BYOD(Bring Your Own Device
(自分のデバイスを持ち込む)

■メリット

・従業員が自分の使い慣れた端末で情報管理を一本化できるため、業務効率の向上に結びつく

・この環境を自宅や出張時に活用することで、使い勝手の良い在宅・遠隔勤務環境を構築できる

・企業が従業員に端末を支給せずに済むため、コスト削減につながる

■従来の懸念点

・セキュリティ上の懸念

・企業の機密情報を入れたスマートフォンやタブレット端末を落としたり盗まれたりして情報漏洩を引き起こす

■懸念点の解決策

◯セキュリティ上の懸念

私物端末を企業内でも安全に、かつ利便性を失わせない形で利用可能にするツールの登場

例）BYOD環境の構築を支援する機能を備えた無線LANシステム

米シスコと米アルバネットワークスがそれぞれ無線LANコントローラーと管理サーバーをセットにして提供

※ユーザー、端末の種類、アプリケーションの種類、場所などの総合的な情報をポリシーと照らし合わせ、適切なアクセス制御を実施する。

◯情報漏洩を引き起こす

リモートから端末の情報を削除したり端末にロックをかけたりできる「MDM」（Mobile Device Management）と呼ぶツール/サービスが有効

支援環境

■MDM(モバイルデバイス管理ツール)
◯代表的な機能
・遠隔ロック
・データ消去(ワイプ)
・位置や使用状況の監視
・セキュリティポリシーの適用
　アプリケーションの利用、インストールの可否
　カメラ等デバイスの機能制御
・アプリケーションの配布
◯タイプ
デバイス側にエージェントソフトをインストールする「エージェント型」と
デバイスの基本機能を利用して、インストールしない「エージェントレス型」がある
◯製品例
・Symantec Mobile Management
・Apple Conviguration(無料)

支援環境

■ネットワーク

◯代表的な機能

・アクセス制限

制限例）

・ゲストが社内に持ち込んだスマートフォンやタブレットにはインターネットへの接続のみを許可

・従業員の私物デバイスでユーザーが認証されたものにはグループウエアサーバーへのアクセスを許可

・会社支給のデバイスにはファイルサーバーや業務アプリケーションのサーバーへのアクセスを許可

■仮想化

◇デスクトップ仮想化

・XenDesktopによる仮想デスクトップ

◇ActiveDirectoryの移動ユーザープロファイル

導入事例

●アジア航測

・半期に1度のチェックリストによる私有端末のチェックは、ルール順守を確認する棚卸しの意味がある。ユーザーへの注意喚起にも役立つ

・MDMは紛失・盗難時の備えのほか、セキュリティ監査の証跡として使うこともできる

●インテル

・同社では、BYODポリシーに関する誓約書として、エンドユーザーライセンス契約（EULA）に同意させる。これは同社の人事と法務が協力して作成したもの。新規に作ったポリシーではなく、従業員を雇用する際に使っている雇用契約条件の中からBYODに関連する項目を抜き出したものだ。会社からの強制ではなくユーザーの自発的な意思に基づくことを確認する意味がある。

・BYODの効果を定量的に測ったところ、1日当たり約1時間分の生産性向上が見られた

・端末のプラットフォームごとに標準のセキュリティ機能が異なるので、それぞれに合わせた対策が必要となる

●エス・アンド・アイ

・スマートフォンの通信料を個人と会社で折半

・BYODの促進には、ユーザーにメリットが出るような施策が重要

・紛失に最初に気付くのはユーザー自身なので、早期の対処にはセルフ・リモートワイプが効果的

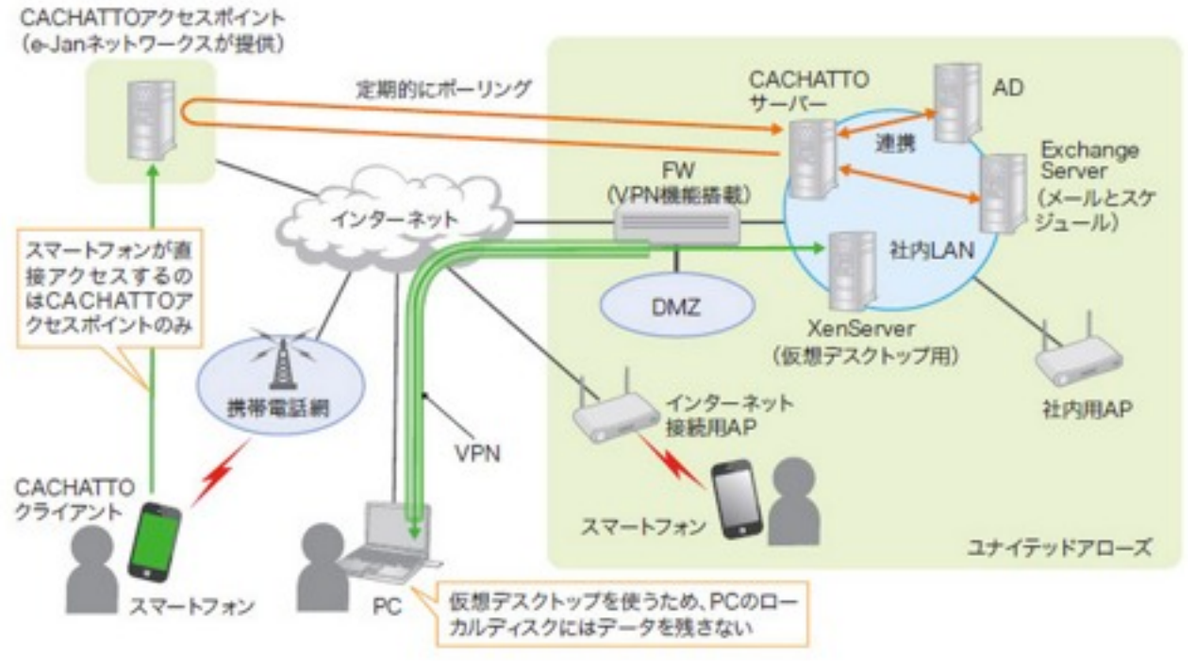
●ユナイテッドアローズ

・私有端末には、スマートフォンであれPCであれ、データを残さない

・データを残す場合は、会社支給端末にする

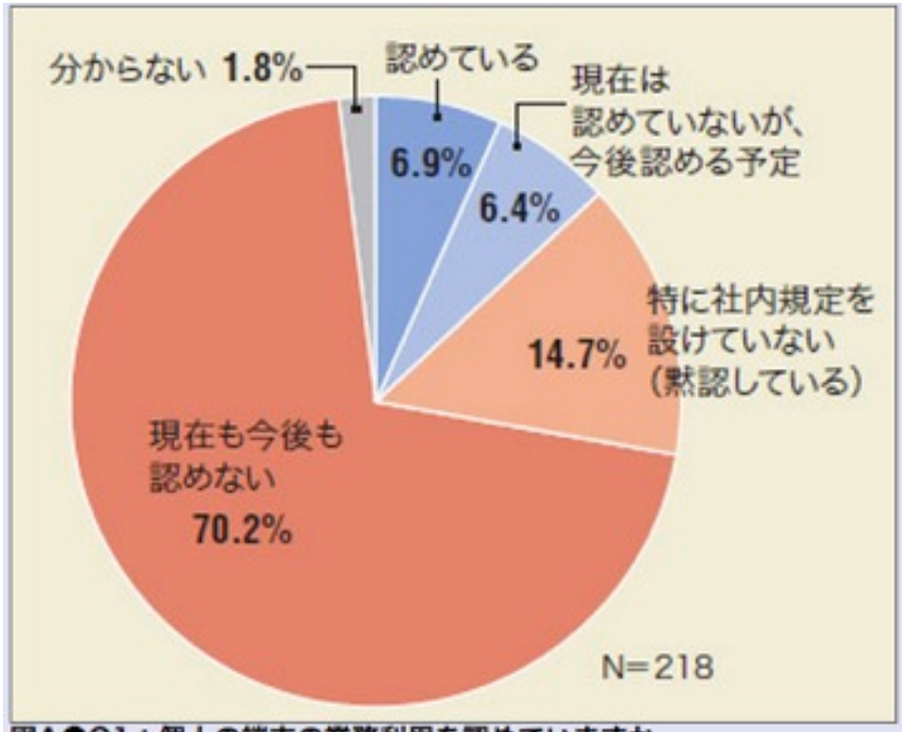
・私有端末から情報漏洩するリスクはないので、MDMで管理しない

図2-5●ユナイテッドアローズのBYOD向けネットワーク構成



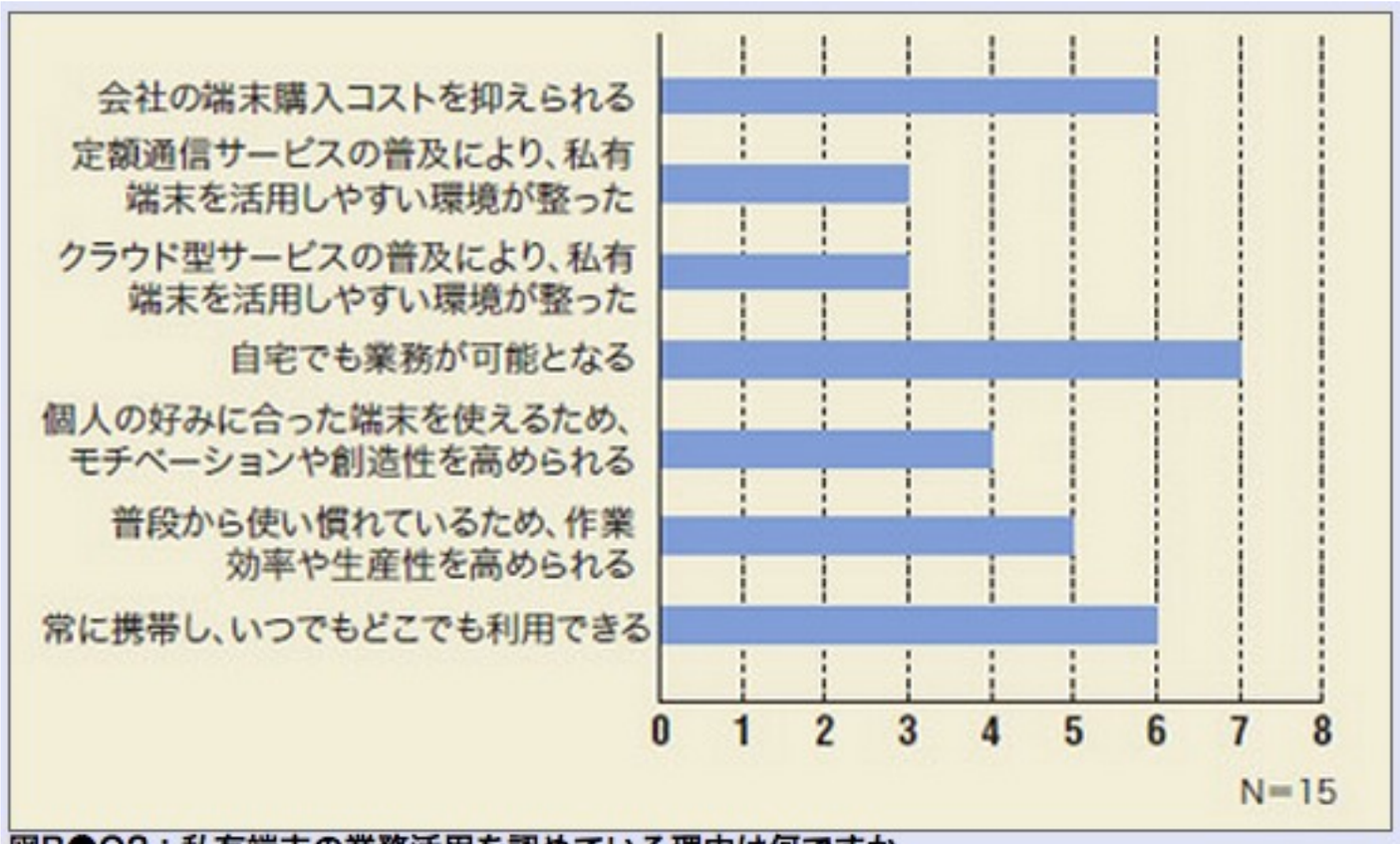
日経コミュニケーション読者アンケート

実施期間：2012年3月14日～22日　回答企業数：405社中218社(53.8%)



図A●Q1：個人の端末の業務利用を認めていますか

http://itpro.nikkeibp.co.jp/article/COLUMN/20120710/408238/?ST=byod&P=3



図B●Q2：私有端末の業務活用を認めている理由は何ですか

（Q1で認めていると回答した企業が対象、複数回答）

肯定的（肯定しながらも課題を認識）	否定的
BYODに取り組まなくてはならないという認識はあるものの、その課題に情報システム部門が向き合うのはそれほど簡単なことではない。先進的な気性のある人のモチベーションを保ちつつ、他の従業員にも均等に機会を与えなければ平等性を欠いてしまうし、管理コストも増大する。何よりもミッションとして情報システム部門にマンパワーが不足しているのが現状だ	私物の端末を業務に使う行為を許す時点で、管理側の責任が飛躍的に大きくなる。今の枯れてないMDM製品群でセキュリティリスクをどこまでカバーしきれるのか疑問である。疑問である以上、導入は見送らざるを得ない状況である
BYODは、リモートアクセスのみで端末にデータが残らないものに限定して許可している。リモートワイプだけではデータを間違いなく消せたかどうか確認できず、満足のいく漏洩対策にならない	社員のセキュリティ意識が高い企業ではBYODの導入が可能だと思うが、当社ではまだその域に達していないと考えている
ある程度のセキュリティを保った状態で、私物機器の導入を進め、必要性や数が増えた段階で、会社支給に切り替える方針。導入に当たっては、管理規定を定め、定期的に棚卸し、要件を満たしたものだけ導入を許可している	ITインフラを一定レベルに維持することが困難になり、個人機器の機能によってデータ互換性が取れなくなることを危惧している。安全対策上も個人機器の持ち込みはマイナス要素を感じており、現時点では有効に機能するとは考えていない
スマートフォンやクラウドを利用して業務の効率化を図れる可能性は否めない。今後どのようにポリシーを定めていくか悩ましい	MDMで利用制限をかけたいが、規制すると私物として使うときも利用できなくなってしまう
タブレットやスマートフォンでの業務利用ニーズは高まりつつあり、BYODについては実施すべきと考える。ただ、会社規定・方針に縛られて実施が困難なうえ、経営へのリスク説明や理解を得ることも難しい	過去には一部例外を認めていたが、余計な管理が必要になったり、セキュリティに注意しなければならなかったりと、システム部門の負担だけが増えることになったので、現在は一切認めていない
メールチェックやスケジュール管理ということであれば非常に有効だと思われるが、利用範囲の制限などIT部門で対応できる余力がないため、安全性を考えて利用不可としている。先進的な一部のユーザーは利用しているかもしれないが、それに対応できない状況である	企業活動で私有端末を利用することは、セキュリティや資産管理の観点からはおかしいと思っている。しかし、各自がプライベートで使用するのに最新の機器を保有しており、会社資産の機器と私有機器との差が顕著になってきたため、社員の不満が聞こえてくることが多くなってきた
企業情報を守る、コストを抑える、個人の利便性を高める――のバランスをみて、BYODの活用を考えることとなる。これまでは、個人IDでのみアクセス管理してきたが、それだけではアクセス管理ができない。デバイスのプロファイリングなどが必要となるが、それほどたやすくない	規定のみによる規制は社員のモラルに依存しているため、物理的な制限が施されていなければ実質無法地帯と同様だと感じる。会社貸与に費用がかけられないのであれば、私有端末手当のようなインセンティブと引き換えに安全対策を徹底させるなどの施策が効果的ではないだろうか
現在は認めていないし、認める具体的な検討もしていない。しかし、私有端末を認めないと言い切ってしまってよいのか最近疑問を感じている。昨年の東日本大震災を経験し、BCPやスマートフォン/タブレットの利用拡大などの観点から、一律に「ダメ」ではなく、なぜだめかを明確にして解決策を導き出せばよいと考えるようになった	個人的には私有端末を認めたい。しかし、業務利用と個人利用との区別がつきにくくなると思う。性善説に立ちたいのだが、社員が多いと目が届かないのも事実。必要なものは会社で用意しておくのが本来の姿なので、私有端末を認めることはないと考えている
今後の業務遂行の利便性や時代の流れを考えるとBYODは認めていかざるを得ないと考える。セキュリティ技術が進化して、安全に利用できる環境ができるようになる	今まで企業は、パソコンも携帯電話も社用と私用を切り離して物事を考えていた。なぜ「BYOD」という新しい言葉を作ってまで私有端末の業務利用を考えるのか理由が分からない
仕事の道具としてとらえるのなら、自由に使ってもらっても構わないと考える。守る必要のあるデータ、情報を守れれば問題ない	BYODについては否定的。業務に必要なインフラや端末は会社側の責任として準備すべき
社内ネットワークに直接接続しないと利用できないようなシステムではBYODを許可しないが、グループウエアやメール、SFA（営業支援ツール）など、社内にシステムを保持する必要のないものは社外サービスを活用し、BYODで利用可能とするなどの使い分けを考えており、その方向で進んでいる	私有端末はスマートフォンに代表されるが、昨今Androidを対象としたスパイウエアやウイルスが広がっており危険度が高くなっている。にもかかわらず、ユーザーの認識が依然低いままであるため、危険度はPCの比ではない
社有端末を与えても償却の関係からすぐに買い替えられず、私有端末のほうが高性能である場合がほとんどなので、ある程度運用ポリシーを決めて利用しているのが実情だ	私有端末の存在は情報漏洩対策を困難にするので現状の方向性に合致しない。また、端末の購入選定がバラバラだとトラブル発生時にシステム部門がサポートすることが困難になり、業務の継続性を損なうことになる