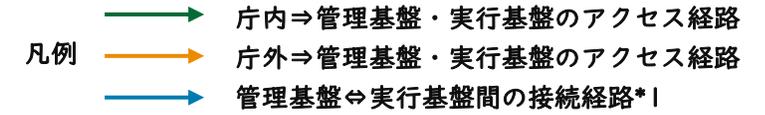


資料2の別紙3： 非機能要件 補助資料

1. 非機能要件：9.情報セキュリティに関する事項

1-1. 接続方式の全体像と要件の概要



パターンA：管理基盤が閉域接続可能の場合（IaaS構成）

パターンB：管理基盤が閉域接続不可の場合（iPaaS構成）



管理基盤への接続方式・要件	接続方式	① 閉域接続	② インターネット接続 (大阪府SCを経由しない)	③ インターネット接続 (大阪府SCを経由する)	④ インターネット接続 (大阪府SCを経由しない)
	方式のポイント	庁内から閉域アクセスができること	多要素認証を必須とし、 <u>事業者のグローバルIPで通信制御</u> ができること	多要素認証を必須とし、 <u>大阪府SCの出口IPで通信制御</u> ができること	②に同じ
	9-1 認証・認可	<ul style="list-style-type: none"> 認証基盤：ActiveDirectory、EntraIDに対応していること 認証：SSO、Basic、クライアント証明書に対応していること 認可：ロールベース管理に対応していること 	<ul style="list-style-type: none"> 認証：Basicに対応していること 多要素認証：必須（電話、SMS、Authenticatorのいずれか） 認可：ロールベース管理に対応していること 	<ul style="list-style-type: none"> ②に同じ 	<ul style="list-style-type: none"> ②に同じ
	9-2 アクセス制御	<ul style="list-style-type: none"> 権限設定：アクセスできる機能/データは権限設定に基づいて適切に管理すること アクセス制限：ユーザー単位・ユーザーグループ単位、またデータの項目単位の全部またはいずれかでアクセス制限ができること 	<ul style="list-style-type: none"> 権限設定：①に同じ アクセス制限：①に同じ 管理基盤にアクセスする事業者のグローバルIPで通信制御ができること 	<ul style="list-style-type: none"> 権限設定：①に同じ アクセス制限：①に同じ 大阪府SCの出口IPで通信制御ができること 	<ul style="list-style-type: none"> ②に同じ
	その他要件	<ul style="list-style-type: none"> その他のセキュリティ要件は非機能要件（9.情報セキュリティに関する事項）を参照すること 			
実行基盤への接続方式・要件	⑤ ①に同じ	⑥ ②に同じ	iPaaSの製品の仕様上、実行基盤へのアクセスは発生しない		

3 *1 管理基盤⇄実行基盤間の接続は受注者にて検討し、発注者と協議すること

2. 非機能要件：12. 運用保守に関する事項

2-1. 運用保守業務 補助説明対象

非機能要件に定める運用保守業務の中で、「アプリケーションの業務運用」と「インシデント管理・復旧対応」の業務プロセスを示し、役割と業務内容を明確化する

非機能要件（運用に関する事項/保守に関する事項）		運用保守業務内容概要	本資料該当箇所
システム維持	稼働状況報告	<ul style="list-style-type: none"> 稼働状況の監視・結果報告 システム稼働状況踏まえた改善提案 	-
	ジョブ運用	<ul style="list-style-type: none"> 定期又は臨時で実施するデータ一括処理における処理の実行及び実行状況の確認 	-
	バックアップ運用	<ul style="list-style-type: none"> バックアップの取得・管理 	-
	ログ運用	<ul style="list-style-type: none"> ログの管理・保管 	-
	セキュリティ運用	<ul style="list-style-type: none"> セキュリティ監査対応、アクセス管理、システム監査対応、システムの設定変更、大阪市セキュリティ基準の準拠状況の確認 	-
	アプリケーションの業務運用	<ul style="list-style-type: none"> 計画停止 情報資産管理 連携アプリケーションのデプロイ・リリースまでのサポート 	P.6-P.11
	業務運用支援	<ul style="list-style-type: none"> 運用ガイドラインの定義・更新 組織改正対応・人事異動等に伴うユーザー管理 	-
	変更管理	<ul style="list-style-type: none"> 変更要求管理 変更作業の実施 	-
システム監視運用	システム管理およびメール通知	<ul style="list-style-type: none"> 利用状況の監視及び記録 	-
障害時対応	インシデント管理・復旧対応	<ul style="list-style-type: none"> 障害時の一次対応（障害検知、障害内容確認、振分け） 復旧対応 再発防止対応 	P.12-13
問い合わせ回答・調査	問合せ対応	<ul style="list-style-type: none"> 利用者からの問い合わせ対応 	-
バージョンアップ対応	バージョンアップに伴う影響調査、改修/テスト	<ul style="list-style-type: none"> バージョンアップ計画の立案・実施 バージョンアップ対応 	-

2-2. アプリケーションの業務運用における業務一覧

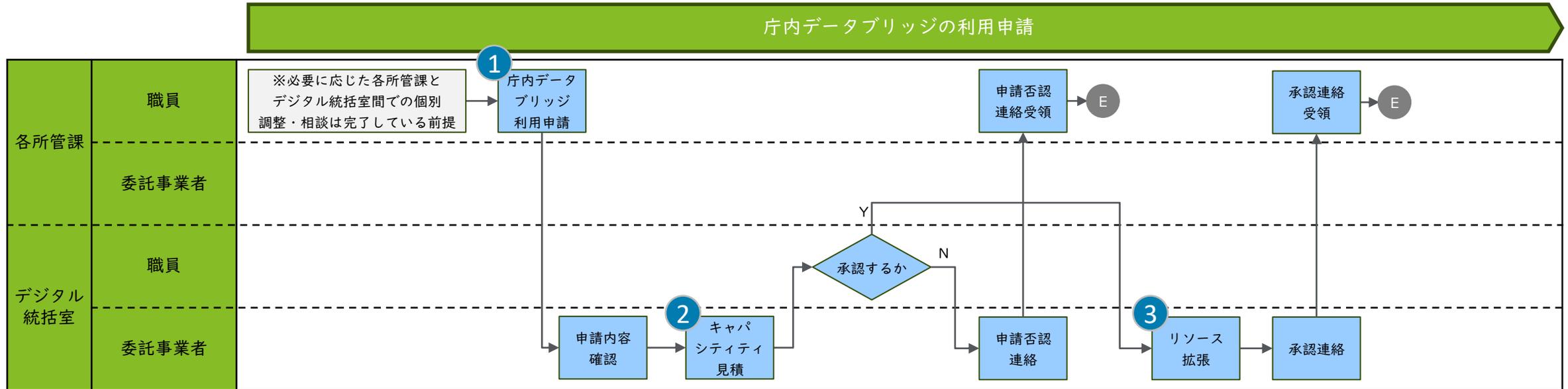
アプリケーションの業務運用のうち、庁内データブリッジを用いた連携アプリケーション開発を実施するための、利用申請～デプロイ対応までの業務プロセスを定義する

■ アプリケーションの業務運用における業務項目

#	業務	業務概要	該当頁	
1	連携アプリケーションのデプロイ・リリースまでのサポート	庁内データブリッジの利用申請対応	<ul style="list-style-type: none"> 連携アプリケーションを調達する各所管課（各所管課の委託事業者を含む）からの利用申請を受けて、必要なキャパシティの見積りを行い、利用申請時点の稼働状況から必要なキャパシティが確保できるか、拡張が必要かの検討を行う 連携アプリを構築するにあたって、専用ホストを準備するべきであるかも合わせて検討する 	P. 7
2		庁内データブリッジのアカウント発行	<ul style="list-style-type: none"> 連携アプリケーションを調達する各所管課（各所管課の委託事業者を含む）からの申請を受けて、アカウント発行を実施する 各アカウントのアクセス制御範囲の設定も含めて実施する 	P. 8
3		開発ガイドラインへの準拠状況の確認	<ul style="list-style-type: none"> 運用・保守設計にて作成した開発ガイドラインに沿って、連携アプリケーションの構築作業が実施されているかを確認する 申請内容に不備などがある場合は連携アプリケーションを調達する各所管課（各所管課の委託事業者を含む）へのヒアリングを実施する 	P. 9
4		連携アプリケーションデプロイ対応	<ul style="list-style-type: none"> 連携アプリケーションを調達する各所管課（各所管課の委託事業者を含む）からのデプロイ申請を受けて、デプロイ可否の確認及びデプロイ日程・デプロイ環境の調整を実施する 	P. 10、11
5	計画停止	<ul style="list-style-type: none"> 事前に計画したスケジュールに基づき、定められた手順で告知した上で、情報システムの停止・再起動を実施する 	-	
6	情報資産管理	<ul style="list-style-type: none"> 扱う資産（製品名、バージョン、ライセンス期間、アドイン、ライブラリ等）や、共通機能/設定（インフラ設定、共通機能の設定）を「資産管理台帳」にて管理する 	-	

#1：庁内データブリッジの利用申請対応の業務プロセス

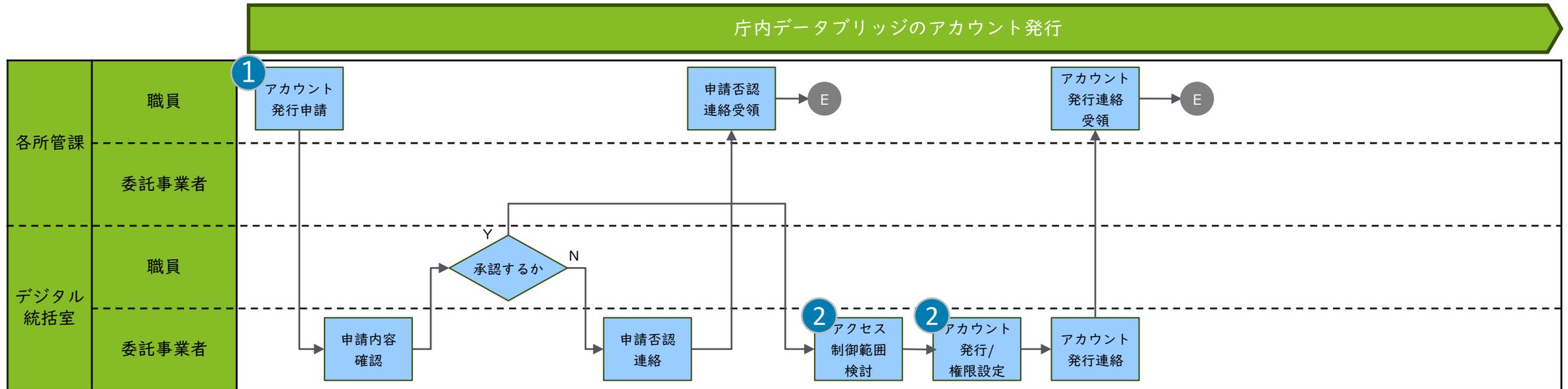
庁内データブリッジの利用申請時に、各所管から受領した要件（概算レベル）を基に必要なキャパシティを概算で見積もり、稼働状況から必要なキャパシティが確保できるかの検討及び必要なリソース拡張を行う。



#	ポイントとなる業務プロセス	業務プロセス上の留意事項
1	庁内データブリッジ利用申請	<ul style="list-style-type: none"> 本プロセス開始前に、各所管課とデジタル統括室間にて、セキュリティや実現時期等に係る調整・相談は完了している前提とする 庁内データブリッジ利用申請は、各所管課側で連携アプリケーションの構築/既存アプリケーションの利用が検討された段階でデジタル統括室に申請が来る 利用申請時に、現時点での想定要件（規模・性能要件）も受領する想定
2	キャパシティ見積	<ul style="list-style-type: none"> 庁内データブリッジ利用申請受領後、受領した要件を基に、現状の庁内データブリッジのリソースで充足可能かを見積もる
3	リソース拡張	<ul style="list-style-type: none"> リソースの拡張が必要と判断される場合には、リソースの拡張を行う なお、連携アプリケーションの開発・テスト完了後に当初の見積り以上に基盤の拡張が必要な場合は、業務整理（バッチの間隔調整、タイミングの調整など）による運用面での調整を検討し、それでも難しい場合は追加契約を検討する

#2：庁内データブリッジのアカウント発行の業務プロセス

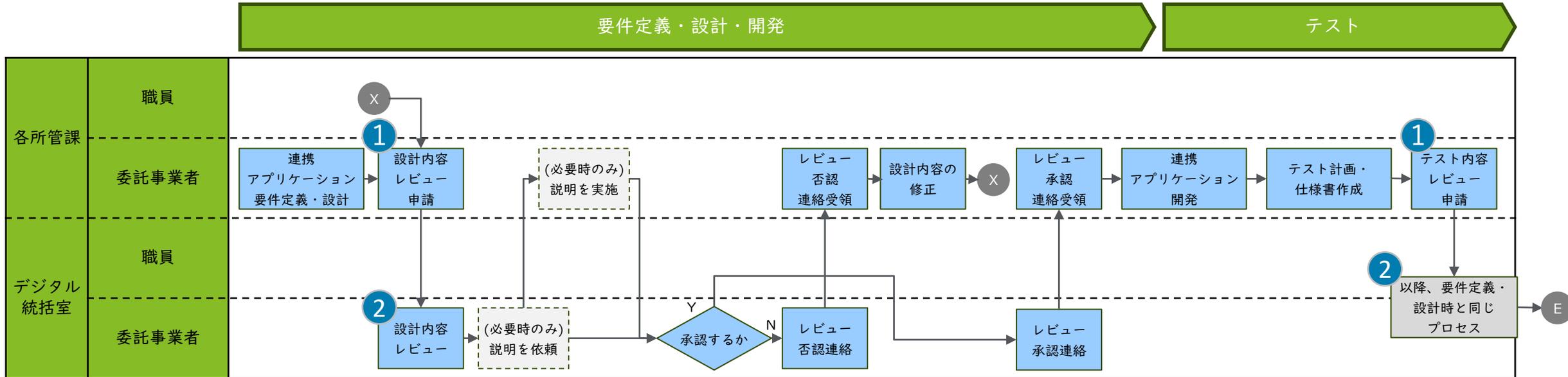
各所管課（職員/委託事業者）からの申請を受け取り、新規アカウントを発行する。
アカウント発行に際して、適切な権限設定を行う。



#	ポイントとなる業務プロセス	業務プロセス上の留意事項
1	アカウント発行申請	<ul style="list-style-type: none"> 庁内データブリッジの利用申請承認後、庁内データブリッジのアカウント発行申請を受領する 申請対象者名や利用期間、必要な権限など、後続のアカウント発行プロセスに必要な情報を受領すること
2	アクセス制御範囲検討・アカウント発行/権限設定	<ul style="list-style-type: none"> アカウント発行時の権限設定は、調達仕様書6章で定義している、環境・役割別に合わせた権限を設定すること 特に各所管課の委託事業者への権限は、その開発に必要なリソース（アプリケーション情報）のみアクセスできるよう、詳細な権限の設定ができること

#3：開発ガイドラインへの準拠状況の確認の業務プロセス

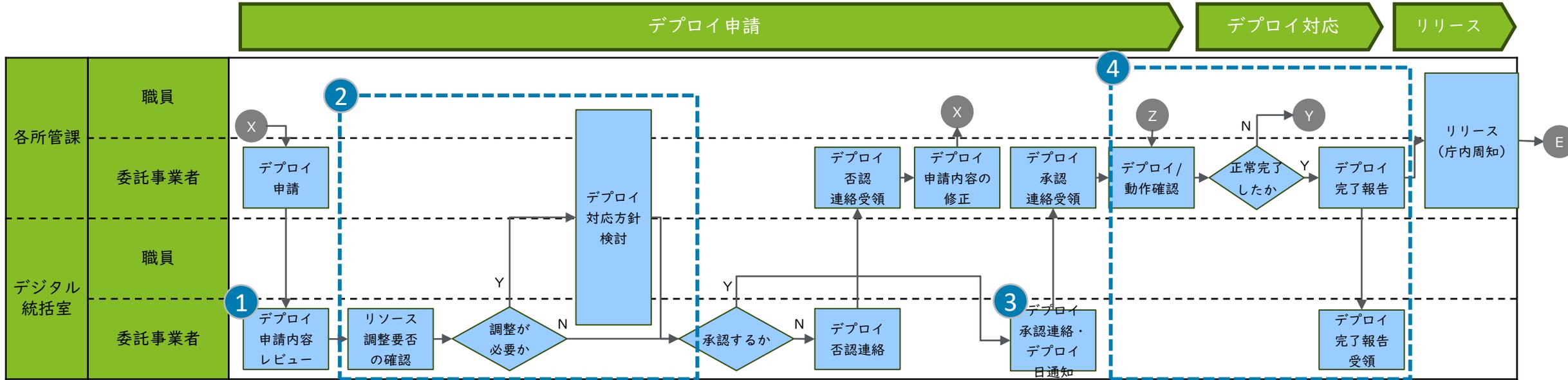
各所管課（職員/委託事業者）が連携アプリケーションを開発ガイドラインに準じて設計/構築しているかを確認する。
 なお、チェックリストを用いた所管課でのセルフレビューを基本とするが、必要に応じてヒアリングを実施する



#	ポイントとなる業務プロセス	業務プロセス上の留意事項
1	設計内容レビュー申請・テスト内容レビュー申請	<ul style="list-style-type: none"> 開発標準化のために、事前に定義・各所管に周知する開発ガイドラインに準拠した成果物になっているかの観点で、設計プロセス終了時及びテスト計画策定時に、標準準拠のレビューを行う 各所管課は、デジタル統括室側で事前に定義・各所管課に周知する標準準拠チェックリストを基にセルフレビューを行い、その結果を添付してレビュー申請を行う
2	設計内容レビュー・テスト内容レビュー	<ul style="list-style-type: none"> 各ポイントでの、デジタル統括室側での標準準拠のレビューは、各所管課のセルフレビュー結果が全て満たしているかの観点で確認・承認を行う 設計プロセス終了時における確認は、必要に応じて各所管課と設計内容の説明・確認を行う場を設ける

#4：連携アプリケーションデプロイ対応の業務プロセス（1/2）

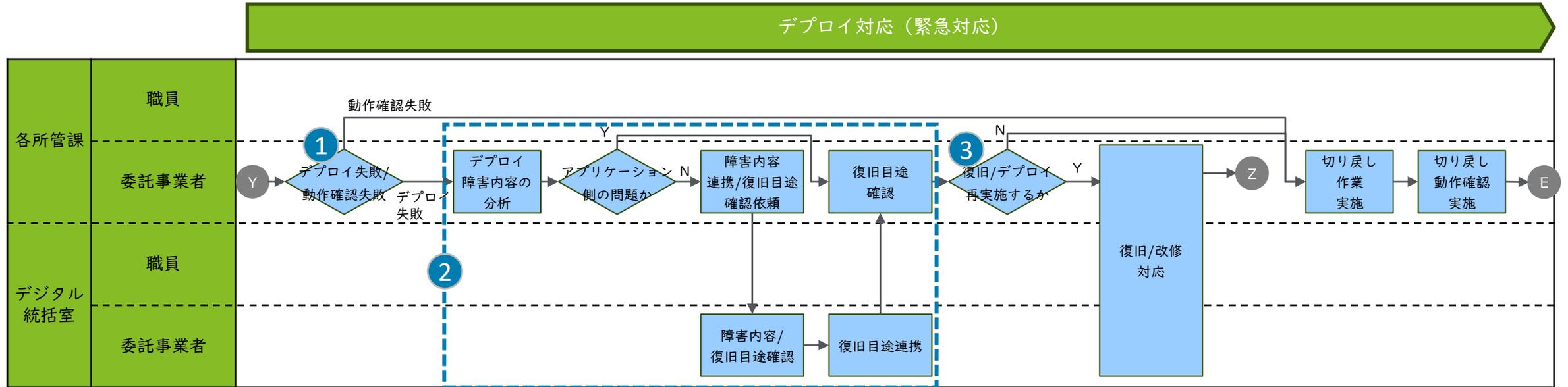
各所管課からのデプロイ申請を受けて、必要に応じて、庁内データブリッジのリソース調整とデプロイ日の調整を実施する



#	ポイントとなる業務プロセス	業務プロセス上の留意事項
1	デプロイ申請内容レビュー	<ul style="list-style-type: none"> 各所管課でのテスト終了/リリース判定後に、連携アプリケーションのデプロイの申請を行う デプロイ申請時には、テスト結果、最終的な規模・性能要件値、デプロイタイミング、デプロイ手順書等の情報を受領する デプロイ作業は各所管課側で実施するため、ガバナンスの観点でデプロイ手順書のひな型・手順に含めるべき作業・観点はデジタル統括室側で定義・周知しておく
2	リソース調整	<ul style="list-style-type: none"> デプロイ申請時に受領した規模・性能値を基に、再度庁内データブリッジのキャパシティの調整を行う キャパシティの拡張が難しい場合は、アプリケーションの実行タイミングや頻度を減らすなどの対応や、デプロイ時期の延伸等の調整を各所管課と行う
3	デプロイ日通知	<ul style="list-style-type: none"> リソース調整の結果を基に、デプロイ日を調整し、各所管課側に連携する
4	デプロイ/動作確認	<ul style="list-style-type: none"> デプロイ/動作確認作業は各所管課にて実施するが、基盤側に起因する問い合わせに対応できるようにしておく

#4：連携アプリケーションデプロイ対応の業務プロセス（2/2）

デプロイ/動作確認時に障害が発生した場合は、各所管課にて障害内容の切り分けを行い、責任分界に応じて庁内データブリッジの復旧/改修を実施する



#	ポイントとなる業務プロセス	業務プロセス上の留意事項
1	デプロイ失敗/動作確認失敗時の対応	<ul style="list-style-type: none"> デプロイ失敗時には失敗の原因を分析、再デプロイ可否を検討するが、動作確認失敗時は、連携アプリケーションの処理ロジックや内容に不備がある可能性（改修・テストの再実施も必要）があるため、デプロイ作業は継続せず切り戻しを行い作業を中止する
2	デプロイ失敗時の障害内容分析	<ul style="list-style-type: none"> デプロイ作業/動作確認中に障害が発生した場合は、各所管課にて原因の切り分けを行う 基盤側に原因がある場合は、各所管課よりデジタル統括室に復旧目途確認依頼を受領する デジタル統括室側で、原因分析し、復旧目途を各所管課に連携する
3	デプロイ失敗時の復旧/改修対応	<ul style="list-style-type: none"> 各所管課側で、障害内容及び復旧目途を確認後、本デプロイ作業内で復旧・改修を行うかを検討する 復旧/改修を行うかの判断基準（目安となる時間や、復旧対象となる障害の基準（基盤側のキャパシティ不足等））は、ガバナンスの観点で標準ルールをデジタル統括室側で定義・周知しておく 復旧/改修を実施する場合は、必要に応じてデジタル統括室側で作業を行い、復旧/改修後に再度デプロイ・動作確認を行う

2-3. インシデント管理・復旧対応で定義する業務項目

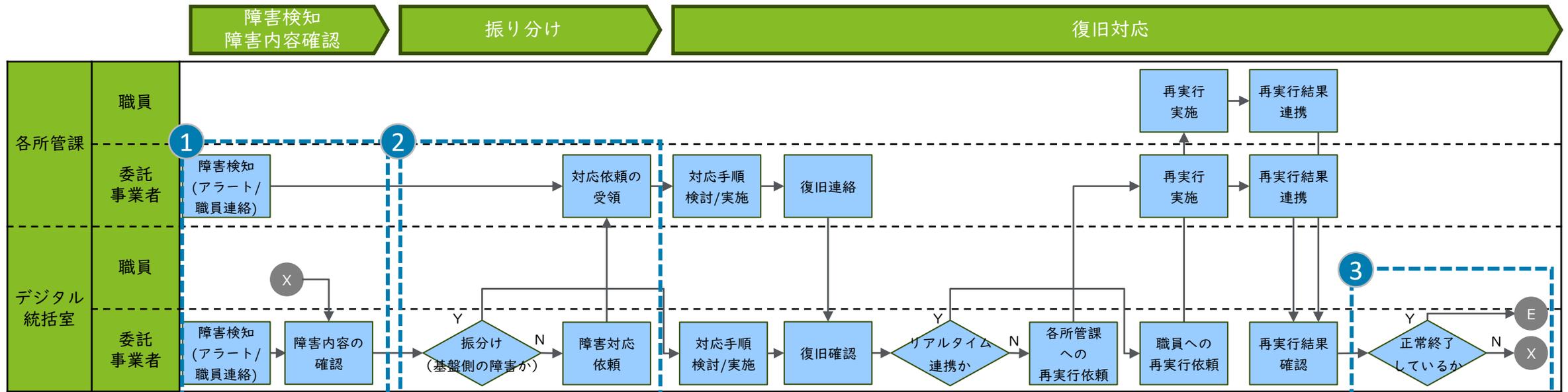
インシデント管理・復旧対応のうち、障害の検知から復旧対応までの業務プロセスを定義する

■ インシデント管理・復旧対応における業務項目

#	業務		業務概要	該当頁
1	障害時の一次対応 (障害検知、障害内容確認、振り分け)	障害検知・障害内容確認	<ul style="list-style-type: none"> 障害発生を検知し、障害内容を確認する 	P.13
2		振り分け	<ul style="list-style-type: none"> 障害の内容に応じて、障害対応の実施主体を定め、対応依頼を行う 	
3	復旧対応	復旧対応	<ul style="list-style-type: none"> 対応方針を検討し、復旧対応を実施する 障害の影響度に応じて、他委託事業者や大阪市に対して対応方針を伝達し合意する 	
4	再発防止対応		<ul style="list-style-type: none"> 障害の再発防止に向けた対応方針を検討し、対応策を実行する 	-

#1-#3：障害時の一次対応（障害検知、障害内容確認、振り分け）、復旧対応の業務プロセス

障害発生時の一次対応として、障害検知・障害内容確認、振り分けを実施する。
一次対応の結果を受けて、対応主体を決定して復旧対応を行う



#	ポイントとなる業務プロセス	業務プロセス上の留意事項
1	障害検知	<ul style="list-style-type: none"> 連携アプリケーション側の障害も含め、障害検知の一次受けはデジタル統括室側で受ける ただし、早急な復旧対応ができるよう、連携アプリケーション側で設定しているアラートは各所管課側でも受け取る
2	対応主体の振り分け	<ul style="list-style-type: none"> 障害時のログを基に障害内容を分析し、復旧対応主体に振り分けを実施する (データブリッジの保守運用担当、連携アプリケーションの保守運用担当、連携アプリケーションを利用するシステムの保守運用担当など、複数の所管課が並行して障害内容を確認すると、アラインが困難になるため)
3	復旧処理結果の確認	<ul style="list-style-type: none"> 復旧後に各所管課に連携処理の再実行を実施頂いた後、正常に処理が完了しているかをデジタル統括室側でログを基に判断する