報道資料

平成 27 年９月 11 日
内閣官房内閣サイバーセキュリティセンター（NISC）

サイバーセキュリティ基本法第 27 条第３項に基づく勧告について

本日、「日本年金機構における個人情報流出事案に関する原因究明調査結果」（平成 27 年８月 20 日サイバーセキュリティ戦略本部決定）、「検証報告書」（平成 27 年８月 21 日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）等を踏まえ、サイバーセキュリティ戦略本部長から厚生労働大臣に対して、サイバーセキュリティ基本法第 27 条第３項に基づく勧告を行いました。

勧告の内容につきましては、別添を御覧ください。

（お問合せ先）
内閣官房内閣サイバーセキュリティセンター(NISC)
企画官　　櫻井　秀和
電話:03-3581-3959

（別添）
平成27年９月11日

厚 生 労 働 大 臣　　塩　崎　恭　久　殿

サイバーセキュリティ戦略本部長　菅　　義　偉

サイバーセキュリティ基本法第 27 条第３項の規定に基づき、別紙のとおり勧告する。

別紙

勧　　告

サイバーセキュリティ基本法（平成26年法律第104号）第25条第１項第３号の規定に基づく「日本年金機構における個人情報流出事案に関する原因究明調査結果」（平成27年８月20日サイバーセキュリティ戦略本部決定)、「検証報告書」（平成27年８月21日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）等を踏まえ、同法第27条第３項の規定に基づき、下記の所要の措置を講じるよう勧告する。

記

１　体制整備

（厚労省の体制）

(1) 厚生労働省（以下「厚労省」という。）は、人員・予算・業務・情報を管理する権限を有する最高情報セキュリティ責任者（CISO: Chief Information Security Officer）の下、情報セキュリティインシデント対応チーム（CSIRT: Computer Security Incident Response Team）の実効ある体制強化を含め、情報セキュリティ確保及び情報セキュリティ事案における対処のための省内体制を速やかに見直すこと。特に、担当部署等の役割・責任・権限を明確にするとともに、これら担当部署等の有機的な連携体制を構築すること。また、CSIRTの役割、窓口

等の必要事項を全職員に周知徹底すること。

（機構の体制）

(2) 厚労省は、日本年金機構（以下「機構」という。）において、すべての役職員の情報セキュリティに関する役割・責任・権限を明確にするとともに、組織の一体性を確保し、実効性のある情報セキュリティ対策を実現するための体制を構築するよう、監督すること。

（機構の CSIRT）

(3) 厚労省は、機構において、CSIRT を速やかに組織するよう、監督すること。

（厚労省と機構の連絡・連携体制）

(4) 厚労省は、機構との間において、情報セキュリティインシデント発生後の連絡・連携を迅速かつ的確に行うための体制を構築すること。

２　技術的対策

（厚労省と機構の情報システム等）

(1) 厚労省は、厚労省及び機構の情報システムにおいて、大量の個人情報や機微な情報を取り扱う業務に対してインターネット経由の攻撃が及ばないよう、情報システムの分離を確実に行うとともに、分離された情報システム内で業務が円滑に完結するよう情報システム設計・構築・運用及びルール徹底を行うとともに、機構においても同様の措置をとるよう、監督すること。

（機構の情報セキュリティ対策）

(2) 厚労省は、機構において、インターネットに接続された情報システムに対し、「政府機関の情報セキュリティ対策のための統一基準」（平

成 26 年５月 19 日情報セキュリティ政策会議決定）及び「高度サイバー攻撃対処のためのリスク評価のガイドライン」（平成 26 年６月 25 日情報セキュリティ対策推進会議策定）等において示されている対策と同等の多重防御の情報セキュリティ対策を講じるよう、監督すること。特に、ネットワークを管理する重要な機器を攻撃させないための情報システム設計・構築・運用を行うよう、監督すること。

（機構の運用管理対策）

(3) 厚労省は、機構において、セキュリティパッチの適用、管理者権限の適切な管理、ネットワークシステムの常時監視（モニタリング）等の運用管理対策（情報セキュリティに関する契約内容の具体化による外部委託先の適切な管理を含む）を講じるよう、監督すること。

（機構の外部情報セキュリティ監査）

(4) 厚労省は、機構において、内部監査とは異なる視点から問題点を把握するため、独立した外部の専門家による情報セキュリティ監査の実施を定期的・継続的に受け、結果を厚労省と共有するよう、監督すること。

３　教育・訓練

（厚労省の教育研修・訓練）

(1) 厚労省は、職員が、国民の個人情報を取り扱うことの責任を認識し、業務や組織、情報、システムに応じて定められている情報セキュリティ対策を理解した上で、役割に応じた責務を果たすべく、教育研修・訓練を定期的・継続的に実施すること。

（機構の教育研修）

(2) 厚労省は、機構において、役職員が、国民の個人情報を取り扱うことの責任を認識し、その役割に応じた情報セキュリティ対策に関する責務を果たすべく、教育研修を定期的・継続的に実施するよう、監督すること。

（機構の訓練）

(3) 厚労省は、機構において、役職員に対して、適切な情報セキュリティインシデント対応を可能とすべく、インシデントを想定した実践的な情報セキュリティ対策の訓練を定期的・継続的に実施するよう、監督すること。また、当該訓練内容には、厚労省の担当部署等との連携も含めるよう、監督すること。

（厚労省の職員の認識と所管法人等監督）

(4) 厚労省は、所掌の業務において機微な個人情報を含む多くの重要情報を取り扱っており、その適切な管理を国民から期待されていることを各職員に認識させるとともに、このような認識の共有を図りつつ、所管の法人等の指導監督にあたること。

4　成果の評価と報告

（機構の成果評価と報告）

(1) 厚労省及び機構は、当分の間、毎年度末及び必要に応じ、勧告の実施により得られた成果について、各々可能な限り客観的に評価をすること。また機構は評価結果について厚労省に報告すること。

（厚労省の報告）

(2) 厚労省は、上記の評価終了後速やかに、評価結果を含む本勧告の履行状況について、サイバーセキュリティ戦略本部長に報告すること。