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。