事　務　連　絡
令和８年10月14日

都道府県旅行業担当課　御中

観光庁参事官（旅行振興）

不正アクセスによる漏えい等の事案を踏まえた対応について（依頼）

内閣官房国家サイバー統括室（NCO）では、ウェブシステムに係る脆弱性の悪用、サプライチェーンを通じた侵害、堅牢さを欠くデータ管理などにより、大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案を複数確認しております。

こうした状況を踏まえ、内閣官房国家サイバー統括室において別添の通り、不正アクセスによる漏えい等の事案を踏まえた注意喚起が取りまとめられました。

貴都道府県におかれましては、上記趣旨をご理解いただくとともに、貴都道府県登録の旅行業者等に対して、上記及び別添の内容を周知いただきますようお願いいたします。

なお、周知にあたっては以下３点にご留意ください。

・本注意喚起においては、事業者の情報セキュリティ担当者等実務層のみならず、経営層へのメッセージも含まれております。それぞれの経営層にもお伝えいただきたい旨、併せて周知してください。
・サイバー攻撃の被害にあった際は、更なる攻撃被害の拡大を防ぐため、当該サイバー攻撃に関する情報を登録行政庁に速やかに共有いただけますようお願いします。
・政府で実施している事業者向けサイバーセキュリティ対策の資料も添付しておりますので参考にしていただければと思います。（一部、対象分野限定の支援メニューもあります）
（別添「主なサイバーセキュリティ対策支援等メニュー例」）

■添付資料
・【別添１】（内閣官房国家サイバー統括室通知）不正アクセスによる漏えい等の事案を踏まえた対応について
・【別添２】主なサイバーセキュリティ対策支援等メニュー例

不正アクセスによる漏えい等の事案を踏まえた対応について

２０２６年１０月９日
内閣官房国家サイバー統括室

国家サイバー統括室では、ウェブシステムに係る脆弱性の悪用、サプライチェーンを通じた侵害、堅牢さを欠くデータ管理などにより、大量の個人情報を取り扱う事業者等の情報システムが不正アクセスにより侵入され、個人情報を含むデータが窃取される事案を複数確認しております。

こうした状況を踏まえ、特に、大量の個人情報を取り扱う事業者や機微な情報を取り扱う事業者等におかれましては、以下にお示しする主な対策のポイントをご参照いただき、より一層の対策の徹底を速やかに検討いただくようお願いいたします。

１．ウェブシステム等の適切な管理

ウェブシステムは、企業活動や顧客サービスの基盤として不可欠な存在となっています。一方で、インターネットに公開されているシステムは特に攻撃の対象となりやすいため、「いつ攻撃を受けてもおかしくない」という前提で対策を講じることが重要です。

（１）脆弱性の適切な管理

脆弱性情報が公表されると、攻撃者は短期間のうちに悪用を開始する場合があります。修正プログラムの適用を後回しにせず、インターネットに公開されていない内部のサーバ等も含め、リスクを適切に判断し、計画的かつ迅速に対応することが求められます。

- OS、ミドルウェア、CMS（コンテンツ・マネジメント・システム）、アプリケーション等のセキュリティパッチやアップデートを速やかに適用する
- サポートが終了している製品・バージョンを利用しない
- 利用していないシステムや機能は停止・削除する
- 定期的に脆弱性診断等を実施する
- 不要なポート、プロトコル、サービス等を無効化する

（２）アカウント管理・認証

適切な認証対策により、不正アクセスのリスクを大幅に低減させることが可能です。

- 多要素認証（MFA）を導入する
- 推測されやすいパスワードの使用を禁止する
- 管理者アカウントの利用者、アクセス権を必要最小限にする
- 退職者、異動者や利用されていないもの等の不要なアカウントを速やかに無効化する

（3）レジリエンスの向上

侵入を完全に防ぐことは困難です。不審な挙動の早期発見と迅速な対応が被害発生及び拡大の防止につながります。

・ログを適切に取得・保管する
・不審な通信や大量のアクセスを監視する
・侵入検知・防御システムを活用し、パターンファイル等を定期的に更新する
・外部からの異常な認証試行を把握する
・事業継続計画等にサイバーセキュリティを組み入れる
・インシデントが起きた場合の対応態勢を整備する

2．サプライチェーンを通じた侵害への対策

サイバー攻撃への対策は、自社システムのみを対象として考えるのではなく、個人情報や業務情報を預ける委託先企業等を含むサプライチェーン全体で安全性を確保する観点で取り組むことが重要です。攻撃者は、比較的防御が弱い委託先企業等を足掛かりとして侵入し、その後、標的となる企業へアクセスを拡大する手口を用いることがあります。そのため、「委託先企業と共に管理する」という認識の下で、適切な安全管理措置を講じることが求められます。

（1）委託先企業等のセキュリティ対策状況の把握

・委託先等の情報セキュリティ方針、管理体制や委託先等との役割分担・責任分界を確認する
・個人情報や業務情報の取扱状況を定期的に点検する
・セキュリティ認証の取得状況や監査結果を確認する
・再委託先を含む管理状況を把握する
・契約締結時だけでなく、継続的に確認を行う

（2）委託契約におけるセキュリティ要件の明確化

・情報の取扱方法を明確に定める
・アクセス権管理やログ管理の実施を求める
・不正アクセスや漏えいが発生した場合の報告義務を規定する
・インシデント発生時の委託先との連携体制を整備する

（3）情報共有範囲の適正化

・委託先へ提供する個人情報や業務情報を必要最小限とする
・業務終了後の委託先でのデータ削除を徹底する
・委託先に付与するアクセス権を適切に管理する

（4）サプライチェーン全体のリスクマネジメント

・重要な取引先や委託先を洗い出す
・サプライチェーンを含めた情報資産の流れを可視化する
・サプライチェーン上の重要な依存関係を把握する
・定期的にリスク評価を実施する

3．データの適切な管理

企業が保有する個人情報や業務情報は、重要な経営資産です。一方で、不必要な情報の保有や、アクセス権限の管理や保管方法が不十分である場合には、不正アクセスを受けた際に被害が大規模化するおそれがあります。また、近年の攻撃者は、窃取した情報を公開すると脅迫したり、不正に売買するなど、情報そのものを標的とする傾向を強めています。そのため、「保有する情報資産を守る」という視点に立った安全管理措置が求められております。

（1）保有する情報資産の適切な管理

どのような情報資産を保有しているのか把握できていなければ、適切な保護措置を講じることはできません。まずは、自社が保有する情報資産の全体像を把握することが重要です。

・個人情報や業務情報の所在や管理者を把握する
・重要な情報資産を分類し、管理対象を明確にする
・利用目的や保存期間を明確にする
・定期的に情報資産の棚卸しを実施する

（2）保有情報の最小化

万が一情報漏えいが発生した場合でも、保有する情報が少なければ被害の拡大を抑えることが可能です。

・利用目的を終えた情報は速やかに削除する
・法令上の保存期間を経過した情報は適切に廃棄する

（3）適切なアカウント管理・アクセス制御

必要以上の権限が付与されている場合、不正アクセス時に大量の情報が一度に取得されるおそれがあります。

・業務上必要な者のみにアクセスを許可する
・閲覧権限と更新権限を適切に分離する
・管理者権限の付与を必要最小限とする
・定期的にアカウントや権限設定を確認する

（4）データ保護の徹底

情報が窃取された場合であっても、適切な保護措置が講じられていれば悪用のリスクを低減することができます。

・保存データを暗号化する
・通信経路を暗号化する
・パスワードや認証情報を平文で保存しない
・外部電磁的記録媒体の利用やデータ保存等に関するルールを整備する
・バックアップデータについても適切に保護する
・クラウドサービスを利用する場合は、サービス仕様を理解し、保存領域やデータベース等の公開設定及びアクセス権限設定をよく確認する

（５）ログ取得・監視・分析の強化

不正アクセスを早期に発見し、被害範囲を迅速に特定するためには、適切な監視・分析体制が不可欠です。また、不正侵入される事案が複数確認されている状況に鑑み、不審な通信や大量のアクセスの痕跡がないか、アクセスログ等の点検・分析を実施することを推奨します。

・個人情報や業務情報へのアクセス記録を取得する
・不審なアクセスや大量データの取得を監視する
・ログを一定期間保管する
・異常を検知した場合の対応態勢を整備する

サイバー攻撃による被害は、もはや情報システム部門だけの問題ではありません。不正アクセスによって個人情報や業務情報が流出した場合、事業停止、顧客対応など、多方面にわたる経営リスクへと発展する可能性があります。AI の悪用を含むサイバー攻撃の手法が高度化・巧妙化する中、経営層の皆様におかれましては、サイバーセキュリティ対策を経営課題と位置づけ、必要な投資や人的体制整備を含む対策の強化をお願いいたします。

また、被害にあわれた組織にあっては、更なる攻撃被害の拡大を防ぐため、サイバー攻撃に関する技術的な情報を、内閣官房国家サイバー統括室や所管省庁、専門機関等に速やかに共有いただけますよう、何卒ご協力をお願いいたします。

（参考資料）

・重要インフラのサイバーセキュリティ対策のための統一基準
・重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン
・サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集
・サイバーセキュリティ人材フレームワーク 2026

以上

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

◆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

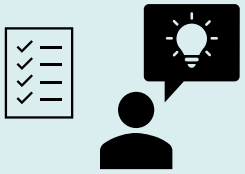
重要インフラ統一基準と分野別安全ガイドライン

- 事業分野の特性に応じたセキュリティ対策水準を明示



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



インシデント対処

相談窓口

- セキュリティに関する相談を幅広く受け付け



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



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



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

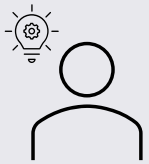


【セキュリティ対策水準】
情報セキュリティ対策の自己点検チェックリスト

【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

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

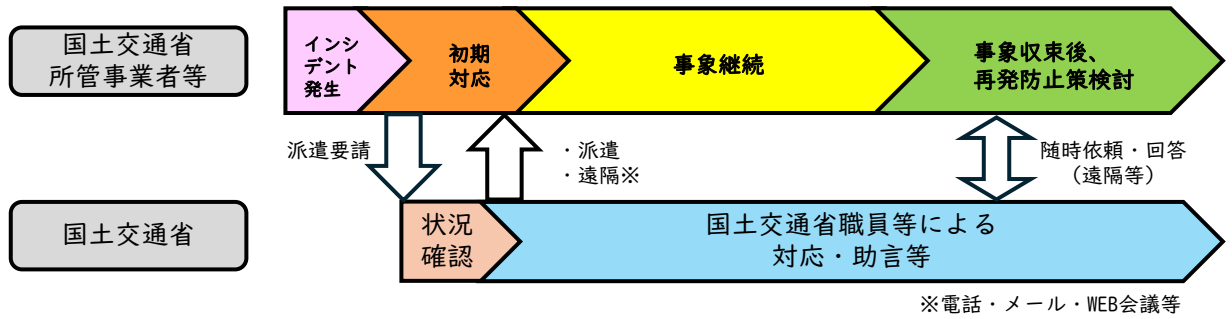
① 調査の観点や調査結果から次のアクションの判断などの助言

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



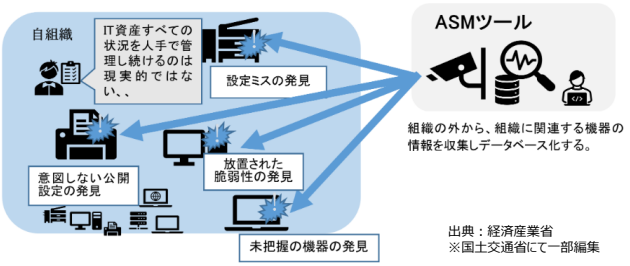
【脆弱性情報等提供】
ASM

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

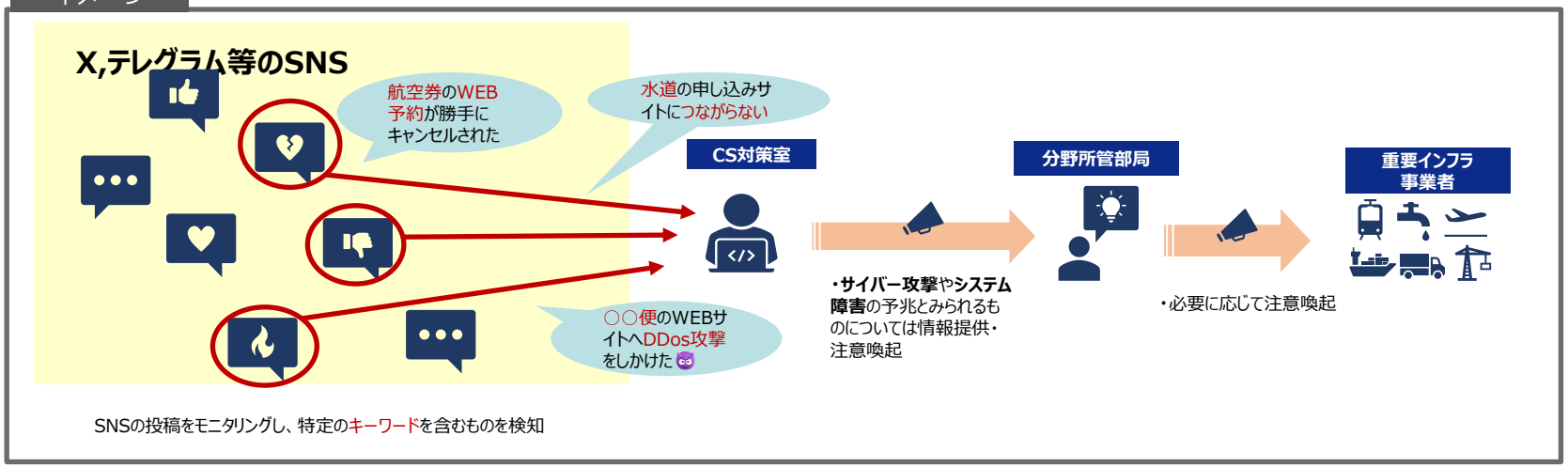
【対象】国土交通省が所管する重要インフラ事業者

- **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



【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