

「サイバー攻撃を防ぐ鍵はあなた」



情報セキュリティ専門部会

「サイバー攻撃を防ぐ鍵はあなた」



日建連TOPページ



情報セキュリティ専門部会

サイバーセキュリティ月間（2/1～3/18）

林内閣官房長官メッセージ



内閣サイバーセキュリティセンター（NISC）HP

産学官民で連携

サイバー攻撃は益々**深刻化**

フィッシング詐欺が多発

企業を襲うランサム攻撃の**勢いが増す**

ランサムウェア被害の約半数は**中小企業**

基本的な対策を徹底する

不審なリンクを開かない

最新バージョンにアップデート

全員参加で取り組む

サイバーセキュリティ月間（オンデマンドセミナー）



サイバー攻撃を防ぐ鍵はあなた

サイバーセキュリティ対策の必要性～サイバー犯罪の脅威と対策～
（警視庁サイバーセキュリティ対策本部）

中小企業の情報セキュリティ対策
（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）

サイバー攻撃を防ぐ鍵はあなた～最新の脅威事例と「次の一手」～
（情報セキュリティ専門部会）

日建連ICT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）

建築生産委員会 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実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担当者やセキュリティ担当者の課題解決の一助となる各種情報を紹介するセミナーを以下のとおり開催いたします。ぜひ、多くの皆様のご参加をお待ちしております。

公開期間 2025年2月1日（土）9:00～3月2日（日）17:00

参加形式 オンデマンドセミナー（事前申込制）

参加費 無料

スケジュール 講演①：サイバーセキュリティ対策の必要性～サイバー犯罪の脅威と対策～
（講師：警視庁サイバーセキュリティ対策本部） ●30分
講演②：中小企業の情報セキュリティ対策
（講師：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
普及啓発・振興部 普及啓発グループ） ●30分
講演③：サイバー攻撃を防ぐ鍵はあなた～最新の脅威事例と「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
講演④：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 主査） ●5分

申込み <https://webinar.builders/seminars/form/407b2K7oMjRGCCoekE4YalNntbuoRX>
申し込みは右の二次元コードから >>



サイバーセキュリティ月間（オンデマンドセミナー）

警視庁

「サイバーセキュリティ対策の必要性 ～サイバー犯罪の脅威と対策～」

実例) サポート詐欺

インターネット検索 → PCの偽警告画面

→ 記載された電話番号に電話

→ PC遠隔操作 → サポート名目の電子マネー要求

実例) メール等を利用したサイバー攻撃

8年で100倍以上の件数

法人口座を狙った不正送金

ビジネスツールの主役はメール

「0101…で始まる電話は詐欺の可能性が高い」

実例) ランサムウェア

ランサム攻撃のビジネス化Raas (Ransom as a Service)

狙い先：大手企業だけではなく防御が手薄な企業

サイバーセキュリティ月間（オンデマンドセミナー）

I P A

「中小企業の情報セキュリティ対策」

【現状認識】

DX（デジタル化）推進
データ化した情報のやり取りが**ビジネスの中心**
利用システムの管理難易度が上昇
会社内外の**境界があいまい**
サイバー攻撃の脅威も増大

【ランサムウェア攻撃対策】

脆弱性対策、
機器を減らす（インターネット接続）、
バックアップ、BCP、訓練

KADOKAWAグループ（2024/6）、HOYA（2024/3）、
LINEヤフー（2023/11）、名古屋港運協会（2023/7）、
大阪急性期総合医療センター（2022/10）

2025年 情報セキュリティ10大脅威

| 順位 | 「組織」向け脅威 | 2016年以降 |
|----|-----------------------|-----------|
| 1 | ランサム攻撃による被害 | 10年連続10回目 |
| 2 | サプライチェーンや委託先を狙った攻撃 | 7年連続7回目 |
| 3 | システムの脆弱性を突いた攻撃 | 5年連続8回目 |
| 4 | 内部不正による情報漏えい等 | 10年連続10回目 |
| 5 | 機密情報等を狙った標的型攻撃 | 10年連続10回目 |
| 6 | リモートワーク等の環境や仕組みを狙った攻撃 | 5年連続5回目 |
| 7 | 地政学的リスクに起因するサイバー攻撃 | 初選出 |
| 8 | 分散型サービス妨害攻撃（DDoS攻撃） | 5年ぶり6回目 |
| 9 | ビジネスメール詐欺 | 8年連続8回目 |
| 10 | 不注意による情報漏えい等 | 7年連続8回目 |

IPA 情報処理推進機構HP

2025年 情報セキュリティ10大脅威

「個人」向け脅威（五十音順）

2016年以降

| | |
|-----------------------------|------------------|
| インターネット上のサービスからの個人情報の窃取 | 6年連続9回目 |
| インターネット上のサービスへの不正ログイン | 10年連続10回目 |
| クレジットカード情報の不正利用 | 10年連続10回目 |
| スマホ決済の不正利用 | 6年連続6回目 |
| 偽警告によるインターネット詐欺 | 6年連続6回目 |
| ネット上の誹謗・中傷・デマ | 10年連続10回目 |
| フィッシングによる個人情報等の詐取 | 7年連続7回目 |
| 不正アプリによるスマートフォン利用者への被害 | 10年連続10回目 |
| メールやSMS等を使った脅迫・詐欺の手口による金銭要求 | 7年連続7回目 |
| ワンクリック請求等の不当請求による金銭被害 | 3年連続5回目 |

IPA 情報処理推進機構HP

サイバーセキュリティ月間（オンデマンドセミナー）

情報セキュリティ専門部会

「サイバー攻撃を防ぐ鍵はあなた ～最新の脅威事例と「次の一手」～」

情報セキュリティの難しさ：**攻撃側と防御側の圧倒的な差**
相手は命がけで攻撃（北朝鮮）
家の鍵はかけるのに、

サイバーセキュリティ経営ガイドライン
サイバーセキュリティ対策評価制度
自工会

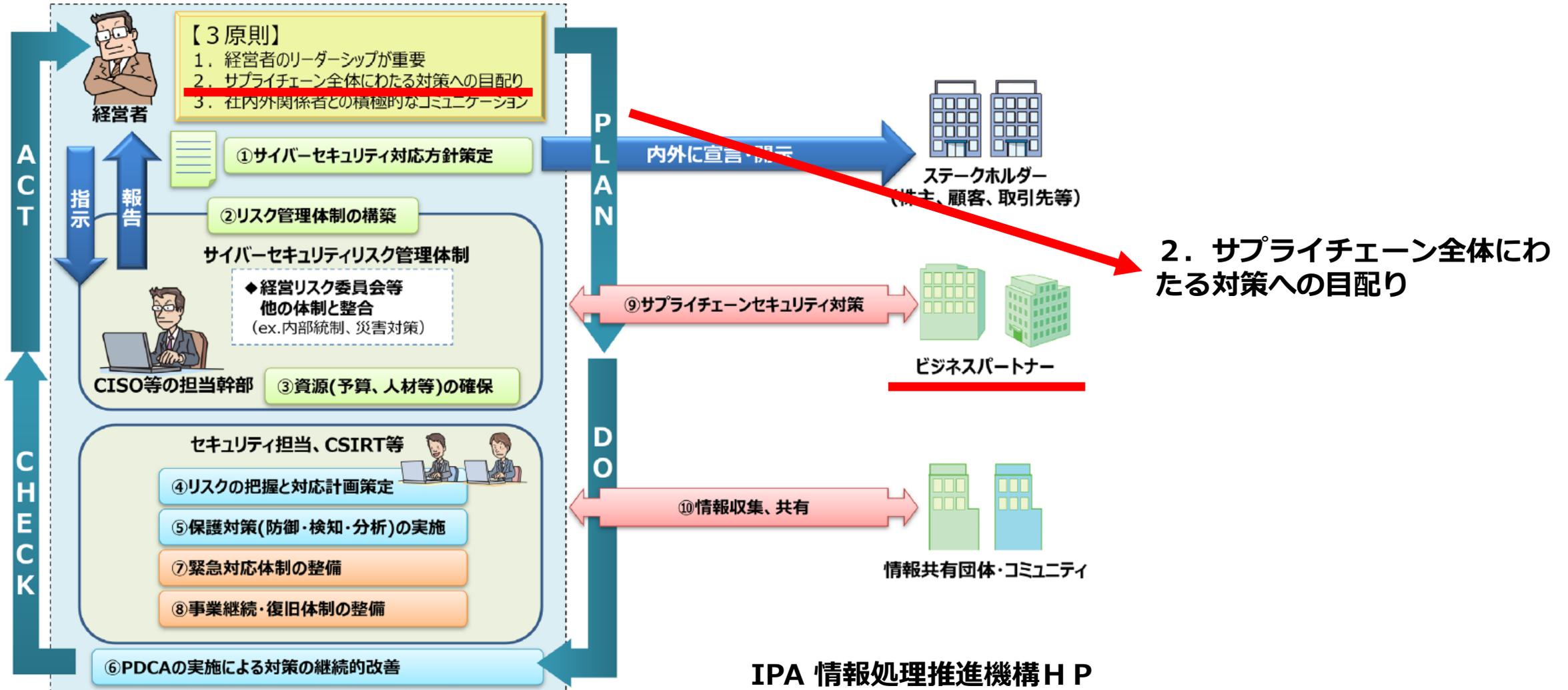
IDパスワード流出：オンラインサイトや自宅パソコンからが多い

EPP：入場制限、EDR：万引きGメン

次の一手（小規模～50人）：サイバーお助け隊

サイバーセキュリティ月間（オンデマンドセミナー）

サイバーセキュリティ経営ガイドライン 第3版 2023年3月発行



サイバーセキュリティ月間（オンデマンドセミナー）

サイバーセキュリティ対策評価制度

「サプライチェーン強化に向けたセキュリティ対策評価制度」構成・内容イメージ

IPA

- ◆ サイバー攻撃により、取引上共有している機微情報の漏洩や部品・サービスの供給途絶など、自社のみならずサプライチェーン全体に影響を及ぼす事態が発生しうる。このようなインシデントの予防・抑制を目的に、サプライチェーン構成企業全体のセキュリティ対策レベルの向上と、実施状況の効率的な確認ができる手法として「サプライチェーン強化に向けたセキュリティ対策評価制度」を提案。
- ◆ 中小企業を含めた多様なサプライチェーン企業が参照できるよう、三段階のセキュリティレベルを想定。

| | 三つ星（★3） | 四つ星（★4） | 五つ星（★5） |
|---------------------------|---|---|--|
| 段階の考え方 (企業がどういう状態にあるか) | 現場レベルや部分的なレベルでのセキュリティ対策が実践されている | 自社に合わせたセキュリティ対策の組織的・継続的な実施・改善 (PDCA) がなされている | サイバー空間上のリスクを適宜適切に把握し、合理的な対策を実施、継続的改善がなされている |
| 対象として想定する事業者 | サプライチェーンを形成するすべての企業等 | ・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）のサプライチェーンにおいて重要な機能・役割等を担うサプライヤー企業 | ・産業界を代表・牽引する立場の企業等（それを目指す企業等を含む）のサプライチェーンにおいて特に重要な機能・役割等を担うサプライヤー企業等 |
| 対策セットの考え方 (対策の規模感) | 上記に該当する企業等が、最低限実装すべきセキュリティ対策の水準 (15項目程度) | 上記に該当する企業等が、標準的に目指すべきセキュリティ対策の水準 (~50項目程度) | 上記に該当する企業等が、現時点で到達点として目指すべきセキュリティ対策の水準 (100項目~) |
| 実施状況の評価・確認方法 | ・自己適合宣言（社内外の登録セキュリティ等専門家による確認） | ※既存のガイドラインや認証制度などを活用可能なスキームを検討※ ・自己適合宣言（★3と同様） ・第三者評価 と二段階に分けることも考えられる (★4、★4 plus) | ・第三者評価 |

→ サプライチェーン構成企業全体のセキュリティ対策レベルの向上と、実施状況の効率的な確認ができる手法

サイバーセキュリティ月間（オンデマンドセミナー）

日本自動車工業会

The screenshot shows the JAMA website's 'IT・標準化' section. The main heading is '自動車産業サプライチェーンへの推進活動'. Below it, a breadcrumb trail reads: 'HOME > 自工会の活動 > IT・標準化 > サイバーセキュリティ推進活動 > 自動車産業サプライチェーンへの推進活動'. The main text describes the '自動車産業サイバーセキュリティガイドライン' and mentions a meeting for implementation and expansion. A list of links includes: '2024年度 自己評価の実施・展開及び経営層向け説明会' (2024年7月4日公開), '2024年度 自己評価の実施・展開及び経営層向け説明会資料' (2024年9月24日公開), and '2024年度 自己評価の実施・展開及び経営層向け説明会アーカイブ動画' (2024年9月24日公開). A video player is embedded, showing a presentation slide titled '2024年度 経営層向け説明会 「自動車産業サイバーセキュリティガイドライン」 自己評価の実施・展開のお願い'. The slide lists the organizing bodies: '日本自動車工業会' and '日本自動車部品工業会', and the date: '2024年 8月, 9月, 10月'. A red arrow points from the text on the right to the video player.

「自動車産業
サイバーセキュリティガイドライン」

自己評価の実施・展開のお願い

JAMA 日本自動車工業会HP

2024年度 建築のICTセミナー

サイバーセキュリティ月間（ポスター）



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



JAPAN FEDERATION OF CONSTRUCTION CONTRACTORS
JFCC

サイバーセキュリティ月間（動画）

建設現場における「情報漏えい事故例」と「注意ポイント」

6分30秒



「建設現場ネットワークの構築と運用ガイドライン」改定

(利用が拡大しているオンラインストレージ等のクラウドサービスの利用に関する記述を中心に追加)

| | |
|-----|--|
| I | 建設現場における情報セキュリティガイドライン：2024/2 修正 |
| | 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 | 元請会社における情報セキュリティガイドライン：2024/2 修正 |
| | 元請会社が確実に実施すべき情報セキュリティ対策をとりまとめたもの |
| III | 協力会社における情報セキュリティ対策について：2024/2 修正 |
| | 協力会社の情報セキュリティ対策の強化を促す際の参考資料としてとりまとめたもの |
| IV | 建設現場ネットワークガイドライン：2024/12 改訂 |
| | 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 |
| V | 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：2024/2 修正 |
| | 誰でも手軽に利用できるスマートデバイスを活用するにあたっての基本的な考え方や注意点を解説 |

他団体との活動（SC3）

- 各業界の取組を参考にして
協力会社へのセキュリティ対策を検討していく
- 建設業に見合う活動を提言

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

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）について

高度化するサイバー攻撃は企業にとって大きな脅威であり、サイバー攻撃に適切に対処できない場合、事業継続性に加えて企業の信用にも影響を及ぼす重大な問題になり得ます。また、近年、攻撃対象企業の取引先といったサプライチェーン上の弱点となり得る部分を狙った攻撃も増加しており、セキュリティ対策が強固とはいえない中小企業が攻撃の標的となり、サプライチェーンに関わる他の企業にも被害が及ぶケースも確認されています。

このような背景のもと、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て「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。

IPA 情報処理推進機構HP

他団体との活動（SC3）

高度化するサイバー攻撃は企業にとって**大きな脅威**であり、サイバー攻撃に適切に対処できない場合、**事業継続性**に加えて企業の**信用にも影響**を及ぼす重大な問題になり得ます。また、近年、攻撃対象企業の取引先といった**サプライチェーン上の弱点**となり得る部分を狙った攻撃も増加しており、セキュリティ対策が強固とはいえない**中小企業が攻撃の標的**となり、サプライチェーンに関わる他の企業にも被害が及ぶケースも確認されています。

このような背景のもと、**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て「**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。

他団体との活動（お助け隊）



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。

ワンパッケージで安価に！

見守り

(異常の監視)

24時間365日監視
挙動や問題のある攻撃を
検知しあなたのPCと
ネットワークを守ります。

駆付け

問題が発生したときに、
地域のIT事業者等が
駆付け対応します。
(リモート支援の場合あり)

保険

簡易サイバー保険で、
駆付け支援等インシデント
対応時に突発的に発生する
各種コストが補償されます。



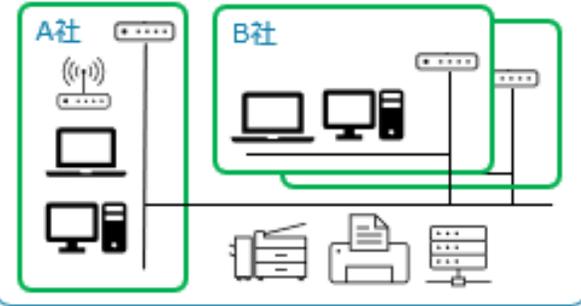
中小企業向けの安価なサービス
「見守り」（ネットワーク監視）
「駆付け」（発生時対策）
「保険」（サイバー保険）

IPA 情報処理推進機構HP

日建連→建築→IT-WEB →【ガイドライン・教育資料集】



(1) 現場事務所内ネットワーク



(2) 企業内ネットワーク



インターネット網
携帯通信網
衛星通信網等



(3) 施工現場でのネットワーク



7章 外部関係者



オンラインストレージ
オンラインサービス

【背景：建設業界】

- ・セキュリティレベルの低い
中小企業が多い
- ・系列関係が希薄
(統制が効きにくい)
- ・事業所(工事)が社外にある
- ・ネットワークで各社がつながる
- ・情報共有が必須

日建連：協力会社のセキュリティレベルの向上を重点に取り組む

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
遠藤 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
上月 章裕
山口 正志
種村 崇
仙波 幹徳