

ある日突然サイバー攻撃の被害に (そのサイト大丈夫?!)

建設業においても年々増加するサイバー被害、
ランサムウェア・**二重脅迫**等その手口は高度化・巧妙化して
きています。

協力会社を含めたサプライチェーン全体での取り組みが必須
になっており、業界全体での底上げに向けて、日建連での取
り組みを紹介します。

情報セキュリティ専門部会

2023 7月4日 ランサムウェア感染により
名古屋港の全ターミナルが機能停止

2022 3月1日 取引先企業へのサイバー攻撃で
トヨタ自動車の国内全工場が稼働停止

経済産業省

サイバーセキュリティ経営ガイドライン Ver 3.0 (2023/3/24)

経営者が認識すべき3原則

- ・ 自らのリーダーシップのもとで対策を進めることが必要
 - ・ サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
 - ・ 関係者との積極的なコミュニケーションが必要
-

2024年 情報セキュリティ10大脅威

2023年

2024年

表 1.1 情報セキュリティ10大脅威 2023 「個人」および「組織」向けの脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等のニューノーマルな働き方を狙った攻撃
不正アプリによるスマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の不当請求による金銭被害	10	犯罪のビジネス化(アンダーグラウンドサービス)

1) ランサムウェアによる被害

2) サプライチェーンの弱点を悪用した攻撃

3) 内部不正による情報漏えい等の被害

4) 標的型攻撃による機密情報の窃取

ある日突然
サイバー攻撃の被害に
オンデマンドセミナー

2023年
11月6日(月) 8:00~
11月19日(日) 17:00

参加費無料
要事前申込



EMOTETの再流行やランサムウェア攻撃など、サイバーセキュリティへの対策はますます重要性を増しています。いつ、自社や自分自身がサイバー攻撃の標的になるかわからない状況で、企業のIT担当者やセキュリティ担当者は、いざという時の対応準備が求められています。

そこで、建設生産委員会 ICT推進部会 情報セキュリティ専門部会は、建設業界で発生しているサイバー攻撃の事例を紹介するとともにセキュリティ対策の専門家をお招きし、各企業のIT担当者、セキュリティ担当者の課題解決の一助になる各部署を紹介する録音セミナーをオンデマンド形式で開催いたします。

日時 2023年11月6日(月) 8:00~11月19日(日) 17:00

場所 オンデマンドセミナー (事前参加申込)

参加費 無料

- ある日突然サイバー攻撃の被害に～その操作が原因かも～
(講師：警視庁サイバーセキュリティ対策本部) 30分
- ある日突然サイバー攻撃の被害に～その時、対応するのは誰？～
(講師：日本シーサート協議会) 30分
- 脅威の事例と企業規模・利用シーン別「次の一手」
(講師：ICT推進部会情報セキュリティ専門部会 委員) 40分
- 日建連ICT推進部会情報セキュリティ専門部会について
(講師：ICT推進部会情報セキュリティ専門部会 会長) 10分

参加登録 <https://webinar.builders/seminars/form/VRO1EMdcvenH8rW259QpbUDIXYKpuCLs>
セミナー終了の2週間前まで申込可能



ある日突然
サイバー攻撃の被害に

ある日突然サイバー攻撃の被害に～その操作が原因かも～
(警視庁サイバーセキュリティ対策本部)

ある日突然サイバー攻撃の被害に～その時対応するのは誰～
(日本シーサート協議会)

脅威の事例と事業規模・利用シーン別の次の一手
(情報セキュリティ専門部会)

日建連 I C T 推進部会情報セキュリティ専門部会について
(情報セキュリティ専門部会)

警視庁

実例) サポート詐欺

PCの警告画面 → 記載された電話番号に電話 → PC遠隔操作
→ 電子マネーカード購入

実例) SNSの注意点

職場写真（企業・個人情報の映り込み）の投稿

実例) フィッシング詐欺

23年上半期の被害額：過去最多30億円

「急いでいる時」「思い込んでいる時」「疲れている時」

実例) サイバー攻撃

セキュリティ対策の進んでいないサプライチェーンを攻撃対象に

CSIRT

CSIRT (シーサート) セキュリティ事故を専門に扱う組織

→ **消防署の役割**

リスク (脅威) はコントロールできない

- ・ **被害抑制力**と**被害軽減力**で影響を小さくする
- ・ 「ミス無くせば事故を防ぐことができる」
→ 「被害を最小限に食い止めるための措置」 (ダメージコントロール)

組織のなかで有効に働くマネジメントシステムは「一つ」

- ・ ITだから特別なものではない
- ・ 「**まず落ち着け**」「**緊急時に多くのことはできない**」
(手順や判断基準はシンプルに)

作戦司令室を作る、キックオフ、チーム、定時報告の仕組み、ホワイトボードを用意、

日建連

(脅威の事例)

ID・パスワードの流出

ダークウェブ上で多くのIDが売買されている
全世界からアタック（不正ログイン）が多数
乗っ取られEMOTETの送信

フィッシング

本物と見分けがつかないメール/サイト

情報搾取ウイルス

2018年以降**6,000%の増加**
一般的ウイルス対策ソフトでは検知できない

二重脅迫型ランサムウェア

ダークウェブ上でサービス提供されている

日建連

企業規模・利用シーン別「次の一手」

(～50名程度)

ルータへの攻撃：診断、問題があればルータを最新機種に変更

「**サイバーセキュリティお助け隊**」ネットワーク監視型（月額6,000円～1万円）
ウィルス感染は防げないが外部へのデータ送信を遮断

パソコンを持ち出す場合は

「**サイバーセキュリティお助け隊**」エンドポイント型（月額2,000円/1台）
ウィルス感染は防げないが外部へのデータ送信を遮断

クラウドサービス利用の場合は

2段階認証 2要素認証

オフィシャルサイト：改ざん検知サービス（月額数千円）

日建連

企業規模・利用シーン別「次の一手」

(100名～数百名程度)

外から接続口（VPN利用等）が狙われやすい

OSやソフトウェアを常時**最新化**

ASM（Attack Surface Management）（中小企業向けに100万円程度のものあり）

クラウド型UTMの採用（運用が容易）（月額10万円程度から）

パソコン・サーバ

EDR（ふるまい検知型ウィルス対策）

NGAV（Next Generation Anti Virus）

運用まで任せるMDRサービスあり

日建連

企業規模・利用シーン別「次の一手」

(500名～)

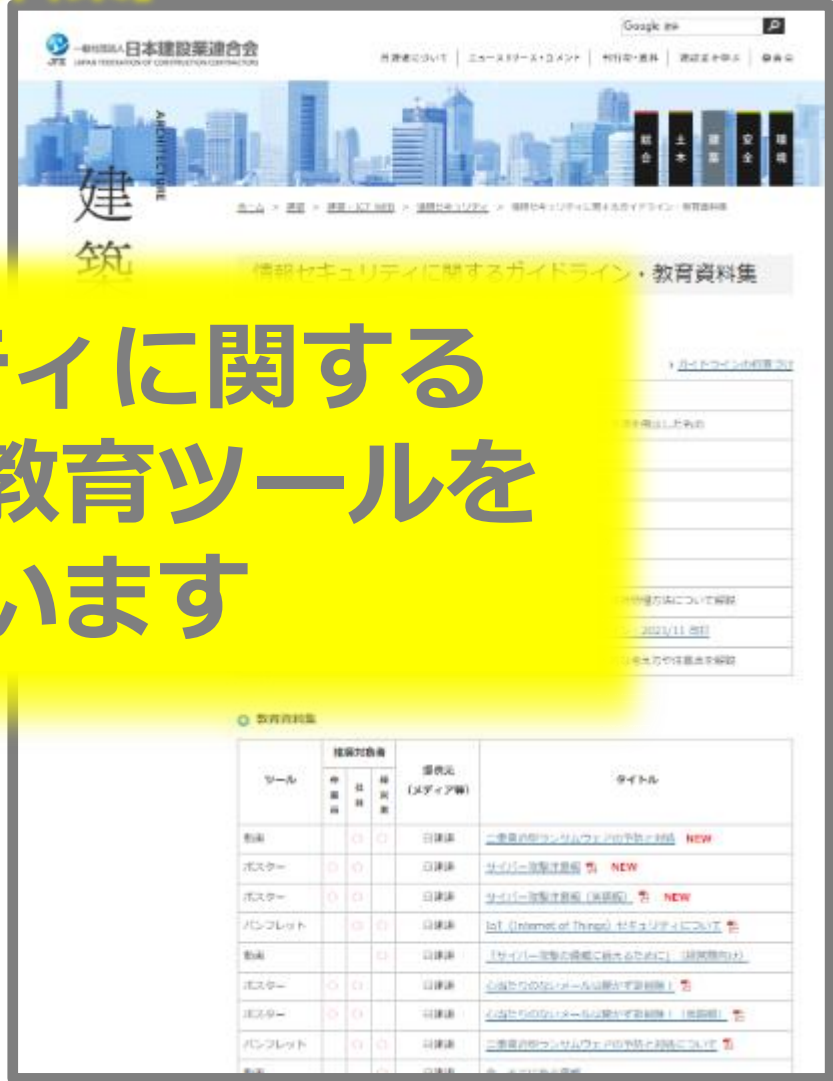
(対策にはきりがないところがあるが)

外部からの接続機器、クラウドサービス、サーバ、パソコン、ネットワーク

日建連→建築→IT-WEB →【ガイドライン・教育資料集】



情報セキュリティに関する
ガイドライン・教育ツールを
公開しています





教育動画_追加作成 「情報セキュリティ 5大脅威」 ミャンマー語字幕版

全体版 (建設会社社員用)	7分00秒
抜粋版 (現場作業員用)	3分30秒
項目別	
情報機器の紛失盗難	47秒
環境写真の漏えい	情報
図面紛失、報告遅延	
メール誤送信	情報セキュリティ「5大脅威」(英語版)
コンピュータウイルス感染	情報セキュリティ「5大脅威」(中国語-簡体字 字幕)
	情報セキュリティ「5大脅威」(インドネシア語 字幕)
	情報セキュリティ「5大脅威」(タイ語 字幕)
	情報セキュリティ「5大脅威」(ベトナム語 字幕)
	情報セキュリティ「5大脅威」(ミャンマー語 字幕)

သတင်းအချက်အလက်ကိစ္စများပျောက်ဆုံးခြင်း၊ အစိုးရခြင်း	7min03s	YouTube	download (213MB)
လုပ်ငန်းခွင်၏ ဝါတ်ပုံ ငေါက်ကြားခြင်း	3min33s	YouTube	download (123MB)
သတင်းအချက်အလက်ကိစ္စများပျောက်ဆုံးခြင်း၊ အစိုးရခြင်း	47s	YouTube	download (23.5MB)
လုပ်ငန်းခွင်၏ ဝါတ်ပုံ ငေါက်ကြားခြင်း	57s	YouTube	download (26.2MB)
ဆွဲထားသောရုပ်ပုံအသွယ်အရေးကြီးသောစာရွက်စာတမ်းများပျောက်ဆုံးခြင်း၊ အစိုးရခြင်း	53s	YouTube	download (20.8MB)
အီးပေးလ်များပို့ခြင်း	1min16s	YouTube	download (31.6MB)
ကွန်ပျူတာစိုင်းရပ်စ်ပိုးကူးစက်ခြင်း	1min27s	YouTube	download (34.5MB)

● ဆောက်လုပ်ရေးလုပ်ငန်းနယ်ပယ်၏ 「သတင်းအချက်အလက်လုံခြုံမှု」 ခြိမ်းခြောက်မှုကြီး ၅ခု



All version (For the staff of the construction company)	7min03s	YouTube	download (21.3MB)
Site workers version (For the construction site workers)	3min33s	YouTube	download (12.3MB)
By item			
သတင်းအချက်အလက်ကရိယာများပျောက်ဆုံးခြင်း၊ အစိုးခံရခြင်း	47s	YouTube	download (23.5MB)
လုပ်ငန်းခွင်၏ ဝါတ်ပုံ ပေါက်ကြားခြင်း	57s	YouTube	download (20.2MB)
ဆွဲထားသောရုပ်ပုံစသည့်အရေးကြီးသောစာရွက်စာတမ်းများပျောက်ဆုံးခြင်း၊ အစိုးခံရခြင်း	53s	YouTube	download (20.8MB)
အီးမေးလ်မှားပို့ခြင်း	1min16s	YouTube	download (31.6MB)
ကွန်ပျူတာစိုင်းရပ်စ်ပိုးကူးစက်ခြင်း	1min27s	YouTube	download (34.5MB)

Don't post photos of your construction site on social media!

လုပ်ငန်းခွင်ဓာတ်ပုံကိုမတင်ပါနှင့်!

一般社団法人 日本建設業連合会
 JFCC JAPAN FEDERATION OF CONSTRUCTION CONTRACTORS

内容	時間
全体版(建設会社社員用)	7分03秒
詳細版(現場作業員用)	3分33秒
(項目別)	
情報機器の紛失盗難	47秒
現場情報の漏洩	57秒
図面紛失、報告遅延	53秒
メール誤送信	1分16秒
コンピュータウイルス感染	1分27秒



音声	表示	字幕
日本語	日本語	—
英語	英語	—
英語	英語	中国語
英語	英語	インドネシア語
英語	英語	タイ語
英語	英語	ベトナム語
英語	英語	ミャンマー語

協力会社向け
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について～
情報管理も大事な仕事の一つです

(会社名)

近年、個人情報やランサムウェア感染等による情報漏えい事故がテレビ・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。

工事に關する「情報」とは >>>

- ・ 図面、工程表、写真、打合せ記録
- ・ 建築主、元請け、従業員、近隣等の個人情報 (個人を特定できる情報が記載された書類等)
- ・ 施工建物の内部や設備の状況が分かる写真
- ・ 会社の技術やノウハウ (標準仕様等)
- ・ 契約書、見積書、発注書等の各種書類
- ・ 業務で作成する資料

など、業務で取り扱うすべてのものが工事に關する情報です

もし、「情報」が漏れてしまったら…>>>
万が一「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ます。(例え過失でも、解雇や懲戒などの可能性もあります)
- ・ 会社は信用を失い、工事を受注できなくなります。
- ・ 刑事責任・損害賠償責任を問われる恐れがあります。

なぜ、どうして「情報」が漏れたの…>>>

ほとんどが次の例のような不注意や認識不足、警備不十分、です。

- ・ 知人から送られたものの、内容に心当たりはないメールの添付ファイルを開いたらウイルスに感染してパソコンに保存された業務データやメールがすべて流出してしまった。
- ・ 工事に携わる社員が、作業用内の写真をツイッターに投稿して、建築主に見つかり叱責を受けた。
- ・ 工事情報や個人情報を保管したパソコンやスマートフォン、USBメモリを紛失し、パスワード保護もしていなかったためデータが流出した。

「情報」を守るための9つのポイント

万が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、このトを自覚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 ウィルス対策ソフトを必ずパソコンに入れる >>>

- ・ パソコンには、ウィルスを検知・駆除するためのウィルス対策ソフトを常に最新の状態で更新してください。
- ・ OS やソフトウェアのアップデートを自動に設定して、常に最新の状態に保ってください。

ポイント3 私有パソコンや私有スマートデバイスを業務に使わない >>>

- ・ 私有のパソコンやスマートデバイスを業務に使用しないでください。
- ・ 私有パソコン等に業務データがある場合は速히削除してください。
 - 私有のパソコンやスマートデバイス等は、会社買入のものに比べてセキュリティ対策が不十分なため、情報流出のリスクが高くなります。

ポイント4 パソコンは、必ずディスクを暗号化し、ログインパスワードを設定する >>>

暗号化とは、パソコンやスマートデバイスに保存されたデータの暗号化を指し、不正アクセス防止に有効です。

ポイント7 しっかりと保管する >>>

- ・ 情報を扱うパソコンのハードディスクは暗号化し、情報を保管するUSBメモリ・外付ハードディスク等の外部記憶媒体は自動暗号化機能の付いた製品を利用してください。
- ・ 図面・書類や外部記憶媒体は、決められた場所に保管し、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。
 - 作業所事務所等には24時間の機械警備を導入して盗難を防止してください。

「情報」は絶対に口外しない >>>

住宅等の個人情報の取扱いに注意してください。個人情報法で厳しく定められており、法令に違反した場合罰金を課せられます。

口外しないでください。 (飲食店、等)では仕事の話をしないようにしましょう。

・ ログ(個人日記)、掲示板、SNS等、口外した内容を公開しないようにしてください。

➢ 建物内部や工事状況の写真や動画を撮影して、SNS等にアップロードしないようにしてください。

ポイント2 不要なメール、Webサイトの閲覧などに注意する

- ・ ウィルスへの感染は、巧妙に偽装されたメールの添付ファイルをクリックしたりすることで起こります。
 - 送信者が知人や顧客であっても心当たりのない内容のメールには、開かないようにしてください。
 - 最近は、請求書、宅配便到着通知、オンラインショッピング、メールアドレス等を巧妙に偽装したものが多く、見分けが難しくなっています。
- ・ 正規のWebサイトでも、攻撃者に乗っ取られて改ざんされているWebサイトにアクセスしない、広告のクリックに注意してください。

・ データの送信にファイル転送サービスやオンラインストレージを使う場合は、会社許可した安全なサービスを利用してください。

ポイント8 「情報」の持ち出しや持ち歩きには注意する >>>

- ・ 図面、書類やパソコン、外部記憶媒体を必要以上に現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やスマートデバイスは、紛失・盗難に備えて、パスワード設定、暗号化等の対策を行ってください。
- ・ 現場の外では持ち歩きに注意してください。電車内で網棚、座席ポケットに置いたり、駐車時に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。
 - 外食や飲酒、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9 「情報」は確実に返却・廃棄する >>>

- ・ 工事が完了したら、保管が認められた情報以外は、契約に基づき、必ず返却・廃棄・消去してください。廃棄・消去する際は、情報が漏れないよう、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。
 - CD、DVD等の外部記憶媒体はハサミで切断するなど、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。ゴミ箱からの削除だけでは復元できるため、ゴミ箱から削除したうえで完全削除を行う。(専用ソフトやcipher.exeコマンド等)
 - パソコンを廃棄するときは情報できる業者に依頼する。

もしも「情報」が漏れてしまったら

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判断した場合には、直ちに会社の上層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、弊社社員にお尋ねください。

パンフレット_改定
「情報漏えい防止の徹底について」

情報を守るための9つのポイント

ウイルス対策ソフトを必ずパソコンに入れる

不審なメール、Webサイトの**閲覧**などに注意する

私有パソコンや**私有**スマートデバイスを業務に使わない

パソコンは、必ずディスクを暗号化し、ログインパスワードを設定する

「情報」の社外への送信は最小限にとどめ、**誤配**に注意する

「情報」の持ち出しや持ち歩きには注意する

しっかりと**保管**する

工事に関する「情報」は絶対に**口外**しない

「情報」 は確実に**返却・廃棄**する



林内閣官房長官メッセージ

フィッシング詐欺の被害金額は、昨年、過去最多
サポート詐欺の被害も増加
中小企業などサプライチェーンの弱点を狙う
基本的な対策を徹底して頂くことがとても重要

— 確かなものを地球と未来に —



一般社団法人 日本建設業連合会
JAPAN FEDERATION OF CONSTRUCTION CONTRACTORS

日建連について

会長等コメント、提言・要望

刊行物・資料

建設業を知る、学ぶ

総合

土木

建築

安全

環境

ホーム > 建築 > 建築 - ICT WEB > 情報セキュリティ

「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

2024/01 発行

サイバーセキュリティ月間

「情報セキュリティの強化」発信



ICT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。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合わせて、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。

建築 - ICT WEB

ICT推進部会の紹介

建築のICT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)
- > 教育・研修用動画

先端ICT活用

■ 本サイトに掲載する情報は、最新の情報となります。ご活用の際は、必ず最新の情報をご確認ください。

■ 本サイトに掲載する情報は、著作権者(株)日建連の登録商標であり、無断で複製・転載を禁じます。

■ 本サイトに掲載する情報は、第三者に開示することにより、損害を被る可能性があります。ご活用の際は、必ず最新の情報をご確認ください。

■ 本サイトに掲載する情報は、著作権者(株)日建連の登録商標であり、無断で複製・転載を禁じます。

「そのサイト大丈夫!？」ポスター（日本語版）

推奨対象者：作業員、社員

提供元：日建連



ダウンロード

「そのサイト大丈夫!？」ポスター（英語版）

推奨対象者：作業員、社員

提供元：日建連



ダウンロード

動画：「サイバー攻撃の脅威に備えるために【改訂版】」（経営者向け）



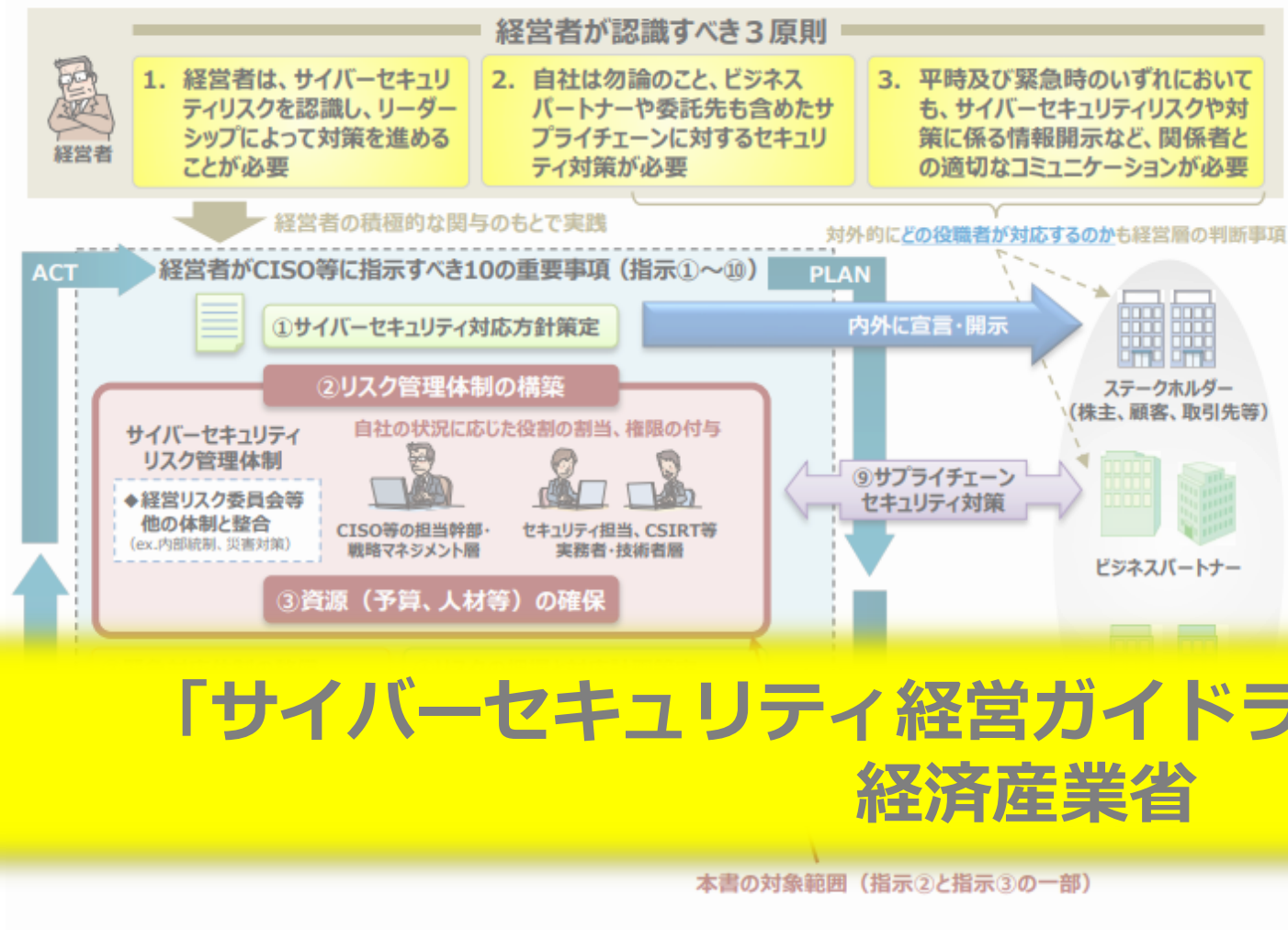
動画公開ページ (Youtube & ダウンロード)

オンデマンドセミナー「ある日突然サイバー攻撃の被害に」【再配信】



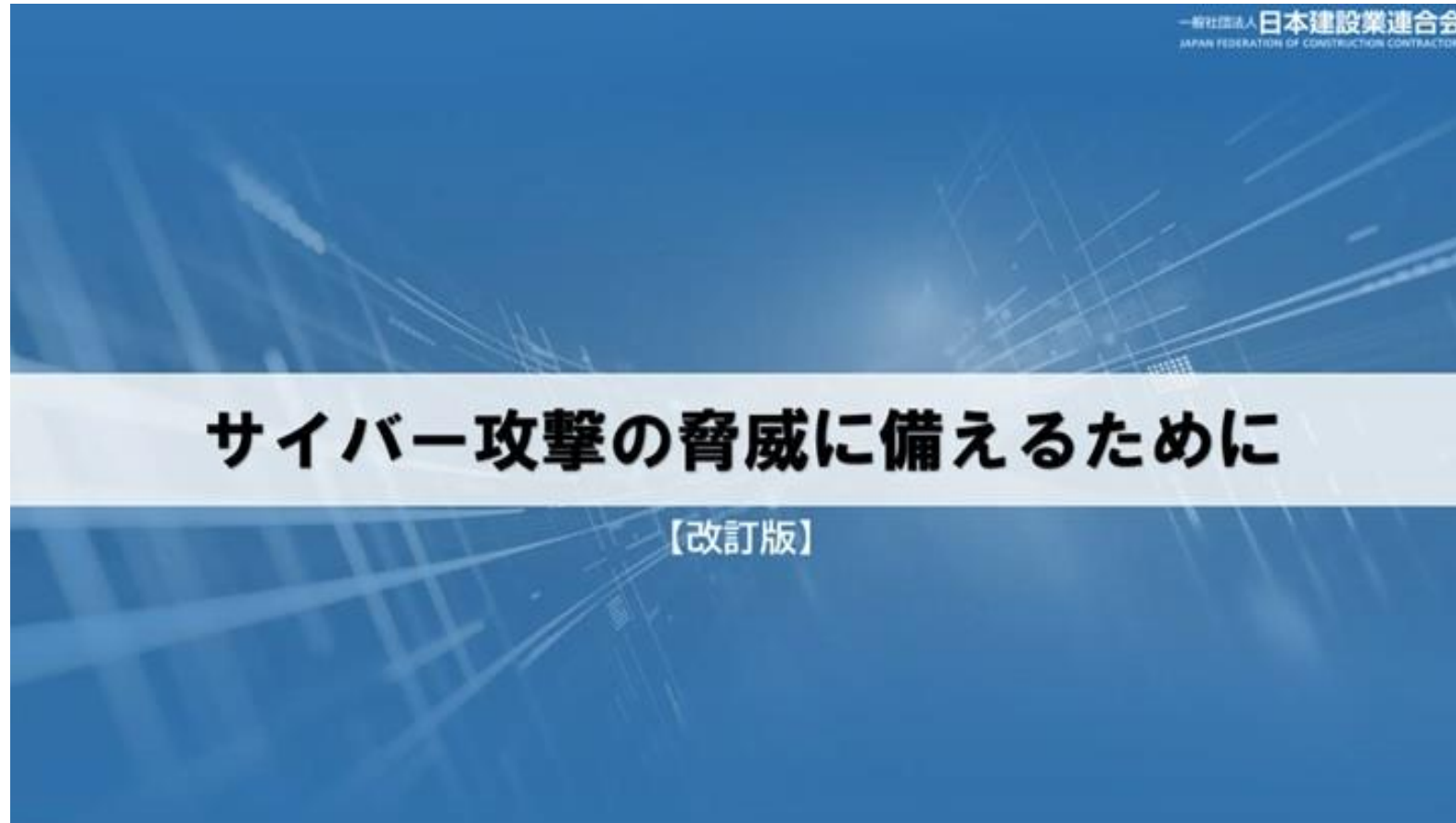
ダウンロード

図表1 サイバーセキュリティ経営ガイドラインの全体像と本書の位置付け



「サイバーセキュリティ経営ガイドライン Ver3.0」公開 経済産業省

動画：「サイバー攻撃の脅威に備えるために【改訂版】」（経営者向け）





SC3 サプライチェーン・サイバーセキュリティ・コンソーシアム

お問い合わせ リンク集 English

HOME SC3とは 会員一覧 ニュース 活動状況

サプライチェーン・サイバーセキュリティ・コンソーシアム (SC3) とは

HOME / サプライチェーン・サイバーセキュリティ・コンソーシアム (SC3) とは

English

組織概要 規約・規則等 入会について

2020年11月1日に、産業界が一体となって中小企業を含む**サプライチェーン全体**でのサイバーセキュリティ対策の推進運動を進めていくことを目的とした「サプライチェーン・サイバーセキュリティ・コンソーシアム (SC3)」が設立されました。



サイバーセキュリティお助け隊サービス



IT導入補助金 で

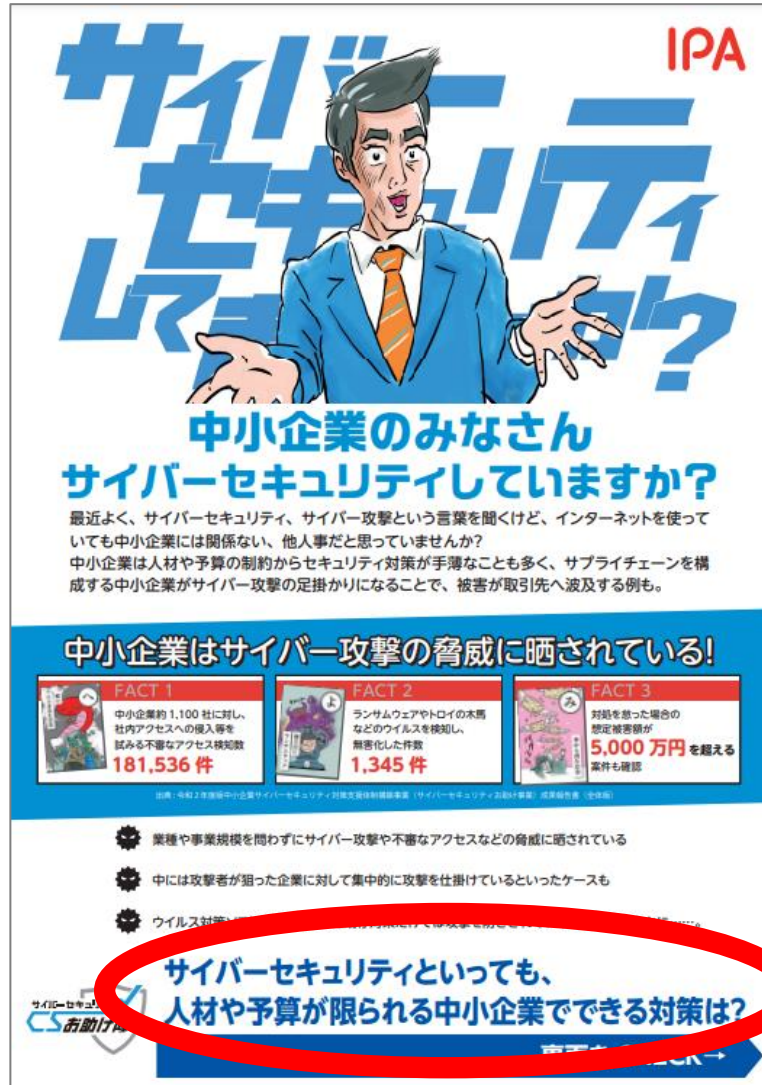
「サイバーセキュリティお助け隊サービス」の
サービス利用料が支援対象となります！



IT導入
補助金
とは？

中小企業・小規模事業者のみなさまが
ITツール導入に活用いただける補助金です。
IT導入補助金で「サイバーセキュリティお助け隊サービス」
のサービス利用料の支援が受けられます。

▼ くわしくはこちら ▼



サイバーセキュリティお助け隊サービス

IPA

中小企業のみなさん サイバーセキュリティしていますか？

最近よく、サイバーセキュリティ、サイバー攻撃という言葉聞くけど、インターネットを使っても中小企業には関係ない、他人事だと思いませんか？
中小企業は人材や予算の制約からセキュリティ対策が手薄なことも多く、サプライチェーンを構成する中小企業がサイバー攻撃の足掛かりになることで、被害が取引先へ波及する例も。

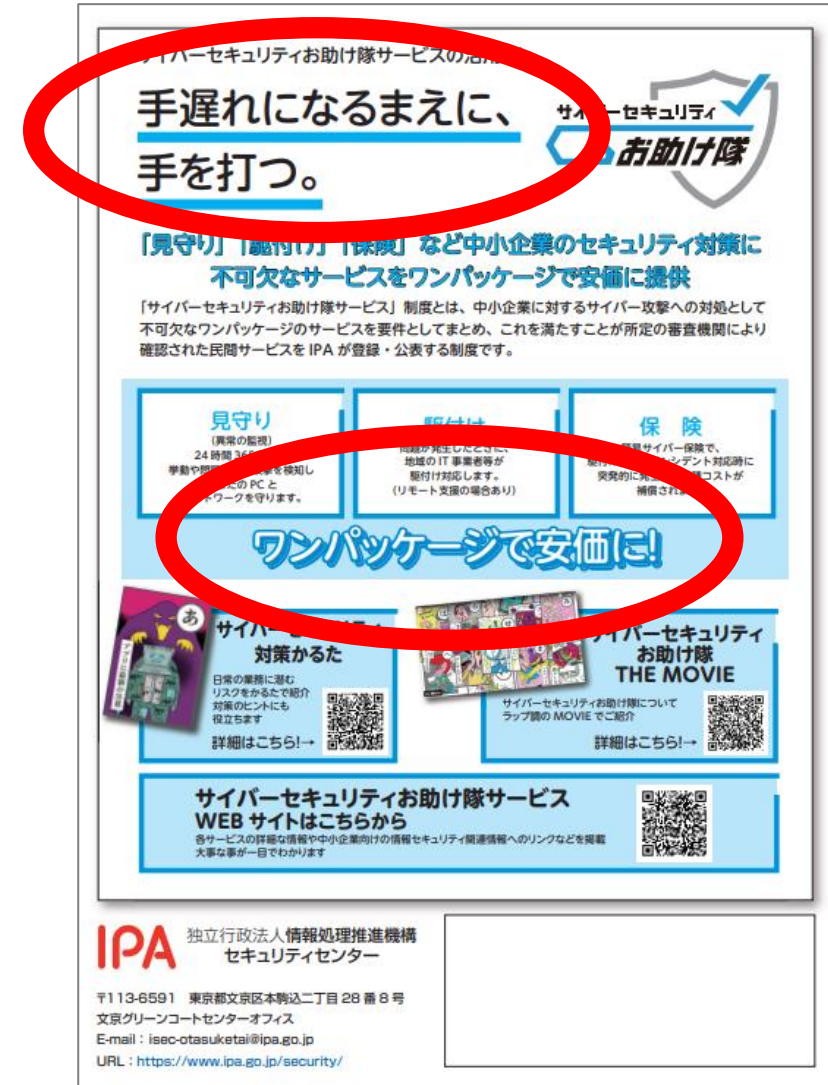
中小企業はサイバー攻撃の脅威に晒されている！

FACT 1	FACT 2	FACT 3
中小企業約 1,100 社に対し、社内アクセスへの侵入等を試みる不審なアクセス検知数 181,536 件	ランサムウェアやトロイの木馬などのウイルスを検知し、無害化した件数 1,345 件	対策を怠った場合の想定被害額が 5,000 万円 を超える 案件も確認

出典：令和2年度中小企業サイバーセキュリティ対策支援特別調査報告書（サイバーセキュリティお助け隊） 成果報告書（全体版）

- 業種や事業規模を問わずにサイバー攻撃や不審なアクセスなどの脅威に晒されている
- 中には攻撃者が狙った企業に対して集中的に攻撃を仕掛けていくといったケースも
- ウイルス対策...

サイバーセキュリティといっても、 人材や予算に限られる中小企業でできる対策は？



サイバーセキュリティお助け隊サービス

手遅れになるまえに、手を打つ。

「見守り」「駆け付け」「保険」など中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供

「サイバーセキュリティお助け隊サービス」制度とは、中小企業に対するサイバー攻撃への対応として不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすことが所定の審査機関により確認された民間サービスをIPAが登録・公表する制度です。

見守り	駆け付け	保険
（真実の監視） 24時間365日、 手動や自動でPCとネットワークを守ります。	即時発生したサイバー攻撃に対し、地域のIT事業者等が駆け付け対応します。（リモート支援の場合あり）	見守りサイバー保険で、突発的な被害発生時に補償されるコストが

ワンパッケージで安価に！

サイバーセキュリティ対策かるた
日常の業務に潜むリスクをかるたで紹介。対策のヒントにも役立ちます
詳細はこちら！→

サイバーセキュリティお助け隊 THE MOVIE
サイバーセキュリティお助け隊についてラップ観のMOVIEで紹介
詳細はこちら！→

サイバーセキュリティお助け隊サービス WEBサイトはこちらから

各サービスの詳細な情報や中小企業向けの情報セキュリティ関連情報のリンクなどを掲載。大事な事が一目でわかります

IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス
E-mail: isec-otasuketai@ipa.go.jp
URL: https://www.ipa.go.jp/security/

日建連→建築→IT-WEB →【ガイドライン・教育資料集】



目次

- I 建設現場における情報セキュリティガイドライン（2022/11/28訂）
- II 情報セキュリティマネジメントシステムの構築と関係性、実施すべき事項を定めたもの
- III 建設現場における情報セキュリティガイドライン（2022/11/28訂）
- IV 建設現場に実施すべき情報セキュリティ対策をまとめたもの
- V 建設現場における情報セキュリティガイドライン（2022/11/28訂）
- VI 建設現場における情報セキュリティ対策をまとめたもの
- VII 建設現場における情報セキュリティガイドライン（2022/11/28訂）
- VIII 建設現場における情報セキュリティ対策をまとめたもの
- IX 建設現場における情報セキュリティガイドライン（2022/11/28訂）
- X 建設現場における情報セキュリティ対策をまとめたもの

教育資料集

ジャンル	建築対象者			提供元 (メディア種)	タイトル
	事業者	建設者	労働者		
動画	○	○	○	日建連	二重層の防壁システムでの防壁の役割 NEW
ポスター	○	○	○	日建連	サイバー攻撃は情報 NEW
ポスター	○	○	○	日建連	サイバー攻撃は情報（英語版） NEW
パンフレット	○	○	○	日建連	IoT（Internet of Things）がセキュリティについて
動画	○	○	○	日建連	「サイバー攻撃は情報」をまとめたもの（英語版あり）
ポスター	○	○	○	日建連	建設現場のセキュリティ対策をまとめたもの
ポスター	○	○	○	日建連	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	○	○	○	日建連	二重層の防壁システムでの防壁の役割について

安全なサイバー空間を目指して

安心して、ICT活用を推進するために
皆様のご協力をお願い致します

情報セキュリティ専門部会

安藤ハザマ
竹中工務店
大林組
鹿島建設
清水建設
大成建設

高馬 洋一
豆腐谷 洋一
杉山 宜督
田口 慶
平林 直樹
葛原 徹

東急建設
戸田建設
フジタ
前田建設工業
三井住友建設

藤井 隆行
藤田 直紀
山口 正志
種村 崇
仙波 幹徳