特集論文

スマートフォンで社内に安全にアクセス “セキュアスマートフォンアクセスサービス”

柘場純一*
木岡宣明*

"Secure Smartphone Access Service"：Service for Secure Access to Office

Junichi Haseba, Yoshiaki Kioka

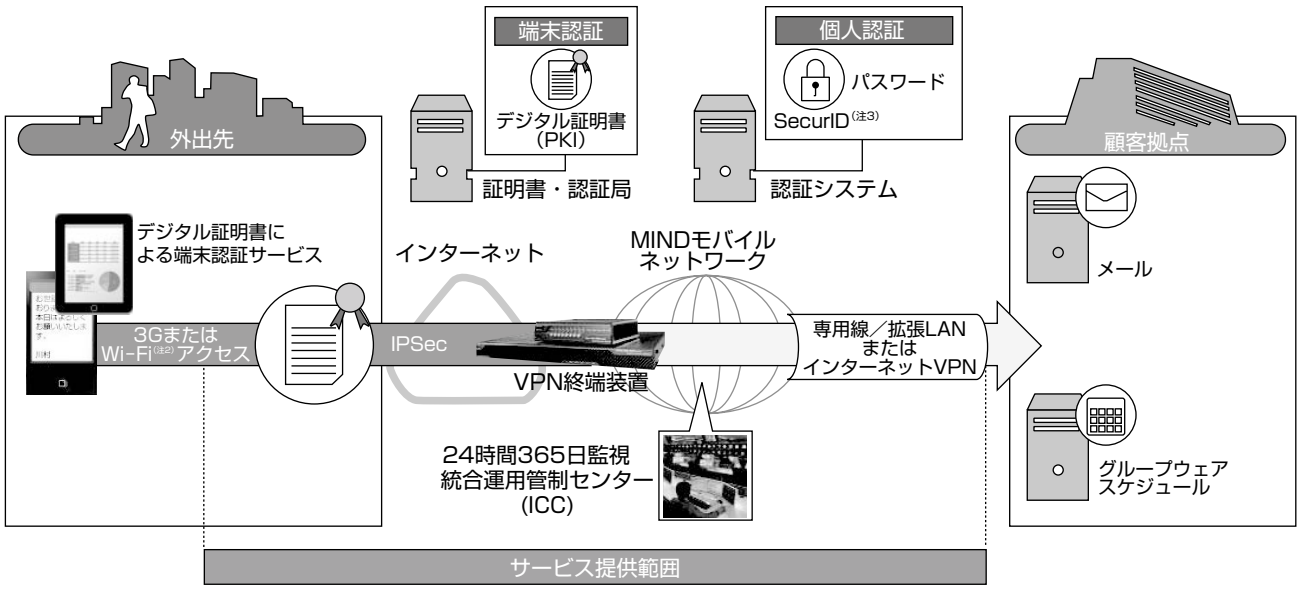
要　旨

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リモートから安全・安心にアクセスできるリモートアクセスサービスを提供し，企業ユーザーから高評価を得ている。ネットワークの設計・構築・稼働後の運用保守，アウトソーシングまでをMINDがワンストップで提供し，ユーザーはモバイル端末を用意するだけでリモートから社内業務システムが利用可能となる。iPhone／iPad(注1)の市場投入を皮切りに，モバイル端末の利用ニーズは，従来のモバイルパソコン主体から手軽で操作性が優れた端末として注目されているスマートフォン／タブレット端末に移ってきている。

一方，セキュリティ面では，従来のモバイルパソコンと同等のセキュリティレベルを維持しつつ，スマートフォン／タブレット端末特有のセキュリティ対策を必要とすることから，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”“スマートフォンマネージサービス”を提供することで解消し，スマートフォン／タブレット端末でも利便性とセキュリティを兼ね備え，快適・安心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”は，現行のモバイルネットワークサービスのユーザーID認証及び暗号化通信に加え，証明書による“端末認証”を組み合わせ，許可された端末のみ社内の業務システムにアクセス可能にしている。スマートフォンマネージサービスは，スマートフォン／タブレット自体の端末管理を可能とし，紛失時に遠隔で端末ロック・データ消去を可能とした。

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



（注2）　Wi-Fiは，Wi-Fi Allianceの登録商標である。
（注3）　RSA SecurIDは，EMC Corp. の登録商標である。

3G　：3rd Generation
IPSec：Security Architecture for Internet Protocol
PKI　：Public Key Infrastructure
VPN　：Virtual Private Network

“セキュアスマートフォンアクセスサービス”の概要

セキュアスマートフォンアクセスサービスは，データ通信を暗号化（IPSec）しデジタル証明書による端末認証とユーザーID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機能を実現している。

*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，1997年サービス開始当初から，顧客の業務システムを社内アクセスと同様にリモートから安全・安心に利用できることが特長で，ネットワークサービスの設計・構築・稼働後の運用保守，アウトソーシングまでをワンストップサービスとして提供している。今回，スマートフォン／タブレット端末を利用可能とした“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”の提供を開始した。

本稿では，スマートフォン／タブレット端末利用における利便性とセキュリティを兼ね備えた“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／タブレット自体の端末管理を可能とした“スマートフォンマネージサービス”の特長やサービス内容について述べる。

2. 市場動向

2.1 スマートフォン／タブレット端末の市場動向

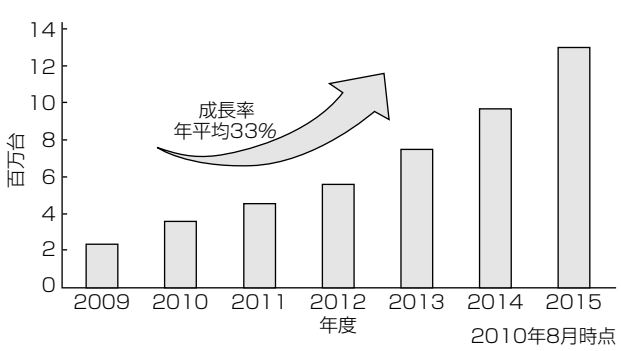
iPhoneの市場投入を皮切りにコンシューマー市場でスマートフォンが急速に普及し，国内のスマートフォン／タブレット端末の市場は，年平均33%のペースで成長している。2015年には1,300万台まで増えると予測されている（**図1**）。

モバイルパソコンに比べ手軽に持ち運べるというスマートフォン／タブレット端末の利便性から，企業でも社内の業務システムを利用するモバイル端末として顧客ニーズが高まっている。

2.2 顧客ニーズとセキュリティ課題

企業で，スマートフォン／タブレット端末は，モバイルパソコン並みの情報処理能力を持った多機能携帯端末ととらえられ，メールやグループウェアを外出先から効率的に活用できる新たなモバイル端末としての利用ニーズは高い。

一方で，企業が適用しているモバイルパソコンのセキュリティレベルを維持しつつ，スマートフォン／タブレット端末特有の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，本格展開にまで至っていない企業も少なくない。



出典：日本スマートフォン市場分析2010，(株)ROA Group

図1．スマートフォン市場の規模予測（2009～2015年）

従来のモバイルパソコンに対して，スマートフォン／タブレット端末に特有な次のようなセキュリティリスクが考えられる。

(1) 端末が個人所有物であるケースが多くなり，場所や周りを気にせず利用する機会が増える。そのため，通信やユーザーID／パスワードの盗聴による脅威や企業が許可していない端末から不正アクセスされるリスクが大きくなる。

(2) 端末がモバイルパソコンと電話を兼ね備えた機能を保有しているため，企業の機密データだけでなくアドレス帳などの個人情報も保有することが多い。そのため，紛失・盗難時や多種多様なアプリケーションソフトウェアの利用時等における個人情報漏洩（ろうえい）の事故が発生するリスクが大きくなる。

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

企業がスマートフォン／タブレット端末導入に求めるセキュリティ機能を次に挙げる。

(1) 企業が貸与または許可した端末のみアクセスを許可
(2) 企業が許可したユーザーのみ社内へのアクセスを許可
(3) 業務システムとのデータ通信は暗号化
(4) 利用したアクセスログなどの収集管理
(5) スマートフォン／タブレット端末の状態管理
(6) 紛失による情報漏洩の防止と遠隔制御の実現
(7) 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使用禁止

このような背景から，企業がモバイルパソコン利用に適用している情報漏洩対策のセキュリティ機能を継続しつつ，不許可端末の利用防止や端末の状態管理など，スマートフォン／タブレット端末に関する特有のセキュリティ対策について，モバイルネットワークサービスの機能拡充を図る必要があった。

3. リモートアクセスソリューション

3.1 セキュアスマートフォンアクセスサービス

ユーザーの社内システムへのアクセス制御機能（**2．3節**(2)），データ通信の暗号化機能（**2．3節**(3)），利用したアクセスログ等の収集管理機能（**2．3節**(4)）は，モバイルネットワークサービスの既存の認証システムと連携した仕組みを実現することで可能とした。

端末のアクセス制御機能（**2．3節**(1)）は，既存の認証システムにはなく，スマートフォン／タブレット端末の端末認証機能を加える必要があった。個々のスマートフォン／タブレット端末を識別し，3GモデルやWi-Fiモデルの機種に依存せず認証可能な仕組みとして，端末識別情報に紐（ひも）づけたデジタル証明書による端末認証を搭載した。デジタル証明書による認証の仕組みは次のとおりである（**図2**）。

①端末識別情報を基に指定端末のデジタル証明書を発行

する。

②発行されたデジタル証明書を指定端末にインストールする。インストール時に指定端末であるかを証明書認証局で認証し，認可されればインストールされる。

③デジタル証明書がインストールされたスマートフォン／タブレット端末からVPN(Virtual Private Network)クライアントソフトウェアを利用しIPSec集線装置に接続する。IPSec集線装置で，アクセス許可されたデジタル証明書であるかの認証を実施する。アクセス許可された端末であれば認可し，許可されていない端末であれば拒否する(端末認証)。

④認証システムで，ユーザーID及びパスワードの認証を実施する。アクセス許可されたユーザーID及びパスワードであれば認可し，許可されていないユーザーID及びパスワードであれば拒否する(個人認証)。

⑤端末認証及び個人認証で許可された端末かつユーザーのみ，アクセス回線経由で業務用サーバにアクセス可能となる。

3.2 スマートフォンマネージサービス

スマートフォン／タブレット端末の状態管理(**2. 3節**(5))，紛失による情報漏洩の防止や遠隔制御(**2. 3節**(6))，管理者が指定したアプリケーションソフトウェア以外の使用禁止(**2. 3節**(7))を実現し，管理者に代わってMINDが“スマートフォンマネージサービス”として提供する。

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。また，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などの情報を収集する機能を有し，インベントリ情報を可視化できる。**図3**にスマートフォンマネージサービスを示す。

このサービスの機能は，①セキュリティ機能，②ポリシー管理機能，③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1**，**表2**，**表3**に示す。

スマートフォンマネージサービスは，Apple社から提供されているiPhone／iPad iOS4.0で制御可能な端末管理“モバイルデバイスマネジメント(MDM)”の仕組みを利用

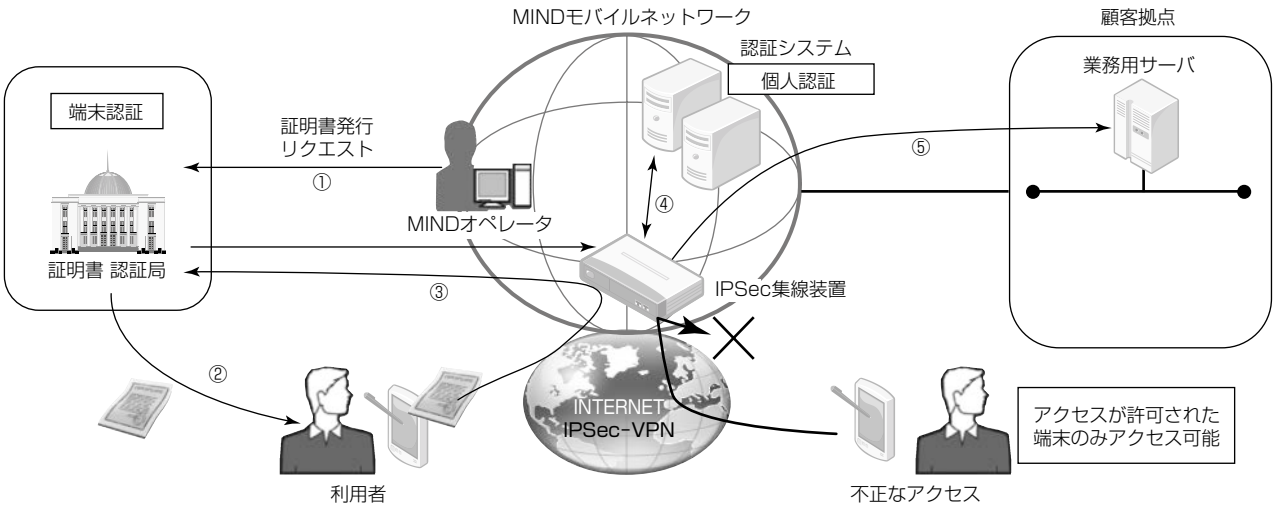


図2．デジタル証明書による認証

エンドユーザーに配布されたスマートフォン端末を遠隔制御・状態管理し，情報漏洩防止を実現
⇒ 盗難・紛失時の端末ロックやデータ消去
⇒ 許可されたアプリケーションソフトのみ利用，不許可アプリケーションソフトを削除

顧客に代わり，管理者から命令を送信(運用代行)，
日常運用はもちろん，いざという時にも，すばやく確実に対応！

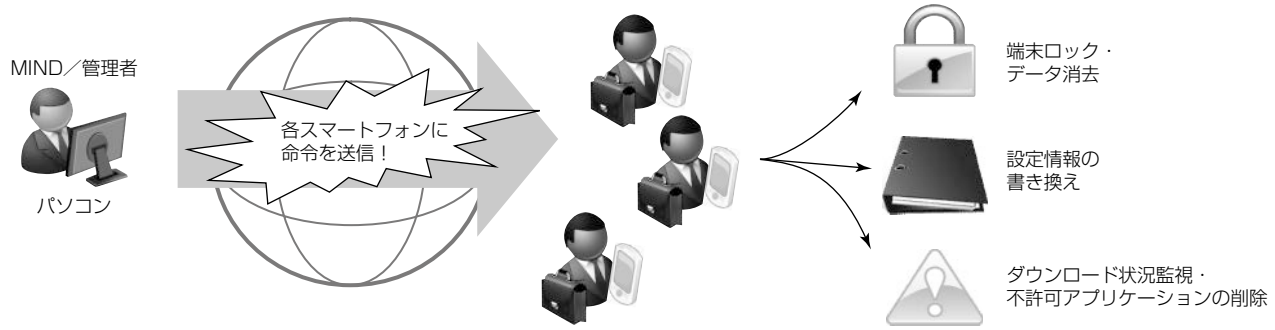


図3．スマートフォンマネージサービス

表1．主なセキュリティ機能

機能名	内容
リモートワイプ	データ消去(工場出荷時に初期化)
リモートロック・アンロック	ロック・アンロックの実行
必要なパスコード数	最小パスコード長の設定
パスコード更新頻度	パスコードの更新頻度の設定
許容される失敗数	パスコードの失敗回数の設定

表2．主なポリシー管理機能

機能名	内容
アプリケーションのインストール	新たなアプリケーションのインストール可否
カメラの使用	カメラの利用可否
画面キャプチャ	画面キャプチャの実行可否
Safari(注3)の利用	Safariの利用可否
YouTube(注4)の利用	YouTube利用の実行可否

(注3)　Safariは，Apple Inc. の登録商標である。
(注4)　YouTubeは，Google Inc. の登録商標である。

表3．主な端末管理機能

機能名	内容
Wi-Fi設定	Wi-Fiのアクセスポイント情報の設定
ネットワーク接続	ネットワーク接続に関する設定追加
VPN設定	VPN構成の情報設定

している。MDMの動作を**図4**に示す。

①モバイルデバイス管理サーバ(MDMサーバ)の情報を含む構成プロファイルをデバイスに送る。送信手段としては，3G回線やWi-Fi又は送信用パソコンからUSB(Universal Serial Bus)で送信する。

②送信された構成プロファイルをデバイスにインストールしてMDMサーバから管理されることを許可する。

③デバイスにインストールされるとデバイス情報がMDMサーバに配送され，管理対象のデバイスとして登録される。

④管理対象として登録されたデバイスに対し，APNs(Apple Push Notification service)サーバを介し対象デバイスに通知が行われ，その後MDMサーバからデバイスのポリシーコントロールが行われる。

⑤対象デバイスへのポリシー設定は，管理者がMDMサーバから対象デバイスに指示・要求することで行われる。

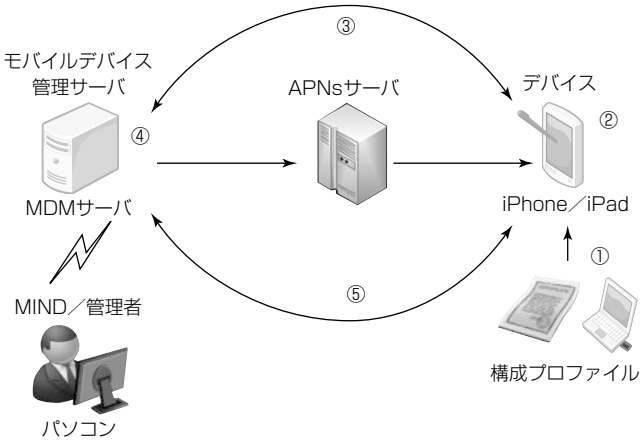


図4．モバイルデバイスマネジメントの動作

“セキュアスマートフォンアクセスサービス”“スマートフォンマネージサービス”が提供する機能によって，モバイルパソコンと同等のセキュリティポリシーやソリューションを適用することができ，手軽で操作性を損なわないというスマートフォンの特長を生かしつつ，リモートから社内の業務システムを安心・安全に利用できる。

4. 今後の課題

スマートフォン市場では，iOSを内蔵したiPhone／iPad以外にAndroid(注5)OSを内蔵したスマートフォン／タブレット端末も多く出荷されている。現在MINDが提供している“セキュアスマートフォンアクセスサービス”“スマートフォンマネージサービス”は，iPhone／iPadに対応しているが，Android OSのスマートフォン／タブレット端末も今後サポートする予定である。Android OSでのサービス提供機能の検証を行い，サービスメニューの拡充を図っていく。

(注5)　Androidは，Google Inc. の登録商標である。

5. むすび

ITの技術進歩や利用環境の多様化から，リモートアクセスの分野でもITシステムにおけるネットワークサービスが複雑化している。常に利用者のワークスタイルにあったサービス提供を心掛ける必要があり，今後も顧客ニーズをとらえ，快適・安全に利用できるネットワークを継続提供していく所存である。