参考資料3

サイバーセキュリティ対策支援メニュー例

2026年5月28日

国土交通省

主なサイバーセキュリティ対策支援メニュー例

国土交通省

◆関係省庁・関係機関と連携して、サイバーセキュリティ対策の実施及び更なる対策の強化につながる支援を行っています。

セキュリティ対策水準

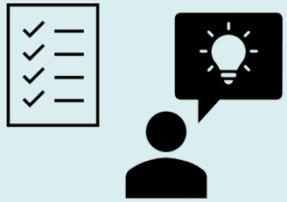
重要インフラ統一基準と分野別安全ガイドライン

- 事業分野の特性に応じたセキュリティ対策水準を明示

国土交通省

チェックリスト

- 自組織の情報セキュリティ対策の現状を確認



国土交通省

相談窓口

- セキュリティに関するご相談を幅広く受け付け

国土交通省

インシデント対処

駆けつけ支援

- サイバー攻撃の初期対応・被害拡大防止等の支援

国土交通省

脆弱性情報等提供

ASM

- オープンソース情報を収集・分析し、評価レポートを作成

国土交通省

人　材　育　成

インシデント対処研修

- CSIRT体制における連携強化とインシデント対応能力向上を目指す。

国土交通省

CYDER（実践的サイバー防御演習）

国立研究開発法人
情報通信研究機構（NICT）

中核人材育成プログラム

IPA産業サイバーセキュリティセンター（ ICSCoE ）

SNSモニタリング

- SNS投稿をモニタリングし、インシデント予兆をいち早くキャッチ

国土交通省

※上記はあくまでも一例です。この他にも支援メニューがありますので、相談窓口までお問い合わせください。

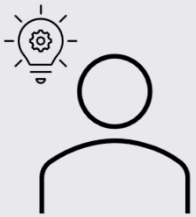
【セキュリティ対策水準】
情報セキュリティ対策の自己点検チェックリスト

国土交通省

【対象】国土交通省が所管する全ての事業者

【目的】事業者の担当者が自組織の業種や規模に応じた適切なセキュリティ対策を実施することで、自組織の情報を守り、サイバー攻撃や情報漏えいのリスクを減らす。

期待される効果

				
セキュリティ対策レベルの向上	セキュリティ対策の現状を手軽に確認	おさらいによる対策見落とし防止	セキュリティルールや対策計画策定時の参考資料として活用	定期的なセキュリティ対策見直しへの役立て

チェック項目の例

●最低限実施すべきと考えられる基本的な対策を確保するための項目
- 会社等のセキュリティルールを決め、従業員に説明していますか？
- 委託先や協力会社等のセキュリティ管理状況を定期的に確認していますか？

●より高度なセキュリティ対策を実施し、リスクを低減するための項目
- 不正アクセスを検知する仕組みを導入していますか？
- 定期的にセキュリティインシデント対応訓練を行っていますか？

※掲載先（国土交通省HP）：https://www.mlit.go.jp/sogoseisaku/jouhouka/sosei_jouhouka9999.html

【横断的な支援】
相談窓口

国土交通省

【対象】国土交通省が所管する重要インフラ事業者

- 国土交通省が所管する重要インフラ分野を対象として、
  セキュリティに関するご相談を受け付ける相談窓口を設置します。

「チェックリストに記載されている情報セキュリティ対策の改善方法を教えてほしい」、「情報セキュリティインシデントが発生したが、対応方法が分からない」、「自組織のセキュリティ対策状況を客観的に確認する方法を知りたい」など、セキュリティに関するご相談を幅広く受け付けます。

STEP 1
情報セキュリティに関する疑問、悩みごと。

STEP 2
相談窓口へ連絡

STEP 3
質問等に対する回答・助言や、適切な相談窓口の紹介など

【インシデント対処】
駆けつけ支援

国土交通省

【対象】国土交通省が所管する全ての事業者

- WEB改ざん、ランサムウェア感染など、サイバー攻撃被害が発生した際、国土交通省から専門的知見を有する職員等を派遣し、初期対応・被害拡大防止・再発防止策検討などの支援を実施。

支援内容

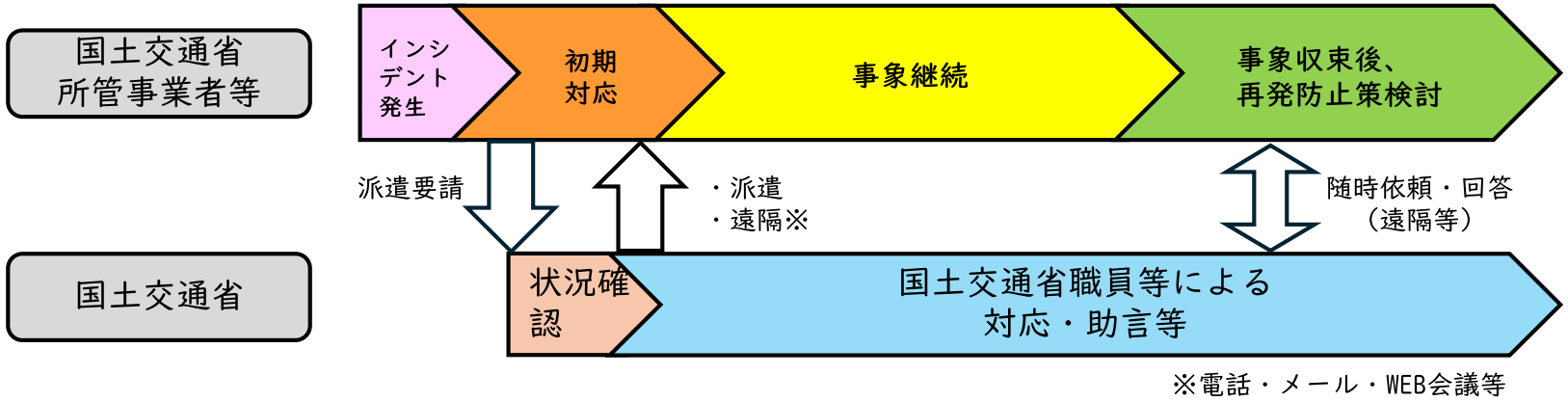
① 調査の観点や調査結果から次のアクションの判断などの助言

② 保守事業者等からの専門的な説明内容を、経営層等にわかりやすく解説するなどのフォロー

③ 事業者CSIRTに同伴して情報収集、助言

④ 収集した情報を選別・分類し、事業者CSIRTと調整した上で国土交通省へのインシデント報告等

対応例
※初期対応時に
派遣要請した想定



※電話・メール・WEB会議等

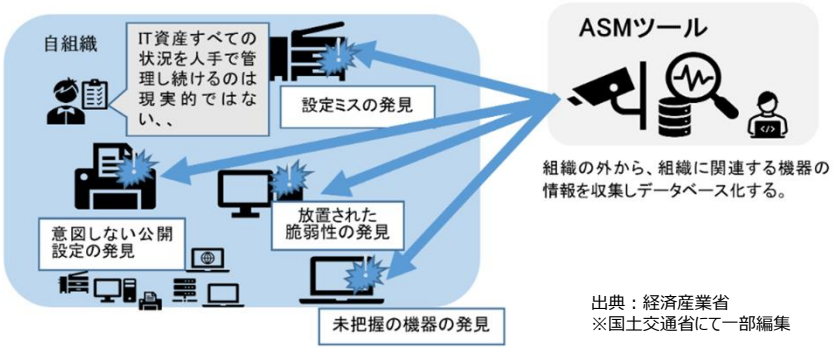
【脆弱性情報等提供】ASM

国土交通省

【対象】国土交通省が所管する重要インフラ事業者

- **オープンソース情報を収集・分析することで、所管重要インフラ事業者※1を対象としたASM※2を実施**
- **得られた情報から個別事業者の評価レポートを作成**

（参考）一般的なASM（アタックサーフェスマネジメント）の特徴とイメージ



出典：経済産業省
※国土交通省にて一部編集

※１　所管重要インフラ事業者
航空、空港、鉄道、水道、物流、港湾の6分野の事業者

※２　ASM（Attack Surface Management）
サイバー攻撃者の視点からセキュリティリスクを評価、数値化・可視化することで「攻撃されやすさ（脆弱性）」を定量的に示す。

サイバーセキュリティ対策室

- リスクレーティング実施
- 定期レポートを四半期ごとに送付し、緊急性の高い脆弱性情報等は随時送付

・レーティング結果展開
・緊急性の高いものは速やかな対策を促す

分野所管部局

- 所管分野の傾向を把握

所管重要インフラ事業者等

- セキュリティ上の弱点を把握し、事前対策の実施やレジリエンス改善を図る
- レーティング結果を経営層への説明に活用

【脆弱性情報等提供】
SNSモニタリング

国土交通省

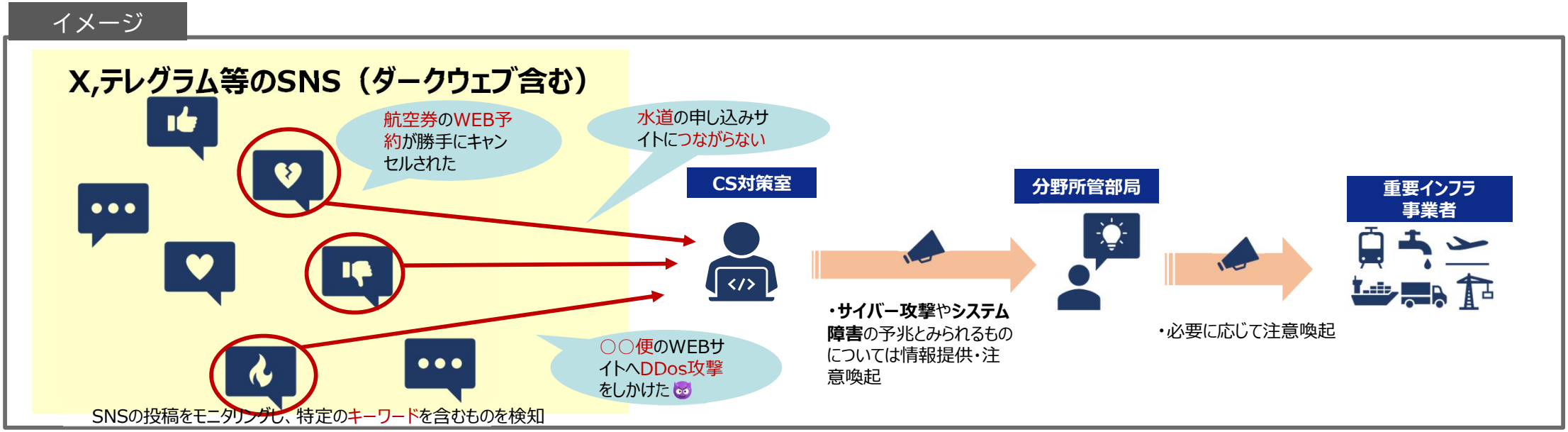
【対象】国土交通省が所管する重要インフラ事業者

- **SNS投稿をモニタリングし、インシデント予兆をいち早くキャッチ**
- **インシデント未然防止、発生時の早期対応につなげる。**

□ 国土交通省においてSNS投稿をモニタリングし、インシデントの予兆と考えられる情報を速やかに提供する

□ 所管重要インフラ事業者に関係するSNS投稿を収集し、**システム障害**や**サイバー攻撃**の予兆と推定されるものをピックアップし、国土交通省内関係者及び該当する事業者へ**共有・注意喚起**を図ることにより、サイバーセキュリティインシデントへの事前対処を促す

イメージ



【人材育成】
インシデント対処研修及び演習

国土交通省

【対象】国土交通省が所管する重要インフラ事業者

◆目的

国土交通省のCSIRT職員及びシステム担当者並びに所管重要インフラ事業者を対象として、近年巧妙化・頻発化する高度サイバー攻撃等のセキュリティリスクに備えるべく、CSIRT体制における連携強化とインシデントへの対応能力向上を目指す。

◆参加人数

国土交通省10名、重要インフラ事業者10名、計20名

◆対象者

国土交通省CSIRT職員、省内における大規模システムや社会的な影響の大きいシステム等のシステム担当者、重要インフラ事業者のセキュリティ担当者 等

◆実施時期

令和8年7月～令和8年11月

	項目名	実施形式	技術レベル
1	インシデント対応机上演習（初級）	座学・ワーク形式	初級：セキュリティ担当 1～2年目向け
2	ネットワーク・システム構成等に係る基礎知識講習	オンライン 講義形式	初級：セキュリティ担当 1～2年目向け
3	インシデント対応技術研修（ログ解析）	体験型 ハンズオン形式	中級：セキュリティ担当 2～5年目向け
4	インシデント対応技術研修（フォレンジック）	体験型 ハンズオン形式	中級：セキュリティ担当 2～5年目向け
5	インシデント対応机上演習（中級）	ロールプレイ形式	中級：セキュリティ担当 2～5年目向け

【人材育成】CYDER（実践的サイバー防御演習）〈NICTの取組〉

【対象】国の機関、地方公共団体、企業に所属する者

◆国立研究開発法人情報通信研究機構（NICT）による取組で、サイバー攻撃を受けた際の一連の対応（インシデント対応）をパソコンを操作しながらロールプレイ形式で体験できる演習。

＜2026年度実践的サイバー防御演習「CYDER」について＞

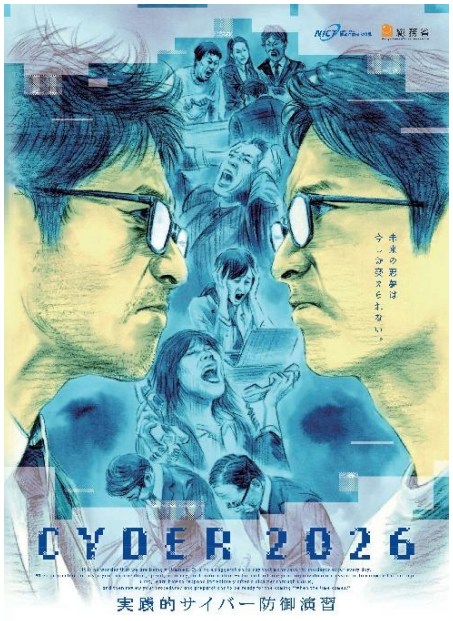
■ 集合演習

Aコース（7月～9月開催分）

- 国の機関・地方公共団体：申込受付中
- 民間企業：6月2日（火）申込受付開始予定

■ プレCYDER

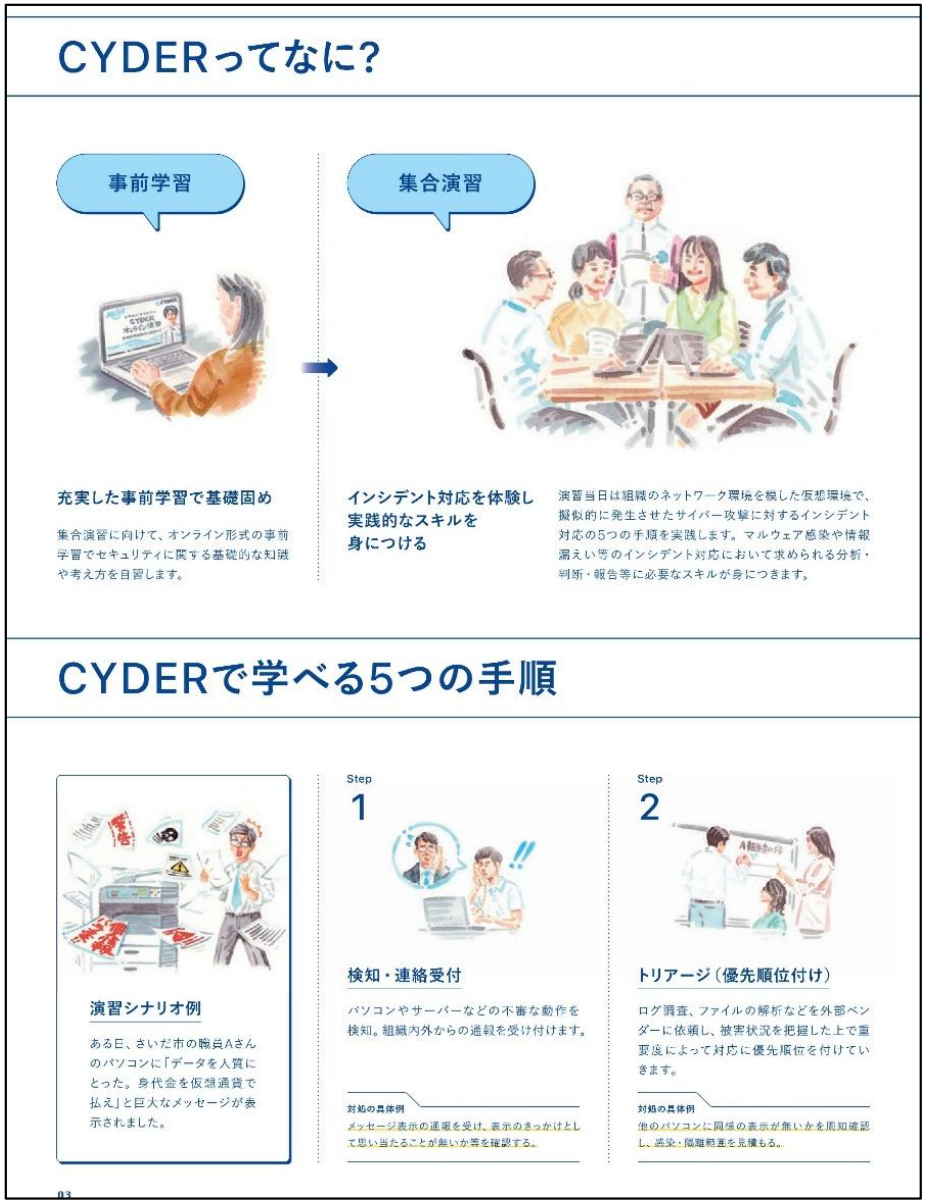
- ケーススタディ1期／ドリル1期：5月19日（火）開講・申込受付中



コースの種類

コース名		演習形式	レベル	主な対象組織	期間※2		開催エリア
					事前学習	演習	
CYDER	Aコース	集合対面	初級	全ての組織	2～5時間程度	1日間	全国47都道府県
	Bコース※1	集合対面	中級	全ての組織		1日間	東京・名古屋・大阪・福岡
	Cコース	集合対面	準上級	全ての組織		2日間	東京・大阪
プレCYDER	ケーススタディ	eラーニング	入門	全ての組織	なし	2～3時間程度	オンライン
	ドリル	eラーニング	入門	全ての組織	なし	5時間程度	オンライン

［※1］Bコースでは、省庁・企業の一般的なシステム環境を模した仮想環境で演習を行います。なお、地方公共団体の方にも取り組みやすいよう、三層の対策の考え方に基づくα'モデル等を参照しつつ演習内容を構成しています。ご所属の組織に関係なくご受講可能です。［※2］申込期限について：（集合演習）Webから申し込む場合の期限は開催日の5営業日前までです。以降に申込をご希望の方は、事務局までお問い合わせください。受講席数に限りがございますので、早めのお申し込みをお勧めします。（プレCYDER）演習当日でもお申し込みいただけます。



※「CYDER2026」ホームページ及びパンフレットから抜粋（https://cyder.nict.go.jp/）（https://cyder.nict.go.jp/assets/pdf/cyder2026pamphlet.pdf）

【人材育成】中核人材育成プログラム〈IPAの取組〉

【対象】企業に所属する者

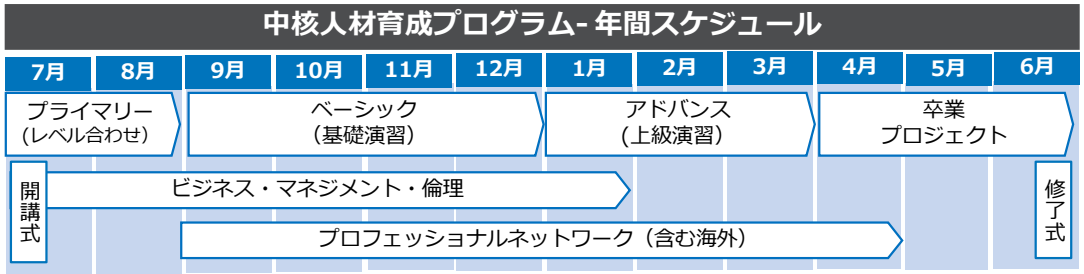
◆ IPA産業サイバーセキュリティセンター（ICSCoE）による取組で、社会インフラ・産業基盤のサイバーセキュリティ対策の強化をテーマに、テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ。 ※2026年度は募集終了。

IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□ １年を通じた集中トレーニング「中核人材育成プログラム」

□ 電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人、第９期：55人）



- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

→ **現場を指揮・指導するリーダーを育成**

□ 米・英・仏等の海外とも協調したトレーニングを実施

➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

※経産省「第5回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化）半導体産業サブワーキンググループ」資料から抜粋
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_semiconductor/pdf/005_s03_00.pdf）