商 地 第 ２０９ 号
令和８年 10 月 20 日

各関係団体の長　様

静岡県サイバーセキュリティ戦略本部長
（静岡県副知事　平木　省）

情報セキュリティ対策の徹底について（注意喚起）

日頃から本県の行政運営に御理解と御協力を賜り、厚く御礼申し上げます。

現在、企業等に対する不正アクセスにより大量の個人情報の漏えいが疑われる事案が相次いで発生しています。

サイバー攻撃や不正アクセスによる被害は、個人情報の漏えいのみならず、業務の停止、停滞につながるおそれがあることから、継続して情報セキュリティ対策に取り組むことが重要です。

つきましては、令和８年 10 月 16 日に緊急開催されました静岡県サイバーセキュリティ戦略本部会議の抜粋資料及び、内閣官房国家サイバー統括室からの注意喚起を下記のとおり送付しますので、貴団体におかれましては、内容を御覧いただき、保守運用等事業者と連携の上、必要な情報セキュリティ対策を改めて徹底いただきますようお願いいたします。

また、所属会員様にもこの旨周知いただきますよう、重ねてお願い申し上げます。

記

１　添付資料

・別添１「令和８年度第１回静岡県サイバーセキュリティ戦略本部会議資料」
（抜粋）

・別添２「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」
（内閣官房国家サイバー統括室）

２　その他

サイバーセキュリティ対策に関する相談窓口は、別添１の資料内に記載がありますので、参考にしてください。

担　　当　　静岡県経済産業部地域産業課
電話番号　　０５４－２２１－２５２０

令和８年度 第１回静岡県サイバーセキュリティ戦略本部会議

日 時　令和８年10月16日（金）
午前11時～11時30分
会 場　東館５階特別会議室

次　　第

１　開　　会

２　議　　題

(1) サイバー攻撃（不正アクセス等）の状況　【資料１】

(2) 国の注意喚起を踏まえた事業者・県民への対応について【資料２】

(3) 県庁内におけるサイバーセキュリティ対策の強化　【資料３】

３　本部長指示事項

４　閉　　会

【事業者のみなさまへ】不正アクセスによる漏えい等の事案を踏まえた対応【概要】 資料２

【内閣官房国家サイバー統括室からの注意喚起（令和８年10月９日）】

背景

システムの脆弱性の悪用、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により、事業者等の情報システムが不正アクセスを受け、大量の個人情報を含むデータ窃取が複数発生した。

趣旨

大量の個人情報や機微な情報を取り扱う事業者は、主な対策のポイントを参照し、一層の対策を徹底。

※サイバーセキュリティは情報部門の問題ではない。
経営課題として投資・体制を含めた対策が必要

【主な対応のポイント】

1 ウェブシステム等の適切な管理

(1) 脆弱性の適切な管理

ＯＳ、アプリケーション等のセキュリティパッチ適用
サポートが終了した製品・バージョンの利用を禁止

(2) アカウント管理・認証

多要素認証（MFA）の導入
推測されやすいパスワードの使用禁止

(3) レジリエンスの向上

ログの適切な取得・保管
不審な通信や大量アクセスの監視

2 サプライチェーンを通じた侵害への対策

(1) 委託先企業等のセキュリティ対策状況の把握

個人情報・業務情報の取扱状況の定期的な点検(含再委託)

(2) 委託契約におけるセキュリティ要件の明確化

アクセス権管理やログ管理の実施を求める。
インシデント発生時の委託先との連携体制整備

(3) 情報共有範囲の適正化

提供情報を最小限にし、業務終了後のデータ削除を徹底

(4) サプライチェーン全体のリスクマネジメント

取引先や委託先を洗い出し、情報資産の流れを可視化

3 データの適切な管理

(1) 保有する情報資産の適切な管理

個人情報や業務情報の所在や管理者の把握
利用目的や保存期間の明確化

(2) 保有情報の最小化

利用目的を終えた情報の速やかな削除
法令上の保存期間を経過した情報の適切な廃棄

(3) 適切なアカウント管理・アクセス制御

アクセスを必要な者に限る(管理者権限の付与は最小限に)。

(4) データ保護の徹底

保存データ・通信経路の暗号化、バックアップデータの保護

(5) ログ取得・監視・分析の強化

アクセス記録の取得
不審なアクセスや大量データの取得の監視

※ 内閣官房国家サイバー統括室の注意喚起資料を元に、静岡県が作成。 詳細は、国家サイバー統括室ＨＰを参照

【県民のみなさまへ】情報漏えい事案の二次被害を防ぐ対応

【デジタル大臣記者会見（令和８年10月６日）を元に、静岡県が作成】

背景

企業等を標的とした不正アクセスが相次ぎ、大量の個人情報が流出する事案が発生しています。
情報が流出すると、**なりすましや不正送金、詐欺等の二次被害**につながるおそれがあります。

【二次被害を防ぐ主な対応】

１　パスワードの適切な管理

同じパスワードを複数のサービスで利用すると、ひとつのサービスから情報流出した場合に、他のサービスでも不正ログインされる危険があります。

対応

- **利用するサービスごとに異なるパスワードを設定する。**
  （パスワードを使い回さない。）

２　多要素認証の利用

スマートフォン認証やワンタイムパスワードなどの多要素認証を設定することで、不正なログインを防止できる可能性が高くなります。

対応

- **スマートフォンのパスキーを設定する。**
- **ワンタイムパスワードを利用する。**

３　不審なメール等への注意

実在する企業や行政機関を装ったメールやSMSによって、IDやパスワード等を盗み取る、「フィッシング」が増加しています。

対応

- **メールやＳＭＳに記載されたリンク（ＵＲＬ）を安易にクリックしない。**
- **公式ウェブサイトや公式のアプリからアクセスする。**

※ デジタル大臣記者会見（１０月６日）を元に、静岡県が作成。詳細は、デジタル庁ＨＰを参照

※家庭や個人でできる対策はＩＰＡホームページ「情報セキュリティ10大脅威 2026個人編」や「ここからセキュリティ！」を参照
https://www.ipa.go.jp/security/10threats/10threats2026.html 、 https://www.ipa.go.jp/security/kokokara/measure/

【各部局への依頼】
事業者や県民のみなさまへのサイバーセキュリティ対策の徹底を周知

1 外郭団体や、関係する団体等を通じた事業者への注意喚起

・国家サイバー統括室からの注意喚起について、所管する外郭団体や、関係する団体等を通じて県内事業者に広く周知してください。

2 県民への周知

・県民に対し、県ホームページや公式ＳＮＳ等で、情報漏えいの二次被害を防ぐ対応を周知します。各部局が持つ県民（個人、家庭等）へのチャネルを使った情報発信をお願いします。

（参考）事業者から対応等に関する相談があった場合の窓口

区分	相談先	備考
情報セキュリティに関する一般的な相談	独立行政法人情報処理推進機構（ＩＰＡ） 企業組織向けサイバーセキュリティ相談窓口 https://www.ipa.go.jp/security/support/soudan.html	中小企業などにおける、情報セキュリティ対策ガイドラインや各種支援ツール・支援施策などを御案内します。
不正アクセス等の被害を受けた場合		初動対応に関する相談として、応急措置案の助言、専門業者や報告先等の紹介をします。
	警察庁ＨＰサイバー事案に関する通報(電子申請) https://www.npa.go.jp/bureau/cyber/soudan.html 緊急の場合は最寄りの警察署	都道府県警察に対し、サイバー事案に関する通報を行うもの。被害に遭った具体的な事実の通知を伴う場合に御利用ください。
被害を受けた可能性がある場合	警察相談専用電話（＃９１１０）	被害を受けた可能性がある場合や、警察へ相談したい場合に御利用ください。