

建設業界の情報セキュリティ 5大脅威 <2017年>

2017年に建設業界で影響の大きかったセキュリティ上の脅威を、日建連「情報セキュリティ専門部会」で実際に発生した事故をベースに選出し、順位付けした。

事故の原因は、本人の認識不足やルール違反と共に会社側の教育・指導不足があげられる。ひとたび事故が発生すると、施主の信用失墜や損害賠償などに繋がり、経営上の大きなリスクとなる。

順位	脅威	事例と解説
1	パソコン等の情報機器紛失・盗難	業務終了後、急遽酒席となり思わず泥酔してしまった。気が付くとパソコンが入った鞆ごと紛失していた。原則パソコンは持ち出さない。酒席となった場合は摂取量を控えるなど工夫ができるよう指導する。
2	ブログ等SNSへの投稿による現場写真の漏えい	現場作業員が現場の写真を個人のブログに投稿し、施主側が投稿に気づいた。スマホ世代(若者)に投稿傾向がみられる。新規入場者教育など業務の初期段階でしっかり意識付けすることが有効。
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	図面紛失後、施主へ事故報告がなされないうちに、警察から施主に遺失物届連絡が入り、事故が発覚した。社員または協力会社への教育・指導力不足を疑われるので事故発生時の対応については繰返し確認することが必要。
4	メール誤送信による図面データ等の漏えい	メールの誤送信には宛先アドレスの間違いと添付ファイルの間違いの2パターンがある。いずれもメールを送る前に宛先アドレス、添付ファイルの中身をしっかり再確認することで回避可能。
5	標的型攻撃メールによるコンピュータウイルス(ランサムウェア*1)感染	パソコンまたはサーバ上のファイルが暗号化され読取不可となり業務が停止。バックアップが無いと大きな手戻りが発生する。不審なメールの添付ファイルもしくはメール内のリンクは絶対にクリックしないよう指導すると共に疑似的攻撃メールを使った訓練も有効。

*1 ランサムウェア パソコンやサーバ内にあるファイルを暗号化し閲覧できない状態にしたりするウイルス。元の状態に戻すために仮想通貨などを支払うように求めてくる。日本をはじめ世界的に被害が広がっている。