2013 年度卒業論文

山田正雄ゼミナール

高度情報化社会における
個人情報保護

―スマートフォンの普及に見る個人情報漏えいの現状と対策―

日本大学法学部 政治経済学科 4 年

学籍番号：1020153

川端 宥太

2013 年度 山田正雄ゼミナール 卒業論文
高度情報化社会における個人情報保護
1020153　川端宥太

はじめに

高度情報化社会では、情報通信技術が日々着実に進化を遂げており、我々の生活や企業活動などに多くの利便性をもたらしている。このような高度情報化社会においては、個人情報が大量、かつ瞬時に処理され、企業活動や、行政活動の作業の迅速化などに貢献している。

しかしその一方で、インターネット上で、一旦個人情報が漏えいしてしまうと、その被害回復はほぼ不可能であり、個人のプライバシーが脅威にさらされることになる。実際、個人情報がインターネット等を経由して漏えいする事件が後を絶たず、最近でも、米政府がテロ対策を名目に、インターネット上の個人情報を極秘に収集していたことが明らかになり、社会に大きな衝撃を与えている。

また最近では、スマートフォンからの個人情報漏えいという問題も発生している。近年、スマートフォンが急速に普及してきており、我が国の携帯電話端末の総出荷台数に占めるスマートフォン出荷台数比率は、2012 年度、約 71.0%を占めており、同年末にはスマートフォンの世帯普及率が約 3 割となり前年度の約 3 倍増となるなど、幅広い層への普及が進んできているといえる。高度な情報処理機能が備わったスマートフォンは、様々なアプリケーション、通称アプリをインストールすることにより、電話やメール機能などの他に多様な目的のために活用することができる。

しかしその一方で、スマートフォンを利用していると、アプリ・ネットワーク・OS の各レイヤーから、情報が漏えいする危険性がある。特にアプリにおける問題は大きく、アプリがスマートフォンの内部に蓄積された利用者の利用履歴や通信履歴にアクセスし、それぞれの情報がどのように共有され利用される可能性があるか、利用者が十分に把握しないままに、情報が漏えいしているという実態がある。

そこで本論文では、個人情報とは何か、ということを踏まえたうえで、近年の個人情報漏えいの概況を、事例などを交えながら考察していく。そして、スマートフォンによる個人情報漏えいの現状・問題点・対策などを考察した上で、個人・組織・教育機関という観点から個人情報漏えいへの対策を提案したい。

また展望として、新たにマイナンバー法の導入や、ビッグデータの活用が広がる中で、どのように個人情報を取り扱っていくべきか、また、個人情報保護法の改正が検討されている中で、現状の法律の問題点や社会状況を考察した上で、どのような改正が望まれるのか、などという点についても考察していきたい。

- 目次 -

1　個人情報とは

1.1　個人情報とは何か

そもそも個人情報とはどのようなものを指すのか。平成 15 年 5 月 23 日に成立し、2 年後の平成 17 年 4 月 1 日に全面施行した、「個人情報の保護に関する法律」（以下「個人情報保護法」）では、「生存する個人に関する情報であって、その情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができることとなるものを含む。）をいう」と個人情報を定義している（2 条 1 項）。

ここでポイントとなることが二点ある。一点目は、「生存する個人」だけが対象となる点である。「個人」に関する情報であるため、法人そのものの情報は含まれない。しかし、法人の役員、担当者の情報は「個人」の情報であるため、これに含まれるため、名刺に記載された情報や、会社の従業員、退職者などの情報、外国人の情報なども個人情報になり得る。次に、「生存する」個人に関する情報であるため、死者に関する情報は含まれない。しかし、死者の情報であってもこれが同時に遺族や相続人を識別し得る情報である場合には、遺族や相続人自身の個人情報になる。例えば、相続財産に関する情報は、死者である被相続人の情報であるとともに、遺族や相続人自身の個人情報になる場合がある。

二点目は「特定の個人を識別することができるもの」という点である。例えば、氏名はこれだけで特定の個人を識別できることから個人情報に該当する。さらに他の情報と容易に照合することができ、それにより特定の個人を識別することができるものも識別可能性があるものとして含まれる。したがって、住所や生年月日、電話番号など、単独では特定の個人を識別できない情報についても、他の情報と容易に照合することができて、特定の個人を識別することができる限り個人情報に該当する。また、メールアドレスについても、それがユーザー名及びドメイン名などから特定の個人を識別することができるものは個人情報に該当し、企業の顧客情報や従業員情報を番号や記号などで管理している場合でも、データベース等に簡単にアクセスすることにより、これらの情報と照合して特定の個人を識別することができるのであれば、個人情報に該当する。

以上のように、個人情報保護法でいう個人情報の定義は非常に広く、特定の生存する個人を識別できるものは、すべて個人情報に該当するのである。

なお、図表 1 は個人情報に該当する事例・しない事例をまとめたものである。

図表 1：個人情報に該当する事例・しない事例

	該当する事例	該当しない事例
個人情報	・本人の氏名 ・生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報 ・防犯カメラに記録された情報等本人が判別できる映像情報 ・特定の個人を識別できるメールアドレス情報(keizai_ichiro@meti.go.jp 等のようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイイチローのメールアドレスであることがわかるような場合等) ・特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報 ・雇用管理情報（会社が従業員を評価した情報を含む。） ・個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できた場合は、その時点で個人情報となる。） ・官報、電話帳、職員録等で公にされている情報（本人の氏名等）	・企業の財務情報等、法人等の団体そのものに関する情報（団体情報） ・記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報(例えば abc012345@xyzisp.jp。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。) ・特定の個人を識別することができない統計情報

（出典；『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』より筆者作成）

1.2　個人情報保護法

個人情報保護法は、平成 15 年 5 月に成立した。官民共通のルールを定めた基本法に相当する、第 1 章から第 3 章までの部分と、民間事業者の遵守すべき義務等を定めた一般法に相当する、第 4 章から第 6 章の部分から構成されている。

この法の対象者となるのは、個人情報取扱事業者である。この個人情報取扱事業者とは、個人情報を含む集合物であって「特定の個人情報を電子計算機を用いて検索できるように体系的に構成したもの（2 条 2 項)」等の「個人情報データベース等」を事業の用に供している者である場合、「個人情報取扱事業者」に該当する（2 条 3 項）とされている。しかし、個人情報データベース等を構成する個人情報によって識別される特定の個人の叢話が 5000 人を超えない場合、当該事業者は個人情報取扱事業者からは除外される。

つまり、「データベースの形で、事業者用に、大量（5000 人分超）に個人情報を取り扱っている者」が、「個人情報取扱事業者」となって法律の適用を受けることとなる。

また、個人情報取扱事業者には個人情報保護法における以下の規定等が適用される。

・ 利用目的の特定

個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的をできるだけ限定。利用目的の変更は変更前と相当の連関性を合理的に認める範囲を超えてはならない（第 15 条)。

・ 利用目的による制限

個人情報取扱事業者は、あらかじめ本人の同意を得ないで、第 15 条により特定された利用目的達成に必要な範囲を超えて、個人情報を取り扱ってはならない（第 16 条)。

・ 適正な取得

偽りその他不正の手段により個人情報を取得してはならない(第 17 条)

・ 第三者提供の制限

あらかじめ本人の同意を得ないで個人データ[1]を第三者に提供してはならない（又は、必要な事項をあらかじめ本人に通知等し、本人の求めに応じて第三者への提供を停止する）（第 23 条)。

・ 利用停止等

第 16 条、第 17 条、第 23 条に違反して取り扱われているという理由により、利用停止等を求められた場合の対応（第 27 条）　。

[1] 個人データ･･･個人情報データベース等を構成する個人情報のこと。（第 2 条第 4 項）

・ 苦情の処理

個人情報取扱事業者による苦情の適切かつ迅速な処理、必要な体制の整備（第 31 条)。

個人情報取扱事業者が法に違反した場合には、まず、主務大臣が違反の是正のための勧告を行い、次にもし、個人情報取扱事業者が主務大臣の是正勧告に従わなかった場合には、最高で 6 ヶ月以下の懲役又は 30 万円以下の罰金に処せられることになる。ただし、報道機関や学術研究機関、宗教や政治目的による場合は、日本国憲法で保障された「表現の自由」「信教の自由」「政治活動の自由」などとの関係を調整するため、個人情報取扱事業者から除外されている。

なお、個人情報保護法は、プライバシーに関連するあらゆるものを保護することを目的とはしていない。そもそも個人情報とプライバシーとはどのような関係にあるのか。プライバシー権はかつて、「一人で放ってもらう権利」や、「私生活をみだりに公開されない法的保障ないし権利」、とされてきた。しかし現在では、高度情報化社会の進展に伴い、より積極的な概念として、「自己に関する情報をコントロールする権利（自己情報コントロール権)」とする考えも有力になっている。

個人情報保護法とプライバシーの関係について「基本方針」では、個人情報保護法 3 条の基本理念に則し、プライバシーの保護を含めた個人の権利利益を保護することを目的としていることが規定されている。したがって、個人情報保護法の目的においては、プライバシー保護を中心とした個人の権利利益の保護が念頭に置かれていると考えられる。諸外国では、米国のように個人情報保護法制のことをプライバシー法と名付けていることもある。

しかしながら、個人情報保護法は、プライバシーに関連するあらゆる問題を解決しようとする制度ではない。個人情報保護法制は、個人情報が情報通信技術によって処理されている現状において、プライバシー等の侵害の危険性が一般的に高まっているという認識の下、インターネット上で処理される個人情報を中心にその適正な取扱いルールを確立し、それを遵守させることによりプライバシーを含む個人の権利利益侵害を未然に防止することをねらいとしている。

したがって、個人情報の取扱いとは関係のないプライバシー問題や、検索することのできない個人情報の取扱いに伴うプライバシーなどは、この法律の対象とすべき本来的な問題とはならない。プライバシー侵害などが実際に発生した後の個人の権利利益の救済については、従来どおり、民法上の不法行為や刑法上の名誉棄損罪等によって図られることになる。

1.3　個人情報保護法の成り立ちと背景

高度情報化社会の進展に伴い、個人情報の利用が著しく拡大してきていた中で、個人情報が漏えいする事件が後を絶たず、プライバシー侵害に対する国民の不安が高まっていた。このようなプライバシー侵害への不安の高まりを背景に、企業・国家に向けた個人情報の保護に向けた取組への要請が強まっていた。

このような状況を背景として、個人情報を利用している側と利用されている側との間で、個人情報の適正な取扱いのルールを確立するという目的の下、個人情報保護法は作成された。

欧米では､1970 年代より個人のプライバシー保護に関する法整備の要請が高まっており、1980 年には、各国の規制の内容の調和を図る観点から、経済協力開発機構（OECD）[2] において､「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」が採択されていた。

そこでは､「OECD 8 原則」と呼ばれる原則が掲げられ、OECD 加盟国において国内法の中でこれらの原則を考慮することが求められた。OECD 8 原則は、現在個人情報に関する国際標準として、各国の個人情報保護政策の基礎とされ、我が国の個人情報保護法においても、これらの原則が具体化されている。以下が OECD 8 原則の具体的な内容である。

OECD 8 原則 [3]

(1) 収集制限の原則 ：適法・公正な手段により、必要な場合には情報主体に通知又は同意を得て収集されるべき。）
(2) データ内容の原則 ：利用目的に沿ったもので、かつ、正確・完全・最新であるべき。
(3) 目的明確化の原則 ： 収集目的を明確にし、データ利用は収集目的に合致するべき。
(4) 利用制限の原則 ： データ主体の同意がある場合又は法律の規定による場合以外は目的以外に利用してはならない。
(5) 安全保護の原則 ： 合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護されるべき。
(6) 公開の原則 ： データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき。
(7) 個人参加の原則 ： 自己に関するデータの所在及び内容を確認させ、または異議申立てを保証するべきである。
(8) 責任の原則 ： 管理者は諸原則実施の責任を有する。

[2] OECD（経済協力開発機構）はヨーロッパ諸国を中心に日・米を含め 34 ヶ国の先進国が加盟する国際機関であり、先進国間の自由な意見交換・情報交換を通じて、①経済成長、②貿易自由化、③途上国支援に貢献することを目的としている。

[3] 『ガイドブック 個人情報保護法』内藤貴昭　法学書院　2008 年、2 項より引用

こうした欧米の動きを受けて、我が国においても昭和 63 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」が制定された。この法律は国の行政機関を対象とするものであったが、平成 6 年 8 月、高度情報化社会の構築に向けた施策を総合的に推進するために政府内に「高度情報通信社会推進本部」が設置され、さらに、平成 11 年 11 月に「我が国における個人情報保護システムの在り方について（中間報告)」が取りまとめられ、この中で我が国の個人情報保護システムの中核となる基本原則等を確立するために、官民の全分野を包括する基本法の制定の必要が指摘された。

平成 12 年 10 月には、高度情報化推進本部の個人情報保護法制化専門委員会において、「個人情報保護基本法制に関する大綱」が取りまとめられたのを受けて、情報通信技術戦略本部において、この大綱を最大限尊重し、個人情報保護に関する基本法制の立案作業を進める旨の決定がなされた。

このような経過を経たうえで、平成 13 年 3 月、「個人情報の保護に関する法律案」が国会に提出された。しかしながら、この法案についてはメディア規制色が強いものであるとの批判が起こり、一旦、審議未了、廃案となった。

その後、この法案を一部修正した形で再度法案が提出された結果、平成 15 年 5 月 23 日に個人情報保護法が成立した。

1.4　個人情報の利用範囲

個人情報保護法において、どの範囲まで個人情報の利用が認められているのか。社内においては、同意を得た目的の範囲内での利用であれば第三者提供にはあたらないため、部門間などでの個人情報の共有が可能である。

では社外の場合はどうなるのか。この点に関しては、個人情報保護法の第三者提供の制限（第 23 条）が大きく関わってくる。第 23 条では、個人情報取扱事業が、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならないことが規定されている。この規定により、個人情報取扱事業者は個人データを第三者に提供する場合、原則としてあらかじめ本人の同意を得る（オプトイン）ことが必要になる。

しかし例外として、事前の同意が不要な場合がある。それは、本人の求めに応じて第三者への提供を停止する（オプトアウト）形をとる場合である。この場合は、①第三者への提供を利用目的とすること、②第三者に提供される個人データの項目、③第三者への提供の手段または方法、④本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること、の 4 点を満たしており、あらかじめこれら一定の事項について本人に通知しまたは本人が容易に知り得る状態においてあれば、本人の事前同意を取得することなく個人情報を第三者に提供することができる。

しかし、ここでいう「本人が容易に知り得る状態」とは、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」において、「問い合わせ窓口を設け、問い合わせがあれば、口頭又は文章で回答できるよう体制を構築しておくこと。」や、「店

舗販売において、店舗にパンフレットを備え置くこと。」、「電子商取引において、問い合わせ先のメールアドレスを明記すること。」などを例として挙げているが、これが「本人が容易に知り得る状態」と言えるかは、疑問が残るため、より利用者が容易に認識できるような改善をすべきであると思われる。

また、第 23 条第 4 項においては、第三者に該当しない場合を規定している。それは、①委託先への提供、②合併に伴う提供、③グループによる共同利用の場合である。

①委託先への提供としての具体例は、ダイレクトメール配信事業者にその配信を委託したり、データ処理会社にデータの打ち込みを委託したり、宅配業者に商品発送を委託するような場合である。この場合、委託元である個人情報取扱事業者は、委託先に対し第 22 条によって監督責任を負うこととなる。

②合併に伴う提供とは、合併その他の事由による事業の承継に伴って個人データが提供される場合は、第三者に該当しないということである。

③グループによる共同利用とは、グループ企業などで、総合的なサービスを提供する場合や、企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲内で個人データを共同利用する場合には、第三者に該当しないということである。しかしこの場合は、共同利用者の範囲、利用する情報の種類、利用目的、情報管理の責任者の名称等についてあらかじめ本人に通知し、又は本人が容易に知り得る状態に置かなければならないとされている。

こういった点を踏まえ、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（経済産業省作成）では、第三者提供とされる事例・されない事例、共同利用を行う事例を以下の通り挙げている。

【第三者提供とされる事例】

事例 1）親子兄弟会社、グループ会社の間で個人データを交換する場合
事例 2）フランチャイズ組織の本部と加盟店の間で個人データを交換する場合
事例 3）同業者間で、特定の個人データを交換する場合
事例 4）外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】（ただし、利用目的による制限がある。）

事例）同一事業者内で他部門へ個人データを提供すること。

【共同利用を行うことがある事例】

事例 1）グループ企業で総合的なサービスを提供するために取得時の利用目的の範囲内で情報を共同利用する場合
事例 2）親子兄弟会社の間で取得時の利用目的の範囲内で個人データを共同利用する場合
事例 3）外国の会社と取得時の利用目的の範囲内で個人データを共同利用する場合

事例 4) 企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲内で個人データを共同利用する場合

しかし現実には、この共同利用に関連した問題も起きている。例えば TUTAYA などの経営を行うカルチュア・コンビニエンス・クラブ株式会社（Culture Convenience Club Company, Limited、以下、CCC）では、CCC グループの共通会員証である「T カード」を基盤としたポイントサービスである「T ポイント」によって集められた利用者情報の活用法に関して、問題視する声が挙がっている。

CCC では、加盟している企業間で、利用者情報を共有してサービスを提供しており、加盟店で集められた購買情報等は、CCC で一元管理されている。そのため、加盟店で集められた情報と、氏名や住所などの個人情報が統合されると、誰が何を買ったのか、どういった嗜好を持つのか等が特定可能になる。これは前述した「共同利用」に該当しており、「T 会員規約」においても、共同利用者の範囲、利用する情報の種類、利用目的、情報管理の責任者の名称等について明記しており、法律やガイドラインには違反しておらず、一見すると問題がないように思われる。

しかしながら道義的に検討した場合、いくつかの問題点が考えられる。一点目としては、自身の購買履歴などを共同利用されていることに対して認識している人がどの程度存在するのかという問題がある。CCC ではこの共同利用に関して、「T 会員規約」において明記しているが、会員規約すべてに目を通している人は多くはないと考えられる。

二点目としては、共同利用を認める範囲が広すぎることである。個人情報保護法では、共同利用の範囲に関して、「グループ企業などで、総合的なサービスを提供する場合や、企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲内で個人データを共同利用する場合には」という記述があり、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」においても同様の事例が示されている。しかしながら、そのような範囲ではあまりに広すぎると思われる。

例えば CCC の場合は、多種多様な 100 社以上の企業が提携しているため、ある本屋で本を購入しただけで、提携先のレストラン、旅行会社、スポーツショップなどの多様な事業者にその購買情報が知れ渡ってしまうのである。「T 会員規約」において「ポイントサービスの円滑な運営のため」という曖昧な目的を設定しているが、その情報をもとに各事業者が販促活動などを行っていると考えられ、それは利用者が入会した際に想定し得る利用目的の範囲を超えていると思われる。

これらの問題を解決するためには、同意の取得方法の改正や共同利用の範囲の厳格化といった個人情報保護法の改正が必要であると思われる。同意の取得方法としては、利用規約の中の重要事項（利用目的や共同利用の概要など）については別途簡潔な説明書を用意することやイラスト等、分かりやすい利用ガイドの作成を義務化するなどの改正が望まれる。また共同利用の範囲としては、共同利用を認める範囲をより明確に線引きし、範囲を

より限定的にしていくことが望まれる。

このように、ICT の発展や新たな経営戦略の出現等によって、現行の法やガイドラインには現代に適合しきれていない部分が存在する。そのため、現状で起きている問題点を考慮し、改正をすることによって、時代に即した法やガイドラインとなり、利用者の情報が独り歩きしてしまうような状況を回避できるものと思われる。

2　個人情報漏えいの現状

本章では個人情報漏えい事件・事故の現状はどの程度のものなのか、JNSA セキュリティ被害調査ワーキンググループ[1]による『情報セキュリティインシデントに関する調査報告書』を参照し、考察する。なおこのデータは、新聞やインターネットニュースなどで報道されたインシデントの記事、組織からリリースされたインシデントに関連した文書などをもとにインシデントの情報を集計したものである。

2.1　個人情報漏えいに関する概要データ

2010 年、2011 年の個人情報漏えい事件・事故の概要データは図表 2、3 の通りである。2011 年の漏えい件数は、1551 件であり、前年と比べ 128 件の減少となっている。それにも関わらず、2011 年の漏えい人数が前年の 557 万 9316 人から 628 万 4363 人に増加しているのは、2011 年に発生した事件・事故のうち、大規模なものが数件あったためである。

しかし、全体的には、2007 年以降減少傾向にある。これは、漏えい件数が増加する一方で、一件あたりの漏えい人数が小さい 100 人未満の事件が増加していることが影響している。なお、2011 年の想定損害賠償総額は 1899 億円 7379 万円と、前年に比べ、約 85 万円の増加となった。

図表 2：2010 年 個人情報漏えいインシデント[2] 概要データ

漏えい人数	557 万 9316 人
インシデント件数	1679 件
想定損害賠償総額	1215 億 7600 万円
一件あたりの漏えい人数	3468 人
一件あたり平均想定損害賠償額	7556 万円
一人あたり平均想定損害賠償額	4 万 3306 円

（出典；「2010 年情報セキュリティインシデントに関する調査報告書」より引用）

図表 3：2011 年 個人情報漏えいインシデント 概要データ

漏えい人数	628 万 4363 人
インシデント件数	1551 件
想定損害賠償総額	1899 億 7379 万円
一件あたりの漏えい人数	4238 人
一件あたり平均想定損害賠償額	1 億 2810 万円
一人あたり平均想定損害賠償額	4 万 8533 円

（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より引用）

[1] JNSA セキュリティ被害調査ワーキンググループ･･･ネットワーク社会の情報セキュリティレベルの維持・向上及び日本における情報セキュリティ意識の啓発に努めるとともに、最新の情報セキュリティ技術および情報セキュリティへの脅威に関する情報提供などを行う特定非営利活動法人 (NPO)。

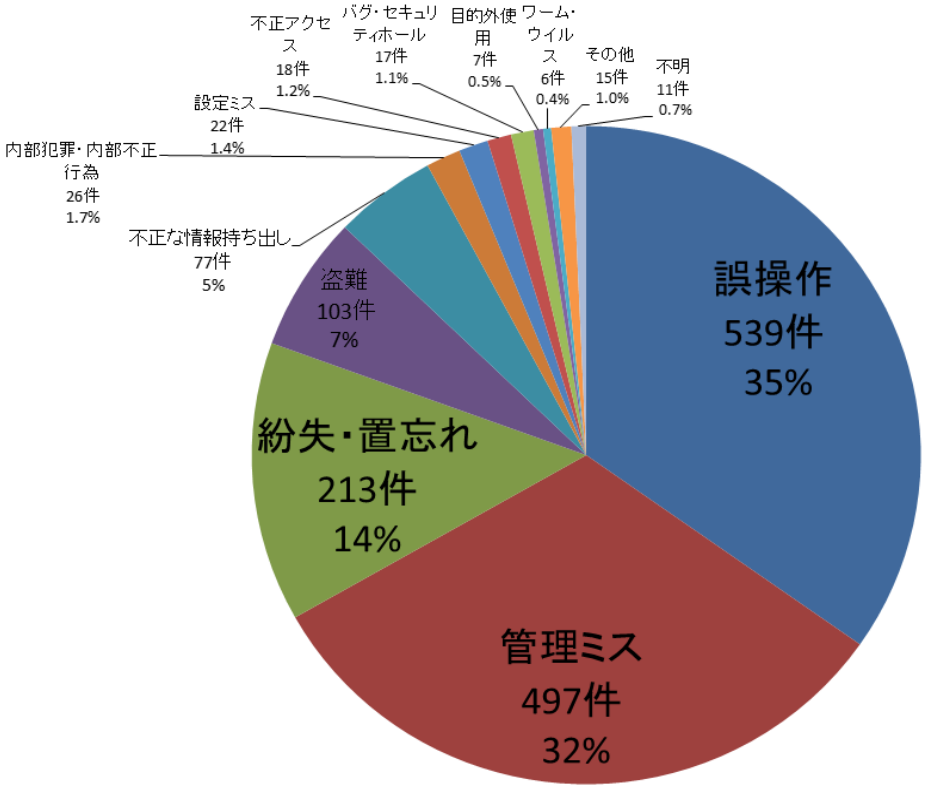
[2] インシデント･･･事件、出来事、ハプニングなどの意味を持つ英単語。ICT の分野では、情報管理やシステム運用に関して保安上の脅威となる現象や事案(セキュリティインシデント)のことを指す場合が多い。

2.2 個人情報漏えいの原因比率

2011 年の個人情報漏えい件数の原因比率は図表 4 の通りである。2011 年は「誤操作」、「管理ミス」、「紛失・置忘れ」で約 80%を占めた。「管理ミス」に区分されるものは、組織としてルールが整備されていないもしくはルールは存在しているものの遵守されていないために社内や主要な流通経路で発生する事件・事故である。組織としてルールが整備されていないことによる事件・事故は、発見が遅れ漏えいに至った経路を明確化できない場合も多い。一方、ルールが徹底されていないことによって発生する漏えいは、比較的早く発見され、経緯も明確化しやすい場合が多い。以上の事から考えられるのは、組織内で個人情報を守るためのルール作りをし、それを徹底することが、「管理ミス」による漏えいを防ぐ最も効果的な手段と言える。また万が一問題が発生した場合には、できる限り迅速に問題を発見し、発生経緯を明確にすることで、被害を最小限に留める必要がある。

最も大きな割合を占めた「誤操作」と 3 番目の割合を占める「紛失・置忘れ」は、ヒューマンエラー[3]である。そのための対策としては、人的な対策として担当者へのセキュリティ教育、および組織的な対策としてはヒューマンエラーを減らす予防効果が期待できる手順作りが重要となる。これに加え、ヒューマンエラーは必ず起こることを前提として暗号化などの漏えい対策や、紛失しても被害が拡大しない対策をあわせて行うことも必要である。

図表 4：2011 年 個人情報漏えい原因比率（件数）

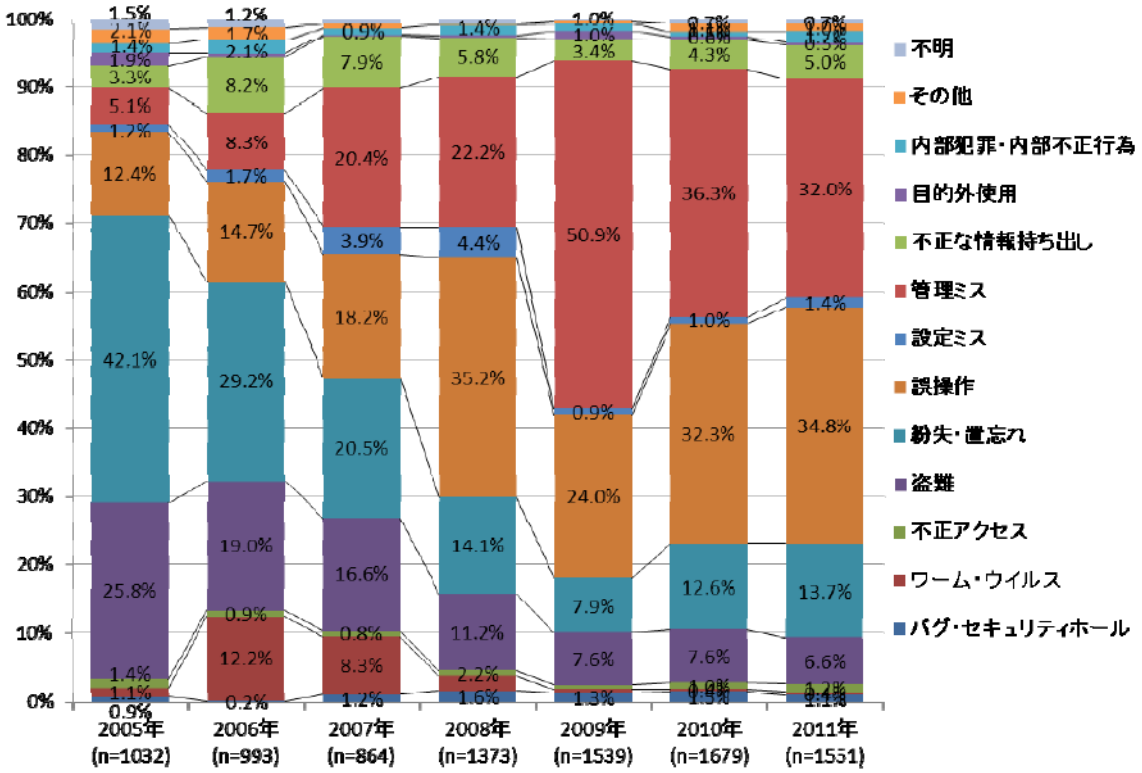


（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より筆者作成）

[3] ヒューマンエラー･･･事故の原因となる人的ミスのこと。

図表 5 に示したのは、個人情報漏えい件数の原因比率の経年変化である。2005 年と比較すると、管理ミスや誤操作の件数が大きく増加していることである。管理ミスおよび誤操作は、先にも述べたように、組織内のルールの整備・徹底をするによって改善することができるため、これらの増加は、個人情報の取り扱いに関する担当者の意識低下が原因であると考えられる。

図表 5：個人情報漏えい原因比率の経年変化（件数）

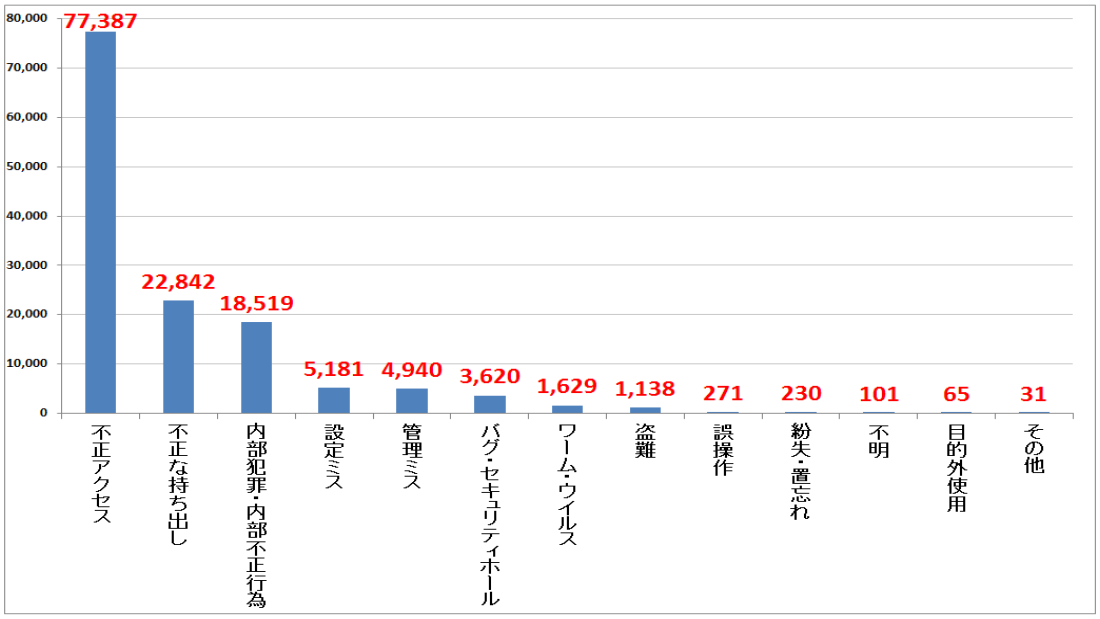


（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より引用）

2.3 漏えい原因別の一件あたりの漏えい人数

漏えい原因別の一件当たりの漏えい人数を図表 6 に示した。このグラフから見て取れるのは、「不正アクセス」の一件あたりの漏えい人数の多さである。先程参考にした漏えい原因別の件数では、非常に少なかったが、人数でみると非常に多く、被害が大きいことがわかる。「不正アクセス」は、悪意のあるものが個人情報の集まりであるファイルやデータベースを対象にして行うため、発覚すると常にまとまった数の個人情報件数が漏えいすると考えられ、件数が多い人的ミスと合わせて、万全な対策が求められる。

図表 6：漏えい原因別の一件あたりの漏えい人数（単位：人数）

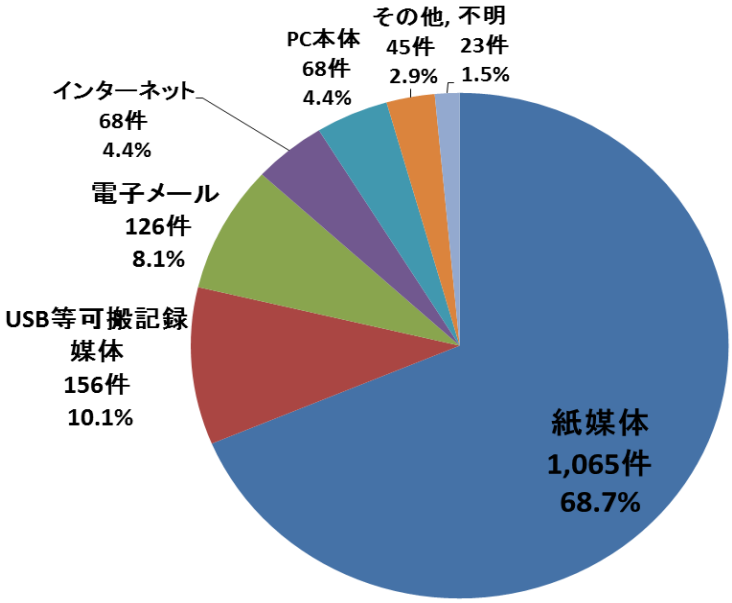


（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より筆者作成）

2.4 情報漏洩の媒体・経路

図表 7 に示したのは、漏えい媒体・経路別の事件・事故件数である。漏えい媒体・経路では、「紙媒体」が全体の 68.7%を占めている。紙媒体は、業種や業務内容に関わらず、どのような場面においても利用される、使用機会の多い媒体であるため、それだけ漏洩することが多いのである。

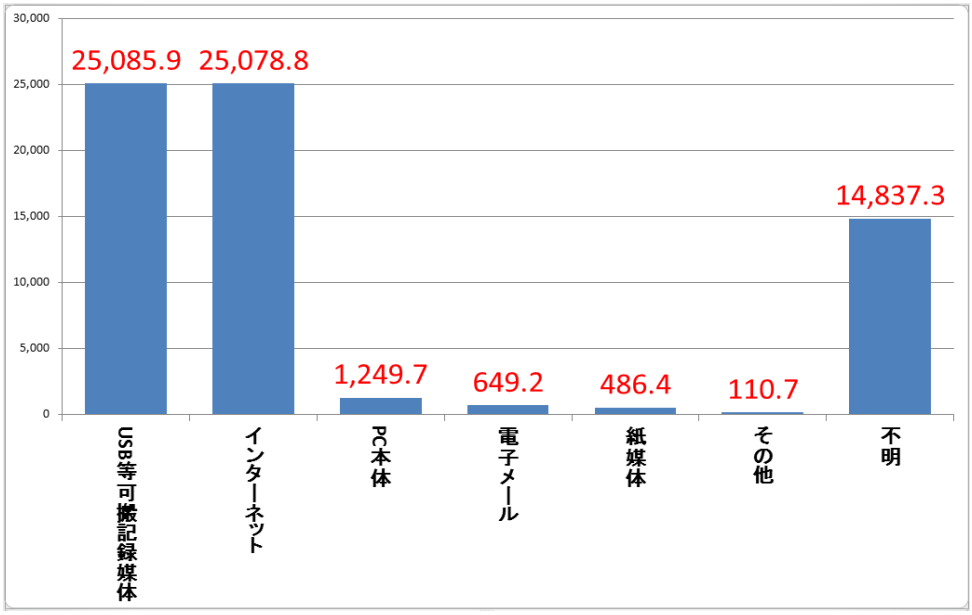
図表 7：漏えい媒体・経路（件数）



（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より筆者作成）

続いて図表 8 に示したのは、漏えい媒体・経路別の事件・事故一件あたりの漏えい人数である。漏えい媒体・経路別の一件あたりの平均漏えい人数は、「USB 等可搬記録媒体」「インターネット」が多い。これらが多い理由は、いずれも個人情報が扱いやすい電子データ（ファイル）に保存されており、一度に大量の個人情報が操作できることから、それらのデータを受け渡しやすい USB メモリやインターネットを経由して漏えいしたものと思われる。これらのことから、「USB 等可搬記録媒体」「インターネット」は「紙媒体」よりも漏洩する可能性は少ない反面、漏えいした場合に、大量の個人情報が漏えいする危険性があり、取扱いには十分な注意が必要になることがわかる。

図表 8：漏えい媒体・経路（人数）



（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より筆者作成）

2.5 経年分析

図表 9 に示したのは、2005 年から 2011 年の漏えい人数とインシデント件数の経年変化である。2011 年のインシデント件数は、2010 よりやや減少した。その一方で、漏えい人数は 2010 年よりも増加している。結果的には、個人情報が漏えいした人は、日本の人口の約 20 人に 1 人の割合であった。

また 2008 年以降、2006 年や 2007 年のような漏えい人数が非常に多い状況は発生していないが、2008 年から見れば、減少傾向にあるとはいえず、改善の余地がある。[4]

[4] 2006 年は winny などのファイル共有ソフトによって被害者数が大幅に増加し、2007 年は大日本印刷株式会社が大規模な個人情報漏えいを引き起こしたため、被害者数が多かった。

図表 9：漏えい人数とインシデント件数の経年変化

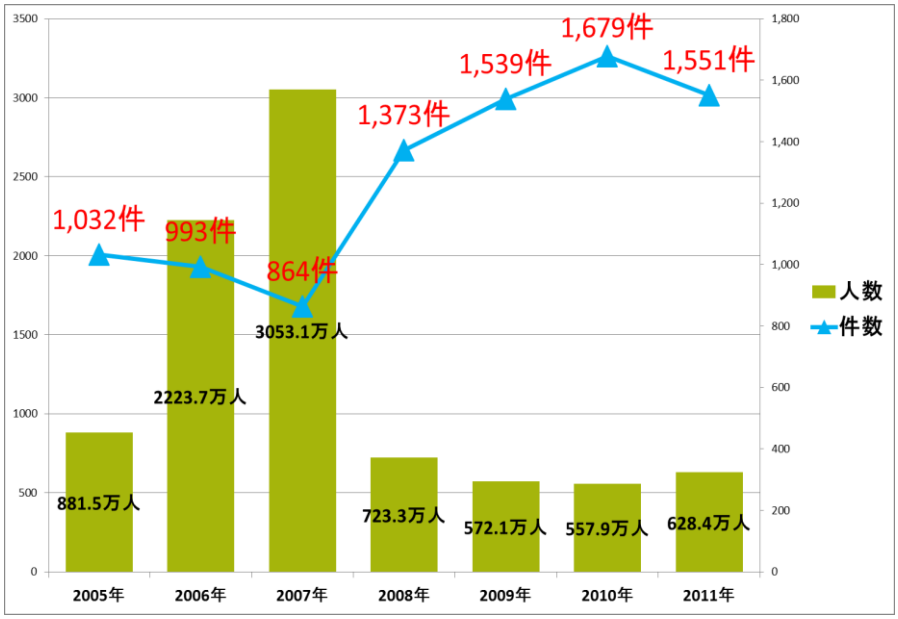
	インシデント件数	漏えい人数	一件あたりの平均漏えい人数※
2005 年	1,032 件	881 万 4,735 人	8,922 人
2006 年	993 件	2,223 万 6,576 人	2 万 3,432 人
2007 年	864 件	3,053 万 1,004 人	3 万 7,554 人
2008 年	1,373 件	723 万 2,763 人	5,668 人
2009 年	1,539 件	572 万 1,498 人	3,924 人
2010 年	1,679 件	557 万 9,316 人	3,698 人
2011 年	1,551 件	628 万 4,363 人	4,238 人

（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より引用）

次に、インシデント件数と漏えい人数の経年変化を図表 10 に示す。個人情報保護法が完全施行された 2005 年以降、個人情報漏えい事件を起こした組織が、積極的に事件を公表する姿勢が定着してきており、毎年 1,500 件程度の個人情報漏えい事件が公表されている。

突発的に発生する大規模な個人情報漏えい事件によって、その年の漏えい人数の傾向が大きく左右されることもあるが、2005 年から 2007 年まで増加傾向であったが、2008 年以降は減少傾向にある。それに対し、インシデント件数が増加傾向にある。このことから、大規模な漏えい事件が減少する一方で、小規模な事件が多く発生しているということである。

図表 10：インシデント件数と漏えい人数の経年変化



（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より筆者作成）

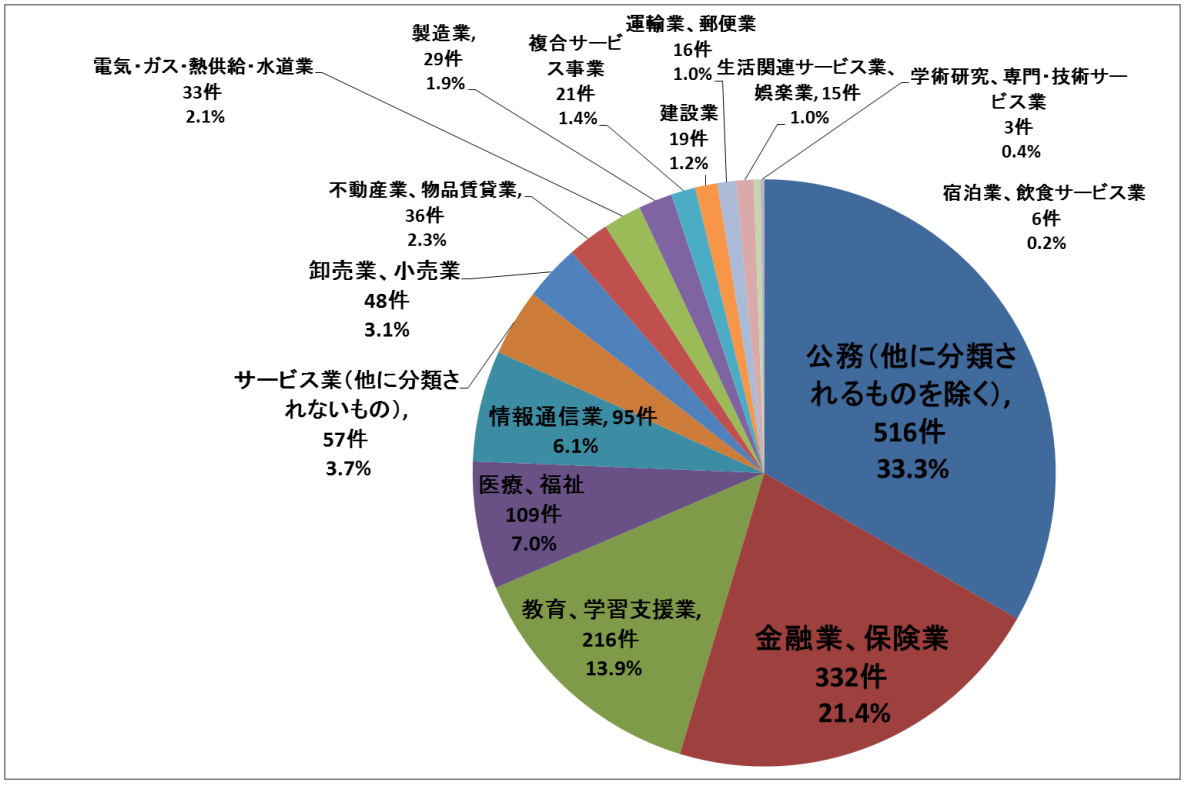
2.6 業種別比率

図表 11 に示したのは業種別のインシデント件数である。インシデント件数の多い業種は、「公務」（33.3%）、「金融業、保険業」（21.4%）、「教育、学習支援業」（13.9%）、「医療、福祉」（7.0%）であり、全体の約 75%を占めている。

「公務」および「金融業、保険業」については、2004 年以降、常に上位を占める結果となっている。これは、個人情報を取り扱うことが多いことに加え、個人情報保護に関する行政の指導が強く働いている業種であり、小規模な漏えい事件であっても公表することが多いためと考えられる。

しかし、個人情報を取り扱うことが多い業種であるからこそ、より厳重な対策について検討し、漏えい事件・事故の減少に尽力すべきであると思われる。

図表 11：業種別比率（件数）



（出典；「2011 年情報セキュリティインシデントに関する調査報告書」より筆者作成）

2.7 2 章まとめ

2.2 個人情報漏えいの原因比率で示した通り、2011 年では個人情報漏えいの原因で多いものが「誤操作」、「管理ミス」、「紛失・置忘れ」と人的ミスによるものが約 80%を占めた。原因比率の経年変化を見ても、2005 年と比較すると、管理ミスや誤操作の件数が大きく増加していることである。これらを減少させるためには、組織内で個人情報を守るためのル

ール作りをし、それを徹底することが、「管理ミス」による漏えいを防ぐ最も効果的な手段と言える。また万が一問題が発生した場合には、できる限り迅速に問題を発見し、発生経緯を明確にすることで、被害を最小限に留める必要がある。

しかしながら、このような人的ミスは、ケアレスミスが原因であることが多いため、完全にゼロにすることは難しい。よって、電子メールや USB メモリなどを利用し、データを扱う際は、暗号化やパスワードの設定などをし、誤送信や紛失をした場合にも情報が漏えいしないよう対策することも合わせて必要である。

また　2.3 漏えい原因別の一件あたりの漏えい人数で示した通り、「不正アクセス」の一件あたりの漏えい人数が非常に多い。被害件数は少ないものの、「不正アクセス」は、ファイルやデータベースを対象にして行うため、多くの人数のデータが漏えいしてしまう。紙での管理から電子データでの管理になり、利便性が向上する反面、まとまったデータが漏えいする危険性があるため、その点を留意し、取り扱う必要がある。

そして 2.6 業種別比率で示した、業種別の漏えい比率では「公務」および「金融業、保険業」の比率が高いことが分かった。この 2 業種が取り扱う個人情報は、非常に機密性の高いものであることも多く、個人情報を取り扱うことが多い業種であるからこそ、より厳重な対策について検討し、漏えい事件・事故の減少に尽力すべきであると思われる。

これまでのデータを見る限り、USB メモリや、インターネットから情報が漏えいした事件は、紙媒体などから情報が漏えいした事件よりも件数自体は少ないものの、一度に大量の個人情報が漏えいする傾向にあり、被害も甚大になる傾向にある。これらのことから、ネットワークや情報機器の利用によって個人情報を扱いやすくなり、利便性が向上した反面、大規模な情報漏えい事件になり得るリスクも高まっているといえる。これらのことから、個人情報の取り扱い、とりわけ、ネットワーク上や情報機器を利用した個人情報の取り扱いには、注意を払うべきであると思われる。

また参考までに、現時点で最新のデータとなる 2012 年上半期の集計結果を、以下に示しておく。

図表 12：2012 年上半期 個人情報漏えいインシデント 概要データ【速報】

漏えい人数	123 万 9626 人
インシデント件数	954 件
想定損害賠償総額	347 億 9865 万円
一件当たりの平均漏えい人数	1349 人
一件当たり平均損害賠償額	3787 万円
一人当たり平均損害賠償額	5 万 7710 円

（出典；2012 年情報セキュリティインシデントに関する調査報告書【上半期 速報版】より引用）

図表 13：2012 年上半期 個人情報漏えいインシデント 概要データ【速報】

No.	漏えい人数	業種	原因
1	40 万 6632 人	金融業，保険業	管理ミス
2	17 万 1518 人	情報通信業	不正アクセス
3	11 万人	サービス業(他に分類されないもの)	不正アクセス
4	10 万人	金融業，保険業	管理ミス
5	8 万人	運輸業，郵便業	管理ミス
6	3 万 5694 人	医療，福祉	紛失・置忘れ
7	3 万人	生活関連サービス業，娯楽業	盗難
8	2 万 7567 人	サービス業(他に分類されないもの)	設定ミス
9	2 万 7284 人	金融業，保険業	管理ミス
10	2 万 1764 人	金融業，保険業	管理ミス

（出典；2012 年情報セキュリティインシデントに関する調査報告書【上半期 速報版】より引用）

3　事例から見る個人情報保護

本章では、過去にあった個人情報漏えい事件や社会で大きな注目を集めた個人情報収集事例などを取り上げ、その被害の規模や手口などを考察していく。

3.1　ヤフーBB 顧客情報漏えい事件

当事件は、2004 年 2 月に発生した、ソフトバンクグループが運営する ADSL サービス「ヤフーBB」の加入者名簿約 462 万人分が漏えいし、恐喝の材料に利用されていた事件で、日本最大規模の情報漏えい事件である。

事件の概要は以下の通りである。「ヤフーBB」の加入者情報が記録された DVD を入手した男が、同サービスの運営母体である「ソフトバンク」のグループ企業関係者に数十億円を要求し、警視庁に恐喝未遂容疑で 2 グループ計 4 人が逮捕された、というものである。

ソフトバンク側は殺到する苦情に対しお詫びの電子メールを送付したが、苦情が沈静化しないことから、ソフトバンク BB 全加入者に対して 500 円の金券を配布し謝罪した。しかし、5 月 19 日、大阪地方裁判所において、この事件の個人情報漏えいで精神的苦痛を受けたとして、Yahoo! BB 会員ら 5 人が、運営会社の BB テクノロジーとヤフーに、慰謝料など 1 人当たり 10 万円の損害賠償を求めた民事訴訟の判決があり、1 人につき 6000 円の支払いが命じられた。今回は少額の賠償金と少人数による訴訟であったが、仮に被害に遭った会員全員から賠償請求があったとしたら、膨大な金額になっていたことになる。

漏えいした原因としては、サポートセンターに所属している数千人の派遣社員が同一の ID、パスワードでデータにアクセス可能だったずさんな情報管理体制にあり、その ID とパスワードから顧客データベースにアクセスされ、情報が漏えいした。

データベースの形で個人情報を管理することによって、利便性が向上するが、情報の管理体制を万全なものにしておかなければ、大規模な被害に繋がってしまう典型的な例であると言える。

3.2　PlayStation Network 個人情報漏えい事件

当事件は、2011 年 4 月にソニー・コンピュータエンターテインメント(SCE)が PlayStation シリーズに提供するオンラインサービスである PlayStation Network (PSN)への不正アクセスにより、同サービスに登録している会員の全員分である 7700 万件の個人情報を含む会員情報が漏えいした事件である。会員は米国が中心で、アジアの約 900 万人の大半は日本人であるという（1 人の利用者が複数のアカウントで登録できるため、登録会員数と実際の人数は一致しない)。流出した個人情報は、「氏名」「国と住所」「メールアドレス」「誕生日」「性別」「PSN のログインパスワード」「PSN のオンライン ID」である。

不正アクセスを受けた根本的な原因としては、アプリケーションサーバーの脆弱性に対処していなかったことにあるといわれている。PSN では、アプリケーションサーバーと呼ばれるプログラムにすでに認識されていた脆弱性があり、ここを犯人に突かれて侵入され

た。ファイアウォールや IPS（侵入防止システム）はあったものの、それを通り抜けて攻撃を受けている。これについてソニーの業務執行役員・長谷島眞時氏は「正規の通信として、入って出てくる方法で脆弱性を突かれている。そのため不正アクセスとして検知できなった」と述べている。

最大の問題は、脆弱性に対処していなかったことにあり、多くの利用者の個人情報を所有しているにも関わらず、対処を怠っていたことは、ネットワークの管理方法に問題があったといえる。

今回の事件を受けて同社では、従来から予定されていたサンディエゴのデータセンター移転を前倒しし、よりセキュリティレベルの高いデータセンターへシステムを移転。不正アクセスに対するソフトウェアの自動的なプロセス監視機能、環境設定項目の管理機能を強化し、データ保護と暗号化のレベル強化、PSN への不明なソフトウェアの侵入、不正アクセス、不信行為の検知能力の向上、新たなファイアウォールの増設といった技術的対策を行った。その後、2011 年 5 月から段階的にサービスが再開されたが、犯人は未だに特定されていない。

この事件は、不正アクセスにより、世界中のサービス利用者の個人情報が漏えいした。インターネットを利用することにより、世界中といつでもどこでも通信できる反面、情報漏えい事件が起きた場合、世界規模にまで被害が拡大してしまう危険性があるということが示された事件であるといえる。

3.3　大日本印刷の関連会社元社員による個人情報漏えい

当事件は、2007 年 3 月、印刷会社である大日本印刷が、2001 年から 2004 年の間に DM 印刷等のために企業から預かった個人情報が業務委託先の元社員によって不正に持ち出されていた事件である。持ち出された個人情報は取引先の 43 社分で、合計 863 万 7405 件にのぼり、流出した個人情報の内容は、「郵便番号」「住所」「氏名」「電話番号」「生年月日」「性別」「メールアドレス」「ユーザーID」などで、「クレジットカード番号」も流出した企業もある。

ダイレクトメールのデータを加工する電算処理室に出入りしていたシステム開発会社の元社員が、2006 年 3 月まで約 5 年間にわたって、フロッピーディスクや MO ディスクに書き込んで持ち出し、一部をカード詐欺グループに売り渡していた。667 万円もの実害が発生しているにもかかわらず、元プログラマへの容疑は MO ディスク 1 枚、250 円相当の窃盗であるという。

大日本印刷によると、流出が分かった 43 社のうち、最も件数が多かったのはアメリカンホーム保険（150 万 4857 件）であった。その他にもイオン（58 万 1293 件）、NEC ビッグローブ（21 万 4487 件）、日本ヒューレット・パッカード（16 万 3111 件）、UFJ ニコス（119 万 336 件）、トヨタ自動車（27 万 3277 件）、KDDI（11 万 3696 件）、NTT ファイナンス（43 万 9222 件）などの企業の情報が流出している。

また同社は同年 2 月に、大手信販会社であるジャックスから販促用ダイレクトメールの作成のために預かった「JACCS カード」の会員情報約 15 万件が、業務委託先の元社員によって持ち出され、インターネット通販詐欺グループに売り渡されていた事実を明らかにしていた。この事件では、会員情報が悪用された結果、49 会員、667 万 2989 円分の実害が発生していた。

同社はこれまで、委託先との個人情報に関わる契約の締結、電算処理室におけるプライバシーマークの取得、電算処理室への監視カメラ設置、電算処理室での生体認証による入退室管理、データなどの持ち出し防止を目的とするポケットのない作業服の着用、アクセスログの取得などを実施し、情報管理体制の強化を実施してきたという。しかし同社は「今回のような、悪意を持った内部者による不正な記憶媒体へのデータ書き出し行為を防止する上で、結果として管理に不十分な面があった」と原因を分析している。

この事件を受け同社は、(1) 個人情報の取扱者の限定、(2) データ書き出し防止とチェック機能の強化、(3) 外部の IT ベンダーなどによる監査、といった運用面の対策を行った。個人情報を記憶媒体に書き出す担当者を大日本印刷および同社子会社の計 4 人に限定し、個人情報を書き出しできるエリアを決め、同エリア内では扱うデータに暗号化を施す。データ書き出し作業のログと対応する出荷記録、記憶媒体の数量をそれぞれ毎日確認するという対策を施した。

大日本印刷は事件が発生する以前にも、一定程度の情報管理体制を整えていたが、多くの個人情報を有している企業として、また入退出の管理などのセキュリティ関連ビジネスなども展開している企業としては、不十分な情報管理体制であったといえる。

当事件は、外部からの攻撃に対する対策だけでなく、企業内部の不正行為によって情報が漏えいする危険性を考慮した情報管理体制を整えることの必要性を示しているといえる。会社支給の PC、少なくとも転職者や退職者が使用していたものについてはすぐにデータを消去するのではなく、不正な利用履歴がないか調査をしたうえでデータを消去すべきであると思われる。

また、大日本印刷はプライバシーマークを取得していたにも関わらず、大規模な情報漏えい事件を発生させてしまったことや、その後、プライバシーマークの「認定取消」に至らなかったことから、プライバシーマークは「絶対保証」の制度ではなく、人的対策の整備や委託先の監督を含めた継続的改善が伴わなければ意味をなさないという課題が浮き彫りになった事件であるといえる。

3.4　三菱 UFJ 証券、顧客情報漏えい事件

当事件は、大手証券会社である三菱 UFJ 証券のシステム部の元社員が顧客情報 148 万 6651 人分を不正に持ち出し、うち 4 万 9159 人分の情報を名簿業者に売却した事件である。流出した顧客情報は氏名、住所、電話番号、性別、生年月日、職業、年収区分、勤務先名、勤務先の住所と電話番号、部署名、役職、業種である。

元社員はシステム部の部長代理で、エンドユーザーのコンピュータの操作やデータ処理などを支援する立場を悪用した。2009 年 1 月 26 日、元社員は顧客データ処理担当の社員の ID とパスワードを悪用し、障害対応目的と偽って顧客データ管理用のサーバーにアクセスした。サーバーを設置していた部屋には監視カメラがあり、かつ IC カードで入退管理をしていたという。元社員は 148 万 6651 人分の顧客情報を暗号化し、作業用のサーバーに保存した。作業用のサーバーには元社員を含む 8 人がアクセス可能で、個別に ID とパスワードを付与していた。

通常は作業用サーバーから外部記録媒体に顧客情報をコピーして持ち出すことはできないが、元社員は毎月 1 回のマーケット情報を記録した CD を作成する作業の際に、オペレータに対して「特殊な作業」と偽り、暗号化した顧客情報を CD に保存するよう指示。CD をシステム部で作業すると偽って自宅に持ち帰り、パソコンのハードディスクに顧客情報を保存した。

元社員は金銭目的で、顧客情報を名簿業者に売却し、業者には 1 万人分の単位で情報をメールで送信した。名簿業者 3 社に対して、2008 年 10 月 3 日から 2009 年 1 月 23 日までに計 4 万 9159 人分の顧客情報を売却し、その後流出先が 98 社まで拡大した。同社は 3 月中旬以降、「(同社に) 最近提出した連絡先に業者から勧誘があった」との連絡を顧客から受け、緊急対策本部を設置して調査を進めていた。名簿の転売先は不動産投資会社などで、顧客からの問い合わせ件数は 6 月には 1 万 5000 件超に上った。顧客に対し、夜間に勧誘の電話がかかったり、1 日に何度も電話がかかったりしたという。中には精神的苦痛を訴える顧客もいた。

金融庁は元社員が不正行為の監視対象外であったことや、情報を CD に保存したり貸し出しをしたりする際の承認手続の確認が徹底されていなかったことが情報流出の要因であると指摘し、情報システムの管理をシステム部自身の所管としていたためにけん制が働きにくかった点などを挙げて、「内部管理態勢が十分でない」とし、業務改善命令と勧告を求めた。また同社の調査では、元社員が顧客情報データベースにアクセスする際に使用した嘱託社員 ID は、本来なら使用できなかったもので、嘱託社員が異動の際にアクセス権限は削除されるはずだが手続き上のミスで残っていたという。これらのことから、同社の情報管理体制が不十分であったことがわかる。

同社は事件後、これまではシステム部内でセキュリティを管理していたものを、別部署である情報セキュリティ管理部が一元管理することで監視・けん制を強化した。さらにシステム部をシステム統括部とシステム推進部という二つの組織に分割し、システム推進部を運用と開発のそれぞれの組織に分けてお互いがけん制できる態勢にするなどの対策を行った。

その後、元社員は懲役 2 年の実刑判決を受けた。当事件により同社は、148 万人のうち情報が流出した約 5 万人に対して、「お詫びのしるし」として 1 万円相当のギフト券を 6 月下旬から発送した。この費用が約 5 億円であった。このほか、事件調査や顧客からの問い合

わせ対応、顧客情報の売却先となった業者と交渉するための弁護士費用、機関投資家からの発注減少による逸失利益などを合算すると、約 70 億 3500 万円の損失になったという。

当事件から、個人情報が漏えいした場合、その被害の大きさや対応によっては、企業にとって莫大な損失になることがわかる。そして何より、個人情報の管理体制が不十分であったことが明るみになった場合、社会的信用が大きく損なわれ、その後の企業活動に悪影響を及ぼすことが最も大きな損失であると考えられる。

3.5　米国家安全保障局による個人情報収集

2013 年 6 月、米国家安全保障局（NSA）がテロ対策を名目に個人の通話記録やインターネット上の情報を秘密裏に収集していたことが明らかになり、世界中に衝撃を与えた。NSA とはアメリカ国防総省の諜報機関で、通信、電磁波、信号などを媒介とした情報収集活動や分析などをおこなっている。

NSA による個人情報収集が明るみに出た経緯は以下の通りである。まず 2013 年 6 月 6 日、複数の海外メディアが Apple、Google、Facebook、Microsoft などが運営するネットサービスのサーバーに NSA が直接アクセスしてユーザーのデータを収集する「PRISM」という取り組みを行っていると相次いで報道した。さらに英 Guardian 紙は同じ 6 月 6 日、NSA が米大手通信会社である Verizon からサービス加入者の通話記録を収集していたことが、極秘の裁判所命令を入手したという記事をオンライン版に掲載した。この極秘命令は、Verizon に対して国内および国際通話に関するすべての情報を、継続的に毎日 NSA に提出するよう要請している。外国情報監視裁判所（FISC）が 4 月 25 日に発行したもので、7 月 19 日までの 3 カ月間にデータを収集する無制限の権限を政府に認めている。同命令のもと、通話者双方の電話番号、位置情報、通話時間といった情報が引き渡されたが、会話の内容は含まれていないという。

6 月中旬になり、NSA の情報収集の手口をリークした元 CIA 職員、エドワード・スノーデン氏が実名でインタビューに登場した。スノーデン氏は CIA 退職後に NSA の外注契約職員として、NSA の個人情報収集プログラムに関わってきた。スノーデン氏によると、NSA は中国をはじめとする世界中で情報収集のためのハッキングを繰り返しており、米国内でも裁判所の令状無しに違法に通信を傍受しているという。

こうした報道を受けて、人権団体などを中心に強い批判の声が上がった。こうした批判に対して、NSA のジェームズ・R・クラッパー長官は 6 月 8 日、「最近掲載された記事により、誤った印象がもたれている」とする声明を発表した。声明によると、PRISM は「米政府が法で認められた権限により、裁判所の監督下で、電子通信サーヴィスプロヴァイダーから米国外の諜報情報を収集するのを促進するために利用される、米政府内のコンピュータシステム」であり、情報収集の対象は基本的に米国外にいる「非米国人」に限られるという。続く 6 月 15 日には米上院の情報委員会が、NSA の情報収集プログラムによって米国と世界 20 カ国以上で数十に及ぶテロを阻止できたとして、その重要性を強調する報告書

を公開した。文書には、NSA のプログラムが「外国情報監視裁判所（FISC）」によって承認されていること、プログラムが 90 日ごとに精査されていること、収集した情報は 5 年経過すると消去されることなどが記されており当局が収集しているデータには電話番号や通話時間が含まれているが、通話内容、携帯電話の位置情報は含まれていない。米国外のテロリストが米国内の実行犯などと連絡を取り合っていることなどを察知して、当局は初めて詳細を調べる。その数が 2012 年の 1 年間で 300 件未満だったと説明した。

一方、NSA の情報収集に協力していると名指しされた大手 IT 企業のうち、Google と Facebook は 6 月 7 日、PRISM への関与を否定するコメントを発表した。このうち Google は 6 月 11 日、米司法長官と米連邦捜査局（FBI）に、外国情報監視法（FISA）にもとづく情報開示要請の件数などの公表を許可するよう求める書簡を送った。Google は違法な情報収集への協力を否定する一方で、合法な情報開示要請があったことは認めている。そのうえで、情報開示要請の件数および範囲を同社の「Transparency Report」に掲載して、政府の情報開示要請に応じた対象アカウントが全アカウントのごく一部に過ぎないことを示したかったためである。その後、Google に続いて Microsoft、Facebook なども情報開示要請の公表を許可するよう米政府に要求。Microsoft、Facebook、Apple は 6 月中旬、要請件数および対象となったアカウント数を 1000 単位の大まかな数字で公表した。最初に声を上げた Google は 6 月 18 日、情報開示要請の総数ではなく、国家安全に関する個別の件数と対象アカウント数といった、より詳細な情報を開示できるように求める動議を外国情報監視裁判所（FISC）に提出したが、いまだに許可は得られていない

また 2013 年 9 月 5 日、NSA や GCHQ（英国政府通信本部）は、「HTTPS」や「SSL」などを含むインターネット上の暗号化通信を解読可能であると、2013 年 9 月 5 日に英ガーディアン紙や米ニューヨークタイムズ紙などが報じた。エドワード・スノーデン氏がガーディアンに提供した秘密文書から判明したという。これを受けて Twitter や Microsoft などが対抗策を強化しているといわれている。

さらに、9 月 7 日には、ドイツの週刊誌「SPIEGEL」が、米国と英国の情報当局がほぼすべての主要メーカーのスマートフォンに侵入して個人情報を入手できる状態であることを示す極秘文書を確認したと報じた。SPIEGEL の記事によると、NSA は、米 Apple の「iPhone」やカナダ BlackBerry のスマートフォン、および米 Google のアンドロイドを搭載したスマートフォンから、連絡先リスト、ショートメッセージングサービス（SMS）トラフィック、位置情報など、ほとんどの重要データにアクセスできるという。また同誌は 9 月 15 日にも、NSA が銀行やクレジットカードの国際決済も広く監視していることを報じた。NSA は、金銭追跡部門が収集したデータを「Tracfin」と呼ばれるデータベースに保存し、2011 年に 1 億 8000 万件の記録が集められ、そのうち約 84%はクレジットカード取引に関するものであったという。また 2010 年に、NSA は欧州、中東、アフリカを監視する目的で、Visa など大手クレジットカード会社の顧客の決済記録を監視していたことも判明したとしている。

情報をリークした元 CIA 職員、エドワード・スノーデン氏は現在、ロシアに亡命しており、今後も米政府の機密情報をリークする可能性が高く、NSA が行っていた情報収集に対する全容はつかめない。そのような中、2013 年 12 月 16 日に、米ワシントン DC の連邦地方裁判所が NSA の個人情報収集活動に関して、「違憲の疑いが強い」との見解を示し、これまで入手した通話記録の廃棄を命じた。裁判所の判決理由によると、米国人の通話のほとんどを自動記録する NSA のプログラムは米国憲法に違反している可能性が極めて高いと判断したためという。ただし、政府が上訴するまでの期間、命令の履行を保留するとしている。その一方で、米ニューヨーク連邦地裁は 2013 年 12 月 27 日、SA の個人情報収集活動に関して「すべてを集めるからこそテロ対策の重要な武器になる。テロ対策は空前の規模になっている」と必要性を認め、合衆国憲法に合致するとの判決を下した。このように地裁によって判断が分かれたことで、合憲性を巡る判断は最終的に最高裁に委ねられるとみられており、今後 NSA による情報収集活動がどのような展開を見せるかは不明確である。

しかし、その活動は継続される可能性もあり、また情報収集活動を行っているのが米政府のみでない可能性も考えられる。そのため、インターネット上のサービスを利用する際は、利便性と引き換えに個人情報を提供している、また、個人情報が漏えいする危険性がある、という意識を持ったうえでの節度ある利用を心掛ける必要があると考えられる。

3.6　「LINE」による電話帳情報収集

当事例は、現行の個人情報保護法では違反には当たらないものであるが、道義的に検討した場合いくつかの問題点が考えられる、「LINE」による情報収集の事例について考察する。

「LINE」とは、LINE 株式会社から提供されている無料通話やチャットが行えるアプリケーションであり、ほとんどのユーザーはスマートフォンで利用するが、フューチャーフォン、PC でも利用することができる。サービス開始後から爆発的な普及が進み、2013 年 11 月 25 日には登録ユーザー数が全世界で 3 億人を突破した。

「LINE」を利用するには、自身の電話番号を登録するだけで、ユーザー登録が完了し利用を始めることができる。「LINE」を利用して連絡を取る場合は、「友だち」に相手ユーザーを追加することで連絡することができる。しかし、この「友だち」に追加する方法にいくつかの問題点が存在する。

サービスが開始された 2011 年 6 月当初、「LINE」を利用するにはアドレス帳に登録された情報を運営会社のサーバーにアップロードすることが必須であった。この点に関してユーザーから批判を受けたため、同年 11 月にアドレス帳の利用を選択できるように変更したが、現在もアドレス帳の内容をアップロードする人が大多数である。その理由は「友だち」登録の手軽さにある。アドレス帳を利用した場合、LINE に登録している「友だち」と自動的にマッチングされ、連絡を取ることができる。したがって、この機能を利用しない場合、1 人ずつ手動で登録しなくてはならず、手間がかかってしまうのである。

しかし、「LINE」のユーザーがアドレス帳の内容をアップロードした場合、アドレス帳に登録された全員の情報が、本人が把握していないところで運営会社のサーバーに送信されることになる。LINE 株式会社は、「アドレス帳の利用目的はプライバシーポリシーに記載し、同意したユーザーにだけ送信して頂いている。極力、情報は取らない方針だ」として、LINE が収集する情報は、電話番号のみで、アドレス帳の名前、住所、などは対象ではないと説明している。

これに関して個人情報保護法の観点から検討した場合、電話番号のみで個人を特定することはできないため、「個人情報」には当たらない。そのため、個人情報保護法による規制は受けないことになる。しかしながら、本人が把握していないところで電話番号が第三者に送信されるというのは、道義的に問題が生じると思われる。アップロードされたアドレス帳の情報は、暗号化された上で保存されるというが、自分の知人・友人の個人情報が本人の許諾なく送信されるという点については、ユーザーへの周知が不足しているように思われる。現行の個人情報保護法では規制対象ではないため、LINE 株式会社としては、ユーザーが不安を感じないためのサービスの改善を検討するべきであると思われる。また、サービスに対して不信感を持つユーザーは、アドレス帳をアップロードしない設定にすることや LINE の利用を中止するべきであると考えられる。

現在、LINE に限らず、無料通話やチャットをすることができるアプリは利用者を拡大してきているため、上記で示したような問題に対しても対処できるような個人情報保護法の改正を検討すべきであると思われる。

4　スマートフォンの普及にみる個人情報漏えい

近年、スマートフォンが急速に普及してきている。我が国の携帯電話端末の総出荷台数に占めるスマートフォン出荷台数比率は、2012 年度、約 71.0%を占めており、同年末にはスマートフォンの世帯普及率が約 3 割となり前年度の約 3 倍増となるなど、幅広い層への普及が進んできているといえる。

高度な情報処理機能が備わったスマートフォンは、様々なアプリケーション、通称「アプリ」をインストールすることにより、電話やメール機能などの他に多様な目的のために活用することができる。

しかしその一方で、アプリがスマートフォンの内部に蓄積された利用者の利用履歴や通信履歴にアクセスし、それぞれの情報がどのように共有され利用される可能性があるか、利用者が十分に把握しないままに、個人情報が漏えいしている可能性がある。

またスマートフォンからの情報漏えいの危険性としては、アプリレイヤーからだけでなく、ネットワークレイヤー、OS レイヤーからの漏えいの危険性もあり、この 3 つのレイヤー別に対策を講じていく必要性がある。

そこで本章では、近年のスマートフォンの普及に伴い増加している、「アプリ」から個人情報が漏えいしている現状を中心に考察し、その後ネットワークレイヤー、OS レイヤーからの漏えいの危険性についても考察し、それぞれの対策を検討する。

4.1　スマートフォンの現状

4.1.1　スマーフォンとは

スマートフォンの明確な定義は存在しないが、本論文では、「高度な情報処理機能が備わった携帯電話端末」ではなく、「電話機能が備わった小型 PC」と定義したい。

スマートフォンの主な特徴としては、以下のような特徴が挙げられる。

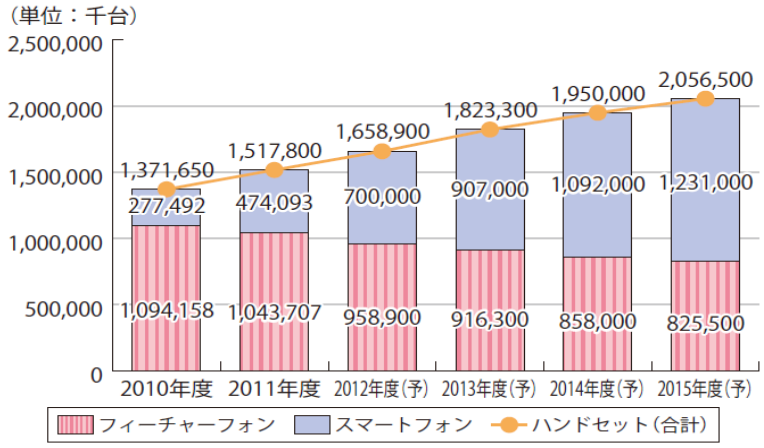
・アプリをインストールし、様々なサービスの利用や自分好みの機能カスタマイズが可能。
・携帯電話回線だけでなく、無線 LAN 等を通じてインターネットに接続可能。
・タッチパネルが採用され、PC・スマートフォン向けウェブサイトを閲覧可能。
・PC と同等の高い処理機能を搭載している。

4.1.2　普及率

上記のような特徴があるスマートフォンは近年、世界的な普及がみられる。図表 14 は、国内外フィーチャーフォン、スマートフォンの出荷台数実績・予測を示したグラフである。2011 年の全体に占めるスマートフォンの比率は、世界市場では約 3 割に達し、国内では約 6 割にまで達している。今後もスマートフォンの比率は拡大を続け、2014 年には世界市場においても 5 割を超える見通しとなっている。

図表 14：国内外のハンドセット（フィーチャーフォン+スマートフォン）出荷台数実績・予測

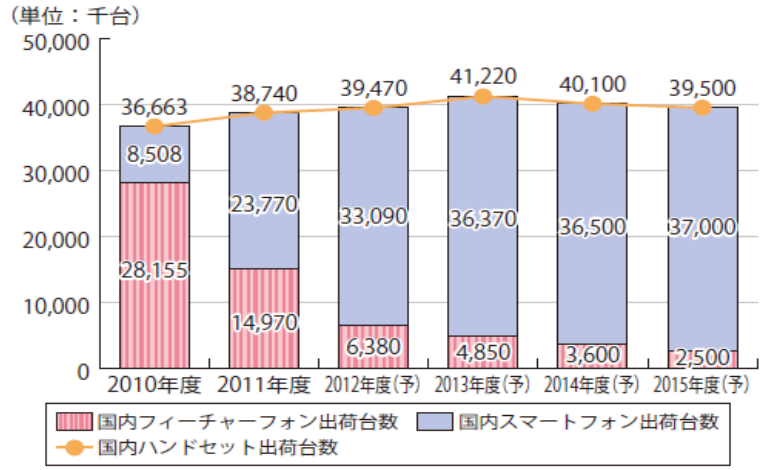
【世界市場】



単位：千台

	2010年度	2011年度	2012年度（予）	2013年度（予）	2014年度（予）	2015年度（予）
フィーチャーフォン	1,094,158	1,043,707	958,900	916,300	858,000	825,500
スマートフォン	277,492	474,093	700,000	907,000	1,092,000	1,231,000
ハンドセット（合計）	1,371,650	1,517,800	1,658,900	1,823,300	1,950,000	2,056,500

【国内市場】



単位：千台

	2010年度	2011年度	2012年度（予）	2013年度（予）	2014年度（予）	2015年度（予）
国内フィーチャーフォン出荷台数	28,155	14,970	6,380	4,850	3,600	2,500
国内スマートフォン出荷台数	8,508	23,770	33,090	36,370	36,500	37,000
国内ハンドセット出荷台数	36,663	38,740	39,470	41,220	40,100	39,500

（出典；『平成 25 年版 情報通信白書』より引用）

4.2　スマートフォンをめぐるサービス構造

従来の携帯電話端末においては、通信事業者が端末、プラットフォーム [1] 及びコンテンツ・アプリケーションの各々に影響を与えると言われる垂直統合モデルのサービス提供構造があり、利用者に対して通信事業者がワンストップにサービスを提供する傾向にあった。

一方、日本国内市場において 2008 年 7 月に iPhone が 2009 年 7 月にアンドロイド OS 搭載端末が発売された。その後急速に普及が進んだスマートフォンにおいては、水平分業モデルのサービス提供構造が見受けられ、様々な事業者が特定のレイヤー[2] または複数のレイヤーに係る事業を展開している。

この中でスマートフォンに搭載されるオペレーティングシステム（OS）[3] を提供する者は、コンテンツやアプリ提供サイトの運営 [4] も行っており、端末開発、通信ネットワーク利用、アプリケーション提供、課金や認証等の各レイヤーに影響力を有する存在であるといえる。

また、コンテンツ市場においては、100 万以上の「アプリ」が提供されているといわれており、「アプリ」を自由にインストールして利用することが一般的であるスマートフォンの特性を踏まえ、多種多様な「アプリ」が様々な開発者等によって提供されている。

スマートフォンのアプリケーションの中には、無料または低額で利用可能となるものが多くある。このようなサービス構造において、広告配信による収益化を図る場合もあり、さらには広告配信事業者が提供する情報収集モジュール [5] を組み込むことにより、アプリケーション開発者が一定の対価を得る事例もあると指摘される（図表 15）。これについては、後に詳しく考察する。

このように、水平分業モデルのサービス提供構造になったことで、通信事業者がすべてのサービスを把握することが難しくなっている現状がある。

---

[1] プラットフォーム･･･アプリケーションソフトを動作させる際の基盤となるオペレーションシステム（OS）の種類や環境、設定などをいうが、広義には、コンテンツやアプリケーションなどの利用を可能とする「場」のことをいう。

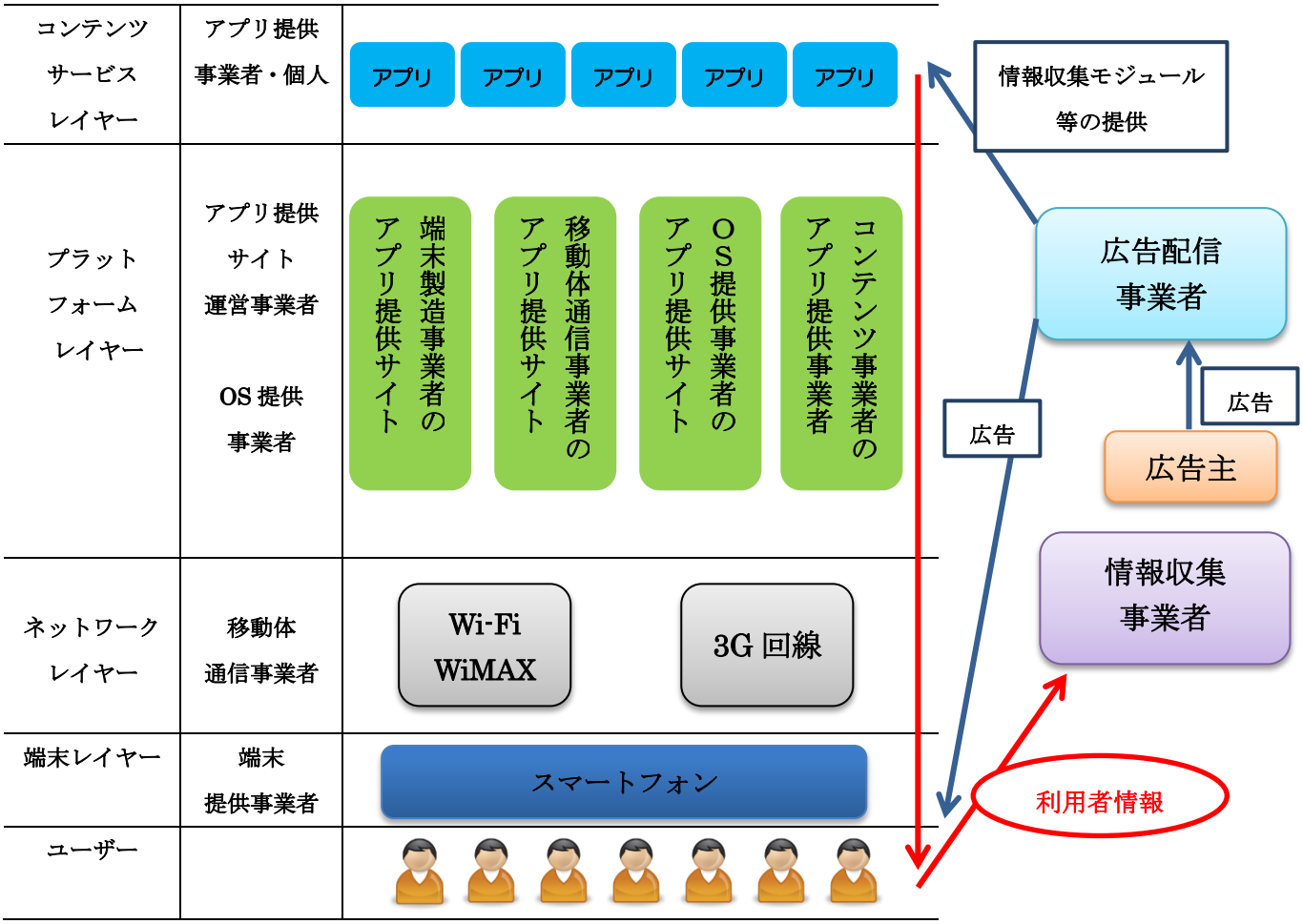
[2] レイヤー･･･ 構造や設計などが階層状になっているとき、その一つ一つの「階層」（レイヤー）のことをいう。

[3] オペレーションシステム（OS）･･･コンピュータシステム全体を管理するソフトウェアで、多くのアプリケーションソフトから共通して利用される基本的な機能を提供する。一般的に「基本ソフトウェア」と呼ばれている。

[4] アップル社は iOS を提供し App Store を運用。グーグル社はアンドロイドを提供し、Google Play を運用。マイクロソフト社はウィンドウズフォン（Windows Phone）を提供し Windows PhoneMarketplace を運用。

[5] 情報収集モジュール･･･スマートフォン等に蓄積された様々な情報を収集する機能を持つ、アプリケーションに組み込んで利用される一連のプログラムのこと。

図表 15 スマートフォンをめぐるサービス構造



（出典;『スマートフォンプライバシーイニシアティブ －利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－』より筆者作成）

4.3 スマートフォンにおける利用者情報

主に、電源を入れてネットワークに接続した状態で持ち歩くスマートフォンは、行動履歴や通信履歴など、PC よりも詳細な利用者の情報が蓄積される。

スマートフォンにおける主な利用者情報としては、図表 16 のようなものが挙げられる。

図表 16：スマートフォンにおける利用者情報の例

区分	情報の種類	含まれる情報
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報
	クッキー技術を用いて生成された識別情報	ウェブサイトを訪問時、ウェブブラウザを通じて一時的にPCに書込み記載されたデータ等
	契約者・端末固有ID	OSが生成するID（Android ID）、独自端末識別番号（UDID）、加入者識別ID（IMSI）、端末識別ID（IMEI）、MACアドレス等
第三者の情報	電話帳で管理されるデータ	氏名、電話番号、メールアドレス等
利用者の状態に関する情報（通信サービス上の行動履歴や）	通信履歴	通話内容・履歴、メール内容・送受信履歴
	ウェブページ上の行動履歴	利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等
	位置情報	GPS機器によって計測される位置情報、基地局に送信される位置登録情報
	写真、動画等	スマートフォン等で撮影された 写真、動画

（出典；『スマートフォンプライバシーイニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－』より引用）

図表 16 で示したような情報がスマートフォンを利用しているうちに、内部に蓄積されているのであるが、この中には、当然、個人情報に該当するものも含まれる。それらの情報の中には、アプリ等を経由し、事業者によって収集されている場合がある。

4.4　アプリによる情報収集事例

本節では、アプリからスマートフォンに蓄積された利用者情報が収集されている現状について、事例を検証しながら考察していく。

【事例 1】: 懐中電灯アプリ（アンドロイド端末向けアプリ）

このアプリは、アンドロイド端末向けに無料で提供されているアプリであり、機能としては、スマートフォンのライトを点灯させることで懐中電灯代わりになるというものである。しかしこのアプリは、それらの機能だけではなく、位置情報や、インターネットの閲覧履歴情報などの利用者情報をアプリ製作業者などに送信する機能が組み込まれており、利用者にはわかりづらい形で利用者情報を収集している。

【事例 2】: 金魚すくいゲーム

このアプリは、金魚すくいを楽しむことのできる無料ゲームアプリである。KDDI 研究所がこのアプリを解析したところ、GPS で測定されたスマートフォンの位置情報を 1 分間に 1 回、組み込まれた情報収集モジュールによって、米国の広告会社に送信される仕組みになっていた。アプリをインストールする際、画面上に「許可するアクセス権限　位置情報」と表示され、位置情報の読み取りについて同意が求められるが、その目的や、外部に送信することは触れられていない。アプリは端末の操作で楽しむゲームであり、ゲームに位置情報は必要ない。製作したアプリ開発会社によると、同様に位置情報を米国の広告会社に送信するアプリを 2010 年 10 月以降、238 種類出しており、延べ計 150 万人がインストールしたという。収集した位置情報は、アプリ利用者の所在地と関連性の高い広告を表示するために利用されていた。

【事例 3】: 雑誌・新聞等の閲覧アプリ（該当アプリ :「ビューン」「マガストア」「産経新聞」）

これらのアプリは、スマートフォン上で雑誌や新聞などを閲覧することのできるアプリである。しかしこれら 3 つのアプリは、閲覧履歴及び契約者・端末固有 ID 等を十分に利用者に説明しないまま取得し、外部に送信していたことが分かった。

「ビューン」は、2012 年 1 月 20 日、閲覧履歴情報および端末識別情報の取得について利用規約に明記するとともに、同年 4 月中に当該情報の収集について個別の同意を取る措置の実施、端末識別を目的とした独自 ID を導入することで対処した。

「マガストア」は同年 1 月 13 日、利用規約に閲覧情報を収集することを明記するとともに、収集データと端末 ID との紐付けを防止する措置を実施し、2012 年 2 月 27 日には同意した利用者の情報のみ収集するよう措置した。

「産経新聞」は、開発中に試験的に組み込んだ機能について、情報の利用・蓄積はしていないとしつつ、2012 年 1 月 31 日付で同機能を削除した。

【事例 4】ウイルス対策アプリ

このアプリは、「ウイルス対策」などと謳い、電話帳データを抜き取った不正アプリである。この抜き取ったデータから出会い系サイトの勧誘メールを他人名義で送りつけたとして、アプリ製作者は逮捕された。このアプリは 2012 年 11 月～2013 年 3 月で、述べ約 81 万人にインストールされ、やく 3700 万人分の電話帳データが抜き取られた。

【事例 5】コンテンツ視聴アプリ「アップティービー」

このアプリは、動画コンテンツを無料提供する代わりに、利用者の利用履歴などの情報を取得するというものである。このアプリで問題となったのは、利用者情報を取得することに同意をする確認画面が表示された瞬間から契約者・端末固有 ID 等を取得するという不備があり、利用者の同意を得る前の段階で情報を取得していたのである。その後、アプリ提供事業者である「ミログ」は 2012 年 4 月に解散し、サービスは終了した。

【事例 6】動画系アプリ

これは、人気のゲーム名等などのタイトル名に「the Movie」を付けた動画系の複数のアンドロイド用の無料アプリである。いずれも無料動画を楽しめると称している。アプリをインストールしようとすると、「ネットワーク通信」「個人情報」「電話／通話」について OS の利用許諾を求める画面が表示され､利用者がこれを許諾してアプリをダウンロードしインストールすると、端末内の電話帳に登録された名前、電話番号、メールアドレス等の情報を送信される仕組みとなっていた。流出した個人情報は約 3700 万人分に上る可能性があるという。

KDDI 研究所によれば、2011 年 8 月に収集したアンドロイド上で動作する 980 個のアプリケーションの利用許諾について分析を行った結果、558（56.9%）のアプリケーションに合計 1,065 の情報収集モジュールが存在していたとされる。

また、OS の利用許諾の内容については、端末 ID 等を取得可能とする電話／通話の利用許諾は 57.9%、GPS を用いた位置情報の利用許諾は 26.4%に存在していた。さらに、980 個のうち 400 個のアプリケーションについて、2011 年 12 月から 2012 年 1 月の間に 5 分間の挙動解析を行い、外部への送信情報を確認した結果、Android ID の送信が 12.5%、端末 ID（IMEI）の送信が 14.3%、位置（緯度・経度）の外部送信が 8.0%であったとされる。

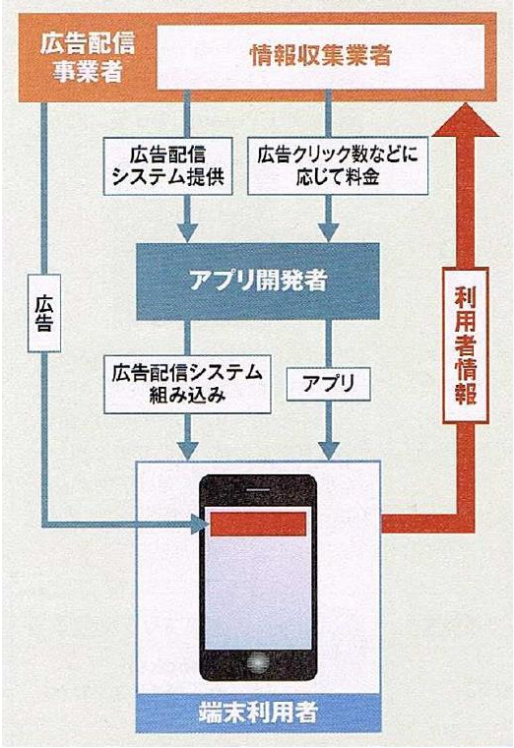
一方､何らかの形で ID あるいは位置情報を送付していた 181 のアプリケーションのうち、14 件（7.7%）にはアンドロイドによる利用許諾とは別に、アプリケーションによる説明があり、10 件（5.5%）は同意等を取得していたが、それ以外の 167(92.3%)のアプリケーションについてはアンドロイドによる利用許諾以外の説明はアプリケーション内において表示されなかったとしている。

4.5　アプリを利用した広告ビジネス

前述で示したように、アプリが利用者の情報を収集し、外部に送信するという事例が数多く出ている。それではなぜこのようなことが行われているのか。中には例外も見受けられるが、上記でも何度か触れたように、そこには広告ビジネスが絡んでいる。

図表 17 に示すように、アプリ製作事業者は、ネットリサーチ会社などの情報収集業者から情報収集モジュールの提供を受け、開発したアプリにそれを組み込む。利用者には、無料、もしくは低額でアプリを提供する代わりに、端末にある利用者情報を収集するのである。すると広告配信事業者が利用者に応じた広告を配信し、クリック数などに応じて、アプリ製作事業者も収益を得ているという仕組みである。もちろん、利用規約の明示とその同意があれば情報取得に関して問題はないとされるものの、実際はどのように利用されているのか、判然としない場合が多い。

図表 17：アプリを利用した広告配信の仕組み



（出典；週刊ダイヤモンド 2012 年 6 月 2 日号 P37 より引用）

また図表 18 は、大手広告代理店を頂点に、大量の個人情報がより付加価値を増しながら大きな収益に代わっていく、ピラミッド型の構造を示したものである。

アプリの利用者（ユーザー）から利用者情報を直接収集するのは、アプリ製作事業者である。しかし、アプリ製作事業者の多くは単に利用者情報を収集するのみで、その情報はアプリ製作を依頼しているネットリサーチ業者に送られている。アプリ製作事業者は、ユーザーの位置情報や購入履歴、インターネットの閲覧履歴などの利用者情報を集め、それを数万円でネットリサーチ事業者へそのまま引き渡していると言われている。

ネットリサーチ業者は、わずか数万円で入手したデータを性別や年代、職業といった属性ごとに分類し、広告代理店の子会社などのマーケティング会社に数十万円程度で売却するという。また一部では、メールアドレスなどが、スパムメール業者に横流しされているともいわれている。

マーケティング会社は、買い取った属性分けされたデータをより洗練させている。データからユーザーの趣味や嗜好、行動パターンを分析し、マーケティングに有効活用できるように、人々の最新のトレンドを浮き彫りにする。

こうして洗練された情報は最終的に大手広告代理店に引き渡される。この時点で、収集されたデータの価格は、アプリ制作事業者が集めたのみの段階のデータから、100 倍近く、100 万～300 万円に上ると言われている。

ピラミッドの頂点である広告代理店は、子会社などから得たアプリを分析したデータをもとにクライアントに営業をかけ、広告やイベント、新事業を提案していくのである。この時、広告代理店がクライアントに提案するデータは、「年収が中の上クラスの親を持ち、かつ、○○系のファッションに興味がある 10 代～20 代前半の女性は、週末午後、△△街 A 通りの B 店でランチを食べ、次に C 店で××を□□円で購入している。」という極めて具体的なデータになっているという。この段階で、元は二束三文だったデータは、1000 万円以上の価値になるといわれ、さらに事業化までにつなげることができれば、その利益は数千万円にまで跳ね上がると言われている。

また大手広告代理店は近年、Google や Facebook などと業務提携をし、同様のマーケティングを加速させている。

このように、アプリが利用者情報を収集している背景には、大手広告代理店を頂点とした広告ビジネスが存在している。これは、ほとんどのユーザーがアプリの利用規約を読んでいないことに、付け込んだビジネスと言える。

図表 18：スマートフォンから収集された利用者情報の流れ

（出典；週刊ダイヤモンド 2012 年 6 月 2 日号 P37 より引用）

4.6　個人情報保護法の観点から見たアプリによる情報収集

本節では、アプリによる個人情報収集において、収集される情報が個人情報保護法上の個人情報に該当するのか、また、アプリ提供者や情報収集事業者等が個人情報取扱い事業者に該当するのかということ等について検討していく。

4.6.1　個人情報への該当性

1 章でも示した通り、個人情報保護法において「個人情報」とは、「生存する個人に関する情報であって、その情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができることとなるものを含む。）をいう」（2 条 1 項）と定義されており、特定の生存する個人を識別できるものを指している。ここからは、スマートフォン、アプリを利用する際の様々な状況から、どのような情報が個人情報に該当するのかを検討する。

【個人の識別が可能な場合】

スマートフォンからアプリケーション提供者または第三者が取得する利用者情報によって、個人を識別できる可能性がある場合、その情報は個人情報に該当する。例えば、電話帳には、氏名、電話番号、メールアドレス等の情報が登録されており、個人を識別することができると考えられるため、個人情報に該当する可能性が高い。その他にも契約者情報等も該当すると考えられる。

【他の情報と容易に照合することで個人の識別が可能となる場合】

スマートフォンからアプリケーション提供者または第三者が取得する利用者情報のみでは個人を識別することができない場合であっても、取得した者が所有している情報等、他の情報と容易に照合することで個人の識別が可能となる場合には、個人情報に該当する場合がある。例えば、電話番号、メールアドレス、契約者・端末固有 ID などの情報が単体では個人を識別することができない場合でも、契約者の氏名等個人情報と容易に結びつくことによって、個人を識別できる可能性がある。

【行動履歴や利用履歴に関する情報】

行動履歴や利用履歴に関する情報としては、GPS や基地局・Wi-Fi アクセスポイント情報に基づく位置情報、通話履歴（通話内容・履歴、メール内容・送受信内容など）、ウェブページ上の行動履歴、アプリの利用により蓄積される情報などが当てはまる。また、位置情報、ウェブ閲覧履歴、アプリ利用状況などは、それ自体では個人を識別する可能性は少ないが、長期間にわたって、収集・記録した場合等において、個人を識別することが可能となる場合もある。

4.6.2　個人情報取扱事業者への該当性

1 章でも示した通り、個人情報保護法における個人情報取扱事業者とは、「データベースの形で、事業者用に、大量（5000 人分超）に個人情報を取り扱っている者」とされている。アプリケーション提供者等の中には、個人情報を含むスマートフォンの利用者情報を取得し、データベース等を構築し事業用に取り扱っている場合もあるため、個人情報保護法が適用されるか否かは個別の判断が必要にはなるが、個人情報を含む利用者情報を蓄積し活用しているアプリケーション提供者等は個人情報取扱事業者となる場合も十分あると考えられる。アプリケーション提供者等が個人情報取扱事業者に該当した場合に、個人情報保護法の規定において注意すべき点がいくつかある。

⑴利用目的の特定（第 15 条）、利用目的による制限（第 16 条）

第 15 条では、利用目的をできる限り特定することを求めており、第 16 条では本人の同意を得ずに、第 15 条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならないとされている。

したがって、「データを解析することで、何か有益な情報を得ることができるかもしれない」といったように、明確な利用目的を示さずに個人情報を取り扱うことは、第 15 条の違反となる可能性が高いということになる。また、当初の利用目的とは関係のない別の目的のために、本人の同意を得ないまま個人情報を取り扱うことは、第 16 条の違反となる可能性が高い。

これらの規定があるため、アプリケーション提供者は、利用者が利用目的を明確に理解しやすいような観点から、プライバシーポリシー等を作成すべきであると思われる。

⑵適正な取得（第 17 条）

個人情報保護法、第 17 条では、偽りやその他不正の手段により、個人情報を取得してはならないことが定められている。

例えば、利用者が気付かないようにアプリをインストールさせ、個人情報の送信を隠ぺいしつつ情報を収集した場合、違反となる可能性が高い。

また、アプリが利用者の個人情報を外部に送信する場合、OS の利用許諾によって、アプリがアクセスする情報は明らかにされているものの、個人情報を取得することが明示されていない場合には、OS の利用許諾とは別に、個人情報を取得することの通知又は公表もしくは同意を得ることなどを行うことが必要であると考えられる。現時点では、個人情報を取得することの通知又は公表や同意を得ることへの義務や手順などは存在しないため、適正な個人情報の取得の方法について検討するべきであると考えられる。

⑶第三者提供の制限（第 23 条）

第 23 条では、事前に本人の同意を得ずに、個人データを第三者に提供してはならないと

されている。この規定により、アプリケーション提供者が所有している個人データを第三者に提供する場合、原則として事前に本人の同意（オプトイン）が必要となる。

なお、第 23 条第 2 項において、本人の求めに応じて第三者への提供を停止する（オプトアウト）形をとる場合は、一定の条件を満たすことで、本人の同意を得なくとも、第三者への提供ができるものと規定されている。しかしながら、スマートフォンのアプリの場合、一度に大量の情報を取得し第三者に提供することが技術的に可能であり、一度情報が第三者提供された場合にその情報を取り出し、削除等をすることが困難であるため、プライバシーポリシー等にオプトアウトについて記載するだけでは、個人の権利侵害を十分に防止することは難しいと考えられる。

4.6.3　情報収集モジュールを用いた情報収集の場合

アプリケーション提供者により組み込まれた情報収集モジュール等により、スマートフォンからアプリケーション提供者を経由することなく、直接情報収集モジュール提供者（情報収集業者、広告配信事業者等）へ個人情報などが送信される場合、情報収集モジュール提供者による個人情報の取得となる。情報収集モジュール提供者が、5,000 件を超える個人情報を、電子計算機を用いて検索できるように体系的に構築する場合、個人情報取扱事業者として、個人情報保護法におけるいくつかの義務を負うことになる

一方、情報収集モジュール提供者は、一般に利用者に対する接点を直接持っておらず、利用者側も情報収集モジュールの種類や提供する企業名等の情報を提供されない限り、情報収集モジュールに関する詳細な情報を得ることができない。

また情報収集モジュールの中には、アプリケーション提供者が一部改良を施した上でアプリ内に組み込むものもあり、変更内容についてはアプリケーション提供者でないと正確に分からない場合もあると指摘されている。このため、詳細は情報収集モジュール提供者が掲載するプライバシーポリシー等を通知又は公表し説明する必要があるものの、アプリケーション提供者のプライバシーポリシーにおいて情報収集モジュール別に最低限必要な情報を利用者に通知又は公表するなど、アプリケーション提供者と情報収集モジュール提供者の間の役割分担により透明性を高めることが必要であると考えられる。

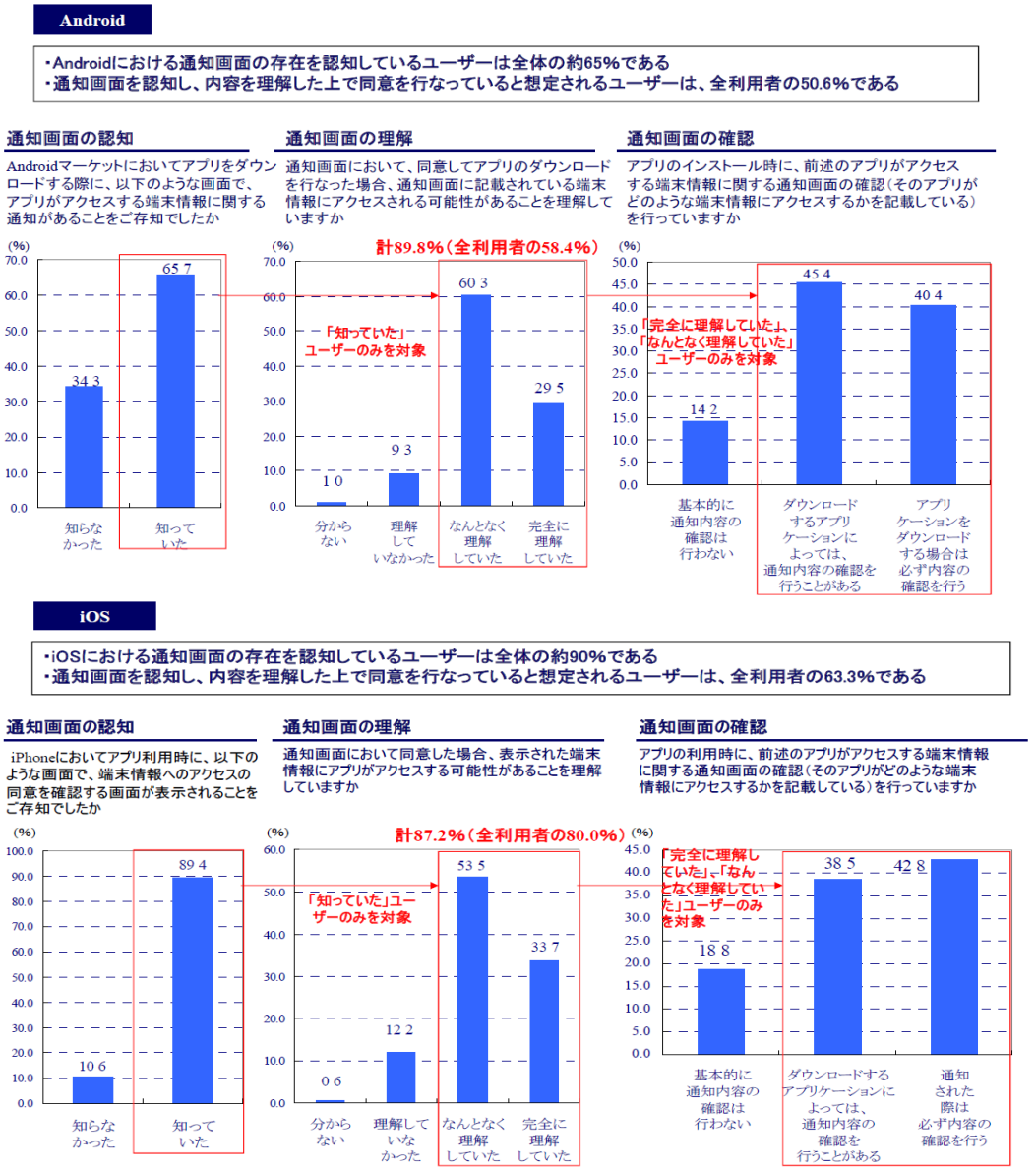
4.7　アプリの利用に対する利用者の意識

ではアプリの利用に関して、利用者はどのような点に不安などを覚えているのか。2012 年 2 月に総務省が行ったウェブアンケート調査[6]によれば、通知・同意画面を一定程度理解し確認している利用者は 5～6 割程度いるが（図表 19 参照。）、8 割のユーザーは通知・同意画面に何らかの不満・不安を有している（図表 20 参照。同意しないとアプリケーションが利用できない（約 40%）、同意・許可した後にどのようなことが起こるか分からない（約

[6] 総務省ウェブアンケート調査（2012 年 2 月実施）：有効回答数 1,576 人、スマートフォン利用者を対象。

36%）等)。また、アプリケーションの機能に必要な場合以外にも利用者情報を外部送信することについては、23%の利用者は情報送信されたくないとし、半数以上の利用者は利用目的や情報提供先の開示を希望している。(図表 21 参照。)

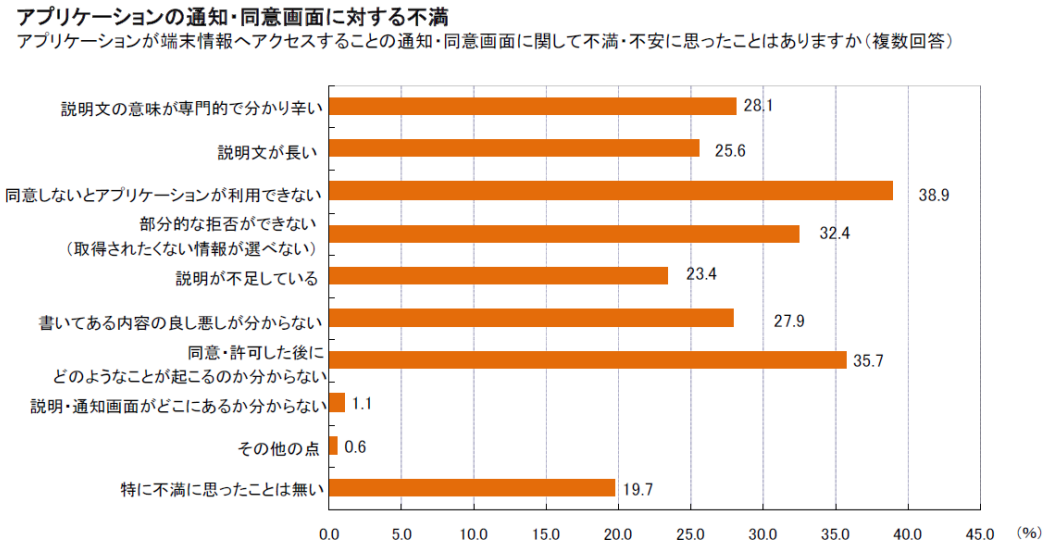
図表 19：通知画面の認知・理解・確認（アンドロイド OS 端末、iPhone 利用者）



（出典；『スマートフォンプライバシーイニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－』より引用）

図表 20：アプリケーションの通知・同意画面に対する不満

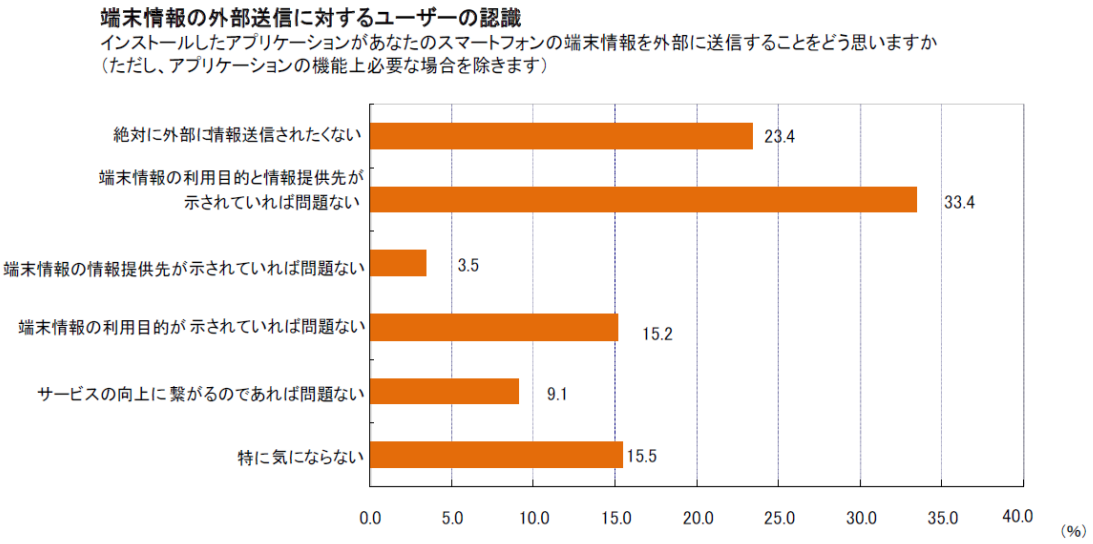
・通知・同意画面に対する不満として「同意しないとアプリケーションが利用できない」と回答したユーザーは 全体の約40%と最も多い
・次いで、「同意・許可した後にどのようなことが起こるか分からない」と回答したユーザーは35.7 %である



（出典；『スマートフォンプライバシーイニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－』より引用）

図表 21：端末情報の外部送信に対するユーザーの認識

・端末情報の利用目的と情報提供先が示されていれば、端末情報の外部送信について問題ないと考えるユーザーは、全体の約33%である

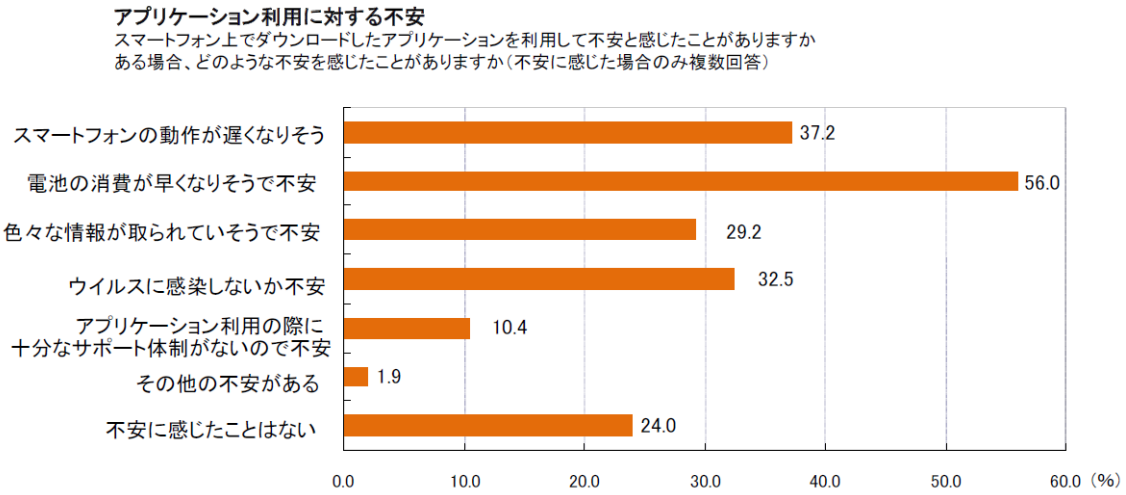


（出典；『スマートフォンプライバシーイニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－』より引用）

またアプリ利用に対する不安として、「色々な情報を取られていそうで不安」とする利用者は約 3 割程度いるが（図表 22 参照。）、情報を収集しているアプリが数多くある中で、この数字は少ないように感じる。

図表 22：アプリケーション利用に関する不安

・76 %のユーザーがアプリケーションの利用に関して何らかの不安を感じている
・不安を感じる主な理由は、「電池の消費速度への影響」、「端末動作速度への影響」といった端末の性能に係わるものが多い
・ユーザー情報を取得されることやウィルスへの感染に対して不安を感じるユーザーは、約3割である



（出典；『スマートフォンプライバシーイニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－』より引用）

総務省のウェブアンケート結果によれば、アプリケーションがスマートフォンにおける利用者情報にアクセスする可能性があることを認知している利用者は全体の約 8 割弱であり、利用者が各分野のアプリケーションにアクセスされていると想定する利用者情報は、図表 23 のとおりであった。

例えば、通信系アプリケーションは電話帳情報にアクセスしている可能性があることを 5 割弱のユーザーが認識し、地図系、天気系又は交通系アプリケーションが位置情報にアクセスしている可能性があることを約 4 割の利用者が認識している。一方、ゲーム系やニュース系についてはどのような端末情報にもアクセスされているとは思わないと約 4 割の利用者が認識しており、利用者がアプリによる情報収集の実態に対して誤った認識をしている可能性が見受けられる。

図表 23：アプリケーション利用に関する不安

	アクセスされていると想定する利用者情報（回答%）			
通信系アプリ	自分の電話番号（49.2%）	電話帳情報（47.3%）	端末ID（37.6%）	端末情報へのアクセスはない（20.9%）
SNS系	端末ID（32.2%）	おおよその現在地（基地局）（31.7%）	端末情報へのアクセスはない（27.1%）	詳細な所在地（GPS）/通話先の電話番号：（24.6%）
ゲーム系	端末情報へのアクセスはない（37.0%）	端末識別番号（31.0%）	おおよその現在地（基地局）（22.1%）	詳細な所在地（GPS）（15.1%）
ニュース系	端末情報へのアクセスはない（39.9%）	おおよその現在地（基地局）（27.4%）	端末識別番号（20.9%）	詳細な現在地（GPS）（18.7%）
天気系	おおよその現在地（基地局）（41.3%）	詳細な現在地（36.3%）	端末情報へのアクセスはない（29.2%）	端末識別番号（シリアル番号）（19.5%）
地図系	おおよその現在地（基地局）（49.4%）	詳細な現在地（44.2%）	端末情報へのアクセスはない（25.1%）	端末識別番号（シリアル番号）（20.4%）
交通系	おおよその現在地（基地局）（42.4%）	詳細な現在地（40.8%）	端末情報へのアクセスはない（27.7%）	端末識別番号（シリアル番号）（19.5%）

（出典；『スマートフォンプライバシーイニシアティブ
－利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－』より引用）

4.8 アプリによる情報収集の問題点と対策

4.7 で示した利用者のアプリに対する意識に関するいくつかのデータから考えうる問題点は以下の通りである。

(1) 情報収集への通知・同意画面に対する不満・不安を抱えている利用者が多く、改善が求められる。
(2) アプリケーションの機能に必要な場合以外にも利用者情報を外部送信することについては、情報送信されたくないと考える利用者、利用目的や情報提供先の開示を希望している利用者が多く、収集への同意の方法について改善が求められる。
(3) 情報を収集されている実態に対し、利用者の理解が深まっていない、もしくは誤った認識がなされている可能性がある。

（1）（2）に関しては、情報収集に対する通知・同意の方法について改善を図ることが求められる。通知・同意画面についてはよりわかりやすく、具体的にどのような情報が収集され、その情報がどのように使用されるのかということを簡潔に明記する必要がある。またより詳しい情報についてはプライバシーポリシーを作成し、利用者が容易に参照できる場所に掲示またはリンクを張り、スマートフォンの画面上でも容易に理解できるような、分かりやすい概要版を提示する。このような取り組みをすることで、どのような情報が収集され、それがどのように利用させるのか、利用者が完全に理解した上でアプリの利用を始められる環境を整えることができるのではないだろうか。

また(3)に関しては、事業者側（アプリ製作事業者、OS 提供事業者、移動体通信事業者等）、利用者側（消費者団体等、教育関係者、保護者）、国が一体となって、利用者に対する情報提供・周知啓発を行っていくべきであると思われる。

この取り組みによって、スマートフォンによるアプリの利用によって、情報が収集されている実態に対して、正しい認識を、幅広い年代に広めることができると考えられる。実際に国は、2012 年 4 月に「スマートフォン安心・安全利用促進プログラム」という政策を発表し、スマートフォンの利用に関する周知啓発活動を推進している。

上記の問題点に加えて、アンドロイド端末特有の問題点も見受けられている。アンドロイド OS のユーザーは、他の OS のユーザーよりも、不正アプリの被害を受けていると言われている。それにはいくつかの理由が存在する。アンドロイド端末の公式マーケットである Google Play には、アプリ公開への事前審査を人手ではなく、自動で行う仕組みを採用している。この審査をすり抜ける方法も開発されており、悪質なアプリが公開されやすい体制になっているといえる。これに対し Apple の事前審査は、人の手でアプリを起動してから、正常なのか、品質面で耐えられるか、プライバシーの侵害が問題になるかなどいくつもの面から審査される。また審査を通らないとアプリが公開できないほか、変な挙動を取るアプリ 1 つを審査に出すと、その開発者のすべてのアプリが Appstore から削除されるケースがあるため、開発者や発行者には不正なアプリを審査にかけることに対する高いハードルとなっている。Google は不正なアプリが自動で行われている審査をすり抜け、Google Play に公開されてしまう状況を鑑み、2012 年に、「バウンサー」と呼ぶウイルスチェック機能を入れて、有害アプリの駆除に乗り出した。しかしその後、バウンサーを長期間すり抜けていたアプリなどが発見されたことで、バウンサーが期待されている動作をできていないとみられている。

またアンドロイド端末では、Google 以外の非公式マーケットからのインストールが可能である。審査などしていないアプリには、不正なものが多くある傾向にあり、これもアンドロイド端末のユーザーが、多く被害を受けている原因の一つである。

これらの問題に関しては、ビジネスモデルや経営方針の違いなどが原因の一つとして考えられるため、すべてを統一することは困難であると思われるが、Google は事前審査の見直しや、非公式マーケットからのアプリのインストールの禁止などを検討するべきである

と思われる。

4.9　個人でのアプリによる情報漏えいへの対策

では、アプリによる個人情報漏えいにはどのように対処すべきか。本節では、個人がアプリをダウンロードする際に注意すべき点について考察する。

一点目は、アプリはインストールする際は、公式マーケットから入手するということである。iPhone の場合、App Store からのみダウンロードする仕組みとなっており、App Store にあるすべてのアプリは Apple 社による事前審査を受けたもののみであるため、悪意ある不正アプリが混入する可能性は低い。

一方で、アンドロイド OS のスマートフォンは、4.8 でも触れたように、公式マーケットである Google Play 以外からもアプリを自由にインストールすることができる。審査などを受けていないアプリには悪意のある不正アプリである可能性があるため、公式マーケットにある事前審査を受けたアプリをインストールすべきである。

二点目は、「レビュー」確認することである。4.3 アプリによる情報収集事例で紹介した中には、公式マーケットから提供されていたものもあるため、公式マーケットにあるアプリ全てが安全であるとは限らない。そこで判断機銃の一つとして、アプリをインストールする際に表示される「レビュー」を確認するという方法が挙げられる。

レビューとは、アプリを使用した他の利用者の感想やコメントのことであり、不正が疑われたりするものはレビューでの評価も低くなる。同じ提供元が提供している他のアプリのレビューを見比べ、傾向を掴むことも対策の一つである。ただし、レビューの中には嘘の情報を書き込む利用者もいるため、よく情報を見極めたうえで、判断の材料にしていくことが求められる。

三点目はアプリの利用には関係のない情報を収集するアプリに対して、注意をするということである。懐中電灯アプリであるのに、位置情報へのアクセス許可を求めるアプリ、動画の再生を行うアプリにも関わらず、電話帳へのアクセスを求めるアプリなどには、情報収集を目的としている場合があるため注意が必要である。

四点目は、アップデート時の変更点を確認するということである。アプリをインストールしてしばらくすると、アップデートの知らせがくるものがある。これは主にアプリの機能の追加や不具合の改善を行うものであるが、中にはその際に、情報を収集するための新たな機能を追加するものがある。そのため、アップデート時の変更点は、逐一確認し、不審な点がないかを見極める必要がある。

他にも、アプリがどのような利用者情報にアクセスしているのかの詳細な説明や、発行元などをわかりやすく表示し、アプリのリスクを判定できるサイト等もあるため（ネットエージェント株式会社提供のサイト「secroid」）、これらのサイトなどを有効活用し、インストールをするか否かの判断をしていくべきである。

4.10　サービス提供者に求められる取組

本節では、アプリによる情報収集が行われている中で、サービス提供者側が、利用者が個人情報やプライバシーの観点から安全・安心にサービスを活用できるようにするにはどのようなことをするべきか、検討する。

4.10.1　プライバシーポリシーの作成

利用者情報を収集するアプリケーション提供者、広告事業者をはじめとした情報収集モジュール提供者は、各アプリや情報収集モジュールなどについて、個別のプライバシーポリシーを作成する必要がある。そして作成したプライバシーポリシーは、利用者が容易に参照できる場所に掲示またはハイパーリンクを掲載することが求められる。そのプライバシーポリシーに記載すべき項目は以下の 8 項目[7]である。

プライバシーポリシーに記載すべき事項

①情報を取得するアプリケーション提供者等の氏名又は名称
- アプリケーション提供者等の名称、連絡先等を記載する。

② 取得される情報の項目
- 取得される利用者情報の項目・内容を列挙する。

③ 取得方法
- 利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか等を示す。

④ 利用目的の特定・明示
- 利用者情報を、アプリケーション自体の利用者に対するサービス提供のために用いるのか、それ以外の目的のために用いるのか記載する。
- 広告配信・表示やマーケティング目的のために取得する場合には、その旨明示する。

⑤ 通知・公表又は同意取得の方法、利用者関与の方法
- 通知・公表の方法、同意取得の方法：プライバシーポリシー等の掲示場所や掲示方法、同意取得の対象、タイミング等について記載する。
- 利用者関与の方法：利用者情報の利用を中止する方法等を記載する。

[7]「スマートフォン　プライバシー　イニシアティブ　ー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー」　総務省　2012 年、59 項より引用。

⑥ 外部送信・第三者提供・情報収集モジュールの有無
・ 外部送信・第三者提供・情報収集モジュールの組込みの有無を記載する。

⑦ 問合せ窓口
・ 問合せ窓口の連絡先等（電話番号、メールアドレス等）を記載する。

⑧ プライバシーポリシーの変更を行う場合の手続
・ プライバシーポリシーの変更を行った場合の通知方法等を記載する。
（当初取得した同意の範囲が変更される場合、改めて同意取得を行う。）

以上の点を踏まえた上で、プライバシーポリシーを作成し、利用者がアプリによる情報収集に対し、概要を理解し、安心・安全に利用することができる体制を整えることが求められる。

4.10.2　その他関係事業者による取組

利用者が安全・安心にアプリを利用するためには、アプリケーション提供者や広告事業者をはじめとした情報収集モジュール提供者以外の関係事業者も、何かしらの取組を行うことが求められる。

【移動体通信事業者・端末提供事業者】

移動体通信事業者・端末提供事業者には、スマートフォン販売時等に、従来の携帯電話との違いや、アプリによる情報収集、不正アプリの存在等について周知することが求められる。スマートフォンの利用を始める際に周知することで、被害を未然に防ぐことに効果を発揮するものと思われる。

また移動体通信事業者のアプリケーション提供サイトにおいて、アプリケーション提供者等に対し、適切なプライバシーポリシー等の作成・公表等の対応を促すことも求められる。プライバシーポリシー等の表示場所を提供するなど、アプリケーション提供者等が適切な対応を行うような環境を整えることが求められる。

【アプリケーション提供サイト運営事業者、OS 提供事業者】

アプリケーション提供サイト運営事業者、OS 提供事業者にも、アプリケーション提供者等に対し、適切なプライバシーポリシー等の作成・公表等の対応を促すことや、アプリケーション提供者等がプライバシーポリシー等の表示場所を提供するなど、適切な対応を行うような環境を整えることが求められる。

また OS による利用許諾がある場合、注意すべき利用許諾等の際は、プライバシーポリシ

ーへのリンクを表示し、プライバシーポリシーの参照を改めて促す等の方策を導入すべきであると思われる。

4.10.3 業界団体によるガイドラインの策定

上記で示してきた取り組みを、より効率的に普及させるために、各業界団体が、ガイドラインを策定することが望まれる。2012 年 1 月、世界的な携帯通信事業者の業界団体 GSMA Association）は、携帯端末向けのプライバシー原則、プライバシーデザインのガイドラインを発表しているが、それが日本において普及しているとは言い難い。

そのため、各業界団体が業界の状況を踏まえた上でガイドラインを策定し、事業者がこれに沿った活動を進めることで、利用者が安心して利用できるための環境が整えられると思われる。

本節では、サービスの提供者側による対策などを示してきたが、スマートフォンの利用によって、個人情報が収集される可能性や、不正アプリが存在すること、プライバシーポリシーに目を通す必要があることなどについて、利用者が認識する必要がある。そのために、事業者側（アプリ製作事業者、OS 提供事業者、移動体通信事業者等）、利用者側（消費者団体等、教育関係者、保護者）、国が一体となって、利用者、特に青少年や高齢者を中心に情報提供・周知啓発を行っていくべきであると思われる。

4.11 アプリレイヤー以外からの情報漏えいの危険性と対策

本章の冒頭でも述べたとおり、スマートフォンからの情報漏えいの危険性としては、アプリレイヤーからだけでなく、ネットワークレイヤー、OS レイヤーからの漏えいの危険性もある。そのため本節では、ネットワークレイヤー、OS レイヤーからの情報漏えいの危険性と対策について考察していく。

4.11.1 ネットワークレイヤーからの情報漏えいの危険性と対策

ネットワークレイヤーからの情報漏えいとは、通信傍受による情報漏えいである。スマートフォンにおいては、Wi-Fi の自動接続における情報漏えいの危険性が大きく考えられる。これは、公衆無線 LAN のアクセスポイントになりすまし、接続した端末とのデータのやり取りを傍受するもので、Wi-Fi フィッシングなどと呼ばれている。通信が暗号化されていない場合は、傍受している側にインターネットでやりとりした内容が漏えいする。特にスマートフォンは Wi-Fi の自動接続を有効にしている場合、ユーザーが気づかず上記のようなになりすましホットスポットに接続してしまう危険性が高い。ユーザーがこうしたなりすましホットスポットにつないでしまった場合は，公衆無線 LAN サービスに接続するためのユーザーID やパスワード，クレジットカード番号が漏えいする危険性がある。

対策としては、信頼できない Wi-Fi は使用しない、暗号化されずにパスワードや重要情報が送信されるサービスを利用しない、VPN や SSL といった通信の暗号化するなどの方法

が考えられる。

4.11.2　OS レイヤーからの情報漏えいの危険性と対策

OS レイヤーからの情報漏えいとは、OS がマルウェア[8]に感染したことなどによって発生する情報漏えいである。マルウェアに感染した場合、端末の個人情報が抜き取られたり、端末を遠隔操作されたりする危険性がある。

近年のマルウェアの傾向としては、「ボット型」と呼ばれる遠隔操作で端末を操る手口と、「標的型」と呼ばれる特定の組織や企業から機密情報の奪取を狙う手口とがある。ボット型マルウェアとは、外部から遠隔で操作されるマルウェアのことであり、保存されているデータや、操作中のスクリーンショットデータやキー入力データを収集して特定のサーバーに送ることなども可能であるという。標的型マルウェアとは、特定の組織を狙ったサイバー攻撃で、従来のコンピュータウイルスは愉快犯による犯罪も多くあったが、標的型マルウェアの目標は特定の組織の情報を盗み出したり、システムを破壊したりすることにある。

このようなマルウェアは、スマートフォンにおいては主にアプリから感染するケースがほとんどである。ここからは、Apple が提供する iOS と、Google が提供するアンドロイド OS に分けて対策などについて考察する。

まず iOS についてであるが、現時点では iOS に感染するマルウェアは世界的に報告されていない。この理由は 4.8 でも触れたとおり、iOS 端末に配布されるアプリは、Apple の厳密な審査が必要な AppStore 経由に限定されているためである。したがってユーザーに被害をもたらす恐れのあるアプリは審査を通ることができないのである。例外として企業向けには iOS Developer Enterprise Program という、AppStore 以外の企業独自のアプリ配信ライセンスが提供されているが、企業が自社員にマルウェアアプリを配布することは考えにくい。つまり iOS はアプリの配信形態の制御という手法で、マルウェアの感染を防止している。

しかし、厳密にはこれら以外の方法で勝手にアプリを iOS 端末へとインストールする方法がある。それは「JailBreak」と呼ばれる iOS の改造である。この改造により Apple によって施されているさまざまな制限を外すことができ、AppStore 以外のマーケットからアプリをインストールすることが可能になる。もちろん、AppStore 以外から提供されているアプリをインストールした場合、マルウェアに感染する危険性が高くなる。実際、JailBreak をした端末を狙い撃ちしたマルウェアも報告されているという。

また、JailBreak をしなければ安全というわけではなく、ユーザーが知らないうちに勝手

---

8 マルウェア･･･コンピュータウイルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェアのこと。遠隔地のコンピュータに侵入したり攻撃したりするソフトウェアや、コンピュータウイルスのようにコンピュータに侵入して他のコンピュータへの感染活動や破壊活動を行ったり、情報を外部に漏えいさせたりする有害なソフトウェアのことを言う。

に JailBreak させてしまうセキュリティホールも存在する。これは PDF のプログラムを応用したもので、例えばこのプログラムが含まれている PDF ファイルのサイトを Safari などで閲覧しただけで、その端末は JailBreak が施されてしまうのである。

この OS の脆弱性は iOS 4.3.4 で修正されたが、それ以前のバージョンを使用しているユーザーは速やかにアップデートを行うべきである。

これらのことから、iOS のマルウェア対策としては JailBreak をしない、iOS のバージョンを最新のものにするという対策が有効であると考えられる。

次に、アンドロイド OS についてであるが、4.8 で触れたとおり、アンドロイドは iOS とは異なり、公式マーケットである Google Play 以外からもインストールすることができるため、マルウェアに感染する危険性は高いと言える。

そのため、Google はマルウェアに対して主に 3 つの対策を行っている。

（1）GooglePlay アプリのセキュリティチェック

4.8 でも簡単に触れたが、これは 2012 年から導入されている「バウンサー」という検疫システムである。Google Play に登録されるアプリに対してマルウェアかどうかをチェックするものである。Google はこのバウンサーによって、Google Play からダウンロードされたマルウェアは 40%減少したと発表しているが、バウンサーを長期間すり抜けていたアプリなどが発見されたことで、期待されている動作ができていないとみられている。

（2）マルウェアの遠隔削除

バウンサーによる検疫を回避し Google Play に公開されてしまったマルウェアでも、Google が悪質なマルウェアと判断した場合は Google Play から削除するだけでなく、すでにインストールされていた端末からも削除することがあると言われている。このマルウェアの遠隔駆除については、Google は正式なアナウンスを行なっていない。しかし信頼性を保つためにも、積極的に告知するべきであると思われる。

（3）Android 4.2 マルウェア検出機能

Google Play に公開されているアプリについては上記方法で対策が行われているが、公式マーケットからのアプリのインストールへの対策として Google は、Android 4.2 から OS の標準機能に「application verification service」というマルウェアの検疫機能を搭載し、GooglePlay 以外のマーケットから入手したアプリであっても、マルウェアの検疫を行えるようになった。しかし米ノースカロライナ州大学の Xuxian Jiang 氏が 2012 年 12 月に発表したところによると、この「application verification service」のマルウェアの検出率は 15%に過ぎず、市販のマルウェア検疫ソフトでは 80～100%の検出率であるため、まだ信頼性は低いといえる。今後、検出率は高まることが期待されるが、現時点では市販のマルウェア検疫ソフトが必要であると言える。

このように特にアンドロイド OS は、マルウェアに感染する危険性が高いため、非公式マーケットからのアプリのインストールは控える、市販のマルウェア検疫ソフトを導入することなどの対策が必要であると考えられる。

これまで示してきたとおり、アプリレイヤー以外からの情報漏えいの危険性も考えられるため、スマートフォンユーザーはネットワークレイヤー、OS レイヤーからの情報漏えいへの対策も進めていくべきであると思われる。

4.12　国に求められる取組

本節では、国が取り組むべきであると思われる点について検討する。現時点で国では、スマートフォンからの個人情報漏えいへの対策として、いくつかの取り組みを行っている。2012 年 4 月に「スマートフォン安心・安全利用促進プログラム」という政策を発表し、スマートフォンの利用に関する周知啓発活動を推進している。また、総務省は 2014 年度から、スマートフォンに蓄積した情報をアプリが無断で抜き取っていないか調査し、安全性を「○」や「×」で判定する取組を行う。具体的には、アプリのプライバシーポリシーを検証し、実際の運用がプライバシーポリシーどおりになっているかを調査する。プライバシーポリシーが未作成だったり取得する情報の種類や利用目的が非開示だったりすれば「×」と判定する。プライバシーポリシーに記載のない情報の抜き取りが見つかった場合も「×」と判定する。問題があれば提供会社に改善を要請することで、不正アプリの削減につなげようとしている。

またそれらの取り組みに加え、法の整備を進めるべきであると思われる。4.10 において、プライバシーポリシーに記載すべき項目の提案や、各業界団体によるガイドラインの策定を提案したが、アプリケーション提供者の中には、業界に加入しない企業や、個人で活動している者もおり、それらが必ずしも守られるとは限らない。

そこで、二点の解決策を提案したい。一点目は現在の個人情報保護法とは別に、新たにスマートフォンの利用に関わる法律の作成を検討することである。現行の個人情報保護法には「スマートフォン」や「アプリケーション」という言葉はなじみにくく、個人情報保護法を改正することで、規制を進めることは困難であると思われる。また、施行令や施行規則という形で規制をするにも、本法の改正が必要なため、現実的ではない。そのため、新たにスマートフォンの利用に関する法律を定め、利用者が安全にスマートフォンやアプリを利用できる環境を整えていくことができると思われる。

二点目は、不正指令電磁的記録に関する罪（ウイルス作成罪）において、不正アプリもウイルスとみなすような改正を加えるという方法である。ウイルス作成罪には「スマートフォン」や「アプリケーション」という言葉を加えることはそれほど難しいことではないと考えられる。また新たにスマートフォンに関する法律を策定するよりも、成立へのハードルはそれほど高くはないため、現実的であると考えられる。

4.13　教育による対策

スマートフォンからの情報漏えいの危険性や対策や危険性について、利用者に広く認知・理解させるには、企業等の組織内や教育機関による教育が必要であると思われる。

そこで本節では、スマートフォンからの情報漏えいの危険性を、教育によって周知する方法について考察する。

4.13.1　組織内の教育

近年、その利便性から、スマートフォンを企業等の組織で活用しようとする動きが活発化してきている。実際に BOYD（Bring Your Own Device）[9]の導入やクラウドサービスと組み合わせて活用するなどして、作業の効率化を図っている。しかし利便性が高い反面、利用方法を誤れば、個人情報などが大量に漏えいする危険性がある。そのため、組織内でスマートフォンの利用に関するガイドラインの作成やセミナーなどを開催し、スマートフォンによる情報漏えいを未然に防止する活動をしていくことが望まれる。

では、ガイドラインの作成やガイダンスを行う際に、盛り込むべき項目はどのようなものが考えられるのか。

一点目は紛失・盗難時の対処法の策定である。スマートフォンは、そのコンパクトさゆえに紛失・盗難の危険性も高い。そのため、事前にガイドラインで紛失・盗難後の対処法を策定しておき、紛失・盗難が発生した場合は、それに準拠して迅速に対処することが情報漏えいのリスクを最小限に留めることにつながる。具体的な対処法には、位置情報検出→リモートロック [10]→リモートワイプ [11] といった手順が考えられる。まず端末の位置情報を検出することによって、端末の場所を特定し発見を試みる。その後リモートロックを実行し、他人による操作を受け付けないように設定する。それでも発見できない場合は、リモートワイプを実行し、端末内のデータを削除する。このような対処法をガイドライン上で策定し、セミナー等で教育を行っておくことで、迅速な対処が可能になるものと思われる。

二点目はアプリに関するルールの策定である。これまで 4 章で述べてきたとおり、アプリの中には、情報を収集するものが数多く存在している。そのため、アプリを利用することによって、社員や顧客の個人情報などの企業の機密情報が漏えいする危険性がある。会社が貸与する端末に関しては、アプリのインストールを禁止する設定にしておくことが可

---

[9] BYOD（Bring Your Own Device）･･･企業などで従業員が私物の情報端末などを持ち込んで業務で利用すること。

[10] リモートロック･･･携帯電話やスマートフォン、ノートパソコンなど持ち運び型の情報端末を、遠隔地から通信回線を通じて指示を出すことによりロックし、操作を受け付けない状態にすること。

[11] リモートワイプ･･･リモートワイプとは、携帯電話やスマートフォンなどのモバイル端末を遠隔地から操作し、端末に保存されているデータを削除する機能およびサービスのこと。

能であるが、BYOD を採用している場合や、顧客の電話番号・住所などを私物のスマートフォンに登録している場合には、不正アプリの存在や情報漏えいの危険性を示し、インストールする際に安全性を確認する項目を策定しておくべきであると思われる。

三点目は OS の不正改造の禁止である。4.11.2 でも触れたとおり、スマートフォンには、OSを不正改造することによって､様々な制限を解除することができる｡iOS では｢JailBreak｣という方法で AppStore 以外のマーケットからアプリをインストールすることなどが可能になる。アンドロイド OS では root 化という方法で、通常は禁止されている設定の変更を行うことができるようになる。しかしながらこのような OS の不正改造は、不正アプリをインストールしてしまう危険性が高まることや、企業が社員に端末を貸与する前に制限した設定を解除することで、システム管理者が想定している情報漏えい対策の前提が崩れてしまうため、情報漏えい防止の観点では OS の不正改造は禁止すべきであると考えられる。

四点目は、スクリーンショットの禁止である。スマートフォンにはスクリーンショットという機能がある。これは、ディスプレイに表示されている画面を画像ファイルとして保存することができる機能である。メモ代わりに利用できることや、簡単に利用できることから多くの人がこの機能を活用している。しかしながら、ビジネスで活用する際は情報漏えいの観点において問題となる部分がある。例えば、企業としてクラウドサービスなど利用をし、端末にデータを残さないようにしていても、社員がクラウドサービスを利用している画面をスクリーンショットで保存してしまうと、画像としてデータが端末に残ってしまうのである。そうすると、端末を紛失・盗難された場合にその画像データを閲覧され、機密情報が閲覧されてしまう可能性があるのである。そのため、セキュリティ意識が高いとされている金融業界などでは、スクリーンショットの利用を禁止している。以上のことから、ビジネスで活用する際には、ガイドラインにスクリーンショットの利用を禁止する旨を明記しておくべきであると思われる。それらに加え、スクリーンショットができるアプリや画面の操作記録を動画として記録することができるアプリなどもあるため、それらの利用の禁止に関してもガイドライン、セミナーにおいて周知・啓発しておくべきであると思われる。

これらのような項目をガイドラインに盛り込み、セミナー等によって社員教育を行うことによってスマートフォンからの情報漏えいのリスクを軽減することができると考えられる。またそれらに加え、普段からガイドラインのチェックを義務付けるなどして、ガイドラインの徹底に向けた活動も合わせて行うべきであると思われる。

4.13.2　教育機関による教育

近年のスマートフォンの普及は青少年の間にも広がっており、気軽にアプリをインストールできることなどから、ゲームや SNS をスマートフォンで利用している。しかし、不正アプリの存在やスマートフォンの利用に関する危険性について十分な知識がないままに利用してしまうことで、個人情報が漏えいする危険性がある。そのため、学校等の教育機関

を中心に、青少年に対する教育をしていくことが望まれる。

現在、小中高において、スマートフォンの利用法や危険性についての授業は義務化されておらず、基本的には行われていない。ただし、文部科学省が小学生、中学生向けに携帯電話とスマートフォンの利用方法や危険性を啓発するためのリーフレットを作成し、各学校に配布しているが、活用の仕方は学校に委ねられている。こうした状況からも、今後、「情報」や「技術・家庭」の授業などでスマートフォンの利用方法や危険性に関する教育を、学習指導要領に追加し、青少年にスマートフォンの利用による危険性の周知・啓発を進めていくべきであると思われる。また小学生についても、全国で一貫した情報教育をしていくために、学習指導要領に情報教育に関する教科・科目を盛り込み、教科書を作成するべきであると思われる。

また大学生に関しては、入学時や新学期などの時期に、スマートフォンの危険性についてガイダンス等を行い、周知・啓発していくことが望まれる。

スマートフォンの普及によって青少年にとってインターネットがより身近なものになっているため、それに伴い、教育内容も改善していくべきであると考えられる。

4.14　4 章まとめ

これからもスマートフォンの普及は進み、アプリの利用者もそれに合わせて増えていくと考えられる。4.9 では個人レベルにおける情報収集を提案したが、アプリを利用している以上、個人情報の収集を完全に阻止するのには限界がある。アプリをインストールする、とりわけ無料アプリをインストールするということは、自分自身の個人情報・プライバシー情報を提供していることに等しいといっても過言ではない。利便性と危険性はトレードオフの関係にあり、情報を収集されたくないと感じる人は、アプリをインストールしないことである。情報収集に対して、「気持ちが悪い」と感じる程度は人によって違うため、アプリの利用に関しては、便利さと許容度のバランスをよく考えて利用していくべきであると考えられる。

またアプリ以外からの情報漏えいに対しては、その現状に関する認識や知識があれば、対策を行えるものがほとんどである。そのため、危険性や対策に関する教育・周知が重要であると思われる。

5　対策

これまで、個人情報とは何かということを考察したうえで、個人情報漏えいの現状や事例を検討し、その中でもスマートフォンからの個人情報漏えいについて大きく取り上げ、考察してきた。

ではスマートフォン以外からの個人情報漏えいへの対策はどのようなものが考えられるのか。そこで本章では、個人、組織、教育機関という観点から高度情報化社会における個人情報漏えいへの対策についてそれぞれ考察していく。

5.1　個人による対策

近年、情報通信技術の発展により、年齢を問わず、だれもが PC や携帯電話、スマートフォンなどからインターネットに接続・利用できる環境にある。しかしながら、PC のウイルスの感染や、悪質なウェブサイトへのアクセスなどが原因で、個人情報が漏えいしてしまう危険性も存在する。そこで本節では、個人レベルでの個人情報漏えいへの危険性と対策を考察していく。

(1)ウイルス対策

PC がウイルスに感染すると、データが破壊される危険性や、PC が遠隔操作されたりする危険性に加え、個人情報が漏えいする危険性がある。そのため、PC を利用する際は、ウイルス対策を行わなければならない。対策としては以下のようなものが考えられる。

一点目は、ウイルス対策ソフトのインストールである。ウイルス対策ソフトは、ウイルスの侵入を予防したり、除去したりするソフトであり、無料のものから有料のものまで数多く存在する。しかし無料のソフトは、性能や保障が不十分であったり、中にはウイルス対策ソフトを装い、個人情報やクレジットカード番号の入手を目的としたりするものも存在するため、信頼できる企業が提供する有料のウイルス対策ソフトをインストールすべきであると思われる。またウイルスは常に新種のものが生み出されるため、それに対応できるようにこまめにウイルス対策ソフトを更新し、最新のものを利用する必要がある。

二点目は、メールの添付ファイルやダウンロードしたファイルへの対応である。ウイルスは、メールの添付ファイルやインターネット上からダウンロードした画像ファイル、音楽ファイル、映像ファイルに埋め込まれている可能性があるため、使用する前にウイルス対策ソフトなどのウイルス検査を行うことが必要である。また見知らぬ相手先から受信したメールの添付ファイルへの注意はもちろん、知人から受信したメールの添付ファイルにもウイルスが混入している可能性があるため、ファイルを使用する際は、ウイルス検査をこまめに行うことが安全性を高めることに繋がると思われる。

三点目は、OS やソフトウェアを常に最新の状態にしておくことである。ウイルスには、OS や各種ソフトウェアにある脆弱性（セキュリティホール）を利用して侵入するウイルスが存在する。そのため、セキュリティホールを解消するための修正プログラムを適用する

ために、定期的にアップデートを確認するか、自動更新設定にしておく必要がある。

上記のような対策を行えば、ウイルスに感染し、個人情報が漏えいしてしまう事態を回避できるものと思われる。

⑵フィッシング対策

フィッシングとは、正規のメールやウェブサイトを装い、クレジットカード番号や暗証番号などの個人情報を詐取する詐欺のことを指す。典型的な手口としては、クレジットカード会社や銀行からのお知らせと称したメールなどで、パスワードの変更を促す内容や、懸賞に当選したなどという内容で、正規のウェブサイトに類似した偽造したウェブサイト誘導し、そこでクレジットカード番号などの個人情報の入力を促し、入力された情報を盗み取る手口である。またメールだけではなく、掲示板や SNS の投稿に URL を記載してアクセスさせ誘導する手口や、アルファベットの o（小文字のオー）を数字の 0 にしたり、アルファベット I（大文字のアイ） を l（小文字のエル）にしたりして、閲覧者を見間違えさせたり信用させたりし､本物の URL に見せかけてアクセスさせる手口なども存在する。

このようなフィッシングへの対策としては以下のようなものが考えられる。一点目は、常に正規のウェブサイトにアクセスすることを心掛けることである。フィッシングでは、メール利用して虚偽のウェブサイトへ誘導する場合が多いため、例えば、金融機関の ID・パスワードなどを入力するウェブサイトにアクセスする場合は、アカウントなどを作成した際に金融機関から通知を受けている URL をブラウザに直接入力するか、ブックマークに正しい URL を記録しておき、毎回そこからアクセスするようにするなどし、常に正規のウェブサイトにアクセスするようにしておくべきである。また、本物の Web サイトのドメイン名や URL を常に意識して、正しい Web サイトにアクセスしているかを確認することを意識することも重要である。

二点目は、インターネットではセキュリティアイコンおよび証明書の確認である。インターネットバンキングやオンラインショッピングのように重要な個人情報を送受信する必要がある場合には、「SSL」のような暗号化プロトコルが必要になる。SSL プロトコルを利用するウェブサイトのアドレスには、「http://」ではなく「https://」となり、セキュリティサイトである「鍵」のアイコンが表示される。暗号化プロトコルは、個人情報をやり取りするウェブサイトにとっては必須のシステムであるため、「鍵」マークが表示されないウェブサイトは信頼に値しないため、偽装ウェブサイトである可能性が高く、注意が必要である。しかし、暗号化プロトコルは誰でも利用可能であるため、「鍵」のアイコンが表示されるだけでは、正当性は判断できない。そのため、「鍵」のアイコンをダブルクリックすることで表示される「セキュリティ証明書」を確認することが必要である。企業などが採用している正規のセキュリティ・システムであれば、信頼性の高い「発行者」による証明書が表示されるのに対し、偽造ウェブサイトの場合は、発行者と発行先（申請者）が同じであったり、有効期限が切れているような証明書が表示されたりする場合があるため、フィッ

シングを疑うべきである。

3 点目としては、直接問い合わせることである。金融機関などの名前で送信されてきた電子メールの中で、通常と異なる手順を要求された場合には、内容を鵜呑みにせず、金融機関に直接電話やメールなどで確認することも有効な対策となり得る。

インターネットバンキングやオンラインショッピングなどの金銭に関わるウェブサイトを利用する際は、手間がかかってしまうが、前述したような対策を行うことによってフィッシングによる被害の回避に繋がるものと考えられる。

(3)パスワード漏えい対策

インターネット上のサービスなどを利用する際や PC やスマートフォンのセキュリティを高めるために、パスワードを設定することが多くある。そのため、多くのパスワードが必要になるため、安易なパスワードやパスワードの使い回しなど、パスワードの運用・管理上危険な取扱いをしている利用者も多い。

しかし、そのパスワードが推察されたり、漏えいしたりすることで、個人情報の漏えいや本人になりすましてサービスを不正利用される危険性がある。そのため、推察されにくいパスワードの設定や定期的にパスワードを変更することによって、対策しておく必要がある。

パスワードの設定方法としては、以下のようなものが考えられる。

- 他人に推測されやすいもの（電話番号や誕生日等）にしない
- 大文字・小文字・数字・記号を組み合わせる
- パスワード長くする（8 桁以上が推奨されている）
- 推測しづらく自分が忘れないパスワードにする
- 無作為で意味を持たない文字列にする

パスワード漏えい対策としては、以下のようなものが考えられる。

- 定期的にパスワードを変更する
- 紙に書き留めたまま放置しない
- PC に保存しない
- 人に教えない
- パスワードの使い回しをしない

また最近では、複数のインターネット上のサービスで使い回されているパスワードを標的にした、「パスワードリスト攻撃」による被害が増加しきている。パスワードリスト攻撃とは、あるウェブサイトへの攻撃で手に入れた ID やパスワードを他のサイトへの侵入に利

用する手口である。これは同じ ID・パスワードを使い回す利用者が多いことが背景にある。2013 年に入ってから T サイトや goo、フレッツ光にはじまり、JR 東日本や資生堂、クラブニンテンドーや KONAMI ID など、業種を問わずさまざまなウェブサイトに対し、「不正ログイン」が試みられ、実際にいくつかの ID についてはログインを許してしまったことが報じられている。攻撃者が利用するのは実在する ID やパスワードであるため、攻撃を受けた段階では通常のログインとは見分けがつきにくく、事業者にとって、パスワードリスト攻撃からの防御は難しいという。同じ IP アドレスから 1 秒間に数十回というログインが試されるため「異常」は検知できるものの、気づいた時には一定の情報は漏えいしてしまっている場合が多い。

そのため、ユーザーはサービスごとに、異なるパスワードを設定することが必要であるが、それらすべてを記憶しておくことは困難である。そのため、パスワード管理ソフトの利用や、表計算ソフトなどを利用し、同ソフトに ID とパスワードを記録しておき、そのファイルをパスワード付きで保存するなどの対策が有効である。また、パスワードが流出した場合、そのパスワードの変更、利用を中止することも被害を防ぐ手段の一つである。

また最近では、使い捨てのパスワードを発行する「ワンタイムパスワード」や、2 段階認証を採用するサービスもあるため、それらの機能を積極的に利用することも有効な対策になると考えられる。

(4)不正アクセス対策

不正アクセスとは、2012 年 5 月 1 日に改正施行された不正アクセス禁止法（不正アクセス行為の禁止等に関する法律）によると、以下のような行為を指す。

①コンピュータの OS やアプリケーションあるいはハードウェアに存在するセキュリティホールを利用して、コンピュータのアクセス制御機能を迂回し、コンピュータ内に侵入する行為

②他の人に与えられた、利用者 ID およびパスワードを、その持ち主の許可を得ずに利用して、持ち主に提供されるべきサービスを受ける行為

このような不正アクセスにはどのように対処していくべきか。②に関しては、前述の(3)パスワード漏えい対策で示した対策を行えば、パスワードが漏えいすることによる不正アクセスはある程度防げるものであると考えられる。

では、①に関してはどのような対策を行えばよいのか。一つ目として考えられるのが、修正プログラムの適用である。(1)ウイルス対策でも述べたように、OS やブラウザなどのソフトウェアにはセキュリティホールが発見されることがある。セキュリティホールが存在する OS やソフトウェアを使用していると、不正アクセスの侵入口となり、個人情報を窃盗される危険性がある。そのため、セキュリティホールを解消するための修正プログラムを適用するために、定期的にアップデートを確認するか、自動更新設定にしておく必要があ

る。

二点目として考えられるのが、インターネット接続方法への注意である。家庭や出先で PC をインターネットに接続する場合は、その接続方法により、不正アクセスを受け易い状態になる場合がある。特に公衆無線 LAN や、ホテルなどでの LAN 接続等、不特定多数の利用者が同一 LAN 上に接続する可能性のある環境で、インターネットに接続する場合は、同一 LAN 上の他の利用者から不正アクセスを受ける可能性がある。このような環境では、この場合は、ファイル共有設定を無効化やローカルエリア接続の設定の変更、セキュリティ対策ソフトを利用するなどして対処しておく必要がある。

三点目としてはファイアウォールの導入である。ファイアウォールは、インターネットと PC のデータのやり取りを監視することにより、悪影響を与えると思われる通信に対して、警告を表示し、侵入をブロックする機能であり、不正アクセスの制限に有効である。そのため、OS に内蔵されたファイアウォール機能を有効にすることや、ファイアウォール機能を持つ統合ウイルスソフト、またはパーソナルファイアウォールソフトを活用するが望まれる。

これらの対策を施すことによって、不正アクセスによる被害を防ぐことができると考えられる。

(5)PC を処分する際の個人情報漏えい対策

PC を処分する際、ファイルを削除したり、ハードディスクを初期化したりした場合でも、復元ソフトなどでファイルを復元される可能性がある。そのため、専用のハードディスク消去ソフトを使用して、ファイルを完全に消去することが望まれる。

(6)ファイル共有ソフトからの個人情報漏えいへの対策

ファイル共有ソフトとは、インターネットを介して不特定多数のコンピュータの間でファイルを共有、交換するためのソフトである。このファイル共有ソフトで共有されているファイルの多くはウイルスに感染されていることが多く、過去にも、代表的なファイル共有ソフトの一つである Winny を使用した東京都の警察官が、ウイルスに感染し、約 1 万人分の個人情報を含んだ捜査書類を流出した事件や、同じく Winny を使用した職員が 1 万人以上の市民の名簿を流出させるなど、甚大な被害をもたらしている。

このように非常に危険性の高いファイル共有ソフトは使用を避けることがセキュリティ上最善策であるといえる。

(7)インターネット上の無料サービスからの個人情報漏えいへの対策

近年、ウェブメールやオンラインストレージ、SNS（ソーシャル・ネットワーキング・サービス）などの無料のインターネット上のサービスを利用している人が増えてきている。しかしながら、そのような無料のサービスは効果的な広告を配信するなどの目的で、利用

者の個人情報を収集している場合が多い。特に Google による個人情報収集に関しては批判の声も多く、2012 年 3 月には新たなプライバシーポリシーを導入し、検索サービスのほか、メール、地図、写真管理、動画配信、スケジュール管理、自動翻訳など、60 以上のサービスで顧客情報を統一して管理するという。これによって多くのサービスを利用すればするほど、個人の行動記録や趣味嗜好などの情報が Google に蓄積され、アンドロイド OS のスマートフォンを利用している場合、GPS 機能を通じてより詳細な行動記録が収集されることになる。

収集される利用者情報はそれら単体では個人情報に該当しない場合でも、それらの情報を組み合わせることによって個人情報になる可能性もある。そのため無料のサービスを利用する際は、どのような情報が収集され、その情報がどのように利用されるのか、プライバシーポリシーなどによく目を通したうえで利用の判断を下すべきであると考えられる。そして利用をする際は、情報が収集されることを念頭に置いた節度ある利用が求められる。インターネット上の無料サービスを利用する際は、便利さと許容度のバランスを考慮した上で利用していくべきであると考えられる。

⑻SNS から個人情報漏えいへの対策

現在、Twitter や Facebook などの SNS が人気を博しており、ビジネスにおいても活用する動きが高まっている。これらのサービスは、今の自分の行動や考えを簡単にインターネット上に発信できることや、同じ趣味や考えを持つ利用者同士の交流の場として利用できることが特徴となっており、多くの利用者を集めている。しかし利用方法を誤れば、個人情報の漏えいに繋がってしまう場合がある。SNS から個人情報が漏えいしないようにするにはどうすればよいのか。対策は以下の通りである。

一点目は公開範囲の見直しである。各 SNS では、氏名や生年月日、連絡先、投稿内容などの公開範囲を自分好みにカスタマイズすることができる。初期設定では、制限なくインターネット全体に公開する設定になっている場合が多いため、友人や家族のみに公開するような設定にしておくべきである。

二点目は、位置情報の送信への注意である。SNS の中には、投稿する際に位置情報を添付する機能がある。しかし、投稿内容と照らし合わせることで、自宅や仕事場が推測される危険性があるため、送信を行わない設定にしておくべきである。またスマートフォンなどで撮影した写真を投稿する場合、その写真に位置情報が埋め込まれていた場合、読み取りソフトによって位置情報を読み取られる危険性がある。そのため、スマートフォンの位置情報はオフにしておくべきであると考えられる。

これらのことだけでなく、SNS ではリアルタイムの活動内容を投稿する場合が多いため、投稿内容に注意しなければ、ストーカー被害等に繋がる危険性がある。住所や連絡先、勤務先などを入力する項目があるが、極力そのような情報は登録しないことが得策である。SNS を利用する際は、個人情報が漏えいする危険性があることを念頭に置き、節度ある利

用を心掛けるべきであると思われる。

これまで、様々な場面で考えうる個人レベルでの個人情報漏えいへの対策を述べてきた。しかしながら、3.5 でも述べたように NSA によって、インターネット上の活動が収集されているという実態もある。そのため、インターネットを利用する際は、ある程度自身の個人情報が収集・漏えいしていると考え、個人情報を書き込んだり登録したりし過ぎない、節度ある利用を心掛けるべきであると思われる。

5.2　組織による対策

大規模な個人情報漏えい事故は、企業などの組織のずさんな管理体制が原因で漏えいしているものも多くある。そのため、組織内で個人情報の取り扱い方を徹底しなければ、個人情報が流出し、訴訟問題に発展したり、社会的な信用を大きく損なったりする可能性がある。そのため本節では、企業などの組織が講じるべき個人情報漏えいへの対策について、セキュリティ面と組織内体制の整備の面の二つの側面から考察する。

5.2.1　セキュリティ対策

企業などの組織においてセキュリティ対策はどのように行えばよいのか。経済産業省が 2009 年に発表した「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」では、「組織的」「人的」「物理的」「技術的」の 4 つの観点から安全管理措置を講じなければならないとしている。その内容は以下の通りである。

▽組織的安全管理措置

組織的安全管理とは、安全管理について従業者（法第 21 条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】
①個人データの安全管理措置を講じるための組織体制の整備
②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
③個人データの取扱い状況を一覧できる手段の整備
④個人データの安全管理措置の評価、見直し及び改善
⑤事故又は違反への対処

▽人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】
①雇用契約時及び委託契約時における非開示契約の締結
②従業者に対する教育・訓練の実施

▽物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

【物理的安全管理措置として講じなければならない事項】
①入退館（室）管理の実施
②盗難等の防止
③機器・装置等の物理的な保護

▽技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】
①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録
⑤個人データを取り扱う情報システムについての不正ソフトウェア対策
⑥個人データの移送・送信時の対策
⑦個人データを取り扱う情報システムの動作確認時の対策
⑧個人データを取り扱う情報システムの監視

これらの事項は情報セキュリティ対策として一般的なものであり、最低限守るべきものであるため、組織内でこれらの措置がぬかりなく行われているのか、今一度見直し、徹底させることが重要である。

ここからは、特に注意すべきセキュリティ対策について考察していく。

(1)入退管理の徹底

過去にあった大規模な情報漏えい事件には、ずさんな入退管理が原因で職員に情報が持ち出されてしまった事件もあるため、情報漏えいへの対策として入退管理は重要な項目の一つである。

機密情報や個人情報を扱う部署や端末を保管するスペースは、セキュリティ区画として物理的に隔離することが望ましい。例えば来訪者に応対する応接場所などのスペースは、セキュリティスペースを通らずに応接場所に通せるようなレイアウトにすることが望ましいと思われる。またそういったセキュリティ区画は、入室が許可されている者のみが入室できる仕組みにし、なおかつ守ろうとする資産の重要度に応じて物理的に区画を分けて、より重要性の高い情報資産が取り扱われる区画への入室にはセキュリティゲートを通過するといった対策が望ましいと考えられる。

また組織内の人間と組織外の人間を区別する必要もある。そのために職員には名札の着用を義務付けることや、来訪者には「ゲスト」といった名札を着用させるといった方法が考えられる。そして来訪者の入退履歴を記録することも重要であり、それは万が一漏えいが判明した場合、漏えい者や漏えい原因の特定に繋がる。

(2)ID・パスワードの強度と取扱い

個人情報へのアクセスは、ID とパスワードによる制限が基本である。過去に合った大規模な情報漏えい事件では、数千人の職員が同じ ID とパスワードを使用していたことが原因で個人情報へ簡単にアクセスを許してしまった事件もあった。そのため、ID は職員ごとに付与し、強度の高いパスワードを設定する必要がある。また職員ごとに ID を設定することによって、個人情報へのアクセスログを取得することができるため、情報漏えい時に原因の早期発見に繋がることも期待できる。

パスワードの設定方法、漏えい対策については、5.1 個人による対策の(3)パスワード漏えい対策にあるものと同様の方法で設定することが望まれる。また作成したパスワードに関しては、パスワードの強度検査を行い、強度をチェックできる体制づくりも重要である。そして設定したパスワードには、1 か月もしくは 3 か月といった有効期限を設けることでパスワードの変更を強制的なものにし、また変更時には、過去に使用したパスワードは使用できない設定にしておくことが望まれる。

(3)アクセスログの保存・解析

アクセスログを徹底的に取得することは。不正アクセスを行った犯人や被害範囲を特定するうえで非常に重要である。アクセスログの取得と一定期間の保存や定期的なログの分析が手続きとして遵守されていることと、内部の関係者に対する周知は、内部の不正アクセスに対する牽制手段として非常に有効であるため、必ず行うべきことの一つである。

⑷記憶媒体への使用の制限

個人情報が職員によって持ち出されるもので多いのが、USB メモリや CD といった記憶媒体である。それを防ぐために、基本的に組織内の PC では CD や USB メモリの使用ができない設定にしておき、限定的にそれらの記憶媒体を使用可能な PC を別途用意しておくが重要である。

⑸コンピュータ機器の修理と処分

前節でも述べたとおり、PC や記憶媒体といったコンピュータ機器を処分する際の情報漏えい対策も重要である。2002 年 1 月には、名古屋市内の大学生が購入した中古 PC に、医療機関が健康保険組合などに医療費を請求するために作成した診療報酬明細書（レセプト）のデータが記録されていたことが判明している。通報した大学生によると、PC の画面上ではデータが消去されていたが、市販のソフトを使用してハードディスクのデータを復元したところ、レセプトの画像データが見つかったというものである。

この事件からもわかるように、通常ハードディスク上などのデータは、再フォーマットしただけでは完全に消去できない。市販の復元ソフトなどで第三者に情報が漏えいする危険性がある。そのため、コンピュータ機器を安全に処分するための手続きをあらかじめ定めておく必要がある。そのデータ消去方法としては、専用のハードディスク消去ソフトを使用して削除する方法、専用装置にて電気的、時期的に塗りつぶしを行う方法、ハードディスクを物理的に破壊する方法などがある。

またコンピュータ機器の修理が必要な場合の情報漏えい対策も必要である。保守契約のもとに ICT ベンダーの技術者が派遣されてくるときには、修理時に立ち会うなど、監視下での作業とする、ICT ベンダーへ機器を送り修理してもらう場合は、データのバックアップをとったうえで消去作業を実施し発送する手続きを徹底するなどの対策が必要である。

⑹脆弱性の管理

不正アクセスへの有効な対策の一つとして、セキュリティホールを経常的に塞ぐ保守活動、すなわち脆弱性マネジメントシステムの確立が挙げられる。

脆弱性マネジメントとは、組織としてシステム上の脆弱性を常に正確に補足し、適切な対処がタイムリーに行われることで脆弱性を可能な限り排除する仕組みである。脆弱性マネジメントシステムは組織内で構築する他に、ICT ベンダーがシステムを提供しているため、それを導入する方法もある。

不正アクセスの被害にあうことは、個人情報を漏えいする加害者となる可能性も秘めているため、非常に重要な対策項目である。

⑺ソフトウェアの管理

ソフトウェア、特にフリーソフトの中には、スパイウェア等が混入しているものもある。

そのため、組織内のシステムに組み込むソフトウェアのチェック体制を整備する、職員によるソフトウェアのインストールができない設定にしておく必要がある。

(8)標的型攻撃への対策

近年、特定の組織を執拗に狙うサイバー攻撃である「標的型攻撃」による被害が相次いでいる。攻撃の手口も年を追うごとに巧妙になってきており、2000 年代初頭は、攻撃者は、一人程度で実施しているような突発的な攻撃が多かったのに対し、2005 年頃から徐々にグループ化し、今ではサイバー攻撃がプロ集団によって行われるようになっている。攻撃も一つのウイルスで完結するのではなく、複数のウイルスを駆使したり、あるいはサーバーとウイルスが連携するような仕組みを用意したりして攻撃を行ったり、セキュリティホールを狙うなど、従来以上にウイルスに感染される確率を上げる手口を使うようになってきている。

標的型攻撃は、一般的に攻撃者からのウイルスが付与されたもの、あるいはウイルスが組み込まれたウェブサイトに誘導するメールが、情報窃取を狙う組織の職員に届くところから始まることが多い。職員がこのウイルスが仕込まれた添付ファイルを開いたり、あるいはウェブサイトに誘導されたりすることで PC がウイルスに感染する。攻撃者は感染した PC を入り口として、機密情報の窃取に取り掛かるのである。この最初のきっかけとなるウイルス感染を引き起こすために、主にソーシャル・エンジニアリングとセキュリティホールが使われる。ソーシャル・エンジニアリングとは、人間の心理的な隙に付け込んで攻撃を成功させる手法のことである。標的型攻撃の場合は、メールの件名や文面を工夫することで攻撃対象者の興味を引くことで、添付ファイルを開かせたり、リンクに誘導したりする。

セキュリティホールには、脆弱性を攻撃するように細工をしたファイルを、脆弱性が残ったままのソフトウェアで読み込むことで、攻撃が成功してしまう。セキュリティホールに対しては、前述したセキュリティホールを経常的に塞ぐ保守活動をしておくことで攻撃を防ぐことができる。

このような標的型攻撃には、ICT ベンダーが対策製品を販売しているため、それらの導入を検討すべきである。そして、ウイルス感染において入口となるのは、多くの場合職員個人である。したがって、セキュリティ対策を強化する一方で、職員に対する啓発・教育活動にも努めることが求められ、模擬訓練の実施なども有効である。

また標的型攻撃に対しては、アクセスログの保存・解析や脆弱性の管理の徹底も重要となるため、総合的なセキュリティ対策が必要であると考えられる。

5.2.2　組織内体制の整備

組織の中には、組織内規定を策定しても全く運用されていないという企業も少なからず存在するため、個人情報保護の推進には、組織内体制の整備が不可欠である。組織内体制

の整備に関して重要な項目は以下の通りである。

⑴保護責任者の選任・保護委員会の編成

適正な個人情報保護体制を構築するために、個人情報保護に対する責任者を選任し、保護委員会を編成すべきである。保護委員会では、作成された個人情報の管理、外部委託先の管理、職員の教育、緊急時の対応、監査結果による改善実施などを行い、個人情報保護体制を整備する活動を行う。また様々な部署と密に連携し、情報の交換を日々行っていくことも重要である。

⑵漏えい事故が発生した場合の対処法の策定

万が一漏えい事故が発生した場合に備え、対処法を策定しておく必要がある。手順としては、状況の把握、状況の公表通知、セキュリティ体制の再構築、被害者等への対応、加害者・責任者への処分、漏えい者や監督者に対する厳格な処分の検討といった手順が迅速に行われなければならず、普段からマニュアルやチェック項目を整理し、対応の不備や遅れが生じないようにしておく必要がある。

⑶職員の教育

組織内規定や漏えい事故が発生した場合の対処法などを職員に意識づけるためには、教育が重要である。個人情報漏えい事故の原因の多くは職員によるヒューマンエラーであり、そのような業務上のミスなどは教育によってある程度防ぐことができるものと思われる。

教育すべき内容は、基本的なセキュリティの知識、組織内規定やシステム利用のマニュアル、そして個人情報漏えいのリスクをケーススタディなどで教育していくべきである。また過去に合った失敗事例や顧客からの苦情を紹介することも有効であると思われる。そしてアンケートの実施や理解度テストなどを行い、教育効果の検証も合わせて行うべきである。

教育は、職員の個人情報保護に対する意識を高めるだけでなく、万全なセキュリティ対策を講じていることを周知することで、内部犯行に対する牽制手段としても有効であるため、定期的に教育を行っていくべきである。

個人情報保護体制を整えることは、組織にとって重要な社会的責任である。漏えい事故が発生した場合は、組織にとっても大きな損失になるため、万全な漏えい対策を講じるべきであると考えられる。

5.3　教育機関による対策

近年、情報通信技術の発展により、我が国ではインターネットに接続しやすい環境が整ってきている。最近では、小学生が PC や携帯電話を所有することも珍しくなく、青少年の

ほとんどがインターネットを利用している。しかしながら、十分なインターネットリテラシーが身に付いていないままに利用を続けた場合、個人情報を漏らしてしまったり、フィッシングなどの被害などに合い個人情報が漏えいしてしまったりする危険性がある。

そのため本節では、現在の学習指導要領をもとに、教育機関による個人情報保護に関する教育に対し、どのような改善が必要か検討していく。

現在、小学校、中学校、高等学校における個人情報保護に関する情報教育はどの程度行われているのか。各学習指導要領を検討してみる。

小学校における個人情報保護に関する情報教育はどのようになっているのか。2011 年度より導入されている学習指導要領によると、小学校での情報教育は、「各教科などでのコンピュータ利用を促し、そこから技術やモラルを学ぶ」としている。中学校や高等学校のように具体的に、情報教育の教科・科目は開設されていない。こうした小学生における教科書がない中の情報教育として、国としては情報モラルの学習としてリーフレットを各学校に配布している。このリーフレットには携帯電話やスマートフォンの利用方法や危険性を啓発するものなどがある。しかしながら活用の仕方は学校に委ねられてしまっており、教科書も作成されていない状況では、全国で同水準の情報教育が展開されているとは考えにくく、個人情報保護に関する教育も十分に行われているとは考えにくい。近年では、小学生の PC の使用や携帯電話の所有がほぼ当たり前になりつつある現状からも、全国一律に学習指導要領に情報教育に関する教科・科目を盛り込み、教科書を作成するべきであると考えられる。そしてその教科の中で、小学生にもわかりやすい形で、個人情報を漏えいさせない、PC や携帯電話、スマートフォンの安全な使用方法を教育していくべきであると考えられる。

次に中学校における個人情報保護についての情報教育はどのようになっているのか。2012 年度より導入されている「技術・家庭」の学習指導要領の中には、個人情報保護を取り扱う項目は少なく、著作権などの項目に付随して簡単に触れられている程度である。またウイルスに関しては簡単に触れられているが、フィッシングなどの具体的な脅威には触れられておらず、スマートフォンについて触れている項目もない。これらを見る限り、中学生の多くが PC や携帯電話、スマートフォンを使用し、インターネットに接続している状況から考えても、不十分であると思われる。特にスマートフォンに関する項目は、中学生にとってインターネットに接続する非常に身近なツールであるため、利用方法や危険性に関する教育を盛り込むべきであると考えられる。

次に、高等学校における個人情報保護についての情報教育はどのようになっているのか。2013 年度から導入されている高等学校の「情報」の授業の学習指導要領の中には、個人情報保護に関する項目が多くあり、ウイルスの存在、フィッシングなどにも触れられており、小学校、中学校での情報教育よりもより充実した内容になっていると感じる。しかしながら、中学校と同様にスマートフォンについても項目は存在しない。スマートフォンは青少年が気軽にインターネットに接続できるツールの一つであるため、項目を設けてアプリの

危険性やスマートフォンの安全な利用方法に関する項目を盛り込むべきであると考えられる。

これらの情報を見る限り、我が国において個人情報保護に関する情報教育は十分であるとは言い難く、小学校での情報教育に関する教科・科目の新設、中学校、高等学校での個人情報保護に関する教育の充実が求められる。そのためには、学校の ICT 環境整備、教員の ICT 活用指導力の向上も合わせて行うべきであると考えられる。

6　展望

本章では、情報通信技術が日々進歩している社会状況の中で、インターネット上の個人情報保護はどのような展開を見せるのか、ビッグデータやマイナンバー法などを取り上げ考察していく。また個人情報保護法の改正が検討されている中で、現状の法律の問題点や社会状況を考察した上で、どのような改正が望まれるのか、などという点についても考察していきたい。

6.1　ビッグデータを活用する際の個人情報保護

近年、ビッグデータの利用に注目が集まっており、マーケティングや交通インフラの改善などに利用しようとする動きが活発化している。すでに様々な企業や官公庁で利用されており、その経済効果は年間 7 兆 7700 億円に達するといわれている。

しかしながら、個人情報保護、プライバシー保護の観点から検討するとデータの収集方法や提供方法などにいくつかの問題点もある。そのため、本節では個人情報保護、プライバシー保護の観点から、ビッグデータのどのような点が問題となるのか、そして今後どのような展開を見せるのか、展望を考察していく。

ビッグデータとは、情報通信技術の発展により生成・収集・蓄積などが可能・容易になった、従来よりも大量かつ種類が豊富なデータのことを指し、それらを分析・活用することで企業などはマーケティングなどに活用している。しかし、ビッグデータの個人情報保護、プライバシー保護の観点からみると、収集方法や販売方法などにいくつかの問題点が存在する。

例えば 2013 年 7 月、JR 東日本は、同社が展開している IC カードである「Suica」の利用データを日立製作所に販売していたことで大きな問題となり、9 月には Suica の利用データの販売を当面見合わせると発表した。JR 東日本が販売した利用データは、氏名や電話番号など個人を識別する情報を取り除き、カードの ID（SuicaID）も別の仮名 ID に変換したものであった。しかし利用者の拒否反応は強く、あらかじめ設けてあったオプトアウトを受け付ける窓口には、10 月初頭の時点で販売拒否の要望が約 5 万 5000 件寄せられた。ここまで大きく批判を浴びたのは、利用者への事前説明や情報公開が不十分であったこと、オプトアウトの手続きの周知が不十分であったこと、匿名化処理が不十分なまま販売していたことなどが原因であった。

また 1.4 個人情報の利用範囲で触れた CCC による問題にもビッグデータが関わっており、収集された情報はビッグデータとしてマーケティング等に利活用されている。この件に関しては、同意の取得方法や利用範囲などに問題が見受けられる。

では今後、ビッグデータに関して個人情報保護の観点からどのようなルール作りをしていくべきなのか。まず一つ目は、匿名化処理の方法の確立である。現在では、データの匿名化処理の方法においては各企業に委ねられており、Suica の事例の場合、それが不十分なまま行われていたために、批判の声が多く上がった。そのため、法律などにより、十分な

匿名化処理の方法を定め、それを各事業者に遵守させる必要がある。

二つ目は、個人情報を収集する際の同意の取得方法の改善である。1.4 でも触れたとおり、CCC が個人情報を共同利用することは会員規約に明記してあるが、それに関して完全に理解した上で同意をしている人は多くはないと思われる。そのため、個人情報を収集する際の同意の取得方法について、別途説明書などを用意し、わかりやすい説明をするように義務付ける必要がある。

三つ目は、事業者の監督や外部提供などを検証する第三者機関の設置である。第三者機関を設置することにより、個人情報をどうとらえるか、どのような使い方なら許容できるかといった疑問に対して統一された見解・判断基準を示すことができる。これに関しては、政府によって検討が進んでおり、個人情報保護保護法の改正などに伴い設置する試みであるという。

ビッグデータは今後も利活用が進んでいき、あらゆる組織で導入が図られていくと思われる。しかし、現状では問題がいくつかのあり、早急なルール作りと個人情報保護法の改正が求められる。それらを整備することによって、ビッグデータの安全な利活用が広がっていくと考えられる。

6.2　マイナンバー制の導入による個人情報漏えいへの懸念

2013 年 5 月 24 日、国民一人ひとりに 12 桁の番号を割り当てて、氏名や住所、生年月日、所得、税金、年金などの個人情報を、その番号で管理する共通番号制度、いわゆるマイナンバー法が参議院で可決、成立した。2016 年 1 月から運用が開始される。このマイナンバー制は、政府にとっては、行政コストの削減や事務の効率化に、国民にとっては手続きの簡素化などによる行政サービスの向上に役立つといわれている。

しかしながら、マイナンバー制の導入によって個人情報の漏えいを懸念する声も多い。では実際に個人情報漏えいの危険性はあるのか。政府は個人情報を保護するために、「情報提供ネットワークシステム」と呼ぶ、情報連携のために用いる専用システムを構築し、セキュリティを高めるという。これは、個人情報を役所などの組織間でやり取りする際に、そのシステムを介することで、番号そのものではなく、番号に対する別の符号を使って間接的に行うというものである。情報連携が始まると、所得情報や年金の給付状況など大量の個人情報が行政ネットワーク内を飛び交うが、このシステムにより、これらの情報には個人番号や氏名、住所など個人を特定できる情報は一切含まれず、漏えいの危険性を回避しているという。

しかし、セキュリティが万全であったとしても、自分の共通番号を安易に他人に示したりしないことや、マイナンバーを悪用した新たな犯罪に巻き込まれないように、国民側の自衛が求められる。また個人情報の取扱いの監視などを担う第三者機関については、強い権限と独立性を確保することが必須である。

マイナンバー制の導入が円滑に進めば、地方自治体、特に市町村の行政サービスは大き

く変化すると期待されている。そのためにも導入前に、十分なセキュリティ対策、国民への利用法、犯罪の危険性などの周知活動、行政側の情報管理の徹底などの体制を整えておく必要があると考えられる。

6.3　Google による個人情報収集

米大手 ICT 企業である Google は、2012 年 3 月には新たなプライバシーポリシーを導入し、検索サービスのほか、メール、地図、写真管理、動画配信、スケジュール管理、自動翻訳など、60 以上のサービスで顧客情報を統一して管理するという。これによって多くのサービスを利用すればするほど、個人の行動記録や趣味嗜好などの情報が Google に蓄積され、アンドロイド OS のスマートフォンを利用している場合、GPS 機能を通じてより詳細な行動記録が収集されることになる。

ここで問題となるのがプライバシー侵害の恐れがある点である。単なる利用履歴などの情報が、あらゆるサービス統合して管理されることにより、個人を識別できる情報になる可能性があるということである。この新方針に対しては、総務省と経済産業省の連名で文書が通知された。その文書には、法令順守及び利用者へのわかりやすい説明などが重要であることや、新方針に基づくサービス提供にあたり目的外利用や第三者提供をしてはならないことなどが示されている。また諸外国からも批判の声が多く上がっており、EU では規制の強化の検討、米国ではプライバシー保護団体などによる訴訟が行われている。

では、今後 Google のような企業によってプライバシーが侵害される危険性に対してどのように対処していくべきか。主に三点あげられる。一点目は、新たな利用者保護の仕組みの確立である。インターネット上におけるプライバシー保護のため、追跡の拒否（米国)、忘れられる権利（EU）など新たな試みが提案されている。利用者による自己情報の管理や保護のための自衛手段には限界があるため、事前にプライバシー保護対策を講じて権利侵害を予防する仕組み（プライバシーバイデザイン）を事業者に求める動きもある。

二点目は、個人情報保護方針のルールの策定である。個人情報保護法では個人情報取扱事業者に関して、利用目的の特定、第三者提供の制限などの義務が課せられるが、個人情報保護方針の公表は法律上では義務付けられていない。そのため、法律によって適正な表示ルールの確立と、表示義務付けをしていくべきである。

三点目は、国境を越えた個人情報保護への取り組みや国内における統一的な法執行が可能な機関の設置である。第三者機関を設置することにより、個人情報をどうとらえるか、どのような使い方なら許容できるかといった疑問に対して統一された見解・判断基準を示すことができる。これに関しては、政府によって検討が進んでおり、個人情報保護保護法の改正などに伴い設置する試みであるという。

今後も Google は、ウェアラブル端末である Google Glass などの新たなサービスを用い、利用者情報を収集していくと考えられ、そのような新たなサービスが提供されるたびに、プライバシーが侵害される危険性が高まっていく。そのため、上記で述べた対策を国が中

心となって行い、プライバシー保護の対策を講じていくべきであると考えられる。

6.4　個人情報保護の改善点

個人情報保護法が制定されてから 10 年以上が経過し、制定当時には想定できなかった個人情報の利活用や問題などが発生するなど、社会状況が大きく変化したため、個人情報保護法の改正が検討されている。そのため、本節では現行の個人情報保護法をどのように改正するべきか考察していく。

一点目は、第三者機関の設置である。現在、個人情報保護法を所管しているのは消費者庁であるが、消費者庁は制度の基本方針の策定と推進を担っているにすぎない。そのため、民間部門に関しては各省庁の主務大臣が監督しているが、個人情報の扱い方に関して統一した見解が示せなかったために、施行後には、過剰反応などが起こり混乱を招いた。

諸外国では、行政機関などから独立した立場の監督機関である「プライバシーコミッショナー」が対応している。そのため日本においても第三者機関を設置することにより、個人情報をどうとらえるか、どのような使い方なら許容できるかといった疑問に対して統一された見解・判断基準を示したり、統一的な法執行を行えたりすることが可能になると考えられる。

二点目は匿名化処理の方法の確立である。これは 6.1 でも触れたが、現在では、データの匿名化処理の方法においては明確な規定はなく、その判断は各企業に委ねられている。このままの状況では、匿名化処理が不十分なまま、個人情報がやり取りされる危険性がある。そのため、法律によって、十分な匿名化処理の方法を定め、それを各事業者に義務化させる必要がある。

三点目は、プライバシー性が高い個人情報をセンシティブデータと位置付けることである。今後、ビッグデータは医療においても活用が進んでいくことが予想される。しかしながら、遺伝子情報などは氏名や住所などの個人情報よりもよりプライバシー性が高いと思われる。そのため、そのようなプライバシー性が高いデータはセンシティブデータと位置づけ、その他の情報とは違う匿名化処理の方法を義務付けることや、ビッグデータとしては活用することは禁止するなどの特別な対応をしていくべきである。センシティブデータか否かの判断は困難ではあるが、議論を重ね、慎重に決定していくべきであると思われる。

四点目は、第三者提供の条件の見直しである。現行の個人情報保護法では、第三者提供する際は原則としてあらかじめ本人の同意を得る（オプトイン）形をとらなければならないとしている。しかし例外として本人の求めに応じて第三者への提供を停止する（オプトアウト）形をとった場合は本人事前同意を得ることなく第三者に提供することができるとしている。

しかしながら、ビッグデータの活用が盛んな中で、オプトアウトによって第三者提供がされている場合、簡単な通知のみで自分の個人情報が様々な企業の間などで独り歩きしてしまっている状況になりかねない。そのため、第三者提供は二点目で触れたような定めら

れた匿名化処理を行ったうえで、個人を特定できない情報に限るべきであると思われる。

また第三者提供の例外として共同利用という項目がある。これに関しては、1.4 個人情報の利用範囲でも触れたように、共同利用を認める範囲が広すぎると感じるため、共同利用を認める範囲をより明確に線引きし、範囲をより限定的にしていくことが望まれる。

またこれらの法の改正に加えてガイドラインの改正も合わせて行うべきである。その際には、以前のように各省庁が作成するのではなく、第三者機関が統一した解釈・見解で改正していくことが望まれる。

現在、保護法の改正については、内閣に設置されている「高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）」によって議論がなされており、2013 年 12 月 10 日に、個人情報保護法制の見直しを求める「方針案」をまとめた。政府は、2014 年 6 月までに法案の大綱をまとめ、15 年の通常国会に関連法案の提出を目指すという。今後マイナンバー法の導入やビッグデータの活用が広がる中で、個人情報保護法の改正が持つ意味は大きい。そのため、改正後にまた新たな不備が発生しないよう十分な議論を重ね、改正がなされることを期待したい。

おわりに

今後、ビッグデータの利活用はますます拡大し、マイナンバー制の導入も始まる中で、高度情報化社会における個人情報の保護に関する注目はより一層集まり、様々な議論やルール作りがなされていくと思われる。そのような中で、特に留意しなければならないのは、「気持ち悪いと感じる程度は人によって違う」ということである。この点を踏まえたうえで、個人情報の保護と利用の最適バランスをどこで見つけるかが今後の課題となる。事業者、利用者双方の落としどころをみつけ、法の改正などを含め、検討していくべきであると思われる。

また、個人がインターネット上のサービスを利用する際は、利便性と引き換えに個人情報を提供している、また、個人情報が漏えいする危険性がある、という意識を持ったうえでの節度ある利用が求められる。

そして個人情報を取り扱う事業者は、組織内で個人情報の取り扱いに関するルール作りをし、組織内でそれを徹底することが必要であり、個人情報を収集する場合には、利用者にどのような情報を集め、利用するのか、ということをわかりやすく明示し、利用者が納得したうえで承諾を得、収集をしていく必要がある。

また我が国において個人情報保護に関する情報教育は十分であるとは言い難く、現在の社会状況に対応した教育を、教育機関が中心になって行っていくことが求められる。

このような取り組みが進んでいけば、個人情報漏えい事件の減少や、利用者が収集されたくないと感じる情報が収集される事態も避けられ、個人情報を安全に利活用できる環境が整えられると考えられる。

以上

参考文献及び参考資料

≪書籍≫

・内藤貴昭　『ガイドブック 個人情報保護法』　法学書院　2008 年
・監修者：松田政行　編者：IT 企業法務研究所　『図解 よくわかる個人情報保護法』日刊工業新聞社　2004 年
・個人情報保護基本法性研究会　『Q&A 個人情報保護法[第 3 版]』　有斐閣　2005 年
・牧野和夫 『個人情報保護法ハンドブック -50 の Q&A でわかる企業対応！-』学陽書房 2005 年
・小川登美夫　『個人情報保護法 ここがポイント！　あなたの仕事の流れで理解する』日本経済新聞社　2005 年
・田島泰彦　『個人情報保護法と人権-プライバシーと表現の自由をどう守るか-』明石書店　2002 年
・佐々木俊尚　『徹底追及 個人情報流出事件』 三松堂印刷株式会社　2004 年
・岡村久道　 『個人情報保護法入門』 商事法務 2003 年
・藤原靜雄　個人情報保護法制研究会　『個人情報保護法の解説（改訂版)』　株式会社ぎょうせい 2005 年
・北原弘章　『漏えい事件、Q&A に学ぶ 個人情報保護と対策 改訂版』　日経 BP 社 2005 年
・御池鮎樹　『スマートフォン 個人情報が危ない！』　株式会社工学社　2013 年
・御池鮎樹　『インターネット個人情報防衛マニュアル』　株式会社工学社　2004 年
・山崎文明　『情報セキュリティと個人情報保護完全対策 改訂版』　日経 BP 社　2004 年
・宮崎貞至　『図解 いますぐ使える個人情報保護マニュアル』　株式会社ぎょうせい 2005 年
・持丸浩二郎　『とっておきの秘技 迷惑メール・スパイウェアの撃退法！』　シーアンドアール研究所　2005 年
・堀部政男　『プライバシー・個人情報保護の新課題』　商事法務　2010 年

≪雑誌・新聞≫

・週刊東洋経済 2013 年 1 月 19 日号
・週刊ダイヤモンド 2012 年 6 月 2 日号
・読売新聞夕刊 17 面 2011 年 11 月 28 日付
・読売新聞夕刊 13 面 2012 年 1 月 31 日付
・読売新聞 35 面 2012 年 4 月 14 日付
・日本経済新聞 2012 年 4 月 11 日付
・日本経済新聞 2012 年 4 月 12 日付
・日本経済新聞 2012 年 5 月 14 日

≪URL≫

・平成 24 年版 情報通信白書
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h24/pdf/24honpen.pdf
・平成 25 年版 情報通信白書
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/pdf/25honpen.pdf
・個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf
・2012 年情報セキュリティインシデントに関する調査報告書【上半期 速報版】
http://www.jnsa.org/result/incident/data/2012H1_incident_survey_sokuhou_v1.0.pdf
・「スマートフォン　プライバシー　イニシアティブ　ー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー」
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
・「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf
・「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」等に関する Q&A
http://www.meti.go.jp/policy/it_policy/privacy/q&a.htm
・IPA 対策のしおりシリーズ　http://www.ipa.go.jp/security/antivirus/shiori.html
・高等学校学習指導要領解説 情報編
http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2012/01/26/1282000_11.pdf
・中学校学習指導要領解説 技術・家庭編
http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2011/01/05/1234912_011_1.pdf
・ITpro　http://itpro.nikkeibp.co.jp/
・日本経済新聞電子版　http://www.nikkei.com/
・YOMIURI ONLINE　http://www.yomiuri.co.jp/
・マイナビニュース　http://news.mynavi.jp/
・BCN Bizline　http://biz.bcnranking.jp/
・MSN 産経ニュース　http://sankei.jp.msn.com/
・SAFETY JAPAN　http://www.nikkeibp.co.jp/sj/2/column/u/03/
・アプリリスク判定ウェブサイト「secroid」　http://secroid.jp/
・IT 用語辞典 e-Words　http://e-words.jp/
・ビジネス+IT　http://www.sbbit.jp/

※URL は、2014 年 1 月 22 日現在のものである