2016 年 8 月 4 日
みずほ銀行　産業調査部

Mizuho Industry Focus　Vol. 184

我が国のデータ利活用の促進に向けて
～サイバーセキュリティと個人情報保護に関する「不安」解消の観点から～

澤田　洋一
youichi.sawada@mizuho-bk.co.jp

〈要　旨〉

○ 近年、データ利活用の重要性は世界中で広く認知されており、産業界で注目を集めている IoT においても「データ」をいかに活用するかに本質がある。データ利活用にはエコシステムが存在し、このエコシステムを形成できるか否かが企業の競争力を左右すると言っても過言ではない。

○ 一方、我が国のデータ利活用の状況を見てみると、米国と比べて取り組みが遅れていることが分かる。その要因としては事業者側でも主なデータの提供者である個人の側でも様々な要因が考えられるが、「データセキュリティ上の不安」と「プライバシーの侵害（＝個人情報保護）に関する不安」は両者に共通すると言える。

○ 我が国において、サイバーセキュリティや個人情報保護に関する取り組みは進捗しつつある。サイバーセキュリティに関しては、サイバーセキュリティ基本法や経営者向けのガイドラインが制定され、個人情報保護に関しては、個人情報保護法が 10 年振りに改正され、「個人情報」の定義の明確化や、「匿名加工情報」が新設される等、パーソナルデータ利活用を後押しすることが期待されている。

○ ただし、米国や EU 等の動向を見てみると、我が国の取り組みはまだ十分とは言えない。サイバーセキュリティに関しては、情報共有体制等の制度面の整備や、中小企業対策、産業としての強化等が課題として挙げられ、対応策としては業界単位の情報共有体制（ISAC）の拡充や、サプライチェーン単位での中小企業セキュリティの強化、官民ファンドを活用した民間企業の海外投資支援等が考えられる。

○ また、個人情報保護に関しては、匿名加工に関するルールの整備やデータ利活用の仕組みの整備が課題として挙げられ、個人情報保護委員会のサポート体制強化や、削除項目を明示する等の匿名加工ルールの制定、公的認定制度を活用したデータ利活用の仕組みの整備等が具体的な対策として考えられよう。

○ データ利活用を進めていくには、制度や仕組みの整備に加え、個人や企業の利活用に対する意識を変えていく必要がある。我が国におけるデータ利活用拡大が実現するその意義も踏まえ、利活用拡大に向けた国としての力強い後押しを期待したい。

目 次

我が国のデータ利活用の促進に向けて
～サイバーセキュリティと個人情報保護に関する「不安」解消の観点から～

Ⅰ．はじめに

米国のプラットフォーマーがデータ利活用により圧倒的な存在感を示す

近年、Google や Amazon、Facebook といった米国のインターネットサービス事業者が「ネットの検索履歴」や「商品の購入履歴」から「友人関係」に至るまで、各社の提供するサービスを通じてユーザーから得られた様々なデータを活用し、ユーザー毎のニーズに合わせたサービスを提供するプラットフォーム[1]を形成している。代表的なプラットフォーマーである上記 3 社は、独自のビジネスモデルを確立して成功を収め、今や時価総額で世界のトップ 10 に入り（2016 年 3 月末時点）、圧倒的な存在感を示している。このようなプラットフォーマーの台頭により、既にデータ利活用の重要性は世界中で広く認知されている。

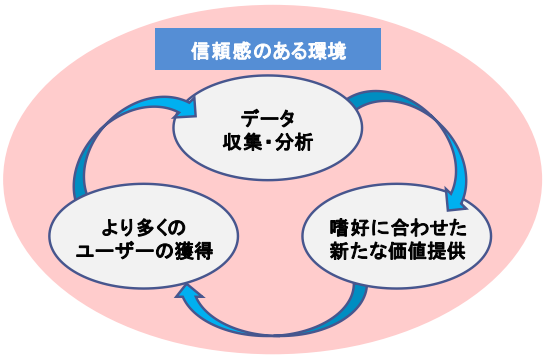
IoT においてもデータの利活用が重要なポイントになっている

また、産業界で注目を集めている IoT（Internet of Things）においても、その本質はあらゆるモノがインターネットに繋がることによって収集した「データ」をいかに活用するかである。例えば、製造機器の稼働状況に係るデータをリアルタイムで取得できるようになり、それを分析することで生産の効率性を高め、コスト削減やアウトプットの極大化に繋げることが可能となる。その他にも、農業分野の例で言えば、農園に設置したセンサから温度、湿度、降水量、日射量などのデータを収集・分析することで、農作物の品質の安定化や改善、生産の効率化に繋げることも可能となる。

データ利活用のエコシステムにはセキュリティ面に不安のない環境が不可欠

データ利活用にはエコシステムが存在する。企業がデータを収集し、そのデータを分析してユーザーの嗜好に合わせた新たな価値やサービスを提供し、その新たな価値やサービスでより多くのユーザーを獲得することで、さらに多くのデータが集まるようになる。このエコシステムを形成できるか否かが、今や企業の競争力を左右すると言っても過言ではない。それに加えて、このエコシステムを形成するには、サービス利用者（データ提供者）に「データが安全に守られる」「プライバシーが侵害されない」といった、信頼感を与えることも不可欠である（【図表 1】）。

【図表 1】データ利活用のエコシステム



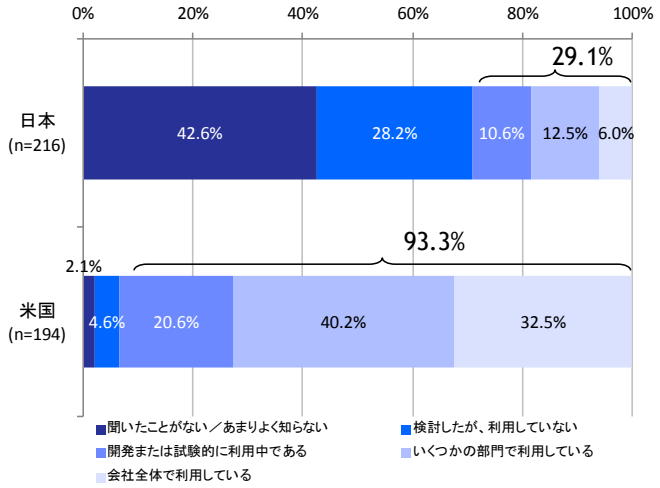
（出所）みずほ銀行産業調査部作成

[1] ユーザーが目的を果たすために使用する「場」

我が国はデータ利活用に遅れを取り、その差はさらに広がる可能性

こうした中、実際に日米のデータ利活用の状況を見てみると、我が国の取り組みは米国と比べて大きく遅れていることが分かる(【図表 2】)。データ利活用のエコシステムを考えると、取り組みが遅れれば遅れるほど、米国のプラットフォーマー等の先行企業にデータが集中する一方、我が国企業にはデータが十分に集まらず、その結果、企業の競争力においても追いつけない程にまでその差が広がる可能性がある。

【図表 2】ビッグデータの活用状況の違い(日米)



(出所)「IT を活用した経営に対する日米企業の相違分析(JEITA & IDC Japan)」よりみずほ銀行産業調査部作成

国や経済界でもデータ利活用の取り組みの遅れが懸念されている

我が国のデータ利活用の状況については、国や経済界でもその取り組みの遅れを懸念する声があがっている。2014 年に立ち上げられた経済産業省の「日本の稼ぐ力創出研究会」では「ビッグデータの活用について、一部の先進的な事例を除き日本は遅れているという危機感を持っている」[2]という意見が出ており、経団連から 2015 年 2 月に出された「個人情報保護法等の制度改正に向けた意見」でも、パーソナルデータに関して「事業者の躊躇と消費者の不安が生じており、利活用に向けた取り組みが遅れている」とのコメントが記載されている。

データ利活用が進まない要因には、データ提供者側の不安もある

なぜ我が国のデータ利活用は、なかなか進まないのだろうか。その要因にはデータを利活用する側(主に事業者)でもデータを提供する側(主に個人)でも様々な要因が考えられる。事業者側の要因としては、「データを分析できる人材不足」や「データ利活用のメリットが見出せない(データの価値が分からない)」等が挙げられる。

他方、サービスの利用を通じてデータを提供することにもなる個人の目線で見ると、データの利活用を前提としたデータ提供には、「データセキュリティ上の不安(漏えいリスク)」や「プライバシーの侵害に関する不安」等を感じれば、躊躇せざるを得ない面があると考えられる。

[2] 日本の「稼ぐ力」創出研究会(第 8 回)議事要旨より

また、こうした個人側の「不安」の存在は、事業者にとっても、データの取り扱いを誤ると、補償金やレピュテーション毀損など大きな問題に繋がる「リスク」として認識される。上述のように、事業者が、データ利活用のメリットを十分に理解していない状況であれば、こうしたリスクテイクそのものを躊躇している可能性がある。

とはいえ、我が国でも2015年9月に個人情報保護法が改正される等、データ利活用拡大に向けた取り組みは着実に進んでいる。そこで本稿では、上記に挙げた「セキュリティ」と「個人情報保護」に焦点を当て、特にセキュリティについては近年注目されているサイバーセキュリティ[3]に着目し、データ利活用の拡大に向け、さらなる改善策などについて考察していきたい。

Ⅱ. 我が国のデータ利活用の状況

(1)データの定義の整理

まず、本論に入るにあたり「データ」の定義を整理しておきたい。

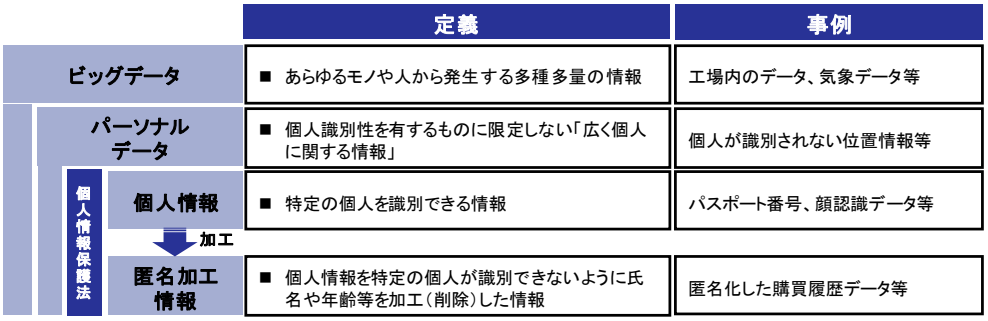
パーソナルデータとは個人識別性を有するものに限定しない「広く個人に関する情報」を表す

本稿では、データを広範なものから順に、ビッグデータ、パーソナルデータ、個人情報、匿名加工情報の4つに分類し使い分ける。但し、特定する必要がない場合には単純に「データ」と呼ぶこととする。「パーソナルデータ」とは、「パーソナルデータの利用・流通に関する研究会」(総務省)の報告書において、個人識別性を有するものに限定しない「広く個人に関する情報」と整理されている。あらゆるモノや人から発生する多種多量なデータをビッグデータとするならば、パーソナルデータは、個人に関連する情報全般と言える。

個人情報と匿名加工情報は、パーソナルデータに包含される

一方、「個人情報」とは、個人情報保護法で定義されている「特定の個人を識別できる情報」を指す。2015年9月の個人情報保護法改正において新たに導入・定義された「匿名加工情報」は、「個人情報」を個人が特定・識別できないように氏名や年齢等を加工(削除)した情報とされている。したがって、上述の「パーソナルデータ」との関係においては、「個人情報」と「匿名加工情報」は「パーソナルデータ」に包含される概念ということになる(【図表3】)。

【図表3】データ毎の定義



(出所)各種資料よりみずほ銀行産業調査部作成

[3] コンピューターへの不正侵入、データ改ざんや破壊、情報漏洩、ウイルス感染等がなされないように、コンピューターやコンピューターネットワークを守るためのセキュリティ

個人情報とされるデータを具体的に示す

具体例を示すと、氏名や住所、顔写真が載った運転免許証などは、個人情報である。また、先般の法改正では、指紋データや顔認識データ等の「特定の個人の体の一部の特徴を電子化した符号」も個人情報の対象になるとされた。一方、匿名加工情報の例としては、各種ポイントカード等の氏名や生年月日・住所・購買履歴等が含まれる原データ元の情報から、個人が特定できないように氏名・住所・生年月日の一部を加工(削除)した情報等が挙げられる。

こういったデータに関する言葉の定義の認知が世間一般に広まっておらず、「パーソナルデータ」や「個人情報」といった言葉が感覚的に、時には解釈を間違って使われることが、「個人情報保護」を過剰に意識し、不安を増幅する一つの要因になっていると考えられる。

データ利活用の主体は「自身(自社)」と「第三者」の2つ

上記に加え、「データ利活用」の主体についても整理しておきたい。「データを利活用する」と言った場合、その主体は大きく分けて「自身(自社)」と「第三者」の2つある。ポイントカードを例に挙げると、消費者が商品の購入時にポイントカードを提示し、自身の属性や購買情報を事業者に提供する代わりに、ポイントをもらうことは「自身での利活用」であり、当該事業者がポイントカードの情報を自社の販売促進に活用するのも「自身(自社)での活用」である。一方、第三者が当該事業者から匿名加工したポイントカードの情報を購入し、自社のマーケティングに活用することは「第三者の利活用」と言える。データ利活用を考察する上では、このような「主体の違い」も認識しておく必要がある。

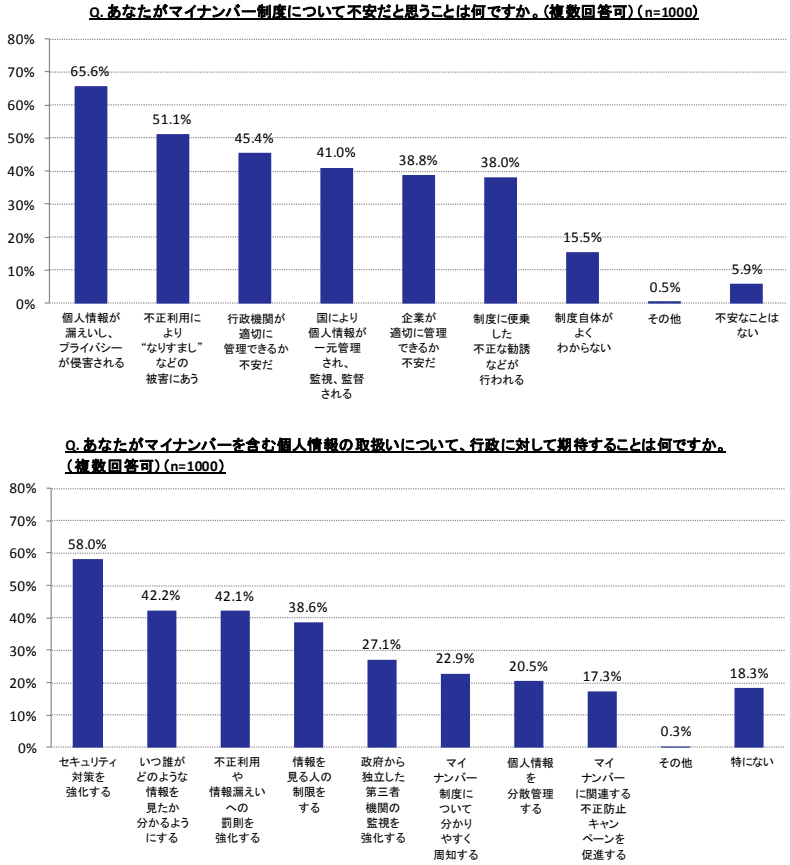
(2)データ利活用の状況と課題

マイナンバーに関するアンケートでも、セキュリティとプライバシーの不安が課題に挙げられている

ここで、2016年3月にJIPDEC[4]が実施した「マイナンバーに関する意識調査」を見てみたい(【図表 4】)。「マイナンバー制度に対する不安(Q3)」への回答では、トップに「プライバシーの侵害」(=個人情報保護)が、次に「不正な利用による被害」が挙げられている。また、「行政に対して期待すること(Q4)」への回答では、トップに「セキュリティ対策強化」が挙げられ、その他にも「誰に情報を見られたか分かるようにする」「情報を見る人を制限する」等が回答の上位を占めている。このことからも、少なくともマイナンバーに代表されるパーソナルデータの利活用拡大のためには、「セキュリティ」と「個人情報保護」に関する不安を如何に軽減するかがポイントと言えるだろう。

[4] 日本情報経済社会推進協会

【図表 4】マイナンバー制度に関するアンケート結果

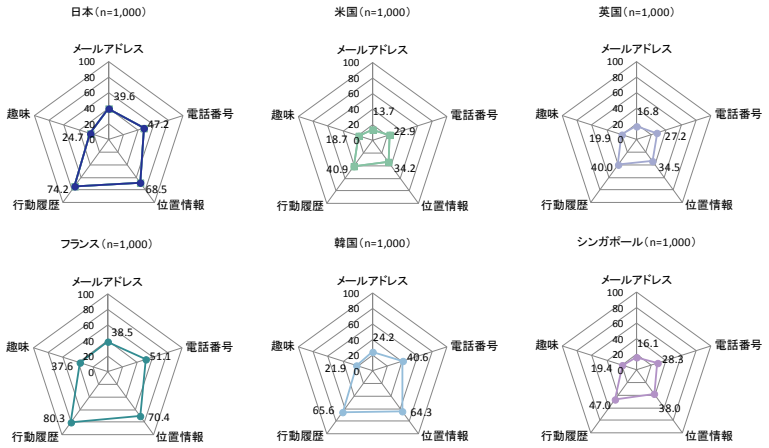


（出所）日本情報経済社会推進協会（JIPDEC）資料よりみずほ銀行産業調査部作成

日本人は相対的にプライバシーに関する意識が高い

また、個人情報保護の問題を考えるに際しては、「プライバシーに関する意識の高さ」についても考慮する必要があり、国毎に違いがある。一例として、【図表 5】の「どのような場合でも提供・公開したくないデータ」の国際比較を見てみると、日本はフランスと並んで、どの項目でも他国比高い割合となっている（＝提供、公開に抵抗があるデータが多い）。パーソナルデータの利活用が進む米国・英国と我が国では回答状況に大きな違いがあり、日本人はプライバシーに関する意識が高いことが分かる。パーソナルデータ利活用を進める上ではこういった我が国の特徴も認識しておく必要があるだろう。

【図表 5】「どのような場合でも提供・公開したくないデータ」の国際比較



（出所）総務省「H25 年度情報通信白書」よりみずほ銀行産業調査部作成

(3) 具体的な事象からみる不安の原因

データ利活用に際して、「サイバーセキュリティ」や「個人情報保護」に不安を抱くようになった要因としては、上述したような日本人の高いプライバシーへの意識だけではないと見られる。近年、我が国において発生し、報道されたいくつかの事案も、データ利活用に係わる個人の不安あるいは企業側のリスク回避意識を増幅させている要因と思われる。

政府機関でも被害にあい、サイバーセキュリティの難しさが再認識された

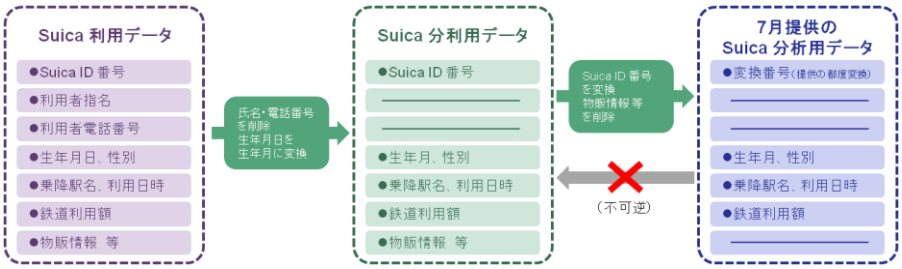
まず、政府機関が狙われた有名な事件として、2015 年 5 月に起きた日本年金機構のサイバー攻撃による個人情報漏えい事件が挙げられる。日本年金機構の報告によれば、これは「標的型サイバー攻撃」による被害であり、職員がウイルス付きメールを開いたことで職員のパソコンがウイルス感染し、結果的に 125 万件もの個人の年金情報が流出して大きな問題となった。この事件では、高いセキュリティ体制が求められる政府機関でも攻撃が防げないという、「サイバーセキュリティ対策の難しさ」や「対策にゴールのない不安」が想起された。

JR スイカ事件は、我が国の個人情報を取り巻く問題が集約された事件だった

次に個人情報の取り扱いが問題になった JR 東日本の乗車履歴データに関する事案（以降、JR スイカ事案）が挙げられる。本件は JR 東日本がスイカの乗降履歴データを日立製作所に「利用者への事前の説明なく」販売したことがマスコミ等に取り上げられ、利用者の大きな反発に繋がった。パーソナルデータの利活用とプライバシー保護の問題を世間に広く知らしめた事案である。

実際には、JR 東日本はスイカの乗降履歴データを個人が特定できないように氏名・電話番号・生年月日（日にちのみ削除）、物販情報を削除して日立製作所に提供しており、当該取引自体は法令上問題無いという解釈が一般的である（【図表 6】）。加えて、日立製作所との間で、特定の個人を識別する行為を禁じる契約も締結するなどの措置も講じていた。それでも、利用者からは「個人の情報を勝手に使っていいのか」「本当に個人を特定されないのか」という不安・反発を招き、結果的に販売契約の打ち切りを余儀なくされた。個人のプライバシーに関する意識の高さや、個人情報の定義の不明確さ等が改めて問題視された事案と言える。

【図表 6】スイカ利用データの加工項目



(出所)JR 東日本 HP よりみずほ銀行産業調査部作成

ベネッセの事件でも大量の情報漏えいにより、不安を募らせ、また、企業のリスクの大きさも認識された

上記 2 つの事案に加え、サイバーセキュリティと個人情報保護の両方の問題が内在したものとして、ベネッセにおける情報漏えい事件(以降、ベネッセ事件)が挙げられる。これは同社の元社員がデータベースにあった個人情報(会員情報)を不正に入手し、名簿業者に販売し 2,000 万件超の大量の個人情報漏えいに繋がり大きな問題となった。事件の報告書によれば、本件は情報の重要性に応じたアクセス権限の設定や、異常なアクセスログや通信ログへのアラート設定等が適切になされなかったことが原因とされている。

内部不正を防ぐためにも、サイバーセキュリティは重要

本件では、200 億円を超える損害賠償が発生し、企業における個人情報の漏洩リスクの大きさが認識されたことに加え、外部からのサイバー攻撃だけでなく、内部不正を防ぐ上でもサイバーセキュリティの重要性が再認識された。さらには、犯罪を抑止するような法制度(罰則)が整備されていなかったことも問題となり、改めて法改正の必要性が認識された事件である。

このような事件もあり、個人も企業もデータ利活用を躊躇している

データ利活用によってもたらされる経済効果が「光」ならば、サイバーセキュリティや個人情報保護に関する不安は「影」と言えるだろう。今後、この「影」がさらに濃くなれば、利活用が進むどころか、利活用の足枷にもなりかねない。

以降では、サイバーセキュリティと個人情報保護の問題それぞれについて、日本と海外の取り組みを順々に確認していきたい。まずは第Ⅲ章でサイバーセキュリティに関する動向を見ていく。

Ⅲ. サイバーセキュリティの課題と対応策

1. 日本のサイバーセキュリティに関する取り組み

(1)制度面

サイバーセキュリティ基本法が施行され、NISC への権限一元化等が明確化された

我が国ではサイバーセキュリティに関する施策を総合的且つ効果的に推進するため、2015 年 1 月にサイバーセキュリティ基本法が施行された。これに基づき、内閣官房にサイバーセキュリティ戦略本部及び内閣サイバーセキュリティセンター(NISC)が設置され、従来各府省等に分かれていた監査機能の NISC への一元化や、政府機関への第三者(サイバーセキュリティ戦略本部及び NISC)による監査権限が法的根拠を持つ形で明確化された。

加えて、同法に基づいて我が国の「サイバーセキュリティ戦略」についても見直しが行われた。2020 年のオリンピック・パラリンピック東京大会の開催や IoT

サイバーセキュリティ戦略も見直され、国としてのサイバーセキュリティ強化が明示された

時代の到来といった環境変化を踏まえつつ、官民間や民民間でのインシデント情報[5]の共有などの連携体制強化や、サイバーセキュリティの「産業化」の推進など、国としてサイバーセキュリティを強化・推進していく方針が明示されたことは大きな一歩と言える。

また、2015 年 12 月に経済産業省から「サイバーセキュリティ経営ガイドライン Ver1.0」が公表された。当該ガイドラインでは経営者のリーダーシップにより情報セキュリティ責任者に指示すべき重要な 10 項目が示され、各項目の対応例や対策を行わなかった場合のリスクシナリオ等も記載されている(【図表 7】)。

サイバーセキュリティ経営ガイドラインにより、経営者の意識を高めることを目指す

企業におけるサイバーセキュリティの導入・拡大にあたっては、経営者がその重要性を認識し、自社にとって、どの情報がコストをかけて堅固に守るべき情報なのかといった「経営判断」を行うことが不可欠であり、当該ガイドラインは経営者のサイバーセキュリティに対する意識を高める施策として的を射たものであると言える。

【図表 7】サイバーセキュリティ経営ガイドライン Ver1.0 概要

サイバーセキュリティ経営の重要10項目	
リーダーシップの表明と体制の構築	①サイバーセキュリティリスクの認識、組織全体での対応の策定
	②サイバーセキュリティリスク管理体制の構築
サイバーセキュリティリスク管理の枠組み決定	③サイバーセキュリティリスク把握と実現するセキュリティレベルを踏まえた目標と計画の策定
	④サイバーセキュリティ対策フレームワーク構築(PDCA)と対策の開示
	⑤系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
リスクを踏まえた攻撃を防ぐための事前対策	⑥サイバーセキュリティ対策のための資源(予算、人材)確保
	⑦ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
	⑧情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
サイバー攻撃を受けた場合に備えた準備	⑨緊急時の対応体制の整備、定期的且つ実践的な演習の実施
	⑩被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

(出所)経済産業省資料よりみずほ銀行産業調査部作成

政府が主導する情報共有の取り組みとして、CEPTOAR 制度がある

サイバーセキュリティの対策としては、インシデント情報共有制度の拡充も重要である。政府が主導する情報共有に関する代表的な取り組みとしては、重要インフラに指定される通信や鉄道等 13 業種[6]を中心とした CEPTOAR[7]制度がある。CEPTOAR では業界内外で発生したインシデント情報を、政府機関から各構成員へ提供・共有し、注意喚起する取り組みや、分野横断のサイバーセキュリティ共同演習等が進められている。

ISAC は民間主導による業界単位の実務的な情報共有制度

更に、参加企業相互間でのより実務的な情報共有を目指す民間主導の取り組みとして、金融業界と通信業界では業界単位の情報共有制度である ISAC[8]を立ち上げ、情報共有を積極的に進めている(【図表 8】)。通常、自社のサイバー攻撃被害に関する情報を広く世間に公表することは、風評面におけるマ

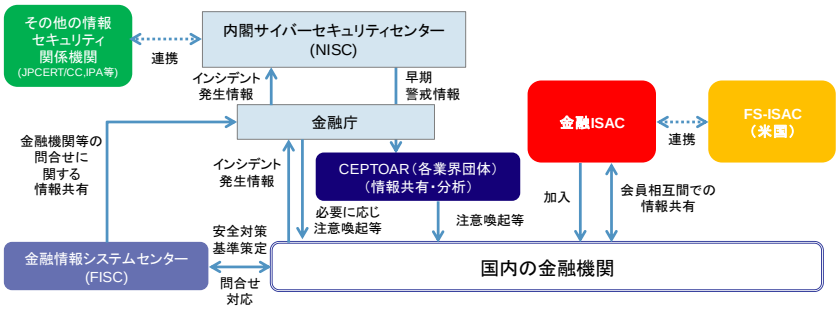
[5] コンピューターやネットワークのセキュリティを脅かす事象
[6] 情報通信、金融、航空、鉄道、電力、ガス、行政サービス、医療、水道、物流、クレジット、石油、化学
[7] Capability for Engineering of Protection,Technical Operation, Analysis and Response の略称。国が指定する重要インフラの分野ごとに整備された情報共有制度
[8] Information Sharing and Analysis Center の略称

イナス効果以外にも更なるサイバー攻撃を誘引する可能性もあることから忌避される。ISAC においては、業界単位で「クローズかつ信頼できるネットワーク」を構築し且つ、企業のサイバーセキュリティの実務者が参加することで、より実効性のあるインシデント情報の共有を可能にしている。

ISAC はその有用性が評価されており、更なる拡大が期待されている

ISAC では、「この IP アドレスからサイバー攻撃を受けた」という情報や「こういうウイルスメールが送られた」といった「今」起きたインシデント情報を、会員相互間でリアルタイムに共有することで、業界内での更なる被害拡大を防ぐことができ、その有用性が評価されている。このような ISAC の仕組みは情報共有の一つのモデルケースと言え、他の業種にも広げていくことが期待される。

【図表 8】金融業界の情報共有体制



（出所）金融庁資料よりみずほ銀行産業調査部作成

中小企業は取り組みが遅れており、中小企業向けの対策も重要

中小企業にフォーカスを当てた対策も重要である。中小企業は大企業以上にサイバーセキュリティを強化するための人的・経済的余裕がないことから、対策が進みづらく、実際、大企業と中小企業の対策状況を見ても、その取り組みには大きな開きがあり、中小企業への対策の必要性が分かる（【図表 9】）。

実際に中小企業が狙われた事例もあり、踏み台にされる被害も増えている

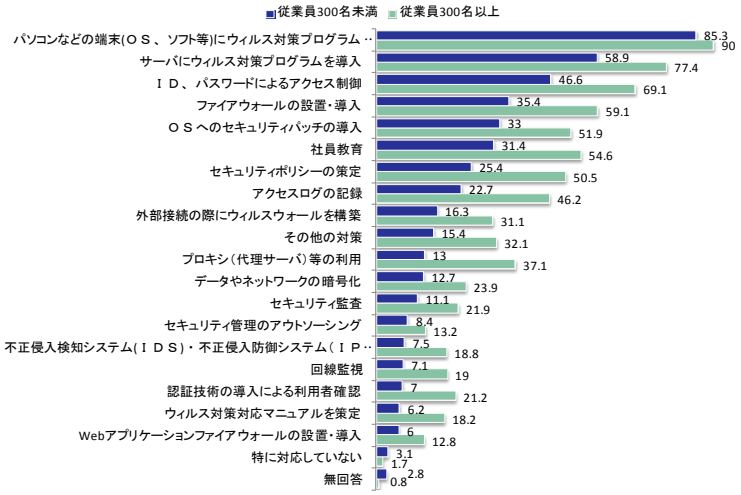
実際、最近でも従業員 10 人の中小企業の自社 EC サイトがサイバー攻撃を受け、顧客のクレジットカード情報が流出した事件も起きている。IPA[9]や JPCERT/CC[10]からも国内企業のサイトがサイバー攻撃の踏み台にされるリスクが高まっていると指摘され、注意喚起がなされている。具体的には、セキュリティの甘い PC やサーバーに不正にアクセスされ、そこを経由（踏み台に）してその企業の取引先や関連会社にサイバー攻撃が仕掛けられるケース等がある。しかしながら、最近の IPA のアンケート調査[11]では、セキュリティの強化を計画する中小企業は 9.5%に留まっており（大企業は 27%）、中小企業自身のセキュリティに対する意識は高まっているとは言えない。

東京都が警視庁等と連携して、都内の中小企業向けの取り組みを開始

そのような中、2016 年 1 月に東京都と警視庁が都内の中小企業におけるセキュリティ対策の強化を支援する取り組みを開始している。セキュリティ対策が十分に強化されていない都内の中小企業に対して啓蒙活動を行い、またインシデント情報共有や相談体制の構築などを行うことで、サイバー攻撃の脅威から中小企業を守ることを目指している。このような自治体単位での取り組みもさらに広げていくことが重要だろう。

[9] Information-technology Promotion agency（独立行政法人情報処理推進機構）
[10] Japan Computer Emergency Response Team Coordination Center の略称
[11] IPA「企業におけるサイバーリスク管理の実態調査 2015」

【図表 9】大企業と中小企業のセキュリティ対策の状況



（出所）総務省「平成 26 年通信利用動向調査」よりみずほ銀行産業調査部作成

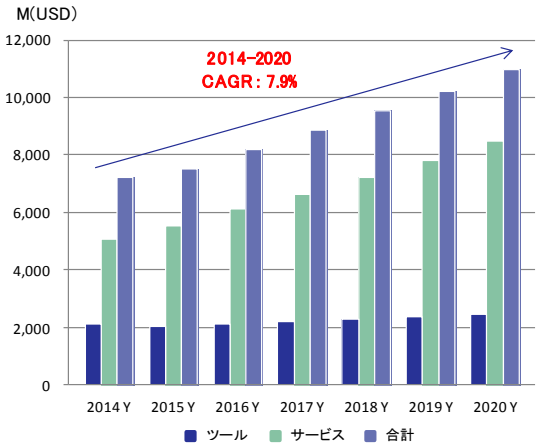
(2)産業面

続いてサイバーセキュリティの産業としての動向を見ていきたい。政府が 2015 年 9 月に公表した「新サイバーセキュリティ戦略」においては、「経済社会の活力の向上及び持続的発展」という観点からサイバーセキュリティ対策を「費用」ではなく「投資」と捉えるように促し、「産業化」を目指すことが謳われている。

サイバーセキュリティの国内市場規模は高い成長が見込まれる

直近のサイバーセキュリティの国内市場規模は IT サービス市場（約 10 兆円）の 1 割弱、概ね 8,000 億円程度とみられる（【図表 10】）。今後もサイバー攻撃の深刻化・高度化に伴って需要は堅調に推移することが見込まれ、2020 年までの CAGR は 7.9%[12]と IT サービス市場全体（1.5%）と比して高い成長率が予想される。

【図表 10】サイバーセキュリティ市場推移（国内）



（出所）Gartner, *Forecast: Information Security, Worldwide, 2014-2020,1Q16 Update*, 10 May 2016 よりみずほ銀行産業調査部作成

（注）ツール：Identity Access Management、Infrastructure Protection、Network Security Equipment、Consumer Security Software、サービス：Security Services、数字は Software spending ベース

[12] Source: Gartner"Forecast: Information Security, Worldwide, 2014-2020,1Q16 Update"10 May 2016

日本企業も積極的な取り組み方針を打ち出している

国内大手 IT ベンダーは、サイバーセキュリティを「重点分野」に掲げ、取り組み強化の方針を打ち出している。例えば、富士通は 2014 年 1 月にサイバーセキュリティに関連する製品・サービス群を体系化した「Fujitsu Security Initiative」を発表し、同部門で 2016 年度に約 1,300 億円の売り上げを目指すとしており、NEC も 2014 年 4 月に全社横断組織として「サイバーセキュリティ戦略本部」を立ち上げ、2017 年度の売上目標を 2,500 億円とするなど、ターゲット分野としての期待は高まっているように思われる。

サイバーセキュリティの各分野にはグローバルプレーヤーが存在

ただし、サイバーセキュリティの各分野においては既に有力なグローバルプレーヤーが存在しており、我が国においてもセキュリティツール（ソフト・ハード）分野では既に大きな存在感を示している（【図表 11】）。今後は、グローバルプレーヤーがコンサルティングや運用（マネージドサービス）といった分野を強化してくることも考えられ、日本企業もマーケットの伸び率以上のシェアを確保するには、一層の取り組み強化が求められるだろう。

【図表 11】サイバーセキュリティの主な分野毎の主要プレーヤー

コンサルティング		ツール（ソフト・ハード）		SI		運用（マネージドサービス）	
日系企業	グローバル企業	日系企業	グローバル企業	日系企業	グローバル企業	日系企業	グローバル企業
NTT Com Security Fujitsu Hitachi NEC Lac	Deloitte IBM PwC Ernst & Young	Trend Micro NEC Hitachi Digital Arts FFRI	Symantec Intel (McAfee) IBM EMC	Fujitsu Hitachi NEC NTT Data	IBM Accenture Deloitte HP	NTT Com Security Fujitsu Hitachi NEC Lac	IBM CSC Dell Secure Works Verizon Symantec

（出所）各種資料よりみずほ銀行産業調査部作成

2. 米国のサイバーセキュリティに関する取り組み

ここからは海外の動向を見ていきたい。まずはサイバーセキュリティ市場で高いプレゼンスを有する米国の取り組みを（1）制度面と（2）産業面に分けて見ていくこととする。

（1）制度面

NIST のフレームワークは日本も参考にすべき指針

米国のサイバーセキュリティのガイドラインとしては、NIST（アメリカ標準技術研究所）が 2014 年 2 月に公表した重要インフラ向けのフレームワークがある（【図表 12】）。このフレームワークでは産業界で効力を発揮している標準、ガイドライン、およびベストプラクティスを集約し、押さえるべき 5 つの大分類から、詳細な管理策を示すサブカテゴリー97 項目まで細分化して示している。重要インフラ以外の業種も含めて、規模を問わず幅広い企業で活用できるとして、近年グローバルベースで急速に利用が広まっている[13]。我が国も企業の対策を更に促すためには、参考にすべきガイドラインと言える。

[13] 公表から約 1 年半で海外企業（127 カ国）の 35%が採用（出所：PwC「グローバル情報セキュリティ調査 2016」）

【図表 12】NIST のサイバーセキュリティフレームワークの概要

機能	内容	カテゴリー	サブカテゴリー
特定	■どのようなリスクがあるかを「特定」	■資産管理等5項目	■「企業内の物理デバイス一覧を作成」等24項目
防御	■リスクの多寡に応じて適切な予防策を講じる「防御」	■アクセス制御等6項目	■「「資産に対する物理アクセスを管理し、保護している」等35項目
検知	■防御策を突破されたことをいち早く察知する「検知」	■異常とイベント等3項目	■「イベントがもたらす影響を特定している」等18項目
対応	■異常が検知され、必要な処置を講じる「対応」	■対応計画の作成等5項目	■「定められた基準に沿って、イベントを報告している」等15項目
復旧	■異常への恒久措置を施し、元通りの状態に回復させる「復旧」	■復旧計画の作成等3項目	■「イベントの発生中または発生後に復旧計画を実施している」等6項目

（出所）各種資料よりみずほ銀行産業調査部作成

米国では ISAC 等の情報共有体制も進む

また、情報共有体制についても米国では取り組みが進んでいる。業界単位毎の情報共有制度である ISAC は 2016 年 5 月時点で 18 団体にまで広がり、更なる拡大も期待されている。これに加えて、2015 年 2 月に大統領令で情報共有分析組織 ISAO[14]の創設が決定した。これは業界毎の ISAC に加えて、事業規模や地域単位等で ISAO を設立し、ISAC メンバー以外との情報共有も進め、より広範な情報共有ネットワークの構築を目指す取り組みである。

米国でも中小企業への対策はまだ十分とは言えない

他方、中小企業への対策としては、米国政府の独立機関である連邦通信委員会が「Ten cybersecurity tips for small business」において、注意すべき 10 カ条を示し、中小企業のセキュリティ対策に関する意識を高めている。ただし、内容は「ファイアーウォールを設定する」「重要データはバックアップを取る」等の基礎的な対策に留まっており、全体として先行する米国においても、中小企業に対する対策はまだ十分とは言えず、サイバーセキュリティの底上げの難しさが感じられる。

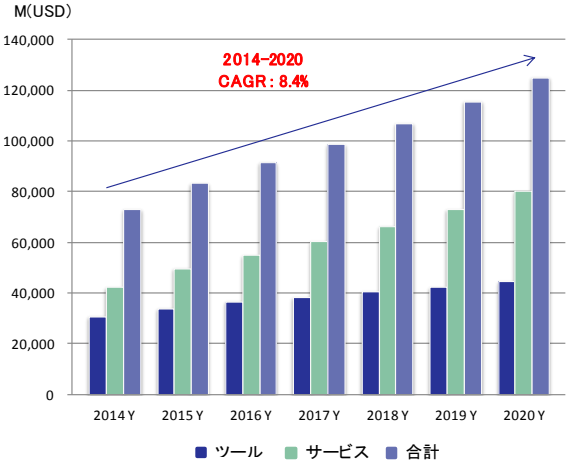
(2)産業面

世界のサイバーセキュリティ市場では米国企業が高い存在感を示す

ガートナーの調査によると、世界のサイバーセキュリティの市場規模は 2015 年時点で約 8.7 兆円[15]となっており、100 兆円規模の IT サービス市場との比較ではまだ小さいものの、2019 年までの CAGR は 8.4%[16]と日本のサイバーセキュリティ市場以上に高い成長率が期待されている（【図表 13】）。そして 2015 年時点でこの世界の市場規模の約 4 割を米国が占めている。さらに、【図表 14】のようにサイバーセキュリティツール市場のベンダー上位 10 社のうち 7 社が米国企業であり[17]、米国が市場の牽引役として高い存在感を発揮している。因みに、米国ではサイバーセキュリティ関連企業に投資するファンド（ファンド名：HACK）も NY 証券取引所に上場しており、このことから米国ではサイバーセキュリティが産業・業種として認知されていると言える。

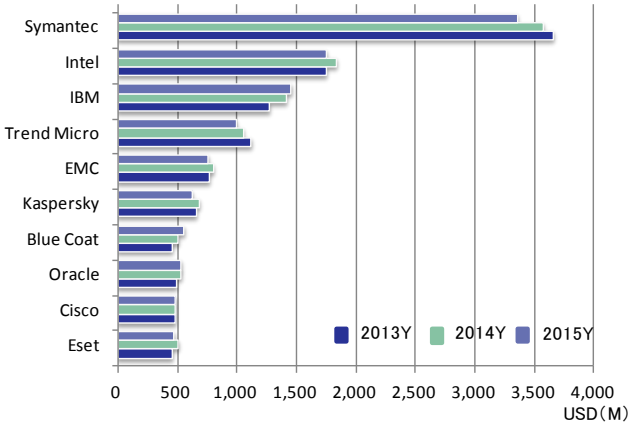
[14] Information Sharing and Analysis Organization の略称
[15] Source: Gartner“Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update”10 May 2016
[16] Source: Gartner“Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update”10 May 2016
[17] Source: Gartner“Market Share: Security Software, Worldwide, 2015”06 April 2016

【図表 13】サイバーセキュリティ市場推移（グローバル）



（出所）Gartner, *Forecast: Information Security, Worldwide, 2014-2020, 1Q16 Update*, 10 May 2016 よりみずほ銀行産業調査部作成
（注 1）セグメントの内訳は【図表 10】に同じ
（注 2）数字は Software spending ベース

【図表 14】セキュリティソフトウェア市場の上位企業（グローバル）



（出所）Gartner, *Market Share: Security Software, Worldwide, 2015*, 06 April 2016 よりみずほ銀行産業調査部作成
（注）数字は Software revenue ベース

米国のサイバーセキュリティ市場は軍需の大きな下支えがある

このようにサイバーセキュリティ市場における米国の存在感が大きいことの要因の一つに産業面・人材面での防衛予算を含めた国家予算による下支えが挙げられる。米国は国が主体となってサイバーセキュリティを国防として強化しており、日米の 2016 年のサイバーセキュリティに関する国家予算を比べてみても、米国は日本の 30 倍の予算を付与しており（国家予算自体は日本の約 4 倍）、サイバーセキュリティ産業に対する国の関与の違いが分かる（【図表 15】）。

【図表 15】日本と米国のサイバーセキュリティ関連予算の比較

	日本	米国	米国／日本
国家予算に占めるサイバーセキュリティ関連費用	約700億円	約2.1兆円	30倍
上記のうち軍のサイバー防衛関連予算	約100億円	約0.6兆円	60倍
（参考）軍のサイバー防衛部隊人数	約100人	約6,000人	60倍

（出所）各種資料よりみずほ銀行産業調査部作成

米国企業はイスラエル等のサイバーセキュリティ先進国企業を積極的に買収

また、大きな官による需要を受け皿にして、米国企業はイスラエル等のサイバーセキュリティ先進国の企業を積極的に買収し、自社の技術・サービスの更なる強化を進めている（【図表 16】）。米国のようなトップレベルの国（企業）でも、新しく且つより高度なセキュリティ技術を獲得するためにグローバルベースで M&A を進めており、日本企業にとっても参考にすべき取り組みと言えるだろう。

【図表 16】米国企業のイスラエル企業買収事例

年月	被買収企業			買収企業
	企業名	設立年	買収金額(M$)	
2015年6月	IdMlogic	2004年	20	CA Technology
2014年11月	Aorato	2011年	200	Microsoft
2014年3月	Cyvera	2011年	200	Palo Alto Networks
2012年2月	Insightix	2004年	NA	Intel(McAfee)

(出所)各種公表資料よりみずほ銀行産業調査部作成

3. EU・英国のサイバーセキュリティに関する取り組み

次にEUと英国の取り組みを概観する。EUは政府主導によるデータ利活用の取り組みが進んでおり、それを支えるサイバーセキュリティの対策も進んでいると考えられる。また、2012 年のロンドン五輪では、英国のサイバーセキュリティの取り組みが注目された。2020 年に東京五輪が控えている我が国にとって、英国の取り組みは参考になろう。

EU ではサイバーセキュリティ戦略を定め、国家間の連携も強化している

2013年2月に欧州委員会は、サイバー空間の脅威やサイバー攻撃への対応に関する包括的なビジョンを記した「サイバーセキュリティ戦略」を公表している(【図表 17】)。この戦略では優先的に取り組むべき 5 分野を示しており、例えばその一分野である「サイバー攻撃の耐性構築」の分野では、2014 年度の具体的な取り組みとして域内及び近隣の29カ国から200以上の組織が参加したサイバー演習「Cyber Europe2014」の開催が掲げられた。サイバー空間の脅威やサイバー攻撃への対応は各国間の連携が重要だという認識に基づいた取り組みであり、日本も国家間の連携方法として参考にするべきだろう。

【図表 17】EU サイバーセキュリティ戦略

優先取り組み分野	2014年度の主な活動内容	補足
サイバー耐性を構築する	Cyber Europe2014開催	ENISA(European Network and Information Security Agency)が開催するサイバー演習
サイバー犯罪を激減させる	Joint Cybercrime Action Taskforce(J-CAT)設立	各国の警察が連携してサイバー犯罪に対抗するために設立されたタスクフォース
共通安全保障・防衛政策に関するサイバー防衛政策・能力を確立する	EUサイバー防衛政策フレームワークを検討中	欧州理事会で新たな安全保障課題への対応として、同フレームワーク策定に合意
サイバーセキュリティに向けた産業・技術資源を確保する	Horizon2020開始	統一的な戦略のもとで研究・開発イノベーション分野の資金を配分する、多国間研究開発・イノベーション促進プログラム
首尾一貫したEUの国際サイバー空間政策を確立し、EUの核心にある価値を促進する	サイバー対話開催	2014年10月、日ーEUサイバー対話実施 2014年12月、米ーEUサイバー対話実施

(出所)(独)情報処理推進機構「情報セキュリティ白書 2015」を基にみずほ銀行産業調査部作成

ロンドン五輪ではサイバーセキュリティに通常の倍以上の予算がかけられた

英国は2012年のロンドン五輪の期間中(2週間)に2億回ものサイバー攻撃を受けたものの、大きな被害もなく無事に大会を終えたことでそのサイバーセキュリティ対策が注目された。同国のサイバーセキュリティの関連予算は五輪前の2011年からの4年間で約1,000億円と金額自体は日本と比べても大きくないものの、当時の同国の公共部門予算が大幅に削減されていた中でサイバーセキュリティに通常の 2 倍以上の予算が取られたことは、国としての重要度の表れと言える[18]。

[18] IPA サイバーセキュリティシンポジウム 2014「2012 年ロンドンオリンピックのセキュリティ～我々の経験をご紹介～(オリバー・ホーア氏講演録)」より

これに対し、日本の 2016 年度のサイバーセキュリティ関連予算は約 700 億円と 2012 年度予算（370 億円）に比べると 2 倍近く増加している。ただし、サイバー攻撃自体も 2012 年からさらに増加[19]していることを考えると、この予算が 2020 年に向けて十分な水準だと言い切ることはできないだろう。

英国では新たに中小企業向けにサイバーセキュリティ対策の手引きを定めている

また、英国ではロンドン五輪後の 2015 年 3 月に中小企業向けにサイバーセキュリティ対策の手引きを定め、中小企業を含めた国全体のセキュリティ強化に取り組んでいる。具体的には①基礎的対策、②リスク評価アプローチ、③サイバーエッセンシャルズ（セキュリティ認証）の取得、の 3 段階の対策が示された手引きとなっている。

ロンドン五輪（2012 年）でサイバーセキュリティを強化した英国でも中小企業への対策は道半ばである。このことからも、サイバーセキュリティの底上げを図ることの難しさと、対策に要する期間の長さが分かる。

4. 日本の課題と対応策

サイバーセキュリティに関しては、制度面、産業面ともに、まだ改善の余地あり

ここまで見てきたように、我が国ではサイバーセキュリティ強化に向けた取り組みが具体的に進められているものの、海外の状況と比較するとまだ制度面等を含め改善の余地があると言えるのではないだろうか。また、サイバーセキュリティを「産業」として見ても、まだ取り組みの余地があると言えるだろう。

人材不足も大きな問題であるが、セキュリティに限らず、IT 人材全般の問題として議論すべき

サイバー攻撃に対応できるようなセキュリティ人材の不足についても深刻な問題と言われている。直近の経済産業省の調べではセキュリティ人材が 2020 年に約 20 万人も不足すると試算されており、高度なサイバー攻撃対策が求められる 2020 年の東京オリンピックに向けて、この人材不足の問題も早急に取り組むべき課題であることは間違いない。ただし、この問題はセキュリティ人材に限らず IT 人材全般に共通する課題であり、サイバーセキュリティの枠を超えて議論すべきテーマである。

「見える化」、「中小企業のセキュリティ強化」、「セキュリティ産業の強化」が課題

このように課題はいくつも考えられるが、ここまでの内容を踏まえ、以下では取り組むべきサイバーセキュリティの課題として、「サイバーセキュリティの見える化」、「中小企業のサイバーセキュリティ強化」、「サイバーセキュリティ産業の強化」の 3 点を挙げ、その課題に対する対応策を示していく（【図表 18】）。

【図表 18】サイバーセキュリティに関する課題と対応策

	項目	実施主体	状況・課題	具体的な施策
（1）	サイバーセキュリティの見える化	国 民間	■ インシデント情報の共有体制が不十分 ■ どこまで対策をすべきかが分からない	① ISACの対象業界拡大 ② サイバーセキュリティ経営ガイドラインの更なるバージョンアップ ③ 情報セキュリティ格付の活用
（2）	中小企業のサイバーセキュリティ強化	中小企業 国・自治体	■ 中小企業はセキュリティ投資にコストが掛けられず、対策が進まない	① クラウドサービスを活用したセキュリティ強化とクラウドに切り替える際の費用補助 ② 大企業が自社のグループ内や、サプライチェーン内の中小企業向けにクラウドサービスの環境を提供
		大企業	■ 中小企業を経由して大企業も狙われるリスクあり	
（3）	サイバーセキュリティ産業の強化	国 民間	■ 産業としての強化が求められるものの、軍需を含め国による下支えは限定的	① 官民ファンドを活用し、民間企業の海外サイバーセキュリティ関連企業の買収を後押し

（出所）みずほ銀行産業調査部作成

[19] 警察庁によると、2015 年に事業者から報告があった標的型メール攻撃の件数は 2012 年対比で 3.8 倍に増加（「H27 年におけるサイバー空間をめぐる脅威の情勢について」より）

(1)サイバーセキュリティの見える化

(課題)情報共有体制やガイドラインがまだ不十分。他社との比較指標もない

我が国において対策の必要性(=サイバーセキュリティ投資)が十分に認識されない要因の一つには、「どのような攻撃を受けたか」という情報が不足していることがあろう。例えば、ISAC 等のインシデント情報の共有体制は、一部(金融と通信)での取り組みに留まっており、十分とは言えない。

また、「どこまで対策をすべきか」というガイドラインについても課題が残る。2015年12月に出された「サイバーセキュリティ経営ガイドライン Ver1.0」は最初の一歩としては評価されるものの、内容としては主に経営層にサイバーセキュリティの重要性を認識させる定性的なものに留まっている。各企業がセキュリティ対策を強化するには、具体的にどのような対策が必要かを「見える化」し、「何をすべきか分からない」という「不安」を軽減する必要がある。

加えて、他社がどこまでのセキュリティレベルなのか、延いては自社のセキュリティレベルがどの程度なのかが「見えない」というセキュリティ固有の「不安」も問題の根底に存在することも認識する必要があるだろう。

対応策①ISAC制度の拡大

「見える化」のための具体的な対応策として、まずは情報共有体制の拡充が考えられる。実際に、事業者からのヒアリングでも ISAC の実務的な有効性が評価されており、我が国も金融と通信業界だけでなく、少なくとも、重要インフラに指定されている13業種に広げることを目指すべきではないだろうか。本制度は業界の自主的な取り組みではあるものの、普及のスピードを上げるためにも、重要インフラ業種の指定と同様に、ISAC の設置について、国のサイバーセキュリティ戦略に盛り込むのも一つの手段ではないだろうか。

対応策②ガイドラインの更なるバージョンアップ

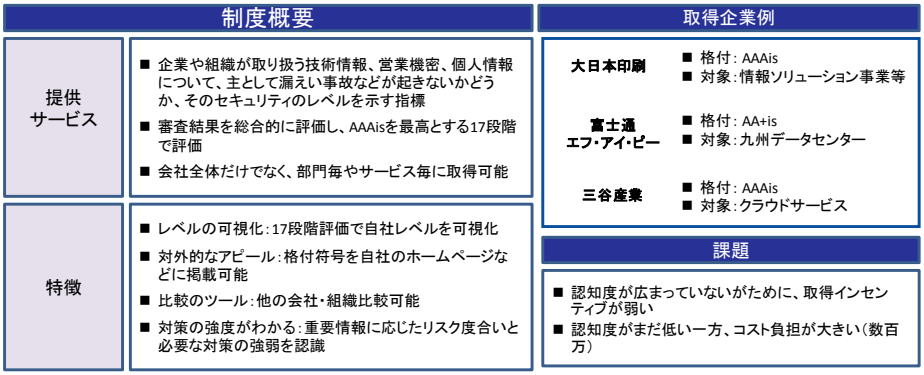
次に、「サイバーセキュリティ経営ガイドライン Ver1.0」のバージョンアップが必要だと考える。企業のセキュリティ対策を更に促すためには米国 NIST のフレームワークのような細分化された指標を示し、自社が取り組むべき対策をより細かく「見える化」することが効果的である。そのことが延いてはセキュリティに対する不安の解消にも繋がるだろう。

対応策③情報セキュリティ格付制度の活用

さらに、セキュリティレベルを「見える化」するツールとして「情報セキュリティ格付」のような制度の活用も考えられる。情報セキュリティの認証基準としては既に ISO27001(情報セキュリティマネジメント:ISMS)があるものの、これはあくまでも「認証を取得しているか否か」の二分法である。「どこまで対策すれば良いのか分からない」という不安を軽減・解消していくためには、自社の取り組み状況をより細分化なレベル分けして可視化することのできる「格付」の普及促進を図ることも有効ではないだろうか。

我が国には、情報セキュリティ格付機関としてアイ・エス・レーティング(富士通や R&I 等がメインスポンサー)が 2008 年に設立され、格付サービスを提供しているものの、まだ広く普及しているとは言えない(【図表 19】)。制度を普及させるためには、格付取得費用に見合うメリットが必要であろう。それには、直接的に格付取得費用を補助する方法や、間接的な方法として「格付を取得した企業に対する公的融資の金利優遇」、「官公庁の入札要件への組み入れ」、「格付によるサイバー保険の保険料割引」等の施策が考えられる。

【図表 19】アイ・エス・レーティングのセキュリティ格付サービス概要



（出所）㈱アイ・エス・レーティング HP を基にみずほ銀行産業調査部作成

（2）中小企業のサイバーセキュリティ強化

（課題）中小企業のセキュリティ対策は遅れており、中小企業を経由して他社が狙われる恐れあり

サイバーセキュリティは弱いところ（企業）が狙われ、そこを踏み台にして他社にも攻撃が広げられるという特徴がある。このことから、セキュリティ対策が遅れがちな中小企業の対策を強化しなければ、日本全体のセキュリティ強化は実現せず、セキュリティに対する不安も解消されない。一方、中小企業はセキュリティ対策に掛けられる資金も人も限られており、各社の自主的な取り組みに任せていては対策が進みづらい。

我が国も米英同様に一般的な中小企業に向けたセキュリティ対策は IPA 等で示されている。とは言え、我が国産業のサプライチェーンの一翼を担い、その技術力の高さにも注目が集まる中小企業が今後さらに狙われる可能性があり、企業のサプライチェーン全体を強化する観点からも、より踏み込んだ対策が必要ではないだろうか。

対応策①クラウドサービスと費用補助を組み合わせることで、セキュリティ強化を図る

ここで具体的な対応策を二つ挙げたい。一つ目は、国や自治体の費用補助と合わせたクラウドサービスの普及促進である。サイバーセキュリティも防災対策の考え方と同様に「まずは自助（自分で身を守る）」という考えが前提であり、中小企業自身でセキュリティを高める必要がある。クラウドサービスであれば中小企業が自前でセキュリティ対策を実施するよりも、一般的にはコストが安く且つメンテナンスもベンダーに任せられるという利点がある。具体的な方法としては、セキュリティ対策ソフトのクラウド化から各種のデータを管理するサーバーのクラウド化まで、企業の状況に合わせて色々な方法が考えられる。

また、費用面については中小企業の IT 利活用促進という観点からも、クラウドサービスに切り替える費用を期限付きで国や自治体が補助することで、中小企業のネックとなるコスト負担を和らげながら、普及の促進が図れるだろう。既に東京都が「省エネに繋がるクラウド化」については費用補助を行っている実例があり、「セキュリティ強化に繋がるクラウド化」についても同様の枠組みを活用できるのではないだろうか。

対応策②大企業が自社のコミュニティを守る発想も必要

二つ目は大企業によるコミュニティクラウドの提供である。これは上記の「自助」での取り組みに加え、「共助（お互いで助け合う）」の取り組みとして大企業が自社のグループ内やサプライチェーン内の中小企業を守るという考え方に基づくものである。具体的な方法としては自社グループやサプライチェーンとい

ったコミュニティ単位でクラウドサービスを導入する「コミュニティクラウド」のような仕組みを大企業が構築・提供する方法があるだろう。

これまでの大企業のサイバーセキュリティに関する考え方は、いかに「自社」を守るかという点に主眼が置かれてきたが、既述のとおり、子会社はもとよりサプライチェーンまで守備範囲を拡張して検討しなければ、もはや実効性のある対策とはなり得ない。また、コミュニティクラウドの活用は、コミュニティ全体のIT コストの低減や、サプライチェーンの業務効率化等、セキュリティ強化以外のメリットも期待できるものでもあり、大企業にとっても導入意義はあると考えられる。

(3)サイバーセキュリティ産業の強化

(課題)現状の取り組みではまだ産業化に時間が掛る

我が国はサイバーセキュリティを産業として強化する方針を打ち出しているものの、米国のような官の需要による大きな下支えがない中、現状のままでは政府が目指す「産業化」には時間を要するだろう。

対応策①官民ファンドを活用し、民間企業の海外企業 M&A を後押し

サイバーセキュリティを産業として拡大・強化(＝産業化)するには、我が国企業も今まで以上に M&A を活用すべきだと考える。産業化の時間軸を早めるには、買収によって先行する海外企業のサイバーセキュリティに関する技術・サービスを取り込むとともに、国内需要の拡大を待つのではなく、既に需要がある海外に打って出ることも必要であろう。買収によって日本企業が海外の高度なサイバーセキュリティ技術やネットワークを獲得できれば、日本企業のグローバルな競争力が高まるとともに、日本のサイバーセキュリティ強化にも繋がるだろう。

サイバーセキュリティの重要性を再度認識し、官民一体となった取り組みに期待

ただし、そのためには、投資負担(リスク)を民間企業のみに負わせるのではなく、投資資金の一部に官民ファンドを活用することで官と民でリスクシェアをし、民間企業の投資を後押しすることも必要ではないだろうか。日本企業のサイバーセキュリティ分野での海外展開支援や、高度な海外のサイバーセキュリティ技術を日本に取り込むという意義を考えれば、㈱海外通信・放送・郵便事業支援機構や㈱産業革新機構等の官民ファンドが活用できるのではないだろうか。サイバーセキュリティの重要性を改めて認識し、官民一体となった取り組みを期待したい。

Ⅳ. 個人情報保護に関する課題と対応策

続いて、個人情報保護に関する動向を見ていきたい。まずは足元の我が国の取り組みを確認し、その後海外の取り組みを見ることでその違いから我が国における課題を把握し、対応策を考察していく。考察にあたっては、パーソナルデータの利活用の仕組み(インフラ)の整備についても、個人情報保護のための取り組みと捉え、併せて見ていくこととする。

1. 日本の個人情報保護に関する取り組み

(1)制度面

個人情報保護法が 10 年振りに改正された

我が国での最近の個人情報保護に関する一番大きなトピックスは、個人情報保護法の改正である(【図表 20】)。2005 年 4 月の個人情報保護法施行から 10 年が経過し、その間に IT 利活用の拡大、高度化が進み、所謂「ビッグデータ活用」に注目が集まる中、第Ⅱ章で説明した「JR スイカ事案」や「ベネッセ事件」等がきっかけとなり、個人情報に関する制度改正を求める声が拡大した。それを受けて、2015 年 9 月に個人情報保護法が改正され、個人情報の定義の明確化や匿名加工情報の新設等、データ利活用を後押しする改正と期待されている(2017 年施行予定)。

第三者機関である個人情報保護委員会が設置され、権限も一元化された

上記に加えて、第三者機関である個人情報保護委員会を設置したことも大きなポイントである。第三者機関ができたことで、従来業界ごとの所管省庁に分かれていた大臣の管理・監督権限が一元化され、立ち入り検査が可能となる等権限自体も強化されており、重要な取り組みと言えるだろう。尚、業界単位等で設置している認定個人情報保護団体[20]は引き続き残り、今後は匿名加工情報に関する加工方法のガイドライン策定を当団体が担う方向で検討が進んでいる。

匿名加工情報に対する期待も高まる

匿名加工情報の制定により、企業が従来活用していなかった、もしくはその活用方法に気付いていなかったパーソナルデータが新たにマーケティング等の材料になることが期待されているものの、現状、まだ匿名加工に関する具体的な規則は個人情報保護委員会から示されていない。

【図表 20】個人情報保護法改正のポイント

項目	主な内容	ポイント
定義の明確化	•個人情報の定義の明確化(顔認識データ等も対象に) •センシティブ情報に関する規定の整備	グレーゾーンの解消
適切な規律の下で個人情報等の有用性を確保	•匿名加工情報に関する加工方法や取り扱い等の規定の整備 •個人情報保護指針の作成や届け出、公表等の規定の整備	利活用ルールの明確化
個人情報の流通の適正さを確保	•オプトアウト規定による第三者提供のルールを明確化 •トレーサビリティの確保	第三者提供のルールが煩雑との声も
個人情報保護委員会の新設及びその権限	•個人情報保護委員会を新設。現行の主務大臣の権限を一元化 •「報告の徴収」や「助言」に加えて、「立入検査」「指導」の権限も	監督機関を設置し、報告や指導体制を整備
海外へのデータ移転ルール	•従来なかった「第三国」へのデータ移転のルールを規定 •日本と同水準の保護レベルの国もしくは、個別契約での対応に	EUデータ保護規則への対応
その他	•違反者には6カ月以下の懲役または30万円以下の罰金が科される •全ての事業者が対象に(個人情報保有件数の条件を撤廃)	従来は5,000件超のデータ保有事業者のみ対象

(出所)個人情報保護委員会資料等を基にみずほ銀行産業調査部作成

[20] 個人情報保護法で定められた認定制度。一般的には業界単位で設けられている。主に、個人情報の取り扱いに関する苦情の処理や、個人情報の適正な取り扱いに寄与する事業者への情報提供等を担う。

(2)利活用の仕組み

パーソナルデータの利活用に際しては、その仕組み作りも重要である

個人情報の利活用に際しては、自身での利活用においても第三者による利活用においても、法整備だけでなく、利活用できる仕組み作りも重要である。一般的にパーソナルデータは個人本人ではなく、公的機関や企業が様々な組織に分かれて関連するデータを所有している。そのため、個人にせよ、企業にせよ、あるパーソナルデータを何時でも自由に活用できる状態にはないケースが大半である。例えば、ある人の医療データ(カルテ)は各病院が所有しており、電気の使用データは各電力会社が持っている。したがって、それぞれの利用者本人が当該データを利活用しようとしても、自由には取得できない。このような状況も、利活用を進みづらくしている要因の一つと考えられる。

利活用の仕組みとして代理機関(仮称)や情報銀行等の検討が行われている

このような状況を踏まえ、情報を円滑且つ有効に活用できる仕組み作りを目指し、国や大学が主体となって個人情報を管理・仲介する機関の在り方が検討されている。具体的には、内閣官房 IT 戦略室で議論されている「代理機関(仮称)」(以下、代理機関)や、東京大学と慶應大学が中心となってコンソーシアムを立ち上げている「情報銀行」等がある。

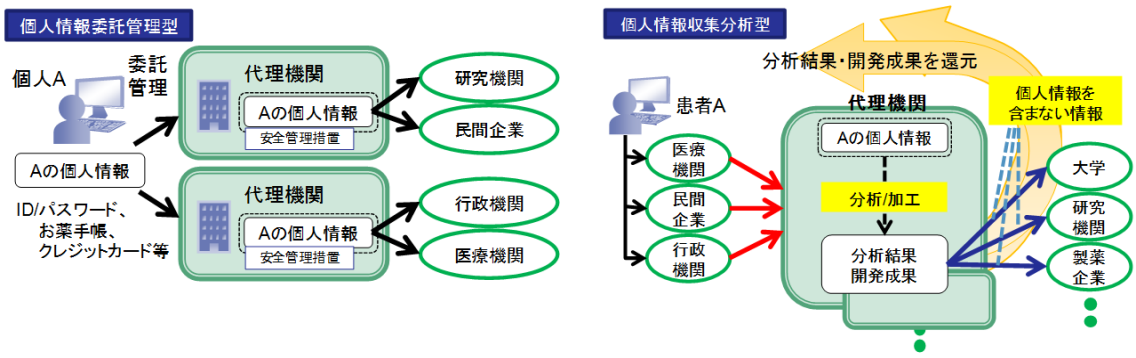
代理機関は公的な後押しにより利活用を進めようとする仕組み

ここで、その中でも検討が進んでいる代理機関について見てみたい。代理機関とは公的機関が民間企業等に認定を与える、つまり、公的機関が安全性に「お墨付き」を与えることで、パーソナルデータの利活用を促そうとする取り組みである(【図表 21】)。

代理機関には「個人情報委託管理型」と「個人情報収集分析型」の 2 つの検討モデルが示されており、前者は本人の同意に基づき自身の個人情報を活用するために、代理機関に個人情報を預け、第三者が活用するモデルであり、後者は本人の明確な同意なしに、多種多様な機関にある個人情報を代理機関が収集し、分析・加工した上で他の研究機関等で活用するモデルである。

まだ制度自体も不明な部分が多いものの、公的な後押しにより、利活用を進めようとする取り組みの方向性は、正しいと言えるだろう。ただし、個人情報委託管理型モデルは「本人同意に基づく仕組みであるため、現行の法制度で運用が可能」との理由から、現状は代理機関に関する議論が進んでいない。今後の具体的な議論の動向は注視していく必要がある。

【図表 21】代理機関の検討モデル



(出所)各種資料よりみずほ銀行産業調査部作成

2. 米国の個人情報保護に関する取り組み

ここからは海外の動向を見ていきたい。まずはデータ利活用で先行する米国の取り組みを確認し、続いて個人情報の保護に重きを置く取り組みや、政府主導でデータ利活用の制度整備が進められている EU・英国の取り組みを見ていくこととする。

(1)制度面

米国では包括的な個人情報保護法制はない

米国の個人情報保護法制は一部の業種(金融、医療等)やテーマ別(子供の保護等)に個別法が定められているものの、我が国の個人情報保護法のような一般法はない(【図表 22】)。

匿名化に関する包括的な規定はないが、医療分野では具体的な匿名加工方法が定められている

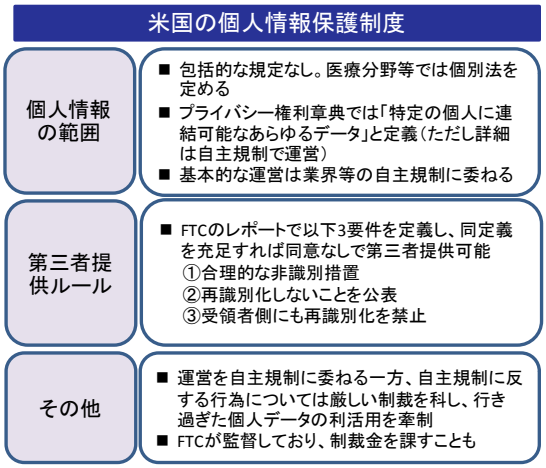
個人情報の監督機関としては、1915 年に設置された FTC[21]があり、1974 年の連邦プライバシー法(公的部門向け)制定以降、プライバシー関係も FTC が監督している。匿名加工情報については、同機関が「レポート」という形で取り扱いに関する指針を示しているものの、匿名加工方法に関する包括的な規則はない。ただし、個別法で個人情報保護を定めている医療分野については匿名加工に関する規定が存在する。具体的には、医療分野の法律である HIPAA[22]では名前、電子メールアドレス、社会保障番号などの 18 項目の情報を除去することが明確化されている。我が国も匿名加工の規則を考える上ではこういった例が参考にできるだろう。

自主規制に支えられたデータ利活用が進展。ただし、近年はプライバシー保護の機運も高まる

対応する個別法の無い業種・分野における個人情報の保護は、「自主規制」として事業者の裁量に委ねられている。このような裁量を活かしてデータ利活用を進めている例として民間のデータブローカーの存在が挙げられる。データブローカーとは個人に関わる情報を様々な情報ソースから収集し、プロファイリング[23]した上で第三者に販売する事業者であり、上場しているデータブローカーが存在することからも、米国ではデータ利活用が社会に広く受け入れられていることが分かる。この「受容性」が米国のデータ利活用を支えるポイントの一つと言えるだろう。ただし、近年は FTC がデータブローカーに対するレポートを公表する等、プライバシー保護の機運も高まってきている。

[21] 連邦取引委員会、Federal Trade Commission の略称
[22] Health Insurance Portability and Accountability Act、医療保険の相互運用性と説明責任に関する法
[23] 履歴データなどから人物像を描く(推測する)行為

【図表 22】米国個人情報保護制度の概要



（出所）各種資料よりみずほ銀行産業調査部作成

（2）利活用の仕組み

政府主導の利活用の取り組みであるスマートディスクロージャー制度

パーソナルデータの利活用の仕組みとしては、政府が主導する「スマートディスクロージャー」制度が挙げられる。これは政府や企業が保有するパーソナルデータをデジタル化してユーザー（本人）に提供する取り組みであり、消費者がより良いサービスや商品を選択する際の意思決定をサポートする取り組みである。

実際に医療、教育、エネルギー、金融などの複数の分野でこの制度に基づいたデータ利活用が始まっている。例えば医療分野では「ブルーボタン・イニシアティブ」という取り組みがあり、一部の医療機関では本人が WEB サイト上で自身の医療情報をテキストファイル等でダウンロードでき、当該情報を他の医療機関に提供することを可能にしている。このような取り組みはまだ限定的ではあるものの、データの本来の所有者である個人が自身のデータを自分の意思で活用できるような仕組み作りと言える。

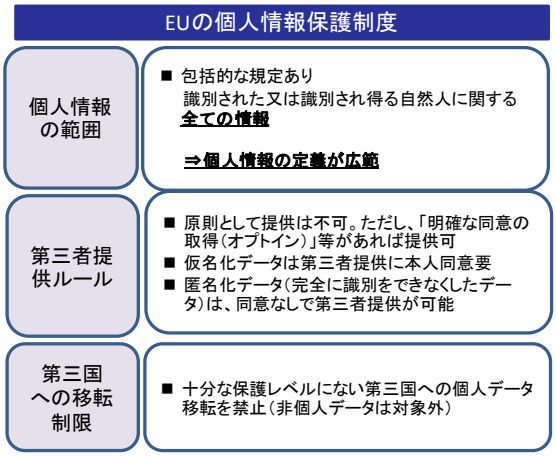
3. EU・英国の個人情報保護に関する取り組み

（1）制度面

EU では個人のプライバシーを中心に制度が考えられている

EU では「プライバシーは重要な人権の一つ」という基本理念が重視され、個人情報保護制度は「個人の権利」を中心に考えられており、法律（EU データ保護規則）で定められている（【図表 23】）。米国を情報の「利活用」を中心とした仕組みとするならば、EU は情報の「保護」が中心に置かれた仕組みだと言えるだろう。個人情報の定義も広範なことに加え、十分な保護レベルにない第三国への移転も制限し EU 市民の個人情報を保護していることからも、その「保護」の意識の強さが窺える。

【図表 23】EU の個人情報保護制度の概要



（出所）各種資料よりみずほ銀行産業調査部作成

イギリスやフランスの監督機関は、長い実績あり

EU においても匿名加工方法に関する包括的な規則はなく、識別に用いられるあらゆる情報を踏まえて各国の監督機関が判断するとされている。EU 域内の監督機関としては、イギリスの ICO[24]（1984 年設置）やフランス CNIL[25]（1978 年設置）等、長く実績を重ねた機関も多く存在する。

EU の匿名加工情報に類似する定義は 2 種類あり

匿名加工情報に関しては、個人情報保護法で規定された日本の匿名加工情報に類似する「匿名化データ」と「仮名化データ[26]」の 2 種類のデータがあり、そのうち「仮名化データ」が日本の匿名加工情報に近い概念と言える。匿名化データは「データ主体がもはや識別できないデータ」であるため、そもそも EU データ保護規則の適用対象外であり、第三者提供も制限されるものではない。他方、「仮名化データ」は「個人データ（個人情報）」と見做され、第三者提供には原則個人の同意が必要となっている。このことから、データ利活用においても、保護を意識した制度となっていることが分かる。

（2）利活用の仕組み

利活用についても個人の権利を中心にした発想から生まれている

データ利活用に関する取り組みも「個人により良いサービスを選ぶ権利を与える」という個人の権利を起点として考えられている。英国ビジネスイノベーション・職業技能省が 2011 年に始めた「midata」プロジェクトは、消費者が民間企業の持つ自分の個人データに自由にアクセスでき、電子データとしてダウンロードできるようにすることで、個人が自分の意思でより良いサービス、商品の選択に繋げようとする取り組みである。

金融分野やエネルギー分野で具体的なサービスあり

具体的に金融分野で利用されているサービスとしては、個人が取引銀行のオンラインサイトで自身の 12 カ月分の取引履歴をダウンロードし、金融サービス比較サイトで同データをアップロードすると、同サイトのアルゴリズム解析により、データ分析され最適な金融商品等を紹介するサービスがある。また、エネルギー分野では、電気やガスの使用データをダウンロードし、同データをもとに他社との料金プラン比較や、節電アドバイスが受けられるサービス等が提供されている。

[24] ICO：Information Commissioner
[25] CNIL:Commission nationale de I’informatique ct dcs libcrtcs
[26] 追加情報の利用なくしては、特定のデータ主体に結び付けできないように処理した個人データ

このような取り組みも米国の「スマートディスクロージャー」と同様に、政府主導でデータの利活用ができる仕組みを整備し、個人が自身の意思でその仕組みを活用するというのが先進国における一つのトレンドと言えるだろう。我が国でも、2016 年 5 月に経済産業省から出された「新産業構造ビジョン」の中間整理案の中で、データ利活用における今後の取り組みとして、「本人関与の下での個人データ利用の仕組みの検討」が方向性として示されており、こうしたトレンドを捉えた取り組みと言える。

4. 日本の課題と対応策

匿名加工情報は評価できる取り組みであるものの、まだ課題が残る

ここまで見てきたように、我が国も個人情報保護法改正等、個人情報保護に関する取り組みが進んでいないわけではない。匿名加工情報を包括的に法律で定めようとする取り組み自体は米・EU よりも踏み込んだ対応との評価もある。しかしながら、改正個人情報保護法も 2017 年の本格施行までにはまだ時間が掛かり、匿名加工情報に関しても匿名加工に関する規則が決まっていない等、まだ制度としては取り組むべき課題が残る。

匿名加工情報の詳細制度を固め、利活用のインフラも整備する必要あり

また、我が国の国民性としてプライバシーの意識が高いという特徴もあり、データ利活用で先行する欧米諸国に追いつくためには、この匿名加工情報をデータ利活用の起爆剤とするべく早期に制度の詳細を固め、それに加えてデータ利活用を促す仕組み（インフラ）も早急に整備する必要があるだろう。ここではこの 2 点を取り組むべき課題とし、その対応策を考察していきたい（【図表 24】）。

【図表 24】個人情報保護に関する課題と対応策

	項目	実施主体	課題	対応策
（1）	匿名加工に関するルールの整備	国	■ 匿名加工の規則等がまだ具体的に決まっていない ■ 保守的なルールになると利活用が進まない可能性あり	① 個人情報保護委員会が認定個人情報保護団体のガイドライン策定までサポート ② 匿名加工方法の工夫（削除項目を明示する等） ③ 匿名加工方法にテクノロジーを活用
（2）	利活用の仕組みの整備	国	■ 利活用を後押しするインフラがまだ整備されていない	① 医療分野で代理機関の成功モデルを示し、その他の業種にも広める ② 代理機関、情報銀行を別々で検討するのではなく、まずは一つのモデルケースを作る ③ 加工しない個人情報を管理・仲介する機関についても公的な認定を活用

（出所）みずほ銀行産業調査部作成

（1）匿名加工に関するルールの整備

（課題）匿名加工に関する正式な規則や公表時期も未定

データ利活用を促す新たな制度として期待される「匿名加工情報」であるが、まだ制度のポイントとなる匿名化に関する規則やガイドラインが示されていない（【図表 25】）。規則・ガイドラインの内容が保護と利活用のバランスのとれたものになるのか、公表されるタイミングはいつなのか等現状まだ不明な点が多い。

また、現状の制度設計としては、個人情報保護委員会が匿名化に関する規則を定め、各認定個人情報保護団体がより細かいガイドラインを策定するというものである。これは団体毎に柔軟にガイドラインが策定できるプラスの面がある一方、各団体任せとなって形式的なガイドラインとなれば結果的に使いにくくなってしまうマイナス面も懸念される。

対応策①個人情報保護委員会のより踏み込んだ指導を期待。人員の拡充も必要

利活用を後押しする制度とするためにも、ガイドライン策定やその後のメンテナンスについては、個人情報保護委員会に監督機関として一歩踏み込んだ指導を期待したい。例えば、各認定保護団体に対し個人情報保護委員会が監督するだけでなく、ガイドライン策定も含めたコンサルテーションまで提供することも必要ではないだろうか。ただし、他国と比べて我が国の同委員会はまだ経験が浅いため、その分人員の拡充は必要となろう。イギリスの ICO 職員数 379 名（2015 年 3 月末）に対し、我が国の同人数は 52 名（2016 年 3 月末）であり、現状も十分な人員が確保できているとは言えない。

対応策②匿名加工方法については米国や EU の事例も参考にすべき

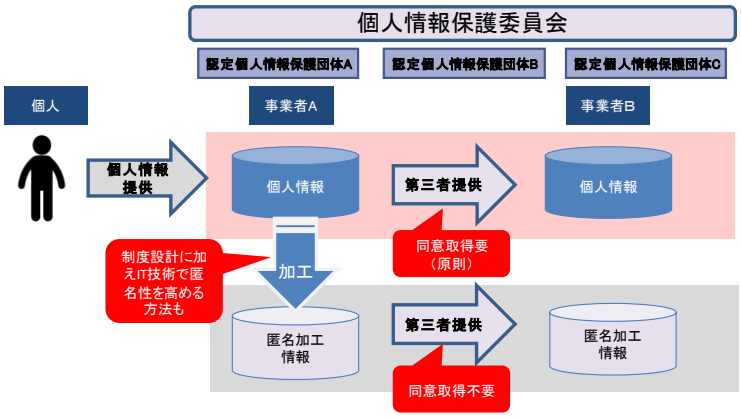
また、匿名加工の方法についても、より利活用が進むような工夫が必要だろう。現状、利活用に対する不安が強い我が国としては、利活用が浸透するまでは、まず米国の医療分野のように加工（削除）すべき項目を明確化し、個人に匿名化に対する安心感を与え、次のステップで規則を緩和する（例えば、削除すべき項目を減らす）ような、2 段階で制度の浸透を図るというのも一案だと考える。

対応策③匿名化技術に関するテクノロジーも活かし、匿名加工情報の安心感を高めることも重要

加えて、匿名加工情報の信頼性を高めるには匿名化方法をテクノロジーで補強するという方法も考えられる。具体的な例をあげると、NTT が開発したパーソナルデータ匿名化システムは、匿名性と有用性のトレードオフをバランスさせ、データの有用性が損なわれにくい匿名化データを得ることを可能としている。また、最近では、日立製作所がパーソナルデータを暗号化した状態で匿名化する技術も開発している。

こういった IT 企業のテクノロジーを活用することで、上記のような匿名加工に関する制度面での工夫に加え技術面でも補強を加えることで、匿名加工情報の安心感を高めることも制度を広める一つの方法ではないだろうか。

【図表 25】個人情報と匿名加工情報の体系



（出所）各種資料よりみずほ銀行産業調査部作成

(2)利活用の仕組みの整備

(課題)代理機関や情報銀行もまだ検討途上であり、仕組みが未整備

現在、利活用の仕組みとして検討されている代理機関や情報銀行はまだ検討段階の域を出ていない。代理機関については、具体的にどのような企業や機関が代理機関に成り得るのか、どういう認定フローがあるのか等、詳細設計がまだ不明である。データ利活用を促すためにも、このような利活用の仕組みの整備を急ぐ必要がある。

対応策①医療分野で成功モデルを示し、他分野にも広げる

現在、内閣官房の次世代医療 ICT 基盤協議会にて医療分野で匿名加工情報の活用を想定した代理機関の制度整備が進められており、まずはこの取り組みが先行事例として進展することを期待したい。これにより、今まで十分に活用できていなかった個人の医療情報等を匿名化して活用することができるようになれば、新薬の研究開発や新しい治療方法の発見、延いては国民の健康はもちろん、我が国の重要課題である医療費(社会保障費用)削減なども期待できよう。このような「成功モデル」を医療分野で示すことができれば、その他の業種にも波及的に広まっていくことが期待できる。

対応策②利活用の仕組みとしてまず一つのモデルケースを作るべき

また、制度整備を早めるためにも、利活用の仕組みとして、国と大学それぞれで検討している「代理機関」と「情報銀行」を、別々で検討するのではなく、官・学の取り組みを結集させ、まず一つのモデルケースを作るという考えも一案ではないだろうか。内閣官房 IT 総合戦略室の資料[27]でも「将来に向けた検討」として情報銀行のモデルを取り入れた仕組みが示されており、このような検討が具体的に進んでいくことを期待したい。複数の仕組みを作るよりは、一つの仕組みにデータを集める方が、データ利活用の「効果」という観点でも有効だと考える。

対応策③加工しない個人情報についても認定制度を活用する

さらに、現在医療分野で検討されている個人情報を加工(匿名化)して活用することを想定した代理機関の認定だけでなく、【図表 21】の個人情報委託管理型モデルのような個人情報をそのまま管理・仲介する機関についても同様に公的な認定を与え、個人情報を加工せずに利活用する取り組みも後押しすべきではないだろうか。当該モデルについては、まだ代理機関認定の議論が進んでいないが、公的な認定制度を活用し、取り扱う機関の信頼性を高めれば、匿名加工情報よりも利活用を躊躇しがちな個人情報の利活用も、より進みやすくなるだろう。

最終的に目指すべき利活用の姿は、企業主導ではなく、個人主導の利活用である

最終的に目指すべきパーソナルデータ利活用の仕組みは、個人が自分の意思で自身のパーソナルデータを自由に取得・活用できる仕組み(インフラ)であり、従来の「企業主導」の利活用ではなく、個人が活用する情報の種類や自身のニーズに合わせてどの情報をどのように活用するのかを選ぶ、「個人主導」の利活用だと言える。そのゴールを目指し、ここで挙げたような制度や仕組みの整備が少しでも早く進んでいくことを期待したい。

[27] 2016 年 5 月 20 日、情報通信技術(IT)の利活用に関する制度整備検討会資料より

Ⅴ. おわりに

「新産業構造ビジョン」の具体的な戦略でもデータ利活用の促進が挙げられている

2016 年 4 月に公表された経産省の新産業構造部会の「新産業構造ビジョン」の中間整理案でも、第 4 次産業革命による新たな成長に向けた我が国の具体的戦略の一番最初の項目に「データ利活用促進に向けた環境整備」と記載されており、政府のデータ利活用に対する期待の大きさと優先度の高さが分かる。

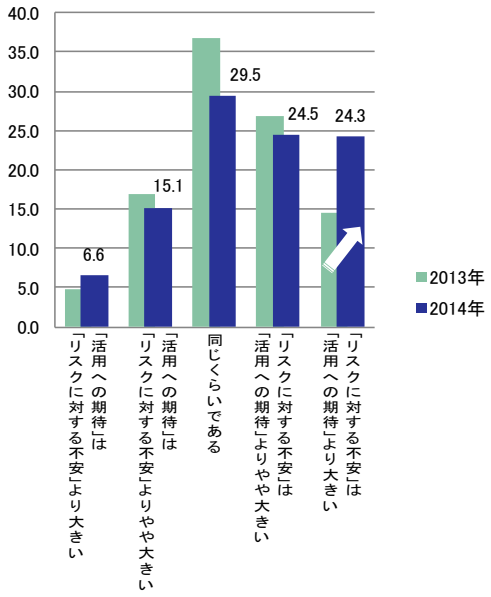
GDP600 兆円の目標達成には、データ利活用は欠かせない

データ利活用がもたらすその経済効果は、総務省の産業を限定した試算[28]で 7.7 兆円と示されており、全産業に広げればより大きな経済効果が期待できるだろう。また、2016 年 5 月に経産省から発表された製造業での IoT による GDP の押し上げ効果は約 13 兆円と試算されており、データ利活用から波及的に広がるその経済効果の大きさが分かる。加えて、データ利活用と表裏をなすサイバーセキュリティにおいても「産業化」に向けた取り組みが進めば、更なる経済効果を期待できよう。2020 年までに GDP600 兆円を目指す我が国にとっては、「データ利活用」と「サイバーセキュリティの強化」はもはや目標達成のための前提条件と言っても過言ではない。

現状は利活用のメリットよりも、不安の方が大きい

ただし、データ利活用を進めていくには、ここまで挙げてきた制度や仕組みの整備に加えて、個人と、そして企業もデータ利活用に対する意識を変えていく必要がある。既に述べた通り、我が国は個人におけるプライバシーに関する意識が他国と比べて高いという特徴もあり、データ利活用の重要性は認識されつつあるものの、データ利活用に対する意識としては、いまだに利活用のメリットよりも不安の方が高まっている可能性がある(【図表 26】)。

【図表 26】生活者情報の利活用に対する期待と不安の大きさ



(出所) 日立・博報堂ビッグデータに関する調査(2014 年 6 月調査)
を基にみずほ銀行産業調査部作成

[28] 小売業、農業、製造業、インフラ(道路・交通)4 つの分野且つ特定の事業に対する推計

不安以上のメリットを示せば、利活用は進む

データ利活用を広めるには、この不安を軽減し、不安以上に利活用による大きなメリットを示していくことが重要だと考える。そのためには、今回新たに定められた匿名加工情報を活用したユースケースを様々な分野で積み上げていき、「データ利活用に対する安心感」や「利活用によるメリット」を個人にも企業にも広く浸透させていくことが求められよう。

安全でデータ利活用が進む国を目指し、最初のひと押しは国が担うべき

サイバーセキュリティの強化により安全性が高まり、データの利活用が拡大すること自体の直接的な受益者は企業や消費者を含めた経済社会全体である。一方、これまで見てきたように様々な課題もあることから、企業や個人による自主的な取り組みのみに任せていたのではサイバーセキュリティもデータ利活用もそのモードチェンジには時間を要す。安全なデータ利活用が進む国を少しでも「早く」実現するためにも、その取り組み意義（国益）も踏まえ、データ利活用拡大に向けた国としての力強い後押しを期待したい。

（本稿に関する問い合わせ先）
みずほ銀行産業調査部
テレコム・メディア・テクノロジーチーム　澤田　洋一
youichi.sawada@mizuho-bk.co.jp

【主要参考文献】

1. 資料・書籍等
- 「H25 年情報通信白書」「H26 年情報通信白書」（総務省）
- 「情報セキュリティ白書 2015」（独立行政法人情報処理推進機構）
- 「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」（独立行政法人情報処理推進機構）
- 「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」（消費者庁）
- みずほ産業調査「IoT（Internet of Things）の現状と展望」
- 城田真琴「パーソナルデータの衝撃」ダイヤモンド社
- 小林慎太郎「パーソナルデータの教科書」日経 BP 社

2. 新聞・雑誌等
- 日本経済新聞（日本経済新聞社）
- 日経産業新聞（日本経済新聞社）
- 日経コンピュータ（日経 BP 社）

3. Web サイト
- 経済産業省(http://www.meti.go.jp/)
- 総務省(http://www.soumu.go.jp/)
- 首相官邸(http://www.kantei.go.jp/)
- 個人情報保護委員会(http://www.ppc.go.jp/)
- 独立行政法人情報処理推進機構(https://www.ipa.go.jp/)
- Japan Computer Emergency Response Team Coordination Center(https://www.jpcert.or.jp/)
- National Institute of Standards and Technology（NIST）(http://www.nist.gov/)
- Federal Trade Commission（FTC）(https://www.ftc.gov/)
- Information Commissioner（ICO）(https://ico.org.uk/)

そのほか、IT ベンダー各社の Web サイト、プレスリリース等

Mizuho Industry Focus／184　2016　No.8　　平成 28 年 8 月 4 日発行

編集／発行　みずほ銀行産業調査部　　東京都千代田区大手町 1-5-5　Tel. (03) 5222-5075


MIZUHO


OneMIZUHO
未来へ。お客さまとともに