協力会社作業員向け
情報セキュリティ教育資料

協力会社のみなさんへ

～情報漏えい防止徹底のお願い～

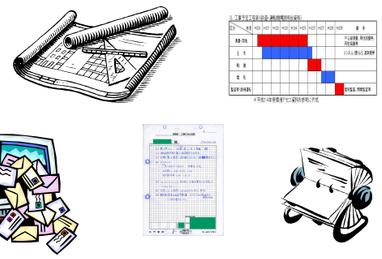
情報管理も大事な仕事の一つです

株式会社竹中土木

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）
- 当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」が漏えいしたら、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※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・・・＞＞＞

「意識不足」「放置」「誤操作」「管理ミス」といったヒューマン エラーが大半。まさか漏れるとは思ってもいなかった・・・。

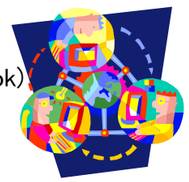
- 現場の写真を個人のブログに投稿し、重要な設備の情報が漏れてしまった。
- パソコン、スマホ等のモバイル機器を電車に置き忘れたら、ネットオークションで販売されてデータも流出した。
- 工事情報や個人情報を保管した USB メモリを紛失した。
- メール誤送信により重要なデータが流失してしまった。

「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。

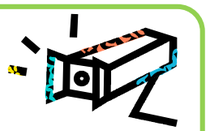
ポイント１ 工事に関する「情報」は絶対に口外しない ＞＞＞

- 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 SNS(X、Instagram、Facebook)やブログ・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メモリ等）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。



ポイント3　業務で使用するパソコンに**業務で私用しないソフト**を入れない　＞＞＞

- 業務で使用するむやみにファイル共有、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。
  - ➢ 情報漏洩するリスクが高いです。

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利用中に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、常に最新の状態に更新してください。
- 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なってください。
- 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、メール使用は最小限にとどめ**誤配に注意**　＞＞＞

- 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。
  - ➢ USB 等の外部記憶媒体は物理的に破壊する。
  - ➢ 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。

（2024.4.1 版）

参考資料

➢ 協力会社における情報セキュリティ対策について

建設現場に従事する協力会社の情報セキュリティ対策の強化を目的とした資料

https://www.nikkenren.com/publication/fl.php?fi=1387&f=security_kg_gl_202402.pdf

➢ （経営層向け）「サイバー攻撃の脅威に備えるために【改訂版】」

建設業の経営層を対象に、建設業界が直面しているサイバー攻撃の脅威とそれらへの対策について解説した動画

https://www.youtube.com/watch?v=IIhVYJ5mRSk

➢ （経営層向け）二重脅迫型ランサムウェアの予防と対処

二重脅迫型ランサムウェアへの最低限の予防と対処について解説した動画

https://www.youtube.com/watch?v=7biysala__o

➢ （職長・作業員向け）建設業界の「情報セキュリティ」5 大脅威

情報セキュリティに関する 5 大脅威に関して解説した動画

1. パソコン等の情報機器紛失・盗難
2. ブログ等 SNS への投稿による現場写真の漏えい
3. 図面等重要書類の紛失・盗難による情報漏えいと事故報告遅延
4. メール誤送信による図面データ等の漏えい
5. 標的型攻撃メールによるコンピュータウィルス（ランサムウエア）感染

https://www.youtube.com/watch?v=S7ga49EL2RI （日本語）

（日本語）

（英語）

上記動画について視聴できない場合、下記 URL を参照願います

【日本建設業連合会　教育・研修用動画】

https://www.nikkenren.com/kenchiku/ict/security/movie.html#a1