（別紙）私的年金分野における個人情報の技術的安全管理措置Ｑ＆Ａ

【第１　技術的安全管理措置の規定（抜粋）】

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）

（１）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。」について

Ｑ１－１　基幹系ネットワークと情報系ネットワークを論理的に分離するには、具体的にどのようなことを行えば良いですか。

Ａ１－１　例えば、ＶＬＡＮ、Ｌ３スイッチ、ルータ、ファイアウォール等を用いてインターネットに接続されていない基幹系ネットワークとインターネットに接続されている情報系ネットワークを分離し、相互通信をできないようにすることが考えられます。なお、ファイアウォールやＬ３スイッチの設置等がなされていても、それらの設定内容と設置場所が適切ではなく、インターネットを通じてウイルス等が侵入を未然に防ぐことのできない構造になっている場合は論理的切断がされているとは認められません。

Ｑ１－２　基幹システムの範囲はどのシステムまで指すものですか。いわゆる自社のシステムだけを指すのか、資産管理契約等を結んでいる信託銀行等の管理するシステムも含まれますか。

Ａ１－２　内部イントラネットで接続されている等、当該会社からインターネットに接続することなくアクセスできるシステムであれば、基幹システムに当たります。

Ｑ１－３　「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）」とあるが、「インターネット」には社内イントラネットは含まれないという理解で良いでしょうか。

Ａ１－３　ご指摘の通り、当該規定中の「インターネット」には社内イントラネットは含まれません。

Ｑ１－４　通常業務に使用する職員用端末と年金個人情報を扱う個人情報取扱い端末を二つ持たなければならないのか。１つの端末で対応できないのか。

Ａ１－４　論理的分離はVLANやＬ３スイッチ、ルータ等によって基幹系ネットワークと情報系ネットワークを相互通信できないよう制御する機能でありますので、取扱端末は１つであっても、基幹系ネットワークと情報系ネットワークとで接続する度に接続先を適切に切り替えていただければ可能であります。また論理的分離の導入が困難な機関に関しましては、インターネットに接続されていない共用の個人情報取扱用端末を１つ以上確保していただき、個人情報を取り扱うときのみ前述の専用端末を使用する方法で物理的分離を図ることも可能です。

（２）一「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。」について

Ｑ２－１　インターネットからの切断については、物理的切断だけでなくファイアウォールなどの論理的切断も認められますか。

Ａ２－１　適切に論理的切断がなされており、インターネットに接続できない状態になっていれば、個人情報を取り扱うことは認められます。スイッチ制御等によりインターネットとの接続の可否が制御されているパソコンの場合は、スイッチ制御によりインターネットと接続できない状態においては個人情報を取り扱うことができますが、インターネットと接続できる状態においては「インターネットに接続されたパソコン」に該当し、個人情報を取扱うことは認められません。

Ｑ２－２　本告示以外の方法であっても、不正アクセスを遮断し、外部流出を防ぐ手立てを講じることで個人情報の十分な安全管理措置が講じられると考えるが、本告示以外の方法でもその理解でよいか。

Ａ２－２　本規定は不正アクセスを遮断し、外部流出を防ぐ手立てを講じるための適切な例を提示したものであり、本規定と同等以上のセキュリティが担保される他の方法で対策を講じることも認められます。その際は、当該方法が不正アクセスを遮断し、外部流出を防ぐ手段として適切であるか専門家の意見等を踏まえ、適切に対応してください。

Ｑ２－３　「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。」と規定されていますが、以下のような行為は認められますか。

①　パソコンがインターネットに接続されている状態で、基幹システムのデータをダウンロード若しくは編集する行為又は基幹システムにデータをアップロードする行為。

②　パソコンがインターネットに接続されていない状態で基幹システムからデータをダウンロードし、スイッチ制御等によりインターネットに接続された状態になった後に当該情報を使用して業務に必要な作業を行なうこと。

③　パソコンがインターネットに接続されている状態で、業務に必要な作業として作成や編集を行った個人情報をパソコンがインターネットに接続されていない状態でアップロードする行為（アップロード後、当該情報は削除する）。

Ａ２－３　①は認められませんが、②と③は認められます。なお、②と③を行う

場合は、作業終了後は速やかに情報を削除し、必要に応じて情報の取扱記録を残す等、個人情報の安全な管理を徹底してください。

Ｑ２－４　テレワーク環境において、基幹システムに保管されている個人情報を取り扱うことは可能ですか。

Ａ２－４　テレワーク環境において個人情報を直接取り扱う場合には、以下の要件を全て満たしている必要があります。ただし、特定個人情報を取り扱うことは認められません。

・ＩＤ・パスワード等によるアクセス制限、通信暗号化等により仮想の専用線が構築されている（ＶＰＮ接続等）。
・基幹システムに接続している間は、ＰＣ内のブラウザ等による外部インターネットへの接続ができない状態になっている。

具体的な方法については、「テレワークセキュリティガイドライン第５版」（令和３年５月総務省）や「テレワークの適切な導入及び実施の推進のためのガイドライン」（令和３年３月 25 日厚生労働省）に挙げられている各種対策を参考に、適切なセキュリティ対策が講じられているか専門家の意見等を踏まえながら、適切に対応してください。

なお、テレワークの実施に当たっては、上記ガイドラインを踏まえ、技術面のほか、組織面・運用面からもテレワークにおける情報セキュリティリスクを適切に評価し、必要な対策を実施していただくことが重要です。

（３）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する、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。」について

Ｑ３－１　送信する情報が僅少である場合は電子メールでの送信も認められるか。

Ａ３－１　送信する情報が僅少であっても、原則、インターネット等を介した電子メール等での送信は控えてください。なお、郵送により送付する方法は認められます。

Ｑ３－２　即時に情報伝達を行う必要があり、電磁的記録媒体による個人データの授受が行えない場合、例外的に暗号化・パスワード等の設定を行ったうえでインターネット等を介した電子メールで送信することも認められますか。

Ａ３－２　必要性・緊急性が高くやむをえない場合等は、例外的に電子メールでの送信も認められますが、本文には個人情報を記載せず、添付ファイルに暗号化・パスワードの設定を行い、作業終了後は速やかに情報を削除すること、取扱記録を残すこと等を行って、個人情報の安全な管理を徹底してください。

Ｑ３－３　「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する、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」とあるが、規定された手法を取り得ない環境であれば、暗号化・パスワード等の設定を必ず行ったうえでインターネット等を介した電子メールでの送信も認められるのか確認したい。

Ａ３－３　僅少であるとしても情報漏えいの可能性があるため、不可です。郵送などによる対応が求められます。

Ｑ３－３－１　改正された個人情報の保護に関する法律（以下「改正個人情報保護法」という。）第 33 条の規定に基づく本人情報の開示請求において、電磁的記録の提供方法として電子メールによる送付を要望されたが、個人データを当該本人に対して、インターネット等を介した電子メールに添付して送信してよいか。

Ａ３－３－１　「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）」において、電磁的記録の提供による方法についてはできる限り本人の要望に沿った形で対応することが望ましいとされ、具体的方法の事例として、電磁的記録を電子メールに添付して送信する方法が示されています。

このため、改正個人情報保護法等の要請に基づく対応であることから、本告示にかかわらず、開示請求において本人からの要望があったときに、当該本人の個人データを、電子メールに添付して送信することは差し支えありません。

なお、電子メールの送信に際して、誤送付等に伴う情報漏えいのリスクの低減を図る観点から、以下に示すような対策を講じることが望まれます。

①　確認メールを送信するなどして、申出のあったメールアドレスの真正性を事前に確認した上で、個人データを送信する。

②　電子メールに添付する個人データは、必要に応じ暗号化して送信する。

③　メール送信のために、インターネットに接続されたパソコンに一時的に保存した個人データは、メール送信後、確実に消去する。

Ｑ３－３－２　加入員原簿の閲覧等にあたり、本人から電子メールによる送付を要望されたが、個人データを当該本人に対して、インターネット等を介した電子メールに添付して送信してよいか。

Ａ３－３－２　「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）」において、電磁的記録の提供による方法についてはできる限り本人の要望に沿った形で対応することが望ましいとされ、具体的方法の事例として、電磁的記録を電子メールに添付して送信する方法が示されています。

また、「往訪閲覧縦覧規制」を定める法令等の規定について、規制の点検・見直しが行われ、加入員原簿の閲覧等については、デジタルに適合した方法で行うことが可能とされました。

これらを踏まえ、本告示にかかわらず、加入員原簿の閲覧等について、本人から要望があったときに、改正個人情報保護法第 33 条の規定に基づく本人情報の開示請求に準じる対応として、当該本人の個人データを電子メールに添付して送信することは差し支えありません。

なお、電子メールの送信に際して、誤送付等に伴う情報漏えいのリスクの低減を図る観点から、以下に示すような対策を講じることが望まれます。

① 確認メールを送信するなどして、申出のあったメールアドレスの真正性を事前に確認した上で、個人データを送信する。

② 電子メールに添付する個人データは、必要に応じ暗号化して送信する。

③ メール送信のために、インターネットに接続されたパソコンに一時的に保存した個人データは、メール送信後、確実に消去する。

Ｑ３－４　個人情報を、国税関係では e-Tax、地方税関係では eLTax を使って送付することがあるが、これは本告示上、問題ありませんか。

Ａ３－４　問題ありません。

Ｑ３－５　個人情報の暗号化・パスワードの設定が行えないものの、電子認証等により端末・利用者を限定した専用画面から、専用回線等のセキュリティが確保された通信経路を使用する等、当該規定と同等以上のセキュリティが担保される方法によって個人情報を移送することは可能ですか。

Ａ３－５　当該規定の方法と同等以上のセキュリティが担保される方法であれば可能です。例えば、インターネットバンク等で行われているように、インターネット側からは基幹系ネットワークに直接接続されておらず、コピー情報を扱う方法は認められます。

Ｑ３－６　「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」と規定されているが、「専用線等」とはどのような回線が認められますか。

Ａ３－６　「専用線等」とは、一義的に盗聴や改ざん等の第三者からの介入を排除した通信であり、インターネットに接続されていないネットワーク網とし

て利用されているもの（専用線、公衆網、閉域 IP 通信網）を指します。

また、インターネットを利用した接続の場合においても Internet-VPN サービスのような通信経路の暗号化、あるいは TLS のような暗号化通信手法であれば「専用線等」として認められますが、適切な接続が行われていなければ（例えば、他の対策を施さず、いわゆるフリーWi-Fi 等を経由してインターネットへ接続する等）、暗号化の過程で盗聴等のリスクがあることから、「専用線等」としては認められません。

Ｑ３－７　「企業年金等に関する特定個人情報の取扱いについて」（平成 27 年 10 月５日年発 1005 第２号）の記載と同様に、「暗号化・パスワードの設定等」の記載については、「暗号化又はパスワードの設定等」という解釈で良いですか。

Ａ３－７　問題ありません。

※参考　「企業年金等に関する特定個人情報の取扱いについて」（平成 27 年 10 月５日年発 1005 第２号）

第二　安全管理措置について

一　（略）

(1)　企年連、国基連又は企業年金等が特定個人情報等を取り扱う場合にあっては、以下の通りとすること。

①　（略）

②　特定個人情報等を電子計算機上で保存するにあたっては、当該情報の暗号化又はパスワードの付与を行った上で保存すること。また、当該パスワードは定期的に変更すること。

③　（略）

④　特定個人情報等の保存について、電子媒体に記録し、保存する場合にあっては、当該情報の暗号化又はパスワードの付与を行った上で保存するとともに、鍵のついた金庫に保管する等、外部から遮断できる環境において保管し、当該保管状況について、事務取扱担当者が一週間に一回等実情に合わせた定期的な確認をするものとすること。また、当該パスワードは定期的に変更すること。

(2)　企年連、国基連又は企業年金等が本人以外の者に対して、電子媒体、通信又は書面を用いて、特定個人情報等の送付を行う場合、以下の取扱いとすること。

①　電子媒体を用いる場合には、保存する特定個人情報等の暗号化又はパスワードの付与を行い、かつ、当該電子媒体の紛失を防ぐため、施錠できる搬送容器を使用する等の措置を講じた上で、送付履

歴が分かるようにすること。

② 通信を用いる場合には、送信する特定個人情報等について暗号化又はパスワードの設定を付した上で、電子メール等での送信は行わず、専用回線等のセキュリティが確保された通信経路を使用すること。セキュリティが確保された通信経路は以下のものが考えられる。

（略）

③ （略）

（４）二「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。」について

Ｑ４－１　「作業終了後のデータ消去を徹底すること」と規定されているが、データ消去が求められるのは作業用パソコン内であり、アクセス権限が適切に付与されている社内の共用サーバーに保存した個人情報データは削除の対象外でしょうか。

Ａ４－１　作業終了後の個人情報については、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）から削除する必要があります。そのため、個人情報を保管する場合には情報系ネットワークと物理的又は論理的に分離された基幹系ネットワーク上で保管することが必要です。

Ｑ４－２　業務上、照会対応等のために一定期間、個人情報をパソコン等に保存することは許容されますか。

Ａ４－２　照会対応等の継続した作業が発生する場合、当該作業時間内はパスワードの設定等を行った上でパソコン等に管理を行い、作業終了の都度、直ちに個人情報の消去をし、再度当該個人情報を利用される時はその都度ダウンロード等をするという安全管理措置を徹底してください。

（５）その他

Ｑ５－１　廃止された「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 28 年厚生労働省告示第 290 号。以下「私的年金ガイドライン」という。）に規定されている「第三者提供の制限に関する例外　法令に基づく場合」として明記されている事例のうち私的年金制度特有の事例（※）の記載は、「私的年金分野における個人情報の技術的安全管理措置」（平成 29 年厚生労

働省告示第 211 号）から削除されていますが、変更はないという認識で良いですか。

Ａ５－１　ご認識の通り、私的年金ガイドライン廃止後でも明記されている事例について変更はございませんので、引き続き参考としていただく分には問題ありません。

※事例：私的年金ガイドラインの該当部分

第７ 個人データの第三者提供に関する義務

２ 第三者提供の制限に関する例外【法第 23 条第１項関係】

次のいずれかに該当する場合は、１の規定にかかわらず、個人データを第三者に提供することができる。

(1) 法令に基づく場合

（例）

・私的年金関係事業者が加入者原簿の作成等のために加入者の氏名、性別、生年月日、基礎年金番号等を基金等から取得すること（確定給付企業年金法施行規則（平成 14 年厚生労働省令第 22 号）第 22 条等）

・私的年金関係事業者の地方公共団体情報システム機構からの生存情報の取得（住民基本台帳法（昭和 42 年法律第 81 号）第 30 条の９）

・私的年金関係事業者の地方公共団体情報システム機構からの個人番号の取得（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）第 14 条第２項）

Ｑ５－２　「中小規模事業者」であれば、「私的年金分野における個人情報の技術的安全管理措置」の対象外とされていますが、「中小規模事業者」の条件を満たす、実施事業主又は基金の定義とは、具体的には以下３つの条件を満たす者との理解で良いでしょうか。

①実施事業主の従業員の数が 100 人以下であること。

確定給付企業年金制度或いは厚生年金基金制度の基金については、当該基金の従業員の数が 100 人以下であること。

②その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６月以内のいずれの日においても 5,000 を超えないこと。

③委託を受けて個人データを取り扱う者では無いこと

Ａ５－２　貴見の通りです。なお、基金が中小規模事業者であっても、基金を実施する事業所の事業主については、各事業所のそれぞれの従業員数により判断され、その従業員の数が 100 人以下である必要があります。

また中小規模事業者であっても、「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 28 年個人情報保護委員会告示第 6 号）」にて例示されている「中小規模事業者における手法の例示」を参考に、個人情報保護委員会の定める基準の安全管理措置を遵守する必要があります。