

【2015.11.06 ワークスタイル変革セミナー】

# ワークスタイル変革に対応した セキュリティ対策

株式会社アイ・ティ・アール



シニア・アナリスト 館野 真人

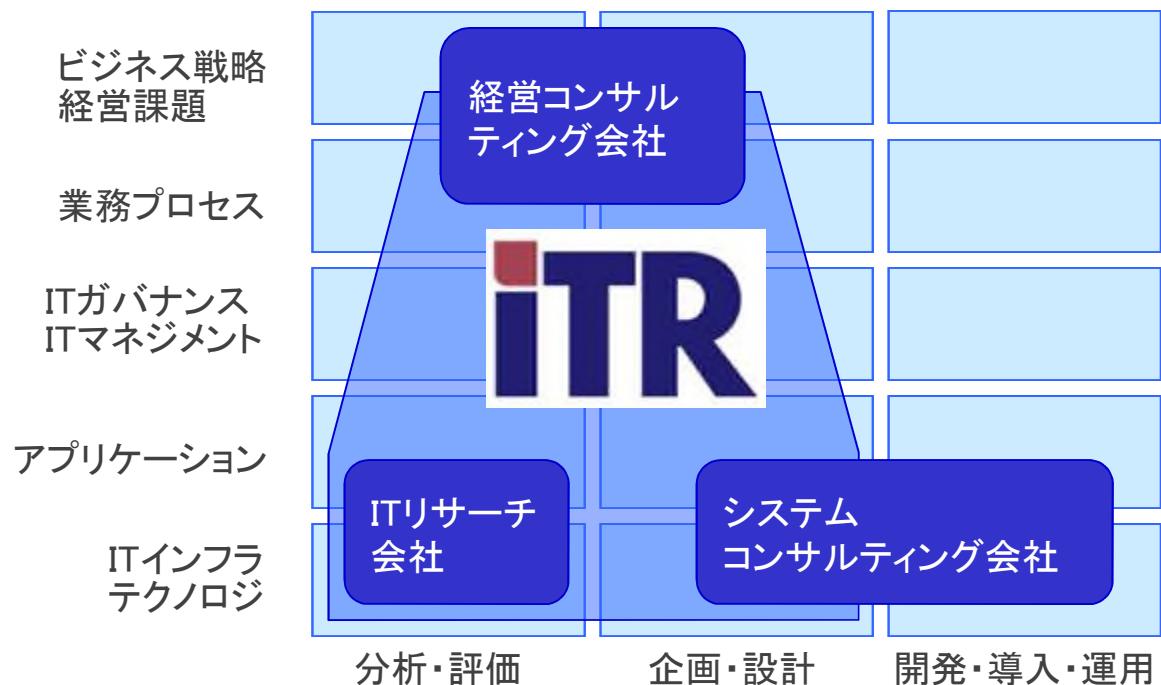
## 本日の論点

- ワークスタイル変革が求められる背景には何があるのか？
- ワークスタイル変革を促すための重点IT施策とは何か？
- 新しいワークスタイルに対応したセキュリティ対策のあり方はどのようなものか？

ビジネス環境や人口構成の変化などに伴い、柔軟な働き方を実現するための「ワークスタイル変革」が企業の経営戦略上重要なテーマとなっています。IT部門は、その目標を具現化するために、ITを活用した新しいワークスタイルと、不安を取り除くためのセキュリティ対策を同時に構想化する必要があります。本日は、最新の調査結果や技術動向に基づき、企業のIT関係者が着眼すべきポイントを整理してお伝えします。

# iTRのご紹介

iTRは、従来経営コンサルティング会社、システムコンサルティング会社及び、リサーチ会社が別個に行っていったサービスを連携し、業務プロセスと情報インフラの強い連携を実現するアドバイス及びコンサルティングを提供しています。



## iTRの特徴

- ・リサーチ事業を持ち、市場・技術動向を提供する一方で、実地のコンサルティングを行うことで具体的で実現可能な解決策を提示
- ・アドバイザリー事業を持ち、ユーザー事例の蓄積を持つ
- ・独立系調査会社であり、中立的・客観的な評価を提供
- ・常駐形式を採らないため、低予算でサービス提供が可能

## 主要テーマ

- ・経営課題と情報技術
- ・情報化投資と効果の最適化
- ・戦略的データ活用
- ・基幹業務システム再構築
- ・ベンダー／製品の評価・選定
- ・情報技術の将来動向

# 自己紹介



館野 真人 Masato Tateno

## シニア・アナリスト

### <専門分野>

- IT投資戦略、IT組織改革
- Future of Work
- コミュニケーション／コラボレーション
- ソーシャルメディア、モバイルデバイス
- 各種ユーザー企業調査 など

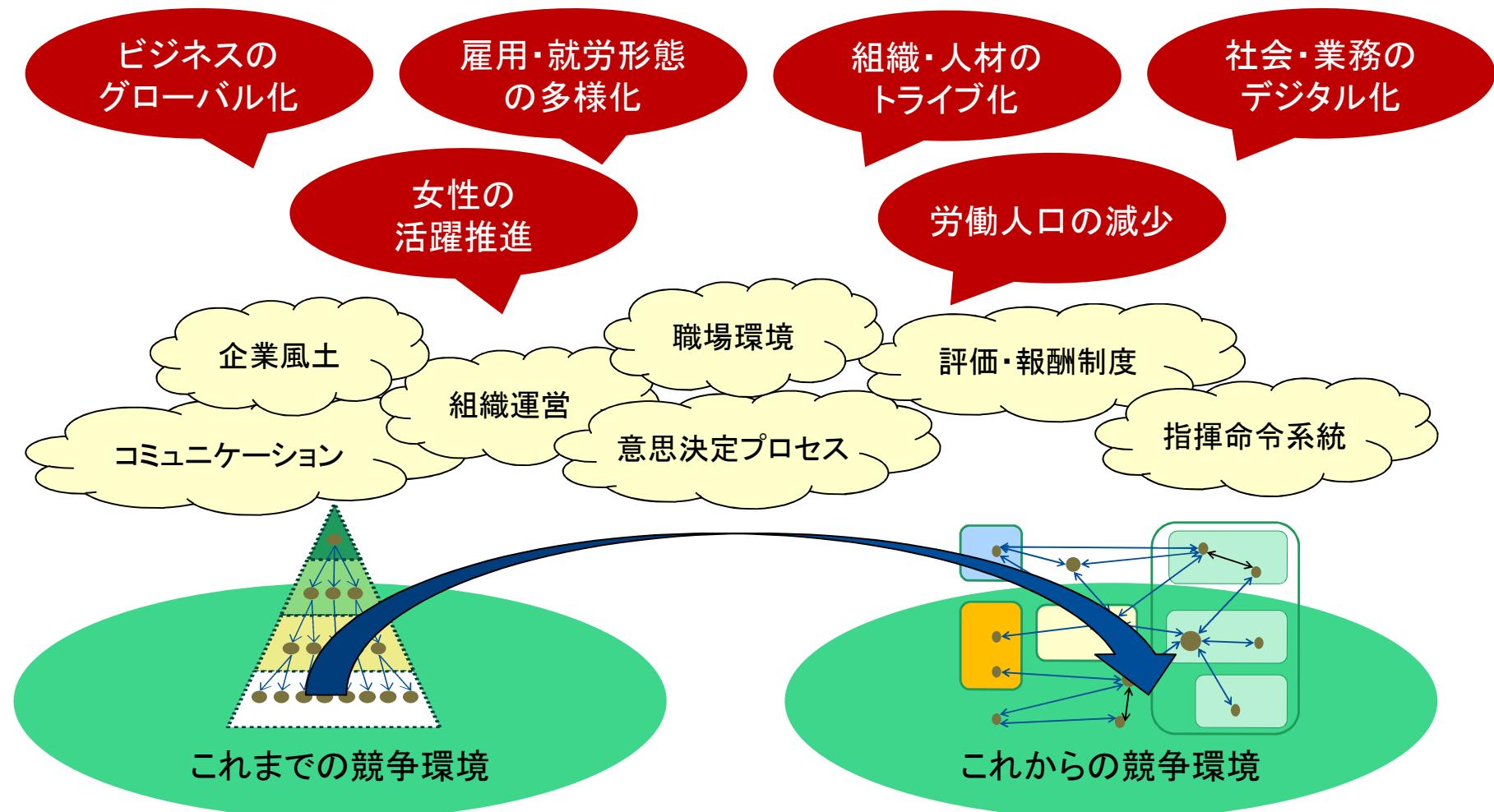
IDGジャパンにおいて「月刊CIO Magazine」の編集に携わり、企業のCIO・情報システム部門長を相手に、経営／IT戦略立案、システム導入プロジェクトにかかる取材・執筆を精力的に手がけ、2004～2008年には同誌編集長を務めた。2009年1月より現職。

現在は、IT投資戦略、IT組織改革、情報セキュリティ、ソーシャルメディア、スマートデバイスなどの分野を担当し、ユーザー企業のIT戦略策定や製品選定などの支援に取り組んでいる。また、ユーザー企業を対象とした各種調査も手がけている。

### ■最近の分析レポート

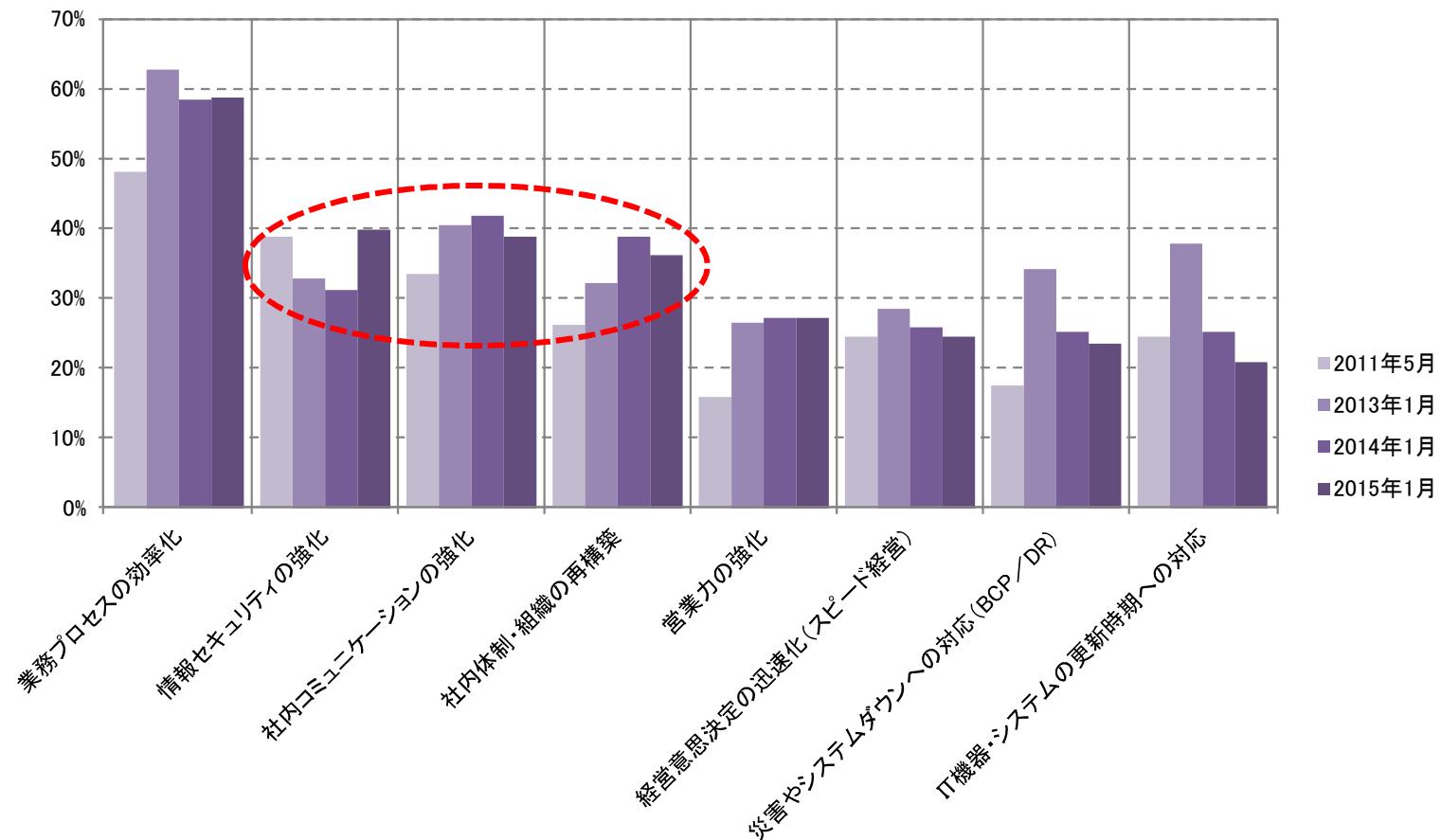
- デジタルワークプレース構想化の論点
- 本格化する管理の「モバイルファースト」— Windows 10登場で変わるPC／デバイス管理 —
- ソーシャル型の「流儀」を取り入れよ— 変化するコミュニケーション・プロトコル —
- オフィスワーカーが求める「機動性」とは
- ITR White Paper:「公立学校におけるタブレット教育のベスト・プラクティス」
- クラウド型セキュリティ・サービスの利用価値
- モバイル・ポリシー策定における要点 など

## 「ワークスタイル変革」が求められる背景



## 戦略上の重要施策

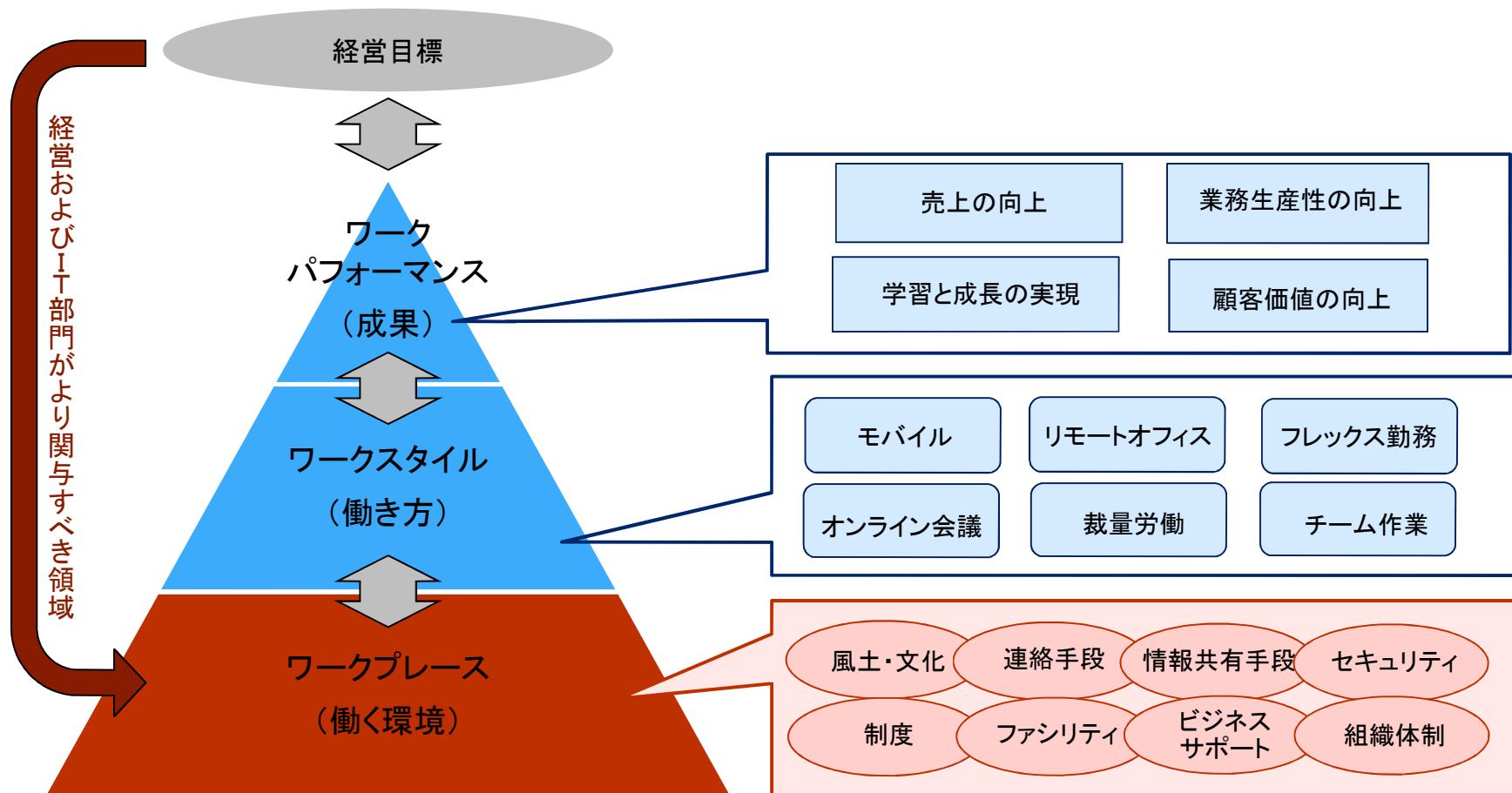
- 「社内コミュニケーションの強化」「社内体制・組織の再構築」といったワークスタイルに関わるテーマは、経営課題の面からも近年重視されている。
- 一方、「情報セキュリティの課題」も2015年調査では、重視する企業が大きく増加した。



出典: JIPDEC/iTR「企業IT利活用動向調査2015」

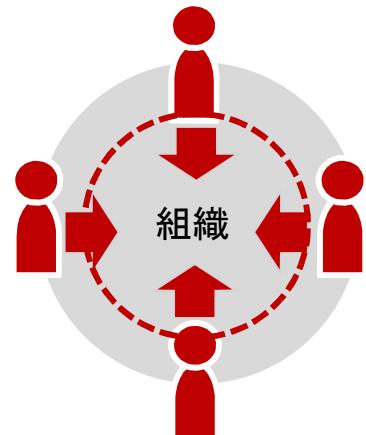
# 「ワークスタイル」の位置づけ

- しかし、ワークスタイルはあくまでも手段であり、最適な働き方は個人ごとに異なる。
- 経営およびIT部門が真に注力すべきテーマは、ワークスタイルを支える「ワークプレース」をデジタル技術によって成熟化することである。



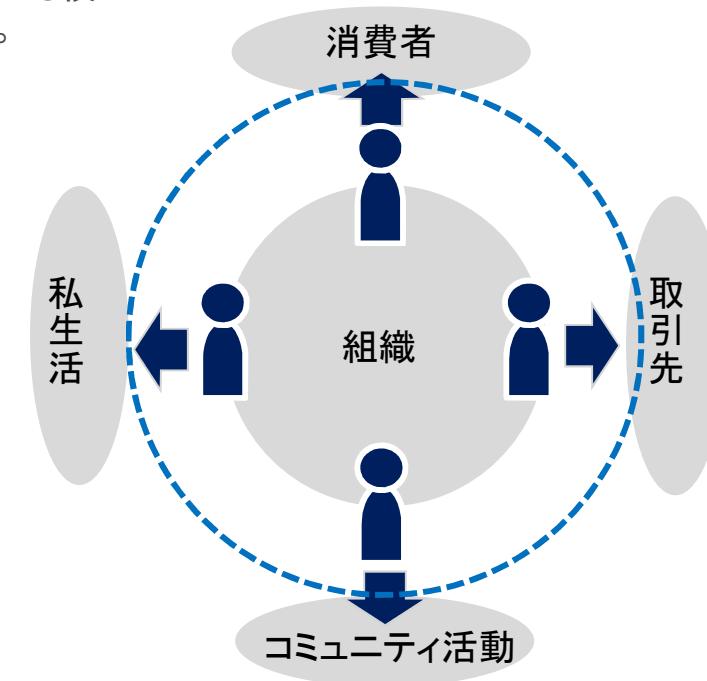
# 「求心力」と「遠心力」

- 経営目標が明確であった時代は「求心力」が重視されたが、消費者や従業員の価値観が多様化する中では、社外とも積極的に交わりながら組織運営を行うことが求められる。



求心力型組織

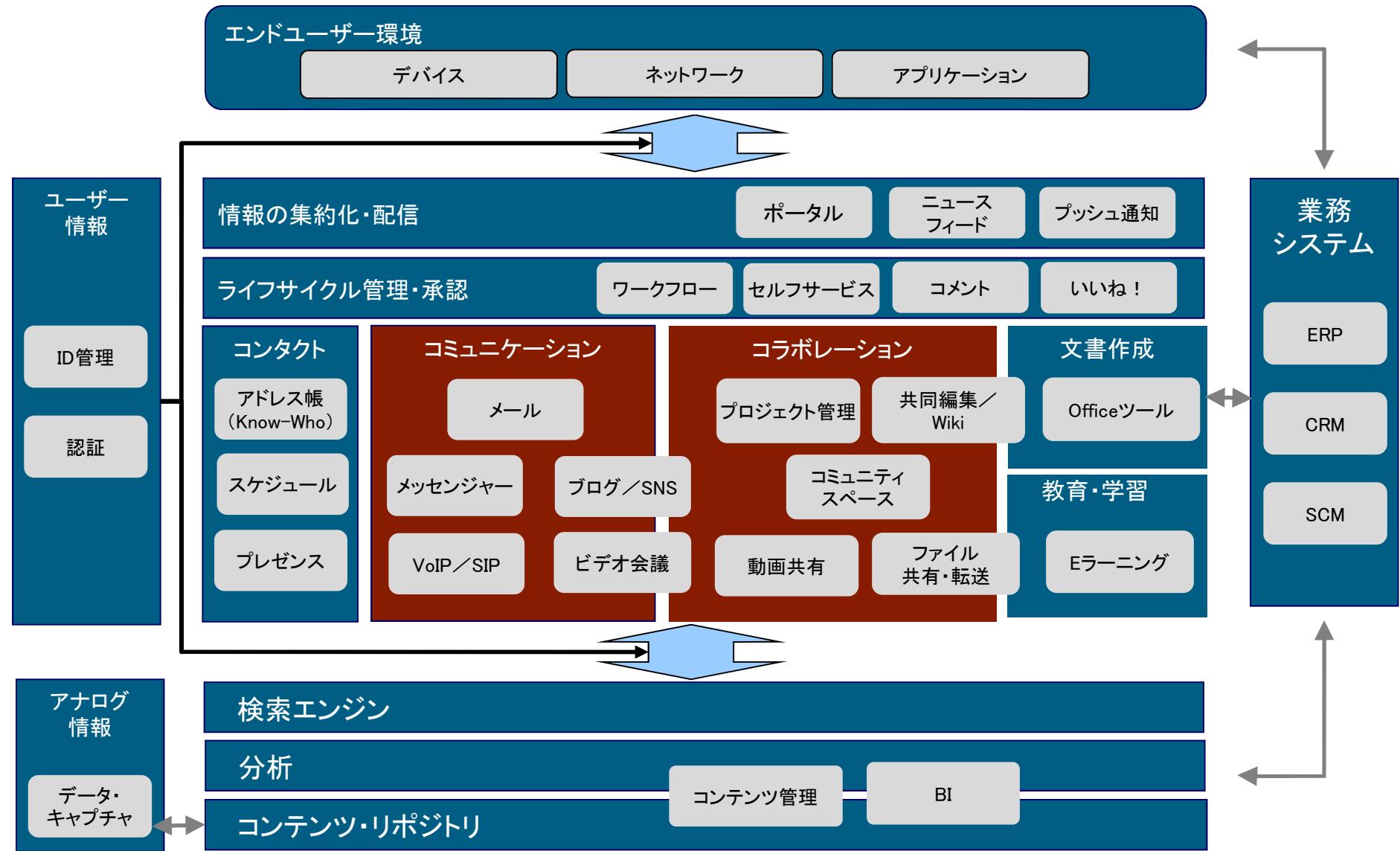
強固な団結力を持つが、  
広がりがない



遠心力型組織

個々の活動を通した  
広がりを重視

# デジタルワークプレースの主な技術要素



# ワークスタイル変革に向けて検討すべきIT施策

①コミュニケーション経路の多様化

②マルチデバイスへの対応

③コンテンツ管理の見直し

④テレワーク環境の整備

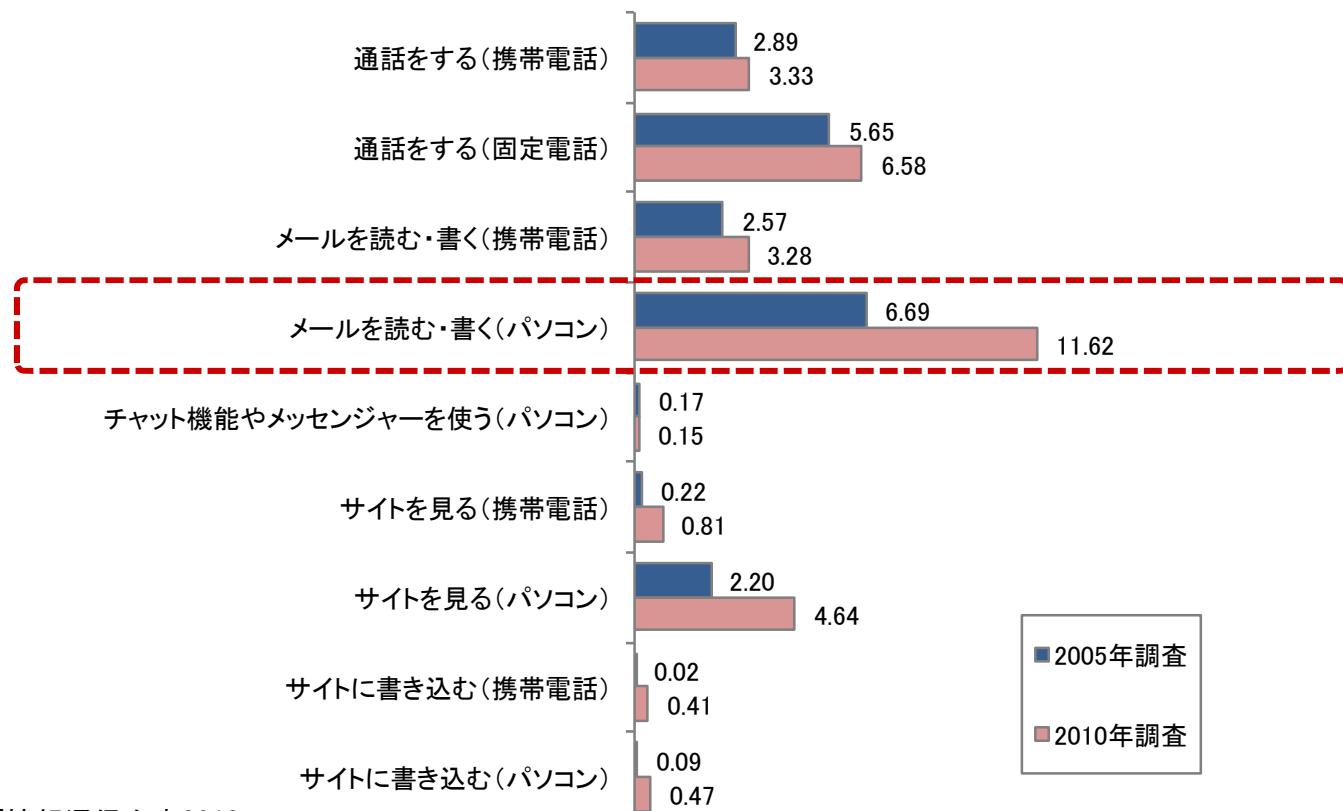
生産性向上

セキュリティ強化

## ①コミュニケーション経路の多様化 「メール依存」からの脱却

- メールを巡っては、処理量が増加の一途をたどっているという問題がある
- 総務省の統計によれば、企業の従業者が、仕事中にPCを利用してメールを読み書きする時間は、2005年から2010年にかけて実に2倍近くに増加している

仕事中におけるコミュニケーション・ツールの利用状況(単位は分／日)



出典：総務省「情報通信白書2012」

# ①コミュニケーション経路の多様化 標的型攻撃メールの脅威

**News & Trend**

**日本年金機構、標的型攻撃で年金情報流出**

社保庁時代からの情報共有方法があだに  
2015/06/04  
井上 英明=日経コンピュータ (筆者執筆記事一覧)

[記事一覧へ >>](#)

103 3 22 30 255 保存する

おすすめ 共有 ブックマーク Pocket ツイート

シェア

**日本などの銀行を狙い打ちする標的型攻撃メールが**

パロアルトネットワークスは8月25日、同社の提供するサイバービス「AutoFocus」で、8月20日までの直近2週間で西ヨーロッパとするRetefeを配信する電子メールが急増していることが検出された。Retefeとは、現在インターネット上で最大の金融組織を狙う標的型攻撃組織で、ZeusやCitadelといった他のマルウェアが世界中の銀行のウェブサイトで多く採用されているのに対し、Retefeは一貫して日本、スウェーデン、オランダなどヨーロッパの銀行を標的としている。

**Destination Countries**

最近のRetefeトロイの木馬の受信者を示すAutoFocus (Destination Countries=宛先の国)

攻撃用メールでは、標的とする国に合わせてさまざまな「注文」で、より重要視されるように日付のあるファイル名を使用。電子メールの場合は、近隣の家電量販店を名乗り、日本では、国内大手ECサイトを装ったメールのケースが確認されている。

日本年金機構は2015年6月1日、125万件の年金情報が流出したことを公表し、水島藤一郎理事長が謝罪した（写真）。企業や団体から機密情報を盗む「標的型攻撃」に遭った。社会保険庁時代から引き続き使っている情報共有の仕組みが被害拡大につながった。

漏洩した情報は3種類ある。約116万7000件と最も多いのが基礎年金番号と氏名、生年月日の3項目から成る個人情報。次に多いのがこれに住所を加えたもので、約5万2000件流出した。最も流出が少なかったのが基礎年金番号と氏名から成るもので約3万1000件が漏れた。機構は流出した基礎年金番号を変更するという。

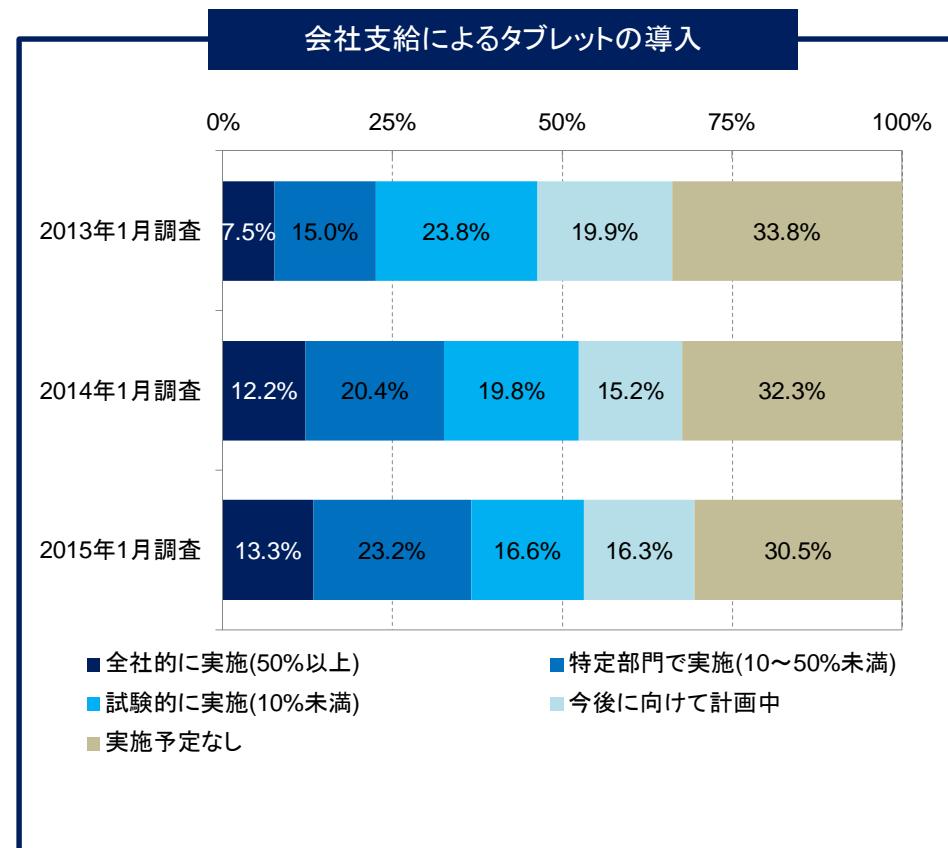
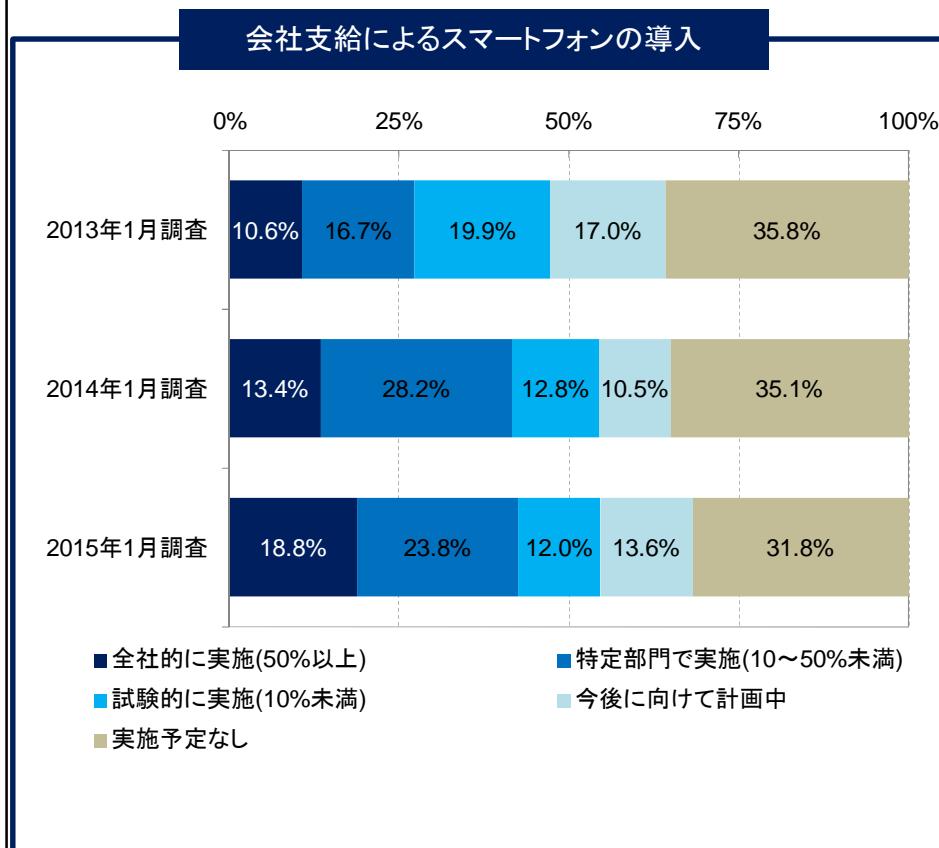
機構のシステム統括部の川田高寛システム管理グループ長は「5月8日に最初の不審メールがフリーメールのアドレスから届き、18日までに何通も届いた」と話す。機構の公開アドレスのほか、「職員のメールアドレスにも直接送られてきた」。受信者には、入社年数や年齢などの個人情報を記載した書類が添付されており、個人情報を漏洩する危険性がある。

写真 日本年金機構の本部（東京・杉並）と、6月1日に厚生労働省で情報漏洩について記者会見する同機構の水島藤一郎理事長（右）。右の写真は時事通信社提供  
[画像のクリックで拡大表示]

## ②マルチデバイスへの対応

### 多台数化が進むスマートデバイス

- 新規導入企業は頭打ちながら、導入企業におけるスマートフォン、タブレットの台数は増加傾向にある。

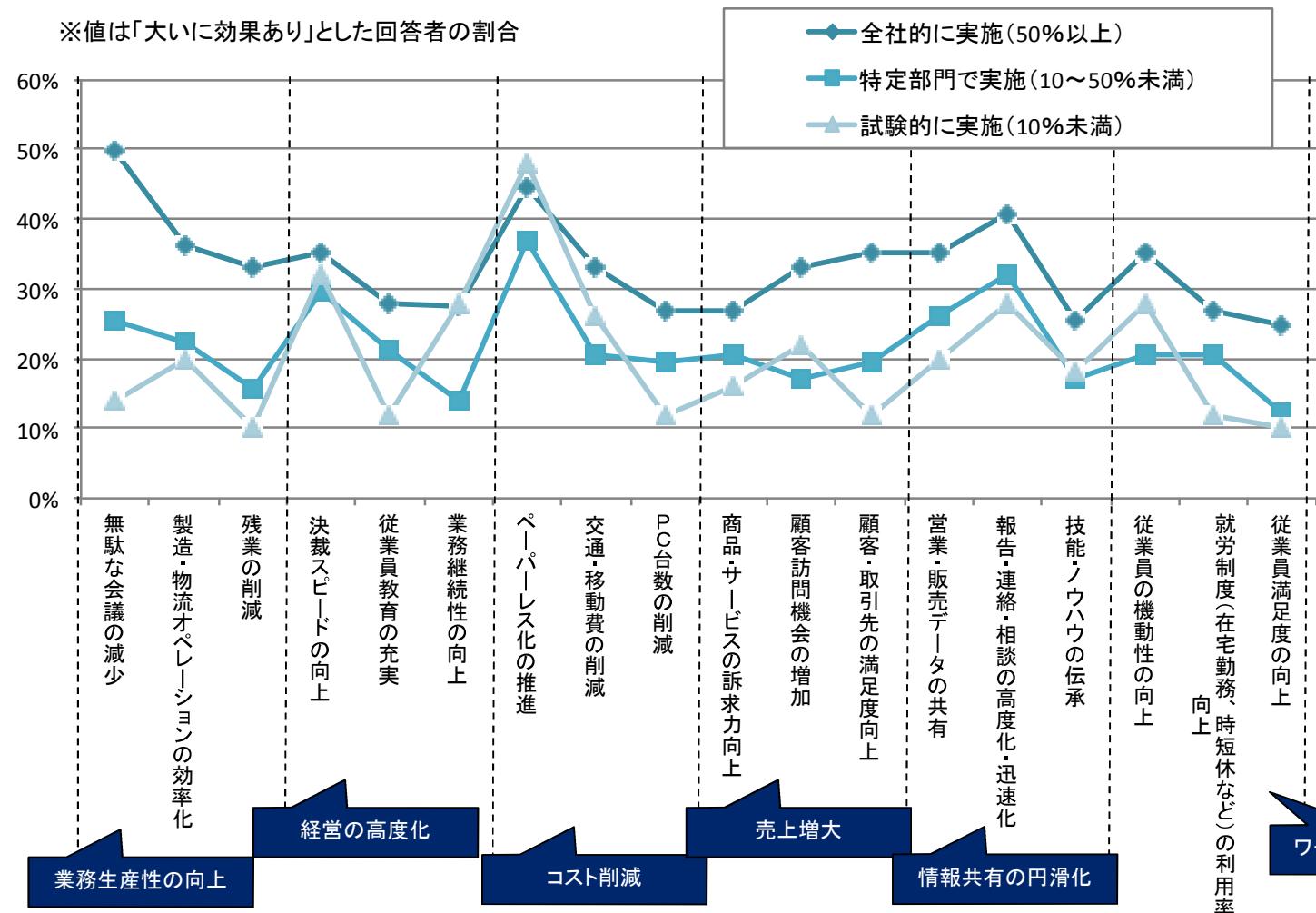


出典: JIPDEC/iTR「企業IT利活用動向調査2015

## ②マルチデバイスへの対応

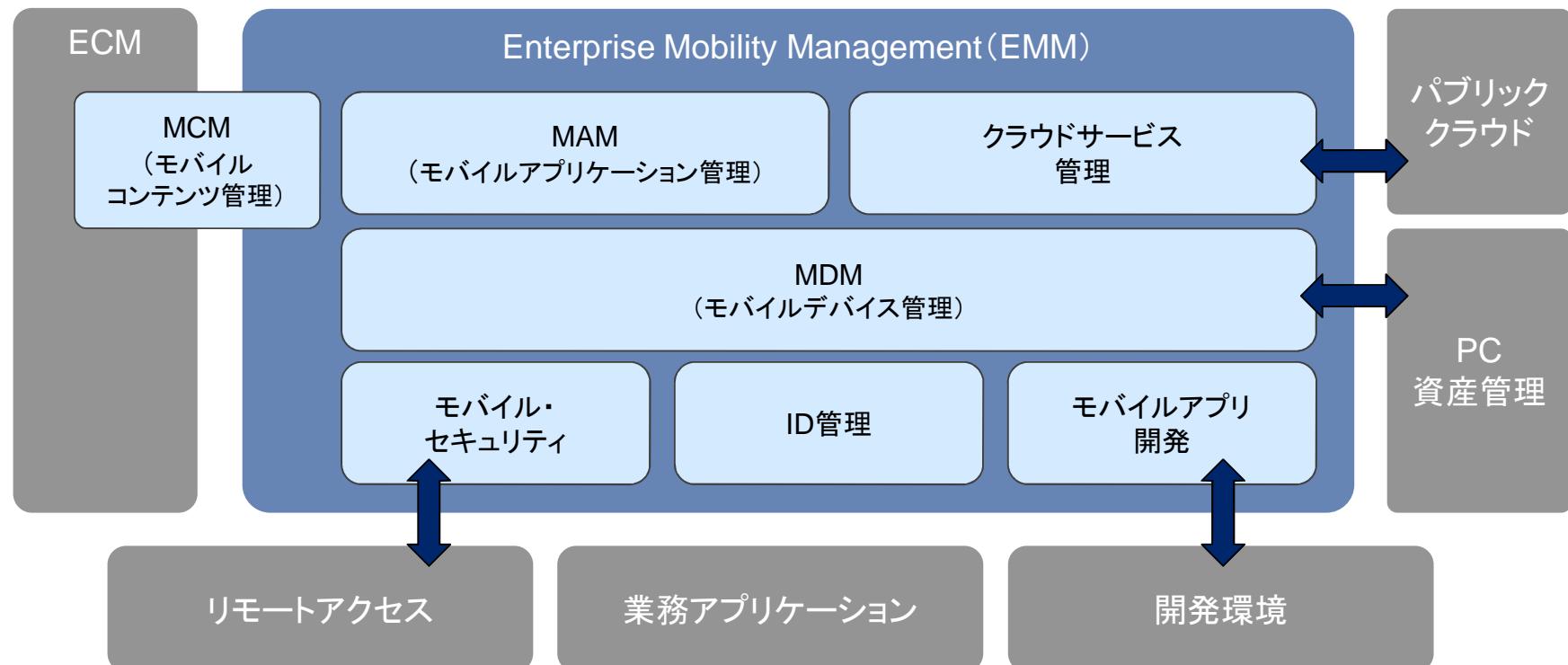
# スマートフォンの支給状況と効果の関係

- 導入企業の効果の実感度合いは、広範囲に支給を実施している企業ほど高い。
- 特に業務生産性の向上、売上(顧客価値)の増大と関連する項目はその差が大きい。



## ②マルチデバイスへの対応 EMMの概念

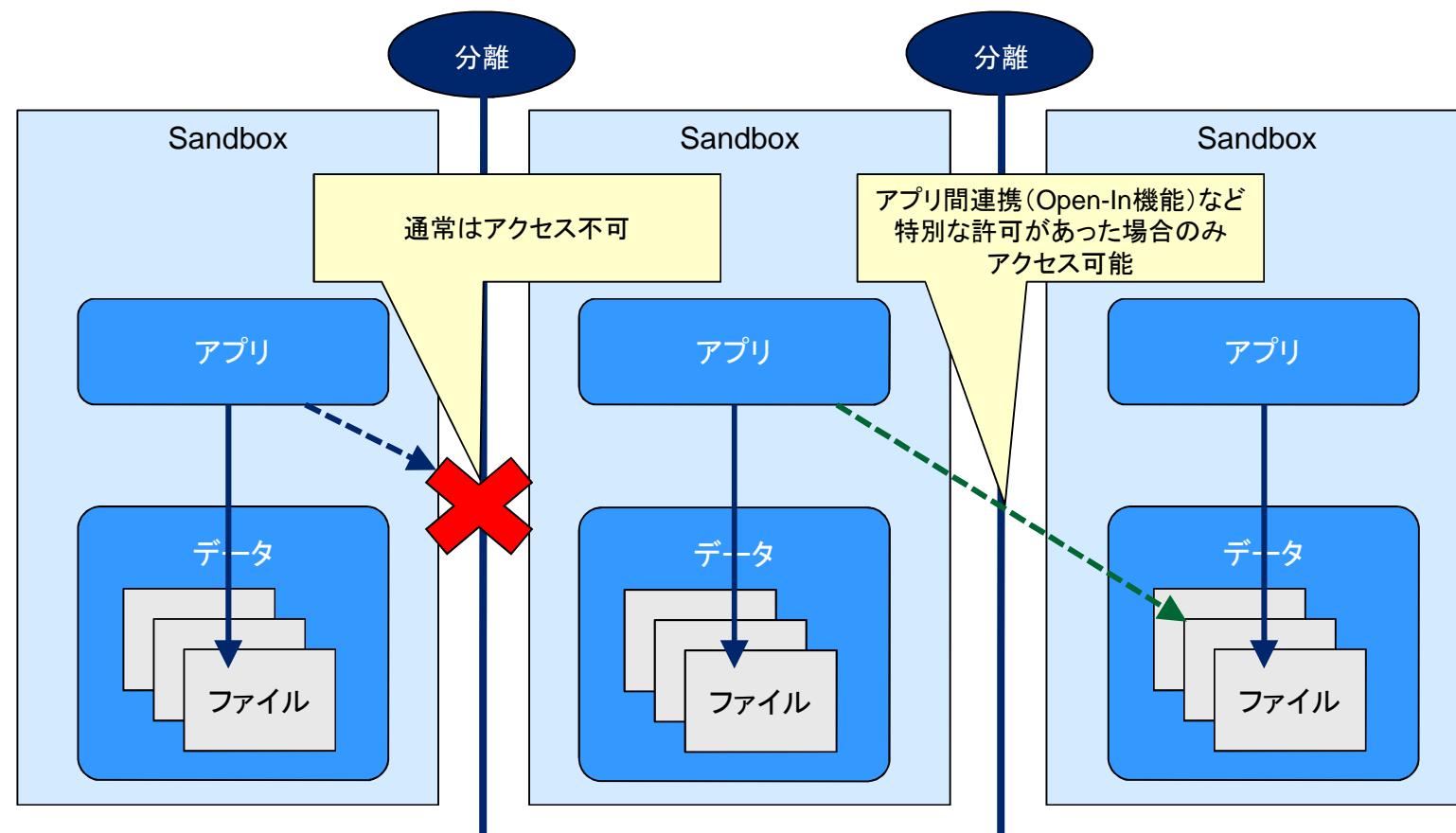
- 昨今は、モバイル管理ツールの統合化が進展。
- MDMを中心として、さまざまな要件を組み合わせたEMM(エンタープライズ・モバイル管理)と呼ばれる環境が提供されている。



## ②マルチデバイスへの対応

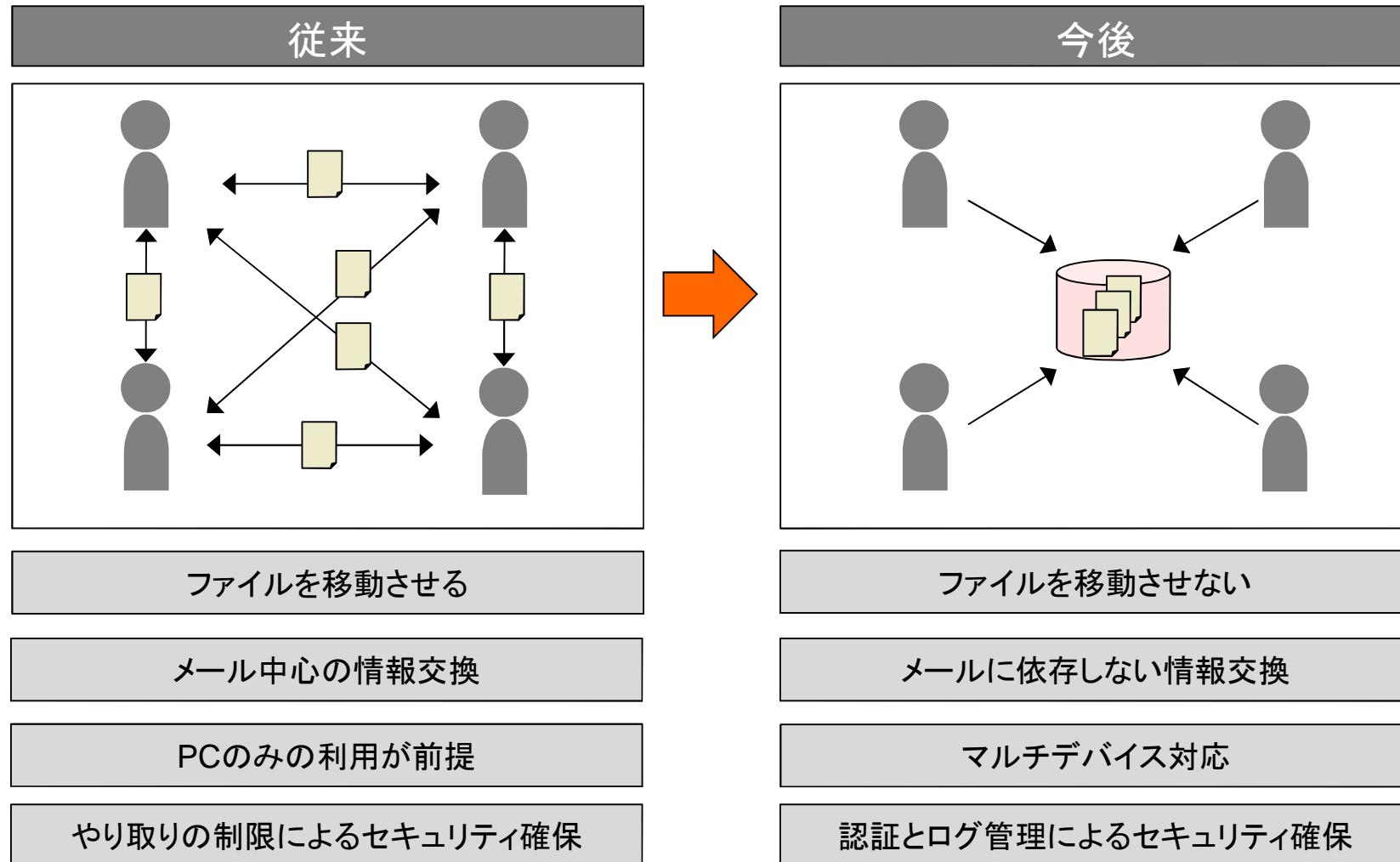
### スマートデバイス・アプリケーションの特性

- iOS、Androidは、アプリケーションがサンドボックス構造である。Windows 10も、この構造を採用しており、これが、「スマートデバイスOSの方が安全」と考えられる理由である。
- この特性を生かして、今後は「アプリケーション管理」の重要性がより高まると考えられる。



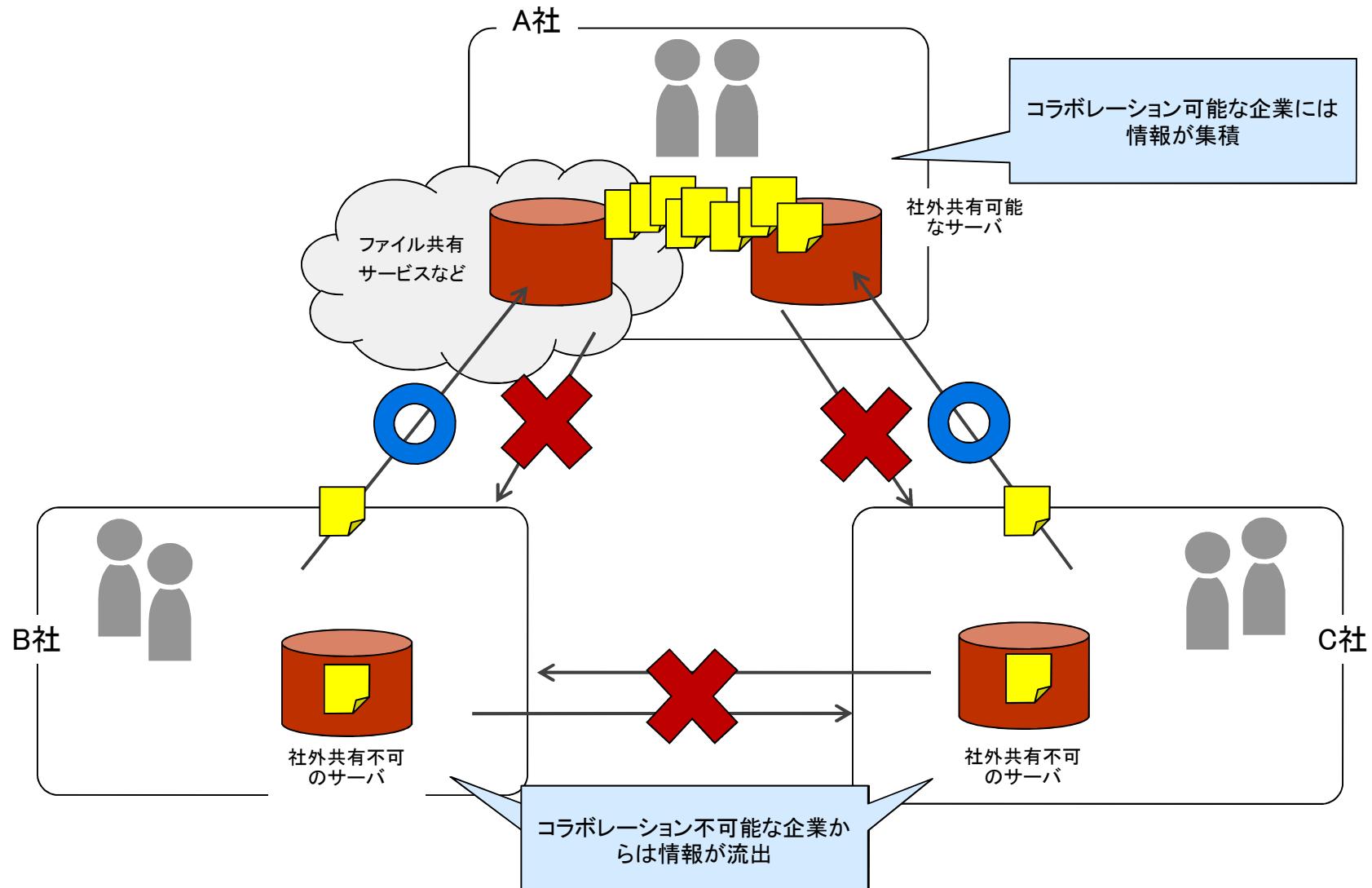
### ③コンテンツ管理の見直し 再考が迫られるファイル保管方法

- 働き方やデバイス環境が柔軟になれば、必然的にファイルの「置き場」は厳格にしなければならない



### ③コンテンツ管理の見直し B2Bコラボレーションへの対応

- 企業間とのコラボレーションでは、安全なファイル共有環境の整備が急務となる。



### ③コンテンツ管理の見直し データ保護技術の活用

- システム環境に依存することなく、データそのものを保護するための技術も進展している。
- 昨今では、クラウド型のファイル共有サービスにおいても、標準で採用されるようになってきている。

#### IRM

(Information Rights Management)

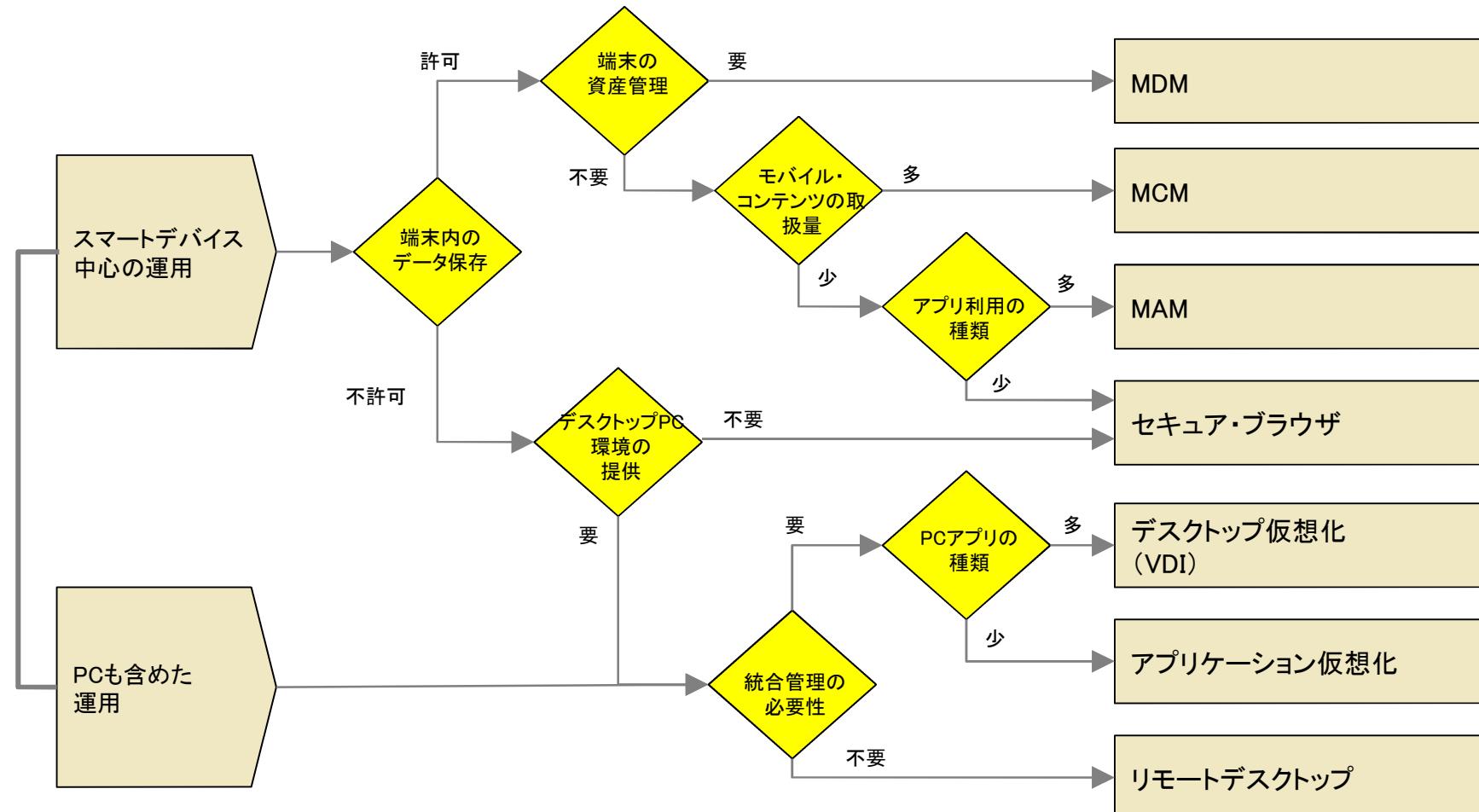
- データの属性(重要度)とエンドユーザーの権限をマッチングさせることにより、特定のファイルについて、特定の権限をもつ人のみに、特定の行動(閲覧・編集・印刷など)を許可する技術
- サーバベースのアクセス制御、あるいはクライアント・ソフトの配布によって、社外ユーザーに対しても、ポリシーの適用が可能
- ファイルは常時暗号化されているため、たとえ管理権限外に持ち出されても操作の無効化が可能

#### DLP

(Data Loss Prevention)

- 内包するキーワードやデータ形式などを分析し、PCやファイルサーバ上にある「重要文書」を識別。重要文書のみの操作を制限することで、データの漏洩・消失を防止する技術
- 製品としてはストレージ・サーバ検索型、クライアントPC常駐型、メールの送受信を検閲するゲートウェイ型などが存在する
- 最近は、PCからの外部ストレージへの持ち出しなど特定の行動のみを禁止するエントリー製品も登場

## ④テレワーク環境の整備 業務支援環境の選択肢

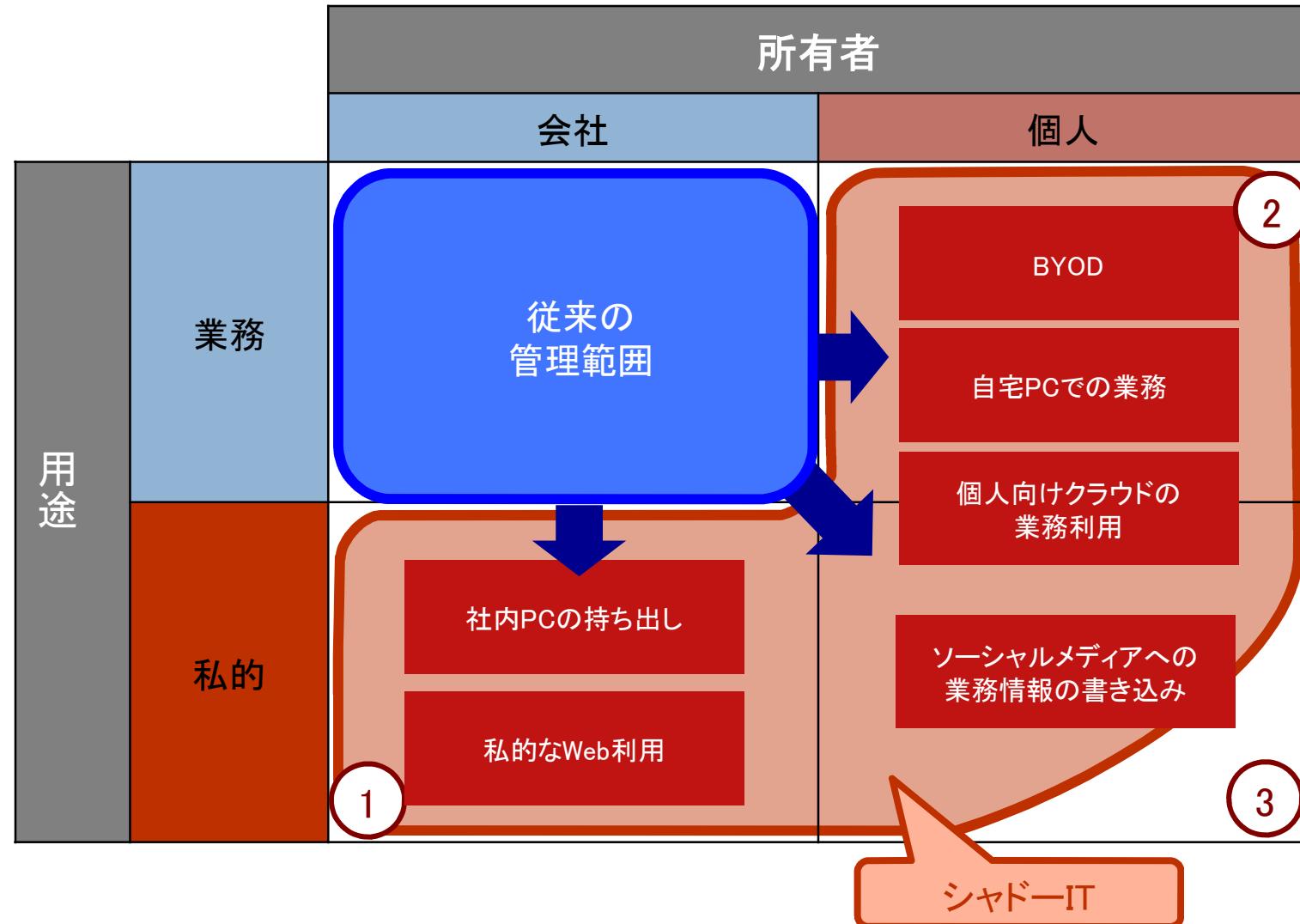


## IT部門に求められる管理方針の転換

- 新しいワークスタイルやテクノロジが普及は、IT部門とユーザー部門との関係にも変化をもたらす
- それによって価値を得ようとするのであれば、IT部門にも方針の転換が求められる



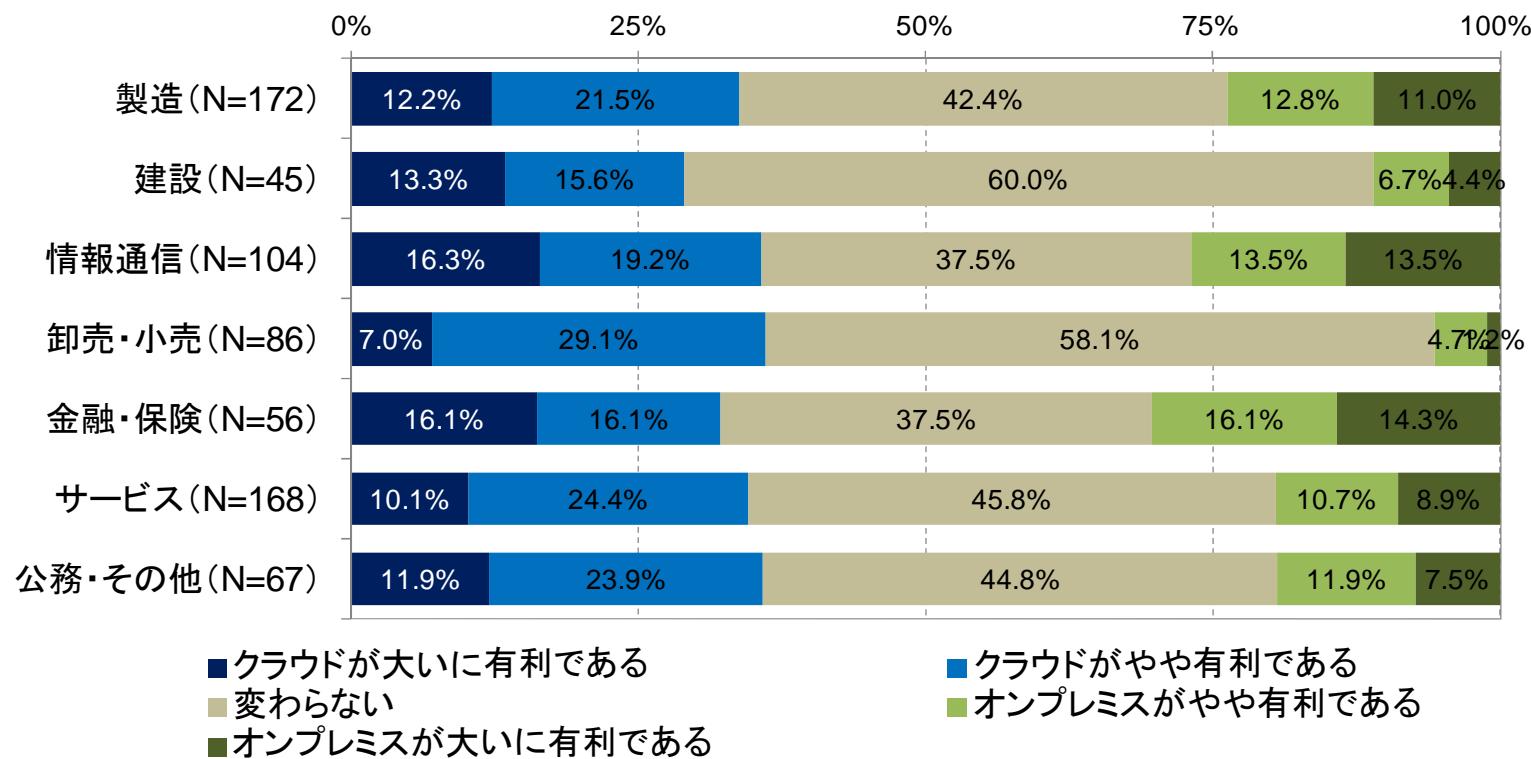
## “シャドーIT”への対処 ~見て見ぬ振りから緩やかなコントロールへ~



## 最新情報の収集と先入観の除去

- セキュリティへの不安が取りざたされるクラウド・コンピューティングであるが、実は多くの企業はすでに「クラウドのほうがリスクが少ない」と判断するようになっている。

「情報漏洩被害の軽減」における、クラウド及びオンプレミス環境の評価



出典: JIPDEC/iTR「企業IT利活用動向調査2015」

## まとめ

ワークスタイル変革は、これから企業経営において不变の課題であり、ITに  
関わる以上、向き合い続けなければならない

IT施策として優先すべきは、「コミュニケーション経路の多様化」「マルチデバイス対応」「コンテンツ管理の見直し」「テレワーク環境の整備」である。

IT施策を構想化する上では、生産性(価値)の向上とセキュリティを一体で捉  
えることが求められる。

IT管理者は、従来の固定観念や先入観を取り払って、新しい働き方やテクノロジと向き合うべきである。

