スマートデバイスに関する疑問一挙解決

一般社団法人 日本コンピュータシステム販売店協会
サポートサービス委員会

© 一般社団法人 日本コンピュータシステム販売店協会 2013

はじめに

近年、スマートフォンやタブレットといったスマートデバイスが個人利用において爆発的に普及しております。

この流れは、クラウド環境の整備・普及、スマートデバイス利用時のセキュリティー対策の充実、ＭＤＭ（Mobile Device Management）機能の強化などと相まって、ビジネスシーンにも拡大しつつあり、私達のワークスタイルを劇的に変化させる可能性を秘めています。

この様なビジネス環境の変化をとらえ、本書ではスマートデバイスの基本的な知識から、セキュリティー対策、モバイルデバイスの管理手法、スマートデバイス活用によるビジネススタイルの変化や今後の発展予測までを分かりやすく解説しています。

今後、スマートデバイスのビジネスでの活用について検討する際に、本書がなんらかのお役に立てば幸いです。

一般社団法人
日本コンピュータシステム販売店協会
サポートサービス委員会 委員長 平野 一雄

© 一般社団法人 日本コンピュータシステム販売店協会 2013

目次

はじめに

1. スマートデバイスの種類と特徴 ---------- 1

1.1 スマートデバイスの種類 ---------- 1

1.2 各デバイスの特徴 ---------- 5

2. スマートデバイス普及の背景 ---------- 7

2.1 スマートデバイス市場予測 ---------- 7

2.2 スマートデバイス普及の背景 ---------- 9

3. スマートデバイス導入に伴う
セキュリティー対策 ---------- 27

3.1 セキュリティー対策が身近な問題 ---------- 27

3.2 守るべき大事なもの ---------- 29

3.3 守ってくれるもの、守ってくれないもの ---------- 31

3.4 自分で守るべきところ ---------- 35

3.5 スマートデバイスのセキュリティー対策 ---------- 39

3.6 OS共通のセキュリティー対策 ---------- 41

3.7 OS毎のセキュリティー対策 ---------- 45

4. MDM（モバイルデバイス管理） ---------- 51

4.1 MDMとは？ ---------- 51

4.2 MDMの必要性 ---------- 51

4.3 MDMで提供される機能 ----------53

4.4 MDMサービスの費用 ----------55

4.5 MDMサービスの選択 ----------57

4.6 MDMサービスの導入 ----------59

5. デスクトップ仮想化とスマートデバイスの活用 -61

5.1 デスクトップ仮想化の必要性 ----------61

5.2 デスクトップ仮想化のメリット ----------63

5.3 スマートデバイスへの応用 ----------63

6. スマートデバイス導入による
業務形態の変化と課題 ----------67

6.1 スマートデバイス導入による変化 ----------67

6.2 働き方の変化例 ----------67

6.3 スマートデバイスの活用例 ----------71

6.4 今後の課題 ----------73

7. BYOD導入の課題と対応策 ----------77

7.1 BYODとは ----------77

7.2 BYOD導入のメリット ----------79

7.3 BYOD導入の課題と対策 ----------81

8. 今後の発展の予測 ---------- 83

あとがき

© 一般社団法人 日本コンピュータシステム販売店協会 2013

© 一般社団法人 日本コンピュータシステム販売店協会 2013

1. スマートデバイスの種類と特徴

1.1 スマートデバイスの種類

スマートデバイス（“スマート”は「賢い」の意味）とは、情報処理端末のうちでも、単一の端末に複数の機能を集約した高機能端末を指します。

(1) スマートフォン

上記のスマートデバイスのなかでも、従来の携帯電話機能を基に、個人用のコンピュータ機能を加えたデバイスを指します。本体にOS（オペレーティングシステム）を搭載していて、購入後も対応アプリケーションをダウンロードすることで、機能をカスタマイズすることが可能です。

OSとして、主流となるiOS 、Androidのほか、BlackBerry やWindows Phoneも存在します。

タッチパネル式の製品が多いために、「タッチパネルケータイ」と言われることもありますが、一部に、キーボード式のスマートフォンもあります。

インターネットとの親和性が高いことに加え、持ち運びしやすいサイズのため、出先での利用を目的とした普及が進みました。

＜スマートフォンの利用例＞

(2) タブレット

「タブレット」とは、コンピュータ製品の分類のひとつで、板状の筐体の片面をタッチパネルで操作できるタイプのものを指します。

広義にはスマートフォンもタブレットと見なすこともあります。しかし、その中でも、パソコンを源流としているものに関しては「タブレットPC」として区別することが一般的です。

板状の筐体の前面が、すべて液晶画面になっていて、キーボードの代わりに画面に指やペンなどで触れて操作することで、従来よりも直感的な操作を可能としました。サイズが大きいために、持ち運びの点ではスマートフォンには劣りますが、映像を見たり、作業を行なうなど、大きな画面が求められる場面で活躍します。

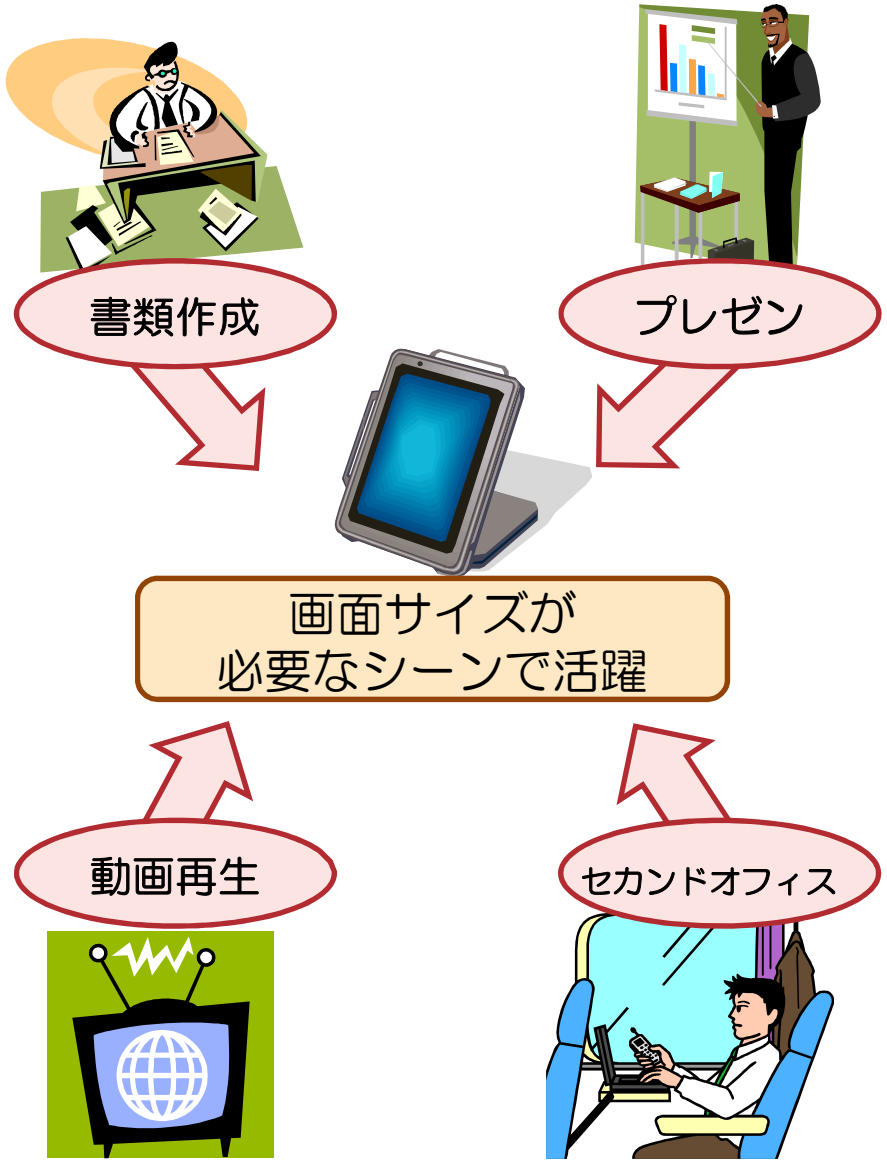
OSは主流のiOS 、Androidに加え、Windowsも注目を集めていて、特にWindows７以降を搭載しているものは「スレートPC」（2010年にMicrosoft社が提唱）と呼ばれます。スレートPCはWindows対応ソフトがそのまま利用可能*なことから、企業内での特定業務向けに浸透が見込まれています。

---

*: Windows on ARMで動作するスレートPCに関しては、一部例外があります。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

＜タブレットの利用例＞



© 一般社団法人 日本コンピュータシステム販売店協会 2013

1.2 各デバイスの特徴

各デバイスは下記の特徴を有します。

	スマートフォン	タブレット	スレートPC
主なOS	iOS Android BlackBerry Windows Phone	iOS Android	Windows
主なメーカー	Apple サムスン ソニーモバイル	Apple サムスン シャープ	NEC 富士通
主な機種	iPhone GALAXY Xperia	iPad GALAXY Tab GALAPAGOS	VersaP`ro STYLISTIC
強み	持ち運びに便利 携帯電話機能	作業効率が高い	Windows対応 ソフトが動作
弱み	事務作業に向かない	持ち運びにはサイズが大きい	

スマートフォンとタブレットでは、サイズが一番の違いとなっています。利用シーンに応じた選択が望まれます。

＜スマートデバイスの分類＞

スマートデバイス

＜x86とARM＞

コンピュータがハードウェアを動かすために用いる命令の集合体（命令セットともいう）には主流であるx86やARMなどの種類があります。

ARMはx86に比べ消費電力を抑えることが可能な命令セットであるため、タブレットのOSやゲーム機に広く用いられています。しかし、命令セットが異なるために、x86上で動作するソフトと互換性がない場合もあるので注意が必要です。

2. スマートデバイス普及の背景

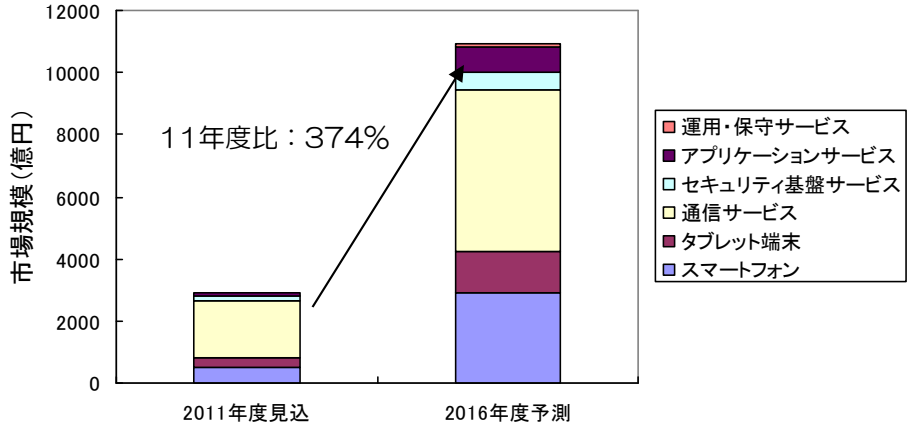
2.1 スマートデバイス市場予測

(1) 法人向けスマートデバイス関連ビジネス市場

■法人向けスマートデバイス関連ビジネス市場

	2011年度見込	前年度比	2016年度予測	11年度比
スマートフォン	520億円	165%	2,900億円	558%
タブレット端末	320億円	267%	1,350億円	422%
通信サービス	1,792億円	138%	5,176億円	289%
セキュリティ基盤サービス	174億円	146%	595億円	342%
アプリケーションサービス	100億円	270%	825億円	825%
運用・保守サービス	20億円	222%	103億円	515%
合計	**2,926億円**	**154%**	**1兆949億円**	**374%**

法人向けスマートデバイス関連ビジネス市場



出典：富士キメラ総研「2012法人向けスマートデバイス関連ビジネスの全貌」*

---

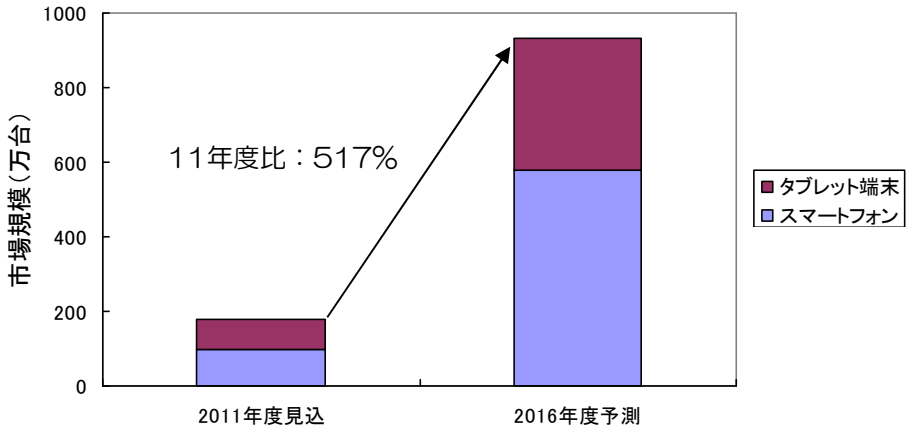
*: URL: http://www.fcr.co.jp/pr/12001.htm

(2) 法人向けスマートデバイス市場

■法人向けスマートデバイス端末市場

	2011年度見込	前年度比	2016年度予測	11年度比
スマートフォン	100万台	167%	580万台	580%
タブレット端末	80万台	267%	350万台	438%
スマートデバイス端末合計	**180万台**	**200%**	**930万台**	**517%**

法人向けスマートデバイス端末市場



出典：富士キメラ総研「2012法人向けスマートデバイス関連ビジネスの全貌」*

---

*: URL: http://www.fcr.co.jp/pr/12001.htm

2.2 スマートデバイス普及の背景

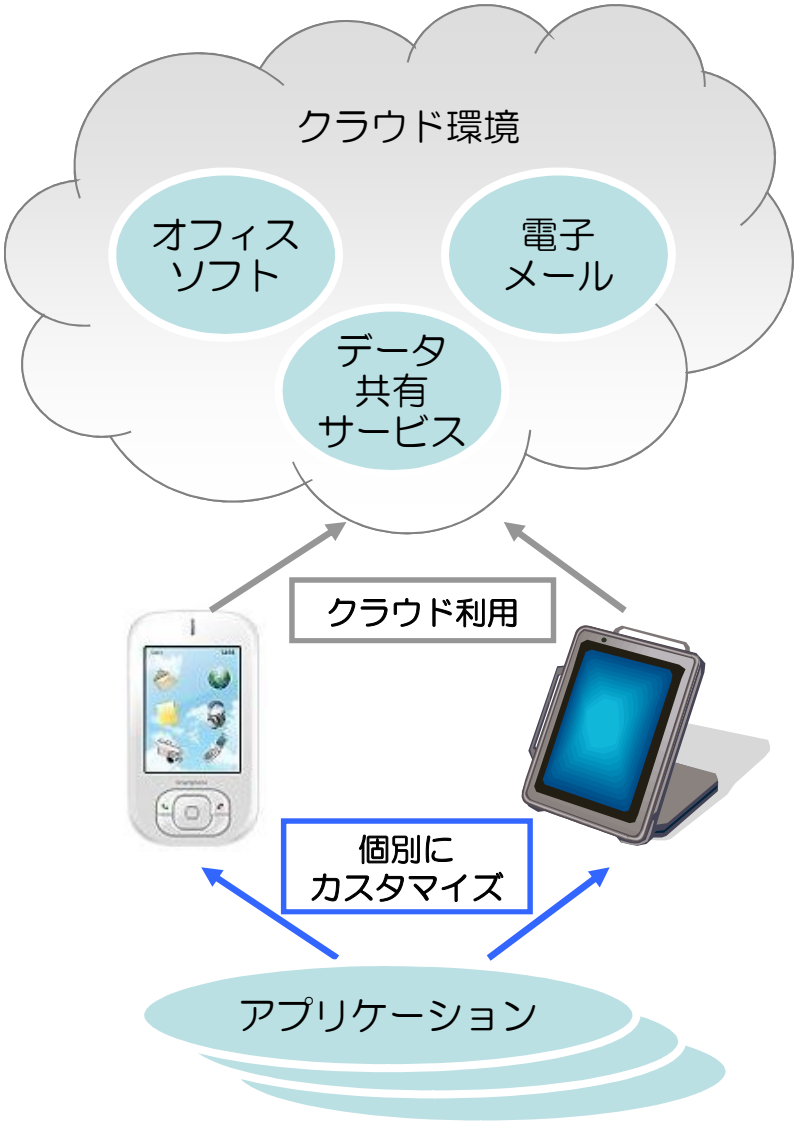
(1) クラウド環境の整備・普及

時間、場所、デバイスを選ばず利用ができるクラウドは、持ち運びに特化しているスマートデバイスと非常に相性の良いサービスと言えます。

例えば、軽量化 / 小型化が進むスマートデバイスは、リアルタイムでの情報収集には最適ですが、本体での複雑な処理や大容量データ保存には向きません。しかし、クラウドを利用して、負荷が大きい処理はサーバーに任せてしまえば、デバイス側からは閲覧とデータ入力のみを快適に利用することができます。

また、スマートデバイスの大きな特長としてもう1つ、アプリケーションと連携しての多機能さが挙げられます。こちらについても、クラウド環境を用いれば豊富なアプリケーションから必要ものだけを随時利用することができる上、最近では開発環境そのものも充実し始めました。

現に、昨今のクラウドサービスには、スマートデバイスでの利用を視野にいれたものが多く登場していて、その利便性は導入を検討している企業にとって追い風となっています。



© 一般社団法人 日本コンピュータシステム販売店協会 2013

© 一般社団法人 日本コンピュータシステム販売店協会 2013

(2) セキュリティー対策の充実

スマートデバイスの活用は社員の業務環境を充実させますが、不正利用や紛失 / 盗難などのリスクを考慮し、導入を見送る企業も数多くあります。

その懸念を払拭すべく、最近になってスマートデバイスのセキュリティー対策が進んでいます。

① MDM（Mobile Device Management）

日本語でモバイルデバイス管理と言われるツールで、スマートデバイスの基本的な管理手法として一般的になりつつあります。

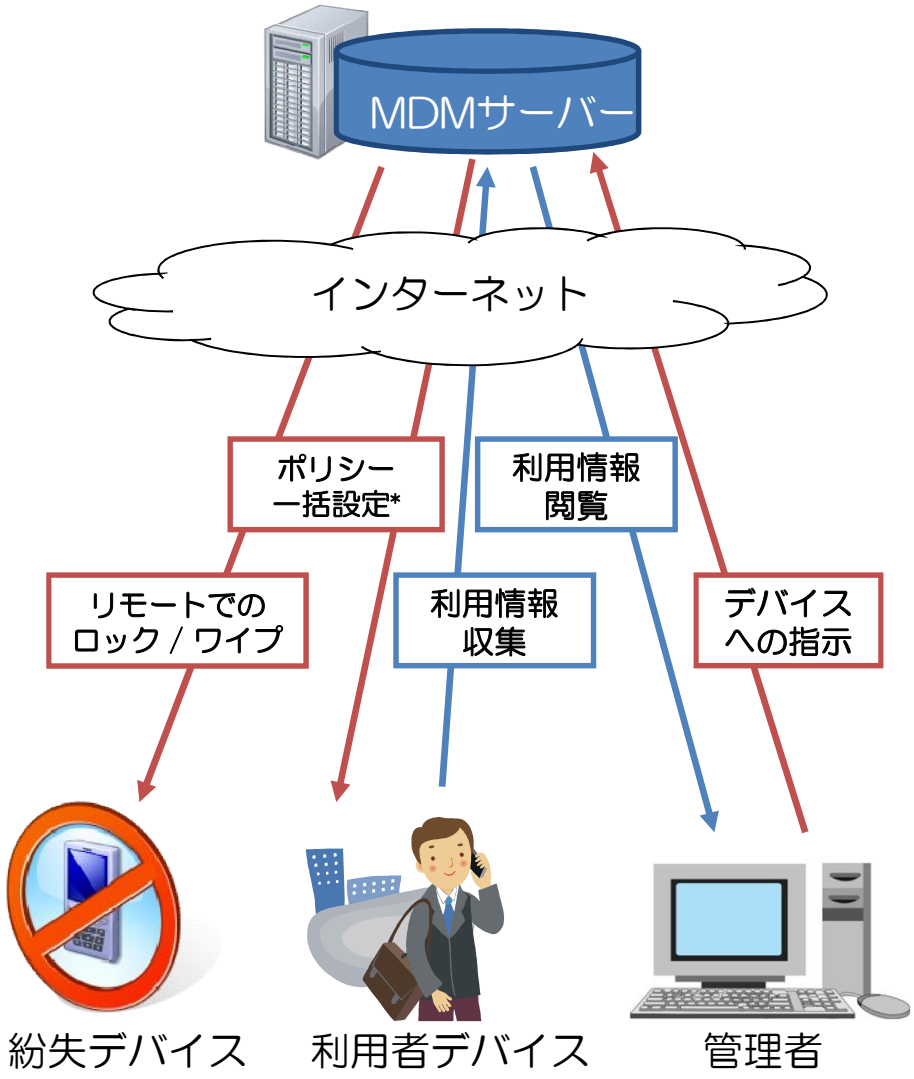
主な働きとして、デバイスのロック / ワイプ（データ消去）、機能の制限、デバイス情報の収集、セキュリティーポリシーの設定などをリモートで実施することがあります。最近では、ビジネスモードとプライベートモードの切り替えができる次世代MDMも登場しています。

② セキュリティーソフトの充実

スマートデバイス向けでは、従来のウイルス対策に加え、ワイプ機能やデバイスの位置検索などの紛失 / 盗難対策も考慮されている点が特長的です。

また、MDMと組み合わせセキュリティーと管理機能を併せて提供するベンダーも現れています。

＜MDMイメージ＞



---

*: 会社毎に定めているセキュリティー基本方針に沿った機能制限を、該当デバイスに対して、一斉に適用することができます。

(3) スマートデバイスの高性能化・低価格化

スマートデバイスは、ここ数年のうちに急激な進化を遂げ、それらに比例するように、普及率も上昇を見せています。

①高性能化

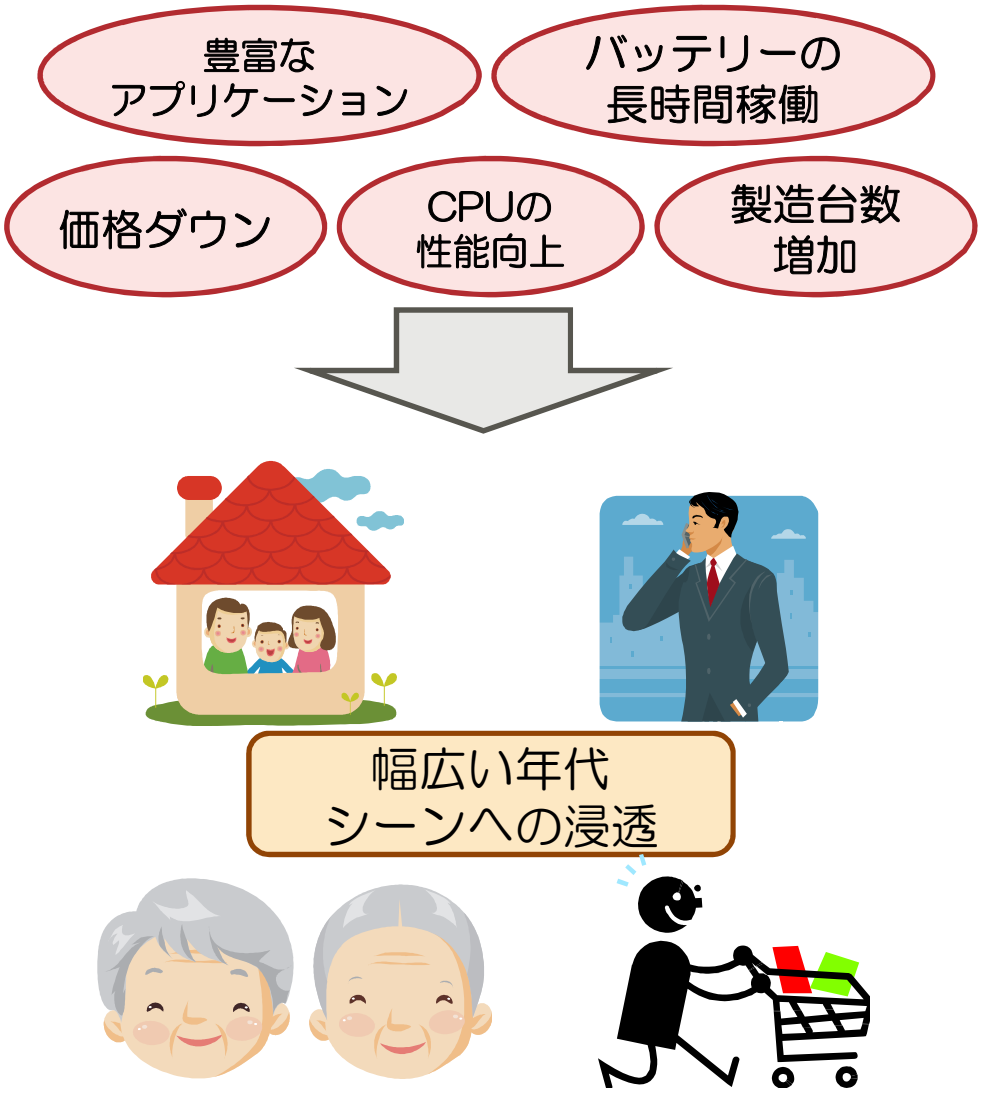
高性能化を支えている要因としては、ハードウェア面での技術進歩と、ソフトウェア面でのアプリケーションの増加が挙げられます。

ハード面では、CPUの性能向上によって軽快な操作を実現すると共に、バッテリーの稼働時間が延び、業務利用にも耐えられるようになりました。

ソフトウェア面では、数多くのアプリケーションから利用シーンや目的に適したものをダウンロードすることで、個々人の好みに沿ったデバイスのカスタマイズが行なわれています。

②低価格化

2010年のiPhone及びiPadの成功を受けて各社がスマートデバイスの開発に注力した結果、製造台数は大幅に増加し、低価格での提供が可能となりました。これにより、スマートデバイスは幅広い層に受け入れられ、市場での爆発的な普及を果たしました。



(4) BCP対策

東日本大震災以降急速に高まった事業継続の重要性について、スマートデバイスが担う役割が大きく注目されています。

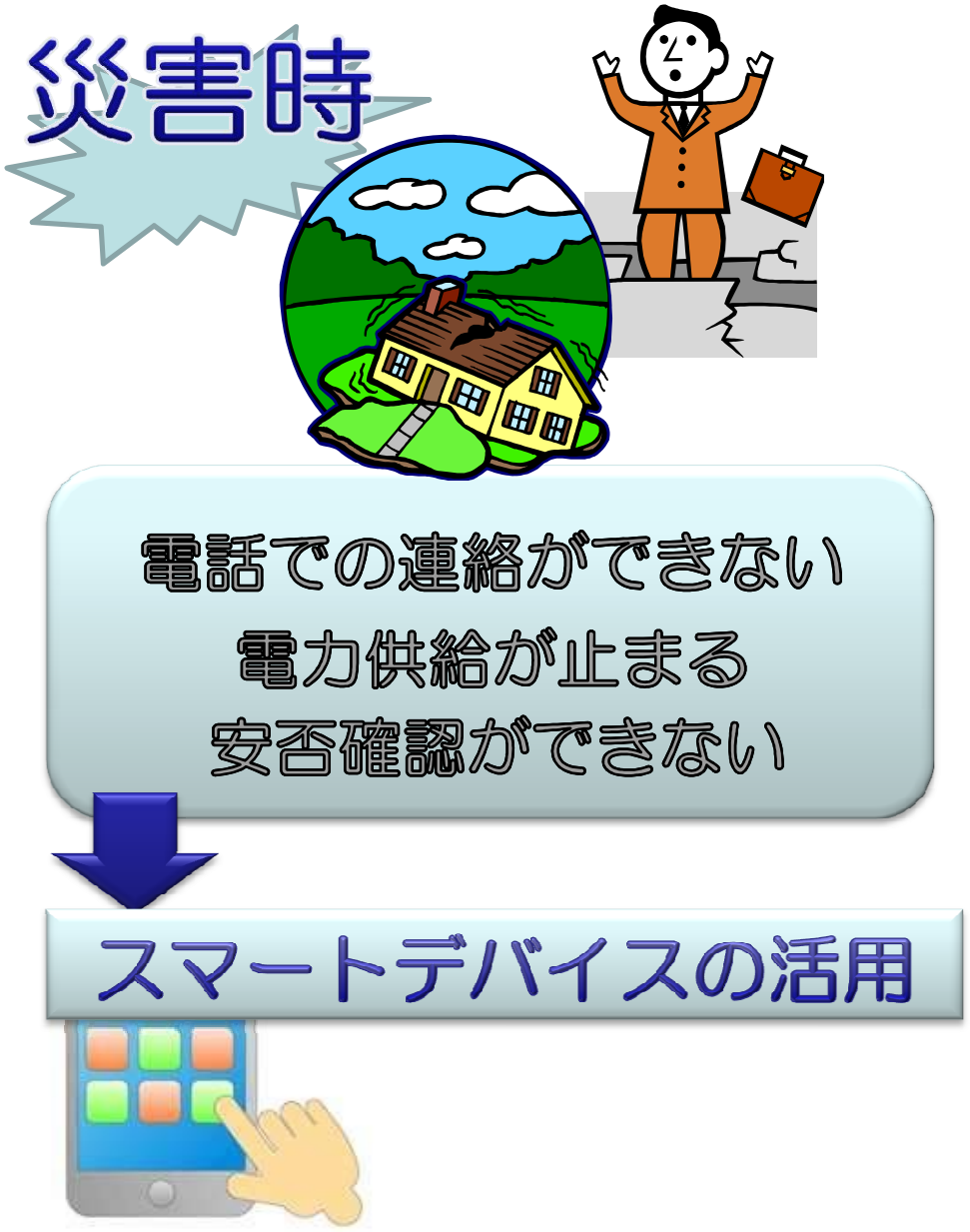
①計画停電

震災による電力不足のため、政府により計画停電が実施されました。該当区域は完全に電力供給が止まってしまうため、通常のコンピュータ端末では支障が起きる場合があります。スマートデバイスであれば、電池での急速充電も可能であり、かつどこでも対応が可能なため、災害への簡易な事前準備対策としても有効であると言えます。

②通話の混雑

震災時、通話はコール数が一気に増加すると交換機に負荷がかかり、通信規制にて繋がりにくい状態となってしまいました。そんな時でも、インターネットは音声通信ではなくパケット通信のため、接続が可能でした。

災害などの異常事態発生時に、個人・法人を問わず、ネット通信での緊急回避、掲示板を利用した安否確認、交通機関麻痺に対する情報収集などを行うことが可能であることから、今後の需要はますます高まっていくことが予想できます。



(5) 回線の高速化・定額化

各キャリアで高速化及び通信価格の低価格競争が激化しています。インフラ環境の整備がスマートデバイス普及に大きな効果を与えています。

①第4世代（4G）通信

スマートデバイスのユーザーは、増加の一途をたどっていて、今後もデータ通信量の増加が見込まれます。各キャリアは現状に対応するため通信高速化の取り組みに注力をしています。

通信高速化の取り組みによって、現在の３G回線から「LTE*」や「WiMAX」という4G回線の通信サービスが登場し、複雑化、大容量化するアプリやデータなどへも対応ができるよう環境整備が進んでいます。

②通信価格の低価格競争

各キャリアとも顧客の囲い込みのため、定額制・低価格でのサービスに拍車がかかっています。

新しい第4世代（4G）通信においては、現状では右図のようなサービス提供になっているが、今後はキャリアごとに個人、法人に対するサービスやプランが多様化されてくることが見込まれます。

---

*: Long Term Evolution:「WiMAX」と並ぶ新たな通信規格で、場所や通信環境もよりますが、最大で光ファイバーレベルの数十Mbpsのスピードを実現できます。

＜4Gサービス一覧＞

キャリア	LTE名	パケット定額制（料金プラン）
NTTドコモ	Xi（クロッシィ）	Xiパケ・ホーダイ　フラット 5985円/月 Xiパケ・ホーダイ　ライト 4935円/月
KDDI（au）	4G　LTE	パケット定額 5985円/月
ソフトバンク	Softbank　4G LTE	パケット定額 5985円/月

NTT ドコモ　　単位:Mbps

	受信時最大	送信時最大	3Gとの差(受信時)
4G LTE(xi)	75	25	約5倍

au　　単位:Mbps

	受信時最大	送信時最大	3Gとの差(受信時)
WiMax	40	15.4	約4倍
4G LTE	75	25	約8倍

ソフトバンク　　単位:Mbps

	受信時最大	送信時最大	3Gとの差(受信時)
4G LTE	75	25	約10倍

2012.11現在

⑹無線LANスポットの充実

公共施設や野外での無線LANスポットの充実および拡大が進んでおり、外出先でのスマートデバイス活用できる環境が整備されてきています。

以前は、駅など一部のエリアのみに限定されていました。しかし、最近ではカフェ・図書館・美容室・ホテル・遊技場・地下鉄・レストランなど様々な施設で無線LANスポットが設置拡大され、スマートデバイスのユーザー増加の一因となっています。

高速な通信を実現でき、かつ集客効果や宣伝効果も期待できることが無線LANスポット普及の背景にあると言えます。

街中で少し注意を払えば、以下のような看板を目にすることができるでしょう。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

⑺ デザイン性

従来の携帯電話は折り畳み式やスライド式など個性豊かなデザインが大きな特徴となっていました。スマートフォンは、単体では大きな画面とボタンという、一見同じような外見のデバイスがほとんどです。この画面の傷付きを防ぐカバーや保護シール、イヤホンジャックアクセサリなどのパーツが様々な会社から提供され、ユーザーのオリジナリティーをもったデザインにすることができます。

デコレーションのカスタマイズ製品を使用することで、より個性的で使いやすさを追求するユーザーの心をつかんでいるとも言えます。また、これらのパーツ販売はハンドメイド一点物で売買されているものもあり、新たなビジネスにもなっています。

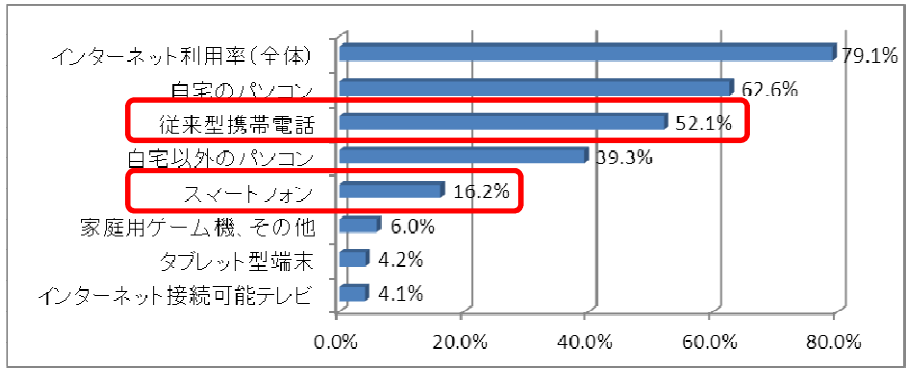
© 一般社団法人 日本コンピュータシステム販売店協会 2013

(8) 見やすい画面

総務省の平成23年1年間の「端末別インターネット利用調査」（下図参照）によると、携帯電話でのインターネット利用者の割合は、50%を超えています。それに対してスマートフォンでの利用割合はまだ16%程度です。

しかし、スマートフォンは急速に普及しつつあります。その主な理由は、画面が見やすいため、インターネットが快適に利用できるという点でしょう。総務省の調査でも（右図参照）スマートフォンへの乗換理由として、「パソコンと同じ画面でネット閲覧ができる」、「画面が大きくて見やすい」が上位を占めています。

端末別インターネット利用状況*（人口普及率）

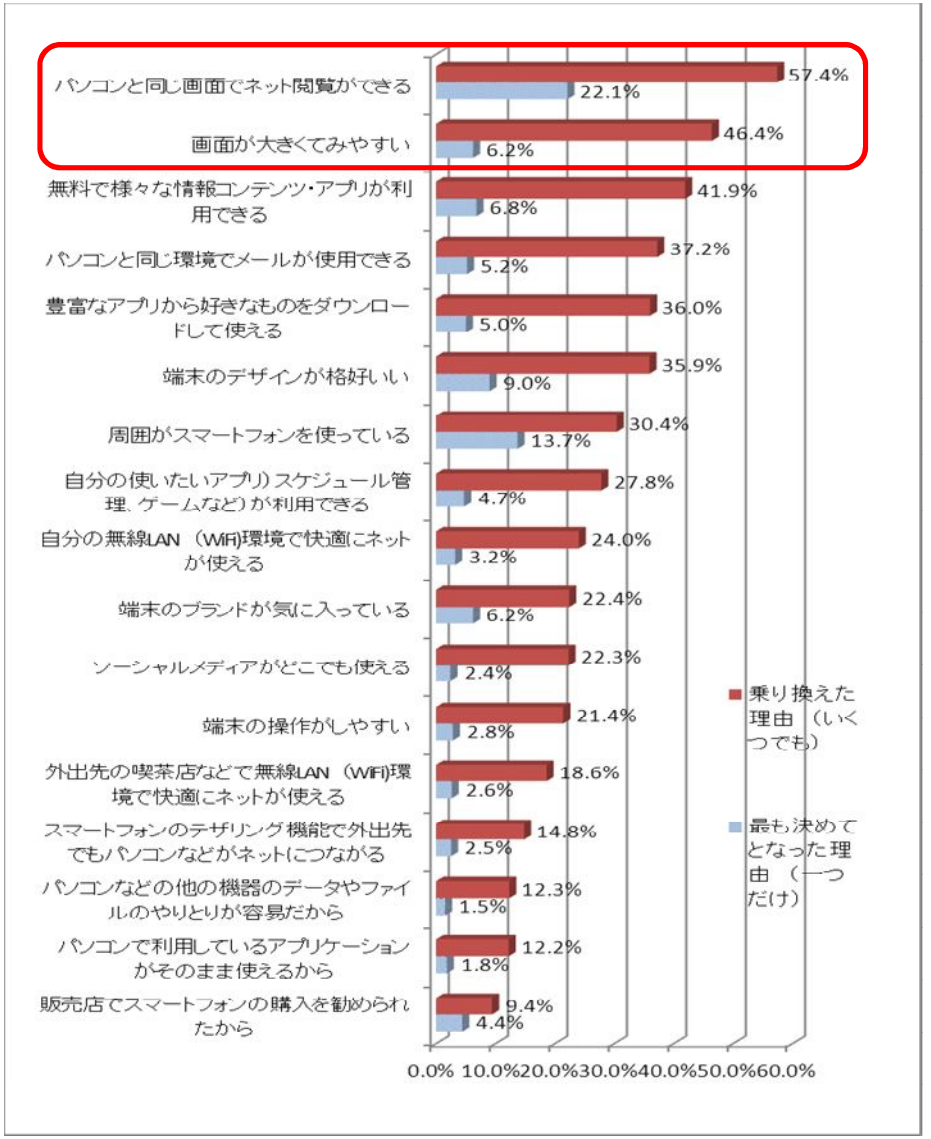


出典:　総務省「平成２３年通信利用動向調査の結果」

---

*:　当該端末を用いて平成23年の1年間の間にインターネットを利用したことのある人の比率を指します。（調査回答者　41,900名）

スマートフォン選択理由



(9) 直観的な操作性

スマートフォンをはじめとするスマートデバイスの操作上の特長は、指で画面にタッチして、直観的な操作ができることです。画面にタッチして画像を拡大、縮小したり、左右上下にスライドできますので、Web閲覧も比較的スムーズです。文字を入力する時は、画面にキーボードの絵を表示して、文字をタッチします。

また、「アイコン」と呼ばれる絵が画面上に並んでいますが、それらは電話、メール、Web閲覧、カレンダー、スケジュール管理表、地図情報など、さまざまな機能を表しています。アイコンにタッチすれば、利用したい機能を起動させることができます。

(10) 豊富なアプリケーション

アプリケーションは略してアプリとも言われるソフトウェアのことで、さまざまな種類があります。生活に密着したものでは、交通の乗換情報や天気予報、ゲームなどがあります。ビジネスツールで代表的なものには、名刺情報管理や、スケジュール管理などがあります。

アプリには無料と有料のものがあります。利用者はニーズや予算に合わせて、アプリをインターネットからダウンロードしてスマートデバイスにインストールして利用します。スマートフォン利用者に対する調査によると、無料アプリでは生活に密着したものが利用率が高く、有料アプリではビジネスツールが利用率が高い傾向にあります。

(11) ソーシャルメディアの登場

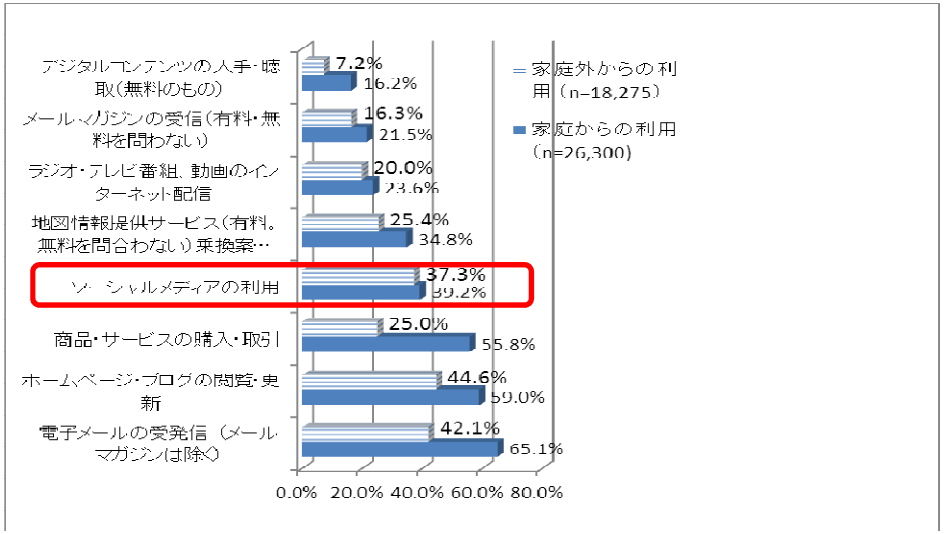
ソーシャルメディアとは、インターネット上で個人や団体などから不特定多数の人々に向けて情報を発信をしたり、意見を募ったりすることで、不特定多数の人々の感想や情報が集まり、コミュニケーションが広がり形成されるメディアを言います。例としては、ホームページ、ブログ（日記のようなもの）、Twitter、ソーシャルネットワークサービス（略してSNSともいうWeb版の会員制コミュニティサイト、Facebookなどを含む）、動画投稿・共有サイトなどがあります。

個人の普及状況を見ると、インターネット利用者のうち40%弱が利用しています。（右上図参照）

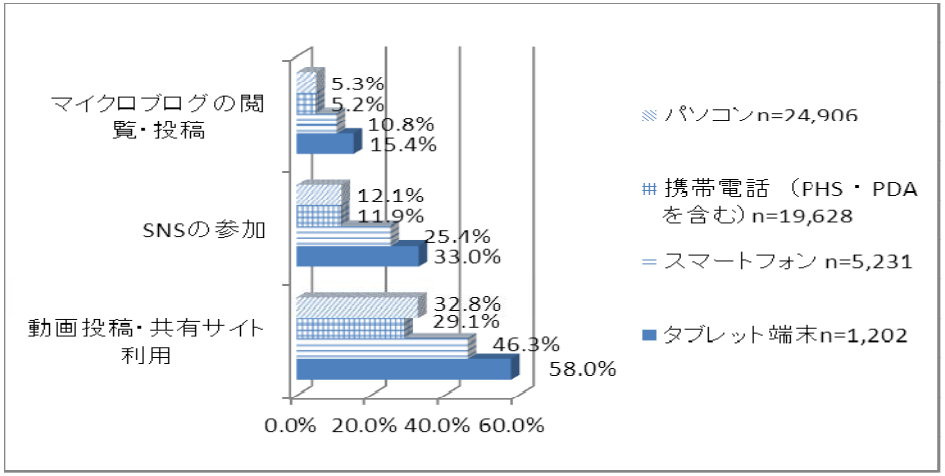
利用されている端末に注目すると、タブレット端末の割合が最も高く、その次がスマートフォンとなっています。特に動画投稿・共有サイトの利用者がそれらの端末を利用する傾向にあります。（右下図参照）

ソーシャルメディアの普及の背景には、いつ、どこからでも話題探しをしたい、知り合いとの間でコミュニケーションを取っていたい、という人々の欲求が考えられます。使いやすいという利点を持つスマートデバイスは、ソーシャルメディアとあいまって、今後普及がスピードアップしていくでしょう。

家庭内・家庭外からのインターネット利用の機能・サービス（個人）（複数回答）（平成23年末）



利用端末別ソーシャルメディア利用率（平成23年末）



出典: 総務省「平成23年通信利用動向調査の結果」

3. スマートデバイス導入に伴うセキュリティー対策

3.1 セキュリティー対策は身近な問題

スマートフォンが普及し、これまで以上にセキュリティーについて注目されるようになったのはなぜでしょうか？

これまでパソコンで行っていた作業の一部を、持ち運び可能なスマートデバイスを使って、いつでもどこからでも行なえるようになったため、ノートPCを外に持ち出すのと同じほどセキュリティーに配慮する必要が出てきました。

この章ではスマートデバイスを安心して使い続けるために、どのような要素を考慮しておくべきなのかを解説します。また個人として、企業として、どのようなセキュリティー対策を行なえるのか、実際例を交えて紹介します。

(1) スマートデバイスにも脆弱性がある

「脆弱性」という用語が良く聞かれますが、これはスマートデバイスにも当てはまります。「脆弱性」は「もろくて弱い性質」や「安全上の欠陥」のことを指しますが、そう言える要素の1つに「バグ」と呼ばれる製造上の欠陥が OS やアプリケーションに潜在していることが挙げられます。

もう1つは、開発者が意図しなかった設計上の欠陥が、経年使用後に明らかになることが挙げられます。

(2) メーカ対応を待つ間にできることがある

もし脆弱性が発見されてしまったらどのような対処が行なえるでしょうか？

開発メーカの対応を待つ間も、利用者自身である程度自衛することができます。脆弱性発見の警告を軽んじることはできませんが、その先の被害にはどんなものがあるかを個人的に知っておくことのほうが重要です。

自分で守れる部分を知っておくことで、安心だと思っていた部分が万が一破られたとき、無防備な状態を避けられます。では、守るべき大事なものとは何かを以下に説明します。

3.2 守るべき大事なものとは何か？

個人や企業にとって、守るべきものとは何でしょうか？

大事なものの中には、有形無形に関わらず、それが損なわれたり悪用されると、利用者自身だけでなく家族や友人にも害が及んだり、さらに会社の経営活動に大きな損害を与えてしまったりするものがあります。例えば、次のようなものがあります。

(1) 個人が守りたいもの

・プライバシー
・財産

(2) 企業が守りたいもの

・信用や評判
・大事な顧客との取引関係
・機密情報

スマートデバイスに含まれている情報が漏洩したり紛失したりすると、悪用されて前述のような事態に発展します。では具体的に何を守ったらよいのでしょうか？次表にまとめてみました。

悪用・漏洩・紛失から守るべきもの

経済的損害と結びつくもの	・電子マネー情報 ・ブラウザーに記憶させたIDやパスワード
信用や評判に関わるもの	・メモ帳などに貼り付けたネットワークへの接続手順やアカウント情報 ・社外秘、部外秘、機密扱いの一時保存ファイル ・顧客や社員や友人が登録されたアドレス帳
プライバシに関わるもの	・プロファイルに登録された個人情報 ・個人が特定できる顔写真ファイル
その他損害につながりかねないもの	・機密情報が記録されたメール ・通話履歴、Web参照履歴 ・テキストメモ、画面メモ

3.3 守ってくれるもの、守ってくれないもの

もともとスマートデバイスには安全を意識した設計が施されていますが、利用者が守りたいと思っている情報をどこまで保護してくれるのでしょうか？

スマートデバイスに組み込まれている安全上の仕組み（セキュリティーモデル）はOSによって異なります。以下では、代表的なOSにおけるセキュリティーモデルについて紹介します。

(1) Apple 社の「iOS」

iOS が動作しているスマートデバイスでは、利用者が悪意あるソフトウェア（マルウェア）を誤ってインストールしてしまう事態から、以下のように保護してくれます。

アプリの入手経路が1つ（AppStore）に限定されており、Apple 社の厳しい審査を通過したアプリのみが公開されるため、スマートデバイスへのマルウェア侵入が防がれます。

(2) オープンソースの「Android」

Android は自由に改変可能な Linux が基盤に使われているため、iOS や Windows Phone や BlackBerry 以上にセキュリティーを堅固にできる潜在能力があるといえます。

とはいえ、現実にはセキュリティーの対応はデバイスの提供元メーカに依存しています。そのため、利用者自身がスマートデバイスへのマルウェア侵入に警戒しなければなりません。

(3) RIM 社の「BlackBerry」

BlackBerry はハードウェアを含め、すべて RIM 社が提供元になっているため、OS の核となる部分（カーネル）の改ざんを検出し保護してくれます。

iOS や Windows Phone と同じように、審査を通過したアプリだけが利用できます。また BES（BlackBerry Enterprise Server）と呼ばれる管理サーバーを企業内に配置すれば、管理者が許可したオリジナルアプリを配信することもできます。

(4) Microsoft 社の「Windows Phone」

Windows Phone も iOS と同じようにアプリ審査があります。Microsoft 社の審査を通過したアプリのみが Windows Marketplace に公開されるため、スマートデバイスへのマルウェア侵入が防がれます。

⑸ Microsoft 社の「Windows 7」

Windows 7 が標準で持っているマルウェア対策機能（Windows Defender）にはウイルス検知・駆除機能がないので注意が必要です。

一般のパソコンと同様に、好き勝手にアプリをインストールすることができるため、提供元メーカの対応や利用者の意識的自衛が求められます。

⑹ Microsoft 社の「Windows 8」

Windows 8 の Windows Defender に新たにウイルス検知・駆除機能が追加され、必要最低限のマルウェア対策が可能になりました。

また、「Designed for Windows 8」ロゴを掲げたＰＣであれば、セキュアブート機能（ハードウェアレベルで Microsoft のデジタル署名が付されたファイルのみ実行を許可する）が追加され、Windows 起動時のルートキット* 侵入を保護してくれます。

スマートデバイス専用の 、Windows on ARM ではアプリの入手経路が1つ（Windows ストア）に限定されるため、マルウェア侵入を防いでくれます。

---

*: 侵入者により悪意のある意図で遠隔操作するために巧妙に仕掛けられたツール群を指します。

OS別セキュリティーモデル

		OS カーネル改ざん検出	OS 起動時におけるルートキット侵入保護	マルウェアからの保護	ユーザーデータの保護*
スマートデバイス	iOS	×	×	○	×
	Android	×	×	×	×
	BlackBerry	○	×	○	×
	Windows Phone	×	×	○	×
	Windows on ARM	×	○	○	×
パソコン	Windows 7	×	×	△ ウイルス対策無	×
	Windows 8	×	○	○	×

---

*: ユーザーデータはOSが保護してくれないので、利用者本人が保護する必要があります。

3.4 自分で守るべきところ

プラットフォームが持つ安全上の仕組みにより、悪意あるアプリからの保護は得られます。しかし個人情報やユーザーデータの保護は利用者自身が意識しなければなりません。では、個人情報とユーザーデータをどのように保護できるのか、実際的例を交えて紹介します。

(1) 最低限必要なこと

・OS を最新の状態に維持する
・ウイルス対策
・セキュリティー強度を下げる行為はしない
・検索結果に表示されるサイトの安全性を確認できるツールをブラウザーに組み込む

(2) 紛失時に役立つこと

・パスワードを保存しない
・自動ロック
・リモートロック、ワイプ手順を確認しておく
・バイオ認証のように当人でないと使えない機能の付いたスマートデバイスを選ぶ
・忘れ物、なくし物防止グッズを活用する

(3) 予防措置

①安全性が確認されているアプリでも、既定の設定のまま使わない。安全な設定例をWebなどから調べ、使う前にセキュリティーに関する設定項目をすべて確認しておく。

②パスワードは単一にせず、重要度に分けて使い分ける。

・銀行口座やセンシティブ情報への照会用
・ショッピングやマイレージポイント照会用
・その他の登録制会員サイトへの認証用

③個人情報が傍受されるリスクを排除するため、Webに情報入力する前に、そのページが 暗号化通信*で接続されていることを確認する。

---

*: URLの先頭は、通常 http:// であるが、https:// で接続されていれば暗号化されています。下図参照

⑷ スマートデバイス故障時に備える

・大切な情報は、暗号化された外部媒体にバックアップする、もしくはメーカの提供するデータ預かりサービスを利用する

⑸ 廃棄時に行なえること

・廃棄業者に任せず、自分で消せるものは消しておく
・Webサイトに登録したアカウントの解約漏れがないよう、登録サイトの URLを1箇所にまとめて保管しておく

⑹ まとめ

脆弱性対策ツールおよびマルウェアからの保護手段は、提供元メーカから入手することができます。

一方、個人情報やユーザーデータの保護は、現状のスマートデバイスの仕組みだけでは完全に保護し切れないので、利用者自身による意識的な自衛（情報漏えいし難い設定、紛失や盗難に遭っても被害を抑える運用）が必要となります。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

残存リスクは利用者自身で回避する

© 一般社団法人 日本コンピュータシステム販売店協会 2013

3.5 スマートデバイスのセキュリティー対策

(1) OSの種類と特徴

スマートデバイスのセキュリティーを考える場合、デバイスに利用されるOSのオープン性について把握しておくことが有効です。

- オープン性が高い：アプリ開発や公開の自由度が増す半面、危険なアプリが増える
- オープン性が低い：アプリ開発や公開の自由度が減る半面、危険なアプリが減る

このようなオープン性とセキュリティーの関係で見ると、現在、日本市場で提供されているスマートデバイスで利用されている各OSには、次のような特徴があると言えます。

① iOS

オープン性は低いものの、多くのアプリが登録されています（2012年4月時点で約60万本）。不正アプリは、ほとんど見つかっていません。

②Android

オープン性が最も高く、最も多くのアプリが登録されています（2012年9月時点で約67万本）。その半面、多くの不正アプリが確認されています（2012年6月時点で約6万本）。

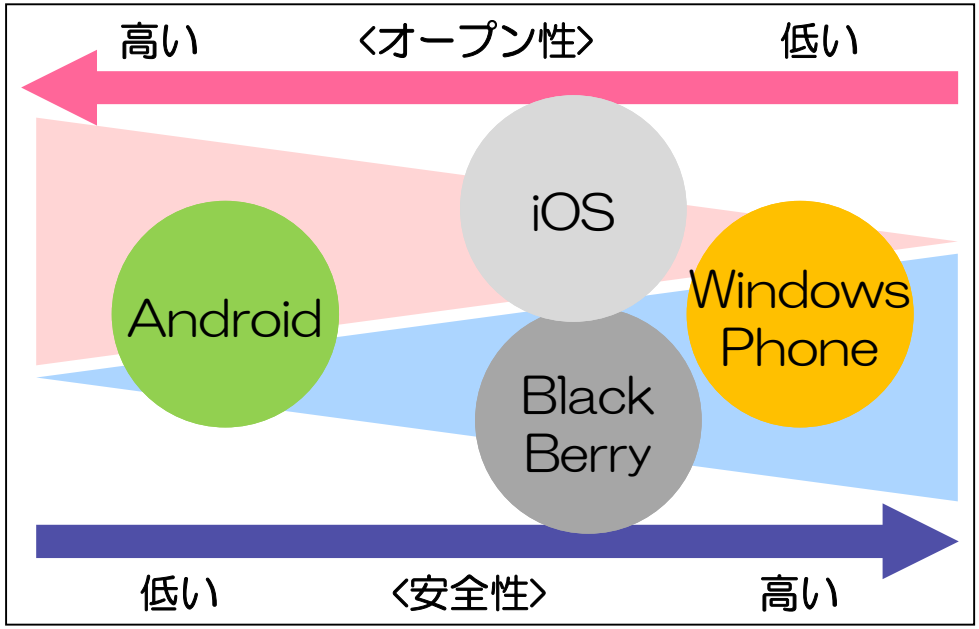
③BlackBerry

オープン性は低く、不正アプリは、ほとんど見つかっていません。登録アプリの数は2012年5月時点で約6万本です。

④Windows Phone

オープン性は低く、現在、最も安全性が高いと言われています。登録アプリの数は、2012年5月時点で約6万本ですが、不正アプリは、ほとんど見つかっていません。

オープン性と安全性から見た各OSの関係



3.6 OS共通のセキュリティー対策

スマートデバイスのセキュリティー対策のために注意すべき点として、以下の点が挙げられます。

(1) パスワードロック

スマートデバイスは、その持ち運びの容易さから他人の手に触れる機会が多いと言えます。デバイス内の情報を保護するために、パスワードロックの設定が推奨されます。

(2) 信頼できる無線LANの利用

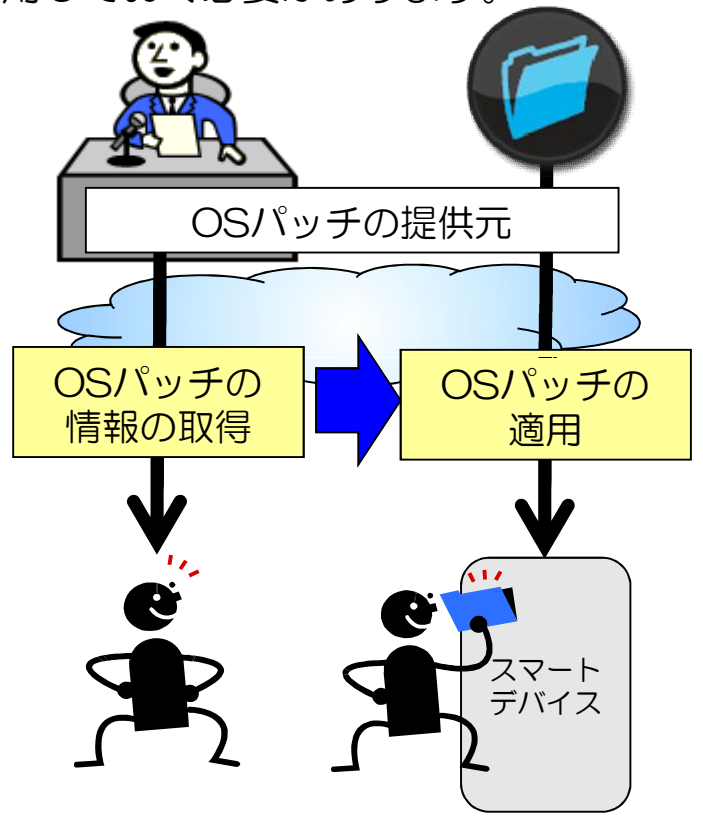
スマートデバイスは、キャリア各社が提供する3G、LTEなどの回線の他に、各種の無線LANを経由してインターネットに接続する機会も多くなります。無線LANは便利な半面、不特定多数の人物が同時に接続することから、スマートデバイスの情報のやりとりを盗聴される危険性が考えられます。

無線LANに接続する際、安全性向上の観点から次の点に注意することが推奨されます。

- 提供元が信頼できる無線LANを利用する
- 接続にパスコードが必要な無線LANを利用する
- 個人情報を含む情報をやりとりする場合は、暗号化された通信を利用する

(3) セキュリティーパッチの適用

パソコンと同様、スマートデバイスにも、OSの脆弱性を攻撃する不正プログラムが存在しています。脆弱性を悪用されないように、常に最新のOSパッチを適用しておく必要があります。



セキュリティー上、常に最新のOSパッチを適用することが望ましい

(4) 管理者権限を取得しない

スマートデバイスでは、利用者に一般ユーザー権限のみを与えることでセキュリティーを強化していますが、特殊な方法を使うと管理者権限が取得できてしまう場合があります。管理者権限を取得すると、利用者の自由度が上がりますが、同時にアプリの自由度も上がります。結果、通常ではできなかった不正な動作を、アプリが実施できてしまう、というリスクが生じます。

セキュリティー上、デバイスの管理者権限は取得しないようにすることが強く推奨されます。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

(5) 信頼できるアプリを利用する

パソコンと同様、スマートデバイスを狙った不正アプリが出現しています。特にAndroid向けの不正アプリが突出して多く、その数は2012年の上半期で6万本、2012年末には12万本を超えると予想されています。

不正アプリによって、電話の通話履歴や現在の所在地などの情報を悪意のある第三者に取得される、といった事例が見つかっています。このようなセキュリティーリスクを減らすために、不正アプリをインストールしないようにすることが重要です。不正アプリをインストールしないための対策として次のようなことが考えられます。

- 信頼できる提供元から配布されているアプリを利用する。
- インストール前に、アプリの評判や機能、アプリが利用する権限について調べる。
- セキュリティーベンダーが提供する対策アプリを導入して、不正なアプリを検知する。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

3.7 OS毎のセキュリティー対策

「3.6」で紹介した注意すべき点のうち、「セキュリティーパッチの適用」、「管理者権限を取得しない」、「信頼できるアプリを利用する」の3つの項目について、日本市場での利用者が多いと言われるiOS、Android、Windows Phoneについて、それぞれ詳しく説明します。

(1) iOS

①セキュリティーパッチの適用

iOSは、OSとデバイス共にApple社から提供されており、iOSのパッチも同様にApple社から提供されます。

②管理者権限を取得しない

iOSの管理者権限を取得することは、一般的に「Jailbreak」と呼ばれ、その方法はインターネット上で容易に見つけることができます。

管理者側での対策として「利用者の教育」や「MDMによるJailbreakされているデバイスの検知」などが考えられます。

③信頼できるアプリを利用する

iOS用アプリの入手元は、Apple社が運営するAppStoreのみとなります。

AppStoreは、アプリの登録時にApple社により厳しい検査が行われており、不正アプリが登録される可能性は低いと言えます。

そのためか、主要なセキュリティーベンダーは、iOS向けの対策アプリは提供していません。ただ、今後もこのような安全な状況が続くとは限らないため、継続的な注意が必要です。

(2) Android

①セキュリティーパッチの適用

Androidデバイスは、複数のベンダーから提供されており、Android OSのパッチは、各デバイスのベンダーから提供されます。

②管理者権限を取得しない

Android OSの管理者権限を取得することは、一般的に「root化」と呼ばれます。root化の方法はインターネット上で容易に見つけることができます。

管理者側での対策として「利用者の教育」や「MDMによるroot化されているデバイスの検知」などが考えられます。

③信頼できるアプリを利用する

まず、Android用アプリは、インストール時に利用する権限を表示する仕組みが用意されています。利用者自身でアプリが利用する権限をインストール前に把握しておくことも、セキュリティーリスクを減らすために重要と言えます。

（アプリが利用する権限とリスクの例）

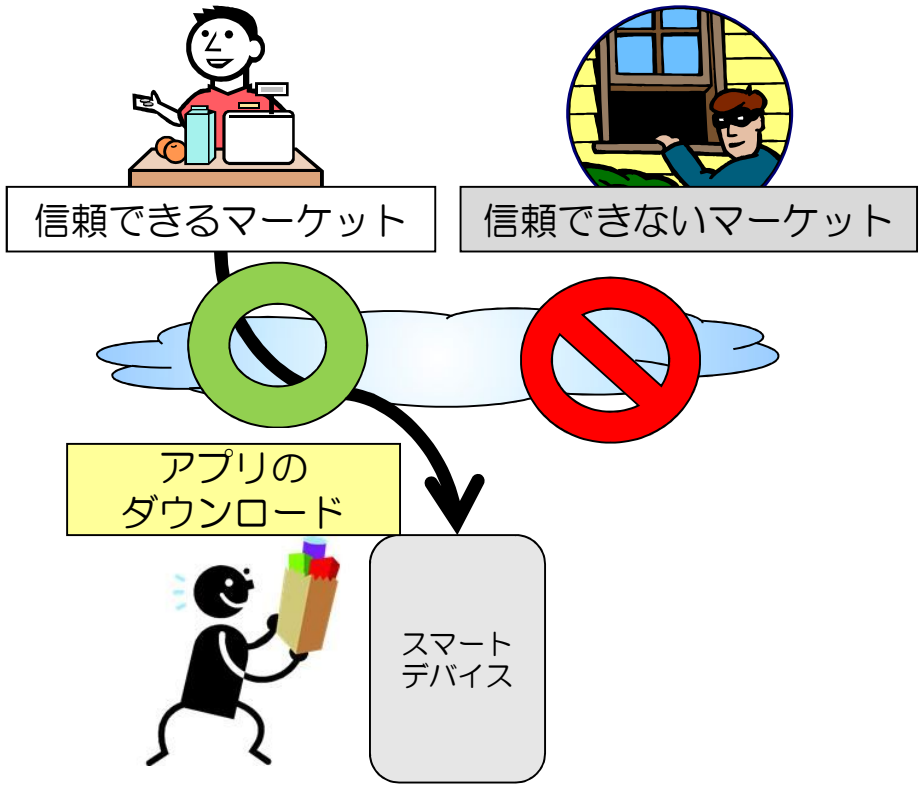
権限	リスク
個人情報	ブラウザの履歴／ブックマーク、アドレス帳などの連絡先情報の書き込み、読み取り
料金の発生するサービス	SMSや電話の発信
送受信したメッセージ	SMSの受信、読み取り、編集など
現在地	デバイスの位置情報の取得

Android用アプリの入手元としては、Google社が運営するGoogle Play Marketがあります。その他にも、Google社以外の第三者が運営するマーケットや、Webサイトから入手が可能です。

第三者が運営するマーケットでは、登録時に検査が行われていない場合があるため注意が必要です。特に海外のマーケットでは不正アプリが多く見つかっています。

インストール時に表示される、アプリが利用する権限の例

このことから、運営者の素性がわからないような場所からはアプリを入手せず、信頼できる場所から入手することが推奨されます。



管理者側での対策としては、「利用者の啓蒙」や「各セキュリティーベンダーから提供されている集中管理型の不正アプリ対策ツールの導入」などが考えられます。

(3) Windows Phone

①セキュリティーパッチの適用

Windows Phoneは、OSがMicrosoft社から、ハードウェアは複数ベンダーから提供されます。OSのパッチは、Microsoft社から提供されます。

②管理者権限を取得しない

現状、root化やJailbreakのような管理者権限の取得は困難と言われています。しかし、Microsoft社の有償の開発プログラムに参加すると、一部権限が取得できますので厳重に管理する必要があります。

③信頼できるアプリを利用する

Windows Phone用アプリの入手元は、Microsoft社が運営するMarketplaceのみです。Marketplaceは、アプリの登録時にMicrosoft社によって厳しい検査が行われており、不正アプリが登録される可能性は低いと言えます。ただ、今後もこのような安全な状況が続くとは限らないため、継続的な注意が必要です。

なお、Windows Phoneとして、現在7.5が主に利用されていますが、今後、主流になっていくWindows Phone 8においても、同様のセキュリティー対策が必要と考えられます。

4. MDM（モバイルデバイス管理）

4.1 MDMとは？

MDMとは「Mobile Device Management」の頭文字を取った略語で、スマートフォンやタブレットデバイスなどを効率良く管理するためのサービスのことです。

MDMは、デバイスにMDMエージェントといわれるアプリケーションをインストールし、クラウド上のMDMサーバーと通信することで、デバイスの管理を行います。

4.2 MDMの必要性

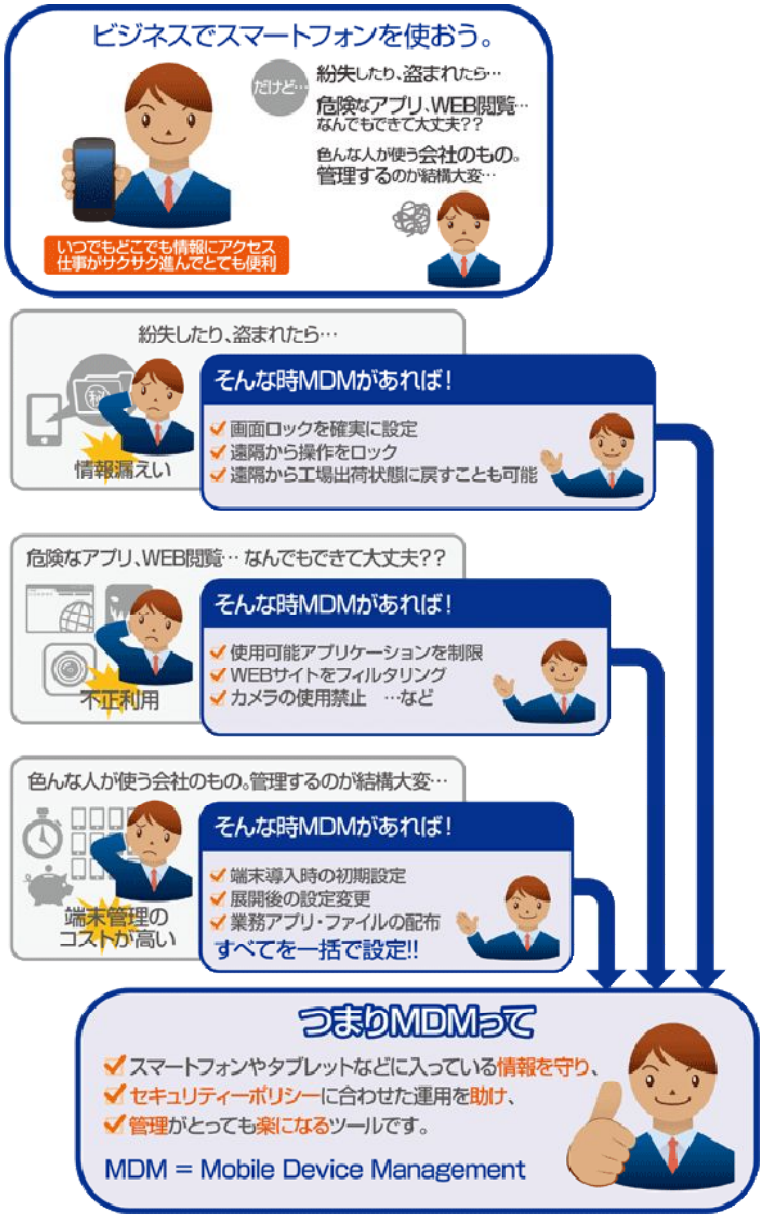
スマートデバイスの利用において、様々なリスク回避や、利便性の向上を図る必要があります。

- 情報漏洩のリスク回避
- 利用環境の整備、キッティング*
- ログやインベントリの回収
- デバイスの利用制限

これらを効率良く実施し、一元的な管理を行うツールとしてMDMが必要となります。

---

*: パソコンなどに、動作に必要なOSやソフトウェアをインストールしたり、環境情報を設定したりすることを指します。「4.5 MDMサービスの選択」参照ください。



株式会社オプティム社のホームページより引用
http://www.optim.co.jp/products-detail/case/155

4.3 MDMで提供される機能

MDMサービスを提供している会社によって、提供される機能に違いがありますが、代表的な機能をまとめたのが右図になります。リモートロック・ワイプや、デバイス情報の配信、アプリケーションの配布などは、ほとんどのMDMでサポートされています。それ以外の機能については、主にスマートデバイスの主流OSである、AndroidとiOSについて解説しています。

一般にApple社が公開しているAPIしか利用できないiOSは機能差が無く、オープンソースのAndroidは、会社によっては提供される機能が大きく異なる場合があります。提供されるサービスを検討し、自社のポリシーに合った機能が提供されるMDMサービスを選択する必要があります。

また、一部製品では「接続ネットワーク種別」、「接続URL」、「起動アプリケーション」などによってポリシーをビジネスモードとプライベートモードに、自動に切り替えるMDMサービスも登場しました。これらプライベートモードをサポートしたMDMは、BYOD*を行う上で有効なツールとなります。

---

*: Bring Your Own Device: 個人所有のデバイスを業務に使うことを指します。

項目	説明文
リモートロック、ワイプ	スマートデバイスを紛失・盗難時に、遠隔地より操作しデバイスを操作できないようロックをすること（リモートロック）またデータを削除すること（リモートワイプ）
操作ログの取得	情報漏えいやウイルス感染時に、どのような操作をしていたか確認すること。ブラウザーの接続履歴の取得など。
位置情報の取得	GPSによる位置情報の取得
デバイス設定の配信	プロファイル、Wi-Fiホワイトリスト設定、お気に入りの一括配信など
インベントリー収集	資産管理やデバイス管理のため、デバイス情報やOSバージョン、ビルド番号、機種名、製造番号などを収集すること
アプリケーション配布	必要なアプリケーションのインストールや、不要になったアプリケーションの削除
アプリケーションの利用制限	ダウンロードの禁止や、許可されていないアプリケーション使用時に禁止メッセージを出す、独自ランチャーによるアプリの制限（製品固有デスクトップを表示させない）
デバイスの利用制限	SDカード、USB、Wi-Fi、カメラなどデバイスの利用制限をすること

4.4 MDMサービスの費用

料金体系は、サービスを行っている会社によって異なりますが、初期導入費用＋毎月の使用料となっているのが一般的です。スマートデバイスは、外に持ち出すことが多いため、MDMサーバーのほとんどはクラウドに置かれます。

毎月の使用料は、ライセンス料とクラウドに置かれたMDMサーバーの維持費と説明されます。多くの機能を備えたMDMサービスでは、使用する機能によって料金が変動し、多くの機能を使用する程、毎月の使用料が高くなります。

この他、専用端末のような使い方をし、外部と通信せず社内のネットワークにしか接続しない場合は、イントラネット内にサーバーを置く必要があります。その場合は、サーバー構築 / 保守などの費用が別途かかることになります。サーバーを自社で管理する場合MDMエージェントや、管理ツールのUpdateを行うためにソフトウェア保守契約が必要であったり、ライセンス形態が複雑になります。しかし、クラウドに置かれたサーバーの使用料が発生しないため、ライセンスの一括買い取りならば、毎月の使用料は下がるケースが多いと考えられます。

基本機能：基本料金で利用できる機能

オプション機能：追加料金が発生

株式会社オプティム社のカタログより引用

4.5 MDMサービスの選択

導入には、以下の要件が必須になります。

・使用するデバイスのプラットフォーム、バージョンがサポートされている
・自社で絶対に必要なサービスが提供されている
・予算内に収まる料金である

必須ではありませんが、以下の要件もMDMサービスの選択には、重要なファクタになります。

・キッティングのしやすさあるいはキッティングを委託する場合の価格）
・管理ツールの使い勝手
・サービスを提供している会社の信頼性

デモ環境で管理ツールを実際に使用し、自社が求めている機能が、どんな形で実装されているか確認しましょう。

また、導入する場合、キッティングを含めてどの程度、費用（あるいは工数）がかかるのか、シュミレーションすることが必要です。

＜キッティング ってなに？＞

キッティングとは英語のkittingであり、元々は「装備、配備」などの意味です。

ITの世界では、導入するデバイスの、必要なメモリーや周辺装置などの増設、OSのセットアップ、アプリケーションのインストール、各種設定を行って、実際にデバイスが使用できる環境まで設定する作業を指します。

例えば、Windows7がインストールされたパソコンであれば、ボリュームライセンス版のOSメディアを使ってマスターPCを作成すれば、そのイメージを別のマシンへ複製*することで、ほぼ同じ設定のデバイスを量産することができます。

しかし、AndroidやiOSでは、作り込んだイメージを別のマシンに複製することができません。そのために、MDMサービスを使ったアプリケーションや、設定の配信などが注目されています。

＊：OEM版のOSイメージの複製は、Microsoft社により禁止されています。

4.5 MDMサービスの導入

MDMの機能を有効化するには、デバイスへのMDMエージェントのインストールとアクティベーションが必要になります。アクティベーションが終わり、MDMのエージェントが動作する状態になれば、その他のアプリケーションの配布や、デバイス設定情報の配信などはサーバー側から行うことが可能になります。そのため、スマートデバイスのキッティングは、MDMの機能を使って次の様に行われることがあります。

①初期セットアップと最低限のセキュリティー設定
②MDMエージェントと、アンチウイルスソフト*のインストール
③インターネットに接続
④MDMエージェントと、アンチウイルスソフトのアクティベーション
⑤MDMサーバーと設定の同期

スマートデバイスは、パソコンと違いイメージの複製ができません。そのため、MDMを使ったキッテングは、大量導入にはかなり有効です。

---

*: 特にAndroidでは、ウイルスの脅威があるためネットワークに接続する前に、アンチウイルスソフトをインストールすることが推奨されます。

＜アクティベーション ってなに？＞
アクティベーションとは英語のactivationであり、一般には「活性化する」と訳されています。

つまり、インストールしたアプリケーションを「活性化」するわけですが、MDMエージェントやアンチウイルスソフトなどは、インストールしただけでは動作せず、このアクティベーションの操作が必要になります。下の画面コピーは、Android用のTrend Micro Mobile Securityのアクティベーション画面です。サーバーに登録された固有情報や、アカウント＆パスワードを入力する必要があり、その情報から管理されるデバイスを特定します。

5. デスクトップ仮想化とスマートデバイスの活用

5.1 デスクトップ仮想化の必要性

スマートデバイスの登場以前、社外に持ち出すデバイスはノート型のパソコンが主流でした。Windows 95の発売以来、デスクトップ環境はMicrosoft社のWindows系のOSがデファクトスタンダードだった言っても過言ではないでしょう。長年培われたWindowsのアプリケーションを、スマートデバイスでも利用できたら？と考えるのは、自然の成り行きでしょう。

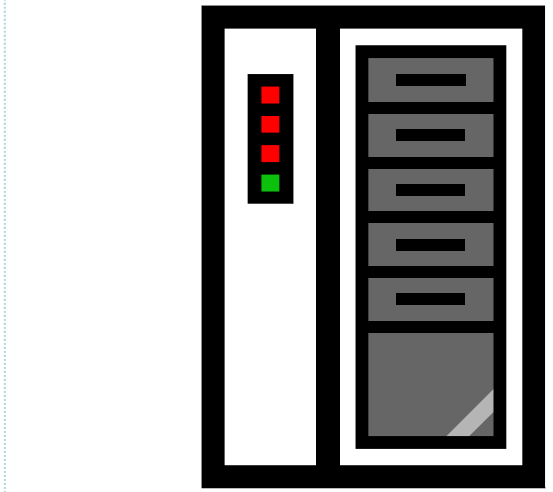
しかし、Windowsと、スマートデバイスで使われているAndroid / iOSは、全く異なったOSでありアプリケーションに互換性はありません。そこで登場にするのが、デスクトップ仮想化といわれる技術ですが、元々はシンクライアント*を実現するために生れた技術でした。

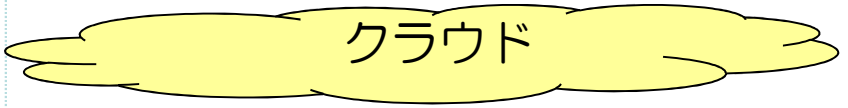
現在主流になっている方式は仮想マシン型（仮想PC方式）といわれるもので、サーバー側の仮想環境（仮想PC）でOSを含めたアプリケーションが実行され、ネットワークを通じて画面 / KB / マウスの情報が、シンクライアントとやり取りされる方式です。

---

*:データ処理、保存のほとんどをサーバーで行い機能を最小限に絞った端末を指します。

仮想PCを動かすサーバー





シンクライアント

5.2 デスクトップ仮想化のメリット

デスクトップの仮想化によって得られるメリットは様々考えられますが、大きくは次の２点に絞られます。

(1) セキュリティーの向上

言うまでもなく、データの持ち出しをサーバー側で制限できるため、情報漏洩のリスクを軽減することができます。また、OSのパッチや、アンチウイルスソフトのパターンファイルの更新などサーバー側で管理できるため、マルウェアによるリスクも低減します。

(2) 管理コストの低減

デスクトップ環境が、サーバーに集約されているため、サーバー上で仮想マシンの管理を行うことができます。このため、アプリケーションのインストールやデスクトップ環境の変更、ポリシーの適用などを容易に行うことが可能になります。

5.3　スマートデバイスへの応用

デスクトップ仮想化のソリューションは、多く存在しますが、仮想マシン型（仮想PC方式）の製品では、Citrix社のXenDesktopとVMware社のVMwareViewが大きなシェアを持っています。

＜デスクトップ仮想化にはお金がかかる？＞

シンクライアントの普及が、予想より進まなかった理由の1つにデスクトップ仮想化環境の構築に、お金がかかり過ぎるというものがありました。もう1つの理由は、外出先のネットワーク速度が現在よりもかなり遅く（アクセスポイントも少なく）、実用的なパフォーマンスで利用できる環境が限られていました。

実際、デスクトップ仮想化環境の構築には、かなりお金がかかっていました。理由は色々ありますが、サーバーのパフォーマンスが低かったので、役割ごとにサーバーを用意しなければならず、サーバーの台数が非常に多く必要でした。また、共有ストレージもFibre Channelを使った非常に高価なものが使用されていました。

しかし、現在では共有ストレージは安価なiSCSIが主流になっており、サーバー価格性能比も格段に向上しています。用意するサーバーの数も、仮想化によって1台のサーバーに複数の役割をさせるなどで、減らせるようになりました。

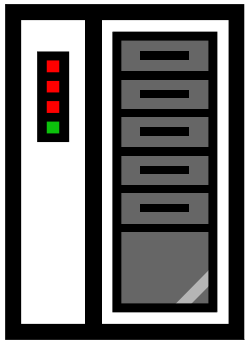
最新のサーバーを使った構成で、今一度検討してみてはいかがでしょうか？

各々の製品についての詳細は割愛しますが、これらデスクトップ仮想化製品の、クライアント側のアプリケーションにはスマートデバイスの代表的なOSである、iOSとAndroidがサポートされています。

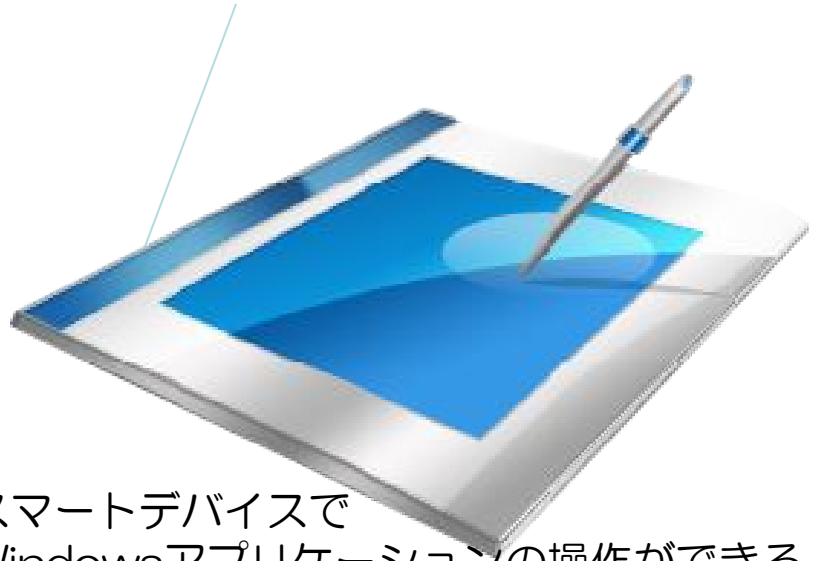
・Citrix Receiver
・VMwareView Client

これらのソフトをスマートデバイスにインストールすることによって、Windows上のアプリケーションを、あたかもスマートデバイス上で動作しているように操作することができます。なお、アプリケーションが実際に動作しているのは、サーバー上の仮想PCであり、データもサーバーに接続されている共有ストレージなので、セキュリティーも万全です。

このように、本来全く違ったプラットフォームであるWindowsのアプリケーションを仮想PC上で動作させ、スマートデバイスにReceiverソフトをインストールしてシンクライアントの様に利用することで従来のWindowsクライアントで動作していた多くのアプリケーションを、スマートデバイスから操作することが可能になります。



仮想PCを動かす
サーバー



スマートデバイスで
Windowsアプリケーションの操作ができる

6. スマートデバイス導入による業務形態の変化と課題

6.1 スマートデバイス導入による変化

パソコンや携帯電話を中心に使用していた今までの業務形態は、スマートデバイス導入によって変化が起こります。ここでは、業務形態がスマートデバイス導入によって変化する点、変化しない点をまとめました。（詳細は右ページ参照）

(1) 機器・アプリなどから見た変化

スマートデバイス導入によって、「場所」や「回線」の制約から解放され、より「その仕事に適した場所・機器・ソフト」での作業が可能となります。

(2) 働き方から見た変化

全体としては、作業場所が固定されなくなるため、これまで社内（事務所内）で行っていた作業が社外でできるようになります。

6.2 働き方の変化例

まず、一般的な想定として、営業と総務での仕事の変化を挙げてみます。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

＜スマートデバイス導入による変化＞

（変わる点）

	従来		これから
機器	パソコン ケータイ	→	スマートフォン タブレット
ネットワーク	固定回線 携帯回線		Wi-Fi 高速回線（LTEなど）
入力	キーボード マウス テンキー		タッチパネル
アプリ・データベース	ローカル サーバー		クラウド
作業場所	固定席		どこでも
報告・決裁	社内で		どこでも

（変わらない点）

大量の入力作業	機器の制約（能力など）から、スマートデバイスでの作業には不向き
画像処理・編集	
文書の（大幅な）編集	
移動のメリットがない場合 （社内で完結する作業）	移動できることより画面の大きさなどのメリットが大きい場合は、引き続きパソコンでの作業が選択される
セキュリティーなどの問題で情報が一元化されている作業 （総務・人事系の作業など）	

© 一般社団法人 日本コンピュータシステム販売店協会 2013

(1) 営業の働き方

スマートデバイスにカタログやマニュアルを入れることで、今まで紙媒体で持ち歩いていた書類の大幅な削減が期待できます。

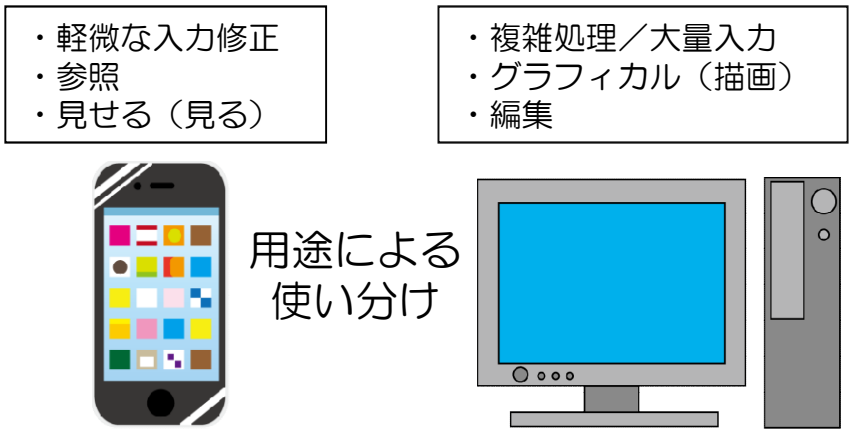
外出先から社内システムにアクセスできるため顧客対応のスピードがあがり顧客満足度が向上しました。また、報告業務も社内に戻る必要が無くなり残業の削減に繋げられると考えられます。

スキル向上のため、ｅラーニングを隙間時間を利用し実施することで商品知識などのスキル向上に活用が可能です。

その他、ファイル共有、プレゼンテーション、メール、スケジュール管理に活用し営業活動のスピードアップ、パフォーマンス向上の効果が想定されます。

(2) 総務の働き方

スマートデバイスの恩恵にあずかりづらいと思われる社内での作業でも、各種申請・決裁のスピードアップや、社外に出ている社員との連絡や転送が密になることで、連絡待ちや取次にかかる時間を削減でき、本来業務に集中できる効果が期待できます。



6.3 スマートデバイスの活用例

業務ごとの事例を、以下に示します。

(1) 自動車販売、アフターサポート

車両販売の商談でスマートデバイスを利用し、動画などのデジタルコンテンツを説明に使い商談に活用しています。

また、車を整備するメカニック担当者がマニュアルや電子カタログを活用し効率化に効果を上げています。

(2) 医療

病院では、医師が電子カルテ閲覧に、看護師が入院患者への作業メニューの確認に利用しています。

(3) 飲食店

飲食店では、スマートデバイスを注文受付専用端末として活用し人件費の抑制、注文ミスの削減に効果があがっています。

(4) 教育

教育現場でもスマートデバイスを利用し、多数の資料を持ち歩くことなく大量の情報を教育に活用しています。

(5) コンピュータ保守

コンピュータの保守業務では、入力済の作業予定と、スマートフォンで出先から入力した作業状況から、エンジニアの空き時間を見計らい、日中発生した保守依頼の自動アサインを実現しています。ＧＰＳ機能の活用で、顧客先への到着に要する時間の割り出しも可能になっています。

また、多種多様な機器の最新の修理手順を、外出先から本社のサーバーへ接続して確認できるので、急遽発生した障害についても簡単な修理であればその場で対応することが可能となり、お客様のダウンタイム短縮に貢献しています。

6.4 今後の課題

スマートデバイスの導入は、単純にパソコンでの作業の置き換えとはならない場合もあるため、導入の可否、導入対象業務（人）などを事前に検討し、目的を明確にすることが必要です。

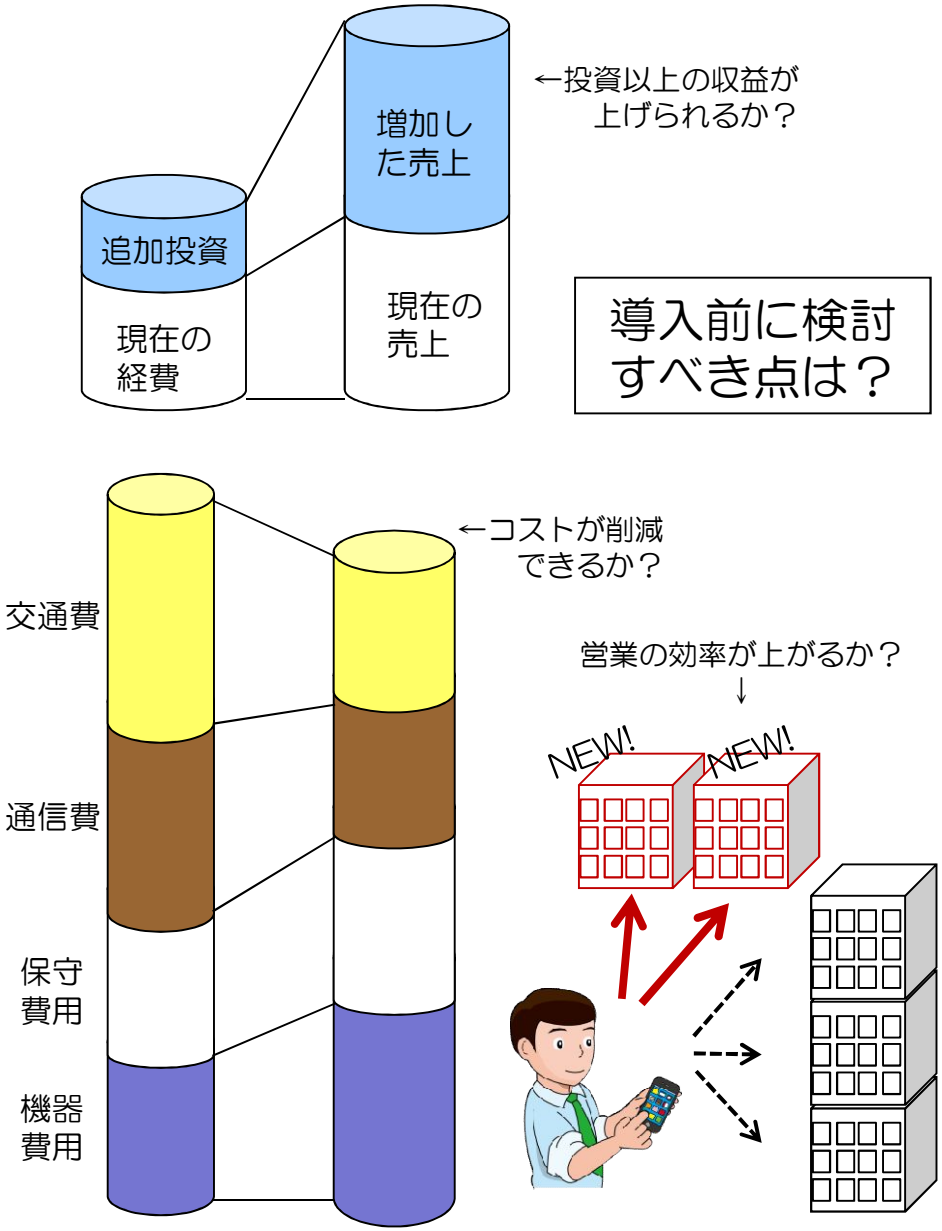
(1)費用対効果の明確化

ノートPCと携帯電話で行なっていた業務がスマートデバイス1台で可能となった場合、スマートデバイスの機器導入コストは必要ですが、通信コストを削減できます。

また、スマートデバイス利用で外出先で業務が完結できるため、自宅からの直行直帰が可能になり、残業代・交通費削減などの効果があります。

一方、スマートデバイスだけではすべてのIT業務を代替できないため、業務の棚卸・目的の明確化ができない導入は、単に導入・保守費用の増大となり効率化につながらないことに留意が必要です。

また、導入の際にも、購入するか / リース（月額料金）するかなど、負担を軽減化する工夫が必要になることがあります。



⑵管理手法の具体化

これまでみてきたように、これまでの一元的・固定的な機器導入管理とは違った、多種多様なデバイスや情報流通の管理が必要になります。

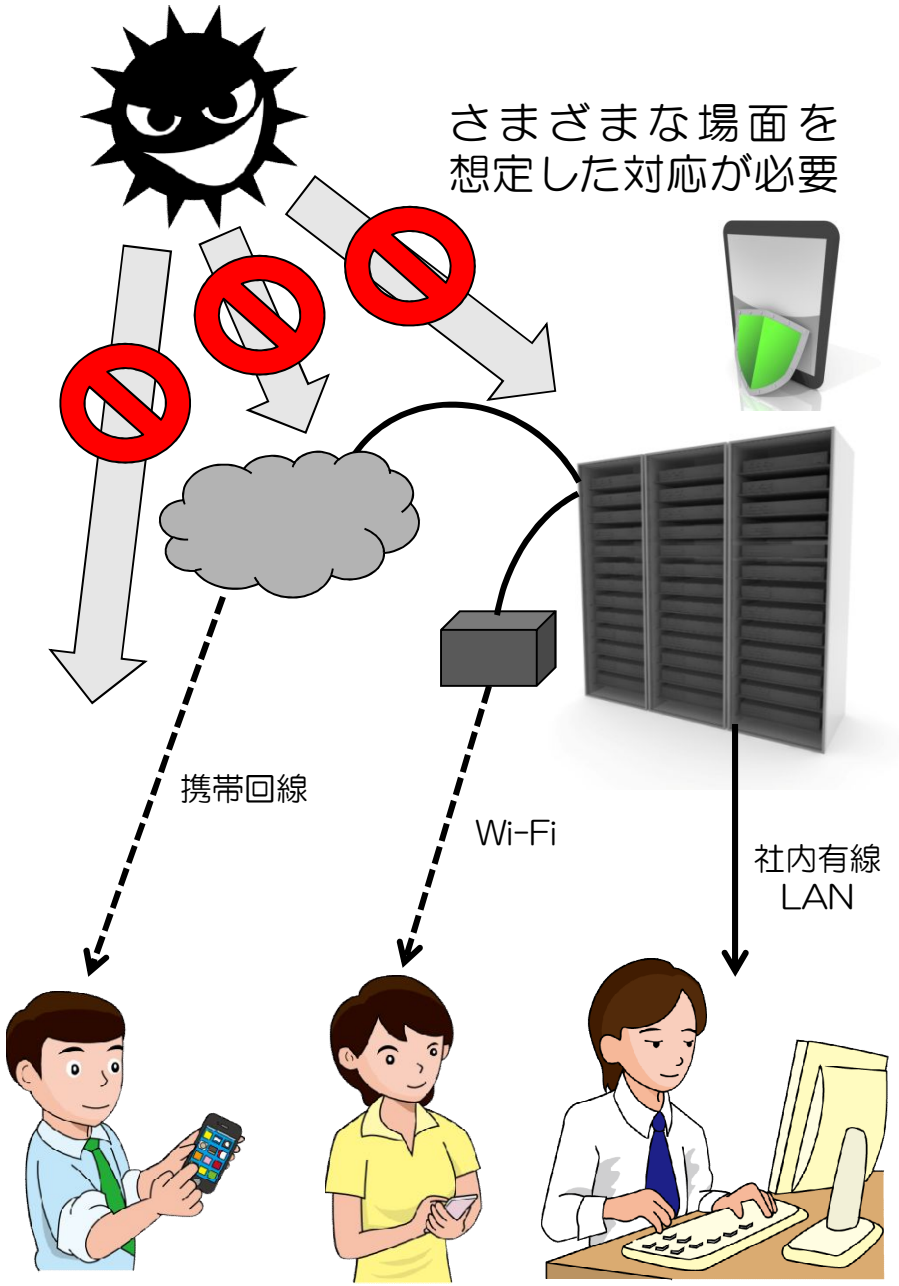
また、これらの管理を円滑に進めるためにも、これまでとは違った方法が必要になります。以下に課題と管理手法を列挙します。（具体的な説明は「4. MDM 」を参照ください）

・全体的な機器・情報管理　⇒　MDM
・盗難・紛失時の対応　⇒　iCloudなどベンダーの基本サービス、またはMDM
・デバイスへのアプリ配布・管理　⇒　MDM

⑶セキュリティー対策の強化

セキュリティーも同様に「常に社外へ持ち出されている」、「会社のネットワーク以外で接続されている」ことを念頭に、対策を実施する必要があります。

セキュリテイーポリシーの一斉配布なども、漏れなく実施するための仕掛けを組み込んでおく必要があります。（具体的な説明は、「3. スマートデバイス導入に伴うセキュリティー対策」を参照ください）



7. BYOD導入のメリットと課題

7.1 BYODとは？

BYODとは、Bring Your Own Device の略称で、スマートフォンなど個人所有のデバイスを会社に持ち込み、それを業務に使用したり、会社以外の場所から業務システムにアクセスできるようにすることを意味することばです。

BYODへの動きは、数年前から米国を中心に海外で盛んになってきており、日本でも導入する企業が出始めています。こうした動きの背景として、どこでもネットワークに接続できて高機能な、タブレットやスマートフォンの普及、デバイスの種類を問わずに利用できるクラウド型サービスの普及などが挙げられます。

しかし、導入についてはBYOD導入のメリットだけでなく、課題と対応策をあわせて検討する必要があります。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

BYOD = 個人所有のデバイスを業務に利用

© 一般社団法人 日本コンピュータシステム販売店協会 2013

7.2 BYOD導入のメリット

BYOD導入のメリットとしては以下のような項目が挙げられます。

①いつでも、どこでも業務ができ時間の有効活用ができます。

②個人で自由にデバイスを選べるため、自分にあったデバイスを使え生産性が向上します。

③時間や場所を問わないためBCP（Business Continuity Plan）対策となります。

④業務用デバイスと個人デバイスを両方持ち歩く必要が無くなります。

⑤企業は、業務用デバイスの導入に関する機器購入 / 保守費用の削減が可能となります。

© 一般社団法人 日本コンピュータシステム販売店協会 2013

© 一般社団法人 日本コンピュータシステム販売店協会 2013

7.3 BYOD導入の課題と対策

BYOD導入に際しては、私物のデバイスを業務利用するためのセキュリティー上 / システム上の懸念があり、下記の様な課題と対策が挙げられます。

(1) デバイスの盗難、紛失などによる情報漏えいなどのセキュリティー事故の対策が必要

「3. スマートデバイス導入に伴うセキュリティー対策」で記載したセキュリティー対策や、「4. MDM」で記載したMDMサービスを利用し、情報漏えいのリスクを回避します。

(2) プライベートとビジネスの切り分けが必要

特に通話料の精算では、通話記録を基に業務用通話を会社に請求する方法が一般的ですが、これでは請求の事務処理や経理処理に手間がかかり過ぎてしまいます。解決策の例として、NTTコミュニケーションズが提供する「0035ビジネスモード*」の利用があります。このサービスは「0035+43+相手先電話番号」で発信した通話料をあらかじめ契約している会社側に請求できるというものです。

---

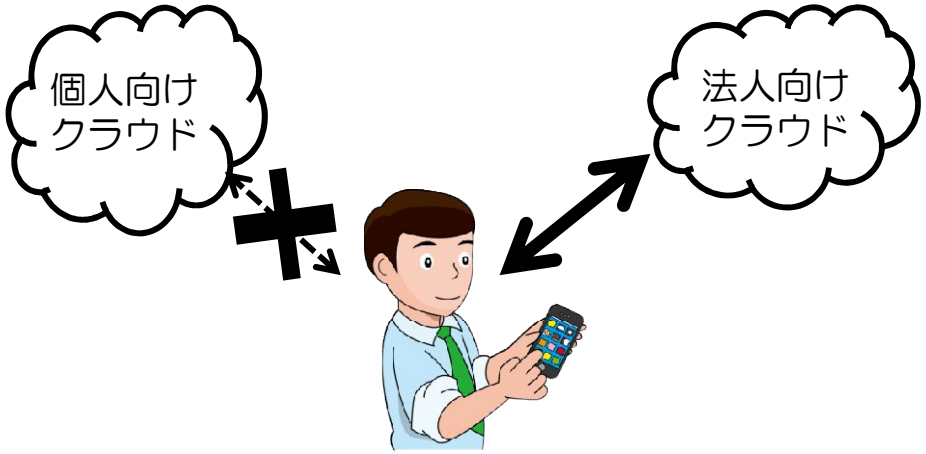
*: サービス内容や契約条件は以下を参照ください。
http://www.ntt.com/0035bm/

(3) 業務データなどのアクセス管理が複雑になり、コストアップの可能性

社内に設置する、無線LANコントローラと管理サーバーを組み合わせ、ユーザー、デバイス・アプリケーションの種類など総合的な情報からアクセスを制御するシステムを導入し、設備・管理コストを削減することも可能です。

また、私物のスマートフォンやタブレットで個人向けクラウドサービスを業務利用することで生産性が向上する一方、利用基準が明確になっていないことでリスクが隠れてしまう課題があります。

リスクを低減するためには、個人向けクラウドと同等の機能を持った法人向けクラウドの利用や、業務利用に対するルール整備が必要となります。



8. 今後の発展の予測

これまでスマートデバイスやそれを取り巻く環境について解説をしてきました。それでは、これからこれらのスマートデバイスはどう使われるようになっていくのでしょうか。

通信各社は高速の無線回線であるLTEサービスを提供し始めており、これら通信の高速化により、使用者の利便性が増してきています。また、この通信回線の先にはインターネットが接続されており、業務として使用する時にはVPNを経由して会社のクラウドなどにアクセスすることが可能です。

さらに、最近では個人契約のクラウドを使用、スケジュールや業務データを転送して、会社の業務を行うケースもあると聞きます。

このように環境が整って来ている今、その可能性は無限にあり、どういう使い方をすればより便利になるか、またそれを利用して、いかに効率的に業務を遂行し、他社に先んじるか、ますますスピードとアイデアが求められる時代になってきています。

いつでも、どこでも、誰とでも、というユビキタスの時代で私たちのワークスタイルはどう変わっていくのでしょうか。

【ビジネスシーンでは】

出勤前に：スマートフォンから今日のスケジュールを確認。伝言は動画でチェック。天気予報・交通情報もチェックして家を出る。

出勤時：車通勤の場合は、カーナビにスマホを使用し、渋滞情報もリアルタイムに入手。電車通勤の場合は、運行状況、会社への到着予測時間なども確認可能。

会社では：パソコンで各種データ作り。作った資料はクラウド上に保管。これでいつでもどこでも、どのデバイスからでも参照できる。会議は自席のパソコンのWebカメラを通じて、また、外出先のスマートフォンからも参加可能。

外出先では：資料はどこからでもクラウドを介して参照可能。必要に応じて客先にも提示できる。作業がある場合には、動画で作業手順などを表示。作業報告をデバイスから入力し、その日の勤務は終了、次の日のスケジュールを確認し、自宅に直接帰宅。自己啓発のための雑誌や書籍もすべてスマートデバイスにダウンロードして勉強できる。

もちろん、これらの通信を支えるセキュリティーやMDMの機能は、ますます充実していくでしょう。

【ライフスタイルの中では】

・学校の教科書がタブレットから参照可能となり重い教科書の持ち運びが不要に。

・大学のカリキュラムを自宅で受講できる。

・図書館での書籍の貸し出しも電子化され、タブレットにダウンロード。

・セミナーの講演内容や美術館での音声説明や文字表示にタブレットを利用。（聞き取りが不自由な方にも対応）

・国民のIDの一元化（年金、保険証、納税、医療履歴、パスポートなど）が進みいつでもどこでも国民サービスを受けられるようになる。

・自動車や家電のセンサーの情報の通信で各種制御や情報の取得が可能になる。

・高齢者への医療相談、買物代行、緊急通報サービスをタブレットで実現。

・観光地や動物園、ペットの情報の監視や配信をタブレットで。またGPSの活用で近辺のお店の情報をタイムリーに配信。

・すべての電気製品をスマートデバイスで操作

・書籍も全てデジタルデータ化し、どこででもタブレットで参照可能。

近い将来、これらのデバイスに慣れた高齢者の増加、また趣味でのアプリの作成により、無料アプリの増加や、スマートデバイスを用いたサービスが多く登場するかもしれません。

技術の発達により、紙のように薄く、折り曲げられる材質のディスプレイにより、見た目はこれまでのままで、中身は自在に変化できるデバイスの登場もあるでしょう。

スマートデバイス時代に移行するにつれて、我々が、望むと望まないにかかわらずインフラを含む環境が急速に変化・発展していきます。それらをいかに先取りしてビジネスに生かしていくか、企業の皆様の先見性やアイデアやセンスが試される時代になってきているようです。

あとがき

今年度は、個人中心に広まっているスマートデバイスをITシステムに取り込む動きについて調査しました。

この解説書をまとめていく過程で、クラウドサービスとは、スマートデバイスをはじめ、仮想化、セキュリティー、高速無線LANなど、さまざまなテクノロジと新しいアプリケーションを組み合わせた総合的なサービスであることを実感しました。

スマートデバイスに代表されるように、テクノロジーは、これからも進歩し、さまざまな新しいアプリケーションが開発されていくでしょう。これまで「クラウドサービスはなかなかビジネスにならない」と良く耳にしてきましたが、これからは、クラウドビジネスが大きく広がっていくと期待して良いのではないでしょうか。

ITサービスの提供側としてのメーカや販売店は、これらのテクノロジーを組み合わせて提供していくと共に、これらをいかに易しくお客様に伝え、理解して使っていただき、お客様のビジネスの効率化や拡大に貢献できるか、ということを考えていかなければならない時代になってきていると思います。

サポートサービス委員会事務局

© 一般社団法人 日本コンピュータシステム販売店協会 2013

© 一般社団法人 日本コンピュータシステム販売店協会 2013

本書は下記の方々のご協力により作成しました。

	氏名	所属
リーダ	太刀川　浩	株式会社富士通エフサス
サブリーダ	森　　恭志	株式会社富士通エフサス
	根津　史明	株式会社システナ
	藤井　宏幸	株式会社システナ
	小林　香澄	ＮＥＣフィールディング株式会社
サブリーダ	松田　利昭	東芝情報株式会社
	木村　茎太	トレンドマイクロ株式会社
	黒木　直樹	トレンドマイクロ株式会社
	廣瀬　勝雄	日本事務器株式会社
	伴野　浩之	日本事務器株式会社
サブリーダ	仲西　隆三	株式会社シーシーダブル
	芳賀　明夫	株式会社大塚商会
	地神　明寛	株式会社ブロードリーフ
	大島　章宏	日興通信株式会社
	市川　　茂	リコーテクノシステムズ株式会社
	岩崎　　透	
	佐藤　昭博	
事務局	加藤　　誠	日本コンピュータシステム販売店協会

ー禁無断転載ー

スマートデバイスに関する疑問 一挙解決

発行 一般社団法人 日本コンピュータシステム販売店協会
東京都文京区湯島１－９－４　鴨原ビル２階
電話　03-5802-3198
ホームページ　http://www.jcssa.or.jp
発行日　平成２５年１月（初版）

© 一般社団法人 日本コンピュータシステム販売店協会 2013

JCSSA

© 一般社団法人 日本コンピュータシステム販売店協会 2013