

「作業所におけるスマートフォンなど フィールド情報機器活用について」パートⅡ

～情報セキュリティについて～

（社）日本建設業連合会 IT推進部会 セキュリティ専門部会

目 次

1) スマートデバイスのセキュリティについて

- 1-1) スマートデバイスの特徴
- 1-2) セキュリティリスク
- 1-3) セキュリティ対策
- 1-4) 利用にあたっての注意点

2) その他 活動報告

- 2-1) クラウドについて
- 2-2) 現場用ポスター作成
- 2-3) ガイドラインの改定

スマートデバイス



1-1) スマートデバイスの特徴

普及の理由

パソコンと同じ機能であり、携帯性で優位

個人利用(SNS等の普及と同期)から普及

OSの種類

i-os: Apple社の集中管理(端末・OS・アプリ配信等)

★セキュリティリスクが低い

Andoroid: オープンソース、自由度が高い

★セキュリティリスクが高い(i-osに比べて)

BlackBerry、WindowsPhone、、

スマートデバイス



1-2) セキュリティリスク

「一般的には」

不正アプリ、不正webサイトアクセス、
盗難紛失、不正侵入、スパムメール、、

「建設現場では」

盗難紛失、SIMカード抜取、
落下水没による故障、覗き見、、

上記の状況のため、スマートデバイスでは、パソコンや
電子記憶媒体と同様のセキュリティ対策が必要となります。

スマートデバイス



1-3) セキュリティ対策

(MDM: Mobile Device Management)

サービス(商品)が順次拡大

株式会社NSD 提供

要件	アンチウイルスベンダー				
					
会社	トレンドマイクロ社	シマンテック社	マカフィー社	ソフォス社	エフセキュア社
製品名	Trend Micro Mobile Security5.5 Advance版	Symantec Mobile Management	Enterprise Mobility Management	Sophos Mobile Control	F-Secure Mobile Security for Android
契約形態	年間契約	年間契約	年間契約	年間契約	年間契約
提供形態	ソフトウェア販売	ソフトウェア販売	ソフトウェア販売	ソフトウェア販売	ソフトウェア販売 + サービス提供
iOS	×	○ (v4.1 以上)	○ (v4 以上)	○ (v4 以上)	×
Android	○ (v2.1 以上)	○ (v2.2 以上)	○ (v2.2 以上)	○ (v2.2 以上)	○ (v1.6 以上)
Docomo	○	○	○	○	○
AU	△【制限あり】	△【制限あり】	△【制限あり】	△【制限あり】	△【制限あり】
Softbank	○	○	○	○	○
アンチウイルス機能	△ (個人向け)	△ (個人向け)	△ (個人向け)	×	○ (Android のみ)

サービス別比較表

(形態、対応os、対応キャリア、ウィルス、リモート制御、、)

スマートデバイス



1-3) セキュリティ対策 (各種ガイドライン)

「スマートフォン活用ガイドラインβ版」

JNSA

「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」

JSSEC

「スマートフォン・クラウドセキュリティ研究会
中間報告」

総務省

スマートデバイス



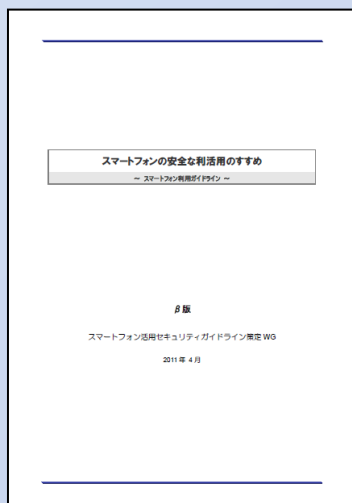
1-3) セキュリティ対策 (各種ガイドライン)

「スマートフォン活用ガイドラインβ版」

2011年4月 発行

JNSA 日本ネットワークセキュリティ協会

http://www.jnsa.org/result/2010/smap_guideline_Beta.pdf



- ・スマートフォンとはどのようなものか
- ・スマートフォンの利用におけるセキュリティ上の課題
- ・スマートフォンの安全な利用方法
- ・スマートフォン端末の管理
- ・スマートフォンの利用シーンとセキュリティの課題
- ・サポート

スマートデバイス

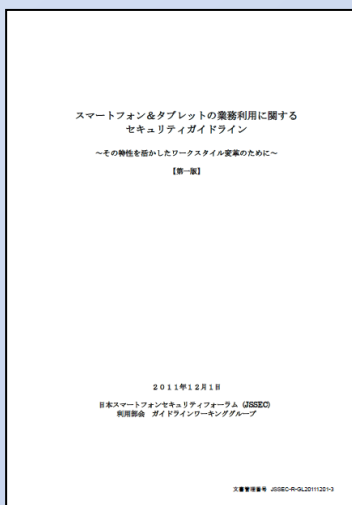


1-3) セキュリティ対策 (各種ガイドライン)

「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」 2011年12月 発行

JSSEC 日本スマートフォンセキュリティフォーラム

http://www.jssec.org/dl/guidelines2011_v1.0.pdf



- ・はじめに
- ・スマートフォンの利活用によるメリット
- ・スマートフォンのしくみと概要
- ・スマートフォンの特性と留意点
- ・利用シーンからみる脅威と対策
- ・ライフサイクルにおける留意点

スマートデバイス



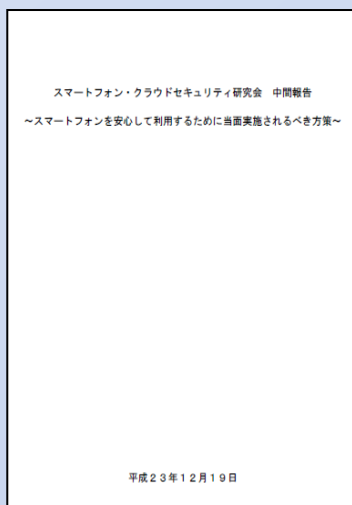
1-3) セキュリティ対策 (各種ガイドライン)

「スマートフォン・クラウドセキュリティ研究会 中間報告」

2011年12月 発行

総務省

http://www.soumu.go.jp/main_content/000139819.pdf



- ・スマートフォンを取り巻く環境
- ・スマートフォンの情報セキュリティ対策の考え方
- ・事業者において導入を検討されるべき対策
- ・一般利用者への普及啓発のあり方
- ・「スマートフォン情報セキュリティ3か条」

スマートデバイス



1-4) 利用にあたっての注意点

「組織として」

- ・利用目的を明確にする
- ・利用ルールの作成(ガイドラインを参考に)
私物の取扱、デバイス一括管理、紛失時対応、接続方法、、
- ・ユーザ教育

「利用者として」

- ・Pwd管理(複雑、変更)、Pwdロック
- ・設定変更(Jailbreak)の禁止
- ・ウィルス駆除ソフト、バックアップ、、

スマートデバイス



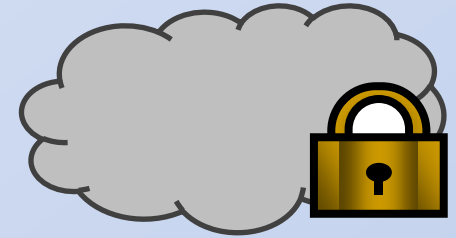
1-4) 利用にあたっての注意点

「提言」

スマートデバイスは普及期のため、
パソコンと比較すると、セキュリティ対策が脆弱です。
特に利用者の注意不足が、
「情報漏えい」につながります。

各社で利用する場合は、
「利用者ヘルールを守らせること」
を絶対条件として下さい。

その他 活動報告



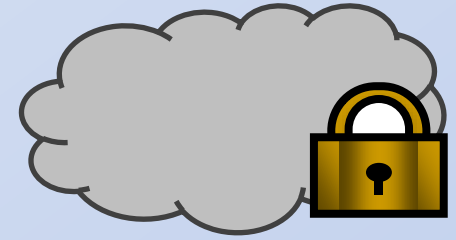
2-1) クラウドについて

- ・インターネットを利用するサービス
- ・データやツールは自社(PC/ネットワーク)に持たない
- ・様々な分野で、急速に普及

「代表的なサービス」

- ・Webメール
- ・オンラインストレージ
(図面の共有、関係者との情報共有)
- ・写真・動画共有サービス

その他 活動報告



2-1) クラウドについて

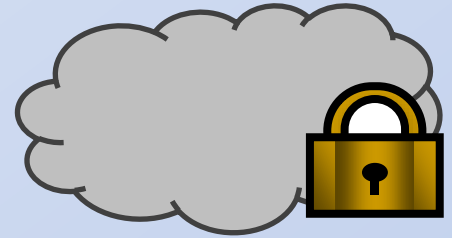
「利点」

- (組織として) ・システム構築・運用負担からの解放
- ・迅速対応(導入、資源の変動)
- (利用者として) ・特定PC以外からアクセス可能

「注意点」

- ・社内システムとの二重管理
- ・利用料金の増加の可能性
- ・データ外部保管の是非

その他 活動報告



2-1) クラウドについて

「セキュリティ対策」(各種ガイドライン)

「クラウドサービス利用のための
情報セキュリティマネジメントガイドライン」

2011年4月 発行
経済産業省

<http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html>

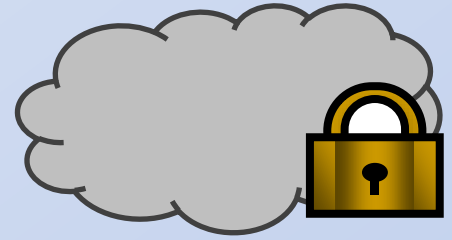
「クラウドサービス利用者の保護とコンプライアンス
確保のためのガイド」

2011年7月 発行

ASPIC ASP・SaaS・クラウドコンソーシアム

<http://www.aspicjapan.org/information/press/pdf/110712.pdf>

その他 活動報告



2-1) クラウドについて

「セキュリティ対策」(重要事項)

- ・基本は「ID／pwd」**厳重管理**
- ・利用ルールの策定
 - ・クラウド管理者の任命
 - ・クラウド管理者による利用ユーザの管理

その他 活動報告

2-2) 現場用ポスター作成

情報漏えいリスクの低減のため

(これまで)

- ・パンフレット 「情報漏えい防止徹底のお願い」
- ・教育用動画 「情報漏えい防止徹底のお願い」

(今回)

- ・現場用情報セキュリティポスター作成



パンフレット「情報漏えい防止徹底のお願い」 1/2

協会社作業員向け
情報セキュリティ教育資料

協会社のみなさんへ

～情報漏えい防止徹底のお願い～

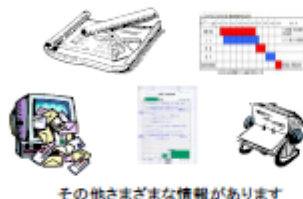
情報管理も大事な仕事の一つです

配布元会社名

近年、情報漏えいに関する事故がテレビ・新聞等で大きく報道されています。一旦、このような事故が起こると会社だけでなく、個人に対しても厳しく責任が追及されます。このような事故を未然に防ぐために、この資料に書かれているポイントをよく理解して、情報漏えい防止に努めてください。

工事に関する「情報」とは >>>

- ・ 図面、工程表、写真、打合せ記録
- ・ 発注者、近隣、工事関係者の個人情報（個人の名前が記載された書類等）
- ・ 建物の内部や設備の状況（写真等）
- ・ 会社の技術やノウハウ（標準仕様等）
- ・ みなさんの会社の管理情報



その他さまざまな情報があります

もし、あなたの過失で「情報」が漏れてしまったら…>>>

万が一「情報」が漏れいしたら、どのような事態を招くことになるのでしょうか？

- ・ 当事者、関係者は厳しく処分される可能性があります。
- ・ 会社の信用を失い、仕事や工事を失う恐れもあります。
- ・ 法律や契約等に抵触し、厳しく責任を問われます。
 - 法による制裁
 - 損害賠償など

※ 個人情報保護法、不正競争防止法、守秘義務契約など



なぜ、どうして「情報」が漏れたの…>>>

ほとんどが不注意や認識不足。まさか漏れるとは思ってなかった…。

- ・ 私物（自宅）パソコンで仕事をしていた。ちゃんと設定すればWinny（ウィニー）も大丈夫と思っていたが、ウイルスに感染してパソコンに保存された業務データや電子メールがすべて流出した。
- ・ パソコンを電車で置き忘れたら、ネットオークションで販売されてデータも流出した。
- ・ 工事情報や個人情報を保管した USB メモリを紛失した。



「情報」を守るための9つのポイント

万一情報漏えい事故を起こしてお互いに迷惑をかける前に、ここに書かれた最低限の守るべきポイントを日頃から守ってお互いの信頼関係を築いてゆきましょう。

ポイント1 工事に関する「情報」は絶対に口外しない >>>

- ・ お客様、近隣住民、工事関係者の個人情報の取扱いに注意してください。
 - 個人情報の管理は、法律でも厳しく定められています。過失による個人情報の流出でも、会社だけでなく個人も罰せられる可能性があります。
- ・ 工事に関する情報は、絶対に口外しないでください。
- ・ 次のような行為はもちろん禁止です。
 - 工事に関する情報を、インターネットのブログ（個人日記）や掲示板（2ちゃんねるなど）に書き込む。
 - 工事関係者や工事関連会社のリストを無断で持ち出す。
 - 建物内部や工事状況の写真を無断で撮る。



ポイント2 しっかりと保管しましょう >>>

- ・ 図面、書類や外部記憶媒体（USBメモリ、CD、DVDなど）は、決められた場所に保管してください。
- ・ 特に重要な情報が記録されたものは、鍵を掛けて保管してください。
 - 事務所荒らしによるパソコンの盗難が多発しています。事務所に防犯対策を施すことも大切です。



パンフレット 「情報漏えい防止徹底のお願い」 2/2

ポイント3 Winnyなどのファイル交換ソフトを入れない >>>

- ・ 業務で使用するパソコンにファイル交換ソフトを絶対インストールしないでください。
 - 代表的なファイル交換ソフトは、以下の通りです。
Winny(ウィニー)、Share(シェア)、Cabos(カボス)、LimeWire(ライムワイヤ)など



ポイント4 私物パソコンを業務に使わない >>>

- ・ 私物のパソコンを業務に使用しないでください。
 - 私物パソコンは、ウイルスやスパイウェアなどで情報流出のリスクが高いです。
- ・ 私物パソコンに業務データがある場合は直ちに削除してください。
- ・ 業務に使用するパソコンを私的に利用したり、家族と共用したりしないでください。
例: 家族が共用パソコンに Winny を導入し、ウイルスに感染したため情報が漏えいした。



ポイント5 ウイルス対策ソフトは必ずパソコンに入れましょう >>>

- ・ パソコンには、ウイルスを検知・駆除するためのウイルス対策ソフトを必ず入れてください。
(パソコンショップで、数千円程度で市販されています)
- ・ ウイルス対策ソフトは、常に最新の状態で更新してください。
- ・ マイクロソフトのセキュリティ修正プログラムは適宜適用してください。



ポイント6 パソコンには、必ずパスワードを設定しましょう >>>

- ・ 使用するパソコンには、必ずログインパスワードを設定してください。
 - パソコンや業務システムを利用する際に使う金庫の鍵のようなものです。万一の盗難や不正利用のリスクを最小限にしてくれます。
- ・ パスワードは、他人に推測されにくいものにしてください。
- ・ パスワードは他人に漏れないように管理してください。
(紙に書いて貼っておくことは厳禁です)



ポイント7 「情報」の持ち出しや持ち歩きには注意しましょう >>>

- ・ 図面、書類やパソコン、外部記憶媒体を必要以上に職場から持ち出さないでください。
- ・ パソコン、外部記憶媒体を持ち出す場合には、暗号化やパスワード設定など盗難・紛失時のリスク回避策を行ってください。
- ・ 職場の外では肌身離さないよう注意してください。電車の網棚に置いたり、車中に放置したりしてはいけません。
- ・ 持ち出し時には、目的地に直行してください。
 - プライベートな用件などの寄り道は気の緩みが生じ、事故のもととなります。



ポイント8 コピー、FAX、郵送、メールの使用は最小限にとどめ、誤配に注意しましょう >>>

- ・ 関係者に渡す「情報」は最小限にとどめてください。
- ・ 郵送、FAX、電子メールなどで「情報」を送信する際には、宛先や送付する書類に間違いがないかよく確認してください。
- ・ 重要な情報を電子メールで送信するのは控えてください。
やむを得ず送信する場合は、必ず暗号化をおこなうか、パスワードを設定してください。



ポイント9 「情報」は確実に返却・廃棄しましょう >>>

- ・ 工事が完了したら、保管の必要な情報以外は全て返却または廃棄してください。
廃棄する際は図面、書類やパソコンから情報が盗みだされることが無いよう、次の対策を実施しましょう。
 - 図面、書類はシュレッダーにかける。
 - CD、DVD 等の外部記憶媒体はハサミで裁断するなど、物理的に破壊する。
 - パソコン内の不要なデータを削除する。(ごみ箱からも必ず削除する)



もしも「情報」が漏えいしてしまったら

万が一にも、情報漏えい事故が発生した場合、また情報漏えい事故の恐れがあると判断した場合には、社員は直ちに自社の上司または担当者に報告してください。報告を受けた会社は、元請会社などの関係先に連絡してください。

情報漏えい防止対策について、この資料に書かれていることで分からないことがありましたら、当社社員にお尋ねください。

(2009.5.26 版)



BCS 情報漏えい防止徹底のお願い

「情報管理も大事な仕事の一つです」



現場用情報セキュリティポスター

■「あなたのパソコンが狙われています」ポスター

B2 (728×515) S=Free

図面・書類・PC・外部記憶媒体 徹底管理

あなたのパソコンが狙われています!

Cybercrime



ワイヤーでPCを固定



保管時にはしっかり施錠

保管管理の徹底
事務所荒らしによるパソコンの盗難が...

図面・書類・外部記憶媒体 (USBメモリー/CD等) は決められた場所に施錠し、保管してください!

社団法人日本建設業連合会

■「情報が狙われています」ポスター

A3 (420×297) S=Free

情報が狙われています!

情報は絶対に口外せず
確実に返却・破棄しましょう
///CAUTION///

Cybercrime



社団法人日本建設業連合会

その他 活動報告

2-3) ガイドラインの改定

発行済「ガイドライン」

建設現場における
情報セキュリティガイドライン
【元請会社編】



平成22年4月

社団法人 建 業 協 会
社団法人 日本土木工業協会

- ・ JVネットワークガイドライン（2005/4発行）
（主な内容）JV現場事務所でのネットワーク構築ルール
- ・ 現場事務所セキュリティガイドライン（2008/11発行）
（主な内容）現場事務所内のセキュリティ対策
- ・ 同（元請会社編）（協力会社編）（2010/6発行）
（主な内容）情報漏えい防止の対策

その他 活動報告

2-3) ガイドラインの改定



(改定の経緯)

- ・現状のICT環境(＊)と既存ガイドラインとのギャップ解消
(＊ 無線LAN、スマートフォン、クラウド、、)

(今後の予定)

- ・今年度:会員会社へのアンケート、骨子の検討
- ・来年度:ガイドライン策定作業

メンバー(会社名順)

平井 明	大成建設
豆腐谷 洋一	竹中工務店
長沼 秀明	戸田建設
高馬 洋一	間組
山口 正志	フジタ
藤野 芳徳	前田建設工業
長谷 芳春	三井住友建設

(社) 日本建設業連合会 IT推進部会 セキュリティ専門部会