第１３回社会保障審議会年金事業管理部会
平　成　２　７　年　８　月　２　６　日
資料２－１

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について

平成27年8月20日
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

1. 不正アクセスによる個人情報流出事案の概要

＜不正アクセスの概要＞

○5月8日(金)以降、標的型メールを合計で124通受信。そのうち、メールの添付ファイル等を開封した機構の職員は合計5名。

○感染した端末は合計31台。

○お客様の約125万件の個人情報は、5月21日(木)から23日(土)までの間に流出。

※情報流出した端末のログ解析により判明。

＜お客様の個人情報流出の概要＞

○不正アクセスによるお客様の個人情報流出の件数

⇒ 約125万件(対象者は約101万人)

○お客様約101万人の個人情報流出件数の内訳

・4情報(基礎年金番号、氏名、生年月日、住所) ⇒ 約 5.2万件(約 1.5万人)

・3情報(基礎年金番号、氏名、生年月日) ⇒ 約116.7万件(約96.9万人)

・2情報(基礎年金番号、氏名) ⇒ 約 3.1 万件(約 3.0万人)

※約55万件のデータについては、パスワード未設定。

○6月1日(月)の本事案公表後、感染端末等について解析等を行うフォレンジック調査(詳細はP3参照)など当機構で確認を進めた結果、現時点において、警察から提供された資料に基づいて判明した約125万件以外のお客様の個人情報の流出は確認されていない。

○基幹システムへの侵入及び基幹システムからの情報漏洩は確認されていない。

2. 事案の経緯

＜事案の経緯＞

5月 8日(金)　内閣サイバーセキュリティセンター(以下「NISC」という。)より厚生労働省情報政策担当参事官室(以下「情参室」という。)、年金局を通じ、「不審な通信を検知」との通報を受領。該当端末を特定し、抜線。

5月15日(金)　運用委託会社より「新種ウイルスは、外部に情報を漏洩するタイプではない」との解析結果を受領し、一旦収束したと判断。

5月18日(月)　不審メール受信(99通)。

5月19日(火)　高井戸警察署に相談及び捜査依頼。不審メール受信(18日から20通)。

5月20日(水)　不審メール受信(3通)。

5月21日(木)　NISCより情参室を通じ、不審メールの解析結果を受領。同日から端末より個人情報流出が始まる。

5月22日(金)　NISCより情参室を通じ、「不審な通信を検知」との通報を受領。該当端末を特定し、抜線。同日中に該当拠点の統合ネットワークを通じたインターネット接続を遮断。

5月23日(土)　運用委託会社より、「不審な通信を検知」との連絡を受領。該当端末を特定し、抜線。同日中に該当拠点の統合ネットワークを通じたインターネット接続を遮断。個人情報流出が止まる。

5月28日(木)　警察より、「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。

5月29日(金)　機構全体の統合ネットワークを通じたインターネット接続を遮断。

6月 1日(月)　事案公表。

6月 4日(木)　メール送受信専用外部回線を遮断。

3. 感染端末等に関するフォレンジック調査等(注)の結果

(注)フォレンジック調査(端末やサーバのデータやログ等から不正アクセスの記録を収集・解析し、証拠性を明らかにする調査)及びセキュリティインシデント調査(ログ解析等の調査)

＜調査対象及び調査方法＞

①調査対象:端末31台、認証サーバ1台、共有ファイルサーバ1台

②調査方法:ウィルス感染が疑われる端末等について、削除されたファイルの復元等の措置を講じ、端末等に残された痕跡から、不正プログラムの内容、攻撃者の操作、情報流出の可能性のあるファイル等を収集、解析

※フォレンジック調査は、攻撃者の操作のすべてを解明するものではないが、一定の調査結果が明らかになった。

＜調査結果＞

①お客様の個人情報に関しては、「約125万件」以外の新たな情報流出は確認されていない。

②お客様の個人情報以外の情報流出の可能性

○機構職員の個人情報流出の可能性225件

○職員の業務用個人メールアドレスの一部が流出している可能性(件数不明)

○その他流出している可能性がある情報は以下のとおり。

	分類	概要
i	組織関係情報	各拠点(事務センター、年金事務所)の職員配置状況
ii	業務マニュアル等	事務ソフトの利用マニュアル、事務連絡の一部、報告書様式
iii	システム関係の情報	共有ファイルサーバ上のファイル名称一覧(攻撃者が共有ファイルサーバを捜索した処理結果)等

③攻撃者の挙動として判明した事実

○5月8日(金)、外部通信時に職員のメールアドレスの一部が窃取されていた可能性がある。

○5月20日(水)、攻撃者が管理者権限を窃取し、その権限を使用して他の端末への感染を拡大させた。

4. 機構の事案対応に関する検証・評価①

＜検証の視点＞

（1） 本事案は標的型メール攻撃であり、まず、攻撃の各局面における機構の対応のどこに問題があったかについて検証する。その際、原因の徹底究明と再発防止を行うという観点から、事後的に判明した事実も含め、また、機構内でルール化されていない対策も含めて、情報流出を防ぐために実施すべきであったと考えられる対策項目が本事案についてどこまで実施できていたかを検証・評価する。

○具体的な対策項目については、本事案の経緯を踏まえ、同様の標的型メール攻撃があった場合にどのように対応すべきかという観点から以下のとおり整理した。（参考2に対応状況一覧を記載）

（標的型メールの受信に関し対応すべき項目）

①受信の確認 ②受信者の範囲の特定 ③開封・感染の確認、抜線（受信者ヒアリング）
④送信元受信拒否設定 ⑤全職員への注意喚起 ⑥端末の回収、検体の確保 ⑦ウィルスの解析依頼
⑧URLフィルタリング（不審URLへの通信の遮断） ⑨ウィルスパターンファイル（ワクチン）の適用
⑩メール送受信専用外部回線の遮断

（不審通信に関し対応すべき項目）

①通信の確認 ②端末の特定、抜線 ③感染経路の特定（職員ヒアリング） ④ログ確認による感染範囲の特定
⑤URLフィルタリング（不審URLへの通信の遮断） ⑥通信監視体制の強化 ⑦端末の回収、検体の確保
⑧ウィルスの解析依頼 ⑨ウィルスパターンファイル（ワクチン）の適用 ⑩感染部署のインターネット遮断
⑪インターネット全面遮断

なお、このほか、不審通信を把握した場合に情報流出が疑われるときは、情報流出の有無・内容等を把握し、その後の対応を検討するために必要となるフォレンジック調査を行うことが求められる。

（2） また、個人情報を共有ファイルサーバに置き、インターネット接続環境下で取り扱うことを許していたことが、今回の個人情報流出につながった。こうした共有ファイルサーバのこれまでの管理の実態について検証する。

（3） あわせて、端末利用におけるインシデント対応の問題点について検証する。

4. 機構の事案対応に関する検証・評価②

＜攻撃の各局面における対応＞

○5月8日(金)からの一連の対応状況を検証した結果、5月8日(金)・15日(金)、18日(月)、20日(水)、21日(木)、22日(金)・23日(土)における対応が、21日(木)から23日(土)までの間の個人情報流出の防止に向けて改善できた可能性のある重要なポイントであったことが判明した。

＜ポイント1　5月8日(金)・5月15日(金)＞

送信元メールアドレスの受信拒否の設定を行わなかった

⇒フォレンジック調査の結果により、不審通信時にメールアドレスの一部が窃取されている可能性があることが判明した。仮にこの段階で機構全体として「送信元メールアドレスの受信拒否」を設定できていれば、同月18日(月)以降の攻撃の防止につなげられた可能性があった。

⇒5月8日(金)にA拠点の職員1名が不審メールのリンク先にあるファイルを開封した。この事実をNISCから不審通信を指摘されるまで把握できなかった。

標的型メール攻撃ではないかとの疑いが組織として共有されなかった。

⇒情報セキュリティ担当部署の担当者は5月8日(金)の攻撃を標的型メール攻撃ではないかとの疑いを持ったが、その疑いが組織としては共有されず、同月15日(金)のウィルス解析結果が「外部に情報を漏洩するタイプではない」との連絡を受けたことから、一旦収束したと判断。

＜ポイント2　5月18日(月)＞

標的型メール受信者全員に個別に添付ファイルの開封の有無を確認しなかった

⇒職員3名が添付ファイルを開封した事実について情報セキュリティ担当部署は把握していなかった。このことから、事案への対応(端末を抜線・解析し、不審通信先を特定してURLのフィルタリングを実施するなど)が遅れた。ただし、この感染による情報流出はなし。

＜ポイント3　5月20日(水)＞

標的型メール受信者全員に個別に添付ファイルの開封の有無を確認しなかった

⇒B拠点の職員1名が添付ファイルを開封した事実について情報セキュリティ担当部署は確認できなかった。このことから、事案への対応(端末を抜線・解析し、不審通信先を特定してURLのフィルタリングを実施するなど)が遅れ、感染が拡大した。

⇒また、フォレンジック調査の結果により、感染した同日中に管理者権限が窃取され、複数台の端末へ感染が拡大したことが判明した。仮にこの段階で感染の事実を情報セキュリティ担当部署が把握できていれば、少なくともB拠点の統合ネットワークを通じたインターネット接続を遮断することができ、以降の情報流出が防止できた可能性があった。

4. 機構の事案対応に関する検証・評価③

＜ポイント４　　５月21日（木）＞

NISCの解析結果に基づくフィルタリングを行わなかった

⇒NISCの解析結果を手がかりとして感染端末を特定し、仮にこの段階でその通信先について情報セキュリティ担当部署がフィルタリング（不審URLへの通信の遮断）ができていれば、以降の情報流出が防止できた可能性があった。

＜ポイント５・６　　５月22日（金）・23日（土）＞

機構内すべての統合ネットワークを通じたインターネット接続の遮断を行わなかった

⇒22日（金）にA拠点、23日（土）にB拠点の遮断により、それぞれからの情報流出は停止したが、仮にこの段階で22日（金）中に機構全体の統合ネットワークを通じたインターネット接続を遮断できていれば、以降の情報流出が防止できた可能性があった。

○情報セキュリティポリシー上は、インシデント対応の必要性が規定され、その具体化はリスク管理一般の規定等に委ねられており、上記のポイントとなる各対応について、いずれも具体的なルールは定められていなかった。

○上記のとおり、標的型メール攻撃に対し十分な対応ができなかったことの要因としては、以下のような構造的な問題があった。

・本事案については、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たが、基本的対応は担当者任せとなっており、CIOや部長から具体的指示を行った事跡は確認できていない。

・理事長、最高情報セキュリティ責任者（副理事長）への報告も適時適切に行われない場合があり、組織として迅速な対応が行われなかった。

・情報セキュリティ担当部署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者が配置されていなかった。

・厚生労働省との情報共有について、案件の内容や重要性に応じてどのレベルで連絡し、相談するかに関するルールがあらかじめ定められていなかったため、担当者レベルに止まっていた。

4. 機構の事案対応に関する検証・評価④

＜共有ファイルサーバの取扱い＞

○「日本年金機構共有フォルダ運用要領」により、個人情報等の重要情報は共有ファイルサーバに保管しないことを原則とし、例外的に保管する場合のパスワード設定などのセキュリティ措置を規定するなどのルールはあったが、徹底が図られていなかった。

○また、インターネット接続環境下にある共有ファイルサーバに個人情報を置く、ということに伴い外部からの脅威にさらすことになるというリスクへの認識が甘く、対策を検討してこなかった。５月８日(金)に本件の最初の攻撃が行われた時点でも、この点の危険性への対策について、役員により検討されることはなかった。

○共有ファイルサーバの管理が適切に行われず、情報流出につながったことの要因としては、以下のような構造的な問題があった。

・個人情報をインターネット接続環境下に置く、という問題を持ったシステム設計を改善しておらず、役員はもとより組織全体としてサイバーセキュリティの危機意識に欠けていた。

・共有ファイルサーバの運用ルールを定める際に、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、というリスク認識に欠けていた。

・担当する文書管理担当部署においては、パスワードをかけるなどの運用ルールが、全拠点において、本当に実行されているかなどの点検・確認が行われておらず、運用ルール自体が有名無実化していた。

＜端末利用におけるインシデント対応の問題点＞

○標的型メール攻撃に対する日頃からの継続的な注意喚起が不十分であり、５名の職員が標的型メールの添付ファイル等を開封したが、そのうちの４名の職員は不審メールを受信した旨を情報セキュリティ担当部署に報告していなかった。これまでの職員研修などでは危機意識や、万一開封してしまった際に対応するノウハウが徹底されていなかった。

○標的型メールの添付ファイル等を開封した職員は、業務上の理由でインターネットの閲覧規制が解除されていたが、情報セキュリティ担当部署等からは、標的型メール攻撃への注意喚起がされることはなかった。

○今回の攻撃発生後、注意喚起のために全職員に送られたメールの内容も、削除指示に限られ、誤って添付ファイルを開封した場合の具体的対処方法や、情報セキュリティ担当部署に連絡すること、などが記載されていなかった。

○こうした点についても、上記共有ファイルサーバの取扱いと同様、あらかじめのリスク分析と対応方針の策定が行われておらず、また、役員もリスクの認識に欠けていた。

4. 機構の事案対応に関する検証・評価⑤

＜全体評価＞

○このたびの初動対応をみると、情報セキュリティ担当部署の担当者は5月８日(金)の攻撃を標的型メール攻撃ではないかとの疑いを持ったが、情報セキュリティに関わる幹部の問題認識の甘さにより、この疑いが組織として共有されなかった。また、とられた対策の有効性等に関する分析もなされず、体系的な対応方針の検討も行われなかった。

○情報流出の直接的な要因は、５月18日(木)から23日(土)までの一連の対応において、標的型メールを受信した際の対策として、抜線以外に具体的なルールの定めがなく、開封・感染の確認、URLフィルタリング（不審URLへの通信の遮断）などの対策を講じなかったことにある。特に、B拠点が感染した20日(水)の時点で感染が確認できていれば、これらの対策を講じることができ、お客様の個人情報流出を防止できた可能性があった。

○不審通信を把握した後の対策（端末の特定・抜線、ログ確認による感染範囲の特定、通信監視体制の強化、ウィルスの解析依頼など）については基本的な対応は行い、情報流出の拡大の防止にはつながった。しかし、そもそも上記のような「標的型メールを受信した際の対策」について対応できなかったために、情報流出自体の防止にはつながらなかった。

○初動対応の遅れを招いた背景は、年金個人情報を守るという組織として一貫した方針の下、こうした対応への議論が平素から行われておらず、組織全体としての対応方針の明確なルール化と訓練等によるその徹底を図ってこなかったことにある。

○共有ファイルサーバの取扱いや端末利用におけるインシデント対応については、そのリスクについて、役員から職員に至るまで認識が徹底しておらず、そのことが今回の情報流出の極めて大きな原因となったと言える。

○上記の各点は、いずれも、情報セキュリティに対する役員の認識が、極めて不十分だったことを示していると言わざるを得ない。あわせて、その根底には、機構が抱える次のような構造的な問題が、今なお根深く残っていると言わざるを得ない。

- 現場における業務の実態が幹部を含む本部に伝わらない、幹部を含む本部に業務の実態を把握する努力が不足しているといった組織としての一体感の不足
- インシデント発生時に即時適切に対応するために指揮命令系統をあらかじめ明確化しておくこと、ルール不在の緊急事態に際して幹部が適切な判断をするということ、ができなかったこと。
- 実態を踏まえてルール設定を行うという努力不足
- ルールが遵守されていることを確認する仕組みの欠如

○このような重要な事案を機構の最高意思決定機関である理事会に諮っておらず、事案の重要性に対する役員の認識が欠けていた。

○一部職員がインターネット掲示板に書き込みするなど、職員のモラルの問題も明らかになった。国民の年金を預かる、という緊張感、責任感、使命感に立ち戻り、意識改革を行って、職員が心を一つに一丸となって、改めて組織全体の改革に取り組まなくてはならない。

5. 個人情報流出に関するお客様対応

＜お客様へのお詫びとお問い合わせ対応＞

○お詫びとお願いの文書の送付 （6月3日(水)～4日(木) : 約1.5万人、6月22日(月) ～29日(月) : 約100万人）

○未送達者への対応 （7月～）

○専用コールセンターの開設 （6月～ : 約1000人体制）

○年金事務所の土日開所 （6～7月 : 全国312事務所、8月 : 59事務所）

＜お客様の被害防止に向けた取組＞

○基礎年金番号の変更のお知らせ文書の送付 （8月下旬～ : 約96万人）

○住所変更・金融機関変更の手続者への対応 （6月上旬～ : 対象者への戸別訪問等）

○不審電話への対応 （6月～ : 通報者への戸別訪問等）

○ホームページによる情報提供等 （6月～ : 不審電話に対する注意喚起、具体的な事例等を掲載）

○関係機関と連携した広報 （6月～ : 消費者庁、国民生活センター、警察庁、市町村等と連携）

（参考）情報流出事案に要した費用

上記の対応にこれまでに要した費用は合計約6億円で、そのうち政府広報に要した費用である約2億円については既存の予算から支出しており、本事案による新規支出費用は約4億円。なお、今後、新たな基礎年金番号と年金手帳等の郵送に要する費用は約4億円程度と考えられる。（8月20日(木)現在）

※個人情報流出に関するお客様への説明誤り事案

○お客様からの個人情報流出の有無に関する問い合わせに対し、一部のお客様に誤った説明（個人情報が流出していたにもかかわらず、流出は確認されていないと説明）を行っていたことが判明。

説明誤りのあったお客様　2,449名　⇒「該当表示（アラート表示）」の付加誤り　：　2,426名

コールセンターにおける説明誤り　：　23名

○該当のお客様に対しては、6月27日(土)より、年金事務所職員が戸別に訪問し、正しい回答の説明と謝罪を行っていたが、お客様への対応に専心していたため、国民への公表が遅れた（7月13日(月)公表）ほか、監督官庁である厚生労働省への報告もしなかった。早期の情報共有という本事案発生時の教訓を生かせず、誤りを繰り返してしまったことは、率直に認めざるを得ない。なお、個人情報が流出していないが流出していたという誤った説明を行っていたケースも14件あり、8月10日(月)に公表した。

○今後、迅速で正確な組織内の二重チェック体制の徹底、厚生労働省への報告ルールの見直し（案件の内容や重要性に応じてどのレベルで連絡し相談するかのルール策定）等、再発防止策を確実に実施していく。

6. 再発防止に向けた今後の取組①

＜今後の機構システム全体のあり方＞

○機構のシステム全体について、標的型メール攻撃を含め、想定し得るあらゆるインシデントに耐え得る強力な防御体制を整備する。

○基幹システム及び個人情報等重要情報を扱うシステムについては、インターネット接続環境からの完全な遮断によって守ることとする。

○将来的なインターネット環境の構築に当たっては、「基幹システムはインターネット接続環境下に設置しないこと」はもとより、「個人情報を扱う業務の共有ファイルサーバは基幹システムの領域内に設置すること」及び「個人情報はインターネット接続環境下に置かないこと」を基本として、具体的には外部の情報セキュリティ専門家等ともよく相談しながら検討する。

○当面の対応としては、既存の機構LANシステムとは物理的に独立したインターネット環境を構築することを検討する。

＜情報セキュリティ体制の強化＞

○標的型メール攻撃等への多重防御体制を整備する（入口対策、内部対策、出口対策の強化）。

○本事案を踏まえ、情報セキュリティ対策の司令塔としての組織（「情報管理対策本部（仮称）」）を新設し、以下の対策を早急に進め、情報セキュリティに関する機構全体のガバナンスを強化する。

①情報セキュリティの専門家の招聘（最高情報セキュリティアドバイザー）又は専門機関との契約

②標的型メール攻撃等に対する諸規程・要領・手順書などの整備（諸規程の改正）

③システム運用委託業務の手順書の明確化（委託業者との役割分担やルール等）

④ISO27005を踏まえた、標的型メール攻撃等を想定したリスクアセスメント調査の実施

⑤情報セキュリティに関するルールの徹底（情報セキュリティ研修の充実）

○「情報管理対策本部（仮称）」は、理事長の下で、システムのリスク評価も含め情報セキュリティ対策の司令塔として、外部からの脅威、内部からの脅威の双方への対策を強化する。

6. 再発防止に向けた今後の取組②

＜職員研修及び内部監査＞

○情報セキュリティ研修については、毎年、全職員を対象に実施していたが、標的型メール攻撃に対する内容が不十分だったため、今後はさらなる充実を図る。

・標的型メール攻撃等に対する訓練（模擬メールテストなど）
・外部講師による情報セキュリティ研修（最新動向や注意点等）　等

○機構の内部監査についても、これまで、通常の事務処理がルールどおりに行われていたかということに重点を置いて監査を行ってきたが、今後は、情報セキュリティに関するリスクにも重点を置いて監査を行う。

・業務監査として、共有ファイルサーバの点検状況等を監査
・システム監査として、システムのリスク分析や情報セキュリティ体制・緊急時対応手順等を監査

＜ガバナンス・組織風土のゼロベースからの抜本改革＞

○情報、とりわけ「悪い知らせ」が組織の上層部に効率よく集約され、それに基づき、ルールを踏まえて組織の意思決定が行われ、決定事項は過不足なく、正確かつ迅速に組織の隅々に至るまで伝わり、職員全員が心を一つにして着実に実行される組織として、機構を再構築する。

○ガバナンス・組織風土に関するゼロベースからの抜本改革を行い、次のような取組を実施するため、理事長をトップとする「日本年金機構再生本部（仮称）」を設置し、旧社会保険庁時代から指摘されてきた体質から完全脱却し、厚生労働大臣の監督の下で、責任ある年金事業を確実に執行する、風通しの良い組織に生まれ変わる。

・職員提案制度の活用などにより、お客様に直接接する職員の声を聴くことを通じて、より現場の実態を踏まえたルールを設定し、かつ、その設定したルールを現場において遵守する。
・人事評価制度を抜本的に見直す。
・年金事務所等の地域の各拠点と本部との一体感を高めるため、本部と現場間の人事異動の促進や、人事の一元化をさらに進める。

○機構は、公的年金制度の最も大切な執行部分を担っているという緊張感、責任感、使命感を持って、厚生労働省との的確かつ緊密な情報共有体制を構築する。

・規程等の事前調整のルール化、事務処理誤りの事前報告のルール化等、機構の業務執行のあり方を見直し、厚生労働省との情報共有を図る。
・情報共有に当たっては、担当者レベルのみならず、理事長、副理事長、理事、部長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。）を厚生労働省とともに構築し、遵守する。

7. 本事案が発生した構造的な要因と今後の対策①

1. インシデントへの対応体制

＜要因＞

○本事案については、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たが、以下の問題があった。

①基本的対応は担当者任せとなっており、CIOや部長から具体的指示を行った事跡は確認できていない。

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、組織として迅速な検討が行われなかった。

③ ラインに情報セキュリティの専門家がおらず、セキュリティアドバイザに任命されていた担当者も他の業務に当たっていた。

④情報セキュリティ担当部署と、運用委託会社との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であった。

＜今後の対策＞

○情報セキュリティ対策の司令塔として、一元的に管理する「情報管理対策本部（仮称）」を新設する。

○情報セキュリティの専門家の招聘（最高情報セキュリティアドバイザー）又は専門機関との契約

○情報セキュリティの専門家を計画的に育成する。

○情報セキュリティに関する担当ラインを当面有事対応とし、緊急対策本部（本部長：理事長、6月14日（日）設置）による対応とする。

2. 共有ファイルサーバの管理

＜要因＞

○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った。

○インターネット接続環境下にある共有ファイルサーバに個人情報を置くというリスクへの認識が甘かった。

○運用ルールを定めていた文書管理担当部署においては、ルールが本当に実行されているかなどの点検・確認が行われておらず、有名無実化していた。

＜今後の対策＞

○機構のシステム全体について、多種多様なインシデントに耐え得る強力な防御体制を整備する。

○個人情報等重要情報については、インターネット接続環境から完全に遮断する。

○共有ファイルサーバの管理業務を情報セキュリティ管理担当部署に移行し、ルールの遵守状況などの確認を徹底する。

7. 本事案が発生した構造的な要因と今後の対策②

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た。

○厚生労働省の改正内容を後追いで情報セキュリティポリシーに反映させるのみで、研修、訓練も行われておらず、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、役員を含め、精緻な検討・議論がされていなかった。

4. 職員研修

＜要因＞

○情報セキュリティ研修の内容に関しては、実質的に情報セキュリティ担当部署の担当者レベルで決定されており、担当部署として責任を持った意思決定が行われていなかった。

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。組織としての一体感が不足していた。

○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た。重層的な情報共有のルールがなかった。

○説明誤り事案についても一部幹部の思い込みが招いた失態。

＜今後の対策＞

○標的型メール攻撃等への多重防御体制を整備する（入口対策、内部対策、出口対策の強化）。

○「情報管理対策本部（仮称）」を新設し、一元的に情報セキュリティに関する業務を責任を持って実施する。

・情報セキュリティポリシーを改正するとともに、NISCのガイドラインやISO27005などを参照し、標的型メール攻撃に対する具体的対処手順を整備し、職員への周知・徹底を図る。

・情報セキュリティに関する研修内容に関し、「情報管理対策本部（仮称）」による意思決定が行われるよう、ルール化を図る。

・研修の成果について、模擬訓練等によりチェックし、継続的に研修内容を改善する。

＜今後の対策＞

○理事長をトップとする「日本年金機構再生本部（仮称）」を設け、ゼロベースからのガバナンス・組織風土改革に取り組む。

○規程等の事前調整のルール化、事務処理誤りの報告のルール化等、機構の業務執行のあり方を見直し、厚生労働省との情報共有を図る。

8. まとめ

○ フォレンジック調査を含むこれまでの調査等の結果、お客様の個人情報流出は、約125万件以外確認されていない。

○本事案について経緯を省みると、まず第１回目の攻撃があった５月８日(金)の時点での対応、情報流出の直接的要因となった５月１８日（月）からの対応について、もし現在までに検討されてきた対策がルール化・体系化され、それが誠実、忠実に実行されていたならば、情報流出の防止につながり、多くの年金受給者・加入者にご迷惑をおかけすることを回避することが可能であったと考えられる。特に、数次にわたる標的型メールを受信した際の対応・対策に多くの問題があったことは、率直に認めなくてはならない。

○また、共有ファイルサーバに個人情報を置けるようになっていたことは、今回の情報流出につながった極めて大きな問題であり、個人情報の重みに対する意識に欠けていたと言わざるを得ない。

○今後は、最も重要な個人情報を扱う基幹システムはもとより、個人情報のインターネット接続環境からの完全遮断を行うこと、情報セキュリティ対策の司令塔としての「情報管理対策本部（仮称）」の新設、多重防御体制の整備といった情報セキュリティ対策の強化に取り組む必要がある。

○ こうした問題の要因は、基本的な対応が担当者任せとなっており、責任の所在を明らかにしつつ、熟慮してルールを定め、定められたルールを誠実、忠実、厳格に実行するという対応が不十分であったこと、専門人材が配置されていないこと、共有ファイルサーバの管理についてのリスクの認識の甘さ、厚生労働省との情報共有体制の不備等の構造的要素が大きい。

○その根底には、ガバナンスの脆弱さ、組織としての一体感の不足、リーダーシップの不足、ルールの不徹底など、旧社会保険庁時代から指摘されてきた諸問題があり、また、厚生労働省が責任を担う公的年金制度の、最も大切な実際の執行部分を責任を持って請け負うという緊張感、責任感、使命感が共有されるに至っていなかった、という組織全体の基本姿勢に関わる問題がある。

○本事案を通じ、これら積年の問題の解消・解決が急務であることが改めて明らかになった。今後ゼロベースから組織全体を総点検し、ガバナンスや組織風土の抜本的な改革に向け、職員全員の力を結集していかなければならない。そのため、理事長をトップとする「日本年金機構再生本部（仮称）」を新たに設け、これらの問題を払拭するため、組織を挙げて、全力で取り組むこととする。

○理事長をはじめとした役員及び関係者の責任については、本調査結果や、厚生労働大臣の下に設置された「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」の検証結果等を踏まえ、機構に設置されている制裁審査委員会の審議を経て、厳正に対処することとする。

○今後とも、個人情報が流出した方々の基礎年金番号の変更、専用コールセンターにおける対応をはじめ、二次被害発生防止対策に全力を尽くす。

○今後は、厚生労働大臣の下に設置された検証委員会の検証結果や、政府全体の取組を踏まえ、年金事業管理部会へも説明責任を果たしつつ、国民からの信頼回復及び再発防止に向け、不動の決意を持って取り組む。

（参考１）「不正アクセスによる情報流出事案に関する調査委員会」について

○調査委員会は平成27年６月４日（木）に機構の内部委員会として設置

＜設置目的＞

①不正アクセスに対する機構の対応経過の検証・評価

②機構におけるこれまでの情報セキュリティ対策などの検証・評価

③調査結果から判明した原因に即した責任の所在と具体的な改善策・再発防止策の検討

＜委員会の構成＞

（委員長）　理事長

（委　員）　役職員５名（監事、事業企画部門担当理事、年金給付業務部門担当理事、
特命担当理事、監査部長）
外部委員１名（弁護士）

＜委員会の開催実績＞

○全７回開催

（平成27年６月８日(月)、12日(金)、19日(金)、７月６日(月)、23日(木)、30日(木)、８月18日(火)）

＜調査手法・体制＞

○調査は、関係者からのヒアリングと関係資料（メール、内部資料等）の検証を主として実施

○ヒアリングは、委員、事務局職員及び事務局が指定する調査員が実施

（調査対象者）

・職員、運用委託会社より、合計201名、のべ221回のヒアリング（面談又は電話）を実施

（調査対象期間）

・NISCが不審通信を検知した平成27年５月８日(金)から、本報告書作成時点まで

（参考2）5月8日からの一連の対応に関する検証・評価

○原因の徹底究明と再発防止を行うという観点から、事後的に判明した事実も含め、また、現在機構内でルール化されていない対策も含めて、情報流出を防ぐために実施すべきであったと考えられる対策項目が本事案についてどこまで実施できていたかを検討・評価する。

○具体的な対策項目と対応状況について、本事案の経緯を踏まえ、同様の標的型メール攻撃があった場合にどのように対応すべきかという観点から整理すると、以下のとおり。

※「○」は適切に実施。「△」は対応遅れ、部分的実施。「×」は対応の相当の遅れ、未対応。

＜標的型メールの受信に関し対応すべき項目＞

	対応すべき項目	メール① 5/8	メール② 5/18	メール③ 5/18 5/19	メール④ 5/19	メール⑤ 5/20
1	受信の確認	△	○	△	○	○
2	受信者の範囲の特定	×	○	△	○	○
3	開封・感染の確認、抜線（受信者ヒアリング）	△	×	×	○	×
4	送信元受信拒否設定	×	○	△	○	○
5	全職員への注意喚起	△	△	△	△	×
6	端末の回収、検体の確保	○	○	△	×	○
7	ウィルスの解析依頼	○	△	△	−	△
8	URLフィルタリング（不審URLへの通信の遮断）	○	×	×	−	×
9	ウィルスパターンファイル（ワクチン）の適用	○	○	○	−	○
10	メール送受信専用外部回線の遮断	×	×	×	×	×

※メール①～⑤は、送信元メールアドレスごとに受信日別で整理

＜不審通信に関し対応すべき項目＞

	対応すべき項目	不審通信① 5/8	不審通信② 5/22	不審通信③ 5/23
1	通信の確認	○	○	○
2	端末の特定、抜線	○	○	△
3	感染経路の特定（職員ヒアリング）	○	○	△
4	ログ確認による感染範囲の特定	○	○	○
5	URLフィルタリング（不審URLへの通信の遮断）	○	△	○
6	通信監視体制の強化	○	○	○
7	端末の回収、検体の確保	○	○	○
8	ウィルスの解析依頼	○	○	○
9	ウィルスパターンファイル（ワクチン）の適用	○	○	○
10	感染部署のインターネット遮断	×	○	○
11	インターネット全面遮断	×	×	×