LAC ともに、イキル

2015 年 6 月 9 日

日本年金機構の情報漏えい事件から、我々が得られる教訓

本資料は、2015 年 6 月 1 日に日本年金機構が発表した、基礎年金番号を含む個人情報が漏えいした事件に関して、背景や想定される原因を、当社が知り得た範囲で整理し、対処方針など他山の石として学ぶべきことを提言するものです。

日本年金機構は、何らかの目的をもって攻撃を繰り返す犯罪者により、個人情報の窃取という被害を受けました。
攻撃は執拗かつ巧妙であると見られ、その手法は標的型サイバー攻撃という、限られた攻撃対象に対して特化された電子メールやウイルスを仕込んで行われたものでした。
本来は情報系システムとは切り離された基幹系システムで管理されている個人情報が窃取された原因は、日本年金機構内で行われていた業務手順により、情報系システムに個人情報がコピーされていたためでした。

情報を守るために切り離された 2 つのネットワークの使いにくさが、逆にセキュリティの弱さにつながったのです。

この事件から我々が取るべき行動は

1. 事件・事故前提の組織体制構築
2. 社員や職員の意識改革と教育
3. 事故対応チームの組織化
4. セキュリティ監視と不正通信の洗い出し
5. 事件発生を見越した演習

ではないか、と考え本資料にまとめました。

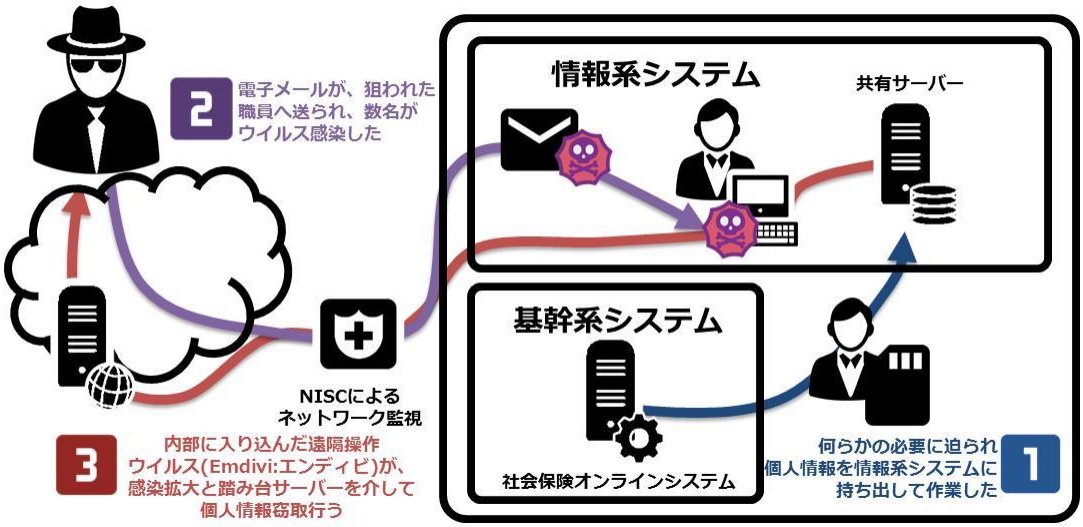
なお、本事件の技術調査などには、当社は一切関与しておりません。

事件の概要

本事件は、多くの報道でも指摘されているように、攻撃対象の組織や人を執拗に狙い撃ちにする「標的型サイバー攻撃[1]」と呼ばれる手段がきっかけとなり、引き起こされたものです。標的型サイバー攻撃は、2010 年 1 月に、米国の Google 社に対する事件により大きな話題となったもので、日本においても 2011 年後半に、大手重工メーカーや、衆参両院に対する事件により広く知られるようになりました。
（標的型サイバー攻撃に関する詳しい説明は、当社が公開している「日本における、標的型サイバー攻撃の事故実態調査レポート[2]」をお読みください。）

今回攻撃対象となった日本年金機構は、公的年金業務の適正な運営と国民の信頼の確保を図るため、2010 年 1 月に社会保険庁の業務の一部を引き継ぎ、特殊法人として設立されました。国民の年金に関する情報は、日本年金機構の社会保険オンラインシステム（基幹システム）で管理され、一般業務やメール、インターネット閲覧など外部との通信が可能ないわゆる情報系システムとは直接的に接続できない設定となっており、一般に「閉鎖ネットワーク」とみなされる状況でした。

今回の事件は、本来閉鎖ネットワークで厳重に管理されているべき基礎年金番号などの情報約 125 万件[3]（6 月 4 日現在公表されている件数）が、なぜか情報系システムに複製され、標的型サイバー攻撃を契機とした一連の攻撃により盗み出されたものです。



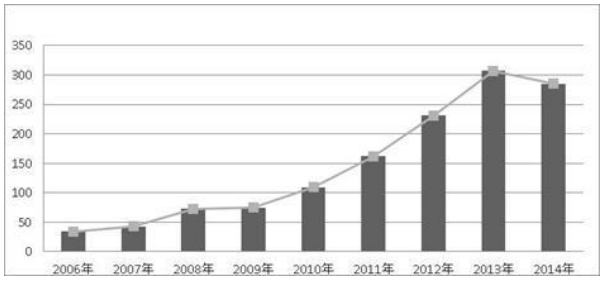
[1] 「高度標的型攻撃」または「APT 攻撃」とも呼ばれる

[2] http://www.lac.co.jp/security/report/2014/12/16_cgview_01.html

[3] http://www.nenkin.go.jp/n/data/service/0000150601ndjIleouIi.pdf

当社が考える事件の発生原因

本件のようなセキュリティ侵害事件は日常的に発生しています。当社が一年に対応する深刻な事故の背景にも、標的型サイバー攻撃の割合が増加している現実があります。

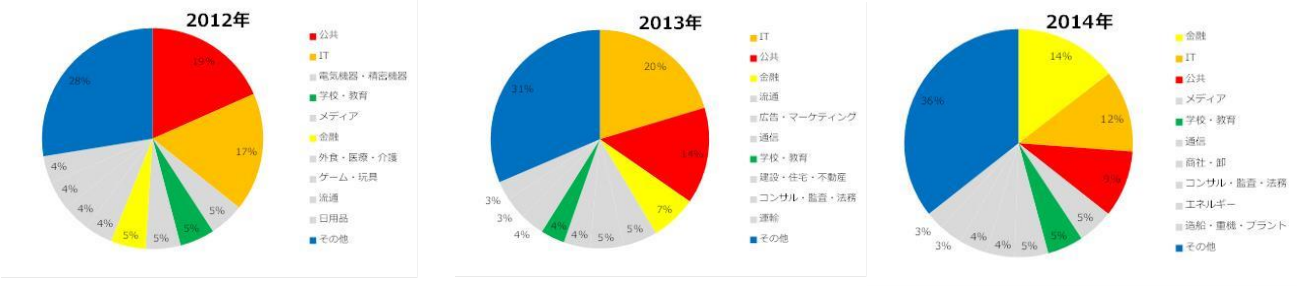


標的型サイバー攻撃による企業内への侵入行為と、情報窃取による被害発生は、当社が事故対応支援をした件数の 13%に上ります。（当社が公開している「サイバー事故現場からの手紙 vol.1[4]」をお読みください。）

外部からの不正侵入	ウイルス感染	標的型攻撃	IDの不正使用	USB等の不正持出し	その他
35%	29%	13%	12%	3%	9%

公共団体は狙われやすいという意識を持たなかった

本件が大きな衝撃をもって捉えられたのは、マイナンバー制度のスタートを目前に控えた段階での公共団体からの情報流出という深刻さと、125 万件という情報量の大きさによるものと考えられます。



公共団体は、国民の多くの個人情報を持っていることから、情報窃取により「不正収益を得る」、「社会的不安喚起の材料とする」など、攻撃者に多くの動機をもたらしていると考えられます。事実、当社に寄せられる事故対応要請の上位には公共団体が位置しています。

これは、公共団体のセキュリティ担当にとっては至極当たり前であると考えられていることが、組織全員にまでは浸透せず、理解が進んでいなかったためだと推測できます。

本件においても、百数十通送られた標的型攻撃メールを開いたのは、わずか数名といわれています。当社が提供する標的型攻撃対策訓練 「IT セキュリティ予防接種」においては、多い組織では約半数の方がメールを開いて添付ファイルを実行してしまうという結果が出ています。[5]つまり、本件においては多くの職員が攻撃を見抜き、回避したのです。問題は回避した職員はそのことを誰にも告げず、もしくは無視してしまったことにあります。

公共団体は攻撃の対象になりやすいことから特に必要なことですが、攻撃を認知した場合にしかるべき部門と共有する仕組みがあれば、もしかすると被害が抑制できていたかもしれません。

[4] http://www.lac.co.jp/security/report/2015/03/30_cec_01.html

[5] http://www.lac.co.jp/education/inoculation/index.html

実際の運用と、システムの実装がマッチしていない

公表されている情報によると、基幹系システムと情報系システムのネットワークは分離され、基幹系システムで管理されている基礎年金番号を含む個人情報には、容易にはアクセスできない仕組みになっていたとのことです。しかしながら、運用現場においては業務のために個人情報を DVD-R などの外部記憶媒体に保存し、情報系システムのファイルサーバーに複製していたとされています。この行為そのものが、今回の事件の根本的な問題であったことは間違いありません。

システムの設計に起因する使いにくさを、システムそのものの改善でなく、運用上の「工夫」により「使いやすく」活動すると、結果的にセキュリティ侵害を手助けとすることになります。作り上げたルールや仕組み、それに基づくシステム設計が、実際の運用環境にあっていない場合などに見られるこのような「工夫」は、システム設計における予算や期間の見積もりが甘かったことや、実際の業務を十分把握せず設計してしまったことにより生じるシステム上のリスクです。

ウイルス対策と標的型攻撃の対策の違いが理解されていない

各種報道によると、感染が発覚したきっかけは、2015 年 5 月 8 日に標的型サイバー攻撃により一台のコンピュータが感染したことでした。これは内閣サイバーセキュリティセンターによる監視・分析[6]活動の結果であり、その内容は厚生労働省を通じ日本年金機構に伝えられたとされています。この際、感染したコンピュータの特定が行われ、そのコンピュータを隔離し、ウイルス対策ベンダーによる解析が行われたとのことです。

また、それ以降も標的型サイバー攻撃が断続的に行われ、その結果多くのコンピュータが感染したとのことです。この執拗な攻撃行為が問題となり、警視庁への被害相談につながったものと考えられます。

攻撃行為があったことが把握でき、被害を受けたコンピュータが特定され、解析も進められ、最終的に警察組織への連携も図られた本対応に関して、何が問題だったのでしょうか。

端的に言うと、標的型サイバー攻撃の対応は、従来のウイルス対策とは全く逆のアプローチを取るべきと考えます。

無差別に攻撃を行い、人間の意思が深く入り込まない従来型のウイルスの場合、基本的に感染したコンピュータを隔離して分析、その結果を部内の他のコンピュータの調査に反映して感染駆除を行います。多くの場合、ウイルスの駆除により安心してしまい、それ以上の詳細分析は行われず、そのまま業務を継続することでしょう。

対して標的型サイバー攻撃では、たった一人への攻撃が成功した時点ですでに複数の人が感染し、複数のウイルスが入り込んでいる、と疑ってください。攻撃者は、最初の一台への攻撃が成功したあと、他のコンピュータへの再感染を試み、そしてこれまでに使用していたウイルスとは異なるウイルスに変更し、同様の調査では発見されにくくする工夫をします。そのため、最初に発見されたウイルスを調べても、巧妙に姿を変える遠隔操作ウイルスが組織内に入り込んだことを探し出す参考にはなりません。

[6] http://www.cas.go.jp/jp/gaiyou/jimu/nisc.html

	従来のウイルス感染の対応	標的型サイバー攻撃への対応
ウイルス感染コンピュータへの対処	ウイルス感染のチェックは、ウイルス対策ソフトで行い、駆除を行う。	感染したコンピュータの内部を詳細に分析するため、可能な限り操作や駆除作業は行わない。
ネットワークの稼働状況	そのまま運用を継続しても良い。	外部との通信を遮断して閉鎖環境にする。
ファイルサーバーやデータベースなどコンテンツサーバー	ウイルスなどの実行ファイルが保存されていないか、サーバー上でウイルスチェックする。	サーバーの稼動を停止し、情報窃取や不正ソフトの設置が行われていないかを確認する。
通信機器の動作確認	特に詳細な分析は行わなくても良い。	通信ログなどを分析し、接続先や送信データ分析の情報を得る。

ウイルス感染対応と標的型サイバー攻撃への対応の違い

標的型サイバー攻撃の対処としては、コンピュータの感染や不正な通信が見つかった段階で、その組織からの外部通信をすべて遮断し、遠隔操作ウイルスをネットワーク内に封じ込めます。これにより自動的に行われる破壊活動はとめられませんが、組織内の情報を窃取される危険は減ります。
遠隔操作ウイルスは、攻撃者に連絡を取ろうと通信を試みます。この動きを発見することで不正な動作をするコンピュータをすべて発見し、確実に駆除してゆくのです。（ネットワーク上の不正を発見するには、情報漏えいチェックサービス[7]のような特殊な調査が必要です。）

標的型サイバー攻撃と単純なウイルス感染の区別は非常に困難です。
標的型サイバー攻撃の対処は大掛かりな取り組みになります。業務に多大な影響が出るとともに、風評被害などの実害が想定されるため、経営層が十分な検討を行い、慎重に進めなければなりません。
たとえば、以下のような判断基準を平時の段階で検討しておき、ウイルス感染をきっかけとして標的型サイバー攻撃の対象になっているかどうかを判断するか、セキュリティ専門家への支援要請を行ってください。

- 攻撃に狙われる可能性のある企業である
  - 多くの個人情報を保管している
  - 企業の知名度、設計データなどの貴重な情報がある
  - 標的型サイバー攻撃に狙われやすい企業との取り引きがある。
- 感染経路に特徴がある
  - メール経由で感染し、その内容は本物としか思えない内容だった
  - Web 経由で感染し、いつも見に行くようなサイトだった
  - 感染した PC において普段利用したことがない USB や SD カードなどを使用した覚えがある
- 事故対応チーム、もしくはセキュリティ関連企業による調査結果から
  - ウイルス対策ソフトで検知できない
  - ウイルスが外部との通信を始める

[7] http://www.lac.co.jp/service/incident/forensic-dlp.html

本事件が社会に与える影響

当社は年間約 300 件の事故対応を行っており、標的型サイバー攻撃はその中で約 13%を占めています。すでに標的型サイバー攻撃は特殊な攻撃方法ではなく、本事件についても多くの犯罪の中のひとつの事例といえます。
本件で窃取されたとされる、基礎年金番号とそれに紐付く個人情報は、たとえば交通違反や犯罪情報、納税などの他の情報とリンクされるような社会生活におけるキーとなる情報ではないため、悪影響の範囲は限定的であると考えられます。
今回の事件をきっかけに、マイナンバーが不安視される傾向にありますが、マイナンバーで扱う個人情報の保護に対しては法律による厳しい基準が設けられています。そのため、いたずらに不安を感じる必要はなく、当社を含む専門家がしっかりと情報保護にかかわるべきと考えています。

実際に発生しうる影響としては、本件が大きく報道で取り上げられ国民の過度な不安をあおることにより、振り込み詐欺犯罪者などが犯罪の話題に本件を悪用することなどが想定されます。
もっとも大きな影響は、日本年金機構の窓口業務が当分の間混雑するなど、行政サービスの遅延ではないかと考えられます。

今回の報道により多くの国民が本件を深刻な事態であると認知するに至りました。組織や企業においては、職員や社員の意識改革、無理無駄のない安全な情報システムの構築、対策が非常に困難な標的型サイバー攻撃への対策という大きな課題が突きつけられた格好です。本件が大きく報道されたことで、多くの組織が事故の事実を公表しない方向に向かい、結果として対策を講じる上で貴重となる犯罪の手法などの情報が社会で共有できなくなることを懸念しています。

われわれは、標的型サイバー攻撃に対して、どのように対処すべきか

私たち IT を活用する立場としては、本件からどのような学びを得て、対処に活かすべきなのでしょうか。
多くの IT 管理者が苦労されている、実際の運用とシステムの実装との整合、ウイルスやネットワーク侵入といった脅威への対策については、この文書で整理するにはあまりに大きなテーマであり、各社の実情に合わせた取り組みを、システム開発者やセキュリティ会社のコンサルタントと議論すべきです。

1. 社員や職員の意識改革と教育

標的型サイバー攻撃への備えで重要なことは、これが特殊な攻撃方法ではなく日常的に行われている脅威だと認識することです。人間は、自分と関係がない、対岸の火事であると感じただけで内容を理解する扉を閉ざしてしまいます。このことについて、企業の経営者だけでなく、組織の構成員全員が同じ意識を持たなければなりません。標的型のサイバー攻撃は、いつも経営者に対して行われるのではなく、人事担当や総務、開発者、派遣社員などすべての人間が使うコンピュータが対象なのです。そしてわずか一人への攻撃が成功した時点で、攻撃者が組織全体を手に入れられる可能性があるのです。

2. 事件・事故前提の組織体制構築

標的型サイバー攻撃は、防ぐことはできません。アナログ時代には、筆跡や声色で本人確認ができました。しかしデジタル時代のコミュニケーションスタイルにおいて、無味乾燥なフォントは、誰が書いたか、誰が出したかを特定する情報にはなりえません。ウイルス対策ソフトは、一日に 100 万件近く[8]も生み出されるといわれるウイルスを全て防ぐことは困難です。脆弱性対策も、闇雲にソフトのアップデートをすることは別の互換性問題を引き起こすこともあるため慎重にならざるを得ません。もちろん、セキュリティ監視といったプロの取り組みにおいても、標的型サイバー攻撃を確実に発見することは困難です。

つまり、狙われた場合には避けることができないと考えたほうが論理的なのです。

では標的型サイバー攻撃を防げないとしたらどうするのか。被害を最小に抑え、重要な情報を窃取される前にゲートを閉じて原因を追究するのです。この姿勢を攻撃者に見せなければ、常につきまとわれることとなります。当社の調査[9]では、事故対応を完了した組織が、再度標的型サイバー攻撃を受ける割合が増加しているという傾向が判明しています。

（※事故発生後にセキュリティ監視を導入され、発見率が高まっているという可能性もあります）

2012年	2013年	2014年
8%	21%	28%

事故対応後に再度攻撃を受けた組織の割合

3. 事故対応チームの組織化

大企業やグローバル企業では増えていますが、CSIRT（事故対応チーム）を構築し、企業内で発生したセキュリティ事故を、管理・監督・統制する専任組織を維持することも重要です。

事故が発生した際に、当該部門、経営層、IT 部門、広報部門と連携し、問題を解きほぐし最小のダメージだけで切り抜けるには、お客様と会社のために常にニュートラルな立場でいられる組織が必要となります。

4. セキュリティ監視と不正通信の洗い出し

本件においても重要な役割を担ったのが、セキュリティ監視です。5 月 8 日に内閣サイバーセキュリティセンターが不正な通信を見つけていなければ、一連の被害は発覚していなかったと思います。セキュリティ監視は、セキュリティの見える化を進め、対策の羅針盤として機能する重要な役目を負っています。遠隔からセキュリティの専門家がネットワークを見張る仕組みは、今後の主流になると考えられます。

また、リアルタイムにセキュリティ状況を監視する場合、詳細な通信内容までを事細かく分析することは困難です。そのため、企業内部でどのような通信が流れ、その中に不正な通信がないかを見つける「人間ドック」のような棚卸し作業を行うことは、社内に潜む遠隔操作ウイルスをあぶり出すのに重要です。当社の実績として、企業内の通信を分析することで、ほぼすべての企業で何らかの不正な通信が検知され、過去に受けた標的型サイバー攻撃で残置されたウイルスなどを発見されており、定期的な不正通信の洗い出しを行うことが有効です。

[8] http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

[9] http://www.lac.co.jp/security/report/2015/03/30_cec_01.html

5. 演習

本件においても、職員が標的型サイバー攻撃を受けた際の行動が具体的に示され、避難訓練のように報告の仕方を経験していたならば、より早く危機管理部門への報告が行われていたと考えられます。また組織の上層部も事件・事故が発生した際の取り組みを理解し、社員に対して叱ることなく速やかな処理が行えたはずです。
災害や火災、盗難、そしてサイバーセキュリティといった犯罪に対しては、それを想定した演習を行い、各人の役割やプロセスを理解し経験させる必要があります。
標的型サイバー攻撃対策の演習や、社内システムに向けて攻撃が行われた際の防御技術の習得など、昨今注目を浴びている演習の機会を活用して、経験値を増やしてください。

まとめ

今回の事件は、日本国民として衝撃的なものです。私たちの情報を託している組織で行われていたずさんな管理に驚くとともに、危機感を持った方も多かったと想像します。

しかし、今回の事件は評価されてよい点がありました。
ひとつは、内閣サイバーセキュリティセンターが、初期の不正な行動を発見し、報告したことです。この発見と報告がなければ、その後の調査もすべて後手に回っていた可能性があります。
そして、日本年金機構においても、5 月 18 日に継続的な攻撃が行われていることを把握し、警視庁へ届出をする勇気を見せたことです。警視庁が動くことにより本事件は解明に向けて進展を見せました。今後のサイバー犯罪の抑止に対する大きな進歩につながると考えています。
そして、今回の立役者である警視庁の取り組みも、わが国国民として誇れるほどにすばらしいものでした。短期間に被害環境を調べ上げ、踏み台とされる他組織のサーバーを特定、確保、分析したのです。

IT はまだまだ未熟なところのある業界であり、犯罪に対しての十分な対応ができていないかもしれません。しかし本件のように事件を経験し、その知見を広く共有することで、情報管理全体のレベルが向上します。

当社は、事件の一部を見て批判するのではなく、IT を活用する全ての組織と連携し、より犯罪に対抗しうる人材とシステム、制度を作り上げることで、健全な IT の活用による豊かな社会を作り上げる取り組みを行っていきたいと考えております。

以上