「サイバー攻撃の『加害者』にならないための第一歩」

サイバーセキュリティ
月間に伴う
情報セキュリティ強化

情報セキュリティ専門部会

2025年度建築ICTセミナー

「サイバー攻撃の『加害者』にならないための第一歩」

日建連建築ICT　TOPページ

情報セキュリティ専門部会

2025年度建築ICTセミナー

サイバーセキュリティ月間（2/1～3/18）

高市総理メッセージ

産学官民で連携

サイバー攻撃は日々発生

ランサムウェア攻撃が多発

暮らしや経済活動にも大きな影響が発生

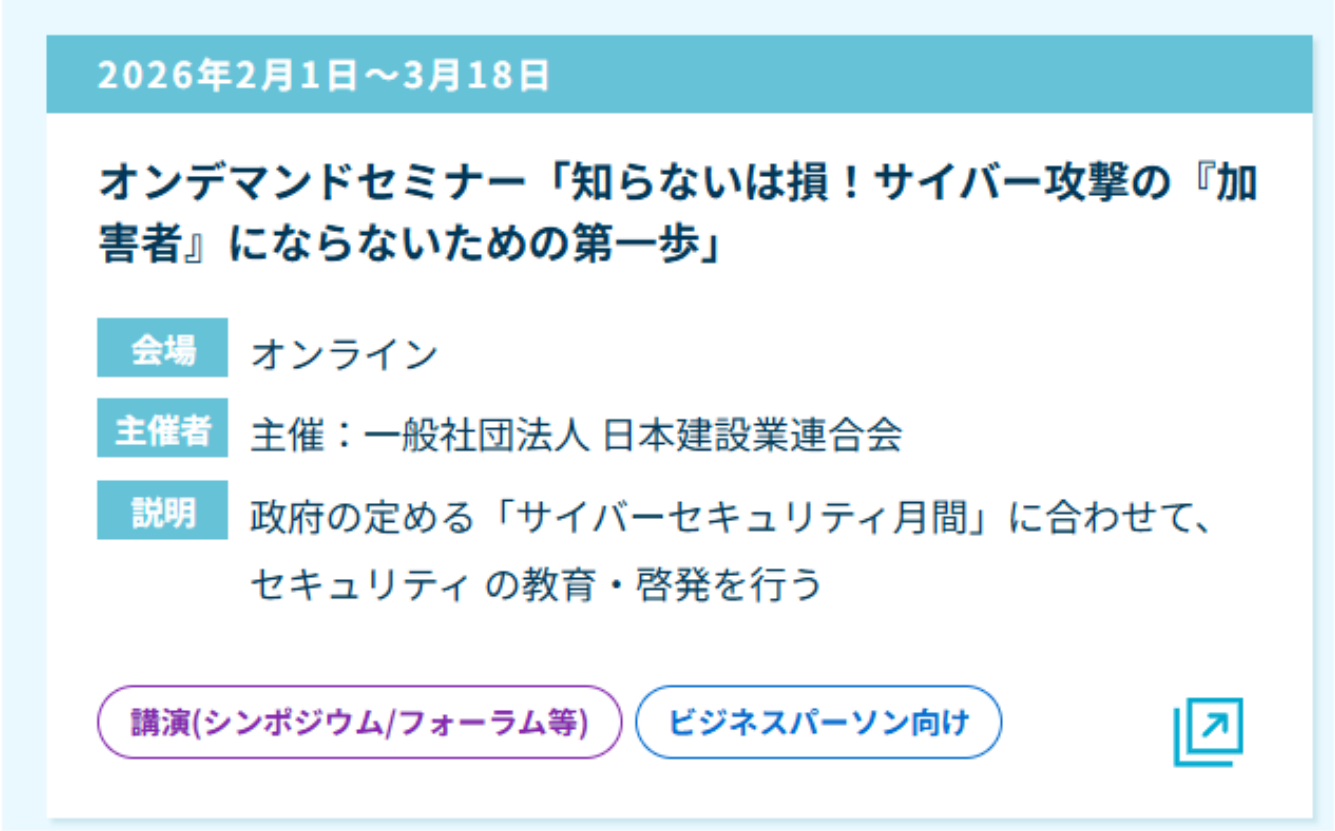
「能動的サイバ防御」を可能に

サイバーセキュリティ戦略を策定
「自由・公正かつ安全なサイバー空間」
を守る

サイバー攻撃はひとごとではない！
自分事として、全員参加で取り組む
「不審なメールのリンクは開かない」
「多要素認証の活用」

出典：首相官邸ホームページ　https://www.kantei.go.jp/jp/104/discourse/20260202message.html

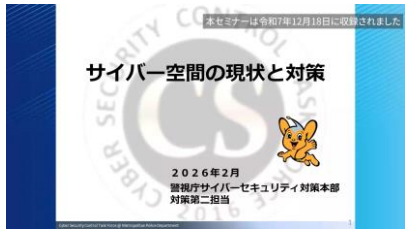
サイバーセキュリティ月間の関連イベント



https://security-portal.cyber.go.jp/cybersecuritymonth/2026/events/index.html

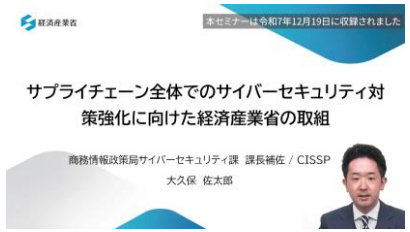
サイバーセキュリティ月間（オンデマンドセミナー）

サイバー空間の現状と対策
（警視庁サイバーセキュリティ対策本部
対策第二担当）



中小企業におけるサイバー攻撃・被害の実態と現実的対策
（大阪商工会議所　経営情報センター）

サプライチェーン全体でのサイバーセキュリティ対策強化に向けた経済産業所の取り組み
（経済産業省商務情報政策局
サイバーセキュリティ課）



2025年　情報セキュリティ１０大脅威（組織）

順位	脅威内容	2025年度	2016年移行
1	ランサムウェアによる被害	1	11年連続11回目
2	サプライチェーンの弱点を悪用した攻撃	2	8年連続 8回目
3	AIの利用をめぐるサイバーリスク	―	初選出
4	システムの脆弱性を悪用した攻撃	3	6年連続9回目
5	機密情報等を狙った標的型攻撃	5	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃	7	2年連続 2回目
7	内部不正による情報漏洩	4	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	6	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	8	2年連続 7回目
１０	ビジネスメール詐欺	6	9年連続 9回目

出展：IPA　https://www.ipa.go.jp/security/10threats/10threats2026.html

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	**7年連続10回目**
インターネット上のサービスへの不正ログイン	**11年連続11回目**
インターネットバンキングの不正利用	**4年ぶり8回目**
クレジットカード情報の不正利用	**11年連続11回目**
サポート詐欺（偽警告）による金銭被害	7年連続7回目
スマホ決済の不正利用	7年連続7回目
ネット上の誹謗・中傷・デマ	11年連続11回目
フィッシングによる個人情報等の詐取	8年連続8回目
不正アプリによるスマートフォン利用者への被害	11年連続11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	8年連続8回目

出展：IPA　https://www.ipa.go.jp/security/10threats/10threats2026.html

アサヒグループHDで発生したサイバー攻撃の概要

2025年9月29日、アサヒグループHDは「システム障害」を公式発表。原因はサイバー攻撃。
事件発生約10日前、グループ内の拠点にある**ネットワーク機器（VPNが濃厚）から侵入**。
のちに**データセンターへ到達**し、パスワード脆弱性を悪用して**管理者権限を奪取**。
そのまま**業務時間外に偵察・横展開を継続**後、**認証サーバからランサムウェアを一斉実行**。

①主な被害　**・個人情報の漏洩（約191万件）**　※顧客相談窓口・慶弔関係先・従業員・家族他
・基幹業務の停止（受注･出荷関連）

②攻　撃　者　ロシア系とみられる**ハッカー集団「Qilin」**。2022年から活動が確認され、
過去複数の日本企業を含む各国の企業が被害に遭っている。
犯行声明では、アサヒの内部文書や社員の個人情報とする画像29枚を公開、
約9300件、27ギガバイト分のファイルを盗んだと主張。

今回の攻撃に伴い、**受注や出荷等を管理する国内の物流関連システムが停止**したことで、
サプライチェーン全般に影響が発生。急遽、**手作業（紙／FAX／Excel）による代替運用**
への切替を実施。

SCS（SupplyChainSecurity）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に関する制度構築方針（案）について

経済産業省及び内閣官房国家サイバー統括室は、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業のセキュリティ対策を提示しつつ、その対策状況を可視化する仕組みの構築に向けた検討の結果として、「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に関する制度構築方針（案）」（SCS（Supply Chain Security）評価制度の構築方針（案））を公表。令和8年度（2026年度）末頃の制度開始を目指す予定

構築する評価制度（案）

成熟度の定義	★3	★4	★5［検討中※4］
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	第三者評価

出典：経済産業省　https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

●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活用する中小企業向け支援策について

経済産業省及びIPAでは、中小企業が同制度の★3及び★4を安価かつ簡便に取得できるよう、新たな支援策として「サイバーセキュリティお助け隊サービス」（新類型）を創設する予定。

お助け隊サービス（新類型）のイメージ

STEP1：課題の可視化

✓本制度の要件項目毎に中小企業の**対策状況を診断**

✓本制度の**更新時に、各対策項目の対策状況を評価**

STEP２：対象サービスの選定と対応実施

✓診断結果に基づき、以下の支援を実施

【サービス例】

✓**ITツールによる支援**
★３・★４取得に推奨されるITツールを導入

✓**ITツール以外の支援**
セキュリティポリシーやインシデント手順書の整備、セキュリティ教育など、中小企業が自助努力で達成しづらい項目を支援

STEP1・STEP2の支援サービスを一定の価格要件の下で提供

STEP3：★取得

✓ 本制度の★3もしくは★４の**項目要件をすべて充足することで★を取得**

出典：経済産業省　https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

サイバーセキュリティ月間（ポスター）

「慌てない　電話しないで、画面を閉じて！」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

「慌てない　電話しないで、画面を閉じて！」ポスター（多言語版）

※英語、中国語、タイ語、インドネシア語、ミャンマー語、ベトナム語、韓国語

推奨対象者：作業員、社員

提供元：日建連

ダウンロード

出展：日建連サイバーセキュリティ月間に伴う情報セキュリティ強化
https://www.nikkenren.com/kenchiku/ict/security/202601_cybersecurity_notification.html

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」

- 全体版（日本語）
- 全体版（英語）
- 全体版（中国語）
- 全体版（タイ語）
- 全体版（インドネシア語）
- 全体版（ミャンマー語）
- 全体版（ベトナム語）
- 全体版（韓国語）

出典：日建連HP　https://www.nikkenren.com/kenchiku/ict/security/movie.html#v3

日建連→建築→ IT-WEB →【ガイドライン・教育資料集】

ホーム ＞ 建築 ＞ 建築 - ICT WEB ＞ 情報セキュリティ ＞ 情報セキュリティに関するガイドライン・教育資料集

情報セキュリティに関するガイドライン・教育資料集

ガイドライン

› ガイドラインの位置づけ

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

教育資料集

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		
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（日本語版）
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（英語版） NEW
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（中国語版） NEW
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（タイ語版） NEW
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（インドネシア語版） NEW
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（ミャンマー語版） NEW
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（ベトナム語） NEW
動画	○	○		日建連	建設現場における情報漏えい事故例と注意ポイント（韓国語版） NEW
ポスター	○	○		日建連	慌てない　電話しないで、画面を閉じて！（日本語版） NEW
ポスター	○	○		日建連	慌てない　電話しないで、画面を閉じて！（英語版） NEW
ポスター	○	○		日建連	慌てない　電話しないで、画面を閉じて！（中国語版） NEW
ポスター	○	○		日建連	慌てない　電話しないで、画面を閉じて！（タイ語版） NEW
ポスター	○	○		日建連	慌てない　電話しないで、画面を閉じて！（インドネシア語版） NEW
ポスター	○	○		日建連	慌てない　電話しないで、画面を閉じて！（ミャンマー語版） NEW

出典：日建連HP　https://www.nikkenren.com/kenchiku/ict/security/guideline.html

安心してICTを活用するために

一人ひとりが自分事としてとらえ、全員参加のもと安心して、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

三井住友建設	仙波 幹徳	五洋建設	吉川 遵
竹中工務店	豆腐谷 洋一	清水建設	遠藤 樹
安藤ハザマ	高馬 洋一	大成建設	葛原 徹
安藤ハザマ	石津 理	東急建設	藤井 隆行
大林組	杉山 宜督	戸田建設	上月 章裕
奥村組	岸本 雅彦	フジタ	山口 正志
鹿島建設	矢口 賢一	前田建設工業	有原 敦