<NewsRelease>
報道関係各位

NO MORE 情報漏えい
情報漏えいの「自分ごと化」プロジェクト。

MOTEX
2014年12月2日
エムオーテックス株式会社

～NO MORE 情報漏えい プロジェクト～
30代男女のビジネスパーソン600名に聞いた
「業務用スマートデバイスの利用実態調査」
スマートデバイスを介した情報漏えい“スマ漏れ”に要注意!!
情報漏えいのリスクとなり得る「紛失」を10人に1人が経験！

エムオーテックス株式会社（本社：大阪市淀川区、代表取締役社長：河之口達也、以下MOTEX）は、社会的問題である「情報漏えい」の解決、防止に貢献していく**“NO MORE 情報漏えいプロジェクト”**を10月に発足。プロジェクト第二弾として、今回、スマートデバイスを会社から支給されている全国30代男女のビジネスパーソン600名を対象に「業務用スマートデバイスの利用実態」を調査いたしました。

調査結果については、**“NO MORE 情報漏えいプロジェクト”**の監修者である**徳丸浩氏**（HASHコンサルティング株式会社代表）より解説をいただいております。

以下が調査結果となります。本調査結果を是非ご活用いただけますと幸いです。

＝　調査結果ダイジェスト　＝

- **業務用スマートデバイスの1日の利用時間は平均約3時間。**
  個人用の携帯電話より、1日あたりの接触時間が約2時間長い状況。
- **業務とは無関係のアプリをインストールした経験がある・・・40.5%**
  建設業・情報通信業の２人に１人が経験あり。
- **情報漏えいリスクとなる「紛失」を10人に1人が経験。“スマ漏れ”に要注意！**
- **会社から業務用スマートデバイスの管理をされていると思う・・・72.3%**
- **管理の告知により、不正利用防止につながると思う・・・58.3%**

＝　調査概要　＝

■調査方法	：インターネット調査
■調査機関	：楽天リサーチ株式会社
■調査期間	：2014年9月22日（月）～24日（水）
■対象者	：会社からスマートデバイス（スマートフォン・タブレット）を支給されている男女のビジネスパーソン（600名）
■調査対象地域	：全国
■調査対象者年代	：30代

業務用スマートデバイス利用状況について

■業務用スマートデバイスの1日の利用時間は平均約3時間。
個人用の携帯電話より、1日あたりの接触時間が約2時間長い状況。

Q： 業務用スマートデバイスと個人用の
スマートデバイス・携帯電話を合わせた
一日の利用時間はどのくらいですか？
（n=400）

Q： 業務用スマートデバイスは、
一日何時間くらい使っていますか？
（n=400）

平均 3.8時間

その差 1.1時間

平均 2.7時間

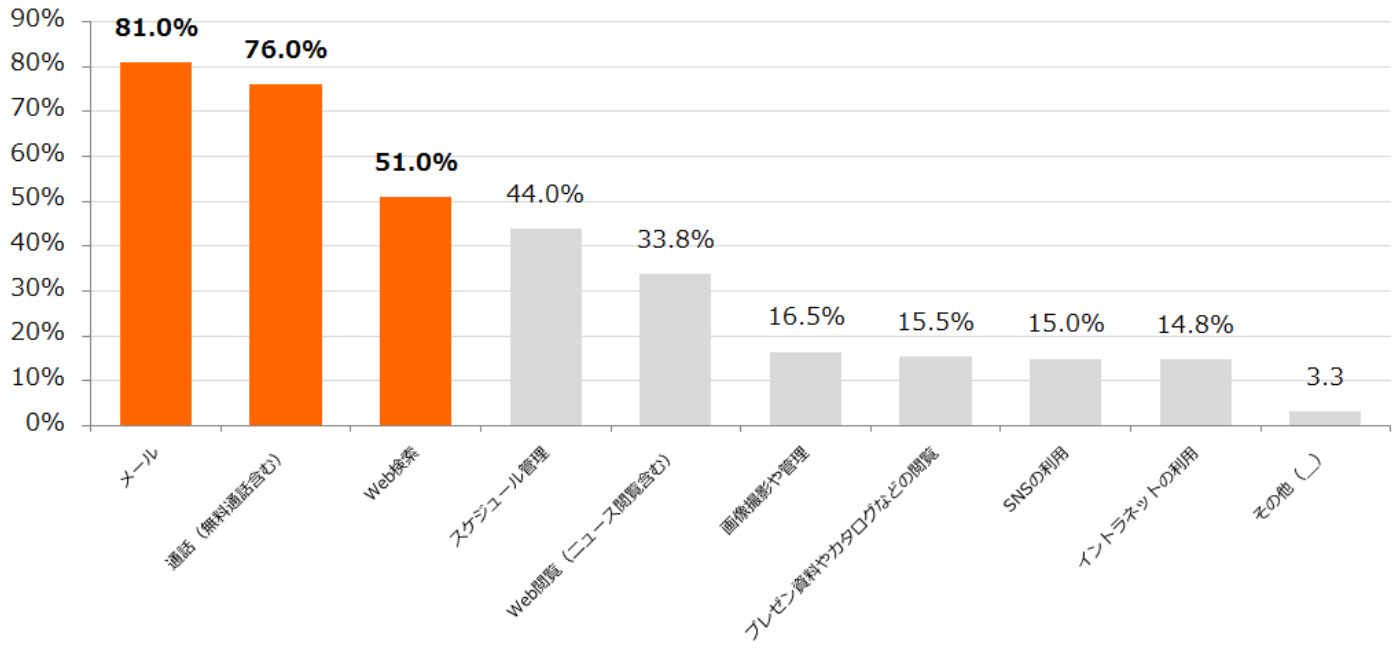
**個人用のスマートデバイス・
携帯電話の一日の平均利用時間**

その差 1.6時間

業務用スマートデバイスの1日の利用時間は平均2.7時間、個人用のスマートデバイス・携帯電話の利用時間は平均1.1時間という結果に。**業務用スマートデバイスの方が個人用より1日あたりの接触時間が1.6時間と約2時間長いことが分かりました**。

■業務用スマートデバイスの使用用途ランキング、
第1位：メール、第2位：通話、第3位：Web検索。

Q: 業務用スマートデバイスは、どのようなことに使っていますか？　（5MA n=400）

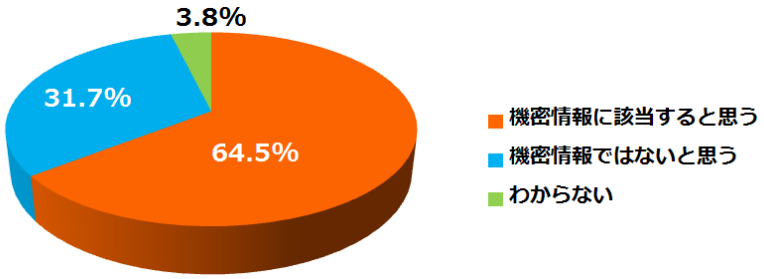


業務用スマートデバイスの使用用途を伺ったところ、メールが81.0%となり第1位、次いで、通話（無料通話を含む）（76.0%）、Web検索（51.0%）という結果に。

業務用スマートデバイス利用状況と情報漏えいリスクについて

■スマートデバイス内の業務情報が機密情報に該当すると思う・・・64.5%

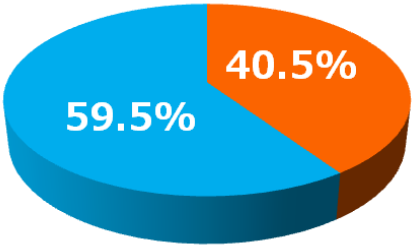
Q： スマートデバイス内の業務情報は機密情報に該当すると思いますか？
（SA n=業務用スマートデバイスに業務に関する情報が入っていると回答した290人）



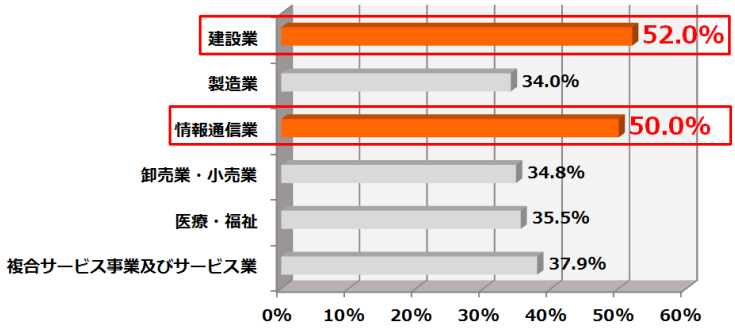
■業務とは無関係のアプリをインストールした経験がある・・・40.5%

建設業・情報通信業の2人に1人※1が経験あり。 ※1：n=25以上の業種

Q： 業務用スマートデバイスに、業務とは関係のないアプリをインストールしたことはありますか？（SA n=400）

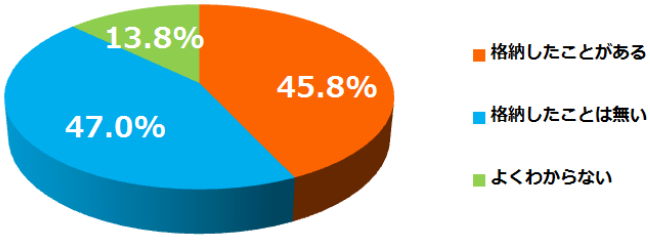


業種別では「建設業」と「情報通信業」に所属するビジネスパーソンの2人に1人が業務とは無関係のアプリをインストールした経験があると回答。
（n=25以上の業種）



■クラウドサービスに業務上の情報を格納した経験がある・・・45.8%

Q： 業務上の情報を、クラウドサービス（Evernote、DropBox、BOXなど）に格納したことはありますか？
（SA n=400）



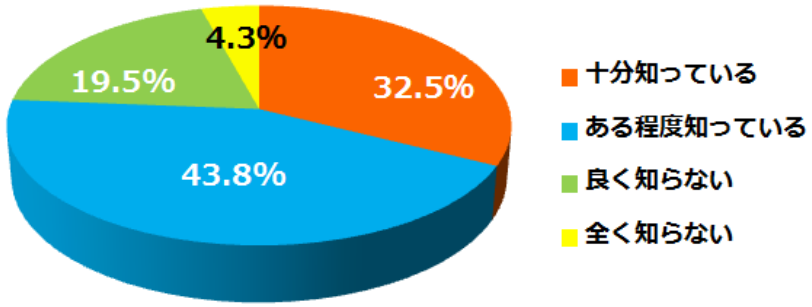
業務用スマートデバイス内に機密情報に該当すると思われる情報が入っていると6割以上（64.5%）のビジネスパーソンが回答。また、業務とは関係のないアプリを端末にインストールした経験があると4割以上が回答。業種別に見ると、建設業、情報通信業に所属するビジネスパーソンの2人に1人がインストール経験があることが分かりました。さらに、約半数近いビジネスパーソンが業務上の情報をクラウドサービスに格納したことがあると回答しました。

【徳丸先生コメント】
会社支給のスマートデバイスに業務外のアプリをインストールすることは、多くの場合就業規則などに違反する行為と考えられます。また、「便利なアプリ」の中にはスパイウェアという情報を漏えいさせるウイルスである可能性があることや、クラウドサービスからパスワードリスト攻撃などによる情報漏えいのリスクがあります。

業務用スマートデバイスを介した情報漏えいに対する意識とその実態について

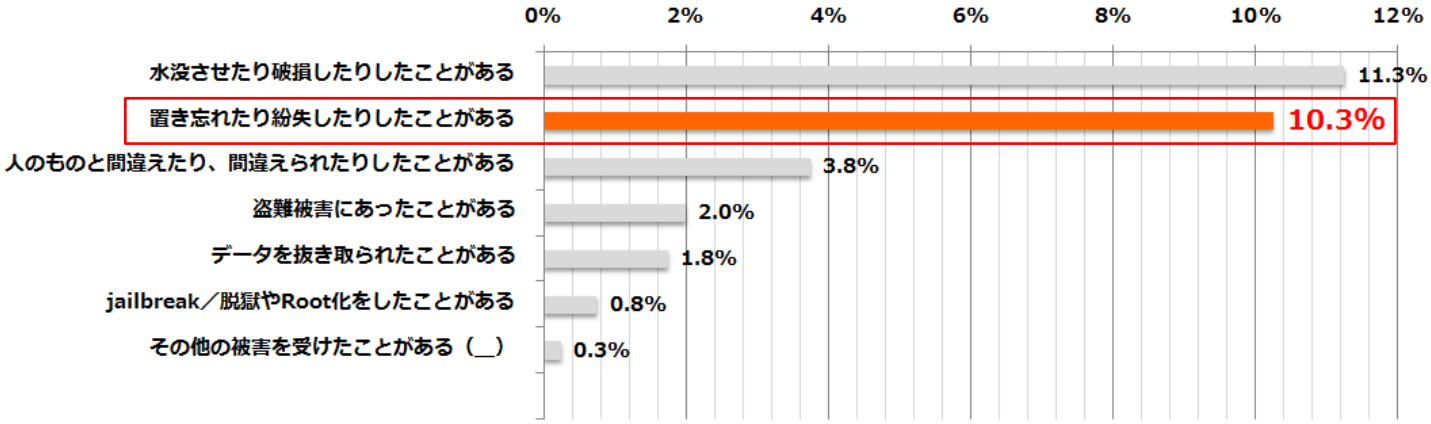
■スマートデバイスを介した情報漏えいが発生してしまうことを8割近くのビジネスパーソンが認識している。

Q： スマートデバイスを介し、情報漏えいが発生してしまうことをご存知でしたか？
（SA n=400）



■情報漏えいリスクとなる「紛失」を10人に1人が経験。“スマ漏れ”に要注意！

Q： 業務用スマートデバイスについて、以下の経験はありますか？
（MA n=以下項目のいずれかの経験があると回答した120人）



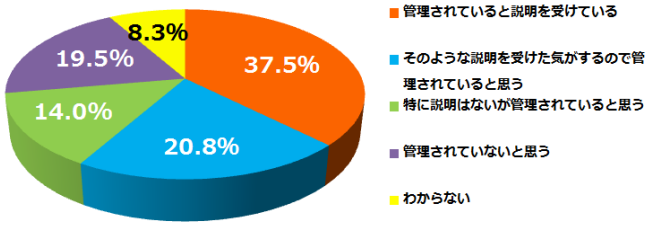
スマートデバイスを介した情報漏えいが発生してしまうことを知っていたか聞いてみたところ、「十分知っている（32.5%）」、「ある程度知っている（43.8%）」を合わせると、76.3%となり8割近くのビジネスパーソンが認識している結果に。スマートデバイスを介した情報漏えいの認識率が高い一方、そのリスクとして挙げられる代表的な**「紛失」の経験があると10.3%が回答、10人に1人が経験していることがわかりました。**“スマ漏れ（スマートデバイスを介した情報漏えい）”の恐れがあるリスクについては普段から意識して、注意する必要がありそうです。

【徳丸先生コメント】
会社支給のスマートデバイスにはメールや業務アプリなどに大量の機密情報があることから、紛失による情報漏えいの可能性は常にあります。10%ものビジネスマンがスマートデバイスの紛失経験があるというのは意外に多いと感じました。やはり、紛失を現実的な脅威として、事前に対策を講じておくことが重要ですね。

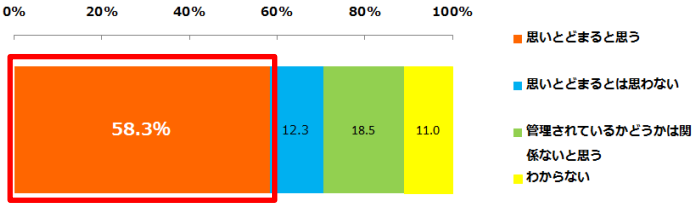
業務用スマートデバイスの管理状況について

■会社から業務用スマートデバイスの管理をされていると思う・・・72.3%
管理の告知により、不正利用防止につながると思う・・・58.3%

Q：業務用のスマートデバイスは、会社から何かしらの管理（不正利用や、閲覧制御など）をされていますか。
（SA n=400）



Q：業務用スマートデバイスが会社によって管理されていることをあらかじめ知らされていたら、業務用スマートデバイスの誤操作や不正利用を思いとどまると思いますか。
（SA n=400）



業務用スマートデバイスの運用にあたり、会社から不正利用や閲覧制限といった管理をされているか調査。「管理されていると説明を受けている（37.5%）」、「そのような説明を受けた気がするので管理されていると思う（20.8%）」、「特に説明はないが管理されていると思う（14.0%）」となり、7割以上のビジネスパーソンは会社から管理されていることを認識。また、管理されていることを運用前に説明を受けることで不正利用を思いとどまると思う。と58.3%が回答。業務用スマートデバイスの安全な運用や情報漏えいを未然に防ぐためにも、社員への管理についての説明は重要だと考えられます。

＝　徳丸先生の調査総括　＝

企業におけるスマートデバイス活用が急速に進んでいることを感じるとともに、スマートデバイスの管理については課題が多いなと感じました。おそらく、管理側は厳し目の統制を目指しているがその徹底度が非常に不十分なザル状態というのが現状と思われます。発想を変えて、ここから先は絶対に譲れないという緩めのラインを引いて、その緩めのラインは徹底するという方法が良いと考えます。ストレージサービスなども一律に禁止するのではなく、会社で使うストレージサービスを決めてプリインストールした上で、利用法も指導していくような形がよいのではないでしょうか。

徳丸 浩（とくまる・ひろし）
HASHコンサルティング株式会社代表
エムオーテックス株式会社技術顧問
独立行政法人情報処理推進機構(IPA)非常勤研究員

1985年京セラ株式会社入社後、ソフトウェアの開発、企画に従事。
1999年に携帯電話向け認証課金基盤の方式設計を担当したことをきっかけにWebアプリケーションのセキュリティに興味を持つ。2004年に同分野を事業化し、2008年独立。脆弱性診断やコンサルティング業務のかたわら、ブログや勉強会などを通じてセキュリティの啓蒙活動を行っている。

NO MORE 情報漏えいプロジェクト 特設サイト

プロジェクト発足に合わせて特設サイトをオープン。本サイトでは、「情報漏えい」に対する知識を深め自分ごと化していただくためにケーススタディやコラムを公開。そのほか、一般公開アンケートによる意識調査レポートの発表や「情報漏えい」のリスクを分かりやすく覚えることのできる、妖怪キャラクターを用いた“情報漏えい 百鬼夜行”という診断コンテンツを展開していきます。

サイト名　　：NO MORE 情報漏えいプロジェクトサイト
サイト公開日　：2014年10月27日（月）
サイトURL　　：http://www.motex.co.jp/nomore/
Facebook　　：www.facebook.com/motex.nomore

～プロジェクト第一弾～セキュリティツール 日本初の無償提供 LanScope An Free 11月27日リリース！

NO MORE 情報漏えいプロジェクトの活動、第一弾として、スマートフォン・タブレットの資産管理・行動管理・セキュリティ対策を実現するスマートデバイス管理ツール “LanScope An（ランスコープ アン）”を、紛失・盗難対策機能に限定して無償提供することを決定。スマートデバイス紛失・盗難対策ツールとしては日本国内初となる“LanScope An Free（ランスコープ アン フリー）”を2014年11月27日より提供しています。

製品名　　：盗難・紛失対策ツール『LanScope An Free』
機　能　　：リモートロック、ワイプ、パスワードポリシー
その他　　：製品版LanScope Anへのアップグレード可
提供開始　　：2014年11月27日
サイトURL　　：http://www.lanscope.jp/an/free/

エムオーテックスについて

ネットワークセキュリティ、IT資産管理ソフトウェアLanScopeシリーズを展開するソフトウェア開発会社です。代表的なソフトウェア“LanScope Cat”は、1996年の発売以来、時代のニーズに応じて進化しつづけ、その結果を多くの企業の信頼を集め、2014年10月時点、7,500社が導入、国内シェアならびに顧客満足度※2において国内No.1の実績を誇ります。ソフトウェア開発・販売のみならず、LanScope活用事例コンテスト「LanScope AWARD」や全国各地を巡るセミナー「革新者サミット」など、利用価値を高める情報提供活動にも積極的に取り組んでいます。

※2：日経BP社「日経コンピュータ 顧客満足度調査 2014-2015」

【会社概要】

社名　　：エムオーテックス株式会社
代表取締役社長　　：河之口 達也
設立　　：1996年
資本金　　：2,000万円
本社所在地　　：大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル