日本年金機構
平成27年10月27日

日本年金機構情報管理対策本部について

○ 不正アクセスによる情報流出事案に関する検証・調査結果及び厚生労働省からの業務改善命令等を踏まえ、情報セキュリティ対策を一元的に管理することで、リスク管理や情報セキュリティに関する機構全体のガバナンスの強化を図るため、理事長を本部長とした「日本年金機構情報管理対策本部」を10月１日に設置。

○ 情報管理対策本部の体制と主な所掌事務は別紙１のとおり。

○ 具体的なセキュリティ対策等について、サイバーセキュリティ基本法第27条第3項に基づく勧告（H27.9.11NISC）、情報セキュリティ強化等に向けた組織・業務改革（H27.9.18厚生労働省）等を踏まえ、検討を進めている（別紙２）。

○ 情報管理対策本部における検討内容については、再発防止策の推進体制等の具体的な内容をNISCに報告するとともに、平成27年12月初旬までに厚生労働省へ提出する改善計画に反映させる予定。

別紙1

日本年金機構情報管理対策本部の概要

- 理事長を本部長とする情報管理対策本部の下で情報セキュリティ対策を一元的に管理することで、リスク管理や情報セキュリティに関する機構全体のガバナンスの強化を図る。

理事長
副理事長

最高情報セキュリティアドバイザー
（外部有識者）※来年度設置予定

情報管理対策本部
※本部長：理事長

（情報管理対策本部の主な所掌事務）
① 機構が管理する個人情報の保護・管理
② 文書管理に係る企画・指示
③ 情報セキュリティに関する研修及び訓練内容の決定、成果の評価
④ 機構の情報資産のリスク管理方針の策定
⑤ 情報セキュリティに係る諸規程・手順書等の整備
⑥ 情報セキュリティに係る緊急時の組織の対応方針の決定及び対応

情報管理対策室
※ 情報管理対策本部の実行部隊として3グループ体制で対応

情報管理G
- 情報管理対策本部の事務局
- 共有ファイル・文書等の管理・個人情報保護
- 情報セキュリティ関係の教育・訓練

情報リスク分析G
- リスクアセスメント調査の実施・分析・評価
- 規程・手順書等の整備・運用・指導

機構CSIRT

インシデント対策G
（平時）
脆弱性調査、情報収集、自己点検、セキュリティ監査
（有事）
発生事案の調査・分析・対応指示

支援要員
（他部署）
※ 事案発生時に招集

監視・検知報告 → 運用・保守ベンダー（外部委託）

監査報告 情報提供 → セキュリティベンダー（外部委託）
※ 来年度契約予定。それまでは、支援業者による職員支援

連携 → NISC 厚生労働省 他

連携

各部情報セキュリティ責任者

日本年金機構における情報セキュリティ対策の取組み状況①

別紙２

1. 体制整備

NISC勧告の内容	主要事項	方針	取組み状況
○すべての役職員の情報セキュリティに関する役割・責任・権限を明確にするとともに、組織の一体性を確保し、実効性のある情報セキュリティ対策を実現するための体制を構築する。 ○機構において、CSIRTを速やかに組織する。	情報管理対策本部の設置	情報セキュリティ対策の司令塔となる「情報管理対策本部」を新設し、情報セキュリティに関する業務を責任を持って一元的に実施する。	• 10月１日に情報管理対策本部を新設。情報セキュリティ関係の重要事項の検討開始。
	情報管理対策室の設置	情報セキュリティ対策の実務部門を強化し、情報セキュリティに関する機能を集約するために情報管理対策室を設置する。	• 10月１日に情報管理対策本部の実行部隊として情報管理対策室を新設し、共有ファイルや文書等の情報の一元的な管理や個人情報の保護体制を構築。 • 組織立ち上げに係る体制作り等について、支援業者による職員支援を実施（11月～）
	機構CSIRTの設置	セキュリティインシデントへの即応性を向上させるため、CSIRT（Computer Security Incident Response Team）を設置する。	• 10月１日に情報管理対策室（インシデント対策G）及び他部署の支援要員で構成する機構CSIRTを設置。
	最高情報セキュリティアドバイザーの設置	最高情報セキュリティアドバイザーについて、情報セキュリティ専門家の招聘又は専門機関との契約を行う。	• 機構の最高情報セキュリティアドバイザーの選定に向けて準備中。（28年度設置予定）
	情報セキュリティポリシーの改正	不正アクセスによる情報流出事案に関する検証・調査結果等で指摘された標的型メール攻撃に対する多重防御対策に関する規定等を整備。	• 直近の政府統一基準等との整合性を確認中。（11月改正予定）

日本年金機構における情報セキュリティ対策の取組み状況②

2. 技術的対策

NISC勧告の内容	主要事項	方針	取組み状況
○大量の個人情報や機微な情報を取り扱う業務に対してインターネット経由の攻撃が及ばないよう、情報システムの分離を確実に行う。 ○インターネットに接続された情報システムに対し、多重防御の情報セキュリティ対策を講じる。 ○独立した外部の専門家による情報セキュリティ監査の実施を定期的・継続的に受ける。	リスクアセスメント調査の実施	ISO27005やNISCのガイドライン等を踏まえたリスクアセスメント調査を実施する。	• 第三者によるリスク評価に向けて、機構LANシステムを中心とした個人情報等の重要情報を取扱う業務の実態把握とリスク分析について、機構自ら実施中。（11月目途）
	個人情報をインターネット環境に置かないシステム構築	○機構のシステム全体について、多種多様なインシデントに耐え得る強力な防御体制を整備する。 ○基幹システムや個人情報等の重要情報については、インターネット接続環境から完全に遮断する。 ○将来的なインターネット環境の構築に当たっては、「個人情報を扱う業務の共有ファイルサーバは基幹システムの領域内に設置すること」「個人情報をインターネット接続環境下に置かないこと」を基本とする。	• システムの構築に向けて、個人情報等の重要情報を確実に管理しつつ、業務を円滑に進めるための仕組みを工夫する必要があることから、リスクアセスメント調査等で把握した業務実態を踏まえた検討が必要。（12月初旬目途）
	情報セキュリティに関する監査の強化	業務監査に当たり、情報セキュリティに関するリスクにも重点を置いた監査を実施するとともに、独立した外部の専門家によるシステム監査を実施する。	• 平成27年度監査から、各拠点の自主点検項目に情報セキュリティに関する事項を追加し、その点検状況を監査項目に追加した。

日本年金機構における情報セキュリティ対策の取組み状況③

3. 教育・訓練

NISC勧告の内容	主要事項	方針	取組み状況
○役職員が、国民の個人情報を取り扱うことの責任を認識し、その役割に応じた情報セキュリティ対策に関する責務を果たすべく、教育研修を定期的・継続的に実施する。	情報セキュリティ研修の充実	情報セキュリティに関する研修内容に関し、情報管理対策本部による意思決定が行われるようルール化を図る。	• 外部機関が開催する情報セキュリティ研修に積極的に参加していく。（厚生労働省・総務省・NISC等） • 来年度の情報セキュリティに関する研修計画の策定に向けて、職員の理解と意識改革を促す内容となるよう検討を開始。
	情報セキュリティインシデントに対する訓練の実施	研修の成果を模擬訓練等によりチェックし、継続的に研修内容を改善する。	• インターネットメール環境を利用する状況にない現状を踏まえ、標的型メールの訓練に優先して対処すべき脅威（ウイルス感染やホームページ改ざん等）への訓練計画を検討中。