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

～発生確率編～

第 1.0 版

2012 年 12 月 27 日

NPO 日本ネットワークセキュリティ協会
セキュリティ被害調査ワーキンググループ

もくじ

JNSA 調査研究部会 セキュリティ被害調査ワーキンググループ

ワーキンググループリーダー

大谷	尚通	株式会社 NTT データ(※)

メンバー

井口	洋輔	株式会社損保ジャパン・リスクマネジメント
猪俣	朗	トレンドマイクロ株式会社
大溝	裕則	株式会社 JMC(※)
岡本	一郎	株式会社 インフォセック
川上	昌俊	株式会社ラック(※)
北野	晴人	日本オラクル株式会社(※)
田中	洋	株式会社 インフォセック(※)
広口	正之	リコージャパン株式会社(※)
丸山	司郎	株式会社ラック(※)
山田	英史	株式会社ディアイティ(※)

（※）：報告書 執筆担当者　　無印：検討～レビューの担当者

著作権・引用について

本報告書は、NPO 日本ネットワークセキュリティ協会（JNSA） セキュリティ被害調査ワーキンググループが作成したものである。著作権は当該 NPO に属するが、本報告書は公開情報として提供される。ただし、全文、一部にかかわらず引用される場合は、「(引用) JNSA 情報セキュリティインシデントに関する調査報告書 ～発生確率編～ (2011 年)」と記述して欲しい。なお、報告書の文書を改変して使用する、あるいは報告書内の集計データを独自に再編して新たなグラフを作成するなど、報告書内の情報を加工して使用する場合は「引用」ではなく「参考」と表記していただきたい。

また、書籍、雑誌、セミナー資料などに引用される場合は、JNSA のホームページ上にある問い合わせフォームを利用してご連絡頂きたい。

1. エグゼクティブ・サマリー

1.1. インシデントの年間発生確率

2011 年の調査は、2010 年に比べて調査対象人数が大幅に増え、有効回答数が 2 万人を超えた。しかし算出された情報セキュリティインシデントの発生確率の値は、2010 年の調査結果から大きく変化は見られなかった。このことから 2010 年、2011 年ともに、十分な有効回答数を収集できていると考えられる。

最も発生確率が高い情報セキュリティインシデントは電子メールの誤送信で、10%を超えた。電子メールの誤送信は、ちょっとしたミスや気の緩みといったことが原因で、最も引き起こしやすいインシデントだといえる。また SNS による情報漏えいは、今後、企業において SNS の活用が促進されたり、個人の利用が普及するのにしたがって増加する恐れがある。今後も、SNS による情報漏えいなどのインシデントの推移を見守る必要がある。

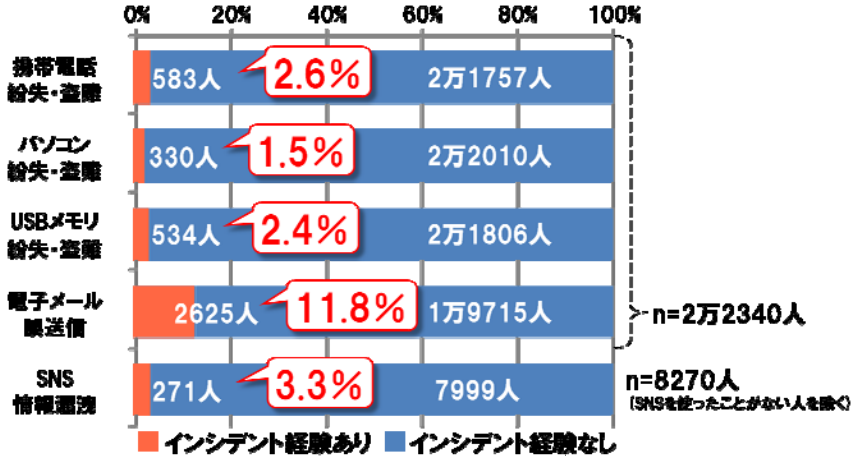


図 1-1：各インシデントの年間発生確率

この情報セキュリティインシデントの年間発生確率の値は全国平均であるため、自組織の業種や対策の実施状況によって、年間発生確率は異なると考えられる。相応の対策を実施している組織は、当然これより低い値である可能性が高い。したがって、自組織の年間発生確率を計測していない組織は、この値をひとつの目安として、自組織の年間発生確率の予測やリスク試算などに活用していただきたい。情報セキュリティインシデントの発生確率の値は、リスク試算などに活用することによって、対策投資効果の推定や、対策投資額の適正化などに役立てていくことができる。

各種対策によって発生確率を小さくすることはできるものの、発生確率の値がゼロになることはありえない。必ずインシデントは起きると想定し、事後対応によって被害を最小にとどめるようなセキュリティ対策を検討・実施して欲しい。

1.2. インシデントと個人特性

2012 年の調査では、個人特性とインシデントの発生の関係に注目した。情報セキュリティの知識がある人は、情報漏えいなどのインシデントをおこしにくいのではないか。忘れ物をしやすい人は、携帯電話や USB メモリなどを紛失しやすいのではないか。これらの仮説を検証するために、個人の知識、行動、性格の情報も取得し、各種インシデント経験の有無を分析した。

1.2.1. 性格とセキュリティインシデントの関係

「きちょうめんな/大雑把な」「悲観的な/楽天的な」「生真面目な/いい加減な」「慎重な/おっちょこちょいな」の 4 つの性格の例と 5 種類のインシデントを分析した。例えば、携帯電話の紛失・盗難の経験があるグループとその経験がないグループについて、きちょうめん／大雑把な性格による違いを分析したところ、以下のようになった。

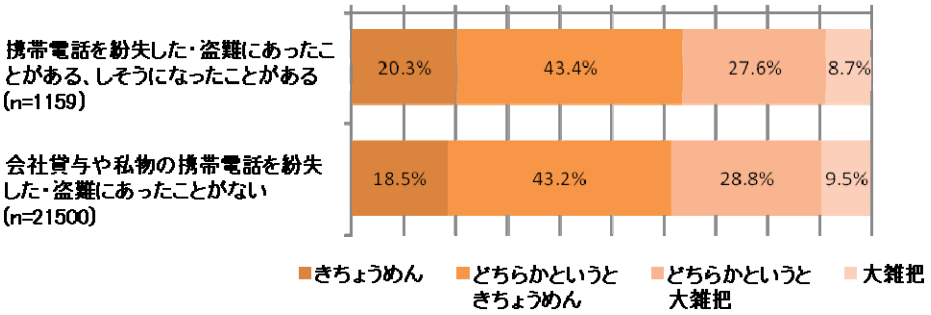


図 1-2：きちょうめん／大雑把な性格と携帯電話の紛失・盗難の関係

どちらのグループも、性格の違いによる割合がほとんど同じであった。つまり、携帯電話の紛失・盗難インシデントの経験と、きちょうめん／大雑把な性格との間には、顕著な関係がない事がわかった。さらに、携帯電話の紛失・盗難インシデントと残りの 3 つの性格の間にも、顕著な関係がない事がわかった。

パソコン/USB メモリの紛失・盗難インシデント、電子メールの誤送信、SNS での機密情報漏えいと性格の間にも、顕著な関係が見つからなかった。よって、セキュリティインシデントの発生と性格は関係性が低いといえる。「おっちょこちょいな人はメールを誤送信しやすい」という仮説は棄却された。

1.2.2. 行動とセキュリティインシデントの関係

「遅刻」「約束の勘違い」「整理整頓」「忘れ物」「居眠り」「ウェブサーフィン」「SNS 書き込み」「雑談」の 8 つの行動の例と 5 種類のインシデントを分析した。例えば、携帯電話の紛失・盗難の経験があるグループとその経験がないグループについて、8 つの行動特性による違いを分析したところ、以下のようになった。

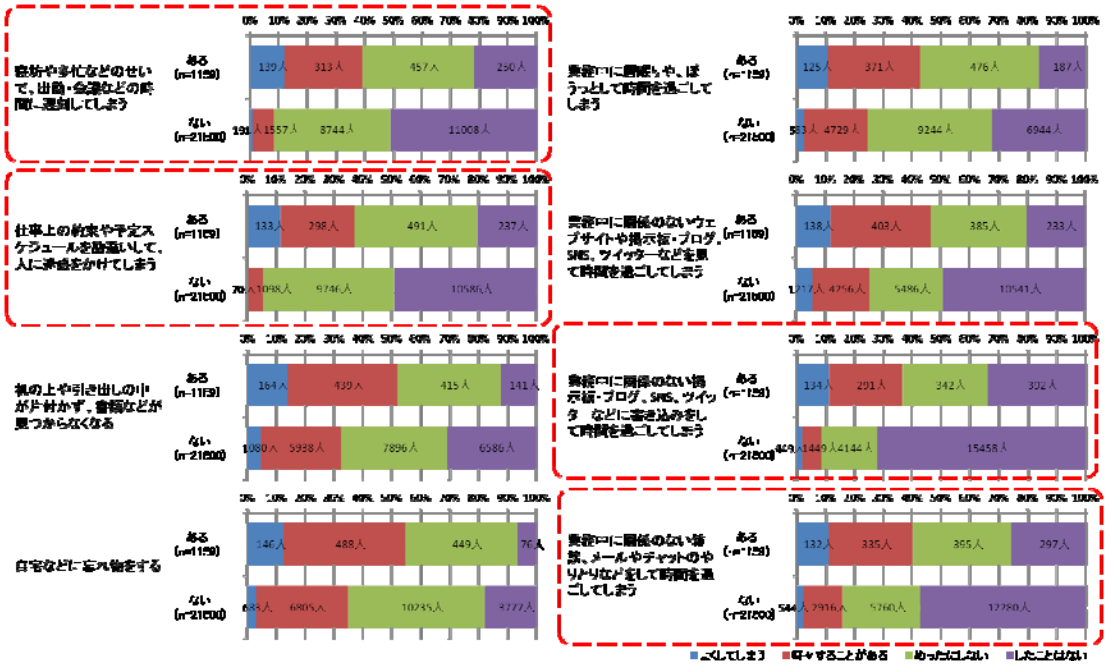


図 1-3：行動特性と携帯電話の紛失・盗難経験の関係

携帯電話の紛失・盗難の経験があるグループと経験がないグループの間には、「遅刻」「約束の勘違い」「SNS 書き込み」「雑談」の 4 つの行動に関して顕著な違いがあった。残りの「整理整頓」「忘れ物」「居眠り」「ウェブサーフィン」の 4 つの行動に関しては、携帯電話の紛失・盗難の経験があるグループと経験がないグループの間に顕著な違いがなかった。よって、「遅刻」「約束の勘違い」「SNS 書き込み」「雑談」の 4 つの行動とる人は、行動しない人に比べて携帯電話の紛失・盗難を起こす確率が高いと思われる。

パソコン/USB メモリの紛失・盗難インシデント、電子メールの誤送信、SNS での機密情報漏えいと行動の関係も分析したところ、携帯電話の紛失・盗難と同様、「遅刻」「約束の勘違い」「SNS 書き込み」「雑談」の 4 つの行動に関してのみ、顕著な違いがあった。「遅刻」「約束の勘違い」「SNS 書き込み」「雑談」の行動とる人は、行動しない人に比べて全般的にインシデントを起こす確率が高い事がわかった。

情報セキュリティインシデントの発生と特定の行動の間には、関係性が高いと思われる。

1.2.3. 知識とセキュリティインシデントの関係

IT 用語、セキュリティ用語、セキュリティ&IT 用語について、それぞれ 5 段階の難易度別の専門用語を用いて知識を調査し、インシデントの経験があるグループとその経験がないグループについて、知識の有無による違いを分析した。例えば、携帯電話の紛失・盗難の経験があるグループとその経験がないグループについて、知識の有無との関係を分析したところ、以下のようになった。

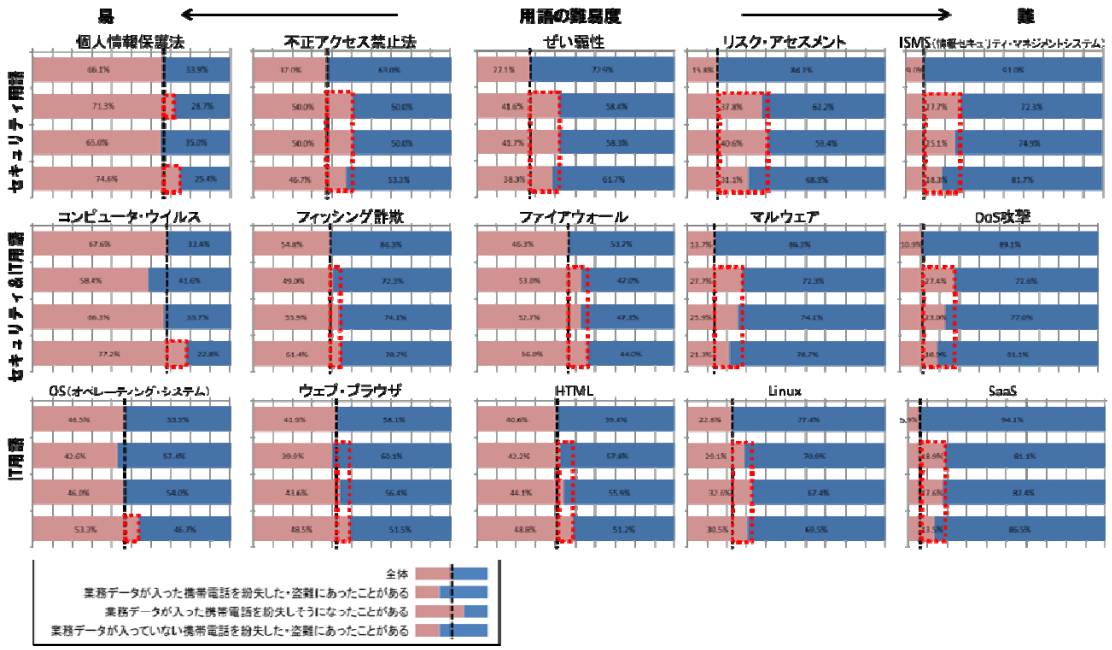


図 1-4：携帯電話の紛失・盗難と知識の関係

IT やセキュリティに関する知識がある人の方が、インシデントを起こしにくいと思われているが、分析した結果、難易度の高い IT 用語やセキュリティ用語を知っている人のグループのほうが、携帯電話の紛失・盗難の経験者の割合が高かった。

パソコン、USB メモリの紛失・盗難についても、IT やセキュリティの難易度が高い用語を知っている人のほうが、紛失・盗難の経験者の割合が高かった。ただし、電子メールの誤送信、SNS への機密情報の書き込みのインシデントは、IT やセキュリティの専門用語の知識とインシデントの経験との間に関係がなかった。

1.2.4. まとめ

2012 年の調査および分析の結果、性格および知識と情報セキュリティインシデントの発生確率との関係性は低いことがわかった。つまり、情報セキュリティインシデントを起こしやすい人は、性格や知識といった内面性から判断することは難しいと思われる。

一方、一部の行動は、情報セキュリティインシデントの発生確率と関係が高いことがわかった。客観的にわかる一部の行動は、情報セキュリティインシデントを起こしやすい人を判断する手がかりになると思われる。

2. アンケートの実施概要

2.1. 調査目的

JNSA セキュリティ被害調査 WG では、一般に公開されたインシデントの情報を集計し各種統計分析を行う「情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～」を過去数年にわたり作成・公表してきている。上記のレポートは、企業が把握しかつ公表に至ったインシデント、または各種メディアが報道したインシデントを情報源としていることから、世間の実態との乖離が懸念されている。実際、企業の情報セキュリティ管理への取り組み姿勢によって、把握できているインシデントや公表するインシデントの数に大きな乖離があることが分かっている。

そこで、より高い精度で情報セキュリティインシデントの実態を把握する手段の一つとして、2010 年より就業者を対象とした情報セキュリティインシデントのアンケート調査を行っている。

2011 年分の調査では、2010 年分の調査から調査項目を一部変更、追加した。以下に変更、追加項目の例を示す。

- 調査対象期間は、2011 年 1 月 1 日～12 月 31 日の 1 年間分
- 「落としそうになった」 場合を別項目へ分離
- 個人特性に関する質問項目を追加
- FAX の誤送信に関する設問を削除
- SNS のインシデントに関する設問を追加

2.2. 調査方法

マーケティング調査会社に依頼し、「予備調査」と「本調査」の 2 段階に分けた Web アンケート方式の調査を行った。

■ 調査期間：2012 年 1 月 31 日(火)～2012 年 2 月 3 日(金)

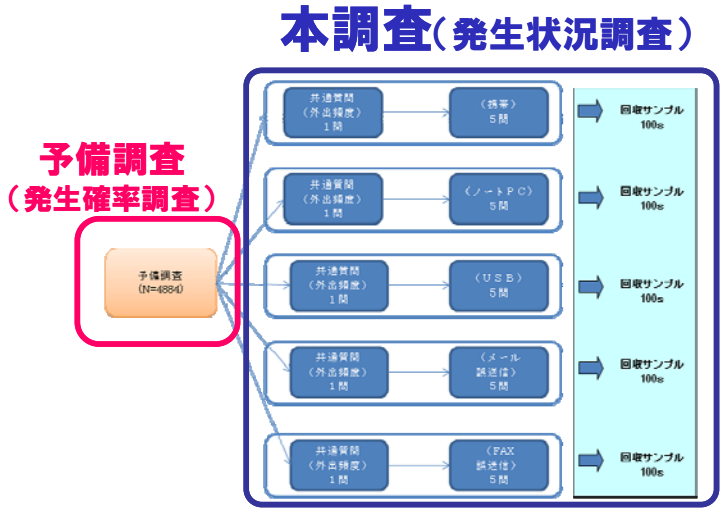


図 2-1：調査方法

2.3. 予備調査

まず予備調査として、調査対象をインシデントの経験者のみに絞り込むため、図 2-1 に示す 5 種類の情報セキュリティインシデント（①携帯電話／②ノート PC／③USB メモリの紛失、④電子メールの誤送信、⑤SNS への不適切な書き込み）を経験したことがある人を対象に各々のサンプル数が 100 件になるまで回答を収集した。

その際、5 種類の調査項目の各々において、母集団の出現率が均等になるよう 18 歳～29 歳、30 歳～39 歳、40 歳～49 歳、50 歳以上の 4 つの年齢層について均等に 25 名ずつ、労働力人口を参考に男性 15 名、女性 10 名の割合で合計 100 名となるよう割付を行っている。また、仕事をしている人のみを調査対象とするため、学生、無職・休職中・求職中、その他の人は対象から除外している。

■ 予備調査の有効回答者数：26162 人

調査分析には、有効回答者数から「学生」「無職・休職中・求職中」「その他」を除いた人数が 22340 人のデータを使用した。

表 2-1：職業・職種（予備調査 N=22340）

No	職業・職種	回答者数	割合(%)
1	会社経営者・役員・団体役員	765 人	2.9%
2	会社員・団体職員（正社員）	10740 人	41.1%
3	会社員・団体職員（契約・派遣）	1971 人	7.5%
4	地方公務員	953 人	3.6%
5	国家公務員	195 人	0.7%
6	自営業・個人事業主・フリーランス	2804 人	10.7%
7	自由業（開業医・弁護士事務所経営・プロスポーツ選手など）	405 人	1.5%
8	パート・アルバイト・フリーター	4507 人	17.2%
9	学生	0 名	0.0%
10	無職・休職中・求職中	0 名	0.0%
11	その他	0 名	0.0%

表 2-2：年齢層（予備調査 N= 22340）

No	年齢層	回答者数	割合(%)
1	18～29 歳	2709 人	12.1%
2	30～39 歳	5031 人	22.5%
3	40～49 歳	7706 人	34.5%
4	50 歳以上	6894 人	30.9%

2.4. 本調査

本調査では、予備調査で抽出された母集団を対象に、具体的にインシデントが発生した原因や、状況、実施していた対策の内容及びインシデント発生後の対応についてより掘り下げた調査を実施している。

3. トピック

3.1. 社員が紛失や誤送信する確率

予備調査から判明した 5 種類の情報セキュリティインシデント（携帯電話／ノート PC／USB メモリの紛失、電子メールの誤送信、SNS での機密情報漏えい）の経験者数とその割合を図 3-1 に示す。

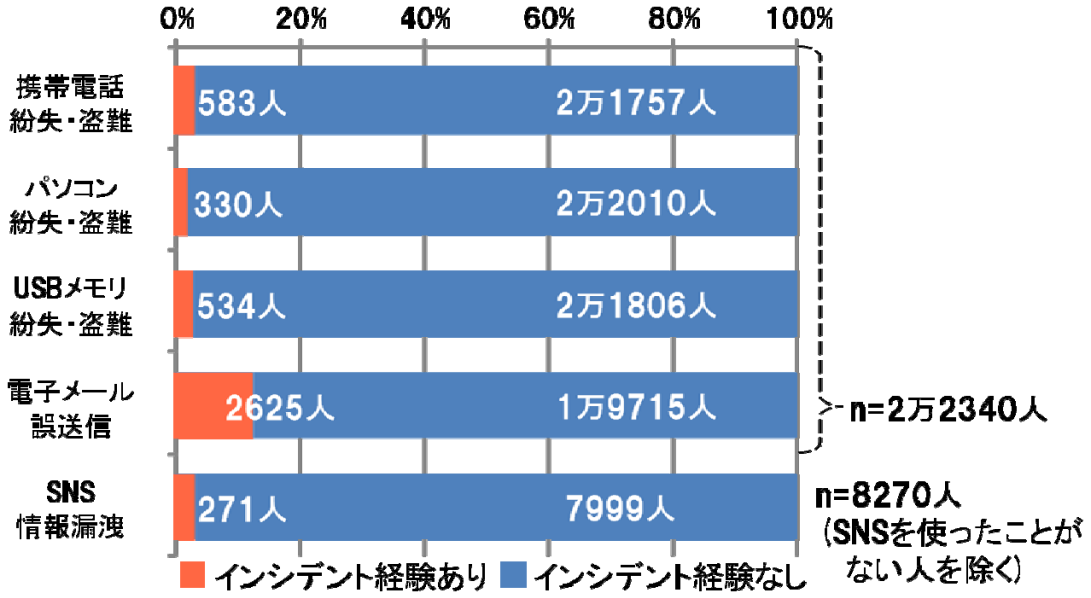


図 3-1：情報セキュリティインシデントの経験者数と割合

この情報セキュリティインシデントの経験者の割合と、本調査から判明した情報セキュリティインシデントの発生年の情報から、単年の情報セキュリティインシデントの年間発生確率を算出した。2009 年の推定値と、2010 年と 2011 年の年間発生確率を表 3-1 に示す。

表 3-1：紛失・盗難、誤送信の年間発生確率

調査対象	2009 年	2010 年 (N=4884)	2011 年 (N=22340)
携帯電話	6.6%	6.4%	2.6%
パソコン	3.1%	3.7%	1.5%
USB メモリ	4.1%	4.7%	2.4%
電子メール	17.1%	40.3%	11.8%
FAX	12.1%	39.0%	－
SNS	－	－	3.3%

2011 年の調査は、質問の表現や調査項目を工夫してわかりやすくしたため、2010 年と比べて、やや数値が変化した。ただし、2010 年調査時の回答人数 4884 人より大幅に多い、22340 人の回答を得られたことと、質問の表現や調査項目を工夫してわかりやすくしたことから、得られた数値の精度は向上したと予想する。特に電子メールの誤送信の数値は、2010 年の質問項目に誤解される恐れがある箇所があり、それを修正したため、大きく数値が変化したと思われる。

3.1.1. 携帯電話

予備調査から、携帯電話を紛失したおよび盗難にあった人は 583 人であった。母数 22340 人から、携帯電話の紛失・盗難の確率は、約 2.6%であることがわかった。社員 100 人あたりに換算すると、年間 2.6 人が会社貸与または私物の携帯電話を紛失していることになる。たとえば、社員 200 人の会社の情報セキュリティ担当者は、1 年間に 5 回程度、携帯電話の紛失インシデントに対応すると予想し、必要な年間予算や稼働を見積っておくべきである。

3.1.2. パソコン、USB メモリ

パソコンの紛失・盗難のインシデント発生確率は 1.5%であり、携帯電話や USB メモリと比較して低い値となった。USB メモリの紛失・盗難のインシデント発生確率は 2.4%であり、携帯電話のインシデント発生確率と近い値であった。デバイスの大きさが小さい USB メモリが一番、紛失しやすいと思われるだろうが、実際は、携帯電話のインシデント発生確率が一番高く、USB メモリ、パソコンの順であった。USB メモリは携帯電話より小さいが、社内での使用が制限されたり、社外へ持ち出すことが少なくなったりしため、携帯電話よりも紛失確率が低いと思われる。

2009 年の推定値、2010 年と 2011 年の発生確率の値ともに、インシデント発生確率はこの順序関係であった。すなわち、調査時のデバイスの使用状況や技術の変化に応じて値が変化しても、発生確率の値の大小関係は、しばらくはこの順序関係が保たれると思われる。

3.1.3. 電子メール

メールの誤送信が発生しても、通常、高額な損害賠償には至らない。これは、ほとんどの場合、誤送信先が固定かつ特定可能で、影響範囲が特定しやすく、回収や削除の依頼も可能だからである。したがって、メール誤送信から、二次漏えいによる被害拡大は発生しにくく、被害額も小さい。

メール誤送信の発生確率は、調査した 5 つのインシデントの中で最も高く 11.8%であった。メールの誤送信は、発生確率こそ最も高いが、大きなリスクではないと考えている。メー

ルの誤送信は、ほとんどの場合、誤送信先が固定明確で、かつ特定可能である。そのため、影響範囲が特定しやすく、誤送信したメールの回収や削除の依頼もほとんど可能だからである。したがって、メール誤送信から、二次漏えいによる被害拡大は発生しにくく、被害額も小さい。。つまり、メールの誤送信は、比較的容易にインシデントの収拾が可能である。

2011 年の調査では、質問の表現や調査項目を工夫してわかりやすくしたため、2010 年と比べて、やや数値が変化した。これは、2010 年の質問項目に誤解される恐れがある箇所があり、それを修正したため、大きく数値が変化したと思われる。

3.1.4. SNS

SNS の不適切な書込みの年間発生確率(1.2%)は、メール誤送信の年間発生確率(11.8%)より低い。しかし、SNS の不適切な書込みは、なかなか事態を終息できなかったり、損害賠償が発生したりした事例があるなど、インシデントが発生した場合のリスクが大きい。これは、情報の閲覧者が不特定多数であり、情報の漏洩、拡散範囲の特定が困難であることが理由の一つである。このように、SNS の不適切な書込みは、影響範囲を特定できず、漏洩した情報の回収や削除も困難であることから、SNS の不適切な書込みは 1 回あたりの被害額は大きくなる。

3.2. 情報セキュリティ知識とインシデントの関係

情報セキュリティの知識や IT の知識の量によってインシデントの起こしやすさに違いがあるのかを調べるため、それぞれの知識を問う質問を行った。

3.2.1. インシデントの経験と知識の関係

アンケート対象者へ、次の 5 段階の難易度をもつ IT 用語、セキュリティ用語、セキュリティ&IT 用語について、他人へ大まかな説明ができる程度に知っているかどうかを調査した。

表 3-2：情報セキュリティ知識に関する質問項目

質問：あなたは、情報セキュリティや IT に関する以下の言葉について、他人に大まかな説明ができるくらいに知っていますか。（お答えはいくつでも）	
セキュリティ用語	個人情報保護法、不正アクセス禁止法、ぜい弱性、リスク・アセスメント、ISMS（情報セキュリティ・マネジメントシステム）
セキュリティ&IT 用語	コンピュータ・ウイルス、フィッシング詐欺、ファイアウォール、マルウェア、DoS 攻撃
IT 用語	OS（オペレーティング・システム）、ウェブ・ブラウザ、HTML、Linux、SaaS

母集団と、携帯電話／ノート PC／USB メモリの紛失・盗難、電子メールの誤送信、SNS での不適切な書き込みの各インシデントを経験したことがあるグループについて、上記の専門用語の既知／未知の割合を比較した。以下にその比較グラフを示す。専門用語は、難易度順に並べた。

(1). 携帯電話の紛失・盗難と知識の関係

インシデントを経験したことがあるグループは、「業務データが入った携帯電話を紛失した・盗難にあったことがある」「業務データが入った携帯電話を紛失しそうになったことがある」「業務データが入っていない携帯電話を紛失した・盗難にあったことがある」の 3 グループを用意した。この 3 グループについて、以下の 3 つの専門用語の既知／未知の割合を比較した。

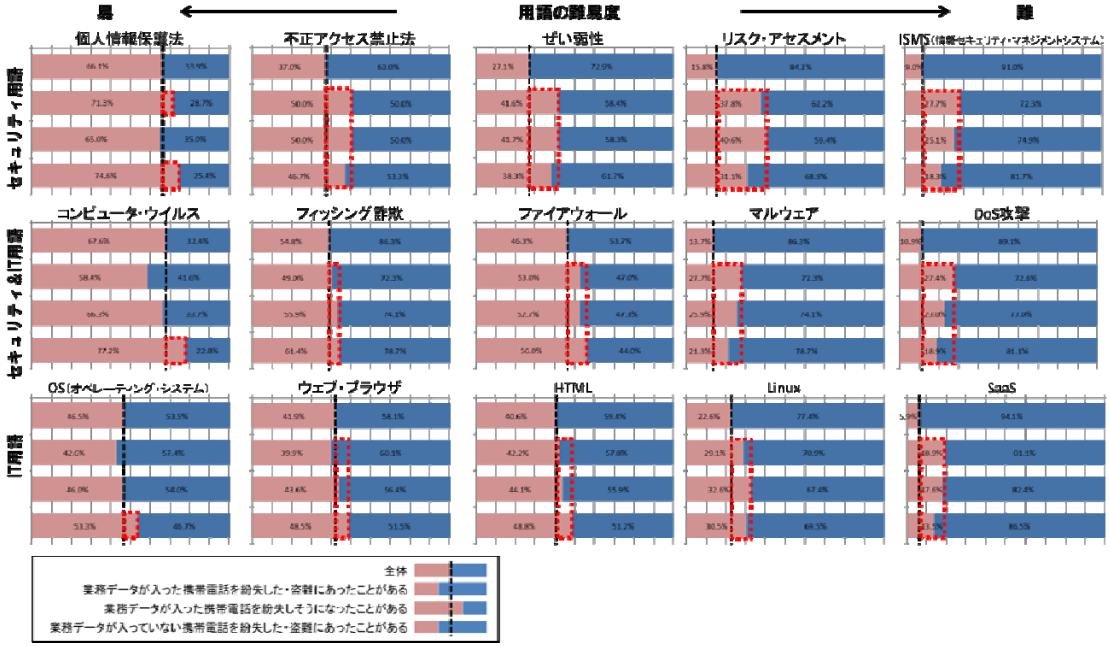


図 3-2：携帯電話の紛失・盗難と知識の関係

どの専門用語も、全体的に難易度が高い専門用語を知っている人ほど、携帯電話の紛失・盗難を経験する人の割合が母集団よりも高くなっている。特に「業務データが入った携帯電話を紛失した・盗難にあったことがある」グループは、その傾向がほぼきれいにあらわれている。一方、「業務データが入っていない携帯電話を紛失した・盗難にあったことがある」グループは、専門用語の難易度にかかわらず、携帯電話の紛失・盗難を経験する人の割合がほぼ一定である。

(2). パソコンの紛失・盗難の経験と知識の関係

インシデントを経験したことがあるグループは、「業務データが入ったパソコンを紛失した・盗難にあったことがある」「業務データが入ったパソコンを紛失しそうになったことがある」「業務データが入っていないパソコンを紛失した・盗難にあったことがある」の 3 グループを用意した。この 3 グループについて、以下の 3 つの専門用語の既知／未知の割合を比較した。

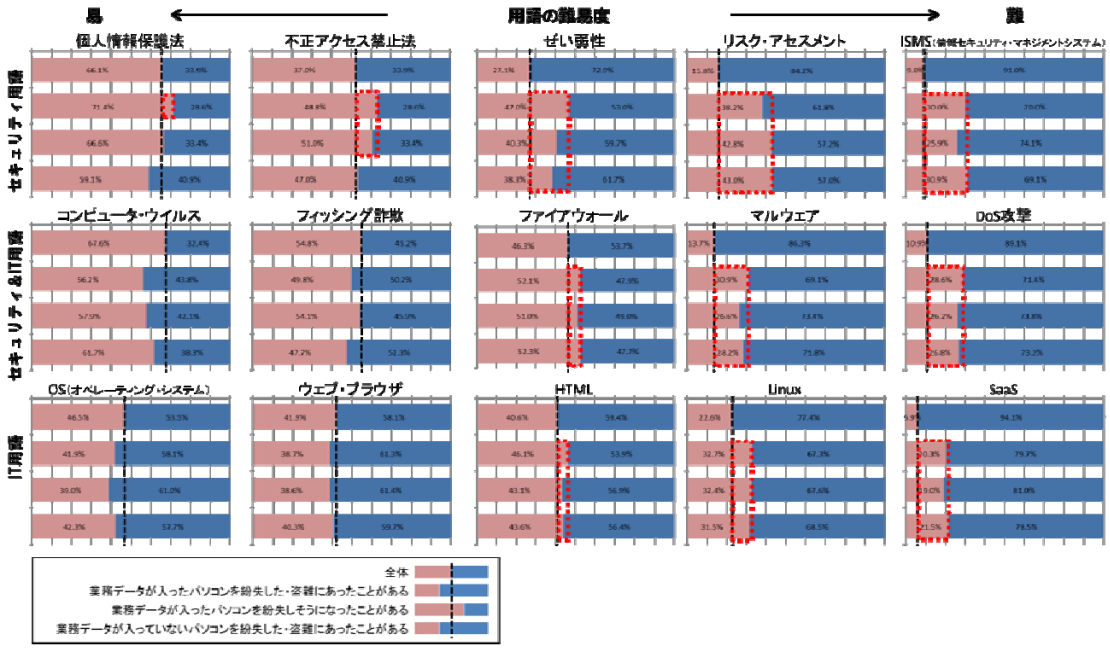


図 3-3：パソコンの紛失・盗難の経験と知識の関係

やはり、全体的に難易度が高い専門用語を知っている人ほど、パソコンの紛失・盗難を経験した人の割合が母集団よりも高くなる傾向がある。

セキュリティ＆IT 用語と IT 用語の難易度が低い専門用語を知っている人は、パソコンの紛失・盗難を経験した人の割合が母集団よりも低くなっている。つまり、少なくとも一般的なセキュリティ用語、IT 用語を知っている人は、平均よりもインシデントを起こしにくいと思われる。

(3). USB メモリの紛失・盗難経験と知識の関係

インシデントを経験したことがあるグループは、「業務データが入った USB メモリを紛失した・盗難にあったことがある」「業務データが入っていない USB メモリを紛失した・盗難にあったことがある」の 2 グループを用意した。この 3 グループについて、以下の 3 つの専門用語の既知／未知の割合を比較した。

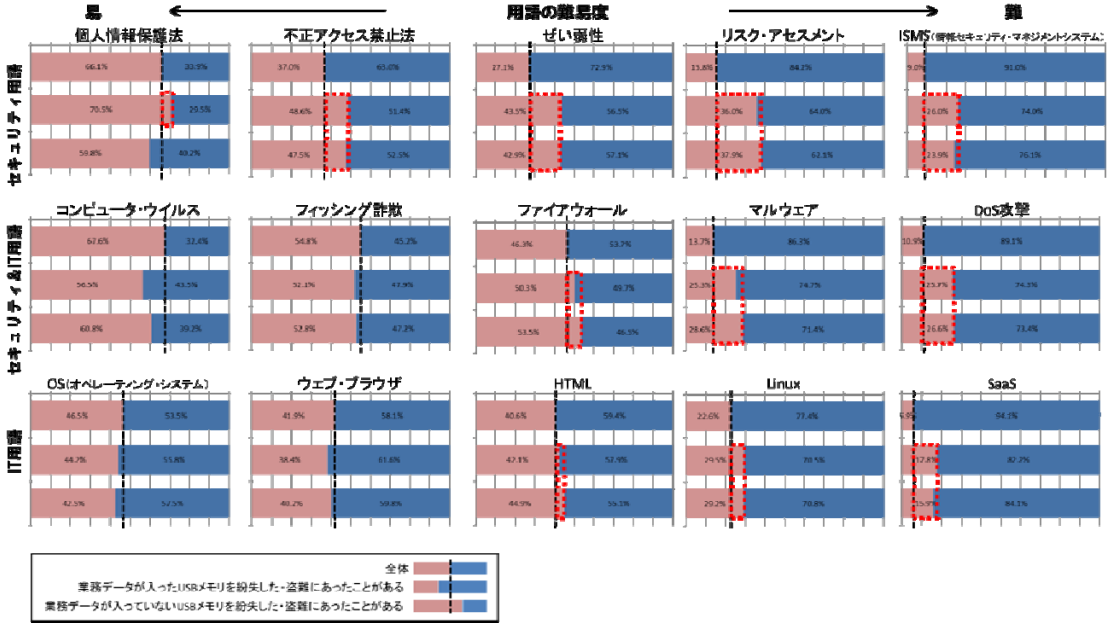


図 3-4：USB メモリの紛失・盗難経験と知識の関係

(4). 電子メールの誤送信経験と知識の関係

母集団と誤送信したことがあるグループを比較した。携帯電話／パソコン／USB メモリの紛失・盗難の場合と比較すると、専門用語の難易度と誤送信を経験した人の割合の関係には、明確な傾向がない。メールの誤送信と IT・セキュリティ知識の間には、明確な関係がないと思われる。

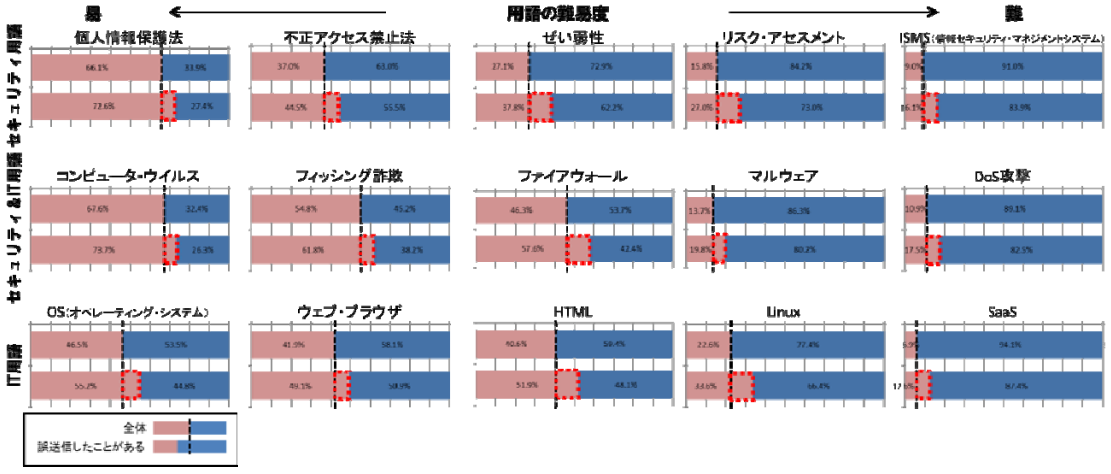


図 3-5：電子メールの誤送信経験と知識の関係

(5). SNS の不適切な書き込み経験と知識の関係

母集団と SNS で不適切な書き込みをしたことがあるグループを比較した。携帯電話／パソコン／USB メモリの紛失・盗難の場合と比較すると、専門用語の難易度と誤送信を経験した人の割合の関係には、明確な傾向がない。メールの誤送信と IT・セキュリティ知識の間には、明確な関係がないと思われる。

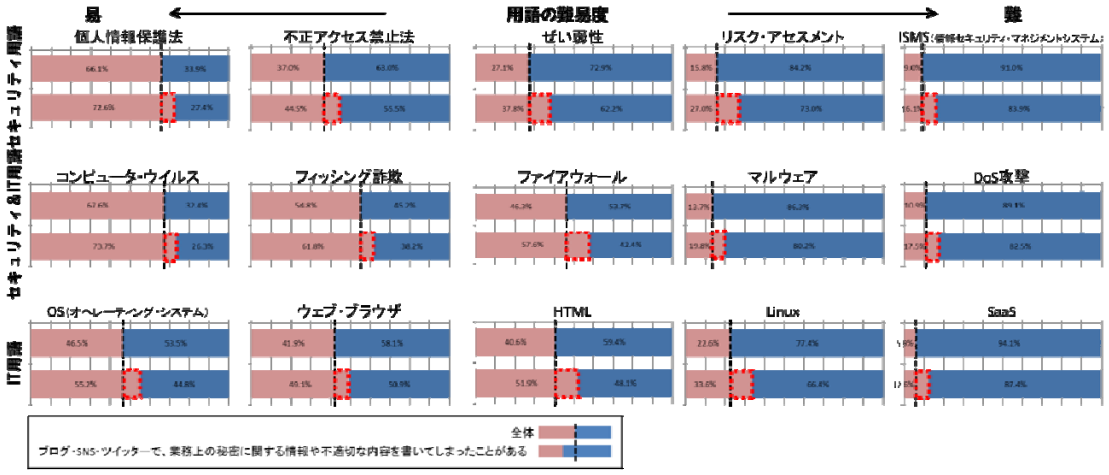


図 3-6：SNS の不適切な書き込み経験と知識の関係

(6). インシデントと知識の関係のまとめ

IT やセキュリティ知識を持っている人のほうが、パソコン、USB メモリも紛失・盗難の経験者の割合が高い。つまり、IT/セキュリティ知識を持っている人のほうが、デバイスの紛失・盗難の確率が高い。これは、IT/セキュリティ知識を持っている人のほうが、電子デバイスの保有率や使用頻度が高いため、紛失・盗難にあう確率が必然的に高くなるのではないだろうか。

電子メールの誤送信、SNS への不適切な書き込みは、IT/セキュリティ知識と経験者の割合の関係性が低い。

3.2.2. 情報セキュリティ知識と IT 知識の相関関係

情報セキュリティや IT の専門用語の既知/未知の状況を 10 点満点で採点し、情報セキュリティの知識と IT の知識の程度を測定した。情報セキュリティの知識の程度は、情報セキュリティ用語 5 個とセキュリティ＆IT 用語 5 個から、既知の専門用語の数を元に採点した。同様に、IT の知識の程度は、IT 用語 5 個とセキュリティ＆IT 用語 5 個から、既知の専門用語の数を元に採点した。

被験者 22340 人の情報セキュリティの知識の平均は 3.48 点、標準偏差は 2.74、IT の知識の平均点は 3.51 点、標準偏差は 3.04 となった。

表 3-3：情報セキュリティの知識と IT の知識の平均点と標準偏差(n=22340)

対象知識	平均点	標準偏差
情報セキュリティの知識（10 点満点）	3.48	2.74
IT の知識(10 点満点)	3.51	3.04

情報セキュリティの知識と IT の知識の相関係数は 0.898 となった。相関係数が大きいことから、情報セキュリティに関する知識量と IT に関する知識量には強い相関関係があると言える。このため、どちらか一方の傾向を分析すれば、もう一方の傾向も似た結果になると考えられる。情報セキュリティの知識と IT の知識には、強い相関があるため、以降は、情報セキュリティの知識に関する分析結果のみを記載する。

3.2.3. 情報セキュリティ・IT の知識が多い人はインシデントを起こしにくいのか

情報セキュリティ知識が多い人の方が、少ない人より情報セキュリティインシデントを起こしにくいというイメージがある。本当にそうだろうか。その疑問に答えるため、情報セキュリティの知識量とインシデントの発生確率の関係について分析した。

携帯電話、パソコン、USB メモリの紛失・盗難の有無や、メール・SNS でのインシデント経験の有無と情報セキュリティの知識に関する質問の平均点の関係を集計した結果を下表に示す。平均点以上の値は、赤字で示した。

表 3-4：インシデント経験と情報セキュリティ・IT の知識の平均点の関係

情報セキュリティインシデント経験		情報セキュリティ知識平均点（10 点満点）	IT の知識平均点（10 点満点）
携帯電話の紛失・盗難	ある	3.78	3.20
	しそうになったことがある	4.00	3.66
	両方	5.77	5.26
	ない	3.46	3.50
パソコンの紛失・盗難	ある	3.87	3.35
	しそうになったことがある	3.95	3.43
	両方	6.11	5.47
	ない	3.47	3.50
USB メモリの紛失・盗難	ある	4.35	3.82
	ない	3.47	3.50
電子メールでの宛先誤り、他人のメールアドレス送信、機密情報誤送信	誤送信をしたことがある	4.28	4.33
	誤送信したことはない	3.38	3.40
ブログ・SNS・ツイッターで業務上の秘密に関する情報や不適切な内容の記載	書いてしまったことがある	4.16	3.89
	書いてしまったことはない	4.16	4.39
	使ったことがない	3.09	3.00

パソコンの紛失・盗難に着目すると、紛失・盗難の経験がある人の情報セキュリティ知識は 3.87 と平均点より高い。また、両方（紛失・盗難しそうになったことがあり実際にしたこともある）と答えた人の情報セキュリティ知識は 6.11、IT 知識は 5.47 であり、さらに点数が高いことが分かる。携帯電話と USB メモリの紛失・盗難、電子メールの誤送信についても同様に、インシデント経験がある人の方が点数が高い傾向がある。SNS については、秘密に関する情報や不適切な内容を書いてしまったことがある人もない人も点数が高いが、使ったことがない人は点数が低い傾向がある。

SNS 以外は、どれも情報セキュリティ・IT 知識が多い人の方がインシデントを起こしやすいように見える。これは「情報セキュリティや IT の知識が多い人の方が情報セキュリティインシデントを起こしにくい」というイメージと逆の結果である。

では、なぜこのような結果になったのか。外出頻度と紛失確率の関係の分析結果から、携帯電話、パソコン、USB メモリを持って外出する頻度が高い方がそれらの紛失・盗難にあいやすいことが分かっている。そこで、外出頻度と知識の関係を分析した。

情報セキュリティ知識が平均点以上のグループを「情報セキュリティ知識高群」、平均点

未満のグループを「情報セキュリティ知識低群」と定義して、それぞれ携帯電話、パソコン、USB メモリを持って外出する頻度との関係を集計した。その結果を「表 3-5：携帯電話を持って外出する頻度と情報セキュリティの知識の平均点の関係」に示す。

表 3-5：携帯電話を持って外出する頻度と情報セキュリティの知識の平均点の関係

外出頻度	情報セキュリティ知識高（平均点以上）		情報セキュリティ知識低（平均点未満）	
毎日、外出(出張)し、頻繁に移動する	1018 人	9.76%	727 人	6.10%
毎日、外出(出張）するが、移動回数は少ない	266 人	2.55%	216 人	1.81%
１週間に 1～2 回程度、外出(出張)している	524 人	5.02%	291 人	2.44%
１ヶ月に 1～2 回程度、たまに外出(出張)する	279 人	2.67%	206 人	1.73%
ごく稀に外出(出張)する	461 人	4.42%	346 人	2.91%
会社貸与の携帯電話を持って外出(出張）しない	532 人	5.10%	592 人	4.97%
会社貸与の携帯電話を持っていない、使用していない	7350 人	70.47%	9532 人	80.03%
総計	10430 人		11910 人	

携帯電話を持って「毎日、外出(出張)し、頻繁に移動する」人は、情報セキュリティ知識高群の方が低群より約 290 人多く、割合で見ると 3.66%多い。それ以外でも、頻度を問わず、外出する人は情報セキュリティ知識高群の方が多い。逆に、「会社貸与の携帯電話を持っていない、使用していない」人は、情報セキュリティ知識高群の方が低群より約 2200 人少なく、割合で見ると 9.56%少ない。

同様にパソコンと USB メモリについても、知識が多い人の方が外出頻度が高い傾向にある。これは、外出が多いため、必要に迫られて携帯電話やノート PC 等を使うことが多く、その結果、携帯電話やノート PC、USB メモリの紛失や盗難のリスクが高くなる。そのため、そのリスクを減らすために、それらの取り扱いやセキュリティ対策の教育・研修が増え、知識が多くなったという可能性が考えられる。なお、ここでは情報セキュリティの知識についてのみ示したが、IT の知識についても同様の傾向があることが分かっている。

以上より、知識が多い人がインシデントを起こしやすいのではなく、

もともと外出頻度が高く、携帯電話、パソコン、USB メモリの紛失・盗難のインシデントが起きやすい人が、その対策の一環の教育によって知識は多くなっていると推測する。

メールの誤送信についても、知識が多い人の方がメールの使用頻度が高く、インシデントが起きやすいと予想されるが、今回のアンケートの内容からはそれを裏付けることはできなかった。

しかしながら、これらの結果から、情報セキュリティや IT の知識だけあっても、情報セキュリティインシデントを起こしにくいというわけではないと言える。

3.2.4. 教育・研修と誓約書によるインシデント数の減少

では、教育・研修を行うことは意味が無いのであろうか。本節では、教育・研修に加え、規定、ルール、誓約書などの職場対策の効果を調べるため、各情報セキュリティインシデントの経験と職場対策の関係について集計した結果を下表に示す。

表 3-6：セキュリティインシデント経験と職場対策の関係

		情報セキュリティについての規程類が定められている	職場のパソコンについて、外部への持ち出しを禁じるルール、または持ち出す際の手続きのルールが定められている	私物や業者のパソコンについて、職場への持ち込みを禁じるルール、または持ち込む際の手続きのルールが定められている	情報セキュリティ事故が起きた場合の、報告先や報告手続きのルールが定められている	従業員に対して情報セキュリティについての教育・研修が行われている	従業員に対して守秘義務についての誓約書などを提出させている
携帯電話の紛失・盗難	ある	52.02%	47.47%	32.83%	29.80%	23.74%	18.18%
	しそうになったことがある	42.39%	42.75%	44.57%	43.12%	38.77%	27.17%
	両方	69.39%	74.49%	69.39%	61.22%	46.94%	37.76%
	ない	39.58%	39.02%	30.17%	30.21%	31.57%	29.88%
パソコンの紛失・盗難	ある	61.44%	57.52%	38.56%	36.60%	28.76%	21.57%
	しそうになったことがある	40.71%	43.81%	47.79%	40.27%	33.19%	23.01%
	両方	75.00%	81.25%	71.88%	67.19%	48.44%	39.06%
	ない	39.59%	39.00%	30.19%	30.25%	31.62%	29.88%
USB メモリの紛失・盗難	ある	53.08%	57.53%	44.18%	41.10%	29.79%	22.95%
	ない	39.68%	39.05%	30.36%	30.36%	31.69%	29.87%
電子メールの誤送信	誤送信をしたことがある	51.09%	49.60%	39.28%	41.03%	41.14%	33.07%
	誤送信したことはない	38.36%	37.92%	29.38%	29.10%	30.40%	29.34%
SNS の不適切な書き込み	書いてしまったことがある	51.29%	48.34%	43.91%	37.64%	32.10%	23.62%
	書いてしまったことはない	41.34%	40.74%	31.73%	32.43%	33.12%	32.32%
	使ったことがない	38.78%	38.29%	29.61%	29.27%	30.82%	28.46%

携帯電話の紛失・盗難に着目すると、紛失・盗難経験がある人で、かつ「情報セキュリテ

ィについての規程類が定められている」と答えた人の割合は52.02%であった。これに対し、紛失・盗難経験がある人で、「従業員に対して情報セキュリティについての教育・研修が行われている」と答えた人の割合は 23.74%と低く、「従業員に対して守秘義務についての誓約書などを提出させている」と答えた人の割合は18.18%とさらに低い。つまり、携帯電話の紛失・盗難インシデントは、情報セキュリティの教育・研修によって減少し、守秘義務に関する誓約書を提出させることによって、さらに減少すると考えられる。

携帯電話以外でも同様の傾向があった。

以下に、情報セキュリティの知識が平均点以上の群と平均点未満の群の携帯電話の紛失・盗難インシデントと、セキュリティ教育や誓約書の関係を分析した結果を示す。

表 3-7：情報セキュリティの知識量と職場対策の有効性の関係

			情報セキュリティについての規程類が定められている	職場のパソコンについて、外部への持ち出しを禁じるルール、または持ち出す際の手続きのルールが定められている	私物や業者のパソコンについて、職場への持ち込みを禁じるルール、または持ち込む際の手続きのルールが定められている	情報セキュリティ事故が起きた場合の、報告先や報告手続きのルールが定められている	従業員に対して情報セキュリティについての教育・研修が行われている	従業員に対して守秘義務についての誓約書などを提出させている
携帯電話の紛失・盗難	セキュリティ知識高（平均点以上）	ある	66.29%	59.55%	55.06%	46.07%	40.45%	29.21%
		しそうになったことがある	66.18%	63.97%	57.35%	61.03%	57.35%	46.32%
		両方	78.79%	75.76%	78.79%	65.15%	59.09%	45.45%
		ない	49.69%	49.28%	40.29%	41.12%	41.73%	37.41%
	セキュリティ知識低（平均点未満）	ある	40.37%	37.61%	14.68%	16.51%	10.09%	9.17%
		しそうになったことがある	19.29%	22.14%	32.14%	25.71%	20.71%	8.57%
		両方	50.00%	71.88%	50.00%	53.13%	21.88%	21.88%
		ない	30.76%	30.07%	21.34%	20.70%	22.72%	23.32%

情報セキュリティ知識高群で携帯電話の紛失・盗難経験が「ある」と答えた人のうち、「情報セキュリティについての規程類が定められている」と答えた人の割合は66.29%であるのに対し、「情報セキュリティについての教育・研修が行われている」の割合は40.45%、「守秘義務についての誓約書などを提出させている」の割合は29.21%であった。情報セキュリ

ティ知識低群では、それぞれ、40.37%、10.09%、9.17%であった。つまり、知識量に関係なく「情報セキュリティについての教育・研修が行われている」ことや、「守秘義務についての誓約書などを提出させている」ことによって、インシデント経験の割合が減少する傾向があることがわかった。なお、ここでは携帯電話のインシデント経験のみを記載しているが、他のインシデント経験についても同様の結果が得られている。

さらに、携帯電話のインシデント経験における外出頻度と職場対策の関係を集計した結果を下表に示す。

表 3-8：情報セキュリティの知識量と職場対策の有効性の関係

			情報セキュリティについての規程類が定められている	職場のパソコンについて、外部への持ち出しを禁じるルール、または持ち出す際の手続きのルールが定められている	私物や業者のパソコンについて、職場への持ち込みを禁じるルール、または持ち込む際の手続きのルールが定められている	情報セキュリティ事故が起きた場合の、報告先や報告手続きのルールが定められている	従業員に対して情報セキュリティについての教育・研修が行われている	従業員に対して守秘義務についての誓約書などを提出させている
携帯電話の紛失・盗難	毎日、外出（出張）し、頻繁に移動する	ある	28.28%	19.70%	13.64%	10.61%	10.10%	8.08%
		しそうになったことある	13.04%	11.23%	9.78%	11.23%	11.23%	8.33%
		両方	31.63%	26.53%	27.55%	27.55%	22.45%	22.45%
		ない	3.73%	3.42%	2.77%	3.06%	3.09%	2.67%
	毎日、外出（出張）するが、移動回数は少ない	ある	7.07%	9.60%	6.06%	5.05%	4.04%	2.02%
		しそうになったことがある	6.52%	6.88%	6.88%	5.07%	5.43%	3.62%
		両方	13.27%	20.41%	17.35%	12.24%	9.18%	3.06%
		ない	0.84%	0.77%	0.60%	0.61%	0.67%	0.68%
	1週間に1～2回程度、外出（出張）している	ある	7.58%	8.59%	5.05%	6.06%	4.55%	3.54%
		しそうになったことがある	9.78%	11.59%	11.23%	10.14%	6.88%	5.07%
		両方	9.18%	13.27%	12.24%	9.18%	8.16%	5.10%
		ない	1.84%	1.81%	1.54%	1.59%	1.56%	1.40%
	1ヶ月に1～2回程度、たまに外出（出張）する	ある	3.03%	3.03%	1.01%	1.52%	0.51%	0.51%
		しそうになったことがある	2.54%	2.90%	5.07%	3.99%	2.90%	1.09%
		両方	9.18%	13.27%	12.24%	9.18%	8.16%	5.10%

		ない	1.18%	1.17%	0.98%	0.99%	1.04%	0.83%
	ごく稀に外出（出張）する	ある	1.52%	1.01%	2.02%	0.51%	0.00%	0.51%
		しそうになったことがある	2.90%	3.26%	3.62%	4.71%	3.99%	2.17%
		両方	6.12%	6.12%	3.06%	5.10%	1.02%	2.04%
		ない	2.04%	1.89%	1.58%	1.64%	1.62%	1.39%
	会社貸与の携帯電話を持って外出（出張）しない	ある	0.00%	1.01%	0.51%	0.51%	0.51%	0.51%
		しそうになったことがある	1.09%	1.09%	2.17%	2.54%	1.45%	2.17%
		両方	1.02%	1.02%	2.04%	1.02%	2.04%	2.04%
		ない	2.41%	2.42%	1.99%	1.90%	2.02%	1.82%
	会社貸与の携帯電話を持っていない、使用していない	ある	4.55%	4.55%	4.55%	5.56%	4.04%	3.03%
		しそうになったことがある	6.52%	5.80%	5.80%	5.43%	6.88%	4.71%
		両方	5.10%	5.10%	4.08%	4.08%	3.06%	3.06%
		ない	27.54%	27.54%	20.70%	20.41%	21.58%	21.09%

毎日、外出（出張）し、頻繁に移動していて、携帯電話の紛失・盗難の経験が「ある」人のうち、「情報セキュリティについての規程類が定められている」の割合は 28.28%であるのに対し、「情報セキュリティについての教育・研修が行われている」の割合は 10.10%と低く、「守秘義務についての誓約書などを提出させている」の割合は 8.08%とさらに低くなっている。これは、外出頻度に関係なく、同様の傾向があらわれている。なお、ここでも携帯電話のインシデント経験のみを記載しているが、他のインシデント経験についても同様の結果が得られている。

以上より、知識量や外出頻度に関係なく、教育・研修や誓約書があると、情報セキュリティインシデントを減少させることができ、特に誓約書は効果が高いことがわかった。つまり、規定やルールを定めるだけでは情報セキュリティインシデントを減少させる効果は十分ではなく、規定やルールの内容を周知する教育・研修を実施した上で、誓約書を提出させることが重要であると考えられる。

3.2.5. **まとめ**

全体的に見ると、知識を持っている人のほうが、発生確率が高い結果になっている。これには、次のような理由が考えられる。

- もともと情報セキュリティのリスクが高い仕事をしているので、業務上の知識を持っているか、教育研修を受けている。

- IT 技術や情報セキュリティに詳しいので、自分は全てのリスクを回避できると思い込んで、自らリスクが高い状況へ踏み込んで、インシデントを起こしている。
- 情報セキュリティの概念的なの知識はあっても、具体的な対策レベルの知識を持ちあわせておらず、情報セキュリティインシデントを軽減、回避できていない。
- 知識はあっても、具体的な行動には結びついていないため、情報セキュリティインシデントを軽減、回避できていない。

以上より、もはや情報セキュリティに関する表面的な知識だけの教育では、情報セキュリティインシデントの軽減や回避にあまり効果がないということがわかる。情報セキュリティのリスクが高い仕事をしている状況を変更することは難しいが、情報セキュリティ教育や研修やの内容や、セキュリティ対策のための具体的な行動やその実践状況は、改善することが可能である。

まず、表面的な知識だけの教育研修ではなく、具体的な対策レベルの知識まで、教育や研修を実施する。さらにセキュリティ対策が、具体的な行動に反映されているかどうか、自主点検や情報セキュリティ監査によって確認することによって、初めてセキュリティ対策が実践できていると保証できるレベルに到達する。この自主点検や監査によって、故意に情報インシデントを発生させる行動を抑制することもできる。

3.3. 行動特性とインシデントの関係

2011 年の調査では、ユーザの行動と情報セキュリティインシデントの関係に注目した。たとえば、忘れ物をしやすい人は、携帯電話や USB メモリを紛失しやすいと、誰もが予想するだろう。そこで、情報セキュリティインシデントの経験と普段の行動との間には、関係があると仮定して、回答者の普段の行動に関する質問を追加した。当 WG が立てた仮説の一例は、以下のとおりである。

- 忘れ物をしやすい人は、携帯電話や USB メモリなどを紛失しやすい
- 約束やスケジュールを勘違いしやすい人は、メールを誤送信しやすい
- 仕事中に SNS を頻繁に使用している人は、不用意に会社の機密情報を書き込んでしまいやすい

以下のインシデントに関係するかもしれない 8 つの行動について、普段の自分の行動が当てはまるかどうか、「よくしてしまう」「時々することがある」「めったにしない」「したことはない」の 4 段階のどれに当てはまるか調査した。

表 3-9：質問した 8 つの行動特性

No	行動特性名	具体例
1	遅刻	寝坊や多忙などのせいで、出勤・会議などの時間に遅刻してしまう
2	約束の勘違い	仕事上の約束や予定スケジュールを勘違いして、人に迷惑をかけてしまう
3	整理整頓	机の上や引き出しの中が片付かず、書類などが見つからなくなる
4	忘れ物	自宅などに忘れ物をする
5	居眠り	業務中に居眠りや、ぼうっとして時間を過ごしてしまう
6	ウェブサーフィン	業務中に関係のないウェブサイトや掲示板・ブログ、SNS、ツイッターなどを見て時間を過ごしてしまう
7	SNS 書き込み	業務中に関係のない掲示板・ブログ、SNS、ツイッターなどに書き込みをして時間を過ごしてしまう
8	雑談	業務中に関係のない雑談、メールやチャットのやりとりなどをして時間を過ごしてしまう

アンケート結果から、回答者の普段の行動特性とインシデントの発生状況の関係を分析した結果を以下に説明する。

3.3.1. 携帯電話のインシデントと行動特性

当 WG は、忘れ物をしやすい人や整理整頓が苦手な人は、携帯電話を紛失しやすいだろうと予想した。そこで、まず携帯電話を紛失した・盗難にあったことがある人と、その人の行動特性を分析した結果を示す。この携帯電話を紛失した・盗難にあったことがある人の中には、携帯電話を紛失しそうになった人は含まれない。

以下のグラフは、携帯電話を紛失した・盗難にあったことがある人と行動特性の関係を示したものである。

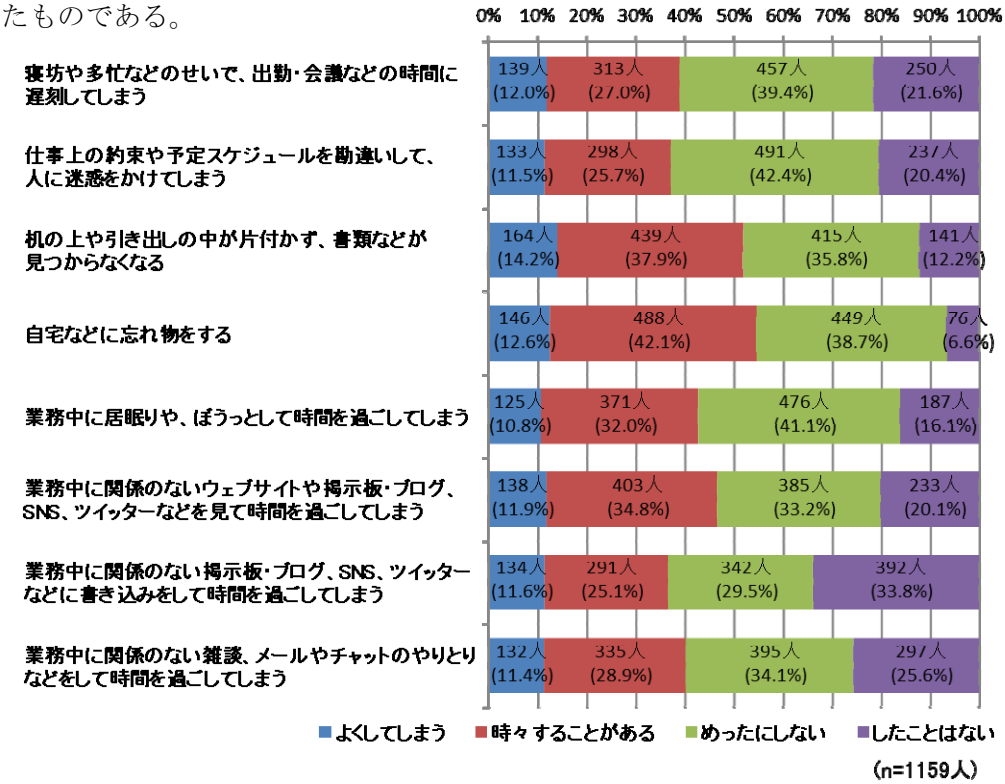


図 3-7：携帯電話のインシデントと行動特性

携帯電話の紛失・盗難の情報セキュリティインシデントの経験の有無と行動特性の関係を分析した。図 3-8 の各グラフを用いて、携帯電話の紛失・盗難の情報セキュリティインシデントの経験がある人とない人のグループについて、8 つの行動特性を比較した。以下の図 3-8 に示すように、8 つの行動特性のグラフのうち、破線で囲った 4 つのグラフにおいて、携帯電話の紛失・盗難の情報セキュリティインシデントの経験の有無のグループ間で、行動特性の回答の割合が大きく異なることがわかった。携帯電話の紛失・盗難の情報セキュリティインシデントの経験がある人のグループに比べて、経験がない人のグループは、4 つの行動特性について「めったにしない」「したことはない」と回答した人の割合が高く、すべて 80%以上である。つまり、遅刻、予定の勘違い、ネット書き込み、雑談を行わないグループは、携帯電話の紛失・盗難の情報セキュリティインシデントを起こしにくいと思われる。

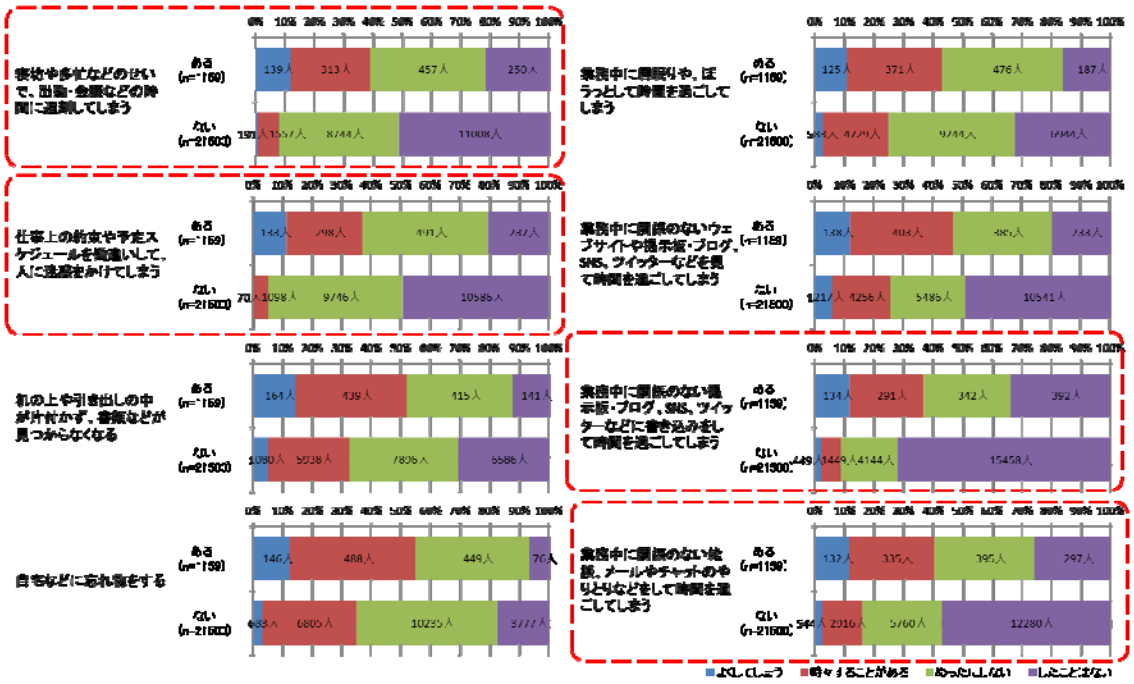


図 3-8：携帯電話のインシデントの有無と行動特性

忘れ物をしやすい、整理整頓が苦手、という行動特性は、図 3-8 の破線で囲った 4 つの行動特性のグラフほど、携帯電話の紛失・盗難の情報セキュリティインシデントの経験の有無のグループ間の顕著な違いがないが、携帯電話を紛失しやすい・盗難にあいやすい傾向がある遅刻、予定の勘違い、ネット書き込み、雑談を行わないグループは、携帯電話の紛失・盗難の情報セキュリティインシデントを起こしにくいと思われる。

3.3.2. パソコン、USB のインシデントと行動特性

パソコンは、携帯電話よりも大きい。したがって、携帯電話よりも紛失する確率が低いと予想できる。そこで、パソコンを紛失した・盗難にあったことがある人の行動特性を分析した。このパソコンを紛失した・盗難にあったことがある人の中には、パソコンを紛失しそうになった人は含まれない。

パソコンを紛失した・盗難にあったことがある人の各行動特性の回答の割合は、どの行動特性においても、大きな差がないことがわかった。「よくしてしまう」と回答した人の割合の差は 5%以内、「時々することがある」「めったにしない」と回答した人の割合の差は 10%以内であった。

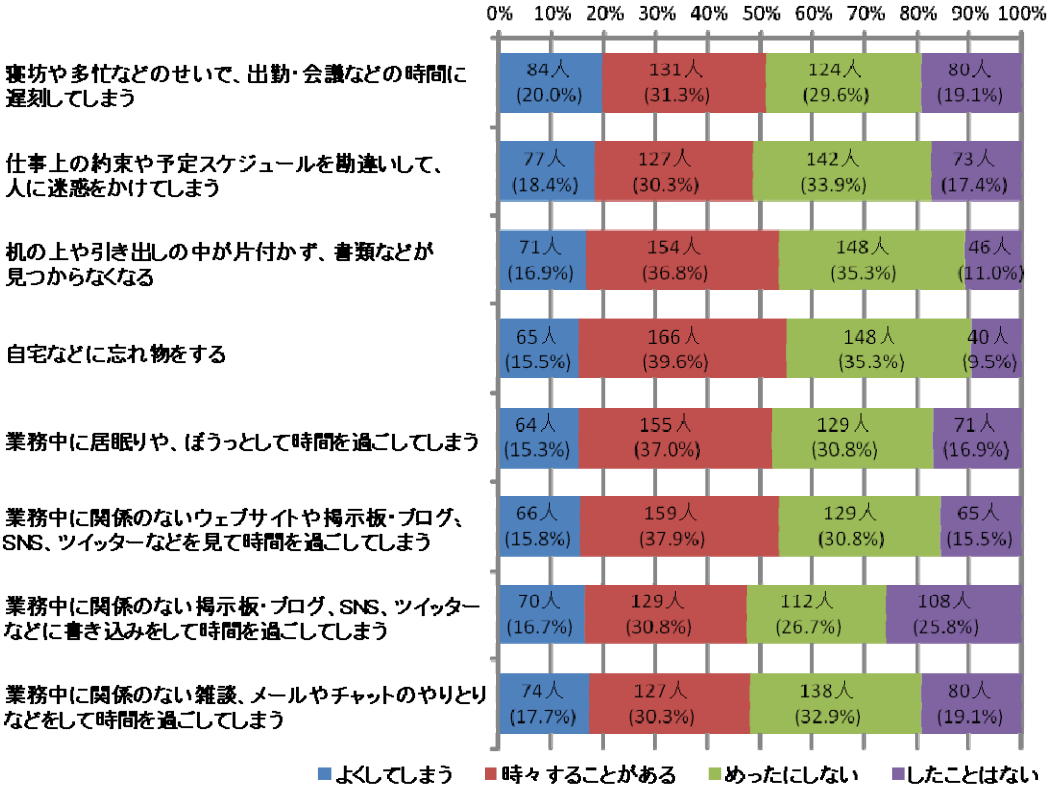


図 3-9：パソコンのインシデントと行動特性

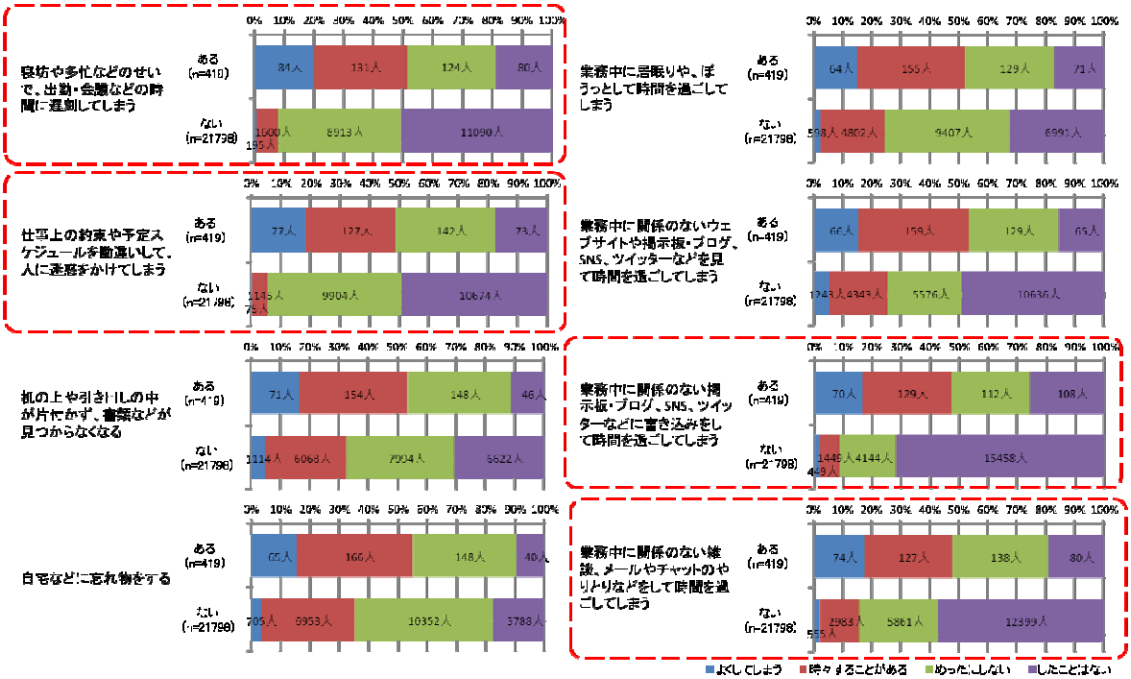


図 3-10：パソコンのインシデントの有無と行動特性

図 3-10 の破線に囲まれた 4 つグラフは、パソコンの紛失・盗難の情報セキュリティインシデントの経験がある人のグループとない人のグループの行動特性の回答の割合に大きな違いがある。パソコンの紛失・盗難の情報セキュリティインシデントの経験がある人のグループに比べて、経験がない人のグループは、「めったにしない」「したことはない」と回答した人の割合が高く、すべて 80%以上であった。この傾向は、「図 3-8：携帯電話のインシデントの有無と行動特性」とよく似ている。

3.3.3. USB メモリのインシデントと行動特性

USB メモリの場合も、携帯電話の紛失・盗難の情報セキュリティインシデントの場合と似た傾向である。

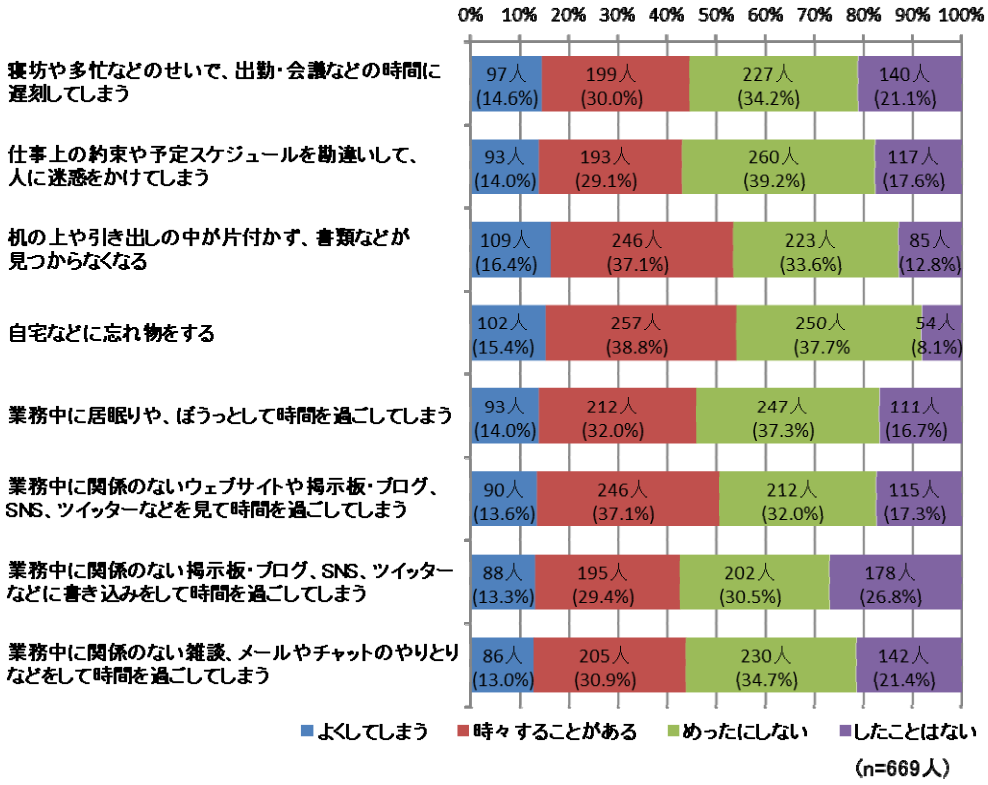


図 3-11：USB メモリのインシデントの有無と行動特性

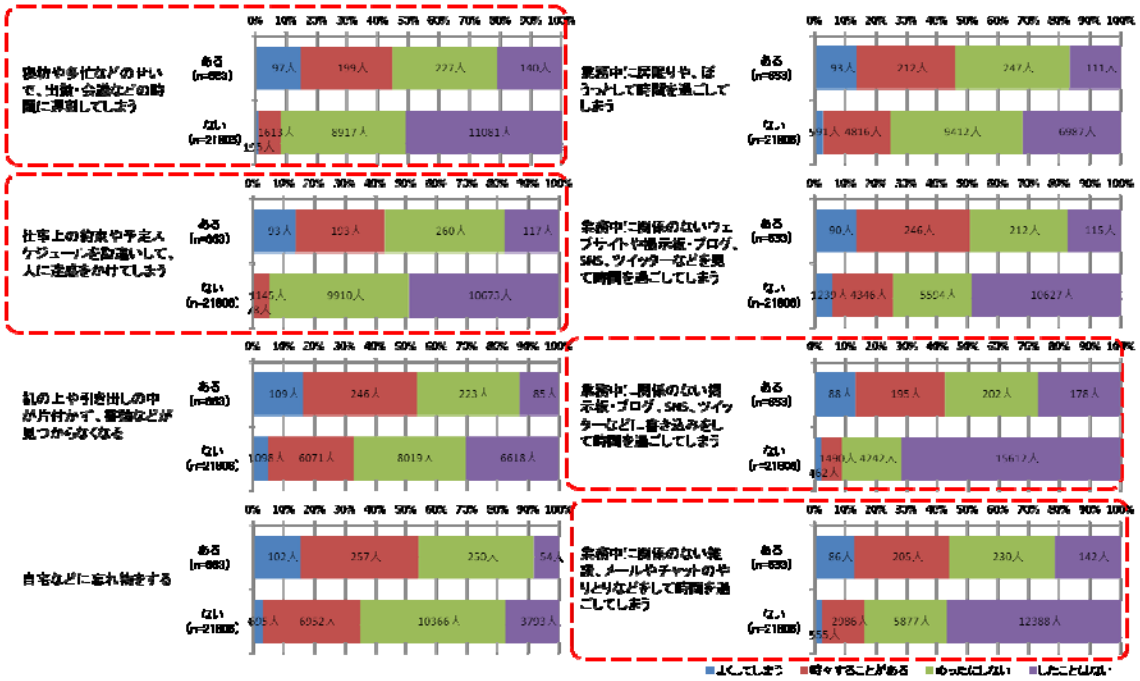


図 3-12：：USB メモリのインシデントの有無と行動特性

3.3.4. 電子メールのインシデントと行動特性

電子メールの場合は、前記の携帯電話、パソコン、USB メモリの場合とやや異なった傾向が現れている。

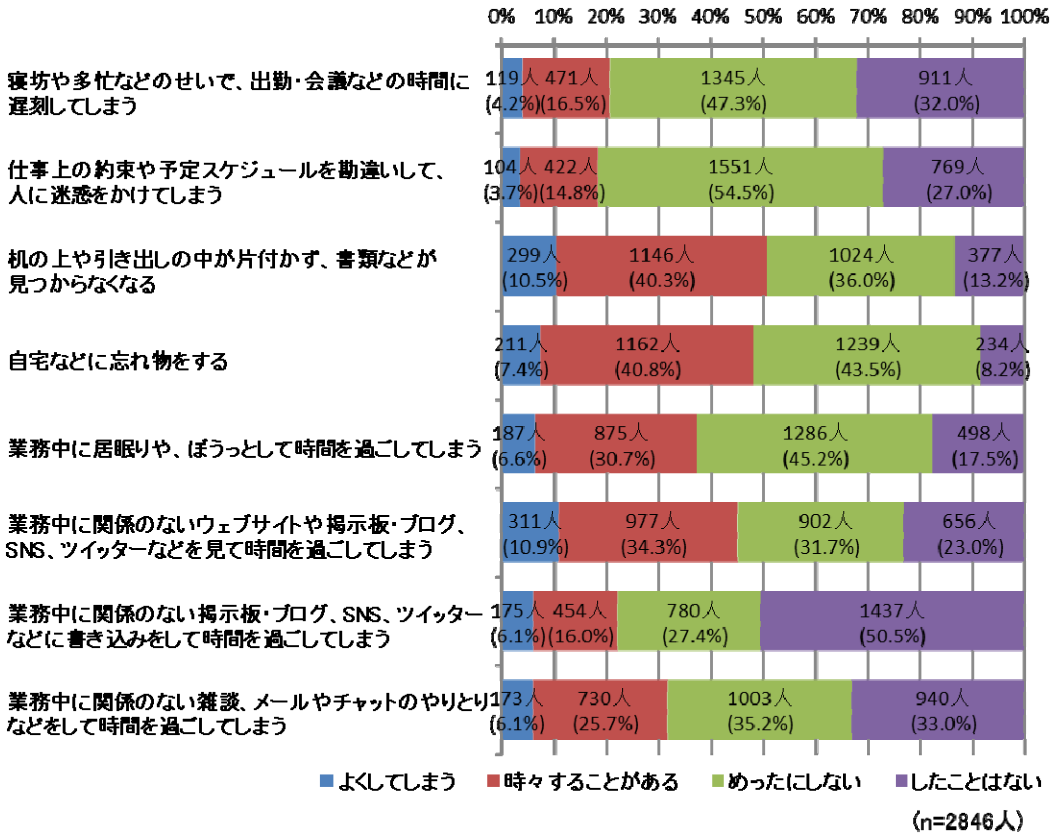


図 3-13：電子メールのインシデントと行動特性

携帯電話や PC、USB と比べてインシデントを起こした人が 2800 人と多い。この影響か、「図 3-14：電子メールのインシデントの有無と行動特性」の破線で囲った情報セキュリティインシデントの経験の有無のグループ間での行動特性の割合の差があるグラフであっても、その差が少ない。また、携帯電話／パソコン／USB メモリの場合と異なり、「業務中に関係のないウェブサイトや掲示板・ブログ、SNS、ツイッターなどを見て時間を過ごしてしまう」行動特性において、情報セキュリティインシデントの経験の有無のグループ間の違いが現れた。

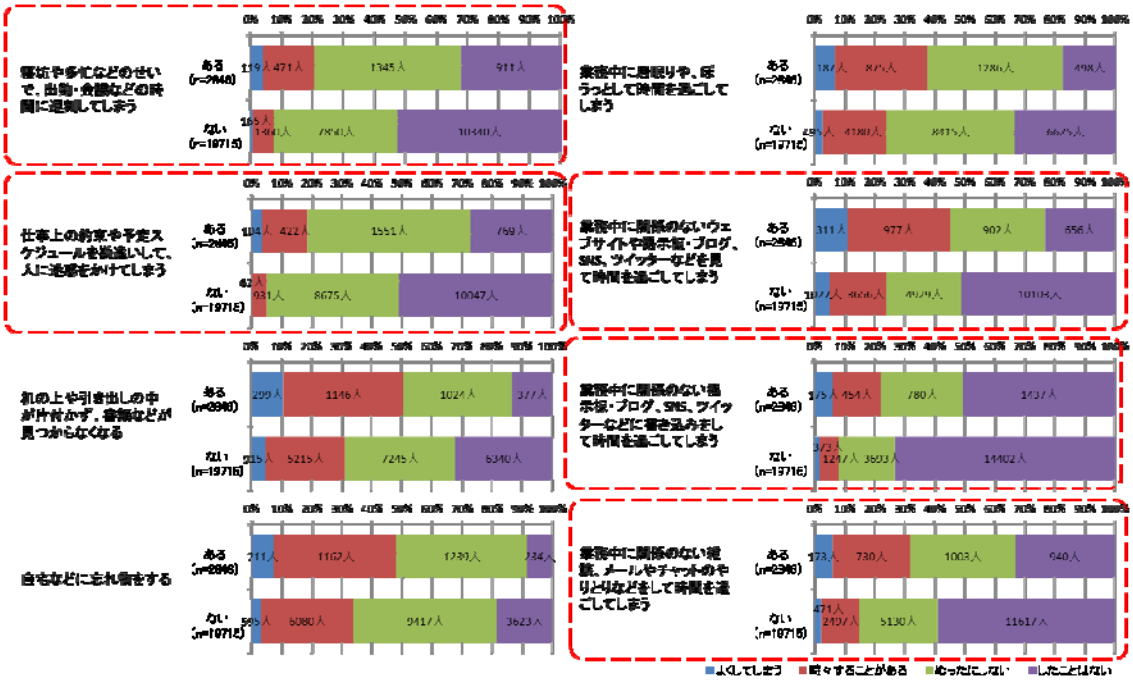


図 3-14：電子メールのインシデントの有無と行動特性

3.3.5. SNS のインシデントと行動特性

SNS の場合は、携帯電話／パソコン／USB メモリの紛失・盗難の情報セキュリティインシデントの場合と似た傾向が現れている。

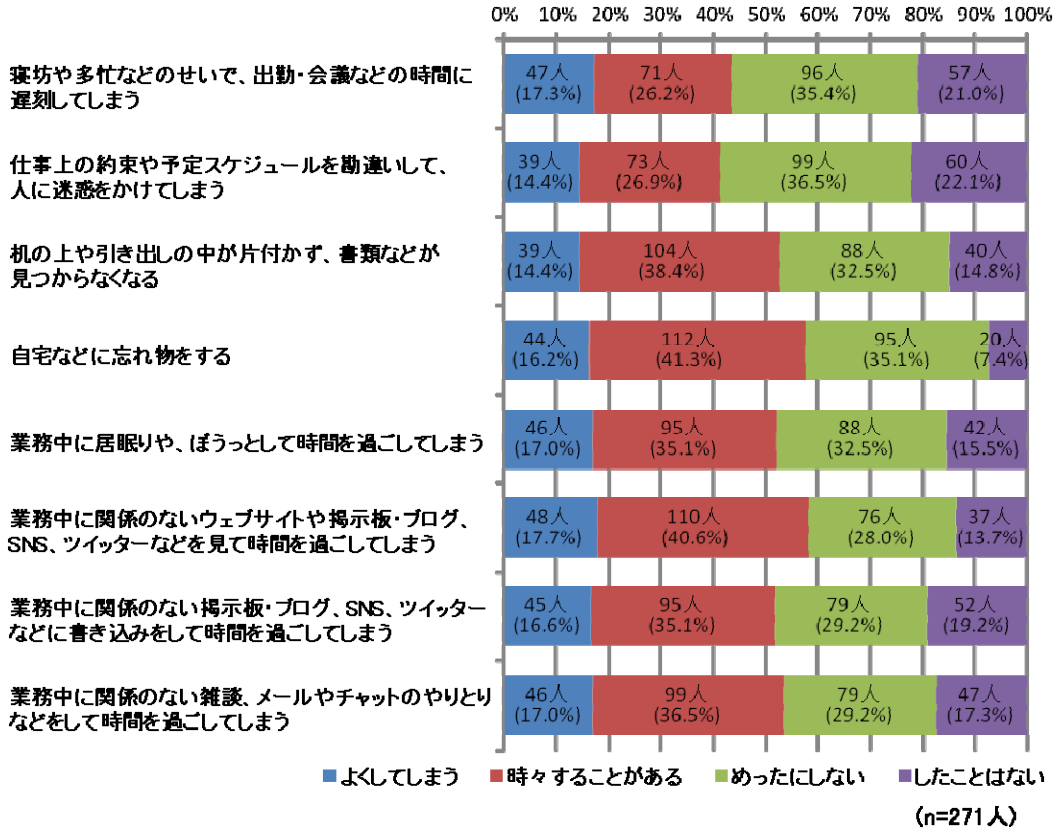


図 3-15：SNS のインシデントと行動特性

携帯電話／パソコン／USB メモリの紛失・盗難インシデントと、ブログ・SNS・ツイッターで業務上の秘密に関する情報や不適切な内容を書いてしまうインシデントは、インシデントの性質が大きく異なる。しかし、どちらも同じ 4 つの行動特性に特徴が現れており、その程度も同程度であった。

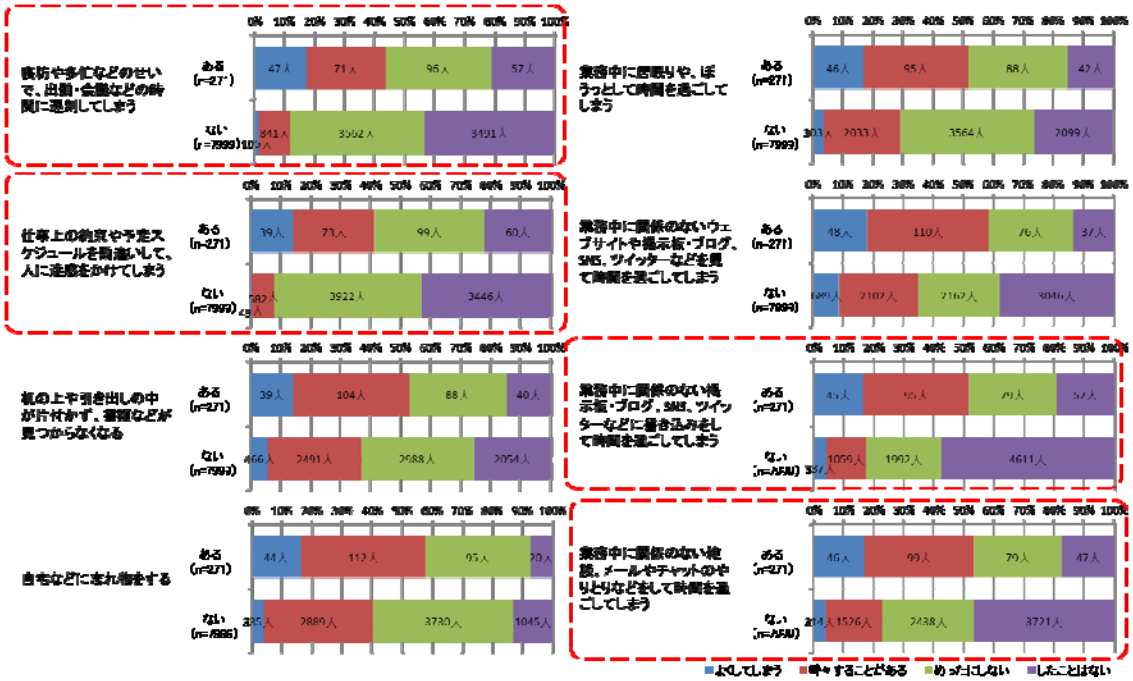


図 3-16：SNS のインシデントの有無と行動特性

3.3.6. まとめ

情報セキュリティ上のインシデントと行動特性の間には、関連があることがわかった。行動特性が原因となって情報セキュリティ上のインシデントが発生しているのか、あるいは、共通の原因があってインシデントと行動特性に関連があるのか、どちらであるか断言できないが、関連していることは明確である。行動特性は本人だけでなく、周囲の人でも客観的に把握できることである。したがって、遅刻や勘違いが多かったり、業務に関係ない書き込み、雑談等をしていたりする社員については、特に注意を払うことによって、インシデントの発生を抑制できる可能性がある。

遅刻や勘違いは、誰でも少しは経験しているものと思われるが、業務多忙になってくると発生しやすいものである。インシデントも業務多忙だと発生しやすいと考えられる。したがって、業務多忙の原因を除去することによって、インシデントの発生を抑制できるかもしれない。一方、業務に関係ない書き込み、雑談等は、職場のルール違反を黙認、放置しているからではないかと思われる。一般的にルール違反が常態化しているとインシデントは発生しやすい。したがって、職場のルール違反の黙認や放置をしないことによって、インシデントの発生を抑制できるかもしれない。

3.4. 性格とインシデントの関係

今回の調査では、更に個人の性格とインシデントの関係にも注目した。直感的なイメージでは、「大雑把な人よりきちょうめんな人のほうが紛失事故を起こしにくい」「慎重な人のほうがおっちょこちょいな人より紛失事故を起こしにくい」などと、いわゆる性格とインシデントが関係すると考えられる。そこで実際に何らかの傾向が見られるのかを調査・検討することとした。

性格を調べるために「人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ 1 つ)」という質問を、以下４つの項目に対して行った。

1	きちょうめん	どちらかというときちょうめん	どちらかというと大雑把	大雑把
2	悲観的	どちらかというと悲観的	どちらかというと楽天的	楽天的
3	生真面目	どちらかというと生真面目	どちらかというといい加減	いい加減
4	慎重	どちらかというと慎重	どちらかというとおっちょこちょい	おっちょこちょい

3.4.1. インシデントの経験と性格の関係

携帯電話紛失、パソコン紛失、USB メモリ紛失、メール誤送信、SNS への書き込みの５種類について、インシデントを起こしたことがある人とない人のグループに分けて、4 つの性格分類との間の傾向を比較検討した。その結果、今回の調査においては、いずれのインシデントにおいても、性格による違いがほとんど見られなかった。以下にデータの比較結果を示す。

(1). 携帯電話の紛失・盗難と性格の関係

「業務データが入った携帯電話を紛失した・盗難にあったことがある」「業務データが入った携帯電話を紛失しそうになったことがある」「業務データが入っていない携帯電話を紛失した・盗難にあったことがある」と言った、携帯電話の紛失・盗難のインシデントを経験したグループと、紛失・盗難のインシデントを経験していないグループを用意し、「きちょうめんな/大雑把な」「悲観的な/楽天的な」「生真面目な/いい加減な」「慎重な/おっちょこちょいな」の 4 つの性格の割合を調査した。

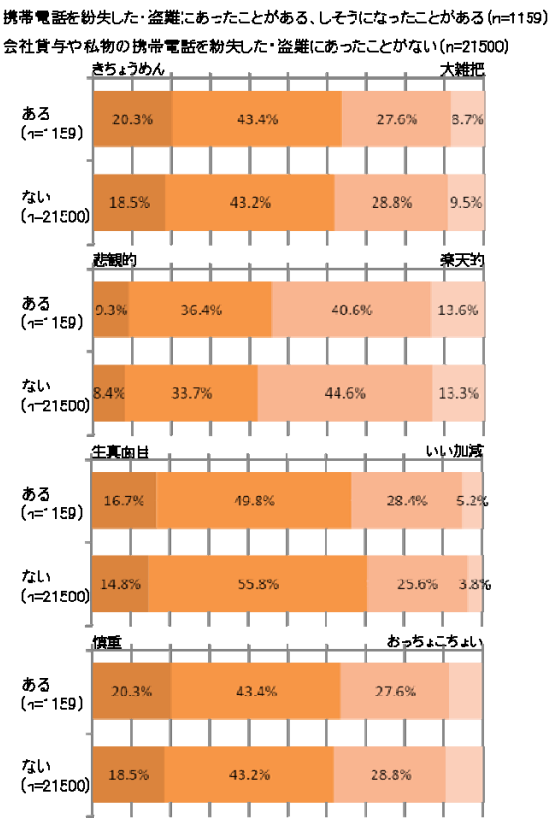


図 3-17 : 携帯電話の紛失・盗難と性格の関係

図 3-17 の 1 つ目の棒グラフは、インシデントを経験したグループの「きちょうめんな/大雑把な」性格の比率である。1 つ目の棒グラフは、インシデントを経験していないグループの「きちょうめんな/大雑把な」性格の比率である。この 2 つを比較すると、「きちょうめんな/大雑把な」性格の比率は、インシデント経験の有／無のどちらもほぼ同じである。つまり、きちょうめんな性格でも、大雑把な性格でも、携帯電話の紛失漏洩確率の値は変わらない。よって、「きちょうめんな/大雑把な」性格は、インシデント発生確率に関係ないと言える。

同様に、他の 3 つの性格も、携帯電話の紛失漏洩のインシデントを経験したグループとインシデントを経験していないグループの間で、性格の比率に顕著な差は無い。したがって、携帯電話の紛失漏洩のインシデントの発生確率と性格は、無関係と言える。

(2). パソコン、USB メモリの紛失・盗難の経験と性格の関係

パソコンと USB メモリの紛失漏洩のインシデントも、2 つのグループの間で性格の比率に顕著な差が無い。したがって、パソコンと USB メモリの紛失漏洩のインシデント発生確率と性格も、無関係と言える。

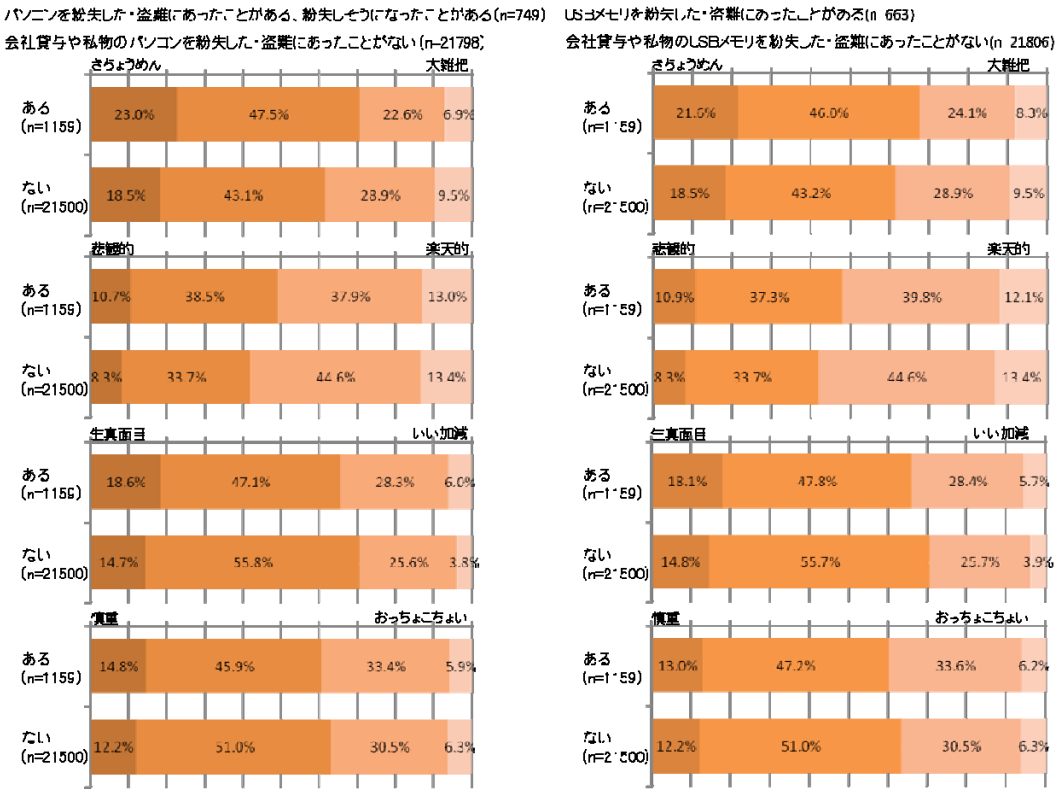


図 3-18：パソコン、USB メモリの紛失・盗難と性格の関係

(3). 電子メールの誤送信、SNS の不適切な書き込み経験と性格の関係

電子メールの誤送信と SNS の不適切な書き込みのインシデントも、2 つのグループの間で性格の比率に顕著な差が無い。したがって、電子メールの誤送信と SNS の不適切な書き込みのインシデント発生確率と性格も、無関係と言える。

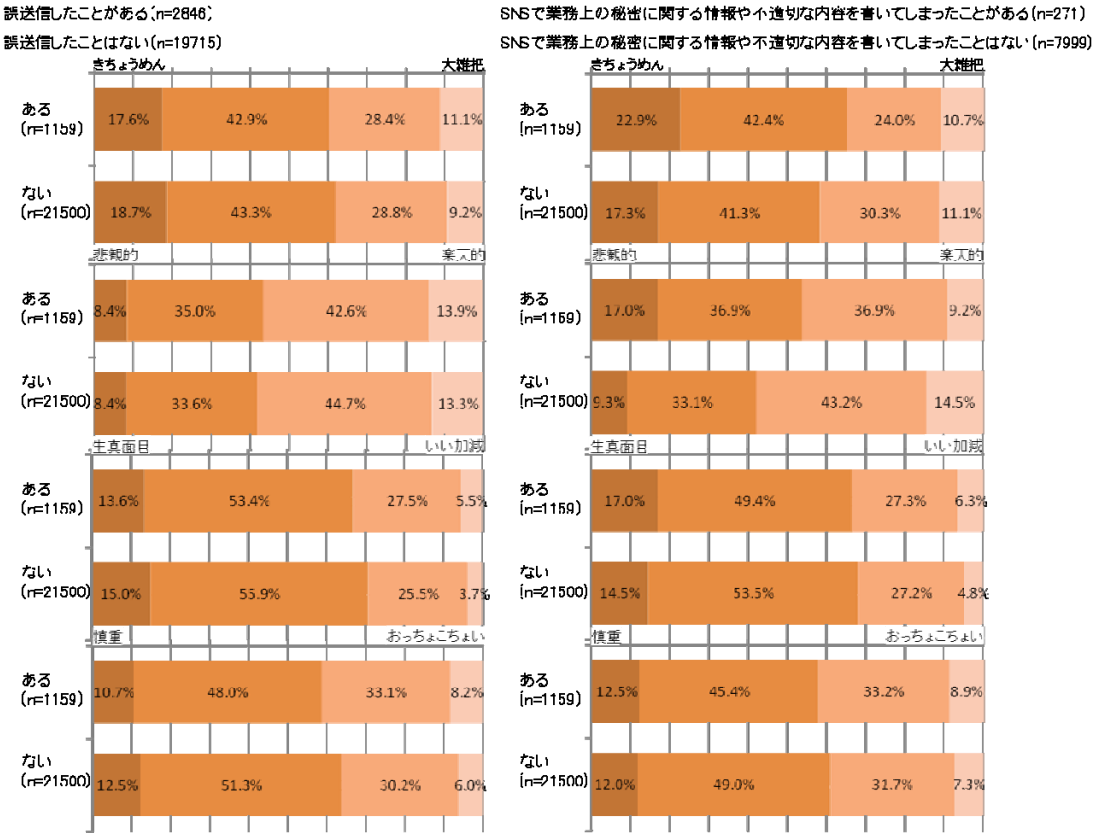


図 3-19：電子メールの誤送信経験と知識の関係

3.4.2. インシデントの発生と性格の関係についての考察

直感的なイメージに反して今回の調査では有意な差は見られなかった。性格の自己判断結果とインシデントの因果関係がない。自分は几帳面／慎重だから、大丈夫だとは、思わないほうが良い。

その原因は、2 つある思われる。

- 調査の仕方が悪くて、正しい結果が得られなかった
- 本当にインシデントと性格は関係がない

来年以降、以下のことを検討したい。今回は比較的単純で数少ない質問によって性格を自己申告する形を取っているが、自己申告であると、必ずしも正しい傾向が出てこないのではないか、と考えられる。性格特性を判定するための質問方法、質問数について見直し、より正しく性格特性を判定できるように、検討する必要がある。本当に性格とインシデントに関係がない場合は、外部環境とインシデントの関係を調査したい。

(1). 職場環境の影響

今回の調査結果から、実はインシデントの発生確率は、個人の性格特性とはあまり関係がなく、むしろ職場の雰囲気やモラルの状況、同僚など周囲の人との対人関係などに影響を受けるのではないかという推論も成り立つ。(他の調査機関では、不正持ち出しのインシデント発生と職場のコミュニケーションの状況に相関関係があるという調査結果が存在する)したがって、次回調査にあたっては職場の環境も併せて質問し、それらの相関関係を見ることによってこの点を明らかにするといったアプローチも検討したい。

3.5. おっちょこちょいのプロフィール

3.5.1. 携帯電話、パソコン、USB メモリを重複して紛失した人

業務データが入った会社貸与の携帯電話、パソコン、USB メモリを 2011 年の一年間に重複して紛失した人を調査した。

表 3-10：携帯電話、パソコン、USB メモリを重複して紛失した人の割合

		会社携帯紛失		会社 PC 紛失		会社 USB 紛失		会社(N)
1	アンケート全体	161 人	0.7%	124 人	0.6%	133 人	0.6%	22340 人
2	業務データが入った会社貸与の携帯電話を紛失した・盗難にあったことがある			85 人	52.8%	84 人	52.2%	161 人
3	業務データが入った会社貸与のパソコンを紛失した・盗難にあったことがある	85 人	68.5%			78 人	62.9%	124 人
4	業務データが入った会社貸与の USB メモリを紛失した・盗難にあったことがある	84 人	63.2%	78 人	58.6%			133 人

表を見てわかるように、重複して紛失している人が各項目で 50%を超えている。前回のアンケート調査でも同様に 50%を超えていたが、前回のアンケート調査は 1 年間で区切っていないので、物を紛失しやすい人は存在し、且つ短期間で紛失する事も多いと考えられる。

複数の会社貸与の機器を紛失した人は延べ人数で 247 人であるが、携帯電話、パソコン、USB メモリの三つとも紛失した人が、65 人いるので、複数の会社貸与の機器を紛失した人（おっちょこちょい）は実際には 117 人となっている。

3.5.2. おっちょこちょいな人の知識

おっちょこちょいな人の特徴を見つけるために、アンケート結果を分析した。まず知識面について分析した結果を表 3-11 に示す。

表 3-11：他人に大まかな説明ができるくらいに知っていますか

		既知人数 (22340 人)	割合(%)	おっちょこちょい人数 (117 人)	割合(%)
1	個人情報保護法	14767 人	66.1%	98 人	83.8%
2	不正アクセス禁止法	8263 人	37.0%	65 人	55.6%
3	ぜい弱性	6062 人	27.1%	65 人	55.6%
4	リスク・アセスメント	3529 人	15.8%	56 人	47.9%
5	ISMS(情報セキュリティ・マネジメント)	2018 人	9.0%	47 人	40.2%
6	コンピュータ・ウイルス	15101 人	67.6%	69 人	59.0%
7	フィッシング詐欺	12245 人	54.8%	67 人	57.3%
8	ファイアウォール	10345 人	46.3%	66 人	56.4%
9	マルウェア	3071 人	13.7%	45 人	38.5%
10	DoS 攻撃	2439 人	10.9%	46 人	39.3%
11	OS(オペレーティング・システム)	10377 人	46.5%	54 人	46.2%
12	ウェブ・ブラウザ	9361 人	41.9%	47 人	40.2%
13	HTML	9060 人	40.6%	59 人	50.4%
14	Linux	5051 人	22.6%	40 人	34.2%
15	SaaS	1319 人	5.9%	31 人	26.5%
16	上記で知っている言葉はない	3806 人	17.0%	4 人	3.4%

アンケート全体と比較すると、概ね知識があることがわかる。特に情報セキュリティで用いられる言葉は、よく知っているようだ。おっちょこちょいな人は、IT や情報セキュリティに関連する言葉を比較的知っているか、知っていると思っている人が多いようだ。また、インシデントをよく起こす人に知識を与える教育を実施しても、あまり効果がないのかもしれない。

3.5.3. おっちょこちょいな人の行動

うっかりした失敗についてのアンケート集計でも、おっちょこちょいな人は、どの場面でも「よくしてしまう」「時々することがある」の回答が多くなっている。一例として忘れ物についてのアンケート全体とおっちょこちょいな人を比較した表が次の表である。

表 3-12：自宅などに忘れ物をすることが、どれくらいありますか

		既知人数（22340 人）	割合(%)	おっちょこちょい人数（117 人）	割合(%)
1	よくしてしまう	764 人	3.4%	22 人	18.8%
2	時々することがある	7160 人	32.1%	54 人	46.2%
3	めったにしない	10576 人	47.3%	34 人	29.1%
4	したことはない	3840 人	17.2%	7 人	6.0%

忘れ物を時々することがあると回答した人が、全体と比較すると倍近くなっているのがわかる。行動面をみるとおっちょこちょいな人は、遅刻をしたり、忘れ物をする割合が高く、業務中に仕事に関係ない Web 閲覧や書き込みをしている人の割合も高くなっている。

3.5.4. 自分はおっちょこいと思っていない

自分の性格に対する自己評価をアンケート集計してみると、きちょうめんで、生真面目で、悲観的であるという割合がアンケート全体とおっちょこちょいな人を比較すると高くなっている。また、自分はおっちょこちょいかの設問には、次の表の通りである。

表 3-13：自分に最も近い性格は

		既知人数（22340 人）	割合(%)	おっちょこちょい人数（117 人）	割合(%)
1	慎重に近い	2726 人	12.2%	17 人	14.5%
2	どちらかというと慎重に近い	11391 人	51.0%	55 人	47.0%
3	どちらかというとおっちょこちょいに近い	6828 人	30.6%	40 人	34.2%
4	おっちょこちょいに近い	1395 人	6.2%	5 人	4.3%

比較してわかるように、あまり顕著な差が出ていない。つまり、自分はおっちょこちょいだと自覚している人のほうが多いという結果になっている。

ステレオタイプ的な書き方になりますが、IT や情報セキュリティの知識があり、自分のことをおっちょこちょいだと思っていないが、忘れ物をしやすい人は実はおっちょこちょいである可能性が高いかもしれない。

3.5.5. **外出の多い人は要注意**

以下は、外出の頻度に関するアンケート集計から、全体とおっちょこちょいな人を比較した表である。

表 3-14：会社貸与の携帯電話を持って外出する頻度

		既知人数 (22340 人)	割合(%)	おっちょこちょい人数 (117 人)	割合(%)
1	毎日、外出（出張）し、頻繁に移動する	1745 人	7.8%	71 人	60.7%
2	毎日、外出（出張）するが、移動回数は少ない	482 人	2.2%	15 人	12.8%
3	１週間に 1～2 回程度､外出(出張）している	815 人	3.6%	12 人	10.3%
4	１ヶ月に 1～2 回程度、たまに外出（出張）する	485 人	2.2%	5 人	4.3%
	ごく稀に外出（出張）する	807 人	3.6%	6 人	5.1%
	会社貸与の携帯電話を持って外出（出張）しない	1124 人	5.0%	2 人	1.7%
	会社貸与の携帯電話を持っていない、使用していない	16882 人	75.6%	6 人	5.1%

外出する頻度が多い人の割合が高い。週に 1、2 回以上外出する人が 80%以上となっている。これは、もちろんおっちょこちょいな人が外出が多い訳ではなく、外出先や移動中に紛失や盗難が発生している事が推測できる。外出の多い人は持ち物に細心の注意が必要である。

3.6. 本当は怖かった パソコン「社内紛失」

2010 年の調査に引き続き、2011 年の調査でも、パソコンの紛失・盗難の年間発生確率を調査した。その結果、調査対象者 22340 人のうち 584 人(2.6%)が、過去 1 年間に業務データの入ったパソコン[1]を紛失・盗難にあった、または無くしそうになったと回答している[2]。

2010 年の調査で判明した知見のひとつ「パソコンの紛失・盗難インシデントのうち、約 30%が“勤務中、社内で無くした”」というものを覚えておられるだろうか。

従来、パソコンの紛失原因として思い浮かぶことが多いのは、酩酊して電車の中に置き忘れた場合や、車上荒らしにあった場合などではなかったろうか。

こうした直感的なイメージに反して、実際には社内の紛失した場合が多いという調査結果は、印象的ではあったが、一方で当 WG の間でも様々な疑問・疑念をもたらした。

- 前回の調査では偶然、社内紛失が多かったのではないか。次回以降の再調査では結果が異なるのでは？
- 前回の調査では、パソコンの紛失・盗難として「無くしそうになった」という場合も含めて集計していた。“社内で無くした”という回答者は、実際には「無くしそうになった」だけの場合が多いのではないか？
- パソコンを“社内で無くした”などということが、本当にそんなに多く起きるのか？実際にはパソコンが紛失しているわけではなく、“棚卸しをした際に台帳と合わなかった”などといった書類の記載ミスが原因ではないのか？
- たとえ、実際にパソコンが紛失したと言っても、たとえば使用していない古いパソコンや、倉庫に保管中の空っぽのパソコンなどではないのか？ つまり、情報セキュリティインシデントとしての被害は軽微ではないか？

2010 年の調査では、残念ながらこれらの疑問に答えられるだけの調査データを取っていなかった。この反省を活かして、2011 年はこれらの疑問に応えられる調査項目を用意して、データを採取している。[3]

本節ではこのデータをもとに、正体不明の“社内紛失”の実態を解き明かしていきたい。

---

[1] ここでは会社貸与のパソコン、私物のパソコンを含む。

[2] パソコン紛失・盗難インシデントの発生確率の集計は、本報告書 3.1.2 を参照。

[3] 2010 年の調査ではデータ不足のなかで可能な範囲の推測を行った。2010 年の報告書 3.4. 節「パソコン紛失のリスクは社内にあり!?」を参照。

3.6.1. 紛失・盗難全体に占める「社内紛失」の割合

2010 年の分析と同様、パソコンを紛失・盗難した回答者を以下のⅠ～Ⅳ群に分類したところ、割合は下表のとおりであった。なお、この表の母数である 100 件には、実際に紛失・盗難した場合のほか「無くしそうになった」という回答者も含む。

表 3-15：パソコン紛失・盗難全体での「社内紛失」の割合（2011 年の 1 年間）

分類	分類の説明	回答数	回答率
Ⅰ 社内紛失群	Q2 で選択肢 1～6（社内の状況での紛失）を選んだ回答者	63 件	63%
Ⅱ 勤務外または社外紛失群	Q2 で選択肢 7～11（社内以外の状況での紛失）を選んだ回答者	15 件	15%
Ⅲ 盗難群（分析対象外）	Q2 で選択肢 12～15（盗難）を選んだ回答者	8 件	8%
Ⅳ 不明群（分析対象外）	Q2 で選択肢 16「いつ、どこで無くなったのか分からない」を選んだ回答者	14 件	14%
合計		100 件	100%

まず特筆すべきは、Ⅰ「社内紛失」群の割合の多さである。2010 年の調査ではⅠ「社内紛失」群は約 3 割（29%）であったが、2011 年の調査ではこれを大きく上回る数字であるように見える。

しかし 2010 年の調査で集計したⅠ「社内紛失」群は、過去 1 年間ではなく過去数年間にわたっての紛失・盗難経験を含んでいた。2010 年の調査データでパソコンの紛失・盗難についての回答を調査年で分類し直すと、社内紛失の割合は下表のとおりである。

表 3-16：パソコン紛失・盗難全体での「社内紛失」の割合（2010 年調査データ）

分類	過去 1 年間(*)以内 2010 年		1～2 年前 2009 年		2～3 年前 2008 年		3 年前より以前 2007 年以前		総計	
	回答数	回答率	回答数	回答率	回答数	回答率	回答数	回答率	回答数	回答率
Ⅰ 社内紛失群	18 件	51%	5 件	17%	2 件	15%	4 件	17%	29 件	29%
Ⅱ 勤務外または社外紛失群	13 件	37%	21 件	72%	6 件	46%	10 件	43%	50 件	50%
Ⅲ 盗難群（分析対象外）	3 件	9%	2 件	7%	4 件	31%	8 件	35%	17 件	17%
Ⅳ 不明群（分析対象外）	1 件	3%	1 件	3%	1 件	8%	1 件	4%	4 件	4%
合計	35 件	100%	29 件	100%	13 件	100%	23 件	100%	100 件	100%

(*)調査時点では 2010 年 11 月だったため、正確には過去 11 ヶ月間。

「表 3-16」で分かるとおり 2010 年の調査データでも、過去 1 年以内に限った I「社内紛失」群の割合は 50%超であり、2011 年の調査の結果に近かった。その一方で、1 年以上前の紛失・盗難については、社内紛失の割合が急激に減少している。この傾向の原因が、回答者の記憶が薄れたことによるが原因だとするなら、最近 1 年間の記憶にもとづく 2011 年の調査の結果が、もっとも実態を反映していると考えるべきであろう。

また、社内紛失は社外での紛失・盗難に較べて忘れ去られやすいということは、「社内紛失」が実際には多数発生しているにもかかわらず、当 WG のイメージではそれほど脅威と感じていないことにも説明がつく。

3.6.2. 実際に紛失被害が発生する可能性はどれくらいか

前述の「社内紛失」63%というのは、「無くしそうになった」だけの回答者も含む割合である。そこで、無くしそうになったがあとで見つかった場合を除いた、実際に社内で紛失した場合の割合を調査した。2011 年の調査項目では Q1 において実際に紛失したかどうかを質問したため、その内訳を示す。

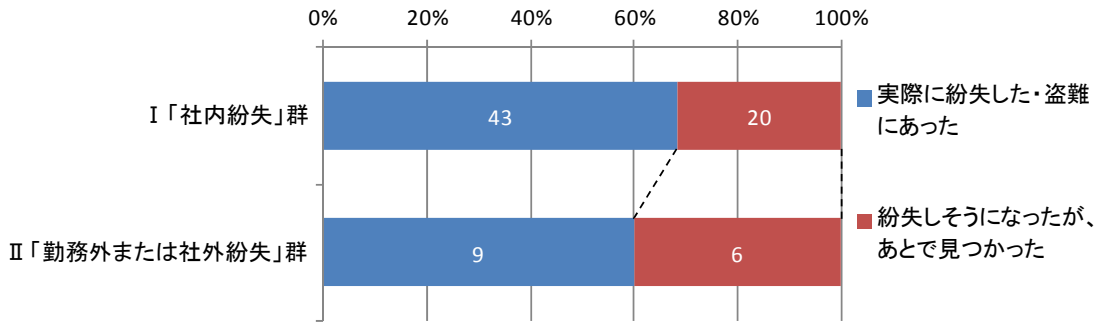


図 3-20：実際に紛失被害が発生しているか

図 3-20 のとおり、「社内紛失」とそれ以外の紛失とを比較しても、実際に紛失した（あとで見つかっていない）割合に大きな違いはない。むしろ、勤務外または社外の紛失が 60%であるのに対し、「社内紛失」が 68.3%と、「社内紛失」のほうがやや多い。

全調査対象者のうち 2.6%が過去 1 年間のパソコン紛失・盗難経験を報告している（社内・社外を問わず。「無くしそうになった」も含む）。そのうち、社外や勤務外ではなく社内での紛失で、あとで見つからなかった実際の紛失に限ると、全調査対象者の 1.1%が 1 年間にパソコンを紛失・盗難していることになる。1000 台のパソコンがある会社では、毎年 11 台ずつ社内で紛失していることになる。

3.6.3. 社内紛失パソコンの中身は…？

こうして社内で紛失したパソコンのうち、時間が経っても見つからなかった場合のみに焦点をあてて、さらに分析を試みた。紛失・盗難経験があると回答した 100 人のうち、時間が経っても見つからなかったと回答した人は 43 人であった。これらの「社内紛失」が発生した状況の内訳は、図 3-21 のとおりである。

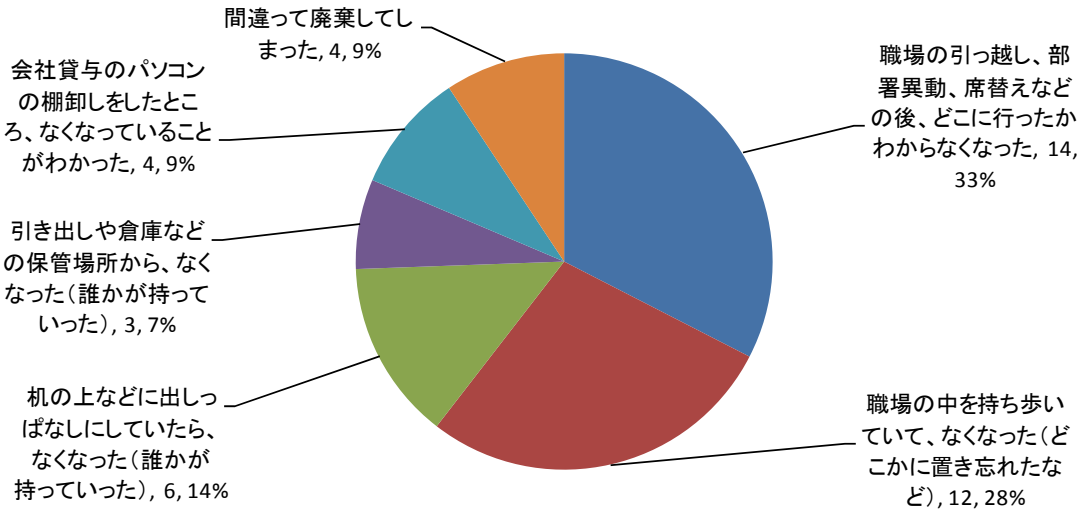


図 3-21：パソコンの「社内紛失」の内訳（N=43）

紛失が発生した状況の第 1 位は、職場の引っ越し等の際の紛失である。組織や物理的な配置が大きく変わるときには資産の管理責任に空白が生じがちであり、このようなインシデントが起きないよう肝に銘じるべきである。

しかし、第 2 位と第 3 位の「職場の中を持ち歩いて」と「机の上などに出しっぱなし」の状況から紛失した場合のほうが、より問題が大きいと思われる。この 2 つの紛失だけで、合計 40%を越える。これらのパソコンを持ち歩いたり、机の上に置いたりする状況から想像すると、おそらく紛失したのは普段から業務で使用しているパソコンであろう。そうしたパソコンを置き忘れたり、出しっぱなしにしたりするずさんな管理状態が紛失インシデントを招いたと思われる。

なお、上記の状況では、盗難にあった恐れもある。ただし、盗難であるはっきりした証拠が見つかるまでは、紛失として扱われるのであろう。社内の人間が盗んだ場合には、職場内の人間関係などもあり、犯人探しは困難である。

3.6.4. 紛失したパソコンの内容

また、これら社内紛失して見つからなかったパソコンには、どのようなデータが入っていただろうか。

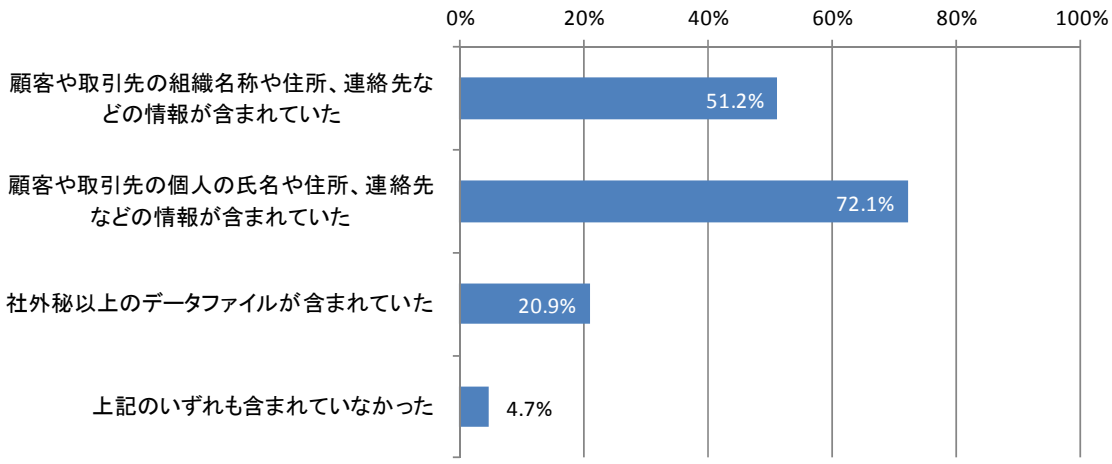


図 3-22：社内紛失パソコンに入っていた情報（N=43，複数回答あり）

実に、顧客や取引先の情報、社外秘以上のデータファイルのいずれも含まれていなかったのは僅かに 4.7%のみであり、残りの 95.3%ではいずれかの情報が含まれていた。社内で紛失したパソコンのほぼ全てに、漏えいすべきでない情報が含まれていたと言っても差し支えないだろう。

3.6.5.「社内紛失」のリスクとは何か

以上の分析から、以下のことが判明した。最近 1 年間で全台数の 1.1%のパソコンが、社内で紛失している。ある会社に 1000 台のパソコンがあるとしたら社内紛失は「毎年 11 台ずつ」である。これらの消えたパソコンのうち、かなりの部分が普段から業務に使っていると思われるパソコンであり、そしてほぼ全てが顧客・取引先の情報や社外秘以上のデータなどを含んでいると思われる。

さて、こうした「社内紛失」は、「リスク」だろうか？ パソコン内部に含まれる情報が社外に流出する「漏えいリスク」の観点では、リスクはごく小さい、という見方もある。「どれだけ情報が紛失しようが、所詮は社内でのことで、漏えいとは言えない」という考え方である。確かに「紛失」イコール「漏えい」と考えるのは、短絡に過ぎるだろう。リスクを過大に見て対策を行うのは、百害あって一利なしである。

だが、少し待ってほしい。私たちは回答者が「社内で紛失した」と答えたパソコンを、「社内紛失」パソコンと呼んだ。だが、これらのパソコンは、本当に今も社内のどこかにあるのだろうか。社内で紛失したのなら、探せば見つかるはずではないか。「社内で紛失した」と思い込んでいるだけで、実際はそうではないパソコンもあるのではないのか。

例えば、以下の様な場合が想定される。

- 社外を持ち歩いたときに無くしたのを、「社内でなくした」と思い込んでいるかもしれない。（または言い出せなかった）
- 置きっぱなしにしたパソコンを誰かが持っていったと思っているが、社外から侵入した窃盗犯の犯行かもしれない。（または同僚が黙って持ち帰った）
- 保管場所から消えたパソコンは、じつは不正に持ち出されて、大事なデータが入ったまま、インターネットオークションで売りだされているかもしれない。

あなたの会社で「社内紛失」したパソコン 11 台のうち、このように社外に流出しているものが 1 台もしくは 2～3 台、もしかすると、半分くらいが社外に流出して、内部の情報を抜き取られている恐れもある。この想定を否定できるほど、あなたの会社では、社内で起きているパソコン紛失の実態を把握しているだろうか。

パソコンの「社内紛失」の本当のリスクとは、「きっと社内でなくしたに違いない」と考えて、十分な追究がなされなかったり、そのまま忘れられてしまったりすることにある。社外を持ち歩くパソコンばかりに目を向けず、社内においても、当然行うべきセキュリティ対策を当然のように実施することが大事である。

- パソコンは社内にあっても、きちんと整理整頓すること。セキュリティワイヤーをつける、使わない時には施錠保管すること
- 紛失時に備えて HDD 暗号化、データの自動バックアップをおこなうこと
- 定期的な棚卸しなどを行って、紛失や盗難がないか確認すること
- 紛失事故が起きたときには紛失状況を詳しく調べて、本当に社外流出のおそれがないことを確認すること
- 従業員の１人１人に規定・ルールを周知し、誓約書を書かせるなどして、リスク意識を浸透させること

このような日々のセキュリティ対策を社内に浸透させることで、正体不明の紛失事故の数を減らすことにつながるのであろう。

3.7. 私物は危険か？

会社貸与品と私物について、盗難または紛失に対しての対策、および盗難または紛失発生後の対応を比較することで、会社貸与品と私物のリスクの差異を分析し検証する。分析は、本アンケート結果から、携帯電話、パソコン、USB メモリを対象に“会社貸与品”と“私物”に分類し、業務データが入っていた機器を紛失した・盗難にあったと回答した場合について、以下の分析を行った 。

a) 紛失した・盗難にあったことがある携帯電話、パソコン、USB メモリの「会社貸与」「私物」「両方」の割合
b) ポリシーの策定や教育等の職場におけるセキュリティ事項を実施されていない場合の携帯電話、パソコン、USB メモリの紛失・盗難の割合。（設問 SC6）
c) 盗難または紛失の対策していなかった場合の携帯電話、パソコン、USB メモリの紛失・盗難の割合。（携帯電話・パソコン＝設問 Q4、USB メモリ＝設問 Q3）
d) 盗難または紛失後に会社、組織に報告・連絡した場合、および何もしなかった場合の携帯電話、パソコン、USB メモリの割合。（携帯電話・パソコン＝設問 Q5、USB メモリ＝設問 Q4）

3.7.1. 会社貸与と私物の割合

業務データが入った状態で紛失・盗難がおきた携帯電話、パソコン、USB メモリについて、そのデバイスの所有「会社貸与」「私物」「両方」の割合を以下に示す。

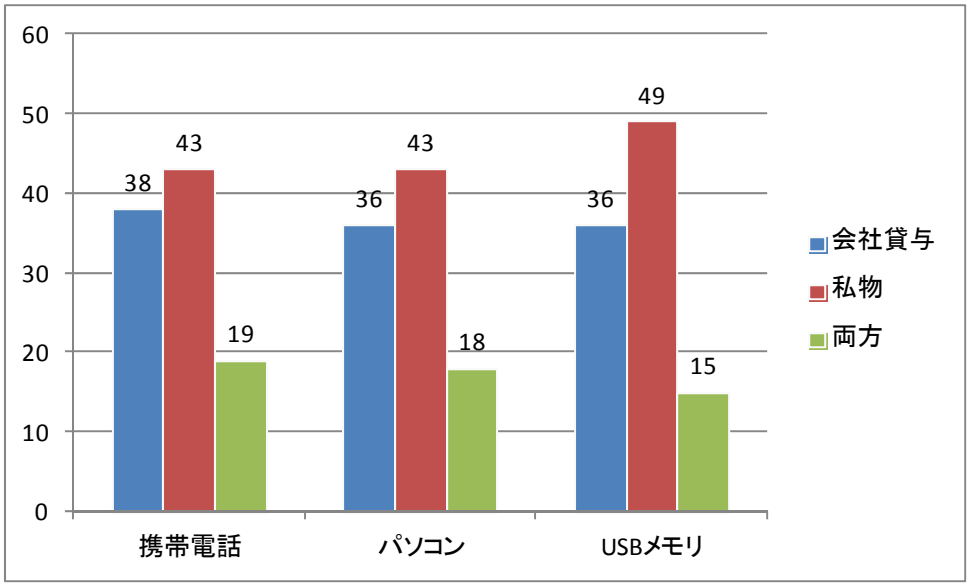


図 3-23：業務データが入った状態で紛失・盗難がおきたデバイスの内訳（台数）

業務データが入った携帯電話、パソコン、USB メモリを紛失・盗難した人のうち、それが私物である人が多い。

3.7.2. 紛失・盗難対策

携帯電話、パソコン、USB メモリを紛失・盗難にあった人、それぞれ 100 人から、事前に紛失・盗難に対する対策を実施していなかった人を抽出し、その人が使用していた携帯電話、パソコン、USB メモリの所有「会社貸与」「私物」「両方」の割合を調査した。

表 3-17： 盗難または紛失に対する対策をしていなかったものの人数

	会社貸与	私物	両方	合計
携帯電話	10 人	11 人	2 人	23 人
パソコン	9 人	7 人	6 人	22 人
USB メモリ	12 人	16 人	5 人	33 人

(1). 携帯電話

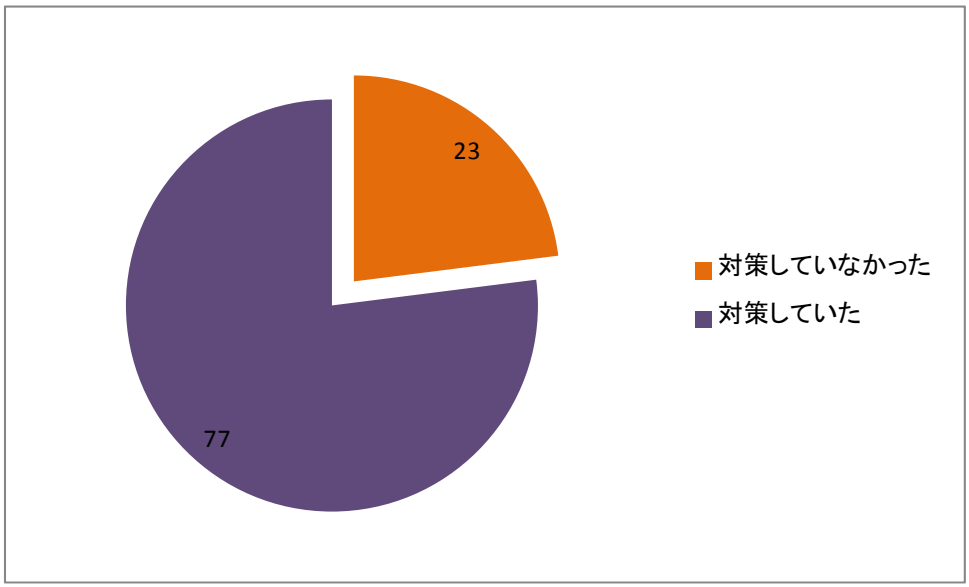


図 3-24：携帯電話の盗難紛失の対策の実施状況（人数）

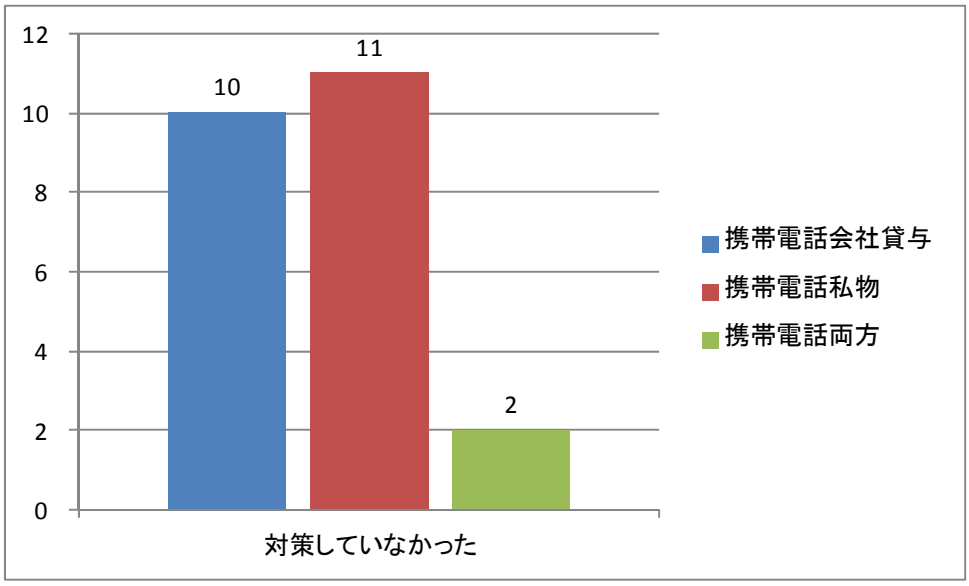


図 3-25：盗難紛失対策をしていなかった携帯電話の内訳（人数）

業務データが入った携帯電話を紛失した・盗難にあった者 100 人の内、紛失・盗難の対策をしていなかった人は、23 人であった。そのうち、会社貸与の携帯電話を対策せずに紛失・盗難した人が 10 人、私物の携帯電話対策せずに紛失・盗難した人が 11 人であった。ほとんど人数に違いはない。よって、携帯電話の紛失・盗難の確率は、未対策の会社貸与の携

帯電話と私物の携帯電話の間に違いはない。

(2). パソコン

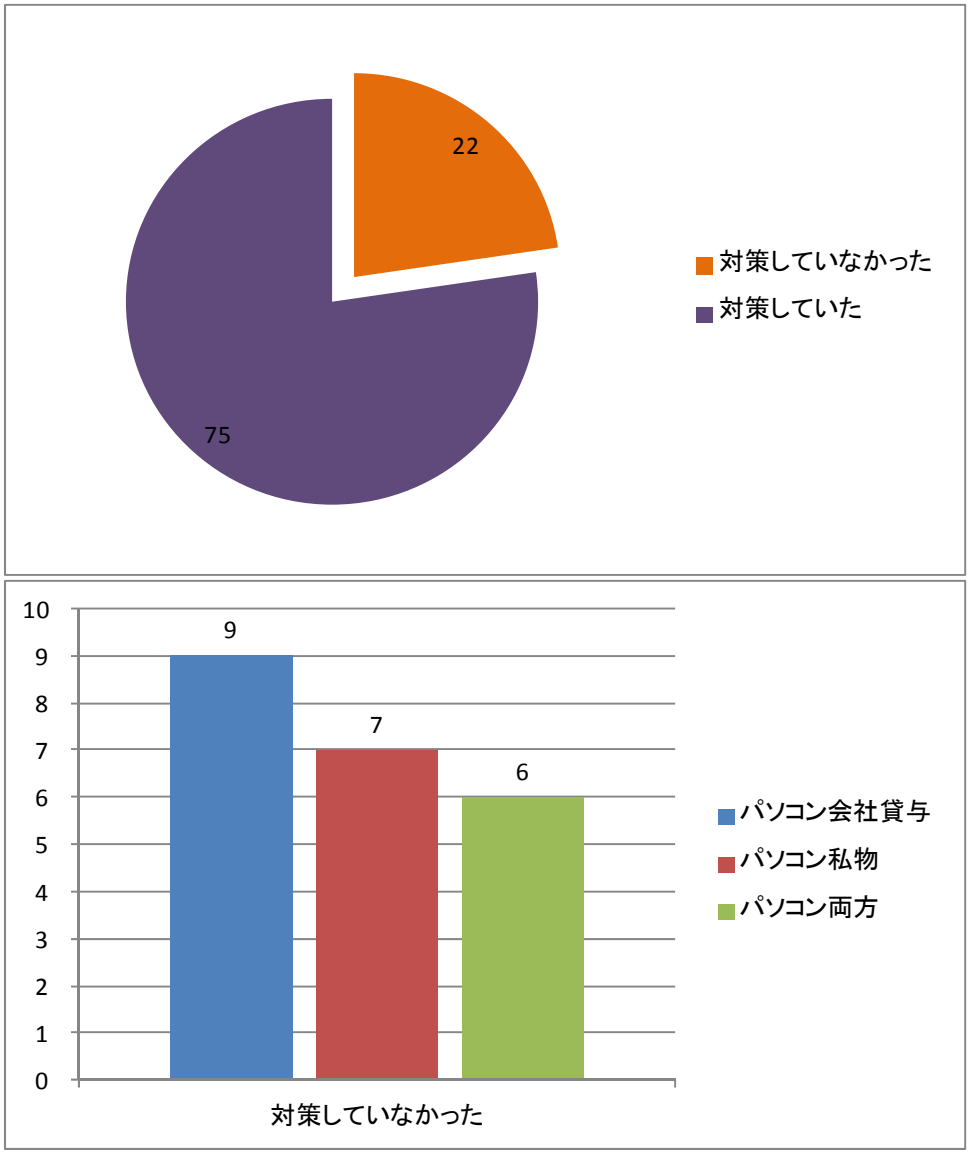


図 3-27：盗難紛失対策をしていなかったパソコンの内訳（人数）

業務データが入ったパソコンを紛失した・盗難にあった者 97 人の内、紛失・盗難の対策をしていなかった人は 22 人であった。そのうち、会社貸与のパソコンを対策せずに紛失・盗難した人が 9 人、私物のパソコンを対策せずに紛失・盗難した人が 7 人であった。パソコンの紛失・盗難についても、未対策の会社貸与パソコンと私物パソコンの間で顕著な差があるとは言えない。

(3). USB メモリ

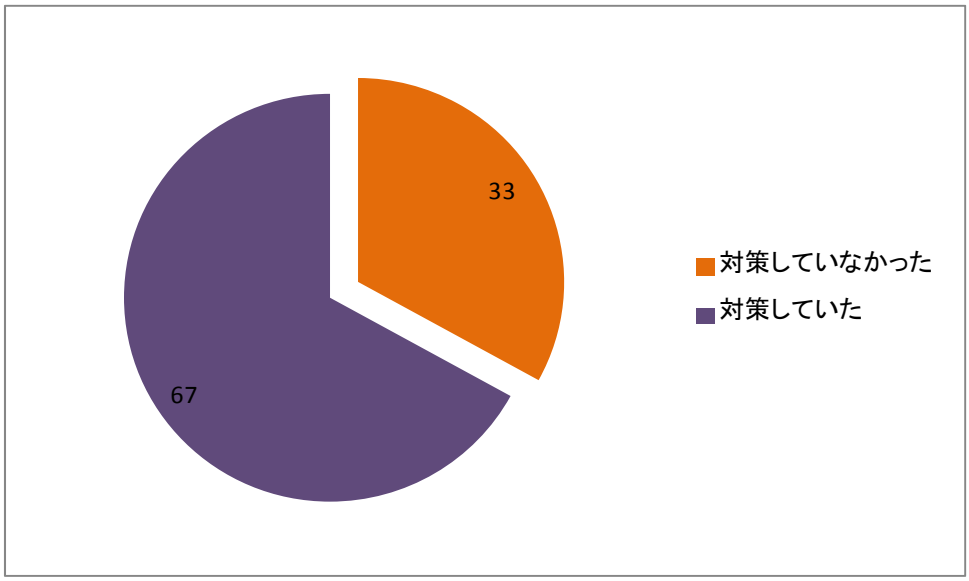


図 3-28：USB メモリの盗難紛失対策の実施状況（人数）

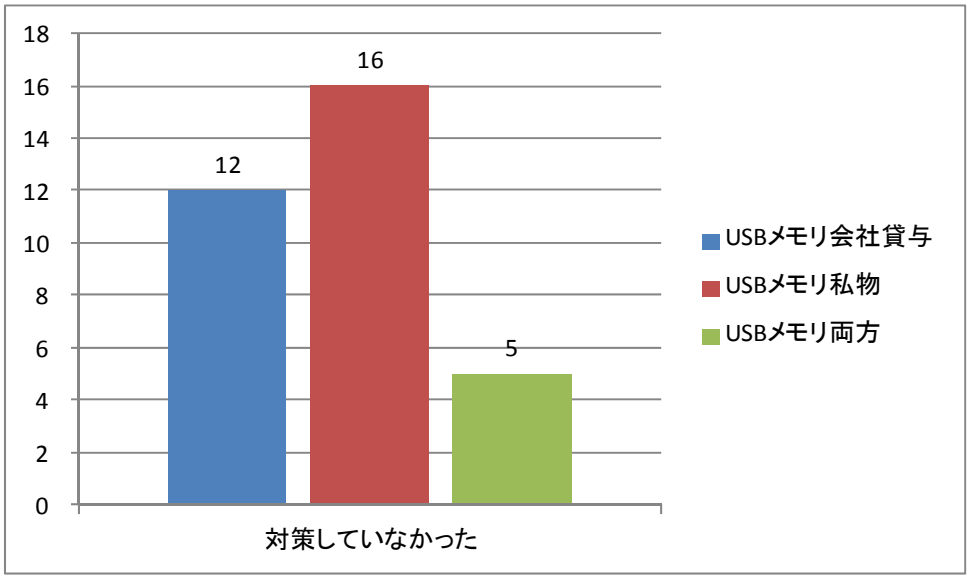


図 3-29：盗難紛失対策をしていなかった USB メモリの内訳（人数）

業務データが入った USB メモリを紛失した・盗難にあった者 100 人の内、紛失・盗難の対策をしていなかった人が 33 人であった。そのうち、会社貸与の未対策の USB メモリを紛失・盗難した人が 12 人、私物の未対策の USB メモリを紛失・盗難した人が 16 人であった。私物の未対策の USB メモリを紛失・盗難する確率のほうがやや高くなっている。これは、組織内で USB メモリの使用を禁止していることによる影響が現れていると予想する。

3.7.3. 事後対応

携帯電話、パソコン、USB メモリを紛失・盗難にあった人、それぞれ 100 人について、紛失・盗難後に会社、組織に報告・連絡した場合と何もしなかった場合について、「会社貸与」「私物」「両方」の割合を調査した。

表 3-18：盗難・紛失の報告/未報告の人数

	報告した				何もしなかった			
	会社貸与	私物	両方	合計	会社貸与	私物	両方	合計
携帯電話	19 人	10 人	12 人	41 人	10 人	11 人	4 人	25 人
パソコン	16 人	12 人	8 人	36 人	10 人	7 人	6 人	23 人
USB メモリ	13 人	12 人	5 人	30 人	11 人	15 人	4 人	30 人

(1). 携帯電話

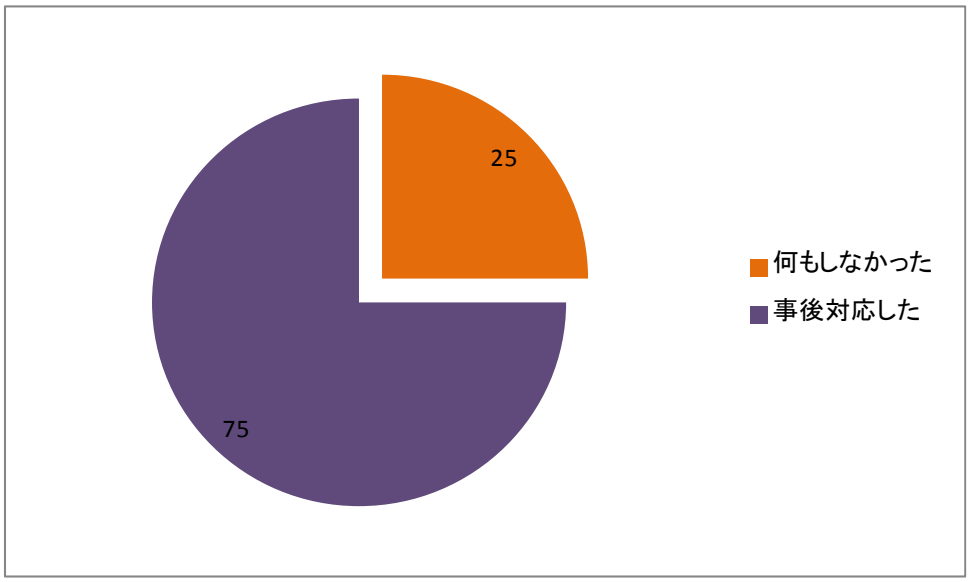


図 3-30：携帯電話の盗難紛失後の対応状況（人数）

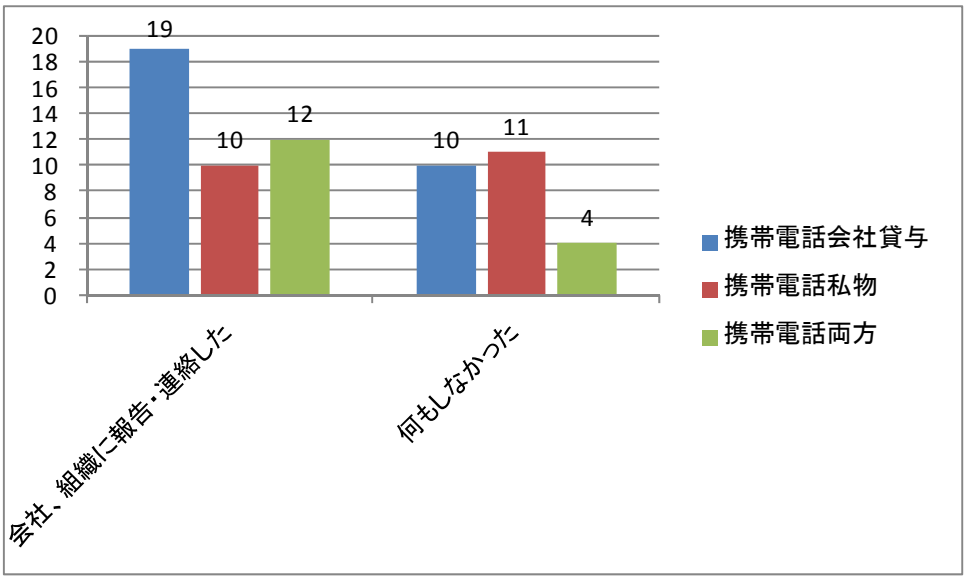


図 3-31：携帯電話の盗難紛失後の対応状況の内訳（人数）

業務データが入った携帯電話を紛失した・盗難にあった者 100 人の内、事後に何も対応しなかった人は 25 人であった。そのうち、それが会社貸与の携帯電話の場合は 10 人、私物の携帯電話の場合は 11 人であった。事後に報告・連絡した人は、会社貸与の携帯電話の場合は 19 人で私物が 10 人であった。会社貸与の携帯電話を紛失・盗難した場合は、多くの場合、会社へ連絡していることがわかる。ただし、約 1/3 は連絡を行っておらず、問題である。

(2). パソコン

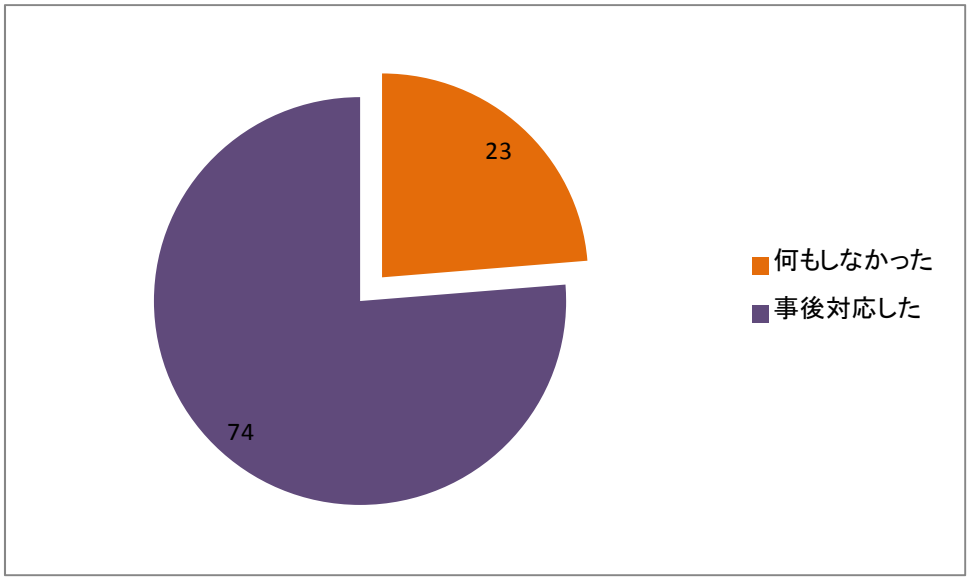


図 3-32：パソコンの盗難紛失後の対応状況（人数）

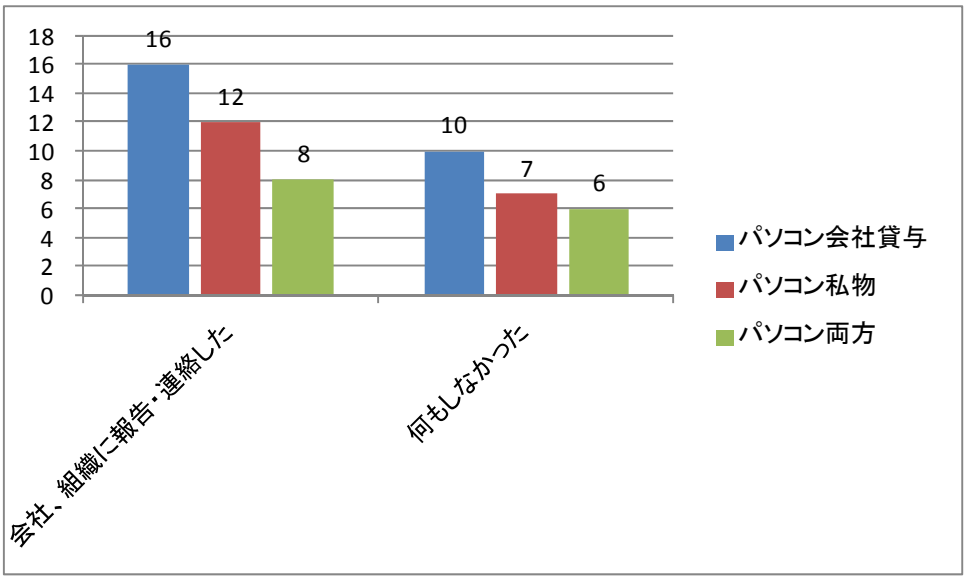


図 3-33：パソコンの盗難紛失後の対応状況の内訳（人数）

業務データが入ったパソコンを紛失した・盗難にあった者 97 人の内、事後に何も対応しなかった人が 23 人であった。そのうち、会社貸与のパソコンの場合が 10 人、私物パソコンの場合が 7 人であった。事後に報告・連絡した人は、会社貸与のパソコンの場合が 16 人、私物のパソコンの場合が 12 人であった。こちらも、会社貸与のパソコンの紛失・盗難を連絡していない人が多い。

(3). USB メモリ

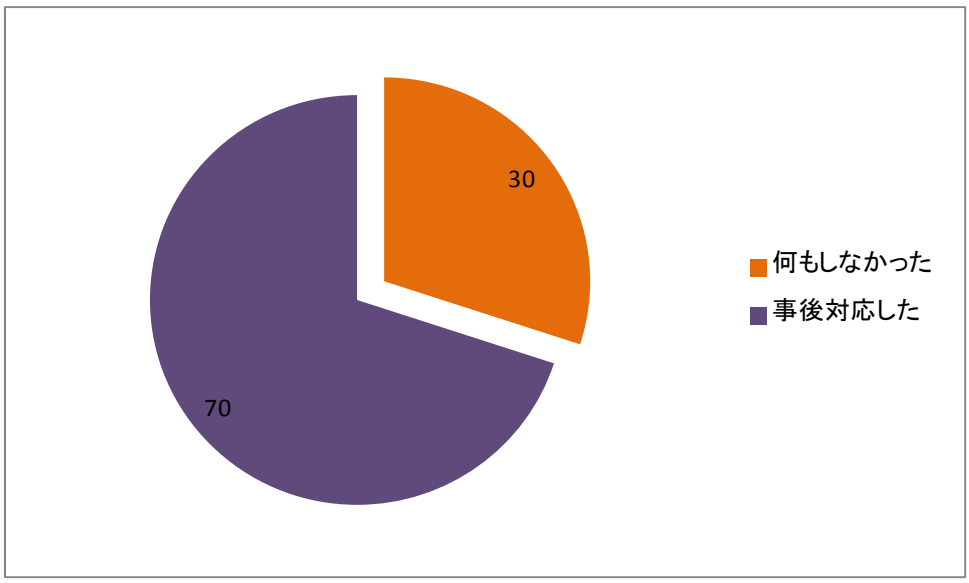


図 3-34：USB メモリの盗難紛失後の対応状況（人数）

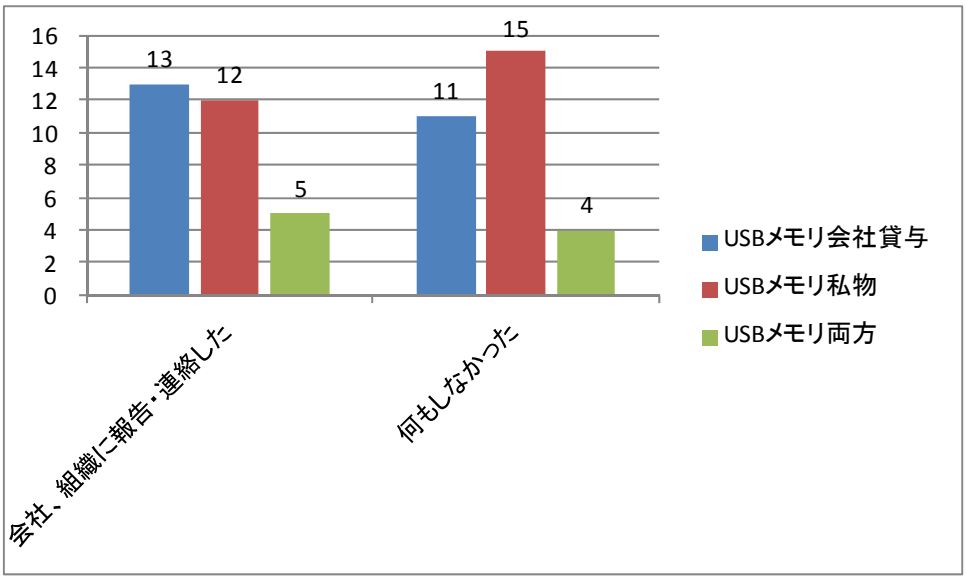


図 3-35：USB メモリの盗難紛失後の対応状況の内訳（人数）

業務データが入った USB メモリを紛失した・盗難にあった者 100 人の内、事後に何も対応しなかった人は 30 人であった。そのうち、会社貸与の USB メモリの場合が 11 人、私物の USB メモリの場合が 15 人であった。事後に報告・連絡した人は、会社貸与の USB メモリの場合が 13 人、私物の USB メモリの場合が 12 人であった。

3.7.4. 私物を業務に使用するリスク

以上の分析から、事前の盗難・紛失対策が実施されていない携帯電話とパソコンは、会社貸与であっても私物であっても、発生確率に大きな違いはないことがわかった。USB メモリは、私物の未対策の USB メモリを紛失・盗難する確率のほうがやや高くなったが、組織内で USB メモリの使用を禁止していることによる影響が現れていると予想する。

つまり、会社貸与の物と私物の紛失・盗難インシデントの発生確率に大きな違いはなく、紛失・盗難のリスクの差はないと思われる。

4. まとめ

今回の調査結果を踏まえ、JNSA セキュリティ被害調査ワーキンググループでは、日本の情報セキュリティはどうあるべきか、これからどのようなことをすればよいのかなどについて討議を重ねた。その結果、次のように提言したい。

4.1. 個人特性の分析結果から

今回の調査結果から、IT 知識や情報セキュリティ知識を持っている人のほうが、情報セキュリティインシデントの発生確率が高いことがわかった。この理由の一つとして、概念的な知識はあっても、知識が具体的な対策レベルになっていない場合や、知識が具体的な行動に結びついていない場合が考えられる。また、情報セキュリティ知識を持っている分、自分は全てのリスクを回避できると思い込んで、自らリスクが高い状況へ踏み込んでしまう場合も考えられる。当 WG では、もともと情報セキュリティインシデントが発生する確率の高い仕事をしている人々は、組織内でおり、必ず IT 知識や情報セキュリティ知識の教育を受けなければならないために必然的に知識を持っている場合が多く、上記のような調査結果が現れたのではないかと考える。いずれにせよ、知識を持っているだけでは情報セキュリティインシデントの発生は減らせず、行動が伴わなければ意味がない。

また、性格と情報セキュリティインシデントの発生確率は、関係性が低いことがわかった。つまり、自分は慎重派だと思っていても、情報セキュリティインシデントの発生確率は、他人とはあまり違いがないのである。

一方、特定の行動特性とインシデントには関連があることがわかった。行動特性は、本人だけでなく、周囲の人でも客観的に把握できる。したがって、周囲の人は、対象者の行動特性を手掛かりにして、情報セキュリティインシデントの発生確率の高低を予想したり、インシデントの発生を抑制できるかもしれない。例えば、業務多忙によって、遅刻や勘違いが多発している場合は、情報セキュリティインシデントの発生確率も上昇している恐れがある。その場合は、その要因である業務多忙な状況を改善することによって、情報セキュリティインシデントの発生を抑制できるかもしれない。

4.2. 次の対策は

知識を持っているだけでは情報セキュリティインシデントは減少しないと言っても、教育は必要である。ただし、対象者へは、「携帯電話を社外で紛失しない」「機密情報が添付された電子メールを誤送信しない」といった漠然とした禁止事項や表面的な知識だけを教育するだけでは不十分である。具体的な対策を実行できるレベルの知識まで教育する必要がある。対象者が具体的な対策を実行できるレベルとは、「携帯電話は暗証番号を掛ける」「機密情報を含む重要なメールは長期間保存しないで削除する」「機密性が高い情報を送信する

時は、通信内容を暗号化し、送信相手の受信確認が行える等の安全なファイル送信システムを使用する」といった具体的な行動例を提示して、実施させることである。

さらに対象者が具体的な対策を実施しているかどうか、自主点検や情報セキュリティ監査によって確認するべきである。対象者へ、具体的な対策を確実に実施させるには、対策に関連する具体的な行動の実施を自己宣言させて責任感を持たせること、自主点検だけでなく、第三者による監査を取り入れる方法が有効である。また、自主点検では信ぴょう性が足りない場合も、第三者による監査が有効である。これらを実施することによって、初めて対策を実行しているレベルに到達したといえる。

なお、罰則を厳しくするとインシデントを報告しなくなる傾向がある。したがって、インシデントをもれなく報告させるためには、速やかに報告した場合は罰則を適用しないというルールが有効である。もちろん、インシデントは早期に対応し、被害を最小に押さえなければならないため、インシデント報告の遅延や虚偽の報告、インシデントの隠蔽には厳罰を適用すべきである。

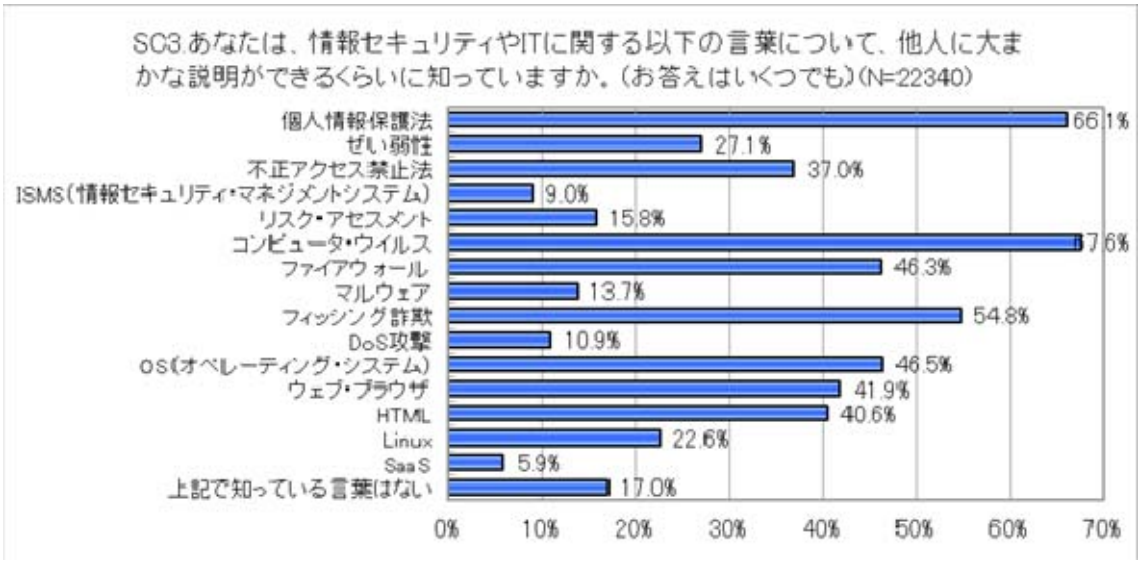
特定の行動特性とインシデントには関連があることがわかっているため、周囲の人が対象者の行動を客観的に把握し、注意を払うことによって、インシデントの発生を抑制できる可能性がある。

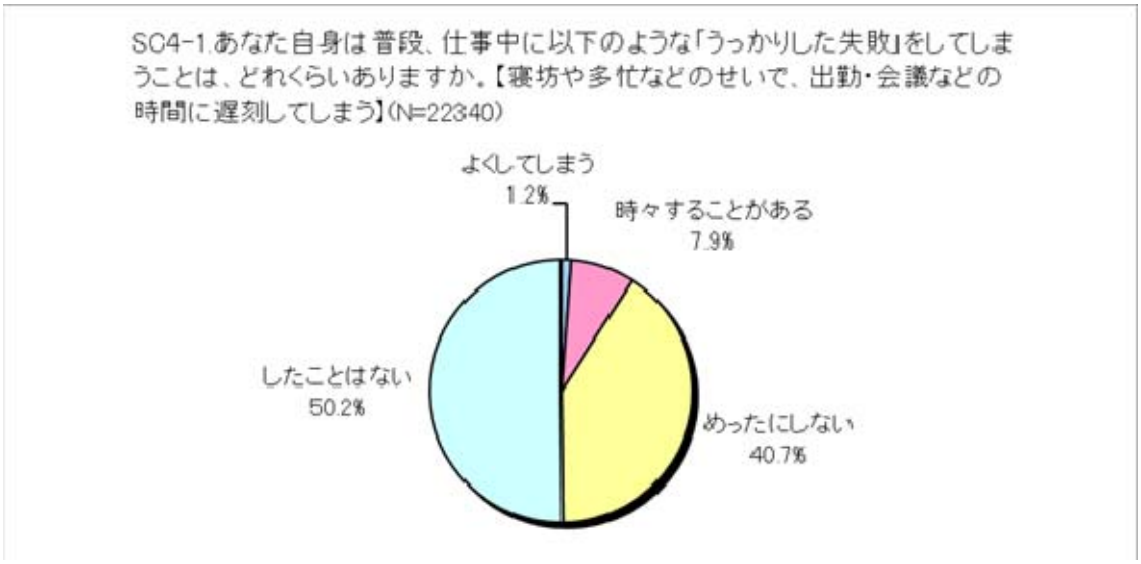
誰でも少しは経験しているが、業務多忙になってくると遅刻や勘違いが発生しやすいものである。インシデントも業務多忙だと発生しやすくなる。したがって、業務多忙の原因を除去することによって、インシデントの発生を抑制できるかもしれない。遅刻や勘違いが多かったり、業務に関係ない書き込み、雑談等をしている職場は、このルール違反を黙認、放置していると、一般的にルール違反が常態化し、インシデントが発生しやすい環境になる。したがって、職場のルール違反の黙認や放置をしないことによって、インシデントの発生を抑制できるのではないだろうか。

明るくかつ統制のある良い雰囲気の職場作りやプロジェクト管理が必要なのかも知れない。

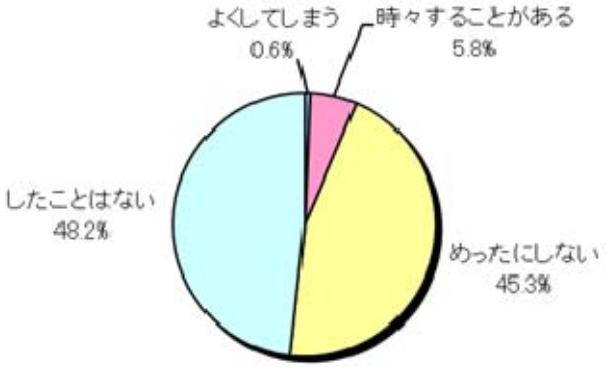
5. 付録:単純分析

5.1. 共通質問

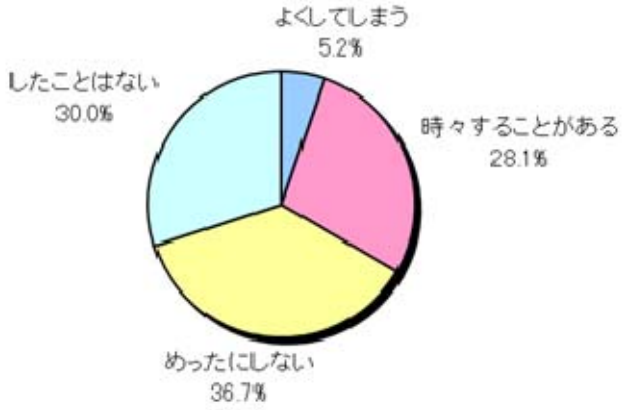




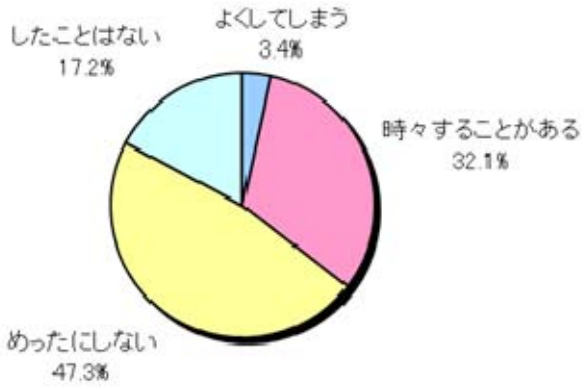
SC4-2.あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【仕事上の約束や予定スケジュールを勘違いして、人に迷惑をかけてしまう】(N=22340)



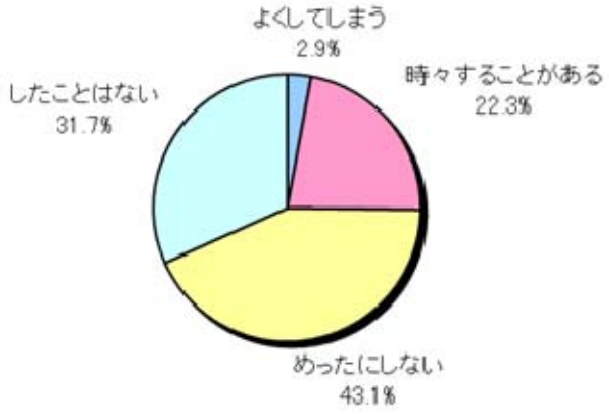
SC4-3.あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【机の上や引き出しの中が片付かず、書類などが見つからなくなる】(N=22340)



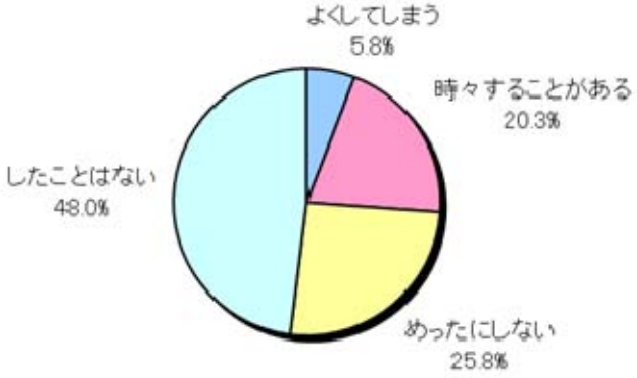
SC4-4.あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【自宅などに忘れ物をする】(N=22340)



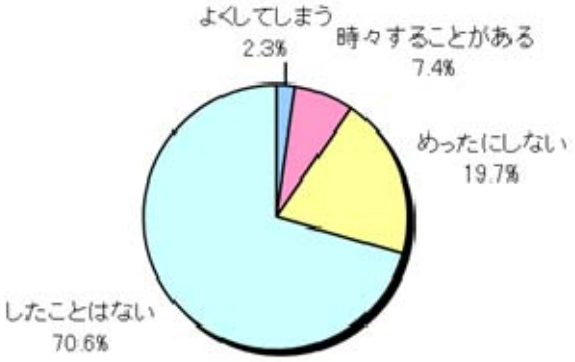
SC4-5.あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に居眠りや、ぼうっとして時間を過ごしてしまう】(N=22340)



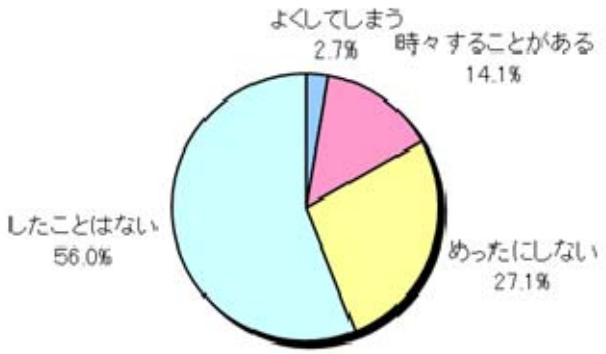
SC4-6.あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に関係のないウェブサイトや掲示板・ブログ、SNS、ツイッターなどを見て時間を過ごしてしまう】(N=22340)



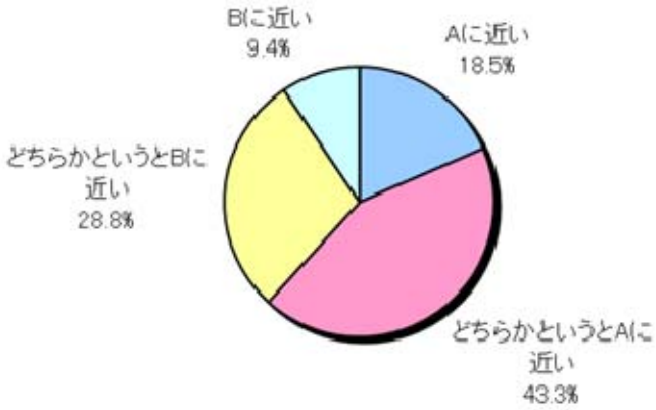
SC4-7.あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に関係のない掲示板・ブログ、SNS、ツイッターなどに書き込みをして時間を過ごしてしまう】(N=22340)



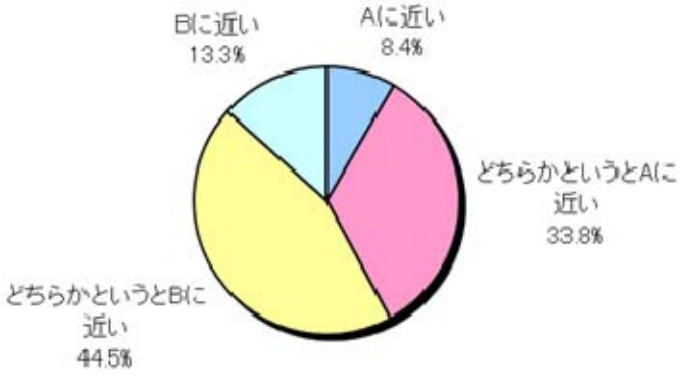
SC4-8.あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に関係のない雑談、メールやチャットのやりとりなどをして時間を過ごしてしまう】(N=22340)



SC5-1.人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ1つ)【きちょうめんな/大雑把な】(N=22340)



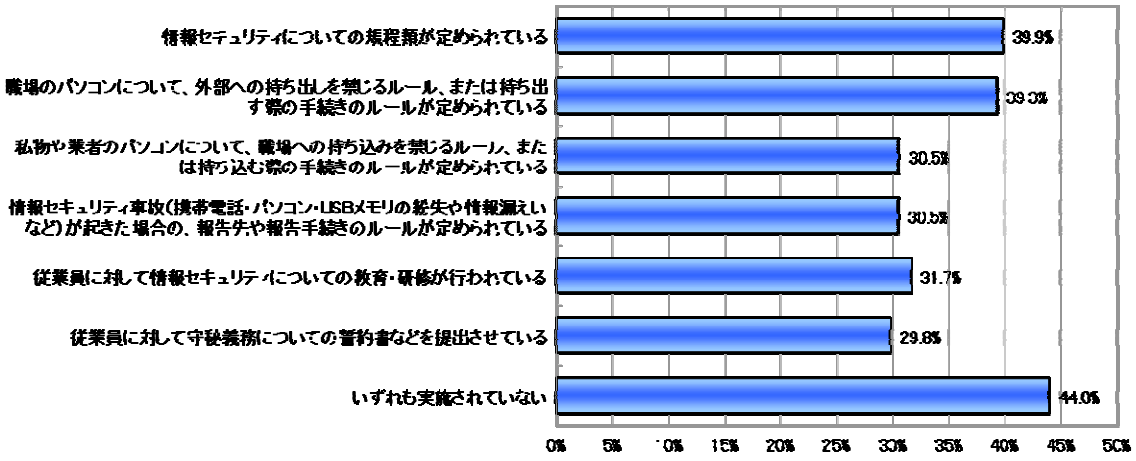
SC5-2.人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ1つ)【悲観的な/楽天的な】(N=2234Q)

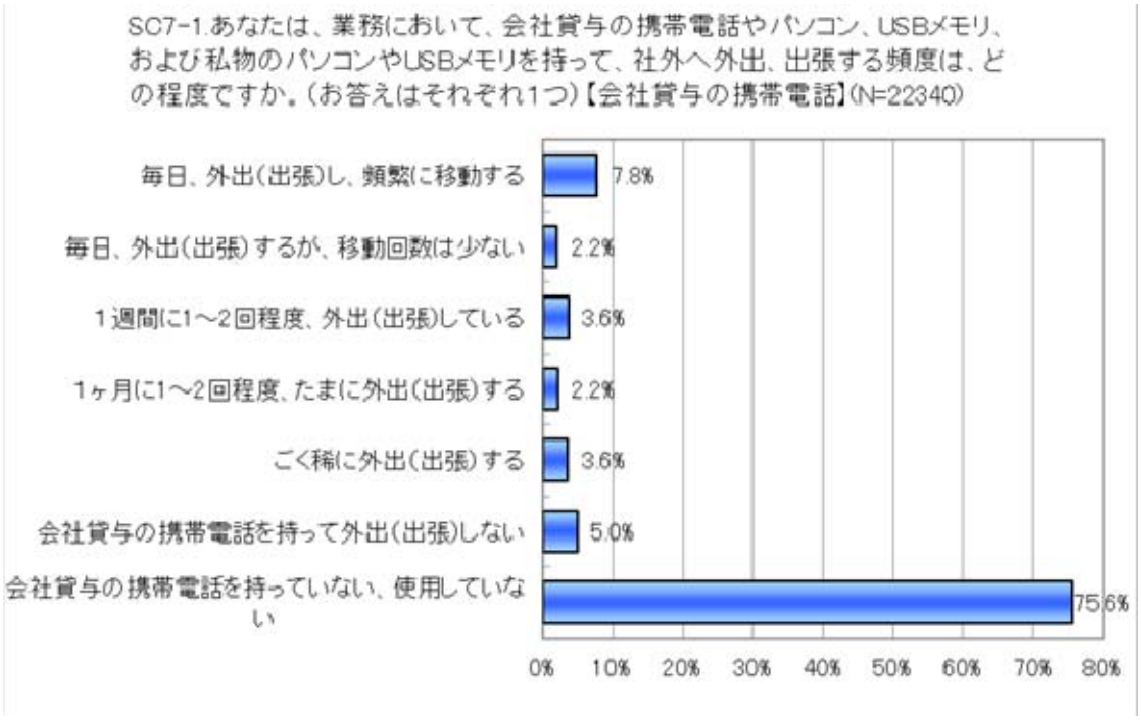


SC5-3.人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ1つ)【生真面目な/いい加減な】(N=2234Q)

SC5-4.人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ1つ)【慎重な/おっちょこちょいな】(N=22340)

SC6. あなたが働いている職場で、以下の事項は実施されていますか。(お答えはいくつでも)(N=22340)

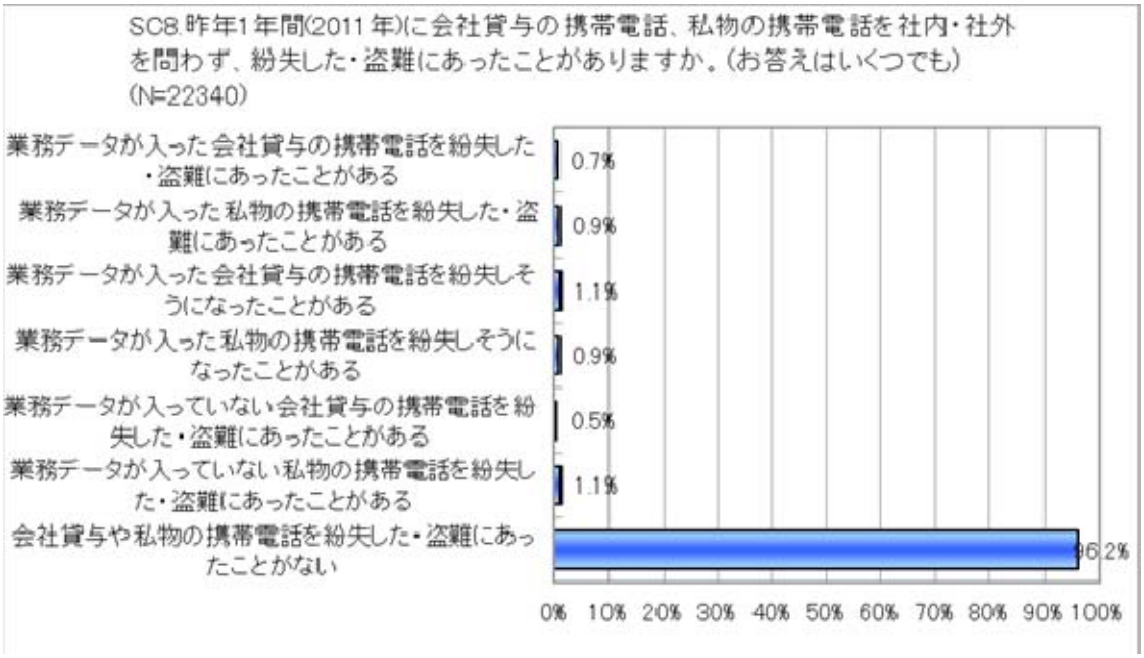




仕事をしている人 22340 人への調査によると、会社から携帯電話が貸与された人の外出頻度は、「毎日、外出(出張)し、頻繁に移動する」が 1 番多いが、2 番目には「会社貸与の携帯電話を持って外出(出張)しない」となっている。一方で「会社貸与の携帯電話をもっていない、使用していない」との回答が 75%を超えており、社員に携帯電話を必要としない、もしくは私物の携帯電話を利用することで十分と考える会社も多いことが分かる。

5.2. 携帯電話

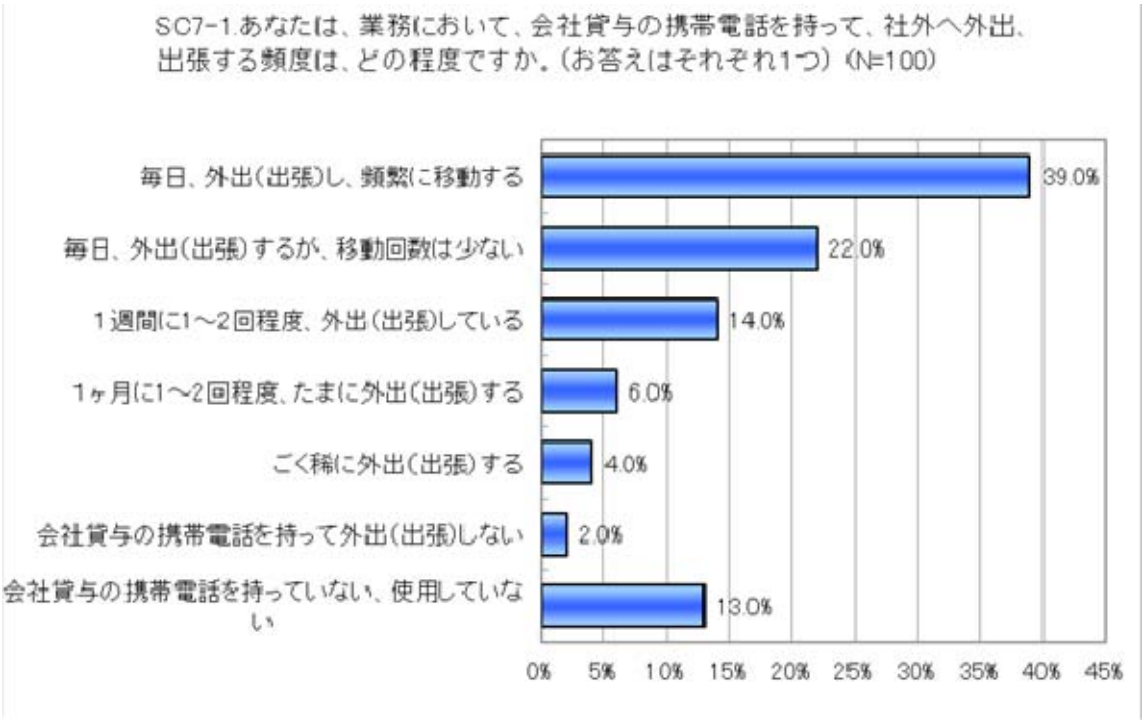
5.2.1. 予備調査の分析結果



私物、会社貸与の携帯電話を問わず、携帯電話をなくしたこと、なくしそうになったことがある人は全体約 4%である(全体から「会社貸与や私物の携帯電話を紛失した・盗難にあったことがない」を除く割合)。

最終的に会社携帯をなくした人(業務データが入っている場合と入っていない場合を合算)は、全体の 1.2%、私物携帯をなくした人は全体の 2.0%となっている。

以下は、各インシデントを経験した 100 人による回答である。



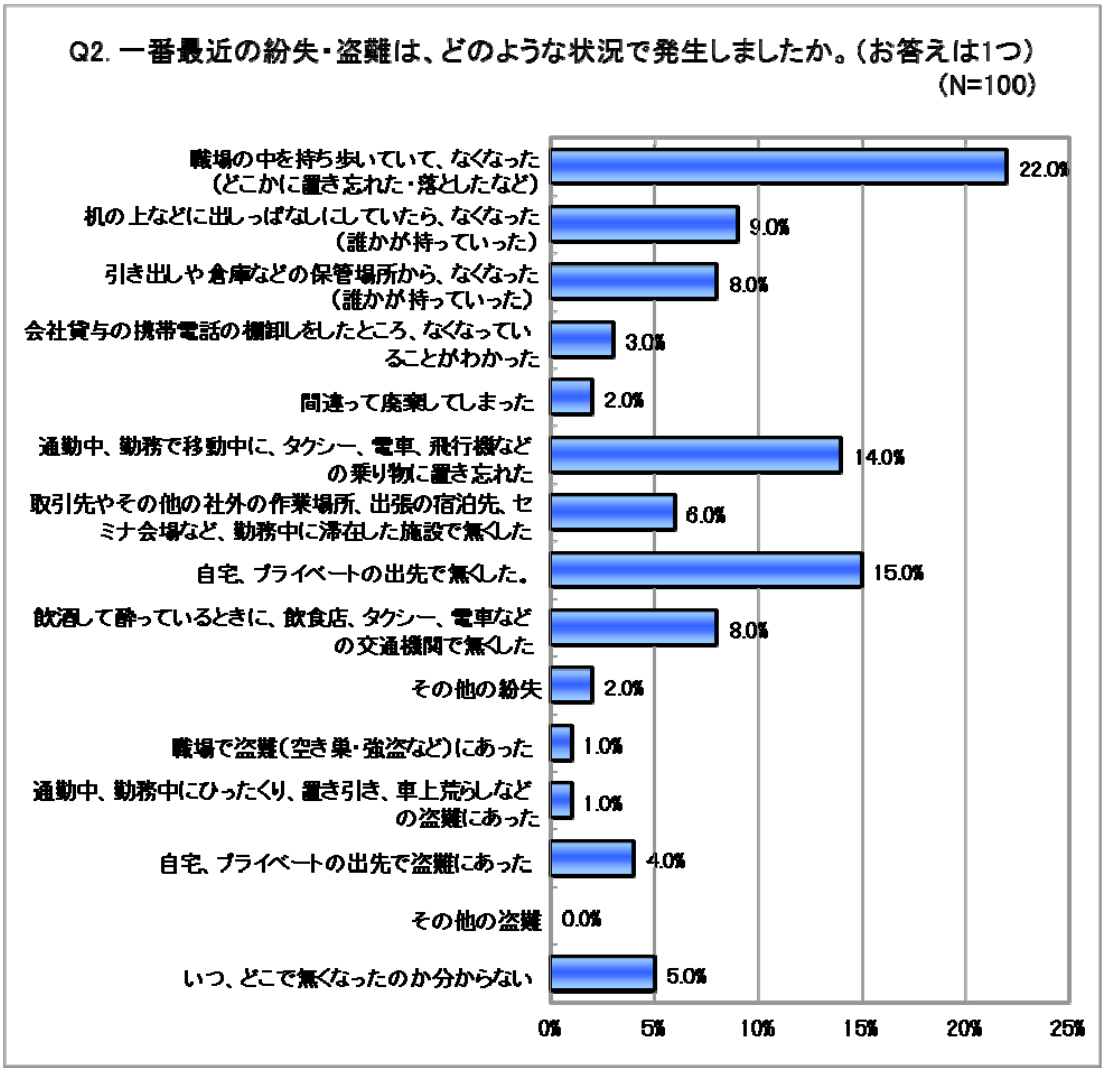
携帯電話を紛失した 100 人を対象とすると、外出頻度が多い人が携帯電話を紛失する割合が高くなり、外出頻度が低いと紛失する割合が低くなる傾向が確認された。

携帯電話の紛失・盗難に関しては業務における外出頻度が影響していることがわかる。

携帯電話を紛失した 100 人を対象とすると、「業務データ入った私物の携帯電話を紛失した・盗難にあったことがある」との回答が 62.0%に上る。「業務データ入っていない私物の携帯電話を紛失した・盗難にあったことがある」の割合が 9.0%であることを踏まえると、紛失した私物の携帯電話には業務データが入っている傾向が高いといえる。

「業務データが入った会社貸与の携帯電話を紛失しそうになったことがある」との回答が、「業務データが入った私物の携帯電話を紛失しそうになったことがある」という回答の倍近い割合となっている。これは、貸与された携帯の場合、一時的にでも見つからなくなった時点で紛失・盗難の可能性を考え捜索を行う可能性が高いためと想定される。

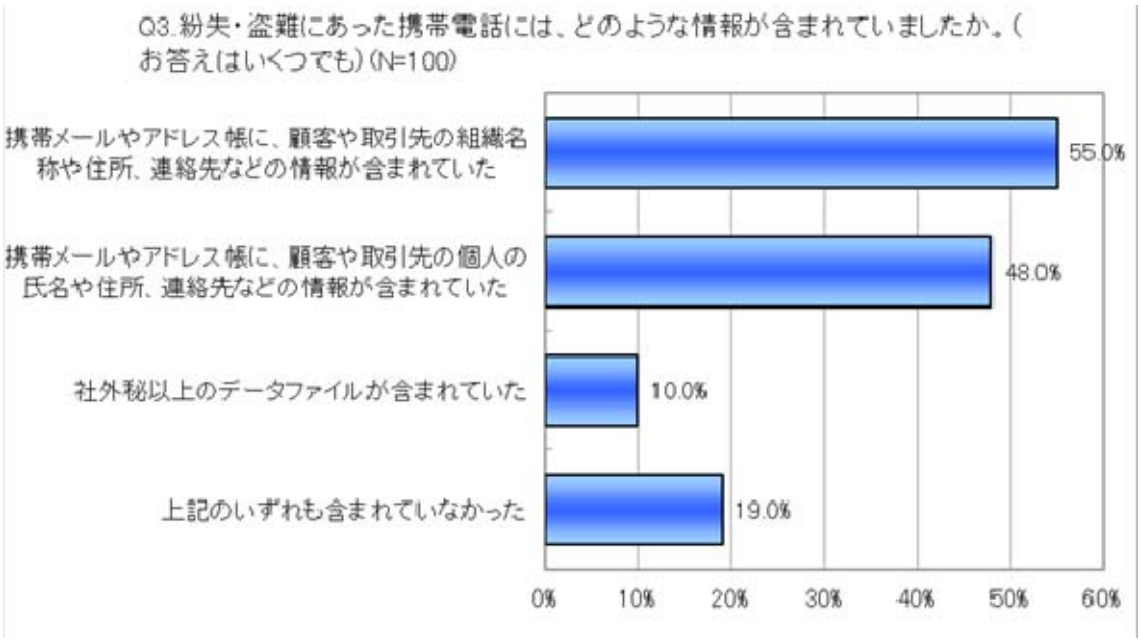
5.2.2. 本調査の分析結果



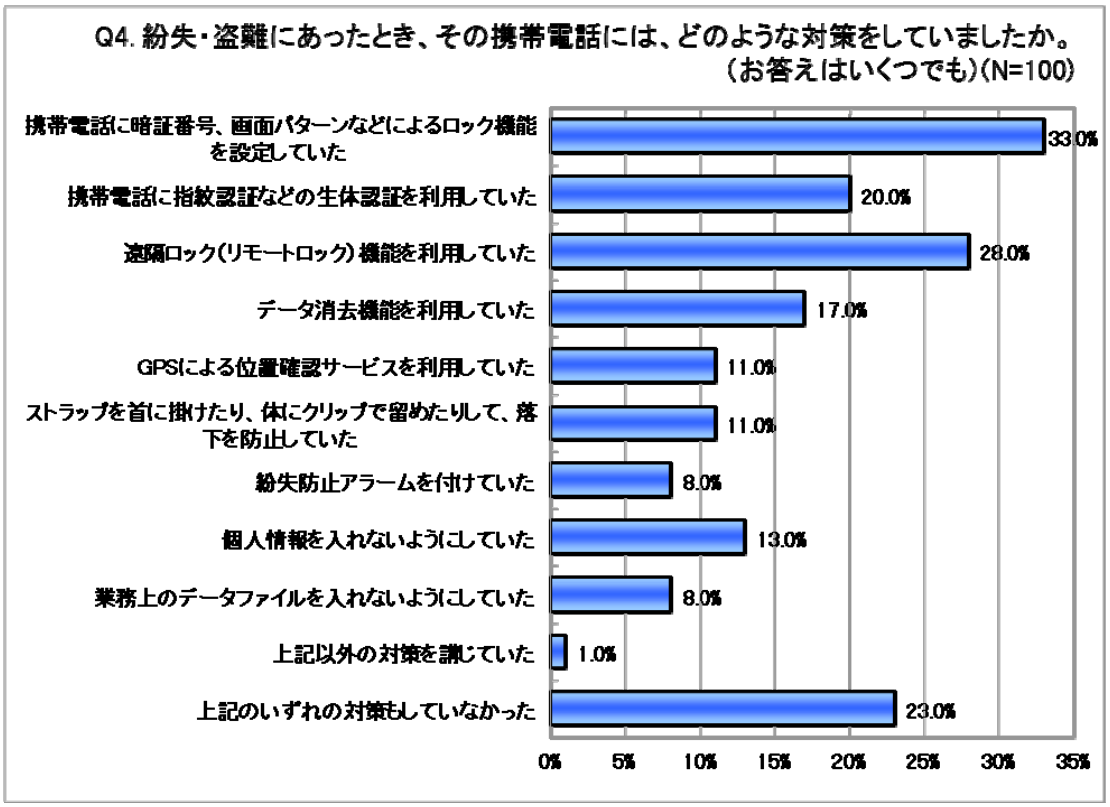
Q2FA1	一番最近の紛失・盗難は、どのような状況で発生しましたか。【その他の紛失(FA)】		
1	女性	52 才	職場のトイレに置き忘れて、探したがなくなっていた
2	男性	37 才	バイクで移動中に落とした

本調査では、紛失・盗難が発生した状況として「職場の中を持ち歩いて、なくなった」が22.0%と一番多く、次いで「自宅、プライベートの出先で無くした。」が 15.0%、「通勤中、勤務で移動中にタクシー、電車、飛行機などの乗り物に置き忘れた。」が 14.0%となっている。

なお、紛失においては、実際は盗難であった場合においても、回答者が明らかに盗難にあったと判断できる場合以外は、紛失として捉えられているものと考えられる。



紛失・盗難にあった携帯電話に、顧客データや社外秘以上のデータ等、業務に関係する情報が含まれていた場合は 81.0%(全体から「上記のいずれも含まれていなかった」を除く割合)であった。つまり紛失した携帯電話には、多くの場合で、なんらかの保護すべき企業の情報が含まれていることが分かる。

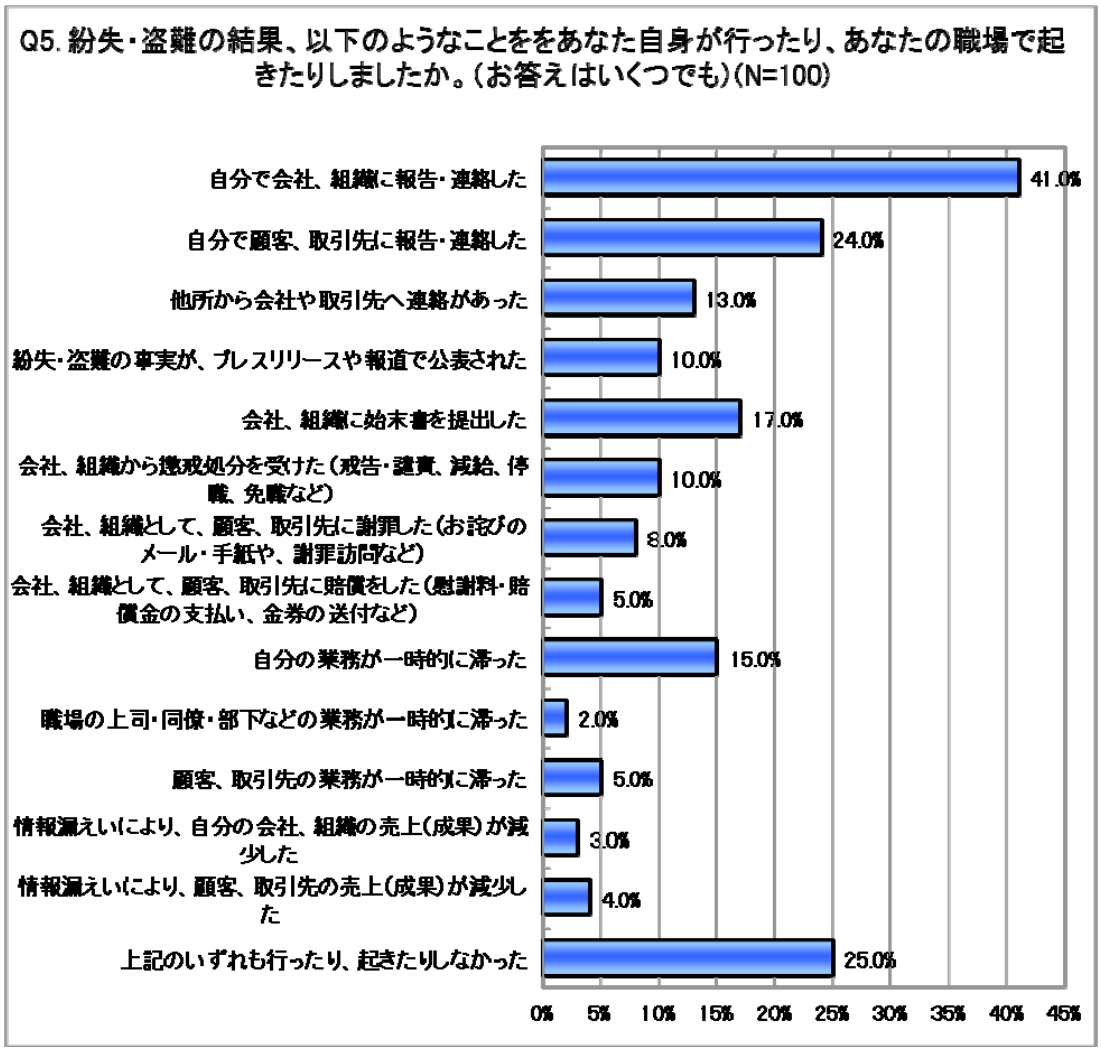


暗証番号は携帯電話では実装が容易な対策であり、文字数が適切であれば紛失した場合に情報漏えいを防ぐ有効な対策である。携帯電話によっては、画面パターンや生体認証も容易に実装ができる。対策の高い実施率が示すとおり、これらの認証機能の実装は携帯電話に必須と考えるべきである。

遠隔ロックも、割合が高く普及してきた対策とみることができる。紛失した後に実施できる携帯電話への対策としてメリットも大きい。紛失した携帯電話が電波の届く範囲にあるときのみ有効であることには留意しておきたい。

首かけストラップやクリップ、紛失防止アラームは紛失しないための対策であるが、紛失した携帯電話において、実施していたとする回答がそれぞれ 8.0%になっている。ストラップの損傷や紛失防止アラームの故障等、対策が機能しない状況が発生したと想定される。

「いずれの対策もしていなかった」が 23.0%となっている。多くの場合、携帯電話に個人情報や業務データが含まれるため、2 割以上の紛失した携帯電話が、容易に情報が盗み見られるという状況は、改善すべき問題である。

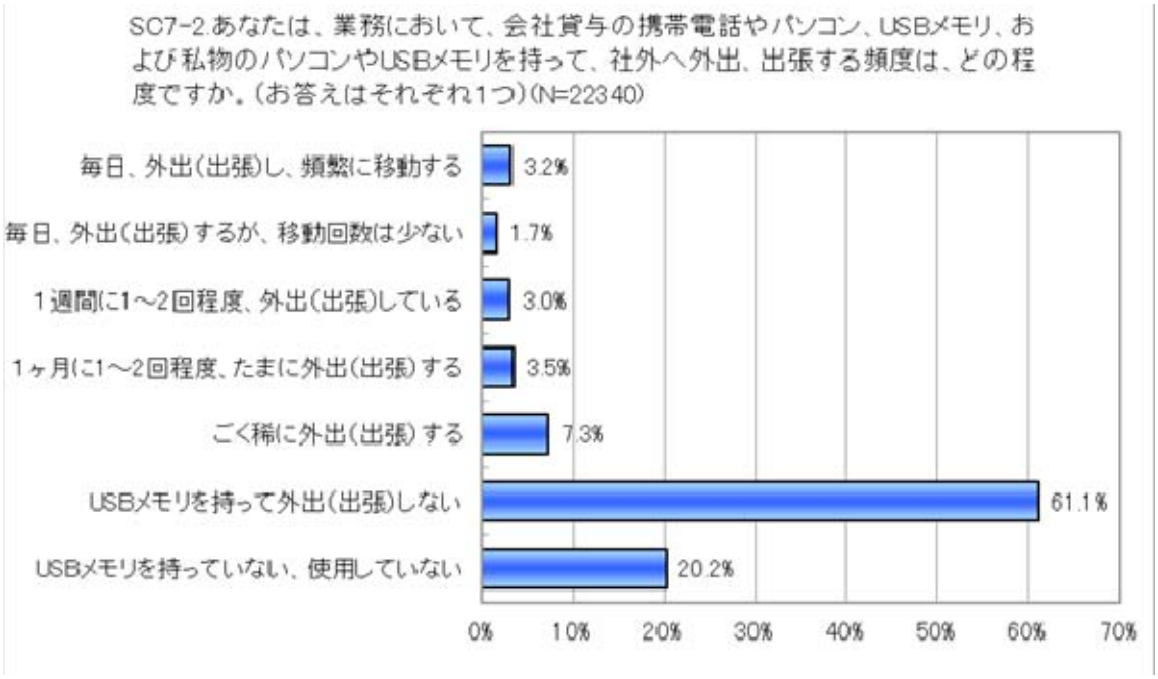


「顧客や取引先の業務が一時的に滞った」が 5.0%、及び「顧客、取引際の売上が減少した」が 4.0%あり、発生した携帯電話の紛失・盗難により顧客や取引先に実害をもたらしている。

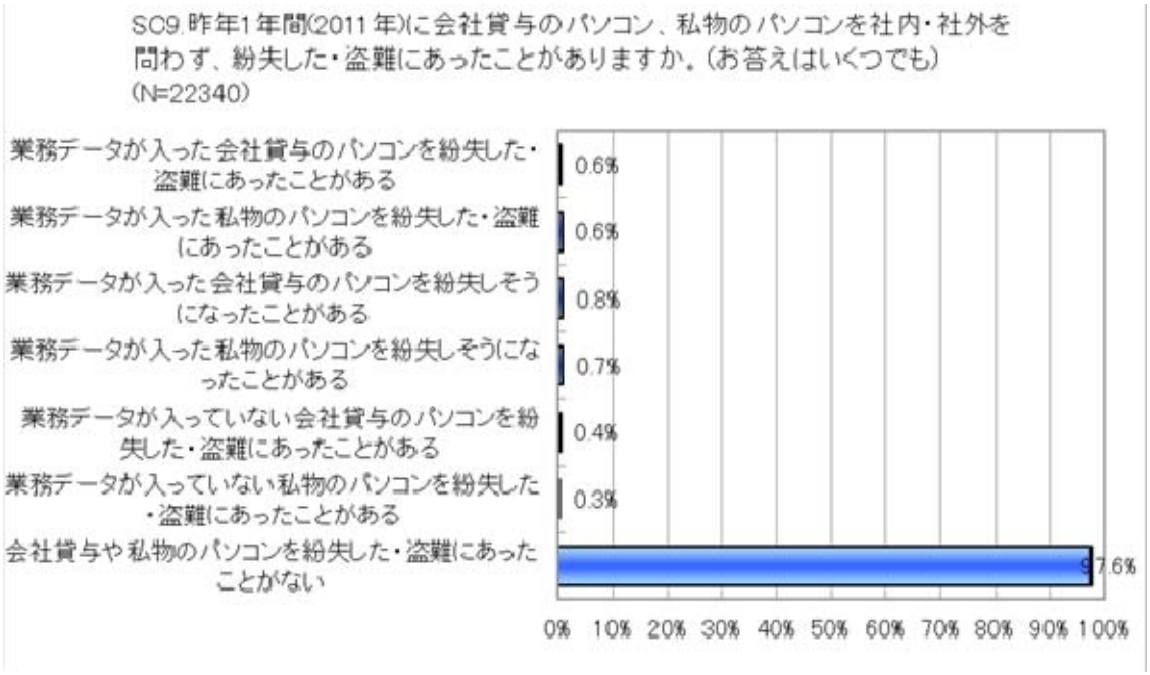
「上記のいずれも行ったり、起きたりしなかった」が 25%とあるが、これは報告さえしなかった割合である。紛失した際に報告する必要がない携帯電話は「業務データが入っていない私物の携帯電話」と考えられるが、それらの携帯電話が紛失する割合は 9%にとどまる(SC8 の回答による)。そのため報告さえしない回答の 25%は、問題のある割合である。

5.3. パソコン

5.3.1. 予備調査の分析結果



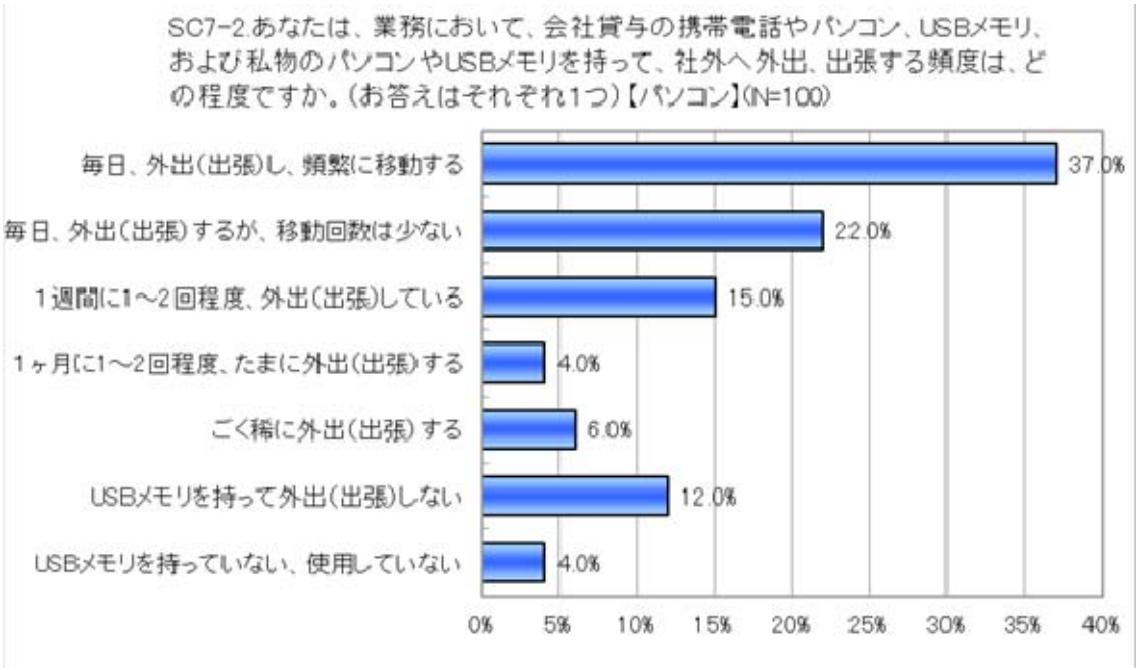
仕事をしている人 22340 人への調査によると、業務でパソコンを利用している割合は約 8 割に至るが、全体の 6 割はパソコンを利用しているものの「持って外出しない」。全体の約 2 割が、パソコンを社外に持ち出す割合(全体から「持って外出しない」と「持っていない、使用していない」を除く割合)である。



「会社貸与や私物のパソコンを紛失した・盗難にあったことがない」の回答が 97.6%に至る。全体から「会社貸与や私物のパソコンを紛失した・盗難にあったことがない」と「紛失しそうになった」の割合を除いた、実際に紛失・盗難が発生した割合は、1.9%であり低い割合である。

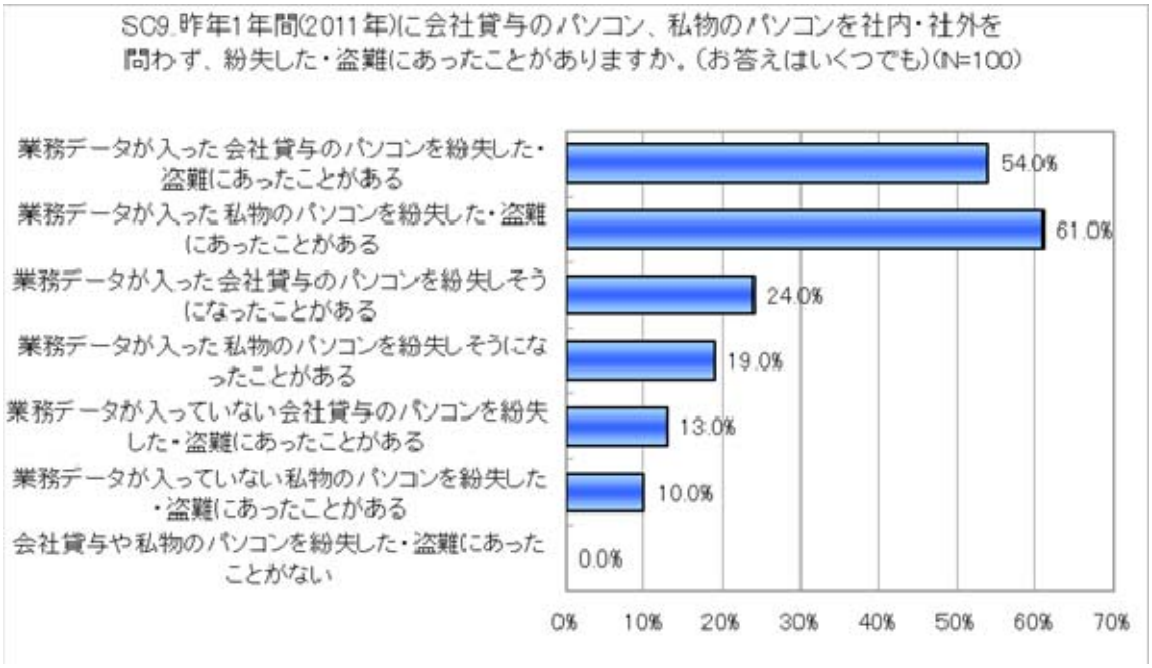
ただ、パソコンは膨大なデータを保管できる。そのため、紛失・盗難の発生確率が低くとも、一度の被害が大きくなる可能性は注意すべきである。上記の紛失・盗難確率をパソコン 1000 台あたりに換算すると、1 年間あたりの紛失・盗難台数は、以下のようになる。

業務データが入った会社貸与のパソコンを紛失した・盗難にあったことがある=5.5 台
業務データが入った私物のパソコンを紛失した・盗難にあったことがある=5.8 台
業務データが入った会社貸与のパソコンを紛失しそうになったことがある=7.8 台
業務データが入っていない会社貸与のパソコンを紛失した・盗難にあったことがある=6.9 台
合計=26 台



パソコンを紛失した 100 人を対象とすると、外出頻度が多い人がパソコンを紛失する割合が高くなる傾向を示す。一方で、「持って外出しない」人の紛失も 12.0%である。これは「たまに外出する」人が紛失する割合よりも大きい。

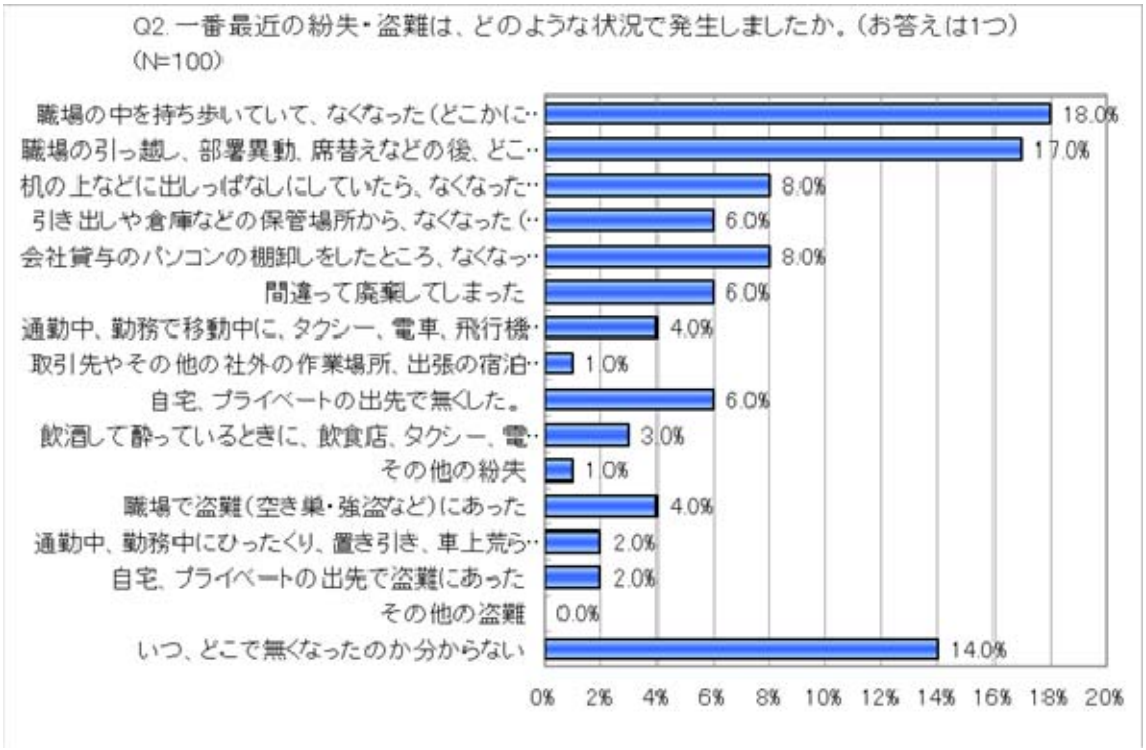
回答は、パソコンを持って「毎日、外出し頻繁に移動する」場合の管理が重要である一方で、社内にあるパソコンにも十分に注意すべきことを示唆している。



パソコンを紛失した 100 人を対象とすると、「業務データが入った私物のパソコンを紛失した・盗難にあったことがある」との回答が 61.0%に上る。「業務データが入っていない私物のパソコンを紛失した・盗難にあったことがある」との回答が 10.0%であることを踏まえると、紛失した私物のパソコンには業務データが入っている傾向が高いといえる。

「会社貸与のパソコンを紛失しそうになったことがある」との回答が、私物のパソコンの場合よりも多い。これは、貸与されたパソコンの場合、一時的にでも見つからなくなった時点で紛失・盗難の可能性を考え捜索を行う可能性が高いためと想定される。

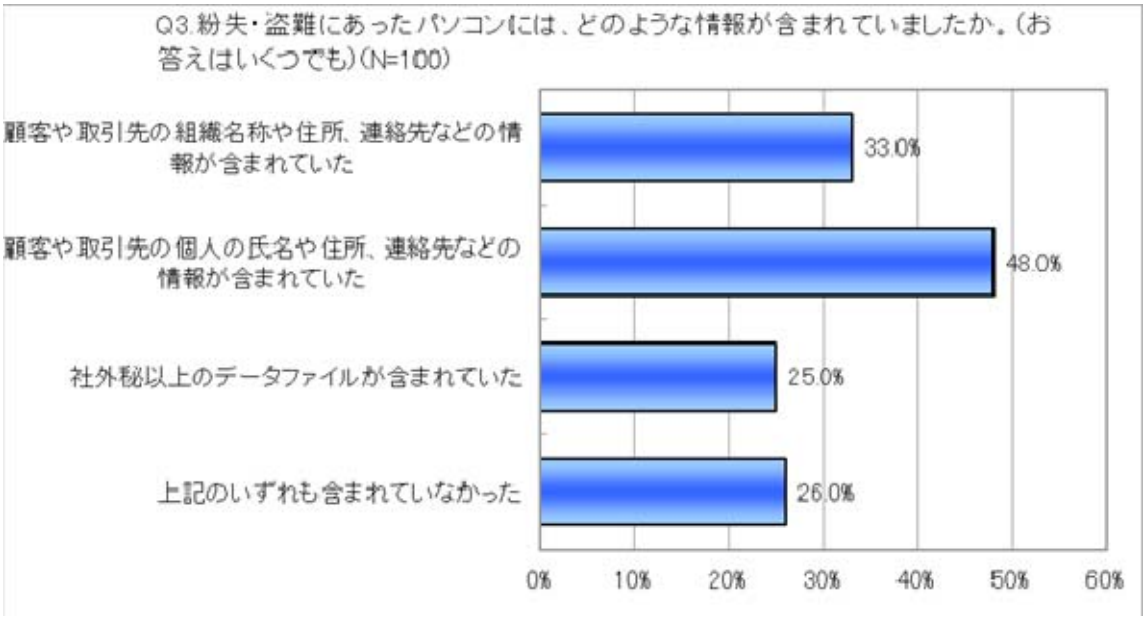
5.3.2. **本調査の分析結果**



Q2FA1	一番最近の紛失・盗難は、どのような状況で発生しましたか。【その他の紛失(FA)】			
1	男性	50 才	東京都	修理に出すかどうかで店員に渡したまま、受け取り状を発行され忘れられた

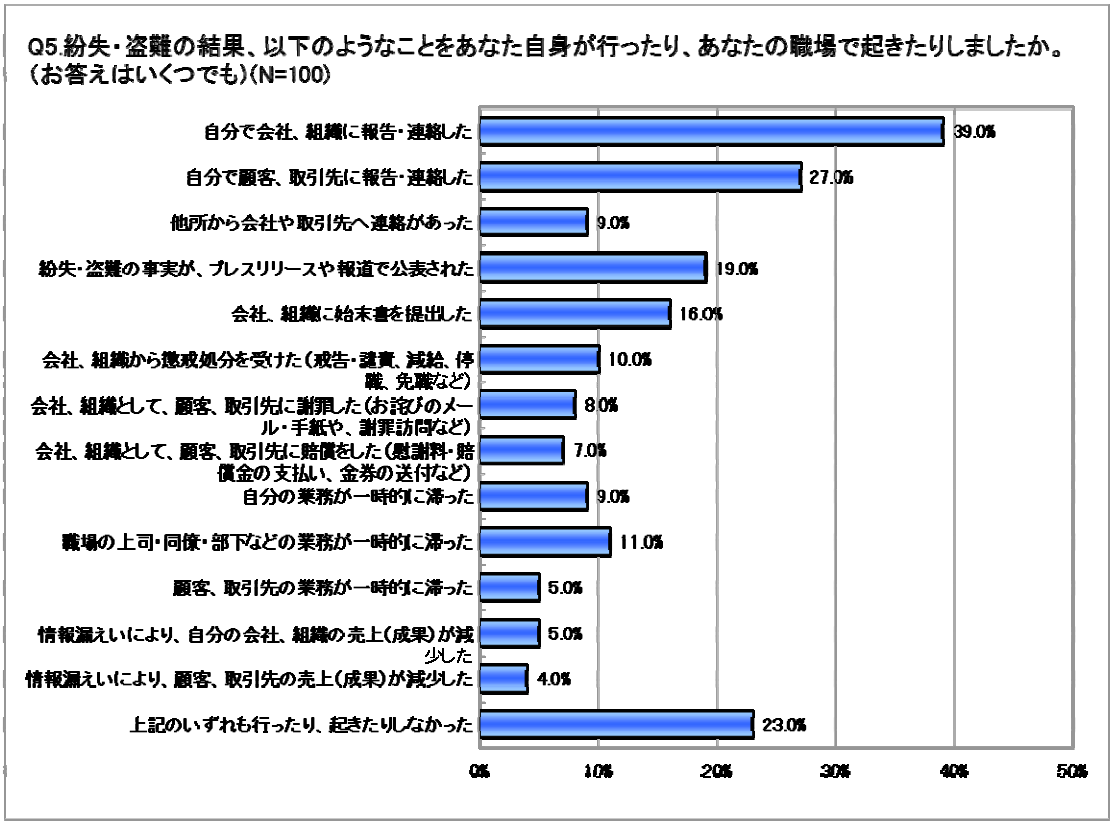
実際にパソコンの紛失・盗難にあった 100 人の回答によると、紛失・盗難の発生場所は社内が上位を占める。

「いつ、どこで無くなったのか分からない」も 14%に至り、その割合が目立つ。パソコンは一定の大きさをもつ機器であるため、携帯電話や USB メモリのように何かに紛れたり、知らぬ間に落としたりする可能性は低い。在庫管理などの組織的な管理の不備によって引き起こされているように思える。



実際にパソコンの紛失・盗難にあった 100 人の回答によると、紛失・盗難にあったパソコンに、顧客データや社外秘以上のデータなどの業務に関係する重要な情報が含まれていた割合は 74.0%(全体から「上記のいずれも含まれていなかった」を除く割合)であった。

シンクライアンなどパソコンに業務データを保管しない仕組みが普及しつつあるが、多くのパソコンについては、依然なんらかの保護すべき企業の情報が含まれていることが分かる。

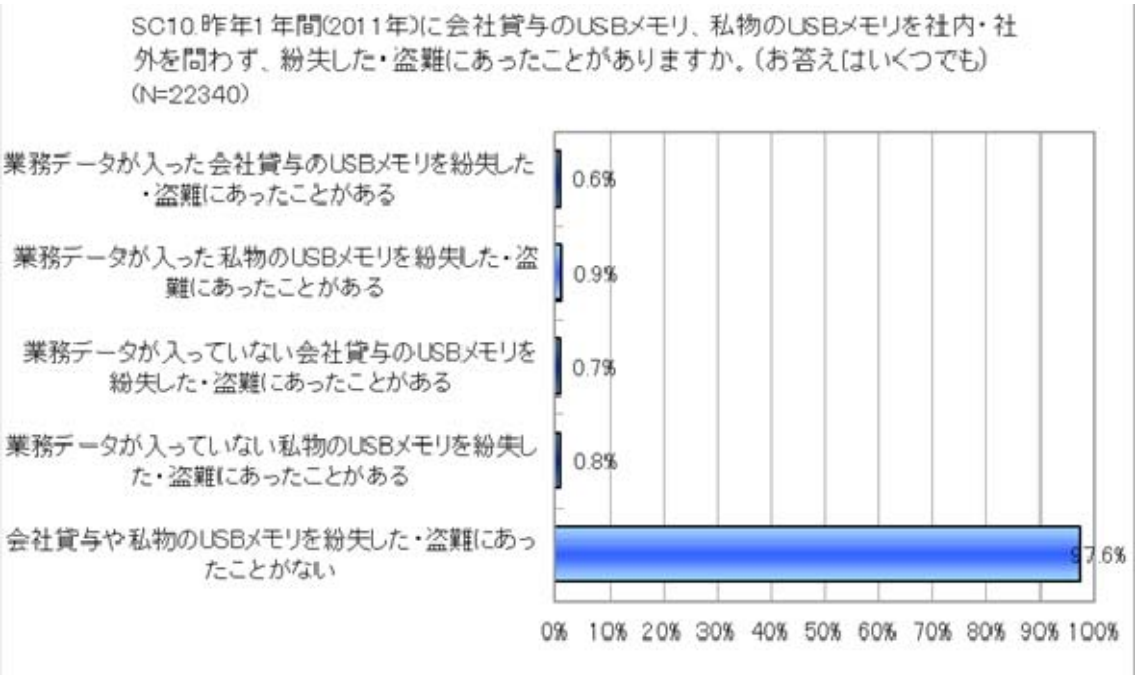


「顧客や取引先の業務が一時的に滞った」が 5.0%、「顧客、取引際の売上が減少した」が 4.0%となり、パソコンの紛失・盗難が、顧客や取引先に実害をもたらしている。

「上記のいずれも行ったり、起きたりしなかった」が 23%とあるが、これは報告さえしなかった割合である。紛失した際に報告する必要がないパソコンは「業務データが入っていない私物のパソコン」と考えられるが、それらのパソコンが紛失する割合は 10%にとどまる(SC9 の回答より)。そのため報告さえしないという回答の 23%は、問題のある割合である。

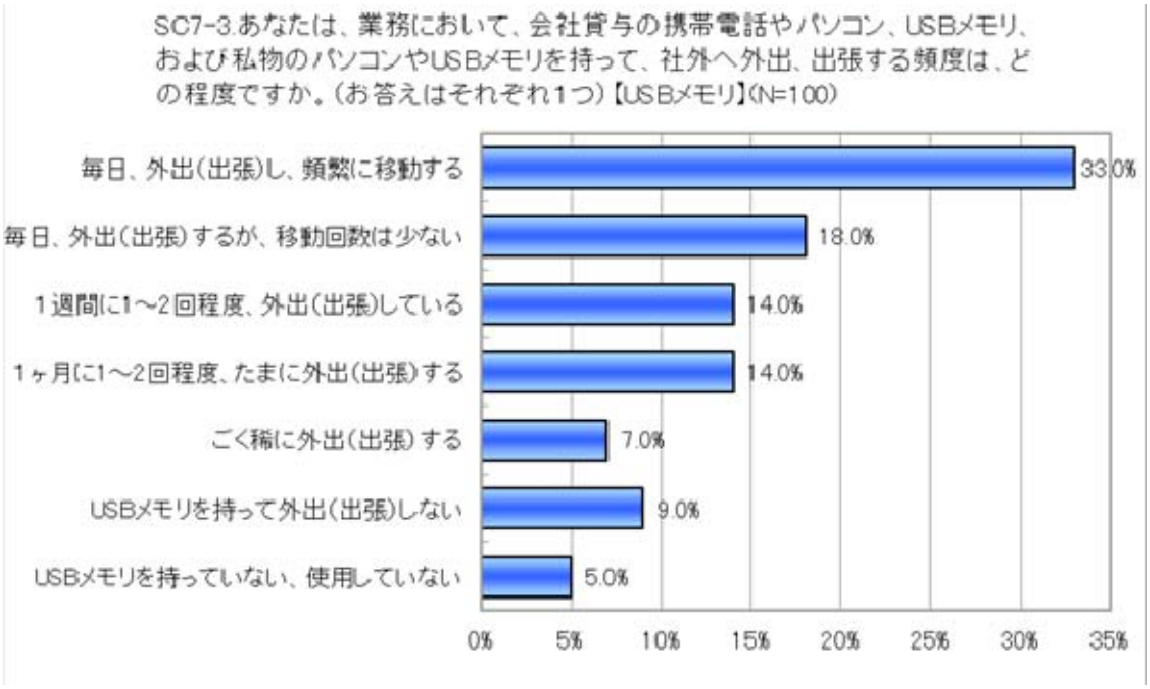
5.4. USB メモリ

5.4.1. 予備調査の分析結果



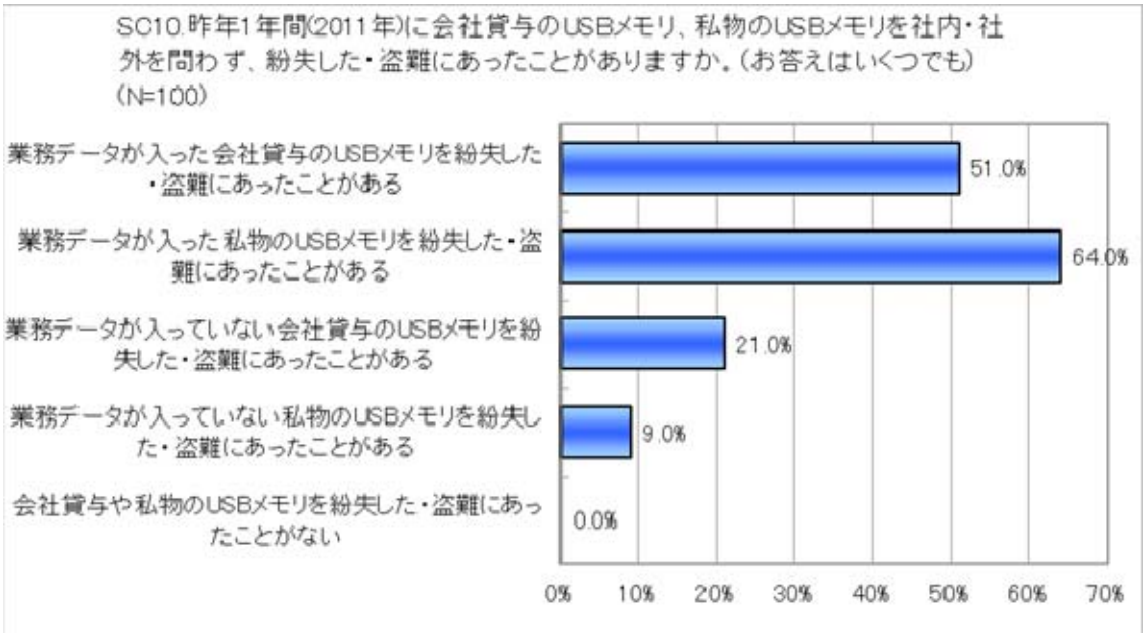
私物、会社貸与を問わず、USB をなくしたことがある人は全体約 2.4%である(全体から「会社貸与や私物の携帯電話を紛失した・盗難にあったことがない」を除く割合)。

以下は、各インシデントを経験した 100 人による回答である。



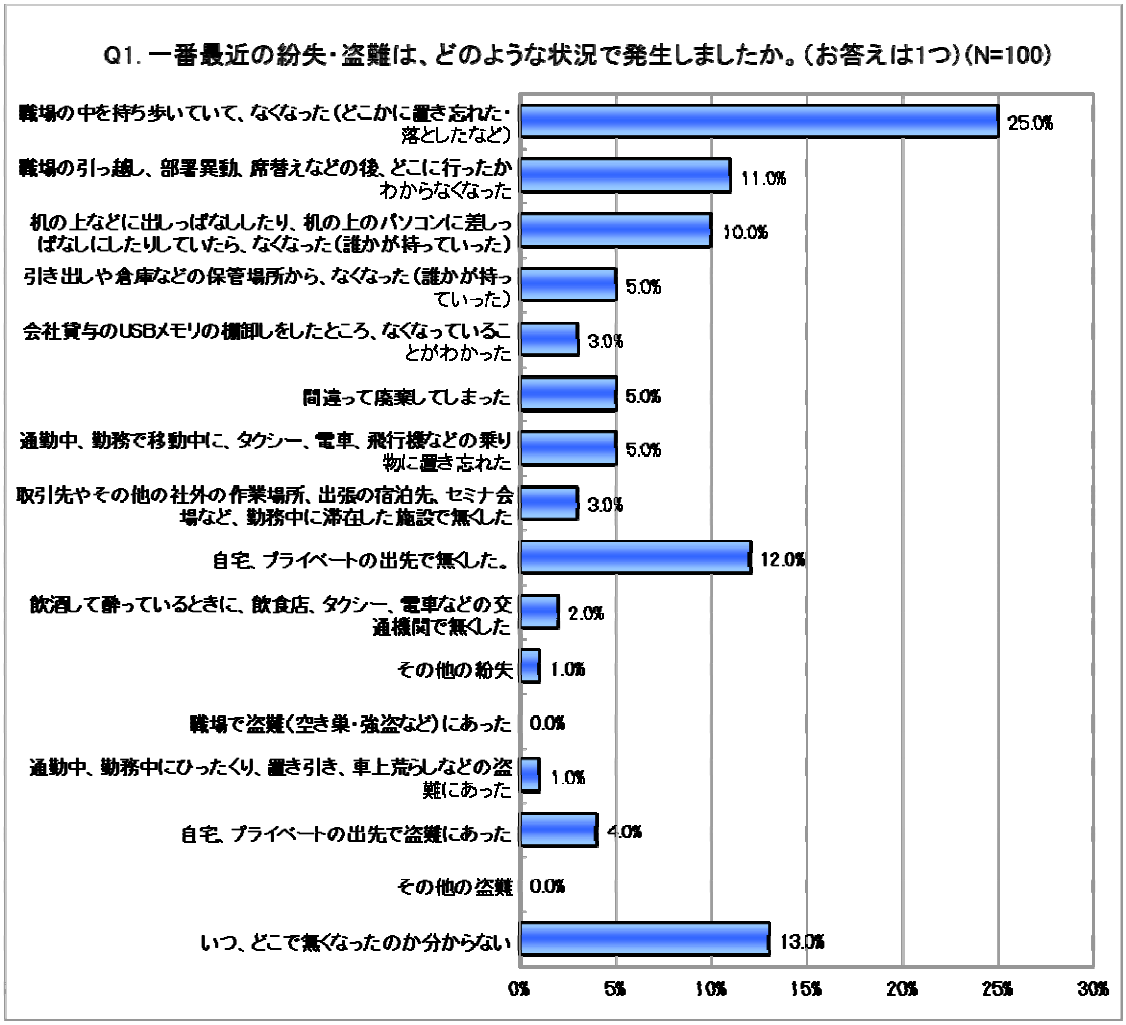
USB メモリを紛失した 100 人を対象とすると、外出頻度が多い人が USB メモリを紛失する割合が高くなる傾向を示す。

USB メモリの紛失・盗難に関しては業務における外出頻度が影響していることがわかる



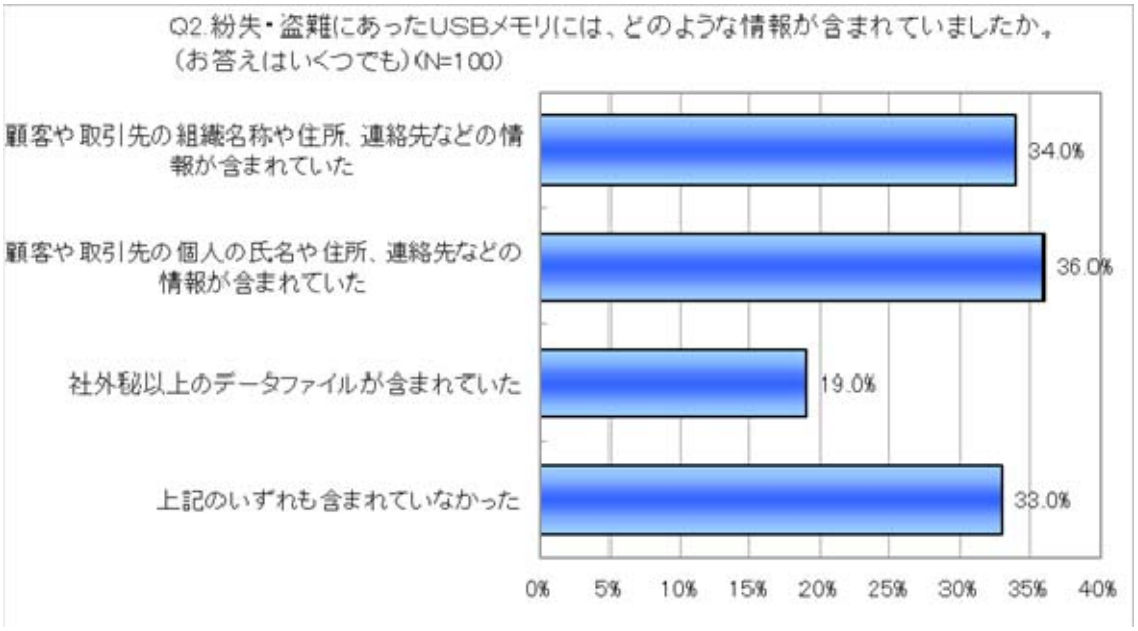
USB メモリを紛失した 100 人を対象とすると、「業務データが入った私物の USB メモリを紛失した・盗難にあったことがある」との回答が 64.0%に上る。「業務データが入っていない私物の USB メモリを紛失した・盗難にあったことがある」との回答が 9.0%であることを踏まえると、紛失した私物の USB メモリには業務データが入っている比率が高いといえる。

本調査の分析結果

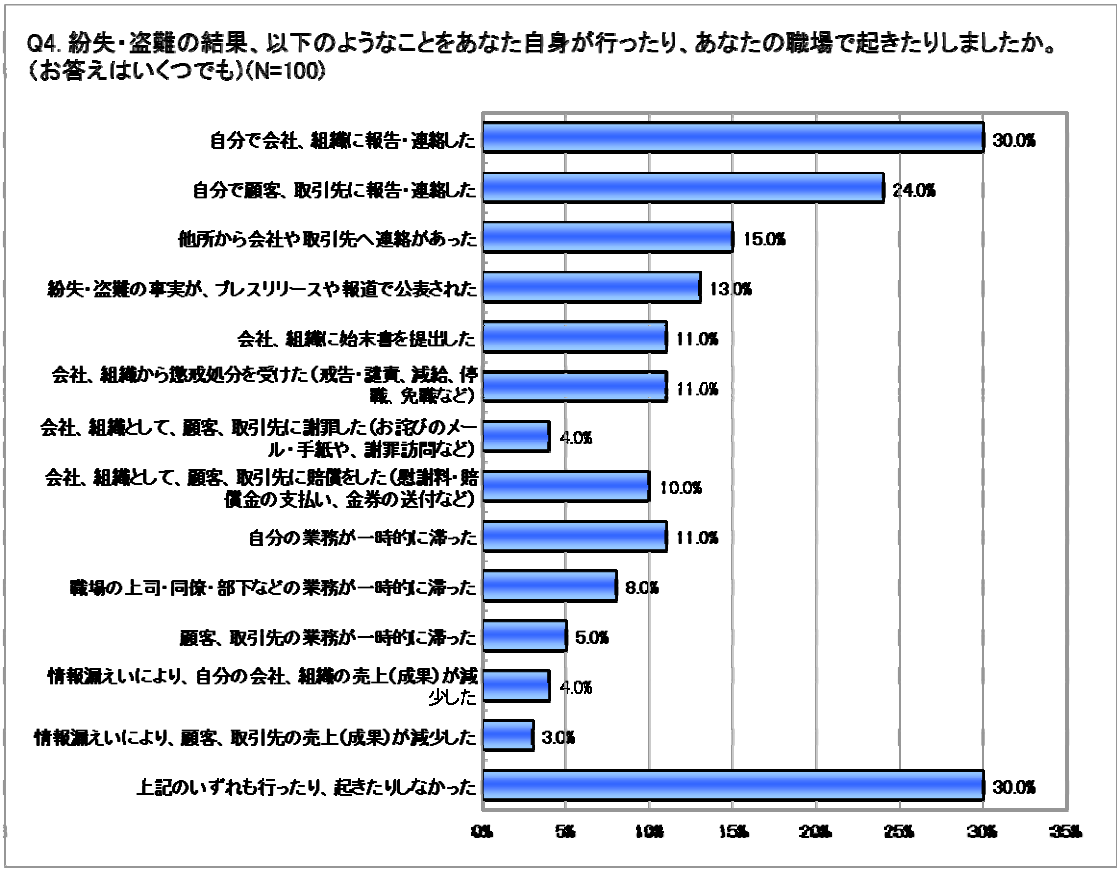


Q1FA1	一番最近の紛失・盗難は、どのような状況で発生しましたか。【その他の紛失(FA)】	
1	女性　62 才	税理士事務所から送ってきて、その後私の手元には届かず誰がなくしたかわからない。

実際に USB メモリの紛失・盗難にあった 100 人の回答によると、紛失・盗難の発生場所は社内が上位を占める。中でも「職場の中を持ち歩いていて、なくなった」が全体の 25%に至る。社内で USB メモリを持ち歩くことに注意が必要である。



紛失・盗難にあった USB メモリに、顧客データや社外秘以上のデータ等、業務に関係する情報が含まれていた場合は 67%(100%から「上記のいずれも含まれていなかった」と回答した人数を引いた割合)であった。紛失した多くの USB メモリは、保護すべき企業の情報が含まれていることがわかる。

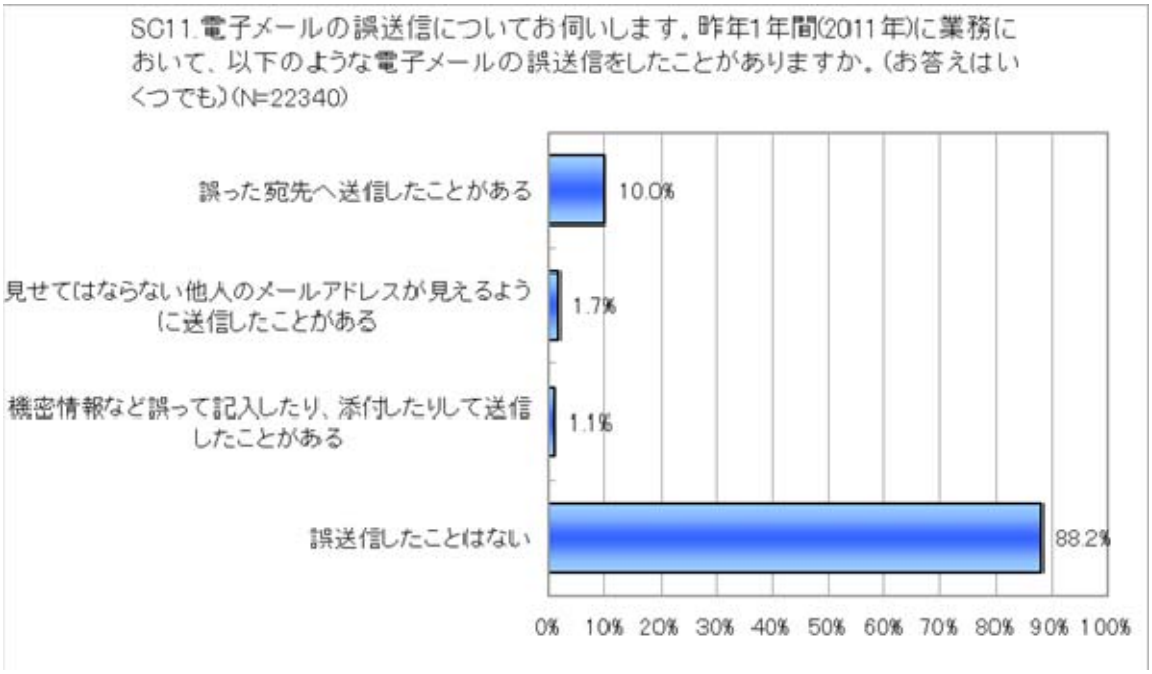


「顧客や取引先の業務が一時的に滞った」が 5.0%、「顧客、取引際の売上が減少した」が 3.0%となり、USB メモリの紛失・盗難が、顧客や取引先に実害をもたらしている。

「上記のいずれも行ったり、起きたりしなかった」が 30%とあるが、これは報告さえしなかった割合である。一番回答の多い「自分で、会社、組織に報告・連絡した」と同率である。紛失した際に報告する必要がない USB メモリは「業務データが入っていない私物の USB メモリ」と考えられるが、それらの USB メモリが紛失する割合は 9%にとどまる(SC10 の回答より)。そのため報告さえしないという回答の 30%は、問題のある割合である。これは、携帯電話、パソコンに比べ、大きな割合である。

5.5. 電子メール

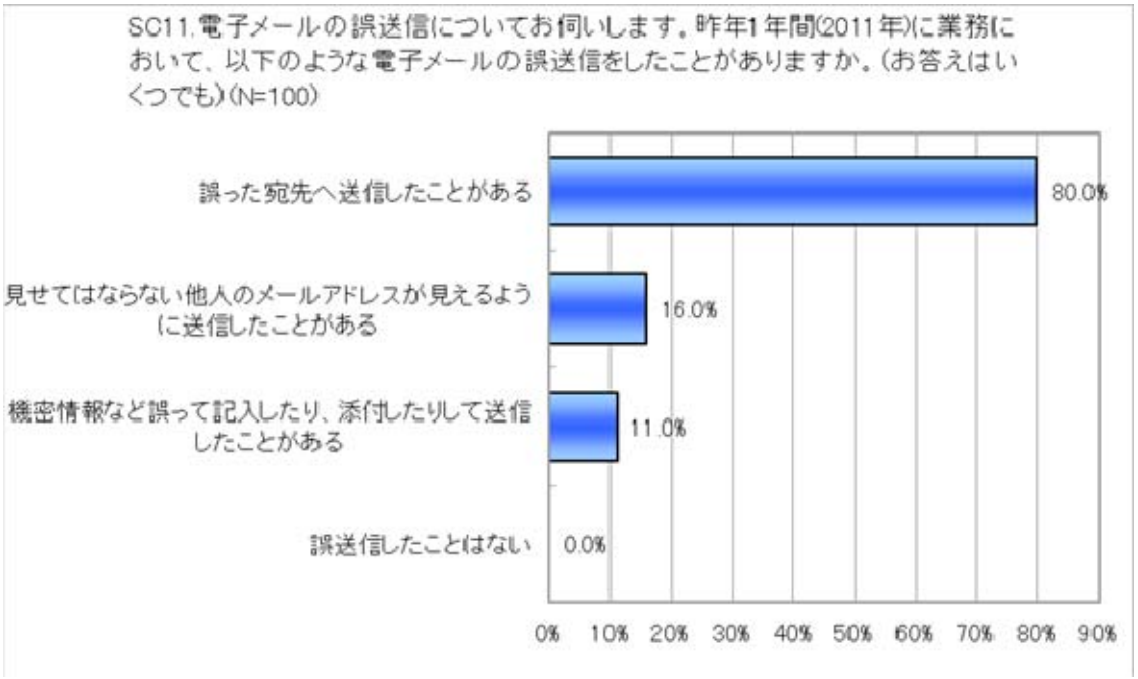
5.5.1. 予備調査の分析結果



22340 人を対象とした Web アンケートの結果から、2011 年の 1 年間に電子メールの誤送信を行ったことがある人が、1 割以上（11.8%）ある。つまり、電子メールの誤送信は 1 年間に 1 割以上発生しており、企業における情報インシデントの中でも最も発生確率の高いものであり注意を要するものであることが分かる。

また、個人情報の漏えいが、1.7%（379 件）、機密情報の漏えいが 1.1%（244 件）発生している。

以下は、各インシデントを経験した 100 人による回答である。



2011 年の 1 年間に電子メールの誤送信を行った人 100 人を対象としたアンケートでは、その 8 割が、宛先間違いである。また、メールアドレスの漏えいが、16 件、機密情報の漏えいが 11 件発生しており、直接的な情報漏えいが 1 割以上発生している。

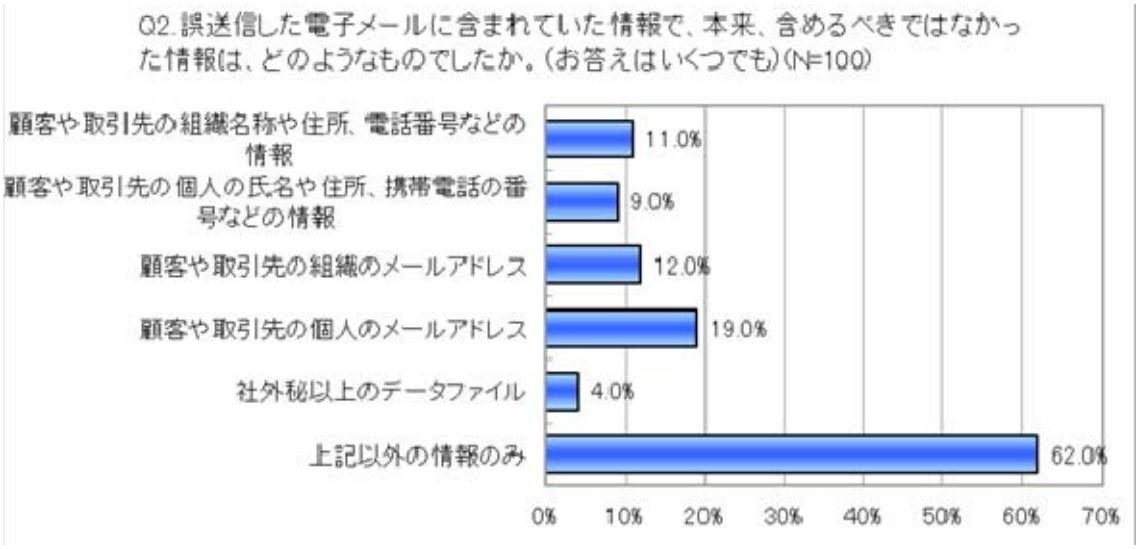
5.5.2. **本調査の分析結果**

Q1FA	一番最近の誤送信は、どのような状況で発生しましたか。【上記以外の状況で発生した(FA)】		
1	男性	49 才	流用したメールの宛先自体が間違っていた
2	男性	38 才	ファイルを添付し忘れて送信してしまった
3	男性	69 才	ファイルを添付し忘れた
4	女性	50 才	内容を書いてないのに返信してしまった。
5	女性	69 才	短銃に相手を間違えた
6	男性	27 才	返す相手を間違えた
7	男性	24 才	ファイルの添付忘れ

誤送信した時の状況は、「アドレス帳から間違ったメールアドレスを選択してしまった。」(40%)、「メールアドレスの手入力するときに、打ち間違えた」(27%)、「間違ったファイルを添付してしまった」(9%)の順に多い。

この順位は、2010 年の調査と同じ結果であり、傾向は変わっていない。

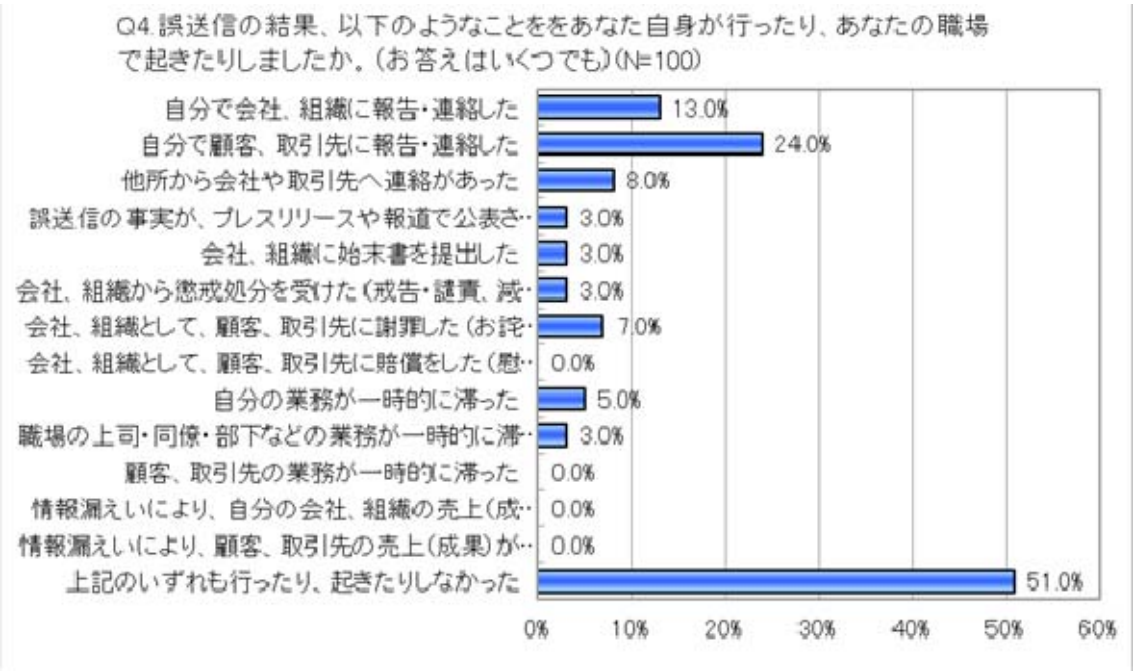
アンケート項目以外の誤送信の種類としては、セキュリティ上のインシデントとは見なす必要はないが、添付忘れ等が多く見られた。



この調査結果からは、漏えいして困る内容はあまり含まれていなかった（62%）という傾向が見える。これは、2010 年の 32%とは大きく異なっている。

その理由としては、2010 年の調査結果は、誤送信したタイミングは関係なく過去に発生したもの、もしくは、誤送信しそうになったものの両方を対象にしていたが、今回の調査が 2011 年の 1 年間に限定したものかつ、実際に誤送信してしまったものを対象にしていることに起因していると考えられる。

「いずれの対策もしていなかった」(48%)が、2010 年の調査結果（28%）にくらべ、増えている。何らかの対策を行ったひとは誤送信の可能性が低くなっているものと考えられる。



メールの誤送信により影響がなかった人が、51%と多い。また、外部への公表や、組織として処罰などの割合が低い。

- 誤送信の事実が、プレスリリースや報道で公表された
- 会社、組織に始末書を提出した
- 会社、組織から懲戒処分を受けた（戒告・譴責、減給、停職、免職など）
- 会社、組織として、顧客、取引先に謝罪した（お詫びのメール・手紙や、謝罪訪問など）

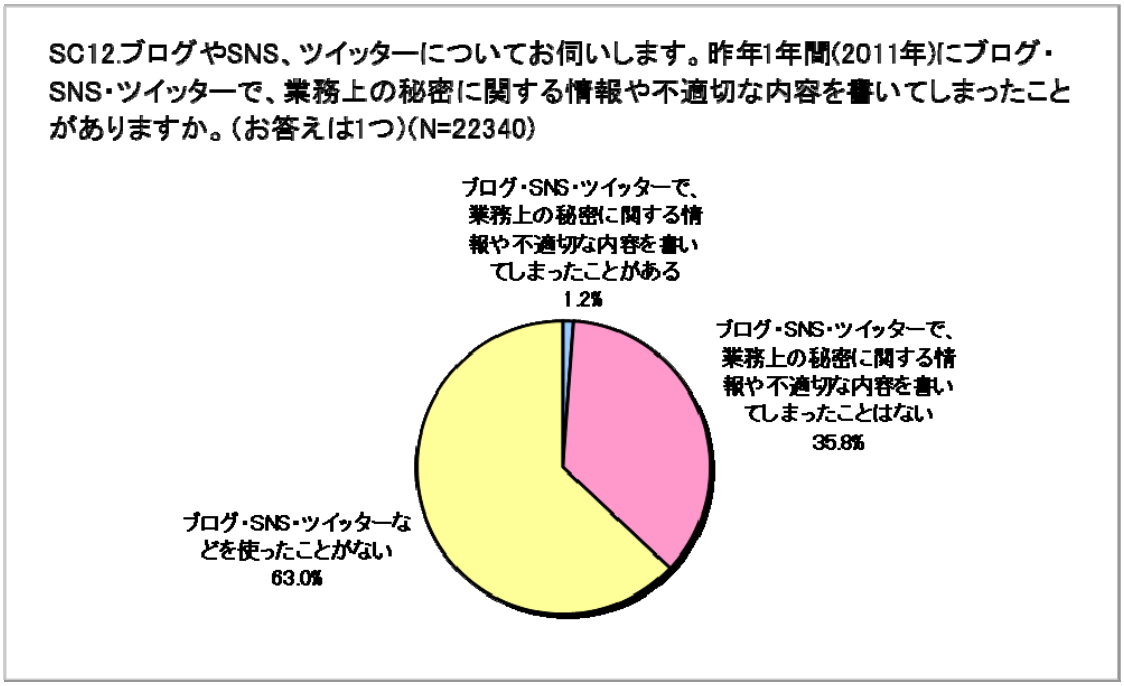
さらに、以下の項目が 0%であり、メール誤送信では金銭的な影響は発生していないことがわかる。

- 会社、組織として、顧客、取引先に賠償をした顧客、取引先の業務が一時的に滞った
- 情報漏えいにより、自分の会社、組織の売上（成果）が減少した
- 情報漏えいにより、顧客、取引先の売上（成果）が減少した

これらのことから、メール誤送信は、発生頻度は高いがあまり重大なインシデントとはなっていないことがわかる。

5.6. SNS

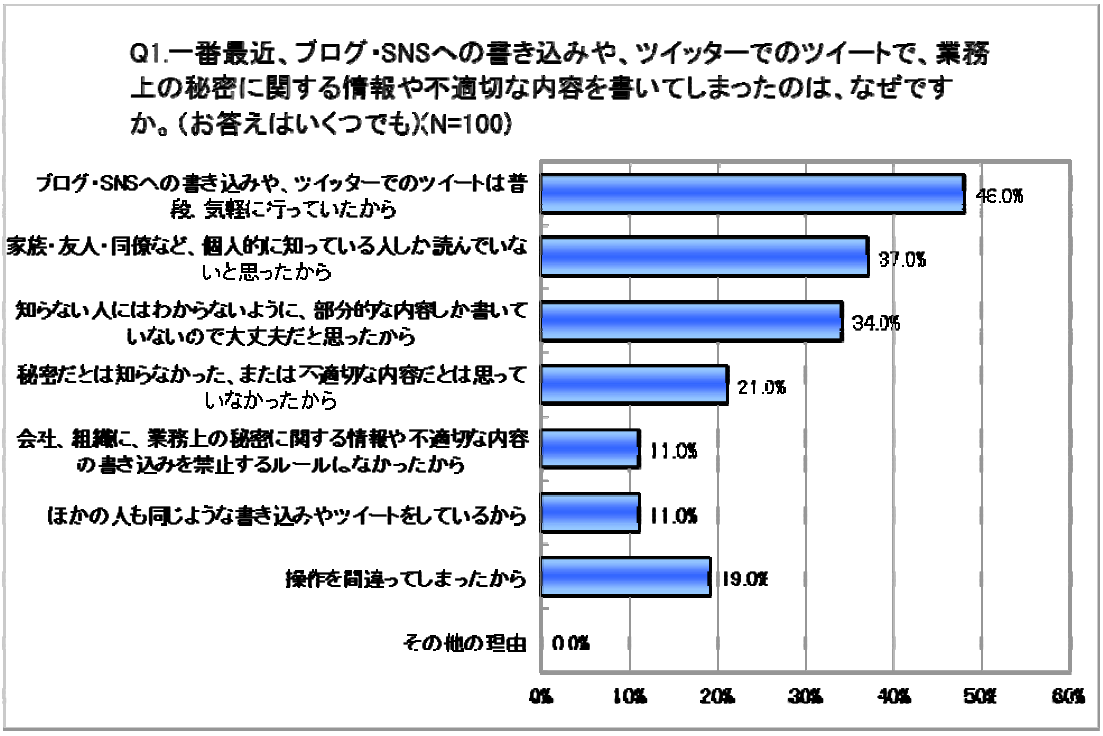
5.6.1. 予備調査の分析結果



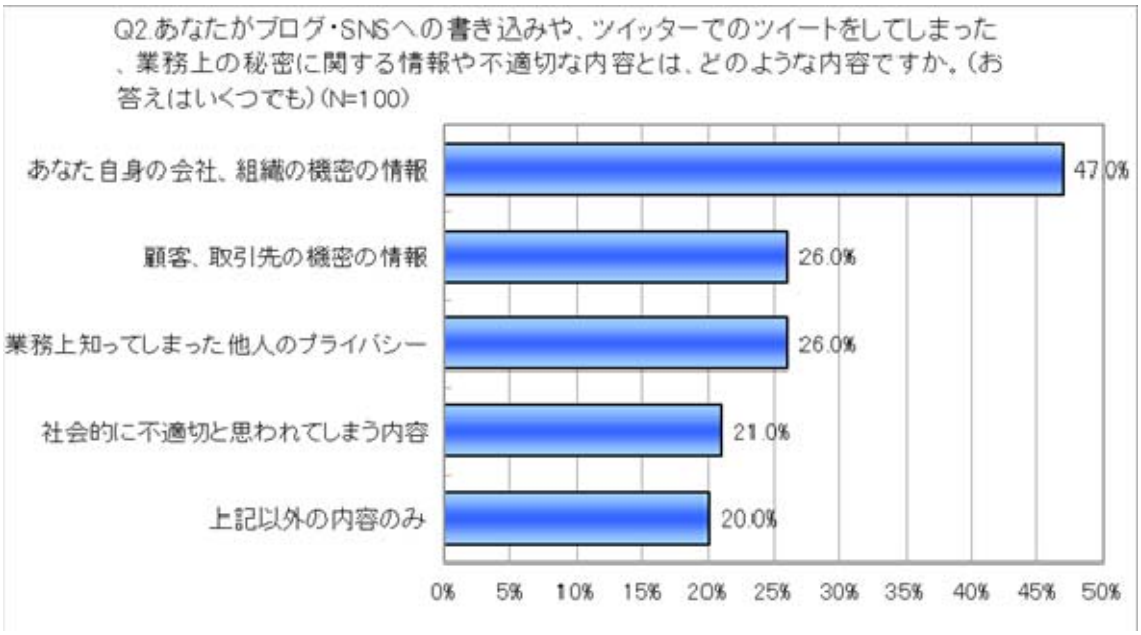
22340 人を対象とした Web アンケートの結果から、2011 年の１年間にブログ・SNS・ツイッターで、業務上の秘密に関する情報や不適切な内容を書いてしまったことがある人は、２７１人（1.2%）である。

ブログ・SNS・ツイッターを使ったことがない人が６３％であることから、使ったことがある人（３７％）の割合で考えると 3.3%となり、今後スマートフォンの普及に伴い、SNS やツイッターの利用者が増加することで、このリスクが問題になると考えられる。

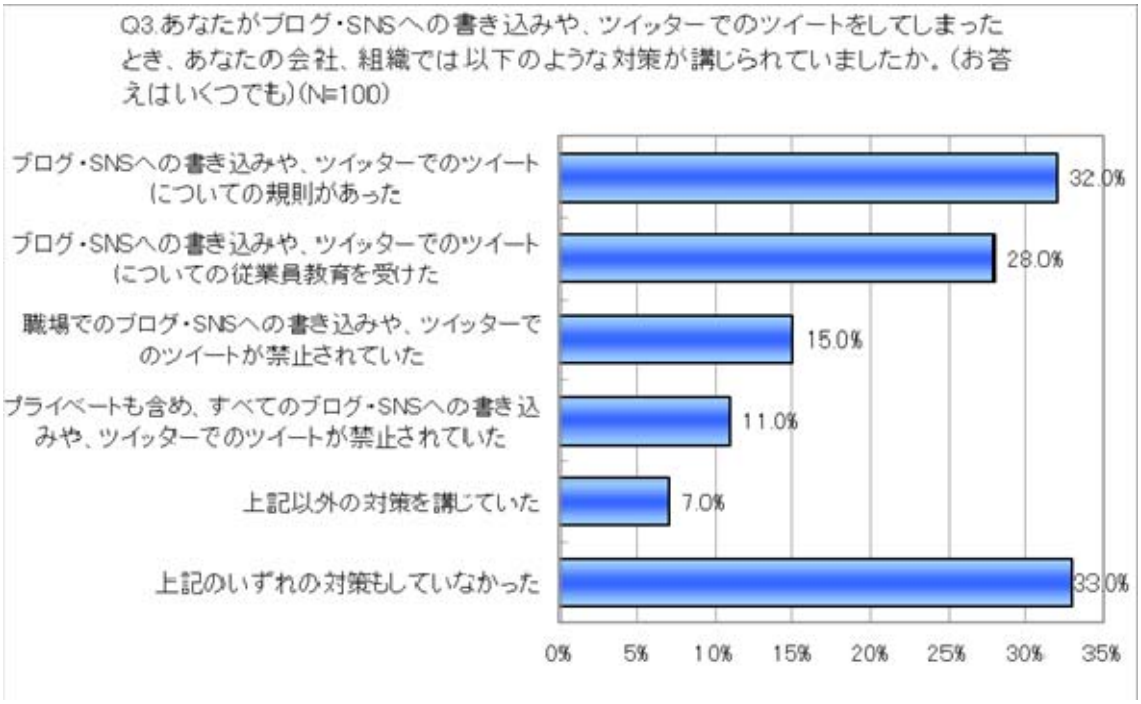
5.6.2. 本調査の分析結果



不適切な内容を書いてしまった理由としては、「普段、気軽に行っていたから」48%、「知り合いしか読んでいないと思った」37%、「わからないと思った」34%など、ブログ・SNS・ツイッターの影響範囲をよく理解していなかった、という回答が目立つ。これらは、社内での啓発や教育などの対策を行うことで、改善が見込めるものと考えられる。

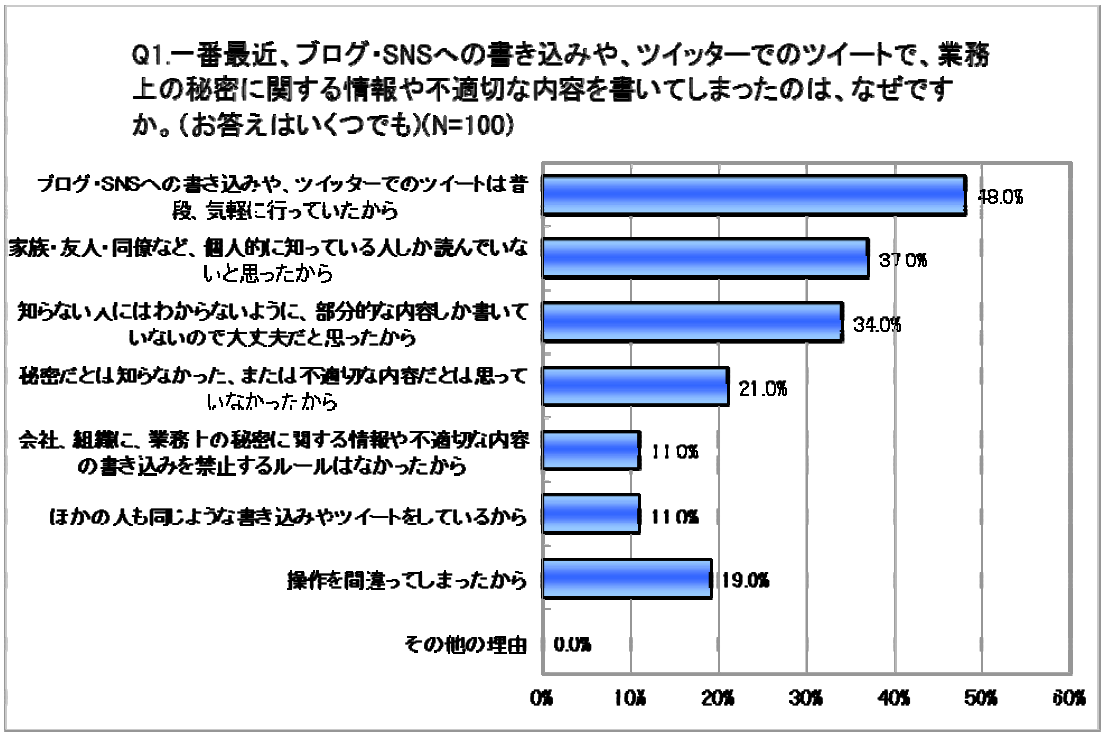


書き込みをしてしまった不適切な内容としては、自社の機密情報が 47%と半数を占め、顧客の機密情報や、他人のプライバシーが各々26%と続く。自社の機密情報であれば、自社内で閉じた問題として取り扱うことができるが、顧客や他人の情報の場合には、対外的な問題となり、取引停止や賠償など重大な問題への発展の可能性がある。



不適切な書き込みをしてしまった人が所属する組織において、なんの対策もしていなかった割合が 33%であり、残りの６７%の人は、何等かの対策が行われていても失敗していることがわかる。

今後、ブログ・SNS・ツイッターの利用が拡大していくことは明らかであり、組織としては、従来にもまして、規則の制定、教育に加え、監査の実施、誓約書の取得等の対策を充実させるべきと考える。



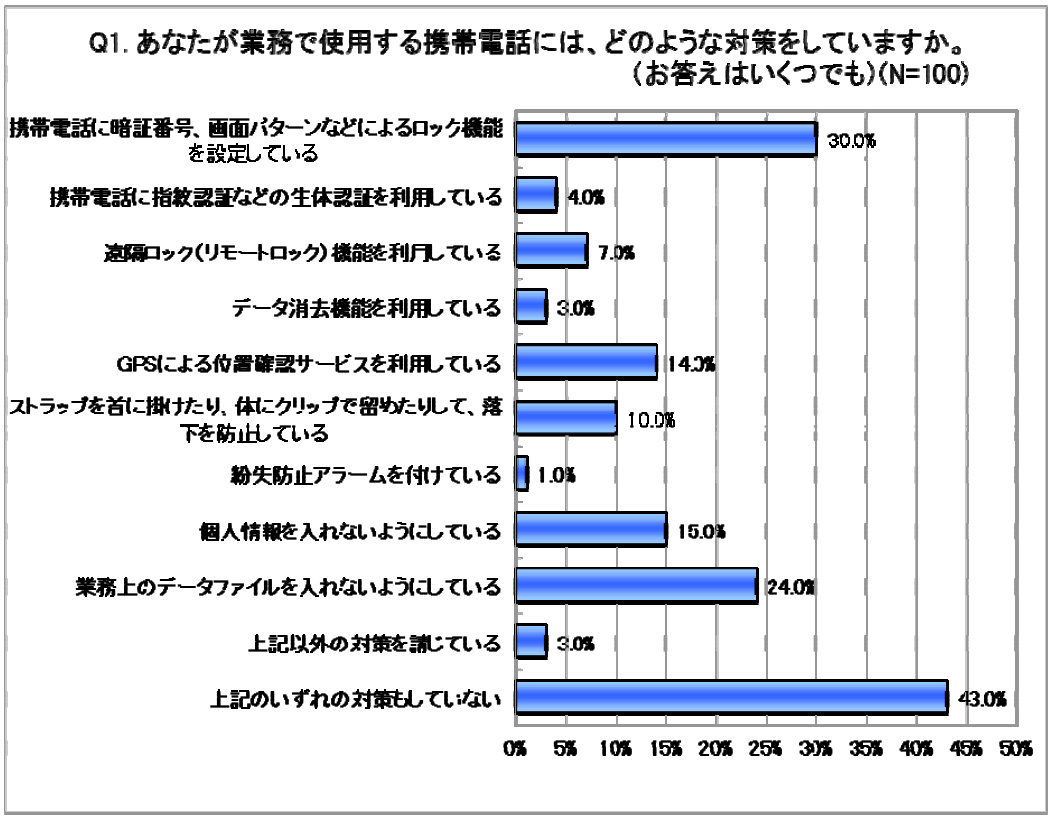
不適切な内容を書いたことで何等かの影響が出た人は 65%と半数以上である、
また、メール誤送信では 0%であった以下の項目において、金銭的な影響が発生している。

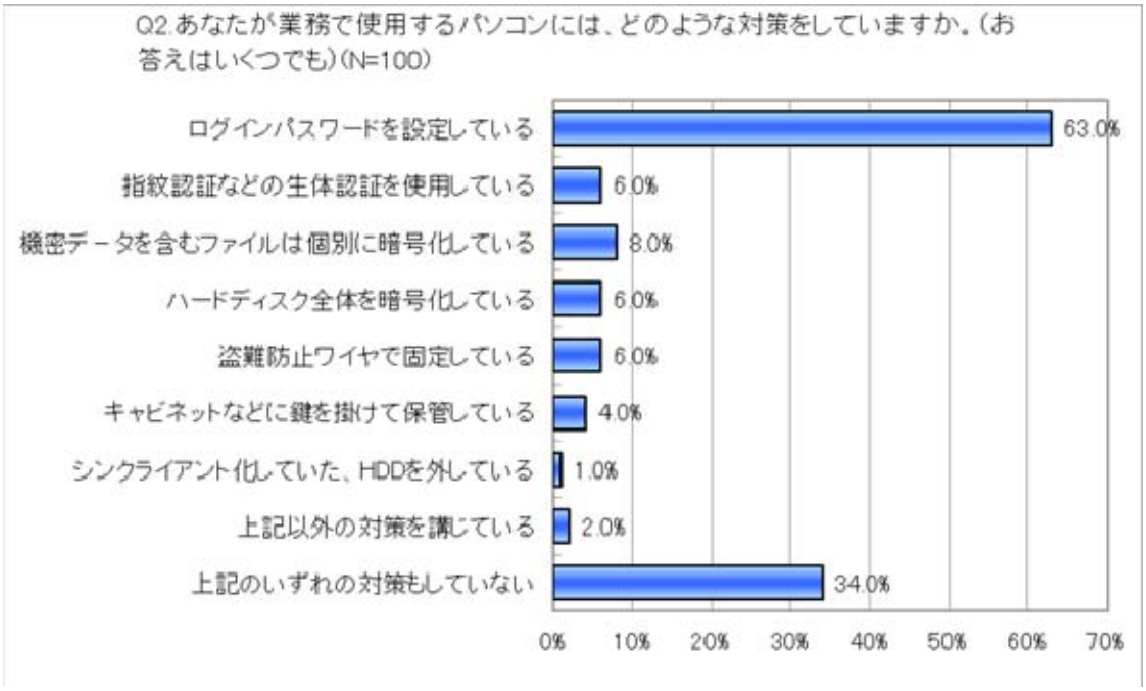
- 会社、組織として、顧客、取引先に賠償をした(6%)
- 顧客、取引先の業務が一時的に滞った(6%)
- 情報漏えいにより、自分の会社、組織の売上（成果）が減少した(6%)
- 情報漏えいにより、顧客、取引先の売上（成果）が減少した(5%)

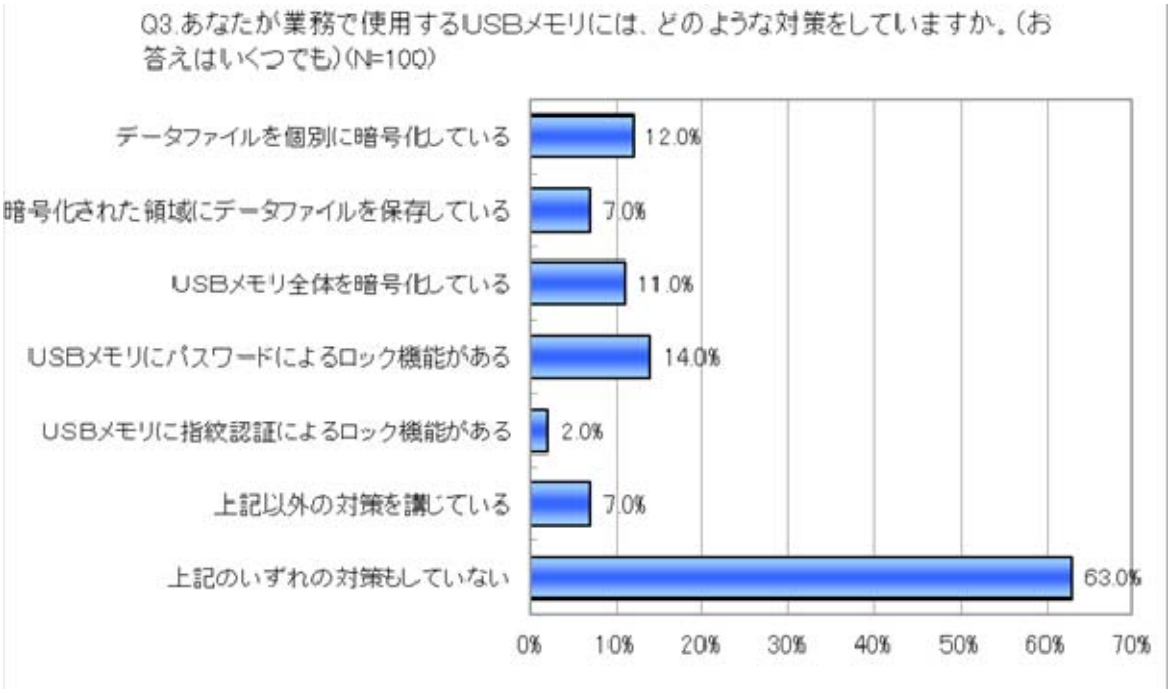
メール誤送信は送付先が限定されており、その影響範囲が特定できその対策も可能であるが、ブログ・SNS・ツイッターなどインターネットに公開されてしまった情報は、完全には消すことができず、影響範囲が特定できないため、インシデントが発生した後のリカバリが困難であり、損害賠償や機会損失などの金銭的な影響につながっていると思われる。

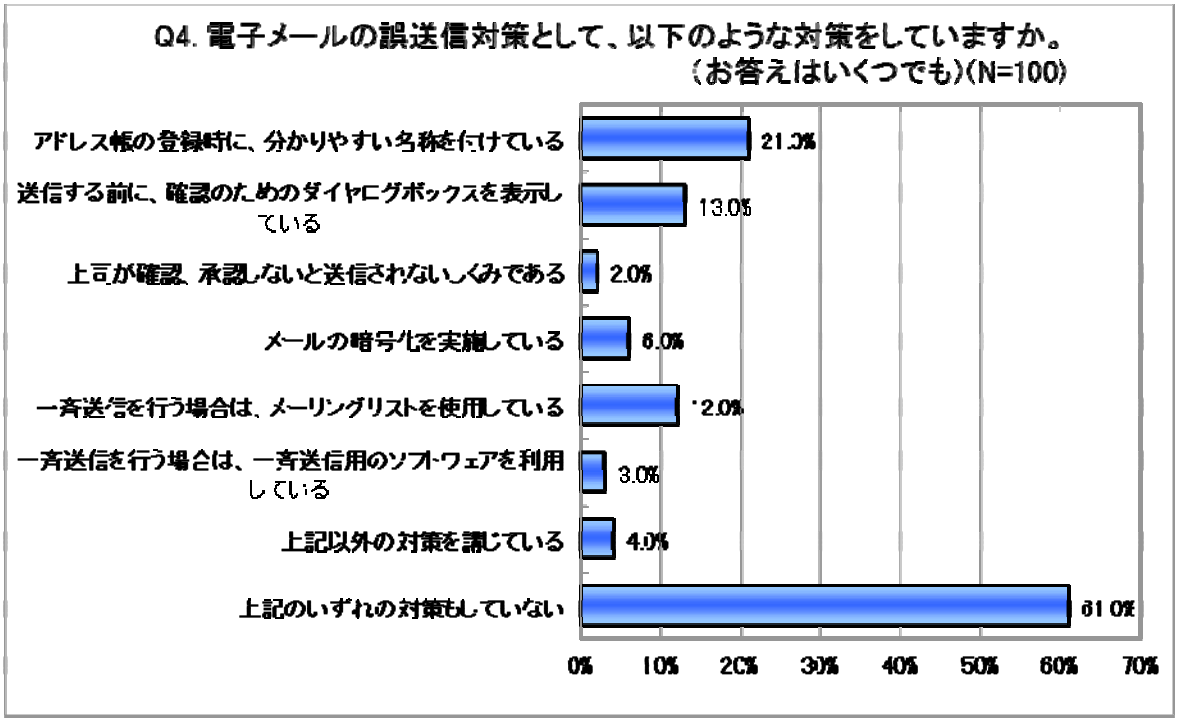
5.7. 無事故

5.7.1. 本調査の分析結果

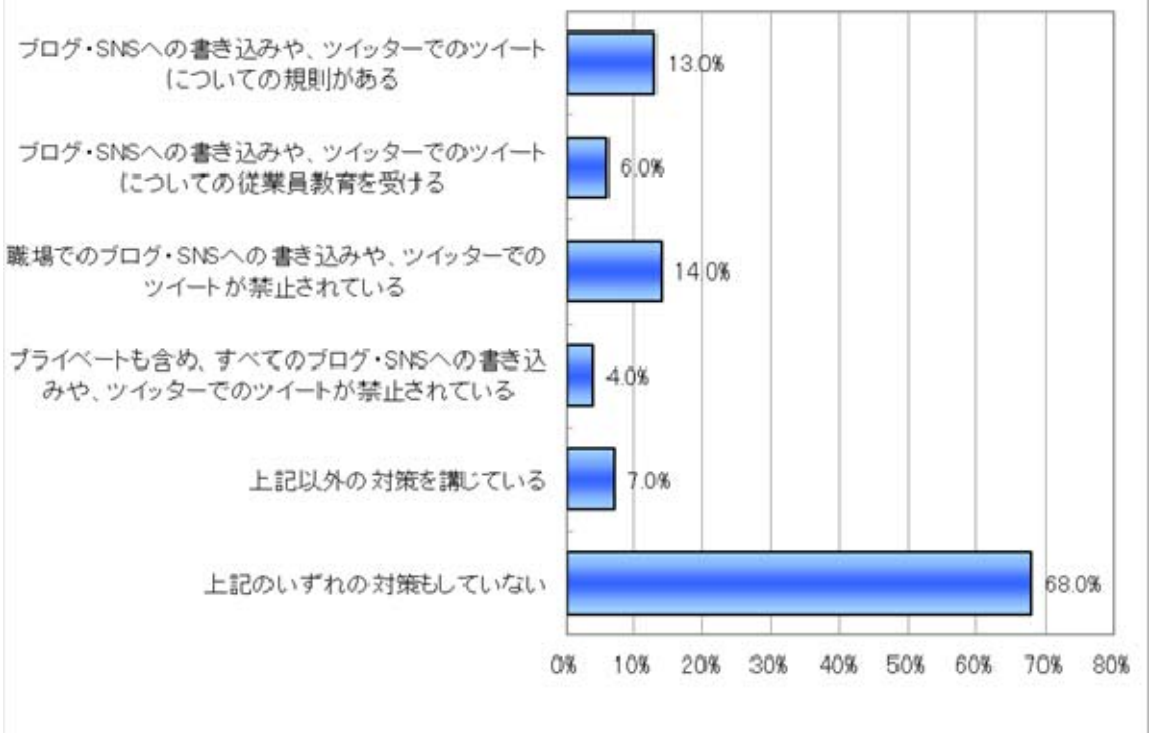





Q3.あなたが業務で使用するUSBメモリには、どのような対策をしていますか。(お答えはいくつでも)(N=100)
データファイルを個別に暗号化している
12.0%
暗号化された領域にデータファイルを保存している
7.0%
USBメモリ全体を暗号化している
11.0%
USBメモリにパスワードによるロック機能がある
14.0%
USBメモリに指紋認証によるロック機能がある
2.0%
上記以外の対策を講じている
7.0%
上記のいずれの対策もしていない
63.0%
0%
10%
20%
30%
40%
50%
60%
70%


Q4. 電子メールの誤送信対策として、以下のような対策をしていますか。
(お答えはいくつでも)(N=100)
アドレス帳の登録時に、分かりやすい名称を付けている
21.0%
送信する前に、確認のためのダイヤログボックスを表示している
13.0%
上司が確認、承認しないと送信されないしくみである
2.0%
メールの暗号化を実施している
6.0%
一斉送信を行う場合は、メーリングリストを使用している
12.0%
一斉送信を行う場合は、一斉送信用のソフトウェアを利用している
3.0%
上記以外の対策を講じている
4.0%
上記のいずれの対策もしていない
61.0%
0%
10%
20%
30%
40%
50%
60%
70%

Q5.ブログ・SNSへの書き込みや、ツイッターでのツイートで、業務上の秘密に関する情報や不適切な内容などを書いてしまわないように、あなたの会社、組織では以下のような対策が講じられていますか。(お答えはいくつでも)(N=100)



6. 付録：アンケート設問・回答データ

6.1. 予備調査の設問

SC1	SA	あなたのご職業・ご身分を教えてください。（お答えは 1 つ）
SC1	1	会社経営者・役員・団体役員
SC1	2	会社員・団体職員（正社員）
SC1	3	会社員・団体職員（契約・派遣）
SC1	4	地方公務員
SC1	5	国家公務員
SC1	6	自営業・個人事業主・フリーランス
SC1	7	自由業（開業医・弁護士事務所経営・プロスポーツ選手など）
SC1	8	パート・アルバイト・フリーター
SC1	9	学生
SC1	10	無職・休職中・求職中
SC1	11	その他
SC2	SA	従業員数を教えて下さい。（お答えは1つ）
SC2	1	10 人未満
SC2	2	10 人以上、30 人未満
SC2	3	30 人以上、100 人未満
SC2	4	100 人以上、300 人未満
SC2	5	300 人以上、1000 人未満
SC2	6	1000 人以上、3000 人未満
SC2	7	3000 人以上、10000 人未満
SC2	8	10000 人以上
SC3	MA	あなたは、情報セキュリティや IT に関する以下の言葉について、他人に大まかな説明ができるくらいに知っていますか。（お答えはいくつでも）
SC3	1	個人情報保護法
SC3	2	ぜい弱性
SC3	3	不正アクセス禁止法
SC3	4	ISMS（情報セキュリティ・マネジメントシステム）
SC3	5	リスク・アセスメント
SC3	6	コンピュータ・ウイルス
SC3	7	ファイアウォール
SC3	8	マルウェア
SC3	9	フィッシング詐欺
SC3	10	DoS 攻撃
SC3	11	OS（オペレーティング・システム）
SC3	12	ウェブ・ブラウザ
SC3	13	HTML
SC3	14	Linux
SC3	15	SaaS
SC3	16	上記で知っている言葉はない
SC4-1	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【寝坊や多忙などのせいで、出勤・会議などの時間に遅刻してしまう】
SC4-1	1	よくしてしまう

SC4-1	2	時々することがある
SC4-1	3	めったにしない
SC4-1	4	したことはない
SC4-2	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【仕事上の約束や予定スケジュールを勘違いして、人に迷惑をかけてしまう】
SC4-2	1	よくしてしまう
SC4-2	2	時々することがある
SC4-2	3	めったにしない
SC4-2	4	したことはない
SC4-3	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【机の上や引き出しの中が片付かず、書類などが見つからなくなる】
SC4-3	1	よくしてしまう
SC4-3	2	時々することがある
SC4-3	3	めったにしない
SC4-3	4	したことはない
SC4-4	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【自宅などに忘れ物をする】
SC4-4	1	よくしてしまう
SC4-4	2	時々することがある
SC4-4	3	めったにしない
SC4-4	4	したことはない
SC4-5	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に居眠りや、ぼうっとして時間を過ごしてしまう】
SC4-5	1	よくしてしまう
SC4-5	2	時々することがある
SC4-5	3	めったにしない
SC4-5	4	したことはない
SC4-6	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に関係のないウェブサイトや掲示板・ブログ、SNS、ツイッターなどを見て時間を過ごしてしまう】
SC4-6	1	よくしてしまう
SC4-6	2	時々することがある
SC4-6	3	めったにしない
SC4-6	4	したことはない
SC4-7	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に関係のない掲示板・ブログ、SNS、ツイッターなどに書き込みをして時間を過ごしてしまう】
SC4-7	1	よくしてしまう
SC4-7	2	時々することがある
SC4-7	3	めったにしない
SC4-7	4	したことはない
SC4-8	SA	あなた自身は普段、仕事中に以下のような「うっかりした失敗」をしてしまうことは、どれくらいありますか。【業務中に関係のない雑談、メールやチャットのやりとりなどをして時間を過ごしてしまう】
SC4-8	1	よくしてしまう
SC4-8	2	時々することがある
SC4-8	3	めったにしない

SC4-8	4	したことはない
SC5-1	SA	人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ 1 つ)【きちょうめんな/大雑把な】
SC5-1	1	A に近い
SC5-1	2	どちらかというと A に近い
SC5-1	3	どちらかというと B に近い
SC5-1	4	B に近い
SC5-2	SA	人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ 1 つ)【悲観的な/楽天的な】
SC5-2	1	A に近い
SC5-2	2	どちらかというと A に近い
SC5-2	3	どちらかというと B に近い
SC5-2	4	B に近い
SC5-3	SA	人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ 1 つ)【生真面目な/いい加減な】
SC5-3	1	A に近い
SC5-3	2	どちらかというと A に近い
SC5-3	3	どちらかというと B に近い
SC5-3	4	B に近い
SC5-4	SA	人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ 1 つ)【慎重な/おっちょこちょいな】
SC5-4	SA	人の性格をあらわす以下の言葉の中から、あなた自身の性格にもっとも近いと思う選択肢を選んでください。(お答えはそれぞれ 1 つ)【慎重な/おっちょこちょいな】
SC5-4	1	A に近い
SC5-4	2	どちらかというと A に近い
SC5-4	3	どちらかというと B に近い
SC5-4	4	B に近い
SC6	MA	あなたが働いている職場で、以下の事項は実施されていますか。(お答えはいくつでも)
SC6	1	情報セキュリティについての規程類が定められている
SC6	2	職場のパソコンについて、外部への持ち出しを禁じるルール、または持ち出す際の手続きのルールが定められている
SC6	3	私物や業者のパソコンについて、職場への持ち込みを禁じるルール、または持ち込む際の手続きのルールが定められている
SC6	4	情報セキュリティ事故(携帯電話・パソコン・USB メモリの紛失や情報漏えいなど)が起きた場合の、報告先や報告手続きのルールが定められている
SC6	5	従業員に対して情報セキュリティについての教育・研修が行われている
SC6	6	従業員に対して守秘義務についての誓約書などを提出させている
SC6	7	いずれも実施されていない
SC7-1	SA	あなたは、業務において、会社貸与の携帯電話やパソコン、USB メモリ、および私物のパソコンや USB メモリを持って、社外へ外出、出張する頻度は、どの程度ですか。(お答えはそれぞれ1つ)【会社貸与の携帯電話】
SC7-1	1	毎日、外出(出張)し、頻繁に移動する
SC7-1	2	毎日、外出(出張)するが、移動回数は少ない
SC7-1	3	1週間に 1～2 回程度、外出(出張)している
SC7-1	4	1ヶ月に 1～2 回程度、たまに外出(出張)する
SC7-1	5	ごく稀に外出(出張)する
SC7-1	6	会社貸与の携帯電話を持って外出(出張)しない
SC7-1	7	会社貸与の携帯電話を持っていない、使用していない

SC7-2	SA	あなたは、業務において、会社貸与の携帯電話やパソコン、USB メモリ、および私物のパソコンや USB メモリを持って、社外へ外出、出張する頻度は、どの程度ですか。(お答えはそれぞれ1つ)【パソコン】
SC7-2	1	毎日、外出(出張)し、頻繁に移動する
SC7-2	2	毎日、外出(出張)するが、移動回数は少ない
SC7-2	3	1週間に 1～2 回程度、外出(出張)している
SC7-2	4	1ヶ月に 1～2 回程度、たまに外出(出張)する
SC7-2	5	ごく稀に外出(出張)する
SC7-2	6	USB メモリを持って外出(出張)しない
SC7-2	7	USB メモリを持っていない、使用していない
SC7-3	SA	あなたは、業務において、会社貸与の携帯電話やパソコン、USB メモリ、および私物のパソコンや USB メモリを持って、社外へ外出、出張する頻度は、どの程度ですか。(お答えはそれぞれ1つ)【USB メモリ】
SC7-3	1	毎日、外出(出張)し、頻繁に移動する
SC7-3	2	毎日、外出(出張)するが、移動回数は少ない
SC7-3	3	1週間に 1～2 回程度、外出(出張)している
SC7-3	4	1ヶ月に 1～2 回程度、たまに外出(出張)する
SC7-3	5	ごく稀に外出(出張)する
SC7-3	6	USB メモリを持って外出(出張)しない
SC7-3	7	USB メモリを持っていない、使用していない
SC8	MA	昨年 1 年間(2011 年)に会社貸与の携帯電話、私物の携帯電話を社内・社外を問わず、紛失した・盗難にあったことがありますか。(お答えはいくつでも)
SC8	1	業務データが入った会社貸与の携帯電話を紛失した・盗難にあったことがある
SC8	2	業務データが入った私物の携帯電話を紛失した・盗難にあったことがある
SC8	3	業務データが入った会社貸与の携帯電話を紛失しそうになったことがある
SC8	4	業務データが入った私物の携帯電話を紛失しそうになったことがある
SC8	5	業務データが入っていない会社貸与の携帯電話を紛失した・盗難にあったことがある
SC8	6	業務データが入っていない私物の携帯電話を紛失した・盗難にあったことがある
SC8	7	会社貸与や私物の携帯電話を紛失した・盗難にあったことがない
SC9	MA	昨年 1 年間(2011 年)に会社貸与のパソコン、私物のパソコンを社内・社外を問わず、紛失した・盗難にあったことがありますか。(お答えはいくつでも)
SC9	1	業務データが入った会社貸与のパソコンを紛失した・盗難にあったことがある
SC9	2	業務データが入った私物のパソコンを紛失した・盗難にあったことがある
SC9	3	業務データが入った会社貸与のパソコンを紛失しそうになったことがある
SC9	4	業務データが入った私物のパソコンを紛失しそうになったことがある
SC9	5	業務データが入っていない会社貸与のパソコンを紛失した・盗難にあったことがある
SC9	6	業務データが入っていない私物のパソコンを紛失した・盗難にあったことがある
SC9	7	会社貸与や私物のパソコンを紛失した・盗難にあったことがない
SC10	MA	昨年 1 年間(2011 年)に会社貸与の USB メモリ、私物の USB メモリを社内・社外を問わず、紛失した・盗難にあったことがありますか。(お答えはいくつでも)
SC10	1	業務データが入った会社貸与の USB メモリを紛失した・盗難にあったことがある
SC10	2	業務データが入った私物の USB メモリを紛失した・盗難にあったことがある
SC10	3	業務データが入っていない会社貸与の USB メモリを紛失した・盗難にあったことがある
SC10	4	業務データが入っていない私物の USB メモリを紛失した・盗難にあったことがある
SC10	5	会社貸与や私物の USB メモリを紛失した・盗難にあったことがない
SC11	MA	電子メールの誤送信についてお伺いします。昨年 1 年間(2011 年)に業務において、

		以下のような電子メールの誤送信をしたことがありますか。（お答えはいくつでも）
SC11	1	誤った宛先へ送信したことがある
SC11	2	見せてはならない他人のメールアドレスが見えるように送信したことがある
SC11	3	機密情報など誤って記入したり、添付したりして送信したことがある
SC11	4	誤送信したことはない
SC12	SA	ブログや SNS、ツイッターについてお伺いします。昨年 1 年間(2011 年)にブログ・SNS・ツイッターで、業務上の秘密に関する情報や不適切な内容を書いてしまったことがありますか。（お答えは 1 つ）
SC12	1	ブログ・SNS・ツイッターで、業務上の秘密に関する情報や不適切な内容を書いてしまったことがある
SC12	2	ブログ・SNS・ツイッターで、業務上の秘密に関する情報や不適切な内容を書いてしまったことはない
SC12	3	ブログ・SNS・ツイッターなどを使ったことがない

6.2. 本調査の設問と回答（携帯電話）

Q1　昨年 1 年間(2011 年)に、実際に紛失・盗難が発生しましたか。（お答えは 1 つ）

		N	%
全体		100	100.0%
1	実際に紛失した・盗難にあった	58	58.0%
2	紛失しそうになったが、あとで見つかった	42	42.0%

Q2　一番最近の紛失・盗難は、どのような状況で発生しましたか。（お答えは 1 つ）

		N	%
全体		100	100.0%
1	職場の中を持ち歩いていて、なくなった（どこかに置き忘れた・落としたなど）	22	22.0%
2	机の上などに出しっぱなしにしていたら、なくなった（誰かが持っていった）	9	9.0%
3	引き出しや倉庫などの保管場所から、なくなった（誰かが持っていった）	8	8.0%
4	会社貸与の携帯電話の棚卸しをしたところ、なくなっていることがわかった	3	3.0%
5	間違って廃棄してしまった	2	2.0%
6	通勤中、勤務で移動中に、タクシー、電車、飛行機などの乗り物に置き忘れた	14	14.0%
7	取引先やその他の社外の作業場所、出張の宿泊先、セミナ会場など、勤務中に滞在した施設で無くした	6	6.0%
8	自宅、プライベートの出先で無くした。	15	15.0%
9	飲酒して酔っているときに、飲食店、タクシー、電車などの交通機関で無くした	8	8.0%
10	その他の紛失	2	2.0%
11	職場で盗難（空き巣・強盗など）にあった	1	1.0%
12	通勤中、勤務中にひったくり、置き引き、車上荒らしなどの盗難にあった	1	1.0%
13	自宅、プライベートの出先で盗難にあった	4	4.0%
14	その他の盗難	0	0.0%
15	いつ、どこで無くなったのか分からない	5	5.0%

Q3　紛失・盗難にあった携帯電話には、どのような情報が含まれていましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	携帯メールやアドレス帳に、顧客や取引先の組織名称や住所、連絡先などの情報が含まれていた	55	55.0%
2	携帯メールやアドレス帳に、顧客や取引先の個人の氏名や住所、連絡先などの情報が含まれていた	48	48.0%
3	社外秘以上のデータファイルが含まれていた	10	10.0%
4	上記のいずれも含まれていなかった	19	19.0%

Q4　紛失・盗難にあったとき、その携帯電話には、どのような対策をしていましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	携帯電話に暗証番号、画面パターンなどによるロック機能を設定していた	33	33.0%
2	携帯電話に指紋認証などの生体認証を利用していた	20	20.0%
3	遠隔ロック（リモートロック）機能を利用していた	28	28.0%
4	データ消去機能を利用していた	17	17.0%
5	GPS による位置確認サービスを利用していた	11	11.0%
6	ストラップを首に掛けたり、体にクリップで留めたりして、落下を防止していた	11	11.0%
7	紛失防止アラームを付けていた	8	8.0%
8	個人情報を入れないようにしていた	13	13.0%
9	業務上のデータファイルを入れないようにしていた	8	8.0%
10	上記以外の対策を講じていた	1	1.0%
11	上記のいずれの対策もしていなかった	23	23.0%

Q5　紛失・盗難の結果、以下のようなことををあなた自身が行ったり、あなたの職場で起きたりしましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	自分で会社、組織に報告・連絡した	41	41.0%
2	自分で顧客、取引先に報告・連絡した	24	24.0%
3	他所から会社や取引先へ連絡があった	13	13.0%
4	紛失・盗難の事実が、プレスリリースや報道で公表された	10	10.0%

5	会社、組織に始末書を提出した	17	17.0%
6	会社、組織から懲戒処分を受けた（戒告・譴責、減給、停職、免職など）	10	10.0%
7	会社、組織として、顧客、取引先に謝罪した（お詫びのメール・手紙や、謝罪訪問など）	8	8.0%
8	会社、組織として、顧客、取引先に賠償をした（慰謝料・賠償金の支払い、金券の送付など）	5	5.0%
9	自分の業務が一時的に滞った	15	15.0%
10	職場の上司・同僚・部下などの業務が一時的に滞った	2	2.0%
11	顧客、取引先の業務が一時的に滞った	5	5.0%
12	情報漏えいにより、自分の会社、組織の売上（成果）が減少した	3	3.0%
13	情報漏えいにより、顧客、取引先の売上（成果）が減少した	4	4.0%
14	上記のいずれも行ったり、起きたりしなかった	25	25.0%

6.3. 本調査の設問と回答（パソコン）

Q1　昨年 1 年間(2011 年)に、実際に紛失・盗難が発生しましたか。（お答えは 1 つ）

		N	%
全体		100	100.0%
1	実際に紛失した・盗難にあった	57	57.0%
2	紛失しそうになったが、あとで見つかった	43	43.0%

Q2　一番最近の紛失・盗難は、どのような状況で発生しましたか。（お答えは 1 つ）

		N	%
全体		100	100.0%
1	職場の中を持ち歩いていて、なくなった（どこかに置き忘れたなど）	18	18.0%
2	職場の引っ越し、部署異動、席替えなどの後、どこに行ったかわからなくなった	17	17.0%
3	机の上などに出しっぱなしにしていたら、なくなった（誰かが持っていった）	8	8.0%
4	引き出しや倉庫などの保管場所から、なくなった（誰かが持っていった）	6	6.0%
5	会社貸与のパソコンの棚卸しをしたところ、なくなっていることがわかった	8	8.0%
6	間違って廃棄してしまった	6	6.0%
7	通勤中、勤務で移動中に、タクシー、電車、飛行機などの乗り物に置き忘れた	4	4.0%
8	取引先やその他の社外の作業場所、出張の宿泊先、セミナ会場など、勤務中に滞在した施設で無くした	1	1.0%
9	自宅、プライベートの出先で無くした。	6	6.0%
10	飲酒して酔っているときに、飲食店、タクシー、電車などの交通機関で無くした	3	3.0%
11	その他の紛失	1	1.0%
12	職場で盗難（空き巣・強盗など）にあった	4	4.0%
13	通勤中、勤務中にひったくり、置き引き、車上荒らしなどの盗難にあった	2	2.0%
14	自宅、プライベートの出先で盗難にあった	2	2.0%
15	その他の盗難	0	0.0%
16	いつ、どこで無くなったのか分からない	14	14.0%

Q3　紛失・盗難にあったパソコンには、どのような情報が含まれていましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	顧客や取引先の組織名称や住所、連絡先などの情報が含まれていた	33	33.0%
2	顧客や取引先の個人の氏名や住所、連絡先などの情報が含まれていた	48	48.0%
3	社外秘以上のデータファイルが含まれていた	25	25.0%
4	上記のいずれも含まれていなかった	26	26.0%

Q4　紛失・盗難にあったとき、そのパソコンには、どのような対策をしていましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	ログインパスワードを設定していた	50	50.0%
2	指紋認証などの生体認証を使用していた	18	18.0%
3	機密データを含むファイルは個別に暗号化していた	29	29.0%
4	ハードディスク全体を暗号化していた	22	22.0%
5	盗難防止ワイヤで固定していた	11	11.0%
6	キャビネットなどに鍵を掛けて保管していた	9	9.0%
7	シンクライアント化していた、HDD を外していた	6	6.0%
8	上記以外の対策を講じていた	1	1.0%
9	上記のいずれの対策もしていなかった	22	22.0%

Q5　紛失・盗難の結果、以下のようなことををあなた自身が行ったり、あなたの職場で起きたりしましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	自分で会社、組織に報告・連絡した	39	39.0%
2	自分で顧客、取引先に報告・連絡した	27	27.0%
3	他所から会社や取引先へ連絡があった	9	9.0%
4	紛失・盗難の事実が、プレスリリースや報道で公表された	19	19.0%
5	会社、組織に始末書を提出した	16	16.0%
6	会社、組織から懲戒処分を受けた（戒告・譴責、減給、停職、免職など）	10	10.0%

7	会社、組織として、顧客、取引先に謝罪した（お詫びのメール・手紙や、謝罪訪問など）	8	8.0%
8	会社、組織として、顧客、取引先に賠償をした（慰謝料・賠償金の支払い、金券の送付など）	7	7.0%
9	自分の業務が一時的に滞った	9	9.0%
10	職場の上司・同僚・部下などの業務が一時的に滞った	11	11.0%
11	顧客、取引先の業務が一時的に滞った	5	5.0%
12	情報漏えいにより、自分の会社、組織の売上（成果）が減少した	5	5.0%
13	情報漏えいにより、顧客、取引先の売上（成果）が減少した	4	4.0%
14	上記のいずれも行ったり、起きたりしなかった	23	23.0%

6.4. 本調査の設問と回答（USB メモリ）

Q1　一番最近の紛失・盗難は、どのような状況で発生しましたか。（お答えは 1 つ）

		N	%
全体		100	100.0%
1	職場の中を持ち歩いていて、なくなった（どこかに置き忘れた・落としたなど）	25	25.0%
2	職場の引っ越し、部署異動、席替えなどの後、どこに行ったかわからなくなった	11	11.0%
3	机の上などに出しっぱなししたり、机の上のパソコンに差しっぱなしにしたりしていたら、なくなった（誰かが持っていった）	10	10.0%
4	引き出しや倉庫などの保管場所から、なくなった（誰かが持っていった）	5	5.0%
5	会社貸与の USB メモリの棚卸しをしたところ、なくなっていることがわかった	3	3.0%
6	間違って廃棄してしまった	5	5.0%
7	通勤中、勤務で移動中に、タクシー、電車、飛行機などの乗り物に置き忘れた	5	5.0%
8	取引先やその他の社外の作業場所、出張の宿泊先、セミナ会場など、勤務中に滞在した施設で無くした	3	3.0%
9	自宅、プライベートの出先で無くした。	12	12.0%
10	飲酒して酔っているときに、飲食店、タクシー、電車などの交通機関で無くした	2	2.0%
11	その他の紛失	1	1.0%
12	職場で盗難（空き巣・強盗など）にあった	0	0.0%
13	通勤中、勤務中にひったくり、置き引き、車上荒らしなどの盗難にあった	1	1.0%
14	自宅、プライベートの出先で盗難にあった	4	4.0%
15	その他の盗難	0	0.0%
16	いつ、どこで無くなったのか分からない	13	13.0%

Q2　紛失・盗難にあったUSBメモリには、どのような情報が含まれていましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	顧客や取引先の組織名称や住所、連絡先などの情報が含まれていた	34	34.0%
2	顧客や取引先の個人の氏名や住所、連絡先などの情報が含まれていた	36	36.0%
3	社外秘以上のデータファイルが含まれていた	19	19.0%

4	上記のいずれも含まれていなかった	33	33.0%

Q3　紛失・盗難にあったとき、そのUSBメモリには、どのような対策をしていましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	データファイルを個別に暗号化していた	24	24.0%
2	暗号化された領域にデータファイルを保存していた	27	27.0%
3	USBメモリ全体を暗号化していた	24	24.0%
4	USBメモリにパスワードによるロック機能がある	20	20.0%
5	USBメモリに指紋認証によるロック機能がある	9	9.0%
6	上記以外の対策を講じていた	3	3.0%
7	上記のいずれの対策もしていなかった	33	33.0%

Q4　紛失・盗難の結果、以下のようなことををあなた自身が行ったり、あなたの職場で起きたりしましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	自分で会社、組織に報告・連絡した	30	30.0%
2	自分で顧客、取引先に報告・連絡した	24	24.0%
3	他所から会社や取引先へ連絡があった	15	15.0%
4	紛失・盗難の事実が、プレスリリースや報道で公表された	13	13.0%
5	会社、組織に始末書を提出した	11	11.0%
6	会社、組織から懲戒処分を受けた（戒告・譴責、減給、停職、免職など）	11	11.0%
7	会社、組織として、顧客、取引先に謝罪した（お詫びのメール・手紙や、謝罪訪問など）	4	4.0%
8	会社、組織として、顧客、取引先に賠償をした（慰謝料・賠償金の支払い、金券の送付など）	10	10.0%
9	自分の業務が一時的に滞った	11	11.0%
10	職場の上司・同僚・部下などの業務が一時的に滞った	8	8.0%
11	顧客、取引先の業務が一時的に滞った	5	5.0%
12	情報漏えいにより、自分の会社、組織の売上（成果）が減少した	4	4.0%
13	情報漏えいにより、顧客、取引先の売上（成果）が減少した	3	3.0%

14	上記のいずれも行ったり、起きたりしなかった	30	30.0%

6.5. 本調査の設問と回答(電子メール)

Q1　一番最近の誤送信は、どのような状況で発生しましたか。(お答えは 1 つ)

		N	%
全体		100	100.0%
1	メールアドレスを手入力するときに、打ち間違えた	27	27.0%
2	アドレス帳から間違ったメールアドレスを選択してしまった	40	40.0%
3	アドレスを BCC に入れるべきところを、TO に入れてしまった	4	4.0%
4	アドレスを BCC に入れるべきところを、CC に入れてしまった	4	4.0%
5	流用したメールの宛先を変更すべきところを、そのまま送信してしまった	6	6.0%
6	流用したメールの本文を変更すべきところを、そのまま送信してしまった	3	3.0%
7	間違ったファイルを添付してしまった	9	9.0%
8	上記以外の状況で発生した	7	7.0%

Q2　誤送信した電子メールに含まれていた情報で、本来、含めるべきではなかった情報は、どのようなものでしたか。(お答えはいくつでも)

		N	%
全体		100	100.0%
1	顧客や取引先の組織名称や住所、電話番号などの情報	11	11.0%
2	顧客や取引先の個人の氏名や住所、携帯電話の番号などの情報	9	9.0%
3	顧客や取引先の組織のメールアドレス	12	12.0%
4	顧客や取引先の個人のメールアドレス	19	19.0%
5	社外秘以上のデータファイル	4	4.0%
6	上記以外の情報のみ	62	62.0%

Q3　誤送信したときは、以下のような対策をしていましたか。(お答えはいくつでも)

		N	%
全体		100	100.0%
1	アドレス帳の登録時に、分かりやすい名称を付けていた	17	17.0%
2	送信する前に、確認のためのダイヤログボックスを表示していた	10	10.0%
3	上司が確認、承認しないと送信されないしくみだった	6	6.0%

4	メールの暗号化を実施していた	9	9.0%
5	一斉送信を行う場合は、メーリングリストを使用していた	13	13.0%
6	一斉送信を行う場合は、一斉送信用のソフトウェアを利用していた	6	6.0%
7	上記以外の対策を講じていた	7	7.0%
8	上記のいずれの対策もしていなかった	48	48.0%

Q4　誤送信の結果、以下のようなことををあなた自身が行ったり、あなたの職場で起きたりしましたか。(お答えはいくつでも)

		N	%
全体		100	100.0%
1	自分で会社、組織に報告・連絡した	13	13.0%
2	自分で顧客、取引先に報告・連絡した	24	24.0%
3	他所から会社や取引先へ連絡があった	8	8.0%
4	誤送信の事実が、プレスリリースや報道で公表された	3	3.0%
5	会社、組織に始末書を提出した	3	3.0%
6	会社、組織から懲戒処分を受けた(戒告・譴責、減給、停職、免職など)	3	3.0%
7	会社、組織として、顧客、取引先に謝罪した(お詫びのメール・手紙や、謝罪訪問など)	7	7.0%
8	会社、組織として、顧客、取引先に賠償をした(慰謝料・賠償金の支払い、金券の送付など)	0	0.0%
9	自分の業務が一時的に滞った	5	5.0%
10	職場の上司・同僚・部下などの業務が一時的に滞った	3	3.0%
11	顧客、取引先の業務が一時的に滞った	0	0.0%
12	情報漏えいにより、自分の会社、組織の売上(成果)が減少した	0	0.0%
13	情報漏えいにより、顧客、取引先の売上(成果)が減少した	0	0.0%
14	上記のいずれも行ったり、起きたりしなかった	51	51.0%

6.6. 本調査の設問と回答（SNS）

Q1　一番最近、ブログ・SNS への書き込みや、ツイッターでのツイートで、業務上の秘密に関する情報や不適切な内容を書いてしまったのは、なぜですか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	ブログ・SNS への書き込みや、ツイッターでのツイートは普段、気軽に行っていたから	48	48.0%
2	家族・友人・同僚など、個人的に知っている人しか読んでいないと思ったから	37	37.0%
3	知らない人にはわからないように、部分的な内容しか書いていないので大丈夫だと思ったから	34	34.0%
4	秘密だとは知らなかった、または不適切な内容だとは思っていなかったから	21	21.0%
5	会社、組織に、業務上の秘密に関する情報や不適切な内容の書き込みを禁止するルールはなかったから	11	11.0%
6	ほかの人も同じような書き込みやツイートをしているから	11	11.0%
7	操作を間違ってしまったから	19	19.0%
8	その他の理由	0	0.0%

Q2　あなたがブログ・SNS への書き込みや、ツイッターでのツイートをしてしまった、業務上の秘密に関する情報や不適切な内容とは、どのような内容ですか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	あなた自身の会社、組織の機密の情報	47	47.0%
2	顧客、取引先の機密の情報	26	26.0%
3	業務上知ってしまった他人のプライバシー	26	26.0%
4	社会的に不適切と思われてしまう内容	21	21.0%
5	上記以外の内容のみ	20	20.0%

Q3　あなたがブログ・SNS への書き込みや、ツイッターでのツイートをしてしまったとき、あなたの会社、組織では以下のような対策が講じられていましたか。（お答えはいくつでも）

		N	%
全体		100	100.0%
1	ブログ・SNS への書き込みや、ツイッターでのツイートについての規則があった	32	32.0%
2	ブログ・SNS への書き込みや、ツイッターでのツイートについての従業員教育を受けた	28	28.0%
3	職場でのブログ・SNS への書き込みや、ツイッターでのツイートが禁止されていた	15	15.0%

4	プライベートも含め、すべてのブログ・SNS への書き込みや、ツイッターでのツイートが禁止されていた	11	11.0%
5	上記以外の対策を講じていた	7	7.0%
6	上記のいずれの対策もしていなかった	33	33.0%

Q4　ブログ・SNS への書き込みや、ツイッターでのツイートをしてしまった結果、以下のようなことををあなた自身が行ったり、あなたの職場で起きたりしましたか。(お答えはいくつでも)

		N	%
全体		100	100.0%
1	自分で会社、組織に報告・連絡した	29	29.0%
2	自分で顧客、取引先に報告・連絡した	23	23.0%
3	他所から会社や取引先へ連絡があった	18	18.0%
4	誤送信の事実が、プレスリリースや報道で公表された	13	13.0%
5	会社、組織に始末書を提出した	13	13.0%
6	会社、組織から懲戒処分を受けた(戒告・譴責、減給、停職、免職など)	8	8.0%
7	会社、組織として、顧客、取引先に謝罪した(お詫びのメール・手紙や、謝罪訪問など)	6	6.0%
8	会社、組織として、顧客、取引先に賠償をした(慰謝料・賠償金の支払い、金券の送付など)	6	6.0%
9	自分の業務が一時的に滞った	7	7.0%
10	職場の上司・同僚・部下などの業務が一時的に滞った	6	6.0%
11	顧客、取引先の業務が一時的に滞った	5	5.0%
12	情報漏えいにより、自分の会社、組織の売上(成果)が減少した	6	6.0%
13	情報漏えいにより、顧客、取引先の売上(成果)が減少した	5	5.0%
14	上記のいずれも行ったり、起きたりしなかった	35	35.0%