資料2-1

6月17日に公表した全国健康保険協会の4台の職員端末の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

（概要）

平成27年12月25日

全国健康保険協会

１　個人情報漏えいの有無と４台の端末に保管されていた個人情報

○　協会の通信記録や不信通信を行った端末などに対する詳細な事実確認の結果、協会からの外部への個人情報の漏えいは確認されませんでした。

○　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並びに本部の4台の端末には、以下の約70.7万人分の協会加入者分の個人情報が暗号化やパスワードの設定なしに保管されていました。こうした扱いは協会の内規上不適切なものです。

	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

注１：ファイルの種類は、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

注２：他に保存されていた主な情報は、事業所名、医療機関名、診療報酬点数、病名、債権額・支払額

２　情報セキュリティ及び個人情報保護の強化策

今回の事案を踏まえ、以下の情報セキュリティ及び個人情報保護の強化策を実施していきます。

①　個人情報等の適正な管理と職員の教育

・　27 年度中を目途に文書ファイルの自動暗号化システムを導入。そのシステムを前提とした個人情報等の取扱いに関する協会内規の見直しを進めている

・　本事案を踏まえ情報セキュリティ教育の内容の見直しも進めており、職員に対する訓練も 12 月以降順次実施する予定

・　情報セキュリティの自己点検や内部監査・外部監査を確実に実施

②　基幹系・情報系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）

・　基幹系・情報系システムのインターネットからの遮断は継続

・　基幹系・情報系システムとは別個のインターネット接続システムを構築。構築に当たっては、標的型攻撃の侵入防止・早期検知・侵入範囲拡大防止等のための仕組みを導入

・　インターネット接続システムにも自動暗号化システムを導入（再掲）

③　協会の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）

・　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、システム構築・運用とは独立したインシデント対応の専門チーム（CSIRT: Computer Security Incident Response Team）設置を準備している

・　CSIRT 体制の下で、現在の報告手順に加え、感染・攻撃等への新たな対応手順書を整備

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）

・　災害対策を中心に進めている協会のリスク管理のあり方を見直し、より幅広いリスクへの対応の在り方を検討