仕　様　書

国立研究開発法人新エネルギー・産業技術総合開発機構

目次

1. 件名

プロジェクトマネジメントシステム及び連携システムの基盤更改に係る全体アーキテクチャ設計・移行業務

2. 背景及び目的

発注者が基幹システムとして利用しているプロジェクトマネジメントシステムを始めとする連携システムは、これまで仮想化基盤及び物理サーバ上で稼働させているが、ハードウェアの老朽化に伴いこれらのシステムの基盤更改を行う必要がある。

更改にあたり、政府としての全体方針である「デジタル社会の実現に向けた重点計画（令和3年12月24 日閣議決定)」であるクラウド・バイ・デフォルト原則に基づき、移行先の基盤にクラウドサービスを採用し、移行を行う予定である。

本業務は、クラウド基盤への移行において全体アーキテクチャ設計、構築及び移行業務を調達することを目的とする。

3. 用語の定義

本仕様書で使用する用語の定義を「別添1　用語の定義一覧」に示す。

4. 業務・情報システムの概要

移行対象となるプロジェクトマネジメント及び連携システムは「8.(1)③情報システムの概要」に示す。現在の仮想化基盤及び物理サーバ上での構成は「別添2　現在の構成」のとおりである。

5. 履行期限

2024年3月29日（金）

6. 業務の概要

(1) 環境構築に関する要件
(2) 移行作業等に関する要件

7. 作業スケジュール

本業務の作業スケジュールを「図1　作業スケジュール」に示す。詳細なスケジュールについては、発注者と調整のうえ決定すること。

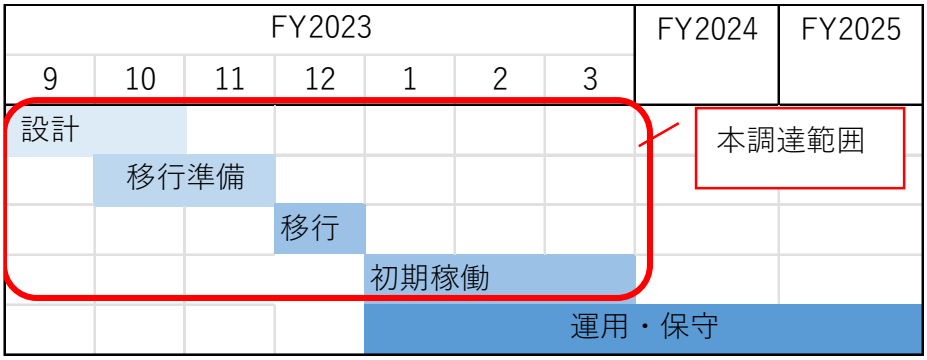


図 1　作業スケジュール

8.　業務の詳細

(1)　環境構築に関する要件

受注者は、現在オンプレミスで稼働している発注者が保有する以下のシステムの移行先となるクラウド基盤の設計、構築及び一部システムの移行を行うこと。システムの移行に際しては、発注者と調整し、システムの運用保守業者と協力して行うこと。

①　システム構成概要図

発注者の現在のシステム稼働環境については、「別添 3　NEDO システム構成図」、「別添 4 NEDO ネットワーク論理構成図」及び「別添5　仮想化基盤_ハードウェア構成図」に示す。また、今回移行対象となるシステムはすべて「別添 3　NEDO システム構成図」に記載のデータセンター1（磯子）に配置している。

②　移行方針

システムの移行は、できる限りアーキテクチャを変更しない迅速なクラウドリフトの実施、リソースの集約や BYOL 及びサブスクリプションの活用によるコストの最適化を目的とし、以下の移行方針に基づいて検討すること。なお、移行先のクラウド基盤は Oracle Cloud Infrastructure（OCI）を採用する予定である。

1)　今回の移行作業は、限られた期間での実施を最優先とするため、既存のシステムをそのまま移行することを前提とする。そのため、現在利用しているソフトウェア等については原則変更しないこととする。ただし、クラウドサービスで利用できないソフトウェアについては、発注者と協議のうえ変更可能とする。

2)　既存のシステムは、データベース及び運用監視サーバは物理サーバ、それ以外は仮想環境で稼働している。物理サーバで稼働しているものについては、適切なクラウドサービスへ、仮想環境で稼働しているものについては、ネットワーク構成も含めてそのまま移行することができる Oracle Cloud VMWare Solution （OCVS）を利用することとする。

3)　構成最適化の観点から、OCVS は 3 ノード・1 クラスタ構成とする。

4)　現在物理サーバで稼働しているデータベースは、Oracle Database Standard Edition 2 を Real Application Clusters (RAC)を利用した高可用性構成で利用しており、クラウド移行後も同等以上の可用性を維持する必要がある。また、これまで Oracle Database のバックアップ取得

や障害対応、チューニング等の運用管理に工数とコストがかかる等の課題があり、その解決も求めている。これらの観点から、既存の可用性レベルを維持することができ、かつ、運用管理を自動化した機能として有する Oracle Autonomous Database (ADB)を利用すること。

5) 現在仮想化統合環境でも Oracle Database Standard Edition 2 を利用しているが、こちらは事前にオンプレミス環境で Windows Server2019、Oracle19c へアップグレードを行ったうえで OCVS への単純移行を行う。バージョンアップ作業については本業務の範囲外とする。

6) 運用管理サーバ及び NTP サーバについては、OCVS とは別に IaaS の仮想サーバ（Compute VM　Instance）を利用すること。

7) クラウドサービス側でマネージドサービスが提供されている各種サービス（E-Mail 送信、内部 DNS 等）については、極力置き換えて利用すること。

③　情報システムの概要

移行対象システムを以下に示す。

1) プロジェクトマネジメントシステム

発注者が行う委託等事業において事業者と発注者の間で実施される契約管理等を行うシステム。

プロジェクトマネジメントシステムのアプリケーションサーバは仮想環境（VMWare）上で、データベースサーバは物理サーバで稼働している。「②移行方針」のとおり、アプリケーションサーバは OCVS へ、物理サーバは ADB へ移行を行うこと。また、運用管理サーバ等については、OCI 上の IaaS 等、適切なサービスを利用すること。

なお、プロジェクトマネジメントシステムの Oracle Database は、事業者用、NEDO 用にデータベース・インスタンスを分けているが、移行にあたりこれらのデータベースは統合する予定である。本業務では統合後の移行先となるデータベースを準備すること。

2) 会計系システム

発注者が行う委託等事業を含め管理費等すべての会計に関する業務及び連携システムの SSO を行う統合認証システムを保有するシステム。

会計系システムは、仮想環境（VMWare）で稼働しており、クラウド基盤への移行は OCVS を利用すること。

3) 統合認証システム

会計系システムの一部として会計系システムの運用保守事業者が管理を行っているシステム。

統合認証システムは、仮想環境（VMWare）で稼働しており、クラウド基盤への移行は OCVS を利用すること。

4) 委員会システム

発注者が主催する委員会の情報及び委員の登録、管理を行うシステム。

委員会システムは、仮想環境（VMWare）で稼働しており、クラウド基盤への移行は OCVS を利用すること。

5) 資産管理システム

発注者及び委託等事業で取得した資産を登録、管理するシステム。

資産管理システムは、仮想環境（VMWare）で稼働しており、クラウド基盤への移行は OCVS を利用すること。

6)　文書管理システム

発注者が保有する法人文書及び特定法人文書の保管、決裁等を行うシステム。

文書管理システムは、仮想環境（Hyper-V）で稼働しており、クラウド基盤への移行は OCVS を利用すること。なお、事前にオンプレミス環境の VMWare 上に移行した後にクラウド基盤へ移行するか、クラウド基盤へ移行時に Hyper-V から VMWare へ変換するかについては現在検討中であり、変換作業は本業務の対象外とするが、発注者からの相談に応じて必要な支援は行うこと。

7)　ＡＳＰシステム

マイクロソフト社の Active Server Pages（ASP）を使用して作成された複数のシステムの総称。相手先登録依頼、相手先口座登録依頼、会議議題登録等のシステムがある。クラウド基盤移行前には他の基盤への移行を検討しているが、移行ができない場合には本業務の対象とする。

ＡＳＰシステムは、仮想環境（VMWare）で稼働しており、クラウド基盤への移行は OCVS を利用すること。

④　システム方式に関する要件

1)　規模に関する事項

本システムの利用者は、発注者の職員及び委託等事業者である。

発注者の職員数：1,500 名

委託先等事業者登録 ID 数：12,000ID

2)　性能に関する事項

レスポンス等は、現在と同等以上とし、現行の性能よりも劣化しないこと。なお、システムに関与したレスポンス低下の場合は、解決のための支援を行うこと。

3)　ネットワークに関する事項

OCI のデータセンターに対して、発注者の情報基盤サービスから冗長化した専用回線を新規敷設すること。また、現在利用しているデータセンター（磯子）から移行用のネットワーク回線を敷設し、移行終了後に撤去すること。移行用の回線についてはシングル構成とし、帯域はそれぞれ 1Gbps とする。

受注者は、発注者が別途調達する専用線ネットワークのベンダーと協力し、専用線を介した接続の実現に向け、クラウド環境側の構築・設定を行うこと。

4)　可用性に関する事項

(a) すべてのシステムの Web サーバ及びデータベースは、サービスレベルとして 99.9%以上の可用性を確保すること。本番 Web サーバ及びデータベースは 24 時間 365 日稼働を原則とするが、システムメンテナンス等で計画停止する場合は、事前に発注者へ連絡のうえ、原則として発注者のシステム利用時間外に作業を行う事。システム利用時間は、8 時から翌 4 時となる。なおシステム利用時間に関して短縮は可能であるが、発注者の業務時間は 8 時から 18 時 45 分のため留意する事。

(b) システムのバックアップを取得し、RTO として 12 時間を満たすこと、また、RPO として前日のシステム利用終了時のデータに復旧できること。

(c) 移行時は、災害対策環境としてバックアップデータの保管のみを行うが、OCVS 上に構築したシステムの見直しを行う際に、改めて災害対策について検討すること。

5)　バックアップに関する事項

クラウド移行時のバックアップ手法は以下のとおり。

(a) Compute VM Instance で稼働させるサーバ（運用管理、NTP 等）については、クラウドサービスの標準機能を利用してバックアップを取得すること。Object Storage へ保管したバックアップは、クロスリージョンコピーにより大阪の Object Storage へ遠隔地保管を実施すること。

(b) ADB については、自動で取得されるバックアップ機能を利用すること。

(c) OCVS 上の仮想サーバについては下記のクラウド機能を利用すること。

- SDDC に Block Volume を追加でアサインして仮想マシンクローン先を Block Volume とし、ブロックボリュームバックアップを利用し、バックアップを Object Storage へ保管することを想定する。
- Object Storage へ保管したバックアップは、クロスリージョンコピーにより大阪の Object Storage へ遠隔地保管を実施することとする。

なお、手動で取得したバックアップは災害時を考慮し、Object Storage のレプリケーション機能を利用して遠隔地（関西）のクラウド・データセンターに転送し、管理すること。

6)　クラウドサービス提供各種機能に関する事項

クラウド化にあたり、クラウドサービス側で提供されている機能については、極力置き換えて利用すること。OCI の利用においては、「表 1　機能一覧」に示す機能の利用を想定している。

表 1　機能一覧

項番	現在の機能	OCI で検討している機能	補足事項
1	内部 DNS	プライベート DNS	
2	メール送信	Email Delivery	
3	内部用証明書認証	Certificates 及び Key Vault	
4	インターネット接続	Internet Gateway	
5	NTP サーバ	Compute Instance（Oracle Linux）	
6	プロキシサーバ	Internet Gateway 又は Network Firewall の機能で代替	これまでは内から外へインターネット接続をするために利用していたものであり、キャッシュ機能は不要であるため

7)　運用監視に関する事項

現在のシステムでは運用監視ツールとして Hinemos を利用している。移行後の運用監視は、OCVS を利用する仮想環境については原則として環境の変更をしない方針に基づき、運用監視ツールは Hinemos を継続利用すること。Hinemos は障害ポイント分離の観点から OCVS 上ではなく、クラウドサービスの仮想サーバ（Compute Instance）上に配置すること。

また、ハードウェアやネットワーク等のクラウドサービスの機能を利用する予定のコンポーネントについては、クラウドサービスを利用した監視を行うことを想定している。

表２　検討している機能一覧

項番	目的	OCI で検討している機能
1	クラウドサービスのメトリック収集	Monitoring
2	ログの収集	Logging
3	ログの横断的な分析	Logging Analytics
4	イベントベースでの通知	Events
5	イベント及び閾値ベースでの通知	Notifications

また、現在の運用監視における課題を以下に示す。これらについては、本業務の範囲外だが参考情報として記載する。

- サーバのリソース情報が 1 時間単位のため、障害ポイントでのリソース状況が把握できない。
- アプリケーションのエラーが多発しても検知が出来ず、原因不明となるケースが発生している。
- データベースのログが収集できないため、障害時の問題特定に時間を要する。

これらの課題については、クラウドサービス移行完了後に、「表 2　検討している機能一覧」のとおり提供機能の利用を検討するが、本業務の範囲外とする。

8)　セキュリティに関する事項

現行のセキュリティ対策と同様のものを実装し、さらにクラウドサービス利用におけるセキュリティ対策を強化するため、「表 3　セキュリティ機能一覧」のとおり提供機能の利用を検討すること。なお、現行と同等のセキュリティを満たせない場合は、機能の実装を検討すること。

＜現行のセキュリティ対策＞

- 事業者向け（外部）サイトの web アプリケーション診断
- NISC による定期的なシステム監査
- 既存データセンターのサービスによる FW、IPS、WAF（TrendMicro　Deep Security）の実装及び監視
- 以下のシステムにてそれぞれユーザ認証機能を実装
  - 事業者向けの外部サイト：二段階認証を実施
  - その他の業務システム：HPE　Icewall による各システムでの SSO
- 運用管理サーバ（Hinemos）でのセキュリティログの一元管理
- アンチウイルスソフトの導入

表３　セキュリティ機能一覧

項番	目的	OCI で検討している機能
1	潜在するセキュリティリスクを可視化し、情報漏洩等に繋がるセキュリティインシデントを抑止	Cloud Guard
2	効率的なセキュリティリスク管理にて、運用・管理におけるワークロードの最適化	Threat Intelligence
3	社内外からの不正なネットワークトラフィックを検知・防御し、脆弱性の悪用や情報漏えい等のセキュリティリ	Network Firewall

	スクを抑止	
4	Web アプリケーションに特化した攻撃を検知・防御し、Web アプリケーションを攻撃から防御	Web Application Firewall
5	ユーザの権限管理やンソールへのアクセス制御及び二要素認証等による認証強化にて不正ログインを防止	Identity and Access Management
6	セキュリティ関連のログ等を集約し、分析・通知等を基にインシデントへ対応	Logging Analytics

受注者は、これらのクラウドサービスの設定を行うこと。なお、クラウドサービスを使用した監視や運用については発注者が別途調達とするが、監視や運用の方法を決定するうえでの支援を行うこと。

⑵ 作業の実施内容に関する事項

受注者は本仕様書に記載された作業内容や各要件を参照のうえ必要な作業を実施すること。納入成果物、作業結果等は適宜発注者の了承を受けたうえで各工程、各作業を完了させること。また、各種ドキュメントの記述は第三者が容易に理解できるように留意すること。

① プロジェクト管理に係る作業

受注者は、「(1)環境構築に関する要件」に記載の内容を確認し、本業務を進めるためのプロジェクト管理を行うこと。

1) プロジェクト計画書の作成

受注者は、本業務に係るプロジェクトの目的・概要、体制、マススケジュール、WBS、工程ごとの成果物、開始終了基準、構築方針（設計、構築、テスト等)、プロジェクト管理方法等を記載したプロジェクト計画書を作成し、発注者の了承を得ること。プロジェクト計画書は、必要な修正等を行った場合は、発注者の了承を得ること。

2) 進捗管理

受注者は、各タスクの状況把握及びスケジュール管理を実施するため、以下の進捗管理を実施すること。

- WBS により作業工程ごとに必要な納入成果物、作業タスクを明確にすること。
- 業務の進捗状況を管理する進捗管理表及び各作業タスクの進捗状況等を定量的に分析した報告書を定期的（週 1 回の頻度）に作成及び提出し、発注者の了承を得ること。
- 計画から遅れが生じた場合は、原因を調査し、遅れを取り戻すための改善策を提示すること。

3) 課題管理

プロジェクト遂行にあたり発生した各種課題を管理するため、以下の課題管理を実施すること。

- 課題の内容、発生日、優先度、解決予定日、担当者、対応状況、対応策、対応結果及び解決日等の情報を一元管理した課題管理表を作成すること。
- 定期的（週 1 回の頻度）に対応状況を確認及び報告し、課題の経過状況を発注者と共有し、迅速な解決に取り組むこと。

4) リスク管理

プロジェクトの円滑な進行を阻害する内外のリスクを特定し、対応策の検討及び実施状況等を

管理するため、リスク管理表を作成し、以下の要件を満たすリスク管理を実施すること。

- プロジェクトの遂行に影響を与えるリスクを特定し、その発生要因、発生可能性、影響度及びリスク軽減策を整理すること。
- 定期的にリスク監視及び評価を行い、その結果を発注者と共有することでリスクによる影響の把握に努めること。
- リスクの発生に備え、緊急対応時の体制及び計画を整備すること。

5) 品質管理

改修及び機能追加するシステム及び設計書等の納入物の品質を保証するため、以下の要件を満たす品質管理を実施すること。

- 作業工程ごと納入成果物ごとに品質評価基準等を設定し、評価結果を発注者に報告すること。
- 検証、品質改善策の検討及び実施を管理する体制を構築すると共に、品質改善のための各種取組が、事前に決められた手続きに則って実施されていることを的確に確認・報告すること。

6) 変更管理

設計書、移行実施手順書等の納入物の構成及び変更履歴を管理するため、以下の要件を満たす構成及び変更管理を実施すること。

- 各種設計書、手順書等、変更の履歴を管理する構成管理対象を特定し、適切に管理すること。
- 変更履歴を管理するだけでなく、移行スクリプト等の構成管理対象は、プログラム変更によるデグレード（ソフトウェアのバージョンアップに伴う品質低下）対策のため、最新版や特定時点の版（不具合発生前の版等）を、いつでも提供できる仕組みを確立すること。

7) コミュニケーション管理

プロジェクトに関するすべての参画者が円滑かつ効率的なコミュニケーションを可能とするため、以下の要件を満たすコミュニケーション管理を実施すること。

- 作業工程ごとにおける各種作業に関する打ち合わせ、納入物等のレビューのほか、進捗・課題等に関する報告のため定期的に会議及び報告会（以下「会議等」という。）を開催すること。開催方式は、対面、オンライン（MS Teams）又はハイブリッドのいずれかの方式で行うこと。対面で実施する際の会議室手配等の付帯する費用は受注者が負担すること。なお、発注者の会議室を利用することも可能であり、その場合は事前に希望を発注者へ申し出ること。
- 会議等については、会議等の内容、対象者及び開催頻度等を明確にすること。会議等の開催頻度等は、各作業工程の状況等を鑑みて、発注者と協議のうえ必要に応じて変更すること。
- 会議等の開催後発注者の 5 営業日以内に受注者にて議事録を作成し、発注者の了承を得ること。なお、課題事項や宿題事項については議事録の提出に先行し、会議等終了後ただちに共有すること。

8)　セキュリティ管理

各作業工程におけるセキュリティに関する事故及び発生を未然に防ぐため、受注者の品質管理部門等の第三者又は外部機関によるセキュリティ監査が実施される場合、セキュリティ監査に協力すること。また、監査結果に対する改善や対策の実施状況について、発注者に報告すること。

9)　プロジェクト管理者の資格要件

プロジェクト管理者とは、プロジェクトすべての運営管理に関する責任を持つ者である。プロジェクト管理者に求める要件は以下のとおり。

- 情報処理技術者試験のプロジェクトマネージャー又は PMI（米国プロジェクトマネジメント協会）が認定する PMP（Project Management Professional）の資格又はこれと同等の能力があること。

②　設計・構築に係る作業

受注者は、「8.(1)環境構築に関する要件」を確認し、発注者が別途調達するクラウドサービス上にシステムを移行するための基盤設計及び構築を行うこと。

1)　クラウド基盤設計

受注者は、「8.(1)環境構築に関する要件」を確認のうえ要件を満たすために必要なクラウド構成を検討し、基本設計及び詳細設計を行い、発注者の了承を得ること。また、必要に応じて、当該要件の改定を行うこと。なお、設計に際しては、政府の設計・開発ガイドライン等に準拠して実施すること。

- 受注者は、プロジェクト計画書に基づき、設計工程の実施状況を発注者に報告すること。
- 受注者は、プロジェクト実施体制表を発注者に提出し、この体制に基づいてプロジェクトを進めること。
- 受注者は、クラウド基盤基本設計書及びクラウド基盤詳細設計書を作成し、発注者の了承を得ること。
- 定常時及び障害発生時において想定される運用を想定のうえ運用実施手順案を作成し、発注者の了承を得ること。運用実施手順案には、安定稼働のための監視やシステムの起動停止、ログ管理、障害時の情報収集と復旧手順等を含めること。

2)　構築

受注者は、基本設計及び詳細設計に基づき、必要な環境を構築すること。基盤構築の実施にあたり、環境を構築するための手順等を記載したクラウド基盤構築手順書を作成し、システム環境構築結果を発注者に報告すること。

構築するサーバは「8.(1)環境構築に関する要件」の「③情報システムの概要」のシステム及び「④システム方式に関する要件」のバックアップ、運用監視に必要な各クラウドサービスとする。

3)　クラウド基盤テスト

受注者は構築した基盤が要件を満たすか、障害時に想定どおりの動作となるかについてテストを行うこと。

- クラウド基盤テストの実施にあたり、目的、範囲、テスト方針、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ作成基準、品質管理基準及び合

否判定基準等を記載したクラウド基盤テスト実施計画書を作成し、発注者の了承を得ること。

- クラウド基盤テスト実施計画書に基づき、各テストを実施し、テスト結果の実績、残課題、品質評価結果及び次工程開始の見通し等をまとめたクラウド基盤テスト結果報告書を作成し、発注者の了承を得ること。
- テストの項目としては、障害テストとしてバックアップからの復元や、冗長構成になっている機器について、縮退運転時の動作確認も実施すること。
- システムテストに必要な機器、テストツール等の準備については、受託者が用意すること。
- テスト実施時に使用したアクセス権限等は、本番稼働前までに完全に消去すること。
- 受注者は、設計、構築、テストで担当変更を行う場合は、設計担当者によるテスト項目レビューを必須とすること。

③　アプリケーション移行に係る作業

受注者は、「(1)環境構築に関する要件」に記載の要件を確認し、構築したクラウド基盤にシステムを移行する支援を行うこと。

1)　イメージ移行できるシステム

OCVS に移行するサーバについては、システム運用保守事業者及び既存のインフラ提供業者と協力し、受注者がイメージを移行すること。また、移行にあたっては事前にソフトウェアのバージョンアップと検証等を行うこととするが、事前のバージョンアップ作業等は発注者が別途調達で実施するため、本業務ではバージョンアップ済みの環境を移行対象とすること。

- 受注者は、システムの移行方式、移行ツール、移行スケジュール及び移行テスト（移行手順、移行後の動作確認等）の計画を行い、移行実施計画書、移行実施手順書を作成し、発注者の了承を得ること。
- 移行実施計画書には、移行時の障害発生等による切り戻し作業等、緊急時や不測の事態が発生した場合の対応策を含めること。

2)　イメージ移行できないシステム

Compute 上に構築するサーバ及びデータベースについては、受注者が基盤の構築と設計を行い、システム運用保守事業者が移行を行うこと。受注者は発注者の指示のもと、必要に応じてシステム運用保守事業者を支援すること。

- Compute 環境については、環境を構築し、OS の初期設定までを行った状態で、システム運用保守事業者に引き渡すこと。OS の初期設定にあたっては発注者の指示のもとシステム運用保守事業者にヒアリングを行うこと。
- データベースはサービスを起動し、初期設定を行った状態でシステム運用保守事業者に引き渡すこと。初期設定にあたっては発注者の指示のもと、システム運用保守事業者にヒアリングを行うこと。
- データ及びシステムの移行は本業務には含まないこと。

3)　受入テスト支援

受注者は、発注者からの依頼に応じて業務要件を満たしているか確認するための受入テストの

支援を実施すること。

9. 納入成果物等

(1) 納入成果物

納入成果物、記載場所及び納入期限を「表 4　納入成果物一覧」に示す。

表 4　納入成果物一覧

項番	納入成果物	記載箇所	納入期限
1	プロジェクト計画書	8.(2)①1)	契約締結から 5 日以内
2	クラウド基盤基本計画書	8.(2)②1)	構築開始まで
3	クラウド基盤詳細設計書	8.(2)②1)	構築開始まで
4	クラウド基盤構築手順書	8.(2)②2)	構築開始まで
5	クラウド基盤テスト実施計画書	8.(2)②3)	テスト実施まで
6	クラウド基盤テスト結果報告書	8.(2)②3)	テスト終了後 5 日以内
7	移行実施計画書	8(2)③1)	移行実施まで
8	移行実施手順書	8(2)③1)	移行実施まで
9	運用実施手順案	8.(2)②1)	移行実施まで
１０	議事録	8.(2)①7)	会議等終了から 5 日以内

(2) 納入方法

① 納入成果物はすべて日本語で作成すること。ただし、固有名詞及び英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。

② 情報処理に関する用語の表記については、日本産業規格（JIS）の規定に準拠すること。

③ 受注者は、「表 4　納入成果物一覧」を電子媒体（DVD 等）で 1 部納入すること。電子媒体に保存する形式は、Adobe PDF 又は Microsoft Office 365 で扱える形式とすること。納入する DVD に保管されている内容のインデックス、構成等については紙媒体で 1 部納入すること。紙媒体の納入は A4 判又は A3 判（A3 判を用いる場合は、折り込んで A4 判に収まる形態）でファイリングし、背表紙等を付けること。

④ 納入成果物は、納入後に発注者において改変が可能となるよう図表等の元データも併せて納入すること。

⑤ 納入成果物が外部に不正に使用されたり、納入過程において改竄されたりすることのないよう、安全な納品方法を提案し、納入成果物の情報セキュリティの確保に留意すること。

⑥ 電子媒体での納入に際しては、不正プログラム対策ソフトウェアによる確認を行う等して、納入成果物に不正プログラムが混入することのないよう適切に対処すること。

⑦ 納入成果物の作成及び納入にあたり、内容及び構成等について発注者が指摘した場合には、指摘事項に対応すること。

(3) 納入場所

〒212-8554

神奈川県川崎市幸区大宮町 1310　ミューザ川崎セントラルタワー20 階

10. 業務完了の通知

受注者は、全ての業務が完了したときは、完了報告を 2024 年 3 月 29 日（金）までに書面により発注者に通知すること。

11. 知的財産権の帰属等

(1) 本業務の作業により作成する納入成果物等に関し、著作権法（昭和 45 年法律第 48 号）第 21 条、第 23 条、第 26 条の 3、第 27 条及び第 28 条に定める権利を含む全ての著作権は発注者に帰属するものとする。なお、受注者は発注者に対し、一切の著作者人格権を行使しないものとし、第三者をして行使させないものとする。また、受注者は本調達の納入成果物に係る著作物を自ら使用し、又は第三者として使用させる場合は、発注者と別途協議し、発注者の許可を得るものとする。
(2) 納入成果物に第三者が権利を有する著作物が含まれているときは、発注者が特に使用を指示した場合を除き、受注者は当該著作物の使用に関して費用の負担を含む一切の手続きを行うものとする。
(3) 本調達の作業に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合、当該紛争の原因が専ら発注者の責めに帰す場合を除き、受注者は自らの負担と責任において適切に処理するものとする。

12. サプライチェーン・リスク対応要件

本業務のサプライチェーン・リスク対応要件を以下に示す。

(1) 受注者は、システムを構成する候補となる機器等について、あらかじめ発注者に一覧を記載したリストを提出し、発注者がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、発注者と迅速かつ密接に連携し提案の見直しを図ること。機器等の構成を変更する場合も同じ。
(2) 受注者は、資本関係・役員の情報、本業務の実施場所、本業務の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報を提示すること。履行期間中に従事者を変更する場合は、事前に発注者へ連絡し、了承を得ること。
(3) 受注者は、システムを構成する要素（機器等）に対して、不正な変更があった場合に識別できる構成管理体制を確立していること。また、当該構成管理体制が書類等で確認できること。
(4) 受注者がシステムを構成する要素として採用した機器等について、不正な変更が加えられていないことを検査する体制が受注者において確立していること。また、当該検査体制が書類等で確認できること。
(5) システムの提供、運用保守の各工程において、発注者の意図しない変更や機密情報の窃取等が行

われていないことを保証する管理が、一貫した品質保証体制のもとでなされていること。また、具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。第三者機関による品質保証体制を保証する書類等が提出可能な場合は提出すること。

(6) 現行システムに発注者の意図しない変更が行われる等の不正が見つかったときに、追跡調査や立ち入り調査等発注者と連携して原因を調査し、排除するための手順及び体制（例えば、運用保守業務におけるシステム操作ログや作業履歴等を記録し、発注者から要求された場合には提出させるようにする等）を整備していること。また、当該手順及び体制が妥当であることを証明するための書類を提出すること。

(7) 受注者は、本契約の履行について、請負業務の全部又は一部（主体的部分）を第三者に委任し、又は請け負わせてはならない。ただし、請負業務の一部（主体的部分）であって、あらかじめ発注者の承認を得た場合は、この限りではない。発注者の承認を得た場合には、受注者は発注者との契約上受注者に求められる水準と同等の情報セキュリティを請負業務の一部（主体的部分以外を含む。）を委任し、又は請け負わせた第三者（以下「下請負人」という。）においても確保すること。また、受注者は下請負人が実施する情報セキュリティ対策及びその実施状況について、発注者に報告すること。

(8) 本業務において取り扱う情報について、下請負人が閲覧することが無いように、受注者は情報を厳重に管理すること。やむを得ず下請負において業務に係る情報を開示する必要がある場合には、受注者は事前に発注者と調整し、発注者の指示に従うこと。

(9) 受注者は、下請負人における本業務の従事者の所属、専門性（資格等)、実績及び国籍に関する情報を提示すること。履行期間中に従事者を変更する場合は、事前に発注者へ連絡し、許可（又は確認）を得ること。

13. 情報管理体制

受注者は、情報管理体制に係る以下の規定を順守すること。

(1) 受注者は、本業務で知り得た情報を適切に管理するため、次の履行体制を確保し、発注者に対し「情報取扱者名簿」（指名、所属、役職、国籍等が記載されたもの）及び「情報管理体制図」（情報セキュリティを確保するための体制を定めた書面）を契約前に提出し、発注者の同意を得ること。また、本業務の情報取扱者の個人住所、生年月日、パスポート番号を発注者から求められた場合は、速やかに提出すること。なお、情報取扱者は、本業務の遂行のために最低限必要な範囲で設定すること。

(2) 契約を履行する一環として受注者が収集、整理、作成等を行った一切の情報が、発注者が保護を要さないと確認するまでは、情報取扱者名簿に記載がある者以外に伝達又は漏えいされないことを保証する履行体制を有していること。

(3) 本業務で知り得た一切の情報について、情報取扱者以外の者に開示又は漏えいしてはならない。ただし、発注者の承認を得た場合はこの限りではない。

(4) (1)の情報セキュリティを確保するための体制を定めた書面又は情報取扱者名簿に変更がある場合

は、あらかじめ発注者に提出し、同意を得ること。

(5) 発注者が提供した資料又は発注者が指定した資料の取扱い（返却・削除等）については、発注者の指示に従うこと。

14. 機密保持

(1) 受注者は、本業務に係る作業を実施するにあたり、発注者から取得した情報（電子媒体、文書、図面等の形態を問わない。）を含め契約上知り得た情報を、第三者に開示又は本業務に係る作業以外の目的で利用しないものとする。ただし、次の①から⑤のいずれかに該当する情報は除くものとする。

① 発注者から取得した時点で、既に公知であるもの

② 発注者から取得後、受注者の責によらず公知となったもの

③ 法令等に基づき開示されるもの

④ 発注者から秘密でないと指定されたもの

⑤ 第三者への開示又は本業務に係る作業以外の目的で利用することについて、事前に発注者と協議のうえ、承認されたもの。

(2) 受注者は、発注者の許可なく、取り扱う情報を指定された場所から持ち出し、又は複製しないものとする。

(3) 受注者は、本業務に係る作業に関与した受注者の所属職員が異動した後においても、機密が保持される措置を講じるものとする。

(4) 受注者は、本業務に係る検収後、受注者の事業所内部に保管されている本業務に係る発注者に関する情報を、裁断等の物理的破壊、消磁その他復元不可能な方法により速やかに抹消するとともに、発注者から貸与されたものについては、契約終了後 1 週間以内に発注者に返却するものとする。

15. 情報セキュリティに関する受注者の責任

(1) 情報セキュリティを確保するための体制の整備

受注者は、受注者組織全体の情報セキュリティを確保するとともに、発注者から求められた本業務の実施において情報セキュリティを確保するための体制を整備すること。

(2) 情報セキュリティが侵害された場合の対処

本業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され、又はその恐れがある場合には、直ちに発注者に報告すること。これに該当する場合には、以下の事象を含むこととする。

① 受注者に提供し、又は受注者にアクセスを認める発注者の情報の外部への漏えい及び目的外利用

② 受注者による発注者のその他の情報へのアクセス

また、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、発注者の求め

に応じて成果物と共に発注者に引き渡すこと。

情報セキュリティが侵害され、又はその恐れがある事象が本業務に係る作業中及び契約に定める契約不適合期間中に発生し、且つ、その事象が受注者における情報セキュリティ上の問題に起因する場合は、受注者の責任及び負担において次の各号を速やかに実施すること。

① 情報セキュリティ侵害の内容及び影響範囲を調査のうえ当該情報セキュリティ侵害への対応策を立案し、発注者の了承を得たうえで実施すること。

② 発生した事態の具体的内容、原因及び実施した対応策等について報告書を作成し、発注者へ提出して了承を得ること。

③ 再発防止対策を立案し、発注者の了承を得たうえで実施すること。

④ 上記のほか、発生した情報セキュリティ侵害について、発注者の指示に基づく措置を実施すること。

(3) セキュリティ対策の改善

受注者は、本業務における情報セキュリティ対策の履行状況について発注者が改善を求めた場合には、発注者と協議のうえ必要な改善策を立案して速やかに実施するものとする。

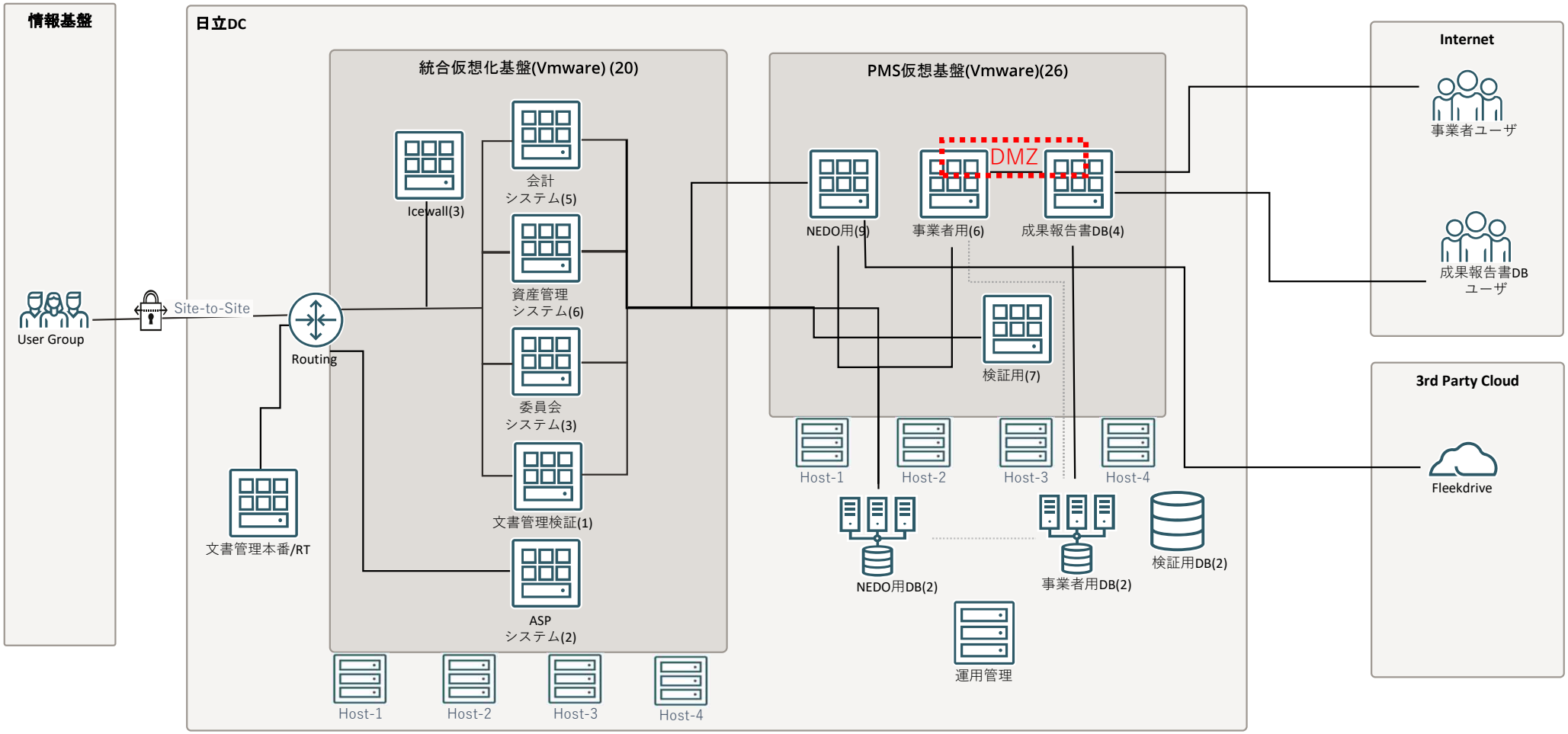
16. その他

仕様にない事項又は仕様について生じた疑義については、発注者と協議のうえ解決すること。

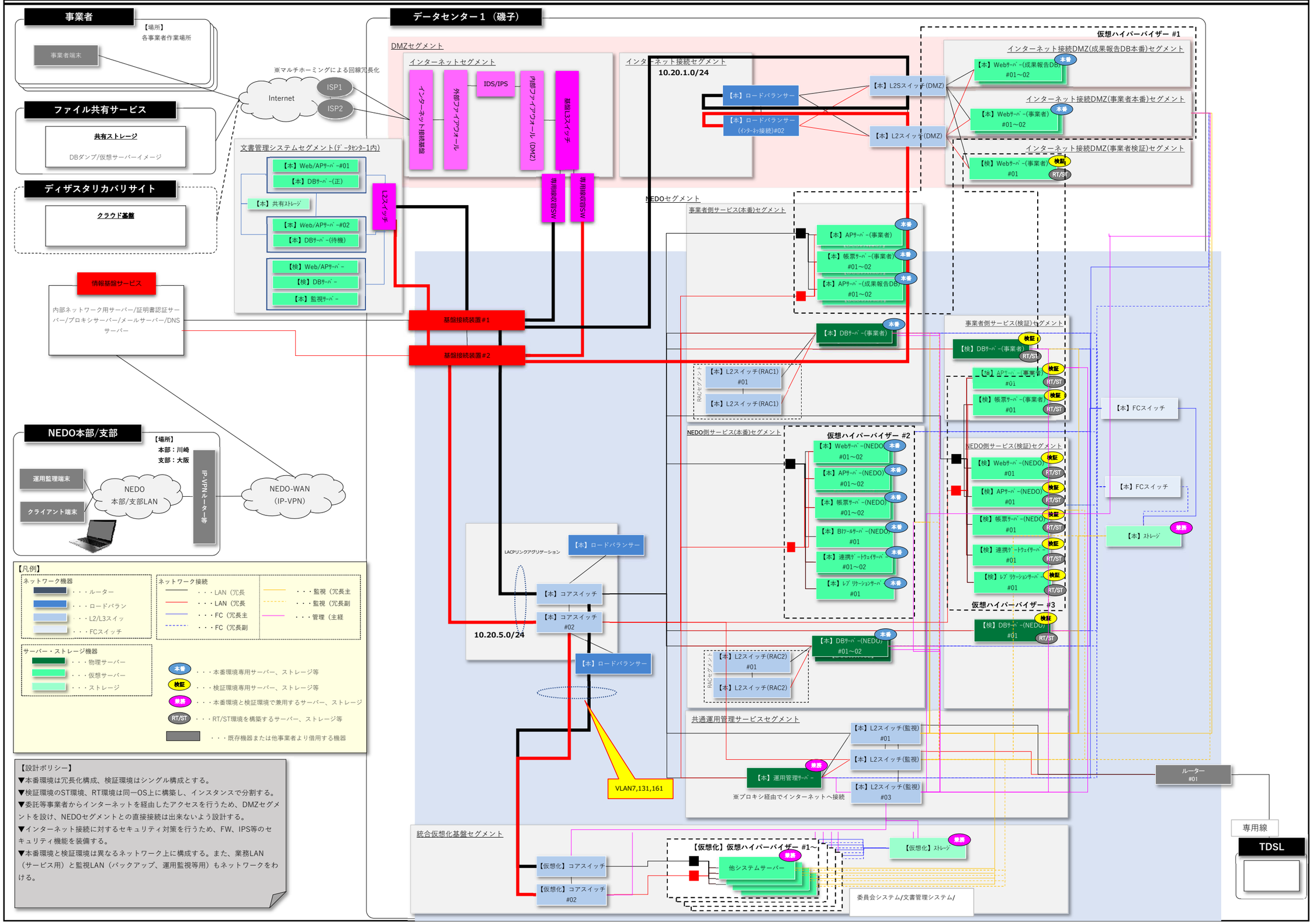
別添1 用語の定義一覧

No.	用語	説明
1	NEDO	国立研究開発法人新エネルギー・産業技術総合開発機構を指す。
2	事業者	NEDOの技術開発プロジェクトに参加する事業者を指す。
3	PMS	プロジェクトマネジメントシステムを指す。
4	RT	受け入れテストを指すが、本資料では受け入れテストを実施する環境を指す。NEDOでは研修用の環境も兼ねる。
5	ST	システムテストを指すが、本資料ではシステムテストを実施する環境を指す。
6	運用管理サーバ	OCVS上の仮想サーバの運用監視、ジョブ管理を行うサーバを指す。
7	踏み台サーバ	OCVS上の仮想サーバの各アプリケーションの運用保守ベンダー用の中継サーバを指す。
8	BYOL	Bring Your Own License（所有しているライセンスの持ち込み）の略。
9	発注者の情報基盤サービス	別運用保守事業者が提供している発注者が利用するPC、ネットワーク、モバイル機器等のサービスを指す。

別添２ 現在の構成

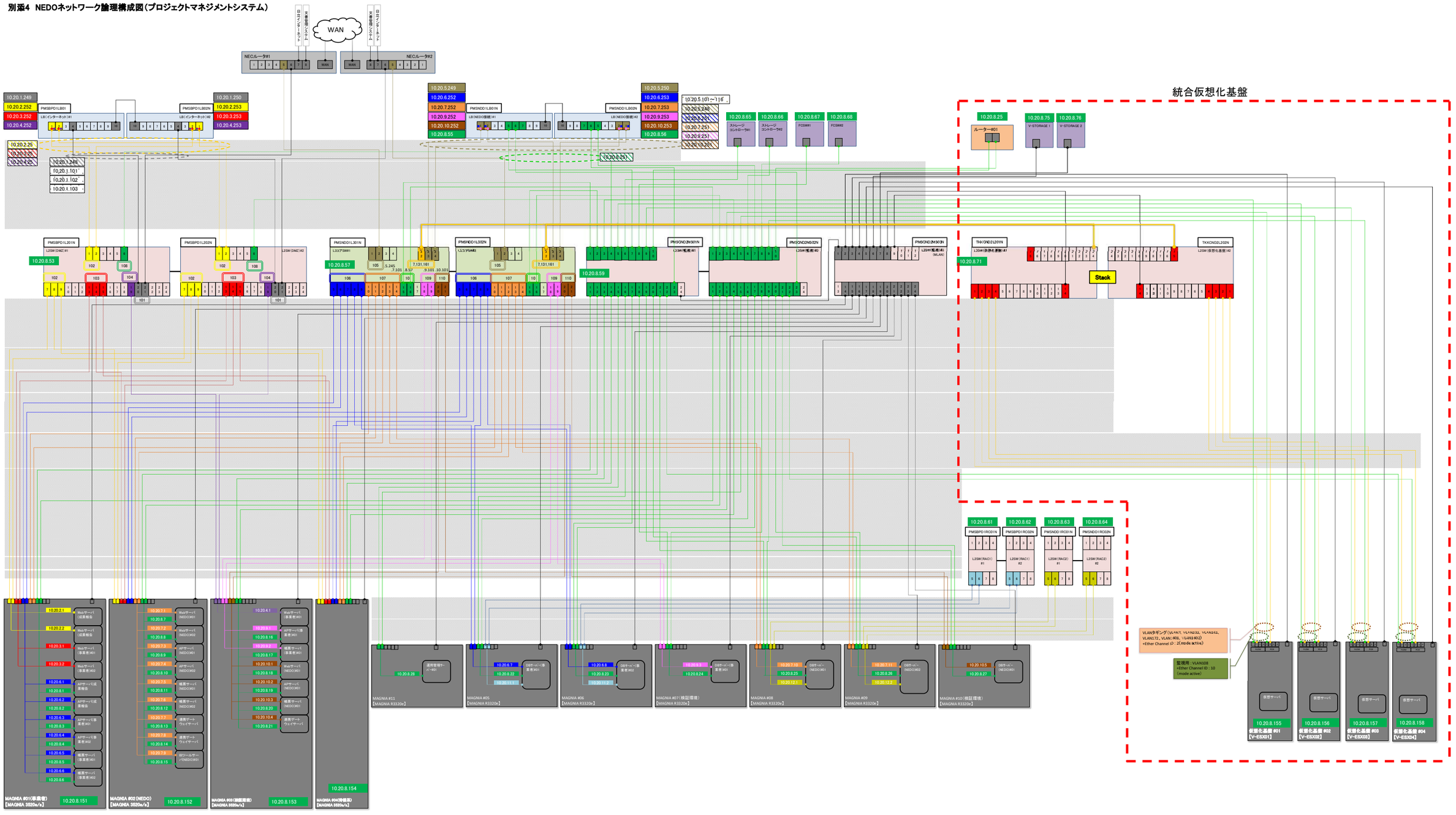

情報基盤
日立DC
統合仮想化基盤(Vmware) (20)
PMS仮想基盤(Vmware)(26)
Internet
事業者ユーザ
成果報告書DB
ユーザ
3rd Party Cloud
Fleekdrive
User Group
Site-to-Site
Routing
Icewall(3)
会計
システム(5)
資産管理
システム(6)
委員会
システム(3)
文書管理検証(1)
ASP
システム(2)
文書管理本番/RT
Host-1
Host-2
Host-3
Host-4
NEDO用(9)
事業者用(6)
DMZ
成果報告書DB(4)
検証用(7)
Host-1
Host-2
Host-3
Host-4
NEDO用DB(2)
事業者用DB(2)
検証用DB(2)
運用管理

文書名	システム構成図	システム名
		プロジェクトマネジメントシステム,連携システム

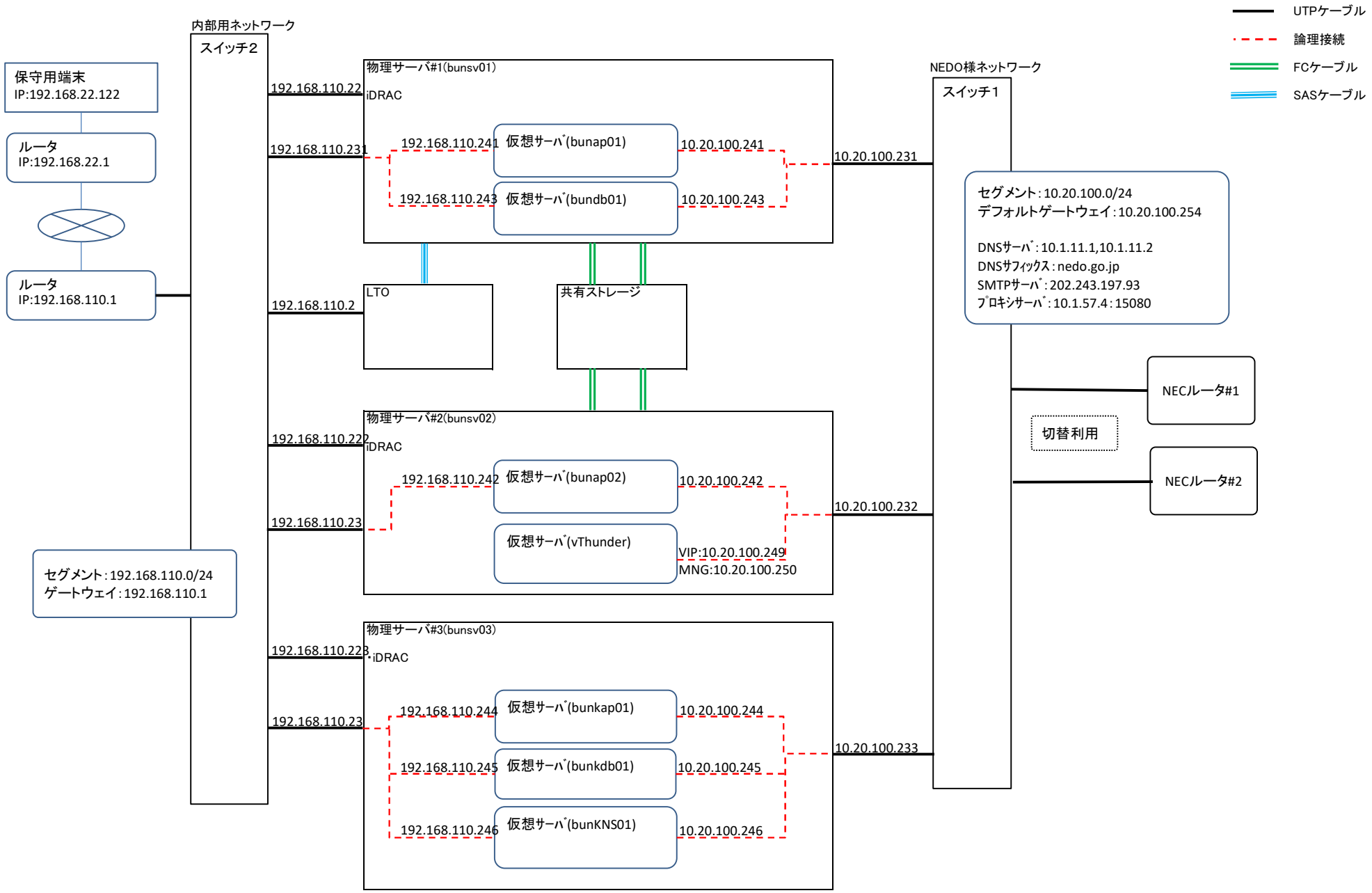


【設計ポリシー】
▼本番環境は冗長化構成、検証環境はシングル構成とする。
▼検証環境のST環境、RT環境は同一OS上に構築し、インスタンスで分割する。
▼委託等事業者からインターネットを経由したアクセスを行うため、DMZセグメントを設け、NEDOセグメントとの直接接続は出来ないよう設計する。
▼インターネット接続に対するセキュリティ対策を行うため、FW、IPS等のセキュリティ機能を装備する。
▼本番環境と検証環境は異なるネットワーク上に構成する。また、業務LAN（サービス用）と監視LAN（バックアップ、運用監視等用）もネットワークをわける。

別添4　NEDOネットワーク論理構成図（プロジェクトマネジメントシステム）



別添4　NEDOネットワーク論理構成図（文書管理システム）



別添5_仮想化基盤_ハードウェア構成図