

「公費負担医療給付システム」のマイナンバーに関する情報セキュリティについて

対象受検機関：健康医療部保健医療室地域保健課

事務事業の概要	検出事項	改善を求める事項(意見)				
<p>1 対象事務事業の概要</p> <p>(1) 公費負担医療給付システム（以下「給付システム」という。）は、健康医療部保健医療室地域保健課において、大阪府公費負担医療事務を支援するシステムである。</p> <p>(2) うち、小児慢性特定疾患医療及び療育医療受給者（政令市・中核市民を除く。）並びに特定医療費（指定難病）受給者について、マイナンバー情報を保有している。</p> <table border="1" data-bbox="299 583 1279 663"> <tr> <td>特定医療費（指定難病）受給者（難病認定G）</td> <td>50,000件</td> </tr> <tr> <td>小児慢性特定疾患医療費及び療育医療費受給者（母子G）</td> <td>4,000件</td> </tr> </table> <p>※療育医療費受給者の実績なし。</p> <p>(3) 健康医療部保健医療室地域保健課で、マイナンバーを取り扱う業務は、以下のとおりである。</p> <p>ア 保健所にて対象府民から『申請書』及びマイナンバーの『証拠書類』を受領し、地域保健課にて公費負担医療給付システムに申請内容を入力する。</p> <p>イ マイナンバーの登録業務は、次の2つの方法により行われている。</p> <p>① 『申請書』及び『マイナンバー証拠書類』に基づき、公費負担医療給付システムに対象府民のマイナンバーを入力する。</p> <p>② 府の住基ネット端末を利用して住基サーバから対象府民のマイナンバーのデータを取得し、公費負担医療給付システムに当該データを取り込む。</p> <p>(4) 平成28年度、庁内ネットワークから切り離し、個人番号利用事務ネットワークに移設するため、システム改修が行われた。</p> <p>2 平成29年度情報セキュリティ等監査の視点、着眼点</p> <p>(1) 保有するマイナンバー情報は最小限となっているか</p> <p>(2) マイナンバー情報へのアクセス可能者は、職務上必要な者のみとしているか</p> <p>(3) 不要なマイナンバー情報は、速やかに削除・廃棄しているか</p> <p>(4) 入力ミス等、人的なミスを防止する仕組みがあるか</p> <p>(5) 外部連携先や、大阪府内他システムに悪影響を与えない様、考慮されているか</p> <p>(6) 情報セキュリティに係る全庁的なルールは整備されているか</p> <p>(7) 各所属、IT・業務改革課、外部委託先の役割分担は適切か（特に、分担の漏れが生じたり、委託先任せになっていないか）</p> <p>3 実施方法と確認手法</p> <p>事前ヒアリングにより事業の概要等を調査した上で、質問票を作成し、受検機関に回答を求めた。</p> <p>平成29年度情報セキュリティ等監査の着眼点に基づき、監査手続を実施した。</p>	特定医療費（指定難病）受給者（難病認定G）	50,000件	小児慢性特定疾患医療費及び療育医療費受給者（母子G）	4,000件	<p>1 マイナンバーを取り扱う業務に係るシステム上の情報セキュリティについて</p> <p>(1) アクセス権限について、システム利用者別に設定する必要があるが、給付システムでは、端末ごとにアクセス権が設定されており、利用者別にアクセス権が設定できない。</p> <p>(2) パスワードの変更について、職務上必要なもの以外による不正なアクセス防止のため、システム利用者本人により、定期的かつ類推困難なものに変更可能とする必要があるが、給付システムでは、利用者本人によるパスワード変更がシステム上は可能であるものの、パスワードが端末に紐づいており、かつ複数の利用者で端末を共有していることから、実務上はパスワード変更ができない。</p> <p>(3) 入力されたマイナンバーの閲覧について、入力者であっても、事後で閲覧できなくする必要があるが、給付システムでは、同システム利用者であれば、誰でも閲覧可能であり、不正にマイナンバーを参照される可能性がある。</p> <p>ただし、事後的に確認作業を行う場合に備え、極めて限定された管理者のみ閲覧可能とし、当該管理者の操作ログを監視する仕組みが必要である。</p> <p>(4) 職員離席時において、第三者使用を防止するための機能を設定する必要があるが、給付システムでは機能がなく、かつパソコンのスクリーンセーバー機能を作動させることも困難であるため、職務上必要でないものが、不正なシステム操作によるマイナンバー情報へのアクセスが行われる可能性がある。</p> <p>(5) アクセスログについて、職員の権限でも、システム管理者等上位の権限で適時閲覧し、モニタリングできるようにする必要があるが、職員の権限ではログを参照できない仕組みとなっている。</p>	<p>1 給付システムにおける、(1) アクセス権限、(2)パスワードの変更、(3)入力されたマイナンバーの閲覧、(4)職員離席時における第三者使用防止機能、(5)アクセスログのモニタリング、(6)入力ミス等の人的なミスを防止する仕組みに関するシステム上の課題については、システム更新時に、費用対効果を勘案し、改善に取り組まれない。</p> <p>また、(7)ユーザー受入テストが可能な環境については、本番環境とは別に配置することについて検討されたい。</p> <p>2 マイナンバーに係る証拠書類等について、情報セキュリティの一層の強化のため、改善策を検討されたい。</p>
特定医療費（指定難病）受給者（難病認定G）	50,000件					
小児慢性特定疾患医療費及び療育医療費受給者（母子G）	4,000件					

	<p>(6) 入力ミス等、人的なミスを防止する仕組みについて、システム上、入力した人と別の人が確認するまでデータ確定しないようにする等、人的ミスを防止する仕組みを導入する必要があるが、給付システムでは、対象府民のマイナンバーを入力する場合、入力者1名で入力から確定まで可能となっているため、誤ったマイナンバー情報がシステムに登録される可能性がある。</p> <p>(7) 府のネットワークに本番環境を、ベンダ内に開発環境を配置していることから、府内でのユーザー受入テストができない可能性があるため、ユーザー受入テストが可能な環境の配置を検討すべきである。</p> <p>2 マイナンバーに係る証拠書類等について、職員のみが立ち入ることのできる区域内の常時施錠されたキャビネット等に保管する必要があるが、職員以外が立ち入ることができる区域の鍵付きキャビネットに保管されている。</p> <p>【個人情報の取扱い及び管理に関する要綱】 (適正管理)</p> <p>第12条 担当職員は、個人情報取扱事務において収集した個人情報の適切な管理を行うため、個人情報が記録された行政文書及び行政文書が記録された電磁的記録媒体を管理者が定めた原則施錠可能な保管庫等で保管しなければならない。特に、特定個人情報及び条例第7条第5項各号に規定する個人情報（センシティブ情報）が記録された行政文書については、厳重に保管しなければならない。</p> <p>2 管理者は、前項の保管庫等について、職員のみが立ち入ることのできる区域に設置する。</p>	
--	---	--

措置の内容

<p>1 本件給付システムの更新については、入札の結果、平成30年8月に契約を締結し、平成30年12月末までに新しいシステムの構築が完了したところである。 「改善を求める事項（意見）」(1)～(6)については、以下(1)～(6)のとおりシステムの改善を図った。また、「改善を求める事項（意見）」(7)については、以下(7)のとおりユーザー受入テストが可能な状況について、本番環境と別に配置することとした。</p> <p>(1)アクセス権限 ・新システムでは、システム利用者別にアクセス権の設定をできるようにした。</p> <p>(2)パスワードの変更 ・利用者別にパスワードの設定及び変更ができるようにした。</p>
--

・事前にシステムに設定した期間を超えると、パスワードの変更を促す仕組みとし、変更がされるまでシステムの利用ができなくなるようにした。

(3)入力されたマイナンバーの閲覧

・あらかじめ権限が付与されている利用者のみが閲覧可能とした。

(4)職員離席時における第三者使用防止機能

・離席後、一定時間端末を利用しない場合、システムはタイムアウトされ、かつ、端末はロック（スクリーンセーバーで設定）される設定とした。

(5)アクセスログのモニタリング

・新システムでは、ログ照会機能を有しており、各種条件でのログの検索が可能とした。

(6)入力ミス等の人的なミスを防止する仕組み

・申請入力されたデータに対し、入力者とは別の職員がチェックを行うことで確定する仕組みとした。

・システム上での誤入力があれば、エラーとして検出される仕組みとした。

(7)ユーザー受入テストが可能な環境（受託業者と調整のうえ、本番環境とは別の環境を確保）

・受託業者のデータセンターに設置している、テストサーバに環境が構築されており、クラウド経由で受入を実施する仕組みとした。

2 マイナンバーに係る証拠書類等については、執務室内など職員のみが立ち入ることのできる区域内にスペースを確保の上、鍵付きキャビネットに保管するなど、一層の保管体制の強化を図った。

監査（検査）実施年月日（委員：一年一月一日、事務局：平成29年8月25日から同年12月21日まで）