連 載

官の情報システム研究部会報告（19）
第 19 回：大量情報漏えいと情報セキュリティマネジメント

内田勝也 （うちだ　かつや）
情報セキュリティ大学院大学

1. はじめに

2015 年，日本年金機構への外部不正アクセスが発覚し，約 125 万件の個人情報が流出した．流出原因は，日本年金機構を狙った電子メールによる標的型攻撃である．

今回，日本年金機構というわが国において年金に係る一連の運営業務を担う組織（非公務員型の特殊法人）で発生した本事件を一つの契機として，官の組織全体が標的型攻撃に対する認識を改め，標的型攻撃への防止策の検討が求められている．小稿では本事件をもとにして，標的型攻撃に関する考察を情報セキュリティマネジメントの視点から行い，再発防止策を検討する点に狙いがある．

小稿では，まず今回の標的型攻撃について概観する．次に本事件の考察を通して，防止策の検討を行っていく．

2. 主要項目の考察

今回の日本年金機構の大量情報漏えいを，リスクやセキュリティの観点から考える．これは今回の事故は，技術的な問題よりも，セキュリティマネジメントの問題が遙かに大きいと考えるからである．

2.1 流出件数と日本年金機構の情報システム

今回の事件によって，流出した個人情報は約 125 万件であり，表 1 に示す内容である．

表 1　流出個人情報と各件数

流出した情報	件数（万件）
2 情報（基礎年金番号，氏名）	約 3.1
3 情報（上記 2 情報，生年月日）	約 116.7
4 情報（上記 3 情報，住所）	約 5.2
合　計	約 125.0

また，日本年金機構のシステムは，大きく 2 つあり，1 つは，基幹システムで，保険料や納付・支払い状況，氏名，生年月日等を保持し，他は職員の PC とネットワークで繋がり，職員の PC は外部とも繋がっていた．職員は，基幹システムから，個人年金情報を可搬媒体に書込み，サーバーにある共用ファイルに暗号化して保存することになっていた．

2.2 標的型メール攻撃について

「標的型」とは，不特定多数を対象にするのではなく，ある特定の対象を攻撃する．特定の組織を対象とするため，その組織の職員が興味を持つ言葉を使う，職員になりすますなどである．攻撃対象者の心理をうまく利用する，技術というより，「欺術」である．

この標的型攻撃には，メールメッセージに URL が書いてあり，それをクリックするとファイルをダウンロードするような指示があり，そのファイルをダウンロードする場合と添付ファイル付き電子メールが送られてきて，添付ファイルをクリックすると，添付ファイルに含まれているプログラムが起動するという 2 つの方法がある．

今回の標的型メール攻撃では，差出人は「フリーメール[1)]」アドレスを利用しているが，利用者のメールソフトによっては，図 1 に示すようにメールアドレスが見えないこともある．

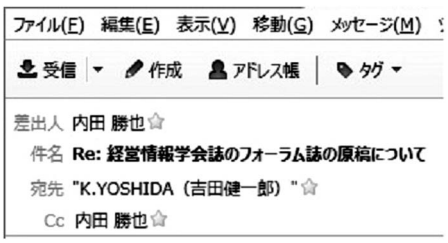

図 1　受信メールの例

「標的型攻撃」や「標的型メール」という言葉は，既に，2011年8月に出現しているが，横浜市では，2008年8月に標的型訓練[1]を行っており，9月に，NHK「ニュースウオッチ9」が「標的型攻撃メール」として，標的型添付メール攻撃の仕組みの解説や横浜市の訓練結果等についての報道を行っている．この報道の中では，中央官庁や国立大学に届いた標的型メールについても言及しており，標的型メールは国内でも決して新しいものではない．

標的型メール訓練は，上記横浜市や藤沢市が抜き打ち的な訓練を行い[2]，両市とも約40%の職員が添付ファイルやメール記載のURLをクリックした．内閣官房情報セキュリティセンターの訓練では，事前に訓練を行うとの情報を提供したが，添付メールは10.1%, URLでは，3.1%の職員がクリックした[3]．標的型メール攻撃に対し，100%完璧に防ぐことは難しいことがわかる．

今回の日本年金機構への標的型メールでは，フリーメールアドレスを使っているが，フリーメールアドレスが利用されるとは限らず，国内の組織等のメールアドレスで送られてくることもある．標的型メールの特徴を考えると標的型メールと一般メールの区別することは難しく，標的型メールをクリックする可能性が高い．

2.3 情報の共有化

5月8日に日本年金機構の九州ブロック本部でマルウェアが起動し，不正アクセスがあったが，内閣サイバーセキュリティセンターから連絡を受けた厚生労働省の係長は，日本年金機構にLANケーブルを抜くよう指示したが，17日間，係長が対応し，上司への報告はなかった[4]．厚生労働省ガイドラインでは，外部からウイルスメールなどの不正アクセスがあれば課長や室長に報告することが定められており，係長の内規違反の疑いもある[5]．

5月18日に，標的型メールが117通送付され，外部未公開のアドレスにも届き，一部のメールは「厚生年金徴収関係研修資料」というタイトルで送付された．更に，21日に九州ブロック本部，25日に東京本部のPCが外部サーバーとの通信が見つかり，管理を請け負っていた大手IT企業からの連絡を受け，本部のネット接続を遮断した．

大量の個人情報漏えいは，基幹システムから，基礎年金番号や氏名などの一部を可搬媒体にコピーし，年金事務所等の情報系サーバーやPCに保存していた．情報セキュリティポリシーでは情報の保存の際，パスワード設定をすることになっていたが，約55万件の情報にパスワードは未設定であった．

厚生労働省の担当部門も日本年金機構も，情報共有がされていない印象を受ける．係長が上司に報告したとの報道もあるが，報告の有無より，重要なチーム対応ができていない．

2.4 考察

人間は「関心がない」「1つの事に集中している」際などは，周りが見えない．実際，「見えないゴリラ」という心理学の実験では，ビデオをみても，多くの参加者はゴリラが見えない[6][7]．

また，係長が一人で対応し，組織として業務遂行をしていない．近年，医療分野や商用航空機内でのチーム活動は，患者や乗客の生命に影響があるため，教育・訓練等も行われている．Team STEPPSと呼ばれる教育・訓練では，①リーダーシップ，②状況モニタリング：上記「見えないゴリラ」等での体験，③相互支援：一度言って終わりでなく，重要な事柄については，最低，二度は言う，④コミュニケーション：気にかかる事柄を（1）Concerned（気になる），（2）Uncomfortable（不安），（3）a Safety issue（安全上の問題発生，中止を）のどの段階だと思っているのかをはっきり表現し，チーム作りの教育・訓練を行っている．

厚生労働省の係長が何故，上司に報告しなかったのかは不明であるが，21日に日本年金機構の九州ブロック本郡で外部サーバーとの通信が見つかっており，厚生労働省と日本年金機構が情報を共有し，対処していれば，被害は小さく済んだ可能性もある．

8日の時点で，マルウェアの対応を厚生労働省と日本年金機構で危機管理を発動していれば，個人情報の漏えいはなかったのではないだろうか．

125万件の内，40%以上の50万件のデータにパスワード等が未設定であった[8]．システム構築を行うICT部門や情報セキュリティ部門に，情報セキュリティポリシーでパスワード等の設定を決めたから，順守しない利用部門に問題があるとの意識があったのではないだろうか．個人情報に対し，パス

ワード等が未設定状態である可能性は，手作業処理を考えれば，情報セキュリティポリシー作成時に予想でき，パスワード等が未設定の個人情報がどの程度あるかを実施後，定期的に検証すべきであったといえる．さらに，40% 以上の個人情報があるのを知りながら，放置していたとしたら，セキュリティ上の責任放棄と言える．利用者は利便性が悪くても，利用者自身の問題と考える傾向がある [9]．

3. 防止策の検討

以上の事件の概要及び考察から，大量個人情報漏えいへの防止策を「電子メール」「パスワード設定」「マネジメント体制」の 3 つの視点から検討する．

3.1 電子メール

多くの職員が外部との送受信が必要な電子メールを持つ必要があるだろうか．問題を解決する方法には，(1) やめる／なくす，(2) できないようにする，(3) わかりやすくする，(4) やりやすくする等がある [10]．

日本年金機構内の電子メールの送受信は必要であっても，外部との送受信が不要であれば，内部のみの送受信可能な電子メールは，外部からのメールはブロックする．かつて，一部の国内大手銀行は，支店の営業担当者も通常の電子メールであったが，現在は利用できない．

外部との送受信が必要な職員には，標的型メールの教育・訓練を課し，1 回／四半期程度で実施すべきであるが，ゼロにはならないことも知っておく必要がある．標的型メール攻撃やフィッシングメールの周知を職員に行う必要がある．余り技術的でないものも官庁のウェブにもあるので活用すべきであろう [11]．

3.2 個人情報の転送とパスワード設定

基幹システムから，個人情報を可搬記録媒体で持ち出し，年金事務所等の情報系サーバーやパソコンに保存していたが，以下のような可能な情報セキュリティ対策を検討する必要がある．

①全ブロック本部で共通のものは，基幹システムで対応する

②年金事務所等の情報系サーバーへの保存は，自動的に暗号化して保存すれば，無権限者による情報漏えいを防ぐ

③基幹システムからの転送も可搬媒体でなく，暗号化してファイル転送を行う

3.3 情報セキュリティマネジメント体制の確立

日本年金機構や大企業の大量の個人情報漏えいが発生しており，発表資料やマスコミ情報等から検証しているが，リスク評価が行われていない．

情報セキュリティポリシーや業務遂行のためのチェックリストがあっても，見直し（修正ではない）がされていないことが多い．時間の経過や環境の変化があれば，リスクも変わる．システムは時間が経過すれば，当初と同じリスクでない．

今回の標的型メール攻撃は 2008 年に話題になっており，7 年前である．攻撃方法の変化に対応する教育・訓練やハードウェア／ソフトウェアの導入は，それらの情報を基に行う必要がある．情報セキュリティ対策は，ファッションではない（ポーズでやっていれば良いわけではない）．隣の組織で未導入でも自組織では必要になることもあり，その反対もある．

このような点を鑑み，日本年金機構等のような ICT 利用組織，しかも大量の個人情報を保有している官の組織では，情報セキュリティマネジメント体制の構築が必要になる．情報セキュリティ機器の導入，職員教育・訓練，情報セキュリティ計画の策定及び推進等を行う情報セキュリティマネジャーが必要であり，技術者は外部の力を借りることもできる．また，大規模情報漏えいが発生した多くの大企業の記者会見では，専門性を持った情報セキュリティマネジャーが，その事案（情報セキュリティプロジェクト）に対応していない点も課題であると判断できる．

情報セキュリティ技術者の出番ではなく，情報セキュリティマナジャーの出番なのだが，そのような専門家の育成が不十分であると感じる．

4. おわりに

今回の事案は，情報セキュリティマネジメント上の問題が遙かに大きく「情報セキュリティ≠技術セキュリティ」の観点から考察を行った．マルウェア

の動作，誰が作成したのかと言った日本年金機構の立場から不要と思われる考察等は省略し，誌面の都合で日本年金機構のシステムの全体像等も省略した．

また，標的型メールをクリックした職員や厚生労働省の係長等の問題でなく，情報セキュリティマネジメントを含めた組織体制の問題を考える必要がある．情報セキュリティマネジメント体制を構築できなければ，再発の可能性もあり得るであろう．

注

1） フリーメール：無料で提供される電子メールで，申込をすれば誰でも利用できるため，犯罪に利用されることもあるが，四六時中利用できる利便性があるため，所属組織のメールとは別に利用する人も多い．

参考資料

［1］山口健太郎，他『ユーザへの予防接種というアプローチによる標的型攻撃対策―2』情報処理学会第71回全国大会，https://www.ipsj.or.jp/award/9faeag0000004ej9-att/6E_4.pdf（平成27年6月30日最終アクセス）

［2］NHKクローズアップ現代『年金情報流出の衝撃～あなたは大丈夫？～』http://www.nhk.or.jp/gendai/kiroku/detail02_3665_all.html（平成27年6月30日最終アクセス）

［3］内閣官房情報セキュリティセンター『平成23年度標的型不審メール攻撃訓練結果の概要（中間報告）』http://www.nisc.go.jp/active/general/pdf/hyoutekigata_120119.pdf（平成27年6月30日最終アクセス）

［4］朝日新聞『年金機構攻撃，17日間幹部に知らせず係長以下が対応』http://www.asahi.com/articles/ASH653G5MH65UTFL007.html（平成27年6月30日最終アクセス）

［5］毎日新聞『年金情報流出：担当係長，内規違反の疑い』http://mainichi.jp/select/news/20150609k0000m040067000c.html（平成27年6月30日最終アクセス）

［6］クリストファー・チャプリス/ダニエル・シモンズ（著）木村博江（訳）『錯覚の科学　あなたの脳が大ウソをつく』文藝春秋，2011年，16–20ページ．

［7］Christopher Chabris/Daniel Simons『The Invisible Gorilla』http://www.theinvisiblegorilla.com/videos.html（平成27年6月30日最終アクセス）

［8］産経新聞『内規違反のずさん管理　55万件「パスワード設定せず」』http://www.sankei.com/affairs/news/150601/afr1506010046-n1.html（平成27年6月30日最終アクセス）

［9］D.A.ノーマン『誰のためのデザイン　認知科学者のデザイン原論』pp. 54–56 新曜社（2009年）

［10］河野龍太郎『医療におけるヒューマンエラー　なぜ間違える　どう防ぐ』医学書院，2006年，146–148ページ．

［11］政府広報オンライン：「あなたを狙う「標的型攻撃メール」「フィッシングメール」被害防止には一人一人の情報セキュリティ対策が重要です（2014年3月3日）」http://www.gov-online.go.jp/useful/article/201202/3.html

略歴

内田　勝也（うちだ　かつや）

1968年電気通信大学電気通信学部卒業，2006年中央大学大学院理工学研究科博士後期課程修了，博士（工学）．ITベンダーにて，COBOL開発等やユーザ／社員教育等やシステム監査／業務監査等を米系銀行にて推進し，中央大学でのセキュリティ関連の2プロジェクトの推進，情報セキュリティ大学院大学にて，情報セキュリティマネジメント，リスクマネジメント等の講座を担当し，横浜市CIO補佐監などを歴任．

2010年より，情報セキュリティ大学院大学名誉教授．