Risk Solutions Report monthly No.21
銀泉リスクソリューションズ株式会社

■経営リスク情報■ 2014.04.07

スマートデバイスの業務利用における企業のリスク対策

1. はじめに

スマートフォンやタブレット PC といったスマートデバイス（以下、単に「スマートデバイス」という）を積極的に業務に活用し、ワークスタイル変革を推進する企業が増えています。その一方で、セキュリティ面の脆弱性も度々問題となっており、企業にとってスマートデバイスのセキュリティ対策は喫緊の課題です。

スマートデバイスの脆弱性は企業の情報漏えいリスクに直結するため、どんな企業にとっても脅威です。それは、スマートデバイスの業務利用を許可していない企業も例外ではありません。むしろ、そうした管理を行っていない企業の方がより高いリスクを抱えているとすらいえます。

そこで本レポートでは、特に情報漏えいリスクに注目しながら、企業の抱えるスマートデバイスの具体的リスクを整理し、企業がとるべき対策について解説します。

図表 1

出所：一般社団法人日本コンピュータシステム販売店協会サポートサービス委員会

２．スマートデバイスをとりまく現状

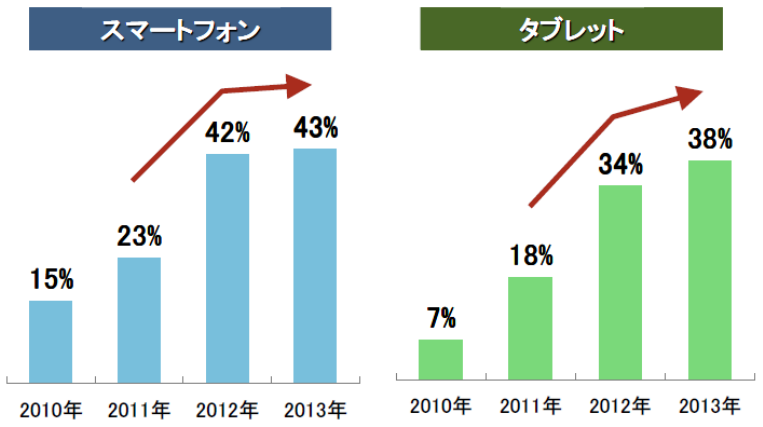
（１）業務利用状況

スマートデバイスが業務利用されるケースは、図表 2 のとおり近年増加傾向にあります。

利用目的としては、メールの送受信や web 検索による情報収集など、スマートフォンもタブレット PC もほぼ同様です（図表 3 ご参照）。特にスマートフォンでは、電話やメール等の通信手段としての利用が大部分を占めており、携帯電話の延長としての利用が目立ちます。

スマートデバイス特有の利用目的としては、「情報収集（web 検索）」、「顧客情報閲覧」、「商品案内・

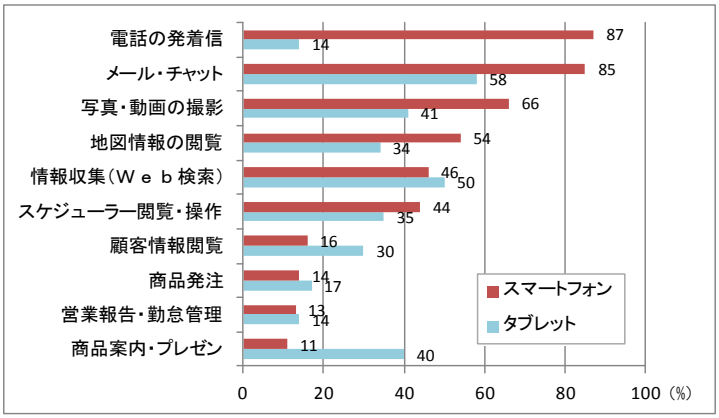
図表 2
企業におけるスマートデバイスの導入状況



出所：スマートモバイル活用委員会調査 WG
「企業におけるスマホ・タブレット利用動向と BYOD の実態」
（2013 年 11 月）
集計方法：企業のモバイル機器の導入決裁権者または決裁関与者 1,806 人を対象としたアンケート調査による

プレゼンテーション」、「ドキュメントの作成」などが挙げられます。いずれもスマートフォンよりもタブレット PC での利用が多く、携帯電話よりも大きな画面、ノートパソコンよりも優れた携帯性をもつ、スマートデバイス特有の利用目的であるといえます。

図表 3
スマートデバイスの利用目的



出所：スマートモバイル活用委員会調査 WG
「企業におけるスマホ・タブレット利用動向と BYOD の実態」
（2013 年 11 月）より当社作成
集計方法：企業のモバイル機器の導入決裁権者または決裁関与者 1,806 人を対象としたアンケート調査による（複数回答）

（２）業務利用による情報漏えいリスク

ここで、スマートデバイスからの情報漏えいの原因について整理してみます。

①スマートデバイスの紛失・盗難・不適切な廃棄

スマートデバイス自体が物理的に他人の手に渡ってしまうケースです。ノートパソコンや携帯電話といった、スマートデバイス以外の携帯端末でも発生し得ますが、スマートデバイスの場合、ノートパソコンよりも携帯性に優れている、携帯電話よりも多くの情報を保存できる、という理由から、端末が他人の手に渡った際の被害は拡大しやすいということがいえます。

②不正アプリの利用

一般アプリになりすました不正アプリを利用することで、端末を遠隔操作されたり情報流出を引き起こされたりするケースです。2012 年に発見された「the Movie」※1 が有名です。

OS 別にみると、iOS であれば、App Store が全アプリを審査しているため、JailBreak※2 を行わない限り不正アプリによる被害は発生しないといわれています。ただし、JailBreak が行われなくても入力情報が傍受される可能性があるとの報道もあり、絶対に安全とはいえません。

もう 1 つの代表的 OS である Android では、アプリの提供ストアが多数あり審査基準がストアによって異なっているため、不正アプリによる被害が発生する可能性は iOS に比べ高いといえます。

※1　人気ゲームなどのタイトルに「the Movie」などと付加した名前の不正アプリにより、1180 万件の個人情報が流出する事件が発生した（2012 年 10 月 30 日、日本経済新聞電子版）
http://www.nikkei.com/article/DGXNASDG3002Q_Q2A031C1CC1000/

※2　開発者が設定した制限を取り除き、開発者が意図しない方法でソフトウェアを動作できるようにすること

③不正なアクセスポイントへの接続

不正なアクセスポイントを通じてインターネットに接続してしまうケースです。スマートデバイスでは、携帯電話事業者の回線だけでなく、無線 LAN により様々なアクセスポイントに接続できます。そのため、不正なアクセスポイントに接続してしまい、端末内に保存された個人情報が流出したり通信内容が傍受されたりすることがあります。実際に空港などで、不正アクセスポイントにつながったユーザーの端末から、メールやネットバンキングの情報などを盗み取られる被害が発生しています。

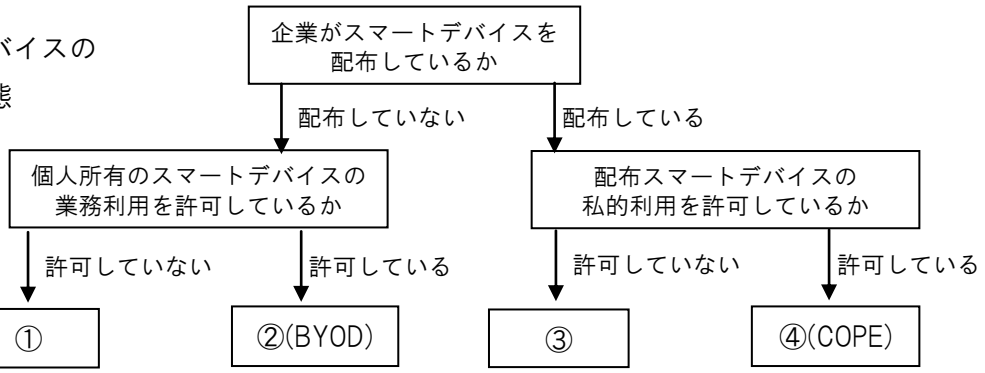
④管理外スマートデバイスによる社内ネットワークへの不正アクセス

個人所有のスマートデバイスなど、企業が管理していない端末で社内ネットワークにアクセスしてしまうケースです。そのスマートデバイスがウイルス等に感染していた場合、社内ネットワークにウイルスが拡散し、そのウィルスによって情報が漏えいする可能性があります。

３．スマートデバイスの業務利用形態と問題点

スマートデバイスの業務利用形態は様々です。整理すると図表 4 のように分類されます。ここでは、それぞれの特徴と問題点について解説します。

図表 4
スマートデバイスの
業務利用形態



出所：各種資料をもとに当社作成

（１）利用形態ごとの特徴

①個人が所有するスマートデバイスを業務利用することを許可しない形態

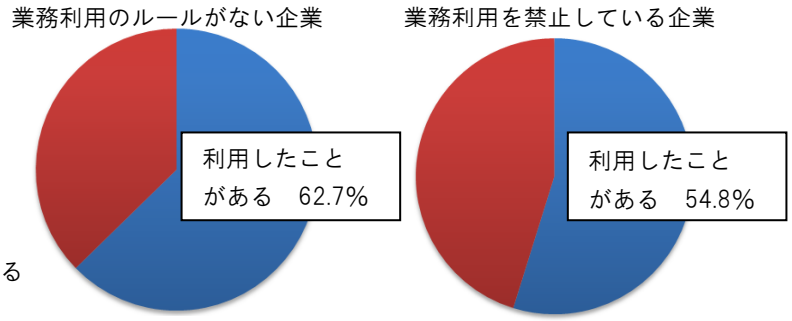
企業が許可しないにもかかわらず、従業員が個人所有するスマートデバイスを勝手に業務利用するケースがあります。この利用形態は、どんな企業でも発生し得ると考えるべきです。

また、図表 5 のとおり、業務利用を禁止している企業でも過半数の回答者が個人所有のスマートデバイスを業務利用したことがあると回答しています。

図表 5
個人所有のスマートデバイスの
業務利用状況

※ここでの「利用」は、音声通話は除きます。電子メールや業務文書の閲覧、業務システムへのアクセスなどです。

出所：株式会社トレンドマイクロの公表するデータより当社作成



集計方法：日本国内で勤務する 1548 人を対象としたアンケート調査による　（2012 年 6 月）

②個人が所有するスマートデバイスを業務利用することを許可している形態（BYOD）

従業員が個人所有するスマートデバイスを業務利用することを許可する利用形態をＢＹＯＤ（ビーワイオーディー）（Bring your own device）といいます。㈱トレンドマイクロの 2012 年の調査によると、この利用形態の企業は 38.0%※3 となっており、近年普及しつつあるといえます。従業員は使い慣れた端末を業務に利用することができ、企業は、導入コストを抑えることができるなどのメリットがあります。

※3　組織全体で認めている：18.8%、一部の従業員に認めている：19.2%
株式会社トレンドマイクロ「セキュリティマガジン　TREND PARK」
http://www.trendmicro.co.jp/jp/trendpark/mobile/byod-report-2012/20130819054651.html

③企業がスマートデバイスを配布し私的利用は許可しない形態

上記トレンドマイクロの調査では、従業員や役員にスマートデバイスを配布している企業は 30.5%※4 となっており、リスク管理の面から、その内のほとんどが、この利用形態であるとみられます。

この利用形態では、配布されたスマートデバイスの私的利用が許可されないため、私的利用したい場合、従業員は別のスマートデバイスを所有する必要があります。そして、業務利用は配布された端末のみで行い、私的利用は個人所有の端末で行うというように、利用目的によって端末を使い分けることとなります。

※4　組織全体で貸与：5.1%、一部の従業員に貸与：25.4%

④企業がスマートデバイスを配布し私的利用を許可している形態（COPE）

企業がスマートデバイスを配布し私的利用を認めるという利用形態をCOPE（コープ）（corporate owned, personally enabled）といいます。2012 年 2 月頃から海外で浸透し始めた比較的新しい利用形態であり、日本国内ではまだ浸透しているとはいえませんが、導入事例はあります※5。

私的利用されるスマートデバイスが企業の所有物であるため、企業によるセキュリティの管理が比較的容易であるといえます。また、従業員は個人用のスマートデバイスを購入する必要がなくなるというメリットがありますが、必ずしも自分の要求する端末が配布されるとは限りません。

※5　医療機器のシスメックス㈱では、2014 年 4 月から国内全社員に iPhone を配布し、私的利用を許可することが報道されている。（2014 年 2 月 22 日、日本経済新聞）

（２）利用形態ごとの問題点

①個人が所有するスマートデバイスを業務利用することを許可しない形態

この形態の場合、従業員は企業に隠れて業務に利用することが考えられます。そのため企業は、従業員のスマートデバイスの業務利用状況とそれによるリスクを全く把握することができません。実態の把握できないリスクに対しては対策を講じることもできないので、企業はそのリスクに対して無防備とならざるを得ません。従って、この形態でのスマートデバイスの業務利用による情報漏えいリスクは、②のように企業によって業務利用が許可・管理された利用形態による情報漏えいよりも、より危険性が高いといえます。

②個人が所有するスマートデバイスを業務利用することを許可している形態（BYOD）

個人所有のスマートデバイスが業務利用されるため、情報漏えいに配慮したセキュリティ対策が強く求められます。

まず、従業員によるスマートデバイスの利用状況を、企業が完全に管理することができない、という問題があります。

個人所有のスマートデバイスは、当然のことながら個人利用が優先されます。従って、従業員個人が許可されないアプリのインストールを行う可能性や、個人データと業務データを混在させる可能性、また、従業員個人によって OS の不正改造が行われる可能性すらないとはいえません。そして、そうした判断は、各従業員個人のモラルや知識に委ねられてしまいます。

次に、従業員個人の持つスマートデバイスが、必ずしも最新の OS に対応したものとは限らない、と

いう問題があります。

オンライン上の脅威は常に進化しており、OS もその脅威に対応するために常にバージョンアップがなされています。従って、従業員個人の所有するスマートデバイスが旧型であり、最新の OS に対応していない場合、新しい脅威に対応しない脆弱な OS を業務利用することとなります。

一方、厳しすぎるルールは利便性を損なう、という問題があります。インストールしてよいアプリや、OS バージョンの範囲などの制限を厳しくしすぎると、従業員が個人所有のスマートデバイスを業務利用申請しなくなる可能性があります。従業員が申請せずにスマートデバイスを業務利用する場合、企業の管理は全く及ばなくなってしまうため、企業は①と同様のリスクを抱えることとなってしまいます。

③企業がスマートデバイスを配布し私的利用は許可しない形態

安全性の高い利用形態といえます。2.（2）でみたリスクと照らしながらみていきます。「スマートデバイスの紛失・盗難・不適切な廃棄」については、多くの場合では MDM（Mobile Device Management）とよばれる端末管理ツールが適用されているため（図表 6 ご参照）、紛失・盗難等が発生した場合にも即座に情報の削除が可能です。「不正アプリの利用」と「不正なアクセスポイントへの接続」についても、それらが行われた場合、システム管理者が端末の状態を随時確認することができるため、すぐに感知し対応することが可能です。さらに、企業からの配布端末であるため、「常に企業に利用内容を把握されている」という抑止力が従業員に働き、結果的に従業員が不正な行動を控えるという効果も期待できます。「管理外スマートデバイスによる社内ネットワークへの不正アクセス」については、配布端末は管理されているため、発生する可能性は低いといえます。

以上の理由から、この利用形態は安全性が高いということができますが、一方で問題点もあります。最大の問題点はコストです。スマートデバイスを従業員に配布する場合、一般的には、端末 1 台につき、本体価格が約 5 万円、月額料金が約 6 千円程度かかります。さらに、MDM のようなセキュリティ対策費も発生します。

仮に、既に携帯電話を従業員に配布していて、既存の携帯電話と置き換えるとしても、一般的にはスマートデバイスの方が携帯電話よりも本体価格、月額料金ともに高いため、コスト増は避けられません。安全性が高いとはいえ、現実的にはこの対策を実施できる企業は限られているといえます。

図表 6　MDM（Mobile Device Management：端末管理ツール）の主な機能

機能例	解説
①紛失盗難対策	遠隔操作により端末をロック、あるいはデータを消去する
②モニタリング	ネットワーク経由で端末情報（端末状況、ログ、導入アプリケーション等）を収集する
③大規模導入支援	設定やアプリケーションの配布、更新が遠隔で自動的に行えるようにする
④アクセス コントロール	社内ネットワークへの接続・端末上のデータ・アプリケーションの利用の権限者を、一部のユーザーに限定する

出所：労政時報　第 3849 号/2013.7.12「企業における BYOD の導入、運用のポイント」をもとに当社作成

④企業がスマートデバイスを配布し私的利用を許可している形態（COPE）

情報漏えいリスクについては、どこまで従業員の私的利用を許すか、どこまで従業員の私的利用の部分を管理するか、などの点で、ルールを整備する必要があります。

また、企業がスマートデバイスを配布するため、③と同じくコストの問題もあります。ただし、私的利用を許可するため、基本料金や通信費などの一部を従業員に負担させることも可能と考えます。

利用形態自体が新しいため、今後、どのようなルール、費用負担が浸透するか、注目していく必要があります。

４．企業がとるべき対策

前章でみたとおり、企業がスマートデバイスを配布すれば安全性は高いといえますが、コスト面の問題があります。一方で、個人所有のスマートデバイスの業務利用を禁止しても、業務利用を完全に防ぐことは難しいといえます。従って、現実的にはその折衷案である、BYOD あるいは COPE を実施することが有効と考えられます（BYOD および COPE については図表 7 をご参照ください）。本章では、企業はそれらを実施する上で具体的にどのような対策を実施するべきか、以下に詳しくみていきます。

図表 7　BYOD と COPE

利用形態	端末の所有者	私的利用	業務利用
BYOD（Bring your own device）	個人（従業員）	○	許可
COPE（corporate owned, personally enabled）	企業	許可	○

出所：各種資料をもとに当社作成

（１）BYOD の場合

①ルールを整備する

BYOD を導入するためには、ルールの整備が必要なことはいうまでもありませんが、具体的にどのようなルールが必要なのでしょうか。必要な項目と解説を図表 8 に示しました。ただし、図表 8 に挙げた

図表 8　BYOD を導入するために必要なルール

項目	解説
① BYOD を許可する条件	・対象者の範囲（特定の部署・職位）を明確にします。 ・管理外の BYOD を排除するため、事前申請を必須とする必要があります。 ・スマートデバイスが旧型である可能性や、セキュリティ対策が適切になされていない可能性が考えられるため、BYOD の対象とするスマートデバイスの範囲、前もって従業員が導入すべきウイルス対策ソフト等を明示する必要があります。 ・教育・研修の定期的受講を必須とする必要があります。
② 禁止事項	・不正アプリ・アクセスポイントの利用を禁止する必要があります。 ・不正アプリについては、別途ブラックリストとして定め、随時更新し周知します。
③ スマートデバイスの管理・監視	・事故に対応するため、MDM を行う必要があります。特に盗難・紛失などの事故発生時には、情報漏えいを防ぐため遠隔操作によりデータを削除する必要があります。 ・ただし、BYOD で利用されるスマートデバイスは個人所有のものであるため、個人情報・プライバシーに配慮してどのような管理・監視を行うかを具体的に明示する必要があります。

出所：各種資料をもとに当社作成

項目はあくまでも必要な項目の一部であり、すべての項目を網羅しているわけではありません。一般社団法人コンピュータソフトウェア協会が下記ホームページで、「私有スマートデバイス取扱規程」及び「セキュリティポリシー」のサンプルを公表していますので、そちらもご参照ください。
（「BYOD」導入検討企業向け情報提供ページ　http://www.csaj.jp/activity/byod/index.html）

②誓約書を提出させる

①に記載したルールの遵守を、従業員に誓約書を提出させるという形で管理することが重要です。誓約書を提出させる理由は、主に 2 つあります。以下に解説します。

(ア)スマートデバイスの管理・監視についての同意を取り付ける

図表 8③で述べたとおり、事故発生時にはデータを削除する必要がありますが、BYOD において端末は従業員の個人所有であり、私的データも保存されています。データを削除する際にはそうした私的データも併せて削除することになる場合もあることから、その点についての同意を取り付ける必要があります。また、スマートデバイスの監視についても、従業員のプライバシーに関わるデータを取得する場合があるため、この点についても、従業員の同意を取り付ける必要があります。

誓約書の提出を業務利用開始の条件とすることで、上記のような事態が発生した際の従業員とのトラブルを回避する効果も期待できます。ただし、私用データの不要な削除や過度のプライバシー侵害があった場合には、たとえ誓約書の提出があったとしても従業員から訴訟を受ける可能性があるので、注意が必要です。

(イ)従業員のセキュリティ意識を高める

スマートデバイスは一般には携帯電話の延長ととらえられることが多く、個人使用のイメージが強いものです。しかし実態としては、スマートデバイスは「電話機能を持つ小型化したパソコン」として取り扱われるべきだといえます。このように、スマートデバイスは実態と認識に差異があり、そのことが企業のセキュリティ対策にとって大きな懸念材料となります。

BYOD の導入のためには、スマートデバイスは小型化したパソコンであり、その業務利用にはリスクが潜在しているということを、従業員に認識させなければなりません。①で述べたルールを遵守することの重要性や、ルールに抵触した場合の就業規則上の懲戒処分なども含めて、従業員にしっかりと認識させるためにも、誓約書を提出させることが必要不可欠といえます。

③教育・研修を実施する

たとえ誓約書を提出し、スマートデバイスを業務利用することのリスクを認識したとしても、従業員の知識やセキュリティ意識が必ずしも十分なものとなるわけではありませんし、スマートデバイスを使いこなせなくても個人所有スマートデバイスを業務利用したい従業員は、常に存在します。また、当初は十分な知識と意識を持っていても、常に最新の知識を得ることは難しいですし、セキュリティ意識が弛緩してしまう可能性もあります。そのため、事故事例を含む継続的な利用者教育・研修を実施し、従業員の知識やセキュリティ意識を絶えず向上させることが必要です。

（２）COPE の場合

BYOD と COPE は、同一の端末を業務にも私的にも利用するという点で共通しています。従って、基本的には COPE を導入する際も、BYOD と同様の対策が必要になります。ただし、個人所有の端末

か企業配布の端末かという違いから、BYOD には必要だが COPE には不要な対策、またその逆に、COPE に必要な対応があります。それぞれを図表 9 に示しました。

企業配布の端末であるため、図表 9①に挙げたルールは不要といえます。また、紛失・盗難等が発生した場合にはデータを削除する必要がありますが、企業が所有する端末のデータであるため、個人所有のスマートデバイスのデータを削除するよりも容易に行えるものと思われます。

一方、図表 9②に挙げたような COPE に必要な対応もあります。

COPE では通常、従業員に端末選択の余地はあまりありません。企業に配布された端末が、従業員にとって使い勝手の悪いものだった場合、従業員は別に私用の端末を購入・使用する可能性があります。従業員が個人所有の端末を業務利用すれば、それは未許可の BYOD と同様となり、企業は情報漏えいリスクを抱えることとなります。

BYOD でも、ルールを厳しくしすぎると従業員が個人所有のスマートデバイスを利用申請しないまま業務利用するリスクを生む、という問題がありますが、COPE においては、端末が企業の配布したものであるため、BYOD よりもルールは厳しくなると考えられます。さらに、従業員にとっては、使い慣れた端末ではないため、従業員が使い慣れた個人所有の端末を勝手に業務利用するリスクは潜在しているといえます。

従業員に常に最新のスマートデバイスを配布するというのは現実的ではありませんが、使い勝手の悪い端末を配布し従業員に私的利用されないのであれば、COPE を導入した意味がありません。従業員の声がシステム担当者のもとに届く仕組みづくり、また、できる限り従業員の声を反映することが必要となります。

図表 9　COPE 導入にあたっての BYOD との違い

① BYOD には必要だが、COPE には不要な対策	(ア)事前申請を必須とする。 (イ)スマートデバイスの範囲、前もって従業員が導入すべきウイルス対策ソフト等を明示する。
② COPE に必要な対応	(ア)従業員の使い勝手について配慮する。 (イ)従業員の声を吸い上げ、反映する。

出所：各種資料をもとに当社作成

５．おわりに

スマートデバイスの普及が急速に広がった現在、スマートデバイスによる情報漏えいリスクは、どんな企業にとっても対岸の火事ではありません。

スマートデバイスのリスクを正確に見極め、そのリスクを制度の中で適切に管理していくことが、どんな企業にとっても必要です。本文中で述べた BYOD や COPE を実施しても、ルールを厳しくしすぎたり従業員の声を無視したりして、結局、従業員が企業に隠れて個人の所有するスマートデバイスを勝手に業務利用したのでは、制度の意味がありません。情報漏えいリスクに配慮しつつも、一方で従業員にとっての利便性も確保する必要があります。

スマートデバイスの特性を考慮したとき、情報漏えいリスクを完全に断ち切ることは不可能と思われます。リスクを認識した上で、本文で述べたような対策をとることが必要となります。

なお、一部の保険会社では、個人情報や取引先等の企業情報が漏えいした場合に生じる法律上の損害

賠償金や訴訟費用、謝罪広告・会見費用など各種費用を補償する「情報漏えい保険」を販売しています。できる限りのリスク対策を実施し、それでも残ってしまうリスクについては、保険の活用も併せて検討することが必要です。

今回はスマートデバイスによる情報漏えいを取扱いましたが、Risk Solutions Report No.9（2013 年 4 月 19 日発行）では、「従業員のソーシャルメディア利用における企業のリスク」を解説しております。併せてご参照いただけると幸甚です。

【参考文献】

・一般社団法人日本コンピュータシステム販売店協会サポートサービス委員会 2013
「スマートデバイスに関する疑問一挙解決」（2013 年 1 月）http://www.jcssa.or.jp/img/jcssa-pdf121226.pdf

・NEC ネクサソリューションズ HP「スマートデバイス　ビジネス活用上の課題とその対策」
http://www.nec-nexs.com/sl/sol/cons_column06_15.html

・日本スマートフォンセキュリティフォーラム（JSSEC）利用部会　ガイドラインワーキンググループ
「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」（2012 年 10 月）
http://www.jssec.org/dl/guidelines2011_v1.1.pdf

・株式会社日立ソリューションズ
「JNSA の活動で得たスマートデバイスのリスク対策のポイント」（2013 年 6 月）
http://www.hitachi-solutions.co.jp/forum/tokyo/vol67/pdf/pb_seminar67_2.pdf

・総務省「インターネットトラブル事例集（Vol.3）（平成 23 年度版）http://www.soumu.go.jp/main_content/000173733.pdf

・一般社団法人日本スマートフォンセキュリティ協会技術部会ネットワーク WG「スマクラガイド」（2013 年 5 月）
http://www.jssec.org/dl/smacluguide.pdf

・スマートフォン活用セキュリティガイドライン策定 WG「スマートフォンの安全な利活用のすすめ」（2013 年 3 月）
http://www.jnsa.org/result/2012/smap_guideline_v1.0.pdf

・株式会社エス・ピー・ネットワーク　総合研究室
「情報セキュリティ編～情報漏洩における人的リスク～」（2013 年 6 月）
http://www.sp-network.co.jp/pdf/riskfocusreport_02_1306.pdf

・the guardian MOBILE ONLY　「Corporate owned,personally enabled-better than bring your own device?」
http://www.theguardian.com/media-network/media-network-blog/2013/apr/24/corporate-owned-personally-enabled-cope-byod

【本レポートに関するお問合せ先】

銀泉リスクソリューションズ株式会社　保険リスクコンサルティング第一部　帆足　祐毅

102-0074　東京都千代田区九段南 3-9-14

Tel : 03-5226-2212　　Fax : 03-5226-2884　　http://www.ginsen-risk.com/

＊本レポートは、企業のリスクマネジメントに役立てていただくことを目的としたものであり、事案そのものに対する批評その他を意図しているものではありません。