平成２４年度　ＩＣＴ基盤・サービスの高度化に伴う新たな課題に関する調査研究の請負

報告書

平成 25 年 3 月

総務省情報通信国際戦略局情報通信経済室
（委託先：みずほ情報総研株式会社）

～目　次～

1. 調査の背景･目的

ＩＣＴ分野における技術革新の進展に伴うＩＣＴ基盤・サービスの高度化により、スマートフォンやソーシャルメディアといった新たなＩＣＴトレンドが普及するとともに、個人に関するデジタルデータが日々大量に生成されるようになった。

これに伴い、ビッグデータビジネスとして、多種多様なデジタルデータを処理し、利活用による新たな付加価値等の創出が期待されているところである。他方、ＩＣＴ基盤・サービスの高度化に伴い、データの不正取得によるプライバシーの侵害や、標的型攻撃の増加やスマートフォン等を狙ったマルウェアの増加といった情報セキュリティに関する脅威の拡大など、ネット社会に対する不安についても国民の関心は高まってきている。

本調査研究では、利用者アンケート調査を国内外で実施し、今後の「スマート革命」の進展も踏まえたＩＣＴ利活用状況と利用する上での意識について国際比較を行い、我が国の消費者意識の国際的位置づけと今後の課題について分析を行った。また、これらの課題に関連する諸外国の政策動向についても情報収集・整理を行った。

なお、本調査研究結果は、平成２５年情報通信に関する現状報告（情報通信白書）へ掲載した。

2. 各国利用者の意識に係るウェブアンケート調査の企画・実施・集計・分析等

2.1 ウェブアンケート調査の実施概要

2.1.1 調査の目的

ここでは、「スマート革命」の進展に伴う ICT の利用状況の変化や新たな課題に関する調査・分析として、インターネット上で提供されている各種サービスに係る利用行動やその変化に着目し、情報セキュリティやデータ保護、データプライバシーなどの顕在化している課題を把握した。

図表 2-1 ウェブアンケートの調査項目

調査項目	内容
インターネット利用者の消費の変化・利用意向に関する調査	・属性（年代、性別等） ・インターネット環境（接続端末、利用頻度等） ・インターネットサービスの利用状況及び変化
インターネット上における消費・利用の変化がもたらす課題に関する意識調査	・情報セキュリティなどの認知状況や安全対策状況 ・個人情報の捉え方 ・各種インターネットサービス利用にかかる個人情報の取り扱いに関する意識
総務省の関連政策の浸透度に関する調査	・スマートフォンセキュリティ 3 か条の認知状況 ・忘れられる権利の認知状況

2.1.2 調査の方法

本調査はウェブ（Web）アンケートの方法にて実施した。

日本、米国、アジア主要国（韓国、シンガポール）、欧州主要国（英国、フランス）の合計 6 カ国を対象とし、各国比較を行った。なお、対象国の選定にあたっては、スマートフォンの活用が消費行動に影響を与えるとの仮説のもと、一定程度の普及がされている国を対象とした。

また、情報セキュリティ分野、プライバシー分野の学識経験者へのヒアリングを実施し、アンケート調査設計、分析結果の精緻化をはかった。

図表 2-2 対象国の選定

国	選定理由
日本	・ 【スマートフォンは普及期】日本のスマートフォンの普及率は、29.3%、タブレット端末は 8.5%（「平成 24 年度　情報通信白書」より）。
米国	・ 【スマートフォンが急速に普及】2011 年 7 月現在で、米国のスマートフォン利用者数は 8,220 万となっており、4 人に 1 人以上がスマートフォンユーザー（comScore 社）。 ・ 【通信回線には課題あり】AT&T では、2010 年 6 月に、モバイル・データ通信のトラヒックの急増に対応するため、スマートフォン向けの定額無制限データプランの提供を停止し、従量制データプランに切り替えを行った。新機種や低価格帯のスマートフォンのラインナップの拡充を行っているほか、 アプリストア市場への参入、モバイル通信網の強化を行っている。
英国	・ 【スマートフォンの普及】2009 年からモバイルデータサービスの利用が急増しており、PC・ラップトップに接続するドングルを通じたインターネット接続とモバイル端末によるデータサービス利用が増加している。2010 年にはモバイルデータ量が 67%増加しており、この背景は、2011 年 3 月時点で英国の人口の 26%が所有していることが一因である。
フランス	・ 【スマートフォンの急速な普及。若年層がターゲット】2011 年 9 月末で仏国内の移動端末所有に占めるスマートフォンの割合は 1 年前の 10%台から 40%に増加、2011 年末には 50%を超えると予測。2011 年後半に入り、各事業者は特に 35 歳以下のスマートフォンユーザーに向けた低価格の対応契約の開発に注力。 ・ 【国の施策により、電子商取引が活発】「デジタル・フランス 2012」の成果により、電子商取引の売上高が 2007 年の 150 億ユーロ（約 1.5 兆円）から 2011 年の 370 億ユーロ（約 3.7 兆円）に拡大。この期間にオンライン販売サイトが 3 万 5500 から 10 万まで増加。
韓国	・ 【スマートフォンの普及率が高い】2012 年上半期には携帯加入者に占めるスマートフォン普及率は 50%に迫る。 ・ 【コミュニケーション系アプリの普及】韓国発のモバイル・メッセンジャーアプリ「カカオトーク」は、全利用者数 6,500 万（2012 年 9 月末現在）のうち半数以上が韓国内の利用者。韓国ではスマートフォン利用者のほぼ全員がカカオトークを利用している。
シンガポール	・ 【スマートフォンの普及率が高い】スマートフォンの普及率は、7 割を超えるといわれ、他国と比較しても非常に高いスマートフォン普及率となっている。また、タブレット PC の普及率も高く、2012 年末までには 60%近くまで伸びる見込み。

2.1.3　調査の実施概要

本調査では、上述のように、日本と諸外国の国民のインターネット上の個人情報（パーソナルデータ）取扱いの考え方や情報セキュリティへの意識を把握・比較することを目的に、日本、米国、英国、フランス、韓国、シンガポールの 6 カ国を対象としたウェブアンケート調査を実施した。調査の概要は以下の通りである。

図表 2-3　調査の概要

<table>
<tr><td>調査方法</td><td>ウェブアンケート調査</td></tr>
<tr><td>調査期間</td><td>平成 25 年 3 月</td></tr>
<tr><td>調査地域</td><td>日本、米国、英国、フランス、韓国、シンガポール</td></tr>
<tr><td>対象</td><td>20 歳以上の男女</td></tr>
<tr><td>対象の選定方法</td><td>ウェブアンケート調査会社が保有するモニターから、世代（20 代、30 代、40 代、50 代、60 代以上）、男女比が均等になるよう抽出・割付</td></tr>
<tr><td>回収数</td><td>各国 1,000 件、6 カ国計 6,000 件
各国の世代、性別ごとの回収数は以下の通りである。
<table>
<tr><th></th><th>20 代</th><th>30 代</th><th>40 代</th><th>50 代</th><th>60 代以上</th><th>合計</th></tr>
<tr><td>男性</td><td>100</td><td>100</td><td>100</td><td>100</td><td>100</td><td>500</td></tr>
<tr><td>女性</td><td>100</td><td>100</td><td>100</td><td>100</td><td>100</td><td>500</td></tr>
<tr><td>合計</td><td>200</td><td>200</td><td>200</td><td>200</td><td>200</td><td>1,000</td></tr>
</table></td></tr>
<tr><td>主な調査項目</td><td>・　インターネット接続・利用状況
・　パーソナルデータの範囲の認識
・　パーソナルデータの利用・取扱いへの意識
・　パーソナルデータを活用した個別ケース（利用シーンやスマートフォンの利用等）における影響
・　個人情報保護に関する考え方
・　情報セキュリティ全般の認識・意識
・　スマートフォンの情報セキュリティに係る認識・意識
・　情報セキュリティに係る対策状況
・　回答者属性（年齢、性別等）</td></tr>
</table>

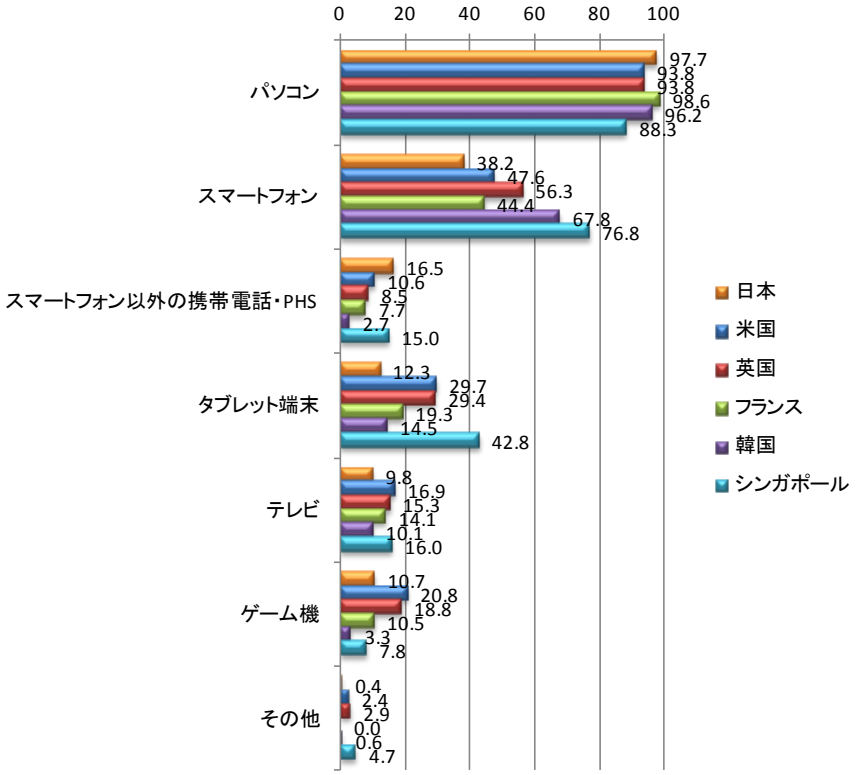
2.2　インターネット利用者の消費の変化・利用移行に関する調査

インターネット利用者のサービス（コンテンツ含む）に係る消費の実態及び変化に関する調査を行い、その要因や利用者の意識に関する分析を行う。また、今後の利用意向について調査を行い、O2O やスマート端末のマルチスクリーン利用、その他新しいサービスに関する利用者の受容性に関する評価・分析を行った。国際比較の観点から 6 カ国の分析を行い、グローバルトレンドを把握した。

2.2.1　インターネットの利用状況

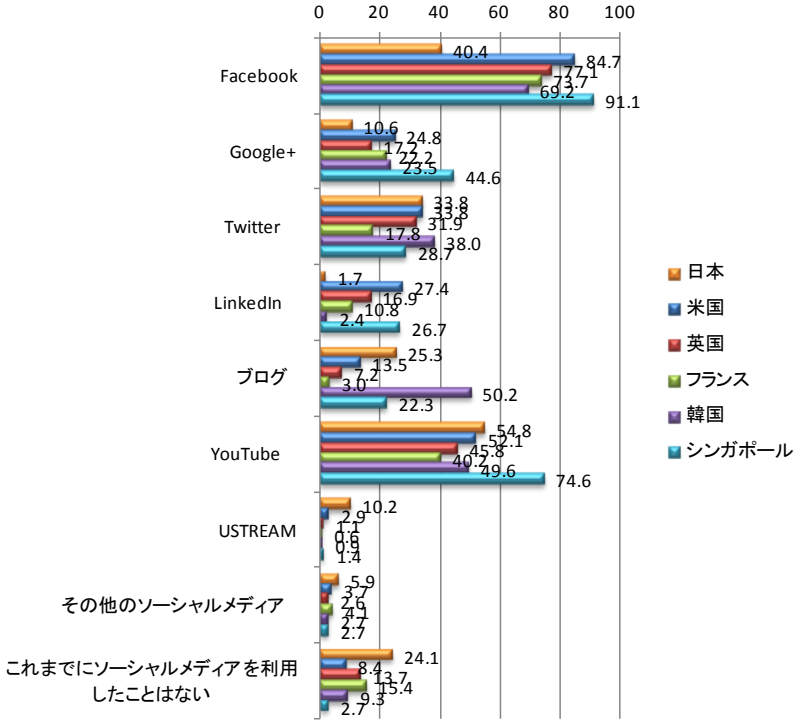
今回の調査対象とした日本、米国、英国、フランス、韓国、シンガポールの 6 か国におけるインターネット接続端末の保有状況、ソーシャルメディアの利用状況を比較した結果を下記に示す。

日本の結果に着目するとスマートフォン普及率は 38.2%と調査対象の 6 カ国の中で最も低く、また各種ソーシャルメディアの利用率についても低い利用率が伺える結果となった。



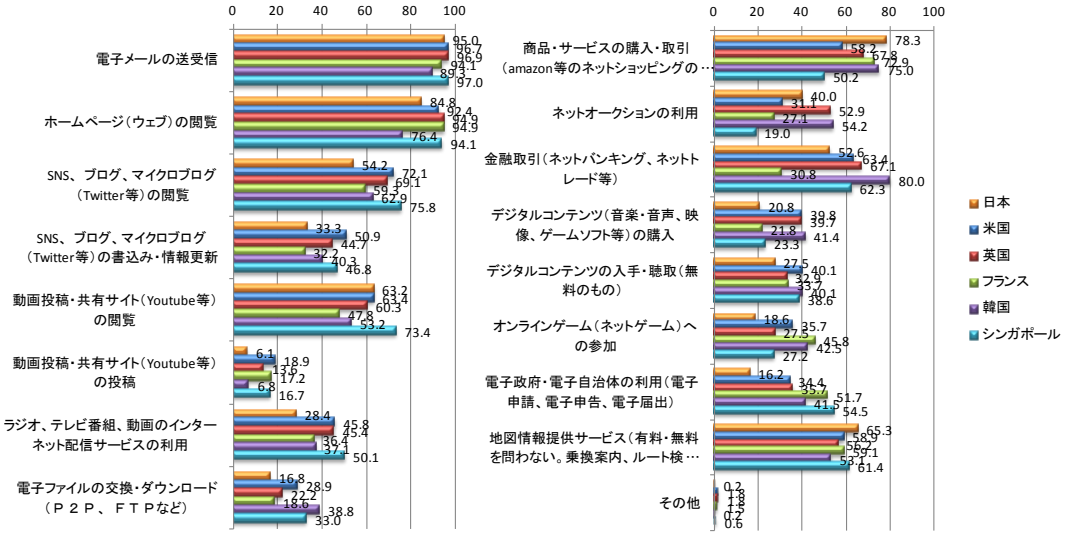
図表 2-4　インターネット接続に利用する端末[1]

[1] 日本、米国、英国、フランス、韓国、シンガポールのサンプル数は各 1000 件となっている。以下のグラフで、サンプル数の表記のないものは同様である。



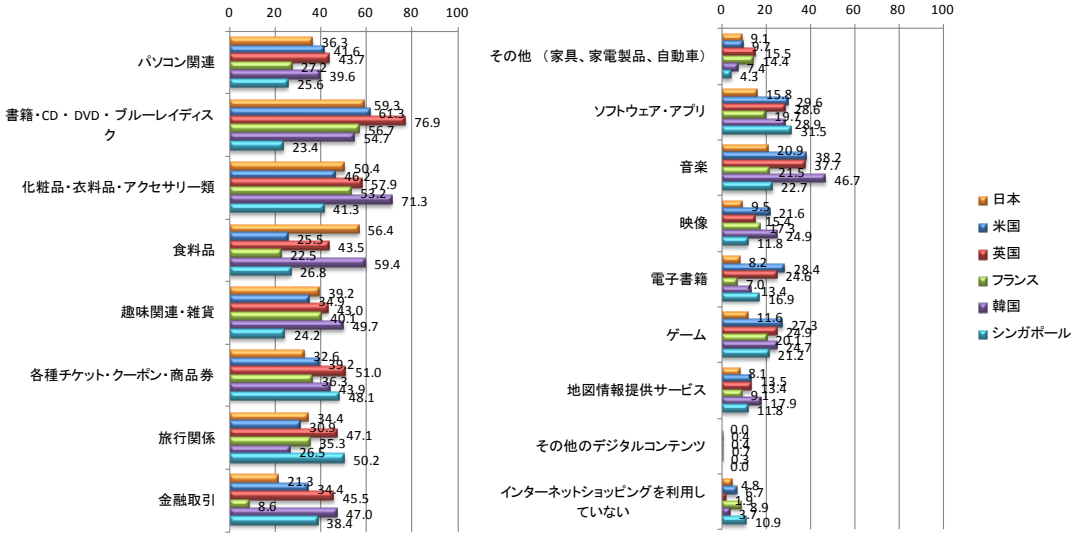
図表 2-5　ソーシャルメディア利用率

インターネットの各種サービスの利用状況についてを見ると、取引サービスの代表例とみることのできる「商品・サービスの購入・取引」については、日本は 78.3%と 6 か国中最も利用率が高かった。その一方、「電子政府・電子自治体の利用（電子申請、電子申告、電子届出）」については、16.2%となっており各国と大きな格差があることがわかる。



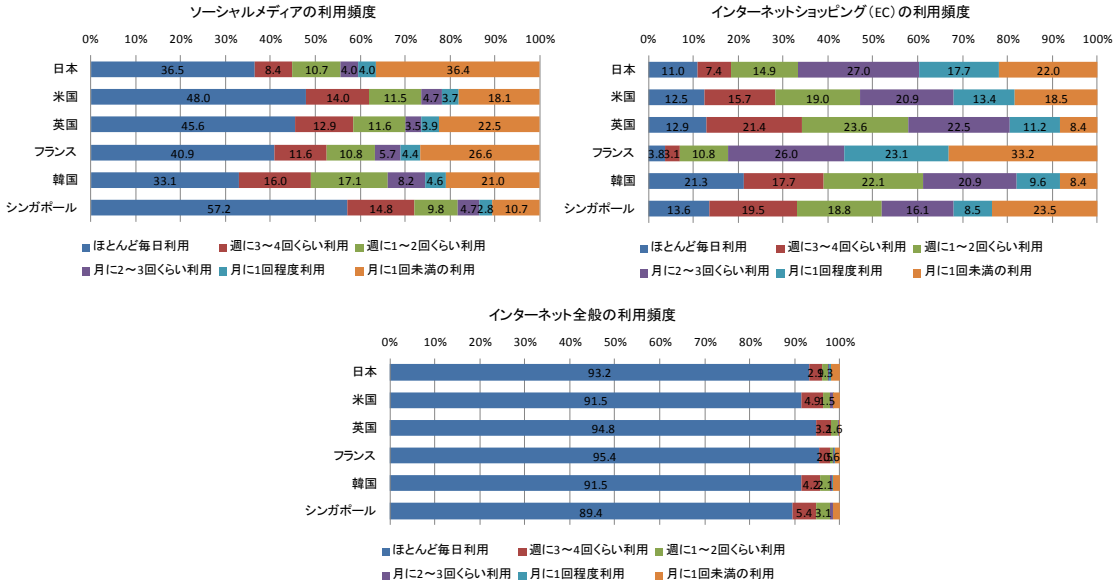
図表 2-6　用途別インターネット利用率

上述のインターネット利用状況においても把握した、EC（インターネットショッピング）における購買品目の結果を下記に示す。この結果によると、日本では、「書籍、CD、DVD、ブルーレイディスク」、「食料品」、「化粧品・衣料品・アクセサリー類」の順で利用率が高く、生活用品をインターネットショッピングで利用している割合が高い。



図表 2-7　インターネットショッピングの利用状況

ソーシャルメディア、インターネットショッピング、インターネット全般の利用頻度を下記に示す。この結果によると、シンガポールでは、57.2%がソーシャルメディアをほぼ毎日利用している。インターネットショッピングの利用頻度は各国でばらつきがみられる。フランスの利用頻度は他の国と比較してやや少ない。



図表 2-8　各種インターネットサービスの利用頻度

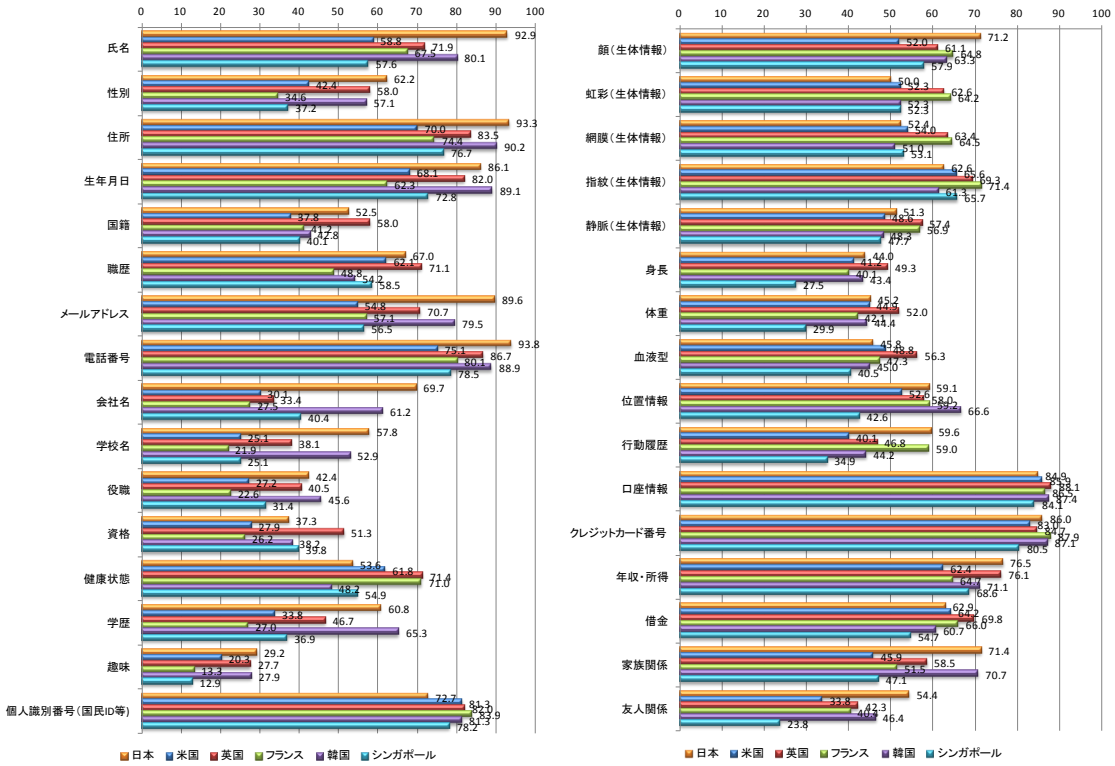
2.3　インターネット上における消費・利用の変化がもたらす課題に関する意識調査

インターネット上における消費・利用に係る課題について調査・分析を行う。具体的には、深刻さを増す情報セキュリティなどの安全対策に係る課題や、ビッグデータの利活用等の進展に伴う個人情報の取扱いなどプライバシーに係る国際的な課題をはじめ、各種課題について利用者の意識や個人の対策状況について調査を実施した。

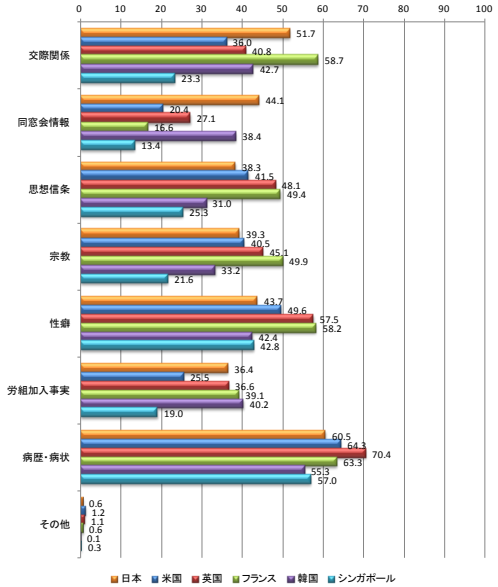
2.3.1　パーソナルデータの取扱いに関する利用者意識

保護されるべきパーソナルデータの範囲として、現行の個人情報保護法では「特定の個人を識別することができるもの」と定義されているが、その中には氏名のように昨今はソーシャルメディア上でも一般的には公開されている情報から、人に知られたくない情報まで、プライバシー性には違いがある。本調査では、保護されるパーソナルデータについて利用者の意識を尋ね、その結果に関し、「一般パーソナルデータ（プライバシー性が高くないパーソナルデータ）」、「慎重な取扱いが求められるパーソナルデータ（プライバシー性が高いパーソナルデータ）」、「センシティブデータ（プライバシー性が極めて高いパーソナルデータ）」の 3 つに区分し、それぞれのデータの取扱いに係る利用者意識の比較を行った。

なお、本調査において、幅広くデータの種類を提示し、対象者がパーソナルデータと認識していると回答した項目は下記の通りである。



図表 2-9　パーソナルデータと認識している情報①

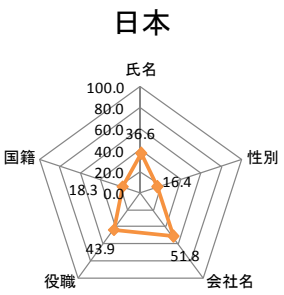


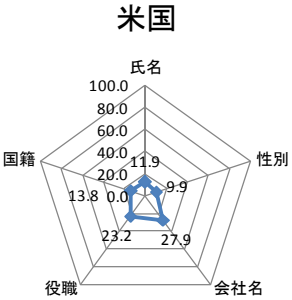
図表 2-10　パーソナルデータと認識している情報②

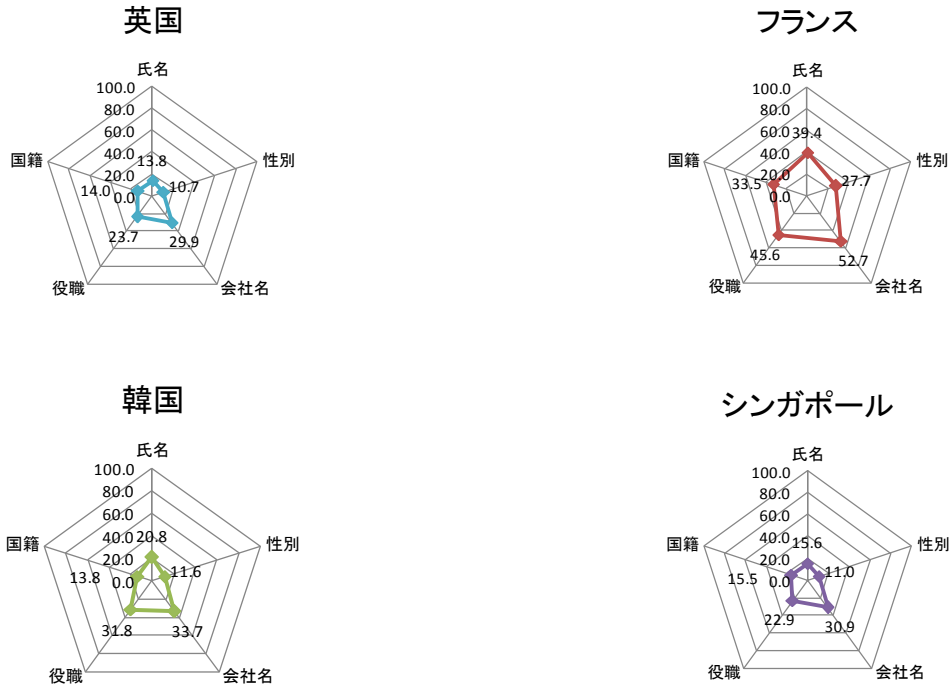
(1)　パーソナルデータの取扱いに係る認識

「一般パーソナルデータ」となる可能性があるものとして、ここでは、氏名、性別、会社名、役職及び国籍の 5 項目について、「当該情報をどんな場合でも提供・公開したくない」と回答した利用者がどの程度あるかをまとめた結果は下記の通りである。

この結果によると、全般的に「どんな場合でも提供・公開したくない」と回答した割合は低く出ているが、フランスは他国と比較した場合、「どんな場合でも提供・公開したくない」との回答が高く出る結果となっている。レーダーチャートの形状が各国とも類似している点も特徴として挙げられる。



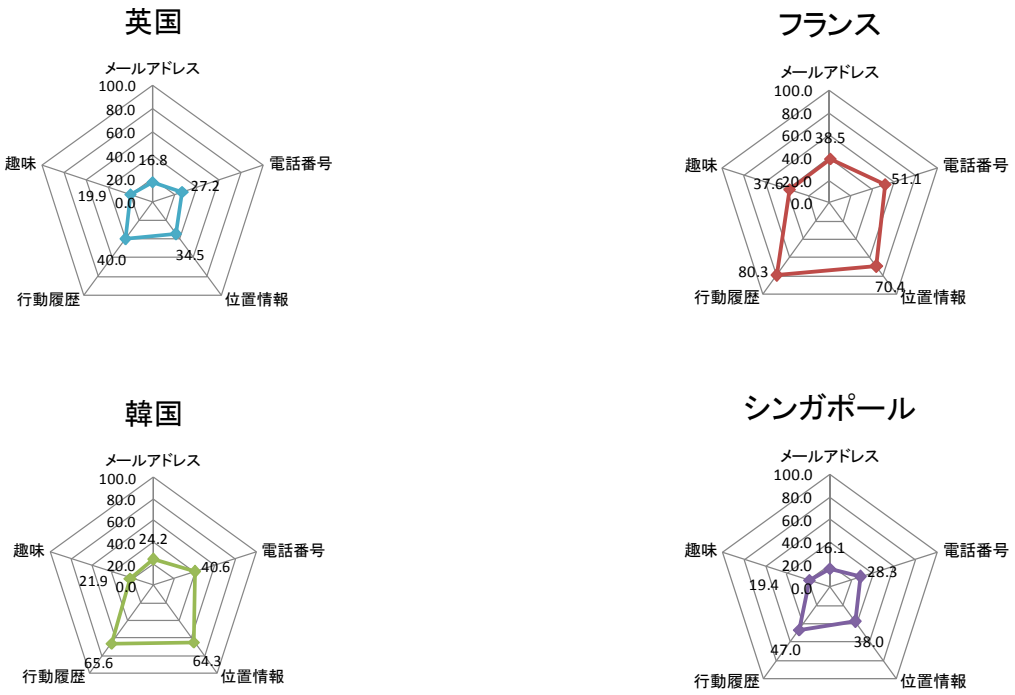




図表 2-11　どのような場合でも提供・公開したくないデータ
（一般パーソナルデータ）

「慎重な取扱いが求められるパーソナルデータ」として、メールアドレス、電話番号、位置情報、行動履歴及び趣味の 5 項目について、「当該情報をどんな場合でも提供・公開したくない」と回答した利用者がどの程度存在するかについて比較を行った。

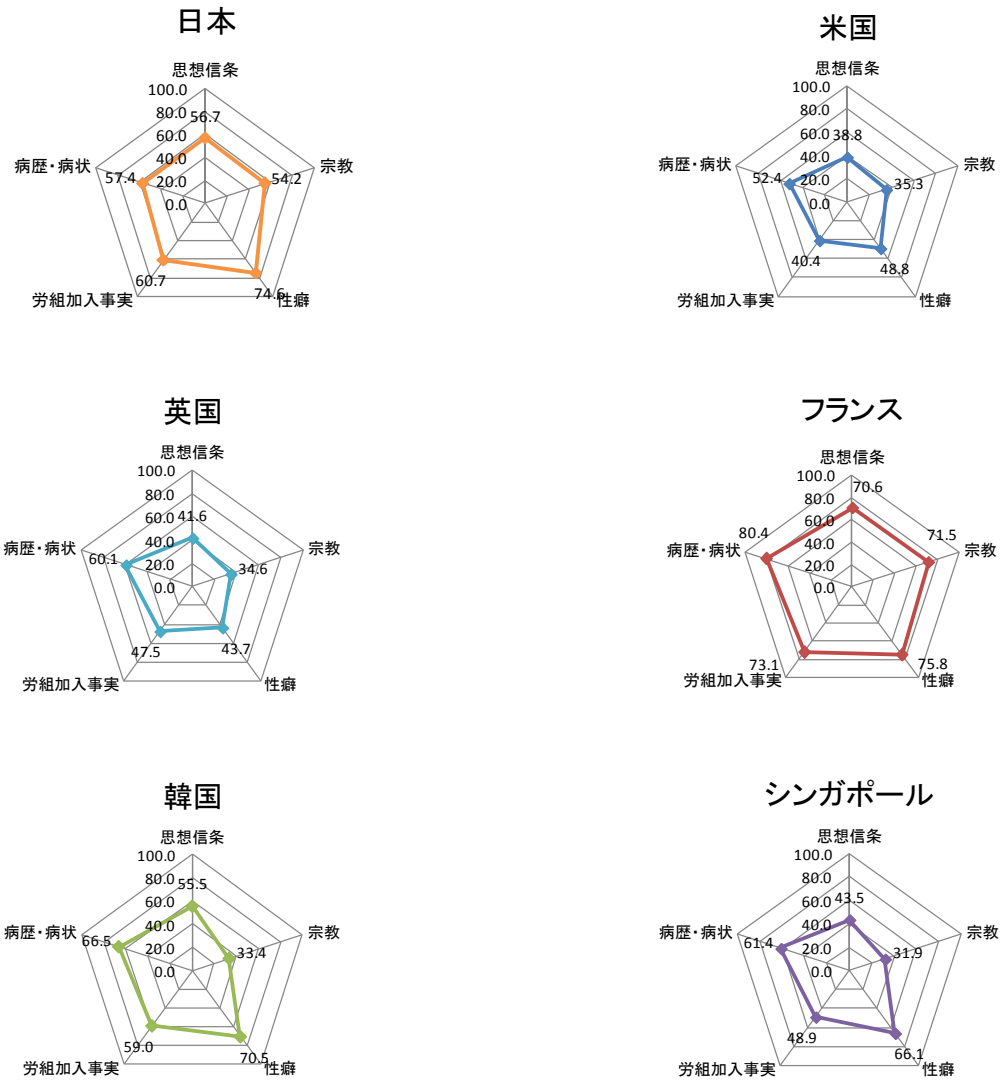
いずれの国でもメールアドレスや趣味については、「どんな場合でも提供・公開したくない」との回答は比較的低く出ているのに対し、位置情報、行動履歴については、比較的高く出ている。日本、フランス及び韓国では、「どんな場合でも提供・公開したくない」との回答が他の 3 か国より高く出る結果となっている。また、レーダーチャートの形状が各国とも類似している点についても、一般パーソナルデータの結果と同様である。



図表 2-12　どのような場合でも提供・公開したくないデータ
（慎重な取扱いが求められるデータ）

さらに、「センシティブデータ」として、ここでは思想信条、宗教、性癖、労組加入事実及び病歴・病状の 5 項目について、「当該情報をどんな場合でも提供・公開したくない」と回答した利用者がどの程度存在するかについて比較を行った。「センシティブデータ」は他のデータに比べて、どの国でも「どんな場合でも提供・公開したくない」と回答した割合は高めに出ている。

また、米国や英国ではいずれの項目も比較的低く出ているのに対し、フランスではいずれの項目も比較的高く出る傾向は、一般パーソナルデータ及び慎重な取扱いが求められるパーソナルデータの場合と同様である。5 項目の中で比較すると、米国、英国及びフランスでは病歴・病状を「どんな場合でも提供・公開したくない」と回答した割合が他の項目と比べて高いのに対し、日本、韓国及びシンガポールでは性癖が最も高い結果となった。



図表 2-13　どのような場合でも提供・公開したくないデータ
（センシティブデータ）

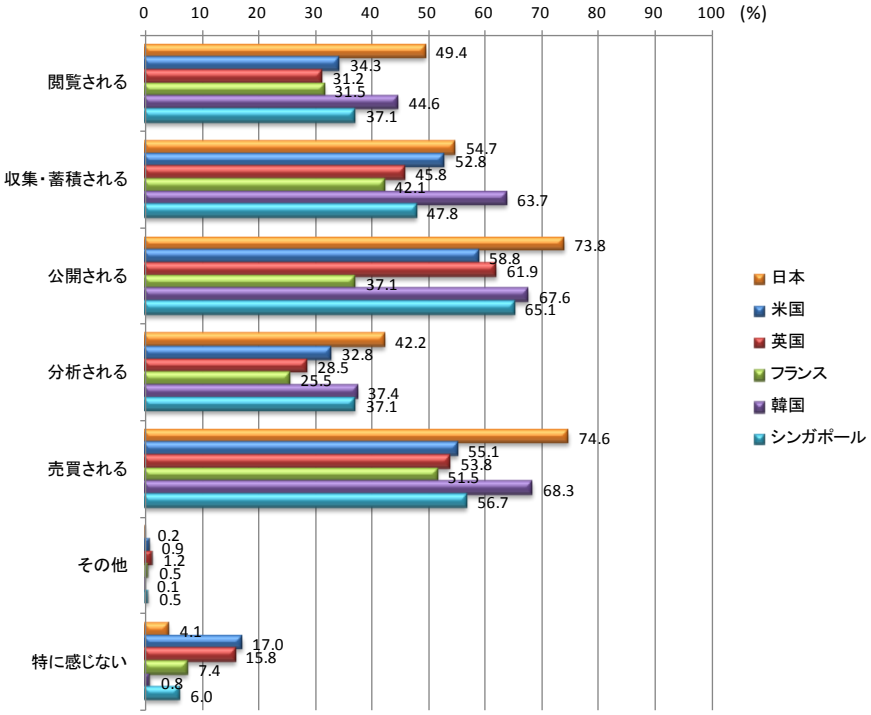
(2)　サービス提供事業者の利用方法に対する利用者の意識

サービス提供事業者からサービス利用者に対し、サービス向上等を理由にパーソナルデータの利用を求められた場合、どのような利用方法に対して抵抗感を感じるかについて、6か国で比較を行った。

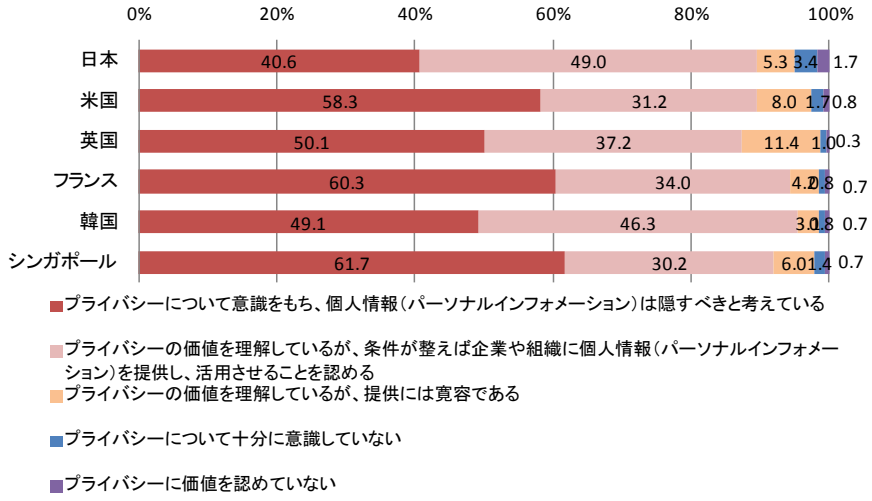
結果、日本では、閲覧、収集・蓄積、公開、分析、売買等、いずれの利用方法においても、他の国と比較すると「抵抗を感じる」という回答の割合が高い。特に欧米と比較すると、様々な行為に対して抵抗を感じるという結果となっている。

パーソナルデータについて、回答者自身の考え方を見ると、日本は「プライバシーにつ

いて意識を持ち、個人情報は隠すべきと考えている」という回答が他の国と比較して約 1 割程度低い。



図表 2-14　サービス提供事業者によるパーソナルデータの利用方法のうち、抵抗感を感じる方法

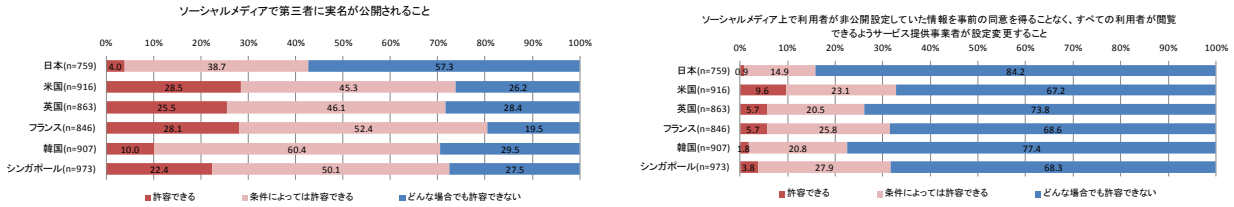


図表 2-15　パーソナルデータの利用・取扱いの考え方で最も近いもの

(3) パーソナルデータの取扱いに関する許容範囲

＜ソーシャルメディア利用の際のパーソナルデータの取扱いに関する意識＞

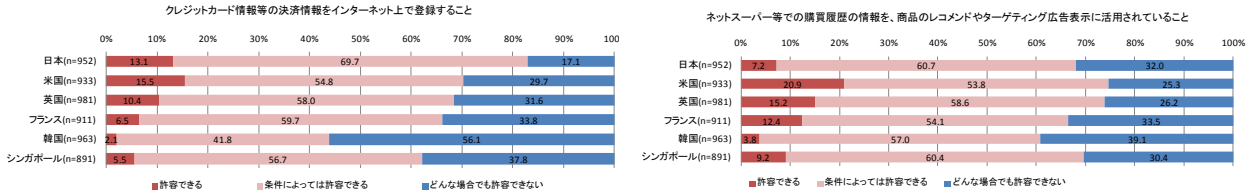
「ソーシャルメディアで第三者に実名が公開されること」については、日本が他の 5 か国より抜きん出て「どんな場合でも許容できない」との回答が高い結果となった。「ソーシャルメディア上で利用者が非公開設定していた情報を事前の同意を得ることなく、サービス提供事業者がすべての利用者が閲覧可能なように設定変更すること」については、いずれの国でも「どんな場合でも許容できない」との回答が高い結果となった。



図表 2-16　パーソナルデータの取扱いに関する許容範囲（ソーシャルメディア利用時）

＜インターネットショッピングを利用する際に登録したパーソナルデータの取扱いに関する意識＞

「クレジットカードの決済情報をインターネット上で登録すること」については、韓国では 56.1%が「どんな場合でも許容できない」と答えたのに対し、日本では 17.1%にとどまっている。また、購買履歴を商品のレコメンドやターゲティング広告表示に活用することについては、いずれの国も 3 割前後が「どんな場合でも許容できない」との回答であった。



図表 2-17　パーソナルデータの取扱いに関する許容範囲（インターネットショッピング利用時）

＜ビッグデータ関連サービスへの意識＞

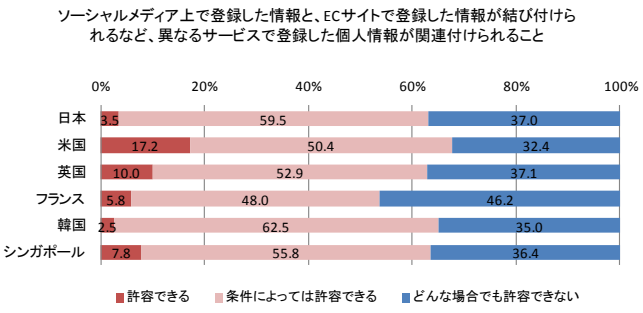
ビッグデータ関連サービスに対する利用者の意識を尋ねた結果を下記に示す。この結果によると、異なるサービスで登録されたパーソナルデータが関連づけられることについては、どの国も 4 割前後の利用者が、また、会員登録サービスにパーソナルデータを登録した場合、別のサービス提供事業者が当該データを利用することについては、5 割前後の利用者が「どんな場合でも許容できない」としている。そして、フランスでは「許容できない」の割合が、他の国より高く出ている。

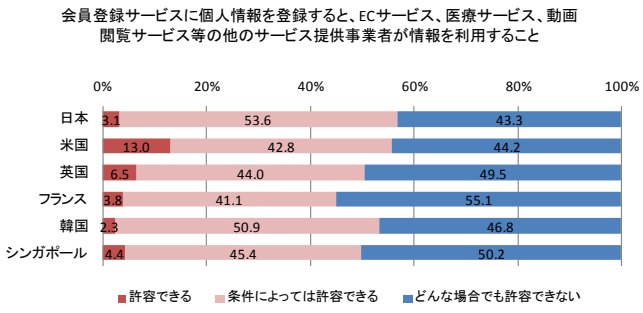
「取得した位置情報をもとに近隣のお勧め情報がスマートフォン等の携帯端末に通知されること」は、アジア圏では「許容できる」、「条件によっては許容できる」といった回答が半数を占める結果となった。

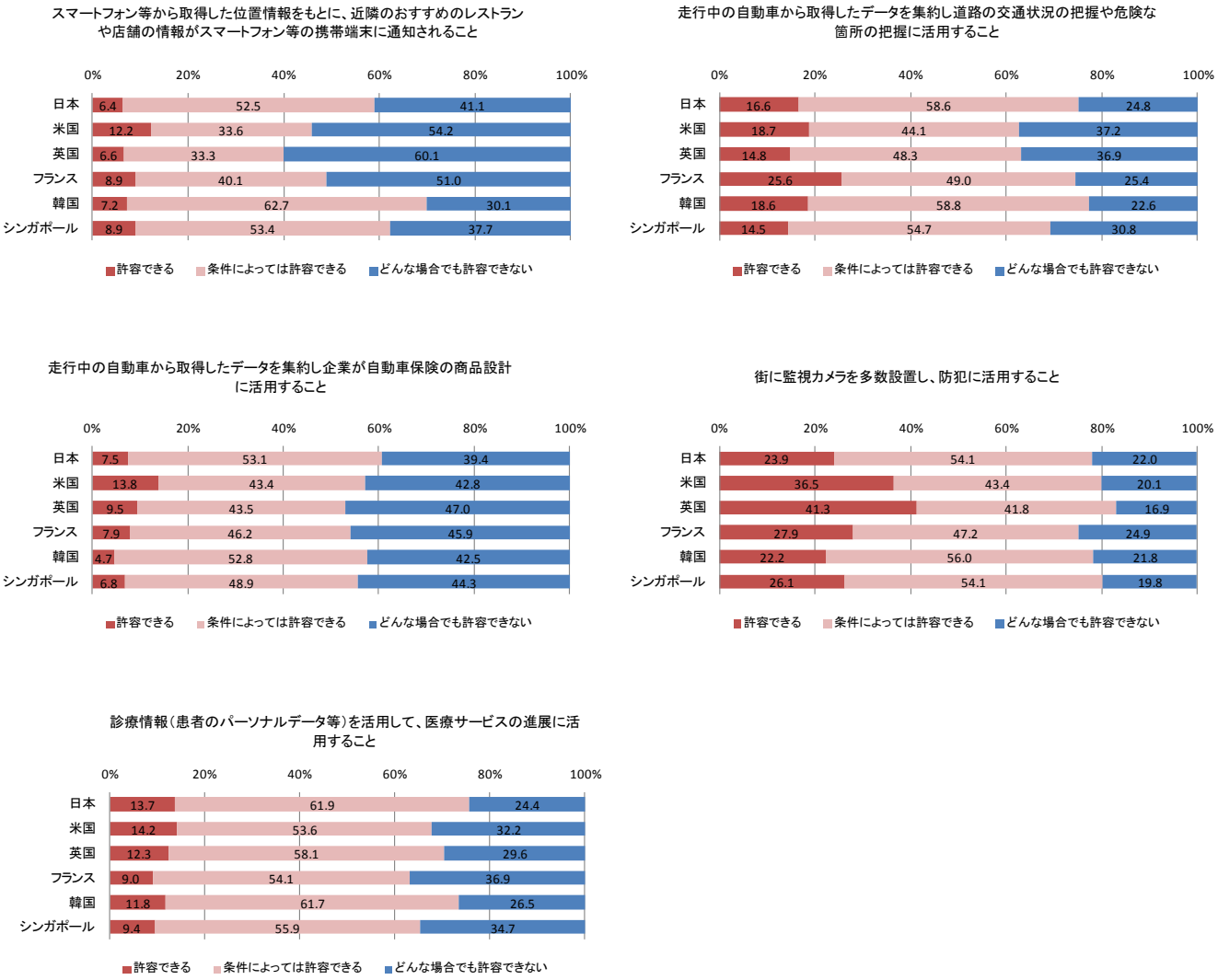
「走行中の自動車から取得したデータを集約し交通状況の把握や危険な箇所の把握に活用すること」については、いずれの国も 6 割以上が「許容できる」、「条件によっては許容できる」と回答したが、「走行中の自動車から取得したデータを集約し企業が自動車保険の設計に活用すること」については、それをやや下回る結果となっている。

「街に監視カメラを多数設置し、防犯に活用すること」については、いずれの国も 8 割前後が「許容できる」、「条件によっては許容できる」と回答している。現時点で監視カメラの設置が進んでいる英国では「許容できる」の割合が他国と比較してやや高いことも特徴である。

「診療情報（パーソナルデータ）を医療サービスの進展に活用すること」については、いずれの国も 6 割以上が「許容できる」、「条件によっては許容できる」と回答している。このように具体的な利用イメージがあり、かつ、特に安心・安全の観点から利用者にとってメリットがあると思われる利用方法については、利用者の抵抗感は小さいという結果がうかがえる。





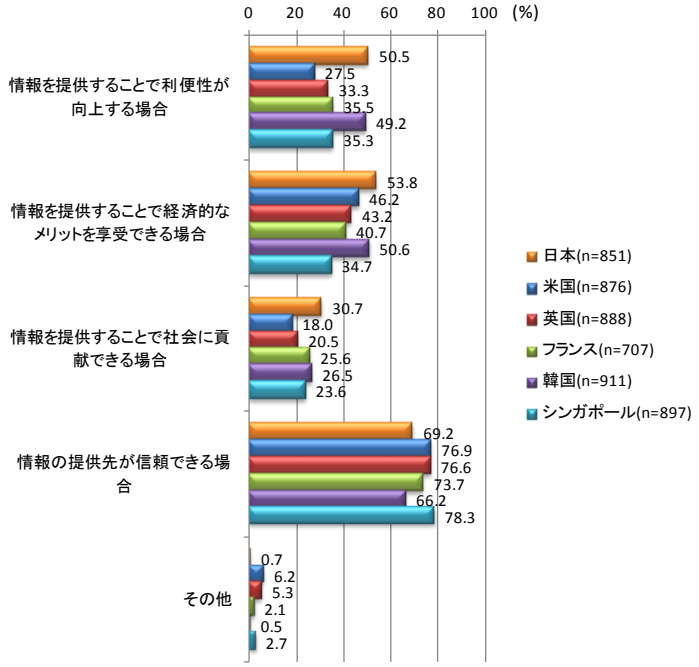


図表 2-18　パーソナルデータの取扱いに関する許容範囲（ビッグデータ関連サービス）

(4)　サービス提供事業者にパーソナルデータを提供する条件

パーソナルデータをサービス提供事業者に提供する条件を尋ねたところ、全体的な傾向としては「情報の提供先が信頼できる場合」であれば提供しても良いという回答がいずれの国においても高い結果になった。

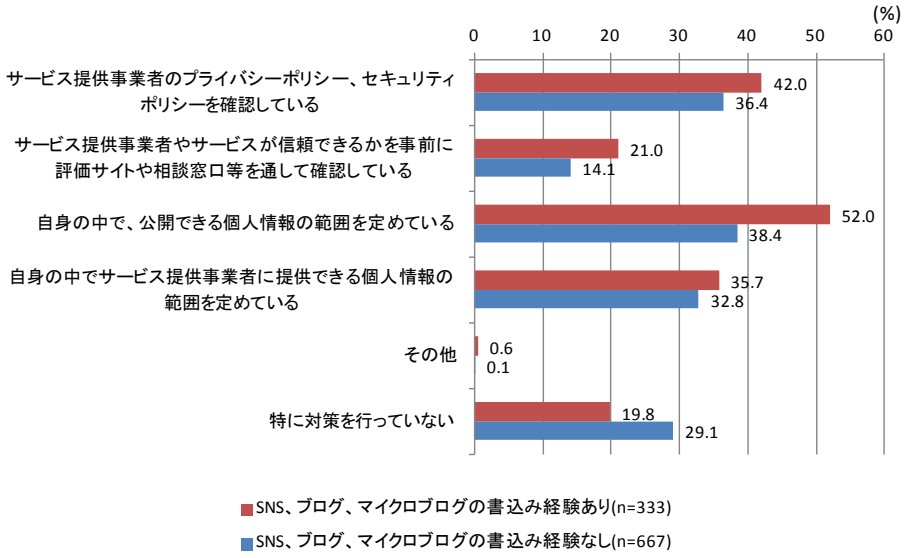
国ごとに比較すると、日本では、「情報を提供することで経済的なメリットを享受できる場合」と「情報を提供することで利便性が向上する場合」が回答の 5 割を超えて高いという特徴が見られる。なお、この傾向は韓国も類似している。



図表 2-19　パーソナルデータをサービス提供事業者に提供する条件

(5)　パーソナルデータ保護のための対策の実施状況

パーソナルデータの保護のために日常から対策を講じているか否かについて日本の利用者に限って、SNS、ブログ及びマイクロブログへの書き込み経験の有無により、どの程度差が生じるか分析を行った。その結果、これらへの書き込み経験を有する利用者は経験を有しない利用者に比べ、いずれの対策についても、「講じている」と回答した割合が高く出る結果となった。

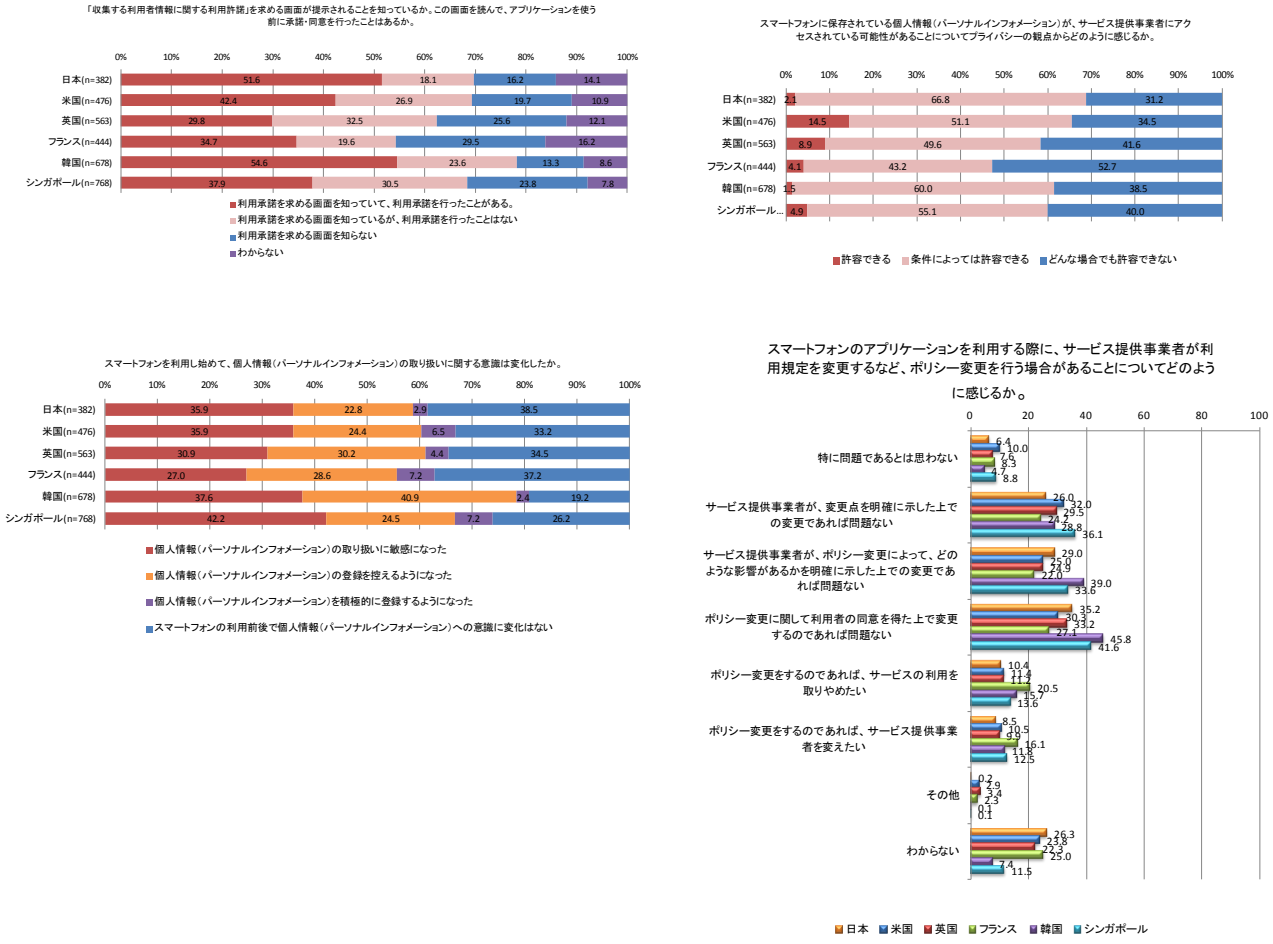


図表 2-20　パーソナルデータ保護のために日常から講じている対策

(6) スマートフォンにおける利用者情報収集に関する意識

スマートフォン利用者におけるパーソナルデータの取扱いに関わる意識について尋ねた結果は下記の通りである。利用承諾を求める画面の認知度（「利用承諾を求める画面を知っていて、利用承諾を行ったことがある」、「利用承諾を求める画面を知っているが、利用承諾を行ったことはない」）は、韓国が 78.2%、日本は 69.7%と高かったのに対し、フランスは 54.3%とやや低い結果が出た。スマートフォンに保存されている利用者情報がサービス提供事業者からアクセスされることについては、いずれの国でも 3 割以上が「どんな場合でも許容できない」と回答している。

スマートフォンを利用するようになって、利用者情報への意識に変化があったかを聞いたところ、韓国やシンガポールでは「取扱いに敏感になった」、「登録を控えるようになった」との回答の合計が 6 割を超える結果となった。日本を含め他の国でも 5 割を超えている。スマートフォンのアプリ利用時にサービス提供事業者がポリシー変更を行うことについては、日本を含む 5 か国では「利用者の同意を得た上で変更するならば問題ない」との回答が最も高くなったが、米国は「サービス提供事業者が変更点を明確にすれば問題ない」との回答が最も高い結果となった。

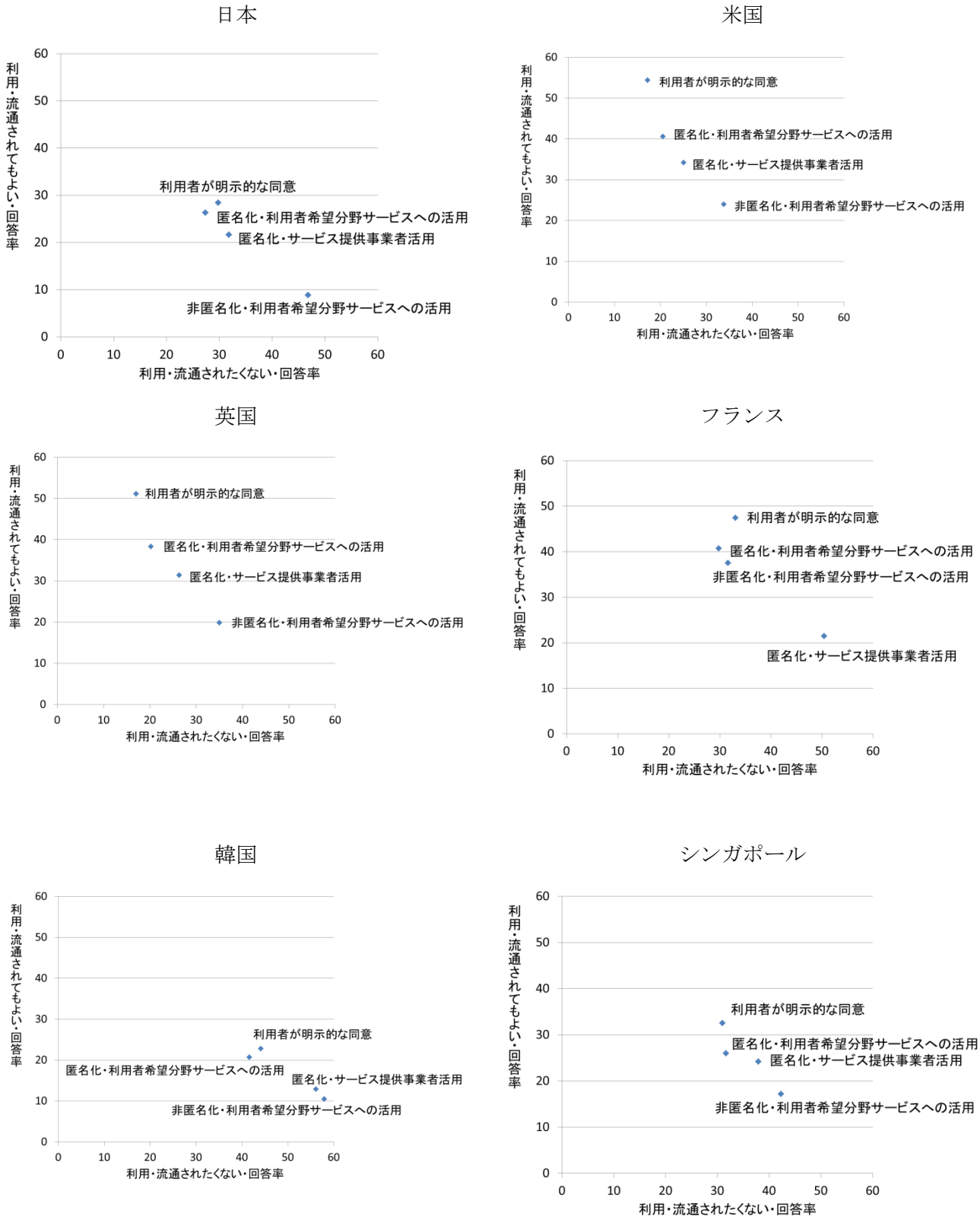


図表 2-21　スマートフォンにおける利用者情報の取扱いに関する意識

(7) パーソナルデータの利用・流通のための条件

パーソナルデータの利用・流通のための条件について、「利用者が明示的な同意を行った場合」、「サービス提供事業者が匿名化を行った場合」、「サービス提供事業者が匿名化を行った上で、利用者が希望する分野・サービスに限って活用する場合」、「利用者が希望する分野・サービスにおいて、匿名化を行わない場合」の 4 つの条件について、パーソナルデータの利用・流通を認めるかを各国の利用者に尋ねた結果を下記に示す。下記の図は、「利用・流通されても良い」の回答率と「利用・流通されたくない」の回答率を示している。

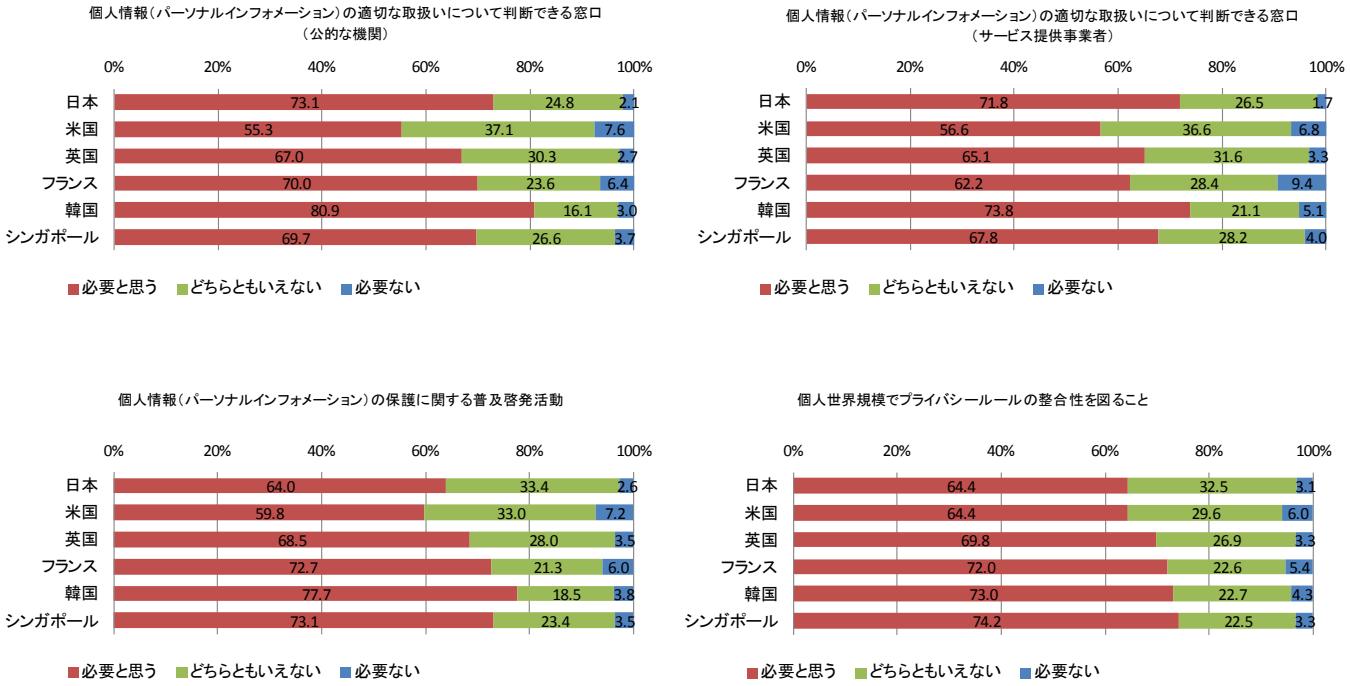
この結果によると、いずれの国も「利用者が明示的な同意を行った場合」では、「利用・流通されても良い」回答率が最も高くなる結果となった。ただし、欧米では 5 割前後に達するのに対し、アジアでは 3 割程度にとどまった。また、フランス以外の対象国では、「サービス提供事業者が匿名化を行った上で、利用者が希望する分野・サービスに限って活用する場合」、「サービス提供事業者が匿名化を行った場合」の順に「利用・流通されても良い」回答率が高くなる結果となったのに対し、フランスでは「サービス提供事業者が匿名化を行った場合」より「利用者が希望する分野・サービスにおいて、匿名化を行わない場合」の方が「利用・流通されても良い」回答率が高い結果となった。



図表 2-22　パーソナルデータの利用・流通のための条件

(8) プライバシー保護のために必要と思う政策

プライバシー保護のために必要と思う政策について各国の利用者に尋ねた結果を下記に示す。この結果によると、「公的な機関またはサービス提供事業者における個人情報の適切な取扱いを判断できる窓口の設置」、「個人情報の保護に関する普及啓発活動」、「世界規模でプライバシールールの整合性を図ること」のいずれにおいても、「必要であると思う」との回答が最も高くなった。



図表 2-23　プライバシー保護のために必要と思う政策

(9) まとめ

①国民のパーソナルデータの範囲の認識

日本では、プライバシー侵害の経験を有する回答者は約 2 割で、パーソナルデータを保護するために日常から対策を実施している割合も低い。一般パーソナルデータ、慎重な扱いが求められるデータ、センシティブデータの国民の認識を見ると、日本では氏名よりも会社名の方が「どんな場合でも提供・公開したくない」という回答が多い。位置情報、行動履歴、年収・所得ではフランスが情報の取り扱いに慎重な傾向である。性癖は、米国、英国では、他の国と比較すると情報の取り扱いに寛容な傾向が見られる。日本では、閲覧、公開、分析、売買等の様々な行為に対して「抵抗を感じる」という回答の割合が高く、どの行為が違反となるかその境界が曖昧な傾向が見られる。

②パーソナルデータを活用することによる便益と影響

パーソナルデータをサービス提供事業者に提供する条件として、全体的な傾向としては「情報の提供先が信頼できる場合」であれば提供しても良いという回答がいずれの国においても多い。情報の提供先の信頼性の向上は必須の要件となる。日本においては、他の国と比較して、「情報を提供することで経済的なメリットを享受できる場合」と「情報を提供することで利便性が向上する場合」が回答の 5 割を超えて高い傾向が見られる。

③プライバシーに関する認識向上によるパーソナルデータ流通の促進

パーソナルデータを取り扱う事業者が、どのような対応をすればパーソナルデータを登録し、利用・流通されても良いかについて尋ねた設問の結果を見ると、欧米と比較するとアジアの回答の割合は低いものの、明示的な同意や匿名化・暗号化をすれば、日本においては、2～3 割の回答者がパーソナルデータを「利用・流通されても良い」 としている。ソーシャルメディアへの書き込みを行った経験のある者は、パーソナルデータの「公開・共有される可能性」、「利用される可能性」、「漏えいされる可能性」に不安を感じて、プライバシーの保護対策を行っている割合が高い。ソーシャルメディアの利用がパーソナルデータの正しい取り扱いや認識に影響を与える可能性は大きいと考えられる。

プライバシー保護対策として必要なこととして、「個人情報の適切な取り扱いについて判断できる窓口の設置（公的な機関）」が最も多く 73.1%となった。他の国についても、公的な機関の窓口の設置について、55～80%の回答者が「必要である」と回答している。

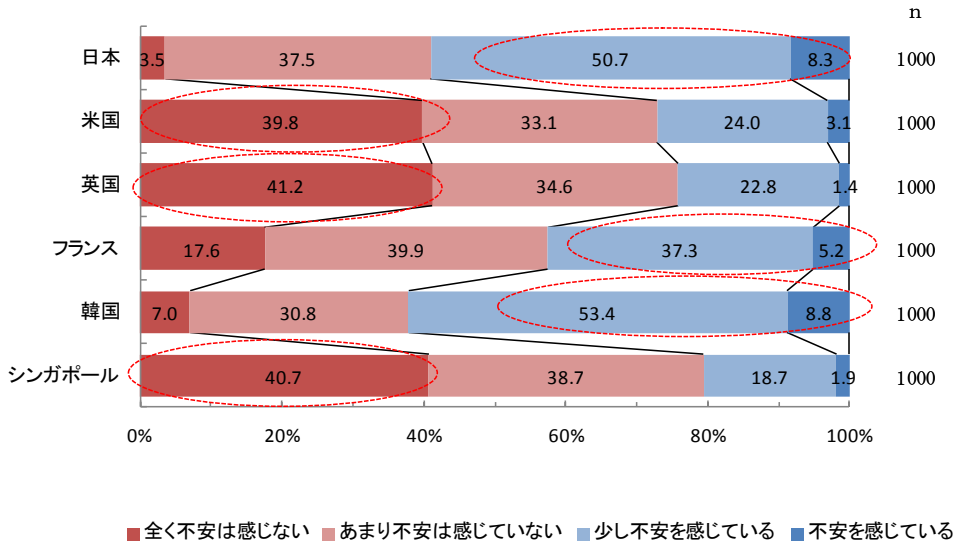
2.3.2　情報セキュリティに係る利用者の意識

日本・米国・英国・フランス・韓国・シンガポールの国別に、情報セキュリティに係る利用者の意識差の把握を目的としてアンケート調査を実施した。以降に結果を示す。

(1) インターネット利用時の不安感

インターネットを利用していて不安を感じているかを尋ねたところ、「不安である」(「少し不安を感じている」＋「不安を感じている」) の回答が高くなった順に、韓国 62.2%、日本 59.0%、フランス 42.5%と続く。

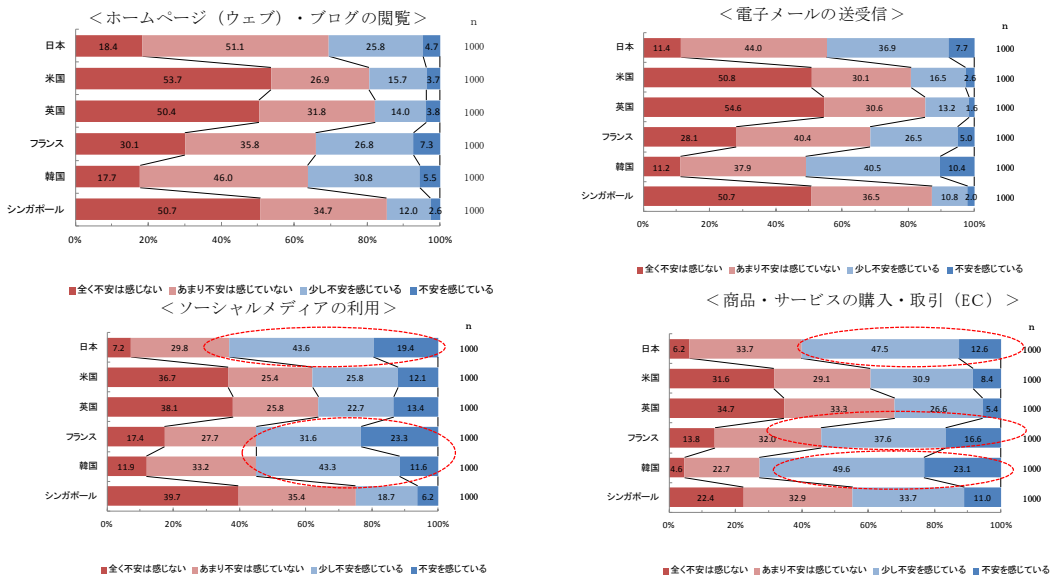
逆に「全く不安を感じない」が高くなったのは、英国 41.2%、シンガポール 40.7%、米国 39.8%となった。



図表 2-24　インターネット利用時の不安感

次に具体的なサービス別に不安感をみる。全回答ベースで「不安である」(「少し不安を感じている」＋「不安を感じている」) の割合が高くなったサービス順に見ると、「商品・サービスの購入・取引」50.5%、「ソーシャルメディアの利用」45.3%、「電子メールの送受信」29.0%、「ホームページ（ウェブ）・ブログの閲覧」25.5%となった。

さらに「不安である」回答割合が最も多くなった「商品・サービスの購入・取引」の国別の傾向をみると、韓国 72.7%、日本 60.1%、フランス 54.2%と続く。次に高くなった「ソーシャルメディアの利用」の国別の傾向をみると日本 63.0%、韓国・フランスがともに 54.9%となった。



図表 2-25　インターネット利用時の不安感（サービス別）

(2) インターネット上の脅威への認知度

インターネットの脅威を例示し回答者が認知しているものがあるかを尋ねた。

各国において認知状況が高くなった脅威を３つあげると、順位の上下はあるが「スパイウェア」、「マルウェア（コンピュータウイルス、以降略）」、「フィッシング詐欺」となった。以降、各国別にみる。

日本では、「フィッシング詐欺」80.4%、「架空請求」75.8%、「スパイウェア」73.4%となった。日本の場合、「架空請求」の認知度が他国よりも高くなったのが特徴的である。

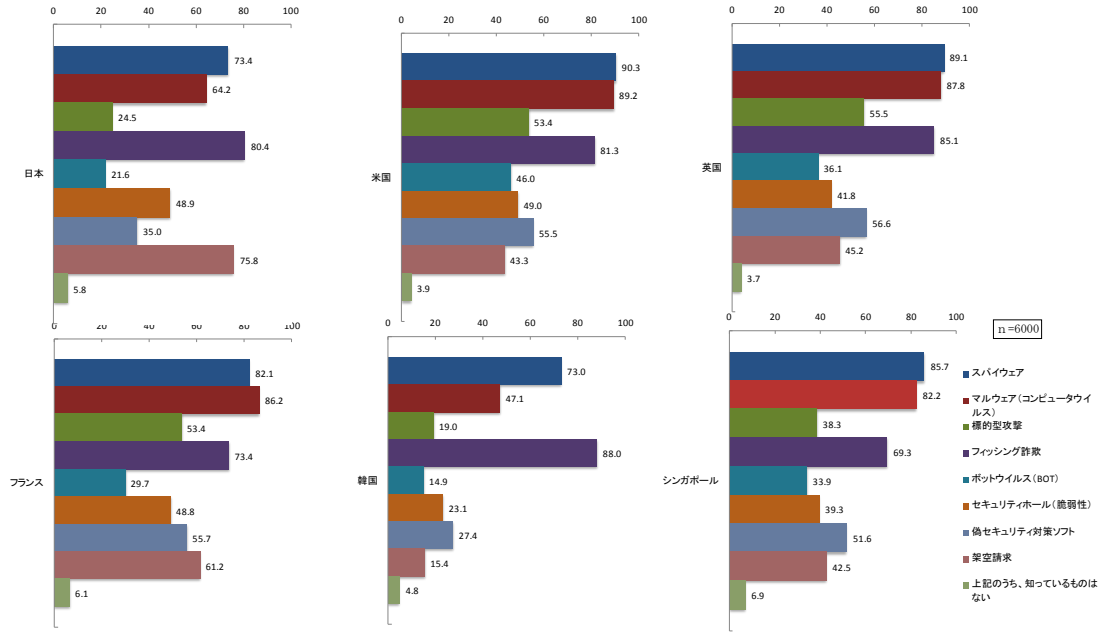
米国では、「スパイウェア」90.3%、「マルウェア」89.2%、「フィッシング詐欺」81.3%となった。

英国では、「スパイウェア」89.1%、「マルウェア」87.8%、「フィッシング詐欺」85.1%となった。米国と同じ順となり、また、それぞれの割合も似ている。

フランスは「マルウェア」86.2%、「スパイウェア」82.1%、「フィッシング詐欺」73.4%。

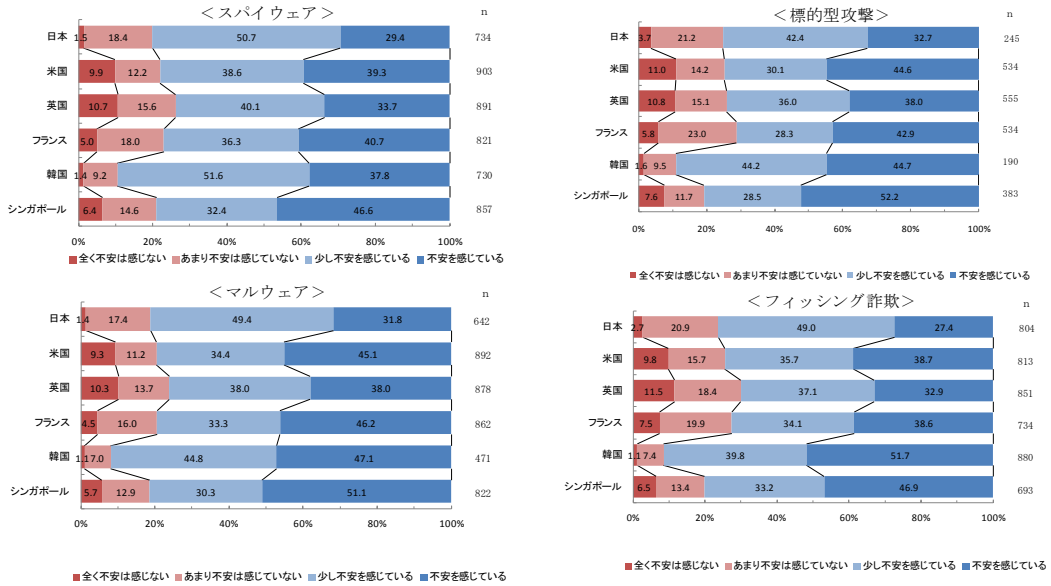
韓国は「フィッシング詐欺」88.0% 、「スパイウェア」73.0%、「マルウェア」47.1% 。

シンガポールでは、「スパイウェア」85.7%、「マルウェア」82.2%、「フィッシング詐欺」69.3%となった。

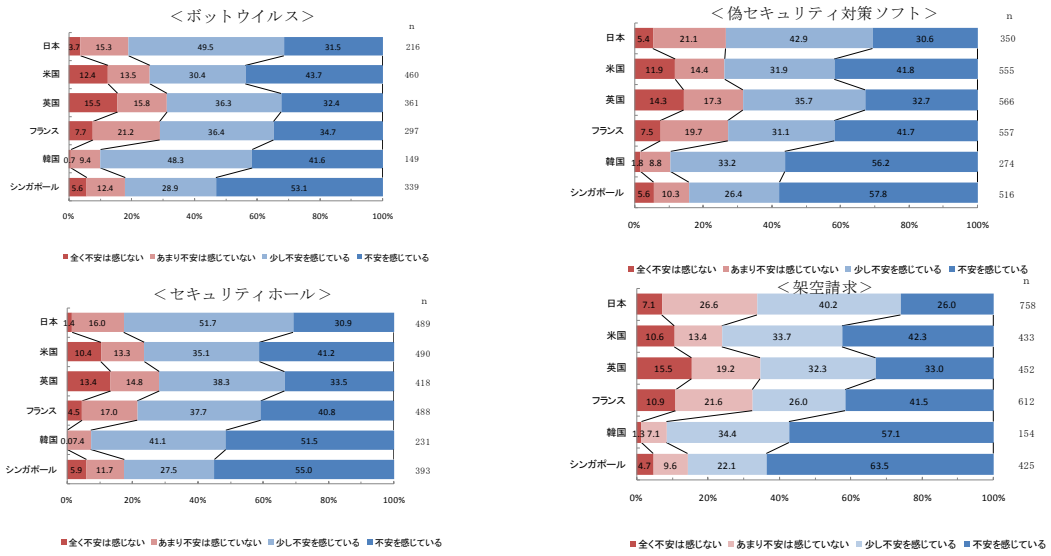


図表 2-26　インターネット上の脅威の認知度

次に各国で認知度が高かった「スパイウェア」、「マルウェア」、「フィッシング詐欺」、さらに日本で高くなった「架空請求」に対する不安感を見る。全般的に脅威として認知しているものに対する不安感は高くなる傾向を示している。特にシンガポールでは「不安を感じている」との回答が他国より高い結果となった。シンガポールでは情報セキュリティ全般に対する漠然とした不安ではなく、具体的な脅威を念頭に置いた上で不安を感じている可能性が高いことがうかがえる。



図表 2-27　インターネット上の脅威への不安（その１）



図表 2-28　インターネット上の脅威への不安（その２）

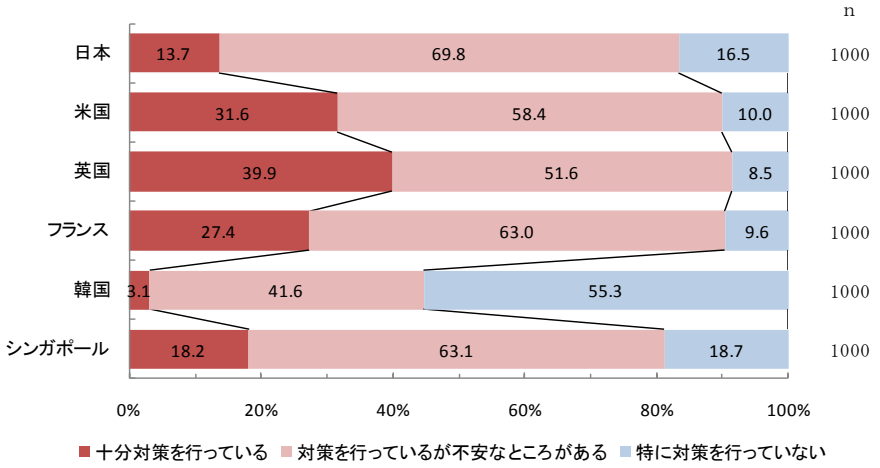
(3)　情報セキュリティ対策の実施状況

情報セキュリティ対策を行っているか否かについて尋ねた。

「十分対策を行っている」が高くなったのは、英国 39.9%、米国 31.6%、フランス 27.4%となった。

逆に「特に対策を行っていない」が高くなったのは韓国で 55.3%となった。

日本は「対策を行っているが不安なところがある」が 69.8%となり、比較対象国中最も高くなった。



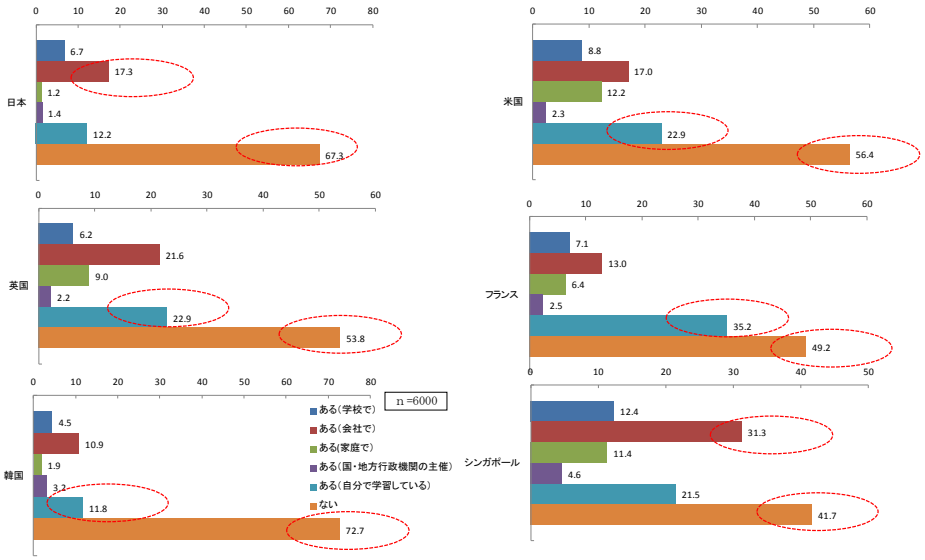
図表 2-29　情報セキュリティ対策の実施状況

(4) 情報セキュリティ教育・研修の受講経験

情報セキュリティ教育・研修の受講経験について尋ねた。

各国とも教育･研修を受けた経験が「ない」が最も高くなった。高くなった順にみると韓国 72.7%、日本 67.3%、米国 56.4%、英国 53.8% 、フランス 49.2% 、シンガポール 41.7%となった。

経験が「ある」場合をみる。「ある（自分で学習している)」が高くなったのは、フランス 35.2%、米国 22.9%、英国 22.9%、韓国 11.8%となった。また、「ある（会社で)」が高くなったのは シンガポール 31.3%、、日本 17.3%となった。



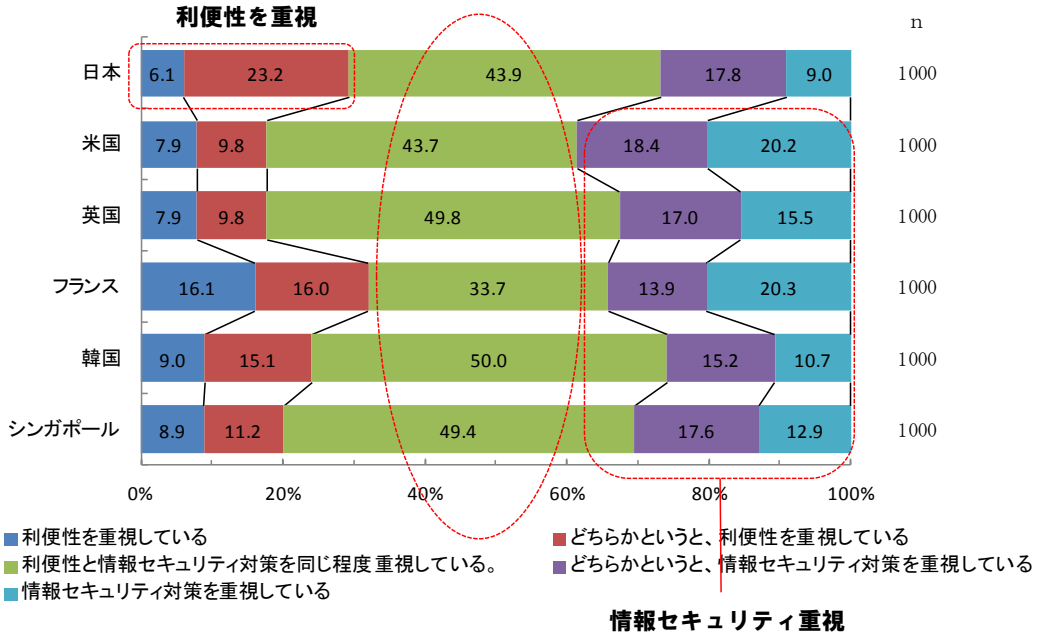
図表 2-30　情報セキュリティ教育・研修の受講経験

(5) 利便性と情報セキュリティ対策のどちらを重視するか

インターネット利用において利便性と情報セキュリティ対策のどちらを重視しているかについて尋ねた。

日本以外の国では「どちらかというと、情報セキュリティ対策を重視している」が高くなった。

各国別に、「利便性を重視」（「利便性を重視している」＋「どちらかというと、利便性を重視している」）と「情報セキュリティ重視」（「どちらかというと、情報セキュリティ対策を重視している」＋「情報セキュリティ対策を重視している」）を比較すると、日本のみ「利便性を重視」（29.3%）の方が高くなった。



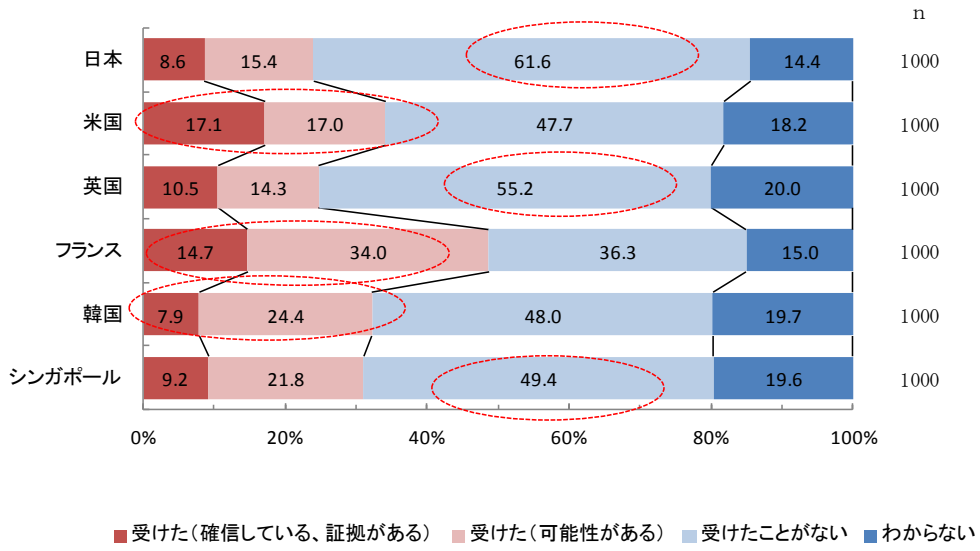
図表 2-31　利便性と情報セキュリティ対策の重視度合い

(6) 情報セキュリティ被害経験

これまでに情報セキュリティ被害の経験があるかについて尋ねた。

「被害を受けた」(「受けた（確信している、証拠がある)」＋「受けた（可能性がある)」)が高くなったのは、フランス 48.7%、米国 34.1%、韓国 32.3%となった。なお、日本は 24.0%で 6 カ国中、最も低くなった。

逆に「受けたことない」との回答が高くなった順にみると、日本 61.6%、 英国 55.2%、シンガポール 49.4%となった。



図表 2-32　情報セキュリティ被害経験

「被害を受けた」(「受けた（確信している、証拠がある)」＋「受けた（可能性がある)」)と回答した人に対して、どのような被害の経験があるについて尋ねた。

ここでは、各国で最も回答が高くなった被害種類をみる。大きくは「コンピュータウイルスの感染」「迷惑メール（スパム）が送られてきた（架空請求メールの受信を除く)」に回答が集中した。

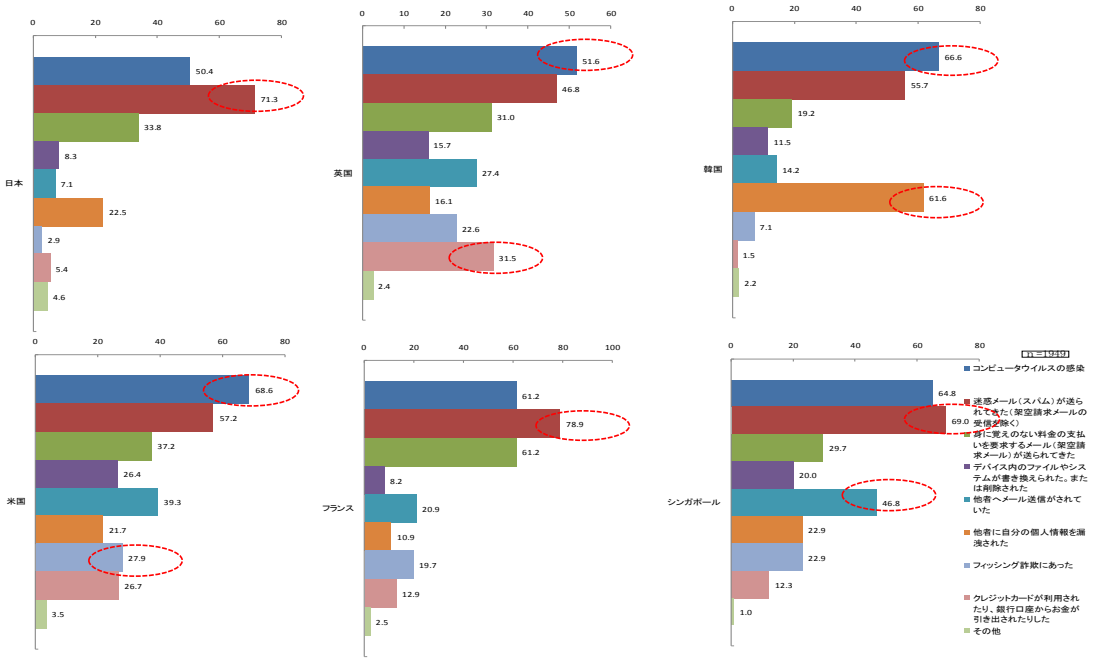
初めに「コンピュータウイルスの感染」が高くなったのは、米国 68.6%、韓国 66.6%、英国 51.6%であった。

次に、「迷惑メール（スパム）が送られてきた（架空請求メールの受信を除く)」が高くなったのは、フランス 78.9%、日本 71.3%、シンガポール 69.0%であった。

逆に、日本で低くなった「フィッシング詐欺にあった 」2.9%は、韓国を除き、一定程度の割合が回答した。最も高くなった米国では 27.9%に上った。

また、「クレジットカードが利用されたり、銀行口座からお金が引き出されたりした 」は、日本では 5.4%であったが、 韓国を除き、一定程度の割合が回答した。 最も高くなった英国では 31.5%と高くなった。

特定国においてのみ目立った回答をみると、韓国で「他者に自分の個人情報を漏洩された」61.6%、シンガポールの「他者へメール送信がされていた」が 46.8%となった。



図表 2-33　情報セキュリティ被害の種類

(7) パソコンの情報セキュリティ対策

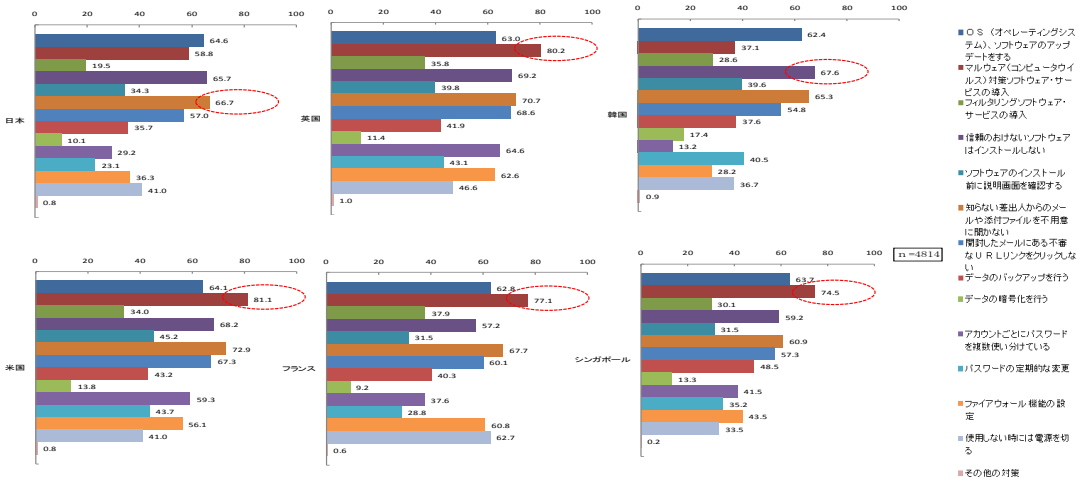
パソコンにどのような情報セキュリティ対策を行っているかについて尋ねた。

各国別に対策取組状況をみる。1 番回答率が高くなった対策に注目すると、3 つに分かれた。

「マルウェア（コンピュータウイルス）対策ソフトウェア・サービスの導入」が多くの国で高くなった。米国 81.1%、英国 80.2%、フランス 77.1%、シンガポール 74.5%となった。

「信頼のおけないソフトウェアはインストールしない」は韓国で 67.6%となった。

「知らない差出人からのメールや添付ファイルを不用意に開かない」が最も高くなったのは日本 66.7%であった。

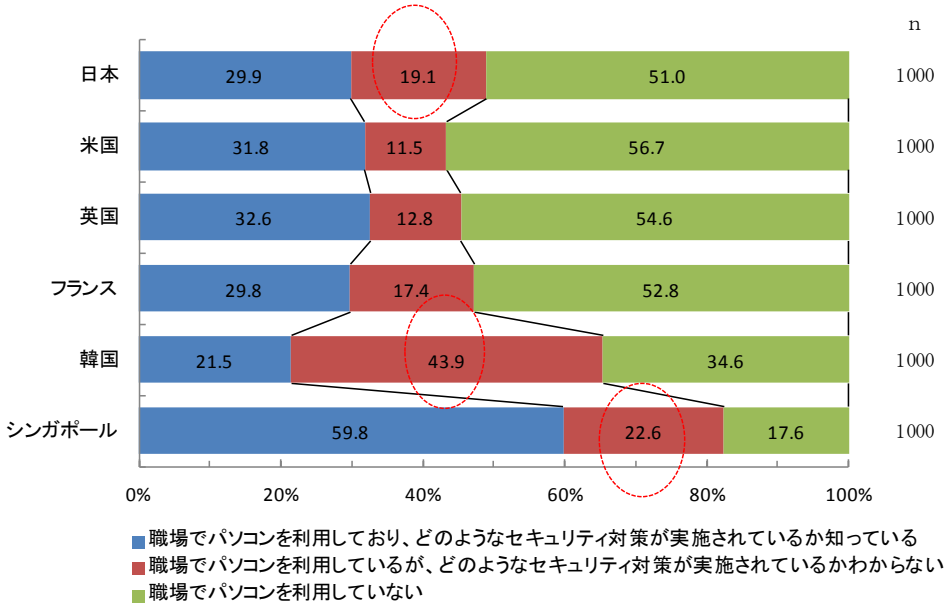


図表 2-34　パソコンへの情報セキュリティ対策

職場でパソコンを利用しているか、さらに利用している場合に職場で支給されているパソコンにどのような情報セキュリティ対策が実施されているか把握しているかについて尋ねた。

「職場でパソコンを利用しているが、どのようなセキュリティ対策が実施されているかわからない」の回答割合が高くなった順に、韓国 43.9%、シンガポール 22.6%、日本 19.1%となった。

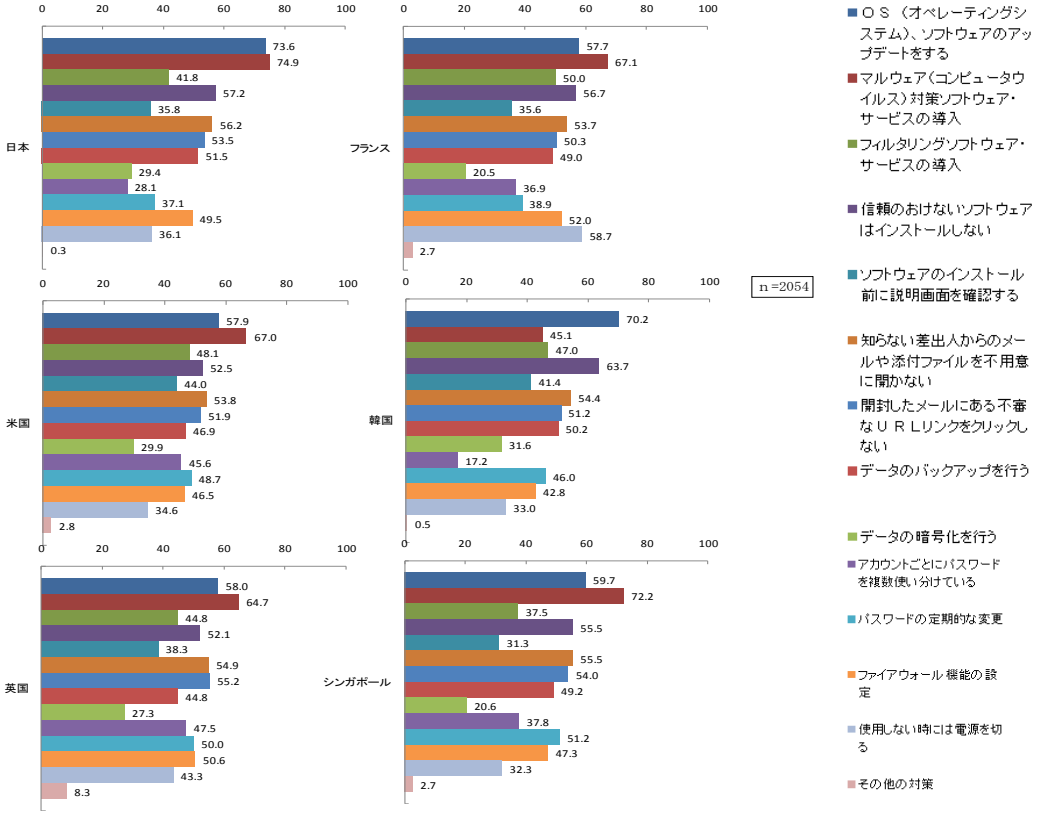
韓国は「職場でパソコンを利用しており、どのようなセキュリティ対策が実施されているか知っている」の回答割合よりも「わからない」が上回っている。



図表 2-35　職場のパソコンのセキュリティ対策の把握

職場のパソコンにどのような情報セキュリティ対策を行っているかについて尋ねた。各国とも「 マルウェア（コンピュータウイルス）対策ソフトウェア・サービスの導入」、「ＯＳ（オペレーティングシステム）、ソフトウェアのアップデートをする」が上位となっている。ただし、韓国では「 マルウェア（コンピュータウイルス）対策ソフトウェア・サービスの導入」は 45.1%と他国よりも低くなっている。また、フランスでは、「使用しない時には電源を切る」58.7%と２番目に高くなっているのが特徴である。

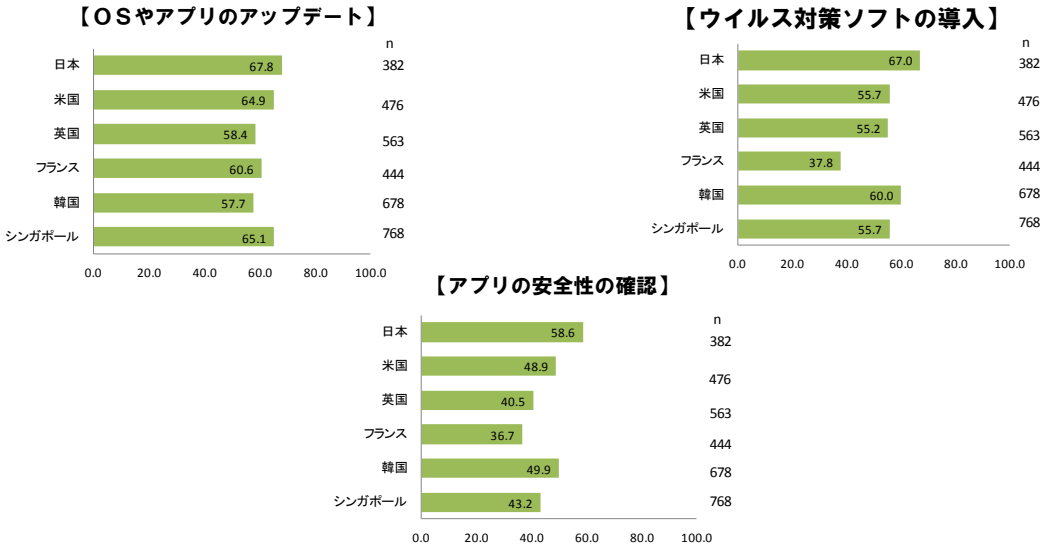
なお、日本では、「 マルウェア（コンピュータウイルス）対策ソフトウェア・サービスの導入」74.9%、「ＯＳ（オペレーティングシステム）、ソフトウェアのアップデートをする」73.6%、「信頼のおけないソフトウェアはインストールしない」57.2%の順で高くなった。



図表 2-36　職場のパソコンに行っているセキュリティ対策

(8)　スマートフォンの情報セキュリティ対策

スマートフォンにおける情報セキュリティ対策については、我が国では「スマートフォンセキュリティ 3 か条」を公表、啓蒙がおこなわれている。本調査で、3 か条に該当する「ＯＳやアプリケーションのアップデート」、「ウイルス対策ソフトの導入」及び「インストールするアプリの安全性の確認」の認知度について尋ねた。その結果、日本は 3 項目全てにおいて回答率が 5 割以上となり、他国より認知度が高くなった。



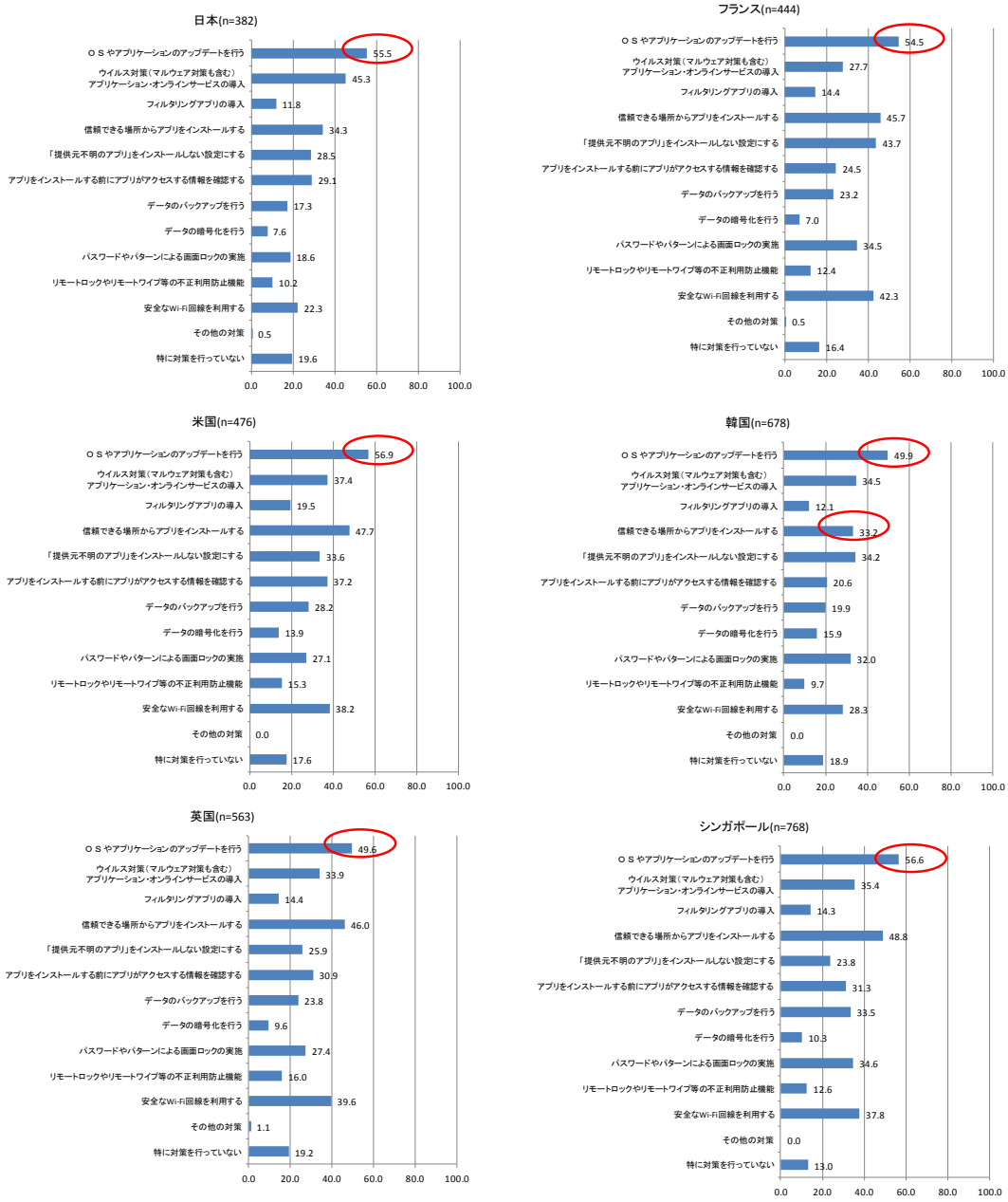
図表 2-37　スマートフォンの情報セキュリティ対策の認知状況

次に、スマートフォンにおける情報セキュリティ対策の実施状況を尋ねた。

各国とも「ＯＳやアプリケーションのアップデートを行う」の回答が高くなり、半数を占めている。

日本をみると、回答が高くなった順に、「ＯＳやアプリケーションのアップデートを行う」55.5%、「ウイルス対策（マルウェア対策も含む）」45.3%、「信頼できる場所からアプリをインストールする」34.3%となった。

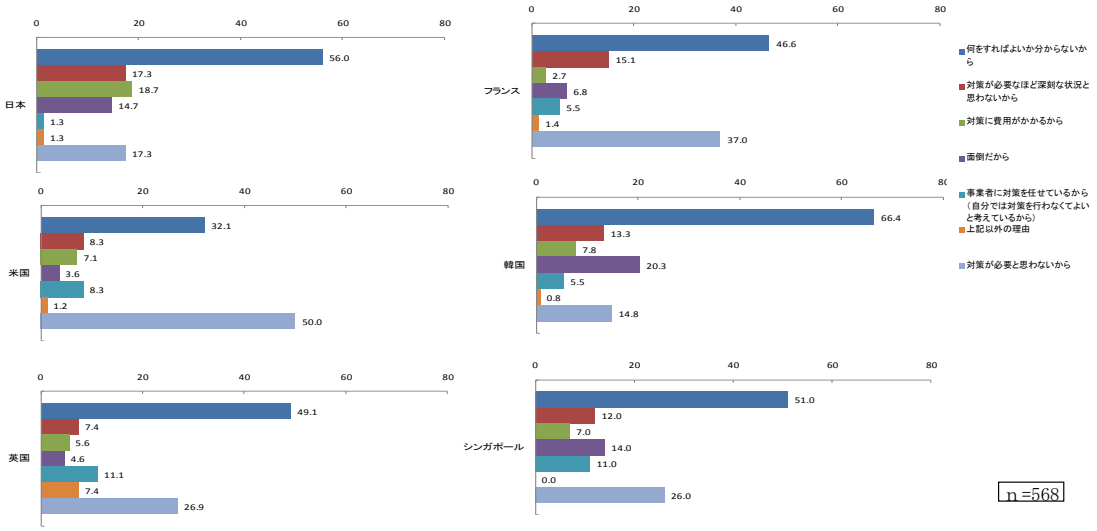
なお、「信頼できる場所からアプリをインストールする」は、米国、英国、フランス、シンガポールでは回答割合が 4 割以上となっており、日本が他国と比較すると低くなっている。同様に韓国も 33.2%と低い。



図表 2-38　スマートフォンの情報セキュリティ対策の実施状況

なお上の設問でスマートフォンの情報セキュリティ対策を行っていない回答者（特に対策を行っていない）に、その理由を尋ねた。各国別にみると米国は「対策が必要と思わないから」が 50.0%となった。

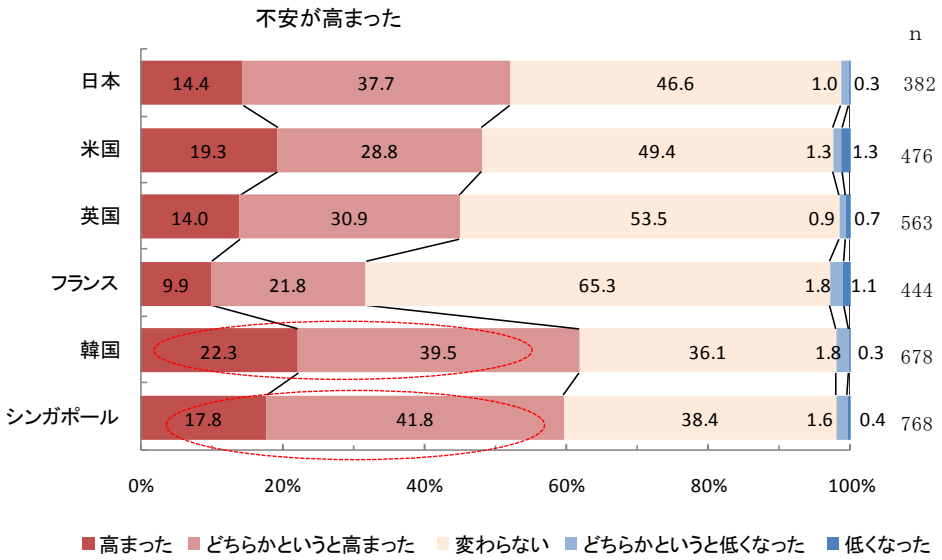
米国以外の国では、「何をすればよいか分からないから」が高くなった。高くなった順に韓国 66.4%、日本 56.0%、シンガポール 51.0%、英国 49.1%、フランス 46.6%となった。



図表 2-39　スマートフォンのセキュリティ対策を行わない理由

なお、スマートフォンを利用するようになって情報セキュリティへの不安が高まったか否かについて尋ねた。「不安が高まった」（「高まった」＋「どちらかというと高まった」）が高くなったのは、韓国 61.8%とシンガポール 59.6%であった。

なお、日本は「不安が高まった」が 52.1%となり、調査対象国中 3 番目に高くなった。



図表 2-40　スマートフォンを利用するようになってからの情報セキュリティへの不安

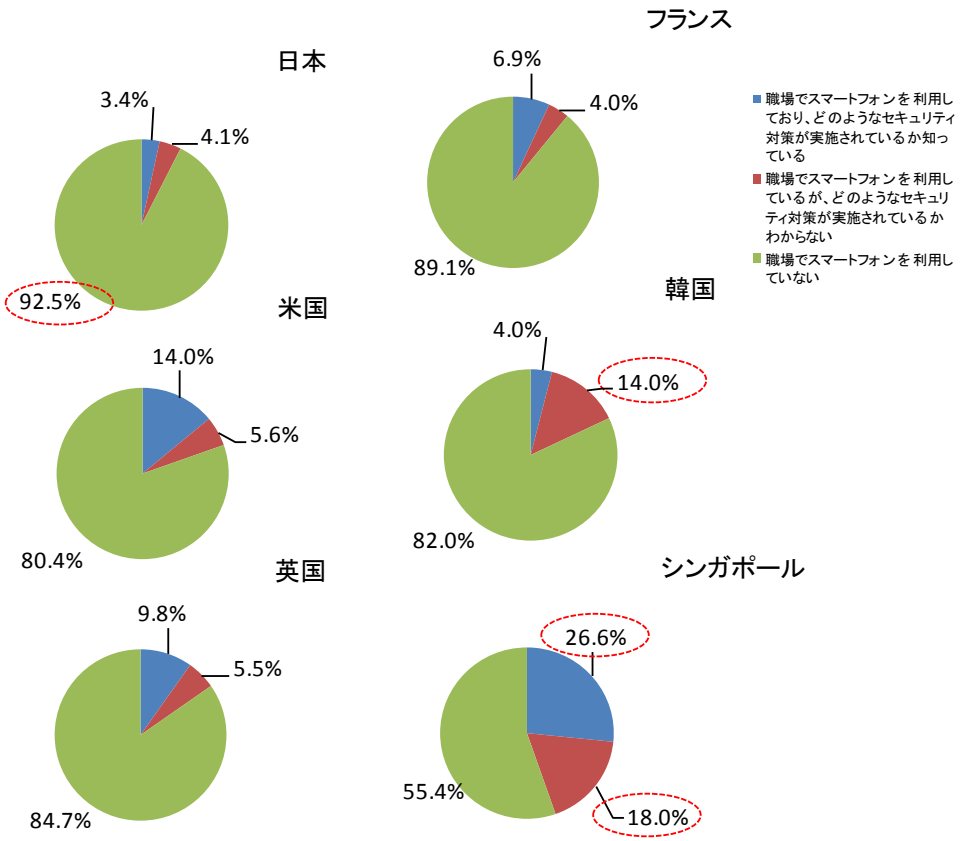
職場でスマートフォンを利用しているか、さらに利用している場合は、職場で支給されているスマートフォンにどのような情報セキュリティ対策が実施されているかを把握して

いるかを尋ねた。

結果、「職場でスマートフォンを利用しているが、どのようなセキュリティ対策が実施されているか分からない」の回答割合が他国よりも高くなったのは、韓国 14.0%、シンガポール 18.0%であった。

なお、シンガポールでは、「職場でスマートフォンを利用しており、どのようなセキュリティ対策が実施されているか知っている」が 26.6%となり、他国よりも高くなった。

日本は「職場では利用していない」が 92.5%となり、他国よりも高くなった。

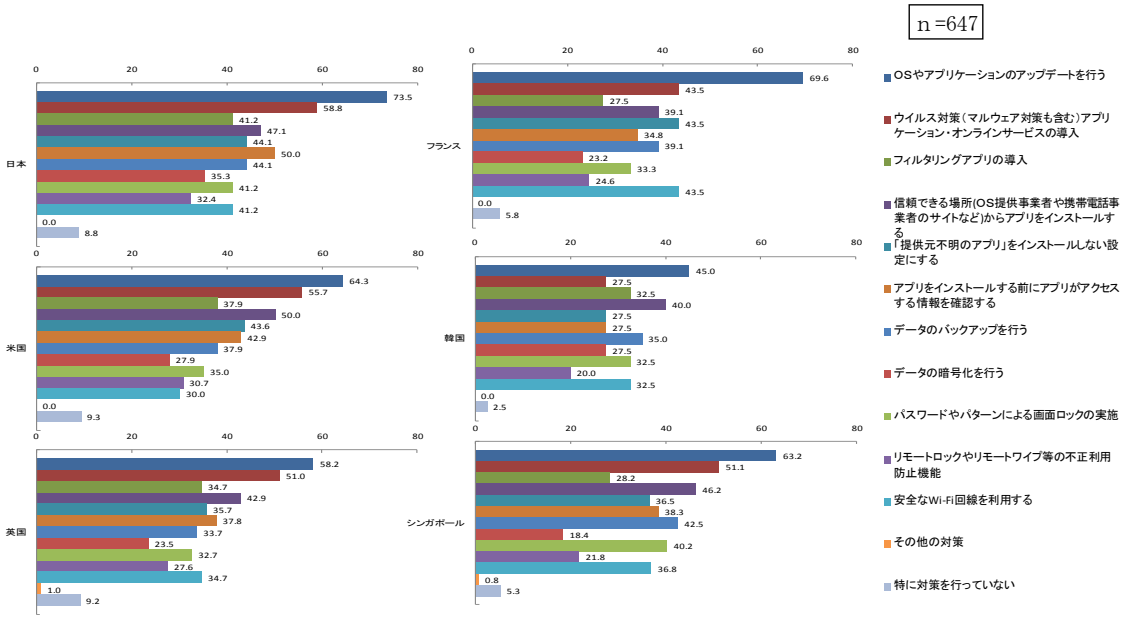


図表 2-41　会社で支給されたスマートフォンのセキュリティ対策の認知度

職場のスマートフォンではどのような情報セキュリティ対策を行っているかについて尋ねた。

日本は他国と比較して、設問に示した各セキュリティ対策を選択する割合が高くなった。

また日本では、「ＯＳやアプリケーションのアップデートを行う」73.5%、「ウイルス対策（マルウェア対策も含む）アプリケーション・オンラインサービスの導入 」58.8%、「信頼できる場所(ＯＳ提供事業者や携帯電話事業者のサイトなど)からアプリをインストールする」47.1%の順に高くなった。

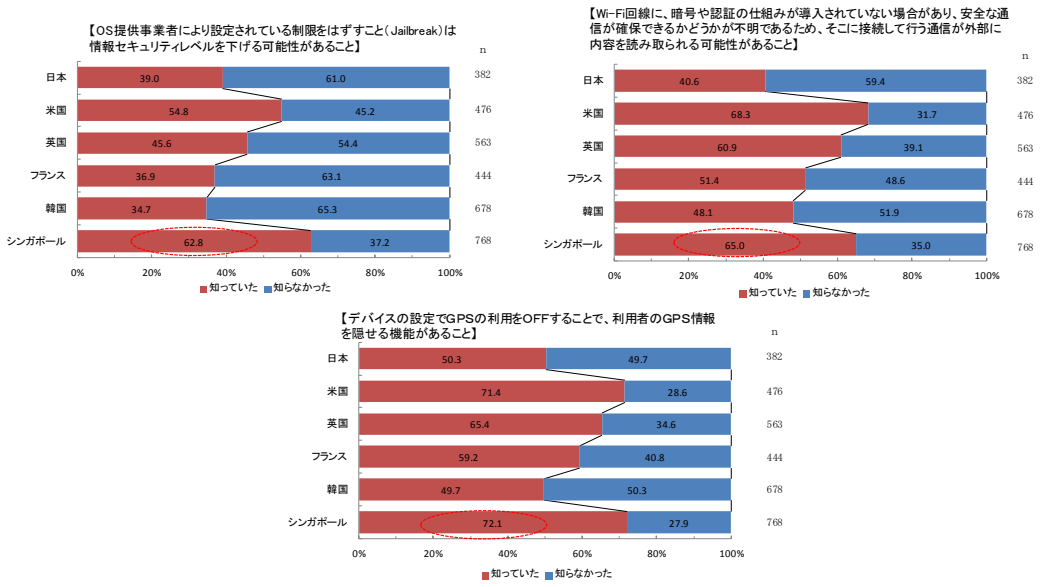


図表 2-42　会社で支給されたスマートフォンへ実施しているセキュリティ対策

スマートフォンを安全に利用するために３事項を例示し、その認知状況を尋ねた。

この結果、シンガポールは、３事項とも「知っていた」の回答割合が高くなった。次に米国も高くなっている

なお、日本は各事項とも「知っている」の回答割合が低くなった。



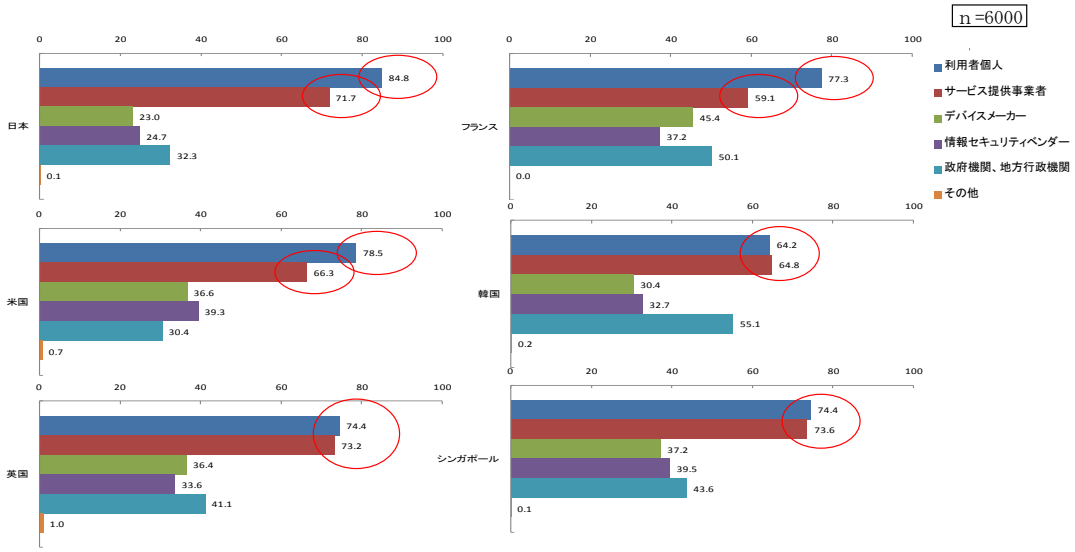
図表 2-43　スマートフォンを安全に利用するにあたり必要な事項

(9) 情報セキュリティ対策情報の入手

情報セキュリティ対策は誰が主体となって行うべきだと思うかを尋ねた。

各国とも「利用者個人」や、「サービス提供事業者」を選択する人が多くなった。日本では、「利用者個人」 84.8% 、「サービス提供事業者」 71.7%となった。

韓国やフランスでは、「政府機関、地方行政機関」を選ぶ割合が半数を超えた。それぞれ55.1%、50.1%となった。

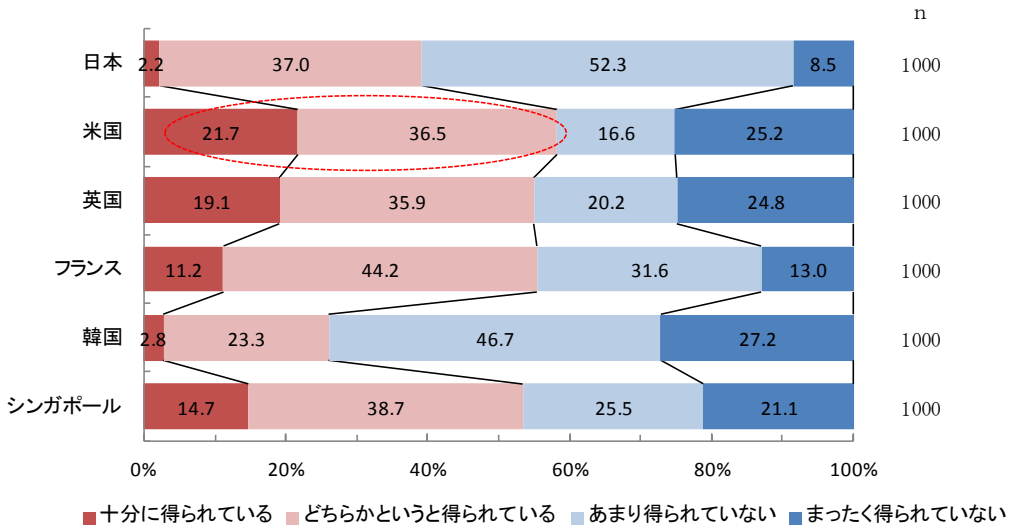


図表 2-44　情報セキュリティ対策の主体

次に、情報セキュリティ対策に関する情報を得られているかについて尋ねた。

各国別に情報を得られているかについてみると、「得られている」(「十分に得られている」＋「どちらかというと得られている」) が半数を超えたのは、米国 58.2%、英国 55.0%、フランス 55.4%、シンガポール 53.4%であった。

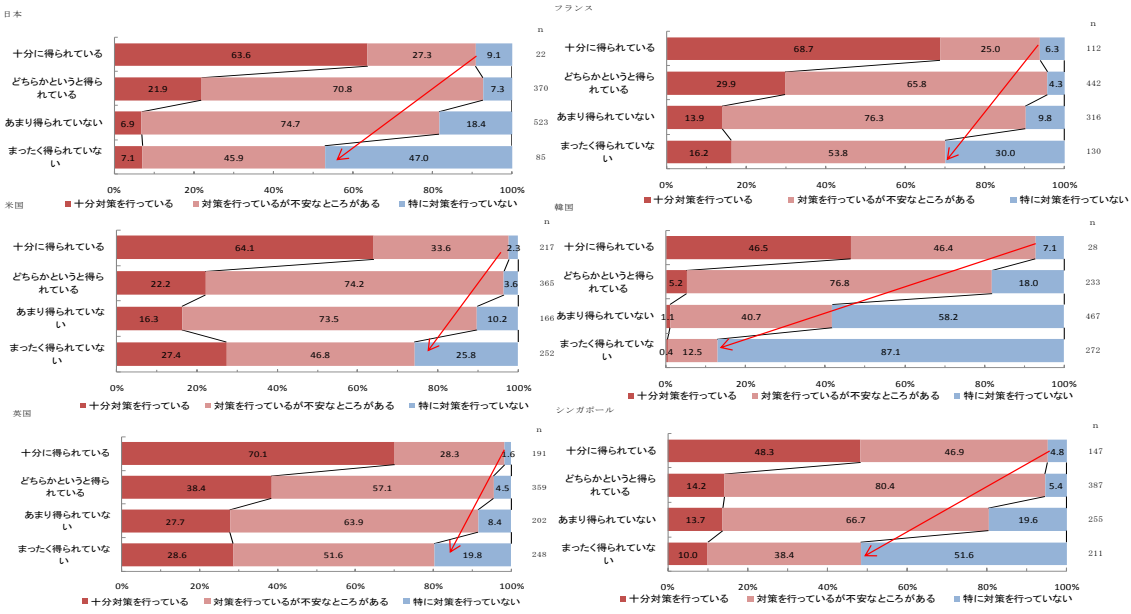
逆に「得られている」との回答が低くなったのは、韓国 26.1%、日本 39.2%であった。



図表 2-45　情報セキュリティ対策情報の入手状況

さらに、情報セキュリティ対策の実施状況と情報セキュリティ対策に関する情報の入手状況をクロスさせて分析を行った。

各国とも情報セキュリティ情報が得られていないほど「特に対策を行っていない」の回答も増える傾向がある。

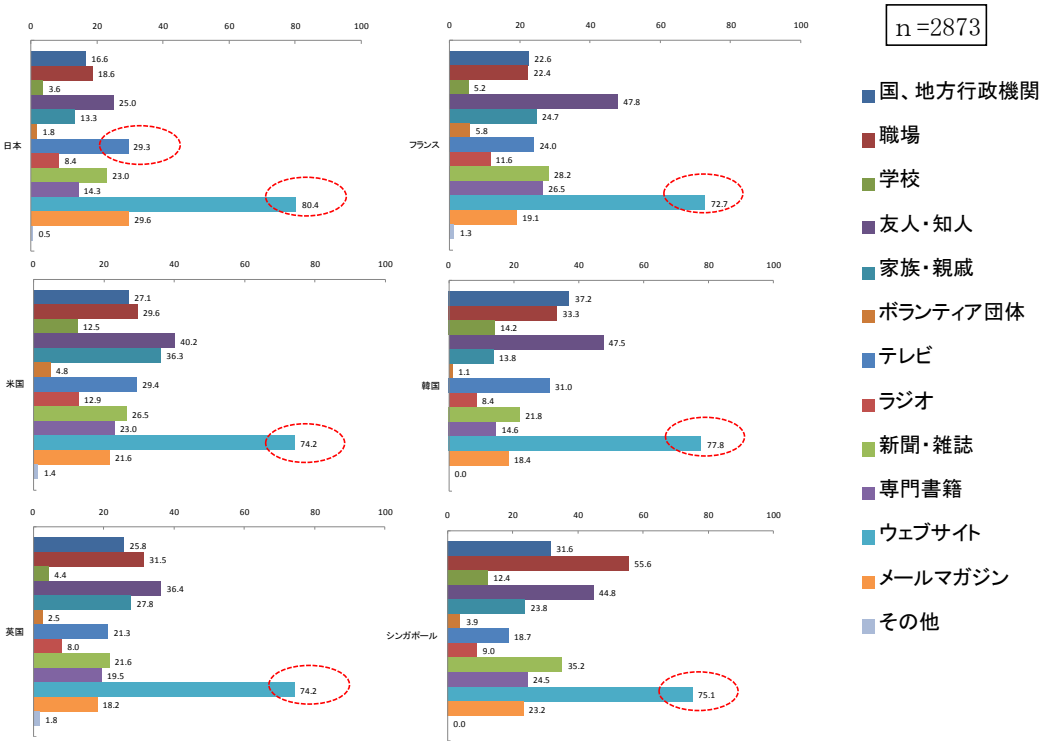


図表 2-46　情報セキュリティ対策の実施状況（情報の入手状況別）

ここでは、どこから情報セキュリティ対策の情報を得ているかについて尋ねた。

各国別に情報入手先をみると、全ての国において「ウェブサイト」が最も高くなった。回答割合は７～８割となった。次に高くなったのは、日本を除き、「友人・知人」となった。回答割合は３～５割となった。

なお、日本で、2 番目に高くなったのは「テレビ」で 29.3%であった。



図表 2-47　情報セキュリティ対策情報の入手先

また、情報セキュリティ対策情報を「あまり得られていない」、「まったく得られていない」と回答した人に対して、情報セキュリティ対策情報を入手するにあたっての課題についても尋ねた。

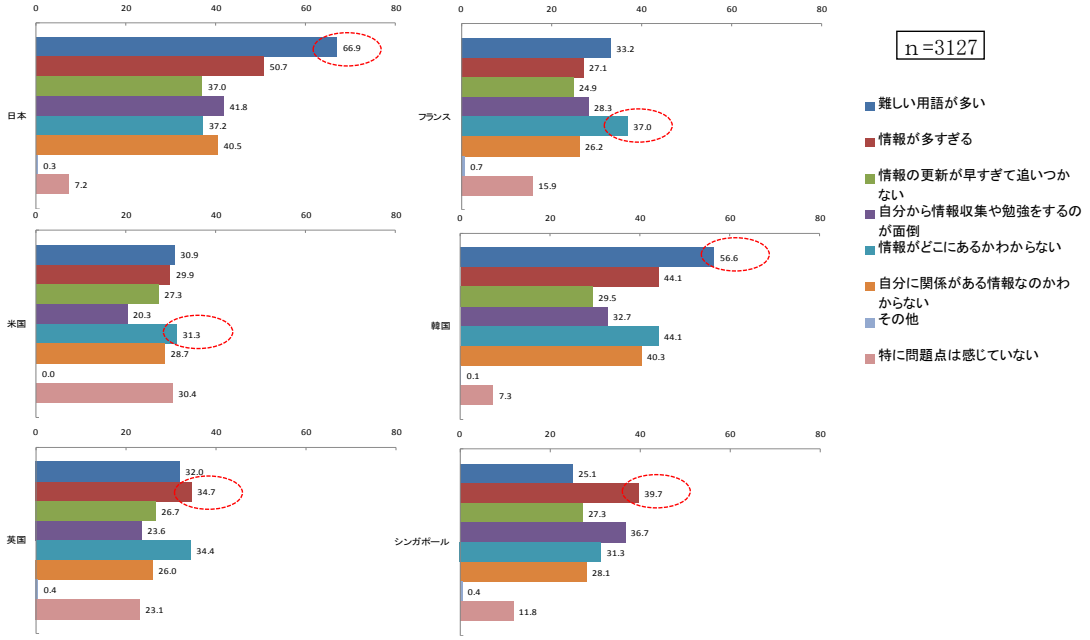
各国別に最も回答割合が高くなった課題に注目すると、大きく 3 つに分かれた。

「難しい用語が多い」が高くなったのは、日本 66.9%、韓国 56.6%となった。

「情報が多すぎる」が高くなったのはシンガポール 39.7%、英国 34.7%となった。

「情報がどこにあるかわからない」が高くなったのはフランス 37.0%、米国 31.3%となった。

なお、日本では、2 番目に高くなったのは「情報が多すぎる」50.7%、3 番目は「自分から情報収集や勉強をするのが面倒」41.8%となった。



図表 2-48　情報セキュリティ対策情報の入手にあたっての課題

(10) 情報セキュリティ向上に必要な取組

国・行政、企業に実施してほしい情報セキュリティ向上のための取組を尋ねた。

各国別に最も回答割合が高くなった取組に注目する。「情報セキュリティ対策や情報セキュリティ事象をまとめたサイトの提供」 が高くなったのは、シンガポール 58.4%、 英国 50.4%、韓国 47.6%、日本 41.9%。

「情報セキュリティに関する相談窓口の設置」はフランスで 52.0%となった。

「インターネット接続機器の情報セキュリティ診断・設定」が最も高くなったのは米国 42.2%であった。

なお、日本において 2 番目に高くなったのは、「インターネット接続機器の情報セキュリティ診断・設定」で 41.2%、3 番目は「情報セキュリティに関する相談窓口の設置」35.1%となった。

なお、米国は「特にない」が 30.3%と他国と比較して高くなった。

図表 2-49　情報セキュリティ向上に必要な取り組み

(11) まとめ

調査の結果、我が国の利用者は他国と比較して、情報セキュリティの被害に遭った経験はそれほど高くないものの、インターネット利用に対する不安意識は高いことがわかった。

さらに、インターネット上の脅威（マルウェア、フィッシング、架空請求等）に関する知識も有していたが、特定の脅威を念頭に置いたものではなく漠然としており、そのためか、一定の情報セキュリティ対策はスマートフォンを含めて実施しているものの、それだけで不安感を払拭するには至らず、また、情報セキュリティに関する情報も十分には得られていないと感じている（対象国中下から 2 番目）、といった結果が得られた。

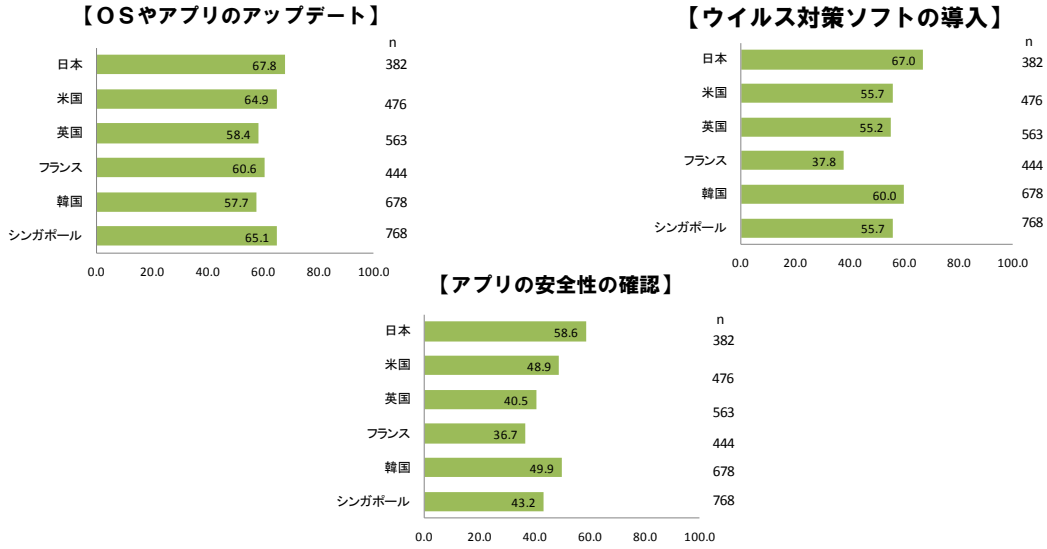
また、本調査では、情報セキュリティに関する情報が得られている人ほど、情報セキュリティ対策を実施している割合が高くなることがわかった（図表 2-46）。

2.4　総務省の関連政策の浸透度に関する調査

総務省では、ICT 基盤・サービスの高度化に伴い、スマートフォンのプライバシー対策やアプリの安全対策等の消費者保護関連施策を講じている。国内における施策への浸透度、施策に関連する情報の認知状況について調査を実施した。

(1) スマートフォンセキュリティ 3 か条の認知状況（再掲）

スマートフォンにおける情報セキュリティ対策については、日本では「スマートフォンセキュリティ 3 か条」を公表、啓蒙がおこなわれている。本調査で、3 か条に該当する「ＯＳやアプリケーションのアップデート」、「ウイルス対策ソフトの導入」及び「インストールするアプリの安全性の確認」の認知度について尋ねた。その結果、日本は 3 項目全てにおいて回答率が 5 割以上となり、他国より認知度が高くなった。



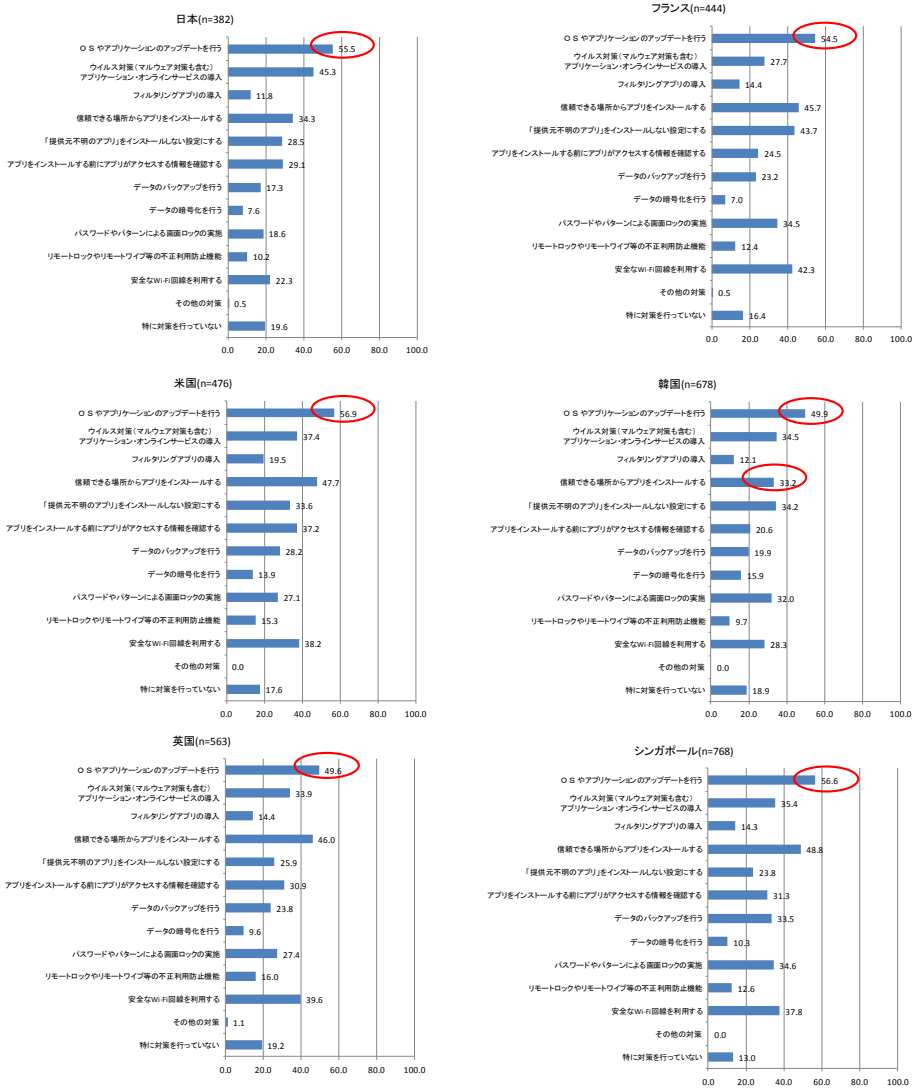
図表 2-50　スマートフォンの情報セキュリティ対策の認知状況

次に、スマートフォンにおける情報セキュリティ対策の実施状況を尋ねた。

各国とも「ＯＳやアプリケーションのアップデートを行う」の回答が高くなり、半数を占めている。

日本をみると、回答が高くなった順に、「ＯＳやアプリケーションのアップデートを行う」55.5%、「ウイルス対策（マルウェア対策も含む）」45.3%、「信頼できる場所からアプリをインストールする」34.3%となった。

なお、「信頼できる場所からアプリをインストールする」は、米国、英国、フランス、シンガポールでは回答割合が 4 割以上となっており、日本が他国と比較すると低くなっている。同様に韓国も 33.2%と低い。

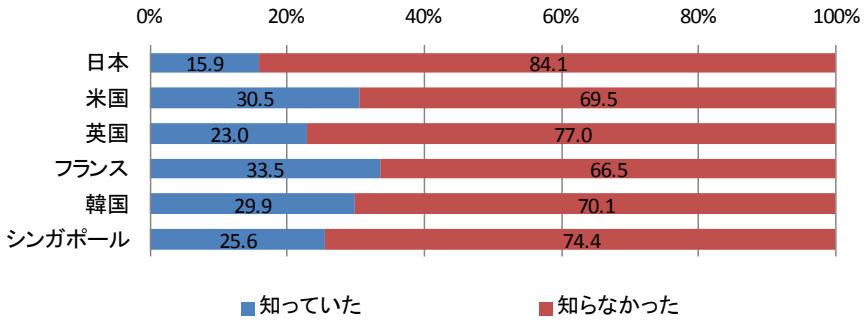


図表 2-51　スマートフォンの情報セキュリティ対策の実施状況

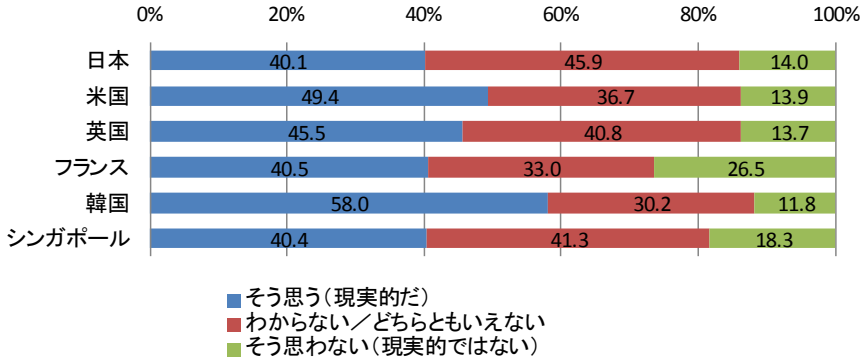
(2)　忘れられる権利の認知状況

「忘れられる権利」とは、サーバーの管理者や検索サービス会社などに対し、個人が自分の情報を削除させる権利のことである。情報を完全に削除することができなくても、この権利を保有することで、情報の拡散防止に役立てることが期待され、特に EU 等で検討が進められている。本調査では、忘れられる権利に関して、その認知状況等の把握を行った。

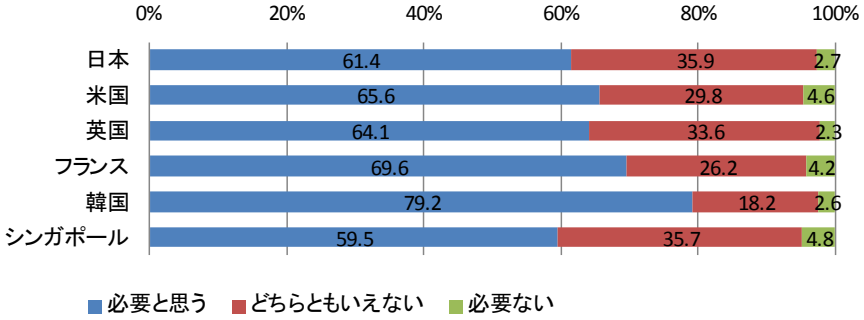
この結果によると、「忘れられる権利」の認知度はフランスが最も高く 33.5%、日本が最も低く、15.9%となった。「忘れられる権利」を「現実的だ」とする回答は韓国では、58.0%、その他の国では約 4～5 割で、フランスでは、26.5%が「現実的ではない」と回答している。「忘れられる権利」で保護されることの必要性について、韓国では 79.2%、フランスの 69.6%が「必要と思う」と回答している。



図表 2-52　「忘れられる権利」の認知状況



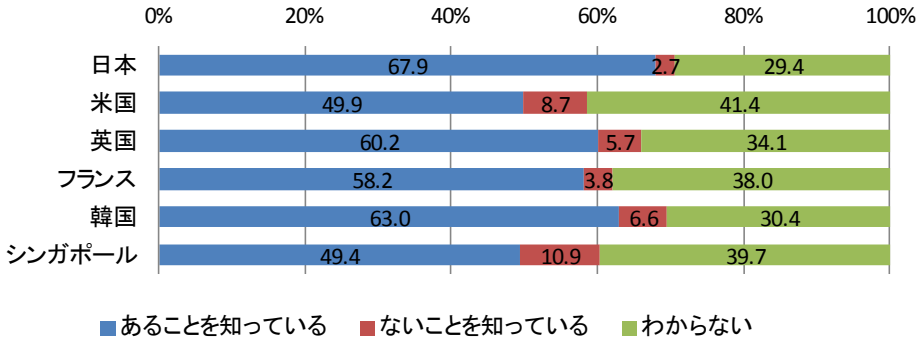
図表 2-53　「忘れられる権利」は現実的な権利だと思うか



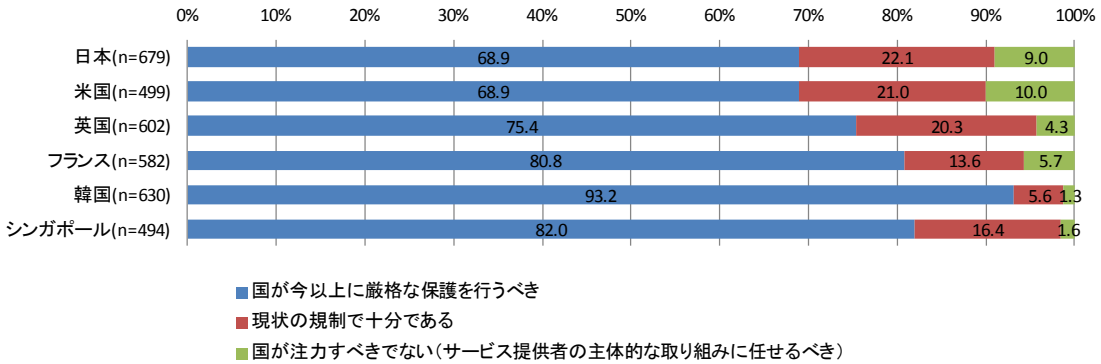
図表 2-54　「忘れられる権利」によって国民が保護されることを必要と感じるか

(3) 自国の個人情報保護に係る制度の認知状況

自国の個人情報保護に関する法律の認知状況について、「自分の国に個人情報保護に関わる法律があるかどうかを知っているか」と尋ねた設問を見ると、日本では、67.9%が「あることを知っている」と回答している。さらに、「個人情報保護規制のあり方についてどのように感じるか」という設問の回答を見ると、日本では、「国が今以上に厳格な保護を行うべき」という回答が 68.9%と他国と比較して低めという結果となった。



図表 2-55 自国の個人情報保護に関する法律の認知情報
（自分の国に個人情報保護に関わる法律があるかどうかをしっているか）



図表 2-56 個人情報保護規制のあり方への意見
（個人情報保護の規制のあり方についてどのように感じるか）

3. 諸外国の関連政策に係る調査

情報セキュリティ対策、データ保護対策・データプライバシー対策に関する諸外国の政策動向の調査・分析を行い、ICT 環境の変化がもたらす社会的・制度的課題に係る論点の整理を行った。EU における個人情報保護ルールの見直しを始め、様々な取組をピックアップした。また、情報セキュリティ対策に係る国際連携も活発になっていることから、我が国を含む国際連携の動向についても調査・整理を行った。

3.1 情報セキュリティ対策に関する諸外国の動向

諸外国におけるセキュリティ対策に関する政策動向（教育・研究開発政策も含めて）や国際連携や国際機関等の動向を調査・整理した。その上で有識者への事実確認を行った。以下に、諸外国での主要な政策動向を整理する。

3.1.1 米国における動向

米国政府における直近の動向として、2013 年（平成 25 年）2 月 12 日にオバマ大統領により署名された「重要インフラのサイバーセキュリティ強化を目的とする大統領令」がある。この命令では、サイバー攻撃に係る情報の共有を軍需産業からすべての重要インフラ事業者に拡大する手続きを確立することや重要インフラに対する情報セキュリティ上のリスクを軽減する枠組みの策定等が盛り込まれている。

また、同日の一般教書演説において、オバマ大統領は「外国による企業機密の窃取や、電力、金融、航空制御システムへの攻撃の発生など、国家安全保障と経済にとっての本当の危機に直面していること」、「情報共有の強化等に関する新しい大統領令に署名したが、それにも関わらず、ネットワークの強靭化と攻撃の阻害を強化するためには、サイバーセキュリティを強化する法整備が必要である」と述べている。

国防総省（Department of Defense, DoD）では、2010 年（平成 22 年）に設置したサイバー司令部の要員を今後数年間で 5 倍強に増強するとともに、同司令部の下に、①発電所や送電網など社会経済的に重要なインフラの防衛、②海外での軍事作戦の支援、③国防総省自身のネットワークの防衛、を目的とする 3 部隊を設ける計画を策定した。

3.1.2 欧州における動向

欧州における直近のサイバーセキュリティの動向として、2013 年 2 月 7 日に欧州委員会通信ネットワーク・コンテンツ・技術総局及び内務総局、欧州連合外務・安全保障政策上級代表が合同で公表した「サイバーセキュリティ戦略及びネットワーク・情報セキュリティに関する指令案」がある。

同指令案は、サイバー攻撃への対応に関する EU の包括的なビジョンとして、①サイバーレジリエンスの実現、②サイバー犯罪の大幅な減少、③サイバー防衛政策及び共通安全保障防衛政策（Common Security and Defence Policy ,CSDP）に関する防衛能力の向上、

④サイバーセキュリティ関連の産業・技術資源の発展、⑤EU のための一貫した国際的なサイバー空間政策の確立及び EU の核心的価値の推進、を優先課題として示している。また、サイバーレジリエンスの達成のために必要な措置の法制化を行っている。

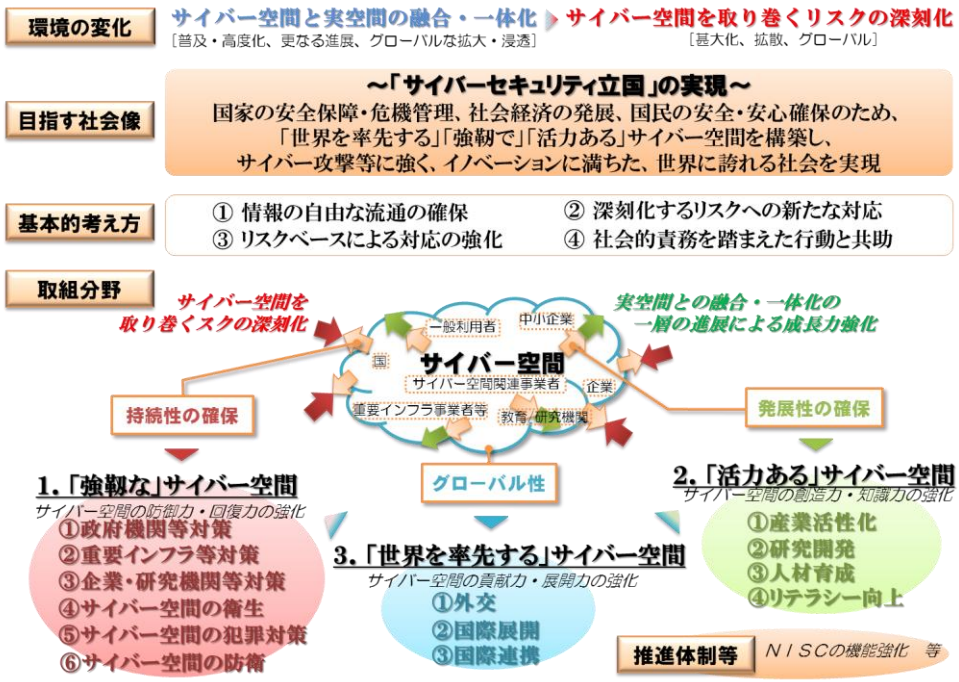
なお、英国では、サイバーセキュリティに係る情報を、政府と産業界で豊富かつ迅速に共有するための枠組みとして「サイバーセキュリティ情報共有パートナーシップ（Cyber Security Information sharing Partnership, CSIP）」を立ち上げることを 2013 年 3 月に発表した。

3.1.3 我が国における取組

(1) 新たな情報セキュリティ戦略の策定

我が国における情報セキュリティ対策は、内閣官房情報セキュリティセンター及び IT 戦略本部の下に設置された情報セキュリティ政策会議が主導している。同会議では、情報セキュリティ分野における基本戦略として、「第 1 次情報セキュリティ基本計画」（2006 年 2 月）、「第 2 次情報セキュリティ基本計画」（2009 年 2 月）及び「国民を守る情報セキュリティ戦略」（2010 年 5 月）が策定され、官民が連携して情報セキュリティ対策の強化に関する取組が進められてきた。

この間、サイバー空間と実空間の融合・一体化が進展するとともに、サイバー空間を取り巻くリスクが甚大化し、拡散し、グローバルレベルのものとなるなど、我が国の情報セキュリティを取り巻く環境が急速に変化している。こうした深刻化する環境変化を踏まえ、現在、同会議においては、国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、新たな情報セキュリティ戦略として、世界を率先する強靭で活力あるサイバー空間を構築し、「サイバーセキュリティ立国」を実現することを基本的な方針とする「サイバーセキュリティ戦略」（仮称）を検討しており、本年 6 月に決定する予定である（図表 3-1）。



図表 3-1　新たな情報セキュリティ戦略のイメージ

（出典）情報セキュリティ政策会議　第 33 回会合資料

3.1.4　セキュリティ分野における国際連携

我が国は情報セキュリティ分野において二国間会合などの国際連携に積極的に取り組んでいる。

(1)　日本－米国の取組

米国との間では、2012 年 10 月 18～19 日に米国ワシントン D.C で開催された「インターネットエコノミーに関する日米政策協力対話（第 4 回局長級会合）」において、サイバー攻撃への対応に関する研究開発協力として、総務省と国土安全保障省（Department of Homeland Security, DHS）との間でサイバーセキュリティ研究開発に関するネットワーク運用のデータ共有が開始されたことを確認している。また、スマートフォンやクラウドコンピューティングサービスのセキュリティの確保の重要性を認識し、ベストプラクティスと現状のアップデートに関する情報共有を継続することが両国で一致した。

(2)　日本－英国の取組

英国とは、2012 年 6 月 19～20 日に「日英サイバー協議」が外務省で開催され、サイバー空間における国際的な規範作り、安全保障面における課題、サイバー犯罪への取組、情報セキュリティ・システム防護、経済的・社会的側面における両国の取組についての紹介や協力の可能性等について幅広い意見交換が行われた。

(3) 日本－EU の取組

EU とは、2012 年 11 月 14～15 日に「日 EU インターネット・セキュリティフォーラム」を東京で開催し、インターネットにおけるセキュリティ確保に関する政策や技術の動向等についての意見交換、インターネットにおけるセキュリティに関するグッド・プラクティス（サイバー攻撃予知・即応技術の研究開発（PRACTICE プロジェクト）、スマートフォンのセキュリティ対策等）の共有、重要インフラ防護や官民の情報共有のあり方についての取組の共有、情報セキュリティに関する意識啓発活動、オンライン上のプライバシー等についての意見交換が行われた。本フォーラムでの議論を通じて、日 EU 双方において、インターネットにおけるセキュリティの確保に向けて取り組むに当たっては国際的な連携を推進することが重要であることが改めて確認された。

(4) 日本－ASEAN の取組

ASEAN（東南アジア諸国連合）とは 2009 年 2 月 25 日に東京で開催された「第 1 回日・ASEAN 情報セキュリティ政策協議」を契機に、日本及び ASEAN 諸国の経済連携を強化し、国家基盤を支える情報インフラの情報セキュリティ対策を向上させるための協力関係が構築されている。2012 年 10 月 10～11 日には、「第 5 回日・ASEAN 情報セキュリティ政策会議」が東京で開催され、日・ASEAN における情報セキュリティ意識啓発に対する取組の推進、情報セキュリティ関連情報共有体制の検討と連絡窓口確認の実施、情報セキュリティにおける一層の連携強化について意識共有が行われた。また、2012 年 10 月 12 日には、「第 1 回日・ASEAN 情報セキュリティ・シンポジウム」が開催され、各国の取組や現状等の報告・共有が行われた。さらに 2013 年 9 月には「日 ASEAN サイバーセキュリティ協力に関する閣僚政策会議」が東京で開催される予定である。

(5) 日本－インドの取組

インドとは、2012 年 11 月に「第 1 回日インド・サイバー協議」を開催し、安全保障分野での課題、サイバー犯罪への取組、情報セキュリティ・システム防護、経済的・社会的側面における両国の取組についての情報交換や両国間での協力の可能性等について意見交換が行われている。

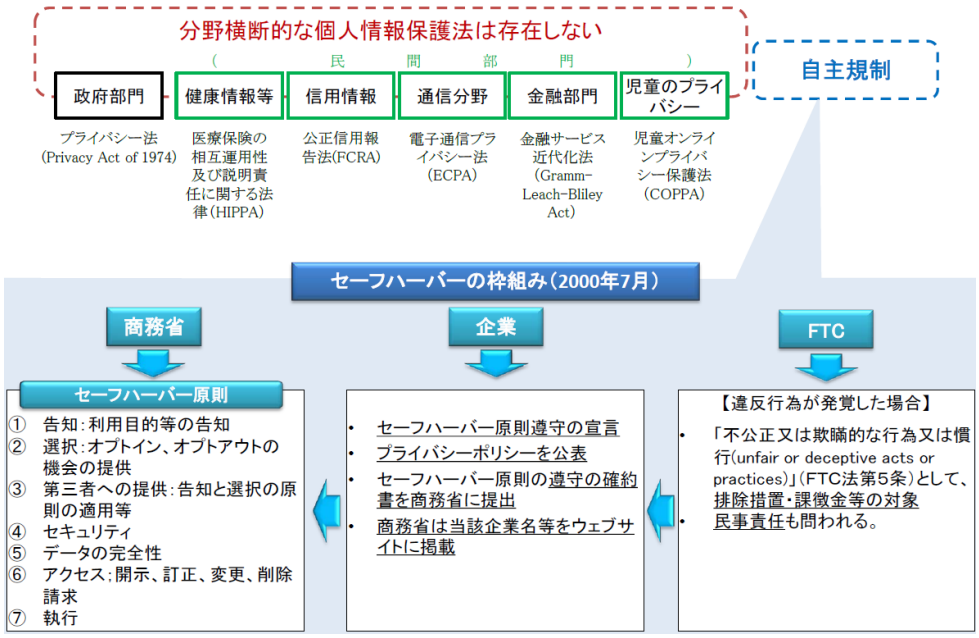
3.2　データ保護・データプライバシーに関する諸外国の動向

諸外国および国際機関等のデータ保護・データプライバシーに関する動向を調査・整理し、政策・制度の最新動向や見直しの動き、その具体的内容を調査・整理した。

3.2.1　米国における動向

(1)　パーソナルデータ保護に関する制度

米国ではパーソナルデータの保護に関して、州法を除けば連邦政府レベルでの包括的な法律は存在せず、分野ごとの個別法と業界等による自主規制を基本とするものとなっている（図表 3-2）。



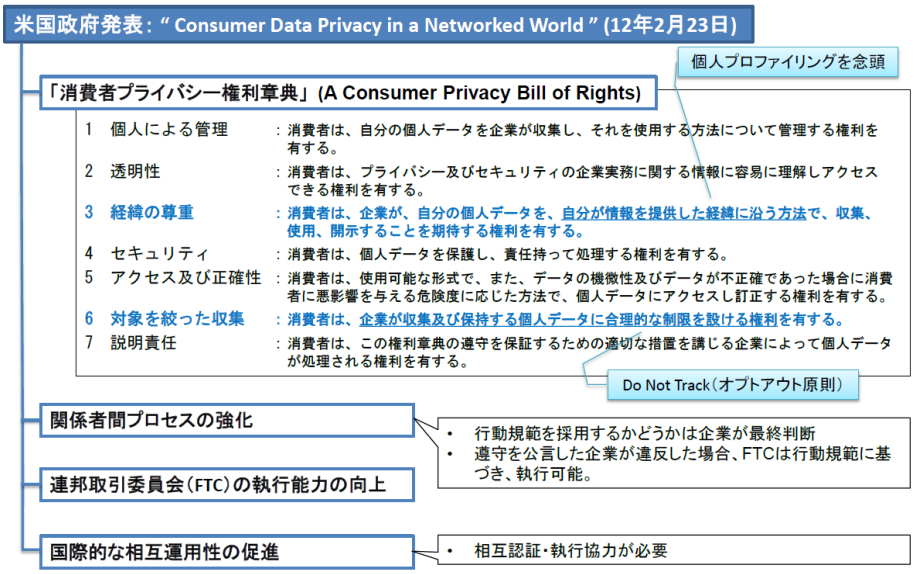
図表 3-2　米国におけるパーソナルデータ保護に関する制度

（出典）総務省「パーソナルデータの利用・流通に関する研究会　第 1 回配布資料」

米国のパーソナルデータの保護については、独立行政委員会である連邦取引委員会（Federal Trade Commission, FTC）が大きな役割を果たしており、自主規制の遵守についての監督、排除措置、課徴金の附課等の執行措置等を行う他、政策提言を活発に行うとともに、国際的な場でも活発な活動を行っている。

(2)　消費者プライバシー権利章典等の動向

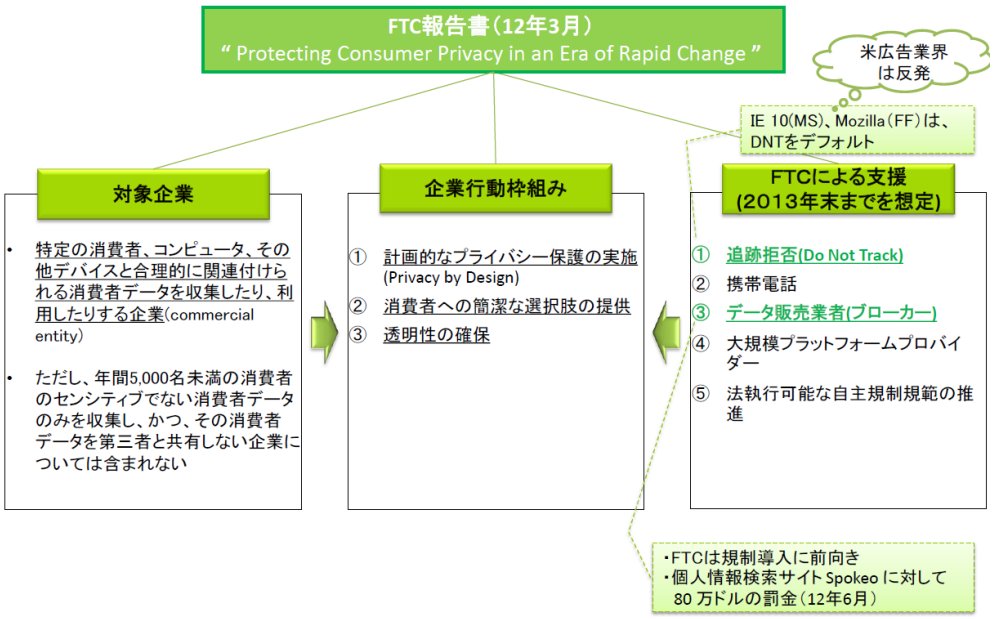
2012 年 2 月 23 日、パーソナルデータを取得し活用するビッグデータ時代に対応するため、ホワイトハウスにより政策大綱「ネットワーク化された世界における消費者データプライバシー」が発表された。同政策大綱では「消費者プライバシー権利章典」が提示された。



図表 3-3 消費者プライバシー権利章典

（出典）総務省「パーソナルデータの利用・流通に関する研究会 第１回配布資料」

また、同政策大綱の発表後、FTC は、2012 年 3 月、消費者データを収集し利用する企業の行動枠組みについてまとめた報告書である「急速に変化する時代における消費者プライバシーの保護」を発表した。同報告書では、「個人等に無理なくリンク可能なデータ消費者データ（reasonably linkable data）」を扱う企業に対し、3 つの事項の実施を要求している（図表 3-4）。



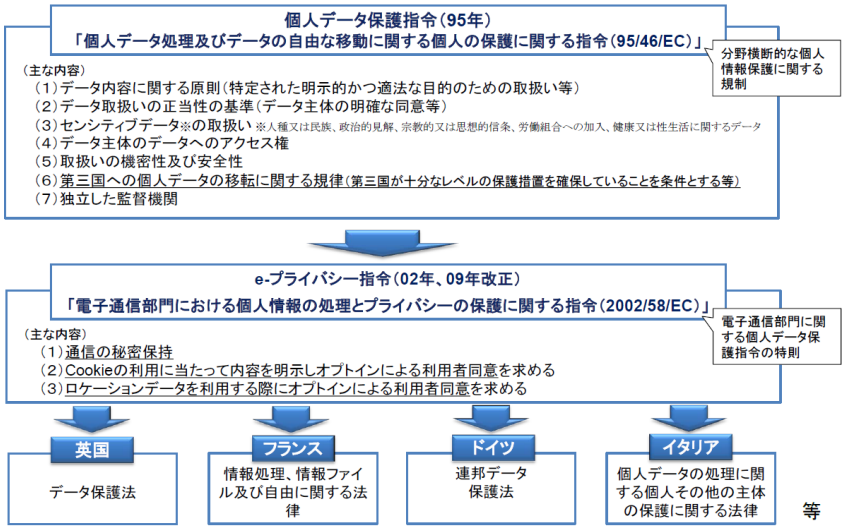
図表 3-4 FTC 報告書の概要

（出典）総務省「パーソナルデータの利用・流通に関する研究会 第１回配布資料」

3.2.2　欧州における動向

(1)　データ保護指令

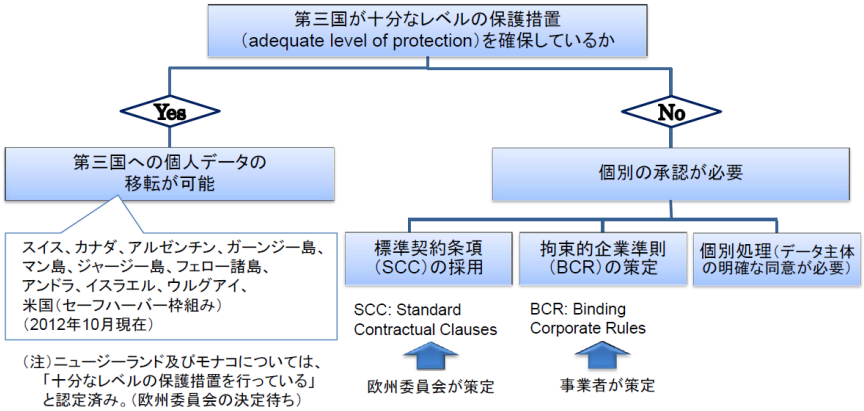
欧州では、「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／EC 指令」が採択され、1998 年に発効された。加盟国は当該指令を遵守するために必要な国内法の整備を義務づけられた。



図表 3-5　EU におけるプライバシー保護に関する制度

（出典）総務省「パーソナルデータの利用・流通に関する研究会　第1回配布資料」

また、同指令第 25 条では、EU 域内から第三国への個人データの移転は、原則として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している。その「十分なレベルの保護措置」の要素の 1 つとして、「独立した機関の形態をなす外部監督の制度」があげられている。



図表 3-6　EU から第三国への個人データ移転

（出典）総務省「パーソナルデータの利用・流通に関する研究会　第 1 回配布資料」

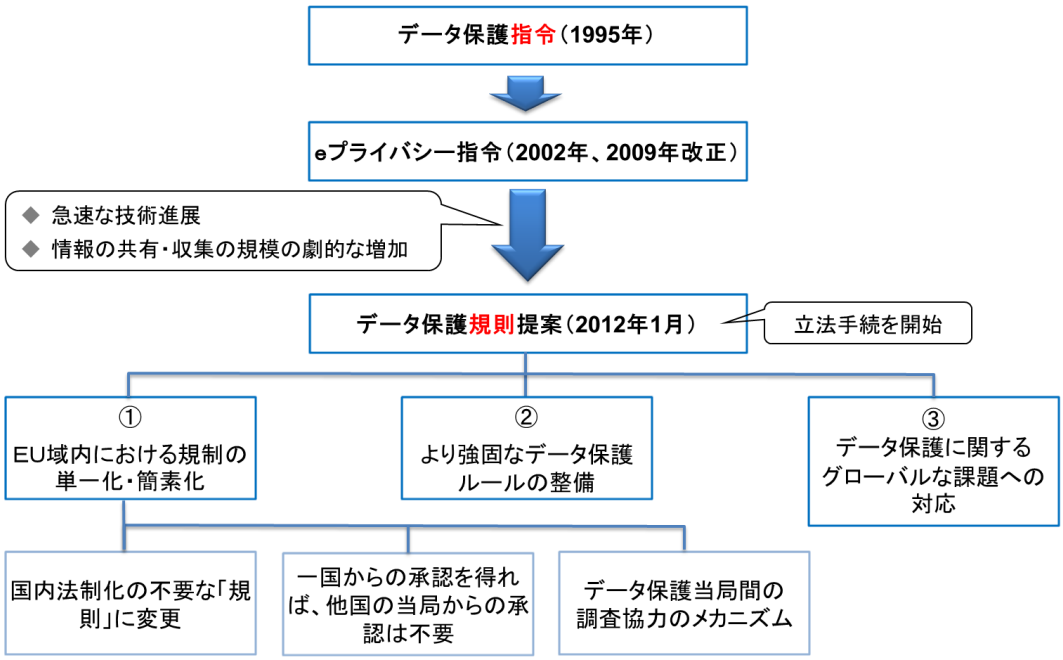
(2)　e プライバシー指令

欧州では、電子通信分野におけるパーソナルデータ保護に関する特則を規定するものとして、2002 年に「電子通信部門における個人データの処理とプライバシーの保護に関する 2002 年 7 月 12 日の欧州議会及び理事会の 2002／58／EC 指令」が採択された。

加盟国は当該指令を遵守するために必要な国内法の整備を義務づけられている。

(3)　データ保護規則提案

2012 年 1 月 25 日、欧州委員会は「データ保護指令」を抜本的に改正する「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則（一般的データ保護規則）の提案」を欧州議会及び欧州理事会に提案・公表した。

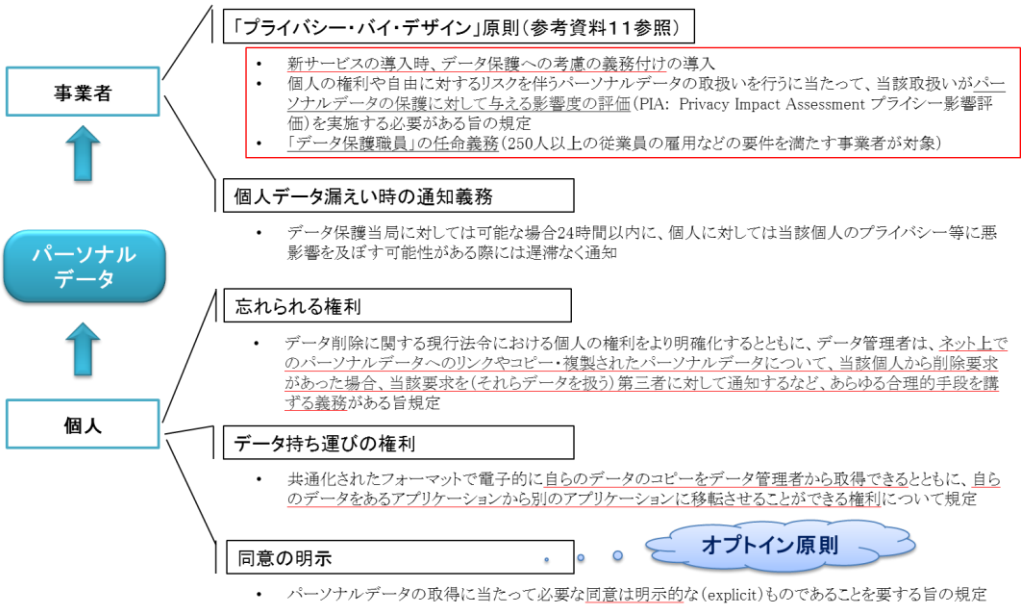


図表 3-7　EU 個人データ保護規則の枠組み

（出典）総務省「パーソナルデータの利用・流通に関する研究会　第 1 回配布資料」

加盟国に対して独立した監督機関の設置を義務づけていること、EU 域内から第三国への個人データの移転は原則として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していることは、現行のデータ保護指令と同様である。主要な改定点として、個人データ保護の権利の強化（自己情報コントロール権の強化など）、 EU 域内でのデータ保護ルールの一元化（EU 域内企業にとってメリット） グローバル環境でのデータ保護ルールの詳細化（第三国移転ルールの詳細化など）等がある。

なお、同規則提案においては、「十分なレベルの保護措置」の要素の 1 つとして、独立した監督機関の存在及びそれが効果的に機能していることが明記されている。



図表 3-8　データ保護規則提案

（出典）総務省「パーソナルデータの利用・流通に関する研究会　第 1 回配布資料」

3.2.3　我が国における取組

「プライバシー保護と個人データの国際流通についてのガイドラインに関する OECD 理事会勧告（OECD プライバシーガイドライン）」 が 1980 年に採択された後は、同勧告を参考に地方公共団体では独自に条例が制定されている。また、国の行政機関については、1988 年に「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」が制定されている。

民間部門については、1987 年に旧大蔵省所管の財団法人金融情報システムセンター（当時）、1989 年に旧通商産業省、1991 年に旧郵政省が、それぞれ所管する事業分野等について、個人情報保護に関するガイドラインを策定している。

その後、2003 年 5 月に「個人情報の保護に関する法律」（以下、個人情報保護法という）が制定され、2005 年 4 月に全面施行された。同時に行政機関の保有する個人情報の保護に関する法律（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を全面的に改正）や独立行政法人等の保有する個人情報の保護に関する法律も制定・施行された。2004 年 4 月には、個人情報保護法に基づき「個人情報の保護に関する基本方針」が閣議決定されている。

個人情報保護法では、監督・執行について専門的な独立した第三者機関を設置せず、各事業等を所管する大臣が主務大臣として監督・執行を行うという主務大臣制がとられている。

3.2.4　国際機関等における動向

⑴ 経済協力開発機構（OECD）

1980 年、OECD は「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（OECD プライバシーガイドライン）」を策定した。

同ガイドラインは、プライバシー保護・個人の自由と個人データの自由な流通の実現の双方のバランスを図り、個人データの取扱いに関する原則（OECD8 原則）などを示したものである。プライバシー保護の主要原則を初めて規定した国際約束であり、各国の個人情報保護法制及び国際的な取組に対し、長年強い影響を及ぼしてきた。パソコンやインターネットが普及する遥か昔の時代に策定されたものでもあることから、時代にそぐわない規定を修正し所要の規定を追加する必要性が高まってきたことから、OECD において、30 年ぶりに同ガイドラインの改正を行うこととされており、2013 年内又は 2014 年初めに改正案が採択される予定である。

⑵ APEC

(a) APEC プライバシーフレームワーク

APEC 域内における電子商取引推進に向けて、パーソナルデータの保護の原則を定める枠組みとして策定された。2004 年に APEC 貿易・投資委員会（Committee on Trade and Investment, CTI）傘下の電子商取引運営グループ（Electronic Commerce Steering Group, ECSG）がとりまとめ、同年 11 月に APEC 閣僚会議で承認された。

(b) CPEA（Cross Border Privacy Enforcement Arrangement：越境プライバシー執行協力）

CPEA は、パーソナルデータが国境を越えて委託、移転、共有等されているときに、国境を越えた先での漏えい等があった場合、移転元エコノミー（国・地域）における執行機関が、自エコノミーにおけるパーソナルデータ保護法令の執行のために、移転先エコノミーにおける執行機関に対し、情報の提供、調査等協力を依頼するための枠組みである。

2009 年 11 月に APEC 閣僚会議で承認された。

(c) CBPR（Cross-Border Privacy Rules System：越境プライバシールール）

APEC プライバシーフレームワークへの適合性を国際的に認証する制度として、2011 年 11 月に APEC 閣僚会議で承認された。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のルールである。

CBPR 制度に参加するためには、①CPEA に参加する、②エコノミーとして CBPR 制度へ参加する、③エコノミーが認証機関を登録するとの３つの手続を踏む必要がある。

CPEA の参加エコノミーのうち、米国及びメキシコが②の手続を完了させている。

(3) データ保護プライバシー・コミッショナー国際会議（International Conference of Data Protection and Privacy Commissioners）

1979 年から毎年開催されている会合で、アルゼンチン、オーストラリア、カナダ、フランス、ドイツ、ギリシャ、アイスランド、イスラエル、イタリア、メキシコ、モロッコ、オランダ、ニュージーランド、ノルウェー、ペルー、韓国、英国、ウルグアイ、米国等 57 ヶ国のパーソナルデータの保護機関がメンバーとして参加している（2012 年現在）。

我が国からはメンバーとして正式な参加が認められている機関はなく、消費者庁にオブザーバー資格が認められている。

同会議では、各国のパーソナルデータの保護機関により、データ保護に関する様々な課題についての議論等が行われている。

なお、同会議の参加資格は以下を満たすパーソナルデータの保護機関とされている。

① 法的文書に基づき設置された公的な機関であること。
② パーソナルデータ又はプライバシー保護に関する法律の実施の監督を行うものであること。
③ 運用する法律がデータ保護又はプライバシーに関する中心的な国際的な文書と整合的であること。
④ その機能を実行するため適切な範囲の法的な権限を有していること。
⑤ 適切な自律性と独立性を有していること。

(4) アジア太平洋プライバシー機関（Asia Pacific Privacy Authorities, APPA）

アジア太平洋地域のパーソナルデータの保護機関がメンバーとして参加し、パーソナルデータに関する様々な課題についての議論等を行っている組織である。1992 年の発足以降、年 2 回のフォーラムを開催している。

2012 年現在、オーストラリア、カナダ、香港、マカオ、ニュージーランド、韓国、米国のパーソナルデータの保護機関がメンバーとして参加している。我が国からは消費者庁がオブザーバーとして参加している。

APPA の参加資格は以下のいずれかを満たすパーソナルデータの保護機関とされている。

① データ保護プライバシーコミッショナー国際会議のメンバーであること。
② APEC・CPEA に参加していること。
③ OECD・GPEN に参加していること。

(5) 欧州評議会（Council of Europe, CoE）

EU 全加盟国、旧ユーゴスラビア諸国、ロシア、ウクライナ、トルコ等の 47 ヶ国が加盟する国際機関である。我が国は欧州評議会のオブザーバー国となっている。

欧州評議会の閣僚委員会は 1980 年に「個人データの自動処理に係る個人の保護に関する

条約（条約第 108 号)」を採択した。同条約は、OECD プライバシーガイドラインとほぼ同様なデータ保護の基本的原則を示したものである。

同条約は欧州評議会非加盟国であっても参加が可能であり（同条約第 23 条)、2013 年 5 月現在で欧州評議会非加盟国のウルグアイを含む 45 カ国が同条約を締結している。

2001 年には､「個人データの自動処理に係る個人の保護に関する条約への監督機関及び越境データ流通についての追加議定書」が採択された。同追加議定書は 3 か条からなり、「独立した監督機関の設置」、「締約国以外の国への個人データの移転の制限」等について定めている。

⑹ ISO（International Organization for Standardization：国際標準化機構）
IEC（International Electrotechnical Commission：国際電気標準会議）

ISO と IEC の合同の専門委員会である JTC1 の傘下に設置された SC27／WG5 が、アイデンティティ管理及びプライバシー技術を担当している。

2011 年に、プライバシーに関する共通的な用語の特定、PII（personally identifiable information：個人識別可能情報）の処理に関する関係者及びその役割の定義等を示す ISO/IEC 29100:2011 Privacy framework が規格化された。

3.3　ICT 環境の変化がもたらす社会的・制度的課題に係る論点

スマート端末の普及に伴い、Android を搭載した機器に対する脅威が増加している。昨今のセキュリティ脅威は、技術だけでは対応できなくなっているため、制度や仕組み、リテラシーの観点での対応が求められる。例えば、スマートフォン等の普及により、十分な情報リテラシーやセキュリティリテラシーを身に着けずにインターネットを利用する消費者が増加している。昨今のセキュリティ脅威は、セキュリティ対策技術で対処できる範囲を超えており、個々の消費者や企業での判断が求められるため、利用者のリテラシー向上が期待される。

また、スマート端末の普及によるデータ保護・データプライバシー侵害が多様化していることも大きな環境変化である。諸外国は、スマート端末の普及に伴う新たなプライバシー侵害を懸念し、検討を進めている。例えば、米国の連邦取引委員会（Federal Trade Commission, FTC）は、スマート端末の普及に伴う個人情報の収集手段の多様化に注目している。特に、児童の個人情報を保護者の同意なしに収集する事案が相次いで発生している。こうした状況を是正すべく、モバイル大手事業者に対して、プライバシー保護強化を求める報告書を作成しており、継続的にこの問題に取り組むとしている。

スマートフォンにおける利用者情報が安心・安全な形で活用され、利便性の高いサービス提供されるために、継続的にスマートフォンに対するより良いプライバシー保護の在り方を検討する必要がある。

スマート端末の普及等に代表される昨今の情報通信技術の革新やそれに伴う社会環境の変化に対応したセキュリティ・パーソナルデータの保護に関する制度や仕組みの構築が喫緊の課題であり、諸外国では対応を急速に進めている。我が国では、情報セキュリティ分野では他国と足並みを揃えつつ、我が国のサイバー空間におけるセキュリティ強化に努めている。

一方、パーソナルデータの保護に関しては、個人情報保護法成立以降、継続的な議論が行われてきたが、欧州・米国等のような社会環境変化への適用が遅れていることが現状である。こうした環境変化に対応すべく、昨今、総務省等では議論の場が立ち上がり、検討が進みつつある。利用者のプライバシーを保護した上で、パーソナルデータを活用したサービスの恩恵を利用者が享受できる環境構築に向けて、更なる議論が期待される。

4. 企業等における関連動向

4.1 情報セキュリティに関する調査

昨今、スマートフォン、タブレット端末、テレビ、ゲーム機などインターネットに簡単に繋ぐことができるデバイスや、無線 LAN・LTE などの高速無線接続サービスも増えており、利用者側のリテラシーがそれほど高くなくともインターネットを利用しやすくなっている。

一方で、コンピュータウイルス、フィッシングに加え、標的型攻撃、SNS での個人情報漏えい、詐欺などネット上に新たな脅威が出現し、セキュリティ被害が拡大している。2011 年には 900 万人が被害にあい、その被害額は 350 億円に達すると推定されている。

ここでは、セキュリティサービスベンダーを調査対象とし、情報セキュリティインシデントの最新状況や対策事例についての状況把握をおこなった。

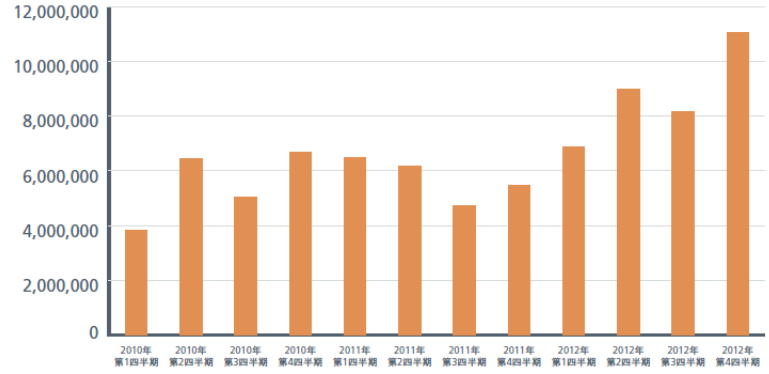
セキュリティサービスベンダーの公開するセキュリティインシデントのレポート、報道や新聞記事、セキュリティ関連報告書等を調査し、本年度のセキュリティインシデントの傾向を把握するとともに、セキュリティベンダーや学識者へのヒアリング調査を実施した。

4.1.1　情報セキュリティに関する動向

(1)　情報セキュリティ脅威の動向

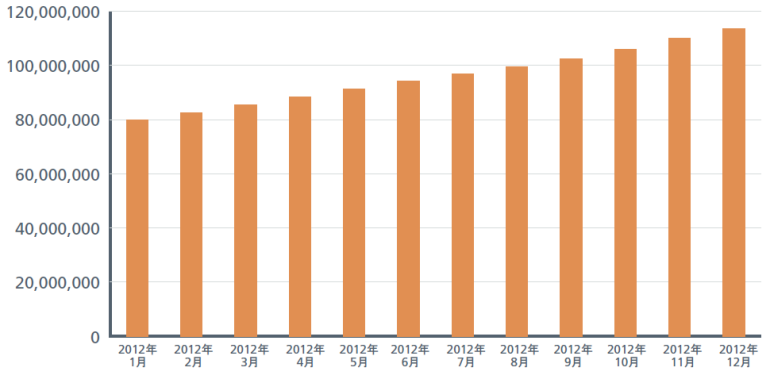
ICT の高度化、クラウドコンピューティング、スマートフォンの普及等によって、新たなリスクも顕在化しており、サイバー攻撃も高度化・複雑化の一途をたどっている。情報セキュリティを取り巻く環境は刻々と変化してきており、早期の情報共有や官民連携の強化といった対策の更なる強化が求められている状況にある。

情報セキュリティ企業が提供するセキュリティ脅威に関するレポートによると、現在、情報セキュリティベンダの McAfee 社データベースに登録されるマルウェアの種類は、1 月あたり約 300 万検体のペースで増加しているとのデータがある。



図表 4-1　マルウェア検体の発見数

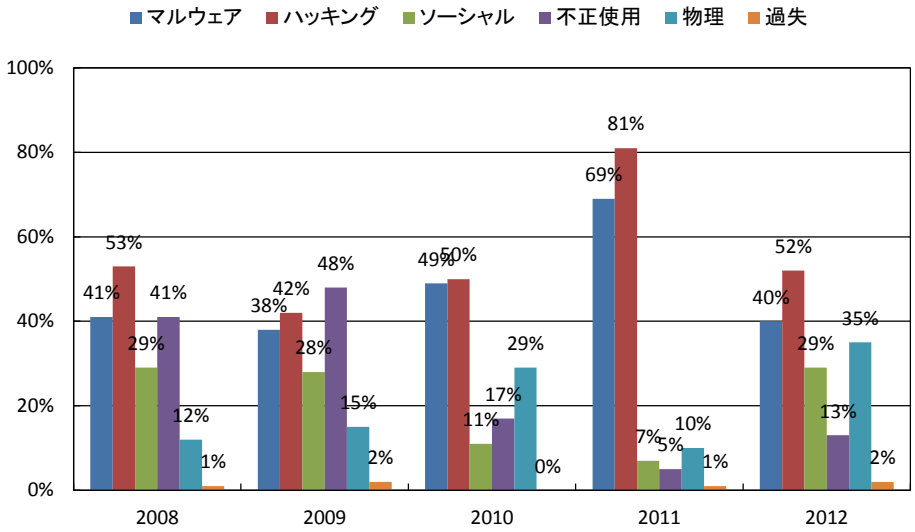
（出典）McAfee 社脅威レポート（2012 年第 4 四半期）



図表 4-2　マルウェア検体の増加状況（データベースに登録されたマルウェア検体の合計）

（出典）McAfee 社脅威レポート（2012 年第 4 四半期）

また、近年発生した情報漏えい／侵害事例の原因としマルウェアやハッキングなどの外部からの攻撃が多くを占める傾向にある。



※合計値が 100%を超えるのは、原因が複数にまたがる事例が多く存在するため。

（出典）Verizon 社 2013 DATA BREACH INVESTIGATIONS REPORT

近年は、スマートフォンやタブレット端末の普及や、ソーシャルメディアやクラウドコンピューティング等の利用拡大に伴い、これらを狙ったセキュリティ脅威の増加など、新たなリスクも表面化している。スマートフォンには、アプリケーションを安全に実行する制御の壁（サンドボックス）が設けられているが、アプリケーションインストール時等における利用者の権限許可項目の確認の怠り等による被害拡大も大きい。

4.1.2 情報セキュリティインシデント

先に述べた情報セキュリティを取り巻く環境の変化は、我が国の経済成長に対して多大な影響を与えるものであり、安心・安全な情報通信環境の確保に向け、時々刻々と変化する情報セキュリティ上の課題に対し、関係者が一体となった対策の強化が必要となっている。2012 年から 2013 年にかけて国内外で発生した主要なサイバー攻撃の事例を以下に示す。国家機密を標的とした攻撃から個人の情報・金銭を標的とした攻撃まで多岐にわたっている。スマートフォン等の普及により、個人レベルにおいても様々なセキュリティ脅威が顕在化しており、政府や企業だけでなく個人における情報セキュリティ対策が求められる時代になったと言える。

技術的な対策によりサイバー攻撃を防ぐことができていたが、昨今はシステムだけでなく、人間系を狙うなど攻撃が多様化しているため技術的に完全に防御することが困難になっている。このような攻撃側に有利な潮流は、システムや社会が大きく変換しなければ止

まらないと言われている。例えば、スマートフォンの個人情報を不正に取得する悪意あるアプリケーションが開発・提供され、実際に多くの人の情報が窃取された（The Movie 事件）が、このアプリケーションの開発や提供に関わった人らは不起訴となり、罪に問われなかったように、法制度の対処も遅れている。

2012 年 4 月～2013 年 3 月に発生した主要なサイバー攻撃事案を図表 4-3 に示す。

図表 4-3 主なサイバー攻撃事例（2012 年 4 月～2013 年 3 月）

時期	対象者（国）	概要
2012 年 4 月	政府等（中国）	「アノニマス」を名乗るハッカー集団が中国を攻撃の標的に定め、数百に及ぶ Web サイトを改ざんした。
2012 年 4 月	個人（日本）	スマートフォンに登録された電話番号などを無断で外部に送信するアプリが出回り、これまでに数百万人の個人情報が流出した恐れがあることが判明した。アプリには「the Movie」という文字が含まれていた。
2012 年 4 月	企業（日本）	顧客情報など様々な情報を管理しているグローバルコンピューターネットワークに対し、サイバー攻撃を受けていたことが判明した。
2012 年 5 月	政府（日本）	独立行政法人の Web サイトの一部が不正アクセスにより改ざんされた。
2012 年 6 月	政府（日本）	独立行政法人の業務用パソコン 19 台がマルウェアに感染し、外部に情報を送った可能性があることが判明した。
2012 年 6 月	自治体（日本）	自治体の Twitter アカウントが乗っ取られ、悪意の第三者がログインしていることが判明した。
2012 年 6 月	政府等（日本）	「アノニマス」を名乗るハッカー集団が日本の政府機関等のウェブサイトに対して、DDoS 攻撃やホームページの改ざんを行った。
2012 年 6 月～9 月	自治体等（日本）	大量殺人予告や爆破予告が自治体のサイトに書き込まれたりメールで送り付けられる。その後、マルウェアに感染したパソコンが外部から遠隔操作された結果であることが判明した。
2012 年 7 月	政府（日本）	中央省庁の職員が使用するパソコン 123 台がウイルスに感染し、外部サイトに向けて不審な通信を行っていたことが判明した。
2012 年 7 月	企業	韓国の通信会社の電算ネットワークがハッキングされ、携帯電話顧客 877 万人の個人情報が流出したこ

時期	対象者 （国）	概要
	（韓国）	とが判明した。
2012 年 8 月	企業 (サウジアラビア)	石油会社が、およそ 30,000 台にのぼる同社のワークステーションがサイバー攻撃の被害を受けたと認める声明を出した。
2012 年 9 月	政府等 （日本）	日本の公的機関や企業のウェブサイトがサイバー攻撃を受け、計 19 のサイトで閲覧障害や改ざんが確認された。
2012 年 10 月	大学 （各国）	「GhostShell」を名乗るハッカー集団が世界の有力 100 大学のサーバーから盗んだ情報 12 万件を、インターネットに掲載したと公言した。その中には日本国内の 5 大学も含まれていた。
2012 年 10 月	金融 （日本）	各銀行のインターネットバンキングのホームページ上で、顧客の暗証番号などの入力を求める偽の画面が表示され、不正送金が行われるケースが判明した。
2012 年 11 月	企業 （米国）	テレビ局のウェブサイトが「pyknik」と称するハッカーにより侵入され、コンテンツが改ざんされた。
2012 年 11 月	金融 （日本）	生命保険会社を退職した社員や代理店の保険販売員が同社のシステムに不正にアクセスしていたとの発表があった。
2012 年 11 月	政府 （日本）	独立行政法人のコンピューターがマルウェアに感染し、外部コンピューターに向けてデータを送信したことが判明した。
2012 年 11 月	国際機関	国際機関のサーバが何者かにハッキングされ、同機関と共に働いている専門家の連絡先などの情報が盗まれたと明らかにした。
2012 年 12 月	企業 （日本）	製造業で業務用パソコン 4 台が新種のウイルスに感染した。
2012 年 12 月	政府 （日本）	独立行政法人が保有する端末がウイルスに感染し、外部のサイトへ通信が行われていた旨発表した。

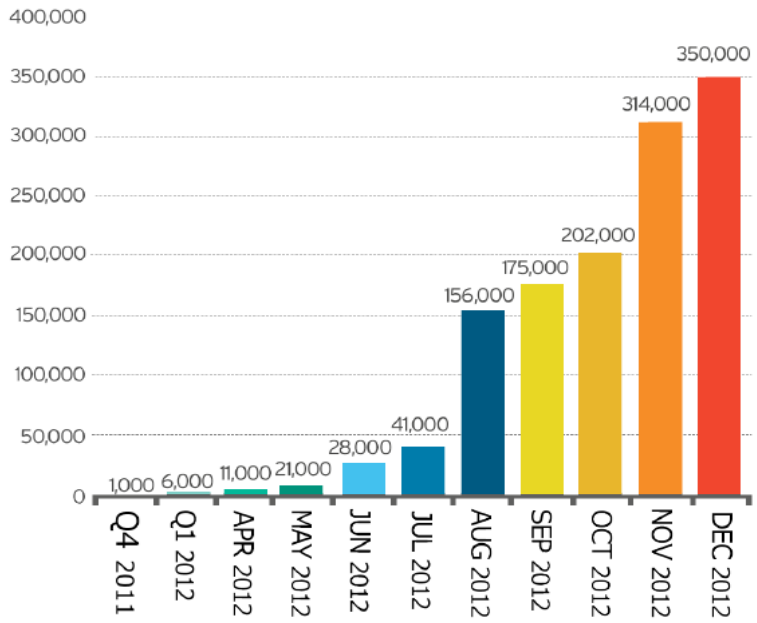
時期	対象者 （国）	概要
2012 年 12 月	企業 （日本）	マスコミの社内システムが不正アクセスを受け、同社が試験的に作成したデータが一時、閲覧できる状態にあった。
2012 年 12 月	企業 （日本）	マスコミの社員が利用するパソコンがウイルスに感染し、社員のメールの一部が外部に流出した可能性があると発表した。
2013 年 1 月	政府 （日本）	中央省庁の公用パソコンがサイバー攻撃を受け、機密文書が外部に流出した疑いがあることがわかった。
2013 年 1 月	政府 （米国）	「NullCrew」を名乗るハッカー集団が、政府機関などの Web サイトに不正アクセスした。
2013 年 1 月	企業 （日本）	企業のホームページの一部に不正アクセスがあり、会員約 47 万人分の個人情報を改ざんされたと発表した。
2013 年 1 月	政府 （日本）	独立行政法人が運用している Web サイトが外部からの不正アクセスによるサイバー攻撃を受け、一部のページが改ざんされた。
2013 年 1 月	自治体 （日本）	自治体でホームページの更新に必要なＩＤとパスワードが何らかの方法で盗まれ、海外のサーバーから不正アクセスを受けた。
2013 年 1 月	政府 （米国）	政府機関のウェブサイトに対して「アノニマス」がサイバー攻撃を行った。
2013 年 1 月	企業 （米国）	マスコミ各社が、中国からハッカー攻撃を受け続けていた旨を相次いで公表した。
2013 年 1 月	政府 （日本）	中央省庁のパソコンからインターネット上の外部サーバーへの不審な通信が確認され、パソコンから文書が流出した疑いがあることが判明した。
2013 年 2 月	企業	Twitter でユーザー情報を狙った不正アクセスが検出された。攻撃者はおよそ 25 万ユーザーのメール

時期	対象者 （国）	概要
	（米国）	アドレス、セッショントークン、暗号化したパスワードにアクセスした可能性があることが判明した。
2013 年 2 月	政府 （米国）	政府機関のサーバー14 台とワークステーション 20 台が不正侵入され、職員数百人の個人情報が流出した。
2013 年 2 月	政府 （米国）	政府機関がサイバー攻撃を受け、個人情報が流出した。
2013 年 2 月	企業 （日本）	企業のサーバーおよび PC 端末 17 台がウイルスに感染し、個人情報を含む営業情報と関連する技術情報が外部に漏えいした可能性があることが判明した。
2013 年 3 月	企業 （米国）	企業は外部からサーバーに不正アクセスを受け、利用者の ID やパスワード、メールアドレスなどが盗まれたおそれがあると発表した。
2013 年 3 月	企業 （日本）	EC サイトが不正アクセスを受け、最大 1 万 2036 件のクレジットカード情報が流出した可能性があると発表した。
2013 年 3 月	政府 （日本）	中央省庁が運営する Web サイトが改ざんされた。閲覧者のパソコン内の情報が盗まれた可能性がある。
2013 年 3 月	企業 （韓国）	銀行や放送局など複数のコンピュータ・ネットワークがサイバー攻撃とみられる攻撃を受けた。
2013 年 3 月	自治体 （日本）	自治体で学校や文化施設など計５３のホームページを管理するサーバーが外部から改ざんされた。
2013 年 3 月	民間 （欧州）	非営利団体のウェブサイトに DDoS 攻撃が行われ、同団体はウェブサイトの停止を余儀なくされた。

（出典）報道記事等をもとにみずほ情報総研作成

(a) スマートフォン等を標的とした不正プログラムの急増

スマートフォンやタブレット端末等の普及に伴い、これらを標的としたマルウェアやアプリが開発され、個人の保有する情報を窃取する事案が増加している。



図表 4-4 Android 向け不正プログラムの増加

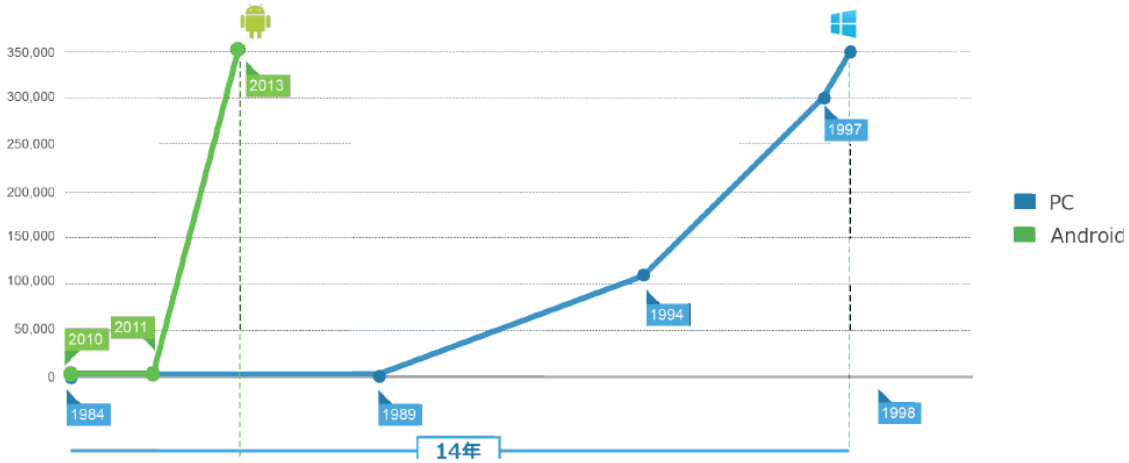
（出典）トレンドマイクロ社「2012 年間セキュリティラウンドアップ」

2012 年 4 月には、「the Movie」と名付けられたスマートフォン向けアプリが、端末に保存された電話帳データ等の個人情報を収集していると報道された。その多くが、人気のあるゲームを模倣したものや魅力的な動画コンテンツを閲覧できる等を謳い文句にしていた。同アプリは、Google が運営する公式マーケット上で配布され、少なくとも 6 万 6 千件以上のアプリがダウンロードされ、その結果、約 1,000 万件の個人情報が窃取されたと言われている。

また、スマートフォン等の端末内には個人に関する多種多様なデータを格納しているほか、最近では、私物端末を業務に持ち込んで利用する BYOD（Bring Your Own Device）の浸透により、ユーザー本人だけでなく知人や所属する組織、取引先等に関係する情報が保存されているケースもある。そのため、情報を窃取された場合、個人に関する情報に加え業務に関する様々な情報まで窃取される恐れがあるなど、新たな情報セキュリティリスクとなっている。

また、スマートフォン等を標的としたワンクリック詐欺も現れている。ユーザーの不安を煽り、画面に表示された連絡先に問い合わせるよう仕向けることにより、当該ユーザーの個人情報が窃取され、執拗な料金請求等につながるといった被害が発生している。

スマートフォン向けのセキュリティ脅威は急速に拡大している。トレンドマイクロ社のレポートによると、PC 向けの不正プログラム数が 14 年かけて 35 万に達したのに対し、Android 端末向け不正プログラム数は 3 年もかからずに到達している。



図表 4-5 不正プログラムの増加傾向

（出典）トレンドマイクロ社「2012 年間セキュリティラウンドアップ」

(b) ソーシャルメディア上における攻撃の出現

Facebook や Twitter 等のソーシャルメディアの普及に伴い、ソーシャルメディア上での新たな攻撃も現れている。例えば、Facebook の「いいね！」ボタンを悪用することでプライバシー情報の公開設定を変更するクリックジャック攻撃や Twitter のアカウントの乗っ取り、偽のアプリケーションの配布などソーシャルメディアの機能を悪用した攻撃が相次いで出現している。以下に、2012 年 4 月～2013 年 3 月までの主な Twitter 等のアカウント乗っ取り事案を示す。

図表 4-6 主なソーシャルメディアの乗っ取り事案（2012 年 4 月～2013 年 3 月）

時期	攻撃対象	概要
2013 年 3 月	英大手放送局	同社の 3 つの Twitter アカウント（ウェザーニュース、アラビア語ラジオ、ラジオ・アルスター）が乗っ取られた。
2013 年 2 月	米大手ファーストフード	Twitter アカウントがハッキングされ、アイコン等が競合企業のものに変更された。
2013 年 2 月	米大手自動車、メーカー	Twitter アカウントがハッキングされ、競合他社等の情報に変更された。

時期	攻撃対象	概要
2012 年 8 月	英大手報道機関	公式 Twitter アカウントの 1 つがハッキングされ、偽ツイートが 22 件投稿されたと発表した。
2012 年 6 月	ゆるキャラ	公式 Twitter が、何者かに乗っ取られる被害を受け、アカウントの乗っ取り対策として新しいアカウントに移行すると発表した。
2012 年 1 月	個人 (参院議員)	参院議員の youtube アカウントが乗っ取られ、何者かが動画投稿サイトに不正アクセスし、ロシア人女性とみられるポルノ広告を掲載していたことが判明した。
2011 年 12 月	個人 (ミュージシャン)	Twitter 及び Facebook アカウントがハッキングされ、フォロワーや友人にリンク入りのスパムメッセージを送信していた。
2011 年 10 月	個人 (タイ首相)	Twitter アカウントがハッキングされ、首相の洪水対策や教育政策などを批判するタイ語の文章が投稿された。
2011 年 7 月	米大手製薬会社	Facebook アカウントがハッキングされた。

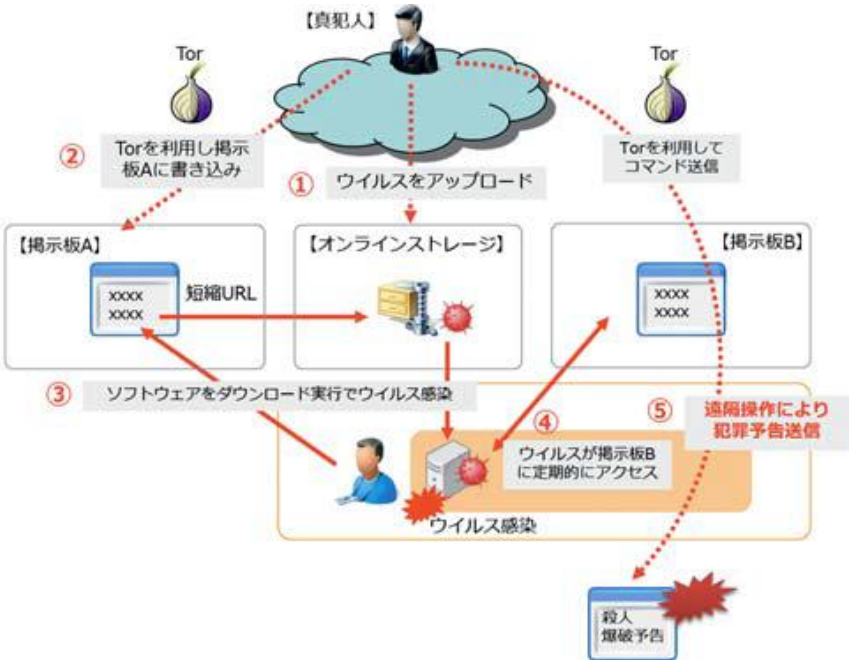
（出典）報道記事等をもとにみずほ情報総研作成

(c) 遠隔操作ウイルスによる攻撃

2012 年は、個人を標的とした「遠隔操作ウイルス事件」が大きな注目を集めた。この事件では、他人のパソコンにウイルスを侵入させ、そのパソコンを遠隔操作する「なりすまし」により、公共機関のウェブサイトや掲示板に犯罪予告が書き込まれた。その後、ウイルスに感染したパソコンの所有者 4 名が逮捕されるなど、報道等で大きく取り上げられ、社会問題にも発展した。

このウイルスは、別の無料レンタル掲示板経由で感染した PC をコントロールすることができ、遠隔から犯罪予告の送信等を行わせることが可能になっている。このように、インターネット経由で遠隔操作ができるという特徴を持っていることから、この事件で利用されたウイルスは「遠隔操作ウイルス」あるいは「なりすましウイルス」と呼ばれている。

掲示板への書き込みやウイルスに感染した PC に対する命令の送信等について、発信元を隠ぺいする匿名化技術が使われていることが特徴であり、送信元や通信経路を追跡することが非常に困難になり、真犯人特定を難しくしている要因にもなっている。



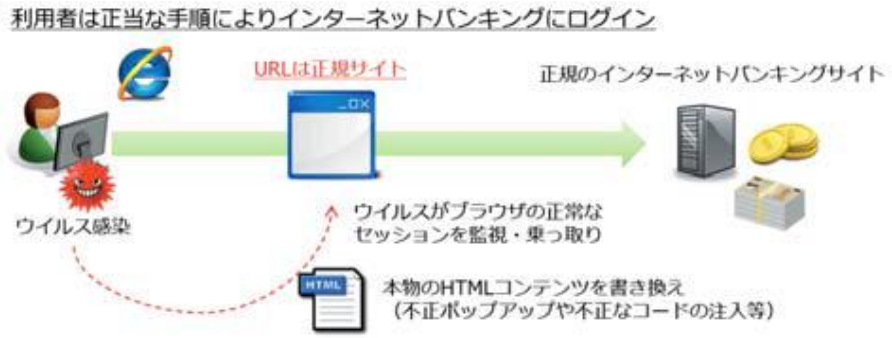
図表 4-7　遠隔ウイルス事件の概要

（出典）「個人を狙ったウイルスの最新動向」（ITU ジャーナル　2013 年 3 月号）

(d)　インターネットバンキングを狙った情報窃取

2012 年度に個人を標的としたサイバー攻撃として注目を浴びた事案に、インターネットバンキングを狙った情報窃取がある。利用者がインターネットバンキングサイトにログインする際、偽装したポップアップ画面を表示し、第二暗証番号や秘密の質問等を不正に窃取するものである。一部の金融機関においては、顧客の口座から別口座に対して不正送金・出金が行われていたことが確認されている。

従来のフィッシングとは異なり、利用者が正当な手順でインターネットバンキングサイトにログインしたにも関わらず、不正なポップアップが表示される点が特徴である。



図表 4-8　インターネットバンキングを狙った情報窃取の概要

（出典）「個人を狙ったウイルスの最新動向」（ITU ジャーナル　2013 年 3 月号）

4.2　パーソナルデータの保護に関する調査

従来、ネット利用に際して、不正利用時にプライバシー被害が大きな情報は、「氏名」「住所」「顔写真」「実名のメールアドレス」とされてきたが、ソーシャルメディアやスマートフォンの利用が活発になるにつれて、最近では「固定 IP アドレス」や「実名 SNS の ID」や「端末識別 ID（UDID、android　ID など)」も重視されるようになっている。

特に端末識別 ID は、ユーザー認証や広告配信などサービスの識別用に使われており、個人を特定できる情報とひも付けがしやすい。

また、ネットを経由して膨大なデータが収集・蓄積されており、事業者にとって新たなビジネスの可能性を有しているが、個人情報やプライバシーの扱いはリスクも伴うため、活用について慎重な姿勢を示している企業が多いのが実態である。このような中で、個人情報の利用目的を開示、積極的に情報を収集利用することでユーザーからの信頼を得、新規ビジネスを立ち上げている企業もあり対応が二極化しつつある。

本調査では、文献情報を用いて国内外の事例収集を行うとともに、国内学識者に対してヒアリングにより情報収集・確認を行った。下記に実施したヒアリング対象者を示す。下記のヒアリング対象者に対して、2 回ずつ、計 4 回のヒアリングを実施した。

図表 4-9　ヒアリング対象

ヒアリング対象者	対象者の経歴
石井 夏生利氏	• 筑波大学　図書館情報メディア系　准教授 • プライバシー、個人情報保護法、情報セキュリティ法等の研究に従事 • 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」委員 • 経済産業省パーソナルデータ WG 委員
新保　史生氏	• 慶應義塾大学総合政策学部教授 • 総務省「パーソナルデータの利用・流通に関する研究会」委員 • 「スマートフォンの利用者情報等に関する連絡協議会」議長 • 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」副委員長

4.2.1　パーソナルデータの保護に関する動向

パーソナルデータの利活用については多くの可能性が期待されている一方で、プライバシーの保護等の観点から様々な課題も指摘されている。例えば、急速に普及しているスマートフォンは、常にネットワークに接続された状態で持ち歩くことから、パソコンに比べ

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数の情報の取得も可能となっている。また、2011 年頃より、スマートフォンにおける利用者情報の取り扱いに関し、議論となった事例が多く報道され、我が国においても利用者の関心が高まってきている。以下に、報道等により注目を集めた事案を示す。

図表 4-10 スマートフォンにおける利用者情報の取扱に関し注目された事案

アプリ名	時期	概要
全国共有電話帳	2012 年 12 月	「全国共有電話帳」は、昨年 10 月、76 万人のデータが流出と騒がれた「全国電話帳」のリメーク版。アプリを導入すると自分のアドレス帳に登録された情報が、登録者全員に共有される。自分自身は公開を OK したとしても、アドレス帳に入っている知人友人、親兄弟は、まったくの無許可で公開されてしまう。
comm	2012 年 10 月	「当社は、すべてのｃｏｍｍ会員記述情報を無償で複製その他あらゆる方法により利用し、また、第三者に利用させることができるものとします」との利用規約が問題とされた。規約は修正済み。
全国電話帳	2012 年 9 月	アプリ自体は、ハローページとタウンページに掲載された情報を元に作成されているが、インストールした利用者のスマホに登録された電話番号や住所、メールアドレスなどが抜き取られ、利用者間で閲覧できる仕組みになっていた。
アップティービー	2012 年 4 月	ユーザーの端末情報を無断で取得し、これをデータコンサルティングやターゲティング広告に利用した。
ビューン	2012 年 1 月	電子書籍閲覧ソフトが、利用者が読んだ雑誌などの内容やページごとの閲覧時間を無断で記録し送信した。
マガストア	2012 年 1 月	販売した電子書籍の書籍内の閲覧動向を収集した。
金魚すくいゲーム	2011 年 11 月	全地球測位システム（GPS）で測定されたスマホの位置情報を１分間に１回、米国の広告会社に送信。アプリは端末の操作で楽しむ金魚すくいゲームで、ゲームに位置情報は必要ない。
産経新聞 iPhone 版	2011 年 11 月	2011 年 11 月に公開したアプリの最新版 3.0.0 に、利用者のページ閲覧履歴を収集し、サーバーに送信する機能が付いていることが明らかになった。
カレログ	2011 年 9 月	恋愛支援アプリと称し、位置情報、バッテリー残量、アプリ一覧、通話記録の外部閲覧が可能であったため問題となった。

（出典）報道記事等をもとにみずほ情報総研作成

事業者側の対応として、現在、端末に保存された利用者情報へのアクセスは、各 OS により異なる制限が行われている。アプリケーション提供サイト運営事業者では、掲載するアプリケーションについて、一定の審査やポリシーが存在している。

一方、アプリケーションが端末内の利用者情報を収集するためのアプリケーションプログラムインタフェース（API）機能が開発者に公開されており、API を用いた情報収集は比較的容易である。収集した情報を含めネットワークに常時接続されるため、クラウドベースの外部サーバーと連携したサービスの構築も容易となっている。

4.2.2　我が国におけるパーソナルデータの利活用をめぐる課題

パーソナルデータの利活用に関する大きな課題として、パーソナルデータの利活用のルールが明確でないため、パーソナルデータを利活用したい企業にとっては、どのような利活用であれば適正といえるかを判断することが困難であることがある。また、利用される側の消費者にとっては、パーソナルデータが適正に取り扱われ、プライバシー等が適切に保護されているかが不明確になることにより、懸念が生じている。

パーソナルデータの利活用において問題となり得るのは、利活用される情報が特定の個人と関連性が高い場合である。パーソナルデータの利活用におけるプライバシー等に係るルールが必ずしも明確でなく、パーソナルデータの利用・流通の過程において、特定の個人との結びつきの強弱を容易に判断することが困難な場合、取扱いに係る判断に困難な問題が生じる可能性がある。特に、パーソナルデータが、第 3 者等により二次利用、三次利用されるような場合において、個別のデータが特定の個人との結びつきが弱かったとしても、多くのデータが集積・分析されることにより、個人識別性が生じるなど特定の個人との関連性が高まる可能性を含んでいる。二次利用者、三次利用者等が消費者の同意を取得すること等は困難であるため、パーソナルデータの利活用に係る取得・流通・利活用までの全体の仕組みの中で適正な取扱いを確保することが求められる。

以上

＜参考資料＞

Q1 - Q1

あなたの性別をお答えください。（回答はひとつ）

❍ 男性（1）
❍ 女性（2）

Q2 - Q2

あなたの年齢をお答えください。（回答はひとつ）

❍ 19 歳以下（1）
❍ 20～24 歳（2）
❍ 25～29 歳（3）
❍ 30～34 歳（4）
❍ 35～39 歳（5）
❍ 40～44 歳（6）
❍ 45～49 歳（7）
❍ 50～54 歳（8）
❍ 55～59 歳（9）
❍ 60～64 歳（10）
❍ 65～69 歳（11）
❍ 70～74 歳（12）
❍ 75 歳以上（13）

Q3 - Q3

あなたの職業をお答えください。（回答はひとつ）

❍ 会社役員（1）
❍ 会社社員（2）
❍ 自営業（3）
❍ 専門職（4）
❍ 公務員（5）
❍ 学生（6）
❍ 専業主婦（7）
❍ パート・アルバイト（8）
❍ 無職（9）

❍ その他（10)_____

Q3A - Q3A

あなたのご家庭の世帯年収をお答えください。（回答はひとつ）

❍ 200 万未満（1)
❍ 200～300 万円未満（2)
❍ 300～400 万円未満（3)
❍ 400～500 万円未満（4)
❍ 500～600 万円未満（5)
❍ 600～700 万円未満（6)
❍ 700～800 万円未満（7)
❍ 800～1000 万円未満（8)
❍ 1000～1200 万円未満（9)
❍ 1200～1500 万円未満（10)
❍ 1500～2000 万円未満（11)
❍ 2000 万円以上（12)
❍ わからない（13)

Q3B - Q3B

あなたの最終学歴をお答えください。（回答はひとつ）

❍ 小学校以下（1)
❍ 中学校（2)
❍ 高校・高専（3)
❍ 専門学校（4)
❍ 短期大学（5)
❍ 大学（6)
❍ 大学院 （修士）（7)
❍ 大学院 （博士）（8)
❍ その他（9)

Q4 - Q4

あなたは普段どのような機器でインターネットに接続していますか？ （回答はあてはまるものすべて）

❑ パソコン（1)

❑ スマートフォン（Android、iPhone、Blackberry、Windows Phone、Windows Mobile 等）(2)
❑ スマートフォン以外の携帯電話・PHS (3)
❑ タブレット端末 (4)
❑ テレビ (5)
❑ ゲーム機 (6)
❑ その他 (7)_____

Q4A - Q4A

あなたが利用しているスマートフォンの OS（オペレーティングシステム）はどちらですか。（回答はあてはまるものすべて）

❑ Android (1)
❑ iOS（iPhone） (2)
❑ Blackberry (3)
❑ Windows Phone、Windows Mobile (4)
❑ Symbian (5)
❑ その他 (6)_____
❍ わからない (7)

Q5 - Q5

利用している通信回線をすべてお答えください。（回答はあてはまるものすべて）

❑ 電話回線 (1)
❑ ケーブルテレビ回線 (2)
❑ FTTH（光回線） (3)
❑ ADSL (4)
❑ 携帯電話回線（2G） (5)
❑ 携帯電話回線（3G） (6)
❑ 携帯電話回線（LTE） (7)
❑ 高速無線通信（WiMAX） (8)
❑ Wi-Fi 回線 (9)
❑ その他 (10)_____
❍ わからない (11)

Q6 - Q6

あなたのソーシャルメディアの利用頻度、インターネットショッピング（EC サイト）の利用頻度、インターネット全般の利用頻度であてはまるものをお答えください。

（回答はそれぞれひとつ）

※ソーシャルメディア（SNS（ソーシャルネットワーキングサービス）、ブログ、マイクロブログ（Twitter 等））や EC サイトの利用については、
閲覧しただけでも 1 回利用と考えてください。

回答は横方向に

	ほとんど毎日利用（1）	週に 3～4 回くらい利用（2）	週に 1～2 回くらい利用（3）	月に 2～3 回くらい利用（4）	月に 1 回程度利用（5）	月に 1 回未満の利用（6）
ソーシャルメディアの利用頻度（1）	❍	❍	❍	❍	❍	❍
インターネットショッピング（EC サイト）の利用頻度（2）	❍	❍	❍	❍	❍	❍
インターネット全般の利用頻度（3）	❍	❍	❍	❍	❍	❍

Q7 - Q7

インターネット接続機器やインターネットの取扱いのレベルについて､最も近いものを選んで下さい。（回答はひとつ）

❍ インターネット接続機器やインターネット接続でのトラブルが起きても、自分で解決できることが多く、困っている人へのアドバイスもできる。（1）
❍ インターネット接続機器やインターネット接続等でのトラブルが起きても、説明書やアドバイスがあれば、ある程度は自分で解決できる。（2）
❍ トラブルへの対応は難しいが、ソフトウェアのインストールやネットワーク関係の設定等、説明書やアドバイスがあれば機器等の設定がある程度は自分でできる。（3）
❍ 機器等の設定は難しいが、メールの送受信、ホームページの閲覧、文章作成などインターネット接続機器やインターネットを利用することには支障がないレベルである。（4）
❍ メールの受信や特定のホームページの閲覧など、ごく簡単（定型的）な操作はできるが、状況に応じて利用方法を工夫することは難しい。（5）

Q8 - Q8

インターネットをどの程度使いこなしていますか。
自身の情報収集・発信のレベルについて、最も近いものを選んで下さい。（回答はひとつ）

❍ メールの送信、ブログ・SNS（ソーシャルネットワーキングサービス）等の書込みなど、自ら情報発信を積極的に行っている。 (1)
❍ メールの送受信、ホームページ・ブログ・SNS 等の閲覧・書込みなど、ネット利用には支障はないレベルである。 (2)
❍ メールの受信や、情報の検索、特定のホームページ・ブログ・SNS 等の閲覧など、情報収集目的の利用は自分ひとりで可能であるが、自ら情報を発信するような利用は難しい。 (3)
❍ メールの受信や、情報の検索、特定のホームページ・ブログ・SNS 等の閲覧など、情報収集目的の利用について、誰かの補助や助言があれば実施できる。 (4)
❍ 上記のようなことをやった経験がほとんどない。 (5)

Q9 - Q9

あなたはインターネットをどのような目的で利用していますか。(回答はあてはまるものすべて)

❑ 電子メールの送受信 (1)
❑ ホームページ（ウェブ）の閲覧 (2)
❑ SNS、ブログ、マイクロブログ（Twitter 等）の閲覧 (3)
❑ SNS、ブログ、マイクロブログ（Twitter 等）の書込み・情報更新 (4)
❑ 動画投稿・共有サイト（Youtube 等）の閲覧 (5)
❑ 動画投稿・共有サイト（Youtube 等）の投稿 (6)
❑ ラジオ、テレビ番組、動画のインターネット配信サービスの利用 (7)
❑ 電子ファイルの交換・ダウンロード（Ｐ２Ｐ、ＦＴＰなど） (8)
❑ 商品・サービスの購入・取引（amazon 等のネットショッピングの利用。ただし、金融取引を除く。） (9)
❑ ネットオークションの利用 (10)
❑ 金融取引（ネットバンキング、ネットトレード等） (11)
❑ デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の購入 (12)
❑ デジタルコンテンツの入手・聴取（無料のもの） (13)
❑ オンラインゲーム（ネットゲーム）への参加 (14)
❑ 電子政府・電子自治体の利用（電子申請、電子申告、電子届出） (15)
❑ 地図情報提供サービス（有料・無料を問わない。乗換案内、ルート検索サービスも含む） (16)
❑ その他 (17)_____

Q10 - Q10

ここ最近（１年以内を目処）で利用しているソーシャルメディアであてはまるものをお答えください。（回答はあてはまるものすべて）

❑ Facebook (1)
❑ Google+ (2)

❑ Twitter　(3)
❑ LinkedIn　(4)
❑ ブログ　(5)
❑ YouTube　(6)
❑ USTREAM (7)
❑ その他のソーシャルメディア　(8)_____
❍ これまでにソーシャルメディアを利用したことはない (9)

Q11 - Q11

ここ最近 1 年以内で､インターネットショッピングで購入した商品についてあてはまるものをお答えください。（回答はあてはまるものすべて）

❑ 【商品・サービス】 (a)
❑ パソコン関連 (1)
❑ 書籍・CD・DVD・ブルーレイディスク (2)
❑ 化粧品・衣料品・アクセサリー類 (3)
❑ 食料品 (4)
❑ 趣味関連・雑貨 (5)
❑ 各種チケット・クーポン・商品券 (6)
❑ 旅行関係 (7)
❑ 金融取引 (8)
❑ その他　（家具、家電製品、自動車） (9)_____
❑
【デジタルコンテンツ】 (b)
❑ ソフトウェア・アプリ (10)
❑ 音楽 (11)
❑ 映像 (12)
❑ 電子書籍 (13)
❑ ゲーム (14)
❑ 地図情報提供サービス (15)
❑ その他のデジタルコンテンツ (16)_____
❑
(c)
❍ インターネットショッピングを利用していない (17)

Q12 - Q12

あなたに関連する情報の中で、個人情報（パーソナルインフォメーション）であると考える情報をお答えください。（回答はあてはまるものすべて）

- ❑ 氏名（1）
- ❑ 性別（2）
- ❑ 住所（3）
- ❑ 生年月日（4）
- ❑ 国籍（5）
- ❑ 職歴（6）
- ❑ メールアドレス（7）
- ❑ 電話番号（8）
- ❑ 会社名（9）
- ❑ 学校名（10）
- ❑ 役職（11）
- ❑ 資格（12）
- ❑ 健康状態（13）
- ❑ 学歴（14）
- ❑ 趣味（15）
- ❑ 個人識別番号（国民 ID 等）(16)
- ❑ 顔（生体情報）（17）
- ❑ 虹彩（生体情報）（18）
- ❑ 網膜（生体情報）（19）
- ❑ 指紋（生体情報）（20）
- ❑ 静脈（生体情報）（21）
- ❑ 身長（22）
- ❑ 体重（23）
- ❑ 血液型（24）
- ❑ 位置情報（25）
- ❑ 行動履歴（26）
- ❑ 口座情報（27）
- ❑ クレジットカード番号（28）
- ❑ 年収・所得（29）
- ❑ 借金（30）
- ❑ 家族関係（31）
- ❑ 友人関係（32）
- ❑ 交際関係（33）
- ❑ 同窓会情報（34）
- ❑ 思想信条（35）
- ❑ 宗教（36）
- ❑ 性癖（37）
- ❑ 労組加入事実（38）
- ❑ 病歴・病状（39）
- ❑ その他（40）_____

Q12A - Q12A

Q12 でお答えいただいた情報の取扱いについてお尋ねします。
あなたの考えにもっとも近いものをお答えください。（回答はそれぞれひとつ）

回答は横方向に

	公開してもよい（1）	条件によってサービス提供事業者に提供してもよい（2）	どんな場合でも提供・公開したくない（3）
氏名（1）	❍	❍	❍
性別（2）	❍	❍	❍
住所（3）	❍	❍	❍
生年月日（4）	❍	❍	❍
国籍（5）	❍	❍	❍
職歴（6）	❍	❍	❍
メールアドレス（7）	❍	❍	❍

	公開してもよい (1)	条件によってサービス提供事業者に提供してもよい (2)	どんな場合でも提供・公開したくない (3)
電話番号 (8)	❍	❍	❍
会社名 (9)	❍	❍	❍
学校名 (10)	❍	❍	❍
役職 (11)	❍	❍	❍
資格 (12)	❍	❍	❍
健康状態 (13)	❍	❍	❍
学歴 (14)	❍	❍	❍
趣味 (15)	❍	❍	❍
個人識別番号（国民 ID 等) (16)	❍	❍	❍
顔（生体情報） (17)	❍	❍	❍
虹彩（生体情報） (18)	❍	❍	❍
網膜（生体情報） (19)	❍	❍	❍
指紋（生体情報） (20)	❍	❍	❍
静脈（生体情報） (21)	❍	❍	❍
身長 (22)	❍	❍	❍
体重 (23)	❍	❍	❍
血液型 (24)	❍	❍	❍
位置情報 (25)	❍	❍	❍
行動履歴 (26)	❍	❍	❍
口座情報 (27)	❍	❍	❍
クレジットカード番号 (28)	❍	❍	❍
年収・所得 (29)	❍	❍	❍
借金 (30)	❍	❍	❍
家族関係 (31)	❍	❍	❍
友人関係 (32)	❍	❍	❍
交際関係 (33)	❍	❍	❍
同窓会情報 (34)	❍	❍	❍
思想信条 (35)	❍	❍	❍
宗教 (36)	❍	❍	❍

	公開してもよい (1)	条件によってサービス提供事業者に提供してもよい (2)	どんな場合でも提供・公開したくない (3)
性癖 (37)	❍	❍	❍
労組加入事実 (38)	❍	❍	❍
病歴・病状 (39)	❍	❍	❍
その他(40)	❍	❍	❍

Q12B - Q12B

Q12A 設問でひとつでも「２．条件によってサービス提供者に提供してもよい」と回答した情報についてお尋ねします。

どのような条件であればサービス提供事業者に情報を提供してもよいと思いますか。
あてはまるものをお答えください。（回答はあてはまるものすべて）

❑ 情報を提供することで利便性が向上する場合 (1)
❑ 情報を提供することで経済的なメリットを享受できる場合 (2)
❑ 情報を提供することで社会に貢献できる場合 (3)
❑ 情報の提供先が信頼できる場合 (4)
❑ その他 (5)_____

Q13 - Q13

普段、あなたは下記のような様々なインターネットの利活用場面で、個人情報（パーソナルインフォメーション）の取り扱いについて不安に思うことはありますか。
（回答はあてはまるものすべて）

❑ 電子メールの送受信 (1)
❑ ホームページ（ウェブ）の閲覧 (2)
❑ SNS、ブログ、マイクロブログ（Twitter 等）の閲覧 (3)
❑ SNS、ブログ、マイクロブログ（Twitter 等）の書込み・情報更新 (4)
❑ 動画投稿・共有サイト（Youtube 等）の閲覧 (5)
❑ 動画投稿・共有サイト（Youtube 等）の投稿 (6)
❑ ラジオ、テレビ番組、動画のインターネット配信サービスの利用 (7)
❑ 電子ファイルの交換・ダウンロード（Ｐ２Ｐ、ＦＴＰなど） (8)
❑ 商品・サービスの購入・取引（amazon 等のネットショッピングの利用。ただし、金融取引を除く。） (9)
❑ ネットオークションの利用 (10)

❑ 金融取引（ネットバンキング、ネットトレード等）（11）
❑ デジタルコンテンツ（音楽・音声、映像、ゲームソフト等）の購入（12）
❑ デジタルコンテンツの入手・聴取（無料のもの）（13）
❑ オンラインゲーム（ネットゲーム）への参加（14）
❑ 電子政府・電子自治体の利用（電子申請、電子申告、電子届出）（15）
❑ 地図情報提供サービス（有料・無料を問わない。乗換案内、ルート検索サービスも含む）（16）
❑ その他（17）_____
❍ 不安に思うことはない（18）

Q14 - Q14

あなたが、個人情報（パーソナルインフォメーション）の取り扱いに不安を感じる理由としてもっともあてはまるものを選択してください。（回答はひとつ）

❍ ご自身の個人情報（パーソナルインフォメーション）が公開・共有される可能性があるから（1）
❍ ご自身の個人情報（パーソナルインフォメーション）が利用される可能性があるから（2）
❍ ご自身の個人情報（パーソナルインフォメーション）が売買される可能性があるから（3）
❍ ご自身の個人情報（パーソナルインフォメーション）が漏洩する可能性があるから（4）
❍ ご自身の個人情報（パーソナルインフォメーション）が収集・蓄積される可能性があるから（5）
❍ その他（6）_____
❍ 不安を感じていない（7）

Q15 - Q15

インターネット上で公開・提供したくない、または公開・提供しないようにしている、あなたの位置に関する情報であてはまるものはありますか。
（回答はあてはまるものすべて）

❑ 自宅周辺（1）
❑ 自宅最寄り駅周辺（2）
❑ 職場・学校周辺（3）
❑ 職場・学校最寄り駅周辺（4）
❑ 家族・親戚の家の周辺（5）
❑ 交際中のパートナーの家周辺（6）
❑ 思想信条・宗教に関する場所（7）
❑ 病院（8）
❑ その他（9）_____

❍ 常に公開・提供しないよう意識している（10）
❍ 特にない（11）

Q16 - Q16

あなたの個人情報（パーソナルインフォメーション）の利用・取扱いの考え方として、もっとも近いものを選択してください。（回答はひとつ）

❍ プライバシーについて意識をもち、個人情報（パーソナルインフォメーション）は隠すべきと考えている（1）
❍ プライバシーの価値を理解しているが、条件が整えば企業や組織に個人情報（パーソナルインフォメーション）を提供し、活用させることを認める（2）
❍ プライバシーの価値を理解しているが、提供には寛容である（3）
❍ プライバシーについて十分に意識していない（4）
❍ プライバシーに価値を認めていない（5）

Q17 - Q17

あなたの個人情報（パーソナルインフォメーション）について、サービス提供事業者からサービス向上等のため利用を求められた場合、
どのような利用方法に抵抗感を感じますか。
あてはまるものを選択してください。（回答はあてはまるものすべて）

❑ 閲覧される（1）
❑ 収集・蓄積される（2）
❑ 公開される（3）
❑ 分析される（4）
❑ 売買される（5）
❑ その他（6）_____
❍ 特に感じない（7）

Q18 - Q18

インターネットサービスの利用中に、プライバシーを侵害された経験はありますか。
プライバシーを侵害されたと疑わしいと思う場合も含めてお答えください。（回答はひとつ）

❍ ある（1）
❍ ない（2）

Q18A - Q18A

どのように対策されましたか。あてはまるものをお答えください。（回答はあてはまるものすべて）

❑ サービスの利用をやめた（1）
❑ サービス提供事業者を変えた（2）
❑ サービス管理者に連絡して情報を削除してもらった（3）
❑ サービスのプライバシー設定を変えた（4）
❑ サービス提供事業者に問い合わせた（相談した）（5）
❑ 事業者団体の相談窓口に問い合わせた（相談した）（6）
❑ 公的機関の相談窓口に問い合わせた（相談した）（7）
❑ 技術的な対策を取った（機密性の高い通信を行う等）　（8）
❑ その他（9）_____
❍ どうしてよいか分からなかった（特に対策していない）（10）

Q19 - Q19

個人情報（パーソナルインフォメーション）を保護するために日常から対策を講じていますか。（回答はあてはまるものすべて）

❑ サービス提供事業者のプライバシーポリシー（個人情報保護方針）、セキュリティポリシーを確認している（1）
❑ サービス提供事業者やサービスが信頼できるかを事前に評価サイトや相談窓口等を通して確認している（2）
❑ 自身の中で、公開できる個人情報（パーソナルインフォメーション）の範囲を定めている（3）
❑ 自身の中でサービス提供事業者に提供できる個人情報（パーソナルインフォメーション）の範囲を定めている（4）
❑ その他（5）_____
❍ 特に対策を行っていない（6）

Q20 - Q20

ソーシャルメディアを利用する際に登録したご自身の個人情報（パーソナルインフォメーション）や、
これまでに書き込んだ個人情報（パーソナルインフォメーション）のうち、あてはまるものをお答えください。
（回答はあてはまるものすべて）

❑ 氏名（1）　❑ 学校名　❑ 家族関係（19）
❑ 性別（2）　（10）　❑ 友人関係（20）

❑ 住所（3）
❑ 生年月日（4）
❑ 国籍（5）
❑ 職歴（6）
❑ メールアドレス（7）
❑ 電話番号（8）
❑ 会社名（9）
❑ 役職（11）
❑ 資格（12）
❑ 所得（13）
❑ 健康状態（14）
❑ 学歴（15）
❑ 趣味（16）
❑ 位置情報（17）
❑ 行動履歴（18）
❑ 交際関係（21）
❑ 同窓会情報（22）
❑ 思想信条（23）
❑ 宗教（24）
❑ 労組加入事実（25）
❑ その他（26）_____
❍ 個人情報（パーソナルインフォメーション）を登録したことはない（27）

Q21 - Q21

ソーシャルメディアを利用する際に、あなたの個人情報（パーソナルインフォメーション）が以下のように取り扱われることについて、
プライバシーの観点からどのように感じますか。
もっともあてはまるものをお答えください。（回答はそれぞれひとつ）

回答は横方向に

	許容できる（1）	条件によっては許容できる（2）	どんな場合でも許容できない（3）
ソーシャルメディアで第三者に実名が公開されること（1）	❍	❍	❍
ソーシャルメディアで趣味や交友関係等が公開されること（2）	❍	❍	❍
一度ソーシャルメディア上で顔写真を登録すると、顔認識技術を使って同じ顔が映っている写真があれば本人の同意を得ることなく、タグ付けされる（写真に写っている人の氏名を自動的に表示する）こと（3）	❍	❍	❍
ソーシャルメディア等への書き込みを企業や学校関係者が閲覧し、進学や就職の結果に影響を及ぼすこと（4）	❍	❍	❍
ソーシャルメディア上で利用者が非公開設定していた情報を事前の同意を得ることなく、すべての利用者が閲覧できるようサービス提供事業者が設定変更すること（5）	❍	❍	❍

	許容できる (1)	条件によっては許容できる (2)	どんな場合でも許容できない (3)
ソーシャルメディアやブログ等に書き込まれた個人情報（パーソナルインフォメーション）等を収集・販売し、プロファイリング情報として顧客サービスに利用されること (6)	❍	❍	❍

Q21A - Q21A

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はそれぞれあてはまるものすべて）

回答は横方向に

	利便性が向上すれば許容できる (1)	経済的なメリットを享受できれば許容できる (2)	社会への貢献が認められるのであれば許容できる (3)	情報の提供先が信頼できれば許容できる (4)
Q21A_1 - ソーシャルメディアで第三者に実名が公開されること	❑	❑	❑	❑
Q21A_2 - ソーシャルメディアで趣味や交友関係等が公開されること	❑	❑	❑	❑
Q21A_3 - 一度ソーシャルメディア上で顔写真を登録すると、顔認識技術を使って同じ顔が映っている写真があれば本人の同意を得ることなく、タグ付けされる（写真に写っている人の氏名を自動的に表示する）こと	❑	❑	❑	❑
Q21A_4 - ソーシャルメディア等への書き込みを企業や学校関係者が閲覧し、進学や就職の結果に影響を及ぼすこと	❑	❑	❑	❑
Q21A_5 - ソーシャルメディア上で利用者が非公開設定していた情報を事前の同意を得ることなく、すべての利用者が閲覧で	❑	❑	❑	❑

	利便性が向上すれば許容できる (1)	経済的なメリットを享受できれば許容できる (2)	社会への貢献が認められるのであれば許容できる (3)	情報の提供先が信頼できれば許容できる (4)
きるようサービス提供事業者が設定変更すること				
Q21A_6 - ソーシャルメディアやブログ等に書き込まれた個人情報(パーソナルインフォメーション）等を収集・販売し、プロファイリング情報として顧客サービスに利用されること	❑	❑	❑	❑

Q22 - Q22

インターネットショッピング（EC サイト）を利用する際にご自身の個人情報（パーソナルインフォメーション）を登録しましたか。
どの情報を登録したかあてはまるものをお答えください。（回答はあてはまるものすべて）

❑ 氏名 (1)
❑ 性別 (2)
❑ 住所 (3)
❑ 生年月日 (4)
❑ メールアドレス (5)
❑ 電話番号 (6)
❑ 会社名 (7)
❑ 学校名 (8)
❑ 行動履歴 (9)
❑ 口座情報 (10)
❑ クレジットカード番号 (11)
❑ 年収・所得 (12)
❑ 借金 (13)
❑ その他 (14)_____
❍ 個人情報（パーソナルインフォメーション）を登録したことはない (15)

Q22A - Q22A

インターネットショッピング（EC サイト）を利用する際に、あなたの個人情報（パーソナルインフォメーション）が以下のように取り扱われることについて、
プライバシーの観点からどのように感じますか。
もっともあてはまるものをお答えください。（回答はそれぞれひとつ）

※EC サイト等、インターネット上の各種サイトでは、あなたに関する情報を収集し、嗜好や趣味にマッチした情報を提供する行動ターゲティング広告（Behavioral Targeting Advertising, BTA）が提供されています。

回答は横方向に

	許容できる (1)	条件によっては許容できる (2)	どんな場合でも許容できない (3)
クレジットカード情報等の決済情報をインターネット上で登録すること (1)	❍	❍	❍
ネットスーパー等での購買履歴の情報を、商品のレコメンドやターゲティング広告表示（※）に活用されていること (2)	❍	❍	❍

Q22B - Q22B

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はそれぞれあてはまるものすべて）

回答は横方向に

	利便性が向上すれば許容できる (1)	経済的なメリットを享受できれば許容できる (2)	社会への貢献が認められるのであれば許容できる (3)	情報の提供先が信頼できれば許容できる (4)
Q22B_1 - クレジットカード情報等の決済情報をインターネット上で登録すること	❑	❑	❑	❑

	利便性が向上すれば許容できる (1)	経済的なメリットを享受できれば許容できる (2)	社会への貢献が認められるのであれば許容できる (3)	情報の提供先が信頼できれば許容できる (4)
Q22B_2 - ネットスーパー等での購買履歴の情報を、商品のレコメンドやターゲティング広告表示に活用されていること	❑	❑	❑	❑

Q23 - Q23

EC サイト等、インターネット上の各種サイトでは、あなたに関する情報を収集し、嗜好や趣味にマッチした情報を提供する行動ターゲティング広告（Behavioral Targeting Advertising, BTA）が提供されています。
その際に、あなたの個人情報（パーソナルインフォメーション）が上述のように取り扱われることについて、プライバシーの観点からどのように感じますか。
もっともあてはまるものをお答えください。（回答はひとつ）

❍ 許容できる (1)
❍ 条件によっては許容できる (2)
❍ どんな場合でも許容できない (3)

Q23A - Q23A

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はあてはまるものすべて）

❑ 利便性が向上すれば許容できる (1)
❑ 経済的なメリットを享受できれば許容できる (2)
❑ 情報の提供先が信頼できれば許容できる (3)

Q24 - Q24

下記のビッグデータを利用したサービスの説明をお読みください。
「インターネットショッピングの買い物履歴やソーシャルメディア等のインターネットサービスを利用する際の利用者登録情報等、あなたの個人情報（パーソナルインフォメーション）を蓄積・分析し、あなたに合わせたサービスのリコメンドや提供といった、ビッグデータを用いたサービスが始まっています。」
このようなサービスがあることを知っていましたか。（回答はひとつ）

❍ 知っていた (1)
❍ 知らなかった (2)

Q25 - Q25

ビッグデータに関わる各種サービスに接触する中で、あなたの個人情報（パーソナルインフォメーション）が以下のように取り扱われることについて、
プライバシーの観点からどのように感じますか。
もっともあてはまるものをお答えください。（回答はそれぞれひとつ）

回答は横方向に

	許容できる (1)	条件によっては許容できる (2)	どんな場合でも許容できない (3)
ソーシャルメディア上で登録した情報と、EC サイトで登録した情報が結び付けられるなど、異なるサービスで登録した個人情報（パーソナルインフォメーション）が関連付けられること (1)	❍	❍	❍
会員登録サービスに個人情報（パーソナルインフォメーション）を登録すると、EC サービス、医療サービス、動画閲覧サービス等の他のサービス提供事業者が情報を利用すること (2)	❍	❍	❍
インターネット上で様々な個人情報（パーソナルインフォメーション）を登録していくと、あなたに必要のない情報と結び付けられ、それにより EC サイトであなたが必要としない商品をお勧めされたり、動画共有サイトであなたに必要のない動画を勧められたりすること (3)	❍	❍	❍
スマートフォン等から取得した位置情報をもとに、近隣のおすすめのレストランや店舗の情報がスマートフォン等の携帯端末に通知されること (4)	❍	❍	❍
走行中の自動車から取得したデータを集約し道路の交通状況の把握や危険な箇所の把握に活用すること (5)	❍	❍	❍
走行中の自動車から取得したデータを集約し企業が自動車保険の商品設計に活用すること (6)	❍	❍	❍
街に監視カメラを多数設置し、防犯に活用すること (7)	❍	❍	❍
診療情報（患者のパーソナルデータ等）を活用して、医療サービ	❍	❍	❍

	許容できる (1)	条件によっては許容できる (2)	どんな場合でも許容できない (3)
スの進展に活用すること (8)			

Q25A - Q25A

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はそれぞれあてはまるものすべて）

回答は横方向に

	利便性が向上すれば許容できる (1)	経済的なメリットを享受できれば許容できる (2)	社会への貢献が認められるのであれば許容できる (3)	情報の提供先が信頼できれば許容できる (4)
Q25A_1 - ソーシャルメディア上で登録した情報と、EC サイトで登録した情報が結び付けられるなど、異なるサービスで登録した個人情報（パーソナルインフォメーション）が関連付けられること	❑	❑	❑	❑
Q25A_2 - 会員登録サービスに個人情報（パーソナルインフォメーション）を登録すると、EC サービス、医療サービス、動画閲覧サービス等の他のサービス提供事業者が情報を利用すること	❑	❑	❑	❑
Q25A_3 - インターネット上で様々な個人情報（パーソナルインフォメーション）を登録していくと、EC サイトであなたが必要としない商品をお勧めされたり、動画共有サイトであなたに必要のない動画を勧められたり、あなたに必要のない情報と結び付けられること	❑	❑	❑	❑
Q25A_4 - スマートフォン等から取得した位置情報をもとに、近隣のおすすめのレストランや店	❑	❑	❑	❑

	利便性が向上すれば許容できる (1)	経済的なメリットを享受できれば許容できる (2)	社会への貢献が認められるのであれば許容できる (3)	情報の提供先が信頼できれば許容できる (4)
舗の情報がスマートフォン等の携帯端末に通知されること				
Q25A_5 - 走行中の自動車から取得したデータを集約し道路の交通状況の把握や危険な箇所の把握に活用すること	❑	❑	❑	❑
Q25A_6 - 走行中の自動車から取得したデータを集約し企業が自動車保険の商品設計に活用すること	❑	❑	❑	❑
Q25A_7 - 街に監視カメラを多数設置し、防犯に活用すること	❑	❑	❑	❑
Q25A_8 - 診療情報（患者のパーソナルデータ等）を活用して、医療サービスの進展に活用すること	❑	❑	❑	❑

Q26 - Q26

下記のクラウドコンピューティングサービスの説明をお読みください。

「クラウドコンピューティングサービスとは、
データをご自身のパソコンやスマートフォン等の端末ではなく、
インターネット上のサーバー群に保存する使い方、サービスのこと」
この仕組みを知っていましたか。（回答はひとつ）

❍ 知っていた (1)
❍ 知らなかった (2)

Q27 - Q27

「クラウドコンピューティングサービス」にあなたの個人情報（パーソナルインフォメーション）を預けることについて、プライバシーの観点からどのように感じますか。
もっともあてはまるものをお答えください。（回答はひとつ）

❍ 許容できる (1)

❍ 条件によっては許容できる（2）
❍ どんな場合でも許容できない（3）

Q27A - Q27A

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はあてはまるものすべて）

❑ 利便性が向上すれば許容できる（1）
❑ 経済的なメリットを享受できれば許容できる（2）
❑ 情報の提供先が信頼できれば許容できる（3）

Q28 - Q28

「クラウドコンピューティングサービス」に預ける個人情報（パーソナルインフォメーション）として、下記のどの情報であれば抵抗感なく預けることができますか。
（回答はあてはまるものすべて）

❑ 氏名（1）
❑ 性別（2）
❑ 住所（3）
❑ 生年月日（4）
❑ 国籍（5）
❑ 職歴（6）
❑ メールアドレス（7）
❑ 電話番号（8）
❑ 会社名（9）
❑ 学校名（10）
❑ 役職（11）
❑ 資格（12）
❑ 健康状態（13）
❑ 学歴（14）
❑ 趣味（15）
❑ 個人識別番号（国民 ID 等）(16)
❑ 顔（生体情報）（17）
❑ 虹彩（生体情報）（18）
❑ 網膜（生体情報）（19）
❑ 指紋（生体情報）（20）
❑ 静脈（生体情報）（21）
❑ 身長（22）
❑ 体重（23）
❑ 血液型（24）
❑ 位置情報（25）
❑ 行動履歴（26）
❑ 口座情報（27）
❑ クレジットカード番号（28）
❑ 年収・所得（29）
❑ 借金（30）
❑ 家族関係（31）
❑ 友人関係（32）
❑ 交際関係（33）
❑ 同窓会情報（34）
❑ 思想信条（35）
❑ 宗教（36）
❑ 性癖（37）
❑ 労組加入事実（38）
❑ 病歴・病状（39）
❑ その他（40）_____
❍ いかなる個人情報（パーソナルインフォメーション）も預けたくはない（41）

Q29 - Q29

個人情報（パーソナルインフォメーション）は国によって取扱いが異なります。
あなたの個人情報（パーソナルインフォメーション）をクラウドサービス提供事業者が国外に保管することについて、どのように感じますか。
もっともあてはまるものをお答えください。（回答はひとつ）

❍ 許容できる（1）
❍ 条件によっては許容できる（2）
❍ どんな場合でも許容できない（3）

Q29A - Q29A

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はあてはまるものすべて）

❑ 経済的なメリットを享受できれば許容できる（1）
❑ セキュリティが担保されるのであれば許容できる（2）
❑ クラウドサービス提供事業者が信頼できれば許容できる（3）
❑ あなたが信頼できる国に保管されるのであれば許容できる（4）
❑ その他（5）_____

Q30 - Q30

あなたは下記のようなケースに遭遇した場合、プライバシーの観点からどのように感じますか。
もっともあてはまるものをお答えください。（回答はそれぞれひとつ）

回答は横方向に

	許容できる（1）	条件によっては許容できる（2）	どんな場合でも許容できない（3）
メール等のサービスで収集した個人情報（パーソナルインフォメーション）を、利用者の事前同意を得ることなく、同じサービス提供事業者が他のサービスでも活用すること（1）	❍	❍	❍
写真や動画で地理情報（地図の情報）を確認できるインターネットサービスを見ると、人の顔や車のナンバープレートが確認できる状況であること（2）	❍	❍	❍

Q30A - Q30A

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はそれぞれあてはまるものすべて）

回答は横方向に

	利便性が向上すれば許容できる (1)	経済的なメリットを享受できれば許容できる (2)	社会への貢献が認められるのであれば許容できる (3)	情報の提供先が信頼できれば許容できる (4)
Q30A_1 - メール等のサービスで収集した個人情報（パーソナルインフォメーション）を、利用者の事前同意を得ることなく、同じサービス提供事業者が他のサービスでも活用すること	❑	❑	❑	❑
Q30A_2 - 写真や動画で地理情報（地図の情報）を確認できるインターネットサービスを見ると、人の顔や車のナンバープレートが確認できる状況であること	❑	❑	❑	❑

Q31 - Q31

あなたは、スマートフォンのアプリケーションをダウンロードする際やアプリケーションを利用する際に、
「収集する利用者情報に関する利用許諾」を求める画面が提示されることを知っていましたか。
この画面を読んで、アプリケーションを使う前に承諾・同意を行ったことはありますか。（回答はひとつ）

❍ 利用承諾を求める画面を知っていて、利用承諾を行ったことがある。 (1)
❍ 利用承諾を求める画面を知っているが、利用承諾を行ったことはない (2)
❍ 利用承諾を求める画面を知らない (3)
❍ わからない (4)

Q32 - Q32

あなたは、スマートフォンを利用する際に、あなたの年齢、性別、位置情報、登録している友人の連絡先などの
個人情報（パーソナルインフォメーション）がサービス提供事業者等に取得されていることを知

っていましたか。
（回答はひとつ）

❍ 知っていた（1）
❍ 知らなかった（2）

Q33 - Q33

スマートフォンに保存されている個人情報（パーソナルインフォメーション）が、
サービス提供事業者にアクセスされている可能性があることについてプライバシーの観点から
どのように感じますか。
もっともあてはまるものをお答えください。（回答はひとつ）

❍ 許容できる（1）
❍ 条件によっては許容できる（2）
❍ どんな場合でも許容できない（3）

Q33A - Q33A

どのような条件であれば許容できますか。
あてはまるものをお答えください。（回答はあてはまるものすべて）

❑ 利便性が向上すれば許容できる（1）
❑ 経済的なメリットを享受できれば許容できる（2）
❑ 社会への貢献が認められるのであれば許容できる（3）
❑ 情報の提供先が信頼できれば許容できる（4）

Q34 - Q34

あなたはスマートフォンを利用し始めて、個人情報（パーソナルインフォメーション）の取り扱
いに関する意識は変化しましたか。
あなたに最も当てはまるものをお選びください。（回答はひとつ）

❍ 個人情報（パーソナルインフォメーション）の取り扱いに敏感になった（1）
❍ 個人情報（パーソナルインフォメーション）の登録を控えるようになった（2）
❍ 個人情報（パーソナルインフォメーション）を積極的に登録するようになった（3）
❍ スマートフォンの利用前後で個人情報（パーソナルインフォメーション）への意識に変化は
ない（4）

Q35 - Q35

スマートフォンのアプリケーションを利用する際に、サービス提供事業者が利用規定を変更する
など、

ポリシー変更を行う場合があることについてどのように感じますか。
あてはまるものをお答えください。（回答はあてはまるものすべて）

❍ 特に問題であるとは思わない (1)
❑ サービス提供事業者が、変更点を明確に示した上での変更であれば問題ない (2)
❑ サービス提供事業者が、ポリシー変更によって、どのような影響があるかを明確に示した上での変更であれば問題ない (3)
❑ ポリシー変更に関して利用者の同意を得た上で変更するのであれば問題ない (4)
❑ ポリシー変更をするのであれば、サービスの利用を取りやめたい (5)
❑ ポリシー変更をするのであれば、サービス提供事業者を変えたい (6)
❑ その他 (7)_____
❍ わからない (8)

Q36 - Q36

あなたが、個人情報（パーソナルインフォメーション）を登録する際にサービス提供事業者に望むものとしてあてはまるものをお答えください。
（回答はそれぞれひとつ）

回答は横方向に

	必要と思う (1)	どちらともいえない (2)	必要ない (3)
登録した個人情報（パーソナルインフォメーション）の取り扱いが明確であるなど、情報の取り扱いの透明性の確保 (1)	❍	❍	❍
パーソナルインフォメーション登録時の利用者の登録情報の選択権の確保 (2)	❍	❍	❍
事前の明示的な同意の取得 (3)	❍	❍	❍
データを消去する権利の確保 (4)	❍	❍	❍

Q37 - Q37

あなたは、下記のような場合であれば、サービス提供事業者に個人情報（パーソナルインフォメーション）を登録し、
利用・流通されてもよいと思いますか。（回答はそれぞれひとつ）

回答は横方向に

	利用・流通されても良い (1)	どちらともいえない (2)	利用・流通されたくはない (3)
利用者が明示的な同意を行った場合 (1)	❍	❍	❍
サービス提供事業者が個人情報（パーソナルインフォメーション）を匿名化、暗号化して流通させる場合 (2)	❍	❍	❍
匿名化された個人情報（パーソナルインフォメーション）が利用者の希望する分野のサービスに活用される場合 (3)	❍	❍	❍
匿名化等をしない状態で利用者が希望する分野のサービスに活用される場合（希望する分野の課題解決に役立てる場合） (4)	❍	❍	❍

Q38A - Q38A

あなたは、下記のような「忘れられる権利」を知っていますか。（回答はひとつ）

「忘れられる権利とは、サーバーの管理者や検索サービス会社などに対し、
個人が自分の情報を削除させる権利のこと。
情報を完全に削除することができなくても、この権利を保有することで、
情報の拡散防止に役立てることが期待されている。」

❍ 知っていた (1)
❍ 知らなかった (2)

Q38B - Q38B

また、「忘れられる権利」は、現実的な（意味のある）権利だと思いますか。（回答はひとつ）

「忘れられる権利とは、サーバーの管理者や検索サービス会社などに対し、
個人が自分の情報を削除させる権利のこと。
情報を完全に削除することができなくても、この権利を保有することで、
情報の拡散防止に役立てることが期待されている。」

❍ そう思う（現実的だ） (1)
❍ わからない／どちらともいえない (2)
❍ そう思わない（現実的ではない） (3)

Q38C - Q38C

さらに 「忘れられる権利」によって国民が保護されることを必要と感じますか。（回答はひとつ）

「忘れられる権利とは、サーバーの管理者や検索サービス会社などに対し、
個人が自分の情報を削除させる権利のこと。
情報を完全に削除することができなくても、この権利を保有することで、
情報の拡散防止に役立てることが期待されている。」

❍ 必要と思う (1)
❍ どちらともいえない (2)
❍ 必要ない (3)

Q39A - Q39A

あなたは自分の国に、個人情報保護に関わる法律があるかどうかを知っていますか。（回答はひとつ）

❍ あることを知っている (1)
❍ ないことを知っている (2)
❍ わからない (3)

Q39B - Q39B

あなたは個人情報保護の規制のあり方についてどのように感じますか。（回答はひとつ）

❍ 国が今以上に厳格な保護を行うべき (1)
❍ 現状の規制で十分である (2)
❍ 国が注力すべきでない（サービス提供者の主体的な取り組みに任せるべき） (3)

Q40 - Q40

プライバシーの保護対策として、必要だと思うものをお答えください。(回答はそれぞれひとつ)

回答は横方向に

	必要と思う (1)	どちらともいえない (2)	必要ない (3)
個人情報（パーソナルインフォメーション）の適切な取扱いについて判断できる窓口（公的な機関） (1)	❍	❍	❍
個人情報（パーソナルインフォメーション）の適切な取扱いについて判断できる窓口（サービス提供事業者） (2)	❍	❍	❍

	必要と思う (1)	どちらともいえない (2)	必要ない (3)
個人情報（パーソナルインフォメーション）の保護に関する普及啓発活動 (3)	❍	❍	❍
世界規模でプライバシールールの整合性を図ること (4)	❍	❍	❍

**InfoQ41 - **

ここからは、インターネットの利用についてお答えください。

Q41 - Q41

あなたはインターネットを利用していて不安を感じますか。（回答はひとつ）

❍ 全く不安は感じない (1)
❍ あまり不安は感じていない (2)
❍ 少し不安を感じている (3)
❍ 不安を感じている (4)

Q42 - Q42

次のインターネットサービスを利用する際に不安を感じますか。（回答はそれぞれひとつ）

回答は横方向に

	全く不安は感じない (1)	あまり不安は感じていない (2)	少し不安を感じている (3)	不安を感じている (4)
ホームページ（ウェブ）・ブログの閲覧 (1)	❍	❍	❍	❍
ソーシャルメディアの利用 (2)	❍	❍	❍	❍
電子メールの送受信 (3)	❍	❍	❍	❍
商品・サービスの購入・取引（EC） (4)	❍	❍	❍	❍

Q43 - Q43

あなたは次にあげるインターネットの脅威について知っているものはありますか。(回答はあてはまるものすべて)

❑ スパイウェア (1)
❑ マルウェア（コンピュータウイルス） (2)

❑ 標的型攻撃 (3)
❑ フィッシング詐欺 (4)
❑ ボットウイルス（BOT） (5)
❑ セキュリティホール（脆弱性） (6)
❑ 偽セキュリティ対策ソフト（「FakeAV」、「Fake Alert」、「Fake Antivirus」等） (7)
❑ 架空請求 (8)
❍ 上記のうち、知っているものはない (9)

Q44 - Q44

前述のインターネットの脅威について不安を感じますか。 （回答はそれぞれひとつ）

回答は横方向に

	全く不安は感じない (1)	あまり不安は感じていない (2)	少し不安を感じている (3)	不安を感じている (4)
スパイウェア (1)	❍	❍	❍	❍
マルウェア（コンピュータウイルス） (2)	❍	❍	❍	❍
標的型攻撃 (3)	❍	❍	❍	❍
フィッシング詐欺 (4)	❍	❍	❍	❍
ボットウイルス（BOT） (5)	❍	❍	❍	❍
セキュリティホール（脆弱性） (6)	❍	❍	❍	❍
偽セキュリティ対策ソフト（「FakeAV」、「Fake Alert」、「Fake Antivirus」等） (7)	❍	❍	❍	❍
架空請求 (8)	❍	❍	❍	❍

Q45 - Q45

あなたは情報セキュリティの教育や研修を受けた経験がありますか。(回答はあてはまるものすべて)

❑ ある（学校で） (1)
❑ ある（会社で） (2)
❑ ある(家庭で） (3)
❑ ある（国・地方行政機関の主催） (4)
❑ ある（自分で学習している） (5)
❍ ない (6)

Q46 - Q46

インターネット利用において利便性と情報セキュリティ対策のどちらを重視しますか。
あなたの考えに近いものを選んでください。（回答はひとつ）

❍ 利便性を重視している (1)
❍ どちらかというと、利便性を重視している (2)
❍ 利便性と情報セキュリティ対策を同じ程度重視している。 (3)
❍ どちらかというと、情報セキュリティ対策を重視している (4)
❍ 情報セキュリティ対策を重視している (5)

Q47 - Q47

インターネットの利用の際に情報セキュリティ被害の経験がありますか。（回答はひとつ）

❍ 受けた（確信している、証拠がある） (1)
❍ 受けた（可能性がある） (2)
❍ 受けたことがない (3)
❍ わからない (4)

Q47A - Q47A

どのような被害の経験がありますか。（回答はあてはまるものすべて）

❑ コンピュータウイルスの感染 (1)
❑ 迷惑メール（スパム）が送られてきた（架空請求メールの受信を除く） (2)
❑ 身に覚えのない料金の支払いを要求するメール（架空請求メール）が送られてきた (3)
❑ デバイス内のファイルやシステムが書き換えられた。または削除された (4)
❑ 他者へメール送信がされていた (5)
❑ 他者に自分の個人情報を漏洩された (6)
❑ フィッシング詐欺にあった (7)
❑ クレジットカードが利用されたり、銀行口座からお金が引き出されたりした (8)
❑ その他 (9)_____

Q48 - Q48

あなたは情報セキュリティ対策を行っていますか。（回答はひとつ）

❍ 十分対策を行っている (1)
❍ 対策を行っているが不安なところがある (2)
❍ 特に対策を行っていない (3)

Q48A - Q48A

パソコンにどのような情報セキュリティ対策を行っていますか。(回答はあてはまるものすべて)

❑ ＯＳ（オペレーティングシステム)、ソフトウェアのアップデートをする (1)
❑ マルウェア（コンピュータウイルス）対策ソフトウェア・サービスの導入 (2)
❑ フィルタリングソフトウェア・サービスの導入 (3)
❑ 信頼のおけないソフトウェアはインストールしない (4)
❑ ソフトウェアのインストール前に説明画面を確認する (5)
❑ 知らない差出人からのメールや添付ファイルを不用意に開かない (6)
❑ 開封したメールにある不審なＵＲＬリンクをクリックしない (7)
❑ データのバックアップを行う (8)
❑ データの暗号化を行う (9)
❑ アカウントごとにパスワードを複数使い分けている (10)
❑ パスワードの定期的な変更 (11)
❑ ファイアウォール機能の設定 (12)
❑ 使用しない時には電源を切る (13)
❑ その他の対策 (14)_____

Q49 - Q49

あなたは、職場でパソコンを利用していますか。
利用している場合､職場で支給されているパソコンにどのような情報セキュリティ対策が実施されているか把握していますか。（回答はひとつ）

❍ 職場でパソコンを利用しており、どのようなセキュリティ対策が実施されているか知っている (1)
❍ 職場でパソコンを利用しているが、どのようなセキュリティ対策が実施されているかわからない (2)
❍ 職場でパソコンを利用していない (3)

Q49A - Q49A

職場のパソコンではどのような情報セキュリティ対策を行っていますか。(回答はあてはまるものすべて)

❑ ＯＳ（オペレーティングシステム)、ソフトウェアのアップデートをする (1)
❑ マルウェア（コンピュータウイルス）対策ソフトウェア・サービスの導入 (2)
❑ フィルタリングソフトウェア・サービスの導入 (3)
❑ 信頼のおけないソフトウェアはインストールしない (4)
❑ ソフトウェアのインストール前に説明画面を確認する (5)

❑ 知らない差出人からのメールや添付ファイルを不用意に開かない（6）
❑ 開封したメールにある不審なＵＲＬリンクをクリックしない（7）
❑ データのバックアップを行う（8）
❑ データの暗号化を行う（9）
❑ アカウントごとにパスワードを複数使い分けている（10）
❑ パスワードの定期的な変更（11）
❑ ファイアウォール機能の設定（12）
❑ 使用しない時には電源を切る（13）
❑ その他の対策（14）_____

Q50 - Q50

スマートフォンは携帯電話と比べ、安全に利用するためには対応が必要ですが、以下のうち、あなたがご存じのことをお選びください。
（回答はあてはまるものすべて）

❑ ＯＳやアプリケーションのアップデートを行うこと（1）
❑ ウイルス対策アプリを導入すること（2）
❑ フィルタリングアプリを導入すること（3）
❑ インストールするアプリが安全かどうかの判断をすること（4）
❑ アプリがアクセスできる情報の許可・不許可について設定をおこなうこと（5）
❑ 情報セキュリティ対策がされている安全な Wi-Fi 回線を利用すること（6）
❑ その他（7）_____
❍ 安全に利用するためには対応が必要であることは知らなかった（8）

Q51 - Q51

スマートフォンにどのような情報セキュリティ対策を行っていますか。（回答はあてはまるものすべて）

❑ ＯＳやアプリケーションのアップデートを行う（1）
❑ ウイルス対策（マルウェア対策も含む）アプリケーション・オンラインサービスの導入（2）
❑ フィルタリングアプリの導入（3）
❑ 信頼できる場所(ＯＳ提供事業者や携帯電話事業者のサイトなど)からアプリをインストールする（4）
❑ 「提供元不明のアプリ」をインストールしない設定にする（5）
❑ アプリをインストールする前にアプリがアクセスする情報を確認する（6）
❑ データのバックアップを行う（7）
❑ データの暗号化を行う（8）

❑ パスワードやパターンによる画面ロックの実施（9）
❑ リモートロックやリモートワイプ等の不正利用防止機能（10）
❑ 安全な Wi-Fi 回線を利用する（11）
❑ その他の対策（12）_____
❍ 特に対策を行っていない（13）

Q51A - Q51A

対策を行っていない理由をお答えください。（回答はあてはまるものすべて）

❑ 何をすればよいか分からないから（1）
❑ 対策が必要なほど深刻な状況と思わないから（2）
❑ 対策に費用がかかるから（3）
❑ 面倒だから（4）
❑ 事業者※に対策を任せているから（自分では対策を行わなくてよいと考えているから）
※ＯＳ提供事業者や携帯電話事業者、インターネットプロバイダー（5）
❑ 上記以外の理由（6）_____
❍ 対策が必要と思わないから（7）

Q52 - Q52

あなたは、職場で支給されたスマートフォンを利用していますか。
利用している場合、職場で支給されているスマートフォンにどのような情報セキュリティ対策が実施されているか把握していますか。
（回答はひとつ）

❍ 職場でスマートフォンを利用しており、どのようなセキュリティ対策が実施されているか知っている（1）
❍ 職場でスマートフォンを利用しているが、どのようなセキュリティ対策が実施されているかわからない（2）
❍ 職場でスマートフォンを利用していない（3）

Q52A - Q52A

職場のスマートフォンではどのような情報セキュリティ対策を行っていますか。（回答はあてはまるものすべて）

❑ ＯＳやアプリケーションのアップデートを行う（1）
❑ ウイルス対策（マルウェア対策も含む）アプリケーション・オンラインサービスの導入（2）
❑ フィルタリングアプリの導入（3）

❑ 信頼できる場所(ＯＳ提供事業者や携帯電話事業者のサイトなど)からアプリをインストールする（4)

❑ 「提供元不明のアプリ」をインストールしない設定にする（5)

❑ アプリをインストールする前にアプリがアクセスする情報を確認する（6)

❑ データのバックアップを行う（7)

❑ データの暗号化を行う（8)

❑ パスワードやパターンによる画面ロックの実施（9)

❑ リモートロックやリモートワイプ等の不正利用防止機能（10)

❑ 安全な Wi-Fi 回線を利用する（11)

❑ その他の対策（12)_____

❍ 特に対策を行っていない（13)

Q53 - Q53

スマートフォンを利用するようになって情報セキュリティへの不安は高まりましたか。(回答はひとつ)

❍ 高まった（1)

❍ どちらかというと高まった（2)

❍ 変わらない（3)

❍ どちらかというと低くなった（4)

❍ 低くなった（5)

Q54 - Q54

スマートフォンを安全に利用するにあたり以下のことをご存知ですか。(回答はそれぞれひとつ)

回答は横方向に

	知っていた (1)	知らなかった (2)
OS 提供事業者により設定されている制限をはずすこと（Jailbreak）は情報セキュリティレベルを下げる可能性があること（1)	❍	❍
Wi-Fi 回線に、暗号や認証の仕組みが導入されていない場合があり、安全な通信が確保できるかどうかが不明であるため、そこに接続して行う通信が外部に内容を読み取られる可能性があること（2)	❍	❍
デバイスの設定でＧＰＳの利用をＯＦＦすることで、利用者のＧＰＳ情報を隠せる機能があること（3)	❍	❍

Q55 - Q55

情報セキュリティ対策は誰が主体となって行うべきだと思いますか。（回答はあてはまるものすべて）

❑ 利用者個人（1）
❑ サービス提供事業者（2）
❑ デバイスメーカー（3）
❑ 情報セキュリティベンダー（4）
❑ 政府機関、地方行政機関（5）
❑ その他（6）_____

Q56 - Q56

あなたは情報セキュリティ対策に関する情報を得られていますか。（回答はひとつ）

❍ 十分に得られている（1）
❍ どちらかというと得られている（2）
❍ あまり得られていない（3）
❍ まったく得られていない（4）

Q56A - Q56A

あなたはどこから情報を得られていますか。（回答はあてはまるものすべて）

❑ 【他から知識を得ている】（a）
❑ 国、地方行政機関（1）
❑ 職場（2）
❑ 学校（3）
❑ 友人・知人（4）
❑ 家族・親戚（5）
❑ ボランティア団体（6）
❑
【自分で探す】（b）
❑ テレビ（7）
❑ ラジオ（8）
❑ 新聞・雑誌（9）
❑ 専門書籍（10）
❑ ウェブサイト（11）
❑ メールマガジン（12）

❑

【その他】 (c)

❑ その他 (13)_____

Q56B - Q56B

あなたは情報セキュリティ対策情報を収集するにあたってどのような問題を感じていますか。（回答はあてはまるものすべて）

❑ 難しい用語が多い (1)
❑ 情報が多すぎる (2)
❑ 情報の更新が早すぎて追いつかない (3)
❑ 自分から情報収集や勉強をするのが面倒 (4)
❑ 情報がどこにあるかわからない (5)
❑ 自分に関係がある情報なのかわからない (6)
❑ その他 (7)_____
❍ 特に問題点は感じていない (8)

Q57 - Q57

国・行政、企業に実施してほしい情報セキュリティ向上のための取り組みはありますか。（回答はあてはまるものすべて）

❑ 情報セキュリティ対策や情報セキュリティ事象をまとめたサイトの提供 (1)
❑ 情報セキュリティに関する相談窓口の設置 (2)
❑ 情報セキュリティを学ぶ機会を増やしてほしい (3)
❑ 自分で学ぶことができるツールを提供してほしい（テキストや映像） (4)
❑ インターネット接続機器の情報セキュリティ診断・設定 (5)
❑ 情報セキュリティ対策ソフトの配布 (6)
❑ その他 (7)_____
❍ 特にない (8)