

## 情報セキュリティ教育資料

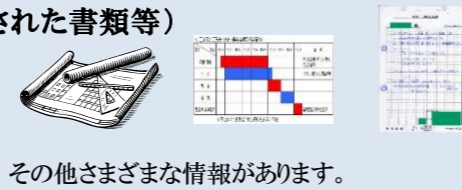
協力会社の社員及び作業員のみなさんへ  
～ 情報漏えい事故防止の徹底のお願い～  
★スマートデバイスの紛失や SNSの投稿による  
情報漏えい対策のポイントをまとめています。



解説)スマートデバイスは、スマートフォン、タブレット等を対象としています。  
解説)SNSとは、ツイッターやLINE、Facebook等を対象としています。

### ○「工事情報」とは

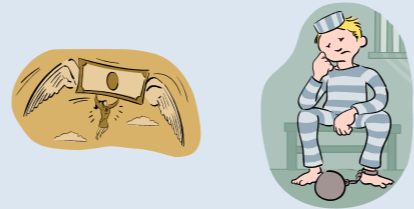
- 図面、工程表、写真、打合せ記録
- 発注者、近隣、工事関係者の個人情報(個人の名前が記載された書類等)
- 建物の内部や設備の状況(写真等)
- 会社の技術やノウハウ(標準仕様等)
- みなさんの会社の管理情報



### ○もし、あなたの過失で「工事情報」が漏れてしまったら

万が一「工事情報」が漏れいたら、どのような事態を招くことになるでしょうか？

- 当事者、関係者は厳しく処分される可能性があります。
- 会社が信用を失い、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



### ●スマートデバイス利用に関する【5のポイント】

対象者)建設現場に入場する協力会社の社員及び作業員  
対象物)建設現場に持ち込む社有、私有を問わないスマートデバイス

- ①スマートデバイスは、許可なく業務に使わない。
- ②工事情報をSNSに投稿しない。
- ③工事情報を業務の完了後、速やかに削除する。
- ④盗難・紛失・情報漏えいの対策をする。
- ⑤工事情報が漏れいした場合、速やかに報告する。

#### ①スマートデバイスは、許可なく業務に使わない。

- スマートデバイスを、電話として利用することは問題ない。
- スマートデバイスにおいて、電話以外の機能(カメラ機能、メール機能、インターネット閲覧機能等)を業務で利用する場合は、作業所長の許可を得ること。



#### ②工事情報をSNSに投稿しない。

- SNSの投稿により、情報が不特定多数に公開されますので、建物の内容(写真を含め)や作業所周辺の写真など工事に関連しない情報でも、それらをSNSに投稿することは、発注者に不利益となったり、発注者が不快に感じたりする可能性があります。
- 発注者に不利益となる投稿を行った場合、建設業全体の信頼を失うことにもなりかねません。また、発注者が個人の場合、プライバシー侵害の問題となりますので、注意してください。



- 例1) ある発注者から依頼を受けた新棟建設の工事中、旧棟の会議室が見えたので、作業員がその会議の状況をSNSに書き込んだ。  
旅館の増築工事中、「この旅館は土曜日なのに客がいらない」と掲示板に書き込んだ。
- 例2) 著名人の自宅のリフォームを請け負った会社の作業員が現場の状況を家族に話した。  
その家族は「〇〇さんの家の台所はこんなだったそうだよ。」とSNSに書き込んだ。

#### ③工事情報を業務の完了後、速やかに削除する。

- スマートデバイスにおいて、電話以外の機能(カメラ機能、メール機能、インターネット閲覧機能等)を業務で利用したことによって、スマートデバイス内に保存された工事情報は、情報漏えいしないように業務の完了後、速やかに削除する。

#### ④盗難・紛失・情報漏えいの対策をする。

- 盗難・紛失対策として、パスコード/パスワードやローカルロックを設定し、常に肌身離さず持ち歩き、置き忘れのないように注意する。
- インターネット接続時の情報漏えい対策として、必要に応じて、セキュリティ対策ソフトを導入する。
- 機器の改造等はしない。



#### ⑤工事情報が漏れいした場合、速やかに報告する。

- 万が一、盗難・紛失やウイルス感染等によって、情報漏えい事故の恐れがあると感じた場合は、速やかに作業所長や元請会社の社員に報告する。

(2016.03 版)

- 参考  
総務省の国民のための情報セキュリティサイト  
日建連の建設現場における情報セキュリティガイドライン(第2版)【元請会社編/協力会社編】  
独立行政法人 情報処理推進機構の中小企業の情報セキュリティ対策ガイドライン  
■ 不明な点は、会社担当者に問い合わせ下さい。