

年金機構などの監査強化 サイバー基本法改正検討

日本経済新聞 2015/6/4

政府は日本年金機構がサイバー攻撃を受けて年金情報が流出した問題をめぐり、サイバー攻撃対策の司令塔機能を担う「内閣サイバーセキュリティセンター（NISC）」の権限強化に向けた法改正の検討に着手する。菅義偉官房長官が4日の記者会見で表明した。日本年金機構など特殊法人への監査権限を強化する方策を盛り込む。

今年1月に施行したサイバーセキュリティ基本法は、NISCを事務局とするサイバーセキュリティ戦略本部に国の行政機関への監査権限を与えた。一方、特殊法人などについては「資料提出などの必要な協力を求めることができる」といった規定にとどめ、NISCの権限を弱くした。

菅官房長官は「NISCの体制増強や監査対象の拡大は極めて大事だ」と強調。「年金機構のような極めて国民にとって大事なものについても（基本法を含め）見直しをすべきだ」と話した。

法改正は、特殊法人や独立行政法人についてNISCに防御策の監査や勧告などの権限を与えたり、報告義務を課すことなどを検討する。日本銀行など48の事業者も新たに監査対象に入ることになる。

法改正のほか、現在、約120人のNISCの人員を今後、増強していくことも検討する。

年金情報流出、警察に相談後も感染か 対応後手で拡大

2015/6/4 14:00 日本経済新聞 電子版

日本年金機構がサイバー攻撃を受け約125万件の年金情報が流出した問題で、同機構が警視庁に被害を相談した2日後の5月21日に、人事部門の職員が不正メールの添付ファイルを開いて端末を感染させていたことが4日、関係者への取材で分かった。感染端末は直後から3日間にわたって外部と不審な通信を行っており、この間に個人情報などが大量流出した可能性があるという。

年金情報流出問題の経緯

最初のウイルス感染。内閣サイバーセキュリティセ

5月8日 ンターが外部との大量通信に気付き、厚労省と日本

年金機構に連絡

18日 数十台の感染が判明

19日 機構が警視庁に相談

21日 人事部門の職員の端末も感染、直後に大量流出か

28日 警視庁から情報流出の連絡、塩崎厚労相に報告

6月1日 年金機構が問題公表

同機構はサイバー攻撃による被害を明確に認識した後も職員に対策を徹底せず、被害拡大を招いた形だ。

機構はこれまで、職員2人が5月8～18日に不正メールに貼り付けられたアドレスをクリックしたり、添付ファイルを開いたりしてウイルスに感染したと説明していた。

関係者によると、人事部門の職員は5月18日までに不審なメールを受け取り、添付ファイルを開封。これによって端末がウイルスに感染したとみられる。

直後から3日間にわたり、外部との不審な通信があったといい、この期間に年金情報などが大量に引き出された可能性がある。警視庁もこうした経緯を把握しており、機構から経緯を聴くとともに、端末などを解析して詳しく調べる方針。

機構は5月8日に、内閣サイバーセキュリティセンター（NISC）から「異常通信がある」と連絡を受け、ウイルス感染を認識。塩崎恭久厚生労働相が初めて報告を受けたのは20日後の同月28日夕で、機構が情報流出を公表したのは6月1日だった。

年金機構、不正メール100通以上届く 非公開アドレスに5月

2015/6/4 13:14 日本経済新聞

日本年金機構がサイバー攻撃を受け約125万件の年金情報が流出した問題で、外部に公開していない職員のメールアドレスなどに、5月18日ごろ100通以上の不正メールが届いていたことが4日、機構などへの取材で分かった。警視庁は5月8日に初めに感染した職員の端末からアドレスが流出した可能性があるとして、感染拡大の経緯などを詳しく調べる。

不正メールには少なくとも3種類以上のウイルスが含まれていたことも判明。1通のメールに複数種のウイルスが仕込まれていた例もあった。感染端末を遠隔操作するタイプのほか、機構内部の情報を盗み取るものもあったとみられる。

機構などによると、最初に感染したウイルスが仕込まれていたメールは、厚生労働省の報告書と同じタイトルで、公開されている調達部門のアドレスに届いた。すぐに感染端末を隔離したものの、18日ごろ非公開の職員アドレスなどに大量のメールが届いたという。

件名は「給付研究委員会オープンセミナーのご案内」「医療費通知」「厚生年金徴収関係研修資料」などで、添付ファイルを開くと、遠隔操作ウイルスなどに感染するものだった。

同日までに東京の本部の職員が開封して感染したほか、機構のLAN（端末情報通信網）を通じて数十台に感染が拡大したとみられる。

厚生省、年金情報流出で検証委員会を設置

日経新聞 2015/6/4

厚生省は4日、日本年金機構がサイバー攻撃を受け約125万件の年金情報が流出した問題を巡り、原因究明と再発防止策を検討するための「日本年金機構不正アクセス事案検証委員会」を設置すると発表した。最高裁判事で元東京高検検事長の甲斐中辰夫氏が委員長を務める。

このほか、セキュリティー会社「ディアイティ」（東京・江東）の青嶋信仁取締役、フューチャーアーキテクト(4722)の斎藤洋平氏などが委員に選ばれた。事務局長は中央大法科大学院教授の野村修也氏が務める。〔日経QUICKニュース（NQN）〕

年金情報流出、不正サイトに誘導型も 職員の端末感染

2015/6/3 13:45 日本経済新聞

日本年金機構がサイバー攻撃を受け約125万件の年金情報が流出した問題で、職員の1人はメールに貼られた不正サイトに誘導され、端末がウイルスに感染していたことが3日、厚生労働省や捜査関係者などへの取材で分かった。別の職員はメールの添付ファイルを開いて感染しており、攻撃者は様々なメールを送りつけて情報を引き出そうとしたとみられる。

厚生省などによると、5月8～18日に不正メールによってウイルス感染したのは東京と福岡の2職員。このうち1人は添付ファイルを開いて感染したことが判明している。厚生省などは攻撃者がこの感染端末を遠隔操作し、大量の年金情報を引き出したとみている。

もう1人はメール本文に貼り付けられていたアドレスをクリックしたところ、ウイルスを仕込んだ不正サイトに誘導され、感染したことが新たに分かった。厚生省などはこの端末からは大規模な情報流出に至らなかったとみているもようだ。

捜査関係者などによると、不正メールは5～6種類あり、件名が厚労省の報告書と同じものや学術関係者を装ってセミナー参加を促すものがあった。メールによって異なるウイルスが仕込まれていた可能性があり、警視庁は感染端末の分析を進める。

攻撃者は感染端末を遠隔操作し、年金情報を東京都内の企業のサーバーに送信させていたとみられる。サーバーは企業に無断で使っていた可能性が高い。

年金情報流出、件数拡大も 衆院委で集中審議

日経新聞 2015/6/4 0:59

衆院厚生労働委員会は3日、日本年金機構から公的年金の個人情報が出た問題に関する集中審議を開いた。水島藤一郎同機構理事長は、現在約125万件と公表している流出件数がさらに増える可能性を示唆した。厚労省や年金機構の新たな不手際も発覚し、全容解明と事態収拾は見通せない状況だ。

塩崎厚労相と年金機構の 主な発言
水島年金機構理事長
◦ 流出件数が増える可能性はあり得る
◦ 漏れた基礎年金番号の変更は3カ月で完了させたい
塩崎厚労相
◦ 第三者委員会で原因究明、再発防止策について速やかに結論
◦ この問題を理由に被害が発生した場合の賠償は考えていない
集中審議でわかった新事実
◦ 基礎年金番号、氏名、住所、生年月日の4情報が漏れたのは少なくとも約1万6000人分
◦ 内規で禁じられている共有フォルダ上での個人情報の保管が発覚

水島理事長「残念ながら、さらに流出件数が拡大する懸念はある」

今回の問題では、機構の多数のパソコンがウイルスに感染した。そうした端末のハードディスクに機密情報があれば、そこから年金情報の流出の可能性が残る。水島氏は「警察に届けている（端末の）記録を解析した結果を踏まえて分かる」とし、被害範囲が確定で

きていないと認めた。

情報漏れした約 125 万件のうち、基礎年金番号、住所、氏名、生年月日の 4 情報すべてが流出した件数は約 5 万 2000 件。重複ケースがあると見られ、少なくとも約 1 万 6000 人の 4 情報が流出したもようだ。

塩崎恭久厚生労働相「何もしていなかったわけではない」

問題の発端は 5 月 8 日に九州ブロック本部（福岡市）で受信した不正メールの添付ファイルを開いたことだ。民主党は機構と厚労省が同日中に最初のウイルス感染を把握しながら、全パソコンのインターネット接続を遮断しなかったと指摘。「大規模な情報流出は防げたはずだ」と言う。

塩崎厚労相は数日後から新ワクチンを機構の全端末にインストールした例を挙げ「対策は順次進めた」と反論した。機構は職員に不審なメールを開かないよう注意喚起したが、全端末のネット接続の遮断など抜本策は取らなかった。

水島理事長「掲示板の書き込みは承知している」

民主党は問題公表前の 5 月 28 日から、ネットの掲示板に情報流出に関する内部情報とみられる書き込みがあったと指摘した。水島理事長は「極めて遺憾だ」と事実上、職員の書き込みであると認めた。情報管理のずさんさは前身の旧社会保険庁でも問題視されていた。

民主党の枝野幸男幹事長は 3 日、塩崎厚労相の責任問題について記者団に「当然、近い将来そういう話になる」と語った。第 1 次安倍政権は「消えた年金」問題をきっかけに失速した。岡田克也代表は今回の問題を「漏れた年金」と位置づけ、政権や閣僚の責任問題も追及していく方針だ。

日本年金機構は 3 日、個人情報流出した加入者に対し、おわびの文書の発送を始めたと発表した。文書には流出した情報の種類や基礎年金番号の変更なども通知している。同日だけで約 9 千人に郵送した。

年金機構、端末数十台が感染 LAN 経由で拡大か

2015/6/4 1:51 日本経済新聞

日本年金機構がサイバー攻撃を受け約 125 万件の年金情報が流出した問題で、ウイルス感染した端末が数十台に上ることが 3 日、機構などへの取材で分かった。機構などは、不正メールによって感染した端末を通して機構の LAN（構内情報通信網）に侵入し、次々に他の端末を感染させたとみている。

機構などによると、5 月 8 日に福岡の職員がメールに貼り付けられたアドレスをクリックしたところ、不正サイトに誘導されウイルスに感染。東京の職員も不正メールの添付ファイルを開いて別のウイルスに感染した。18 日に数十台の感染が判明した。

いずれも新種のウイルスで、機構はセキュリティー会社に依頼して対策ソフトを作成。22日までに全端末を駆除したというが、28日に個人情報外部のサーバーに流出しているのが見つかった。

セキュリティーの専門家によると、業務上の連絡などを装って送りつける「標的型メール」による攻撃では、最初に感染した端末を遠隔操作してシステムに侵入し、よりアクセス権限の強い端末を乗っ取るのが一般的。

職員になりすましてウイルス付きのメールを送りつけて他の端末を感染させたり、ネットワーク内に保管されているID・パスワードのリストを盗み出したりして、遠隔操作できる範囲を次々に拡大するという。

警視庁も感染が拡大した経緯について、ウイルスを分析するなどして詳しく調べる方針だ。

厚労省文書装う不正メール5～6種類 年金情報流出

感染、東京と福岡で

2015/6/2 13:30 日本経済新聞

日本年金機構の職員の端末がサイバー攻撃を受け約125万件の年金情報が流出した問題で、機構に対し、厚生労働省の報告書と同じ件名を含む5～6種類の不正メールが送りつけられていたことが2日、機構や捜査関係者への取材で分かった。東京と福岡の職員の端末が不正アクセスされていたことも判明した。

警視庁公安部は業務上の連絡を装って公的機関の情報を狙う「標的型メール」とみて、ウイルス感染の経緯を詳しく調べている。

同機構などによると、不正メールの1つはタイトルが「厚生年金基金制度の見直しについて（試案）に関する意見」となっていた。

社会保障審議会年金部会の専門委員会が2013年2月、同制度の見直しについて同じタイトルの報告をまとめており、厚労省のホームページ（HP）で公開されている。警視庁は何者かが同HPを閲覧するなどし、機構職員が不信感を抱かないような件名の業務連絡を装い、ウイルスを送りつけた可能性があるともみている。

機構などによると、5月8日に福岡にある事務所の職員が不正メールの添付ファイルを開いた直後、契約しているセキュリティー会社が外部との不審な通信を検知。東京の本部の職員も添付ファイルを開き、端末が感染したことを18日までに確認した。

今回の攻撃は、無害なプログラムや文書ファイルを装って不正プログラムを送りつける「トロイの木馬」と呼ばれるタイプ。攻撃者はバックドア（裏口）と呼ばれる秘密の入り口を感染端末に仕込んで、機構の共有サーバーに侵入し、年金情報を盗み出した可能性がある。

機構によると、流出したのは年金記録を管理するため一人ひとりに割り当てられている基礎年金番号と氏名の計125万件。このうち約116万7千件に生年月日、約5万2千件には住所と生年月日が含まれていた。

機構は19日に警視庁に相談。同庁公安部は年金情報の外部流出を確認し、不正アクセス禁止法違反や不正指令電磁的記録作成などの容疑を視野に捜査している。

▼トロイの木馬 無害のプログラムを装って、パソコン端末などに侵入するウイルスの一種。情報流出や不正サイトへの強制接続などの被害を受ける。兵士を忍ばせた巨大な木馬を城に侵入させて奇襲したギリシャ神話にちなんで名付けられた。

感染端末を遠隔操作して内部のネットワークに侵入する「バックドア型」、不正プログラムが作動する「ドロPPER型」などがある。

年金情報流出、厚労省が対策チーム 菅長官「認識に甘さ」

機構に電話3万9000件

日経新聞 2015/6/2

日本年金機構がサイバー攻撃を受け、約125万件の年金情報が流出した問題で、塩崎恭久厚生労働相は2日の閣議後の記者会見で、第三者による検証委員会とともに省内に対策チームを立ち上げることを明らかにした。機構は同日、全国の年金事務所などで、年金受給者らからの問い合わせなどに対応、被害の拡大防止に乗り出した。

菅義偉官房長官は2日の閣議後の記者会見で「日本年金機構の認識の甘さがあった。責任は免れない」と批判。「情報流出の事態把握を徹底的に行い、流出した方々に迷惑をかけないよう万全の再発防止策に全力で取り組んでいる」と強調した。内閣官房のサイバーセキュリティセンター（NISC）で、厚労省と年金機構の調査を支援するチームを設置し

たことも明らかにした。

塩崎厚労相は、機構の水島藤一郎理事長らについて、「根源的な理由を調べた上で必要な処分をしたい」と述べた。

機構は1日に設けたフリーダイヤルの専用窓口で相談を受け付けている。同日夕から2日午前10時までに、流出した個人情報の対象者かどうかを問い合わせる内容など計約3万9千件の電話が寄せられたという。

このほか、各地の年金事務所でも年金受給者らからの流出の有無の確認などに応じている。情報流出が確認された人については、順次個別に文書で通知して謝罪し、基礎年金番号を変更する。

今回流出した基礎年金番号、氏名、生年月日、住所という4つの情報があっても個人情報は免許証などで確認した上で答えているとしており、機構は「なりすまし行為が行われることは考えにくい」と説明する。

日本年金機構の個人情報流出対象者への対策

- 流出対象者の基礎年金番号を変更する
- 流出対象者には文書で個別に連絡。電話連絡はしない
- 流出対象者から年金にかかわる手続き申請があった場合、本人確認の上対応する
- ウイルス感染したパソコンを隔離、ウイルスを除去し、警視庁に捜査を依頼
- 情報流出防止のため、全拠点でインターネットへの接続を遮断

日本年金機構の専用電話窓口

フリーダイヤル	0120-818-211
受付時間	午前8時半から 午後9時まで

ただ、該当者の情報を扱う場合は職員の端末の画面が点滅して警告する仕組みを2日から始めた。機構は該当者については「細心の注意を払って本人確認を徹底する」としている。

年金情報流出でサイバー対策見直し 課題は人材

日本経済新聞 電子版 2015/6/2 2:00

政府は中央省庁の情報システムへの大規模なサイバー攻撃を想定し、省庁の枠を超えて

実践的な演習や訓練を繰り返してきた。だが情報安全分野で先行する米欧に比べると、人材の質・量ともに見劣りする。今回の日本年金機構の人為的ミスのように、組織の隅々までサイバー攻撃への危機感を共有できていないことも課題になる。



政府は1日、サイバーセキュリティ対策推進会議を急きょ開き、杉田和博官房副長官が各府省庁に対して(1)情報システムの点検の実施(2)所管する独立行政法人や特殊法人での個人情報を含む重要情報の管理徹底——を指示した。最大の懸念は他の政府機関に被害が飛び火することだ。

日本の政府機関への不正アクセス件数は2011年度の約66万件から、13年度は約508万件と7倍超に急増。年金機構が受けた攻撃と同様に、特定の相手を狙った標的型攻撃が大半だった。不正アクセスの97%は海外からとみられる。

政府はこうした攻撃に対処する目的で、1月に菅義偉官房長官を本部長とするサイバーセキュリティ戦略本部を設けた。総務省や経済産業省、警察庁などから人材を集約した内閣サイバーセキュリティセンター (NISC) を事務局にして、政府内の司令塔を担わせる仕組みだ。

NISCの人員は年初の約80人から100人超にまで増加。自衛隊のサイバー防衛隊を加えると政府全体で約200人の体制になった。

それでも米欧に比べると、十分な体制と言えない。米国は16年末までにサイバー攻撃に対処する米軍部隊だけで現在の約3倍の6200人規模に増やす計画。フランスの国家情報システムセキュリティ庁の約350人体制は、年内に約500人にまで膨らむ。

今回の問題を受け、日本政府もサイバー攻撃に対する陣容の拡充が早急な検討課題になる。組織全体でサイバー攻撃に対する危機意識を高めることも必要だ。

マイナンバーに逆風も 政府、管理体制洗い直し

日本経済新聞 電子版 2015/6/2

日本年金機構の情報流出問題は、2016年1月から始まる税と社会保障の共通番号（マイナンバー）制度にも影響しかねない。政府は税や社会保険料の個人情報に加え、18年度から医療や戸籍など、より私的な個人情報にも活用する方向。今回の年金機構の問題を受けて個人情報保護への不信感が高まれば、今後のマイナンバーの運用に逆風になる可能性がある。

「国民の目が厳しくなるのは間違いない」。年金機構の問題を聞いた政府のマイナンバー担当者はこう漏らす。政府はカルテや診療報酬明細（レセプト）などの医療情報へのマイナンバーの活用方針を決めたばかり。今後は法改正などの対応が必要になる矢先だけに、不安は消えない。

マイナンバーは行政手続きの効率化を目的に導入する制度だ。国税庁や日本年金機構、各自治体など、あらゆる行政のシステムがつながる。政府は「仮にマイナンバーが漏れても、簡単には個別の情報にアクセスされないシステム体制だ」（内閣官房）と説明する。

甘利明経済財政・再生相は1日、マイナンバーと年金の情報は「独立した別の機関が管理し、ファイアウォール（安全隔壁）も引かれている」と安全性を強調した。

だが今回の問題を受けて「マイナンバーの情報管理は従来以上に厳しく求められる」（第一生命経済研究所・星野卓也エコノミスト）との声が多い。政府はマイナンバーの導入を前に、職員の管理体制が十分かどうかを洗い直す見通しだ。

年金機構の甘さ、傷口広げる 警告浸透せず流出

日本経済新聞 電子版 2015/6/2 1:30

日本年金機構で発覚した大規模な個人情報の流出は、年金記録問題などで傷ついた国民の公的年金制度への信頼回復をさらに遠ざけそうだ。発端は外部からのウイルスメールによる不正アクセスだが、同機構の対応の不手際が傷口を広げた点は否めない。安倍晋三首相にとって年金問題は第1次内閣でも苦しんだ鬼門だけに、首相官邸も火消しに躍起になっている。

塩崎恭久厚生労働相は1日、問題の発覚を受けた記者会見で「深刻に受け止めて早期解明するとともに、不正利用されて支払いに影響が出ないようにする」と語った。

実は政府の関係機関が外部からサイバー攻撃を受けることは珍しくない。昨年3月にも独立行政法人の建築研究所で330件のメールアドレスなどが流出している。しかし、今回の125万件は「過去に記憶がない」（内閣官房）ほどの規模で、被害はさらに拡大するとの見方も強い。

年金機構のシステムにはウイルスを検知するソフトが組み込まれていたというが、何ら

かの理由でこれをすり抜けてしまい端末が感染した。塩崎厚労相は「悪意を持った攻撃を
防げなかった」と語る。だが、不祥事続きだった旧社会保険庁を前身とする年金機構内部
のまずい対応が影響を大きくした面もある。

企業・官公庁から情報が流出した主な事例		
流出元	発覚時期	被害件数・内容
★法務省	2014年9月	法務省や法務局が運用する内部ネットワークへの不正アクセスで情報流出の可能性
ベネッセコーポレーション	2014年7月	業務委託先の元社員が氏名や住所など約3500万件分の顧客情報を名簿業者に売却
★ヤフー	2013年5月	不正アクセスで最大2200万件のIDが流出した可能性
★農林水産省	2013年1月	公用パソコンがサイバー攻撃を受け、内部文書流出の疑い
セディナ	2011年8月	最大約15万8千人分の顧客情報が外部に持ち出された可能性

(注) 件数は当事者発表による。★はサイバー攻撃

同機構の職員の端末で最初にウイルス感染が確認されたのは5月8日だった。職員が受け取ったメールに添付されたファイルを開いたことで、ウイルスに感染し不正アクセスを許した。その時点で同機構は端末を隔離し、「不審なメールは開けないように」と職員らに注意を促した。

しかし、その警告は浸透しなかった。その後も別の職員がメールを受け取り、添付ファイルを開けてしまった。警視庁への捜査依頼も18日までに何度か不正アクセスを検知した後だった。もう少し早く対応していれば被害をもっと小さくできた可能性が高い。

個人情報が出た経緯にも不手際が重なっている。個人情報にはパスワードをかけるのが年金機構の内規になっている。こうした流出が起きても中身にアクセスできないようにするためだ。だが、同機構は1日に開いた記者会見で125万件のうち約55万件はパスワードをかけていなかったと明らかにした。トラブルに備えた内規の形骸化も浮き彫りになった。

2010年設立の年金機構は「消えた年金」問題や職員の年金記録ののぞき見などで、信頼を失った年金行政の立て直しのシンボルだった。同機構は今回流出した情報のほかにも、電話番号や個人の所得を推測できる標準報酬月額、毎月の保険料額などの重要な個人情報も抱えている。それだけに信頼回復途上での今回の一件は政権にとって大きな痛手といえる。

安倍首相は年金問題に苦い経験がある。第1次内閣では約5000万件の年金記録漏れ問題が発覚し、支持率低下や07年参院選の敗北につながった。今回も対応を誤れば政府不信が強まり、今後の国会運営や内閣支持率に影響しかねない。

標的型メール、年金狙う 重要情報への攻撃巧妙化

日経新聞 2015/6/1

年金に関する 125 万件の個人情報流出した問題では、日本年金機構の複数の職員がウイルスが仕込まれたメールを開いて端末を感染させていた。今回のような「標的型メール攻撃」は官公庁や企業の重要情報を狙って急増し、業務上の連絡を装うなど手口も巧妙化している。専門家は「不審なメールは開封せず、自衛策が必要だ」と指摘している。

標的型メール攻撃はサイバー攻撃の一種だ。2011 年に表面化した三菱重工業への攻撃で注目された。業務連絡を装ったり、代金請求を装ったりしたメールを送りつけ、添付ファイルを開くとパソコンがウイルスに感染。不正プログラムによって攻撃者に特定の企業や組織のネットワークに侵入され、情報が抜き取られる恐れがある。

警察庁によると、企業を狙った標的型メールによる攻撃は 13 年が 492 件、14 年は上半期が 216 件だったが下半期は 1507 件に急増。計 1723 件となり、前年と比べて約 3.5 倍となった。防衛、製薬、鉄鋼などの業種が攻撃対象となっており、機密性の高い情報が狙われた可能性が高い。

14 年下半期には、商品代金請求などの連絡を装った英文メールが急増した。「ばらまき型」攻撃といわれ、大半の不正プログラムはセキュリティー対策ソフトで検知できるという。

攻撃の手口は巧妙で執拗になっている。情報処理推進機構（IPA）によると、事前に所属部署や氏名、担当業務を調べ、業務連絡のように装った件名や差出人名を使うケースが目立つという。顧客相談窓口にクレームを装ったメールを送ったり、幹部職員や監査役など社内関係者を名乗ったりする手口もある。

「就職活動をしているが、問い合わせ先はこちらでいいか」などと何回かメールのやりとりをしてからウイルスを送りつける「やりとり型」も出現している。

IPAが今年3月までに確認した標的型メール攻撃 939 件のうち、114 件（12%）は同じ攻撃グループが送信者の可能性が高いという。特定の9社を狙い、2年7カ月にわたって攻撃が続いていた。

警察庁は標的型メール対策として「面識のない送信者や心当たりのない件名のメールは開かずに削除する」「ウイルス対策ソフトを導入し更新する」などを推奨する。「重要」「至

急」と過度に強調するメールなどにも警戒が必要とされる。

I P Aの金野千里・技術ラボラトリー長は「日本年金機構は長期間にわたって狙われていた可能性がある。重要な情報を取り扱う組織は、社員らに心当たりのないメールの添付ファイルを開かないことを徹底させることが大事だ」と指摘する。

年金機構 125 万件流出 職員、ウイルスメール開封

日経新聞 2015/6/1

日本年金機構は1日、職員の端末がサイバー攻撃を受け、約125万件の年金情報が外部に流出したと発表した。いずれも加入者の基礎年金番号（3面きょうのことば）と氏名が含まれ、うち約5万2千件は生年月日や住所も流出した。国内の公的機関としては過去最大規模の情報流出。被害はさらに拡大する可能性もあり、国の情報管理のあり方に対する国民の不信が高まりそうだ。警視庁は不正アクセス禁止法違反容疑を視野に捜査する。（関連記事2、3、5面、社会面に）

個人情報流出し、謝罪する日本年金機構の水島理事長(中) ら（1日午後、厚労省）

機構は国からの委託で公的年金の保険料徴収や給付実務を担っている。今後、情報流出が確認された人の基礎年金番号を変更する。現時点では基幹システムである「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。

安倍晋三首相は「受給者のことを第一に考えて万全を期すよう塩崎恭久厚生労働相に指示した」と記者団に述べた。政府は関係府省庁でつくるサイバーセキュリティ対策推進会議を開き、情報の適正管理を指示した。社会保障と税の共通番号（マイナンバー）制度の導入を控え、政府は対策強化を迫られそうだ。

機構の水島藤一郎理事長は記者会見で「深くおわびする。誠に申し訳ない」と陳謝した。

機構によると、流出したのは年金記録を管理するため一人一人に割り当てられている基礎年金番号と氏名の計約125万件。このうち約116万7千件に生年月日、約5万2千件には住所と生年月日が含まれていた。番号は年金を受け取る権利の確認などに使われる。

学術機関の職員を装った電子メールに、セミナーの案内状と称したウイルス付きの文書

ファイルが添付されており、これを開封した少なくとも2人の機構職員の端末が感染した。端末同士をつなぐLANシステム内のファイル共有サーバーに保管されていた基礎年金番号や氏名などの情報が、ファイルごと抜き取られたとみられる。

年金受給額などを管理する社会保険オンラインシステムとLANシステムはつながっていない。

職員の端末がウイルスに感染していることが分かったのは5月8日。18日までに別の職員の端末も感染していることが確認され、翌日に警視庁に相談した。同月28日、同庁からの連絡で情報流出が判明した。

警視庁は公的機関の情報を狙った「標的型メール」が送られたとみて、不正アクセス禁止法違反容疑などを視野に調べる方針。ただウイルスの発信元が海外の場合、接続経路をたどるのは容易ではなく、難しい捜査を迫られそうだ。

機構は情報が流出した加入者に個別に連絡し謝罪する。これらの人から年金に関わる手続きの申請があった場合は本人確認をした上で対応する。専用電話窓口も設けた。

国や公的機関などがサイバー攻撃を受け、情報流出などの被害に遭うケースは後を絶たない。

農林水産省は12年1～4月に内部文書124点が流出した可能性があるとの調査結果を13年に明らかにした。環太平洋経済連携協定（TPP）交渉への参加をめぐる内部文書も含まれるとみられる。警視庁によると、09年以降、政府機関や防衛・重要インフラ関連企業など30以上がサイバー攻撃を受け、100台以上のパソコンでウイルス感染が確認された。

政府はサイバー犯罪対策を急いでいる。サイバーセキュリティ基本法が今年1月に全面施行。内閣に司令塔となるサイバーセキュリティ戦略本部を新設し、各省庁に防御策などを勧告する権限を持たせた。

情報流出で専用ダイヤル 日本年金機構が設置

日経新聞 2015/6/1

個人情報約125万件の流出を発表した日本年金機構は1日、不審な連絡があった場合などに、問い合わせに応じる専用電話窓口を設けた。電話番号は、フリーダイヤル（0120）818211。14日までの受付時間は、平日休日を問わず午前8時半～午後9時。15日以降の

受付時間は、日本年金機構のホームページで知らせる。〔共同〕

年金情報流出、身を守るには 不正に住所変更され洩れる恐れ／公的機関かたる電話に注意

朝日新聞 2015年6月5日



流出した情報は3パターンある／日本年金機構の対応

老後の暮らしを支える年金に関する個人情報日本年金機構から大量に流出し、問題になっています。どんな情報が漏れたのか、悪用の恐れはないのか、ポイントをまとめました。

Q 流出したのはどんな情報なの。

A 年金の受給者や加入者（現役世代）の情報だ。それぞれの基礎年金番号、氏名、生年月日、住所の4種類が流出した。番号と氏名だけ漏れた人もいれば、4種類全てが流出した人もいる。今のところ、合計で約125万件に上るとみられているんだ。

Q どうやって漏れたの。

A 5月8日から下旬にかけて、機構に多数の不審なメールが送りつけられた。2人の職員がメールに添付されていたファイルを開封するなどしてパソコンがウイルスに感染したのが原因だ。内閣サイバーセキュリティセンターは5月8日の時点で、機構から外部への異常な通信を検知して厚生労働省に連絡した。機構は最初に感染したパソコンはシステムから遮断したけれども、他のパソコンは外部と接続したままにしていたんだ。警視庁が5月28日に情報流出を確認するまで、流出には気づいていなかった。

Q 管理が甘いのでは？

A インターネットにつながっている端末で個人情報を扱える状態だったこと自体がお

かしいと指摘する専門家がいる。保存する情報にはパスワードを設定して、外部に漏れても簡単には中身を見られないよう管理する決まりもあったが、流出ファイルの大半には設定されていなかった。塩崎恭久厚労相は「備えが不十分だった」と謝罪したよ。

Q 基礎年金番号や氏名などのほか、給与や保険料の納付状況などのデータが流出した可能性はないの？

A そうした記録の本体は基幹システムで保存されていて、ウイルスが侵入したシステムとはつながっていない。機構は「不正アクセスは確認されていない」と説明している。

Q 流出した情報が悪用されるのが心配だけど……。

A 頭に浮かぶのは「なりすまし」だよね。本人に代わって年金の振込先を勝手に変更して引き出したり、給料などの情報をのぞき見したりする人が現れたら大変だ。ただし、年金機構はその心配はないと言っている。振込先の変更には金融機関の証明印なども必要で、流出した情報だけではできない。また、機構が年金相談を受け付ける際には写真付きの運転免許証などで必ず本人確認するので、万が一、なりすましを試みる人がいても、本人でないことは分かると説明しているよ。

Q 漏れた情報で住所変更はできると聞いたけど。

A 実はそのとおりで、年金受給者の住所変更は、届け出書に基礎年金番号、氏名、生年月日の3情報を記入して送付すればできる運用になっている。不正に住所が変更されると、新たな情報流出にもつながる。今後、情報が流出してしまった人から住所変更の届け出があったときは、本人確認を徹底して不正を防ぐと言っているよ。

■怪しい電話、すぐ切って

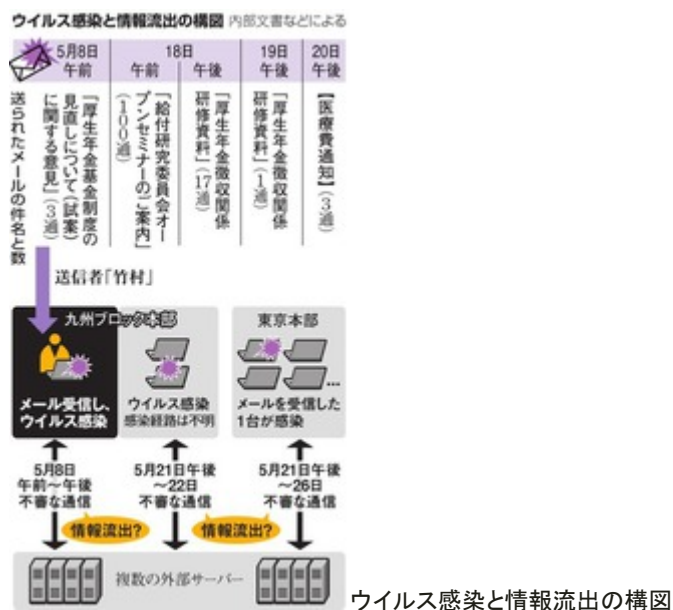
Q ほかに心配はないの。

A 大規模な情報流出がニュースになると便乗した不審な勧誘などが出てくる。公的機関をかたって「流出した名簿に名前が載っているのを削除してあげる」と持ちかけてお金を送らせたり、「あなたの情報が流出していないか確認している」などと言い、反対に個人情報聞き出そうとしたり。公的な機関が、そうした電話をすることはない。振り込め詐欺などに悪用される心配もあるので、怪しい電話を受けたら相手にしないですぐに切り警察や消費生活センターなどに相談しよう。

(中村靖三郎、兼田徳幸)

5月8日「竹村」からのメールで始まった 年金情報流出

朝日新聞 2015年6月5日



日本年金機構の専用電話窓口

☎ 0120・818211

午前8時半～午後9時(14日まで毎日)

- **機構側から情報流出の該当者に電話はありません**

15日からの受付時間は日本年金機構のホームページで知らせる。全国の年金事務所でも問い合わせに応じている

5月8日午前10時28分、日本年金機構九州ブロック本部(福岡市)の外部窓口のメールアドレスに、「竹村」という送信者から1通のメールが届いた。サイバー攻撃により個人情報大量に流出した事件は、ここから始まった。内部文書や関係者の証言などからウイルス感染と情報流出の経緯がわかってきた。

年金情報流出、厚労相の責任を野党追及へ

特集：年金情報流出

「竹村」のアドレスは、無料で取得できるヤフーのフリーメールアドレスだった。厚生年金基金制度の見直しに関する意見書を出したとの内容で、関連団体の「企業年金連絡協議会」を「企年協」と略すなど、年金事情をよく知る人物が装われていた。

職員がメール末尾にあったURL(アドレス)をクリックした。ウイルスの実行ファイルのダウンロードが始まった。パソコンが感染した。メール受信から21分後、午前10時49分だった。

すべてのパソコンには、ウイルス対策ソフトが入っていた。だが、このウイルスは、対

策ソフトで検出できない「新種」。解析結果などによると、感染したパソコンの利用者IDなど、まずは身近な情報を集めた。さらに、新たなウイルスが送り込まれた。これも新種で、このパソコンを本格的に乗っ取り、遠隔操作できるものだった。

ウイルスは、パソコン内で複数に分裂した。一つを削除しても復活する仕掛けが施されていた。これらのウイルスの動きによって外部のサーバーと通信した痕跡があり、他のパソコンに感染を広げるような動きもあったという。

外部との不審な通信に気づいたのは、政府の情報セキュリティ対策を担う「内閣サイバーセキュリティセンター」(NISC)だった。連絡を受けた機構は、感染したパソコンのケーブルを引き抜き、午後3時25分、通信を遮断した。

■ 2分間にメール100通

ウイルスの活動時間は約4時間半。NISCの通報で事態は収束したかに見えた。

だが、10日後、攻撃が始まる。18日午前9時51～52分の2分の間に、ウイルスが添付された不審なメール100通が一気に送りつけられた。「標的型メール攻撃」だ。職員個人など外部に公開していないアドレスにも届いた。機構の情報が外部に漏れたとみられる。

発信元のアドレスは8日のウイルス感染で使われたメールと同じだった。だが、画面に表示される「差出人」の名前は、実在する機構職員の名前に書き換えられていた。

メール攻撃は午後も続いた。「厚生年金徴収関係研修資料」という件名で17通。この日、届いたのは計117通に上り、事態を重く見た機構は、全職員に対し、メールの内容を具体的に記した注意喚起のメールを送った。感染が最初に発覚した8日も注意喚起を送っていたが、この時は具体的な不審メールの件名や文面など、参考になる情報を記載していなかった。

被害は止まらなかった。

21日、九州ブロック本部で外部サーバーと通信しているパソコン2台が新たに見つかった。うち1台は、8日に感染した職員に新たに貸与されたものだった。23日になり、今度は東京本部(東京都杉並区)で19台が外部サーバーと通信しているのが見つかった。管理を請け負っている大手IT企業から「東京の2台が外部に向けて大量の通信を始めた」と連絡を受け、判明した。機構は、本部のネット接続を遮断した。

この間に、情報が次々と流出したとみられる。

届いた不審なメールは計124通。この中から四つの新種ウイルスが見つかった。機構の調査で、この間に少なくとも27台のパソコンがウイルスに感染していた疑いが強い。

しかし原因が特定できたのは、最初に感染した九州ブロック本部の1台と、18～25日にウイルス付きのメールを開いて感染した東京本部のパソコンの計2台にとどまる。他がどうやって感染したかはまだわかっていない。