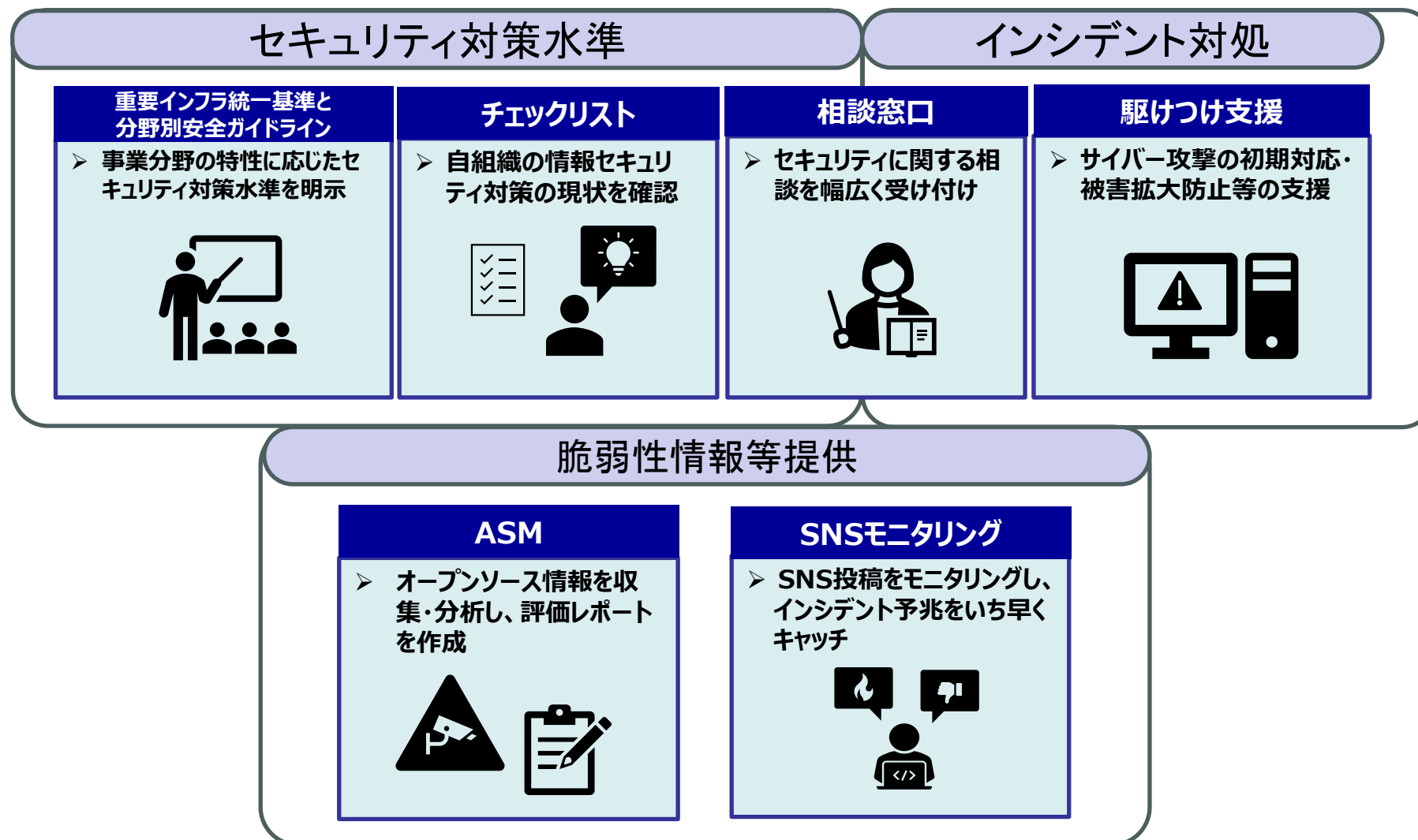


主なサイバーセキュリティ対策支援等メニュー例

◆国土交通省では、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。

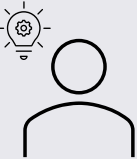


【セキュリティ対策水準】 情報セキュリティ対策の自己点検チェックリスト

【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

【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事業者を対象として、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。

「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。



【インシデント対処】

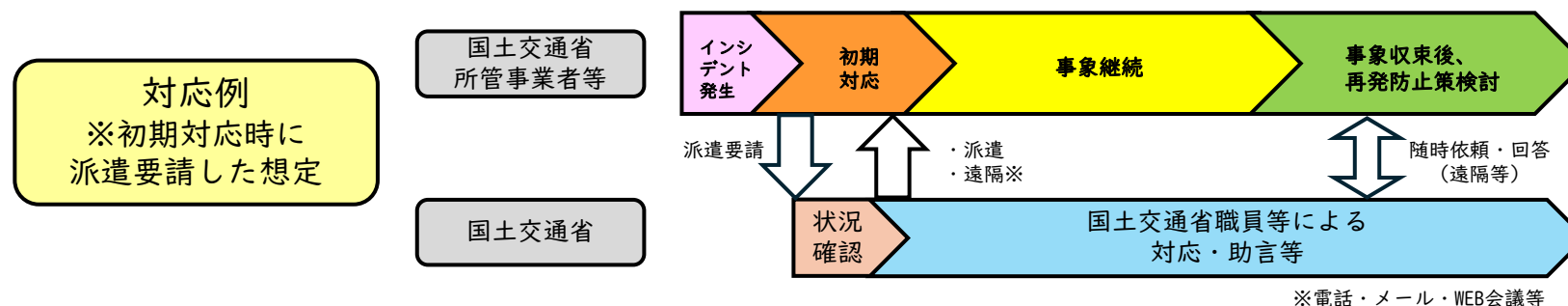
駆けつけ支援

【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

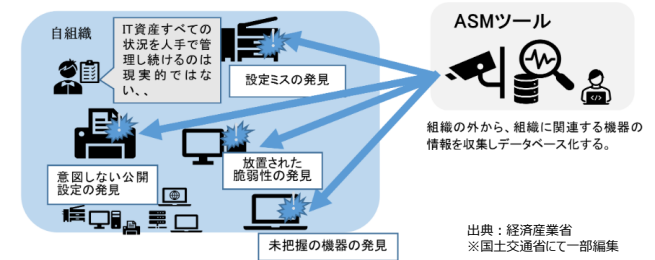
※1 所管重要インフラ事業者

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。

(参考) 一般的なASM (アタックスurfaceマネジメント) の特徴とイメージ



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



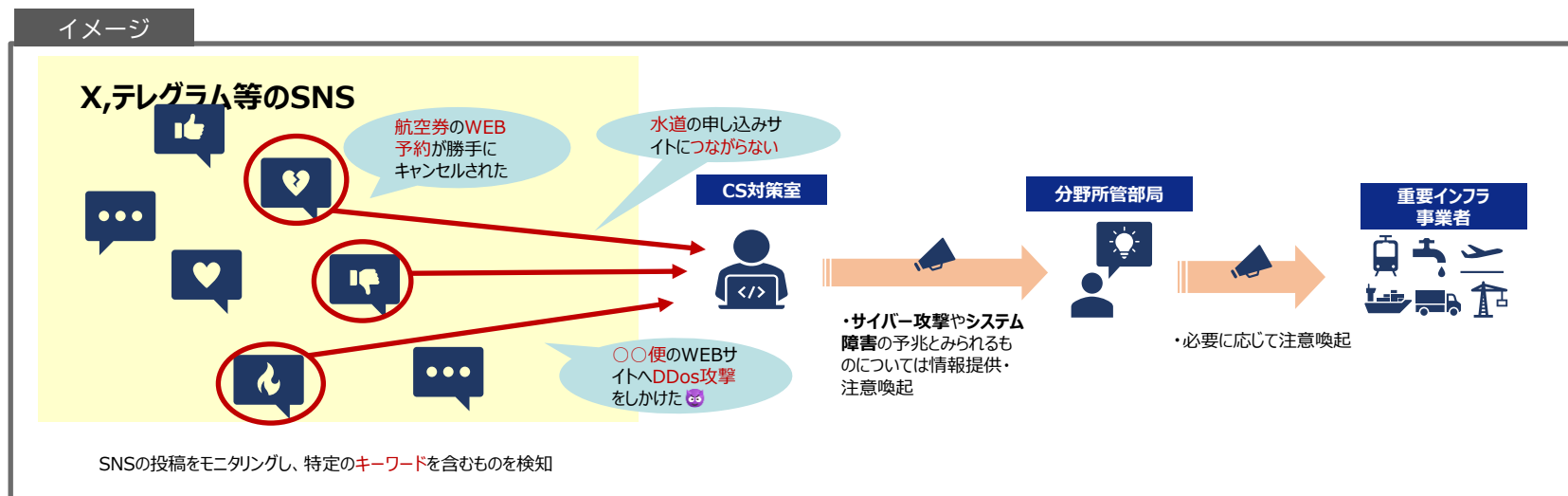
- セキュリティ上の弱点を把握し、事前対策の実施やレジリエンス改善を図る
- レーティング結果を経営層への説明に活用

SNSモニタリング

【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



【参考】他省庁等の関連情報

- 個人情報保護委員会：
大規模な漏えい等事案を踏まえた対応について（注意喚起）
https://www.ppc.go.jp/files/pdf/261007_houdou.pdf
- 警察庁：
サイバー警察局便りR8Vol.19「情報流出に注意」（R8.10.8）
https://www.npa.go.jp/bureau/cyber/pdf/R8_Vol.19cpal.pdf
- 経済産業省、独立行政法人情報処理推進機構：
 - ・ 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（SCS評価制度）
<https://www.ipa.go.jp/security/scs/index.html>
 - ・ サイバーセキュリティお助け隊サービス制度
<https://www.ipa.go.jp/security/sme/otasuketai/index.html>
 - ・ サイバーセキュリティお助け隊サービス（新類型）実証事業
<https://www.ipa.go.jp/security/sme/otasuke-scs.html>