日本年金機構
Japan Pension Service

Press Release

平成２７年８月２０日
（照会先）
経営企画部　部長　峯村　芳樹
経営企画グループ長　樋口　俊宏
（電話直通　０３－５３４４－１１０７）
法務・コンプライアンス部　部長　福原　元
小野　健一郎
（電話直通　０３－５３４４－１１１２）
経営企画部広報室
（電話直通　０３－５３４４－１１１０）

報道関係者　各位

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

日本年金機構への不正アクセスにより、お客様の個人情報が流出した件につきまして、当機構内に設置した「不正アクセスによる情報流出事案に関する調査委員会」における調査結果がまとまりましたので、公表します。

このたびの個人情報流出及びその後の当機構の一連の対応に関し、国民の皆様に多大なご心配とご迷惑をおかけしましたことをお詫び申し上げるとともに、今後、報告書記載の再発防止策の確実かつ速やかな実施に全力を尽くしてまいります。

○別添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
○別添２：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

以上

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	×	×	×

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

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

目　次

Ⅰ．はじめに

本年６月１日(月)に公表した当機構が保有する個人情報の流出事案に関し、国民の皆様方に多大なるご心配、ご不安をおかけしたことにつきましては、誠に申し訳なく、改めて心よりお詫びを申し上げます。

また、公表後、個人情報の流出に関するお客様からの問い合わせに対する説明誤りが発生したことにつきましても、重ねてお詫びを申し上げます。

本事案は、当機構のコンピュータシステムのうち、インターネット接続環境下にある機構ＬＡＮシステム（内部事務処理のための情報系ネットワークシステム）に対し、ウィルスメールに起因す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情報の一部が流出したものです。

当機構といたしましては、流出したお客様の個人情報が不正に利用されたり、お客様がなりすまし被害等にあわれることが万が一にもないよう、万全の対応をとるとともに、本事案の原因究明及び再発防止策の検討を速やかに実施すべく、本年６月４日(木)に「不正アクセスによる情報流出事案に関する調査委員会」(以下「当委員会」という。)を設置し、調査を進めてまいりました。

これまでの調査結果等は後述のとおりですが、本事案につきましては、現在も警察による捜査が続けられていることから、本報告に当たっては、捜査上及びセキュリティ上の影響にも配慮した上でとりまとめを行っておりますことを申し添えます。

Ⅱ．当委員会について

１．趣旨

当委員会は、不正アクセスに対する当機構の対応経過や当機構のこれまでの情報セキュリティ施策などの検証・評価、及び調査結果から判明した原因に即した責任の所在の把握と具体的な改善策・再発防止策の検討をその任務としています。

２．構成

当委員会は、委員長を当機構の理事長とし、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）と外部委員として弁護士１名を加えた構成としています。

また、当委員会の事務局は、当機構の法務･コンプライアンス部コンプライアンスグループ及び同部法務グループが担当しています。

３．開催実績

当委員会は、本年６月４日(木)に設置して以降、これまで７回開催しています（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)）。なお、議事は非公開としています。

４．調査手法・体制

当委員会における調査は、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しています。

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しています。

調査対象者及び調査対象期間は、以下のとおりです。

（調査対象者）

これまで、当委員会として、当機構の職員及び機構ＬＡＮシステム等の運用委託会社（以下単に「運用委託会社」という。）の職員201名からのべ221回のヒアリング（面談又は電話）を実施しています。

（調査対象期間）

当委員会では、内閣サイバーセキュリティセンター（以下「ＮＩＳＣ」という。）が当機構内からの不審通信を検知した本年５月８日(金)から、本報告書作成時点までを、調査対象期間としています。

上記のほか、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）を実施しています。

なお、これらの調査は、当機構が運用委託会社に依頼して実施しています。

Ⅲ．不正アクセスによる情報流出事案に関する調査について

１．事案の概要

（１）不正アクセスの概要

○今回のウィルスメールによる攻撃は、標的型メール攻撃と呼ばれるものでした。標的型メール攻撃は、特定の拠点の職員に対し、実在する職員の名前を騙ったり、業務内容に関係した内容を装ったりするなど、極めて巧妙な手口によりウィルスを感染させ、情報流出などの被害を与えることを目的とするサイバー攻撃です。

○５月８日(金)以降、当機構における標的型メール受信件数は合計で124通であり、その詳細は以下の表のとおりです（送信元のメールアドレスからシステムで抽出確認）。

＜表：受信メール一覧（送信元メールアドレスごとに受信日別で整理）＞

項番	受信日	受信件数	開封件数 (※1)	宛先
1	５月８日(金)	２通(※2)	１通	業務用メールアドレス
2	５月18日(月)	99通	３通	職員個人の業務用メールアドレス

3	5月18日(月) 5月19日(火)	19通	0通	職員個人の業務用メールアドレス
4	5月19日(火)	1通	0通	職員個人の業務用メールアドレス
5	5月20日(水)	3通(※3)	1通	業務用メールアドレス
合計		124通	5通	

(※1)標的型メールの添付ファイルを開封したり、リンク先のファイルをダウンロード・開封した件数。

(※2)受信したうちの1通は、メールの受信確認漏れの防止の観点から、職員10人に自動転送されるように職員が設定していました。

(※3)受信したうちの1通は職員10人に、別の1通は職員5人に、メールの受信確認漏れの防止の観点から、それぞれ自動転送されるように職員が設定していました。

○項番1及び2のメールは、送信元のメールアドレスが同じでした。

○標的型メールの件名は、当機構の職員が業務として連想しやすいものとなっていました。

○標的型メールの添付ファイル等を開封した当機構の職員は合計で5名いましたが、それぞれの利用端末の感染が確認されました。標的型メールに起因して感染した端末の合計は31台で、添付ファイル等を開封した職員の利用端末の一部から感染が広がったと考えられます。

○感染の結果、約125万件のお客様の個人情報が、5月21日(木)から23日(土)までの間に流出しました。(情報流出した端末のログ解析により判明。流出の概要は(2)で後述。)

○標的型メールの本文中の宛先について、5月8日(金)の項番1の2通のメールは、業務用メールアドレスの担当部署に実在する職員の苗字がそれぞれ記載されていました。また、5月18日(月)及び19日(火)に届いたメール(項番2、3及び4)については、職員個人の業務用メールアドレスあてに、職員氏名が具体的に記載されたものが送られていました。

一方で、差出人名についても、当機構に実在する職員氏名と一致しているケースも見受けられました。

(2)お客様の個人情報流出の概要

○このたびのウィルスメールに起因する不正アクセスにより、お客様の個人情報が約125万件(対象者は約101万人)流出しました。4情報(基礎年金番号、氏名、生年月日及び住所)、3情報(基礎年金番号、氏名及び生年月日)及び2情報(基礎年金番号及び氏名)の流出が確認された件数及びお客様の人数は、以下のとおりです。また、都道府県別の内訳は、別添資料1(個人情報が流出した方の内訳)のとおりです。

【流出件数(人数)の内訳】

・4情報の流出　　約　5.2万件(約1.5万人)

・3情報の流出　　約116.7万件(約96.9万人)

・２情報の流出　　約　3.1万件（約3.0万人）

○この約125万件のデータについては、当機構の端末から不審通信を行っていた外部のサーバに流出したことが、警察から提供された資料に基づいて判明しました。

○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ません。（フォレンジック調査等の結果については、２で後述。）

○なお、流出した約125万件のお客様の個人情報は複数の当機構の拠点で保有されていましたが、このうち約55万件のデータについてはパスワードが設定されていませんでした。

○基幹システム（年金業務に必要な被保険者及び年金受給者の資格記録や給付記録を管理するシステム）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ません。

【事案の経緯】

５月　８日(金)	ＮＩＳＣより厚生労働省政策統括官付情報政策担当参事官室（以下「情参室」という。）、厚生労働省年金局（以下「年金局」という。）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「新種ウィルスは、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。

2．フォレンジック調査等

本事案判明後、当機構においてフォレンジック調査及びセキュリティインシデント調査を、１通目の標的型メールが届いた本年５月８日(金)以降について、実施しました。その内容は以下のとおりです。

なお、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ありませんが、一定の調査結果が明らかになりました。

（１）調査方法

○まず、フォレンジック調査等を行うに当たり、プロキシサーバログの解析、メール送受信ログの解析を行いました。これにより、フォレンジック調査等を行う対象機器の特定を行いました。

○その後、フォレンジック調査等として、対象機器について、削除されたファイルの復元等の措置を講じ、ハードディスクに残された痕跡を見出し、送り込まれた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、解析しました。

（２）調査対象

○フォレンジック調査等は、プロキシサーバログの解析等を行い、対象機器として端末31台、認証サーバ（アクセス権等を管理しているサーバ）１台、共有ファイルサーバ１台について調査を行いました。

（３）調査で判明した事実

①お客様の個人情報

○フォレンジック調査等の結果、お客様の個人情報に関しては、現在判明している「約125万件」以外の新たな情報流出は確認されていません。

②その他判明した事実

（ア）５月８日(金)の不審通信

○これまで当機構では、５月８日(金)の標的型メールと疑われるメール攻撃において情報流出は確認されていないと説明してきました。しかしながら、調査の結果、５月８日(金)にメールソフトの職員個人の業務用メールアドレスの圧縮ファイルが生成されており、その一部が流出しているおそれがあることが判明しました。具体的な件数等の詳細は不明です。

（イ）５月20日(水)以降の感染及び情報生成・収集

○５月20日(水)に当機構の職員が標的型メールの添付ファイルを開封したことにより不正プログラムが実行され、不審通信が発生しました。その後、攻撃者は、複数の端末に侵入し、不正プログラムを送り込んだ上でそれを実行し、他の端末への感染を拡大し、お客様の個人情報以外の情報について、情

報収集、圧縮ファイルの生成等を行っていました。

○また、22日（金）には、攻撃者は認証サーバの管理者権限を窃取し、その権限を使用していました。

（ウ）お客様の個人情報以外の流出情報

○個人情報に関しては、当機構で管理する職員情報の一部（225名分）について圧縮ファイルが生成されており、情報流出しているおそれがあることが判明しました。

○個人情報以外に関しては、各拠点（事務センター、年金事務所）の職員配置状況などの当機構の組織関係情報、業務マニュアル関係（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）、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）について、圧縮ファイルが生成されており、情報流出しているおそれがあることが判明しました。

（4）攻撃者の操作

①5月8日(金)

○5月8日(金)の不審通信は、当機構の職員が標的型メールと疑われるメールのリンク先にあるファイルを開封したことがきっかけでしたが、この段階で、端末がまずバックドア型の不正プログラムに感染し、C&Cサーバと呼ばれる外部サイトと通信を始めました。その後、当該サイトから不正プログラムが持ち込まれ、当該端末に埋め込まれました。その後、C&Cサーバとの外部通信時に職員個人の業務用メールアドレスの一部を少量ずつ窃取されていた可能性があると考えられます。

②5月20日(水)及び21日(木)

○5月20日(水)以降の不審通信は、当機構の職員が標的型メールの添付ファイルを開封したことがきっかけでしたが、5月8日(金)と同様に端末がバックドア型の不正プログラムに感染し、C&Cサーバと呼ばれる外部サイトと通信を始めました。

3．当機構における事案対応に関する検証・評価

このたびの標的型メールによる攻撃者は、当機構に対し、1回にとどまることなく、複数回にわたるメール攻撃を仕掛けてきました。

当機構は、この複数回にわたる一連のメール攻撃に対し、それぞれの局面において、端末の抜線（ネットワークからの切り離し。以下同じ。）、全職員への注意喚起、ウィルスの解析、送信元メールアドレスの受信拒否設定、不審通信先ＵＲＬのフィルタリング、統合ネットワークを通じたインターネット接続の遮断などの対応を行ってきました。また、こうした対応過程の中で、ＮＩＳＣ、警察及び運用委託会社から不審通信の状況、検体の内容等に関する情報提供も受けました。

しかしながら、これらの対応にもかかわらず、結果として、一連のメール攻撃により、約125万件ものお客様の個人情報を流出させる事態となりました。

当委員会では、まず、攻撃の各局面における当機構の対応のどこに問題があったかについて検証しました。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・評価することとしました（後述（1））。

具体的な対策項目について、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、「標的型メールの受信に関し対応すべき項目」と、「不審通信に関し対応すべき項目」に分けてそれぞれ整理すると、具体的には以下のとおりです。

＜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＞

【Ⅰ　標的型メールの受信に関し対応すべき項目】

①メール受信の確認
②メール受信者の範囲の特定
③添付ファイルの開封・感染の確認、抜線（受信者ヒアリング）
※ここで添付ファイルの開封等を把握した場合は、下記Ⅱの手順も対応
④送信元メールアドレスの受信拒否設定
⑤全職員への注意喚起（添付ファイルを開封した場合の対処法なども記載）
⑥端末の回収、検体の確保
⑦ウィルスの解析依頼
⑧不審通信先ＵＲＬのフィルタリングの実施
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

【Ⅱ　不審通信に関し対応すべき項目】

①不審通信の確認
②端末の特定、抜線（情報セキュリティポリシーどおりの手順）
③感染経路の特定、不審通信を行っていた端末利用者からのヒアリング（不審メールの受信、添付ファイルの開封等の事実確認）
※ここで標的型メールの受信を把握した場合は、上記Ⅰの手順も対応
④プロキシサーバ等のログ確認による端末等の感染範囲の特定
⑤不審通信先ＵＲＬのフィルタリングの実施
⑥プロキシサーバ等への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不審通信を行っていた端末が所在する部署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

⑪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の遮断

※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必要。

また、当委員会では、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このたびの個人情報流出につながったと考えており、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しました（後述（２））。

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も検証しました（後述（３））。

（１）標的型メール攻撃の各局面における対応

○当委員会では、今回の複数回にわたるメール攻撃に際し、前記の＜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＞Ⅰ及びⅡの実施状況や、実施していなかった場合にはその理由について、関係者からヒアリングを行うとともに、仮に適切に実施された場合に、お客様の個人情報流出の防止に向けて改善できた可能性の有無について、検証を行いました。

○検証の結果は、以下①から⑨までのとおりです。加えて、当機構の対応状況の詳細については、別添資料２（５月８日からの一連の対応に関する検証・評価）に整理しました。なお、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)及び 22 日(金)・23 日(土)における対応が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ました。

①５月８日(金)・５月 15 日(金)の対応

(対応できたこと)

○５月８日(金)に関しては、情報セキュリティ担当部署に対し、情参室、年金局を通じてＮＩＳＣから不審通信の連絡がありました。当機構では、連絡受領後１時間以内に不審通信を行っていた端末（Ａ拠点に所在）を特定し、抜線しました。

○抜線後、当該端末の利用者からのヒアリング（５月８日(金)）により、当該者が不審メールのリンク先にあったファイルを開封していたことが判明し、不審通信がウィルス感染によるものとの疑いが強まりました。

○端末利用者からのヒアリングと並行して、情参室を通じてＮＩＳＣに対し、不審通信が止まったかどうかを確認するとともに、他の端末で同様の不審通信がないかどうかの確認を運用委託会社に依頼し、同様事象がないことを確認しました。その後、当日中に、不審通信先ＵＲＬのフィルタリングを運用委託会社

に指示し、実施しました。

○抜線した端末からウィルスの検体を確保し、当日中に運用委託会社に解析を依頼しました。その後、5月12日(火)に、当該不審通信の原因となったウィルスのパターンファイル（ワクチン）を適用しました。

○不審通信の原因が特定できておらず、再度同様の不審通信が発生する可能性も考えられたことから、当日中に運用委託会社にプロキシサーバ等への通信監視体制の強化を指示しました。

○理事長及び副理事長には、ＮＩＳＣから不審通信の連絡があったこと、及び抜線した結果、不審通信が止まったことなどの対応状況の概要について、当日中にそれぞれ報告がありました（詳細報告は5月11日(月)）。

(対応が不十分又はできなかったこと)

○5月8日(金)には不審メールが合計2通届いていましたが、情報セキュリティ担当部署では、不審通信が確認された端末以外にメールを受信した者がいないかどうかの確認についてルール（手順）がなかったため、もう1通のメール受信者への個別確認を行いませんでした。なお、確認できた1通のメール受信・開封の事実についても、ＮＩＳＣから不審通信を指摘されるまで把握できませんでした。

○2通とも業務用メールアドレスあてに送られていたことから、仮にこの段階で送信元メールアドレスから他の職員に不審メールが送付されているかどうかを確認していれば、業務用メールアドレスが狙われている旨の注意喚起を実施できたと考えられます(5月20日(水)に職員が添付ファイルを開封したメールは業務用メールアドレスで受信)。

※結果的に受信未確認の1通については、当該メールの添付ファイル等は開封されておらず、感染は確認されていません。

○情報セキュリティ担当部署において、「同じメールアドレスからの再攻撃の可能性は低い」と判断し、また、ルール（判断者、判断基準）が定まっていなかったことから、送信元メールアドレスの受信拒否設定を行いませんでした。

○仮にこの段階で受信拒否設定を行っていれば、5月18日(月)の標的型メール（2ページの表の項番2のメール)は届かなかったことも考えられます。また、フォレンジック調査等の結果により、同月8日（金）の不審通信時に職員個人の業務用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ました。仮にこの段階で当機構全体として受信拒否設定を行っていれば、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と考えられます。

○メール等により当機構全職員への注意喚起を当日中に実施しましたが、内容は不審メールの削除指示だけとなっており、添付ファイルを開封した場合の具体的対処法や万が一に開封した場合の連絡先などは記載していませんでした。(別添資料3－1（注意喚起メール①）参照)

○インターネット接続の遮断については、情報セキュリティ担当部署において、

統合ネットワークを通じたインターネット接続やメール送受信専用外部回線の遮断を検討していましたが、外部とのメールのやりとりができなくなるなど当機構の業務への影響(※)が非常に大きいことから、リスクを見極めその可否について決定することは難しい判断でした。こうした判断を適切に行うためには、どのような事態の場合に遮断を行うのか、あらかじめ検討の上、当機構全体としてのルール（判断者、判断基準）を定めておくことが必要ですが、これを定めていませんでした。

(※)影響の出る業務例

＜インターネットの使用制限により影響が生じる業務＞

・インターネット情報の閲覧（例：厚生年金保険徴収事務における滞納事業所ホームページ、厚生年金保険未適用対策における適用調査対象事業所のホームページ等の閲覧）

・インターネット公売　　など

＜インターネットメールの使用制限により影響が生じる業務＞

・厚生労働省や厚生局との連絡・調整（例：国民年金の強制徴収の認可申請）

・委託業者への連絡（例：納付書の引抜き依頼）　　など

○インターネット遮断のルール（判断者、判断基準）が定まっていなかったことから、統合ネットワークを通じたインターネット接続の一部又は全部の遮断については、実施しませんでした。また、メール送受信専用外部回線の遮断についても、同様に実施しませんでした。

○５月８日(金)のメールについて、情報セキュリティ担当部署の担当者は、標的型メール攻撃ではないかとの疑いを持っていましたが、その疑いは組織としては共有されませんでした。具体的には、担当者は標的型メール攻撃の疑いを持ち、当機構全職員への注意喚起メールにも標的型メールの特徴を参考として記載しました。担当部長はその注意喚起メールの発出を決裁していましたが、標的型メールであった場合の対応について検討を指示せず、ＣＩＯ（システム部門担当理事）も注意喚起メールの発出をｃｃで受け取りながら、具体的な指示は行いませんでした。もし、標的型メール攻撃であることが組織として共有されていれば、情報セキュリティ担当部署やその他の関係部署、運用委託会社間において、この対応結果から得られた教訓・反省点などをまとめ、「to doリスト」などで課題を共有し、最終的には手順書としてルール化し、関係部署内で共有することも可能であったと考えられます。

○その後、５月 15 日(金)、運用委託会社から「新種ウィルスは外部に情報を漏洩するタイプではない」との解析結果を入手したことに伴い、一旦収束したと判断しましたが、フォレンジック調査等の結果を踏まえると、ウィルス感染後の危険性に対する判断として適切ではありませんでした。

なお、前述の２（４）①のとおり、５月８日（金）に端末がバックドア型の不正プログラムに感染し、Ｃ＆Ｃサーバから不正プログラムが持ち込まれましたが、感染した端末のごみ箱から同月 13 日(水)に、不審メールのリンク先にあっ

たと思われるファイルを運用委託会社が発見し、解析を始めました。その解析結果については、同月 24 日(日)に運用委託会社より、「情報を盗む動作は行われていない」旨の回答を受領しました（ウィルスのパターンファイル（ワクチン）は６月２日(火)に適用)。

②５月 18 日(月)の標的型メール（２ページの表の項番２のメール）の受信に関する対応

(対応できたこと)

○５月８日(金)の対応は不審通信の連絡から始まりましたが、同月 18 日(月)から 20 日(水)までの対応は当機構の複数職員からの不審メール受信の連絡から始まりました。

○不審メール受信の連絡があった際、情報セキュリティ担当部署では、他にメールを受信している者がいないかどうかの確認を当日中に運用委託会社に依頼し、同日中にメール受信者を確認しました。

○ウィルスの検体を確保し、当日中に運用委託会社に解析を依頼しました。その後、５月 22 日(金)に、不審メールの添付ファイルから検出されたウィルスのパターンファイル（ワクチン）を適用しました。

○不審メールの送信元のメールアドレスについて、当日中に運用委託会社に受信拒否設定を指示し、実施しました。

○理事長及び副理事長には、大量の不審メールが届いていること及び対応状況の概要について、当日中に報告がありました。その際、理事長及び副理事長から警察に相談するよう指示があったことから、翌日、情報セキュリティ担当部署等が管轄の警察署に相談しました。

(対応が不十分又はできなかったこと)

○情報セキュリティ担当部署では、不審メール受信の連絡があった際、個別に添付ファイルの開封などをしていないかどうかを確認していましたが、連絡がない場合には、「メール受信者への個別確認をすると、不審メールの添付ファイルを興味本位や操作ミスで開封してしまうリスクが高まる。また、本人が開封したことを自覚していないこともあるので、聴取りをしても確実な確認はできない」と判断し、メール受信者全員に個別に連絡をして添付ファイル開封の有無を確認しませんでした。また、メール受信者に対する確認事項が明示的に定まっておらず、確認した際の事蹟も書面で残さないなど、ルール（手順）が定まっていなかったこともあり、適切な対応ができていませんでした。

○５月 18 日(月)には、全国で３名の当機構の職員が不審メールの添付ファイルを開封し、端末が感染しましたが、上記のとおり、具体的な確認を行わなかった結果、情報セキュリティ担当部署では、その事実を把握していませんでした。なお、この感染による情報流出は確認されていません。

○このことから、添付ファイル開封の有無・端末の感染を把握し、速やかに端末

を抜線するとともに、端末の解析を行って不審通信先（C＆Cサーバ）を特定することにより不審通信先ＵＲＬのフィルタリングを実施するなどの対応が遅れました。

○メール等により当機構全職員への注意喚起を当日中に実施しましたが、内容は不審メールの削除指示だけとなっており、添付ファイルを開封した場合の具体的対処法や連絡先などは記載していませんでした。

（別添資料３－２（注意喚起メール②）参照）

○ウィルスの検体を確保しましたが、情参室への登録（ＮＩＳＣへの提供）については翌日となりました。これは、情報セキュリティ担当部署において、ＮＩＳＣへの提出は単なる情報提供であると誤認し、緊急性があるものではないと考えていたことによるものでした。

○不審メールの受信を受け、５月８日(金)の攻撃との関連や対処方針の検討などについて、情報セキュリティ担当部署や関係部署、運用委託会社間において十分な議論・検証がなされておらず、また、インターネット遮断のルール（判断者、判断基準）が定まっていなかったことから、統合ネットワークを通じたインターネット接続の一部又は全部の遮断については、実施しませんでした。メール送受信専用外部回線の遮断についても実施しませんでした。

○これまでにない大量の不審メールが届いたにもかかわらず、管理職以上のレベルでの厚生労働省への連絡を行いませんでした。

③５月 18 日(月)～19 日(火)の標的型メール（３ページの表の項番３のメール）の受信に関する対応

(対応が不十分又はできなかったこと)

○５月 18 日(月)の不審メール（２ページの表の項番２のメール）の受信拒否設定を行った同日に、当機構の職員から新たな別のメールが届いた旨の連絡がありました。

○情報セキュリティ担当部署は、不審メール受信の連絡があった際、個別に添付ファイルの開封などをしていないかどうかを確認していましたが、連絡がない場合には個別に連絡をして確認することをしませんでした。

また、メール受信者に対する確認事項が明示的に定まっておらず、確認した際の事蹟も書面で残さないなど、ルール（手順）が定まっていなかったこともあり、適切な対応ができませんでした。

○不審メール受信の連絡があった際、他にメールを受信している者がいないかどうかの確認を運用委託会社に依頼していましたが、翌日の依頼となっていました。これは、不審メール受信の連絡が情報セキュリティ担当部署あてにメールされていたものの、担当者が離席中で確認が遅れ、運用委託会社との契約担当部署（以下単に「契約担当部署」という。）の担当者に当日中に連絡することができなかったことによるものでした。対応が担当者の個人ベースで行われ、担当者不在の際のルール（判断者、判断基準）が定まっていませんでした。

○同様に、ウィルスの検体を確保し、運用委託会社に解析を依頼するとともに、情参室に登録（ＮＩＳＣに提供）していましたが、依頼・登録がともに翌日となっていました（その後、５月26日(火)に、不審メールの添付ファイルから検出されたウィルスのパターンファイル（ワクチン）を適用しました)。

○不審メールの送信元のメールアドレスについて、運用委託会社に受信拒否設定を指示していましたが、指示・実施がともに翌日となっていました。

○機構ＬＡＮの職員用電子掲示板のテロップ表示により当機構全職員への注意喚起を実施していましたが、３ページの表の項番４のメールとあわせて翌日の実施となっていました。

○これらの対応がいずれも翌日となっていたことは、対応のルール（判断者、判断基準）がなかったことによるものですが、危機感が十分ではありませんでした。

○不審メールの受信を受け、５月８日(金)の攻撃との関連や対処方針の検討などについて、情報セキュリティ担当部署その他の関係部署、運用委託会社間において十分な議論・検証がなされておらず、また、ルール（判断者、判断基準）が定まっていなかったことから、統合ネットワークを通じたインターネット接続の一部又は全部の遮断については、実施しませんでした。メール送受信専用外部回線の遮断についても実施しませんでした。

○理事長及び副理事長には報告がされておらず、組織全体としての情報共有が図られていませんでした。また、管理職以上のレベルでの厚生労働省への連絡を行いませんでした。

④５月19日(火)の標的型メールの受信に関する対応

（対応できたこと）

○５月18日(月)に引き続き、当機構の職員から不審メールを受信した旨の連絡がありました。

○情報セキュリティ担当部署では、不審メール受信の連絡があった際、個別に添付ファイルの開封などをしていないかどうかを当日中に確認していました。

○不審メール受信の連絡があった際、他にメールを受信している者がいないかどうかの確認を当日中に運用委託会社に依頼し、同日中にメール受信者が他にいないことを確認しました。

○不審メールの送信元のメールアドレスについて、当日中に運用委託会社に受信拒否設定を指示し、実施しました。

（対応が不十分又はできなかったこと）

○機構ＬＡＮの職員用電子掲示板のテロップ表示により当機構全職員への注意喚起を実施していましたが、内容は不審メールの削除指示だけとなっており、添付ファイルを開封した場合の具体的対処法や連絡先などは記載していませんでした。

○不審メールがすでにメール受信者により削除されていたことから、検体が確保できず、ウィルス解析やパターンファイル（ワクチン）の適用ができませんでした。

○不審メールの受信を受け、５月８日(金)の攻撃との関連や対処方針の検討などについて、十分な議論・検証がなされておらず、また、ルール（判断者、判断基準）が定まっていなかったことから、統合ネットワークを通じたインターネット接続の一部又は全部の遮断については、実施しませんでした。メール送受信専用外部回線の遮断についても実施しませんでした。

○理事長及び副理事長には報告がされておらず、組織全体としての情報共有が図られていませんでした。

⑤５月 20 日(水)の標的型メールの受信に関する対応

(対応できたこと)

○５月 19 日(火)に引き続き、当機構の職員から不審メールを受信した旨の連絡がありました。

○不審メール受信の連絡があった際、情報セキュリティ担当部署では、他にメールを受信している者がいないかどうかの確認を当日中に運用委託会社に依頼し、同日中にメール受信者を確認しました。

○ウィルスの検体を確保し、当日中に運用委託会社に解析を依頼しました。その後、５月 27 日(水)に、不審メールの添付ファイルから検出されたウィルスのパターンファイル（ワクチン）を適用しました。

○不審メールの送信元のメールアドレスについて、当日中に運用委託会社に受信拒否設定を指示し、実施しました。

(対応が不十分又はできなかったこと)

○５月 20 日(水)には、Ｂ拠点の１名の職員が不審メールの添付ファイルを開封し、端末が感染しました。Ｂ拠点から情報セキュリティ担当部署にメール受信の連絡は入っていましたが、その後、情報セキュリティ担当部署では、どのようなファイルが添付され、開封・クリックしたかどうかなど、具体的に一つ一つの確認事項を明確に特定した聴取りを行わず、同日中に添付ファイル開封の有無を確認できませんでした。また、連絡がないメール受信者への個別確認をしていませんでした。

○このことから、添付ファイルの開封・端末の感染を把握し、速やかに端末を抜線するとともに、端末の解析を行って不審通信先（Ｃ＆Ｃサーバ）を特定することにより不審通信先ＵＲＬのフィルタリングを実施するなどの対応が遅れ、感染が拡大しました。

○また、フォレンジック調査等の結果により、感染した５月 20 日(水)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ました。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していれば、上記の対

応を遅れずに実施できた可能性がありました。また、同様の不審通信を行っている端末を特定し、複数台の端末の感染が確認されれば、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りました。

○５月 21 日(木)には、Ｂ拠点からＡ拠点（同月８日(金)の感染部署）に感染したことが判明しました。同月８日(金)に感染したＡ拠点の端末については、回収・交換されていましたが、端末番号やＩＰアドレスは変更しませんでした。このことから、Ｂ拠点の感染端末を通じ、Ａ拠点に感染が拡大していたと考えられます。

○ウィルスの検体を確保しましたが、情参室への登録（ＮＩＳＣへの提供）が翌日となりました。

○メール等により当機構全職員への注意喚起については、すでに 18 日に一般的な注意喚起を実施済みであったことから、再周知は不要と情報セキュリティ担当部署で判断し、実施しませんでした(後日、５月 25 日(月)に注意喚起を実施(別添資料３－３（注意喚起メール③）参照))。

○不審メールの受信を受け、５月８日(金)の攻撃との関連や対処方針の検討などについて、情報セキュリティ担当部署その他の関係部署、運用委託会社間において十分な議論・検証がなされておらず、また、ルール（判断者、判断基準）が定まっていなかったことから、統合ネットワークを通じたインターネット接続の一部又は全部の遮断については、実施しませんでした。メール送受信専用外部回線の遮断についても実施しませんでした。

○理事長及び副理事長には報告がされておらず、組織全体としての情報共有が図られていませんでした。

⑥５月 21 日(木)のＮＩＳＣからの標的型メールの解析結果受領後の対応

(対応ができなかったこと)

○情参室を通じてＮＩＳＣから、５月 18 日(月)の２通のメール（２ページの表の項番２及び３ページの表の項番３のメール）及び５月 20 日(水)のメール（３ページの表の項番５のメール）についての解析結果を受領しました。解析結果については、当日中に情報セキュリティ担当部署から契約担当部署にメールで展開されましたが、契約担当部署の担当者が不在であったため、運用委託会社への提供が翌日となっていました。このことは、前述のとおり、対応が担当者任せとなっていることを示すものです。また、理事長及び副理事長には報告がされておらず、組織全体としての情報共有が図られていませんでした。

○ＮＩＳＣからの解析結果には不審メールの添付ファイル等を開封した場合の不審通信先のＵＲＬの記載があったことから、情報セキュリティ担当部署において、当該ＵＲＬへの通信記録の有無を確認するとともに、当該ＵＲＬのフィルタリングや通信監視体制の強化をすることが可能でした。しかし、その時点では添付ファイルの開封が確認されていなかったため、情報セキュリティ担当部

署において解析結果の内容を十分に咀嚼することができず、これらの対策については結果的に実施しませんでした。また、フィルタリング等のルール（判断者、判断基準）についても、定められていませんでした。

○インターネット接続の遮断のルール（判断者、判断基準）が定まっていなかったことから、解析結果の受領後、統合ネットワークを通じたインターネット接続の遮断やメール送受信専用外部回線の遮断については、実施しませんでした。

○ＮＩＳＣの解析結果を手がかりとして、仮にこの段階で不審通信先ＵＲＬについて情報セキュリティ担当部署がフィルタリングを実施し、また、複数台の端末からの不審通信・感染が確認されれば、当該ＵＲＬへの不審通信を行っている端末を速やかに抜線するとともに、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し、以降の情報流出が防止できた可能性がありました。

⑦５月 22 日(金)の不審通信に関する対応

（対応できたこと）

○５月 22 日(金)の不審通信については、５月８日(月)と同様、情参室を通じてＮＩＳＣから不審通信の連絡を受けた後、１時間以内に当該不審通信を行っていたＡ拠点内の端末を特定し、抜線しました。

○抜線後、情参室を通じてＮＩＳＣに対し、不審通信が止まったかどうかを確認するとともに、他の端末で同様の不審通信がないかどうかの確認を運用委託会社に依頼したところ、同社においてＡ拠点内の別の端末からの不審通信を検知したことから、当該端末も速やかに抜線しました。その後、他の端末で同様の不審通信がないことを運用委託会社に確認しました。

○抜線した端末からウィルスの検体を確保し、当日中に運用委託会社に解析を依頼しました。その後、５月 26 日(火)から順次当該不審通信の原因となったウィルスのパターンファイル（ワクチン）を適用しました。

○不審通信の原因が特定できておらず、再度同様の不審通信が発生する可能性も考えられたことから、当日中に運用委託会社にプロキシサーバ等への通信監視体制の強化を指示しました。

○同じＡ拠点内で複数の端末の不審通信が確認されたことから、当日中にＡ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しました。

※Ａ拠点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については、情報セキュリティ担当部署において、複数台の端末の感染が確認された場合には、該当拠点のインターネット遮断を行うべきとの議論が行われていたことにより、この対応に結びつきましたが、これが対応ルールとして定められたのは５月 25 日(月)になってからでした。

（対応が不十分又はできなかったこと）

○不審通信先ＵＲＬのフィルタリングを運用委託会社に指示していましたが、当日中にＡ拠点内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して

おり、緊急的に対応が必要との認識がなかったことから、指示・実施がともに5月25日(月)となりました。

○当機構の一連の対応について、不審通信を把握してからの対応に関しては、想定される対応はおおむね実施していましたが、インターネット遮断のルール(判断者、判断基準)が定まっていなかったことから、当機構全体のインターネット接続の遮断については実施しませんでした。仮にこの段階で5月22日(金)中に当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、以降の情報流出は防ぐことができていました。このため、A拠点だけの遮断ではこの時点においてすでに不十分な対応でした。

○このインターネット接続の遮断については、5月24日(日)になってからメールで理事長、副理事長に報告されました。

⑧5月23日(土)の不審通信に関する対応

(対応できたこと)

○5月23日(土)の不審通信については、運用委託会社の監視により検知されました。運用委託会社から不審通信の連絡を受けた後、当該不審通信を行っていた2台の端末(B拠点に所在)を特定し、抜線しました。

○抜線後、不審通信が止まったかどうか、また、他の端末で同様の不審通信がないかどうかを運用委託会社に確認したところ、B拠点内の別の17台の端末が不審通信をしていたことが判明したことから、不審通信先URLのフィルタリングを運用委託会社に指示・実施するとともに、当日中に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しました。

○抜線した端末からウィルスの検体を確保し、当日中に運用委託会社に解析を依頼しました。その後、5月28日(木)から順次、当該不審通信の原因となったウィルスのパターンファイル(ワクチン)を適用しました。

○不審通信の原因が特定できておらず、再度同様の不審通信が発生する可能性も考えられたことから、当日中に運用委託会社にプロキシサーバ等への通信監視体制の強化を指示しました。

(対応が不十分又はできなかったこと)

○運用委託会社が不審通信を検知した17台の端末についての抜線は、契約担当部署において、当日中にB拠点内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っており、対応が必要との認識がなかったことから、5月25日(月)に理事長の指示を受けてから実施しました。

○不審通信を行っていた端末利用者へのヒアリングについては、当日が営業日ではなかったことから、5月25日(月)に実施しました。

○当機構の一連の対応について、不審通信を把握してからの対応に関しては、想定される対応はおおむね実施していました。この対応により、情報流出が止まったことは事後的に確認されてはいますが、他拠点への感染が拡大していたリ

スクを考え、本来、5月23日(土)の時点で当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するべきでした。B拠点だけの遮断ではこの時点においてすでに不十分な対応でした。結果的に、A拠点及びB拠点以外における感染は確認されていません。

○このインターネット接続の遮断については、5月24日(日)になってからメールで理事長、副理事長に報告されました。

⑨5月28日(木)の警察からの情報流出疑いの一報を受けた後の対応

(対応できたこと)

○5月28日(木)に警察から情報流出の疑いの一報を受け、当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維持すべきかについて、理事長を含めた幹部及び情報セキュリティ担当部署その他の関係部署において議論がなされました。

○最終的には、5月29日(金)、メール送受信専用外部回線は遮断せずに残し、当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することとしました。

(対応が不十分又はできなかったこと)

○幹部及び情報セキュリティ担当部署その他の関係部署は、これまでの標的型メール攻撃による不審通信が統合ネットワークを通じたインターネット接続から特定サイトへの通信であったことから、今後、メール送受信専用外部回線が利用される可能性はかなり低いと考えていました。
また、メール送受信専用外部回線を利用停止とした際の業務影響が大きいと考えたことから、最終的には、メール送受信専用外部回線は遮断せずに残すこととしました。

○その後、6月4日(木)には、メール送受信専用外部回線も遮断しましたが、これは、外部への感染拡大の危惧と、ウィルスメールの再侵入、メール送受信専用外部回線の利用による更なる情報流出などを防止する観点から、理事長の判断で遮断に踏み切ったものでした。しかし、本来であれば、5月29日(金)の時点で、当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の遮断と同時に実施すべきでした。

＜標的型メール攻撃に対し対応ができなかった構造的要因＞

○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程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（判断者、判断基準、手順）は定められていませんでした。

○標的型メールに対し十分な対応ができなかった要因としては、当機構における次のような構造的な問題があったものと考えられます。

・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ましたが、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ません。
・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ませんでした。
・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職員が配置されていませんでした。
・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ました。

（２）ＬＡＮシステムにおける共有ファイルサーバの取扱い

（別添資料４（日本年金機構のシステムイメージ）参照）

○このたび流出したお客様の個人情報については、当機構の基幹システムから機構ＬＡＮシステムに移行され、機構ＬＡＮシステムにおける共有ファイルサーバに保存されていました。この機構ＬＡＮシステムについては、当時の旧社会保険庁ＬＡＮシステム（第１期は平成15年に構築）を引き継いだ形で平成22年１月から運用を開始したものです。

○機構ＬＡＮシステムにおける共有ファイルサーバの取扱いについては、平成22年９月以降、順次、文書管理担当部署が運用ルールを定めてきました。具体的には、共有ファイルサーバには個人情報など情報漏洩対策を必要とする情報は保管しないことを原則とした上で、業務上必要なデータについては、パスワードやアクセス制限の設定など情報セキュリティ対策を講ずることを前提として取り扱うことを可能としていました。また、業務目的を果たした後は、速やかに個人情報を削除することとしていました。

○こうした共有ファイルサーバの運用ルールについては、基本的に本部各部署及び各拠点においてその徹底を図るよう指示してきましたが、平成25年度以降は、本部各部署及び各拠点に対し、共有ファイルサーバの管理状況について文書管理担当部署への報告を求めていました。その後、これらの運用ルールについては、本年３月に改めて「日本年金機構共有フォルダ運用要領」として要領化しました。

○基幹システムから機構ＬＡＮシステムにおける共有ファイルサーバに個人情報を移行する際の業務の取扱いについては、具体的には以下のとおりです。

【本部においてデータ抽出する場合】

・本部においてデータ抽出する場合としては、制度改正に応じた相談対応や記録補正等の業務を各拠点に実施させるため、当該業務に必要な範囲内で個人情報を基幹システムから媒体（ＤＶＤ等）を介して抽出し、必要に応じて加工の上、共有ファイルサーバに移行し、当該業務に活用しています。
・なお、個人情報が基幹システムから抽出され、媒体を介する際には、情報セキ

ュリティ対策として、システム上自動的にパスワードが付される仕組みとなっています。

・また、データ移行後に移行に用いた媒体（ＤＶＤ等）を廃棄するとともに、当該業務終了後には個人情報（データ）を共有ファイルサーバから削除するルールとなっています。

【各拠点においてデータ抽出する場合】

・各拠点においてデータ抽出する場合としては、日本年金機構中期計画等において当機構の事業運営における最重要課題の一つとして位置付けた国民年金の収納対策関連業務があります。

・具体的には、お客様の状況に応じて個別に納付勧奨等を実施するため、本部において当該業務に必要な情報の範囲をあらかじめ設定し、各拠点においてその設定された範囲内で必要な個人情報を基幹システムのサブシステムから媒体（ＤＶＤ等）を介して抽出の上、共有ファイルサーバに移行し、当該業務に活用しています。

・なお、個人情報を共有ファイルサーバに保存する際には、情報セキュリティ対策として、システム上自動的にパスワードが付される仕組みとなっています。

・また、データ移行後、移行に用いた媒体（ＤＶＤ等）は廃棄するとともに、当該業務終了後には当該個人情報（データ）を共有ファイルサーバから削除するルールとなっています。

○こうした運用ルールの下、共有ファイルサーバは運用することとされてきましたが、本事案において流出したお客様の個人情報の一部には、パスワードもアクセス制限も設定されていないものがありました。また、個人情報が流出した拠点では、業務目的を果たした後も、個人情報を削除せずにそのまま共有ファイルサーバに保管を続けているケースがありました。

さらに、定期点検において、個人情報が流出した拠点からは、「共有ファイルサーバの整理及び個人情報のパスワード設定等については本年４月末までにすべて対応済」との報告がされていましたが、当該拠点のいくつかの拠点では、確認が十分されないまま報告されていました。

※情報流出した約 125 万件の個人情報に関するセキュリティ対策（パスワード又はアクセス制限の設定）の実施状況は、パスワード及びアクセス制限の設定を行っているもの約 68 万件、パスワード設定のみ行っているもの約 2 万件、アクセス制限のみ行っているもの約 53 万件及びセキュリティ対策無しのもの約 2 万件となっていました。

○文書管理担当部署は、共有ファイルサーバの運用ルールを決定し、それに基づき管理をしていましたが、インターネット接続環境の中に個人情報を保有するリスクを十分認識しておらず、それがルールの徹底ができなかった要因の１つとなりました。

○このように、運用ルールが定められていたにもかかわらず、本部各部署及び各拠点においてその徹底が図られていませんでした。

○また、本事案のような外部からの不正アクセスに対しては、パスワード設定は一定の効果があるものの、アクセス制限は十分な情報セキュリティ対策ではなかったと考えられます。これまでの共有ファイルサーバの運用ルールについては、当機構内部からの情報窃取の防止に重点を置いたものでした。

○したがって、本事案を踏まえると、個人情報等の重要情報を含むファイルについては、共有ファイルサーバの使用を含めてルールの徹底を改めて図るとともに、外部からの不正アクセスに対してはルールによる対処だけでは必ずしも有効ではないことを認識し、今後はルールによって守るだけではなく、インターネット接続環境から遮断することによって不正アクセスから守るべきであると考えています。

○ 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、対策を検討してきませんでした。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ありませんでした。

○なお、共有ファイルサーバが実際にどのように運用され、運用ルールが徹底されていたかどうか、また、共有ファイルサーバに保存されているファイルにどのような個人情報が含まれていたかについては、現在、調査を行っています。

＜適切な対応が行われなかった構造的要因＞

○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、次のような構造的な問題があったものと考えられます。

・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・確認が適切に行われておらず、運用ルール自体が有名無実化していた。

（３）端末利用におけるインシデント対応の問題点

○Ⅲ１（１）に記載のとおり、標的型メールの手口は巧妙でしたが、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、結果的に５名の職員が標的型メールの添付ファイル等を開封していました。また、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ませんでした。標的型メール受信者が添付ファイル等を開封することは完全には防ぎきれないと考えられますが、これまでの職員研修等では危機意識や、万一開封してしまった際に対応するノウハウが職員に徹底されていませんでした。

○当機構では、通常、インターネットは一定の閲覧規制がかかっていますが、添付ファイル等を開封した職員は、業務上の理由で閲覧規制が解除されており、標的型メールのリンク先にアクセスできる状態となっていました。インターネットの閲覧規制の解除を申請し、受理された者に対し、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ありませんでした。

○外部への不審通信が確認された端末の一部には業務終了後に電源が切られていない状態となっていたものもあり、当該端末からは大量の不審通信が確認されました。業務終了時には端末の電源は落とすルールとなっており、毎月の職員の自主点検のチェック項目にもなっていますが、結果的に徹底されていませんでした。

○（1）でも述べたとおり、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ませんでした。

○こうした点についても、（2）の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処方針の策定が行われておらず、役員もリスクの認識が欠けていました。

4．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あるとの疑いを持っていましたが、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は共有されませんでした。また、同月15日(金)のウィルス解析結果で一旦収束したと判断したことにより、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ませんでした。

情報流出の直接的な要因は、5月18日(月)から23日(土)までの一連の対応において、標的型メールの受信に関する対策については、抜線以外に具体的なルール（判断者、判断基準）の定めがなく、開封・感染の確認、ＵＲＬフィルタリングなどの対策を講じなかったことにあります。特に、Ｂ拠点が感染した20日(水)の対応が最大のポイントでした。お客様の個人情報は、21日（木）から23日(土)までにＢ拠点から流出しており、20日(水)の時点で感染が確認できていれば、開封・感染の確認、ＵＲＬフィルタリングなど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りました。

「不審通信に関し対応すべき項目」(端末の特定・抜線、ログ確認による感染範囲の特定、不審通信先ＵＲＬのフィルタリング、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りました。しかし、そもそも上記のような「標的型メールの受信に関し対応すべき項目」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りませんでした。

初動対応の遅れを招いた背景には、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があります。

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、そのことがこのたびの情報流出の極めて大きな原因となったと言えます。

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ません。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ません。

・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の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

当機構の最高意思決定機関は理事会ですが、このような重要な事案を事案発生後の直近の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ました。

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りました。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、改めて基本姿勢を正すための組織全体の改革に取り組まなくてはなりません。

Ⅳ．不正アクセスによる情報流出事案におけるお客様への対応状況について

１．これまでの対応等

当機構では、本事案により、お客様に大変なご迷惑をおかけしており、当機構としてできる限りの対応を行っています。（別添資料５（お客様への対応状況）参照）

まず、個人情報が流出した約125万件（約101万人）の方への対応として、６月中にお詫びの文書を送付するとともに、５月８日(金)から６月１日(月)までに住所変更・金融機関変更の手続を行った方に対しては、訪問等により本人確認を行い、なりすましがなかったことを確認しました。

また、約125万件以外の方で、５月８日(金)から６月１日(月)までに住所変更・金融機関変更の手続を行った方に対しても、お手紙又は訪問により本人確認を行っています。

このほか、お客様の不安や不信を解消するため、本事案に関する専用電話を６月１日(月)から開設するとともに、土日も含め、８時30分から21時まで運用し、年金事務所の窓口も当面、土日も開所し、ご相談に応じる体制を確保しています。

さらに、２次被害を防ぐべく、年金事務所はもとより多くの公的機関にチラシを設置していただき、注意喚起を行っています。

【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～：現在は約1000人体制で受電件数に合わせて対応中。）

○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手続の実施（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・都道府県警察、市町村等と連携）

今後、個人情報が流出したお客様に対しては、順次、基礎年金番号の変更を行い、お知らせと年金手帳等を郵送する予定です。

当機構といたしましては、これからもお客様の二次被害発生防止のための取組を継続していくことが極めて重要であると考えており、引き続き、国民の皆様の年金を守るため、必要な取組に全力で取り組んでまいります。

※情報流出事案に要した費用

上記の対応にこれまで費用は合計約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4億円です。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ます。（8月20日(木)現在）

2．個人情報流出に関するお客様からの問い合わせに対する説明誤り

これまで、個人情報流出の対象となったお客様への対応を最優先で進めてきましたが、その中で、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しました。

説明誤りのあったお客様（2,449名）に対しては、6月27日(土)から、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ましたが、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ていませんでした。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ません。

また、この結果、国会やメディアへの説明責任を十分に果たせませんでした。

説明誤りの原因は、以下の２点にあることが判明しています。

①「該当表示（アラート表示）」の付加誤り：2,426 名

・窓口装置（お客様からの相談に応じる際に用いている端末）に流出した基礎年金番号であることを示す表示（アラート表示）を付加し、個人情報流出の有無をお答えしていましたが、一部アラート表示の付加誤りがありました。

・付加誤りの原因は、６月２日(火)にアラート表示を開始するため、ごく短期間に入力作業を行いましたが、その際に入力誤りがあったものです。

※アラート表示の付加誤りのあった 100,286 件にはすべてアラート表示を付加しています。

・誤りの内容は単純なものであり、ベリファイ調査など、二重チェック体制をとっていなかったことで生じたものでした。

②コールセンターにおける説明誤り：23 名

・アラート表示が付加されていたにもかかわらず、「情報の流出は確認されていない」と誤って説明したケースがありました。

・オペレーターに短期間で応答方法を習得させたこともあり、表示の見間違いや誤認、思い込みなどによる説明誤りが生じたと考えられます。

なお、その後の調査で、お客様からの問い合わせに対し、実際には個人情報が流出していないにもかかわらず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（すべてコールセンターによる説明）あったことが判明し、８月 10 日（月）に公表しました。

当機構といたしましては、同じ誤りを繰り返さないためにも、今後、以下の再発防止策を確実に実施していくことが必要不可欠と考えています。

①事務処理誤り及び説明誤りの根絶

・迅速で正確な組織内の二重チェック体制の徹底

・コールセンター委託業者に対する指導の強化

②厚生労働省への報告の徹底

・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）　　など

Ⅴ．再発防止に向けた今後の取組について

１．今後の機構システム全体のあり方

本事案を踏まえ、６月４日(木)から機構における外部への送受信はすべて遮断していますが、現状では、年金業務に一部支障をきたしており、セキュリティ上の安全を

確保した上で、できる限り早期にインターネット環境を構築することを検討しています。このため、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えます。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、ルールによって守るだけではなく、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します。

（1）将来の方向性

○年金業務の安定的な運営を行うためには、当機構における情報セキュリティ強化が喫緊の課題であり、迅速に対応していく必要があります。

○将来的なインターネット環境の構築に当たっては、まずお客様の個人情報等の重要情報は確実に守ることを大前提に、セキュリティを担保できる合理的なシステム構成及びインターネット環境を整備することを検討します。「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していきます。

（2）当面の対応

○当面の対応としては、サイバー攻撃等のリスクを考慮し、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暫定環境を構築することを検討します。

2．情報セキュリティ体制の強化

（1）現在の体制

○当機構の情報セキュリティ体制については、情報セキュリティ対策の包括的な規程である情報セキュリティポリシーにおいて、最高情報セキュリティ責任者（副理事長）、統括情報セキュリティ責任者（ＣＩＯ（システム部門担当理事））、統括情報セキュリティ管理者（システム統括部長）及び情報セキュリティ責任者（本部各部長及び拠点長等）を定め、それぞれの役割を規定しています。また、リスク管理委員会において、必要に応じて情報セキュリティについて検討を行うこととしています。

○端末設備運用管理及び機構ＬＡＮシステム設備等の運用保守については、運用保守等を調達・契約している当機構のシステム部門部署が運用委託会社と契約して実施しています。

（2）現状の問題点

①標的型メール攻撃に対する諸規程・要領・手順書などの不備又は未作成

○情報セキュリティポリシーでは、標的型メール攻撃に関する特徴と対応の必要性に関する記載はありましたが、基本的対策事項等に関する記載が不足していました。

○システム障害が発生した際の手順書は定められていましたが、標的型メール攻撃に対するインシデント対処手順書は定められていませんでした。

②運用委託の手順書の内容

○運用委託会社との契約では、事故発生時の対応に関する手順は定められていましたが、標的型メール攻撃への具体的な処理手順は定められていませんでした（ウィルス感染を検知した場合のみ、当該端末のネットワークからの切り離しとウィルスの駆除を行う旨の手順が定められていました）。

③リスクアセスメントの不備

○当機構のリスクアセスメントについては、平成26年度から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ませんでした。

④標的型メール攻撃へのシステム対応の不備

○外部からの不正な侵入を検知し、防止するシステムとしてＩＤＳ（Intrusion Detection System：不正侵入監視システム）やＩＰＳ（Intrusion Prevention System：不正侵入防止システム）、メールゲートウェイによるウィルスチェックの仕組みが用いられていましたが、未知の不正侵入に対する備えとしては不十分でした。

⑤情報セキュリティに関するルールの不徹底

○パスワードの設定など、個人情報を含む文書の管理に関するルールが遵守されていませんでした。

⑥本部のガバナンス及び組織対応の不備

○標的型メール攻撃をはじめとするサイバー攻撃に適時適切に対応するための本部における責任体制が分散しており、役員を含めた幹部による情報セキュリティ体制に関する議論・検討が行われていないなど、情報セキュリティに対するガバナンスが機能していませんでした。

○また、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機能を持つ部署がありませんでした。

○当機構における通信を監視し、ウィルス感染等を早期に検知する機能（ＳＯＣ等）が整備されていませんでした。

○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不足しており、また、それを補うための外部有識者等が十分に活用されていませんでした。

（３）今後の対策

○本事案は、インシデント対応が十分でなかったこと等により、個人情報流出という被害を招いただけでなく、年金記録管理の信頼性も揺るがす事態であったことを踏まえ、二度とこのようなことを生じさせないようにする必要があります。

○このため、標的型メール等への多重防御体制を整備（入口対策、内部対策、出口対策の強化）します。

○また、組織の情報セキュリティ実施体制を抜本的に見直し、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）」を新設し、以下①から⑤までの対策を早急に進め、リスク管理や情報セキュリティに関する当機構全体のガバナンスを強化します。なお、これらの対応については、技術の進展や攻撃の巧妙化に対応できるよう、不断の見直しを行います。

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

・当機構における情報セキュリティに関する各種対策に係る助言・支援を適時適切に受けるため、情報セキュリティの専門家の「最高情報セキュリティアドバイザー」としての招聘又は情報セキュリティ専門機関との契約を検討します。

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

・当機構の情報セキュリティポリシーにおいて、以下の事項を記載します。

ｉ）組織内部への侵入を低減する対策（入口対策）、外部との不審通信を検知して対処する対策（内部対策）、外部に情報を流出させようとする通信等を早期検知して対処する、及び流出の困難度を上げる対策（出口対策）を講じること

ii）最高情報セキュリティアドバイザー又は情報セキュリティ専門機関を設置すること

iii）情報セキュリティインシデントに備えた体制を整備すること

・標的型メール攻撃を認知した際の報告ルールや当機構外との情報共有を含む対処の手順を整備します。

③システム運用委託業務の手順書の明確化

・各システムの運用委託業者が作成する情報セキュリティ侵害等が発生した場合の対応を示した手順書について、インシデント発生時の役割分担やルールを明確化します。

④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

・標的型メール攻撃等を想定したリスクの特定を行い、リスク分析・リスク評価を適切に行います。

・具体的には、リスクアセスメント調査は、ISO27005（情報技術 - セキュリティ技術 - 情報セキュリティリスクマネジメント）を踏まえ、様々な状況を設定した上で、その状況下におけるリスクを特定し、当該リスクの発生可能性・影響度を評価する調査を実施します。また、リスクアセスメント調査が適切に実施できるよう、ＮＩＳＣが作成している「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」や「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」も踏まえながらチェックリストを策定し、より質の高い評価を目指します。

⑤情報セキュリティに関するルールの徹底

・「お客様の年金個人情報は必ず守る」という使命を改めて全職員で共通の認

識とし、情報セキュリティに関する研修の充実によりルールを徹底します。

○「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、外部からの脅威及び内部からの脅威の双方への対策を強化する仕組みとします。

3．職員研修及び内部監査

（1）情報セキュリティ研修などの職員研修

○当機構では、毎年、全職員を対象に情報セキュリティに関する研修を実施していましたが、研修教材の中で標的型メール攻撃に関する記載内容が不十分でした。機構内報において標的型メール攻撃に関する内容を周知したこともありましたが、実際に必要とする対応方法に即したものになっておらず、職員への十分な周知・徹底には至りませんでした。

○また、標的型メール攻撃に対する訓練（模擬メールテストなど）が行われておらず、職員への標的型メール攻撃に対する対処訓練が不十分でした。

○本事案を踏まえ、６月に全職員を対象に情報セキュリティ研修を実施し、不審メールの受信等の際には情報セキュリティ担当部署に速やかに連絡するといった標的型メール攻撃への対応手順等の周知・徹底を改めて図りました。

○今後は、標的型メール攻撃に対する訓練や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、高度な情報セキュリティ維持が必要な組織の職員としての責任や役割など）の実施など、職員研修のさらなる充実強化が必要であると考えています。

（2）内部監査（業務監査・システム監査）

○業務監査に関しては、個人情報の流出防止という観点から、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を重点に置いて行ってきましたが、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います。

○共有ファイルサーバの管理状況に関しては、実効性を高める観点から、本年度より本部各部署及び各拠点の自主点検項目に取り入れるとともに、その点検状況を監査項目に取り入れました。

○また、システム監査に関しては、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、情報セキュリティ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監査を行っていました。今後は当機構全体の情報セキュリティ体制や緊急時の対応手順などの監査を行います。

○さらに、２（３）④で述べた新たなシステムリスクアセスメント調査の結果を踏まえて実施される対策、及び新たな監視システム導入後の状況に対して適宜監査を行い、システム監査の充実強化を図ります。

4．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、当機構を再構築します。

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ことを目指します。

・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。

当機構は、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ため、以下に取り組みます。

・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、当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。

Ⅵ．不正アクセスによる情報流出事案が発生した構造的な要因と今後の対策について

本事案を構造的な要因という観点から改めて分析・考察し、これまでと重複する部分がありますが、以下の５点について、それぞれ要因の詳細と今後の対策について整理します。

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、組織として迅速な検討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。

＜今後の対策＞

○理事長の下で、システムの運用管理も含め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）」を新設します。

○当機構における情報セキュリティに関する各種対策に係る助言・支援を適時適切に受けるため、情報セキュリティの専門家の「最高情報セキュリティアドバイザー」としての招聘又は情報セキュリティ専門機関との契約を検討します。

○計画的に情報セキュリティの専門職員を育成していきます。現在、当機構には「情報セキュリティスペシャリスト」の資格を有する職員がいますが、これらの者が情報セキュリティ担当部署に配置されていません。これらの者を核として専門職員の育成を早急に行います。

○情報セキュリティに関する担当ラインについては、当面の間、緊急対策本部（本部長：理事長、本年６月 14 日(日)設置）による有事対応体制とします。具体的には、情報セキュリティに関するインシデントについては、すべて緊急対策本部への報告を義務づけ、対処方針の決定は同本部が行います。この本部には、新たに設置する専門家又は専門機関の出席を求めます。

※日本年金機構リスク管理規程（抄）

（緊急対策本部）

第 10 条　機構は、機構の業務運営又は組織に重大な影響を与えるリスクが発生した場合又は発生するおそれがある場合に、各部署が連携して組織一体となって対応するため、理事長を本部長とする緊急対策本部を設置する。

２・３　（略）

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。

＜今後の対策＞

○当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します。

○一時保管であっても、個人情報等重要情報については、ルールによって守るのではなく、インターネット接続環境から完全に遮断します。

○共有ファイルサーバの管理業務を情報セキュリティ担当部署に移行し、システム面からの情報セキュリティ対策を強化するとともに、ルールの遵守状況などの確認を徹底します。

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。

＜今後の対策＞

○「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します。

・情報セキュリティポリシーを改正するとともに、NISCが作成している「高度サ

イバー攻撃対処のためのリスク評価等ガイドライン」やＩＳＯ27005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、周知徹底します。

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。

＜今後の対策＞

○「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します。

・情報セキュリティ研修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、ルール化を図ります。

・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します。

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。

＜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・組織風土の抜本改革に取り組みます。

○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こととします。

○また、当機構と厚生労働省との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、遵守します。この案件対応状況について、当機構の運営会議に報

告し、案件の状況、共有の状況をチェックする仕組みとします。
※案件ごとに、担当理事と年金局課長、担当部長と年金局課長又は課長補佐等の対応関係を整理した表を作成し、情報共有に漏れのないようにします。

Ⅶ. まとめ

このたびの不正アクセスによる情報流出事案に関し、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に関しては、「約125万件」以外確認されていません。

本事案について、これまでの経緯を省みると、まず第1回目の攻撃があった5月8日(金)の時点での対応及び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ます。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りません。

本調査において、当機構の対応について、標的型メールの受信を把握した際の対応・対策について多くの問題があったことが判明しました。特に、5月20日(水)に標的型メールが開封されていたにもかかわらず適切な対応がとられていなかったことは、決定的な要因であったと考えられます。もし、対処方針がルール化・体系化されていれば、標的型メールを受信した際、即座に感染した端末を特定・抜線し、ログを調べ、不審通信先ＵＲＬのフィルタリングを行い、他の端末への感染を特定し、当該組織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、このたびの情報流出は防止できたものと考えられます。

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、このたび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ません。

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、多重防御の仕組み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ります。

こうした問題の要因は、基本的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と考えます。

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、使命感が役職員全員に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ります。

本事案を通じて、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りました。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、職員全体の力を結集していかなければなりません。このため、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します。

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、当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します。

当機構といたしましては、個人情報流出に伴う二次被害が万が一にもお客様に発生することがないよう、現在、組織全体を挙げて取り組んでいます。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します。

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んでまいります。

最後に、このたびの個人情報流出及びその後の当機構の一連の対応に関し、国民の皆様に多大なご心配とご迷惑をおかけしましたことを、重ねてお詫び申し上げます。

不正アクセスによる情報流出事案に関する調査委員会委員長
日本年金機構理事長　水島藤一郎

別添資料１

個人情報が流出した方約101万人の内訳

項番	都道府県名	合計	【内訳】	
			被保険者	年金受給者
1	北海道	41,668	27,539	14,129
2	青森県	8,769	5,739	3,030
3	岩手県	4,755	2,410	2,345
4	宮城県	10,865	6,196	4,669
5	秋田県	3,577	1,410	2,167
6	山形県	3,383	1,349	2,034
7	福島県	6,453	3,056	3,397
8	茨城県	14,937	8,292	6,645
9	栃木県	13,589	7,493	6,096
10	群馬県	16,295	8,300	7,995
11	埼玉県	59,756	29,292	30,464
12	千葉県	45,248	20,271	24,977
13	東京都	96,172	50,560	45,612
14	神奈川県	73,826	38,770	35,056
15	新潟県	12,120	4,085	8,035
16	富山県	5,398	1,454	3,944
17	石川県	9,771	3,734	6,037
18	福井県	4,974	2,020	2,954
19	山梨県	5,896	2,637	3,259
20	長野県	14,807	5,685	9,122
21	岐阜県	14,902	6,987	7,915
22	静岡県	23,105	9,489	13,616
23	大阪府	96,884	52,051	44,833
24	兵庫県	42,179	19,186	22,993
25	愛知県	55,062	27,203	27,859
26	三重県	15,624	6,426	9,198
27	滋賀県	7,016	2,525	4,491
28	京都府	16,499	7,433	9,066
29	奈良県	11,845	5,501	6,344
30	和歌山県	22,945	3,349	19,596
31	鳥取県	6,330	3,224	3,106
32	島根県	9,181	4,878	4,303
33	岡山県	17,077	6,990	10,087
34	広島県	24,530	11,394	13,136
35	山口県	12,793	5,032	7,761
36	徳島県	6,924	2,776	4,148
37	香川県	8,668	4,014	4,654
38	愛媛県	10,117	3,368	6,749
39	高知県	6,578	2,417	4,161
40	福岡県	45,221	19,391	25,830
41	佐賀県	5,423	1,754	3,669
42	長崎県	11,214	4,471	6,743
43	熊本県	14,887	5,624	9,263
44	大分県	9,699	3,531	6,168
45	宮崎県	10,580	4,068	6,512
46	鹿児島県	18,573	7,553	11,020
47	沖縄県	38,538	24,931	13,607
合計		1,014,653	485,858	528,795

別添資料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、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・評価しました。

○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、以下のとおりです。

※「○」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	×	×	×

別添資料３－１

[redacted]

差出人: 機構本部システム統括部　特殊
送信日時: 2015年5月8日金曜日 20:07
宛先: 全職員メーリングリスト
件名: 【注意喚起】不審なメールについて

重要度: 高

【注意喚起】

職員各位

最近、外部から機構宛に不審なメールが相次いでいます。

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してください。

〔参考〕

中には巧妙なものもありますので、参考までにご紹介します。。

「標的型メール」と呼ばれるサイバー攻撃があります。

特定の標的に対して、怪しくないように見えるメールを送りつけて
添付されたウイルスをクリックさせるものです。
怪しくないように見せる方法は、たとえば、次のようなものがあります。

（１）一般的な問合せをしてきて、それに対して回答をすると、
回答に対する追加問合せを装って、ウイルスを送りつけてきます。

（２）一般的な問合せをしてきて、それに対して回答をすると、
メールアドレスと職員の名前を先方は入手できます。
厚生労働省や機構の HP を見て、記されている事実をもとに、
もっともらしい文面を組み立てます。
入手したメールアドレスと職員の名前を宛先として
ウイルスを送りつけてきます。

これらに共通するのは、最後にウイルスをクリックさせることです。
つまり、機構外部から送信されたメールで、ファイルをクリックさせるようなものは、
まず、疑ってかかるべき、ということです。

昨今、標的型メールの完成度は上がってきてはいますが、
宛先や送り主の名前や所属、本文の文体など、まだどこかに不自然なところがあります。
ファイルをクリックさせるメールは、少しでも不自然なところがあれば
送り主に直接電話で確認する等してください。

標的型メールで使用されるウイルスは、未知のものであることが多いです。
ウイルス対策ソフト（マカフィー等）は、既知のウイルスを検出するものですので
未知のウイルスに対しては、万全の防御策ではありません。
ウイルス対策ソフトが入っているから安心、とは思わないでください。

照会先 ： システム統括部 システム管理G （[redacted]）

別添資料３－２

[redacted]

差出人: 機構本部システム統括部　特殊
送信日時: 2015年5月18日月曜日 12:02
宛先: 全職員メーリングリスト
件名: 【注意喚起】不審なメールについて

【注意喚起】

職員各位

本日、外部から機構職員宛に以下の内容の不審なメールが相次いで送信されています。

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してください。

〔不審メール内容〕

差出人：[redacted]＜[redacted]@yahoo.co.jp＞
件名：給付研究委員会オープンセミナーのご案内
添付ファイル：給付研究委員会オープンセミナーのご案内.lzh

○○　○○　様

平成 27 年 5 月に横浜国立大学と企年協が共同で実施いたしました企業年金アンケート結果の報告会と意見交換会を下記の通り実施いたします。
アンケートの集計結果に基づく報告会は、今後の企業年金の方向性を考えるうえでも、基金関係者にとって大いに参考になると思います。

会員の皆様の積極的なご参加をお願い申し上げます。

お申し込みは添付資料をクリックしてください。

[redacted]

照会先 ： システム統括部 システム管理G （[redacted]）

別添資料３－３

[redacted]

差出人: 機構本部システム統括部　特殊
送信日時: 2015年5月25日月曜日 12:03
宛先: 全職員メーリングリスト
件名: 【重要：注意喚起】不審なメールについて

【注意喚起】

職員各位

先般より、外部から機構職員宛に不審なメールが相次いで送信されています。

不審なメールが届いた場合は、添付ファイルや記載されているＵＲＬをクリックせずに、
削除してください。
万一、添付ファイルや記載されているＵＲＬをクリックした場合は、
ただちに下記照会先までご連絡ください。

照会先　：　システム統括部　システム管理Ｇ　（[redacted]）

【メールが不審であるかどうかの判断ポイント】

①　添付ファイルが付いている。
②　本文中にリンクがあり、クリックするようになっている。
このどちらかに該当するインターネットメールを受信した場合は、
身に覚えのある人からのメール、たとえ機構職員からのメールであってもまず疑って、
本文をよく読んで、不審な点がないか、確認してください。

【受信した不審メールの例】

〔例１〕

差出人：[redacted]@yahoo.co.jp
件名：「厚生年金基金制度の見直しについて（試案）に関する意見」
記載されているＵＲＬ：[redacted]

> ○○　○○ 様
> ５月１日に開催された厚労省「厚生年金基金制度に関する専門委員会」最終回では、厚生年金基金制度廃止の方向性を是とする内容が提出されました。これを受けて、企年協では「厚生年金基金制度の見直しについて（試案）に関する意見」を、５月５日に厚労省年金局企業年金国民年金基金の渡辺課長に提出いたしました。
> 添付ファイルをご覧ください。
> ＊＊
> [redacted]
> [redacted]

〔例２〕

差出人：[redacted]@excite.co.jp>
件名：【医療費通知】
添付ファイル：医療費通知のお知らせ.lzh

> 本メールは、保険を利用して診察や診療を受けられた方に、医療費のご負担額等をお知らせしています。
> Windows-PC で開けてください。

〔例３〕

差出人：[redacted]＜[redacted]@yahoo.co.jp＞
件名：給付研究委員会オープンセミナーのご案内
添付ファイル：給付研究委員会オープンセミナーのご案内.lzh

○○　○○　様

平成 27 年 5 月に横浜国立大学と企年協が共同で実施いたしました企業年金アンケート結果の報告会と意見交換会を下記の通り実施いたします。
アンケートの集計結果に基づく報告会は、今後の企業年金の方向性を考えるうえでも、基金関係者にとって大いに参考になると思います。

会員の皆様の積極的なご参加をお願い申し上げます。

お申し込みは添付資料をクリックしてください。

[redacted]

〔例４〕

差出人：[redacted]＜[redacted]@yahoo.co.jp＞
件名：厚生年金徴収関係研修資料
添付ファイル：厚生年金徴収関係研修資料(150331 厚生年金徴収支援 G).lzh

○○　○○　様

いつもお世話なっております。
遅くなりましたが、先日、お話しした
第１回養成研修のときに使用した「研修のご案内」等のデータを
送付します。これらを参考にして、加工していただければと思います。
お忙しい中、ご負担をおかけしておりますが、何卒、よろしくお願いします。
何かありましたら、何なりとお問い合わせください。

[redacted]

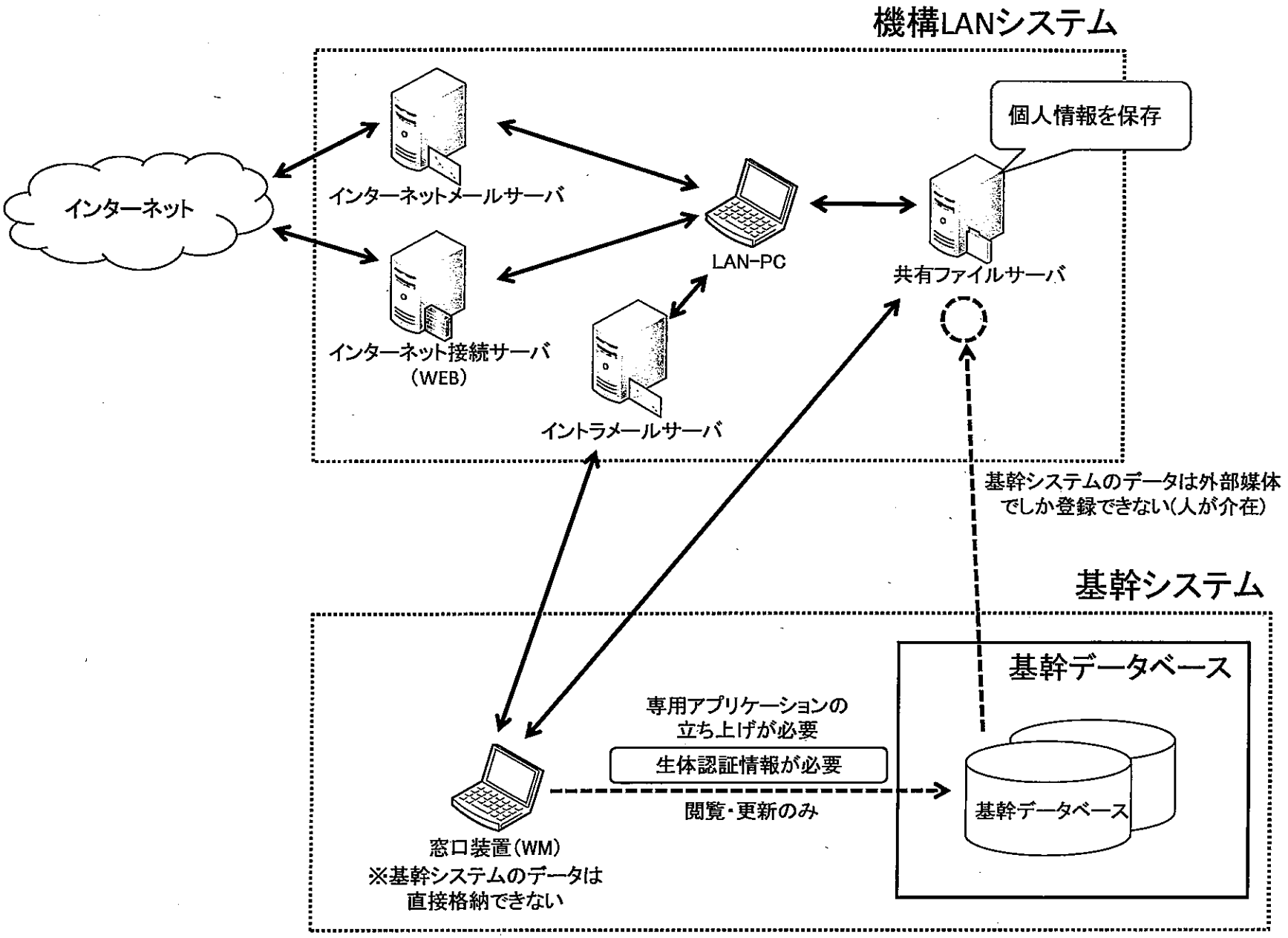
※同一の内容でＵＲＬ（[redacted]）が記載されたメールも確認しています。

++

〒168-8505 東京都杉並区高井戸西 3-5-24
日本年金機構本部 システム統括部 システム管理G
(TEL:代表)03－5344－1100
(TEL:直通)03－5344－1120
++

別添資料４

日本年金機構のシステムイメージ



別添資料５

お客様への対応状況

日本年金機構では、このたびの事態を受け、お客様の不安の解消、年金の支払に影響が出ることのないよう、流出した個人情報による被害の防止に向け「緊急対策本部」を設置しました。「緊急対策本部」においては、年金事業に対する信頼回復とお客様の年金を守るため、次の対策に継続的に取り組んでいます。

１．お客様へのお詫びとお問い合わせ対応
（1）お詫びとお願いの文書の送付 ○個人情報が流出した125万件のデータを分析し、約101万人の対象となるお客様に対してお詫びとお願いの文書を送付しました。 ・４情報（基礎年金番号・氏名・生年月日・住所）が流出したお客様約1.5万人へは、６月３日(水)～４日(木)に送付。 ・２情報（基礎年金番号・氏名）、３情報（基礎年金番号・氏名・生年月日）が流出したお客様約100万人へは、６月22日(月)～29日(月)に送付。 ○なお、７月中旬よりお詫びとお願いの文書が返送（未着）となったお客様に対しては、当初の送付先と別住所の確認を行い、順次、再送付を行っています。また、別住所が判明しないお客様に対しては、全国の年金事務所職員による戸別訪問を実施し、８月中旬までに対応を完了する予定としています。
（2）専用コールセンターの開設 ○６月１日(月)の記者会見後から、お問い合わせ窓口として、専用コールセンター（フリーダイヤル）を開設し、1,000人体制で対応（8:30～21:00：土・日・祝日を含む）を実施しています。 ※６月１日(月)は50席、６月２日(火)100席、６月３日(水)から1,000席で受けられるよう対応を強化しています。受電件数に合わせて対応中です。
（3）年金事務所におけるお客様対応 ○６月１日(月)から全国の312年金事務所において相談窓口を設置し、窓口と電話による相談を実施しています。（土・日・祝日は、9:30～16:00） ※休日の開所につきましては、８月は開所する事務所数を一時的に縮小しますが、基礎年金番号の変更通知書を送付する際には、全国の年金事務所対応に戻す予定です。
（4）情報が流出しているのに「流出していない」と誤った説明を行ったお客様への対応 ○誤った説明をした2,449名のお客様に対し、６月２７日(土)から７月31日(金)にかけて全国の年金事務所職員が戸別訪問により、お詫びとお願いの文書を手渡し説明と謝罪を実施しました。個別訪問の際にいただいたご意見につきましては、専用コールセンター及び年金事務所におけるお客様対応等に活用させていただくこととしています。

2．お客様の被害防止に向けた取り組み

（1）なりすましによる手続きの防止対策

①基礎年金番号の変更手続き

・個人情報が流出したお客様のうち、約96万人のお客様に対し、なりすましによる手続きの防止のため、８月下旬より、新しい基礎年金番号への変更手続きを実施します。

②住所変更、受取り金融機関等の変更手続き

・個人情報が流出した約101万人の対象となるお客様の中で、５月８日(金)から６月１日(月)までに住所変更や受取り金融機関等の変更手続きをされたお客様 436人に対し、全国の年金事務所職員が戸別訪問により、届出がご本人によるものであることを確認しています。６月２日(火)以降に変更手続きを取られたお客様につきましても、新たな基礎年金番号を発行するまでの間は、本人確認手続きの徹底を引き続き継続していきます。

・また、個人情報の流出が確認されていないお客様で、５月８日(金)から６月１日(月)までに住所変更や受取り金融機関等の変更手続きを取られた方につきましても、８月上旬までに戸別訪問をし、できる限りご本人確認を実施します。

（2）不審電話への対応

○全国の年金事務所等へ通報をいただいた不審電話で対応が必要と思われる事象につきましては、職員が訪問により状況を確認し、個別にお客様対応を実施しています。

（3）ホームページによる情報提供とホームページの不正改ざん防止

○日本年金機構のホームページに、情報流出事案の概要や通報のあった不審電話の主な内容と手口等を掲載し、便乗詐欺やなりすまし手続き防止のための注意喚起を行っています。

・６月１日(月)から不正アクセスによる情報流出事案を掲載

・６月５日(金)から不正アクセスによる情報流出事案を悪用した不審電話に対する注意喚起を掲載

・通報のあった不審電話の主な内容と手口等を掲載（６月24日(水)～随時更新中）

・６月６日(土)にホームページに脆弱性が発見され一時運用を停止
→ ６月８日(月)に暫定版で運用を再開し、６月22日(月)に復旧

（4）関係機関と連携した広報（便乗詐欺・なりすまし手続き防止）

○便乗詐欺・なりすまし手続き防止のため、以下のような関係機関と連携した広報を実施しています。

・消費者庁、国民生活センター、警察庁・都道府県警察のホームページ上で注意喚起を実施

・警察と連携した詐欺被害防止のためのチラシを作成し、年金事務所等で掲示及び配布　　※ 厚生労働省地方厚生局を通じ、全国の市町村へも協力を要請

・内閣広報室の支援の下でツイッター投稿を開始

・全国71紙の新聞に政府広報を掲載、全国18のラジオ局でお知らせを実施

・全国社会保険委員会連合会の総会にて注意喚起の協力要請

・厚生労働省作成の注意喚起チラシ及びＱ＆Ａの配布、ホームページへの掲載
「地域年金事業運営調整会議委員」
（学識経験者、自治体、教育委員会、商工会、受給者協会、社労士会など）
「全国社会保険協会連合会の会員」
「ＮＰＯ法人 年金・福祉推進協議会」ホームページ