NTT docomo
Mobile driven Solutions
――― ドコモでビジネスが加速する

スマートフォンの市場動向とセキュリティ

2011年5月25日
株式会社NTTドコモ
ソリューションビジネス部
堀口　賞一

1. スマートフォン市場動向

- 「フューチャーフォン」 から 「スマートフォン」 へ
- ドコモのスマートフォンへの取組み
- 法人ユーザの利用動向

2. Android端末のセキュリティについて

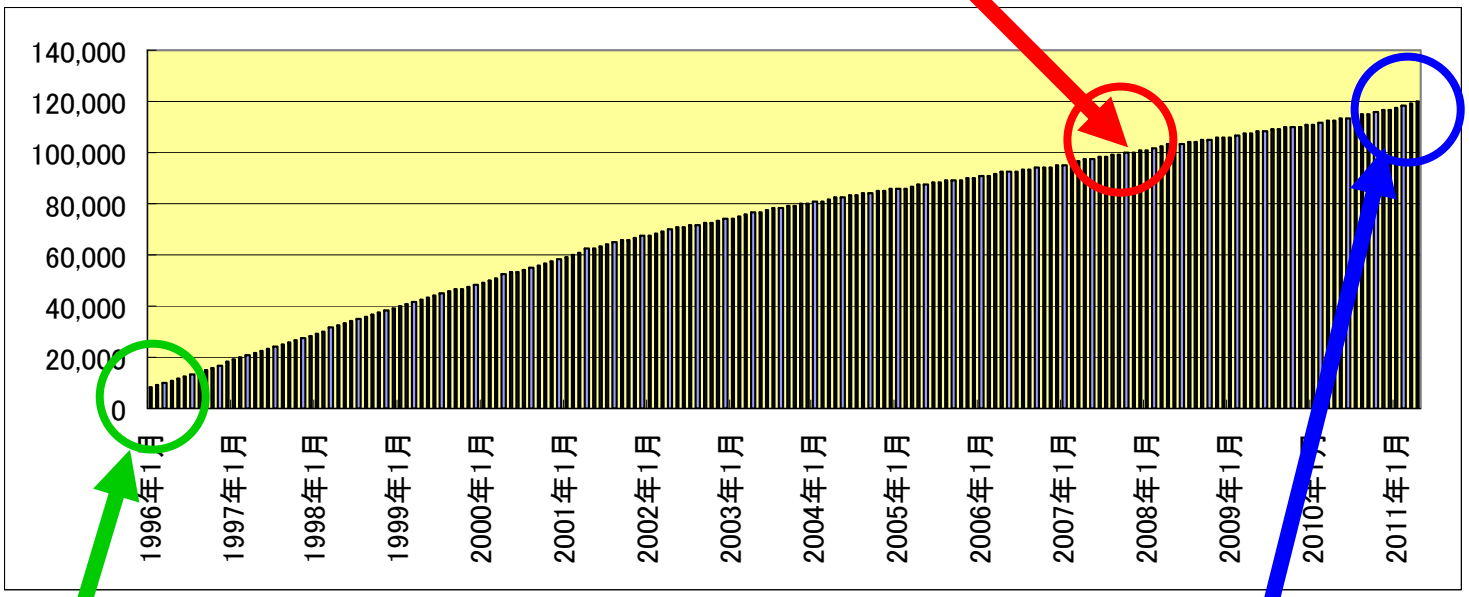
- スマートフォン（Android端末）のセキュリティ課題
- ドコモが考えるセキュリティ対策とは？

1．スマートフォーン市場動向

― 「フューチャーフォン」から「スマートフォン」へ ―

■日本の携帯電話契約数推移

2007年12月1億契約突破

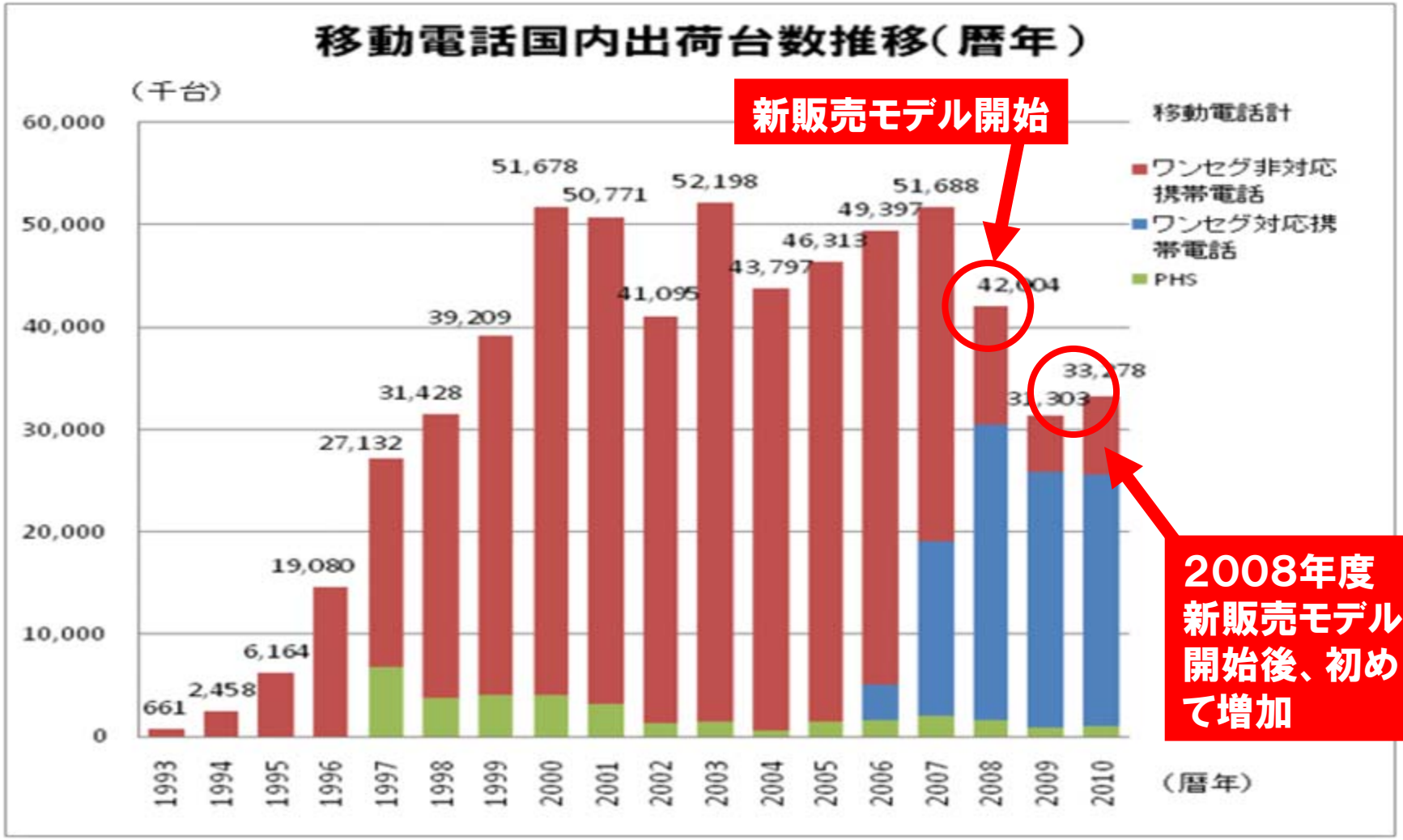


出所：(社)電気通信事業者協会報告(契約数は、1000台未満四捨五入)

8,670,000契約(1996年1月)

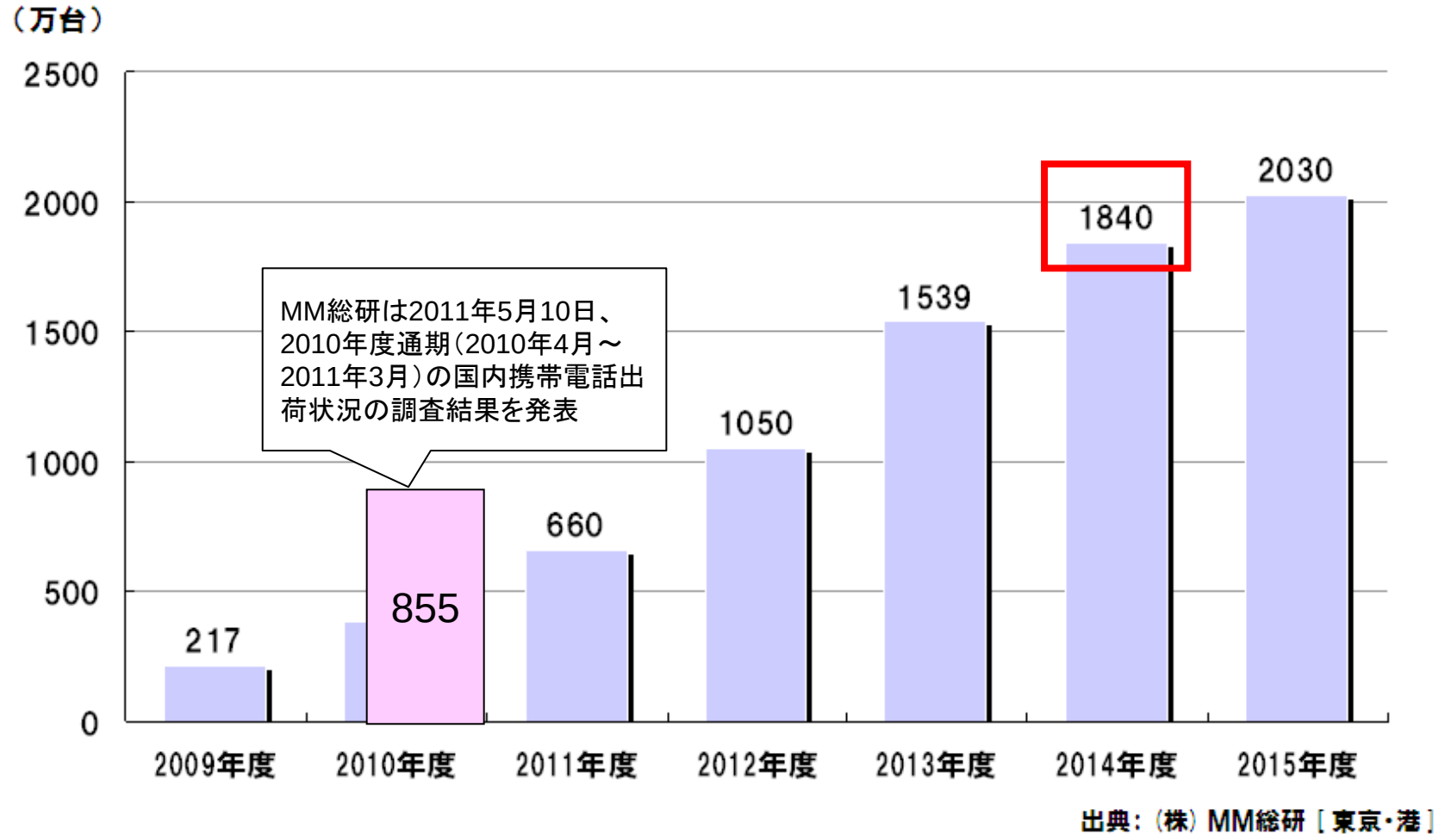
120,177,000契約(2011年4月現在)

■ケータイの出荷台数



出所：（社）電気通信事業者協会

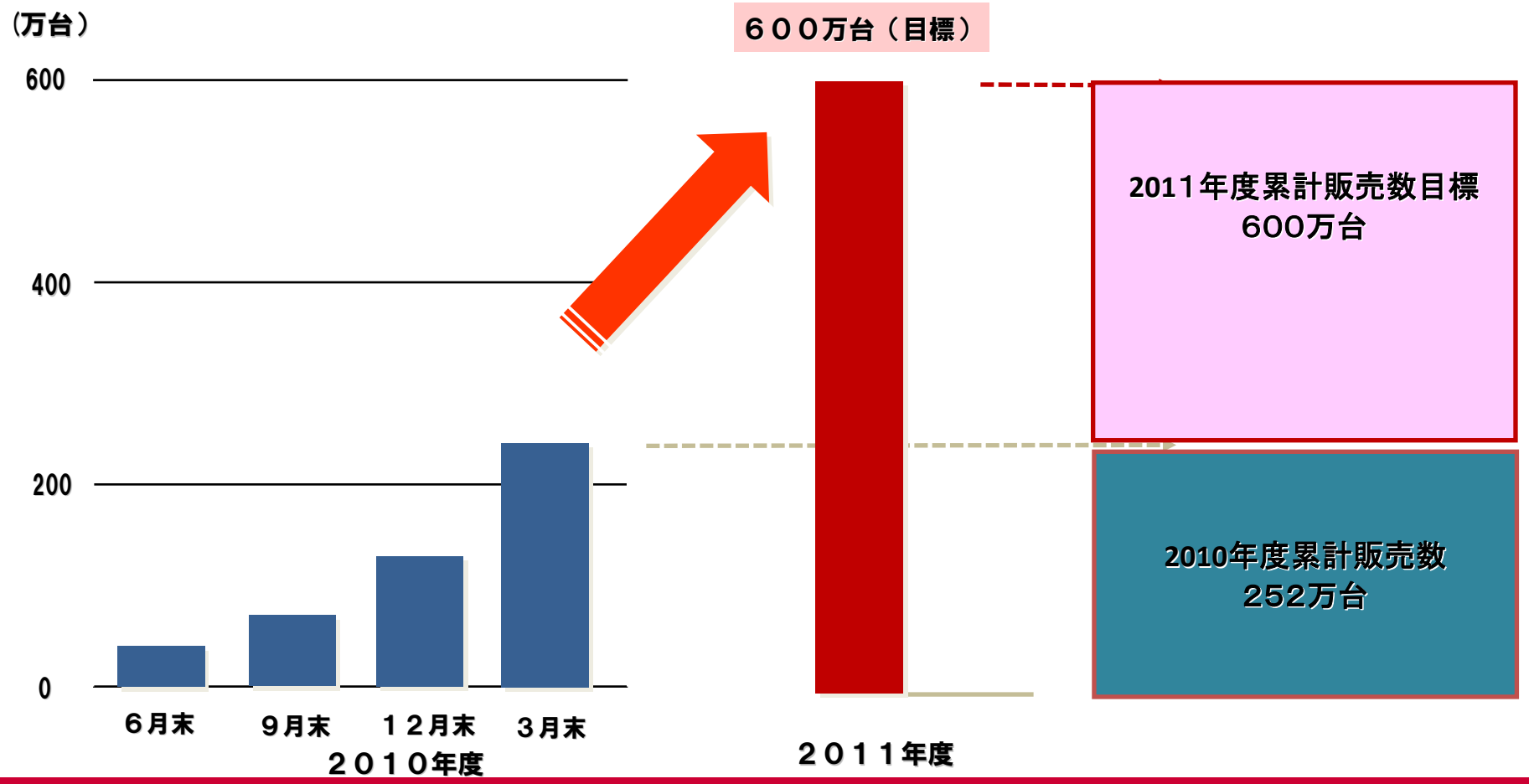
2014年度には半数がスマートフォン？



■ドコモのスマートフォン販売数推移、２０１１年度目標

・スマートフォン２０１０年度累計販売数は２５２万台
・２０１１年度販売数は、６００万台を目指す。

スマートフォン 販売数



１．スマートフォーン市場動向

ー　ドコモのスマートフォンへの取組み　ー

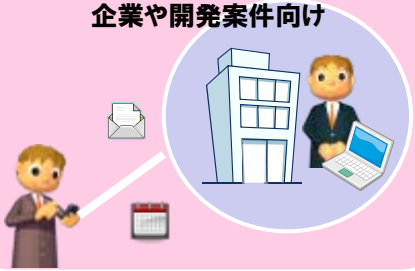
■ＮＴＴドコモのスマートフォンへの取り組み

ＮＴＴドコモはスマートフォン市場に対し、①ＷｉｎｄｏｗｓＭｏｂｉｌｅ、②Ａｎｄｒｏｉｄ、③ＢｌａｃｋＢｅｒｒｙの三種類のプラットフォームを用意し、より多くのお客様のご要望にお応えします

①Windows Mobile®

- Microsoft®提供するモバイル端末向けOS
- パソコンの一部の機能をモバイルで使用出来る
  - -OutlookMobile、OfficeMobile、Internet Explore®
  - -Windows系サーバ（Exchange等）と相性が良い
- 周辺機器、ソリューションが豊富

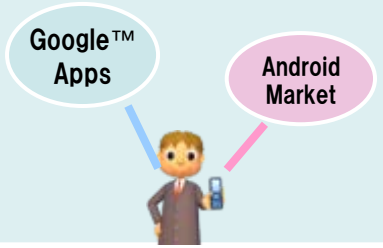
既に社内環境が整備されている企業や開発案件向け



②Android

- OHA（Google™社中心）が共同で開発するモバイル用PF
- Google™サービスとの相性が良い
  - -Google Apps™を利用したビジネス利用がオススメ
- 豊富なアプリケーションをダウンロードして利用出来る

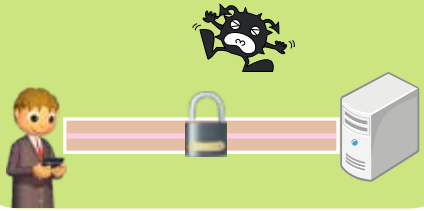
サーバを建てずにクラウドサービスを活用したい企業向け



③BlackBerry®

- RIM社が提供：世界130ヶ国、3,200万人以上が使用
- BlackBerry®ネットワークサービスとセットでの利用が前提
  - -プッシュメール、暗号化通信、デバイスマネジメント
- Microsoft® Exchange, Lotus Notesを高セキュリティに利用できる

セキュリティ要求の高い企業向け



※2010年1月現在

ドコモ スマートフォン

LYNX 3D

REGZA Phone

Optimus chat

GALAXY S

GALAXY Tab

BlacyBerryCurve9300

Xperia arc

MEDIAS

Optimus Pad

ドコモ スマートフォン

2011夏モデル

F-12C

Optimus bright
L-07C

MEDIAS WP
N-06C

P-07C

AQUOS PHONE
SH-13C

GALAXY S Ⅱ
SC-02C

AQUOS PHONE
SH-12C

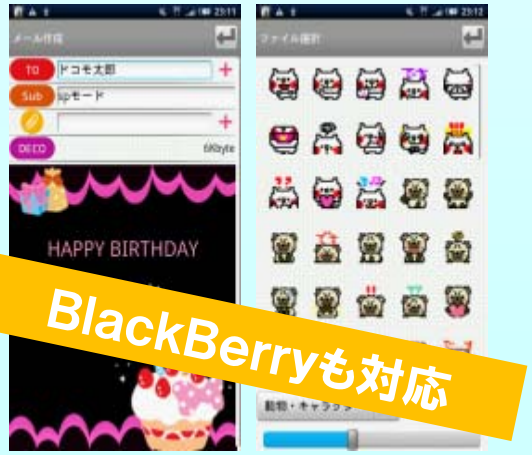
Xperia™ acro
SO-02C

BlackBerry®
Bold™ 9780

spモード －スマートフォン向けISP－

《メールサービス》

iモードのメールアドレスが利用できる
@docomo.ne.jp



BlackBerryも対応

《アクセス制限サービス》

有害サービスをブロック

《コンテンツ決済サービス》

ドコモの電話料金と一緒に支払える

Androidマーケット™対応

《「電話帳バックアップ」の提供》

《基地局データを活用した位置情報提供》

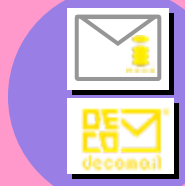
■スマートフォンの基本サービス拡充

これまで	2010年度	2011年度以降

iモード端末

SH-01B SH-02B SH-03B

iモードのサービス



スマートフォン

BlackBerry Bold T-01A HT-03A SC-01B

iモードサービスの取り込み

spモード

おサイフケータイ対応端末の開発

Xperia LYNX dynapocket BlackBerry Bold 9700

LYNX 3D REGZA Phone

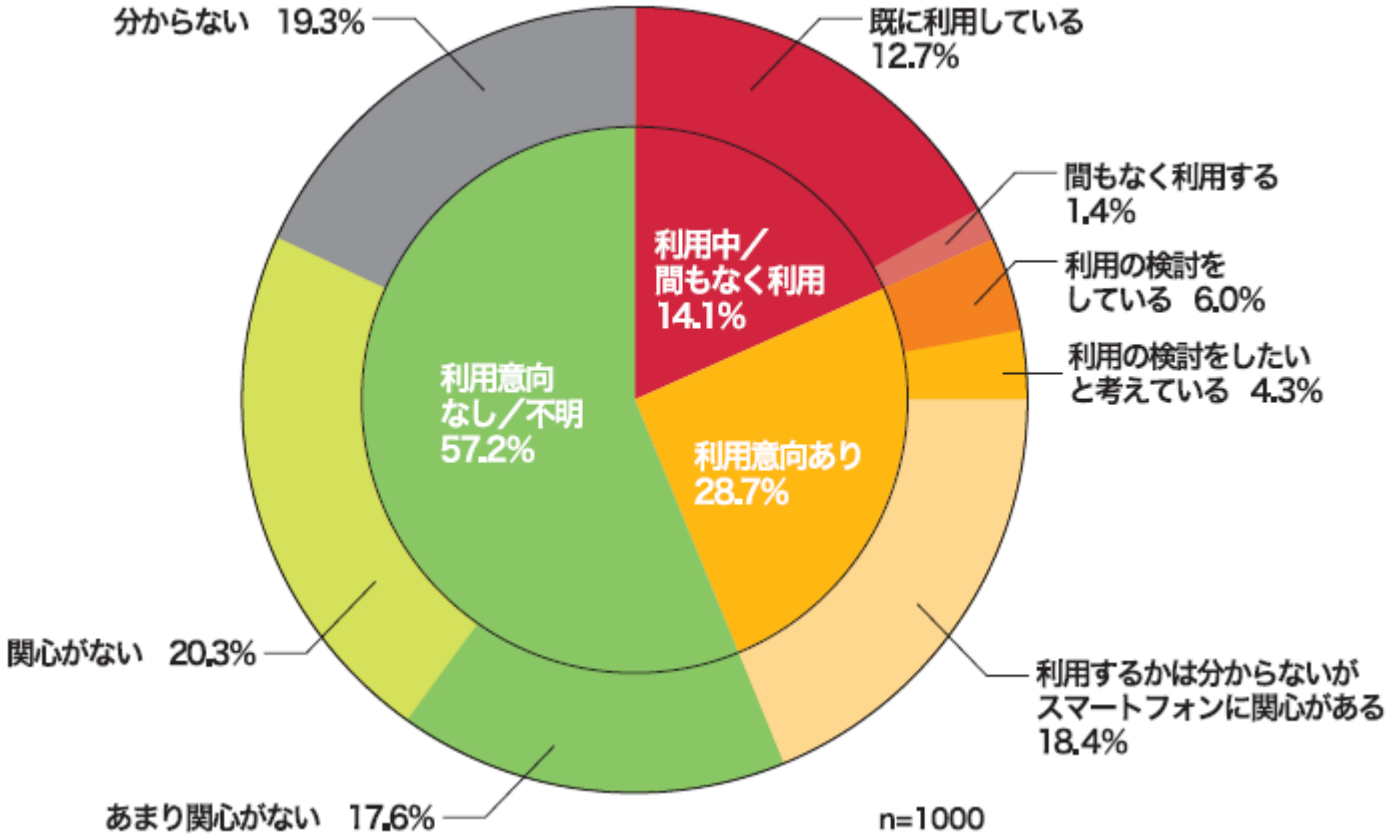
ドコモマーケット

コンテンツ決済サービス対応

1．スマートフォーン市場動向

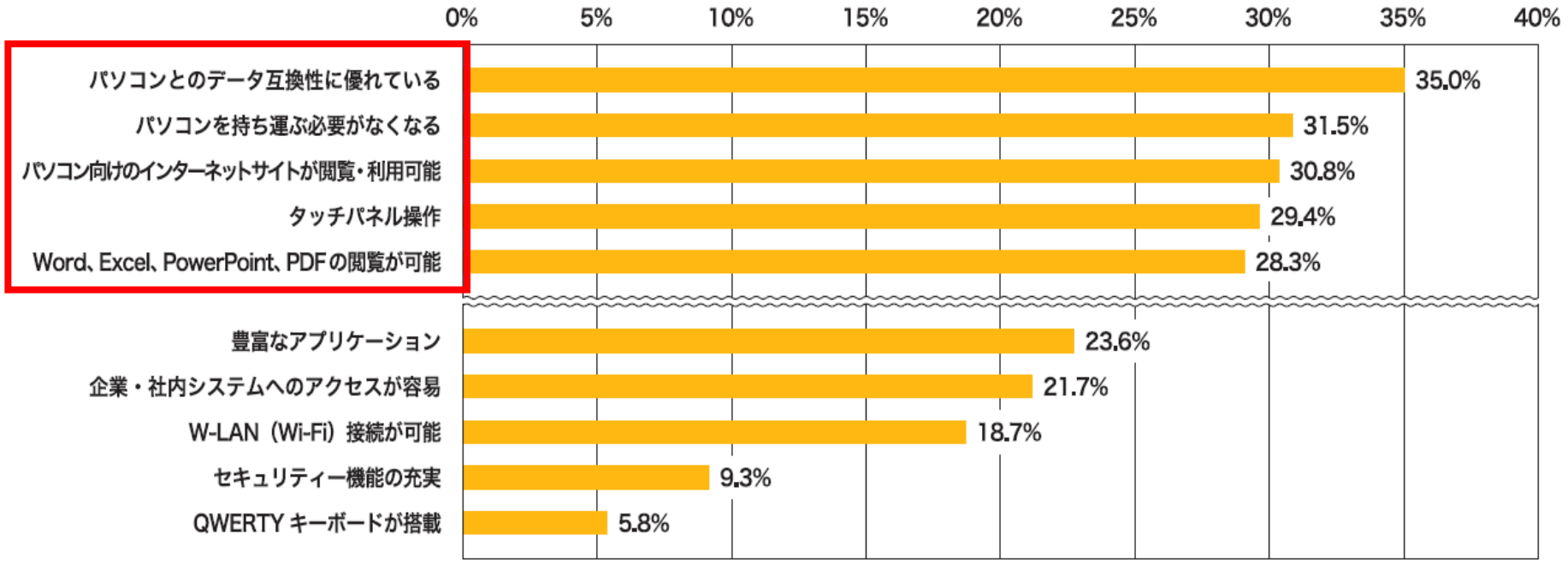
ー　法人ユーザの利用動向　ー

既に利用している企業は12.7％
利用意向ありも含めると42.8％



2010.8 企業のスマートフォン利用実態／利用意向調査より

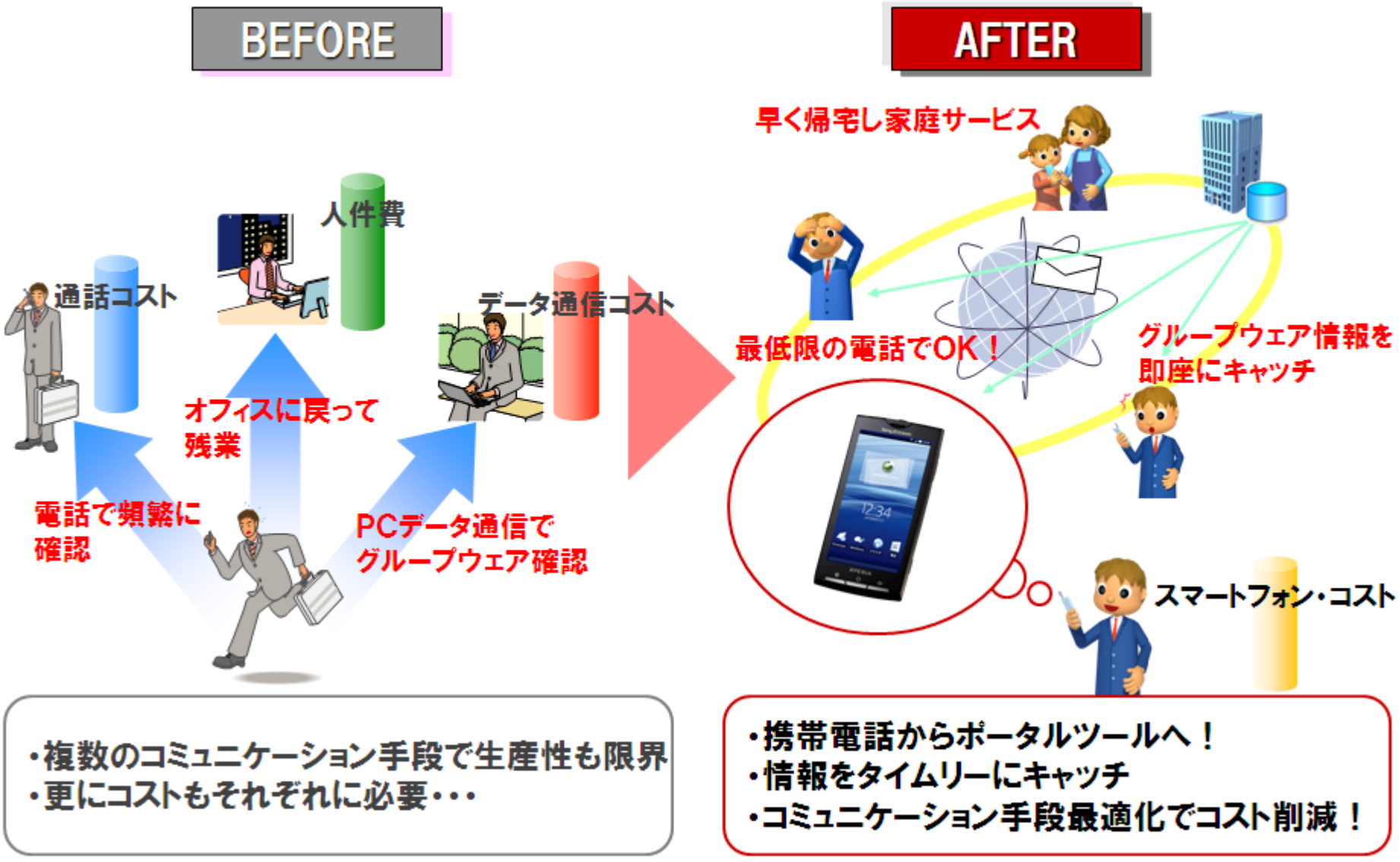
パソコンとの互換性・代替性が一番の魅力



2010.8 企業のスマートフォン利用実態/利用意向調査より

ケータイの移動性×PCの高機能×使いやすさ

■スマートフォンの活用とワークスタイルの変革



2. Android端末のセキュリティについて
ー　スマートフォンのセキュリティ課題　ー

- **JIS Q 27002（ISO/IEC 27002）では、情報セキュリティを以下のように定義**

  情報の機密性、完全性および可用性を維持すること。さらに、真正性、責任追跡性、否認防止および信頼性のような特性を維持することを含めてもよい。

- **機密性**：
  情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること
- **完全性**：
  情報が破壊、改ざん又は消去されていない状態を確保すること
- **可用性**：
  情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること
- **真正性**：
  ある主体又は資源が、主張どおりであることを確実にする特性
- **責任追跡性**：
  あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できる事を確実にする特性
- **否認防止**：
  ある活動又は事象が起きたことを、後になって否認されないように証明する能力
- **信頼性**：
  意図した動作及び結果に一致する特性

■ 主なセキュリティ脅威として、下記のように様々な脅威が想起される。

- 従来の携帯電話機では、通信事業者としてセキュリティを確保してきた部分が多くありました。しかし、オープンプラットフォームであるAndroidに代表されるスマートフォンでは、パソコン同様、ユーザにてセキュリティ対策を実施して頂く環境であると考えます。

- 一般的にパソコンの世界で想定されるセキュリティ脅威に加え、モビリティ性の高いスマートフォンは、携帯電話機利用時に想定されるセキュリティ脅威も追加されます。

- 更に、Android対応アプリの課題として、アプリケーション自身の脆弱性の課題があると思います。なりすましや改竄など悪意のあるアプリケーションを排除するしくみ作りが重要と考えます。

2. Android端末のセキュリティについて
ー ドコモが考えるセキュリティ対策とは？ ー

■ 主なセキュリティ脅威に対して、複数のセキュリティ対策アプリケーションが必要。

■スマートフォン利用時におけるお困りごと

	お困りごと		解決策
①	セキュリティ対策の強化	スマートフォン紛失時のデータ流出が心配だな…	**遠隔ロックや初期化による端末紛失時対応が可能！** 紛失時には端末を遠隔ロック、見つからない場合は端末初期化を行う事でセキュリティを確保します。
②	端末セキュリティ管理業務の効率化	社員に貸与する100台のスマートフォンのセキュリティ設定、一括で出来れば楽なんだけど…	**WEBの管理画面から複数端末のセキュリティ設定を一括実施することが可能！** 管理画面から対象の電話番号を選択し指示を行う事でセキュリティ設定等の制御を実施します。複数選択することで一括の指示も可能となります。
③	端末利用制限による経費削減	スマートフォンのプライベート電話の発信利用を制限したいな…	**発信先制限を設定が可能！** 業務に関係のない発信通話利用の制限が可能となります。

※制御、監視可能な項目は端末、OSによって異なります

■「スマートフォン遠隔制御サービス」とは

「スマートフォン遠隔制御サービス」とは、企業で利用・管理しているスマートフォン端末に、インストールしたアプリケーションを制御する事で、スマートフォン端末を安心、便利にご利用いただくためのASPサービスです。端末紛失時のロックやデータ削除、発信先制限や不要な操作を防止するデバイス利用制限等、
さまざまな設定、制御を管理画面上より一括して行うことができます。

- 管理端末(ブラウザ)上から一括管理
- リアルタイムな制御が可能

紛失時対策

- 端末ロック・アンロック
- 端末初期化
- 個別データ削除　など

不正利用の防止

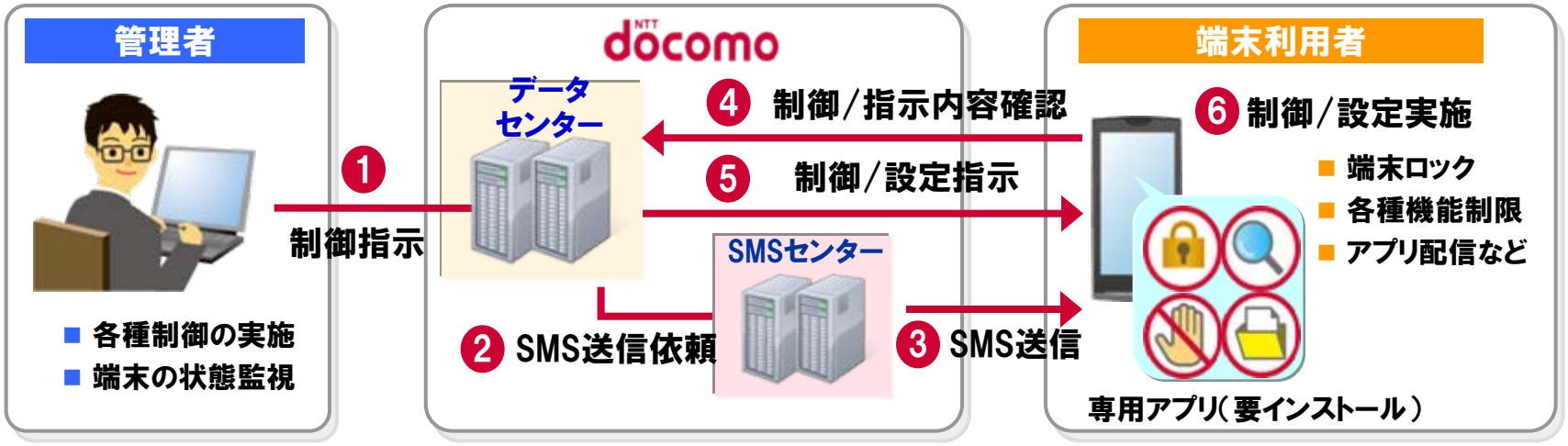
- 発信先制限
- アプリケーション利用制限
- 各種デバイス利用制限
- その他各種設定

端末管理の効率化

- ファイル配信
- 各種デバイスの利用制限の一括設定
- インストールアプリ情報の取得
- ロック状態の確認　など

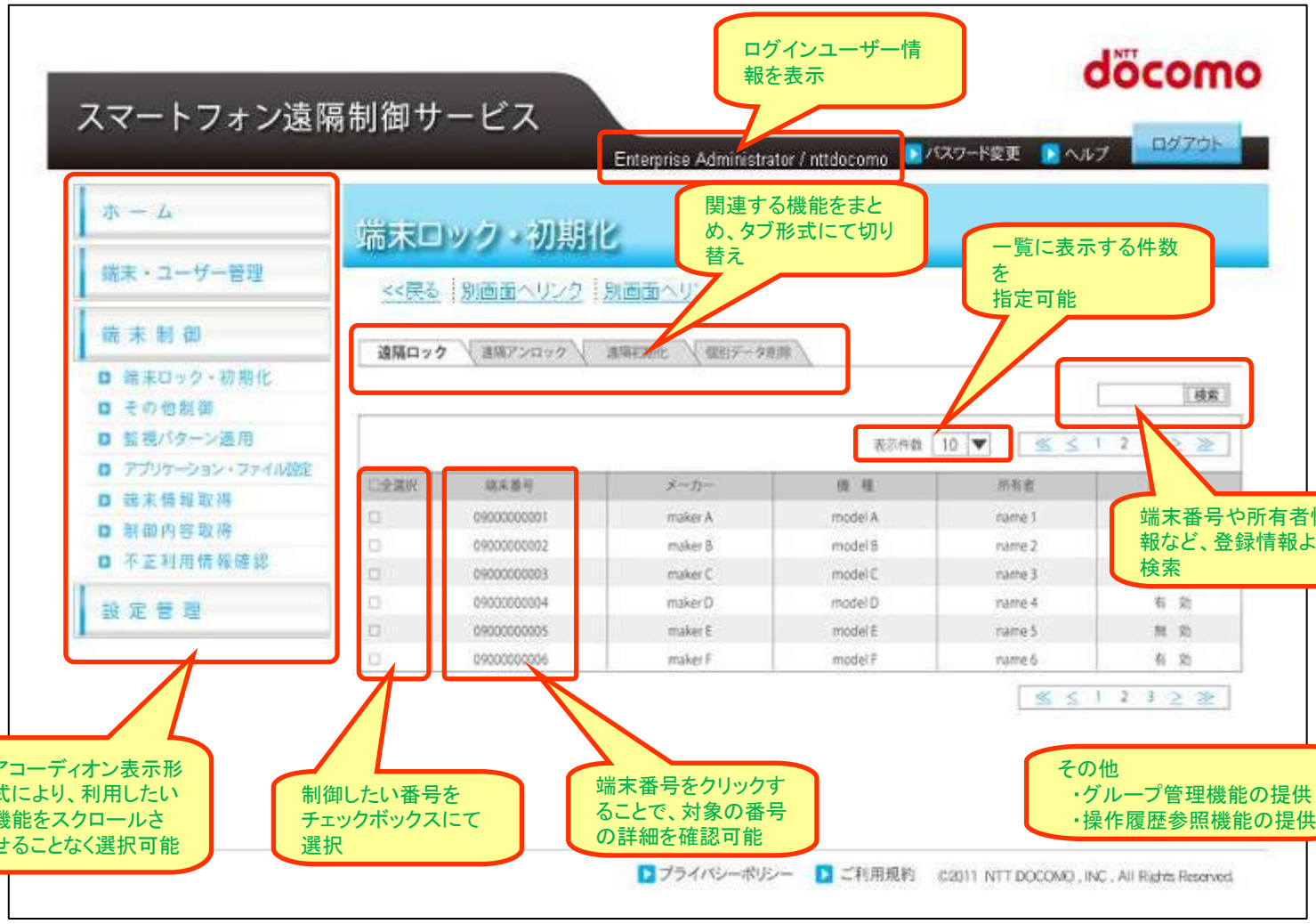
※制御、監視可能な項目は端末、OSによって異なります

制御指示にSMS(ショートメッセージサービス)を利用することでリアルタイムに制御が可能です

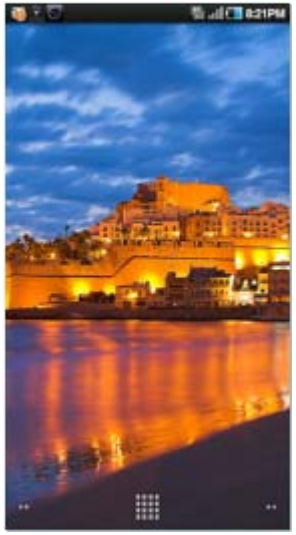


	一般的なポーリング方式	SMS方式
方式の詳細	あらかじめ設定した間隔(数分～数十分等)毎に、データセンターへ制御/設定内容を確認	SMS受信時にデータセンターへ制御/設定内容を確認
リアルタイム性	設定した間隔による	ほぼリアルタイム
	着信時通話中・圏外・電源断の場合は、待ち受け復帰時後の最初のポーリングにて即時制御が可能	着信時通話中・圏外・電源断でも、待ち受け復帰時に即時制御が可能
バッテリの負担	データセンターへ定期的にアクセスする度、バッテリを消費	必要時にデータセンターへアクセスした場合のみ、バッテリを消費
備考	間隔を狭くすると、リアルタイム性が高まるが、バッテリ消費が高い。	

■利用画面イメージ（管理者画面）



ホーム画面



アプリケーション一覧

※本サービス独自のホームアプリに変更になります。

遠隔ロック指示中
（通信中）

遠隔ロック中

※UIM（SIM）カードを抜いた場合、別のUIM（SIM）カードを挿入した場合もロックが掛かります。

1. スマートフォン市場動向

- 2010年後半より、物凄い勢いでスマートフォンへのニーズが高まっています。
- 特に、Android端末の出荷台数が伸びてきています。
- ドコモとして、端末、サービス共にスマートフォンへ積極的に取り組みます。
- 法人ユーザのスマートフォン利用意向は非常に高いです。
- ドコモもビジネスを加速させるためのソリューションを提供します。

2. Android端末のセキュリティについて

- 現状、スマートフォンでは、パソコン同様、ユーザにてセキュリティ対策を実施して頂く環境であると考えます。
- パソコンの世界と共通するセキュリティ対策に加え、モバイル特有のセキュリティ対策を加味する必要があります。
- スキャンソフト、デバイスマネージメント、VPNソフト等を活用し、安心安全な環境でスマートフォンをビジネス活用して頂きたいと思います。
- Android対応アプリの課題として、アプリケーション自身の脆弱性の課題があると思います。なりすましや改竄など悪意のあるアプリケーションを排除するしくみ作りが重要と考えます。

ご清聴ありがとうございました。