

事 務 連 絡  
平成 27 年 7 月 17 日

各 都道府県 消費生活協同組合主管部（局） 御中

厚生労働省社会・援護局地域福祉課  
消費生活協同組合業務室

**【注意喚起】個人情報管理の更なる徹底について**

今般、厚生労働大臣認可消費生活協同組合に対し別紙のとおり通知したので、各都道府県におかれては、別紙を参考に貴管内組合に周知・徹底頂くとともに、その取扱いについて万全が期されるよう必要な支援をお願いいたします。

事 務 連 絡  
平成 27 年 7 月 17 日

各 厚生労働大臣認可 消費生活協同組合 御中

厚生労働省社会・援護局地域福祉課  
消費生活協同組合業務室

【注意喚起】個人情報管理の更なる徹底について

消費生活協同組合（以下「生協」という。）における個人情報の取扱いについては、先般の「日本年金機構における個人情報の流出事案を踏まえた対応について」（平成 27 年 6 月 4 日付け事務連絡。以下「事務連絡」という。）等を通じて、個人情報の流出防止などの安全確保措置の徹底をお願いしてきたところです。

しかしながら、先般、事務連絡を受けての当省所管生協の対応状況を確認した結果、各生協においては、サイバー攻撃に対してファイヤーウォールやウィルス対策ソフトの導入など、外部から組織に入り込まれないような対策（以下「入口対策」という。）が概ね講じられていることが認められた一方で、中には業務サーバー等からの外部への情報流出防止対策（以下「出口対策」という。）が全く講じられていない生協も見受けられたところです。

また、今なお新聞報道等で各種団体における情報漏えい事案等が報じられているところです。

一般的には、標的型攻撃に代表される、メールや外部メディア等で組織内部の従業員の端末や組織のシステム内部まで入り込むようなサイバー攻撃については、入口対策では防ぎきれない場合があることから、以下のような出口対策により、情報流出の防止を図ることが重要であるとされており、

- 1) 最重要部のインターネット直接接続の分離設計
- 2) 容量負荷監視による感染動作の検出
- 3) 重要攻撃目標サーバーの防護
- 4) 個人情報の含まれるデータの暗号化（パスワード付与） 等

※ セキュリティ問題の解決の参考として、詳細は、下記の（独）情報処理機構「新しいタイプの攻撃」の対策に向けた設計・運用ガイド」等を参照。

前述のとおり、各生協においては、入口対策だけでは限界があることから、ウイルス感染予防だけでなく、感染してしまうことを想定した上で、感染後の被害低減のために出口対策を含む「多層防御」について、下記参考にある（独）情報処理推進機構の情報を参考に、必要な対策を判断いただき、個人情報の流出防止に努めていただきますようお願いいたします。

【 参考 】

○独立行政法人 情報処理推進機構

- ・【注意喚起】 ウイルス感染を想定したセキュリティ対策と運用管理を  
<https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html>
- ・「新しいタイプの攻撃」の対策に向けた設計・運用ガイド改訂第2版  
<https://www.ipa.go.jp/files/000017308.pdf>
- ・「高度標的型攻撃」対策に向けたシステム設計ガイド  
<https://www.ipa.go.jp/files/000046236.pdf>
- ・情報セキュリティ 対策のしおり（全般）  
<http://www.ipa.go.jp/security/antivirus/shiori.html>

（以上）