

企業が抱える情報漏えいリスクに関する意識調査

セキュアなペーパーレス会議システムSONOBA COMET(ソノバ コメット)を販売する株式会社CIJ(代表取締役社長 堀 信一)は、2014年5月2日～8日の7日間、20歳以上のビジネスパーソンを対象に「企業が抱える情報漏えいリスクに関する意識調査」をモバイルリサーチ(携帯電話によるインターネットリサーチ)にて実施いたしました。

上記リサーチ結果から2,000名の有効サンプルを分析してみえてきた、「企業が抱える情報漏えいリスク」に関する現状をレポートいたします。

Topics

【ビジネスパーソンの“炎上”リスク】

- SNSの書き込み「告発目的なら、内部情報を公開してもよい」1割
- 「立場を隠してSNSで自社肯定の投稿をしても問題ない」20代で13%

【私的利用端末の業務利用実態】

- ビジネスパーソンの2割がタブレット端末を個人所有、部長職以上では3割半
- 個人所有のPCを業務利用3割強、タブレット端末は3割弱、スマホは4割強

【ビジネスパーソンの情報漏えいリスク管理実態】

- 個人PCで業務メールするビジネスパーソン 3人に1人がXP使用
- 半数近くはノーガード? 「スマホ・タブにパスワード設定」5割強、「セキュリティソフト利用」は5割弱
- 公衆無線LAN利用時のセキュリティ対策は不十分?
「公衆無線LANで大事な情報やり取りをしない」2割弱、「無線LAN暗号化の規格をチェックする」1割
- 生活者視点では厳しい態度 「情報流出歴のある会社のサービスは利用しない」16%

【職場の情報漏えいリスク管理実態】

- 個人端末に内部資料を保存「禁止されている」職場は4割強、5割強の職場はルールを整備・周知不足
仕事の持ち帰りに関するルール、整備・周知不足の職場が5割
- ビジネスパーソンの個人端末は職場の機密情報の山?
「内部資料入っている」1割半、「仕事を持ち帰って自宅作業」2割弱、「顧客の連絡先登録してある」2割強
- スマートデバイス普及で“シャドーIT”増加?
ルール未整備の職場では「個人端末に内部資料保存」3割弱が実行、「顧客の連絡先登録」は4割

【ビジネスシーンの情報漏えいトラブル／ヒヤリ・ハット実態】

- 情報漏えいの3大ヒヤリ・ハット?
「居酒屋でオフレコトーク」「机上に放置・引き出し未施錠」「FAXを誤送信」
- あわや情報漏えい事件に発展!? 会議情報の漏えいヒヤリ・ハット
「会議資料が裁断されずゴミ箱へ」1割が目撃、「ホワイトボード消し忘れ」「コピー機に原本放置」なども

【情報漏えい対策に対するビジネスパーソンの意識】

- 部長職以上の6割半が「情報漏えい対策に不安なし」、一般社員では5割強に留まる
- 「情報漏えい対策は社員教育が大事」9割強も、「職場内にどんなに教育してもダメな人がいる」6割半
- 「情報漏えい対策を優先すると業務効率を損なう」5割強、
タブレットをビジネスに活用中の方は7割半が同意

調査概要

- 調査タイトル : 企業が抱える情報漏えいリスクに関する意識調査
- 調査対象 : 20歳以上のビジネスパーソン
- 調査期間 : 2014年5月2日～8日
- 調査方法 : インターネット調査(モバイルリサーチ)
- 調査地域 : 全国
- 有効回答数 : 2,000サンプル *有効回答から下記年代区分で均等に抽出
(内訳)20代・30代・40代・50代以上 各500名
- 調査協力会社 : ネットエイジア株式会社

調査結果

◆SNSの書き込み「告発目的なら、内部情報を公開してもよい」1割

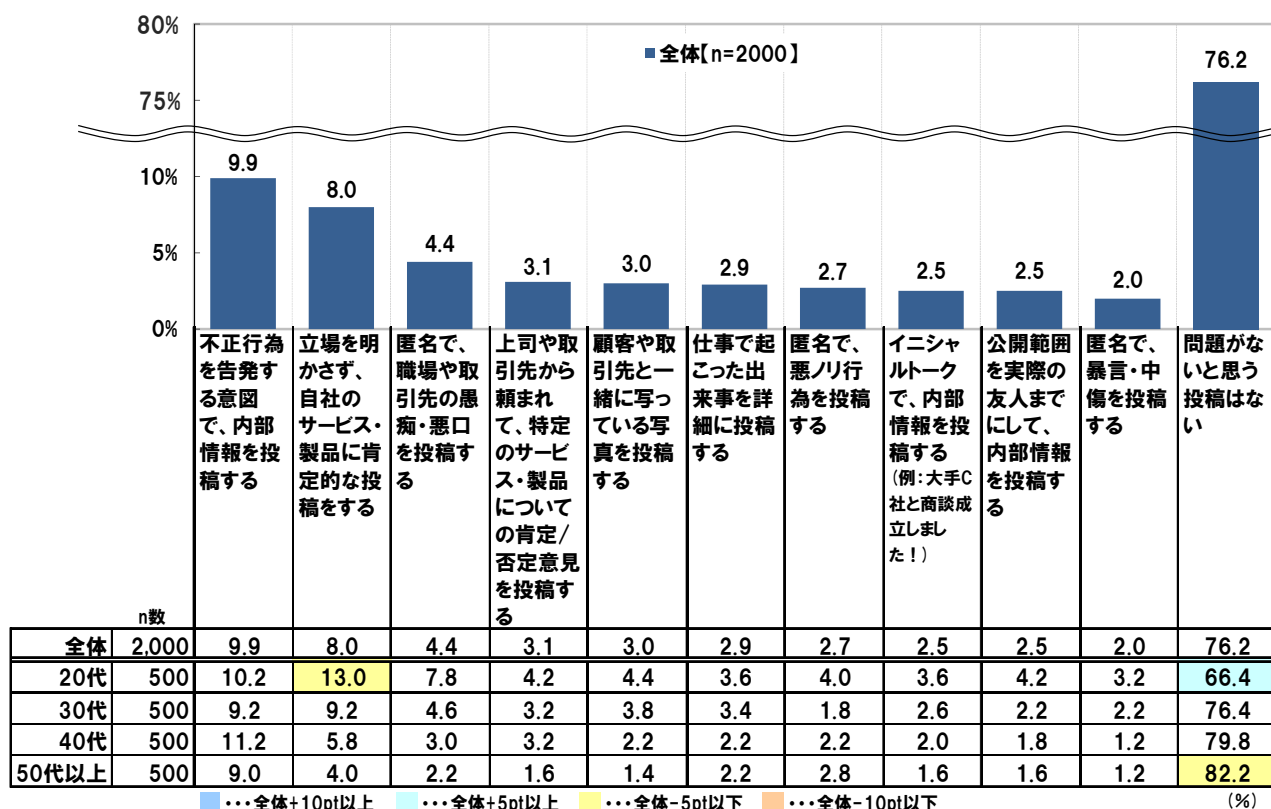
◆「立場を隠してSNSで自社肯定の投稿をしても問題ない」20代で13%

始めに、企業が抱えるソーシャルメディア上の情報漏えいリスクと従業員が起こす“炎上”のリスクを探るため、SNS利用意識に関する質問を行いました。

20歳以上のビジネスパーソン2,000名(全回答者)に対し、業務上の情報漏えいやソーシャルメディアの炎上に繋がりそうな内容の投稿を例示し、SNSの個人アカウントに投稿して“問題ない”と思うものを聞いたところ、「不正行為を告発する意図で、内部情報を投稿する」は1割(9.9%)が問題ないと回答しました。内部告発の意図があれば、勤め先の内部情報を投稿しても問題ないだろうと考えるビジネスパーソンが10人に1人の割合でいるようです。また、“自作自演”や“ステマ(利益誘導)”行為として炎上に繋がりそうな投稿である、「立場を明かさず、自社のサービス・製品に肯定的な投稿をする」(8.0%)や、「上司や取引先から頼まれて、特定のサービス・製品についての肯定／否定意見を投稿する」(3.1%)といった投稿や、身元を特定された場合、勤め先に不利益を及ぼしそうな投稿である、「匿名で、職場や取引先の愚痴・悪口を投稿する」(4.4%)などが上位回答となりました。

年代別にみると、20代は「立場を明かさず、自社のサービス・製品に肯定的な投稿をする」が13.0%と他の年代よりも高くなり、利益誘導行為と取られそうな投稿による炎上リスクについて、危機意識が低い様子が窺えました。

◆SNSの個人アカウントに投稿して“問題ない”と思うもの(複数回答)



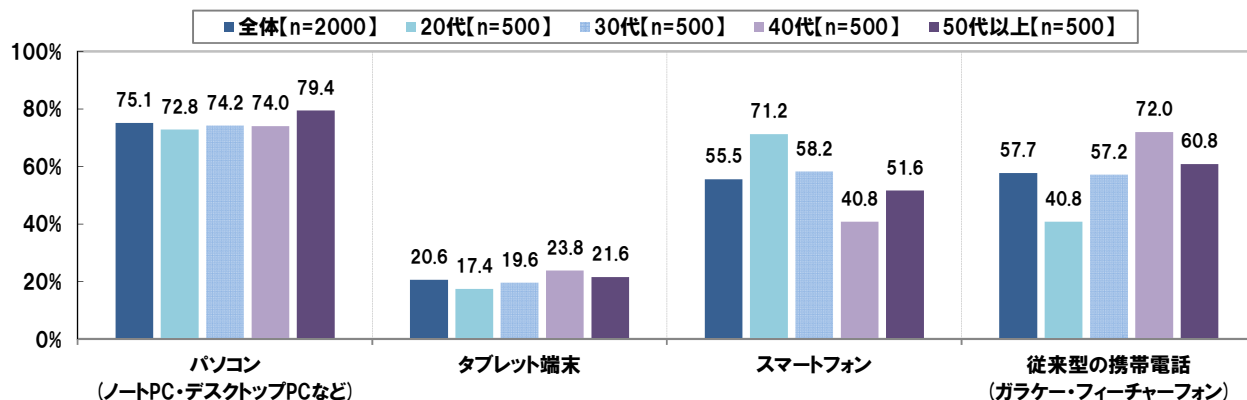
◆ビジネスパーソンの2割がタブレット端末を個人所有、部長職以上では3割半

◆個人所有のPCを業務利用3割強、タブレット端末は3割弱、スマホは4割強

全回答者(2,000名)に対し、個人所有している情報端末を聞いたところ、「パソコン(ノートPC・デスクトップPCなど)」は7割半(75.1%)、「タブレット端末」は2割(20.6%)、「スマートフォン」は5割半(55.5%)、「従来型の携帯電話(ガラケー・フィーチャーフォン)」は6割弱(57.7%)となりました。

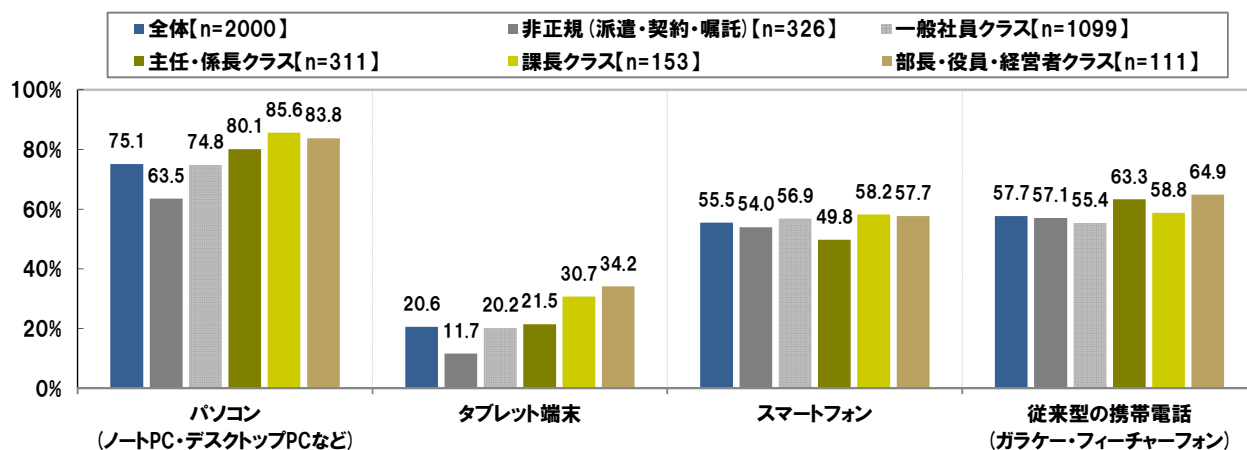
年代別に傾向をみると、20代は「従来型の携帯電話」(40.8%)よりも「スマートフォン」(71.2%)の所有率が高く、40代以上は「スマートフォン」(40代40.8%、50代以上51.6%)よりも「従来型の携帯電話」(40代72.0%、50代以上60.8%)の所有率が高くなっていることがわかります。

◆個人所有している情報端末 年代別(複数回答)



また、役職別にみると、上の役職ほど「タブレット端末」の所有率が高く、課長クラスでは3割(30.7%)、部長・役員・経営者クラスでは3割半(34.2%)の所有率となりました。

◆個人所有している情報端末 役職別(複数回答)

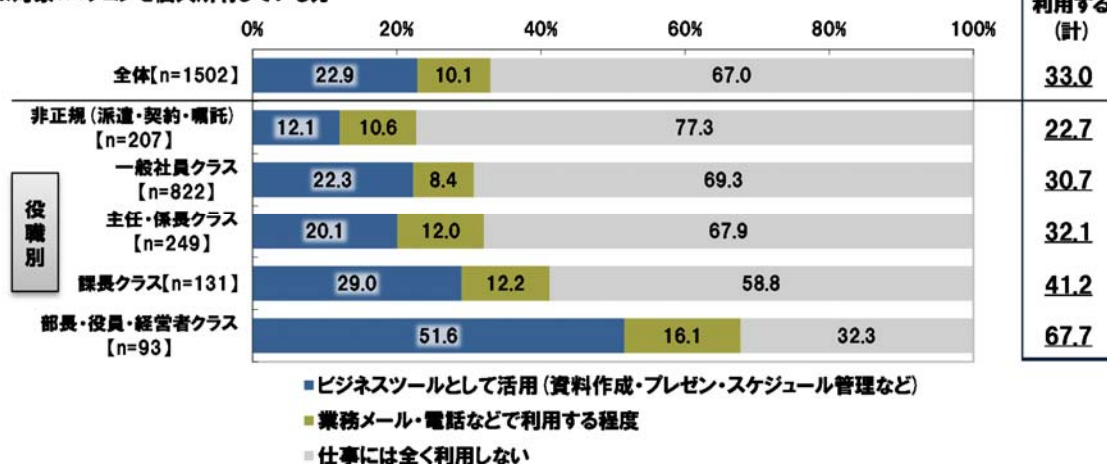


それでは、ビジネスパーソンが個人所有しているこれらの情報端末は、どの程度ビジネスシーンで利用されているのでしょうか。

それぞれの情報端末を個人所有している方に対し、個人所有の情報端末をどの程度仕事で利用するか聞いたところ、個人所有の【パソコン】では、「ビジネスツールとして活用(資料作成・プレゼン・スケジュール管理など)」が22.9%、「業務メール・電話などで利用する程度」が10.1%となり、合計で3割強(33.0%)の方が『仕事で利用する』と回答しました。ビジネスパーソンの3人に1人は個人所有しているパソコンで仕事をするようです。

◆個人所有の【パソコン】をどの程度仕事で利用するか(単一回答)

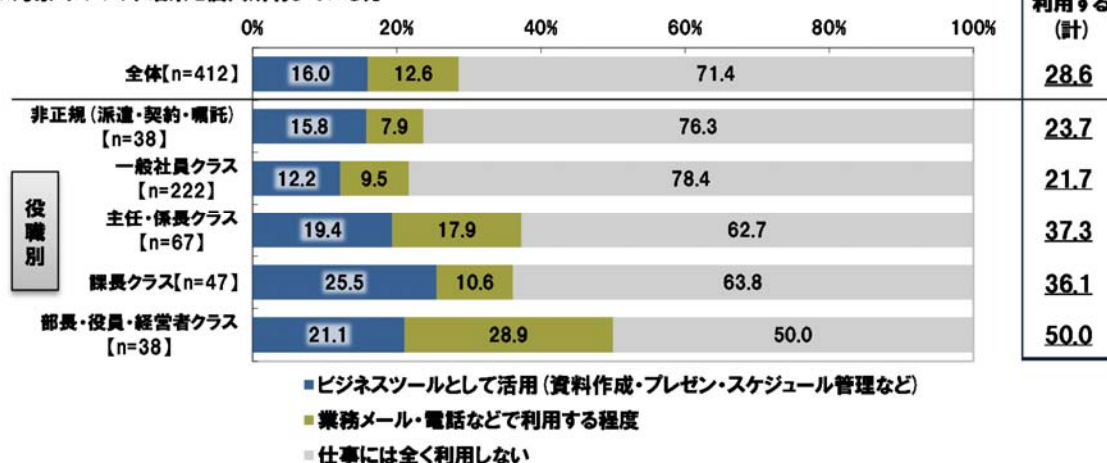
※対象:パソコンを個人所有している方



また、個人所有の【タブレット端末】では、『仕事で利用する』が3割弱(28.6%)となり、部長・役員・経営者クラスでは5割(50.0%)と、半数の割合に達しています。

◆個人所有の【タブレット端末】をどの程度仕事で利用するか(単一回答)

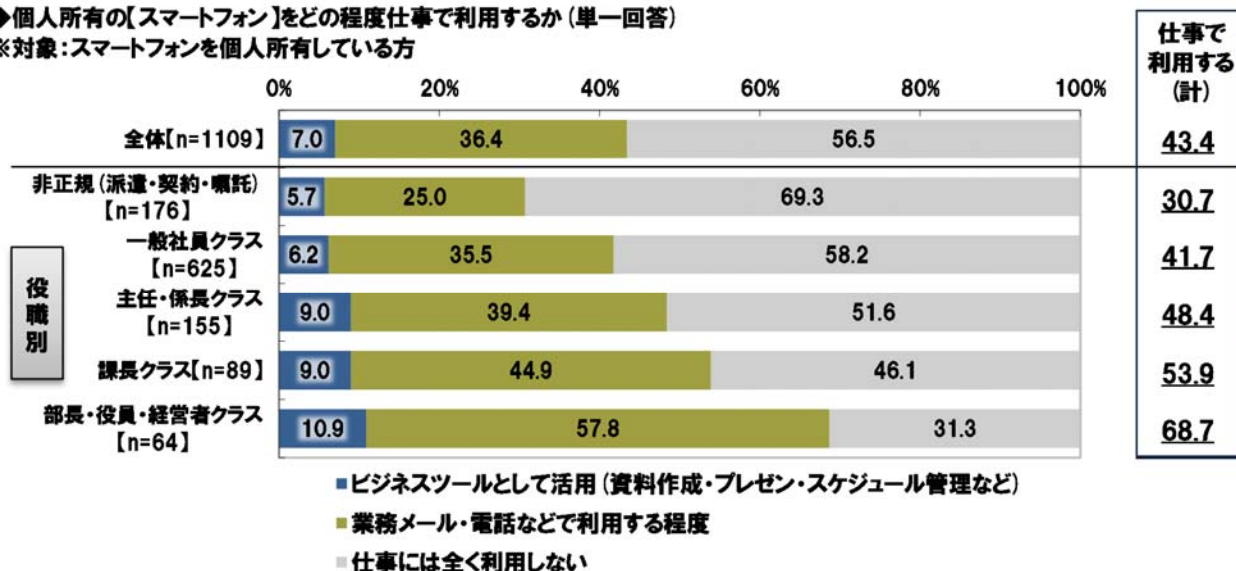
※対象:タブレット端末を個人所有している方



個人所有の【スマートフォン】と【従来型の携帯電話】では、連絡手段として利用されることが少なくないようで、「業務メール・電話などで利用する程度」の割合が他の情報端末に比べて高く(スマートフォン36.4%、従来型の携帯電話49.3%)、『仕事で利用する』割合は【スマートフォン】では4割強(43.4%)、【従来型の携帯電話】では5割強(52.9%)となりました。

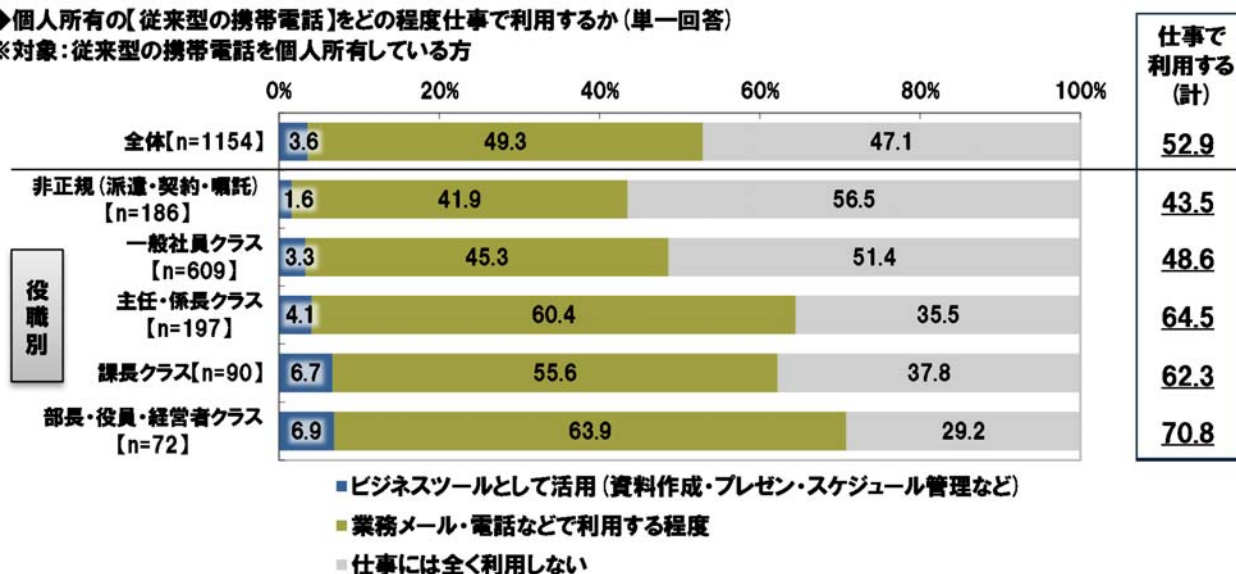
◆個人所有の【スマートフォン】をどの程度仕事で利用するか(単一回答)

※対象:スマートフォンを個人所有している方



◆個人所有の【従来型の携帯電話】をどの程度仕事で利用するか(単一回答)

※対象:従来型の携帯電話を個人所有している方



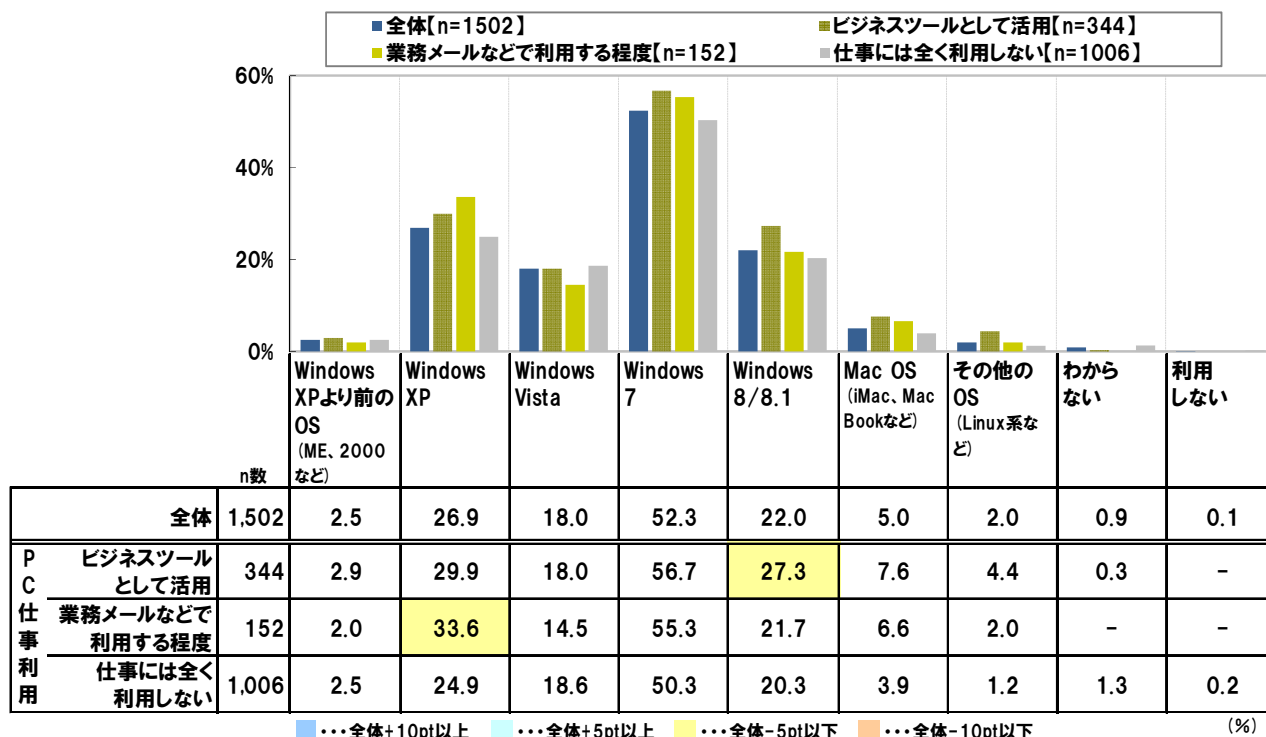
- ◆個人PCで業務メールするビジネスパーソン 3人に1人がXP使用
- ◆半数近くはノーガード?「スマホ・タブにパスワード設定」5割強、「セキュリティソフト利用」は5割弱
- ◆公衆無線LAN利用時のセキュリティ対策は不十分?
「公衆無線LANで大事な情報やり取りをしない」2割弱、「無線LAN暗号化の規格をチェックする」1割
- ◆生活者視点では厳しい態度「情報流出歴のある会社のサービスは利用しない」16%

個人所有の情報端末を業務利用する方が少なくないことがわかりましたが、ビジネスパーソンはどの程度、情報漏えいリスクの管理を行なっているのでしょうか。

パソコンを個人所有している方(1,502名)に対し、利用しているパソコンのOSを聞いたところ、「Windows XP」が26.9%、「Windows 7」が52.3%、「Windows 8/8.1」が22.0%となりました。

また、個人所有のパソコンを業務メールなどで利用すると回答した方は、サポートの終了した「Window XP」を継続利用している割合が3人に1人の割合(33.6%)となりました。サポートが終了したOSは、サポートが継続しているOSに比べて、マルウェアの感染などによる情報漏えいリスクが高まっているため、ビジネスパーソンが個人のパソコンを業務利用している状態は、組織の管理が及ばないところで予期しない情報漏えいリスクに晒されている可能性があります。

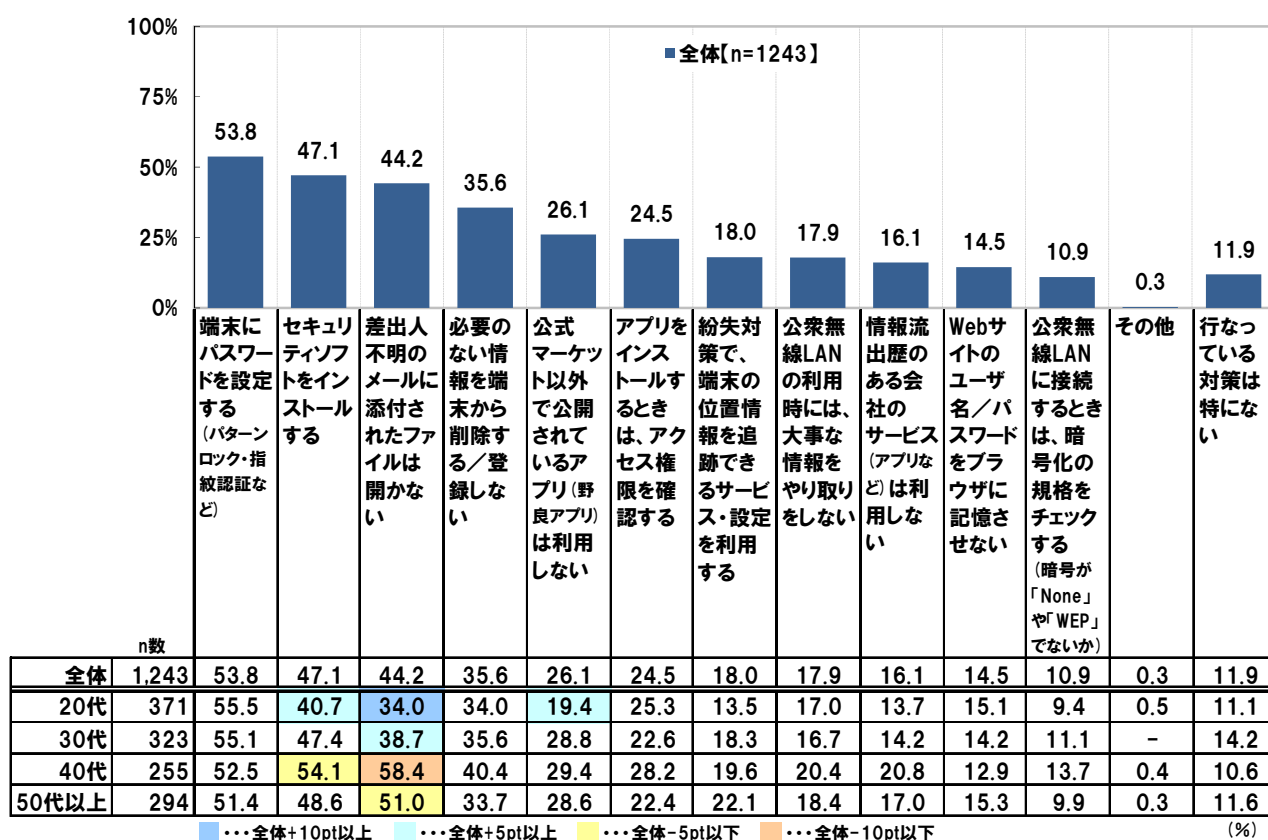
◆個人利用しているパソコンのOS(複数回答) ※対象:パソコンを個人所有している方



続いて、スマートデバイス(スマートフォン・タブレット端末)を個人所有している方(1,243名)に対し、個人所有のスマートデバイスで行なっているセキュリティ対策を聞いたところ、「端末にパスワードを設定する(パターンロック・指紋認証など)」が5割強(53.8%)で最も高くなりました。見方を変えると、端末のパスワード設定でさえも、実施している方は半数程度に留まっていると言えます。以下、対策を行なっている割合は半数を下回り、「セキュリティソフトをインストールする」(47.1%)や「差出人不明のメールに添付されたファイルは開かない」(44.2%)は4割台、「必要のない情報を端末から削除する／登録しない」は3割半(35.6%)の割合となりました。そのほか、公衆無線LANの利用に際し、セキュリティ対策を意識している割合はそれぞれ1割台で低く、「公衆無線LANの利用時には、大事な情報のやり取りをしない」は17.9%、「公衆無線LANに接続するときは、暗号化の規格をチェックする(暗号が「None」や「WEP」でないか)」は10.9%となっています。他方で、「情報流出歴のある会社のサービス(アプリなど)は利用しない」は16.1%となっており、生活者の視点では、企業の情報漏えいに対して厳しい態度を取っている様子も窺えました。

◆個人所有のスマートデバイスで行なっているセキュリティ対策(複数回答)

※スマートデバイス(スマートフォン・タブレット端末)を個人所有している方



◆個人端末に内部資料を保存「禁止されている」職場は 4 割強、5 割強の職場はルールを整備・周知不足

◆仕事の持ち帰りに関するルール、整備・周知不足の職場が 5 割

◆ビジネスパーソン個人の個人端末は職場の機密情報の山？

「内部資料入っている」1 割半、「仕事を持ち帰って自宅作業」2 割弱、「顧客の連絡先登録してある」2 割強

◆スマートデバイス普及で“シャドーIT”増加？

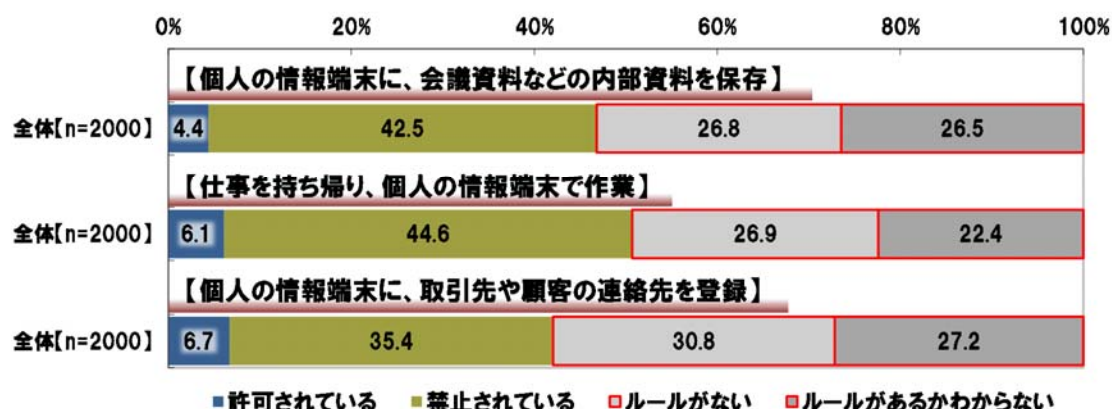
ルール未整備の職場では「個人端末に内部資料保存」3 割弱が実行、「顧客の連絡先登録」は 4 割

ビジネスパーソンが個人所有している情報端末からの情報漏えいリスクが浮き彫りになりましたが、職場では、どの程度、私的利用端末の業務利用についてのルール整備が進んでいるのでしょうか。

全回答者(2,000 名)に対し、仕事の持ち帰りなど、私的利用端末への業務情報持ち出しに関する、職場のルール整備状況を聞いたところ、【個人の情報端末に、会議資料などの内部資料を保存】では、「許可されている」は 4.4%、「禁止されている」は 42.5%となりました。内部資料を私的利用端末に保存することを許可している職場は 1 割以下と少数派で、禁止している職場が多いようです。また、「ルールがない」は 26.8%、「ルールがあるかわからない」は 26.5%となり、合わせて 5 割強(53.3%)の職場では、内部資料を私的利用端末に保存することに対し、『ルールの整備・周知不足』の状態であることが明らかになりました。

そのほかの質問項目についても『ルールの整備・周知不足』の割合は同様の水準で、【仕事を持ち帰り、個人の情報端末で作業】では 5 割(49.3%)、【個人の情報端末に、取引先や顧客の連絡先を登録】では 6 割弱(58.0%)となりました。

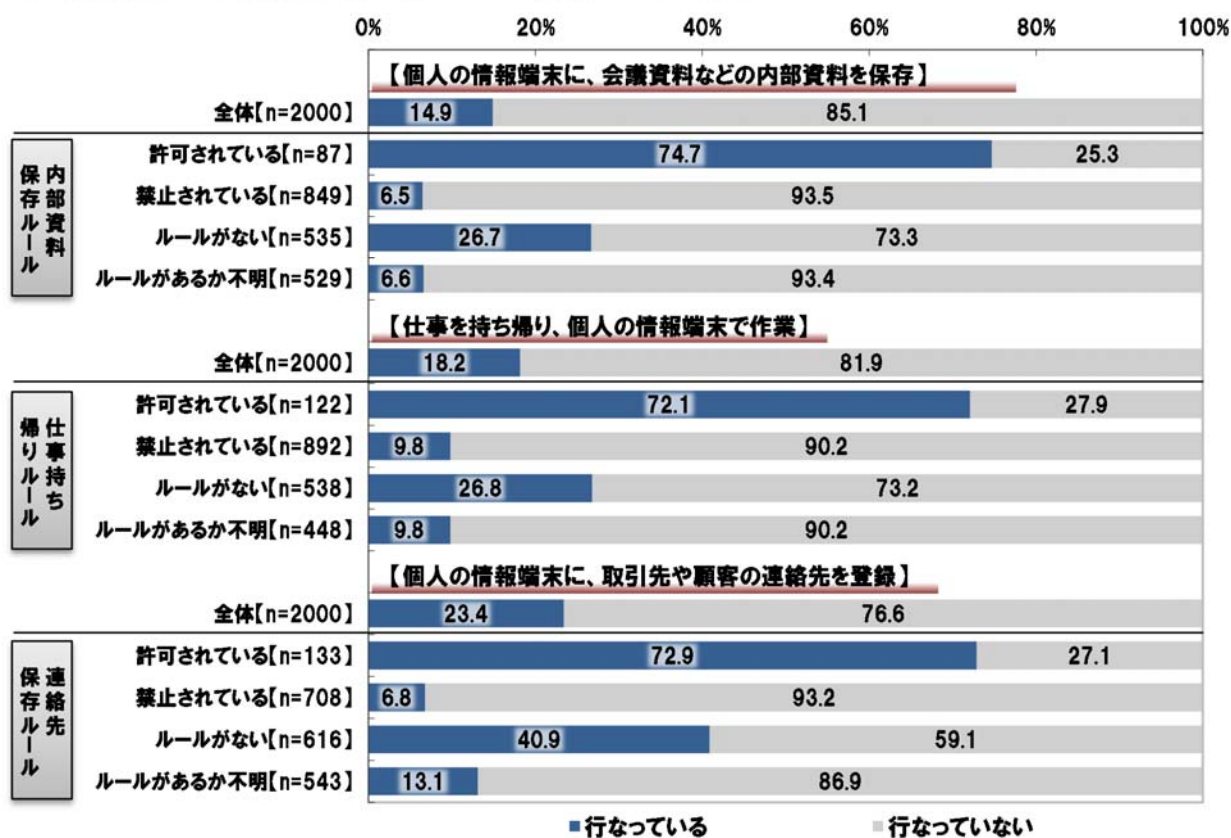
◆私的利用端末への業務情報持ち出しに関する、職場のルール整備状況（項目ごとに単一回答）



続いて、私的利用端末への業務情報持ち出しを行っているか聞いたところ、【個人の情報端末に、会議資料などの内部資料を保存】では、「行なっている」割合が1割半(14.9%)となりました。職場のルール整備状況別にみると、禁止されている職場では6.5%、ルールがない職場では26.7%の割合で内部資料が保存されていることがわかります。スマートデバイスの普及に伴い、これらの“シャドーIT(許可されていない私的利用端末やサービスの業務利用)”による、情報漏えいリスクに晒されている職場も増加傾向にあるのではないのでしょうか。

そのほか、【仕事を持ち帰り、個人の情報端末で作業】では、「行なっている」割合が18.2%、禁止されている職場では9.8%、ルールがない職場では26.8%と、同様の傾向となりました。また、【個人の情報端末に、取引先や顧客の連絡先を登録】では、「行なっている」割合が23.4%とおおよそ4人に1人の割合となり、ルールがない職場では、4割(40.9%)となっています。

◆私的利用端末への業務情報持ち出しを行っているか(項目ごとに単一回答)



◆情報漏えいの3大ヒヤリ・ハット？

「居酒屋でオフレコトーク」「机上に放置・引き出し未施錠」「FAXを誤送信」

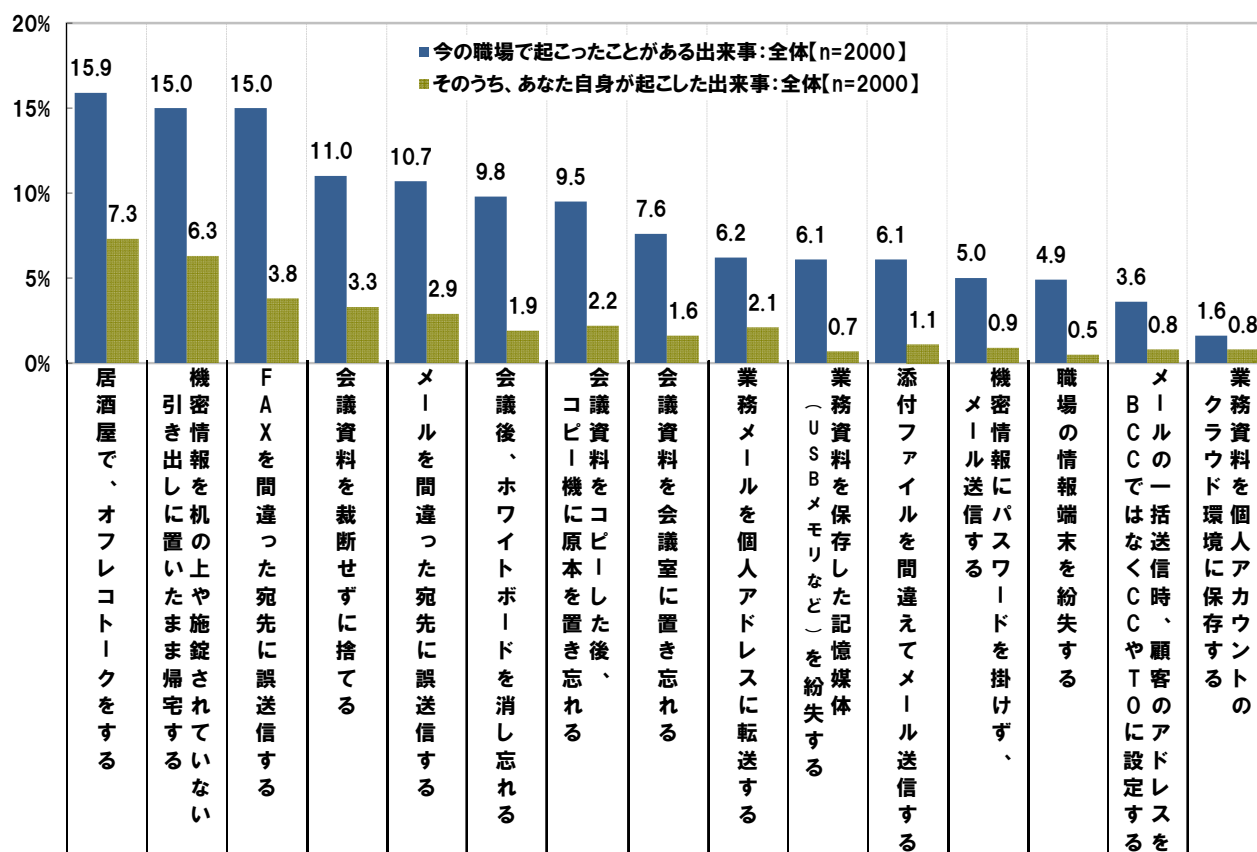
◆あわや情報漏えい事件に発展！？会議情報の漏えいヒヤリ・ハット

「会議資料が裁断されずゴミ箱へ」「1割が目撃」「ホワイトボード消し忘れ」「コピー機に原本放置」なども

では、実際に職場で情報漏えいのトラブルやヒヤリ・ハットは、どの程度起こっているのでしょうか。

今の職場で起こったことがある出来事を聞いたところ、「居酒屋でオフレコトークをする」(15.9%)や「機密情報を机の上や施錠されていない引き出しに置いたまま帰宅する」(15.0%)、「FAXを間違った宛先に誤送信する」(15.0%)などが1割半で続き、情報漏えいの3大ヒヤリ・ハット事例となりました。また、機密度の高い情報を扱うことも多い、会議に関連する項目では、「会議資料を裁断せずに捨てる」(11.0%)や「会議後、ホワイトボードを消し忘れる」(9.8%)、「会議資料をコピーした後、コピー機に原本を置き忘れる」(9.5%)、「会議資料を会議室に置き忘れる」(7.6%)などがそれぞれ1割前後の割合で上位回答となり、会議の資料や情報が適切に管理されないために、機密情報が漏えいしかねない事態が起こっている職場が散見されました。

◆今の職場で起こったことがある出来事／そのうち、あなた自身が起こしたこと（項目ごとに複数回答）



- ◆部長職以上の6割半が「情報漏えい対策に不安なし」、一般社員では5割強に留まる
- ◆「情報漏えい対策は社員教育が大事」9割強も、「職場内にどんなに教育してもダメな人がいる」6割半
- ◆「情報漏えい対策を優先すると業務効率を損なう」5割強、タブレットをビジネスに活用中の方は7割半が同意

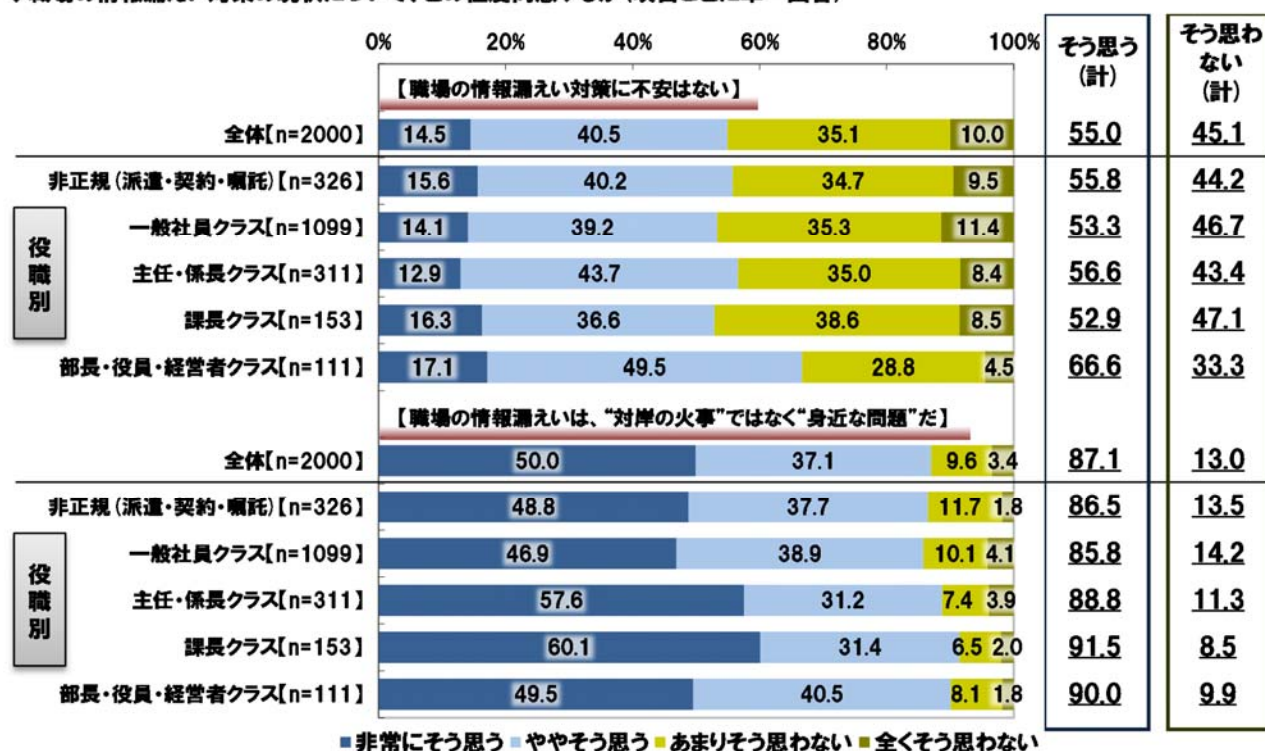
職場の情報漏えい対策の現状についてどのように感じているか、質問を行いました。

全回答者(2,000名)に対し、【職場の情報漏えい対策に不安はない】の項目に、どの程度同意するか聞いたところ、『そう思う』(非常に+やや、以下同様)が55.0%、『そう思わない』(全く+あまり、以下同様)が45.1%となりました。

役職別にみると、部長・役員・経営者クラスでは『そう思う』が66.6%となり、一般社員クラス(53.3%)などと比較して、不安がないとする割合が高くなりました。情報漏えい対策の実施状況について、現場側と管理側とで、意識にギャップがある様子が窺えます。

また、【職場の情報漏えいは、“対岸の火事”ではなく“身近な問題”だ】の項目では、『そう思う』が9割弱(87.1%)となり、情報漏えいについて、決して人ごとではないと危機感を抱いている様子が窺えました。

◆職場の情報漏えい対策の現状について、どの程度同意するか(項目ごとに単一回答)

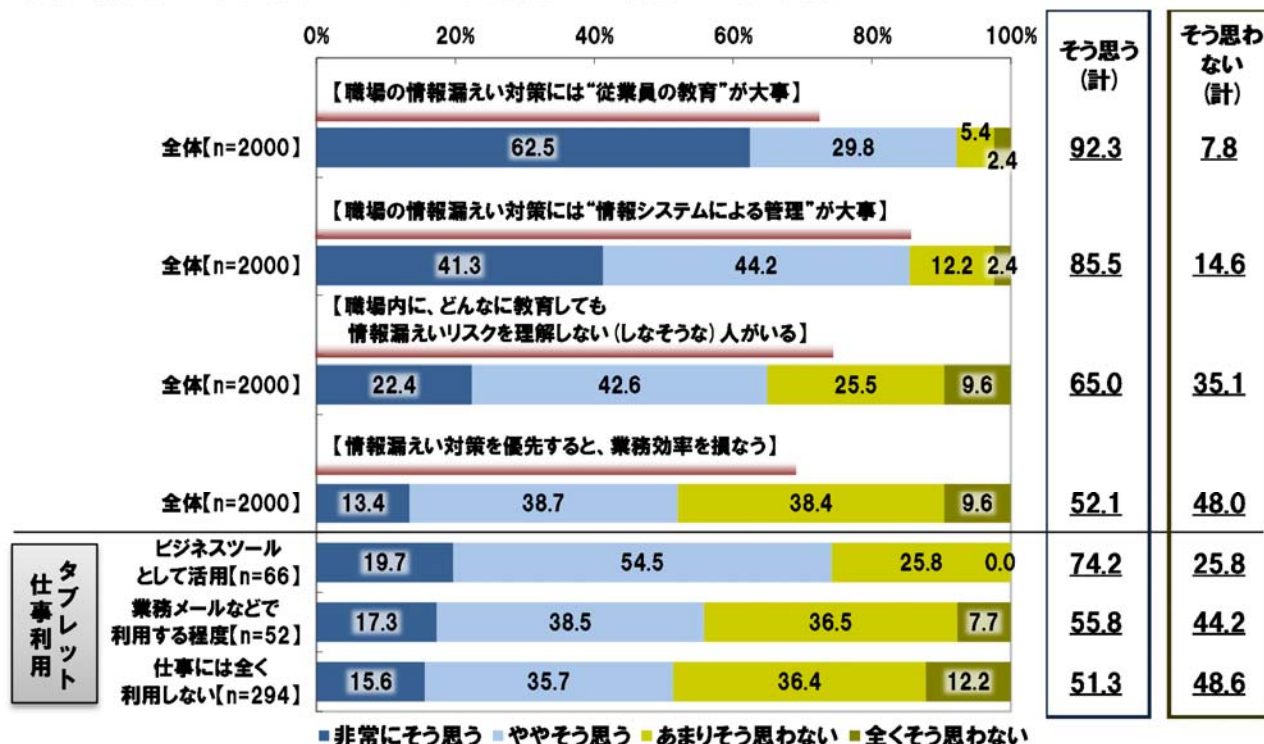


同様に、職場の情報漏えい対策の強化について聞いたところ、【職場の情報漏えい対策には“従業員の教育”が大事】では、『そう思う』が9割強(92.3%)、【職場の情報漏えい対策には“情報システムによる管理”が大事】では、『そう思う』が8割半(85.5%)となりました。内部情報を扱う従業員の教育とIT技術によるシステムの管理のどちらも重要だと考えられているようです。

他方で、【職場内に、どんなに教育しても情報漏えいリスクを理解しない(しなそうな)人がいる】では、『そう思う』が6割半(65.0%)となり、教育による対策の限界を感じている様子が窺えます。

また、【情報漏えい対策を優先すると、業務効率を損なう】では、『そう思う』が5割強(52.1%)となり、個人所有のタブレット端末をビジネスツールとして活用している方では7割半(74.2%)となりました。セキュリティを強化することで、手続きの煩雑化や極端な利用制限が起こり、生産性の低下に繋がることを不安視している様子が窺えました。

◆職場の情報漏えい対策の強化について、どの程度同意するか(項目ごとに単一回答)



以 上

本件に関するお問い合わせ先

本リリースに関するご質問などは、以下までご連絡お願いいたします。

■本社 営業本部

電話 : 045-324-2898
Eメール : sonoba@cij.co.jp
FAX : 045-322-2798