第一回スマートフォン企業利用実態調査レポート

[文書管理番号：JSSEC-PRDR-RP20130312]

2013 年 3 月 12 日

(Rev.1.0)

一般社団法人日本スマートフォンセキュリティ協会(JSSEC)
パブリックリレーションズ部会
調査分析ワーキンググループ

目次

1 はじめに

一般社団法人日本スマートフォンセキュリティ協会（以下、JSSEC）パブリックリレーション部会に所属する「調査分析ワーキンググループ」では、スマートフォンの利活用に関する利用実態を調査し、リアルな実態を反映した統計データを提供することを目的として 2012 年度から活動を始めた。

今回の調査は、その活動の第一弾としてスマートフォンの企業利用の実態調査を実施した。近年ビジネス面でスマートフォン活用をベースにした展開が広がっていると実感してきているが、その反面活用や取り組みの事例が多く公開・共有されていないため不安を抱えたままの状態で足踏みされている企業が少なくないと思われる。本調査は、ビジネス活用の期待が高いスマートフォンの企業利用の実態を把握することで、安心した活用とスマートフォンのビジネス利用の一助となることを期待している。

今後は、今回の企業利用実態調査に加えてスマートフォンの利用や普及状況に関して利用者の立場や利用環境などについて幅広く調査を行い、スマートフォンをより安心して活用していただくための情報を提供する計画である。

2 調査分析ワーキンググループ 活動メンバー

リーダー	小椋 則樹	（ユニアデックス株式会社）
メンバー	田上 利博	（サイバートラスト株式会社）
	前田 裕文	（株式会社日本総合研究所）
	浅井 奈津樹	（アイ・ティー・シーネットワーク株式会社）
	松本 照吾	（株式会社インフォセック）
	本間 隆修	（日本システム開発株式会社）
	遠藤 宗正	（デジタルアーツ株式会社）
	吉田 明子	（デジタルアーツ株式会社）
	（順不同）	
プロモーション担当		
	パブリックリレーション WG	
	吉田 明子	（デジタルアーツ株式会社）

3 「第一回スマートフォン“企業”利用実態調査」の概要

3.1 調査目的

- 技術や活用方法が急激に変化を繰り返しているスマートフォンについて、企業における実態を捉え、利用面でのニーズを把握する。これによりスマートフォンの導入を検討されている、または本格的なビジネス利用にシフトを計画されている企業利用者に役立つ調査報告の提供を目的としている。

  ※「スマートフォン」とは、スマートフォン、タブレット端末を総称している。

3.2 調査概要

・ 調査項目

企業におけるスマートフォン利用を、以下の 4 つのライフサイクルに分類して、そのフェーズをもとに普及状況を把握する。なお、JSSEC から提供されているガイドラインなどにもライフサイクルについて記述されているが、本調査では利用と普及の観点から以下の 4 つに定義している。

- 計画フェーズ：機種の選定基準、利用場所検討など
- 導入フェーズ：導入規模、通信形態、利用アプリなど
- 利用フェーズ：接続するサービス、セキュリティ対策など
- 運用フェーズ：運用管理方法、管理ツールなど

各設問項目は、主に JSSEC から提供されている各種ガイドライン（巻末の参考文献）などをもとにして、活動メンバーにて新たに設計し作成した。

・ 実施時期

- 2012 年 10 月 1 日～2012 年 10 月 31 日

・ 調査手法

- JSSEC 会員企業メンバーにメールで回答依頼を送付し、Web にてオンライン又は EXCEL ファイル送付により回答。設問数は 50 問、主に選択方式。一部、自由記入方式を使用している。

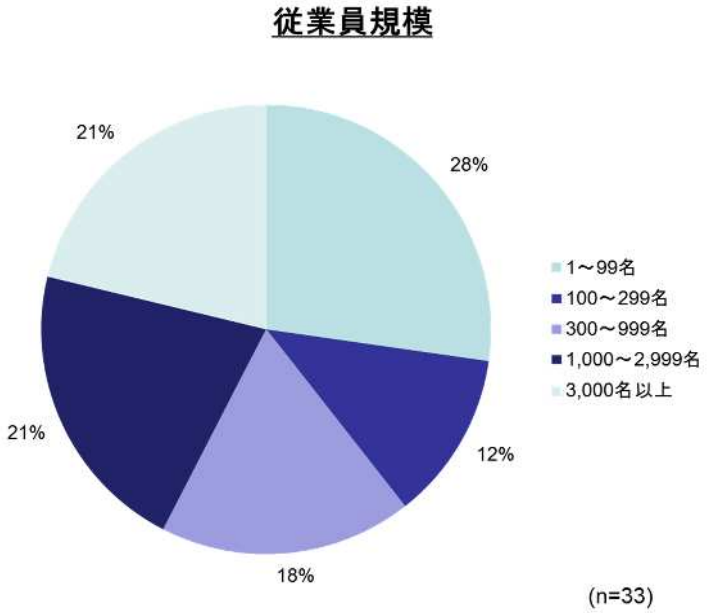
・ 実施対象者

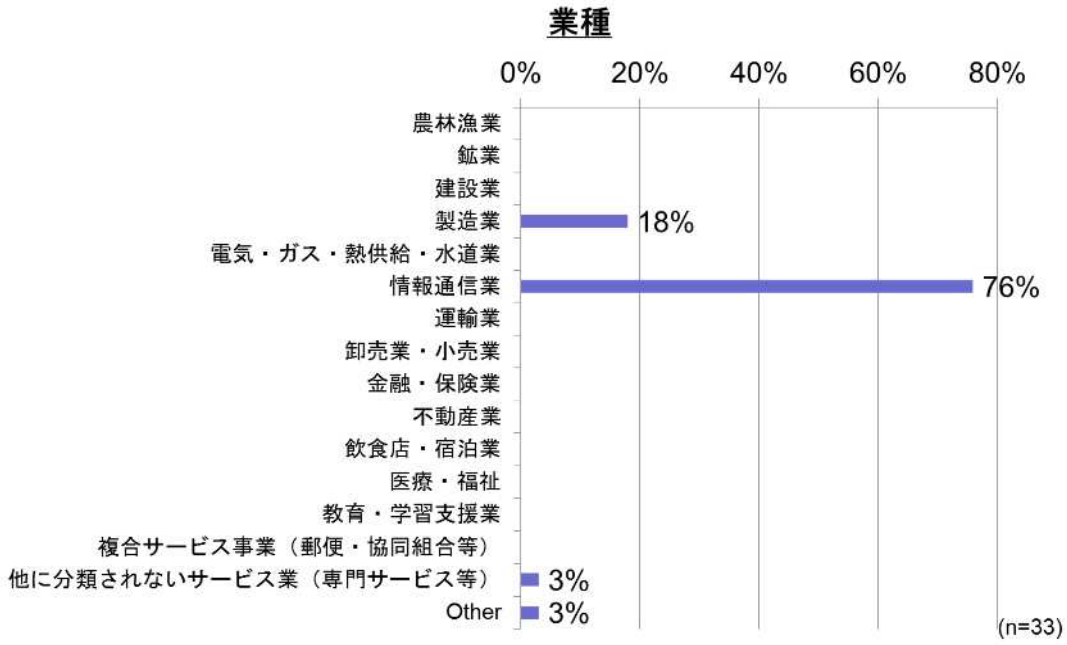
- JSSEC 会員企業（一部会員企業の関連企業も含む）の情報システム部責任者、IT インフラ運用責任者、運用担当者。企業の重複回答はない。

・ 回答企業数

- 33 社

4 調査結果 回答企業内訳





最初に、回答があった企業のプロファイルを示しておく。

まず、企業規模の目安として従業員数を取得した。グラフが示す通り、今回の回答企業の規模は大小平均的に分散している。

業種に関しては情報通信業界が多数であり、主にスマートフォンをビジネスとして積極的に利用する企業と判断している。こ

れは、この調査結果の傾向に影響する要因として捉える必要がある。

以下、各利用フェーズについて調査結果にコメントする。なお、回答によっては、意図と外れたものやデータとして傾向を示さない結果があり、その設問については省略している。

また、設問に付与している記号の意味は、以下の回答方式を示している。

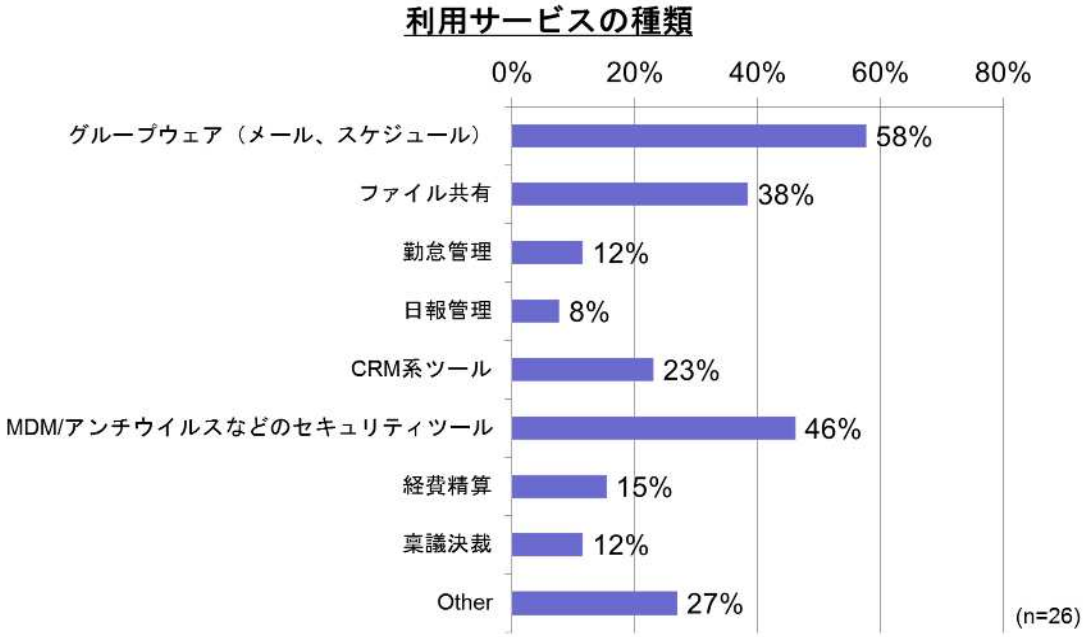
MA：複数回答項目
SA：単一選択項目
FA：自由記入項目

5 計画フェーズ

このフェーズでは、スマートフォンを導入するにあたり最初に検討・準備する段階である。
スマートフォンの導入に対する要求があがり、情報システム部門または利用部門の管理者が、企業内のルール、既存の環境を踏まえて計画していることを想定している。
その利用シーン、活用機能範囲、セキュリティ、運用、コストなどその要件を検討することになる。たとえば、機種の選定基準、通信環境の見直し、利用するアプリ、制限する機能、運用手順、機器情報の把握方法など。
このフェーズは、企業がスマートフォンの利用を目的としているか、事業化の対象としているかで対応が検討の進め方や検討期間が大きく分かれる。

5.1 利用サービスの種類（MA）

スマートフォンを導入し、どのようなサービスを利用するかを検討したかを問いかけている。



(考察)

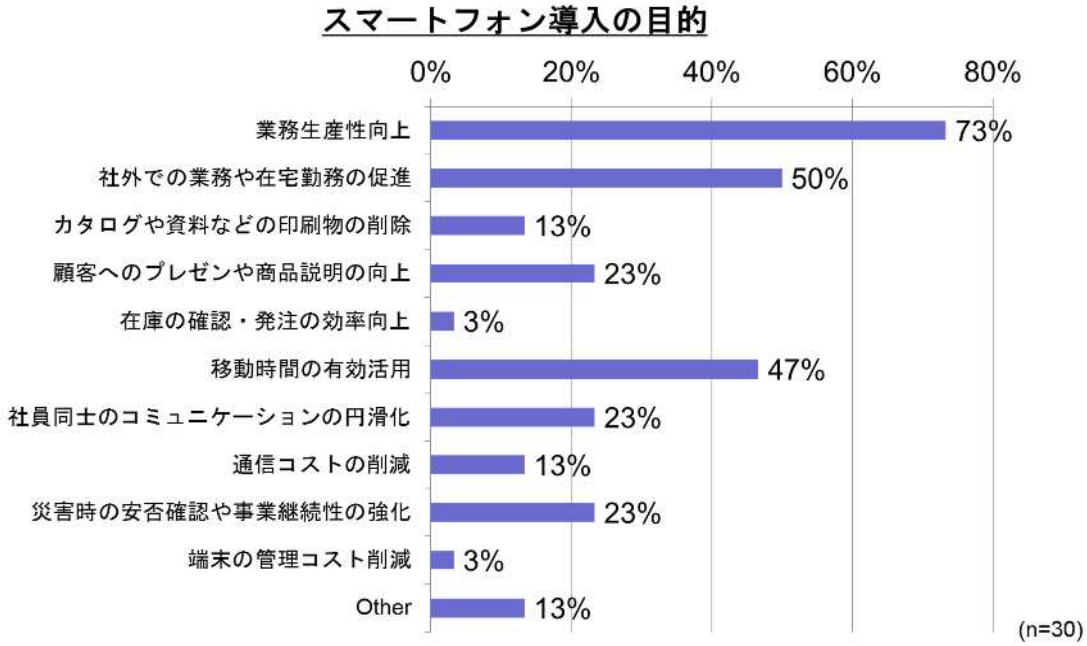
「グループウェア」の利用が多いのは、外出先からメールやスケジュールを即座に確認したいというニーズと導入の手間が少なくすぐに利用できるという提供側のメリットがマッチした結果であり、利用初期段階として多くみられる傾向である。

「MDM/アンチウィルスなどのセキュリティツール」は、企業利用においては必須である。MDM による紛失時の遠隔ロック/ワイプ処理や Android 端末におけるアンチウィルスソフトなどがあげられる。

反面、「勤怠管理」、「日報管理」、「経理清算」、「稟議決済」など企業内手続きとの連携サービスの利用は少ない傾向にあり、業務への活動が進む過渡期にあると推測する。

5.2　スマートフォン導入の目的 (MA)

スマートフォン導入の目的を業務、場所、コストの面からで問いかけている。

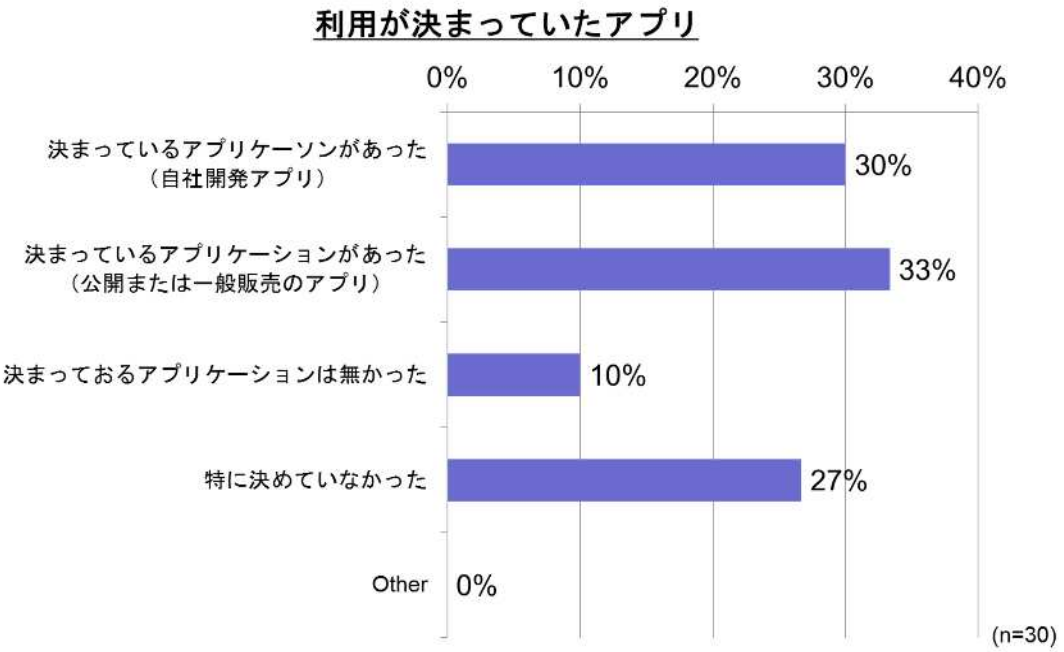


(考察)

スマートフォンの導入の目的としては、「業務生産性向上」が圧倒的に多く、続いて「社外での業務や在宅勤務の促進」、「移動時間の有効活用」と続いた。スマートフォンをネットワークに繋がる機器としてだけではなく、業務とリアルタイムに連携できかつ柔軟な操作性など優れたユーザインタフェースを利用できる機器として捉えている。また、これまで業務遂行の対象ではなかった場所や時間を有効に活用することを期待している。

5.3　スマートフォン導入計画時に決まっていた利用アプリ（MA）

スマートフォンの特長のひとつであるアプリに関して、導入のきっかけになる要因であったかを問いかけている。

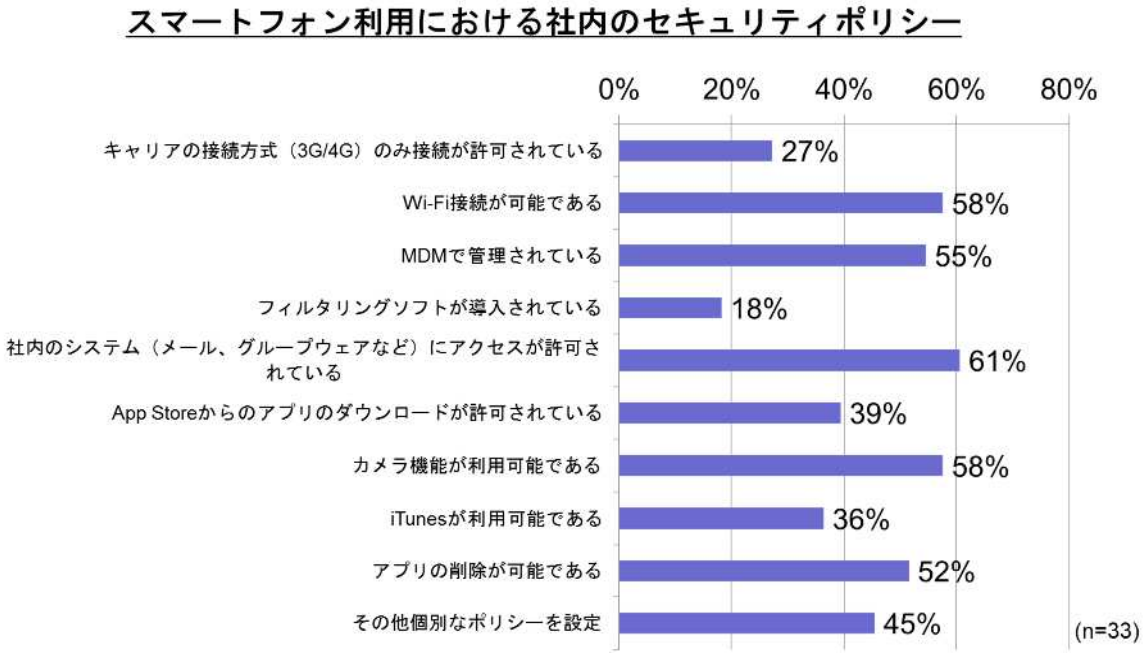


(考察)

ここでは約 3 割の企業において利用シーンを予め設定してスマートフォンを導入したことを示している。自社開発アプリについては、ソリューション提供企業が多いことからその割合が多く表れていると思われる。また、「特に決めていなかった」も 3 割程度あり、これは現段階でワークスタイルの見直しを進めており利用シーンの再設計なども含めて検討していると想定する。

5.4　スマートフォン利用における社内のセキュリティポリシー（MA）

企業での導入においてセキュリティ面の考慮は必須であり、新しいデバイスであるスマートフォンをどの範囲で扱うかを問いかけている。



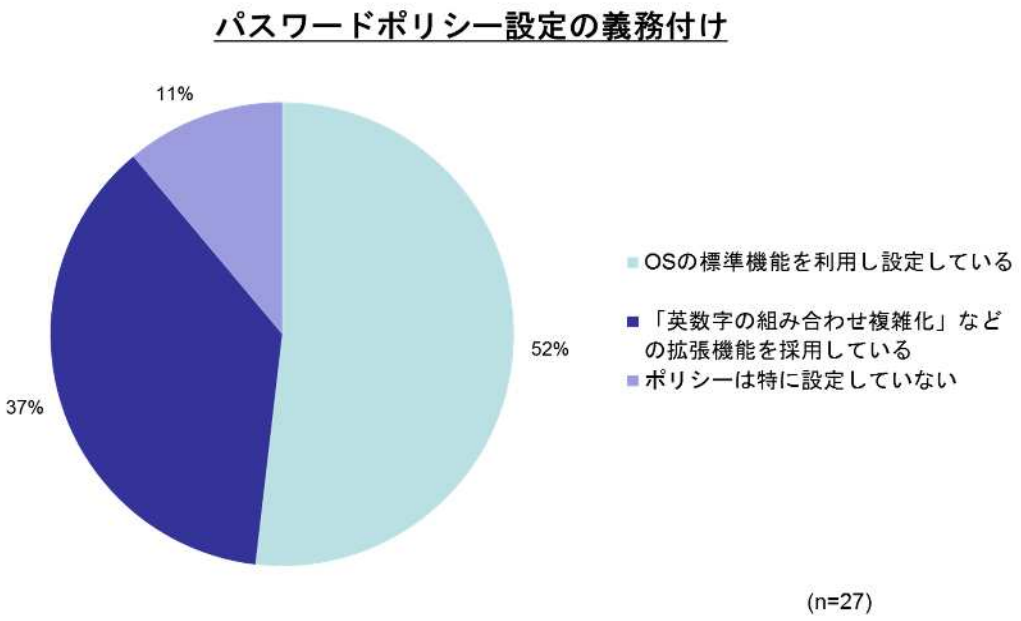
(考察)

企業利用において、セキュリティの対策は非常に重視される。スマートフォンに対しては、ノート PC におけるセキュリティ対策と比較され検討が行われているようである。

ここでも、社内環境への接続（「Wi-Fi 接続が可能である」、「社内システム」）、端末の運用管理（「MDM で管理されている」、「アプリの削除が可能である」）、装着デバイスの制御（「カメラ機能が利用可能である」）といったノート PC において対応している同様の項目の割合が高く出ている。その反面、スマートフォン独自の項目（「AppStore からのアプリのダウンロード」、「iTunes が利用可能である」）は低い割合になっている。スマートフォンの特長はなるべく活用する方向性の表れと捉えることもできる。

5.5　パスワードポリシー設定の義務付け (SA)

パスワードポリシーの設定において利用する機能について問いかけている。

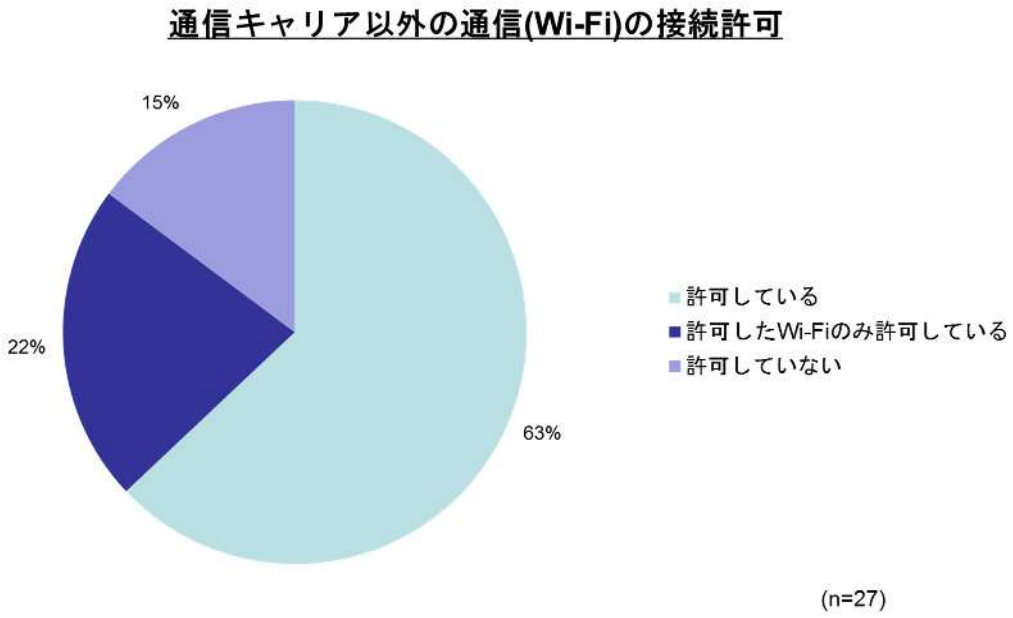


(考察)

セキュリティ対策の基本項目であるパスワードのポリシーについては、約半数が「OS の標準機能を利用し設定している」である。つまり、既成の数字やパターン入力などメーカーが標準として提供する機能の利用を前提にポリシーを設定している。逆に社内のセキュリティポリシーに準ずるように機能を拡張しているのは 37%であり、情報システム部門の統制が行われていると思われる大企業などに多くみられる。また、「ポリシーは特に設定していない」が 1 割もあり、企業として統制するのではなくユーザの判断に任せている。これは、セキュリティの強化と利便性の向上とは諸刃の剣であり、現段階では利便性の向上を重視している傾向が表れている。

5.6　通信キャリア以外の通信 (Wi-Fi) の許可 (SA)

社内ネットワークへの接続において、スマートフォンの Wi-Fi 通信を利用したネットワーク接続が許さているかどうかを問いかけている。

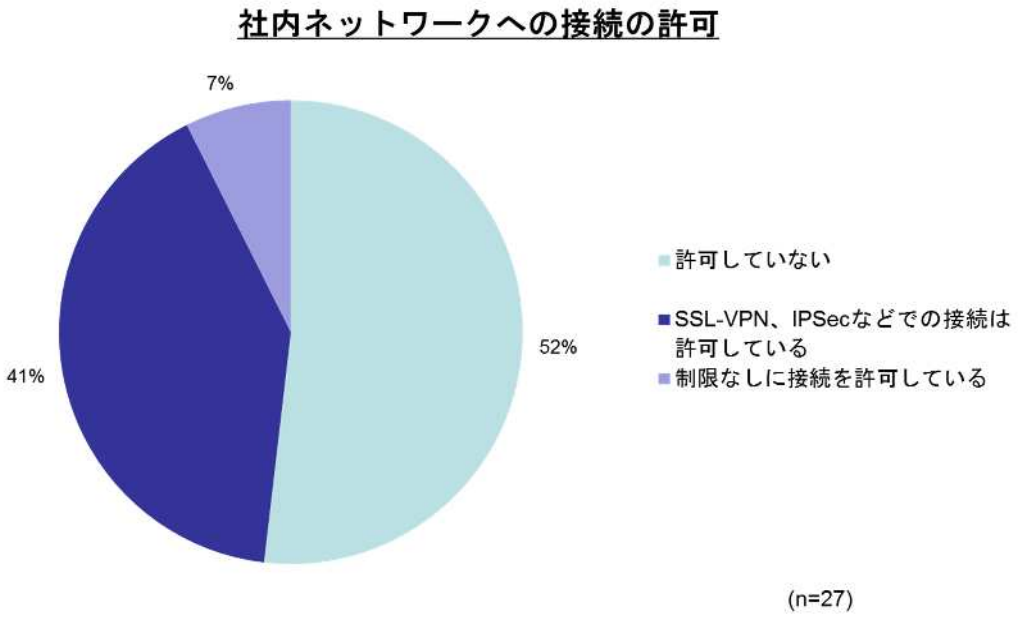


(考察)

「許可している」が 63%、「許可した Wi-Fi のみ許可している」を合わせると 85%に達しており多くの企業が Wi-Fi 利用を許可されている。利用にあたっては、端末認証や MDM(Mobile Device Management)ツールなどにより管理された状況のもとで利用されている傾向がある。これは回答した企業が JSSEC 会員企業であり、スマートフォン活用に積極的である傾向が表れている。

5.7　社内ネットワークへの接続の許可 (SA)

社内のネットワーク環境への接続が許されているのか、またどのような形態で許されているのかを問いかけている。主にWi-Fi を利用したケースを想定しており、USB や Bluetooth で PC などを経由する場合は考慮していない。



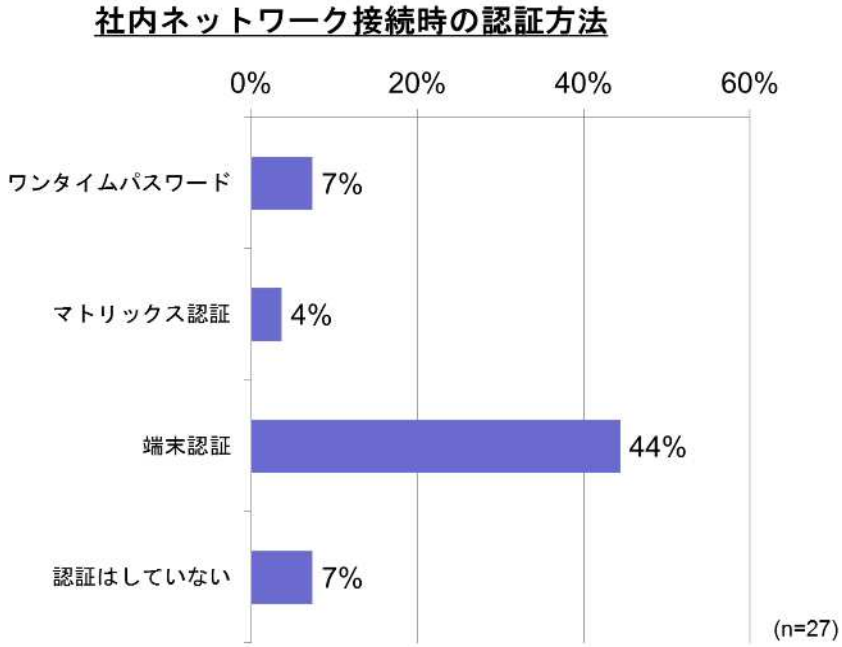
(考察)

およそ半数がスマートフォンの社内ネットワークへの直接接続を許していない。また、SSL-VPN、IPSec VPN など企業が認めたネットワーク経路を利用できる端末は約 40%が社内ネットワークへの接続を許されている。これは、社内リソースをうまく利用するよりも社外のサービスを中心に活用 (社内リソースも社外から) することを意図している。社内のセキュリティ運用 (管理、監視、制御など) やスマートフォンに対応したサービス整備が整っていないために、許可していないことも考えられる。

制限なしで接続されている企業は、安全性が提供メーカーから保障されている端末または安全に管理できる状態に整備した端末を利用しているケースである。

5.8　社内ネットワークへの接続の際、採用している端末の認証方法（MA）

社内ネットワークへ Wi-Fi などで直接接続または VPN 経由で社外ネットワークから接続する場合に利用する端末の認証方法について問いかけている。

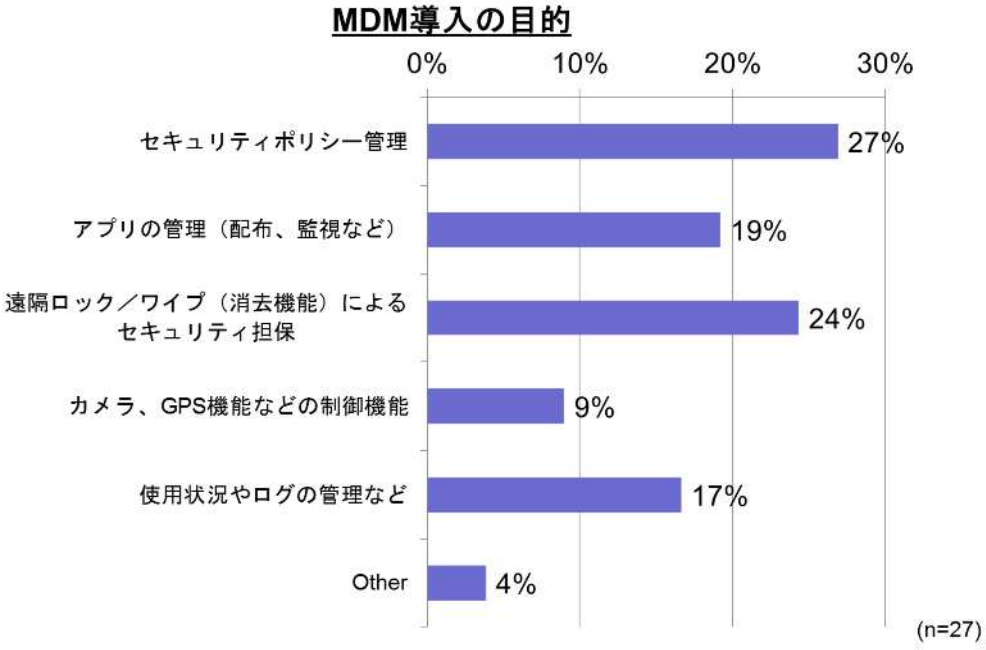


(考察)

端末認証が 44%となり多数を示しており、これは社内ネットワークへ接続する端末は社内で認められたものに限定していることを示している。ただし、どのレベルの厳格さを適用するかは、運用上のコストとの兼ね合いがある。現在の段階においては、ノート PC などで利用している既存の仕組みを流用しているものと推測している。

5.9 MDM の導入を計画した目的 (MA)

MDM (Mobile Device Management) 導入の目的についてポリシー管理、不正利用防止、情報収集、緊急対応に分類して問いかけている。



(考察)

「セキュリティポリシー管理」、「遠隔ロック/ワイプによるセキュリティ担保」というセキュリティ目的が上位を占めている。企業利用において、統一されたセキュリティ対応を集中的に行っていることを重視していると読み取ることができる。その反面、機能を制限に対しては比較的緩くしている。スマートフォンの特徴をより生かして活用していこうという姿勢が表れていると思われる。

また、「other」の回答も少数あるが、これはＭＤＭツールを取り扱う企業であった。まだ利用企業においてはＭＤＭのフル機能[1]を使った管理の段階に入っていないと思われる。

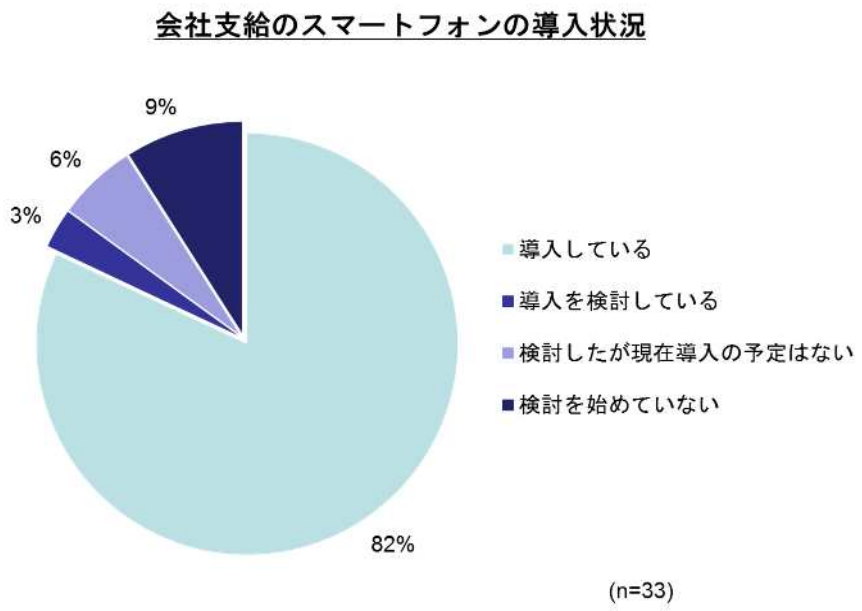
[1] MDM 機能については、JSSEC 『MDM 導入・運用検討ガイド』 “3.3 ＭＤＭの機能”参照

6 導入フェーズ

このフェーズでは、計画に従って企業内へ展開する段階である。
情報システム部門または利用部門の管理者は、展開の環境面での準備と利用者との調整を行うことになる。機器の購入、検証作業、キッティングの方法・設定範囲、利用アプリの準備、利用手順の教育、ヘルプデスク/サポート体制の準備などが行われることを想定している。
準備段階において利用者が個別で ID を取得し、その ID を機器に個別設定する、クローニングに制限があるなど大量に効率よく準備する方法が充実していないため展開においてボトルネックになる段階である。

6.1 会社支給のスマートフォンの導入状況（SA）

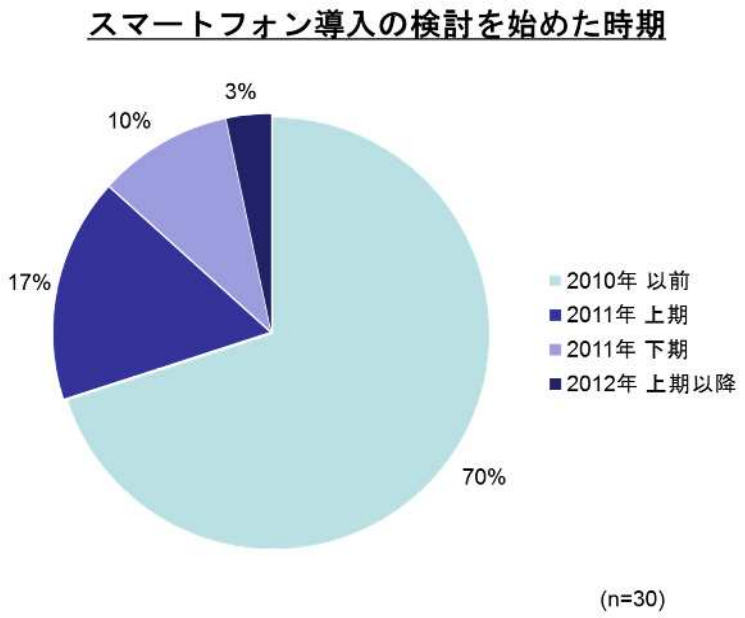
現在、スマートフォンを会社から支給されて利用しているかどうかについて問いかけている。



(考察)
約 8 割が既にスマートフォンを会社から支給されて利用している。これは、一般的な企業対象のデータよりも多い割合であり、本協会参加企業からの回答の特徴が表れている。

6.2　導入の検討を始めた時期（SA）

スマートフォンの社内への導入を検討し始めた時期について問いかけている。

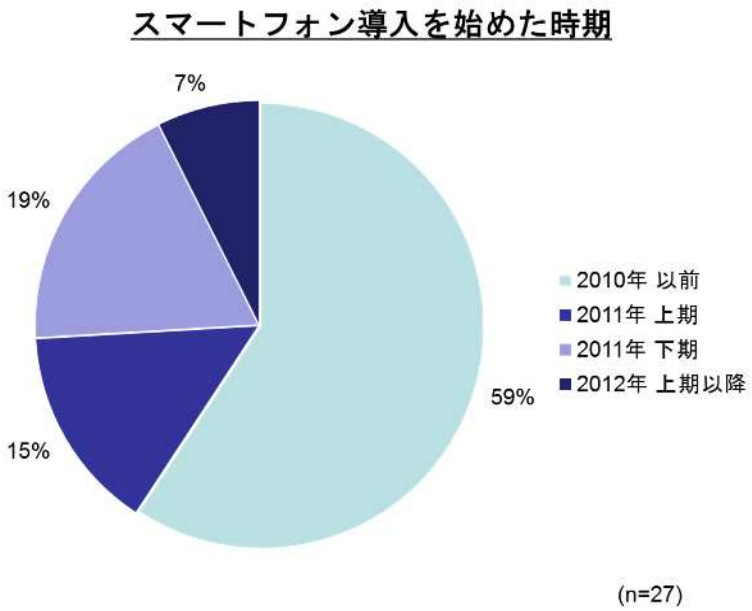


(考察)

7 割が 2010 年以前に企業への導入検討を始めている。これは、本協会参加企業がスマートフォンの導入に積極的な取り組みを行っていることが表れている。

6.3　導入を始めた時期（SA）

検討後、実際にスマートフォンの導入を開始した時期を問いかけている。



(考察)

約 6 割の企業が 2010 年以前に導入を始めている。2010 年以前に導入を検討している企業はほとんど 2010 年以前に導入を始めている。前設問と同様に企業の取り組みの積極性が表れている。2011 年以降のデータをみると検討から導入までの期間は、半年ほどであることが多い。これは、ドキュメントの整備や運用ツールが揃ってきたことが影響し、導入への障壁が低くなったと推測する。

6.4　導入の検討をしていない理由 (FA)

企業としてスマートフォンの導入を現時点で検討していない理由について問いかけている。

(考察)

導入の検討を行っていない理由では、スマートフォンの活用によるビジネスイノベーションよりも、貸与、支給の必要性から考えているという企業が存在することも伺える。また、“幹部社員等の一部使用”と“組織としての使用”をわけて考えている企業が存在することから、一部導入を含めた利用企業の割合は、企業は本調査よりも多いことが推察される。

6.5　今後導入の検討を始めるための条件 (FA)

現時点でスマートフォンを導入してないが、今後検討を始めるにあたりその前提となる条件について問いかけている。

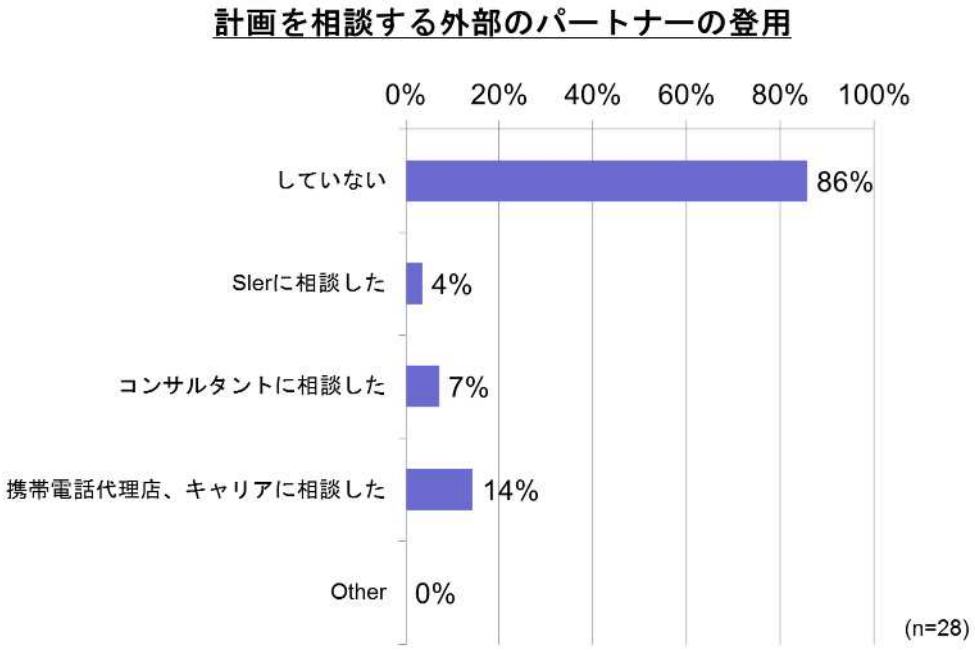
(考察)

少数の回答であったが、代表的な傾向であると思われる。一つは、スマートフォンの有効な活用は社内システムとの連携にあり、そのためには安全に社内のリソースへアクセスできる仕組みが重要であること。もう一つは、現在のワークスタイルが確立しておりスマートフォンの特長であるモビリティや操作性などを生かす場面がないこと。

本調査対象がスマートフォンを利用する企業が多いため少数の回答であったが、一般にこの傾向は少なくないと推測する。スマートフォンの動向に注目しつつも、自社の企業環境と照らし合わせてその導入のタイミングを慎重に見定めている。このような企業では、たとえば自社のポリシーに準じたセキュリティが確保できる仕組みが登場すれば一気に導入が決まる可能性がある。利用事例などを公開することにより導入が加速すると思われる。

6.6　スマートフォン導入にあたり、計画を相談する外部パートナーの登用（MA）

スマートフォンを導入する際に、その作業計画について社外のパートナーに相談したかどうかを問いかけている。



(考察)

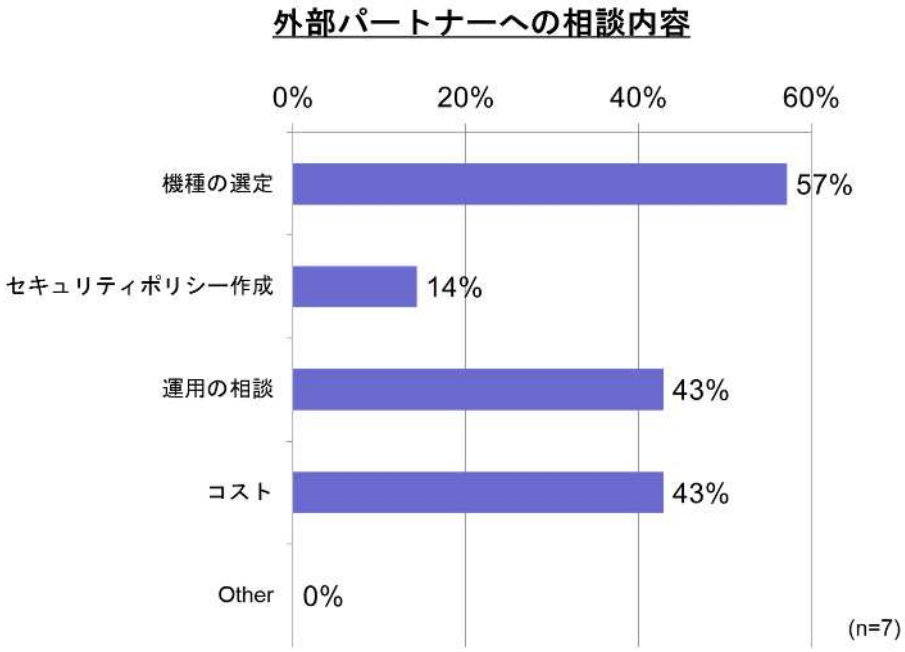
8 割以上が相談していないという結果である。これは回答のあった企業の 7 割が 2010 年以前に導入を検討しているため、その時期にはまだ相談先が少なかったためと思われる。相談した企業は、比較的最近の導入を行った企業であった。

ちなみに日本におけるスマートフォンの販売は、ソフトバンクから iPhone（3G）が 2008 年 7 月、Docomo からは HT-03A が 2009 年 7 月、au からは IS01 が 2010 年 6 月に始まっている[2]。

[2] 「iPhone」
http://ja.wikipedia.org/wiki/IPhone
「Andoid 端末一覧」
http://ja.wikipedia.org/wiki/Android%E7%AB%AF%E6%9C%AB%E4%B8%80%E8%A6%A7

6.7　外部パートナーへの相談内容 (MA)

上記設問で社外のパートナーに相談した場合、主にどのような内容について相談したかを問いかけている。



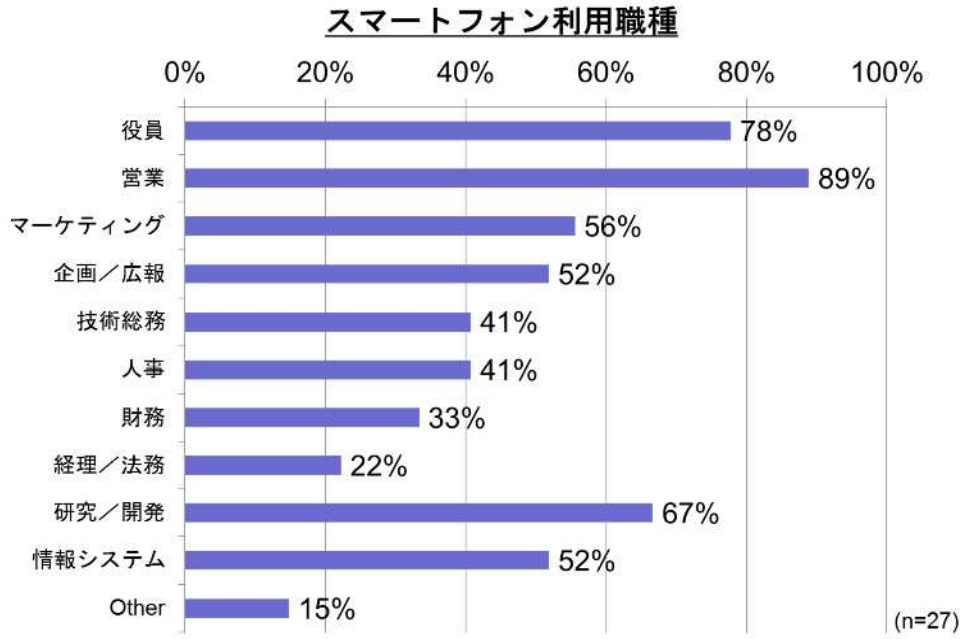
(考察)

外部パートナーへの相談した企業は少ないが、2011 年以降に導入を行った企業が多い。その中でも相談した内容としては「機種選定」、「運用の相談」、「コスト」が上がっている。機種選定に関しては、新機種への切り替わり、OS のバージョンにより利用できる機能に制限がある、外部装置の性能向上など利用用途と出荷時期により選択肢が多くなるため購入のタイミングが非常に難しいためと思われる。

反面、「セキュリティポリシー作成」は少数であり、これはまず開発者が既存のポリシーを適用することで開始したと思われる。

6.8　スマートフォンを利用している職種（MA）

社内でスマートフォンを利用している職種について問いかけている。

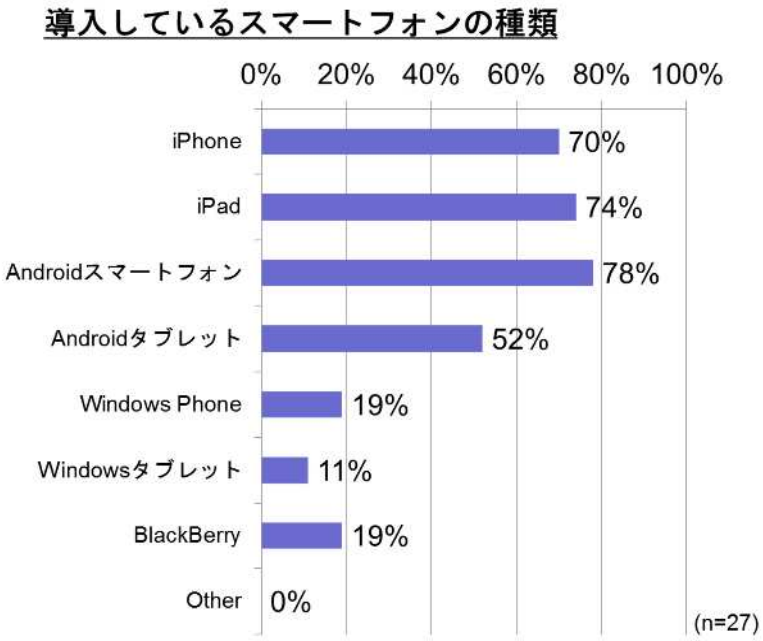


(考察)

スマートフォン利用の傾向として、外勤の割合が多い職種（役員、営業）と利用（社内、ビジネス）を対象とする職種（情報システム、研究開発、マーケティング）が多く利用されている。前者は、スマートフォン導入にあたり当初予定していたメールやスケジュールをまず利用する対象としての役割と、社外からの利用形態を測定するモデルとしての役割を期待していると思われる。また、人事、財務などの内勤の職種の割合が低いことから社内システムとの連携、社内会議での活用など社内での活用方法がまだ整備されていないと推測される。外勤者からの利用場面に応じたニーズの取り込みと、社内システムの連携が今後の普及のポイントになると推測する。

6.9　導入しているスマートフォンの種類（MA）

社内に導入しているスマートフォンについて OS 別の種類を問いかけている。



(考察)

ここでは、スマートフォンとタブレットを OS ごとに分類して調査を行った。その結果は他の調査報告と同様の傾向が表れている[3]。

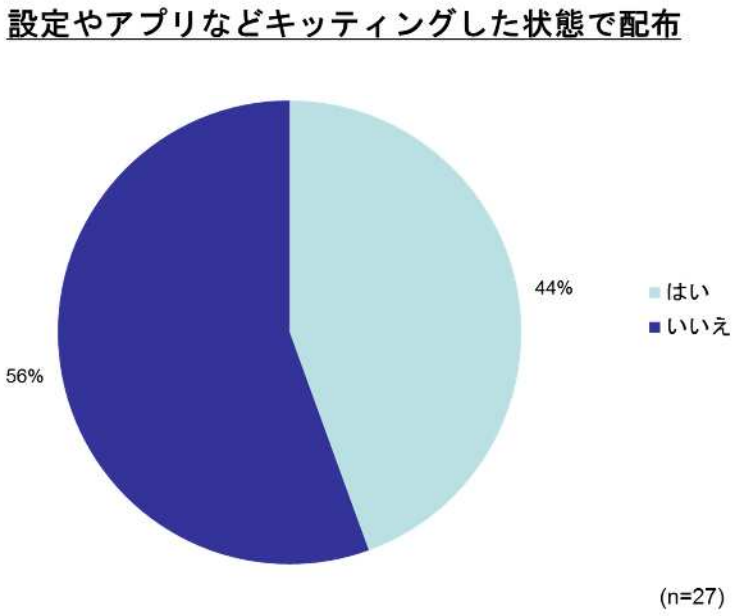
スマートフォンについては、僅差であるが Android について iPhone、タブレットについては、iPad について Android タブレットとなった。タブレットについては、導入時期が早い企業が多いことから Android 系タブレットの出荷が少なかったことも影響していると考えられる。

今後 Android タブレットの出荷数が増え、また企業利用においてはやはり既存システムとの連携から Windows8 搭載のタブレットの出荷動向により、スマートフォン、タブレットの利用する割合も含めて変化が出てくると思われる。

[3]キーマンズネット「業務用スマートフォンの導入状況(2012 年)」
http://www.keyman.or.jp/at/pcmob/mobile/30004611/

6.10　配付後すぐに使用できるように、設定やアプリケーションなどをキッティングした状態で配布しているか？（SA）

社内へ配布した際、利用者がすぐに使えるように個別のキッティング作業を行っているかどうかを問いかけている。



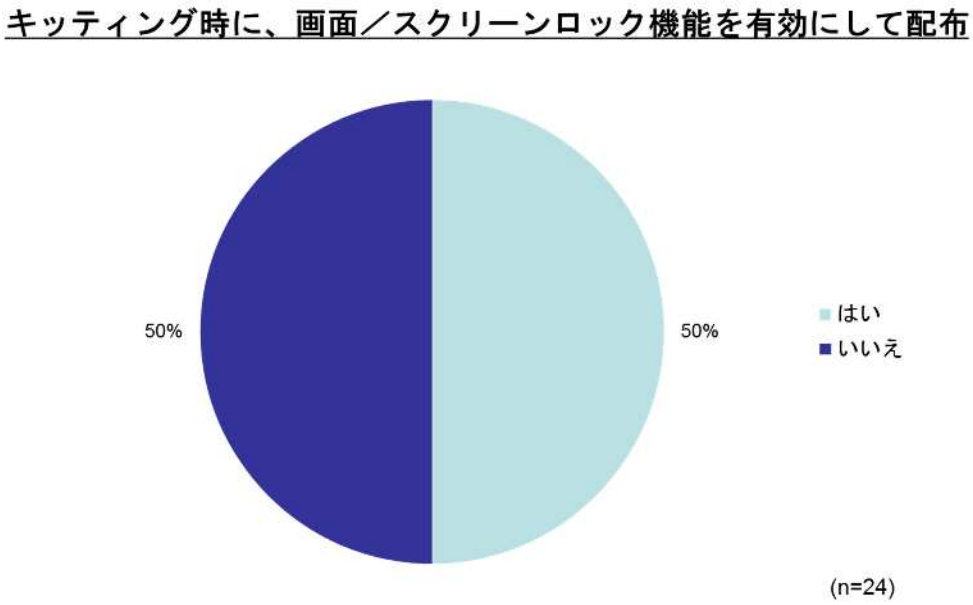
(考察)

前の設問にあるスマートフォンを導入した職種と関連する。つまり、役員や営業などのスマートフォンを利用する部門へ配布する場合には利用できる状態に設定し、これから活用を検討する情報システム部門や研究開発部門へは設定はしないで配布すると推察している。

スマートフォンのキッティングについては、まだ効率的な方法が確立できていない。個別設定に必要な情報を事前に利用者個人で準備しておく必要があり、現実的には共通でできる設定と個別で設定できるものとの作業を分けることになると推測する。

6.11　キッティング時に画面／スクリーンロック機能を事前に有効にして配布しているか？（SA）

キッティング作業において、セキュリティ対策として画面/スクリーンロック機能を有効にした上で配布しているかどうかを問いかけている。



(考察)

アプリなどの設定はしないで、セキュリティ上画面ロック機能だけを設定して配布するとの回答があり、前設問に対してこのような結果となっている。

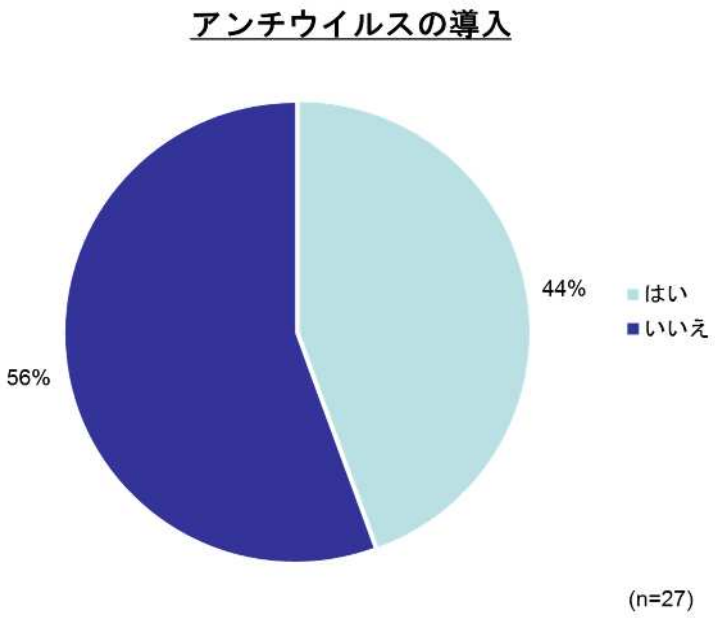
セキュリティの設定は利用者に任せことは完全性を確保できないため好ましくない。ただし、今回の回答は利用者とセキュリティリテラシーがあるシステム部門の割合に依存すると考えられる。スマートフォンの利用が普及すれば、この設問に対する「はい」の割合は上がってくると想定している。

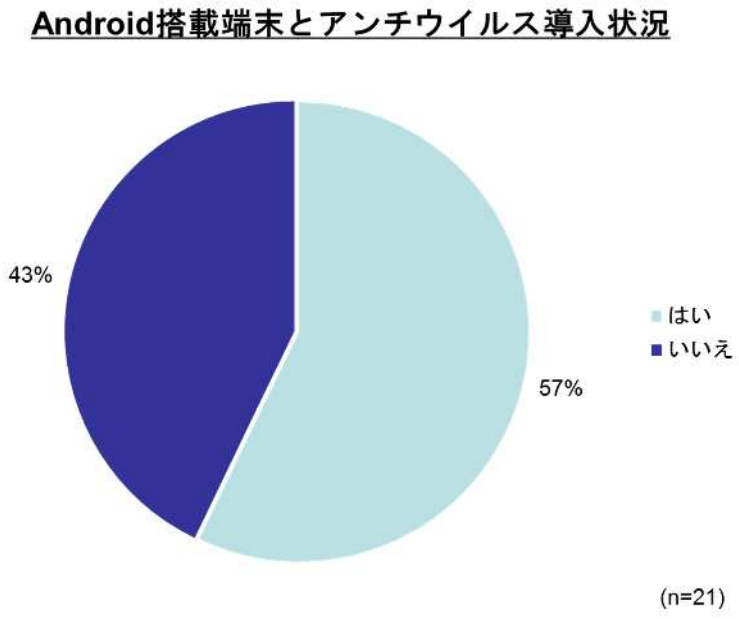
7 利用フェーズ

このフェーズでは、利用者が機器を配布され利用手順やルールに基づいて使う段階である。
情報システム部門または利用部門の管理者は、計画どおりに利用されているか、予期しない（プラス面、マイナス面）利用の監視などを行うことを想定している。
改善要求や利用方法の拡大に対する更なる要望が利用者から上がるため、それらをうまくくみ取ることでその解決策から付加価値へつなげることができる。
利用企業においては事業拡大へのチャンスを創る段階であり、事業化の企業にとっては差別化要素を創出する重要な期間となる。

7.1　導入したスマートフォンにアンチウイルス対策ソフトを導入しているか？（SA）

スマートフォンにウィルス対策としてアンチウィルスソフトを導入しているかを問いかけている。





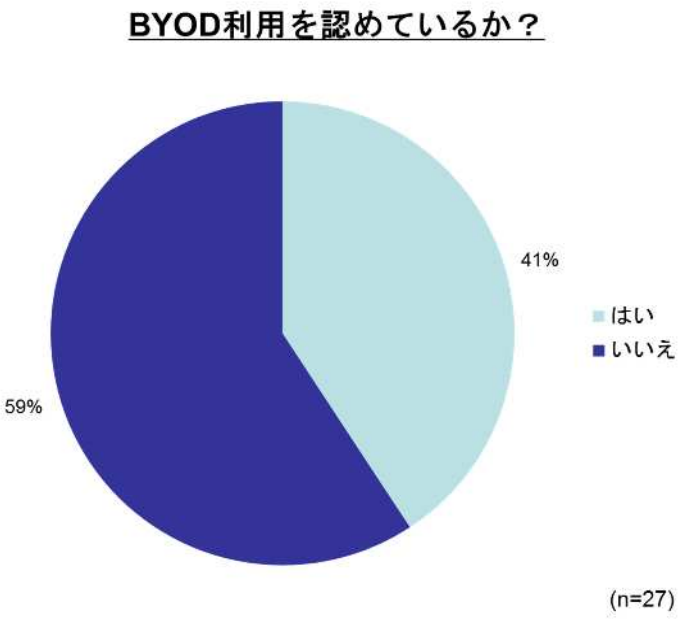
(考察)

OS の区別なく導入しているかどうかの結果を見ると「いいえ」のほうが多くなっている。ここにはアンチウィルスソフトが存在しない iOS のデータも含まれている。Android 搭載に限定して結果をみると導入している方が多い結果となる。しかし、Android

に限定してもまだ約4割は導入していない。これはアプリの導入を制限したり、利用シーンを限定したりするなど運用面でカバーしていると推測する。

7.2　スマートフォン導入において BYOD の利用を認めているか？（SA）

社内においてスマートフォンの利用を認めている場合、BYOD(Bring Your Own Device、社員の私用端末を業務用としても利用すること)を企業として認めているかを問いかけている。



(考察)

約 4 割が BYOD を認めている。これは一般的な調査結果に比べると割合として多い結果が表れている[4]。回答した企業が JSSEC 会員企業であり、スマートフォン活用に積極的であるためである。

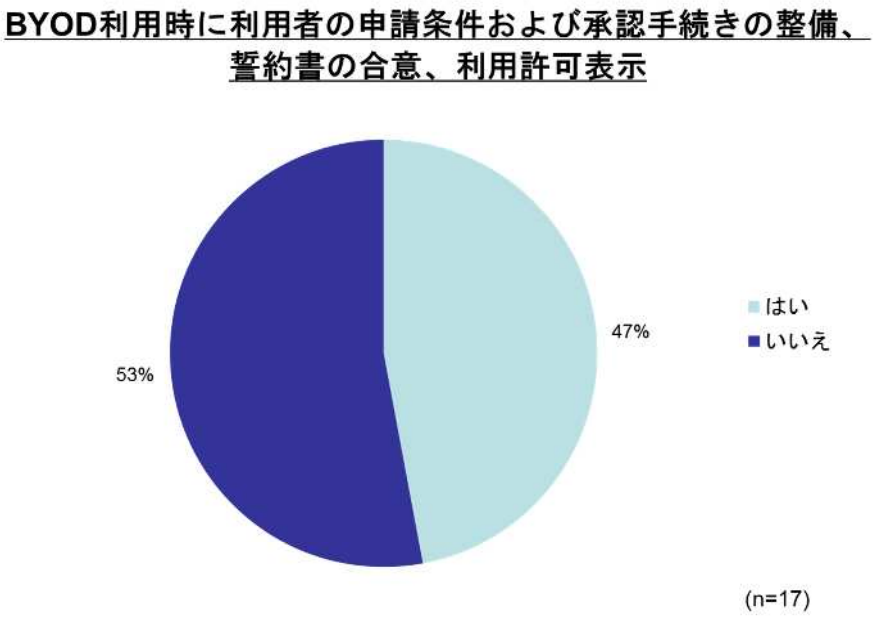
日本企業において BYOD は、海外企業とは異なり PC に対しても浸透していないため、企業文化として認められるためにはまだまだ準備が必要であると思われる。BYOD の考え方や定義[5]を改めて認識したうえで、対応を検討する必要がある。

[4] たとえば、日経コミュニケーション 2012 年 10 月号「スマートフォン活用の実像」では、BYOD を現在許しているはわずか 8%である。

[5] JSSEC『スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン』付録 B「BYOD の現状と特性」を参照のこと

7.3　BYOD 利用時に利用者の申請条件および承認手続きの整備、誓約書の合意、利用許可表示はできているか？（SA）

BYOD 利用が認められている企業において、その申請手続きの流れが決められているかを問いかけている。

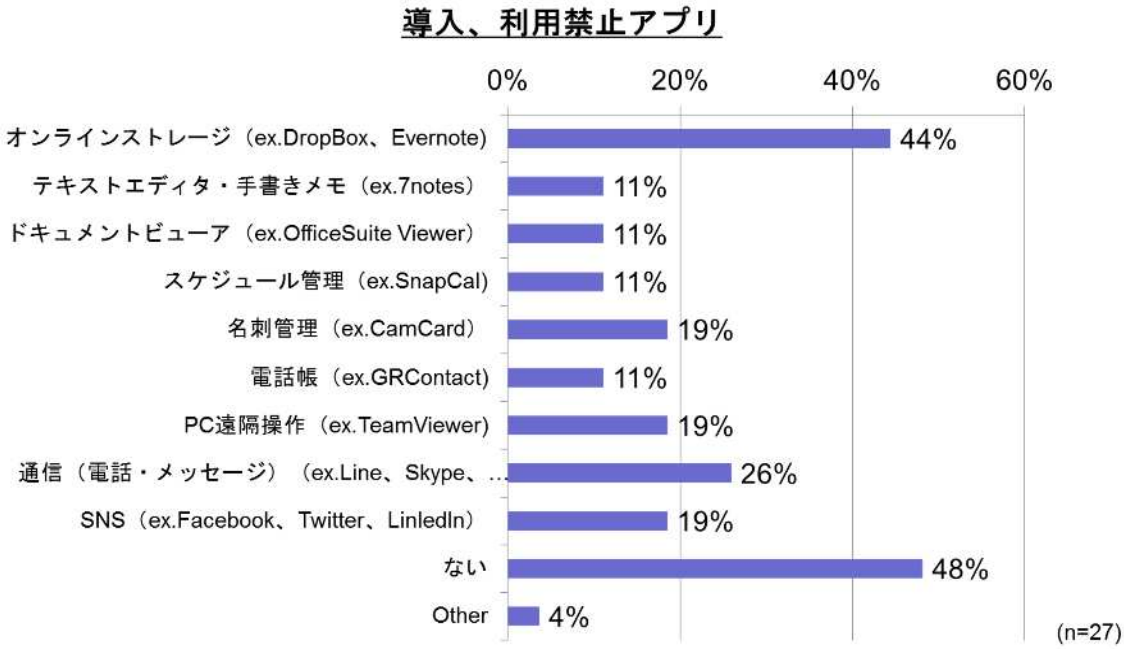


(考察)

BYOD 利用が認められていても、約半数がその利用環境が整備されずに開始をしている。これは前設問と同様に BYOD の考え方や定義を改めて認識したうえで、対応を検討する必要がある。

7.4　会社として導入、利用を禁止しているアプリ？（MA）

利用しているスマートフォンに対して、企業の方針として導入を禁止しているアプリがあるかを問いかけている。

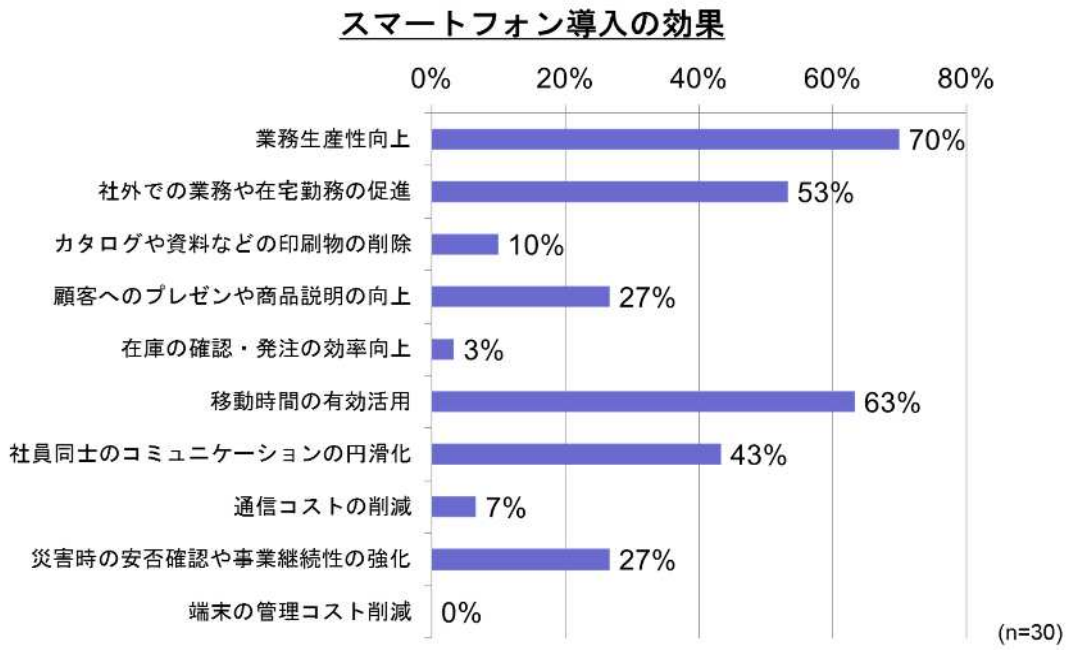


(考察)

オンラインストレージのアプリは、全体の 44%において導入を禁止しており、PC と同様のセキュリティポリシーが適用され割合として多くなっている。他のオフィス系、コミュニケーション系などのアプリはあまり厳しく禁止されているわけではない。ここで禁止アプリは「ない」との回答の割合が最も多く約半数を示している。これは、スマートフォンの特長のひとつであるアプリによる機能拡張性を重視しており、最初から制限するのではなくより多く利用することを重視していると推測している。スマートフォンに対する期待度の表れであり、その有効性を模索していると思われる。

7.5　スマートフォンを導入した結果、得られた効果は？（MA）

スマートフォンを導入し、利用する中で得られた効果について問いかけている。計画フェーズにおいて期待した効果と対比した問いになる。



(考察)

計画フェーズでの期待とほぼ同様に各項目の割合の傾向がでている。ただし、もっとも期待が高かった「業務生産性向上」については、若干ではあるが効果として下がっている。これはまだ利活用の途中経過の状態にあり、期待した効果以上の成果がでていないものと思われる。

伸び率では「移動時間の有効活用」が大きく、今までは活用できなかった僅かな時間や場所を仕事に活用できたことを表している。これにより、仕事の質を向上させたのか、勤務時間を短縮させたのかなどは今後の調査課題として残る。

7.6　スマートフォンの導入で得られた具体的な効果（FA）

スマートフォンを導入した結果、利用者から反響として得られた具体的な効果について問いかけている。

(考察)

業務生産性の向上としてあげられた例のは、スケジュールや決裁等が社外から可能となることをあげた場合が多く、技術的には従来のフィーチャーフォンでも可能であった領域とも言える。ただし、操作性向上やネットワークの品質向上等とあいまって、導入効果を実感しているのではないかと推察する。

7.7 スマートフォン導入後に認識した課題 (FA)

スマートフォンの導入後に、認識した想定範囲外の課題について問いかけている。

(考察)

スマートフォンを利用する中で顕在化してきた課題をまとめると以下となる。

- 携帯電話の代わりに配布された場合、通話品質の低下やバッテリー切れによる可用性の悪化などがあげられる。
- 機種のモデルチェンジの早さや OS のバージョンアップ頻度の多さなどにより、統一した利用環境の整備ができない。これに加えて BYOD 利用への対応は非常に難しい。
- 配布に関して効率化が難しく、コスト低減できない。
- 企業利用にマッチした (特にセキュリティ機能) アプリやサービスが出てこない。
- 企業利用を支援するツールがない。

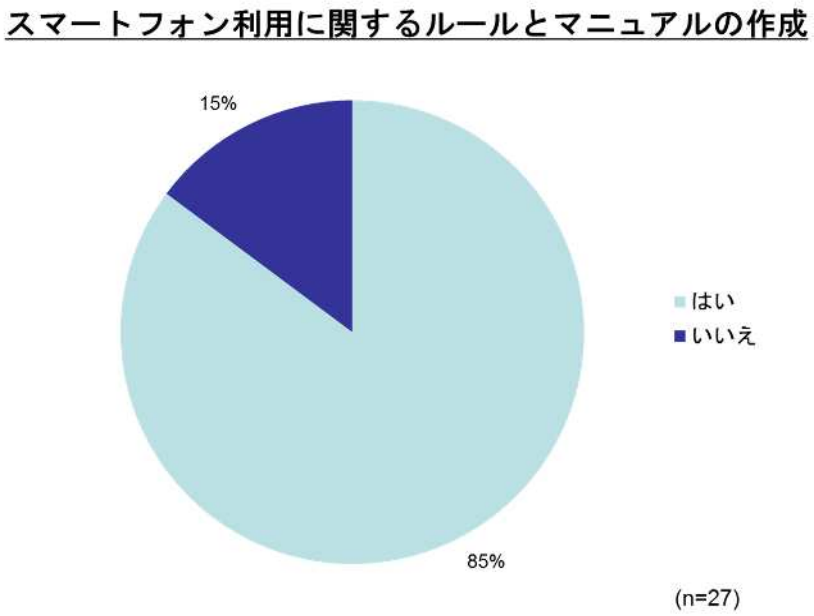
8 運用フェーズ

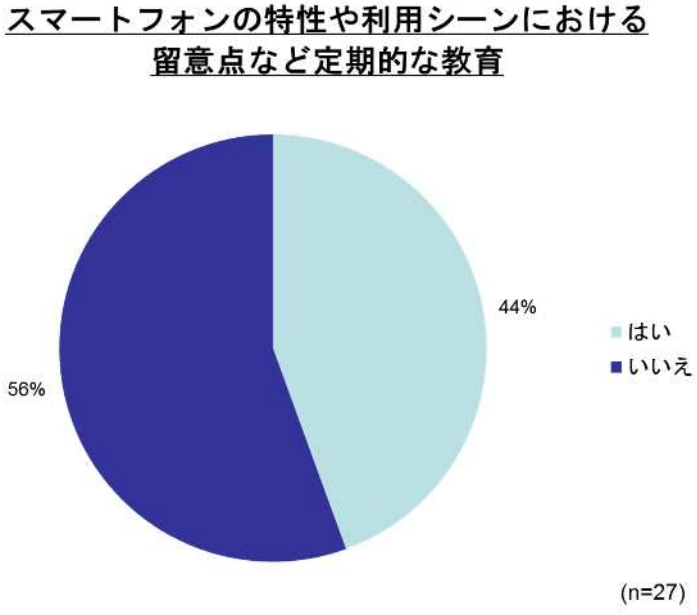
このフェーズでは、スマートフォンを企業活動のツールとして企業内で広く受け入れられ、その稼働率が日常の企業活動に影響を及ぼす状況になった段階である。

情報システム部門または利用部門の管理者は、利用されている機器が正常に稼働し続けるため、または故障などが起こっても即時に代替できる対応を行うことになる。そのため、企業内のルール作り、管理手順、配布されたまたは予備として保管されている機器の状況を把握、ソフトウェア更新、サポートレベル設定、新機種対応など日々情報を管理しておく必要がある。

8.1　スマートフォン利用に関するルールとマニュアルの作成（SA）

スマートフォンの利用方法のルール作成し、マニュアルなどのドキュメント化したかを問いかけている。





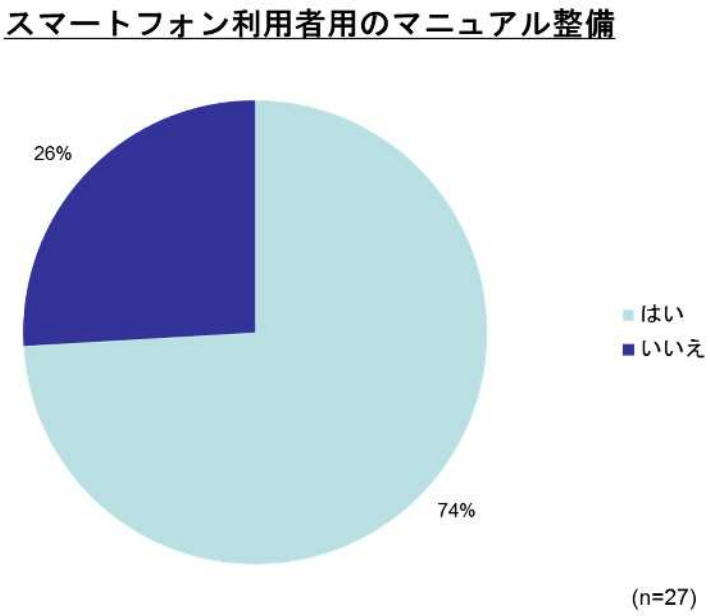
(考察)

スマートフォン利用においては、携帯電話やノート PC とは利用場面やセキュリティ対策なども異なることから事前にルールなどを作成し運用者の間で共有し徹底していると推測する。また、新機種、OS のバージョンアップ、アプリの非互換などの対応についても定期的に教育する割合が高くなっている。対応機種やソフトウェアのバージョンアップ頻度など複雑化してくる可能

性があり運用面で大きな負担になってくる。この負担を軽減する方策がスマートフォン利用を定着させるためには必要になる。

8.2 スマートフォンの利用者用マニュアルの整備（SA）

スマートフォンの利用者に対して、利用のためのマニュアルを作成したかを問いかけている。

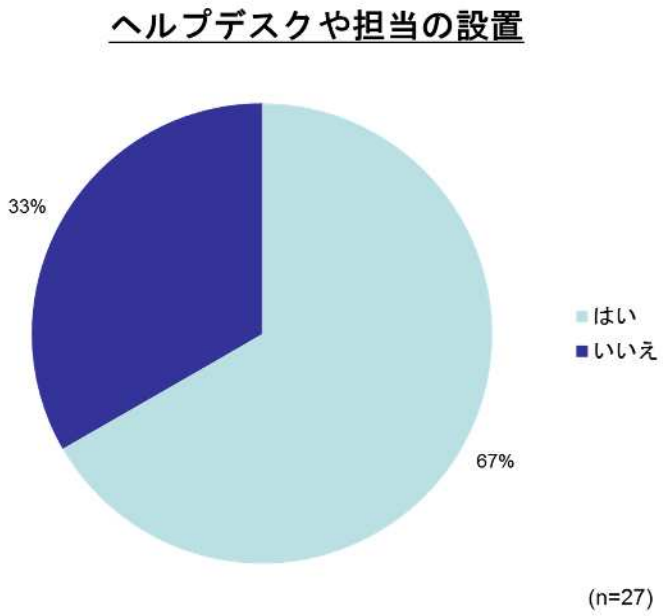


(考察)

約 7 割が利用者用のマニュアルの整備を行っている。スマートフォンの操作は直感的でありマニュアルの整備はあまり必要ないように思われるが、初めて触れる利用者や既存システムとの操作の互換性などについては必要とされるため、導入初期段階においては必要になると推測する。本格的な利用に入るとその利活用は多岐に渡るため、マニュアル整備は対応しきれない可能性がある。操作の簡略化やユーザインタフェースの工夫などによりこの作業を軽減する必要がある。

8.3　スマートフォンの会社での利用にあたり、ヘルプデスクや担当の設置（SA）

スマートフォン利用者からの問い合わせに対応するためヘルプデスクまたは対応担当者を設置しているかを問いかけている。

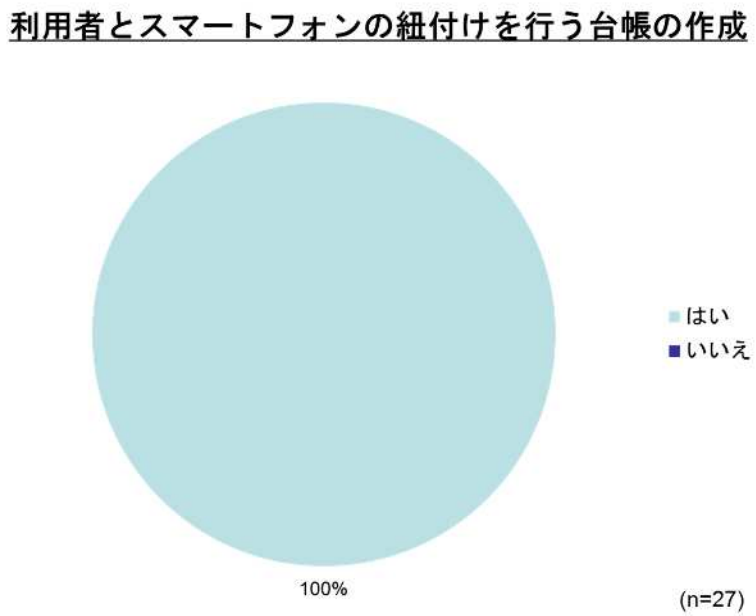


(考察)

前設問と同様に導入初期の段階では、利用者を支援する体制がスマートフォン利用を定着させるため重要となり高い割合を示している。ここへの問い合わせは、セルフサポート体制と連携することで作業の軽減が可能になる。

8.4　利用者とスマートフォンの紐付けを行う台帳の作成（SA）

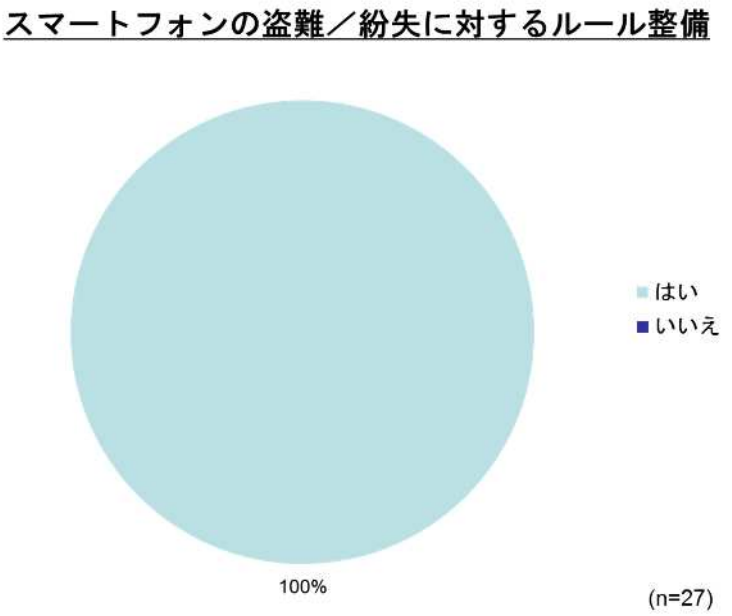
スマートフォン利用の運用管理として利用者と利用する端末の台帳作成を行っているかを問いかけている。

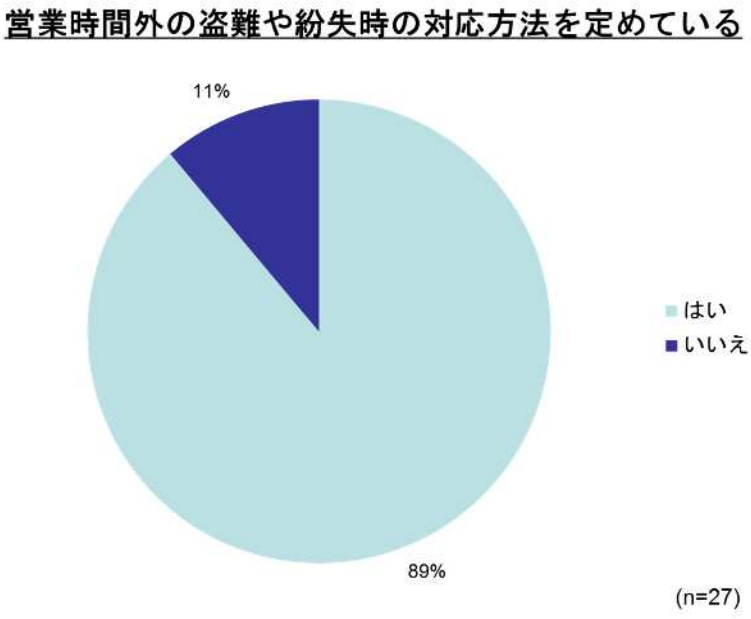


(考察)
スマートフォンの利用形態としては、主に1つの端末はシングルユーザで利用することにより、端末とその利用者を紐づけることでスマートフォン管理の基本としている。企業利用の運用管理では必須の項目である。

8.5　スマートフォンの盗難／紛失に対するルールの整備（SA）

スマートフォンを盗難されたまたは紛失に気付いたとき運用管理者がどのように対応するかのルールを作ったかを問いかけている。

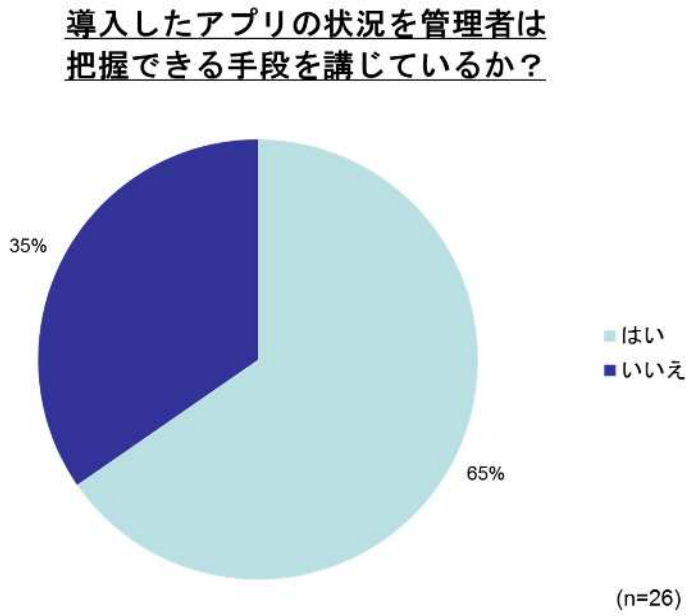




(考察)
小型であること、移動性があることはスマートフォンの長所でもあり欠点でもある。そのため盗難や紛失といったリスクに対してはすべての企業において事前にルールを設定している結果が得られた。また、緊急を要する対応も必要であり、ほとんどの企業において時間外の対応を行っている。企業におけるスマートフォンの運用において必須項目の一つである。

8.6　スマートフォンに導入したアプリケーションの状況について、管理者は把握できる手段を講じているか？（SA）

利用者がスマートフォンに導入したアプリを管理者が随時自動的に把握できる手段を適用しているかを問いかけている。

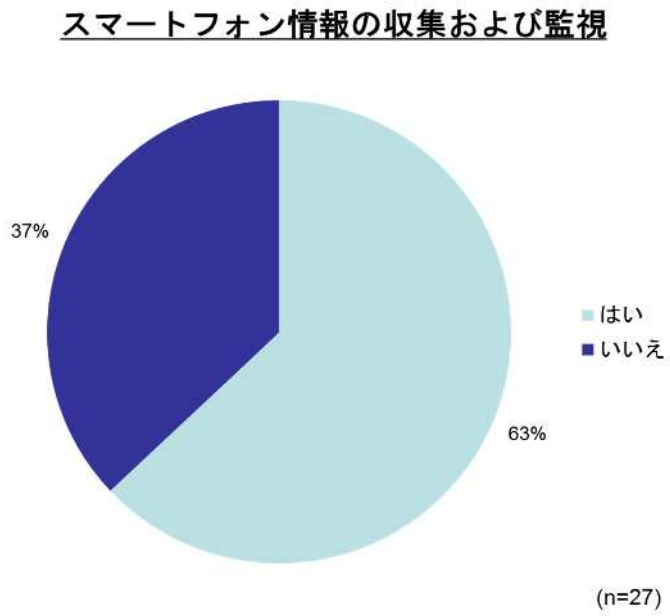


(考察)

6 割強が MDM などのツールを利用して、導入アプリの状況を把握できるようにしている。これは、利用フェーズの設問にあったようにアプリ導入の制限を行う意図よりも状況の把握によりスムーズな運用を行うためと推測する。ここで 3 割強がアプリの状況を把握していないのは、要求にあった MDM ツールがない、または運用状態にないなどの理由によるものと思われる。

8.7　スマートフォン情報の収集（ハードウェア情報、OS 情報、導入アプリ情報、各種端末設定機能制限、OS の改造有無）および監視はできるか？（SA）

使用しているスマートフォンに関する情報を随時収集でき、リアルタイムに監視できる仕組みがあるかを問いかけている。

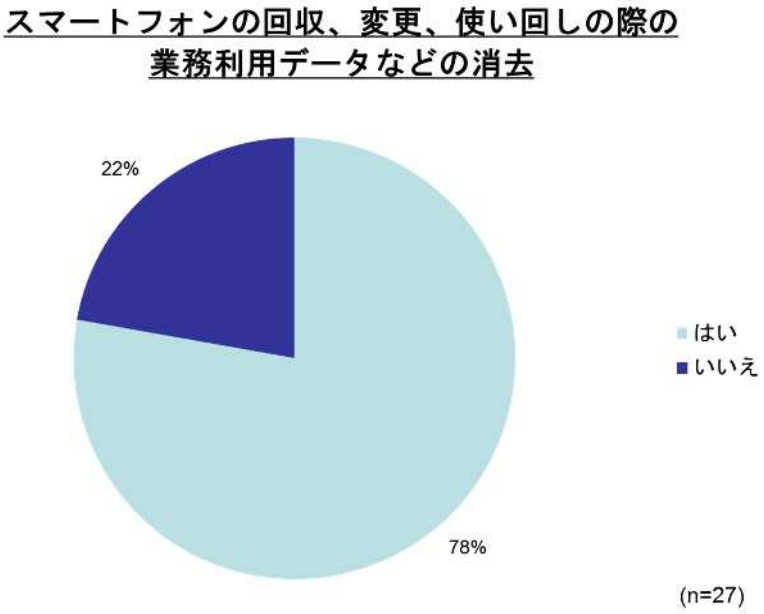


(考察)

前設問と同様の結果であり、約 6 割強が MDM などのツールにより実施している。

8.8　スマートフォンの回収、変更、使い回しの際に業務利用データ、各種端末設定情報、アプリケーションの削除、外部サービスの認証情報を含むキャッシュの消去を行っているか？（SA）

使用していたスマートフォンを再利用する場合、以前の使用情報をクリアしているかどうかを問いかけている。



(考察)

スマートフォンはシングルユーザで利用するため、利用者が変更される場合には情報をクリアしてから再利用することを示している。「いいえ」については、再利用の運用を行っていない、レンタル会社に返却するなどの理由によると推測する。

9 総括

9.1 スマートフォンの普及状況

キャリアから販売される携帯電話はスマートフォンに移り変わる段階にあり、スマートフォンの企業への普及が進んでいる。電話機能だけでなく、導入にあたりスマートフォンの特徴である拡張性、操作性を有効に活用することが検討され、利用場面を想定しながら導入されている。そしてその利用の中でその価値を見出そうとしている。現時点では導入フェーズから利活用する利用フェーズへの移行段階にあると言える。スマートフォンが更に普及しその企業利用が定着するためには、有効な利用方法に加えて、その運用の簡易化が重要である。現在はまだニーズにあった運用管理ツールがなく、安定した運用フェーズに至っていない状況である。

9.2 スマートフォン導入の用途、目的

多くの企業は、業務の生産性向上を目的としての導入を計画している。そこで、これまで業務で使わなかった時間、場所を有効に使うため、まず外出頻度の多い従業員を対象に導入し、比較的容易に利用できニーズの多いメールやスケジュールへのアクセスから利用始めている。社外から社内システムへのアクセスする方法やスマートフォン向けのユーザインタフェースの準備が整いつつあり、次のステップとして業務システムとの連携に拡大してくると思われる。更に、クラウドシステムやアプリなどと連携し、より高度な活用に範囲を広げ双方向に利用する方向に向かっている。よって、今後は利用部門からの要求をより多く上げていく必要がある。

9.3 企業におけるスマートフォンセキュリティの動向

スマートフォン導入にあたり計画段階においてセキュリティの検討はノートＰＣや携帯電話での対応をベースに慎重に行われている。ただし、パスワードポリシーやセキュリティ設定が比較的緩く、導入アプリのポリシーがないなど制限する方向ではなく、利用者への利便性を重視した対応が行われている。これはスマートフォンの拡張性とその可能性を引き出すため、利用場面や運用でセキュリティをカバーする工夫をしている。

9.4 ＢＹＯＤ利用における課題

スマートフォンを利用する環境は、年々複雑化している。つまり、新機種投入時期、ＯＳやアプリのバージョンアップサイクルなどによりその組み合わせは管理コストを上昇させる。それに加えて、ＢＹＯＤ利用を認めた場合個人利用と企業利用の部分を使い分けることでより複雑性が増し管理が難しくなる。日本企業の場合、ＢＹＯＤの文化がないところから始める必要がある。ＢＹＯＤが企業利用として普及するためには、まずＢＹＯＤの定義や考え方を浸透するところから始めていくことになると思われる。

またスマートフォンの利用状況について、計画、導入、利用、運用の 4 つのライフサイクルでまとめると、下図表となる。本調査は主に JSSEC 会員を対象としており、セキュリティに対するリテラシーが一般よりも高いことが想定されるため、業務利用のスマートフォンに対するアンチウィルスソフトの導入や、利用マニュアル作成は既に行っている企業が多数存在する。一方で、JSSEC 会員であっても、Android 端末を利用している企業の約 4 割がアンチウィルスソフトを導入していなかったり、約半数の企業が OS の標準機能のパスワードを利用していたりと、セキュリティ上懸念すべき点がいくつか発見された。
今後本ワーキンググループの取り組みとして、JSSEC 会員外を含めた一般の企業において、スマートフォンが適切に利用されているのか、引き続き把握に努めることが重要であると考える。

	本調査結果	今後に対する考察
計画	• 業務生産性の向上を目的としてスマートフォンの導入を計画する企業が増加。ただし、利用アプリケーションが決まっていなかったり、初期のセキュリティレベルのままで利用する企業も一部存在する。	• パスワードや、セキュリティポリシーの設置・準備など一部において不安が感じられる部分がある。
導入	• 回答者のスマホ・タブレット導入率は80%と高い（注：回答者はJSSEC会員）。また各社2010年度と比較的早い段階で導入について検討を開始。	• スマートフォンのモビリティを活かしたサービス、アプリケーションの普及につれて、導入を検討する企業は今後再増加する。
利用	• アンチウイルスソフト、スクリーンロック等、一部の事業者は対策している一方で、対策していない企業も相当数存在する。 • スマホ利用により、7割の企業が業務生産性向上を実感。	• 取組方針は企業によって大きく分かれ、明確なルールを持たずに自由な利用を認める企業と、しっかりとしたルールによって管理しようとする企業に分かれると想定される。 • BYODの導入にあたって。さらに企業ごとの方針は分かれると予想される。
運用	• 利用マニュアル、ヘルプデスクや紛失時の対応等、基本的な運用に関する取組は今回の回答多くで行われている。	• 利用に対する対応は行われていると認識できるが、現状で運営時のセキュリティについて、どの程度意識されているかを分けて把握することが重要と予想される。

参考文献

本調査において設問項目や結果考察のなかで参照したドキュメントを以下にまとめる。

日本スマートフォンセキュリティ協会 部会・WG からの報告/成果物

http://www.jssec.org/report/

『スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン』【第一版（基礎資料収録版）】2012/11/19

http://www.jssec.org/dl/guidelines2011_v1.1.pdf

『スマートフォンネットワークセキュリティ実装ガイド』【第一版】2012/12/27

http://www.jssec.org/dl/NetworkSecurityGuide1.pdf

『MDM 導入・運用検討ガイド』【第一版】2013/1/28

http://www.jssec.org/dl/MDMGuideV1.pdf