一生涯のパートナー
第一生命
Dai-ichi Life Group

第一生命 年金通信

年金トピック

No.2016－111

2016 年 10 月 13 日
団体年金サービス部

私的年金分野における個人情報の安全管理措置について

今般、厚生労働省告示の「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」についてのQ＆Aが公開されました。
当年金通信では、「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」のガイドラインおよびQ＆Aについてご案内いたします。

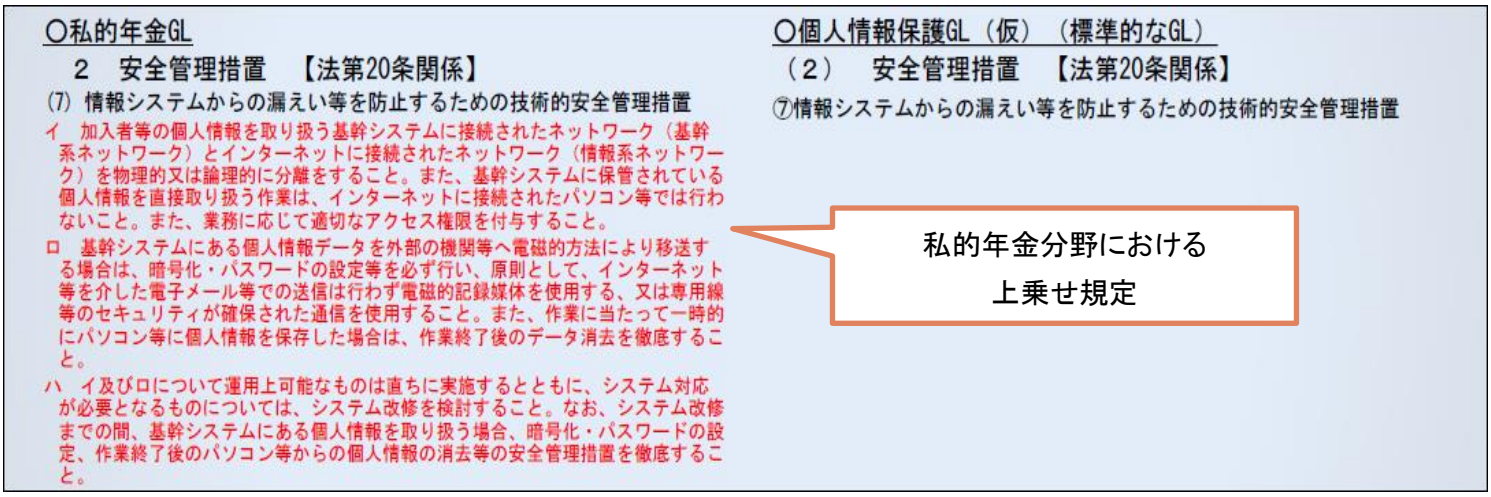
【要約】

1.「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」について

従来の個人情報保護法および基本方針を踏まえ、私的年金関係事業者が講じる措置がより適正かつ、有効に実施されるように、具体的な指針として「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」制定されました。
このガイドラインでは、従来の「企業年金等に関する個人情報の取扱いについて」（局長通知）規定に加えて、①安全管理措置の徹底、②適正取得の徹底、③委託先の監督の徹底の3つの措置が新たに規定されました。

2.安全管理措置の上乗せ規定について

私的年金分野においては安全管理措置を十分に配慮する必要性があることから、「私的年金分野における個人情保護に関するガイドライン」では、標準的なガイドライン（個人情報ガイドライン）に上乗せして、「情報システムからの漏えい等を防止するための技術的安全管理措置」について上乗せで規定しています。



「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」のQ&AおよびガイドラインのQ&Aの詳細については、別紙 1～3をご参照ください。
（本紙）　私的年金分野における個人情報の安全管理措置について
（別紙 1）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について
（別紙 2）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Q&A
（別紙 3）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Q&Aに関する要望と質問への回答

別紙１

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について

平成２８年９月２７日
厚生労働省年金局
企業年金国民年金基金課

私的年金ガイドライン制定の趣旨

「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GL」という。）は、
①個人情報保護法・基本方針に基づく具体的な指針を定める
②私的年金各法に基づいて個人情報の適正な取扱・管理に必要な措置を講ずる
必要性から制定されました。

〇私的年金GL

第１　趣旨【法第１条関係】

このガイドラインは、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）第６条及び第８条に基づき、また、法第７条第１項に基づく「個人情報の保護に関する基本方針」（平成16年４月閣議決定。平成20年４月及び平成21年９月一部変更。以下「基本方針」という。）を踏まえ、**私的年金関係事業者が個人情報の適正な取扱いの確保に関して行う活動を支援するため、私的年金関係事業者が講じる措置が適切かつ有効に実施されるよう具体的な指針として定める**ものである。

また、国民年金法（昭和34年法律第141号）、石炭鉱業年金基金法（昭和42年法律第135号）、確定給付企業年金法（平成13年法律第50号）、確定拠出年金法（平成13年法律第88号）、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25年法律第63号。以下「平成25年改正法」という。）附則第５条及び第38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25年改正法第１条による改正前の厚生年金保険法（昭和29年法律第115号）並びに関係法令の規定に基づき、その**業務の遂行に必要な範囲内で加入者等の個人に関する情報を収集し、保管し、及び使用することが認められ、それに当たっては、個人に関する情報を適正に管理するために必要な措置を講ずることが求められることも踏まえ、このガイドラインを定める**ものである。

法は、個人情報の取扱いに当たっては、個人情報の有用性に配慮しつつ、受給者等、個人の権利利益を保護することを目的としており（法第１条）、当該目的は、このガイドラインにおいても、同様である。

（以下略）

私的年金GL制定の経緯

私的年金GLは以下のような経緯で定められました。なお、今後、個人情報保護委員会によるガイドラインに一元化される予定です。
（内容に変更はありません。）

平成15年11月　「個人情報の保護に関する法律」（平成15年法律第57号。以下、「個人情報保護法」という。）その他関係法令の制定に伴い、各府省は所管の事業分野についてのガイドラインを規定することとなりました。

平成16年10月　厚生労働省年金局においても、「企業年金等に関する個人情報の取扱いについて」（通知）の制定により私的年金分野における個人情報の取扱いが規定されました。

平成26年11月　消費者庁より、各府省に対してガイドラインの見直し・改定を求められたことを受けて、厚生労働省年金局でも、消費者庁によって定められた総則や標準的なガイドラインに従い、私的年金GLを策定する動きとなりました。
※　総則により、名称の共通化、形式や使用用語の統一化の他、事業者や国民の理解を得るべく、分かりやすいGLを制定することが定められました。

平成28年 7月　私的年金GLを告示の形式で新たに策定したことに伴い、従来、個人情報の取扱いを規定していた前述の平成16年の通知を廃止し、私的年金分野における個人情報の取扱いの規定は私的年金GLへと移行し、施行されました。

平成28年 9月　安全管理措置についての規定部分のみ、先日9月1日に施行されました。

平成28年11月　安全管理措置の規定部分を除き、私的年金GLは個人情報保護委員会の策定する個人情報保護法ガイドライン（仮）に一元化される予定です。

従来の私的年金分野の個人情報取扱規定

「企業年金等に関する個人情報の取扱いについて」（通知）（平成16年10月 1日発出）にて私的年金分野の個人情報取扱が規定されました。

○　個人情報保護法施行に伴い、私的年金における個人情報の取扱いについて定める必要が生じたため、上記通知の発出により、取扱いについては「企業年金等に関する個人情報の取扱い準則」に明記されました。

○　個人情報保護法に基づいて、私的年金関係事業者の遵守すべき指針が定められました。

しかし

○　理念的な指針に留まっており具体性に乏しく、他分野の指針との統一性が欠如しておりました。

※参考（通知で明記された事項）
第一　定義に関する事項
第二　利用目的に関する事項
第三　本人の同意に関する事項
第四　安全管理措置及び従業員の監督に関する事項
第五　委託先の監督に関する事項
第六　第三者提供の制限に関する事項
第七　訂正等、利用停止等及び理由の説明に関する事項
第八　開示等の求めに応じる手続に関する事項
第九　苦情の処理に関する事項
第十　個人情報取扱事業者以外の事業者による個人情報の取扱い

○　従って、前述の問題に対応すべく新たに具体的なGLを制定することとなりました。

私的年金GL制定による新たな措置

従来の「企業年金等に関する個人情報の取扱いについて」（局長通知）の規定に加え、***新たに、①安全管理措置の徹底、 ②適正取得の徹底、 ③委託先の監督の徹底の３つの措置が明記されました。***

Ⅰ　安全管理措置の徹底

事業主等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に望まれる措置として、事業主等の内部の監査実施体制の整備や、情報システムからの漏えい等を防止するための技術的安全管理措置等を規定しています。

Ⅱ　適正取得の徹底

事業主等が第三者からの提供により個人情報を取得する場合には、提供元の個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合には、その取得の自粛を含め、慎重に対応することが望ましい旨を規定しています。

Ⅲ　委託先の監督の徹底

事業主等が資産管理事務を資産管理機関に委託する場合等において、委託先の個人データの取扱いに対する適切な監督のために望まれる措置として、委託先に対する定期的な監査の実施や、再委託等を実施する場合の承認手続等を規定しています。

Ⅰ. 安全管理措置の徹底①（私的年金GL第６の２参照）

私的年金分野において安全管理措置は十分配慮する必要性があることから、当該規定のみ個人情報保護法ではなく、各個別法令（例：確定給付企業年金法）を制定根拠として上乗せルールを定めております。

〇私的年金GL

２　安全管理措置　【法第20条関係】

(7) 情報システムからの漏えい等を防止するための技術的安全管理措置

イ　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。

ロ　基幹システムにある個人情報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。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。

ハ　イ及びロ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）

なお、不特定多数者が書店で随時に購入可能な名簿で、事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、事業者の安全管理措置の義務違反にならない。

〇個人情報保護GL（仮）（標準的なGL）

（２）　安全管理措置　【法第20条関係】

⑦情報システムからの漏えい等を防止するための技術的安全管理措置

（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）

なお、不特定多数者が書店で随時に購入可能な名簿で、事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、事業者の安全管理措置の義務違反にならない。

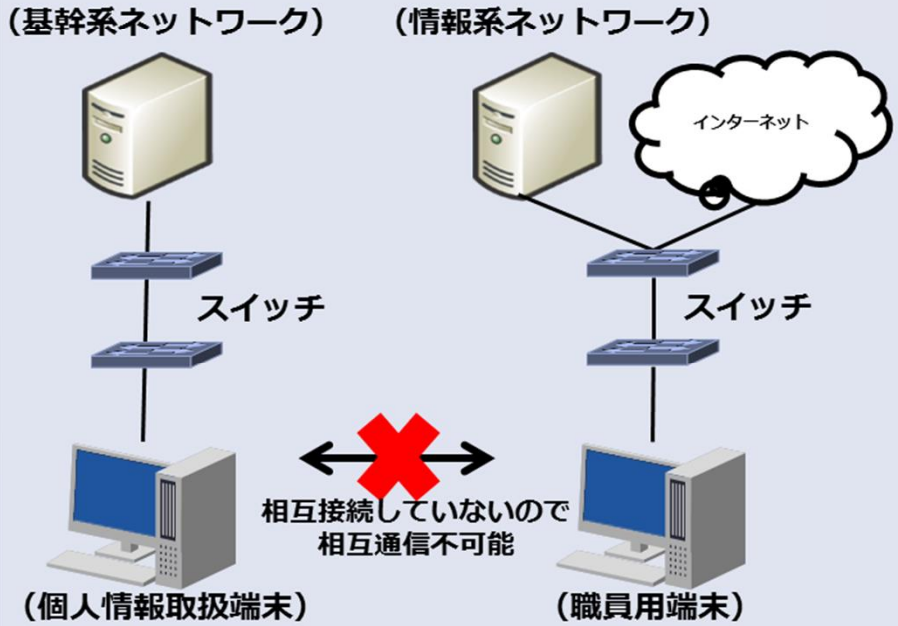
安全管理措置の徹底②

私的年金GL第６の２（７）イ

○　加入者等の個人情報を取り扱う基幹系ネットワークとインターネットに接続された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。
○　基幹システムにあ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、適切なアクセス権限を付与すること。

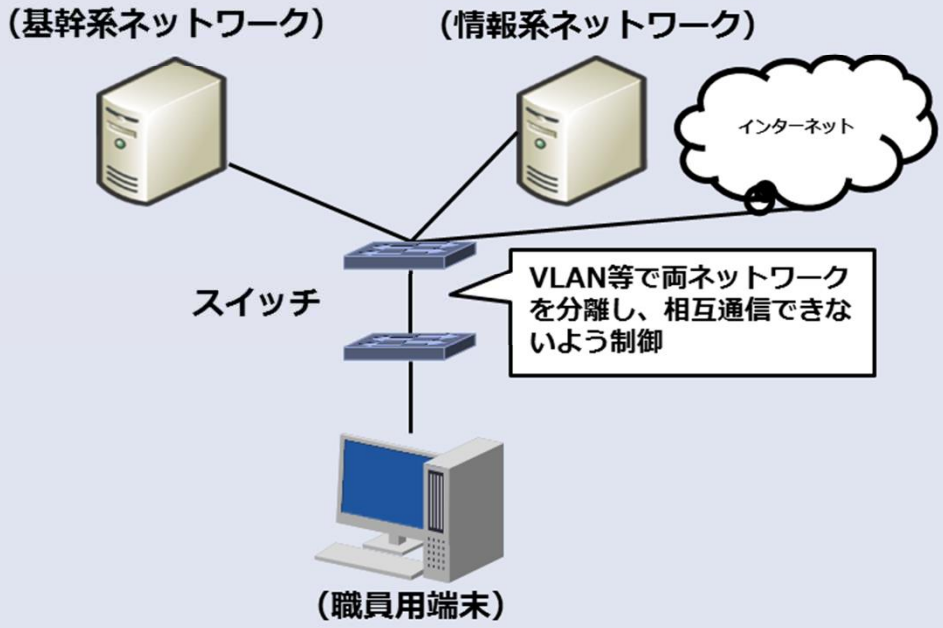
物理的分離

経路（ケーブル）及びネットワーク機器（スイッチ等）を物理的に分離することにより、ネットワーク間の相互通信が不可能な状態



論理的分離

経路（ケーブル）及びネットワーク機器（スイッチ等）を共有する箇所があるが、ネットワークの設定（VLANを用い通信制御を行うなど）により、ネットワーク間の相互通信が不可能な状態

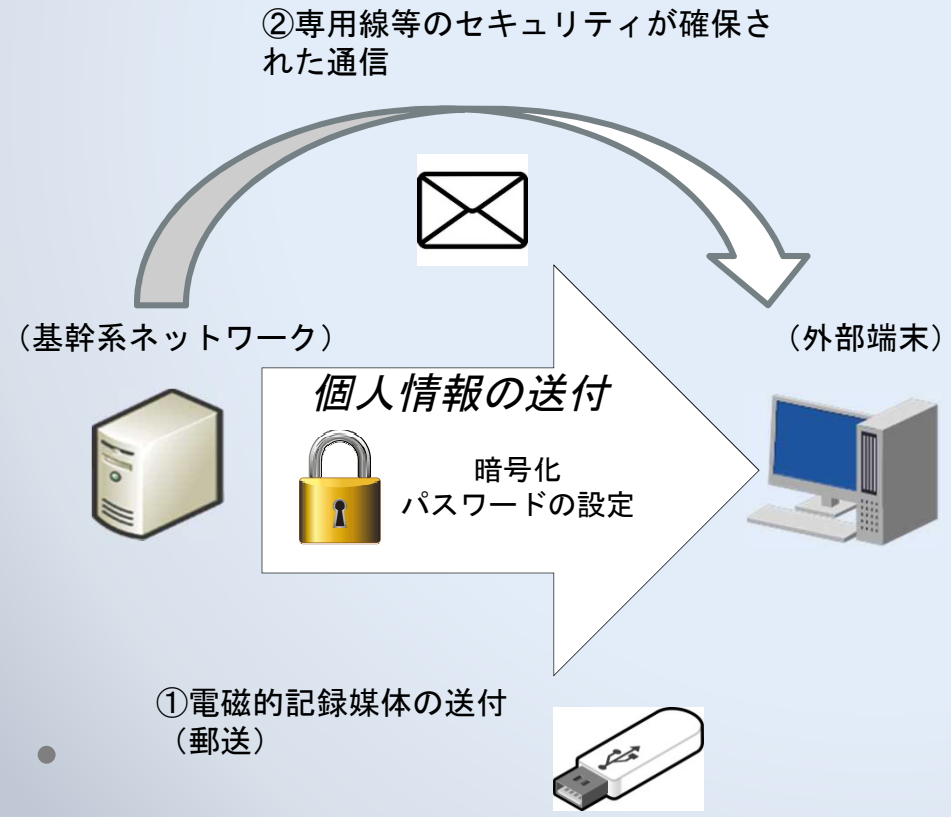


※５年ごと機器更改していれば論理的分離は、ほぼこのケースのみ

安全管理措置の徹底③

私的年金GL第６の２（７）ロ

○　基幹システムにある個人情報を外部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する電子メール等での送信はせ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。
○　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。



個人情報の送信の際は必ず電子ファイルに記載し、暗号化等の設定を行います。
※社内イントラネット接続時の社内間のメールは除く

そして上記を満たした上で、

①USBメモリ等、電磁的記録媒体を使用し、郵送等により送付する方法
②専用線等のセキュリティが確保された通信を使用し、電子メール等を用いて送信する方法

のいずれかによって移送することが認められます。

安全管理措置の徹底④

私的年金GL第６の２（７）ハ

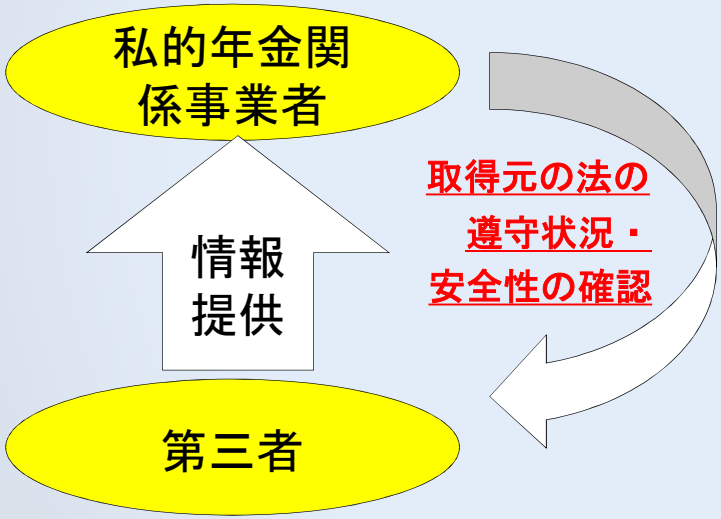
○　イ及びロについて運用上可能なものは直ちに実施するとともに、システム対応が必要となるものについては、システム改修を検討すること。
○　システム改修までの間、基幹システムにある個人情報を取り扱う場合、暗号化・パスワードの設定、作業終了後のパソコン等からの個人情報の消去等の安全管理措置を徹底すること。

○　イ及びロの規定については、直ちに実施あるいはシステム改修の検討をすることが求められます。

○　システム改修が必要なものについては、システム改修には時間を要すると思われますし、施行と同時にイ及びロの規定を実現することは困難であることから、システム改修までの間、個人情報を取り扱う場合の臨時的措置を講じることを求めるものです。

○　システム改修の間は従来の安全かつ徹底した個人情報の取扱をお願いします。

Ⅱ. 適正取得の徹底（私的年金GL第５の１参照）



従来の規定

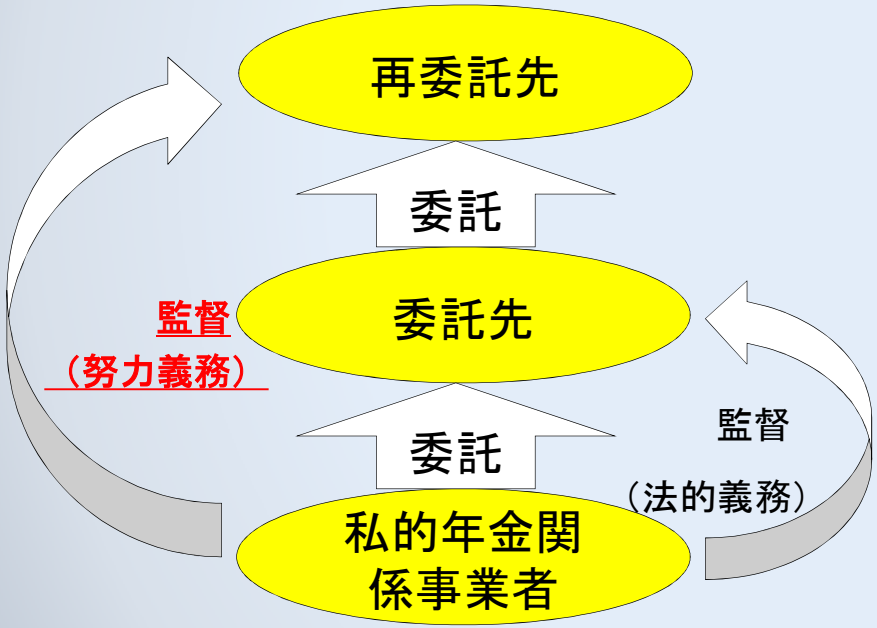
〇私的年金関係事業者は、偽りその他不正の手段により個人情報を取得してはなりません。

新たに追加された規定

〇第三者提供の個人情報を取得する場合には、**提供元の法の遵守状況を確認**し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、**当該個人情報の取得方法等の確認**をお願いします。

　当該個人情報が適法に取得されたことが確認できない場合は、その取得には慎重に対応することが望ましいです。

Ⅲ.委託先の監督の徹底（私的年金GL第６の４参照）



従来の規定

〇事業者は、個人データの取扱いを外部委託する場合は、委託先に対する必要かつ適切な監督を行わなければなりません。

新たに追加された規定

〇委託先の選定に当たっては、委託先の安全管理措置の状況について適切に評価することが望ましいです。

〇委託先における委託された個人データの取扱状況を把握するため、定期的な監査が望ましいです。

〇委託先が再委託を行おうとする場合は、委託元は委託を行う場合と同様、再委託先の詳細について、委託先に事前報告又は承認手続を求め、**定期的に監査を実施する等により監督や再委託先の安全管理措置状況の確認することが望ましい**です。

安全管理措置の徹底に関するQ&A

①イについて

質問：本措置内容については、特定個人情報の内容とまったく同内容であり、担当者の端末を２台用意しなければならないものである。本年実施された情報交換会の席上、貴課ご担当官より「端末の２台所持までを求めるものではない」との見解に相違する内容である。２台所持以外に分離する方法とはどのようなものがあるのか例示いただきたい。

回答：論理的分離は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。

安全管理措置の徹底に関するQ&A

②ロについて

質問：現状、全てのRKや運営管理機関では事業主や加入者がインターネット経由（TLS／SSL等にて暗号化された専用WEBサイト経由通信）にて、各種個人情報の登録、メンテ処理等を実施しています。本仕組みは関係者の利便性と作業効率化には必須となっております。該当の仕組みを経由した処理を許容いただきますようお願いします。万が一不可となった場合、関係者、現行業務継続が困難になることが想像されます。

回答：SSLにつきましては脆弱性が指摘されているため、Webの暗号化通信手法につきましては現在TLSを推奨しています。

③ロについて

質問：「Internet-VPNサービスのような通信経路が暗号化されたネットワークであれば「専用回線」として認められますが、SSL-VPNやIPsecを利用して通信を行う場合には、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～)暗号化の過程で盗聴等のリスクがあることから、「専用回線」としては認められません。」とあるが、「他の対策」とは何をさすか。

回答：一義的に盗聴や改竄等の第三者からの介入を排除した通信と同等レベルのセキュリティが担保されており、専門家等が十分な対策と判断するに事足りるレベルでの対策を指します。

安全管理措置の徹底に関するQ&A

④全般について

質問：個人情報の流出リスクを抑止するという趣旨は理解するが、本内容を遵守するためには多額の情報システム投資、及び多くの時間を要することとなり、現実的ではなく、緩和願いたい。

回答：日本年金機構の情報流出事案を踏まえて、NISC（内閣サイバーセキュリティセンター）の要請を受け、年金関係について高度な安全管理措置を講ずる必要性が生じました。またシステム改修には時間を要すると思われますし、施行と同時にイ及びロの規定を実現することは困難であることから、システム改修までの間、個人情報を取り扱う場合の臨時的措置も講じているところです。システム改修の検討を含め、今般のガイドラインの改定の趣旨・経緯を御理解いただき、御協力いただければ幸いです。

安全管理措置の徹底に関するQ&A

⑤全般について

質問：企業年金基金（以下、基金）の類型を問わず、多くの基金の実態は、人的、物的両面から母体企業への依存度が非常に高い。情報システム環境においても例外ではなく、基金の役職員が母体社員を兼務しているケースも多いことから、多くの基金では、母体企業と情報システム環境が共有されている。そのため、個人情報データが保存されているファイルサーバ等については、サーバ自体や傘下のフォルダへのアクセス権が十分に管理された状態（基金内外を含む他の担当者からのアクセスができない状態）であれば、サーバ等を共有して使用することは差し支えない旨明示いただきたい。

回答：まず母体企業が個人情報データを個人番号で管理する場合、『特定個人情報の適正な取扱いに関するガイドライン』の適用対象となるため、当該ガイドラインに従った措置を取っていただければと思います。母体企業が個人情報データを個人番号で管理していない場合であっても、母体企業として個人情報を扱うシステムは既に不正アクセスを遮断し、外部流出を防ぐ等の手段を講じていることとなっているところです。したがって当該手段により管理することが求められます。一方、私的年金についても本告示の求める水準を確保するため、くれぐれも基金情報を扱う端末と基金以外の企業の情報を扱う端末のサーバ等を共有して使用することはお控え下さい。

参照条文

○個人情報の保護に関する法律（平成15年法律第57号）

（法制上の措置等）
第六条　政府は、個人情報の性質及び利用方法にかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるものとする。

第七条　政府は、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、個人情報の保護に関する基本方針（以下「基本方針」という。）を定めなければならない。
２　　基本方針は、次に掲げる事項について定めるものとする。
一　個人情報の保護に関する施策の推進に関する基本的な方向
二　国が講ずべき個人情報の保護のための措置に関する事項
三　地方公共団体が講ずべき個人情報の保護のための措置に関する基本的な事項
四　独立行政法人等が講ずべき個人情報の保護のための措置に関する基本的な事項
五　地方独立行政法人が講ずべき個人情報の保護のための措置に関する基本的な事項
六　個人情報取扱事業者及び第四十条第一項に規定する認定個人情報保護団体が講ずべき個人情報の保護のための措置に関する基本的な事項
七　個人情報の取扱いに関する苦情の円滑な処理に関する事項
八　その他個人情報の保護に関する施策の推進に関する重要事項
３～５　（略）

（地方公共団体等への支援）
第八条　国は、地方公共団体が策定し、又は実施する個人情報の保護に関する施策及び国民又は事業者等が個人情報の適正な取扱いの確保に関して行う活動を支援するため、情報の提供、事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その他の必要な措置を講ずるものとする。

（個人情報の適正な取扱いを確保するための措置）
第十条　国は、地方公共団体との適切な役割分担を通じ、次章に規定する個人情報取扱事業者による個人情報の適正な取扱いを確保するために必要な措置を講ずるものとする。

（適正な取得）
第十七条　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

（安全管理措置）
第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき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じなければならない。

（委託先の監督）
第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

参照条文

○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）

（加入者等の個人情報の取扱い）

第八十五条の二　事業主等は、その業務に関し、加入者等の氏名、性別、生年月日、住所その他の加入者等の個人に関する情報を収集し、保管し、又は使用するに当たっては、その業務の遂行に必要な範囲内で当該個人に関する情報を収集し、保管し、及び使用するものとする。ただし、本人の同意がある場合その他正当な事由がある場合は、この限りでない。

２　事業主等は、加入者等の個人に関する情報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。

○石炭鉱業年金基金法施行規則（昭和42年厚生省令第41号）

（坑内員等の個人情報の取扱い）

第三十一条の二　基金は、その業務に関し、坑内員及び坑内員であつた者（以下この条において「坑内員等」という。）の氏名、性別、生年月日その他の坑内員等の個人に関する情報を収集し、保管し、又は使用するに当たつては、その業務の遂行に必要な範囲内で当該個人に関する情報を収集し、保管し、及び使用するものとする。ただし、本人の同意がある場合その他正当な事由がある場合は、この限りでない。

２　基金は、坑内員等の個人に関する情報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。

○国民年金基金規則（平成2年厚生省令第58号）

（加入員等の個人情報の取扱い）

第五十一条の三　基金は、その業務に関し、加入員及び加入員であった者（以下この条において「加入員等」という。）の氏名、性別、生年月日、住所その他の加入員等の個人に関する情報を収集し、保管し、又は使用するに当たっては、その業務の遂行に必要な範囲内で当該個人に関する情報を収集し、保管し、及び使用するものとする。ただし、本人の同意がある場合その他正当な事由がある場合は、この限りでない。

２　基金は、加入員等の個人に関する情報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。

○確定拠出年金法施行規則（平成13年厚生労働省令第175号）

（事業主のその他の行為準則）

第二十三条　法第四十三条第三項第二号の厚生労働省令で定める行為は、次のとおりとする。

一～六　（略）

七　企業型年金加入者等の個人に関する情報を適正に管理するために必要な措置を講じていないこと。

参照条文

○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26年厚生労働省令第20号）

（加入員等の個人情報の取扱い）

第十七条の五　存続厚生年金基金は、その業務に関し、加入員及び加入員であった者（以下この条において「加入員等」という。）の氏名、性別、生年月日、住所その他の加入員等の個人に関する情報を収集し、保管し、又は使用するに当たっては、その業務の遂行に必要な範囲内で当該個人に関する情報を収集し、保管し、及び使用するものとする。ただし、本人の同意がある場合その他正当な事由がある場合は、この限りでない。

２　存続厚生年金基金は、加入員等の個人に関する情報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。

別紙２

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Ｑ＆Ａ

【ガイドライン中の安全管理措置の規定（抜粋）】

(7) 情報システムからの漏えい等を防止するための技術的安全管理措置

イ　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。

ロ　基幹システムにある個人情報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。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。

ハ　イ及びロ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。

第１．イ「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できる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。

第２．イ「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るが、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、個人情報を取り扱うことは認められません。

Ｑ２－２　本ガイドライン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、本ガイドライン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。

第３．ロ「基幹システムにある個人情報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。郵送などによる対応が求められる。

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、これは本ガイドライン上、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る。

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、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。

第４.「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、当該作業期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うことは構いませんが、作業終了後に個人情報の消去等の安全管理措置を徹底してください。

別紙３

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Q&A に関する要望と質問への回答

項番	分類	対象	内容	回答
1	質問	第1	別紙について、ネットワーク構成図を例示いただいているが、本内容については、特定個人情報の内容とまったく同内容であり、担当者の端末を2台用意しなければならないものである。本年3月4日に実施された貴課と企年協との情報交換会の席上、貴課ご担当官より「端末の2台所持までを求めるものではない」との見解に相違する内容である。2台所持以外に分離する方法とはどのようなものがあるのか例示いただきたい。	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、取扱端末は一つであっても、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	質問	第1	IB型やⅡ型基金が、総幹事会社である信託銀行等のシステムと接続するには、外部のインターネット環境経由で使用する方法以外は無い（SSL等対応）のが現状である。A1-2では、インターネット経由で接続するシステムは基幹システムではないとも読み取れるが、基幹システムではない場合は本項の適用外であることから、従来どおり使用できるとの認識でよろしいか明示いただきたい。	基幹システム以外のシステムにて加入者等の個人情報を取り扱っている場合は、外部のインターネットと接続された状態で個人情報を取り扱うことになるので、第3のロに該当し、原則として電磁的記録媒体を使用するか専用線等のセキュリティが確保された通信を使用する場合のみ、システム使用は認められます。
3	要望	第1（別紙）	A1－1の別紙（イメージ）のうち「論理的分離」の図ですが、VLANのみに限定された内容となっており、Q&A1－1で容認されているファイアウォール（通過させてはいけない通信を阻止する仕組み）・L3スイッチ・ルータ等を解釈することが難しいと考えます。そのため、本ガイドラインQ&Aの別紙を作成頂くに際しては、以下のいずれかの対応をお願い申し上げます。 ①ファイアウォール・L3スイッチ・ルータ等を解釈し得る内容に修正する。 ②VLANに限定した図と位置づけ、その旨を明記する。	別紙「論理的分離」の図につきましては、インターネットに接続されている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の相互通信を制御する論理的分離のシステムについてイメージがしやすいように示されている図でありますので、「VLAN等」と図に記載のように相互通信を制御する機能を持つ機器であればVLANに限らず、ファイアウォール、L3スイッチ、ルータ等でも構いません。
4	質問	第2 イ	今回のガイドラインを踏まえると、加入者等の個人情報を取り扱う基幹システム自体をクラウド上に構築し、私的年金関係事業者の社内からインターネット経由で利用する事務形態は、今後は認められなくなるということでしょうか。	基幹システム自体をクラウド上に構築することは認められますが、社内からインターネット経由で利用する事務形態については、貴見の通り認められなくなります。ただし、専用線等のセキュリティが担保された通信を使用する場合は認められます。
5	質問	第2	13-(4)で定義されるものとして、「確定給付企業年金法第3条第1項第2号規定する企業年金基金及び企業年金基金を実施する厚生年金適用事業所の事業主」とあるが、本ガイドラインは企業年金基金（以下、基金）のみならず、いわゆる基金の母体事業所にも本内容がすべて適用されると読み取ることができる。これについて、適用とのことならば、現時点でその周知方法はいかがお考えであるか。（13-(5)及び13-(7)においても同じ。）	貴見の通り、本告示に規定する私的年金関係事業者全てに本告示は適用されます。周知方法につきましては、従前通りの周知・徹底を願いたく存じます。
6	質問	第2	項番2のようにインターネットに接続しなければ取り扱えない業務の考え方を明示いただきたい。これはQ3-4とも共通する事項である（e-tax、eLtaxはインターネットの無い環境では取り扱えないため）。	項番2に同じです。
7	質問	第2	「本ガイドライン以外の方法」とあるが、例示をいただきたい。	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ますので、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、適切に御対応願います。
8	質問	第2	①Qの①～③の内容の趣旨が理解できず、内容・表現ともに再検討いただきたい。 ②Q2-1とも共通する内容であるが、「インターネットに接続できる・できない」「インターネットに接続された状態・されていない状態」とは具体的にどのような状態を示すのか。インターネットエクスプローラー等のブラウザやメールソフトを起動させていない状態は、「接続できない、接続されていない状態」と考えて差し支えない旨を明示いただきたい。	①説明会の開催等を予定させていただきます。 ②「インターネットに接続されていない状態」とは物理的にケーブルの分離或いはネットワークと端末の接続による相互通信を完全に遮断する状態を示すので、ブラウザやメールソフトを起動していない状態だけでは接続されていないとは認められません。
9	質問	第2	2行目「インターネットに接続されたパソコン等」とあるが、これはQ2-1と同様に、論理的に切断されている場合は「インターネットに接続されたパソコン等」に該当しない理解でよいか。	貴見の通りです。
10	質問	第2	2行目「専用回線等のセキュリティが確保された通信」とあるが、プロバイダの提供する共有ドメイン・独自ドメインでのインターネットメールは、「セキュリティが確保された通信」に該当するのか。	「専用回線等のセキュリティが確保された通信」とはA.3-6に記載のように、一義的に盗聴や改竄等の第三者からの介入を排除した通信を指します。お尋ねの共有ドメイン・独自ドメインのインターネットメールの利用というだけでは「セキュリティが確保された通信」に該当せず、A3-6に記載のように通信事業者が提供するInternet-VPNのような専用線等を利用した「セキュリティが確保された通信」である必要がございます。

11	要望	第3	現状、全てのRKや運営管理機関では事業主や加入者がインターネット経由（TLS/SSL等にて暗号化された専用WEBサイト経由通信）にて、各種個人情報の登録、メンテ処理等を実施しています。本仕組みは関係者の利便性と作業効率化には必須となっております。Q3にて該当の仕組みを経由した処理を許容いただきますようお願いします。万が一不可となった場合、関係者、現行業務継続が困難になることが想像されます。	SSLにつきましては脆弱性が指摘されているため、Webの暗号化通信手法につきましては現在TLSを推奨しています。したがってTLSにつきましては検討させていただきます。
12	要望	第3	【ご要望】 Q&Aの「A3-6」(専用線等の例示)について、現在のVPN等の他に、 SSL/TLS等を活用して暗号化された通信等も例示に含めて頂きたい。 【要望事由】 「A3-5」では、インターネットバンク(一般的にSSL/TLSを使用)が認められている為。	SSLにつきましては脆弱性が指摘されているため、Webの暗号化通信手法につきましては現在TLSを推奨しています。したがってTLSにつきましては検討させていただきます。
13	質問	第3	一律に電子メールの使用は控えるべきとのことであるが、現在の主たる業務連絡手段は電子メールになっており、これに依らない場合は業務効率の低下、所要時間の増大、費用の増大等が見込まれることから、Q3-2と同条件でぜひ緩和いただきたい。	他分野において既に実施の御協力をいただいてる安全管理措置でありますので、御理解・御協力いただければ幸いです。
14	質問	第3	同等以上のセキュリティが担保される方法として、いわゆるファイル授受サービス（システム）の使用は差し支えないもの（ファイルは暗号化又はパスワード設定必須）として例示いただきたい。	ファイル授受サービスにつきましては、専用線等と同等以上のセキュリティが確保され、第三者からの盗聴や改竄を完全に排除されるサービスの質や情報保護が担保されていることが約款に明記されていることを確認し、専門家の意見等を踏まえ、適切に対応することが求められます。

15	質問	第3	企業年金等に関する特定個人情報の取扱い準則に以下の記載があり。 第二(2)② 通信を用いる場合には～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。 ア 専用回線 イ VPN等専用回線に準じたもの ウ SSL/TLS等を活用した暗号化による通信 とあるが、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Q&A A3-6には、以下の表記となっている。 Internet-VPNサービスのような通信経路が暗号化されたネットワークであれば「専用回線」として認められますが、SSL-VPNやIPSecを利用して通信を行う場合には、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～)暗号化の過程で盗聴等のリスクがあることから、「専用回線」としては認められません。 質問1.「SSL/TLS等を活用した暗号化による通信」では基準を満たさないのか。 TLS (Transport Layer Security) 質問2.「他の対策」とは具体的にどういう対策なのか。 質問3.外部記憶媒体に記録された特定個人情報を、信託銀行等の管理するシステムに アップロードする場合は、インターネットに接続されたネットワークでの作業に該当するのか。(ハードディスクに記憶させなければ運用上可能ですか?)	質問1.SSLにつきましては脆弱性が指摘されているため、Webの暗号化通信手法につきましては現在TLSを推奨しています。したがってTLSにつきましては検討させていただきます。 質問2.一義的に盗聴や改竄等の第三者からの介入を排除した通信と同等レベルのセキュリティが担保されており、専門家等が十分な対策と判断するに事足りるレベルでの対策を指します。 質問3.Q.2-3の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」にあたりますので、インターネットに接続されたネットワークでの作業に該当します。そのため専用線等のセキュリティが担保された通信を使用することが求められます。 なお運用上可能であるか否かは、、『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9条別表等に照らし合わせるか、個人情報保護委員会に確認をするなどして、適切に対応することが求められます。
16	質問	第3	Q3－2と3－3の回答おいて、3－2では「例外的に電子メールでの送信も認められます」とされる一方、3－3では「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」とされていますが、3－3の回答は、「恒常的」に電子メールで送信する場合を前提としている回答という理解でよろしいでしょうか。	貴見の通りです。

17	質問	第3	Q3－6を以下のように修正いただきたい。 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。」とありますが、セキュリティが確保された通信とはどのようなものですか？ A3－6 セキュリティが確保された通信とは以下のものが考えられます。 ア 専用回線 イ VPN等専用回線に準拠したもの ウ SSL/TLS等を活用した暗号化による通信 理由：貴省から出状されている「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2(2)②の記載に合わせていただきたいもの。 個人情報以上に厳格な管理が求められる特定個人情報において認められているセキュリティ水準が本Q3－6では認められないようにも読め、その場合、個人情報と、より厳格な管理が必要な特定個人情報との間でセキュリティーレベルが逆転することとなる。	・通知「企業年金等に関する特定個人情報の取扱いについて」発出時と現時点において厚生労働省が求めるセキュリティ水準が変化したという意図はなく、セキュリティが確保された通信に、左記ア～ウは含まれますが、SSLにつきましては脆弱性が指摘されているため、Webの暗号化通信手法につきましては現在TLSを推奨しています。したがってTLSにつきましては検討させていただきます。なお具体的な文言は、検討の上提示させていただきます。
18	質問	第3	Q3－3に対し、「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」とご回答をいただいております。しかしながら、当該Qは、送信する情報量の多寡に関わらず、「専用線の利用や外部記憶媒体の郵送など、ガイドラインに規定された手法をとり得ない場合の電子メール送信の可否」についてお伺いするものです。 そのため、恐縮ですが、改めて以下の内容を照会させていただきます。 【再照会】 「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。 また、認められるのであれば、その旨Q&Aにてお示しいただきたい。	Q.3-3の「僅少」につきましては情報量の多寡ではなく、情報漏洩の可能性にかかっております。そのため、暗号化・パスワードの設定を行った上でも、送付通信経路の過程で情報漏洩の可能性が僅少でもあるため、必要性・緊急性が高くやむをえない場合を除き、規定されない手法を取り得ない環境であれば、電子メールによる個人情報の送付は認められません。

19	質問	第3 ロ	「原則として」の意図するところをご教示ください。	個人情報の即時な情報伝達の必要性・緊急性がある時という場合の例外を除き、個人情報を電子メールで送信することを禁止する意図でございます。
20	質問	第4	「社内の共用サーバに保存したデータについて、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」とのことであるが、サーバのネットワーク上の分離のイメージがつかめないため、より具体的に明記及び図示いただきたい。 また、企業年金基金(以下、基金)の類型(ＩＡ型、ＩＢ、Ⅱ型)を問わず、多くの基金の実態は、人的、物的両面から母体企業への依存度が非常に高い。情報システム環境においても例外ではなく、基金の役職員が母体社員を兼務しているケースも多いことから、多くの基金では、母体企業と情報システム環境が共有されている。そのため、個人情報データが保存されているファイルサーバ等については、サーバ自体や傘下のフォルダへのアクセス権が十分に管理された状態(基金内外を含む他の担当者からのアクセスができない状態)であれば、サーバ等を共有して使用することは差し支えない旨明示いただきたい。	前段につきましては、説明会の開催による説明等を予定させていただきます。 後段につきましては、まず母体企業が個人情報データを個人番号で管理する場合、『特定個人情報の適正な取扱いに関するガイドライン』の適用対象となるため、本ガイドラインの規定に従った措置を取っていただければと思います。母体企業が個人情報データを個人番号で管理していない場合は、母体企業として個人情報を扱うシステムは既に不正アクセスを遮断し、外部流出を防ぐ等の手段を講じていると思慮されるため、これに準じて管理することが求められます。その場合でも本告示の求める水準を確保するため、くれぐれも基金情報を扱う端末と基金以外の企業の情報を扱う端末のサーバ等を共有して使用することはお控え下さい。
21	要望	全般	全般的に記載内容が難しく、ある程度情報システムに精通していなければ理解できない内容である。多くの基金は情報システムの専任者を設置していないことから、平易な表現に改めていただきたい。	説明会の開催等を予定させていただきます。
22	要望	全般	個人情報の流出リスクを抑止するという趣旨は理解するが、本内容を遵守するためには多額 の情報システム投資、及び多くの時間を要することとなり、現実的ではなく、緩和願いたい。	他分野において既に実施の御協力をいただいてる安全管理措置でありますので、御理解・御協力いただければ幸いです。
23	質問	全般	特定個人情報の管理と同水準の管理を求められている項目が多く、本ガイドライン及びQ&A における「特定個人情報」と「個人情報」との差異を明示していただきたい。	「特定個人情報」については、『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)』第二条第八項に規定する、「個人番号をその内容に含む個人情報」をさします。年金関係の個人情報は個人番号に紐つけられる事が多いので、このような安全管理措置を規定しています。

24	質問	全般	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り扱い端末を二つ持たなければならないのか。一つの端末で対応できないのか。	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、取扱端末は一つであっても、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。
25	質問	全般	年金個人情報を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、専用回線等を使用するとあるが、電子メール等での送信が無理だと実務が回らなくなる。年金個人情報はマイナンバーと紐つけて対応している企業年金が多いため、特定個人情報レベルの措置をとられると、厳しい。	他分野において既に実施の御協力をいただいてる安全管理措置でありますので、御理解・御協力いただければ幸いです。
26	要望	全般	説明会を開催していただきたい。	近日中の開催を予定しております。
27	要望	全般	VLAN、L3スイッチなどの専門用語は、企業年金関係者が理解し難く、また、例えばQ&A2－3の事例などは直ちに具体的なケースが想起できないことも考えられますので、全体的に分かり易い表現にしていただきたいと思います。	説明会の開催等を予定させていただきます。
28	要望	全般	実施形態（基金型・規約型）、受託会社への委託形態（Ⅰ型・Ⅱ型）や規模などによって、各企業年金の置かれた状況は様々であり、Q&Aの発出にあたりましては、当該状況を踏まえ、企業年金関係者からの意見を十分に検討いただきますよう、お願い致します。 なお、ガイドラインの第1（趣旨）の末尾に「このガイドラインにおいて記載した具体例については、これに限定する趣旨で記載したものではない」と記述されていますので、企業年金からの安全管理措置に関する個別の照会等にはそれぞれの企業年金の事情も斟酌いただき、弾力的にご対応いただきますよう、お願い致します。	検討させていただきます。

29	要望	全般	【意見】 「ガイドラインの共通化の考え方について」に準じて本ガイドラインを作成されたと考えるが、例示については私的年金分野に関連しないものは、削除していただきたい。 （今回の修正稿においていくつか削除されているが、依然として関連しないものがあると思われる。誤植と思われる箇所も含め「別紙」のとおりご連携するのでご確認の上、修正いただきたい。） 【例】 ・「製品に重大な欠陥があるような緊急時に、メーカーから顧客情報を求められ、これに応じる必要がある場合」という例示について、修正前告示案の第4の5(2)の箇所では削除しているが、第7の1(2)においては例示したままとなっている ・地域がん登録事業関係、感染症予防事業関係、児童虐待関係　等	あくまでも各々の事項の多くの具体例を列記することで、より一層イメージしやすくするものとして提示しているため、私的年金と直接関係性がなくても、問題がない限り、告示案のまま存置させていただきます。
30	質問	全般	不正アクセスや外部流出等を防ぐ手段として、本ガイドラインに記載されている例示以外の方法であっても、例えば、通知「企業年金等に関する特定個人情報の取扱いについて」で認められている方法や専門家が適切と判断する方法も認められるという理解で良いか。 もし良いのであれば、Q2－2を冒頭に移動する等して、全般のQ&Aとして追加いただきたい。	貴見の通りです。全般のQ&Aへ追加することについては検討させていただきます。
31	質問	告示第6の4 (3)ハ	業務委託契約等において定めることが望ましいとされた「委託された個人データの再委託に関する事項」において、「事前報告又は承認」以外に「委託先が定めた選定基準により、委託先が審査の上再委託先を選定すること。またその結果について報告すること。」も認められるという理解で良いか。 もし認められるのであれば、Q&Aに追加いただきたい。	再委託先の選定につきましては、委託元は委託を行う場合と同様、再委託する業務内容及び個人データの取扱方法等について事前に把握した上で、委託先に対して承認手続を求め、再委託後も、直接又は委託先を通じて定期的に監査を実施する等により、再委託先が安全管理措置を講じているかを十分に確認することが望ましいため、委託先に選定を完全に委任し、結果の事後報告を求めることは、告示の趣旨に合致しません。