官の情報システム研究部会報告（20）
第 20 回：日本年金機構の個人情報流出事件の詳細と教訓

須藤龍也（すどう　たつや）
朝日新聞社

1. はじめに

2015 年 5 月に発生した，日本年金機構を狙ったサイバー攻撃は記憶に新しい．加入者の基礎年金番号や氏名，住所，生年月日といった約 125 万件の個人情報が外部に流出した，日本の政府関係機関を標的とした最大の個人情報流出事件である．日本年金機構と内閣サイバーセキュリティセンター（以下，NISC）は 3 カ月後の同年 8 月，それぞれ調査結果を公表した．インシデントの経過が詳細に記された異例とも言える内容で，今回の被害の深刻さを知ることができる大変貴重な資料である．

小稿では報告書などの公表資料に独自の取材結果や非公開の内部資料を交え，「その時，何が起きたのか」を検証する．なお，ここに書いた事実関係の一部は 2015 年 6 月 5 日付朝日新聞朝刊に掲載したが，その後の機構側の調査で事実関係や数字に修正が加えられている．その点をお断りしておきたい．

2. 3 段階の攻撃

まず，今回のサイバー攻撃がどのような流れで行われたのかについて述べる．

2.1　第 1 の攻撃

始まりは 1 通の不審なメールであった．

2015 年 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）のパソコン（PC）がメールを受信した．差出人名は「竹村」，送信元アドレスはヤフーのフリーメール（wstamn2001@yahoo.co.jp）．公表されている業務用アドレスに届いた（図 1）．

件名は「厚生年金基金制度の見直しについて（試案）に関する意見」．文末には「添付ファイルをご覧ください．」とあり，オンラインストレージサービス「Yahoo! ボックス」のリンク先 URL が書かれていた．

差出人：wstamn2001@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：Yahoo!ボックス

○○　○○ 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。
＊＊
Yahoo!ボックス
201505*******

図 1　不審メール

メールを受信した 21 分後の午前 10 時 49 分，年金機構職員が URL をクリック．ファイルがダウンロードされ，Word ファイルを偽装したウイルスが実行された．ウイルスは，外部の指令サーバー（以下，C&C サーバー）との接続を確認すると，C&C サーバーから別のウイルスをダウンロードした．

これは典型的な感染の手口である．まずは組織への侵入を目的とした必要最小限の機能を備えた「ダウンローダー」を送り込み，外部との通信を確立．その後 PC を乗っ取り，遠隔操作するウイルス本体にすり替わる．

NISC のその後の調査で，感染した PC から年金機構職員の一部，225 人分のメールアドレスをまとめた圧縮ファイルが見つかった．攻撃者は手に入れたメールアドレスを使い，後述する第 2 の攻撃を仕掛けたとみられる．

ウイルスは国内外 3 カ所の C&C サーバーと通信を繰り返したが，午後 3 時 25 分，この通信を検知した NISC の通報により，機構側が PC の LAN ケーブルを引き抜き，通信を遮断した．ウイルスの活動は約 4 時間半，続いた．このほか別の PC2 台でも同じ内容の不審メールを受信したが，感染しなかった．

機構内の PC にインストールされていたウイルス対策ソフトは，新種ウイルスのため検知しなかった．ソフトを作った大手情報セキュリティー会社は

PCに残っていたウイルス2種を見つけた．感染から1週間後の15日，「新種のウイルスは，外部に情報を漏洩するタイプではない」との解析結果を機構側に伝えた．

これを受けて機構はインシデントが収束したと判断し，調査を打ち切った．職員のアドレス流出がこの時判明していれば，次の攻撃があると予見できた可能性がある．

2.2　第2の攻撃：職員への不審メール

そして10日後の18日午前9時51分，再び不審メール99通（図2では100通とあるが，その後の調査で修正された）が九州ブロック本部に送りつけられた．発信元は8日のメールと同じアドレスだが，差出人の表記が「竹村」から「田中○○」と，実在する職員名に書き換えられていた．メールの宛先は機構職員の個人アドレスで，表記も漢字のフルネームが使われており，内部情報が攻撃者側に渡ったことが認められる．件名も「給付研究委員会オープンセミナーのご案内」と，年金関係者を装う内容であった．

メールにはLZH形式の圧縮ファイルが添付され，展開するとWord文書のアイコンで偽装されたウイルスの実行ファイル（exe）が現れた．このウイルスに感染したPCは3台．半日あまり，外部との通信を試みた形跡があるが，いずれも失敗に終わっている．

攻撃者はさらに，別のヤフーのフリーメール（kazuyiro@yahoo.co.jp）を使い，「山田○○」と実在の職員名を差出人に，「厚生年金徴収関係研修資料」という件名で，翌19日までに計20通（図2では17＋1通），職員個人のアドレスに不審メールを送った．この時は外部との通信は発生しておらず，添付ファイルを開封した職員はいなかったものと思われる．

いずれも職員の通報で不審メールの存在が発覚した．連絡を受けた機構側はメールからウイルスの検体を見つけ，情報セキュリティー会社に提供した．ただネットワークの遮断やPC内部の調査を行わなかったと，調査結果にはある．

2.3　第3の攻撃：東京本部へ

攻撃者は次に年金機構東京本部（杉並区）を狙った．機構とNISCの調査で，個人情報125万件の情報流出が判明した攻撃である．20日午後3時33分，外部に公開する機構への問い合わせアドレスに3通

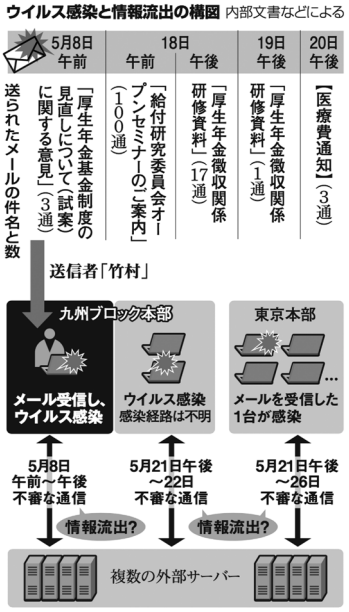

図2　サイバー攻撃の流れ（6月5日付朝日新聞朝刊から．本文の数字と一部ズレがある）

の不審メールを送りつけた．差出人名は「健康保険組合運営事務局」となっていた．

アドレスはこれまでのヤフーから，エキサイトのフリーメール（kenpo--web@excite.co.jp）に変わった．件名は「【医療費通知】」．「医療費通知のお知らせ」というLZH形式の圧縮ファイルが添付されていた．展開すると18日の手口と同じ，Word文書のアイコンを偽装したウイルスの実行ファイルが現れた．ファイルを開いた東京本部人事管理部のPC1台がウイルスに感染した．

内部資料によれば，攻撃者はウイルスがC&Cサーバーと通信を始めたのを確認すると，このPCを遠隔操作し，約30分後にはPCの管理者権限のIDとパスワードを手に入れた．翌21日にかけて東京ブロックのPC15台にウイルス感染が広がり，機構LANシステム（イントラネット）を介し九州ブロック本部のPC2台にも感染した．うち九州の1台は8日に感染した職員の代替機であった．8日の感染PCとコンピューター名，IPアドレスが同じであったため，容易に感染したとみられる．

感染したPC17台はいずれも管理者権限のIDとパスワードが共通していた．うち2台は24時間稼

働し続けるPCであった．これらが短時間で感染を広げる要因につながったと考えられる．

3．125万件の情報流出

情報流出は日本国内にある1カ所のC&Cサーバーを経由して行われた．東京都港区にある海運会社のウェブサーバーが乗っ取られ，水面下でC&Cサーバーに悪用された．

機構のPCがこのサーバーと通信を始めたのは，東京本部に不審なメールが送られて間もない21日午後4時ごろ．サーバーに向け大量のデータが送られるようになった翌22日午前には，23台のPCがウイルスに感染，遠隔操作され，うち20台が海運会社のサーバーと通信，機構LANシステムに接続された共有ファイルサーバー（以下，共有サーバー）に保存された個人情報を送っていたとみられる．

ここで共有サーバーの運用について述べる．

共有サーバーは機構LANシステムで結ばれ，東京本部と各地のブロック本部，年金事務所が利用する．「日本年金機構共有フォルダ運用要項」によれば，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うえで，業務上必要なデータについては，パスワードとアクセス制限の設定などを前提に取り扱いを認めている．業務の目的を果たした後は，速やかに個人情報を削除すると定めている．

年金加入者情報については，ネットに接続されていない年金基幹システムからDVDなど記録媒体にダウンロードし，必要に応じて加工のうえ，共有サーバーにコピーする運用が取られているという．

ところが今回の情報流出によって，こうしたルールが守られておらず，業務終了後も情報を削除していなかった事態が明らかになった．

今回情報流出した125万件にも，ルール違反のまま保存されていた情報が含まれる．内訳は▽パスワードもアクセス制御もない情報が2万件▽アクセス制御のみ53万件▽パスワード設定のみ2万件▽いずれも対策済み68万件，であった．

このほか機構内部の情報も流出した．各地の年金事務所の職員配置や業務マニュアル，共有サーバーのファイル名一覧などが圧縮ファイル形式でまとめられ，外部に送信された痕跡が認められる．

4．活動を抑制，そして収束へ

外部との通信が最も多かった22日午前，東京本部18台，九州ブロック本部2台のPCが海運会社のサーバーと通信していた．ところが正午をすぎた段階で通信するPCが6台まで減った．

一方で午後4時すぎ，情報を送り続けていた九州ブロックのPC2台が再び，8日と同じタイプのウイルスに感染した．海外にあるC&Cサーバー2カ所と通信を始めたところ，NISCが検知し，九州ブロック本部のネット接続を遮断した．

しかし，東京本部の活動は続いていた．翌23日午前1時すぎ，さらにPC1台が感染した．海運会社のサーバーに向けて通信を始め，別の1台と未明まで大量の通信を続けていたところ，ネットワークの監視を請け負っていた大手IT企業が検知，東京本部のネット接続を遮断した．これにより一連の攻撃は収束に向かうことになった．

この日は土曜日で，稼働していたPCが少なかった．無人のオフィスで特定のPCが大量の通信を外部と行っていた．サイバー攻撃被害に気づく有力な端緒の一つである．

5月28日，警視庁がこの海運会社のサーバーに保存されていた100万件超の個人情報を見つけたと機構側に連絡した．サイバー攻撃による不正アクセス被害はこれまで数多く起きているが，盗み取られた情報が外部のサーバーから見つかったことが公になった初めてのケースである．

攻撃者はあらかじめ年金分野を下調べするなど，用意周到ぶりがうかがえる．不審メールに使った件名や文面はいずれも，民間の企業年金の実務者らで構成する「企業年金連絡協議会」（以下，企年協）が会員向けに出した文書と酷似していた．

最初のメールは「厚生年金基金制度の見直しについて（試案）に関する意見」（5月8日）．企年協が2013年2月に会員向けウェブサイトに掲載した文章とほぼ同じ内容である．ただし，文中の日付と厚生労働省年金局の課長名が今年5月現在に書き換えられていた．年金機構職員あてに99通送りつけた「給付研究委員会オープンセミナーのご案内」（5月18日）も，2010年10月にサイトに掲載した文書とほぼ同じであった．

これらは企年協の会員しか見られない．攻撃者が

なぜ入手できたのか．経緯はわかっていない．

5．攻撃の背景

年金機構へのサイバー攻撃については，セキュリティー会社や専門家らの調査で，2014年以降本格化した日本国内を標的にした一連の攻撃の一つとみられている．以下，各社により呼称は異なるが，内容は一緒である．

・Cloudy Omega（Symantec）
・BLUE TERMITE（Kaspersky）

主な手口は「医療費通知のお知らせ」と題した不審メールが送りつけられ，Wordの文書ファイルのアイコンを偽装したウイルス実行ファイルが添付されているというのが特徴である．年金機構のインシデントと同じ手口である．

使われたウイルスも共通しており，「Emdivi」（エムディヴィ）と呼ばれる．特徴はC&Cサーバーの多くが日本国内にあり，ウイルスの感染も日本国内に限られるという点である．Kasperskyの調査では，C&Cサーバーの93%が国内にあり，Symantecは2014年11月の調査で，同じ国内クラウドホスティング事業者のサーバーが改ざんされ，C&Cサーバーにされていた，との共通点を挙げている．国内サーバーへのアクセスなら気づかれにくい，そんな攻撃者の狙いが読み取れる．

感染は国内の広範囲に及び，「政府関連」「情報通信産業」「化学・製造業」「防衛・航空宇宙産業」「金融」「報道機関」など（Kaspersky）．規模はわかっていないが，年金機構の情報流出発覚後，石油連盟や東京商工会議所，健康保険組合連合会，早稲田大学など数多くの団体，組織がサイバー攻撃による不正アクセス被害について発表した．いずれもメールによる感染など共通点は多く，警視庁の捜査で一連の攻撃によるものと断定された．

6．おわりに

日本年金機構を狙った今回の手口は，典型的な「標的型メール攻撃」である．攻撃者は，年金関連業務を装ったウイルス感染を引き起こすメールを執拗に送りつけ，容赦のない感染拡大と情報の窃取を行った．その裏で入念な準備と，攻撃で得られた情報を次の攻撃に活かす緻密さを重ね，125万件もの個人情報を盗み取った．

年金機構は批判にさらされた．だが果たして我が身に降りかかった時，メールを開けずに済むことができるだろうか．周囲を見渡せば，業務のために個人情報を一時的にとはいえ，誰でもアクセスできる状態で保存した人がいないだろうか．

インシデントから読み取れる教訓は多い．

年金機構へのサイバー攻撃は，最初の発生から16日間で計31台，のべ46台のPCがウイルスに感染し，国内外23カ所のC&Cサーバーが使われた．これだけ大規模なキャンペーン（作戦）は，もはや個人の手によるものと考えるのは無理があろう．

見つかった不審メールの文書ファイルは，中国語フォントや簡体字が使われている．一方で文書の日本語に不自然さは感じられない．

攻撃者は何者なのか．残念ながら，何一つわかっていない．これだけ痕跡を追うことができるにもかかわらず，である．

参考資料

［1］朝日新聞「新種ウイルス　送信者『竹村』」，2015年6月5日朝刊
［2］朝日新聞「年金団体文面と酷似」，2015年6月5日夕刊
［3］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結果報告について」，2015年8月20日
［4］内閣サイバーセキュリティセンター「日本年金機構における個人情報流出事案に関する原因究明調査結果」，2015年8月20日
［5］Kaspersky「BLUE TERMITE（ブルーターマイト）～日本を標的にするAPT攻撃」，2015年6月4日
［6］Symantec公式ブログ「Cloudy Omega攻撃」，2014年11月12日　http://www.symantec.com/connect/ja/blogs/cloudyomega

略歴

須藤　龍也（すどう　たつや）
1994年朝日新聞社入社，同社エンジニアとして新聞製作システムや選挙システムの開発に従事した後，1999年に記者職へ転向，2016年4月からサイバーセキュリティ担当の編集委員．