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～

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
2011 年 3 月 31 日

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
　佳山　こうせつ　　富士通株式会社
　菊谷　広　　ドコモ・システムズ株式会社
　北野　晴人　　日本オラクル株式会社(※)
　佐藤　康彦　　マイクロソフト株式会社
　田中　洋　　株式会社 インフォセック(※)
　長久　浩三　　株式会社 アイ・ティ・フロンティア
　馬鳥　雄也　　日本オラクル株式会社
　広口　正之　　リコー・ヒューマン・クリエイツ株式会社(※)
　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(※)
　吉田　裕美　　株式会社ラック
（※）：報告書 執筆担当者　　無印：検討～レビューの担当者

協力：　リスク評価検討ワーキンググループ

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

予備調査と本調査の結果から、1 年間に 5 種類の紛失盗難、誤送信の情報セキュリティ・インシデントを経験した会社員の割合を算出した。最近の 1 年間における各インシデントのおおよその発生確率を表 1.1-1 に示す。

会社員のうち、1 年間に携帯電話を紛失する人、盗難にあう人、紛失しそうになる人の割合は、約 6.5%となった。同様に、パソコンの場合は、約 3.5%となった。USB メモリを紛失する人、盗難にあう人の割合は、約 4.5%となった。1 年間に電子メールや FAX の誤送信を行う会社員の割合は、どちらも約 40%となった。

表 1.1-1：紛失・盗難、誤送信の年間発生確率

調査対象	年間発生確率
携帯電話	約 6.5%
パソコン	約 3.5%
USB メモリ	約 4.5%
電子メール	約 40.0%
FAX	約 40.0%

パソコンの紛失盗難の年間発生確率よりも、USB メモリの紛失盗難の年間発生確率が高い。USB メモリのほうが小さく、紛失しやすいからと予想される。大きさと紛失確率に関係があるとすれば、携帯電話よりも USB メモリの紛失盗難の発生確率が高くなるはずである。しかし、USB メモリは、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ているため、携帯電話よりも紛失確率が低いと思われる。

電子メールと FAX の誤送信の年間発生確率は、どちらも同じ約 40%となった。片や FAX または複合機などの装置を使った物理的な操作であり、片やパソコンや携帯電話上のソフトウェアを使った操作であるが、奇しくもその年間誤送信確率が極めて近いことは、大変興味深い。どちらも、送信先からの返答などから送信先の正確性を確認する前に情報を送出してしまう方式であり、誤送信を防止する方法が人的な対策に頼っていることが、関係していると予想する。

1.2. おっちょこちょいの比率

業務データが入った携帯電話を紛失しそうになった人をターゲットにして、実際に携帯電話を紛失・盗難にあっているか集計をした結果の考察してみた。その結果を以下に示す。

表 1.2-1：携帯電話を紛失しそうになった人が実際に紛失した割合

紛失・盗難の対象	会社携帯（業務データあり）		私物携帯（業務データあり）		会社・私物の両方の携帯電話		携帯紛失・盗難なし		全体
アンケート全体	184	3.8%	204	4.2%	631	12.9%	3,906	80.0%	4,884
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	15	8.4%	22	12.4%	46	25.8%	132	74.2%	178
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	7	3.6%	12	6.1%	28	14.3%	168	85.7%	196
業務データが入った会社と私物両方の携帯電話を紛失しそうになったことがある	33	36.3%	34	37.4%	44	48.4%	47	51.6%	91

※「会社と私物の両方の携帯電話」には、業務データが入っていない携帯電話も含む

会社貸与の携帯電話を紛失しそうになった人の実際に紛失した割合は、アンケート全体における会社貸与の携帯電話を紛失した人の割合よりも 2 倍以上高い。会社と私物の両方の携帯電話を紛失しそうになった人が実際に紛失・盗難にあった割合は、アンケート全体における割合の８倍以上である。

表 1.2-2：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		全体
アンケート全体	184	3.8%	148	3.0%	146	3.0%	4,884
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			108	58.7%	102	55.4%	184
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	108	73.0%			97	65.5%	148
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	102	69.9%	97	66.4%			146

携帯電話・パソコン・USB メモリのいずれかの紛失・盗難にあった人は、50%以上の確率で他の物の紛失・盗難にあっている。特に、会社貸与のパソコンの紛失・盗難にあっている人が会社貸与の携帯電話の紛失・盗難にあう確率は 70%を超える。

以上から、紛失しやすい人、おっちょこちょいは、存在すると予想する。上記より、複数の物を紛失した人は、およそ 100 人であることから、おっちょこちょいの比率は、約 2%と推定される。

1.3. パソコン紛失のリスクは社内にあり!?

パソコンの紛失は、居酒屋など、外出先で飲酒したときに発生する確率が高いイメージがある。しかし、予想外にも、パソコンおよび USB メモリの紛失・盗難が起きたときの状況は、「勤務中、社内で無くした」がもっとも多い。パソコンの紛失を分析した結果を表 1.3-1 に示す。「Ⅱ 勤務外または社外紛失群」は勤務外や社外での全ての紛失を対象としているため最も割合が高く、全体の 50%を占める。次は「Ⅰ 社内紛失群」の割合が高く 29%を占める。

表 1.3-1：パソコン紛失・盗難全体での「社内紛失」の割合

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「勤務中、社内で無くした」を選んだ回答者	29 件	29%
Ⅱ 勤務外または社外紛失群	Q2 で選択肢 2～6（社内以外の状況での紛失）を選んだ回答者	50 件	50%
Ⅲ 盗難群（分析対象外）	Q2 で選択肢 7～9（盗難）を選んだ回答者	17 件	17%
Ⅳ 不明群（分析対象外）	Q2 で選択肢 10「いつ、どこで無くなったのか分からない」を選んだ回答者	4 件	4%
合計		100 件	100%

以上の分析結果から、社内での紛失事故の発生頻度は飲酒時を上回ることがわかった。社内で紛失したパソコンには顧客、取引先に関する情報などが入っている場合も多く、セキュリティ対策があまり行われていない傾向があった。このことから、あまりセキュリティが意識されておらず、社内の管理が行き届いていないパソコンが紛失しやすい傾向にあるものと思われる。

また、社内でのパソコンの紛失は、会社や組織への報告・連絡がよく行われている傾向があることから、会社や組織が行う棚卸しなどの業務によって紛失が発覚しているものと思われる。逆に言えば、資産の棚卸しなどが行われなければパソコンの紛失は発覚せず、誰にも気づかれないままひっそりと、多数のパソコンが紛失し続けている恐れがある。パソコンを外部に持ち出した際の紛失は、本人が気づきやすい事故であるが、社内管理の不備による社内紛失は、定期的にきちんと棚卸しを行って管理を行わない限り発覚しにくい。

よって、社内で紛失するパソコンは、対策を検討すべき重要なリスクと考えるべきである。こうした紛失事故のリスクを抑えるためには、社外に持ち出すパソコンばかりに対策を集中するのではなく、社内使用のパソコンにも紛失・盗難対策を行き届かせ、定期的な棚卸しによる管理と意識の浸透に心がけることが必要と言える。

2. アンケートの実施概要

2.1. 調査目的

JNSA インシデント被害調査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」を過去数年にわたり作成・公表してきている。

このレポートは、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、一般の仕事を行っている個人を対象としたアンケート調査を行うこととした。

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：2010 年 10 月 15 日(金) ～ 10 月 19 日(火)**

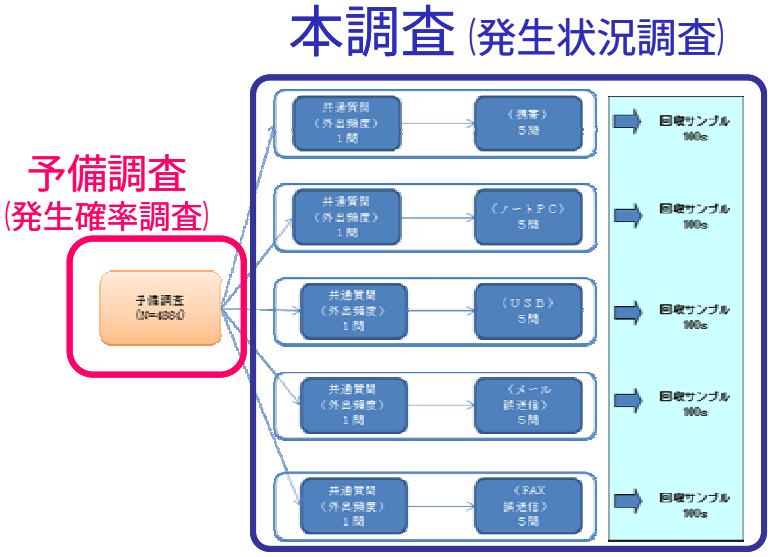

図 2.2-1：調査方法

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 2.2-1 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／⑤FAX の誤送信）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・求職中等の人は対象から除外している。

■ **予備調査の有効回答者数：4,884 名**

表 2.3-1：年齢層（予備調査 N=4884）

No	年齢層	回答者数	割合(%)
1	18～29 歳	481 名	9.8%
2	30～39 歳	1,268 名	26.0%
3	40～49 歳	1,426 名	29.2%
4	50 歳以上	1,709 名	35.0%

表 2.3-2：職業・職種（予備調査 N=4884）

No	職業・職種	回答者数	割合(%)
1	会社経営者・役員・団体役員	240 名	4.9%
2	会社員・団体職員（正社員）	2,787 名	57.1%
3	会社員・団体職員（契約・派遣）	388 名	7.9%
4	地方公務員	144 名	2.9%
5	国家公務員	40 名	0.8%
6	自営業・個人事業主・フリーランス	582 名	11.9%
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）	101 名	2.1%
8	パート・アルバイト・フリーター	602 名	12.3%
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%

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／FAX の誤送信）の経験者数とその割合を図 3.1-1 に示す。

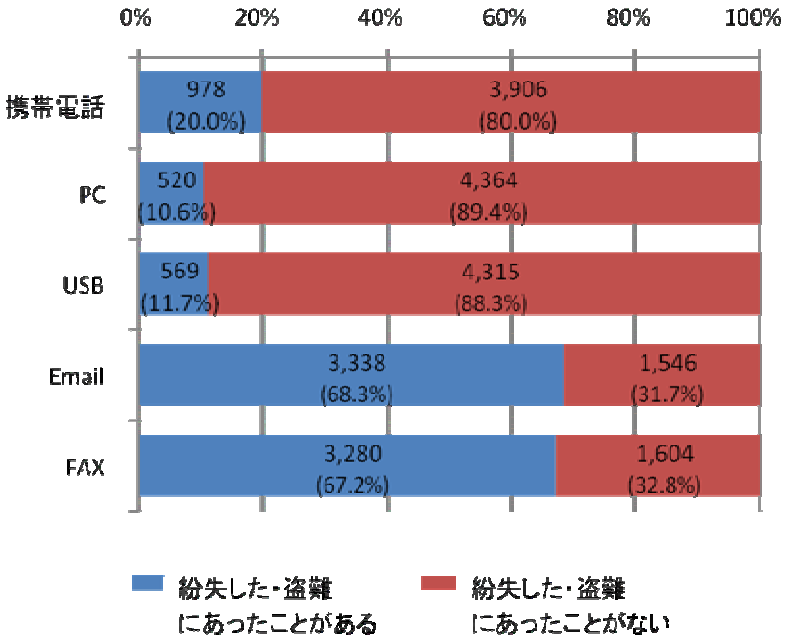

図 3.1-1：情報セキュリティ・インシデントの経験者数と割合

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・インシデントの発生確率を算出した。算出した 2009 年と 2010 年の発生確率を表 3.1-1 に示す。

表 3.1-1：紛失・盗難、誤送信の年間発生確率

調査対象	2010 年	2009 年
携帯電話	6.4%	6.6%
パソコン	3.7%	3.1%
USB メモリ	4.7%	4.1%
電子メール	40.3%	17.1%
FAX	39.0%	12.1%

3.1.1. 携帯電話

本調査から、携帯電話を紛失・盗難した人と紛失しそうになった人の 100 人のうち、それが「2010 年」または「2009 年」に発生した人の割合は、それぞれ約 30%であることが判明した。予備調査から判明した携帯電話を紛失・盗難した人と紛失しそうになった人の割合「20.0%」と上記の本調査の値から、1 年間に携帯電話を紛失・盗難する、または紛失しそうになる会社員の確率は、約 6.5%と想定される。

ただし、会社貸与の携帯電話と私物の携帯電話の両方が対象であることに注意してほしい。

3.1.2. パソコン、USB メモリ

パソコン、USB メモリについても、同様に計算した結果、会社員のパソコンの年間紛失・盗難確率（紛失未遂も含む）は約 3.5%、USB メモリの年間紛失・盗難確率は約 4.5%となった。

パソコンの年間紛失確率よりも、USB メモリの年間紛失確率が高い。USB メモリのほうが小さく、紛失しやすいからであろう。大きさと紛失確率に関係があるとすれば、USB メモリの紛失確率が最も高いはずであるが、USB メモリの年間紛失確率は、携帯電話の年間紛失確率より低い。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。

携帯電話、パソコン、USB メモリは、2009 年の発生確率と 2010 年の発生確率の差が少ない。同じ人が、携帯電話、パソコンや USB メモリを毎年紛失することは、あまりないと感じる。つまり、携帯電話、パソコン、USB メモリの紛失、盗難はそれほど頻繁に発生しないため、2009 年と 2010 年の発生確率は、それぞれ独立事象となっていると予想する。

したがって、2009 年の発生確率と 2010 年の発生確率は近い値になり、この値を直近の年間発生確率（携帯電話 約 6.5%、パソコン 約 3.5%、USB メモリ 約 4.5%）と考えてよいと思われる。

3.1.3. 電子メール、ＦＡＸ

会社員の電子メールと FAX の年間の誤送信の発生確率は、どちらも約 40%となった。これは、過去 1 年間で少なくとも 1 回の誤送信を行った人の存在する確率であり、その中には誤送信を複数回行った人も含まれていると予想される。本調査において、電子メールと FAX の 2007 年より以前の誤送信の発生数は、それほど多くない。（詳細は、「本調査の設問と回答（電子メール）」「本調査の設問と回答（FAX）」参照。）電子メールも FAX も使用回数が多いこと、誤送信を経験する確率も高いことから、2 年以上前の誤送信があまり記憶に残っていない可能性がある。電子メールの 2009 年の発生確率が約 17%と低く、2010 年が約 40%と高い理由は、毎年電子メールの誤送信を一回以上行っている人は、2010 年に回答しているからだと思われる。

片や FAX または複合機などの物理的な装置であり、片やパソコンや携帯電話上のソフトウェアであるが、奇しくもどちらも、送信先の正確性を確認する前に情報を送出してしまうシステムであり、その年間誤送信確率が極めて近いことは、大変興味深い。

本調査では、アンケート回答者に、紛失や盗難、誤送信を行った時期を「2010 年」「2009 年」「2008 年」「2007 年以前」の 4 つの中から 1 つだけを選択させた。したがって、回答者は、直近の情報セキュリティ・インシデントの発生年を回答している。2009 年と 2010 年の両方の年に電子メール、FAX を誤送信した人は、2010 年を選択している。したがって、2010 年と比べて、2009 年の誤送信の発生確率が特別に低いわけではない。また、「2008 年」と「2007 年以前」以前の発生確率も低い値になった。これは、2 年以上前の電子メールや FAX の誤送信は、上記の理由に加え、記憶が曖昧になっているため、正確な値が得られなかったと予想される。

2010 年 10 月中旬時点において取得したデータであるため、2010 年 1 年間に紛失や盗難、誤送信を行った人数は、やや少ない値であることが予想される。今後、調査時期や数値補正を検討する。

3.2. リスク相当金額の算出

以下に示す比較的単純で、基本的な確率の計算手法を適用しやすいセキュリティ・インシデントを取り上げ、企業におけるリスク（被害想定金額）の算出を試みる。試算を行うにあたっては本報告書にある調査結果の中から、USB メモリの紛失・盗難を取り上げた。

3.2.1. 想定企業プロファイル

ここでは JNSA による「2003 年度情報セキュリティ・インシデントに関する調査報告書」に掲載されている「個人情報漏えい事件での緊急対応費用の推定」において使用された企業プロファイルを利用して、試算することとした。

【企業プロファイル】

想定した企業は、雑誌やインターネット上のカタログに商品を掲載し、商品の販売を行う通信販売業とした。近年は、インターネットショッピングサイトも運用し、インターネットショッピングサイトの売り上げは、会社全体の売り上げの約 10%程度とした。以下に想定企業のプロファイルを示す。（インターネットショップ部門の利益率＝約 10%、年間成長率＝約 10%とする。）

表 3.2-1：想定企業のプロファイル

企業規模		
売上高	約 1000 億円	
従業員	約 1000 名	
カタログ販売部門		インターネットショップ部門
会員数	約 600 万人	約 100 万人
売上げ	約 900 億円	約 100 億円
従業員		約 30 名

この企業は、CRM 用の顧客情報として以下の項目を収集・管理している。

- 氏名、氏名フリガナ、性別、年齢（区分）、職業
- 郵便番号、住所、電話番号
- 購入履歴情報（商品コード、購入日時）
- ショッピングサイトのログインＩＤ／パスワード
- クレジットカード番号、有効期限、金融機関の口座番号

  ただし、上記の信用情報は分離された別システムで取扱い、企業内から参照できない。

また、この企業ではカタログ販売にともなう商品の配送委託先やショッピングサイトに出店・商品を提供している企業等と顧客情報を日常的にやりとりしており、このデータの持ち運びには USB メモリを利用している。これはメール添付による誤送信事故を防ぐために

行われており、USB メモリは会社が社員に対して支給しているが、暗号化等の対策は行われていない。企業内でこうした業務に従事している外回り関係の従業員は全体の 10%、100 名程度である。

3.2.2. 被害金額の想定

まず漏えい事件が発生した際の想定被害金額を試算する。JNSA の「2009 年情報セキュリティインシデントに関する調査報告書」における「漏えい媒体・経路別の一件あたりの漏えい人数」によると、USB メモリ等の可搬型媒体を経由した情報漏えい事件における漏えい人数の平均は 28,339.8 人となっている。そこで、ここでは全体の会員情報の中から 20,000 人の情報が USB メモリの紛失によって漏えいしたものとする。

ここではサイトの閉鎖等の対応はなく、逸失利益、機会損失等の直接被害はないと考えて間接被害については以下のように計算した。

表 3.2-2：間接被害の内訳

項目		費用
業務継続費用	対策組織業務に係る人件費（１ヶ月分）	500 万円
	損害賠償費用（訴訟参加率=0.1%）	36 万円
	弁護士費用・裁判費用	30 万円
見舞い品費用	見舞い品代＋送料他（２万人分）	1,400 万円
謝罪訪問費	謝罪訪問に掛かる費用（10 人分）	110 万円
広報費用	謝罪広告費	なし
	情報公開ページ作成費用（２回）	10 万円
臨時的な対策費用	コールセンター設置費用（１ヶ月分）	500 万円
	問い合わせ窓口常駐人員（１ヶ月分）	200 万円
合計		2,786 万円

前提条件：
①訴訟参加率については、近年の個人情報保護意識の高まり等を鑑み、やや高めの想定。
②弁護士費用については、実務的な現実では相当額の着手金が必要なことから、民事訴訟等の着手金における現実的な金額として30万円を想定した、（参考：日本弁護士連合会「中小企業のための弁護士報酬目安[2009年アンケート結果版]」

3.2.3. USB メモリ紛失の発生率からリスクを試算

この企業で日常的に USB メモリを使って顧客情報を持ち運んでいる社員が 100 名であることから、この 100 名に対して本調査による紛失・盗難の発生確率 4.5%を適用する。また紛失した USB メモリに個人情報が含まれている確率は、本調査において紛失・盗難の USB

メモリに個人情報が含まれていたとの回答が 100 人中 33 人から得られており、これを適用すると、約 33%に個人情報が含まれていることになる。
従って事象としては以下のようになる。

①事象 A として「USB メモリの紛失・盗難に遭う」とする。
②事象 B として「紛失した USB メモリに個人情報が含まれている」とする。

ここで事象 A と事象 B が同時に起こる確率を考えるので、これは A と B の積事象 A∩B である。また、現実的に「USB メモリを紛失する」という行為と「USB メモリに個人情報を格納する」という行為は相互に影響を及ぼすことはなく、従ってこの事象 A と B は独立事象であると考えることができる。そこで２つの事象が同時に起こる確率は乗法定理を適用し、P（A∩B）＝P(A)・P(B)で求めることができる。実際に計算すると、事象 A が起きる確率は 4.5%、事象 B が起きる確率は 33%であるから、乗法定理を適用すると 4.5% × 33%＝約 1.5%となる。従って 1 年間に個人情報を格納した USB メモリを紛失する確率は従業員 1 人あたり約 1.5%である。（ここでは USB で顧客情報を持ち歩く社員が、実際にどこで紛失するかはわからないため、紛失場所が社内であるか、社外であるかという点については考慮していない。本調査では紛失場所は社内が多いという結果になっている。）
さらに、日常的に USB メモリで顧客情報を持ち運んでいる社員が 100 名であるとすると実際に事故が起きる予測件数は 100 人×1.5%/人＝1.5 人となる。従って、表 3.2-2 より、1 回のインシデントで予想される損失金額が 2,786 万円なので、2,786 万円×1.5 人＝4,179 万円をリスクとして考えることができる。

この計算が成り立てば、上記のようなプロファイルの組織において、年間 4,179 万円以下であればこの事故を防止するためのセキュリティ対策に投資しても良いということができる。さらに現在の IT 機器、ソリューションなどのライフサイクルがおおむね 3 年程度であることを考えれば、4,179 万円×3＝1 億 2,537 万円までを 3 年分としてまとめて投資をすることも検討の余地があるといえる。
また逆に損失金額が小さくリスク算出額が対策のための投資額を下回るようなら、あえて費用をかけることはせず「リスクを受容する」というリスク管理上の選択もあり得る。

ただし現実の情報セキュリティリスク管理として精度を上げるためには事故発生確率が従業員ごとに違うことも考慮に入れ、（次章「おっちょこちょいの比率参照」）これらの統計的処理を行って企業全体での事故発生確率の精度を高める必要等がある。

3.3. おっちょこちょいの比率

3.3.1. 携帯電話を紛失しそうになったことがある人は、実際に紛失しているか

業務データが入った携帯電話を紛失しそうになった人をターゲットにして、実際に携帯電話を紛失・盗難にあっているか集計をした結果の考察してみた。

表 3.3-1：携帯電話を紛失しそうになった人が実際に紛失した割合

紛失・盗難の対象	会社携帯（業務データあり）		私物携帯（業務データあり）		会社・私物の両方の携帯電話		携帯紛失・盗難なし		全体
アンケート全体	184	3.8%	204	4.2%	631	12.9%	3,906	80.0%	4,884
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	15	8.4%	22	12.4%	46	25.8%	132	74.2%	178
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	7	3.6%	12	6.1%	28	14.3%	168	85.7%	196
業務データが入った会社と私物両方の携帯電話を紛失しそうになったことがある	33	36.3%	34	37.4%	44	48.4%	47	51.6%	91

※「会社と私物の両方の携帯電話」には、業務データが入っていない携帯電話も含む

- 会社貸与の携帯電話を紛失しそうになった人は、アンケート全体の集計結果と比較すると、紛失している人が多くなっている。
- 私物の携帯電話を紛失しそうになった人は、アンケート全体の集計結果と比較しても変わらなかった。紛失も盗難にも合っていない人は、全体の集計結果よりも比率が増加している。
- 会社と私物の両方を紛失しそうになった人は、実際に紛失・盗難にあっている率が、全体の集計の 8 倍以上になっている。

以下の仮説が考えられる。

- 私物の携帯電話は、会社貸与の携帯電話より大事にしている。もしくは、いつも持ち歩いているので紛失しにくい。なくなりそうになってもすぐ気付く。
- 会社と私物の両方の携帯電話を紛失しそうになった人は、紛失しやすい人（おっちょこちょい）の可能性が高い。一定の割合で存在するおっちょこちょいには、注意が必要である。

3.3.2. パソコンを紛失しそうになったことがある人は、実際に紛失しているか

業務データが入ったパソコンを紛失しそうになった人をターゲットにして、実際にパソコンが紛失・盗難にあっているか集計をした結果の考察してみた。

表 3.3-2：パソコンを紛失しそうになった人が実際に紛失した割合

紛失・盗難の対象	会社 PC（業務データあり）		私物 PC（業務データあり）		会社・私物の両方の PC		PC 紛失・盗難なし		全体
アンケート全体	148	3.0%	129	2.6%	307	6.3%	4,364	89.4%	4,884
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	21	16.5%	16	12.6%	35	27.6%	92	72.4%	127
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	2	2.0%	4	4.1%	8	8.2%	90	91.8%	98
業務データが入った会社と私物両方のパソコンを紛失しそうになったことがある	24	35.8%	24	35.8%	36	53.7%	31	46.3%	67

※「会社・私物の両方の PC」には、業務データが入っていない PC も含む

- 会社貸与のパソコンを紛失しそうになった人は、アンケート全体の集計結果と比較すると、多くなっている。
- 私物のパソコンを紛失しそうになった人は、アンケート全体の集計結果と比較しても変わらなかった。紛失も盗難にも合っていない人は、全体の集計結果よりも比率が増加している。
- 会社と私物の両方を紛失しそうになった人は、実際に紛失・盗難にあっている率が、全体の集計の 10 倍以上になっている。

以下の仮説が考えられる。

- 私物のパソコンは、会社貸与のものより大事にしている。
- 会社と私物の両方を紛失しそうになった人は、紛失しやすい人（おっちょこちょい）の可能性が高いので注意が必要である。

3.3.3. 携帯電話、パソコン、USB メモリを重複して紛失した人は多いか

業務データが入った携帯電話・パソコン・USB メモリを紛失・盗難にあった人が、他の物も紛失・盗難にあっている傾向を考察してみた。

表 3.3-3：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		全体
アンケート全体	184	3.8%	148	3.0%	146	3.0%	4,884
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			108	58.7%	102	55.4%	184
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	108	73.0%			97	65.5%	148
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	102	69.9%	97	66.4%			146

- 携帯電話・パソコン・USB メモリを紛失・盗難にあった人は、50%以上の確率で他の物も紛失・盗難にあっている。
- 特に、会社貸与のパソコンを紛失・盗難にあっている人は会社貸与の携帯電話の紛失・盗難の率は 70%を超えている。

以下の仮説が考えられる。

- 物を紛失しやすい人（おっちょこちょい）は、存在する。
- 携帯電話・パソコン・USB メモリを同じバッグに入れて、紛失・盗難にあっているケースが多いのかもしれない。

3.3.4. 物を紛失しやすい人は誤送信もしやすいか

業務データが入った携帯電話・パソコン・USB メモリを紛失・盗難にあった人が、メールや FAX の事故を起こしている傾向を考察してみた。

表 3.3-4：業務データの入った会社貸与物の紛失・盗難と誤送信

紛失・盗難の有無	業務データが入った会社貸与の携帯電話		業務データが入った会社貸与のパソコン		業務データが入った会社貸与の USB メモリ	
	あり	なし	あり	なし	あり	なし
メールを誤った宛先へ送信したことがある	129 (70.1%)	2,916 (62.0%)	115 (77.7%)	2,930 (61.9%)	122 (83.6%)	2,923 (61.7%)
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	65 (35.3%)	405 (8.6%)	61 (41.2%)	409 (8.6%)	66 (45.2%)	404 (8.5%)
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	42 (22.8%)	189 (4.0%)	39 (26.4%)	192 (4.1%)	43 (29.5%)	188 (4.0%)
FAX で誤った宛先へ送信したことがある	134 (72.8%)	2,523 (53.7%)	110 (74.3%)	2,547 (53.8%)	120 (82.2%)	2,537 (53.5%)
FAX で間違った文書を送信したことがある	69 (37.5%)	978 (20.8%)	62 (41.9%)	985 (20.8%)	68 (46.6%)	979 (20.7%)
メールを誤送信したことはない	40 (21.7%)	1,506 (32.0%)	20 (13.5%)	1,526 (32.2%)	13 (8.9%)	1,533 (32.4%)
FAX を誤送信したことはない	34 (18.5%)	1,570 (33.4%)	25 (16.9%)	1,579 (33.3%)	14 (9.6%)	1,590 (33.6%)
全体	184	4,700	148	4,736	146	4,738

- 携帯電話・パソコン・USB メモリを紛失・盗難にあった人は、メールや FAX の事故も紛失・盗難にあっていない人よりも多い。
- 特に、「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」「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」の項目では４～5 倍の率になっている。

以下の仮説が考えられる。

- 物を紛失しやすい人（おっちょこちょい）は、誤送信の事故も起こしやすい。

3.4. パソコン紛失のリスクは社内にあり!?

本報告書5.2 および5.3 の単純集計に見られるとおり、パソコンおよび USB メモリの紛失・盗難が起きたときの状況は、「勤務中、社内で無くした」がもっとも多い。

パソコンを「勤務中、社内で無くした」と回答された事故はおそらく、資産台帳と実際の保有資産が一致しなかったケースや、部署異動・廃棄などの際の管理漏れ、あるいは職場の同僚が勝手に他部署で使用しているといった盗難とは言えない紛失などのケースが含まれていると推測される。こうした詳細の情報収集は、将来の調査課題である。

本節は、今回の調査で収集したデータの分析から、パソコンの社内紛失・盗難の実態を推測すべく考察を行うものである。

3.4.1. 社内でのパソコン紛失はどれほどのリスクか

(1). 紛失・盗難全体での割合

分析を試みるにあたり、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。

表 3.4-1：パソコン紛失・盗難全体での「社内紛失」の割合

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「勤務中、社内で無くした」を選んだ回答者	29 件	29%
Ⅱ 勤務外または社外紛失群	Q2 で選択肢 2～6（社内以外の状況での紛失）を選んだ回答者	50 件	50%
Ⅲ 盗難群（分析対象外）	Q2 で選択肢 7～9（盗難）を選んだ回答者	17 件	17%
Ⅳ 不明群（分析対象外）	Q2 で選択肢 10「いつ、どこで無くなったのか分からない」を選んだ回答者	4 件	4%
合計		100 件	100%

Ⅱ「勤務外または社外紛失」群は紛失場所を限定せずに、勤務外や社外での紛失を合計しているため最も割合が大きく、全体の 50%となっている。しかしⅠ「社内紛失」群もまた、紛失・盗難全体のうち 29%もの部分を占めている。

本節での以降の分析は、社内での紛失とその他の紛失とを比較するため、Ⅰ「社内紛失」群とⅡ「勤務外または社外紛失」群とで事故発生の状況にどのような差異があるかを見ていくこととする。

(2). 実際に紛失被害が発生しているか

今回の調査では、パソコンの紛失については、実際に「紛失したことがある」回答者だけでなく、「紛失しそうになったことがある」場合についても回答者に含んでいる。

社内での紛失により、実際に損失が発生する可能性（リスク）が大きいかどうかを考察す

るためには、紛失しそうになった場合ではなく実際に紛失事故が発生した割合を、勤務外または社外の紛失と比較しておく必要がある。

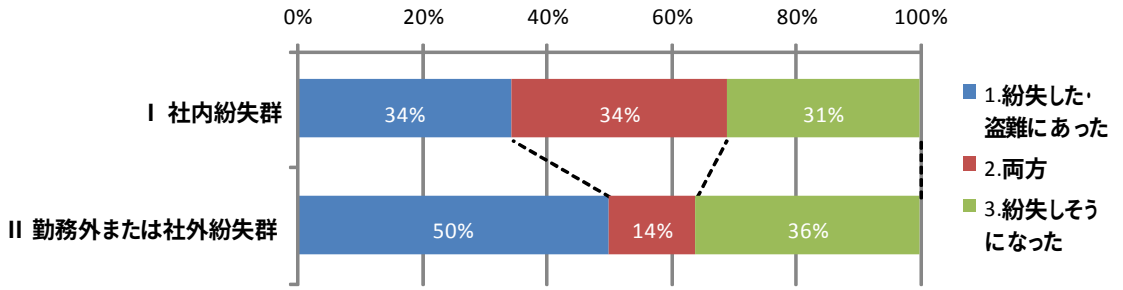

図 3.4-1：実際に紛失したか、紛失しそうになっただけか

上図は、予備調査における SC4 の回答から、パソコンを実際に「紛失したことがある」回答者、「紛失しそうになったことがある」回答者、および両方の経験のある回答者の 3 グループに分けて、Ⅰ「社内紛失」群とⅡ「勤務外または社外紛失」群での分布を比較した。

今回の本調査では、一人の回答者で複数回の紛失・盗難経験がある場合は「一番最近のものについてお答えください」としたため、両方の経験者については本調査への回答が実際の紛失・盗難についてのものか、紛失しそうになっただけのケースかは不明である。

したがってⅠ「社内紛失」群のうち、確実に実際の紛失被害が発生したと断定できる件数は「紛失した」のみを経験した回答者 10 件（34%）であり、これはパソコンの紛失・盗難全体のうち 10%にあたる。

この割合は Q2 で「自宅、プライベートの出先でなくした」や「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」を選択した回答者の割合（それぞれ 8%、4%）よりも大きく、社内での紛失リスクは、自宅持ち帰り時や飲酒時の紛失リスク以上に大きいことがわかる。

3.4.2. 社内ではどのようなパソコンが紛失しているのか

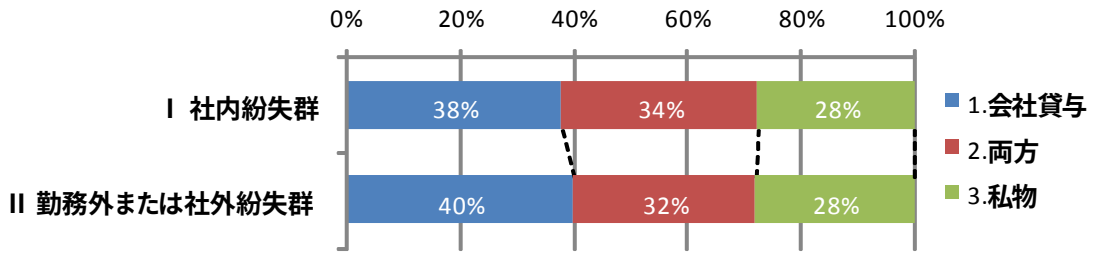

図 3.4-2：社内で紛失したパソコンは会社貸与か私物か

上図は、予備調査における SC4 の回答から、会社貸与のパソコンの紛失経験のある回答者、私物の紛失経験のある回答者、およびそれらの両方の経験のある回答者の 3 グループに分けて、Ⅰ「社内紛失」群とⅡ「勤務外または社外紛失」群での分布を比較した。

比較の結果として明らかな差異はみられず、社内で紛失しているパソコンは会社貸与のものだけでなく、社内に持ち込まれた私物パソコンも多く含まれていることがわかる。

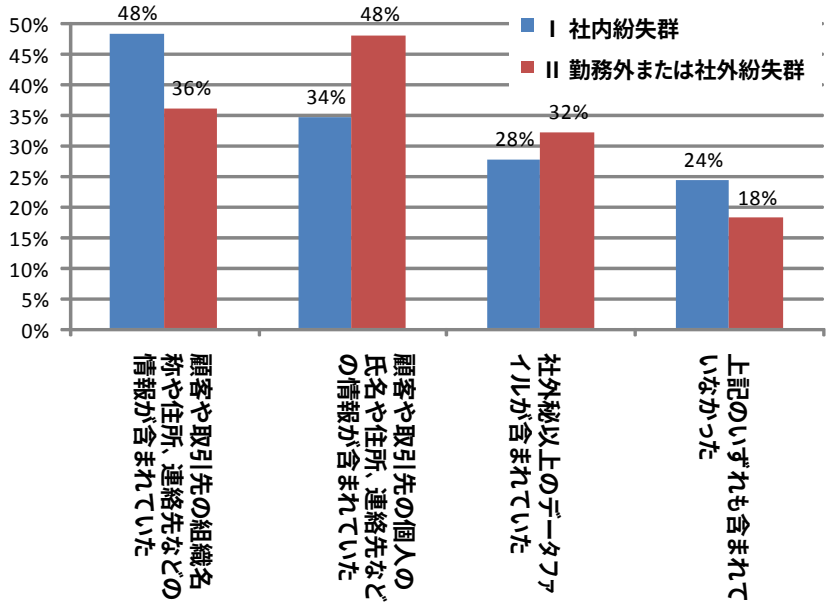

図 3.4-3：社内で紛失したパソコンにはどのような情報が含まれていたか

上図は Q3 の回答から、紛失にあったパソコンにどのような情報が含まれていたかについて、Ⅰ「社内紛失」群とⅡ「勤務外または社外紛失」群での分布を比較した。

Ⅰ・Ⅱ群で幾分の差異はあるものの、全体として明らかな傾向は見られなかった。社内で紛失しているパソコンは、含まれている情報の機密性について明らかな傾向はないことがわかる。

3.4.3. 社内ではどのような使い方をしてパソコンを紛失しているのか

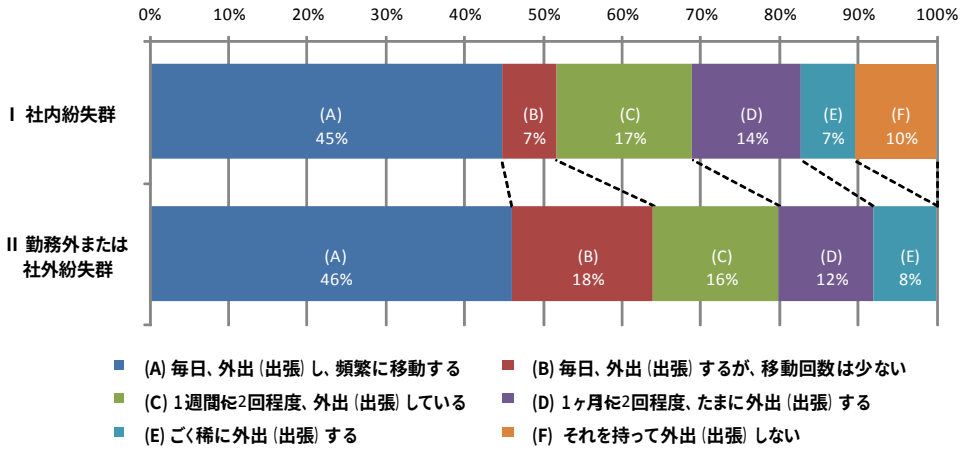

図 3.4-4：会社貸与パソコンの持ち出し状況

予備調査の SC2 の回答から、パソコンを持って外出する頻度について、Ⅰ「社内紛失」群とⅡ「勤務外または社外紛失」群での分布を比較した。なお、「それを持って外出（出張）しない」という回答者は当然ながらⅡ「勤務外または社外紛失」群では 0 件である。

Ⅰ群とⅡ群の比較では、Ⅰ群では「毎日、外出（出張）するが、移動回数は少ない」という回答者の割合が低かったものの、全体としては外出頻度に関する顕著な傾向はみられなかった。社内での紛失は、外部でパソコンを持ち歩くことが多いかどうかには関わりなく発生していると思われる。

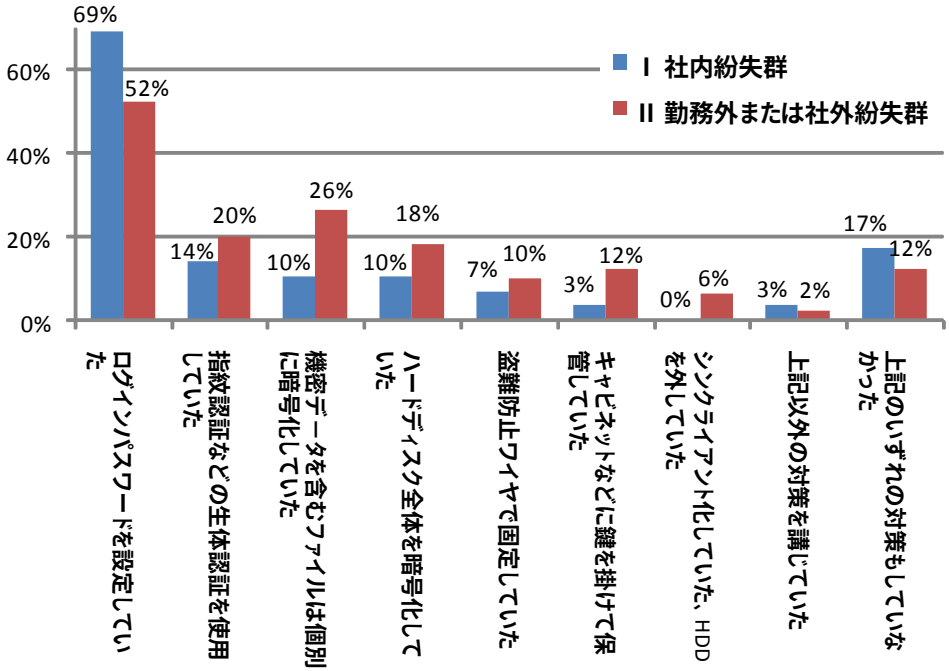

図 3.4-5：紛失・盗難対策を行っているか

上図は Q4 の回答から、紛失・盗難したパソコンには普段から紛失・盗難対策を行っていたかどうかについて、Ⅰ「社内紛失」群とⅡ「勤務外または社外紛失」群の分布を比較した。

Ⅰ群の対策状況は、Ⅱ群と較べて「ログインパスワードを設定していた」だけは実施率が高いものの、その他のセキュリティ対策はすべてⅡ群よりも実施率が低かった。またⅠ群は「いずれの対策もしていなかった」という回答者が 17%にものぼった。

社内で使用しているパソコンには管理上、ログインパスワードの設定が求められることは多い。しかし、それ以上のセキュリティについては意識されないまま、パソコンが社内で紛失しているものと思われる。

3.4.4. 社内でのパソコン紛失は報告･公表されているか

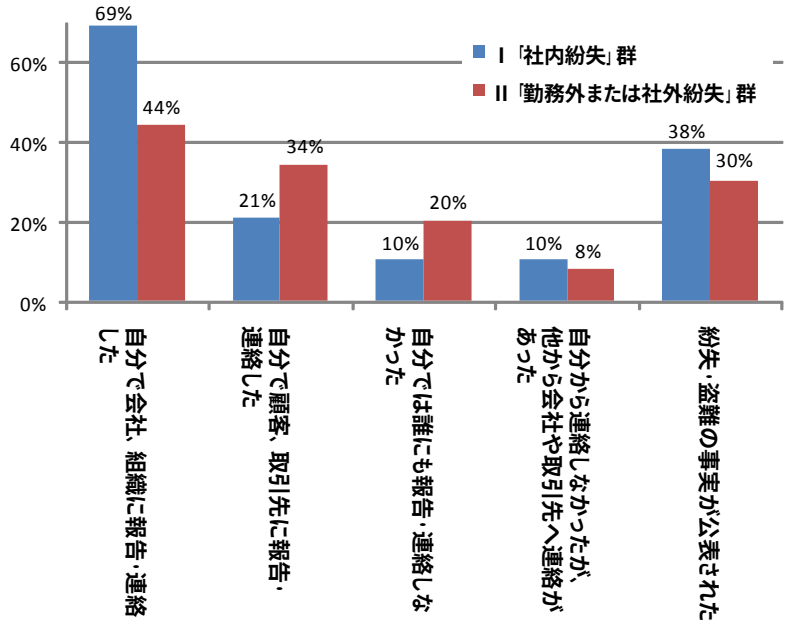

図 3.4-6：紛失の報告・連絡および公表をしたか

上図では Q5 の回答から､紛失したパソコンについて会社､組織への報告をしたかどうか､および会社、組織は紛失の事実を公表したかどうかについて、Ⅰ「社内紛失」群とⅡ「勤務外または社外紛失」群での分布を比較した。

「自分から会社、組織に報告・連絡した」という回答者の割合はⅠ群のほうがⅡ群に較べて多かった。このことからⅠ「社内紛失」群の事故の多くは、会社での棚卸しの結果としてパソコンが行方不明であること発覚する等、会社や組織に報告があがりやすいパターンの事故であろうことが推測される。

「自分で顧客、取引先に報告・連絡した」という回答者の割合は、Ⅰ群のほうがⅡ群よりも少なかった。また、紛失の事実が「公表された」割合がⅠ群のほうがⅡ群より多かった。これらの傾向は、紛失した本人から会社や組織に報告が上がっているため、会社や組織から顧客、取引先への報告・連絡および公表を行うことができているためと推測される。

3.4.5. 社内紛失のリスクについての考察

以上の分析結果から、勤務中に社内で紛失されるパソコンについては、以下の事柄が示唆される。

社内での紛失事故の発生頻度は飲酒時を上回る。また､社内で紛失したパソコンには顧客、取引先に関する情報などが入っている場合も多く、対策を検討すべき重要なリスクと考えるべきである。

また､社内で紛失するパソコンはセキュリティ対策があまり行われていない傾向があった。このことから、あまりセキュリティが意識されておらず、社内の管理が行き届いていない

パソコンが紛失しやすい傾向にあるものと思われる。また、社内でのパソコンの紛失は、会社や組織への報告・連絡がよく行われている傾向があることから、会社や組織が行う棚卸しなどの業務によって紛失が発覚しているものと思われる。

逆に言えば、資産の棚卸しなどが行われなければパソコンの紛失は発覚せず、誰にも気づかれないままひっそりと、多数のパソコンが紛失し続けている恐れがある。

パソコンを外部に持ち出した際の紛失は、本人が気づきやすい事故であるが、社内管理の不備による社内紛失は、定期的にきちんと棚卸しを行って管理を行わない限り発覚しにくい。

こうした紛失事故のリスクを抑えるためには、社外に持ち出すパソコンばかりに対策を集中するのではなく、社内使用のパソコンにも紛失・盗難対策を行き届かせ、定期的な棚卸しによる管理と意識の浸透に心がけることが必要と言える。

3.4.6. USB メモリの社内紛失について

なお、本節の分析はパソコンの社内紛失を対象に行ったが、今回の調査では USB メモリの社内紛失についても、ほぼ同様の分析結果が出ていることを補足しておく。

したがって、本節の考察はパソコンだけに限定されたものでなく、持ち運びが可能な情報機器や媒体全般について当てはまるものと思われる。

3.5. 私物利用よりも未報告が危ない

会社貸与品より私物の方がリスクは高いという仮説を立て、それを裏付けるために本アンケート結果から、携帯電話、PC、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ケースで「紛失した・盗難にあったことがある」「紛失しそうになったことがある」にチェックが入った回答を抽出し以下の分析を行った 。

a. 携帯電話、PC、USB メモリそれぞれの、「会社貸与」「私物」「両方所持」の割合
b. a で抽出したものの内、「対策なし」の割合
c. a で抽出したものの内、会社、組織または顧客、取引先に「報告・連絡した」の割合

3.5.1. 携帯電話の分析結果

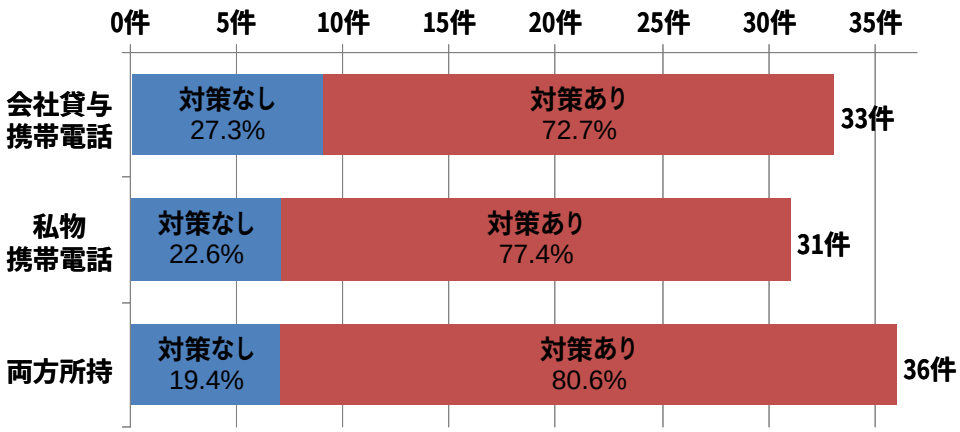

図 3.5-1：業務データ入り携帯電話の紛失・盗難と対策の割合

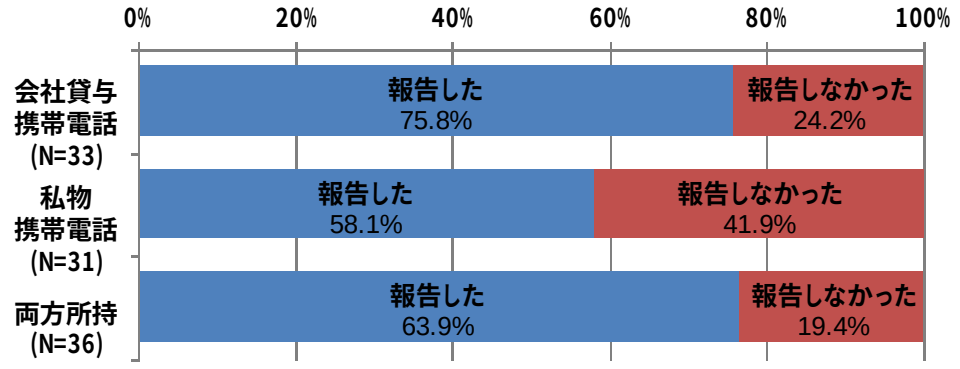

図 3.5-2：業務データ入り携帯電話の紛失・盗難と報告の割合

携帯電話は、私物の「対策なし（22.6%）」、「報告しなかった（41.9%）」の割合が高く、会社貸与よりリスクが高い傾向を示した。

3.5.2. パソコンの分析結果

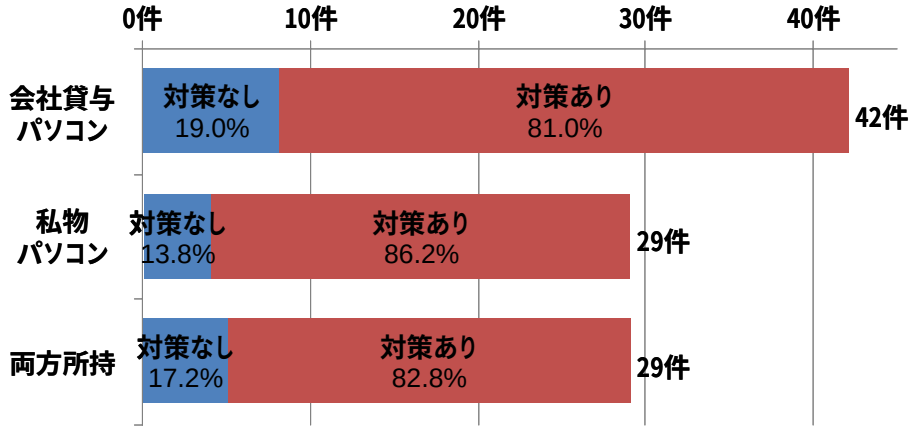

図 3.5-3：業務データ入りパソコンの紛失・盗難と対策の割合

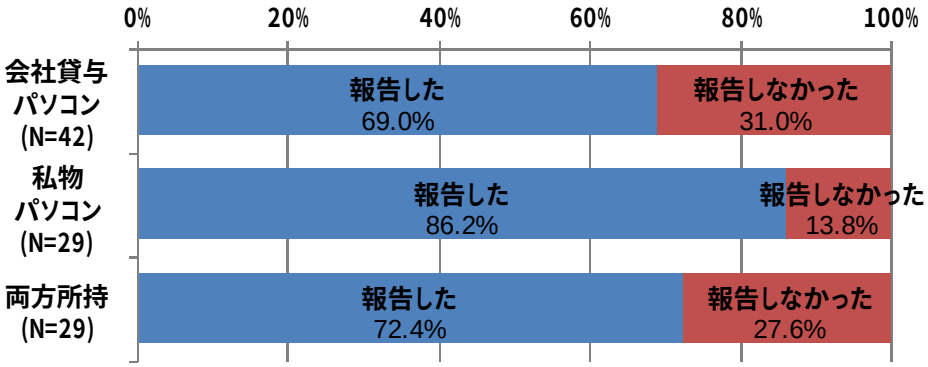

図 3.5-4：業務データ入りパソコンの紛失・盗難と報告の割合

パソコンは、私物の「対策なし（13.8%）」、「報告しなかった（13.8%）」の割合が特に高いとは言えない。 「報告した」割合は、私物が 86.2%と高い。

パソコンは、保存するデータ量が多く、紛失・盗難のインパクトが大きいため、報告する意識が高くなっている可能性がある。

3.5.3. USB メモリの分析結果

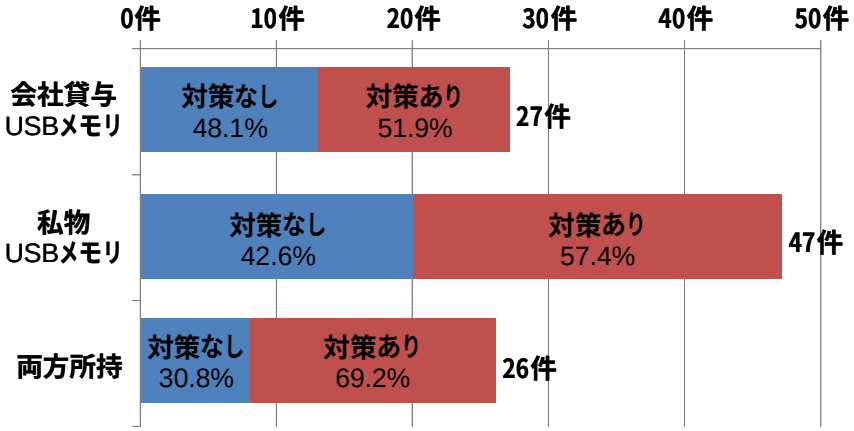

図 3.5-5：業務データ入り USB メモリの紛失・盗難と対策の割合

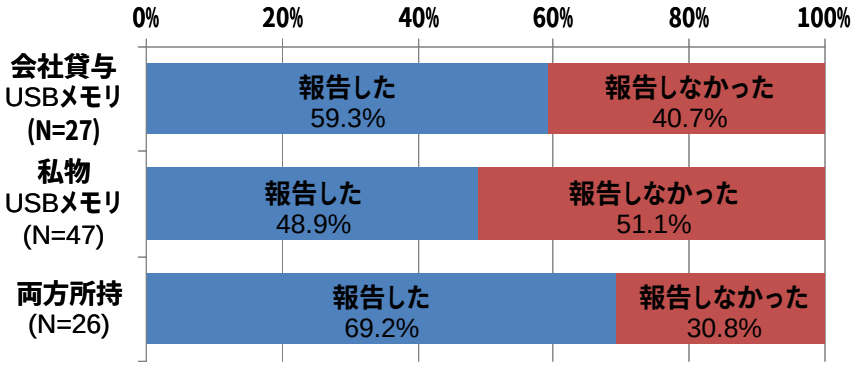

図 3.5-6：業務データ入り USB メモリの紛失・盗難と報告の割合

USB メモリは、私物のほうが紛失している割合が高い。紛失した USB メモリの 40%以上は、会社貸与、私物ともに対策されていない。

USB メモリは、私物の「報告しなかった（51.04%）」の割合が高く、リスクが高い傾向を示した。

ただし、会社貸与も私物も両方紛失した「両方所持」グループに着目すると「対策あり」と「報告した」の割合が高くなっている。今回のアンケートにおいては両方所持者が会社貸与と私物のどちらに対策を講じていてどちらに講じていなかったのか、また、どちらの紛失の際に報告したのかは分けてして集計できないため、「両方所持」グループの評価は今後の課題として保留しておきたい。

3.5.4. 私物を業務に使用するリスク

携帯電話、USB メモリにおいては、私物の方が会社貸与のものよりリスクが高くなる可能性を示したが、パソコンにはそのような傾向は見られなかった。

パソコンは紛失・盗難が発生した場合のインパクトが高いため、私物であっても報告する傾向にある可能性が考えられる。 あるいは、多くのケースで私物のパソコンを業務使用す

る場合は会社に届け出て承認を受ける手続きを取っている可能性もあり、その場合は報告する割合が増加するものと予想される。しかし、今回のアンケートではそれを裏付けるデータは取っていないため、想像の範囲を超えることはできない。

私物が会社貸与よりリスクが高いという相関を証明するためには、以下の検証も必要と考えられる。

- ルールの有無
  私物利用の容認やインシデント発生時の報告の義務など運用ルールが影響している可能性がある。
- 承認の有無
  私物利用の容認に加え、承認を受けて利用したのか未許可で利用したのかも影響する。未許可で利用した場合は、ルール違反を隠すため報告しなかった可能性がある。
- 実被害の有無
  今回は、「紛失した・盗難にあったことがある」という実際にインシデントが発生したケースと「紛失しそうになったことがある」というヒヤリハットのケースを混在したまま分析した。私物か会社支給かではなく、実際にインシデントが発生し実被害があったことが「報告した」に結びついている可能性がある。実被害があったケースとヒヤリハットのケースを分離した分析も必要である。

3.6. 公表率はどのくらいか

一般に、情報セキュリティの事故や事件（以下「インシデント」という。）が発生したとき、公表される場合と、公表されない場合がある。公表されるインシデントは氷山の一角である、ともいわれる。今回のアンケートでは、組織から公表されたかどうかを質問した。回答によれば、23%から 31% が公表されているという結果であった。これは、かなり大きい数字ではないかと思われる。そこで、この公表の比率について、考えてみたい。

表 3.6-1：今回の調査による公表率

	種類	公表率
1	携帯電話紛失	24%
2	パソコン紛失	31%
3	USB 紛失	23%
4	メール誤送信	27%
5	FAX 誤送信	27%

3.6.1. 公表率の分母

公表率を分母と分子に分けて考えてみる。まず、分母である。分母は対象として取り上げたインシデントになるが、ここには「公表すべきインシデント」と「公表の必要のないもの」が含まれていると考えられる。「公表すべきインシデント」には、例えば、次のようなものが挙げられる。

・すでに報道等で知られている
・被害が大きい
・被害者数が多い
・すべての被害者には連絡がとれていない
・二次被害の発生回避に役立つ
・類似インシデントの発生回避に役立つ

「公表の必要のないもの」は、ほぼ、上記の否定形になる。

・報道等で知られていない
・被害が小さい
・被害者数が少ない
・すべての被害者に連絡がとれている

・二次被害の発生回避に役立たない
・類似事案の発生回避に役立たない

なお、「公表の必要のないもの」には、次のように、インシデントに該当しないと考えられるものも含まれる。

・重要情報や個人情報が含まれていなかった
・短時間、行方不明であったが、その後、発見された
・短時間、手元を離れたが、その後、発見された。
・当該組織の管理対象でない

「公表すべきインシデント」と「公表の必要のないもの」の境界線は、報道の有無など、明確なものもあるが、被害の大小など、明確ではないものもある。分母として取り上げた事象の中に「公表すべきインシデント」以外のものも多く含まれていれば、公表率は小さくなる。その反対に、「公表すべきインシデント」以外のものが少なければ、公表率は大きくなる。今回のアンケートの結果から考えると、回答していただいた事象には、もともと「公表すべきインシデント」以外のものが少なかったのかもしれない。

3.6.2. 公表率の分子

次に、分子について考えてみる。分子は「実際に公表されたインシデント」ということになるが、「公表」という表現には、次のように、いくつかのレベルが考えられる。

・テレビ、新聞で報道された
・インターネット上のニュースサイトに掲載された
・自組織の公式ウェブサイトに掲載した
・自組織の受付等に掲示した
・関係組織に連絡した
・組織全体で公表した
・部門内で公表した

一般的には、「自組織の受付等に掲示した」以上のものを「公表」と呼び、組織全体や部門内での「公表」は「公表」とは呼ばないものと思われるが、今回のアンケートから考えると、「関係組織に連絡した」や「組織全体に対する公表」、「部門内の公表」も公表に含めてお答えいただいた人がいたのかもしれない。

3.6.3. A市の事例について

積極的にインシデントを公表している市（以下「A 市」とする。）がある。この A 市だけで 2009 年 1 月から 12 月の 1 年間に 194 件のインシデントを公表している。

表 3.6-2：A 市の職員数とインシデント公表数

職員数	職員数	公表件数	職員 10 万人あたりの公表件数
A 市	2 万 7579 名	194 件	703 件

この市を除く全国の都道府県、市町村の同時期のインシデントは、あわせて 305 件であった。

表 3.6-3：全国自治体の職員数とインシデント公表数

職員数	職員数	公表件数	職員 10 万人あたりの公表件数
都道府県	154 万 2705 名	103 件	6.7 件
指定都市（A 市以外）	21 万 7224 名	202 件	17.0 件
市町村	97 万 1173 名		
合計	273 万 1102 名	305 件	11.2 件

（注）職員数は、総務省の地方公務員団体定員調査の 2009 年のデータによる
公表件数は、JNSA の調査結果による

仮に、インシデントの比率が職員数に比例すると仮定し、さらに A 市以外の全国の自治体でも A 市と同程度の頻度でインシデントが発生したと仮定する場合、あわせて 1 万 9211 件のインシデントが発生していたことになる。

推定インシデント発生数　＝ 194 件 × 273 万 1102 名／2 万 7579 名
＝ 1 万 9211 件

上記のように推定したインシデント数と実際に公表されたインシデント数から、推定される公表率は次のようになる。

推定公表率 ＝ 305 件／1 万 9211 件 ＝ 1.6%

この割合は、約 60 件に 1 件しか公表されていないことになり、今回のアンケート結果に比べてかなり低い数字である。A 市は、他の地方自治体に比べて、積極的に公表しているだけであり、インシデントが頻発しているとは考えにくい。したがって、一般の都道府県、

市町村は、公表することに対して消極的であるものと思われる。

3.6.4. プライバシーマーク取得事業者の事例について

プライバシーマークを取得している事業者（組織）は、個人情報に関するインシデントが発生すると、日本情報処理開発協会（JIPDEC）等に報告する義務がある。平成 21 年度（平成 21 年 4 月～平成 22 年 3 月）の統計によれば、報告件数は 624 件であった。また、JNSA の調査によって、同時期にインシデントを公表した事業者のうち、プライバシーマークを取得している事業者、あるいは、インシデントの公表後 1 年以内にプライバシーマークを取得した事業者は、51 件であった。なお、複数のインシデントが発生している場合は、重複を除いた件数とした。

表 3.6-4：プライバシーマーク取得業者のインシデントの件数

種類	インシデントの件数
JIPDEC に報告された件数	624 件
公表された件数	51 件

（注）「JIPDEC に報告された件数」は、JIPDEC の報告書による。
（参考）http://privacymark.jp/reference/pdf/H21JikoHoukoku_100712.pdf
「公表された件数」は、JNSA の調査結果による

プライバシーマーク取得事業者が日本情報処理開発協会（JIPDEC）等に事故報告をした件数と公表されたインシデントの件数から、推定される公表率は次のとおりである。

51 件／624 件 ＝ 8.2%

これは、一般的な地方自治体に比べれば高いものの、今回のアンケート結果に比べると、低い数字である。約 12 件に 1 件しか公表されていないことになる。JIPDEC に対しては、個人情報が 1 件でも含まれていれば報告することになっているため、報告件数が多いものと思われる。その一方で、公表の必要性が低いものは、報告はしても公表しないと判断しているものと思われる。

公表率については、アンケート結果と、地方自治体、プライバシーマーク事業者の事例でかなり開きのある数字が出てきた。今後の調査では、公表率を左右する条件について掘り下げてみたい。

4. まとめ

今回の調査結果を踏まえ、JNSA インシデント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. 組織はインシデントを把握せよ

今回の調査で、インシデントの種類にもよるが、実際に発生しているインシデントのうち、本人から組織に事実を伝えたインシデントは約半分にすぎず、また、組織が事実を把握しても公表に至るのはさらにその半分、全体の 4 分の 1 程度にすぎないことが確認された。

インシデントの内容によっては公表する必要のないものもあるが、組織としては、少なくともリスクの高いインシデントはすべて把握すべきである。その上で、インシデントの発生原因や傾向などを分析し、必要に応じて対策を講じることによって、将来のインシデントの発生を効果的に防止することができる。実態を知らずに場当たり的に対策を講じても、効果的な対策であるかどうかは疑問である。なお、二次的被害や類似インシデントの発生防止のために必要な場合は、公表も行う必要がある。

インシデントを把握する一つの方法として、当事者本人が容易に報告できるような環境を整備することが考えられる。単に、報告せよと言うだけでは、自分に不利な報告はなかなか上がってこないものである。例えば、報告してもペナルティを課さない、速やかに自発的に報告すれば軽い処分にする、報告が遅れた場合や、報告がない場合は重い処分にする、虚偽の報告を行った場合は厳罰にするなど、報告を促進する仕組みを整備する必要がある。また、報告を受ける側には、的確な初期対応が実施できる人材を配置すべきである。報告を受けても、真摯に対応しないでいると、報告が上がってこなくなる。

インシデントを把握するもう一つの方法は、モニタリング（監視）を行うことである。電子メールの全文を保存しておき、ランダムに選んで内容を確認するとか、業務に関係ないようなキーワードで抽出する、許可されていない機器を接続したら検出する、ダウンロードしたファイル名のログを残しておく、などの方法がある。ただし、最初からモニタリングに多額の投資をすることはあまり推奨できない。次のような順序で徐々にモニタリングの段階を高めてゆき、抑止効果が得られたら、その段階を維持することを推奨する。

- 第一段階：　モニタリングしていることを社内に公表する
- 第二段階：　モニタリング結果を部分的に公表する
- 第三段階：　モニタリング結果に基づいて処分する

なお、モニタリングを実施していることは社内に公表すべきであるが、何をどこまでモニタリングしているのかについては、伏せておいたほうが手の内を知られなくてよい。モニ

タリングしていることを公表するだけで、かなりの牽制効果が期待できる。

そろそろ、インシデントが発生することが「とんでもない」ことであるという認識からは脱却したほうがよいと考える。故意に情報を漏洩するとか、情報を破壊するなどの行為は厳罰に処するほかないが、過失や不注意、軽微な違反であれば、インシデントの影響度に見合った処分でよいのではないか。インシデントの発生を少なくしようとして、些細なインシデントでも厳罰にしてしまうと、インシデントが報告されなくなり、重大なインシデントが防止できなくなるおそれがある。インシデントはないほうがよいが、一定の確率で発生するものである、というインシデントの発生を前提とした考え方に立脚したほうがよいと考える。

4.2. 必要なら、携帯電話やＰＣは支給せよ

インシデント防止の観点からは、個人所有の携帯電話や PC を業務に使用することは推奨できない。第一の理由は、個人所有であると、管理も個人まかせになるためである。例えば、個人所有の携帯電話をセキュリティ機能の高いものに買い換えたり、個人所有の PC のウイルス対策ソフトを高性能のものに変更したりすることは、なかなか強制できない。第二の理由は、刑事責任に問えなくなる可能性が高いためである。日本には情報窃盗罪がないので、個人所有の機材に情報をコピーされて持ち出された場合には、窃盗罪は成立しない。

個人所有の携帯電話や PC を業務に使用することを完全に禁止できるのであれば、それが最も簡単な解決方法である。しかし、業務上どうしても必要な場合は、完全に禁止しても個人所有のものを隠れて使用する人が出てくるものである。禁止していないときよりも、隠れて使用されているときのほうが危険である。完全に禁止できない場合は、許可を得れば使用できることとし、その代わりに、セキュリティ機能やウイルス対策ソフトを整備してもらうのがよい。しかし、もっとよい方法は、携帯電話や PC を組織として支給することである。

インシデントに遭遇しやすいタイプの、いわゆるおっちょこちょい（3.3 項参照）の従業者に対しては、機密情報を扱わない仕事に従事してもらうのが一番よい。やむを得ず、携帯電話や PC を業務で使用する場合は、紛失しても情報が漏れないよう、セキュリティ機能のある携帯電話や、シンクライアント型の PC を優先的に配布するのがよい。

4.3. FAX、メールは、事故前提で使おう

FAX 誤送信や電子メール誤送信のインシデントの発生確率は、一人当たり年間で約 40%とかなり高い。電話であれば、最初のやり取りで相手を確認するため、間違い電話を掛けてしまっても、情報漏えい以前に間違い電話であることに気が付く。しかし、FAX で番号を間違えた場合、その番号がたまたま電話回線ではなく FAX 回線であれば、そのまま相手先に届いてしまう。電子メールも、メールアドレスの綴りを間違え、そのアドレスがたま

たま存在していれば、そのまま相手先のメールボックスに入ってしまう。また、アドレス帳からの選択を間違えると、有効なメールアドレスなので、そのまま別人に届いてしまう。このような理由から、そもそも、FAX や電子メールは危険な通信手段であると考えたほうがよい。

絶対に間違わない、インシデントが発生しないという前提で考えると、かえって危険である。間違いは絶対に発生しないものではなく、一定の確率で発生するものである。そして、FAX や電子メールでは、1 つの間違いが、そのままインシデントに結びつく可能性が高い。また、間違いが起こらない、インシデントが発生しないという前提で考えると、電子メールの本文に機密情報を記載しても問題ないなどと考えてしまうかもしれない。むしろ、間違いが起こるかもしれない、インシデントが発生するかもしれないという前提で考えることが必要である。インシデントを前提として考えると、機密情報は暗号化してから電子メールに添付するとか、FAX では機密情報を送信しない、FAX 以外の通信手段を使用するなどの対策を講じるようになるのではないだろうか。

5. 付録:単純分析

5.1. 携帯電話

5.1.1. 予備調査の分析結果

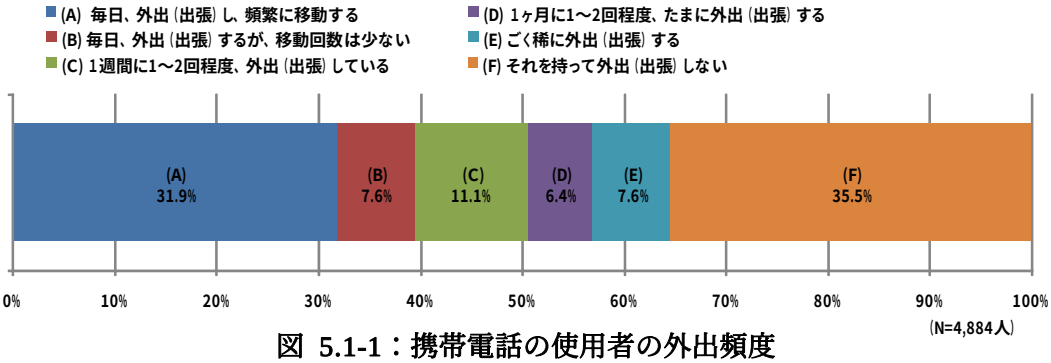

図 5.1-1：携帯電話の使用者の外出頻度

仕事をしている人、約 5000 人への調査によると、業務で携帯電話を使い頻繁に外出する人が約 1/3、ほとんど外出しない人が 1/3。日本のビジネス環境において、外出する際に携帯電話を使わないことはほとんど考えられないことから、業務上頻繁に外出する人の割合が約 1/3、ほとんど外出しない人が 1/3 と読み替えても差し支えないと考えられる。

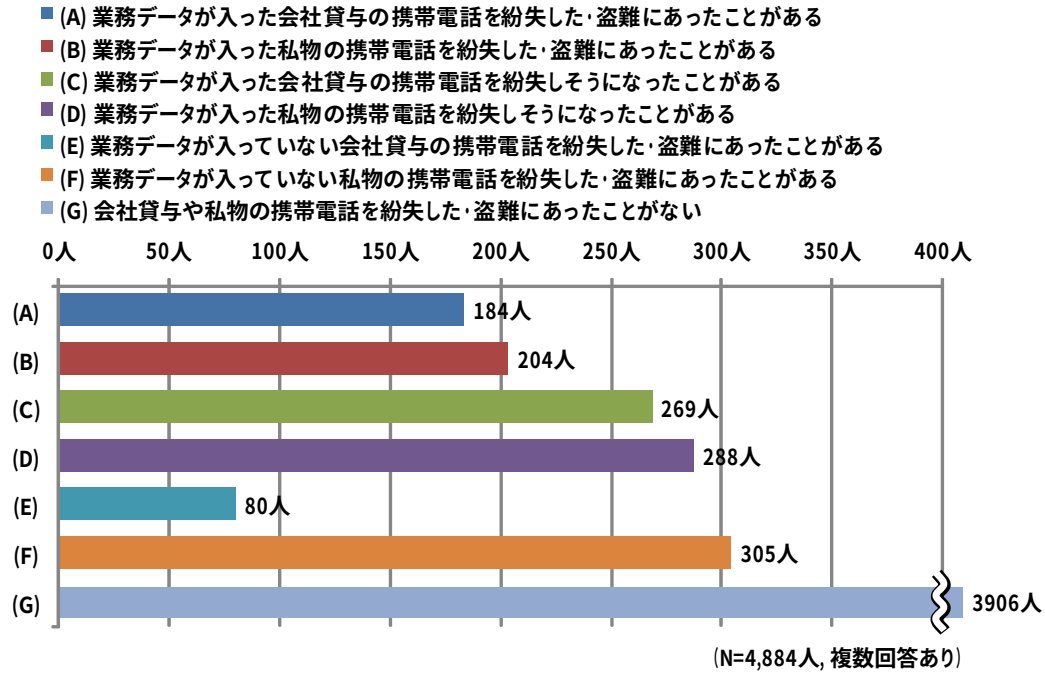

図 5.1-2：携帯電話の紛失・盗難の経験

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、978 人（約 20%）である。会社携帯をなくしたこと、およびなくしそうになったことがある人は 9.1%、うち、会社携帯をなくしたことがある人は 4.8%である。私物携帯をなくしたこと、なくしそうになったことがある人は 14.3%、うち、私物携帯をなくしたことがある人は、9.7%。

5.1.2. 本調査の分析結果

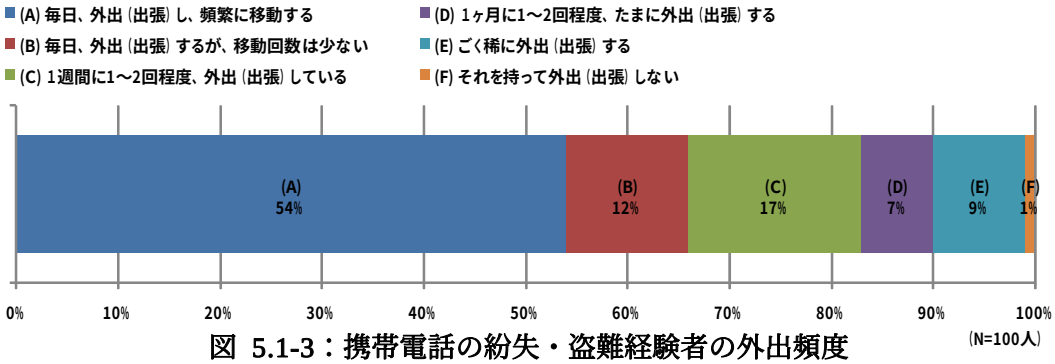

図 5.1-3：携帯電話の紛失・盗難経験者の外出頻度

仕事をする人、約 5,000 人を対象とした調査では、「業務において毎日、外出（出張）し、頻繁に移動する」人の割合は 39.9%であった。携帯電話を紛失した 100 人を対象とした本調査では、携帯電話を無くしたことがある人のうち、「業務において毎日、外出（出張）し、頻繁に移動する」人は 54%と最も高い。また、同様に「それをもって外出（出張）しない」の割合は 1.0%であった。以上のことから、携帯電話の紛失・盗難に関しては、外出（出張）の頻度が大きく影響していることが分かる。

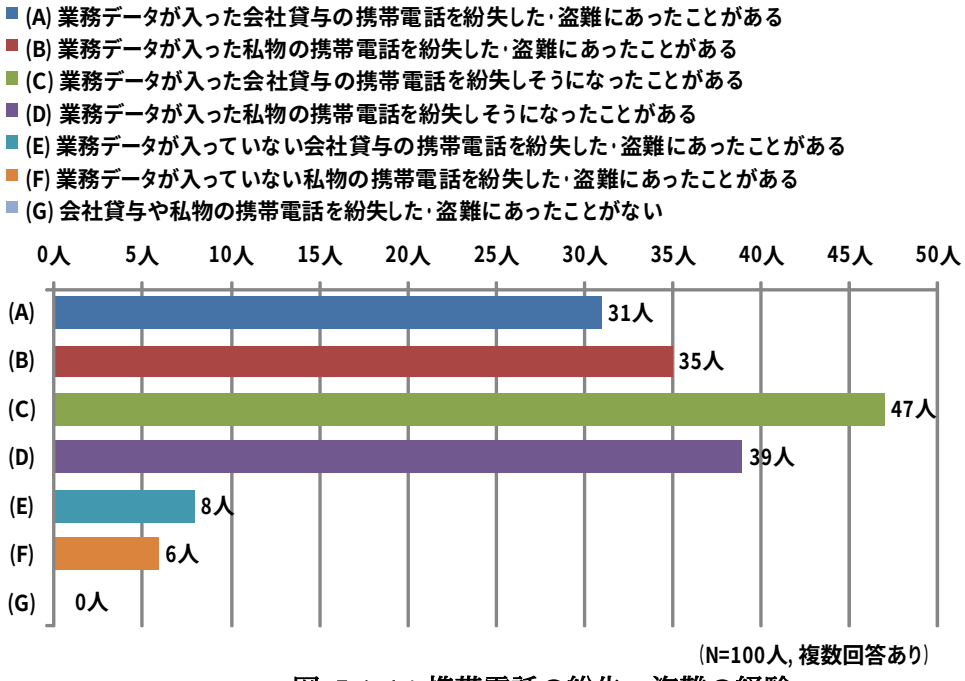

図 5.1-4：携帯電話の紛失・盗難の経験

業務データが入っていない携帯電話を無くした人は、のべ 14 人（12%）。うち 2%は同じ人が重複して紛失している。それ以外の紛失・盗難にあった携帯電話は、なんらかの業務データが入っていたことになる。業務データが入った携帯電話を、紛失・盗難したことがある人の割合は、会社貸与の携帯電話（31%）より、私物の携帯電話（35%）の方が多い。いまだに多く人が個人の携帯を業務に使っており、その中に業務データが含まれている状況が伺える。

一方、なくしそうにったケースにおいては、会社貸与の携帯電話の方が多くなっている。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。

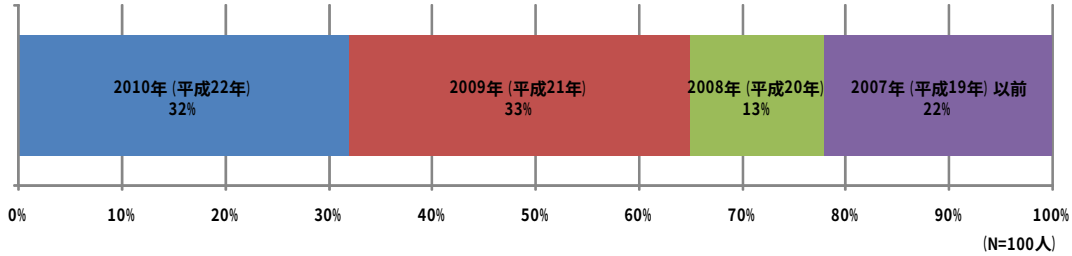

図 5.1-5：携帯電話の紛失・盗難の経験時期

携帯電話を紛失した年を一つ選択させる設問であることから、紛失した直近の年を選んでいる。紛失してから時間が経った場合、記憶があいまいになることから、2009 年、および 2010 年の紛失確率から、100 人中 1 年間で約 30 人が無くしたもしくは失くしそうになったものと考えられる。業務データありの携帯電話を紛失した、もしくは紛失しそうになった割合が全体で 18%であることから、毎年 6%程度の携帯電話が紛失・盗難の危機にあっていると考えられる。

本データは、2010 年 10 月中旬時点において取得したデータであるため、2010 年 1 年間に紛失や盗難、誤送信を行った人数は、やや少ない値であることが予想される。

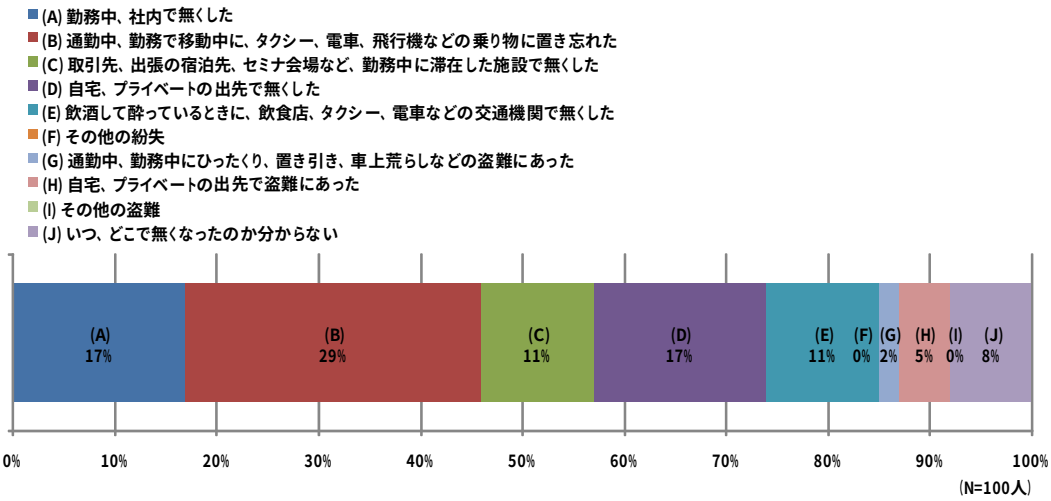

図 5.1-6：携帯電話の紛失・盗難の状況

紛失・盗難が発生した状況としては、「乗り物に置き忘れた」が 29%と一番多く、次いで、「勤務中、社内で無くした」「自宅、プライベートの出先で無くした」が 17%である。「勤務中、社内で無くした」が 17%あるが、これは原因が紛失と盗難のどちらか判断できないために紛失という扱いになっている可能性が考えられる。盗難については、勤務中、プライベート合わせて 7%しかなく、明らかに盗難にあったと判断できるケース以外は、紛失としてとらえられているものと考えられる。

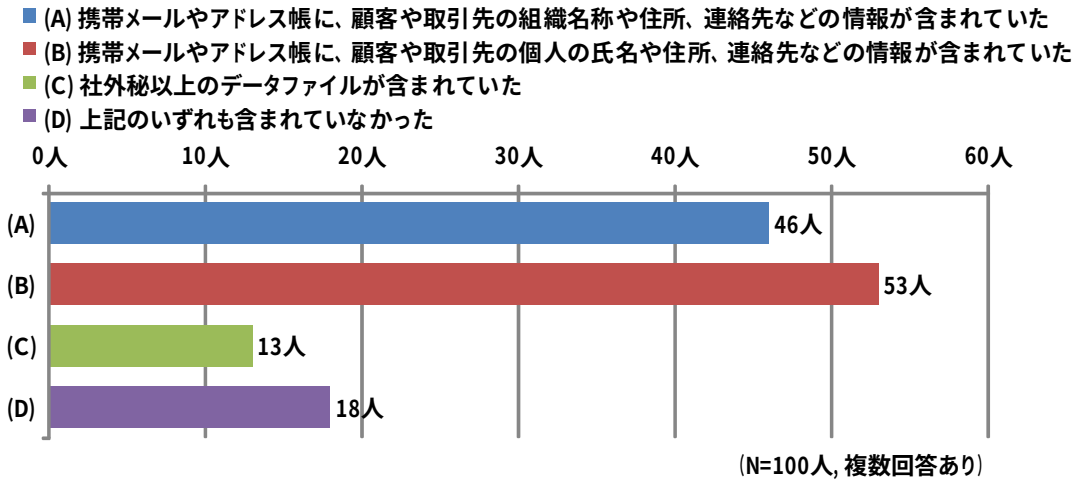

図 5.1-7：紛失・盗難された携帯電話に含まれる情報

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 82 人であった。つまり、紛失した携帯電話には、多くのケース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。私物携帯でも、企業の情報が入っていることが多い。

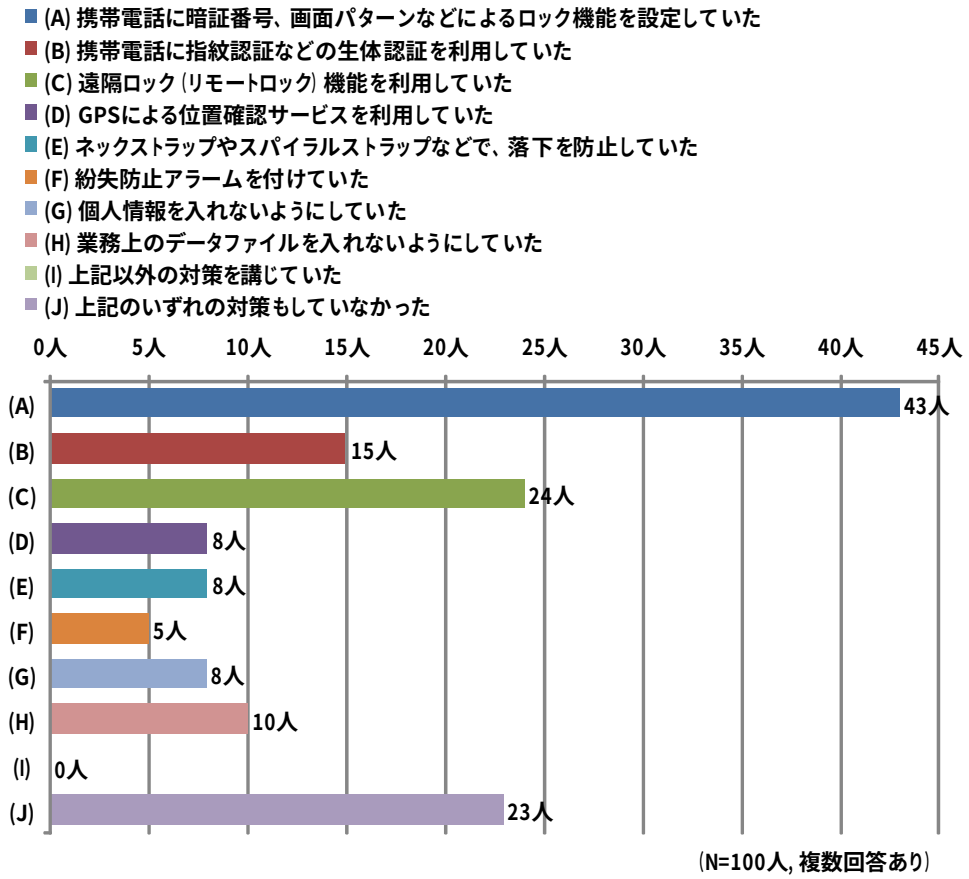

図 5.1-8：携帯電話の盗難・紛失対策

携帯電話を紛失した 100 人においては、盗難・紛失事故への事前対策は、「ロック機能」（43 人）が最も多い。ただし、ロック機能へ設定したパスワードの文字数が少ない場合は簡単に解除できてしまうことから、リモートロック機能、GPS による位置確認などの併用が望まれる。

盗難・紛失に対する物理的な対策である「落下防止」、「紛失防止アラーム」を対策していた割合が低い。これは、そもそもその対策をしている人が少ない可能性と、対策によって紛失を防止されたため割合が低い可能性がある。しかし、これらの対策を施していても100%の事故防止は不可能なことが分かる。

また、「いずれの対策もしていない」が 23 人も存在することから、紛失・盗難にあった携帯電話に含まれる業務データは無防備な状態であることが伺える。

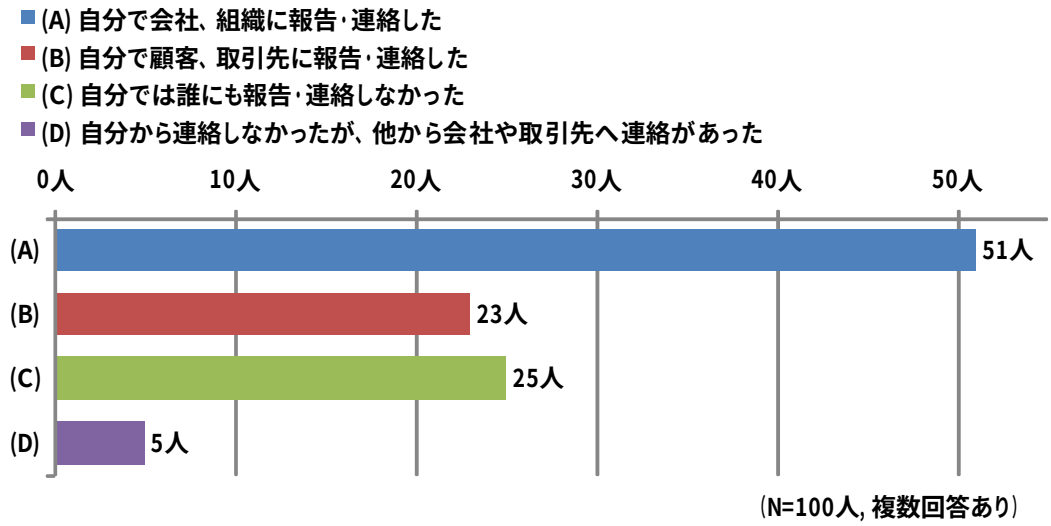

図 5.1-9：携帯電話の盗難・紛失の報告

「自分で会社、組織に報告・連絡した」は、100 人中 51 人と約半数であった。残り約半数の携帯電話の紛失は報告されておらず、「自分では誰にも報告・連絡しなかった」と回答した人も 25 人であった。よって、会社、組織が、業務データを含んだ携帯電話の紛失・盗難を把握できていない場合が、少なからず存在する。携帯電話は保有者情報がわかることから、「他から会社や取引先に連絡があった」場合も回答があった。外部から連絡をもらう前に、自発的に報告・連絡する組織文化の醸成が必要と考える。

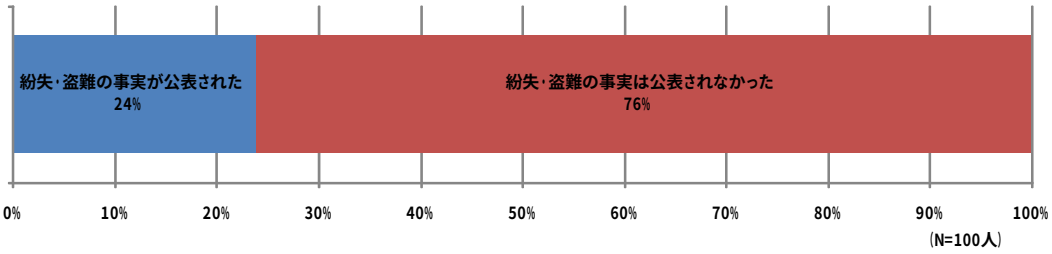

図 5.1-10：携帯電話の盗難・紛失の公表

「会社、組織が携帯電話の紛失・盗難を認識している」割合が 75%程度と考えられるが、そのうち「紛失・盗難の事実が公表された」場合は 24%であった。

5.2. パソコン

5.2.1. 予備調査の分析結果

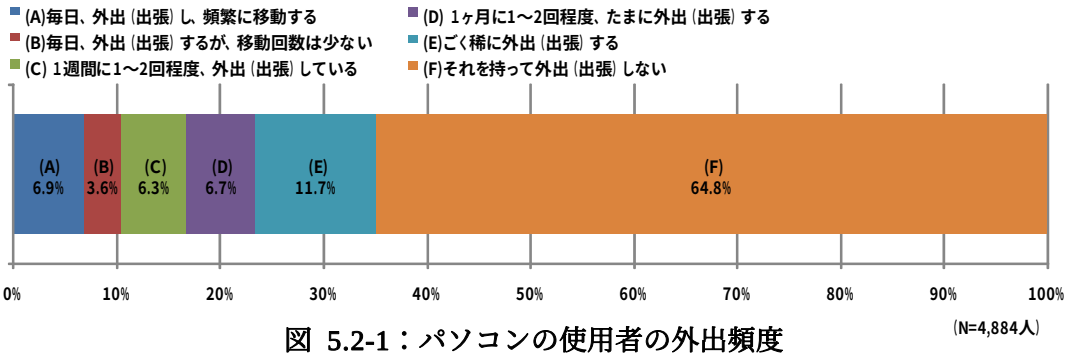

図 5.2-1：パソコンの使用者の外出頻度

仕事をしている人、約 5000 人への調査によると、パソコンの持ち出し状況は、携帯電話とは異なり、「毎日、外出（出張）し、頻繁に移動する」割合が 6.9%と少なく、「外出（出張）しない」が 64.8%と多数を占めた。

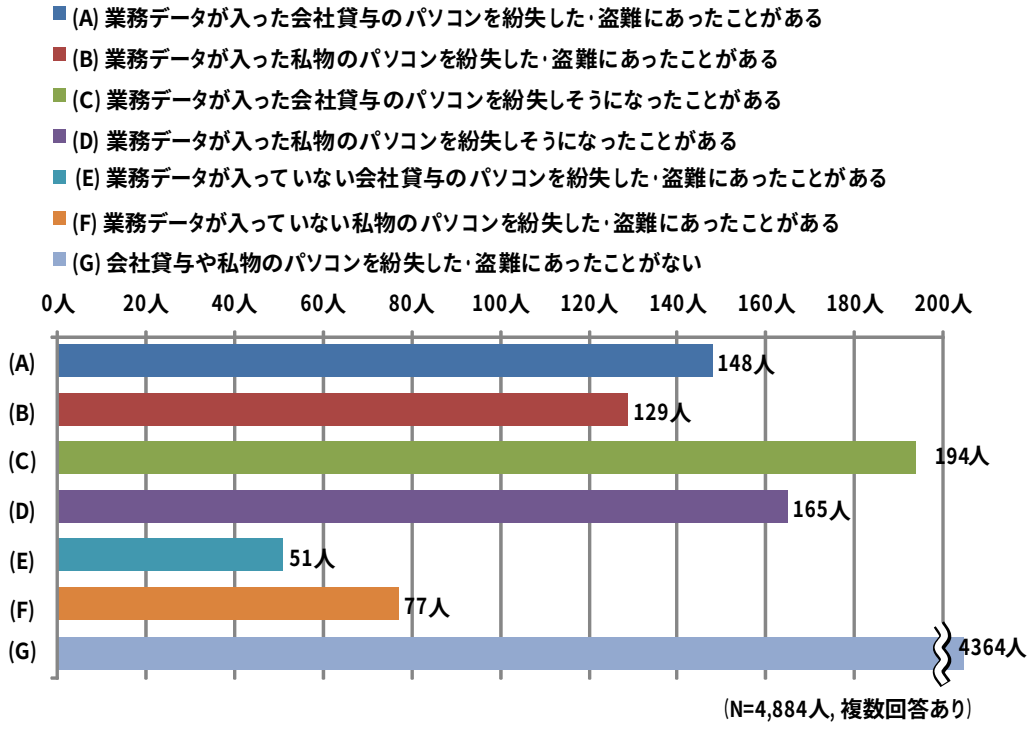

図 5.2-2：パソコンの紛失・盗難の経験

私物、会社貸与のパソコンを問わず、パソコンをなくしたこと、なくしそうになったことがある人は 520 人（10.6%）であった。

5.2.2. 本調査の分析結果

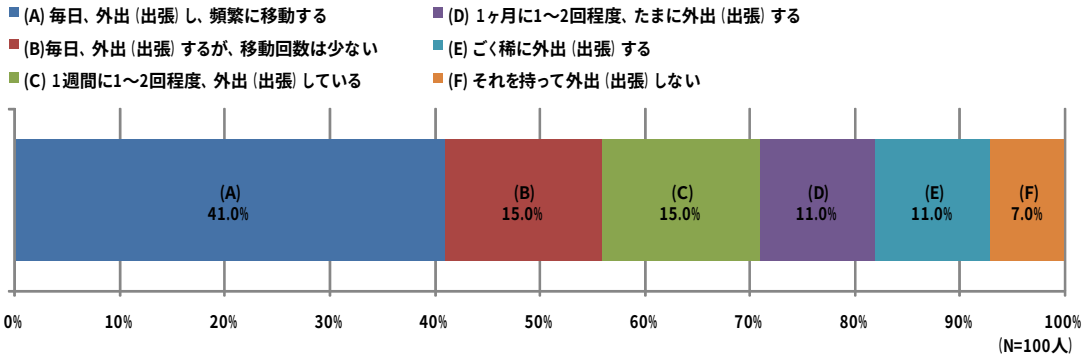

図 5.2-3：パソコンの紛失・盗難経験者の外出頻度

仕事をする人、約 5,000 人を対象とした調査では、「業務において毎日、外出（出張）し、頻繁に移動する」人の割合は 6.9%であった。パソコンを紛失した 100 人を対象とした本調査では、「業務において毎日、外出（出張）し、頻繁に移動する」人は 41%であった。また、同様に「それをもって外出（出張）しない」の割合は、7.0%であった。

以上のことから、パソコンの紛失・盗難に関しても、外出（出張）の頻度が大きく影響していることが分かる。ただし、社内でのパソコンの紛失も多いことから、「外出が多いこと」と「パソコンの紛失・盗難」に直接の因果関係があるとは限らない。

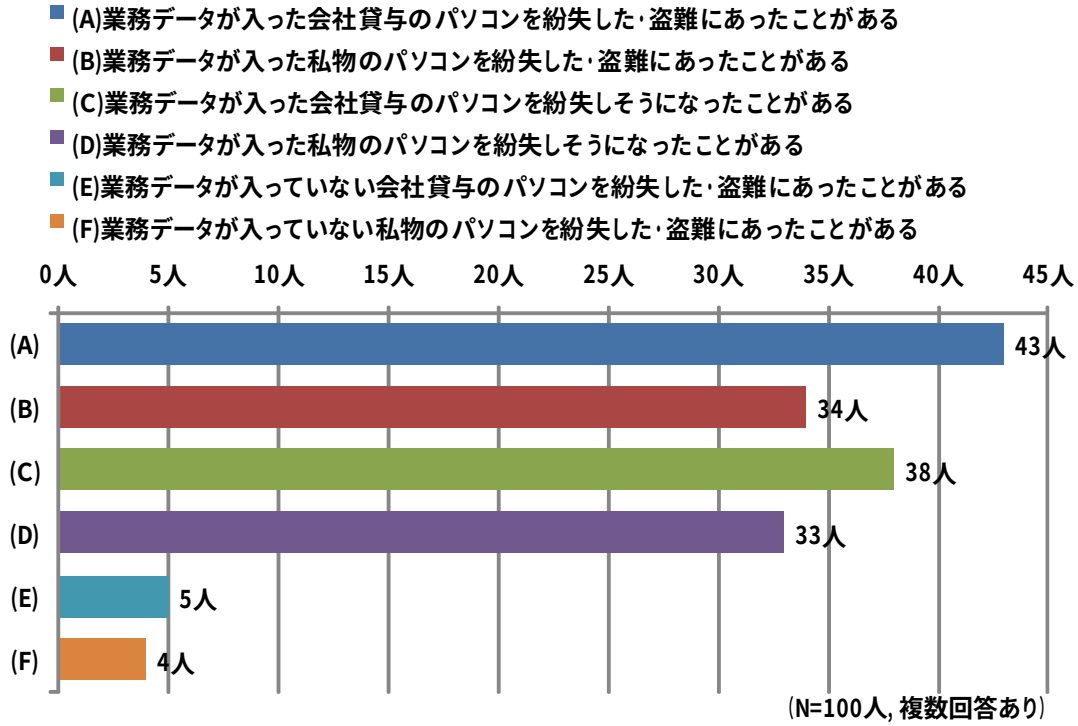

図 5.2-4：パソコンの紛失・盗難の経験

業務データが入っていないパソコンを無くした人は、のべ 9 人（8%）。うち 1%は同じ人が重複して紛失している。それ以外の紛失・盗難にあったパソコンは、なんらかの業務データが入っていたことになる。業務データが入ったパソコンを、紛失・盗難したことがある人の割合は、会社貸与パソコン（43%）、私物パソコン（34%）である。いまだに多く人が個人のパソコンを業務で使用しており、その中に業務データが含まれている状況が伺える。

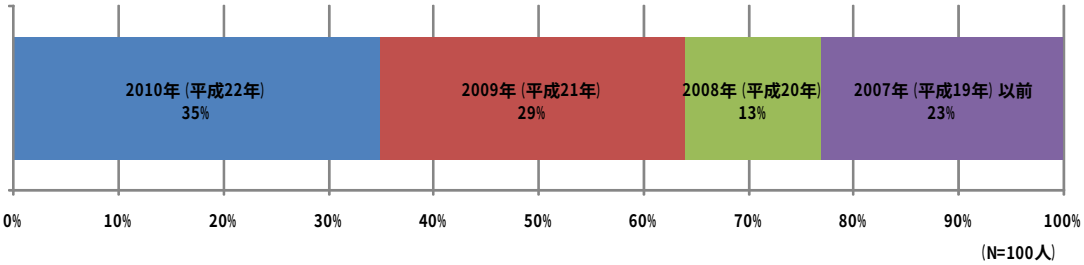

図 5.2-5：パソコンの紛失・盗難の経験時期

パソコンを紛失した年を一つ選択させる設問であることから、紛失した直近の年を選んでいる。1 年で約 3 分の 1 の人が無くした、もしくは無くしそうになったものと考えられる。

業務データありのパソコンが紛失・盗難にあった割合は、全体で 12.4%であることから、毎年 4%程度のパソコンが紛失・盗難の危機にあっていると考えられる。

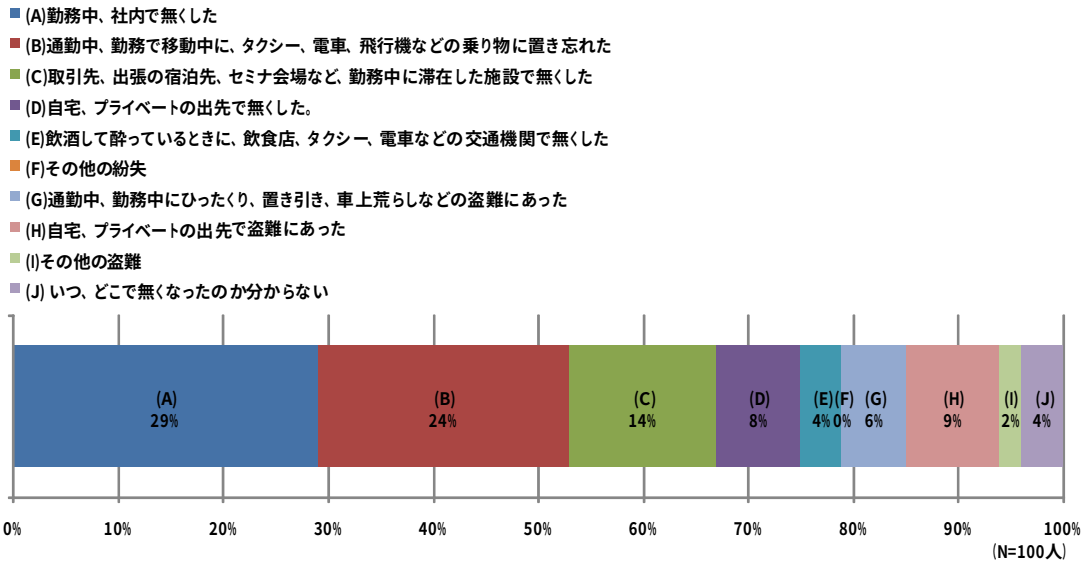

図 5.2-6：パソコンの紛失・盗難の状況

意外な結果として、紛失・盗難が発生した状況の内、「勤務中、社内で無くした」が 29%

と一番多かった。これらの理由としては、資産管理上の不整合、部署異動時や廃棄時の管理漏れ、盗難とは断定できない紛失など様々な理由が含まれると考えられる。ついで多いのが、「乗り物に置き忘れた」の 24%で「飲酒後の交通機関での紛失」4%と合わせ 28%と移動中の紛失も多いことが伺える。

盗難については、勤務中、プライベート合わせて 15%ほどで、明らかに盗難にあったと判断できるケース以外は、社内も含め紛失としてとらえられているものと考えられる。

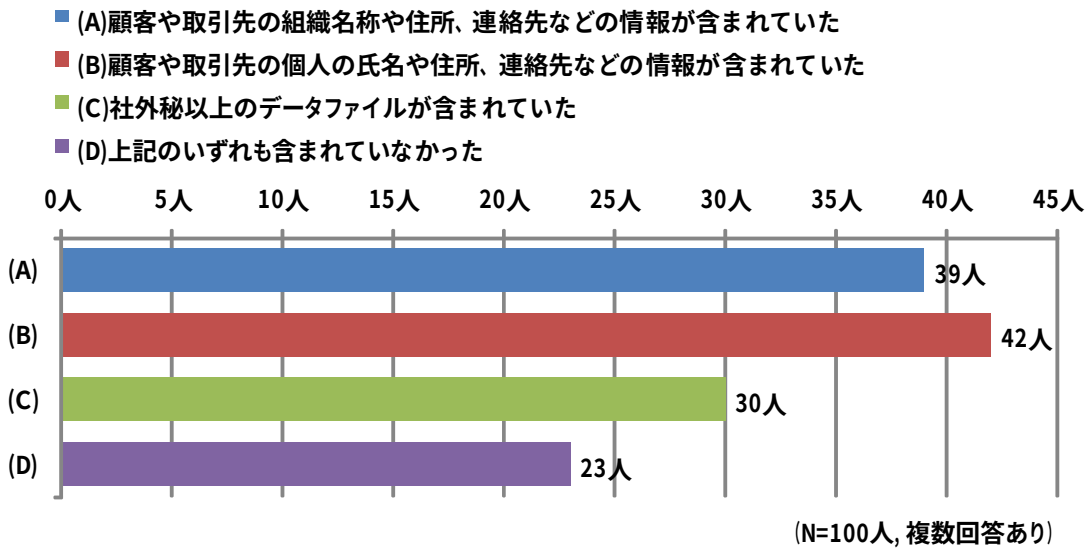

図 5.2-7：紛失・盗難されたパソコンに含まれる情報

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等が含まれていた場合は 77 人であった。つまり、紛失したパソコンには、多くのケースでなんらかの保護すべき情報が含まれていたことが分かる。「社外秘上のデータファイル」が含まれていた場合は 30 人あり、携帯電話の 13 人と比べ、その特性から、組織にとってよりリスクの高いものであることが分かる。

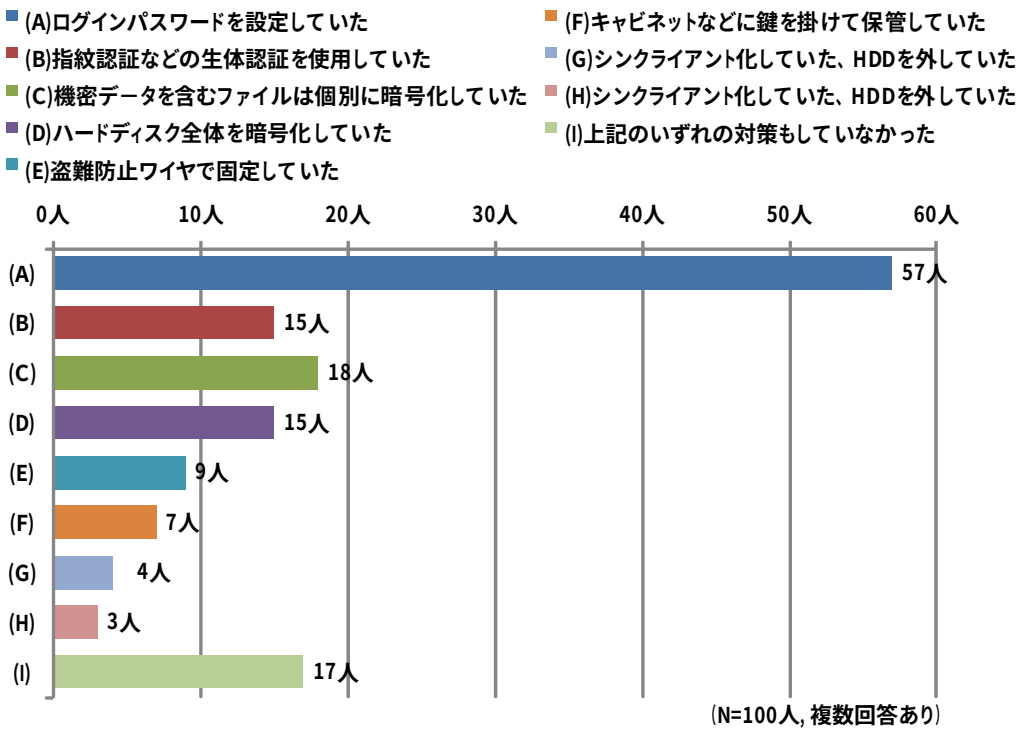

図 5.2-8：パソコンの盗難・紛失対策

盗難・紛失に対する物理的な対策として、「ワイヤで固定」（9 人）、「キャビネットで施錠」（7 人）などがあるが、これらの対策をしていても紛失・盗難にあった、あいそうになった人は、大部分が勤務外・社外での紛失・盗難であった。これらの対策を施していても、その対策の対象外となった場合に、紛失・盗難が発生している。

盗難・紛失事故への事前対策として、「ログインパスワードの設定」（57 人）、「個別ファイルの暗号化」（18 人）、「生体認証」（15 人）、「ハードディスクの暗号化」（15 人）、「シンクライアント化」（4 人）などがある。ただし、ログインパスワードの設定だけであれば、CD ブートや、ハードディスクの抜き出しにより、データへのアクセスが出来てしまうことから、ファイル暗号化などの実質的に有効な対策との併用が望まれる。

また、「いずれの対策もしていない」が 17 人も存在することから、デスクトップＰＣを含め、さらなる紛失・盗難への対策が望まれる。

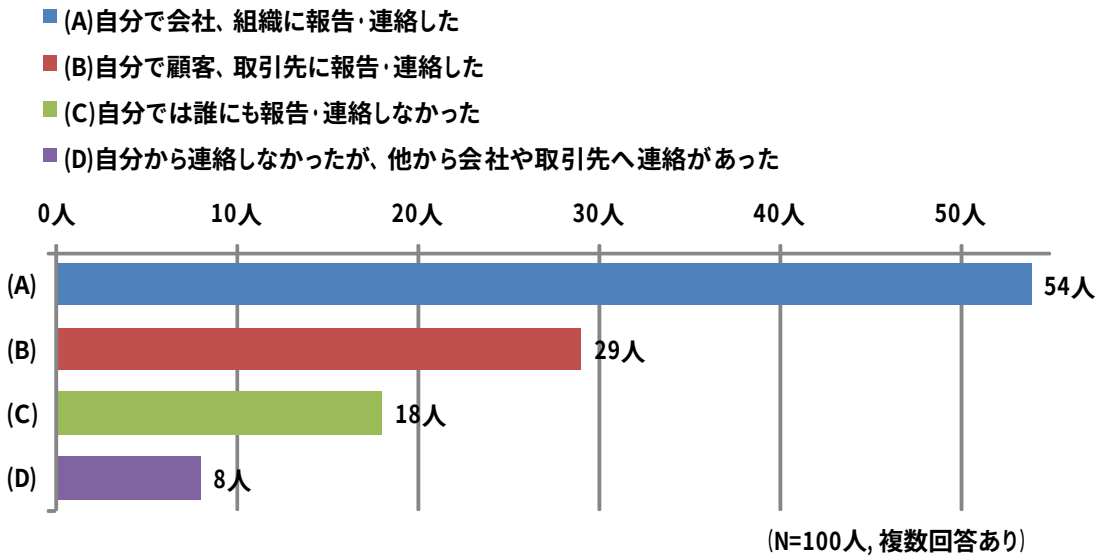

図 5.2-9：パソコンの盗難・紛失の報告

「自分で会社、組織に報告・連絡した」は、100 人中 54 人と半数を占めている。一方で、「自分では誰にも報告・連絡しなかった」と回答した人が 18 人であった。よって、会社、組織がパソコンの紛失・盗難を把握できていない場合が、少なからず存在する。「他から会社や取引先に連絡があった」場合も 8 人あった。外部から連絡がある前に、自発的に報告・連絡する組織文化の醸成が必要と考える。

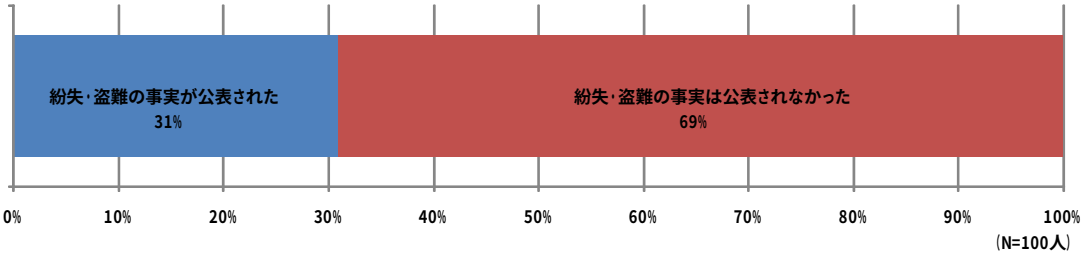

図 5.2-10：パソコンの盗難・紛失の公表

「会社、組織が携帯電話の紛失・盗難を認識している」割合が 82%程度と考えられるが、そのうち「紛失・盗難の事実が公表された」割合は 31%であった。

5.3. USB

大容量化と小型化が進み、持ち運びやすくなった一方で、USB メモリからの情報漏えい事故が起きている。そこで、USB メモリによる情報漏えい動向の調査を実施し、使用状況や格納情報と情報漏えい事故との因果関係を調査した。この調査により、企業が USB メモリの使用を許可する際に留意すべきポイントを洗い出したい。

5.3.1. 予備調査の分析結果

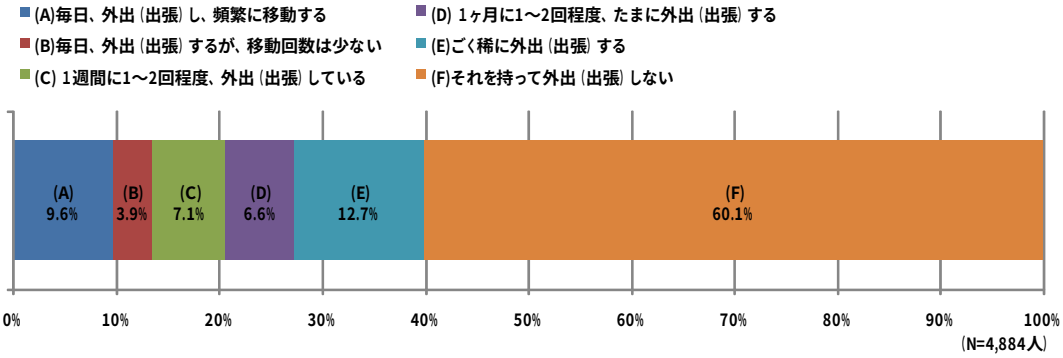

図 5.3-1：USB メモリの使用者の外出頻度

仕事をしている人、約 5000 人への調査によると、USB メモリの持ち出し状況は、「毎日、外出（出張）し、頻繁に移動する」割合が 9.6%と当WGの想定よりもかなり少なく、「外出（出張）しない」が 60.1%と多数を占めることがわかった。業務では USB メモリをあまり持ち歩かないことが伺える。

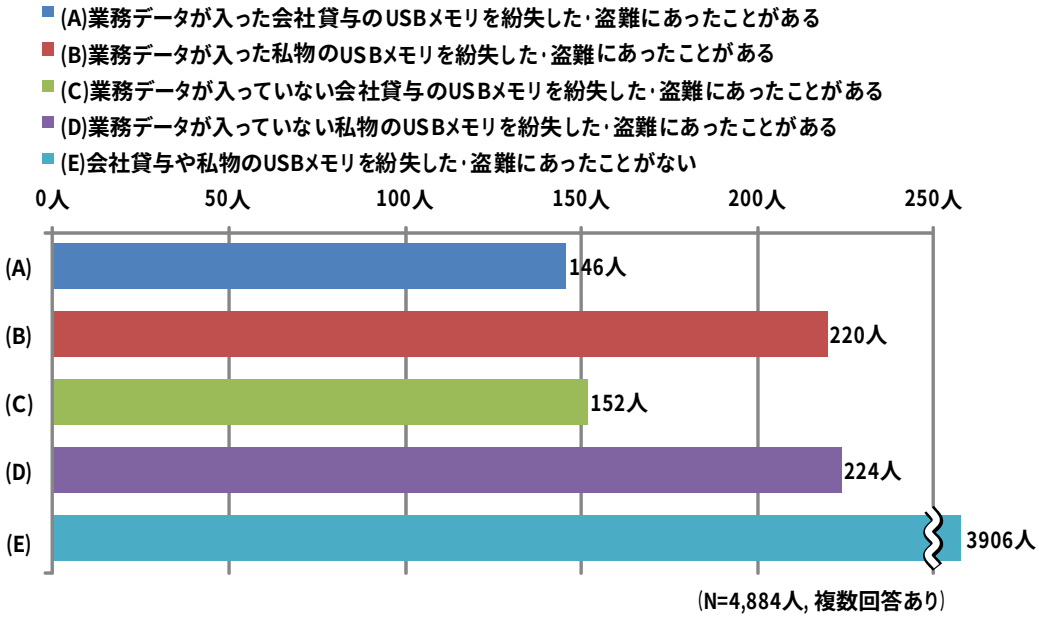

図 5.3-2：USB メモリの紛失・盗難の経験

私物、会社貸与の USB を問わず、USB をなくしたこと、なくしそうになったことがある人は 978 人（11.3%）である。会社 USB をなくしたことがある人は 5.3%、私物 USB をなくしたことがある人は 8.3%である。USB メモリに関する、紛失・盗難の割合が携帯電話よりすくないというのは想定外の結果であった。

5.3.2. 本調査の分析結果

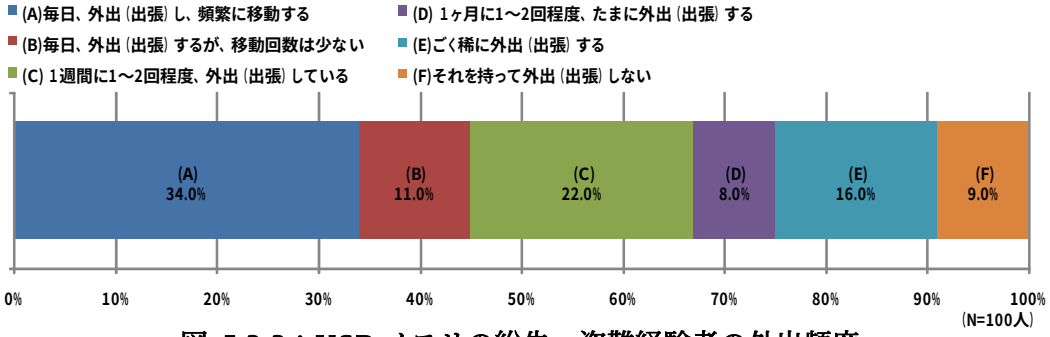

図 5.3-3：USB メモリの紛失・盗難経験者の外出頻度

仕事をする人、約 5,000 人を対象とした調査では、「業務において毎日、外出（出張）し、頻繁に移動する」人の割合は 9.6%であった。USB メモリを紛失した 100 人を対象とした本調査では、USB メモリを無くしたことがある人のうち、「業務において毎日、外出（出張）し、頻繁に移動する」人は 34%と最も高い。また、同様に「それをもって外出（出張）しない」の割合は 9.0%であった。以上のことから、USB メモリの紛失・盗難に関して、外出（出張）の頻度が大きく影響していることが分かる。一方、外出頻度と紛失割合が単純に比例していないことから、たまの外出時に紛失する危険性が高まるという想定もできる。

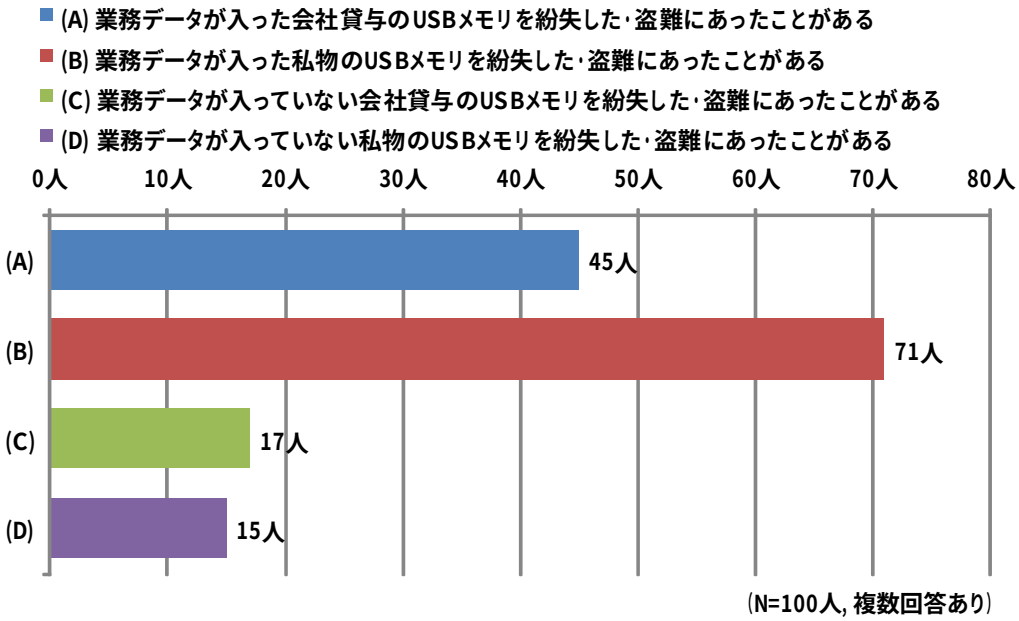

図 5.3-4：USB メモリの紛失・盗難の経験

業務データが入っていない USB メモリを無くした人は、のべ 22 人（15%）。それ以外の紛失・盗難にあった USB メモリは、なんらかの業務データが入っていたことになる。業務データが入った USB メモリを、紛失・盗難したことがある人の割合は、会社貸与（45%）より、私物（71%）の方が多い。USB メモリは、多くの人が個人の私物を業務に使っており、かつその中に業務データが含まれている状況が伺える。

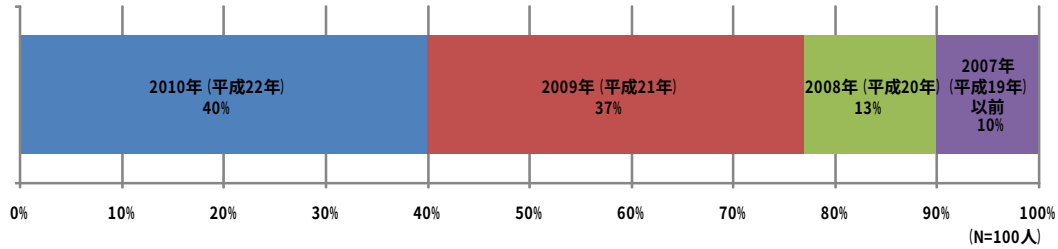

図 5.3-5：USB メモリの紛失・盗難の経験時期

USB メモリを紛失した年を一つ選択させる設問であることから、紛失した直近の年を選んでいる。USB メモリを紛失した 100 人のうち、2010 年に無くした、もしくは失くしそうになった人は 40%であった。業務データが入った USB メモリを紛失した、もしくは紛失しそうになった割合が全体で 11.7%であることから、2010 年中に 4.7%程度の USB メモリが紛失・盗難の危機にあっていると考えられる。

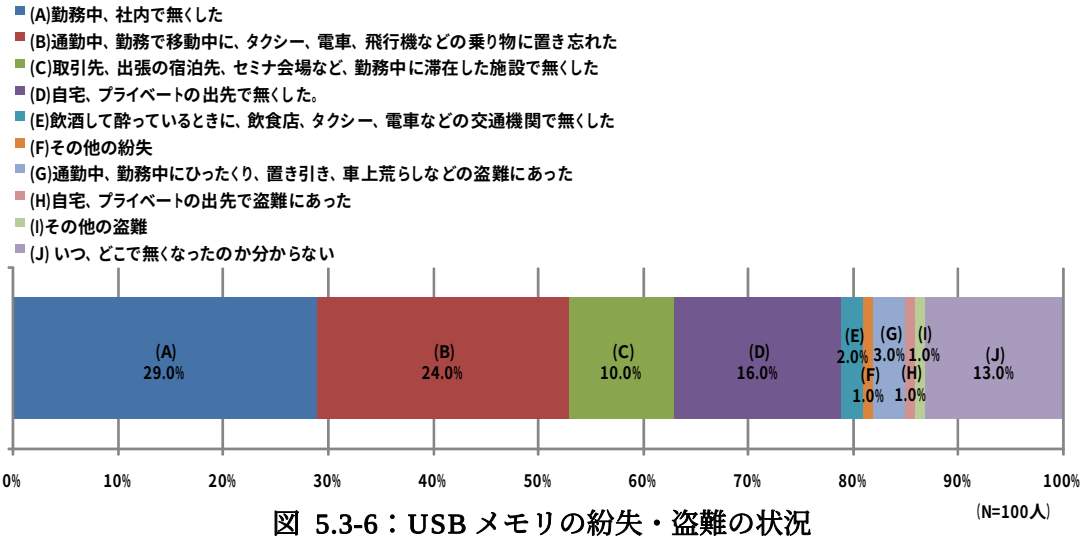

図 5.3-6：USB メモリの紛失・盗難の状況

意外な結果として、紛失・盗難が発生した状況の内、「勤務中、社内で無くした」が 29%と一番多かった。続いて「乗り物に置き忘れた」24%と「飲酒後の交通機関での紛失」2%のように移動中の紛失が多い。盗難は、勤務中、プライベートと合わせて 4%しかない。

USB メモリの特徴として、「いつ、どこ無くなったのかわからない」場合が 13%あり、携帯電話（8%）、パソコン（4%）と比べて多い。サイズが小さいことから、いつの間にかな

くなっているケースが多いことが想定される。

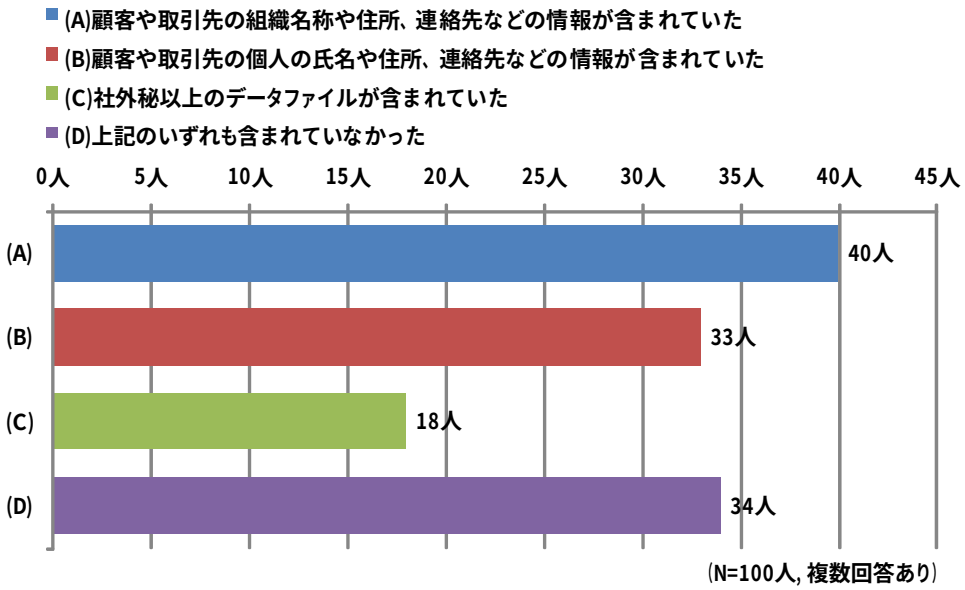

図 5.3-7：紛失・盗難された USB メモリに含まれる情報

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 66 人であった。紛失した USB メモリの半数以上には、なんらかの保護すべき情報が含まれていることが分かる。「社外秘上のデータファイル」が含まれていた人は 18 人であり、パソコンの 30 人と比べると、重要情報を保存先としては敬遠される傾向が伺える。

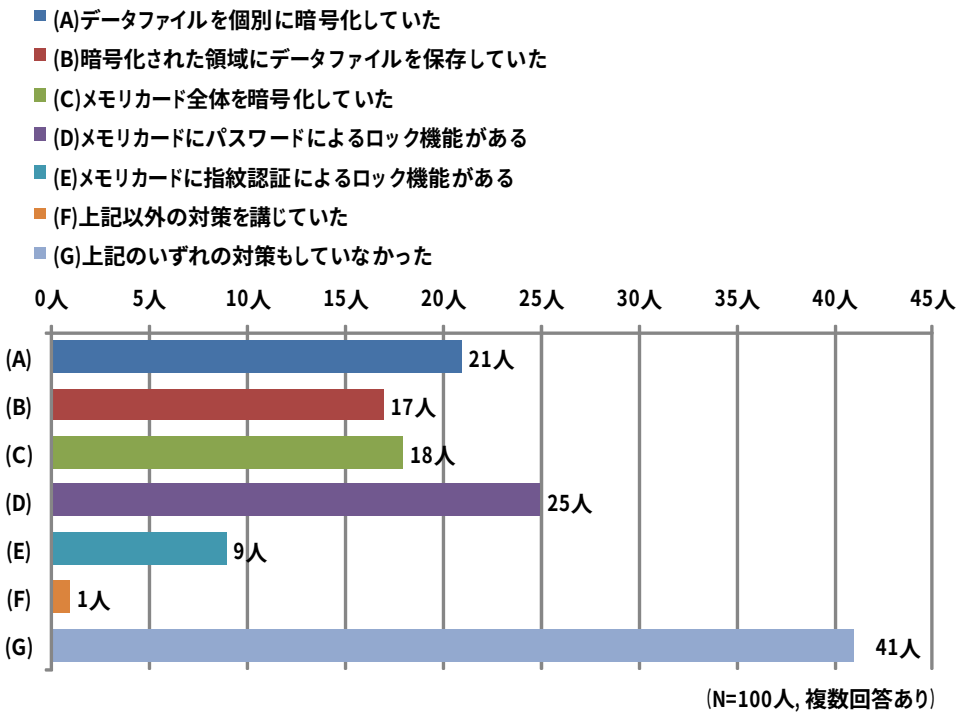

図 5.3-8：USB メモリの盗難・紛失対策

USB メモリの紛失・盗難対策の主流は、暗号化であることが分かる。ただし、「いずれの対策もしていない」が 41 人も存在することから、紛失した場合のリスクは相対的に高いものとなっている。

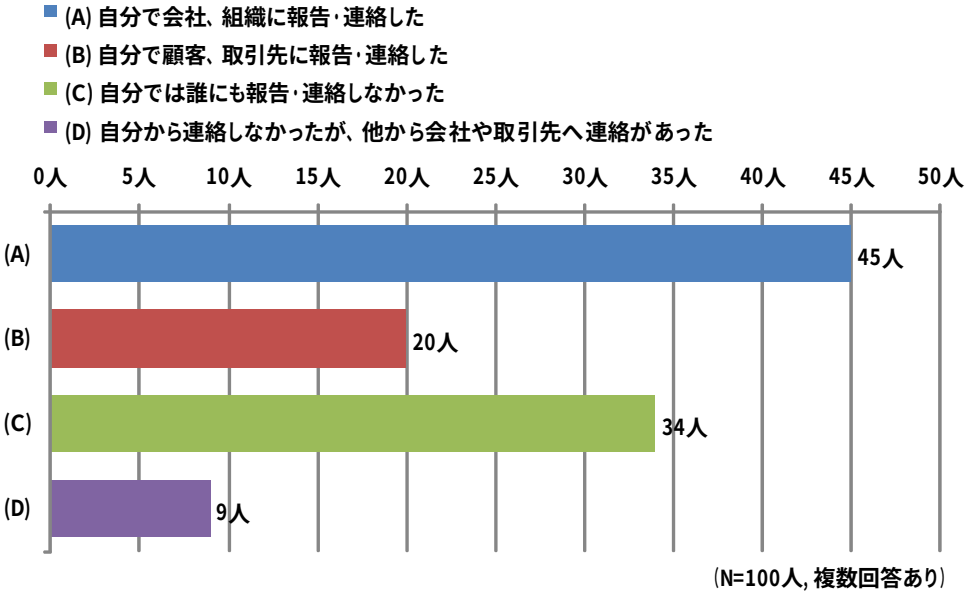

図 5.3-9：USB メモリの盗難・紛失の報告

「自分で会社、組織に報告・連絡した」は、100 人中 45 人と、パソコンの 54 人、携帯電話の 51 人と比べてやや少ない。一方で、「自分では誰にも報告・連絡しなかった」が 34 人であった。よって、会社、組織が、業務データを含んだ USB メモリの紛失・盗難を把握できていない場合も、少なからず存在する。私物を利用している割合が高いことが、影響していると想定される。また「他から会社や取引先に連絡があった」場合が 9 人あった。拾得した人が簡単に中身の確認ができ、失くした人を特定できるという特徴が伺える。

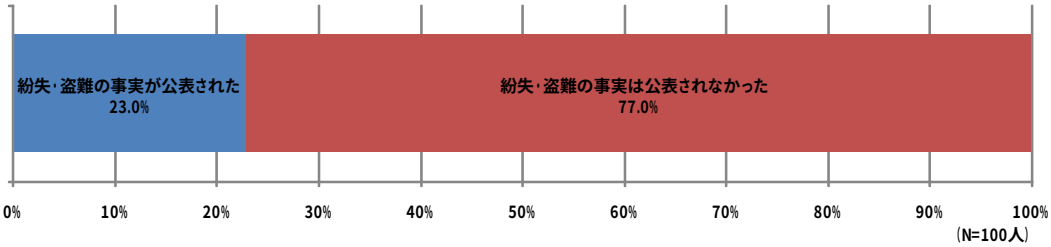

図 5.3-10：USB メモリの盗難・紛失の公表

もともと私物を利用する割合が高く、紛失しても届け出る割合が低いうえに、会社や組織としても、外部に公表する割合が 23%と低い。実際に USB メモリの紛失が判明して、外部に公表される場合は、携帯電話やパソコンと比べると少ないと予想される。

5.4. 電子メール

5.4.1. 予備調査の分析結果

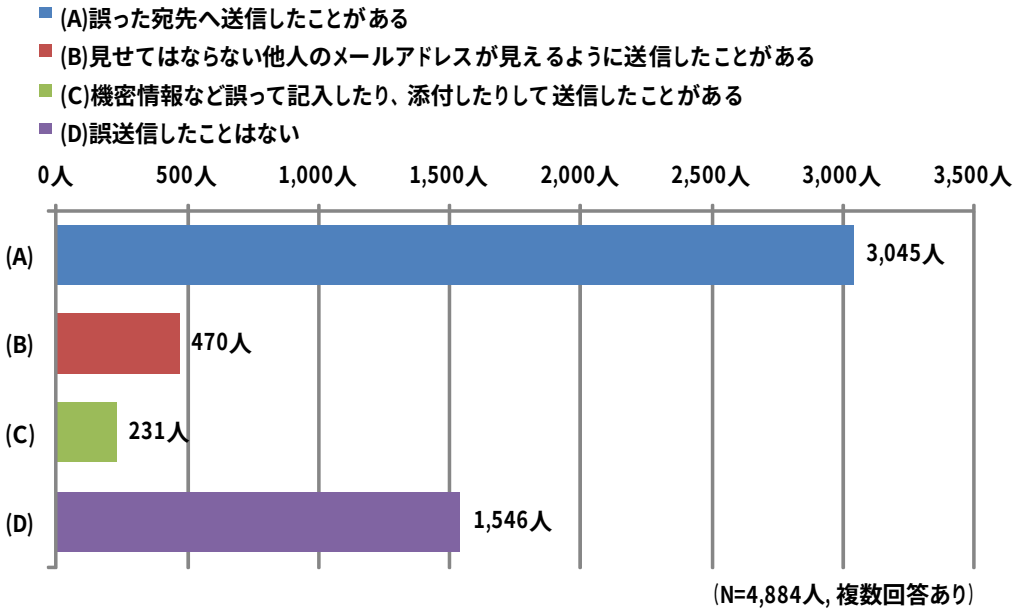

図 5.4-1：電子メールの誤送信の経験

仕事をしている人、約 5000 人への調査によると、3 分の 2 以上の 3,338 人（68.3%）が電子メールの誤送信を経験したことがある。その中でも、違った宛先への送信が 3,045 人と圧倒的に多数を占めている。今回の調査結果から、情報セキュリティ・インシデントの中でも特に発生確率が高い。

5.4.2. 本調査の分析結果

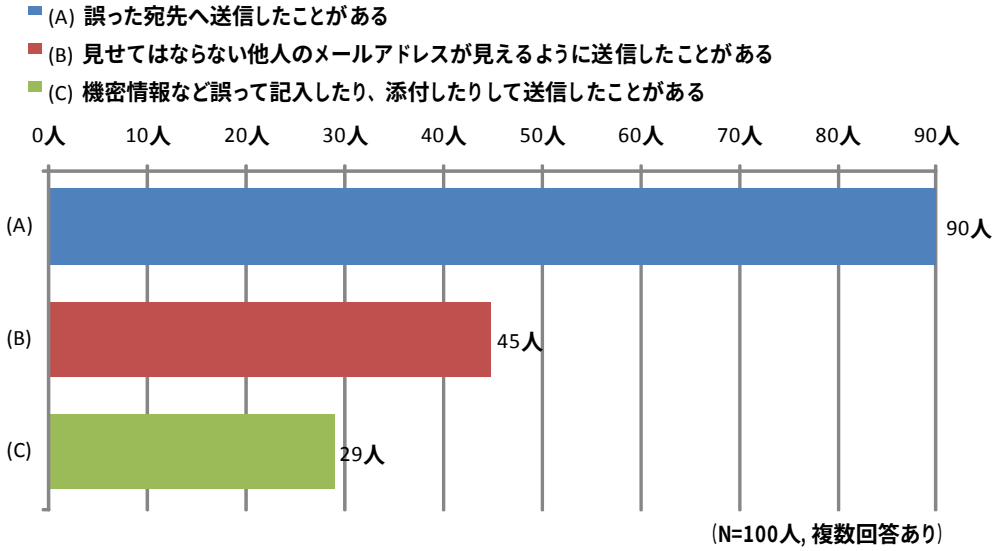

図 5.4-2：電子メールの誤送信パターン

メールの誤送信を経験したことがある 100 人に対して、誤送信のパターンを確認すると、90 人が「誤った宛先への送信」の経験をあげている。なぜか、100 人を対象とした調査では、約 5,000 人を対象とした調査と比べて、「他人のメールアドレスが見えるように送信した」「機密情報などの送信」の割合が高い。

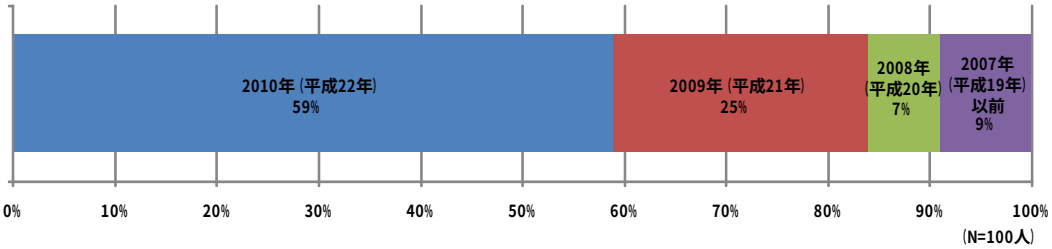

図 5.4-3：電子メールの誤送信の経験時期

電子メールを誤送信した年を一つ選択させる設問であることから、紛失した直近の年を選んでいる。2010 年が 59%と多数を占めている。2010 年と比べて、2009 年の割合が大きく下がっていることから、メールの誤送信は、これまでに複数回を経験している人が多いと予想される。

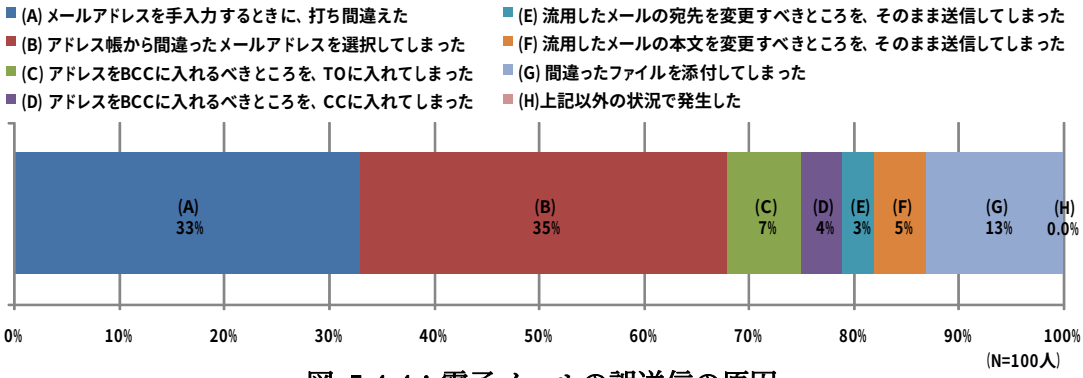

図 5.4-4：電子メールの誤送信の原因

電子メールの誤送信は、「(B) アドレス帳からの選択ミス」（35%）、「(A) アドレス入力時の打ち間違い」（33%）、「(G) 間違ったファイルの添付」（13%）の順に多い。

近年のメールソフトは、アドレスの自動補完機能などが充実しており、大変使いやすいものとなっている。その結果、メールはその利便性の高さの代償として、情報漏洩の危険性が非常に高いものとなっており、個人のちょっとした不注意が原因となり、組織にとって重大な問題を引き起こす可能性を秘めている。

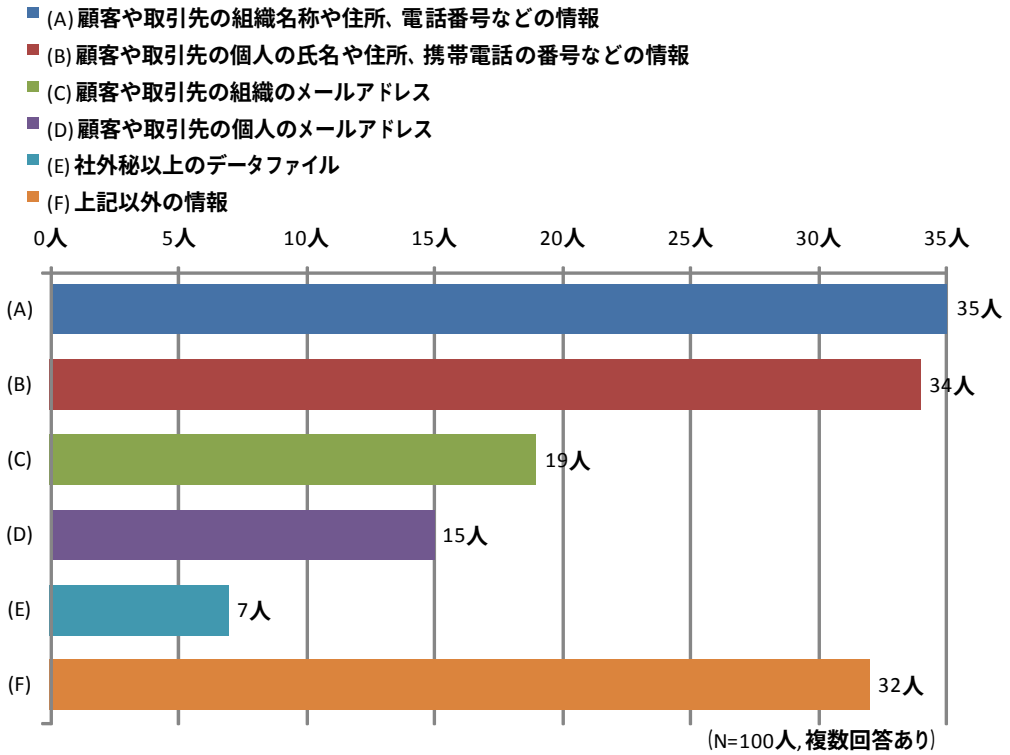

図 5.4-5：電子メールで誤送信した情報

顧客や取引先の情報の誤送信が、ほとんどを占める。社外秘以上のデータの誤送信は 7 人であった。「上記以外の情報」（32 人）については、社外秘ほどではないが、不適切な情報

を送ってしまったものと考えられる。

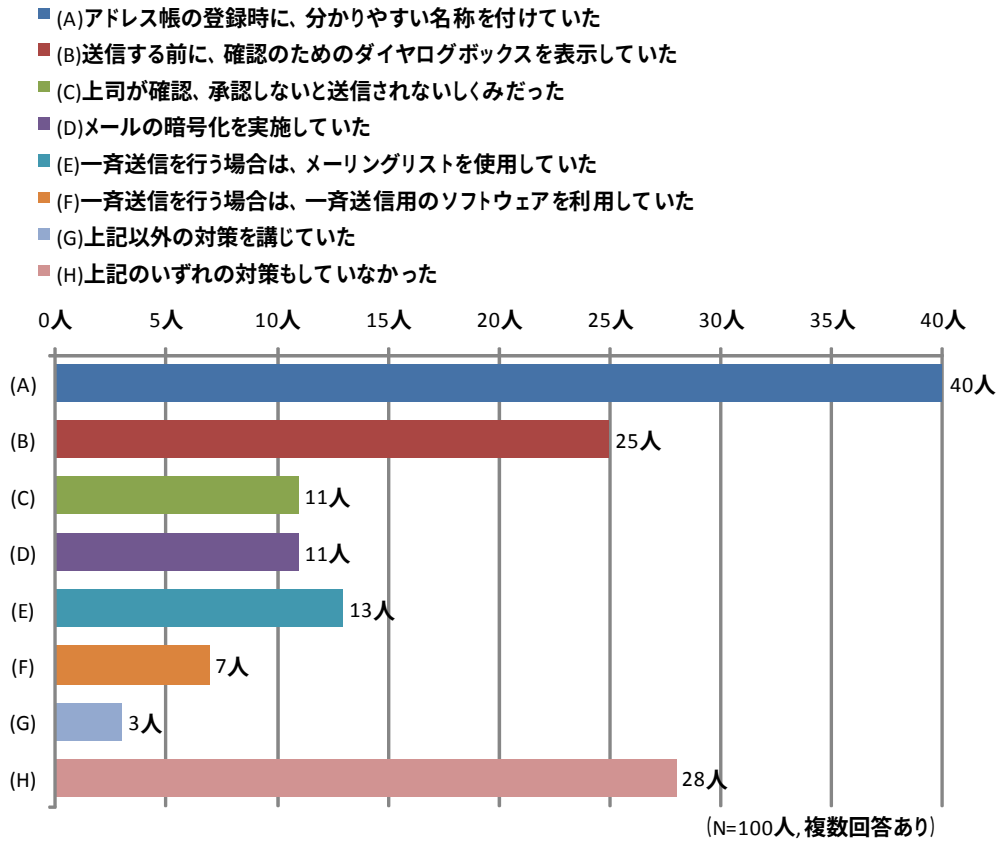

図 5.4-6：電子メールの誤送信対策

「アドレス帳の登録時に、わかりやすい名前を付けていた」が 40 人と最も多い。「上司が確認、承認しないと送信されないしくみ」（11 人）が導入されていても、誤送信が発生していることから、二重チェックなどでも防ぎきれていないことが分かる。

また、「いずれの対策もしていない」と回答した人が 28 人も存在することから、メールの誤送信の発生確率が高いことをもっと認知させ無ければならない。

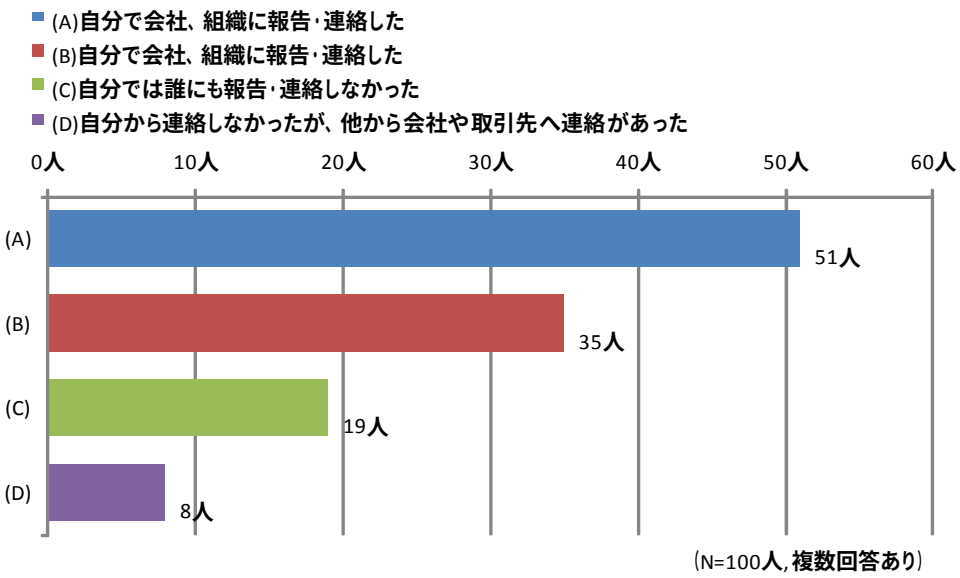

図 5.4-7：電子メールの誤送信の報告

「自分で会社、組織に報告・連絡した」は、100 人中 51 人と半数を占めている。一方で、「自分では誰にも報告・連絡しなかった」場合が 19 人あった。よって、会社、組織は、メールの誤送信をあまり把握できていないと思われる。また「他から会社や取引先に連絡があった」場合が 8 人あった。外部から連絡がある前に、自発的に報告・連絡する組織文化の醸成が必要と考える。

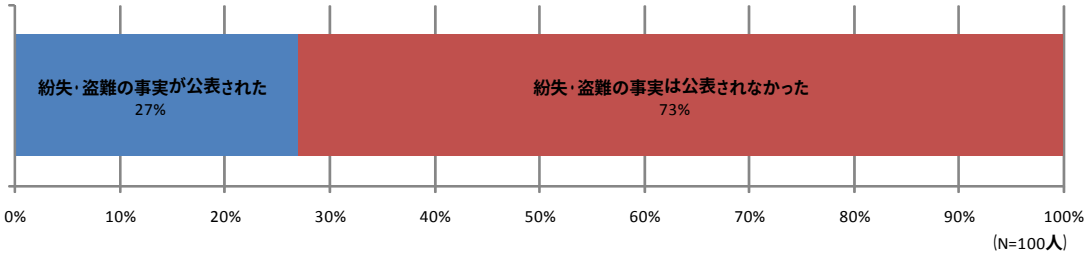

図 5.4-8：電子メールの誤送信の公表

「紛失・盗難の事実が公表された」割合は 27%であった。会社や組織が電子メールの誤送信を把握する割合が低く、公表を必要としない場合も多いと予想されることから、実際に外部へ公表される場合は、上記の値よりも少ない思われる。

5.5. ＦＡＸ

5.5.1. 予備調査の分析結果

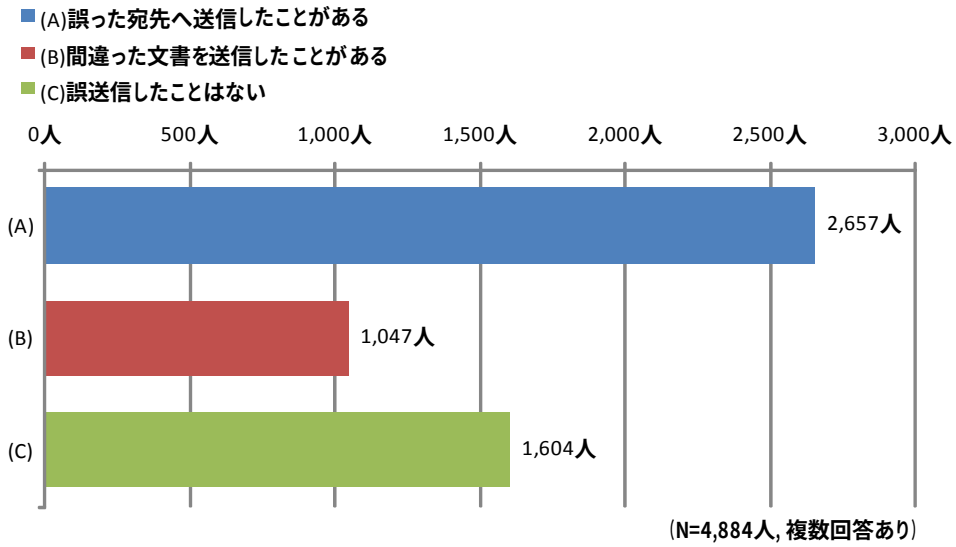

図 5.5-1：FAX の誤送信の経験

仕事をしている人、約 5000 人への調査によると、、ほぼ 3 分の 2 の 3,280 人（67.2%）が何らかの FAX の誤送信を経験したことがある。その中でも、違った宛先への送信が 2,657 人（54.4%）を占めている。今回の調査結果から、情報セキュリティ・インシデントの中でもメールの誤送信に次いで、発生確率が高い。

5.5.2. 本調査の分析結果

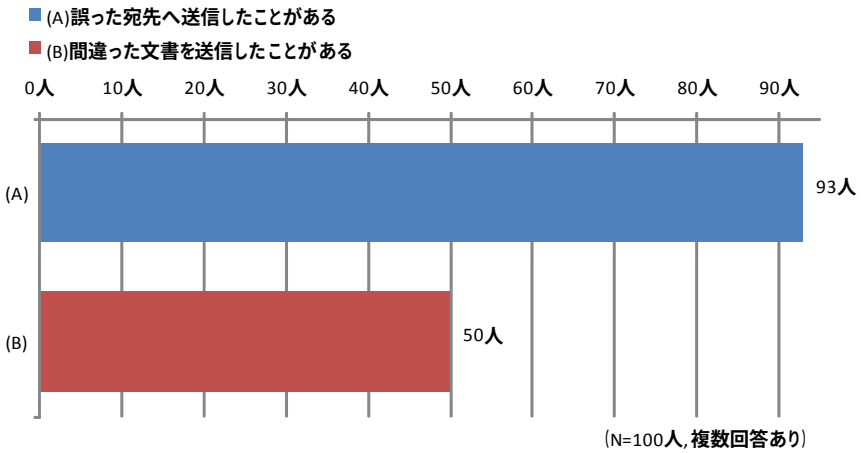

図 5.5-2：FAX の誤送信パターン

FAX の誤送信を経験したことがある人 100 人に対して、誤送信のパターンを確認すると、

93 人が「誤った宛先への送信」の経験をあげている。「誤った宛先への送信」をしたことがある人のうち、約半数は「間違った文章の送信もしたことがある」と回答している。再発の可能性が高いことが想定される。

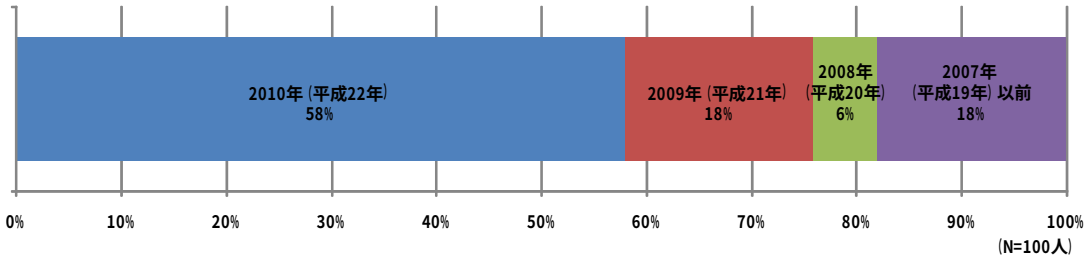

図 5.5-3：FAX の誤送信の経験時期

電子メールを誤送信した年を一つ選択させる設問であることから、紛失した直近の年を選んでいる。2010 年が 58%と多数を占めている。電子メールと同様、2010 年と比べて、2009 年の割合が大きく下がっていることから、FAX の誤送信も、これまでに複数回を経験している人が多いと予想される。

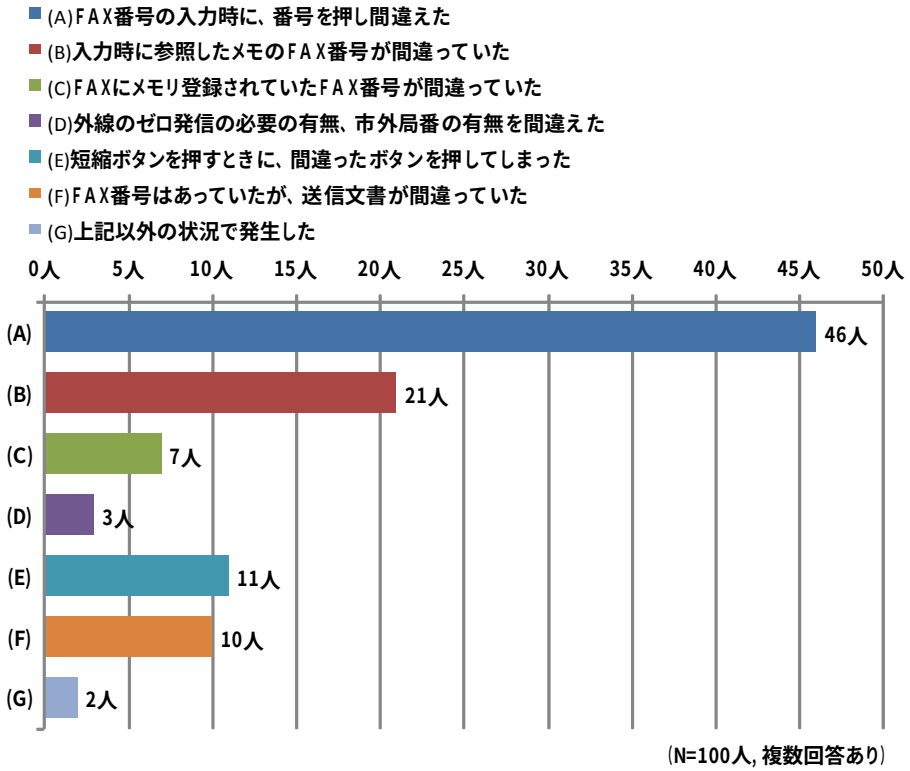

図 5.5-4：FAX の誤送信の原因

FAX の誤送信は、「(A) 番号の入力時に押し間違えた」（46 人）、「(B) 参照した番号が間

違っていた」（21 人）、「(E) 短縮ボタンを押し間違えた」（11 人）の順に多い。

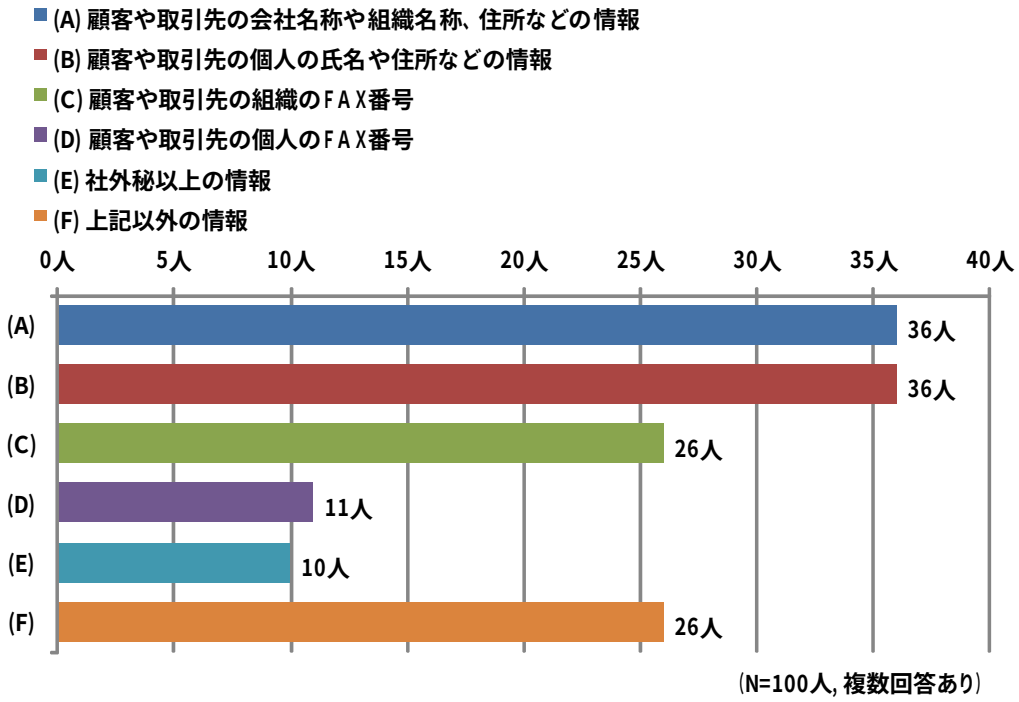

図 5.5-5：FAX で誤送信した情報

顧客や取引先の情報の誤送信が、ほとんどを占める。社外秘以上のデータの誤送信は 10 人であった。「上記以外の情報」（26 人）については、社外秘ほどではないが、自社にとって不適切な情報を送ってしまったものと考えられる。

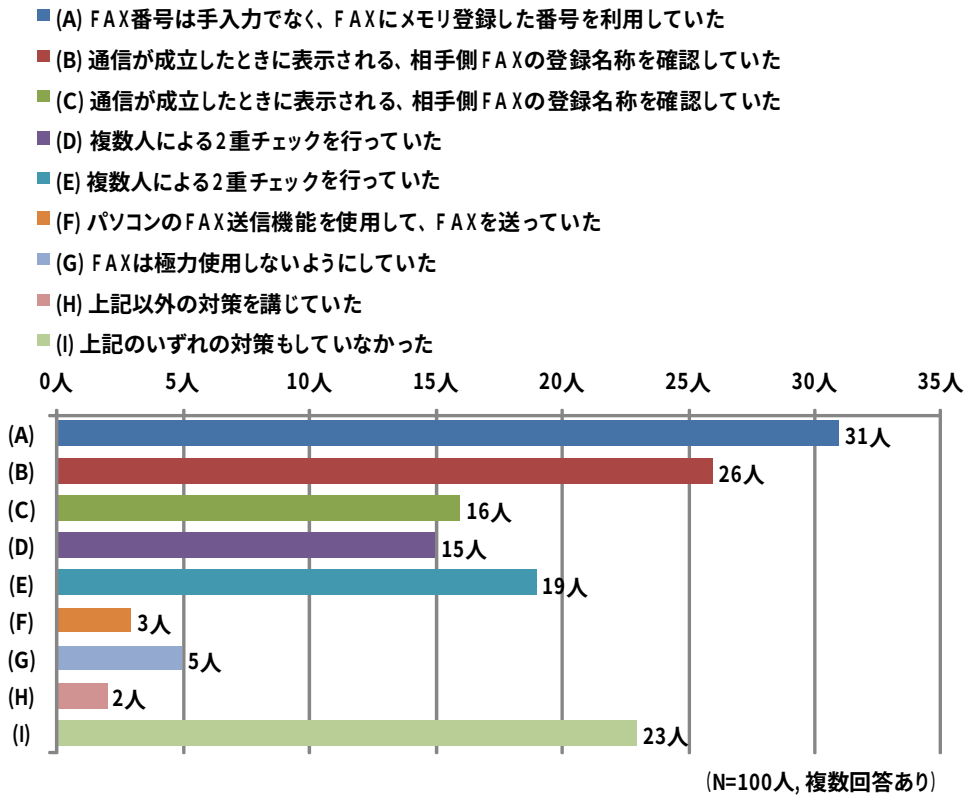

図 5.5-6：FAX の誤送信対策

「手入力ではなく、メモリ登録した番号を利用」が 31 人と最も多い。「通信成立時に、相手先を確認」（26 人）、「FAX 送信前後での電話確認」（19 人）、「2 重チェック」（15 人）、「上司が確認、承認しないと送信されないしくみ」（11 人）が導入されていても、誤送信は発生している。

「いずれの対策もしていない」と回答した人が 23 人も存在することから、FAX の誤送信リスクに対する認知度の向上と、複数の対策の組み合わせ実施が望まれる。

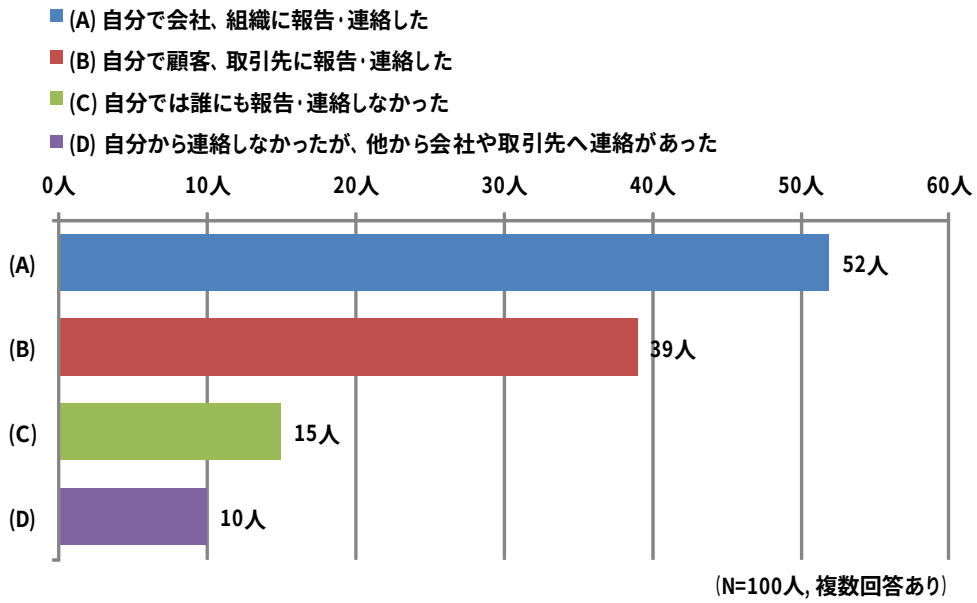

図 5.5-7：FAX の誤送信の報告

「自分で会社、組織に報告・連絡した」は、100 人中 52 人と半数を占めている。一方で、「自分では誰にも報告・連絡しなかった」場合が 15 人あった。よって、会社、組織は、メールの誤送信をあまり把握できていないと思われる。また「他から会社や取引先に連絡があった」場合が 10 人あった。外部から連絡がある前に、自発的に報告・連絡する組織文化の醸成が必要と考える。

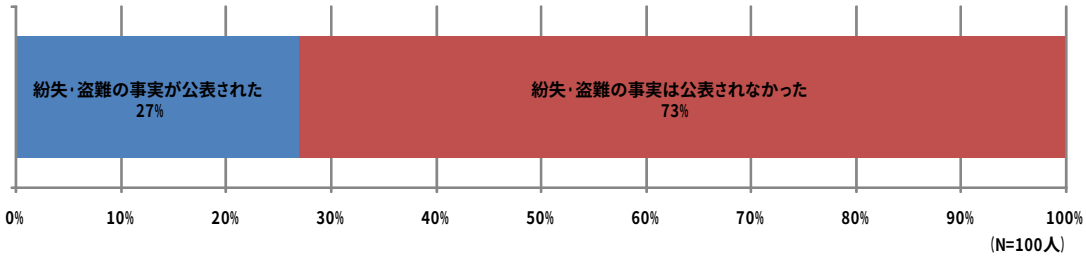

図 5.5-8：FAX の誤送信の公表

「紛失・盗難の事実が公表された」割合は、27%であった。会社や組織が電子メールの誤送信を把握する割合が低く、公表を必要としない場合も多いと予想されることから、実際に外部へ公表される場合は、上記の値よりも少ない思われる。

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
SC2-1	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）【携帯電話】
SC2-1	1	毎日、外出（出張）し、頻繁に移動する
SC2-1	2	毎日、外出（出張）するが、移動回数は少ない
SC2-1	3	1週間に 1～2 回程度、外出（出張）している
SC2-1	4	1ヶ月に 1～2 回程度、たまに外出（出張）する
SC2-1	5	ごく稀に外出（出張）する
SC2-1	6	それを持って外出（出張）しない
SC2-2	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】
SC2-2	1	毎日、外出（出張）し、頻繁に移動する
SC2-2	2	毎日、外出（出張）するが、移動回数は少ない
SC2-2	3	1週間に 1～2 回程度、外出（出張）している
SC2-2	4	1ヶ月に 1～2 回程度、たまに外出（出張）する
SC2-2	5	ごく稀に外出（出張）する
SC2-2	6	それを持って外出（出張）しない

SC2-3	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】
SC2-3	1	毎日、外出 (出張) し、頻繁に移動する
SC2-3	2	毎日、外出 (出張) するが、移動回数は少ない
SC2-3	3	1週間に 1～2 回程度、外出 (出張) している
SC2-3	4	1ヶ月に 1～2 回程度、たまに外出 (出張) する
SC2-3	5	ごく稀に外出 (出張) する
SC2-3	6	それを持って外出 (出張) しない
Q1	MA	これまで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)
Q1M1	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
Q1M2	1	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
Q1M3	1	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
Q1M4	1	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
Q1M5	1	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
Q1M6	1	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
Q1M7	1	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
Q2	MA	これまで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)
Q2M1	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
Q2M2	1	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
Q2M3	1	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
Q2M4	1	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
Q2M5	1	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
Q2M6	1	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
Q2M7	1	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
Q3	MA	これまでに会社貸与の 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)
Q3M1	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
Q3M2	1	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
Q3M3	1	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

Q3M4	1	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
Q3M5	1	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
Q4	MA	電子メールの誤送信についてお伺いします。これまでに業務において、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）
Q4M1	1	誤った宛先へ送信したことがある
Q4M2	1	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
Q4M3	1	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
Q4M4	1	誤送信したことはない
Q5	MA	FAX の誤送信についてお伺いします。これまでに業務において、以下のような FAX の誤送信をしたことがありますか。（お答えはいくつでも）
Q5M1	1	誤った宛先へ送信したことがある
Q5M2	1	間違った文書を送信したことがある
Q5M3	1	誤送信したことはない

6.2. 本調査の設問と回答（携帯電話）

Q1　いつごろ、紛失･盗難が発生しましたか。（お答えは 1 つ）

		回答数	%
全　体（N）		100	100.0
1	2010 年（平成 22 年）	32	32.0
2	2009 年（平成 21 年）	33	33.0
3	2008 年（平成 20 年）	13	13.0
4	2007 年（平成 19 年）以前	22	22.0

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）

		回答数	%
全　体（N）		100	100.0
1	勤務中、社内で無くした	17	17.0
2	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	29	29.0
3	取引先、出張の宿泊先、セミナー会場など、勤務中に滞在した施設で無くした	11	11.0
4	自宅、プライベートの出先で無くした。	17	17.0
5	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	11	11.0
6	その他の紛失	0	0.0
7	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
8	自宅、プライベートの出先で盗難にあった	5	5.0
9	その他の盗難	0	0.0
10	いつ、どこで無くなったのか分からない	8	8.0

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）

		回答数	%
全　体（N）		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	46	46.0
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	53	53.0

3	社外秘以上のデータファイルが含まれていた	13	13.0
4	上記のいずれも含まれていなかった	18	18.0

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

		回答数	%
全　　体 (N)		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	43	43.0
2	携帯電話に指紋認証などの生体認証を利用していた	15	15.0
3	遠隔ロック(リモートロック)機能を利用していた	24	24.0
4	GPS による位置確認サービスを利用していた	8	8.0
5	ネックストラップやスパイラルストラップなどで、落下を防止していた	8	8.0
6	紛失防止アラームを付けていた	5	5.0
7	個人情報を入れないようにしていた	8	8.0
8	業務上のデータファイルを入れないようにしていた	10	10.0
9	上記以外の対策を講じていた	0	0.0
10	上記のいずれの対策もしていなかった	23	23.0

Q5-1　紛失･盗難の事実をどのように報告、連絡しましたか。(お答えはいくつでも) また、紛失･盗難の事実は公表されましたか。(お答えは 1 つ)

		回答数	%
全　　体 (N)		100	100.0
1	自分で会社、組織に報告･連絡した	51	51.0
2	自分で顧客、取引先に報告･連絡した	23	23.0
3	自分では誰にも報告･連絡しなかった	25	25.0
4	自分から連絡しなかったが、他から会社や取引先へ連絡があった	5	5.0

Q5-2　紛失･盗難の事実をどのように報告、連絡しましたか。(お答えはいくつでも) また、紛失･盗難の事実は公表されましたか。(お答えは 1 つ)

		回答数	%
全　　体 (N)		100	100.0
1	紛失･盗難の事実が公表された	24	24.0
2	紛失･盗難の事実は公表されなかった	76	76.0

6.3. 本調査の設問と回答（パソコン）

Q1　いつごろ、紛失･盗難が発生しましたか。（お答えは 1 つ）

		回答数	%
全　体（N）		100	100.0
1	2010 年（平成 22 年）	35	35.0
2	2009 年（平成 21 年）	29	29.0
3	2008 年（平成 20 年）	13	13.0
4	2007 年（平成 19 年）以前	23	23.0

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）

		回答数	%
全　体（N）		100	100.0
1	勤務中、社内で無くした	29	29.0
2	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	24	24.0
3	取引先、出張の宿泊先、セミナー会場など、勤務中に滞在した施設で無くした	14	14.0
4	自宅、プライベートの出先で無くした。	8	8.0
5	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	4	4.0
6	その他の紛失	0	0.0
7	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	6	6.0
8	自宅、プライベートの出先で盗難にあった	9	9.0
9	その他の盗難	2	2.0
10	いつ、どこで無くなったのか分からない	4	4.0

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）

		回答数	%
全　体（N）		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	39	39.0
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	42	42.0
3	社外秘以上のデータファイルが含まれていた	30	30.0

4	上記のいずれも含まれていなかった	23	23.0

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

		回答数	%
全　体 (N)		100	100.0
1	ログインパスワードを設定していた	57	57.0
2	指紋認証などの生体認証を使用していた	15	15.0
3	機密データを含むファイルは個別に暗号化していた	18	18.0
4	ハードディスク全体を暗号化していた	15	15.0
5	盗難防止ワイヤで固定していた	9	9.0
6	キャビネットなどに鍵を掛けて保管していた	7	7.0
7	シンクライアント化していた、HDD を外していた	4	4.0
8	上記以外の対策を講じていた	3	3.0
9	上記のいずれの対策もしていなかった	17	17.0

Q5-1　紛失･盗難の事実をどのように報告、連絡しましたか。(お答えはいくつでも)

		回答数	%
全　体 (N)		100	100.0
1	自分で会社、組織に報告･連絡した	54	54.0
2	自分で顧客、取引先に報告･連絡した	29	29.0
3	自分では誰にも報告･連絡しなかった	18	18.0
4	自分から連絡しなかったが、他から会社や取引先へ連絡があった	8	8.0

Q5-2　また、紛失･盗難の事実は公表されましたか。(お答えは 1 つ)

		回答数	%
全　体 (N)		100	100.0
1	紛失･盗難の事実が公表された	31	31.0
2	紛失･盗難の事実は公表されなかった	69	69.0

6.4. 本調査の設問と回答（USB）

Q1　いつごろ、紛失・盗難が発生しましたか。（お答えは 1 つ）

		回答数	%
全　　体（N）		100	100.0
1	2010 年（平成 22 年）	40	40.0
2	2009 年（平成 21 年）	37	37.0
3	2008 年（平成 20 年）	13	13.0
4	2007 年（平成 19 年）以前	10	10.0

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）

		回答数	%
全　　体（N）		100	100.0
1	勤務中、社内で無くした	29	29.0
2	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	24	24.0
3	取引先、出張の宿泊先、セミナー会場など、勤務中に滞在した施設で無くした	10	10.0
4	自宅、プライベートの出先で無くした。	16	16.0
5	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
6	その他の紛失	1	1.0
7	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	3	3.0
8	自宅、プライベートの出先で盗難にあった	1	1.0
9	その他の盗難	1	1.0
10	いつ、どこで無くなったのか分からない	13	13.0

Q3　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）

		回答数	%
全　　体（N）		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	40	40.0
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	33	33.0

3	社外秘以上のデータファイルが含まれていた	18	18.0
4	上記のいずれも含まれていなかった	34	34.0

Q4　紛失･盗難にあった 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)

		回答数	%
全　　体 (N)		100	100.0
1	データファイルを個別に暗号化していた	21	21.0
2	暗号化された領域にデータファイルを保存していた	17	17.0
3	メモリカード全体を暗号化していた	18	18.0
4	メモリカードにパスワードによるロック機能がある	25	25.0
5	メモリカード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	1	1.0
7	上記のいずれの対策もしていなかった	41	41.0

Q5-1　紛失･盗難の事実をどのように報告、連絡しましたか。(お答えはいくつでも)

		回答数	%
全　　体 (N)		100	100.0
1	自分で会社、組織に報告･連絡した	45	45.0
2	自分で顧客、取引先に報告･連絡した	20	20.0
3	自分では誰にも報告･連絡しなかった	34	34.0
4	自分から連絡しなかったが、他から会社や取引先へ連絡があった	9	9.0

Q5-2　また、紛失･盗難の事実は公表されましたか。(お答えは 1 つ)

		回答数	%
全　　体 (N)		100	100.0
1	紛失･盗難の事実が公表された	23	23.0
2	紛失･盗難の事実は公表されなかった	77	77.0

6.5. 本調査の設問と回答（電子メール）

Q1　いつごろ、誤送信が発生しましたか。（お答えは 1 つ）

		回答数	%
全　　体（N）		100	100.0
1	2010 年（平成 22 年）	59	59.0
2	2009 年（平成 21 年）	25	25.0
3	2008 年（平成 20 年）	7	7.0
4	2007 年（平成 19 年）以前	9	9.0

Q2　どのような状況で誤送信が発生しましたか。（お答えは 1 つ）

		回答数	%
全　　体（N）		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	33	33.0
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	35	35.0
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	7	7.0
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	3	3.0
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	5	5.0
7	間違ったファイルを添付してしまった	13	13.0
8	上記以外の状況で発生した	0	0.0

Q3　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）

		回答数	%
全　　体（N）		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	35	35.0
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	34	34.0
3	顧客や取引先の組織のメールアドレス	19	19.0
4	顧客や取引先の個人のメールアドレス	15	15.0
5	社外秘以上のデータファイル	7	7.0
6	上記以外の情報	32	32.0

Q4　　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)

		回答数	%
全　　体 (N)		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	40	40.0
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	25	25.0
3	上司が確認、承認しないと送信されないしくみだった	11	11.0
4	メールの暗号化を実施していた	11	11.0
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	7	7.0
7	上記以外の対策を講じていた	3	3.0
8	上記のいずれの対策もしていなかった	28	28.0

Q5-1　　紛失･盗難の事実をどのように報告、連絡しましたか。(お答えはいくつでも)

		回答数	%
全　　体 (N)		100	100.0
1	自分で会社、組織に報告･連絡した	51	51.0
2	自分で顧客、取引先に報告･連絡した	35	35.0
3	自分では誰にも報告･連絡しなかった	19	19.0
4	自分から連絡しなかったが、他から会社や取引先へ連絡があった	8	8.0

Q5-2　　また、紛失･盗難の事実は公表されましたか。(お答えは 1 つ)

		回答数	%
全　　体 (N)		100	100.0
1	紛失･盗難の事実が公表された	27	27.0
2	紛失･盗難の事実は公表されなかった	73	73.0

6.6. 本調査の設問と回答（FAX）

Q1　いつごろ、誤送信が発生しましたか。（お答えは 1 つ）

		回答数	%
全　　体（N）		100	100.0
1	2010 年（平成 22 年）	58	58.0
2	2009 年（平成 21 年）	18	18.0
3	2008 年（平成 20 年）	6	6.0
4	2007 年（平成 19 年）以前	18	18.0

Q2　どのような状況で誤送信が発生しましたか。（お答えは 1 つ）

		回答数	%
全　　体（N）		100	100.0
1	ＦＡＸ番号の入力時に、番号を押し間違えた	46	46.0
2	入力時に参照したメモのＦＡＸ番号が間違っていた	21	21.0
3	ＦＡＸにメモリ登録されていたＦＡＸ番号が間違っていた	7	7.0
4	外線のゼロ発信の必要の有無、市外局番の有無を間違えた	3	3.0
5	短縮ボタンを押すときに、間違ったボタンを押してしまった	11	11.0
6	ＦＡＸ番号はあっていたが、送信文書が間違っていた	10	10.0
7	上記以外の状況で発生した	2	2.0

Q3　誤送信したＦＡＸ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）

		回答数	%
全　　体（N）		100	100.0
1	顧客や取引先の会社名称や組織名称、住所などの情報	36	36.0
2	顧客や取引先の個人の氏名や住所などの情報	36	36.0
3	顧客や取引先の組織のＦＡＸ番号	26	26.0
4	顧客や取引先の個人のＦＡＸ番号	11	11.0
5	社外秘以上の情報	10	10.0
6	上記以外の情報	26	26.0

Q4　　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)

		回答数	%
全　　体 (N)		100	100.0
1	ＦＡＸ番号は手入力でなく、ＦＡＸにメモリ登録した番号を利用していた	31	31.0
2	通信が成立したときに表示される、相手側ＦＡＸの登録名称を確認していた	26	26.0
3	個人情報や、社外秘以上の情報を削除したものを送信していた	16	16.0
4	複数人による2重チェックを行っていた	15	15.0
5	ＦＡＸ送信の前または後に、相手先に電話を入れて確認していた	19	19.0
6	パソコンのＦＡＸ送信機能を使用して、ＦＡＸを送っていた	3	3.0
7	ＦＡＸは極力使用しないようにしていた	5	5.0
8	上記以外の対策を講じていた	2	2.0
9	上記のいずれの対策もしていなかった	23	23.0

Q5-1　　紛失･盗難の事実をどのように報告、連絡しましたか。(お答えはいくつでも)

		回答数	%
全　　体 (N)		100	100.0
1	自分で会社、組織に報告･連絡した	52	52.0
2	自分で顧客、取引先に報告･連絡した	39	39.0
3	自分では誰にも報告･連絡しなかった	15	15.0
4	自分から連絡しなかったが、他から会社や取引先へ連絡があった	10	10.0

Q5-2　　また、紛失･盗難の事実は公表されましたか。(お答えは１つ)

		回答数	%
全　　体 (N)		100	100.0
1	紛失･盗難の事実が公表された	27	27.0
2	紛失･盗難の事実は公表されなかった	73	73.0