クラウド・イノベーション・シンポジウム

BYODでコスト削減を実現する クラウド型スマートフォンソリューション

株式会社ネクストジェン
事業戦略室　クラウドサービス事業本部
牧野 俊雄
2012年7月6日

本日の内容

- **イントロ**
  - ネクストジェン会社紹介
  - 日本スマートフォンセキュリティ協会(JSSEC)におけるネクストジェンの活動内容
- **スマホトレンド説明**
  - スマートフォンを取り巻く環境
- **クラウドサービス動向**
  - クラウドサービスによるワークスタイルの変革
- **スマートフォンの導入におけるセキュリティ面からの考慮点**
- **スマートフォン&タブレットの業務利用に関するセキュリティガイドライン**
- **BYOD**
  - BYODによるワークスタイルの変革
- **U3 Voice(ユーキューブボイス)紹介**
  - クラウドPBX
  - ベーシック
  - ゲートウェイ
- **まとめ**

ネクストジェン会社紹介

ネクストジェン会社概要

株式会社ネクストジェン（ジャスダック上場）

- 設立　：2001年11月16日
- 所在地　：東京都千代田区麹町
- 代表取締役社長　：大西 新二
- 従業員数　：75名（2012年5月末現在）
- 事業内容　：ＮＧＮ（次世代通信網）に関わるソフトウェア製品の開発・販売・保守サポート及びコンサルティング
- 筆頭株主　：サクサ株式会社

ネクストジェンソリューション一覧

主な製品			
シリーズ名	概要	サービス内容	製品概要
U³ Voiceシリーズ	加入者間通話無料のマルチキャリア対応 スマートフォン向けクラウドサービス	IP電話サービス	ベーシック、オフィス、クラウドPBXのニーズに合わせた3タイプのサービスをご提供
SIP/VoIPセキュリティ診断サービス	通信キャリア、開発ベンダ、一般企業向けに実施するSIP/VoIP環境のセキュリティや脆弱性診断サービスです。		

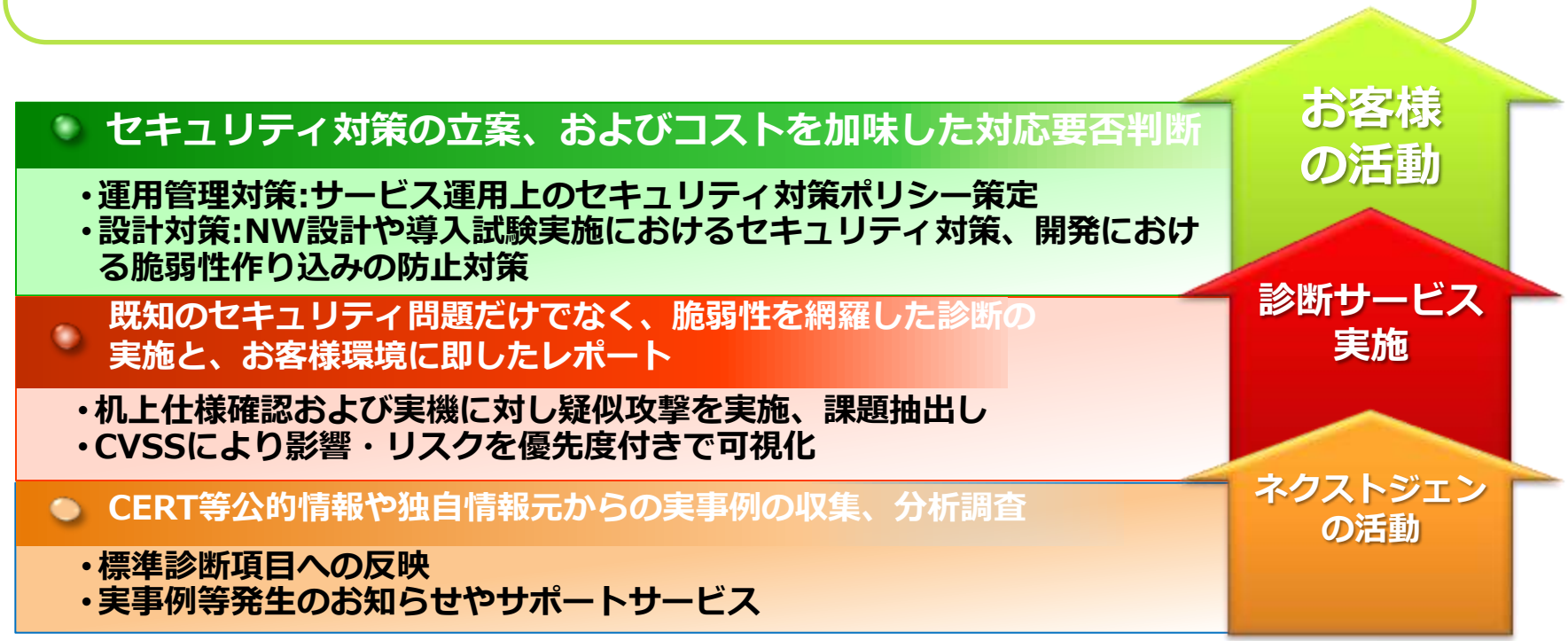
主なエンタープライズ向け製品			
シリーズ名	概要	製品	製品概要
E1000	エンタープライズ向けIP電話サーバ およびIP電話事業者接続ゲートウェイ	NX-E1000	ビジネスで求められる電話機能をSIPサーバ上で実現
		NX-E1010	IP電話事業者と企業内のIP電話サーバと相互に接続するサーバ IP電話事業者毎に異なる相互接続仕様をこの1台で吸収
C3000	通話録音サーバ	NX-C30	発信または着信の際に、利用者が操作することなく自動で通話を録音・保存する

主な通信事業者向け製品			
シリーズ名	概要	製品	製品概要
C1000	通信事業者向けIP電話サーバ	NX-C1000	ビジネスで求められる電話機能をサーバ上で実現する通信事業者向けSIPサーバ 1つのシステムを複数の企業で共有することが出来る
C2000	3rd Party Call Controlサーバ ※WebとIP電話の融合を実現	NX-C2100	クリックトゥダイヤル、クリックトゥカンファレンス、ペイパーコールといったインターネットと電話とを融合したサービスを実現
C3000	通話録音サーバ	NX-C300 NX-C3000	発信または着信の際に、利用者が操作することなく自動で通話を録音・保存する
B5000	相互接続サーバ（セッションボーダコントローラ）	NX-B5000	IP電話事業者のネットワークを外部からの攻撃から守るファイアウオール IP電話で用いるSIPプロトコルの仕様や実装の差異を吸収する
C6000	セキュリティ監視装置、診断ツール	NX-C6000 NX-C6100 NX-C6200	VoIP対応フォレンジック/IDSシステム SIP/VoIP試験装置 SIP Fuzzingツール

ネクストジェンの3PCCソリューション　C2000（応用編）

VoIPセキュリティ診断サービスの導入効果

- セキュリティ、脆弱性の課題の可視化
- 課題対応の必要性、優先順位に対し正確な判断を可能に
- 課題に対し適切なコスト範囲での対応を可能に
- 導入時や運用に必要なセキュリティポリシーを策定、PDCAサイクルの向上に



何故SIP/VoIP環境が狙われるのか

最近のSIPに関するセキュリティ事件

シスコiosの脆弱性を突かれての不正利用が発覚

2012年4月、欧州のとあるスモールオフィスがCisco製call gatewayを不正使用され、後日通話料$30,000の請求が来た事で発覚。

英BBC放送が電話を通じた高度なサイバー攻撃を受けたことを発表

2012年3月、 BBCがイラン向けに提供しているペルシャ語のサービスに対し、高度なサイバー攻撃が仕掛けられていると報じました。DoS/DDoSによる攻撃で、電話を使用したDoS攻撃も行われたことが示唆されている。

ロンドン警視庁とFBIの電話会議がハッカーグループ"Anonymous"に盗聴される

2012年2月、国際ハッキンググループへの対応について、議論していた内容の録音が約15分公開される

PBX設置から7日後に不正アクセスされ6時間で約2000ドルの被害

2012年1月、SBCとIP-PBXを用いたハニーポットを置いた実験。ハニーポット設置から7日後にはUserが乗っ取られて不正通話がなされ、6時間で約2000ドルの被害にあう。不正アクセスに対してサービスプロバイダは全く気付かず、クレジットカード会社からの警告により発見

企業用IP-PBXが不正アクセスされる実態について、テレビで特集が組まれる

2011年6月22日放送 テレビ東京 ワールドビジネスサテライト。2010年7月～2011年3月の間に計16万件の不正アクセス。また、不正アクセスを受けた企業は2日間で1300件の国際電話をかけられ、270万円の通話料が発生

米国TelePacificのネットワークが攻撃を受けてダウンしFBIが捜査

2011年3月にDDoS攻撃を受け数日にわたってダウン。数十万ドルの被害

IP電話の不正利用初摘発 他人ID使い料金免れた疑い

2010年8月、他人のＩＤでＩＰ電話使用、料金免れる　バングラデッシュ人の男逮捕

なりすましによる「So-net フォン」への不正アクセス及び不正利用発覚

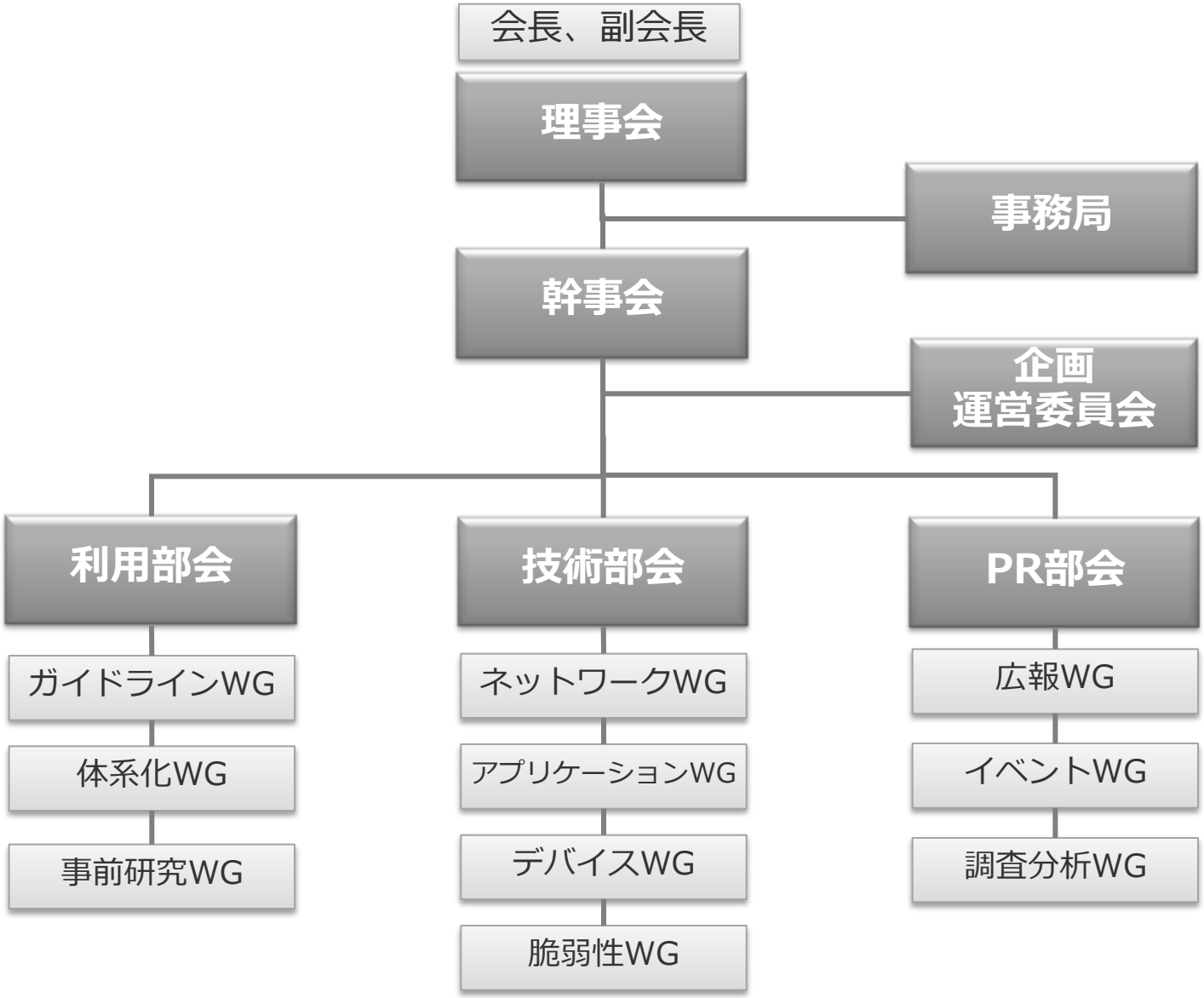
•2010年7月、So-net ID/パスワードを不正に入手し、So-net フォンサービスへ加入。451ユーザに対し2,311の不正アクセス、339の不正利用があったことが発覚。
•Number HarvestingによるSo-netフォンユーザの情報入手の可能性あり。

日本スマートフォンセキュリティ協会(JSSEC)における ネクストジェンの活動内容

日本スマートフォンセキュリティ協会（JSSEC）

急速に普及するスマートフォンの利便性の裏に潜むリスクに対し、発足来、会員企業120社が分担して、利用と技術の両面からこれらのリスクを体系立てて、政府・関連機関・会員企業・一般向けにガイドラインや提言書、刊行物、TV報道などの形にして告知、課題提起、検討結果の発表などを行っている団体。

JSSEC組織（2012年度）



JSSECにおけるネクストジェンの活動内容

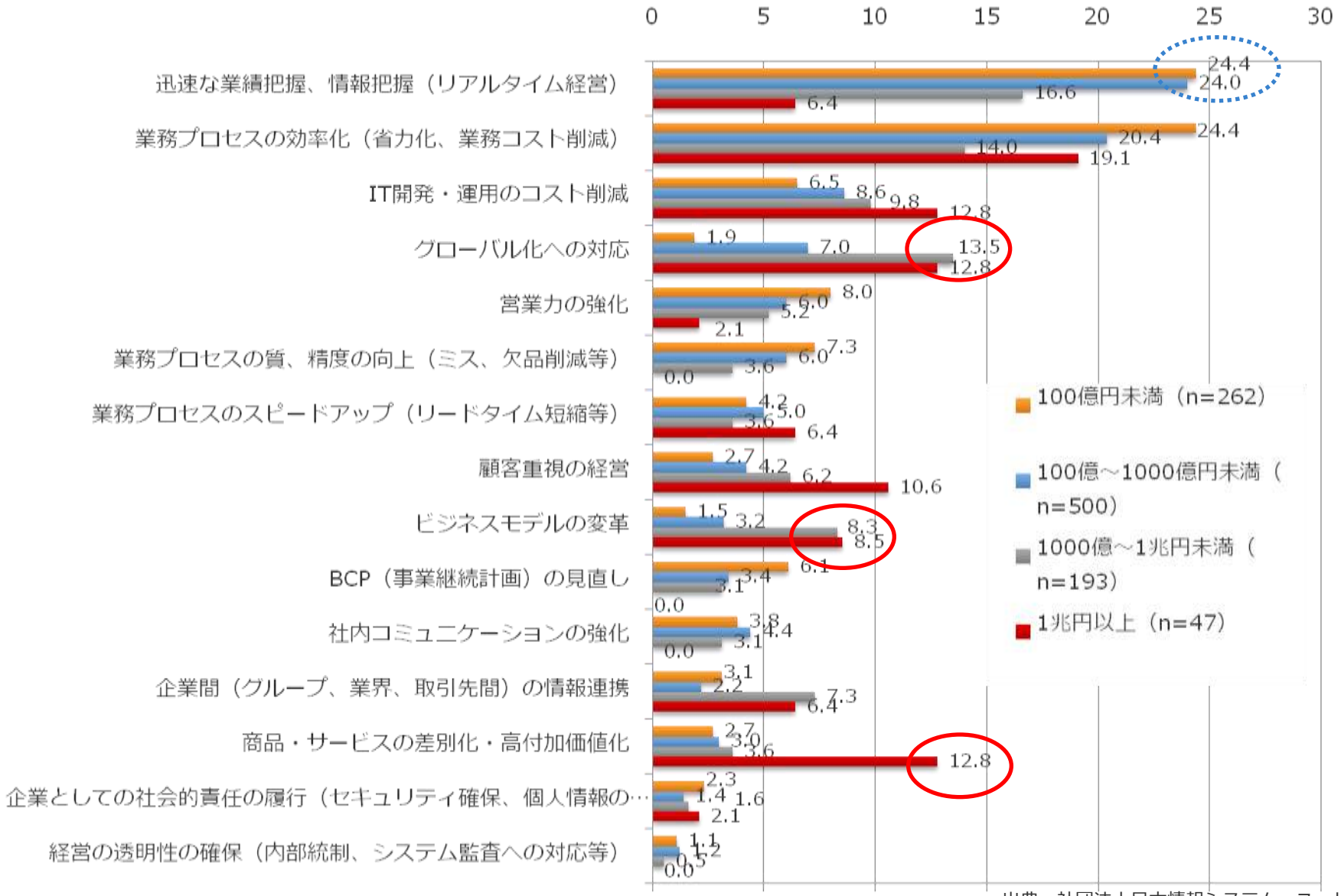
- 代表取締役社長　大西 新二
  - JSSEC 理事
- 事業戦略室室長 クラウドサービス事業本部本部長　牧野 俊雄
  - JSSEC 幹事
  - 利用部会副部会長、利用部会ガイドラインWGガイドラインTF
  - PR部会
- ネットワークセキュリティ事業本部本部長　杉岡弘毅
  - 技術部会脆弱性WG
- 事業戦略室副室長　二村 廉太
  - 技術部会ネットワークWGネットワークタスクフォース
  - 技術部会デバイスWG MDMタスクフォース
  - 技術部会デバイスWG端末堅牢化タスクフォース
- 事業戦略室　浅利 レナ
  - PR部会広報WG

ネクストジェンによるガイド類の執筆

- 2011年12月11日
  - スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン
  - 牧野
- 2012年6月19日
  - スマートデバイス堅牢化ガイド【β版】
  - 二村
- 2012年6月26日
  - MDM導入・運用検討ガイド【β版】
  - 二村
- 2012年7月初旬公開予定
  - スマートフォンネットワークセキュリティ実装ガイド【β版】
  - 二村

スマートフォンを取り巻く環境

売上高規模別
IT投資で解決したい中期的な経営課題



出典：社団法人日本情報システム・ユーザー協会
第18回企業IT動向調査2012（11年度調査）

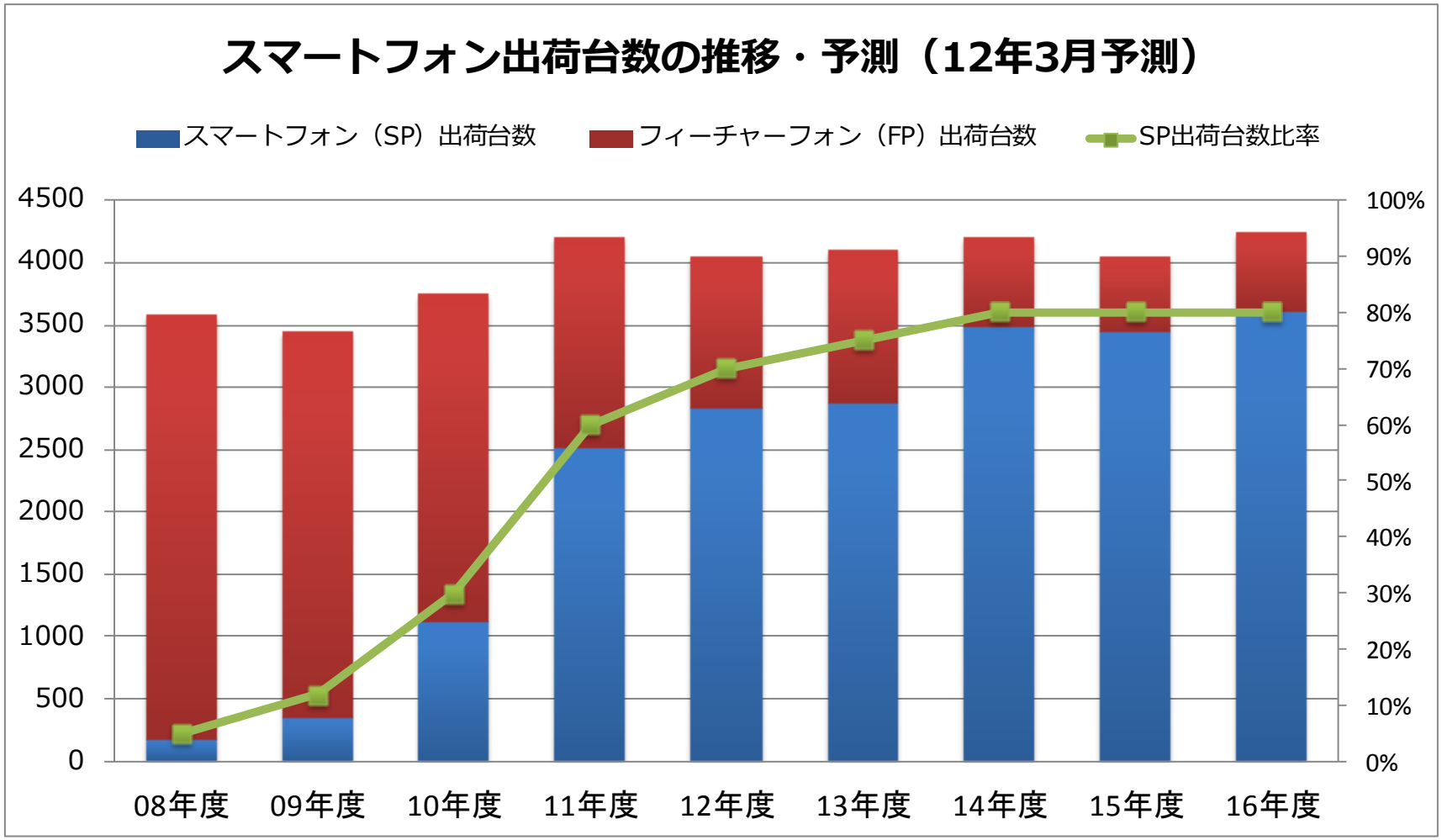
スマホによるワークスタイル変革例

- コミュニケーションの活性化と業務効率化
- 意思決定の迅速化
- 外出時の移動効率化
- ペーパレスによるコスト削減と業務効率化

仮に1人あたり1日に1時間の削減ができた場合、
月では約20時間（20営業日と仮定）の削減
従業員が500人と仮定すると、月あたり1万時間
（1,250営業日）分の業務効率化、コスト削減効果

満員電車の中ですら、メールやスケジュール程度なら確認できる利便性は圧倒的！

市場トレンド　スマートデバイス



出典：株式会社MM総研「**スマートフォン市場規模の推移・予測（12年3月）**」

スマホにシフトする3つの理由

- サービス事業者
  - スマホはパケット通信料が上限まで到達するケースが殆どで、音声+パケット通信料の合計では、フィーチャーフォンのARPUを上回る
  - 音声ARPUが下がり続ける中、データARPUをあげることで収益を伸ばさざるを得ない
- 端末メーカー
  - 日本独自の「ガラケー」の開発費は世界規格で生産するスマートフォンより割高
  - 生産台数も大きな開きがあるのでコスト面で勝負にならず、スマホへの移行が事実上唯一の選択肢
- 利用者
  - 提供者がスマートフォンにシフト
  - 一部機種では0円スマホも出現するなど価格的にもこなれてきた
  - おさいふケータイ、赤外線、ワンセグの3種の神器の搭載
  - キャリアメールのスマホへの搭載と移行

スマホの2つの側面

- 総務省様の定義
  - スマートフォンとは、従来の携帯電話端末の機能に加え、高度な情報処理機能が備わった携帯電話端末
- JNSA様の定義
  - スマートフォンとは、従来の携帯電話端末の機能に加え、高度な情報処理機能が備わった携帯電話端末
- JSSECでの定義
  - スマートフォンとは、従来の携帯電話の機能に加え、高度な情報処理機能が備わった携帯デバイス

スマホ＝高度な情報処理端末＋携帯電話

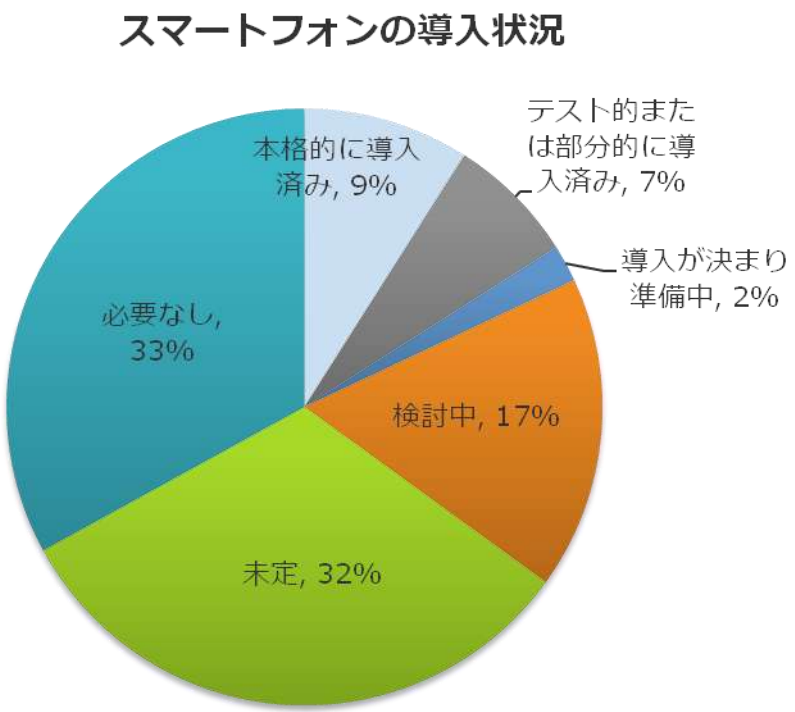
スマホの特性－タブレットとの相違

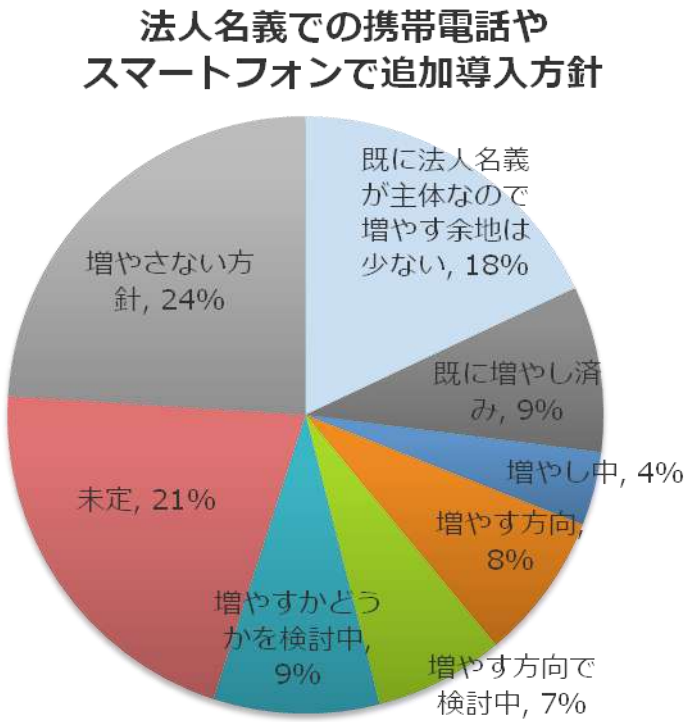
- できることはPCと同等
- **画面サイズが小さい**
  - キーボードは基本的には無い（SWキーボード）
- 記憶領域は少ない
  - 広大なクラウドストレージの入り口にもなっている
- **携帯性に優れる**反面、**紛失しやすい**
- 電源ONが常態なので、起動が早い
- **電源が入っている限り、**常時ネットワーク接続

スマホの最大の弱点は電源、MDMも電源が入っていなければ無力

スマホ企業導入率

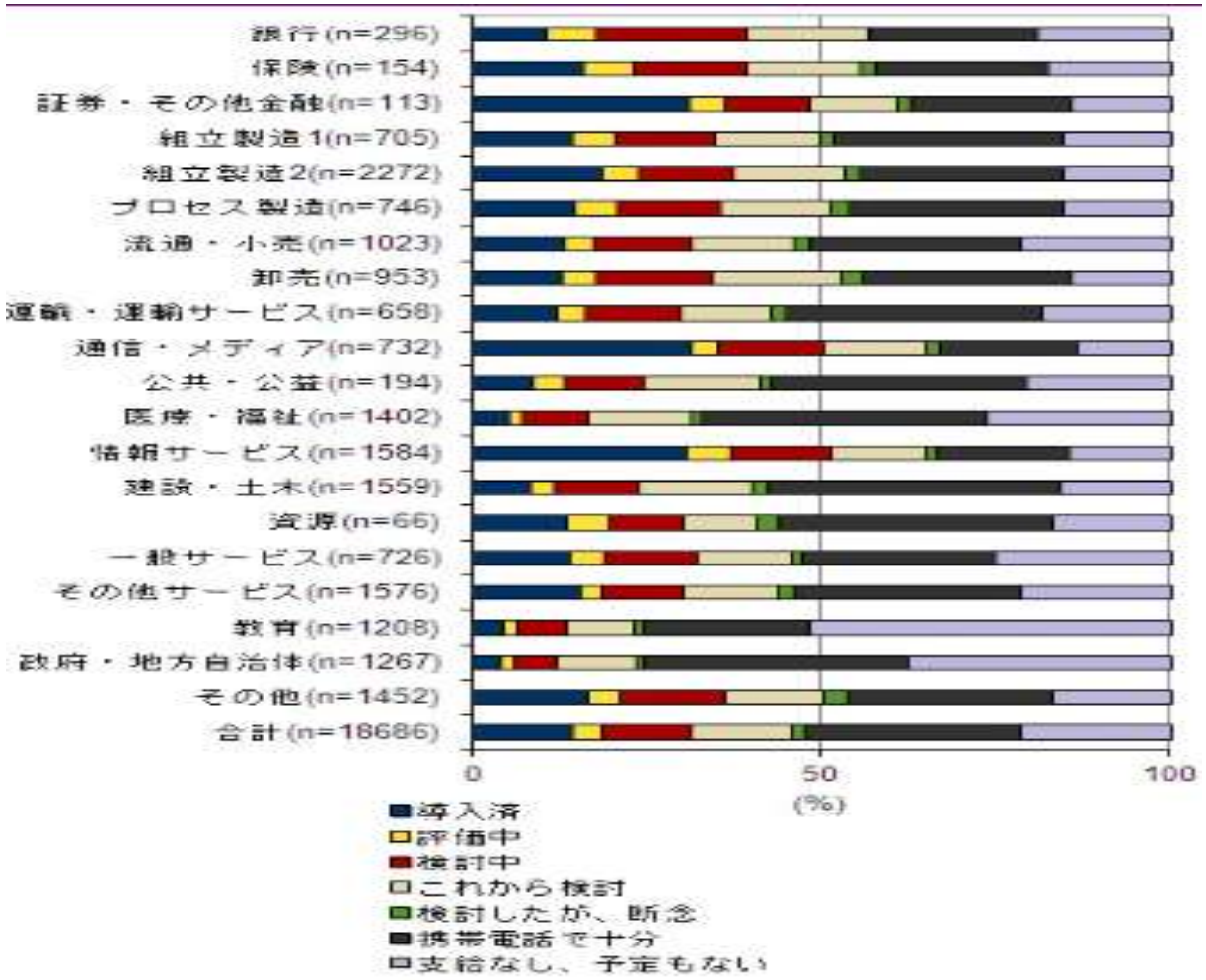
- スマートフォンの企業導入率は16%
- 37%が法人契約の拡大を実施・検討





出典：MM総研（goo）サーチによる調査　11月1日）

スマホ業種別企業導入率

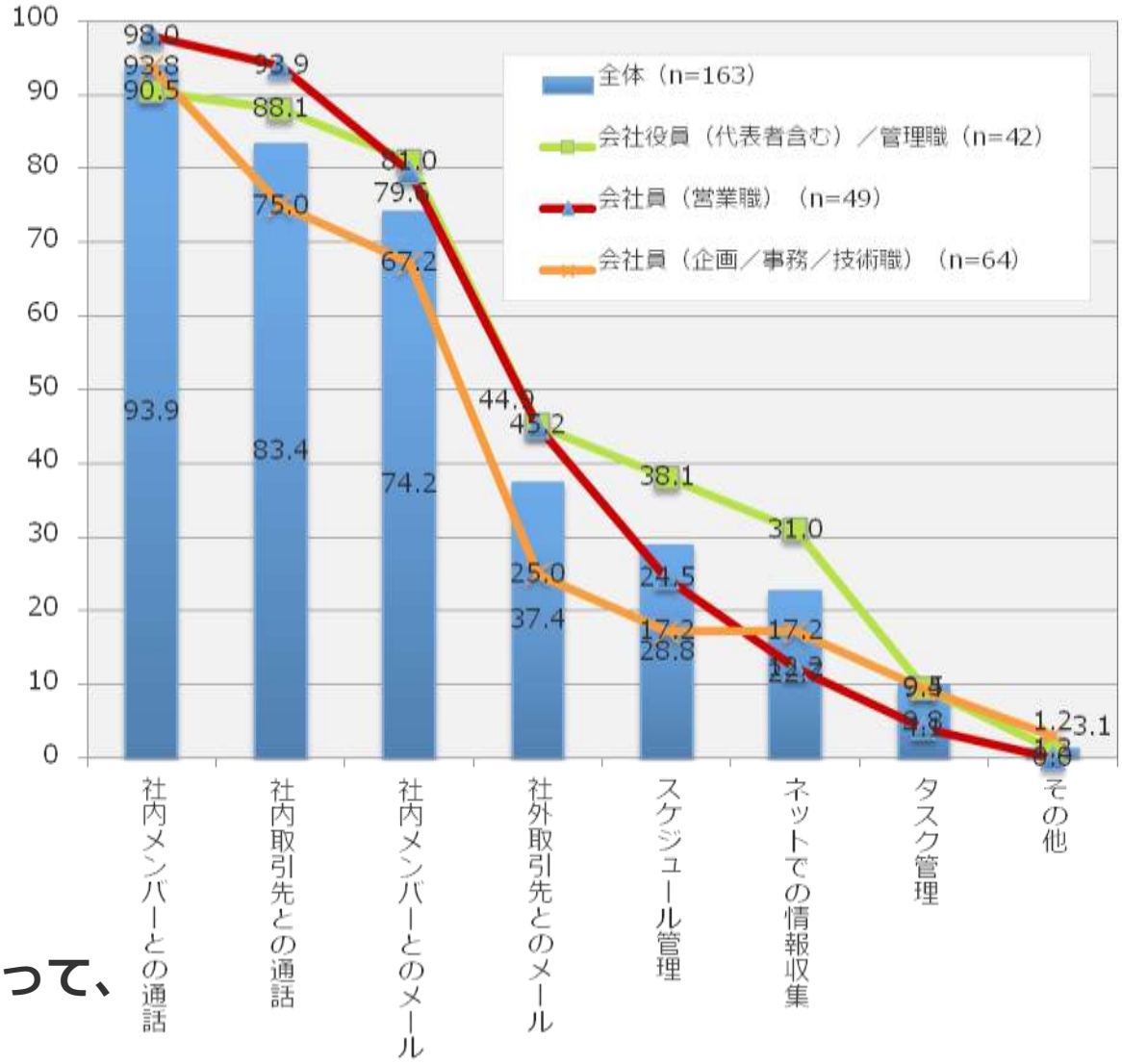


証券、通信・メディア、情報サービスの普及が進んでいる

出典：IDC Japan

会社から支給されているフィーチャーフォン、スマートフォンの用途

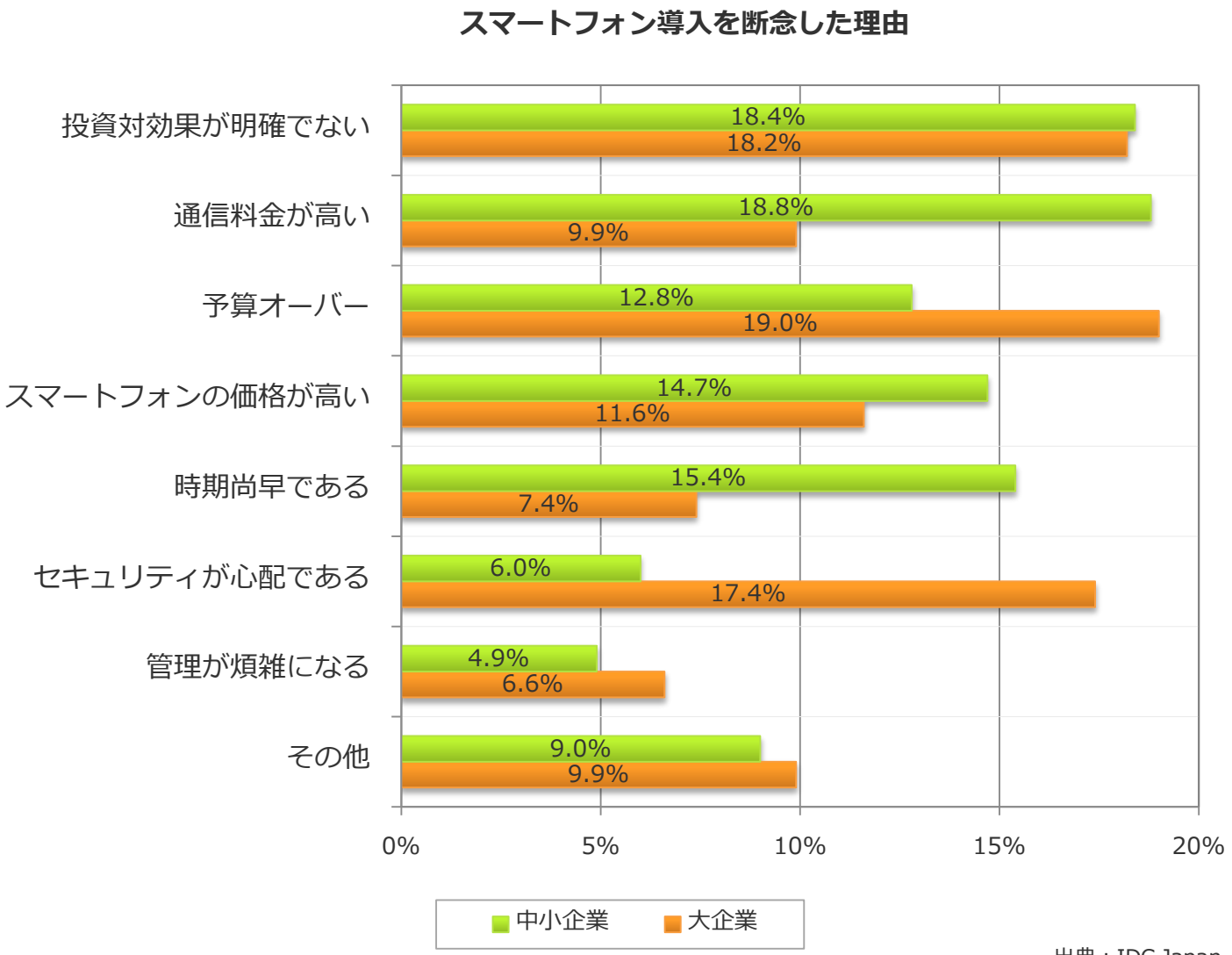
- 全体で見ると通話の用途が高い
- 「会社員（営業職）」は「通話」が高め。通話機能がメインとなるフィーチャーフォンの支給が多いことも関連している
- 一方、「会社役員／管理職」は「スケジュール管理」や「ネットでの情報収集」が高い傾向
- 職種によって仕事で必要な通信環境は変わってくる



役職、配布されている種別によって、利用用途に差がある

出典：IT PRO　2012011　対象：ネットマイルユーザーのスマホパネル560

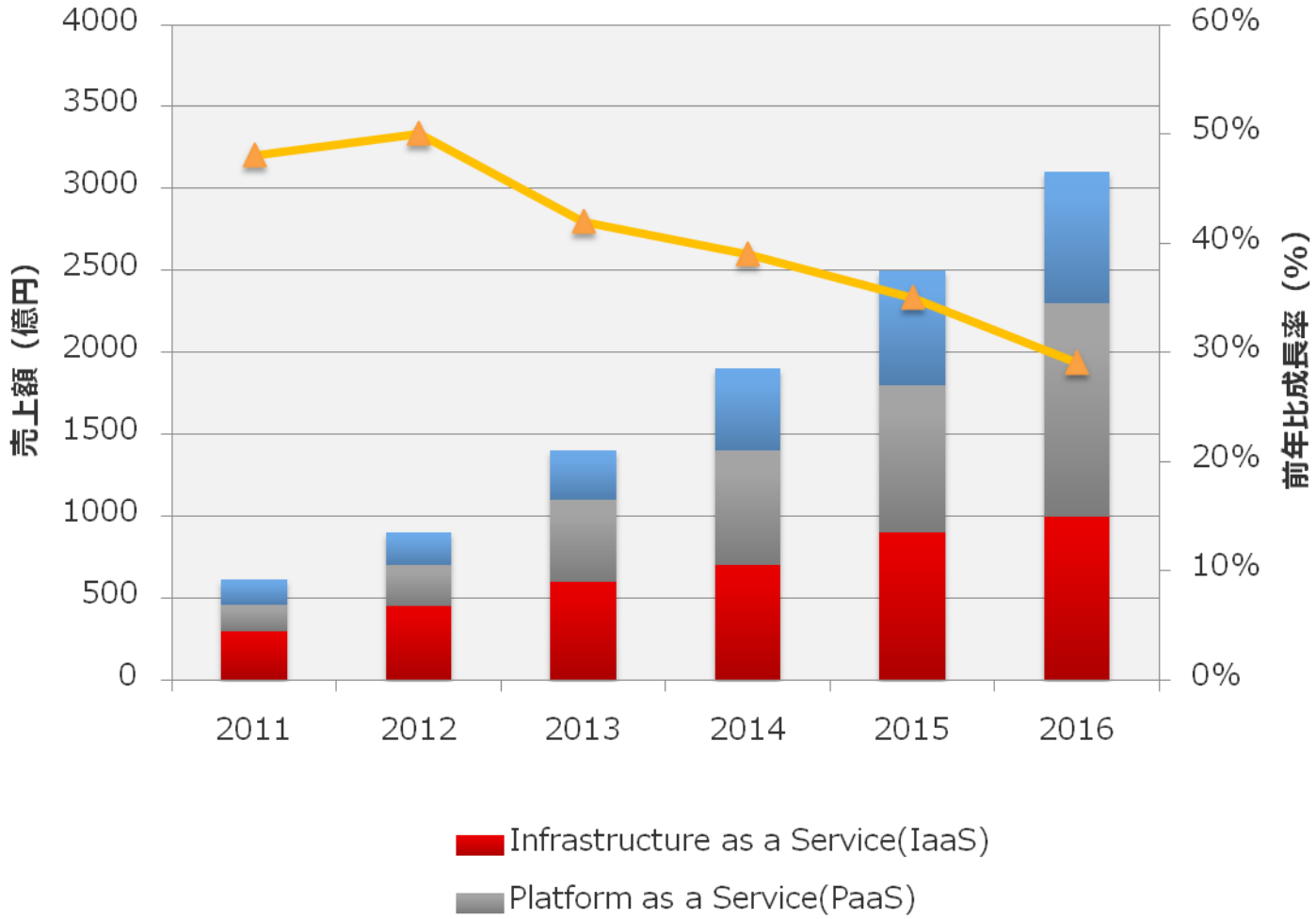
企業規模別スマホ導入断念の理由



出典：IDC Japan　November 2011

クラウドサービスによる
ワークスタイルの変革

市場トレンド　クラウドサービス



2012年→2015年で市場規模は約3倍に

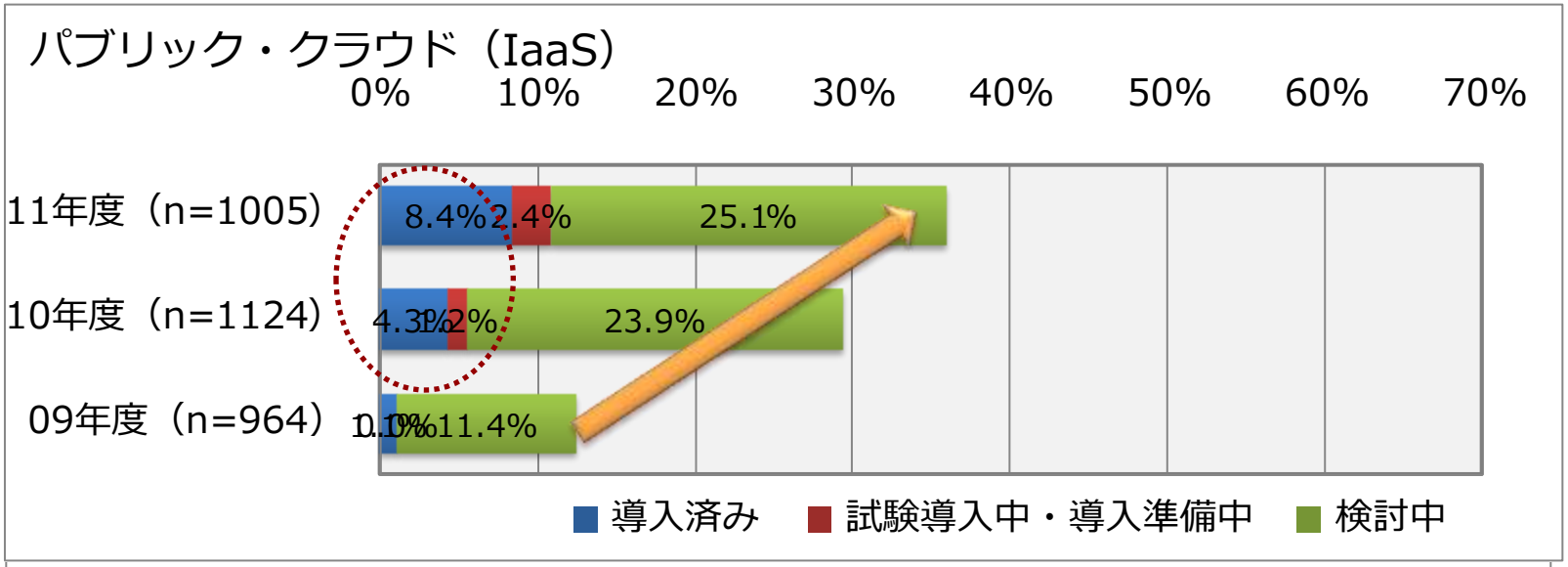
出典:IDC Japan　国内パブリッククラウドサービス市場予測

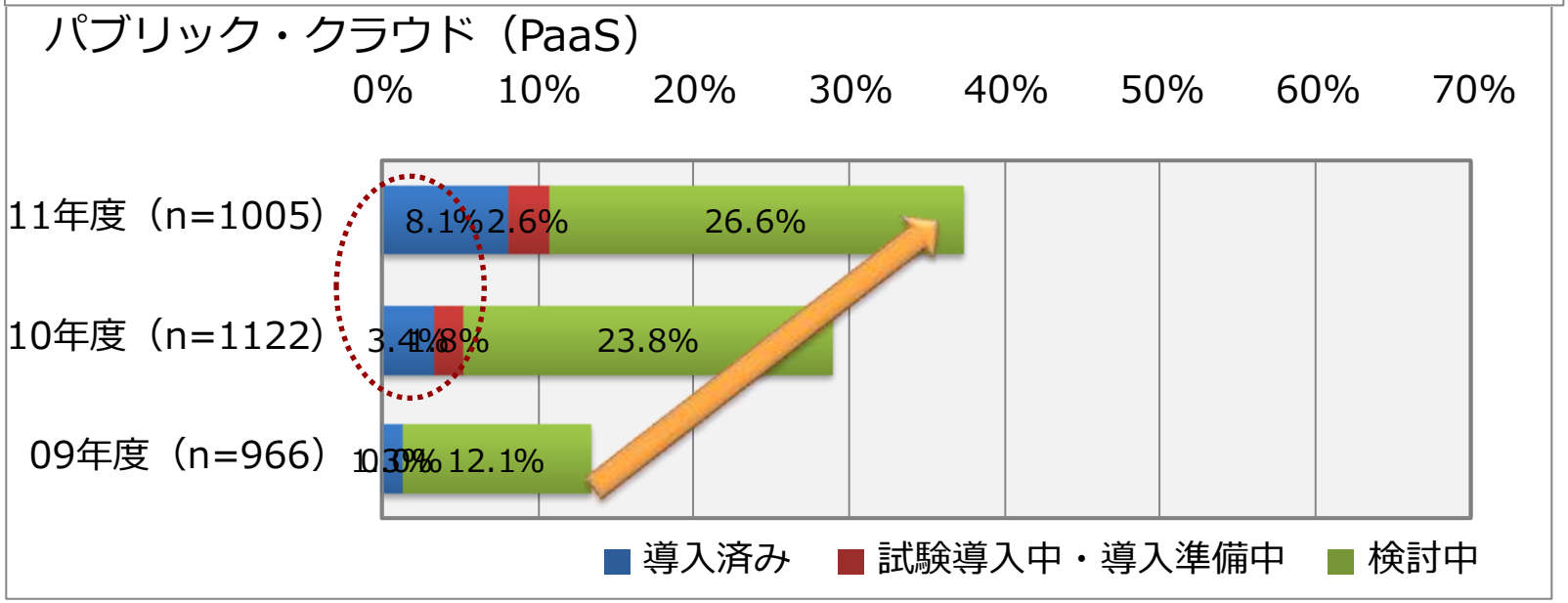
クラウドサービスの可能性

- 「これまでは最新の技術は、大手企業しか導入できなかったが、クラウドではすべての企業が民主的に、スピーディーに導入できるようになる点が異なる」
  - マーク・ベニオフ　CEO salesforce.com
- 常時ネットワーク接続された端末の爆発的な普及
- LTE/WiMAX等の高速通信の整備
- 格安のオンラインストレージ等、サービスの充実
- 大震災以降は、堅牢なDCでシステムを運用することへの理解が深まる

日本市場においても、クラウドサービス利用の垣根が低くなった

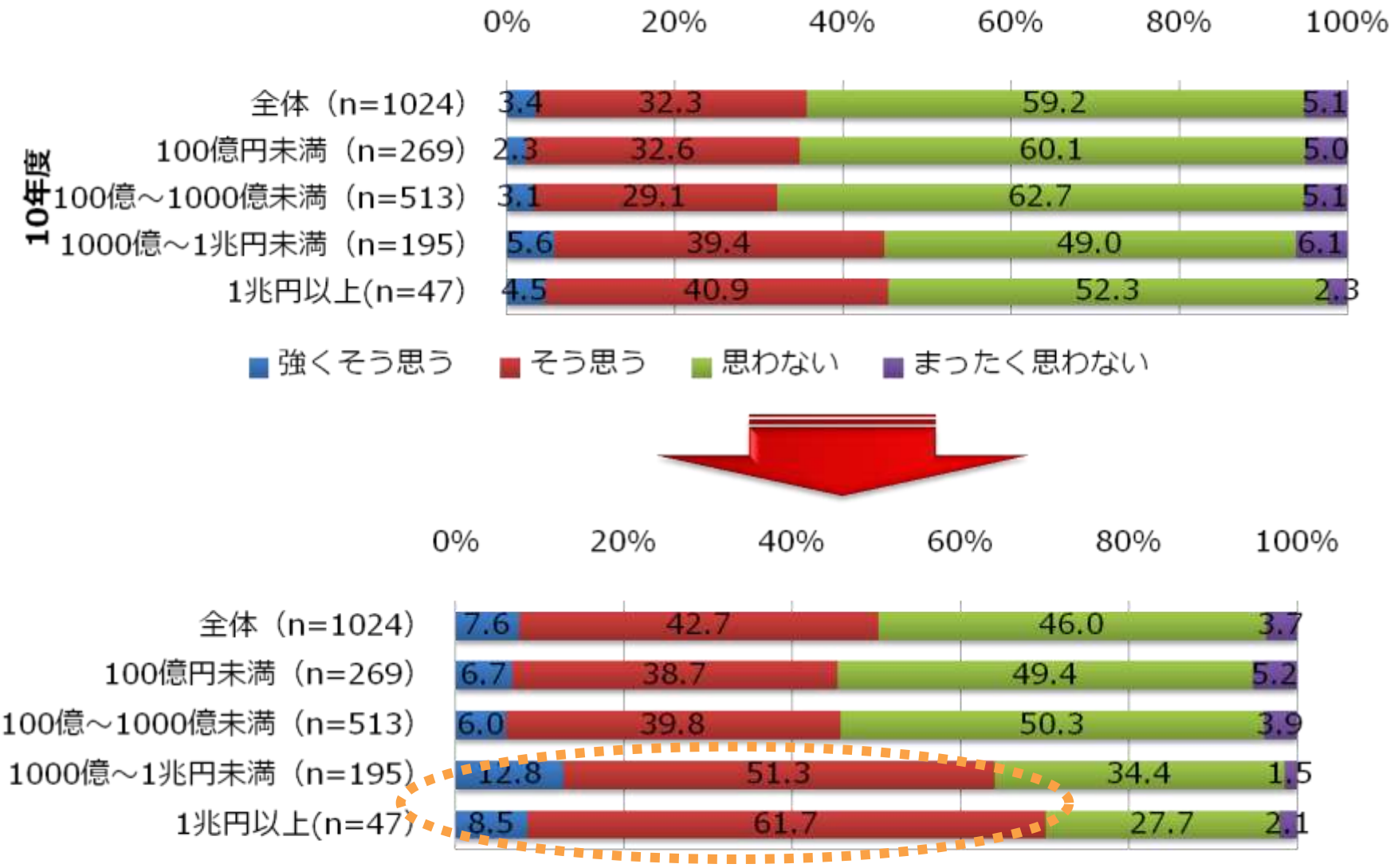
パブリッククラウドの導入検討状況についての年次変化





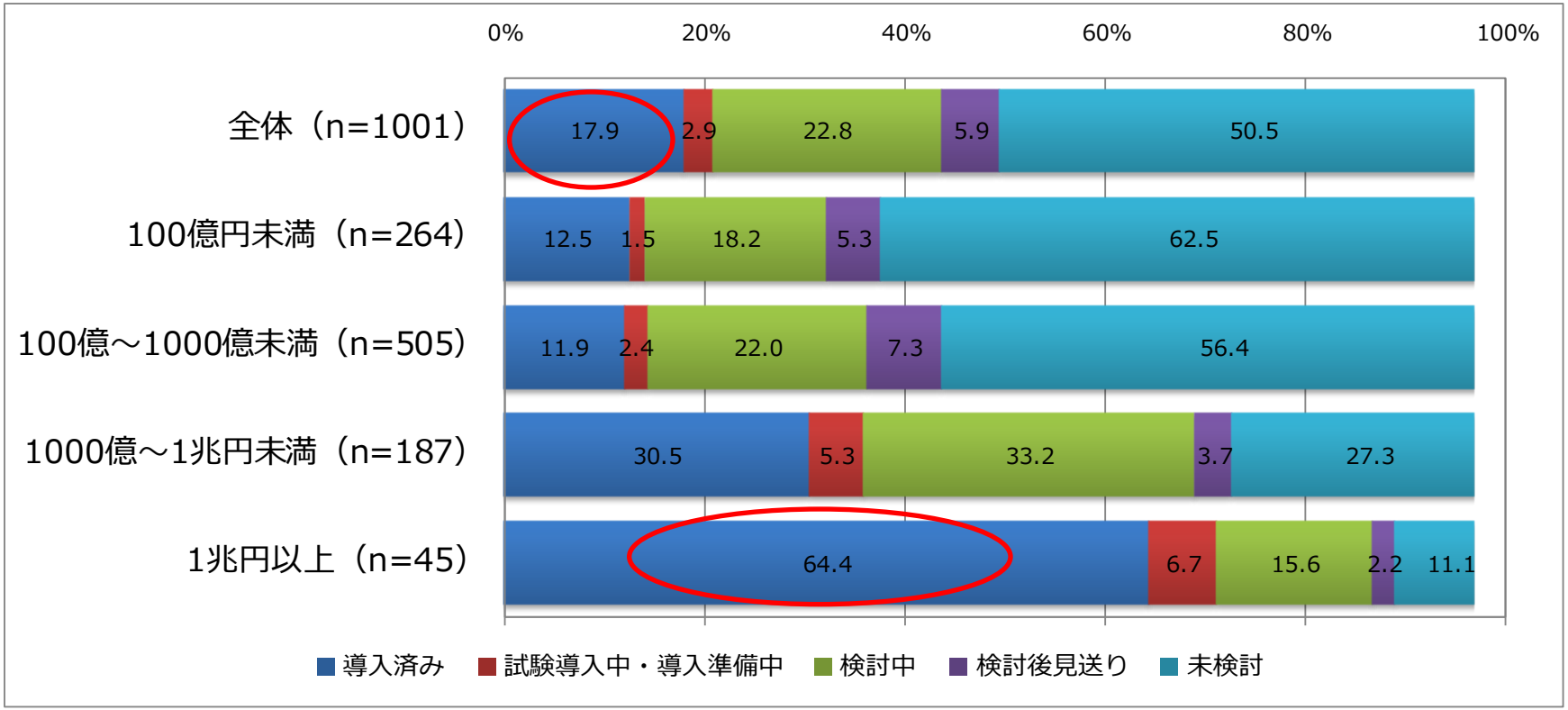
出典：社団法人日本情報システム・ユーザー協会　第18回企業IT動向調査2012（11年度調査）

導入には積極的になるべきだ（売上高別）



出典：社団法人日本情報システム・ユーザー協会
第18回企業IT動向調査2012（11年度調査）

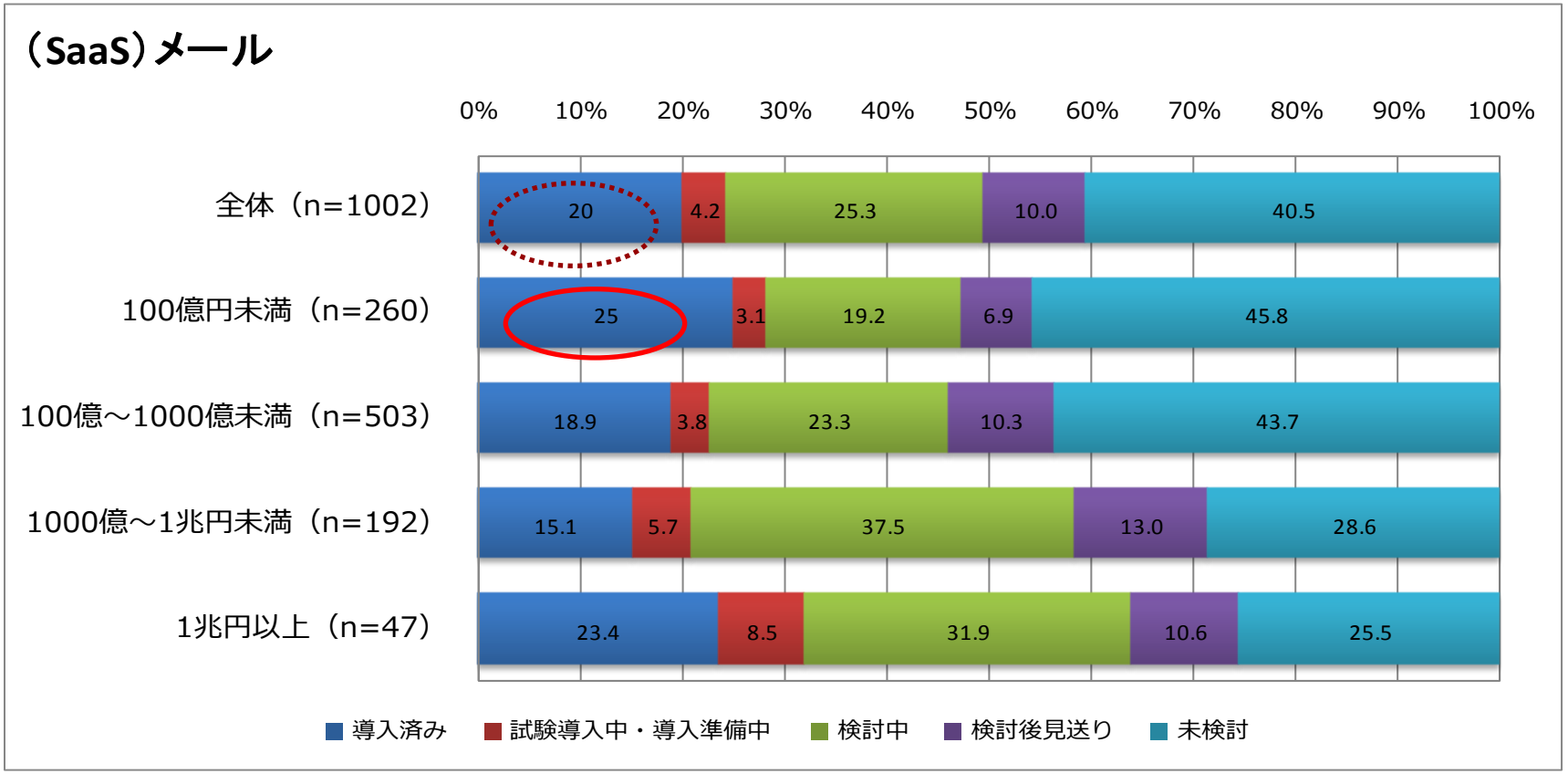
プライベートクラウドの導入検討状況（売上高別）



セキュリティ重視の大手企業はプライベートクラウド導入が中心

出典：社団法人日本情報システム・ユーザー協会
第18回企業IT動向調査2012（11年度調査）

パブリック・クラウド（SaaS）の導入検討状況（売上高別）



パブリッククラウドは、利用用途によっては中堅企業のほうが積極的

出典：社団法人日本情報システム・ユーザー協会
第18回企業IT動向調査2012（11年度調査）

スマートフォンの導入における
セキュリティ面からの考慮点

守るべきものは企業の情報資産

- **機密性（Confidentiality）**
  - 許可された者だけが情報にアクセス可能
    - 情報漏洩等
- **完全性（Integrity）**
  - 情報が正確かつ完全であることの維持
    - 改竄
- **可用性（Availability）**
  - 許可されたものが必要なときにいつでも情報にアクセス可能
    - サービス停止等

デバイスの紛失が問題なのではない

参考：総務省　情報資産の維持管理

情報資産のラベル付けと格納場所・アクセス方法

- 情報のラベル付け（例）
  - 極秘　　Top secret
  - 機密　　Confidential
  - 社外秘　　Internal use only
- 物理的な格納場所
  - 社内サーバ
  - ASP利用
  - プラベートクラウド
  - パブリッククラウド
  - Etc.
- アクセス方法
  - Local network
  - Remote access
    - VPN
    - Remote Desktop
    - Etc.

情報資産のラベリングと格納場所が決まれば、企業のセキュリティポリシーと照らし合わせて、アクセス方法とデバイスは自ずと決まってくる

各OS・アプリの特徴　スマホは黎明期

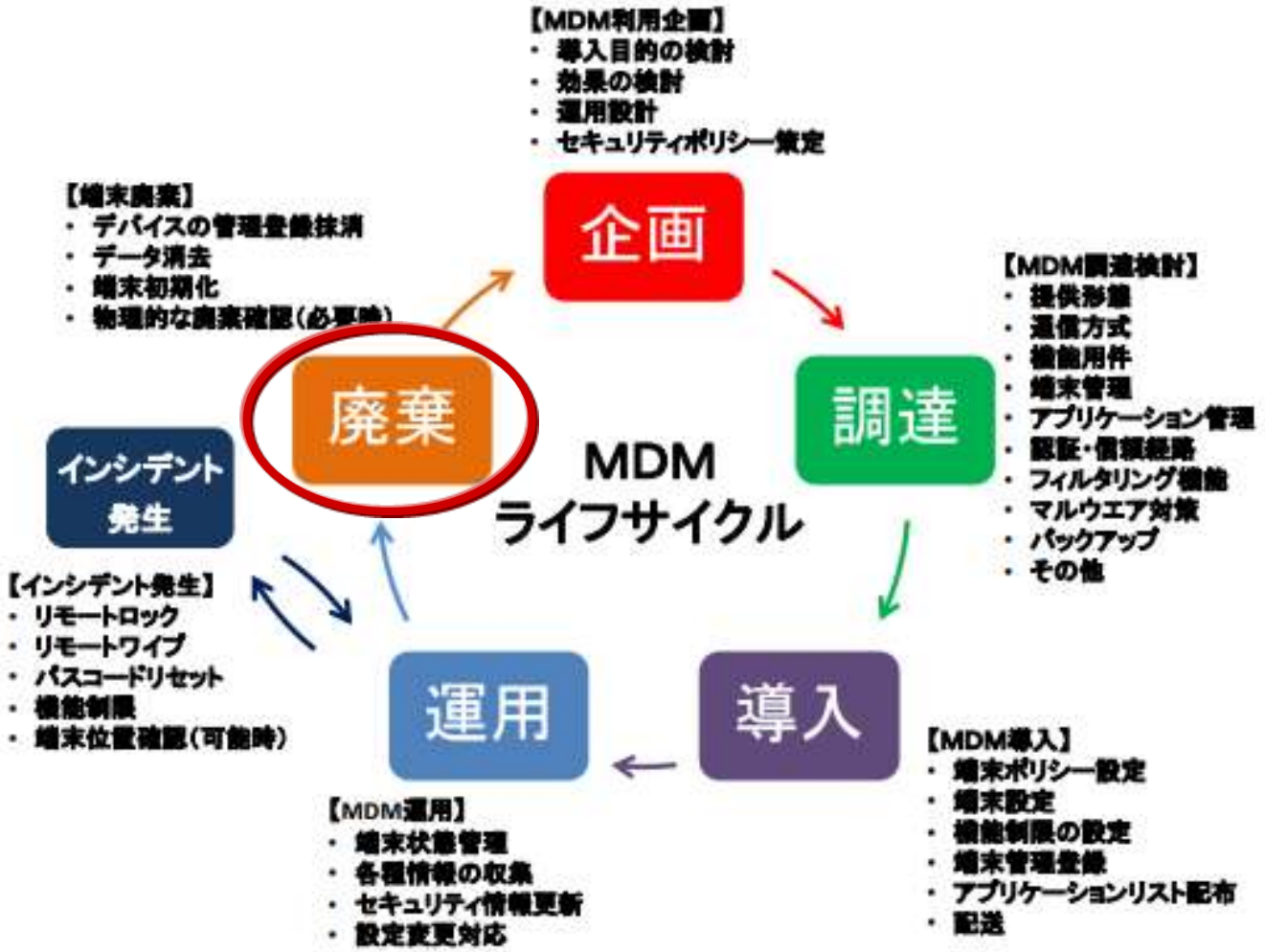
OS の種類	OS 提供元	特徴
iOS (iPhone/iPad)	Apple Inc.	OS、デバイス、アプリケーションマーケット全て垂直統合型で展開。iPhone/iPad 上でのみ稼動し、最新バージョンの適用が容易。
Android	Google	OS、デバイス、アプリケーションマーケット全て水平分業型で展開。デバイスの選択肢が豊富。オープンソースの OS であり、基本的には、各デバイスメーカーが独自に開発したデバイスにカスタマイズして搭載。OS バージョンが同一でも機種依存がある。
BlackBerry OS	Research In Motion（以下 RIM）	OS、デバイス、アプリケーションマーケットを、基本的には垂直統合型で展開。高次のセキュリティ機能を BES/BIS サーバで提供。現在は BlackBerry 上でのみ稼動。主要機種に QWERTY キーを搭載。
Windows Phone 7	Microsoft（以下 MS）	OS、デバイスは水平分業型で展開。デバイスの選択可。既存 Microsoft 資産と連携できる設計。METRO UI と Exchange 等による管理機能搭載。

提供元	マーケット	マーケットの特徴
iPhone/iPad	「App Store」	Apple 社が審査した他社のアプリケーションを登録。アプリケーションの配布や使用時には Apple 社と契約し、Apple 社が発行する証明書が必要。App Store から配布、課金。
Android	①Google 「Android マーケット」②各通信事業者等の運営するマーケット	① Google 社は審査せず、その活用は利用者裁量。 ② 通信事業者等が、それぞれの基準で登録。 配布・課金モデルあり。
BlackBerry	「App World 」	RIM 社が審査した他社のアプリケーションを登録。App World から配布、課金。
Windows Phone	「Marketplace」	MS 社が審査した他社のアプリケーションを登録。Marketplace から配布、課金。

発展途上のスマホは、PCと同様のセキュリティ対策は現状では取れない！

出典：日本スマートフォンセキュリティ協会「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」

MDMライフサイクル



BYODにおいては、特に機種変更や下取り時の情報漏えいに注意

出典：日本スマートフォンセキュリティ協会　MDM導入・運用検討ガイドβ版

スマートフォン&タブレットの業務利用に関するセキュリティガイドライン(抜粋)

日本スマートフォンセキュリティ協会
利用部会ガイドラインWG
ガイドラインタスクフォース

利用ガイドラインの基本方針

目的

・スマートフォン業務活用検討者/導入決定者の皆さんに
「気付いて」いただき、将来の判断基準となるよう構成。

「こういうことがしたい」→「こういうリスクがある」→「解決するためには」

対象

・OS　：iOS、Android、 BlackBerry OS、Windows Phone 7
・スマートフォンの資産形態：
①会社資産
②個人所有（BYOD：Bring Your Own Device)
・PCとの違い（**スマートフォンらしさ**）に焦点

第一版のもくじ （2011/12/1版）

1章. はじめに
1.1. 本ガイドライン利用にあたって
1.2 本ガイドラインの目的
1.3. 本ガイドラインが対象とする読者
1.4. 本ガイドラインが対象とする範囲
1.5. 本ガイドラインの構成

2章. スマートフォンの利活用によるメリット
2.1. 導入のねらいと理由
2.2. 活用例と効果
2.3. スマートフォンを取り巻く動向

3章. スマートフォンのしくみと概要
3.1. デバイスの特徴とOSの種類
3.2. アプリケーションとその入手形態
3.3. 通信形態とネットワーク
3.4. これまでのPCセキュリティとの相違

4章. スマートフォンの特性と留意点
4.1. 特性
4.2. 特性から見る脅威と対策
4.3. 将来における留意点

第一版のもくじ （2011/12/1版）

5章. 利用シーンから見る脅威と対策

5.1. アドレス帳を利用する
5.2. 電話を利用する
5.3. メールを利用する
5.4. スケジュールを利用する
5.5. ブラウザを利用する
5.6. ネットワークに接続する
5.7. 社内ネットワークを利用する
5.8. 組織契約のSaaS/ASPを利用する
5.9. アプリケーションを利用する
5.10. デバイスの機能を利用する
5.11. データの可搬媒体として利用する
5.12. バックアップを取る/同期する
5.13. 【参考】ｲﾝﾀｰﾈｯﾄｽﾄﾚｰｼﾞｻｰﾋﾞｽを利用する
5.14. 【参考】SNSを利用する

6章. ライフサイクルから見る脅威と留意点

6.1. 計画
6.2. 導入
6.3. 運用
6.4. 廃棄

7章. おわりに

7.1. 利用目的とセキュリティのバランス
7.2. 組織のセキュリティポリシーと意思決定
7.3. 情報収集継続の必要性

8章. 用語解説・付録

- 特性別 / 利用シーン別 対策チェックシート
- 手順書に記載する項目の例
- 誓約書に記載する項目の例
  （法人所有/BYOD）

利用シーンからの考察例

アドレス帳

- 電話、メール、SNS、インスタントメッセージなどの入り口として利用する機能や、利用履歴を記録する機能＝出口を持つ。
- データの保存場所は、デバイス、外部記憶媒体、外部サービスを選択可能。
- 外部サービスでは、他者と共有するサービスあり。
- 保存場所は利用者に分かりにくい。
- **アプリケーションの動きを調べて注意を喚起することが推奨される。**
  Androidの場合、アプリケーションをマーケットからダウンロードする際に、アプリケーションが適切なアクセス許可を求めているかも重要。

可搬媒体

- スマートフォン本体をデータ移動媒体として利用する場合をさす。
- 機能の一面として大容量のストレージである。
- 紛失時の影響度は、PC同等。
- デバイスやアプリケーションによっては、セキュリティ対策も可能だが、紛失時の対策は必須。
- 可搬媒体としての**使用は推奨しない。**

PCとも携帯電話とも違う管理スタイル

管理＝ライフサイクルのＰＤＣＡ

計画

目的を明確化する

・社内ルールを整備する
・利用マニュアルを整備する
・サポート体制を整備する
（ヘルプデスクや担当設置）
・教育を実施する

導入　PCとは手順が変わる

・利用開始手続きを行う
・備品を用意または装着する
・アカウントを取得する/させる
・デバイスを初期設定する
・デバイスのロック機能を有効にする
・メールアドレスを取得/設定する/させる
・アプリケーションを導入する
・デバイスを配付する

運用　先回りして考える

・デバイス情報を収集/監視する
・デバイスの機能を制御する
・OSのバージョンを管理する

廃棄　データを削除する

・デバイスの回収/廃棄、変更
・別部署への使いまわし

PDCAをまわしましょう

チェックシート/手順書/誓約書のイメージ

付録 A

A-1 特性別 対策チェックシート

推奨レベル：■強く推奨 □推奨

節番号	分類	脅威	対策 または [illegible]	推奨レベル
4.2	特性から見る脅威	デバイスの盗難、紛失	・デバイスをロック設定する。 ・ロック解除失敗時に強制的にデータを消去する。 ・本体および外部記憶媒体のデータ領域を暗号化する。 ・ユーザ ID やパスワードを非保存設定にする。 ・定期的にデータのバックアップをとる。	■ ■ □ □ □
		SIM カードの盗難	・通信事業者へ連絡し回線利用を停止する。	■
		水没や落下による故障	・定期的にデータのバックアップをとる。 ・落下防止用ストラップ等を装着する。 ・防水や耐衝撃性の高いデバイスを選択する。	□ □ □
		覗き見	・覗き見防止シート等を装着する。	□
		誤操作	・慎重に操作するよう注意を喚起する。 （静電容量方式を採用したパネルが多いため、静電気の影響を受けやすい）	□
		脆弱性	・デバイスや OS の種類を絞り込む、または統一する。	□
		信頼できないマーケット	・信頼できるマーケットからアプリケーションを入手する。 ・アプリケーションのインストール時に不用意にアクセス許可をしない。 ・アプリケーションに関する最新情報（不正な動き、意図しない動き、信頼できる事業者）を入手する。 （5.3 節「アプリケーションを利用する」参照）	■ □ □
		[illegible]	[illegible]	■

A-2 利用シーン別 対策チェックシート

推奨レベル：■強く推奨 □推奨 －対象外

節番号	分類	脅威	対策 または [illegible]	推奨レベル
5.1	データ情報を利用する	誤操作 知識不足	・手順書を作成する。（付録参照） ・アプリケーションの動き（データ保存場所、データの公開範囲等）を調べる。 ・業務専用の保存場所を決める。 ・利用者には保存場所を選択させないようにする。	－ □ □ □
		プライベートデータの操作【BYOD】	・誓約書にサインさせる。（付録参照） ・データを区分する（プライベートと業務の保存場所の区分）。 ・退職時、利用終了時にはすべての業務データの保存場所に対し、データを削除したことを明示させる。	－ □ ■
5.2	電話を利用する	盗聴	・VoIP を利用する際には、通信経路を暗号化する。	□
		不正利用	・IP PBX サーバの機器やサービスを正しく設定する。	□
		不正アクセス	・IP PBX サーバにパスワードをかけるなど周辺環境のセキュリティ強化を行う。デバイスを認証する。	□
		私的利用	・手順書を作成する。（付録参照） ・通話履歴を取得する。	－ □
5.3	メールを利用する	不正利用	・手順書を作成する。（付録参照） ・誓約書にサインさせる。（付録参照） ・Web メールなどデバイスにデータを残さないメールを使う。 ・本文や添付ファイルを暗号化する。	－ － □ □
		誤操作	・手順書を作成する。（付録参照） ・誓約書にサインさせる。（付録参照） ・ファイルの添付は禁止し、別手段を用意する。 ・本文や添付ファイルを暗号化する。 ・サーバにデータを残して原本を保存する。	－ － □ □ □

A-4 誓約書に記載する項目の例

A-4-1 法人所有版

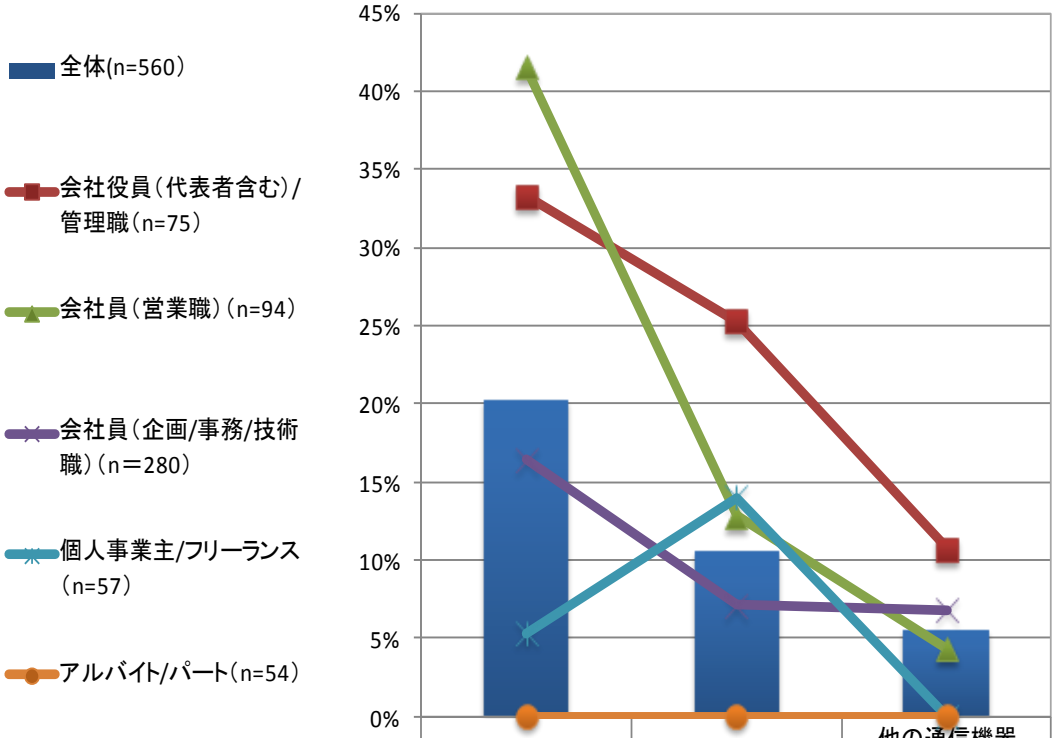
推奨レベル：■強く推奨 □推奨

分類	項目	概要（ねらい）	誓約書作成上の注意事項	推奨レベル
利用目的の明示	利用目的と範囲の明確化	スマートフォンの利用目的、利用範囲などを明記し組織の定めたルールの順守を確認する。		■
管理	組織による情報収集に対する個人の承諾（情報収集、監視などを行う場合）	不正な利用防止やマルウェア被害防止などから、スマートフォンの利用状況の収集を行うことを合意する。	スマートフォンは常時携帯するため、位置情報などを取得する場合には、「プライバシーの侵害」に注意して文書を作成する。 システム的な情報収集および、管理者による情報確認、どちらも含む。	■
	組織による制御に対する個人の承諾（制御、OS のアップデートなどを行う場合）	設定変更、機能制限やデータ削除を組織として行うことを合意する。	OS やアプリケーションのアップデートは、組織が管理する。 システム的な制御および、管理者による設定変更、利用者への設定指示なども含む。	■
	バックアップデータの保護	機密情報などの保護のため、個人所有 PC へのバックアップの禁止などを合意する。		□
届け出	特定の事象が発生した場合の届け出	紛失や盗難などが発生した場合、機密情報や個人情報の保管有無で、事故の影響を確認するため、直ちに届け出ることを合意する。	組織の定めたルールに従って届け出をする。 例：「破損」「故障」「不具合」「盗難」「紛失」など	■
禁止事項	端末、OS、アプリケーションの改造	セキュリティ上の脅威を防止するため、改造しないことを合意する。		■
	端末メーカー、通信事業者の利用規約に対する違反行為	提供元の意図に反する利用は行わないことを合意する。		□
	組織の許可しないアプリケーションの導入	マルウェアなどの侵入を防ぐため、許可されたアプリケーション以外を導入しないことを合意する。	導入して良いアプリケーション（ホワイトリスト）又は、導入してはいけないアプリケーション（ブラックリスト）などを別途定める。	□
	私的利用	コストの増加や業務生産性低下、情報漏えいなどを防ぐため、私的利用しないことを合意する。		□
	第三者への貸与、譲渡、販売	本人以外の利用を禁止することを合意する。		□
	紛失または盗失による情報漏えい	データを持ち歩くことや個人の発信機会が増えるため、注意を喚起する。情報漏洩時には、企業がリリースに従い対処する。	企業情報書き込み等への制限、不用意な情報拡散及び漏洩に十分注意する旨を明記する。	□
利用の終了	端末の返却	情報の削除、端末の回収を実施することを合意する。	データのバックアップ取り扱い、返却のルールは別途手順とする。	■
誓約への違反	罰則規定	組織の定めた罰則規定の適用対象となることを明示する。		□

BYODによる
ワークスタイルの変革

会社支給端末の割合①

会社から携帯電話／スマートホンを支給されているか



	携帯電話を支給されている	スマートフォンを支給されている	他の通信機器(PHSなど)を支給されている
全体(n=560)	20.2%	10.5%	5.5%
会社役員(代表者含む)/管理職(n=75)	33.3%	25.3%	10.7%
会社員(営業職)(n=94)	41.5%	12.8%	4.3%
会社員(企画/事務/技術職)(n＝280)	16.4%	7.1%	6.8%
個人事業主/フリーランス(n=57)	5.3%	14.0%	0.0%
アルバイト/パート(n=54)	0.0%	0.0%	0.0%

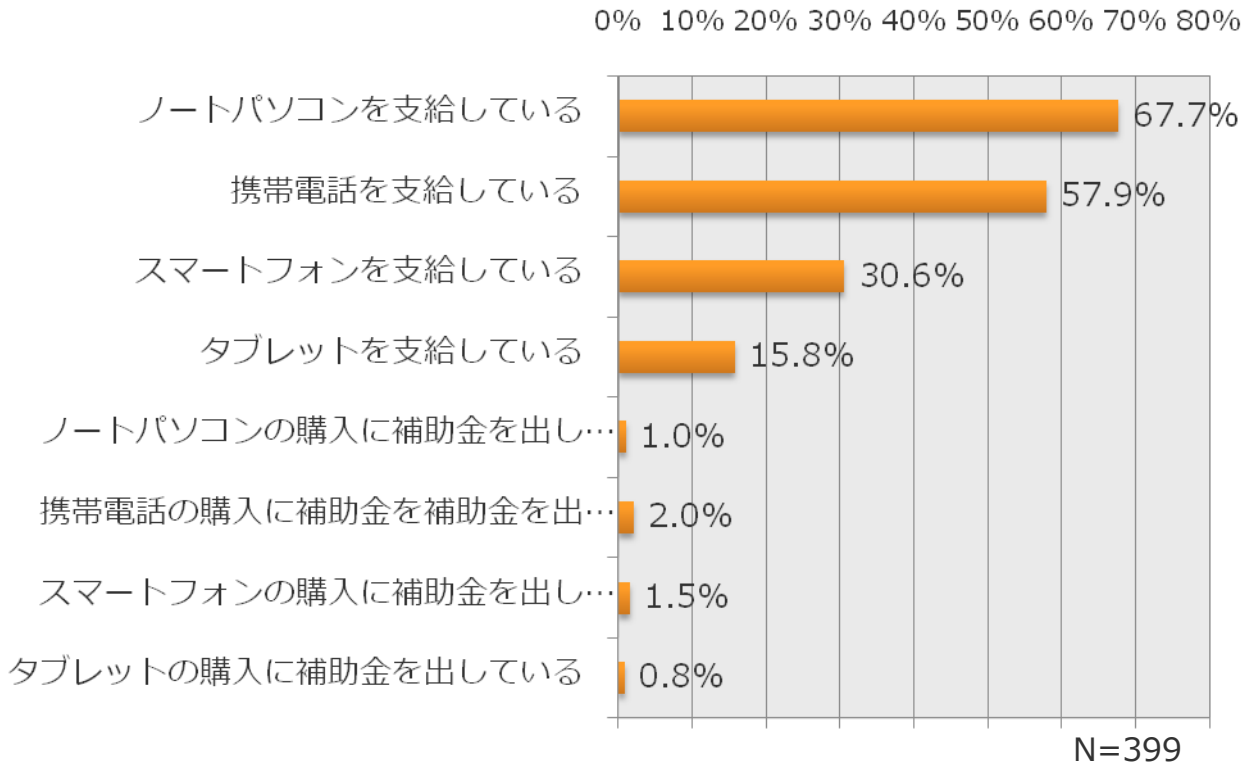
会社支給率は
フィーチャーフォン　20%
スマートフォン　10%

役職により、スマホ配布率は大きく異なる

出典：ネットマイル株式会社　調査
2011年12月28日～2012年1月3日
235万会員のうちスマホパネルのみ対象（回答560）

会社支給端末の割合②

- **あなたの勤務先企業では、モバイル機器を従業員に支給していますか（複数選択）**



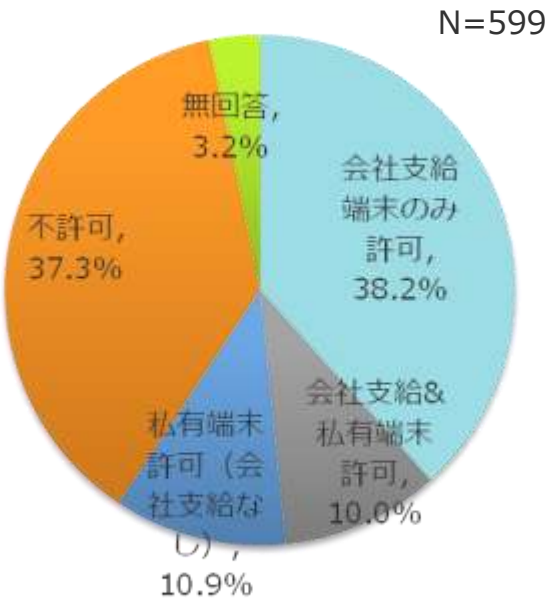
PCは7割弱、スマホは3割、勤務先が支給

出典：IT Pro　調査
2012年4月5日～13日
IT Pro読者（回答399）

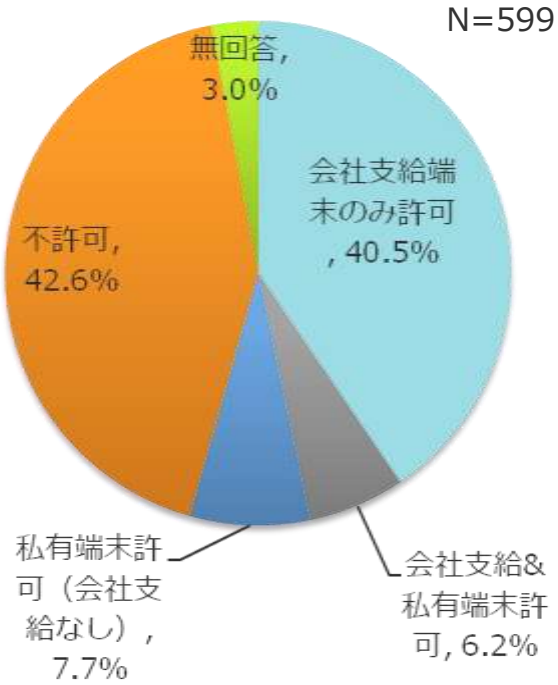
BYODと会社支給端末の割合

- スマートフォン・タブレット端末における会社支給と私物利用の割合（単一回答）

スマートフォンの業務利用



タブレット端末の業務利用

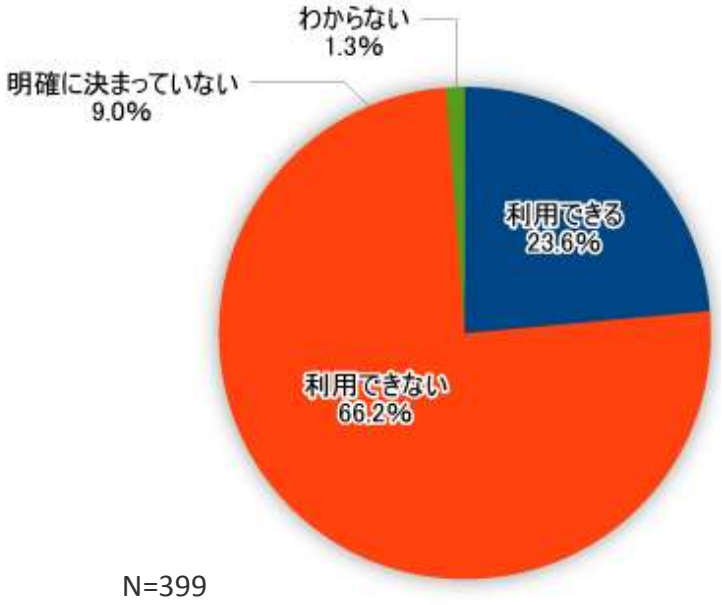


◆私物端末の利用を許可する企業は、
スマートフォン　20.9%
タブレット端末　13.9%
◆会社支給
スマートフォン　48.2%
タブレット端末　46.8%

出典：NRIセキュアテクノロジーズ株式会社
2011年8～9月に、東証1部・2部上場企業を中心とする
3,000社の企業を対象にしたアンケート結果より（回答599社）

BYODについて

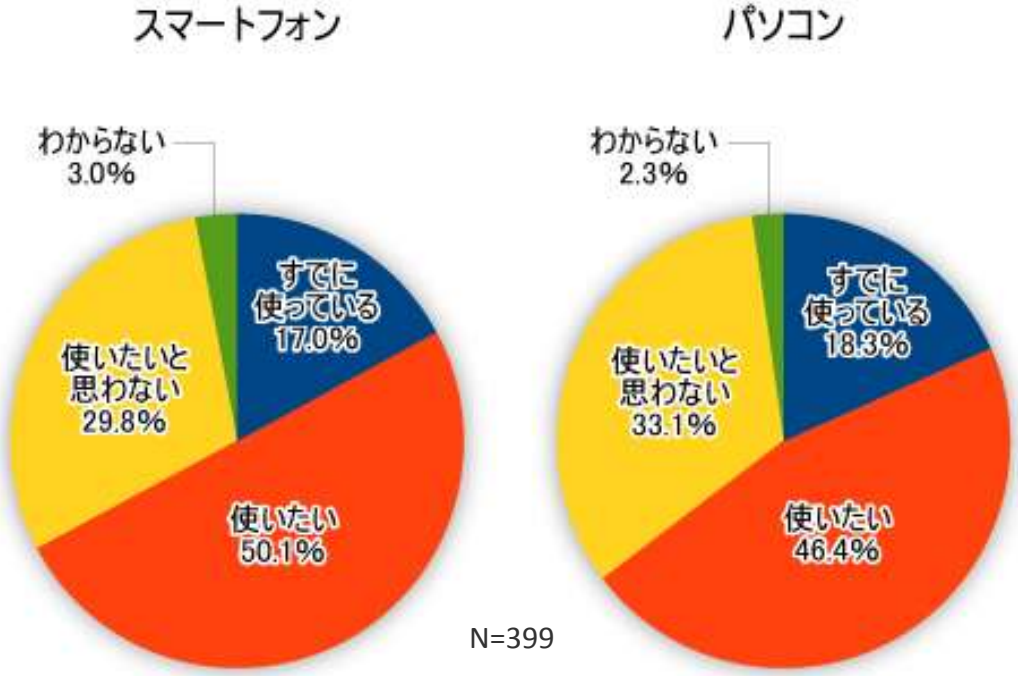
■あなたの勤務先企業では
私物デバイスを社内の情報システム／
ネットワークで利用できますか（単一選択）



N=399

私物デバイスを利用できる＝
BYODを認めている　は、23.6%

■社内の情報システム／ネットワークを
自分が所有するスマートフォンで
使いたいと思いますか（単一選択）



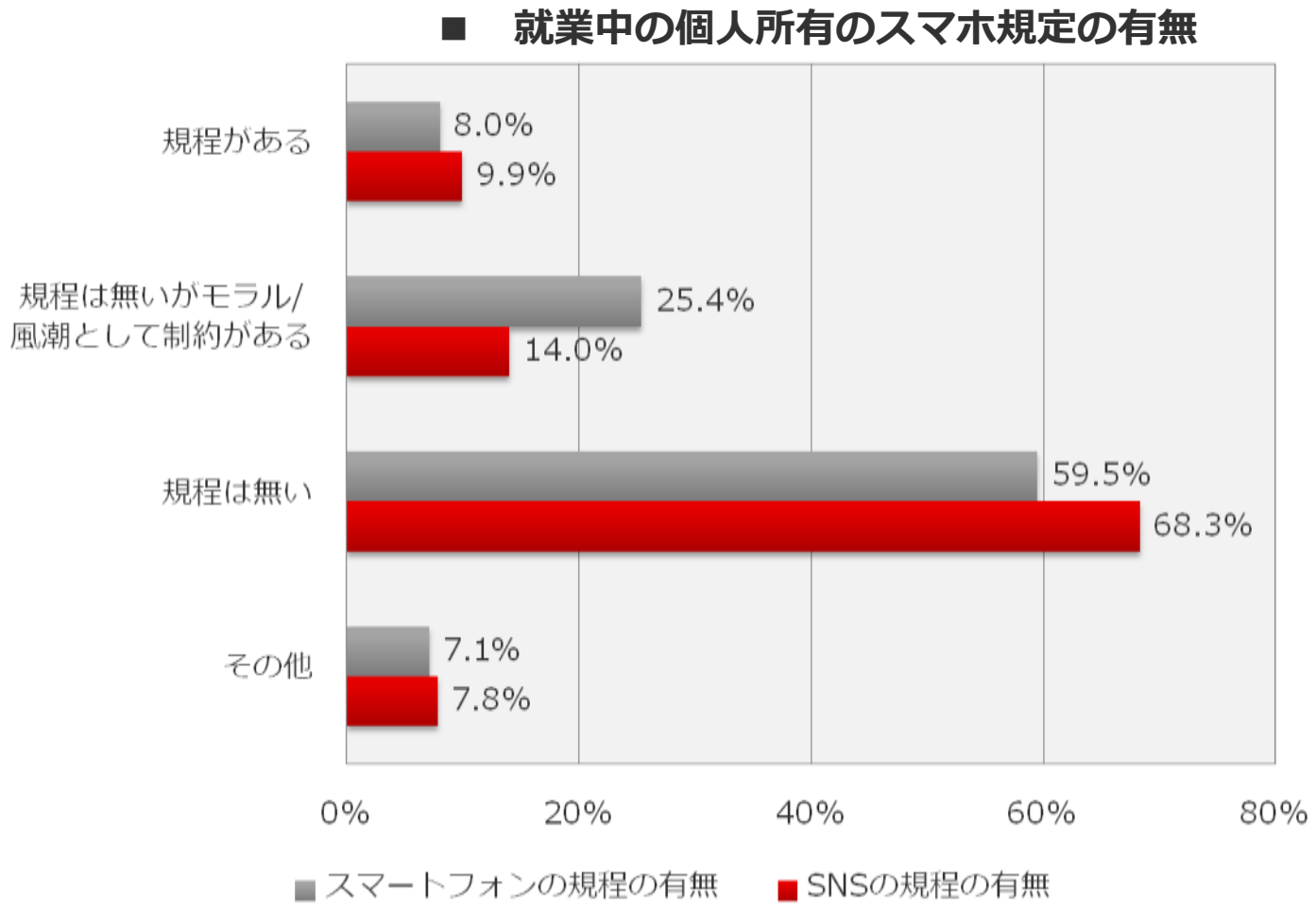
N=399

約5割が私物デバイスを使いたいと考えている。
（既に使っている2割を合わせれば約7割）

既に¼の企業はBYOD容認、従業員の約半数はスマホでの社内システム利用を希望

出典：IT Pro　調査
2012年4月5日～13日
IT Pro読者（回答399）

スマホ・SNS利用における規程の有無

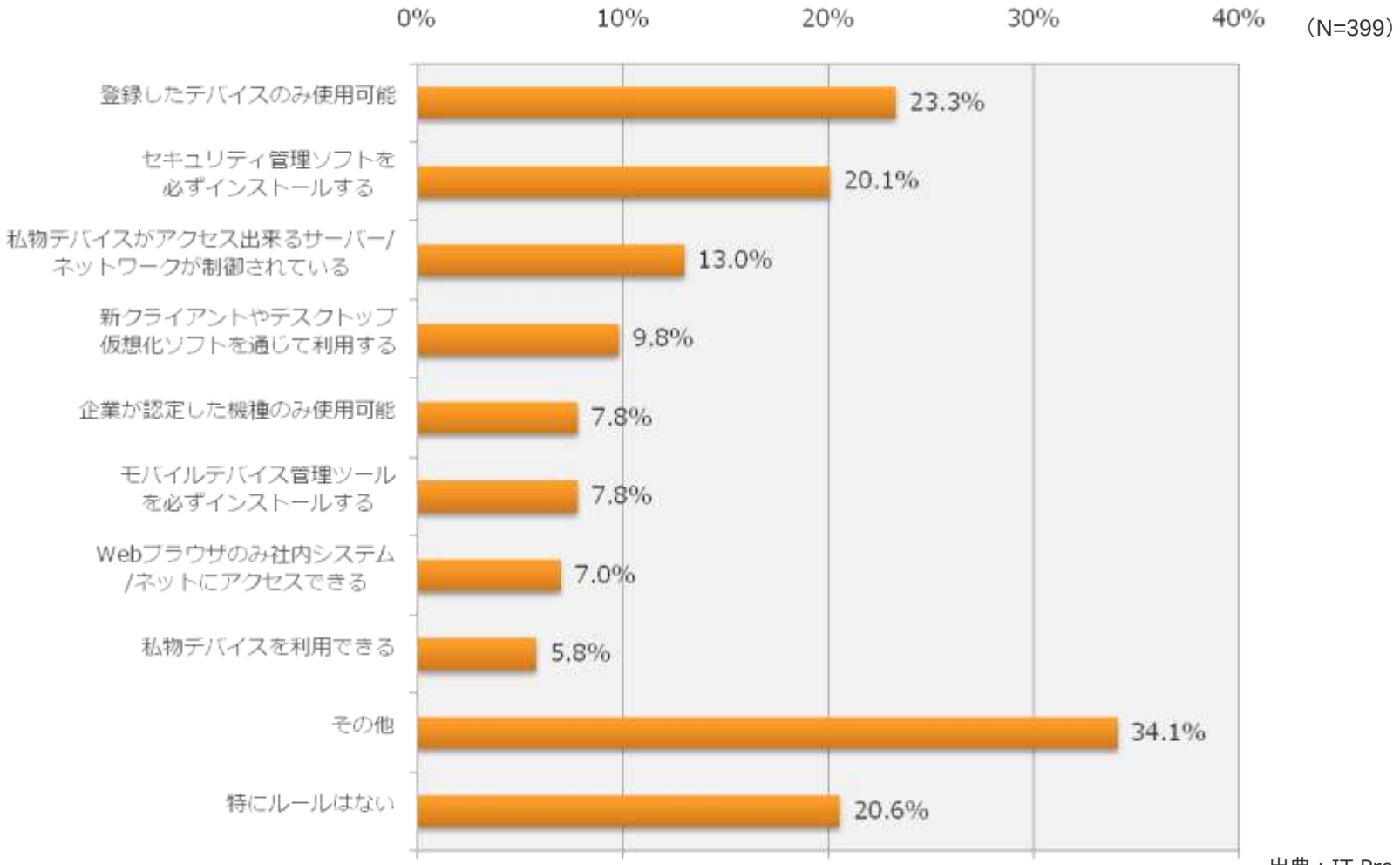


現状では、規定を設けている企業は1割以下

出典：IT Pro　20120417
／モバイルマーケティング･ジャパン、ネットマイルアンケート
2012年4月1日～4月6日　アウマホリサーチパネル　回答

私物デバイス利用におけるルール

■ 私物デバイス利用にあたって、どのようなルールを定めていますか（複数選択）

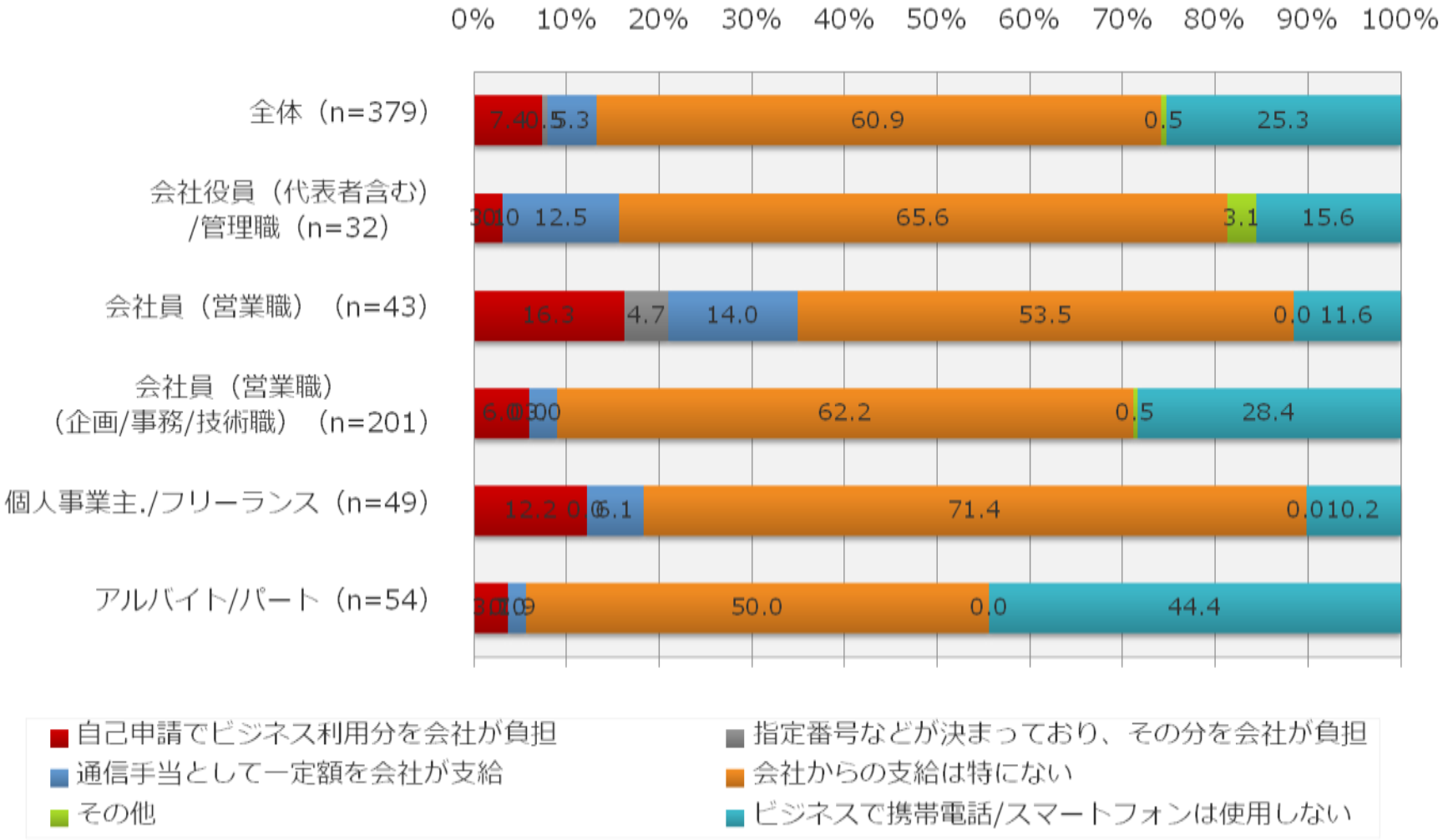


私物利用可とルールなしを合わせると約1/4の企業はBYOD容認

出典：IT Pro　調査
2012年4月5日～13日
IT Pro読者（回答399）

仕事で私物携帯電話を使っても、約6割は通信料金の会社負担なし

■仕事で利用する携帯電話の通信料金負担状況
（フィーチャーフォン/スマートフォンを支給されていない人のみ）



通信料金負担なしの従業員の潜在的不満は非常に大きいと思われる

出典：IT PRO 20120116

BYOD(スマートフォン)まとめ

- スマホの支給率は1割～3割で調査によりばらつき
  - 今後はフィーチャーフォンの提供は確実に減少するので、スマホの支給率は増加する見込み
  - 役職によりスマホ支給率は異なるが、今後は一般職含めた支給率の増加が予想される
- スマホ利用においても、一番利用するのは通話
  - 特に社内メンバーとの通話は、どの職種においても一番
- 約1/4の企業はBYODを容認
- 約6割は通信料金の負担なし

- **今後、確実に普及が予想されるスマートフォンの活用が成長のキーポイント**
- **現状でも一番利用率の高い、通話料金の削減の必要性**
- **従業員の私物利用(BYOD)採用による、コスト削減とセキュリティの担保**
- **発展途上のスマートフォンを熟知したサービス提供者の選択**

NEXTGEN
connect to the next generation

U³ Voice（ユーキューブボイス）

お客様のニーズを幅広く満たす 3タイプのサービスをご提供します

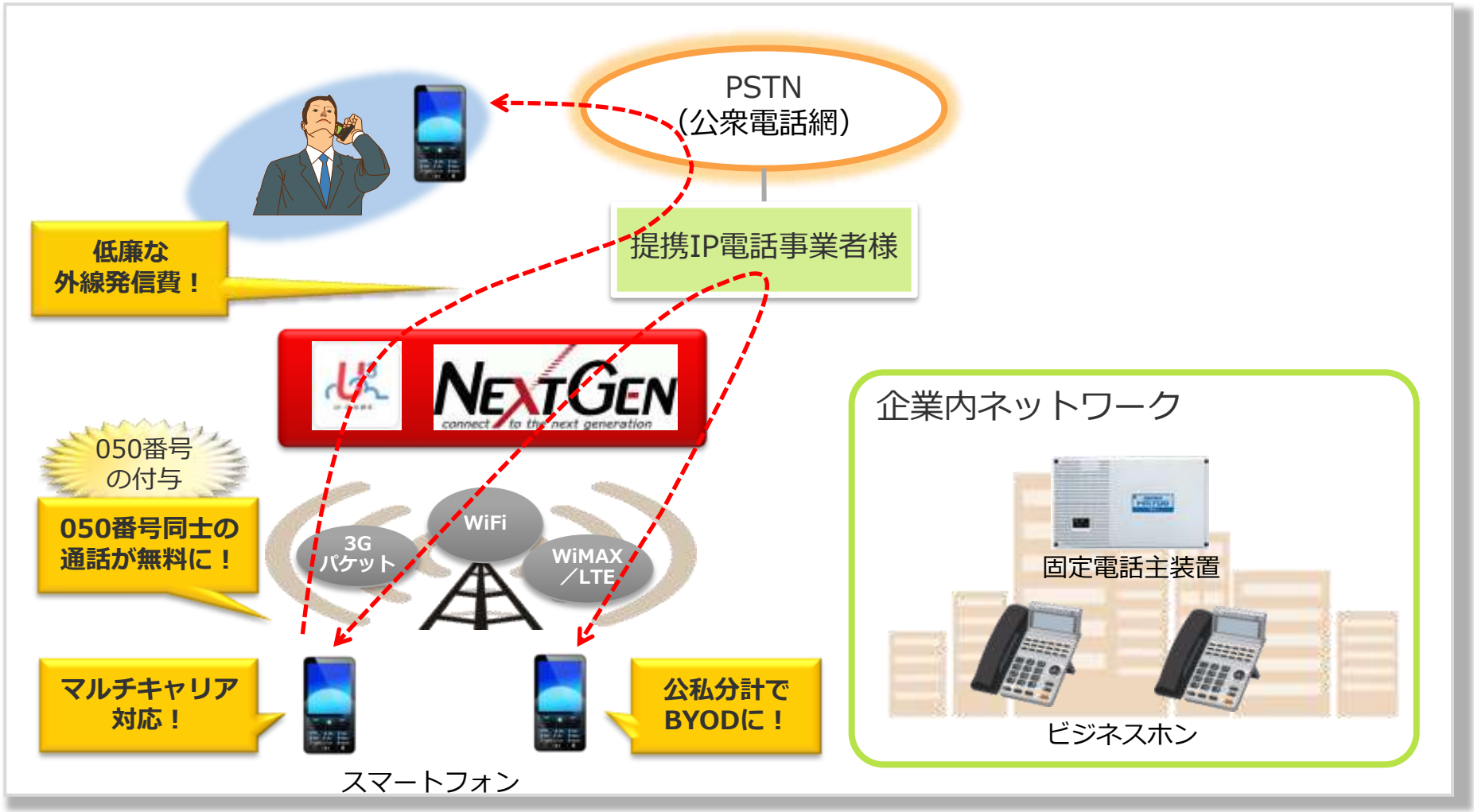
- **U³ Voiceベーシックタイプ**
  オフィスのビジネスホンとは切り離し、個々の社員が外線発着信を直接行えるサービスを利用したい

- **U³ Voiceオフィスタイプ**
  オフィス内のビジネスホンはそのまま活用するが、外出者や在宅勤務者の電話と連携させたい

- **U³ VoiceクラウドPBXタイプ**
  オフィスのビジネスホンを廃止して、堅牢なデータセンタからのクラウド型ビジネスホン機能を利用したい

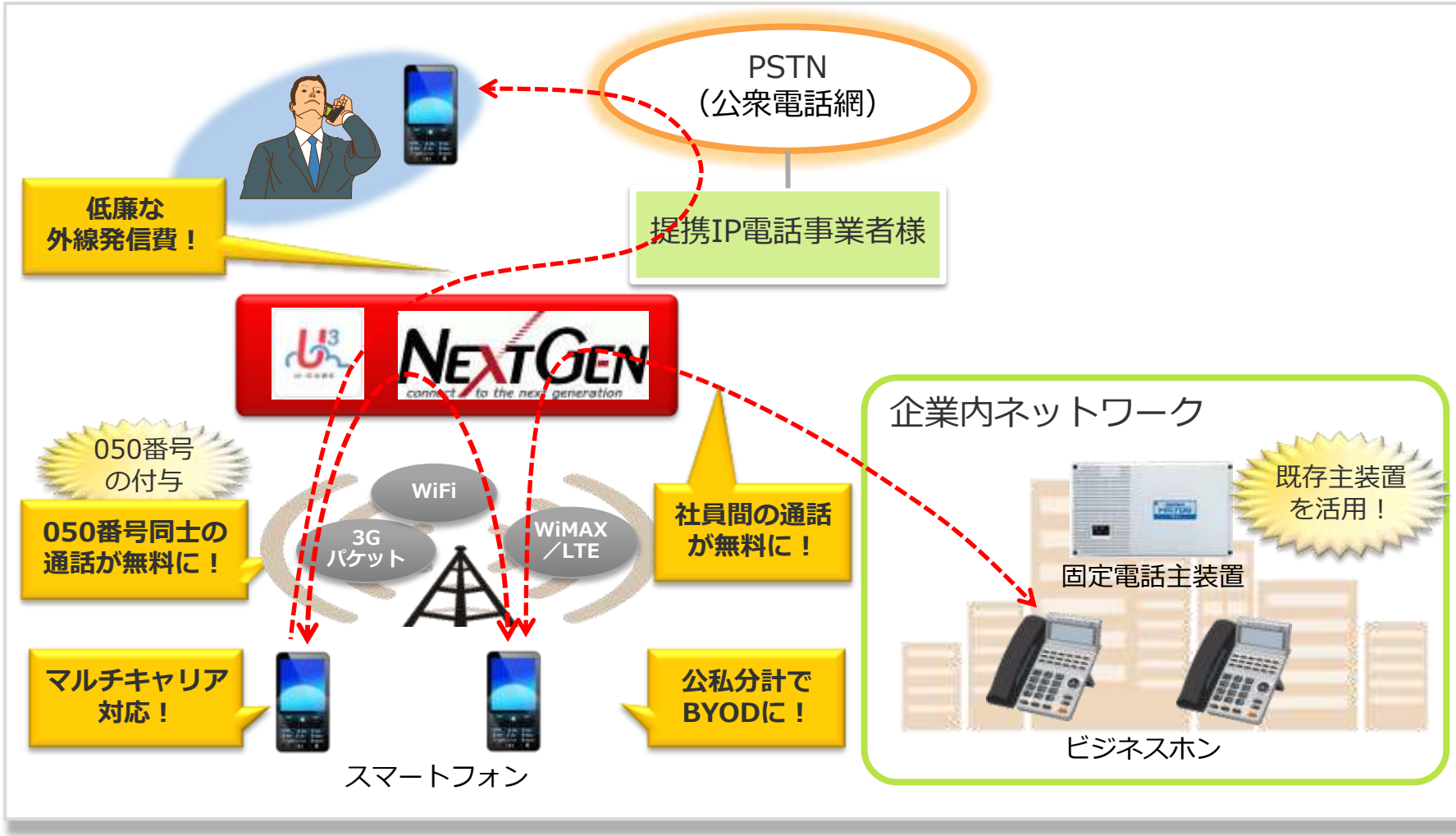
U³ Voiceベーシックタイプ
携帯の通話料金を廉価にするシンプルなサービス提供

導入メリット
- サービス加入者間通話無料
- 050番号による外線発信機能
- マルチキャリア対応
- 低廉な外線通話料金によるコスト削減
- 公私分計でBYODにも最適



U³ Voiceオフィスタイプ
ビジネスフォンと外出社員との無料通信を実現

導入メリット
- U3 Voiceベーシックの機能
- 社内電話とスマホ間の通話無料
- 既存の電話主装置や回線を利用
- スマホに050番号を付与しなくても社内通話は無料
- ゲートウェイ機器等の設置は不要

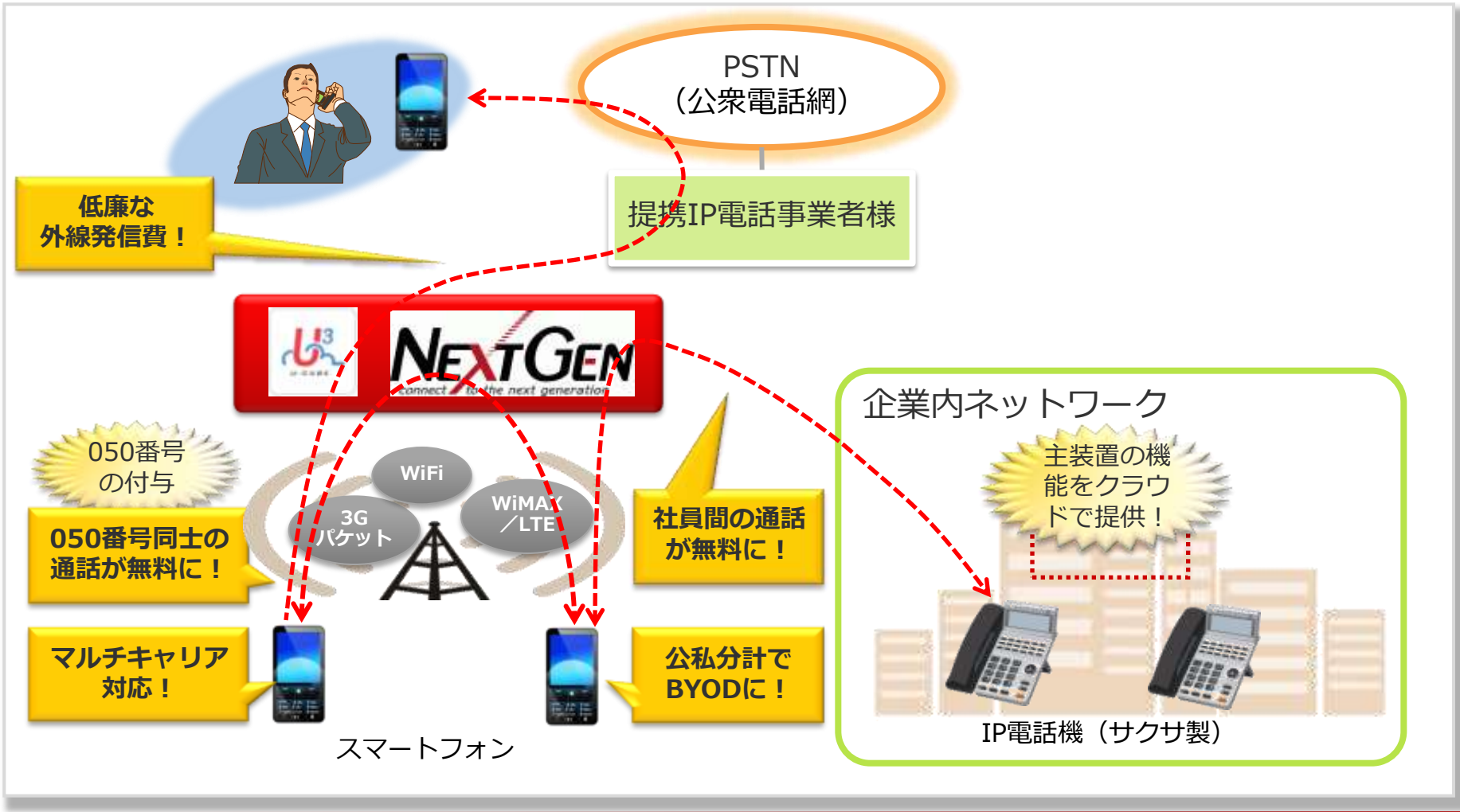


U³ Voiceクラウド PBXタイプ

クラウド型ビジネスフォンサービスを提供

導入メリット

- U3 Voiceベーシックの機能
- 電話主装置運用コストの削減
- IP電話機の利用も可能
- パーク保留や転送等のPBX機能
- ID毎の課金による無駄の無い運用
- 堅牢なデータセンターで安心の運用



VoIPクライアントの対応予定機種（予定）

- **NTT docomo**
  - Android
    - ✓ SAMSUNG Galaxy S SC-02B
    - ✓ SAMSUNG Galaxy S II SC-02C
    - ✓ SONY Xperia arc SO-01C
    - ✓ SHARP AQUOS PHONE SH-12C
- **SoftBank Mobile**
  - Android
    - ✓ SHARP AQUOS PHONE 006SH
  - iOS
    - ✓ Apple iPhone 4
    - ✓ Apple iPhone 4S
- **KDDI au**
  - Android
    - ✓ Xperia acro IS11S
  - iOS
    - ✓ Apple iPhone 4S

ネクストジェン U³ Voiceの特長

- 大手通信事業者に電話システム(VoIP)を提供してきた、ネクストジェンならではの「キャリアグレード」の品質
- JSSEC等の活動を支えるエキスパートクラスの技術者陣
- 社内通話コストの大幅な削減
- 低廉な外線通話コスト
- 050番号付与による公私分計、BYOD対応
- 柔軟な運用が可能なマルチキャリア対応
- クラウド電話帳(開発予定)による、端末に情報を持たせない、セキュアな利用環境の提供

↓↓↓詳しくはこちらをごらんください↓↓↓

NextGen WEBサイト

http://www.nextgen.co.jp/u3voice/

マイナビ連載記事

http://news.mynavi.jp/articles/2012/07/09/nextgen1/index.html

Beyond The Next Generation

株式会社　ネクストジェン

〒102-0083　東京都千代田区麹町3-3-4
TEL. 03-3234-6855(代)
FAX. 03-3234-6857
http://www.nextgen.co.jp