BYODガイドライン2013

企業の生産性と従業員の満足度を両立させる導入方法を解説

株式会社アイキューブドシステムズ

2013/3

BYODガイドライン2013

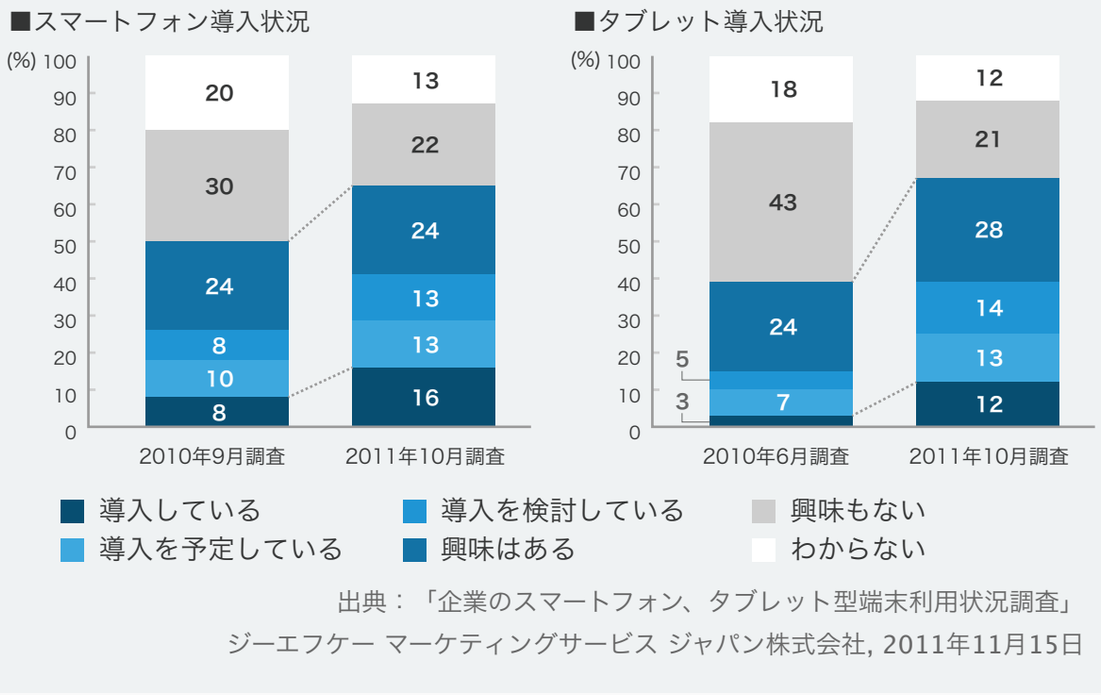
1. BYOD -Bring Your Own Device- とは？

急速に普及するスマートデバイスの法人利用

2013年度に各通信キャリアから発表された新機種モデルでは、旧来のフィーチャーフォンモデルがほぼ一掃されたほど、スマートデバイスは一般化しています。子供からお年寄りまで年齢を問わず、誰もが直感的に理解できる操作性や、いつでもどこでも、時間や場所を問わずにインターネットを利用出来る環境が一般的になりました。

このような個人利用での普及とともに、法人利用においても着実な拡がりを見せています(図1)。

図1. 企業におけるスマートデバイスの普及状況



出典：「企業のスマートフォン、タブレット型端末利用状況調査」
ジーエフケー マーケティングサービス ジャパン株式会社, 2011年11月15日

スマートデバイス導入の新たな潮流「BYOD」

スマートデバイスをビジネスに活用しようとする中で、従来型の「会社支給」に変わる導入方法として注目を集めているのが、「BYOD - Bring Your Own Device」です。

BYOD は**「個人所有のコンピューティング機器を業務用途としても利用すること」**を指しています(図2)。

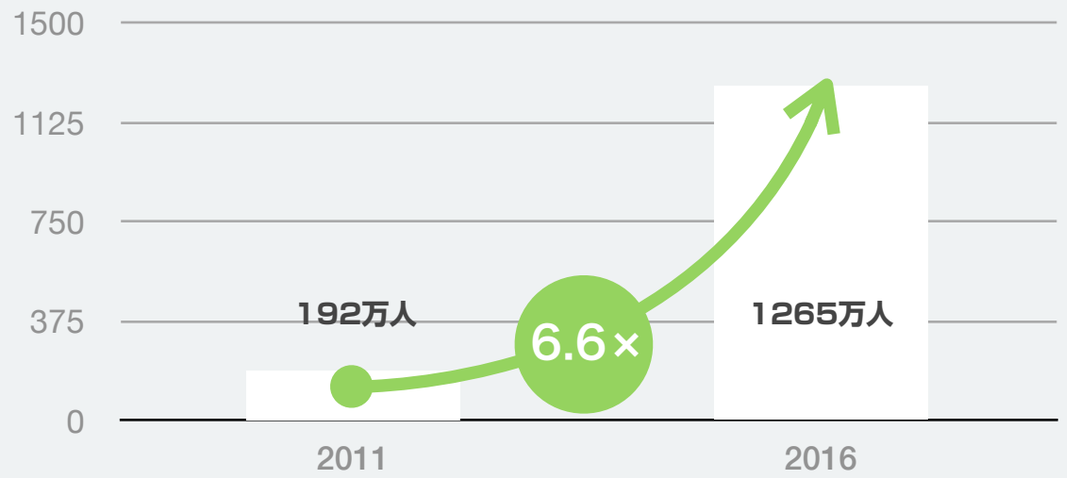
図2. 一般的なBYOD端末の利用用途

2. 急速に拡がるBYOD

2016年には6.6倍の1200万ユーザーへ

BYOD は世界中で急速な拡がりを見せており、日本国内においてもそのユーザー数は 2011年時点で192万人を数え、5年後の2016年には **6.6倍の1265万人に達する** と予想されています(図3)。

図3. BYOD ユーザー数の増加予測



出典： IDC Japanプレスリリース
「2013年 国内BYOD利用実態調査結果を発表」（2013年1月17日）

使い勝手の良さが普及を後押し、経営層の注目も高い

BYOD は、適切に実現されれば会社支給と比較してメリットの多い運用方法です(表1)。特に、経営者の注目を集めているポイントは以下の２点です。

> **①端末・通信コストを低減する**
> **②従業員の業務効率が向上する**

現在の BYOD ユーザー の大半が従業員による自主的な導入であることを踏まえると、②を実感している従業員は既に多いと考えられます。

表１. BYODと会社配布のメリット比較

		BYOD	会社配布
企業視点	端末・通信コスト	相互に負担 デバイス購入費や通信費を従業員と分担するため、コストが少なくなるケースがある。	企業が全て負担 デバイス購入費や通信費を法人が全て負担するため、コストが大きくなる。
企業視点	学習コスト	少ない 従業員が使い慣れたデバイスを活用するため、使い方などの学習コストは少ない。	多い 最も低いITリテラシーを想定した学習プランを用意する必要があり、学習コストが多くなる。
企業視点	先端テクノロジーの導入	比較的 短期間 従業員自身が必要に応じて買い替えるため、比較的新しいデバイス・テクノロジーを利用できる。	比較的 長期間 全社的に取り組む必要があり、デバイスのリプレースやテクノロジーの採用が先延ばしになりがち。
ユーザー視点	業務効率	使い慣れた端末 従業員自身が好きなデバイスを選択し、利用できるため、満足度は非常に高い。	会社指定の端末 従業員自身のデバイスと、使い慣れない会社支給のデバイスを持ち、使い分ける必要がある。

3. BYODを取り巻く課題

6〜8割が未承認？他人事ではない情報漏えいリスク。

BYOD ユーザー数の増加予測に示されるユーザー数のうち、最低でも **65.2% が「シャドー IT 」**と呼ばれる「企業が業務において、私物端末の試用を許可しない状況で従業員が使用するケース」「BYOD 利用規定を定めないで使用するケース」であることが明らかになっています(出典： IDC Japan プレスリリース「2013年 国内BYOD利用実態調査結果を発表」(2013年1月17日))。

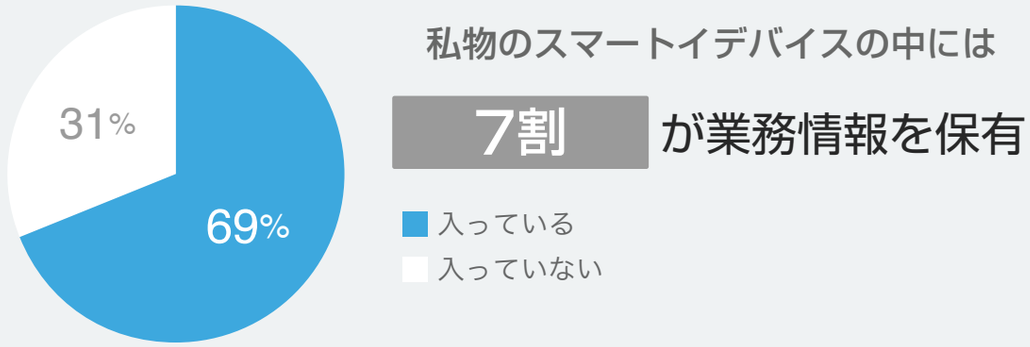
また、**「私物のスマートデバイスの７割には業務用データが保存」されており**(図5)、その中には**「機密ファイル(文書/画像)**(図6)**』** が含まれる事実を認識し、真摯に受け止めなければなりません。

興味の有無に関わらず、全ての企業にとっての重要課題

これまでのデータから、「 BYOD の必要性を企業が感じている / いない」 にかかわらず、BYOD は全企業に必須の検討課題であると言っても過言ではない事が分かります。

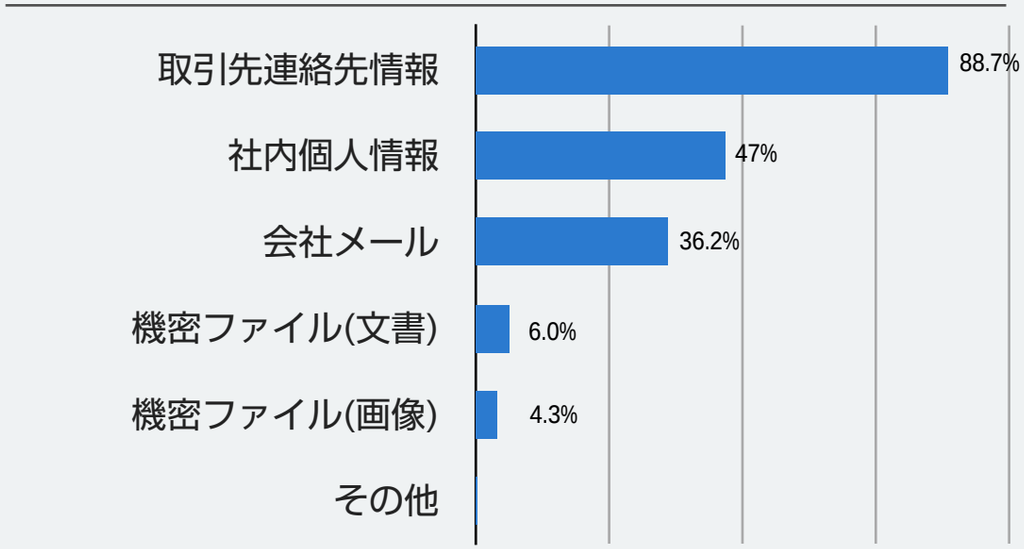
勝手な BYOD が拡がる前に、私物スマートデバイスの業務利用についての IT ポリシーを早急に策定する必要があります。

図5. 私物のスマートデバイスに保存された業務データに関する調査



出典：株式会社クロス・マーケティング
「スマートフォンのBYOD利用に伴うコミュニケーションアプリに関する調査」

図6. プライベート用のスマートデバイスに保有する業務上の情報内容



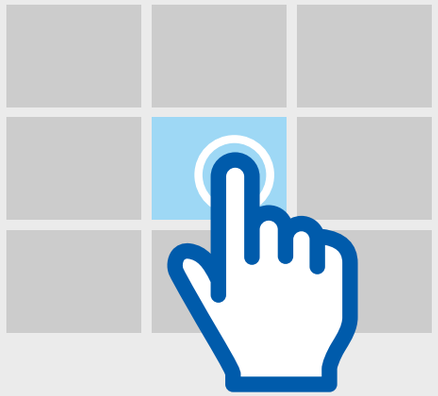
出典： 株式会社クロス・マーケティング
「スマートフォンのBYOD利用に伴うコミュニケーションアプリに関する調査」

4. BYOD 実現のための４つのキーサクセスファクター

アイキューブドシステムズでは、4,500社を超えるユーザー様のスマートデバイス導入・活用の支援から得たノウハウをもとに、企業の生産性と従業員の満足度を両立する BYOD を実現するための検討項目を抽出し、以下の４項目にまとめました。

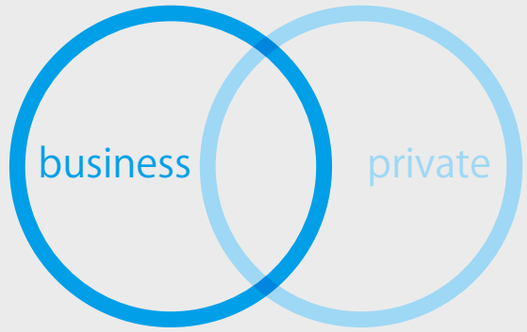
Ⅰ デバイスの利用用途を決定する

スマートデバイスをどのような業務に利用するのか、用途を決定します。



Ⅱ 守るべき情報の範囲を決定する

決定した利用用途の中で、保護する情報の範囲を決定します。

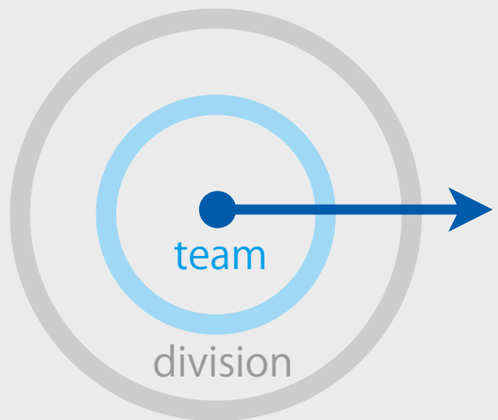


Ⅲ 運用方針を決定する

「保護対象の情報」とそれを利用する私物スマートデバイスを「どのような方針で運用するか」を決定します。

Ⅳ 展開方法を決定する

社内での展開方法を検討します。



4-1. デバイスの利用用途を決定する

メールやカレンダーなど、まずはシンプルな用途から

　はじめに検討すべき項目は、スマートデバイスの利用用途です。利用用途を決定する上で重要な点は、「利用シーンを具体的にイメージすること」です。

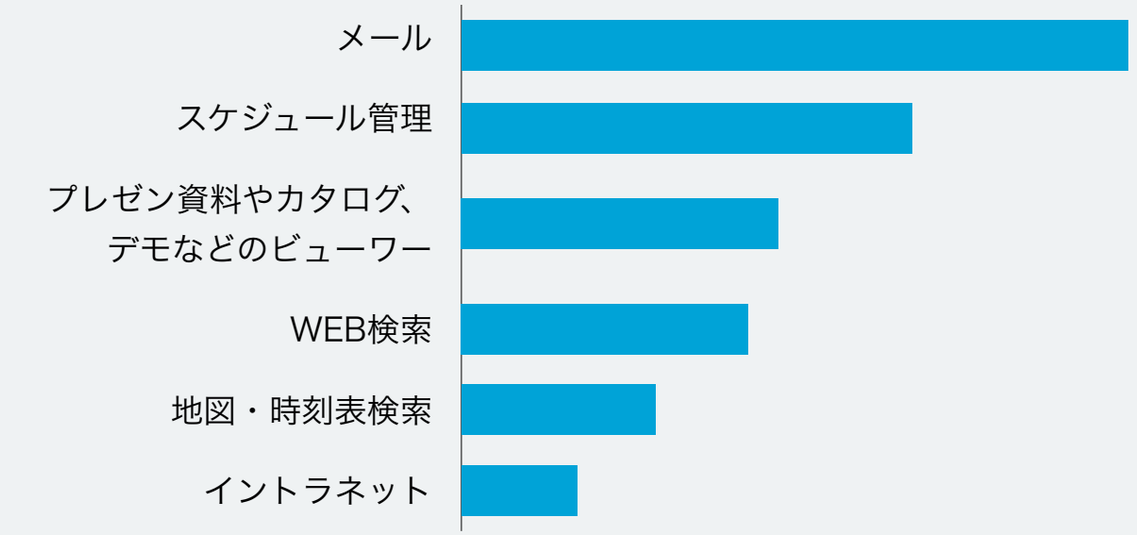
　しかし、はじめから革新的な使い方をイメージする必要はありません。スマートデバイスでビジネスを革新したガリバーインターナショナル様も、「メール・カレンダー」の閲覧からスタートし、効果を測定しながら徐々に利用用途を見つけ、拡大した結果として「買取業務の効率化」や「ビジネスモデルの革新」を実現しました。

最低限実施させたいことを明確化する

　スマートデバイスの業務利用では、**「メールのチェック」「スケジュールの確認」「プレゼンテーション」など、標準的な用途**で利用されています(図7)。重要なのは、私物のスマートデバイスで**「最低限実施させたいこと」を決定すること**です。

　利用イメージを持ちづらければ一度、他社の導入事例や、既にスマートデバイスを業務に利用しているユーザーを社内で探し、どのように利用しているのか、何に困っているのか、などを調査することをオススメします。

図7.スマートデバイス業務利用の用途



出典：アイティメディア株式会社
スマートデバイスに関するアンケート調査（2012年9月）より、上位6位迄抜粋

参考：スマートデバイス利用用途チェックシート

以下に、一般的なスマートデバイスの業務用途をまとめました。「業務での利用用途」を検討する際の参考としてご活用ください。

- [ ] **電話**
  通話機能を使い、業務上の連絡やコミュニケーションを行う
- [ ] **メール**
  業務メールの閲覧・送受信や添付ファイルの閲覧を行う
- [ ] **スケジュール**
  商談予定や社内イベントなど業務予定の管理を行う
- [ ] **連絡帳**
  取引先や社内メンバーの連絡帳からいつでも連絡が取れるようにする
- [ ] **WEBブラウジング**
  業務に必要な情報の検索や収集を行う
- [ ] **ファイルビューワー**
  カタログデータやデモムービーの閲覧・プレゼンテーションを行う
- [ ] **イントラネット**
  社内システムや社内ポータルにアクセスし業務情報を閲覧する
- [ ] **クラウドサービス**
  グループウェアやCRMなど企業が契約しているクラウドサービスを利用する
- [ ] **カメラ**
  点検業務やバーコードリーダーなど、カメラ機能を業務に利用する
- [ ] **ボイスメモ**
  商談やミーティング内容の記録などにボイスメモを利用する
- [ ] **ビデオチャット**
  取引先や社内メンバーとビデオチャットでコミュニケーションを実施する
- [ ] **位置情報**
  現在地などの位置情報を業務に利用する
- [ ] **オリジナルアプリ**
  自社で開発した業務用アプリを利用する
- [ ] **一般向けアプリ**
  マーケットプレイスで公開されている特定のアプリを利用する
- [ ] **その他①**
  その他に実施したい内容がある場合は記載
- [ ] **その他②**
  その他に実施したい内容がある場合は記載

4-2. 守るべき情報の範囲を決定する

守るべき情報を明確化する

　利用用途が明確になった後に検討すべき項目は「守るべき情報の範囲」です。業務データとプライベートデータが共存する BYOD においては、企業が**「どの情報を保護すべきか」**を明確に判断した上で、それに則した運用方法を策定する必要があります。前頁で決定した「利用用途」に関係するデータ**を「企業内の情報として留めるべきもの」「一般向けに公開して問題がないもの」「企業が保護する必要がないもの」の3つ**に分類し、企業が確実に保護すべき対象を明確化します。

ⅰ.企業内の情報として留めるべきもの

　業務上のメール情報や企業の売上情報など、一般公開すべきではないものを指します。

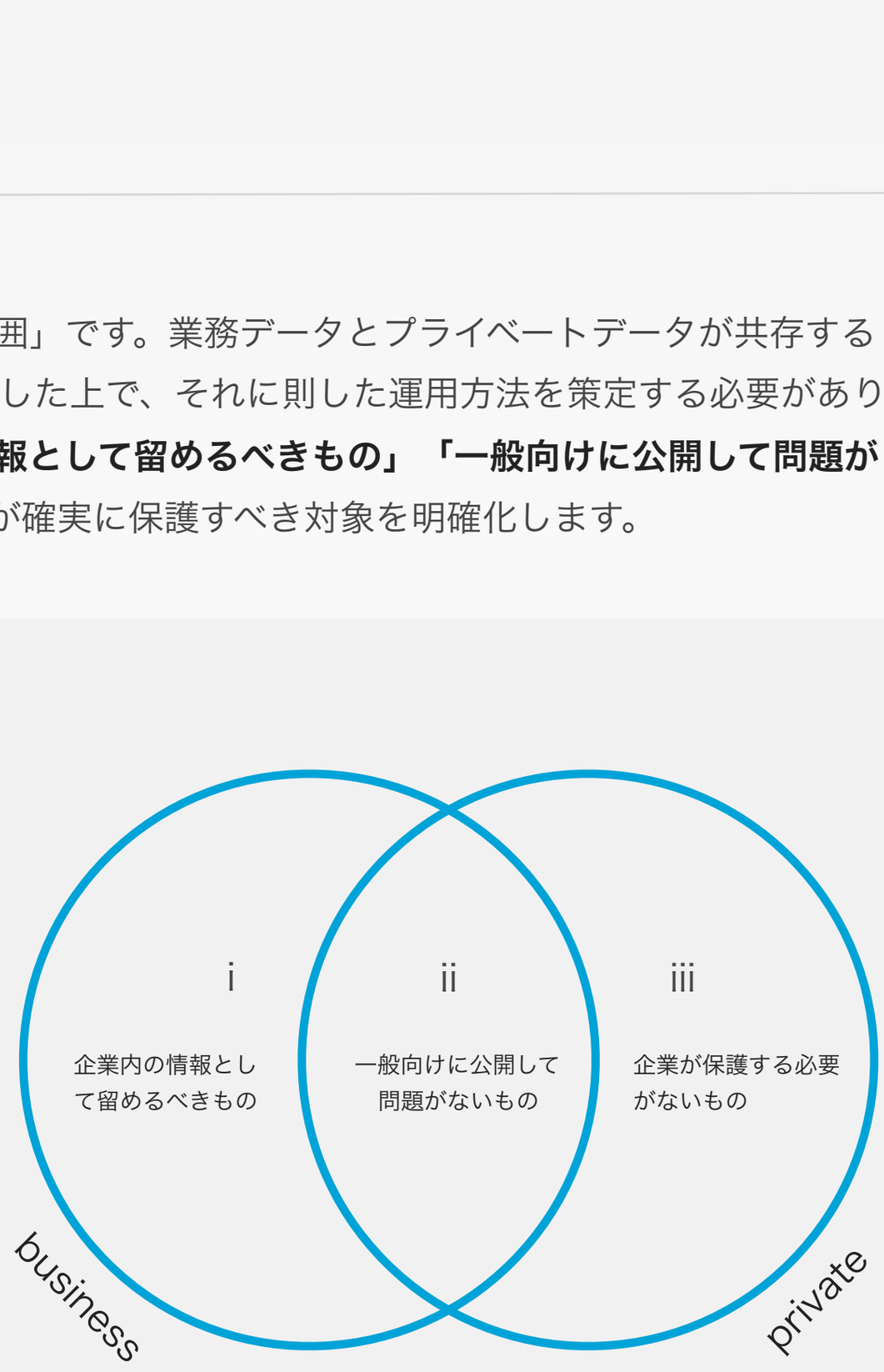
　私物スマートデバイスを経由して、「プライベートで利用中のクラウドサービスへの勝手なバックアップ」や「SNS などに公開されること」を避けるべき情報です。取り扱い方法やルールを設計・徹底した上で、従業員に利用させることが求められます。

ⅱ.一般向けに公開して問題がないもの

　チラシやカタログなど、業務に関わる情報ではあるものの、一般向けに公開されても問題がないものを指します。情報漏えいのリスクを配慮する必要がなく、各従業員の裁量に運用を任せることができます。

ⅲ.企業が保護する必要がないもの

　音楽やムービーファイル、ゲームデータなど、従業員がプライベートで利用している情報を指します。企業が保護・関与する必要がなく、逆にアクセスすることで、プライバシーの問題から従業員の反発にあう可能性があります。



4-3. 運用方針を決定する

利用者と企業とが双方で合意できるレベルを探ることが重要

保護対象が明確化した後には、「保護対象の情報とそれを利用する私物スマートデバイスをどのように運用するか」を検討します。運用の考え方は、大きく以下の3レベルに分けられます。企業が考える管理体制を一方的に押し付けるのではなく、どこまでに企業が干渉するかを、従業員と双方で納得する方針を探ることが何よりも重要です。

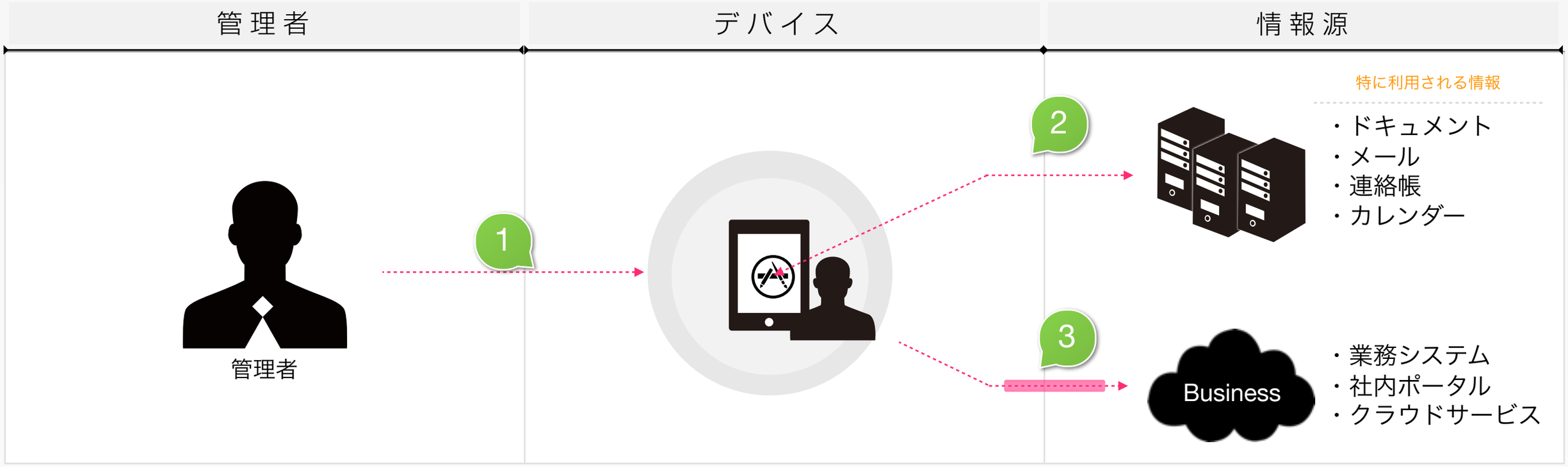
運用方針	盗難・紛失対策	業務用途	プライベート用途
ⅰ.業務中のプライベート用途での利用を強制的に制限する 最もセキュリティレベルが高い運用方法です。業務時間内は、企業が指定する業務用途以外にスマートデバイスを利用できず、また、業務用途についても、企業側が予め指定するルールが強制された状態（添付ファイル保存禁止・連絡帳の転送禁止など）での利用に制限されます。	◯ 消去 / 起動制限	◯ 取扱ルールを強制	◯ 業務中の利用を制限
ⅱ.業務用途での利用時にのみ企業ルールを強制する プライベートを認めつつ、業務用途でのセキュリティレベルを維持する運用方法です。業務時間内にも、写真や動画など、個人データ領域にアクセスできますが、業務用途については、企業側が予め指定するルールが強制された状態（添付ファイル保存禁止・連絡帳の転送禁止など）での利用に制限されます。	◯ 消去 / 起動制限	◯ 取扱ルールを強制	ルール強制しない
ⅲ.万が一の盗難紛失対策のみ実施する セキュリティレベルが最も低い運用方法です。業務用途についても、企業が特別に指定した情報保護やルールは必要なく、各従業員の裁量に任されています。万が一の盗難・紛失時には、対象となる情報の消去やデバイスロックなど、最低限の対策が実施可能な状態です。	◯ 消去 / 起動制限	ルール強制しない	ルール強制しない
実現方法	デバイス全体を対象 CLOMO MDM 業務データを対象： CLOMO SECURED APPs	イントラネット利用時： CLOMO SECURE SUITE 業務アプリ利用時： CLOMO SECURED APPs	業務用途とプライベート利用時のルールの切り替え： CLOMO MDM

セキュリティ強度

⚠ ユーザとの合意難易度について… セキュリティ強度を高めれば高める（◯の数が多い）ほど、ユーザーの合意取得が難しくなります。試験運用およびアンケートを繰り返しながら、使い勝手とセキュリティの適正なラインを探ることが重要です。詳しくは P12 を参照下さい。

参考：運用イメージ例

前頁の方針に則った運用を実施するにあたり、具体的に次のようなサービスを利用することで実現が可能です。



1 デバイスを運用する

デバイス自体を管理することで、盗難・紛失時の対策はもちろん、時間帯による業務ルールの切り替えなど、柔軟な運用が可能になります。

CLOMO MDM
で解決できます
http://www.i3-systems.com/mdm.html

2 業務データ(アプリ)を管理する

メールデータや連絡先、ドキュメントなど、業務データを保持するアプリ自体を管理します。ルールを強制した状態で、業務用途に利用させることが可能になります。

CLOMO SECURED APPs
で解決できます
http://www.i3-systems.com/securedapps.html

3 ネットワーク接続を保護する

社内システムや社内ポータルの利用時に、管理対象のデバイスにのみ、接続を許可するなど、運用性と安全性を両立した利用を実現することが可能になります。

CLOMO SECURE SUITE
で解決できます
http://www.i3-systems.com/secure-suite.html

4-4. 展開方法を決定する

スモールスタートで改善する

　最後に、社内への展開方法を検討します。スマートデバイスは発展途上のテクノロジーであり、ビジネス利用においても「絶対的な正解」が存在しません。そのため、**壮大な計画を練り、時間をかけて実現するのではなく、「スモールスタート」と「トライアンドエラー」を高速で実施することが重要**です。例えば、一部の部署やチームで私物スマートデバイスの利用を許可した上で実態調査を行い、従業員のニーズに基づいた導入を実施することが重要です。

　一方で、「用途を伝えずスマートデバイスの利用を許可する」「各部署ごとに少人数での利用を許可する」方法は失敗を招きがちです。前者では、従業員が目的意識を持った活用となりづらいため、何も実行・検証がされないまま試用が終了してしまい、後者では、「チームとしてのアイデア創出」を妨げてしまい、価値のあるアイデアが生まれづらい状況となってしまいます。

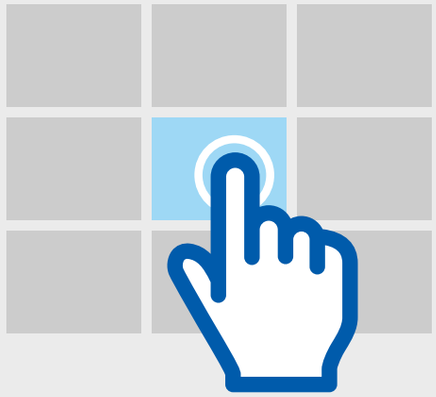
インフォテリア株式会社「タブレット企業導入を支える５つのポイント」より、一部改変の上引用

まとめ

「利用用途を決定する」～「運用方法を決定する」を繰り返し、徐々に利用シーンおよびに展開範囲を拡大・適正化することで、成功へ着実に近づく、実利用に即した BYOD の実現が可能となります。
本ガイドラインによって、貴社のビジネス革新に貢献できることを願っています。

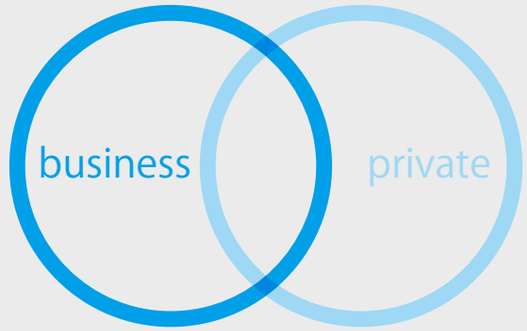
Ⅰ デバイスの利用用途を決定する

スマートデバイスをどのような業務に利用するのか、用途を決定します。



Ⅱ 守るべき情報の範囲を決定する

決定した利用用途の中で、保護する情報の範囲を決定します。

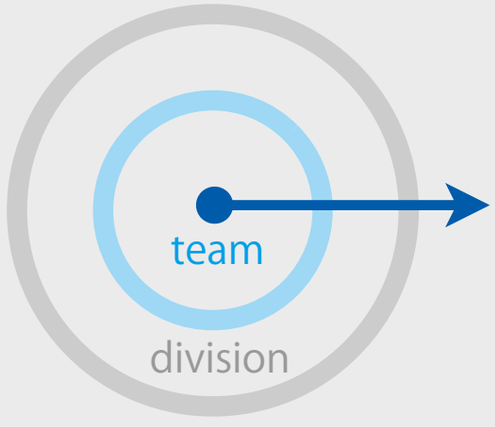


Ⅲ 運用方針を決定する

「保護対象の情報」とそれを利用する私物スマートデバイスを「どのような方針で運用するか」を決定します。

Ⅳ 展開方法を決定する

社内での展開方法を検討します。



本ガイドラインについての問い合わせ先：http://www.i3-systems.com/

Innovation^3