LAC ともに、イキル

2015年8月31日

# 日本年金機構の事件報告を受けて、なすべき最低限の対策について

株式会社ラック
取締役専務執行役員　最高技術責任者
西本逸郎

2015年6月1日に発表された日本年金機構における個人情報流出事件は、他国による組織的犯行とも目される「標的型攻撃」の実態を私たちにまざまざと見せつけ、今後、国内のあらゆる組織がその脅威と戦い続けなければならない現実を突きつけました。

攻撃に備えるに際して参考となるのは、事件を検証するためにまとめられた3つの報告書です。8月20日には日本年金機構の「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」とサイバーセキュリティ戦略本部の「日本年金機構における個人情報流出事案に関わる原因究明調査結果」が、翌21日には厚生労働省の「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検証報告書」が公開されており、それらを注意深く読み解くことで私たちはさらに詳細な攻撃の実態を知ることができます。

中央官庁や行政サービス機関、安全保障に携わる組織、社会基盤を担う企業や日本をけん引する大企業は、この現実と社会的責任をよく理解し、すでに対策に取り掛かっています。一方、一般企業や地方自治体も攻撃の標的になっていることは関連した事件報道などからも明白ですが、多くの組織ではその当事者意識がなく、意識があっても予算がなく、予算はあっても人が足りず、人はいても運用できない現実に直面しつつも、他国からとおぼしき高度な組織的攻撃に対し、孤軍奮闘しなければなりません。

特に、マイナンバーの導入を控えた日本中の自治体においては待ったなしの対策が求められています。しかしながら、地方の自治体、学校、企業でのセキュリティ対策の実態は名ばかりで、当社は全国各地での講演や一般財団法人草の根サイバーセキュリティ運動全国連絡会（Grafsec-J）での活動などを通じ、攻撃の実態に即していない実情を見てきました。ましてや高度な標的型攻撃に対抗するには程遠い内容なのが現状です。

このような状況下で攻撃被害が発覚した際、事件への対応を誤ると社会的な制裁を受けるだけではなく、自治体の場合は住基ネットや LG-WAN（総合行政ネットワーク）から切り離され、業務を継続できなくなる事態にも陥りかねません。この状況を打開するには、現実を見据えたセキュリティ対策について地場のプロと共に取り組む「地産地消」のモデルを築くことです。ところが予算を確保し、例え一般的なレベルであっても標的型攻撃への対策を一般企業や地方自治体に要求したとしても、それをこなせるプロがいないのが現実です。そのためには各組織で段階を追って対策を推進していくことが肝となります。

ある面、追い込まれた状況にある地方自治体が今すぐ取り組むべき対策とは何なのか。その対策をどのように進めるのか。この難しい課題に対して、当社として支援できる具体的な提案を今後行っていきます。すでに当社では7月28日、標的型攻撃への対処法を網羅した「標的型攻撃　対策指南書（第1版）」を無料公開しました。対象としたのは、セキュリティの必要性があまり理解されていない、また、理解はしていても人的・予算的な問題から対策が進んでいない一般企業や地方自治体です。絵に描いた餅となりがちな理想論は盛り込まず、こうした組織でも実行できる施策を示していますので、まずはご覧ください。

さて、本題です。これまでの事件報道などから、標的型攻撃によるウイルスの侵入については、完全に防ぐことが困難なだけでなく、自分たちでは感染に気づくことすらできないことが明らかになっています。「気づけない」「防げない」のが現実ならば、侵入されたとしても被害を最小限に抑え込み、組織としてのガバナンスが適切に働いたことを証明できるようにするところから始めましょう。そのためには、１．ルール違反の放置（“割れ窓”）が発生しないように適切に管理し、それを経営レベルで監督する仕組みを構築すること、２．外部から何らかの異常を知らされたときに的確に対応できるよう、対処方法について十分理解して準備し、訓練を行っておくことがスタート地点となるでしょう。

また、標的型攻撃は高度な攻撃だけではなく、例えば低レベルの攻撃も混在させて組織を安心させ、その油断に付け込み侵入する機会をうかがい続けますので、１、２に併せて３．職員や従業員の「デジタル力」を向上させる教育を実施することも重要になります。

さらに、２においては自組織が被害を受けている場合だけではなく、自サイトが改ざんを受けたり指令サーバーが勝手に設置されたなど他の組織への攻撃拠点となっている疑念に関する連絡に対しても、予め経営レベルでその対応方針を決めておくことが重要です。攻撃を未だ気づいていない他組織の被害を抑え、攻撃者の狙いを暴くなど、特に公共機関においては極めて重要な対応となり、悪辣な攻撃者にみんなで対抗していく礎となります。

以上のことから当社は、地方自治体など向けに、地域のシステムインテグレーター様やデータセンターサービス事業者様と共に、次のようなセキュリティ対策を推進する仕組みを検討しています。

**① 理解と教育**

1） 標的型攻撃緊急対応マニュアルの提供

2） 基礎教育（基礎的な知識を説明するための教育コンテンツ）実施の支援

**② 演習や訓練**

1） 基礎訓練（標的型攻撃メール訓練や机上訓練）実施の支援

2） 自己点検（遠隔操作ウイルス感染などのチェック）に関する実施訓練の支援

3） 緊急対応演習の支援（需要に応じて）

**③ 監督・監査**

重要情報取り扱いチェックシートによる「割れ窓」チェックの実施支援

**④ 気づく・見つける**

1） 標的型攻撃健康診断（プロキシサーバーログの確認）の支援

2） 自己点検（遠隔操作ウイルス感染などのチェック）の実施支援

3） 簡易版セキュリティ監視（SecureNet®）の実装支援

4） 標的型攻撃監視(次世代ファイアウォールなど)の実装支援（需要に応じて）

**⑤ 防御・予防**

1） ネットワーク分離確認の支援

2） 重要情報取り扱いルール策定の支援

3） 各種セキュリティ対策の実施支援（需要に応じて）

以上