ＥＣにおける個人情報保護に関する活動報告書２００９

平成22年３月

次世代電子商取引推進協議会

ＥＣにおける個人情報保護に関する活動報告書２００９

平成２２年　３月

次世代電子商取引推進協議会

裏

はじめに

１００年に一度と言われる世界的な経済不況の中で企業は、ワークスタイルの大きな変革が求められている。　社内システムの環境も「所有」から「利用」へ「自社管理」から「アウトソーシング」へなど情報処理の形態も変化しつつある。

又、環境問題に対応した各家庭内のエネルギー利用情報や高齢者のさりげない見守りなど、個々の家庭におけるライフスタイル情報があらゆる場面で必要になってくる。　この様に急速に変化する情報環境で適切な個人情報の保護と個人情報の活用を推進し、消費者の利便性を図らなければならない。

個人情報保護に関する活動や認識は、十分浸透したと言っても過言ではないが、その一方で「過剰な反応」が個人情報を活用する上で障壁となっていることも事実である。又、個人情報の漏えい事故も依然として多発している。

このような状況を鑑み、安全・安心ＥＣ環境整備グループ／個人情報保護ワーキンググループでは、平成２１年度の活動として「個人情報保護の国内動向」、「個人情報保護の国際動向」、「個人情報利活用に関する検討」などについて取り組んだ。

本報告書は、上記に係わる活動を中心に取りまとめたものである。　本報告書が会員企業並びに各企業において今後の個人情報保護活動推進に貢献できることを願うものである。

最後に、本報告書の作成にあたり、個人情報保護ワーキンググループにご参加頂いた会員企業有志各位、有識者各位、関係団体より、多くのご意見やご支援を頂き、この場をお借りして厚く御礼申し上げる。

平成２２年３月

次世代電子商取引推進協議会

裏

目　　次

裏

1. 個人情報保護の国内動向

1.1 行政の動向

「個人情報の保護に関する法律」（以下、「保護法」という）が全面施行（平成 17 年 4 月１日）されて、５年目となる平成２１年度は、「経済産業分野を対象とする個人情報保護ガイドライン」（以下、ガイドラインという）の大幅な改正が行われ、平成２１年１０月９日付けで告示された。

本ガイドラインは、平成１９年９月と平成２０年２月に改正され、この度の改正で３度目となる。平成２０年２月の改正では、漏えい事故への対応に留まったが、今回の改正は内閣府国民生活審議会（現在、内閣府消費者委員会）での検討の結果と「パーソナル情報研究会」で取り上げられた課題等を対象に広範囲に改訂作業が行われた。（1.2 にて詳述）

一方、経済産業省への個人情報漏えい事故の報告状況では、流出件数の少ない事案が大幅に増加し、全体的にも増加傾向にある。　個人情報漏えい事故件数の推移を表 1 に示す。

	平成 17 年度	平成 18 年度	平成 19 年度	平成 20 年度
事故件数	1169	785	1722	2589

表 1　保護法施行後からの漏えい事故報告件数推移

また、国際化対応としては、ＡＰＥＣフレームワークに沿った個人データの越境ルール（ＣＢＰＲ）を検証する「パスファインダープロジェクト」のパイロットプロジェクト（project9）が開始された。我が国も、オブザーバー参加であるがパイロットプロジェクトの検証作業に参加協力を行った。　パイロットプロジェクトには、ECOM 会員企業のご協力を頂いたことを追記する。

1.2 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の改正について

（1）改正の主旨

個人情報保護に関する国民の意識の高まりとともに事業者の取組みも進んでいる一方、依然として社会的な耳目を引く個人情報漏えい事案が跡を絶たない状況にある。　また、保護法に対する誤解等に起因して、必要とされる個人情報の提供までもが行われず、事業活動が抑制され、消費者の利便性が図れない「過剰反応」といわれる状況も一部みられる。

これらの保護法施行後の諸状況と対応については、内閣府国民生活審議会（現在:内閣府消費者委員会）で検討がなされ、「個人情報の保護に関する基本方針」（以下、基本方針という）の一部変更等が行われている。　他方、一人ひとりの個性やニーズに応じたビジネ

ス・サービスが展開されつつある昨今では、個人に関する情報の重要性がますます大きくなっており、有効な個人情報の利活用を進めて行く上で、保護法のさらなる明確化等を望む声も高まっている。

経済産業省では、平成１９年１２月に「パーソナル情報研究会」を設置し、ＩＴを活用して個人情報の管理や個人の特性に応じたサービスの提供を行うビジネスモデルが拡大する中、安全・安心を確保しつつ多様なサービスの提供を可能にするための課題につき検討を行ってきたところである。

このような状況を踏まえ、基本方針の一部変更等に伴い、また、事業者が行う個人情報の適切な取扱いの確保や有用な個人情報の利用に関する活動を支援することを目的とし、「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」の全部を改正し、平成２１年１０月９日付で告示した。

（２）改正の内容

①　「個人情報の保護に関する基本方針」の一部変更への対応

消費者等の権利利益の一層の保護に関する記述を追加

・保有個人データの自主的な利用停止等
・委託処理の透明化
・利用目的の明確化
・個人情報の取得元又は、取得方法の具体化

②　「個人情報の保護に関する法律施行令」の一部改正への対応

施行令第２条（個人情報取扱事業者から除外される者）の改正に伴い、記述を修正

・施行令第２条に規定する「特定の個人の数」に算入しないものとして、「不特定かつ多数の者に販売することを目的として発行され、かつ、不特定かつ多数の者により随時に購入することができるもの又はできたもの」が追加されたことに伴い、その具体例として、「自治体職員録、弁護士会名簿等」を記述するなど、記述を修正。

③　「個人情報の保護に関するガイドラインの共通化について」への対応

利用目的による制限等の適用除外の事例を追加

ａ利用目的による制限の適用除外（法令に基づく場合等）

・犯罪による収益の移転防止に関する法律第９条第１項に基づく特定事業者による疑わしい取引の届出
・児童虐待の防止等に関する法律第６条第１項に基づく児童虐待に係る通告
・統計法第１３条による国税調査などの基幹統計調査に対する報告　等

ｂ利用目的の通知又は公表等の適用除外（当該個人情報取扱事業者の権利等を害するおそれ）

・暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、業務妨害行為を行う悪質者情報を取得したことが明らかになることにより、情報提供を受けた企業に

害が及ぶ場合

c 保有個人データの開示の適用除外（他の法令に違反することとなる場合）

・刑法第１３４条（機密漏示罪）や電気通信事業法第４条（通信の秘密の保護）に違反することとなる場合

④　「パーソナル情報研究会」で検討を行った各課題への対応

個人情報の利用を進めるために必要と考えられる課題に対応し、記述を修正

a 性質に応じた個人情報等の取扱い

・漏えい等をした場合の主務大臣等への報告について、ファクシミリやメールの誤送信の場合には、月に１回ごとにまとめて実施することができるよう、記述を修正

b 「事業承継」に係るルールの明確化

・事業承継のための契約を締結するより前の交渉段階で、事業承継の相手会社から自社の調査（デューデリジェンス）を受け、自社の個人データを相手会社へ提供する場合は、当該データの利用目的及び取扱方法、漏えい等が発生した場合の措置、事業承継が不調となった場合の措置等、相手会社に安全管理措置を遵守させるため必要な契約をすることにより、本人の同意がなくとも個人データを提供することができるよう、記述を修正

c 「共同利用」制度の利用普及に係る具体策

・共同利用の事例として、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を追加するほか、共同利用の際に本人通知等をすべき情報のうち、これまで変更することができなかった情報（共同して利用される個人データの項目及び共同利用者の範囲）について、共同利用を行う事業者の名称のみの変更で当該事業者の事業内容に変更がない場合、共同利用を行う事業者について事業の承継が行われた場合や本人の同意を得た場合には、変更することができるよう、記述を修正

⑤　その他

不正の手段により個人情報を取得している事例を追加

・法第２３条に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

・不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

１．３ 民間部門における電子商取引に係る個人情報保護に関するガイドライン（Ver. 7.0）への反映について

「経済産業分野に関する個人情報保護ガイドライン」の改正に伴ってＥＣＯＭガイドラインへの反映するべき個所を以下の表２－1～２－３に示す。

表２－１　平成２１年度改正に伴うＥＣＯＭガイドラインとの対比表

項番	経済産業分野に関する個人情報保護ガイドライン改正箇所		ＥＣＯＭガイドライン（Ver.7.0）	
1	1. 適用範囲	経済産業分野において個人情報取扱事業者でない事業者についても、「個人情報は、個人の人格尊重の理念の下に慎重に取扱われるべきものであることに鑑み、その適正な取扱が図られなければならない」（法第３条）という法の基本理念を踏まえ、このガイドラインに規程されている事項を遵守することが望ましい。	第２条 適用範囲	平成 21 年改訂済み
2	2-1-3 個人情報取扱事業者	特定の個人の数に算入しない事例 不特定かつ多数の者に販売することを目的として発行され、かつ、不特定かつ多数のものにより随時に購入することができる又はできた個人情報データベース等であること（例：自治体職員名簿、弁護士会名簿など） 又、算入しない個人情報データベースを編集・加工していないこと	第３条 3-(3) 個人データに該当しない事例	当該個所に同左記述の追記が必要
3	2-1-5 ④ 保有個人データ	事例の追加 犯罪収益との関係が疑わしい取引(疑わしい取引)の届出の対象情報	第３条 3-(1) ④ 保有個人データ	解説に同左記述を事例として追記が必要
4	2-2-1(1) 利用目的の特定	*「なお、利用目的の特定の際に、利用する個人情報の項目及び入手先の事業名等を特定することまで求められるわけではない」*を削除 また、消費者等、本人の権利利益保護の観点からは、事業活動の特性、規模及び実態に応じ、事業内容を勘案して顧客の種類ごとに利用目的を限定して示したり、本人の選択によって利用目的の限定ができるようにしたりする等、本人にとって利用目的がより明確になるような取組が望ましい。	第６条　1 利用目的の特定 （解説）	解説１の*「なお、利用目的の特定の際に、利用する個人情報の項目及び入手先の事業名等を特定することまで求められるわけではない」*記述の削除が必要 又、同左記述の挿入が必要
5	2-2-1(5) 適用除外	法令に基づく場合の法令事例の追加記述　ガイドライン参照のこと	第７条 3-(1) 法令に基づく場合	解説３の(1)に法令事例を追加記述　ガイドライン参照 同(4)に追記
6	2-2-1(5) 適用除外 国の機関等への協力	事例３）を追加 ガイドライン参照のこと	第７条 3-(4) 国の機関等への協力	同左事例の追加記述が必要 ガイドライン参照

表２－２　平成２１年度改正に伴うＥＣＯＭガイドラインとの対比表

項番	経済産業分野に関する個人情報保護ガイドライン改正箇所		ＥＣＯＭガイドライン（Ver.7.0）	
7	2-2-2(1) 適正取得	【個人情報取扱事業者が不正の手段により個人情報を取得している事例】 事例４)、事例５)を追加 ガイドライン参照のこと	第８条 (解説)	【不正な手段により個人情報を取得している事例】の追加 事例４)、事例５)を追加記述が必要 ガイドライン参照
8	2-2-2(5) 適用除外	(ⅱ)当該個人情報取扱事業者の権利等を害するおそれ 事例２)を追加 ガイドライン参照のこと	第１２条 (解説)	【当該事業者の権利等を害するおそれがある場合の事例】 事例２)を追加記述が必要 ガイドライン参照
9	2-2-3-2 安全管理措置	【各項目を実践するために講じることが望まれる手法の例示】 (エ)影響を受ける可能性のある本人への連絡 ・高度な暗号化…にただし書き追加 ・漏えい等をした…にただし書き追加	第３９条 1と2 漏えい等が発生した場合の措置 巻末資料1 組織的、人的、物理的及び技術的安全管理措置の具体的事項	1と2の記述内に(ただし…)で本人通知不要となっている箇所への下記内容の追記が必要 ・主務大臣への報告に際して措置内容が技術的に判断できることを具体的に報告する **（ア）組織的安全管理措置** 【各項目を実践するために講じることが望まれる手法の例示】の⑤ (エ)影響を受ける可能性のある本人への連絡 ・高度な暗号化…にただし書き追加記述が必要 ・漏えい等をした…にただし書き追加記述が必要
10	2-2-3-2 安全管理措置	【各項目を実践するために講じることが望まれる手法の例示】 (オ)主務大臣への報告 例示ｃが追加	巻末資料1 組織的、人的、物理的及び技術的安全管理措置の具体的事項	**（ア）組織的安全管理措置** 【各項目を実践するために講じることが望まれる手法の例示】の⑤ (オ)主務大臣への報告 例示ｃが追加記述が必要
11	2-2-3-2 安全管理措置	【各項目を実践するために講じることが望まれる手法の例示】 （カ）事実関係、再発防止策等の公表 ・高度な暗号化…にただし書き追加 ・漏えい等をした…にただし書き追加	巻末資料1 組織的、人的、物理的及び技術的安全管理措置の具体的事項	**（ア）組織的安全管理措置** 【各項目を実践するために講じることが望まれる手法の例示】の⑤ （カ）事実関係、再発防止策等の公表 ・高度な暗号化…にただし書き追加記述が必要 ・漏えい等をした…にただし書き追加記述が必要
12	2-2-3-4 委託先の監督	文中にタイトルを設ける ①委託先の選定 ②委託契約の締結 ③委託先における個人データ取扱状況の把握	第２６条 委託先の監督 （解説）	解説文をガイドラインに沿って変更、追加記述が必要

表２－３　平成２１年度改正に伴うＥＣＯＭガイドラインとの対比表

項番	経済産業分野に関する個人情報保護ガイドライン改正箇所		ＥＣＯＭガイドライン（Ver.7.0）	
13	2-2-4 第三者への提供	（３）第三者に該当しないもの （ⅱ）事業の承継 事業承継の契約前段階での個人データ提供に関する取り決め方法が追加	第３０条 第三者に該当しない場合	解説-２に事業承継の契約前段階での個人データ提供に関する取り決め方法の追加記述が必要 ガイドライン参照のこと
14	2-2-4 第三者への提供	（３）第三者に該当しないもの （ⅲ）共同利用 追加、変更及び事例の追加	第３０条 第三者に該当しない場合	解説-３共同利用 追加、変更及び事例の追加記述が必要 ガイドライン参照のこと
15	2-2-5-2 保有個人データの開示	「また、消費者等、本人の権利利益保護の観点から、事業活動の特性、規模及び実態を考慮して、個人情報の取得元又は取得方法を、可能な限り具体的に明記し、本人からの求めに一層対応して行くことが望ましい」を文中に追加 （ⅲ）他の法令に違反することとなる場合の事例２）が追加	第３２条 開示	第３２条第１項に同左文書を追加記述が必要 【他の法令に違反することとなる場合の事例】に事例２を追加記述が必要 ガイドライン参照のこと
16	2-2-5-4 保有個人データの利用停止等	「また、消費者等、本人の権利利益保護の観点から、事業活動の特性、規模及び実態を考慮して、個人情報の取得元又は取得方法を、可能な限り具体的に明記し、本人からの求めに一層対応して行くことが望ましい」を最終行に追加	第３４条 利用停止等	解説の最終行に追加記述が必要
17	5.	個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格	参考	ガイドライン参照

ガイドラインの改正項目をＥＣＯＭガイドラインの項目とマッピングをした。
より具体的な解説および事例の追加によって保護法の理解を深めてもらう目的である。
尚、ＥＣＯＭガイドラインの改訂箇所を以下に示す。　また、ＥＣＯＭガイドラインは、後日、ホームページに公表する。

「民間部門における電子商取引に係る個人情報保護に関するガイドライン」改訂項目箇所について

「経済産業分野に関するガイドライン」の改正に伴い「ＥＣＯＭガイドライン」の改訂該当箇所を太字・アンダーラインで記述した。

第３条（定　義）

3.　個人データ・保有個人データの定義関係

(1)　企業が管理する「個人情報データベース等」を構成する個人情報を個人データと定義し、その中で企業が本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する個人データを「保有個人データ」と定義している。なお、政令により、その存否が明らかになることにより公益その他の利益が害されるものとしてガイドライン 3. 定義（6）の①から④に示されるもの及び短期間（6ヶ月以内）に消去されるものは除外される。

①　その個人データの存否が明らかになることで、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの。

事例）　家庭内暴力、児童虐待の被害者の支援団体が、加害者（配偶者又は親権者）及び被害者(配偶者又は子)を本人とする個人データを持っている場合

②　その個人データの存否が明らかになることで、違法又は不当な行為を助長し、又は誘発するおそれがあるもの。

事例 1)　いわゆる総会屋等による不当要求被害を防止するため、事業者が総会屋等を本人とする個人データを持っている場合

事例 2)　いわゆる不審者、悪質なクレーマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人データを保有している場合

③　その個人データの存否が明らかになることで、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの。

事例 1)　製造業者、情報サービス事業者等が、防衛に関連する兵器・設備・機器・ソフトウェア等の設計、開発担当者名が記録された個人データを保有している場合

事例 2)　要人の訪問先やその警備会社が、当該要人を本人とする行動予定や記録等を保有している場合

④　その個人データの存否が明らかになることで、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの。

事例１）　警察からの捜査関係事項照会や捜索差押令状の対象となった事業者がその対応の過程で捜査対象者又は被疑者を本人とする個人データを保有している場合

事例２）　犯罪収益との関係が疑わしい取引（疑わしい取引）の届出の対象情報

(2)　事業者が個人データを受託処理している場合で、その個人データについて、何ら取り決めがなく、自らの判断では本人に開示等をすることができないときは、本人に開示等の権限を有しているのは委託者であって、受託者ではない。

【個人情報データベース等に該当する事例】
事例 1)　電子メールソフトに保管されているメールアドレス帳（メールアドレスと氏名を組み合せた情報を入力している場合）
事例 2)　ユーザＩＤとユーザが利用した取引についてのログ情報が保管されている電子ファイル（ユーザ ID を個人情報と関連付けて管理している場合）
事例 3)　キャンペーン、イベント等の実施にあたりウェブ画面を通して申し込みを受け付けた場合の申込者リストを検索できる状態にしている場合
事例 4)　ウェブ画面を通じて行った、個人情報を含むアンケート結果そのものを保存した電子ファイルを検索できる状態にしている場合
事例 5)　氏名、住所、企業別に分類整理されている市販の人名録

【個人情報データベース等に該当しない事例】
事例 1)　従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いていても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合
事例 2)　アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

【個人データに該当する事例】
事例 1)　個人情報データベース等から他の媒体に格納したバックアップ用の個人情報
事例 2)　コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

【個人データに該当しない事例】
事例）　個人情報データベース等を構成する前の入力帳票に記載されている個人情報

(3)　本ガイドラインでは、ある程度の規模を持つ企業だけでなく、個人レベルで事業を営むケースも多いことから両者を総称する意味で「事業者」とした。このガイドラインを通じて、その適用対象である「個人情報の全部又は一部をインターネット等の情報ネットワークによって取り扱う事業者」を指す。なお、第２条（適用範囲）（解説)３に示すように、このガイドラインは、適用対象の事業者に対して法的な拘束性を持つものではないので、個人情報保護法における「個人情報取扱事業者」の範囲と異なり、その取り扱う個人情報の量や利用方法により適用除外となる事業者等を規定しない。なお、政令では、その事業

の用に供する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数の合計が過去6ヶ月以内のいずれの日においても5000を超えない者は個人情報取扱事業者から除外されるとされている。さらに、**氏名、住所・居所、電話番号のみが掲載された個人情報データベース等（例えば、電話帳、カーナビゲーション）であること、又は、不特定かつ多数の者に販売することを目的として発行され、かつ、不特定かつ多数の者により随時に購入することができる又はできた個人情報データベース等（例えば、自治体職員録、弁護士会名簿等）であること。又、事業者自らが、その個人情報データベース等を**編集し、又は加工することなくその事業の用に供するときは、これを構成する個人情報によって識別される特定の個人の数は、個人情報取扱事業者の範囲を画する際の個人情報によって識別される特定の個人の数に算入しないとされている。

第6条（利用目的の特定）

1　事業者は、個人情報を取り扱うにあたっては、本人が事業者において最終的にどのような目的で個人情報を利用するかを判断できる程度に可能な限り具体的にその利用の目的（以下「利用目的」という。）を特定しなければならない。

2　事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

（解説）

1.　事業者は、利用目的をできる限り具体的に特定しなければならない。 利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、事業者において最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定する必要がある（電話帳、カーナビゲーションシステム等の取り扱いについての場合を除く。）。

具体的には、「○○事業における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられるが、定款や寄附行為等に想定されている事業の内容に照らして、個人情報によって識別される本人からみて、自分の個人情報が利用される範囲が合理的に予想できる程度に特定している場合や業種を明示することで利用目的の範囲が想定される場合には、これで足りるとされることもあり得るが、多くの場合、業種の明示だけでは利用目的をできる限り具体的に特定したことにはならない。また、単に「事業活動」、「お客さまのサービスの向上」等のように抽象的、一般的に特定することは、できる限り具体的に特定したことにはならない。

また、消費者等、本人の権利利益保護の観点からは、事業活動の特性、規模及び実態に応じ、事業内容を勘案して顧客の種類ごとに利用目的を限定して示したり、本人の選択によって利用目的の限定ができるようにしたりする等、本人にとって利用目的がより明確に

なるような取組が望ましい。　なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨特定しなければならない。

2.　雇用管理情報の利用目的の特定に当たっても、単に抽象的、一般的に特定するのではなく、労働者等（事業者に使用されている労働者、事業者に使用される労働者になろうとする者及びなろうとした者並びに過去において事業者に使用されていた者。以下同じ。）本人が、取得された当該本人の個人情報が利用された結果が合理的に想定できる程度に、具体的、個別的に特定しなければならない。

【具体的に利用目的を特定している事例】

事例 1)　「ネット販売業における商品の発送、代金決済、新商品・サービスに関する情報の通知のために利用する。」

事例 2)　「××サービスの提供にあたりサービス内容の確認、代金決済、サービスご提供後の満足度調査のお願いのために利用する。」

事例 3)　「お客様向けメール・マガジンの送付先として使用する。」

事例 4)　「お客様からの相談に関する回答のためにのみ利用する。」

【具体的に利用目的を特定していない事例】

事例 1)　「当社の事業活動に供するため」

事例 2)　「弊社が提供するサービスの向上のため」

事例 3)　「マーケティング活動に用いるため」

3.　上記２により特定した利用目的は、社会通念上、本人が想定することが困難でないと認められる範囲内で変更することは可能である。変更された利用目的は、本人に通知するか、又は公表しなければならない。なお、本人が想定することが困難であると認められる変更を行う場合は、法第１６条に従って本人の同意を得なければならない。

【本人が想定することが困難でないと認められる範囲内に該当する事例】

事例)「当社の行う○○事業における新商品・サービスに関する情報のお知らせ」とした利用目的において「既存の商品・サービスに関する情報のお知らせ」を追加すること。

参考　個人情報保護法第 15 条

第 7 条（利用目的による制限）

1　事業者は、あらかじめ本人の同意を得ないで、第 6 条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。

2　事業者は、合併その他の事由により他の事業者から事業を承継することに伴って個人情

報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3　前２項の規定は、次に掲げる場合については、適用しない。

①　法令に基づく場合

②　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

③　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

④　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（解説）

1.　一旦取得した個人情報について当初の利用目的の達成に必要な範囲を超えて取り扱うときには、あらかじめ本人の同意を得なければならない。同意を得るために個人情報を利用すること（メールの送付や電話をかけること等）は、当初の利用目的として記載されていない場合でも、目的外利用には該当しない。

【同意が必要な事例】

事例 1)　苦情受付のためのお客様相談センターにて収集された情報をもとに、自己商品の販売促進のために試供品を送る場合

事例 2)　就職のための求職者からの履歴書情報をもとに、自己商品の販売促進のために自己販売サイトの案内メールを送る場合

2.　「本人の同意」とは、本人が個人情報の取り扱いに関する情報を与えられたうえで、本人の個人情報が、事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいう。ネットワーク上で行う場合には、本人による同意する旨のウェブ画面上のボタンのクリック、本人からの同意する旨のメールの受信等がこれにあたる。

3.　本条第３項①～④の適用除外の具体的事例は次のとおり。

(1)　法令に基づく場合　（第３項①関連）

法令に基づいて個人情報を取り扱う場合は、その適用を受けない。

上記の根拠となる法令の規定としては、刑事訴訟法第２１８条（令状による捜査）、少年法第６条の５（令状による触法少年の調査）、所得税法第２３４条（所得税に係る税務職員の質問検査権）、地方税法第７２条の７（事業税に係る徴税吏員の質問検査権、その他各種税法に類似の規定あり）等が考えられる。これらについては、強制力を伴っており、一律これに該当する。

事例１）　金融商品取引法第２１１条により裁判所許可状に基づいて証券取引等監視委員の職員が行う犯則事件の調査への対応

事例２）　犯罪による利益の移転防止に関する法律第９条第１項に基づく特定事業者による疑わしい取引の届出

事例３）　児童虐待の防止等に関する法律第６条第１項に基づく児童虐待に係る通告

事例４）　所得税法第２２５条第１項等による税務署長に対する支払調書等の提出

事例５）　統計法第１３条による国税調査などの基幹統計調査に対する報告

一方、刑事訴訟法第１９７条第２項（捜査に必要な取調べ）や少年法第６条の４（触法少年の調査に必要な質問や調査関係事項照会等）は、強制力を伴わないが、法令に根拠があるのでこれに該当する。また、弁護士法第 23 条の 2（弁護士会からの照会）の場合も、同様に対象となると考えられるが、提供にあたっては同照会制度の目的に即した必要性と合理性が認められるかを考慮する必要がある。

事例１）　金融商品取引法第２１０条により証券取引等監視委員会の職員が行う犯則事件の調査への対応

事例２）　刑事訴訟法第５０７条による裁判執行関係事項照会への対応

事例３）　刑事訴訟法第２７９条、心神喪失等の状態で重大な他害行為を行った者の医療及び観察等に関する法律第２４条第３項による裁判所からの照会への対応

事例４）　民事訴訟法第１８６条、第２２６条、家事審判規則第８条による裁判所からの文書送付や調査の嘱託への対応

事例５）　家事審判規則第７条の２に基づく家庭裁判所調査官による事実の調査への対応

事例６）　犯罪被害財産等による被害回復給付金の支給に関する法律第２８条による検察官や被害回復事務管理人からの照会への対応

事例７）　会社法第 381 条３項による親会社の監査役の子会社に対する調査への対応

事例８）　会社法第 396 条及び証券取引法第１９３条の２の規定に基づく財務諸表監査への対応

事例９）　製造･輸入業者が、消費生活用製品安全法第 39 条第 1 項の規定による命令（危害防止命令）を受けて製品の回収等の措置をとる際に、販売事業者が、同法第 39 条第３項の規定に基づき製品の購入者等の情報を製造･輸入業者に提供する場合

事例１０）　統計法第３０条及び第３１条による国税調査などの基幹統計調査に関する協力要請への対応

⑵　人の生命、身体又は財産の保護（3②関連）

人（法人を含む。）の生命、身体又は財産といった具体的な権利利益が侵害されるおそれがあり、これを保護するために個人情報の利用が必要であり、かつ、本人の同意を得ることが困難である場合（他の方法により、当該権利利益の保護が十分可能である場合を除く。）は、その適用を受けない。

事例 1)　急病その他の事態時に、本人について、その血液型や家族の連絡先等を医師や看護師に提供する場合

事例 2)　私企業間において、意図的に業務妨害を行う者の情報について情報交換される場合

事例 3)　製品事故が生じたため、又は、製品事故は生じていないが、人の生命若しくは身体に危害を及ぼす急迫した危険が存在するため、製造事業者等が消費生活用製品をリコールする場合で、販売事業者、修理事業者又は設置工事事業者等が当該製造事業者等に対して、当該製品の購入者等の情報を提供する場合

(3)　公衆衛生の向上等（３③関連）

公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。）は、その適用を受けない。

事例 1)　健康保険組合等の保険者等が実施する健康診断やがん検診等の保健事業について、精密検査の結果や受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的として疫学研究又は統計調査のために、個人名を伏せて研究者等に提供する場合

事例 2)　不登校や不良行為等児童生徒の問題行動について、児童相談所、学校、医療行為等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合

(4)　国の機関等への協力（３④関連）

国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であり、協力する民間企業等が目的外利用を行うことについて、本人の同意を得ることが当該事務の遂行に支障を及ぼすおそれがあると認められる場合は、その適用を受けない。

事例 1)　事業者等が、税務署の職員等の任意調査に対し、個人情報を提出する場合

事例 2)　事業者等が警察の任意の求めに応じて個人情報を提出する場合

事例３）　一般統計調査や地方公共団体が行う統計調査に回答する場合

4.　個人情報保護法の施行前に第６条１項により特定される利用目的以外の目的で個人情報を取り扱う旨の同意に相当するものがある場合は本項の同意があったものとみなされる。

参考　個人情報保護法第 16 条　附則第 2 条

第 8 条（適正な取得）

事業者は、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。

（解説）

1.　個人情報の取得に際し、事業者は本人に対し、個人情報の利用目的を偽るなど不正な手

段を用いて取得してはならない。
　なお、不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、詐欺等により取得したり、使用・開示した者には不正競争防止法（平成５年法律第４７号）第２１条により刑事罰（５年以下の懲役又は５００万円以下の罰金）が科され得る。

2.　偽りその他不正な手段（騙す、脅す、盗むなどをいう。）により取得した第三者から、不正な手段の介在を知りながら間接的に取得してはならない。また、個人情報保護法で規定されている第三者への提供の措置を行っていない第三者からその事実を知りながら間接的に取得してはならない。
3.　住民基本台帳法の改正により運用の始まった「住民票コード」のように法令により取得を禁止されているものは取得してはならない。

【事業者が不正な手段により個人情報を取得している事例】
事例 1)　親の同意がなく、十分な判断能力を有していない子どもから、取得状況から考えて関係
のない親の収入事情などの家族の個人情報を（情報ネットワークを通して）取得する場合
事例 2)　法第２３条に規定する第三者提供制限違反をするよう強要して個人情報を取得した
場合
事例 3)　他の事業者に指示して上記事例１）又は事例２）などの不正の手段で個人情報を取
得させ、その事業者から個人情報を取得する場合
事例４）　本人の同意を得ることなく、かつ、法第２３条の各項各号に定める方法によることなく個人情報が提供されようとしていることを知り、又は、容易に知ることができるにもかかわらず、当該個人情報を取得する場合
事例５）　上記１）又は上記２）などの不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

参考　個人情報保護法第 17 条

第 12 条（取得時及び利用目的の変更時の措置の適用除外）
　前第 9 条から第 11 条の規定は、次に掲げる場合については適用しない。
①　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

② 利用目的を本人に通知し、又は公表することにより当該事業者の権利又は正当な利益を害するおそれがある場合
③ 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
④ 取得の状況からみて利用目的が明らかであると認められる場合

（解説）
個人情報保護法第 18 条第４項において、上記の４項目は、取得に際しての利用目的の通知等の原則的な規定の適用が除外される事項として記されている。

【本人又は第三者の権利利益を害するおそれがある場合の事例（①関連)】
事例） いわゆる総会屋等による不当要求等の被害を防止するため、当該総会屋担当者個人に関する情報を取得し、相互に情報交換を行っている場合で、利用目的を通知又は公表することにより、当該総会屋等の逆恨みにより、第三者たる情報提供者が被害を被るおそれがある場合

【当該事業者の権利等を害するおそれがある場合の事例（②（関連)】
事例１） 通知又は公表される利用目的の内容により、当該事業者が行う新商品等の開発内容、営業ノウハウ等の企業秘密にかかわるようなものが明らかになる場合
事例２） 暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、業務妨害行為を行う悪質者情報を取得したことが明らかになることにより、情報提供を受けた企業に害が及ぶ場合

【国の機関等への協力がある場合の事例（③関連)】
事例） 公開手配を行わないで、被疑者に関する個人情報を、警察から被疑者の立ち回りが予想される事業者に限って提供する場合、警察から受け取った当該事業者が利用目的を本人に通知し、又は公表することにより、捜査活動に重大な支障を及ぼすおそれがある場合

【利用目的が自明の場合の事例（④関連)】
事例 1) 商品・サービス等を販売・提供する場合、住所・電話番号等の個人情報を取得する場合があるが、その利用目的が当該商品・サービス等の販売・提供のみを確実に行うためという利用目的であるような場合
事例 2) 一般の慣行として名刺を交換する場合、書面により、直接本人から、氏名・所属・肩書・連絡先等の個人情報を取得することとなるが、その利用目的が今後の連絡のためと

いう利用目的であるような場合（ただし、ダイレクトメール等の目的に名刺を用いることは自明の利用目的に該当しない場合があるので注意を要する）。

参考　個人情報保護法第 18 条第 4 項

第 26 条（委託先の監督）

1　事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託した個人データの安全管理が図られるよう、受託者に対する必要かつ適切な監督を行わなければならない。

（解説）

1.　近年の情報化の進展に伴い、企業における情報処理業務がますます多様化、複雑化していることから経営の効率化や顧客サービスの向上等のために情報処理業務を外部に委託するケースも多くなっている。その際、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然のこととして、取扱いを委託する個人データの内容を踏まえ、本人の個人データが漏えい、滅失またはき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質および個人データの取扱い状況等に起因するリスクに応じた、必要かつ適切な監督を講ずるものとする。「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に当該個人データに係る安全管理措置を遵守させるために必要な契約を締結すること、委託先における当該個人データの取り扱い状況を把握することが含まれる。

①　委託先の選定

委託先を適切に選定するためには、委託先において実施される個人データの安全管理措置が委託する業務内容に相応しいものであることを確認することが必要である。また委託先の評価は適宜実施することが望ましい。

②　委託契約の締結

委託契約には、当該個人データの取扱に関する、必要かつ適切な安全管理措置として、委託元、受託先双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で相互が確認することも含まれる。

なお、本人からの損害賠償請求に係る責務を、安全管理措置に係る責任分担を無視して一方的に受託者に課すなど、優越的地位にある者が委託者の場合、受託者に不当な負担を課すことがあってはならない。

③　委託先における個人データ取扱い状況の把握

・　個人情報の処理を委託している場合において、本人からの開示・訂正・削除等の求めに応ずる責任を負うのは、直接的には委託元の事業者である。ただし、委託の業態に応じ

て、委託先に対し、開示・訂正・削除等の請求を受ける窓口事務や、場合によっては、求めに応じて開示・訂正・削除等を行うこと自体を委託契約のなかで定めることもできる。

・　委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託がある場合は注意を要する。

・　漏えいした場合に二次被害が発生する可能性が高い個人データ（例えば、クレジットカード情報を含む個人データ等）の取り扱いを委託する場合は、より高い水準において「必要かつ適切な監督」を行なうことが望ましい。

・　**消費者等、本人の権利利益保護の観点から、事業内容の特性、規模及び実態に応じ、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めることが望ましい。**

【受託者に必要かつ適切な監督を行っていない場合の事例】

事例 1)　個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合

事例 2)　個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合

事例 3)　再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

【個人データの取り扱いを委託する場合に契約に盛り込むことが望まれる事項】

○　委託者及び受託者の責任の明確化

○　個人データの安全管理に関する事項

・　個人データの漏えい防止、盗用禁止に関する事項

・　委託契約範囲外の加工、利用の禁止

・　委託契約範囲外の複写、複製の禁止

・　委託契約期間

・　委託契約終了後の個人データの返還・消去・廃棄に関する事項

○　再委託に関する事項

・　再委託を行うに当たっての委託者への文書による報告

○　個人データの取扱状況に関する委託者への報告の内容及び頻度

○　契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）

○　契約内容が遵守されなかった場合の措置

○　セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

参考　個人情報保護法第 22 条

第 30 条（第三者に該当しない場合）
1　次の各号のいずれかに該当する場合は、当該個人データの提供を受ける者は、第 28 条及び第２９条の規定の適用については、第三者に該当しないものとする。
①　利用目的の達成に必要な範囲内において個人データの取り扱いの全部又は一部を委託する場合
②　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
③　個人データを特定の者との間で共同して利用する場合であって、以下のことをあらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。
ア　共同利用する旨
イ　共同して利用される個人データの項目
ウ　共同して利用する者の範囲
エ　利用する者の利用目的
オ　当該個人データの管理について責任を有する者の氏名又は名称
2　前項③号に規定する項目のうち、エ又はオを変更する場合は、変更する内容について、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。

（解説）
1. 個人情報の処理を外部に委託することは、個人情報を取得した事業者の目的の範囲内で行われる一般的な行為であるため、個人情報保護法でも委託先は第三者に該当しないとしている。ただし、個人情報取扱事業者には、委託先に対する監督責任が課される（法第２２条関連）。

【委託に伴って個人データが提供される場合の事例】
事例１）データの打ち込み等、情報処理を委託するために個人データを渡す場合
事例２）ネットショップが注文を受けた商品の配送のために、宅配業者に個人データを渡す場合
事例３）　ネットショップ商品代金回収業務を宅配業者に委託する場合。

2. 合併、分社化、営業譲渡等により事業が承継され個人データが移転される場合は、第三者に該当しない。事業の承継のための契約を締結するより前の交渉段階で、相手会社から自社の調査を受け、自社の個人データを相手会社へ提供する場合は、**当該データの利用目的及び取扱方法、漏えい等が発生した場合の措置、事業承継の交渉が不調となった場合**

の措置等、相手会社に安全管理措置を遵守させるため必要な契約を締結しなければならない。

事業の承継後も、個人データが譲渡される前の利用目的の範囲内で利用しなければならない。

【事業の承継に伴って個人データが提供される場合の事例】
事例 1) 合併、分社化により、新会社に個人データを渡す場合
事例 2) 営業譲渡により、譲渡先企業に個人データを渡す場合

3. 本条１項③号については、複数の企業が個人情報を共有することでより効率的、一体的かつ円滑な事業展開を行うケース等が想定される。ただし、この共同利用はあらかじめ個人情報の利用目的にグループによる共同利用がある旨を本人に通知し、又は容易に知りうる状態に置くことが条件になっているので注意が必要である（この場合の複数の企業とは必ずしも資本関係の有無を条件としない。）。例として、旅行業界で顧客情報を共有する場合やクレジットカード利用に関する個人信用情報照会システムなどがあげられる。なお、事業者がこの共同利用を行うにあたっては、共同利用対象会社の個人情報保護推進部門と連携を取りつつ行うものとする。

共同利用する場合、以下のア）からエ）までの情報のほか、あらかじめ一定の事項につき取り決めておくことが望ましい。共同利用の対象となる個人データの提供について、必ずしも当該共同利用者の範囲に属するすべての事業者が行う必要はない。

なお、共同利用か委託かは、個人データの取扱いの形態によって判断されるものであって、共同利用者の範囲に委託先事業者が含まれる場合であっても、委託先との関係は、共同利用となるわけではなく、委託先の監督義務を免れるわけでもない。

例えば、グループ企業でイベントを開催する場合に、各子会社から親会社（幹事会社）に顧客情報を集めた上で展示会の案内を発送する場合は共同利用となるが、自社でイベントを開催する場合に、案内状を発送するために発送代行事業者に顧客情報を提供する場合は、共同利用者の範囲に含まれるグループ企業内の事業者への提供であったとしても、委託であって、共同利用とはならない。

【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（法第１５条第２項の規定に従い変更された利用目的を含む。　以下同じ）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

ア）　共同して利用される個人データの項目

事例 1）氏名、住所、メールアドレス
事例 2）氏名、商品購入履歴

イ）　共同利用者の範囲（本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。）
事例）　最新の共同利用者のリストにつき本人が容易に知り得る状態に置かれているとき

ウ）　利用する者の利用目的（共同して利用する個人データの全ての利用目的）

エ）　開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称（共同利用者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する事業者を、「責任を有する者」といい、共同利用者の内部の担当責任者をいうのではない。　責任を有する者は、利用目的の達成に必要な範囲内において、共同利用者間で利用している個人データを正確かつ最新の内容に保つよう努めなければならない。）

【上記、アからエまでの事項のほかに取り決めておくことが望ましい事項】
①共同利用者の要件（グループ会社であること、特定のキャンペーン事業の一員であること等、共同利用による事業遂行上の一定の枠組）
②各共同利用者の個人情報取扱責任者、問い合わせ担当者および連絡先
③共同利用する個人データの取扱いに関する事項
・個人データの漏えい等防止に関する事項
・目的外の加工、利用、複写、複製等の禁止
・共同利用終了後のデータの返還、消去、廃棄に関する事項
④共同利用する個人データの取扱いに関する取決が遵守されなかった場合の措置
⑤共同利用する個人データに関する事件・事故が発生した場合の報告・連絡に関する事項
⑥共同利用を終了する際の手続

上記、③および④については、社会通念上、本人が想定することが困難でないと認められる範囲内で変更することができ、変更する前に、本人に通知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。　また、上記①および②については、原則として変更は認められないが、次の場合、引き続き共同利用を行うことができる。

【引き続き共同利用を行うことができる事例】

事例１）　共同利用を行う事業者の名称が変更するが、当該事業者の事業内容に変更がない場合

事例２）　共同利用を行う事業者について事業の承継が行われた場合

事例３）　共同利用を行う事業者や個人データの項目の変更につき、あらかじめ本人の同意を得た場合

4.　個人情報保護法の施行前に本人に通知されているときは当該通知は本条 1 項の規定により行われたものとみなされる（個人情報保護法附則第 5 条)。

参考　個人情報保護法第 23 条第 4 項・第 5 項　附則第 5 条

第 32 条（開　示）

1　事業者は、保有個人データについて、本人から当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。）を求められた場合は、本人確認のうえ遅滞なくこれに応じなければならない。ただし、事業者は、開示することにより、次に該当する場合はその全部又は一部を開示しないことができるものとし、開示ない旨の決定をしたときはその旨を本人に対して遅滞なく通知を行う。

①　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

②　事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

③　他の法令に違反することとなる場合

2　事業者は、前項で定める開示にあたっては、書面を交付する方法により行うこととする。ただし、開示の求めを行った者が同意した方法があるときは、当該方法で行うことができる。

（解説）

1.　第３１条の解説 1.に示すように誤った情報により本人の権利が侵害されることがあるため、本人は事業者に対し、保有個人データの開示を求めることができる。

2.　事業者は本人からの開示の求めに対し、本条１項①から③の場合を除き、遅滞なく開示しなければならず、また、本条 1 項①から③の場合に該当し、開示しないことを決定したときもその旨を遅滞なく通知しなければならない。「遅滞なく」とは本人からの申し出に対

して、いたずらに時間をかけることなく速やかに行われることをいい、通常の場合は 2 週間以内が妥当と考えられる。

3. 政令により、開示の方法としては、原則として、書面により交付することとし、開示の求めを行った者が同意した方法があるときは当該方法で行うことができる。これについては、開示の求めを行った者から開示の方法について特に指定が無く、事業者が提示した方法に対して異議を述べなかった場合（電話での開示の求めがあり、必要な本人確認等の後、そのまま電話で問い合わせ等に回答する場合を含む。）は、当該方法について同意があったものととみなすことができる。

4. 雇用管理情報の開示の求めに応じる手続については、事業者はあらかじめ労働組合等と必要に応じ協議したうえで、本人から開示を求められた保有個人データについて、その全部又は一部を開示することによりその業務の適正な実施に著しい支障を及ぼすおそれがある場合に該当するとして非開示とすることが想定される保有個人データを定め、従業者等に周知させるための措置を講ずるよう努めなければならない。

5. 消費者等、本人の権利利益保護の観点から、事業活動の特性、規模および実態を考慮して、個人情報の取得元又は取得方法（取得源の種類等）を、可能な限り具体的に明記し、本人からの求めに一層対応していくことが望ましい。

【本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合の事例】

事例） 医療機関等において、病名等を開示することにより、本人の心身状況を悪化させる恐れがある場合

【事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合の事例】

事例 1） 試験実施機関において、採点情報のすべてを開示することにより、試験制度の維持に著しい支障を及ぼすおそれがある場合

事例 2） 同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなる等、業務上著しい支障を及ぼすおそれがある場合

【他の法令に違反することとなる場合の事例】

事例１） 金融機関が「組織的な犯罪の処罰及び犯罪収益の規制等に関する法律」第５４条第１項に基づいて、主務大臣に取引の届出を行っていたときに、当該届出を行ったことが記録**されている保有個人データを開示することが同条第２項の規定に違反する場合**

事例２） 刑法第１３４条（秘密漏示罪）や電気通信事業法第４条（通信の秘密の保護）に違反することとなる場合

参考　個人情報保護法第 25 条・政令第 6 条

第 34 条（利用停止等）

1　事業者は、本人から、当該本人が識別される保有個人データがその利用目的の制限に違反して取り扱われているという理由若しくは適正な取得に違反して取得されたものであるという理由又は第三者への提供の制限に違反して第三者に提供されているという理由によって当該保有個人データの利用の停止若しくは消去（以下「利用停止等」という。）又は第三者への提供の停止を求められた場合で、その求めに理由があることが判明したときには、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行い、又は遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの利用停止等又は第三者への提供の停止に多額の費用を要する等、その実施が困難な場合であって、本人の権利利益を保護するために必要な代替措置をとるときは、この限りでない。

2　事業者は、前項の規定に基づき求められた保有個人データの全部又は一部について、利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、又は第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

（解説）

1.　個人情報保護法第 27 条にて本人は事業者に対し、同第 16 条の利用目的の制限に違反して取り扱われる場合及び同第 17 条の適正な取得に違反して取得した場合、その個人データの利用の停止又は消去を求めることができるとし、さらに同第 23 条第 1 項の第三者への提供の制限に違反して第三者への提供がされている場合、第三者への提供の停止を求めることができるとしている。

2.　開示請求、訂正等請求と同様に、本人の求めに対し、事業者はその事実関係を調査し、それが正当な求めであることが判明した場合は、いたずらに時間をかけることなく、原則として当該措置を行わなければならない。通常の場合、2 週間以内に作業を完了することが望ましい。なお、保有個人データの全部消去を求められた場合であっても、利用停止によって手続違反を是正できる場合であれば、そのような措置を講ずることにより、義務を果たしたことになり、必ずしも、求められた措置をそのまま実施する必要はない。

また、消費者等、本人の権利利益保護の観点から、事業活動の特性、規模および実態を考慮して、保有個人データについて本人から求めがあった場合には、ダイレクトメールの発送停止等、自主的に応じる等、本人からの求めに一層対応していくことが望ましい。

＊「原則」…違反を是正するための必要な限度を超えている場合や手続違反である旨の指摘が正しくない場合には、利用の停止等を行う必要はない。ただし、その場合には遅滞なく、利用の停止等を行わない旨を本人に通知しなければならない。

3. ただし、個人情報保護法では、利用停止等に応ずる際、その実施に多額の費用を要する等によりその実施が困難な場合、あるいは、例えば事業者が保有するデータベース内でその本人の個人情報のみ利用停止することで、データベースが長期間使用できなくなり、業務上大きな支障が発生したりする場合は、そのことに代えて本人の権利利益を保護する措置が取れるのであればその限りでないとしており、本条においてもそれに従っている。

参考　個人情報保護法第 27 条

第 39 条（漏えい等が発生した場合の措置）

1　事業者は、自己が取り扱う重要な個人データについて漏えい等（滅失、き損を含む。以下同じ。）の事実を把握した場合は当該漏えい等に関する事実関係および二次被害の拡大防止策を本人に速やかに通知するものとする（ただし対象となる個人データが高度な暗号化等の秘匿化が施されている場合、紛失した個人データを第三者に見られることなく、速やかに回収した場合を除く）。

2　事業者は、自己が取り扱う重要な個人データについて漏えい等の事実を把握した場合は二次被害の拡大防止、類似事案の発生回避の観点から、可能な限り事実関係及び発生原因を遅滞なく公表するものとする（ただし対象となる個人データが高度な暗号化等の秘匿化が施されている場合、本人全てに連絡がついた場合を除く）。　**注：巻末資料組織的安全管理⑤－（エ）参照**

3　事業者は、自己が取り扱う重要な個人データについて漏えい等の事実を把握した場合は発生原因及び対応策を所管する省庁に直ちに報告するものとする。認定個人情報保護団体の対象事業者は上記の報告に代えて自己が所属する認定個人情報保護団体に報告することが可能であるが、クレジットカード情報など重要な個人データが漏えいした場合は主務大臣に速やかに報告するものとする。　**注：巻末資料組織的安全管理⑤－（オ）参照**

（解説）

1. 事業者は、自己の取り扱う重要な個人データの漏えい等の事実を把握した場合は、当該本人が適切に対応できるようにするため、事実関係を本人に速やかに通知するものとする。この場合の重要な個人データとは漏えい等があった際に当該本人に与える影響が大きいと思われる情報を指し具体的には

①クレジットカード会員番号などの決済関連情報

②病歴・加療記録、生体認証データなどの身体・健康関連情報

③事業者が個別に判断し本人通知対象として取り扱う情報（プライバシー度が高い商品・サービスに関わる購入履歴、独自に取得・保有している顧客情報でプライバシー度が高いと判断したものなど）が該当する。また、何らかの事由により住民基本台帳番号、基礎年金番号等公的ＩＤ番号を保有しこれを漏えいした場合もこれに該当する。

2. 事業者は、自己の取り扱う重要な個人データの漏えい等の事実を把握した場合は、二次被害の拡大、類似事故の発生回避のため可能な限り事実関係等を遅滞なく公表するものとする。

3. 事業者は、自己の取り扱う重要な個人データの漏えい等の事実を把握した場合は、事実関係、発生原因、対応策を当該事業者の行う事業を所管する省庁へ届け出るものとする。

4. 漏えいした個人データが適切な暗号化等により秘匿化されている場合は本人通知および公表が省略できる場合があるので事前に十分な対策を講じておくことが望まれる。

（ア）　組織的安全管理

組織的安全管理措置とは、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、見直しおよび改善
⑤事故または違反への対処

【各項目を実践するために講じることが望まれる手法の例示】

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」を実践するために講じることが望まれる手法の例示

・従業者の役割・責任の明確化

＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。

・個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））の設置
・個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置および作業担当者の限定

・個人データを取り扱う情報システム運用責任者の設置および担当者（システム管理者を含む。）の限定
・個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化
・監査責任者の設置
・監査実施体制の整備
・個人データの取扱いに関する規程等に違反している事実または兆候があることに気づいた場合の、代表者等への報告連絡体制の整備
・個人データの漏えい等の事故が発生した場合、または発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備
＊個人データの漏えい等についての情報は代表窓口、苦情対応窓口を通じ、外部からもたらされる場合もあるため、苦情の対応体制等との連携を図ることが望ましい（法第３１条を参照）。
・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
・漏えい等の事故発生時における主務大臣および認定個人情報保護団体等に対する報告体制の整備

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」を実践するために講じることが望まれる手法の例示
・個人データの取扱いに関する規程等の整備とそれらに従った運用
・個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用
＊なお、これらについてのより詳細な記載事項については、下記の【個人データの取扱いに関する規程等に記載することが望まれる事項】を参照。
・個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
・個人データの取扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
・定められた規程等に従って業務手続が適切に行われたことを示す監査証跡※の保持
※保持しておくことが望まれる監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかを記録）、教育受講者一覧表等が考えられる。

③「個人データの取扱い状況を一覧できる手段の整備」を実践するために講じることが

望まれる手法の例示

・個人データについて、取得する項目、明示・公表を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取り扱いに必要な情報を記した個人データ取扱台帳の整備

・個人データ取扱台帳の内容の定期的な確認による最新状態の維持

④「個人データの安全管理措置の評価、見直しおよび改善」を実践するために講じることが望まれる手法の例示

・監査計画の立案と、計画に基づく監査（内部監査または外部監査）の実施

・監査実施結果の取りまとめと、代表者への報告

・監査責任者から受ける監査報告、個人データに対する社会通念の変化および情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善

⑤「事故又は違反への対処」を実践するために講じることが望まれる手法の例示

・以下の（ア）から（カ）までの手順の整備

ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられる。

（ア）事実調査、原因の究明

（イ）影響範囲の特定

（ウ）再発防止策の検討・実施

（エ）影響を受ける可能性のある本人への連絡

事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。

ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。

・ 紛失等した個人データを、第三者に見られることなく、速やかに回収した場合

・ 高度な暗号化等の秘匿化が施されている場合**（ただし、（オ）に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。）**

・ 漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合**。ただし、（オ）に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること）**

（オ）主務大臣等への報告

ａ．個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合

認定個人情報保護団体の業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができる。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告する。

ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。

- 機微にわたる個人データ（(a)思想、信条又は宗教に関する事項、(b)人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、(c)勤労者の団結権、団体交渉その他団体行動の行為に関する事項、(d)集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、(e)保健医療又は性生活に関する事項等）を漏えいした場合
- 信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合
- 同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合
- その他認定個人情報保護団体が必要と考える場合

b．個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合

経済産業大臣（主務大臣）に報告を行う。

なお、認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。

a. 及び b. のいずれかの場合も、事業者は次の事例について、認定個人情報保護団体又は主務大臣への報告を月に１回ごとまとめて実施することができる。

・ファクシミリやメールの誤送信（宛名及び送信者名以外に個人情報が含まれていない場合）。なお、内容物に個人情報が含まれない荷物等の宅配又は郵送の誤配については、報告不要である。

（カ）事実関係、再発防止策等の公表

二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。

ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。

- 影響を受ける可能性のある本人すべてに連絡がついた場合
- 紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
- 高度な暗号化等の秘匿化が施されている場合**（ただし、（オ）に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。）**

・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合。**ただし、(オ)に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること**）

【個人データの取扱いに関する規程等に記載することが望まれる事項の例】

以下、①取得・入力、②移送・送信、③利用・加工、④保管・バックアップ、⑤消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。

①取得・入力

ア．作業責任者の明確化

・個人データを取得する際の作業責任者の明確化
・取得した個人データを情報システムに入力する際の作業責任者の明確化
（以下、併せて「取得・入力」という。）

イ．手続の明確化と手続に従った実施

・取得・入力する際の手続の明確化
・定められた手続による取得・入力の実施
・権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という）での入力作業の実施
・ 個人データを入力できる端末の、業務上の必要性に基づく限定
・ 個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする。）

ウ．作業担当者の識別、認証、権限付与

・個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定
・個人データの取得・入力業務を行う作業担当者に付与した権限の記録

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、および作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と、権限外作業の有無の確認

②移送・送信

ア．作業責任者の明確化

・個人データを移送・送信する際の作業責任者の明確化

イ．手続の明確化と手続に従った実施

・個人データを移送・送信する際の手続の明確化
・定められた手続による移送・送信の実施
・　個人データを移送・送信する場合の個人データの暗号化等の秘匿化（例えば、公衆回線を利用して個人データを送信する場合）
・　移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用）
・ＦＡＸ等におけるあて先番号確認と受領確認
・個人データを記した文書をＦＡＸ機等に放置することの禁止
・暗号鍵やパスワードの適切な管理

ウ．作業担当者の識別、認証、権限付与

・個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない）
・個人データの移送・送信業務を行う作業担当者に付与した権限の記録

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と、権限外作業の有無の確認

③利用・加工

ア．作業責任者の明確化

・個人データを利用・加工する際の作業責任者の明確化

イ．手続の明確化と手続に従った実施

・個人データを利用・加工する際の手続の明確化
・定められた手続による利用・加工の実施
・権限を与えられていない者が立ち入れない建物等での利用・加工の実施
・個人データを利用・加工できる端末の、業務上の必要性に基づく限定
・個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする）

ウ．作業担当者の識別、認証、権限付与

・個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。）
・個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

エ．作業担当者及びその権限の確認

・手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と権限外作業の有無の確認

④保管・バックアップ

ア．作業責任者の明確化

・個人データを保管・バックアップする際の作業責任者の明確化

イ．手続の明確化と手続に従った実施

・個人データを保管・バックアップする際の手続※の明確化

※情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム（ＯＳ）やアプリケーションのバックアップも必要となる場合がある。

・定められた手続による保管・バックアップの実施
・個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化
・暗号鍵やパスワードの適切な管理
・個人データを記録している媒体を保管する場合の施錠管理
・個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理
・個人データを記録している媒体の遠隔地保管
・個人データのバックアップから迅速にデータが復元できることのテストの実施
・個人データのバックアップに関する各種事象や障害の記録

ウ．作業担当者の識別、認証、権限付与

・個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない）

・個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録

エ．作業担当者及びその権限の確認

・手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認

・アクセスの記録、保管と権限外作業の有無の確認

⑤消去・廃棄

ア．作業責任者の明確化

・個人データを消去する際の作業責任者の明確化

・個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

イ．手続の明確化と手続に従った実施

・消去・廃棄する際の手続の明確化

・定められた手続による消去・廃棄の実施

・権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施

・個人データを消去できる端末の、業務上の必要性に基づく限定

・個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に１回または複数回上書きする。）

・個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）

ウ．作業担当者の識別、認証、権限付与

・個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定

・ID とパスワードによる認証、生体認証等による作業担当者の識別

・作業担当者に付与する権限の限定

・個人データの消去・廃棄を行う作業担当者に付与した権限の記録

エ．作業担当者及びその権限の確認

・手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認

・アクセスの記録、保管、権限外作業の有無の確認

1．4 個人情報漏えい事故状況と傾向

（１）概要と前提条件

個人情報漏えい事故（以下、事故という）が依然として減少傾向にないのは、一体、何処に原因があるのだろうか。　事故の大半が人的過失によるものが原因とされている。

事故を起こした本人自身の責任は当然のことではあるが、その根本的な原因は、激しい市場の変化に組織や職場環境が旧態依然のままで実態と合っていないのかもしれない。　事故状況から何か気付く事が発見できるのではと期待しつつ調査した。

今回の個人情報漏えい事故の情報収集元は、「Security-NEXT ニュース」が掲載している個人情報漏えい事故の記事から集計したものである。

・個人情報漏えい事故件数の収集は、2007 年 1 月 1 日～2009 年 12 月 31 日とした。

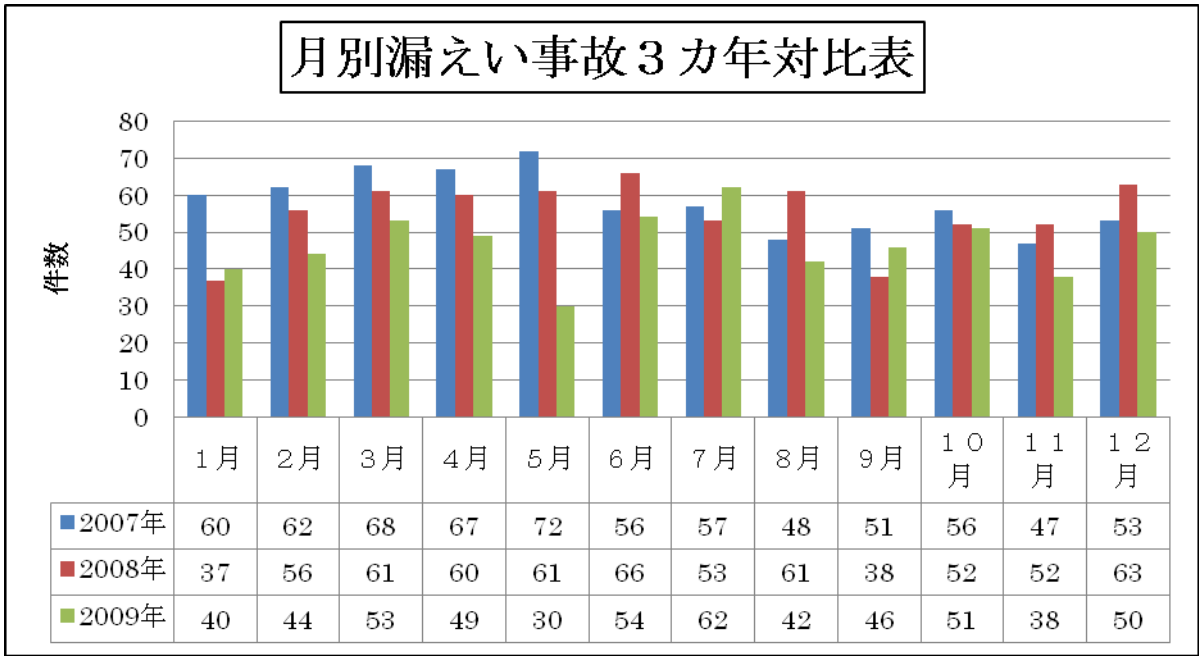
・年間の区切りを 1 月 1 日～12 月 31 日とした。

（２）個人情報漏えい事故状況

2007 年の総事故件数 697 件、2008 年の総事故件数 660 件、2009 年の総事故件数 559 件の結果となった。　データ上では、減少している結果となったが、経済産業省の事故報告件数では増加傾向となっている。　Web に掲載される記事はあくまでも話題性のあることを考慮しなければならない。　したがって、記事になり得る事故は減少しているが、軽微な事故等（記事にならない事故）の増加によって、全体的には増加傾向にあると判断できる。

2007 年、2008 年 2009 年の 3 カ年を月別に事故件数を以下の図 1 に示し確認をした。

事故発生の傾向が時期的なものと関連があるか期待した。



	１月	２月	３月	４月	５月	６月	７月	８月	９月	１０月	１１月	１２月
2007年	60	62	68	67	72	56	57	48	51	56	47	53
2008年	37	56	61	60	61	66	53	61	38	52	52	63
2009年	40	44	53	49	30	54	62	42	46	51	38	50

図 1

確認の結果、事故発生の傾向は、年度末時期や催事時期などに影響されるものではないと判断した。

①2009 年の事故状況をグラフ化したので以下に示す。

図２及び表３で示す通り、官公庁関連が 31%、金融関連が 12%、教育関連が 10%となり全体で 53%を占めていた。

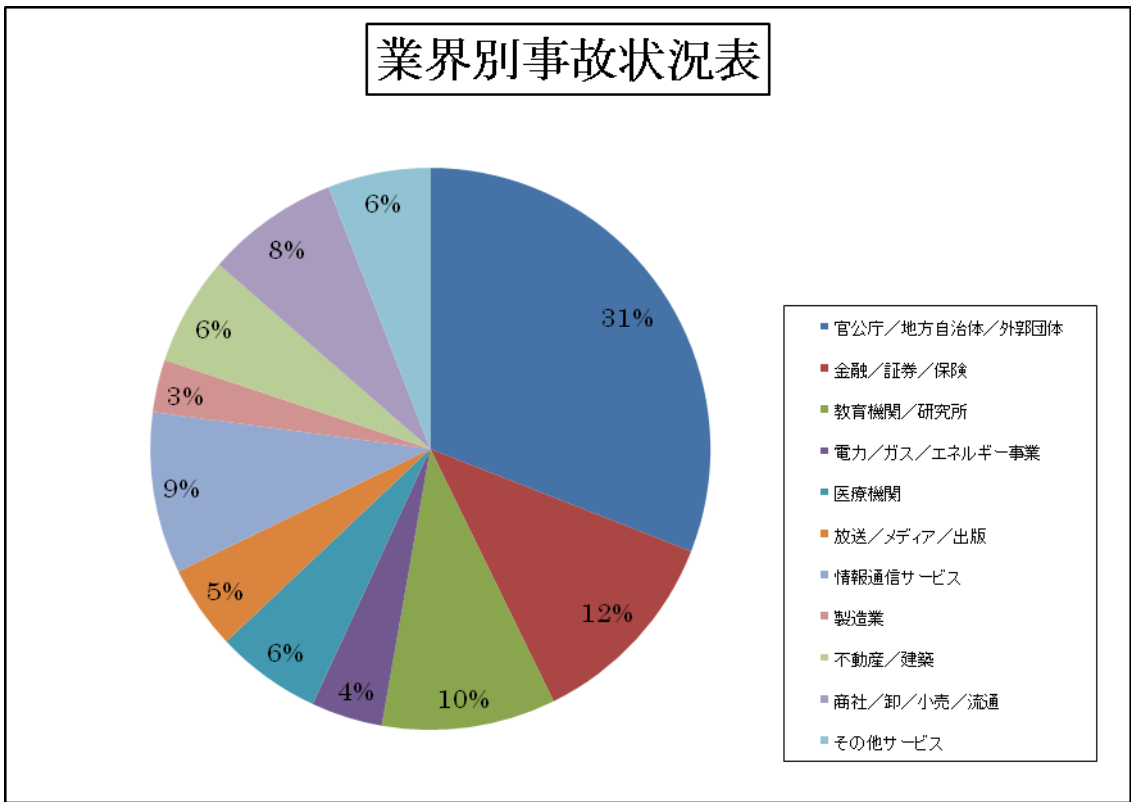


図２↑　　表３↓

業界区分	件数
官公庁／地方自治体／外郭団体	173
金融／証券／保険	66
教育機関／研究所	56
電力／ガス／エネルギー事業	23
医療機関	34
放送／メディア／出版	27
情報通信サービス	52
製造業	17
不動産／建築	35
商社／卸／小売／流通	43
その他サービス	33

②事故区分別での結果は、図３、表４に示す通り、盗難、紛失、誤配信／誤配送で全体 85%を占めている。

紛失事故では、「誤廃棄」の報告が目立っていた。

調査でのトピックスとして、「個人情報の拾得者が紛失企業に対して恐喝する事件」が起こっている。

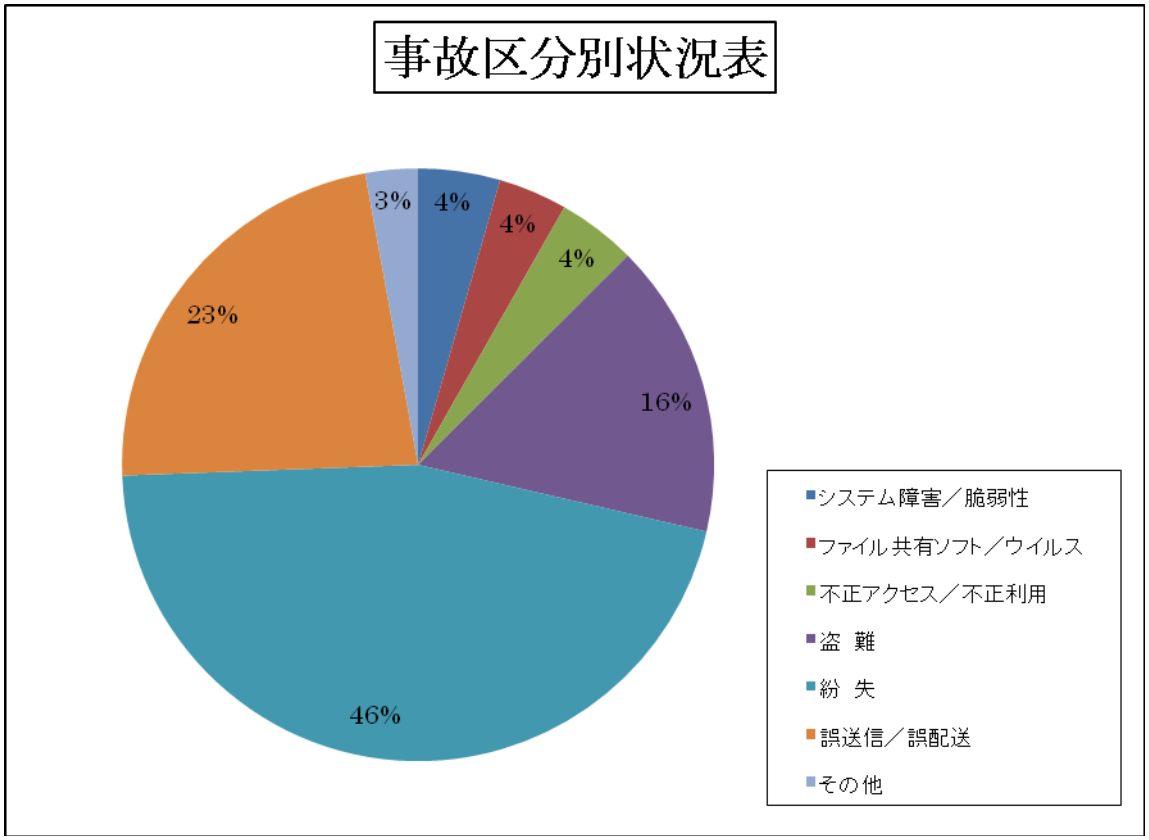


図３

事故区分	件数
システム障害／脆弱性	25
ファイル共有ソフト／ウイルス	21
不正アクセス／不正利用	24
盗　難	90
紛　失	256
誤送信／誤配送	127
その他	16

表４

③事故が発生した場所について確認した。事故全体では、事務所での事故が 66%の結果となった。(図４、表５参照)　一方、盗難事故における発生場所を確認すると個人宅 20%、通勤／帰宅時 10%、その他（途中立ち寄り）21%で就業時間外での発生が 51%であると判断できる。(図５、表４参照)

やむを得ず、個人情報を携帯することになったであろうが、途中、飲食店や娯楽場への立寄りは、本人の意識で改善できるものと考える。

また、立ち寄り事の事故は、車上荒らしによる盗難が非常に多い結果となっている。

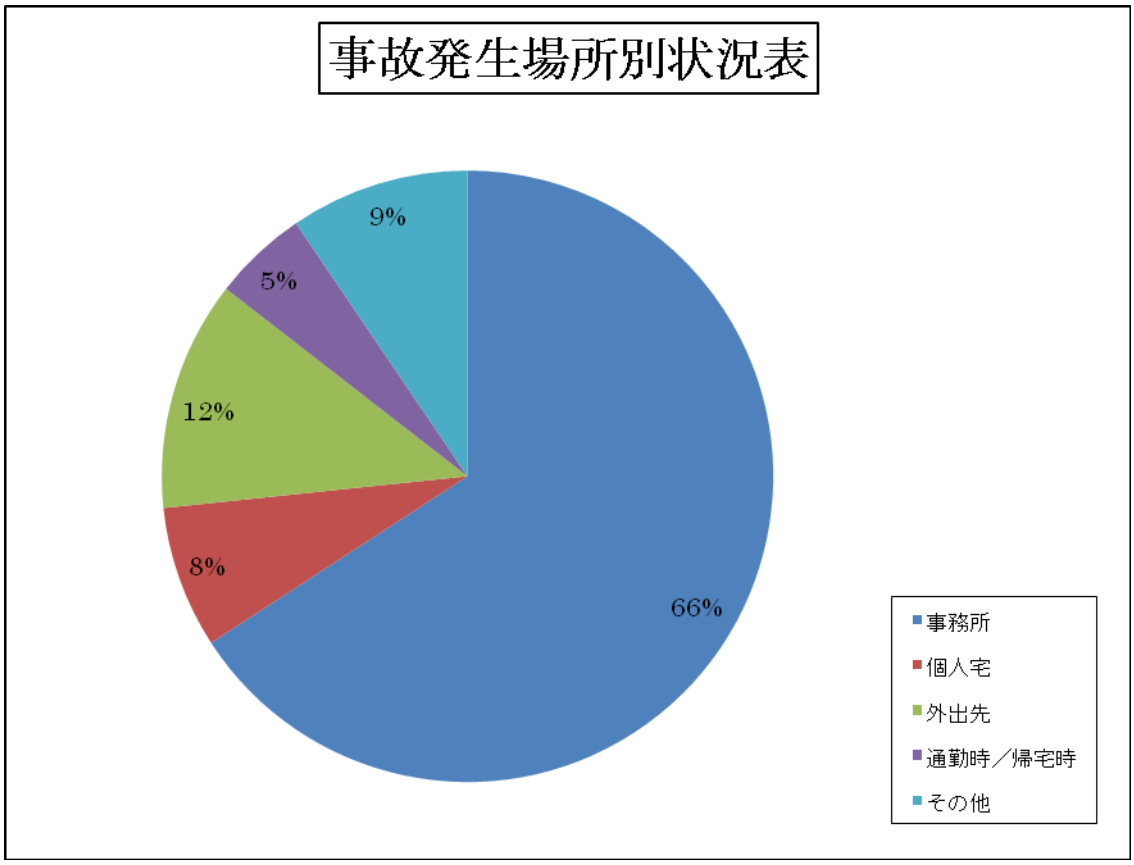


図４

事故発生場所区分	件数
事務所	368
個人宅	42
外出先	68
通勤時／帰宅時	28
その他	53

表５

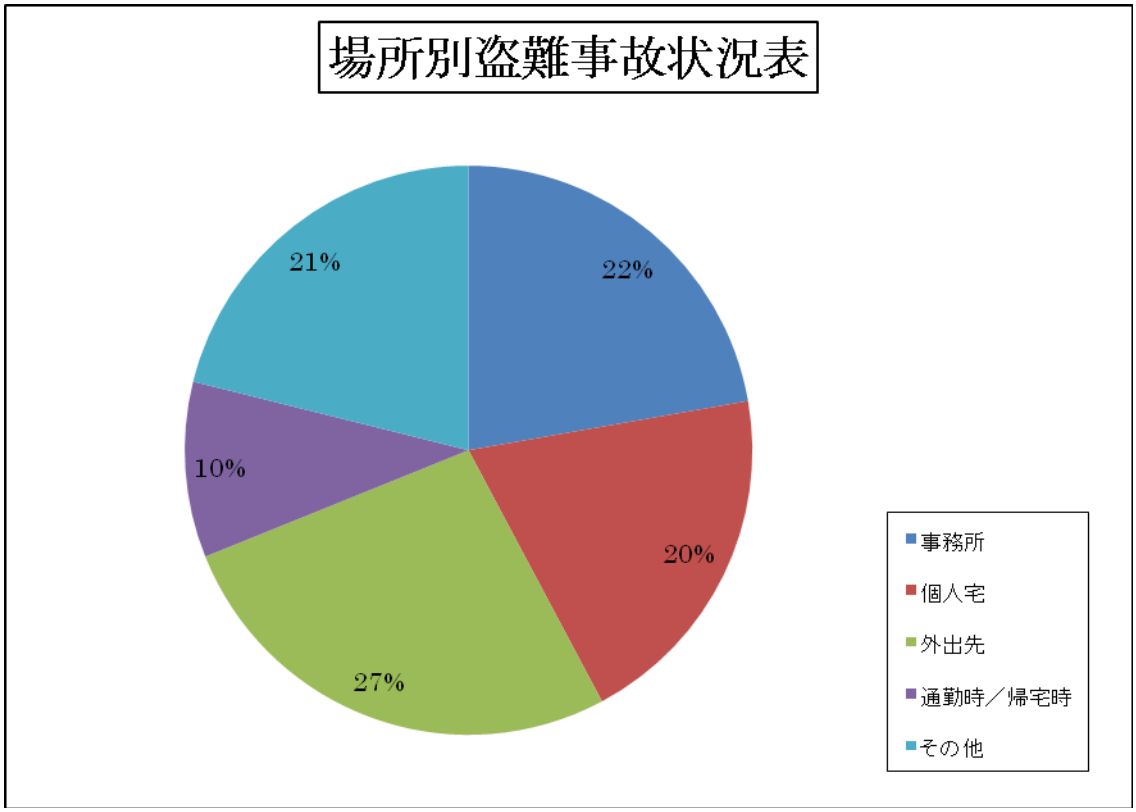


図５

事故発生場所区分	件数
事務所	20
個人宅	18
外出先	24
通勤時／帰宅時	9
その他	19

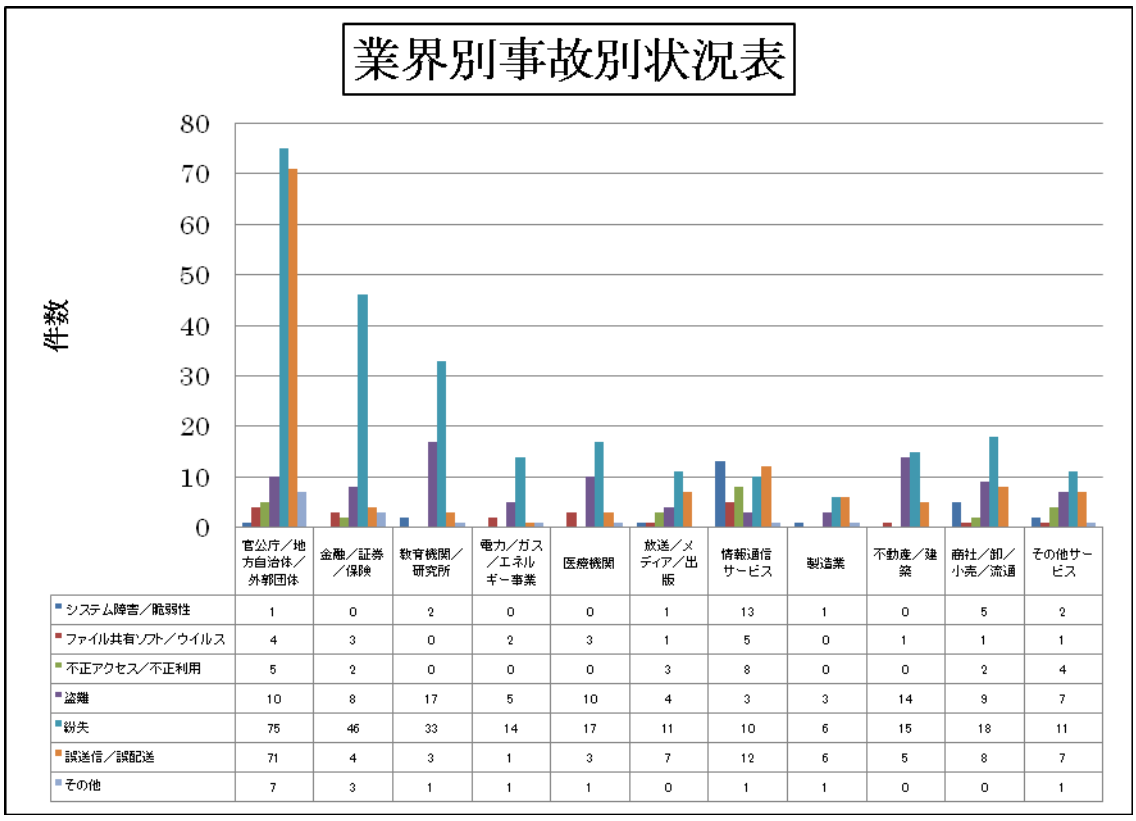
表６

④業界別事故区分別の状況を図６に示す。

紛失事故では、官公庁関連 29%、金融関連 18%、教育機関 13%の 3 業界で 60%となる。

誤配信／誤配送では、官公庁関連 56%、情報通信サービス 9%の 2 業界で 65%となる。

事故の内容では、紛失は「誤廃棄」、誤配信は「mail アドレスが他の人に閲覧可能状態で配信された」、誤配送は「宛名ラベルの間違いによる二重のラベルが貼られた事故」等が多く報告されていた。



	官公庁／地方自治体／外郭団体	金融／証券／保険	教育機関／研究所	電力／ガス／エネルギー事業	医療機関	放送／メディア／出版	情報通信サービス	製造業	不動産／建築	商社／卸／小売／流通	その他サービス
システム障害／脆弱性	1	0	2	0	0	1	13	1	0	5	2
ファイル共有ソフト／ウイルス	4	3	0	2	3	1	5	0	1	1	1
不正アクセス／不正利用	5	2	0	0	0	3	8	0	0	2	4
盗難	10	8	17	5	10	4	3	3	14	9	7
紛失	75	46	33	14	17	11	10	6	15	18	11
誤送信／誤配送	71	4	3	1	3	7	12	6	5	8	7
その他	7	3	1	1	1	0	1	1	0	0	1

図６

⑤盗難事故と紛失事故の媒体区分を確認した。（図７、表７参照）

当然ながら、書類関係が 59%を占めているが、つぎに USB が全体の 15%となっている。紙媒体を除く電子媒体類の情報セキュリティ対策状況も気になるので確認した。

図８に示す通り、パソコンのセキュリティ対策状況は 40%が対策されていた。

以下、USB が 8%、その他電子媒体(CDR, DVD 等)が 45%、携帯電話／専用端末が 48%の結果となった。　携帯電話と専用端末を一つに纏めたため数値が低くなったが、例えば検針用端末機器など専用端末は 90%以上がセキュリティ対策を施されていたことを改めて報告しておく。

USB のセキュリティ対策状況が 8%の結果となったことには、脅威を感じる。

USB は、コンパクトで低価格、大容量と三拍子そろったメモリー機器であることからバックアップ媒体、移送用媒体などに広く利用されているのは周知の事である。

USB の手軽さは、利用増加に伴ってリスクも拡大傾向にあり事故件数も増加していた。セキュリティ対策状況が他の媒体と比べて低い値となっていることの原因を考える必要がある。　昨今では、セキュリティ機能付 USB が市場にあること、反面、景品や粗品として単純なものなども多く流通していること、利用者が保存、コピー等の対象となる情報の重要度に応じて、これらの USB を必要に応じて正しく使い分けを行うことが重要である。

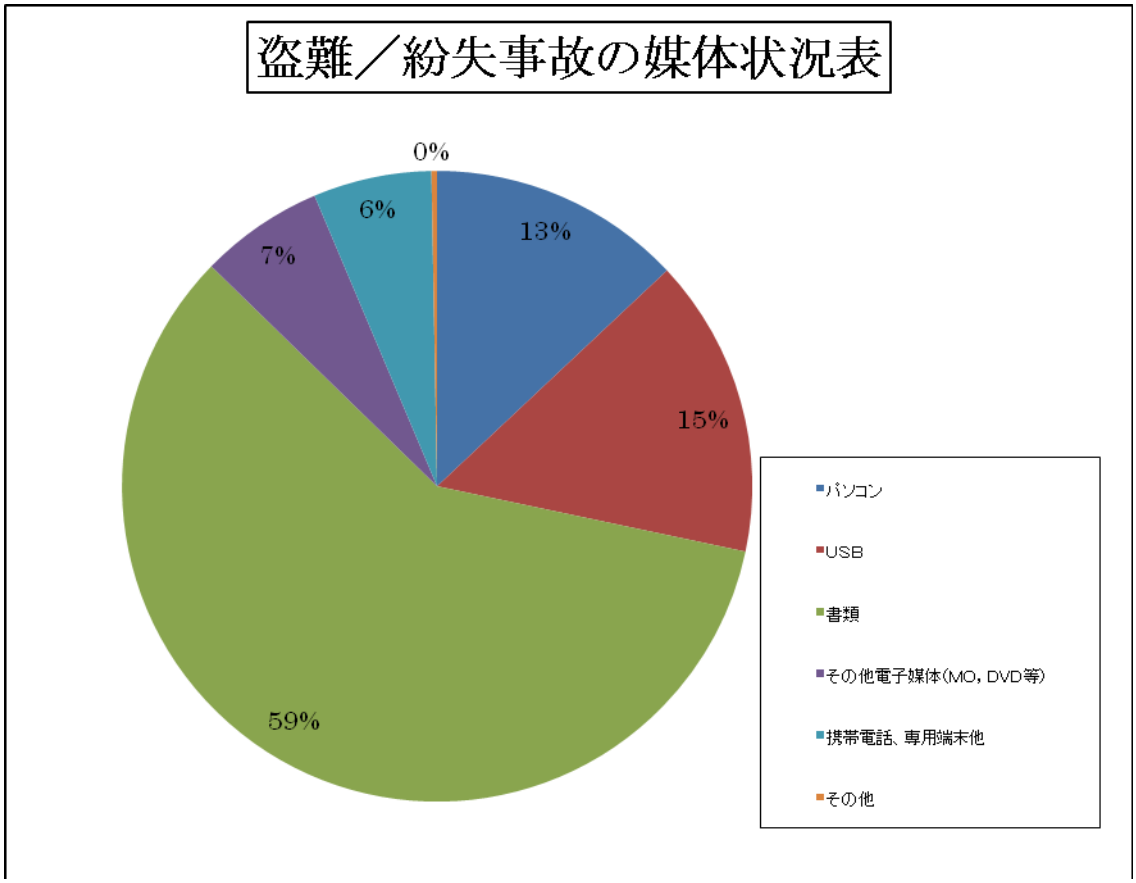


図７

媒体区分	件数
パソコン	45
ＵＳＢ	53
書類	204
その他電子媒体（ＭＯ，ＤＶＤ等）	22
携帯電話、専用端末他	21
その他	1

表７

移送や保存などに、過去主流として利用されてきた「MO、CDR、DVD 等」が、いまや USB に移行してきたことが分かる。　又、デジカメや音楽収録などで広く利用されてきた SD カードなども従来の電子媒体に代わって利用されるのではないだろうか。したがって、SD カードなどは、さらにコンパクトで大容量になるが、未だ、セキュリティ機能など装備されていないため、取扱には十分留意することが必要である。

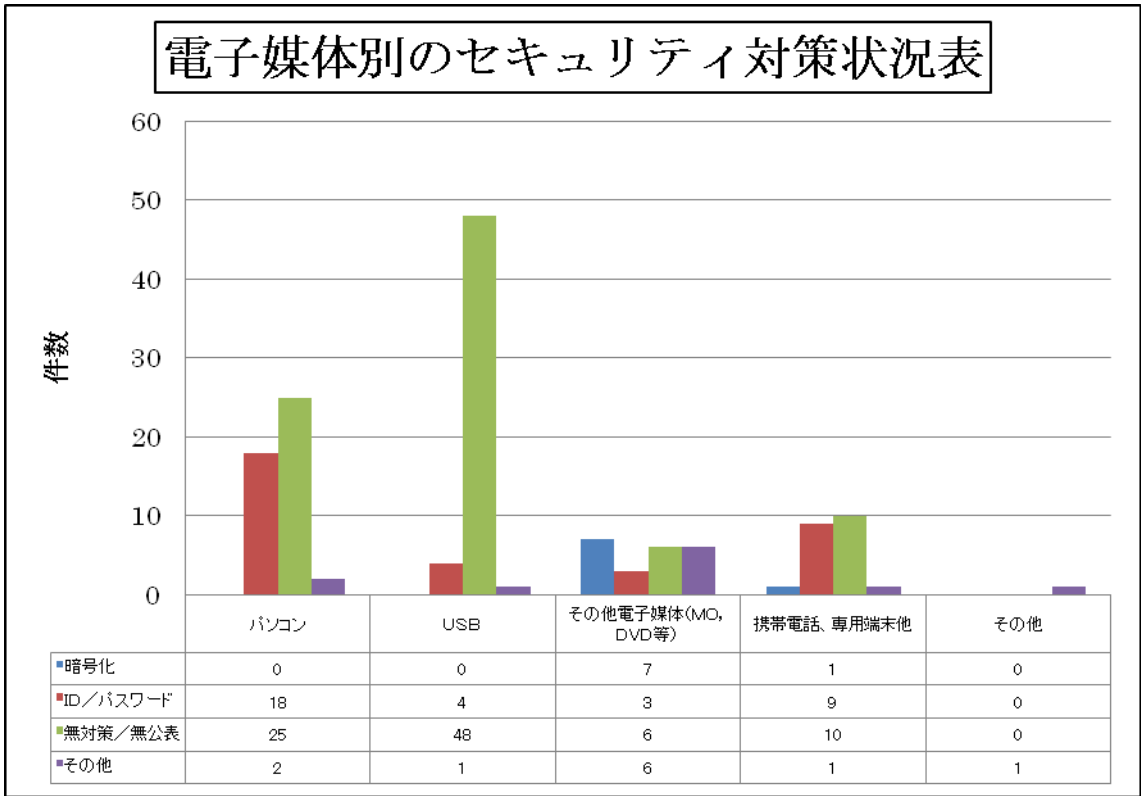


図８

⑥不正アクセス／不正利用について報告をする。（図９参照）

不正アクセス／不正利用による流出件数を確認したところ、10 万件以上の事故が 4 件発生したことが分かる。この 4 件の内訳は、内部からの流出が 3 件、外部からの流出が 1 件である。　内外何れもマスコミに大きく取り上げられた事故であった。

不正アクセス／不正利用の内部からの大量流出事故は増加傾向にあると言える。（図 10 参照）

本調査では、原因の追及まで至らなかったが多くは、個人の金銭的な原因で不正に持ち出したと報告されていた。

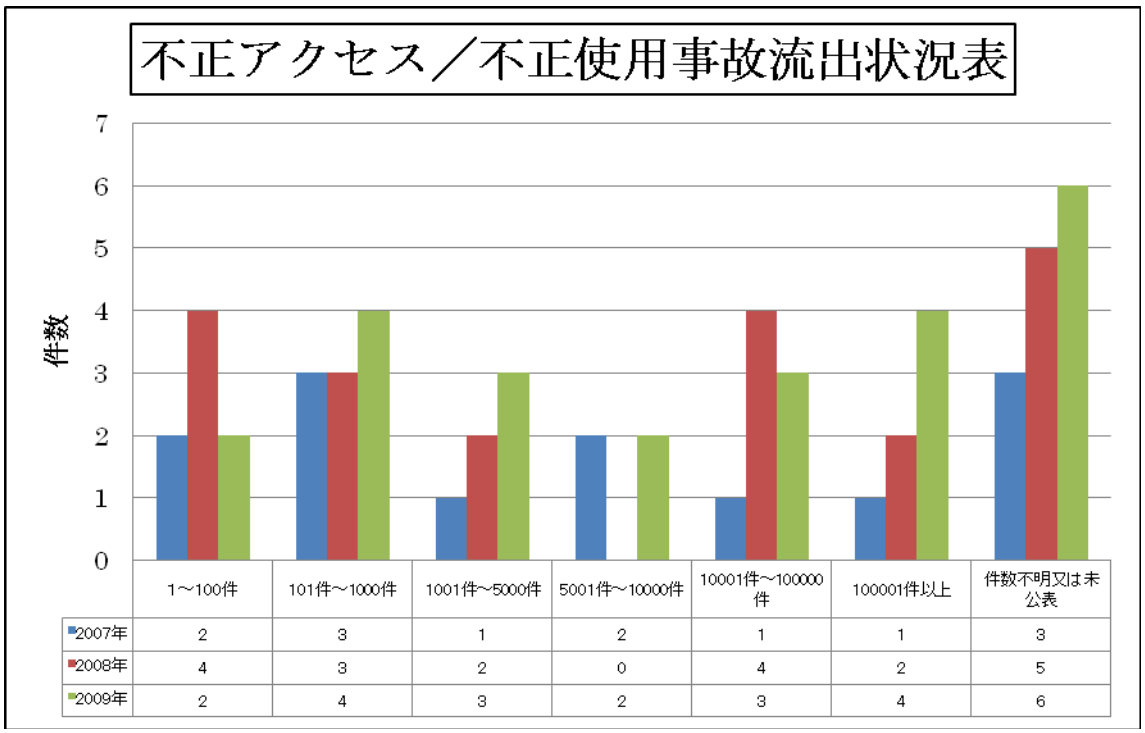

不正アクセス／不正使用事故流出状況表
件数
7
6
5
4
3
2
1
0
1～100件
101件～1000件
1001件～5000件
5001件～10000件
10001件～100000件
100001件以上
件数不明又は未公表
2007年 2 3 1 2 1 1 3
2008年 4 3 2 0 4 2 5
2009年 2 4 3 2 3 4 6

図 9

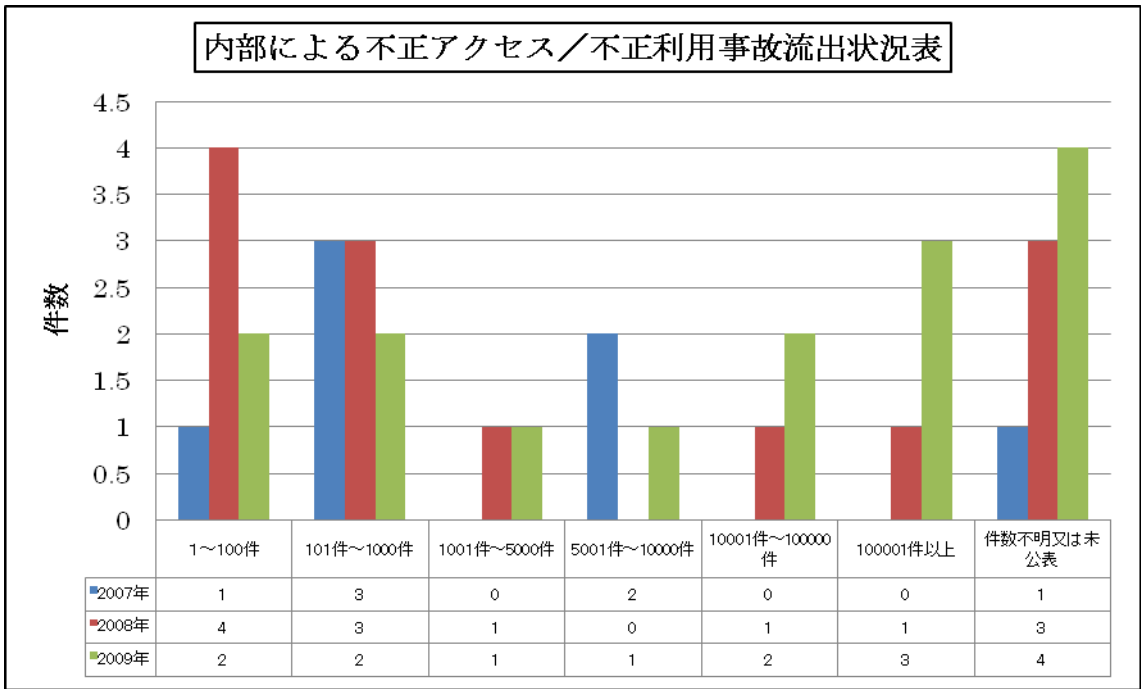

内部による不正アクセス／不正利用事故流出状況表
件数
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
1～100件
101件～1000件
1001件～5000件
5001件～10000件
10001件～100000件
100001件以上
件数不明又は未公表
2007年 1 3 0 2 0 0 1
2008年 4 3 1 0 1 1 3
2009年 2 2 1 1 2 3 4

図 10

⑦不正アクセス／不正利用の大量流出事故の事案紹介

図９に示す４件の大量流出事故を以下個別に報告する。

a 外部からの流出事故

・芸能プロダクション「アミューズ」の通信販売サイト「アスマート」から、カード情報を含む個人情報が流出した。　14 万件
2009 年 7 月 28 日にクレジット会社より流出の可能性を指摘され、問題が判明。
情報漏えいによってクレジットカードの不正利用も確認されている。
（出典：http://www.security-next.com）

b 内部からの流出事故

・陸上自衛隊の隊員や家族に関する個人情報が自衛官によって外部へ流出した。
金銭目的で売却　　14 万件

・三菱ＵＦＪ証券の元社員が、約 148 万件の個人情報を持ち出し、最新の顧客情報 4 万 9159 人分を名簿業者 3 社に 32 万円で売却した。　又、同社は、約 5 万人の顧客に対して、1 万円程度の商品券を配ることを公表した。（約 5 億円の出費）
（出典：http://www.security-next.com）

提言：今回の事案で約 5 万件の個人情報を買い取った名簿業者に対する措置が公表されていない。この様な場合、大量の個人情報がどの様な性質のものか不正利用ではないか疑わしいと思ったはずである。もし、善意に解釈するならばその情報の出所の確認をするはずである。　関係所轄によって名簿業者に対して、調査、指導がなされたと判断するがマスコミ関連の記事では、確認できなかった。　したがって、個人情報を購入した企業の調査、指導内容および企業名を公表することによって、今後、不正な情報の売買や不正利用の抑制に資すると考える。　保護法第１７条「個人情報取扱事業者は、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」としており、「不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合」は不正の手段による個人情報の取得になる。なお、不正の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、不正に取得したり、不正に使用・開示した場合には不正競争防止法第２１条、第２２条により刑事罰が科され得る。以上のことがらを鑑み、買い取り事業者に対する公表の早期実現を望む。

・アリコジャパンは、平成 21 年 7 月に顧客の個人情報が流出したと公表した。
システム開発を委託した中国にある企業の社員が、不正に引き出した可能性が高い。
最大 23 万件の流出の可能性があり、不正利用の被害が 5122 件でている。

中国の捜査当局とも連絡を取り始めた。
しかし、未だ漏えいした個人顧客情報の具体的範囲および実行者の最終的な特定には至っていない
金融庁は、アリコジャパンに対して平成 22 年 2 月 24 日付けで保険業法第 204 条第 1 項に基づき業務改善命令を発出するとともに、個人情報保護法第 34 条第 1 項に基づく勧告を行った。(平成 22 年 3 月 24 日までに書面で報告)
アリコジャパンは再発防止策や顧客情報保護体制の構築、さらに日本における代表者と役員の報酬返上などが盛り込まれている業務改善報告書を金融庁に提出した。(平成 22 年 3 月 24 日提出)
(出典：http://www.security-next.com)

提言：この漏えい事故は、国際犯罪で捜査が進まない。

委託先担当者がホストコンピュータへのＩＤ、パスワードを使い回していたため、実行者の特定が困難な状態であることが一番の問題である。

実行が中国企業であり、ホストコンピュータは米国にあることから、中国から直接米国ホストコンピュータにアクセスし不正行為が日本を経由せずに実行されたことである「被害者は国内にいるのに流出源に手が出せない」状況である。

個人情報の越境移転に関する国際的な保護基準および国際犯罪協力など含め、個人情報保護法の見直しが急務である。

⑧個人情報の漏えい事故が想定されるリスク

a 個人情報のリスクを再確認する。

・個人情報の取得時における脅威

・個人情報の利用、加工時での脅威

・個人情報の保管時における脅威

・個人情報の移送時での脅威

・個人情報の廃棄・焼却における脅威

収集、利用、保管、移送、廃棄などの局面ごとのリスクを分析し適切な対策を施す。

下記、図 11 に代表的な局面でのリスクを表した。

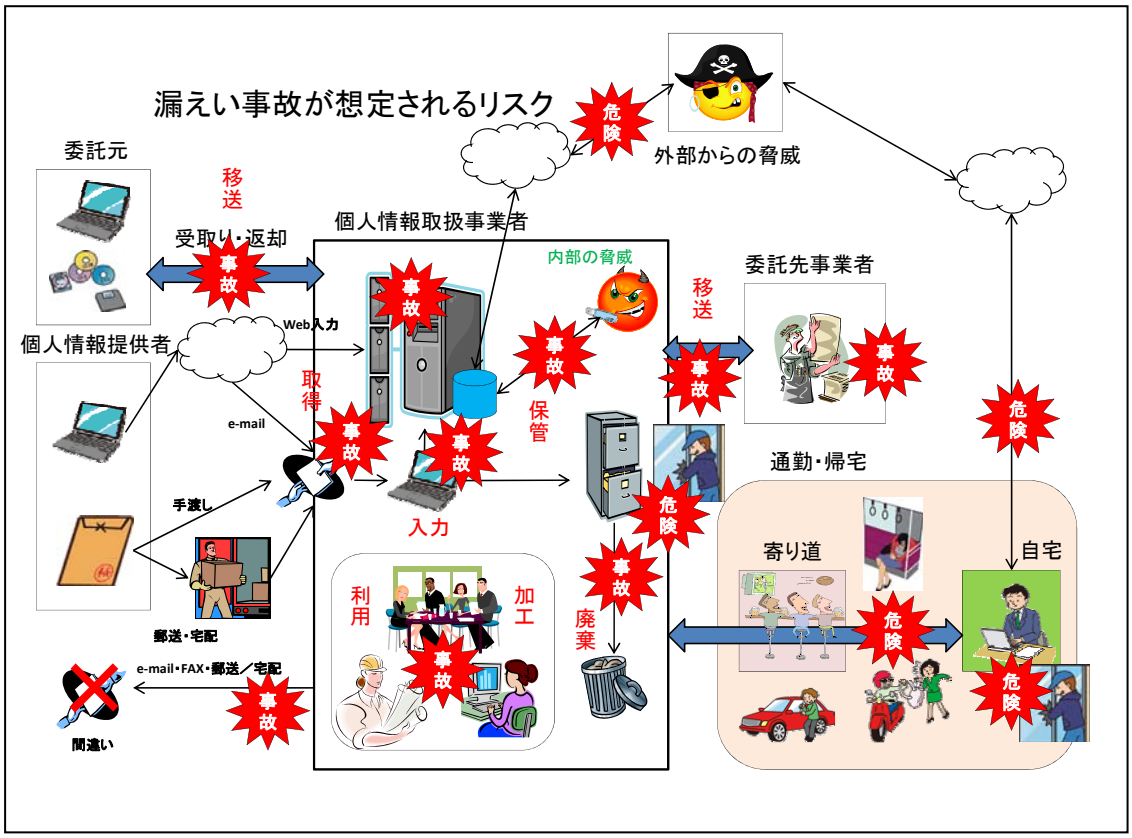


図 11

⑨漏えい事故要因の検討

― 事故が起こる根本的な要因はなにか？ ―

a 担当者の要因

・事故による社会的な影響の認識が希薄

・自分は大丈夫という慢心

・いちいちルールを守っていると仕事ができないという自己都合判断

・仕事の段取りが悪く自己管理ができない

b 社内環境の確認事項を検討
・業務手順と実務が合っていないのではないか（社内の規程が遵守されない）
・業務の負荷が担当者に偏っていないか（操作ミス）
・タイトなスケジュールで結果を要求していないか（自宅での作業）
・社員が会社や上司、同僚などに不満を持っていないか（不正持ち出し）

⑩個人情報をやむを得ず持ち出すとき注意事項
a 担当者は極力、個人情報を持ち出さないで済む工夫を心掛けることが重要
b やむを得ず、個人情報を持ち出すときは、管理者の承認を得ることが重要
c 個人情報の持ち出すときの工夫を考える「一手間を惜しまない」
・電子情報の場合は暗号化やパスワード設定等を行う（盗難、紛失時における USB のセキュリティ対策状況は 8%である）
・量は最小限にとどめる
・紙はできるだけ避けること
・帰宅途中に他の場所に立ち寄らないように心掛ける(盗難時の現場では、他の場所が 21%である)

⑪不正アクセス／不正利用の防止について
特に内部からの流出を予防することは困難ではあるが、検討する必要がある。
・不要なファイルコピーなどの行為に対する監視の検討
・重要なデータのプリント、コピーなどの制御について検討

尚、第４１回ＥＣＯＭセミナーにおいて「最新の個人情報漏えい事故状況と傾向」と題して報告した資料を巻末に添付する。

1.5 海外における個人情報漏えい事故の紹介

海外では、情報漏えい事故としてまとめられているため、個々の情報漏えい事故の中から個人情報が含まれているか特定するのが難しい。　その中から、注目する事故を１つ発見したので紹介する。

『厳格な秘密保持で知られるスイスの銀行の顧客情報約 1500 人分が持ち出され、ドイツ当局に約 250 万ユーロ（約 3 億円）で買い取りの打診があった。　メルケル独首相は「重要な内容なら、データ買い取りに尽くすべきだ」と発言したため、スイス国内に衝撃が走っている。　情報取得の合法性が議論されているが、脱税に関するものも含まれており、「約 1 億ユーロ（約 125 億円）の追徴課税が期待できる」との見方がでている。　ショイブレ財務相は、「原則的には買い取る」との方針を示した。』（参考：asahi.com）　　この事件の結末は、非常に興味深い内容なので継続して調査することとする。

この事件で、「ドイツ当局が情報を買い取った場合」のことを想定した時、ＥＵプライバシーコミッショナーがどの様な対応をとるのかが注目のポイントである、また、政府にとって付加価値があれば、「取得の合法性」如何は問わず「買い取ってくれる」と言うことになれば、金銭目的で同様の事件が多発する恐れがでてくるのではと危惧する。

わが国の「保護法」や「経済産業分野に関するガイドライン」および「ＥＣＯＭガイドライン」に照らし合わせると、金銭のやり取り関係なしに、**「不正な取得」**になる。　また、無理やりだが**「法令に基づく場合」**と解釈することも考えられるが、いずれにしろ情報源は**「疑わしい情報」**と結論付けられる。

2. 個人情報保護に関する国際動向

2.1 EUの個人情報保護の動向

2009年11月に第31回データ保護 プライバシー・コミッショナー国際会議が実施された。

日　程　　2009年11月4日（水）～11月6日（金）
場　所　　スペイン・マドリッド
概　要　　プログラム構成

	セッション	テーマ
1日目 11月4日（水）	オープニング	オープニング・セレモニー
	第1セッション	監視下の社会
	第2セッション	あなたはどこにいるのですか？
2日目 11月5日（木）	第3セッション	プライバシーと企業責任
	第4セッション	児童のプライバシー保護
	クローズ・セッション	コミッショナーのみ参加
3日目 11月6日（金）	第5セッション	計画されたプライバシー
	第6セッション	プライバシーのグロパル規制

今回の会議では、開催国スペイン（スペインデータ保護監督庁）より「個人データ処理に関するプライバシー保護の国際規格」（草案）が提案された。

この草案の作成は、スペインを含む24機関の共同作業で行われた。（アジア域：香港、ニュージーランド）　ＥＵ保護指令が1995年に公示され、ＥＵ構成国は、それぞれの国において対応してきたが、各国の個人情報保護の整備レベルが均質化できていた訳ではなかった。そのため、「個人データ処理に関するプライバシー保護の国際規格」を策定しプライバシー保護を保証する基準を設ける方針が提案され、各国は、概ね賛同を示した。
以下、表8に「個人データ処理に関するプライバシー保護の国際規格」の構成を示す。

区分	原則等	区分	原則等
第 1 章	第 1 条　目的	第 4 章 データ主体の権利	第 16 条　アクセス権
	第 2 条　定義		第 17 条　修正及び削除の権利
	第 3 条　適用範囲		
	第 4 条　追加措置		第 18 条　異議申立権
	第 5 条　制限		第 19 条　当該権利の行使
第 2 章 基本原則	第 6 条　合法性および公平性の原則	第 5 章 セキュリティ	第 20 条　セキュリティ対策
			第 21 条　守秘義務
	第 7 条　目的明示の原則		
	第 8 条　比例の原則	第 6 章 コンプライアンス及びモニタリング	第 22 条　事前対策
	第 9 条　データ品質の原則		第 23 条　モニタリング
	第 10 条　公開の原則		第 24 条　協力及び協調
	第 11 条　責任の原則		第 25 条　責任
第 3 章 処理の正当性	第 12 条　正当性の一般原則		
	第 13 条　センシティブ・データ		
	第 14 条　処理サービスの提供		
	第 15 条　国際移転		

表８

「個人データ処理に関するプライバシー保護の国際規格」は、構成案ができただけで中身はできていない。　これから、構成に基づいて詳細内容を詰めて行く状況である。

2.2 APECの個人情報保護の動向

（1）2009年7月に第20回のＡＰＥＣ電子商取引運営グループ（ＥＣＳＧ）が主催する個人情報越境移転ルール（ＣＢＰＲ）策定に関するセミナー及び会議が開催された。

日　程　　2009年7月25日（土）～7月30日（木）
場　所　　シンガポール
概　要　　プログラム構成

日　程	テーマ
1日目　7月25日（土）	パスファインダー・プロジェクトの非公式会議
2日目　7月26日（日）	デジタル繁栄チェックリスト会議
3日目　7月27日（月）	データ・プライバシー・サブグループ・セミナー
4日目　7月28日（火）	データ・プライバシー・サブグループ会議
5日目　7月29日（水）	ペーパーレス貿易サブグループ会議
6日目　7月30日（木）	プレナリ会議

2008年2月から開始されたパスファインダー・プロジェクトのプロジェクト１（企業の自己査定）及びプロジェクト３（認証機関の企業審査）の実証実験であるプロジェクト９（パイロットテスト）に参加した企業、第三者認証機関（ＡＡ）からの検証報告を取りまとめた結果と今後の方針について、リーダーの米国（商務省）より報告があった。
プロジェクト９（パイロットテスト）に参加した国、企業数、第三者認証機関を以下の表９に示す。

国	参加企業	第三者認証機関
日本	１社	ＪＩＰＤＥＣ
米国	７社	ＴＲＵＳＴｅ
ベトナム	３社	Trustvn
カナダ	１社	オブザーバー
豪州		オブザーバー

表９

プロジェクト９での検証課題が以下の通り報告された。 尚、わが国からの指摘事項は、ほぼ全て掲載されている。
①ポリシー確認調査のプロセスでは、手順の確認には不十分である。（インタビューや現地審査、Web技術の検証等が必要である）
②範囲や適用の明確化が必要である。

③ＡＰＥＣプライバシーフレームワークと国内法の関連の明確化が必要である。
④プロジェクト１の設問に重複がある。
⑤プロジェクト１とプロジェクト３の設問に重複がある。
⑥プロジェクト１の設問に不必要な、又はフレキシブルでないものがある。
⑦用語集が必要である。
⑧認証取引プロセスが必要である。
⑨設問内容の改善が必要である。
⑩新たに要件設定するよりも、現存の規程を活用すべきである。
　又、討議の中で新たに⑪が追加された。
⑪中小企業向けの自己審査設問を策定すべきである。

　パスファインダー・プロジェクトの今後の方針について以下の通り承認された。
①企業向けにプライバシーポリシー策定と業務遂行をサポートするガイダンスを策定する。
②ＣＢＰＲと同様な既存トラストマーク（Ｐマーク等）との要件比較表を策定する。
③ＡＡ認証ドラフティングコミッティの組成。
④サービスプロバイダーや個人情報プロセッサー向けの認証プロセスを策定する。
⑤今回のパイロットテスト参加者のコメント検討を開始する。
⑥工程表を策定する。

（２）2010 年 2 月に第 21 回のＡＰＥＣ電子商取引運営グループ（ＥＣＳＧ）が主催する個人情報越境移転ルール（ＣＢＰＲ）策定に関するセミナー及び会議が開催された。

日　程　　2010 年 2 月 26 日（金）～3 月 3 日（水）
場　所　　日本／広島
概　要　　プログラム構成

日　程	テーマ
1 日目　2 月 26 日（金）	データ・プライバシー・サブグループ非公式会議
2 日目　2 月 27 日（土）	データ・プライバシー・サブグループセミナー
3 日目　2 月 28 日（日）	データ・プライバシー・サブグループ会議
4 日目　3 月 1 日（月）	グローバル・バリューチェーン・ジョイントセミナー
5 日目　3 月 2 日（火）	ペーパーレス貿易・サブグループ会議
6 日目　3 月 3 日（水）	プレナリ会議

　28 日にデータ・プライバシー・サブグループ会議が以下のテーマで議論された。
①2 月 27 日開催のセミナー報告
②パスファインダープロジェクトに関する議論

③ＡＰＥＣプロジェクトに関する議論（2010 年実施提案プロジェクトのスケジュール等）
④ＤＰＳ活動計画の見直し（現行のＤＰＳ活動計画に関する議論）
⑤サブグループメンバーからの報告
⑥越境プライバシーイシューに関する情報共有
⑦データ・プライバシー・フレームワークの国内実施
⑧まとめおよびＤＰＳの今後の活動

第 20 回会議での報告にあったプロジェクト９でのパイロットテストでの指摘に基づいてプロジェクト１ドラフト文書（自己審査）とプロジェクト３ドラフト文書（認証機関審査）の改定が行われ本会議にて一部内容を除いてプロジェクト１改訂文書の最終案が承認された。残された一部内容は電話会議にて検討することとなった。

プロジェクトＮｏ	プロジェクト状況／参加国（太字はリーダー国）
プロジェクト１	完了（一部詳細詰めの作業あり）
プロジェクト２（民間）	完了
プロジェクト２（公共）	**カナダ**、豪州、ニュジーランド、米国、ＩＣＣ
プロジェクト３	**メキシコ**、豪州、カナダ、日本、フィリピン、台湾、米国、ベトナム
プロジェクト４	**豪州**、米国、ＩＣＣ
プロジェクト５～７	完了
プロジェクト８	**豪州**、カナダ、日本、韓国、ニュージーランド、米国 オブザーバー：香港、フィリピン、ベトナム
プロジェクト９	パイロットテスト：完了、プロジェクト運用：一時中断

（３）今後の開催日程・開催地
第 22 回　ＡＰＥＣ／ＥＣＳＧ会議
日程　　：　2010 年 9 月 15 日（水）～9 月 26 日（日）この期間内の 1 週間となる予定
開催地　：　日本／仙台
第 23 回、第 24 回　ＡＰＥＣ／ＥＣＳＧ会議
日程　　：　2011 年 2 月および 9 月を予定
開催地　：　米国／ハワイ

3. 個人情報の利活用に関する検討

大量の情報が瞬時に世界中を駆け巡るネットビジネス社会において、今後のビジネスが大きく変革しようとしている。　携帯電話の機能拡充や電子マネーの普及、電気自動車、家電・住宅設備機器など、ETC、自動改札機などがネットワークにつながることによって、従来の情報に加えて、消費者の行動情報も得ることができる時代となっている。

昨今、個人情報に関する保護への認識は十分浸透してきた反面、過剰反応によるビジネスの停滞も歪めない事実である。　個人情報や行動情報を積極的に活用することで、企業の新規ビジネスの創出、サービス提供による消費者の利便性向上が図れる。

ここでは、今後のビジネスの潮流ともいわれる「クラウドコンピューティングサービス」と「行動ターゲティング」について検討した。

3.1 クラウドコンピューティングサービスの進展と個人情報保護に関する検討

（1）クラウドコンピューティングの概要

クラウドコンピューティングサービス（以下、クラウドサービスという）の検討にあたってクラウドコンピューティングとは何かをもう一度、認識を合わせることとした。

①クラウドコンピューティングとは

クラウドとは、インターネットを図に表す時に雲（Cloud）の形を描いたことからインターネットそのものがコンピュータになるという考え方がクラウドコンピューティング（以下、クラウドという）である。

②クラウドサービスの形態

・IaaS（Infrastructure as a Service）

サーバーやストレージ、ネットワークを提供するサービス。（例：AmazonEC2）

・PaaS（Platform as a Service）

ＯＳやデータベースなどミドルウェアを提供するサービス。（例：Google App Engine）

・SaaS（Software as a Service）

アプリケーションを提供するサービス。（例：Salesforce CRM）

③クラウドサービスの種類

・「パブリッククラウド」

複数のユーザに同一のサービスを提供するクラウドをいう。

・「プライベートクラウド」

特定のユーザの要求に合わせて個別のクラウドサービスを提供するクラウドをいう。

④クラウドサービスの特徴

・高度な拡張性を有する

ユーザは、トランザクションピークに合わせて事前にコンピュータリソースを用意す

る必要はなく、クラウドは膨大なコンピュータリソースを有しているため、リソースが不足すれば自動的、もしくは簡単操作で容易に追加できる。

・抽象化されたコンピュータリソースである

情報処理に使われるコンピュータの機種やそのコンピュータの物理的な所在を意識しなくても良い。

・サービスとして提供される

ユーザは、実際に使用したリソース分だけの料金をサービスプロバイダーに支払う。

・初期投資なしですぐに利用開始が可能である

ユーザは、初期投資が不要ですぐに利用開始ができる。ただし、実際利用開始までにある程度の実用可能性の検証期間が必要である。

以上、簡単ではあるがクラウドサービスについて整理した。

概念図を以下に示す。（図 12 参照）

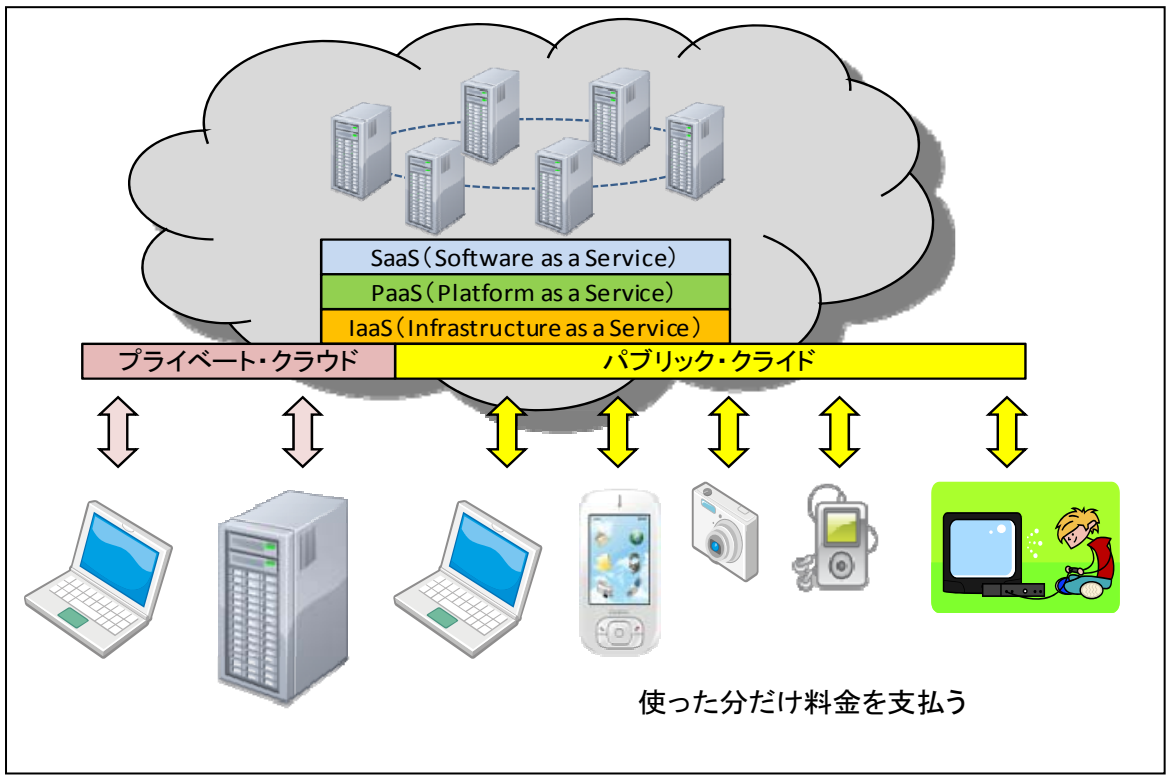


図 12　概念図

（２）SaaS（Software as a Service）利用状況

㈶日本情報処理開発協会が「企業ＩＴ利活用実態調査」（2009 年 3 月）において SaaS 導入状況について公表している。

①SaaS 導入状況の調査結果

・導入済みの企業が　21.4%
・検討中の企業が　9.9%
・導入予定なしの企業が　42.7%
・言葉も聞いたことが無い企業が　10.4%
・具体的な検討は行っていない企業が　15.7%

②SaaS や ASP を利用しないと回答した企業の理由を以下の図 13 に示す。
尚、回答企業数は 302 件、回答理由は複数回答とした。

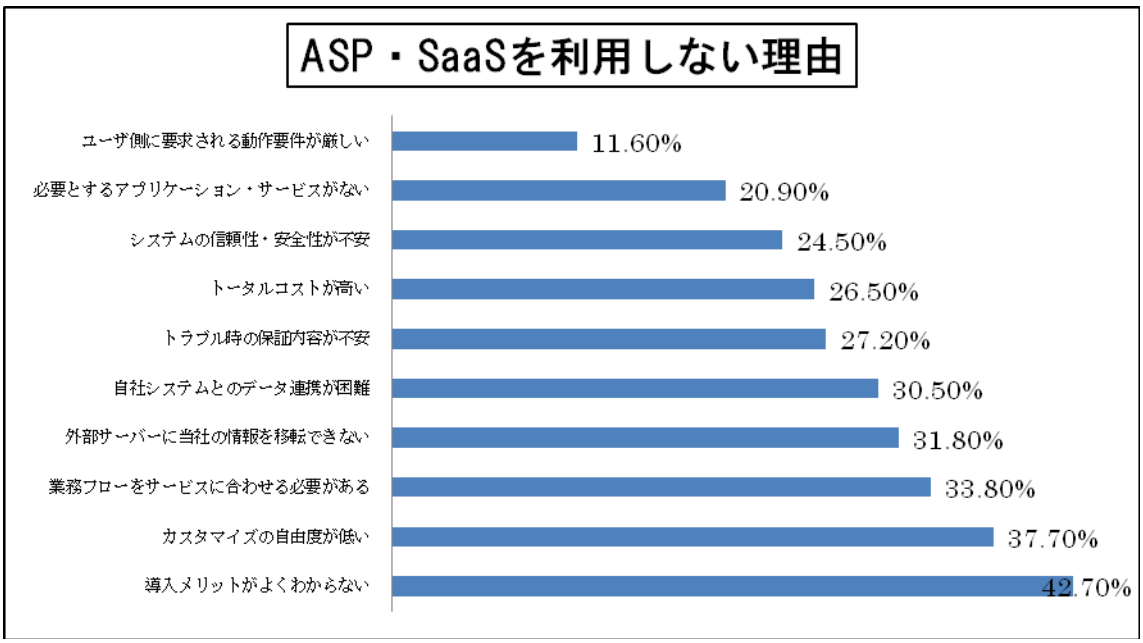


図 13

[N=302, 複数回答]

導入メリットがよくわからない	42.7%
カスタマイズの自由度が低い	37.7%
業務フローをサービスに合わせる必要がある	33.8%
外部サーバーに当社の情報を移転できない	31.8%
自社システムとのデータ連携が困難	30.5%
トラブル時の保証内容が不安	27.2%
トータルコストが高い	26.5%
システムの信頼性・安全性が不安	24.5%
必要とするアプリケーション・サービスがない	20.9%
ユーザ側に要求される動作要件が厳しい	11.6%

表 10

クラウドサービスは、まだ本格的な普及には至っていないが、消費者や企業が日々活用する情報通信サービスの量と蓄積するデータ量の加速的な増大は、クラウドサービスを利用することが否応なく迫ってくると考えられる。

（3）クラウドと個人情報

クラウドサービスにおける個人情報の保護について検討した。

①クラウドサービスの確立された定義が存在していない。

クラウドサービスにおける個人情報保護に関するガイドラインなどの策定が困難である。

ガイドラインが必要性であることの認識は一致している。

②クラウドサービスの情報(個人情報を含む)所在と責任

クラウドサービス事業者が管理責任を担う。　情報は物理的に分散される。

課題：クラウドサービスは分散処理が特徴であるため、リアルタイムで管理・確認ができるのだろうか又、しなくてはならないのか。

③安全・安心の保証

・システム運用に対する不安
・データの保存場所および保存方法に対する不安
・アクセス不能およびデータ遅延に対する不安
・稼働保証に対する不安
・データ喪失に対する不安
等

クラウドサービスを検討するにあたってユーザが持つ不安は同時に個人情報取扱いに対する不安と見なすことができる。

④クラウドサービス事業者は個人情報取扱事業者になるのか

データセンターや倉庫業者は、個人情報取扱事業者でいないと認められているが　クラウドサービス事業者はデータセンターと同様の扱いになるのか、

⑤一般消費者向けのクラウドサービスと企業向けクラウドサービス

a 消費者向けクラウドサービスが先行して普及するのではと予測する。

・安価もしくは無料で利用できる
・携帯電話などモバイル機器で高性能サーバーが利用できること
・ゲーム、音楽などが普及するアプリケーション・サービスとなること
等

b 企業は基幹システム以外の個別対応業務から普及するのではと予測する。

・初期導入費用がいらない
・利用決定から短時間で利用開始ができる
・重要な情報の取扱い以外の業務が中心となる
等

（4）検討の整理

・クラウドサービスは、分散処理技術や仮想化技術によってインターネット上の多数のサーバーが必要に応じて利用する仕組みを提供するため、個人情報が処理されている場所や個人情報が保管されている場所などといった「情報の所在」と「安全性の保証と証明」ができるのか、クラウドサービス事業者とサービスプロバイダー間での「安全性の保証と証明」ができるのか、情報が海外に越境移転する場合の国際的な「安全の保証と証明」ができるかなどクラウドサービス全体の「安全性の保証と証明」ができなければならない。

・クラウドサービス事業者は、個人情報取扱事業者の扱いになるのかここでは、判断ができない。

3.2 行動ターゲティング広告に関する検討

Webサイトは、今や日常生活や仕事の上で情報の収集手段として最大のツールとなっている。　企業は、自社が提供するサービスを的確に必要とされる顧客に情報が伝達できることによって効率の良い商談が実現できる。　又、利用者にとっても、Webサイトから自分の必要とする情報を取り出すことが困難になっているほど、膨大な情報量が流通している。

利用者の「行動情報」は、Webサイトへの訪問や検索行動だけに留まらず、携帯電話のサービス利用情報や電子マネー、電子タグ、自動改札など色々な利用情報が電子データとなって流通している。　これらの行動情報や利用情報が一つのところに集められると、一人ひとりの行動がより詳細に分析することができ、本人の興味あるもの、趣味、嗜好などに関するサービス提供の精度がどんどん向上する。

利用者は、自分が必要とする情報が簡単に入手することができれば、その仕組みや方法に対して理解を示すことだろう。　しかし、利用者は、サービスの利便性の反面、自分がWebサイト上での行動やその他の行動が情報として蓄積されていることの不安と不快感が同時に現れる。　利用者が感じる不快感は、蓄積された情報が「プライバシー」の領域まで入り込んでいるのではと感じている。　又、利用者がもつ不安感は、蓄積された情報がどのように利用され、管理されているのか理解できない（又は、理解できていない）ことや、その情報が漏えいした場合、本人への影響の大小が分からないためである。

このような「行動履歴情報」を利用したサービスのひとつである、「行動ターゲティング広告」に関して検討を行った。

（1）行動ターゲティング広告とは

Webサイトにアクセスした履歴を基に、一人ひとりのユーザに対して適切な広告を配信する仕組みである。

（２）行動履歴情報は、個人情報なのか

「個人情報の保護に関する法律」で定義されている「個人情報」とは、**生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることなるものを含む）**をいう。

パソコンからのWebサイト訪問履歴、検索履歴などは、主にクッキーを利用して取得している。　クッキーは、個々のパソコンを識別するデータやWebサイト訪問先、日時、回数などを記録する。　利用者が使用するWebブラウザーに保存されたクッキーをWebサーバーが取り出すことで利用者を特定している。(利用者が使用するWebブラウザーを特定するだけで個人は特定できない)　このため、クッキーは基本的に個人情報との関連性はなく個々のパソコンからの訪問履歴情報を取得することになる。

しかし、携帯電話の「行動ターゲティング広告」サービスは、クッキー機能がないため、個々の電話機を識別する「個体識別番号」が電話番号とは別に割り振られている。

携帯電話では、この「個体識別番号」を用いてターゲティングを行う。

携帯電話の「行動ターゲティング広告」は、「個体識別番号」を管理している携帯電話キャリアしか実現しない。

（３）「行動ターゲティング広告」とセキュリティ

前項で記述したとおり、パソコンではクッキーを利用するため、個人情報を取得することがなく、目的が達成できるが、「行動履歴情報」と「個人情報」を結びつける行為は、「目的外利用」に該当する、または、「プライバシー領域」に入るなどが考えられるため、注意が必要である。　また、携帯電話については、「個体識別番号」情報がわかれば、携帯電話キャリアが保有するデータベースを参照することで「個人情報」のほか訪問履歴情報や購入履歴情報、位置情報など重要な情報を取得することができることから携帯電話の「行動ターゲティング広告」を適用するにあたっては、パソコンとは、比べ物にならないほど「プライバシー」の領域に入るような問題をはらんでいる。

（４）米国の「行動ターゲティング広告」に関する動向

・米国メディア、広告業界の複数の業界団体が７月２日、消費者のデータを収集するWebサイト向け自主規制ルールを発表した。　特に、行動ターゲティング広告を対象としている。

参加業界団体：米国広告業協会（AAAA)、全米広告協会（ANA)、米ダイレクトマーケティング協会（DMA)、インタラクティブ広告協会（IAB)、米商事改善協会（BBB)

・このルールは、広告主とWebサイトに対し、消費者データを収集していることを明確に開示し、消費者が自分の情報を管理できるようにすることを求めている。

米連邦取引委員会（FTC）が行動ターゲティング広告に対するより強力な自主規制を求めたことから以下の 7 つの原則に沿って策定された。

①教育

行動ターゲティング広告について、個人および企業を啓発する。

②透明性

行動ターゲティング広告に関連するデータの収集や利用について、消費者に明確に開示する。

③消費者による管理

消費者が、行動ターゲティング広告のためのデータ収集・利用を許可するかどうかを選べるようにする。　サービス事業者は事前にユーザの同意を得るとともに、**データを匿名化する**対策を取らなければならない。

④データのセキュリティ

適切なセキュリティを提供し、データ保持を制限する。

⑤変更に際しての同意の取得

行動ターゲティング広告のためのデータ収集・利用方針などを変更する際には、事前にユーザの同意を得る。

⑥機密データの取扱い

子供から収集したデータ、医療・金融関連データについては保護を強化し、13 歳未満の消費者に行動ターゲティング広告を提示する場合は保護者の同意を得る。

⑦アカウンタビリティ

コンプライアンス違反の監視・通告プログラムなど、自主規制ルールを前進させるためのプログラムを開発する。

上記の自主規制ルールは 2010 年初めから実施の予定で整備が進められている。

（5）国内の「行動ターゲティング広告」に関する動向

インターネット広告推進協議会は、「インターネット広告掲載に関するガイドライン集 2009 年度版」に「行動ターゲティング広告」に関するガイドラインを改正し公表した。

①ガイドラインの目的

本ガイドラインは、インターネットユーザ（消費者）の Web サイト上での行動履歴情報を収集し、そのデータを利用して広告を表示する行動ターゲティング広告に関して、媒体社や広告配信事業社が提示すべき内容を定めるものである。

行動ターゲティング広告の利点を踏まえ、プライバシー保護の観点からユーザ（消費者）および広告主の正しい理解を得て、安心してインターネット広告を利用することができる環境を整えることを目的とする。

②本ガイドラインの対象

本ガイドラインは、行動ターゲティング広告を掲載する媒体社や機能を提供する事業

者（掲載媒体社、行動履歴情報提供媒体社、配信事業社）に対して、インターネットユーザ（消費者）に提示する内容と提供する機能についての基準と考え方を示すものである。なお、媒体社が自社のコンテンツサービスにおいて利用する場合については、本ガイドラインの対象には含まないものとする。

③ユーザ（消費者）への明示項目

行動ターゲティング広告を提供する事業者（掲載媒体社、行動履歴情報提供媒体社配信事業社）が各々の Web サイトにおいて明示すべき内容を以下に定める。配信事業社はすべての項目を明示し、掲載媒体社および行動履歴情報提供媒体社は行動ターティング広告を行っていることを明示するとともに配信事業社の該当 Web ページへのリンクを分かりやすく設置するものとする。

［必須項目］

・行動ターゲティング広告の手法の説明
・行動履歴情報を収集・判別している事業者
・行動履歴情報を収集・判別している場所
・行動履歴情報として収集・判別している内容
・行動履歴情報の利用者
・行動履歴情報の広告への利用方法
・広告主に開示している領域
・行動履歴情報を保持している期間

［推奨項目］

・各社それぞれに留意・配慮している領域

④ユーザ（消費者）の行動履歴情報の利用許諾に関して

行動ターゲティング広告において行動履歴情報を利用する場合には、ユーザ（消費者）の許諾を得ることを前提とする。ユーザ（消費者）に対し、前項に挙げた行動履歴情報の広告への利用に関する明示項目（必須項目）を Web サイト内の分かりやすいページにおいてあらかじめ明示することをもって許諾とみなすものとする。ただし、ユーザ（消費者）が許諾できない場合に行動ターゲティング広告機能をオプトアウトできるよう、具体的な方法を提示することを推奨し、次項に定める。

⑤ユーザ（消費者）の行動ターゲティング広告の拒否に関して

行動ターゲティング広告への行動履歴情報の利用においては、前項に定める通りユーザ（消費者）の許諾を得ることを前提とするが、ユーザ（消費者）が許諾できない場合には、行動履歴情報の利用に対して拒否の意志を示す、もしくはユーザ（消費者）自らがクッキーを削除するなどの方法によって、行動ターゲティング広告を拒否できるようにすることを推奨する。

利用拒否の場合の対応としてオプトアウト機能（方法）の提供・提示を行うことを推奨し、利用を拒否したユーザ（消費者）本人の行動履歴情報を行動ターゲティング広

告配信に利用しないことをオプトアウトの提供と定義する。

オプトアウトの提供には以下の対応方法がある。

ａ行動履歴情報の取得・判別そのものを停止するもの。

ｂ行動履歴情報を取得はするが広告配信に使わないとするもの。

また、オプトアウトの具体的な方法としては以下がある。いずれかの方法でユーザ（消費者）にオプトアウト機能（方法）を提供することを推奨する。

・行動ターゲティング広告を提供する事業者が上記ａもしくはｂの状態を提供する方法。

・事業者が、ユーザのブラウザーの操作によってクッキーの送受信を拒否、もしくはクッキーの削除を行う方法などを明示し、その対応をユーザ（消費者）本人に行ってもらうことで上記ａを提供する方法。

⑥補足：行動ターゲティング広告の掲載内容の自主規制に関して

行動ターゲティング広告は、個人情報を利用しているものではないが、広告内容によっては、その掲載頻度によりユーザー（消費者）に対して不快感、不安感を与える場合があることも懸念される。

行動ターゲティング広告を掲載する媒体社においては、独自に広告内容や広告目的制限しているところも一部あるが、公告掲載の可否の決定は各媒体社が自主的な判断において行うものであるため、個々の運用は各社の判断に委ねる。

3.3 行動ターゲッティング広告を活用するための参考ガイド

行動ターゲティング広告に関する国内外の関心も強く適切に対応しつつ推進しなければならない。　ここでは、「行動ターゲティング広告」推進のためのポイントと活用するための掲示・公表の雛型を本ワーキンググループで検討し作成した。

（１）行動ターゲティング広告を企業が推進するためのポイント

行動履歴情報は、今回のテーマである「行動ターゲティング広告」には留まらず、ＧＰＳ機能付き携帯電話の位置情報、電子マネー利用情報（何時、どこで、なにを、いくらで）、定期券入出改札情報､市街防犯ビデオ情報など行動情報が組み合わされる事でサービスの仕組みや、提供方法が大きく変化するだろう。

その反面、取扱いについては、「プライバシー」の領域にまで及ぶ可能性があることか慎重に進めることが必要である。　これらの情報利活用の潮流を踏まえて、「行動ターゲティング広告」に関する企業のスタンスを明確にすることが重要となる。

順不同

①　利用者の個人情報は一切取得していないことを宣言する

② サービスを提供するには、同意を取る（会員向けに行う場合)。又は、公表（不特定多数の訪問者向けの場合）によって理解を得る。
③ 取得する履歴情報を明確にする。
④ インターネット広告（例えば、行動ターゲティング広告）しくみを説明する（個人情報の必要がない事の証明）
⑤ 履歴情報の保管場所や保管期間の公表
⑥ サービスの停止、再開の手順について
⑦ 広告の対象とならないものを公表（例：倫理的に不適切なもの）
⑧ サービスの有無によるメリット、デメリットの説明
⑨ 相談窓口の公表

（2）行動ターゲティング広告を活用するための掲示・公表の雛型

企業が「行動ターゲティング広告」を適用し、利用者が安心して利用できるための雛型は①から⑨の項目を基に作成した。　（次頁：参考）

行動ターゲティング広告の掲示は、消費者が容易に確認できる場所（又は、操作によって）とすることが必要である。　又、従来の個人情報保護方針やプライバシーポリシー等に追加するのではなく、新たに設置することで、より消費者に確認し易い環境にすることが望ましい。

行動ターゲティング広告に関する掲示・公表例

〇〇　株式会社　　行動ターゲティング広告に関する方針

弊社は、お客様が弊社のＷｅｂサイトに訪問、検索等の行為（以下、行動履歴という）を基に独自の分析を行いお客様にとって適切かつ利便性のある情報を提供するサービスを行っています。

お客様が安心してご利用頂けます様に、「個人情報の保護に関する法律」等を遵守するとともにその管理と保護に万全を尽くします。

１．個人情報と行動履歴情報について

弊社は、お客様の「個人情報」について、事前に「同意」（オプトイン）を頂いてお預かり致します。 又、お客様の「行動履歴」情報は、自動的に収集（オプトアウト）させて頂いております。

「個人情報」の取扱につきましては、弊社、「個人情報保護方針」をご参照願います。

http://www.〇〇〇.△△△.□□□/

２．サービスの停止、再開について

弊社では、お客様に最適かつ利便性のある情報提供に努力いたしております。

お客様がこのサービスを不要とご判断された場合やサービスの再開の場合は下記の手順にて停止、再開を致します。

手順の説明文ｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘｘ。

下記、ご案内の内容をご確認の上、ご判断頂けます様、お願い申し上げます。

３．「行動履歴」情報とその内容について

弊社がお客様に提供いたします広告配信は、「行動ターゲティング広告」という方法を利用しております。

「行動履歴」情報は、弊社ホームページに訪問、閲覧、検索等の行為によって、お客様のＷｅｂブラウザーの識別ＩＤと訪問先、日時、回数等を**「cookie」又は、履歴情報収集ソフト**にて取得します。

これらの情報では、個人を特定することはできません。又、Ｗｅｂページ上での広告配信においてお客様の個人情報を収集および利用はしておりませんのでご安心ください。

４．「行動ターゲティング広告」の仕組み

行動ターゲッティングは、お客様が訪問した行動履歴情報を収集し弊社独自の分析によってお客様に最適な広告をＷｅｂページ上で配信します。

お客様が弊社に訪問することで、お客様のＷｅｂブラウザー識別ＩＤを認識しＷｅｂペ

ージに配信します。したがって、弊社からお客様に自ら配信することはございませんのでご安心ください。

５．「行動履歴」情報の安全管理措置と保管場所、保管期間について

弊社では、「行動履歴」情報及び「分析結果」情報は、「個人情報」と同等の安全管理措置を施して管理いたします。

弊社、データセンター（東京都港区ｘｘｘｘ）にて〇〇日間保管いたします。

又、保管期限終了時は、適切に廃棄処理を致します。

６．第三者への提供について

弊社が保管する「行動履歴」情報の一部又は全部を第三者に提供することはありません。

又、取引先や広告主に提供する情報は、統計データ等（個人は特定できない）を提供しますが「行動履歴情報」は提供しません。

（統計データの例：年齢層別や性別などにまとめた集計）

７．不適切な広告配信の排除

弊社では、独自の分類方法にてお客様に最適かつ利便性のある情報提供を心掛けております。　社会、倫理的に不適切と判断した情報や広告の提供は致しません。

８．サービス提供のメリットとサービス停止のデメリットについて

「行動ターゲティング広告」は前述の通り、お客様の「行動履歴」情報に基づいて最適な広告を配信する仕組みです。 お客様のご理解によって弊社に訪問する情報量が増えることによってさらに精度の高い情報提供が可能になります。

したがって、煩わしい「検索」等が不要になります。

反面、サービスを停止した場合は、「行動履歴」情報がありませんので、必要な情報はＷｅｂ検索によってお客様ご自身が選んで頂く事になります。

９．相談窓口

〇　〇　株式会社

△　△　事業部

相談窓口　担当　□□　△△

ＴＥＬ　03-ｘｘｘｘ-ｘｘｘｘ

Email　　soudan@koukoku.　co.jp

以　上

4. おわりに

次世代電子商取引推進協議会（以下、ＥＣＯＭという）個人情報保護ワーキンググループの活動において、多くの会員企業有志の方々ならびに有識者の方々には、永年にわたり、ご支援、ご協力を賜りましたことを、この場をお借りして心から御礼申し上げます。　個人情報保護法が施行された初年度は、多くの企業が混乱と困惑の渦中で体制整備に奮闘していました。　そのような時に、いち早くＥＣＯＭ内にワーキンググループを設置し、保護法の道しるべとなるＥＣＯＭガイドラインを策定、公表したことは、社会的にも貢献してきたと自負しております。

この度、ＥＣＯＭは、平成２１年度をもってその活動の幕を下ろすこととなりましたのでご報告申し上げます。　また、本ワーキンググループの活動を支えて下さいました会員企業殿ならびに関係団体殿、有識者の方々に重ねて御礼申し上げます。

本報告書のはじめに申し上げたとおり、クラウド時代の到来による個人情報の越境移転による国際的な対応と調和が必要であること、住宅設備機器や家電、電子マネー、電気自動車などがネットワークに接続され個人のライフスタイル情報が活用される新しいビジネスの創出となることなど、個人情報の取り巻く環境は日々変化している。

「過剰な反応」、「国際的な対応」、「利活用の推進」、「強化すべき個人情報と緩和すべき個人情報の選択」など調査・研究の活動に終わりはありません。

平成２２年度は、新たに、財団法人日本情報処理開発協会が事務局を務める次世代電子情報利活用推進フォーラムを設立し、今までの資産を継承しつつ引き続き取り組む所存でございます。　会員企業各位におかれましては、新組織での活動支援並びご協力の程、お願い申し上げます。

参考文献および掲載記事

文献　　New　Business　Law　　No.918,919,921,922
発行　　株式会社　商事法務
執筆者　濱野　敏彦

文献　　New　Business　Law　　No.918
発行　　株式会社　商事法務
執筆者　西田　淳二

文献　　日経 SYSTEMS
発行　　日経ＢＰ社

文献　　行動ターゲティング広告
発行　　株式会社　インプレスジャパン
著者　　株式会社　マイクロアド　代表取締役　渡辺　健太郎

文献　　インターネット広告掲載に関するガイドライン集　2009 年度版
発行　　インターネット広告推進協議会

文献　　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
発行　　経済産業省

文献　　個人と連結可能な情報の保護と利用のために
発行　　パーソナル情報研究会　　（経済産業省）

文献　　情報化白書　２００９
発行　　財団法人　日本情報処理開発協会

記事　　http://www.security-next.com
　　http://www.asahi.com/

個人情報保護ワーキンググループ委員名簿

（順不同）

	氏　名	会社名（団体名）
会　員	桑野　孝浩	電気事業連合会
	小林　智恵子	東芝ソリューション株式会社
	岩間　研二	三菱電機株式会社
	吉田　久志	三菱電機インフォメーションテクノロジー株式会社
	行木　直之	マイクロソフト株式会社
有識者	堀部　政男	一橋大学名誉教授
	鈴木　正朝	新潟大学大学院
	新保　史生	慶應義塾大学
	牧山　嘉道	ＴＭＩ総合法律事務所
	鈴木　靖	株式会社シーピーデザインコンサルティング
	藤田　素康	リコー・ヒューマン・クリエイツ株式会社
	上　　茂之	株式会社富士通総研
客員研究員	江口　正裕	
オブザーバー	西田　淳二	経済産業省
	小林　菜摘	経済産業省
事務局	野村　至	次世代電子商取引推進協議会
	那須野元庸	次世代電子商取引推進協議会

巻末資料

第41回ECOMセミナー講演資料

2010 年 2 月 9 日開催

「最新の個人情報漏えい事故状況と傾向」

最新の個人情報漏えい事故状況と傾向

事故の原因は、個人情報の持ち出しと一人ひとりの意識の問題

２０１０年２月９日

次世代電子商取引推進協議会（ＥＣＯＭ）
個人情報保護ワーキンググループ
主席研究員　那須野元庸

1

も　く　じ

2

はじめに

「個人情報の保護に関する法律」が２００５年４月に全面施行されて５年が経過しょうとしている。
個人情報保護に関する消費者の意識も十分浸透してきたことと、企業の取組も積極的に進んできた。
しかしながら、依然として個人情報漏えい事故が跡を絶たない状況にある。
本報告は、Ｗｅｂサイト情報等で公表された漏えい事故を基に独自でまとめた情報である。
全ての漏えい事故が確認できた訳ではないが、この調査結果が今後の個人情報保護推進にお役に立てば幸いである。

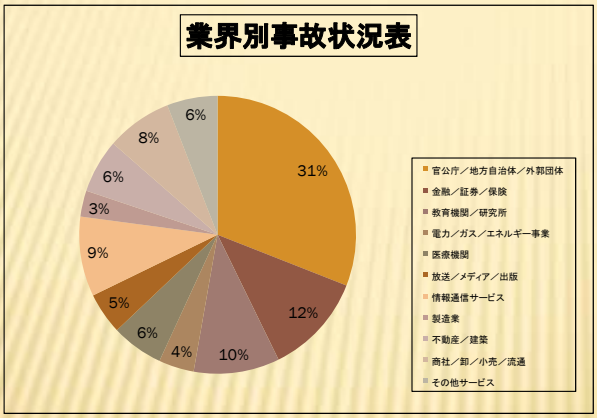
１．漏えい事故状況の総括

個人情報漏えい事故状況の総括

・個人情報漏えい事故の情報収集期間
　２００９年１月１日～２００９年１２月３１日　　事故件数　５５９件
・２００９年の漏えい事故の状況
　ⓐ個人情報漏えい事故は、年々減少傾向にある。
　ⓑ事故の内容では、盗難、紛失、誤配信／誤配送で全体の８５％となった。
　ⓒ事故発生の場所では、個人宅、通勤／帰宅途中、その他（立ち寄り）
　　で２２％となった。（事務所：６６％、外出先：１２％）
　ⓓ盗難、紛失において電子機器や電子媒体に対するセキュリティ対策の
　　実施状況を見ると全体の２９％がセキュリティ対策が施されていた。
　　しかし、ＵＳＢの対策状況は、僅か８％しか施されていなかった。
　ⓔ盗難事故の発生場所をみると事務所での発生は２２％であった。
　ⓕ不正アクセス／不正利用は内部からの事故が惨事につながっている。
・事故の根本的な原因を考える
　漏えい事故が起こるのは、個人の問題か？組織の問題か？

２．２００９年の漏えい事故状況

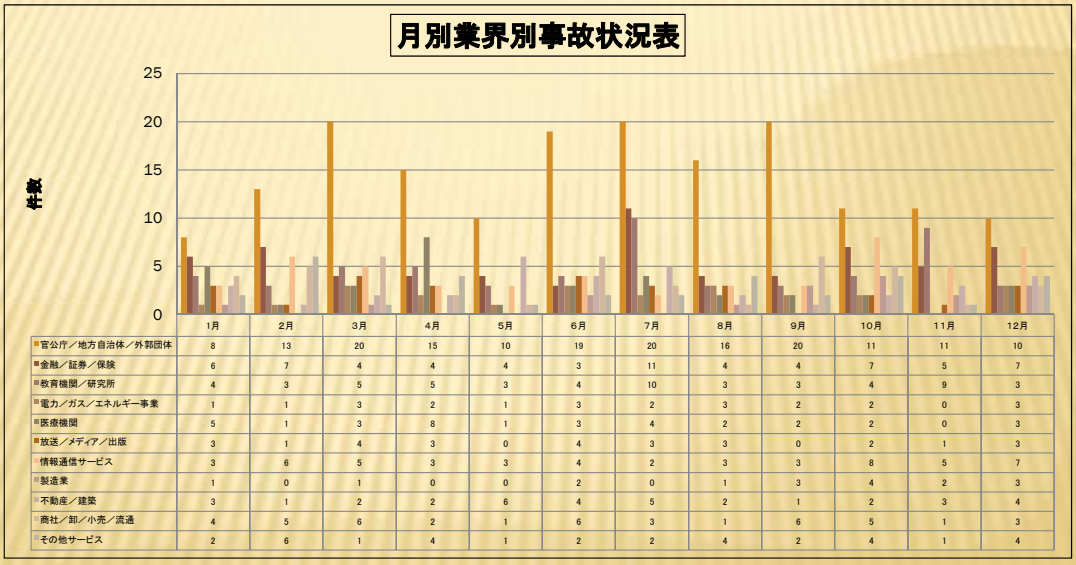
①業界別事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	173
金融／証券／保険	66
教育機関／研究所	56
電力／ガス／エネルギー事業	23
医療機関	34
放送／メディア／出版	27
情報通信サービス	52
製造業	17
不動産／建築	35
商社／卸／小売／流通	43
その他サービス	33

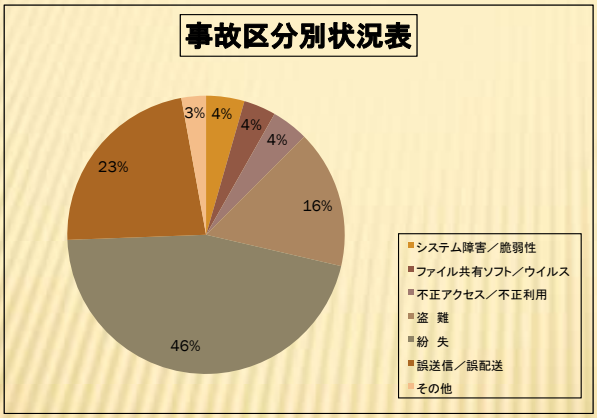
＊業界分類は独断で仕分けしましたのでご了承願います。

①－１　月別業界別事故状況



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
官公庁／地方自治体／外郭団体	8	13	20	15	10	19	20	16	20	11	11	10
金融／証券／保険	6	7	4	4	4	3	11	4	4	7	5	7
教育機関／研究所	4	3	5	5	3	4	10	3	3	4	9	3
電力／ガス／エネルギー事業	1	1	3	2	1	3	2	3	2	2	0	3
医療機関	5	1	3	8	1	3	4	2	2	2	0	3
放送／メディア／出版	3	1	4	3	0	4	3	3	0	2	1	3
情報通信サービス	3	6	5	3	3	4	2	3	3	8	5	7
製造業	1	0	1	0	0	2	0	1	3	4	2	3
不動産／建築	3	1	2	2	6	4	5	2	1	2	3	4
商社／卸／小売／流通	4	5	6	2	1	6	3	1	6	5	1	3
その他サービス	2	6	1	4	1	2	2	4	2	4	1	4

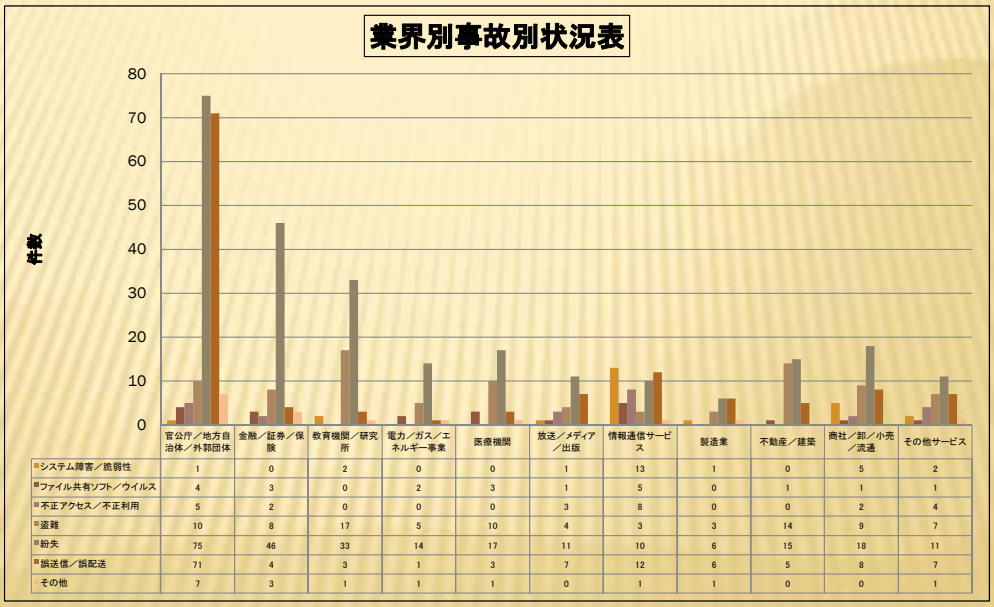
②事故区分別状況



事故区分	件数
システム障害／脆弱性	25
ファイル共有ソフト／ウイルス	21
不正アクセス／不正利用	24
盗　難	90
紛　失	256
誤送信／誤配送	127
その他	16

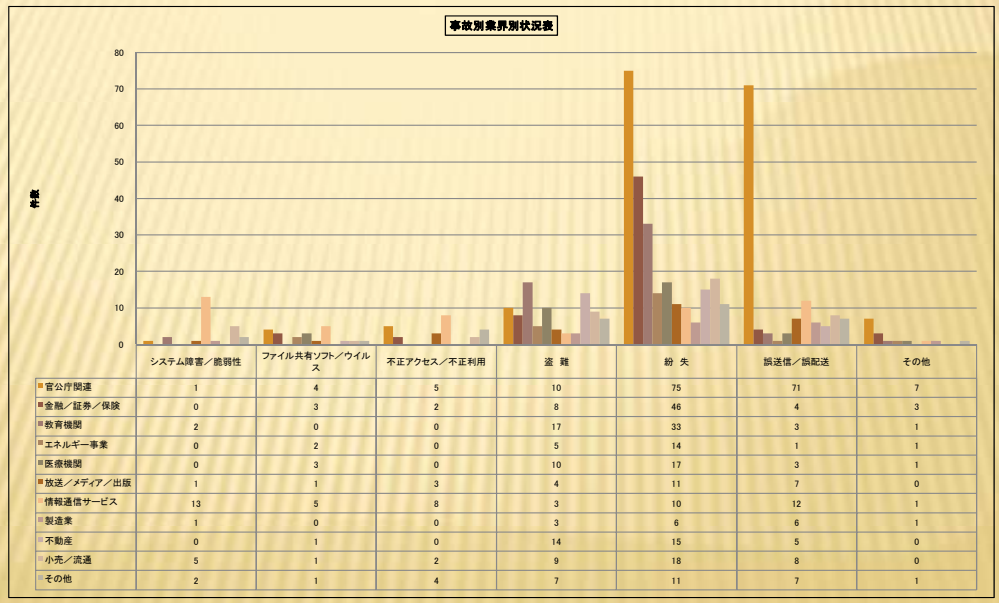
・紛失事故は、誤廃棄が目立った。
・トピックス：個人情報の拾得者が紛失企業を恐喝する事件が発生

②－１　業界別事故状況



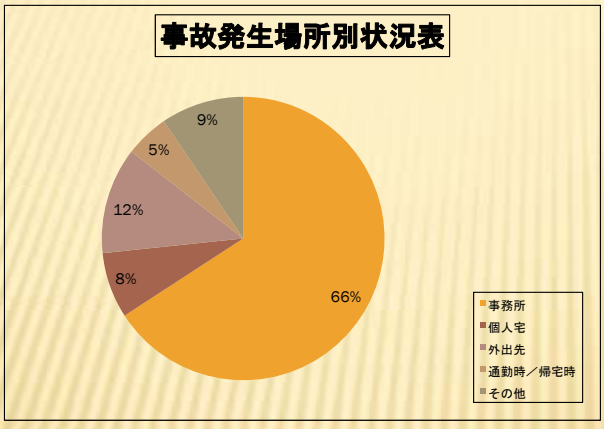
	官公庁／地方自治体／外郭団体	金融／証券／保険	教育機関／研究所	電力／ガス／エネルギー事業	医療機関	放送／メディア／出版	情報通信サービス	製造業	不動産／建築	商社／卸／小売／流通	その他サービス
システム障害／脆弱性	1	0	2	0	0	1	13	1	0	5	2
ファイル共有ソフト／ウイルス	4	3	0	2	3	1	5	0	1	1	1
不正アクセス／不正利用	5	2	0	0	0	3	8	0	0	2	4
盗難	10	8	17	5	10	4	3	3	14	9	7
紛失	75	46	33	14	17	11	10	6	15	18	11
誤送信／誤配送	71	4	3	1	3	7	12	6	5	8	7
その他	7	3	1	1	1	0	1	1	0	0	1

②－２　事故別業界別状況



	システム障害／脆弱性	ファイル共有ソフト／ウイルス	不正アクセス／不正利用	盗　難	紛　失	誤送信／誤配送	その他
官公庁関連	1	4	5	10	75	71	7
金融／証券／保険	0	3	2	8	46	4	3
教育機関	2	0	0	17	33	3	1
エネルギー事業	0	2	0	5	14	1	1
医療機関	0	3	0	10	17	3	1
放送／メディア／出版	1	1	3	4	11	7	0
情報通信サービス	13	5	8	3	10	12	1
製造業	1	0	0	3	6	6	1
不動産	0	1	0	14	15	5	0
小売／流通	5	1	2	9	18	8	0
その他	2	1	4	7	11	7	1

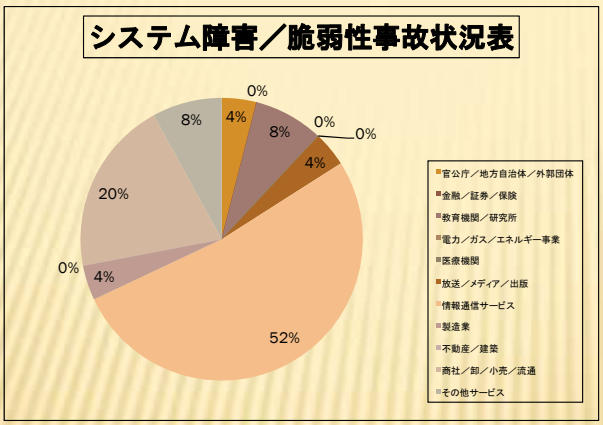
③事故発生場所別状況



事故発生場所区分	件数
事務所	368
個人宅	42
外出先	68
通勤時／帰宅時	28
その他	53

・個人宅、通勤／帰宅途中、その他（立ち寄り）で22%になった。

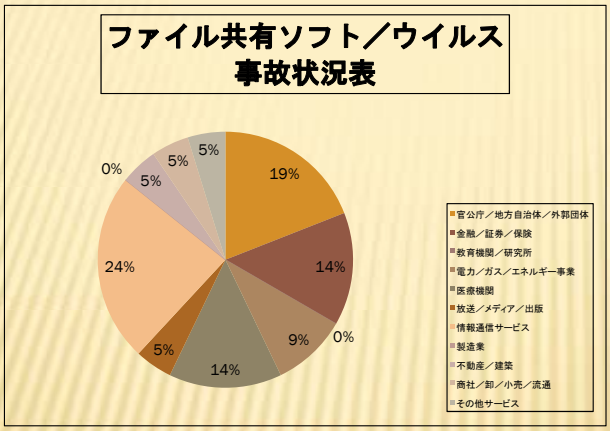
④システム障害／脆弱性による事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	1
金融／証券／保険	0
教育機関／研究所	2
電力／ガス／エネルギー事業	0
医療機関	0
放送／メディア／出版	1
情報通信サービス	13
製造業	1
不動産／建築	0
商社／卸／小売／流通	5
その他サービス	2

・Webサーバーの入れ替え時による設定ミスやシステム障害が起因。

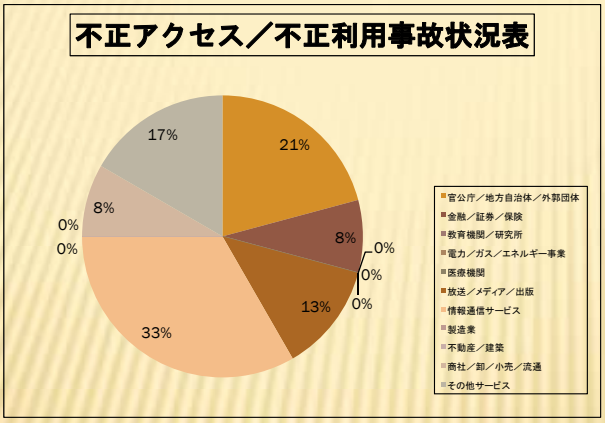
⑤ファイル共有ソフト／ウイルスによる事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	4
金融／証券／保険	3
教育機関／研究所	0
電力／ガス／エネルギー事業	2
医療機関	3
放送／メディア／出版	1
情報通信サービス	5
製造業	0
不動産／建築	1
商社／卸／小売／流通	1
その他サービス	1

・ファイル共有ソフトの利用者は減少したが、事故では20件を確認した。
・私用パソコンからの漏えいが原因。

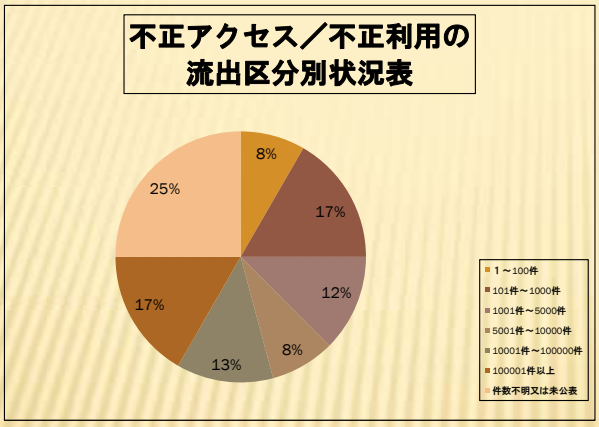
⑥不正アクセス／不正利用による事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	5
金融／証券／保険	2
教育機関／研究所	0
電力／ガス／エネルギー事業	0
医療機関	0
放送／メディア／出版	3
情報通信サービス	8
製造業	0
不動産／建築	0
商社／卸／小売／流通	2
その他サービス	4

・漏えい流出件数が10万件以上の事故が4件起こっている。
・又、4件の内、内部からの流出が3件だった。（⑥－2参照）

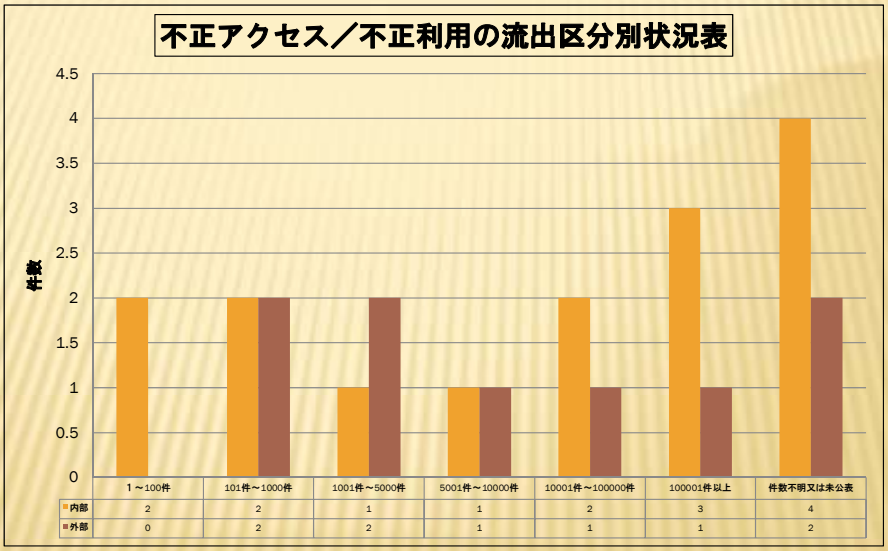
⑥－1　不正アクセス／不正利用の流出区分別状況



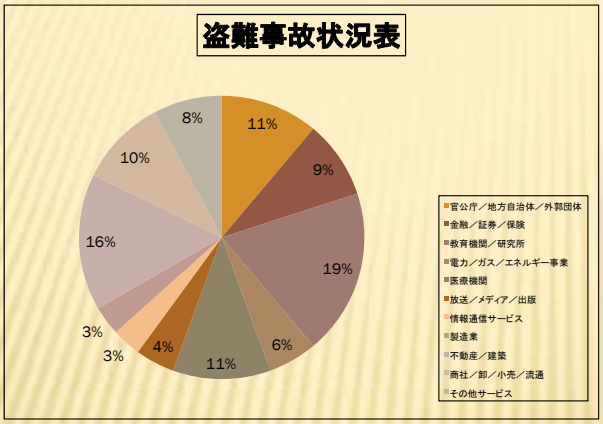
流出件数区分	件数
1～100件	2
101件～1000件	4
1001件～5000件	3
5001件～10000件	2
10001件～100000件	3
100001件以上	4
件数不明又は未公表	6

・10万件以上の流出事故が4件も発生している。

⑥－２　不正アクセス／不正利用の内部／外部の流出区分別状況



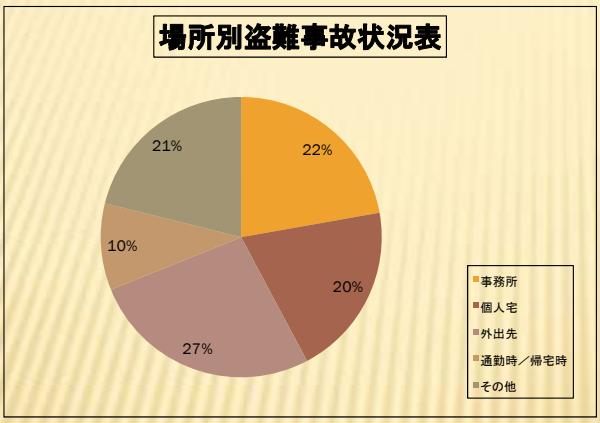
⑦盗難による事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	10
金融／証券／保険	8
教育機関／研究所	17
電力／ガス／エネルギー事業	5
医療機関	10
放送／メディア／出版	4
情報通信サービス	3
製造業	3
不動産／建築	14
商社／卸／小売／流通	9
その他サービス	7

・盗難事故は、業界での偏りは無い。

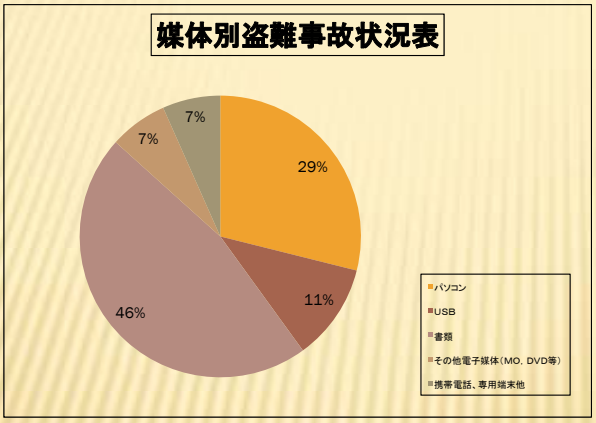
⑦－１　場所別盗難事故状況



事故発生場所区分	件数
事務所	20
個人宅	18
外出先	24
通勤時／帰宅時	9
その他	19

・事故発生場所は、78%が事務所以外で起こっている。

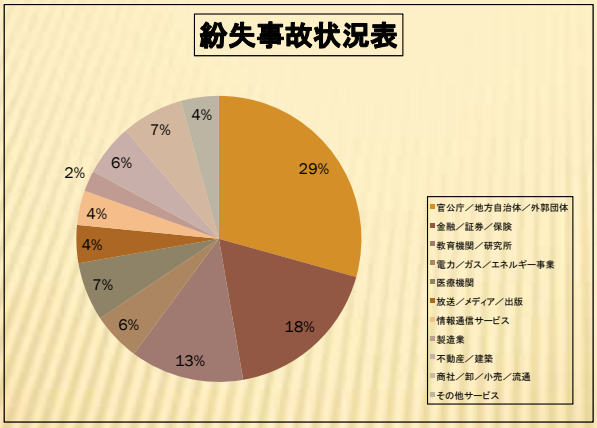
⑦－２　媒体別盗難事故状況



媒体区分	件数
パソコン	26
ＵＳＢ	10
書類	42
その他電子媒体（ＭＯ，ＤＶＤ等）	6
携帯電話、専用端末他	6
その他	0

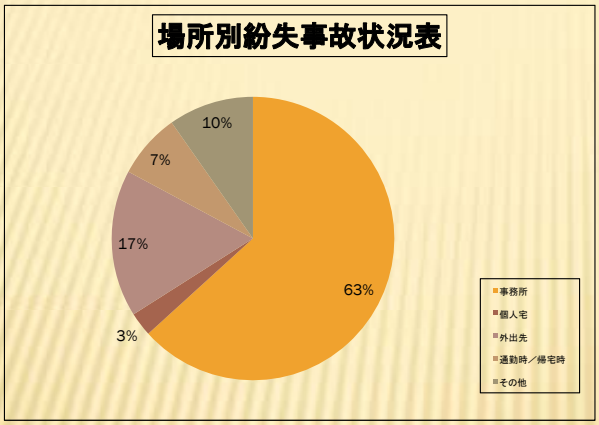
・基本的には、個人情報を目的とした犯行ではない。

⑧紛失による事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	75
金融／証券／保険	46
教育機関／研究所	33
電力／ガス／エネルギー事業	14
医療機関	17
放送／メディア／出版	11
情報通信サービス	10
製造業	6
不動産／建築	15
商社／卸／小売／流通	18
その他サービス	11

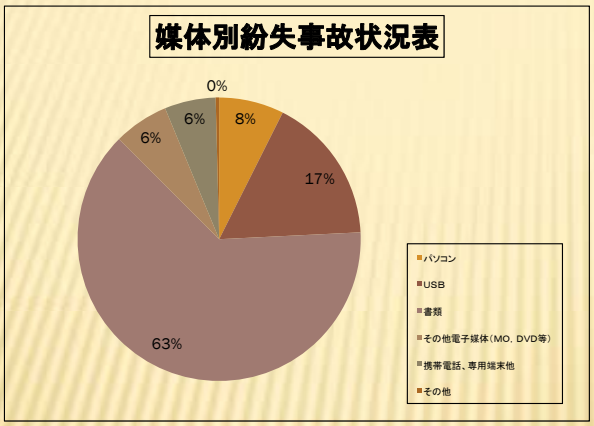
⑧－１　場所別紛失事故状況



事故発生場所区分	件数
事務所	162
個人宅	7
外出先	43
通勤時／帰宅時	19
その他	25

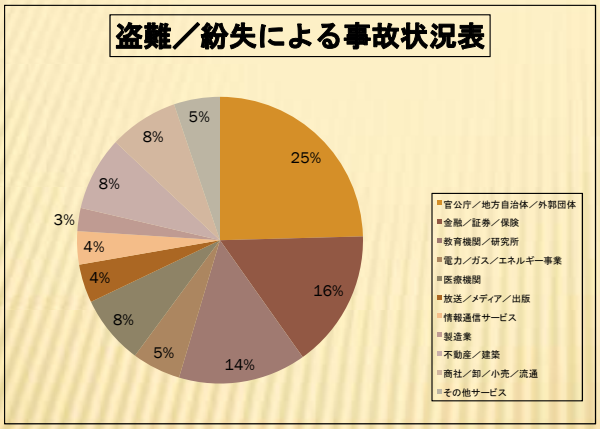
・紛失事故においても事務所以外で94件の事故が起こっている。

⑧－２　媒体別紛失事故状況



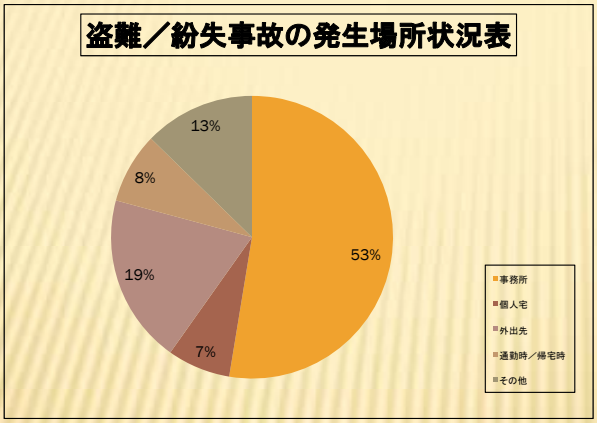
媒体区分	件数
パソコン	19
ＵＳＢ	43
書類	162
その他電子媒体（ＭＯ，ＤＶＤ等）	16
携帯電話、専用端末他	15
その他	1

⑨盗難／紛失による事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	85
金融／証券／保険	54
教育機関／研究所	50
電力／ガス／エネルギー事業	19
医療機関	27
放送／メディア／出版	15
情報通信サービス	13
製造業	9
不動産／建築	29
商社／卸／小売／流通	27
その他サービス	18

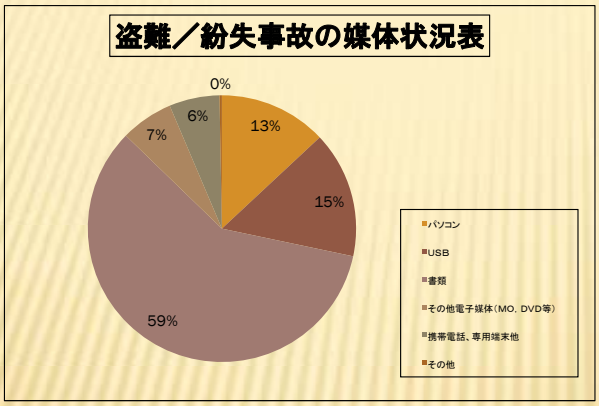
⑨－１　盗難／紛失事故の発生場所状況



事故発生場所区分	件数
事務所	182
個人宅	25
外出先	67
通勤時／帰宅時	28
その他	44

・盗難／紛失事故において事務所以外の事故が47%なる。

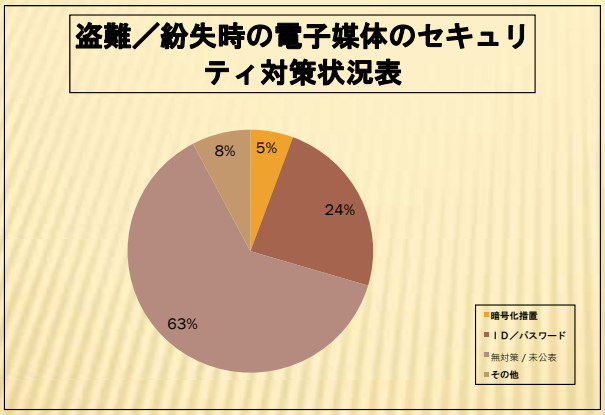
⑨－２　盗難／紛失事故の媒体状況



媒体区分	件数
パソコン	45
ＵＳＢ	53
書類	204
その他電子媒体（ＭＯ，ＤＶＤ等）	22
携帯電話、専用端末他	21
その他	1

・USBは全体の１５%を占めており総括で述べたとおりセキュリティ
対策は10%にも満たない結果となっている。

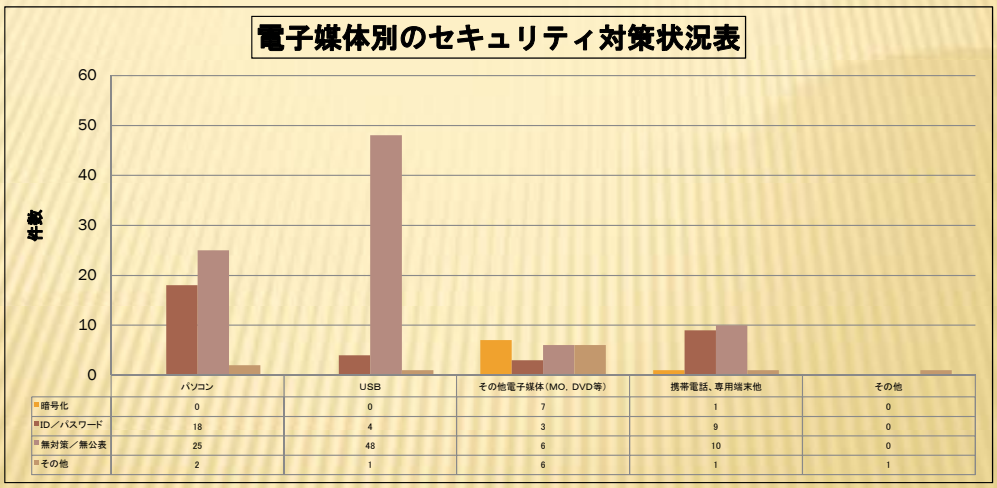
⑨－３　盗難／紛失の電子媒体のセキュリティ対策状況



セキュリティ対策区分	件数
暗号化措置	8
ＩＤ／パスワード	34
無対策／未公表	89
その他	11

・紙媒体を除く、パソコンやUSB、その他電子媒体、携帯電話／専用端末のセキュリティ対策状況を図に示す。

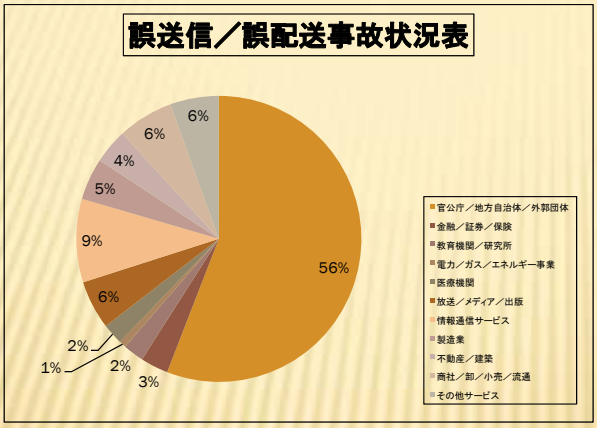
⑨－４　電子媒体別のセキュリティ対策状況



	パソコン	USB	その他電子媒体（MO、DVD等）	携帯電話、専用端末他	その他
暗号化	0	0	7	1	0
ID／パスワード	18	4	3	9	0
無対策／無公表	25	48	6	10	0
その他	2	1	6	1	1

・パソコンは40%、USBは8%、その他電子媒体は45%、携帯電話／専用端末は48%がセキュリティ対策実施率である。

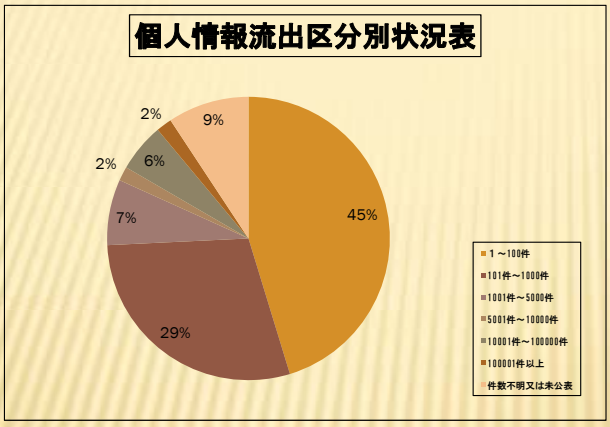
⑩誤送信／誤配信による事故状況



業界区分	件数
官公庁／地方自治体／外郭団体	71
金融／証券／保険	4
教育機関／研究所	3
電力／ガス／エネルギー事業	1
医療機関	3
放送／メディア／出版	7
情報通信サービス	12
製造業	6
不動産／建築	5
商社／卸／小売／流通	8
その他サービス	7

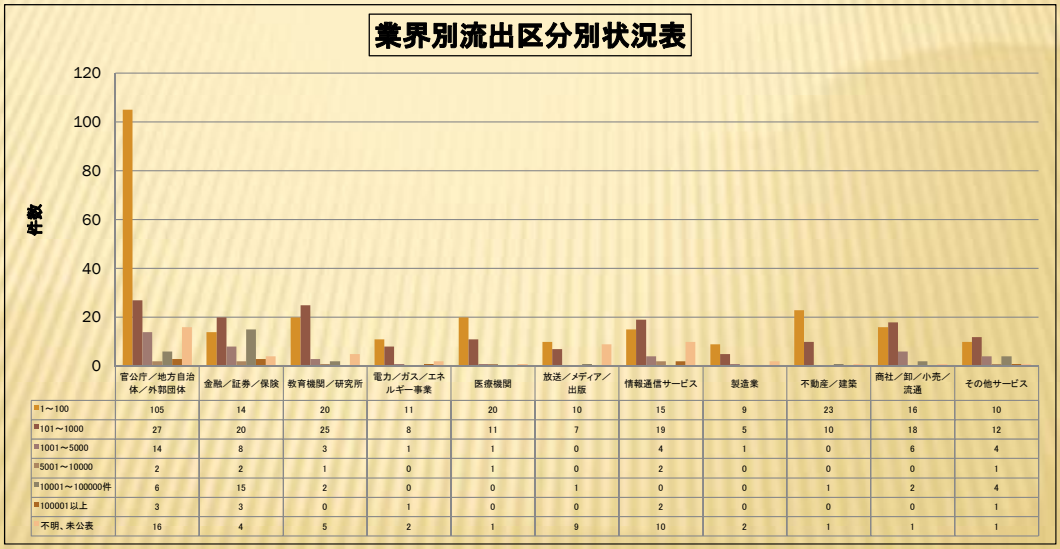
・送信先が他の受信者に閲覧可能状態で配信される事故が大半である。
・誤配送では宛名シールの二重貼り付けによる事故が目立つ。

⑪個人情報流出区分別状況



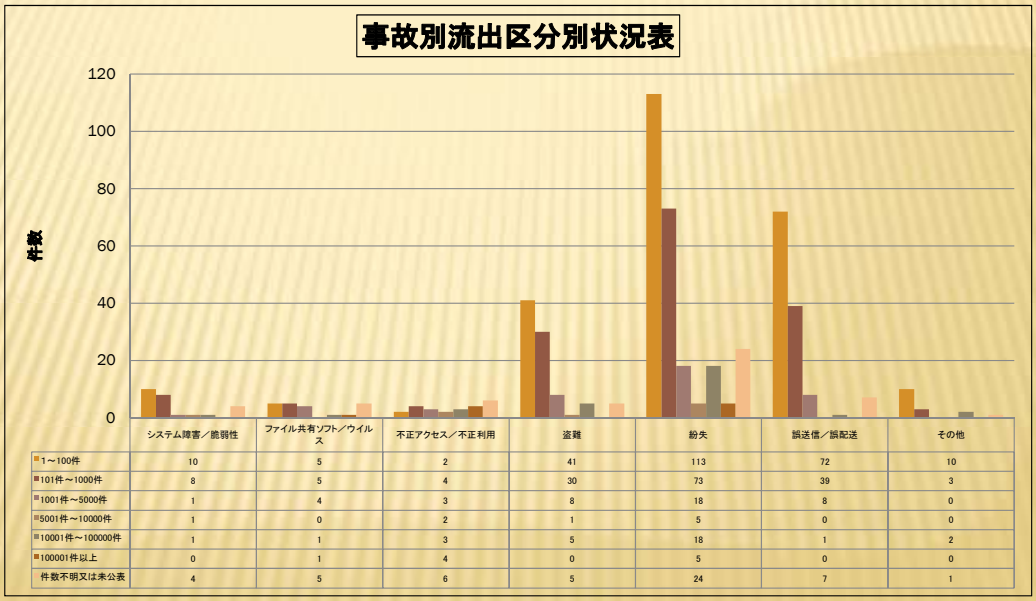
流出件数区分	件数
1～100件	253
101件～1000件	162
1001件～5000件	42
5001件～10000件	9
10001件～100000件	31
100001件以上	10
件数不明又は未公表	52

⑪－１　業界別流出区分別状況



	官公庁／地方自治体／外郭団体	金融／証券／保険	教育機関／研究所	電力／ガス／エネルギー事業	医療機関	放送／メディア／出版	情報通信サービス	製造業	不動産／建築	商社／卸／小売／流通	その他サービス
1～100	105	14	20	11	20	10	15	9	23	16	10
101～1000	27	20	25	8	11	7	19	5	10	18	12
1001～5000	14	8	3	1	1	0	4	1	0	6	4
5001～10000	2	2	1	0	1	0	2	0	0	0	1
10001～100000件	6	15	2	0	0	1	0	0	1	2	4
100001以上	3	3	0	1	0	0	2	0	0	0	1
不明、未公表	16	4	5	2	1	9	10	2	1	1	1

⑪－２　事故別流出区分別状況



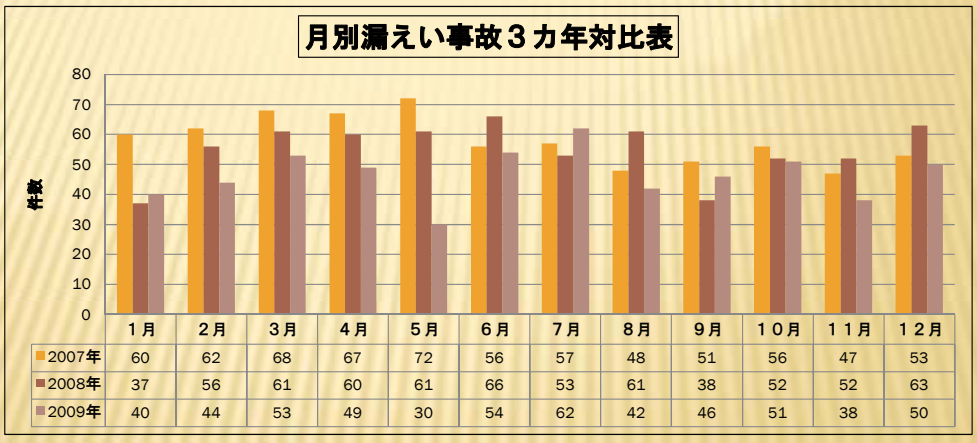
	システム障害／脆弱性	ファイル共有ソフト／ウイルス	不正アクセス／不正利用	盗難	紛失	誤送信／誤配送	その他
1～100件	10	5	2	41	113	72	10
101件～1000件	8	5	4	30	73	39	3
1001件～5000件	1	4	3	8	18	8	0
5001件～10000件	1	0	2	1	5	0	0
10001件～100000件	1	1	3	5	18	1	2
100001件以上	0	1	4	0	5	0	0
件数不明又は未公表	4	5	6	5	24	7	1

３．過去３カ年の漏えい事故状況

34

①過去３年間の月別漏えい事故状況

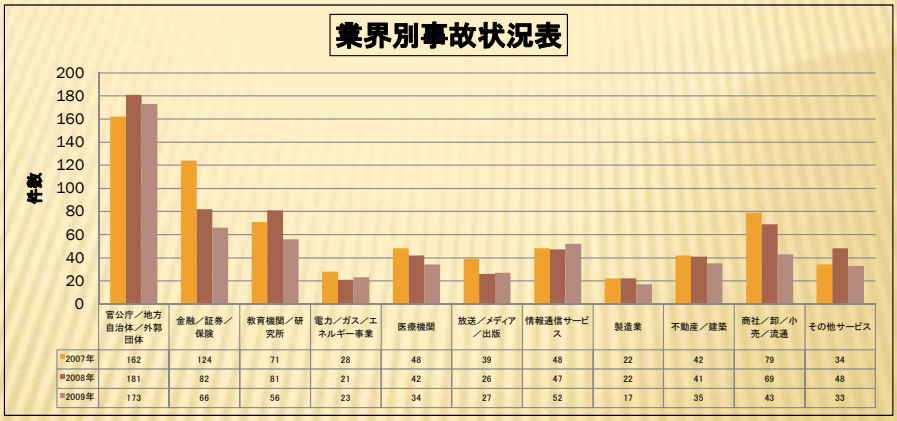
	１月	２月	３月	４月	５月	６月	７月	８月	９月	１０月	１１月	１２月	合計
2007年	60	62	68	67	72	56	57	48	51	56	47	53	697
2008年	37	56	61	60	61	66	53	61	38	52	52	63	660
2009年	40	44	53	49	30	54	62	42	46	51	38	50	559



・2007年は697件、2008年は660件、2009年は、559件で事故件数は減少している。

35

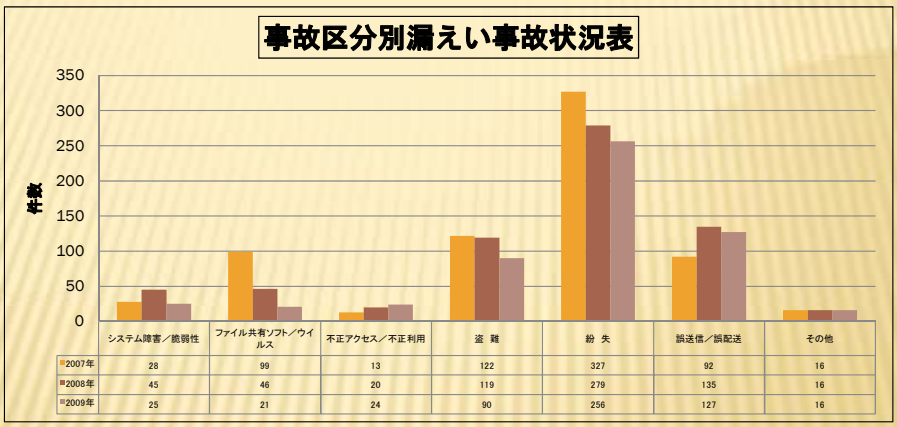
②過去３年間の業界別漏えい事故状況



	官公庁／地方自治体／外郭団体	金融／証券／保険	教育機関／研究所	電力／ガス／エネルギー事業	医療機関	放送／メディア／出版	情報通信サービス	製造業	不動産／建築	商社／卸／小売／流通	その他サービス
2007年	162	124	71	28	48	39	48	22	42	79	34
2008年	181	82	81	21	42	26	47	22	41	69	48
2009年	173	66	56	23	34	27	52	17	35	43	33

・多少の凸凹はみられるが全体的には事故件数は減少している。

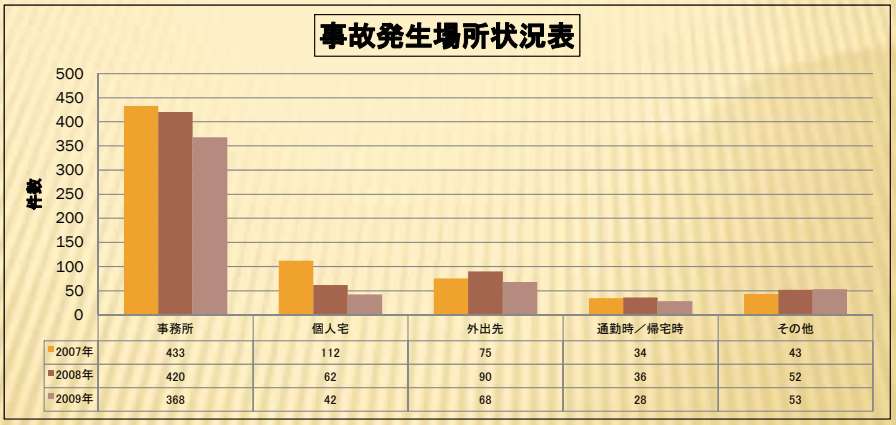
③過去３年間の事故別漏えい事故状況



	システム障害／脆弱性	ファイル共有ソフト／ウイルス	不正アクセス／不正利用	盗　難	紛　失	誤送信／誤配送	その他
2007年	28	99	13	122	327	92	16
2008年	45	46	20	119	279	135	16
2009年	25	21	24	90	256	127	16

・ファイル共有ソフト／ウイルス事故は過去と比べ大幅に減少している。
・不正アクセス／不正利用は微量ながら増加している。

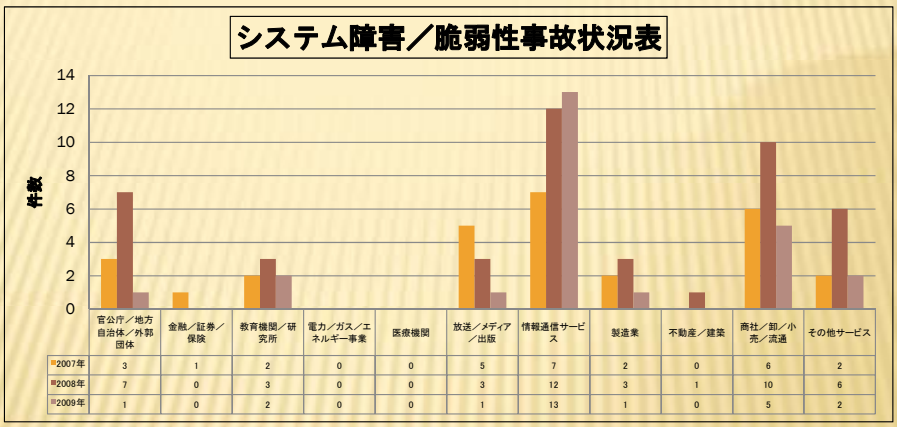
④過去３年間の事故発生場所別漏えい事故状況



	事務所	個人宅	外出先	通勤時／帰宅時	その他
2007年	433	112	75	34	43
2008年	420	62	90	36	52
2009年	368	42	68	28	53

・個人宅や、外出先、通勤／帰宅途中は減少傾向である一方、立ち寄った先での事故が増えている。

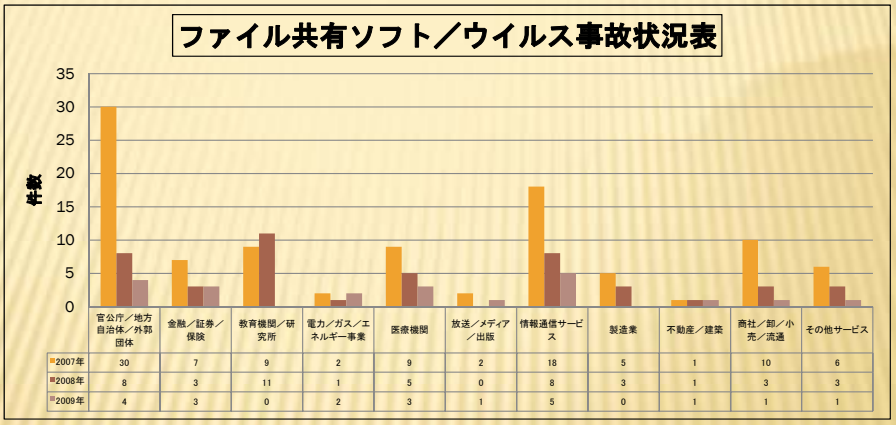
⑤過去３年間のシステム障害／脆弱性事故状況



	官公庁／地方自治体／外郭団体	金融／証券／保険	教育機関／研究所	電力／ガス／エネルギー事業	医療機関	放送／メディア／出版	情報通信サービス	製造業	不動産／建築	商社／卸／小売／流通	その他サービス
2007年	3	1	2	0	0	5	7	2	0	6	2
2008年	7	0	3	0	0	3	12	3	1	10	6
2009年	1	0	2	0	0	1	13	1	0	5	2

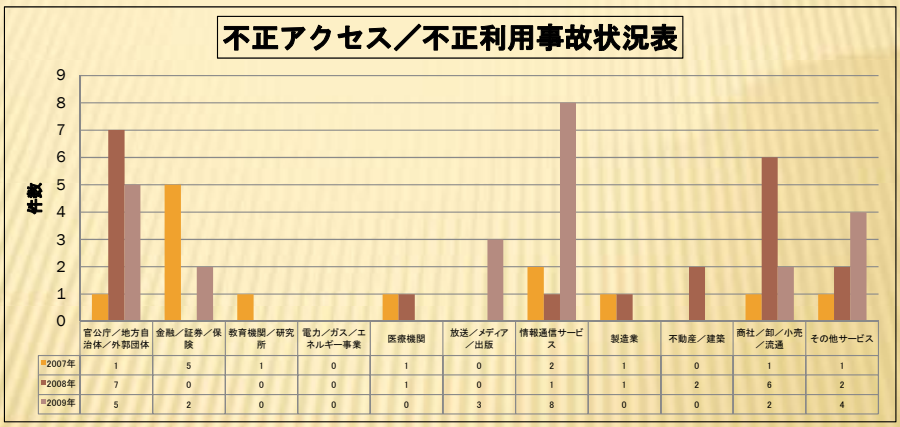
・システム障害／脆弱性事故において情報通信サービス業界が増加傾向。

⑥過去３年間のファイル共有ソフト／ウイルス事故状況



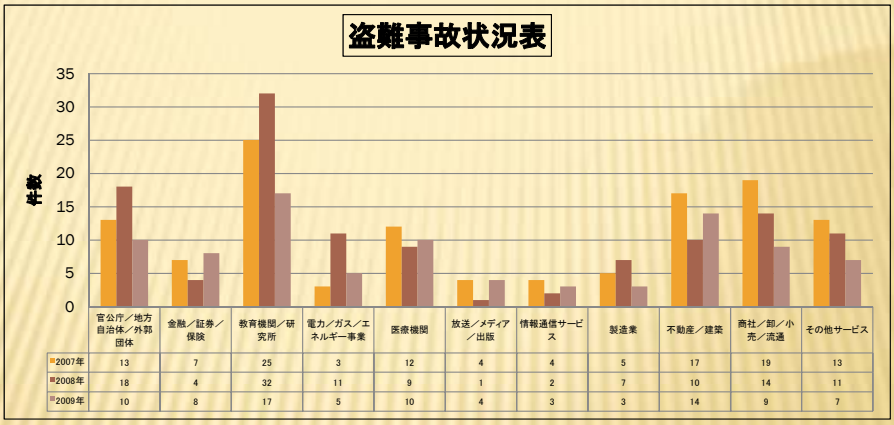
・教育機関の2009年は【ファイル共有ソフト】による事故が0件であった。

⑦過去３年間の不正アクセス／不正利用事故状況



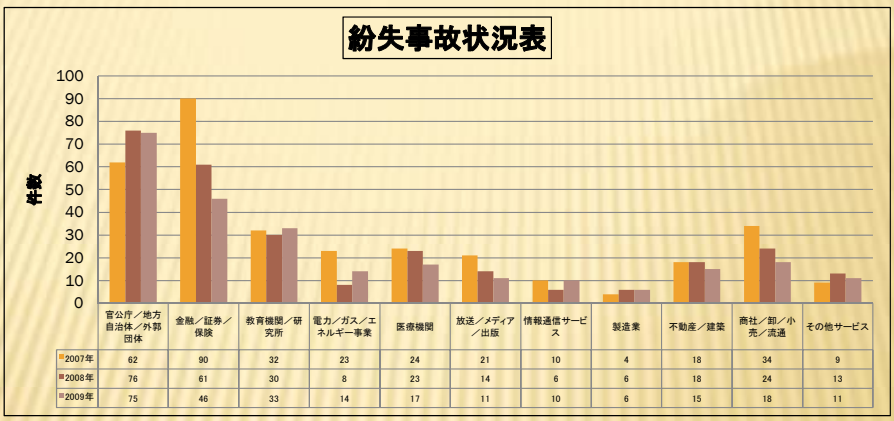
・不正アクセス／不正利用事故は大惨事に繋がっている。

⑧過去３年間の盗難事故状況

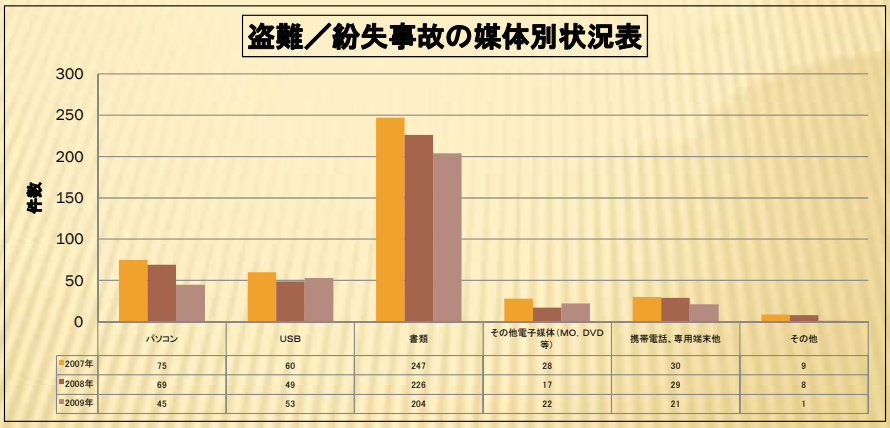


・教育機関は3年連続トップではあるが大幅に減少している。

⑨過去３年間の紛失事故状況

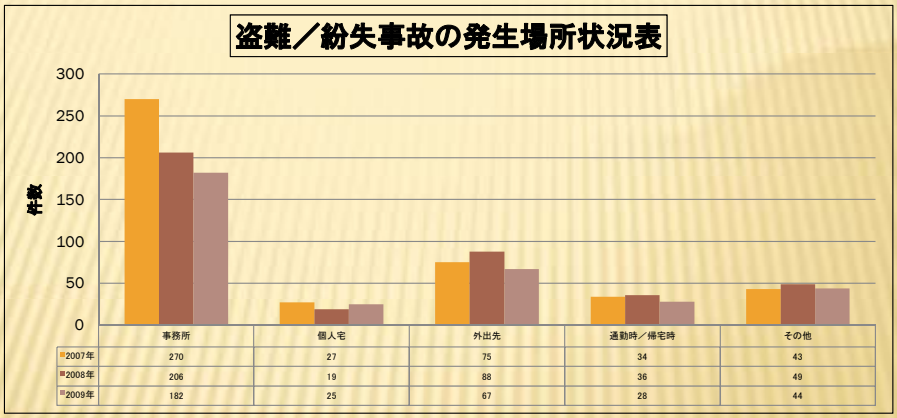


⑨－１　盗難／紛失事故の媒体別状況



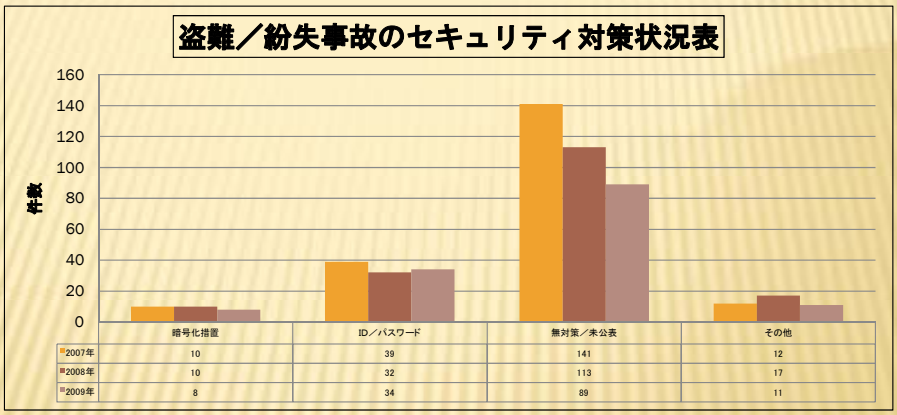
	パソコン	USB	書類	その他電子媒体（MO、DVD等）	携帯電話、専用端末他	その他
2007年	75	60	247	28	30	9
2008年	69	49	226	17	29	8
2009年	45	53	204	22	21	1

⑨－２　盗難／紛失事故の発生場所状況

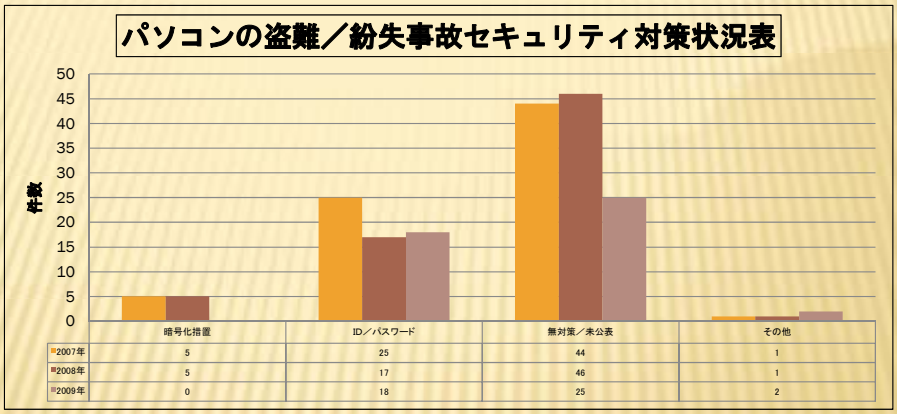


	事務所	個人宅	外出先	通勤時／帰宅時	その他
2007年	270	27	75	34	43
2008年	206	19	88	36	49
2009年	182	25	67	28	44

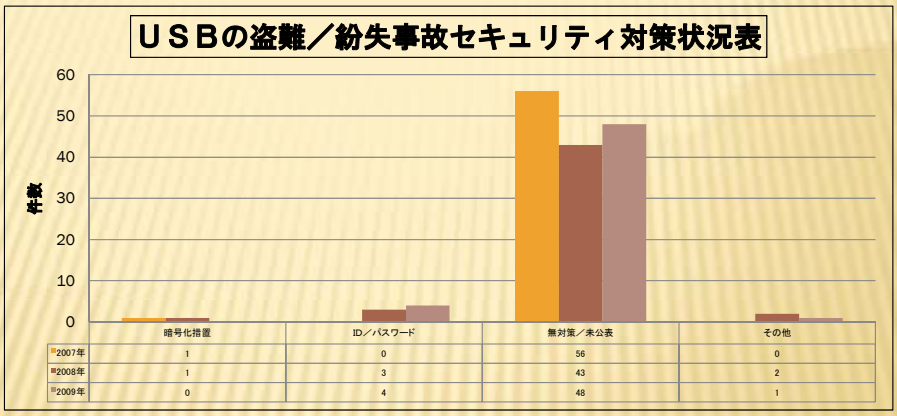
⑨－３　盗難／紛失事故のセキュリティ対策状況



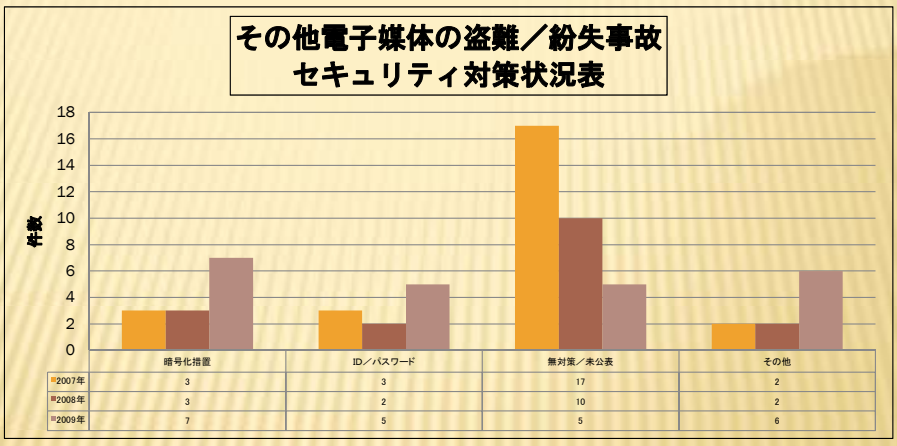
⑨－４　パソコンの盗難／紛失事故セキュリティ対策状況



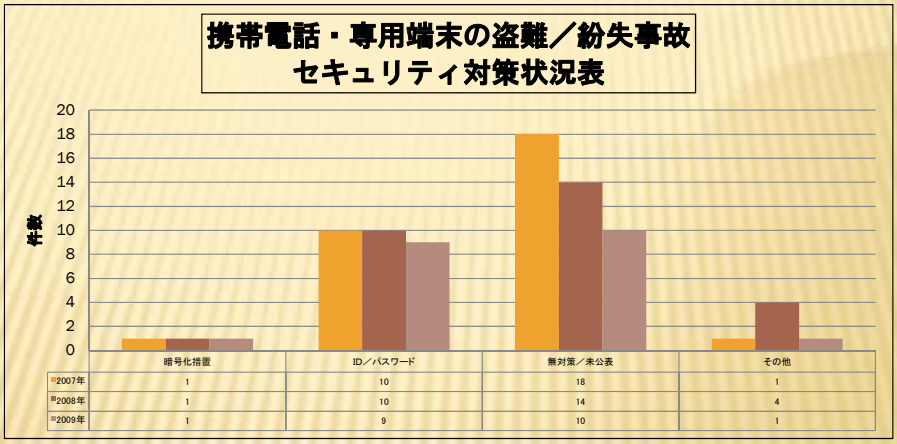
⑨－５　ＵＳＢの盗難／紛失事故セキュリティ対策状況



⑨－６　その他電子媒体の盗難／紛失事故セキュリティ対策状況

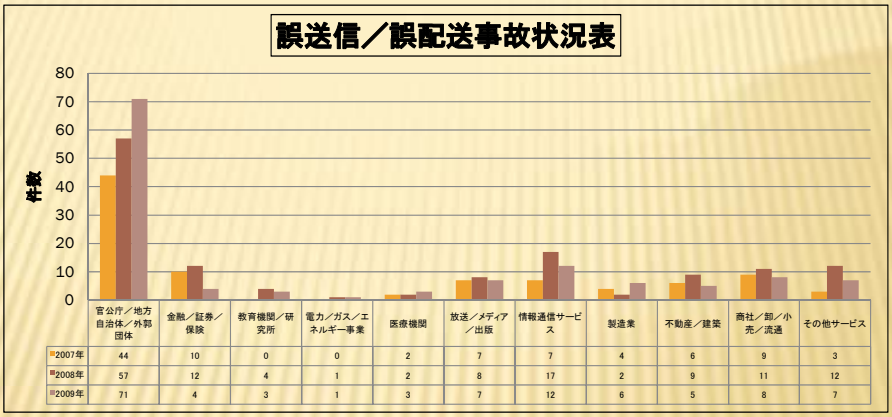


⑨－７　携帯電話・専用端末の盗難／紛失事故セキュリティ対策状況



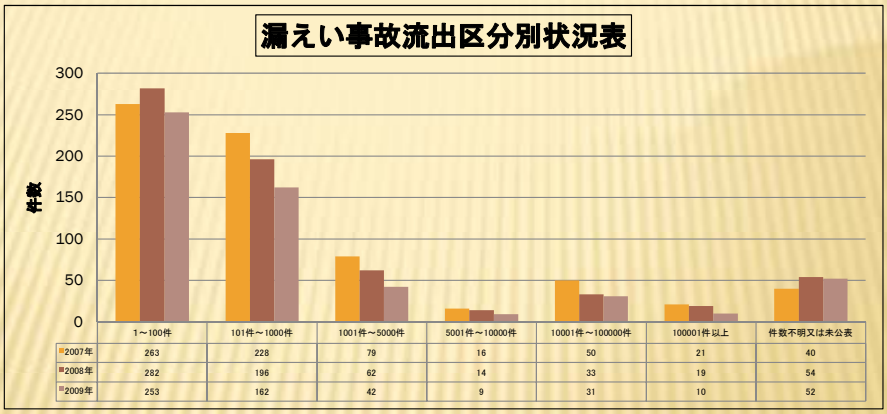
	暗号化措置	ID／パスワード	無対策／未公表	その他
2007年	1	10	18	1
2008年	1	10	14	4
2009年	1	9	10	1

⑩過去３年間の誤送信／誤配送事故状況



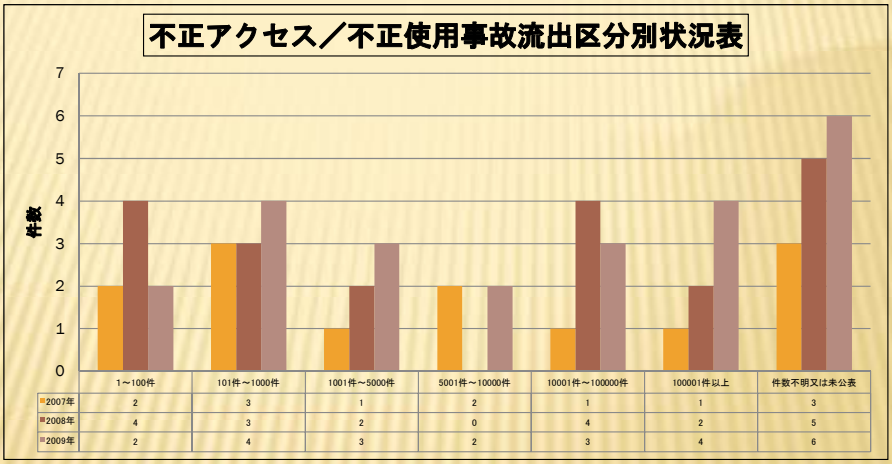
	官公庁／地方自治体／外郭団体	金融／証券／保険	教育機関／研究所	電力／ガス／エネルギー事業	医療機関	放送／メディア／出版	情報通信サービス	製造業	不動産／建築	商社／卸／小売／流通	その他サービス
2007年	44	10	0	0	2	7	7	4	6	9	3
2008年	57	12	4	1	2	8	17	2	9	11	12
2009年	71	4	3	1	3	7	12	6	5	8	7

⑪過去３年間の漏えい事故流出区分別状況



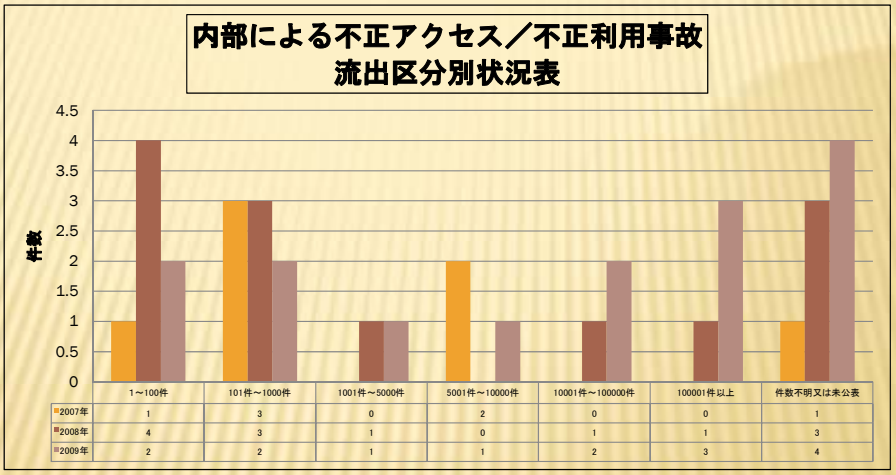
	1～100件	101件～1000件	1001件～5000件	5001件～10000件	10001件～100000件	100001件以上	件数不明又は未公表
2007年	263	228	79	16	50	21	40
2008年	282	196	62	14	33	19	54
2009年	253	162	42	9	31	10	52

⑪－１　不正アクセス／不正利用事故流出区分別状況



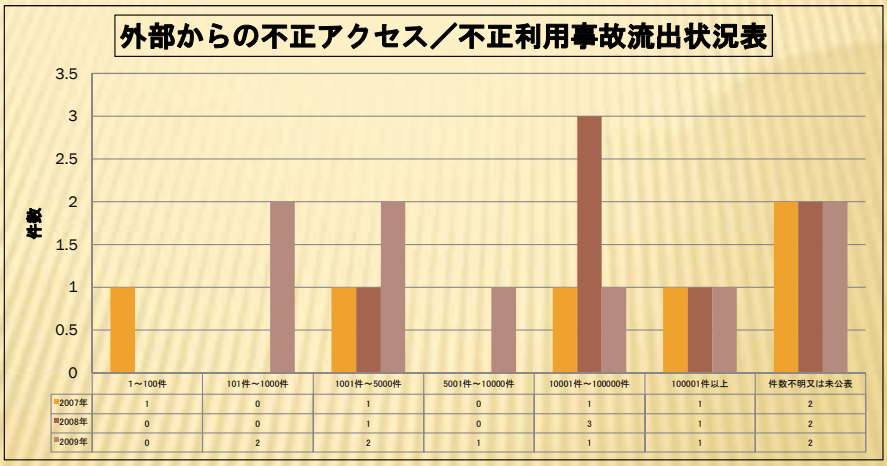
	1～100件	101件～1000件	1001件～5000件	5001件～10000件	10001件～100000件	100001件以上	件数不明又は未公表
2007年	2	3	1	2	1	1	3
2008年	4	3	2	0	4	2	5
2009年	2	4	3	2	3	4	6

⑪－２　内部による不正アクセス／不正利用事故流出区分別状況



・大量流出の事故が増加している。 危険！

⑪－３　外部からの不正アクセス／不正利用事故流出区分別状況



漏えい事故が起こるのは、個人の問題か？組織の問題か？

－ 事故発生の根本的な要因はなにか？ －

●個人情報保護に関する社内規程が整備されているにも関わらず遵守されていないのはなぜ？
漏えい事故の報告では、組織では〇〇を禁止していたが無断で〇〇したと公表しているが、本当に当事者だけの責任でしょうか？

・個人の問題

①事故による社会的な影響の認識が希薄。
②自分は大丈夫という慢心
③いちいちルールを守っていると仕事ができないという自己都合判断
④自己管理の問題（仕事の段取りがわるい）

・社内を見渡してみましょう

①業務手順と実務が合っていますか。（社内の規定が遵守されない）
②業務の負荷が担当者に偏っていませんか。（操作ミス）
③タイトなスケジュールで結果を要求していませんか。（自宅での作業）
④社員が会社、上司、同僚などに不満を持っていませんか。（不正持ち出し）

ＥＣにおける個人情報保護に関する活動報告書２００９

平成２２年　３月　発行

発　行　　次世代電子商取引推進協議会

販　売　　財団法人　日本情報処理開発協会
東京都港区芝公園三丁目５番８号
機械振興会館３階
TEL：０３（３４３６）７５００

この資料は再生紙を使用しています。

ISBN978-4-89078-683-1 C2036