不正アクセスによる情報流出事案以後の日本年金機構における
これまでの情報セキュリティ対策について

平成 28 年 11 月 8 日
日本年金機構

第一　はじめに

○　日本年金機構（以下「機構」という。）においては、昨年５月に発生した不正アクセスによる情報流出事案を受け、厚生労働大臣からの業務改善命令に基づき、同年 12 月に「業務改善計画」を策定。組織の一体化・内部統制の有効性の確保、情報開示の抜本的な見直し、情報セキュリティ対策の強化について取組を進めてきた。特に情報セキュリティ対策の強化については、組織面、技術面、業務運営面からの取組を実施してきた。

○　これらの取組については、厚生労働省による指導・監督や内閣サイバーセキュリティセンター（NISC）・個人情報保護委員会（PPC）による確認を受けてきたが、これらの経緯を踏まえ、マイナンバーの利用に必要な情報セキュリティ対策が講じられたものと判断し、これまでの取組状況について、本報告書をとりまとめた。

第二　情報流出事案以後の機構における情報セキュリティ対策について

１．組織面

○情報管理対策本部の設置

・情報流出事案（以下「事案」）時に責任の所在が不明確で連携が不十分であったこと等から、情報セキュリティ対策を一元的に管理し、リスク管理や情報セキュリティ対策に関する機構全体のガバナンス強化を図るため昨年 10 月１日に設置。理事長を本部長とし各部門の理事等により構成。諸規程・手順書等の整備や緊急時の対応方針の決定等を所掌事務とする。（PPC による立入検査等

で明らかになった課題に対し、同本部で集中的に対策の進捗管理や各拠点への指示等を実施。）

○情報管理対策室の設置

・情報管理対策本部が決定した方針を全職員に適切に実行させる組織として昨年10 月１日に設置。情報セキュリティ研修及び訓練内容の企画、情報セキュリティ対策の実施（諸規程の見直し、対策の評価・管理など）インシデント窓口などを所掌。

○機構 CSIRT の設置

・事案時には設置されておらず、対応が担当者任せとなっていたことや理事長等への報告が適切に行われなかった反省から、インシデントに係る連絡調整等を行う組織として昨年 10 月１日に設置。

○最高情報セキュリティアドバイザー等の設置

・情報管理対策本部や CISO に対し情報セキュリティ対策の推進に係る助言をし、その司令塔機能を強化するため最高情報セキュリティアドバイザーを本年４月１日に設置。その他情報管理対策室等を技術的に支援する情報セキュリティ対策支援業者の設置や、機構における各種取組に係る厚生労働省の関与・監督を強めるための連絡会議の設置を実施。

２．技術面

○事案発生直後のインターネットからの遮断及びシステムの再構築

・事案発生後、６月４日には年金個人情報が置かれていた機構 LAN システム（調査の結果、共有ファイルサーバには、把握できた範囲では個人情報を含むファイルが約 563 万ファイルあったことを確認）をインターネット環境から完全に遮断。

・大量の年金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、基幹システム、機構 LAN システム及びインターネット環境については、それぞれのシステムの独立性・完全性を確保するため分離した仕組みとした。

○年金個人情報等専用共有フォルダの構築

・新たに年金個人情報等の専用共有フォルダを機構 LAN システムから遮断された基幹システムの領域に構築することとし、北関東・信越地域の拠点におけるプロトタイプ検証により得られた業務上の課題を反映しながら、本年 10 月３日より運用開始。

・年金個人情報等専用共有フォルダは、業務端末からのみアクセス可能とするほか、今後、生体認証による同フォルダへのアクセス制限やファイルの自動暗号化を実施する予定。

○その他の取組

・市町村等との間でデータを授受する際の暗号化の実施。

・既知の脆弱性を放置しないようセキュリティパッチの最新化、ネットワークを管理する重要な機器の常時監視（モニタリング）等の運用管理対策の見直し。

３．業務運営面

○情報セキュリティポリシー等の整備

・出所不明の外部媒体をネットワーク上の端末に接続しないこと、インターネットへの接続により発生しうるリスクに対する入口対策、内部対策、出口対策を講じることや情報セキュリティ体制などを規定した情報セキュリティポリシーを整備。加えて、インシデントに対処するための組織・役割分担や運用管理業者との連携などの対処フローを規定した情報セキュリティインシデント対処手順書を整備。

○全役職員対象の研修、インシデント対処訓練の実施

・本部が規定した統一的な内容により全役職員に対し研修を継続的に実施。理解度テストにより理解が進んでいないと考えられる部分や情報セキュリティポリシーの改正内容を講義内容とし、情報セキュリティポリシーを現場へ定着。

・情報セキュリティポリシー及び対処手順書に基づき実際のインシデントを想定した実践的な訓練を厚生労働省と合同で継続的に実施し、訓練内容を自主点検や内部監査を通じて日常業務に反映。

・CSIRT の対応能力向上のため研修等専門知識の習得。

○監査体制の整備

・実効性のある内部監査実施のため、改善対応に係る計画を提出させるとともに監査対象部署の評価を当該部署の長の人事評価に反映。

・監査部は監査結果の要因分析を行い、監査対象部署の取組状況について方針、計画、実施運用を継続的に検証し、適切性・妥当性・有効性の判定を行って必要に応じ是正措置を要求するなど PDCA の強化。

○電子機器、電子媒体の管理等

・拠点内の電子機器・電子媒体の統一的な管理簿の整備。

・個々の電子機器・電子媒体のライフサイクル管理。

・不要になった電子媒体の確実な廃棄。

第三　おわりに

○　機構は、公的年金業務の最も大切な執行部分を請け負う中で、お客様から膨大な個人情報をお預かりしている日本有数の機関であり、いわば個人情報の「塊」といっても過言ではない組織である。また、職員一人ひとりがその自覚と業務に対する誇りを持って個人情報に接することが情報セキュリティ対策の第一のそして最大の対策である。

○　これまでの情報セキュリティ対策に係る一連の取組について、一過性のものとせず守るべき厳格なルールとして取り組むほか、ルールそのものについても現場の実態を踏まえた見直しを行う。

○　平成28年度からの3年間の計画である業務改善計画について必ず成し遂げ、改めて機構がお客様の大切な年金個人情報を任せるに足る機関であると、お客様に安心・信頼していただけるような組織となることを目標とし、今後も情報セキュリティ対策の迅速かつ確実な推進を図っていく。