

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

【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/>