平成27年12月25日開催
第72回運営委員会　資料2-2

（別紙2）

全国健康保険協会の端末における外部との不審な通信に関する事実確認結果と情報セキュリティ等の強化策について

平成 27 年 12 月 25 日

全国健康保険協会

１　はじめに

全国健康保険協会（以下「協会」といいます。）では、４台の職員端末が外部との不審な通信を行っていたことが本年6月16日に判明し、同17日に公表しました。

以下では、詳細な事実関係として個人情報の漏えいの有無及び不審通信を行っていた端末に保管されていた個人情報の内容についての確認結果並びに情報セキュリティ及び個人情報保護の強化策を報告します。

２　個人情報の漏えいの有無について

協会では、協会の通信記録や不審通信を行った端末などに対して二つの専門事業者の支援を得てデジタルフォレンジック調査の手法も用いた情報流出の有無の確認を行いましたが、個人情報の協会外部への漏えいは確認されませんでした。

３　４台の端末に保管されていた個人情報の内容について

外部と不審な通信を行っていた端末は、埼玉支部及び熊本支部並びに本部に置かれていたものです。個人情報の漏えいは確認されなかったものの、埼玉支部及び熊本支部の端末には協会加入者の約 70.7 万人分の個人情報がパスワードや暗号が設定されずに保管されていました。こうした取扱いは協会の内規上不適切なものです。

（本部の端末には協会加入者の個人情報は保管されていませんでした）

（１）本人識別情報の類型別の保存件数

	被保険者記号番号あり	被保険者記号番号なし
４情報（氏名・性別・生年月日・住所全て）	16 人分	23 人分
３情報（性別・生年月日・住所のうちいずれか２つと氏名）	約 18.2 万人分	約 0.6 万人分
２情報（性別・生年月日・住所のうちいずれか１つと氏名）	約 1.7 万人分	約 0.1 万人分
１情報（氏名）	約 49.9 万人分	約 0.3 万人分

（２）ファイルの種類

医療費通知管理簿、債権・支払、解散健康保険組合、レセプト抽出情報、その他

（３）被保険者記号番号・4 情報の他に保存されていた主な情報

事業所名、医療機関名、診療報酬点数、病名、債権額・支払額

４　情報セキュリティ及び個人情報保護の強化策について

今回の事案を踏まえ、協会としては、以下の対策を講じていくことにより、情報セキュリティ及び個人情報保護を強化し、協会加入者の皆様の個人情報を確実にお守りします。

（１）個人情報等の適正な管理と職員の教育

①　文書ファイルの自動暗号化システムの導入

27 年度中を目途に協会のシステム上で作成･保管する文書すべてを自動で暗号化するシステムを導入します。これにより、協会システム上に保管されている全ての文書ファイルは、暗号を解除しない限り協会システム外では閲覧ができなくなります。

②　情報管理関連規程の見直し

上記①の自動暗号化システムを前提にした情報管理関連規程の見直しを進めています。個人情報を含む重要情報の削除・廃棄も具体的なルールを設けます。

③　情報セキュリティ教育の見直しと訓練

本事案を踏まえ情報セキュリティ教育の内容の見直しを進めています。また、情報セキュリティインシデントを想定した職員に対する訓練も 12 月以降順次実施します。

④　情報セキュリティ点検・監査

役職員による情報セキュリティ自己点検を毎年度確実に実施します。また、内部監査・外部監査においても、内規の遵守状況や自己点検の実施状況を確認し、ルールの実効性を高めます。

（２）基幹系・情報系システムとは別システムによるインターネット接続（27 年度末目途より接続開始）

現在、協会のシステムはインターネット接続をせず、加入者の情報を保管する基幹系システムや通常業務に用いる情報系システムはインターネットから遮断されていますが、この状態を継続します。

インターネット接続については、基幹系・情報系システムとは分離した別のシステムを構築します。その際、情報セキュリティを高めるため、近年増加している標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を導入します。

（３）CSIRT の設置等インシデント対応の強化（（２）と同時期を目途にチームを設置）

① CSIRT の設置

現在のインシデント対応体制であるリスク管理委員会に加え、今後インシデント対応の体制を検討し、平時のインシデント発生時に向けた準備とインシデント発生時の対応を専任するシステム構築・運用とは独立した専門チーム（CSIRT: Computer Security Incident Response Team）の設置を準備しています。

② 新たな手順書の整備・訓練

上記①の CSIRT 体制の下で、現在あるインシデント発生時の報告手順に加え、新たな具体的な手順書を作成します。この手順書においては、攻撃認知段階での報告手順や、感染・攻撃拡大への対応手順、事後確認のための調査方法等の一連の手順を明示します。また、この手順書の下での訓練の実施も検討します。

（４）協会経営におけるリスク評価・管理の在り方の検討（28 年度事業計画に明記する予定）

現在災害対策を中心に進めている協会経営のリスク管理の在り方を見直し、本事案のように、事態が深刻化した場合に想定される被害が大きく、かつ協会に脆弱性のあるリスクを洗い出し、優先的に対応できる体制の検討を進めます。