平成 28 年４月 28 日

サイバーセキュリティ戦略本部長　菅　　義　偉　殿

厚生労働大臣　塩　崎　恭　久

平成 27 年９月 11 日になされた勧告の履行状況について、別紙のとおり報告する。

別紙

報　告

平成 27 年５月の日本年金機構（以下「機構」という。）における情報流出事案は、「まれにみる組織的かつ執拗な（標的型）攻撃」（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（以下「検証委員会」という。）検証報告書）が原因であるとはいえ、これに対する構えは、機構のみならず厚生労働省（以下「厚労省」という。）においても極めて脆弱であった。国民の共同連帯の理念に基づき国民の信頼を基礎として実施されるべき政府管掌年金事業において、約 125 万件もの個人情報が流出したことは、国民の年金制度に対する信頼を損なうものであり、極めて遺憾である。

本事案については、平成 27 年８月 20 日に機構が調査結果報告を、サイバーセキュリティ戦略本部（以下「戦略本部」という。）が原因究明調査結果を、また、同年８月 21 日に検証委員会が検証報告書をそれぞれ公表した。その後さらに、政府全体のサイバーセキュリティ体制の抜本強化を図るサイバーセキュリティ戦略が同年９月４日に閣議決定され、また、同年９月 11 日に、戦略本部の本部長である官房長官から厚生労働大臣に対して、戦略本部の原因究明調査結果等を踏まえた勧告がなされた。これらの報告書等においては、本事案の根本原因として、①厚労省、機構ともに標的型攻撃の危険性に対する意識が極めて不足しており、事前の人的体制と技術的な対応も全く不十分であったこと、②インシデント発生後においては、現場と幹部の間、関連する組織間に情報や危機感の共有がなく、組織が一体として危機を克服する万全の体制になっておらず、その結果、数少ない組織内の専門知識を持つ者の動員すらできず、担当者が幹部の明確な指揮を受けることもないままに、場当たり的な対応に終始し、迅速かつ的確な対処ができなかったことが指摘されている。

厚労省は、これらの報告書等の指摘や戦略本部長の勧告を踏まえ、厚労省としての再発防止策を取りまとめ、平成 27 年９月 18 日に、「情報セキュリティ強化等に向けた組織・業務改革－日本年金機構への不正アクセスによる情報流出事案を踏まえて－」（別添１）を公表した。また、この再発防止策を迅速かつ確実に実施するため、同年 10 月１日付けで、厚生労働大臣を本部長とし、政務二役、事務次官、厚生労働審議官及び全局長から成る「情報セキュリティ強化等に向けた組織業務改革推進本部」を設置した。

一方、機構は、平成 27 年８月 20 日の調査報告書及び同年９月 25 日に厚生労働大臣から日本年金機構理事長に対して出された業務改善命令等を踏まえ、同年 10 月１日に理事長を本部長として機構内に設置した「日本年金機構再生本部」及び「情報管理対策本部」にお

いて、情報セキュリティ対策の強化を含む業務改善計画を取りまとめ、同年 12 月９日に、「日本年金機構業務改善計画」（別添２）を公表した。

厚労省及び機構においては、別添１及び別添２を踏まえ、組織的、人的、業務運営、技術的対策、それぞれの観点から、情報セキュリティ対策強化に向けた取組を進めるとともに、厚労省による機構その他厚労省が所管する独立行政法人、特殊法人等（以下「所管法人等」という。）に対する指導監督の強化に取り組んできたところである。これらの取組状況について、厚労省及び機構は、勧告の項目に沿って整理を行うとともに、勧告の実施により得られた成果に係る評価を実施した。これを基に、厚労省は、勧告の履行状況について、下記のとおり取りまとめたので、報告する。

厚労省及び機構においては、勧告等を踏まえつつ、引き続き、本事案を踏まえた再発防止策に全力を挙げて取り組んでまいる所存である。

記

１　体制整備

（１）厚労省における取組

①　組織・人的体制の強化

厚労省における情報セキュリティ対策に関する業務は、省内の情報政策の企画立案、連絡調整等を担当する部署である政策統括官付情報政策担当参事官室（以下「情参室」という。）の情報セキュリティ対策係が担当し、室長補佐以下４人の人員体制で、厚生労働省情報セキュリティポリシー等のルール整備、情報セキュリティに関する教育訓練、インシデント発生時等における NISC や省内担当部局との連絡調整等の業務を行ってきた。しかしながら、情報セキュリティ対策係は、インシデント対応以外の業務も兼務しているため、業務内容や業務量の多さに比べれば職員数が十分ではない。また、情報セキュリティの専門的知識を有する職員が常勤で配置されておらず、非常勤である CIO 補佐官に、最高情報セキュリティアドバイザー（インシデントアドバイザー）として、インシデント発生時の対応も含め、情報セキュリティ対策全般に係る技術的助言を依頼してきたが、CIO 補佐官はインシデント対応以外にも大規模情報システムの刷新業務等に関する支援業務など多くの業務を抱えていたため、今回の機構における情報流出事案（以下「情報流出事案」という。）では、情参室の担当者等と迅速に報告や相談を行うなど緊密な連携ができなかった。このように、情報セキュリティ対策を推進するための人的体制は全く不十分であった。

このため、まずは人的な体制強化を図るため、情参室の情報セキュリティ対策係を

拡充し、平成 27 年 10 月１日に、室長以下８人の職員から成る「政策統括官付情報セキュリティ対策室」を新たに設置した。これにより、情報セキュリティポリシー等のルール整備とそれに基づく教育、情報セキュリティ対策の PDCA（対策推進計画、自己点検、監査）等を担当する企画係と、インシデント発生時の NISC 等との連絡調整や、担当部局への技術的支援、対処指示等を担当する対策係の２つのラインで従来の業務を分担することとした。また、情報政策担当参事官に代わり、情報セキュリティ対策室長を最高情報セキュリティ責任者（CISO）を実務面で補佐する「統括情報セキュリティ責任者」とし、情報セキュリティポリシーや対策推進計画を決定する情報セキュリティ委員会（委員長：CISO）のメンバーとした。

これらの実務要員の体制強化と併せて、専門性向上の観点から、情報セキュリティに関する専門的知識及び経験を有する外部人材(情報セキュリティ対策官)を公募し、平成 28 年３月１日より２名、同年４月１日より２名の計４名を、情報セキュリティ対策室に常勤職員として採用した。また、このうち１名を、「統括情報セキュリティ対策官」として任命し、同年４月１日より、CIO 補佐官に代わり、最高情報セキュリティアドバイザーに指名した。これにより、インシデント対応も含め、情報セキュリティ対策に係る専門的な知見に基づく助言、支援が即時に行われるための一定の体制整備が図られた。さらに、同年４月１日より、情報セキュリティ対策室において、企画係、対策係のラインに加えて、監査を専門的に担当するラインの人員が拡充され、室全体で 20 人の体制となった。

② CSIRT の実効性のある体制強化

厚労省における情報セキュリティインシデント対応チーム（CSIRT）は、インシデント最高責任者を官房長、インシデント統括責任者を情報政策担当参事官、インシデント管理責任者をインシデント担当部局（情報システムの管理・運用部局）の総括課長、インシデント担当者を当該部局の課室長とする等、責任者のみで構成され、インシデント発生時には、CSIRT 内で、情参室と担当部局の責任者の間で報告、連絡が行われるというルールになっていたが、責任者は必ずしも情報セキュリティに関する専門的知見を有しているとは限らない中で、情参室と担当部局との間でインシデントへの対処に係る役割や責任の所在が不明確であった。一方、インシデント発生時における NISC 等との連絡調整や実際の対処に関する業務については、情報セキュリティ対策係が担当部局の課室の担当者との間で行っていたが、これらの実働要員は CSIRT 要員として選任されていなかった。そして、情報流出事案では、情参室、担当部局のそれぞれで、担当者から責任者に対する報告が迅速に行われなかったため、責任者を構成員とする CSIRT が実質的に機能しなかった。さらに、非常勤である CIO 補佐官が CSIRT のインシデントアドバイザーとなっていたが、情参室の担当者等と迅速に報告や相談を行うなど緊密な連携ができなかったことは前述のとおりである。

以上を踏まえ、CSIRT について、主として、即応性と専門性の向上、役割や責任の

明確化の観点から、実効性のある体制強化に向け見直しを行った。

・　厚労省では、CISO、CSIRT 責任者を共に大臣官房長としていたが、官房長は、厚労省全体の予算、人事、業務改革を統括する大臣官房の長として、一定の権限を有しているものの、情報セキュリティ対策は、政策統括官が所掌する情報政策（情報システム投資）と一体となって推進していく必要があることや、厚労省が保有する基幹システムは、大臣官房統計情報部が所管する厚労省統合ネットワークや厚労省 LAN システム以外にも、年金局（機構）、職業安定局（ハローワーク）、労働基準局（監督署）など担当部局が多岐にわたることなどから、情報セキュリティ対策の推進に当たっては、危機管理という観点からのトップマネジメントによる予算・人員の適切な配分に向けた、より一層の権限強化が必要である。一方で、インシデント発生時、特に初動対応においては、情報セキュリティ対策に専門的に従事する者が迅速に対応することが求められる。このため、CISO については、CIO と併せて官房長から厚生労働審議官（次官級）へと変更するとともに、CSIRT 責任者については、日常的に情報セキュリティや情報政策を担当している情報政策・政策評価審議官（副CIO）へと変更することとし、平成 27 年 10 月 1 日付けで厚生労働省情報セキュリティポリシー及びインシデント対処手順書の改定を行った。

・　CSIRT 内で情参室と担当部局との役割や責任の所在が不明確であることにより、インシデントへの迅速かつ的確な対処が損なわれることがあってはならない。このため、これらの間の役割分担を明確となるよう、CSIRT から担当部局（情報システムの管理・運用部局）を切り離し、技術的支援、対処処置に関する指示、勧告、対外的な連絡調整を行うのは CSIRT、実際にインシデントへの対処・復旧を行うのは担当部局として、それぞれの役割分担を明確にした。その上で、CSIRT については、インシデント責任者（情報政策・政策評価審議官）の下に、統括情報セキュリティ責任者（情報セキュリティ対策室長）以下、実際にインシデントの対処支援や、NISC や担当部局との連絡調整に関する業務を行う情報セキュリティ対策室の職員全員を CSIRT 要員とし、それぞれの役割や権限を明確にした。また、担当部局（対処・復旧部局）については、部局情報セキュリティ責任者（総括課長）、課室情報セキュリティ責任者（各課室長）のほか、実際の対処・復旧や、CSIRT や所管法人等との連絡調整に当たる課室情報セキュリティ管理者（各課室の庶務係長等）及び情報システムセキュリティ責任者をインシデント対応体制として位置づけ、それぞれの役割や権限を明確にした。

　その上で、インシデント発生時には、責任者のみならず担当者も含めた実務的な報告、連絡ルートを明確にし、担当部局の担当課室（課室情報セキュリティ責任者又はこれを補佐する課室情報セキュリティ管理者）からインシデント責任者、統括情報セキュリティ責任者、情報セキュリティ対策室員及び最高情報セキュリティアドバイザーから成る CSIRT に対して必ず報告すること、逆に、NISC 等から CSIRT（情

報セキュリティ対策室）に対してインシデント発生に関する通報があった場合には、CSIRT から担当部局及び政務３役、事務４役はじめ幹部に対して、速やかに連絡、報告することとした。また、担当課室においては、各部局の総括課長、部局の局長・審議官に対しては必ず速やかに報告するとともに、個人情報の流出の可能性が高い事案であって国民への影響が大きい場合等においては、政務３役、事務４役はじめ幹部に対して速やかに報告することとした。これらの見直しについては、平成 27 年 12 月 21 日付けで厚生労働省情報セキュリティポリシー及び情報セキュリティインシデント対処手順書を改定してルールを整備し、その内容を省内全職員に対して周知した。

また、情報流出事案では担当者から責任者に対して迅速な報告が行われず、幹部も含めて情報共有が適切に行われていなかったという反省に立ち、組織内の情報共有等に係る意識改革を図るため、平成 27 年度業務適正化推進月間（平成 27 年 10 月 19 日～11 月 13 日）等において、職員間の情報共有や職場のコミュニケーションの確保の徹底に関する研修や、幹部職員を対象とした組織管理に関する研修を実施するとともに、今回のポリシー等の改定を踏まえたインシデント発生時の速やかな報告、連絡体制の構築等について、サイバーセキュリティ月間（平成 28 年２月１日～３月 18 日）中に課室情報セキュリティ管理者等を対象とした研修を実施した。

③　今後の取組

上記のとおり、情報セキュリティ対策強化のための体制整備については、情報セキュリティ対策室の設置や専門的な知識・経験を有する外部人材（情報セキュリティ対策官）の配置、情報セキュリティポリシーの改定等、一定程度の成果を上げたところである。一方で、現在、省内の情報システムや情報セキュリティに関する機能は、情参室、大臣官房統計情報部、その他の部局に分散しているが、情報セキュリティ対策の強化に向け、情報システムの適切な管理運用とサイバーセキュリティ対策、業務改革等を省全体として整合的に進めていくことや、インシデント発生時に円滑な情報共有を図るためには、これらの機能を再集約、再編し、情報セキュリティ対策の司令塔機能を強化する必要がある。

このため、平成 28 年夏を目途に、情参室と、厚労省本省の情報システムの管理・運用を担当する大臣官房統計情報部を統合し、政策統括官（統計・情報政策担当）の下に、情報政策・政策評価審議官に代わって、CISO 及び CIO を補佐し、情報セキュリティ対策と情報政策を総合的・一体的に推進する「サイバーセキュリティ・情報化審議官」（副 CISO、副 CIO）を設置するとともに、その下に情報化推進・情報政策担当参事官、情報セキュリティ担当参事官を置くこととするなどの組織再編を行う予定である。

また、CSIRT（情報セキュリティ対策室）内において、情報セキュリティ対策官からの助言等に基づき、担当部局に対して的確な助言、指示を行うことができる人材、一

方、担当部局においても、CSIRT からの助言、指示等を的確に理解し、実行できる人材を確保、育成していくことが必要である。このため、職員のリテラシー向上のための研修を含め、情報セキュリティに関する教育プログラムの充実に取り組んでいく必要がある。また、今回の情報セキュリティポリシー等の改定を通じて、インシデント発生時の対応基盤としてのハード面（体制、ルール）の整備は図られたが、インシデント発生時に、ポリシーに基づく体制を有効に機能させることができるよう、全ての職員に対し、情報セキュリティに関する危機意識やサイバー攻撃への対処手順を浸透させる必要があり、実践的な訓練の実施などソフト面での対策強化も求められる。

これらを踏まえ、平成 28 年度においても、PDCA の観点からの自己点検、情報セキュリティ監査を引き続き実施するとともに、教育及び訓練の一層の充実を図ることとしている（「３　教育・訓練」参照）。さらに、職員のモチベーションの維持、向上にも配慮しながら、省内で一定の専門性を有する人材の育成に取り組んでいく必要があり、平成 28 年３月 31 日にサイバーセキュリティ戦略本部で決定された「サイバーセキュリティ人材育成総合強化方針」に基づき、厚労省においても、採用、人事交流、研修、キャリアパスの形成等に計画的に取り組む予定である。

さらに、CSIRT においては、実働要員として情報セキュリティ対策室員を位置付け、また、専門人材として情報セキュリティ対策官を常勤で配置したものの、インシデント発生時における対処のほか、平時におけるサイバー脅威に係る情報収集や CSIRT の対処能力向上のため、実働要員の対応能力を踏まえた専門技術的なサポートや、夜間、休日も含めた24時間365日での緊急即応体制を確保することが必要である。このため、平成 28 年度において、インシデント発生時等における CSIRT への緊急・専門的支援業務の外部委託を予定している。

（２）機構における取組

①　組織・人的体制の強化

機構においては、今回の事案の一連の対応において、CIO（システム部門担当理事）と情報セキュリティ担当部署の部長、グループ長及び担当者がラインとして対応していた。しかしながら、その対応体制について、以下の問題があった。

・　基本的な対応は担当者任せとなっており、CIO（システム部門担当理事）や部長が、当該担当者の判断について、判断根拠の確認や具体的指示を行っていなかった。
・　理事長、最高情報セキュリティ責任者（副理事長）への報告が適時適切に行われない場合があり、組織として迅速な検討が行われていなかった。
・　情報流出事案を対応してきたラインに情報セキュリティに関する専門的な知識及び経験を有する職員がおらず、ラインにおいて必要な対応・判断ができなかった。
・　情報セキュリティ担当部署と契約担当部署とが異なり、責任の所在が不明確で連携が不十分となっていた。また、これらの部署間の連携を図ること、あるいは組織

の統合を検討することは CIO（システム部門担当理事）の役割であったが、具体的な行動はとられていなかった。

また、機構は、管理する情報システムにおいて膨大な個人情報を取り扱っていながら、情報セキュリティ関連業務について全体を指揮・命令する権限を有する CSIRT 機能を持つ部署を設置していなかった。さらに、厚労省と機構との間における、事案発生後の情報共有が担当者レベルにとどまり、幹部レベルの情報共有、監督指示などが事案発生から相当の期間が経過するまで行われず、適切な対応を講じることができなかった。

このため、機構においては、情報セキュリティ対策を重要課題と位置付け、組織横断的な対応体制を確立するとともに、その解決に向け、迅速かつ的確な対策を実施することとし、平成 27 年 10 月１日より、理事長を本部長とし、各部門の理事等を本部員とした情報管理対策本部を設置した。そして、情報管理対策本部において情報セキュリティ対策の工程表を策定し、業務改善計画における情報セキュリティ対策の強化に係る指示や情報セキュリティに係る諸規程・手順書等の整備及び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を行った。また、情報管理対策本部の所掌事務の実施に関する事務をつかさどる理事長直轄の推進部署として、情報管理対策室を設置した。情報管理対策室には、情報管理グループ（情報管理対策本部の事務局、個人情報の保護・管理、情報セキュリティに係る研修及び訓練内容の企画等）、情報リスク分析グループ（リスクアセスメント調査・分析・評価、情報セキュリティに係る諸規程等の整備・運用・指導等）、インシデント対策グループ（平時における脆弱性調査・情報収集等、有事における発生事案の調査・分析・対応指示等）の３つのグループを置き、情報セキュリティの専門家からの指導・助言等を受けつつ、実効性のある対策を講ずるための体制を整備した。さらに、統括情報セキュリティ責任者（情報管理対策室長）の下に、情報セキュリティインシデントに係る連絡調整や情報管理対策本部が決定した方針を機構職員に適切に実行させるための指示･管理等を行う「機構 CSIRT」を設置し、機構内外から情報セキュリティインシデント事案等が発生したことの連絡の受付並びに当該事案等の迅速な本部長（理事長）、副本部長（副理事長）及び厚労省等への報告、最高情報セキュリティ責任者から情報セキュリティインシデントにかかる対応方針の指示を受けて、情報セキュリティインシデント対応にあたる機構本部の担当部署に必要な指示の連絡等を行う役割を担わせることとした。機構 CSIRT では、平常時においては、インシデント対策グループ職員により情報セキュリティに関する職員からの総合的な連絡窓口や厚労省等との連絡調整等の業務を行っているが、事案発生時には、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、インシデント対策グループ員以外の情報管理対策室職員及び関係部署からの支援要員（本部の即戦力のある職員に併任発令）を招集できる体制を確保している。

また、業務改善計画に基づく情報セキュリティ対策の実施内容等と合わせて、順次、日本年金機構情報セキュリティポリシー（以下「機構ポリシー」という。）、各種手順書等の改正等を進めている。機構ポリシーは、統一基準や厚生労働省情報セキュリテ

ィポリシーに準拠し改正を行うこととしており、それらに規定されている情報セキュリティ対策について、項目ごとに機構における取組の実情に照らし、適用の必要性等を検証の上、改正を実施した。さらに、緊急時に対処にあたる組織、役割分担のほか、運用管理業者におけるインシデント対応とも連動した職員による具体的な対処フローや機構内外の連絡体制を明確化したインシデント対処手順書を制定した。この他、インシデント発生時の連絡について、厚労省年金局と機構の連絡手順の整合性を図りつつ、インシデント発生時の連絡手順を定め、日頃から年金局と機構が綿密に連絡を取り合い、セキュリティインシデントに備えている。

② 今後の取組

上記のとおり、情報セキュリティ対策強化のための体制整備については、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とし、情報管理対策室、機構 CSIRT を設置したことは一定程度の成果を上げたところである。こうした体制は強化・拡充を進めているところであるが、これから、現場の職員一人一人まで、国民の重要な個人情報の保護に関する責任を自覚し、ルールの内容と、いざというときに自らが何をすべきかの理解を、迅速かつ徹底して深めていく必要がある。また、組織としてインシデントを予防し、適切に対応していくための専門的な視点による情報セキュリティ対策の司令塔機能を強化する必要がある。このため、機構においては、平成 28 年４月より、高度の専門知識・経験を基に、情報管理対策本部及び最高情報セキュリティ責任者（CISO）が情報セキュリティ対策の推進に係る意思決定を行うための助言や支援を行うことを目的として最高情報セキュリティアドバイザーを設置することとするとともに、情報管理対策本部、情報管理対策室及び機構 CSIRT の運営並びに施策等の網羅性及び有効性等の向上を目的として、情報セキュリティ専門家の立場から支援を行う情報セキュリティ対策専門の支援業者を設置することとしている。

２ 技術的対策

（１）厚労省における取組

① 標的型攻撃に対する多重防御対策

今回の情報流出事案では、インターネット接続環境下にある機構 LAN システムに対し、標的型メール攻撃による不正アクセスが行われ、共有ファイルサーバに保存していた個人情報の一部が流出した。この情報の中には、インターネットと論理的に分離している基幹系システムから、業務上、機構 LAN システムに移管され、削除されずにそのまま保管されていたものが含まれていた。

このように、情報システムにおいて、個人情報等の重要情報がインターネットに接続する環境に置かれる状況が生じないようにするためには、本来、業務プロセスにおける情報の適切な取扱いという観点から、そうした状況が発生しうるリスクを評価した上で、業務に応じた情報管理対策をシステムの企画、設計の段階から講じていくことが必要である。

こうした考え方に立脚しつつ、一方で、厚労省の業務内容及びそれに応じたシステムは膨大かつ多様でありリスク評価に基づいたシステム構築には一定の時間を要することから、まずは、緊急的な対応として、個人情報等の重要情報を取り扱うシステムについて、インターネットから物理的又は論理的に分離し、当該情報をインターネットで利用しないこととする措置を講じた（平成 27 年 9 月）。このうち、厚労省 LAN システムで運用していた個人情報等については、インターネットから物理的に切り離した暫定的なスタンドアロン端末を設置し管理することとした。その後、業務単位で関係者が個人情報等を共有できるネットワークを構築し、それを前提とする個人情報等管理端末を暫定端末に代えて設置し、全職員に対して運用上のルールについて周知徹底を図った（平成 28 年 1 月）。平成 28 年度においては、その運用管理に当たり、情報漏えい対策の更なる強化に取り組む予定である。

一方、厚労省が保有する各システムや機構の情報系システムが接続され、これらのシステムのインターネット接続口となっている厚労省統合ネットワークについては、標的型メールのような外部からの攻撃を完全に防御することはできないことを前提に、攻撃を受けても早期に認知、対応し、実際の被害を最小限に止めるための措置を講じる必要がある。このため、標的型攻撃によるウィルスの侵入を低減する入口対策をこれまで講じてきたが、これに加えて、平成 28 年度においては、情報ネットワーク及び情報システムへの侵入拡大や不正な通信をリアルタイムで監視し適正に遮断する機能の導入を始めとする内部、出口対策も含め、標的型攻撃に対する多重防御対策を強化する予定である。この一環として、複数の機器からの不審な通信に係る証跡情報を収集、解析した上で自動遮断を行う運用を平成 28 年度当初より暫定的に開始したところであり、今後、専門人材の助言も受けながら、自動遮断の基準を策定する予定である。

これらの対策は、適切な運用が行われることを前提に、一定の効果が発揮されるものである。また、インシデント発生時の対応を含め、統合ネットワークとこれに接続するシステムとの間で、漏れや重複が無いように対策が行われるよう十分な連携を図っていくことも必要であり、今後、日常的なコミュニケーションの確保や実践的なインシデント訓練の実施が求められる。

② リスク評価

厚生労働行政においては、情報システムの利活用が業務運営に不可欠となっている現在、自らの組織が取り扱っている情報の重要性（情報資産の価値）や当該情報を活

用した業務運営において生じ得るリスクを正しく認識、評価した上で、実現可能な業務プロセスやルール等の業務基盤を整備し、業務が円滑に行われるよう、人的資源の再配置や業務運営に必要な人材の育成を行っていくことが必要である。その際、幹部職員を含む全職員が日常業務を遂行する上で、セキュリティを常に意識できる環境を整えるとともに、業務上取り扱っている情報について、漏えい、改ざん、消失等があった場合のインパクトについて職員自らが意識を持つことが重要である。特に、幹部職員においては、こうした情報セキュリティに関する意識改革だけでなく、業務全体にわたる改善に向けたマネジメント面の意識改革も必要であり、平成 27 年度においては、幹部職員を対象として、マネジメント、生産性向上、働き方の見直し、優先順位の明確化、求められる管理職像等を内容とする研修を実施したところであり、こうした研修は今後継続して実施していくことが必要である。

また、緊急的な対策として個人情報等の重要情報をインターネット接続環境から分離したことにより、サイバー攻撃による情報セキュリティに係るリスクは低減された一方で、業務上の利便性が損なわれ、オペレーションによる同リスクが顕在化する可能性もある。省内の業務、情報システム、情報セキュリティの各担当部局が協働して、リスクを最小化できるよう、省内システムの構築、運用及び業務プロセスの改善に取り組んでいくことが必要である。

このため、平成 28 年度より、厚労省が保有する個人情報等の重要情報を取り扱うシステムや当該情報を取り扱う業務プロセスの現状を把握し、それぞれの実態やリスクを組織的に共有し、業務内容に応じたシステム上、業務運営上の情報管理対策を講じるための一連の取組を「リスク評価」として実施することとしている。その際には、当該情報そのものの価値や業務プロセスに内在する脆弱性について分析し、リスクの特定、抽出を行うこと、インシデント発生時の影響度やリスクの発生確率等について分析を行うこと、業務の継続等の視点から組織に与えるリスクについて評価を行うこと、そして、これらの「リスクアセスメント」を踏まえ、リスクに対応するためのコストを勘案した上で、対策の内容を決定していくことが本来必要となるが、第一段階としては、業務上取り扱う情報の内容や業務フロー、情報の取得から廃棄までの一連のライフサイクルの視点から、業務プロセスを把握することが重要である。このため、平成 28 年度においては、情参室と各部局の業務担当職員、システム担当職員等が一体となって、漏えい等による影響が大きいと考えられる情報の抽出、業務のプロセスや情報セキュリティ対策等の確認を行い、リスクの評価を行った上で情報セキュリティ対策に係る改善策を検討し、改善計画を策定する、これら一連のリスク評価の実施方法の構築（ガイドラインの作成）に取り組む予定である。

（２）機構における取組

① 機構の情報システムとセキュリティ対策等

公的年金業務の実施にあたっては、年金個人情報に対する情報セキュリティ対策として、「政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）」（平成 26 年５月 19 日情報セキュリティ政策会議決定）（以下「統一基準」という。）等を踏まえた情報セキュリティ対策を実施してきた。しかしながら、機構 LAN システムにおいて年金個人情報を保有する際は、パスワード設定などのセキュリティ対策の実施を条件としていたものの、年金個人情報を保管した共有ファイルサーバをインターネット環境下に置くシステム設計は、業務運用の実態を踏まえたリスク管理とは言えず、そもそも問題があった。

機構では、インターネット環境下にある共有ファイルサーバ内に年金個人情報が置かれている実態、リスクを認識していたが、具体的な指摘・提言や対処策の検討が行われていなかった。さらに、共有ファイルサーバの運用ルールは定められていたが、共有ファイルサーバがインターネット環境下に設置されているというリスク認識が十分ではなかったため、外部からの攻撃に対する対策に関して十分な検討が行われず、パスワード又はアクセス制限の設定といった内部からの脅威に重点を置いた情報セキュリティ対策となっていた。また、共有ファイルサーバの運用ルールが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る状況となっていた。

この他、機構におけるリスクアセスメントにおいては、平成 26 年度より外部からのサイバー攻撃をリスク項目として付加していたものの、具体的なリスク対応の立案までは至っていなかった。

機構においては、情報技術の進展や内外の環境の変化等を的確にとらえ、それに応じた情報セキュリティ対策を適切に講じることとしている。

前記２（１）①のとおり、今回の情報流出事案では、年金個人情報をインターネットと接続した機構 LAN システムに置いて作業し、当該システムがインターネットを経由して攻撃された結果、不正アクセスによりインターネットに接続された外部のサーバに年金個人情報が持ち出されたことが直接の原因であり、これを踏まえ、機構においては、大量の年金個人情報や機微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とともに、分離された情報システム内で業務が円滑に完結するよう情報システムの設計・構築・運用及びルール徹底を行うこととしている。

さらに、機構 LAN システムについては、これまで実施してきた情報セキュリティ対策を継続実施した上で、機構職員及び情報セキュリティ対策専門の支援業者により、業務の実態を踏まえたリスク評価を行い、統一基準等に準拠した多重の防御策を講じていくこととしている。具体的には、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にすることとし、インターネット環境を、基幹システム及び機構 LAN システムの領域から分離した領域に新たに構築することとしている。なお、現在禁止しているインターネットメールについては、従前の独自回線経由でメールの送受信を行って

いた環境を、厚労省統合ネットワーク経由に改めるとともに、統一基準等に準拠した情報セキュリティ対策を施した仕様により運用を再開することとして検討を進めている。

また、新たに年金個人情報専用の共有フォルダ（以下「専用共有フォルダ」という。）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し、年金個人情報を管理・運用する領域を基幹システムに限定することとした。さらに、当該専用共有フォルダへのアクセスを限定し、年金個人情報のインターネット環境への移動を物理的に制限することとしている。

この他、インターネットに接続している機構ホームページ等については、運用管理業者等により情報セキュリティ対策の点検を行った。

今後は、専用共有フォルダの安全性を更に高めるため、基幹システムへのアクセスと同様に、生体認証をもってアクセス可能な者を識別する仕組みを導入し、より厳格なアクセス制御を行うこととするとともに、当該フォルダへ年金個人情報等を格納する場合は、自動的に暗号化設定を行う仕組みを導入することとする。

なお、機構LANシステムについては、平成30年度にシステムの更改を予定しており、統一基準等に準拠した情報セキュリティ対策を施した仕様として、要件定義を進めている。

② 機構の運用管理対策

機構においては、ソフトウェアベンダから提供される脆弱性情報を定常的にチェックし、重大な脆弱性に対応するセキュリティパッチの適用を速やかに行う必要があるが、適用作業に伴うシステム停止等により、業務に影響を及ぼすのではないかとの懸念から、その実施が先延ばしにされていた。情報流出事案では、既知の脆弱性を突かれたことにより機構 LAN システムの管理者権限が窃取されたが、この脆弱性は平成 26 年以来指摘されていたものであり、重要な脆弱性に対するセキュリティパッチの適用の遅れがこのような結果を招いた。

また、機構 LAN システムの端末における管理者 ID とパスワードが全て同一であるなど、管理者権限の適切な管理が不十分であったことにより、短時間に広範囲の端末へ感染が拡大した。

さらに、通信を監視し、ウィルス感染等を早期に検知する機能が整備されていなかったことや、運用管理業者が作成する手順書として、情報セキュリティインシデントに関する具体的な手順が明確にされていなかったことなども情報流出事案の一因となっており、こうした教訓を踏まえた運用管理対策を講じていく必要がある。

このため、機構においては、セキュリティパッチの最新化、管理者権限の適切な管理、ネットワークシステムの常時監視（モニタリング）等の運用管理対策（情報セキュリティに関する契約内容の具体化による外部委託先の適切な管理を含む。）を講じる

こととしている。
　具体的には、セキュリティパッチの最新化については、既知の脆弱性を放置しないようオペレーティングシステムやソフトウェアに対する最新のセキュリティパッチの適用を遵守するよう運用管理業者に指示し、適切に最新化を行っている。
　また、機構 LAN システムにおける管理者権限の適切な管理にあたっては、管理者権限の不正利用を防止し、そのセキュリティレベルを向上する観点から、全てのパスワードを変更し、継続的に変更していく運用に見直すとともに、不要な管理者 ID を確実に消去する運用としている。
　さらに、重要機器の監視に関し、機構では、運用管理業者や情報セキュリティ対策専門の支援業者の意見を踏まえながら、監視方法及び監視基準等について規定した上で、監視を行っているところである。
　上記の各対策に加え、運用管理業者が作成する手順書においては、現在契約している運用管理業者と協議の上、今回、改善策を講じた機構 LAN システムに係る運用管理業務について、運用管理業者が作成する情報セキュリティインシデントに関する具体的な手順を改正し、運用管理業者が実施すべき取扱いについて明確に規定した。

　今後、平成 30 年度に予定している機構 LAN システムの更改までの間において、運用管理業務の改善が必要と見込まれる事項が判明した場合は、同様の取扱いを実施する予定である。

③　機構における情報セキュリティ監査

　機構においては、これまで年金個人情報の流出防止という観点から、通常の事務処理がルール通りに行われているかということに重点を置いた業務監査及び個別システムのリスク分析を行い、優先順位をつけた上で、機構ポリシーなどの諸規程等に基づき運用されているかという観点でのシステム監査を行ってきたが、第三者の視点による客観性や専門性を確保できるという長所がある外部の専門家による情報セキュリティ監査は実施してこなかった。
　このような状況を改善するため、情報セキュリティ対策の最先端の技術的な動向を踏まえた独立した外部の専門家による情報セキュリティ監査を定期的・継続的に受け、結果を厚労省と共有することとしている。
　また、外部の専門家による監査だけではなく、内部監査についても体制整備の上、機構ポリシーに基づく基本的な情報セキュリティ対策に係る監査を幅広く実施することとしている。

　平成 28 年度計画では、外部監査は業務改善計画における情報セキュリティ対策の技術面について、内部監査は業務改善計画における情報セキュリティ対策の業務運用面について、それぞれ監査を行うこととしている。

３　教育・訓練

（１）厚労省及び所管法人等における取組

今回の情報流出事案が発生した大きな要因として、厚労省は国民生活に密接に関わる行政を担当しており、本省や地方支分部局、施設等機関及び所管法人等を含め、膨大な個人情報や機微な情報を扱っているにも関わらず、標的型攻撃の危険性を含め、情報セキュリティの重要性に対する意識が省全体として希薄であった。また、こうした中で、職員間、上司と部下の間、関係組織間で情報や危機感が適時、的確に共有されず、組織が一体として迅速に危機に当たることができなかったことも一因として挙げられる。

患者や働く方々などの国民の個人情報を守り、情報セキュリティに関する信頼を得ていくためには、今回の情報流出事案を踏まえ、職員の意識改革やリテラシー向上のための教育訓練を行うとともに、所管法人等においてもその徹底を図っていくことが必要である。このため、厚労省においては、今回の事案発生直後より、幹部を含む全職員を対象に、各種研修や訓練等を順次実施するとともに、所管法人等においても、教育・訓練を含め、必要な情報セキュリティ対策が実施されるよう、法人等に対する指導監督の取組を進めた。

①　厚労省における取組

厚労省の組織全体として危機意識や情報セキュリティに関する意識の向上を図るため、平成 27 年７月以降、政務３役、事務４役、部局長を含む幹部、各部局の筆頭課長（情報セキュリティ責任者）、課室長（課室情報セキュリティ責任者）を対象に、役職階層別の研修を順次実施するとともに、今回の事案発生直後（平成 27 年６月）及び再発防止策取りまとめ直後（同年９月）に、全職員あてに、個人情報等を含む重要情報の適正管理について周知した。

また、業務適正化推進月間（平成 27 年 10 月 19 日～11 月 13 日）では、職員間の情報共有や職場でのコミュニケーションの確保の徹底を図るための研修を実施するとともに、電子政府利用促進週間（同年 11 月２～６日）では、過去に政府等で発生した事案や情報セキュリティに関する最新の動向を踏まえ、部局情報セキュリティ管理者（筆頭課の総務係長）等を対象とした研修を実施した。

サイバーセキュリティ月間（平成 28 年２月１日～３月 18 日）では、今回の情報流出事案を踏まえた平成 27 年 12 月の厚生労働省情報セキュリティポリシー等の改定の内容を基に、インシデント発生時の速やかな報告、連絡体制の構築等について、課室情報セキュリティ管理者（課室の庶務係長等）などを対象とした研修を実施した。また、全職員あてに、標的型攻撃を念頭に置いた不審メールへの対応等について周知す

るとともに、情報セキュリティポリシーに基づくセキュリティ対策や個人情報の適正管理等に関するｅラーニングの受講促進を行い、平成 27 年度末までに約 98%の受講率を達成した。

平成 28 年度においても、引き続き、全職員対象及び役職階層別の情報セキュリティ研修（集合研修、ｅラーニング）、職員間での情報共有の徹底を図るための研修を実施することとしているが、今回の情報流出事案も含め、これまで蓄積されてきた過去のインシデント対応のノウハウについては、それを俗人化させず、組織として共有し、活用できるようにする仕組みを構築することが必要である。こうした観点から、平成 28 年度より毎年「６月」に厚労省独自の集中的取組期間を設定し、今回の事案を風化させないための取組を実施する予定である。また、情報セキュリティ研修の中で、引き続き、過去の事案や情報セキュリティの最近の脅威と対策等の教育を実施するとともに、新たな取組として、インシデント経験者による勉強会形式の研修等の実施について検討することとしている。

標的型メール攻撃訓練については、上記の研修等を通じて周知した内容の徹底を図る観点から、平成 27 年 12 月に、各部局で抽出された職員を対象に抜き打ち的に標的型メールを送付し、受信時や開封した場合の初動対応、CSIRT への必要な報告の実施等の訓練を実施した。また、平成 28 年２月には、情報セキュリティ監査の一環として、全職員を対象とした標的型メール攻撃訓練を実施した。これらの訓練の結果、部局によってメールの開封率等にばらつきが見られたことから、平成 28 年度においても引き続き、標的型メール攻撃への対処について、研修等による一層の周知徹底を図っていく必要がある。

省内での訓練に加えて、CSIRT 要員をはじめ厚労省の職員や、機構を含む所管法人等の職員が総務省主催の「実践型サイバー防御演習（CYDER）」（平成 27 年 10～12 月）に参加したほか、CSIRT 要員は、NISC 主催の CYMAT 研修や、民間企業の実践的なサイバーセキュリティ研修に参加した。そして、平成 28 年３月 18 日に開催された NATIONAL 318(CYBER) EKIDEN では、CSIRT 要員を中心とする厚労省職員が参加し、最優秀チームワークの総務大臣賞を受賞することができた。この結果に満足することなく、インシデント対処能力の更なる向上に向けて取り組んでいく必要がある。

標的型攻撃だけでなく、他のインシデント発生時の対処や報告、連絡体制の確認等のための訓練については、インシデントの発見から封じ込めまでの初動対応に重点を置きつつ実施することが必要である。このため、平成 28 年度においては、引き続き、標的型メール攻撃訓練の実施や、今後は国立研究開発法人情報通信研究開発機構(NICT)で実施される予定の CYDER 等の演習への参加とともに、新たに、外部委託する CSIRT への専門的支援業務の中で、CSIRT の初動対応を含めた演習を実施する予定である。

② 所管法人等における取組

厚労省の所管法人等における情報セキュリティ対策については、当該法人等が責任を持って行うことを基本としつつ、厚労省と所管法人等が一体となって、日常的な対策やインシデント発生時の緊急対応を行うという方針の下に、情報の共有や指導監督の取組を進めてきた。

ア　体制整備

平成 27 年 12 月７日に「厚労省所管法人等における情報セキュリティ対策連絡会議」（以下「連絡会議」という。）を開催し、各法人等の理事長を対象に、CISO、CSIRT の設置を含め、法人等における情報セキュリティ対策の実効性のある推進体制の整備や、情報セキュリティアドバイザーなど具体的なセキュリティ対策に係る助言等ができる人材の育成、確保についてトップダウンでの取組を要請した。

また、同年 12 月 21 日の厚生労働省情報セキュリティポリシー及びインシデント対処手順書の見直しにおいて、所管法人等でのインシデント発生時における当該法人等と厚労省の担当部局の役割の明確化、CSIRT、担当部局の局長・審議官、大臣を始めとする幹部に対する速やかな報告、連絡体制の構築、担当部局の責任者が果たすべき役割、職責の明確化等を内容とする改定を行った。また、当該改定内容について、平成 28 年２月 10 日に各所管法人等の情報セキュリティ担当職員を対象とした研修を実施するとともに、同年２月 18 日には、所管法人等の理事クラスを対象とした連絡会議を開催し、周知を行った。

今回のポリシー改定等に基づき、インシデント発生時に、所管法人等から担当部局を通じて CSIRT や幹部までの報告や円滑な意思疎通がより迅速に行われるよう、所管法人等との日常的なコミュニケーションを積極的に行うとともに、担当部局と所管法人等との間で、連絡、報告体制の構築や、それに基づく実践的な訓練の実施が必要である。こうした観点を含め、平成 28 年度においては、厚労省と所管法人等との連携に係る教育訓練の実施について検討することとしている。

イ　技術的対策

所管法人等においても、個人情報等の重要情報がインターネットに接続する環境に置かれる状況が生じないようにするためには、業務プロセスにおける情報の適切な取扱いという観点から、そうした状況が発生しうるリスクを評価した上で、業務に応じた情報管理対策をシステムの企画、設計の段階から講じていくことが必要である。しかしながら、こうした取組には一定の期間を要することから、緊急的な対応として、全ての所管法人等において、個人情報等の重要情報をインターネットから物理的又は論理的に分離するなど必要なシステム上の措置を実施した（平成 27 年９月）。平成 28 年度においては、厚労省本省と同様に、所管法人等が保有する個人情報等の重要情報を取り扱うシステムや当該情報を取り扱う業務プロセスの現状を

把握し、それぞれの実態やリスクを組織的に共有し、業務内容に応じたシステム上、業務運営上の情報管理対策を講じるための「リスク評価」を実施することとしている。（２（１）②参照）

この他、最近の攻撃の動向等を踏まえ、インターネット接続口の集約化や、DDoS攻撃、ソフトウェアの脆弱性を突いたホームページの改ざん、インターネットに接続されている機器のセキュリティ対策等について適切に対応するよう、平成28年２月の連絡会議において周知を行った。

ウ　教育・訓練

今回の情報流出事案を踏まえ、所管法人等に対しても、個人情報等を含む重要情報の適正管理について周知を行うとともに、担当部局の課室長及び所管法人等の理事、部長クラスを対象とした研修を実施した（平成27年10月）。また、総務省が主催する実践型サイバー防御演習（CYDER）に所管法人等の職員も参加した。（平成27年10～12月）

平成28年２月10日には、所管法人等の情報セキュリティ担当職員を対象とした集合研修を実施し、厚生労働省セキュリティポリシーの改定内容等について周知を図った。また、同年２月18日の連絡会議においても、個人情報等の重要情報の適正管理について改めて周知するとともに、所管法人等においても職員の意識改革、リテラシー向上のための教育・研修等に取り組むよう呼びかけた。

平成28年度においても、引き続き、所管法人等の職員に対する研修や、CYDER等への職員の参加を実施するともに、厚労省の情報セキュリティポリシーや教育、訓練の内容等について、連絡会議等の場で周知を図ることとしている。

また、今後は、各所管法人等において、ポリシー等に基づく情報セキュリティ対策や、教育訓練等の継続的な取組が適切に実施されているか、PDCAの観点から定期的に確認し、実効性を担保していくことが必要である。こうした観点から、所管法人等において自己点検及び第三者による情報セキュリティ監査が実施されるよう徹底を図るとともに、厚労省が所管法人等に対して情報セキュリティ監査を実施する予定である。

（２）機構における取組

情報流出事案以前においては、機構では、機構ポリシーなど情報セキュリティに関する諸規程や各役職員の具体的な役割や取るべき具体的な対応などについて十分な研修等を行っていなかった。また、研修テーマや研修内容などを担当者レベルで決定していた。これは、組織として情報セキュリティに係る教育・訓練の重要性についての認識が十分ではなく、定期的・継続的な研修の取組が不十分であったことによるものである。

こうした反省を踏まえ、機構においては、機構ポリシーに統括情報セキュリティ責任者が役職員の役割に応じた教育内容等を整備することを引き続き明示するとともに、全ての役職員が、計画的に必要な教育・訓練を受けることができるよう、教育実施計画を立案し、その実施体制を整備することを盛り込んだ。

また、機構ポリシー及びインシデント対処手順書等で役職員の役割・責任・権限を明確化し、改正された機構ポリシー等に基づいた研修・訓練を実施した上で、研修・訓練内容が業務に反映されているかを自主点検及び内部監査でチェックすることとした。

さらに、情報セキュリティインシデントの発生に際して、迅速かつ適切に対応できるよう、実際のインシデントを想定した実践的な情報セキュリティ対策の訓練（厚労省の担当部署等との連携も含む。）を定期的・継続的に実施するとともに、機構 CSIRT の対応能力を向上させるため、各府省等が開催する情報セキュリティ研修への参加を含め、情報セキュリティに係る専門知識の習得にも努めているところである。

平成 27 年度の具体的な取組として、全役職員の危機意識の向上のための研修として、全役職員に対し、標的型攻撃に関する攻撃者の手口と対処方法等を追加したテキストによる情報セキュリティ研修を平成 27 年６月末までに実施した。平成 27 年９月 15 日には、本部の幹部職員に対して、リスク管理や危機管理の在り方などのセキュリティマネジメントに係る情報セキュリティ研修を実施した。

また、情報管理対策室職員が、平成 27 年 10 月６日には厚労省及び NISC 共催の「法人等理事及び所管課室長対象の NISC のセミナー」に、同年 11 月 20 日には NISC 主催の「第２回情報セキュリティ勉強会（情報セキュリティ監査）」に参加した。

この他、平成 28 年１月７日には本部各部門の職員が、厚労省主催の「情報セキュリティ研修」に参加した。

さらに、平成 28 年３月には、機構ポリシーの改正及び関連諸規程の制定内容の周知徹底を図るために、機構ポリシー等の改正内容を分かり易くまとめた手引きを作成して、全拠点ごとに集合研修を実施した。

これらの各種研修により、平成 27 年度は全役職員に対して１回以上の研修を実施しており、平成 28 年１月に実施した自己点検においては、個人情報の無断持ち出しの禁止やパスワードの厳格な管理といった個人情報保護や情報セキュリティに係る項目について、ほぼ問題ないことが確認できた。

また、機構 CSIRT に属する職員のインシデント対応能力向上のための研修等として、情報管理対策室職員が、平成 27 年 10 月に総務省主催の研修（CYDER）に、同年 11 月には WASForum 主催（内閣府共催）の「情報セキュリティ演習」に参加するとともに、機構内での取組として、機構 CSIRT 要員に対して、情報セキュリティインシデント対応の取組をリードできる人員の養成を目的とした「CSIRT 研修」（全４回）を実施した。

さらに、平成 28 年３月 24 日には、今回制定したインシデント対処手順書に係る実効性及び機構内関係部署や関係機関（厚労省含む）との連絡・報告体制に係る即応性

を確認することを目的として、情報セキュリティインシデント対処訓練を実施した。

平成 28 年度においては、機構ポリシー等の理解度テストの結果を踏まえて研修内容を見直した上で、機構全職員に対し、機構ポリシーや関連諸規程の周知徹底を行う研修を実施する予定である。また、全職員を対象に情報セキュリティインシデント（標的型メール攻撃等）の訓練（年２回）を実施し、現場でのセキュリティインシデント対処手順を体得させる予定であるほか、平成 27 年度に受講した各府省等が開催した研修への受講を継続する予定としている。

（別添１）

情報セキュリティ強化等に向けた組織・業務改革

―日本年金機構への不正アクセスによる情報流出事案を踏まえて―

平成 27 年 9 月 18 日

厚生労働省

目　次

第１　日本年金機構における情報流出事案に関する総括

＜はじめに＞

本年５月の日本年金機構（以下「機構」という。）における情報流出事案は、「まれにみる組織的かつ執拗な（標的型）攻撃」（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（以下「検証委員会」という。）検証報告書）が原因であるとはいえ、これに対する備えは、機構のみならず厚生労働省においても、極めて脆弱であったことを率直に認めざるを得ません。国民の共同連帯の理念に基づき国民の信頼を基礎として実施されるべき政府管掌年金事業において、約125万件もの個人情報が流出したことは、国民の年金制度に対する信頼を損なうものであり、極めて遺憾です。

年金事業運営を所管する厚生労働省として、深くお詫び申し上げます。

今回の事案については、公表後直ちに元最高裁判所判事の甲斐中辰夫氏を委員長とし、外部有識者で構成される独立性の高い検証委員会を厚生労働省に設置しました。検証委員会では、機構及び厚生労働省の組織並びに初動及び事後の対応について第三者的な立場から検証し、原因の究明を行うとともに効果的な再発防止策について検討していただき、8月21日に検証報告書が厚生労働大臣に対して手渡され、数々の厳しいご指摘を頂きました。

また、機構においても自ら調査を行い、今回の情報流出という結果をもたらした原因について、組織の在り方に遡って徹底的に検証し、再発防止策を含む調査結果報告を8月20日に公表したところです。

さらに、政府全体の情報セキュリティに関する政策及び事案対応の司令塔を担うサイバーセキュリティ戦略本部（以下「戦略本部」という。）においても、20日、原因究明調査結果が公表されるとともに、政府全体のサイバーセキュリティ体制の抜本強化を図るサイバーセキュリティ戦略が9月4日に閣議決定されました。

その上で、9月11日には、戦略本部の本部長である官房長官から厚生労働大臣に対して、本事案を踏まえた再発防止策についての勧告がなされました。

本事案の事実関係については、これらの報告書等に記述されているとおりであり、また本事案の根本原因として、①厚生労働省、機構と

もに標的型攻撃の危険性に対する意識が極めて不足しており、事前の人的体制と技術的な対応も全く不十分であったこと、②インシデント発生後においては、現場と幹部の間、関連する組織間に情報や危機感の共有がなく、組織が一体として危機を克服する万全の体制になっておらず、その結果、数少ない組織内の専門知識を持つ者の動員すらできず、担当者が幹部の明確な指揮を受けることもないままに、場当たり的な対応に終始し、迅速かつ的確な対処ができなかったことが指摘されています。

厚生労働省は、こうした指摘（報告書等の具体的な指摘事項については別紙参照）を当事者として真摯に受け止め、今回の事案を以下の通り総括し、国民の信頼を回復するため、後述する再発防止策に全力で取り組んでまいります。

また、検証委員会の検証報告書が、同委員会への情報提供の遅延等に関連して機構に対して強く促している「徹底的な意識改革」については、厚生労働省自らに対しても指摘されたものと捉え、同様に行っていかねばならないと認識し、深く反省する次第です。

＜今回の事案についての主な反省点＞

今回の事案についての厚生労働省としての主な反省点は以下の三点と考えます。

１．情報セキュリティの重要性に関する意識の欠如

厚生労働省においては、ほぼ全ての職員がインターネットを始めとする情報システムを利用して業務を行っていますが、厚生労働省は国民生活に密接に関わる行政を担当しており、本省やハローワークなどの地方支分部局、施設等機関及び所管する独立行政法人等（以下「厚生労働省所管法人等」という。）を含め、膨大な個人情報や機微な情報を扱っています。にもかかわらず、これまで情報セキュリティ対策の重要性に関する意識は省全体として希薄であり、情報セキュリティ対策を直接担う職員は、専門的知識、人数いずれの面でも極めて不足しているなど、事前の技術的な対応と人的体制の備えがいずれも不十分でした。また、情報システムや情報セキュリティに関する機能が、情報政策担当参事官室（以下「情参室」という。）、統計情報部、そして厚生労働省所管法人等の所管課室と分散している中で、適切な情報共有が行われませんでした。

また、CSIRT 体制も即応性及び専門性は十分ではなく、緊急即応チームという CSIRT の本来の機能からすれば形式的なものでした。

機構についても、国民の重要な個人情報を大量に扱う組織でありながら、長期間にわたり個人情報をインターネットの影響下でリスクに晒された状況に置いていたなど、情報セキュリティに関する意識が極めて低かったことが指摘されていますが、その背景には機構を監督する厚生労働省自身の長きにわたっての意識の欠如があり、これが個人情報の流出につながった大きな要因と考えます。

２．組織的な危機管理対応の欠如

厚生労働省では、１．に記載したように情報セキュリティの重要性に関する意識が欠如し、事前の備えが不十分な中で、事案の発生後、「事案が収束してから書面で上司に報告する」、「自分は単なる窓口」、「他の部署が報告しているだろう」といった認識などから、職員間、上司と部下の間、あるいは関係する組織間で情報や危機感が適時に共有されず、組織が一体として危機に当たることができませんでした。その結果、5 月 8 日以降、機構が累次の攻撃を受け、セキュリティソフトの更新や拠点ごとのインターネットの遮断、警察への相談などを行っている最中に、厚生労働省は一部の担当者を除き、まったく事態の進行を把握できず、漫然と犯行を許すという、国民生活のセーフティネットを担う官庁としてはあってはならない状況を数週間にわたって続けることとなりました。

厚生労働省は「ひと、くらし、しごと」という一人ひとりの国民の生命、健康、生活に密接に関わる行政を担当しています。情報セキュリティに限らず、何か問題が生じた場合には、組織として情報を必要な関係者間で適時、的確に共有し、迅速に対応していかなければなりません。過去の薬害事件などにおいても、厚生労働省が被害の発生や拡大を防止できなかった原因として、情報に基づく迅速な対応が行われなかったことが指摘されています。「悪い知らせこそ早く報告する」ことが危機管理対応の基本ですが、こうした基本的な対応ができず、今回のような事態に至ったことについては、誠に恥ずべきことであり、省全体として痛切に反省しなければなりません。

このことは決して担当者レベルのみの責任ではなく、危機に際しては「途中の状況」であっても「悪い知らせ」が速やかに組織の上

層部に届き、上司がしっかり受け止め率先して対応に当たることができる職場環境が醸成できていないという意味において、厚生労働省幹部に責任があると言わざるを得ません。

また、情報セキュリティに限らず、一たび生じれば国民生活に重大な影響を及ぼす可能性のある事象については、事前の万全の備えが重要ですが、今回の事案が発生するまで業務運営におけるリスクの所在や評価等について組織的に把握、認識されていませんでした。

このことを踏まえれば、自らの組織が取り扱っている情報の重要性や業務運営面で様々に生じ得るリスクを日頃から正しく認識し、どのような事象に関してはどのような意思決定メカニズムで臨み、あるいは、権限を特定部署等に集中してどう備えるべきかを、幹部から現場職員一人ひとりに至るまで組織として事前に的確に定め、共有し、そのために必要な予算、人員等のリソースを確保、配分していくための取組を、特に幹部職員を中心に行っていく必要があります。

３．組織横断的、有機的な連携の欠如

(1) 4月22日の標的型攻撃についての厚生労働省の対応

検証委員会は、同委員会が、5月8日以降の機構への標的型攻撃の「予兆」と指摘する4月22日の厚生労働省への標的型攻撃についての厚生労働省の対応に関し、②で引用する2つの問題を指摘しています。

この問題を考える上で、4月22日の攻撃に対する厚生労働省の対応について、これまで職員から確認した事実関係は、以下のとおりでした。

① 厚生労働省の職員から確認した事実関係

4月22日の攻撃は厚生労働省ネットワークシステムに対する攻撃であったため､統計情報部の担当者は所属長まで報告した上で、最高情報セキュリティ責任者（CISO）である官房長に書面で報告しました。

その後、統計情報部の担当者は、4月23日に、不審な電子メール情報として、省内全職員に対し、攻撃してきた送信者の電子メールアドレス等を電子メールにより注意喚起を行いました｡また、4月24日には、情参室の担当者は、厚生労働省所管法人等

を所管している部局の担当者には、電子メールにより所管法人等へ注意喚起することを依頼しました。

しかしながら、統計情報部からの官房長への報告は、概要等を書面で届けるにとどまり、攻撃の事実等について官房長と認識を共有したことの確認を怠っていました。

また、本件に関して、情参室からの連絡内容は定型的な内容にとどまっており、所管法人等を所管する部局の担当者が実際に各所管法人等に注意喚起を行ったかどうかについても確認しておらず、年金局も、機構に対して何ら注意喚起を行っていませんでした。

以上のように、厚生労働省の関係課室では、担当者に十分な危機意識がなかったのみならず、上司や他の部局の担当者への報告、連絡に当たり、その内容が相手に確実に伝わったのか、理解されたのかを確認しておらず、組織として危険性の認識ができていませんでした。

また、5月8日以降の機構への標的型攻撃については、厚生労働省のCISOに5月28日まで報告されていませんでした。厚生労働省の「情報セキュリティインシデント対処手順書」（以下「対処手順書」という。）では、厚生労働省が所管する特殊法人（機構）において発生した情報セキュリティインシデント（以下「インシデント」という。）は、特殊法人を所管する年金局の課室情報セキュリティ責任者（課室長等）を経由してCISO及び情参室へ報告することになっていましたが、担当者から課室長等への報告が行われず、CISOにも報告されていませんでした。

一方、この対処手順書においては、NISCからの連絡を受けた統括情報セキュリティ責任者（情報政策担当参事官）は受け付けた事案を確認し、課室情報セキュリティ責任者（年金局事業企画課長）に必要な連絡を行うこととされていましたが、情参室からは担当者レベルでの連絡は行われたものの、事案の重要性に鑑みた、迅速な情報共有は行われていませんでした。

これらの点で、厚生労働省セキュリティポリシー等に沿った対応がなされていませんでした。

② 検証委員会の指摘とそれに対する厚生労働省の考え方

ア 4月22日の段階でドメイン単位でURLブロックが行われなか

ったことについて

検証委員会の検証報告書では、4月22日に発生した厚生労働省に対する標的型攻撃は、5月8日以降に発生した機構に対する標的型攻撃と手口が類似しており、4月22日の段階で、厚生労働省統合ネットワークにおいてドメイン単位でURLブロックを実施していれば、5月8日に発生した同一ドメインのC&Cサーバに対する機構との不正な通信は防ぐことができた、と指摘しています。厚生労働省は、5月8日段階で、ドメイン単位でURLブロックを実施していましたが、今般の検証委員会の指摘を踏まえ、今後不審な通信が検知された場合には、業務への影響やドメインの種類等も勘案しつつドメイン単位でのブロックを基本とすることを、厚生労働省セキュリティポリシーや対処手順書において明確にします。

なお、5月8日にドメイン単位でURLブロックを実施した結果、5月18日の機構に対する標的型メールにより感染した3台の端末からの不正な通信はいずれも失敗しており、これは、対策が功を奏したともいえます。

一方、厚生労働省統合ネットワークにおいては、ブロックした不正な通信先を継続的に監視していなかったため、それ以上の対応をとれませんでした。仮に、既にブロックした不正な通信先へ通信を行おうとする端末があるか否かを継続的に監視していれば、他にも感染した端末があることを、不正な通信を行った時点で発見することができ、機構などに注意喚起を行う機会があったと考えられます。

この点についても、厚生労働省セキュリティポリシーや対処手順書において改善します。

イ　厚生労働省から機構に対する情報共有が行われなかったことについて

さらに重要な問題は、5月8日以降の機構に対する標的型攻撃と類似の手口による4月22日の厚生労働省に対する標的型攻撃について、5月8日の段階で、厚生労働省から機構に対して、何ら情報提供が行われず、このため、機構においても、同日の攻撃

が、厚生労働省やその関係機関を狙った一連の標的型攻撃であるとの着想に至らなかった、との指摘です。

①に記載したとおり、5月8日の事案では、省内幹部にも情報共有が行われず、省全体として適時、適切な対応ができませんでした。情報共有が適切になされていれば、厚生労働省内においても、機構においても、4月22日の攻撃との共通性も含め、5月8日の攻撃に関する危機意識が醸成され、その後の対応が異なるものとなった可能性があったという意味において、この時点での厚生労働省の対応は大きな反省点と考えます。

さらにいえば、インターネットの普及により、日頃の情報共有は、素早く、かつ、幅広に情報が共有できる電子メールによって行うことが一般的になっています。しかし、本来、伝える情報の重要性や質を考慮した上で、適切にコミュニケーション手段を選択、併用すべきものであり、重大な事案や相手に行動を起こしてもらう必要がある内容の連絡は、電子メールでの連絡や書面での投げ込みとともに、電話や対面で直接伝え、また、その結果を確認するなどの対応が求められます。このような、行政に携わる者として基本的な動作が日頃からできていなかった点も大きな反省点と考えます。

また、厚生労働省内の各組織の権限や各職員の役割をあらかじめできる限り明確にしておくことはもちろん重要ですが、事前に定められた仕事を確実に遂行するにとどまらず、一歩進んで、国民の立場に立って、相互の意思疎通や組織横断的、有機的な連携を図り、厚生労働省の組織全体として、一丸となって対応していくことが重要ですが、今回の事案ではそのような対応ができていませんでした。

このため、改めて、日頃から組織として職員に対し報告、連絡の仕方など基本的な動作についての指導を徹底するとともに、各組織の在り方についても、厚生労働行政の課題や取り巻く環境の変化に応じて速やかに見直します。

(2) 厚生労働省と機構の関係

厚生労働省と機構の間でも、事案の発生後の対応について情報共有が担当者レベルにとどまり、幹部レベルの情報共有、監督指示などが、事案発生から17日後の5月25日の遅きに失するタイ

ミングに至るまで行われないという、あってはならない事態が生じました。そもそも個人情報の取扱に関する日常業務の実態についても、機構を指導監督する年金局の幹部を始め情報、認識の共有は全く十分ではありませんでした。

また、機構の業務における個人情報の取扱環境やパスワード設定等のルールの遵守状況について、年金局も事案が発生してから問題を把握する状況でした。

6月1日に本事案を公表した以降も、機構が、5月29日に統合ネットワークを通じたインターネットへの接続を遮断した後も独自の電子メール送受信専用外部回線の遮断を行っていなかったこと、また、個人情報が流出した方に対して「流出は確認されていない」と誤って説明したことが機構において判明した際にも、機構独自の対応にとどめてしまい、報道されるまで厚生労働省に報告していなかったことなど、厚生労働省と機構との間で重大な情報が共有されていないという、やはりあってはならない事態も生じました。

さらに、検証委員会からは、機構LANシステムの担当部署が厚生労働省内部で不明確であった点について、「監督官庁としてあり得ないこと」との厳しい指摘がありました。

機構は、様々な問題があった社会保険庁を廃止し、新たに非公務員型の公法人を設けて公的年金に関する業務を行わせることで、提供するサービスの質の向上と業務運営の効率化を実現することを目的として創設されましたが、その前提は、厚生労働大臣の監督の下に、厚生労働大臣と機構の密接な連携が確保されることでした。機構創設の原点に立ち返り、政府管掌年金事業の適正な運営は厚生労働省と機構が車の両輪となって共に担う、との考え方を再確認し、厚生労働省による機構の監督や、機構との連携の在り方について、ゼロベースで点検し、再構築していきます。

＜再発防止に向けた基本的考え方＞

厚生労働省としては、以上の反省点を踏まえ、今回のような事態を二度と引き起こすことがないよう、年金局や機構だけではなく、厚生労働省所管法人等も含めた厚生労働行政全体について、ガバナンスの強化、組織内、組織間連携の強化、リスク認識の強化に努めていきますが、今回の事案に照らし、特に情報セキュリティ対策の観点から、

強化を図ります。

今回の事案の標的型攻撃は、次々と手口を変えて攻撃を継続する極めて執拗かつ組織的なものでしたが、情報技術は今後もさらに発展し、サイバー攻撃も時々刻々と巧妙化して、社会にとって大きな脅威となっていくと予想されます。今回の事案を、厚生労働行政に従事する全ての職員が教訓として記憶し、緊張感を持って、各種対策について不断に取り組んでまいります。

また、公的年金制度を所管し、機構を監督する厚生労働省と、公的年金制度の執行を担う機構が車の両輪となって年金事業を運営していくべく、機構自身の自己改革の取組と併せ、厚生労働省においても、機構との密接な連携を実現するとともに、社会保障審議会年金事業管理部会に監視機能をこれまで以上に強力に発揮していただきながら、機構の今回の情報流出のような事案の再発防止に向けた取組を強化すべく、自らの体制強化も行っていきます。

このため、情報セキュリティの全省的な強化を含め、「情報セキュリティ強化等に向けた組織・業務改革推進本部（仮称）」を設置し、以下のような具体的な取組を着実に実施していきます。

第２ 今回の事案を踏まえた再発防止策

検証委員会や戦略本部の報告書等の指摘や同本部長の勧告を踏まえ、厚生労働省における情報セキュリティ対策については、①組織的、②人的、③業務運営、④技術的な観点から、以下の再発防止策に取り組みます。

また、年金局の体制を充実させるとともに、機構の報告書等に掲げられた再発防止策が着実に進むよう機構に対し指導監督を行っていきます。

さらに、機構以外の厚生労働省所管法人等に対する監督指導や情報セキュリティ対策を強化します。

１．厚生労働省における情報セキュリティ対策の強化

(1) 組織的対策（体制強化、情報共有）

平成 26 年 7 月、情報政策の企画立案部門を集約するため、統計情報部情報システム課の一部と政策統括官（社会保障担当）付情報政策担当参事官が統合されました。

この統合により、厚生労働省の情報セキュリティ対策の実施に関する企画立案、連絡調整、対策の推進や情報セキュリティ事案に関する情報収集、対応に関する事務は情参室に移管されましたが、厚生労働省の情報システムの整備及び管理に関する事務の一部は移管されず、統計情報部の事務として残されました。結果として、今回の事案でも円滑に情報共有が進まなかった原因となった可能性があります。

このため、来年度に向けて、省内の情報システムや情報セキュリティに関する機能を再集約、再編し、情報セキュリティ対策に関する司令塔機能を強化します。こうした機能の見直しに合わせた新たな組織作りを検討するとともに、併せて、各原局との分担、連携の在り方についても見直します。

それまでの間は、以下の措置を速やかに講じます。

① 情報セキュリティ対策室（仮称）の設置

省内の情報政策の企画立案、調整連絡等を担当する部署として情参室が置かれています。このうち情報セキュリティ対策に関する業務は情報セキュリティ対策係が担当しており、情報セキュリティに関する周知啓発、厚生労働省セキュリティポリシーの整備等の他、内閣サイバーセキュリティセンター（以下「NISC」という。）との連絡窓口となっています。人員体制は室長補佐以下４名であり、他の業務も兼務しているため、対応しなければならない業務内容や業務量の多さに鑑みれば、専門的知識や職員数の面からも十分な対応ができる体制とはいえません。

今回の事案では、情報システムの整備、管理担当者と情報セキュリティ担当者の間の情報の共有が円滑にできなかったため、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）を設置し、厚生労働省セキュリティポリシー等のルールの整備、リスク評価、監査（助言）、教育訓練やインシデント発生時の連絡調整、技術的支援、対処措置の指示等に係る業務を一体的に担うこととします。

特に、省内各部局、厚生労働省所管法人等から不審な電子メールやサイバー攻撃等の情報を収集、集約して分析し、攻撃を受けた個別の部署単位では伺い知ることが難しいサイバー攻撃

相互の関連性、攻撃の全体像や受けた攻撃がどの段階にあるのかを把握、予測することにより、次の攻撃を想定した警戒情報や指示を出すなど、先を読んだ対応を行います。

② CISO、CSIRT 体制の見直しについて

厚生労働省においては、インシデントへの対処体制としてCSIRT 体制（インシデント対応チーム）を整備していました。この体制では、インシデント最高責任者を官房長、インシデント統括責任者を情報政策担当参事官、インシデント管理責任者をインシデント担当部局の総括課長とする等、責任者による報告、連絡のための体制となっています。

しかし、今回の事案では、NISC との窓口であるセキュリティ対策係から CSIRT が機能するための大前提である上司への報告が迅速に行われませんでした。また、実際の対処や関係機関等との調整に当たる技術力を有する実働要員が選任されておらず、CSIRT 体制をより実効性のあるものとするための見直しが不可欠です。

このため、即応性の向上、権限の強化（予算面、人事面、業務面）の観点から、CISO を官房長から厚生労働審議官に見直すとともに、CSIRT 体制についても、CSIRT を情報システムの管理運用部局の責任者から独立させ、CSIRT 責任者を官房長から日常的に情報セキュリティや情報政策を担当している情報政策・政策評価審議官に見直し、即応性と専門性を向上させます。

また、新たな CSIRT 体制では、CSIRT 要員として、実際にインシデントの対処支援や関係者との連絡調整に従事する補佐、係長クラスの職員（上記の情報セキュリティ対策室（仮称）の室員）を充て、役割を明確化します。

一方で、現行の CSIRT 体制及び厚生労働省セキュリティポリシーにおける情報連絡体制は、例えば、各部局の局長、審議官は役割が規定されていないなど、通常業務の情報共有、意思決定ラインとは別ルートに定められています。このことが情報を共有すべき者を不明確にしたり、指揮系統の二元化による迅速な判断や意思決定ができないことにならないよう、見直しに際しては、通常業務との関係に十分気を付けます。

(2)　人的対策（意識改革、人材育成）

①　職員の意識改革

危機管理対応では、インシデントがもたらす最悪のケースをあらかじめ想定し、常に危機感をもって対処することが大原則であるにも関わらず、特に、標的型メール攻撃を始めとするサイバー攻撃を含む情報セキュリティ対策については、省全体としての意識が希薄でした。今回の事案を踏まえて、緊張感のある姿勢で日常の業務に臨むよう、職員の徹底した意識改革を行います。

既に、職員全員に情報の安全な取扱について改めて周知徹底を行うとともに、政務三役を含めた幹部職員についても専門家による情報セキュリティ研修を実施し、責任者の危機意識の向上と啓発を行います。

また、全職員に対する情報セキュリティに関する意識の向上を図る観点から、毎年、初任者研修の機会や政府が定める「サイバーセキュリティ月間」（2月）に情報セキュリティ研修等を実施してきましたが、今回の事案を踏まえ、厚生労働省においても情報セキュリティに対する独自の集中的な取組期間を設定し、職員に対して今回の事案の概要や反省点を理解させ、警鐘を発することで多数の情報流出を防ぐことができなかった今回の事案を風化させない取組を行います。

②　マネジメント面の意識改革

厚生労働省は、所管の各分野において毎年のように制度改正を行っています。しかしながら、省全体としてこうした制度改正に注力する必要がある一方で、情報システムの整備や文書管理など日常業務の基盤整備は優先順位において後回しになり、人的資源の配分も少なくなっていたことは否定できません。今回の事案でも情報セキュリティに対応する人的配置が全く不足していたことが指摘されています。

制度を不断に見直し、必要な法律改正を行うことが厚生労働省の一つの組織文化となってきたといえるかもしれませんが、一方で、それを実現するための内部管理、業務体制を十分に整備するという組織文化が欠けていました。

したがって、特に幹部職員においては、情報セキュリティに関する意識改革だけではなく、業務基盤の整備など業務改革を進め

るとともに、人的資源の確保、配分における優先順位の見直し、あるいは限られた人的資源の中で取り組む業務の取捨選択、順序付けを行うというマネジメント面の意識改革を行います。

③　実践的な訓練の実施

現実にインシデントが発生した場合には、事態や被害状況の把握、被害の拡大防止策の実施、復旧の検討、関係者への説明、公表、関係機関との連絡調整等、多方面での対応が必要となり、今回のように、必要な連絡や報告が遅延することのないよう、あらかじめ事案を想定した実践的な訓練が必要でした。

このため、標的型メール攻撃に対する一般職員の危機意識やリテラシーを向上させるため、不審な電子メールの受信時の対応、万が一開封した場合の初動や、必要な報告、連絡を含む実践的な訓練（抜き打ち的なものを含む。）を行います。

また、総務省が主催する「実践型サイバー防御演習（CYDER）」への厚生労働省所管法人等の職員を含めた参加を通じて、情報セキュリティ対策に携わる担当職員の能力向上を図ります。

さらに、民間企業が提供する実践的なサイバーセキュリティ研修サービスを活用し、CSIRT 体制の初動対応を含めた演習を実施します。

④ 専門人材の確保

現在の CSIRT 体制においては、専門的知識を有する者による助言を受けることができるよう、CIO 補佐官にインシデントアドバイザーを依頼していました。

しかし、CIO 補佐官は非常勤であり、また、インシデント対応以外にも大規模情報システムの刷新業務等に関する支援業務など多くの業務を抱えていたため、今回の事案では、情参室の担当者等と迅速に報告や相談を行うなど緊密な連携ができませんでした。厚生労働省においては、必ずしも情報セキュリティの専門的知識を有する職員を組織内部で養成できていないことから、外部人材による助言が重要であり、速やかにこうした助言を受けられる体制の構築が必要です。

このため、新たに設置する情報セキュリティ対策室（仮称）に情報セキュリティに関する外部の専門家を常勤で配置し、インシ

デント発生時には、即時に技術的な助言ができる体制とします。また、インシデント発生時はもとより、インシデントの発生かどうか、警戒すべきかどうかといった状況判断における技術的な助言もその専門家により行います。

なお、配置する際には、情報システムの専門家が必ずしも情報セキュリティ対策の専門家ではないことを念頭に置くとともに、24時間365日の対応や病休時の代替要員の手配等も考慮し、民間企業と業務委託契約により確保することも検討します。また、契約の際には、平時の際の業務として、研修の講師や各種調達への助言、情報セキュリティ対策における設計への助言を盛り込むなど契約内容を工夫します。

専門家の採用に当たっては、概念的、学術的助言や特定の情報セキュリティ製品、技術に特化した知識だけを確認するのではなく、幅広い情報システムを管理できる技術力を持っているか、様々な製品、技術の特性や脆弱性に関する知識を偏りなく持っているか、情報システム管理の作業現場での対応能力を持っているか、インシデント発生現場での問題解決能力を持っているか、コミュニケーション能力が優れているかという点を十分に確認し、採用します。

また、厚生労働省の主要な情報システムの所管部局との連携を強化し、インシデント発生時の即応性を向上させます。なお、深刻な緊急対応時には、NISCの情報セキュリティ緊急支援チーム「CYMAT(サイマット)」への速やかな支援要請や外部事業者に対し、専門的な知識を生かした支援等を委託します。

さらに、組織内での人材養成の観点から、職員に対する独立行政法人情報処理推進機構が実施する「情報セキュリティスペシャリスト」を始めとする情報セキュリティ関連資格の取得勧奨や当該資格を保有する職員に対する人事評価の在り方、情報システムに従事する職員のキャリアパスについて検討を行います。

⑤　教訓や知識の蓄積と継続性の確保

厚生労働省においては情報セキュリティなど危機管理の観点からの人材育成や過去の事案から得られた教訓の蓄積が必ずしも効果的、網羅的に行われているとは言い難い状況にあります。厚生労働省として情報セキュリティ対策を強化していくために

は、これら過去の事案から得られた教訓を取りまとめ、蓄積し、世代を越えて共有していくことが必要であり、さらに、情報セキュリティに関する専門的知識の最新の動向について外部の専門家の助言を得ていく必要があります。

このため、職員が定期的にこれらの教育を受ける機会を設け、危機管理に関する教訓や知識の蓄積と継続性の確保を図ります。

また、その際には、インシデントを経験した職員が講師となり、未経験の職員に対し自らの教訓を伝える職員同士の勉強会形式の研修も採用します。

(3) 業務運営対策（ルールの見直し、徹底）

① 報告及び連絡体制の確立、責任の明確化

今回の事案では、NISCからの不審な通信の検知に関する連絡、事案内容の把握、機構における対処状況、警察への相談といった各過程において、その状況を厚生労働省の担当部局の責任者が適切に把握していなかったことが明らかとなりました。

また、インシデントが発生した場合に、例えば情報システムのインターネットからの遮断等具体的にどのような情報システム上の対処措置を行うべきかについては、幹部を含む全ての職員が高度な知識を有しているわけではありません。一方で、ICT化による行政効率化を推進していく中で、厚生労働行政の業務運営において情報システムは不可欠です。特に、ますます巧妙化するサイバー攻撃に晒される現状に鑑みると、情報セキュリティ対策は、巧妙に偽装された不審な電子メールの開封や他の機関の改竄されたホームページにアクセスしてしまうことは防ぎ切れないという前提のもと、講じていかなければなりません。

このため、厚生労働省セキュリティポリシー及び対処手順書において、以下の見直しを行います。

- インシデント発生時の責任者への報告、連絡体制を見直すとともに、速やかに大臣を始めとする幹部に報告すること等、事案発生からの各対応過程（警察への相談等も含む。）において責任者に対する報告、連絡を明記します。
- 各対応過程において各部局の責任者が果たすべき役割、職責を明確にします。
- CSIRT体制の見直しに伴い、技術的支援、措置に関する指示、

勧告、対外的な連絡調整を行うCSIRTと、実際の対処や復旧に当たる担当部局の役割と責任を明確にします。

・　各組織において、インシデント発生時の対応責任者をあらかじめ決めておき、インシデント発生時には、組織の責任者とは独立して即時に対応できるようにします。

・　インシデントと判断する基準等を一層明確にし、組織内での共有を図ります。特に、不審メールを受信した場合には、標的型メール攻撃であることを念頭に、上司に報告することや危機意識を持った継続的な対応を行うことを前提に対処措置を定めます。

・　職員が対処措置等について検討し判断できるよう、実際に発生した事案において実施した対処措置を整理し、参考とすべき基準として職員に示します。

・　厚生労働省には、毎日のように不審な電子メールが送られてきており、これらに対する注意喚起を促す電子メールも毎日職員に対して送付されています。注意喚起を促す電子メールを受け取る職員が不審な電子メールに対する警戒心を麻痺させ、現実にインシデントが発生した際の対応に遅れが生じないよう関連が予想される複数の攻撃が起こっている場合には、連絡内容や連絡手段を変えるなど工夫します。

②　保有する情報を適切にリスク評価した上での情報管理の徹底

サイバーセキュリティ戦略において、被害を低減する取組として「個人情報や機微な情報を始め、外部に流出することや改ざんされることによって国民・社会等に多大な悪影響を及ぼす機密性・完全性の高い情報への不正なアクセスをより困難なものにするため、業務の内容や取り扱う情報の性質・量に応じた情報システムの分離や運用ルールを含む情報管理の更なる強化に取り組む。」とされています。

厚生労働省では、多種多様な個人情報や機微な情報を扱って業務を遂行していることから、インターネットのもたらす脅威を再認識し、個人情報等重要情報を取り扱う情報システムや業務の現状を把握し、それぞれの実態やリスクを組織的に共有するためリスク評価を実施します。

今後、リスク評価の結果に基づき、業務内容に応じた対策を講

じることとしますが、緊急的な対応として、個人情報等の重要情報を取り扱う省内の情報システムについては、インターネットから物理的又は論理的に分離し、インターネットに接続された端末で利用しないこととする措置を講じたところです。

業務内容に応じた対策を講じるに当たっては、インシデント発生時に国民や社会へ与える被害や影響について定量的、定性的に分析を行い、その結果に基づき、事態の被害や影響を最小化するための対策を検討します。

また、対策の実施に当たっては、リスク評価の結果に基づいた機器の設定等はもとより、規程の見直しや職員への啓発等を行い、組織全体として情報を管理する能力を向上させます。

なお、リスク評価については、業務実態や社会の動向等を踏まえ、専門的な見地から実施します。

(4) 技術的対策（情報システムの強化）

① 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の強化

標的型メールのような外部からの攻撃を完全には防御することはできないことを前提に、攻撃を受けても早期に認知、対応し、実際の被害を最小限にするための措置を講じる必要があります。

このため、統合ネットワークにおいては、「政府機関の情報セキュリティ対策のための統一基準」（平成 26 年 5 月 19 日情報セキュリティ政策会議決定）及び「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成 26 年 6 月 25 日情報セキュリティ対策推進会議）に示されている内容の他、特にサイバーセキュリティ戦略において、政府機関を守るための取組として「情報の窃取・破壊・改ざんを企図したとみられる標的型攻撃を始めとしたサイバー攻撃に対処するため、（中略）全ての政府機関等において、攻撃に直面することを前提とした多層的な対策を講ずる。」とされている点も踏まえ、高度な標的型攻撃に対する多重防御対策に取り組みます。

具体的には、各種ウイルスの侵入を検知する入口対策（水際対策）に加え、情報ネットワーク及び情報システムへの侵入拡大や、悪意がある攻撃者が、重要情報を不正に取得したり、不正にアクセスするための通信をリアルタイムに監視し、適正に遮断する機

能など、標的型攻撃を早期に検知するための内部、出口対策を強化します。

また、複数機器から取得し、整理した証跡情報等を相関分析し、不正な通信が発生した場合には、リスク評価の結果に基づき、業務への影響を最小限にとどめつつ、自動的に遮断するための基準や適用範囲などについて、最新の情報セキュリティ対策に詳しく、実務経験のある専門家やCIO補佐官等の助言を得ながら、設計、構築し、適切な運用を行います。

この他にも、リスク評価により判明したインシデントの発生防止に向けた有効な対策技術について導入を検討し、必要な事項は、厚生労働省セキュリティポリシーに基づき定期的に策定する情報セキュリティ対策推進計画へ速やかに盛り込みます。

② 情報セキュリティの運用設計の見直しと改善

各種機器を導入しただけではその性能のごく一部しか発揮できません。組織や情報システムに導入する情報セキュリティ対策において、各組織間、情報システム間で役割分担を明確化した運用設計がなされることが非常に重要となってきます。

このため、厚生労働省及び厚生労働省所管法人等が保有する情報システムにおいては、同一の考え方に基づき、各業務の実態やリスク評価結果を踏まえた運用設計を行います。さらにインシデント発生時には、より一層の情報連携が必要なことから、各組織間の連携も含めた一元的なインシデント対応を実施します。

③ 調達時の契約内容の見直し

標的型攻撃に対応するためには、ソフトウェアベンダーが提供する脆弱性情報を定期的に確認し、重大な脆弱性に対応する最新のセキュリティパッチを適用する必要がありますが、今回の事案では、機構において、適用作業に伴う情報システムの停止等の影響等の懸念から、先延ばしされていました。

このため、国が情報システムを調達する際には、最新のセキュリティパッチが適用されるよう徹底します。

また、新規構築、更改、改修（軽微な改修を除く。）を行う情報システムの調達においては、ネットワーク機器や情報システムを構成するサーバ、アプリケーションについて、脆弱性検査ツー

ルや点検基準を用いた第三者による検査を徹底するための要件を追加します。

２．厚生労働省と機構の関係の強化

機構は、様々な問題を生じた社会保険庁を廃止し、新たに非公務員型の公法人を設けて、厚生労働大臣の監督の下に、厚生労働大臣と密接な連携を図りながら、政府管掌年金事業の運営に関する業務を担わせることで、提供するサービスの質の向上と業務運営の効率化を実現することを目的として創設されました。

今回の事案を踏まえれば、機構による改革の取組は道半ばです。政府管掌年金事業の適正な運営は厚生労働省と機構が車の両輪となって共に担う、との考え方を再確認し、機構自身の改革の取組と併せて、厚生労働省による機構への指導監督の強化や、年金局の体制強化に取り組みます。

(1)　厚生労働省の機構に対する指導監督の強化

上記のような機構創設の原点に立ち返り、機構におけるガバナンス、組織風土のゼロベースからの抜本改革などの機構の改革と併せて、機構の業務に関する厚生労働省のモニタリング機能の強化、機構の業務運営上定める内規等の共有のルール化や、事件、事故、事務処理誤り等についての報告、連絡や情報共有の徹底など機構に対する指導監督の強化に取り組みます。

また、システムの運用管理も含めた情報セキュリティ対策を一元的に管理する組織の新設など、機構が講じる再発防止策が着実に進むよう取組を行っていきます。

社会保障審議会年金事業管理部会については、新たな委員を任命するとともに、事務局へ民間から複数の参与を任命し、一層国民的視点に立って年金事業の管理がなされるように改めることとしました。また、国民からの意見が年金局を経由せずに直接部会委員一人ひとりへ伝わるよう専用の窓口を設置しました。こうした取組により第三者や国民の視点による年金事業運営に対する監視を強化していきます。この部会に対する説明責任を果たしつつ、着実に取組を進めます。

① システムに対する監督部署の明確化

機構の役職員が日常業務で使用するイントラネットである機構 LAN システムは、厚生労働大臣の監督下にありますが、当該システムに対する監督権限が年金局のどの課室にあるのか不明確でした。

このため、年金局事業管理課システム室を中心に取り組むこととし、権限の所在を明確にしました。

また、インシデント発生時の連絡についても、インシデントの重要度を適切に判断して対応できるよう年金局システム室が情参室及び機構（情報セキュリティ責任者）との連絡調整を行うとともに、速やかに幹部へ報告することをルール化したところですが、同室について、年金関係業務及びシステムに精通する職員を増強するとともに、外部の専門家を加え、体制強化を図ります。これによりシステムの見直し、調達の各段階で、情報セキュリティの観点から厳重なチェックを行う等、機構に対する指導監督能力を強化します。

② モニタリング機能の強化

今回の事案では、一部の個人情報についてパスワード設定等を行っていない等、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となりました。

このため、機構の改革の取組が着実に進むよう、年金局事業企画課年金事業運営推進室職員が機構本部に交代で常駐するとともに、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モニタリング、監査を強化します。

③ 業務運営上定める内規等の共有のルール化

機構が業務運営上定める「基本方針」「規程」「細則」「要領（マニュアル等）」「指示、依頼」について、内部統制強化の観点から、年金局においても改めて確認し、必要な見直しを行うとともに、今後、これらの制定、改廃又は発出を行うときは、年金局の担当部署へ速やかに報告し、年金局がチェックすることとし、そのルール化を行います。

④ 報告、連絡の徹底

「事件、事故、事務処理誤り」については、年金事務所等の各拠点から機構本部へ報告があった時点で、機構から年金局へも報告することとします。

また、事務処理誤りについて、個別の事案が「個別報道発表案件」に該当すると機構が判断したものについて、年金局で確認することとします。

さらに、年金局は、「事件、事故、事務処理誤り」について機構から報告を受けている案件のうち、「個別報道発表案件」に該当するものについて、速やかに公表するよう機構に指示します。

⑤ 情報共有の徹底

機構と厚生労働省との情報共有に当たっては、危機に際して「悪い知らせ」を速やかに共有する意識を徹底するとともに、担当者レベルのみならず、幹部も含めたそれぞれのレベルでの日常的な報告、連絡、相談ルール（各レベルで報告等を行う事項の明確化を含む。）を構築します。

⑥ 年金局と機構の連携の強化

上記のほか、年金局と機構との連携、相互理解を促進するとともに、年金局職員の公的年金に関する実務能力を強化するため、年金局職員と機構職員の相互の人事交流を拡大します。

また、府省共通研修、厚生労働省が実施する研修の受講を促進するとともに、年金局独自の研修を充実します。

さらに、年金局職員については、原則として年金事務所での勤務経験を課長補佐等への登用のキャリアパスとして位置付けます。

特に、年金制度改正の企画立案を担う部署における管理職相当以上の職員には機構への出向経験を求めるなど、年金実務を十分考慮に入れた制度設計が行われるようにします。

(2)　年金局の体制強化

機構自身による改革の推進のために機構に設置される「日本年金機構再生本部（仮称）」と連携し、機構の改革の取組が着実に進

むようにするため、年金局の体制を強化します。

また、機構が運用するシステム全体について、システム刷新に係る計画、設計に始まり、インシデント発生時など緊急時の対応に至るまで、一貫した指導監督ができるよう、体制の強化を図ります。

３．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

厚生労働行政は、厚生労働省の他にも多くの厚生労働省所管法人等が担っていますが、近時、厚生労働省所管法人等への攻撃が相次いで行われています。

患者や労働者などの国民の個人情報を守り情報セキュリティに関する信頼を得ていくためには、こうした厚生労働省所管法人等においても今回の事案を踏まえた対策が必要です。情報セキュリティ対策は、当該法人等が責任を持って行うことを基本としつつ、厚生労働省においても当該法人等の情報を収集し、当該法人等と一体となって日常的な対策やインシデント発生時などの緊急時の対応を行っていきます。

(1)　教育訓練の実施

意識改革や教育訓練は、厚生労働省所管法人等においても徹底される必要があり、標的型メール攻撃を含むサイバー攻撃を始めとする情報セキュリティの脅威と対策の必要性が確実に伝わるよう、関係部局と協力しつつ情参室から積極的な啓発を行う必要があります。

このため、厚生労働省所管法人等を所管する部局の職員、幹部についても、情報セキュリティにおける当該法人等との連携について教育訓練を行います。

また、厚生労働省が行う職員等への教育訓練については、厚生労働省所管法人等にも内容を情報共有し、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）を行います。

(2)　報告、連絡体制の確保

今回の事案では、年金局は機構との間にインシデント発生時の

報告、連絡、相談ルールを明確化しておらず、機構から適時、的確な報告がなされなかったという問題がありました。このため、厚生労働省所管法人等においてインシデントが発生した場合の報告、連絡体制について、速やかな対応が行われるよう報告、連絡体制の見直しを行うことが必要です。

このため､厚生労働省所管法人等でのインシデント発生時における当該法人等と厚生労働省の担当部局の役割の明確化を図るとともに､迅速な情報共有が行われるよう各部局の連絡窓口の見直しを図る等、報告、連絡等のオペレーションを改善します。

(3) 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

全ての厚生労働省所管法人等を対象として､厚生労働省が今後作成するリスク評価ガイドライン等に基づき､リスク評価を実施します。

また､個人情報等の重要情報が､サイバー攻撃等によりインターネットを通じて流出することを防止するため､緊急的な対応として､インターネットに接続されたネットワークから物理的又は論理的に分離するなど必要なシステム上の措置を講じたところです。その上で、上記のリスク評価結果に基づき、業務の内容や情報の性質､量に応じた情報セキュリティ対策の更なる改善に取り組みます。

さらに､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､運用されているか等について、自己点検を実施させるとともに、併せて、当該法人等に対し､厚生労働省に新たに設置する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）を行い、その実施状況を確認し、個人情報等の重要情報の管理を徹底させます。

（別紙）

○　「検証報告書」（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　平成 27 年 8 月 21 日）指摘事項

1　総論

本件情報流出をもたらせた標的型攻撃は、被害者が攻撃を認識し一応の防御をしているにもかかわらず、次々と手口を変えて攻撃を継続する極めて執拗かつ組織的なものであった。

これに対し、こうした標的型攻撃を含むサイバー攻撃に対する対応は、機構及びこれを監督する厚労省のいずれにおいても不十分なものであり、高度化する攻撃に対応可能な体制が整備されていなかったことが個人情報の大量流出という深刻な事態につながったと言わざるを得ない。

このような事態となった根本原因は、①機構、厚労省ともに、標的型攻撃の危険性に対する意識が不足しており、事前の人的体制と技術的な対応が不十分であったこと、②インシデント発生後においては、現場と幹部の間、関連する組織間（例えば、機構と厚労省、同一組織間の各部署、機構と運用委託会社など）、情報や危機感の共有がなく、組織が一体として危機に当たる体制になっておらず、その結果、組織内の専門知識を持つ者の動員ができず、担当者が幹部の明確な指揮を受けることもできないままに場当たり的な対応に終始し、迅速かつ明確な対処ができなかったことにある。

この点は、以下の二つの場面での対応に端的に表れている。

第一に、緊急事態に迅速に対応すべき CSIRT が、機構において組織されていないため、何らの備えもなく 5 月 8 日の第一段階の攻撃を迎え、情報セキュリティの専門知識を有する職員を動員できず、外部の専門家にも協力を得ないままで、担当者と運用委託会社とが、判明した個々の感染端末の特定と抜染に終始し後手に回ったことがあげられる。

第二に、本事案で第二段階の攻撃により標的型メールの一斉送信が行われ、このまま推移すれば、職員のうち誰かがメールの添付ファイルを開封し端末の感染が続発することが容易に予想される事態になったのに、情報の共有に欠け、組織が一体として危機に対処していないために、機構内部はもとより運用委託会社、厚労省からも

インターネット接続の全面遮断との意見が出ず、なすべき決断ができないまま情報流出に至ったことである。

本件情報流出をもたらせた個別的な要因をあげれば、人的体制と技術的な観点から２、３の通り様々な要因があげられるが、それらは、全て上記の根本的な原因に起因するものである。

２　日本年金機構における要因

(1)　サイバー攻撃に対する人的・組織的な準備の不足

機構は、本事案のような外部からのサイバー攻撃による情報流出の可能性について、業務運営上のリスクとして漠然と認識はしていたものの、事務処理誤りや内部者による情報流出等のリスクへの対応を優先し、サイバー攻撃による情報流出の可能性に対しては、認識が乏しく有効な準備を行っていなかった。

とりわけ、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。

①　人的体制の不備

人的体制の準備の面では、最高情報セキュリティ責任者以下情報セキュリティポリシーに定められた所定の体制は構築されていたものの、ポスト指定的に一般の職位に基づいて定めた体制であったため、実効的なリーダーシップに基づく対応が的確に遂行できなかった。また、内部の専門家を活用する努力も払われず、外部専門家にアドバイスを求める体制もなく、人的体制は質・量ともに不備があったと認められる。

②　サイバー攻撃への対応体制の不備

組織的な準備をみると、機構内では緊急時に必要なCSIRTが設けられておらず、そのため現場の担当者が中心となって対応せざるを得なかった。また、標的型攻撃に対する具体的対処が明示されたマニュアルが定められていたとは認められないばかりか、本件のような事態を想定した厚労省との緊急連絡体制も定められていなかった。

さらに、運用委託会社と機構との間の契約によれば、サイバー攻撃等のインシデント発生時の緊急時対応に関する具体的なサービス内容についての明確な合意がなされていなかったため、責任や権限の所在が不明確なまま、本件標的型攻撃に対処していた。

③　情報共有の不足

本事案を通じて、機構内部、機構と運用委託会社及びセキュリティソフト会社との情報共有ができていなかったことも、本件での不適切な対応につながったと認められる。

機構の担当者は攻撃の当初から標的型攻撃を疑っていたが、その懸念は機構の内部にも、また、不正通信を解析する運用委託会社及びセキュリティソフト会社にも共有されていない。機構幹部は、中堅幹部からきちんとした状況の報告や対処の進言を受けることができず、現場の担当者は幹部の明確な指揮を受けられないままに個々の事象の対応に追われていた。

また、運用委託会社は、部分的な情報をもとに5月8日の事象をマルウェアの分析結果に基づき「情報漏えいの可能性は極めて低い」と報告し、機構もその内容を鵜呑みにしてしまった。セキュリティソフト会社も全体の状況が分からないままマルウェア解析の情報提供をするにとどまった。

④　組織としての一体的な対応の不足

本事案の発生後、本事案への対応にあたった機構の役職員においては、相応の危機感が共有されていたことは認められるが、本事案の深刻な標的型攻撃であり、これによって大規模な情報流出が惹起され、機構全体の業務遂行に重大な支障が生じ得るといった可能性が真剣に検討された形跡はみられない。機構LANシステムの運用を担当する基幹システム開発部の一部の人員を中心に事態の対応にあたるのみで、他の部署や現場を広く巻き込んだ組織横断的な対応体制を構築することができなかった。

上記の情報共有の不足とともにこうした対応に終始した背景には、かねてから指摘されている機構のガバナンスの在り方が関係しているものとみられる。

このことは、共有フォルダへの個人情報保管の問題に端的に表れている。誰もが共有フォルダに重要な情報を大量に保管しては

いけないと知りつつ、現場は仕事の都合を優先し、幹部は、現場を知らないままに形式的な対応に終始して長期間を経過し、いつの間にか膨大な個人情報がインターネットの影響下に積み上げられ、今回の情報流出の重要な要因となっている。官民を問わず他の組織では考えられない対応である。

およそ、危機に際しての組織としての一体的な対応は、平素の組織の在り方がそのまま表れる。組織としての一体感のなさが、今回の事案を契機にそのまま表れたものということができる。

⑤　個人情報保護に関する認識の不足

すでにみてきたとおり、平時のシステムの運用に関しては、共有フォルダ上に重要な情報を暗号化等せずに保管していたことが大きな要因と考えられる。規定上定められていたアクセス権の設定、あるいはパスワードによる保護は標的型攻撃への対処としては役立たないものであった。

長期間にわたり個人情報がインターネットの影響下でのリスクに晒された状況にあったこと自体が、国民の重要な個人情報を大量に扱う組織としてはあるまじきことである。

そもそも外部からのサイバー攻撃による潜在的な情報流出のリスクを組織として把握している部署がなかった。その結果、リスク回避のためのアクセス制限やパスワードの設定などの規定が遵守されず、そうした状況が監査においても点検・改善される仕組みになかったことなど、およそ組織全体として個人情報保護に関する意識が低かったと認められ、これが、今回の情報流出につながった大きな要因と指摘せざるを得ない。

⑥　情報セキュリティリスク評価の不備

適切なセキュリティ対策を講じるには、まず、網羅的な情報資産の評価が不可欠である。しかしながら、機構においては、個人情報に限っても、機構内に散在する情報の所在の把握と、それらの情報に対するリスクの把握に必要なリスク・アセスメントが実施されておらず、リスクに基づいた有効な情報セキュリティ対策が講じられていなかった。

(2)　技術的な要因

① 脆弱性対応の不徹底

標的型攻撃への内部対策の一つとして、ソフトウェアベンダーから提供される脆弱性情報を定常的にチェックし、重大な脆弱性に対応するセキュリティパッチの適用を速やかに行う必要があるが、適用作業に伴うシステム停止等の影響等の懸念から、機構においてはその実施が先延ばしされていた。

本事案では、第三段階の攻撃において、既知の脆弱性が突かれたことにより、機構 LAN システムのディレクトリサーバの管理者権限が窃取されている。この脆弱性は昨年以来指摘されていたものであり、重要な脆弱性に対するセキュリティパッチの適用の遅れがこのような結果を招いた。

また、機構 LAN システムの端末における管理者 ID とパスワードが全て同一であったことにより、短時間に広範囲の端末への感染が拡大した。管理者権限の適切な管理が不十分であったと考えられる。

② システム監視の不十分性

機構 LAN システムにおけるシステム監視は標的型攻撃に対して不十分なものであった。機構 LAN システムにおいては、メール及びインターネットアクセスのログの採取は実施していたが、監視(モニタリング)は常時行われていたわけではなかった。また、取得されたログ情報の項目も、攻撃の詳細を把握するには不十分なものであった。

さらに、管理者権限によるシステムの操作履歴や各種サーバの挙動も監視されていなかった。

これらのシステム監視が十分になされなかった結果、攻撃の各段階において状況を把握するために相当の時間を要することとなった。

③ インシデント発生時の感染機器のフォレンジック調査の未実施

機構は、5 月 8 日に標的型攻撃を 4 時間にわたって受けた際、感染端末等に対するフォレンジック調査を行っていなかった。このため、次の攻撃を予測し対策を講ずることができなかった。

インシデント発生時にフォレンジック調査を行うことで、マル

ウェアを用いて攻撃者が機器を操作した状況が明らかになり、サーバまたは他の端末への感染の拡大の有無や窃取された情報などを推定することが可能になる。この調査結果に基づき、感染拡大のリスクに最大限の注意を払って事象の全容を把握する必要があるが、本件対応においてはこうした視点が欠落していたといわざるを得ない。

3　厚生労働省における要因

(1)　情報セキュリティ体制の脆弱性

情報セキュリティ事案に対処する政府の体制は、NISC－厚労省－各部局－年金機構などの特殊法人等、という情報連絡の流れを想定して構築されている。この流れにおいて、連絡のハブの役割を果たす情参室は、情報政策等の業務に加えて情報セキュリティを担当する所掌となっている。

ところが、情参室のセキュリティ担当の係は、通常の人事ローテーションの中で勤務する職員で構成されていた。同係はサイバー攻撃に対するルール整備や研修・訓練の実施も担っていたものの、実質わずか１名の限られた体制の中でマイナンバー制度の施行等多岐にわたる業務を抱えていたこともあり、専門的知見や人員数などの面でみると、その情報システムの規模との比において、到底十分といえる体制とは言い難かった。

厚労省内における専門家としては、CIO補佐官５名が配置されていたが、いずれの者も非常勤であり、かつ、システム刷新業務や調達業務などに加えて情報セキュリティを助言するという状況であったため、インシデントの報告が事後的になるケースが多かったなど、情報セキュリティに関して情参室の担当者等と緊密な連携はとれていなかった。

CSIRT体制も定められているが、その構成員は課室長以上となっており、技術力を持った実働要員が充てられていたわけではない。さらに、厚労省と関連組織とのCSIRT連携はなされていなかった。こうしたこともあり、NISC－厚労省－機構間の情報連携及びインシデント対応に遅れを生じることとなった。

(2)　機構LANシステムに対する監督体制の欠落

厚労省には、情参室、年金局事業企画課、年金局事業管理課の

各課室があるが、厚生労働大臣の監督下にあるはずである機構 LAN について、どれがその監督権限があるかが不明確であり、どの課室も自らに監督権限があるとの意識がない。これでは、機構 LAN で何らかの危機的事態があったとしても適切な指揮監督ができないのはやむを得ない。

(3) 情報連絡の遅延

厚労省においては、情参室に省内及び傘下の特殊法人等のサイバー攻撃に関する情報が報告されることになっている。しかし、その報告は、インシデントが収まってから書面でなされることが多く、肝心な場合には後手に回り適時適切な対応をすることができない。そのため、配置されていた CIO 補佐官の知識を十分に生かすことができなかった。今回の標的型攻撃での対応はその典型例である。

4 4 月 22 日に関する指摘

(1) 平成 27 年 5 月 8 日以降に発生した機構に対する本件標的型攻撃は、これに先立つ同年 4 月 22 日に発生した厚労省に対する標的型攻撃と類似の手口によるものであった。

平成 27 年 4 月 22 日の標的型攻撃は、厚労省年金局及び地方厚生局を対象としたものであり、メールを受信した職員が標的型メールを閲覧し、添付ファイルを開封したことから、職員の端末が感染した。この結果、C&C サーバに対する不正な通信が発生した。この通信のアクセスログによれば、各アクセスは、GET メソッドといわれる、外部から情報を取得する命令文による HTTP 通信であるものの、不明な文字列が付加されているなどの特徴があった。

この不正な通信は、NISC からの通知を受けた厚労省において URL ブロックを行ったことにより、通信発生の約 2 時間後に遮断された。

攻撃者は、次なる攻撃を検討し、機構が狙われるに至ったものと考えられる。4 月 22 日に感染した端末が通信を行った C&C サーバのドメインは、5 月 8 日に機構において感染した端末が通信を行った C&C サーバと同一であり、サブドメインのみが異なるものであった。したがって、仮に 4 月 22 日の段階で、厚労省統合ネットワークにおいて、ドメイン単位での URL ブロックを実施して

いれば、5 月 8 日に発生した同一ドメインの C&C サーバに対する機構との不正な通信は防ぐことができた。

現実には 4 月 22 日の時点で厚労省において実施した URL ブロックはサブドメイン単位のものであり、ドメイン単位での URL ブロックを実施したのは後述するとおり 5 月 8 日に至ってからであった。

(2) 厚労省においては、先に述べたとおり、本件標的型攻撃に先立つ 4 月 22 日に、本事案と類似の手口による標的型攻撃を受け、その際の攻撃に用いられたマルウェアについて、NISC からは感染した場合には被害が大きくなる可能性があるとの情報を得ていた。しかしながら、5 月 8 日の段階で、厚労省から機構に対して、何ら情報提供が行われなかった。

そのため、機構においても、本件が、厚労省やその関係機関を狙った一連の標記型攻撃の一環であるとの着想に至らなかった。

○ 「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」（内閣サイバーセキュリティ戦略本部平成 27 年 8 月 20 日）指摘事項

1 CSIRT(情報セキュリティインシデント対応チーム)の運用等に関する検討

(1) CSIRT の運用に関する検討

政府機関の情報セキュリティインシデント(以下「インシデント」という。)に備えた体制は、「政府機関の情報セキュリティ対策のための統一基準」(平成 26 年 5 月 19 日情報セキュリティ政策会議決定)(以下「政府統一基準」という。)において、情報セキュリティインシデント対応チーム(CSIRT)を整備し、以下の事項を含めて、その役割を明確にすること等を規定している。

- インシデントを認知した際に、CISO や NISC に報告すること(政府統一基準 2.1.1(6)(c)、2.2.4(2)(b)及び 2.2.4(2)(f))
- インシデント発生時に、CISO や NISC 等への連絡のため、各府省庁において報告窓口を含む報告・対処手順を整備すること(政府統一基準 2.2.4(1)(a))
- CSIRT に属する職員については、専門的な知識又は適性を有すると認められる者を選任すること(政府統一基準 2.1.1(6)(b))

厚労省は、政府統一基準に準拠して情報セキュリティポリシーを定める必要があるが、特殊法人である機構は、政府統一基準の適用対象とされていない。ただし、情報セキュリティ対策は、それに関わる全ての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある(政府統一基準 2.1.1)。

このような方針に示されるとおり、厚労省としては、機構が厚労省の所掌事務である年金事務について厚労省と一体となって業務を行っていること、また、機構の取り扱う情報が大量の個人情報であることに鑑みれば、可能な限り政府統一基準と同等レベルの情報セキュリティ対策が講じられるべく、機構を適切に監督する立場にある。

こうした背景を踏まえ、両組織における CSIRT の運用等について調査・検討を行った。

① インシデント発生時等の報告・連絡等について

政府統一基準においては、上述のとおり、インシデントに対応するための体制の整備や、インシデントを認知した際の報告・対処手順を整備するよう求めている。

厚労省は、政府統一基準に準拠し、情報セキュリティポリシーを定めており、インシデントを認知した際は、CISO(官房長)及び NISC に報告する旨規定している。また、インシデントが発生した場合の対処及び報告等の手続きについては、インシデント対処の手順書を定めており、統括情報セキュリティ責任者(情報政策担当参事官)は、すべての行政事務従事者に周知することとしている。報告等の手順の概要をまとめると、インシデント発生時等の報告・連絡については、次のようになっている。

(a)省内外(NISC を含む。)からインシデントの発生の連絡を受け付ける情報セキュリティ担当の窓口は、情参室のサイバーセキュリティ対策専門官及び情報セキュリティ対策係。

(b)行政事務従事者が、インシデントを認知した場合には、その者が所属する課室長等に報告し、課室長等の指示に従う。
(c)当該インシデントに係る課室長等は、CSIRT と情報を共有する。
(d)当該インシデントに係る課室長等は、当該インシデントの発生している当該部局の総括的な課長等に報告し、緊急対応策についての指示をする。
(e)当該インシデントに係る課室長等は CISO に速やかに報告し、CISO は、当該インシデントの発生している当該部局の総括的な課長等に対して、被害拡大防止等の指示等を行う。

今回のインシデントにおいては、厚労省によれば、セキュリティポリシーに基づく手順書に基づいた必要な措置は一応とられていたが、責任者への報告はなされていなかったとしている(今回のインシデントにおいて、機構において発生したインシデントについては厚労省年金局事業企画課長への報告、GSOC からの通知については情報政策担当参事官への報告が、これに該当すると考えられる。)。

なお、機構のセキュリティ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、その具体化はシステム障害対応を主たる目的としたリスク管理一般の規定等に委ねている。そして、リスク管理一般の規定においては、リスクの定義、導入、運用、分析・評価、見直し等の枠組みが規定されているものの、サイバー攻撃を想定した具体的な対応について、明確化されていない。

② CSIRT 体制について

厚労省の情報セキュリティポリシーでは、CSIRT に属する職員について、CISO(官房長)、情報政策担当参事官、当該事案に係る部局の総括的な課長及び担当課室長等、CISO アドバイザ(CIO 補佐官)を充てるとしている。また、CSIRT の庶務は情参室で行い、CISO アドバイザは、専門的な知識及び経験に基づき、緊急時における対応等情報セキュリティ対策全般に対しての助言等を行うこととしている。

今回の事案発生時点においては、CSIRT が機能するための前提となる報告等がなされていなかったが、CSIRT の構成員が課室長等以上であり、実働要員(課長補佐以下の職員)が選任・指名されてい

なかった点にも留意が必要である。

一方、日本年金機構セキュリティポリシーにおいては、インシデント対処の必要性や、その具体的な規定は複数の規程類で規定している。リスク管理全般については、リスクの定義、導入、運用、分析・評価、見直し等の枠組みが規定されているものの、サイバー攻撃を想定した具体的な対応は明確となっていない。また、いずれの規程類においてもCSIRT体制についての定めはなかった。

なお、機構によると、平成27年7月10日からCSIRT体制の構築をはじめとしたセキュリティ体制の整備の検討を開始したとしている。

(2) システムへの多重防御(標的型攻撃対策)に関する検討

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。

典型的なものとしては、システム内部に潜入し、侵入範囲を拡大し、重要な情報を窃取し又は破壊する攻撃活動が考えられる。

① 政府統一基準における対策について

こうした一連の攻撃活動は、未知の脆弱性を悪用する等の手法も用いて実行されるため、完全に検知・防御することは困難であることから、政府統一基準(6.2.4)において、標的型攻撃による組織内部への侵入を低減する入口対策のみならず、内部に侵入した攻撃を早期検知して対処する内部対策、侵入範囲の拡大の困難度を上げる内部対策及び外部との不正通信を検知して対処する内部対策から構成される多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要があることが示されている。

具体的な対策を示すものとして、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(平成26年6月25日情報セキュリティ対策推進会議)(以下「リスク評価等ガイドライン」という。)があり、その適用範囲は、国の行政機関と記述している。

② 厚労省等における状況

厚労省においては、厚労省統合ネットワークにおける標的型攻

撃に対する多重防御の取組を進めていたが、機構の情報系ネットワークは、リスク評価等ガイドラインの取組の対象としておらず、標的型攻撃に対する多重防御の取組が十分でなかった。

さらに、標的型攻撃からの有効な遮断機能を有すると考えられるインターネットに接続していない業務系から、インターネットに接続をしている情報系に個人情報を移して取り扱っていたため、標的型攻撃を受けるリスクに当該個人情報をさらす結果となった。

○　「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」（日本年金機構不正アクセスによる情報流出事案に関する調査委員会平成 27 年 8 月 20 日）において構造的な要因とされた事項等

１．インシデントへの対応体制

＜要因＞

○　本事案の 5 月 8 日（金）以降の一連の対応については、CIO（システム部門担当理事）と情報セキュリティ担当部署の部長、グループ長及び担当者がラインとして対応してきましたが、その対応体制について、以下の問題がありました。

①　基本的対応は担当者任せとなっており、CIO（システム部門担当理事）や部長から、当該担当者の判断について、判断根拠の確認や具体的指示を行った事跡は確認できていません。5 月 8 日（金）の第 1 次攻撃の際、担当者からは標的型メール攻撃の疑いが提起されましたが、担当ラインは特に対応について指示を行わず、また、その後の具体的な対策についても指示を行いませんでした。

②　理事長、最高情報セキュリティ責任者（副理事長）への報告が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ませんでした。

③　本事案を担当してきたラインに情報セキュリティに関する専門的な知識及び経験を有する職員がおらず、また、セキュリティアドバイザーに任命されていた担当者も他の業務に当たっていたことから、ラインにおいて必要な対応・判断ができませんでした。

④　情報セキュリティ担当部署と契約担当部署が異なり、責任の所在が不明確で連携が不十分となっていました。これら両部門の連携を図ること、あるいは組織の統合を検討することは CIO

（システム部門担当理事）の役割でありましたが、具体的な行動はとられていませんでした。

２．共有ファイルサーバの管理

＜要因＞

○　そもそも、パスワード設定などのセキュリティ対策が条件となってはいるものの、個人情報をインターネット接続環境下に置くシステム設計に問題がありました。

○　また、共有ファイルサーバがインターネット接続環境下に設置されているというリスク認識が甘かった文書管理担当部署において、共有ファイルサーバの運用ルールが定められていました。このため、外部からの攻撃に対する対策に関して十分な検討が行われず、パスワード又はアクセス制限の設定といった内部からの脅威に重点を置いた情報セキュリティ対策となっていました。外部からの攻撃に対し、アクセス制限が有効でないことが本事案で明らかとなっています。

○　一方、情報セキュリティ担当部署では、インターネット接続環境下にある共有ファイルサーバ内に個人情報が置かれている実態、リスクを認識していましたが、具体的な指摘・提言はしておらず、対処策の検討も特にしていませんでした。共有ファイルサーバの運用ルールの共同所管部署として果たすべき役割が果たされていませんでした。

○　さらに、運用ルールを定めていた文書管理担当部署において、共有ファイルサーバの運用ルールが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ました。

３．情報セキュリティポリシー等

＜要因＞

○　情報セキュリティポリシーは、厚生労働省の情報セキュリティポリシーに沿って制定・改正してきましたが、その改正に遅れがあり、標的型メール攻撃に対する基本的対策事項等に関する記載が不足していました。また、標的型メール攻撃に対するインシデント手順書も作成されていませんでした。

○　当機構では、膨大な個人情報を保有しているにもかかわらず、厚

生労働省の改正内容を受け身で情報セキュリティポリシーに後追いで反映させるのみで、職員研修や訓練が行われていませんでした。膨大な個人情報を保有しているという緊張感が欠如しており、これまで、役員を含め、精緻な検討・議論がされていませんでした。

４．職員研修

＜要因＞

○　情報セキュリティ研修における研修テーマや教材などの研修内容に関しては、実質的に担当者レベルで決定されており、情報セキュリティ担当部署として、その効果に責任を持った意思決定が行われていませんでした。

５．ガバナンス・組織風土のゼロベースからの抜本改革

＜要因＞

○　組織の上層部に情報が集約されず、定めたルールが組織内に正確・迅速に伝わらないといったように、組織としての一体感が不足しているという従来からの問題点が解消されていませんでした。

○　監督者である厚生労働大臣・厚生労働省と問題共有をする意識、国から厳正な業務執行を請け負っているとの自覚が不足していました。また、重層的な情報共有のルールがありませんでした。

○　個人情報流出に関するお客様への説明誤りの件についても、本事案の重大性に鑑みれば、ただちに厚生労働省に報告するとともに、速やかに公表すべきでしたが、通常の事務処理誤りの対応と同様として個別対処を完了させた後に、月末の定例報告で足りるとしたのは、一部幹部の思い込みにより招いた失態でした。

（別添２）

業務改善計画

日本年金機構

Ⅰ　目的

○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及び情報セキュリティ対策の強化について、厚生労働大臣から業務改善命令（平成２７年９月２５日）を受けたことを踏まえ、日本年金機構再生本部及び情報管理対策本部において検討を進め、改善計画としてとりまとめたもの。

（１）今般の不正アクセスによる情報流出事案により明らかとなった、組織としての一体感の不足、ガバナンスの脆弱さ、リーダーシップの不足、ルールの不徹底などの構造的な問題の抜本的な解決に向けて、自ら考え、自ら改革し、公的年金制度を執行するという緊張感、責任感、使命感にあふれ、職員が一丸となって国民の信頼に応えられる組織として機構を再生する。

（２）情報開示のあり方について、国民の十分な信頼を得られるよう抜本的に見直しを行う。

（３）国民の年金を最優先に守る観点から、情報セキュリティに係る組織面、技術面、業務運営面を全般的に見直し、インターネットからの攻撃をはじめとする情報セキュリティ上の脅威に対して強固な情報システムを構築するとともに、実効性のある対応体制を構築することにより国民の重要な個人情報（以下「年金個人情報」という。）の保護を確実に行う。

Ⅱ　取組期間

○平成２８年度からの３年間を集中取組期間とする。

Ⅲ　業務改善計画の概要

１．組織の一体化・内部統制の有効性の確保について

○以下の３つの改革を進めることにより、組織の一体化を図り、内部統制の有効性を確保する。

（１）組織改革

○縦割りを排除し、本部と現場が一体となった効率的・機能的な執行機関として再構築する。

（２）人事改革

○希望とやりがいをもって組織一体となって業務に取り組む人事を実現する。

○お客様のために努力する職員を高く評価し、国民の年金を確実に守る人材を育成する。

（３）業務改革

○業務効率化・合理化を徹底し、現場実態を踏まえたルール設定・遵守の仕組みをつくる。

２．情報開示の抜本的な見直しについて

○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。

３．情報セキュリティ対策の強化について

○以下の３つの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）組織面

○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。

（２）技術面

○年金個人情報に対して攻撃が及ばないシステムとするため、独立したインターネット環境を構築し、年金個人情報を管理・運用する領域を基幹システムに限定するとともに、機構ＬＡＮシステムからのアクセス制限による分離を徹底するなど、情報システムのリスク評価・分析結果を踏まえ、各システムの入口・内部・出口の多重の防御対策を実施する。

（３）業務運営面

○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、役職員の危機意識の向上、運用ルールやインシデント発生時の対処手順の徹底を図るため、情報セキュリティポリシーの整備及び職員研修の充実を図るとともに監査体制を整備する。

Ⅳ　業務改善計画

１．組織の一体化・内部統制の有効性の確保について

（１）組織改革

◎縦割りを排除し、本部と現場が一体となり、人材を糾合し、現場実態を踏まえた適切な意思決定システムを確立するとともに、お客様のニーズをとらえた機能集約等を図ることで、効率的・機能的な執行機関として再構築する。

①本部

a)常勤役員会の設置

○経営上重要な案件内容及び意思決定過程の共有のために、「常勤役員会」を設置

○理事長、副理事長、常勤理事、常勤監事、経営企画部長及び財務部長の他、理事長が指名する職員により構成

○議事は、案件担当部の部長が説明

b)現場管理統括部署の設置

○年金事務所及び事務センター等の現場管理、指導、評価及び全体情報共有等を横断的かつ一元的に管理する「地域統括部（仮称)」を設置

c)本部組織の再編・効率化

○事業に関連する部門について、国民年金・厚生年金保険等の制度別の縦割りを排除するため、事業企画部門と事業推進部門（仮称）に再編

○お客様との接点に関する施策は、事業推進部門（仮称）が一元的に担当

○本部現業部門を核とした給付関係業務の再編

②ブロック本部

○組織の一体化、意思決定・情報共有ルートの短縮、人員集約及び効率化を目的に、地域分散型機能をもつブロック本部を本部に統合

※現場管理統括部署の設置とブロック本部の統合については、担当理事を発令

③年金事務所

○お客様の利便性を高めつつ業務の効率化を図るため、年金事務所のフルスペック体制を見直し

○法人向け業務の集約及び年金相談の充実のためのチャネルの整備・拡大

④事務センター

○業務の効率化・合理化及び標準化の観点から、県別体制を抜本的に見直し、統合・集約を促進

○障害年金業務については、早期に集約化を実施

（２）人事改革①　～人事制度のあり方・職員の活性化～

◎職員が希望とやりがいをもって、モチベーションを高く保ち、組織一体となって業務に取り組める人事を実現する。

①組織一体化

a)人事権の本部一元化
- ○ブロック本部の人事権を本部人事管理部に統合

b)役職（ポスト）と資格（グレード）の関係の見直し
- ○本部・ブロック本部の統合、年金事務所体制の見直しに伴い、国民接点重視の観点から見直し
- ○職責の困難度、特殊性を考慮した管理職手当のあり方の見直し

c)全国異動の促進とルールの見直し
- ○組織一体化のため、現場相互間の異動に加え、本部・現場間異動を促進
- ○全国一括採用の下で全国拠点網を維持するための全国異動を実施
- ○現行の全国異動ルールの問題点の見直し

②希望とやりがい

a)明確なキャリアパスの提示
- ○専門職とゼネラリスト別のキャリアパスの提示
- ○役員を展望しうるキャリアパスの提示
- ○執行役員制度の検討
- ○職務に応じた人事異動サイクルの明確化

b)給与のあり方の見直し
- ○管理職と一般職との給与逆転現象の解消に向けた見直し（管理職手当と一般職の時間外手当との関係のあり方）
- ○地域調整手当等諸手当のあり方の検討

c)研修制度の充実
- ○多様な研修制度の採用（外部機関、学校、企業による研修（通学・合宿）、海外の外部機関での勤務など）

③非正規職員の活性化と依存の是正
- ○非正規職員に対する無期化制度の活用（地域限定職と位置づけ、主に事務所窓口の専任担当者として育成）
- ○評価の導入と意欲・成果に応じた処遇
- ○業務の効率化による派遣・外部委託の活用

④女性の活躍推進
- ○女性活躍のための多様なキャリアパスの提示（若年女性職員の増加を踏まえた長期的な女性管理職比率の設定）
- ○女性が活躍する分野の拡大と女性管理職育成プログラムの確立
- ○女性役員の登用

（３）人事改革②　～人事評価制度の見直し・管理職の活性化～

◎お客様のために努力する職員を高く評価し、リーダーシップや専門性の高い職員を養成することで、国民の年金を確実に守る人材を育成する。

①信賞必罰の人事評価

a)役員への評価の厳格化

b)意欲・実績ともに低い職員への厳正な対処

○低評価が継続している職員を対象に、再生プログラムの提示と降格の実施

○降格制度の見直しと厳正な運用

c)３６０度アセスメントの導入

○管理職の適格性の指標として活用

②人材育成

a)成果とプロセスのバランスのとれた評価

○能力評価と実績評価の一体化

○絶対評価に基づく相対配分方式の導入

○評価の合議制の義務付け

b)働く意欲に結びつく、メリハリのついた評価と処遇の実現

○賞与配分、評価分布の見直し等

③管理職のレベルアップとリーダーシップの確立・強化

a)役職定年制度と早期退職募集制度の導入

○一度管理職になると一律に定年まで役職にあり続けることの是正とポストの検討

〔役職定年年齢(案)〕

管理職Ａ群 … 55 歳　管理職Ｂ群 … 57 歳　管理職Ｃ群 … 60 歳

〔早期退職募集制度(案)〕

募集により原則として毎年実施、年齢等の要件は募集時に設定

b)管理職への若手登用の促進

○試験に限定している登用制度の見直し(弾力化)

○管理職の負担軽減と若手育成のため「課長代理」「主任」を設置

c)管理職育成プログラムの導入

○現在の業務スキル向上を中心とした研修体系に加え、民間企業との人事交流や体験学習を組込み、直に体験することにより管理者としての意識を醸成するためのプログラムを導入

（4）業務改革①　～業務の効率化・合理化～

◎業務効率化・合理化（人員配置の適正化）と、現場実態を踏まえたルール設定・遵守の仕組みの確立により、お客様対応に注力できる体制を構築する。

①業務の集約化

a)本部への機能集約

○全国に設置している９ブロック本部を本部に集約（本部・現場への人員の再配分）

b)事務センターへの業務集約

○本部の現業業務及び各 40 事務センターの業務の集約の促進（障害年金、記録審査の集約に着手）

c)年金事務所の機能集約

○都市部に点在する年金事務所の徴収・適用対策を強化するため、主要な年金事務所に機能を集約

②業務の改廃・外部委託化・システム化

a)業務の改廃

○業務削減会議（仮称）を設置し、業務の効率化を推進（発送物の統廃合等）

○新規業務開始時における既存業務のスクラップアンドビルドの徹底

b)本部の非現業業務の外部委託化

○本部の非現業業務のうち、給与事務や契約後支払事務などの定型的業務を外部委託化

c)事務センター・年金事務所の事務の簡素化及びシステム化

○年金給付の請求書等の事務処理工程の簡素化

○各種届書の事務処理（受付～決定）のシステム化（電子審査・決裁）や、徴収事蹟管理のシステム化

③年金相談の充実・お客様チャネルの拡充

a)年金相談の予約制の拡充

○お客様の相談待ち時間をなくし、より丁寧な相談対応を行うため、全国の年金事務所の相談窓口を原則として予約制とし、全国の予約状況を案内する年金相談予約センター（仮称）を設置

b)新規チャネルの開設

○お客様が年金相談をしやすい環境を整備するため、遠隔地の市町村役場等に試行的に「テレビ電話」を設置

c)既存チャネルの充実

○ねんきんネットに、再交付申請等の手続き機能や事業所用の情報閲覧機能を追加

④人員配置の適正化

a)業務量調査の実施

○各拠点の職種（正規・非正規・派遣）に応じた業務内容を明確化し、職種毎の業務量調査を実施

b)適正人員の配置

○効率化・合理化策の人員効果と業務量調査の結果を踏まえ、各拠点に正規・非正規職員を適正配置

○将来にわたって、機構の基本計画に沿った人員計画が立てられるよう継続的な適正人員の配置を検討

（５）業務改革②　～ルールの設定・徹底～

◎業務効率化・合理化（人員配置の適正化）と、現場実態を踏まえたルール設定・遵守の仕組みの確立により、お客様対応に注力できる体制を構築する。

①「指示・依頼」発出件数の削減

a)ルールを徹底すべき重要な指示に限定して「指示・依頼」を発出することとし、「５割」削減（平成 26 年比）を目標

【26 年発出件数（本部・ブロック本部）】約 4,300 件(※１)

→【発出ルール等の改善後発出件数】約 2,200 件(※２)

(※１)国からの許認可通知に基づき発出された約 10,000 件の作業指示については件数から除外

(※２)削減対象として想定される「指示・依頼」

・本部からブロック本部へ報告集計を指示したもの：約 1,100 件

・本部の指示内容を補足したもの：約 350 件

・研修受講命令、会議開催案内：約 700 件

b)本部の現場管理統括部署が、新たな発出ルールに基づく「指示・依頼」発出の妥当性及びルール徹底の実効性確保の観点からのチェックを担当

c)ブロック本部（事務センターを含む。）の「指示・依頼」の発出権限を、原則、廃止

②マニュアルの一元化

a)業務処理、内容審査、入力方法と、複数に分かれたマニュアルを統合

b)本部内に年金制度・年金業務に精通した職員を配置したマニュアル担当部署を設置し、マニュアルメンテナンスを一括対応

c)マニュアルメンテナンスの外部委託化すべき範囲と内容を検討

d)業務の標準化を進め、業務手順の地域による相違を排除

③ルール徹底を行う責任部署の明確化

a)現場に対するルール徹底の責任部署は、本部の現場管理統括部署と明確化

b)現場管理統括部署の地域マネージャー（仮称）が「指示・依頼」の伝達結果を把握し、状況に応じた指導を実施

c)現場管理統括部署がマニュアルの改善が必要と判断した場合は、マニュアル担当部署に連絡

d)拠点に「指示・依頼」の伝達担当者を設置し、「指示・依頼」の伝達を行うとともに職員のスキルチェックを実施

２．情報開示の抜本的な見直しについて　～情報開示・共有の促進～

◎透明性を確保し、お客様に安心いただける組織づくりのため、情報開示体制を見直すとともに、組織内及び厚生労働省との間の情報共有を強化する。

（１）情報開示の促進

①情報開示の担当部署と担当理事の設置（理事はコンプライアンス及び監査も担当）

②モニタリングシステムの構築と監査機能の活用

○届書等の受付進捗管理システム、お客様対応業務システムなどの各種情報等をモニタリングし、問題点を早期に把握する仕組みを構築

○その情報に基づき監査を行うことで、事象の洗出しを行い、迅速に開示

③情報開示ルールの見直し・規定化

○現行ルールを見直し、案件把握から開示までの手続き等を明確化

④「悪い知らせ」の報告を促すよう制度を見直し

○起きたことよりも報告しないことを厳しく評価

（２）組織一体化のための情報共有の促進

①本部と現場の情報共有

○現場管理統括部署の地域マネージャー（仮称）を、情報共有のキーマンとし、本部情報の伝達、現場からの情報の吸収に責任を持つポストと位置づけ

○報道発表事項、マスコミ等に取り上げられた事項については、お客様からの照会対応を円滑に行えるよう、原則として即日現場への連絡を徹底

○情報共有ツールとしてＴＶ会議システムを導入

②現場からの日次での業務報告の実施

③本部内の情報共有

○本部内の情報共有の責任部を経営企画部と位置づけ

○主要課題についての各部の対処・共有状況を常勤役員会に報告

（３）厚生労働省との情報共有の強化

○組織的に継続して取り組むべき課題の進捗管理表を作成し、年金局と共有するとともに、年金局と機構の定例連絡会議で報告

○役員等幹部を含めたそれぞれのレベルでの報告・連絡・相談ルールを明確化

○年金局と機構との連携、相互理解を促進するため、年金局職員と機構職員の相互の人事交流を拡大

３．情報セキュリティ対策の強化について

（１）情報セキュリティ対策①　～組織面～

◎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。

①情報管理対策本部の設置

○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「日本年金機構情報管理対策本部」を設置（平成 27 年 10 月１日設置済）

②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（３グループ体制）を設置（平成 27 年 10 月１日設置済）

③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、情報管理対策室（インシデント対策グループ）を中心に本部内の即戦力のある職員で構成する機構ＣＳＩＲＴを設置（平成 27 年 10 月１日設置済）

※ CSIRT：Computer Security Incident Response Team（通称：ｼｰｻｰﾄ）

④最高情報セキュリティアドバイザーの設置

○情報管理対策本部等に対して、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・経験を有する者（又は機関）を設置予定

（2）情報セキュリティ対策②　～技術面～

◎年金個人情報に対して攻撃が及ばないシステムとするため、独立したインターネット環境を構築し、年金個人情報を管理・運用する領域を基幹システムに限定するとともに、機構ＬＡＮシステムからのアクセス制限による分離を徹底するなど、情報システムのリスク評価・分析結果を踏まえ、各システムの入口・内部・出口の多重の防御対策を実施する。

①基幹システム

メインフレームを主体とする基幹システムはシステムアーキテクチャ上の特性から情報セキュリティが確保されていることを踏まえ、引き続きインターネットには接続しないこととし、多重の防御対策を徹底

a)年金個人情報専用の共有フォルダ

○年金個人情報を収納対策等に使用する場合は、基幹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

○当該フォルダへのアクセスは窓口装置(WM)のみ可能とし、ＬＡＮ－ＰＣからは遮断

○年金個人情報を含むファイルは自動暗号化

b)窓口装置(WM)

○基幹システムへのアクセスを生体認証及びＩＤ・パスワードにより管理

○年金個人情報専用の共有フォルダへのアクセスは生体認証により管理

○未知のウィルス検知機能の追加による入口対策を強化

②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、窓口装置（WM）から機構ＬＡＮシステムへのアクセスは業務上必要な機能に限定

a)機構ＬＡＮシステムはイントラネットメール、グループウェア及びマニュアル等を有するが、年金個人情報は保有しない

b)年金個人情報の保護強化の観点から窓口装置（WM）から、機構ＬＡＮのグループウェア等を利用する際は業務上必要な機能に限定

c)運用管理（サーバ・端末）

○セキュリティパッチを最新化、重要機器の監視

○ＬＡＮ－ＰＣの管理者権限のＩＤ・パスワードを個別化、適切な管理

③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、基幹システム及び機構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

a)機能は、ＷＥＢ閲覧、インターネットメールのみ

b)インターネット専用ＰＣを設置（窓口装置(WM)及びＬＡＮ－ＰＣからのアクセスは不可）

④ねんきんネット

○ねんきんネットについては、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

（３）情報セキュリティ対策③　～業務運営面～

◎情報セキュリティに関する役割・責任・権限を明確にするとともに、役職員の危機意識の向上、運用ルールやインシデント発生時の対処手順の徹底を図るため、情報セキュリティポリシーの整備及び職員研修の充実を図るとともに監査体制を整備する。

①情報セキュリティポリシーの改正等

a)情報セキュリティポリシーの改正

○体制の整備、情報の保存方法、外部委託における情報セキュリティの確保及び標的型攻撃対策等、厚生労働省情報セキュリティポリシーに準拠しつつ、実効性のある内容に改正

b)情報セキュリティインシデント対処手順書の制定

○情報セキュリティインシデント発生時に迅速かつ的確に対処するため、具体的な手順を明確に規定

c)関係規程の改正

○情報セキュリティポリシーの改正等に伴い関係規程を整備

②情報セキュリティ研修等の実施

a)情報セキュリティ研修の実施

○情報セキュリティ関係規程等への理解を深め運用ルールを徹底するため、情報セキュリティ対策の内容やサイバー攻撃の動向を踏まえた情報セキュリティ研修を全職員に対して毎年度１回以上実施（採用後３か月以内に実施）

○機構ＣＳＩＲＴに属する職員に対するインシデント対応能力向上のための研修を実施

b)情報セキュリティ対策訓練の実施

○情報セキュリティ対策の運用ルールの更なる徹底を図るため、実践形式の訓練を実施

③監査体制の整備

a)内部監査の強化

○本部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とともに、随時に無予告の監査を行うこと等により、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

b)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

○独立した外部の専門家による情報システムのリスク評価・分析及び脆弱性診断等により、情報セキュリティの問題点を把握するとともに、これに対して適切に対処しているか定期的、継続的に情報セキュリティ監査を実施

４．計画の推進体制の構築

○計画の推進に当たっては、機構の現状について、適時適切に把握・分析・評価を行いながら、計画の内容を確実に実行・進捗管理する。

○このため、理事長直轄の推進部署において、別添に基づき計画の推進・実行・工程管理・実施状況のフォローアップ等を一元的に実施する体制を確立する。
今後、施策内容、工程の精緻化を行い、具体的施策については、各年度計画等において定めることとする。

○また、計画の進捗状況については、組織の一体化等について機構に設置された外部機関のチェックを受けるとともに、情報セキュリティの強化について政府サイバーセキュリティ戦略本部に定期的に報告することとする。

○さらに、理事会及び運営評議会はもとより、社会保障審議会年金事業管理部会にも適時適切に報告することとする。

以上

（ 別 添 ）

業務改善計画　各事項の実施時期

事項		実施時期（年度）27	28	29	30
Ⅳ1（1）組織改革					
本部 ブロック本部	常勤役員会の設置	平成28年1月より設置			
	現場管理統括部署の設置		平成28年4月より設置（順次機能集約）		
	本部組織の再編・効率化		平成28年度より順次実施		
	ブロック本部を本部に統合（人事権の本部一元化含む）		平成28年度より機能別に順次統合		
年金事務所	フルスペック体制の見直し、法人向け業務の集約		平成28年度より機能集約のモデル実施を開始		
事務センター	統合・集約を促進（広域化を促進）		平成28年度より計画的に統合		
	本部・事務センターの障害年金業務及び記録審査業務の集約化			記録審査業務の集約化は平成29年度より実施、障害年金業務の集約化は平成29年度より順次実施	
Ⅳ1（2）人事改革①　～人事制度のあり方・職員の活性化～					
組織一体化 希望とやりがい	明確なキャリアパスの提示、全国異動の促進とルール見直し、研修制度の充実	平成27年度より職員周知を開始し、平成28年度より本格的な運用を開始			
	役職と資格の関係の見直し		平成28年度より順次見直し		
	給与のあり方の見直し			平成29年度より順次見直し	
非正規職員の活性化と依存の是正	位置づけの明確化と育成、評価の導入と処遇		平成28年度中に位置づけ等を明確にし、平成29年度より新評価制度の運用開始		
女性の活躍推進	活躍分野の拡大と育成プログラムの確立、長期的な女性管理職比率の設定		平成28年度より順次実施		
Ⅳ1（3）人事改革②　～人事評価制度の見直し・管理職の活性化～					
信賞必罰の人事評価	役員への評価の厳格化	平成27年度の評価から実施			
	意欲・実績ともに低い職員への厳正な対処	平成27年度より対象者選定等を開始し、平成28年度より降格等の対処を実施			
	360度アセスメントの導入		平成28年度中に実施		
人材育成	成果とプロセスのバランスのとれた評価、働く意欲に結びつく、メリハリのついた評価と処遇の実現		平成28年度中に実施		
管理職のレベルアップとリーダーシップの確立・強化	役職定年制度と早期退職募集制度の導入		役職定年制度については平成28年度上期に制度設計・周知の上、平成28年度末より段階的に実施、早期退職募集制度については平成29年度より実施		
	管理職への若手登用の促進、管理職育成プログラムの導入		平成28年度より実施		

（ 別 添 ）

業務改善計画　各事項の実施時期

事項		実施時期（年度） 27 / 28 / 29 / 30
Ⅳ1（4）業務改革①　～業務の効率化・合理化～		
業務の改廃・外部委託化・システム化	業務削減会議（仮称）の設置	平成28年度上期より実施
	非現業業務の外部委託化、事務の簡素化・システム化	平成28年度より順次実施
お客様サービスの向上	年金相談の予約制の拡充	平成28年度下期より拡充
	テレビ電話の設置	平成29年度下期より試行
	ねんきんネットの拡充	平成30年度より拡充
人員配置の適正化	業務量調査、適正人員の整理、派遣職員の活用	平成28年度より事務センター、平成29年度より年金事務所の適正人員の配置に着手
Ⅳ1（5）業務改革②　～ルールの設定・徹底～		
「指示・依頼」発出件数の削減	「5割」削減の達成	平成28年度の「指示・依頼」より発出基準を見直し、平成26年比で5割削減を達成
	本部以外の「指示・依頼」発出権限の廃止、現場管理統括部署による審査	平成28年度より実施
マニュアルの一元化	マニュアルの統合・標準化作業、マニュアル担当部署の設置（精通した職員の配置、マニュアルメンテナンスの検証）	平成28年度よりPTを立ち上げ、順次実施 （マニュアル担当部署については平成29年度より設置）
ルール徹底を行う責任部署の明確化	責任部署の明確化、ルール徹底のための地域マネージャー（仮称）・伝達担当者の設置	平成28年度より現場管理統括部署を責任部署と位置づけるとともに、ルール徹底のための責任者も明確化
Ⅳ2　情報開示・共有の促進		
情報開示の促進	情報開示の担当部署と担当理事の設置	平成28年1月に担当理事、平成28年4月に担当部署を設置
	モニタリングシステムの構築と監査機能の活用	平成28年度よりモニタリング開始
	情報開示ルールの見直し・規定化、「悪い知らせ」の報告を促すよう制度を見直し	平成28年度より新規程による運用開始
組織一体化のための情報共有の促進	本部内・本部と現場の情報共有、情報共有化のため地域マネージャー（仮称）の設置（責任ポストと位置づけ）	平成27年度より順次実施
	現場からの日次での業務報告の実施	平成28年度より実施
厚生労働省との情報共有の強化	厚生労働省との情報共有の強化	平成27年10月より実施済

（ 別 添 ）

業務改善計画　各事項の実施時期

事項		実施時期（年度） 27	28	29	30
Ⅳ3（1）情報セキュリティ対策（組織面） ～組織の一体性を確保～					
情報管理対策本部の設置		平成27年10月1日設置済			
情報管理対策室の設置		平成27年10月1日設置済			
機構CSIRTの設置		平成27年10月1日設置済			
最高情報セキュリティアドバイザーの設置			平成28年度設置予定		
Ⅳ3（2）情報セキュリティ対策（技術面） ～多重防御対策の実施～					
基幹システム	年金個人情報専用の共有フォルダ	平成27年度に設置、順次セキュリティ機能を強化			
	窓口装置（WM）の入口対策の強化	平成27年度より順次セキュリティ機能を強化			
機構LANシステム	窓口装置（WM）からの利用の限定	平成27年度より実施			
	運用管理の強化	平成27年度より実施			
インターネット環境		平成27年度より順次再開、平成29年度より本格実施			
Ⅳ3（3）情報セキュリティ対策（業務運営面） ～実効性のある対応～					
情報セキュリティポリシーの改正等		平成27年度より順次実施			
情報セキュリティ研修等実施		平成27年度より実施			
監査体制の整備			平成28年度より実施		