

情報セキュリティ教育資料 (協会社様向け)

更新: 2024年7月
株式会社橋本組 総務部IT支援室

1. 最近建設業で発生した情報セキュリティ事件事例
 - ① 宅配業者になりすました、偽のショートメッセージ
 - ② SNS投稿
 - ③ 重要書類(図面等)の紛失
 - ④ パソコン盗難
 - ⑤ ランサムウェア感染
2. 日ごろのセキュリティ対策
3. 自社の情報セキュリティ教育に活用できる資料
4. 自社のサイバーセキュリティ対策に困ったら

1. 最近建設業で発生した情報セキュリティ事故事例

① 宅配業者になりすました偽のショートメッセージ

宅配業者になりすましたショートメッセージ(SMS)をスマホに送り、ログイン情報を盗み取ったり、不審なアプリをインストールさせる攻撃が流行しています。

・ 実例

宅配業者から不在連絡のSMSが届いた。宅急便が届く予定は無かったが、本文に記載されたURLをクリックしてみると、スマホのログイン画面が表示されたので、IDとパスワードを入力したところ、スマホのIDを乗っ取られ、電話帳や写真などのデータが漏洩した。

・ このような事故を発生させないために

身に覚えの無いメッセージは偽物の可能性を疑い、本文に記載されたURLはクリックしないようにしてください。

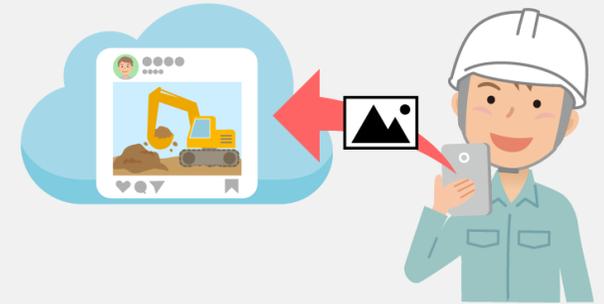
※**大手宅配業者は、不在連絡にSMSを使用していません。**



現場の情報を、SNS(X(旧Twitter)、Instagram、TikTokなど)に投稿する事故が発生しています。

・実例

- ① 運送業者ドライバーが、現場写真を撮影しSNSに投稿。偶然SNSを見た関係者からの情報で発覚した。
- ② 現場で働く作業員が、現場名が推測できる内容を文字のみで投稿。発注者のインターネット監視で発覚した。



・このような事故を発生させないために

業務情報(文字、写真、動画)は絶対に投稿しないでください。たとえ**文字****だけ**であっても、軽い気持ちで行った投稿から発注者に損害を与える大問題に発展するリスクがあります。協力会社にも周知してください。

③ 図面など重要書類の紛失



図面など重要書類の紛失事故が発生しています。

・実例

- ①現場から退出時に、資機材や道具、図面等を社用車に積み込む際、図面を挟んだバインダーを歩道に仮置きしたまま積み忘れ、紛失した。その後、図面を拾得した人に図面を見られてしまった。
- ②コンビニで図面をコピーした後、原稿を置き忘れ、次にコピー機を利用した人に図面を見られてしまった。

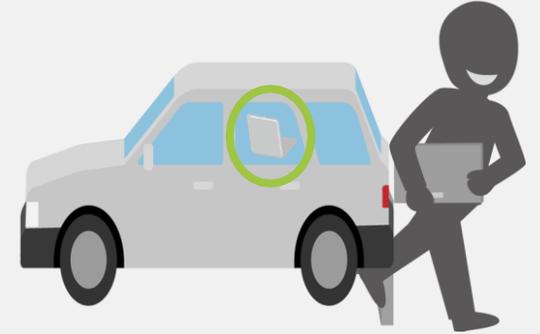
・図面は重要書類

図面等の工事情報は発注者から「機密情報」に指定されているケースが多く、漏洩すると取り返しのつかない事態に発展することがあります。

・このような事故を発生させないために

図面は鞆に入れて持ち運び、置き忘れが起こりやすい歩道や車上、電車の網棚には置かないようにしてください。コピーは会社でおこなってください。

車に放置していたパソコンの盗難被害が発生しています。



・実例

- ① 自宅駐車場に社有車を駐車して帰宅したところ、車上荒らしに遭い、車内に置いていたパソコン入りの鞆を盗まれた。
- ② 自宅駐車場に社有車を駐車して帰宅したところ、車ごと盗まれ、車内に置いていたパソコンと外付けハードディスクも盗まれた。

・被害に遭うと

パソコンに保存していた業務情報が漏洩するリスクがあります。

・被害に遭わないために

たとえ自宅駐車場であっても、パソコンや書類などを車に放置せず、自宅に持ち帰ってください。 ※**電子的な手口による、施錠した車の盗難も流行中**

テレワークなどに利用するVPN機器の脆弱性を利用してランサムウェア（身代金ウイルス）へ感染させる攻撃が流行しています。

・ランサムウェアに感染すると

パソコンやサーバ上のデータが暗号化され利用できなくなり、盗んだデータをインターネットに公開されて脅迫されるケースが増えています。

・実際の事件事例

サーバのデータファイルが突然開けなくなり、身代金要求メッセージが確認された。しかし、バックアップから復旧できたので、それ以上対応しなかった。



後日、ダークウェブ上のサイバー犯罪者のサイトに、サーバに保存していた業務情報が公開されていることが分かった。発注者の重要な図面が含まれていたため、建物所有者やテナントへの報告等に追われた。



・原因

VPN機器のファームウェアアップデートを実施していなかったため、脆弱性（セキュリティ不備）を突いて攻撃をされた。

※機器の管理を委託しているITベンダーが実施を怠ったケースもあります

・データ暗号化や身代金要求されたときは

パソコンやサーバ上の多くの業務情報が漏洩している可能性があります。たとえ復旧できても安心せずに、速やかに警察やセキュリティ専門会社へ相談して、被害を最小限に食い止める行動をしてください。また、発注者へ速報してください。

・被害に遭わないために

VPNのメーカーからファームウェアアップデートが公開されたら速やかにアップデートしてください。ITベンダーに管理を委託している場合は、対応状況を確認してください。



2. 日ごろのセキュリティ対策

- ・メールの添付ファイルやURLを安易にクリックしない
- ・業務に関係のないWebサイトを閲覧しない
- ・フリーソフトを利用しない
- ・セキュリティパッチ、ウイルス対策ソフトを確実に適用する
- ・単純なパスワードを使用しない
- ・必要なファイルは、バックアップされる場所に保管する

一人ひとりが徹底すれば リスクは大幅に下がります
基本的な対策を着実に実施しましょう



3. 自社の情報セキュリティ教育に活用できる資料

● 日建連WEBサイト

情報セキュリティに関するガイドライン・教育資料集

<https://www.nikkenren.com/kenchiku/ict/security/guideline.html>



● IPA中核人材育成プログラム 建設業向け教育動画

・動画(個別版をダウンロード→1分動画が30個)

<https://contents-download.icscoe.jp/construction-cybersecurity/>



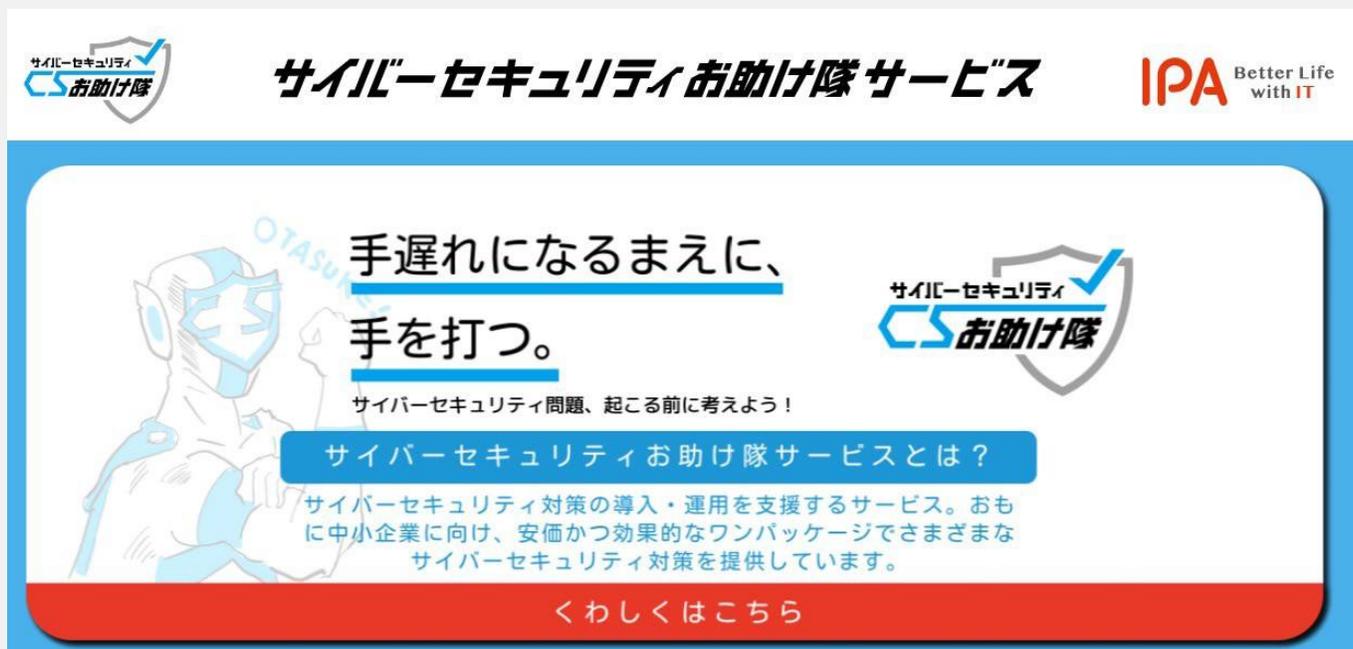
・建設業向けサイバーセキュリティ教育動画一覧リスト

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2023/t6hhco0_00000yssp4-att/t6hhco000000z6bc.pdf



4. 自社のサイバーセキュリティ対策に困ったら

サイバーセキュリティお助け隊サービス (IPA 独立行政法人 情報処理推進機構)



The banner features the 'Cyber Security Otasuketai' logo on the left, which includes a shield with a checkmark and the text 'サイバーセキュリティお助け隊'. The main text reads: '手遅れになるまえに、手を打つ。' (Before it's too late, take action.) followed by 'サイバーセキュリティ問題、起こる前に考えよう！' (Think about cyber security issues before they happen!). Below this, a blue box asks 'サイバーセキュリティお助け隊サービスとは？' (What is the Cyber Security Otasuketai Service?). The answer states: 'サイバーセキュリティ対策の導入・運用を支援するサービス。おもに中小企業に向け、安価かつ効果的なワンパッケージでさまざまなサイバーセキュリティ対策を提供しています。' (A service that supports the introduction and operation of cyber security measures. It is primarily for SMEs, providing various cyber security measures at a low cost and high effectiveness through a single package.) At the bottom, a red bar contains the text 'くわしくはこちら' (For more details, click here).

<https://www.ipa.go.jp/security/otasuketai-pr/>