会計検査院法第30条の2の規定に基づく報告書

「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」

平成２８年１２月

会　計　検　査　院

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、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。そして、厚生労働省及び機構が取り扱う厚生年金保険等の被保険者、年金受給者等の年金個人情報は膨大な件数に上り、また、長期にわたり取り扱われるものである。

年金個人情報は、プライバシー性の非常に高い情報であり、外部に漏えいするなどした場合には極めて重大な結果を招くおそれがある。このため、厚生労働省及び機構は、年金個人情報の管理に当たっては様々な情報セキュリティ対策を実施している。

しかし、平成27年5月に、機構が運用する情報システムの共有フォルダに保存されていた約125万件の年金個人情報がインターネットを通じて不正に外部に流出する事案が発生し、機構における年金個人情報の管理に対する国民の信頼が大きく損なわれることとなった。同事案の発生を受けて、厚生労働省及び機構は、その対応に多額の経費を要することとなったほか、国民年金保険料の納付実績を向上させるための業務の一部を一定期間行わないこととするなどしたことから、機構の業務に様々な影響が生ずるところとなっている。

そして、厚生労働省及び機構は、同事案の再発防止のための各種の取組を行っている。

本報告書は、以上のような状況等を踏まえて、同事案の発生前における機構の年金個人情報に関する情報セキュリティ対策等の状況、同事案の発生後における機構の情報セキュリティ対策及び同事案への対応業務等の状況、同事案の発生が機構の業務に及ぼした影響等について検査を実施し、その状況を取りまとめたことから、会計検査院法（昭和22年法律第73号）第30条の2の規定に基づき、会計検査院長から衆議院議長、参議院議長及び内閣総理大臣に対して報告するものである。

平成２８年１２月

会　計　検　査　院

目　　次

・本文及び図表中の数値は、表示単位未満を切り捨てている。

・上記のため、図表中の数値を集計しても計が一致しないものがある。

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	(1) 厚生労働省 (2) 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	(1) 2943億1116万円　（平成22年度～27年度） (2) 2236億2857万円　（平成22年度～27年度）

1　検査の背景

(1) 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。）、ねんきんネットシステム(注1)等で構成されている。

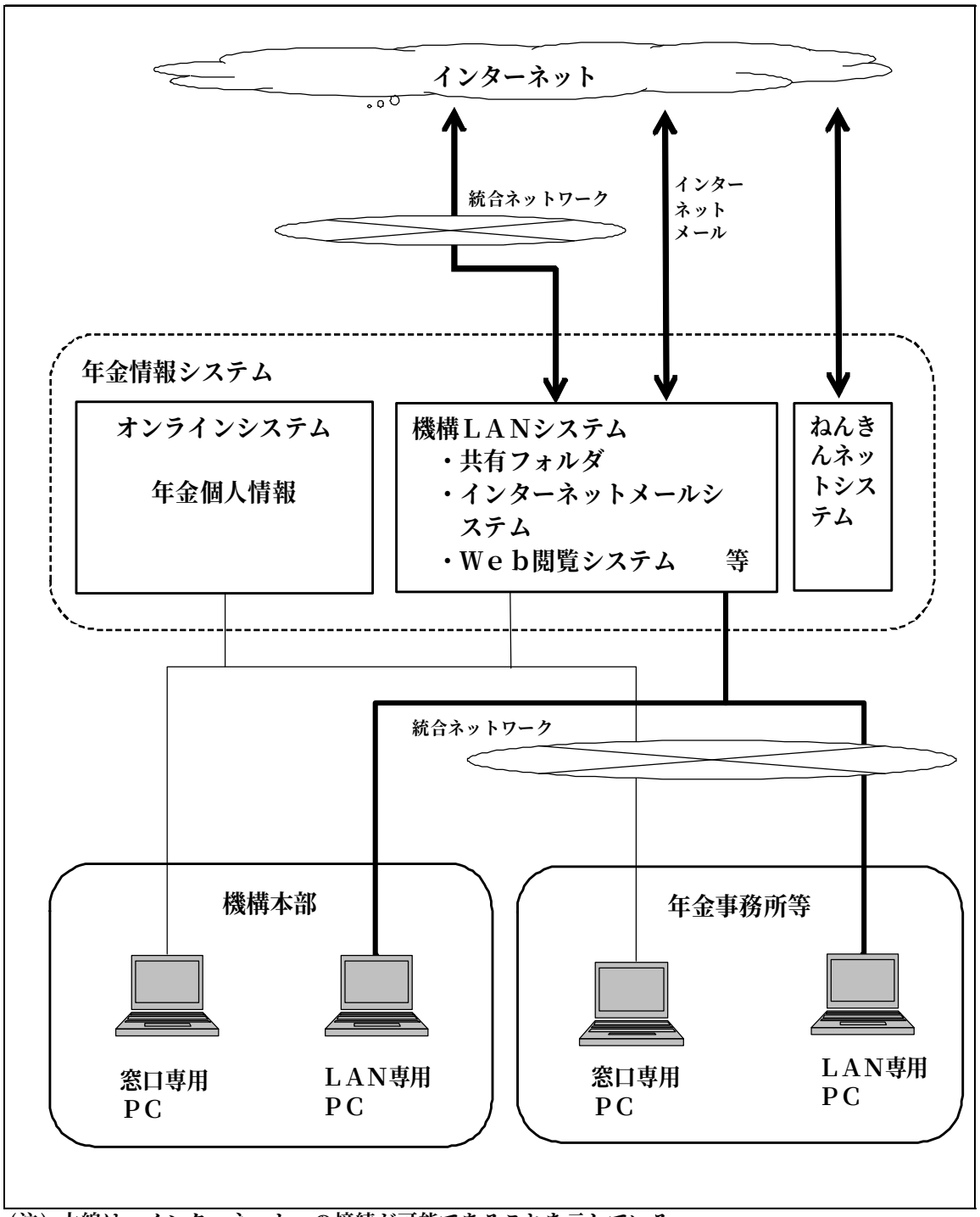
（注1）　ねんきんネットシステム　　被保険者等が自身についての年金記録、将来の年金見込額等の年金に関する様々な情報をインターネットを通じて確認できるシステム

年金情報システムのうち、オンラインシステムは、厚生労働省が年金個人情報を

管理するために開発したもので、端末として窓口専用ＰＣが利用されている。そして、平成22年1月に機構が発足して以降は機構がその運用を行っている。また、機構ＬＡＮシステムは、機構が開発したもので、業務上必要な情報を電子ファイルで保存するための共有フォルダ、インターネットメールシステム、Ｗｅｂ閲覧システム等で構成されており、端末としてＬＡＮ専用ＰＣが利用されている。

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、厚生労働本省、地方支分部局等を接続する複数の通信回線を統合した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、20年4月からその運用を開始している。そして、機構は、発足以降、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（図表1参照）。

図表1　年金情報システムの概要



（注）太線は、インターネットへの接続が可能であることを示している。

上記の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、図表2のとおり、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。

図表2　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厚生労働省及び機構が支出した額（平成22年度～27年度）

（単位：千円）

	厚生労働省			機構			合計
	年金情報システム (A)	統合ネットワーク (B)	計 (C)=(A)+(B)	年金情報システム (D)	統合ネットワーク (E)	計 (F)=(D)+(E)	(C)+(F)
平成22年度	34,125,435	3,354,653	37,480,089	20,954,692	1,299,998	22,254,690	59,734,780
23年度	50,841,202	3,543,933	54,385,136	29,724,629	1,358,383	31,083,012	85,468,149
24年度	42,838,597	2,114,108	44,952,706	44,452,234	924,605	45,376,839	90,329,545
25年度	45,481,512	2,108,036	47,589,548	34,437,229	1,070,034	35,507,264	83,096,812
26年度	47,037,903	2,159,090	49,196,994	46,797,830	1,074,654	47,872,484	97,069,478
27年度	58,551,116	2,155,575	60,706,691	40,498,716	1,035,561	41,534,278	102,240,970
計	278,875,768	15,435,398	294,311,166	216,865,332	6,763,237	223,628,570	517,939,736

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り、それが外部に漏えいするなどした場合には極めて重大な結果を招くおそれがあることなどから、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、高度情報通信ネットワーク社会推進戦略本部に設置された情報セキュリティ政策会議（27年1月9日以降はサイバーセキュリティ戦略本部）が策定した「政府機関の情報セキュリティ対策のための統一基準」（以下「統一基準」という。）等に準拠して定められたものである。そして、厚労省ポリシーは、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たものである。そして、機構ポリシーは、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、情報セキュリティ対策を推進するための体制整備、情報セキュリティに関する内部監査の実施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2)、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2）　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

(ｲ) 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。

(2) 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3)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日から同月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3）　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

流出事案の発生を踏まえて、機構は、同月29日、機構ＬＡＮシステムとインターネットとの接続（インターネットメールを除く。）を遮断し、また、6月4日にはインターネットメールとの接続も遮断して、現在に至っている。

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おり、その概要については図表3のとおりとなっている。

図表3　厚生労働省に設置された検証委員会により取りまとめられた検証報告書等の概要

年月日	報告書名	報告書の位置付け及び委員会等名	主な記述事項
平成27年8月20日	日本年金機構における個人情報流出事案に関する原因究明調査結果	サイバーセキュリティ基本法（平成26年法律第104号）第25条第1項第3号の規定に基づいて取りまとめられた報告書 サイバーセキュリティ戦略本部	○流出事案に関する技術的検討 (注) ○ＣＳＩＲＴの運用等に関する検討 ・機構ポリシーにおいては、インシデント対処体制の必要性を規定し、その具体化をリスク管理一般の規定等に委ねているものの、当該規定等では、サイバー攻撃を想定した具体的な対応は明確化されていない。 ・機構ポリシーにおいては、インシデント対処の必要性が規定されており、その具体的な規定は他の複数の規程類で規定しているものの、いずれの規程類においてもＣＳＩＲＴ体制が定められていない。 ○流出事案におけるサイバー攻撃の特徴と対策 ○サイバーセキュリティ戦略本部及び内閣サイバーセキュリティセンターが執るべき再発防止策
8月20日	不正アクセスによる情報流出事案に関する調査結果報告	機構の理事長を委員長として、役職員5名及び外部委員1名から構成された調査委員会により取りまとめられた報告書 不正アクセスによる情報流出事案に関する調査委員会	○流出事案に関する調査 ○年金個人情報が流出した者への対応状況 ○不正アクセスによる情報流出事案に関する調査 ・標的型攻撃に対する日頃からの継続的な注意喚起が不十分であり、不審なメールを受信したことが年金事務所長等の情報セキュリティ責任者に報告されていないなど、これまでの研修等において、標的型攻撃に対する危機意識や対応方法が職員に徹底されていなかった。 ・流出事案の対応について、基本的な対応は担当者任せとなっており、システム部門担当理事等が具体的指示を行った事跡は確認できなかった。また、理事長等への報告も適時適切に行われない場合があり、組織として迅速な対応が行われていなかった。 ・標的型攻撃を受けた場合の各対応について、ＬＡＮケーブルの抜線以外に具体的なルールの定めがなく、その手順等を具体的に定めたインシデント対処手順書を定めていなかった。 ・流出した年金個人情報約125万件のうち、アクセス制限及びパスワードの設定を行っていたものが約68万件、パスワードの設定のみ行っていたものが約2万件、アクセス制限のみ行っていたものが約53万件となっていて、残りの約2万件については、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。 ・共有フォルダについては、パスワードをかけるなどの運用ルールが全ての年金事務所等において本当に実行されているかなどの点検・確認が適切に行われておらず、運用ルール自体が有名無実化していた。 ○再発防止に向けた今後の取組 ・機構ポリシーは、標的型攻撃に対する対応の必要性等に関する記述はあったものの、標的型攻撃に対する実施すべき基本的な対策に関する事項等の記載が不足していた。
8月21日	検証報告書	流出事案に関し、原因究明、再発防止策を検討することを目的として、厚生労働大臣から委嘱された検証委員会により取りまとめられた報告書 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検証委員会	○検証委員会が認定した事実 ・サイバー攻撃等のインシデント発生時の緊急時対応については、機構にＣＳＩＲＴの制度が設けられていなかったほか、流出事案のような事態を想定した厚生労働省との緊急連絡体制も定められていなかった。 ・アクセス制限もパスワード設定もなされていないまま共有フォルダに保管されているファイルが存在し、また、必要がなくなった年金個人情報がそのまま残置されているケースが認められた。 ・機構の内部監査においては、外部からの攻撃を想定した情報セキュリティ対策は監査対象とされていなかった。 ・機構ＬＡＮシステムの情報セキュリティ態勢に対する厚生労働省の監督体制は有効に機能していたとはいえず、流出事案発生の前後のいずれにおいても適切な監督が行われなかった。 ○標的型攻撃と情報流出の原因 ・機構において、標的型攻撃に適切に対応するためには、しかるべき責任者による指揮の下、組織内外の専門的知見を随時活用して組織を挙げた対応を行うことができる人的体制を整備するとともに、具体的な対応に関する手順書等のマニュアルを整備しておくことが不可欠であるが、そのいずれにおいても対応が不十分であった。 ○再発防止策の提言

(注)　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

検証報告書等によれば、機構において、職員への標的型攻撃に対する注意喚起や対応方法の周知徹底が研修等で行われておらず、職員が不審なメールを受け取った場合でも、年金事務所長等の情報セキュリティ責任者に報告されていなかった。また、機構ポリシーには、標的型攻撃への対応の必要性等については記載されていたものの、実施すべき基本的な対策事項等については十分な記載がなかったとされている。そして、流出事案を発生させた直接的な要因は、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、政府の情報セキュリティ対策推進会議においてＣＳＩＲＴ(注4)の体制を整備することが求められたことを受けて、25年2月にＣＳＩＲＴ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4）　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。

(3) 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、リスク認識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。）を取りまとめて、図表4のとおり、27年9月18日に公表している。

図表4　厚生労働省が取りまとめた組織・業務改革報告書の概要

年月日	報告書の位置付け	再発防止の主な取組
平成27年9月18日	検証委員会の報告書等の指摘を踏まえ、厚生労働省が定めた再発防止策	○厚生労働省における情報セキュリティ対策の強化 ・組織的対策（体制強化、情報共有） 　インシデント対応を含む情報セキュリティ対策の実務部門の強化として情報セキュリティ対策室（仮称）を設置する。 ・最高情報セキュリティ責任者（ＣＩＳＯ）、ＣＳＩＲＴ体制の見直しと即応性の向上、権限の強化の観点からＣＩＳＯ、ＣＳＩＲＴ体制を見直す。 ・人的対策（意識改革、人材育成） 　情報セキュリティ対策室（仮称）に外部の専門家を常勤で配置し、インシデント発生時には、即座に技術的な助言ができる体制を整備する。 ・業務運営対策（ルールの見直し、徹底） 　不審な電子メールの開封等は防ぎきれないという前提のもと、厚労省ポリシー及びインシデント対処手順書の見直しを行う。 ・技術的対策（情報システムの強化） 　各種ウィルスの侵入を検知する入口対策に加え、標的型攻撃を早期に検知するための内部、出口対策を強化する。 ○厚生労働省と機構の関係の強化 ・厚生労働省の機構に対する指導監督の強化 　機構においてルールに定められた情報セキュリティ対策が現場では必ずしも実行されていないことが明らかになったことから、年金局事業企画課監査室について、これまでのシステム監査担当に加え、それ以外の業務監査担当も機構に常駐することとし、厚生労働省の機構に対する監査等を強化する。 ○厚生労働省所管法人等に対する監督と情報セキュリティ対策の強化 ・教育訓練の実施 　厚生労働省が行う職員等の教育訓練については、厚生労働省所管法人等にも情報共有し、適切な教育訓練が行われているかどうか専門家による監査（助言）を行う。 ・リスク評価を踏まえた情報管理の徹底と監査（助言）の実施 　厚生労働省所管法人等において個人情報等の管理が適切になされているか、設定されたルールが適切に遵守、運用されているかなどについて、情報セキュリティ対策室（仮称）が情報セキュリティのＰＤＣＡの観点から監査（助言）を行う。

一方、機構は、27年9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、図表5のとおり、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しているほか、監査部に関する業務を機構の理事長が直接掌理することとするなどの組織改革を実施したとしている。

図表5　機構が策定した業務改善計画の概要

年月日	計画の位置付け	再発防止の主な取組
平成27年 12月9日	厚生労働大臣からの業務改善命令に基づき、機構が厚生労働省に提出した改善計画	○組織の一体化・内部統制の有効性の確保 組織改革、人事改革及び業務改革を進めることにより、内部統制の有効性を確保する。 ○情報開示の抜本的な見直し 情報開示と共有を促進し、透明性を確保し、お客様に安心いただける組織をつくる。 ○情報セキュリティ対策の強化について 組織面、技術面及び業務運営面から対策を強化することにより、年金個人情報を確実に保護する。 (1) 情報セキュリティ対策①～組織面～ ・情報管理対策本部の設置 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の強化を図るため、理事長を本部長とした情報管理対策本部を27年10月に設置した。 ・情報管理対策室の設置 情報管理対策本部の下で情報セキュリティ対策を確実に実施するため、情報管理対策室を27年10月に設置した。 ・機構ＣＳＩＲＴの設置 情報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を27年10月に設置した。 ・最高情報セキュリティアドバイザーの設置 情報セキュリティ対策の推進に係る助言等を行う高度な専門的知識・経験等を有する者を設置する。 (2) 情報セキュリティ対策②～技術面～ ・オンラインシステム オンラインシステムの領域に年金個人情報専用の共有フォルダを設置して管理・運用し、共有フォルダへのアクセスは生体認証により管理する。 ・機構ＬＡＮシステム 機構ＬＡＮシステムはインターネット環境から切り離したシステムとし、個人情報の保護強化の観点から、窓口専用ＰＣから機構ＬＡＮシステムの機能を利用する場合は業務上必要な機能に限定する。 ・インターネット環境 年金個人情報に対してインターネットからの攻撃が及ばないよう、オンラインシステム及び機構ＬＡＮシステムから切り離し、防御対策を講じた安全性の高いシステムを構築する。 ・ねんきんネットシステム 情報セキュリティの強化を図るため、多重の防御対策を整備する。 (3) 情報セキュリティ対策③～業務運営面～ ・情報セキュリティポリシーの改正等 体制の整備、標的型攻撃対策等、厚労省ポリシーに準拠しつつ、実効性のある内容に改正するとともに、インシデント発生時の具体的な手順を明確に規定したインシデント対処手順書を策定する。 ・監査体制の整備 監査部に情報セキュリティに精通した専門チームを設置するなどして、情報セキュリティ対策の実施状況等に係る内部監査を強化する。

(4) 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5)が見込まれるとしている。

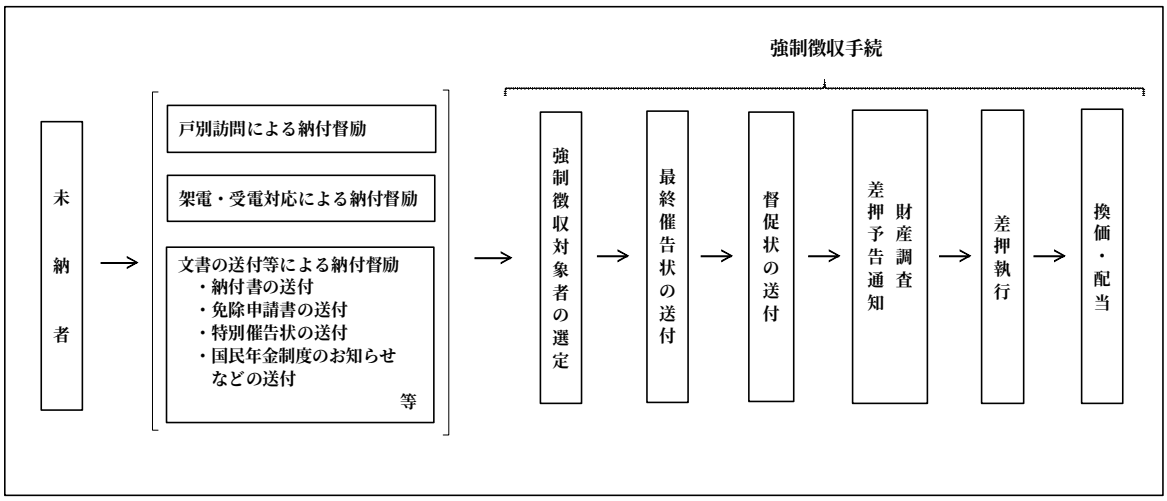
（注5） 約10億円　　平成28年1月8日衆議院予算委員会において行われた流出事案の対応に要する経費に関する厚生労働大臣の答弁による。

また、機構は、流出事案発生以前には、国民年金保険料の納付実績を向上させることなどを目的として、国民年金保険料の未納者に対して戸別訪問、架電、電話による問合せに対する対応（以下「受電対応」という。）、文書の送付等の納付督励業務を行っていた（図表6参照）。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、「競争の導入による公共サービスの改革に関する法律」（平成18年法律第51号）に基づき、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、国民年金保険料の未納者に対して戸別訪問、架電、受電対応、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、特別催告状の送付等を繰り返し行っても納付の意思を示さない未納者に対して、最終的な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、民間事業者が国民年金保険料の未納者に対して、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。

図表6　納付督励業務の概要



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、電話による被保険者等に対する保険料の納付督励等が不審電話と間違えられないようにする必要がある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、通知日以降、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、図表7のとおり、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。）。

図表7　一定期間行われなかった納付督励業務の内容等

業務名		区分	行われなかった期間	業務の詳細
納付督励業務	機構納付督励業務	一定期間行われなかった業務	27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	・戸別訪問による納付督励 ・架電による納付督励 ・文書の送付等による納付督励 　納付書の送付 　特別催告状の送付 ・強制徴収手続 等
		継続して実施していた業務		・受電対応による納付督励 ・文書の送付等による納付督励 　免除申請書の送付 等
	市場化納付督励業務	一定期間行われなかった業務	27年6月2日から同年11月16日までの間	・戸別訪問による納付督励 ・架電による納付督励 ・文書の送付等による納付督励 　国民年金制度のお知らせなどの送付 等
		継続して実施していた業務		受電対応による納付督励

そして、行わないこととしていた納付督励業務については27年11月から再開したものの、厚生労働省では、同年9月から28年2月までの間の国民年金保険料の納付率（保険料納付対象月数のうち納付された月数の割合をいう。以下同じ。）は、1年前に同様の方法で集計した同月の納付率（以下「前年同月納付率」という。）を最大で1ポイント下回ったとしている。この理由について、同省は、同年6月から11月までの約5か月間、納付督励業務の一部を行わなかったことによる影響等を挙げている。一方、同省では、27年度の最終的な納付率は、26年度の納付率63.1%を上回る63.4%になったとしている。この理由について、同省は、当該業務を再開した後、特別催告状の送付等の取組を強化したことなどを挙げている。

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。また、納付督励業務の一部を中止した影響により、27年9月から28年2月までの間の国民年金保険料の納付率は、前年同月納付率を下回っていた。そして、厚生労働省及び機構は、流出事案に関する事実関係、発生原因等について詳細に取りまとめられた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、会計検査院は、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6)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、契約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7)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6）　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7）　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

前記のとおり、機構ポリシーは、厚労省ポリシーに準拠して定められたもので、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。そして、厚労省ポリシーの27年4月28日の改正では、直近の統一基準の改正で標的型攻撃対策の強化が盛り込まれたことから、標的型攻撃に備えて実施すべき基本的な対策事項等が追加されている。

厚労省ポリシーの改正については、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。）が所掌している。そして、機構は、同省所管法人であることから、従来、

機構の監督部局である同省年金局（以下「年金局」という。）を通じて、厚労省ポリシーの改正に関する情報を入手している。

そこで、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、図表8のとおり、厚労省ポリシーの改正から一定の期間を要しており、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。

図表8　流出事案の発生前における厚労省ポリシー及び機構ポリシーの改正の状況

厚労省ポリシーの改正年月日	厚労省ポリシーに準拠するための機構ポリシーの改正年月日	厚労省ポリシーの改正から機構ポリシーの改正までに要した期間
平成23年8月25日	24年4月1日	約7か月
25年2月28日	25年8月9日	約5か月
27年4月28日	27年12月28日	8か月（注）

(注)　機構は、機構ポリシーの改正が、厚労省ポリシーの改正から8か月遅れているのは、流出事案の発生を踏まえて、統一基準及び厚労省ポリシーへの準拠性等を確認するなどしていたためであるとしている。

機構ポリシーが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点について、情報参事官室は、統一基準等の改正があった場合、機構を含む各所管法人等においては、自らその統一基準等の改正内容等を確認するなどしてそれぞれの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、機構ポリシーの改正に当たり、機構が年金局を通じて厚労省ポリシーの改正内容等に関する情報を入手して以降にその改正作業を行っているとは認識していなかったとしている。また、年金局は、機構に対して厚労省ポリシーの改正内容等に関する情報を提供していたものの、機構ポリシーの改正の時期や内容について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、機構法第48条第1項の規定等に基づき、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。そして、情報セキュリティ監査の内訳は、機構本部を対象とした全般的な監査が4回及び特定項目（磁気媒体の管理状況等。以下同じ。）の監査が8回、また、年金事務所等を対象とした特定項目の監査が170回となっていた。

上記のうち機構本部を対象とした全般的な情報セキュリティ監査は、4回とも22年度から24年度までの間に実施されたものであり、25年度以降、機構本部に対しても年金事務所等に対しても実施されていなかった。その理由について、監査室は、25年度以降に機構に対して実施したシステム監査及び情報セキュリティ監査では、機構が行ったシステム監査及び情報セキュリティ監査の有効性を確認するという監査手法を採ったためであるとしている。

また、監査室は、機構本部及び年金事務所等における共有フォルダの管理状況等に対しては、情報セキュリティ監査を実施していなかった。その理由について、監査室は、従来のシステム監査及び情報セキュリティ監査は、オンラインシステムを主な対象として実施していたためであるとしている。

さらに、前記のとおり、厚生労働省は、インシデント対処手順書を策定し、ＣＳＩＲＴを設置しているが、機構はこのいずれも行っていなかった。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

機構の「日本年金機構内部監査規程」（平成22年規程第14号）によれば、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。機構の内部監査には、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。そして、情報セキュリティ監査の内訳としては、機構本部を対象とした全般的な監査が2回及び特定項目の監査が14回、また、年金事務所等を対象とした特定項目の監査が1,441回となっていた。

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。

(ｳ) 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。

そして、検証報告書等によれば、同省は、流出事案の発生する前月の27年4月22日、年金局等において流出事案と類似の標的型攻撃を受けていたのに、機構に対してその情報を伝えておらず、機構に対しても同様の標的型攻撃が行われる可能性があるなどの注意喚起等を行っていなかったとされている。

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8)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。このうち、大手前年金事務所においては、計22ファイル、3,790件の年金個人情報が専用ＰＣのハードディスクに保存されていたことから、これらの年金個人情報の保存履歴等について確認したところ、計16ファイル、2,464件については、流出事案の発生前（25年8月等）から28年6月の会計実地検査時まで継続して専用ＰＣのハードディスクに保存されていた。専用ＰＣは、流出事案発生時点までインターネットに接続されており、そのハードディスクに保存されていた年金個人情報が外部に流出する危険性は、共有フォルダに保存されている年金個人情報と同様であったと認められる。

そこで、28年6月に会計検査院は、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会計検査院に報告した。以上のことから、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の有無及びその件数については不明な状況となっている。

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いて現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8）　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は、図表9のとおり計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。

図表9　機構が流出事案の対応に要する経費としたものの支出額（平成27年度決算額）

費目	金額（千円）
専用コールセンター対応経費	367,612
お知らせ・おわび文書の作成・送付経費	138,475
チラシ等の作成、配布経費	20,208
基礎年金番号の変更に要する経費	505,287
なりすまし防止対策経費	37,152
休日相談に係るオンラインシステムの稼働経費等	15,057
計	1,083,793

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及びその支出額についてみたところ、図表10のとおり、上記以外の経費も見受けられ、支出額は計4730万余円となる。

図表10　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（平成27年度末現在）

費目	金額（千円）
機構ＬＡＮシステム上の共有フォルダに保存されている電子ファイル内に年金個人情報等が存在しているかどうかなどについて調査するための経費	34,550
共有フォルダに保存されている電子ファイル内の年金個人情報等に関するデータに対するアクセス権の設定状況について調査するための経費	11,873
「不正アクセスによる流出事案に関する調査結果報告」の作成経費	885
計	47,309

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、流出事案の発生を踏まえて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、図表11のとおり、流出事案の発生の対応に要する経費に充てるために各種の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。

図表11　機構が流出事案に対応する経費に充てるためにねん出したとする財源の状況（平成27年度末時点）

費目	金額（千円）
年金事務所の新築移転の整備計画の見直し	497,229
庁舎・宿舎の整備計画の見直し（整備中止）など	410,926
事務経費の節減	194,605
計	1,102,760

ウ　おわび文書の送付等の状況

おわび文書、基礎年金番号変更通知等の送付状況等についてみたところ、次のような状況となっていた。

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や戸別訪問等によりおわび文書を届けることができた者等の計972,539人を対象として、基礎年金番号の変更処理を行い、その処理結果については順次、基礎年金番号変更通知等を簡易書留郵便で送付して

いる。そして、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（うち年金受給者計6,988人）については、今後、年金事務所等に来訪したときに、流出事案について説明した上、基礎年金番号変更通知等を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、年金支給を適切に行うため、年金受給者の生存又は死亡の事実（以下「生存等の事実」という。）について、住基情報等により確認している。また、年金受給者が施設に入所していることなどによりその所在を確認できず、住基情報等によっても生存等の事実が確認できない場合には、毎年、現況届の提出を受けて確認している。

そして、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等の事実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、戸別訪問の実施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、おわび文書及び基礎年金番号変更通知等の返送後の住基情報による確認、市区町村に対する照会や戸別訪問の実施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。

機構においては、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、27年度の行動計画によれば、26年の所得控除後の所得が400万円以上であり、かつ国民年金保険料の未納月数が7か月以上の者については、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9)下の77年金事務所が送付した15,812件について、会計検査院において、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。

試算に当たっては、上記15,812件のうち、強制徴収手続を行わないこととした27年6月8日以前の一定期間内（同年4月1日以降）に最終催告状を送付したものについては、行動計画等に基づき最終催告状を送付した翌々月に督促状を送付したと仮定し、行動計画等によれば強制徴収手続を行わないこととした期間に最終催告状を送付する予定となっていたものについては、最終催告状を送付する月の翌々月に督促状を送付したと仮定するなどした。その結果、図表12のとおり、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。

（注9）　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

図表12　消滅時効期間が経過した国民年金保険料の債権額等（会計検査院試算額）

都府県名	人　数 （人）	消滅時効期間が経過した月数 （月）	左に係る国民年金保険料の債権額 （千円）
宮城	214	376	5,527
埼玉	454	645	9,640
千葉	724	1,392	20,777
東京	842	1,469	22,052
神奈川	379	983	14,697
静岡	510	988	14,460
愛知	302	471	6,952
大阪	362	604	8,937
兵庫	130	392	5,801
福岡	455	839	12,306
計	4,372	8,159	121,154

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、図表13のとおり、3,769か月分、5659万余円となる。

図表13　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納付されたと考えられる国民年金保険料の債権額等（会計検査院試算額）

都府県名	人　数 （人）	消滅時効期間が経過した月数 （月）	左に係る国民年金保険料の債権額 （千円）
宮城	80	138	2,075
埼玉	285	419	6,301
千葉	328	599	8,997
東京	447	703	10,561
神奈川	160	380	5,715
静岡	286	527	7,873
愛知	144	213	3,203
大阪	184	283	4,256
兵庫	59	186	2,797
福岡	191	321	4,812
計	2,164	3,769	56,595

(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。そして、27年度における効果率は、未納者の属性別に0.36月から2.79月までとなっている。

特別催告状が送付された者に対しては、その他の納付督励業務も実施されており、機構は、未納者が国民年金保険料を納付した直接の契機が特別催告状であるのか、その他の納付督励業務の実施によるものかについては区別していないとしている。また、前記のとおり、厚生労働省では、納付督励業務を再開した後、特別催告状の送付等の取組を強化したことなどにより、27年度の納付率は、26年度の納付率を上回ったとしている。

しかし、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、会計検査院において、27年度の特別催告状の当初の送付計画数と送付実績数の差にそれぞれの属性別の効果率を乗ずることにより、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、図表14のとおり、計759,967か月分、計118億4788万余円となる。

図表14　収納されたことが見込まれる国民年金保険料の額等（会計検査院試算額）

属性	当初計画数(件) (A)	実績数(件) (B)	差引(件) (C)=(A)-(B)	効果率(月) (D)	収納されたことが見込まれる国民年金保険料の月数(月) (E)=(C)×(D)	左に係る国民年金保険料の額(千円) (E)×27年度の1月当たりの保険料(15,590円)
平成27年度の強制徴収対象者の選定において、免除等の申請を行った場合に承認されると見込まれ、最終催告状の送付対象から除かれた者で、免除等の申請を勧奨しても申請のない者	49,537	34,826	14,711	1.96	28,833	449,506
市場化納付督励業務によっても、納付の意思を示さない、控除後所得400万円以上かつ未納月数4月以上6月以下の者	78,153	57,418	20,735	2.79	57,850	901,881
市場化納付督励業務によっても、納付の意思を示さない、控除後所得350万円以上400万円未満かつ未納月数7月以上の者 市場化納付督励業務によっても、納付の意思を示さない、控除後所得200万円以上350万円未満かつ未納月数7月以上の者	787,049	470,680	316,369	1.11	351,169	5,474,724
控除前所得57万円以下の未納者に対する免除等の申請を勧奨した後、市場化納付督励業務によっても申請のない者	900,832	822,916	77,916	0.36	28,049	437,283
20歳以上23歳未満の3月以上の未納期間を有する者	750,184	784,150	△ 33,966	0.50	△ 16,983	△ 264,764
23歳以上30歳未満の3月以上の未納期間を有する者	1,513,233	1,615,255	△ 102,022	0.65	△ 66,315	△ 1,033,850
控除前所得57万円以上の未納期間を有する者	457,004	449,787	7,217	0.49	3,536	55,126
30歳以上の10月以上16月以下の未納期間を有する者	906,417	724,141	182,276	0.96	174,984	2,728,000
30歳以上の17月以上の未納期間を有する者	1,661,436	1,452,866	208,570	0.54	112,627	1,755,854
30歳以上の4月以上9月以下の未納期間を有する者	1,949,330	1,869,499	79,831	1.08	86,217	1,344,123
計	9,053,175	8,281,538	771,637		759,967	11,847,885

イ　業務委託中止期間を含む委託費の支払

機構は、図表15のとおり、26年度に、6民間事業者との間で26年10月から29年9月までを委託期間とする契約10件、27年5月から30年9月までを委託期間とする契約13

件、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。

図表15　市場化納付督励業務委託契約の締結状況

民間事業者名	件数	契約金額（千円）
株式会社アイヴィジット	6	6,597,720
日立トリプルウィン株式会社	8	6,390,014
株式会社バックスグループ	5	6,069,540
キャリアリンク株式会社	1	966,600
アイティフォー シー・ヴィ・シー共同企業体	2	958,392
東京ソフト株式会社	1	521,640
計	23	21,503,906

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

前記のとおり、厚生労働省は組織・業務改革報告書を取りまとめて27年9月に公表し、また、機構は業務改善計画を策定し同年12月に厚生労働大臣に提出しており、それぞれ情報セキュリティ対策等を強化し、流出事案の再発を防止するための取組を行っている。

そこで、これらの厚生労働省及び機構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、次のとおりとなっていた。

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、図表16のとおり、厚生労働省は、同省の情報セキュリティ対策を向上するために、サイバーセキュリティについて専門的に対応するための組織改革、厚労省ポリシー等の見直し、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。

また、厚生労働省は、機構への指導等の強化について、27年10月から機構の経営企画部に職員を常駐させ、業務についてのモニタリングを実施しているほか、機構ポリシー等の情報セキュリティに関する諸規程等の整備を一元的に所掌している情報管理対策室に、28年7月から年金局の職員を常駐させ、これらの規程やインシデント対処手順書の整備状況や改正内容についての確認を行うなどしていた。

そして、厚生労働省は、機構への監査の強化について、監査室が行う監査の範囲を機構の全ての情報システムとする見直しを行い、27年11月から監査を行うとともに、28年9月に厚生労働省及び機構の職員によって構成される連絡会議を設置し、双方の監査で把握した情報セキュリティに関する課題の確認やその改善計画の進捗状況のフォローアップを行うこととした。

図表16　厚生労働省における再発防止の取組の進捗状況

組織名	主な項目名		左の進捗状況
厚生労働省	○厚生労働省における情報セキュリティ対策の強化	組織的対策（体制強化、情報共有）	インシデント対応を含む情報セキュリティ対策の実務部門を強化するため、平成27年10月に情報セキュリティ対策室（室長は企画官級）を設置した。 その後、サイバーセキュリティについて専門的に対応する体制を強化するため、28年6月に同室を廃止して、新たにサイバーセキュリティ担当参事官（課長級）を設置するとともに、サイバーセキュリティ・情報化審議官を設置していた。
		人的対策（意識改革、人材育成）	インシデント発生時に即時に技術的な助言ができるよう、28年3月から、順次、外部専門家を常勤として雇用（計4名）し、うち1名を同年4月から最高セキュリティアドバイザーに任命していた。
		業務運営対策（ルールの見直し、徹底）	27年10月及び12月に、厚労省ポリシー及びインシデント対処手順書の見直しを行っていた。
		技術的対策(情報システムの強化)	統合ネットワーク等のセキュリティを強化するため、27年度補正予算で4.1億円、28年度当初予算で22.3億円を計上し、高度な標的型攻撃に対する多重防御対策のためのシステム改修を順次実施するなどしていた。
	○厚生労働省と機構の関係の強化		・機構に対する指導等の強化を図るため、機構の経営企画部に職員を常駐させ、業務のモニタリングを実施しているほか、機構ポリシー等の情報セキュリティに関する諸規程等の整備を一元的に所掌している機構の情報管理対策室に、28年7月から年金局の職員を常駐させ、これらの規程やインシデント対処手順書の整備状況やその改正内容についての確認を行うなどしていた。 ・27年9月に監査室の監査範囲の見直しを行い、システム監査及び情報セキュリティ監査については、機構ＬＡＮを含む全ての情報システムを対象とすることに拡大し、同年11月以降監査を実施していた。 ・28年9月に厚生労働省及び機構の職員で構成される連絡会議を設置し、双方の監査で把握した情報セキュリティに関する課題の確認やその改善計画の進捗状況のフォローアップ等を行うこととした。
	○厚生労働省所管法人等に対する監督と情報セキュリティ対策の強化・教育訓練の実施		27年度補正予算で8.5億円を計上し、セキュリティ監査体制を強化して、厚生労働省が保有する情報システム及び所管法人等に対してセキュリティ監査等を実施することにしていた。

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、図表17のとおり、機構は、同年4月に最高セキュリティアドバイザーを設置するとともに、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。

そして、機構は、27年10月に新設された機構ポリシー等の情報セキュリティに関する諸規程等の整備を情報管理対策室が一元的に所掌した上で、厚労省ポリシーに準拠した機構ポリシーの改正を同時期に実施するとともに、28年2月にインシデント対処手順書を策定していた。また、機構は、情報セキュリティ対策に関する各種ルールに対する職員の理解を深め、確実に遵守させるため、同年8月に、職員が業務上守るべき主な事項やインシデント発生時の対応等が記載された手引を策定して配布するとともに、同年9月に全職員の受講を必須とした情報セキュリティ研修を開催した。

機構は、28年4月に情報セキュリティ監査の専門チームを設置し、情報セキュリティ監査の監査体制を整備していた。

図表17　機構における再発防止の取組の進捗状況

組織名	主な項目名		左の進捗状況
機構	○情報セキュリティ対策① ～組織面～	最高情報セキュリティアドバイザーの設置	平成28年4月に、公募により専門的知識・経験を有する外部専門家1名を設置していた。
	○情報セキュリティ対策② ～技術面～	オンラインシステム	28年度当初予算において17.1億円を計上し、年金個人情報を管理・運用する領域をインターネットから完全に分離した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。
		機構ＬＡＮシステム	
		インターネット環境	
		ねんきんネットシステム	
	○情報セキュリティ対策③ ～業務運営面～	情報セキュリティポリシーの改正等	27年10月に新設された機構ポリシー等の情報セキュリティに関する諸規程等の整備を情報管理対策室が一元的に所掌した上で、厚労省ポリシーへの準拠性や機構の実態への整合性を確認するなどし、流出事案の発生を受けて27年12月に実施された厚労省ポリシーの改正に準拠して、同月機構ポリシーを改正していた。 また、28年2月、インシデント発生時の具体的な手順を明確に規定したインシデント対処手順書等を策定していた。
		情報セキュリティ研修等の実施	情報セキュリティ対策に関する各種ルールに対する職員の理解を深め、確実に遵守させるため、28年8月に、職員が業務上守るべき主な事項やインシデント発生時の対応等が記載された手引を策定して配布するとともに、同年9月に全職員の受講を必須とした情報セキュリティ研修を開催した。
		監査体制の整備	28年4月に、情報セキュリティ監査の専門チームを設置し、監査体制を強化していた。

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、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、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していたのに、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、26年8月に内部監査の実施の要否を検討するための事前調査において、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、経営企画部では共有フォルダ要領を制定するなどしていたのに、監査部では、この改善要請は内部監査の結果ではないなどとし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、流出事案の発生する前月の27年4月22日に年金局等に対して流出事案と同様の標的型攻撃が行われていたのに、年金局では、統合ネットワークを使用している機構に対して、その事実を伝えておらず、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た。

そこで、会計検査院は、機構に対して、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等について調査し、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、28年8月から同年9月までの間に、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会計検査院に報告した。以上のことから、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の有無及びその件数については不明な状況となっている。また、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た。

上記のほかに、共有フォルダに保存されている電子ファイル内に年金個人情報が存在しているかどうかを調査するための経費等が見受けられた。また、厚生労働省でも、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、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。

(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、住基情報による確認、市区町村に対する照会や戸別訪問の実施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) 機構は、流出事案の発生に対応するため、強制徴収手続については、最終催告状及び督促状の送付を含め、27年6月から約5か月の間、行っていなかった。

そこで、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、前記約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、サイバーセキュリティについて専門的に対応するための組織改革、厚労省ポリシー等の見直し、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、機構は、同年4月に最高セキュリティアドバイザーを設置するとともに、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、会計検査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。会計検査院は、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。