

2017年 建設業界の 情報セキュリティ5大脅威

2018.2.15 建築のITセミナー
情報セキュリティ専門部会

建設業を取り巻く状況

IoT AI ビッグデータ クラウド 3D デジタル社会 Society 5.0

2020東京 働き方改革 攻めのIT銘柄

i-Construction 建設キャリアアップシステム BIM CIM

サイバー攻撃 情報漏えい 個人情報保護

サイバー月間（内閣府）

情報セキュリティガイドライン

サイバーセキュリティ経営ガイドライン

中小企業の情報セキュリティ対策ガイドライン

IoTセキュリティガイドライン

データベースセキュリティガイドライン

日建連の取組

建築生産の変革に向け、
安心してITを活用するための情報セキュリティ対策は、必須の取組です

建設業界の情報セキュリティレベル向上には
協力会社の底上げが、「重要」かつ「必須」である

経済産業省【サイバーセキュリティ経営ガイドライン(抜粋)】

自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

(解説)

○ サプライチェーンのビジネスパートナーやシステム管理等の委託先がサイバー攻撃に対して無防備であった場合、**自社から提供した重要な情報が流出**してしまうなどの問題が生じる。

○ 自社のみならず、サプライチェーンの**ビジネスパートナー**やシステム管理等の**委託先を含めたセキュリティ対策を徹底することが必要**である。

情報セキュリティ 桶の理論



工事情報＝桶の中の水

「一か所の不備(ex.協力会社)」から情報漏えい

日建連の取組

日建連：建築：建築-IT WEB

> ガイドライン・教育資料集
(協力会社向け含む)

ツール	推奨対象者			提供元 (メディア等)	タイトル
	作業員	社員	経営者		
パンフレット		○	○	日建連	情報漏えい防止徹底のお願い
パンフレット	○			日建連	情報セキュリティ5か条リーフレット
ポスター	○	○		日建連	情報セキュリティポスター「無断で摸らない! 書き込まない!」
ポスター	○	○		日建連	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	○	○		日建連	情報セキュリティポスター「あなたの情報が狙われています!」
eラーニング	○	○		日建連	情報セキュリティポイント学習 Ver.1~3
動画	○	○		日建連	作業所における情報セキュリティ講座
チェックシート	○	○		日建連	情報セキュリティチェックリスト(協力会社用)

建築 IT WEB

> IT 部会の紹介

> 建築セミナー

> 情報セキュリティ

> ガイドライン・教育資料集
(協力会社向け含む)

> 先端IT

> BIM

> 成果集

○ ガイドライン

区分	タイトル
I	建設現場における情報セキュリティガイドライン(第1版) 情報セキュリティマネジメントシステムの構築と運用手順、実施すべき事項を例示したもの
II	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】 "I"を補完するもの。セキュリティ対策のなかでも重要な「情報漏えい」に焦点をあてたもの
III	建設現場ネットワークの構築と運用ガイドライン 建設現場のネットワーク構成とそこでのセキュリティの考え方、導入、維持管理方法について解説

> ガイドラインの位置づけ

ツール	推奨対象者	提供元	タイトル
動画	○	トレンドマイク (YouTube)	ランサムウェアの起爆動画の公開について
eラーニング	○	IPA (専用HP)	建設業・製造業の経営者向けコース
eラーニング	○	IPA (専用HP)	建設業・製造業の管理者向けコース
eラーニング	○	IPA (専用HP)	建設業・製造業の一般社員向けコース

建設現場におけるセキュリティガイドライン
建設現場ネットワークの構築と運用ガイドライン
建設現場におけるスマートデバイス利用に関するセキュリティガイドライン

パンフレット、ポスター、動画、eラーニング、チェックシート

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り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と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。



警視庁サイバーセキュリティ対策本部

中小企業のセキュリティ対策強化への取組

→ 取組の目的が日建連と同様





中小企業のための サイバーセキュリティイベント(2017/11/2)

- ・各社の協力会社呼びかけ
- ・講演で「SNSによる情報漏えい」について

参加費 無料

中小企業のための サイバーセキュリティイベント

昨今、世界的規模で深刻な被害を蒙るランサムウェアの感染や不正アクセス犯罪とした大規模な情報流出被害が発生するなど、企業が有する顧客情報や知的財産は、常に攻撃者からの脅威に晒されており、企業の大小を問わずその対策は喫緊の課題となっています。

このような状況の中、企業もサイバー空間の脅威から守るためには、まず、初めに備わらず一人ひとりがサイバーセキュリティについての正しい知識を持ち、情報セキュリティ・情報セキュリティについて考える必要があります。

今回のセミナーでは、新しいと思われるサイバーセキュリティについて、初心者にも分かりやすい講演を行い、サイバー空間の脅威が身近な問題であることや、今後のサイバー空間との関わり方について解説します。

日時 平成29年11月2日(木) 13:00～16:45

会場 地方独立行政法人東京都立産業技術研究センター(本部)
東京都江東区青海 2-4-10
●ゆりかもめ「テレコムセンター」駅前
●りんかい線「東京テレポート」駅下車 無料送迎バス(乗降時間>3分
送迎バス乗降11 テレコムセンター駅前下車(バス3分(徒歩15分))

定員 200名

主催 地方独立行政法人東京都立産業技術研究センター
警視庁サイバーセキュリティ対策本部

協力 東京中小企業サイバーセキュリティ
支援ネットワーク (Tcyss)

申込方法 都産技研ホームページからお申し込みください。

<http://www.iri-tokyo.jp/site/johogijutsu/cs2017.html>
「Web申込書」からお申し込みください。【申込締切】平成29年10月31日(火)



国とともに、人とともに
 東京都立産業技術研究センター
 警視庁
 サイバーセキュリティ対策本部



中小金融機関向け サイバー攻撃対策訓練

部会メンバー参加
今後の活動の参考に

■サイバー攻撃対処能力向上技術訓練について

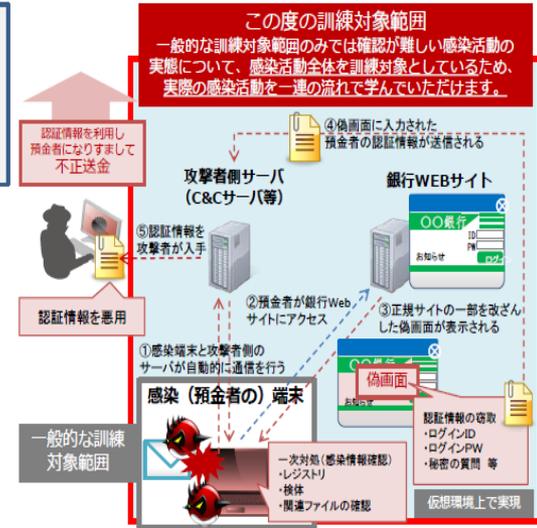
この度の訓練は、どの金融機関でも狙われる可能性のあるサイバー攻撃の手口と、インシデントが発生した際に必要となる対応方法について、金融機関等の職員の皆様を対象に、**実際の感染環境全体をイメージした訓練環境**を使用し、**感染活動を一連の流れで実感・必要知識を習得いただける訓練**です。

1.実施日程:11月8日(水)、11月17日(金)10:00~17:00
※訓練は両日同内容となります。

2.実施場所:トレンドマイクロ株式会社 12階会議室
東京都渋谷区代々木2-1-1 新宿メインズタワー
(R「新宿駅」南口より徒歩5分)

3.訓練内容

1. ネットバンキングマルウェアに関する座学講義 (10:00~12:00、13:15~14:30予定)
 - (1) 不正送金の実害
 - (2) サイバーセキュリティとは
 - (3) ネットバンキングマルウェアの概要
 - (4) ネットバンキングマルウェアの最近の傾向
 - (5) ネットバンキングマルウェアへの対策と、被害発生時の対応
2. 実機を使用した訓練 (14:30~17:00予定)
 - (1) 再現環境を用いて学ぶ、ネットバンキングマルウェア感染の実態
 - (2) 再現環境を用いて学ぶ、ネットバンキングマルウェアの被害発生時の対応





(小冊子) 中小企業向け サイバーセキュリティ対策の極意

✓ 協力会社等の取引先に！

サイバー月間

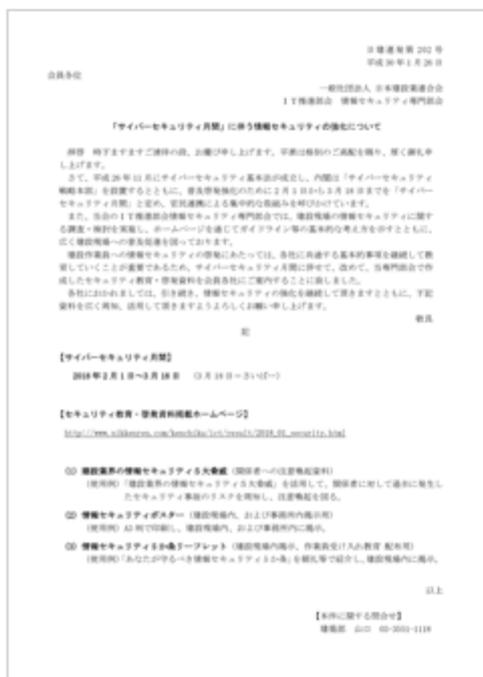
The screenshot shows the homepage of the Japan Federation of Construction Contractors (JFCC) website. The header includes the JFCC logo and navigation links such as '日建連について', 'ニュースリリース・コメント', '刊行物・資料', '建設業を学ぶ', and '委員会'. A search bar with 'Google カスタム検索' is also present. The main content area features a large '建築' (Architecture) title and a navigation menu with categories like '総合', '土木', '建築', '安全', and '環境'. Below the navigation, there is a breadcrumb trail: 'ホーム > 建築 > 建築 - IT WEB'. The main heading is '建築 - IT WEB'. Underneath, there is a 'NEWS' section with a blue circular icon. A news item is displayed with the date '2018.01.26' and the headline '「サイバーセキュリティ月間」に伴う情報セキュリティの強化」を発信しました。'. A blue arrow points from this news item towards the text below.

「サイバーセキュリティ月間」に伴う
情報セキュリティの強化を発信しました

通知文

● 「サイバーセキュリティ月間」に伴う情報セキュリティの強化

2018/01 発行



平成26年11月にサイバーセキュリティ基本法が成立し、内閣は「サイバーセキュリティ戦略本部」を設置するとともに、普及啓発強化のために2月1日から3月18日までを「サイバーセキュリティ月間」と定め、官民連携による集中的な取組みを呼びかけています。

また、当会の IT 推進部会情報セキュリティ専門部会では、建設現場の情報セキュリティに関する調査・検討を実施し、ホームページを通じてガイドライン等の基本的な考え方を示すとともに、広く建設現場への普及促進を図っております。

建設作業員への情報セキュリティの啓発にあたっては、各社に共通する基本的事項を継続して教育していくことが重要であるため、サイバーセキュリティ月間に併せて、改めて、当専門部会で作成したセキュリティ教育・啓発資料を会員各社にご案内することに致しました。

本資料

常に変化するリスク



前提：情報セキュリティ事故は発生する

説明が重要（日々の対策、発生時の対応）

サイバーセキュリティ月間

2/1~3/18

🚨 建設業5大脅威に注意 🚨



パソコンなどの
紛失・盗難



ブログ等SNSへの投稿
による現場写真の漏えい



図面など重要書類の
紛失・盗難



メール誤送信による
図面データ等の漏えい



標的型攻撃メールなど
によるウィルス感染



情報セキュリティ専門部会報告

ご静聴ありがとうございます

メンバー(会社名順)

高馬 洋一
相澤 健次郎
大塚 暁
石垣 順史
葛原 徹
豆腐谷 洋一

安藤ハザマ
大林組
鹿島建設
清水建設
大成建設
竹中工務店

嶽野 聡
長沼 秀明
山口 正志
滝沢 強
仙波 幹徳

東急建設
戸田建設
フジタ
前田建設工業
三井住友建設