○厚生労働省告示第二百十一号

個人情報の保護に関する法律（平成十五年法律第五十七号）第六条及び第八条、石炭鉱業年金基金法施行規則（昭和四十二年厚生省令第四十一号）第三十一条の二第二項、国民年金基金規則（平成二年厚生省令第五十八号）第五十一条の三第二項、確定拠出年金法施行規則（平成十三年厚生労働省令第百七十五号）第二十三条第七号、第二十四条第四号及び第六十条第六号、確定拠出年金運営管理機関に関する命令（平成十三年内閣府令第六号）第十条第九号、確定給付企業年金法施行規則（平成十四年厚生労働省令第二十二号）第八十五条の二第二項並びに公的年金制度の健全性及び信頼性の確保のための厚生年金保険法等の一部を改正する法律の施行に伴う厚生労働省関係省令の整備等及び経過措置に関する省令（平成二十六年厚生労働省令第二十号）第十七条の五第二項の規定に基づき、私的年金分野における個人情報の技術的安全管理措置を次のように定め、平成二十九年五月三十日から適用することとし、私的年金分野における個人情報保護に関するガイドライン（平成二十八年厚生労働省告示第二百九十号）は、同日をもって廃止する。

平成二十九年五月二十九日

厚生労働大臣　塩崎　恭久

私的年金分野における個人情報の技術的安全管理措置

## 第１　技術的安全管理措置

私的年金関係事業者（国民年金法（昭和三十四年法律第百四十一号）第百十五条に規定する国民年金基金、同法第百三十七条の二の五に規定する国民年金基金連合会、石炭鉱業年金基金法（昭和四十二年法律第百三十五条）第二条に規定する石炭鉱業年金基金及び当該石炭鉱業年金基金の会員たる事業主、確定給付企業年金法（平成十三年法律第五十号）第三条第一項第二号に規定する企業年金基金及び当該企業年金基金を実施する厚生年金適用事業所の事業主、同法第四条第一号に規定する事業主、同法第九十一条の二に規定する企業年金連合会、確定拠出年金法（平成十三年法律第八十八号）第二条第二項に規定する企業型年金を実施する厚生年金適用事業所の事業主及び同条第十項に規定する個人型年金加入者を使用する事業主、公的年金制度の健全性及び信頼性の確保のための厚生年金保険法等の一部を改正する法律（平成二十五年法律第六十三号。以下「平成二十五年改正法」という。）附則第三条第十一号に規定する存続厚生年金基金及び当該存続厚生年金基金が設立された適用事業所の事業主、同条第十三号に規定する存続連合会並びにこれらの者からその業務の委託を受けた者であって、個人情報の保護に関する法律（平成十五年法律第五十七号）第二条第五項に規定する個人情報取扱事業者（個人情報の保護に関する法律についてのガイドライン（通則編）（平成二十八年個人情報保護委員会告示第六号）８に規定する中小規模事業者を除く。）であるものをいう。以下同じ。）は、個人情報の保護に関する法律及び同法に基づく命令によるほか

、国民年金法、石炭鉱業年金基金法、確定給付企業年金法、確定拠出年金法、平成二十五年改正法附則第五条及び第三十八条の規定によりなおその効力を有するものとされた平成二十五年改正法第一条の規定による改正前の厚生年金保険法（昭和二十九年法律第百十五号。以下「改正前厚生年金保険法」という。）並びに関係法令の規定に基づき業務を実施する際には、その取り扱う個人データ（個人情報の保護に関する法律第二条第六項に規定する個人データをいう。以下同じ。）を適正に管理するために必要な措置を講ずるものとする。

その際、私的年金関係事業者において、個人データが漏えい、滅失又は毀損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況並びに個人データを記録した媒体の性質等に起因するリスクに応じ、漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講ずるものとする。

特に、事業者の内部又は外部からの不正行為による個人データの漏えい等を防止するための手法として、例えば次のような技術的安全管理措置を講ずること。

一　加入者等の個人情報を取り扱う基幹システムに接続されたネットワーク（基幹系ネットワーク）とインターネットに接続されたネットワーク（情報系ネットワーク）を物理的又は論理的に分離をすること。また、基幹システムに保管されている個人情報を直接取り扱う作業は、インターネットに接続されたパソコン等では行わないこと。また、業務に応じて適切なアクセス権限を付

与すること。

二　基幹システムにある個人データを外部の機関等へ電磁的方法により移送する場合は、暗号化・パスワードの設定等を必ず行い、原則として、インターネット等を介した電子メール等での送信は行わず電磁的記録媒体を使用し、又は専用線等のセキュリティが確保された通信を使用すること。また、作業に当たって一時的にパソコン等に個人情報を保存した場合は、作業終了後のデータ消去を徹底すること。

三　一及び二について運用上可能なものは直ちに実施するとともに、システム対応が必要となるものについては、システム改修を検討すること。なお、システム改修までの間、基幹システムにある個人情報を取り扱う場合、暗号化・パスワードの設定、作業終了後のパソコン等からの個人情報の消去等の安全管理措置を徹底すること。

（例）

・　個人データへのアクセスにおける識別と認証

・　個人データへのアクセス制御

・　個人データへのアクセス権限の管理

・　個人データへのアクセスや操作の記録及び不正が疑われる異常な記録の存否の定期的な確認

・　情報システムへの外部からのアクセス状況の監視及び当該監視システムの動作の定期的な確認

・　ソフトウェアに関する脆弱性対策（セキュリティパッチの適用、当該情報システム固有の脆弱性の発見及びその修正等）

第２　厚生労働大臣による必要な措置についての考え方

本告示に規定されている内容を遵守しない場合、厚生労働大臣は、国民年金法第百四十二条、石炭鉱業年金基金法第三十二条、確定給付企業年金法第百二条、確定拠出年金法第五十二条、第七十八条第二項及び第百四条並びに改正前厚生年金保険法第百七十九条の規定等に基づき、必要な措置を行うことがある。

第３　告示の見直しについて

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩、国際的動向等に応じて変わり得るものであり、本告示は、諸環境の変化を踏まえて、必要に応じ見直しを行うものとする。