはどのようなことかについてまとめ、利用者を対象としたセミナーの開催や利用企業への冊子提供などの支援を実施することが有効と考えられる。

3.3 会員企業

最後になるが、情報を収集しサービスで価値を生み出すビジネスを既に行っている、またはこれから始める会員企業（以下企業）に向け取り組むべき課題やチャンスを示す。クラウドやモバイルを活用したビジネスや、グローバルな環境におけるサービス提供時には、プライバシー保護の課題に取り組むことが必要になってきた。この課題に対して、企業は前節まで述べた国や業界団体の動きを待つだけではなく、企業としてできることから取り組みを行うべきである。これまで多くの企業において個人情報保護法対応としての顧客情報管理は実施されてきたが、米国や EU で見直しが行われているプライバシー保護の動きは日本の参画が遅れており、こうしたプライバシー保護の観点でデータ保護に取り組む企業は非常に少数である。欧米でどのようなデータ保護が求められており、そのためにどのような企業活動が必要であるかを理解している企業も少数である。プライバシーに関わるデータを扱う企業は早急な対応を行うことが必要である。

インターネットやクラウド上に膨大な利用可能な情報があふれビジネスのチャンスが開けている一方で、多くの情報は有効に利用しようと思えば個人情報につながり管理コストの増大やコンプライアンス上のリスクへの懸念から活用することが難しい。サービスの提供者である企業は、サービスの利用者に対する直接的な責任を負う当事者として、プライバシーやデータ保護に関してどのような状況にあるか把握し安全な運用に努めなければならない。セキュリティ状態の把握にあたり、提供サービスにおいて、何の目的で、どんな個人情報を収集し、その情報をどう扱っているか、といった見える化が必要となる。サービスを提供する国毎に関連する制度が異なるため各国制度についても把握に努め、制度とシステム仕様が合っているかを把握すべきである。また、スマートフォンやクラウドコンピューティングの普及により意図しない情報漏えいの予防のためにも、利用方法のガイドラインの策定を進め、自主規制に努めることも大切である。サイバー攻撃からシステムを保護しなければならないし、そのための技術開発を進めることも必要である。

クラウドやモバイルを活用したビジネスを、スピード感を持ち進めるためにもセキュリティと同様に経営上のポリシーとしてプライバシー保護に取り組むことを提案する。総務

省が公表した「スマートフォン　プライバシーイニシアティブ」[40]が参考になる。

3.3.1 プライバシー情報活用の遅れを挽回するための施策

企業が、プライバシー情報を効率的に管理するには、企業全体として統合された規範が必要となる。しかしながら、日本では、プライバシー保護の課題への反応は鈍く、国際的展開のキャッチアップも不十分であった。キャッチアップの重要性は高く、その一環として注目されているのがプライバシー・バイ・デザイン（Privacy by Design: PbD）である。

PbD とは、カナダのオンタリオ州情報・プライバシー・コミッショナーのアン・カブキアン博士が提唱した概念であり、「技術」「ビジネスプラクティス」「物理設計」のデザイン（設計）仕様段階から予めプライバシー保護の取り組みを検討し、実践することである。PbD は、システムでの情報利用のみならず、それにとどまらないビジネス慣行（事業活動）、ネットワークインフラなどの情報システムが前提とする環境についても、同様に意識しなければならないことを明確にしている。

PbD が目指していることを序文から引用すると下記である。[41]

> 従来は、プライバシーを守ろうとすると認証情報を収集できなかったり、あるいはそれまでのビジネス慣行と対立してしまうなど、プライバシーとビジネスのどちらか一方を諦めなければならないゼロサムモデルに基づいていた。しかしゼロサムモデルでは、結果的に IT そのものが利用者に受け入れられず、プライバシーも実現されなかった。このパラダイムをポジティブサムに変えることで、プライバシーの未来はより確かなものになる。

企業が PbD を導入すると、企業活動にどのような効果が期待できるか。PbD では、7 つの基本原則を実践することで「プライバシーの確保」「個人の自己情報に対するコントロール」「組織の持続可能な競争的利点の獲得」を達成できるとしている。

【7 つの基本原則】

① 事後的ではなく、事前的；救済的でなく予防的
② 初期設定としてのプライバシー
③ デザインに組み込まれるプライバシー
④ 全機能的－ゼロサムではなくポジティブサム
⑤ 最初から最後までのセキュリティーすべてのライフサイクルを保護
⑥ 可視性/透明性－公開の維持
⑦ 利用者のプライバシーの尊重

---

[40]「スマートフォン　プライバシー　イニシアティブ　－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－」
http://www.soumu.go.jp/main_content/000171225.pdf

[41] プライバシー・バイ・デザイン（堀部政夫／一般財団日本情報経済社会推進協会（JIPDEC）編）p.94

企業は、PbD を今後のデファクト的な標準として受け入れ、社内で実践するためのアプローチとして、プライバシー強化技術（Privacy Enhancing Technologies: PETs）の採用、プライバシー影響評価（Privacy Impact Assessment: PIA）の実践が挙げられる。

PETs とは、情報システムにおける個人のプライバシー保護を強化する技術の総称である。企業も「設計当初からの配慮」「利用者からのフィードバックを受けた技術の高度化」を重要視し、能動的にプライバシー保護に対応できるツールやシステム環境を求めるべきだ。PETs は、元々、個人データの不要または不法な収集、利用、提供を防ぎ、個人が自己の個人データのコントロールを強化するためのものである。具体的には、Cookie やスパイウェアの削除技術、迷惑メール対策のフィルターなどが挙げられる。

PIA とは、システムにおけるプライバシー保護策についての評価手法である。PIA を適切に実行・導入することで、システムの稼動における個人のプライバシーへの影響を明確化できる。評価には、予め定められたフレームワークに適合しているかをアセスメントする手法が用いられる。PIA を実施する意義は、個人のプライバシーへの影響を最低限にするために取りえる制度面での対応だけでなく、プライバシー保護のために実施可能な技術的な対応までを検討することにある。制度面では、不適合な原因を明らかにして体制を整備することが可能となる。技術面では、前述した PETs を利用した情報セキュリティ対策の必要性の有無の検討の基礎になる。

3.3.2 利用者の理解不足を解消する施策

安全な運用にあたり、企業はサービスの提供者として、サービスの利用者と「同意取得」を通じて信頼関係を構築しなければならない。信頼関係構築のためには、企業は現行の同意取得における問題意識を持ち、改善して行く検討が必要だと考える。

現行の同意取得における問題意識として、プライバシー情報の利用をめぐるトラブルが、利用者が想定していない方法で自らの情報が活用されることに起因している場合が多いことが挙げられる。提供者が利用者に対して、プライバシー情報の活用などについて知らせるために存在する利用規約やプライバシーポリシーは、利用者に十分読まれているとは言えず、利用者の理解を得ているとは言い難い状況にある。また、利用規約やプライバシーポリシーについては、制度遵守やリスク回避の観点を重視し、利用者の理解を得る観点から活用するという認識が薄い傾向にある。そのため、現行のプラクティスでは、プライバシー情報の収集時に利用者が誤解なく、正確に理解することは困難である。

企業は、守るべきところを利用者に明確に示すことが大切であるが、魅力的なサービスを創出する機会を失うほどの過剰反応は不要である。企業は、まずこうした問題意識を持ち、利用者が提供した情報をどのように処理して活用しているかを、どのように明確に利用者に示すか、真剣に検討し改善を継続しなければならない。

利用者が提供した情報をどのように処理して活用しているかを明確に利用者に示すには、

企業はオプトインとオプトアウトをもっと活用するとよい。活用する上での留意点として、オプトインでは、利用規約やプライバシーポリシーの記載方法を改善し、利用者の分かり易さに貢献するアプローチがある。分厚いプライバシーポリシーは誰も読まない。同意の取り方は、可能な限り短く、簡潔に、重要事項だけを明示すべきである。消費者の信頼を得る分かりやすい表示[42]として

(1) 平易でシンプルな表示
(2) ラベルによる一覧表示
(3) アイコンによる表示

が提案されている。また、オプトアウトでは、サービス提供者が利用する情報の目的を変更する場合があるが、利用者が問題と判断した時にスムーズに契約解除ができるようにしなければならない。明示的に同意を取る必要があるのは、利用者が期待・想定していたコンテキストから外れる時である。

3.3.3 魅力的なサービス提供に向けて

プライバシー情報を含むビックデータの活用は今までできなかった魅力あるサービス提供の可能性を示している。最後に、IT 環境の変化を最大限に活用し魅力的なサービス提供を会員企業が創出するために、いくつかの注目する点を挙げる。

ビックデータ分析などで顧客情報などプライバシー情報や様々な情報を活用するといっても、情報の鮮度に対する理解は大事である。鮮度を失ってまでも情報を保持するのではなく、プライバシー情報の利活用は積極的に行うべきだが、一方で不要な保有を最小限にとどめ、利用に必要な期間を過ぎた情報を保持しないといった割り切った運用を取り入れることが運用面では重要である。

前節までで述べたプライバシー情報の取扱いの元、国内向けのサービス提供においては、利用者のプライバシー情報のリスク意識が低いこと、プライバシー情報を自らコントロールするという考えが定着していないことを意識し、サービスで活用するプライバシー情報について分かりやすく説明し同意の上で活用することと（オプトイン）、何らかの理由で利用者があるプライバシー情報の活用を停止したいと望んだ場合、速やかに停止する手段（オプトアウト）をサービスの利用停止も含め、分かりやすく提供することが重要である。このことが、利用者の安心感に繋がるし、万が一問題が発生する可能性があっても回避に繋がるからである。

グローバルなサービス提供においては、プライバシー情報を管理する上でコストを押させるために重要なポイントとなる、プライバシー情報の利用者によるコントロール要求への対応力を挙げておく。

---

[42] 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（第 4 回） - 配付資料
http://www.meti.go.jp/committee/kenkyukai/shoujo/it_yugo_forum_data_wg2/pdf/004_03_00.pdf

日本は、携帯電話での各種サービスやSNS利用、携帯電話内蔵ICカードによる決済など他国に先駆けて非常に高度な利用が進んでいる分野がある。プライバシーに対する独特な考え方や法制度をベースに欧米諸国では発想できない新たなサービスを立ち上げる道もあるのではないだろうか。企業としては、顧客のプライバシー権に十分配慮した上で、本当に魅力のあるサービスを国内のみならずグローバルに提供して、多くの顧客が利用するようになることで、各国の法制度や運用にインパクトを与えることもできるであろう。

おわりに

本報告書では、情報セキュリティ調査専門委員会が、近年の国内外のプライバシーを取り巻く法制度やITを活用した社会経済活動の変化を調査・分析し、日本国及び業界団体、JEITA会員企業が何をすべきかを提言した。

海外のプライバシー保護法制と比肩しうる日本国の法制度の整備や、グローバルなビジネスを展開する上での制度の確立が重要となるのではないか。これに向けて、日本国政府内での委員会等での検討が進められているようであり、その進展に期待したい。また、業界団体等による検討も併せて実施することにより、それぞれの業態に応じた自主的なガイドライン等を早期に整備することが求められる。その一方で我が国企業は、その国際競争力強化のための技術開発の強化や、損失防止のための各国の法制度の調査が求められる。また、各国の法制度やその運用にインパクトを与えるような商品開発を行うことが、日本国全体の利益となるだろう。これらを実現しつつ、その成果に基づく日本発の国際標準化や他国との連携を行うことにより、さらなる我が国の国益の増進が可能となるだろう。

今後の我が国における、ITを活用した安心・安全な社会経済活動の進展とその国際競争力強化、そのために必要となる情報セキュリティ産業の発展のために、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25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