

特定健診等データ管理システム

別冊2_外付けシステムNW接続IF仕様書

第0.1版

2025年5月16日

国保中央会

変更履歴

No.	変更日付	版	頁数	変更/追加箇所	変更内容
1	2025/5/16	0.1	-	新規作成	-
2					
3					
4					
5					

商標など

- ・ Microsoft、Windowsは、Microsoft社の登録商標もしくは商標である。
- ・ Oracle、Oracle Linuxは、Oracle Corporationの登録商標もしくは商標である。
- ・ その他、本書に記載されている会社名、製品名などは、一般に各社の登録商標もしくは商標である。また、本書では、®および™は明記していない。

目 次

1. はじめに.....	2
1.1. 本書の目的	2
1.2. 用語集.....	3
2. 拠点内連携.....	4
2.1. 基本方針	4
2.2. セグメント.....	10
2.3. 接続構成	11
2.4. 物理線(通信メディア)	11
2.5. IP アドレス	12
2.6. NAT.....	13
2.7. ネットワーク障害対策	13
2.8. ルーティング.....	14
2.9. アクセス制限.....	15
2.10. OCI 管理コンソールへの接続.....	16
3. 拠点外連携	17
3.1. 基本方針	17
3.2. セグメント.....	20
3.3. 接続構成	27
3.4. 物理線(通信メディア)	28
3.5. IP アドレス	28
3.6. NAT.....	29
3.7. ネットワーク機器障害対策	30
3.8. ルーティング.....	34
3.9. アクセス制限.....	35
4. 共通事項（拠点内連携/拠点外連携）	36
4.1. 帯域制御	36
5. 外付けシステム接続申請シート	37
5.1. 基本方針	37
5.2. 申請内容	37
5.3. 申請フロー	38

1. はじめに

1.1. 本書の目的

本書では、特定健診等データ管理システム(以下、「標準システム」と表記)がOracle社の提供するパブリック・クラウドであるOracle Cloud Infrastructure (以下、「OCI」と表記)上にクラウドリフトされる場合において、国保連合会が外付けシステムを構築し、標準システムと連携を行うためのネットワーク接続インタフェース仕様を定める。

本書の前提として、外付けシステムと標準システムとの連携方式については、「外付けシステム開発に係る開発標準」[2. 実現方式]に記載の方式とし、これを可能とするための接続仕様とする。

外付けシステムは、外付けシステムの設置拠点により、標準システムとの連携を以下2種類に分類し、各分類での接続仕様を整理する。

- 拠点内連携：外付けシステムをOCI上に構築し、OCI内にて標準システムとの連携を行う。
外付けシステムと標準システムとの通信が多く見込まれる場合の推奨構成となる(標準システムと外付けシステム間通信の遅延が少なくなり、連合会クライアントと外付けシステム間の遅延が大きくなる)。
- 拠点外連携：外付けシステムを国保連合会拠点(データセンター等)上に構築し、国保連医療保険ネットワークを経由し、拠点を跨ぐ形でOCI内の標準システムとの連携を行う。
外付けシステムと保険者ネットワーク間の通信が多く見込まれる場合の推奨構成となる(連合会クライアントと外付けシステム間の遅延が少なくなり、標準システムと外付けシステム間通信の遅延が大きくなる)。

なお、同一国保連合会が両拠点(OCIならびに国保連合会拠点)に外付けシステムを設置し、拠点内連携、拠点外連携を併用する構成も可とする。

また、外付けシステムと標準システムを接続する上で、国保連合会と国保中央会の間で設計情報を取り交わす必要があり、設計情報を取り交わすための書類として『外付けシステム接続申請用シート』および『データ集配信システムフィードバックシート』を使用する。

国保連合会は『外付けシステム接続申請用シート』および『データ集配信システムフィードバックシート』に必要事項を記入し、国保中央会へ書類を提出すること。国保中央会では提出された書類を確認し、標準システム側の設計情報を追記して『外付けシステム接続申請用シート』を国保連合会に返却する。(書類の受付は2025年度上期に開始し、2025年度下期より随時返却を行う予定である)

『外付けシステム接続申請用シート』および『データ集配信システムフィードバックシート』を取り交わした後、記入された設計情報を基に、国保中央会は外付けシステムと接続するために必要な設定を標準システムに対して行い、国保連合会は標準システムと接続するために必要な設定を外付けシステムに対して行う。

1.2. 用語集

本書の前提とするクラウド(OCI)に関する用語とその定義について、以下に示す。

表 1.2-1 用語の定義

No.	養母	定義
1	OCI (Oracle Cloud Infrastructure)	・Oracle社の提供するパブリック・クラウド
2	テナンシ	・OCIを契約した際に払い出される一意のID
3	VCN (仮想クラウド・ネットワーク)	・テナンシ内に構成する仮想ネットワーク。従来のネットワーク構成要素(サブネット、ルーティングテーブル、ゲートウェイ等)はVCNの中で定義
4	DRG (動的ルーティング・ゲートウェイ)	・複数のVCNと既存のオンプレミス・ネットワークを接続する際や複数のVCN同士を接続する際に、構成するゲートウェイ
5	SL (セキュリティ・リスト)	・通信の許可を定義するリスト。サブネットに紐づけることができ、サブネットに所属する機器に適用
6	NSG (ネットワーク・セキュリティ・グループ)	・通信の許可を定義するリスト。サーバのNIC毎に紐づけることができ、通信許可の定義をサーバ毎に指定
7	ルート表	・VCNから外部のネットワークにトラフィックを送信する際に使用されるルーティングテーブル
8	ファスト・コネクト	・お客様環境とOCIのネットワーク接続パターンの1つ。閉域網でインターネットを経由せずにオンプレミス・ネットワークとOCIを接続

※参考：OCI構築に係る参考サイト(Oracle社サイト)

[https://docs.oracle.com/ja-jp/iaas/Content/GSG/Concepts/](https://docs.oracle.com/ja-jp/iaas/Content/GSG/Concepts/baremetalintro.htm#Welcome_to_Oracle_Cloud_Infrastructure)

[baremetalintro.htm#Welcome_to_Oracle_Cloud_Infrastructure](https://docs.oracle.com/ja-jp/iaas/Content/GSG/Concepts/baremetalintro.htm#Welcome_to_Oracle_Cloud_Infrastructure)

<https://docs.oracle.com/ja-jp/iaas/Content/home.htm>

2. 拠点内連携

本章では、拠点内連携として、外付けシステムをOCI上に構築する場合について記載する。

2.1. 基本方針

拠点内連携を行う場合の、外付けシステムにおける連携イメージを、以下に示す。

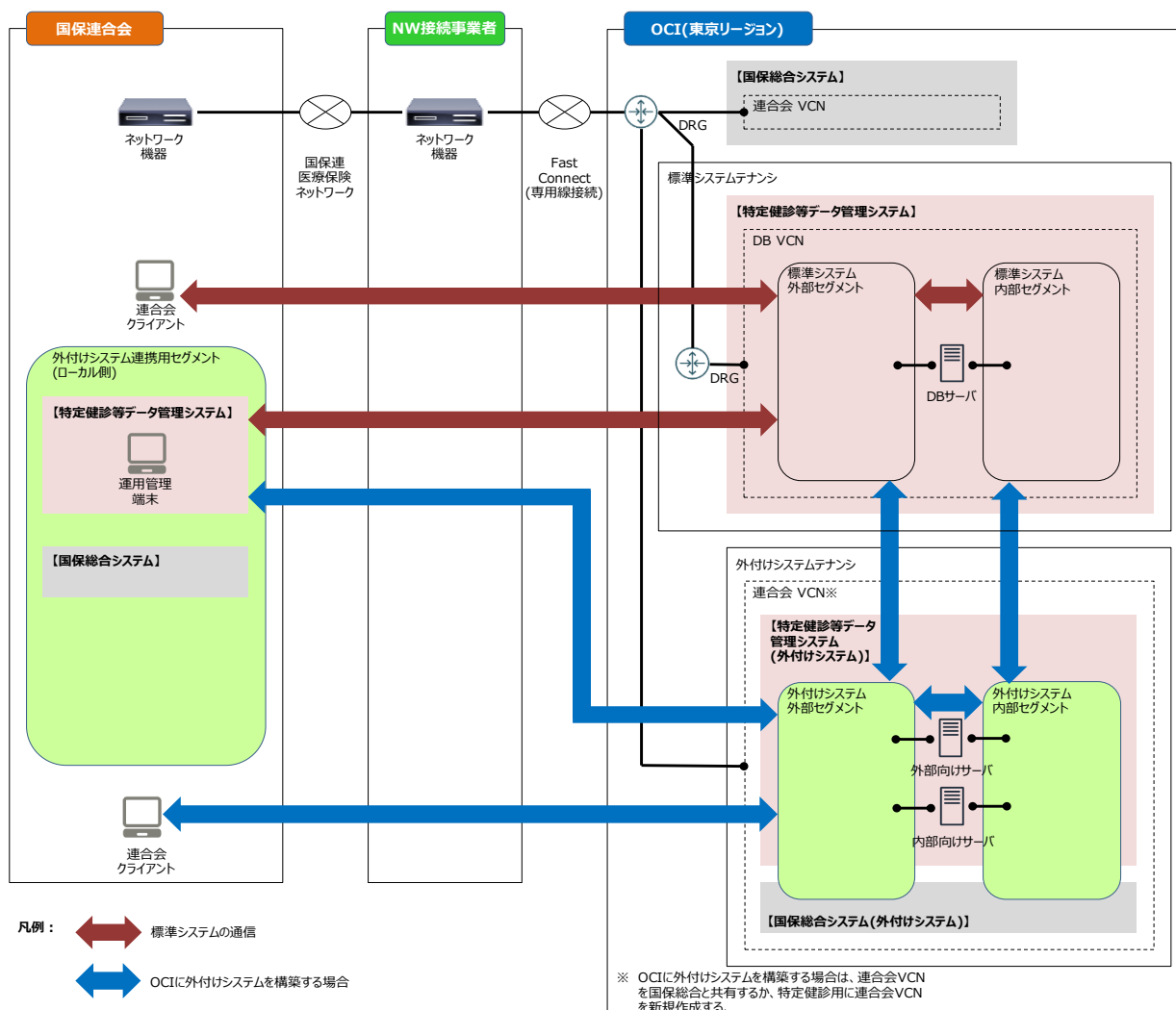


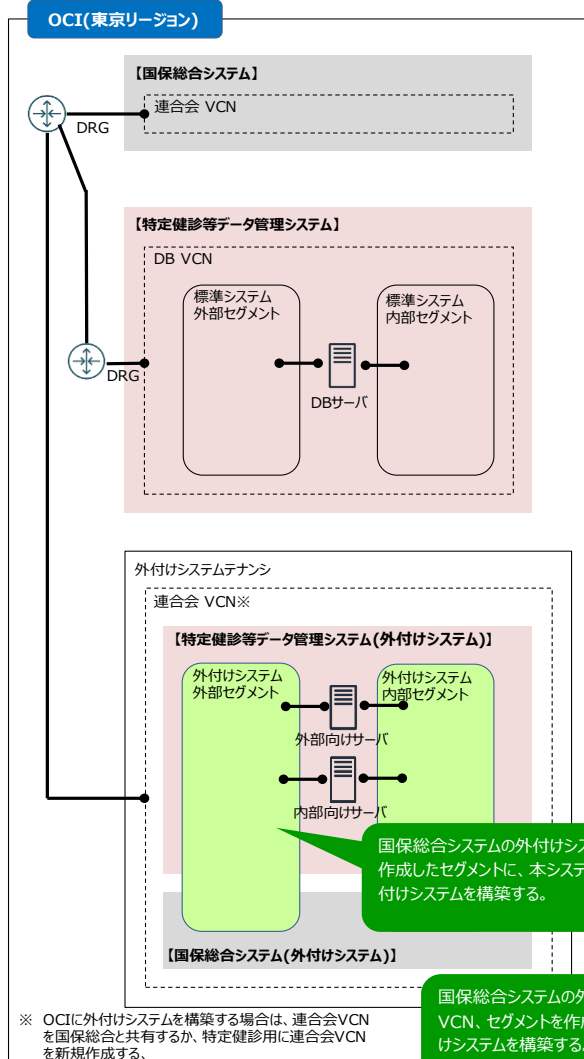
図 2.1-1 外付け連携イメージ(拠点内連携)

拠点内連携を行う場合、国保総合システムの外付けシステムセグメント内に本システムの外付けシステムを構築する場合(パターン①)と、新規にVCNおよび外付けシステム用のセグメントを作成した上で本システムの外付けシステムを構築する場合(パターン②)の2パターンについて以下に示す。

なお、国保連医療保険ネットワークのIPアドレスは枯渇しているため、国保総合システムの外付けシステムで構築した「外付けシステム外部セグメント」に本システムの外付けシステムを構築することを推奨する。新規にVCNおよび外付けシステムのセグメントを作成した場合、必要とする国保連医療保険ネットワークのIPアドレスを払い出せない場合がある。

2. 拠点内連携

パターン①：国保総合システムの外付けセグメント内に本システムの外付けシステムを構築する場合



パターン②：新規にVCNおよび外付けシステム用のセグメントを作成した上で本システムの外付けシステムを構築する場合

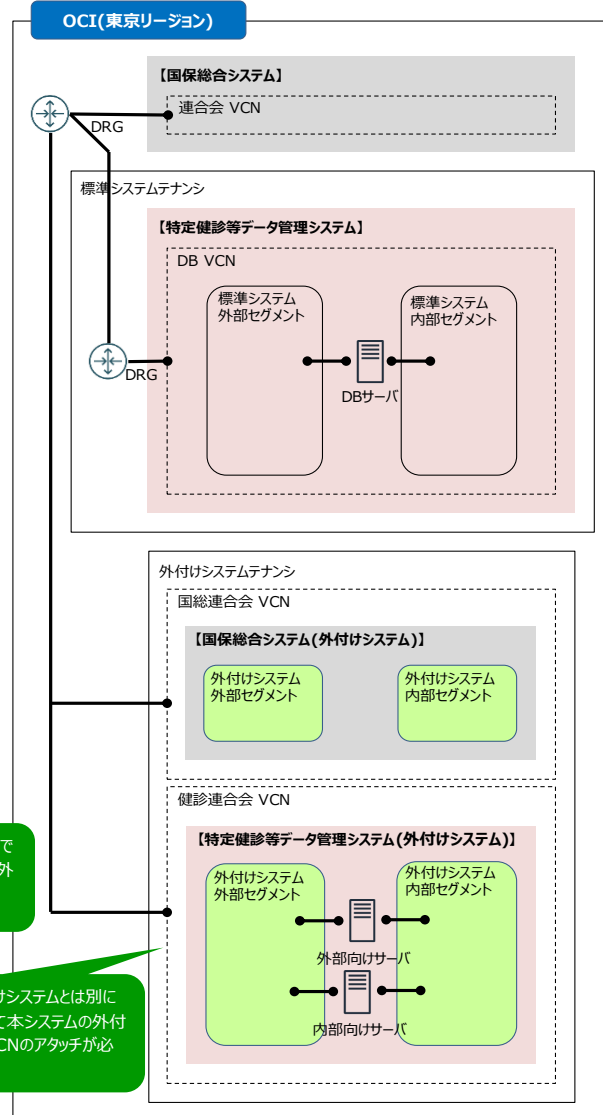


図 2.1-2 外付け連携イメージ(拠点内連携 - パターン別)

【パターン①】

- 国保連合会は、OCI上に構築した国保総合システムの外付けシステム用テナンシに、本システムの外付けシステムを構築する。
- 本システムの外付けシステムのIPアドレスは、国保総合システムの外付けシステムとして国保中央会もしくはデータ集配信システムから払い出された範囲において、国保連合会にて外付けシステムのIPアドレス設計を行う。

(本システムの外付けシステムを設計するにあたり、国保中央会もしくはデータ集配信システムから払い出されたIPアドレスが不足する場合は、新規でネットワークセグメントを国保中央会もしくはデータ集配信システムから払い出すので、国保総合システムの外付けシステムのVCNにネットワークセグメントの追加(CIDRブロックの追加)およびサブネットを追加する)

なお、VCNに追加可能なCIDRブロックの上限は5であるため、国保総合システムの外付けシステムVCNのCIDRブロックがすでに5設定されている場合は、パターン②で本システムの外付けシステムを構築する必要がある。

- 国保総合システムのDRG接続は、国保総合システムの外付けシステムにて実施しているため、本システムの外付けシステムでは不要である。

- 外付けシステムは、国保総合システムのDRGを経由して、標準システム、国保連合会との通信を可能とする。
- 国保連合会拠点から国保連医療保険ネットワークを経由してOCIと通信を行う場合、国総保険者FWにてソースNATを実施する。
- 国保連医療保険ネットワークを経由する通信帯域については、国保連連合会毎に一定の上限を設ける。(通信帯域は、国保総合システム、国保総合システムの外付けシステム等と共有する)
- 標準システムのバッチ用プリンタ、運用管理端末は、国保総合システムと同様に外付けシステム連携用セグメントに構築する。

【パターン②】

- 国保連合会は、OCI上に構築した国保総合システムの外付けシステム用テナンシに、本システムの外付けシステムを構築する。
もしくは、外付けシステム用テナンシを新規に契約し、本システムの外付けシステムを構築する。
- 国保連合会は、OCI上に本システムの外付けシステム用のVCNおよび外付けシステム用のセグメント(外部セグメント/内部セグメント)を構築する。
- 各セグメントのIPアドレスは、国保中央会もしくはデータ集配信システムから払い出された範囲において、国保連合会にてIPアドレス設計を行う。
- 国保連合会にて外付けシステムのVCNを国保総合システムのDRGに接続する。
- 外付けシステムは、国保総合システムのDRGを経由して、標準システム、国保連合会との通信を可能とする。
- 国保連合会拠点から国保連医療保険ネットワークを経由してOCIと通信を行う場合、国総保険者FWにてソースNATを実施する。
- 国保連医療保険ネットワークを経由する通信帯域については、国保連連合会毎に一定の上限を設ける。(通信帯域は、国保総合システム、国保総合システムの外付けシステム等と共有する)
- 標準システムのバッチ用プリンタ、運用管理端末は、国保総合システムと同様に外付けシステム連携用セグメントに構築する。

(1) 外付けシステム構築の流れ

拠点内連携を実現するための外付けシステム構築の流れを以下に示す。

表 2.1-1 外付けシステム構築の流れ(拠点内連携 – パターン①)

No.	国保 連合会	国保 中央会	作業概要
1	○	—	必要事項を記入して『外付けシステム接続申請シート』を国保中央会に提出する。 【記載項目事項】 ・Ⅰ-Ⅰ．標準システムとの接続構成の概略図 外付けシステム連携用セグメント(ローカル側)情報、連合会クライアント用セグメント情報 ・Ⅱ-Ⅲ．外付けシステム内部セグメント (本システムの外付けシステムで、外付けシステム内部セグメントを追加する場合)
2	—	○	必要事項を記入して『外付けシステム接続申請シート』を国保連合会に返却する。
3	○	—	国保中央会オンプレデータ集配信システム(更改後:セキュリティ等管理システム)から払い出したIPアドレスが不足する場合は、国保総合システムの外付けシステムで作成したVCNに、新規ネットワークセグメント(CIDRブロック)の追加およびVCN内にネットワークセグメントを追加する。 ※詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。
4	○	—	外付けシステムサーバ(以下、「外付けサーバ」と表記)を構築し、各サーバを外付けシステム内部セグメント、外付けシステム外部セグメントのいずれか(あるいは両方)のIPアドレスを国保連合会にて設定する。
5	○	—	外付けシステムの通信要件に応じて、外付けシステムのVCNにルート表およびセキュリティ・リストまたはNSGを追加する。 ※詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。
6	—	○	外付けシステムの通信要件に応じて、標準システムのVCNに、ルート表およびセキュリティ・リストまたはNSGを追加する。
7	○	○	必要に応じて、以下に対して Ping 疎通確認を行う。 外付けシステム外部セグメント上のサーバと標準システム外部セグメント上のサーバ間 外付けシステム内部セグメント上のサーバと標準システム内部セグメント上のサーバ間
8	○	—	必要事項を記入して『データ集配信システム（OCI）フィードバックシート』を国保中央会に提出する。 ※ クラウド環境に存在するデータ集配信システム(OCI)用の「データ集配信システム(OCI)インタフェース仕様書」を参照すること。
9	○	—	ウイルス対策ソフトのインストールやWSUS参照先の設定を行う。
10	—	○	『データ集配信システムフィードバックシート』を元にウイルス対策ソフトとWSUSの管理コンソール側設定を行う。

表 2.1-2 外付けシステム構築の流れ(拠点内連携 – パターン②)

No.	国保 連合会	国保 中央会	作業概要
1	○	—	外付けシステム用にOCIを契約し、OCI上に外付けシステムテナンシを作成する。 (国保総合システムの外付けシステムで、OCIを契約していない場合)
2	○	—	外付けシステムテナンシ上にVCNを構築する。

2. 拠点内連携

No.	国保 連合会	国保 中央会	作業概要
			※詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。
3	○	—	VCN内に以下1種類のネットワークセグメントを構築する。 内部セグメント：標準システム(内部セグメント)との通信を可能とするセグメント ※詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。 外部セグメントについては、No.6で中央会から『外付けシステム接続申請シート』が返却されてから構築する。
4	○	—	必要事項を記入して『外付けシステム接続申請シート』を国保中央会に提出する。 【記載項目事項】 ・Ⅰ-Ⅰ．標準システムとの接続構成の概略図 外付けシステム連携用セグメント(ローカル側)情報、連合会クライアント用セグメント情報 ・Ⅱ-Ⅰ．DRG接続情報 (国保総合システムの外付けシステムと別テナンシにVCNを構築する場合) ・Ⅱ-Ⅱ．DRGと接続するVCN情報 ・Ⅱ-Ⅲ．外付けシステム内部セグメント
5	—	○	『外付けシステム接続申請シート』によって国保連合会から提出された情報に基づいて、国保連合会が外付けシステムのVCNを国保総合システムのDRGに接続する作業を可能にするため、国保中央会にて国保連合会に対する権限設定を行う。
6	—	○	必要事項を記入して『外付けシステム接続申請シート』を国保連合会に返却する。
7	○	—	VCN内に以下1種類のネットワークセグメントを構築する。 外部セグメント：国保連合会からの通信を可能とするセグメント ※詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。
8	○	—	国保連合会は、国保中央会から提出された『外付けシステム接続申請シート』の情報に基づいて、外付けシステムのVCNを国保総合システムのDRGに接続する。 ※詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。
9	—	○	国保総合システムにて、外付けシステムのVCNがDRGに接続されたことを確認する。
10	○	—	外付けサーバを構築し、各サーバを外付けシステム内部セグメント、外付けシステム外部セグメントのいずれか(あるいは両方)のIPアドレスを国保連合会にて設定する。
11	○	—	外付けシステムの通信要件に応じて、外付けシステムのVCNにルート表およびセキュリティ・リストまたはNSGを追加する。 ※詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。
12	—	○	外付けシステムの通信要件に応じて、標準システムのVCNに、ルート表およびセキュリティ・リストまたはNSGを追加する。
13	○	○	必要に応じて、以下に対して Ping 疎通確認を行う。 外付けシステム外部セグメント上のサーバと標準システム外部セグメント上のサーバ間 外付けシステム内部セグメント上のサーバと標準システム内部セグメント上のサーバ間
14	○	—	必要事項を記入して『データ集配信システム（OCI）フィードバックシート』を国保中央会に提出する。 ※ クラウド環境に存在するデータ集配信システム(OCI)用の「データ集配信システム(OCI)インタフェース仕様書」を参照すること。
15	○	—	ウイルス対策ソフトのインストールやWSUS参照先の設定を行う。
16	—	○	『データ集配信システムフィードバックシート』を元にウイルス対策ソフトとWSUSの管理コンソール

2. 拠点内連携

No.	国保 連合会	国保 中央会	作業概要
			側設定を行う。

2.2. セグメント

拠点内連携に関するセグメントの詳細を以下に示す。

- 外付けシステム内部セグメント
外付けシステム内部セグメントは、標準システム内部セグメントとの通信を可能とし国保連合会拠点等のOCI外部との通信は不可とする。
- 外付けシステム外部セグメント
外付けシステム外部セグメントは、国保連合会拠点(連合会クライアント等)との通信を可能とする。
原則として、OCI内部(標準システム内部セグメント)との通信は不可とする。
- 外付けサーバ
外付けサーバは、外付けシステム内部セグメント、外付けシステム外部セグメントのいずれか(あるいは両方)のIPアドレスを国保連合会にて設定する。
※ 詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。
- 外付けシステム連携用セグメント(WAN)
国保連合会拠点(連合会クライアント等)から標準システム外部セグメントまたは外付けシステム外部セグメントに通信を行う場合に、国保中央会が国総保険者FWにソースNATを行う必要がある。外付けシステム連携用セグメント(WAN)は、ソースNATの変換後のIPアドレスとして使用する。

2.3. 接続構成

拠点内連携を行う上で構築または設定が必要となる接続構成要素を以下に示す。

- 国保総合システムのDRG

国保総合システム構築時に国保中央会が作成したDRG。

外付けシステムが標準システムや国保連合会拠点(連合会クライアント等)との通信経路を確保するために、国保総合システムのDRGと外付けシステムのVCNを接続する。

国保総合システムの外付けシステムのセグメント内に本システムの外付けシステムを構築する場合は、国保総合システムの外付けシステム構築時にDRGと接続済みであるため、本システムの外付けシステムでは接続を行わない。

- 標準システムのVCN

標準システム構築時に国保中央会が作成する。

標準システム外部セグメントおよび標準システム内部セグメントのIPアドレスをCIDRブロックとして指定する。

- 国保総合システムの外付けシステムVCN

国保総合システムの外付けシステムのセグメント内に本システムの外付けシステムを構築する場合に使用する。本システムの外付けシステムを検討、設計するにあたり、IPアドレスが不足する場合は、新規でネットワークセグメントを国保中央会およびオンプレデータ集配信システム(更改後:セキュリティ等管理システム)から払い出すので、連合会にて国保総合システムの外付けシステムVCNにネットワークセグメントの追加(CIDRブロックの追加)およびサブネットを追加する。

※ 詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。

- 外付けシステムのVCN

本システムの外付けシステムを新規にOCI上で構築する場合、または本システムの外付けシステム用に新規でVCNを作成する場合は、拠点内連携を行うにあたり外付けシステム用のテナンシ上に国保連合会にて作成する。外付けシステム外部セグメントおよび外付けシステム内部セグメントのIPアドレスを、CIDRブロックとして指定する。また、国保中央会から返却された『外付けシステム接続申請シート』の情報に基づいて、国保総合システムのDRGに対する接続設定を国保連合会にて行う。

※ 詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。

2.4. 物理線(通信メディア)

拠点内連携では、OCI上に外付けシステムを構築するため物理線を必要としない。

2.5. IPアドレス

拠点内連携における各セグメントのIPアドレスの詳細を以下に示す。

- 外付けシステム内部セグメント

データ集配信システムより国保連合会が独自に使用するために払い出されている、国保連合会管理のIPアドレスの範囲内で国保連合会にて検討、設計を行う。

ネットワークアドレス範囲については、標準的な値(24ビットマスク)に限定せず、セグメントの規模に応じて適宜分割して使用する。

セグメント情報は、国保連合会が『外付けシステム接続申請シート』に記入し、国保中央会に提出すること。

- 外付けシステム外部セグメント

NTT東日本より、国保連合会拠点と外付けシステムを通信可能とするために払い出されている、国保中央会管理のIPアドレスの範囲内で国保連合会にて検討、設計を行う。

外付けシステム外部セグメントのIPアドレスは、国保総合システムの外付けシステムで払い出させている「10.190.1xx.192/26」を使用すること。

※「xx」は、各国保連合会の都道府県番号を示す。

なお、国保総合システムの外付けシステムで払い出した「10.190.1xx.192/26」のセグメントでIPアドレスが不足する場合や、新規にVCNを構築し外付けシステム外部セグメントを作成する場合は、国保中央会が新規で外付けシステム外部セグメントを払い出す。

(外付けシステム外部セグメント(国保連医療保険ネットワークのIPアドレスは、枯渇しているため必要とする国保連医療保険ネットワークのIPアドレスを払い出せない場合がある)

- 外付けシステム連携用セグメント(WAN)

オンプレデータ集配信システム(更改後:セキュリティ等管理システム)より、国保連合会拠点とOCIを通信可能とするため(NAT用)に払い出されている、国保中央会管理のIPアドレスの範囲内で国保中央会にて検討、設計を行う。

2.6. NAT

拠点内連携におけるNATについて以下に示す。

- 国保連合会拠点からOCIに通信を行う場合、国保中央会が国総保険者FWにてソースNAT(国保連合会拠点側のIPアドレスの変換)を設定する必要がある。そのため、国保連合会は『外付けシステム接続申請シート』にて国保中央会に通信要件の提出を行い、これをもとに国保中央会は国総保険者FWにおけるソースNATの設計、検討を行う。
- ソースNATには、N対1と1対1の2つの方式が存在するため、国保中央会での設計方針とそれぞれの特徴について記載する。
 - N対1方式
国保連合会から提出された通信要件に基づき、国保連合会拠点からOCIへの片方向の通信で、かつ送信元となる装置や端末が多数あるような通信に対してN対1方式を使用する。
複数の送信元IPアドレスが外付けシステム連携用セグメント(WAN側)の1つのIPアドレスに集約して変換されるため、アクセスログ等に出力されるIPアドレスから送信元の装置を特定しにくくなるが、NAT用に使用する外付けシステム連携セグメント(WAN側)のIPアドレス数に限りがあるため、上記の方針にもとづいてN対1方式を採用する。
 - 1対1方式
国保連合会から提出された通信要件に基づき、国保連合会拠点とOCI間で双方向に行われる通信に対して使用する。
1つの送信元IPアドレスが1つの外付けシステム連携用セグメント(WAN側)IPアドレスに変換される。
- 国保中央会は『外付けシステム接続申請シート』にて、ソースNATに関する設定情報(実IPアドレスとNAT後のIPアドレスの変換テーブルやN対1と1対1のどちらの方式で変換するか)を、国保連合会に返却する。国保連合会は、外付けシステムのアクセス制限の検討、設計やIPアドレスにて通信元を特定する場合に、この情報を利用する。

2.7. ネットワーク障害対策

拠点内連携で使用するOCIサービスの冗長性はクラウドサービス事業者にて提供されるため個別の設計は不要である。

2.8. ルーティング

拠点内連携におけるルーティングは、外付けシステム側と標準システム側共に、ルート表に対するスタティックルーティングで制御する。

各セグメントのルート表における、ルーティングの詳細を以下に示す。

- 標準システム外部セグメントのルート表
宛先CIDRに「外付けシステム内部セグメントのネットワークセグメント」および「外付けシステム外部セグメントのネットワークセグメント」を、そのルートターゲットに「国保総合システムのDRG」を国保中央会にて設定する。「外付けシステム内部セグメントのネットワークセグメント」は、国保連合会が『外付けシステム接続申請用シート』にて提出したセグメントを指定する。
- 標準システム内部セグメントのルート表
宛先CIDRに「外付けシステム内部セグメントのネットワークセグメント」および「外付けシステム外部セグメントのネットワークセグメント」を、そのルートターゲットに「国保総合システムのDRG」を国保中央会にて設定する。「外付けシステム内部セグメントのネットワークセグメント」は、国保連合会が『外付けシステム接続申請用シート』にて提出したセグメントを指定する。
- 外付けシステム内部セグメントのルート表
宛先CIDRに「標準システム内部セグメントのネットワークセグメント」および「標準システム外部セグメントのネットワークセグメント」を、そのルートターゲットに「国保総合システムの標準システムDRG」を国保連合会にて設定する。「標準システム内部セグメントのネットワークセグメント」および「標準システム外部セグメントのネットワークセグメント」は国保中央会が『外付けシステム接続申請用シート』にて提出したセグメントを指定する。

OCI上に国総の外付けシステムがない場合は、国保連合会が本システムの外付けシステムVCNを国保総合システムのDRGに接続するまでは、ルートターゲットに「国保総合システムのDRG」を指定できないため、DRG接続後に国保連合会は本作業を行うこと。

※ 詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。

- 外付けシステム外部セグメントのルート表
外付けシステム外部セグメントのルート表で使用するルーティング方式(デフォルトルートの使用、または宛先毎にスタティックルート指定する等)については、国保連合会にて検討、設計を行う。スタティックルートを使用する際のルーティングの宛先は、国保中央会が返却した『外付けシステム接続申請用シート』のNAT情報を基に、宛先CIDRに「外付けシステム連携用セグメント(WAN側)IPアドレス」を、そのルートターゲットに「国保総合システムのDRG」を国保連合会にて設定する。ただし、外付けシステム外部セグメントのIPアドレスしか設定できない外付けサーバが存在し、そのサーバが標準システムとも通信させる必要がある場合に限り、宛先CIDRに「標準システム内部セグメントのネットワークセグメント」および「標準システム外部セグメントのネットワークセグメント」を、そのルートターゲットに「国保総合システムのDRG」を国保連合会にて設定追加する。

OCI上に国総の外付けシステムがない場合は、国保連合会が本システムの外付けシステムVCNを国保総合システムのDRGに接続するまでは、ルートターゲットに「国保総合システムのDRG」を指定できないため、DRG接続後に国保連合会は本作業を行うこと。

※ 詳細手順は「別冊1_外付けシステム連携設定手順」を参照すること。

2.9. アクセス制限

拠点内連携におけるアクセス制限の詳細について以下に示す。

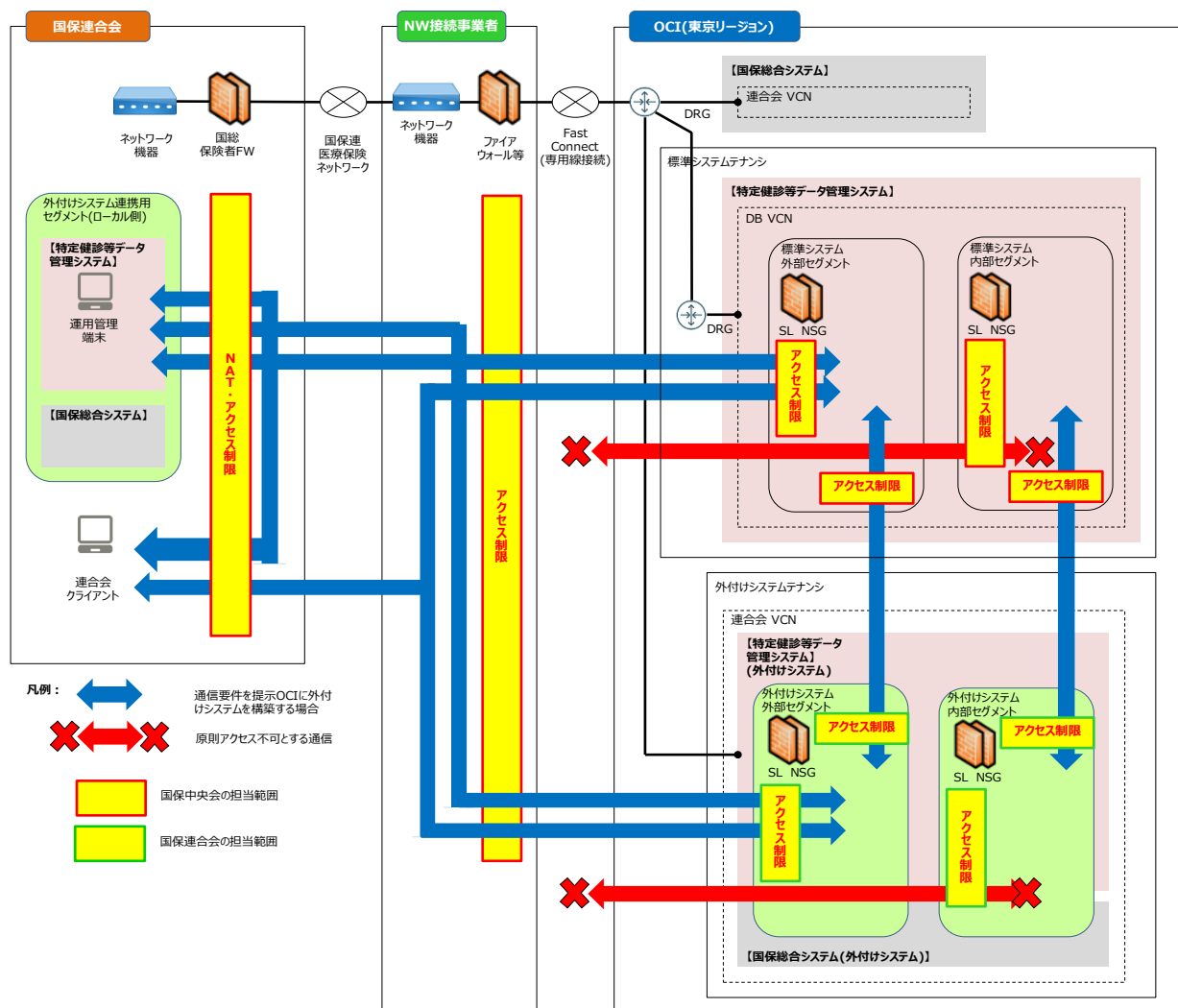


図 2.9-1 各セグメント間のアクセス制御(拠点内連携)

- 国保連合会拠点に設置する国総保険者FW、ネットワーク接続事業所に設置するファイアウォール、OCI上の標準システムのセキュリティ・リストまたはNSGを用いて国保中央会がアクセス制限を行う。アクセス制限はホワイトリストで制限し、原則プロトコルレベルでの制限を設ける。ただし、国保連合会拠点(連合会クライアント等)と外付けシステムの間はIPアドレスでの制限のみ実施し、プロトコルレベルでの制限を行わない。
- 国保中央会がアクセス制御の設定をするために、国保連合会は『外付けシステム接続申請用シート』に通信要件を記入し、国保中央会に提出すること。アクセス制限を行う機器を通過する以下の通信を対象に記入すること。
 - 国総保険者FWを経由する国保連合会拠点内の通信
 - 国保連合会拠点とOCIの間の通信
- 以下の通信はアクセスを禁止するため、『外付けシステム接続申請用シート』の通信要件に記入しないこと。
 - 国保連合会拠点の各セグメントと OCI 上の標準システム内部セグメントの間の通信

2.10. OCI管理コンソールへの接続

外付けシステムをOCIに構築する場合は、OCI管理コンソールへの接続をインターネット経由で行う必要がある。国保総合システムで、運用管理端末(OCI管理コンソール接続用)およびOCI管理コンソールへのインターネット回線を用意し、固定IPアドレスによるOCI管理コンソールへの接続制限を設定済みの場合は、本システムの外付けシステムで、新規に運用管理端末(OCI管理コンソール接続用)およびOCI管理コンソールへのインターネット回線を用意する必要はない。

本システムの外付けシステムを新規でOCIに構築する場合や、運用管理端末(OCI管理コンソール接続用)を増設する場合は、以下の作業が必要となる。

OCIコンソールへの接続ネットワークについては、セキュリティ対策のため固定IPアドレスが払出可能なインターネット回線を用いる。なお、国保総合システムと同様に、既存のインターネット回線(LAC社から提供されている情報系ネットワーク)も固定IPアドレス払出可能なため、こちらを活用して接続することも可能である。

用意したインターネット回線にて外付けシステムのテナンシ毎のOCI管理コンソールに接続後(接続するまでの作業は各国保連合会で実施すること)、セキュリティ対策として接続元の端末が限定されるようアクセス元制御(固定IPアドレスをホワイトリスト登録する)を実施する必要がある。

情報系ネットワークの利用有無については、国保総合システムのクラウド化の際に国保連合会へ確認済みであり、該当する国保連合会に対して国保中央会より固定IPアドレスを連絡(※1)済みである。自連合会で用意したインターネット回線の場合は、ISPへ連絡の上、固定IPアドレスの払出を受けること。

どちらの回線で接続しても本会から国保総合システムで提供した「ホワイトリスト登録手順書(※2)」「多要素認証登録手順書(※2)」に基づき、速やかにOCI管理コンソールにてホワイトリスト登録作業および運用管理端末(OCI管理コンソール接続用)にて多要素認証登録作業を実施すること。

※1 令和4年12月23日発出の「次期国保総合システム更改に関わる情報系ネットワークの固定IPアドレス通知について」にて該当連合会へ連絡済みである。

※2 「ホワイトリスト登録手順書」「多要素認証登録手順書」については、国保総合システムで提供したものを確認するか、添付資料を確認すること。

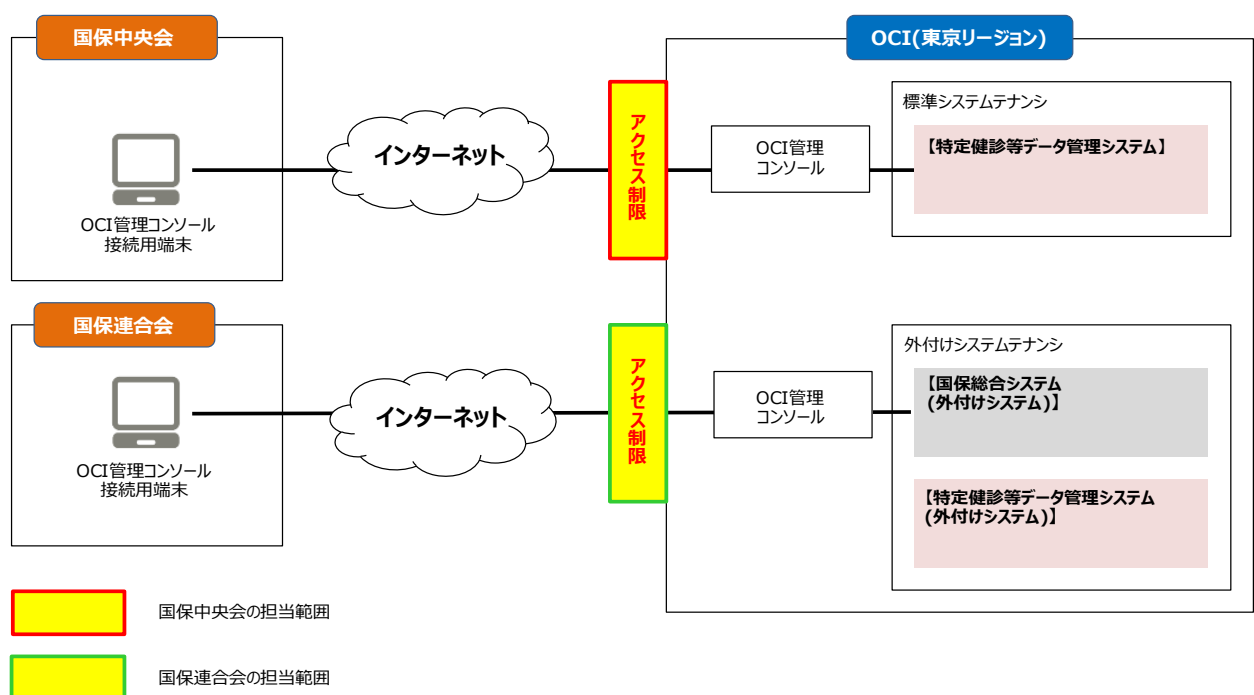


図 2.10-1 OCI管理コンソールへの接続イメージ

3. 拠点外連携

本章では、拠点外連携として、外付けシステムを国保連合会拠点(データセンター等)上に構築する場合について記載する。

3.1. 基本方針

拠点外連携を行う場合の、外付けシステムにおける連携イメージを以下に示す。

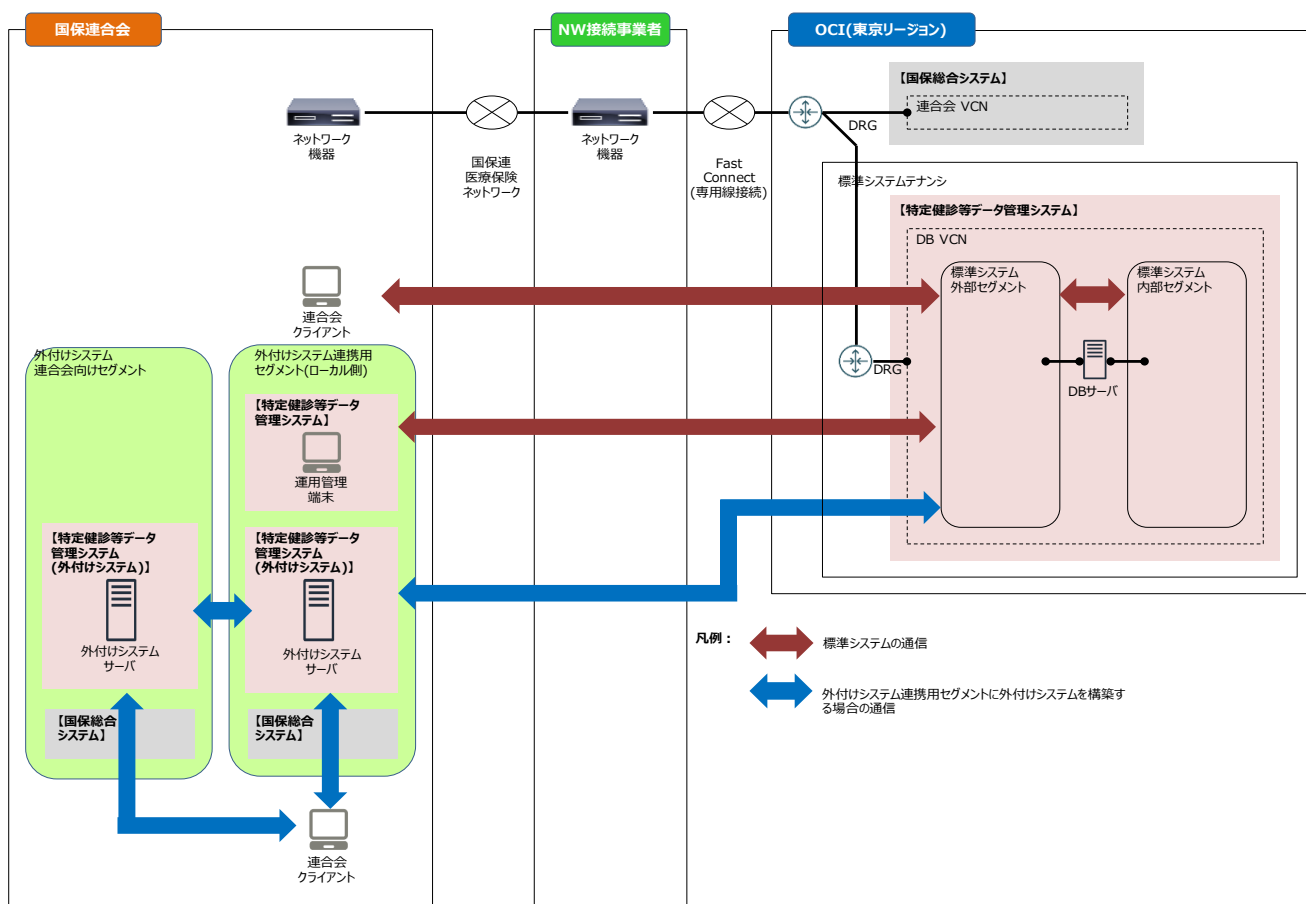


図 3.1-1 外付け連携イメージ(拠点外連携)

- 国保連合会は、外付けサーバを用途に応じて、国保総合システムで作成した外付けシステム連携用セグメント(ローカル側)、または従来の外付けシステム(外付けシステム連合会向けセグメント)に構築する。ただし、従来の外付けシステム(連合会向けセグメント)が、現行の標準システムのネットワーク装置(L3スイッチ等)に接続されている場合は、標準システムのネットワーク機器撤去に向けてコアスイッチ、国保総合システムの外付けシステムで用意した連合会独自NW機器の配下または新規に連合会独自NW機器を用意し移設する必要がある。
- なお、同一国保連合会が両外付けシステム連合会セグメント(外付けシステム連携用セグメント(ローカル側)ならびに外付けシステム連合会向けセグメント)を併用する構成も可とする。

3. 拠点外連携

- 外付けサーバを新規に用意する連合会独自NW機器の配下に設置する場合は、国保連合会は連合会独自NW機器を用意し、国保総合システムの外付けシステムで用意した連合会独自NW機器に接続する。接続に使用するケーブルは、国保連合会にて用意する。
 - 連合会独自NW機器の冗長化については国保連合会にて検討、設計を行う。
 - 外付けシステム連合会向けセグメント／外付けシステム連携用セグメント(ローカル側)／国総保険者FWと連合会独自NW機器の間のセグメントに割り当てるIPアドレスについては、オンプレデータ集配信システム(更改後:セキュリティ等管理システム)より国保連合会が独自に使用するために払い出されている、国保連合会管理のIPアドレスの範囲内で国保連合会にて検討、設計を行う。
 - 国保連合会拠点内のルーティングは原則スタティックルーティングを使用する。
 - 外付けシステム連携用セグメントは、国総保険者FWを経由してOCI上の標準システム外部セグメントとの通信を可能とし、連合会クライアントからのアクセスも可能とする。
- 国保連合会拠点から国保連医療保険ネットワークを経由してOCIと通信する場合、国総保険者FWにてソースNATを実施する。
- 国保連医療保険ネットワークを経由する通信帯域については、国保連連合会毎に一定の上限を設ける。

(通信帯域は、国保総合システム、国保総合システムの外付けシステム等と共有する)

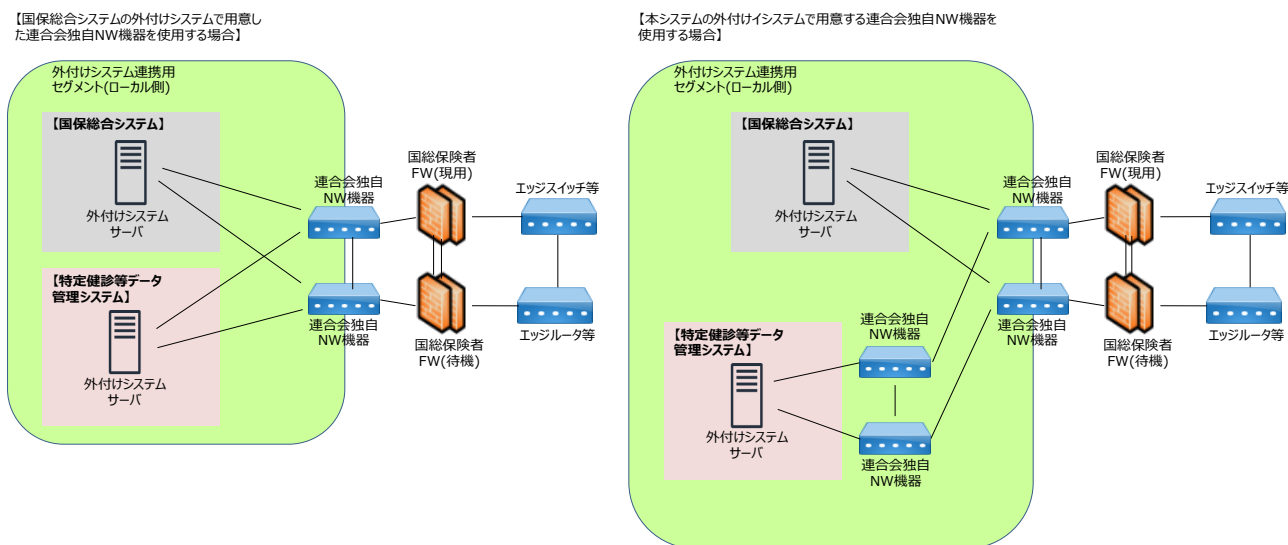


図 3.1-2 国総保険者FW配下に連合会独自NW機器を設置した場合のイメージ

(1) 外付けシステム構築の流れ

拠点外連携を実現するための外付けシステム構築の流れを、以下に示す。

表 3.1-1 外付けシステム構築の流れ(拠点外連携)

No.	国保 連合会	国保 中央会	作業概要
1	○	—	必要事項を記入して『外付けシステム接続申請用シート』を国保中央会に提出する。 【記載項目事項】 ・Ⅰ-Ⅰ．標準システムとの接続構成の概略図 外付けシステム連携用セグメント(ローカル側)情報、連合会クライアント用セグメント情報 ・Ⅲ-Ⅱ．外付けシステム連携用セグメント(ローカル側)情報 (本システムの外付けシステムで、外付けシステム連携用セグメント(ローカル側)を追加する場合) ・Ⅲ-Ⅲ．外付けシステム連合会向けセグメント情報 (本システムの外付けシステムで、外付けシステム連合会向けセグメントを追加する場合)
2	○	—	本システムの外付けシステムで新規に連合会独自NW機器を利用する場合は、国保連合会拠点内に国保連合会が新設する「連合会独自NW機器」に、以下のセグメントを構築する。 外付けシステム連携用セグメント(ローカル側)：OCI上の外部セグメントとの通信を可能とするセグメント ※「連合会独自NW機器」は国保連合会で調達する機器のため手順書展開対象外。
3	○	—	外付けサーバを構築する。連合会独自NW機器を利用する場合は、各サーバを外付けシステム連携用セグメント(ローカル側)へ接続する。
4	—	○	必要事項を記入して『外付けシステム接続申請用シート』を国保連合会に返却する。
5	○	—	連合会独自NW機器を新設する場合は、外付けシステム連携用セグメント(ローカル側)を構築する連合会独自NW機器を、国保総合システムの外付けシステムで用意した連合会独自NW機器へ結線する。 (※接続するために必要な設定をこのタイミングで実施) コアシッチを利用する場合、外付けシステム連携用セグメント(ローカル側)の機器を、コアシッチに結線する。コアシッチ配下に連合会独自NW機器を接続する構成も可とする。
6	○	—	必要に応じて、外付けシステム連携用セグメントからOCI上のDRG、標準システム外部セグメント上のサーバ宛のPing疎通確認を行う。
7	○	—	必要事項を記入して『データ集配信システムフィードバックシート』を国保中央会に提出する。 ※ 国保連合会拠点に存在するオンプレデータ集配信システム(更改後:セキュリティ等管理システム)用の「データ集配信システム インタフェース仕様書」を参照すること。
8	○	—	ウイルス対策ソフトのインストールやWSUS参照先の設定を行う。
9	—	○	『データ集配信システムフィードバックシート』を元にウイルス対策ソフトとWSUSの管理コンソール側設定を行う。

3.2. セグメント

国保連合会拠点内のネットワーク構成は、以下の10パターンを想定している。

表 3.2-1 国保連合会拠点内ネットワークの構成パターン

No.	図番号	構成パターン	概要
1	図 3.2-1	パターン1-A	・国保保険者NW加入連合会 ※連合会独自NW機器を調達
2	図 3.2-2	パターン1-B	・国保保険者NW加入連合会 ※コアスイッチに収容
3	図 3.2-3	パターン2-A	・国保保険者NW非加入連合会 (保険者向けFWの前方に保険者向けネットワーク機器がある構成) ※連合会独自NW機器を調達
4	図 3.2-4	パターン2-B	・国保保険者NW非加入連合会 (保険者向けFWの前方に保険者向けネットワーク機器がある構成) ※コアスイッチに収容
5	図 3.2-5	パターン3-A	・国保保険者NW非加入連合会(VPN接続を利用している構成) ※連合会独自NW機器を調達
6	図 3.2-6	パターン3-B	・国保保険者NW非加入連合会(VPN接続を利用している構成) ※コアスイッチに収容
7	図 3.2-7	パターン4-A	・国保保険者NW非加入連合会 (保険者向けネットワーク機器無し、またはL2スイッチがある構成) ※連合会独自NW機器を調達
8	図 3.2-8	パターン4-B	・国保保険者NW非加入連合会 (保険者向けネットワーク機器無し、またはL2スイッチがある構成) ※コアスイッチに収容
9	図 3.2-9	パターン5-A	・国保保険者NW非加入連合会 (保険者向けFWの後方に保険者向けネットワーク機器がある構成) ※連合会独自NW機器を調達
10	図 3.2-10	パターン5-B	・国保保険者NW非加入連合会 (保険者向けFWの後方に保険者向けネットワーク機器がある構成) ※コアスイッチに収容

3. 拠点外連携

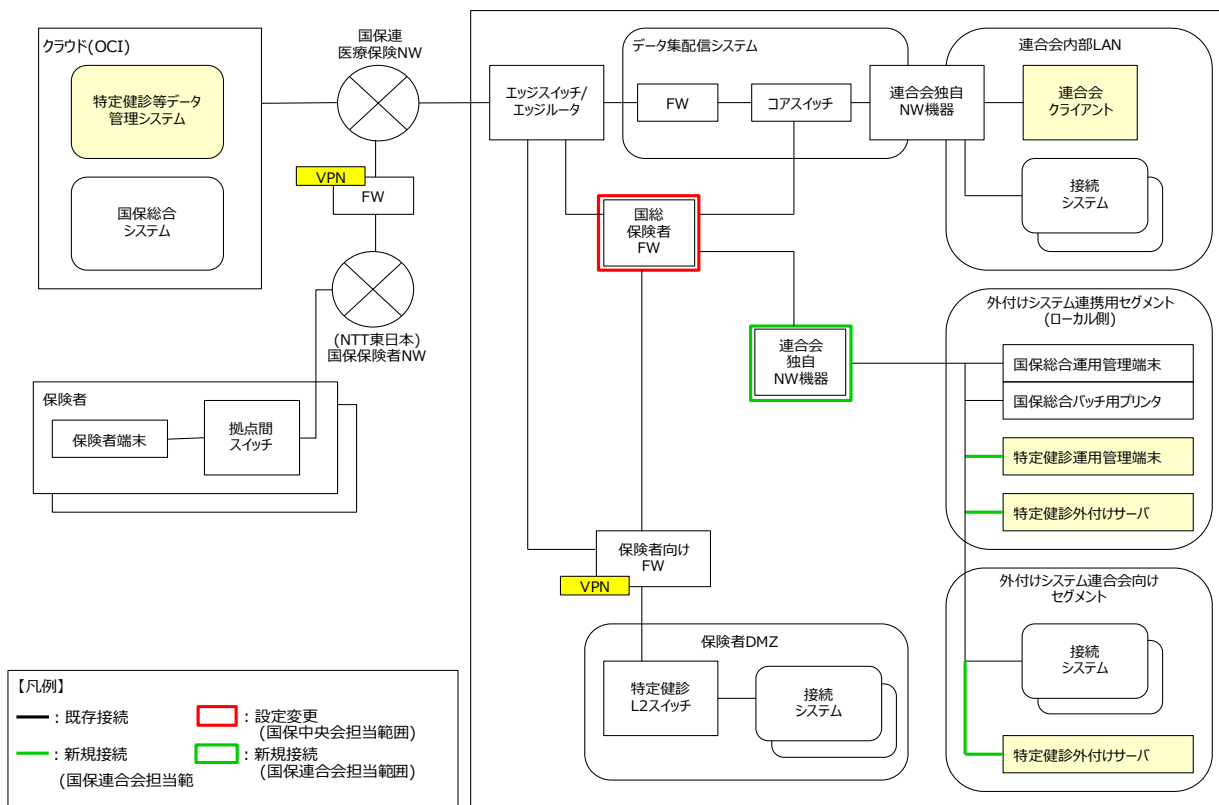


図 3.2-1 パターン1-A

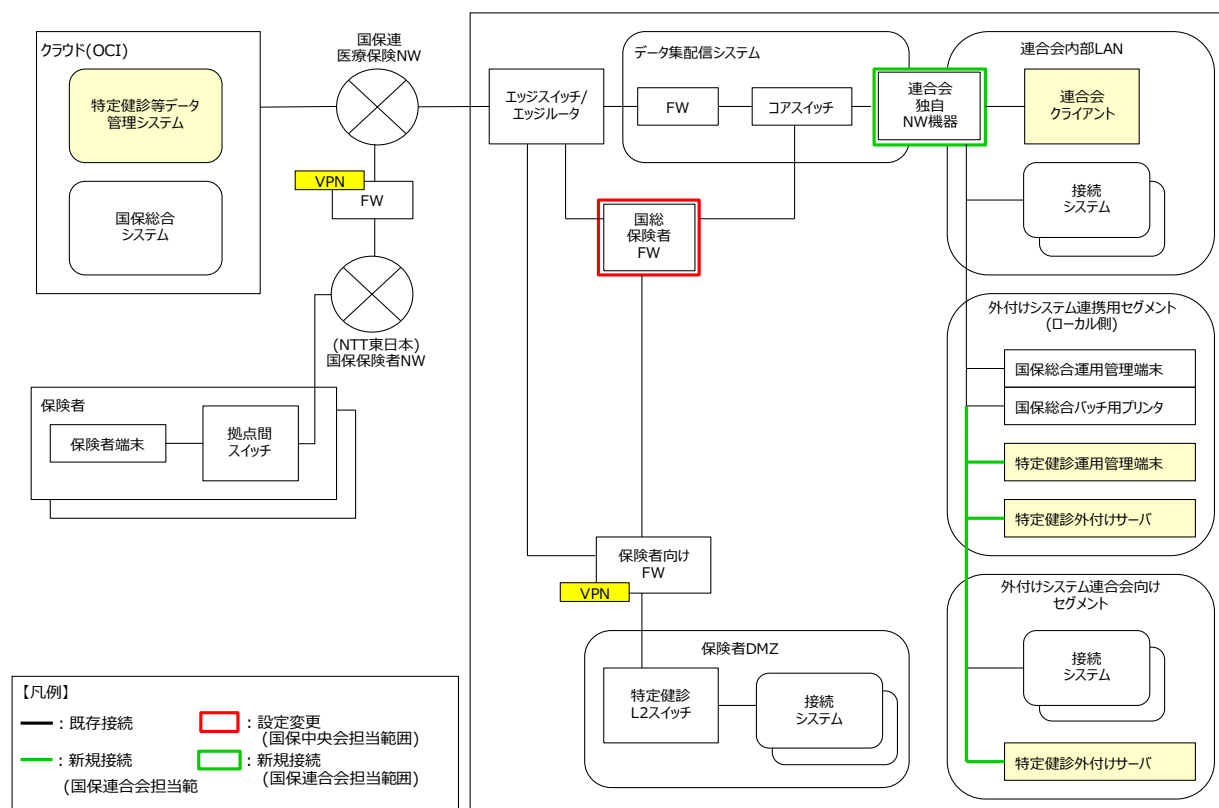


図 3.2-2 パターン1-B

3. 拠点外連携

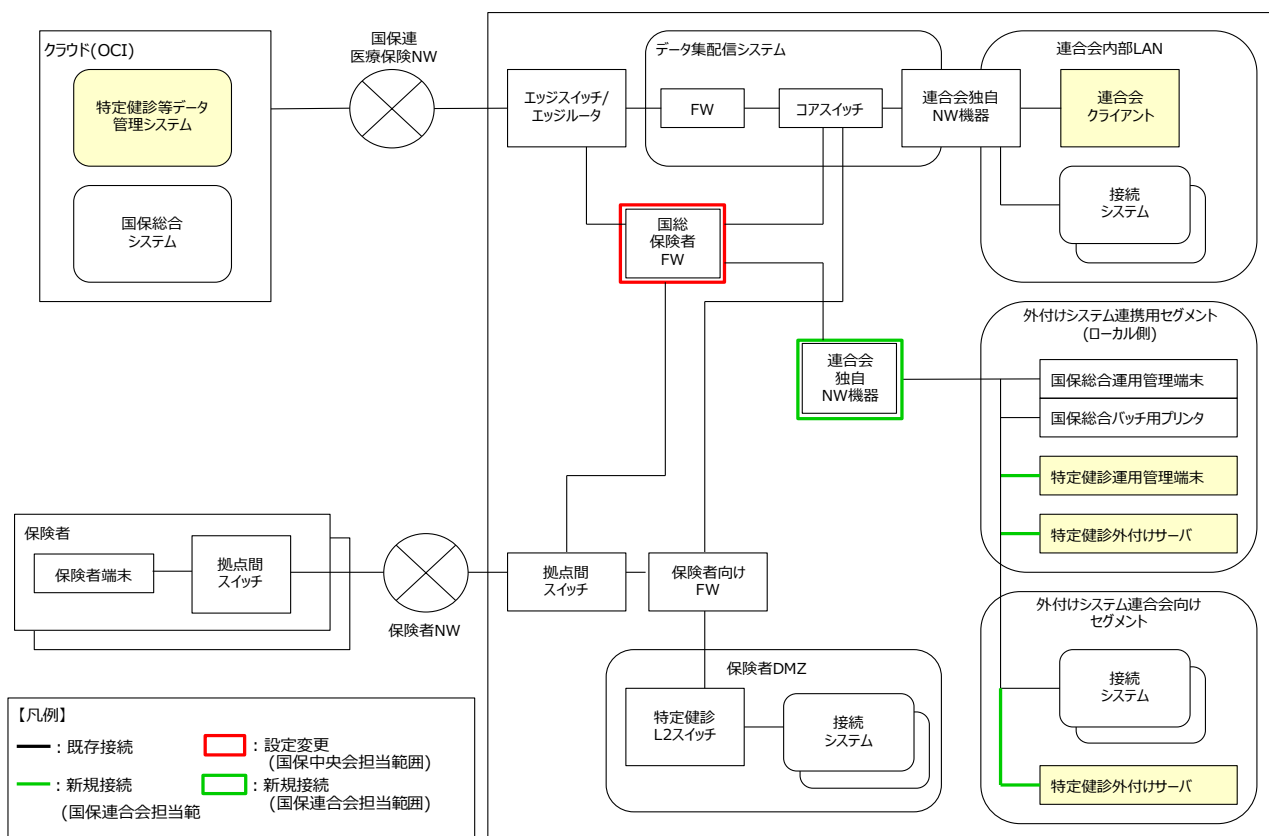


図 3.2-3 パターン2-A

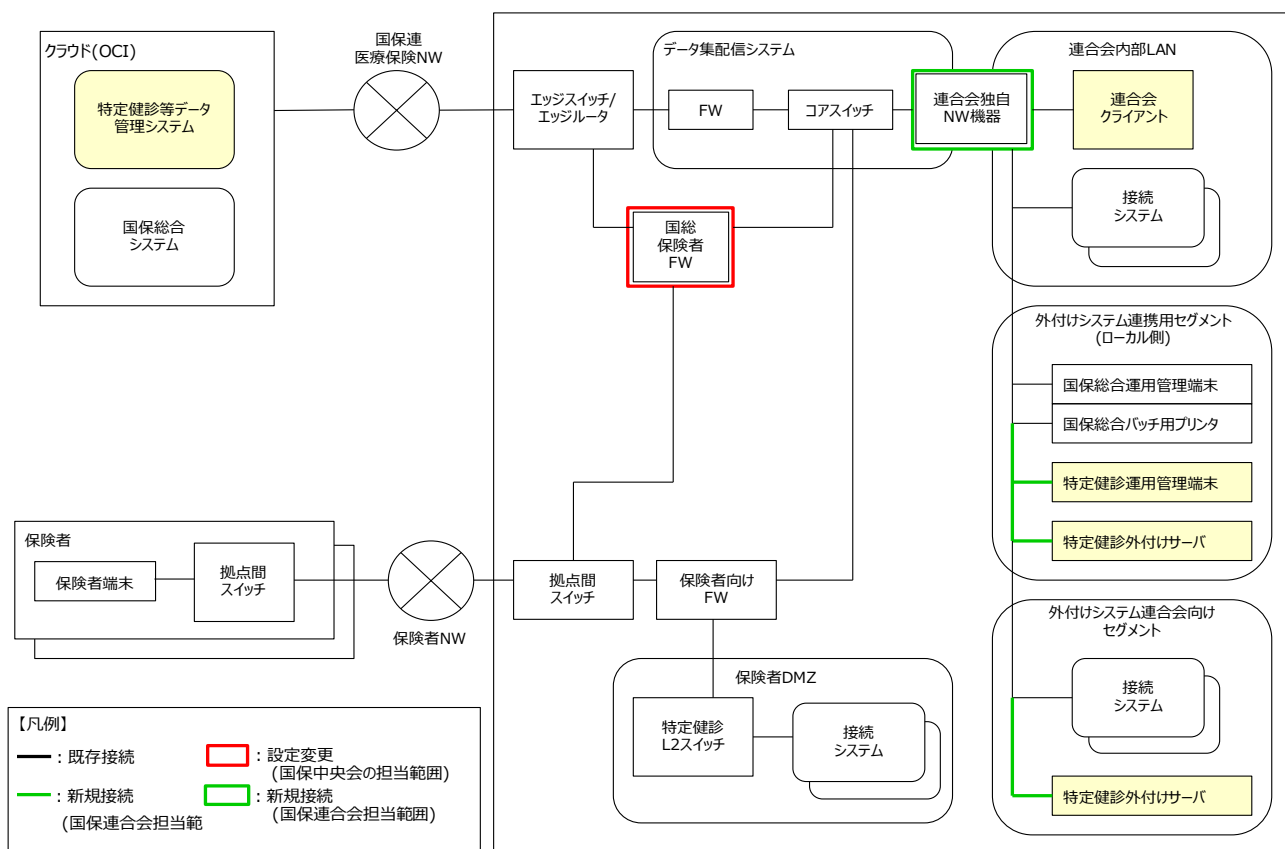


図 3.2-4 パターン2-B

3. 拠点外連携

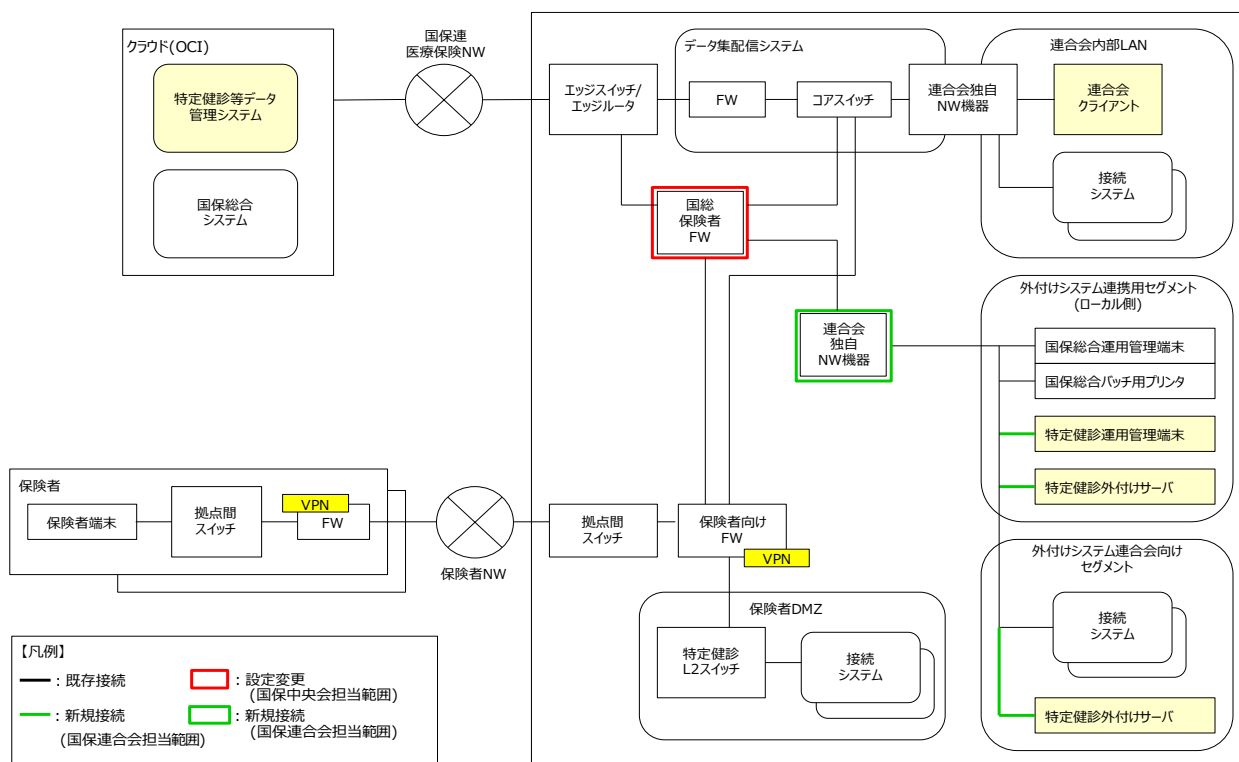


図 3.2-5 パターン3-A

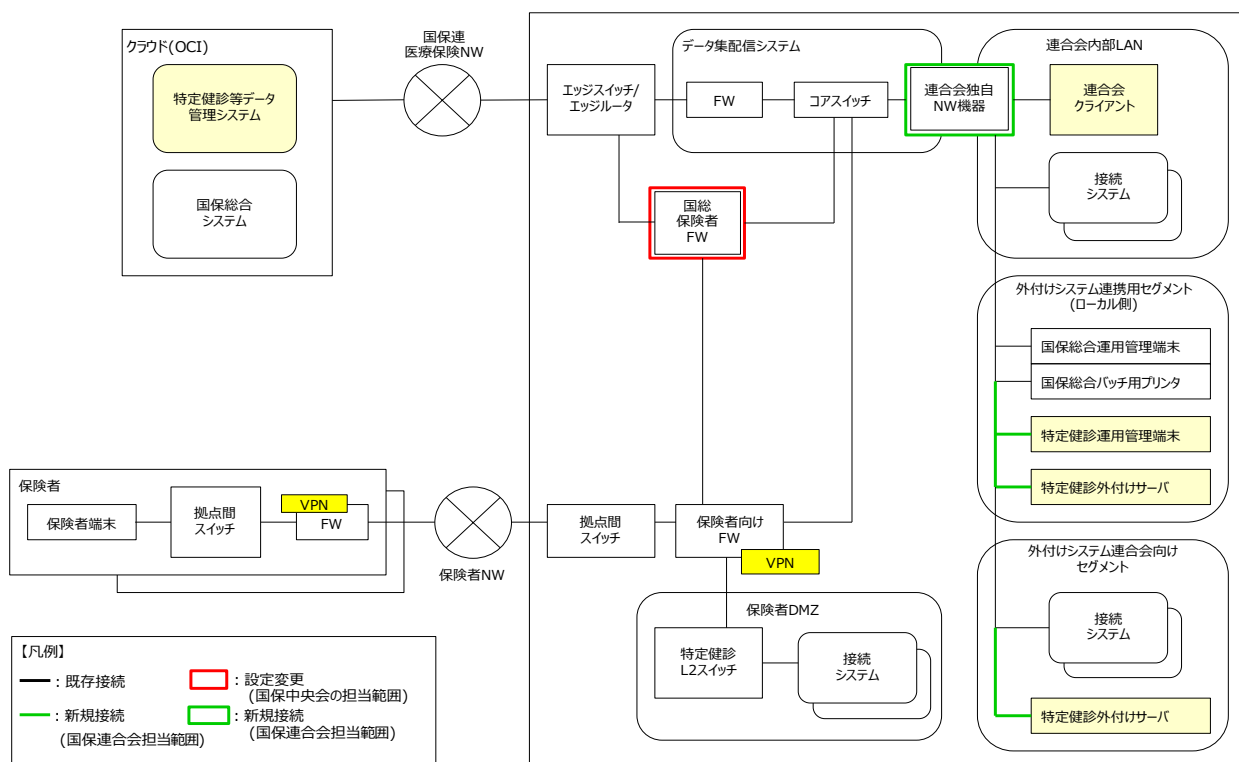


図 3.2-6 パターン3-B

3. 拠点外連携

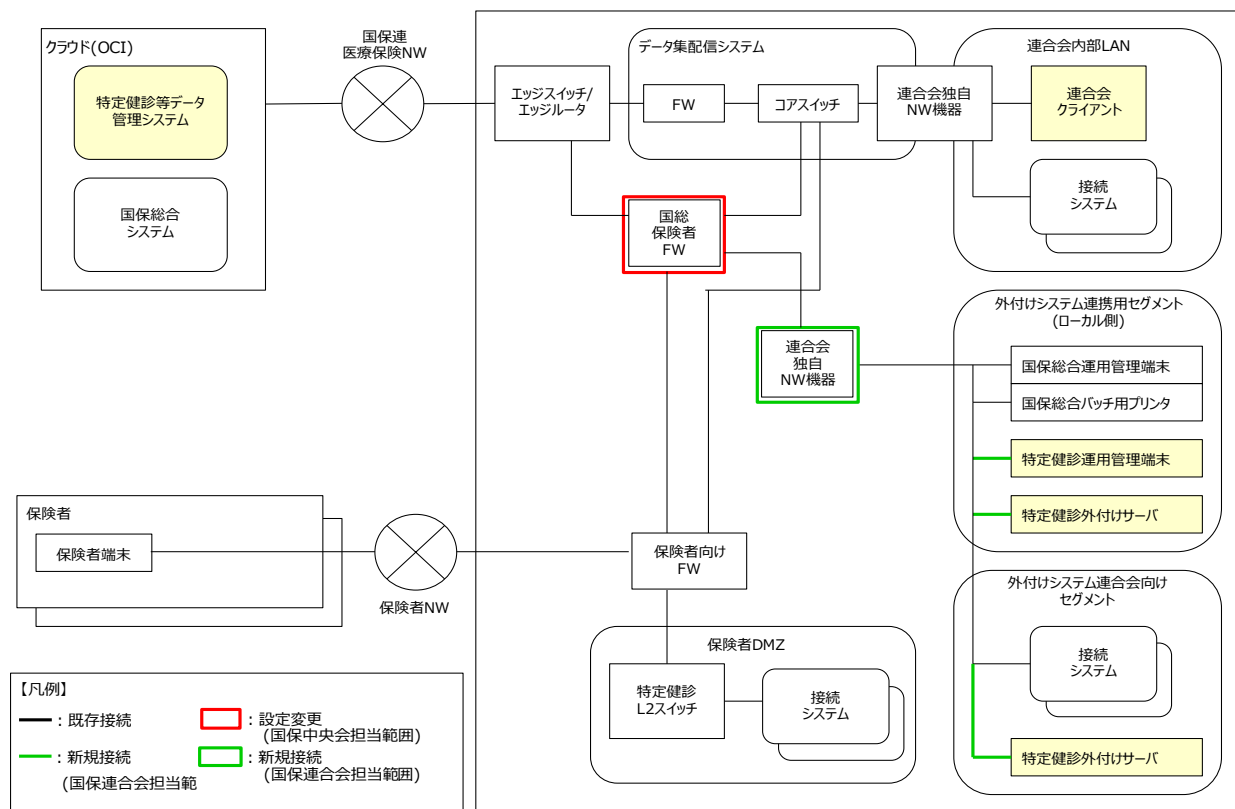


図 3.2-7 パターン4-A

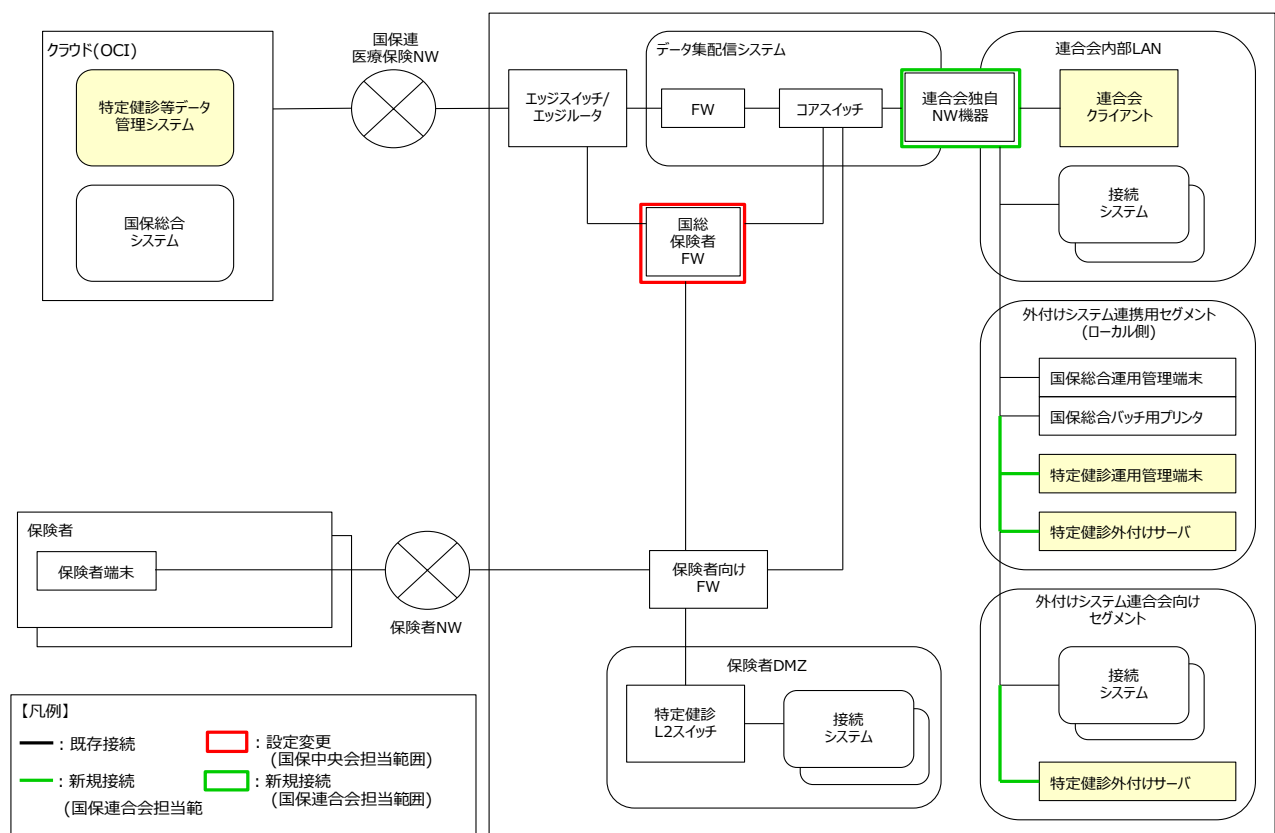
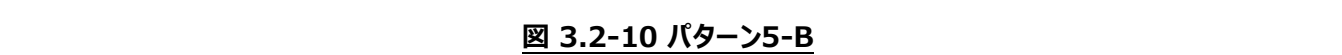


図 3.2-8 パターン4-B



拠点外連携に関するセグメントの詳細を以下に示す。

- 外付けシステム連携用セグメント(ローカル側)
外付けシステム連携用セグメントはOCI上の標準システムと通信する外付けサーバ、バッチ用プリンタ、運用管理端末を設置するために使用する。
OCI上の標準システムだけでなく連合会クライアントへの通信を可能とする。
- 外付けシステム連携用セグメント(WAN)
国保連合会拠点(連合会クライアント等)から標準システム外部セグメントに通信する際、国保中央会が国総保険者FWにてソースNATを行う必要がある。外付けシステム連携用セグメント(WAN)は、ソースNATの変換後のIPアドレスとして使用する。
- 外付けシステム連合会向けセグメント
外付けシステム連合会向けセグメントは、既存の国保連合会向けの外付けシステムを標準システムのネットワーク装置から移設する場合や、従来の国保連合会向けの外付けシステムと同様の目的のサーバを設置する場合に使用する。そのため、OCIとの通信は不可とし、連合会クライアントとの通信のみ可能とする。
- 国総保険者FWと連合会独自NW機器間のセグメント※1
国総保険者FWと連合会独自NW機器を接続するために使用する。
- 国総保険者FWとコアスイッチ間のセグメント
国総保険者FWとコアスイッチを接続するために使用する。

※1 連合会独自NW機器がL2機器の場合は、外付けシステム連携用セグメント(ローカル側)と同一セグメントとなる。

3.3. 接続構成

国保連合会内における各機器との接続構成については、「3.2 セグメント」を参照すること。

各機器における接続の詳細を以下に示す。

- 連合会独自NW機器

国保総合システムの外付けシステムで用意した連合会独自NW機器を本システムの外付けシステムでも使用する。もしくは、本システムの外付けシステムで外付けシステム連携用セグメント(ローカル側)、外付けシステム連合会向けセグメントのいずれかを設けるために国保連合会が連合会独自NW機器を用意する。国保総合システムの外付けシステムで連合会独自NW機器を用意している場合は、国保総合システムの外付けシステム連合会独自NW機器と本システムの外付けシステム連合会独自NW機器を接続する構成とし、国総保険者FWに国保総合システムと本システムで用意した連合会独自NW機器を同時に接続しない。

(※オンプレデータ集配信システム(更改後:セキュリティ等管理システム)のコアスイッチを利用する場合は、連合会独自NW機器を必須としない)

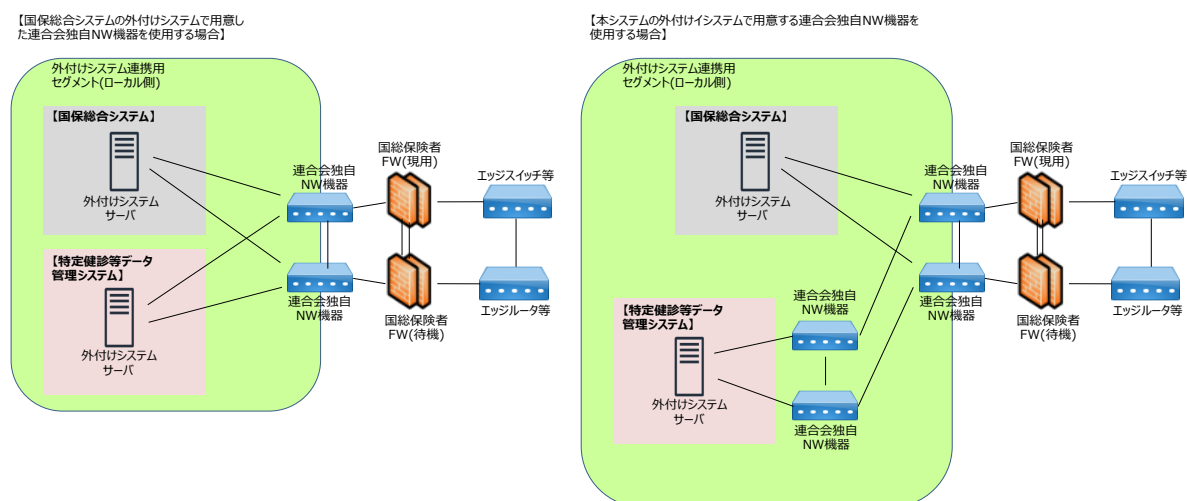


図 3.3-1 連合会独自NW機器設置イメージ

本システムの外付けシステムで連合会独自NW機器を用意する場合は、国保総合システムの外付けシステム連合会独自NW機器との間を1Gbps対応可能なポートで接続するものとする。連合会独自NW機器を2台の冗長構成とする場合は上記に加え、機器の冗長化機能を持つものとする。

国保連合会は、国保総合システムの外付けシステム連合会独自NW機器の現用系待機系と接続するため2ポート(現用待機構成であれば1ポートずつ)用意する。

本システムの外付けシステム連合会独自NW機器と国保総合システムの外付けシステム連合会独自NW機器を接続するポートのSpeed/Duplexはオートネゴシエーションを推奨し、原則としてタグVLANを使用しないアクセスポートとする。また、本システムの外付けシステム連合会独自NW機器と国保総合システムの外付けシステム連合会独自NW機器を接続するポートは連合会にて設計を行うこと。

- 国総保険者FW

国保総合システムで調達した国総保険者FWを本システムでも使用する。現用系待機系の2台による冗長構成で、2台ともコアスイッチと、必要な場合は連合会独自NW機器に接続する。

3.4. 物理線(通信メディア)

国保総合システムの外付けシステム連合会独自NW機器と本システムの外付けシステム連合会独自NW機器を接続する場合は、国保連合会が用意した機器の仕様に従いLANケーブルを用意すること。

3.5. IPアドレス

拠点外連携における各セグメントのIPアドレスの詳細を以下に示す。

- 外付けシステム連携用セグメント(ローカル側)
既存の外付けシステムと同様に、オンプレデータ集配信システム(更改後:セキュリティ等管理システム)より国保連合会が独自に使用するために払い出されている、国保連合会管理のIPアドレスの範囲内で国保連合会にて検討、設計を行う。
ネットワークアドレス範囲については標準的な値(24ビットマスク)に限定せず、セグメントの規模に応じて適宜分割して使用する。
セグメント情報は、国保連合会が『外付けシステム接続申請シート』に記入し、国保中央会に提出すること。
- 外付けシステム連携用セグメント(WAN側)
オンプレデータ集配信システム(更改後:セキュリティ等管理システム)より、国保連合会拠点とOCIを通信可能とするため(NAT用)に払い出されている、国保中央会管理のIPアドレスの範囲内で国保中央会にて検討、設計を行う。
(※詳細は後述 3. 6 参照)
外付けシステム連携用セグメント(WAN 側)のうち、外付けサーバへのアドレス変換に利用可能な IP アドレス数は 50 程度とする。
- 外付けシステム連合会向けセグメント
既存の外付けシステムと同様に、オンプレデータ集配信システム(更改後:セキュリティ等管理システム)より国保連合会が独自に使用するために払い出されている、国保連合会管理のIPアドレスの範囲内で国保連合会にて検討、設計を行う。
ネットワークアドレス範囲については標準的な値(24ビットマスク)に限定せず、セグメントの規模に応じて適宜分割して使用する。
セグメント情報は、国保連合会が『外付けシステム接続申請シート』に記入し、国保中央会に提出すること。
- 国総保険者FWと連合会独自NW機器の間のセグメント
オンプレデータ集配信システム(更改後:セキュリティ等管理システム)より国保連合会が独自に使用するために払い出されている、国保連合会管理のIPアドレスの範囲内で国保連合会にて検討、設計を行う。
ネットワークアドレス範囲については標準的な値(24ビットマスク)に限定せず、セグメントの規模に応じて適宜分割して使用する。
セグメント情報は、国保連合会が『外付けシステム接続申請シート』に記入し、国保中央会に提出すること。
- 国総保険者FWとコアスイッチ間のセグメント
国保中央会は、オンプレデータ集配信システム(更改後:セキュリティ等管理システム)にIPアドレスの払い出し依頼を行い、国総保険者FWの該当セグメントのIPアドレスについて、国保中央会にて設計を行う。

※1 連合会独自NW機器がL2機器の場合は外付けシステム連携用セグメント(ローカル側)と同一セグメントとなる。

3.6. NAT

保連合会拠点から標準システム外部セグメントに通信する際、国保中央会が国総保険者FWにてソースNAT(国保連合会拠点側のIPアドレスの変換)を設定する必要がある。そのため、国保連合会は『外付けシステム接続申請シート』にて国保中央会に通信要件の提出を行う(※通信要件の提出方法の詳細は後述3.9参照)これを基に国保中央会は国総保険者FWにおけるソースNATの設計、検討を行う。

- ソースNATには、N対1と1対1の2つの方式が存在するため、国保中央会での設計方針とそれぞれの特徴について記載する。
 - N対1方式
国保連合会から提出された通信要件に基づき、国保連合会拠点から標準システム外部セグメントへの片方向の通信で、かつ送信元となる装置や端末が多数あるような通信に対してN対1方式を使用する。
複数の送信元IPアドレスが外付けシステム連携用セグメント(WAN側)の1つのIPアドレスに集約して変換されるため、アクセスログ等に出力されるIPアドレスから送信元の装置を特定しにくくなるが、NAT用に使用する外付けシステム連携セグメント(WAN側)のIPアドレス数に限りがあるため、上記の方針にもとづいてN対1方式を採用する。
 - 1対1方式
国保連合会から提出された通信要件に基づき、国保連合会拠点と標準システム外部セグメント間で双方向に行われる通信に対して使用する。
1つの送信元IPアドレスが1つの外付けシステム連携用セグメント(WAN側)IPアドレスに変換される。
- 国保中央会は『外付けシステム接続申請シート』にて、ソースNATに関する設定情報(実IPアドレスとNAT後のIPアドレスの変換テーブルやN対1と1対1のどちらの方式で変換するか)を、国保連合会に返却する。国保連合会は、外付けシステムのアクセス制限の検討、設計やIPアドレスにて通信元を特定する場合に、この情報を利用する。

3.7. ネットワーク機器障害対策

ネットワークの信頼性確保のため、連合会独自NW機器等、国保連合会が用意するネットワーク機器については、機器の二重化を行うことで経路の切り替えが可能な構成を推奨する。

本システムの外付けシステムで連合会独自NW機器を用意する場合は、国保総合システムの外付けシステム連合会独自機器と接続するものとし、国保総合システムの外付けシステム連合会独自機器と本システムの外付けシステム連合会独自NW機器の冗長化については、国保連合会にて検討、設計を行うこと。

参考資料として、国保総合システムの外付けシステムと国総保険者FW間の障害対策を、連合会独自NW機器2台で冗長化を行う場合と1台の場合のそれぞれについて以下に示す。

- 連合会独自NW機器2台で冗長化を行う場合

連合会独自NW機器2台で冗長化を行う場合の設計方針、障害時の動作について以下に示す。

- 設計方針

2台の連合会独自NW機器から、2台の国総保険者FWにそれぞれ1本ずつ、ケーブル接続すること。迂回路として、連合会独自NW機器間の渡り部分もケーブル接続すること。

国保中央会が『外付けシステム接続申請用シート』にて提出するセグメント情報に基づいて、連合会独自NW機器と国総保険者FW間のセグメントおよび連合会独自NW機器の渡り部分のセグメントは、すべて同一セグメントとなるよう、国保連合会で連合会独自NW機器を構築すること。なお、国総保険者FW間の渡り部分はHA専用ケーブルによる接続または上記と異なるセグメントを設定するため、連合会独自NW機器と国総保険者FWの間でループ構成とはならない。

また、国総保険者FWにとって外付けシステム宛のネクストホップとなる連合会独自NW機器のIPアドレスは、国保連合会が検討、設計を行い『外付けシステム接続申請シート』に記入し国保中央会に提出すること。

上記以外の連合会独自NW機器の冗長化方式(スタック接続、VRRP等)については国保連合会にて検討、設計を行う。

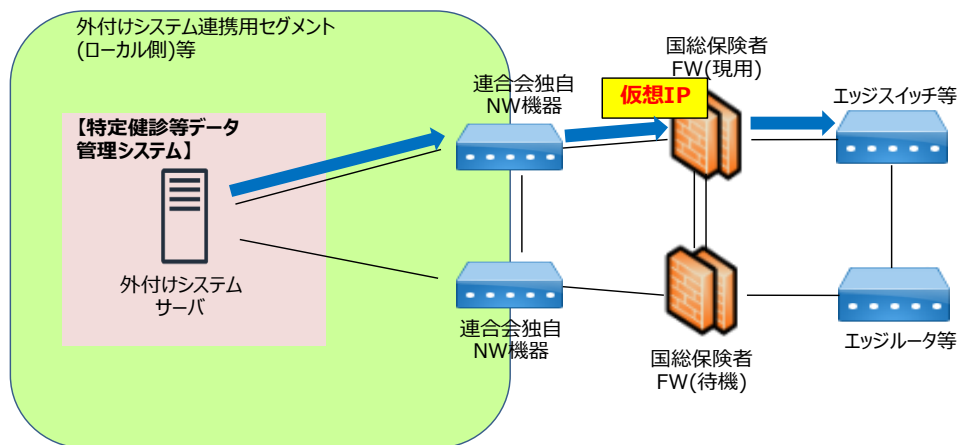


図 3.7-1 連合会独自NW機器冗長化のネットワーク構成※1

※1 連合会独自NW機器がL2機器の場合は、国総保険者FWと連合会独自NW機器の間のセグメントは外付けシステム連携用セグメント（ローカル側）と同一セグメントになる。

➤ 障害発生時の迂回路

連合会独自NW機器から国総保険者FW(現用)の間で障害が発生した場合、国総保険者FWでは現用系と待機系が切り替わる。連合会独自NW機器は国総保険者FW(待機)に仮想IPアドレスが引き継がれたことを認識し、通信経路の切り替えを行う。

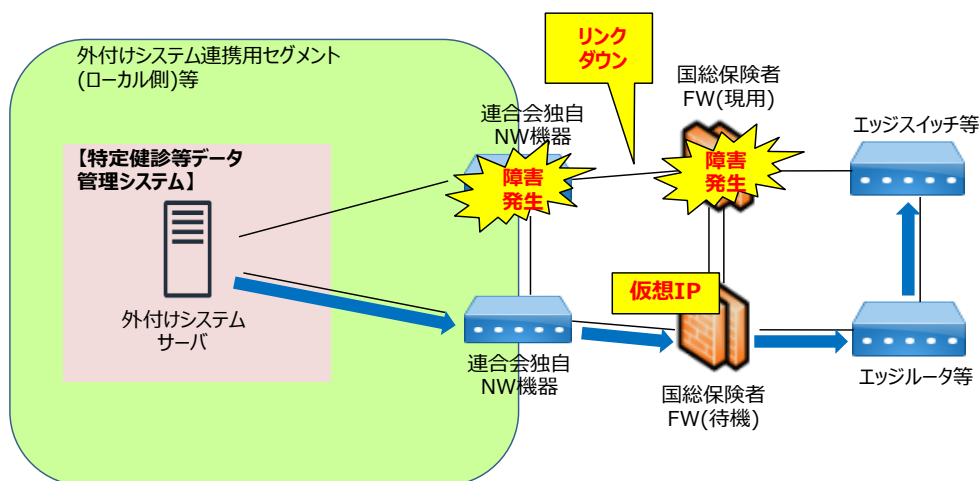


図 3.7-2 連合会独自NW機器を冗長化した場合の障害発生時の迂回路1

なお、連合会独自NW機器と国総保険者FW(現用)の間で障害が発生しない場合(国総保険者FW(現用)とエッジスイッチ、エッジルータ間での回線障害等)でも、国総保険者FWでは現用待機構成により現用系と待機系が切り替わる。この場合においても、連合会独自NW機器は国総保険者FW(待機)に仮想IPアドレスが引き継がれたことを認識し、通信経路の切り替えが行える必要がある。

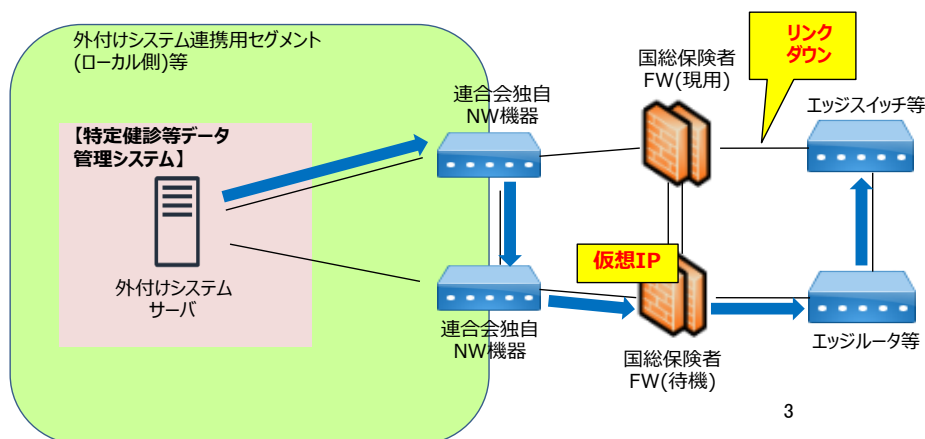


図 3.7-3 連合会独自NW機器を冗長化した場合の障害発生時の迂回路2

- 連合会独自NW機器1台の場合

連合会独自NW機器 1 台の場合の設計方針、障害時の動作について以下に示す。

- 設計方針
- 1台の連合会独自NW機器から、2台の国総保険者FWにそれぞれ1本ずつ、ケーブル接続すること。

国保中央会が『外付けシステム接続申請用シート』にて提出するセグメント情報に基づいて、連合会独自NW機器と国総保険者FW間のセグメントはすべて同一セグメントとなるよう、国保連合会で連合会独自NW機器を構築すること。なお、国総保険者FW間の渡り部分はHA専用ケーブルによる接続または上記と異なるセグメントを設定するため、連合会独自NW機器と国総保険者FWの間でループ構成とはならない。

また、国総保険者FWにとって外付けシステム宛のネクストホップとなる連合会独自NW機器のIPアドレスは、国保連合会が検討、設計を行い『外付けシステム接続申請シート』に記入し国保中央会に提出すること。

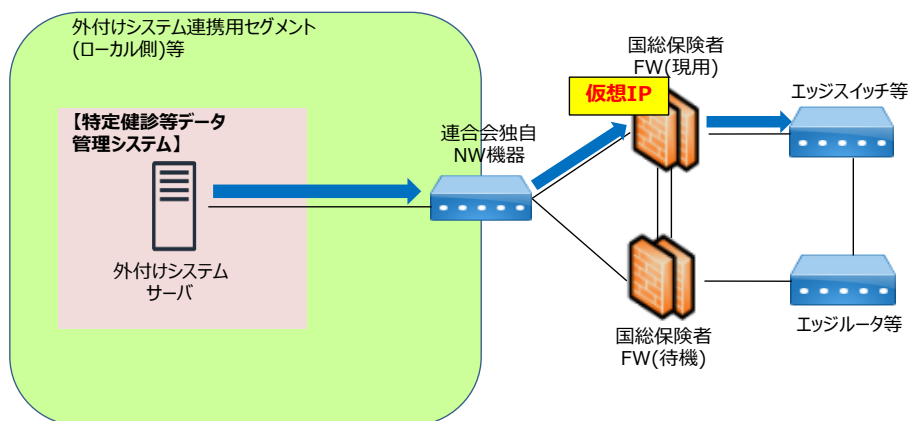


図 3.7-4 連合会独自NW機器1台のネットワーク構成^{※1}

※1 連合会独自NW機器がL2機器の場合は、国総保険者FWと連合会独自NW機器の間のセグメントは外付けシステム連携用セグメント(ローカル側)と同一セグメントになる

➤ 障害発生時の迂回路

国総保険者FW(現用)で障害が発生した場合、国総保険者FWでは現用系と待機系が切り替わる。連合会独自NW機器は国総保険者FW(待機)に仮想IPアドレスが引き継がれたことを認識し、通信経路の切り替えを行う。

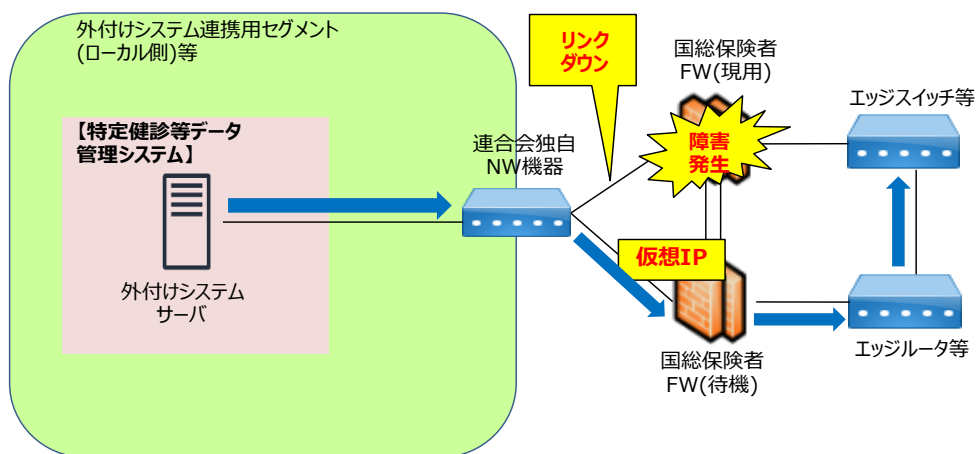


図 3.7-5 連合会独自NW機器1台の場合の障害発生時の迂回路1

なお、連合会独自NW機器と国総保険者FW(現用)の間で障害が発生しない場合(国総保険者FW(現用)とエッジスイッチの回線障害等)でも、国総保険者FWでは現用待機構成により現用系と待機系が切り替わる。この場合においても、連合会独自NW機器は国総保険者FW(待機)に仮想IPアドレスが引き継がれたことを認識し、通信経路の切り替えが行える必要がある。

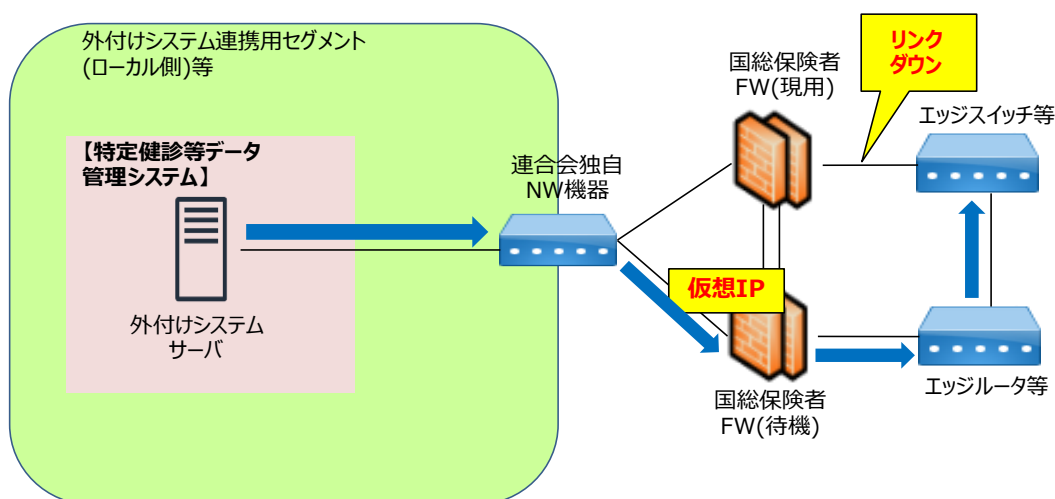


図 3.7-6 連合会独自NW機器1台の場合の障害発生時の迂回路2

3.8. ルーティング

拠点外連携におけるルーティングは、原則スタティックルーティングを使用する。各機器におけるルーティングの詳細を以下に示す。

- コアスイッチ、または連合会独自NW機器配下に接続する装置(外付けサーバ、バッチ用プリンタ、運用管理端末等)

コアスイッチ、または連合会独自NW機器のIPアドレスをネクストホップとする。^{※1}

ルーティング方式(デフォルトルートの使用、または宛先毎にスタティックルートを指定する等)については、国保連合会にて検討、設計を行う。スタティックルートを使用する際のルーティングの宛先は、国保連合会の通信要件に基づいて国保連合会自身で指定すること。また、ネクストホップはコアスイッチ、または連合会独自NW機器の構成(VRRP等の冗長構成を使用した場合には仮想IPアドレスをネクストホップに指定する等)に基づいて指定すること。

- 連合会独自NW機器

本システムの外付けシステムで連合会独自NW機器を用意する場合は、国保総合システムの外付けシステムの連合会独自NW機器のIPアドレスをネクストホップとする。^{※2}

ルーティング方式(デフォルトルートの使用、または宛先毎にスタティックルートを指定する等)については、国保連合会にて検討、設計を行う。スタティックルートを使用する際のルーティングの宛先は、国保連合会の通信要件に基づいて国保連合会自身で指定すること。

- 国総保険者FW

宛先が外付けシステム連携用セグメント、外付けシステム連合会向けセグメント、外付けシステム保険者向けセグメントの場合、コアスイッチ、または連合会独自NW機器のIPアドレスをネクストホップとする。

^{※3}

国保中央会は、国保連合会が『外付けシステム接続申請用シート』にて提出した通信要件に基づいてルーティングの宛先を指定する。なお、ネクストホップとなる国保総合システムの外付けシステムの連合会独自NW機器のIPアドレスは、国保連合会が検討、設計を行い『外付けシステム接続申請シート』に記入し国保中央会に提出したIPアドレスとなるよう、国保連合会で連合会独自NW機器を構築すること。(※詳細は前述 3. 7 参照)

※1 連合会独自NW機器が、L2機器の場合は国総保険者FWをネクストホップとする。

※2 連合会独自NW機器が、L2機器の場合は管理用ルーティング以外不要とする。

※3 連合会独自NW機器が、L2機器の場合のネクストホップは『外付けシステム接続申請シート』に記載したものとする。

3.9. アクセス制限

拠点外連携におけるアクセス制限の詳細について以下に示す。

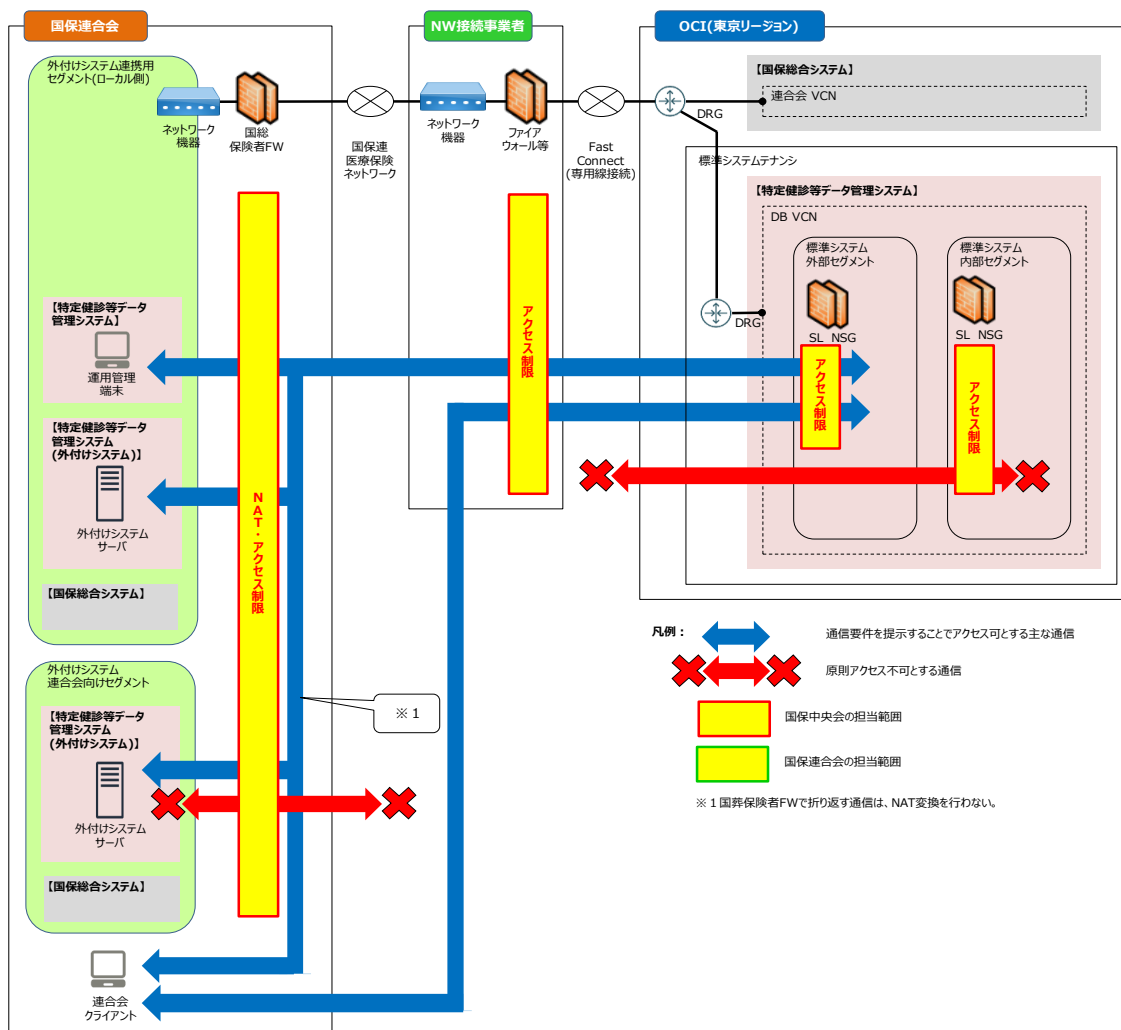


図 3.9-1 各セグメント間のアクセス制御(拠点外連携)

- 国保連合会拠点に設置する国総保険者FW、NW接続事業所に設置するファイアウォール、OCI上の標準システムのセキュリティ・リストまたはNSGを用いて、国保中央会がアクセス制限は行う。アクセス制限はホワイトリストで制限し、原則プロトコルレベルでの制限を設ける。ただし、国保連合会と外付けシステムの間はIPアドレスでの制限のみ実施し、プロトコルレベルでの制限を行わない。
- 国保中央会がアクセス制御の設定をするために、国保連合会は『外付けシステム接続申請用シート』に通信要件を記入し、国保中央会に提出すること。アクセス制限を行う機器を通過する以下の通信を対象に記入すること。
 - 国総保険者FWを経由する国保連合会拠点内の通信
 - 国保連合会拠点とOCIの間の通信
- 以下の通信はアクセスを禁止するため、『外付けシステム接続申請用シート』の通信要件に記入しないこと。
 - 国保連合会拠点の各セグメントとOCI上の標準システム内部セグメントの間の通信
 - 国保連合会拠点の外付けシステム連合会向けセグメントとOCI上の各セグメント間の通信

4. 共通事項（拠点内連携/拠点外連携）

4.1. 帯域制御

帯域制御イメージ（拠点内連携／拠点外連携）を以下に示す。

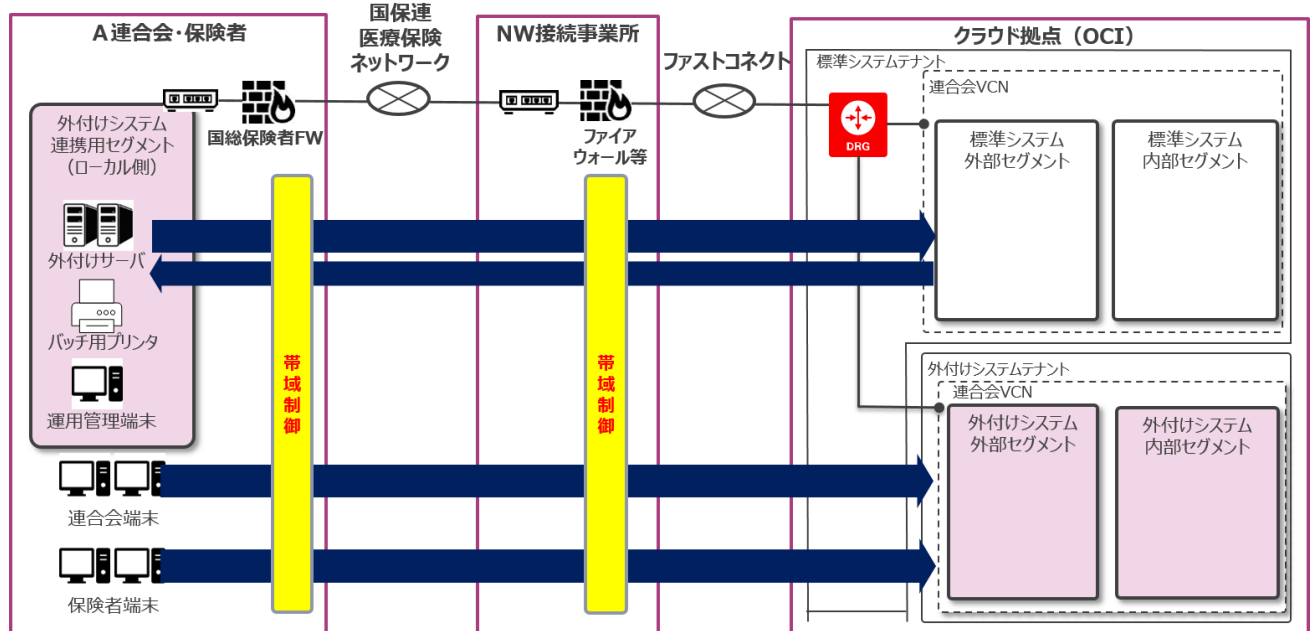


図4. 1 - 1 帯域制御イメージ（拠点内連携／拠点外連携）

- 国保連医療保険ネットワークの通信帯域の逼迫を回避するため、以下の方針に基づき国保中央会にて国総保険者FWまたはNW接続事業所内のファイアウォールで帯域制御を実施する。
 - 国保連合会内の制御機器（国総保険者FW）

以下の通信帯域（合計）が一定以内に収まるよう、帯域上限を設ける。

 - ・ 外付けシステム連携用セグメントからOCIへの通信
 - ・ 連合会クライアント、保険者クライアントからOCIへの通信
 - NW接続事業所内の制御機器

以下の通信帯域（合計）が一定以内に収まるよう、帯域上限を設ける。

 - ・ OCIから外付けシステム連携用セグメントへの通信
- 帯域制御の上限値は、国保連合会にて設計した値を国保中央会にて設定する。

5. 外付けシステム接続申請シート

本章では、外付けシステムと標準システムおよび後期請求システム、特定健診システムを連携するために必要となる『外付けシステム接続申請シート』の申請内容および申請フローについて記載する。

5.1. 基本方針

外付けシステムと連携する上で、国保連合会と国保中央会の間で設計情報を取り交わす必要があり、設計情報を取り交わすための書類として『外付けシステム接続申請シート』を使用する。

国保連合会は『外付けシステム接続申請シート』に必要事項を記入し、国保中央会へ書類を提出すること。

『外付けシステム接続申請シート』に記入された設計情報を基に、国保中央会は外付けシステムと接続するために必要な設定を標準システムおよび他システムに対して行い、国保連合会は標準システムおよび他システムと接続するために必要な設定を外付けシステムに対して行う。

5.2. 申請内容

『外付けシステム接続申請シート』の申請内容を以下に示す。

(1) 国保総合システムおよび保険者接続に関する依頼

標準システムの運用管理端末、プリンタ、連合会クライアントの追加、変更、削除を実施する場合は『外付けシステム接続申請シート』の「Ⅰ. 国保総合システムおよび保険者接続詳細情報」に必要事項を記入して国保中央会に提出する。

なお、KDBシステム、情報集約システム、後期請求システム、特定健診システムにおける運用管理端末等の追加、変更、削除をする場合は各システムの申請方法に従う。

保険者向けネットワーク機器/保険者向けFWの初期構築や機器更改等で当該機器と国総保険者FW間の接続情報を更新する場合は『外付けシステム接続申請シート』の「Ⅰ. 国保総合システムおよび保険者接続詳細情報」に必要事項を記入して国保中央会に提出する。

(2) 外付けシステム（VCN）に関する依頼

外付けシステムのVCNを作成する場合は、『外付けシステム接続申請シート』の「Ⅱ. 外付けシステム（VCN）詳細情報」に必要事項を記入して国保中央会に提出する。

(3) 連合会独自 NW 機器に関する依頼

連合会独自NW機器と国総保険者FW間の初期構築や機器更改等で当該機器と国総保険者FW間の接続情報を更新する場合は『外付けシステム接続申請シート』の「Ⅲ. 連合会独自NW機器詳細情報」に必要事項を記入して国保中央会に提出する。

(4) 外付けシステム（通信要件）に関する依頼

国総保険者FWを経由する通信やOCI上に構築された外付けシステムと標準システムおよび他システム間の通信の追加、変更、削除をする場合は『外付けシステム接続申請シート』および、『別紙_外付けシステム接続申請用_通信要件一覧』に必要事項を記入して国保中央会に提出する。通信要件の作成においては「2.9 アクセス制限」、「3.9 アクセス制限」および『外付けシステム接続申請シート』の「IV. 外付けシステム（通信要件）詳細情報」をあらかじめ確認すること。なお、標準システムおよび他システムの標準通信設定については国保中央会にて設計・設定を行うため、『外付けシステム接続申請シート』の申請は不要とする。

外付けシステムと他システム間との通信要件にも対応するため、各通信要件に関係するシステムを明確にするよう『別紙_外付けシステム接続申請用_通信要件一覧』の様式見直しを行っている。旧様式の通信要件を新様式に転記した上で申請を行う。詳細は『別紙_外付けシステム接続申請用_通信要件一覧』を確認すること。

5.3. 申請フロー

『外付けシステム接続申請シート』の国保中央会への提出（申請）は、業務支援システムを利用する。申請フローを以下に示す。

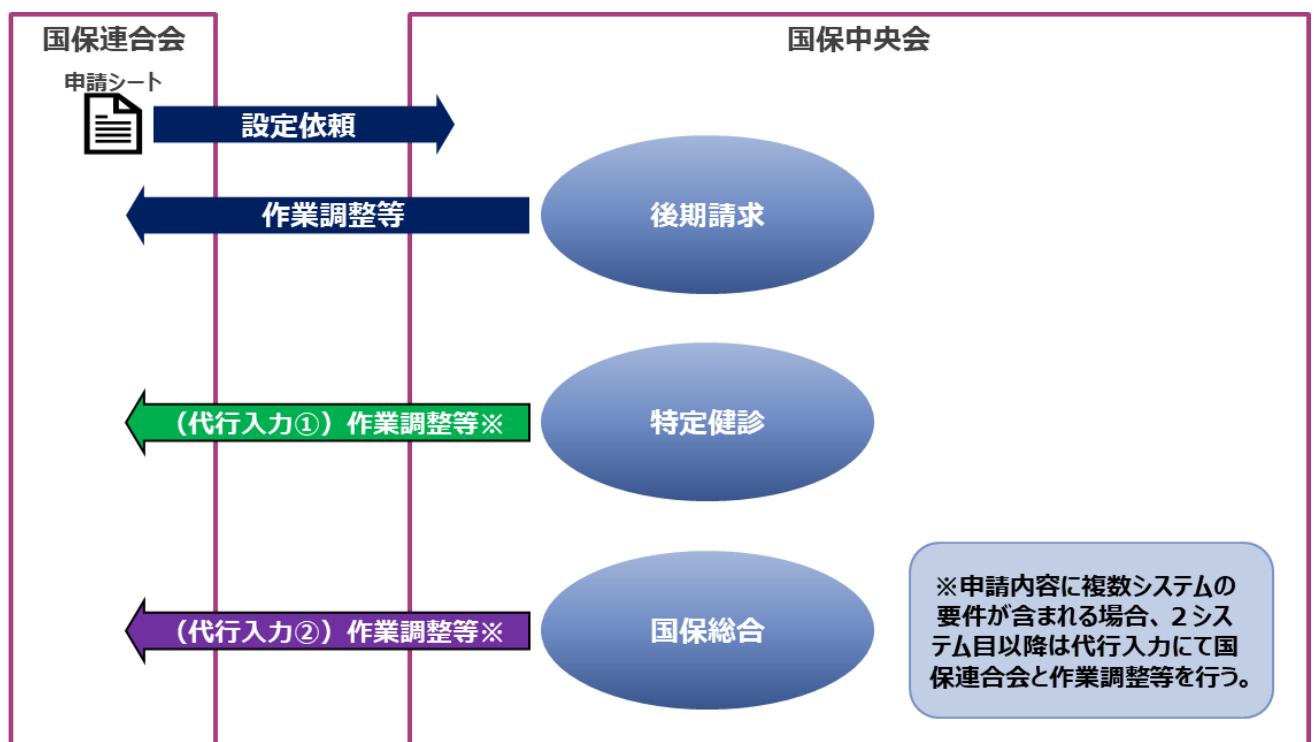


図 5. 3 - 1 外付けシステム接続申請シート申請フロー

業務支援システムにて申請を行う際は、以下の件名およびカテゴリにて申請を行う。

件名：外付けシステム接続申請シートの提出（依頼事項番号^{*1}）

カテゴリ1：システム基盤

カテゴリ2：外付け申請

カテゴリ3：外付け申請

5. 外付けシステム接続申請シート

(注) * 1 『外付けシステム接続申請シート』に記載の依頼事項の番号（Ⅰ/Ⅱ/Ⅲ/Ⅳ）を記載すること。