特集論文

Android端末に対応したセキュアスマートフォンサービス

柘場純一*

Secure Smartphone Service Corresponding to Android Device

Junichi Haseba

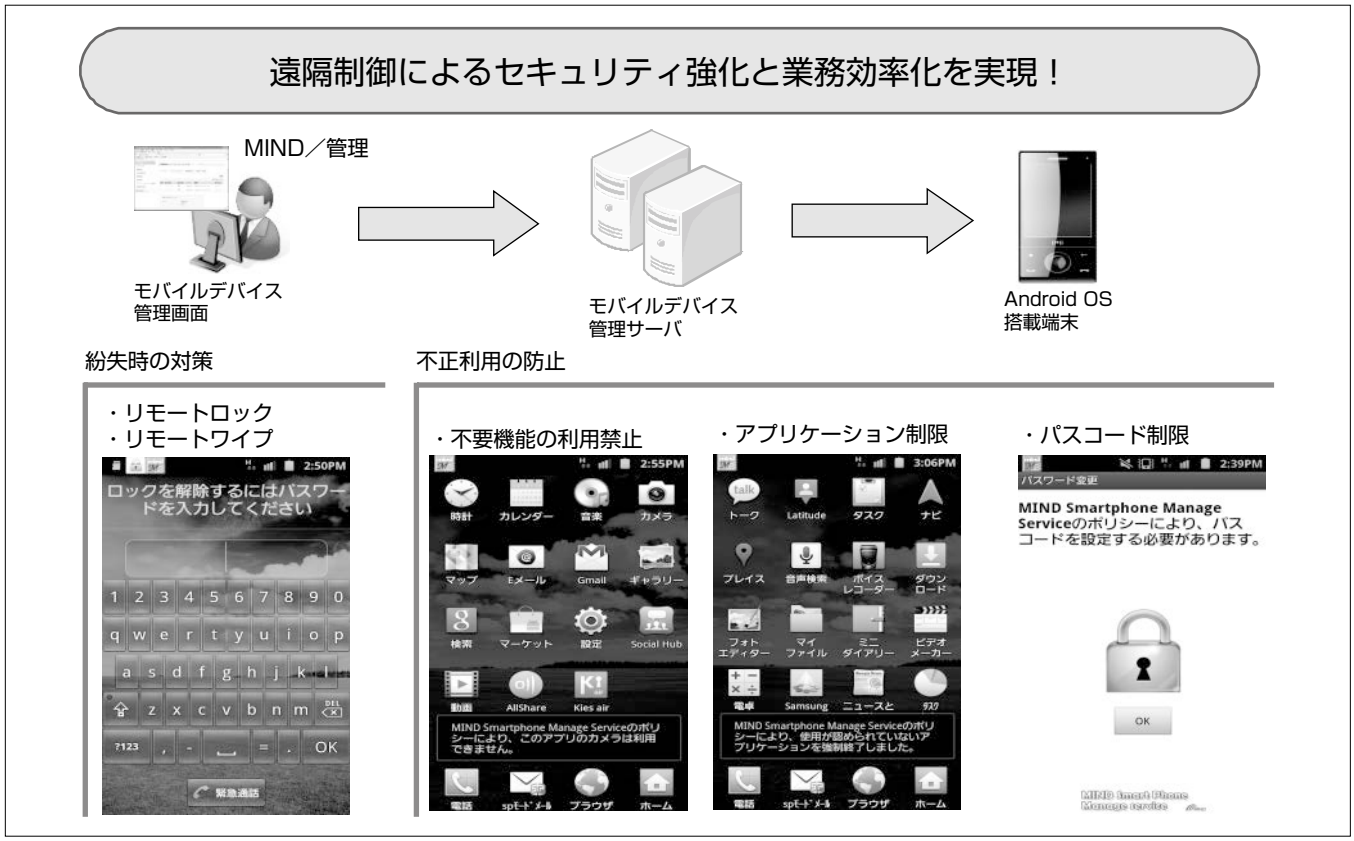
要　旨

三菱電機情報ネットワーク㈱(MIND)のモバイルネットワークサービスは，顧客の業務システムを社内利用と同様に社外から安全・快適にアクセスできるリモートアクセスサービスである。既に，iPhone／iPad(注1)のiOS搭載端末の利用を対象としたサービスを提供しており，多くのユーザーに利用されている。一方，スマートフォン／タブレット端末市場では，iOS搭載端末以外にAndroid(注2)OS搭載端末も多く出荷され，企業での業務システムを利用する端末として顧客ニーズも高い。しかし，ネットワークや端末上アプリケーションの脆弱(ぜいじゃく)性など，セキュリティ面の課題があり業務用端末として導入に踏み切れない企業も少なくない。

MINDは，それらの課題を“セキュアスマートフォンアクセスサービス”及び“スマートフォンマネージサービス”を提供することで解決し，Android OS搭載端末でも利便性とセキュリティを兼ね備え，安全・快適に利用できるリモートアクセスを実現した。

“セキュアスマートフォンアクセスサービス”では，暗号化通信と端末認証と個人認証を組み合わせ，許可された端末だけ社内業務システムにアクセス可能とし，“スマートフォンマネージサービス”では，端末の紛失・盗難時のリモートロック・リモートワイプや業務以外のアプリケーションの利用制限，インベントリィ情報の可視化等，端末の管理・監視・制御を可能としている。

（注１）　iPhone，iPadは，Apple Inc. の登録商標である。
（注２）　Androidは，Google Inc. の登録商標である。



“スマートフォンマネージサービス”

スマートフォンマネージサービスは，紛失・盗難時のためのリモートロックや端末パスコードの設定ポリシーと業務上不要な機能（カメラ，Bluetooth(注3)等）の利用禁止，管理者が指定したアプリケーション以外の使用制限等，端末の管理・監視・制御を実現している。

（注3）　Bluetoothは，Bluetooth SIG，Inc. の登録商標である。

*三菱電機情報ネットワーク㈱

1. まえがき

MINDのモバイルネットワークサービスは，顧客のOA（Office Automation）・メール・グループウェアや業務システム等を社内と同様に社外から安全・安心に利用できることが特長で，iPhone／iPadのiOS搭載端末を対象とした利便性とセキュリティを兼ね備えたサービスである。今回，スマートデバイス市場で急増するAndroid OS搭載端末の利用を可能とする機能を開発し，サービス提供を開始した。

本稿では，Android OS搭載端末の業務利用におけるセキュリティ対策の必要性と課題を示し，その解決策である“セキュアスマートフォンアクセスサービス”と“スマートフォンマネージサービス”の特長とサービス内容について述べる。

2. 市場動向

2.1 Android端末の市場動向

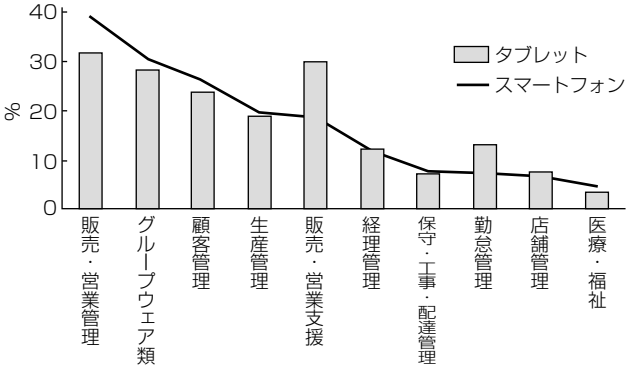
起動が早く軽量であることや画面に直接触れるという操作等，一般のパソコンにない機能が注目され，企業で導入するモバイル端末は，スマートフォン／タブレット端末に移り変わっている。企業が利用しているスマートフォンは，“販売・営業管理”や“グループウェア類”での利用割合が高い。

タブレット端末は，写真，動画，3D画像（CAD（Computer Aided Design）Viewerなど）等のメディアで効果的に情報を伝達できるだけでなく，カタログなどのペーパーレス化を図れる等の評価が高く，外出先から効率的に活用できる販売・営業支援のツールとして導入している企業が多い（**図1**）。

スマートフォン／タブレット端末販売台数の市場シェアを**表1**に示す。2010年に22.7%であったAndroid OS搭載端末の販売台数は，2015年には48.8%まで拡大すると予測されている。iOS搭載端末と比べ高いシェアを占めるAndroid OS搭載端末は，企業での業務システムを利用する端末として顧客ニーズが高まりつつある。

2.2 Android端末の特徴とセキュリティ課題

Android OS搭載端末とiOS搭載端末の特徴を**表2**に示す。



出典：株式会社インプレスR&D Android利用動向調査報告書2012

図1．企業におけるタブレット端末の利用業務

Android OS搭載端末の場合は，数多くの端末メーカーから出荷され，我が国でも㈱エヌ・ティ・ティ・ドコモやKDDI㈱等の大手移動体通信事業者から発売されている。iOS搭載端末と比べると，端末機種やインストールするアプリケーションが豊富で選択肢が多い。また，オープンソースOSを搭載しており，アプリケーションや通信機能等の実装は端末メーカーや通信事業者に依存している。一方，iOS搭載端末の場合は，端末メーカーはApple社だけで，搭載するアプリケーションもApple社によって管理されている。

iOS上のアプリケーションは，Apple社が事前審査したものをApple Storeなどに限定した公式サイトからインストールするのに対し，Android上のアプリケーションはGoogle社が提供するGoogle Playなどに限定されず，通信事業者，端末メーカーを始め数多くのサイトから自由にインストールすることが可能である。そのため，事前審査を行っていないアプリケーションに関して，脆弱性の対策やセキュリティリスクを回避することが課題となっており，業務用端末としての導入に踏み切れない企業も少なくない。

2.3 企業が求めるスマートフォン／タブレット端末導入に必要なセキュリティ機能

企業がスマートデバイスに求めるセキュリティ対策を**表3**に示す。

Android OS搭載端末を業務端末として利用する場合のセキュリティ対策のポイントは，次の3点に大別することができる。

(1) 通信経路のセキュリティ対策
(2) 業務外・不正利用の禁止（デバイス制御）

表1．世界のスマートフォン端末販売台数（OS別）

OS		2010年	2011年	2012年	2015年
iOS	販売台数（千台）	46,598	90,560	118,848	189,924
	市場シェア（%）	15.7	19.4	18.9	18.9
Android OS	販売台数（千台）	67,225	179,873	310,088	539,318
	市場シェア（%）	22.7	38.5	49.2	48.8
他OS	販売台数（千台）	182,824	197,268	201,540	375,656
	市場シェア（%）	61.6	42.1	31.9	32.3
合計	販売台数（千台）	296,647	467,701	630,476	1,104,898

出典：Worldwide Communication Device Open OS Sales to End Users by OS（Thousands of Units）Gartner（April 2011）

表2．端末のOSと特徴

端末のOS	提供元	特徴
iOS	Apple社	①“Apple Store”の登録は，Apple社が審査したアプリケーションを登録 ②アプリケーションの配布や利用時にはApple社と契約。Apple Storeから配布，課金 ③iOS上でだけ稼働し，最新バージョンの適用が容易
Android OS	Google社	①“Google Play”の登録は，Google社は審査せず，その活用は利用者の裁量 ②通信業者などが運営するマーケットへの登録が可能。それぞれの基準で配布，課金 ③オープンソースのOSで，各端末メーカが独自にカスタマイズして搭載 ④デバイスの選択肢が豊富 ⑤OSバージョンが同一でも機種依存あり

(3) 端末・アプリケーション管理の効率化

これらのポイントは，iOS搭載端末でも同様のニーズであったが，Android端末に特有なセキュリティリスクの回避として，利用するアプリケーションの制御や端末のポリシー違反の検知等を強化する必要があった。

3. リモートアクセスソリューション

Android OS端末におけるセキュリティ課題を解決するため，iOS搭載端末対応の既存の認証システムの仕組みと連携することで，端末固有の識別子とデジタル証明書を利用した端末認証やVPN(Virtual Private Network)通信を可能とし，不許可端末の利用防止を“セキュアスマートフォンアクセスサービス”で実現した。さらに，MDM(Mobile Device Management)によるAndroid OS搭載端末の管理・監視・制御を“スマートフォンマネージサービス”で実現し，データ保護及び盗難・紛失対策に加え，きめ細かい管理権限の設定やポリシー違反の検知等の仕組みを実現した。また，複数端末の集中管理による一括設定などの効率化を可能としている(**図2**)。

3.1 セキュアスマートフォンアクセスサービス

このサービスは，データ通信を暗号化(IPSec(注4))し，デジタル証明書による端末認証とユーザーID(IDentitier)とパスワードによる個人認証を組み合わせて，強固なアクセス制御を実現している。iOS搭載端末と同様に，Android OS搭載端末でもIPSecVPNモジュールや端末識別情報(IMEI(International Mobile Equipment Identifier)，MAC(Media Access Control)アドレス等)を搭載している。iOS搭載端末と同じ方式でこれらの端末情報を照合し，Android OS搭載端末の場合もアクセスが許可された端末及びユーザーだけ認可し，許可されていない端末及びユーザーであれば拒否することが可能である。

(注4) Security archtecture for Internet Protocolの略で，IPパケット単位で改ざん防止や秘匿機能を持ったプロトコルである。

表3．企業における主なセキュリティ対策

想定される脅威	脅威への対策
通信傍受・盗聴	暗号化通信による通信データの秘匿
	通信環境に依存しない安全なアクセス
	利用したアクセスログなどの収集管理
不正利用・不正侵入	企業が許可した端末・ユーザーのみ許可
	パスコードポリシーの設定
	業務上不要な機能の利用制限
情報搾取・漏洩・マルウェア感染	スマートフォン／タブレット端末の状態管理
	紛失による情報漏洩(ろうえい)の防止と遠隔制御の実現
	管理者が許可したアプリケーションソフトウェア以外の利用禁止

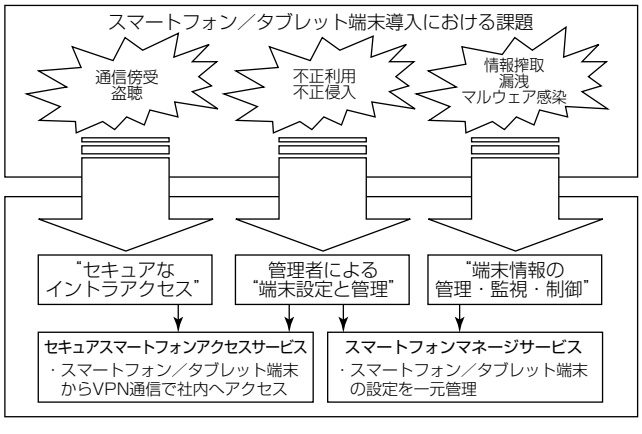


図2．スマートフォン／タブレット端末導入における課題と対策

3.2 スマートフォンマネージサービス

このサービスの機能は，セキュリティ機能，ポリシー管理機能，端末管理機能の3つに分類される。それぞれの主な機能を**表4**，**表5**，**表6**に示す。

このサービスは，複数のスマートフォン／タブレット端末を企業のセキュリティポリシーで管理・監視・制御することを可能としている。利用端末の機種やインストールされているアプリケーション等の情報を収集する機能を持っている。また，端末の状態管理，紛失時の遠隔制御(リモートロック／リモートワイプ)，管理者が指定したアプリケーション以外の使用制限を実現し，企業の端末管理者に

表4．主なセキュリティ機能

No.	分類	機能	内容
1	リモートワイプ	初期化	工場出荷時に初期化
2	リモートロック・アンロック	ロック・アンロック	ロック・アンロックの実行
		サイレン鳴動	リモートロック時にサイレンを鳴動
3	ローカルワイプ	−	ローカルロック時，所定の回数以上パスワードを失敗した際に，データを消去
4	遠隔削除	遠隔初期化	内部SDカード内のデータを消去
		個別データ削除	個別のデータを消去

表5．主なポリシー管理機能

No.	機能名	機能	内容
1	遠隔設定	ローカルセキュリティポリシー	パスワードポリシーの設定
		WLAN設定	無線LANのアクセスポイント情報の設定
		特権SIM設定	SIM交換ロック時の設定
2	利用制限	デバイス利用制限	・カメラ機能の利用可否 ・Bluetoothの利用可否 ・外部メモリ(SDカード)の利用可否 ・無線LANの利用可否 ・緊急番号(110，118，119)以外への発信先制限
3	アプリケーション管理	インストールアプリケーション情報	ホワイトリストによるアプリケーションの利用可否

WLAN：Wireless LAN，SIM：Subscriber Identity Module

表6．主な端末管理機能

No.	機能名	機能	内容
1	遠隔情報取得	ロック・アンロック	ロック・アンロックの状態取得
		端末情報	ファームウェア情報やメモリの空き容量等の情報取得
2	VPN設定	インストールアプリケーション情報	インストールされているアプリケーションの情報取得
		位置情報	端末の位置情報の取得
3	遠隔監視	デバイス利用制限	利用制限状態の取得
		ローカルセキュリティポリシー	ローカルセキュリティポリシー設定の定期取得
		インストールアプリケーション情報	インストールされているアプリケーション情報の定期取得
		位置情報	端末の位置情報の定期取得

代わってMINDがサービスとして提供する。

次に，遠隔から搭載端末の管理・監視・制御する仕組みを述べる。iOS搭載端末の場合，Apple社が提供するAPNs（Apple Push Notification service）とモバイルデバイス管理サーバと端末間の通信・制御プロトコルが決められている。一方，Android OS搭載端末の場合は，Google社から“C2DM（Cloud to Device Messaging）サーバ”が提供されているが，複数端末の一元管理や機能拡張の柔軟性が乏しいため，国内外の大手通信事業者では，これとは方式が異なる国際標準方式のプロトコルを広く採用している。このサービスも国際標準方式のプロトコルを採用し，C2DMで実現できない管理者権限の設定とグループの階層化や企業のポリシーにあわせた複数端末への一括設定を可能とした。

また，セキュリティリスク回避のため，ユーザーの意思にかかわらず管理者からの指示を最優先とし，端末利用中のリモートロックなどの強制制御や端末に対する管理・制御のオペレーションの進捗・成否・レポート管理の情報収集機能を持ち，監査履歴の一元管理を可能としている。

3.2.1　サービス処理フロー

Android OS搭載端末の管理・監視・制御の処理フローを**図3**に示す。遠隔管理の処理は，国際標準のプロトコルであるOMA（Open Mobile Alliance）-DM（Device Management）(注5)方式を使用している。

⑴　端末照合

MDMシステムの端末操作画面で，事前に登録された端末の加入者番号（MSISDN：Mobile Subscriber ISDN（Integrated Services Digital Network）Number）及び端末製造番号（IMEI）を指定し，端末管理の制御要求を送信する（**図3**①）。MDMシステムでは，指定された端末への制御が許可されている場合，制御要求を受け付けると端末に対し制御を開始するためメッセージとしてPackage（以下“Pkg”という。）#0（DMN：DM Notification）を端末へ送信する（**図3**②）。Pkg#0（DMN）を受信した端末はパケット接続及びSSL（Secure Sockets Layer）ネゴシエーションを行う。端末はセッション確立後，IMEIなどの端末情報を含んだPkg#1をMDMシステムへ送信する（**図3**③）。Pkg#1を受信したMDMシステムは，指示された制御対象端末であるかをIMEIの照合によって判定する。

⑵　遠隔制御

判定後，制御コマンドを含んだPkg#2を端末へ送信する（**図3**④）。Pkg#2を受信した端末は，制御コマンドの内容に応じた制御を実行する。端末で制御完了後に，Pkg#3で完了報告をMDMシステムへ送信する（**図3**⑤）。

⑶　制御結果確認

MDMシステムはPkg#4で受信確認を端末へ送信し（**図3**⑥），Pkg#3がMDMシステムで正常に受信されたことを端末が認識すると，DM制御を終了する（**図3**⑦）。同時にMDMシステムは，制御完了報告を端末操作画面に表示し，制御を終了する。また，制御完了時にMDMシステムの操作画面を通して端末の設定状態を確認できる。

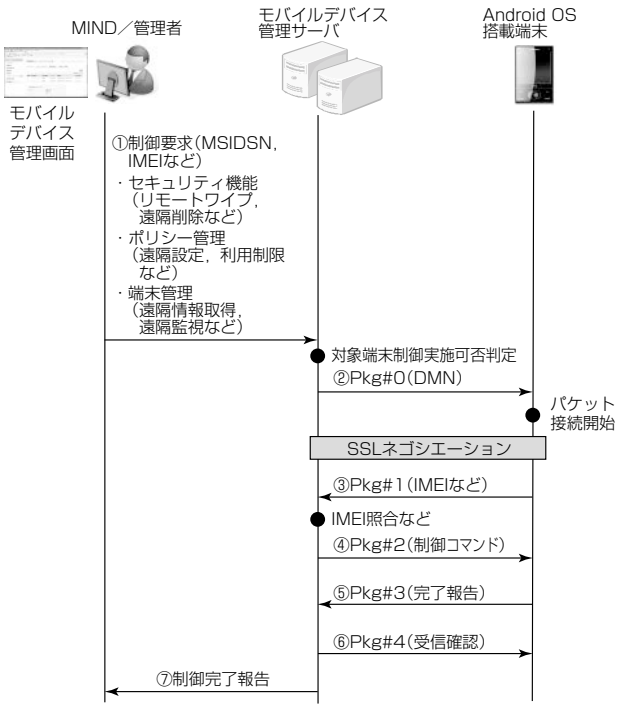


図3．スマートフォンマネージサービス実行時の処理フロー

（注5）　OMAはモバイル関連のアプリケーションの標準化を進める団体であり，DMはデバイス管理機能である。

4. 今後の課題

企業におけるスマートデバイスの業務利用では，セキュリティ対策を維持しつつ，個人管理の端末を業務でも利用するBYOD（Bring Your Own Device）やIT資産管理の統合も注目されている。スマートフォン／タブレット端末のセキュリティ対策機能の拡充とマルチデバイス化の資産管理を可能とした統合的管理機能を付加する等，サービス機能の向上が今後の課題である。

5. むすび

Andoroid OS搭載端末のスマートフォン／タブレット端末から，安全・快適に社外から社内業務システムが利用可能なサービスを実現した。今後は，多機能携帯端末であるスマートデバイスの特長を活用して，社内無線ＬＡＮ（Local Area Network）経由による業務システムの利用，ビデオ会議用端末としての活用等，利用者のワークスタイルにあったワンストップサービスのメニュー拡充を図っていく。

参考文献

⑴　涌井道子，ほか：端末管理に対する多様なニーズに対応した端末管理制御基盤システムの開発，NTT DOCOMOテクニカル・ジャーナル，**17**，No.3，50～54（2009）