別紙 4

年金業務システム開発管理環境接続仕様書

平成 30 年 8 月

厚生労働省年金局事業企画課システム室

目次

1.　本書の目的

本仕様書は年金業務システム開発管理環境（以下「開発管理環境」という。）の提供するサービスを利用するにあたり、本受託者側の環境（以下「受託者環境」という。）と開発管理環境との接続に必要な事項を定める。

2. 開発管理環境の概要

2.1. 概要

開発管理環境は、年金業務システムの設計・開発に係る納品成果物を管理するための日本年金機構（以下「機構」という。）における環境であり、基本設計書等の納品成果物の原本管理（変更管理、構成管理）、関連性管理（要求トレーサビリティ）を行い、各受託者への設計書等の情報提供、機構との間の情報共有等を行うことを目的としている。

また、各受託者と機構との間で効率的に情報共有を行うためにグループウェア機能を実装している。

開発管理環境の利用にあたり、各受託者は、「3.2 用意する物品」に示す開発管理接続端末、ルータ、ハブ、専用通信回線等(回線終端装置含む)を準備する必要がある。

なお、開発管理環境と受託者環境との責任分界点は「図 2-1 システム概要」に示すとおり、外部接続用スイッチングハブ、ルータ②の間とする。

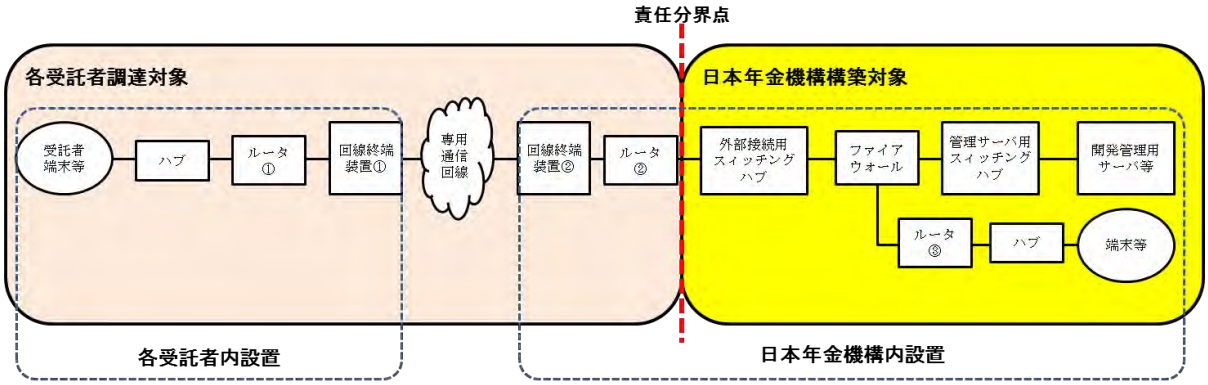


図 2-1 システム概要

本受託者は、契約期間中に更改等により新たな開発管理環境が構築された場合は、旧環境から新環境への接続切替に伴う作業を機構の指示の元行うこと。なお、接続切替作業に伴う一切の費用については本受託者が負担するものとする。

3. 接続条件

3.1. 利用回線

各受託者環境と開発管理環境との間の専用通信回線は、各受託者が準備する。専用通信回線の要件を以下に示す。

（1） 専用通信回線は各受託者、用途等により論理的に分割され、情報資産への機密性を確保する。

（2） 専用通信回線は帯域保障型とする。なお、各機能の利用量を本受託者において見積もり、過不足がない回線帯域とすること。

（3） 他の情報システムから独立した専用の通信回線を構築する。

3.2. 用意する物品

各受託者環境から開発管理環境に接続するために、各受託者が準備すべき物品一覧を「表 3-1 用意する物品（ハードウェア）」、「表 3-2 用意する物品（開発管理接続端末搭載ソフトウェア等）」、「表 3-3 用意する物品（その他）」に示す。

表 3-1 用意する物品（ハードウェア）

項番	項目	数量	用途等	設置場所
1	ルータ①	必要数	各受託者環境と専用通信回線(回線終端装置①)との接続用	各受託者の拠点
2	ルータ②	1 台	専用通信回線(回線終端装置②)と開発管理環境との接続用	機構本部
3	開発管理接続端末	必要数	開発管理環境を利用するために受託者環境内に設置する端末	各受託者の拠点
4	ハブ	必要数	開発管理接続端末とルータ①間の接続用	各受託者の拠点
5	LAN ケーブル	必要数	ネットワークを構成する機器間の接続用	各受託者の拠点

表 3-2 用意する物品（開発管理接続端末搭載ソフトウェア等）

項番	項目	数量	用途
1	以下のいずれかの OS（※） ・Windows7 Professional/Ultimate/Enterprise SP1 32/64bit ・Windows8 Pro/Enterprise 32/64bit ・Windows8.1 Pro/Enterprise 32/64bit	必要数	開発管理環境内の Active Directory のドメインに参加するため。
2	以下のブラウザ ・Internet Explorer 11（desktop 版）		ガルーン 3.7.3 の前提条件。 （ガルーン 3.7.3 の前提条件は IE7-11 だが、Microsoft 社のサポートポリシーの変更に伴い、各 OS が導入可能な最新版の IE11 のみとする。）

（※）Windows10 については、平成 28 年 5 月現在動作保障の対象外となり、利用不可とする。また、Windows7 以降の Intel 第 6 世代 CPU(Skylake)以降搭載端末の場合においては、平成 29 年 7 月 17 日に延長サポートが切れるため、契約期間において延長サポートがされるものに限定する。

なお、更改等により新たな開発管理環境が構築された場合は、必要に応じてバージョンアップ作業を行うこと。

表 3-3 用意する物品（その他）

項番	項目	数量	用途
1	専用通信回線	必要数	開発管理環境と受託者環境間の接続用 各受託者の作業場所が複数あり、それぞれの作業場所で開発管理環境を利用する場合は各作業場所ごとに専用通信回線・回線終端装置を用意すること。 なお、回線終端装置については、ラック内に設置し、転倒防止・機器飛び出し防止等の対策を行うこと。 接続にあたっての詳細は、「4.5 複数拠点の接続」を参照すること。
2	回線終端装置①	必要数	
3	回線終端装置②	1	

受託後に、本受託者が作業の効率化等を目的とし、任意のソフトウェアを導入する場合には、
以下の条件を満たす製品であることを確認した上で、機構の提示する手続きに従い、申請・承認を得ることにより、許可する場合がある。

① 既知の脆弱性が存在するソフトウェアではないこと。また、脆弱性が発見された場合に対策（セキュリティパッチの適用等）が可能であること。

② サポート期間を過ぎたソフトウェアは利用しないこと。

③ 外部との通信を行わないソフトウェアであること。または、外部との通信を行わないように設定が可能なソフトウェアであること。

3.3. 要求仕様

各受託者が調達すべきネットワーク機器(ルータ①、ルータ②)の要求仕様を「表 3-4 ルータ①要求仕様一覧」、「表 3-5 ルータ②要求仕様一覧」に示す。

表 3-4 ルータ①要求仕様一覧

項番	項目	要求仕様
1	種類	回線終端装置との接続に必要なインタフェースを有していること
2	LAN インタフェース	受託者内設置のネットワークに接続できる LAN インタフェースを有すること
3	WAN インタフェース	回線終端装置に対応したインタフェースを有していること

表 3-5 ルータ②要求仕様一覧

項番	項目	要求仕様
1	外形寸法	1U 以下であること
2	電源	AC100V±10%であること(標準周波数 50Hz 及び 60Hz)
3	種類	回線終端装置との接続に必要なインタフェースを有していること
4	LAN インタフェース	10/100/1000BASE-TX×1 ポート以上を有すること
5	WAN インタフェース	回線終端装置に対応したインタフェースを有していること
6	機能	スタティックルーティングに対応していること VLAN(IEEE802.1Q)に対応していること パケットフィルタリング機能を有すること オートネゴシエーション機能を有すること IPv4、IPv6 に対応していること
7	コンソールポート	管理用のコンソールポートを有すること
8	管理	コンソール、telnet 等の設定方法が可能であること NTP による時刻同期に対応していること
9	その他	EIA 規格に準拠した 19 インチラック内のラックトレイに設置可能であること

3.4. 設定情報

3.4.1.IPアドレス

開発管理環境と各受託者環境間の外部接続用セグメントについては、開発管理環境のファイアウォールから各受託者環境のルータ②までとなる。機構から提供する IP アドレスについて、下記「図 3-1 IP アドレス提供箇所」に示す。なお、具体的な IP アドレスについては、受託者との契約後に機構の開発管理環境管理者（以下「機構の管理者」という。）から提供するものとする。

また、各受託者環境内で使用する IP アドレスについては、各受託者が設計すること。

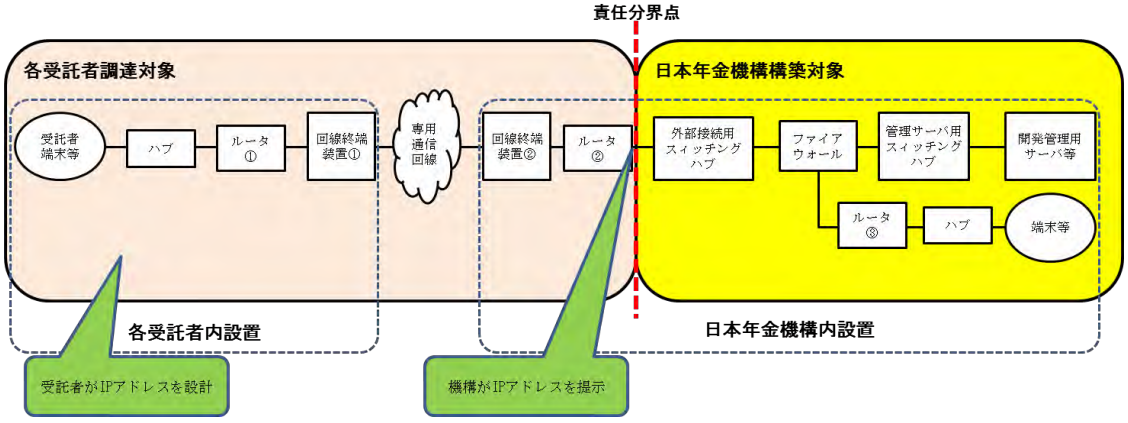


図 3-1 IP アドレス提供箇所

3.4.2.接続ポート

開発管理環境と各受託者環境間の外部接続機器間の接続ポートの情報について、下記「図 3-2 ポート情報提供箇所」に示す。

なお、具体的なポート情報については、受託者との契約後に機構の管理者から提供するものとする。

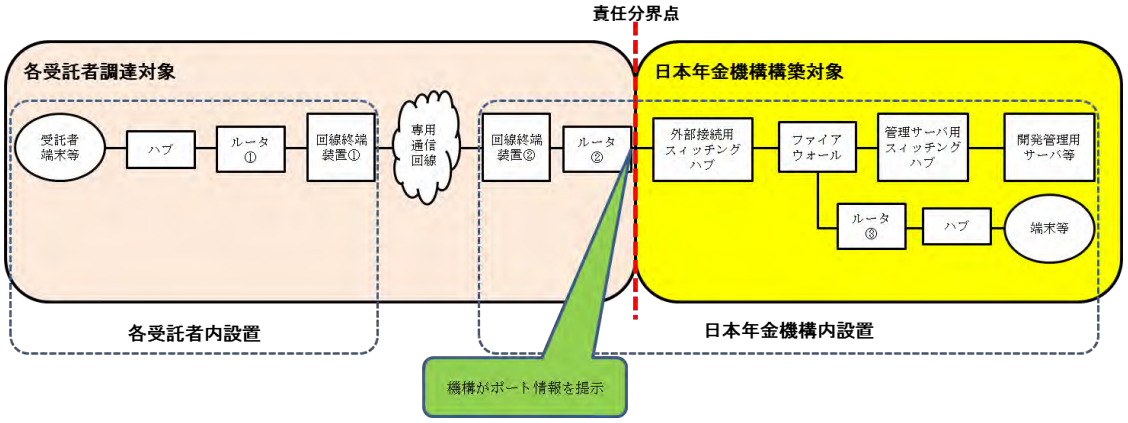


図 3-2 ポート情報提供箇所

3.4.3.認証情報

開発管理環境の Active Directory のドメインに参加するために必要な認証情報（表 3-6 認証情報）は、受託者との契約後に機構の管理者から提供する。

表 3-6 認証情報

項番	項目	内容
1	ログイン ID	ログイン用 ID
2	パスワード	ログイン用パスワード
3	ドメイン名	ログイン用ドメイン

3.4.4.ホスト名

開発管理環境の Active Directory のドメインに参加するために開発管理接続端末に付与するホスト名は、受託者との契約後に機構の管理者が提供する。

3.4.5.ファイル共有

開発管理環境のファイル共有機能を開発管理接続端末で使用するための設定情報は、受託者との契約後に機構の管理者が提供する。

3.4.6.グループウェア機能

開発管理環境のグループウェア機能を開発管理接続端末で使用するための設定情報は、受託者との契約後に機構の管理者が提供する。

なお、グループウェアの登録ユーザーに関しては、保有ライセンス数の範囲内とする。また、本受託者に貸与するライセンス数は 5 ユーザを基本とするが、不足する場合は機構の管理者と調整の上、保有ライセンス数の範囲内において貸与するライセンス数を決定するものとする。

4. 導入条件

各受託者環境から開発管理環境に接続するために必要な導入作業(機器設置、LAN ケーブルの敷設、LAN ケーブルの接続、接続テスト)の役割分担は 4.1～4.4 のとおりとする。また、以下の点を考慮すること。

① 機構内での敷設作業においては、機構の管理者の指示に従うこと。

② 各作業に必要となる各種申請書等の提出やスケジュール調整に関しては、余裕をもって行うこと。

4.1. ラック内機器設置

回線終端装置②及びルータ②の設置については、予め機器の仕様等を機構に報告し承認を得た上で、設置作業について、機構の指示を受けること。

機構本部の開発管理環境既設ラック内のラックトレイへの回線終端装置②及び、ルータ②の設置は各受託者の責任において行うものとする。

4.2. LAN ケーブル敷設

各受託者環境内で必要となるすべての LAN ケーブルの敷設は各受託者が行う。

また、外部接続用スイッチングハブとルータ②間の LAN ケーブルは、機構の管理者が準備したものを使用し、敷設する。

4.3. LAN ケーブル接続

各受託者環境内の各機器間の接続は、各受託者が実施する。

なお、外部接続用スイッチングハブ側の接続は機構の管理者が実施し、ルータ②側の接続は各受託者が実施する。

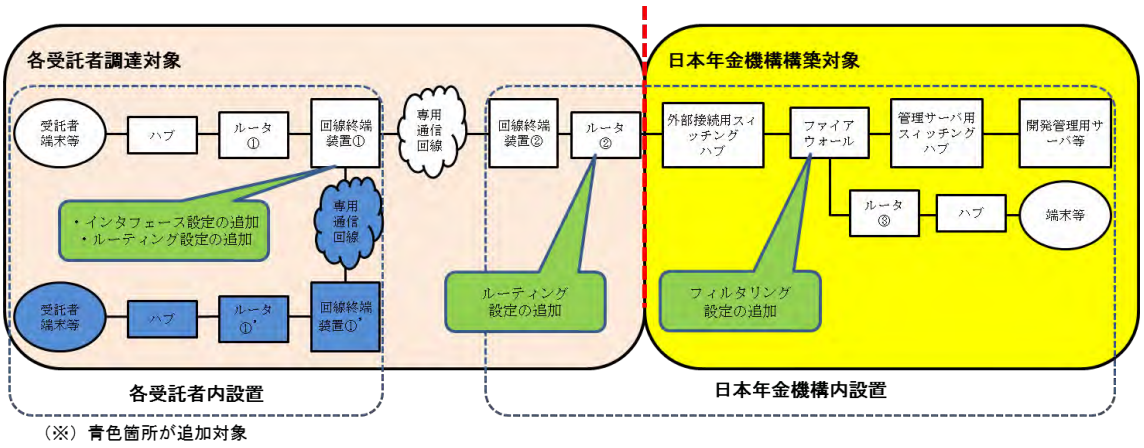
4.4. 接続テスト

（1） 各開発受託者の環境からルータ②までの接続テストは各開発受託者が実施する。

（2） ルータ②と外部接続用スイッチングハブとの結線後に行う接続テストは、機構の管理者と調整した上で各開発受託者が実施する。

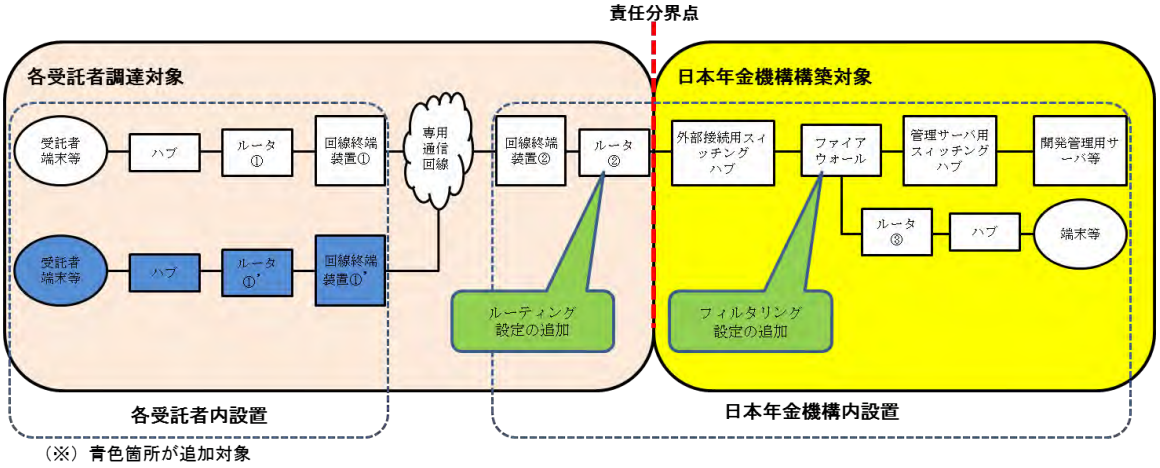
4.5. 複数拠点の接続

各受託者において、複数拠点において本開発管理環境を利用する場合は、下記「図 4-1 複数拠点の構成 パターン①」、「図 4-2 複数拠点の構成 パターン②」に示す構成パターンのいずれかを選択して導入すること。なお、設計・開発の調達において、受託者が共同企業体を形成しており、各構成員の拠点ごとに利用する場合も同様とする。



（※）青色箇所が追加対象

図 4-1 複数拠点の構成 パターン①



（※）青色箇所が追加対象

図 4-2 複数拠点の構成 パターン②

5. セキュリティ条件

各受託者の責任において、以下のセキュリティ対策を必ず実施すること。また、機構からの改善要望・指摘があった場合には対応策を検討、実施すること。

5.1. セキュリティ設定等

各受託者環境においてセキュリティを確保するために、下記対策を実施する。

（1） 回線終端装置①、ルータ①等の機器を受託者内に設置する場合、施錠ができるラック等を利用するか、入退室が管理、制限された部屋に設置するなど十分に安全を確保すること。

なお、厚生労働省及び機構において、必要と判断した場合に、適宜受託者の機器設置場所等の立ち入り検査を受け入れること。

（2） スイッチにおいて、ミラーポートなどの設定が容易に行われ、通信の傍受などがされないように留意すること。

（3） 開発管理接続端末は開発管理環境以外のネットワークとは接続しない。

（4） 開発管理接続端末には必ず「ウイルス対策ソフトウェア(スパイウェア対策機能含む)」を導入する。

（5） コンピュータウイルスやスパイウェア対策ソフトの定義ファイルは常に最新とする。

（6） セキュリティパッチは適用すべきものを判断し、随時適用する。

（7） 各受託者間のセキュリティを確保するため、ルータ①若しくはルータ②においてフィルタリング設定を行うこと。設定内容については、機構の管理者の承認を得た後、本受託者の責任において設定、テスト等を実施すること。

（8） 開発管理接続端末経由で開発管理環境に成果物等を格納する場合は、事前に各受託者の環境においてウィルスチェックを実施し、ウィルスに感染していないことを確認の上格納すること。

5.2. 情報流出対策

年金業務システムに関連する情報の流出対策として、下記運用を実施するように関係者に周知する。

（1） 各受託者が、作業用端末にデータを移行する場合は、作業用端末に対して、本章（5.セキュリティ条件）におけるセキュリティ対策に準ずる対策を実施した上でデータ移行を行うこと。なお、作業用端末は、本業務のみに使用する閉鎖的環境とし、外部のネットワークと接続しないこと。

（2） データの移行の際に使用するUSBメモリ等の外部記憶媒体についても、（1）におけるセキュリティ対策を施した媒体を使用することとし、データ移行の処理のみに使用すること。また、データ移行の処理完了時には、移行データの消去を確実に行うこと。

5.3. 開発管理接続端末の盗難対策

開発管理接続端末の盗難対策として、下記対策を実施する。

（1） 開発管理接続端末の設置場所はパーティション等で隔離し、入退室には必ず認証を必要とすること。

（2） 開発管理接続端末には盗難防止のためのセキュリティワイヤー等を使用して、外部に容易に持ち出すことのできないようにすること。

5.4. 開発管理接続端末の破棄時の対策

作業満了時は必ず以下の何れかの方法によりハードディスクの内容を消去し、厚生労働省及び日本年金機構に消去証明書（任意の様式とする。）を提出する。

（1） 各受託者の責任においてハードディスクの内容が復元されないように必要な消去を行う。

（2） 専門の業者に依頼して、ハードディスクの内容を消去する。

6. 障害時の運用

開発管理環境のシステム障害発生時には、その旨を機構の管理者から各受託者に電子メール等で連絡する。障害回復後は、再度、電子メール等で連絡する。