スマートフォンの業務利用における留意点

Guidelines when using Smartphones for Business Purpose

遠　藤　英　幸

要　約　タッチパネル式の大型ディスプレイを装備したスマートフォンが急速に普及する中で，スマートフォンのビジネスでの利用が始まっている．従来のモバイル PC の代替としたり，携帯性や常時接続性を活かせる業務フローへの組み込みが行われている．本稿では，スマートフォンの特性を，従来型携帯や PC と比較しながら考察し，業務利用におけるセキュリティ面での留意点を述べるとともに，発展途上にあるスマートフォンの段階的導入を提言する．

Abstract　The use of the smartphone for the business purpose begins while smartphones equipped with touch-panel large display spread rapidly. Smartphones are incorporated into the business flow drawing on the portability and the regular connectivity as an alternative for the conventional mobile PC. This paper looks at the characteristics of the smartphone by comparing the conventional portable phone and PC, and discusses the security guidelines when using for the business purpose, as well as proposes the staged introduction of the developing smartphone.

1. は　じ　め　に

日本国内では，2008 年に iOS 搭載の iPhone 3G が発売され，その後，2009 年には Android 搭載の HT-03A の発売に続き，様々な Android 搭載スマートフォンが発売された．出荷される携帯電話の主流は，通話を主眼においた従来の携帯電話（以下，従来型携帯という）から，通話に加えて，データ通信を前提とした様々なアプリケーションを動作可能としたスマートフォンへと急速に変化している．その結果，その利便性に惹かれた利用者が急増することとなり，携帯電話市場においてそのシェアを急速に伸ばしている．その中で，ノート PC に代わる新デバイスとして，スマートフォンのエンタープライズ利用が脚光を浴びている．

本稿では，スマートフォンの特性を，従来型携帯や PC と比較しながら考察し，業務利用におけるセキュリティ面での留意点を述べる．

2. スマートフォンの特性

まず，スマートフォンについての定義であるが，一般的には，従来の携帯電話に，次に示す機能，特徴が加わったものを指すことが多い．

- タッチパネル式大型ディスプレイ
- フルブラウザ
- 無線 LAN
- GPS
- ネイティブアプリケーション

本稿では，これらの機能，特徴を持った携帯電話をスマートフォンとする．なお，さらに大型のディスプレイを有するタブレットについては，スマートフォンに含むものとし，特段の区別はしない．

2.1　スマートフォンの OS

スマートフォンが採用している主要な OS として，iOS，Android OS，Blackberry OS，Windows Mobile（Windows Phone）などがある．特に，Android と iOS の二つで，スマートフォン利用者数の 9 割近くを占めている．そのため，以降では，Android と iOS に限定して考察することとする．

この二つの OS の利用者数は，先行して発売された iOS が，2010 年末までは Android OS を上回っていたが，2011 年初めには逆転し，Android OS の利用者数が上回ってきている．

Android と iOS の大きな違いは，Android は複数のスマートフォンベンダが採用し，それぞれのベンダにおいてカスタマイズがなされているのに対して，iOS は Apple 社の iPhone と iPad にのみ搭載されている点[*1] である．

ベンダによるカスタマイズが行われていることは，Android に脆弱性があった場合の修正アップデートが，ベンダごとに行われざるを得ないことを示している．カスタマイズの範囲によっては，修正アップデートが実施されるまでに相当な時間を要することもある．

2.2　スマートフォンの特性

スマートフォンの特性として，次のものがあげられる．

- 携帯性に優れている
- 携帯電話回線を利用したインターネットへの常時接続性に優れている
- 無線 LAN を利用した高速通信が可能である
- フルブラウザを持つ

特に，従来のモバイル PC と比べた場合，手のひらの上で，いつでもインターネットにアクセスできる点が，大きく利便性を上げている点である．逆に，モバイル PC に比べて劣る点としては，処理能力，記憶容量やディスプレイサイズなどであるが，処理能力，記憶容量については，CPU の高速化，内蔵メモリの大容量化が進んでおり，実質的にその差を体感できるレベルでは無くなりつつある．また，ディスプレイサイズについては，利用形態上，避けることのできないことであり，タブレット型やモバイル PC との棲み分けの大きな要因のひとつである．

2.3　業務利用ニーズとハードル

スマートフォンのビジネス利用のニーズは，従来のモバイル PC と同等の機能に加え，優れた携帯性と操作性を合わせ持つことが浸透するに従って高まりを見せている．スマートフォンが市場に出た当初は，便利そうな新デバイスをビジネスに活用できないかという，スマートフォンをシーズとした，適用箇所を模索している状態であった．それが，先行してビジネス利用を始めた企業の事例等を参考に，具体的な利用シーンを想定したビジネスモデルが描かれるようになってきた．

しかし，スマートフォンを業務に利用することを考える場合，セキュリティ上の対策を合わ

せて考えなければならない．業務に利用するということは，取り扱う情報の中には，当然，機密情報が多く含まれると考えられるからである．これが，業務利用にあたってのハードルとなる．

業務に利用することを想定した場合のセキュリティ上の対策として，次章以降において，次の視点で考察する．

- スマートフォンの機能
- アプリケーションの実装
- スマートフォンを取り巻く脅威

3. スマートフォンの機能面での考察

本章では，スマートフォンが有する機能面でのセキュリティ対策について考察する．

3.1 端末管理

スマートフォンはPC同様の機能を有しているが，これは業務利用においては，脅威ともなり得る．モバイルPCにおいては，企業のセキュリティポリシーに適合するように，一部の機能を無効化したり制限を加えることが多い．スマートフォンにおいても同様のことを実現する方法として，Mobile Device Management（以下，MDMという）がある．しかし，OSに依存する部分が非常に大きく，現状のAndroidでは十分な統制をかけることができないのが実状である．

iOSでは，構成プロファイルを使用することで，細かい設定に至るまで統制をかけることが可能である．これに対してAndroid 2.xでは，端末利用時のパスワードポリシー，画面ロックまでの時間の設定と，リモートからの端末ロックとデータ抹消しかできない．

MDMサービス事業者やMDM製品において若干の機能追加はあるものの，業務利用を想定した場合の端末管理としては，不十分であり，根本的にはAndroidのバージョンアップによる改善を待つしかない状況である．

3.2 データ管理

スマートフォンには，本体メモリと，SDカードメモリなどの外部メモリが装備されている．このことは，通常のPCのハードディスクと同様に，紛失時の情報漏えい対策が必要であることを表している．通常のPCの場合，特に持ち出し用のPCの場合は，ハードディスクの暗号化によって情報漏えいを防止する場合が多い．これに対しスマートフォンの場合は，メモリ上でのデータ保持の方法は，ほとんどの場合が平文での保存となっているのが実情である．そのため，スマートフォンの利用にあたっては，極力，スマートフォン側にデータを保持しないことが望ましいと考えられる．

また，スマートフォンは，通常のPCに比べ本体メモリ容量が小さいことと，常時ネットワーク接続が可能な特性から，クラウド上にデータを持つことが多い．実際，マーケット上では，クラウドサービスを含めたアプリケーションが多くみられ，かつ，その形態のアプリケーションが，よく利用されている傾向にある．このことは，スマートフォンを中継して，企業，組織外への業務データの保存が可能であることを示しており，場合によっては，データ保存場所に関するポリシーに抵触する可能性がある．また，クラウドサービスを利用する場合，信頼のお

けるクラウドサービスであるかどうかの見極めが必要となる．

クラウド上にあるデータに対する脅威として，クラウドサービスへの不正アクセスがある．スマートフォンそのもののセキュリティ対策ではないが，クラウドサービスの認証強度や，サービス事業者の運用管理が，十分に企業，組織のポリシーや基準を満たしているものを選択する必要がある．

3.3　テザリング機能

最近販売されているスマートフォンの多くが，テザリング機能を有している[*2]．テザリングは，スマートフォンをアクセスポイントとし，無線 LAN 機能を有するあらゆる端末からの，インターネットへの接続を中継する機能である．一部の機種には，無線 LAN 接続の代わりに USB 接続をサポートするものもある．

多くの企業，組織において，従業者による任意の無線 LAN アクセスポイントの設置は，認められていないため，スマートフォンのテザリング機能は，脅威となる．インターネットへのアクセスは，企業，組織の定めるプロキシサーバやファイアウォールを経由することで，業務上不要なサイトや，セキュリティ上の脅威となるサイトへのアクセスを抑制しており，従業者が任意に設置したアクセスポイントを使用した場合，この統制が効かなくなるからである．

また，スマートフォンと端末間の無線 LAN 接続方式として，任意の認証と暗号化が選択できるため，仮に脆弱な認証や暗号化が選択されていた場合，盗聴の脅威にもさらされることとなる．

テザリング機能は，配布時における設定で無効化が可能であるが，Android の場合は，MDM による統制ができないため，永続的に無効化することができず，利用者が有効化してしまう可能性がある．

4.　アプリケーションの実装面での考察

本章では，アプリケーションの実装面でのセキュリティ対策を，Web アプリケーションとネイティブアプリケーションについて，それぞれ考察する．

4.1　Web アプリケーション

スマートフォンには，PC のブラウザと同等な機能が搭載されており，Cookie の使用や，Javascript の使用が可能である．基本的には，スマートフォンに対する Web アプリケーション（以下，Web アプリという）の提供方法やセキュリティ対策は，PC に対するものと同じと考えて良いが，次に示す点に注意する必要がある．

- デザインの変更

  PC に比べてディスプレイが小さいため，PC 用に最適化された Web ページでは，視認性，操作性ともに低下する．そのため，ディスプレイサイズに合わせたデザインの変更が必要である．また，タッチパネルであるため，マウスのクリックに相当するタップ時に，ディスプレイ上に表示されているものが，指で隠れてしまうことを想定したデザインをする必要がある．そのため，使いやすさを向上させるためには，スマートフォン用に最適化した Web ページを用意する必要がある．

- コンテンツタイプの変更

  スマートフォンのOSの種類やバージョンによっては，使用できないコンテンツタイプがあるため，そのようなコンテンツを使用せざるを得ない場合は，OSの種類，バージョンを識別した上で適切なコンテンツを送信する必要がある．ほとんどのスマートフォンに搭載されているブラウザは，HTML5に対応していることから，スマートフォンの機種依存を避けるためには，HTML5を使用したコンテンツを用意することが有効である．

ディスプレイサイズからくるデザイン上の制約から，従来型携帯向けのコンテンツを流用することも多いと考えられるが，その場合は，次に示す点に注意する必要がある．

- URLパラメータの隠ぺい

  従来型携帯向けコンテンツでは，Cookieが使用できない機種があるなどのブラウザの制約のため，URLパラメータによるデータの受け渡しが行われている．これは，携帯電話キャリアから公開されている従来型携帯で使用されるIPアドレスを基にアクセス制御を行い，通常のPCや検索エンジンからのアクセスを拒否した上で許容されている方法である．スマートフォンの場合は，重要な情報をURLパラメータで受け渡しすることは，情報漏えいやセッションハイジャックなどにつながる可能性があるため，使用を控えるべきである．そのため，従来型携帯向けコンテンツを流用する場合は，URLパラメータとして受け渡しを行っている部分を，Cookieやformパラメータとして受け渡すように変更する必要がある．

- 従来型携帯固有インターフェースの除去

  従来型携帯向けコンテンツでは，操作性向上のため，数字キーによるインターフェースが組み込まれているものがある．これらは，従来型携帯固有のインターフェースであるため，スマートフォン向けコンテンツに流用する場合，これらを除去する必要がある．

- かんたんログインの見直し

  従来型携帯での，認証時の利用者ID，パスワード入力は，利用者にとって手間がかかるので，2回目以降の入力を省力するため，かんたんログインと言われる機能を実装していることがある．その際に，携帯電話の契約者固有IDを使用していることがあり，サーバ側での取り扱い方によっては，非常にリスクが高い状態となっている場合がある．認証・認可された状態を継続する場合は，サーバ側で発行したセッション管理情報を使用すべきであるとともに，その有効期間についても，Webアプリの特性に合わせて，適切に設定すべきである．

4.2　ネイティブアプリケーション

スマートフォンの特徴であるネイティブアプリケーション（以下，アプリという）は，OSごとに用意された開発キットを使用することにより作成することができる．アプリは，開発キットに準備されたGUIや，開発者が作成したGUIを使用することで，Webアプリケーションに比べ，操作性やデザインを向上させることができる．また，作り方によっては，ネットワークに接続していない状態でも，操作を継続させることが可能であり，スマートフォン内にデータを保存することでデータの永続化が可能である．そのため，Webアプリケーションでは実

現することが難しいものを，アプリによって実現することができる．

作成されたアプリは，オンライン上のストアやマーケットを通じてスマートフォン利用者に配布可能であり，非常に多くのアプリがストアやマーケット上に公開されている．無償あるいは有償であっても比較的低価格のものが多いため，スマートフォン利用者の多くは，ストアやマーケットを通じて他者の作成したアプリを導入している．

アプリを作成する場合，次の点に注意する必要がある．

- データの保存方法

  スマートフォン内にデータを保存することでデータの永続化が可能である反面，スマートフォンの紛失，盗難時に，それらのデータが窃取される可能性がある．そのため，重要なデータをスマートフォン内に保存する必要がある場合は，暗号化すべきである．スマートフォン内に保存する必要がない場合は，サーバ側にデータを預ける方法を取るべきである．

- 認証

  アプリがスマートフォン内にデータを保存する場合や，サーバ側にデータを保存する場合は，アプリ利用時に認証を行うようにすべきである．サーバ側にデータを保存する場合，サーバでも認証するべきであり，その認証情報は，アプリ側で暗号化するなど，安全に保管しなければならない．

- 適切な利用許可情報設定

  Android の場合，スマートフォンのネットワーク通信や，カメラ，ストレージなどのハードウェア機能，アドレス帳などを利用するアプリは，導入時に利用者の許可を必要とする．これは，アプリ開発者が設定した AndroidManifest.xml に基づき，利用許可を求めるものであるため，必要十分な設定にする必要がある．利用許可を得ていない資源の利用はできないばかりではなく，不必要な資源に対して利用許可を求めることは，利用者にアプリの安全性に対して疑念を抱かせることになりかねないためである．

5. スマートフォンを取り巻く脅威に関する考察

本章では，スマートフォンを取り巻く脅威として，マルウェアについて考察する．

5.1 マルウェア

いったん勢いをつけて広まりをみせようとした，スマートフォンの業務利用に対する機運に水を差すことになったのが，スマートフォン上で活動する種々のマルウェアの出現である．従来型携帯は，携帯メーカごとに独自の OS を搭載していたこともあり，マルウェアの攻撃対象とされることは，ほとんどなかった．それに対しスマートフォンは，iOS，Android に代表される数種類の OS が世界レベルで使用されており，マルウェアにとっては絶好の攻撃対象となってしまっている．現在までのところ，スマートフォンを攻撃対象とするマルウェアは，大きく分類すると次の三つのタイプに分けられる．

1） ウイルスタイプ

OS の脆弱性を攻撃し，スマートフォン内部の情報を窃取したり，カメラ，GPS などのハードウェア機能を操作する．マーケット上でアプリとして配布される．

2）コンテンツタイプ

特定のコンテンツの表示・実行用アプリの脆弱性を攻撃し，スマートフォン内部の情報を窃取したり，カメラ，GPS などのハードウェア機能を操作する．攻撃用コンテンツは，メールや Web サイトからのダウンロードファイルとして配布される．

3）スパイウェア

アプリとして動作し，利用者がアプリ上に入力した情報や，スマートフォン上で取得可能な情報を，利用者の承諾を得ずに特定のサイトに送信する．マーケット上でアプリとして配布される．

1），2)については，Android 上で実際の攻撃が確認されており，3)については，Android，iOS のいずれでも確認されている．1)については，ウイルス対策アプリの導入が有効な対策であり，2)については，脆弱性のあるアプリのアップデートが有効な対策だが，3)については，有効な対策が取りにくい．Android においては，導入時に求められるネットワーク通信などの利用許可が，アプリの動作上必要なものかを判断し，不必要と思われる利用許可が求められるものについては，導入を控えることで，ある程度の対策になると考えられる．

いずれの場合も，完全に防御できるものではないことは，PC のウイルス対策と同様に考えておくことが肝要である．

6.　スマートフォンの業務利用における提言

ここまでのところで，スマートフォンを業務利用する上での，機能上の留意点，実装上の留意点，スマートフォンを取り巻く脅威について述べてきた．現実のところ，これらの制約をすべて満たしたうえで，スマートフォンを業務利用することは不可能と思われることから，どの

表 1　段階的なスマートフォンの導入

	第一段階	第二段階	第三段階		第四段階		
利用対象者	限定的	従業者全員	従業者全員		従業者全員		
端末区分	貸与端末	貸与端末	貸与端末		貸与端末		個人端末
使用場所	社内	社内/社外	社内/社外		社内/社外		社内/社外
携帯電話回線への接続許可	許可	許可	許可		許可		
マルウェア対策	要	要	要		要		要
MDM	不要	要	要		要		要
認証ポリシー	不要	要	要		要		要
リモートロック/ワイプ	不要	要	要		要		要
イントラネットへの接続形態	無線 LAN	VPN	VPN	無線 LAN	VPN	無線 LAN	VPN
社内システムの利用制限	無	有	有	無	有	無	有
社内システムのスマートフォン対応要否	不要	要	要	要	要	要	要

程度のリスクを受容できるかという視点で，表1に示す，スマートフォンの段階的な導入を提言する．

6.1　第一段階

スマートフォンの業務利用に向け，試験的に数台のスマートフォンを導入する段階であり，利用者は限定的である．イントラネット上に無線LANアクセスポイントを設置し，スマートフォンはその無線LANアクセスポイントを経由してイントラネットに接続する．社内システムを調査し，スマートフォン対応が必要なシステムの洗い出しと，対応方針を決定する．

この段階におけるリスクは，携帯電話回線を使用したインターネット接続時のマルウェア感染であるが，ウイルス対策ソフトを導入することで，低減することができる．情報漏えいについては，使用場所を社内に限定することと，セキュリティリテラシの高い従業者を利用者とすることで，そのリスクを低減させる．

6.2　第二段階

利用者として従業者全員を対象とする段階だが，イントラネットへの接続は，携帯電話回線を使用したインターネット接続経由で，イントラネット接続用VPN装置に接続する方法をとる．VPN接続時にアクセスできる社内システムを限定することで，インシデント発生時の影響を最低限に抑える．

この段階でスマートフォンの社外への持ち出しを許可するため，盗難・紛失対策が必須となり，データ保管対策，MDMの導入を行う必要がある．また，必要に応じて，社内システムのスマートフォン対応を行う．

6.3　第三段階

イントラネットへの接続として，第二段階の方法に加えて，イントラネット上に設置した無線LANアクセスポイントへの接続を許可する．この段階でスマートフォンは，イントラネット上のサーバ，PCと接続可能となることから，従業者による機密情報の持ち出しに対する対策をとる必要がある．しかし，前述したとおりAndroidの場合，MDMによる制御ではこの対応は難しいため，残存リスクとなる．

6.4　第四段階

最終段階として，個人所有のスマートフォンからイントラネットへの接続を，インターネットVPN装置に接続する方法で許可する．この段階では，個人所有のスマートフォンを，所有者の同意のもとMDMの制御下に置くことになる．

この段階においては，個人所有のスマートフォンを使用するため，導入されているアプリの制限や，MDMで制御できる設定以外は，所有者の責任において対応せざるを得ない．この部分が残存リスクとして加わることとなる．

7.　お　わ　り　に

モバイルPCが企業で使われるようになってから，幾度ものセキュリティ事故を経験し，その上で様々な対策方法が培われてきた．その経験を生かし，スマートフォンの業務利用に対し

ても十分な対策方法をとっていく必要がある．また，スマートフォン自体が急速な進化の最中にあるため，OS の機能追加や脆弱性対策のためのアップデートが随時行われているが，これも，従来の PC の OS やアプリケーションに関して行われてきたことと同じであり，情報の収集とその対応を適切に行っていく必要がある．

なお，Android については，業務利用におけるリスクの更なる低減を図るためには，デバイス管理 API の拡充が必須であり，それを有効に使った MDM システムの構築が必要と考える．現時点では，その不足分を補うために，OS のバージョンや機種，導入するアプリなども考慮に入れた上で，利用形態を決めるべきと考える．

今後も，スマートフォンの利用形態は，ますます多様化すると考えられ，それに合わせて，スマートフォン自体も進化していくであろう．また，セキュリティ上の攻撃もさらに増えていくことが考えられることから，今後の動向を注視し，安全に利用できる環境を検討していきたい．

＊ 1　厳密には携帯音楽プレーヤの iPod touch とセットトップボックスの Apple TV にも搭載されているが，本稿の言及範囲ではない．
＊ 2　iOS（iPhone）のテザリング機能は，日本では端末出荷時に通信キャリアによってロックされており，使用できないようになっている．

参考文献　［1］　日本スマートフォンセキュリティフォーラム，「スマートフォンの業務利用に関するガイドライン案」，2011 年 8 月
［2］　Android developer’s guide，http://developer.android.com/guide/index.html
［3］　JVN iPedia 脆弱性対策情報データベース，JPCERT コーディネーションセンター/情報処理推進機構，http://jvndb.jvn.jp/

※上記参考文献の URL は 2011 年 11 月 15 日時点での存在を確認．

執筆者紹介　遠　藤　英　幸（Hideyuki Endo）
1987 年日本ユニシス（株）入社．オブジェクト指向言語および実行環境の開発，アウトソーシング基盤構築などを担当後．セキュリティサービス全般を担当．現在，システム統括部 Web ビジネス技術室に所属．CISSP．GIAC GSEC．情報処理技術者試験委員．