検　証　報　告　書

平成 27 年 8 月 21 日

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

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

名　簿

委員長	甲斐中　辰夫	弁護士（卓照綜合法律事務所）、元最高裁判所判事、元東京高等検察庁検事長
委員	青嶋　信仁	株式会社ディアイティ　取締役　セキュリティサービス事業部長
	大谷　義雄	全国社会保険労務士会連合会副会長
	齋藤　洋平	フューチャーアーキテクト株式会社　テクノロジーイノベーショングループ　バイスプレジデント
	藤井　眞理子	東京大学先端科学技術研究センター教授
	増田　宏一	公認会計士、元日本公認会計士協会会長
事務局長	野村　修也	中央大学法科大学院教授、弁護士（森・濱田松本法律事務所）、厚生労働省顧問
参与	金子　桂輔	弁護士（黄櫨綜合法律事務所）
	齊藤　貴一	弁護士（卓照綜合法律事務所）
	佐々木　宏幸	株式会社ディアイティ　セキュリティサービス事業部、情報処理技術者試験委員、CISSP
	芝　昭彦	弁護士（芝経営法律事務所）
	鈴木　ひろみ	社会保険労務士（鈴木社会保険労務士事務所）
	永宮　直史	特定非営利活動法人日本セキュリティ監査協会事務局長、情報セキュリティ主席監査人
	西田　恵	株式会社 IHI　情報システム部　技師長
	福田　舞	弁護士（卓照綜合法律事務所）
	松崎　祥三	有限責任あずさ監査法人／KPMG　IT 監査部マネジャー
	松本　卓也	弁護士（阿部・井窪・片山法律事務所）
	山口　達也	有限責任あずさ監査法人／KPMG　IT 監査部パートナー
	山﨑　千春	有限責任あずさ監査法人／KPMG 金融事業部マネージングディレクター

（注）委員及び参与の表記は五十音順。

目　次

第１　検証の概要

１　本委員会設置の経緯

平成 27 年５月８日、厚生労働省（以下「厚労省」という。）及び日本年金機構（以下「機構」という。）は、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）から、機構のネットワークシステムと外部との間で不審な通信が行われている旨の情報を受領した。これを受け、機構は、当該ネットワークシステムに係る保守運用等の委託先会社（以下「運用委託会社」という。）と連携して、関係端末の LAN ケーブルの抜線、セキュリティソフトへの最新の定義ファイルの適用等の対応を行った。しかし、その後も、機構のネットワークシステムに対しては、外部からの不審なメールが波状的に送られるなど、標的型攻撃の兆候が継続してみられた。さらに、同月 28 日には、警視庁の捜査により、上記標的型攻撃によって流出したとみられるデータが機構外部のサーバで発見されるに至り、機構による調査の結果、上記データには、機構の保有する極めて多数の個人情報が含まれていることが判明した。

これらの事態を受け、厚生労働大臣は、厚労省及び機構から独立した第三者からなる検証委員会を早急に立ち上げ、これらの一連の事案についての原因究明と再発防止策を検討させることとし、同年６月４日、「日本年金機構不正アクセス事案検証委員会」（同年７月 17 日付で「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」と名称変更。以下「本委員会」という。）を設置する旨を決定した。

２　委嘱事項

厚生労働大臣は、平成 27 年６月８日、本委員会委員長に対し、機構に対する不正アクセス事案（以下「本事案」という。）により損なわれた厚労省及び機構に対する国民の信頼を回復できるよう、本事案に関し、機構及び厚労省の組織並びに初動及び事後の対応について検証し、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、報告を行うことを委嘱した。

３　本委員会による検証の目的

本委員会による検証の目的は、上記２の委嘱に基づき、本事案の発生に至るまでの機構及び厚労省の組織における問題点並びに本事案発生後の機構及び厚労省の初動及び事後の対応における問題点を検証し、それらを踏まえ、本事案

の原因を究明するとともに、再発防止策を提言することである。

本委員会は、あくまでも機構及び厚労省のいずれからも独立した中立公正な立場から、上記目的のために調査検証を実施するものであり、本事案に関する機構、厚労省その他の組織団体又はその役職員の民事上、刑事上その他の責任の有無を確定し、これを追及することを目的とするものではない。

4　検証方法の概要

本委員会は、上記３の目的を果たすため、平成27年６月８日以降、関係資料の検証分析、関係者のヒアリング等の調査を実施し、その上で、入手した情報について随時必要に応じて委員及び参与の合議により総合分析を行い、同年８月 19 日（以下「本報告基準日」という。）までに入手した情報に基づき、本検証報告書をとりまとめた。

具体的な検証方法の概要は、以下のとおりである。

（１）関係資料の検証分析

本委員会は、厚労省及び機構に対し、関係資料（関係諸内部規程、決裁文書類、関係諸会議体の議事録及び同会議体における資料、運用委託会社との間の関係契約書類、関係ネットワークシステムの構造、運用状況等に関する資料、フォレンジック調査報告書、厚労省及び機構の役職員間等で発受信された電子メール、連絡文書その他の資料等）の開示を要請し、厚労省及び機構から開示を受けたこれら関係資料の検証分析を行った。

また、本委員会は、運用委託会社及び機構のネットワークシステムに導入されたセキュリティソフトの提供会社（以下「セキュリティソフト会社」という。）からも、必要に応じて関係資料の開示を受け、その検証分析を行った。

（２）関係者のヒアリング

本委員会は、厚労省及び機構の役職員をはじめ、必要に応じて運用委託会社及びセキュリティソフト会社の関係者等に対しヒアリングを実施した。ヒアリングに際しては、上記３の本委員会の検証の目的にのみ利用することを説明し、その承諾を得た。本報告基準日までのヒアリング対象者は、合計延べ78名である。

5　本委員会による検証及びその結果の前提

本委員会は、強制的な調査検証の権限を有するものではなく、その調査検証

は厚労省及び機構の役職員その他の関係者の任意の協力を前提としている。また、本委員会と検証の性質上、限られた日時と人員により調査検証せざるを得ず、これらのことから、本委員会による検証及びその結果が一定の制約を免れ得るものではない。なお、本委員会による検証により明らかになった事実等には、公にすることによって攻撃者を利するおそれがあるものが含まれることから、これに該当すると本委員会が認めた事実等については、本報告書の記述から除外していることも付言する。

第２　本委員会が認定した事実

１　サイバー攻撃とその対応

（１）「サイバー攻撃」とは

「サイバー攻撃」とは、特定の組織のコンピュータシステムやネットワークに不正に侵入する等の方法で、情報・データの窃取・改ざん・破壊やシステムの機能阻害等の損害を与える行為である。

サイバー攻撃の主要な形態には、ウェブサイト等に大量の通信を送りつけ、サービス提供を妨害する攻撃（サービス停止攻撃）、様々な攻撃手法を組み合わせて情報・データの窃取・改ざん・破壊やシステムの機能阻害等をもたらす攻撃（標的型攻撃）等がある。本事案におけるサイバー攻撃は、後者の標的型攻撃であったと考えられる。

標的型攻撃は、2000年代初頭から存在していたが、2010年代に入ると世界的な拡大を示し、わが国においても近時その脅威は急速に高まっている。特に、（２）で詳述する標的型メール攻撃については、警察庁が把握した件数に限っても、平成26年下半期に1,507件と同年上半期（216件）から７倍以上に急増し[1]、政府機関を含む多数の組織・企業等において、情報の外部流出等の重大な結果を伴う事案が発生するに至っている。

（２）標的型攻撃の具体的手法

標的型攻撃とは、特定の攻撃対象に狙いを絞り、当該対象の業務内容等の内部情報を事前に入念に調査し、その結果に基づき当該対象に最適化した様々な攻撃手法を組み合わせて行われる、組織的・計画的なサイバー攻撃である。

標的型攻撃の代表的な手口は、攻撃対象となる組織の役職員に対し、マルウェアが含まれるファイルを添付したり、アクセスするとマルウェアがダウンロードされるよう仕組まれたサイトへのリンクを記載したりしたメール（標的型メール）を送りつけるものである[2]。

標的型メールには、攻撃者が事前調査により入手した非公開のメールアドレスや業務上実際に送受信されている電子メール等を活用し、一見しただけでは業務に関係する正規の電子メールと判別困難な巧妙な偽装が施されていることが多い。このような標的型メールの受信者が、偽装に気付くことなく添付ファ

---

[1] 警察庁「平成26年中のサイバー空間をめぐる脅威の情勢について」（平成27年３月12日付、https://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf）

[2] その他、USBメモリ等の媒体にマルウェアを仕込む、対象組織の役職員が業務上頻繁に用いるウェブサイトを事前に乗っ取り、そこにマルウェアを仕込んで待ち伏せする（水飲み場攻撃）等の手法が知られている。

イルを開封したり、記載されたリンクをクリックしたりすることで、当該受信者の利用している端末にマルウェアが感染する。なお、標的型攻撃に用いられるマルウェアは、既存の定義ファイルでは検知できない未知のものであることが多い。

端末に感染したマルウェアは、その後、バックドアの開設、他のマルウェアのダウンロード、端末への認証情報やネットワーク環境に関する情報収集等、その後の攻撃の基盤構築活動を展開する。その上で、攻撃者は、他の端末やサーバの認証情報を窃取してそれらに攻撃範囲を拡大させる等して、システム内の情報の広汎な窃取、システムの機能阻害といった自らの攻撃目的の完遂を目指す。さらに、攻撃者は、攻撃終了後、開設したバックドアを利用する等して継続的に再侵入・再攻撃を試みることもある。

このように、標的型攻撃は、攻撃手法が攻撃対象ごとに巧妙に最適化されている上、未知の攻撃手法も用いられることが通常であるため、攻撃対象の側で、標的型攻撃によるマルウェアの感染を完全に検知・防御することは困難である。攻撃者は、攻撃目的の完遂まで秘密裡かつ執拗に攻撃を継続する可能性が高い。そのため、標的型攻撃は、攻撃の成功可能性・攻撃に成功された場合に生じる影響のいずれも高度であり、それゆえ、単純なマルウェアの感染や不正アクセス等従来型のサイバー攻撃とは質的に異なる対応策が求められる。

（3）標的型攻撃への対応策

標的型攻撃への対応策については、既にNISCや独立行政法人情報処理推進機構（以下「IPA」という。）等によりガイドライン等が公開されている[3]。それらにおいて要求されている対応策は、以下のとおり、大きく「システム設計」「運用管理」「インシデント対応」に分類できる。

ア　システム設計

情報システムは、運用開始後に大幅な設計変更を行うことが困難である。そこで、構築以前の企画・設計の段階から、業務内容やシステム環境の特性等を踏まえたリスク評価を行い、その結果に応じた適切なシステム設計を行うことが重要である。例えば、大量の個人情報を取り扱う業務等、標的型攻撃によるリスクが大きい業務に用いるシステムは、他のシステムとは分離した設計とし、他のシステムにおけるリスクが顕在化した際にその影響が当該システムに波及

[3] NISC「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日付、http://www.nisc.go.jp/active/general/pdf/riskguide.pdf）、IPA「『高度標的型攻撃』対策に向けたシステム設計ガイド」（平成26年9月30日付、https://www.ipa.go.jp/files/000046236.pdf）

することを未然に防ぐ必要がある。

イ　運用管理

運用管理に関する人的対策としては、まず、システム利用者全体を対象として、標的型攻撃その他のサイバー攻撃の手口、対策等に関する最新の情報に基づくセキュリティ教育及び実践的訓練を継続的に行い、組織全体のマルウェアへの感染リスクの低減と異常発生時の対処能力の向上を図ることが重要である。

これに加えて、特に管理職に対しては、システムに異常な事態が生じた際に、その情報が組織内で迅速に共有されるよう、日頃からのコミュニケーションの円滑化の重要性について意識付けを行う必要がある。さらに、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。）への対応に当たる部署には、上記のサイバー攻撃に関する最新の情報の取得に常に努め、これを適時的確に組織内に周知することができる専門家を配置することが必要である。

また、技術的対策としては、前述のとおり、標的型攻撃によるマルウェアの感染を攻撃対象の側で完全に検知・防御することは困難であることから、①従来型のサイバー攻撃への対策として実施されていた、脆弱性管理やセキュリティソフトへの最新の定義ファイルの導入等のマルウェア感染防止のための対策（入口対策）のみならず、②システムへの侵入に成功された場合の被害範囲の最小化を図るための対策（内部対策）や、③情報の外部流出を阻止するための対策（出口対策）を組み合わせて行う「多層防御」が推奨されている。

具体的には、不正アクセスされ、内部へ侵入された場合に備え、ディレクトリサーバの保護、重要情報の暗号化、外部との通信の監視、不要な通信の遮断や通信ログの保全等が必要である。

ウ　インシデント対応

不審メールの受信、外部との不審な通信が検知される等して、標的型攻撃等のインシデントが発生した可能性を把握した際には、そうした不審事象の検知直後の迅速な初動が被害の軽減に欠かせない。そこで、初動の組織横断的な対応を一元的かつ迅速に行うため、CSIRT（Computer Security Incident Response Team）を中心とする緊急対応体制をあらかじめ整備し、継続的な訓練等により対応能力の向上に努める必要がある。

インシデントが発生した場合、その対応には、ネットワークの遮断や業務の一時中断といった組織運営上重要な判断を要するものも含まれる。このため、CSIRTには、こうした高度な判断を伴う対応を行うための十分な権限を付与するとともに、そのような役割と権限の大きさに見合う人的組織体制を整えておくことが必要である。

標的型攻撃におけるマルウェアは、そのプログラム自体や行動履歴を隠蔽したり、コンピュータ内のログを改ざんする等の機能を有しているため、特定が非常に困難である。このため、インシデントの態様によっては、速やかにフォレンジック調査によってシステムに残された攻撃者の痕跡や保全された通信ログの解析等を行うことが必要となる。

2　日本年金機構のネットワークシステムと本件標的型攻撃の概要

（1）機構のネットワークシステムの概要

機構が運用を行っているネットワークシステムは、大きく分けて、基礎年金番号の管理、保険料の計算、年金の支払等、政府管掌年金事業（国民年金事業・厚生年金保険事業）の根幹にかかわる業務に関するサービスを提供する「社会保険オンラインシステム」（「基幹系システム」とも呼ばれる。）と、それ以外のサービスを提供するシステム（「情報系システム」とも呼ばれる。）がある。社会保険オンラインシステムは、政府管掌年金事業を所掌する厚労省が所有し、機構にその運用を委託している。これに対し、情報系システムは、機構が自ら所有し、運用を行っている。

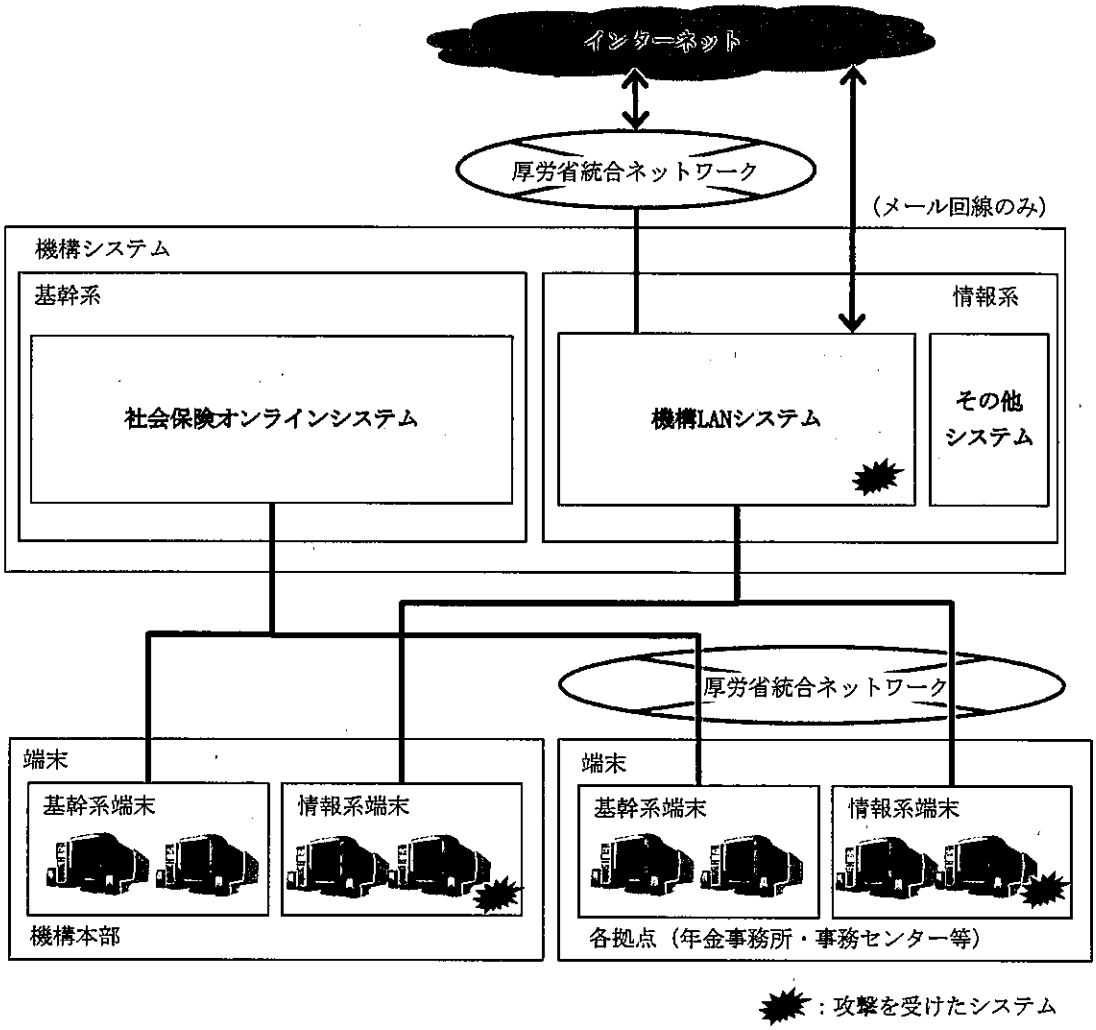
後者の情報系システムの中心をなしているのが、機構の役職員の日常業務で用いるイントラネットである「機構 LAN システム」である。同システムは、インターネット接続や電子メールのほか、ファイルサーバによるファイル共有サービスも提供している。機構においては、このファイル共有のための領域は「共有フォルダ」と呼ばれ、ファイルを共有するユーザーの範囲によって複数の階層に分かれている。

情報系システムは、厚労省統合ネットワークを経由してインターネットに接続されている[4]。基幹系システム・情報系システムのサーバ等と遠隔地の拠点に設置された端末との間も、厚労省統合ネットワークを経由して相互接続されている。基幹系システムと情報系システムは、ネットワーク上で物理的に接続されているものの、ネットワーク機器等によって論理的に分離された状態にある。また、基幹系システムと情報系システムは、それぞれ別個の端末を有し、機構の役職員は、機構本部及び年金事務所・事務センター等の各拠点に設置された両端末を使い分けて各自の業務を遂行している。

以上のシステム相互の関係等を簡略に示したものが次の図である。

---

[4] ただし、情報系システムのうちメールシステムは、厚労省統合ネットワークを経由せずに別の回線を通じて直接インターネットに接続している。



図：日本年金機構のシステム構成イメージ

（２）本件標的型攻撃の概要

本事案において行われた標的型攻撃においては、機構 LAN システムが攻撃を受け、その結果、共有フォルダに保存されていた大量の個人情報等が外部に流出するという重大な被害が生じた。

本件標的型攻撃の時系列的な詳細については後記６で詳述するが、その概要は以下のとおりであった。

ア　第一段階

平成 27 年５月８日午前、機構の２つの公開メールアドレスに対し、同一の送信元アドレスから標的型メールが送信された。受信した機構職員のうち１名がこれを開封し、メール本文に記載されたリンクをクリックしたことを契機に、

当該職員の使用端末がマルウェアに感染し、外部との不審な通信が開始された。

機構のシステム部門は、この不審な通信を検知したNISCの指摘により当該通信を認知し、ただちに発信元端末を特定し、同日午後、当該端末からLANケーブルを抜線した。抜線により不審な通信は停止したが、当該端末では、それまでの約４時間にわたり不審な通信が継続した。

イ　第二段階

５月18日午前から19日午後にかけて、波状的に機構職員計121名の個人メールアドレスに対して標的型メールが送信された。これら標的型メールを受信した機構職員のうち３名がメールを開封し、添付ファイルを開いたことで、当該職員の使用端末がマルウェアに感染した。

このマルウェアも、外部との不審な通信を試みたが、通信先C&Cサーバへの通信が５月８日の時点で厚労省統合ネットワークにおいてブロックされていたため通信は成功せず、それ以上の被害は生じなかったものとみられる。

ウ　第三段階

５月20日、機構の５つの公開メールアドレスに対し、新たな送信元アドレスから標的型メールが送信された。これら標的型メールを受信した機構職員のうち１名がメールを開封し、添付ファイルを開いたことで、当該職員の使用端末がマルウェアに感染した。

このマルウェアは、C&Cサーバとの通信の確立に成功し、さらに他の26端末にも感染を拡大させた。こうした攻撃の過程で、感染端末やディレクトリサーバの管理者権限が窃取された。そして、これらの攻撃の結果得られた情報を利用する等して、共有フォルダに保管されていた大量の受給者等の個人情報等が窃取され、外部に流出した。

一連の攻撃による外部流出が確認されている被保険者・受給者の個人情報は、約125万件に及ぶ。

３　日本年金機構における情報システムの設計と運用

（１）機構LANシステムと基幹系システムの分離の不徹底

上記２で示した通り、機構のネットワークシステムは、大きく社会保険オンラインシステムと機構LANシステム等の情報系システムの二つのシステムから構成されている。このうち、年金に関する個人情報は基幹系システムにおいて処理を行うこととなっており、機構LANシステムではこうした個人情報に関する処理を行うことはないというのがシステム構成の前提となっていた。すなわ

ち、取り扱う情報の種類によって利用するシステムの分離が図られていた。

しかしながら、機構においては、業務の必要を理由に、事務処理を行う機構LAN システムへの個人情報の移管・保管が一定のルールの下で認められ、機構LANシステム上の共有フォルダに個人情報が置かれるという、上記のシステム構成の前提に反する運用が行われていた。共有フォルダへの個人情報の保存に際しては、アクセス権の設定、または、パスワードの付与というルールが規定されていたが、インターネットからの標的型攻撃を想定した場合、こうした運用は適切なものとはいえない。

（2）標的型攻撃を想定したシステム設計及び運用の不十分性

機構においては、基幹系システムの刷新計画が優先され、機構 LAN システムに内在し標的型攻撃を引き起こす可能性のある種々の脆弱性には注意が払われておらず、機構 LAN システムにおいては、標的型攻撃を想定したシステムの設計や運用はなされていなかった。

一例をあげれば、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）が常時行われていたわけではなく、標的型攻撃によるインシデントに対応できる内容とはなっていなかった。このため、攻撃の各段階において状況把握のために相当の時間を要する結果となった。

事案発生時である平成27年5月時点までに、標的型攻撃に関するシステム対策についてのガイドラインがIPAやNISC等から公開されている。標的型攻撃の脅威を認識した上で、これらのガイドラインを参考にシステムの設計、運用を行っている組織は国、民間を問わず存在している。このうち、昨年6月に定められたNISCのガイドラインは、国の行政機関を適用範囲としていたが、取り扱う情報の重要性に鑑みれば、機構においても参考とすべきものであったと考えられる。

4　日本年金機構における情報セキュリティの問題

（1）日本年金機構の情報セキュリティ体制の脆弱性

ア　機構における情報セキュリティ体制

機構は、その情報セキュリティポリシーにおいて、副理事長が最高情報セキュリティ責任者（CISO）として情報セキュリティ対策に関する事務を統括し、システム部門担当理事（CIO）が統括情報セキュリティ責任者として各部署の情報セキュリティ責任者（原則として各部署の長がその職に充てられる。）を統括し、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者が情報セキュ

リティアドバイザーとして情報セキュリティ対策全般に対して助言等を行う等の情報セキュリティ体制を定めている。

また、インシデントへの対応ルールについては、機構の情報セキュリティポリシーにおいて、標的型攻撃発生時には、各部署の情報セキュリティ責任者が情報システムについて不正プログラムの侵入及び感染拡大等を防止するための措置を講ずるものと定められている。その他、システム障害発生時の報告手順を定める対応手順書も作成されている。

しかしながら、上記内部体制及び対応ルールは、次に詳述するように、いずれも不十分なものであったといわざるを得ない。

イ　インシデント対応体制の未整備

第一に、サイバー攻撃等のインシデント発生時の緊急時対応については、機構に CSIRT の制度が設けられていなかったほか、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。このため組織的対応ができず、個々の具体的対処が明示されたマニュアルも存在していなかったため、インシデントの発生に直面し、厚労省への報告・連絡・相談は、場当たり的なものにならざるを得なかった。

第二に、リスクに備えた人員配置が行われていなかった。上記情報セキュリティアドバイザーには、統括情報セキュリティ責任者が所属する部署内の、情報セキュリティスペシャリスト等の資格を有する職員１名が任命されていたが、この職員は役員や管理職などの判断権者に対して率直に進言できるような職位にはなかった。加えて、同人は、本件当時情報セキュリティアドバイザーとしての職務から事実上外れていた上、本事案発生後も直ちに情報セキュリティアドバイザーとしての業務に戻るよう指示等されることはなかった。上記情報セキュリティアドバイザーに任命された職員を含め、サイバー攻撃等のインシデントに自ら対応した経験を有する職員もいなかった。

こうした状況にもかかわらず、情報セキュリティの専門的知見を有する人材を外部から意識的に補うことも行われなかった。

第三に、運用委託会社と機構との間の契約では、情報セキュリティの確保について抽象的な仕様が規定されているのみで、サイバー攻撃等のインシデント発生時における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はなされていなかった。

第四に、機構の一般の職員に対しては、情報セキュリティに関する基本的な研修は実施されていたが、研修資料には、標的型メールを含め、サイバー攻撃への言及がなく、標的型攻撃を含むサイバー攻撃に関する訓練も行われていなかった。機構内での注意喚起においても、添付ファイル等を開かないよう指示

しているだけで、不審メールを受信した場合の具体的な対応方法が記載されていないなど、職員への注意喚起の面で十分だったとは言い難い。

（2）個人情報保護に関する認識の不足

機構における個人情報は、原則として基幹系システムに保管されているが、一定の条件の下で機構 LAN に接続する共有フォルダに保管されていた。

こうした個人情報等の機密データを、機構 LAN システムの共有フォルダに保管することに関するルールは、経営企画部総務室により、最終的に平成 27 年 3 月 23 日付の「日本年金機構共有フォルダ運用要領」にまとめられた。

当該運用要領によれば、共有フォルダのアクセス権を関係者のみに制限するか、ファイルにパスワードを設定すれば、共有フォルダ内で取り扱うことができることとされ、保管する必要がなくなったものは、速やかに削除することとされた。

個人情報のような重要情報を、暗号化等も行わず単にアクセス制限またはパスワードをかければ足りるとする本運用は、そもそも極めてリスクの高い運用であったが、そうしたルールですら厳守が徹底されず、アクセス制限もパスワード設定もなされていないまま共有フォルダに保管されているファイルが存在し、また、必要がなくなった個人情報がそのまま残置されているケースが認められた。しかも、これらのルールの遵守状況を実効的に確認できる仕組みは設けられておらず、一元的な管理がなされていない膨大な個人情報が共有フォルダに積み上げられていた。

（3）システム監査等の機能不全

ア　不十分な自己点検

機構では、情報セキュリティや個人情報保護に関する自己点検が毎月実施されていた。この自己点検の内容は、主に事務ミスや内部不正を想定したものであった上、その方法も職員が自ら回答し、課題がある場合でも回答者本人のみが改善施策を記入することになっているなど、回答結果について組織としての対応を検討するといった観点からの実効性ある自己点検とはなっていなかった。

イ　情報セキュリティ監査の不存在

システム監査のうち機構の情報セキュリティ態勢に対する監査は、平成 24 年度までは年金局事業企画課監査室が行っていたが、平成 25 年度以降は機構における内部監査として行われることとなった。しかしながら、平成 25 年度以降においても機構の内部監査においては、外部からの攻撃を想定した情報セキュリティ対策は監査対象とされていなかった。

監査部が実施しているリスク・アセスメント手順をみても、インターネット接続状況等の標的型攻撃を想定した評価項目がなく、リスク・アセスメントにおいて標的型攻撃を想定した取り組みとなっていなかった。

（4）現場に対するガバナンスの不十分性

機構においては、年間数千件に及ぶ指示依頼が全国の拠点に向けて発出されており、現場における指示依頼の理解及びその徹底については相当な負荷がかかっている状況にある。これは、制度の度重なる改正や関連する移行措置等の複雑な規則に対応するためのものもあり、ある程度やむを得ない事情もあると推察されるが、過去の指示依頼と重畳的な指示依頼が発出されるケースもみられた。

また、ルールは本部が策定するが、その遵守状況の管理は執行部門に任せる形式が一般的であり、ルールの遵守状況や、遵守できない理由について本部が把握できる枠組となっていない。このことは、共有フォルダの把握に関する問題と併せて、機構の現場に対する管理が不十分であったことを表している。

5　日本年金機構の情報セキュリティに対する厚生労働省の監督体制

（1）機構 LAN システムに対する監督体制の欠落

機構は、厚生労働大臣の監督の下に、政府が管掌する厚生年金保険事業及び国民年金事業に関する業務を行うこととされている。機構 LAN システムは、年金局がこれを監督するが、厚労省全体の情報セキュリティ対策は政策統括官付情報政策担当参事官室（以下「情参室」という。）が担当している。しかしながら、実態をみると、いずれの課室も自らが責任部局であるとの認識が希薄であり、積極的な指導監督の姿勢は認められなかった。

結果として機構 LAN システムの情報セキュリティ態勢に対する厚労省の監督体制は有効に機能していたとはいえず、本事案発生の前後いずれにおいても適切な監督が行われなかった。

ア　年金局による機構の監督

厚労省において、厚生年金保険、国民年金等の公的年金に関する担当部局は年金局であり、年金局内では、事業企画課と事業管理課が機構に対する監督を所掌している。

（ア）事業企画課の役割

年金局事業企画課は、機構の組織及び運営一般に関する事務を所掌し、機構のコンプライアンスや品質管理等に対する一般的な監督を行うこととされてい

る。したがって、情報セキュリティ一般に関する監督も同課の所掌となる。

しかしながら、事業企画課が過去に行った機構に対する監督の具体例として、機構の業務実績評価をみると、個人情報保護に関する問題では主に通知書の誤送付等に起因する情報漏えいの発生事例が取り上げられており、本件事象のような外部からのサイバー攻撃に対する防御策等の情報セキュリティ体制は評価の対象とされていなかったなど、機構 LAN システムの情報セキュリティ体制に関する監督を行うべき担当部署としての認識は不十分であった。

そもそも、事業企画課には情報セキュリティ分野に精通した専門職員が全く配置されていなかったほか、機構を監督する同課担当者らにおいても情報セキュリティに関する知見や経験が不足していた。

（イ）事業管理課の役割

年金局事業管理課は、厚生年金保険や国民年金の徴収等に関する事務を所掌し、同課内のシステム室が機構の運用するシステムのうち社会保険オンラインシステムについて監督を行うこととされている。システム室においては、IT システムに関する相当程度の専門性を有する職員らが配置され、機構内部に同室職員の一部が常駐して日常的にシステムの監視や機構職員らとの意見交換等が行われていた。

しかしながら、システム室の監督の対象は、機構が運用するシステムのうち、国が保有する社会保険オンラインシステムのみとされ、本事案が発生した機構 LAN システムは監督の対象外とされていた。

イ　情報セキュリティ担当部署の役割

厚労省には、情報セキュリティ対策の担当部署として情参室が置かれている。情参室は厚労省の情報政策に関することを所掌するものとされ、そのうち情報セキュリティ業務を所掌する部門として情参室内に情報セキュリティ対策係が配置されている。

しかしながら、情参室は、後述のような体制面の問題を抱えていた上、機構に関しては、前述のとおり、年金局が監督するものと整理されていたので、直接に機構の情報セキュリティ体制を監督する状況になかった。情参室が年金局を通じて機構に提供していた情報も、サイバー攻撃の脅威やその被害の増大、サイバー攻撃に対する備えの重要性について注意喚起するには不十分なものであった。

以上に加え、機構 LAN システムと厚労省統合ネットワークシステムの連携の不十分さ、責任分界の不明確さという問題も認められる。厚労省は、機構 LAN システムと厚労省統合ネットワークシステムとのネットワーク接続に際し、機構 LAN システム側においてどのようなネットワーク監視を行うべきであるかに

ついての具体的な指示を行っていなかった。

（2）厚労省における情報セキュリティ体制の脆弱性

ア　サイバーセキュリティ体制の不備

厚労省の情報セキュリティ対策の担当部署である情参室情報セキュリティ対策係の所掌業務は、本件のような情報セキュリティインシデントへの対処のほか、職員への情報セキュリティ教育プログラムの策定・実施、NISC との調整、民間事業者（医療・水道）に対する情報セキュリティ分野の支援業務、マイナンバー制度の施行に関する事務等多岐にわたる。

しかし、その人員体制は、室長補佐以下、わずか４名に過ぎず、一般的な人事ローテーションの中で任用されていたため、高度な専門性に基づく対応が要請される情報セキュリティインシデントに対処できる知識や経験を十分に備えていた専門家とは認め難い。しかも１名の職員が、他の業務と兼務しながら、省全体のサイバーセキュリティ対策業務を中心的に担っていたというのが同対策係の実態であった。

厚労省は、年金行政のほか医療行政や労働行政等を所管し、３万人を超える職員が所属する巨大組織である。多くの機密情報や個人情報を保有していることや、近年、官公庁等を狙った悪質なサイバー攻撃が増加し、その内容も日増しに高度化してきていることに鑑みれば、実質的に１名の職員が他の業務と兼務しつつ厚労省全体のサイバーセキュリティ対策を担当していたという状況は、省全体のサイバーセキュリティ体制としては明らかに不備があったと評価せざるを得ない。

上記のような体制の不備は、厚労省全体（特に幹部層）におけるサイバー攻撃の脅威や厚労省管理下にある情報資産の価値及びその漏えいリスクの重大性等についての意識が低かったことに起因すると考えられる。

イ　情報セキュリティアドバイザーとの連携不足

厚労省には、本件事象発生当時、専門的・技術的見地から支援を行う専門家として内閣官房から割り当てられた CIO 補佐官が５名配置され、うち１名が厚労省の最高情報セキュリティアドバイザー及びインシデントアドバイザーとして任命されていた。

しかしながら、それぞれの CIO 補佐官はいずれも非常勤であり、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についても助言しているという状況であった。情参室の職員ほか厚労省の職員が情報セキュリティに関して CIO 補佐官と緊密な連携がとりやすい環境とは言い難い面があり、平素の準備及びインシデント対応における職員と CIO 補佐官との連携は必ずしも円

滑かつ十分に機能していたとは認めがたい。

ウ　情報連絡の遅延

厚労省及びその外局並びに傘下の独立行政法人においては、過去３年間に限ってみても、ホームページの改ざん等のサイバー攻撃が複数回発生している。こうした事案については、厚労省内部及び外局並びに傘下の独立行政法人から厚労省情参室に報告がなされることとなっている。

しかしながら、そうした報告の多くは事案収束後に行われていたなど、情報連絡が遅延しており、情参室や CIO 補佐官がインシデント対応等に適時に適切な役割を果たすことができる連絡体制とはなっていなかった。

本事案の対応においても、情報セキュリティポリシーに規定されている責任者らへの報告は、最初の攻撃発生後２週間以上が経過してからであったなど、情報連絡の遅延がみられた。

エ　実効性に乏しい CSIRT 体制

厚労省においては、CSIRT 体制も定められていたが、その構成員は課室長以上となっており、情報セキュリティインシデントに対応できるだけの技術力を持った実働要員が充てられていたわけではなかった。また、厚労省と関連組織（独法、特殊法人含め）全体の CSIRT 連携はなされていなかった。

６　本件標的型攻撃とこれに対する対応

（１）本件標的型攻撃に先立つ平成 27 年４月 22 日の攻撃

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。

次項以下では、平成 27 年５月８日以降、機構に対して行われた本件サイバー攻撃とこれに対する関係者の対応を三段階に大別して説明する。

①第一段階　…　平成 27 年５月８日の攻撃とこれに対する対応
②第二段階　…　平成 27 年５月 18 日及び 19 日の攻撃とこれに対する対応
③第三段階　…　平成 27 年５月 20 日の攻撃とこれに対する対応

（２）第一段階

ア　攻撃の態様

平成 27 年５月８日の攻撃は、機構の２つの公開メールアドレス宛に標的型メール２通が送信されることにより開始した。当該メールは、その送信元アドレスがフリーメールアドレスであり、また、本文中に外部のオンラインストレージサービスへの URL のリンクが記載されているものであったことから、標的型攻撃を疑わせるものであったものの、一方で、メール本文中に宛名として記載された姓が受信者の部署に所属する職員の姓と同一であるなど、業務上のメールであると誤認させる要素もみられた。

そして、メールを受信した職員の一人がメールを開封し、メール本文に記載されていた外部のオンラインストレージサービスへの URL をクリックしたところ、当該端末において不正プログラムがダウンロードされ、そのファイルが実行された結果、複数の C&C サーバとの不正な通信が発生した。

この不正な通信は、当該端末から LAN ケーブルを抜線し、LAN から遮断するまでの約４時間、継続した。アクセスログによれば、その間に極めて大量の Web アクセスが行われていた。また、各アクセスは、４月 22 日に発生した不正な通信と同様、GET メソッドの命令文に不明な文字列が付加されているなどの特徴を有していた。

イ　発覚の経緯

５月８日、NISC は、厚労省統合ネットワークを通じて発信されている不審な通信を検知した。NISC から、厚労省の情報セキュリティの窓口である情参室に通報され、情参室は厚労省統合ネットワークの運用保守を担当している統計情報部に不審な通信の発信元の特定を依頼したところ、通信元が機構 LAN システムであることが判明した。

そこで、情参室から機構を所管する年金局の窓口である年金局書記室を経由して年金局事業企画課庶務係に NISC の通報内容が伝達され、年金局事業企画課庶務係から機構の窓口となる部署を経由して、機構の機構 LAN システム担当部署に伝達された。機構の機構 LAN システム担当部署が NISC による通報内容を受領したのは、NISC から情参室に対して通報が行われてから、およそ２時間半後であった。

ウ　機構の対応

（ア）初動対応

機構は、NISC からの通報を受けて、不審な通信の発信元である端末の特定に着手すると共に、機構 LAN の運用を委託している運用委託会社に連絡を取り、対応を要請した。そして、不審な通信の発信元端末を特定した後、直ちに、当該端末の LAN ケーブルを抜線した。

運用委託会社は発信元の端末を回収し、セキュリティソフト会社に解析を依頼するとともに、NISC から通知された情報に基づき、不審な通信先とされる URL について、機構 LAN における URL ブロックを実施した。

なお、翌９日未明に、運用委託会社から機構に対して、アクセスログを解析した結果、情報漏えいの可能性はきわめて低いと考えている旨の報告がなされた。

（イ）マルウェアの解析

機構は以下のとおり、運用委託会社を通じて、セキュリティソフト会社に対し、感染端末から抽出された検体の解析を依頼し、その結果を受領した。

①機構は、５月８日に感染端末から抽出した検体についてその解析を依頼したところ、翌９日に、運用委託会社を通じて、当該検体から新種ウィルス（マルウェア）が検出されたとの結果を受領した。

５月 12 日には、当該新種ウィルスは「トロイの木馬」タイプで、特定のサイトにファイルを取得しにいくものであること、したがって、感染端末から情報を発信することはないとの報告を運用委託会社から受領した。また、５月 15 日にも、運用委託会社より、あらためて、当該新種ウィルスの挙動は従前の報告のとおりである旨の報告がなされた。

このウィルスについては、５月 11 日にセキュリティソフト会社から当該ウィ

ルスを検知するための定義ファイルが提供され、この定義ファイルが翌12日以降配布された。

②5月13日には、8日に感染した端末のゴミ箱にあった不審ファイル（外部のオンラインストレージサービスからダウンロードされたファイル）の解析をセキュリティソフト会社に依頼した。この検体については、セキュリティソフト会社から運用委託会社に対して5月18日に、新種ウィルスが検出されたとの解析結果が報告され、6月2日に定義ファイルが配布された。

（ウ）アクセスログの監視

機構と運用委託会社は、他の端末への感染拡大の有無を確認するため、両者協議の結果、運用委託会社において、NISCから通報のあったURLへのアクセスログの監視を5月8日から13日まで行うこととし、かかる監視が実施されたが、当該期間において、監視対象URLに対するアクセスは検知されなかった。

（エ）職員に対する注意喚起

機構は、5月8日、全職員に対して、外部から機構宛に不審なメールが相次いでいること、送り主の名前に身に覚えのない不審なメールが届いた場合は添付文書やURLなどを開封せず削除するよう注意すること等を記載した注意喚起文書を発した。ただし、この時点での全職員宛の注意喚起では、同日受信した実際の標的型メールの送信元アドレスや件名などを引用した具体的な例示はなされておらず、標的型メールに対する一般的な注意喚起にとどまった。

エ　機構において取るべきであった対応

機構は感染の拡大に対する懸念を有していたものの、その対応としては、特定のURLに対する通信の監視のみにとどまった。

しかしながら、この対応では、当該URLに対する外部への通信が発生しない限り、機構LAN内部において端末の感染が拡大していても直ちに認知することはできず、不十分な対応と言わざるを得ない。

また、不審な通信が約4時間にもわたって継続していたことやそうした不審な通信は不明な文字列が付加された大量の通信であったことを考慮すれば、GETメソッドのHTTP通信であっても、様々な不正プログラムが当該端末に取り込まれている可能性や、当該不明な文字列によって情報が外部に送信されていた可能性をも想定し、ただちに感染した端末のフォレンジック調査及びディレクトリサーバなどの主要サーバの調査に着手すべきであったと考えられる。

仮に、この段階で感染端末のフォレンジック調査を行っていれば、当該端末に残された攻撃者の痕跡などが、より早い段階で確認できたと考えられ、したがって、第二段階以降の機構の対応が異なるものとなっていた可能性がある。

なお、機構の担当者の中には、標的型攻撃の可能性があると認識し、8日の

攻撃に引き続き、さらなる攻撃が行われる可能性もあるとして危機感をもって情報発信を行った者もいたが、こうした危機意識が組織的には共有されるような展開にはならず、適切な対応には至らなかった。

また、機構は、５月８日に受信した標的型メールの送信元アドレスの受信拒否設定を行わなかったため、後述するとおり、18 日に同一のメールアドレスから大量の標的型メールが送信されるに至った。

オ　厚労省の対応

（ア）厚労省内における情報伝達

厚労省においては、先に述べたとおり、NISC からの通報を情参室の情報セキュリティ対策係が受領し、統計情報部からの回答を受けて、年金局を通じて機構の機構 LAN システム担当部署に連絡された。NISC による通報が機構の担当部署に到達するまでの間におよそ２時間半が経過している。

情参室においては、５月８日時点において、係内での情報共有はなされていたものの、上長である参事官へは報告が上がらなかった。これは、機構において LAN ケーブルの抜線がなされ、不審な通信が遮断されたとの一応の状況が確認されたこと、また、それ以上の状況については機構において調査中であったことから、調査結果を待った上で報告を上げるべきものと認識したことによる。年金局事業企画課庶務係においても、情参室と同様の認識により、係長から上長への報告はなされなかった。

（イ）機構に対する指導

厚労省は、機構に対し、感染端末の特定と抜線及びNISC に提供するために本件不審メールに係る検体の提出を求めたが、それ以上の具体的な対応を指示することはなかった。

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は、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的型攻撃の一環であるとの着想に至らなかった。

ただし、厚労省統合ネットワークの運用管理者側では、４月 22 日に発生した不審な通信の通信先のドメインと５月８日に発生した不審な通信の通信先のドメインが同一であったことから、５月８日、同ネットワークにおいてドメイン単位での URL ブロックを実施した。

（3）第二段階

ア　攻撃の態様

次に行われた攻撃は、５月 18 日午前、機構職員の 101 の個人メールアドレス宛に、計 101 通の標的型メールが送信されるというものであった。このときのメールの送信元アドレスは、５月８日の標的型メールの送信元アドレスと同一であった。

これに対し、機構において、当該メールアドレスについての受信拒否設定を行ったところ、同日午後には、異なる送信元アドレスから 17 通の標的型メールが届いた。

翌 19 日午前にも前日午後の送信元アドレスと同じアドレスから、機構の２人の職員の個人メールアドレス宛に、それぞれ１通ずつ計２通の標的型攻撃メールが送信された。機構は、当該メールアドレスについて受信拒否設定を行ったものの、同日午後には、さらに異なる送信元アドレスから職員の個人メールアドレス宛に１通の標的型メールが送信された。

以上の一連の攻撃の中で、５月 18 日の段階で、端末３台が感染し、不正な通信が発生した。これらの感染端末が通信を試みた C&C サーバについては、５月８日に厚労省統合ネットワークにおいて URL ブロックが実施されていたため、結果としてアクセスは成功しなかった。

なお、フォレンジック調査の結果によれば、第一段階の攻撃において、職員のメールアドレスが外部に漏えいされ、漏えいしたメールアドレスが第二段階の攻撃に用いられた可能性が高いことが判明した。

イ　発覚の経緯

機構は、５月 18 日午前に全国の複数の職員から不審メール受信の報告を受けたため、運用委託会社に対し、当該不審メールの送信元アドレスから機構職員宛に送信されたメールの件数を確認したところ、既に 100 件ものメールが送られてきていたことが判明し、標的型攻撃を受けていることを認識した。

ウ　機構の対応

（ア）メールの受信拒否設定と全職員への注意喚起

機構は、不審メールの受信について職員から情報提供を受ける都度、運用委託会社に依頼して、当該不審メールの送信元アドレスからの受信状況を確認するとともに、その受信拒否設定を行った。

また、今回は、不審メールの内容を具体的に摘示した上で、全職員に対する注意喚起を行った。

しかしながら、機構は、不審メールの受信者リスト一覧を運用委託会社から

受領しながらも、メールを受信した職員に対し、個別に添付ファイル開封の有無を確認しなかった。その後の職員による開封を防止し、また、開封の有無が端末の感染の有無を知る端緒ともなるのであるから早期に確認すべきであった。

この対応の結果、機構は18日の時点で3台の端末が感染していたことについて、6月1日まで気が付くことがなかった。この3台の感染端末が不正通信を試みた先のURLについては、先に述べたとおり、厚労省統合ネットワーク側でURLブロックを行っていたため、同時点では外部への情報流出につながらなかったものの、極めて危険な状態であったと言わざるを得ない。

（イ）マルウェアの解析

機構は18日に検体を収集することのできた2通の不審メールについては、運用委託会社を通じてセキュリティソフト会社へ解析を依頼するとともに、19日には厚労省情参室を通じてNISCへも検体を提出した。

19日及び22日には、セキュリティソフト会社から運用委託会社に対し、新種のウィルスが検出されたとの上記検体の解析結果が報告され、それぞれ、22日及び26日に定義ファイルが配布された。

（ウ）捜査依頼

大量の不審メールを受信したことから、機構は、標的型攻撃を受けていると認識し、19日に高井戸警察署に赴き、捜査依頼を行った。

エ　機構において取るべきであった対応

18日に全国各地の機構職員に送信されてきた不審メールはその数100通余りであり、8日のものとは異なり、ホームページ等で一般に外部に公開されていない個別の職員メールアドレス宛であり、かつ、メール本文には、それぞれのメールアドレスに対応した機構職員の姓名が漢字で具体的に記載されているという異常な状況であった。

また、機構において、着信したメールの送信元アドレスを受信拒否設定にする都度、異なるメールアドレスから不審メールが送信されてくるという執拗な攻撃がなされていた。

こうした状況に鑑みれば、機構においては、5月8日から機構を狙った攻撃者が、その手をゆるめず、本格的に大規模な攻撃を仕掛けてきていると、その事態を正しく認識し、また、攻撃者が攻撃目的を達するまで、引き続き執拗な攻撃を仕掛けてくる可能性があるとの危機意識を持つべきであった。

また、このような状況においては、さらなる攻撃による感染拡大を防ぐため、機構において、遅くとも19日の段階でインターネットの全面遮断に踏み切るべきであったと考えられる。

オ　厚労省の対応

厚労省情参室は、19日に機構から18日及び19日の事象について報告を受けた。しかし、報告の内容は、不審メールの受信日と通数であり、さらに踏み込んだ情報、すなわち、公開されていない機構の個別の職員メールアドレス宛に、それぞれ、当該メールアドレスの職員の姓名が記載された不審メールであったという情報は提供されなかった。

その結果、厚労省情参室担当者は、平素より、多数の不審メールの受信報告を受けていたため、約100通という不審メールの通数自体からは、奇異な状況であると認識することができず、危機意識を持つことができなかった。情参室の対応としては、機構から提供された検体をNISCに提供し、NISCからの解析結果を機構に伝えるとの対応にとどまった。なお、NISCから検体の解析結果を受領したのは19日であったが、情参室の担当者が不在であったため、機構への伝達は21日となった。

機構からは、年金局事業企画課庶務係長に対しても、19日の時点で、18日及び19日の事象について情参室に宛てられたものと同様の報告がなされていたが、同係長においては、情報セキュリティに関する専門知識を有している情参室が直接対応しているとの認識から、自らは危機意識を持つことなく、したがって同時点で上長への報告はなされなかった。

（4）第三段階

ア　攻撃の態様

続いて、5月20日、機構の公開メールアドレス宛てに新たな送信元アドレスから標的型メールが合計5通送信された。そして、この標的型メールを受信した機構職員のうち一人が、メールを開封し、その添付ファイルも開封したことから当該職員の端末が感染し、C&Cサーバに対する不正な通信が発生した。

また、上記感染した端末を起点として、さらに、少なくとも2拠点にわたる26台の端末に不正プログラムの感染が拡大した。そして、5月20日以降、5月23日までの間、合計27台の端末から多数のC&Cサーバへの不正な通信が発生し、この過程で、感染端末からのアクセスによって共有フォルダに保管されていた業務情報や個人情報が収集され、外部に流出した。

かかる攻撃の過程において、機構の端末及びディレクトリサーバの管理者権限が窃取された。この点、フォレンジック調査の結果によれば、端末のOS及びディレクトリサーバの既知の脆弱性が利用されたことが原因であると推定される。

イ　機構の対応

（ア）メールの受信拒否設定

機構は、５月 20 日に職員から不審メールを受信したとの報告を受けたため、運用委託会社に依頼して当該不審メールの送信元メールアドレスについて受信拒否設定を行い、併せて、当該不審メールの送信元アドレスからのメールを受信した者を特定した。

しかしながら、機構は、職員の一人が標的型メールの添付ファイルを開封していた事実を５月 25 日まで確認することができなかった。

（イ）マルウェアの解析

機構は、20 日、運用委託会社を通じて、不審メールから確保された検体の解析をセキュリティソフト会社に依頼し、翌 21 日、厚労省情参室を通じて NISC にも検体を提出した。

そして、21 日、NISC から戻って来た解析結果には、当該不審メールの添付ファイルを開封した場合に通信が発生しうる C&C サーバの URL が記載されていた。これらの C&C サーバは、これまでの攻撃で用いられたものとは異なる新たなものであった。

しかしながら、機構は当該解析結果に記載された C&C サーバの URL ブロックや当該 C&C サーバに対する通信の監視といった対策は講じなかった。この結果、５月 21 日の時点で、機構の端末から解析結果に記載された C&C サーバに対する通信が発生していたにもかかわらず、28 日に至るまでその事実を認識することができなかった。

（ウ）不審な通信の検知と拠点単位のインターネット接続の遮断

５月 22 日、機構は、再び NISC から不審な通信を検知したとの連絡を受けた。そこで、機構は、当該不審な通信を発している端末の特定に着手し、同一拠点（A 拠点）にあった２台の端末を特定して LAN ケーブルを抜線するとともに、A 拠点全体の厚労省統合ネットワークを経由したインターネット接続の遮断を実施した。

また、翌 23 日には、運用委託会社が行っていたプロキシサーバのログの監視により、別の拠点（B 拠点）から、特定の URL に対し、大量の不審な通信が断続的に行われていることが判明した。そのため、機構は、当該不審な通信を行っている端末２台を特定し、これらの LAN ケーブルを抜線した。また、当該 URL と通信記録がある端末の有無を確認したところ、B 拠点において 19 台の端末から不審な通信が発生していたことが判明した。そこで、機構は同日、B 拠点についても、感染端末のある部門からの厚労省統合ネットワークを経由したインターネット接続を遮断した。

さらに 25 日には、運用委託会社より上記 22 日及び 23 日の事象について、① 22 日に NISC から通知された不審な通信については、GET メソッドのみ記録され

ていることから情報漏えいが発生した可能性は極めて低いこと、他方、②23 日に確認された通信については POST メソッドが記録されていることから、情報漏洩が発生した可能性は否定できない、との報告を受けた。機構幹部は、インターネット全面遮断による業務への影響を重視し、一定数以上の拠点で端末が感染しなければ全面遮断をしないとの基準を打ちたてた。

機構は、以上のような状況にもかかわらず、22 日、23 日、さらには 25 日のいずれの時点においても、特定の URL についてブロックを行うとともに、アクセスログの監視を実施し、通信監視体制を強化したものの、インターネット接続の全面遮断に踏み切ることはなかった。

（エ）警視庁への捜査依頼

機構は、５月 25 日、警視庁に５月 20 日以降の追加攻撃の概要を説明し、捜査に必要な情報を提供した。

（オ）インターネット接続の全面遮断

機構は、５月 28 日、警視庁から「機構から流出したと考えられるデータを発見した」との連絡を受領した。この情報を受けて、ようやく 29 日に機構全体の厚労省統合ネットワークを経由したインターネット接続の遮断を実施した。

しかしながら、同時点においてもメール送受信専用外部回線については、遮断した場合の業務への支障が大きいこと、また、メール送受信専用外部回線を通じて外部に情報が漏えいすることはないだろうとの判断に基づき、６月４日に至るまで遮断が実施されなかった。

ウ　厚労省の対応

厚労省情参室は、５月 21 日、機構より、19 日の報告後にも新たに不審メールが送信されていたとの報告を受けたが、同時に、５月８日のウィルスについては情報を外部に漏えいするものでなく、同日の事象に関して、これまでのところ情報漏えいは確認されていないとの報告を受けた。このため、担当者においては、５月８日の事象は収束に向かっていると認識し、危機意識を持つことはなかった。

５月 25 日になり、機構から、機構において複数台の端末が感染し、外部へ通信が発生していること、２拠点においてインターネット接続を停止していることなどが厚労省情参室に報告され、担当者はようやく事態の異常さを認識し、上長である参事官に報告するに至った。そして、同日、CIO 補佐官への報告・相談がなされ、CIO 補佐官は 27 日に機構に赴き状況報告を受けたが、初動対応について指示するタイミングとしては時機を逸しており、証拠の保全及び被害拡大の防止についての指示しかできなかった。

５月 25 日には機構から年金局企画調整官に対しても機構がサイバー攻撃を受

けているとの報告がなされ、同日、年金管理審議官まで報告が上がるに至った。

（5）情報流出

機構は、6月1日、不正アクセスにより機構保有の個人情報が約 125 万件、外部に流出していることが5月 28 日に判明したことを公表した。これは、5月 28 日に警察より外部から発見された流出情報が提供され、これを機構において確認・分析した結果、判明したものである。

機構の発表にあるように、流出が確認された個人情報は、職員が共有フォルダに保管していた情報の一部であり、最大で「基礎年金番号」「氏名」「生年月日」「住所」の4情報の流出が確認された件数が約 5.2 万件、「住所」を除く3情報が約 116.7 万件、「基礎年金番号」「氏名」の2情報が約 3.1 万件の合計約 125.0 万件である。これらに該当する人数は、受給者約 53 万人、被保険者約 49 万人の合計約 101 万人である。

機構によれば、基幹システム（社会保険オンラインシステム）への不正アクセスは確認されていないとのことであり、これまでのところ、約 125 万件以外の個人情報の流出は確認されていないこと、また、関係機関と協力し、調査を続けるとしている。なお、不正アクセスが生じた時点で共有フォルダに保存されていた個人情報の全体量がどの程度となっているかについては、引き続き、機構本部で調査が継続している。

第３　本件標的型攻撃と情報流出の原因

１　総論

本件は、機構が保有する機構 LAN システムに対して、いわゆる標的型攻撃が行われたことにより、同システムの共有フォルダ内に保存されていた個人情報が大量に外部へ流出した事案である。

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、関連する組織間に（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、迅速かつ的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線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発信が行われ、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以下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。

ア　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。

イ　サイバー攻撃への対応体制の不備

組織的な準備の面をみると、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は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。

ウ　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。

エ　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、本事案が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。

オ　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、今回の情報流出事案につながった大きな要因と指摘せざるを得ない。

カ　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）技術的要因

ア　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にされていた。

本事案では、第三段階の攻撃において、既知の脆弱性を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。

イ　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、取得されてい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。

ウ　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。

第４　再発防止策の提言

本事案は、システムの脆弱性を突いた執拗かつ組織的な標的型攻撃であり、これを防御するには、以下に述べる組織的、技術的な多層防御体制を構築して備えなければならない。

この組織的、技術的な多層防御を行うには、一部の者だけではなく組織が一体となった体制、運用が必要である。

したがって、再発防止の具体的な方策を提言する前提として、まず、機構等の役職員全員が標的型攻撃に対する危機意識を持つことが必要である。今回の情報流出事件のもたらした結果の重大性と標的型攻撃の危険性を一部の職員だけではなく、機構全ての役職員が自分達のこととして今後も認識し続けなければならない。

次に、標的型攻撃に際しては、組織が全体となってこれに対応する必要がある。それぞれの役職員が、これは自分の仕事ではないとか、自分の担当範囲でも従来通りのパターンを繰り返して漫然と対応するような姿勢ではなく、平素から困難に際し協力し合って逃げずに対処する組織づくりを心がけるべきである。普段からまとまりを欠いた組織では、危機に対し一体となって対処することなどできるはずがない。

以下、このことを前提に、個別的な再発防止策を提言する。

１　人的体制の整備

（１）セキュリティ対策本部の設立

機構には、副理事長をトップとする形だけの情報セキュリティ体制があるが機能していなかった。早急に、十分な判断力のある最高情報セキュリティ責任者の下にセキュリティ対策本部を設立し、役職員の役割・責任・権限を明確にし、各自が自らのなすべきことを熟知し、その責務を果たせるようにするべきである。そして、専門機関などと連携し最新の情報を入手すると共に、有事の際に共同して対処できる関係を構築しておくべきである。

（２）CSIRT の設立

機構は、膨大な個人情報を取り扱っていながら、緊急時に対応すべき CSIRT を設けていない。機構内の的確な判断力を有する幹部から適任者をトップに選び、外部専門家の支援を受ける体制の CSIRT を設立すべきである。その場合、現場で作業するメンバーをも含めた機動的に動ける体制にすべきである。

（3）共有フォルダなどの個人情報の一元的管理と整理

機構の共有フォルダには、膨大な個人情報等が漫然と積み上げられ、これを一元的に管理していなかったことから、共有フォルダに保管されていた情報の調査に長時間を要し、いまだにその全容が明らかになっていない。

個人情報は、インターネットの影響から遮断し、やむを得ないものは分割して厳格に管理すべきである。その際、現場の実情を理解し守れる規則を作るとともに、作った規則は必ず職員に守らせることが必要である。

（4）教育訓練の徹底

サイバー攻撃の端緒を把握するのは、PC 端末を扱う者全てにその機会があるから、そのポストを問わず教育訓練の実施が必要である。特に幹部には、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の教育研修を、その他の職員には疑似メールなどによる実践的な訓練が必要である。

（5）外部監査の実施

独立した専門家による情報セキュリティ監査を行う必要がある。内部の監査機能が不十分である以上、外部の目で問題点を発見するのは民間では当然のことである。また、一連の再発防止策を講じた段階で保証型セキュリティ監査を受けることが望ましい。

（6）明確な情報セキュリティポリシーなどの策定

機構の情報セキュリティポリシーや手順書は、標的型攻撃を予測したものではなかった。このことが今回の攻撃に対し、適切な対応ができなかった一因でもある。速やかに標的型攻撃に備えた明確で活用しやすい情報セキュリティポリシーや手順書を策定すべきである。

2　厚生労働省の監督体制の整備

（1）厚労省の情報セキュリティ体制の整備

厚労省の情報セキュリティの中心となるべき情参室が弱体であることは、既に指摘したが、充て職で形式的な現在の情報セキュリティ体制を専門家をアドバイザーとして加えた機能し得る体制に改めること、セキュリティ情報が集中する情参室を質量ともに充実すること、CIO 補佐官との連携を図ること、CSIRT も技術力を持った実用的なものに改めることなどは着実に実行すべきである。

（2）機構 LAN システムに対する監督部署の明確化

今回標的型攻撃を受けた機構 LAN システムについて、厚労省内部で担当部署が不明確であることは、監督省庁としてあり得ないことである。速やかに担当の課室を明確にし、責任を持って対応に当たらせるべきである。

（3）情報連絡の迅速化

今回に限らず、省内及び傘下の特殊法人等からのインシデント発生後の連絡が遅延しているが、標的型攻撃に対しては迅速な対応が必須である。インシデント発生後直ちに情参室に第一報が入り、それが速やかに最高情報セキュリティアドバイザー等の専門家に通報され、指導を受けるように改めるべきである。

3　技術的観点からの提言

（1）業務の実態とリスクに基づいたシステムの整備

実効性のある技術的対策を行うには、まず業務の実態に基づいて情報セキュリティ上のリスクを的確に把握することが必要である。標的型メールを受けるおそれのある業務、大量の個人情報を取り扱う業務、一般事務など、きめ細かな視点でリスクを評価する必要がある。

その上で、このリスク評価の結果に基づき、リスクに応じたネットワークの区画分割を行い、それぞれの業務内容に応じた対策を講じるべきである。その場合、少なくとも個人情報をインターネットに接続した区画に置くことは避けるべきであり、区画をまたがる通信に関しては不正を検知または阻止できる仕組みの導入が必要である。

また、インシデント対応や保守に伴うシステム停止が他の業務に大きな影響を与えないよう、システム設計の段階から配慮がなされるべきである。特に、単一障害点の存在は、それ自身が大きなリスクを抱えるばかりでなく、サイバー攻撃への対応が困難になることから、設計段階から単一障害点を設けないように注意すべきである。

サイバー攻撃は日々高度化していくことから、定期的にリスクの見直しを行い、セキュリティ対策の継続的な改善を図っていくべきである。

（2）防御力を高めるための運用管理の徹底

技術的対策を実効性のあるものにするためには、システム整備と共に防御力を高めるための運用管理を徹底することが不可欠である。新たな攻撃手法に関する情報を常に収集し、運用における技術的な対応をより迅速に行えるようにすべきである。

機構 LAN システムの運用管理においては、脆弱性管理の不備とシステム監視

の不十分さにより、被害の深刻化を招いた。脆弱性管理においては、管理者権限を適切に管理するとともに、機構 LAN システムに係わる脆弱性情報の適時適切な収集を行い、重要な脆弱性が確認された場合には、速やかに対応の必要性を判断し、セキュリティパッチを適用することが可能な運用体制を構築すべきである。また、サイバー攻撃による外部からの侵入を想定した監視内容や監視方法を定め、異常を即座に検知するための監視体制の構築が必要である。

4　日本年金機構の意識改革

前段でも指摘したように、これらの再発防止策は、機構の役職員が今回の事件に正面から向き合って危機意識を持ち、組織が一体となって対応することが前提である。

しかしながら、今回の検証を通じて見た限りにおいて、残念ながらまとまりと自覚を欠いた姿が目に付いた。これだけの情報を流出して国民に多大の心配をかけていながら、検証委員会の調査を受けるに際し、その後改まったとはいえ、一部の者が重要な資料を出し渋り、墨塗りをするなどの態度は論外である。

年金制度に対する国民の信頼を回復するためにも、これを機会に徹底的な意識改革が必要であると考える。

第５　終わりに

今回の機構に対する標的型攻撃は、まれにみる組織的かつ執拗な攻撃であったが、これに対する機構と厚労省の備えは極めて脆弱であり、結果として大規模な情報流出をもたらし国民の信頼を失墜した。しかし、現在のIT時代において、標的型攻撃を含むサイバー攻撃があるからといって今さら紙媒体の時代に戻ることはありえず、この種攻撃を防御するために攻撃者の偵察・侵入・情報収集・情報窃取など各段階において、体制的かつ技術的な多層防御によりこれに備える必要がある。

標的型攻撃を含むサイバー攻撃は、このところ極めて組織的かつ巧妙化している。今回の事例は、単に機構だけの特殊な問題として捉えるのではなく、官民を問わず全ての組織が、この種の攻撃に対しあらかじめどのような備えができているか、攻撃があった場合に具体的にどう対応するかを真剣に考える契機として生かすことができれば幸いである。

参考　IT用語の解説

英	C&Cサーバ（Command and Controlサーバ）	あらかじめ乗っ取ったコンピュータに対し、サイバー攻撃等に関する命令を送信してこれを制御する、乗っ取ったコンピュータから得た情報を受信する等の役割を果たしている外部のサーバ。C2サーバともいう。
	CIO（Chief Information Officer）	組織全体における情報システムや情報流通に関する事項を統括する最高責任者。
	CSIRT（Computer Security Incident Response Team）	セキュリティインシデントに対応するための組織。平時はインシデント情報等の収集・分析とそれに基づく対応方針・手順の策定にあたり、インシデント発生時には緊急対応を担う。
	GETメソッド	HTTP通信又はHTTPS通信（いずれも、Webブラウザ等のクライアントとサーバの間で行われる通信の仕組み。）において、クライアントがサーバに送信する命令文の種類の一つ。一般的にはサーバから情報を取得する目的で用いられるが、サーバに対し情報を送信する目的で利用することも可能である。
	LAN（Local Area Network）	同一施設内にあるコンピュータや通信機器、プリンタ等の機器を接続し、情報をやり取りするネットワーク。
	OS（Operating System）	機器の制御機能や他のソフトウェアが共通して利用する機能等を備えた、システム全体の基本となるソフトウェア。
	POSTメソッド	HTTP通信又はHTTPS通信において、Webブラウザ等のクライアントがサーバに送信する命令文の種類の一つ。一般的にはサーバに対し情報を送信する目的で用いられる。
	URLブロック	URL（インターネット上の情報の位置を特定するための書式）に特定の文字列を含む通信先との間の通信を遮断する措置。
あ	インシデント	情報セキュリティインシデントのこと。コンピュータシステムのセキュリティに脅威を及ぼし、又はその可能性のある事象。
	ウィルス	マルウェアの一種で、自己伝染機能（他のシステムやプログラムに伝染する）、潜伏機能（時間、起動回数等の条件が揃うまで症状を出さない）、発病機能（情報の送信や破壊等の被害を生じさせる）のいずれかの機能を持つもの。広義ではマルウェア全般をウィルスと呼ぶこともある。
	オンラインストレージサービス	インターネット上でファイル共有のための領域を提供するサービス。
か	クライアント	コンピュータネットワークにおいて、他のコンピュータ（サーバ）に対して情報処理サービスの提供を求め、その提供を受けるコンピュータ・ソフトウェア。
さ	サーバ	コンピュータネットワークにおいて、他のコンピュータ（クライアント）からの求めに応じて何らかの情報処理サービス（ファイルの提供等）を行うコンピュータ・ソフトウェア。
	脆弱性	ソフトウェア等に存在するセキュリティ上の欠陥。サイバー攻

		撃に際し悪用される危険がある。
	セキュリティソフト	マルウェアの検出・駆除その他の情報セキュリティに関する機能を提供するソフトウェア。
	セキュリティパッチ	完成したソフトウェアにおける、既知の脆弱性への対応等の変更点を収録したファイル。
た	単一障害点	コンピュータシステムにおいて、その箇所が毀損した場合にシステム全体の機能が損なわれることとなる箇所。
	定義ファイル	マルウェアに関する情報を収録したファイル。セキュリティソフトがマルウェアを検出するために用いる。パターンファイルとも呼ばれる。
	ディレクトリサーバ	コンピュータネットワークにおいて、ID、パスワード、メールアドレス等の個々のユーザーに関する情報や、ユーザーごとのアクセス権限の設定等を一元管理するサーバ。コンピュータネットワーク内の機器（コンピュータやプリンタ等）に対してプログラムを自動的に導入する機能も持つ。
	ドメイン	インターネット上の個々のネットワーク等を識別する名前。同一ドメイン内のより小さな単位を識別する名前をサブドメインと呼ぶ。
	トロイの木馬	マルウェアの一種で、正体を偽ってコンピュータへ侵入し、データの消去・流出、他のコンピュータへの攻撃等の不正な命令を実行するもの。ウィルスと異なり、自己増殖はしない。
は	バックドア	コンピュータやサーバ、コンピュータネットワークの内部に、ID・パスワードによる認証等の正規の手続を踏むことなく侵入することができる「裏口」のこと。マルウェア（特にトロイの木馬）によって設置されることがある。
	抜線	ケーブルを抜き取る等の物理的な方法で、機器とコンピュータネットワークとの間の接続を完全に遮断すること。
	ファイルサーバ	コンピュータネットワークにおいて、ファイルを共有するためのサーバ。
	フォレンジック	デジタルフォレンジックのこと。コンピュータやネットワークシステムに残されたデータ等を詳細に解析・復元し、過去に行われた情報処理や通信等に関する事実を究明する作業。
	フリーメール	無料でメールアドレスを発行するサービス。
	プロキシサーバ	コンピュータネットワーク内部のコンピュータがインターネットに接続する際に、間に入って通信を中継するサーバ。プロキシサーバを経由することによって、コンピュータネットワーク内部の個々のコンピュータに関する情報を外部に知られることなく通信を行うことができ、コンピュータネットワーク内部への不正アクセス等のリスクを減少させることができる。
ま	マルウェア	不正・有害な動作を行う意図で作成された、悪意のあるソフトウェアの総称。何らかの不正な命令を実行したり、外部への通信を行ったりする。サイバー攻撃の主要な手段。
	メールサーバ	電子メールの送受信を行うサーバ。

ら	ログ	コンピュータやソフトウェアが、その起動や停止、設定変更、処理した情報や通信に関する内容、処理結果、エラーの有無内容等を自動的に時系列で記録したもの。