企業におけるモバイルデバイスの利活用と情報漏洩対策に関する実態調査

ヒアリング報告書

別冊　調査報告書、調査票

2015 年 7 月 31 日

モバイルコンピューティング推進コンソーシアム

セキュリティ委員会

はじめに

MCPC（モバイルコンピューティング推進コンソーシアム、会長：安田靖彦）は、ノートPCや携帯電話スマートフォンを業務に活用しているビジネスユーザーを対象として、モバイル機器の使用状況やネットワークの利用状況と将来へのニーズに関する調査を実施し、その調査結果ならびに分析結果をまとめましたので、お知らせいたします。

１．調査の背景

移動体通信サービスの高速化、エリアのシームレス化、ならびにモバイルデバイス（ノートPC、タブレット、スマートフォン等）の高度化が着実に進展しております。一方、モバイルデバイスの業務利用に関しては、BYOD 等の自由な利用形態がみられる一方、移動業務での利用が忌諱される例が散見されている。

MCPC は、さらなるモバイルコンピューティングの生産性向上を目指した利活用・普及促進を目的に、モバイルデバイスを業務に活用しているビジネスユーザーを対象として、個人情報取り扱いに関するセキュリティポリシーが、デバイスの利活用とどう関係するか、使用状況や、ネットワークの利用状況、普及の疎外要因、将来へのニーズ、等を調査いたしました。

(1) 調査期間：2014 年 5 月 20 日～5 月 22 日
(2) 調査方法：インターネット調査
(3) 有効回答数：522 名

【MCPC について】

MCPC（モバイルコンピューティング推進コンソーシアム 会長：安田靖彦）は、業界を超えたモバイルコンピューティングの普及促進団体として 1997 年に発足いたしました。端末インターフェースガイドライン及び Bluetooth など多数の標準化作業をはじめ、「セキュリティ対策ガイド」発行、「MCPC モバイルソリューションフェア」開催、「モバイルシステム技術検定」実施などを通して、モバイル市場の拡大に貢献しております。

MCPC 加盟企業 155 社 （2015 年 7 月現在）

モバイルコンピューティング推進コンソーシアム（MCPC） 事務局
所在地 ： 〒105-0011 東京都港区芝公園 3-5-12 長谷川グリーンビル 2F
TEL ： 03-5401-1935 FAX ： 03-5401-1937
URL ： http://www.mcpc-jp.org/ E-mail： office@mcpc-jp.org

目次

1 調査概要

1-1 調査の目的

紛失や盗難による情報漏洩の懸念から、社外持ち出しが禁止・制限されることが多くなっていたモバイル PC（パソコン）を、改めて社外に持ち出して使おうとする企業が増えてきている。

持ち出し禁止措置が広がる発端となった個人情報保護基本法の完全施行から 10 年近くが経過しそれぞれの業種・業態に応じた運用ノウハウが企業の間に蓄積されてきたことに加えて、フルディスク暗号化（FDE）※1、遠隔データ消去※2、シンクライアント※3 などの情報漏洩対策ソリューションの普及により、情報漏洩リスクを大きく低減できるようになったことが、その大きな要因といってよいだろう。

オフィスと同様のコンピューティング環境を外出先でも利用できるモバイル PC は、言うまでもなく企業の業務効率化の有力なツールである。これらを有効に活用していくことは、企業の生産性向上、さらには日本経済が成長を目指す上で不可欠といってよい。近年はスマートフォンやタブレット端末などのスマートデバイスを積極的に業務に活用する企業も増加しており、PC とこれらを合わせたモバイルデバイスを社外で安全に利用できる環境の整備は、企業にとって喫緊の課題と言える。

こうした状況を踏まえて、MCPC では、2010 年と 2013 年にモバイルデバイスの紛失・盗難に伴う情報漏洩対策に大きな効果を発揮する遠隔データ消去ソリューションの市場概況に関する調査を実施した。

さらに 2014 年 6 月にはエンドユーザーのモバイルデバイスの利活用の状況と意識を把握するために Web 上で「企業におけるモバイルデバイスの積極的な利活用における個人情報保護法の影響調査」を実施している。

本調査はこれらの調査を深める意味から、企業の具体的なモバイルデバイスの活用の現状と課題などについて、実際にこれらの運用を担っている情報システム担当者に対してヒアリングを行ったものである。本調査が、企業がモバイルデバイスを活用する上での参考になれば幸いである。

1-2 調査の対象

本調査は、MCPC の会員及び非会員企業の中から、モバイルデバイスを積極的に活用している企業を選出、情報システム部門（あるいはモバイルデバイスの持ち出しを所管して

いる部門）に調査の趣旨を打診し、協力を得られた 6 社に対してヒアリングを行ったものである。企業の選出にあたっては業種・業態をある程度網羅することを意識した。

調査の対象とするモバイルデバイスは、モバイル PC とスマートフォン、タブレット端末とした。ここでいうモバイル PC は、企業で広く導入されている Windows 搭載コンピューターの中で、バッテリーで動作し持ち運びが可能なもの、具体的には小型・軽量のノート PC 及びタブレット PC（Windows OS 搭載のタブレット端末）を意味する。MacOS や Linux 搭載の同種のコンピューターも対象になると考えられるが、今回の調査企業には、汎用クライアントとして社内で利用されているケースはなかった。

スマートフォンとタブレット端末は、Android、iOS を搭載したものを調査対象とした。

調査対象企業の具体的なセキュリティ対策に関する内容が含まれることから、報告書には企業名は記載せず、業種・業態の概略を示すにとどめた。

【ヒアリングを実施した企業】

企業	従業員数（国内）	社外に持ち出されている モバイルデバイス （スマートフォンを除く）
A 社（製造業、日用雑貨）	約 1500 名 （グループ企業を含む）	モバイル PC （約 900 台）
B 社（保険業）	1 万名強	タブレット端末 （3000 台）
C 社（製造業、IT ソリューション）	約 10 万名	シンクライアント対応 PC （1 万 9000 台） 遠隔データ消去対応 PC （1 万 4000 台）
D 社（製造業、IT ソリューション）	約 10 万名 （グループ企業を含む）	モバイル PC （数千台～1 万台程度）
E 社（製造業、ソフトウェア・IT サービス）	約 800 名	モバイル PC （約 8 00 台）
F 社（流通業）	5 万名超 （グループ全体）	モバイル PC （1000 台程度） タブレット端末 （1000 台程度）

1-3　調査の方法

ヒアリングでは、企業におけるモバイルデバイスの利用状況と、運用上の大きな課題となる情報漏洩対策を主な調査テーマとした。

あわせて将来のモバイルデバイスの利用計画についても尋ね、モバイルデバイス活用の方向性を把握することを試みた。

また、企業のモバイルデバイスの利活用・情報漏洩対策を大きく左右している、行政及び公益団体の個人情報保護に関するガイドラインに対する意識、これらへの具体的な対策についても調査した。

主な質問項目は以下の通りである。

①企業の概要
②情報システムの概要
③モバイルデバイス（ノート PC、タブレット端末、スマートフォン）の利用実態
④モバイルデバイスの紛失・盗難対策
⑤個人情報保護対策
⑥行政（及び各種団体）の個人情報保護ガイドラインへの意識及び対応
⑦モバイルデバイス活用の今後の方向性

調査は、上記のヒアリングに基づいて基本データをとりまとめ、MCPC セキュリティ委員会で内容を検証する形で行った。

ヒアリングは 2014 年 5 月下旬から 6 月にかけて実施した。記述内容は基本的には 2014 年 9 月上旬のものである。

※1　フルディスク暗号化(FDE:Full Disk Encryption)

モバイルデバイスに内蔵されたストレージ（HDD/SSD など）上のデータをユーザーが意識することなくすべて暗号化できるソリューション

※2　遠隔データ消去ソリューション

管理者の遠隔指示により、モバイルデバイスのストレージ上のデータを削除、あるいはデータへのアクセスを不能にする機能をもつ盗難・紛失、情報漏洩対策製品・サービス

※3　シンクライアント(Thin client)

処理の大半をサーバー側に集中させるコンピューターシステムの総称。クライアントには基本的にはデータが保存されない。具体的な実現技術として仮想デスクトップ（VDI：Virtual Desktop Infrastructure)などがある

2　企業ヒアリング

2-1　A 社（製造業、日用雑貨）

2-1-1 企業の概要

A 社は日用品の製造・販売を手掛けるナショナルブランドメーカーである。産業向け資材を製造する会社など 20 越える企業グループの中核会社でもあり、グループ全体での売上は 1000 億円を超える。主要な営業拠点を東京と大阪に置いており、国内数カ所に工場を持つ。グループ企業は海外にも工場や拠点を持っており、A 社グループの総従業員数はグローバルで約 3000 名。うち約 1500 名、A 社単独では約 1000 名が国内に勤務している。

2-1-2 情報システムの概要

国内ではグループ企業を結ぶ社内ネットワークが整備されており、その上で汎用機から移行した基幹系システムと、交通費精算など多数の Web ベースの情報系システムが利用できる。この他に、グループ企業や部門の独自システムも運用されている。

従業員には原則として PC（OS は Windows 7）が 1 人 1 台（工場を除く）貸与されており、これが基幹系・情報系システムのクライアントとなる。これらの PC の内 8 割がノート PC である。その多くが小型・軽量のモバイル PC で、全体の 6 割程を占める。発注業務など携わる従業員には複数台の PC が貸与されている。

2-1-3 モバイルデバイスの社外持ち出しの現状

貸与されているノート PC を外に持ち出すことが認められている。持ち出しには事前に許可を受ける必要があり、900 台が許可を得ている。

社外に持ち出す PC は HDD 内のデータを暗号化（フルディスク暗号化）することが義務付けられており、申請時に利用規約への同意書の提出が求められる。

社内ネットワークに VPN でセキュアにアクセスできるリモートアクセス環境も整備されているが、利用に際してライセンスフィーに相当するコストが情報システム部門から利用部門に請求されることもあり、VPN 利用者は持ち出し許可を受けているユーザーの 7 割程にとどまる。VPN 利用者には希望に応じて USB 接続タイプのモバイルデータ通信端末が貸与されるが、利用者は 170 名程にとどまっており、多くは自宅のインターネット接続環境などを介して VPN を利用している。

社外持ち出しの許可を受け、VPN のアカウントの付与されることで、社内と同様の環境を外出先で利用することが可能となる。業務を自宅に持ち帰ることは基本的には認められ

ていないが、テレワークが可能な環境は整備されていることになる。

A 社で、モバイル PC が多用されている理由の 1 つとして挙げられるのが、拠点が複数のビルに分散しているケースが多く、会議などで他のビルに PC 持ち運んで利用する必要があることだ。こうしたケースでは必ずしも上記の持ち出し許可を得る必要はないが、紛失などの事故に備え、モバイル PC にはすべてフルディスク暗号化が導入されている。

2-1-4 モバイルデバイスの情報漏洩対策

前節で述べたように A 社ではモバイル PC にフルディスク暗号化（McAfee Endpoint Encryption）が導入されており、これが盗難、紛失による情報漏洩の対策の基本となっている。

もう 1 つ、運用面での情報漏洩対策の柱となっているのが、業務データをネットワーク上のファイルサーバーに保存し、原則的に PC:内にデータを置かないようにしていることだ。とはいえ、ある程度のデータは PC に保存せざるを得ないことから、最終的には暗号化と ID・パスワードによる認証が情報漏洩対策の要となる。

モバイル PC の盗難・紛失などが発生した場合は、エンドユーザーは上長を経由して情報システム部門に速やかに届け出て、PC 内に保存しているデータの内容を申告することが求められる。警察への盗難・紛失の届け出も義務付けられている。

この他にも情報漏洩対策として、①USB メモリなどによる情報流失を防止するために、会社貸与の USB メモリ以外の外部ストレージへのデータのダウンロードが行えない設定にしていること、②マルウェアの感染による情報流出を防止するためのセキュリティソフトを導入するなどの施策が採られている。

2-1-5 個人情報の取り扱い

A 社では 30 年程前に通信販売事業を開始、これを機に個人情報管理の管理を強化した。個人情報保護基本法が施行された 10 年程前からは、顧客情報を専用データベースで管理し、通信販売事業の担当部署の中でも数名の顧客情報管理担当者以外はデータベースにアクセスできないようにするなど、運用の厳格化が図られた。

業務で顧客情報を必要とする場合は担当者に依頼してデータを出してもらうことになるが、顧客情報を PC 内に保存することは禁止されており、PC の紛失・盗難により顧客情報が流出する可能性は基本的には存在しない。

この他、営業部門がキャンペーンなどで取得した個人情報などについては、部門毎にルールを決めて管理されている。こうした運用を行うことで、現在のところ個人情報の流出といった事案は発生していないという。

2-1-6 モバイルデバイス活用の方向性

A 社ではフルディスク暗号化に一定の信頼を置いた上で、モバイル PC の社外利用を広く認めている。顧客情報を特定部署で管理し、一般社員の PC 上には問題となる情報が存在しない環境を整備することで、こうした運用を可能にした。より強固なセキュリティ対策としてシンクライアントの導入も検討されている。

2-2 B 社（保険業）

2-2-1 企業の概要

B 社は従業員数が 1 万名を超える大手の保険会社である。全国に 500 を超える営業拠点を持ち、代理店経由で保険販売を行っている。

2-2-2 情報システムの概要

全国の拠点を結ぶイントラネットが構築されており、これを介して保険の契約内容の確認や保険料の試算等を営業担当が自席の PC で行えるシステムが基幹系として整備されている。この機能を一部切り出す形で代理店向けのシステムも提供されている。

イントラネット上では、電子メールなどの情報系システム、会計システムや各部署の業務システムも運用されている。

2-2-3 モバイルデバイスの社外持ち出しの現状

営業社員には 1 人 1 台 PC が支給されている。その大半がノート PC であるが、原則として社外持ち出しは認められていない。これは業務自体が顧客情報（個人情報）と不可分であるためである。

そこで営業担当は外出先での営業活動を行い帰社後にメール確認や資料作成等を行う、契約内容の照会も電話で会社に問い合わせるなど、必ずしも効率的とはいえない形で業務を行ってきた。顧客や代理店への説明も主に紙の資料が用いられている。

こうした状況を改善するために、B 社では数年前から Android タブレットの導入を開始、現在 3000 台が稼働している。この Android タブレットには LTE の通信モジュールが内蔵されており、基幹システムにアクセスして自席でできる作業の多くを行うことが可能になっている。これにより業務効率の大幅な改善が実現された。

代理店では、保存データが暗号化された PC を顧客宅に持ち出して契約などの手続きを行うことが認められている。過去は主にローカル型のシステムにより帰社後に同期を取るといった運用が行われてきたが、最近では PC 内にデータを残さない Web ベースのシステムが使われることが多くなっている。Web ベースのシステムには契約内容の照会や変更に客

先で対応できるというメリットもある。

2-2-4 モバイルデバイスの情報漏洩対策

B 社ではノート PC の社外持ち出しを禁止しているため、紛失・盗難による情報漏洩リスクは基本的には存在しない。持ち出し用として導入が進んでいるタブレット端末も①端末内にデータをダウンロードできない設定としていること、②複数の認証を組み合わせて不正アクセスを防止することにより、情報漏洩リスクを回避している。

社内の PC についてもデータを内蔵の HDD ではなく、電子キャビネットに保存する形での運用が徹底されており、電源が切れると原則としてローカルデータは全て消去される。そのため仮に社内の PC が盗難にあっても情報漏洩にはつながらない。

その他、①外部とのメールのやり取りでは添付データの暗号化が必須となっており、暗号がかかっていないファイルを添付したメールはシステムが送信を止める、②USB メモリや CDROM などへのデータのコピーも、システム上で上司の承認を受けないと実施できないなど、厳格な情報漏洩対策が行われている。

代理店ではノート PC の社外持ち出しが可能だが、システムから出力した情報は暗号化される仕組みになっていることや蓄積される情報がその日の営業活動に限られることなどから、盗難、紛失による情報漏洩のリスクは小さい。PC に情報を保存しない Web ベースのシステムへ移行することで情報漏洩リスクを回避することが可能になる。

2-2-5 個人情報の取り扱い

保険業では、営業部門などが扱う情報の多くが個人情報であることから、PC の社外持ち出しの制限だけでなく、PC 内に蓄積されている情報の管理も非常に厳格に行われている。プライバシーマークも制度創設時から取得している。

PC を持ち出して使うケースが多い代理店では、過去、年に数件ほど紛失事故が発生していたというが、Web 化の進展により件数は減少している。紛失事故が発生した場合は金融庁に届け出を行う必要がある。

2-2-6 モバイルデバイス活用の方向性

B 社では、ノート PC の持ち出し制限による問題点をタブレット端末の導入により改善し業務効率の大幅な改善を実現した。現行の Android タブレットは、持ち運び易さや起動の速さにメリットがある反面、入力業務に不向きであるなど課題もあるため、社内 PC のシンクライアント化も検討している。

2-3　C 社（製造業、IT ソリューション）

2-3-1 企業の概要

C 社は日本を代表する IT ソリューション企業で、企業や官公庁、通信事業者などの法人顧客向けに多彩な事業を展開している。従業員業数は約 10 万人。

2-3-2 情報システムの概要

全国の拠点を結ぶ社内ネットワークが整備されており、その上で検証用システムを含め数千台のサーバーが稼働している。従業員には業務用として 1 人 1 台の PC（Windows 7 搭載機）が支給されている。デスクトップタイプとノートタイプの比率はほぼ 1：1。開発担当などは複数台の PC を利用するユーザーも多く、社内ネットワークに接続されている Windows PC の総数は 15 万台に及ぶ。

2-3-3 モバイルデバイスの社外持ち出しの現状

上長の承認を受けることで、自席で使っているノート PC を持ち出すことが可能で、リモートアクセスのライセンスを得ている 3 万 3000 名（従業員の約 3 分の 1）が利用できる環境にある。

C 社では社外持ち出しが可能なノート PC を以下の 2 つに限定しており、これらが標準機として支給されている。

主力して使われているのが「シンクライアント対応ノート PC」で、現在 1 万 9000 台が社外利用を申請している。C 社では情報漏えい対策を目的に 2006 年にシンクライアントシステムの導入を開始、新型インフルエンザによるパンデミック時の業務継続性確保等のために急速に普及した、

C 社のシンクライアントシステムの大きな特徴といえるのが、端末として利用しているノート PC の開発を自ら手掛けていることである。当初は Windows SteadyState（Windows のインストールドライブをあらかじめ設定された状態へ戻せる共有 PC 向けのソフト、現在は提供終了）の機能を利用、現在は Windows 7 をカスタマイズする形で、高度なセキュリティを実現している。例えばこの PC では、電源を切るとキャッシュ情報を含む内部のデータが消去（初期化）される。C 社では「ほとんど破る方法がない程にカスタマイズしている」という。

シンクライアント対応ノート PC は標準 PC として従業員に支給されているが、既存の PC に挿入した DVD から専用シンクライアントソフトを起動して対応 PC にすることも可能である。C 社では東日本大震災の際に、出社が難しい従業員に対しバイク便などで DVD

を送付して自宅で作業ができる環境を整えた。

高いセキュリティを求められる業務を行う部署などでは、社外持ち出しを行わない PC についてもシンクライアント化が進められており、シンクライアント対応 PC の総数は 4 万台弱となる。

もう 1 つ、社外持ち出しが可能となっているのが「遠隔データ消去対応ノート PC」である。シンクライアントは、高度なセキュリティを実現できる半面、①ネットワークに接続しないと作業ができない、②ユーザーが個別にツールをインストールすることが難しいなどの制約もある。特にシステムエンジニアの場合、データセンターなど携帯電話の電波が届かない環境で仕事をするケースが多く、シンクライアント対応 PC の利用が困難であった。

こうした用途では暗号化を施したノート PC が使われていたが、一部の顧客からはより高度な情報漏洩対策が求められていた。「遠隔データ消去対応ノート PC」は、こうしたニーズに対応するために開発されたものである。

「遠隔データ消去対応ノート PC」は、ノート PC に、①ワンビの遠隔データ消去ソリューション「TRUST DELETE Biz」と②ウィンマジックのフルディスク暗号化ソリューション「SecureDoc」の 2 つを実装したものだ。

①の TRUST DELETE Biz は遠隔操作によりモバイル PC のストレージ上のファイルやホルダーを上書き消去する機能を、②の SecureDoc はストレージの暗号化と同時に、遠隔操作で PC の動作を不可能にするロック機能を持つ。

「遠隔データ消去対応ノート PC」では、②により暗号化を行うとともに、紛失・盗難時には①と②のデータ消去、コンピューターロックを同時に動作させることで、情報漏洩のリスクを極小化している。

利用者は当初の想定以上に多く現在 1 万 4000 台が使われている。シンクライアントに比べて自由度が高いことが、ユーザーにとっての魅力となっているようだ。

2-3-4 モバイルデバイスの情報漏洩対策

上記の「シンクライアント対応ノート PC」と「遠隔データ消去対応ノート PC」については、事前にシステム上で申請を行い上司の承認を受けることで、社外に持ち出して利用できる。同時にリモートアクセスのアカウントも付与される。承認は 6 カ月間有効で、期間経過後は改めて申請を行う。

「シンクライアント対応ノート PC」は承認を受ければ自由に持ち出すことができるが、後者の「遠隔データ消去対応ノート PC」については、社外に持ち出す度に上長の確認を受

けストレージ上のデータの内容を報告することが義務付けられている（対応は部門によって異なる)。社内規定としてストレージに保管するデータを最小限にすること、飲酒の禁止、電車の網棚には置かない（鞄などに入れて膝の上に置くことを推奨)、スタンバイ状態での持ち出しを避けるなど、80 に及ぶ遵守事項が設けられている。

それでも PC の紛失事故が、年数件程度発生しているという。

紛失・盗難などが発生した場合、上長への報告とともに、事故報告書の提出が求められる。これに基づき各部門の情報セキュリティ責任者が状況を判断、警察への届け出、調査、情報システム部門や渉外対応を行う部門の対処の依頼などを行う。「遠隔データ消去対応ノート PC」では、報告を受けると直ちに消去やロックの双方の処理を行うことで、情報漏洩のリスクを回避する。

ケースによっては個人情報保護ガイドラインに基づく行政への届け出などの措置が必要になるケースもある。遠隔データ消去対応 PC の開発には、こうした過程で従業員の責任が過剰に問われることを防ぐ意図もあったという。

シンクライアント対応 PC は、ストレージにデータを持たないことから、紛失の際は一般的な備品の紛失と同様に処理される。

2-3-5 個人情報の取り扱い

個人情報は顧客情報の管理を行う部署で一括して管理されており、プライバシーマークの取得や個人情報の管理基準の設定などもこの部署で行われている。

管理システムによって個人情報に指定されているデータは共通の基準で管理されている。

社外持ち出しを行う PC には個人情報は保存しないことが原則となっている。

2-3-6 モバイルデバイス活用の方向性

「シンクライアント対応 PC」及び「遠隔データ消去対応 PC」の導入によって、システム面ではモバイルデバイスの社外持ち出しに関する問題はほぼ解消されている。

遠隔データ消去対応ノート PC の社外持ち出しの手続きは、最も厳しい顧客の要望に沿ったものとなっており、運用基準の緩和、柔軟な運用を求める声もあるという。3 段階の認証を経るため起動にやや時間がかかることも、今後改善すべきポイントとして意識されている。

2-4　D 社（製造業、IT ソリューション）

2-4-1 企業の概要

D 社は、広く IT ソリューション事業を展開する大手総合エレクトロニクスメーカーで、PC や携帯電話の製造・販売も手掛ける。国内における従業員数はグループ企業を含めて約 10 万人規模となる。

2-4-2 情報システムの概要

D 社およびグループ企業の拠点を結ぶ社内ネットワークが整備されており、その上で基幹系、情報系をはじめとする多くの業務システムが運用されている。

主なクライアント Windows PC で、社内ネットワークには約 13 万台が接続されている。従来は部門やグループ会社が PC を独自に調達していたが、本社が一括調達する統一仕様の「標準 PC」への置き換えが進められており、現在は 6 万台が「標準 PC」になっている。「標準 PC」はデスクトップ、ノート PC のいずれも選択できるが、会議などで PC を使うことが多くなっていることや、一部の事業所で導入されているフリーアドレスにも対応できることから、ノート PC の利用が推奨されている。最近では、業務を自席以外で行うことがない一部の職種を除き、ノート PC が使われるようになっているという（以下これを「標準ノート PC」と表記する）。

2-4-3 モバイルデバイスの社外持ち出しの現状

全社的なセキュリティポリシーでは、一定の要件（フルディスク暗号化、BIOS と Windows 双方での ID・パスワードの設定など）を満たせば自席で使っているノート PC を社外に持ち出すことが可能となっている。

具体的な持ち出しルールは、部門毎に定められているが、社外でのノート PC の利用が不可欠なシステムエンジニアなどの職種を除くと、紛失・盗難事故を懸念して PC の社外持ち出しに消極的な傾向も見られるという。

D 社ではこうした状況を抜本的に改善するために、VMwear/シトリックスのソリューションをベースとした仮想デスクトップ（シンクライアント）システムの導入が進められている。現行のシステムの同時接続数は 1000 程度だが、これを全社で利用できるようにする計画が進行中である。これに伴い、キーボードが付加できる高性能 Windows タブレットを.標準 PC の選択肢に加えることも検討されているという。

2-4-4 モバイルデバイスの情報漏洩対策

前述の通り PC を社外に持ち出す場合は、フルディスク暗号化と BIOS/OS の 2 段階認証

が義務付けられており、「標準ノート PC」はこれらをサポートしている。運用面では、PC を持ち出す際には飲酒を禁止するなどの細かな行動規範が設けられている。

「標準ノート PC」には 2013 年春まで D 社が開発した「遠隔データ消去ソリューション」が搭載されていたが、現行機種には搭載されていない。

遠隔データ消去ソリューションの実装により情報漏洩リスクを大幅に低減できるが、運用コストとの兼ね合いからこうした措置がとられた。特に高いセキュリティを求める顧客の中に遠隔データ消去ソリューションを導入していても情報漏洩のリスクはゼロではないと考えるケースがあることも、この措置の背景にあるようだ。

D 社では紛失・盗難以外の情報漏洩の要因として指摘されることが多い外部ストレージへのデータコピーについては、会社支給の USB メモリ以外にはコピーができない措置が講じられている。

幹部社員や営業職に支給されている 7000 台程（社給の携帯電話の半数弱）のスマートフォンについても、①データの暗号化、②ID パスワードと指紋の双方での認証、③遠隔データ消去を組み合わせた強固な情報漏洩対策が施されている。

2-4-5 個人情報の取り扱い

D 社としての取り扱い規定はあるが、一部でコンシューマー向けの製品も手掛けるなど、ビジネスの性格が異なることなどから、個人情報の管理方針は部門・グループ会社毎に定められている。

情報システム部門では、データを暗号化して管理できるデータキャビネットなど情報漏洩防止のための仕組みを提供しているが、何を個人情報・機密情報として管理するかは部門・グループ会社の判断となる。

2-4-6 モバイルデバイス活用の方向性

高度な暗号化と認証をサポートした「標準ノート PC」などによりモバイル PC を社外に持ち出せる環境が整備されているが、官公庁など高いセキュリティを求める取引先を多く持っていることから、モバイル PC の持ち出しに慎重になる傾向が強い。

デバイスにデータを保存しない仮想デスクトップの導入は、その突破口になると期待されている。今後、モバイル PC のみならず、スマートフォンやタブレット端末などの多様なモバイルデバイスの活用が想定されることから、D 社ではこれらを一元的に管理できBYOD（私物端末の業務利用）にも対応可能な MDM（モバイルデバイス管理ソリューション）の導入を計画している。これによりデバイス内のデータの内容や外部とのやり取りなどの状況が把握でき、高度なセキュリティが実現できるようになる。

2-5　E 社（製造業、ソフトウェア・IT サービス）

2-5-1 企業の概要

E 社は世界規模でビジネスを展開するソフトウェア開発・IT サービス企業である。日本、米国、中国、欧州などに拠点を置いており、国内には約 800 名が勤務している。

2-5-2 情報システムの概要

日本拠点の社内ネットワーク上ではメールや財務・経理など多くのシステムが運用されており、大半が Web ベースのシステムとなっている。クライアントとして従業員 1 人 1 台、計約 800 台の Windows 7 搭載 PC が支給されており、その 8～9 割はノート PC である。検証機などを含めると、全部で 1000 台弱の PC が社内ネットワークに接続されている。

仮想デスクトップ（シンクライアント）の運用も一部で始まっており、支給されている PC にソフトウェアを導入しハイブリッド型で運用しているユーザーが多い。

海外拠点とともにグローバルでのセキュリティポリシーの下で運用されていることが特徴といえるが、一部日本独自の規定も設けられている。

私物端末の業務利用（BYOD）は認められていない。

2-5-3 モバイルデバイスの社外持ち出しの現状

従業員に支給されているノート PC はフルディスク暗号化が図られており、特別な手続きなしに、社外に持ち出して利用することができる。これらのノート PC は外出先からは VPN で社内ネットワークにアクセスできるが、仮想デスクトップや、コミュニケーションツールとして多用されているメール、チャットなどは SSL などを用いて VPN を張らなくても利用できるようデザインされている。

アクセス回線は特に指定されていないが、従業員の大半にスマートフォンが貸与されているため、テザリングの利用も可能となっている。

2-5-4 モバイルデバイスの情報漏洩対策

社外に持ち出すノート PC にはフルディスク暗号化が導入されている。

グローバルでのセキュリティポリシーが適用されており、数ヶ月に 1 回のパスワード変更が義務付けられ、実施しないと社内ネットワークにアクセスできなくなるなど、厳格な運用がなされている。

USB メモリなどへのデータのコピーはセキュリティポリシーで禁止されているが、システム的にブロックするなどの措置は講じていない。セキュリティ面でのルールを徹底させるために、入社時のセキュリティ講習の他、1 年毎にネットワーク上で「試験」を受けることが義務付けられている。

モバイル PC やスマートフォンを紛失した恐れがある場合は、直ちに上長あるいは情報システム部門に一報を入れることが厳しく求められている。テンプレートに従ってデータの内容を報告、それに沿ってスマートフォンの場合ワイプをかけるなど、所定の措置が採られる。

基本的には、顧客情報の漏洩が生じない措置が講じられているため、それ以上の問題になるケースはないという。

2-5-5 個人情報の取り扱い

顧客情報の管理は、権限を持つ数人以外はデータにアクセスできないようなっており、仮にパスワードが第三者に漏れても外部からアクセスできない特定のデータベース上でデータを保存するなど、顧客情報の管理は厳格に行われている。社外に持ち出される PC に個人情報が存在する可能性は、各部署での管理となる従業員の情報を除けば、ゼロといってよい。官公庁などの入札の参加条件にもなることから、プライバシーマークは早期に取得している。

2-5-6 モバイルデバイス活用の方向性

暗号化を信頼し、顧客情報が個人の PC 上に存在しない環境を整えることで、制約なくモバイル PC を社外に持ち出せる環境を整備している。グローバル・スタンダードに準拠したセキュリティポリシーを導入していることに加え、一般企業に比べ従業員の IT リテラシーが高いことがこうした運用を可能にしているといえる。

セキュリティを強化するために仮想デスクトップの拡充を進めているが、業務の性格上全面的な移行は計画されていない。

2-6　F 社（流通業）

2-6-1 企業の概要

F 社は、スーパーマーケットや専門店、コンビニエンスストアなどを全国展開する大手流通グループの中核会社である。グループの総従業員数は 5 万名を超える。

2-6-2 情報システムの概要

グループ各社の拠点・店舗を結ぶ社内ネットワークが整備されており、この上で基幹系、情報系システムの他、各グループ会社のシステムが稼働している。

店舗の ATM やプリペイド・ポイントカードなどを管理する金融事業は別会社となっており、情報システムも独立している。

PC は従来グループ会社や店舗毎に購入されていたが、情報システム部で一括調達する形への移行が完了しつつある。現在 PC3 万 5000 台、タブレット端末 5000 台が、本部からグループ各社にレンタル（内部処理）されている。PC はその大半がノート PC となっている。

人事、経理などの特定業務を対象に VDI（仮想デスクトップ）化が進められており、最終的には 1 万台規模に拡充される予定だ。

2-6-3 モバイルデバイスの社外持ち出しの現状

従業員に支給されているノート PC は、上長の許可を受けることで社外に持ち出して使うことができる。許可を受けている PC の総数は 1 万台程。そのうちアクティブに持ち出し利用が行われているのは 1000 台程度だという。

F 社では、電子メールなどのコミュニケーションツールとして、あるいは店舗の発注業務用に LTE モジュール内蔵のタブレット端末を活用しているが、これも同様に社外持ち出しが可能となっている。現在 1000 台程度が持ち出し利用されている。

2-6-4 モバイルデバイスの情報漏洩対策

ノート PC にはフルディスク暗号化が導入されている。社内システムへのアクセスは通信サービス会社の VPN アクセスサービスを介して携帯電話の LTE 回線によって行われている。通信サービス会社のサービスを利用することで、高度な認証が可能になる他、詳細な通信ログが提供されるため管理が容易になるというメリットも生じているという。

タブレット端末は携帯電話事業者の LTE 内蔵機種が採用されており、LTE 網を介して社内ネットワークへのセキュアなアクセスが実現されている。盗難・紛失時の遠隔データ消去機能も利用可能だ。

F 社グループの全店舗には無線 LAN が整備されており、暗号化キーの随時変更など、高いセキュリティが実現されている。タブレット端末による発注業務などは主に無線 LAN を使って行われている。

ノート PC、タブレット端末の紛失時には、会社に事故届けを出すと同時に、警察への届け出が義務付けられている。

2-6-5 個人情報の取り扱い

顧客情報の管理は基本的には前述の金融事業会社で金融庁の基準に従って厳格に行われている。F 社自身は顧客の個人情報を保有せず、クレジットカードやポイント・プリペイドカードのデータもそのまま金融事業会社の情報システムに受け渡される。F 社内の PC に顧客情報が存在しないことが、持ち出し利用を可能にする大きな要因となっている。従業員の個人情報などについても VDI 化により対策が講じられる。

2-6-6 モバイルデバイス活用の方向性

顧客情報が個人の PC 上に存在しない環境を整えることに加えて、高度な暗号化、通信サービス会社のリモートアクセスサービスの利用による認証の強化などにより、エンドユーザーが特に意識することなく、モバイル PC を社外で使える環境を整備している。

VDI 化を進めることで、PC の社外利用の環境整備はほぼ完成することになる。

3　考察

3-1 モバイルデバイスの社外利用のトレンド

前章で見たように、様々な業種・業態の企業にモバイル PC を社外に持ち出して利用する動きが広がってきているが、これらは大きく 2 つの類型で捉えることができる。

1 つは、個人情報・機密情報の管理を厳格化し、従業員の PC 内にこれらが存在しない状況を確保した上で、フルディスク暗号化、高度な認証の導入を条件としてモバイル PC の社外持ち出しを比較的自由に認めるというものだ。

海外の企業では一般的な運用形態だが、日本においては個人情報保護基本法試行後にモバイル PC の全面持ち出し禁止に踏み切った企業が多く、こうした手法を取る企業は少数にとどまっていた。ビジネスのグローバル化や個人情報保護法への現実的な対応が模索される中で、改めてこうした手法によりモバイル PC の社外持ち出しを解禁する企業が増えてきているということができる。

他方では、個人情報等の管理を甘いまま放置し、モバイル PC の一律持ち出し禁止を継続している企業も多数存在する。モバイル PC の活用による企業の生産性の向上を実現するには、企業の経営者・情報システム部門の意識改革が重要だと考えられる。

もう 1 つの類型が、シンクライアント（仮想デスクトップ:VDI）の導入によりデバイス上にデータを一切残さないようにした上で、モバイル PC の社外持ち出しを解禁するものだ。
業務自体が個人情報と不可分となる金融機関などでは、監督官庁である金融庁、（運用上は金融情報システムセンター＜FISC＞）の基準にそった形で、モバイル PC の社外持ち出しは極めて限定的にしか行われてこなかった。シンクライアント化はこの状況変える突破口になると期待されている。

近年、シンクライアントの導入が進んできた背景として挙げられるのが、携帯電話事業者が LTE のインフラ整備に注力したことによるアクセス環境の飛躍的な向上だ。通信速度の向上、不感地の減少、遅延の低減により、外出先でも社内と同等のネットワーク環境が利用可能になっているのだ。

ただし、シンクライアントにも限界はある。1 つはネットワークに接続できない（携帯電

話の電波が届かない）環境では基本的には作業ができないこと。もう 1 つはアプリケーションをサーバー側で用意する必要があるため、デバイスにソフトを導入して機能をカスタマイズするといった使い方が難しいことだ。中堅中小企業では導入コストも大きな問題となる。シンクライアントでモバイル PC のニーズを全て代替するのは困難である。

先に述べたフルディスク暗号化と情報管理の徹底は、シンクライアントの導入が難しい用途で PC の社外持ち出しを実現する現実解といえる。これらに加えて、遠隔データ消去ソリューションを導入することで、モバイル PC の情報漏洩リスクを極限まで引き下げることが可能になる。

シンクライアントにタブレット端末を利用するケースもでてきているが、この場合、通信事業者やベンダーが提供する遠隔データ消去（ワイプ）サービスの利用が広く行われている。

モバイル PC やタブレット端末などのモバイルデバイスを MDM で一括管理する動きもでてきた。今後、遠隔消去機能を持つ MDM を導入して、モバイル PC、タブレット端末双方のセキュリティを高める企業が、多くなりそうだ。

3-2 行政のガイドラインなどへの要望

企業におけるモバイルデバイスの社外持ち出しに大きな影響を与えてきたファクターとして、個人情報保護基本法及びこれに基づいて各省庁が定めている個人情報保護ガイドラインが挙げられる。

特に個人情報保護法施行当初の省庁のガイドラインでは、個人情報が保存されているモバイル PC を紛失した場合、省庁への届け出の他、事案によっては本人通知、公表を求めるなど厳しい内容が設けられている。これが、企業が一斉にモバイル PC の社外持ち出しを手控える発端となった。

その後、経済産業省や総務省など一部の省庁ではガイドラインの改正により本人通知や届け出などの要件が緩和されたが、多くは見直しが行われないままになっている。

ヒアリングでは、こうした省庁ガイドラインへの要望などについても尋ねたが、個人情報保護法の施行後 10 年近くが経過し、すでに一定の対応策を見出してきているだけに「特

に要望はない。従業員からの不満も聞かれない」（A 社）、「すでに規制がどうということではなくなっているのではないか」（E 社）という声も聞かれた。

情報漏洩に対して厳格な対応が求められている金融庁所管の企業においては「個人情報を扱っている以上規制が厳しいのは当然」（B 社）と、規制を与件として受け入れた上で、対策を講じようとしている姿勢が浮かび上がる。IT ベンダーにも「暗号化の有効性などを行政当局と議論しても対応が変わることはない。データをデバイスに置かないという対応以外にはないのでは」という見方がある。

高いセキュリティを求められる業種では、VDI がモバイル PC を活用するための有効な手立てになると見られるが、この場合もまず個人情報の漏洩が VDI 化で完全に防げるというコンセンサスを関係者の間で作り上げることが重要になると考えられる。

多様な業種・業態の企業や官公庁を対象にビジネスを展開している IT ベンダーからは、「業種毎に規制の状況が異なっているため、社内でも対応を最も厳しいところに合わせようとする傾向が強く、これがモバイル PC の社外持ち出しを進める上でのネックの 1 つになっている」（D 社）、「どこまでの措置をとれば、届け出などのペナルティを避けられるのか明示されていないため、より安全側に触れる傾向が強い」（E 社）として、ガイドラインの平準化や基準の明確化を求める意見も聞かれた。

MCPC セキュリティ委員会では、こうした企業の意見を踏まえ、有効な情報漏洩対策ソリューションの普及を促すとともに、企業がモバイルデバイスをより使いやすくするための規制緩和策などについても、積極的に提言を行っていきたいと考えている。

4 別冊

モバイルデバイスの積極的な利活用における個人情報保護法の影響調査

調査目的

国内の企業に勤務する対象者に、個人情報保護やセキュリティガイドラインの現状を聴取し、モバイルコンピューティングの促進上の課題を把握する。

●主な調査テーマ

・個人情報取扱の現状
・個人情報保護ガイドラインの制定状況
・個人情報保護ガイドラインによる生産性への影響
・モバイルコンピューティング状況
・モバイルコンピューティングに関するガイドライン制定状況
・モバイルコンピューティングに関するガイドラインによる生産性への影響

●調査方法

インターネット調査　（日経 BP コンサルティングのインターネット調査システム「AIDA」を使用）

●調査期間

2014 年 5 月 20 日～5 月 22 日

●調査対象者

登録上の属性情報、所属部門が以下に該当する、現在もフルタイムの仕事をしている者。

・経営全般/経営企画
・宣伝/広報
・販売/営業
・保守/サポート

※日経 BP コンサルティングの調査モニターを利用

●有効回答数

522 サンプル

●調査機関

調査企画: モバイルコンピューティング推進コンソーシアム
実施・報告書作成： 日経ＢＰコンサルティング

モバイルソリューションを推進する
MCPC

モバイルデバイスの積極的な利活用における個人情報保護法の影響調査

調査報告書
(2014.7)

目次

©All rights reserved by MCPC, 2014
モバイルコンピューティング推進コンソーシアム

1 調査概要

調査概要

●調査目的
国内の企業に勤務する対象者に、個人情報保護やセキュリティガイドラインの現状を聴取し、モバイルコンピューティングの促進上の課題を把握する。

●主な調査テーマ
・個人情報取扱の現状
・個人情報保護ガイドラインの制定状況
・個人情報保護ガイドラインによる生産性への影響
・モバイルコンピューティング状況
・モバイルコンピューティングに関するガイドライン制定状況
・モバイルコンピューティングに関するガイドラインによる生産性への影響

●調査方法
インターネット調査　（日経BPコンサルティングのインターネット調査システム「AIDA」を使用）

●調査期間
2014年5月20日～5月22日

●調査対象者
登録上の属性情報が所属部門が以下に該当する、現在もフルタイムの仕事をしている者。
・経営全般/経営企画
・宣伝/広報
・販売/営業
・保守/サポート
※日経BPコンサルティングの調査モニターを利用

●有効回答数
522サンプル

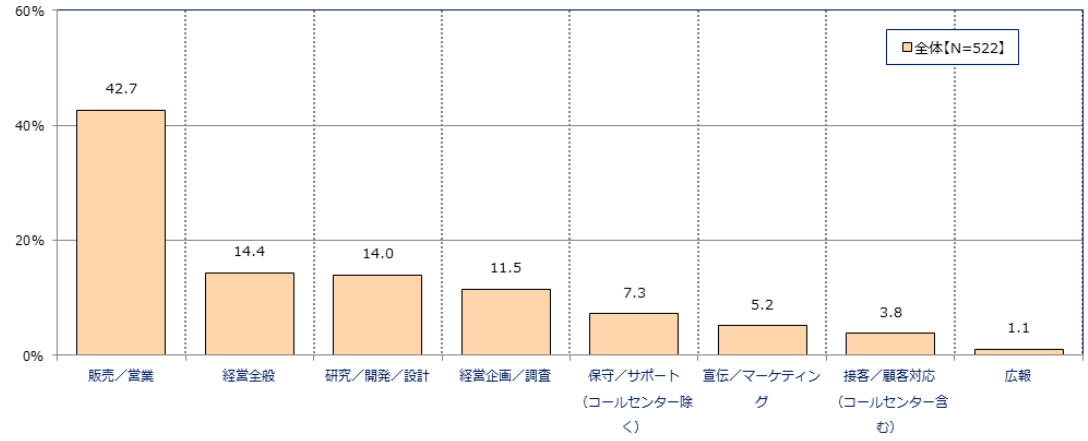
●調査機関
調査企画: モバイルコンピューティング推進コンソーシアム
実施・報告書作成： 日経ＢＰコンサルティング

1.回答者の立場・所属部門(Q2)

- 回答者の職種は「販売/営業」が42.7%で半数近くを占めた。
- その他、「経営全般」(14.4%)、「研究/開発/設計」(14.0%)、「経営企画/調査」(11.5%)が上位にあげられた。

[SA]

※全体の降順でソート

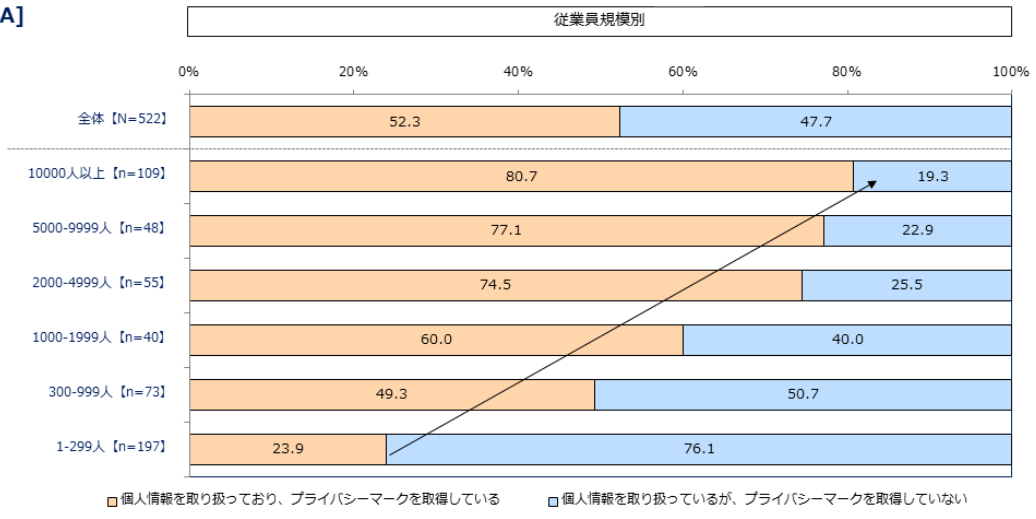


※0.0は表示せず

2.プライバシーマーク取得の有無(Q3)

- プライバシーマークの取得率は従業員の多い企業ほど高く、10000人以上のケースでは80.7%がプライバシーマークを取得している。
- それに対し、1-299人のケースでのプライバシーマーク取得は23.9%にとどまった。

[SA]

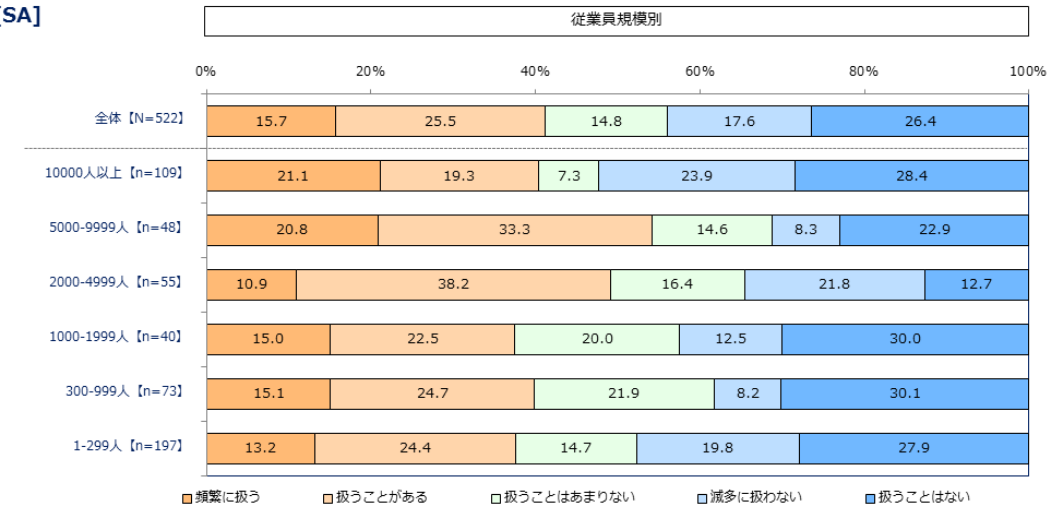


※0.0は表示せず

3.個人情報業務利用の有無(Q4)

- 3000件以上の個人情報を業務で取り扱うかを尋ねた。
- 従業員規模による個人情報の取り扱い頻度の差は見られなかった。

[SA]



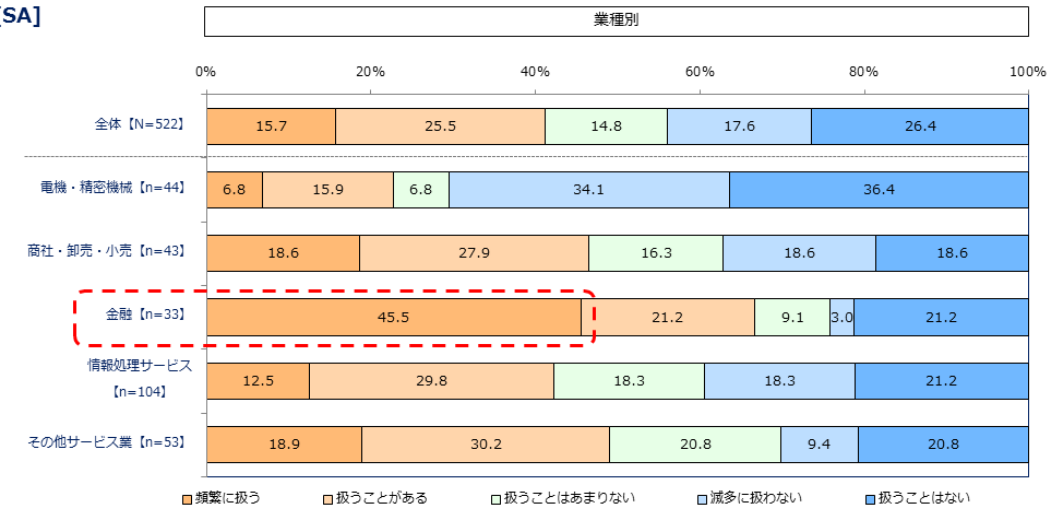
※0.0は表示せず

モバイルコンピューティング推進コンソーシアム

4.個人情報業務利用の有無(Q4)

- 業種別では、金融業での個人情報の取り扱い頻度が突出している。
- 次いで、「商社・卸売・小売」と「その他サービス業」の取り扱い頻度が同水準で並ぶ。

[SA]



※0.0は表示せず

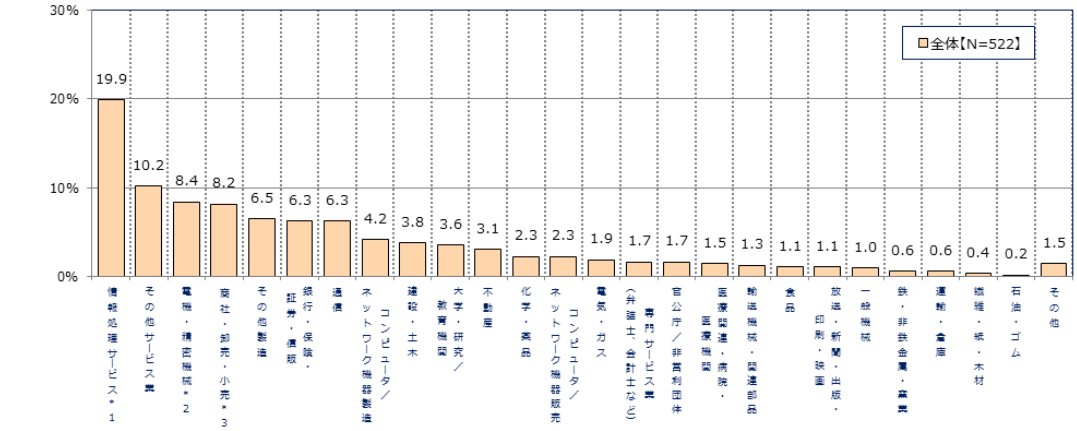
モバイルコンピューティング推進コンソーシアム

5.回答者の業種(Q5)

■回答者の業種は「情報処理サービス」が19.9%で最多であった。

[MA]

※全体の降順でソート



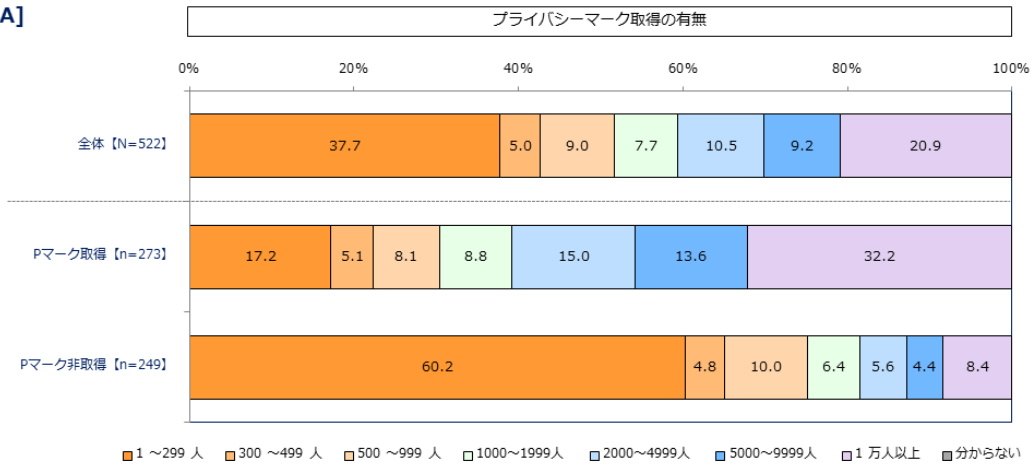
*1：情報処理サービス、システム・インテグレータ、ソフトハウス
*2：電機・精密機械（コンピュータ/ネットワーク機器製造を除く）
*3：商社・卸売・小売（コンピュータ/ネットワーク機器販売を除く）

※0.0は表示せず

6.回答者の勤務先の従業員規模(Q6)

■ Pマークを取得しているケースの方が従業員規模が大きい傾向にある。

[SA]

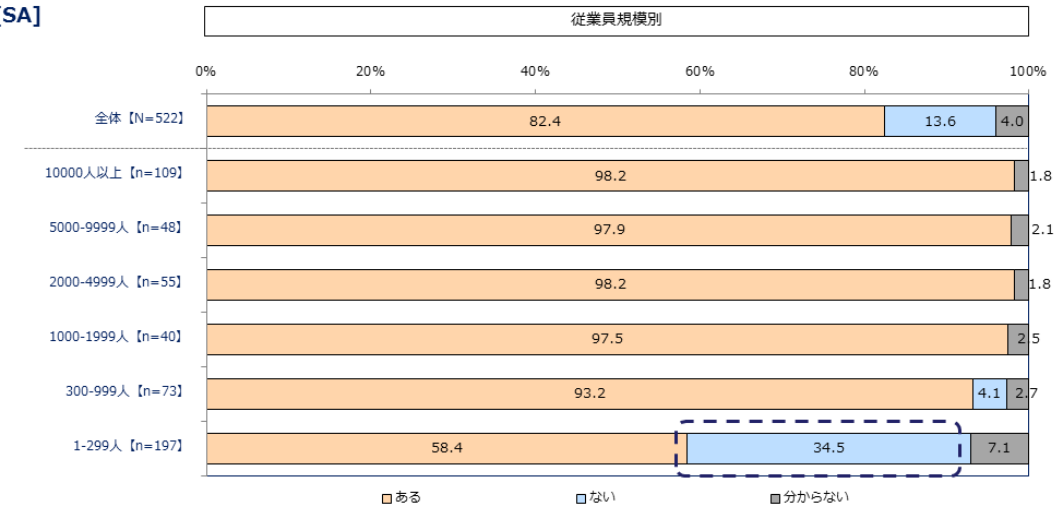


※0.0は表示せず

7.個人情報取扱社内規定の有無(Q7)

- 「1-299人」の中小企業では個人情報取扱社内規定が「ない」割合が34.5%と多い。
- 300人以上の層では、個人情報取扱社内規定があるケースがほとんどである。

[SA]

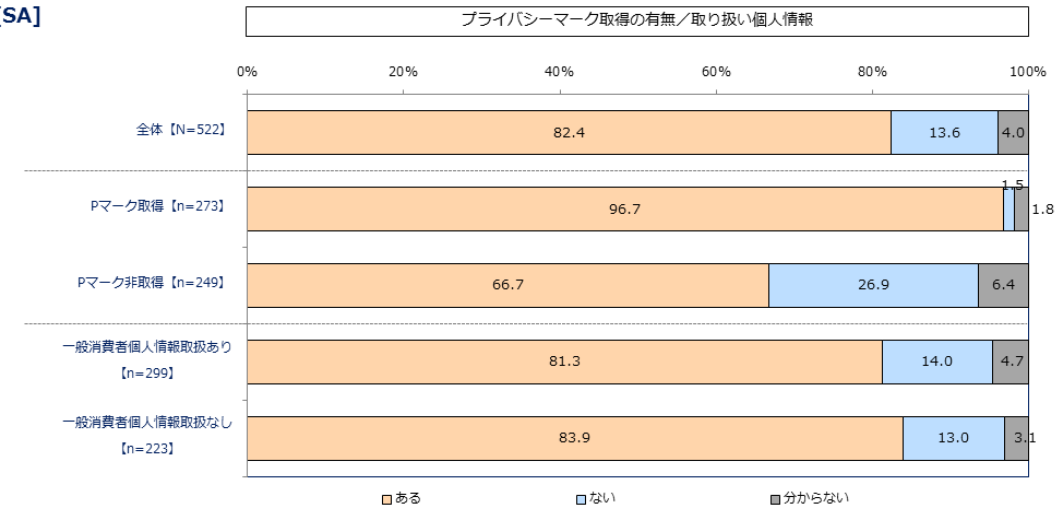


※0.0は表示せず

8.個人情報取扱社内規定の有無(Q7)

- Pマーク取得の場合、ほぼ全ての回答者が「個人情報取扱社内規定がある」と回答した。
- Pマーク非取得でも2/3は個人情報取扱社内規定があると回答した。
- 一般消費者の個人情報取扱による差は見られなかった。

[SA]

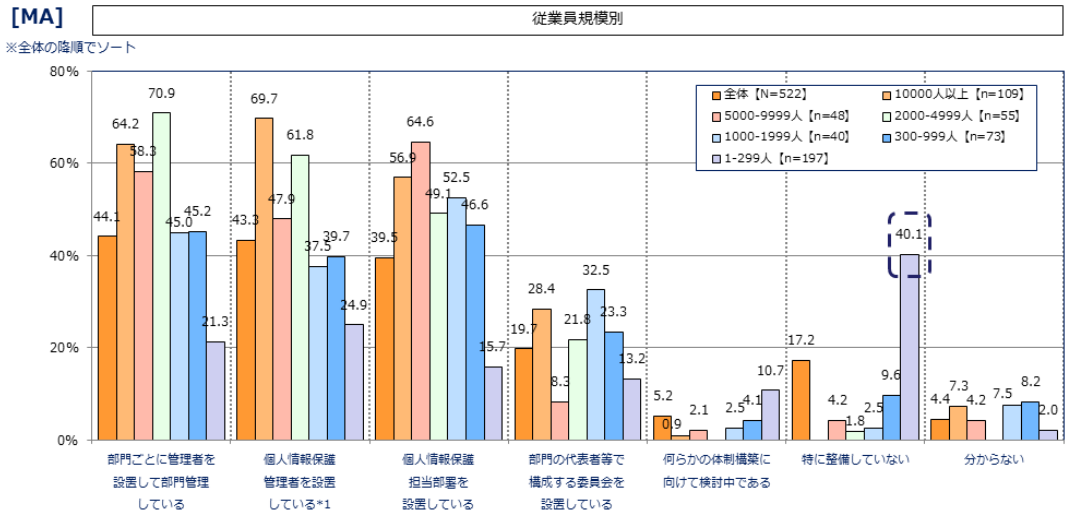


※0.0は表示せず

9.個人情報管理体制について(Q8)

- 「部門ごとに管理者を設置」、「CPOを設置」、「担当部署を設置」が上位にあげられた。
- 従業員規模2000人以上のケースでは「部門ごとに管理者を設置」「CPOを設置」が多い。
- 「特に整備していない」は「1-299人」で40.1%と多い。

[MA]



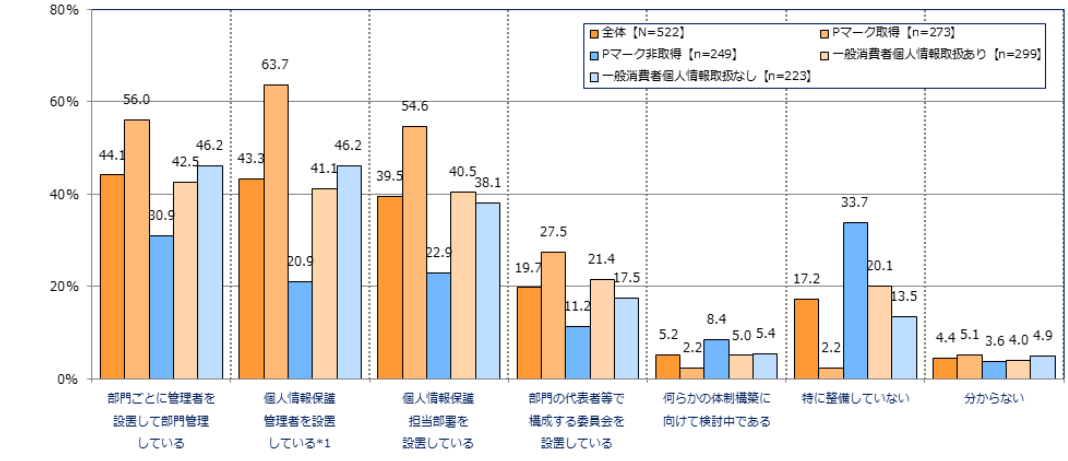
*1：個人情報保護管理者（チーフ・プライバシー・オフィサー,CPO）を設置している

※0.0は表示せず

10.個人情報管理体制について(Q8)

- Pマークを取得と非取得では体制に差が見られ、「部門ごとに管理者を設置」、「CPOを設置」及び「担当部署を設置」の3項目での差が大きい。
- 一般消費者の個人情報の取り扱い有無による差はわずかである。

[MA]

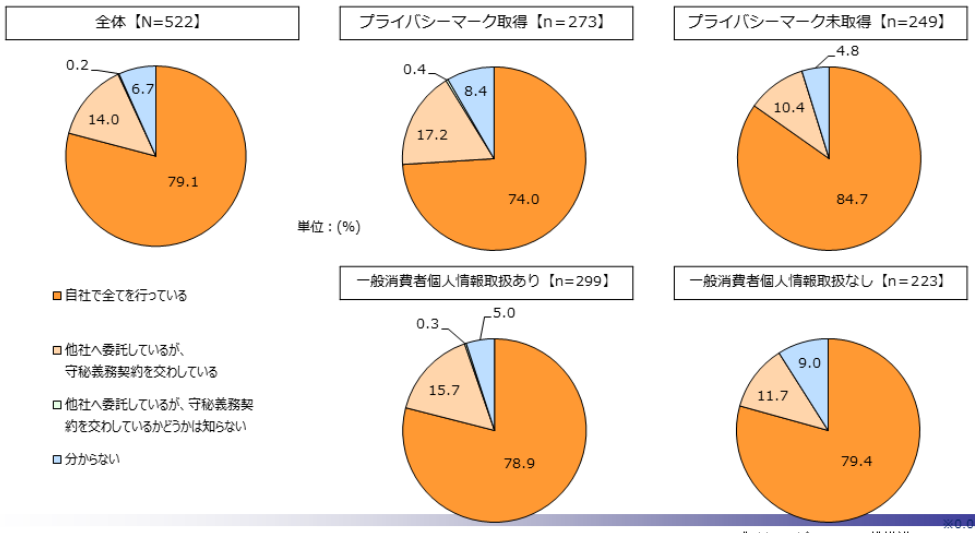


*1：個人情報保護管理者（チーフ・プライバシー・オフィサー,CPO）を設置している

11.個人情報管理部門(Q9)

- 個人情報の取り扱いは大半が「自社で全てを行っている」であった。
- 「他社委託＆守秘義務契約」は14.0%であった。

[SA]

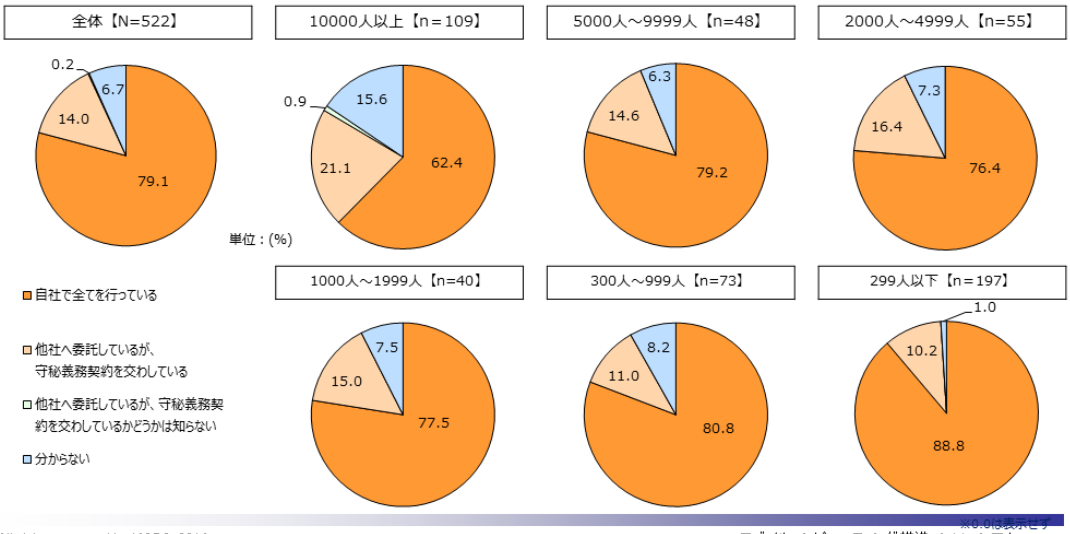


※0.0は表示せず

12.個人情報管理部門(Q9)

- いずれの従業員規模でも自社での管理が大半を占める。
- 従業員規模が大きいケースほど他社委託＋守秘義務契約が増える傾向にあるが、これは系列子会社への委託のケースも含まれると推定される。

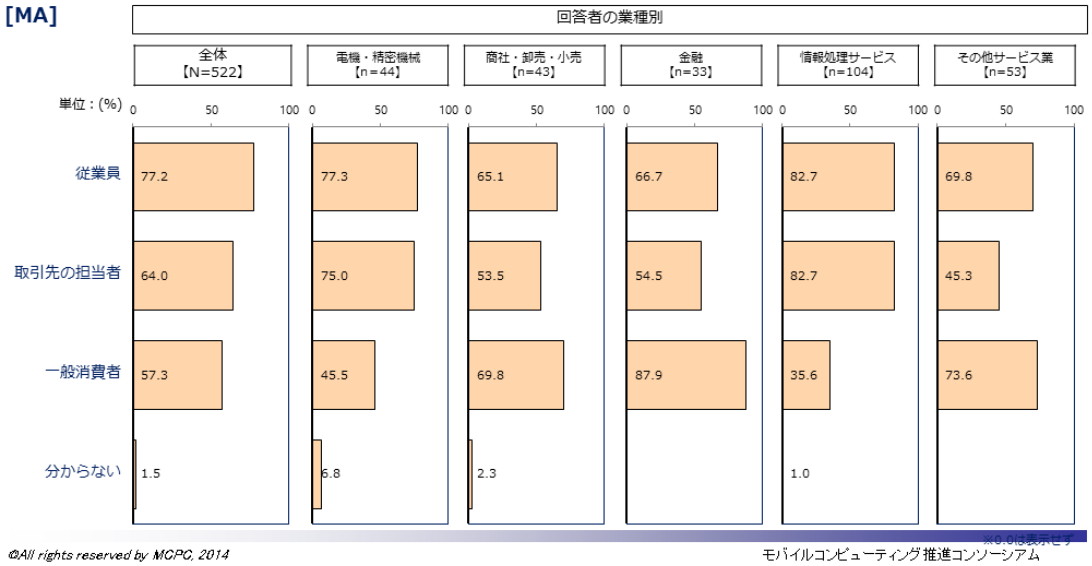
[SA]



※0.0は表示せず

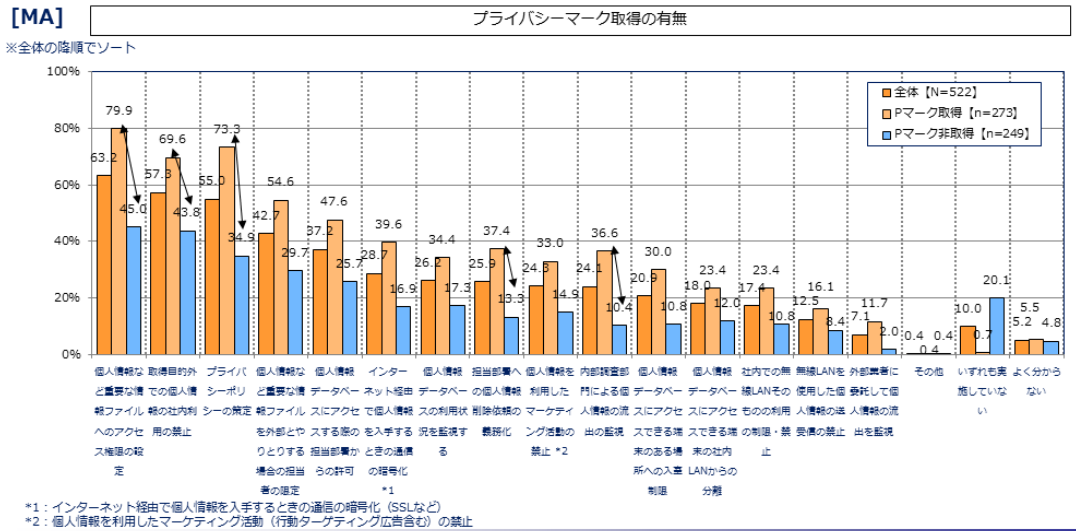
13.取り扱っている個人情報(Q10)

■取り扱い個人情報として「従業員」を挙げたケースは全体の77.2%であった。
■金融業は「一般消費者」の取り扱いが87.9%と突出して多い。



14.個人情報管理の運用(Q11)

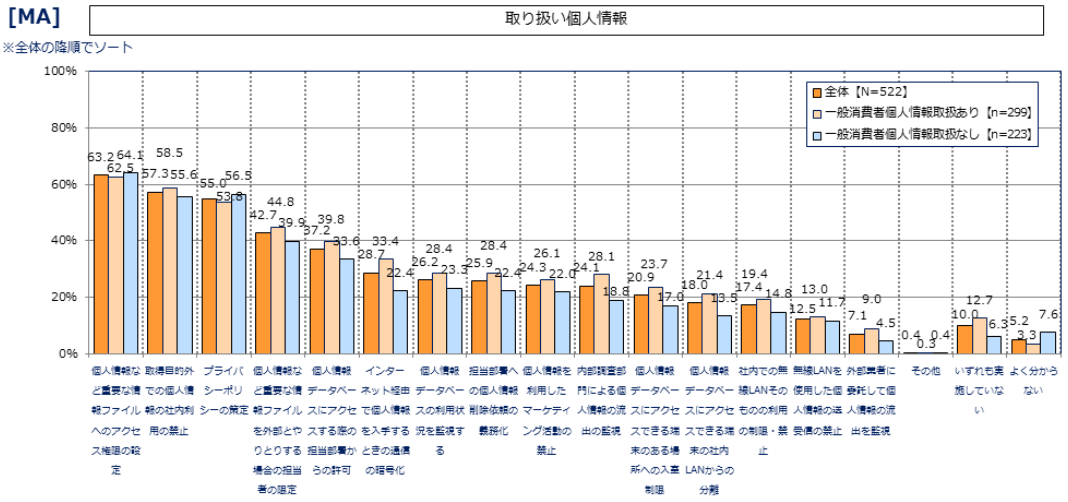
■個人情報管理の運用ルールをたずねた。「アクセス権限の設定」(63.2%)が最多であり、「目的外利用の禁止」(57.3%)、「プライバシーポリシーの策定」(55.0%)などが上位。
■いずれの項目もPマークを取得しているケースが非取得を上回る。



15.個人情報管理の運用(Q11)

- 個人情報取扱の有無による運用ルールの多寡には顕著な差は見られなかった。

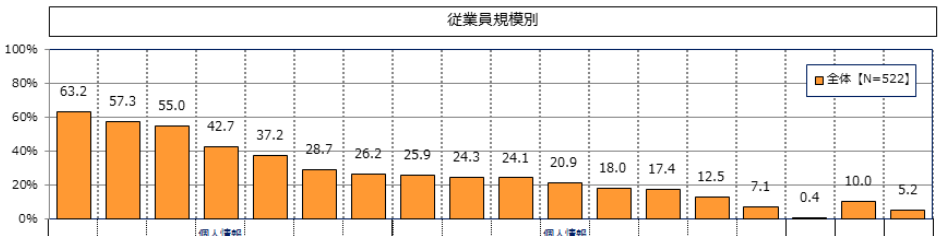
[MA]
※全体の降順でソート



16.個人情報管理の運用(Q11)

■運用ルールは従業員規模が大きくなるにつれて厳しくなる傾向が見られる。
■「1-299人」の中小企業では「いずれも実施していない」が23.9%と高いのが目立つ。

[MA]
※全体の降順でソート

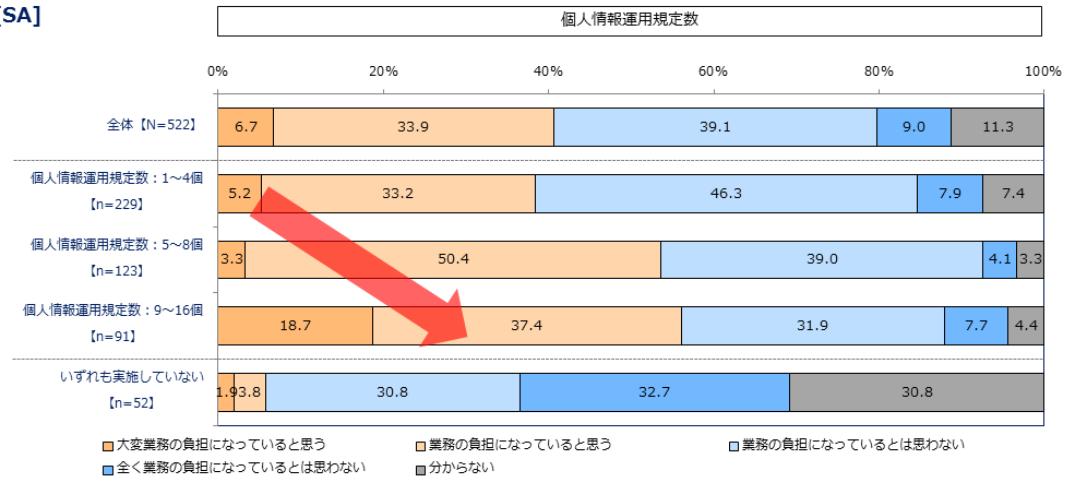


	N=	個人情報など重要な情報ファイルへのアクセス権限の設定	取得目的外での個人情報の社内利用の禁止	プライバシーポリシーの策定	個人情報など重要な情報ファイルを外部とやりとりする場合の担当者の限定	個人情報データベースにアクセスする際の担当部署からの許可	インターネット経由で個人情報を入手するときの通信の暗号化	個人情報データベースの利用状況を監視する	担当部署への個人情報削除依頼の義務化	個人情報を利用したマーケティング活動の禁止	内部調査部門による個人情報の流出の監視	個人情報データベースにアクセスできる端末のある場所への入室制限	個人情報データベースにアクセスできる端末の社内LANからの分離	社内での無線LANそのものの利用・禁止	無線LANを使用した個人情報の送受信の禁止	外部業者に委託して個人情報の流出を監視	その他	いずれも実施していない	よく分からない
全体	522	63.2	57.3	55.0	42.7	37.2	28.7	26.2	25.9	24.3	24.1	20.9	18.0	17.4	12.5	7.1	0.4	10.0	5.2
10000人以上	109	81.7	75.2	66.1	56.0	52.3	38.5	41.3	35.8	31.2	38.5	32.1	25.7	19.3	15.6	9.2	0.9	0.9	5.5
5000-9999人	48	75.0	64.6	56.3	47.9	43.8	31.3	37.5	31.3	31.3	29.2	25.0	22.9	16.7	12.5	10.4	0.0	4.2	8.3
2000-4999人	55	85.5	74.5	80.0	49.1	49.1	36.4	36.4	34.5	32.7	38.2	29.1	21.8	34.5	18.2	10.9	0.0	0.0	1.8
1000-1999人	40	75.0	62.5	72.5	50.0	50.0	27.5	30.0	47.5	25.0	27.5	27.5	22.5	15.0	12.5	2.5	0.0	0.0	10.0
300-999人	73	68.5	60.3	61.6	50.7	38.4	37.0	26.0	20.5	23.3	23.3	20.5	13.7	23.3	13.7	8.2	0.0	2.7	8.2
1-299人	197	39.6	38.6	35.5	27.9	20.8	17.8	11.7	14.2	16.8	10.7	10.2	12.2	10.2	8.6	4.6	0.5	23.9	3.0

17.個人情報管理の束縛レベル[生産性](Q12)

- 個人情報運用規定の回答個数と業務との負担感について分析した。
- 運用規定数が多いケースほど負担感は強まる傾向にある。
- 特に「9～16個」のケースでは18.7%が「大変業務の負担」と回答している。

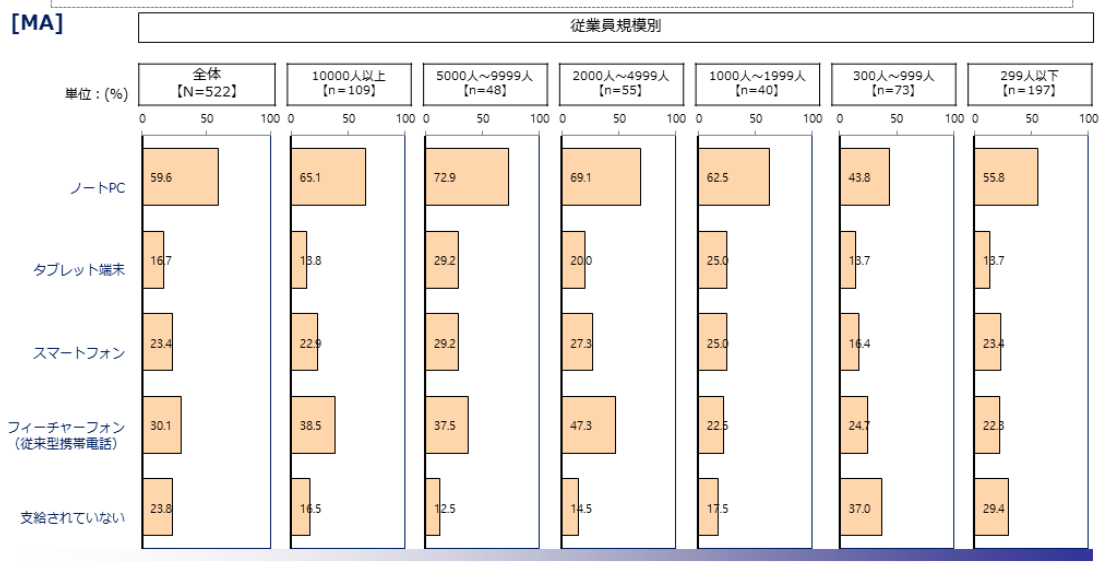
[SA]



18.モバイルデバイスの支給状況(Q14)

■ モバイルデバイスの支給状況についてたずねた。
■ 最も多いのは「ノートPC」（59.6%）。タブレット端末の支給は16.7%にとどまっている。

[MA]

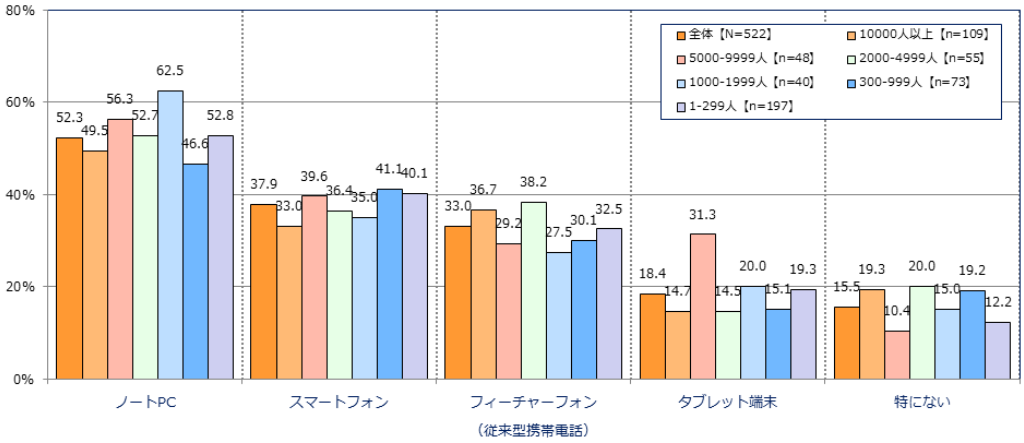


19.回答者の社外でのモバイルコンピューティング状況(Q15)

- 社外で業務に用いるモバイルデバイスの種類についてたずねた。
- 最も多いのはノートPC(52.3%)であり、いずれの従業員規模でもトップ。
- 「スマートフォン」(37.9%)はフィーチャーフォン(33.0%)をわずかながら上回った。

[MA] 従業員規模別

※全体の降順でソート

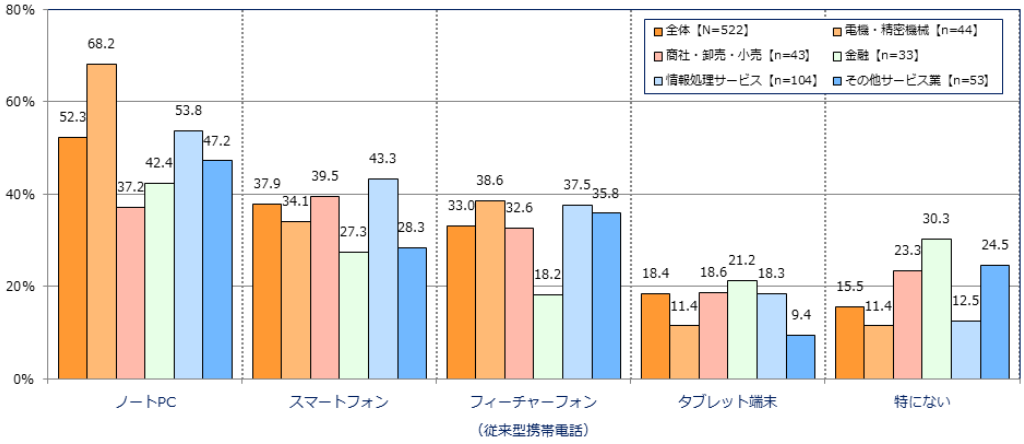


20.回答者の社外でのモバイルコンピューティング状況(Q15)

- 回答者業種別では、商社・卸売・小売でノートPCの社外利用が低い。
- 金融では「フィーチャーフォン」も含め多くのモバイルデバイスの社外使用率が低い一方、タブレット端末が21.2%と若干高い。

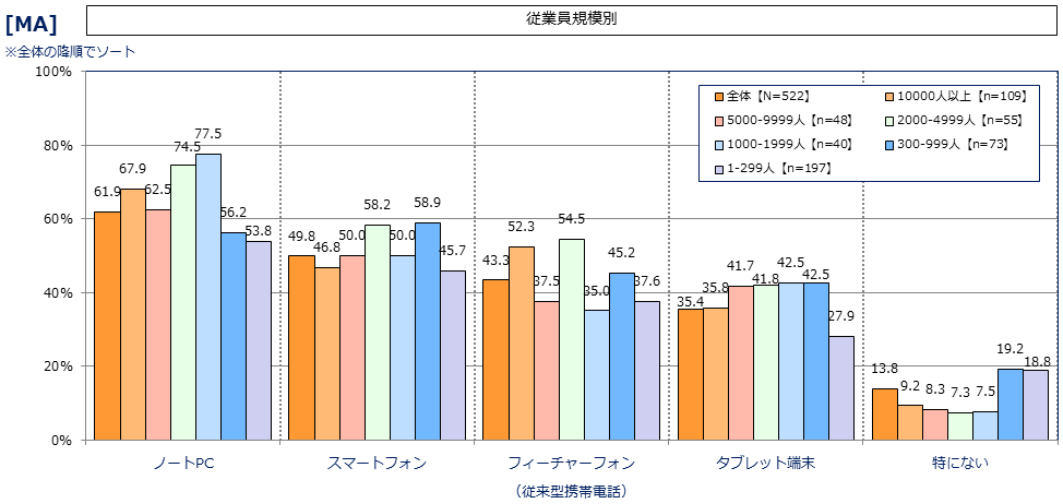
[MA] 回答者の業種別

※全体の降順でソート



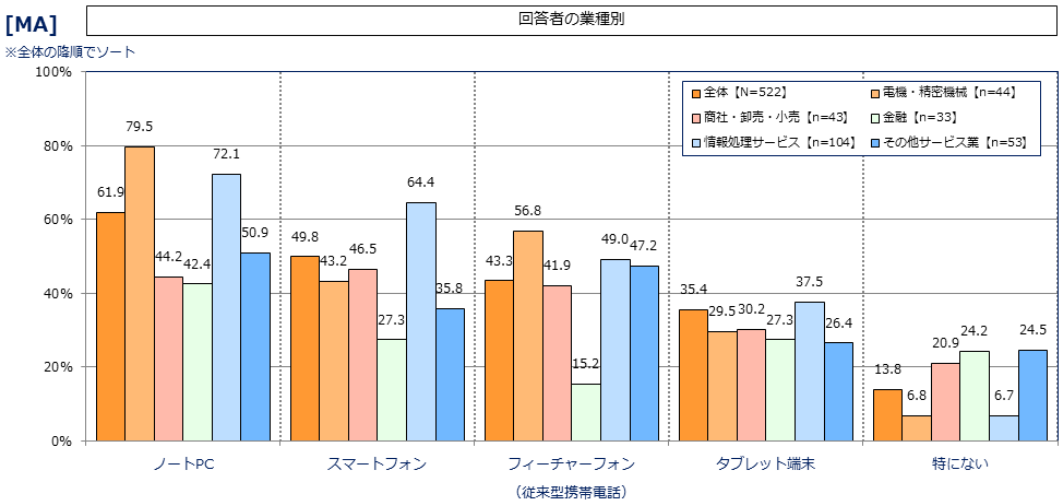
21.回答者の同僚の社外でのモバイルコンピューティング状況(Q16)

- 回答者の同僚の社外モバイルコンピューティング機器についても、「ノートPC」がトップであった。



22.回答者の同僚の社外でのモバイルコンピューティング状況(Q16)

- 業種別での回答者の同僚の社外モバイルコンピューティング状況も、回答者と同様の傾向を示している。

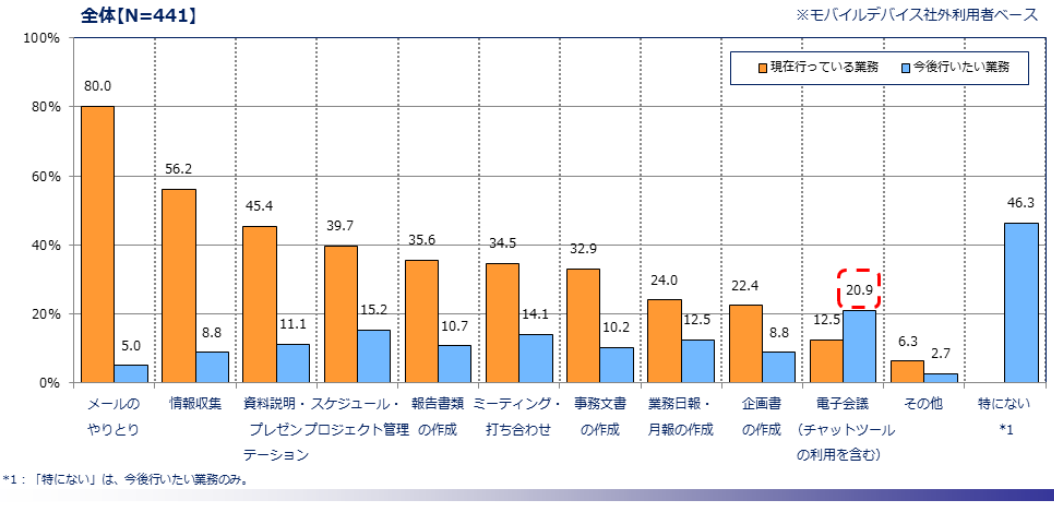


23.回答者の社外でのモバイルコンピューティング業務(Q17＆Q18)

- モバイルデバイス社外使用者の現在行っている業務は、「メールのやりとり」(80.0%)が最も多く、次いで「情報収集」(56.2%)や「プレゼンテーション」(45.4%)が上位。
- 今後行いたい業務としては、「電子会議」(20.9%)が最も多かった。

[MA]

※「現在行っている業務」の降順でソート



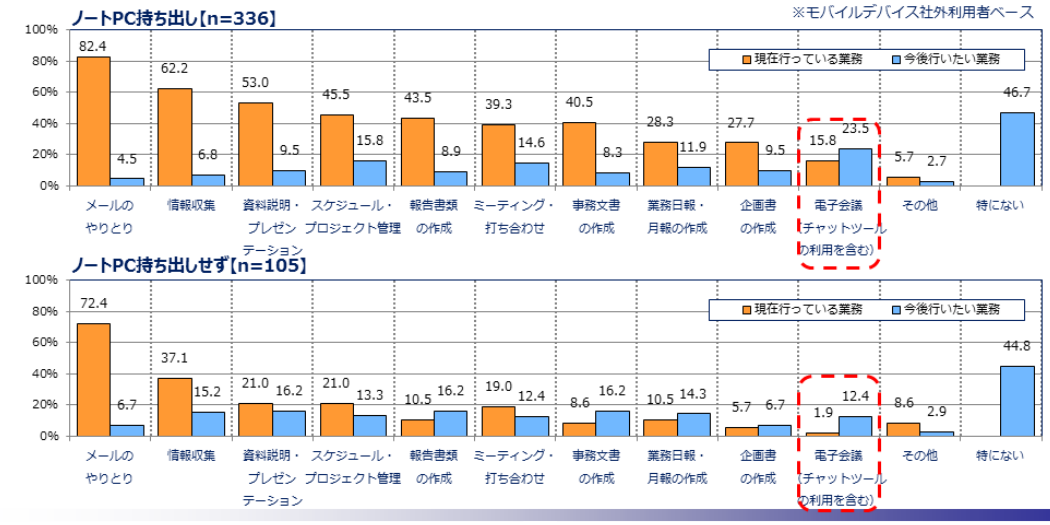
*1：「特にない」は、今後行いたい業務のみ。

24.回答者の社外でのモバイルコンピューティング業務(Q17＆Q18)

- ノートPCを社外に持ち出している回答者は多くの業務をこなしており、電子会議に対するニーズが高い。
- ノートPC以外のデバイスを持ち出している回答者の主業務はメールである。

[MA] ノートPC社外持ち出し別

※「現在行っている業務」の降順でソート



25.回答者の社外でのモバイルコンピューティング業務(Q17＆Q18)

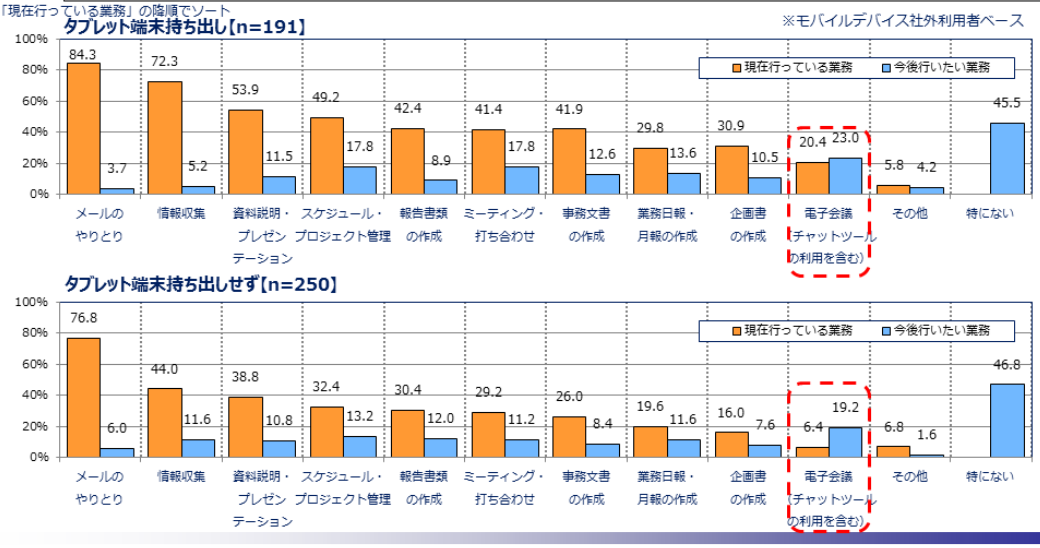
- タブレット端末を社外に持ち出している回答者も、メールや情報収集など多くの業務を行っており、電子会議のニーズは23.0%であった。
- タブレット端末を持ち出していない回答者においても、電子会議のニーズは底堅い。

[MA]

タブレット端末社外持ち出し別

※「現在行っている業務」の降順でソート

※モバイルデバイス社外利用者ベース



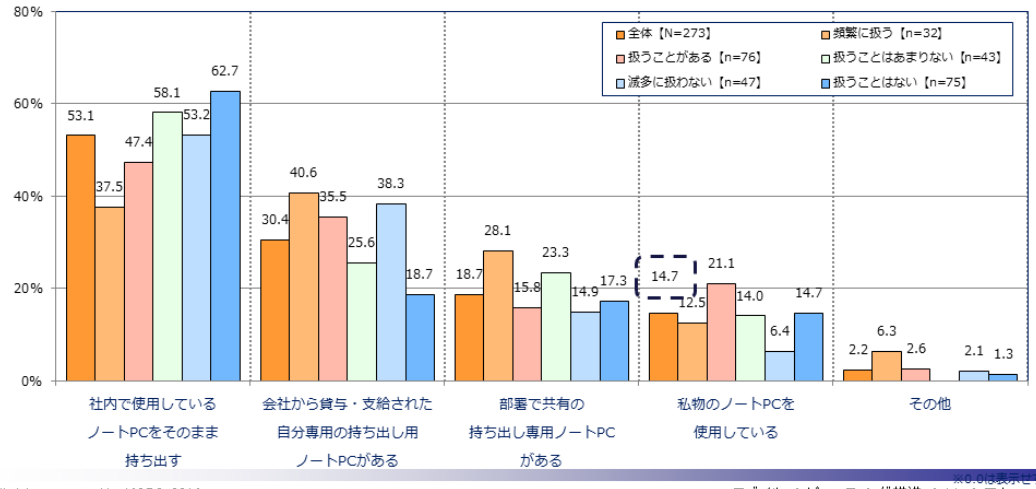
26.回答者の社外ノートPC持ち出し(Q19)

- ノートPC社外持ち出し者に、持ち出し形態をたずねた。
- 最も多いのは「社内で使用しているノートPCをそのまま持ち出す」(53.1%)であった。
- 「私物のノートPC」持ち出し者も14.7%存在している。

[MA]

個人情報業務利用の有無

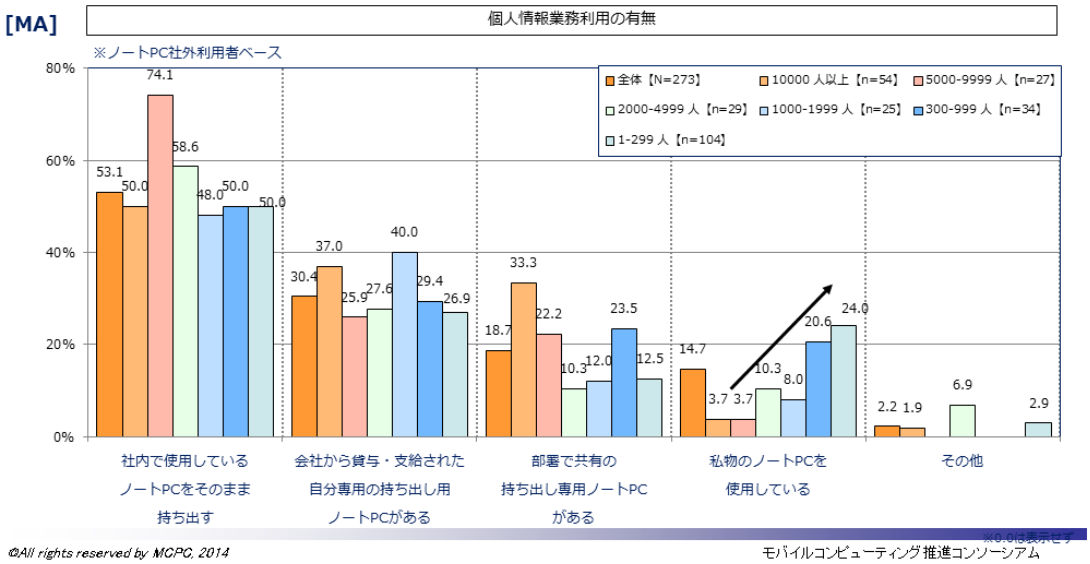
※ノートPC社外利用者ベース



※0.0は表示せず

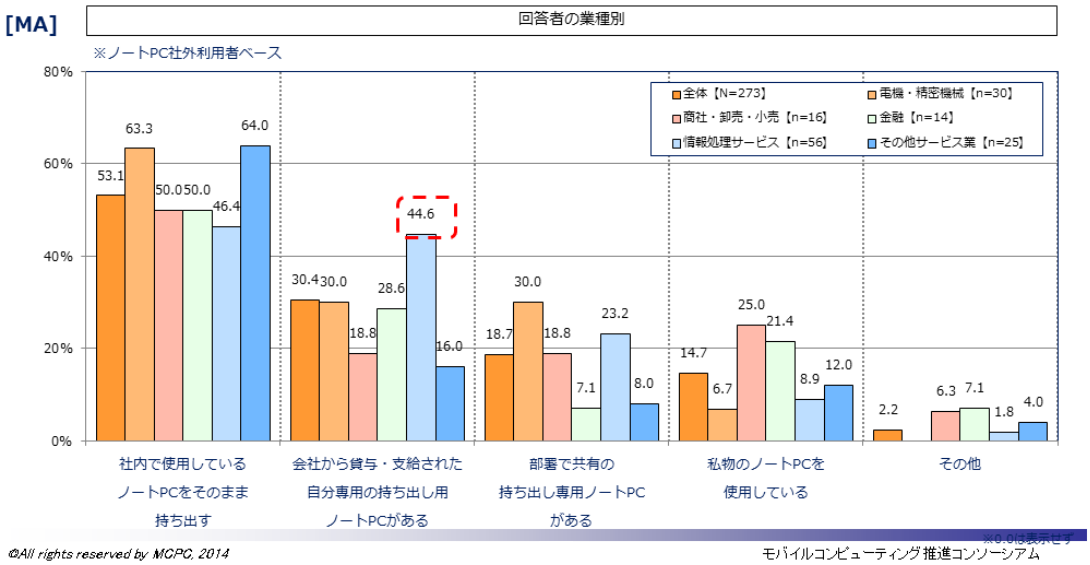
27.回答者の社外ノートPC持ち出し(Q19)

- 従業員規模の小さいケースほど、「私物のノートPC」の使用が増加する傾向が見られる。



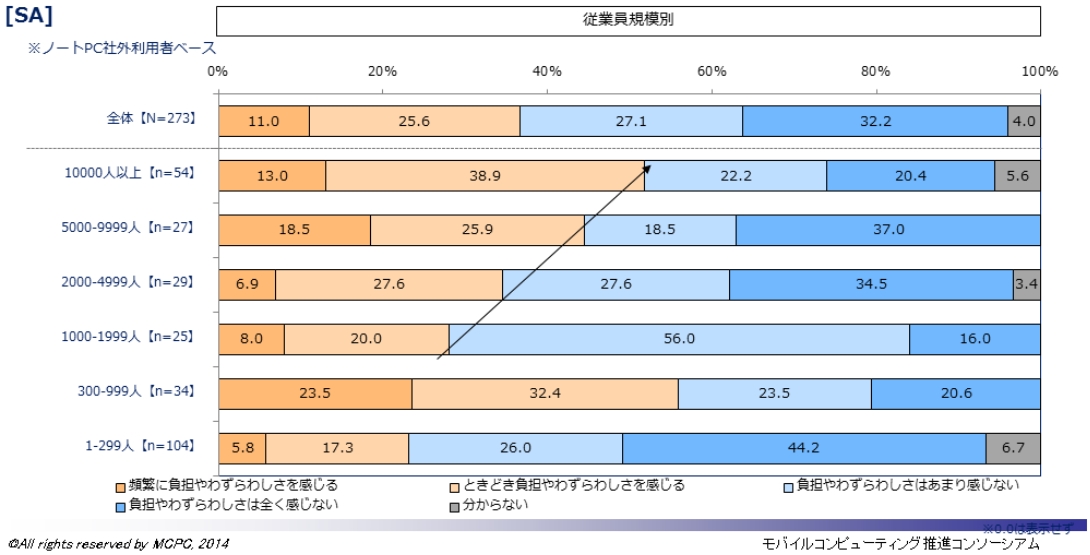
28.回答者の社外ノートPC持ち出し(Q19)

- 情報処理サービス業では、「会社から支給・貸与の自分専用のノートPC」が44.6%と他の業種に比べ多い。



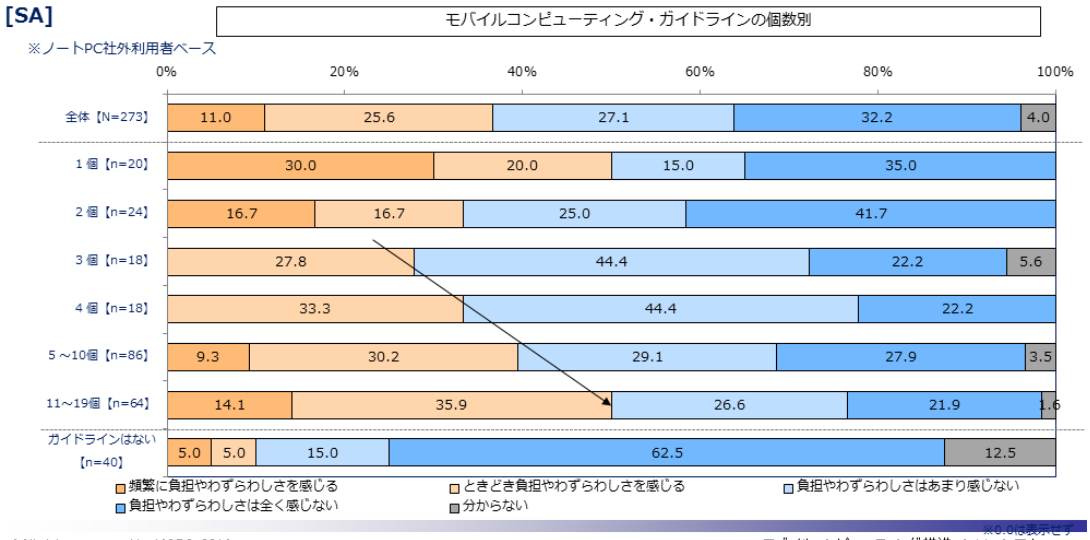
29.ノートPCの持ち出しの手間(Q20)

- ノートPCの持ち出しの手間感は、従業員規模が大きいほど増加する傾向が若干見られる。



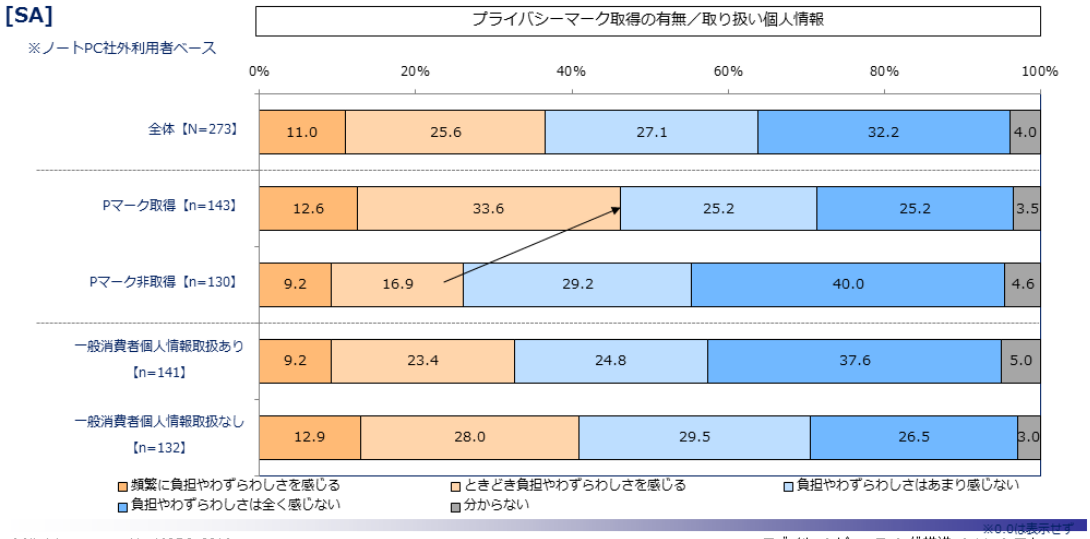
30.ノートPCの持ち出しの手間(Q20)

- Q26のガイドラインの個数別に持ち出しの手間感を分析した。
- 「3個」以上では、参考値ながらガイドラインの個数と「わずらわしさ」には一定の相関が見られる。



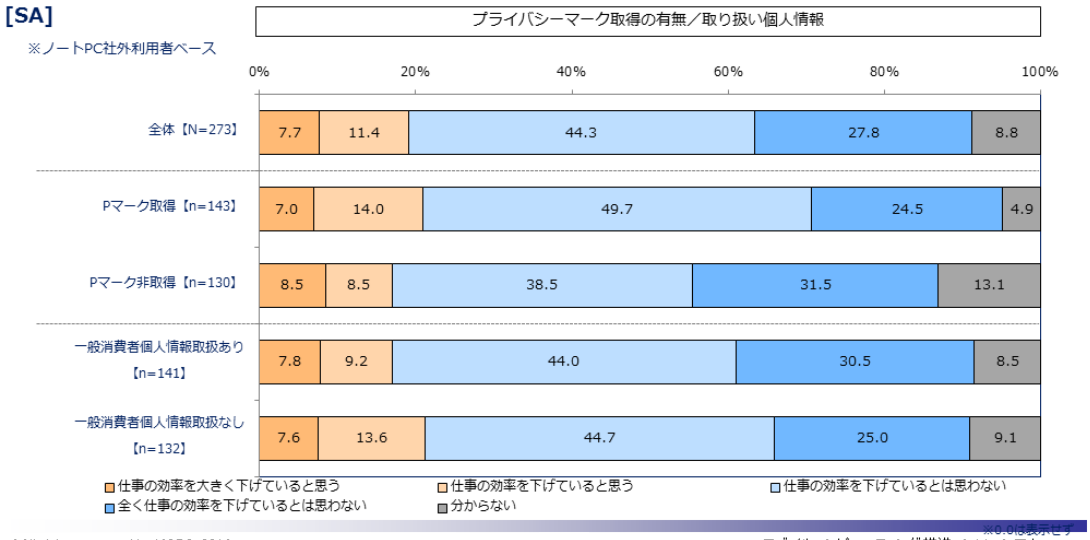
31.ノートPCの持ち出しの手間(Q20)

- Pマーク取得層は、非取得層に比べ「ときどき負担やわずらわしさを感じる」が多く、負担感が強い。
- 一般消費者の個人情報取扱の有無による差は、非取扱層でやや負担感が強い。



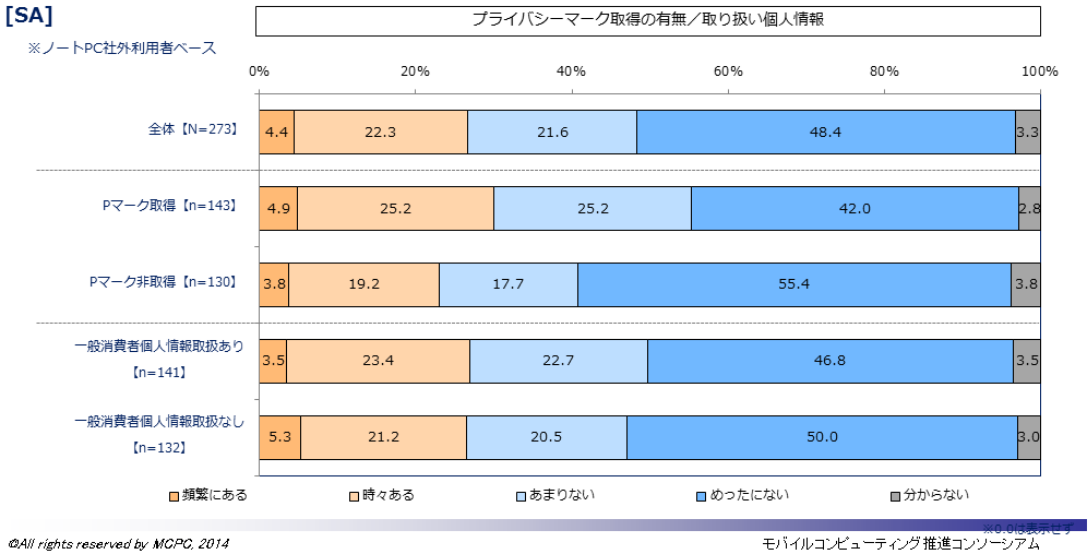
32.ノートPCによる業務効率への影響(Q21)

- ノートPCの社外持ち出しによる業務効率への否定的影響はあまり見られない。



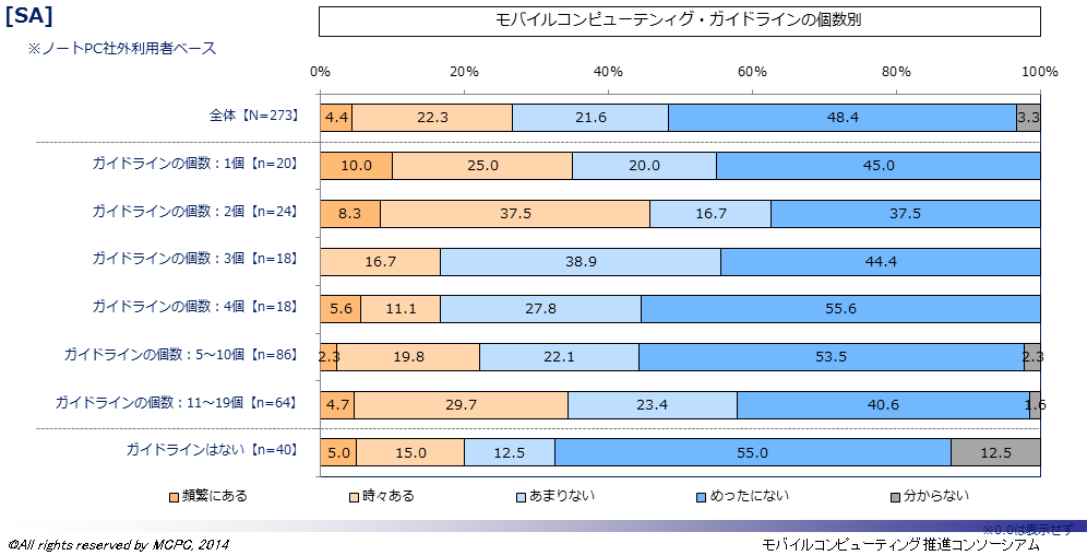
33.持ち出しの手間などによるモバイルコンピューティングの断念(Q22)

- 持ち出しの手間が障壁となってノートPCの持ち出しを断念したことがあるかたずねた。
- Pマーク取得層は非取得層に比べ「時々ある」がやや多い。
- 一般消費者個人情報の取扱有無による差は見られなかった。



34.持ち出しの手間などによるモバイルコンピューティングの断念(Q22)

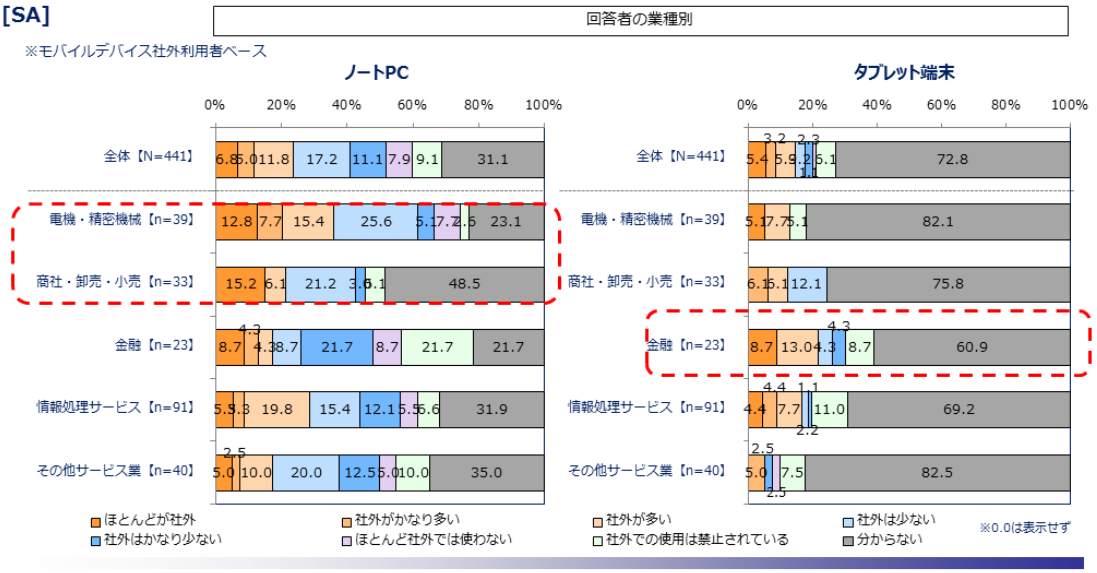
- モバイルコンピューティングのガイドラインに関する個数と、持ち出し断念の頻度には緩やかな相関が見られ、ガイドラインの個数11～19個の層では合計34.4%が断念をしている。



35.回答者の社外でのモバイルコンピューティング比率(Q23)

- モバイルデバイスの社外使用比率をたずねた。
- 「電機・精密機械」及び「商社・卸売・小売」の回答者はノートPCの社外使用率が高い。
- 「金融」はタブレット端末の社外使用率が他業種に比べ高い。

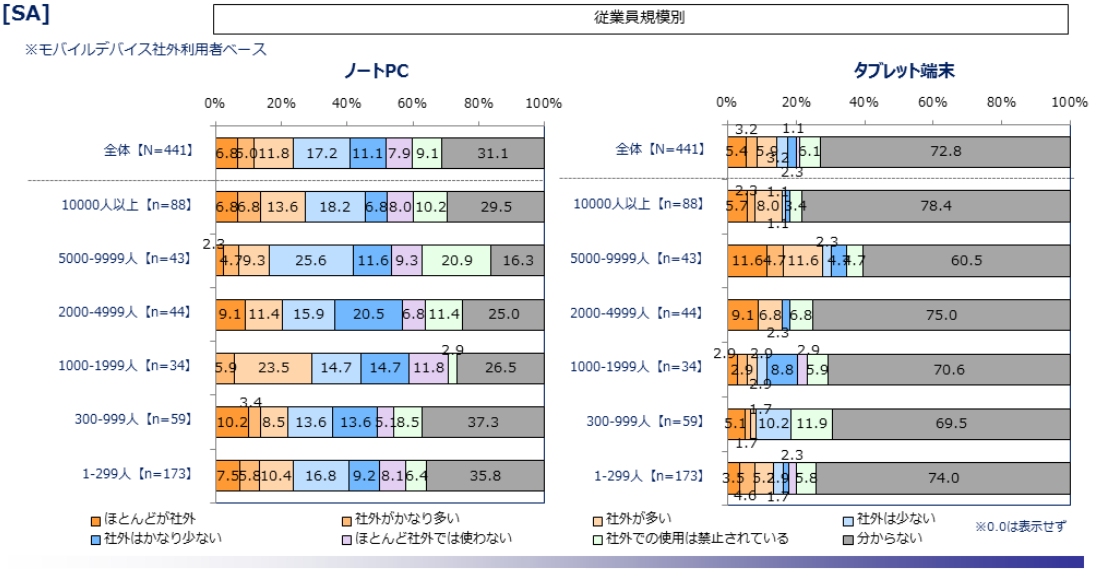
[SA]



36.回答者の社外でのモバイルコンピューティング比率(Q23)

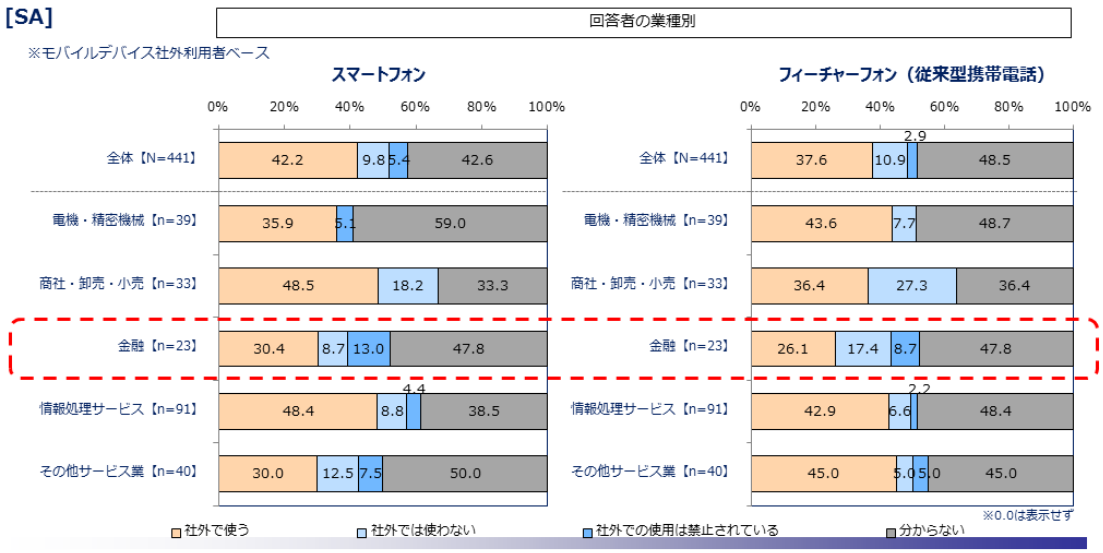
- 従業員規模によるノートPC、タブレット端末の社外使用比率には大きな差は見られない。

[SA]



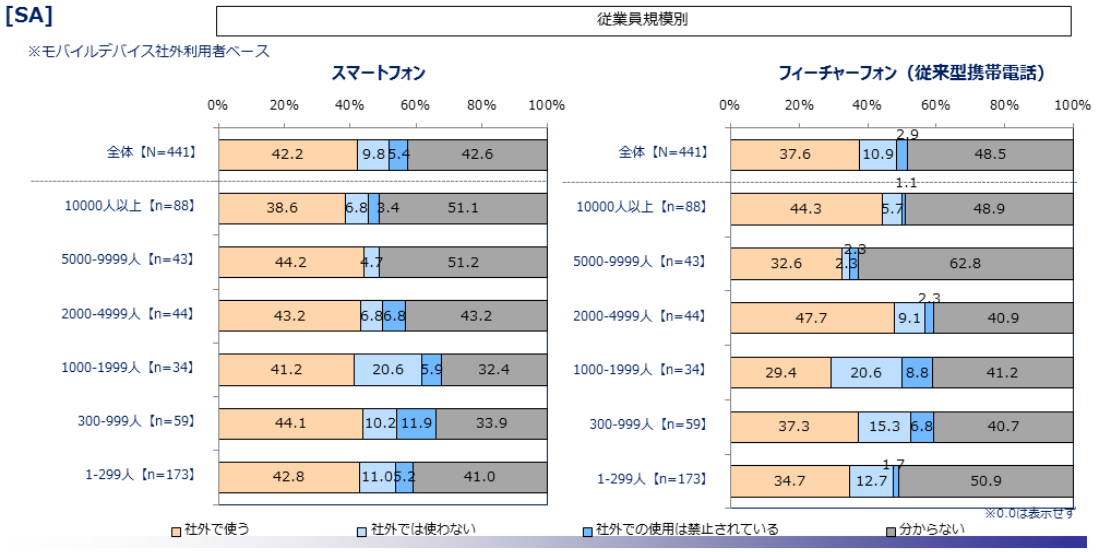
37.回答者の社外でのモバイルコンピューティング状況(Q24)

- スマートフォン・フィーチャーフォンのいずれも、金融業での社外使用率が低く、社外使用禁止率が他業種に比べ高いのが目立つ。



38.回答者の社外でのモバイルコンピューティング状況(Q24)

- 従業員規模によるスマートフォンの社外利用率の差は小さい。
- フィーチャーフォンの社外使用率はばらつきが見られる。



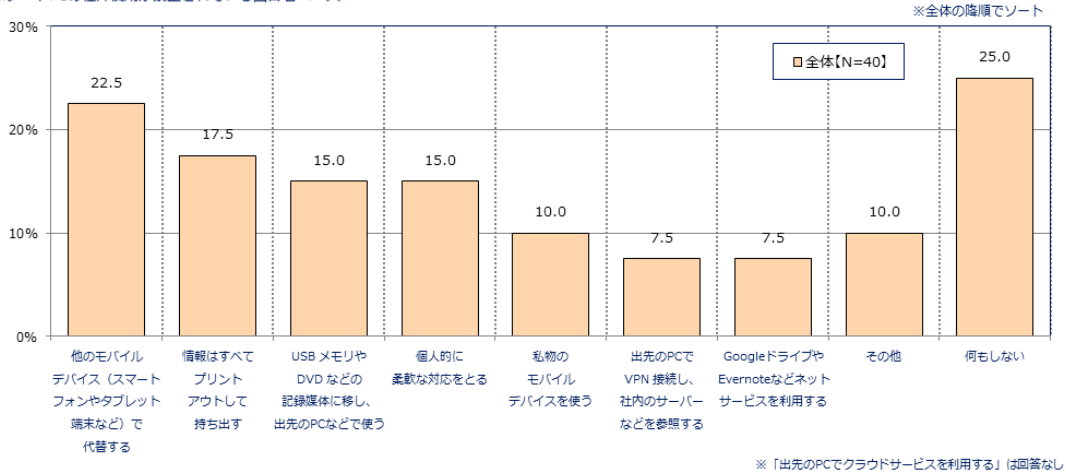
39.社外使用禁止時の代替手段(Q25)

- ノートPCの社外使用が禁止されている回答者に、代替手段をたずねた。
- 「出先のPCでVPN接続」以外の代替手段は、いずれもデータ媒体の紛失等のリスクを伴うものである。
- 最も多かったのは「他のモバイルデバイスで代替する」(22.5%)。

[MA]

※ノートPCの社外使用が禁止されている回答者ベース

※全体の降順でソート



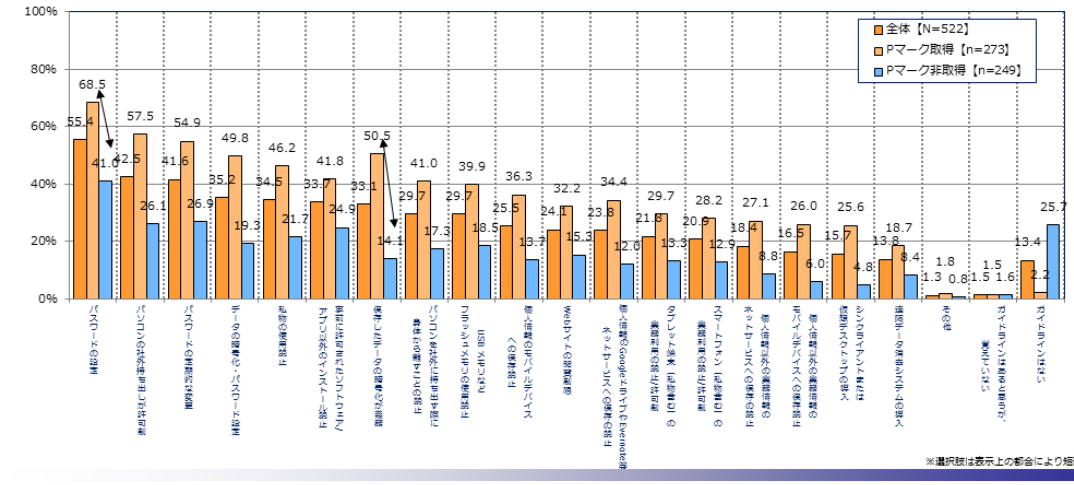
※「出先のPCでクラウドサービスを利用する」は回答なし

40.モバイルコンピューティングに関するガイドラインの内容 (Q26)

- モバイルコンピューティングに関するガイドラインの内容をたずねた。
- 最も多かったのは「パスワードの設定が義務」(55.4%)。
- Pマーク取得層は非取得層よりガイドラインの項目が多く、特に「データの暗号化」(50.5%)が高い。

[MA] プライバシーマーク取得の有無

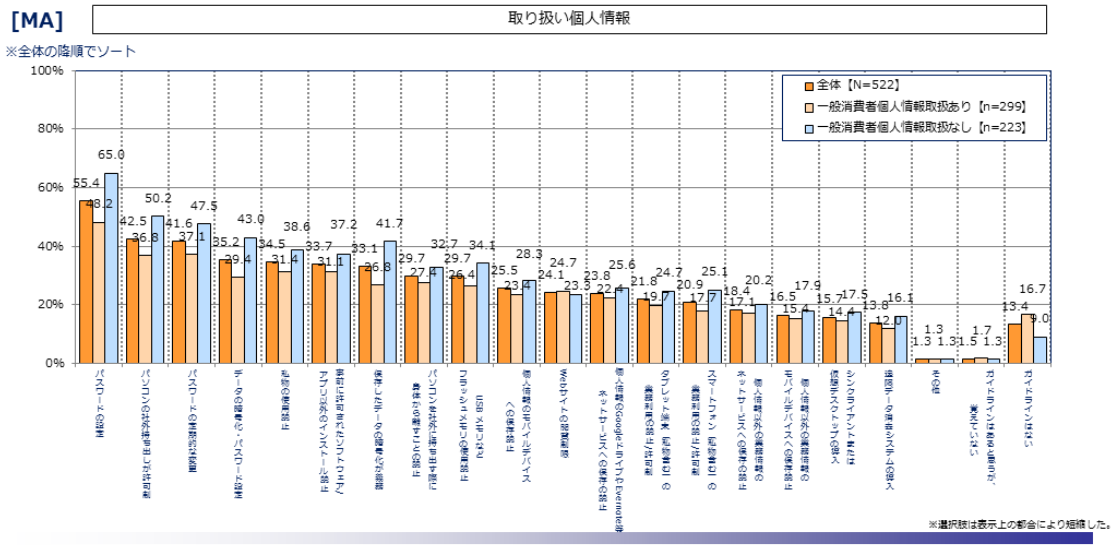
※全体の降順でソート



※選択肢は表示上の都合により短縮した。

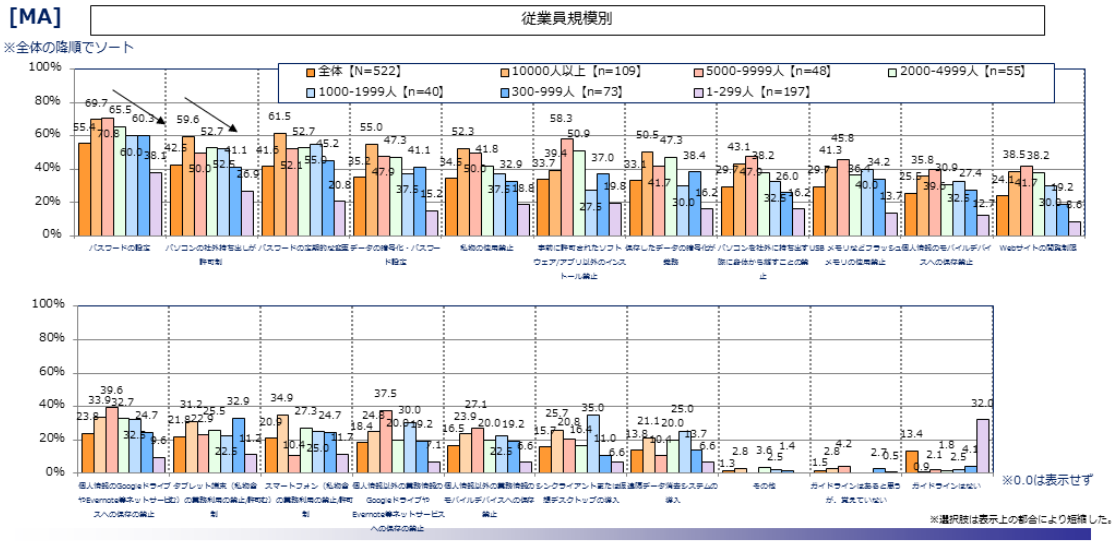
41.モバイルコンピューティングに関するガイドラインの内容 （Q26）

- 一般消費者個人情報の取扱有無によるガイドラインの状況は、一般消費者個人情報の取り扱いがないケースの方が概ね多く挙げられている。



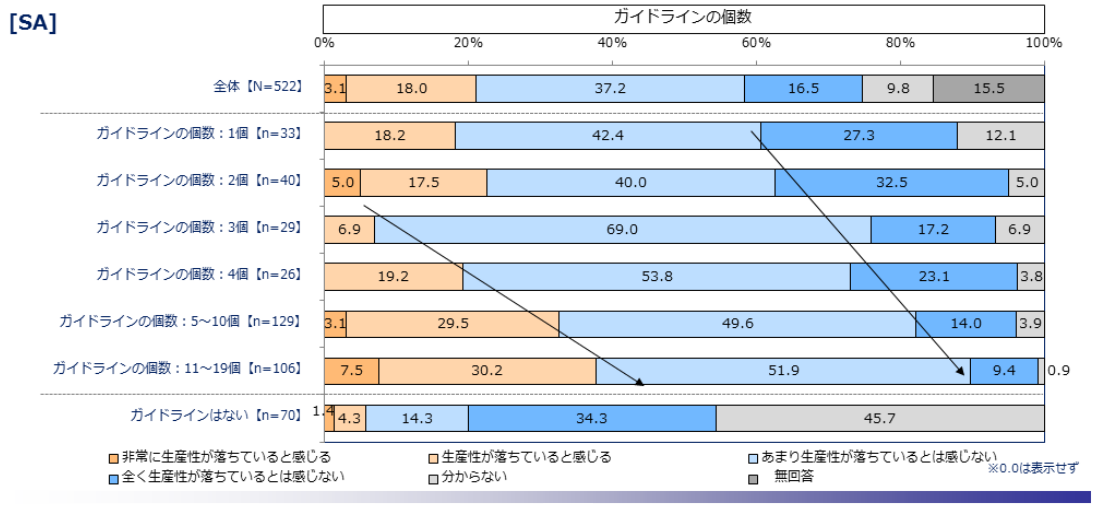
42.モバイルコンピューティングに関するガイドラインの内容 （Q26）

- 従業員規模別では、従業員規模の大きい規模の方が各項目の制定率が高い傾向
- 他方、1-299人の層では、回答者の32%が「ガイドラインはない」と回答している。



43.ガイドラインの束縛レベル(Q27)

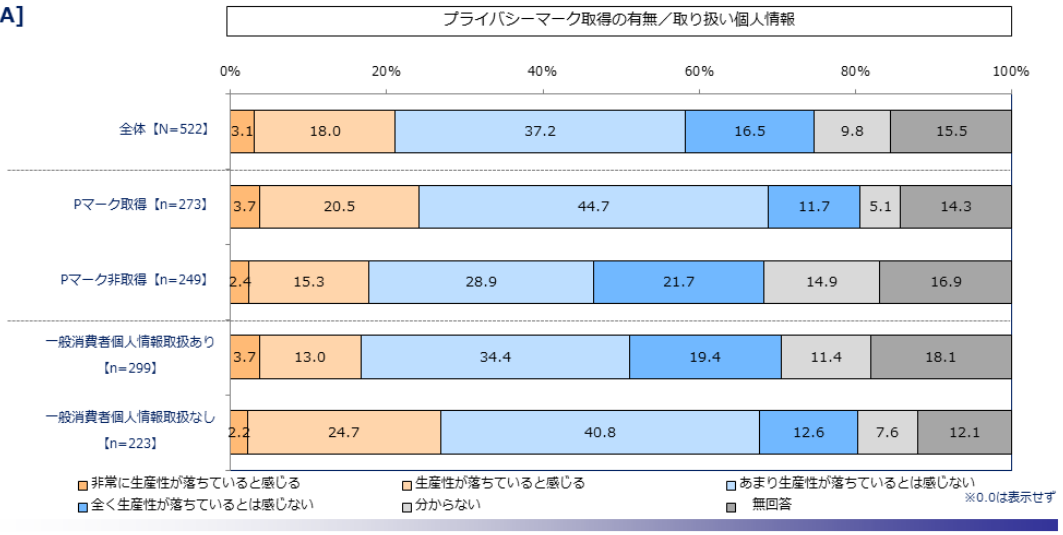
- モバイルコンピューティングに関するガイドラインによる生産性への影響をたずねた。
- ガイドラインの個数と生産性への影響については個数が多くなると「生産性が落ちている」の比率が高まる関係が見られる。
- 特にガイドラインの個数が11～19個のケースでは約4割が生産性が落ちていると回答している。



44.ガイドラインの束縛レベル(Q27)

- Pマークの有無では、ガイドラインの項目が多いPマーク取得層は生産性への悪影響を指摘する割合が非取得層より若干高い。
- 一般消費者個人情報の取扱の有無では「なし」での生産性低下がやや目立つ。

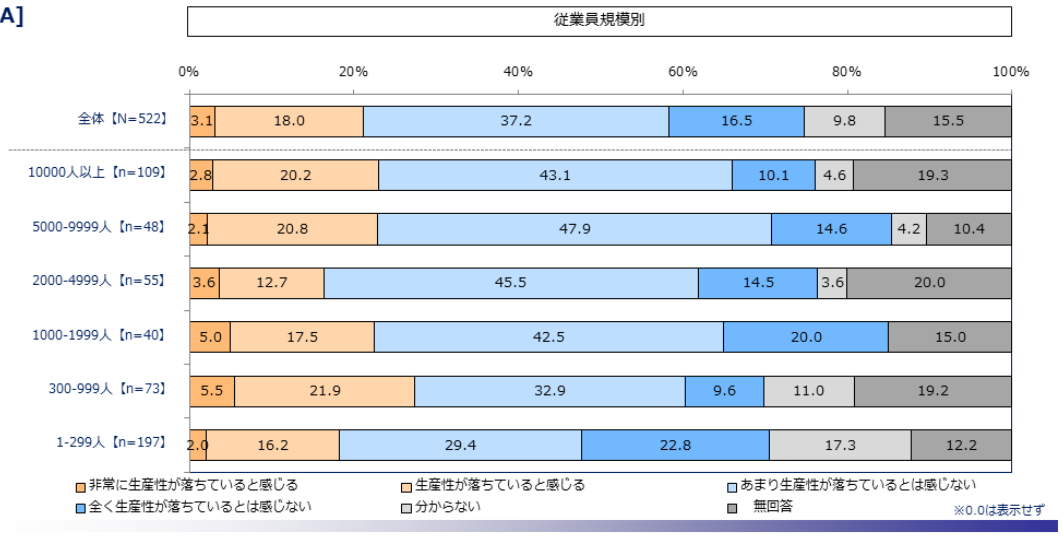
[SA]



45.ガイドラインの束縛レベル(Q27)

- 従業員規模と、ガイドラインによる生産性への悪影響についての関係性は弱い。
- ただし、「1-299人」の層では「全く生産性が落ちているとは感じない」が22.8%と多い。

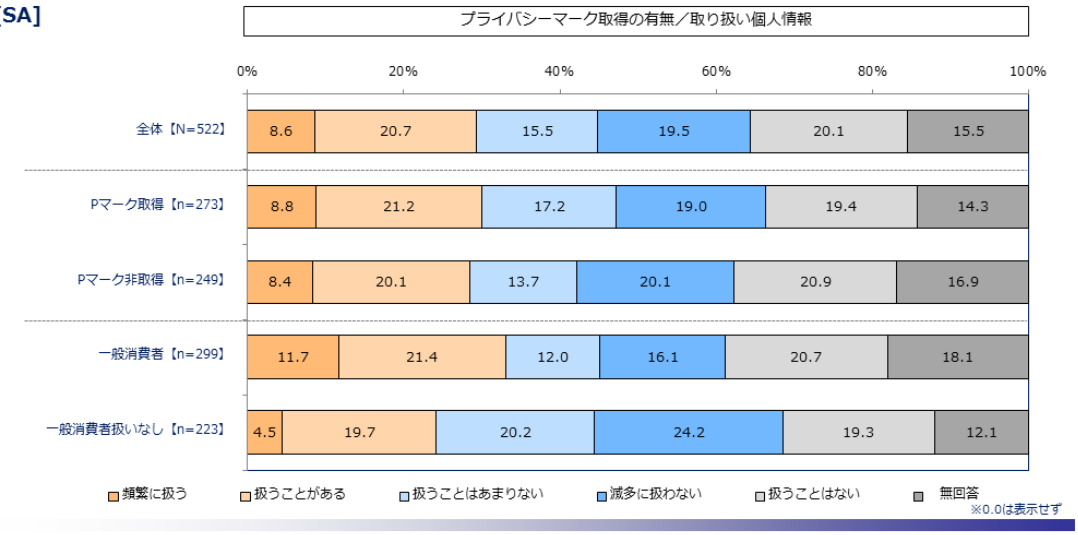
[SA]



46.個人情報社外業務利用の有無(Q28)

- 社外で個人情報を扱う業務をするかたずねた。扱うことがあると回答したのは合計で約3割。
- Pマークの取得の有無、一般消費者個人情報の取扱の有無による社外での個人情報取扱率には大きな差は見られない。

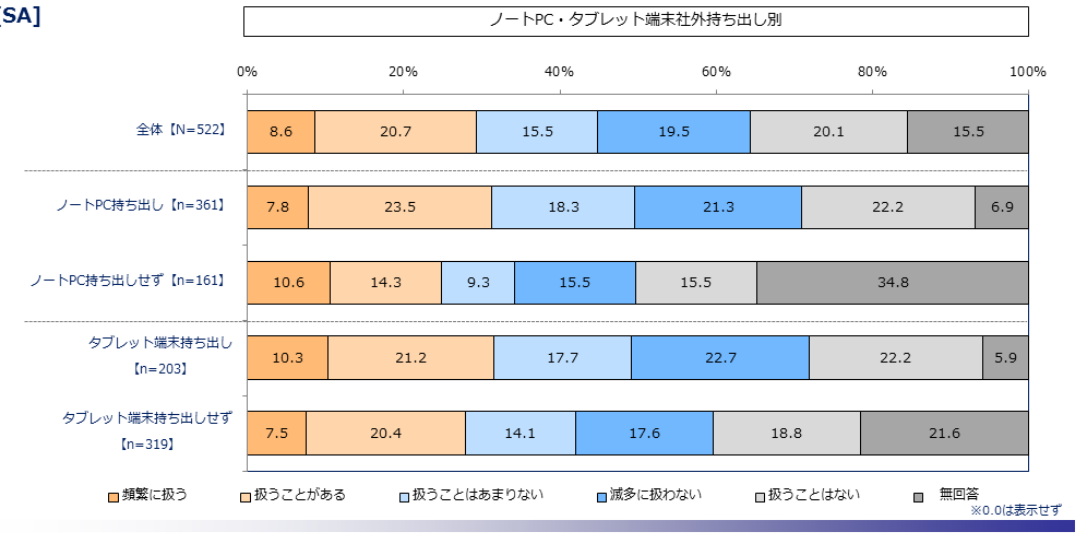
[SA]



47.個人情報社外業務利用の有無(Q28)

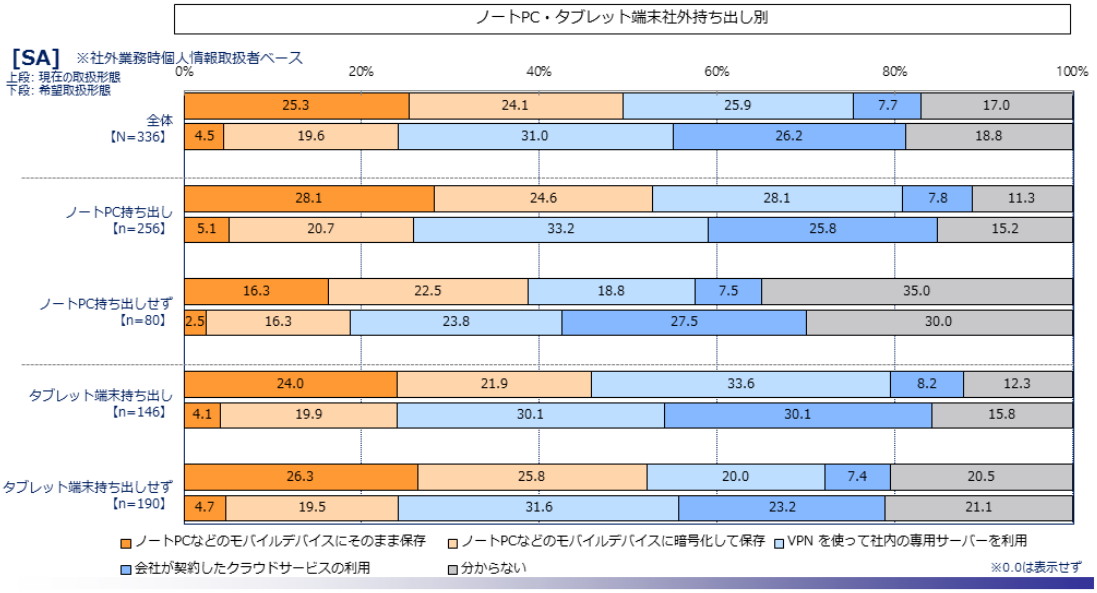
- ノートPC、タブレット端末共に、社外に持ち出すケースでの個人情報社外利用率が非持ち出し層を若干上回る。

[SA]



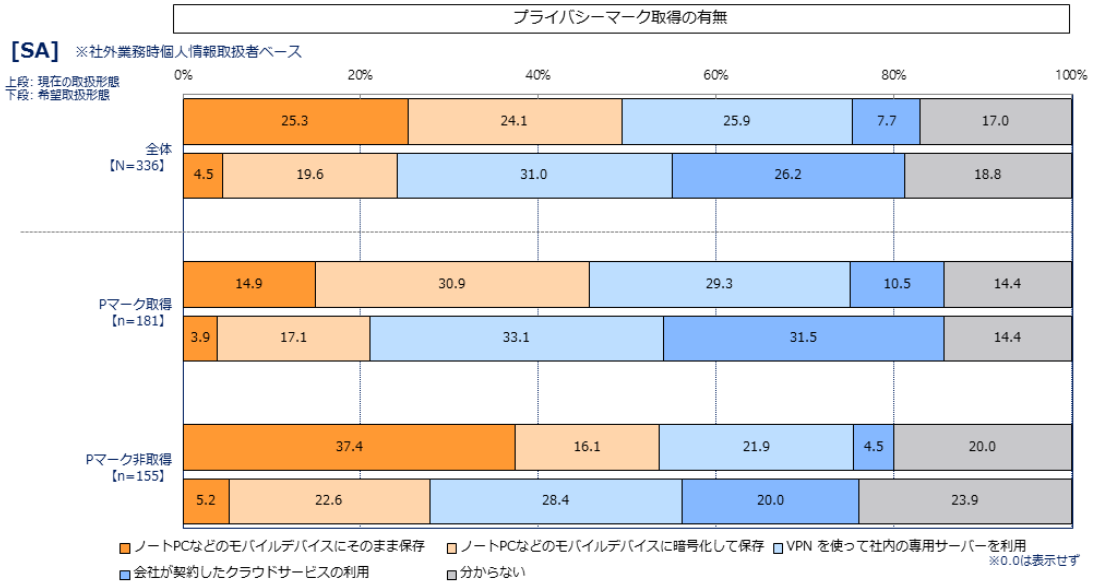
48.個人情報社外業務取扱時の希望形態(Q29)

- 社外で個人情報を扱う際の保存形態について、現状と希望を聞いた。
- 現状はローカルへの保存が多い一方、クラウドやVPN接続を希望する声が多い。



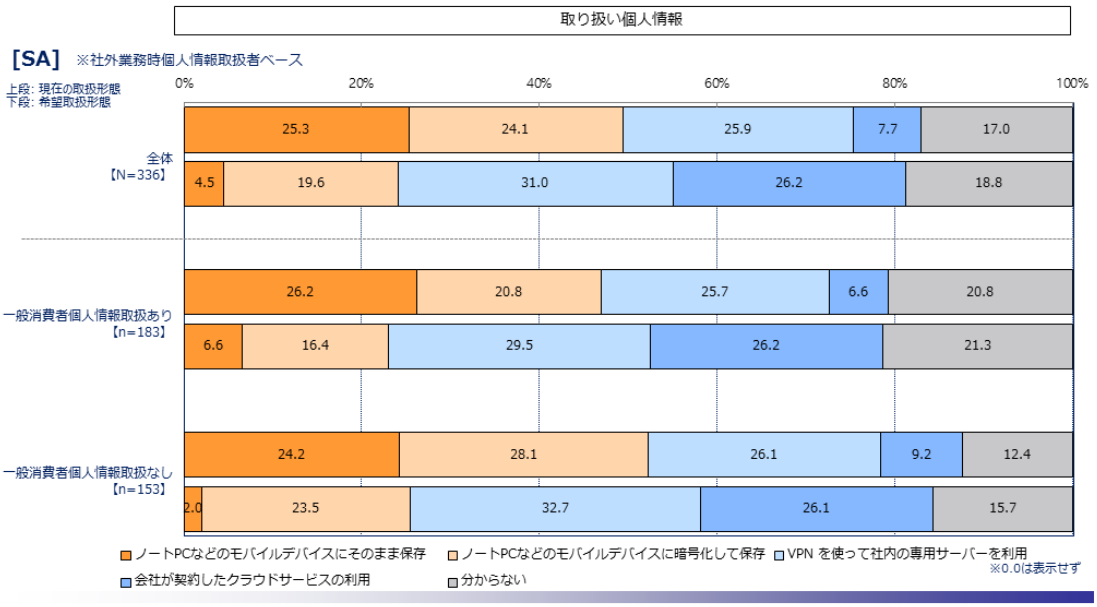
49.個人情報社外業務取扱時の希望形態(Q29)

- Pマークの取得/非取得にかかわらず、VPN利用やクラウドサービスへの希望は強い。



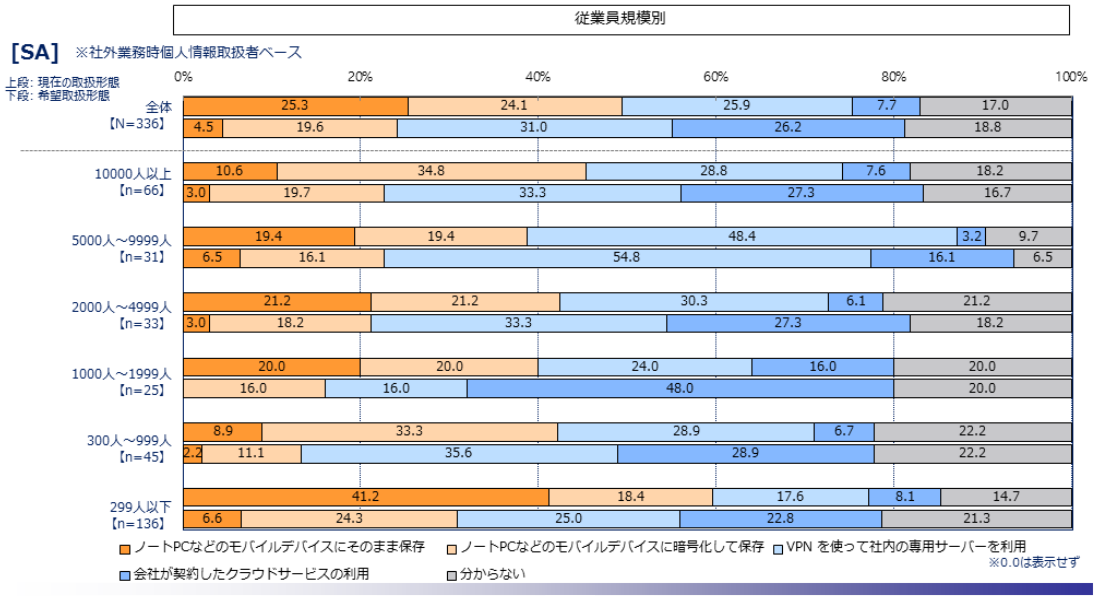
50.個人情報社外業務取扱時の希望形態(Q29)

- 一般消費者個人情報取扱の有無に関わらず、いずれもVPNあるいはクラウドへの個人情報保存を望む声は強い。



51.個人情報社外業務取扱時の希望形態(Q29)

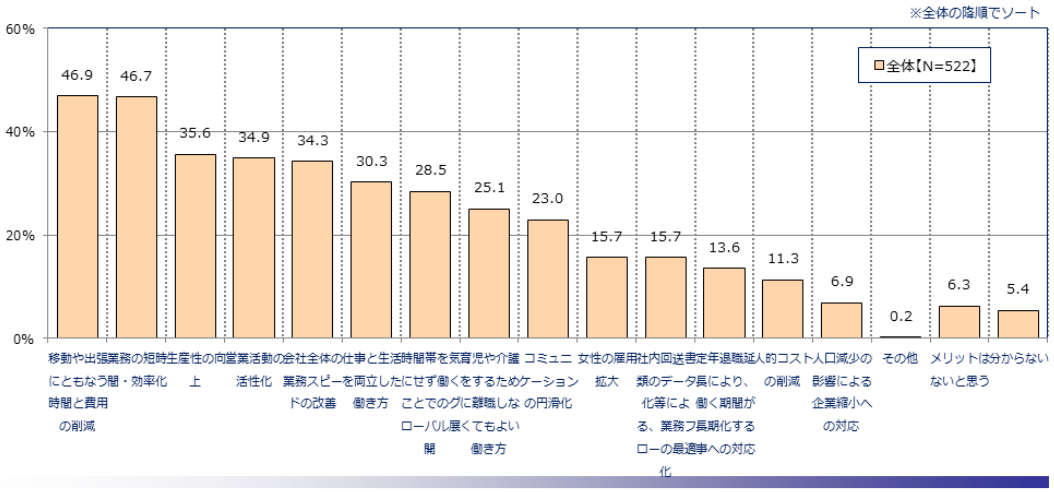
- 299人以下のケースではローカルへの個人情報保存率が高い。
- いずれの従業員規模でも、VPN接続やクラウドを希望する声が中心である。



52.サテライトワークのメリット(Q30)

- サテライトワークが実現するともたらされると考えられるメリットについてたずねた。
- 「移動や出張にともなう時間と費用の削減」と「業務の短時間・効率化」がいずれも5割近く挙げられた。

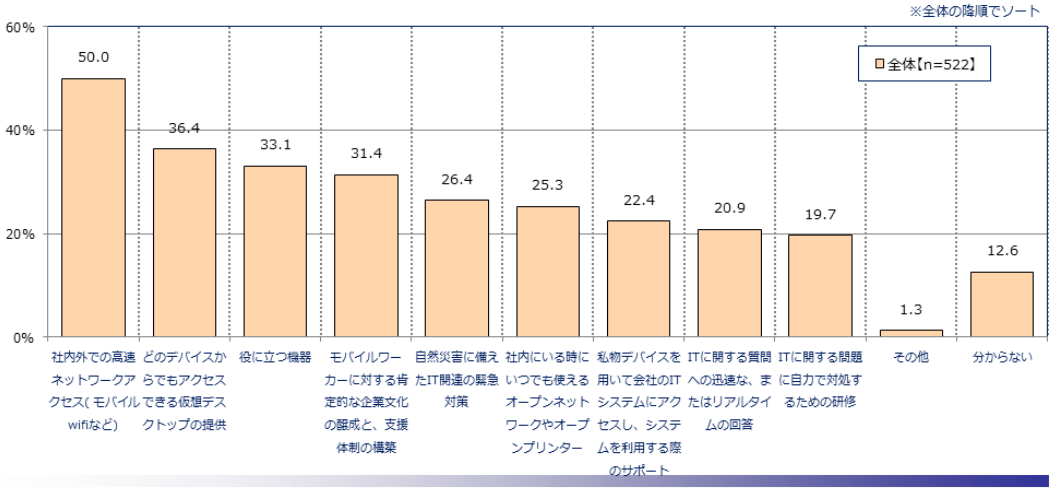
[MA]



53.モバイルワーカーへのサポート(Q31)

- モバイルワーカーへの支援策として最も多く挙げられたのは「高速ネットワークアクセス」でのデバイスからもアクセスできる仮想デスクトップ」(36.4%)、「役に立つ機器」(33.1%)、「モバイルワーカーに対する肯定的な企業文化」(31.4%)が上位に挙げられた。

[MA]



モバイルデバイスの積極的な利活用における個人情報保護法の影響調査				最終版
調査名			モバイルデバイスの積極的な利活用における個人情報保護法の影響調査	特段の指定がない限りすべて回答必須
Qno.	Type		質問文/選択肢	摘要
				スクリーニング
Q1	S		回答者の勤務状況	
			あなたご自身はフルタイムのお仕事をお持ちですか。(ひとつだけ)	
		1	はい	
		2	いいえ →調査終了です	調査終了
Q2	S		回答者の立場・所属部門	
			あなたの勤務先での所属部門は以下のどれにあてはまりますか。(最も近いものひとつだけ)	
		1	経営全般	
		2	経営企画／調査	
		3	情報システム	調査終了
		4	総務／庶務／法務	調査終了
		5	経理／財務	調査終了
		6	人事／教育	調査終了
		7	宣伝／マーケティング	
		8	広報	
		9	販売／営業	
		10	接客／顧客対応(コールセンター含む)	
		11	保守／サポート(コールセンター除く)	
		12	研究／開発／設計	
		13	製造／生産／検査	調査終了
		14	専門職(医師・弁護士など)	調査終了
		15	その他	調査終了
Q3	S		個人情報取扱の有無	順序はそのまま
			あなたの勤務先では、顧客などの個人情報の取扱がありますか。(ひとつだけ)	
		1	個人情報を取り扱っており、プライバシーマークを取得している	
		2	個人情報を取り扱っているが、プライバシーマークを取得していない	
		3	個人情報の取扱はない	従業員の個人情報もあるので本当はあり得ないが調査終了
		4	分からない	調査終了
Q4	S		個人情報業務利用の有無	順序はそのまま
			あなた自身は、個人情報(個人を特定できる3,000件以上の情報)を業務で取り扱っていますか。当てはまるものをひとつお答え下さい。	
		1	頻繁に扱う	
		2	扱うことがある	
		3	扱うことはあまりない	
		4	滅多に扱わない	
		5	扱うことはない	
			ページ遷移	
			ここからは、あなたのお勤め先についておうかがいいたします。	スクリーニング
Q5	S		回答者の業種	順序はそのまま
			あなたの勤務先の業種は、以下のどれですか。(主なものひとつだけ)	
		1	農林・水産・鉱業	
		2	建設・土木	
		3	化学・薬品	
		4	食品	
		5	石油・ゴム	
		6	繊維・紙・木材	
		7	鉄・非鉄金属・窯業	
		8	輸送機械・関連部品	
		9	一般機械	
		10	コンピュータ/ネットワーク機器製造	
		11	電機・精密機械(コンピュータ/ネットワーク機器製造を除く)	
		12	その他製造	
		13	コンピュータ/ネットワーク機器販売	
		14	商社・卸売・小売(コンピュータ/ネットワーク機器販売を除く)	
		15	銀行・保険・証券・信販	
		15	不動産	
		16	運輸・倉庫	
		17	通信	
		18	電気・ガス	
		19	放送・新聞・出版・印刷・映画	
		20	情報処理サービス、システム・インテグレータ、ソフトハウス	
		21	医療関連・病院・医療機関	
		22	大学・研究／教育機関	
		23	専門サービス業(弁護士、会計士など)	
		24	その他サービス業	
		25	官公庁/非営利団体	
		26	その他	
Q6	S		回答者の勤務先の従業員規模	順序はそのまま
			あなたの勤務先の従業者数をお聞かせください。※アルバイト・パート・派遣社員などを含め、全社のおおよその合計人数をお答えください。	
		1	1～299人	
		2	300～499人	
		3	500～999人	
		4	1000～1999人	
		5	2000～4999人	
		6	5000～9999人	
		7	1万人以上	

		8	分からない
ページ遷移			
			ここからは、あなたのお勤め先での個人情報の取扱いについておうかがいします。
Q7	M	個人情報取扱社内規定の有無	
			あなたの勤務先では、個人情報の取扱に関して、ガイドラインや社内規定がありますか。(ひとつだけ)
		1	ある
		2	ない
		3	分からない
Q8	M	個人情報管理体制について	
			あなたの勤務先では、どのような組織体制で個人情報を管理していますか。(いくつでも)
		1	個人情報保護管理者(チーフ・プライバシー・オフィサー, CPO)を設置している
		2	個人情報保護担当部署を設置している
		3	部門ごとに管理者を設置して部門管理している
		4	部門の代表者等で構成する委員会を設置している
		5	何らかの体制構築に向けて検討中である
		6	特に整備していない
		7	分からない
Q9	S	個人情報管理部門	
			あなたの勤務先では、個人情報の収集・管理をどのように行っていますか。(ひとつだけ)
		1	自社で全てを行っている
		2	他社へ委託(アウトソーシング)しているが、守秘義務契約を交わしている
		3	他社へ委託(アウトソーシング)しているが、守秘義務契約を交わしているかどうかは知らない
		4	分からない
Q10	M	取り扱っている個人情報	
			あなたの勤務先では、どのような人の個人情報を取り扱っていますか。(いくつでも)
		1	従業員
		2	取引先の担当者
		3	一般消費者
		4	分からない
Q11	M	個人情報管理の運用	
			あなたの勤務先では、個人情報の管理に関して、以下の中で実際に行っている事はありますか。(いくつでも)※「その他」をお選びの方は、具体的にご記入ください。
		1	個人情報など重要な情報ファイルへのアクセス権限の設定
		2	個人情報など重要な情報ファイルを外部とやりとりする場合の担当者の限定
		3	個人情報データベースにアクセスする際の担当部署からの許可
		4	担当部署への個人情報削除依頼の義務化
		5	取得目的外での個人情報の社内利用の禁止
		6	個人情報を利用したマーケティング活動(行動ターゲティング広告含む)の禁止
		7	無線LANを使用した個人情報の送受信の禁止
		8	社内での無線LANそのものの利用の制限・禁止
		9	プライバシーポリシーの策定
		10	インターネット経由で個人情報を入手するときの通信の暗号化(SSLなど)
		11	個人情報データベースにアクセスできる端末の社内LANからの分離
		12	個人情報データベースの利用状況を監視する
		13	個人情報データベースにアクセスできる端末のある場所への入室制限
		14	内部調査部門による個人情報の流出の監視
		15	外部業者に委託して個人情報の流出を監視
		16	その他
		17	いずれも実施していない
		18	よく分からない
Q12	S	個人情報管理の束縛レベル(生産性)	
			Q11でお答えいただいた事柄に関して、あなたの印象に当てはまるものをひとつお選び下さい。
		1	大変業務の負担になっていると思う
		2	業務の負担になっていると思う
		3	業務の負担になっているとは思わない
		4	全く業務の負担になっているとは思わない
		5	分からない
Q13	OA	個人情報保護ガイドラインに関するOA	
			あなたの勤務先の個人情報保護全般に関し、あなた自身がお感じになっていることをご自由にお書きください。 どのようなご意見でも構いません。
		1	
ページ遷移			
			ここからは、あなたのお勤め先でのノートPC等モバイルデバイスの使用についておうかがいします。
Q14	M	モバイルデバイスの支給状況	
			あなたご自身に勤務先から支給されている機器(モバイルデバイス)について、以下の中で当てはまるものをお答え下さい。(いくつでも) ※私物に対する費用補助などは除いてお答え下さい。
		1	ノートPC
		2	タブレット端末
		3	スマートフォン
		4	フィーチャーフォン(従来型携帯電話)
		5	支給されていない
Q15	Mx/M	回答者の社外でのモバイルコンピューティング状況	
			あなたご自身が、実際に社外で業務用にお使いの機器(モバイルデバイス)をお答え下さい。(いくつでも) ※私物をお仕事に使用しているケースも含めてお答え下さい。
		1	ノートPC
		2	タブレット端末
		3	スマートフォン
		4	フィーチャーフォン(従来型携帯電話)
		5	特にない

Q16	Mx/M		回答者の社外でのモバイルコンピューティング状況 あなたと同じ部署の同僚の方が、実際に社外で業務用にお使いの機器（モバイルデバイス）をお答え下さい。（いくつでも） ※私物をお仕事に使用しているケースも含めてお答え下さい。	
		1	ノートPC	
		2	タブレット端末	
		3	スマートフォン	
		4	フィーチャーフォン（従来型携帯電話）	
		5	特にない	排他, 1=eの場合はQ27へ
Q17	S		回答者の社外でのモバイルコンピューティング業務 あなたご自身が社外で行っている業務の内容について、あてはまるものをお答え下さい。（いくつでも）※「その他」をお選びの方は、具体的にご記入ください。	ランダマイズ
		1	情報収集	
		2	事務文書の作成	
		3	企画書の作成	
		4	電子会議（チャットツールの利用を含む）	
		5	スケジュール・プロジェクト管理	
		6	業務日報・月報の作成	
		7	報告書類の作成	
		8	メールのやりとり	
		9	ミーティング・打ち合わせ	
		10	資料説明・プレゼンテーション	
		11	その他	OA必須
Q18	S		回答者の社外でのモバイルコンピューティング業務 現在は行っていないが、今後社外でできれば良いと思う業務について、あてはまるものをお答え下さい。（いくつでも）※「その他」をお選びの方は、具体的にご記入ください。	ランダマイズ, Q17で**選択されなかったものを表示**
		1	情報収集	
		2	事務文書の作成	
		3	企画書の作成	
		4	電子会議（チャットツールの利用を含む）	
		5	スケジュール・プロジェクト管理	
		6	業務日報・月報の作成	
		7	報告書類の作成	
		8	メールのやりとり	
		9	ミーティング・打ち合わせ	
		10	資料説明・プレゼンテーション	
		11	その他	OA必須
		12	特にない	排他
Q19	M		回答者の社外でのモバイルコンピューティング状況 社外に持ち出すノートPCのあなたの部署での運用形態について、あてはまるものをお答え下さい。（いくつでも）※「その他」をお選びの方は、具体的にご記入ください。	順序はそのまま
		1	社内で使用しているノートPCをそのまま持ち出す	
		2	会社から貸与・支給された自分専用の持ち出し用ノートPCがある	
		3	部署で共有の持ち出し専用ノートPCがある	
		4	私物のノートPCを使用している	
		5	その他	OA必須
Q20	S		ノートPCの持ち出しの手間 ノートPCを社外に持ち出す際の手続きについて、負担やわずらわしさを感じることはありますか。（ひとつだけ）	順序はそのまま
		1	頻繁に負担やわずらわしさを感じる	
		2	ときどき負担やわずらわしさを感じる	
		3	負担やわずらわしさはあまり感じない	
		4	負担やわずらわしさは全く感じない	
		5	分からない	
Q21	S		ノートPCによる業務効率への影響 ノートPCの社外持ち出しと仕事の効率に関し、あなたのお考え・印象にあてはまるものをお答え下さい。（ひとつだけ）	順序はそのまま
		1	仕事の効率を大きく下げていると思う	
		2	仕事の効率を下げていると思う	
		3	仕事の効率を下げているとは思わない	
		4	全く仕事の効率を下げているとは思わない	
		5	分からない	
Q22	S		持ち出しの手間などによるモバイルコンピューティングの断念 社外へのノートPCの持ち出しをあきらめることはありますか。（ひとつだけ）	順序はそのまま
		1	頻繁にある	
		2	時々ある	
		3	あまりない	
		4	めったにない	
		5	分からない	
Q23	Mx/S		回答者の社外でのモバイルコンピューティング状況 社外で業務用にお使いの機器（モバイルデバイス）の**社外使用状況**について、それぞれ当てはまるものをひとつお答え下さい。 **※私物をお仕事に使用しているケースも含めてお答え下さい。**	順序はそのまま
	表側	1	ノートPC	
		2	タブレット端末	
	表頭	a	ほとんどが社外	
		b	社外がかなり多い	
		c	社外が多い	
		d	社外は少ない	
		e	社外はかなり少ない	
		f	ほとんど社外では使わない	
		g	社外での使用は禁止されている	

		h	わからない
Q24	Mx/S		回答者の社外でのモバイルコンピューティング状況 業務用にお使いのスマートフォン・フィーチャーフォン（従来型携帯電話）の**社外使用状況**について、それぞれ当てはまるものをひとつお答え下さい。 **※私物をお仕事に使用しているケースも含めてお答え下さい。**
	表側	1	スマートフォンの業務使用
		2	フィーチャーフォン（従来型携帯電話）の業務使用
	表頭	a	社外で使う
		b	社外では使わない
		c	社外での使用は禁止されている
		d	わからない
Q25	M		社外使用禁止時の代替手段 ノートPCの社外使用が禁止されているとお答えの方に：社外でお仕事をする場合に取られている手段について、あてはまるものはどれですか。（いくつでも） ※「その他」をお選びの方は、具体的にご記入ください。
		1	情報はすべてプリントアウトして持ち出す
		2	他のモバイルデバイス（スマートフォンやタブレット端末など）で代替する
		3	USBメモリやDVDなどの記録媒体に移し、出先のPCなどで使う
		4	出先のPCでVPN接続し、社内のサーバーなどを参照する
		5	出先のPCでクラウドサービスを利用する
		6	GoogleドライブやEvernoteなどネットサービスを利用する
		7	私物のモバイルデバイスを使う
		8	個人的に柔軟な対応をとる
		9	その他
		10	何もしない
Q26	M		モバイルコンピューティングに関するガイドラインの内容 モバイルデバイスを社外で使用する際のガイドラインで、あてはまるものはどれですか。（いくつでも）※「その他」をお選びの方は、具体的にご記入ください。
		1	タブレット端末（私物含む）の業務利用の禁止/許可制
		2	スマートフォン（私物含む）の業務利用の禁止/許可制
		3	私物の使用禁止
		4	パソコンの社外持ち出しは許可制になっている
		5	パソコンを社外に持ち出す（搬送する）際に身体から離すことの禁止
		6	保存したデータの暗号化が義務
		7	パスワードの設定が義務
		8	パスワードの定期的な変更が義務
		9	データの暗号化、パスワードの設定
		10	シンクライアントまたは仮想デスクトップの導入
		11	遠隔データ消去システムの導入
		12	個人情報のモバイルデバイスへの保存禁止
		13	個人情報のGoogleドライブやEvernote等ネットサービスへの保存の禁止
		14	個人情報以外の業務情報のモバイルデバイスへの保存禁止
		15	個人情報以外の業務情報のGoogleドライブやEvernote等ネットサービスへの保存の禁止
		16	USBメモリやマイクロSDカードなどフラッシュメモリの使用禁止
		17	事前に許可されたソフトウェア/アプリ以外のインストールの禁止
		18	閲覧/利用可能なWebサイトの制限
		19	その他
		20	ガイドラインはあると思うが、覚えていない
		21	ガイドラインはない
Q27	S		ガイドラインの束縛レベル あなたが社外でモバイルデバイスを使ってお仕事をされる際、Q26でご回答いただいたガイドラインについてどのようにお感じになっていますか。（ひとつだけ）
		1	非常に生産性が落ちていると感じる
		2	生産性が落ちていると感じる
		3	あまり生産性が落ちているとは感じない
		4	全く生産性が落ちているとは感じない
		5	分からない
Q28	S		個人情報社外業務利用の有無 あなたご自身は社外で仕事をされる際、個人情報を扱う業務をされますか。当てはまるものをひとつだけお答えください。（ひとつだけ）
		1	頻繁に扱う
		2	扱うことがある
		3	扱うことはあまりない
		4	滅多に扱わない
		5	扱うことはない
Q29	Mx/S		個人情報社外業務取扱時の希望形態 社外で仕事される際に個人情報を扱う業務をするとお答えの方に：①現在の個人情報の取扱形態 ②あなたがより望ましいと思う取扱形態 の2つについて、最もよく当てはまるものをお答え下さい。（それぞれひとつだけ）
	表側	1	ノートPCなどのモバイルデバイスにそのまま保存
		2	ノートPCなどのモバイルデバイスに暗号化して保存
		3	VPNを使って社内の専用サーバーを利用
		4	会社が契約したクラウドサービスの利用
		5	分からない
	表頭	a	現在の取扱形態
		b	より望ましい取扱形態
			ページ遷移
			ここからは、お仕事に関するあなたのお考えをおうかがいします。
			サテライトワークのメリット

順序はそのまま	
ランダマイズ	
OA必須	
排他	
ランダマイズ	
OA必須	
排他	
排他	
順序はそのまま	
順序はそのまま	
順序はそのまま	
スクリーニング	

Q30	M		社外で仕事をすることによって、どのようなメリットが得られると思いますか。※営業所や客先常駐による業務は、「社外」に含めないものとします。※「その他」をお選びの方は、具体的にご記入ください。	ランダマイズ
		1	仕事と生活を両立した働き方	
		2	女性の雇用拡大	
		3	育児や介護をするために離職しなくてもよい働き方	
		4	定年退職延長により、働く期間が長期化する事への対応	
		5	人口減少の影響による企業縮小への対応	
		6	業務の短時間・効率化	
		7	移動や出張にともなう時間と費用の削減	
		8	社内回送書類のデータ化等による、業務フローの最適化	
		9	会社全体の業務スピードの改善	
		10	営業活動の活性化	
		11	人的コストの削減	
		12	時間帯を気にせず働くことでのグローバル展開	
		13	コミュニケーションの円滑化	
		14	生産性の向上	
		15	その他	OA必須
		16	メリットはないと思う	排他
		17	分からない	排他
Q31	M	モバイルワーカーへのサポート		
			Q31. モバイルワーカー(外出機会が多く、週に3時間以上、社外で仕事をする従業員)向けに、企業はどのようなITサポートを提供するべきだと思いますか。(いくつでも) ※あなたの勤務先以外のケースも想像してお答え下さい。※「その他」をお選びの方は、具体的にご記入ください。	ランダマイズ
		1	私物デバイスを用いて会社のITシステムにアクセスし、システムを利用する際のサポート	
		2	ITに関する質問への迅速な、またはリアルタイムの回答	
		3	社内外での高速ネットワークアクセス(モバイルwifiなど)	
		4	どのデバイスからでもアクセスできる仮想デスクトップの提供	
		5	社内にいる時にいつでも使えるオープンネットワークやオープンプリンター	
		6	役に立つ機器	
		7	ITに関する問題に自力で対処するための研修	
		8	モバイルワーカーに対する肯定的な企業文化の醸成と、支援体制の構築	
		9	自然災害に備えたIT関連の緊急対策	
		10	その他	
		11	分からない	排他
			●以上でアンケートは終了です。ご協力ありがとうございました。	