BYOD(Bring Your Own Device)について

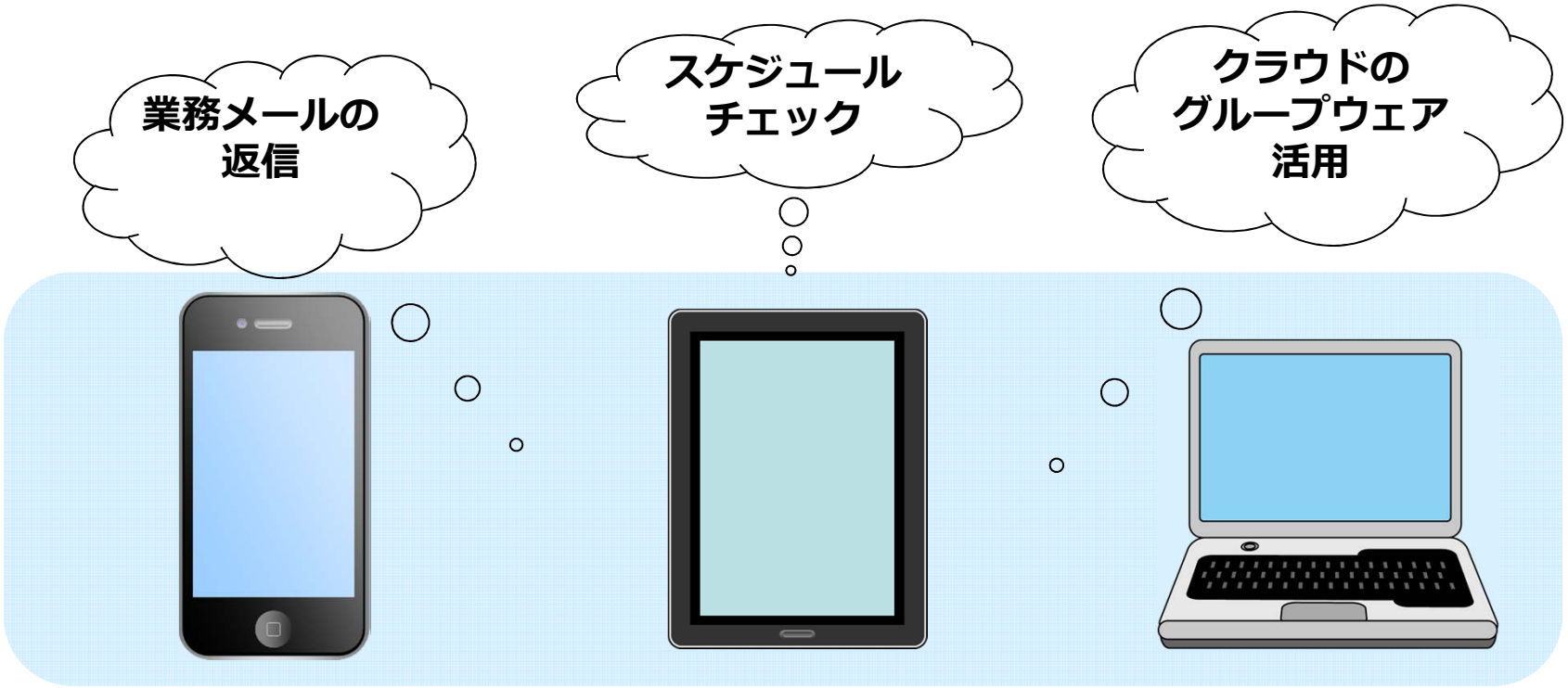
2013月6月

株式会社アイ・シー・アイ

Internet &
Communication
Innovator

BYOD(Bring Your Own Device)とは？

私物の端末(PC,スマートフォン,タブレット端末)を業務で活用ことを指します。



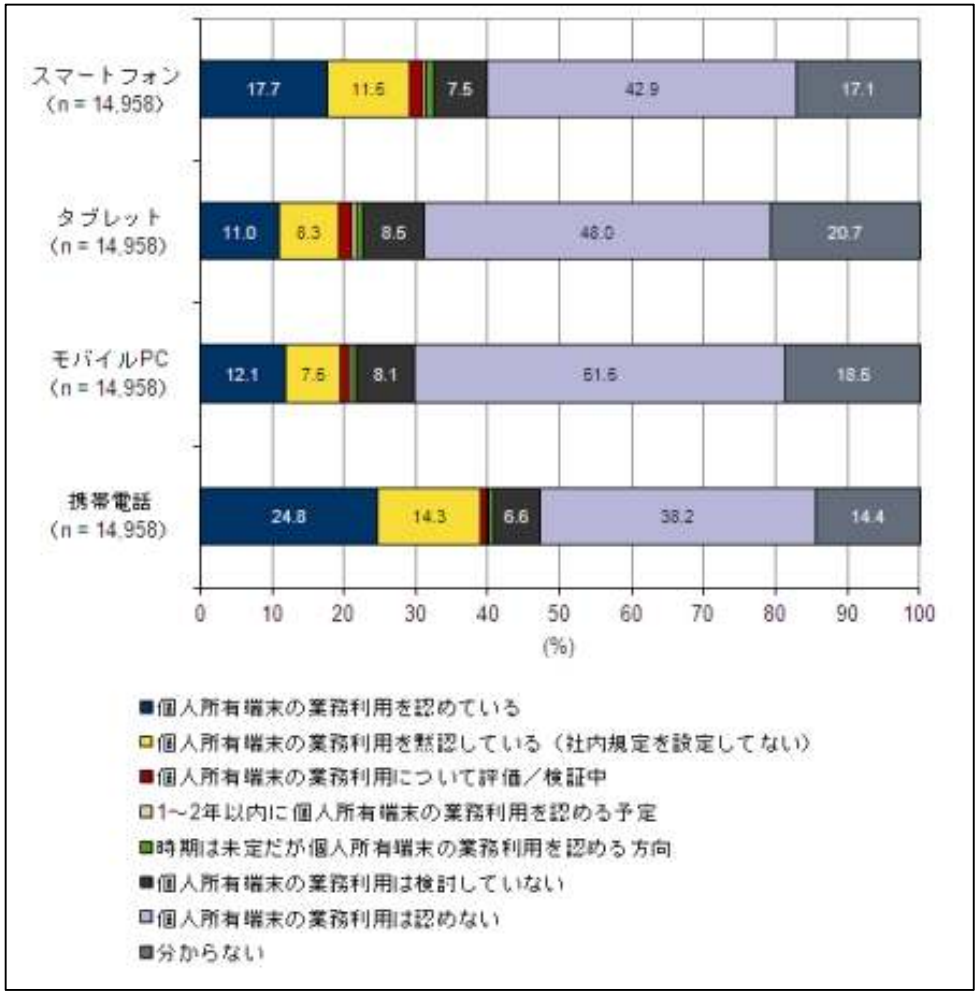
BYODによって、

- 仕事が、**いつでもどこでも**できる！！
- 普段から使い慣れている端末を使うことで、**生産性UP**！！
- 企業は、端末導入に関する**労力や経費を抑えられる**！！

大いに魅力的な面もありますが、、、、

もし、取引先や顧客情報が入った**端末を紛失したら**、**ウイルスが侵入したら**、、、。

BYODの現状



モバイルデバイス別BYOD利用状況（出典：IDC Japan)

日本でのBYOD普及率は、
約30%~50%と言われており、
今後は増加する見込みとなっています。
左図は、企業のBYODに対する利用状況を示したものです。

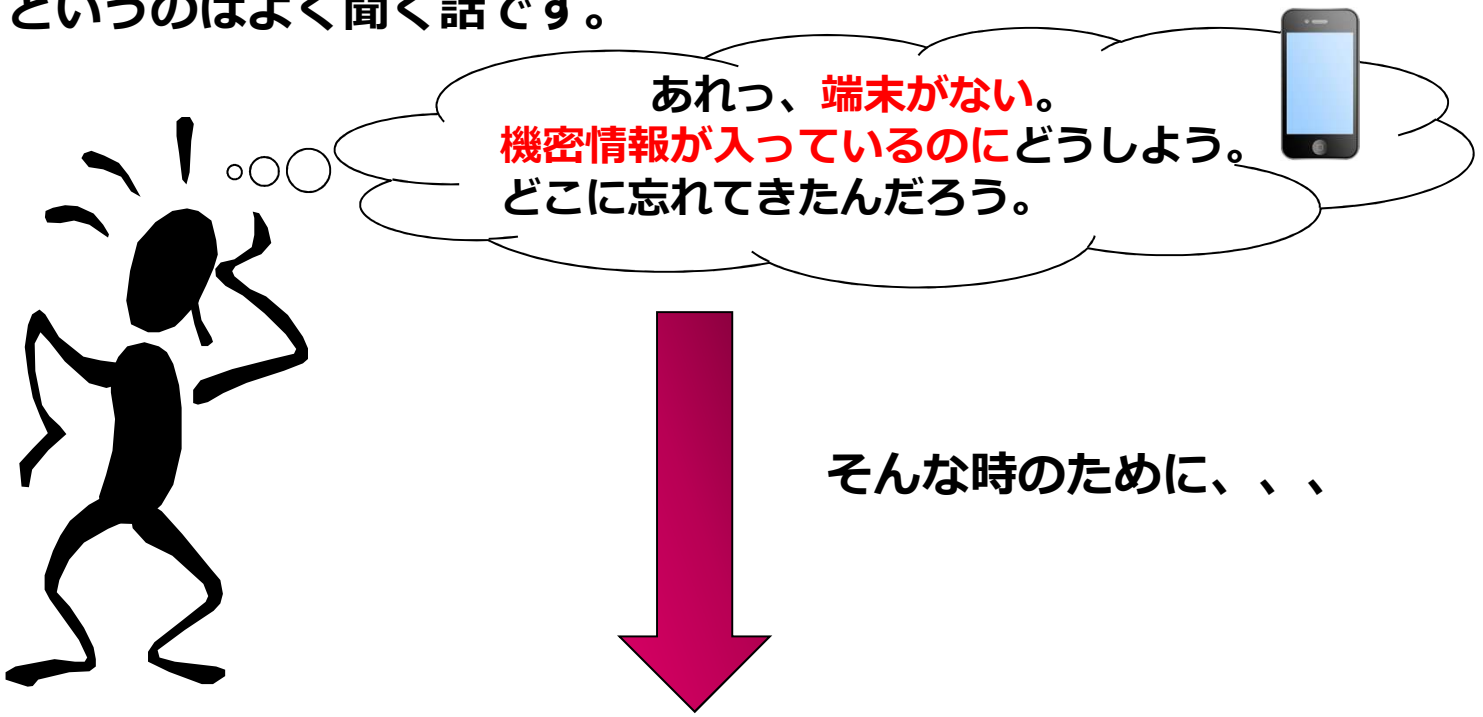
「業務利用を認めない」
が各項目で最高値となっています。
また、「黙認」,「分からない」
を合わせると約30%と高い数値になっています。

企業側も従業員側も、統一されたポリシーのないまま利用しているケースが多そうです。

BYODのリスク

BYODで1番問題になるのは、情報漏えいのリスク・セキュリティです。

携帯電話をはじめ、モバイル端末をどこかに置き忘れたり、紛失したり、というのはよく聞く話です。



そんな時のために、、、

すぐに対応が取れる環境を整えましょう！
今回は3つの対策法をご紹介します。

BYOD セキュリティ対策

- パスワードロック・・・端末自体にパスワードロックをかけましょう。これは、端末をBYODで使用する際の、最低限のマナーと言えます。

- リモートワイプ機能・・・紛失した端末に入っているデータを、遠隔地から消去できる機能です。あらかじめ、端末にリモートワイプ機能の設定をしたり、すぐに事業者に連絡を取ることで、データの消去ができます。
  ※ただし、端末の電源が入っていない場合、圏外の場合は、使用できません。

- MDM(Mobile Device Management)・・・端末データのバックアップ・特定アプリケーションの禁止・ネットワークアクセスの制御・リモートワイプ・ウイルス対策、、、等々、モバイル端末管理に最適なものがまとまっている、ソフトウェアのことです。従業員の私物端末と言えど、企業がMDMで端末管理するのも、強力なセキュリティ対策になります。

最後に

スマートフォンやタブレットデバイスが急速に普及している中、
BYODの在り方は、非常に注目されています。
2016年には,現在の約10倍近くの人がBYODになると予測されています。
{モバイルデバイス別BYOD利用状況（出典：IDC Japan)}

いつでもどこでも・生産性UP・端末導入コスト/労力カット、といった利点を活かし、
セキュリティ対策等の、運用ポリシーを持つことが重要だと言えます。
私物と言えど、社会的責任をもって使用していることを意識を心がけましょう！！