



資料3

# 情報セキュリティ対策の徹底

企画部デジタル改革課

昨今の情報漏えい等を踏まえ、各所属において、改めて組織、人的、物理的、技術的な面から総合的な情報資産の安全管理対策を講じるとともに、外部委託事業者に対しても、県と同様の安全管理対策が確保されるよう指導・監督を徹底する。

## 再発防止のための緊急対応

日付	対応
10月22日（水）	広報広聴課より、県広報Xに係るインシデント報告
10月23日（木）	地域経済課にて、はばタンPay+に係るシステムトラブルを公表
10月27日（月）	<b>副知事通知を発出</b> 各所属に対して、外部委託事業者の監督、公式SNSアカウントの運用、ヒューマンエラーの防止を中心とした総点検を指示
10月31日（金）	<b>政策会議を開催（部長・県民局長等への注意喚起）</b> 副知事通知の内容を改めて共有するとともに、再発防止の徹底とその具体策を指示
11月13日（木）	<b>情報セキュリティ研修の追加実施を指示</b> 例年実施している情報セキュリティ研修（8月15日より順次実施）に加えて、管理職が主体となり、所属単位で全職員を対象とした職場研修の実施を指示（ <b>12月中旬に実施</b> ） → 研修教材や説明ポイント等を提供  <b>情報管理チェックシートに基づく総点検を指示</b> 各所属に対して、過去のインシデント事案等も踏まえた高リスク項目を網羅したチェックシートを配布し、総点検を指示（ <b>12月中旬に報告</b> ）

# 主な対策強化の概要

## 1 外部委託事業者の監督

- ▶ 情報システムの開発・保守運用や個人情報取扱事務を外部委託する場合、契約において「県情報セキュリティ対策指針」等の遵守（管理体制の報告、再委託における書面承認など）を義務付けていることから、改めて既存ルールの徹底を図る。
- ▶ (拡) 個人情報を取り扱う情報システムについて、調達時等に、外部委託事業者に対する動作確認テストの実施状況報告を徹底するなど、所管課による指導・監督を強化する。

## 2 SNSアカウントの適切な管理

- ▶ 各所属において、県公式SNSアカウントの運用状況（パスワードの推定困難度、変更状況など）の総点検を実施する。  
(デジタル改革課において、今後の運用に関する技術的アドバイスを適宜実施中)

## 3 ヒューマンエラーに起因する情報漏えいの防止

- ▶ ヒューマンエラーに起因する事例が散見されることから、各所属において、現行の業務執行体制の総点検を実施する。
- ▶ (拡) 例年実施している情報セキュリティ研修に加えて、管理職が主体となり、**所属単位で全職員を対象とした職場研修**を実施することで、再発防止の意識を徹底する。
- ▶ (新) 今後発生する事案については、所属や職員の属性を伏せた上で、**発生の都度、全職員に周知**し、注意喚起を行う。