RICOH
imagine. change.

スマートデバイス活用に向けたセキュリティ対策

BYODの業務利用に向けた取り組み

2013年9月19日

株式会社リコー　IT／S本部
ITインフラ統合センター
田崎　淳一

目　　次

RICOH
imagine. change.

- 会社概要
- ITガバナンス方針（New　Workstyle）
- 方針の背景（日本ではなく世界に学べ）
- スマートデバイス管理の現状
- BYOD実現に向けての取り組み
- まとめ

リコーグループの概要

■設立年月：1936年2月（創業76年）

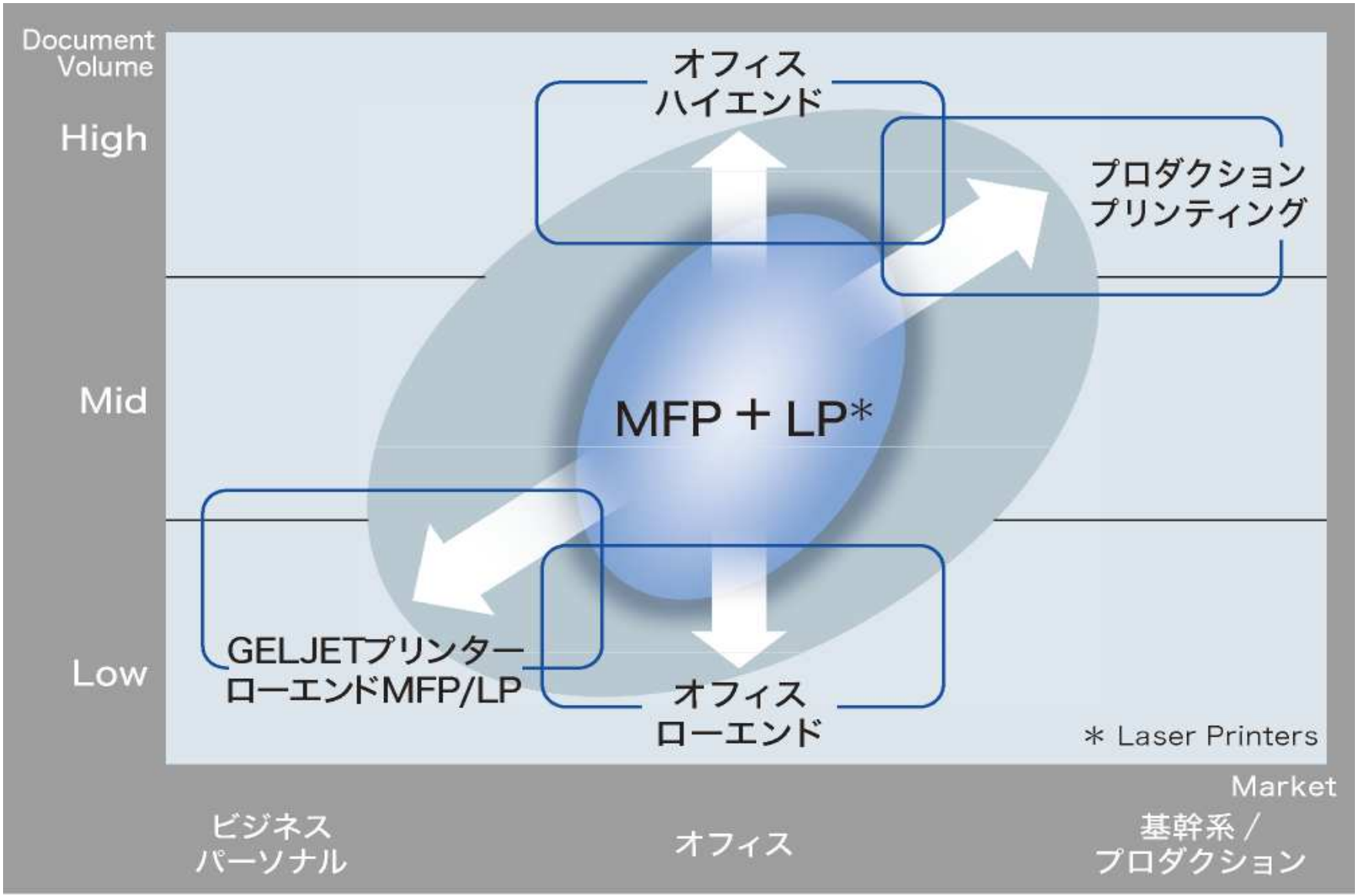
■資本金：1,354 億円

リコーグループでは、複合機やプリンターなどの
情報機器を中心に、製品の開発・生産・販売・
サービス・リサイクルなどの事業を展開しています。

複合機 	レーザープリンター 	プロジェクションシステム 
	プロダクションプリンター 	
ユニファイド コミュニケーション システム 	デジタルカメラ 	サーマルメディア 
IT サービス ITKeeper	MDS（マネージド・ドキュメント・サービス） Managed Document Services MPS and Beyond	半導体 

プリンティング分野における提供価値の拡大

ハード・ソフトの開発力や生産力と、サービス・ソフト・ITソリューション力のシナジーにより、お客様ニーズへの対応を強化しています。



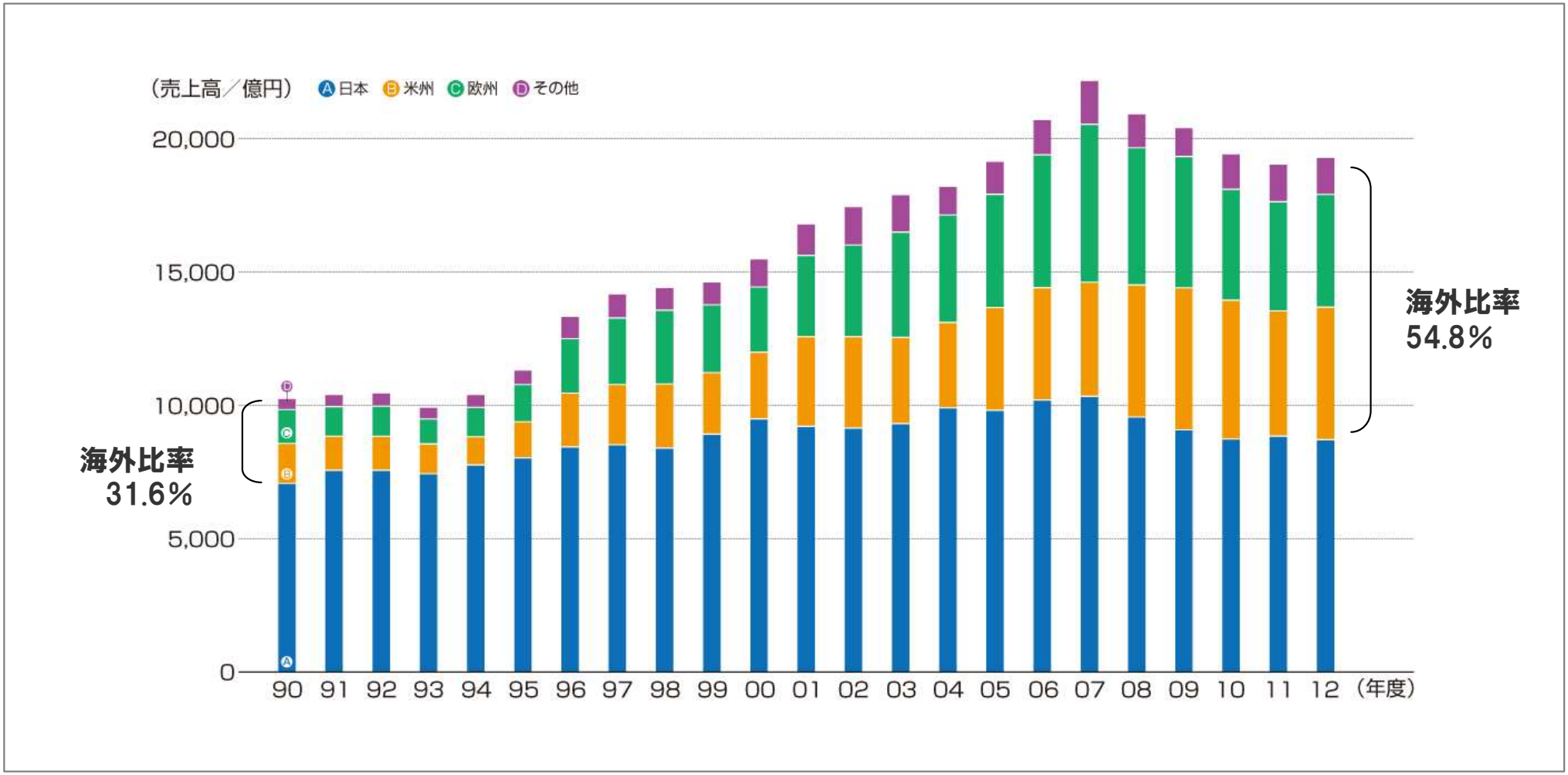
ペンタックス

RICOH
imagine. change.

PENTAX
A RICOH COMPANY

グループ連結業績推移

■連結売上高　　：　1兆9,244億円
■売上高の海外比率　：　54．8％（国内:8,703億円、海外:1兆054億円）

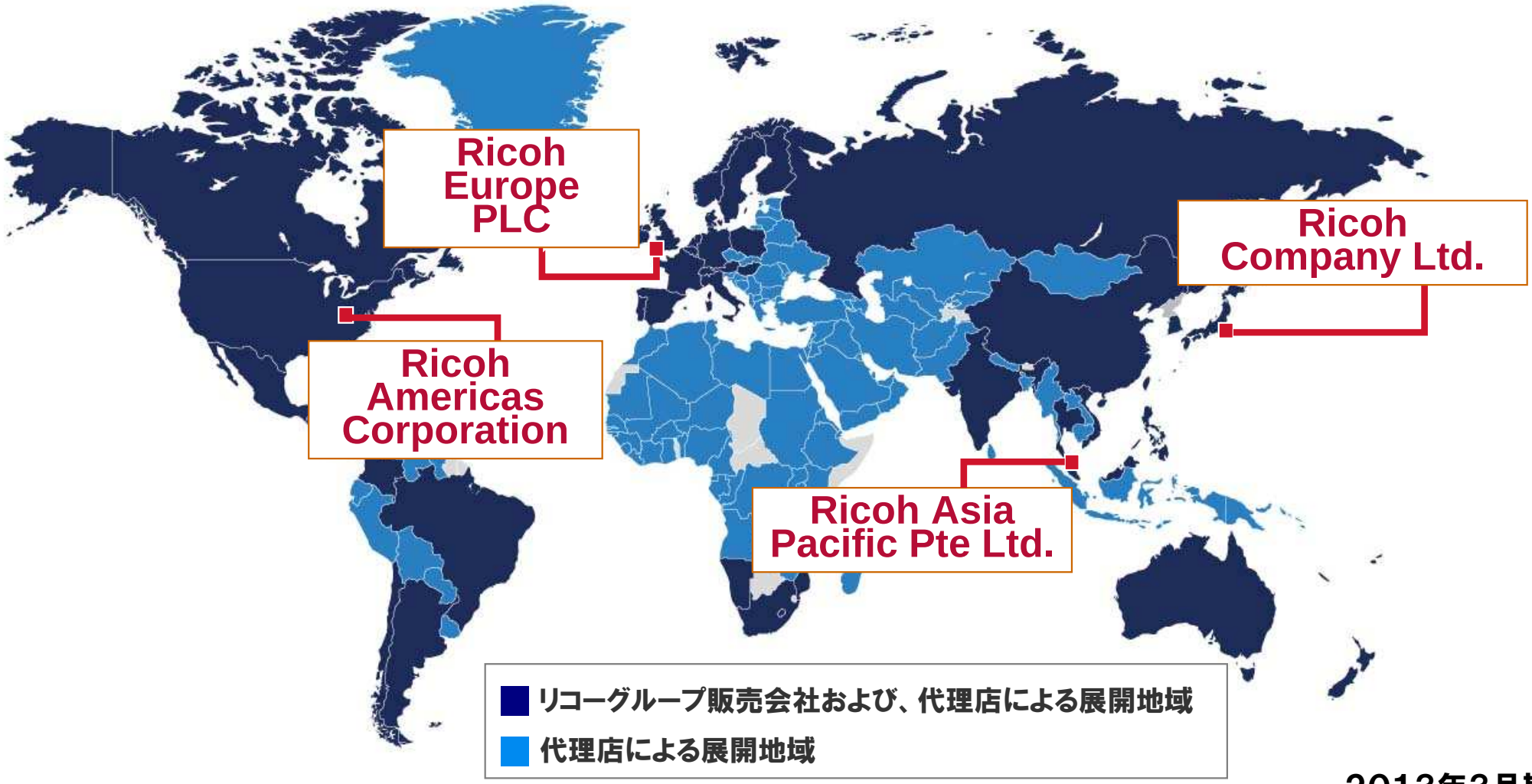


グローバル・リコーグループ

RICOH
imagine. change.

■ リコーグループ　　グループ企業数：228社
グループ従業員数：107,431名　（国内：37,401名、海外：70,030名）

■ 全世界約200の国・地域において、現地に密着した販売・サービスを展開しています。



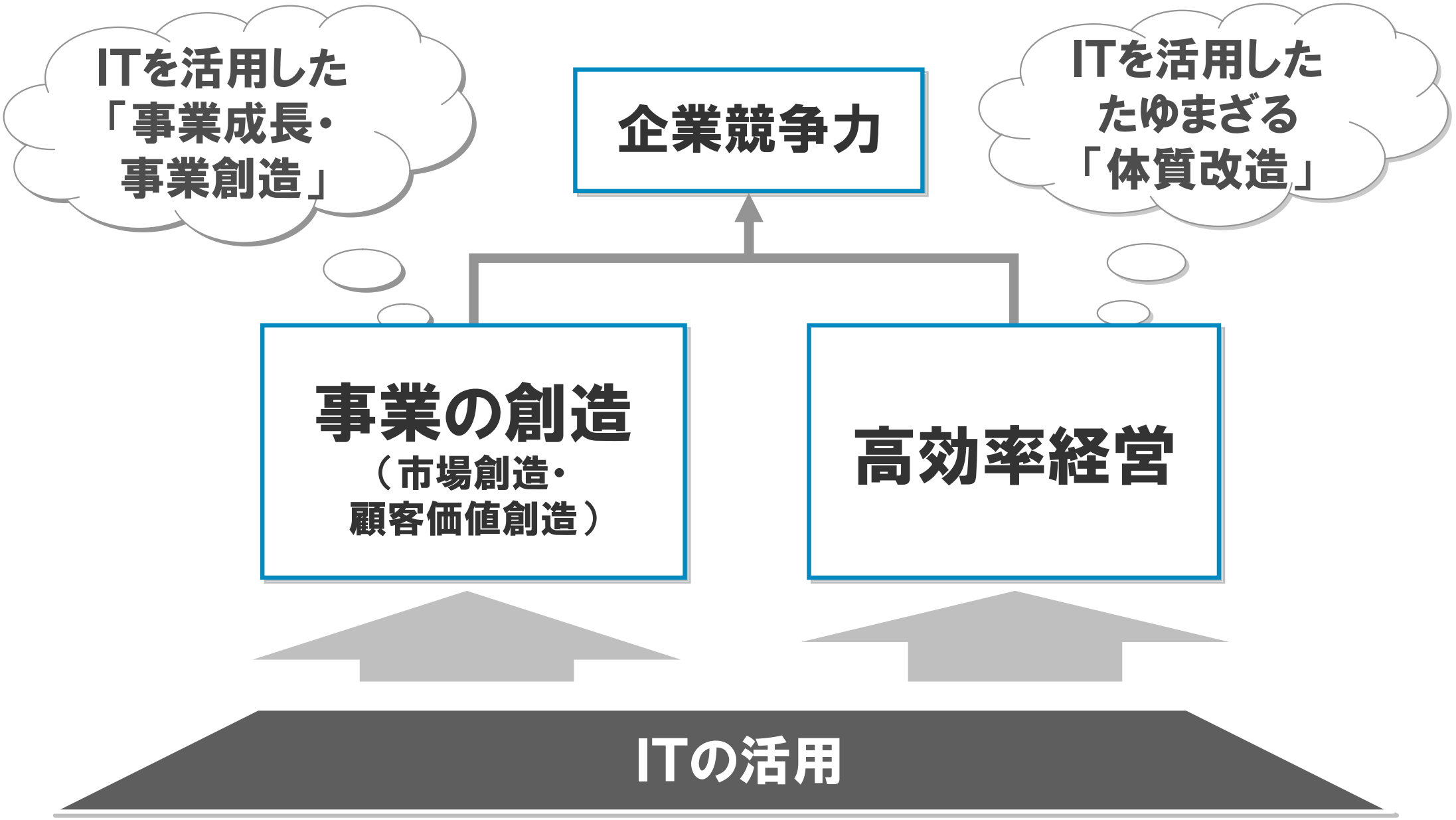
目　　次

- 会社概要
- ITガバナンス方針（New　Workstyle）
- 方針の背景（日本ではなく世界に学べ）
- スマートデバイス管理の現状
- BYOD実現に向けての取り組み
- まとめ

企業競争力を支えるIT

RICOH
imagine. change.

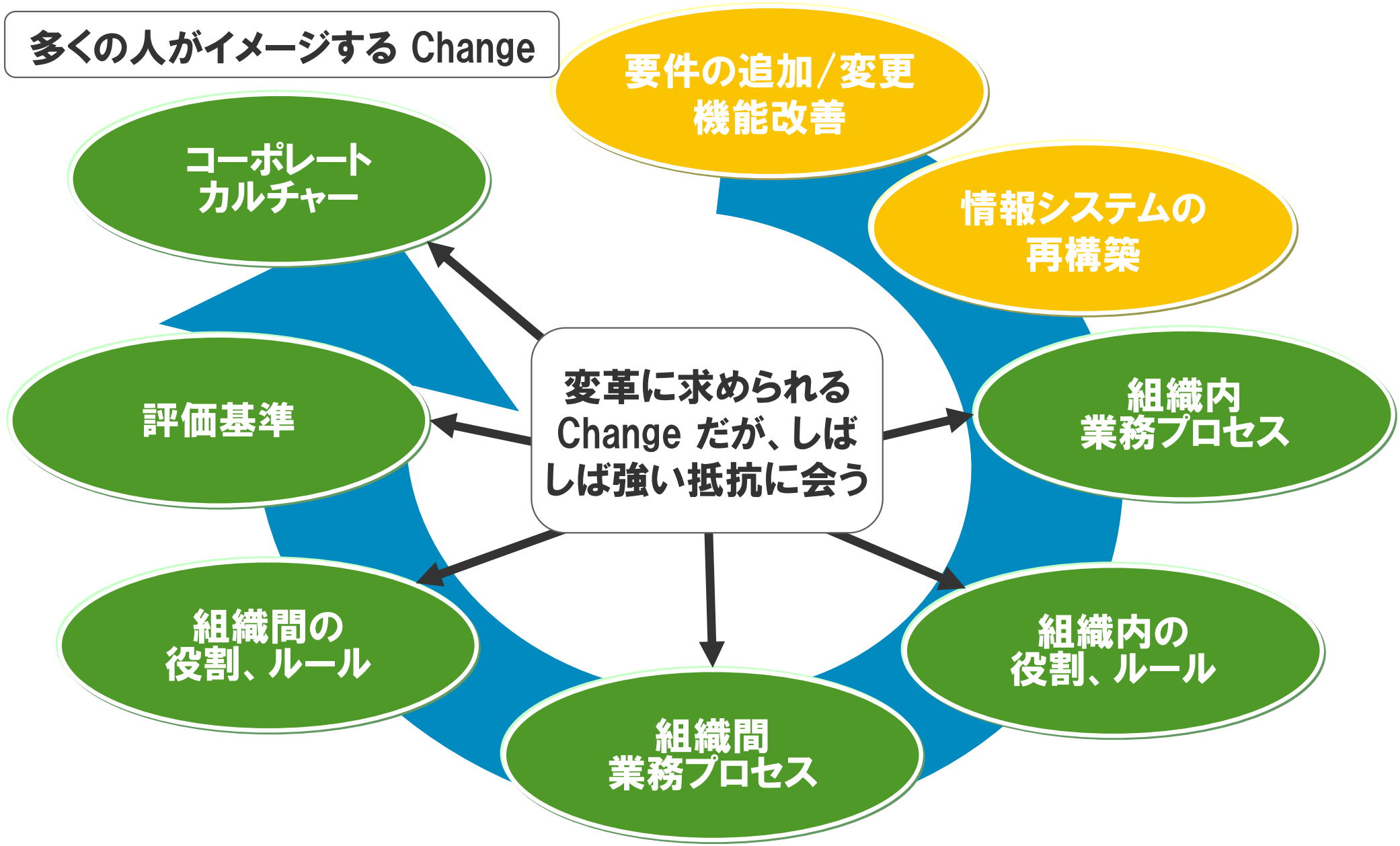
ITを活用し高効率経営と事業の創造の両面で貢献する



変革のリーダー

RICOH
imagine. change.

情報システムを変えるだけでは、仕事は良くならない



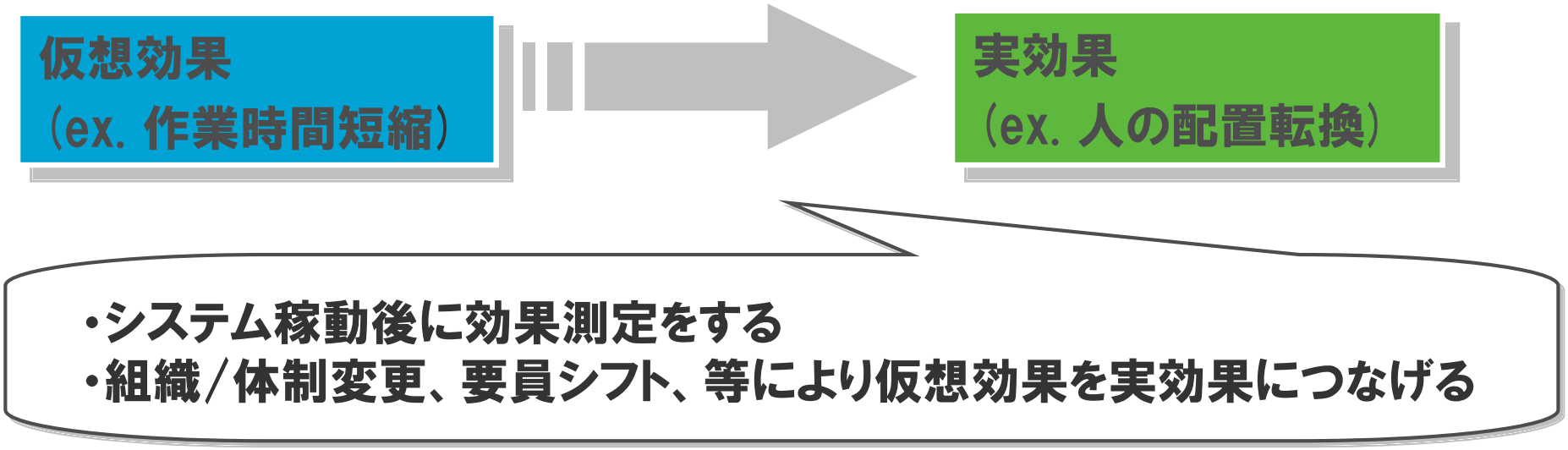
効果の刈り取り

RICOH
imagine. change.

システム稼動はゴールではなく、効果刈り取りの出発点

■ プロジェクト計画段階で目標効果をより広範囲に、より具体的に積み上げる。
現状の姿を明らかにし、業務改革のシナリオを明確にする。

■ 仮想効果を実成果として刈り取る。



■ システム稼動後（プロジェクト解散後）も目標効果を最後まで追いかける。

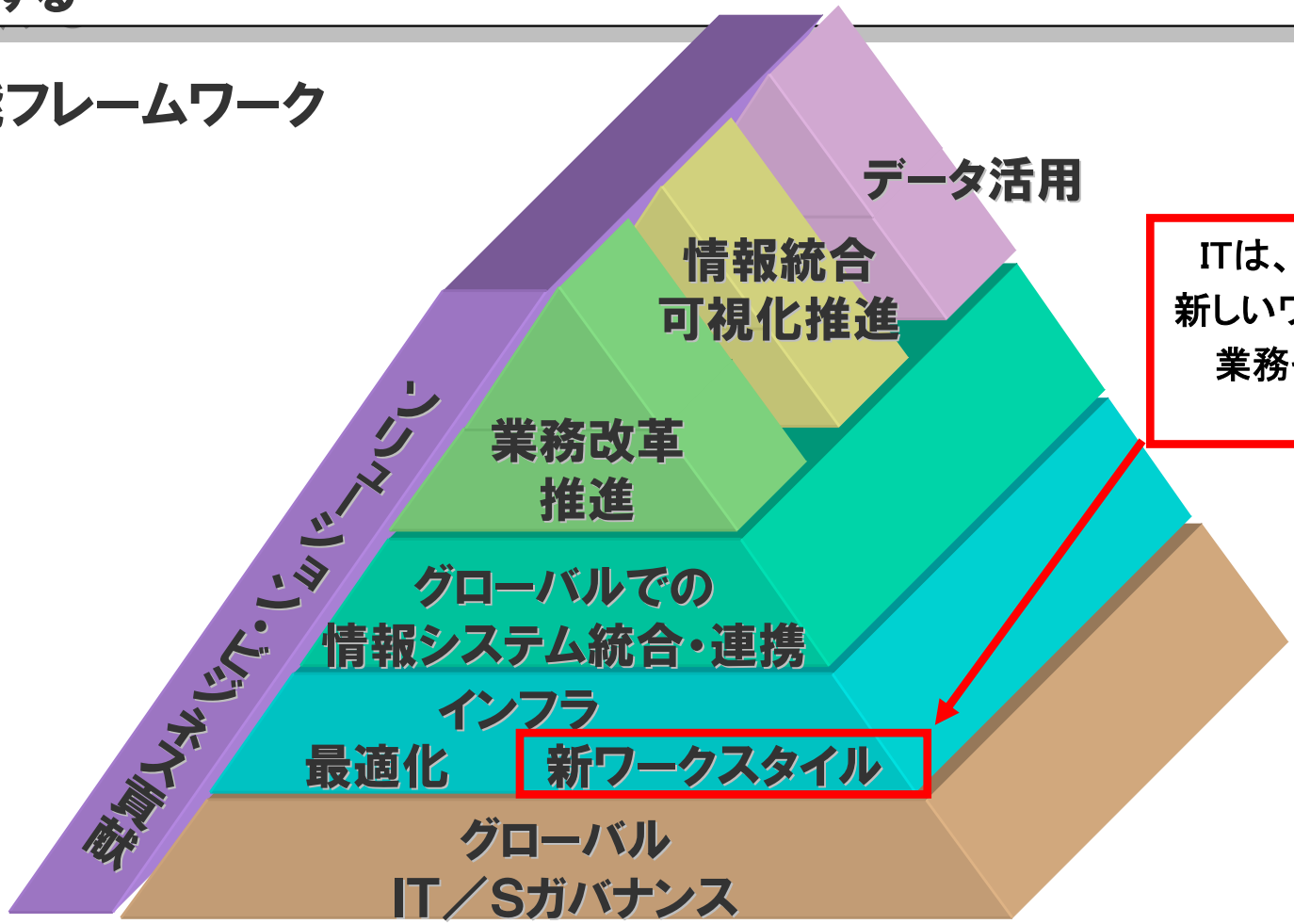
IT／Sのミッションと実現の為の機能フレームワーク

RICOH
imagine. change.

■ IT／S ミッション・ステートメント

1. IT／Sは業務改革を推進し、グローバル・リコーグループの業績向上に貢献する。
2. IT／Sは情報可視化を推進し、グローバル・リコーグループの経営品質向上に貢献する。
3. IT／Sは情報資産（インフラ、アプリケーション、情報）を継続的に改善し、リコーグループの公正かつ適正な業務遂行に貢献する。
4. IT／Sは今後必要となる情報インフラを先行的に整備し、システムソリューション事業の業績向上に貢献する

■ IT／S機能フレームワーク



ITは、時代の変化に応じて
新しいワークスタイルを創造し
業務そのものを変革する
ことが重要

グループIT／Sのさらなる構造改革

RICOH
imagine. change.

4つの領域でグループIT／Sの抜本的な構造改革を実現し、業績のV字回復に貢献する

業績貢献

システム価値向上
コスト削減

投資

全体最適なIT投資

ガバナンス

ITガバナンス強化

戦力強化

人材

戦略的人材育成

組織

グループITの組織力強化
グループITの体質改造

変革のうねりを起こす

改革のうねりを起こす WAVE　プロジェクトを12年度下期より始動

- **W**illing to “Change” 進んで変革を起こし、
- **A**ccelerate the “Change” 変革を加速し、
- **V**enture to “Change” 困難な変革にも意を決して臨むことで、
- **E**njoy the “Change” 変革による利益を享受する。

New Workstyleの実現

RICOH
imagine. change.

「新しい働き方の世界観」実現のためのオープンコミュニケーション環境を実現する

社内コミュニケーション

経営層の想いが知りたい・・・
社員の意見が聞きたい・・・

トップ⇔ボトムのダイレクトなコミュニケーション

④ ポータル　⑤ SNS
⑥ リアルタイムコミュニケーション

社内コミュニケーション

●●プロジェクトについて知りたいけど、誰に言えば良いのだろう・・・

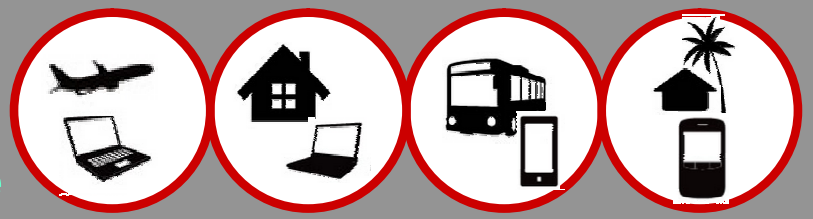
個人の業務知識やノウハウの見える化

④ ポータル　⑤ SNS


お客様


グループ社員

Anytime
Anywhere
Any device




業務システム

社外にいる社員とのコミュニケーション

アメリカ出張中の上司に今すぐ連絡をとりたい・・・

相手と最速にコンタクト

⑤ SNS　⑥ リアルタイムコミュニケーション
① メール　② スケジューラ

社内情報共有

●●プロジェクトの議事録が見れない・・・

組織の階層を超えた情報共有

③ 文書管理

以下の6つのファンクションで実現する

① メール　② スケジューラ　③ 文書管理　④ ポータル　⑤ SNS　⑥ リアルタイムコミュニケーション

目　　次

RICOH
imagine. change.

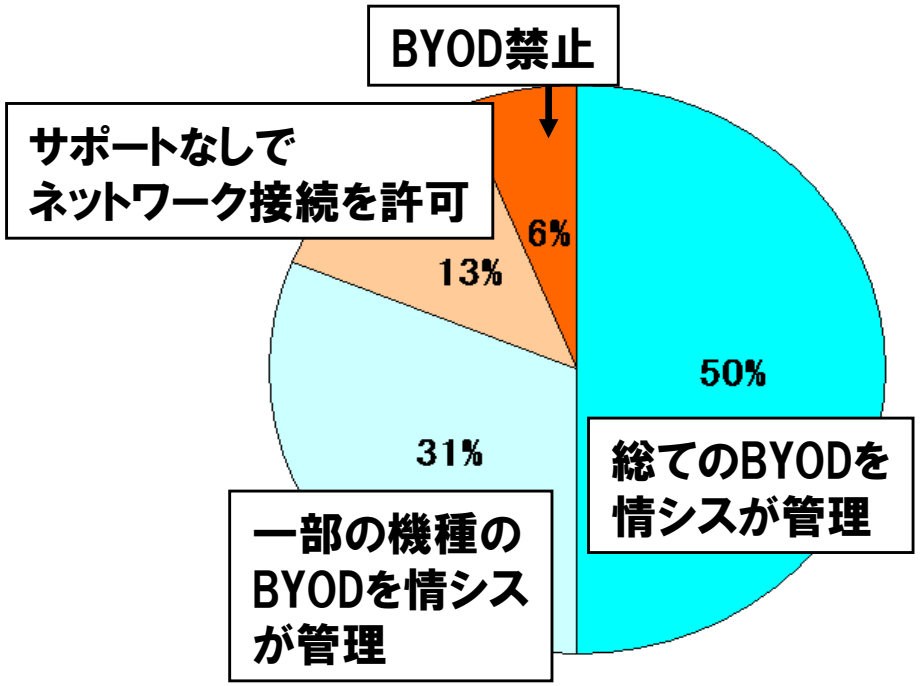
- 会社概要
- ITガバナンス方針（New　Workstyle）
- 方針の背景（日本ではなく世界に学べ）
- スマートデバイス管理の現状
- BYOD実現に向けての取り組み
- まとめ

米国企業におけるBYODの最新動向

シスコIBSGが2012年春に米国の大規模会社（従業員1,000以上）600人、中規模企業（従業員500～999人）312人を調査した結果、**BYODを正式サポートしている企業は81%、サポートなしを含めると94%の企業がBYODを認めている**という結果となった。
またESETの調査によるとBYODの中心はPCとなっている。

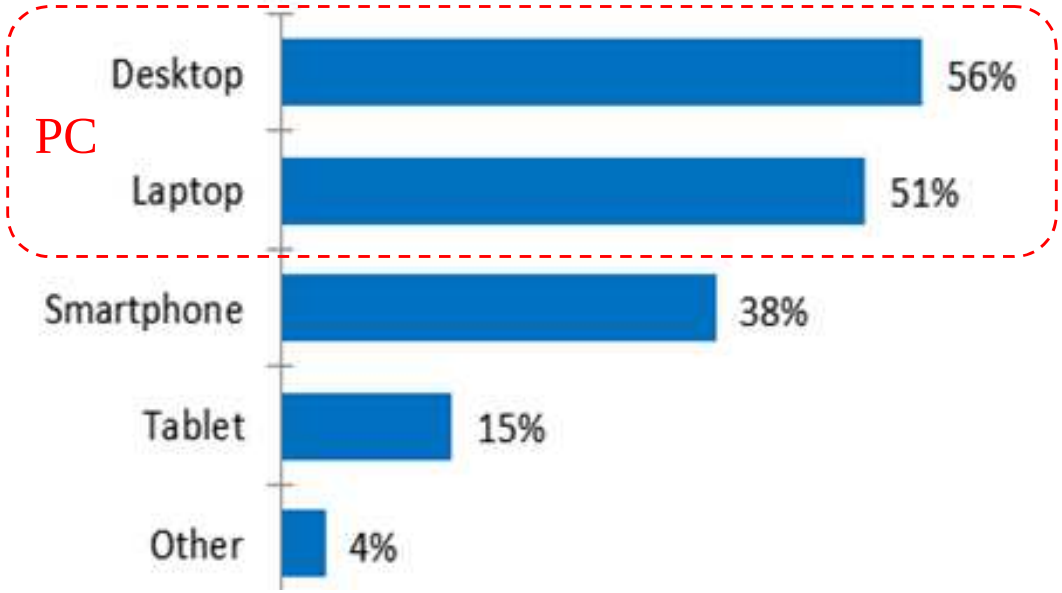
シスコIBSG調査結果

http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons-Global_JPN.pdf



ESETSET調査資料

http://www.welivesecurity.com/2012/02/28/sizing-up-the-byod-security-challenge/

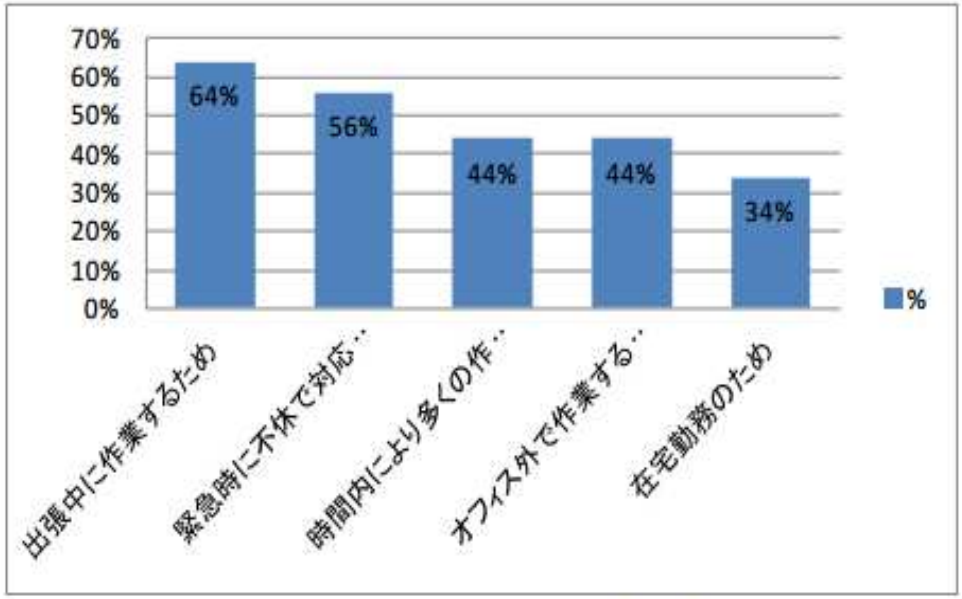


米国企業ではPCも含めてBYODは当たり前の時代となっている。

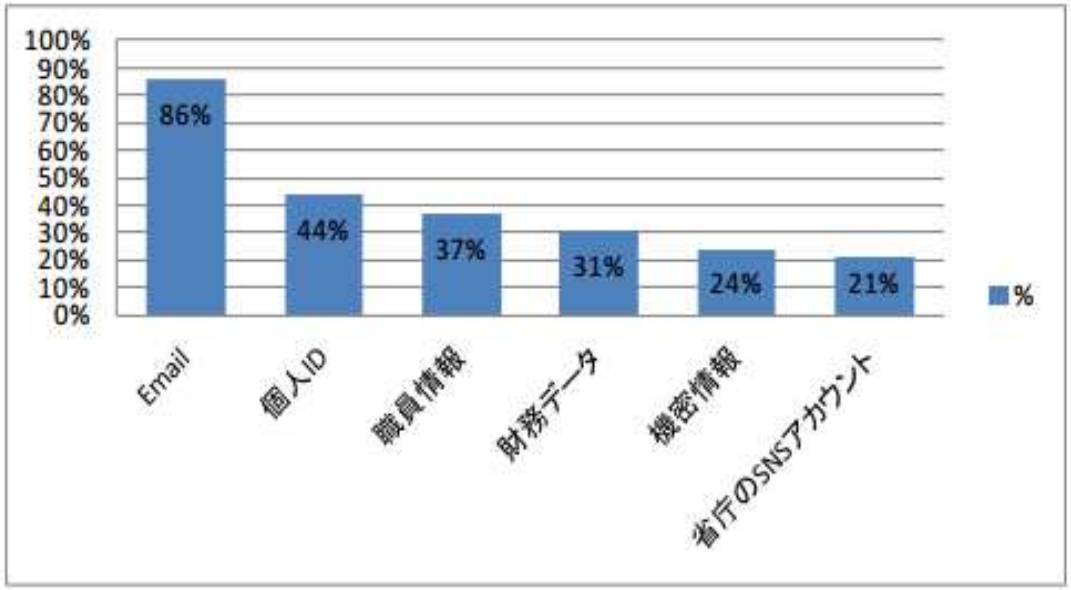
米国政府におけるBYODの最新動向

社団法人　行政情報システム研究所　2012年4月調査資料より抜粋　http://www.iais.or.jp/ja/wp-content/uploads/2012/04/BYOD.pdf

日本の行政の情報化・電子政府を研究している『行政情報システム研究所』が調査した結果、米国は2011年11月に大統領命令として、IT機器のコスト削減を各省に指示し、その半年後の2012年4月時点で**62%の省庁が個人所有の機器で仕事することを許可し、40%以上の職員が実際に個人所有の機器を持ち込んでいる。**



職員によるモバイル機器の利用理由



職員がモバイル機器を通じてアクセスする可能性のあるデータ

米国は政府もBYODで、その変化は半年の単位で起こっている。

リコーグループのBYOD状況

リコー以外のグローバル企業もBYODは米国先行となっている。

目　　次

- 会社概要
- ITガバナンス方針（New　Workstyle）
- 方針の背景（日本ではなく世界に学べ）
- スマートデバイス管理の現状
- BYOD実現に向けての取り組み
- まとめ

利用の要望(ニーズ)

＜ニーズ＞

- 会社貸与と個人の2台持ちは、いやだ。
- 会社貸与の携帯電話は古い。全員に配布されない。
- 性能・使い勝手のよい個人のスマートフォンを使いたい。
- 業務で活用できないか。(経営層)
- ワークスタイルの変革から「いつでも」「どこでも」簡単に使えないか。(経営層)

ニーズを受けて

ニーズを受けて、下記取組みを行ってきました。
取組みの詳細は、以降のスライドでご説明します。

＜活動状況＞

2010年	スマートデバイスを調査 暫定運用の策定
2011年	リスクの調査と対策の検討 MDM(Mobile Device Management)検討
2012年	iOS向け展開(会社資産デバイス)
2013年	Androidへの対応(会社資産デバイス)

＜今後の予定＞

2013年 10月	BYOD(個人資産デバイス)への対応

スマートデバイスを調査（2010年）

＜社内の利用状況と主要機器を調査＞

- グループ内の利用状況（計画を含む）を調査（国内・海外）
  国内では、IT部門を中心に評価・検討開始
  海外では、BlackBerryでメール・スケジュール利用

- 当時（2010年）、発売されている主要機器を調査
  機器（デバイス）やOSごとにセキュリティリスクが異なる
  デバイスに意図せず、データが残る
  紛失・盗難の対策は、パソコンと同等レベルが必要

iPhone	Xperia	BlackBerry	WindowsMobil	iPad
				

調査後の結論（2010年）

RICOH
imagine. change.

＜利用方針＞

セキュリティ対策とルールの明確化が必要である。

しかし、リスクに対する見極めが不十分

また、全てを禁止するとこっそり使いだす可能性もある

この事から**利用を制限して許可**することとした。

＜利用許可＞

CACHATTO（メール／スケジュール）

※既に携帯電話向けに展開しているサービスの一部機能を拡張

＜利用制限＞

社内LAN環境への接続禁止（Wi－Fi接続・リモート接続）

リスクの調査（2011年）

RICOH
imagine. change.

＜ターゲット＞

今後、利用が中心となる「iOS」と「Android」にターゲット

※WindowsPhoneやBlackBerryは、ニーズが高まってきた段階で調査とする。

＜リスク調査＞

- iOSとAndroidでは、リスクが異なる
- アプリケーションマーケットの検疫が、Androidは不十分
- ウィルス対策ソフトはあるが、パソコンより低い（レベル）
- リモート接続でのVPNソフトがAndroid未対応である
- 初期化／リモートワイプで、Androidは完全消去不可

調査結果（2011年）

RICOH
imagine. change.

＜調査結果＞

- iOSに比べAndroidは、リスクが多く（不明点が多い）、現状では対策を十分に取りきれないと判断
  - ウィルス対策
  - SDカードの扱い
  - アプリ導入制限（安全なソフトの見極め）

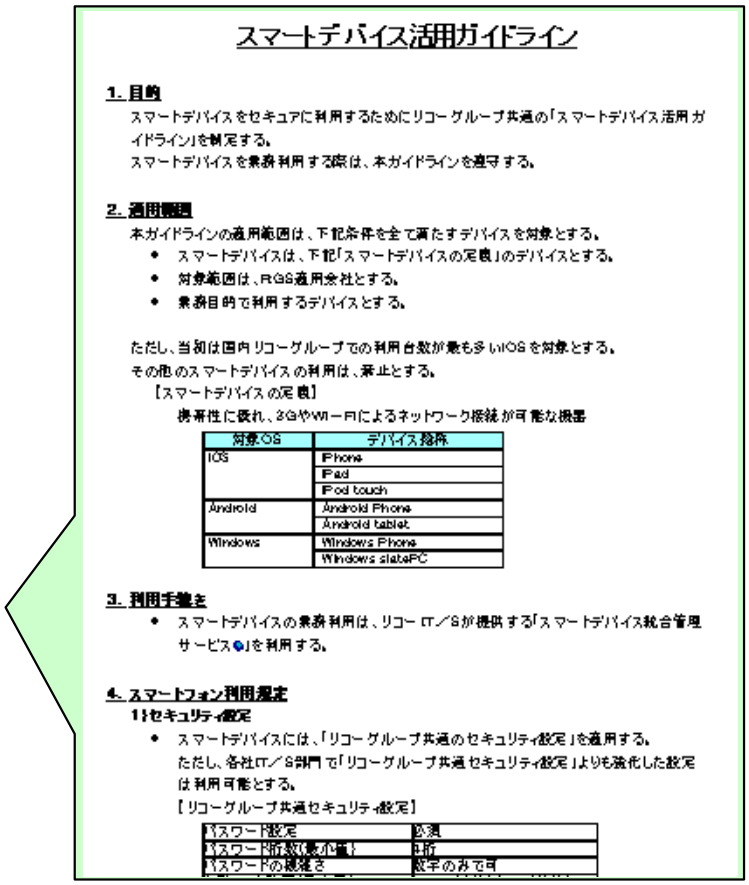
- iOSとAndroidへの対応計画
  - iOSを先行してリリース（2012年度）
  - Androidを次ステップでリリース（2013年度）

対策(ポイントは3点)(2011年)

- **機器(スマートデバイス)への具体的な設定**
  - パスワード設定(桁数・複雑性・ロック時間)
  - パスワードを間違えた際の初期化
  - パックアップの制限(パソコン・クラウド)

- **ルール化して守らせる**
  - 「スマートデバイス活用ガイドライン」の策定
  - 機器への設定だけでは対応しきれない為、ルールと組合せる。

- **管理の仕組み整備**
  - MDM(Mobile Device Management)の導入



スマートデバイス活用ガイドライン

1. 目的

スマートデバイスをセキュアに利用するためにリコーグループ共通の「スマートデバイス活用ガイドライン」を制定する。
スマートデバイスを業務利用する際は、本ガイドラインを遵守する。

2. 適用範囲

本ガイドラインの適用範囲は、下記条件を全て満たすデバイスを対象とする。

- スマートデバイスは、下記「スマートデバイスの定義」のデバイスとする。
- 対象範囲は、RGG適用会社とする。
- 業務目的で利用するデバイスとする。

ただし、当初は国内リコーグループでの利用台数が最も多いiOSを対象とする。
その他のスマートデバイスの利用は、禁止とする。

【スマートデバイスの定義】

携帯性に優れ、3GやWi-Fiによるネットワーク接続が可能な機器

対象OS	デバイス種別
iOS	iPhone
	iPad
	iPod touch
Android	Android Phone
	Android tablet
Windows	Windows Phone
	Windows slatePC

3. 利用手続き

- スマートデバイスの業務利用は、リコーIT／Sが提供する「スマートデバイス統合管理サービス」を利用する。

4. スマートフォン利用規定

1)セキュリティ設定

- スマートデバイスには、「リコーグループ共通のセキュリティ設定」を適用する。
  ただし、各社IT／S部門で「リコーグループ共通セキュリティ設定」よりも強化した設定は利用可能とする。

【リコーグループ共通セキュリティ設定】

パスワード設定	必須
パスワード桁数(最小値)	8桁
パスワードの複雑さ	数字のみで可

MDMを検討（2011年）

スマートデバイスの機器管理・設定の自動化（強制化）・紛失時の対策（遠隔消去）を行う為、MDMの調査を実施

＜MDM調査＞

- 対象OSを「iOS・Android」とする
- 機器への設定や管理項目はどこまでか
- どのような提供形態か→オンプレミス・クラウド
- 利用料金は、いくらか

MDM選定（2011年）

RICOH
imagine. change.

MDM選定では、4製品を比較し、クオリティソフト社のISM CloudOneをMIND社のプライベートクラウドとして採用

＜決定のポイント＞

機能面	大差なし。 但し、製品の趣き度合いで、機能に若干の差がある。 どちらのデバイス（iOS・Android）を主に活用するかで、注意が必要
コスト	製品ごとに金額は、だいぶ異なる。 初期費用が必要な製品（サービス） ライセンス単価が高額な製品
運用のしやすさ	MDMの管理画面の操作は、大差なし。 社内のIT資産管理との連携で、運用工数の削減が見込める。

iOS向け展開を開始(会社資産デバイス)(2012年)

- ルールを策定し、MDMの導入でセキュリティ対策が、可能となった。この為、iOS(スマートデバイス)のネットワーク接続を許可する。

対象デバイス	iOS (iPhone・iPad・iPodTouch)
ルール	「スマートデバイス活用ガイドライン」の遵守
管理ツール	MDM利用を必須化

＜利用開始＞

2012年7月スタート

iOS向け展開を開始（会社資産デバイス）（2012年）

RICOH
imagine. change.

セキュリティポリシーは、２種類

- データを保存する利用
- データ保存しない利用（ブラウジングのみ）

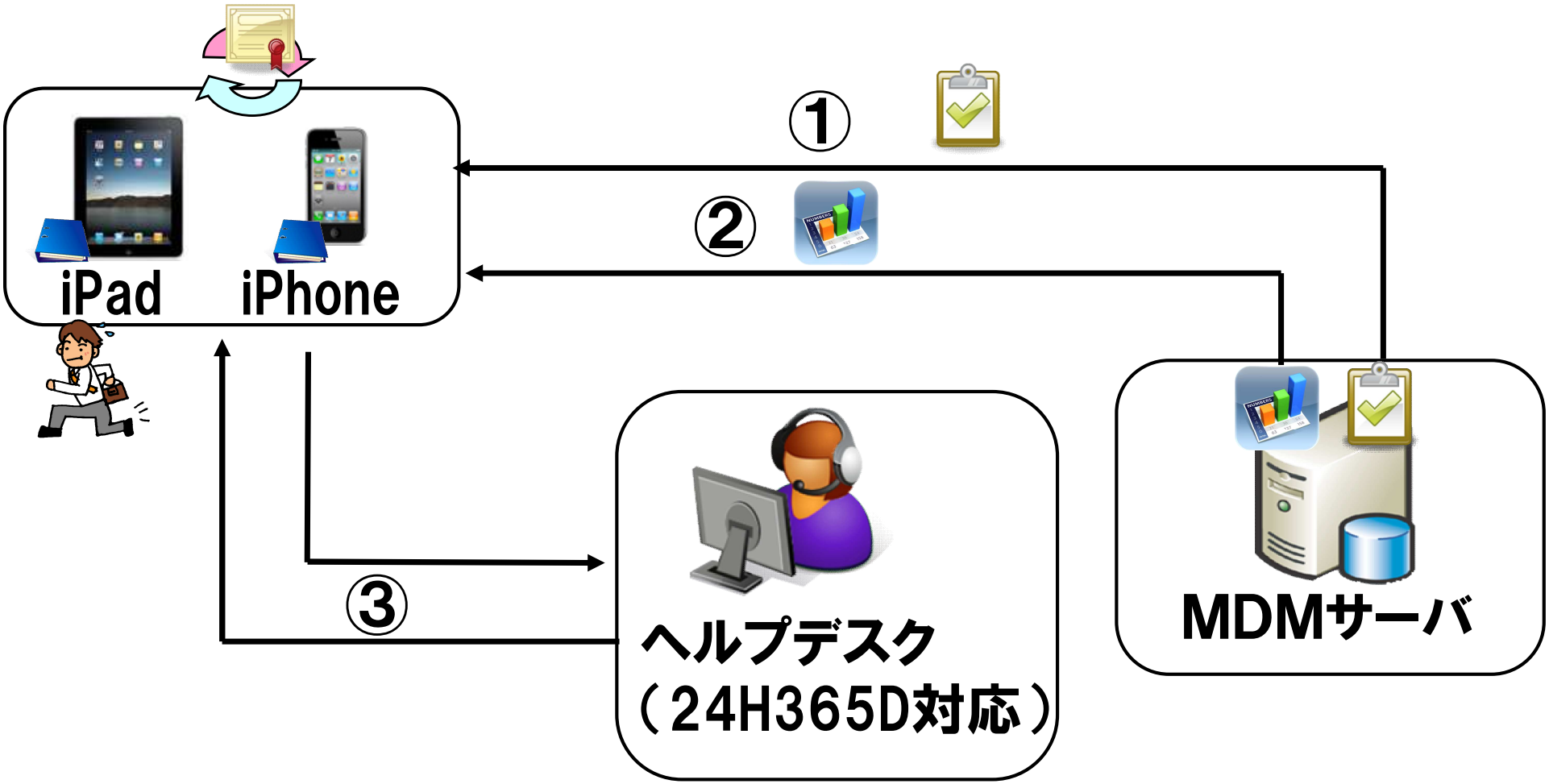
社内LAN環境への接続

- 社内Wi－Fi環境へ接続（接続情報配布）
- リモート環境からの接続（接続情報配布）

※MDM管理下から外れると接続不可（自動的）

利用イメージ（2012年）

①グループ共通のセキュリティポリシー適用
②アプリケーションの配布
③紛失・盗難時にスマートデバイスの情報を遠隔で消去



iOS展開後の課題と対策（2013年）

RICOH
imagine. change.

展開後、利用者や各部門のITサポートメンバーから懸念事項（要望）を受け、一部ルールの見直し

＜課題と対策＞

- スマートデバイスへのポリシーが、厳しく利便性を損ねている。
  - パスワードポリシーを改訂（一部強化）
  - アプリインストールや利用制限を廃止

- 製品開発やデモで利用しているデバイスに対して、ルールが厳し過ぎる。
  - バックアップの制限の緩和
  - 製品開発に限りOSのバージョン制限を緩和

Androidへの対応（会社資産デバイス）（2012年）

RICOH
imagine. change.

Androidの利用に向けた検討を開始（2012年11月～）

＜検討項目＞

- セキュリティポリシーの策定
  iOS向けに策定したセキュリティポリシーをAndroid用に見直し
- ウィルス対策ソフト
  PC同様にウィルス対策ソフトを一本化するか
  キャリア提供のソフト利用では？
- Android機器の調査
  セキュリティポリシーの適用が全てのモデルに可能か
  仮にモデルごとに対策が異なる場合、対象機器を絞るべきか

Androidの展開を開始（会社資産デバイス）（２０１３年）

RICOH imagine. change.

セキュリティポリシーは、１種類

- データ保存することを前提として策定

ウィルス対策ソフト

- キャリア提供のソフトを利用する

Android機種

- OSのバージョンは、最低バージョンを定義（Ver４．１以上）
- 機種は、ISMC評価機種を入手し提示

＜利用開始＞

２０１３年４月スタート

運用イメージは、iOSと同一とした。

目　　次

- 会社概要
- ITガバナンス方針（New　Workstyle）
- 方針の背景（日本ではなく世界に学べ）
- スマートデバイス管理の現状
- BYOD実現に向けての取り組み
- まとめ

BYOD(個人資産デバイス)への対応

RICOH
imagine. change.

＜BYODへの対応に向けて＞

- **ニーズ調査**
  - 個人のスマートデバイスをほんとうに使いたいのか
- **労務上の問題をどうクリアするか**
  - どこまで労働(残業)として、認めるか
  - 通信費用の負担は、どうするか
- **情報のアクセスをどこまで許すか**
  - スマートデバイスにデータを残す場合、紛失時の対策としてリモートロック・リモートワイプが必要となるが、許容されるか
- **BYODのコストは、いくらか**
  - 会社資産のデバイス展開と比べ安くなるのか(運用コスト含む)

BYOD(個人資産デバイス)への対応

RICOH
imagine. change.

＜調査の結果、必要と判断した場合＞

- BYODのアクセス方式の決定

  データを残す方式(社内LANへの接続を許可)

  データを残さない方式(社内LANへの接続は不可)

- リモートワイプについて、利用者と合意する。

  利用は、事前に念書にサイン(トラブル防止)

- サポートの範囲を明確にする。

  一般的な操作・アプリに対する問合せは、対象外

BYODの現状と今後

	PC	スマートデバイス	携帯
			
現状	● 個人資産は設置場所固定 ● アプリ、社内同等(一般事務業務) ● ネットワーク接続(社内:無線LAN・社外:VPN)	● 会社支給のみ ● メール・スケジューラ・シンクライアント・専用業務アプリ ● ネットワーク接続(社内:無線LAN・社外:VPN)	● 個人資産も可 ● メール・スケジューラ限定 ● ネットワーク接続(インターネット:SSL)
今後	● 持出し利用可? 2013年度内判断	● 個人資産も可 2013年10月	● 終息 (スマートデバイスに吸収)
キーワード	● HDD全体の暗号化 ● シンクライアント	● MDM管理 ● シンクライアント ● 専用アプリの活用	● CACHATTO

MAM展開後の利用イメージ

RICOH
imagine. change.

社外クラウドサービス

Office 365　Google Apps　LotusLive

社内アプリ（業務利用）

メール/スケジューラ　情報共有　業務アプリ

インターネット

リモート・
社内LAN

社有デバイスと個人デバイス（BYOD）を業務活用

社内

タブレット型

スマートフォン

モバイル

セキュリティポリシー運用

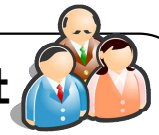
ヘルプデスク
（24H365D）

セキュリティポリシーとウィルス対策ソフトでセキュアな利用

アプリインストール

配信

グループ各社
・申請
・活用ガイドラインの
　遵守



各種
申請

IT資産管理システム
・申請受付
・台帳管理
・ライセンス管理

導入　活用　廃止　管理

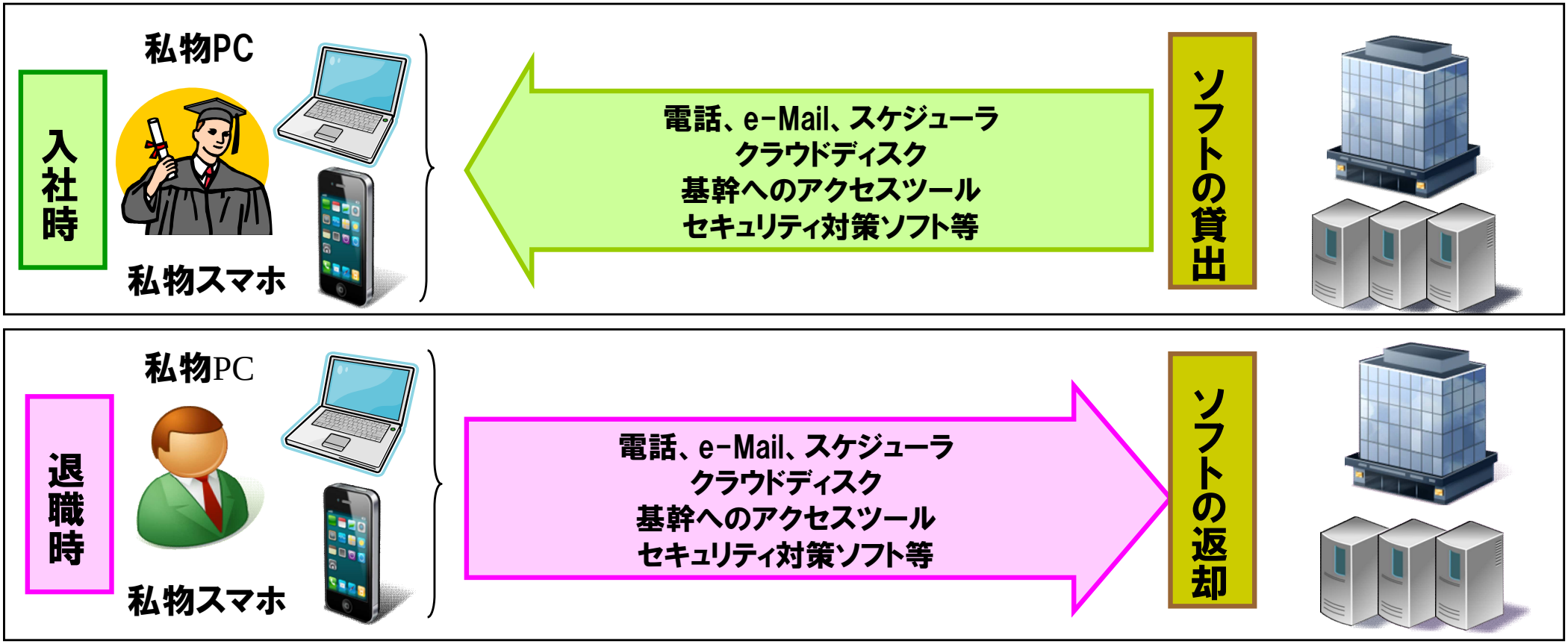
ライフサイクル管理

自動
連携

管理ツール（MDM）
・セキュリティポリシー配信
・必須アプリ配信
・インベントリ収集
・紛失対応（初期化）

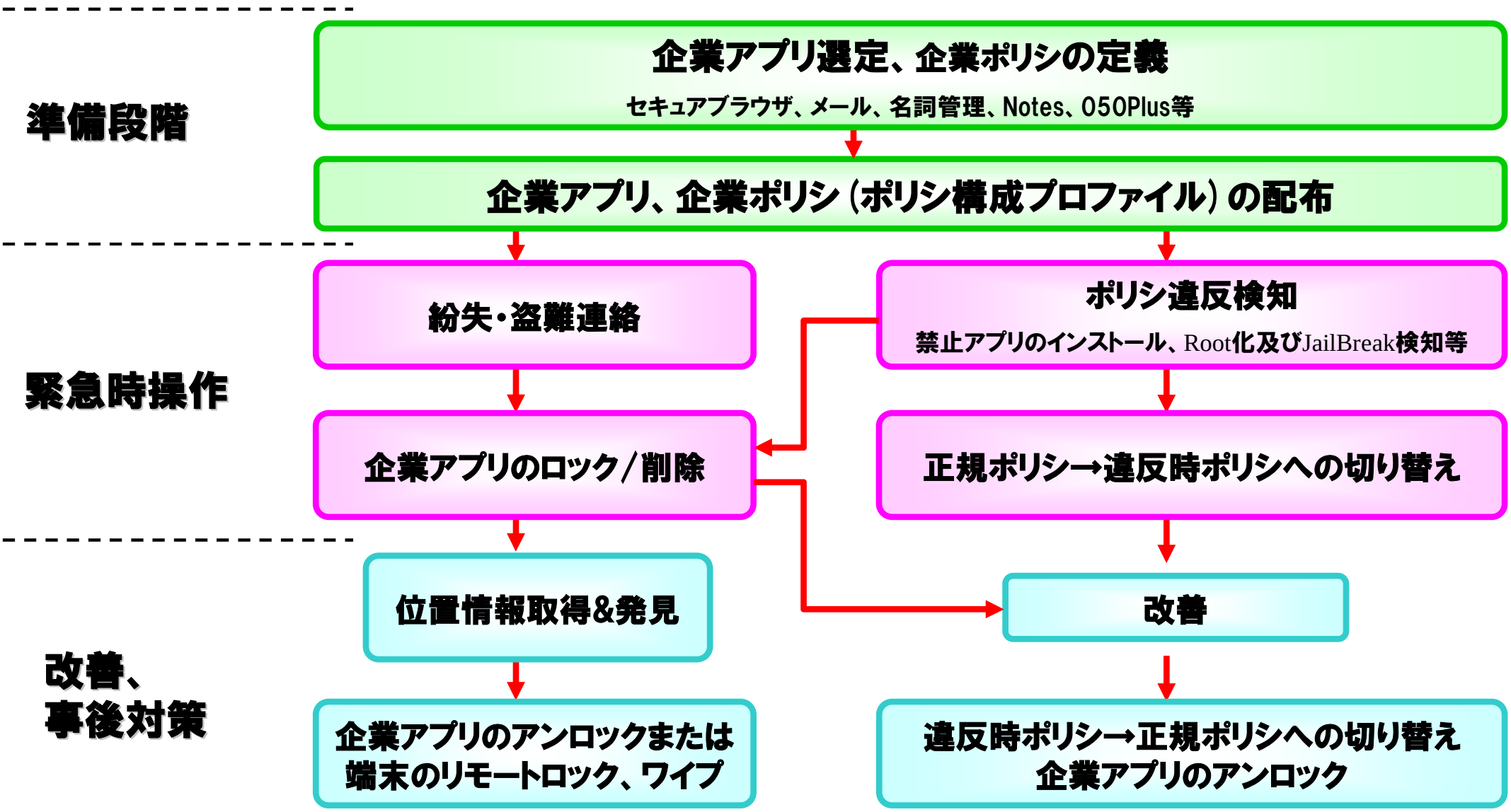
社内アプリケーションストア
セキュアなアプリを利用者に展開

そもそもBYODとは？



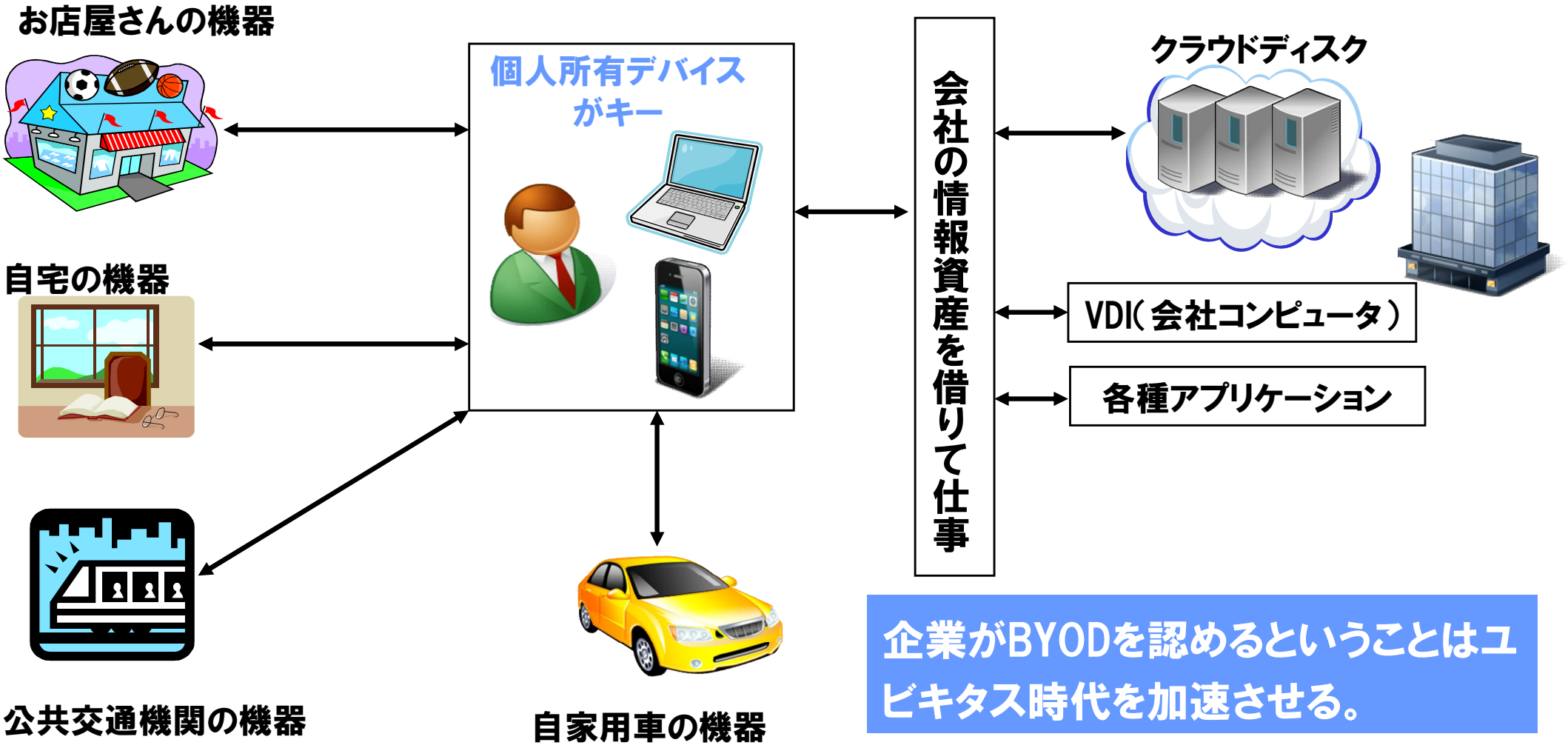
BYODとは社員が入社時に企業側は業務に必要なソフトウェアを貸し、社員が退職する時はそれらのソフトを返却する。すなわち企業がBYODを行うという事は、従来行っていた**IT資産管理から、ソフトの貸出管理すなわちMAM（Mobile Application Management ）に変わる事**を意味している。

MAM(Mobile Application Management)管理の流れ(案)



BYODの行き着く先はユビキタス時代

ユビキタス（Ubiquitous）とは、「いつでも、どこでも、だれでも」が恩恵を受けることができるインタフェース、環境、技術のことである。ユビキタスは、色々な分野に関係するため、『ユビキタスコンピューティング』、『ユビキタスネットワーク』、『ユビキタス社会』のように言葉を連ねて使うことが多い。



企業がBYODを認めるということはユビキタス時代を加速させる。

目　　次

- 会社概要
- ITガバナンス方針（New　Workstyle）
- 方針の背景（日本ではなく世界に学べ）
- スマートデバイス管理の現状
- BYOD実現に向けての取り組み
- まとめ

まとめ

Anytime
Anywhere
Any device

リコーは、クラウド時代を先取りし

- BYODを業務で活用できないか。
- BYOD利用によるワークスタイルの変革から「いつでも」「どこでも」簡単に使えないか。

を目指して、活動していきたいと思っています。

RICOH

ご清聴ありがとうございました