## 第２　年金個人情報に関する情報セキュリティ対策の実施状況及び年金個人情報の流出が日本年金機構の業務に及ぼした影響等について

| | |
|---|---|
| 検　査　対　象 | ⑴　厚生労働省<br>⑵　日本年金機構 |
| 年金情報システムの概要 | 国民年金、厚生年金保険等の被保険者、年金受給者等の基礎年金番号、氏名、生年月日、住所、保険料の納付状況等の個人情報を管理するシステム |
| 年金情報システム等の開発・運用等に支出した額 | ⑴　2943億1116万円（平成22年度～27年度）<br>⑵　2236億2857万円（平成22年度～27年度） |

### １　検査の背景

#### ⑴　日本年金機構における個人情報、情報システム及び情報セキュリティ対策の概要

ア　日本年金機構において取り扱う個人情報、情報システム等の概要

厚生労働省は、健康保険、国民年金及び厚生年金保険の事業に関する事務を所掌しており、これらの事業に関する事務の一部については、日本年金機構法（平成19年法律第109号。以下「機構法」という。）に基づき、同省の監督の下に日本年金機構（以下「機構」という。）が行っている。

厚生労働省及び機構が取り扱う国民年金、厚生年金保険等の被保険者、年金受給者等の基礎年金番号、氏名、生年月日、住所、保険料の納付状況等の個人情報（以下「年金個人情報」という。）は膨大な件数に上り、また、長期にわたり取り扱われる。そこで、厚生労働省及び機構は、年金個人情報を情報システムにより管理して、業務の運営の効率化を図ることとしている（以下、この情報システムを「年金情報システム」という。）。年金情報システムは、社会保険オンラインシステム（以下「オンラインシステム」という。）、機構内のLANシステム（以下「機構LANシステム」という。）等で構成されている。

一方、厚生労働省は、通信回線等の運用経費の削減等を目的として、厚生労働省統合ネットワーク（以下「統合ネットワーク」という。）を構築している。そして、機構は、平成22年１月に発足して以降、オンラインシステム及び機構LANシステムを使用して業務を実施する際の機構本部及び全国に所在する機構の地方組織（以下「年金事務所等」という。）を接続する通信回線として、統合ネットワークを利用している。

年金情報システム及び統合ネットワークの開発、運用、情報セキュリティ対策等のために22年度から27年度までの間に支出した額は、厚生労働省で計2943億1116万余円、機構で計2236億2857万余円、合計5179億3973万余円となっている。

イ　年金個人情報に関する情報セキュリティ対策の概要

㋐　情報セキュリティポリシーの概要

厚生労働省及び機構は、前記のような年金情報システムの開発、運用等に当たり、年金個人情報がプライバシー性の非常に高い情報であることなどから、年金個人情報

等に関する情報セキュリティを確保するための対策等に関する規程（以下「情報セキュリティポリシー」という。）をそれぞれ定めている。

厚生労働省の情報セキュリティポリシー（以下「厚労省ポリシー」という。）は、「政府機関の情報セキュリティ対策のための統一基準」（情報セキュリティ政策会議決定。以下「統一基準」という。）等に準拠して定められており、統一基準が改正された場合には、統一基準の改正内容に準拠して改正されることとなっている。

また、機構の情報セキュリティポリシー（以下「機構ポリシー」という。）は、厚労省ポリシーに準拠して定められており、統一基準の改正等に伴い厚労省ポリシーが改正された場合には、厚労省ポリシーの改正内容に準拠して改正されることとなっている。

厚労省ポリシー及び機構ポリシーには、それぞれ厚生労働省又は機構における情報セキュリティの確保のために必要な年金情報システム等の認証機能やアクセス制御機能に関する規定等が設けられている。そして、厚労省ポリシーによれば、情報セキュリティに関する障害、事故等（故障、インシデント(注1)、サイバー攻撃予告等を含む。）が発生した場合に対処するための具体的な手順等を定めた規程（以下「インシデント対処手順書」という。）を定めることとされている。

（注1）　インシデント　　コンピュータシステムにおけるセキュリティの確保に脅威を及ぼす事象又はその可能性のある事象

⑷　機構における共有フォルダの運用

機構は、25年8月に機構本部内の各部署及び年金事務所等に対して、「共有フォルダの整理（指示・依頼）」（平成25年8月事務連絡。以下「共有フォルダ整理指示依頼」という。）を発している。また、27年3月には、「日本年金機構共有フォルダ運用要領（平成27年要領第171号。以下「共有フォルダ要領」という。）を定めている。これらによれば、年金個人情報を適切に管理するために、インターネットに接続されている機構LANシステム上の共有フォルダに年金個人情報を保存することは、原則として禁止することとされている。ただし、業務上必要がある場合における一時的な措置であれば、所要のアクセス制限やパスワードの設定を行うことを前提に、これを例外的に認めることとされている。そして、共有フォルダに年金個人情報を保存する場合の所要のアクセス制限やパスワード設定については、機構における情報セキュリティ責任者（機構本部内の各部署及び年金事務所等に置かれ、その所掌する部署等の情報セキュリティ対策に関する事務を統括することとされている者。以下同じ。）とされている年金事務所長等が定期点検において確認することとされている。

### ⑵　年金個人情報の流出とその検証の概要

機構は、外部から標的型攻撃(注2)を受けて、その結果、機構LANシステム上の共有フォルダに保存されていた約125万件（対象者約101万人分）の基礎年金番号、氏名等の年金個人情報が27年5月21日から23日までの間にインターネットを通じて不正に外部に流出したとしている（以下、この標的型攻撃による年金個人情報の流出を「流出事案」という。）。

（注２）　標的型攻撃　　不正なプログラムを含むファイルを添付するなどしたメールを職員に対して送りつけ、添付ファイルを開封するなどした職員の端末を介してネットワークに不正に侵入するなどのサイバー攻撃

そして、流出事案の事実関係、原因の究明等は、厚生労働省に設置された検証委員会による「検証報告書」等の報告書（以下「検証報告書等」という。）に取りまとめられている。

検証報告書等によれば、流出事案を発生させた直接的な要因は、機構において、標的型攻撃を受けた場合における対応については、LAN ケーブルの抜線以外に具体的な定めがなく、このため、メールの開封の有無や不正なプログラムへの感染の有無等の事態の確認が遅れ、有効な対策が講じられなかったことであるとされている。

また、厚生労働省は、21 年 9 月にインシデント対処手順書を策定した上で、25 年 2 月に CSIRT(注３) を設置している。しかし、検証報告書等によれば、機構は、流出事案の発生当時、標的型攻撃を受けた場合の対応手順等を具体的に記載したインシデント対処手順書を策定しておらず、また、CSIRT も設置していなかったなどとされている。

（注３）　CSIRT　　組織内の情報セキュリティ問題を専門に取り扱うインシデント対応チーム

さらに、検証報告書等によれば、流出事案により機構の共有フォルダから流出した年金個人情報約 125 万件のうち、所要のアクセス制限及びパスワードの設定を行っていたものは約 68 万件、所要のアクセス制限のみを行っていたものは約 53 万件、所要のパスワードの設定のみを行っていたものは約 2 万件となっていて、残りの約 2 万件については所要のアクセス制限もパスワードの設定も行われていなかったとされている。

### ⑶　流出事案の再発防止に向けた取組の概要

厚生労働省は、検証報告書等の指摘を受けて、情報セキュリティ対策の観点からの組織内・組織間連携の強化等を図って流出事案の再発を防止するために、「情報セキュリティ強化等に向けた組織・業務改革」（以下「組織・業務改革報告書」という。）を 27 年 9 月 18 日に公表している。一方、機構は、同月 25 日に機構法第 49 条第 1 項の規定に基づく厚生労働大臣の業務改善命令を受けて、業務改善計画を策定して同年 12 月 9 日に厚生労働大臣に提出しており、再発防止に向けて機構が既に執った対策及び今後実施する取組を明らかにするなどしている。

### ⑷　流出事案が機構の業務に及ぼした影響の概要

機構は、流出事案の発生により、年金個人情報の管理に対する国民の信頼を大きく損ねたことから、順次、次のような対応を行っている。

すなわち、機構は、年金個人情報が流出した者（以下「年金個人情報流出者」という。）の基礎年金番号を変更することとし、年金個人情報流出者に対して、年金個人情報の流出に対するおわびを記した文書（以下「おわび文書」という。）、基礎年金番号の変更を通知する文書（以下「基礎年金番号変更通知」という。）等の送付を行っている。そして、これらの対応に必要な経費としては約 10 億円(注４) が見込まれるとしている。

（注４）　約 10 億円　　平成 28 年 1 月 8 日衆議院予算委員会において行われた流出事案の対応に要する経費に関する厚生労働大臣の答弁による。

また、機構は、流出事案発生以前には、国民年金保険料の未納者に対して納付督励業務を行っていた。納付督励業務には、機構が自ら実施する業務（以下「機構納付督励業務」と

いう。）と、機構から委託を受けた民間事業者が実施する業務（以下「市場化納付督励業務」という。）とがある。

機構納付督励業務は、未納者に対して戸別訪問、電話による問合せに対する対応（以下「受電対応」という。）、特別催告状等の文書の送付等を行うほか、強制徴収に関する一連の手続（強制徴収対象者の選定から換価・配当に至る手続。以下「強制徴収手続」という。）を行うものである。特別催告状とは、未納者の財産の差押えなどについて明記している文書である。そして、強制徴収手続においては、未納者に対して、自主納付の催告を行う最終催告状が送付されることとなっており、最終催告状の送付後に納付の意思が確認できなかった者に対しては、督促状が送付されることとなっている。

また、市場化納付督励業務は、民間事業者が未納者に対して、戸別訪問、架電、受電対応、国民年金制度のお知らせなどの文書の送付等を行うものである。

しかし、流出事案の発生を踏まえ、機構は、年金個人情報流出者に対する対応等に集中して取り組む必要が生じたことなどを理由として、27年6月に機構本部内の各部署及び年金事務所等に対して通知を発し、一定期間、納付督励業務の一部を行わないこととしていた。そして、機構納付督励業務のうち、特別催告状の送付、強制徴収手続等については同年6月8日（一部については6月4日）から同年10月27日までの間、また、受電対応を除く市場化納付督励業務については同年6月2日から同年11月16日までの間、行われなかった（以下、この市場化納付督励業務を行わないこととされた期間を「業務委託中止期間」という。）。

**2　検査の観点、着眼点、対象及び方法**

前記のとおり、機構は、流出事案の発生に対応するための経費として約10億円が見込まれるなどとしている。そして、厚生労働省及び機構は、検証報告書等を踏まえて、年金個人情報に関する情報セキュリティの確保について様々な対応策を講ずるとともに、再発防止の取組を進めているなどとしている。

そこで、本院は、合規性、経済性、効率性、有効性等の観点から、流出事案の発生前において、機構における年金個人情報に関する情報セキュリティ対策は適切に行われていたか、厚生労働省及び機構におけるその実効性を確保するための監査等は適切に行われていたか、また、流出事案の発生後において、機構の年金個人情報に関する情報セキュリティ対策及び流出事案への対応業務は適切に行われているか、流出事案の発生は機構の業務にどのような影響を及ぼしているか、その後の厚生労働省及び機構における再発防止に向けた取組の進捗状況はどのようになっているかなどに着眼して検査した。

検査に当たっては、厚生労働省、機構本部及び24都道府県(注5)下の159年金事務所等において、年金個人情報に関する情報セキュリティ対策の状況について確認するとともに、監査報告書等の関係書類等により会計実地検査を行った。また、市場化納付督励業務を実施している3民間事業者(注6)において、契約書等の関係書類等により会計実地検査を行った。

（注5）　24都道府県　　東京都、北海道、大阪府、青森、岩手、宮城、秋田、群馬、埼玉、千葉、神奈川、新潟、静岡、愛知、滋賀、兵庫、奈良、広島、香川、福岡、佐賀、宮崎、鹿児島、沖縄各県

（注6）　3民間事業者　　株式会社アイヴィジット、株式会社バックスグループ、日立トリプルウィン株式会社

## 3　検査の状況

### (1)　流出事案の発生前における年金個人情報に関する情報セキュリティ対策等の実施状況及び流出事案発生後における年金個人情報の保存等の状況

ア　流出事案の発生前における機構ポリシーの改正状況

機構が設立された22年1月以降、流出事案の発生前の27年4月までの間における機構ポリシーの改正の状況についてみたところ、厚労省ポリシーの改正から約5か月から約7か月を要しており、厚労省ポリシーの改正後速やかに機構ポリシーが改正されない場合には統合ネットワーク内でセキュリティ水準の異なる期間が生ずるなどしてしまうのに、機構ポリシーが厚労省ポリシーの改正後速やかに改正されてきたとは言い難い状況となっていた。この点について、厚労省ポリシーの改正を所掌している厚生労働省政策統括官付情報政策担当参事官室(28年6月21日以降はサイバーセキュリティ担当参事官室(以下「情報参事官室」という。))は、機構において自らその統一基準等の改正内容等を確認するなどして情報セキュリティポリシーの改正を行うこととしていると認識しており、同省年金局(以下「年金局」という。)は、機構ポリシーの改正の時期等については確認することとしていなかったとしている。さらに、機構は、機構の内部規程上、機構ポリシーの改正事務について所掌が明確でなかったなどとしている。

イ　流出事案の発生前における厚生労働省及び機構による年金個人情報に関する情報セキュリティ監査等の実施状況

(ｱ)　厚生労働省の機構に対する監査の実施状況

厚生労働省は、年金局事業企画課監査室(以下「監査室」という。)を実施部局として、機構に対して業務監査、会計監査等の各種の監査を実施している。そして、業務監査の一環として、オンラインシステムを主な対象として、情報システムの信頼性、効率性等に関する監査(以下「システム監査」という。)及び機構における情報一般(紙媒体を含む。)の管理体制について評価する監査(以下「情報セキュリティ監査」という。)を実施している。

22年度から26年度までの間におけるシステム監査及び情報セキュリティ監査の実施状況についてみたところ、監査室は、システム監査については33回、情報セキュリティ監査については182回実施していた。

しかし、監査室は、機構ではインシデント対処手順書を策定しておらず、また、CSIRTを設置していないなど、情報セキュリティに関する体制整備が十分でないことについては、指摘していなかった。

(ｲ)　機構における内部監査の実施状況

機構における内部監査については監査部が行うこととされており、内部監査の結果は機構の理事長に報告することとされている。内部監査には、会計監査、業務監査、システム監査、情報セキュリティ監査等がある。

このうち、22年度から26年度までの間におけるシステム監査及び情報セキュリティ監査の実施状況をみたところ、監査部は、システム監査については7回、情報セキュリティ監査については1,457回実施していた。

しかし、監査部は、機構ではインシデント対処手順書を策定しておらず、また、CSIRTを設置していないなど、情報セキュリティに関する体制整備が十分でないことについては、指摘していなかった。

⑶　機構の監査部における情報セキュリティの不備への対応状況

前記のとおり、機構は、共有フォルダにおいて年金個人情報を取り扱う場合には所要のアクセス制限やパスワードの設定を行うこととし、年金事務所等の情報セキュリティ責任者はこれを定期点検において確認することとする共有フォルダ整理指示依頼を発するなどしている。

監査部は、26年8月に内部監査の実施の要否を検討するために実施した事前調査において、所要のアクセス制限もパスワードの設定も行われないまま年金個人情報が共有フォルダに1年以上保存されていることを把握しており、同月、機構の経営企画部に対して改善要請を行っていた。そして、この改善要請を受けて、経営企画部は、機構本部内の各部署及び年金事務所等に対して同年10月末までに共有フォルダの整理を確実に行うよう周知するとともに、前記のとおり27年3月に共有フォルダ要領を定めていた。

しかし、監査部は、当該改善要請については、内部監査の実施の要否を検討するために実施した事前調査に基づき行ったもので内部監査の結果ではないなどとして、当該改善要請を行ったことを機構の理事長に対して報告しておらず、また、改善要請を行った後、年金個人情報が共有フォルダに保存されている状況が実際に改善されているかなどについては監査等を実施していなかった。

そして、検証報告書等によれば、流出した年金個人情報のうち約2万件については、所要のアクセス制限もパスワードの設定も行われていなかったとされていることを踏まえると、監査部の改善要請への対応は、機構において徹底されていなかったと認められる。

ウ　流出事案の発生前における厚生労働省の機構に対する情報セキュリティに関する指導等の状況

情報参事官室は、従来、省内の職員に対して、不審メールが送付されてきた場合の対処等について注意喚起等を行っていたほか、独立行政法人等を所管する部局に対しては、所管法人に対しても同様の注意喚起を行うよう依頼していたとしている。

しかし、年金局は、前記のとおり厚生労働省と同じく統合ネットワークを利用している機構に対して、不審メールが送付されてきた場合の対処等についての注意喚起等を十分に行っていなかった。

エ　流出事案の発生後における年金個人情報の保存等の状況

前記のとおり、共有フォルダ要領によれば、年金個人情報については、共有フォルダに保存することが原則として禁止されており、年金個人情報を共有フォルダに保存することができるのは、業務上の必要がある場合の例外的な措置とされている。また、機構が職員に対して実施しているリスク・コンプライアンス研修の配布資料(27年4月版)によれば、機構LANシステムに接続するLAN専用PC等(以下「専用PC」という。)のハードディスクには個人情報を保存しないこととされていることなどから、年金個人情報についてもハードディスクには保存しないこととなっていると認められる。

しかし、流出事案発生後の機構における年金個人情報の保存状況等についてみたところ、27年12月から28年6月までの間に会計実地検査を実施した8年金事務所(注7)等にお

いて、専用 PC のハードディスクに年金個人情報が保存されていることが確認された。

そこで、28 年 6 月に本院は、機構に対して、機構本部及びこれらの 8 年金事務所等を含む全国の年金事務所等において同様に専用 PC のハードディスクに保存されている年金個人情報の有無、及び年金個人情報が保存されている場合にはその件数について調査し、報告するよう求めた。これに対して、機構は、機構本部及び全国の年金事務所等の専用 PC のハードディスクに保存されていた年金個人情報については、同年 8 月から同年 9 月までの間に、今後とも業務上保有する必要があるものを年金個人情報を保存するために新たに設置した共有フォルダ(以下「専用フォルダ」という。)に移し替えるなどした上で全て削除したと本院に報告した。

その後、28 年 10 月及び同年 11 月にそれぞれ実施した機構本部及び高崎広域事務センターに対する会計実地検査において、上記のとおり、機構は、専用フォルダに移し替えるなどした上で全て削除したとしていたのに、専用 PC のハードディスクに年金個人情報等が保存されていることが確認された。

これらを踏まえて、機構は、28 年 8 月当時に専用 PC のハードディスクに保存されていた年金個人情報の有無等につき、同年 11 月時点で可能な調査を行うとともに、専用 PC のハードディスクに保存されている年金個人情報等の状況についても調査するなどとしている。

(注 7) 8 年金事務所等　東京事務センター、盛岡、松戸、幕張、中央、大手前、高松東、浦添各年金事務所

**(2) 流出事案の対応に要する経費の支出、対応業務等の状況**

ア　流出事案の対応に要する経費等の状況

前記のとおり、機構は、流出事案の発生に対応するための新たな業務の実施に要する経費として約 10 億円が見込まれるとしている。そして、機構において取りまとめた当該経費の支出額(27 年度決算額)は、計 10 億 8379 万余円となっており、これらの経費は、年金個人情報流出者に対するおわび、問合せ対応等に要する経費に限定されている。

そこで、流出事案が発生したことにより支出されたと考えられる経費等についてみたところ、機構は、共有フォルダに年金個人情報等が存在しているかどうかの調査等のために計 4730 万余円を支出していた。

また、厚生労働省においても、年金個人情報の流出を口実とする犯罪の発生を防止するためのチラシの配布等のために 2738 万余円、同省に設置された検証委員会の委員手当等として 1949 万余円、計 4687 万余円を支出しており、上記の機構による支出額と合算すると計 9418 万余円となる。

イ　流出事案の対応に要する経費に充てるためにねん出した財源

機構は、流出事案の発生の対応に要する経費に充てるため経費を削減した結果、計 11 億 0276 万円の財源をねん出したとしている。しかし、ねん出したとしている財源の中には、年金事務所の新築移転の延期等のため 27 年度には支出されないものの、28 年度以降において支出する必要があるものが含まれていると認められた。

ウ　おわび文書の送付等の状況

機構は、27 年 6 月以降、年金個人情報流出者 1,014,653 人を対象として、おわび文書

を普通郵便により送付している。そして、宛て先不明等により返送された場合には、住基情報(住民基本台帳ネットワークにおける住所変更の有無等の情報。以下同じ。)、市区町村への照会等により現住所を確認していて、新たな住所が判明した場合には、改めておわび文書の再送付等を行っている。また、同年8月には、これらのおわび文書が返送されてこなかった者等の計972,539人を対象として、順次、基礎年金番号変更通知等を簡易書留郵便で送付し、宛て先不明等の場合には、上記と同様に、住基情報を確認するなどして再送付している。

また、おわび文書又は基礎年金番号変更通知等が返送された者等の計62,554人(うち年金受給者6,988人)については、今後、年金事務所等に来訪したときに、直接手渡すなどして対応することとしている。

一方、機構は、25年8月に、住民票上は死亡しているのに親族から年金受給者が生存しているとする現況届が提出され、年金の不正受給が行われていた事案があったことを踏まえ、26年2月から、現況届の提出により生存又は死亡の事実(以下「生存等の事実」という。)を確認している一定年齢以上の年金受給者については、住民票の住所、実際に住んでいる住所等を記載する年金受給権者現況申告書の提出等により改めてその生存等の事実を確認している。そして、死亡を確認した者又は戸別訪問を実施しても生存の事実を確認できなかった者については、年金支給の差止めを行い、過払いが判明した場合は債務者に対してその返還を求めるなどしていて、その取組状況を27年12月に公表している。

しかし、前記のおわび文書又は基礎年金番号変更通知等が返送された者のうち年金受給者計6,988人に対する年金支給の状況についてみたところ、戸別訪問の実施等によっても年金受給者の所在が確認できないのに、機構は、これらの者の生存等の事実について更に確認しないまま年金支給を継続していた。

機構において、年金支給を適切に行うために、おわび文書等が返送されていて、年金受給者の所在が確認できないという情報を有効に活用し、その生存等の事実を確認することなどについて検討する必要があったと認められる。

**(3)　流出事案の発生により中止した業務の影響等**

前記のとおり、機構は、27年6月2日から同年11月16日までの間、機構納付督励業務の一部及び受電対応以外の市場化納付督励業務を中止していた。

そこで、両業務の中止が機構の業務に及ぼした影響等についてそれぞれみたところ、次のような状況となっていた。

ア　機構納付督励業務の一部を一定期間実施しなかったことによる影響

(ア)　国民年金保険料を徴収する権利の時効消滅の状況

国民年金保険料を徴収する国の権利は、国民年金法(昭和34年法律第141号)第102条第4項の規定により、納付期限から2年の期間を経過したときは時効により消滅することとされているが(以下、この期間を「消滅時効期間」という。)、当該消滅時効の進行は、同条第5項の規定によれば、督促状の送付により中断されることとされている。

機構は、国民年金保険料の収納対策として、毎年度、行動計画策定手順書(以下「行

動計画」という。）を定めており、強制徴収手続を確実に実施することなどとされている。

しかし、前記のとおり、機構は、27年6月から約5か月の間は、強制徴収手続を行っていなかった。そこで、27年度において送付した43,757件の督促状のうち、10都府県(注8)下の77年金事務所が送付した15,812件について、本院において、上記約5か月の間に最終催告状及び督促状を送付しなかったため消滅時効期間が経過した国民年金保険料の債権額等を試算した。

その結果、計4,372名に対する国民年金保険料の債権8,159か月分について消滅時効期間が経過しており、当該月数に国民年金保険料の月額を乗ずるなどして、消滅時効期間が経過した国民年金保険料の債権額を試算すると、1億2115万余円となる。そして、上記計4,372名のうち2,164名については、督促対象期間における国民年金保険料を完納しており、仮に流出事案の影響を受けることなく督促状を送付できていれば、消滅時効が中断され、消滅時効期間の経過前に国民年金保険料を納付したと考えられることから、この2,164名分について消滅時効期間が経過した国民年金保険料の債権額等を試算すると、3,769か月分、5659万余円となる。

（注8） 10都府県　　東京都、大阪府、宮城、埼玉、千葉、神奈川、静岡、愛知、兵庫、福岡各県

(ｲ) 特別催告状の送付の状況

機構は、特別催告状の送付が国民年金保険料の納付実績の向上に与える影響を適切に把握するために、特別催告状を送付した未納者からその後何か月分の国民年金保険料の納付があったかについて調査しており、その実績については特別催告状1件当たりの「効果率」として、未納者の控除後の所得、未納月数等の属性別に算出している。

27年度当初の行動計画等によれば、未納者の属性別に計9,053,175件の特別催告状を送付することとされていたのに、前記のとおり、27年6月から約5か月の間については特別催告状の送付が行われなかったことから、同年度の送付実績は、計8,281,538件となっていた。

そこで、本院において、27年度の特別催告状が当初の行動計画等のとおり送付された場合には収納されたことが見込まれる国民年金保険料の額等について試算したところ、計759,967か月分、計118億4788万余円となる。

イ　業務委託中止期間を含む委託費の支払

機構は、26年度に、6民間事業者との間で計23件の市場化納付督励業務に関する委託契約（以下「市場化納付督励業務委託契約」という。）を締結しており、その契約金額については計215億0390万余円となっている。

27年度分の委託費の支払状況等についてみたところ、前記のとおり、流出事案の発生を踏まえて、機構は、27年6月2日に民間事業者に対して受電対応以外の市場化納付督励業務を行わないよう求めていて、業務委託中止期間がその後の約5か月間に及んでいたのに、委託費の支払に当たっては、従前どおり、市場化納付督励業務委託契約に係る委託契約書（以下「委託契約書」という。）の第27条の約定に基づき、業務委託中止期間を含む27年5月から28年4月までの1年間に係る委託費計66億2112万余円を12等分して、民間事業者に対して毎月、当該額を支払っていた。

なお、機構は、委託費については市場化納付督励業務の実績(国民年金の被保険者に係る国民年金保険料が実際に納付された月数等の合計)に応じた増減を行うものとする委託契約書第7条の約定に基づき、民間事業者が業務委託中止期間中に業務を実施しなかったことによる27年度の実績の減少も踏まえて委託費の精算を行うなどとして、28年10月に、民間事業者6社のうち5社に対して、27年度分の支払済みの委託費計2億3122万余円の返還を求めている。

**(4) 再発防止の取組の進捗状況**

ア　厚生労働省における再発防止の取組の進捗状況

27年9月に組織・業務改革報告書が公表されてから28年9月までの間における再発防止の取組の進捗状況についてみたところ、厚生労働省は、統合ネットワーク等において高度な標的型攻撃に対応するための改修等を行うなどしていた。

イ　機構における再発防止の取組の進捗状況

27年12月に業務改善計画が提出されてから28年9月までの間における再発防止の取組の進捗状況についてみたところ、機構は、年金個人情報の管理・運用を行う領域をインターネットから完全に分離した年金情報システムの構築に向けた取組を進めるなどしていた。

**4　所見**

**(1) 検査の状況の概要**

合規性、経済性、効率性、有効性等の観点から、流出事案の発生前において、機構における年金個人情報に関する情報セキュリティ対策は適切に行われていたか、流出事案の発生は機構の業務にどのような影響を及ぼしているかなどに着眼して検査したところ、次のような状況となっていた。

ア　流出事案の発生前における年金個人情報に関する情報セキュリティ対策等の実施状況及び流出事案発生後における年金個人情報の保存等の状況

(ｱ)　流出事案の発生前における機構ポリシーの改正の状況についてみたところ、厚労省ポリシーの改正から一定の期間、統合ネットワーク内でセキュリティ水準の異なる期間が生ずるなどしてしまうのに、機構において厚労省ポリシーの改正後速やかに機構ポリシーの改正を行っておらず、また、厚生労働省及び機構において、機構ポリシーの改正に向けた連携等が十分とは認め難い状況となっていた。

(ｲ)　流出事案の発生前における厚生労働省の機構に対する監査及び機構の内部監査の実施状況についてみたところ、いずれの監査においても、情報セキュリティに関する体制整備が十分でないことについて指摘したことはない状況となっていた。

また、監査部は、所要のアクセス制限等の設定が行われないまま年金個人情報が共有フォルダに保存されていることを把握し、経営企画部に対して改善要請を発していたが、この要請について機構の理事長に対して報告しておらず、また、実際の改善状況等に対する監査等を実施していなかった。そして、機構において、監査部の改善要請への対応は徹底されていなかったと認められた。

(ｳ)　流出事案の発生前における厚生労働省の機構に対する情報セキュリティに関する指導等の状況についてみたところ、年金局では、機構に対して、所要の注意喚起等を十分に行っていなかった。

(エ) 流出事案の発生後における年金個人情報の保存等の状況についてみたところ、専用PCのハードディスクに年金個人情報が保存されていることが確認され、機構は、28年8月から同年9月までの間に、専用PCのハードディスクに保存されていた年金個人情報について、専用フォルダに移し替えるなどした上で全て削除したとしている。その後、同年10月及び同年11月の会計実地検査において、機構は、専用フォルダに移し替えるなどした上で全て削除したとしていたのに、専用PCのハードディスクに年金個人情報等が保存されていることが確認された。

イ　流出事案の対応に要する経費の支出、対応業務等の状況

(ア) 機構の流出事案の発生に対応するための経費として見込んだ額約10億円の支出額は、27年度決算額で10億8379万余円となっていた。また、このほか、流出事案が発生したことにより支出されたと考えられる経費があり、これらの経費を合算すると計9418万余円(厚生労働省分4687万余円、機構分4730万余円)となる。

また、機構が流出事案の発生に対応する経費に充てるためにねん出したとしている財源の中には、27年度には支出されないものの、28年度以降において支出する必要があるものが含まれていると認められた。

(イ) おわび文書又は基礎年金番号変更通知等が返送された年金受給者計6,988人に対する年金支給の状況についてみたところ、年金受給者の所在が確認できないのに、機構は、これらの者の生存等の事実について更に確認しないまま年金支給を継続していた。機構においては、年金受給者の所在が確認できないという情報を有効に活用し、その生存等の事実を確認することなどについて検討する必要があったと認められる。

ウ　流出事案の発生により中止した業務の影響等

(ア) 最終催告状及び督促状を送付しなかったことにより消滅時効期間が経過した国民年金保険料の債権額等について試算すると、8,159か月分、1億2115万余円となり、このうち、仮に流出事案の影響なく督促状を送付していれば、消滅時効が中断され、消滅時効期間の経過前に納付されたと考えられる国民年金保険料の債権額等について試算すると3,769か月分、5659万余円となる。

また、約5か月の間に特別催告状を送付しなかったことを踏まえ、当初の行動計画等のとおりに特別催告状を送付した場合に収納が見込まれる国民年金保険料の額等について試算すると、計759,967か月分、計118億4788万余円となる。

(イ) 委託費の支払についてみたところ、機構は、受電対応以外の市場化納付督励業務を一定期間実施しないこととした業務委託中止期間が約5か月間に及んでいたのに、業務委託中止期間を含む27年5月から28年4月までの1年間に係る委託費として計66億2112万余円を12等分して毎月支払っていた。

なお、機構は、民間事業者が業務委託中止期間中に業務を実施しなかったことによる27年度の実績の減少も踏まえて委託費の精算を行うなどとして、28年10月に、民間事業者6社のうち5社に対して、27年度分の支払済みの委託費計2億3122万余円の返還を求めている。

エ　再発防止の取組の進捗状況

27年9月から28年9月までの間における厚生労働省の再発防止の取組の進捗状況についてみたところ、統合ネットワーク等において高度な標的型攻撃に対応するためのシ

ステム改修等を行うなどしていた。

また、27年12月から28年9月までの間における機構の再発防止の取組の進捗状況についてみたところ、年金個人情報の管理・運用を行う領域をインターネットから完全に分離した年金情報システムの構築に向けた取組を進めるなどしていた。

**(2) 所見**

流出事案の発生は、年金個人情報の管理に対する国民の信頼を大きく損ねたところであり、また、機構の業務に多方面で多大な影響を及ぼしている。そして、流出事案の発生を踏まえ、厚生労働省及び機構は、前記のとおり、再発防止のための各種の取組を行っている。

ついては、厚生労働省及び機構において、本院の検査により明らかとなった状況等を踏まえ、次のような点に留意して、年金個人情報の管理に関する一層の体制の整備を図るなどの必要があると認められる。

ア　機構において、厚労省ポリシーが改正された場合には、その改正内容に準拠して機構ポリシーを速やかに改正するなどするとともに、厚生労働省と機構との適切な連携等を図るなどして、年金個人情報に関する情報セキュリティ対策を適切に行うこと

イ　厚生労働省及び機構において、年金個人情報に関する情報セキュリティ監査を含め、同省の機構に対する監査及び機構の内部監査を一層実効性のあるものとすること

ウ　機構において、年金支給を適切に行うために、おわび文書等が返送されていて年金受給者の所在が確認できないという情報を有効に活用し、その生存等の事実を確認することなどについて検討すること

エ　機構において、機構が策定した業務改善計画に記載されている再発防止の取組を一層着実に実施すること

厚生労働省及び機構は、年金に関する業務の実施に当たり、今後とも膨大な年金個人情報を長期にわたり保有し、取り扱うことが見込まれる。本院は、これらを踏まえて、機構において情報セキュリティ対策が適切に実施されているか、同省及び機構において実効性のある監査等が行われているか、また、流出事案の影響等を踏まえた適切な対応が行われているか、さらに、機構の再発防止の取組が着実に行われているかなどについて、引き続き検査していくこととする。