Designing The Future

KDDI

企業利用に向けての
スマートフォン戦略について

2011年1月6日

KDDI株式会社
中島 昭浩

アジェンダ

1. Androidデバイスの市場動向

2. Androidデバイスのセキュリティ検証

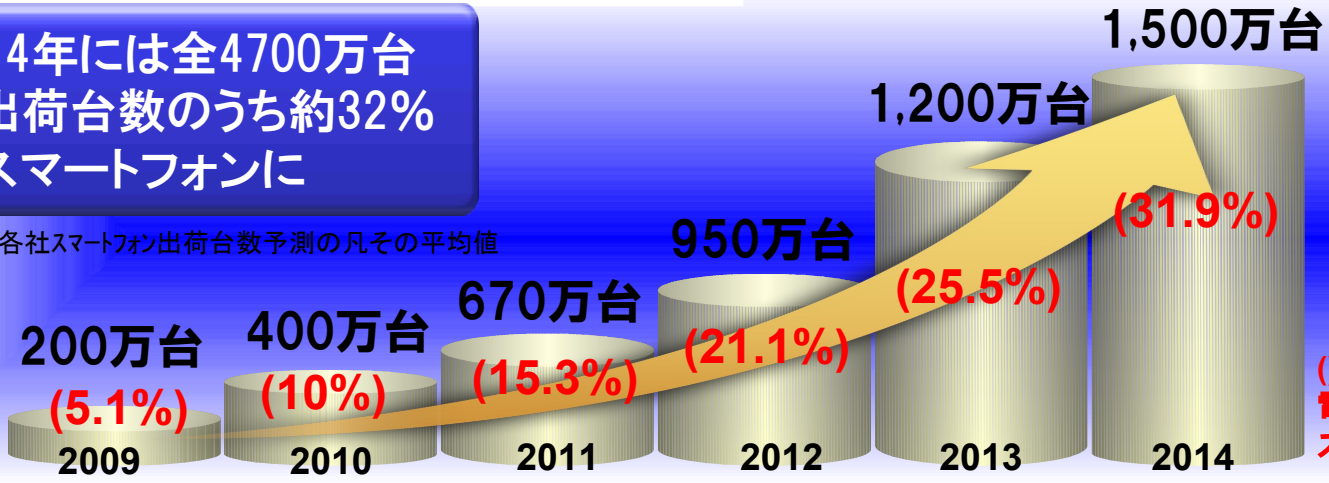
3. Androidデバイスのセキュリティサービスと
企業利用に向けてのスマートフォン戦略について

スマートフォンのマクロ市場動向(国内)

シンクタンクのマクロ予測(出荷台数)

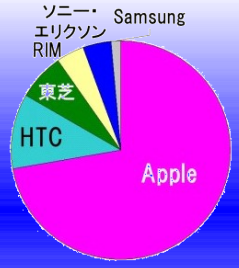
2014年には全4700万台の出荷台数のうち約32%がスマートフォンに

※シンクタンク各社スマートフォン出荷台数予測の凡その平均値



()内の数値は全携帯電話出荷台数に対するスマートフォンの割合

iPhone効果で国内でもスマートフォンの認知度急上昇



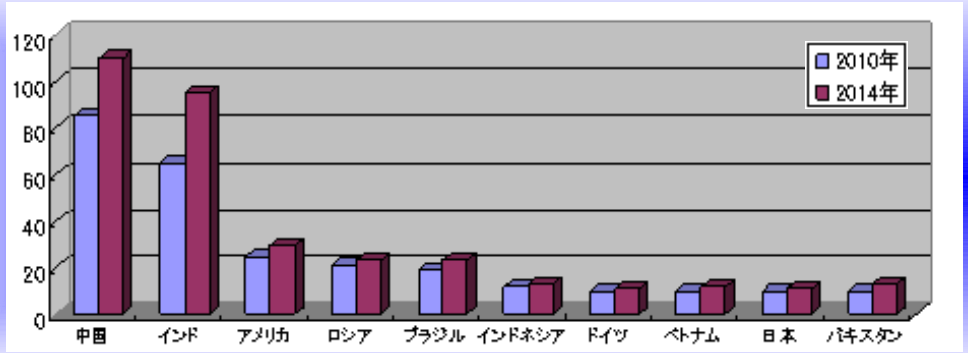
メーカー別にみると日本国内ではiPhoneが圧倒的シェア

2009年OS別出荷台数　MM総研

- iPhone3GSの登場以来iPhoneがスマートフォン市場を牽引

スマートフォンのマクロ市場動向（海外）

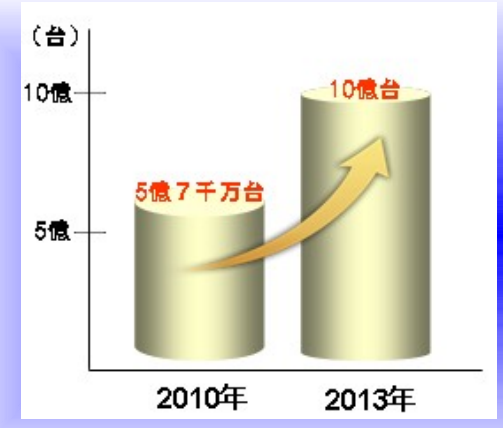
携帯電話の契約台数（予測）



2011年までに用いられる携帯電話の数は50億台に達する見込み

※Newsweek(2010.10.20)記事

世界で使用されているスマートフォンの総台数（予測）



※Newsweek(2010.10.20)記事

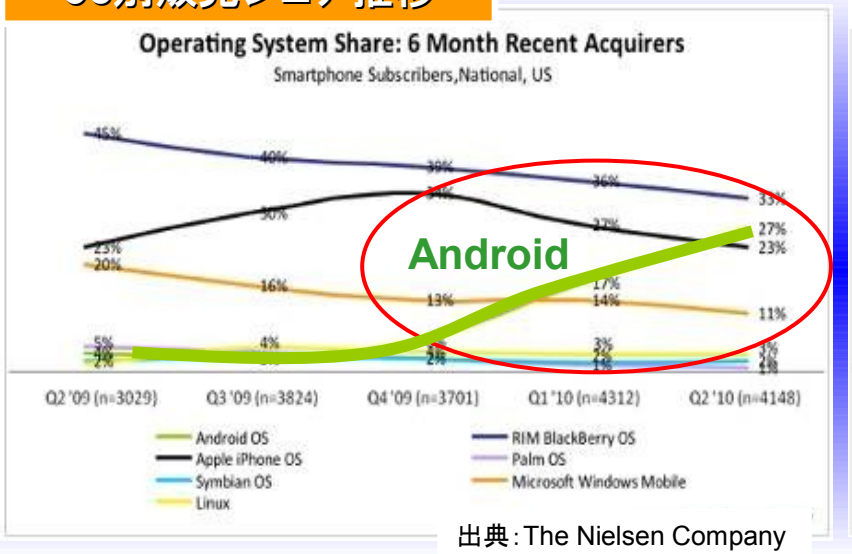
2013年までに用いられるスマートフォンの数は10億台に達する見込み

- 新規登録されるAndroid携帯電話は平均20万台/日
- アメリカ市場においてAndroidはアップルを抜いてスマートフォン向けプラットフォームのシェア1位に

※2011年から10年経てば、販売される携帯電話のほぼすべてがスマートフォンになると予想されている。

スマートフォンのマクロ市場動向（海外）

OS別販売シェア推移



出典：The Nielsen Company

OS別ユーザシェア推移

出典：The Nielsen Company

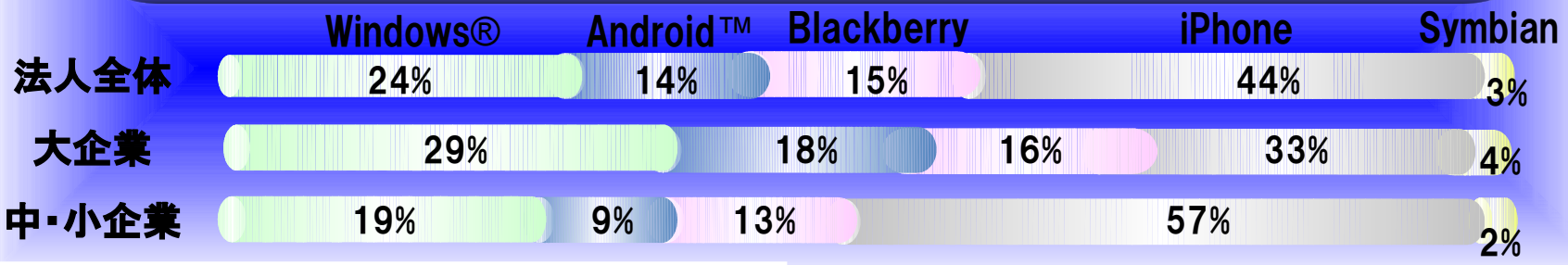
米国では2010年2Qに販売シェアでAndroid™がiPhoneを抜いて2位に。

Windows® phoneの開発予定モデル数や
各メーカーのAndroid™強化宣言などから当面は
Android™ OSが趨勢となることが予想される。

法人におけるスマートフォンOSの採用動向

法人における採用OS毎のシェア

大企業　：セキュリティや開発環境面からWindows®の選択が多い
中小企業　：コストや手軽さからiPhoneがシェアを獲得



※KDDI独自ヒアリングによる結果

お客様の動向

米国ではBlackberryユーザの
58%がAndroid™他OSへの移行を検討

※出典：The Nielsen Company

スマートフォンOSへのこだわりをヒアリング。
「Windows®OS必須：10%」、「こだわりなし：87%」に

※KDDI独自ヒアリングによる結果

今後の予測

Windows phone

6.5系統の端末が少なくなることからシェアダウンと想定

ANDROID

市場認知度の高まり、法人要件への対応、豊富なラインナップでシェアアップ

引き続き注目度は高いが、端末ラインナップが少ないため現状維持と想定

アジェンダ

1. Androidデバイスの市場動向

2. Androidデバイスのセキュリティ検証

3. Androidデバイスのセキュリティサービスと
企業利用に向けてのスマートフォン戦略について

法人のお客さまにおけるスマートフォンニーズ

法人におけるスマートフォンの利用ニーズ

社内外システムとの連携により、モバイル環境での業務効率化に活用

外回り・現場作業向けの業務支援

- 社内メールの送受信
- スケジュール機能
- 日報業務など
- 倉庫などの在庫管理
- 流通などの配送業務支援

管理者視点

情報漏洩防止や
ウイルス対策等の
「安心」、「管理のしやすさ」
が求められるように！

ユーザ視点

これまでの
フィーチャーフォンにない
「使いやすさ」、「見易さ」が
求められるように！

システム提供者視点

開発言語やアプリ配信
といった「開発のしやすさ」、
「アプリ管理のしやすさ」
が求められるように！

「セキュリティ」と「ユーザビリティ」と「開発環境」がスマートフォンのキーワード

アジェンダ

1. Androidデバイスの市場動向

2. Androidデバイスのセキュリティ検証

3. Androidデバイスのセキュリティサービスと
企業利用に向けてのスマートフォン戦略について

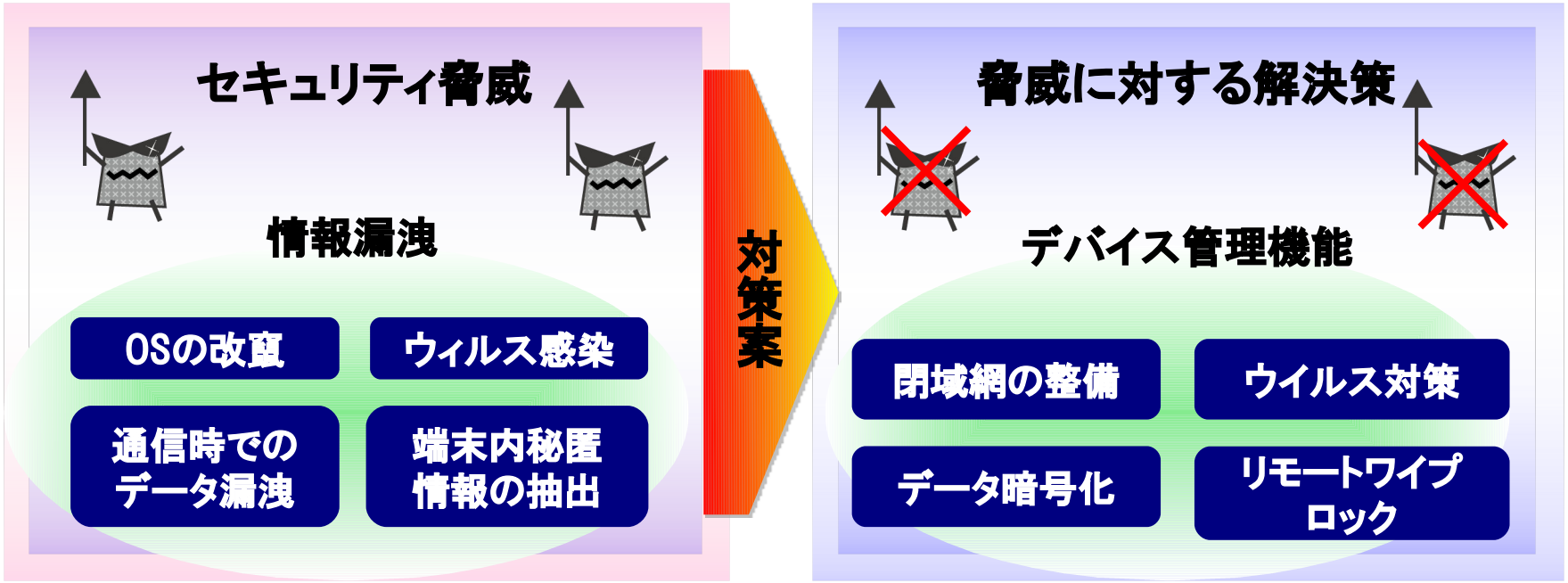
KDDIのセキュリティ課題に対する取り組みについて

セキュリティに関するニーズ

法人におけるスマートフォンのセキュリティニーズ

セキュリティ対策は進んできているものの、まだまだ完全とはいえない

⇒通信時のデータ漏洩リスク対策
⇒root奪取（端末の乗っ取り）を防ぐ対策　等々



法人で安心して使用出来るセキュリティ環境整備が必要

脅威に対して必要とされるセキュリティ対策

脅威の区分	携帯電話における脅威の例	原因	対策に使える技術
なりすまし	フィッシング	メール送信元偽造	スキャン Web Rating 専用セキュアブラウザ
		メールによる偽サーバーへの誘導	
		接続先サーバー偽装	
改ざん	システムファイルやシステムアプリケーションの改変	マルウェア	スキャン
		不適切なファイルパーミッション設定	
		ファームウェア改造	
	ユーザコンテンツの改変	マルウェア	スキャン
		不適切なファイルパーミッション設定	
否認	ユーザが気づかないうちにメール・SMSの送信および音声通話の発信やパケット通信を行う	マルウェア	スキャン
漏洩	個人データ（メール，画像・音声・動画，スケジュール，ブックマーク，電話帳，履歴等）の漏洩	マルウェア	スキャン Anti-Theft 暗号化
		端末盗難・紛失	
		SDカード盗難・紛失	
	Cookie情報の外部サーバへの漏洩	メールによる偽サーバーへの誘導	Web Rating スキャン
		脆弱性を突くデータの受信	
		JavaScriptによるRebinding	
	SIMや機器情報の外部サーバへの漏洩	マルウェア	スキャン
サービス拒否	Bluetooth接続要求の繰り返しによる操作妨害	外部からの送信	ファイアウォール
	メール・SMS/MMSの大量受信および音声通話の断続的な着信	他端末上のマルウェア	ファイアウォール
	音声通話の断続的な着信拒否	マルウェア	スキャン
	無線機能の停止	マルウェア	スキャン
	メール・SMS/MMSの大量送信および音声通話の断続的な発信	マルウェア	スキャン
	端末の機能の異常終了，使用不能，再起動	マルウェア	スキャン ファイアーウォール
		脆弱性を突くデータの受信	
		不適切なファイルパーミッション設定	
権限昇格	root権限の取得 system権限の取得 他のアプリケーション権限の取得	マルウェア	スキャン ファイアーウォール
		脆弱性を突くデータの受信	
		不適切なファイルパーミッション設定	

脅威のモデル化と対策

STRIDEモデルでは、脅威を「Spoofing（なりすまし）」「Tampering（改ざん）」「Repudiation（否認）」「Information disclosure（情報漏えい）」「Denial of service（サービス拒否）」「Elevation of privilege（権限昇格）」の6つに分類します。
これをモバイルデバイスに当てはめ、脅威の可能性と対策案を考えてみます。

スキャン

端末上にあるファイル、あるいはこれから端末にダウンロードしようとしているファイルやデータをチェックし、脆弱性を突くようなデータやマルウェアが含まれていないかを調べるコンテンツスキャン技術。単なるパターンマッチングではなく、対象のファイルの種類や特性、発見対象のマルウェアやデータの特性に応じて最適化された方法を用いることで、シグネチャファイルのサイズが小さく、スキャンによる端末パフォーマンス劣化を最小限に抑える。

Web Rating

閲覧する先のサーバが危険なWebサイト（マルウェアを配布しているWebサイト、フィッシングサイトなど）かどうかをリアルタイムにチェックし、ユーザーにその評価結果を示す技術。日常的に専用サーバが世界中のWebサイトをチェックし、評価をデータベース化している。

Anti-Theft

端末を紛失した、あるいは盗難に遭った場合、遠隔からその端末を使えないようにロック、端末内データの消去、端末位置を示す技術。端末内データの暗号化を含む場合もある。

ファイアウォール

TCP/IP、Bluetoothなどプロトコルスタック上を流れるデータを監視し、必要に応じてデータを遮断する技術。

フィルタリング

ファイアウォールとは異なり、アプリケーションレベルでデータをチェックし、必要があればアクセスを遮断する技術。

この表はすべてを網羅しているわけではありませんが、脅威とその対策方法例を挙げました。これを見ると、脅威の多くがスキャン技術によって対応可能であることが分かると思います。このように、コンテンツスキャンはモバイルセキュリティ対策を行う場合の基本であり、最初に導入を検討すべきことと言えるでしょう。

モバイル用セキュリティソフトウェアに求められること

コンテンツスキャンに代表されるモバイルデバイス用のセキュリティ対策ソフトウェアを端末内で実装する場合、PCの場合とは根本的に異なる特性が求められます。

ポータビリティを持つこと

現在のモバイル業界には、さまざまな種類のOSやモバイルプラットフォームが存在します。これがAndroid-OSのプラットフォームでも、バージョンの違いにより互換性の有無が異なる場合があります。それぞれに全く別の実装をするのではなく、1つの実装がなるべく多くのプラットフォームで動作できるような、なるべく少ないポーティング労力で済むような根本的設計思想が求められます。

少ないリソースで動作すること

モバイルデバイスはPCと比較すると、CPUは高性能化が進んでいますが、複数アプリケーションが使用できるメモリ量が少ない場合があります。またネットワーク通信が伴う場合、その無線インフラの安定性が期待されます。そのような制限のある環境でもユーザーの作業に大きく影響しないパフォーマンスが求められます。

拡張性があること

ティ技術を製品製造時から組み込む場合もあり、一度出荷されてしまうとソフトウェアの入れ替えなどの機能的拡張が困難な場合があります。脅威は進化し、新種のマルウェアがいつ発生するか分かりません。組み込みの場合においても、必要に応じて動的に機能拡張ができる仕組みが求められます。

既存デバイスとAndroidデバイス比較

ニーズ	要件	E05SH (KCP3.0)	Android™ (2.2)	WindowsMobile® (6.5.3)	iPhone (4.0)	BlackBerry (6)
セキュリティ	ロック/ワイプ	○	○	○	○	○
	Root取得防御（OS改竄防御）	○	× NG ※1 → ○	× NG	× NG	× NG
管理機能制限	管理者機能制限	○ 管理者による機能制限設定が可能	× NG ※2 → ○	○ サードベンダーのサービスを利用	○ 構成プロファイルの設定で可能	○ RIM社のサービス利用
開発環境	開発言語（開発者の多さ）	△ BREW	○ JAVA	○ .NET	△ Object-C	○ JAVA
	開発環境	× 有料コンパイラ	○ 主にEclipse	△ Visual Studio	△ Mac要	○ 主にEclipse
	アプリ配信管理	○ KDDIの専用サーバ	× NG ※2 → ○	○ MS Exchangeを利用	× iTunesが必要	○ RIM社のサービス利用
ユーザビリティ	ユーザビリティ	△ タッチパネル非対応	○ 2.2より操作性向上	× レスポンスが悪い	○ 高感度 高レスポンス	△ マルチタッチ非対応

※1：オペレータパックにより改竄防止に対応（本機能はauだけ）

※2：来年度2Q以降にサービス提供予定

Android™ OSバージョン2.2では操作性、セキュリティの一部が向上
法人利用において主流になると想定

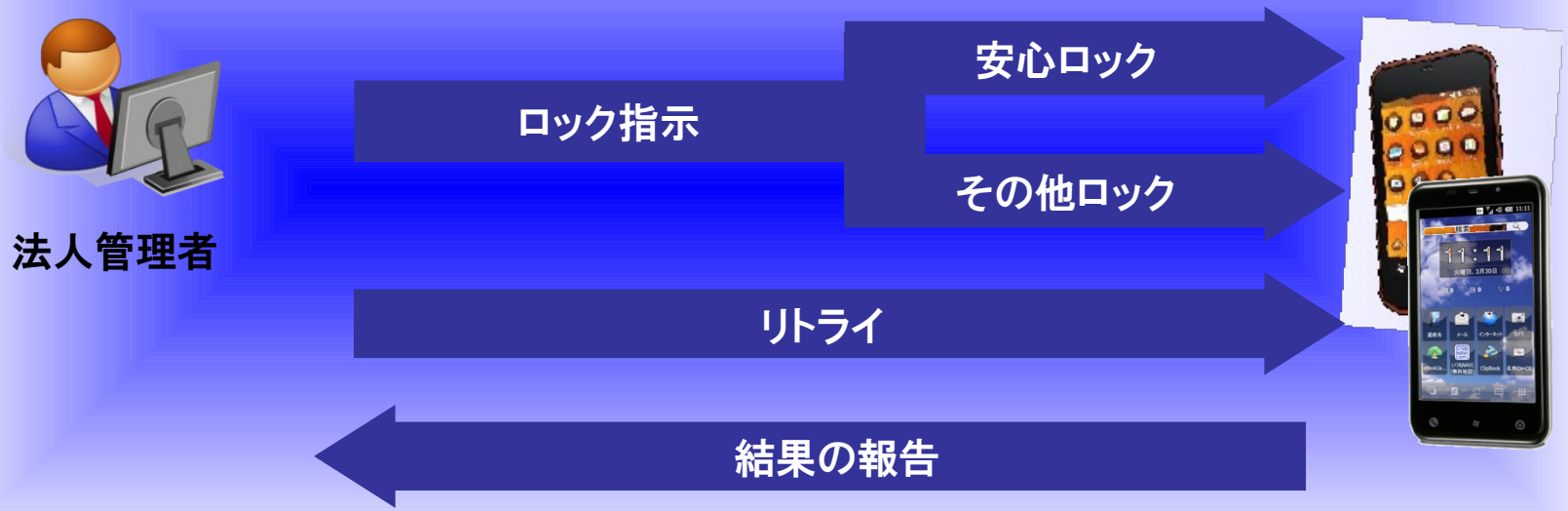
KDDI「法人スマートフォン管理」

デバイス管理

リモートロック（安心ロック）

2010年11月～

- 安心ロックは最もセキュリティレベルの高い（フィーチャーフォン同等）ロックです
- 機種（OSバージョン）を判別し最もセキュリティレベルの高いロックをかけます
- 電源OFFや圏外の場合を想定し、試行に失敗した場合はリトライします



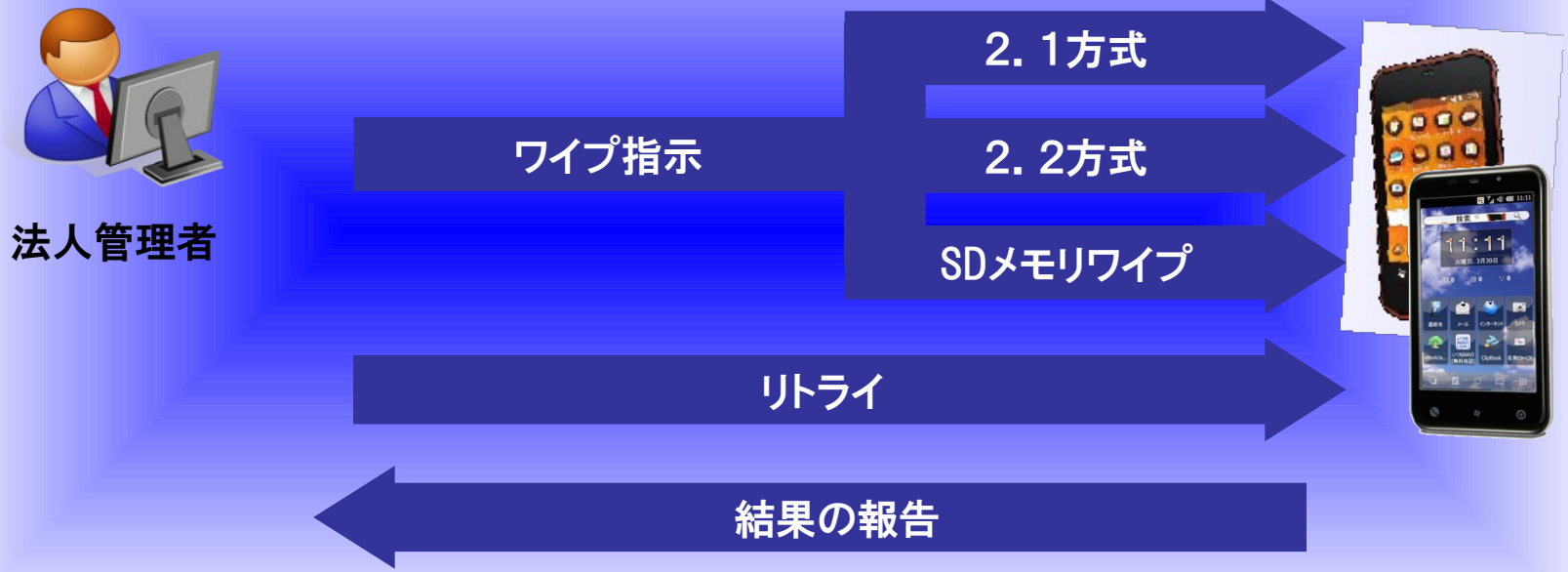
KDDI「法人スマートフォン管理」

デバイス管理

リモートワイプ

2010年12月～

- **機種（OSバージョン）を判別**し最もセキュリティレベルの高いワイプを実施します
- 電源OFFや圏外の場合を想定し、試行に失敗した場合はリトライします



KDDI「法人スマートフォン管理」

デバイス管理

デバイス設定監視アラート

- 管理者が指定するデバイス設定パターンを各端末毎に配信します
- ユーザが管理者パターンで指定するデバイス設定内容を変更すると
  アラートが管理者とユーザにそれぞれ表示されます

【監視項目】
無線ネットワーク/GPS機能/現在地情報の使用/USB/提供元不明のアプリ/UIMロック/
スリープロック/バックグラウンドデータ/DeviceAdministrator(OS:2.2のみ)

KDDI「法人スマートフォン管理」

アプリ管理

違反アプリ削除

- 管理者はインストールを許可するアプリのリスト(ホワイトリスト)を各端末毎に配信します
- ユーザがホワイトリストにないアプリ(違反アプリ)をダウンロードするとそのアプリは自動削除されます

KDDI「法人スマートフォン管理」

デバイス管理

自動デバイス再設定

- 管理者が指定するデバイス設定パターンに**強制的に設定**します
- ユーザが管理者パターンで指定するデバイス設定内容を変更すると
  アラートが管理者とユーザに表示され、管理者パターンに**強制的に再設定**します

【監視項目】
Wifi/カメラ/Bluetooth/SDメモリ/USB

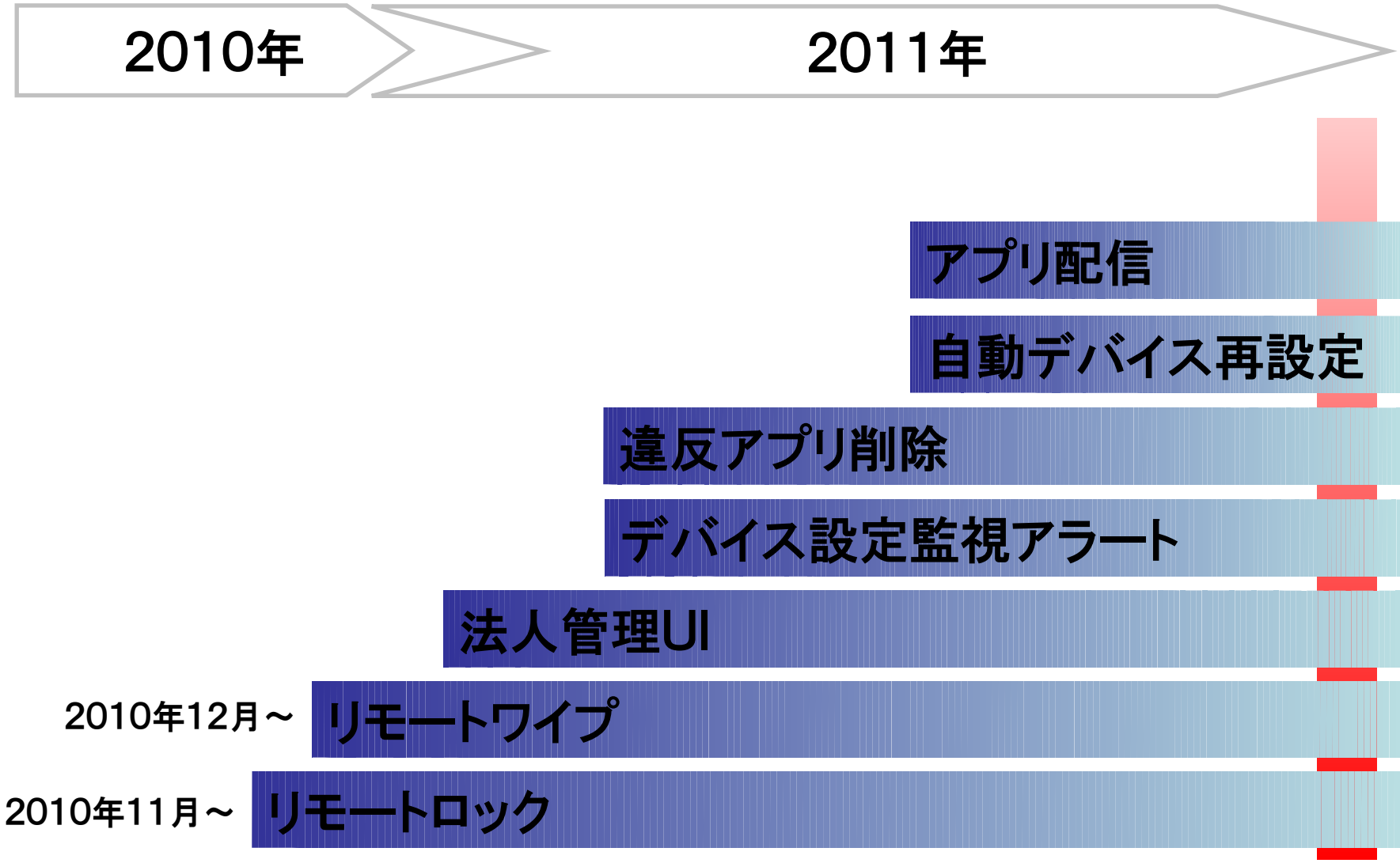
KDDI「法人スマートフォン管理」

アプリ管理

アプリ配信

- マーケットから購入したアプリ、自社開発アプリを端末に**強制的に**インストールします。
- ユーザが指定アプリを削除した場合は、アプリが**自動的に**再ダウンロードされます。

KDDI「法人スマートフォン管理サービス」のロードマップ



更に、企業が期待するスマートフォン管理機能とは、

WindowsOSやBlackBerryと比較した場合、現状のAndroidOSではセキュリティーが低い状況。
今後KDDIとしてはAndroidのセキュリティ対策を強化、他OSへの対抗策を実施予定。

■主なセキュリティ機能（検討中）

・デバイス管理
-アプリケーションデータ、SDカードの暗号化
-Bluetooth、カメラ制限
-端末情報の収集
-第三者によるルート管理

・アプリケーション管理
-アプリが利用出来る端末機能の制限
-アプリインストールの許可設定（ホワイトリスト、ブラックリスト）
-信頼のあるアプリ、勝手アプリの利用制限

・セキュリティ
-VPNクライアント対応
-ネットワークルート制御（例えば、無線LANを使わせない）
-CPAによるネットワークセキュリティ

企業利用に向けての
スマートフォン戦略について

法人におけるスマートフォン管理ニーズ

セキュリティ／管理

◆セキュリティ系
- ・リモートロック
- ・リモートワイプ
- ・無くした場所
- ・パスワードポリシー
- ・メール／URLフィルタ

◆管理系
- ・利用者／電話番号
- ・利用アプリ

ケータイとPCの融合

ケータイと同等のセキュリティ
PC並みの管理

管理／セキュリティ

◆管理系
- ・資産/構成管理
  - ・ハード／ソフトライセンス
  - ・利用者管理
  - ・デバイス利用状況
- ・キッティング
- ・ヘルプデスク

◆セキュリティ系
- ・ウイルス対策
- ・アプリ利用の制限

ケータイ視点

移動機利用の「安心」
（セキュリティ）が必要

セキュリティ＋管理

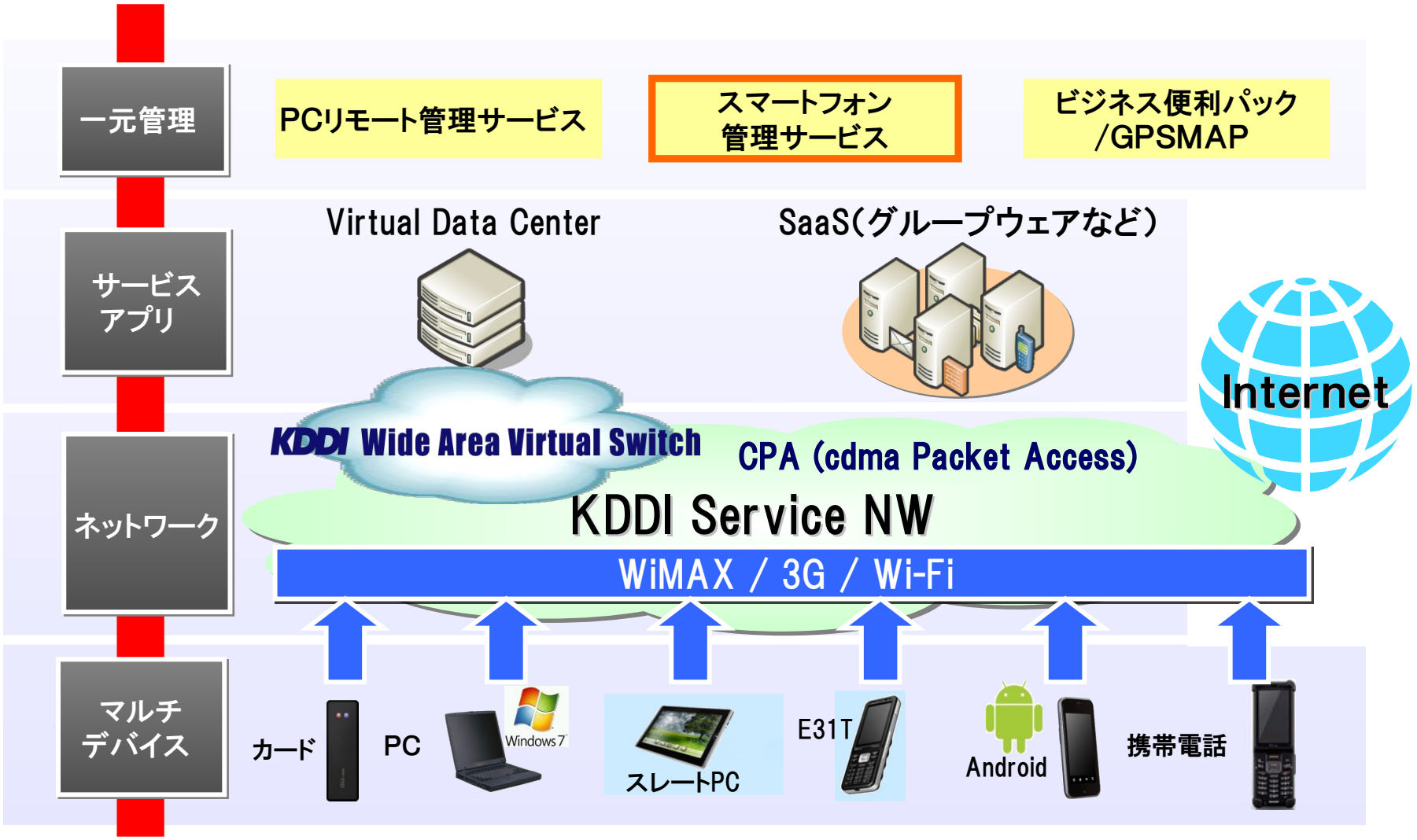
移動機の「セキュリティ」
＋「管理」が
求められるように！

PC視点

PC利用の資産やキッティング・
利用者など「管理」が必要

「セキュリティ」＋「管理」環境をスマートフォンに提供

企業向けスーマフォン管理サービスのポジション



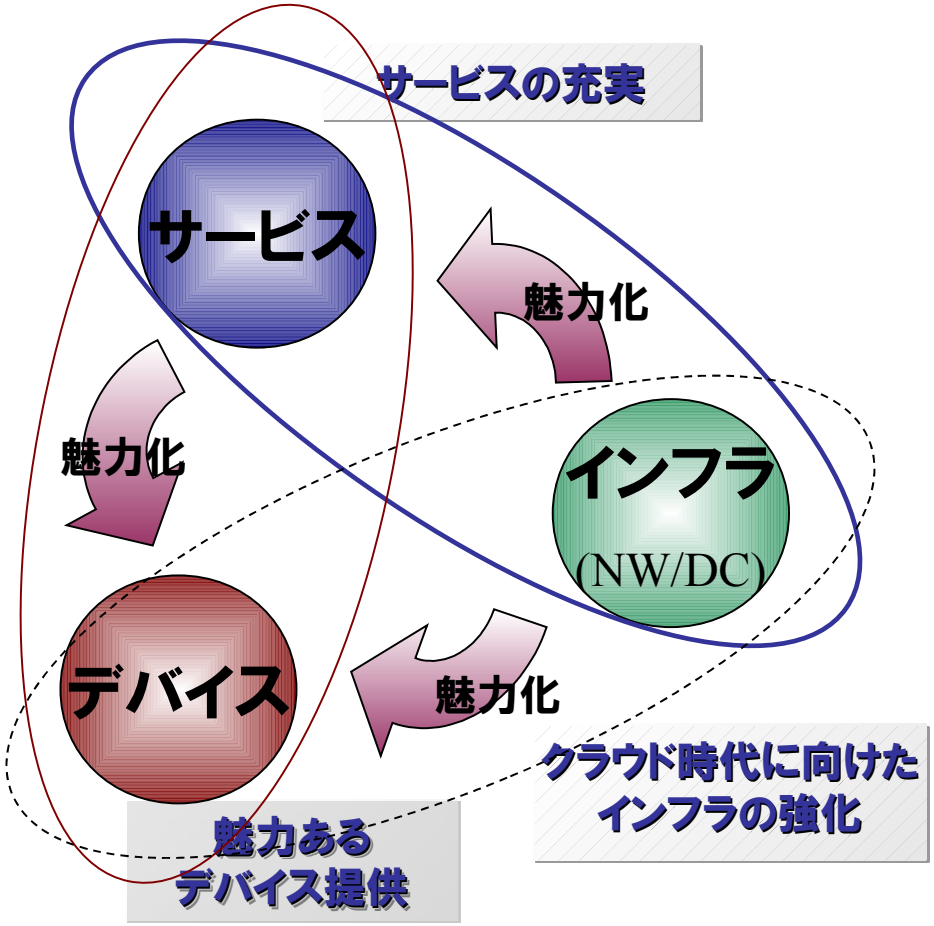
KDDIモバイルビジネス戦略

お客様のニーズに合ったデバイス提供

- Android™端末
- Windows Mobile®端末
- Android™業務特化型スレートノート
- Wimax&cdmaハイブリットカードの提供

デバイスと連携したサービスの投入

- RFIDを活用したソリューションサービス
- モバイルPCと連携したバーチャルデータセンタサービス
- 情報セキュリティ
- 資産管理
- クラウドサービス（SaaS）と連携した認証課金PF等のサービス



「デバイス」「サービス」「インフラ」の三位一体の戦略を実施
お客様の価値向上へのサポート実施していきます

会社力最大化へ。

Designing The Future

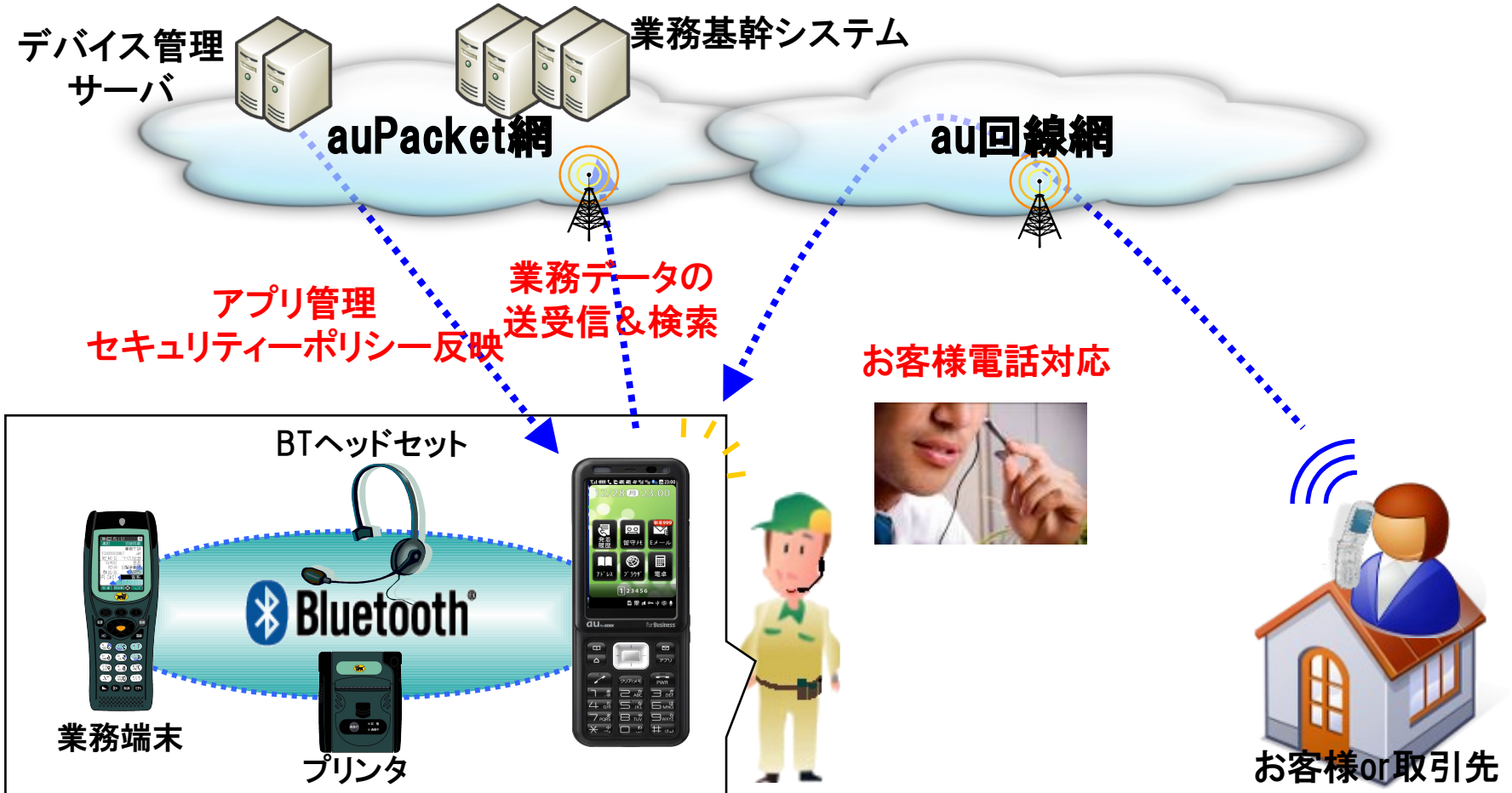
KDDI

KDDI Solution

ご清聴有難うございました。

モバイル活用シーン1

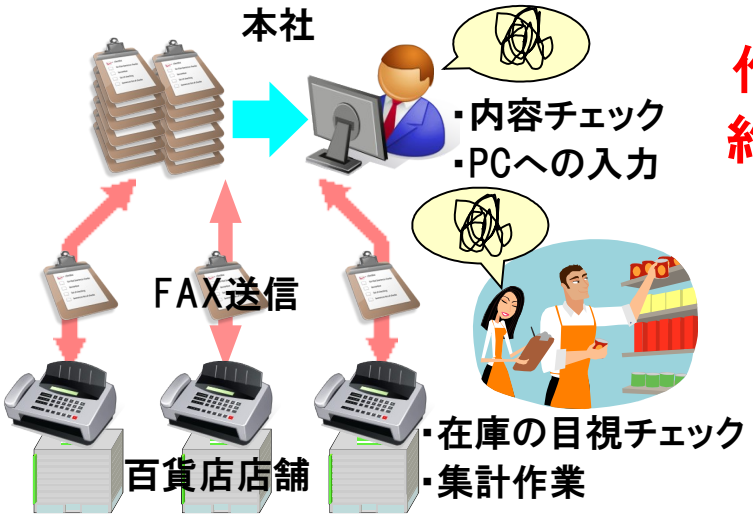
運輸業界におけるスマートフォンの利用シーン



モバイル活用シーン2

アパレル業界向け「販売管理システム」による業務効率化

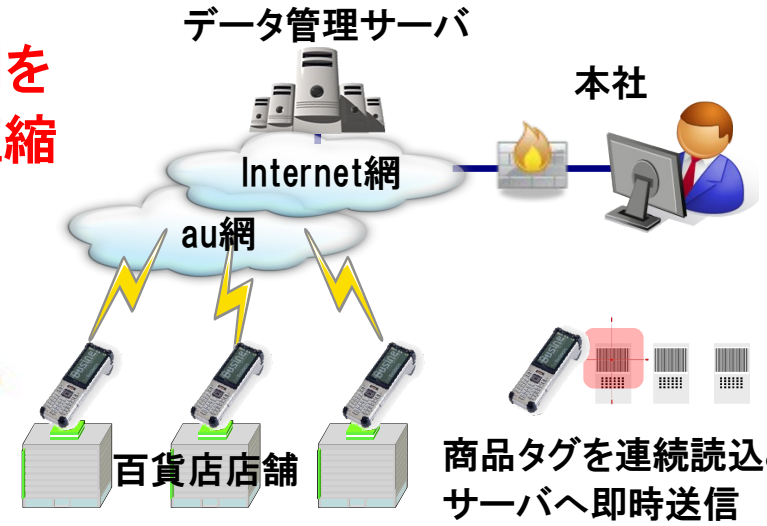
導入前の在庫管理



手作業での在庫管理、紙ベースでの報告のため現場も本部も高負荷

作業時間を
約80%短縮

導入後の在庫管理



端末の在庫管理による作業負荷軽減、在庫情報のデータ化を実現

**在庫管理システムの導入により
棚卸しの精度向上および大幅なスピードアップを実現**

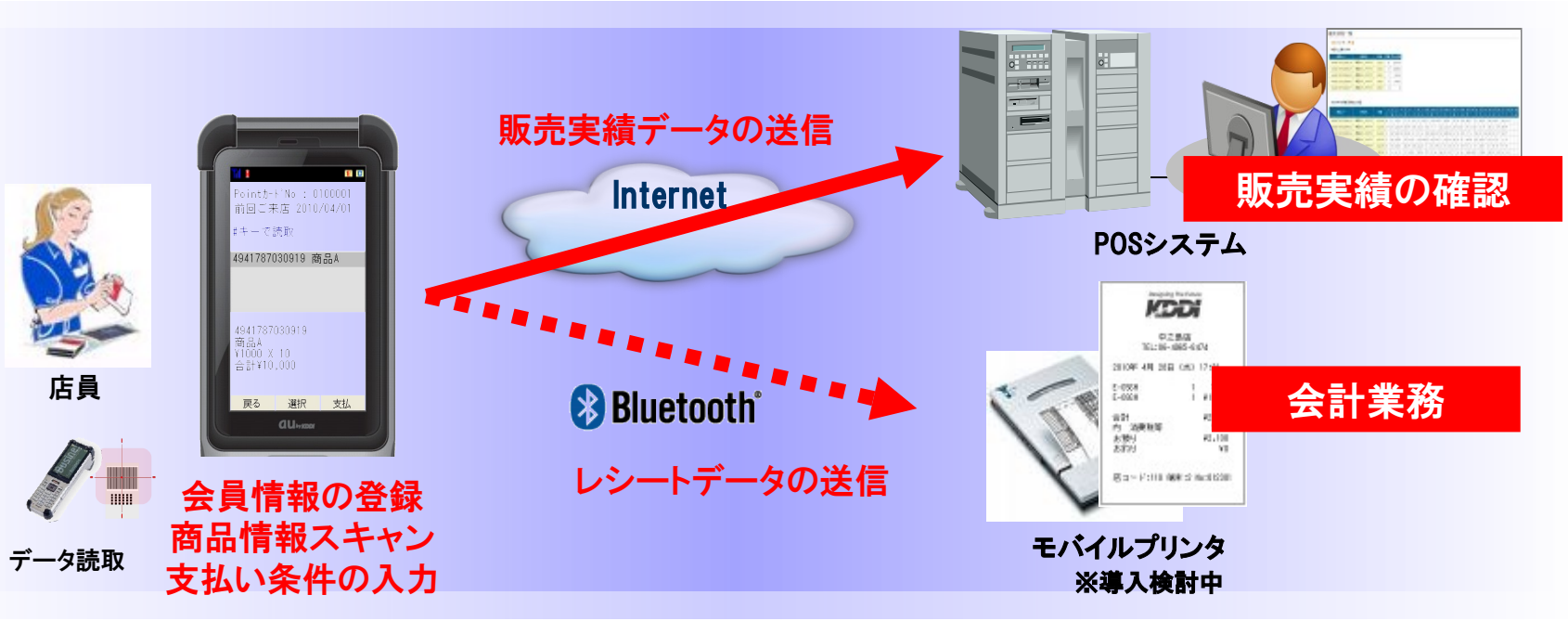
モバイル活用シーン3

■モバイルアプリケーションの利用状況

- 小売業や卸売業、製造業、倉庫運輸業を中心に物品管理（棚卸し）や受発注管理、配送管理用途で活用している。

■店舗の販売管理システムのモバイルアプリケーションとして導入

- デパートの集中レジを利用する専門店や催事販売場での販売実績がリアルタイムに確認可能 !!
- スマートフォンを活用することで初期コストを最小限に抑えられ、機能修正も容易 !!



モバイル活用シーン4

警備業界向け隊員指令システム

auGPS携帯電話を隊員に貸与し、カーナビと基幹システムとの組み合わせにより、
1. 全隊員の現在位置情報を定期的に自動取得出動指令を自動化
2. Bluetoothで携帯電話に送られた出動先情報をワンプッシュ操作でカーナビに登録。出動準備時間の大幅短縮を実現

【システムイメージ】

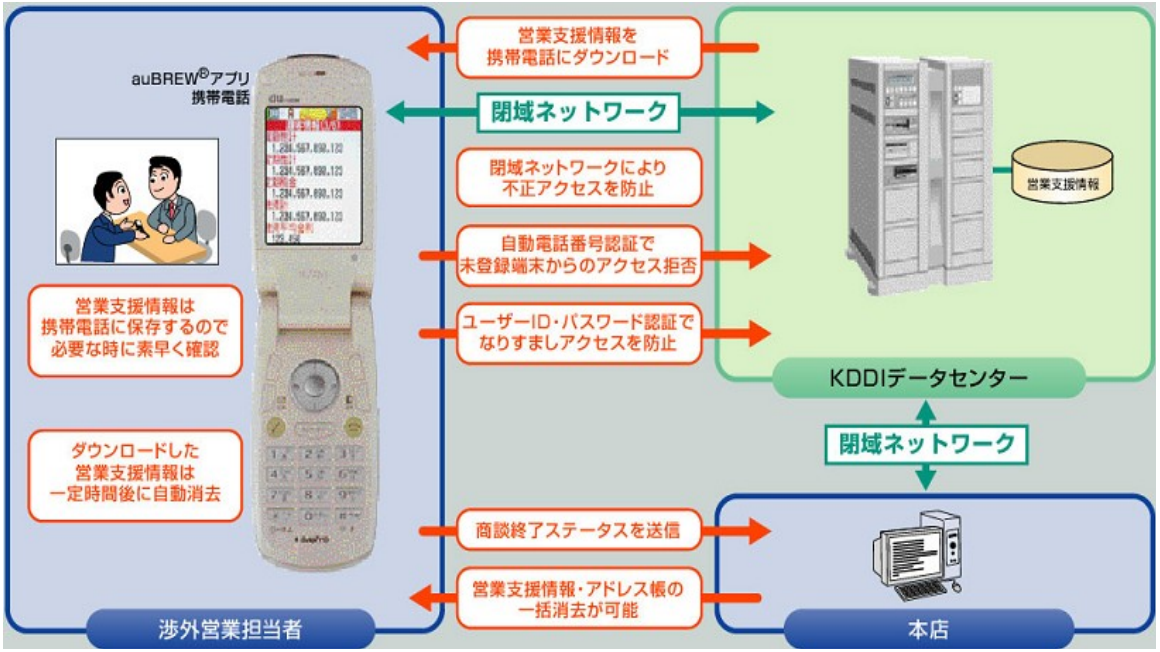
モバイル活用シーン5

営業向け支援システム

個人情報保護法施行以降、社員が利用している携帯電話が持つお客様情報(個人情報)の取扱に対する対策として、

1. 当日の朝に、当日のデータをダウンロード
2. 携帯端末側(アプリケーション側)では、業務時間中のみデータ参照が可能
3. 業務時間後は自動的にデータを削除

【システムイメージ】



【導入効果】

あらかじめ登録した情報だけが、携帯電話上で参照でき、セキュリティ向上を実現。
合わせて、商談終了時は携帯電話から報告が送信されるため、日報作成業務の軽減を実現。

モバイル活用シーン6

タクシー業界向けモバイル環境サービス

①情報共有・カーナビとしての利用

・営業所からの指示にてお客様をお迎えする際、自動的にお客様宅に目的地を設定
・乗車記録、売り上げをリアルタイムで確認
・GPSマップを利用して位置情報、経路をリアルタイムで把握
・ドライバー間での業務情報の共有

②車内無線LANサービスの提供

テザリング機能を用いたサービスを提供することで
乗車中のモバイル環境利用が可能

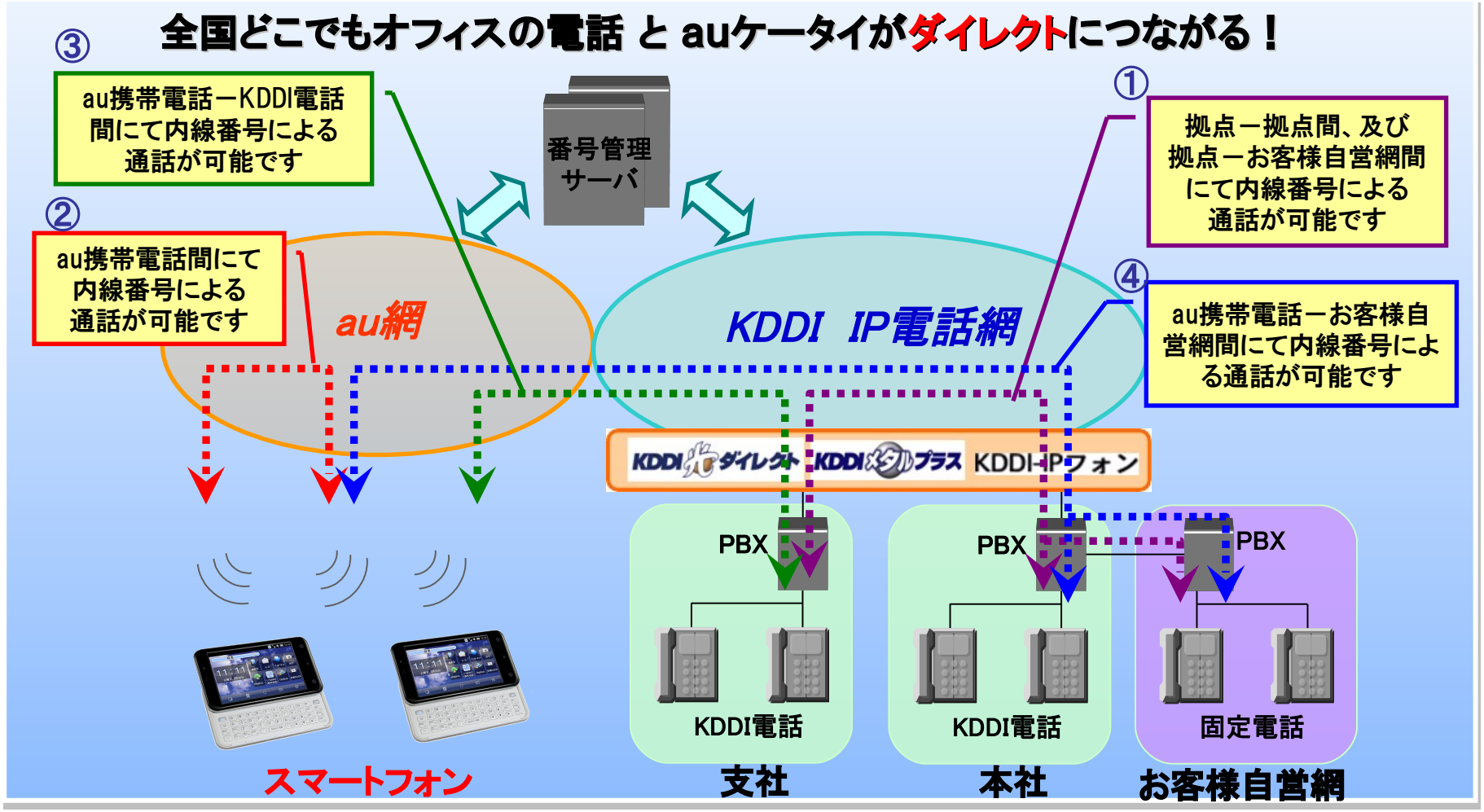
③(将来的に)車内ディスプレイの利用価値向上

・周辺情報の表示
（天気・お店・イベント情報など）
・広告

既存のサービスに比べて
大容量コンテンツ扱える双方向のサービス可能

モバイル活用シーン7

ビジネスコールダイレクトを利用した スマートフォン内線サービスの実現



モバイル活用シーン8

自動テープ起こし(議事録作成)支援サービス

ビジネスマ


①録音　②ﾃﾞｰﾀ送信


⑥補正用Webﾍﾟｰｼﾞへアクセス

⑦リピート再生を聞きながらﾏﾆｭｱﾙ修正

KDDIネットワー

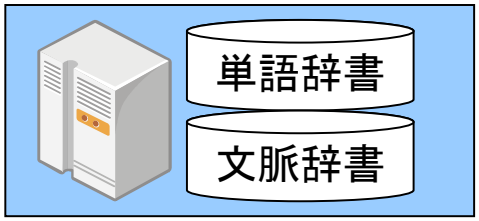
録音時間1時間で約6MBのデータ

モバイル網のみで受付けるサービス

補正後の議事メモテキスト

クラウド側

音声認識エンジン



③テープ起こし；テキスト化

④テキスト化した文章と該当する音声部分をひも付けした補正用Webページを作成

⑤補正用Webページを案内(事前登録されたPCアドレスへも)

文書1 ・・・・・・・・・・・・・ 削除 音声確認・修正

文書2 ・・・・・・・・・・・・・ 削除 音声確認・修正

文書1 ・・ﾏﾆｭｱﾙ修正・ 修正を反映 戻る

文書1 ・・修正部・・・・・修正部・・・・修正部・・・

文書5 ・・・・・・・・・・・・・・・・・・・・・・・

文書6 ・・・・・・・・・修正部・・・・・・・・・・・

一時保管　確定・メール送信後データ消去

モバイル活用シーン9

スマートフォンを用いたカード決済サービス

現在の決済サービスモデル


POS端末

POS端末が高く、また携帯電話以上にガラパコスな状態

利用者
利用できる場所が少ない
為利用しない

加盟店
利用されないので設置しない
(手数料も高い)

カード会社
利用されないので収益が上がらない
（一回払いが多数）

スマートフォンを利用した決済サービスモデル


スマートフォン　　カードリーダー

低価格化によりカード決済端末の設置・導入が容易に

利用者
利用できる場所が増え、
生活が便利になる。

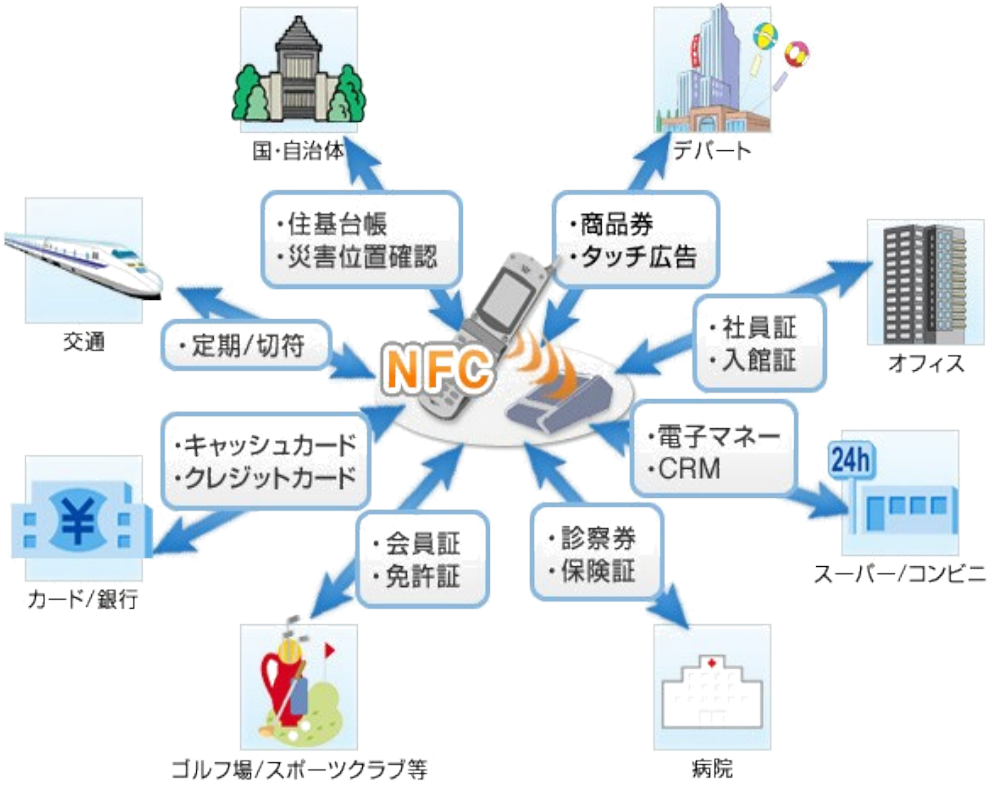
加盟店
手数料が安くなる。

カード会社
収益があがるので、
設置場所を増やそうとする。

デパートのテナントなど通信環境を構築できない、アパレル・化粧品業界へ

モバイル活用シーン10

スマートフォンをNFC機能に対応させることで
在庫管理、決済機能といった様々なソリューションを実現



様々な場面で利用が可能