スマートフォンを セキュアに 使うために

ビジネスで

2012年版

モバイルソリューションを推進する
MCPC

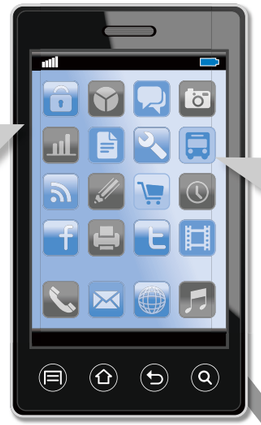
モバイルコンピューティング推進コンソーシアム（MCPC）
技術委員会アプリケーションワーキンググループ

クラウド+スマートフォンはこんなに便利♪♫

モバイルソリューションを推進する MCPC

端末の機能

- 電話および電話帳機能
- 大画面タッチスクリーン
- フルブラウザ搭載
- カメラ、テレビ、ボイスレコーダ
- 音声入力 ・電子マネー（おサイフケータイ）
- GPS端末機能
- 加速度センサや方位センサ etc.



既存のケータイ向けサービス

- 位置検索
- ショートメッセージ、デコメール、Eメール、データバックアップ、着メロ・着うた
- 無線LANスポット、etc.

ソーシャルネットワーク

- Facebook、twitter、mixi、Ustream、etc.
- ブログサイト
- ソーシャルゲーム
- 写真共有、動画共有サイト

1 様々な機能を追加できる

アプリのインストール、コンテンツのダウンロード&アップロード

- 電子書籍や音楽コンテンツ
- オンラインストレージ
- EvernoteやDropbox（マルチデバイスでのマルチドキュメントの活用）
- 地図／ナビ
- ゲーム
- スケジュール

2 位置情報を活用した新たなアプリ

インターネットのWebへアクセス

- PC向けサイトの閲覧
- キーワード検索
- オンライン決済
- ニュース配信 etc.

クラウドサービス

オフィス内の人や情報につながる

プライベートクラウド

自社の情報システム
業務データ

3 どこでも使えるいつでもつながる

情報共有すぐにアクション

社内でも社外でも

企業向けITサービス

- ASPやSaaS
- コンピューティングサービス
- ストレージサービス
- システム運用・監視

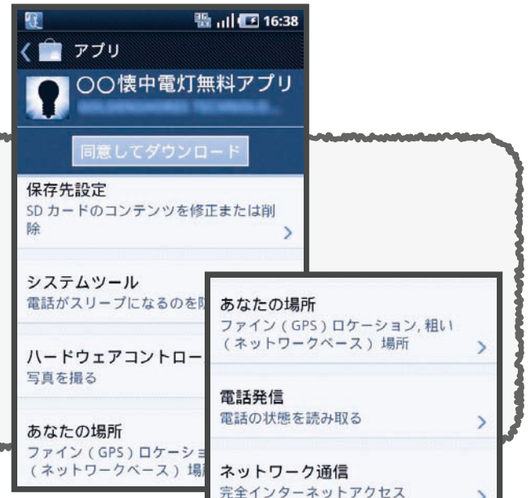
セキュリティの落とし穴、まずはここにご注意！

モバイルソリューションを推進する MCPC

1 不正アプリ・偽装アプリの蔓延

怪しいアプリのインストールに要注意！

- ユーザーの個人情報や機密、マーケティング情報の収集を目的とした偽装アプリが多く見られます。アプリケーションソフトですから、ダウンロード先／インストール先となるスマートフォンの中で勝手に動き回ります。
- 特に、インストール時や更新時にアクセス許可（パーミッション）に不用意に同意してしまうと、情報の収集・発信・流出やデータ破壊を許すことにつながります。



例えば…
液晶画面をまっ白にして、明るく照らすだけの「懐中電灯アプリ」が人気ですが、パーミッションとしてカメラ機能や位置情報やアドレス帳の利用許可、ネット接続や電話発信等の許可を求めてくるものがあります。懐中電灯になぜ…？ 明らかに怪しいですね。

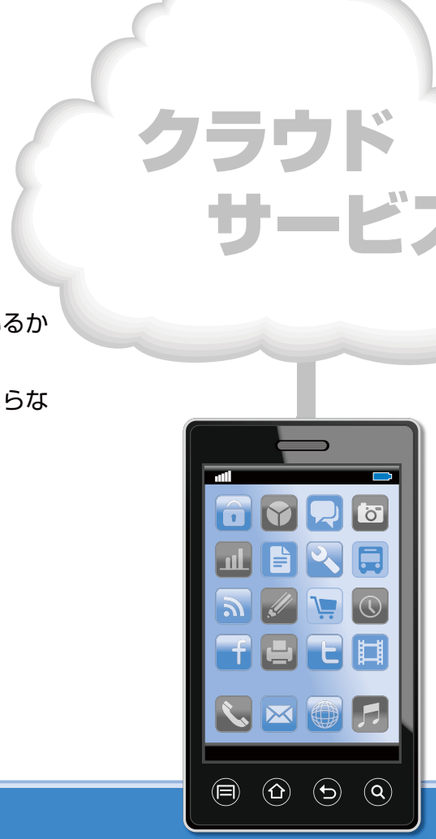
2 位置情報の盗用

位置情報アプリの活用にご注意！

- 写真を撮ると、写真に位置情報が埋め込まれます。
- 自分の居場所が（リアルタイムで）第三者に知られているかもしれません。
- 写真や位置情報が他の情報と結びつくことで、思いもよらない意味を持ってしまうこともあります。

例えば…
敏腕営業マンの方、Facebookやmixiのチェックイン、あるいは撮影写真の位置情報から、得意先や商談相手の住所がアナタの足跡と共に大公開されているかも…。

例えば…
GPS 機能を ON にしたまま twitter で「つまんねー」「早く帰りたいのに…」と何気なくつぶやいたら、その下に貴方の会社の本社住所と会議中の時刻が表示されてしまい…。



3 端末の紛失・盗難

クラウドや会社直結の“入口”が誰かの手に渡ってしまう！

- 機密情報・顧客情報・個人情報の漏えい
- 社内システムへの不正侵入
- 第三者による有償サービスやコンテンツの購入、おサイフケータイの盗用、なりすましによる悪戯等々

例えば…
サービスにアクセスするときのパスワードをスマートフォンに覚えさせていませんか？
画面ロックしてない状態で誰かに拾われたら、高価な買い物も思いのまま？

これだけはやっておきましょう！

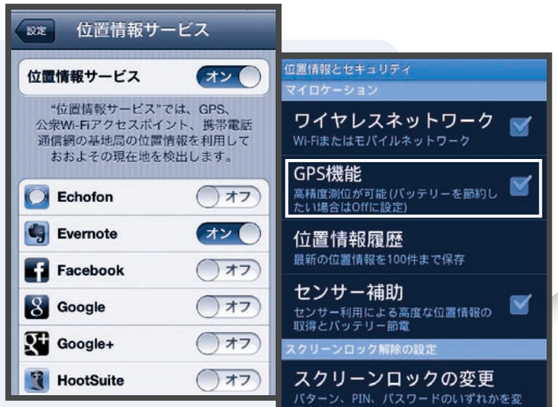
モバイルソリューションを推進する MCPC

1 不正アプリ・偽装アプリへの備え

- アプリのダウンロードは、信頼できるサイトから！（但し、正規マーケットに潜り込んでいる偽装アプリもあります。）
- 「提供元不明のアプリ」がダウンロードされないよう、スマートフォンを設定しておく。
- 不自然に多数のアクセス許可（パーミッション）を求めるアプリはインストールしない。

2 位置情報を使うときの注意

- GPS や Wi-Fi/ モバイルネットワーク等による測位機能の ON/OFF 設定を確認し、必要なときや必要なアプリにだけ使う習慣に。
- SNS にチェックインするとき、書き込むとき、写真をアップするときは、自分の居場所が公開されることを念頭に。



3 端末の紛失盗難対策

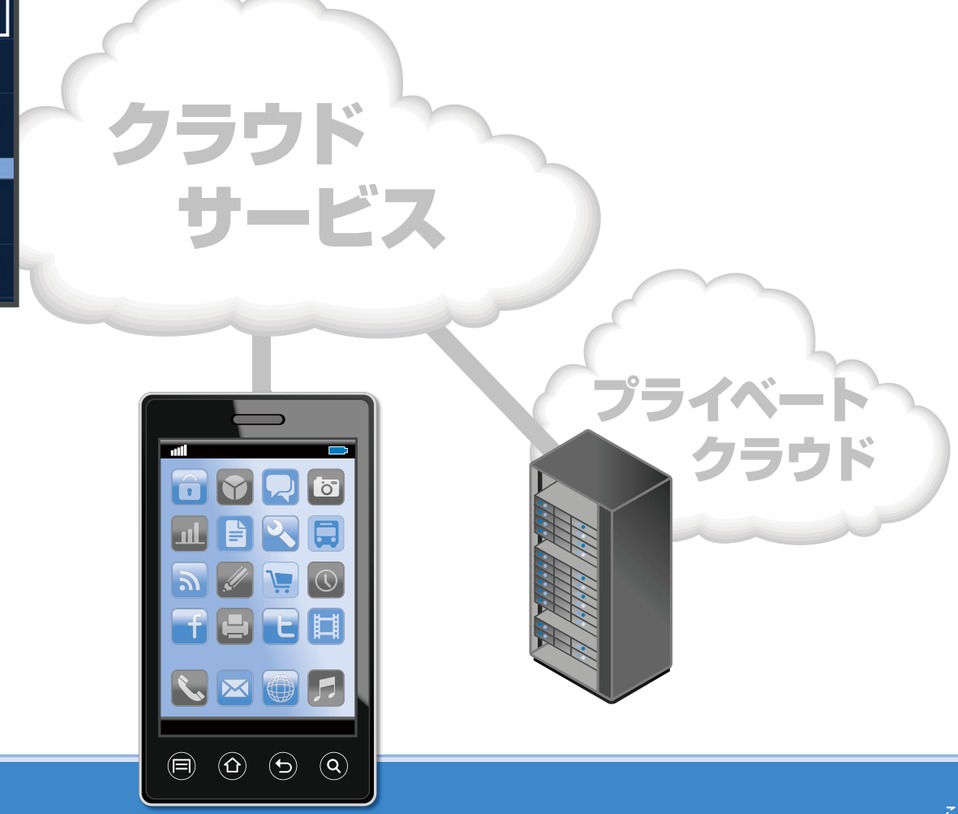
- スマートフォンを買ったら、電話会社やサービス事業者の「遠隔ロック」や「遠隔データ消去（リモートワイプ）」サービスの利用を申し込む。
- 普段持ち歩くときは、端末ロックか画面ロックを忘れずに！
- 紛失・盗難にあったら、すぐに遠隔ロックやリモートワイプを実行し、続いて電話会社に連絡して、通話停止措置の手続きを！（事後対策）

企業としての備えも

- スマートフォンのビジネスユースでは、パソコンと同様の 情報セキュリティ対策が求められます。SNS や SaaS に登録された情報が、企業やユーザー には見えない形で関連づけられていることもあります。
- 企業として重要なことは、自社のセキュリティポリシー に基づいて、スマートフォンの運用規則を明確に定め、適切な運用の徹底を図ることでしょう。MDM（モバイル デバイスマネジメント）の活用も視野に入れましょう。
- スマートフォンを業務に使う際の留意点を、チェックシートにまとめておくとよいでしょう。その一例を下記に掲載してありますので、参考にしてください。

http://www.mcpc-jp.org/smartphone/build.htm

「スマートフォンを安全に使うための企業のチェックリスト例」



モバイルソリューションを推進する
MCPC

【まとめ】

今やスマートフォンは、大方の人々にとって必要不可欠なビジネスツールになりつつあります。次々に登場するクラウドサービスやモバイルサービスによって活用シーンがどんどん広がり、普及に拍車をかけています。

スマートフォンは、大画面タッチスクリーンのユーザーインタフェースや多様なアプリのインストールなどパソコンに匹敵する便利さを備え、かつ、いつでもどこでもインターネット環境に接続できることを特徴としており、場所を選ばずに情報発信・情報共有・情報伝達を実現できます。

スマートフォンを使いこなすことで、ワークスタイルは大きく変わる可能性を持っています。メールやスケジュール、連絡先リスト等をいつでも利用できるほか、社内システムや SaaS にアクセスして稟議決裁や受発注処理など、あらゆる業務をスマートフォンひとつで行うことができます。さらに、Facebook や Evernote といったオープンサービスの活用により、リアルタイムの情報共有と、これまでにない仕事の進め方が可能になります。

一方、企業サイドからは、「スマートフォンの活用は慎重に進めたい」という思いが強く感じられます。その背景には、セキュリティ面に対する漠然とした不安が働いています。

スマートフォンのセキュリティリスクについては昨今、多方面で議論され、また利用者にも伝えられています。しかし議論の中身を冷静に見ていくと、実際にはごく稀にしか発生しない事象であったり、PC や携帯電話でも同様に存在し既にコントロールできているリスクなど、適切な予防措置や使用時の注意で回避できるものがほとんどだと言えます。

大切なのは「使い方」です。リスクに対する過敏さよりも、適切な注意を払う賢さこそが肝要です。的を射た必要かつ十分なセキュリティ対策を講じ、新しい技術とサービスを“スマート”に使いこなしていきましょう。

2012年版

スマートフォンをビジネスでセキュアに使うために

発　行　元　モバイルコンピューティング推進コンソーシアム（MCPC）
発　行　日　2012 年 4 月 20 日
制作／編集　MCPC 技術委員会アプリケーションワーキンググループ

〈検討・制作メンバー〉
主査：後藤義徳（NTT ドコモ）、副主査：塩田岳彦（パイオニア）
安達智雄（NEC）、今城忠浩（ベーステクノロジー）、竹下 清（ソフトバンクモバイル）、
寺西賢二郎（ベーステクノロジー）、平山幸一（トレンドマイクロ）、松本昭彦（リックテレコム）、
米倉和則（KDDI）、事務局：横尾俊夫（MCPC）

問 合 せ 先　MCPC 事務局
〒105-0011 東京都港区芝公園 3-5-12 長谷川グルーンビル 2 階
TEL：03-5401-1935　FAX：03-5401-1937
E-mail：office@mcpc-jp.org　URL：http://www.mcpc-jp.org/

非売品