情報セキュリティ対策の強化

資料2

日本年金機構における不正アクセスによる情報流出事案を踏まえ、日本年金機構をはじめ、厚生労働省及び関係機関の情報セキュリティ対策の一層の強化を図り、安全・安心で国民に信頼されるシステム構築に向けた取組を進める。

情報セキュリティ対策強化の４つの視点

組織、ヒト、ルール、システムの観点から、それぞれ対策を強化

組織的対策 （体制の強化）	人的対策 （意識改革、人材育成）	業務運営対策 （ルールの見直し、徹底）	技術的対策 （システムの強化）
• セキュリティ対策の専門性や即応性向上のための組織強化	• 情報セキュリティ教育の充実 • 実践的なセキュリティ訓練の実施 • 専門人材の確保	• セキュリティポリシーやインシデント対処手順書等の見直し	• 標的型攻撃に対する多重防御の取組 • インターネット接続環境下での情報取扱の厳格化

主な概算要求事項　（約62億円）

厚生労働省・関係機関

■高度な標的型攻撃を想定した入口・内部・出口のセキュリティ強化対策
■厚生労働省CSIRT（Computer Security Incident　Response Team）の体制強化
■個人情報をインターネット環境に置かないためのシステム上の措置
■標的型攻撃に対する実践的訓練の実施
■厚生労働省が保有するシステム及び所管法人等に対するセキュリティ監査の実施

日本年金機構

■高度な標的型攻撃を想定した入口・内部・出口のセキュリティ強化対策
■機構版CSIRT（Computer Security Incident Response Team）の創設
■個人情報をインターネット環境に置かないためのシステム上の措置
■標的型攻撃に対する実践的訓練の実施
■セキュリティ監査の実施

※政府全体の方針を踏まえて、更に検討