会員各位

平成 27 年 12 月 14 日

「今般の日本年金機構における個人情報流出事案を踏まえた金融庁からの要請
について」(平成 27 年 6 月 30 日 会長周知文書)に関する
会員各位の対応について(お知らせ)

常務理事 中 村 元 彦

平成 27 年 6 月 30 日に森会長名のお知らせ「今般の日本年金機構における個人情報流出事案を踏まえた金融庁からの要請について」が発出されており、会員に対して、情報セキュリティ管理態勢及びサイバーセキュリティ管理態勢を点検しつつ、通信記録(ログ)の取得・分析等を通じた情報漏洩の検知を含め、個人情報を含む重要情報の適正な管理を行うよう、要請されています。

これは、6 月 1 日に日本年金機構から公表された個人情報流出事案を受けた金融庁からの要請によるものであり、今般、会員各位の対応に当たっての参考情報として、IT 委員会実務指針第 4 号「公認会計士業務における情報セキュリティの指針」(以下「IT 実 4 号」という。)を中心に本要請に関連する項目について整理いたしましたので、改めてお知らせいたします。

コンピュータウィルス等による情報詐取の事案は増える一方であり、我々公認会計士は、その扱っている情報の重要性を再認識し、情報セキュリティ管理態勢・サイバーセキュリティ管理態勢に関する内部統制を見直し、一層向上させていくことが求められています。

会員各位におかれては、趣旨を理解の上、適切に対応いただきますようお願いいたします。

1. 日本年金機構の個人情報流出事案の概要と根本原因、再発防止策の提言内容

今回の要請に対応するためには、日本年金機構における個人情報流出事案の原因が何かを理解し、自らの状況に置き換えて考えてみるのが有用と思われます。また、特定された再発防止策も、参考になる事項があると思われます。

該当事案が発生した原因分析と対応策の検討結果は、日本年金機構、厚生労働省、内閣サイバーセキュリティセンターから、それぞれ公表されています。

このお知らせでは、厚生労働省から公表されている「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」(以下「報告書」という。)から概要を紹介します。

【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の概要】

<p>事案の概要 (報告書 P.16)</p>	<p>標的型メールを送付する手口によって機構 LAN システムが三段階にわたる標的型攻撃を受けた結果、共有フォルダに保管されていた大量の個人情報等が外部に流出してしまった。</p>
<p>第1段階の攻撃</p>	<p>2つの公開メールアドレス宛てに同一のアドレスから不審メール2通が送信され、受信した職員の一人がこれを開封し、メール本文に記載されていた URL のリンクをクリックしたことで、その端末に不正プログラムがダウンロードされ、外部との不正な通信が発生した。この通信は4時間にわたり続いたものの、発見され、不正プログラムは駆除された。</p> <p>内閣サイバーセキュリティセンターから日本年金機構へ不審な通信に関する通報がなされていたが、日本年金機構内で情報が伝達され、最終的にシステム担当者がこの通報を受け取るまでに2時間半を要した。また、全職員に対しての注意喚起が行われたものの、一般的な事項にとどまり、この攻撃の事実を引用した説明などはなされていなかった。</p>
<p>第2段階の攻撃</p>	<p>第1段階の攻撃から10日後、第1段階の時と同じ送信元アドレスから日本年金機構の職員個人のメールアドレス宛てに101通のメールが送られてきた。日本年金機構はこのメールについて受信拒否設定を行ったが、翌日には、別のメールアドレスから19通のメールが送られてきた。ここでも受信拒否設定を行ったが、同日の午後には、さらに別のメールアドレスから1通のメールが送られてきた。</p> <p>この一連の攻撃により、3台の端末がウィルスに感染したが、第1段階の攻撃の時に取った対策により、外部との不審な通信は行われなかった。</p> <p>日本年金機構は、全職員に対してこの攻撃の事実を引用した注意喚起を行ったが、メールを受信した職員に対する開封確認を行っておらず、3台の端末が感染したことも2週間気付かなかった。</p>
<p>第3段階の攻撃</p>	<p>第2段階の攻撃から2日後、新たな送信元アドレスから公開メールアドレス宛てに5通のメールが送られてきた。このメールを受信した日本年金機構の職員のうち1人がメールを開封し、添付ファイルを開いてしまったため、ウィルスに感染し、そこから26台の端末に感染が拡大してしまった。そして、感染から3日間、外部との不審な通信が行われ、共有フォルダに保存されていた大量の個人情報等が外部へ送信された。</p> <p>日本年金機構は、職員から不審なメールを受信したという報告を受けたものの、添付ファイルを開封していた事実は5日間経過する</p>

	<p>まで把握できなかった。また、外部との不審な通信も1週間把握することができなかった。</p>
<p>根本原因 (報告書 P.27)</p>	<p>日本年金機構、厚生労働省ともに、標的型攻撃の危険性に対する意識が不足しており、事前の人的体制と技術的な対応が不十分であったこと。</p> <p>インシデント発生後においては、現場と幹部の間、関連する組織間に(例えば、日本年金機構と厚生労働省、同一組織間の各部署、日本年金機構と運用委託会社など) 情報や危機感の共有がなく、組織が一体として危機に当たる体制になっておらず、その結果、組織内の専門知識を持つ者の動員ができず、担当者が幹部の明確な指揮を受けることもできないままに場当たりの対応に終始し、迅速かつ的確な対応ができなかったこと。</p>
<p>再発防止策の 提言 (報告書 P.33)</p>	<p>一部の者だけではなく組織が一体となった体制の整備、運用が必要である。</p> <p>日本年金機構等の役職員全員が標的型攻撃に対する危機意識を持つことが必要であり、今回の情報流出事件のもたらした結果の重大性と標的型攻撃の危険性を一部の職員だけではなく、日本年金機構全ての役職員が自分たちのこととして今後も認識し続けなければならない。</p> <p>標的型攻撃に際しては、組織が全体となってこれに対応する必要がある、それぞれの役職員が、これは自分の仕事ではないとか、自分の担当範囲でも従来通りのパターンを繰り返して漫然と対応するような姿勢ではなく、平素から困難に際し協力し合って逃げずに対処する組織作りを心がけるべきである。</p>

2. 会員各位における対応

上記の根本原因分析と再発防止策の提言内容を踏まえると、少なくとも、職員の意識、情報の管理態勢、インシデント発生時の対応方法については、それらが有効に機能しているのかも含めて再確認を行っておくことが重要と考えられます。

また、今回の標的型攻撃の状況や上記以外の個人情報漏洩事案を見ると、情報詐取を完全に防ぐことは難しく、それゆえ、いかに早く発見し、被害を最少にとどめるか、といった視点から考えることも有用と考えられます。

会員の事務所等の状況に応じた対応が必要となりますが、以下に具体的な対応に当たった考え方をまとめましたので、ご留意ください。

(1) 職員向け研修の実施状況・内容の確認・見直し

IT実4号 6「情報セキュリティに関する研修の実施」では「情報セキュリティ・ポリシーを正しく理解し、策定した情報セキュリティ対策に従って組織内部で

業務上使用する各種情報を適切に取り扱うためには、職員等に対する教育研修が不可欠である」とされています。

教育研修が不十分だと、情報セキュリティに対する意識が希薄になり、情報漏洩のリスク及びインシデント発生の可能性が非常に高くなると考えられます。

留意事項としては、例えば以下の事項が考えられます（IT実4号 6参照）。

- 外部環境・内部環境の変化に合わせて教育研修の内容が見直されているか。
- 定期的に教育研修が行われているか。

(2) 内部管理態勢の確認・見直し

公認会計士が業務上取り扱う情報を適切に管理するためには、経営者、情報セキュリティ担当者及び利用者が、果たすべき役割を正しく認識し、実行することが重要と考えられます（IT実4号 、、参照）。

自身の役割の認識が不十分、ないしは、実行できていない場合には、情報漏洩のリスクが非常に高まっていると考えられます。

留意事項としては、例えば以下の事項が考えられます（IT実4号 2～3、5参照）。

- 経営者、情報セキュリティ担当者、利用者は、自身の役割を正しく理解し、実行しているか。
- セキュリティ・ポリシーや規程等が正しく、意図されたとおりに運用されているか。
- 外部環境・内部環境の変化に合わせて内部管理態勢の見直しを行っているか。

なお、公認会計士・監査審査会から公表されている「監査事務所 検査結果事例集」（平成27年7月）では、次の問題点が挙げられています。

- 規程等の運用が行われていることを実態に踏み込んで確認しているか（形式的な確認にとどまっていないか）。

(3) 事案発生時の対応方法の確認・見直し

IT実4号 10「情報漏洩時の対応」では、「情報漏洩の可能性が生じた場合、当該情報の内容、範囲、原因を把握し、漏洩の拡大を防ぐとともに、当該情報の利害関係者の被害を最小限とする対策が必要となる」とされており。

万が一の場合を想定した対応方法が周知、理解されていない場合は、情報漏洩が発生しても気付かず、被害を拡大させるリスクがあります。

留意事項としては、例えば以下の事項が考えられます（IT実4号 3、10参照）。

- 事案発生時の対応を職員が理解しているか。
- 状況に合わせて対応方法の見直しを行っているか。

(4) 情報の整理、所在の把握

公認会計士が業務上取り扱う情報には、監査先の情報やそれらを記載した監査調書など、様々なものがあります。これらの情報はセキュリティ・ポリシーに従い、重要度に応じて分類され、管理することが有用と考えられます(IT実4号 参照)。

管理すべき情報が特定されていない、セキュリティ・ポリシーが実態に即していない、セキュリティ・ポリシーや細則に従った運用がなされていない、といった場合には、情報漏洩のリスクが非常に高まっていると考えられ、情報漏洩となった場合の影響は甚大になることが想定されます。

留意事項としては、例えば以下の事項が考えられます(IT実4号 1(1)～(3) 参照)。

- 情報が重要度に応じて分類されているか。
- 重要度に応じた管理方法が徹底されているか。
- 保管期限を超えた情報が廃棄されているか。

3 . 参考になるウェブサイト

IT委員会実務指針第4号「公認会計士業務における情報セキュリティの指針」

http://www.hp.jicpa.or.jp/specialized_field/main/34_13.html

日本年金機構の情報流出事案に関する報告書

・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書」

<http://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf>

・厚生労働省

「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」

<http://www.nenkin.go.jp/files/XtYrbhaJKiEk4.pdf>

・内閣サイバーセキュリティセンター

「日本年金機構の個人情報流出事案に関する原因究明調査結果」

http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

独立行政法人 情報処理推進機構 (IPA)

・情報セキュリティ安心相談窓口

<http://www.ipa.go.jp/security/anshin/index.html>

・情報セキュリティ対策

<https://www.ipa.go.jp/security/measures/index.html>

特定非営利活動法人 日本ネットワークセキュリティ協会

・情報セキュリティ対策

<http://www.jnsa.org/ikusei/>

以 上