横浜市
受付管理・申請業務支援システム
開発仕様書

令和２年４月１日

本書は、受付管理・申請業務支援システムを開発するにあたっての開発環境等の与条件、プロジェクトの管理体制の考え方を示すものである。

横浜市健康福祉局
保険年金課
医療援助課
介護保険課

【目次】

1　名称

横浜市受付管理・申請業務支援システム（以下、申請管理システム）開発業務委託

2　開発の実施に関する要件

本市では、福祉関係の業務を行うシステムを当面の対象として、これらのシステムで共通に利用すべき機能やデータを、情報共有基盤に集約させることを想定している。 情報共有基盤は今後情報共有基盤により統合される全ての業務システムが利用するもので、これによって、運用などを効率化させることを狙っている。住民記録情報、住登外情報、個人市民税情報及び職員・組織情報が情報共有基盤で共通管理されているため、申請管理システム構築にあたっては、情報共有基盤に構築しなければならない。

情報共有基盤の詳細は、別紙１【情報共有基盤　機能概要説明書】、別紙２【データ連携基盤概要】、別紙３【SS0 連携方式の概要】、別紙４【横浜市情報共有基盤システム仮想基盤利用者ガイドライン】、別紙５【仮想基盤（仮想マシン）の利用可否の条件・仕様について】を参照すること。

3　システムの機能要件

（1）機能要件

申請管理システムの機能要件については、業務説明資料７（２）【申請管理システム機能要件】を参照すること。

業務説明資料に記載したもの以外の機能要件については以下に示す。

ア　運用管理機能

効率的なシステム運用管理を実現するために、申請管理システムの運用管理は、原則として、情報共有基盤が提供する運用管理機能を利用するように検討すること。

イ　ログ出力要件

申請管理システムが出力するシステムログには、アプリケーションログとデータへのアクセスログがあり、障害発生時や監査証跡、セキュリティ違反追跡などに活用される。システムログは、情報共有基盤の運用基盤の仕様に基づき出力すること。

（ア）　アプリケーションログ

申請管理システムのアプリケーションログを出力すること。アプリケーションログの保管期間は１週間とする。ログ保存領域は、サイクリックに利用すること。オンライン処理及びバッチ処理に関する処理結果、運用担当が行う各種運用オペレーションの結果について、情報共有基盤の運用基盤により管理できるよう申請管理システムからログを出力すること。

（イ）アクセスログ

アクセスログについては、「３（４）カ　アクセスログに関する要件」を参照すること。

ウ　バッチ処理要件

オンライン終了後の一連のバッチ処理に関する前提条件と要件を示す。

（ア）前提条件

オンライン終了後に実行する一連のバッチ処理は原則として事前登録したジョブ実行スケジュールに基づき自動実行すること。ジョブ実行スケジュールの登録は、原則として情報共有基盤の運用基盤が提供するバッチジョブ管理機能を利用すること。

（イ）バッチ処理要件

a　バッチ処理はジョブ実行スケジュールに基づいた連続処理実行を可能とすること。

b　臨時処理対応などの理由により手動によるジョブ起動が発生することを想定し、スクリプトなどで実行するなどの運用担当の操作ミスの発生を極小化する仕組みを構築すること。

なお、手動によるジョブ起動の結果確認においても、自動実行処理と同様の仕組みで稼働状況が確認できる仕組みとすること。

c バッチ処理実行中に障害等が発生しデータが失われる、誤って登録される等のデータの不整合が生じた場合において、データのリカバリが行えること。

4　システムの非機能要件

業務要件、機能要件以外の事項に関する要件を示す。

（1）基盤システム機能の活用

情報共有基盤が提供する基盤システム機能を利用すること。なお、申請管理システム構築で当機能を使用時の個別要件を以下に示す。

ア　SSO の利用

保険年金課では情報共有基盤で稼働している国保収対システム等は SSO を利用しているため、ユーザインタフェースの観点から申請管理システムも SSO の利用が望ましいが、申請管理システムの業務要件等により SSO を利用できない場合などは、この限りではない。SSO の詳細は、別紙３を参照すること。

イ　ポータルの利用

システム開発としては受付管理システムと申請業務支援システムとなるが、ポータルには申請管理システムの起動画面へのリンクを設ける。

（2）性能要件

申請管理システムが満たすべき性能についての要件を示す。開発業者はシステムのチューニングを実施し、快適な操作性が得られるまで対応すること。

ア　クライアント台数及び同時接続数

（ア）利用クライアント台数

当初のクライアント台数は 320 台とする。ただし、今後システム対象業務拡大により台数をさらに増やす可能性がある。

（イ）同時接続数

サーバへのリクエストは全利用クライアントの２割のクライアントから同時 に受けられることとする。

イ　オンライン処理性能

（ア）検索

レスポンスタイムの目安としては、個人検索処理でカナ検索を行う場合、ボタン押下から結果表示開始まで 3 秒以内を目安とすること。ただし、個人検索などで条件に当てはまる対象者数が多い場合や絞り込み条件が多岐に亘る場合などはこの限りではない。

（イ）登録・更新

原則、ボタン押下から結果表示開始までを３秒以内を目安とすること。

（ウ）帳票表示

数ページ程度の帳票の場合、表示を指示してから実際に表示されるまで５秒以

内を目安とすること。

ウ　バッチ処理性能

オンライン終了後に実行する一連のバッチ処理は、翌日のオンライン開始並びに情報共有基盤のバックアップ等の運用に支障をきたさない時間までに終了するように構築すること。

（3）信頼性等要件

ア　信頼性要件

申請管理システムは基本的にはオンラインシステムは業務時間帯の稼働、バッチシステムは夜間時間帯の稼働を前提に信頼性要件を以下のとおり定めている。具体的な稼働時間は、本業務内で要件を明確にし、本市担当者と調整の上で決定すること。

（ア）申請管理システムの可用性

サーバ機器に専用のハードウェアを使用する場合、障害箇所をできるだけ局所化できるように設計・構築すること。ハードウェア単一障害等によってシステム全体が停止することがないようにすること、また、アプリケーションの処理状態を適切に管理・保管し、障害が発生した場合でも速やかに障害発生時点の状態に復帰できるようなアプリケーション設計とすること等により、システムの可用性を確保すること。

情報共有基盤では、データのバックアップなどのために必要となるシステム停止時間は必要最小限となるように構成している。詳細は別紙１を参照すること。

（イ）障害発生時におけるシステム利用の継続

申請管理システムは、区役所の窓口において利用するシステムである。システムが停止すると窓口業務に支障が生じ市民サービスの低下に直結するため、システム障害発生時でも回避運用等により極力業務の全面停止にならないよう考慮すること。

障害が発生したときには、復旧までの時間を 30 分以内とする。そのために、バックアップなどの利用により障害発生前の状態に速やかに戻せる仕組みを構築すること。

申請管理システム上で稼働している業務のいずれかで障害が発生した場合でも、他業務の機能は障害発生業務と関連しない範囲で利用が継続できるよう業務別にメンテナンスが可能な構成とすること。

イ　拡張性要件

将来的な世帯及び被保険者の増加等、業務処理量の増加に伴って必要となる性

能の強化に対応できるように、原則として、スケールアウトが可能であること。

ウ　上位互換性要件

制度改正対応等によるシステムのバージョンアップの際、旧バージョンのシステム構成を大きく変えることなく新バージョンに移行できる上位互換性を有すること。

エ　システム中立性要件

連携先のシステムが稼働していないとシステムの利用が出来ない等の過度に他システムに依存した作りとせず、システムの独立性を保つようにすること。なお、情報共有基盤が提供する機能を用いる部分（SSO によるユーザ認証）等、一部例外が存在する。その詳細については本市と調整し決定すること。

オ　事業継続性要件

大規模災害発生時等における事業継続並びにシステム復旧については、本市と協議の上で要件を確定し、必要な対策を講ずること。

（4）セキュリティ要件

ア　個人情報に関する要件

申請管理業務では大量の個人情報を取り扱っていることから、情報セキュリティには十分な対策が必要である。以下の条例などの趣旨を十分理解し、申請管理システムを構築すること。

（ア）横浜市個人情報の保護に関する条例
https://cgi.city.yokohama.lg.jp/somu/reiki/reiki_honbun/g202RG00001340.html

（イ）横浜市個人情報の保護に関する条例施行規則
https://cgi.city.yokohama.lg.jp/somu/reiki/reiki_honbun/g202RG00001341.html

イ　情報セキュリティポリシーに関する要件

本市の情報セキュリティポリシーに準拠すること。セキュリティに十分配慮した設計を行い、利用権限の無い者が不正にアクセスし、データを閲覧したり、更新したりできない設定、構築を行うこと。構築に際しては、以下を参照し、調整が必要な事項があれば速やかに本市と協議し修正すること。

（ア）横浜市情報セキュリティ管理規程　（準拠）
https://cgi.city.yokohama.lg.jp/somu/reiki/reiki_honbun/g202RG00001344.html

（イ）横浜市情報セキュリティ管理要綱　（準拠）別紙６

（ウ）住民情報系ネットワーク　セキュリティ管理ガイドライン（準拠）別紙７

また、Web アプリケーションを構築する際には、独立行政法人 情報処理推進機構 セキュリティセンター「安全なウェブサイトの作り方」を参考にセキュリティ要件に配慮して構築すること。

https://www.ipa.go.jp/security/vuln/websecurity.html

ウ　認証に関する要件

情報共有基盤の SSO 機能を利用すること。また、認証情報は、情報共有基盤の SSO 管理機能で、一元的に追加・更新をできるようにすること。

エ　認可に関する要件

（ア）認可の制御

利用権限の無い者が不正にアクセスし、データを閲覧したり更新したりすることができないような仕組みを持たせること。

画面（URL）単位の権限については、情報共有基盤の SSO 機能にて認可機能を提供する。

なお、申請管理システムでは、情報共有基盤の SSO 機能に加えて、利用者の所属並びに職責に応じて、システムの利用権限管理を行うことを想定している。この要件を明確化し、権限管理に関する機能を実装すること。

オ　アクセスログに関する要件

申請管理システムのアプリケーションがデータにアクセスする際に、別紙８【個人情報を記録したシステムにおける端末機によるデータの更新、検索などの操作の記録に関する要綱（アクセスログ要綱）】に定める内容に基づき、アクセスログを出力すること。また、利用者のログイン及びデータの変更についてもログとして記録すること。

なお、これらのログは、適切な権限保有者のみが参照できるようにすること。

カ　その他セキュリティに関する事項

申請管理システムの設置場所及び本市施設内で作業を行う際は、本市が定めるルールに従うこと。

申請管理システムのデータが、利用者の不注意などによって失われたり、意図しない更新が行われたりしないよう、アプリケーションの設計時に十分に考慮すること。また、故意にデータを失わせるような操作に対しては、アプリケーションによる対応のみでは十分に対策できない場合が想定されるため、データのバックアップを取得するなどの対応をあわせて考慮すること。

（５）情報システム稼働要件

ア　システム構成

要件分析を行った結果を基に設計し、申請管理システムとして必要なシステム構成を明らかにすること。

実際にサービスを提供する本番環境と、本番環境へのリリース前に受入テストなどを行う開発／保守環境、利用者向け研修などを行う研修環境をそれぞれ分けて運用できるように構築すること。

イ　本市システム構成におけるサーバソフト、クライアントソフト

情報共有基盤側で用意されないサーバ及びミドルウェアを導入するにあたっては、情報共有基盤所管部門の許諾を得ること。

クライアントについて、申請管理システムの稼働に必要なインストール作業、設定などがある場合は、関係部署と調整した上で、実施方法を決定し、実施すること。

ウ　サーバに関するシステムインフラ要件

（ア）本市システム構成へのリリース

申請管理システムの本番環境、開発／保守環境及び研修環境へのリリースに関しては開発業者が行うこと。その時に行う手順についてはリリース手順書として本市に納めること。

（イ）サーバ仕様

申請管理システムのサーバで必要とされる性能については、別紙１、別紙４及び別紙５に記載されている要件を満たすこと。また、特殊な要件や構成を求める場合は、情報共有基盤所管部門の許諾を得ること。

エ　クライアントに関するシステムインフラ要件

（ア）クライアントに関する動作環境要件

クライアント機器は、本市が別途調達し、ソフトウェアのインストール及び設定はクライアント機器調達時にあわせて実施することとする。

（イ）クライアント等

クライアント機器は本体（パソコン）の他、バーコードリーダー等を本市が用意する。

（6）システム運用要件

申請管理システムの運用保守業務は別途調達とするが、開発業者は、申請管理システム稼働後の運用を踏まえて開発し、運用設計を行うこと。なお、詳細な運用要件については、開発プロセスの中で検討し、本市と協議の上で内容を決定すること。

申請管理システムの運用は、開庁日に加え、閉庁日においても可能な限りシステムが利用できるような状態にあることが求められる。ただし、システムメンテナンス時間帯でのシステム稼働は制限されることとする。

（7）保守要件

ア　ソフトウェア保守要件

サーバーアプリケーションやクライアントアプリケーション等でパッケージソフトウェアを導入する場合、法改正等の制度改正に伴う大規模改修を除き、パッケージソフトウェアの保守の中で無償対応させること。

（8）ユーザインタフェース要件

ア　基本要件

（ア）窓口で利用することを考慮し、入力に対する反応の早さ、入力の容易さなどの操作性を十分に配慮すること。

（イ）ボタンの配置・順序等が統一されている等、システム全体での操作性がほぼ一致するようにレイアウトの統一性があること。必要とする範囲で画面レイアウトの変更に対応できること。

（ウ）日本工業規格（JIS）で制定されたウェブコンテンツのアクセシビリティに関する規格「JIS X8341　高齢者・障害者など配慮設計指針－情報通信におけるシステム機器、ソフトウェア及びサービス－第 3 部：ウェブコンテンツ」に準拠し、利用者のアクセシビリティを高め、作業効率の向上に寄与できるよう十分に配慮すること。ただし、適用については本市と協議の上確定すること。

イ　利用者支援要件

（ア）アクセシビリティ要件

様々な環境や利用者の特性を考慮し、利用者が誰でも確実に必要な情報に到達できるように、アクセシビリティを実現すること。

a　視覚障害者の配慮（ハイコントラスト対応）

ハイコントラストのスタイルシートを用意するなどにより視覚障害者に配慮すること。

（イ）操作ガイド

利用者の操作把握を促すとともに、利用者自身がシステム利用上の不明点を調べられるようガイダンスやヘルプを表示する機能を用意することについて検討すること。

これらを設計・構築する場合には以下の要件に従うこと。

a　ガイダンス

ガイダンスは、業務処理の説明を示す。業務処理画面中の項目とは明確に区分して表示し、対象画面の処理の目的や処理上の注意などについて簡潔で分かりやすく説明すること。

b　ヘルプ

(a) システム操作に不慣れな者、業務経験が少ない者の利用を前提としたできるだけ平易な記述とすること。

(b) ヘルプは、一貫性のとれた分かりやすい表現とすること。

(c) ヘルプの本文には、外部資料やコードの参照を含めないこと。

(d) ヘルプの内容は、処理中の部分だけでなく業務全体についても表示できるようにすること。

5　プロジェクト管理要件

本業務において開発業者が行うべきプロジェクト管理に関する要件を以下に示す。

（1）　プロジェクト管理方法

開発業者は、提案時に提案書作成要領に従ってプロジェクト管理方法を提示し、本市と内容を協議の上、承認を得ること。また、プロジェクトの計画に変更が発生した際には、随時プロジェクト計画書を改版し、本市の承認を得ること。

（2）　開発・保守環境・機器に関する要件

作業に必要な施設、システム機器及びネットワークなどについては、開発業者が用意すること。

（3）　全体スケジュールに関する要件

作業に必要な施設、システム機器及びネットワークなどについては、開発業者が用意すること、本市が提示するマイルストーンを踏まえて、全体スケジュールを策定すること。全体スケジュールには概要レベルの開発計画スケジュールについても盛り込むこと。

データ連携において、他システムとの連携に関する大まかな要件を明らかにすること。具体的な連携内容、及びそれ以外に改修等の経費支出を伴う影響を他システムに対し与えることが想定される事項については、他システム所管部門と影響度を踏まえた調整すること。開発業者は、調整の際に連携が必要なデータ項目などを提示できるようなスケジュールを策定すること。

要件分析の完了、基本設計の完了等、作業進捗上のマイルストーンにおいて、実施した工程の成果を本市が確認する。確認の結果問題ないと判断できてから次の工程に着手するように作業を管理すること。また、その確認のための期間も考慮してスケジュールを策定すること。

（4）　会議体に関する要件

本プロジェクトで最低限必要とする会議体について、表　5－1に示す。この他にプロジェクト遂行上必要となる会議体について、プロジェクト計画を策定する際に本市担当者と協議の上決定し、プロジェクト計画書に記載すること。

表 5-1 会議体一覧

会議名称	概要	目的	出席者	開催頻度
プロジェクト会議	プロジェクトの最高意思決定機関である。プロジェクト遂行上重要な事項の判断・決定を行う。	・プロジェクト全般の進行状況の把握 ・プロジェクト計画の大幅な変更に関する判断と決定 ・その他プロジェクト全体に影響する事項の決定	【受注者側】 ・プロジェクト責任者 ・プロジェクト管理者 ・業務系リーダー（業務アナリストリーダー、仕様ホルダー） ・システム系リーダー（システムアナリストリーダー、チーフアーキテクト） 【発注者側】 ・プロジェクト責任者 ・プロジェクト管理者 ・本市担当者	別途協議
定例会議	プロジェクトの進捗状況を定期的に把握・管理する。プロジェクト上の種々の課題を把握し、解決に向けた活動を行う。	・プロジェクトの進捗管理、課題管理、品質管理 ・プロジェクト計画の変更に関する判断と決定 ・その他プロジェクト進行に係る事項の決定	【受注者側】 ・プロジェクト管理者 ・業務系リーダー（業務アナリストリーダー、仕様ホルダー） ・システム系リーダー（システムアナリストリーダー、チーフアーキテクト） 【発注者側】 ・プロジェクト管理者 ・本市担当者	週１回程度 （定例のほか、変更管理のために集中検討が必要な場合は、随時）
個別検討会議	業務要件の把握等、個別具体的な事項の確認、調整、検討等が必要な場合に実施する。	個別事項の確認調整等	実施内容に応じてメンバーを選定	随時

（５） プロジェクトの体制に関する要件

別紙９の体制図イメージ及び（６）～（10）の要件を踏まえて、必要な体制案を本市に提案すること。その体制案を基に本市と調整して体制を決定すること。

なお、体制には、福祉業務（医療保険及び介護保険）の知識を有する者が含まれていることが望ましい。

（６） プロジェクト管理者に関する要件（テーラリング、要件分析、開発、テストの管理を行うプロジェクトの責任者）

ア　次の要件を備えた者を１名以上配置すること。

（ア）　開発プロセスの実施経験を有すること

（イ）　複数の開発プロセスの知識を有すること

（ウ）　中規模以上のシステムのプロジェクト管理経験を3年程度有すること

（エ）　中規模以上のシステムの開発経験を5年程度有すること

イ　プロジェクト内の役割を兼任することはできない。

（７） テーラリングマネージャーに関する要件（業務主管課が３課（保険年金課、医療援助課、介護保険課）となるため、システムや業務仕様等のテーラリングを行い、プロジェクトメンバに伝達する）

ア　次の要件を備えた者を１名以上配置すること。

（ア）　中規模以上のシステムのプロジェクト管理経験を3年程度有すること

（イ）　中規模以上のシステムの開発経験を5年程度有すること

イ　プロジェクト内の役割を兼任することはできない。

（８） 要件分析の実施に関する要件

ア　作業実施環境に関する要件

開発業者が要件分析作業を行うために必要な施設、システム機器及びネットワークなどについては、開発業者が用意すること。

本市が参加する各種会議及び打合せは、原則として本市が準備する会議室にて実施すること。

イ　要件分析体制

開発業者は、事前にプロジェクト計画書の中に要件分析体制・要件分析計画を記載し、本市に提示して承認を得ること。体制の変更など、本プロジェクトの遂行にかかる技術水準に変更が生じる場合は、事前に本市と協議の上、本市の承認を得ること。要件分析に携わる者の役割及び求められる具体的な経験・知識を（ア）に示す。また、担当者の兼任ルールを（イ）に示す。各役割を担う要員を必ず体制内に組み込んで、要件分析体制を整備すること。体制を示す資料には各役割の担当者を明記すること。

申請管理システムの開発規模を踏まえた上で、体制を適度なチームに分割すること。

不測の事態などにより作業に遅延などが発生した場合でも、その遅延などを取り戻すことができるように、体制を決定するときに予め考慮すること。

（ア）要件分析担当者の役割と求められる経験・知識

要件分析に携わる者の役割と求められる具体的な経験・知識は、以下のとおりである。要件にない役割であっても必要があれば体制に追加すること。

a　業務アナリストリーダー（業務要件チームの管理者であり、業務要件チームの業務遂行に対する責任がある）

(a) プロジェクト管理経験を有すること

(b) 業務分析の経験を2年程度有すること

b　システムアナリストリーダー（システム分析チームの管理者であり、システム分析チームの業務遂行に対する責任がある）

(a) プロジェクト管理経験を有すること

(b) ミドルウェア製品の知識を有すること

(c) 中規模以上のWebシステムの分析設計経験を３年程度有すること

（イ）要件分析担当者の兼任ルール

プロジェクト管理者は役割を兼任することはできない。

ウ　協力体制

開発業者は主導的な役割を果たして、基幹システム（国民健康保険、介護保険、後期高齢者医療制度）運用保守業者、情報共有基盤（基盤上で稼働しているシステムを含む）の運用保守業者等との調整などを実施すること。

調整に必要な情報の取得については、本市が仲介するので必要事項があれば申し出ること。

（９）　開発の実施に関する要件

ア　開発ツールに関する要件

作業効率向上などのために特定のツールがある場合は、本市と協議の上確定すること。

イ　開発体制

開発業者は、事前にプロジェクト計画書の中に開発体制・開発計画を記載し、本市に提示した上、承認を得ること。

体制の変更など、本プロジェクトの遂行にかかる技術水準に変更が生じる場合は、事前に本市と協議の上で、本市の承認を得ること。

開発に携わる者の役割及び求められる具体的な経験・知識と、体制イメージを

（ア）に示す。また、担当者の兼任ルールを（イ）に示す。各役割を担う要員を必ず体制内に組み込んで、開発体制を整備すること。体制を示す資料には各役割の担当者を明記すること。

申請管理システムの開発規模を踏まえた上で、開発体制を適度なチームに分割すること。

不測の事態などにより開発に遅延などが発生した場合でも、その遅延などを取り戻すことができるように、体制を決定するときに予め考慮すること。

（ア）開発担当者の役割と求められる経験・知識

開発に携わる者の役割と、求められる具体的な経験・知識は、以下のとおりである。要件にない役割であっても、必要があれば開発体制に追加すること。

a　開発管理者（開発の責任者。開発作業の管理を行う。）

(a) 開発プロセスの実施経験を有すること

(b) 複数の開発プロセスの知識を有すること

(c) 中規模以上のシステムのプロジェクト管理経験を 3 年程度有すること

(d) 中規模以上のシステムの開発経験を 5 年程度有すること

b　チーフアーキテクト（アーキテクチャ設計を行う。）

(a) ミドルウェア製品の知識を有すること

(b) アプリケーションサーバの知識を有すること

(c) パッケージソフトウェアのアーキテクチャに精通していること

(d) 中規模以上の Web システムの分析設計経験を 3年程度有すること

c　開発リーダー（作業効率等により開発をチーム分割した場合、その管理者となる。チームの開発作業の管理を行う）

(a) 開発経験及び開発管理経験を有すること

(b) ミドルウェア製品の知識を有すること

(c) アプリケーションサーバの知識を有すること

(d) 中規模以上の Web システムの分析設計経験を 3年程度有すること

（イ）開発担当者の兼任ルール

開発に携わる者の兼任のルールは、以下のとおりである。

a　開発管理者は、開発リーダーを兼ねることができる。

b　開発管理者は、チーフアーキテクトを兼任することはできない。

c　チーフアーキテクトは、開発リーダーを兼ねることができる。

d　チーフアーキテクトは、開発管理者を兼任することはできない。

(10) テストの実施に関する要件

ア　テストツールに関する要件

作業効率向上などのために特定のツールがある場合は、本市と協議の上確定すること。

イ　テスト体制

開発業者は、事前にテスト計画書を本市に提示して、承認を得ること。

体制の変更など、テストの遂行にかかる技術水準に変更が生じる場合は、事前に本市と協議の上で、本市の承認を得ること。

テストに携わる者の役割及び求められる具体的な経験・知識と、体制イメージを（ア）に示す。また、担当者の兼任ルールを（イ）に示す。各役割を担う要員を必ず体制内に組み込んで、開発体制を整備すること。体制を示す資料には各役割の担当者を明記すること。

申請管理システムの開発規模を踏まえた上で、テスト体制を適度なチームに分割すること。

不測の事態などにより開発に遅延などが発生した場合でも、その遅延などを取り戻すことができるように、体制を決定するときに予め考慮すること。

（ア）テスト担当者の役割と求められる経験・知識

テストに携わる者の役割と、求められる具体的な経験・知識は、以下のとおりである。要件にない役割であっても、必要があればテスト体制に追加すること。

a　テスト管理者（テストの責任者。テスト作業の管理を行う。）

(a) 中規模以上の Web システムのテスト仕様作成経験を 3年程度有すること
(b) テスト経験及びテスト管理経験を有すること

b　テストケース作成者（業務仕様を理解し、テスト仕様書を作成する。）

(a) 中規模以上の Web システムのテスト仕様作成経験を 3年程度有すること
(b) テスト経験及びテスト管理経験を有すること

c　テストリーダー（作業効率等によりテストをチーム分割した場合、その管理者となる。チームのテスト作業の管理を行う）

(a) 中規模以上の Web システムのテスト仕様作成経験を 3年程度有すること
(b) テスト経験及びテスト管理経験を有すること

（イ）テスト担当者の兼任ルール

テストに携わる者の兼任のルールは、以下のとおりである。

a　テスト管理者は、テストリーダーを兼ねることができる。
b　テスト管理者は、テストケース作成者を兼任することはできない。
c　テストケース作成者は、テストリーダーを兼ねることができる。
d　テストケース作成者は、テスト管理者を兼任することはできない。

（ウ）受入テストに関する事項

本市が実施する受入テストに向けて、本市が作成する受入テスト仕様書と開発業者が作成する受入テスト仕様書のテスト項目について、本市と合意を得ること。また、受入テストのテスト計画、テストデータの作成、テストのための環境構築は、本市の指示に従い開発業者が実施すること。

（エ）協力体制

開発業者は主導的な役割を果たして、基幹システム（国民健康保険、介護保険、後期高齢者医療制度）運用保守業者、情報共有基盤（基盤上で稼働しているシステムを含む）運用保守業者等との調整などを実施すること。

調整に必要な情報の取得については本市が仲介するので、必要事項があれば、申し出ること。

※中規模以上とは、同時最大稼働人数が 30 人以上のプロジェクトとする。

※体制の変更など、提案書に記載した技術水準に変更がある場合、その変更によりプロジェクト遂行上の問題が生じないことを本市が確認した上で、変更することができる。

6　納品物

申請管理システム開発終了時に納めるべき納品物を、表 6－1に示す。

（1）情報資産一式

導入モジュール（プログラムソースコード含む）など、システム稼働に必要な情報資産一式を納品すること。

（2）開発ドキュメント

要件分析、基本設計、開発の各プロセスの成果物として納品すること。

（3）本書要件に定めたドキュメント

本書各項で要件として定めたドキュメントを納品すること。作成・納品すべきドキュメントの考え方については（4）を参照すること。なお、その他、プロジェクトを進める中で作成した本市が必要とする中間ドキュメントや、本市から収集したドキュメント類についても、取りまとめ納品すること。納品物は、管理・運用・検索のしやすさを考慮し作成すること。納品方法（紙、データでの納品など）や部数などについては、本市と協議の上確定すること。

表 6－1　納品物一覧

No	成果物	成果物内訳	概要
1	プロジェクト計画書	プロジェクト計画書	プロジェクトの概要、プロジェクトの進め方、全体スケジュール、フェーズ毎の体制図、役割分担、品質に対する取り組み、レビュー計画リスク管理方法、変更管理方法などを記載したもの
2	プロジェクト管理手順書	プロジェクト管理手順書	進捗管理、変更管理、構成管理などの手順を記載したもの
3	アーキテクチャ設計書	アーキテクチャ設計書	情報共有基盤に対する SSO 実現方式、データアクセス方式、データ連携方式、機能提供形態(EJB, WebService, DI コンテナなど)などの方式に関して記載したもの
4	プロジェクト進捗報告書	プロジェクト進捗報告書	プロジェクトで実施されているタスクの進捗状況、遅延理由、課題、リスクなどについて説明したもの

5	レビュー結果報告書	レビュー結果報告書	レビューを実施した際にレビュー結果、レビューで発見された欠陥、レビューで発見された課題などについて記載したもの
6	プロジェクト完了報告書兼運用引き継ぎ資料	プロジェクト完了報告書兼運用引き継ぎ資料	システムの導入、研修など全ての作業が完了し、運用業者及び保守業者に引き継ぐために、システムの導入状況、運用保守業務への引き継ぎ事項、残課題などについて記載したもの
7	対象業務一覧表	対象業務一覧表	プロジェクトの対象とする業務を記載したもの
8	業務フロー図	業務フロー図(To-Be)	改善後の業務の流れを図示したもの
9	業務ルール	業務ルール(To-Be)	改善後の業務の詳細なルールを記載したもの
10	用語集	用語集	プロジェクトに出てくる用語とその意味を記載したもの
11	画面設計書	画面一覧(To-Be)	構築するシステムの画面の一覧を記載したもの
		画面遷移図	画面の遷移を記載したもの
		画面項目定義書	画面項目の説明（桁数や書式）を記載したもの
12	帳票設計書	帳票一覧(To-Be)	構築するシステムで出力する帳票の一覧を記載したもの
		帳票レイアウト設計書	帳票のレイアウトを記載したもの
		帳票項目定義書	帳票項目の説明（桁数や書式）を記載したもの
13	データベース設計書	論理 ERD	論理データモデルを表す。物理 ERD を作成する前のものを納品すればよい。
		CRUD 図	機能毎に各テーブルに対するテーブル操作の種類を一覧で示したもの
		物理 ERD	物理データモデルを表す。
		テーブル、インデックス及びビュー一覧	テーブル、インデックス及びビューを一覧にしたもの
		テーブル定義	物理テーブルの定義（論理名、物理名、型、桁数、説明など）を記載したもの
		インデックス定義	インデックスの説明及び定義を記載したもの
		ビュー定義	物理テーブルから作成される仮想的なテーブルを定義したもの
		コード定義	コードの値及び説明を記載したもの
		ユーザ定義	データベーススキーマの説明を記載したもの

		データベース環境定義	データベースのパラメータや表領域の定義などを記載したもの
		制約定義	参照整合性制約などのデータベースで定義できる制約を記載したもの
		データベーススクリプト	DDL などのデータベースを構築するためのスクリプト一式
14	ユースケース一覧	ユースケース一覧(To-Be)	構築するシステムにおける、業務を実施する単位での機能の一覧を記載したもの
15	ユースケース記述	ユースケース記述	システムの振る舞いを、システムに詳しくない利用者が理解できる内容で記述したもの
16	全体システム構成図	全体システム構成図(To-Be)	構築するシステムと外部システムとの関連を示したもの
17	非機能要件定義書	非機能要件定義書	稼働条件、セキュリティ、移行、運用等に係る要件を示したもの
18	業務共通基盤設計書	業務共通機能一覧	業務共通機能の一覧を記載したもの
19	外部インタフェース設計書	外部インタフェース一覧(To-Be)	構築するシステムにおける外部インタフェースの一覧を記載したもの
		外部インタフェース定義	外部インタフェースの定義（フォーマット、連携頻度、連携方法など）を記載したもの
20	バッチ設計書	バッチスケジュール	バッチの実行スケジュール、関連を記載したもの
		バッチ一覧	バッチ処理の一覧を記載したもの
		バッチ定義	バッチ処理の説明を記載したもの。内部ファイルを作成する場合は、その内容も記載すること
21	導入モジュール	アプリケーションサーバ・パラメータ定義	アプリケーションサーバの設定パラメータの説明を記載したもの
		コンフィグレーションファイル	アプリケーションで使用する設定ファイル（メッセージファイルを含む）
		ソースコード	アプリケーションのソースコード一式
		デプロイスクリプト	アプリケーションサーバにアプリケーションをデプロイするために使用するスクリプト
		インストールスクリプト	アプリケーション(PL/SQL, Java など)のインストールを行うためのスクリプト

		単体テストソースコード	単体テストのテストスクリプト(xUnit)
		実行モジュール	実行モジュール一式
		インストール手順書	アプリケーション(PL/SQL, Java など)のインストールの手順を記載したもの
		バッチ処理実行スクリプト	バッチ処理を実行するためのスクリプト
22	結合テスト計画書	結合テスト計画書	結合テストの計画を記載したもの
23	結合テスト結果報告書	結合テスト結果報告書	結合テストの仕様・結果を記載したもの
24	負荷テスト計画書	負荷テスト計画書	負荷テストの計画を記載したもの
25	負荷テストスクリプト	負荷テストスクリプト	負荷テストを行うためのスクリプト
26	負荷テストデータ	負荷テストデータ	負荷テストを行うためのテストデータ
27	負荷テスト結果報告書	負荷テスト結果報告書	負荷テストの仕様・結果を記載したもの
28	システムテスト計画書	システムテスト計画書	システムテストの計画を記載したもの
29	システムテスト結果報告書	システムテスト結果報告書	システムテストの仕様と結果を記載したもの
30	システムテストスクリプト	システムテストスクリプト	システムテストデータの導入スクリプト
31	システムテストデータ	システムテストデータ	システムテストを行うためのテストデータ
32	受入テスト仕様書	受入テスト仕様書	受入テストを行うための仕様を記載したもの
33	リリース手順書	リリース手順書	申請管理システムをリリースするための具体的な手順を記載したもの
34	運用ドキュメント	運用ドキュメント	システム運用に必要な事項を記載したもの。
35	研修計画書	研修計画書	研修内容、研修スケジュールなどを文書化したもの
36	ユーザーズマニュアル	ユーザーズマニュアル	システム（オフラインを含む）の利用方法などを示したマニュアル（共通研修用及び個別研修用のテキストの内容を含む）
37	パッケージ活用説明書	パッケージ活用説明書	申請管理システム構築にあたり、パッケージを適用した機能をマトリックス形式などで説明したもの
38	試験稼働計画書	試験稼働計画書	試験稼働の計画を記載したもの
39	試験稼働結果報告書	試験稼働結果報告書	試験稼働の仕様と結果を記載したもの

（4）作成・納品すべきドキュメントの選定

（3）に示したドキュメントの中には、パッケージソフトウェアに関するドキュメントとして、開発業者側で既に作成し、保有しているものも含まれていると想定される。

本市では、主に以下のような目的のために、開発業者が保有するドキュメントについても開示を求めるものである。

- 情報共有基盤上で申請管理システムの運用を実施するため
- 制度改正等の保守実施範囲を明確化するため
- 本システムがライフサイクルを終え、さらに次の申請管理システムを再構築する際、本システムのシステム化範囲、実装された業務内容、保有しているデータ等、本システムの分析とデータ移行・システム移行に必要な情報を得るため開発業者が保有するドキュメントであっても最低限開示されることを想定しているものについて表 6-2に示す。

また、パッケージソフトウェアの導入に際し（3）に示したドキュメントの中で作成を必要としないものもあると想定される。

どのドキュメントを作成し、納品する必要があるかについては、案を本市に提示の上、本市担当者と調整して決定すること。

表 6-2 開示される開発業者所有ドキュメント（調整前）

No	成果物	成果物内訳	利用目的、代替可能条件
8	業務フロー図	業務フロー図(To-Be)	業務の流れにおけるシステム利用範囲を俯瞰的に把握するため
9	業務ルール	業務ルール(To-Be)	システムに実装されている処理の根拠を把握するため
11	画面設計書	画面一覧(To-Be)	画面により入出力されるデータを把握し、本システムの分析に資するため
		画面項目定義書	
12	帳票設計書	帳票一覧(To-Be)	帳票に出力されるデータを把握し、本システムの分析に資するため
		帳票レイアウト設計書	
		帳票項目定義書	
13	データベース設計書	論理 ERD	保有するデータの項目及び保有方法を把握し、データベースの運用及びデータ移行に資するため 【代替可能条件】 テーブル定義、ビュー定義については、EUC 機能にて、全てのテーブル及びビューを対象に、テーブル名・ビュー名及び列名が論理名称（日本語名称）で確認でき、テーブル内のデータを抽出できる場合には不要 コード定義については、EUC 機能にてコード値とその内容が確認できる場合には不要
		物理 ERD	
		テーブル、インデックス及びビュー一覧	
		テーブル定義	
		ビュー定義	
		コード定義	

14	ユースケース一覧	ユースケース一覧(To-Be)	システムに実装されている処理内容を把握し、保守範囲の明確化及び本システムの分析に資するため 【代替可能条件】処理内容が画面設計書、帳票設計書で把握できる場合には不要
15	ユースケース記述	ユースケース記述	
18	外部インタフェース設計書	外部インタフェース一覧 (To-Be)	他システムとの連携内容について把握し、本システムの分析に資するため
		外部インタフェース定義書	

（注）No、成果物、成果物内訳は、表 6－1　納品物一覧の各項目と一致させている。

（5） 納品物の著作権について

納品物の著作権については、「委託契約約款」第５条及び「電子計算機処理等の契約に関する情報取扱特記事項」第 14 条に定める内容に従うこと。疑義がある場合には本市担当者と協議し、双方合意の上で納品を行うこと。

7　その他補足事項

（1） 委託期間内（開発期間）における制度改正などの仕様変更の対応

委託期間内において制度改正などにより仕様の変更が発生した場合は、本市と協議の上、本業務の委託範囲内として対応すること。なお、スケジュールや改修規模などの制約により対応が困難な場合は、運用による代替手段などを示すこと。

（2） 契約約款について

本書に定める事項の他「委託契約約款」「電子計算機処理等の契約に関する情報取扱特記事項」及び「個人情報取扱特記事項」に定める事項に従い、業務を履行すること。

情報共有基盤　機能概要説明書

初版(1.0)　2010 年 10 月 29 日

改訂版(3.0)　2018 年 10 月 01 日

横浜市総務局　住民情報システム課

改訂履歴

版	年月日	氏名	内容
1.0	2010/10/29	緑川	新規作成
1.1	2010/11/12	緑川	別紙資料の追加 AIST 包括フレームワークの概要 個人基本情報の住民状態遷移 公開インタフェース 誤字修正
2.0	2012/12/01	緑川	３（２）住民記録情報　住基法改正の内容を反映 ３（６）介護保険情報　追加 ３（７）生活保護情報　追加 ５　基盤ポータル　画面イメージを追加 ６　運用基盤　全面改訂 ７　監視基盤　全面改訂 ８（２）端末管理　追加、イ　ウィルス対策、ウ　USB メモリ制限　を１２　基盤ネットワーク　から移動 １０（４）共有フォルダ　追加 １２（２）ネットワークサービスの概要　改訂
2.1	2013/04/18	緑川	２（１）基盤システム構築の背景　の内容を時点修正
3.0	2018/10/01	野牧	仮想基盤の運用開始及び基盤システムの移行に伴い全面改訂 ドキュメント名を「情報共有基盤システム　機能概要説明書」から「情報共有基盤　機能概要説明書」に変更。

目次

1　はじめに

1.1　本書の目的

本書では、横浜市の情報共有基盤及び、その構成要素である情報共有基盤システム（以下、「基盤システム」という。）、情報共有基盤システム仮想基盤（以下、「仮想基盤」という。）、情報共有基盤ネットワーク（以下、「基盤ネットワーク」という。）が持つ機能について概要を説明する。

情報共有基盤を利用しようとする業務システムや利用者、どのようにすれば情報共有基盤を利用できるかを示すことで、業務システムの担当者や利用者が情報共有基盤への理解を深めることが目的である。

1.2　対象読者

本書は、情報共有基盤を利用する業務システムの担当者、開発事業者、運用事業者及び保守事業者を対象とする。

2　情報共有基盤の概要

2.1　情報共有基盤構築の経緯

本市ではこれまでに様々な業務のシステムが構築されてきたが、業務部門ごとに多種多様な規格や機能をもつシステムが導入されたため、各システム間のデータ連携や機器の共有等が困難という課題が生じていた。

こうした状況を改善するため、複数のシステムで共通で利用・連携できるプラットフォームである情報共有基盤システムを平成 23 年度に整備し、ハードウェア、ソフトウェア、データの共有による全体最適化を進めている。

また、平成 28 年度には仮想化技術を活用した仮想化サーバ基盤である情報共有基盤システム仮想基盤を整備し、翌年度には基盤システムを利用している各業務システムの機器更新において仮想基盤への受け入れを実施した。

平成 30 年 6 月現在、情報共有基盤を利用する主な業務システムは以下の通りである。

- 福祉保健システム（平成 24 年 1 月　稼働）
- 障害福祉システム（平成 24 年 1 月　稼働）
- 母子保健システム（平成 25 年 3 月　稼働）
- 生活保護システム（平成 26 年 1 月　稼働）
- 統合番号連携システム（平成 28 年 1 月　稼働）
- 国民健康保険料収納対策支援システム（平成 29 年 5 月　稼働）
- 顔認証システム（平成 29 月 6 月　稼働）

2.2　情報共有基盤の目標

情報共有基盤の目標は、業務システムが情報共有基盤を用いて構築されることで、各業務においてコスト縮減及び信頼され効率的な行政運営を実現することである。具体的には、下記に示す 4 つの目標を掲げている。

(1)　業務の簡素・効率化の実現

複数の業務システムが共通して利用できる住民情報のデータベースを整備し、また、データ連携の仕組みを整備することで、システム個別では実現が難しかったシステム間の情報伝達が正確かつ

迅速にされるようにし、市民サービスを向上させる。

(2)　情報化関連経費の縮減

複数システムでのハードウェア及びインフラの共有、利用技術の統一によるシステム開発及び運用の効率化により、システムの機器調達・構築・運用に要する経費の縮減を図る。

(3)　業務所管部門部署の管理負担の軽減

基盤システム所管部門で一括して管理するサーバ・ネットワーク・端末統制基盤を利用することで、業務システム所管部門の管理負担の軽減を図る。

(4)　ベンダロックインの排除

特定の事業者に依存しない基礎技術を採用することで、情報共有基盤を利用する業務システムの構築に複数の事業者が参画できるようにする。

2.3　AIST 包括フレームワーク

前述のベンダロックインの排除を達成するためには、特定の事業者に依存しない基礎技術を使用して情報共有基盤を構築する必要がある。この基礎技術として情報共有基盤では国立研究開発法人　産業技術総合研究所が開発した AIST 包括フレームワークを用いている。

AIST 包括フレームワークにおけるフレームワークとは、プロセスや成果物作成ルールを中心とし、Java での Web アプリケーション開発のソフトウェア基盤と開発手法の指針を示すガイドラインなどを含む、開発活動を進める上での包括的な環境全体を提供するものである。AIST 包括フレームワークは、一般的なソフトウェア開発工程のうち、要件分析から受入テストまでを対象とし、各工程の手順を定めるプロセス、開発の共通ルールである開発標準、開発を支援するツールを提供する基盤フレームワークから構成されている。

この AIST 包括フレームワークを本市向けにカスタマイズしたものが情報共有基盤に適用されている。

2.4　情報共有基盤が提供するサービス

情報共有基盤は、以下に示すサービスを提供する。

(1)　基盤ネットワーク

情報共有基盤端末や業務システムサーバで利用できる全庁的なネットワークである。また、各種ネットワークサービスを提供している。

本書の 4　情報共有基盤ネットワークで説明している。

(2)　端末統制基盤（情報共有基盤ドメイン）

情報共有基盤端末やサーバの運用・管理のため、資産管理、セキュリティ対策、ドメインサービス、資源配布等の機能を提供している。

本章の 5　基盤端末で説明している。

(3)　仮想基盤

業務システム用の仮想サーバ及び仮想ネットワークを提供する仮想化サーバ基盤である。また、仮想基盤上の業務システム向けの運用・監視、パフォーマンス管理、バックアップ機能を提供している。

本書の 6　仮想基盤で説明している。

(4)　基盤システム機能

業務システムの構築・運用支援サービスとして、シングルサインオン（SSO)、ポータル、基盤データベース、データ連携等の機能を提供している。

本書の 7　SSO システム　～　11　データ連携基盤で説明している。

基盤システムが持つ機能について、図 2-1　情報共有基盤機能構成概要図に示す。

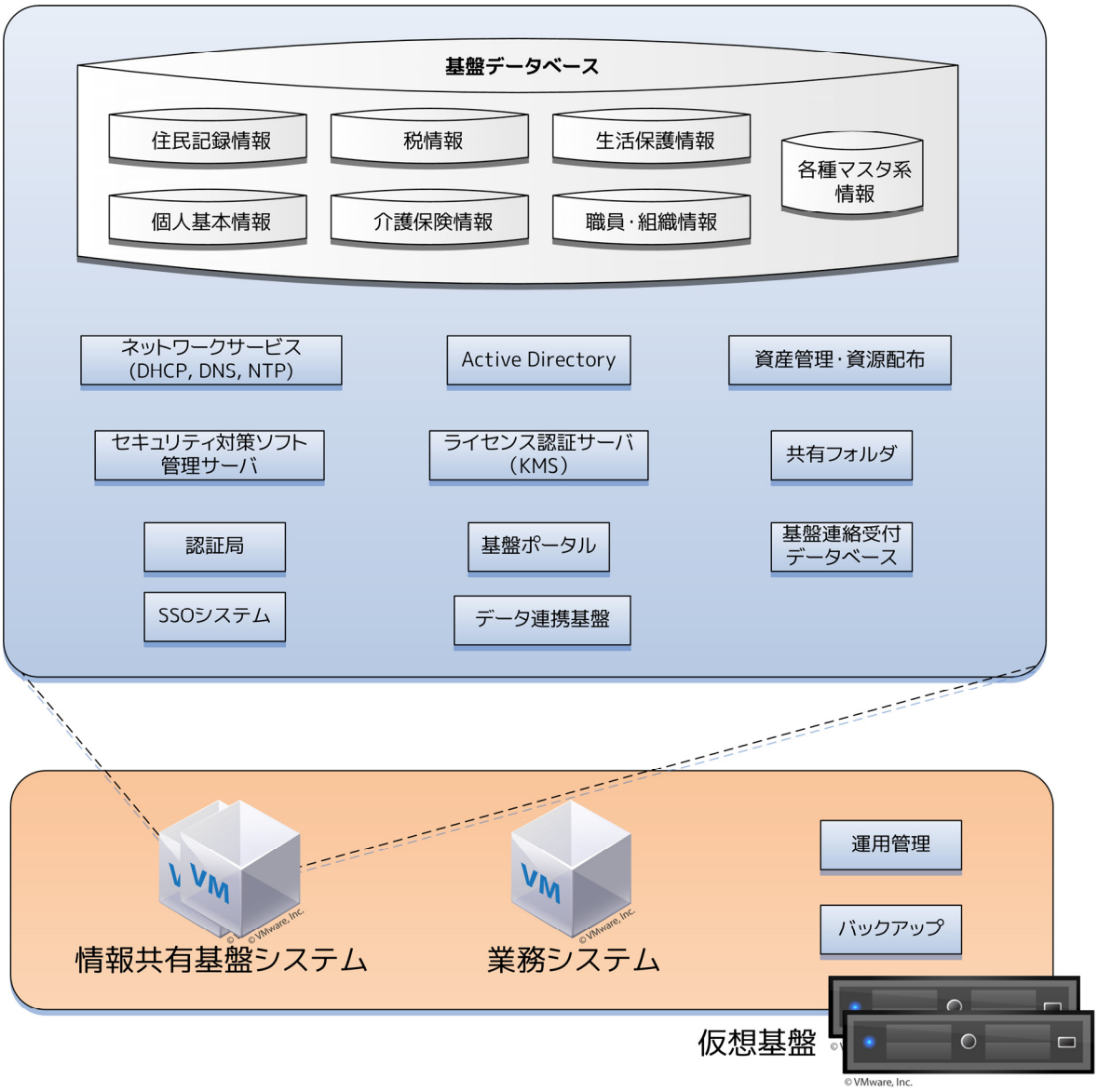


図 2-1　情報共有基盤機能構成概要図

2.5　情報共有基盤の機器構成

情報共有基盤の機器構成の概要を図 2-2　情報共有基盤機器構成図に示す。

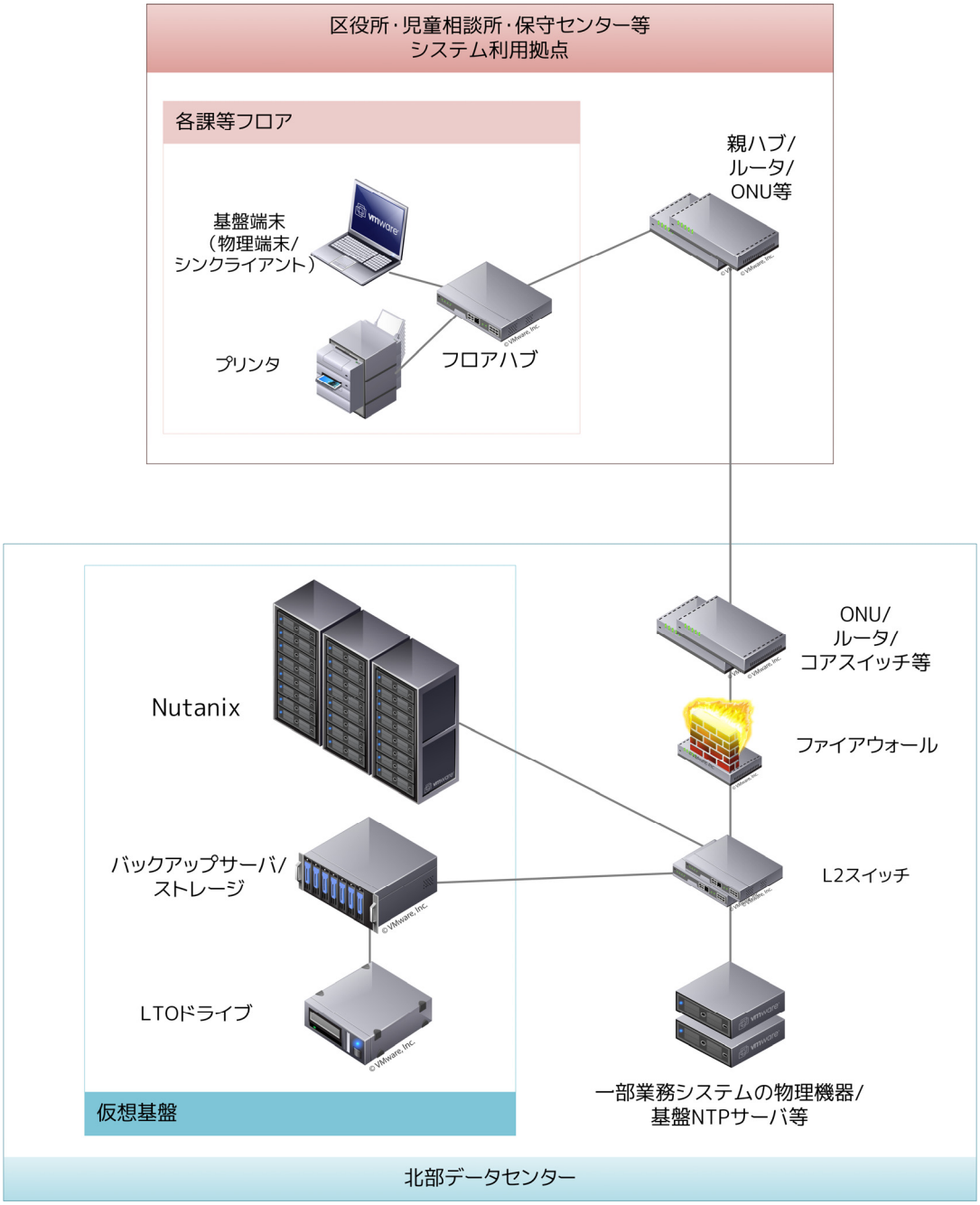


図 2-2　情報共有基盤機器構成図

3　業務システムへの基盤の適用

業務システムが情報共有基盤を利用する際は、情報共有基盤のインフラや機能の全てを必ずしも利用する必要はなく、用途に応じて基盤が提供するインフラ・機能を組み合わせて利用することができる。

現在稼働している代表的な業務システムが採用する、情報共有基盤の構成要素の組み合わせパターンを、表 3-1　情報共有基盤の利用パターンに示す。

表 3-1　情報共有基盤の利用パターン

パターン	ネットワーク	基盤端末	仮想基盤	基盤機能	説明	システム例
ネットワークのみ	使用する	使用しない	使用しない	使用しない	ネットワークのみ使用し、端末・サーバを別途準備する。	統合番号連携システム用端末仮想化環境
ネットワーク・端末のみ	使用する	使用する	使用しない	使用しない	基盤端末を使用し、別途準備したサーバを使用する。	被災者支援システム
ネットワーク・サーバ・SSO のみ	使用する	使用しない	使用する	使用する	基盤機能は SSO のみ使用する。端末は別途準備したシンクライアントを利用する。	国民健康保険料収納対策支援システム
インフラのみ使用する	使用する	使用する	使用する	使用しない	基盤端末、仮想サーバを使用する。基盤機能を使用しない。	顔認証システム
全て使用する	使用する	使用する	使用する	使用する	全ての構成要素を使用し、基盤システムと連携する。	福祉保健システム 障害福祉システム 母子保健システム 生活保護システム 統合番号連携システム

4　情報共有基盤ネットワーク

4.1　情報共有基盤ネットワークの概要

情報共有基盤ネットワーク（以下、「基盤ネットワーク」という。）は、市庁舎や区役所等のシステム利用拠点と北部データセンター（以下、「北部 DC」という。）を結ぶ、全庁的なネットワークである。実態は、住民記録システム等の基幹システム用ネットワークのセグメントの一種である。

基盤ネットワークは広域イーサネットを利用したプライベートな TCP/IP ネットワークであり、インターネットには接続していない。また、地方公共団体間を接続する総合行政ネットワーク（LGWAN）との通信が可能である。

基盤ネットワークの責任分界点は、システム利用拠点の執務室内に設置された管理・監視機能付きのスイッチングハブ（以下、「フロアハブ」という。）であり、業務システムのサーバからフロアハブまでの通信は基盤システム所管部門が管理する。フロアハブから以降の小規模なハブ、端末・プリンタまでの接続については、業務システムの所管部門や拠点の利用者が管理する。

また、各業務システムや基盤端末がネットワークを利用するために必要な各種サービスも情報共有基盤から提供される。

基盤ネットワークの拠点を表 4-1　基盤ネットワークの拠点に示す。

表 4-1　基盤ネットワークの拠点

拠点名	主な役割
北部データセンター	サーバ設置拠点
保守センター	システム開発・運用拠点
市庁舎	利用者拠点
市庁舎周辺ビル	利用者拠点
１８区役所	利用者拠点
４児童相談所	利用者拠点
障害者更生相談所	利用者拠点

基盤ネットワークの構成の概要を図 4-1　情報共有基盤ネットワーク概要図に示す。

なお、各機器は基本的に冗長構成になっているが、図上の表記は省略している。また、システム利用拠点や業務システムの要件に合わせた構成になっているため、一部機器構成が異なる部分がある。

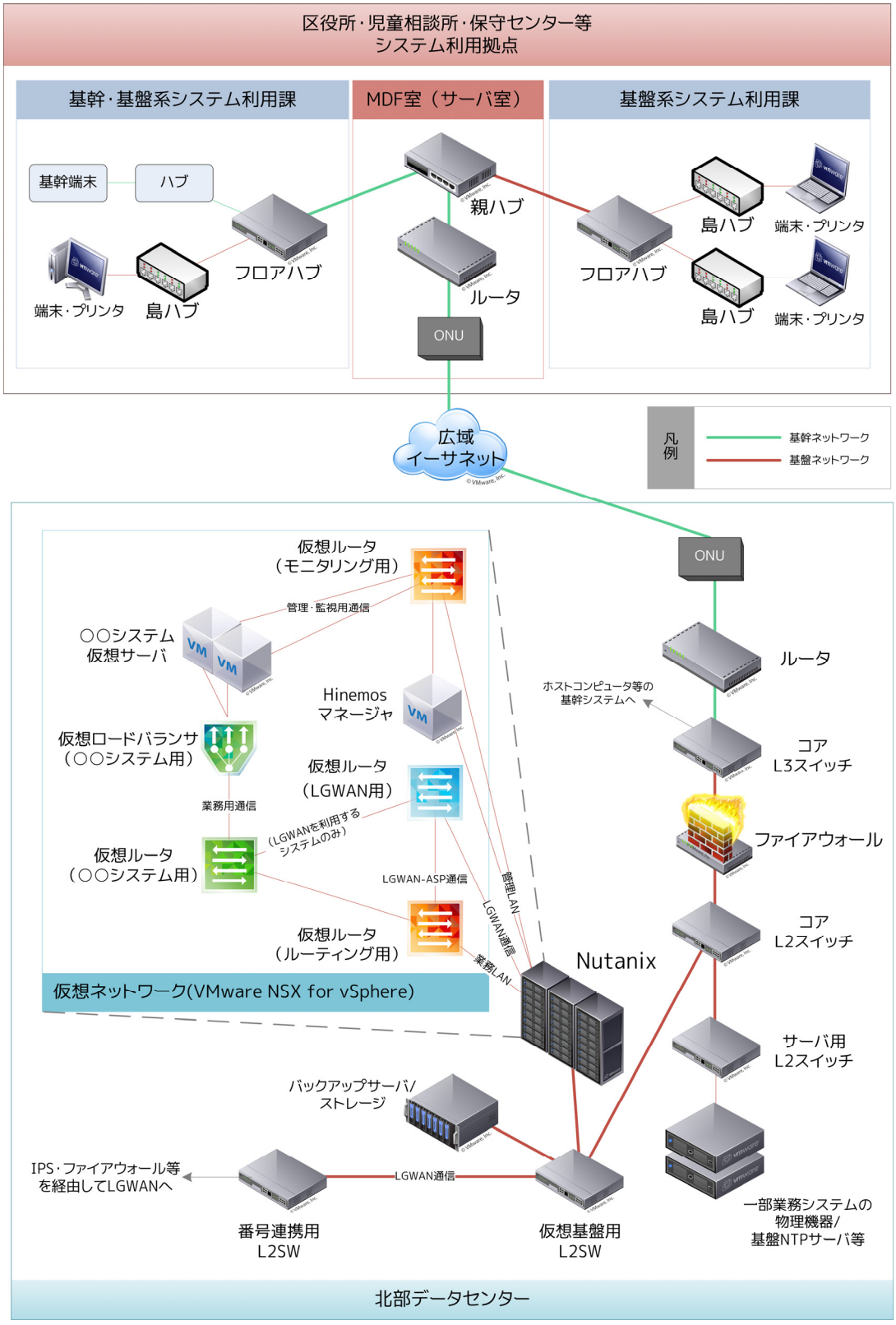


図 4-1　情報共有基盤ネットワーク概要図

4.2　ネットワークサービスの概要

情報共有基盤は、基盤ネットワークを利用する各業務システム及び端末向けに、以下のサービスを提供する。

4.2.1　情報共有基盤ドメイン

情報共有基盤では、Active Directory ドメインサービスによって icbs.kiban ドメインを運用している。icbs.kiban ドメインは単一のドメインであり、フォレスト内に他のドメインは存在しない。基盤端末は icbs.kiban ドメインに参加するため、端末の FQDN には icbs.kiban のドメイン名が使用される。

Active Directory で使用する機能については 5.2.1　Active Directory で説明する。

4.2.2　DHCP

端末・プリンタ等の機器に設定される IP アドレス、サブネットマスク、デフォルトゲートウェイ、機器が利用する DNS サーバの IP アドレス情報は、情報共有基盤の DHCP サーバから配布される。

DHCP サーバには、基盤システム所管部門に対して事前に利用申請をした機器の MAC アドレスと IP アドレスの組があらかじめ登録されている。機器側で DHCP を利用する設定にすることで、常にあらかじめ決まった IP アドレスが設定されるようになる。そのため、機器の故障により基板を交換し、MAC アドレスが変更になった場合は、基盤システム所管部門に登録変更の申請が必要である。なお、DHCP サーバは、登録されていない MAC アドレスを持つ機器に対しては IP アドレスを払い出さない。

また、機器を別の区役所に移設するなど、ネットワークセグメントを越えて機器を移設する場合は、機器の IP アドレスが変更になるため、基盤システム所管部門に登録変更の申請が必要である。

DHCP サーバは、北部 DC の Active Directory サーバ（正/副）と同居し、Active-Active 構成で冗長化されている。端末・プリンタ等の機器は、DHCP サーバ（正/副）に IP アドレス払い出しの要求を送信し、先に応答したサーバから IP アドレスの払い出しを受ける。

4.2.3　DNS

基盤 DNS サーバは、情報共有基盤ドメイン（icbs.kiban）の FQDN の名前解決を行う。

DNS サーバには、業務システムからの依頼により、サーバの正引き/逆引き/CNAME 等のレコー

ドが登録可能である。基盤ドメインに参加した端末・サーバのレコードには、DNS サーバの動的更新設定により、コンピューター名の FQDN と設定された IP アドレスの対応が自動的に設定される。

DNS サーバは、北部 DC の Active Directory サーバ（正/副）と同居し、Active-Active 構成で冗長化されている。

4.2.4 NTP

情報共有基盤では、基盤ネットワーク上の機器の時刻同期を行うために NTP サービスを運用している。

NTP サービスは、南部情報システムセンタの NTP サーバ（GPS タイプ）、北部 DC の NTP サーバ（セカンダリサーバタイプ）、Active Directory サーバ（正/副）によって提供されている。基盤 NTP サービスの階層構造を表 4-2　基盤 NTP サービスの階層構造に示す。どの機器のサービスを利用するかは、機器の設置場所と階層を勘案して選択する。

表 4-2　基盤 NTP サービスの階層構造

階層	サービス提供機器
Stratum 0	（米国国防総省 GPS 衛星）
Stratum 1	保守センター　NTP サーバ
Stratum 2	北部データセンター　NTP サーバ
Stratum 3	Active Directory サーバ（正/副）

4.3 ネットワークセキュリティ

外部から持ち込まれた PC 等が勝手に接続され、データを窃取されるようなことがないように、許可のない端末は基盤ネットワークに接続できないような構成にしている。新たな端末を使用する場合には、基盤システム所管部門に対し申請を行い、許可を得る必要がある。

4.3.1 機器接続制御（MAC アドレスフィルタリング）

4.2.2　DHCP に記載のとおり、基盤 DHCP サーバは未登録の MAC アドレスの機器に IP アドレスを払い出さないため、未登録の機器には適切な IP アドレスが設定されず、ネットワークに接続できない。しかし、機器に IP アドレスを手動設定することで管理外の機器が基盤ネットワークに接続できてしまう可能性がある。そこで、IP アドレスが手動設定された機器の接続を防止するため、拠点側のスイッチングハブには DHCP スヌーピングに対応しているものを導入している。

DHCP スヌーピングとは、スイッチングハブが、機器（DHCP クライアント）と DHCP サーバの通信内容をのぞき見（snooping）し、DHCP サーバから IP アドレスの払い出しを受けていないにもかかわらず通信しようとする機器（IP アドレスが固定設定になっている等）のネットワーク接続を遮断する機能である。

上記の基盤 DHCP サーバの設定と DHCP スヌーピング機能の組み合わせにより、基盤ネットワークにはあらかじめ申請を受けてサーバ側に登録された MAC アドレスを持つ機器しか接続できないようになっているため、実質として、MAC アドレスフィルタリングによる機器接続制御が行われている。

4.3.2　基盤ファイアウォール

サーバ設置拠点である北部 DC には、端末側のネットワークとサーバの境界にファイアウォールを設置している。基盤ファイアウォールは、ファイアウォールを通過しようとするパケットの内容を確認し、アプリケーションレベルで通信を制御することが可能である。

基盤ファイアウォールは、全ての通信を禁止し、必要な通信のみを通過させるホワイトリスト方式を採用している。業務システムが北部 DC 内の基盤ネットワーク以外のセグメント（区役所の端末等）と通信を行う場合は、事前に業務システムの通信要件を整理し、基盤システム所管部門へ提出することで通信の許可を申請する必要がある。

なお、仮想基盤内には仮想マシンごとにファイアウォールを配置することで、仮想基盤上に存在する業務システム間の通信を制限する、VMware NSX for vSphere による分散ファイアウォールが存在する。分散ファイアウォールについては 6.4.1　分散ファイアウォールで述べる。

4.3.3　認証局

基盤端末が業務システムと HTTPS 通信を行うために、ルート証明書及びサーバ証明書（自己証明書）を発行する OpenSSL による認証局を構成管理サーバ上で運用している。

ルート証明書は情報共有基盤ドメインのグループポリシーにより配布され、基盤の認証局は信頼されたルート証明機関として全基盤端末に登録される。各業務システムは、基盤の認証局にサーバ証明書の発行を依頼することができる。発行を依頼する際は、業務システムの FQDN のみを提示すればよい。発行に必要な秘密鍵・公開鍵、証明書署名要求（CSR）は認証局側で用意する。作成されたサーバ証明書は、証明書本体と秘密鍵のペアで各業務システムに受け渡す。このペアは原則として仮想基盤の仮想ロードバランサ上のみで用いるため、利用方法については 6.4.2　仮想ロード

バランサを参照すること。

4.4　LGWAN 接続

基盤ネットワークは総合行政ネットワーク（LGWAN）に接続しているため、拠点の端末や仮想基盤内の仮想マシンから LGWAN-ASP サービスや自治体中間サーバー・プラットフォームにアクセス可能である。

LGWAN への途中経路には、北部 DC の基盤ルータ及びファイアウォール、仮想基盤の仮想ルータ、侵入防止システム（IPS）、番号連携用ファイアウォール、LGWAN 用ファイアウォールが存在するため、新たに LGWAN と通信する際は各機器の管理部門との調整が必要である。

5　基盤端末

5.1　情報共有基盤端末の概要

基盤ネットワークに接続し、情報共有基盤や業務システムを利用する端末を情報共有基盤端末（以下、「基盤端末」という。）という。

情報共有基盤では、基盤端末に対して統一した端末・ソフトウェア調達仕様、端末設定手順、端末統制（ポリシー配信）、セキュリティ対策、資産管理、資源配布の機能を提供するサービスを運用している。基盤端末の管理責任者は各業務システムの所管部門及び外部サービス（中間サーバー、LGWAN-ASP 等）を利用する事業の所管部門（以下、「各所管部門」という。）である。各所管部門は、情報共有基盤が提供する統一した設定と競合しない範囲で自由に端末の設定変更や、ソフトウェアのインストールを実施できる。

基盤端末を利用する各所管部門は、端末台数に応じた情報共有基盤利用料を負担する必要がある。

本章では、情報共有基盤が提供する基盤端末の管理機能について説明する。これらの一部のサービスはサーバでも利用可能である。

5.2　端末・ユーザー管理

5.2.1　Active Directory の運用

情報共有基盤では独自のドメイン（icbs.kiban）を構築し、その運用に Active Directory を用いている。原則として全ての端末がこの独自ドメインに参加している。サーバのドメインへの参加は任意である。

ドメインに参加すると、ドメインユーザー及びグループが利用可能になる。基盤端末には、利用課ごとに割り当てたドメインユーザーを利用してログオンする。このドメインユーザーは Domain Users グループに属する標準ユーザーである。各所管部門が端末の設定変更等、管理者権限を必要とする作業を行う場合は、端末のセットアップ時に設定した、各所管部門で決めたパスワードを持つローカル管理者ユーザーを利用する。

Domain Users グループとは別に、業務システムごとに少なくとも１つのドメイングループを払い出す。後述する共有フォルダの利用権限は、原則としてこのグループに対して設定し、ユーザーには設定しない。これは、機構改革等による権限設定変更作業を必要最小限にするためである。

共有フォルダのアクセス権限を細かく制御したいなどの理由でドメイングループを追加したい

場合は、基盤システム所管部門に依頼する。

ドメインユーザーで端末にログオンした場合、端末には情報共有基盤のグループポリシーが適用される。グループポリシーにより、全基盤端末には基盤認証局のルート証明書、OS や Internet Explorer の設定等、一元的に管理された設定が適用される。また、依頼により、任意のドメインユーザーに対して、業務システム側が作成した任意のログオンスクリプトを実行させることが可能である。

5.2.2　資産管理

各所管部門は、IT 資産管理ソフトウェアである PalletControl（(株) JAL インフォテック）による資産管理機能を利用できる。

全基盤端末には PalletControl のクライアントソフトウェアがインストールされている。このクライアントソフトウェアは、Windows のログオン時に毎回 PalletControl サーバに対して資産情報を送信する。取得する主な資産情報を以下に示す。

- コンピューター名、ログオンユーザー名
- CPU 機種名・動作周波数（GHz)、メモリーサイズ（GB）
- IP アドレス、MAC アドレス
- Windows、Internet Explorer バージョン
- セキュリティパッチ適用状況
- インストール済みソフトウェア情報
- 登録済みプリンタ情報

5.2.3　ライセンス認証（KMS）

Windows クライアント OS 及び Microsoft Office 製品のライセンス認証作業の負担軽減のため、キー管理サービスの認証サーバ（KMS ホスト）を運用している。ボリュームライセンスの Windows 及び Office 製品は、DNS から KMS ホストを解決し、自動的にライセンス認証を行う仕組みになっている。

KMS ホストは、北部 DC の Active Directory サーバ（正/副）と同居し、Active-Active 構成で冗長化されている。端末は、基盤 DNS サーバに KMS ホストとして登録されている上記サーバの

FQDN に対して、定期的に OS と Office 製品のライセンス認証を要求する。Windows Server 用にはサービスを提供していないため、サーバ OS においては電話認証を行う必要がある。

5.2.4　端末の導入

各所管部門が基盤端末を新規に導入する場合は、それぞれの業務システムの要求を満たす仕様及び基盤システム所管部門が用意する「基盤端末仕様書案」の仕様を満たした端末を調達する。また、「基盤端末に必要なソフトウェア等について」のドキュメントに基づいたソフトウェアを調達する必要がある。「基盤端末仕様書案」では、基盤端末に導入必須とされているソフトウェアが適切に動作する最低限の仕様を示している。

各所管部門は、「基盤端末化設定手順書」に従って、コンピューター名、ローカル管理者ユーザー、ドメイン参加及び KMS 認証の設定、利用禁止デバイスの無効化、更新プログラムの適用、基盤端末に導入必須とされているソフトウェアのインストールを実施する。また、マイナンバー利用事務で利用する場合は、二要素認証ソフトウェアを導入する必要がある。なお、二要素認証ソフトウェアとして、基盤を利用する業務システムの１つである顔認証システムを利用することもできる。

新たに端末をネットワークに接続する際には、端末の MAC アドレスと設置場所を提示することで基盤システム所管部門へ申請する必要がある。DHCP により端末に設定される IP アドレス及び端末に設定するコンピューター名はこの申請受付完了時に払い出される。また、プリンタについても同様の運用を行っている。

5.3　資源配布

情報共有基盤では、基盤端末に必要な OS の更新プログラム、外字フォント・外字変換辞書等の、配布して適用する必要がある各種資源を配信する資源配布基盤を運用している。また、資源配布基盤を用いて、各所管部門が、自ら作成した任意のスクリプトの配布・実行、ファイル配信等を基盤システム所管部門に依頼することができる。資源配布基盤には、資産管理機能と同様に PalletControl を用いている。

5.3.1　外字の配信

情報共有基盤の基盤データベースには、住民記録や税務等の基幹システムから連携されたデータが格納されており、このデータには Windows 標準のフォントでは表示できない横浜市独自の外字が含まれている。資源配布基盤は、この外字のフォント及び外字変換辞書を端末に配信して適用することで、業務システムやアプリケーション上で外字の表示・入力ができるようにしている。

5.3.2　任意のスクリプトの配信

各所管部門は、基盤システム所管部門への依頼により、各所管部門が管理する端末に対して、自ら作成した任意のスクリプトの配布・実行ができる。例として、業務システム端末へのプリンタドライバインストール・プリンタ登録、業務システムのクライアントソフトウェアの更新（ファイル配信）、ソフトウェアの修正プログラムの適用等が依頼により実施されている。

PalletControl では製品の公式ホームページにて資源配布に用いるスクリプトのサンプルを配布している。配布されているスクリプトの例を以下に挙げる。

- Microsoft Office、Acrobat Reader 等のインストール
- 権限がない先へのファイルコピー
- レジストリ書き込み
- 管理者権限でファイル実行
- メッセージを表示

サンプルスクリプトにはバージョン 6.3 用のスクリプトとバージョン 8 用のスクリプトの 2 種類が存在するが、基盤端末に導入されている PalletControl8 にはバージョン 6.3 用のスクリプトを実行するためのアドオンが付属しているため、両バージョンのスクリプトを利用できる。

5.4　セキュリティ対策

基盤端末は個人情報を取り扱う業務で用いられることが多い。そのため、情報共有基盤では各種のセキュリティ対策ソフトウェアが利用できる仕組みを構築し、基盤ネットワーク上のすべての機器で統一したセキュリティ対策を実施している。

5.4.1　ウイルス対策

情報共有基盤は、全基盤端末及びサーバ向けに、ウイルス対策ソフトウェアが利用できる仕組みを提供している。各所管部門が端末にウイルス対策ソフトウェアをインストールした後、最新のウイルスパターンファイル及びウイルス検出エンジンは、基盤システムの検証用端末及び全業務システムの開発用サーバに先行して適用した上で、数日後に全端末・サーバに自動的に配布される。

クライアントソフトウェアを利用する業務システムで、特定のフォルダを常時監視（オンアクセススキャン）の対象外にする必要がある場合は、基盤システム所管部門へ申請が必要である。なお、Linux サーバの Oracle Database 領域についてはデフォルトで監視から除外されている。

ウイルス対策ソフトウェアには、基盤端末及び Windows Server 用に McAfee VirusScan Enterprise、Linux サーバ用に McAfee Endpoint Security for Linux を採用している。

5.4.2　データ書き出し制限

個人情報を含むデータが端末の外部に持ち出されることを防ぐため、端末で利用できる USB メモリを制限するデータ保護ソフトウェアを導入している。データ保護ソフトウェアには McAfee DLP Endpoint を採用している。

基盤端末では、基盤システム所管部門に事前に申請してシリアル番号等を登録された USB メモリ（USB 接続の外部記憶媒体）のみが利用できる。未登録の USB メモリは読み込みもできない。USB ポートを経由せず媒体に直接書き出し可能な内蔵カードリーダ等が端末に搭載されている場合は、端末導入時に各所管部門で無効化する必要がある。

内蔵光学ディスクドライブにおいては、グループポリシーで書き込みを制限しており、読み込みのみ可能である。

WPD デバイスについてはグループポリシーにより書き込みを制限している。

5.5　共有フォルダ

情報共有基盤では、業務システムの利用者向けに共有ファイルサーバ（共有フォルダ）を運用している。ファイルサーバ内には各業務システムの単位で共有フォルダが作成されており、業務システム毎に割り当てられた共有フォルダのみ利用可能なようにアクセス制御されている。各システムの共有フォルダへのアクセス権限の付与は、5.2.1　Active Directory の運用に記載したドメイングループに対して行う。

6　仮想基盤

6.1　仮想基盤の概要

情報共有基盤システム仮想基盤は、業務システム用の仮想サーバ及び仮想ネットワークを提供する仮想化サーバ基盤である。また、仮想基盤上のシステム向けの運用・監視及びバックアップ機能を提供している。

仮想基盤は、HCI アプライアンス・仮想化プラットフォーム・仮想ネットワークの組み合わせで構成されており、業務システムからの申請に基づき、仮想基盤保守事業者が仮想マシンを払い出すことで仮想サーバが利用可能になる。

仮想サーバの払い出しを受けた各所管部門は、利用リソースに応じた情報共有基盤利用料を負担する必要がある。

詳細については、別紙　「横浜市情報共有基盤システム仮想基盤　利用者ガイドライン」を参照すること。仮想基盤の利用イメージを図 6-1　仮想基盤の利用イメージに示す。

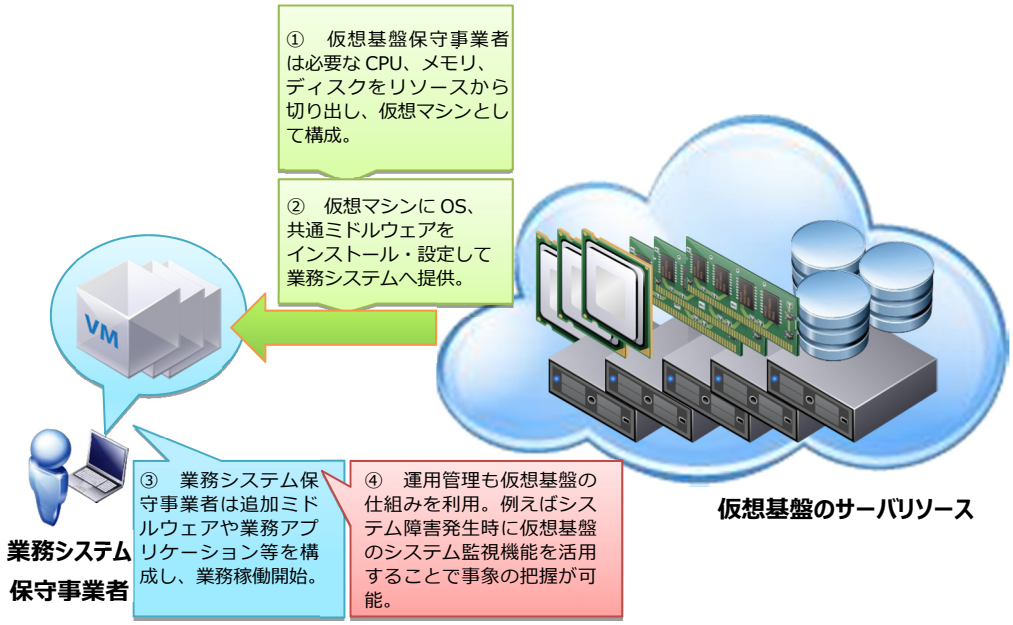


図 6-1　仮想基盤の利用イメージ

6.2　HCI アプライアンス（Nutanix）

仮想基盤の機器には、ハイパーコンバージドインフラストラクチャ（HCI）と呼ばれるアプライアンスである Nutanix（ニュータニックス）を採用している。Nutanix（HCI）は、機器自体は一般的なサーバと同様であるが、Nutanix 専用のソフトウェア（OS）を搭載して機器の制御を行うことで、本来は別途用意するストレージ機器を必要とせずにサーバ及びストレージの機能を利用可能にしている。また、Nutanix の専用 OS は複数の Nutanix 筐体を横断してまとめて制御可能であり、1 つの仮想マシンのデータを複数の筐体に分散して複製するため、仮想基盤においても高可用性を実現している。

注意点として、Nutanix で採用されている分散ファイルシステムの特性により、シングルスレッドかつブロッキング I/O 方式で実装した読み込み処理では、一般的なサーバの HDD に比べてスループットが低下する可能性がある。

6.3　仮想化プラットフォーム（VMware vSphere）

仮想基盤は、仮想化プラットフォームとして VMware vSphere を採用している。仮想マシンの動作環境としては、vSphere のハイパーバイザ製品である ESXi を使用している。ESXi を使用することで、複数の Nutanix 筐体をまとめたサーバ基盤上に、複数の仮想マシンを実行可能にしている。また、vCenter Server を用いて仮想マシンを管理しているため、各業務システムは vSphere Client を用いて仮想マシンの実行管理、スナップショットの取得、パフォーマンス監視等を行える。

仮想基盤では、vSphere が高可用性を保つ機能である vSphere HA（High Availability）を利用している。vSphere HA により、Nutanix または ESXi に障害が発生した際は、自動的に異なる Nutanix 上に仮想マシンを移動して再起動することで、業務システムの停止時間を最小限に抑えることができる。また、Nutanix や vSphere をメンテナンスする際は、手動で仮想マシンを無停止で別の Nutanix に移動することができる vMotion を利用して、基本的に業務システムを停止せずに仮想基盤側のメンテナンスを実行できる。

6.4　仮想ネットワーク（VMware NSX for vSphere）

仮想基盤上の仮想マシン間のネットワークは、ハイパーバイザ上に構築された VMware NSX for vSphere（以下、「NSX」という。）による仮想ネットワークである。仮想ネットワークでは、スイッチ、ファイアウォール、ルータ、ロードバランサ等のネットワークリソースも仮想化している。仮想基盤のスイッチ及びファイアウォールは、分散スイッチ・分散ファイアウォールと呼ばれるハイパーバイザの機能の一部として動作し、ルータ及びロードバランサについては、NSX Edge と呼ばれる

個々の仮想マシン（仮想アプライアンス）としてハイパーバイザ上に存在する。

仮想ネットワークでは、仮想マシンの役割（Web/AP サーバ、DB サーバ等）や構成（ロードバランサ、LGWAN 等の利用）を考慮して、用途ごとにネットワークセグメントを定義している。

6.4.1　分散ファイアウォール

仮想基盤では、仮想マシンの仮想 NIC（セグメント）ごとに NSX の分散ファイアウォールを適用している。

基盤ファイアウォール等の物理ファイアウォールは、ネットワークの境界（異なるセグメント同士の境界）にのみ設置可能で、同一セグメント上の通信を制御できない。一方、分散ファイアウォールはハイパーバイザの機能の一部として実装されるため、ネットワーク構成に関わらず、仮想マシンの全通信を制御できる。

仮想基盤の分散ファイアウォールは、基盤ファイアウォールと同様にホワイトリスト方式を採用しているため、仮想基盤内の他業務システムと通信を行う場合は、事前に基盤システム所管部門へ通信の許可を申請する必要がある。なお、同一業務システムの仮想マシン間の通信及び全ホストとの ICMP 通信（ping コマンドで用いられる通信）はあらかじめ許可されている。また、仮想マシンと拠点などの外部との通信制御は基盤ファイアウォールが担うため、分散ファイアウォールでは制御されない。

なお、分散ファイアウォールは、レイヤ 2～4 の通信をステートフルで監視するため、L3SW におけるアクセス制御リスト（ACL）と同様の通信制御が、同一セグメント間の通信上で可能である。

6.4.2　仮想ロードバランサ

仮想基盤では、Web/AP サーバ等の負荷分散を実現するために、NSX の仮想ロードバランサ（Edge Load Balancer）を利用できる。

仮想基盤を利用する業務システムは、原則として業務システムのサーバ自体と端末間では HTTPS 通信を行わず、端末から見てサーバの手前側に設置された仮想ロードバランサと端末間で HTTPS 通信を行う。仮想ロードバランサには SSL アクセラレータ機能が存在するため、ロードバランサに基盤認証局が用意したサーバ証明書と秘密鍵を導入することで HTTPS 通信のデコードを行う。ロードバランサとサーバ間の通信は HTTP 通信となるため、ロードバランサを経由する構成ではサーバ側へのサーバ証明書の導入は不要である。

6.5　運用管理（Hinemos）

仮想基盤は、Hinemos（(株）NTT データ）によるジョブ管理・状態監視機能を持つ。各業務システムは、仮想サーバに Hinemos エージェントを導入することで、ブラウザから Hinemos Web クライアントを利用して仮想マシンの運用管理を行うことができる。

Hinemos のジョブ管理機能では、業務システムのジョブネットを定義し、登録することで、業務システムのジョブのスケジュール化及び実行結果の管理ができる。また、後述の業務システムのバックアップポリシーも、１つのジョブとしてスケジュール化ができる。

Hinemos の状態監視機能では、業務システムの仮想マシンの各種状態・情報・ジョブ実行結果の監視が可能である。各業務システムにおける Hinemos への監視項目の追加は、業務システムから基盤システム所管部門への申請に基づいて仮想基盤保守事業者が行う。仮想基盤の Hinemos における主な監視項目を以下に示す。

- PING 監視、サービス・ポート監視
- システムログ、イベントログ、ログファイル監視
- リソース監視
- プロセス監視
- Windows サービス監視
- ジョブ監視

6.6　バックアップ機能（NetBackup）

仮想マシンのバックアップ処理には JP1/VERITAS NetBackup ((株)日立製作所) を採用している。各業務システムは、仮想基盤保守事業者が提供する、仮想マシンへのバックアップ設定サービスを利用する形でバックアップポリシーを作成し、バックアップ/リストアを実施できる。また、バックアップポリシーの実行を自動化する場合は、必要なスクリプト等を各業務システム側で作成する必要がある。

バックアップの取得単位は仮想マシン単位であるが、リストアは仮想マシン単位及びファイル単位で実施できる。また、本番環境のバックアップデータのうち、一定容量内のデータについては、申請に基づいて二次バックアップとして LTO テープへ書き込まれ、災害対策として遠隔地に保管することができる。

7　SSO システム

情報共有基盤は、利用者の利便性の向上及び業務システムの実装コストの削減を目的として、認証及びアクセス制御の共通化を実現するエージェント型のシングルサインオン（Single Sign-On, SSO）による認証システムを運用している。SSO システムは、利用者ごとにアカウントを発行し、利用者を認証する機能を提供する。利用者の所属組織ごとに業務システムの URL 単位のアクセス可否を制御することができる。

業務システムに SSO クライアントを組み込むことで業務システム独自の認証機能が不要となるが、業務システム自体へのアクセス可否以外の権限を制御する場合（例えば、更新権限を持つ利用者だけに項目の入力を許可する場合）には、業務システム側での作り込みが別途必要である。この際に使用する情報（職員や所属の情報など）は SSO システムから取得できる。

なお、8　基盤ポータルを利用するためには、SSO システムの利用が必須となる。

SSO システムを利用するにあたっての技術的制約については、添付の別紙『SSO システム_連携方式の概要』を参照すること。

詳細は、業務システム開発事業者へ提供する（システム発注段階においては閲覧に供する）『SSO システムユーザーズガイド』を参照すること。

8　基盤ポータル

基盤ポータルは、SSO ユーザが利用可能な複数の業務システムへのリンクを表示するポータルサイトである。各業務システムにアクセスするための URL へのリンクと、情報共有基盤及び各業務システムから利用者に対してのお知らせ情報が表示されている。業務システムがポータルへのリンク及びお知らせの追加を希望する場合は、基盤システム所管部門に依頼する必要がある。

基盤ポータルの画面イメージを図 8-1　基盤ポータル画面に示す。

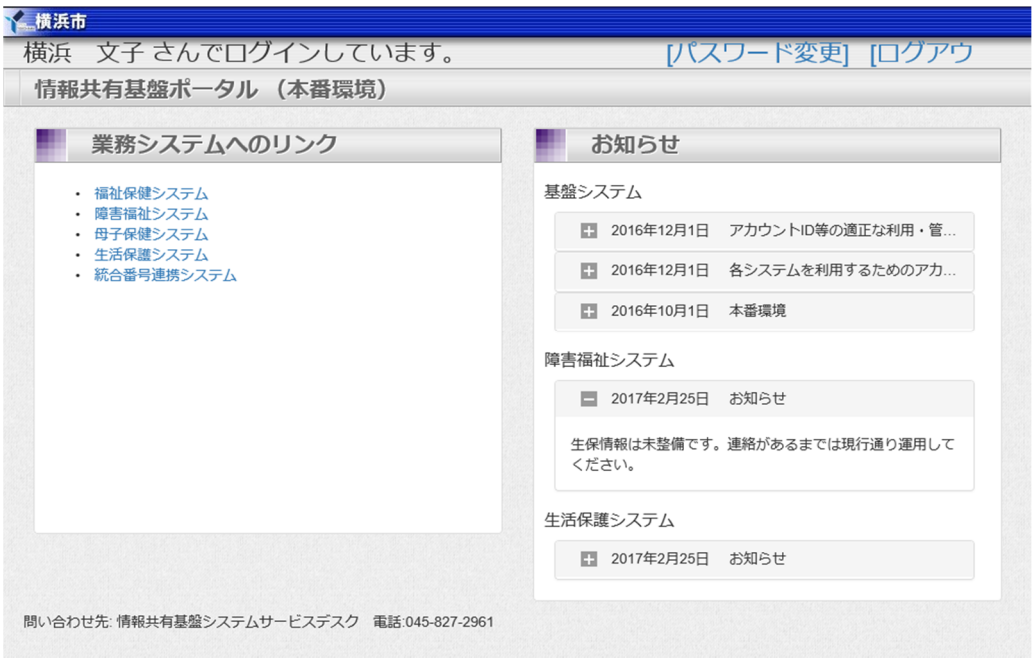


図 8-1　基盤ポータル画面

9　基盤データベース

住民記録、課税情報などの個人情報や、住所コード、金融機関情報などのマスタ情報のように、複数の業務システムが共通して利用する情報については、基盤システムが各システムとデータ連携し、基盤データベースに格納することで共有を可能にしている。

業務システムから基盤データベースに対するデータ登録、更新、削除は許可しない。ただし、後述の「9.2　個人基本情報」については、基盤システムが提供する API を利用することで追加、更新、削除をすることができる。

基盤データベース上の個人情報を利用する場合には、各所管部門が、その個人情報の保有課へ利用申出書を提出する必要がある。また、保有課が利用を許可したことが分かる文書等をあらかじめ基盤システム所管部門に提出の上、利用方式について協議する必要がある。

本章では、基盤データベースが保有する各種情報について説明する。

9.1　住民記録情報

住民記録システムの住民基本台帳情報（日本人及び外国人）を保有している。住民記録情報は、個人基本情報とは独立して存在している。

住民記録システムの情報保有期間に合わせ、現存世帯に関する情報は永続的に保有する。除票された世帯に関する情報は、除票後 5 年間保有し、その後削除する。

9.2　個人基本情報

基盤データベースが保有する、住登者及び住登外者（後述）の個人情報である。

基盤データベースでは住民記録情報を保有しているが、この情報は住民票を管理するためのものであるため、業務システムが必要とする宛名の管理要件とは必ずしも合致しない。(例えば、市外に転出したが、継続してサービスを受ける場合など)

そこで、業務システムが必要に応じて登録、更新、削除できる宛名として、個人基本情報を定義している。

個人基本情報の登録、更新、削除は、基盤システムが提供する API を利用して行うこと。業務システムが基盤データベースを直接更新することは許可しない。

なお、個人基本情報で用いられる用語の意味は以下の通りである。

(1)　住登者

横浜市に住民票がある人のこと。住民記録システムに必ず登録されている。

(2)　住登外者

横浜市に住民票がない人のこと。住民記録システムに登録されていたが、市外転出・死亡等で消除された元住登者も住登外者に含まれる。

9.2.1　個人管理

個人基本情報では住登者及び住登外者を管理するため、市民のみではなく、市外在住者の個人情報についても管理する。

個人が住登者と住登外者のどちらに属するかは、「住民状態」として管理されている。市外転出等の異動により、住登者が自動的に住登外者になるなどの状態遷移が行われる。個人基本情報の状態遷移を図 9-1　個人基本情報の住民状態遷移に示す。

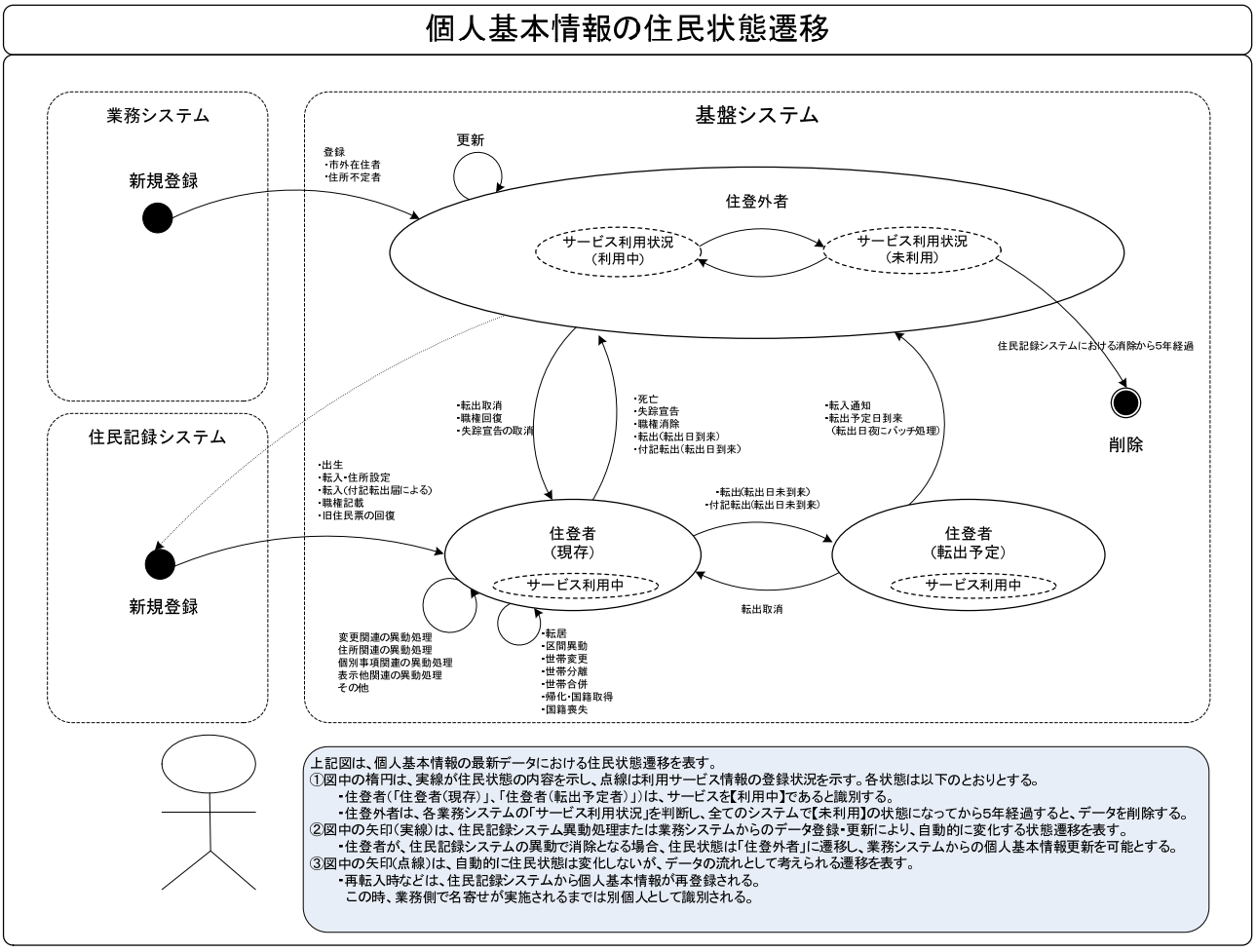


図 9-1　個人基本情報の住民状態遷移

9.2.2　住登者の取り扱い

基盤システムは、データ連携により住民記録システムからの異動情報を受け取り、住民記録情報として登録する。また、同時に個人基本情報にも住登者として登録する。

住登者に対して異動があれば、住民記録システムからの異動情報の連携に応じて、個人基本情報も基盤システムにより随時更新される。

住登者の情報を業務システムから参照することはできるが、更新や削除をすることはできない。

9.2.3　住登外者の取り扱い

基盤システムでは、転出等により住民票から消除された者（元住登者）及び業務システムが登録した者を合わせて、住登外者と呼称している。個人基本情報における住登外者は、複数の業務システムが共有して利用可能である。

業務システムは、以下のルールに従えば、API を使用して住登外者の情報を登録、更新、削除することが可能である。

【ルール】

(1) 登録する前に個人を検索し、同一人物が既に登録されていないかどうかを確認すること

(2) 登録した情報は、他のシステムからも編集可能である。
編集されたくない場合は、個人基本情報を使わずに自システム内で情報を管理する仕組みを用意すること。

(3) 以下の条件に合致する場合は削除できる
削除しようとする住登外者が、削除時点でどの業務システムからも利用されていない状態であること
（後述する利用サービス情報の登録状態で判断する。）

9.2.4　利用サービス情報

利用サービス情報とは、ある個人の個人基本情報をどの業務システムが利用しているかを個人単位に管理するための情報である。

業務システムは、ある個人について業務システムでの管理を開始したら利用サービス開始の登録を行い、管理を終了したら利用サービス終了の登録を行う必要がある。

ここでいう「管理」とは、個人の情報を業務システム上で保有することを指す。

利用サービスの登録は、基盤システムが提供する API を利用して行うこと。

9.2.5　名寄せと付設替え

個人基本情報に対して同一人物のデータが複数件登録されることをシステム的に防止することができないため、「名寄せ」の API を提供する。名寄せにより、複数のデータを同一人物として扱う情報が付加される。

また、業務システムから別人に対する利用サービスの誤登録が行われた場合の修正手段として「付設替え」の API を提供する。

9.3　税情報

税務システムの、個人市民税情報及び税宛名情報を保有している。

(1) 個人市民税情報

税務システムが保有する、個人市民税の台帳情報及び課税情報である。
税務システムの保有期間に合わせ、現年度を含めて 3 年度分の情報を保有している。

(2) 税宛名情報

固定資産税（土地・家屋）及び都市計画税、軽自動車税の 2 つの税情報を税宛名情報として保有している。税宛名情報では賦課の有無のみを保有しており、税目の詳細（課税額等）は保有していない。

9.4　介護保険情報

介護保険システム 1 及び介護保険システム 2 が保有する、介護資格及び要介護度認定に関する情報である。

(1) 介護資格情報

介護保険システム 1 が保有する、介護資格の得喪日、介護保険料の賦課収納に関する情報である。介護資格得喪日については、介護保険システム 1 が管理している範囲での履歴を保有する。

(2) 要介護度認定情報

介護保健システム２が保有する、要介護度認定、居宅介護支援に関する情報である。

9.5　生活保護情報

生活保護システムが保有する、生活保護の開廃及び受給履歴に関する情報である。

(1) 開廃連絡票

生活保護の開始・廃止・停止等の状況に加え、保護措置区や居住地住所、住民票上の住所等を持つ情報である。

(2) 受給履歴

生活保護の開始、廃止、停止等、生活保護の状況に関する情報である。

9.6　職員・組織情報

人事給与システムが保有する、職員個人、職員の所属及び組織に関する情報である。また、人事給与システムが保有しない利用者の情報も登録できる。保有している利用者の種別は以下の通りである。

(1) 人事給与システム対象者

・正規職員

・再任用職員

上記については、人事給与システムで更新されたデータを定期的に取り込んでいる。

(2) その他の基盤システム利用者

・嘱託員

・アルバイト

・システム開発・保守・運用事業者

退職者の情報は退職後５年間保有し、その後削除される。

9.6.1　SSO・ポータルとの連携

職員・組織情報に登録された利用者は、SSO システムに連携され、所属する組織に付与されたシステム利用権限が自動的に与えられる。これにより、利用者が基盤ポータルにログインした際には、利用を許可された各業務システムにアクセスするための URL へのリンクが表示される。

9.7　マスタ系情報

9.7.1　住所コード

基盤システムでは、住所コードマスタとして以下の 2 種類を保有している。

(1) 市内住所コードマスタ

本市が管理する、住民記録情報で用いられている市内の全ての町・字名にコードを割り当てた物。

(2) 市外住所コードマスタ（J-LIS 全国町・字ファイル）

J-LIS が管理する、個人基本情報で用いられている全国の町・字名にコードを割り当てた物。

9.7.2　金融機関

基盤システムでは、金融機関マスタとして 1 種類を保有している。

(1) 金融機関店舗情報（全国銀行協会）

過去に統廃合された銀行・店舗の情報も保有している。

9.7.3　自治体マスタ

基盤システムでは、自治体マスタとして J-LIS の地方公共団体コード住所を保有している。自治体マスタには、全国の都道府県、指定都市、市区町村及び指定都市の区名とコードが含まれる。

9.7.4　情報提供ネットワークシステム配信マスター

社会保障・税番号制度における情報提供ネットワークシステム配信マスター情報のうち、以下の情報を保有している。

- 事務マスター
- 事務手続マスター
- 機関マスター
- 機関種別マスター
- 機関種別機関対応マスター
- 特定個人情報名マスター
- 特定個人情報項目マスター

10　基盤連絡受付データベース

基盤システム所管部門への連絡、問い合わせ及び依頼は、Redmine による基盤連絡受付データベースにチケットを起票する。

基盤連絡受付データベースの画面イメージを図 10-1　基盤連絡受付データベースに示す。

図 10-1　基盤連絡受付データベース

11　データ連携基盤

業務システム同士がファイルを用いたデータ連携を行う際の中継点として、データ連携基盤を利用することができる。データ連携基盤は、ファイル送受信及び文字コード変換の機能を備えている。

業務システムは、データ連携基盤が備えるファイル転送ソフトウェアである HULFT ((株)セゾン情報システムズ）または共有フォルダ（Windows ファイル共有）を利用して、ファイルの送受信をすることができる。データ連携基盤の利用例を図 11-1　データ連携基盤利用の例に示す。

詳細については、別紙　「データ連携基盤概要」を参照すること。

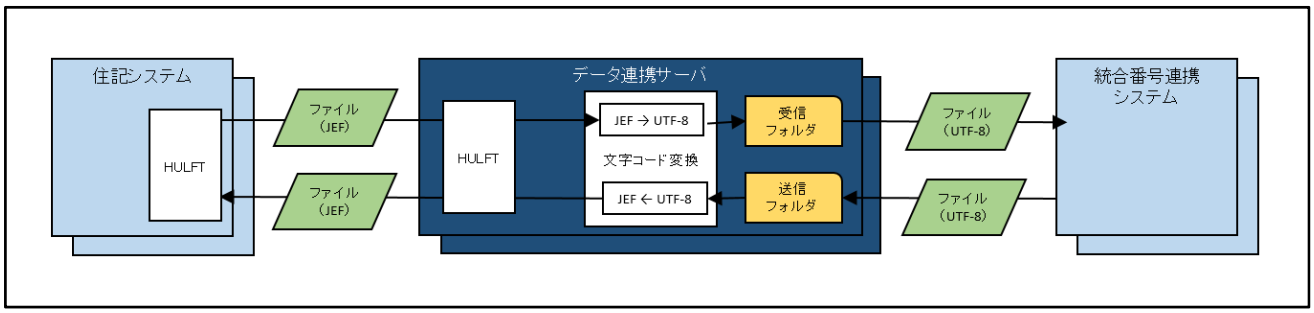


図 11-1　データ連携基盤利用の例

11.1　文字コード変換

業務システムは、データ連携基盤が備える文字コード変換の機能を利用することで、他業務システムに合わせた異なる文字コードのファイルを連携することができる。変換可能な文字コードは表 11-1　変換可能な文字コードのとおりである。なお、JEF 及び Unicode には横浜市独自の外字が登録されており、相互に変換が可能である。

データ連携基盤が行うのは文字コードの変換のみであり、可変長/固定長などのレイアウト変換は行わない。

表 11-1　変換可能な文字コード

	JEF に変換	Unicode（UTF-8/16/32）に変換	Shift-JIS に変換
JEF から		・外字の変換が可能。 ・PACK 形式のバイト列は変換不可。 ・マルチバイト文字列の前後にシフトコードを付加すること。 ・UTF-8 への変換後は、BOM なしとなる。 ・UTF-16/32 への変換後は、BOM 付となる。	・外字の変換は不可。 ・JEF から Unicode に変換したのち、Shift-JIS に変換する。（2 段階）
Unicode（UTF-8/16/32）から	・外字の変換が可能。 ・変換後はマルチバイト ・PACK 形式のバイト列への変換は不可。 ・文字列の前後にシフトコードが付加される。 ・UTF-8 は BOM なしとすること。 ・UTF-16/32 は BOM 付とすること。		・外字の変換は不可。
Shift-JIS から	・外字の変換は不可。 ・Shift-JIS から Unicode に変換したのち、JEF に変換する。（2 段階）	・外字の変換は不可。	

12　用語集

初出ページ	用語	意味
9	シングルサインオン（Single Sign-On）	一度ユーザ認証に成功することで、独立した複数のシステムが利用可能になる特性のこと。
13	LGWAN（総合行政ネットワーク）	地方公共団体を相互に接続する行政専用のネットワーク。このネットワーク上に LGWAN-ASP や自治体中間サーバー・プラットフォームが存在する。
13	基幹（システム・端末・ネットワーク）	ホストコンピュータ上で稼働している業務システム（住民記録、税務、国保等）の総称。また、それらを利用するための端末及びネットワーク。
18	自治体中間サーバー・プラットフォーム	マイナンバー制度における情報連携等を行うために、連携の対象となる個人情報を管理するサーバ。各機関間の連携における中継点となる。
23	WPD デバイス（Windows Portable Device）	Windows における、接続した携帯電話、カメラ等のポータブルデバイスと通信するためのデバイスの認識種別。WPD デバイスとして認識されると、USB メモリと同様に、ポータブルデバイスの記憶域にデータの書き込みができる。
24	アプライアンス	機器と専用のソフトウェアがセットになっているなど、特定の機能に特化した機器の総称。
25	ブロッキング I/O	I/O のスレッド処理において、スレッドがリクエストを処理している間は他のリクエストが割り込まない方式のこと。一方、スレッドがリクエストを処理している間の I/O 待ち時間を活用して他のリクエストを処理することをノンブロッキング I/O という。
37	JEF（JEF 漢字コード）	富士通が策定した文字コード。基幹システムではデータを主に JEF 形式で保持している。Windows 上で文字を読むためには変換が必要になる。
38	BOM（byte order mark）	Unicode で符号化したテキストにおいて先頭に付与される、UTF-8/16/32 のどの形式で符号化しているか判別するためのデータ。

データ連携基盤概要

横浜市総務局住民情報システム課

Ver1.5.0

1　概要

データ連携基盤は、基幹／基盤ネットワークに接続されたシステムが、相互にファイル連携を行うための「ファイル送受信」及び「文字コード変換」の仕組みである。

送信元のシステム（以下、「送信システム」という。）から送信されたファイルに対して「文字コード変換」を行ったうえで、送信先のシステム（以下、「受信システム」という。）へファイルを送信する。

2　利用の開始

『データ連携基盤利用開始申請書』に記入のうえ、基盤システム運用部署へ提出すること。基盤システム運用部署は、申請のあった連携インターフェースを本番環境へ払い出した後で、必要事項を追記した申請書を返却する。

3　利用可能時間帯

データ連携基盤は、下記のメンテナンス時間を除いて、平日、土日祝日問わず利用可能とする。ただし、基盤システム運用部署による問い合わせ受付は、平日の 08:30 から 17:15 までとする。

4　メンテナンス時間

毎週日曜日および月曜日の 04:30 から 06:30 まで

その他にメンテナンスが必要な日（以下の条件に従う）

- 原則として、メンテナンス実施の 1 か月以上前に通知する。
- 原則として、正副両方を同日にメンテナンスすることはない。

上記を前提として、メンテナンス日の調整は不可とする。

5　処理タイプ

以下の処理タイプの中から選ぶことができる。表中の「ファイル送／受信方法」、「連携方式」については、後述する。

処理タイプ	ファイル送信方法	ファイル受信方法	連携方式	起動契機	特記事項
A	HULFT	共有フォルダ	随時	送信システムがファイルを HULFT で配信する。	
B	HULFT	共有フォルダ	単発	送信システムがファイルを HULFT で配信する。	
C	共有フォルダ	共有フォルダ	単発	送信システムがファイルを共有フォルダに配置する。	複数ファイルを共有フォルダに配置した場合に、ファイルの送信順は

					保証しない。（配置した順に送信する保証はない。）
D	共有フォルダ	HULFT	単発	送信システムがファイルを共有フォルダに配置する。	複数ファイルを共有フォルダに配置した場合に、ファイルの送信順は保証しない。（配置した順に送信する保証はない。）
E	共有フォルダ	HULFT	単発	受信システムがHULFTで配信要求を送信する。	共有フォルダに対象ファイルが複数存在する場合は、ファイル名の昇順に連結して送信する。

6　ファイル送受信方法

ファイルの送／受信方法として、HULFT による送受信と、共有フォルダでの送受信が選べる。

(1)　HULFT

原則として、1 つの連携インターフェースにつき 1 つのファイル ID を定義する。例外として、後述の「連携方式」が「随時」の場合は、1 つの連携インターフェースにつきデータ送信用ファイル ID が 1 つと、END ファイル用ファイル ID が 1 つで、合計 2 つのファイル ID を定義する。

(2)　共有フォルダ

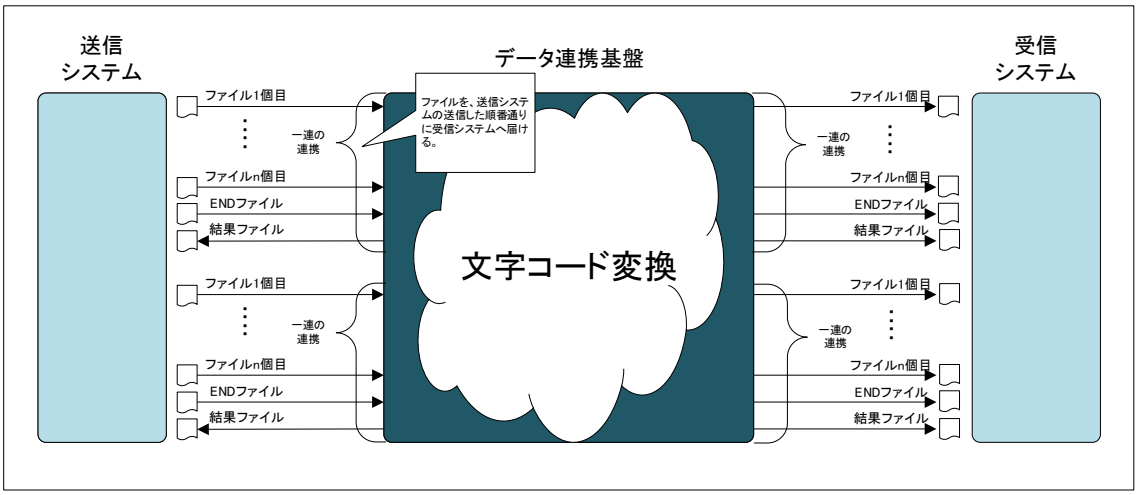
- データ連携基盤を利用するシステムには、共有フォルダを使った連携を行うかどうかに関わらず、システムごとに共有フォルダを払い出す。
- 共有フォルダへのファイルの配置、取得方法として、Windows ファイル共有、FTP、SFTP が利用できる。
- 受信システムの共有フォルダに、送信しようとしているファイルと同じ名前のファイルが既に存在する場合、古いファイルを新しいファイルで上書きする。
- 転送途中のファイルを取得してしまうことを防ぐために、ファイルを共有フォルダへ配置する際にはファイル名の先頭に”Z_”を付加し、配置が完了した後でファイル名先頭の”Z_”を削除することとする。
- 共有フォルダに配置されたファイルの削除は、受け取る側のシステムが行うこととする。すなわち、送信システムの共有フォルダへ配置されたファイルはデータ連携基盤が削除し、受信システムの共有フォルダに配置されたファイルは受信システムが削除する。
- データ連携基盤の共有フォルダはデータの受け渡しに使用するためのものなので、不要になった

ファイルは速やかに削除すること。バックアップなどの目的で過去のファイルを蓄積してはならない。

7　連携方式

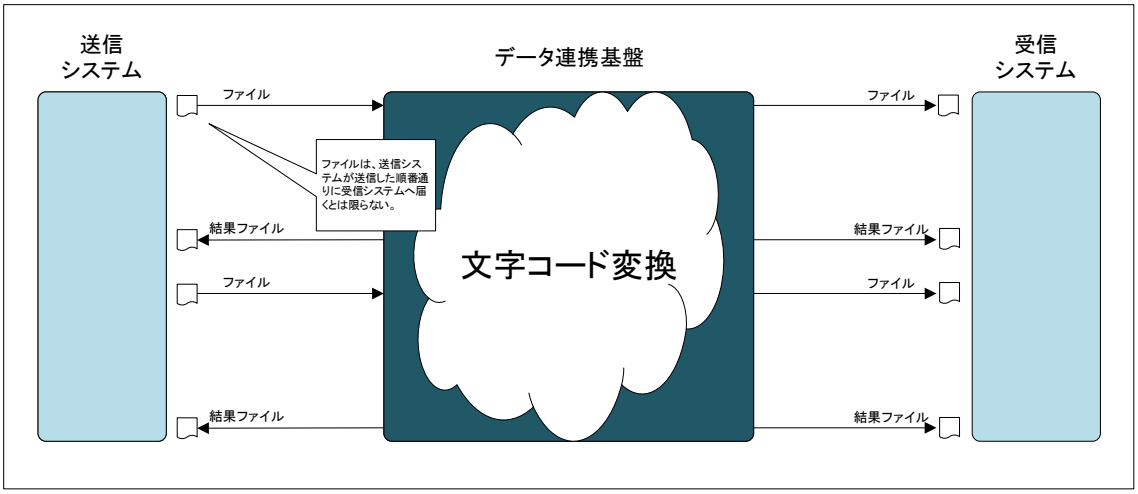
連携方式には、「随時連携」と「単発連携」の 2 種類がある。

（1）　随時連携



- 送信システムから受信システムへ取り決めたファイルを複数回送信する。
- 送信システムからの要求により連携を開始する。
- 送信システムから送信されたファイルが空ファイルの場合は、受信システムへの送信を行わない。
- 送信システムから送信された順序を保って受信システムへファイルを送信する。
- 送信システムは最後に END ファイルを送信すること。
- 随時連携処理完了後、ただちに送信システム及び受信システムの両方に対して結果ファイルを返す。（処理の正否を問わない）
- END ファイルの次に受信したファイルから次の END ファイルまでを一連の連携として扱う。
- END ファイルを受信した後、一連の連携において送信システムから受け取ったファイルの行数合計と受信システムへ送ったファイルの行数合計を比較し、一致しない場合はエラーとする。
- 一連の連携に対して、基盤システム保守業者による監視及び障害対応を行う。
- 一連の連携において障害が発生した場合には、不整合を防ぐために連携を一時停止する。

（2）　単発連携



- 送信システムから受信システムへ取り決めたファイルを 1 回送信する。
- 原則として、送信システムからの呼び出しにより連携を開始する。
- 送信システムから送信されたファイルが空ファイルであっても、受信システムへ送信する。
- 複数回連携を実行することで複数ファイルの送信を行うこともできるが、送信システムが送信した順序通りに受信システムへ送信することは保証しない。（順序の逆転が発生し得る。）
- 単発連携処理完了後、ただちに送信システム及び受信システムの両方に対して結果ファイルを返す。（処理の成否を問わない）
- ファイル送信の後、連携において送信システムから受け取ったファイルの行数と受信システムへ送ったファイルの行数を比較し、一致しない場合はエラーとする。
- 連携に対して、基盤システム保守業者による監視及び障害対応を行う。

8　文字コード変換

下表の組み合わせの文字コード変換機能を提供する。

変換可能な文字の範囲は以下の通り。

- JIS X 2013:2004（非漢字、拡張非漢字、第一水準漢字、第二水準漢字、第三水準漢字、第四水準漢字）
- JIPS 固有文字
- 横浜市外字（JEF と Unicode との間での変換のみ可能。）

	変換後			
変換前		JEF へ	Unicode へ	Shift-JIS へ
	JEF から	-	・ 横浜市外字の変換が可能。 ・ PACK 形式のバイト列は変換不可。 ・ マルチバイト文字列の前後にシフトコードを付加すること。 ・ UTF-8 への変換後は、BOM なしとなる。 ・ UTF-16/32 への変換後は、BOM 付となる。	・ 横浜市外字の変換は不可。 ・ JEF から Unicode に変換したのち、Shift-JIS に変換する。（2 段階）
	Unicode から	・ 横浜市外字の変換が可能。 ・ 変換後はマルチバイト。 ・ PACK 形式のバイト列への変換は不可。 ・ 文字列の前後にシフトコードが付加される。 ・ UTF-8 は BOM なしとすること。 ・ UTF-16/32 は BOM 付とすること。	-	・ 横浜市外字の変換は不可。
	Shift-JIS から	・ 横浜市外字の変換は不可。 ・ Shift-JIS から Unicode に変換したのち、JEF に変換する。（2 段階）	・ 横浜市外字の変換は不可。	-

※Unicode は UTF-8／16／32 が利用できる。

9　結果ファイル

データ連携基盤は、連携の成否に関わらず送信システム及び受信システムに結果ファイルを返す。結果ファイルの内容は以下の通り。なお、結果ファイルの削除は、送信システム及び受信システムがそれぞれ責任を持って行うこと。

(1)　ファイル名

「基盤システム運用部署から払い出される連携 ID」を表す半角英数 8 桁＋「処理終了年月日時分秒」を表す半角数字 14 桁＋”.csv” とする。(例：KH_TG_0001_20170213181421.csv)

同名のファイルが存在する場合は、上書きする。

(2)　項目の意味

項目名	意味	備考
処理結果	後述の「処理結果」の通り。	
受信行数	送信システムから受信したファイルの行数。	
送信行数	受信システムへ送信したファイルの行数。	

(3)　処理結果

正常／異常	処理結果	意味	送信システム用共有フォルダからのファイル削除（共有フォルダ連携の場合）	ファイルが受信システム用共有フォルダへ到達するかどうか	利用者が取るべき対応
正常	0	正常に連携した。	する	する	-
	7	文字コード変換処理において、変換できない文字が存在した。変換できなかった文字は、あらかじめ取り決めた代替文字に変換する。	する	する	-
異常	2	文字コード変換処理が失敗した。	しない	しない	'送信システムが送信したファイルの文字コードが、取り決め通りの文字コードかどうか確認する。

	その他	ネットワーク障害、サーバ障害等、予期せぬ障害によりデータ連携が正常に行えなかった。	原因による。	原因による。	基盤システム運用部署に連絡する。

10 運用ルール

(1) 障害発生時の対応

データ連携基盤のサーバは正・副の冗長構成となっている。副系サーバは待機系ではなく、利用可能時間帯においては常時正系と同じ機能を提供している。したがって、障害発生時の自動切替はない。

一方のサーバで問題が発生した場合は、業務システムが利用するサーバをもう一方のサーバに切り替えること。

(2) 大容量データ転送の事前連絡について

1 つのシステムにおいて 1 日に 2GＢ以上のデータを転送する場合は、基盤システム運用部署に事前連絡すること。

事前連絡の期限は設けないが、直前の連絡では他システムの実施予定と重なる可能性が高く、実施予定の混雑状況によっては、実施不可とする場合がある。

ア 事前連絡する項目

イ 転送実施日

ウ 転送開始時刻

エ データ連携 ID（またはファイル ID）

オ データ連携 ID（またはファイル ID）ごとのファイル数（前回実績値や概算の想定値でも可。）

カ ファイルごとのサイズ

SSO連携方式の概要
本資料について

- 本資料の目的
  - 本資料は、業務システムがSSOシステムと連携し、情報共有基盤システムと連携済みである他業務システムを含めた一元的なユーザー認証・認可を実現するにはどうすればよいのか、その連携方式の概要を示します。
  - これによって、業務システム開発の受注を検討している企業が、自社の体制・技術水準等を踏まえた受注の妥当性や自社製品とSSOシステムの適合度を、見積可能な水準で検討できるようにすることが、本資料の目的です。
  - 「Webアプリケーション」、「クライアントサーバー型システム」という用語は、一般的であるがゆえに、言葉の示す意味の範囲が非常に広くなっています。本資料及びSSOシステムユーザーズガイドにおけるこれらの用語の定義を明確にします。
  - 業務システムにクライアントサーバー型システムを適用しようとする場合、実装方式（P.9の独自方式）によりSSOシステムの利用に制約が生じます。独自方式では、通常のシングルサインオンの実現が困難なことから、調達仕様・要求仕様を満たさないために、横浜市への事前説明・調整が必要になります。
    本資料の中で、クライアントサーバー型システムの場合の注意点について説明します。

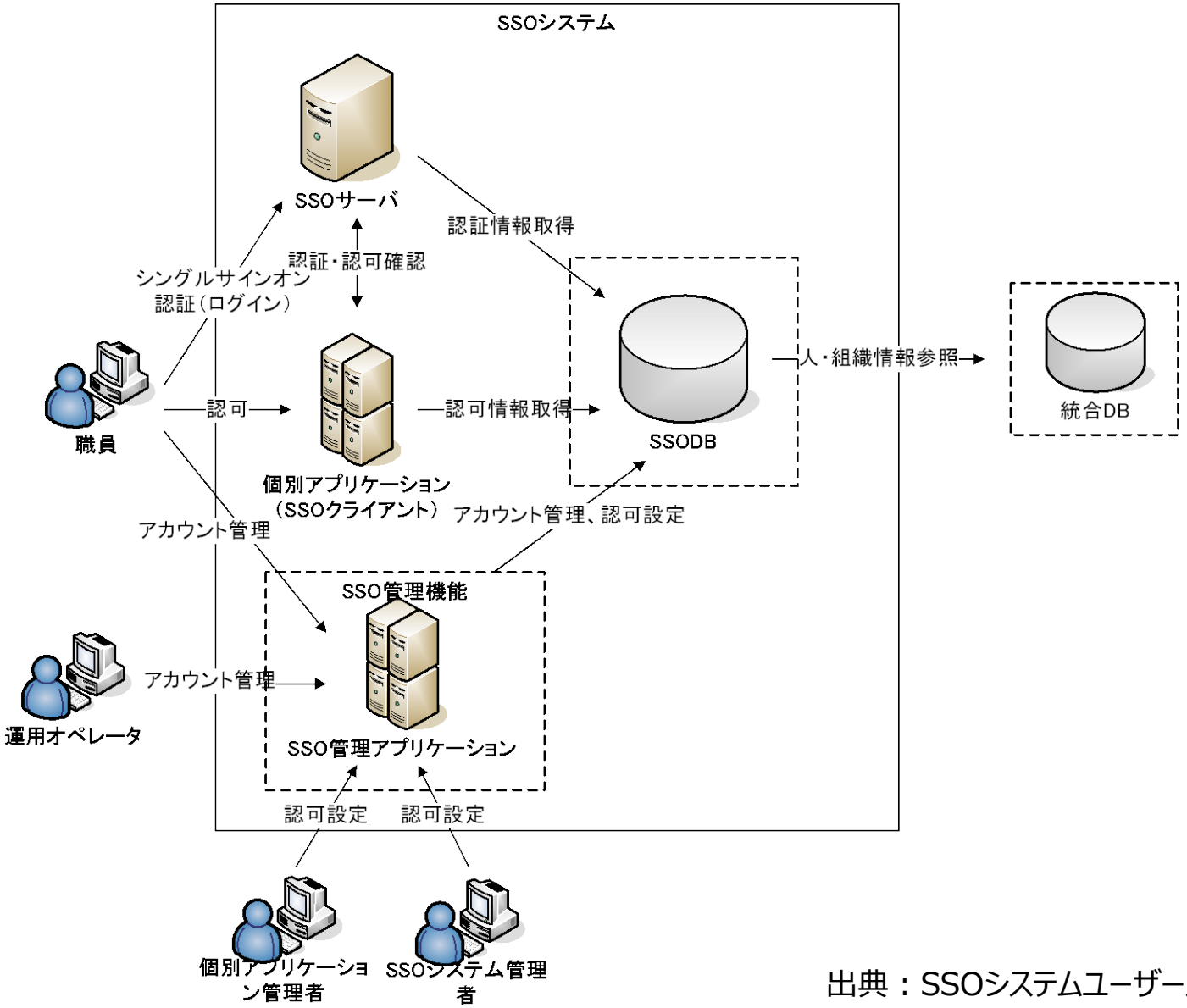
- 対象読者
  - 業務システム開発担当者
  - 業務システム営業担当者

SSO連携方式の概要
SSOシステムについて (1/3) SSOシステムとは

- SSOシステムの目的　（「SSOシステムユーザーズガイド（概要編）」より抜粋）

  - SSOシステムとは、横浜市役所の基幹系ネットワークのシステムを構成する各個別アプリケーションに対して、統一的な認証・認可の基盤を提供するためのシステムである。
  - SSOシステムを導入すると、職員はSSOシステムに対応した個別アプリケーションにアクセスする際、ログインを要求される。要求されたログイン画面でログインを行い一度SSOシステムにおいて認証されると、SSOシステムに対応した別の個別アプリケーションにアクセスする際、あらためてログインを要求されることなく個別アプリケーションを利用できるようになる。
  - また、認証、認可に関する情報を一元管理することができ、セキュリティに関するログの方式を統一できる。

SSO連携方式の概要
SSOシステムについて (2/3) SSOシステム構成図



出典：SSOシステムユーザーズガイド（概要編）

SSO連携方式の概要
SSOシステムについて (3/3) SSOシステム機能一覧

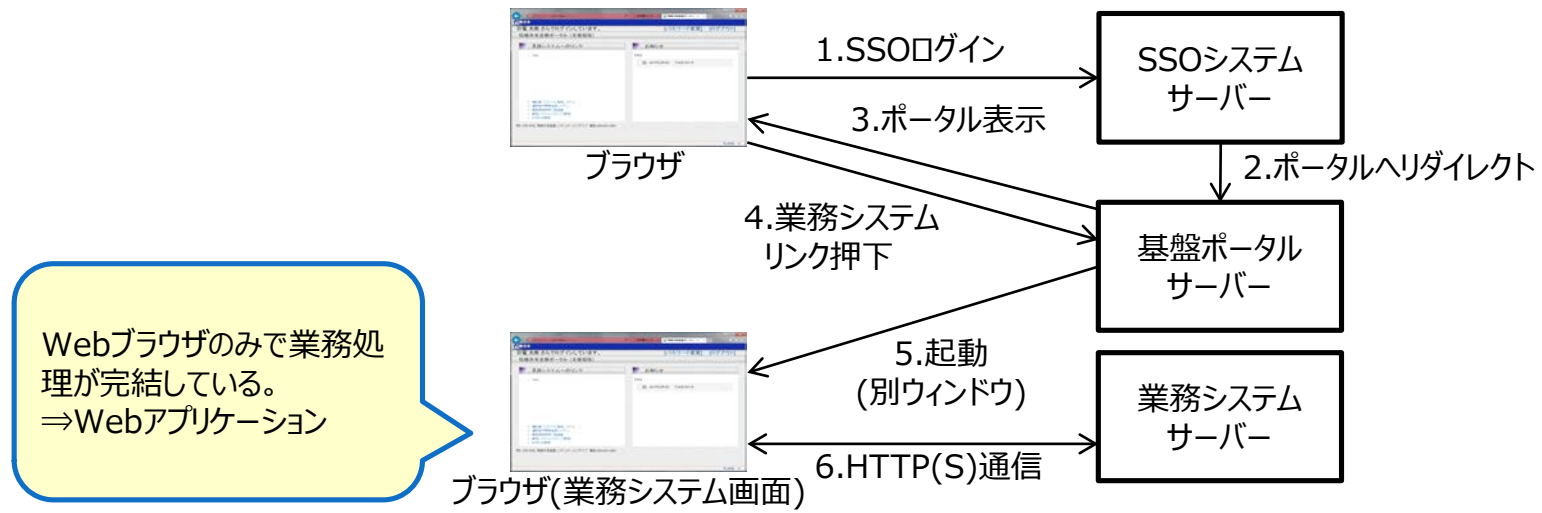
- SSOシステムユーザーズガイドの前提通りにSSOクライアントを利用した場合に実現する機能の一覧です。

No.	SSOの機能	No.	説明
1	ユーザーを認証・認可する	1-1	SSODBの認証情報、認証済情報を使用し、ユーザーがシステムを利用できるか確認をする
		1-2	SSODBの認可情報を使用し、ユーザーがリクエストされたURL（メニュー・画面）の利用権限があるか確認をする
2	認証済情報を管理する	2-1	基盤ポータルでのログインで認証済情報を有効にする
		2-2	ログイン中のいずれかのシステムを最後に操作してから30分経過で認証済情報を無効にする
		2-3	ログインしてから8時間経過で認証済情報を無効にする
		2-4	基盤ポータルでのログアウトで認証済情報を無効にする
3	SSO認証画面を表示する	3-1	ユーザが未認証の場合、HTTPリダイレクトによりSSO認証画面を表示する
		3-2	システム利用中に認証済情報が無効となった場合、HTTPリダイレクトによりSSO認証画面を表示する
4	認証済情報を保護する	4-1	セキュア属性のCookieを使用し、認証済情報を保護する
		4-2	SSL暗号化を使用し、通信内容を保護する
5	認証・認可情報を一元管理する	5-1	職員の認証情報を一元管理する
		5-2	組織および職員の認可情報を一元管理する

SSO連携方式の概要
用語の定義 (1/2) Webアプリケーション

※ 補足説明を 15～16ページ に掲載

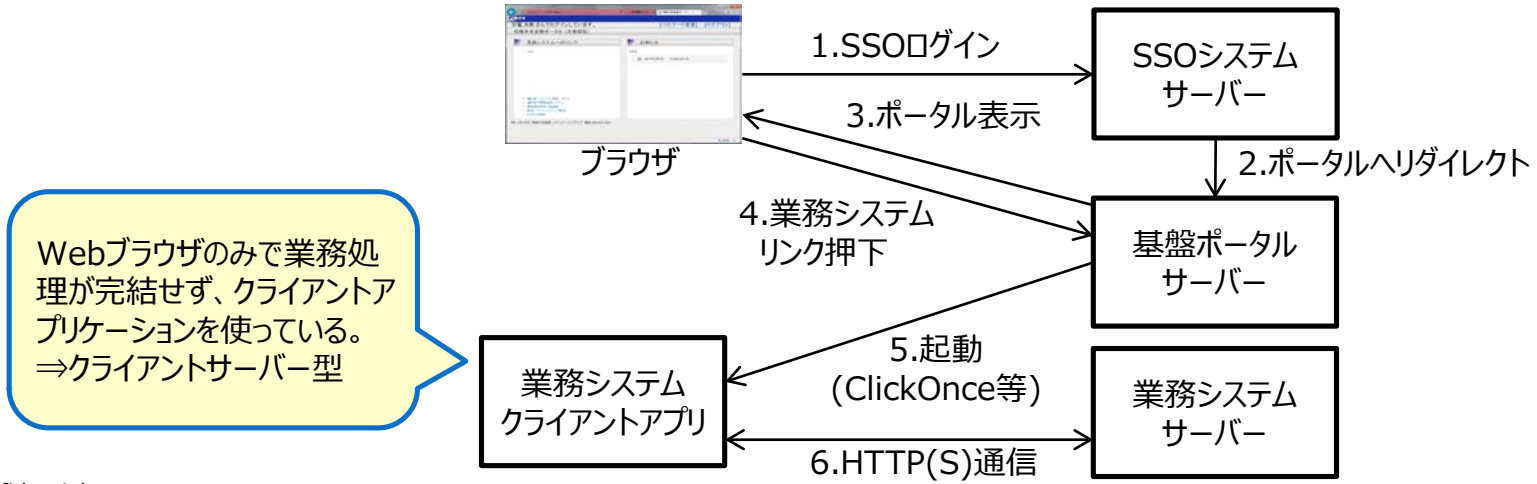
- 本資料及びSSOシステムユーザーズガイドにおいて、「Webアプリケーション」とは、以下の1.～3.の条件を全て満たすシステムのことを指します。
  1. 業務処理を提供するサーバーと、サーバーにアクセスするための端末で構成されます。
  2. 端末にインストールされたWebブラウザを用いてサーバーにアクセスし、処理を行います。
     - ブラウザプラグイン上で稼働してサーバーとの通信を伴うアプリケーション(Javaアプレット、Flash等)は、条件2.を満たしません。
  3. **業務処理はWebブラウザとサーバーの間のHTTP(S)通信のみで完結**し、端末にインストールされた別のアプリケーションを用いません。
  - サーバーの論理構成・物理構成、開発言語、ミドルウェアは問いません。
    - 文脈上、開発言語を限定する場合、本資料では、例えば「JavaのWebアプリケーション」というように開発言語を併記します。



SSO連携方式の概要
用語の定義 (2/2) クライアントサーバー型システム

※ 補足説明を 15～16ページ に掲載

- 業務処理がWebブラウザからのアクセスのみで完結せず、端末にインストールされた別のアプリケーションがサーバーにアクセスして処理を行う形態のシステムは、**Webブラウザからアプリケーションを起動できる、端末とサーバーの間の通信をHTTP(S)で行っている、というような場合であっても、クライアントサーバー型システムに該当**します。
- Webブラウザから仮想デスクトップ(VDI)にHTTP(S)でアクセスし、仮想デスクトップ上に配置されたクライアントアプリケーションを起動してサーバーと通信する形態のシステムは、SSO連携方式の観点からはクライアントサーバー型システムに該当します。
- 例えば、以下のようなシステムは、クライアントサーバー型システムです。
  - Webブラウザを起動し、SSOでログインすると、基盤ポータルに業務システムへのリンクが表示される。
  - 業務システムへのリンクをクリックすると、端末にインストールされたクライアントアプリケーション(Windowsアプリケーション)が起動して、認証・認可済みでシステムが使用できる状態になる。
  - クライアントアプリケーションとサーバーアプリケーションの間はHTTP(S)で通信する。

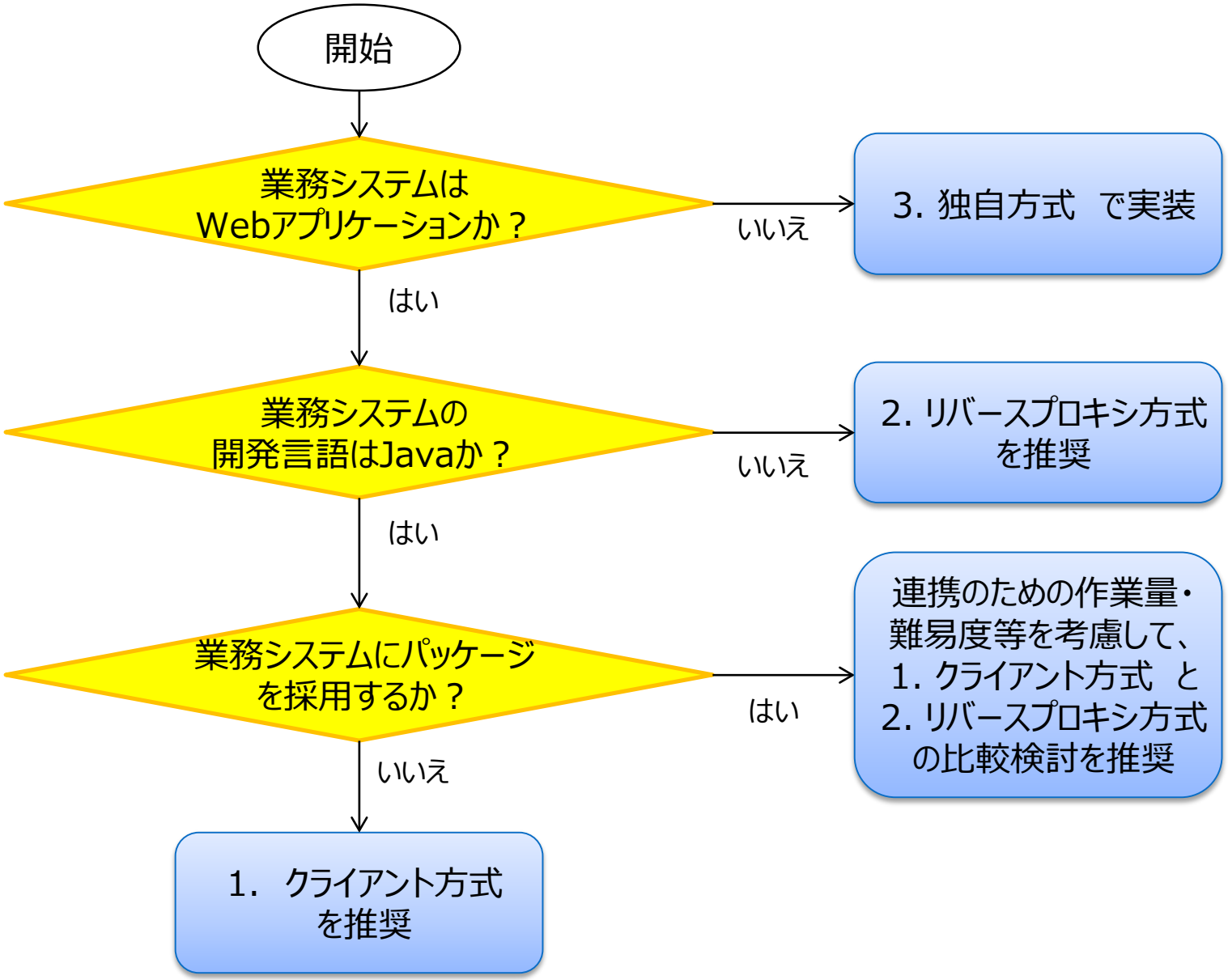


SSO連携方式の概要
SSO連携方式 (1/4) 業務システムをSSOシステムと連携させるための作業量

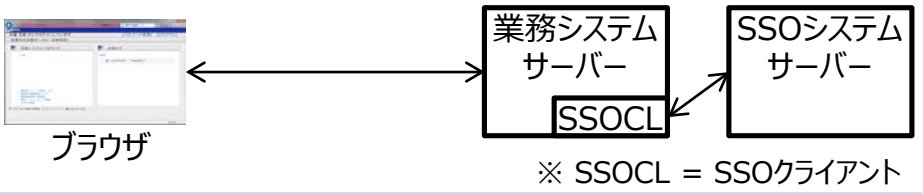
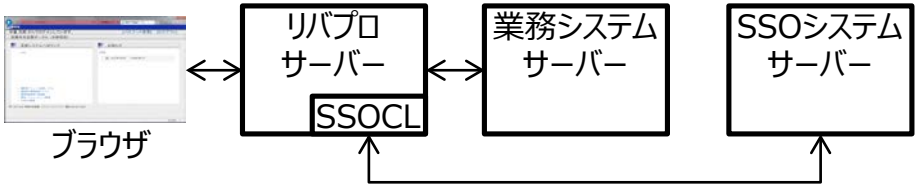
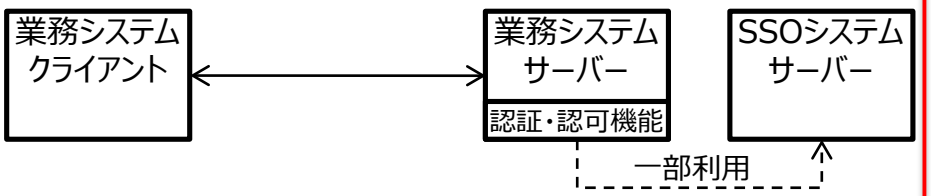
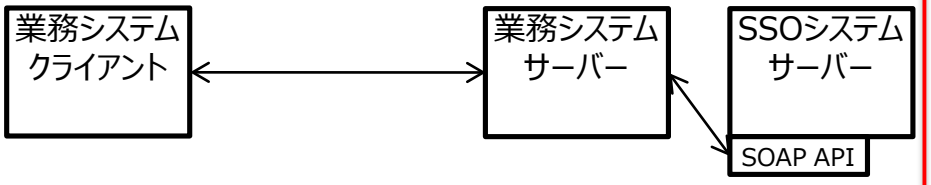
- 業務システムがWebアプリケーションである場合、SSOシステムとの連携を比較的容易に行うことができます。
  - 業務システムがJavaのWebアプリケーションである場合、9ページに後述する「1.クライアント方式」を採用することで、最も少ない作業量でSSOシステムと連携することができます。
    - SSOシステムユーザーズガイドは、「業務システムがJavaのWebアプリケーションである」という前提で記述されています。
  - 業務システムがWebアプリケーションであれば、開発言語に関わらず、9ページに後述する「2.リバースプロキシ方式」を採用できます。

- 業務システムがWebアプリケーションでない場合でも、SSOシステムと連携することは可能です。この場合、9ページに後述する「3.独自方式」を採用します。
  - 但し、「シングルサインオンを実現する ＝ 4ページに示したSSOの機能を実現する」には、SSOシステムが実現している機能（共通認証、認可、セキュリティ制御などの機能）の一部を業務システムが独自に実装しなければならない等、業務システムに対する相当量の作業が発生します。

SSO連携方式の概要
SSO連携方式 (2/4) 推奨する連携方式の簡易判定チャート



SSO連携方式の概要
SSO連携方式 (3/4) SSO連携方式一覧

No.	方式	説明	構成例
1	クライアント方式	業務アプリケーションに、SSOクライアントを組み込む方式です。開発言語がJavaのWebアプリケーション、かつ、基本的にはスクラッチ開発の場合に採用できます。	
2	リバースプロキシ方式	業務アプリケーションとは別に、SSOクライアントを組み込んだリバースプロキシをJavaで開発する方式です。Webアプリケーションであれば開発言語を問わず、パッケージであっても採用できます。	
3	独自方式	業務システム独自に認証・認可を行います。SSOシステムの機能・認証情報の一部を利用する場合も、独自方式に含まれます。SSOシステムを全く利用しない場合は、認証・認可（権限制御）の情報を独自に用意する必要があります。	
	Webサービス（SOAP API）方式	業務システムが、Webサービスにより、SSOシステムの認証機能のみ利用する方式です。アーキテクチャや開発言語を問いません。**<u>但し、以下の制約があります。</u>** ・SSOシステムの機能の一部しか実現できない ・ログイン操作を共通化できないため、基盤ポータルを利用できない	

赤線で囲まれたNo.3独自方式は、<u>シングルサインオンではありません</u>。

SSO連携方式の概要
SSO連携方式 (4/4) SSO連携方式の比較

(※リバプロ方式で業務システム側に独自実装が発生した場合は「独自方式」に該当)

No.	比較ポイント		クライアント方式	リバースプロキシ方式	独自方式	Webサービス方式
1	SSO機能の実現範囲	ユーザーを認証・認可する	○	○	※1	△ ※4
2		認証済情報を管理する	○	○	※1	×
3		SSO認証画面を表示する	○	○	※1	×
4		認証済情報を保護する	○	○	※1	○ ※5
5		認証・認可情報を一元管理する	○	○	※1	○
6	基盤ポータル利用		可能	可能	※2	不可
7	認証・認可情報の独自運用		無	無	※3	無

※1 独自方式によりどこまで実装するかによって、実現範囲は変わります
※2 原則、SSO機能の実現範囲がクライアント方式・リバースプロキシ方式と同一でないと基盤ポータル利用不可
※3 認証・認可情報が一元管理されない場合は、稼動後に職員異動対応等の独自運用が発生します
※4 認証のみ実現(SSOではありません)。認可情報による権限制御は、独自方式として別途実装する必要があります
※5 Cookieを利用しないため、Webサービスとの通信のSSL暗号化のみ実施で○とします

SSO連携方式の概要
クライアントサーバー型システムとSSOシステムの連携のポイント

- クライアントサーバー型システムをSSOシステムと連携させる場合、以下のいずれかを採用します。
  (4ページ「SSOシステム機能一覧」、10ページ「SSO連携方式の比較」参照)
  1. 4ページに示すSSOシステムの機能をどこまで実現するか、及び基盤ポータルを利用するか否かを調整し、実現しない範囲を制約事項とすることを横浜市と調整した上で、独自方式を採用する。
  2. 4ページに示すSSOシステムの機能の一部しか実現できないこと、認証方式がシングルサインオンではないこと、基盤ポータルを利用できないことの3点を制約事項とすることを、横浜市と調整した上で、SSOシステムの認証機能のみ利用するWebサービス方式を採用する。

- いずれの方式を採用するかは、開発しようとする業務システムの業務特性、ユーザビリティに関する要件、セキュリティに関する要件、連携処理の設計・実装難易度等によって決定されます。

- 業務システムにクライアントサーバー型システムを適用する場合、業務システム開発者には、開発プロジェクトの状況を考慮して、市と調整の上でSSOシステムとの適切な連携方式を選択し、設計・実装することが求められます。

SSO連携方式の概要
【補足】SSOシステムユーザーズガイド (1/3)

- SSOシステムユーザーズガイドは、SSOシステムを利用しようとする際に活用できるドキュメント群です。

- SSOシステムユーザーズガイドは、概要編をはじめとした8編で構成されます。
  業務システムの開発・保守・運用担当者が対象読者になっている場合、下線赤字で示します。

SSO連携方式の概要
【補足】SSOシステムユーザーズガイド (2/3)

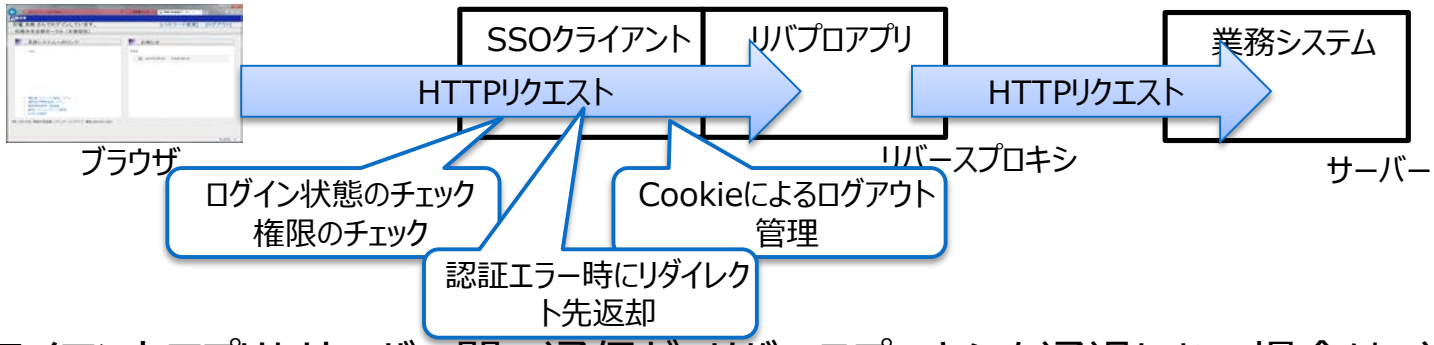
- 概要編
  - 対象読者……SSOシステムを使用しようとする全てのシステム担当者
  - SSOシステムの目的と概要について説明します。
- 導入編
  - 対象読者……業務システム開発担当者、SSOシステム保守・運用担当者(基盤システム保守)
  - SSOサーバー、SSO管理アプリケーション、SSODB連携アプリケーション、職員登録アプリケーションの導入方法について説明します。
- 開発編
  - 対象読者……業務システム開発担当者、業務システム保守担当者
  - 業務システムにSSOクライアントを組み込む方式を用いることでSSOシステムとの連携を実現する方法について説明します。開発用のSSOサーバー(スタブ版)も提供されます。
- Webサービス編
  - 対象読者……業務システム開発担当者、業務システム保守担当者
  - Webサービス(SOAP API)方式でSSOシステムとの連携を実現する方法について説明します。開発用のSSO Webサービスのスタブも提供されます。

SSO連携方式の概要
【補足】SSOシステムユーザーズガイド (3/3)

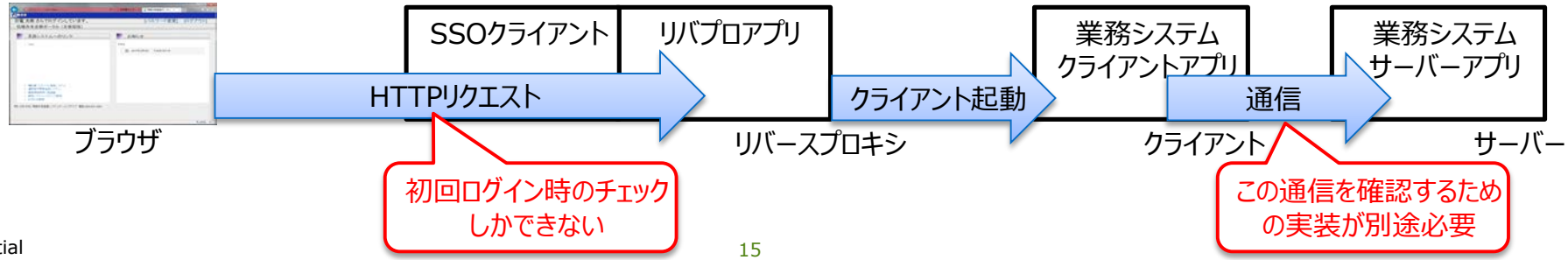
- 管理者編
  - 対象読者……SSOシステム運用担当者、業務システム保守担当者、業務システム運用担当者
  - SSOシステムを管理・運用する上で使用する機能について説明します。
- 職員編
  - 対象読者……業務システムを利用する職員（ユーザー）
  - 一般の職員が利用する機能（ログイン、ログインID変更、パスワード変更）について説明します。
- 運用オペレーター編
  - 対象読者……SSOシステム運用担当者
  - SSOシステムを運用するための機能（ログインID再発行・パスワード再発行）について説明します。
- ツール編
  - 対象読者……SSOシステム運用担当者、業務システム保守担当者、業務システム運用担当者
  - ロールとリソースの関係、ロールと割り当て対象の関係をCSVファイルで一括出力・設定できる導入設定支援ツールについて説明します。

SSO連携方式の概要
【補足】クライアントサーバー型システムにおけるSSO連携上の問題点

- SSOシステムは、端末とサーバー間の通信を確認することで機能を実現しています。そのため、SSOクライアントを全ての通信が通過する必要があります。また、ログアウトや認証エラーの管理のため、SSOシステムでは、CookieやHTTPリダイレクトを利用します。
- 一般的には、Webアプリケーションでは、この前提を満たします。**クライアントサーバー型のシステムでは、この前提を満たしません。**
- リバースプロキシ方式を採用した場合は、ブラウザ/クライアントとサーバー間のすべての通信が、リバースプロキシを通過することで、SSOシステムの機能を実現できます。

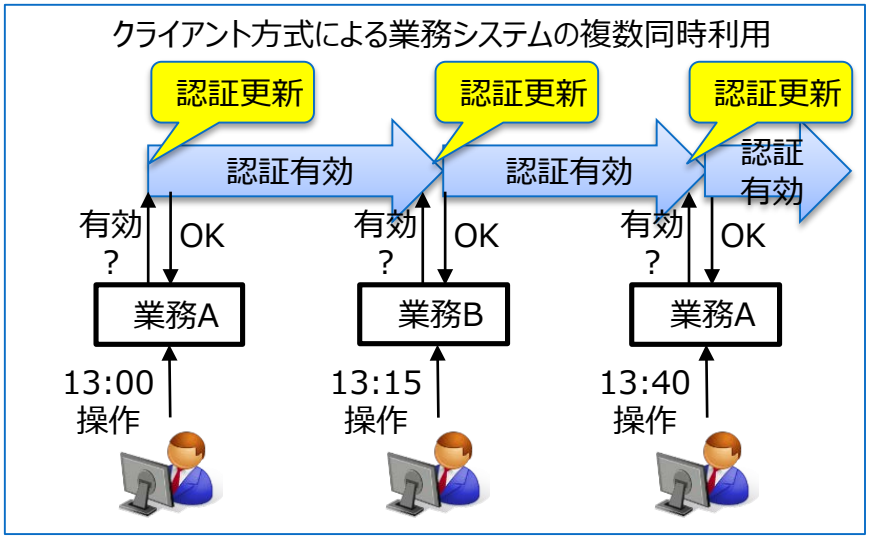


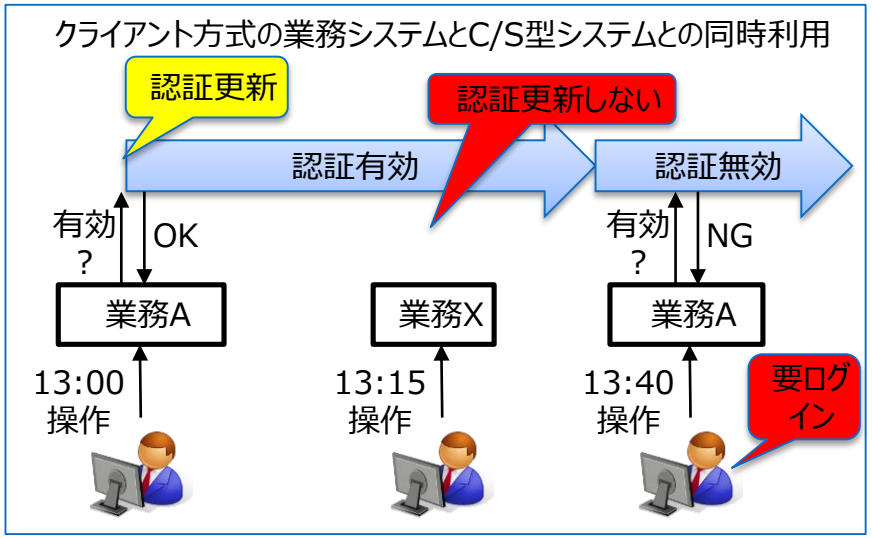
- クライアントアプリとサーバー間の通信が、リバースプロキシを通過しない場合は、通信の確認ができないためSSOクライアントだけでは機能が実現できません。別途作りこみが必要になります。
  - 以下の図は一例。初回ログイン時のみリバプロを通過する方式



SSO連携方式の概要
【補足】SSOシステムの機能が実現できない場合の問題点

- 基盤ポータルを利用している他システムと異なる挙動になり、利用者が混乱する可能性があります。
  - 一例として、SSOには、**「ログイン中のいずれかのシステムを最後に操作してから30分が経過した場合、認証を無効化する機能」**があります。ある業務システムだけ挙動が異なると、以下のような状況が発生します。
    - クライアント方式によるSSO連携を実現した業務システムAと業務システムBを同一端末で利用していた場合、業務システムBを操作していれば、業務システムAが30分以上無操作でも、再ログインせずに利用できます。
    - 一方、業務システムAとクライアントサーバー型の業務システムXを同一端末で利用していた場合、業務システムXを操作していても、業務システムAが30分以上無操作で、その後に操作した場合、再ログインが必要になります。その逆でも同じです。





  - ここで、業務システムAは、操作の都度SSOが処理をして認証情報を記録しています。クライアントサーバー型の業務システムXは、操作の都度SSOが処理できないため、認証情報が無効になります。

横浜市情報共有基盤システム仮想基盤
利用者ガイドライン

第 1.6 版

横浜市総務局住民情報システム課

改訂履歴

版	年月日	氏名	内容
1.0	2016/6/30	日立	新規作成
1.1	2016/7/29	日立	以下の章の 2 次バックアップに関する記載を見直し ・4.6.1 システムバックアップ ・4.6.2 データバックアップ ・4.6.3 ファイルバックアップ
1.2	2017/3/31	日立	・3.1 サービス一覧表の誤記を削除（未提供サービスの削除） ・4.1 仮想マシンテンプレートの OS モジュール構成 について項目を追加 ・4.1 仮想マシンテンプレートのミドルウェア構成 について項目を追加 ・4.1 OS ホスト名の変更は認められない旨の記載を追加 ・4.4.2 監視項目の有効化、無効化 について項目を追加 ・4.4.2 監視項目の「収集」設定について ・4.4.2 監視履歴イベントの保存期間とダウンロード について項目を追加 ・4.5 特記事項一箇所修正（1 次バックアップデータ保存期間と世代について） ・4.5 1 次バックアップの考え方と注意事項 について項目を追加 ・4.5 2 次バックアップの考え方と注意事項 について項目を追加 ・4.7 役割分担表の誤記を修正（システムリストアの担当者） ・6 仮想 LB のセッションタイムアウト間隔に関する記載を追加
1.3	2017/6/9	日立	・4.4 運用管理機能提供サービス Hinemos の同時接続数に関する注意事項を追記
			・4.4.2 監視機能 監視項目から HTTP 監視と HTTP シナリオ監視を削除
			・4.5 バックアップ設定サービス 2 次バックアップに関する運用ルールを追記
			・6 その他制限事項・注意事項 項目の追記
1.4	2017/10/26	日立	・2.3.4 仮想基盤の可用性に関する留意事項を追加 ・6 その他制限事項・注意事項 仮想ロードバランサのセッションタイムアウト間隔に関する記載を見直し
1.5	2018/7/24	横浜市	・4.2 ライセンス提供サービス Oracle Database については、新規のライセンス提供サービスを終了したことを記載した。

1.6	2019/7/23	日立	・3.2 サービス提供時間 業務 LAN1 の記載を削除 仮想基盤業務 SE によるサービス提供時間を訂正 計画メンテナンスの内容を改訂 ・3.3 サービスメニューのリードタイム 誤記修正 ・4.1 仮想マシン提供サービス 仮想化ミドルウェアのバージョン情報を改訂 仮想マシンのリソース変更に関する内容を追記 運用変更に伴い、追加ディスクについては GPT にて提供される旨を追記 ・4.3.1 仮想基盤の内部ネットワーク構成 既存の情報共有基盤システムのサーバ資産事例を"AD 等"から"NTP"に変更 ・4.3.2. 仮想基盤ネットワークと基盤ネットワークの間の通信について "業務 LAN1"の表記を削除 ・4.3.2. 仮想基盤ネットワークと基盤ネットワークの間の通信について 「論理ネットワーク構成の構成例」に記載されているADおよびDNSについては、 「2017 年 11 月のタイミングで仮想基盤側に移行済み」の旨を追記 ・4.3.4 仮想ロードバランサの標準設定値について 新設 ・4.4.2 監視機能 HTTP 監視がサービス提供外となっている理由等を記載 ・4.5 バックアップ設定サービス 1 次バックアップおよび 2 次バックアップの注意事項を改訂 ・5.1.3 セキュリティパッチの適用 内容改訂

内容

1. はじめに

1.1. 本書の位置付け

本書は、横浜市情報共有基盤システム仮想基盤（以下、仮想基盤）において、サービスを利用する側である業務システム事業者が、サービスを利用する前に通読して仮想基盤の概要を理解するためのものです。

1.2. 対象読者

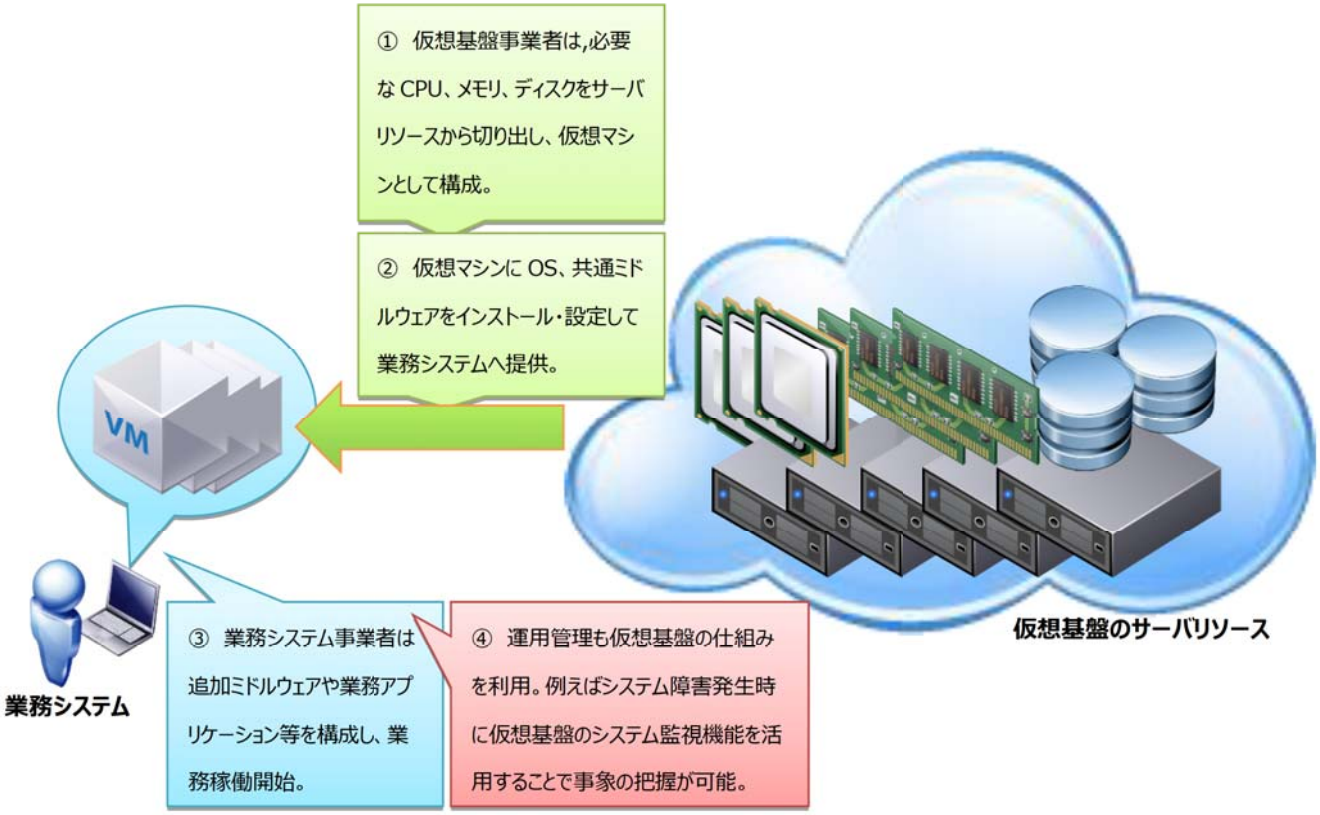
本書は、仮想基盤サービスを利用する業務システム事業者を対象とします。

2. 仮想基盤の概要

仮想基盤とは、基盤システム所管部門が監督し、仮想基盤事業者が運用管理する、業務システム事業者向けのサーバプラットフォームです。これは仮想基盤事業者によるサービス提供型のサーバプラットフォームであることから、プライベートクラウド環境と考えることができます。
したがって、業務システム事業者は、物理的なハードウェア構成やネットワーク構成を意識することなく、仮想基盤が提供する環境上に仮想サーバや仮想ネットワークを構成し、業務システムを稼働させることができます。

また、業務システムとしては、費用面のみならず、ハードウェア構成にかかる一切の労力（物理構成設計、物理環境構築、ハードウェア運用、ハードウェア障害対応、機器リプレース等）を抑えられるため、業務システム関係者はソフト面の構成検討（仮想環境の構成設計、OS やミドルウェアの構成設計）や業務設計、業務運用に集中することができます。その結果として、更なる業務改善や成果を生み出すことが期待できます。

以下の図に、仮想基盤の利用イメージを示します。



2.1. サービス提供範囲

仮想基盤のサービス提供範囲とその概要について、各レイヤーのイメージ図を以下に示します。

・仮想基盤は業務システムに対して、OS・バックアップ機能・ジョブ機能・監視機能を標準で提供します。

・ウイルス対策については、基盤システムからの提供となります。

・Oracle Database については、「導入する・しない」の選択に加え、冗長化構成(RAC 構成を採用する・しない)についても業務システム事業者にて選択可能です。なお、仮想基盤からはライセンス提供のみとなるため、導入設計・インストールから運用に至るすべてのプロセスを業務システム事業者にて実施することになります。

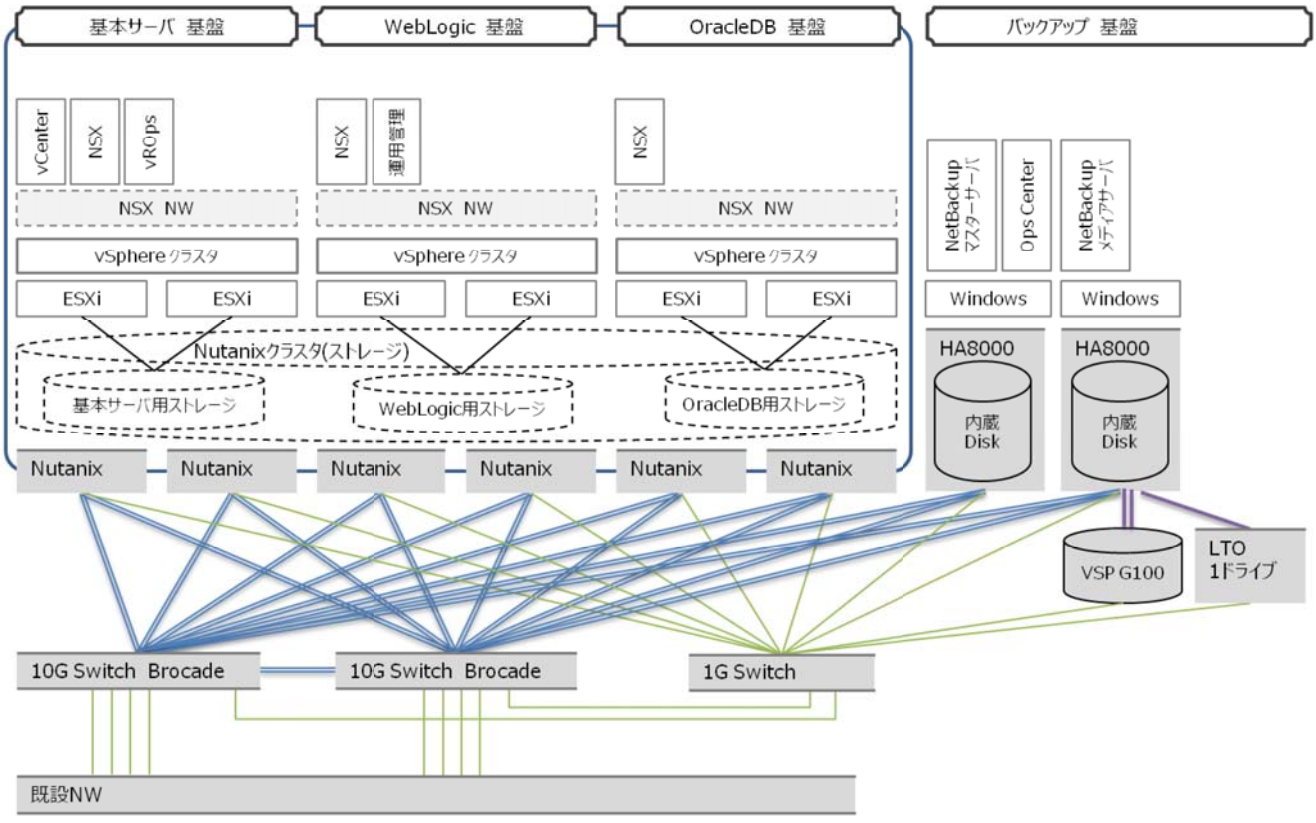
各サービス内容の詳細を、3 章・4 章に示します。

2.2. 仮想基盤の仕組み

仮想基盤では、業務システムに必要となる仮想マシンリソースを提供します。その業務システムに提供するリソースは、仮想基盤全体の中から、対象の業務システムに対して必要な分だけ、物理リソースやミドルウェア環境の一部分を割り当て・払い出す運用となります。つまり、他の業務システムとリソース共有するマルチテナント構成であり、一般的なプライベートクラウド環境となります。
クラウド環境である以上どうしても、オンプレミス環境とは異なり利用に際してはいくらかの制約が生じますが、標準的なシステム構成であれば充足できる内容です。次節より、仮想基盤の仕組みについて説明します。

2.2.1. 仮想基盤のシステム構成

以下の図に、仮想基盤の構成イメージを示します。図を見て分かるとおり、仮想環境と物理環境が混在する構成となっています。この構成は 4 つの基盤と NW 環境に分けて考えることができます。４つの基盤については次節にて説明します。
なお、ハイパーバイザーから下の層は、仮想基盤アプライアンス(図中の Nutanix)により構成されていますが、仮想基盤を利用するにあたって業務システム事業者が意識する必要は無いため、説明を割愛します。



2.2.2. 仮想基盤で用意する４つの基盤

仮想基盤では、ハイパーバイザーに VMware ESXi を採用しています。そのハイパーバイザー上には、VMware vSphere クラスタを３つ構成しています。その３つの VMware vSphere クラスタは用途に応じてそれぞれ、「基本サーバ基盤」、「WebLogic 基盤」、「Oracle DB 基盤」として位置付けています。また、VMware vSphere クラスタとは別に、物理サーバから構成されるバックアップ基盤を用意しています。

業務システム事業者は、それぞれの基盤の用途・機能を理解し、用途に応じて必要な仮想マシンリソースやミドルウェア設定を設計し、利用内容を申請してください。仮想基盤では、業務システム事業者からの申請に基づき、各基盤上に仮想マシンを構築します。以下に、仮想基盤が提供する４つの基盤について示します。

No	基盤名	説明
1	基本サーバ基盤	＜仮想基盤の提供機能＞ ・仮想マシン管理機能(vCenter) ・リソース管理機能(vROps) ＜仮想マシン（業務システム用）配置の考え方＞ ・Windows Server 2012 を使用する仮想マシン ・WebLogic 基盤および Oracle DB 基盤に所属しない仮想マシン
2	WebLogic 基盤	＜仮想基盤の提供機能＞ ・仮想マシン管理機能(vCenter) ・運用管理サーバ（Hinemos による監視機能、ジョブ機能） ＜仮想マシン（業務システム用）配置の考え方＞ ・RHEL6.7/7.1 を使用する仮想マシン ・RHEL 系 OS 上で Oracle WebLogic Server を使用する仮想マシン ・RHEL 系 OS 上で JBoss EAP を使用する仮想マシン
3	Oracle DB 基盤	＜仮想基盤の提供機能＞ ・仮想マシン管理機能(vCenter) ・Oracle ライセンス提供(機能提供無し) ＜仮想マシン（業務システム用）配置の考え方＞ ・RHEL6.7 上で OracleDatabase を使用する仮想マシン
4	バックアップ基盤	＜仮想基盤の提供機能＞ ・バックアップ機能（NetBackup） ・リストア機能（手動） ・バックアップ・リストア用管理コンソール機能(OpsCenter)

2.3. 仮想基盤の可用性

仮想基盤の構成は、物理・仮想を問わず、業務システムの稼働に影響を及ぼす可能性がある部位については、原則として冗長化構成を採用しています。基本サーバ基盤、WebLogic 基盤、Oracle DB 基盤において、業務システムが稼働する部分が対象となります。
仮想基盤における高可用性(vSphere HA：High Availability)とホストアフィニティ設定に関する基本的な考え方は、次に示すとおりです。

- HA (High Availability)
  Oracle DB サーバ（シングルインスタンス構成）のように、1 台構成の仮想サーバに対して適用する。
- ホストアフィニティ
  Oracle RAC 構成時の各 DB サーバを別の ESXi 上で起動するように設定する 。

その一方で、業務システムの稼働部分以外ではサービスダウンの可能性があることに注意してください。具体的には、バックアップ機能が該当します。
また、監視機能・ジョブ機能や仮想マシン管理機能を提供しているサーバについてはホットスタンバイ構成とはなっていないため、障害時には一時的にサービスダウンすることになります。
以下に、業務システム稼働部分における冗長化構成の詳細について示します。

2.3.1. 仮想マシンの冗長化構成

業務システムに提供する仮想マシンについては、ハイパーバイザーのクラスタ機能である vSphere HA(vSphere High Availability)により冗長化を実現します。ハイパーバイザーまたはハードウェアで障害が検出された場合は、自動的に異なる物理サーバに仮想マシンを移動して再起動させることで、業務システムの停止時間を最小限に抑えることができます。
（仮想マシンの OS ハングアップ等の仮想マシン自体の障害時には HA は実行されません）

2.3.2. Oracle Database の冗長化構成

Oracle Databaseについては、Oracleのクラスタ機能である「Oracle Real Application Cluster(以下、Oracle RAC)」により冗長化を実現することが可能です。ハイパーバイザーやハードウェアで障害が検出された場合に加え、DB インスタンス障害や仮想マシン自身の障害時に正常稼働している物理サーバ側へサービス提供場所を引き継ぐことで、業務システムの停止時間を最小限に抑えることができます。

2.3.3. ハードウェアの冗長化構成

ハードウェアについては、Nutanix 社の仮想基盤アプライアンスを採用しています。詳細については業務システム事業者が意識する必要は無いため割愛しますが、この製品機能により、ファイルシステム※1、ネットワーク（NIC）、電源について、冗長化構成を実現しています。

※1 1 台の Nutanix ノードにおいては HDD の冗長化は採用していないが、Nutanix CVM にて別の Nutanix 筐体内の HDD にデータを二重書き込みする仕組みとなっている。仮想基盤においては 6 台の Nutanix にて構成することによりデータ記憶装置の冗長化を実現している。

2.3.4. 仮想基盤の可用性に関する留意事項

仮想マシンが稼動しているESXi（物理サーバ）にて障害が発生した場合、2.3.1に記載のとおりVMware HAが発生し、異なるESXi（物理サーバ）にて当該仮想マシンのOSが自動的に起動されます。VMware HAの機能においてサポートされるのは「仮想マシンのOS起動まで」となります。業務システムのサービス再開にあたって「OS起動 ＋ 何らかのサービス起動やツールの実行が必要」となる場合、VMware HA だけでは「業務システムの復旧」とはなりません。業務システムのアーキテクチャに応じた最適な障害復旧方式・手順を策定してください。

3. サービス内容

3.1. サービスメニュー

サービスメニューとその概要について、以下の一覧に示します。サービスメニュー各項目の詳細につきましては、4 章に記載します。

No	サービスメニュー	サービス概要
1	仮想マシン提供サービス	・利用申請書および受入申請書に基づいた仮想マシンの提供 ・各サービス用アカウントの提供
2	ライセンス提供サービス	・Oracle Database についてのライセンス提供 （ライセンス提供のみであり、環境提供や作業支援はありません。）
3	ネットワーク提供サービス	・利用申請書および受入申請書に基づいた仮想ネットワーク環境の提供 （ルータ、ロードバランサ、ファイアウォールの設定）
4	バックアップ設定サービス	・バックアップ設定申請書に基づいたバックアップポリシーの設定
5	バックアップ・リストア機能提供サービス	・OpsCenter 経由の NBU バックアップジョブ実行環境の提供 ・OpsCenter 経由の手動リストア環境の提供
6	運用管理機能提供サービス	・申請に基づいた Hinemos 監視設定 ・Hinemos によるジョブ実行環境の提供
7	システムリストア支援サービス	・システムリストア申請書に基づいたシステムリストア時の作業支援（必須） （データリストアやファイルリストアといったシステムリストアに該当しない場合、本サービスの利用は不可）

3.2. サービス提供時間

仮想基盤の利用時間については、以下に示すとおり、機能面とサービス面という 2 つの視点があります。

- 機能面（仮想基盤の環境、機能）における利用時間
  基本方針として、仮想基盤の環境停止は実施せず、機能としては 24 時間提供します。
  ただし、保守作業時や計画停止時間を除きます。
  この他に、基盤ネットワーク（業務 LAN2、管理 LAN1）が停止する場合、仮想基盤も事実上の停止と同様の状態となり、機能提供ができません。

- サービス面（仮想基盤業務 SE の作業）における利用時間
  仮想基盤業務 SE によるサービス提供（作業）については、原則として平日 8:30～17:15（土日休日を除く）の範囲に限ります。

次に、サービス停止とその際の周知方法について示します。
仮想基盤においては、基盤環境の安定稼働を目的として、定期的なメンテナンスの実施を計画しています。その際、メンテナンスの内容次第では、**サービス停止を伴う場合**があります。
以下に、定期メンテナンスの年間スケジュールについて示します。

No	種別	内容・注意事項・周知方法など
1	計画メンテナンス	・四半期に一度のサイクルで実施します。 ・具体な実施日（年間スケジュール）は、毎年 4 月頃に基盤システム所管部門より周知します。 **・業務システムの稼働計画として、必ず考慮してください。** **（特に OS・ジョブ・監視などの停止処理と再開処理）** ・予め仮想マシンの停止が必要となる場合があります。その際は各業務システム事業者による停止・起動作業が必要となります。
2	臨時メンテナンス	・不定期に実施します。 ・主に以下理由により発生することを想定しています。 ①仮想基盤のハードウェア/ソフトウェア障害対応 ②緊急度合い、深刻度合い、セキュリティリスクの高いパッチ適用など **・内容次第では、各業務システムのサーバに対してもパッチ適用が必要となる場合があります。（各業務システム事業者による対応をお願いします）** ・実施する際は、基盤システム所管部門より事前にご連絡します。 ・予め仮想マシンの停止が必要となる場合があります。その際は各業務システム事業者による停止・起動作業が必要となります。

3.3. サービスメニューのリードタイム

各サービスメニューのリードタイム（申請受領からサービス提供開始までの期間）について、以下の表に示します。
複数の業務システム事業者からの依頼が重複する場合もあるため、記載内容は目安であり、サービス提供完了までの期間を確約するものではありません。
また、記載している日数は受付日を含みません。

<table>
<tr><th rowspan="2">No</th><th rowspan="2">サービスメニュー</th><th colspan="2">リードタイム</th></tr>
<tr><th>新規提供
（仮想マシン 8 台あたり）</th><th>追加・変更
（仮想マシン 1 台あたり）</th></tr>
<tr><td>1</td><td>仮想マシン提供サービス</td><td rowspan="3">11 開庁日以内
（受入申請書の内容についての疑義事項がすべて解消された日を起点とします）</td><td rowspan="2">2 開庁日以内</td></tr>
<tr><td>2</td><td>ライセンス提供サービス</td></tr>
<tr><td>3</td><td>ネットワーク提供サービス</td><td>個別調整</td></tr>
<tr><td>4</td><td>バックアップ設定サービス</td><td rowspan="2">2 開庁日以内
（バックアップ設定申請書の内容についての疑義事項がすべて解消された日を起点とします）</td><td rowspan="2">1 開庁日以内</td></tr>
<tr><td>5</td><td>バックアップ・リストア機能提供サービス</td></tr>
<tr><td>6</td><td>運用管理機能提供サービス</td><td>4 開庁日以内
（運用管理基盤設定申請書の内容についての疑義事項がすべて解消された日を起点とします）</td><td>1 開庁日以内</td></tr>
<tr><td>7</td><td>システムリストア支援サービス</td><td colspan="2">システムリストア申請書受理後、作業依頼日に実施
（5 開庁日前までの依頼を基本とする）</td></tr>
</table>

「新規提供」は、業務システム事業者が仮想基盤で初めて環境を構築する場合を想定しています。仮想マシン台数が目安を超える場合は、8 台ごとに 2 倍、3 倍のリードタイムを見込んでください。
また、「追加・変更」の依頼は、業務システムの仮想環境一式を提供した後に、追加で依頼があった場合を想定しています。

4. サービスの詳細内容

4.1. 仮想マシン提供サービス

仮想マシン提供サービスでは、利用申請書および受入申請書に基づき、仮想マシン、ディスク構成、OS、ミドルウェアおよび各操作に必要なアカウントを標準サービスとして提供します。（申請内容の詳細については、「仮想マシン提供サービス　利用申請書」をご確認ください。）

- 仮想マシン

  仮想マシンについては、原則として予め用意してある標準構成テンプレートを利用していただきますが、システム要件および必要性に応じて、個別に対応することが可能です。

  本サービスで提供する仮想マシンの標準構成は以下のとおりです。

  【仮想マシンテンプレート一覧】

No	種別	OS/ミドルウェア	CPU	メモリ	HDD※
1	Windows テンプレート	Windows Server 2012 R2 Standard	2 コア	8GB	100GB
2	RHEL7.1 テンプレート	Red Hat Enterprise Linux 7.1	2 コア	8GB	100GB
3	RHEL7.1 + JBoss テンプレート	・Red Hat Enterprise Linux 7.1 ・JBoss EAP 6.4	2 コア	8GB	100GB

※ システム領域のみ

例えば、仮想基盤では以下の種別の OS を用意していますが、以下の OS 群では要件を満たさない場合、OS 無しで仮想マシンを提供することも可能です。その際は、OS のインストール作業から業務システム事業者にて実施いただくことになります。

<予め用意している仮想マシンテンプレート>

・Windows Server 2012 R2
・RHEL 7.1
・RHEL 7.1 + JBoss EAP 6.4

◆Windows 仮想マシンの標準テンプレートにディスク構成を追加する場合
・未割り当てのディスクが OS から確認可能となる状態で提供します。
・フォーマット、ドライブレター割り当ては業務システム事業者にて実施してください。
・ディスクサイズに関係無く、パーティションタイプは GPT となります。

<提供可能となる OS>

・Windows Server 2012 R2
・RHEL 6.7 ※1
・RHEL 7.1

◆RHEL 仮想マシンの標準テンプレートにディスク構成を追加する場合
・ファイルシステム作成までを実施した状態で提供します。
・fdisk、マウントポイント作成は業務システム事業者にて実施してください。

※1　RHEL6.7 は Oracle Database 12c をインストールして使用することを前提として用意しています

- 仮想マシンテンプレートの OS モジュール構成

  ・RHEL7.1 テンプレート、および RHEL7.1+JBoss テンプレートについては、テンプレート作成時点に（2016 年 1 月）おいてリリースされている RPM を適用しています。適用されている RPM については、OS テンプレートの定数設計書を確認してください。

  ・Windows テンプレートに構成されている役割、および機能については OS テンプレートの定数設計書を確認してください。なお、セキュリティパッチ等は仮想マシンが提供された後、実機にてご確認ください。

- 仮想マシンテンプレートのミドルウェア構成

  前述（2.1 サービス提供範囲）のとおり、仮想マシンには仮想基盤で必要となるミドルウェアの一部が標準でインストール済みの状態で提供いたします。
  標準でインストール済みのミドルウェアについて、以下に示します。

  ・各テンプレートにインストール済みのミドルウェア：Hinemos エージェント、NBU クライアント、アンチウイルスソフト
  ・RHEL7.1+JBoss テンプレート にのみインストール済みのミドルウェア：上記ソフトウェア ＋ JBoss6.4

  なお、Oracle DB サーバとして使用される仮想マシンについては Hinemos エージェント、NBU クライアントを予めインストールした状態で提供いたします。Oracle Database ならびにアンチウイルスソフトのインストールは業務システム事業者にて実施いただく必要があります。

- 仮想マシンのホスト名

  仮想マシンのホスト名は以下の 2 種類が存在します。
  ・仮想マシンホスト名　：　vCenter で管理する際に使用する名称
  ・OS ホスト名　　：　仮想マシンにインストールした OS にて管理する名称

  OS ホスト名については資料「横浜市　情報共有基盤システム　ホスト名　命名規則」に従って仮想基盤事業者にて設定します。OS ホスト名の変更は認めません。変更した場合は仮想基盤のサポート対象外となります。

  なお、「VIP 用ホスト名（RAC 用 VIP）」、「SCAN 用仮想ホスト名（RAC 用 SCAN）」については Oracle DB にて設定・管理する名称となるため、命名規則にしたがい業務システム事業者にて設定いただくものになります。

- アカウント

  仮想マシン払い出しの時点において、仮想マシンの OS やミドルウェアで使用するアカウントについては、業務システム事業者が環境構築作業を開始するにあたって必要最小限となるものを組み込んでいます。環境構築にあたって追加で必要となるアカウントについては、業務システム事業者にて任意に追加が可能です。

  予め付与するアカウント種別、アクセス方式、操作内容等の考え方については、「5.3 章　仮想マシンへの接続方式と使用アカウント」を参照してください。

- 仮想化ミドルウェア

  仮想マシン提供に関連する VMware 社のミドルウェアのバージョンは以下のとおりです。
  なお、製品不具合への対応等でバージョンアップを行う可能性があります。
  適用しているバージョンについては基盤システム所管部門までお問い合わせください。

No	ミドルウェア	バージョン
1	VMware ESXi（VDI 基盤以外）	6.0 Patch 3(4192238)
2	VMware ESXi（VDI 基盤）	6.0 Express Patch4(3247720)
3	vSphere Client	6.0.0
4	NSX for vSphere	6.3.1

- 仮想マシンのリソース変更

  払い出した仮想マシンを運用する過程において、リソースの過不足が生じた場合、その理由および希望するリソース値を基盤システム所管部門に報告し承諾を得てください。基盤システム所管部門による承認を得た後に、所定の様式（「仮想マシンリソース変更申請書」）を使ってリソース変更申請をしてください。

  【仮想マシンのリソース変更に関する留意点】

  ・リソース変更時は業務システム事業者にて対象となる仮想マシンを停止いただく必要があります
  （仮想マシンを起動したままでのリソース変更については運用ルール上、対応していません）

  ・既にファイルシステムを作成・割当しているディスクについては、容量を減らすことができません。

  ・システム領域として使用している VMDK ファイルのディスク増量については OS レベルでの不具合が生じる可能性があります。その場合、業務システム事業者の責任にて対応いただくことになります。リスクを考慮して要否を検討してください。

  ・Linux 系 OS の仮想マシンに対するメモリの増量に伴い、SWAP 領域の見直しが必要となる場合は業務システム事業にて対応してください。

4.2. ライセンス提供サービス

※Oracle Database のライセンス提供サービス（新規）は、2017 年 12 月 31 日を持ちまして終了いたしました。

仮想基盤では、OS と Oracle Database のライセンスを提供します。ライセンスを提供する OS ならびに Oracle Database のバージョンは、以下のとおりです。

- Red Hat Enterprise Linux 6.7
- Red Hat Enterprise Linux 7.1
- Windows Server 2012 R2 Standard
- Oracle Database 12c Release1（Oracle Database Standard Edition（12.1.0.1））
  ⇒新規利用者へのライセンス提供は行っておりません。
- Red Hat JBoss Enterprise Application Platform 6.4

仮想基盤において利用を許可する OS とミドルウェアの組み合わせは以下のとおりです。

		OS		
		RHEL6.7	RHEL7.1	Windows2012
ミドルウェア	Oracle DB 12c	○	×	×
	JBoss EAP 6.4	○※1	○	×

※1 RHEL6.7 に JBoss EAP 6.4 をインストールして利用した場合、JBoss のインストールは業務システム事業者にて実施いただくことになります。また JBoss EAP 6.4 のインストールにあたって必要となる前提パッケージ等についても業務システム事業者にて入手および適用いただくことになります。

以下に該当する場合は、事前に基盤システム所管部門に問合せをしてください。

・別バージョンの Oracle Database の使用を希望している場合

・Windows 系のサーバに Oracle Database をインストールする場合

4.3. ネットワーク提供サービス

仮想基盤では、仮想基盤の LAN 構成以外にも、既存環境や外部ネットワークとの接続を考慮したネットワークで構成されています。次節より、その詳細を示します。

4.3.1. 仮想基盤の内部ネットワーク構成

仮想基盤内部のネットワーク構成は、用途ごとにセグメントを分割して構成しています。
各セグメントの内部は、必要に応じて業務システムごとに IP アドレス体系をサブネットマスクで区切り、デフォルトゲートウェイ(Default GW)として各サブネットの末尾 IP アドレスを利用するネットワーク構成です。
なお、業務システムで使用する仮想マシンの IP アドレスは、仮想基盤より払い出しをします。

物理ネットワークでは、既存ネットワークとの接続を考慮し、VLAN 構成については既存の基盤ネットワークの設計方針を踏襲します。また、仮想ネットワークで利用する VLANID は、既存 VLAN の ID と重複しないものとします。

以下の表に、各ネットワークセグメントの用途について示します。

No	名称	ネットワーク用途
1	インフラセグメント	仮想基盤・仮想ネットワーク管理用サーバ群を設置し利用 (vCenter、VMware NSX Manager 等)
2	ルーティングセグメント	既存の基盤 NW とのルーティング接続ポイントとして利用
3	サービスセグメント	各サービスを提供するサーバ郡を設置し利用（バッチサーバ等）
4	バランシングセグメント	ロードバランサで負荷分散されるサーバ郡を設置し利用 (Web サーバ等)
5	AP サーバセグメント	AP サーバ設置セグメント、WEB サーバ～AP サーバ間で利用
6	DB サーバセグメント	DB サーバ設置セグメント、AP サーバ～DB サーバ間で利用
7	DB インターコネクト	DB 間インターコネクト、DB 冗長化用セグメントとして利用
8	RMAN セグメント	RMAN バックアップで利用
9	番号用 LGWAN セグメント	LGWAN 接続経路で利用
10	FW セグメント	LGWAN 接続 FW の FW 間で利用
11	制御通信セグメント	物理機器のハードウェア管理に利用(Nutanix、HA8000 等)
12	モニタリングセグメント	仮想基盤監視用のセグメント 各サーバを収容し、監視及び NBU バックアップの通信で利用

次に、仮想ネットワークとしての構成について示します。
仮想マシンはマルチテナントの考えに従って環境を払い出す構成ですが、VMware NSX(ネットワーク仮想化プラットフォーム、以下 NSX)についても同様に、業務システム単位で"仮想ルータ（Edge GW）"、"仮想 LB(Edge LB)"、"分散 FW(DFW)"を配置します。

仮想基盤としては、既存の情報共有基盤システムのサーバ資産（NTP）を利用するため、既存の基盤ネットワークへの接続が必要となります。その際は、trunk VLAN または access VLAN で接続し、基盤ネットワークおよび LGWAN への通信を可能とします。

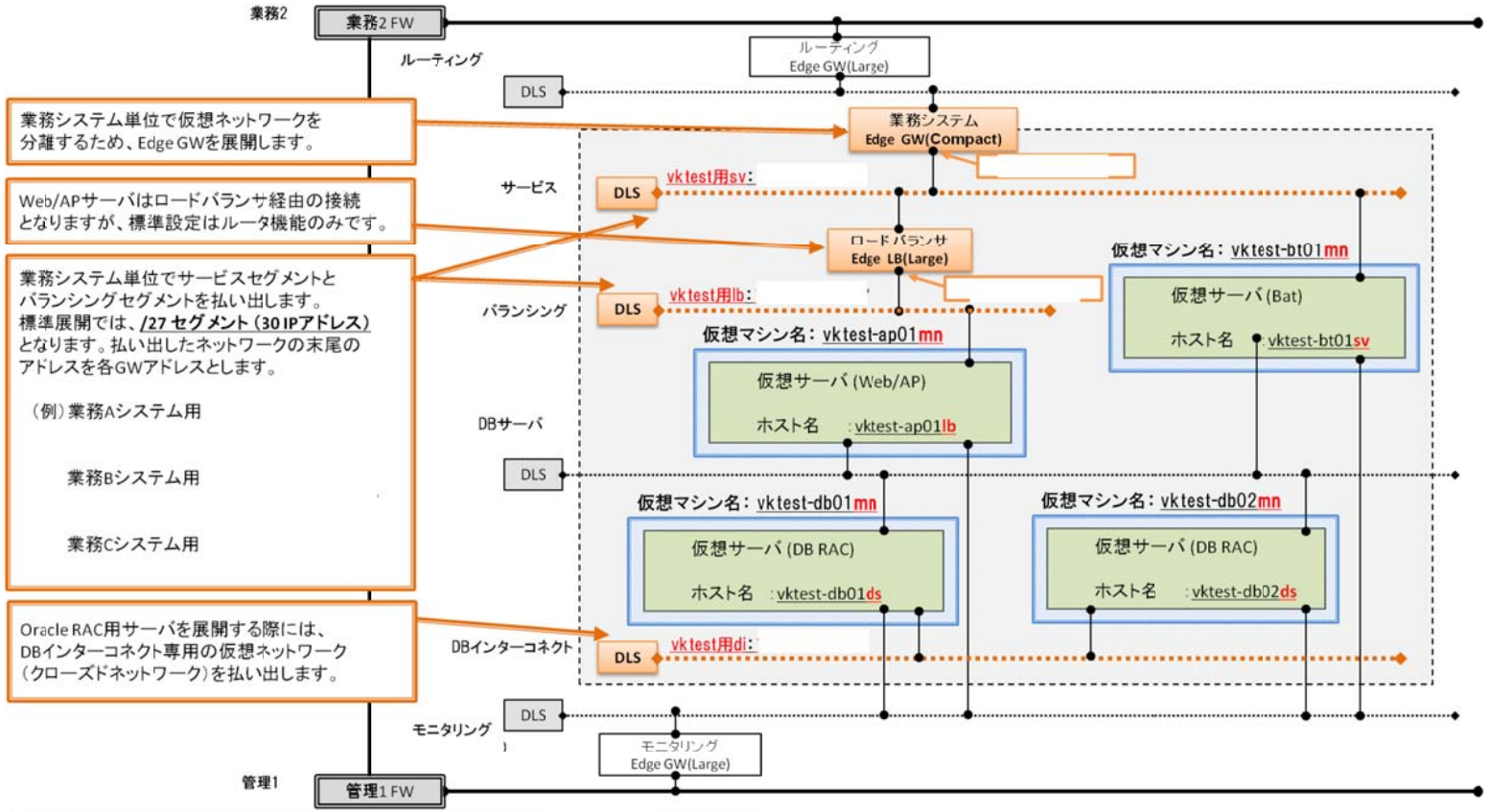
また、業務システム側の要件に応じて、仮想基盤には本番環境以外に保守・開発環境および研修環境を提供することが可能です。その際、仮想 LB のアプライアンスとしては原則として、"本番環境"と"本番環境以外"という考え方で配置をします。本番環境以外は同一の仮想アプライアンスにて複数の VIP を持つ構成とすることでリソースを有効活用します。（ただし、要件および必要性があれば、本番、保守・開発、研修の 3 環境に各々のアプライアンスを設置することが可能です。）

次項では、仮想基盤の本番環境における論理ネットワークの標準構成、および構成例を示します。

4.3.2. 仮想基盤ネットワークと基盤ネットワークの間の通信について

仮想基盤の一部のネットワークセグメントについては、既存の基盤ネットワーク（業務 LAN2、管理 LAN１）との通信が可能な構成となっています。
実現にあたっては仮想マシンに対するスタティックルートの設定が必要になります。仮想マシンに設定するスタティックルートの内容は利用申請書の内容を踏まえ仮想基盤事業者にて設定案を検討します。業務システム事業者による内容確認を経て仮想マシン払い出し時に仮想基盤事業者にてスタティックルートの設定を行います。
なお、仮想マシン払い出し後に新たな通信要件として既存の基盤ネットワークに所属するサーバとのネットワーク接続が必要となった場合は業務システム事業者にてスタティックルート設定を実施いただくことになります。

- 業務システム向け標準仮想ネットワーク展開内容と追加オプション（制約事項）



追加オプション（制約事項）について

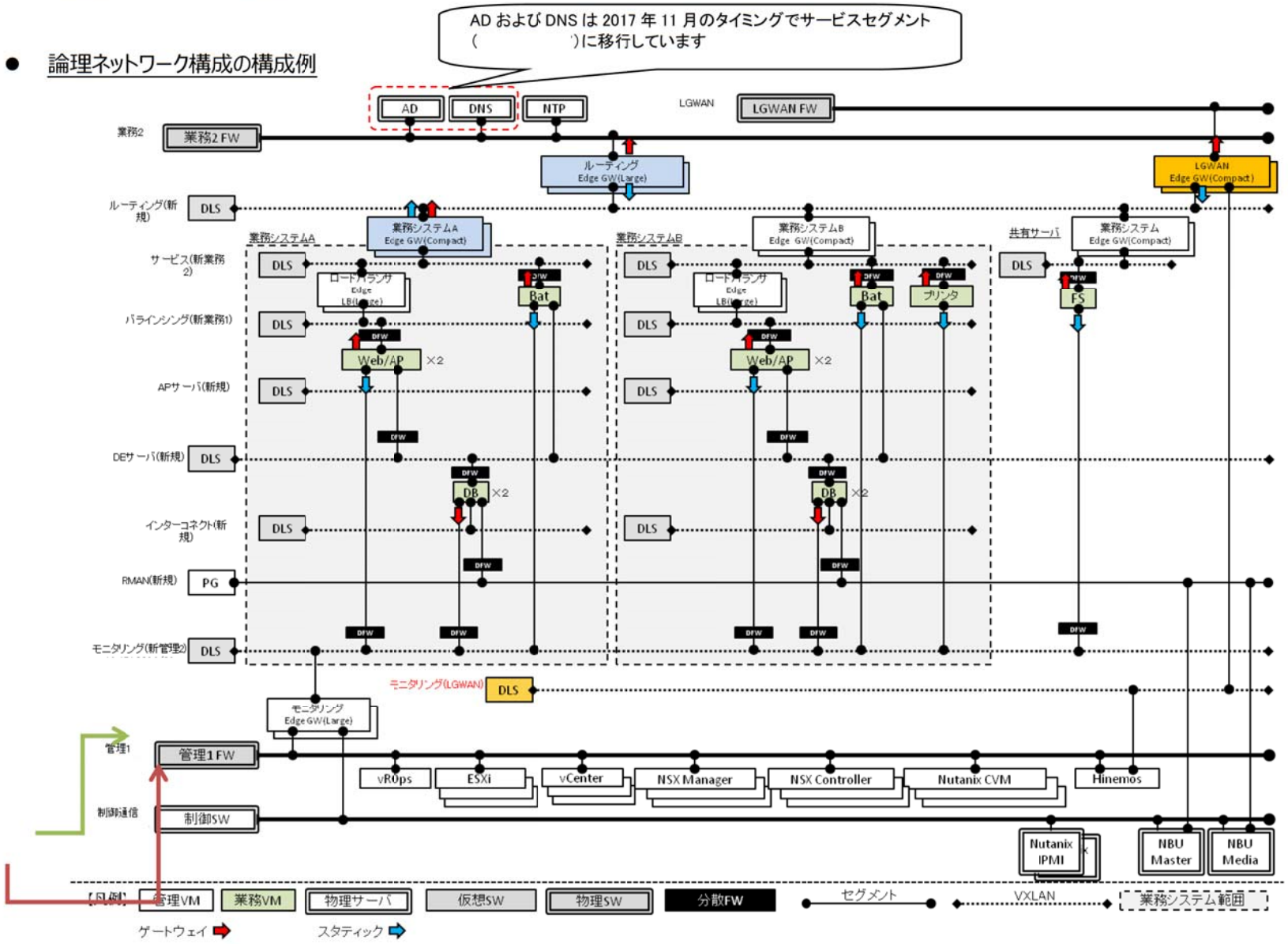
標準仮想ネットワーク展開においては、ルーティング、ロードバランサ、ファイアウォール設定について以下の制約と追加オプションがあります。

（1）ルーティング　：　のネットワークアドレスと接続する場合は確認が必要です。
　　業務システムとして上記IPアドレスと通信が必要な場合は、個別に通信要件のヒアリングと設定が必要となります。

（2）ロードバランサ　：ロードバランサの機能を持たないルータとなります。バランシング機能を有効化する場合は、別途、要件のヒアリングが必要です。

（3）ファイアウォール：標準展開時はフィルタールールを定義していません。
　　本番稼働開始時はフィルターを有効化するため、解放が必要な通信要件をご提示ください。設定は個別調整となります。

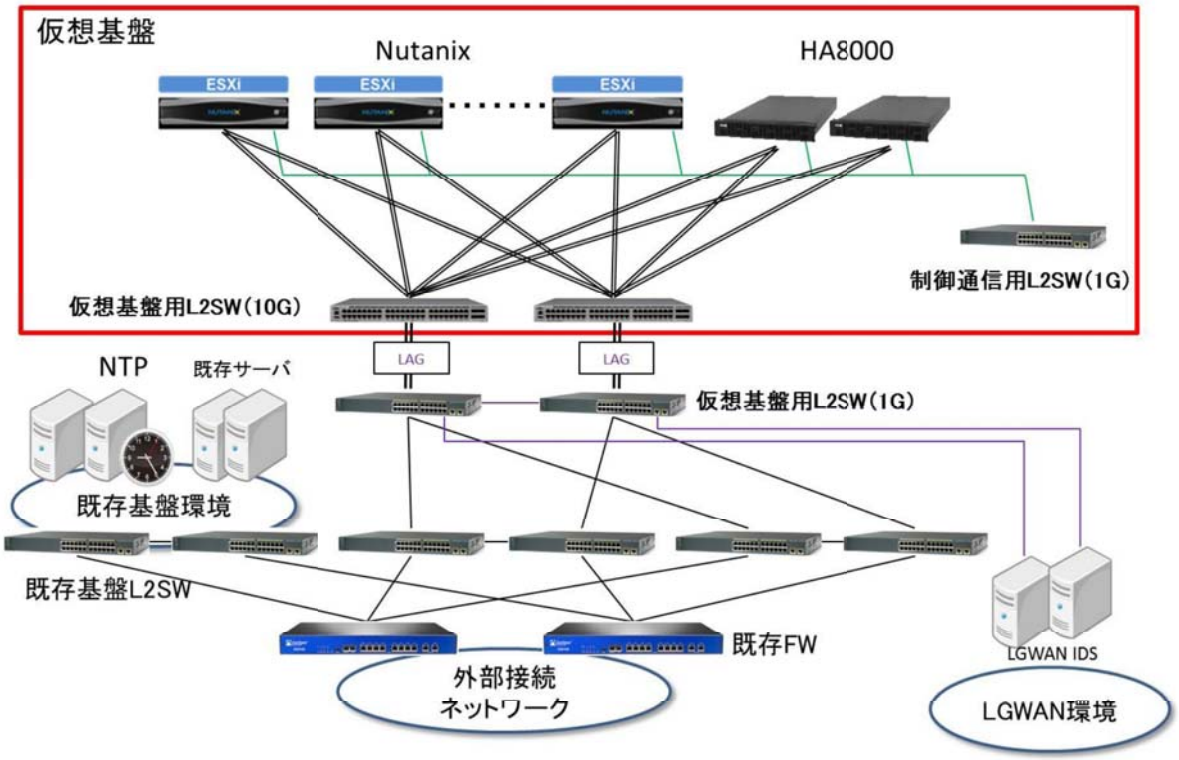
- 論理ネットワーク構成の構成例



4.3.3. 既存環境・外部ネットワークとの接続

仮想基盤の本番稼働開始後は、多数の業務システムが移行され、また、新規の業務システムも受け入れていくことが予想されます。
特にネットワーク構成については、既存環境（情報共有基盤システム等）と仮想基盤との接続に親和性を持たせた方式とすることで、既存環境資産（NTP 等）との連係を図るとともに、既存環境にあるシステムのうち、将来的に仮想基盤への移行を計画しているシステムにおいても従来の機器やシステムとの通信が可能なものとなっています。

以下の図に、仮想基盤と既存環境、外部ネットワークとの接続について、概要を示します。



4.3.4. ロードバランサの標準設定値について

ネットワーク提供サービスにて提供するロードバランサ（仮想アプライアンス）の標準設定値は以下の通りです。
設定内容については変更できないため、業務システム事業者はこの点を考慮してシステム方式設計を行ってください。

No	項目	設定値	備考
1	負荷分散方式	ラウンドロビン	
2	パーシステンス方式	ソース IP	
3	パーシステンスタイムアウト間隔	3,600 秒	
4	セッションタイムアウト間隔	300 秒	NSX Edge6.2.1 の場合
5	サービス監視間隔	5 秒	
6	サービス監視試行回数	3 回	
7	X-Forwarded-For-HTTP ヘッダ	有効	
8	IP アドレス透過有無	非透過	・仮想 LB 配下のサーバは接続元 IP アドレスを認識できない ・アクセスログの取得等、接続元クライアントの IP アドレスが必要となる場合は、サーバ側で X-Forwarded-For（XFF） HTTP ヘッダを用いること

4.4. 運用管理機能提供サービス

仮想基盤では、運用管理の機能として、Hinemos によるジョブ機能およびシステム監視機能をサービスとして提供します。ジョブ機能の利用に際しては、業務システム事業者にてジョブネットの作成・登録が必要となります。監視機能の利用についても、業務システム事業者で監視設定内容を予め検討・決定のうえで仮想基盤側へ設定依頼の申請を行うことが必要です。

なお、本サービスを提供しているサーバ（運用管理サーバ）については予め待機系のサーバを配置するといった冗長化構成は採用されていません。したがって、運用管理サーバにて障害が発生することにより、サービスが一時的に提供できなくなる場合がありますので留意してください。

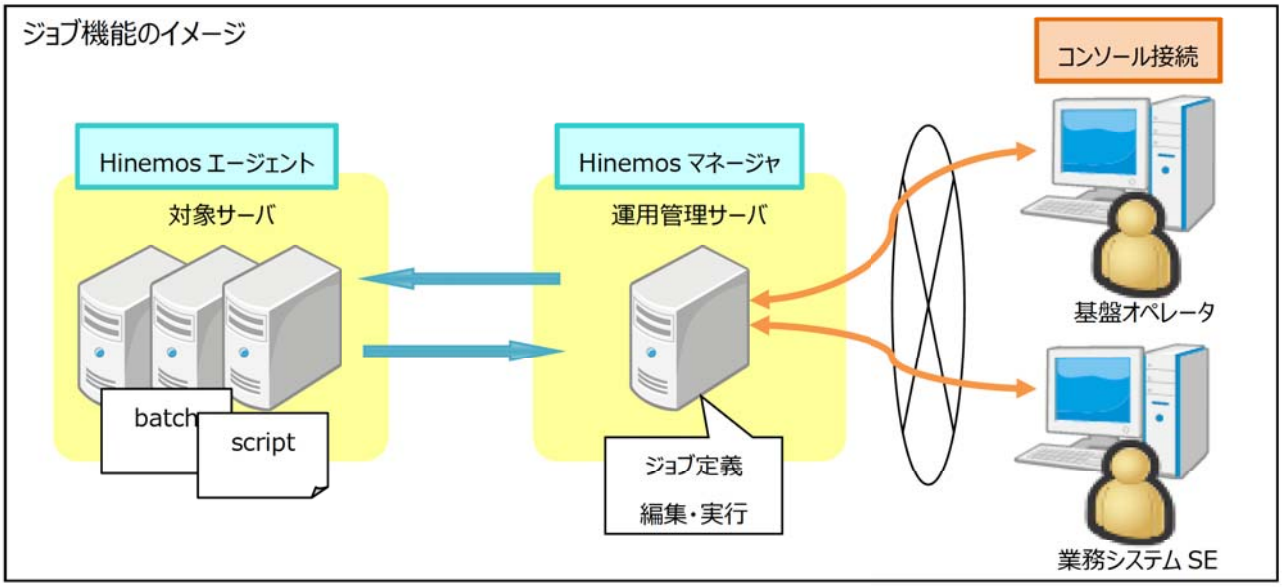
- Hinemos マネージャにログインする際のアカウント
  業務システムごとに、管理者権限を持ったユーザを提供します。
  原則として、こちらのアカウントを使用してください。
- Hinemos マネージャへのログイン数について
  製品仕様上、許可される同時接続数が 32 となります。
  運用管理基盤については、各業務システム事業者にて使用するものであるため、1 つの業務システムにつき同時使用する PC は 2 台以下とするようにしてください。Hinemos を使用しないときのこまめなログアウトを心がけるようにしてください。

4.4.1. ジョブ機能

運用管理機能の１つとしてサービス提供するジョブ機能は、提供した直後の段階では、サービス提供対象の業務システム用のジョブユニットのみ準備されている状態です。操作権限を持った管理コンソールとそのアカウントを提供しますので、業務システム事業者にてジョブ運用およびスケジュール運用を設計し、ジョブネットを定義・作成してください。
また、ジョブの実行を基盤オペレータに依頼する場合、対象となるジョブの概要や異常終了時の取り扱いをルール（内容は基盤システム所管部門に確認してください）に従って資料として準備し、基盤オペレータに引継いでください。

なお、前述のとおりジョブ環境に障害が発生した際は、サービス利用ができません。したがって復旧するまでの間は、業務システムとして、ジョブの手動実行（バッチファイルやスクリプトの手動実行等）や後日に行うリカバリ対応プランなど、回避策を必ず考慮しておいてください。

ジョブ機能の概要について、以下の図に示します。



- Hinemos 環境でジョブ実行する際のアカウント
  ジョブの実行ユーザとして、以下のユーザを割り当てています。
  Windows サーバ：
  RHEL サーバ　：
  上記ユーザ以外をジョブ実行ユーザとして設定したい場合、基盤システム所管部門までご相談ください。

4.4.2. 監視機能

運用管理機能としてサービス提供する監視機能の利用にあたっては、業務システム事業者にて各サーバの監視設計を行い、監視要件を運用管理基盤設定申請書の様式を用いて仮想基盤側に提出していただきます。仮想基盤では、受領した運用管理基盤設定申請書の内容に基づいて、運用管理サーバ（Hinemos）に対してシステム監視の設定を行います。業務システムに対する監視設定が可能となる項目は以下のとおりです。
（製品仕様により申請いただいた内容のとおりに監視が実現できない場合があります。）

[監視項目]

No	監視種別	概要
1	PING 監視	ICMP(Ping)を用いて監視対象の IP アドレス死活を監視する。
2	システムログ監視	RHEL のシステムログに出力されたメッセージを監視する。
3	イベントログ監視	Windows イベントログに出力されたメッセージを監視する。
4	ログ監視	特定のログファイルに出力されたメッセージを監視する。
5	リソース監視	対象機器や OS のリソース状況を監視する。
6	プロセス監視	監視対象サーバのシステム(OS)およびアプリケーションのプロセスを監視する。
7	Windows サービス監視	Windows サービスの状態を監視する。
8	サービス・ポート監視	特定サービス・ポートについて、応答有無や応答時間を監視する。
9	Hinemos エージェント監視	Hinemos エージェントの死活を監視する。
10	SQL 監視	DB サーバの応答有無や応答時間、SQL レスポンスの内容を監視する。
11	JMX 監視	Java アプリケーションのヒープメモリサイズ等を監視する。
12	ジョブ監視	ジョブの実行結果を監視する。

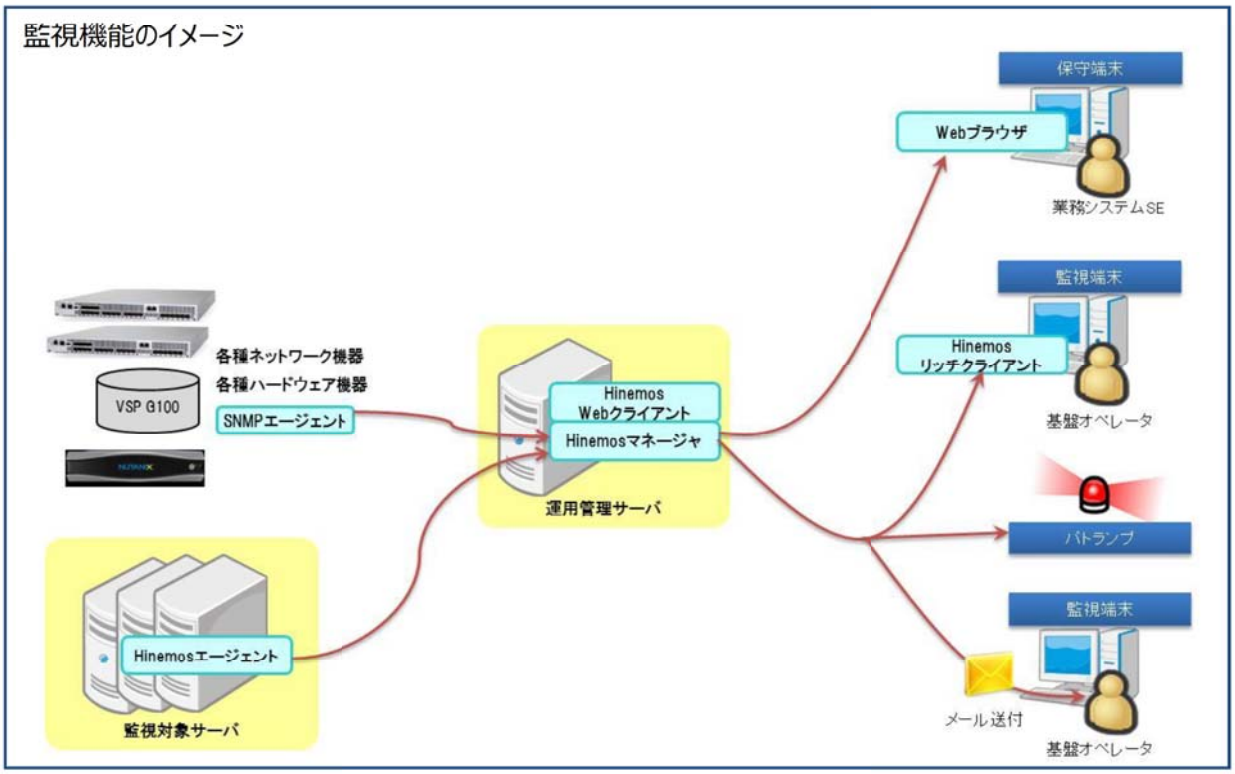
[補足]

HTTP 監視については、SSO システムの保守開発環境において「監視が実現できない」という事象が発生しました。その際に原因究明および解決に至らなかったため、サービス提供リストからは除外しています。システム運用上、必要となる場合は基盤システム所管部門にご相談ください。テストを通じて監視の実現性が確認できた場合、個別利用の是非を検討します。

本番稼働中に障害を検知した場合は、基盤オペレータより業務システム事業者に対して連絡が可能となるように、以下に関する事項を基盤オペレータに引継ぎをする必要があります。

・業務システムの各サーバに対する監視内容
・重大な障害発生（オンライン停止、夜間ジョブ異常終了等）時の連絡先電話番号
（基盤オペレータからの緊急連絡は電話連絡が原則となります。）

以下の図に、監視機能について示します。



- 監視項目の有効化、無効化

  運用管理基盤設定申請書にて申請した監視項目について、仮想基盤では設定を行い(監視項目 ID 作成)、予め監視設定を無効化した状態で業務システム側へ環境を引き渡します。これは被監視対象である業務システム側の準備が完了していないことによる不要なエラー通知の発生を防ぐことを目的としています。
  したがって、本番稼働時には、業務システムにて設定を有効化する必要があります。

  また、本番稼働中でも、メンテナンスや障害対応時等に監視を抑止したい場合は、業務システム事業者にて監視の有効化・無効化を切り替えてください。
  詳細については、別途提供している「運用管理基盤利用手順書(Hinemos)」を参照してください。

- 監視項目の「収集」設定について

  Hinemos の監視項目は、数値、真偽値、トラップ、文字列のいずれかを基準に監視をしています。このなかで数値を基準に監視している項目については、その監視結果を Hinemos の性能管理機能と連動して蓄積、分析等を行うことができます。設定(監視項目 ID)の中の[収集]がそれに該当します。
  仮想基盤のサービスとしては「リソース監視」「JMX 監視」のみ、この「収集」設定を有効としています。予め"無効"となっている監視項目 ID を"有効"に変更することは禁止事項となります。

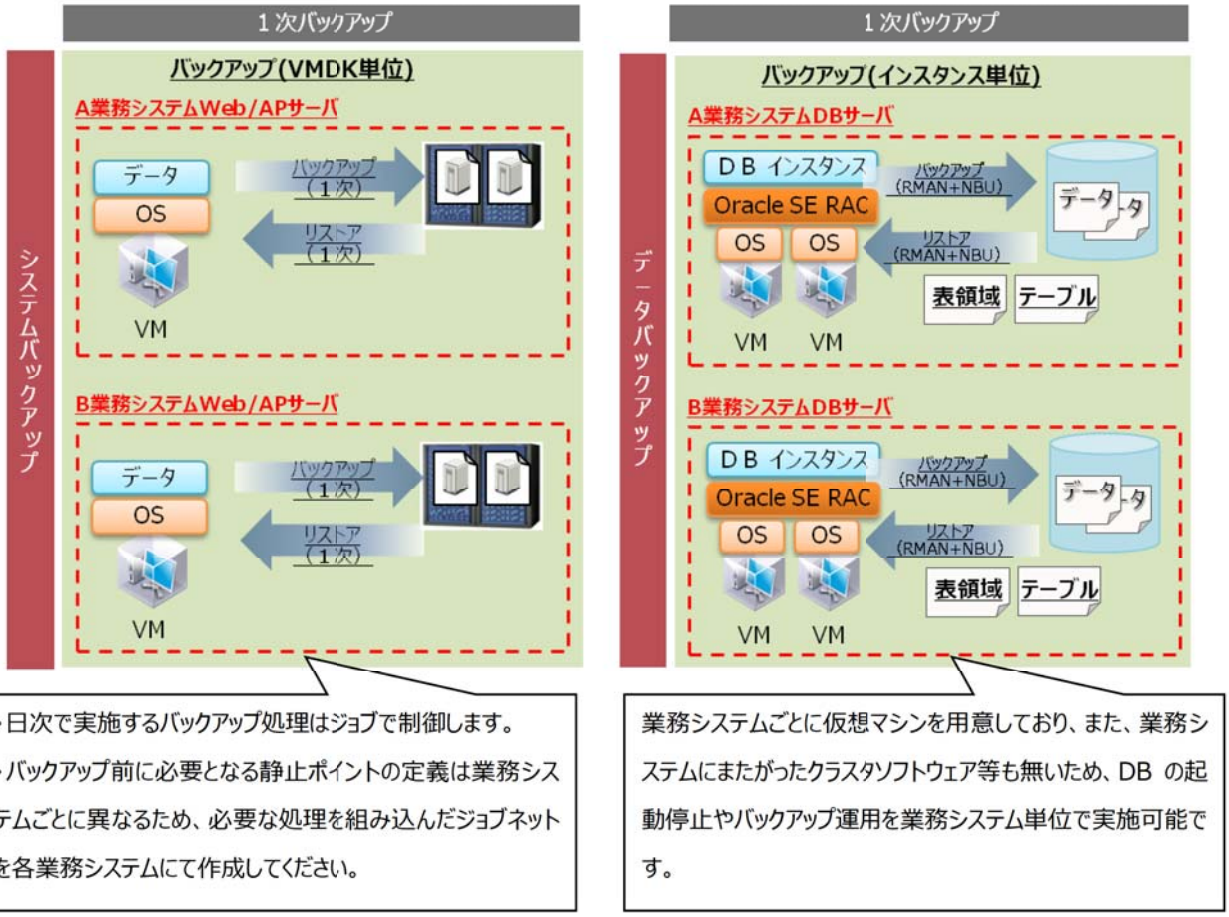
- 監視履歴イベントの保存期間とダウンロード
  イベント通知機能にて監視履歴イベントに出力されたイベントの保存期間は、２カ月です。それ以上の期間、イベントを保存しておきたい場合は、業務システム事業者にて csv ファイルに出力・ダウンロードしてください。
  ただし、一度にダウンロードできる最大件数は 2,000 件となりますので、取得時期やフィルタ条件等は業務システム事業者にて考慮して使用してください。
  csv ダウンロードの詳細については、別途提供している「運用管理基盤利用手順書(Hinemos)」を参照してください。

（前提：バックアップ・リストアサービスについては、4.5 章、4.6 章、4.7 章を一式として読み進めてください。）

4.5. バックアップ設定サービス

仮想基盤では、JP1/VERITAS NetBackup(以下、NBU)を用いたバックアップ環境に対する設定作業を、バックアップ設定サービスとして提供します。業務システム事業者はシステムの「バックアップ対象」「バックアップサイクル」等を運用設計にて定義した後にバックアップ設定申請書に要件を記入し、仮想基盤へ提出してください。仮想基盤では、バックアップ設定申請書に記載された内容に基づき、NBU マネージャに対してバックアップポリシー等の NBU バックアップジョブの動作に必要な設定を実施します。設定完了後、業務システム事業者は管理コンソール(OpsCenter)にて、NBU マネージャへの接続、手動バックアップ実行、手動リストア作業が可能となります。また、新たに作成したバックアップポリシーを Hinemos のジョブ機能にて実行いただくことも可能となります。

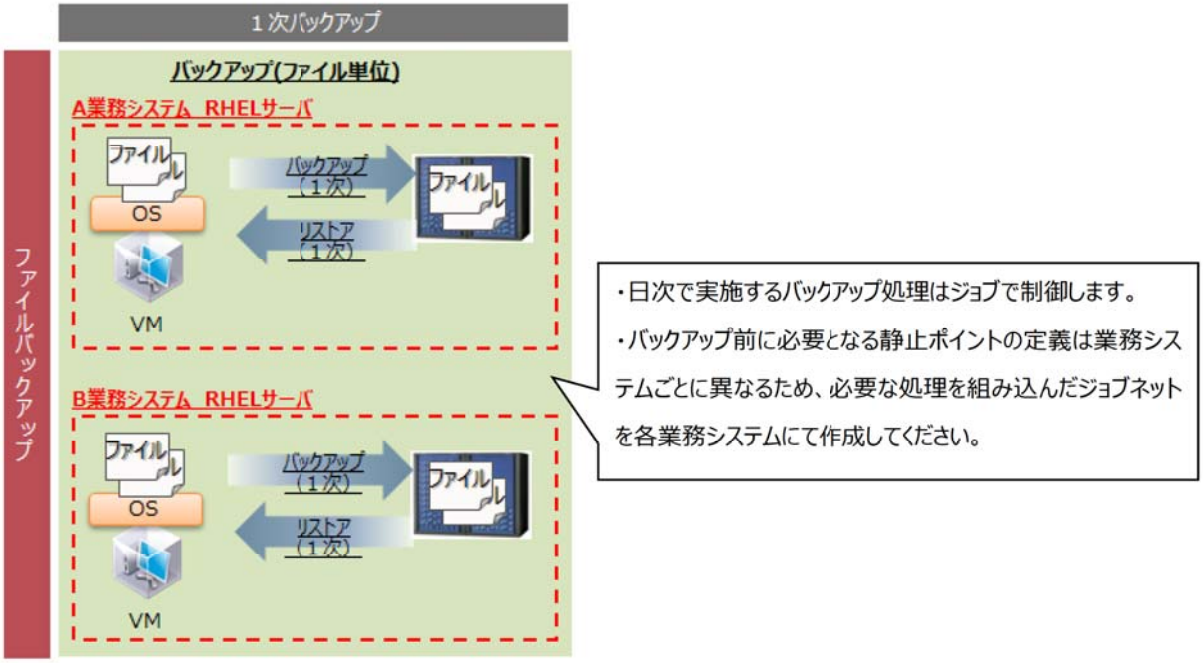
以下の図に、仮想基盤におけるバックアップ方式であるシステムバックアップ、およびデータバックアップ(Oracle RMAN バックアップ)について示します。



・日次で実施するバックアップ処理はジョブで制御します。
・バックアップ前に必要となる静止ポイントの定義は業務システムごとに異なるため、必要な処理を組み込んだジョブネットを各業務システムにて作成してください。

業務システムごとに仮想マシンを用意しており、また、業務システムにまたがったクラスタソフトウェア等も無いため、DB の起動停止やバックアップ運用を業務システム単位で実施可能です。

この他にも仮想基盤では、上図のバックアップ方式（システムバックアップ、データバックアップ）とは別に、ファイル単位のリストア(GRT)機能(※)が未対応である Red Hat Enterprise Linux 7.1（x64）用に、ファイル単位のバックアップ方式を提供します。



（※）GRT 機能(Granular Recovery Technology)・・・ データベースのバックアップから個別の項目がリストア可能な機能

いずれのバックアップ方式においても、ジョブに組み込んでいただくNBUのバックアップ処理部分に関するサンプルコマンドを仮想基盤より提供しますので、必要に応じてご活用ください。

- バックアップ設定サービスに関する特記事項
  ・バックアップの実施に関するスケジュールは業務システム事業者にて検討し、ジョブ機能（Hinemos）を用いて実現いただく必要があります。
  ・バックアップの成否確認は各業務システム事業者にて実施する必要があります。
  ・2016 年 6 月時点におけるバックアップ機器の構成としては「バックアップデータ書き込み処理を担うサーバが 1 台」「1 次バックアップデータを格納するストレージが 1 台」という構成になっています。NBU においてはバックアップ処理の多重度（同時実行数）の上限を設けているため、他システムとバックアップのタイミングが重複することにより開始までの「待ち時間発生」「リソース共有によるスループットの低下」が発生することが想定されます。各業務システムのバックアップ処理は予め時間に余裕をもった実行計画を検討してください。

- 1 次バックアップの考え方と注意事項

・NBU のバックアップポリシーにて取得したバックアップを、1 次バックアップとして扱います。

・1 次バックアップは、Hinemos のジョブ機能を用いてバックアップポリシーを実行するか、OpsCenter(※1)にてバックアップポリシーを手動実行することで取得できます。

・Hinemos のジョブ機能を用いてバックアップポリシーを実行する際に、パラメータとして、"full_day"もしくは"full_week"のいずれかを指定する必要があります。詳細は後述しますが、"full_week"パラメタを指定した 1 次バックアップデータについては、NBU の仕組み上、すべて 2 次バックアップの取得対象となります。構築、開発、テスト期間など本番稼働前に取得する 1 次バックアップについては、"full_day"パラメタを指定して取得してください。（2 次バックアップの動作検証として"full_week"パラメタを指定することは問題ありませんが、回数は必要最低限に抑えてください。）

・1 次バックアップデータの保存期間は 1 週間となります。取得可能な世代数に上限はありません。
（1 次バックアップを 1 日の間に複数回取得することも可能です。）

（※1）詳細については「NetBackup OpsCenter 基本操作手順書」を参照してください。

・実行中の 1 次バックアップを中断したい場合、業務システム事業者にて OpsCenter を用いてポリシーを手動停止してください。

- 2 次バックアップの考え方と注意事項

・2 次バックアップは週次にて LTO テープライブラリに保管し、災害対策として遠隔地保管されます。
（毎週月曜日～水曜日に取得され、毎週木曜日に遠隔地に移動されます。また、格納対象は 1 次バックアップの 1 世代分のみとしてください。詳細は後述のとおりです。）

・2 次バックアップデータからのリストアは災害発生時のみの対応とします。通常運用では 2 次バックアップからのデータリストアやファイルリストアといった依頼には対応いたしかねます。

・2 次バックアップとは、バックアップポリシーで取得した 1 次バックアップを LTO テープライブラリに保存する処理を指します。ただし、対象は"full_week"パラメタを指定した 1 次バックアップに限ります。

・"full_week"パラメタを指定して取得した 1 次バックアップについては、NBU の仕組み上、すべて 2 次バックアップの取得対象となります。しかし、LTO テープライブラリの処理性能と保存容量の観点から、運用ルール（上限）を設けております。ルールを遵守できるようにジョブスケジュールを検討してください。

[2 次バックアップの取得対象に関するルール]

- 本番環境のデータのみ
- 1 システムあたりの取得可能上限を 400GB とする

※1 各システムが 2 次バックアップでどの程度の容量を取得しているかについては定期点検をしています。
400GB を超過するシステムに対しては個別に是正依頼のご連絡をさせていただきます。
また、400GB を超過している 2 次バックアップについては、運用に影響をきたすと判断した場合に住民情報システム課の権限にて強制的に中止とする場合があります。

※2 仮想マシンのサイズが 400GB を超過する Oracle DB サーバにおいて、業務データを 2 次バックアップしたい場合、Dump 形式で出力した後に当該ファイルをファイルバックアップの対象として処理をする等の検

討をしてください。

・２次バックアップデータの保存期間は３週間となります。

・２次バックアップ装置(LTO テープライブラリ)への取得対象と処理時間の関係で、将来的に取得処理のタイミングを見直す場合があります。（例えば、開始曜日の前倒し、取得タイミングの分散など。）

・取得対象の容量により、各業務システムに対して取得対象の見直しをお願いする場合があります。

・2 次バックアップを実行する日については、各業務システム間の実行タイミングの重複を避けるために基盤システム所管部門にて最終決定します。2 次バックアップの運用を開始する前に必ず所定の様式（資料「バックアップ運用開始申請書」）を提出し、基盤システム所管部門の承認を得てください。この様式の提出を契機として 2 次バックアップ実行可能日（月曜日～水曜日のいずれか）を業務システム事業者に連絡します。

4.6. バックアップ・リストア機能提供サービス

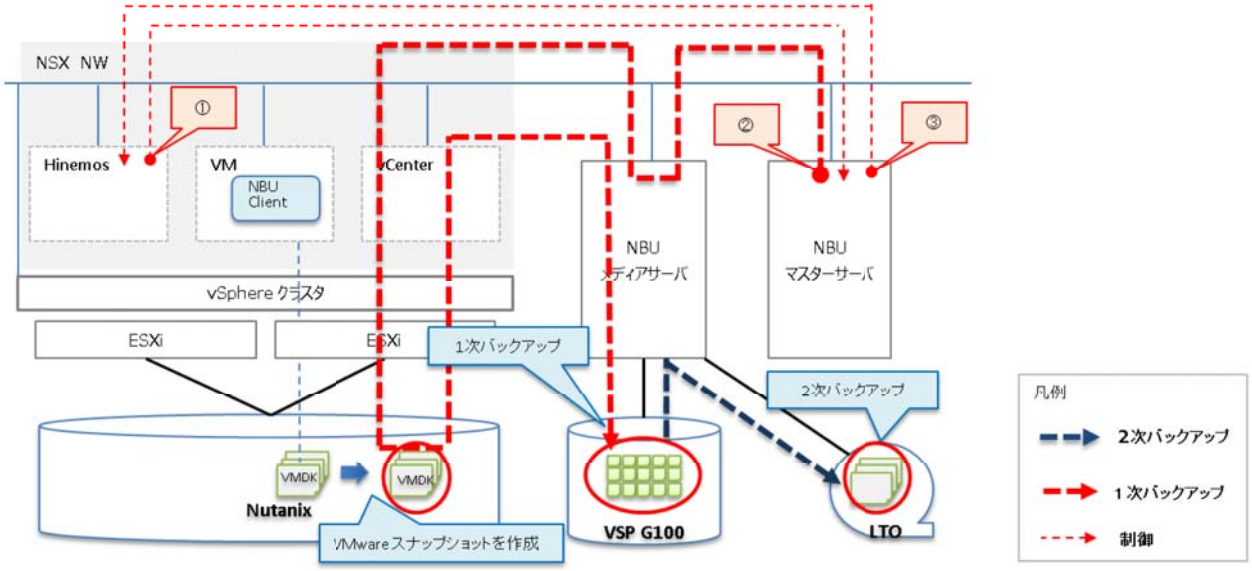
4.6.1. システムバックアップ

VMware の VADP(vStorage API for Data Protection)との機能連携によって、仮想マシンイメージ(仮想マシン全体)をバックアップする方式です。本方式は、仮想マシンのシステムバックアップ/システムリストアと、ファイル単位のリストアを兼ねています。

なお、本方式は、仮想マシン全体がバックアップ対象となるため、仮想マシンへ追加した仮想ディスクもバックアップ対象となります。ただし、独立型形式(Oracle RAC の共有領域)の仮想ディスクは、バックアップの対象外です。

また、システムバックアップ時は、OS 停止やアプリケーションサービスを停止するなど、仮想マシンやアプリケーションが静的な状態でバックアップを実行することを推奨します。システムバックアップ時における OS の停止や業務サービスの停止については、業務システム事業者にて実施してください。

以下の図に、システムバックアップ方式を示します。このバックアップ方式を用いたバックアップについては、業務システム事業者にて実行してください。（1 次バックアップ処理を実行する際に使用する NBU のパラメタを変更することで 1 次バックアップと 2 次バックアップの双方を取得することが可能です。）



No	処理項目	処理内容
①	ジョブ開始	運用管理サーバ(Hinemos)より、バックアップジョブを開始する。 ・NBU マスタサーバへバックアップポリシー実行を指示。
②	バックアップ処理	NBU マスタサーバでバックアップポリシーが開始する。 ・NBU メディアサーバが対象サーバ(仮想マシン)をディスク装置(VSP G100)へバックアップ。
③	ジョブ完了	NBU マスタサーバでのバックアップポリシー完了後、運用管理サーバよりバックアップジョブを完了する。 ・NBU マスタサーバがバックアップポリシー完了後にリターンコードを発行。

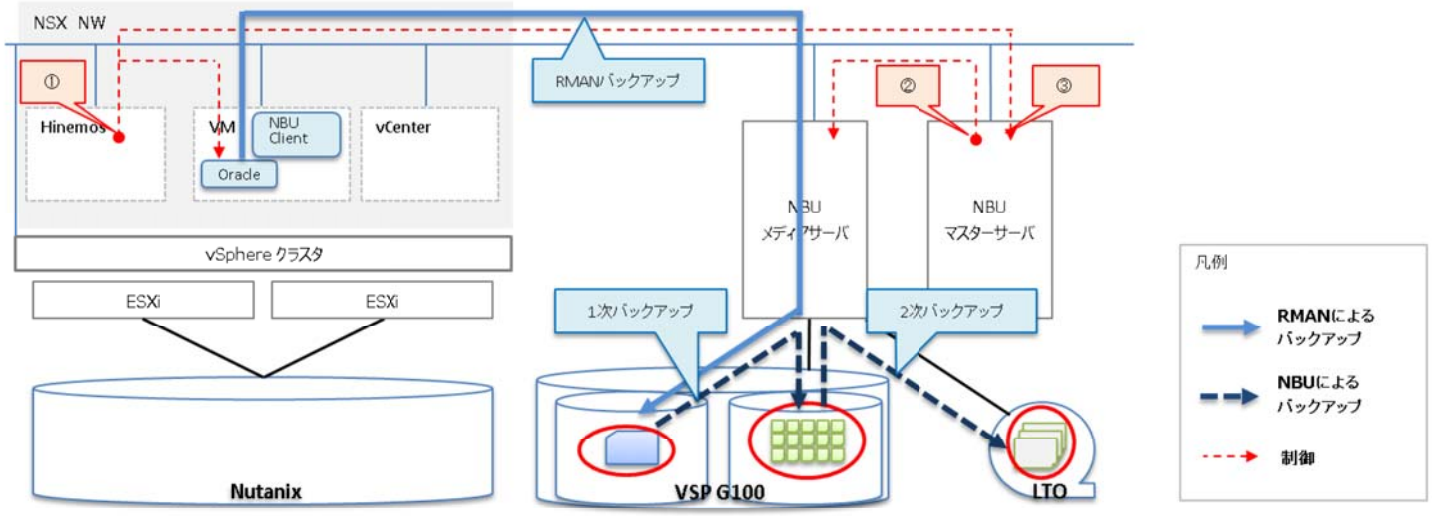
4.6.2. データバックアップ

データバックアップ(Oracle DB(RMAN))方式は、NBU の機能によって NBU メディアサーバの NFS 領域にあるデータをバックアップする方式です。(仮想基盤事業者にて RMAN の実行結果（バックアップデータ）を格納する NFS 領域を NBU メディアサーバに作成し、ディレクトリパスをお伝えします。業務システム事業者は当該ディレクトリをマウントし、RMAN 実行後に結果（バックアップデータ）が格納されることを確認してください。)

本方式は、DB サーバ(Oracle RAC 構成)のデータバックアップ/リストアで使用します。ただし、DB サーバ(Oracle シングルサーバ構成)のデータバックアップ/リストアは、4.6.1 章に記載のシステムバックアップ方式を使用していただくことになるため、本方式の対象外です。

また、データバックアップ時は、オンラインサービスを停止する等、データベースが静的な状態でバックアップを実行することを推奨します。データバックアップ時におけるオンラインサービス等の停止については、業務システム事業者にて実施してください。

以下の図に、データバックアップ(Oracle DB(RMAN))方式を示します。このバックアップ方式を用いたバックアップについては、業務システム事業者にて実行してください。（1 次バックアップ処理を実行する際に使用する NBU のパラメタを変更することで 1 次バックアップと 2 次バックアップの双方を取得することが可能です。)



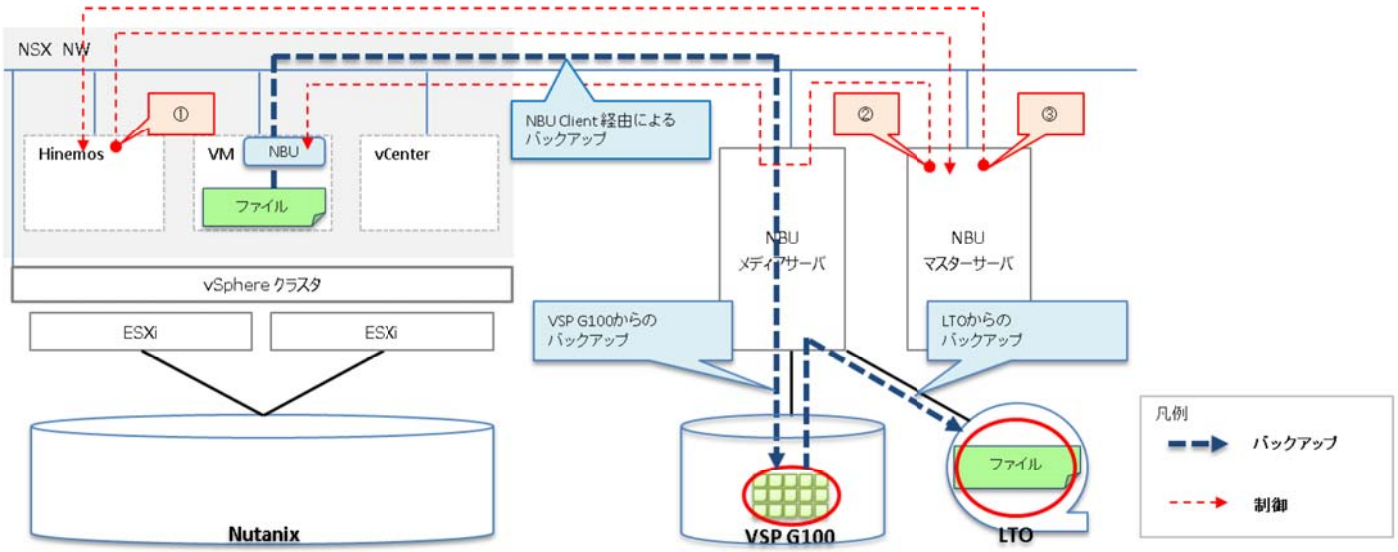
No	処理項目	処理内容
①	ジョブ開始	運用管理サーバ(Hinemos)より、バックアップジョブを開始する。 ・DB サーバ(Oracle RAC 構成)へ Oracle(RMAN)のバックアップ実行を指示。 ・DB サーバ（Oracle RAC 構成）が RMAN 実行完了後にリターンコードを発行。 ・NBU マスタサーバへバックアップポリシー実行の指示。
②	バックアップ処理	NBU マスタサーバでバックアップポリシーが開始する。 ・NBU メディアサーバが RMAN のバックアップデータを VSP G100 へバックアップ。
③	ジョブ完了	NBU マスタサーバでバックアップポリシー完了後、運用管理サーバよりバックアップジョブを完了する。 ・NBU マスタサーバがバックアップポリシー完了後にリターンコードを発行。

4.6.3. ファイルバックアップ

ファイルバックアップ方式は、NBU クライアントの機能によってフォルダ/ファイル単位でバックアップする方式です。本方式は、システムバックアップデータからのファイル単位のリストア(GRT)機能が未対応である Red Hat Enterprise Linux 7.1（x64）のファイルバックアップ/リストアで使用します。（Windows Server 2012 R2、RHEL6.7 でのファイルバックアップの利用も可能です）

また、ファイルバックアップ時は、バックアップ対象データの整合性が確保される状態でバックアップを実行することを推奨します。データの整合性確保のために必要な処理については、業務システム事業者にて実施してください。

以下の図に、ファイルバックアップ方式を示します。このバックアップ方式を用いたバックアップについては、業務システム事業者にて実行してください。（1 次バックアップ処理を実行する際に使用する NBU のパラメタを変更することで 1 次バックアップと 2 次バックアップの双方を取得することが可能です。）



No	処理項目	処理内容
①	ジョブ開始	運用管理サーバ(Hinemos)より、バックアップジョブを開始する。 ・マスタサーバ(NBU)へバックアップポリシー実行の指示。
②	バックアップ処理	マスタサーバでバックアップポリシーが開始する。 ・メディアサーバへバックアップ実行の指示。 ・メディアサーバが対象サーバのデータを VSP G100 へバックアップ。
③	ジョブ完了	マスタサーバでバックアップポリシー完了後、運用管理サーバよりバックアップ用ジョブを完了する。 ・マスタサーバのバックアップポリシー完了を確認。

4.7. システムリストア支援サービス

システムバックアップ方式を用いて取得したバックアップデータを用いたシステムリストア（システムバックアップデータから特定のフォルダやファイルを選択してリストアする GRT 機能を用いる場合は除く）については、業務システム事業者で使用するアカウントでは一部の作業に対する操作権限を持たないため、仮想基盤事業者による作業支援が必要です。以下に、その理由と支援内容について示します。

- 理由：
  VMware 環境の仕様として、同一の vCenter 配下に同じ仮想マシン名が複数存在することができない。したがって、システムリストアの前には対象の仮想マシンを削除、または仮想マシン名をリネームする必要があるが、業務システムに付与する vCenter アカウントに対しては、通常運用時の誤操作（仮想マシン削除等）を防ぐため、この操作権限を割り当てていない。
- 支援内容：
  システムリストア前に、仮想基盤事業者による「仮想マシン削除」または「仮想マシン情報が格納されたフォルダを別階層に移動」の操作を行う。

なお、システムバックアップに対する GRT 機能を用いたファイルリストアについては、仮想基盤事業者による作業支援は不要です。

以下に、システムリストア作業の流れと、業務システム事業者および仮想基盤事業者の役割分担について示します。

No	作業ステップ	作業項目	担当
1	リストア実行前	対象サーバ(仮想マシン)の停止(シャットダウン)	業務システム事業者
2		対象サーバ(仮想マシン)の削除、または仮想マシン名のリネーム	仮想基盤事業者
3	リストア実行	管理コンソール(OpsCenter)からシステムリストアを実行	仮想基盤事業者
4	リストア完了後	VMware 環境の設定作業(仮想マシンへの vSphere HA 等)	仮想基盤事業者
5		リストアした仮想マシン OS の環境設定および動作確認	業務システム事業者

また、システムリストアを実施する際は、5 営業日前までに、基盤システム所管部門に対して申請手続きを行ってください。

5. サービス利用にあたって

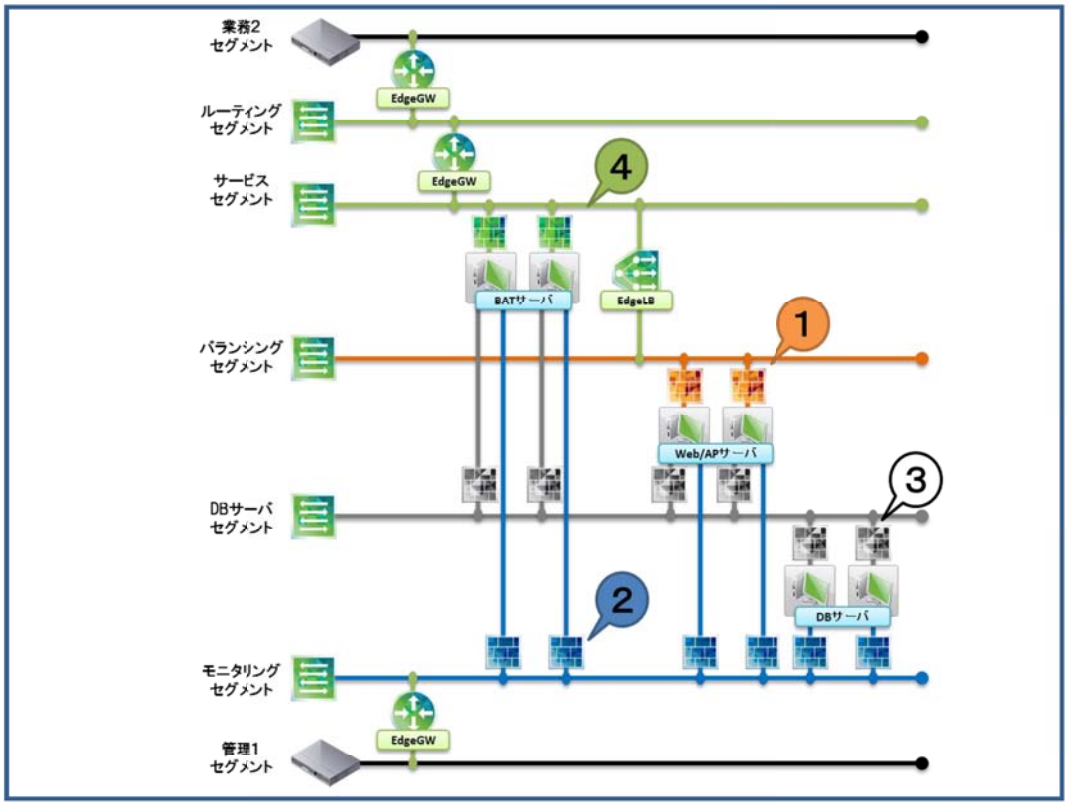
5.1. セキュリティ

5.1.1. 分散ファイアウォール

仮想基盤では、業務システムのセキュリティ確保のため分散ファイアウォールを使用します。仮想基盤上のサーバは分散ファイアウォールにより保護されるため、物理ファイアウォールによるトラフィック制御は実装しません（ただし、既存の基盤ネットワークと仮想ネットワークの間で通信が必要となる場合においてはこの限りではありません）。以下に、仮想基盤における分散ファイアウォール設計を示します。

No	ファイアウォール定義	内容
①	バランシングセグメント向けファイアウォール定義	Web サーバの業務トラフィックを制御する。
②	モニタリングセグメント向けファイアウォール定義	全サーバの管理トラフィックを制御する。 仮想基盤事業者：全サーバへのトラフィックを許可 業務システム事業者：管理対象サーバへのトラフィックを許可
③	DB セグメント向けファイアウォール定義	AP サーバと DB サーバのトラフィックを制御する。
④	サービスセグメント向けファイアウォール定義	各業務システム共通サーバ(ファイルサーバ等)のトラフィックを制御する。

上記に加え、業務システムの通信要件に基づく個別のファイアウォール定義により、各業務システムのトラフィックを制御します。以下の図に、分散ファイアウォールの適用範囲について示します。



5.1.2. 仮想マシンに導入するアンチウイルスソフト

仮想マシンOSには、アンチウイルスソフト(McAfeeエージェント)がインストールされています。このアンチウイルスソフトは基盤システムによる提供機能であるため、仮想基盤では一切の支援、および責任を負うことができません。したがって、質問や確認事項につきましては、基盤システム所管部門にエスカレーションのうえで指示に従ってください。

5.1.3. セキュリティパッチの適用

仮想基盤より提供したOSとミドルウェア、および基盤システムが提供したMcAfeeエージェントにおけるセキュリティパッチの適用については、基盤システム所管部門の判断により業務システム事業者へ適用を依頼する場合があります。
適用を依頼する場面は、緊急度合いやセキュリティリスクの高いパッチが公開された場合が想定されますが、適用作業（適用手順の確認も含め）は、業務システム事業者にて業務アプリケーションへの運用を考慮して速やかに実施いただく必要があります。

なお、緊急度合い（影響の大きい不具合）やセキュリティリスクの高いパッチが公開された場合、基盤システム所管部門から業務システム事業者に対して、パッチの適用を依頼する場合があります。その際は必ず依頼内容に従い、対応をお願いします。

OS に関する主要なパッチのリリース情報を以下のフォルダにて公開しています。仮想マシンの払い出しに使用しているテンプレートについては、テンプレート作成時点で公開されていた一部のセキュリティパッチを適用しています。適用されているパッチについては実機もしくは定数設計書を確認してください。
なお、McAfeeエージェントのパッチの配置場所については、基盤システム所管部門の指示に従ってください。

-

  [補足]
  本資料に掲載されている情報については各業務システムのアーキテクチャを踏まえ、必要に応じて適切な対応をしてください。また、パッチの入手は原則として各業務システム事業者の担当とします。

また、業務システムが独自に導入している OS やミドルウェア、アプリケーション等で緊急度合いやセキュリティリスクの高いセキュリティパッチが公開された場合、速やかに適用を実施してください。この場合、仮想基盤では業務システムが独自に導入している OS やミドルウェア、アプリケーション等については、調査やパッチ提供など一切関知はいたしませんので、必ず業務システム事業者の責任において実施してください。

5.1.4. OS のローカル管理者パスワード

仮想基盤が業務システムへ仮想マシンを提供した際は、OS にはローカル管理者（Windows： 、RHEL ）のアカウント・パスワードが定義されています。そのパスワードにつきましては、初期設定の扱いとします。したがって、業務システムでは仮想マシンを受領後、OS ローカル管理者のパスワードを変更してください。パスワード文字列等の付与ルールについては、業務システムにて決定してください。

環境構築等の実施後にOSローカル管理者のパスワードを変更した場合、サーバ機能の挙動に不具合が生じる可能性がありますので、速やかなご対応をお願いいたします。

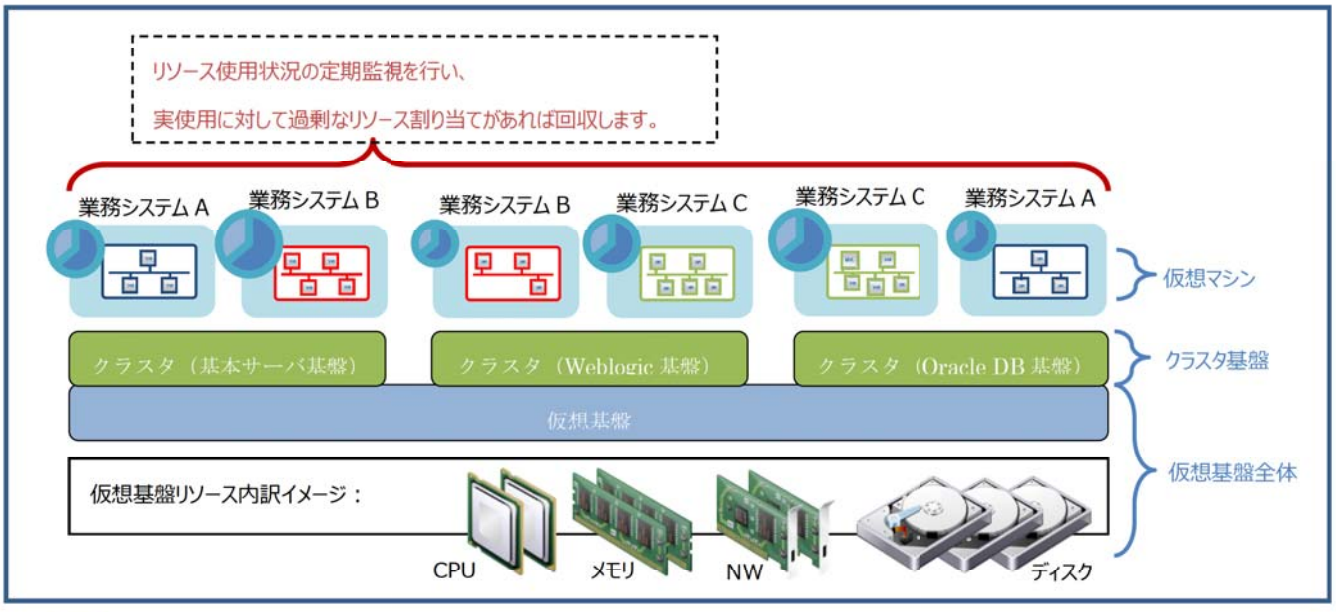
5.2.　仮想基盤のリソース管理

仮想基盤では、業務システムへ提供した仮想マシンのリソース（CPU、メモリ、ディスク領域）について、使用状況の稼働統計情報を定期的に取得しています。統計情報の取得には、VMware 社の仮想アプライアンスである vRealize Operations Manager(以下、vROps)を使用します。

統計情報を確認した結果、リソース使用状況に継続した余裕がある場合、仮想基盤側の必要に応じて、リソースの回収にご協力をお願いすることがあります。
回収とは、例えば仮想マシンに CPU を 4 コア割り当てているが実際の使用状況が常に 2 コアを下回っている場合、仮想マシン設定を 4 コアから 2 コアにダウンサイジングさせていただくことになります。
なお、回収作業は仮想基盤事業者にて実施することとし、その際は事前に実施時期等を調整します。

vROPs を用いて取得した稼働統計情報は「仮想基盤ハードウェアのリソース使用状況」として管理するため、業務システム事業者に対する情報開示は原則実施しません。
各業務システムの仮想マシンのリソース使用状況（各 OS での CPU 使用率、メモリ使用率、ディスク使用率）については「4.4.2 監視機能」に記載している Hinemos のリソース監視機能を用いて情報を取得・確認いただくことになります。

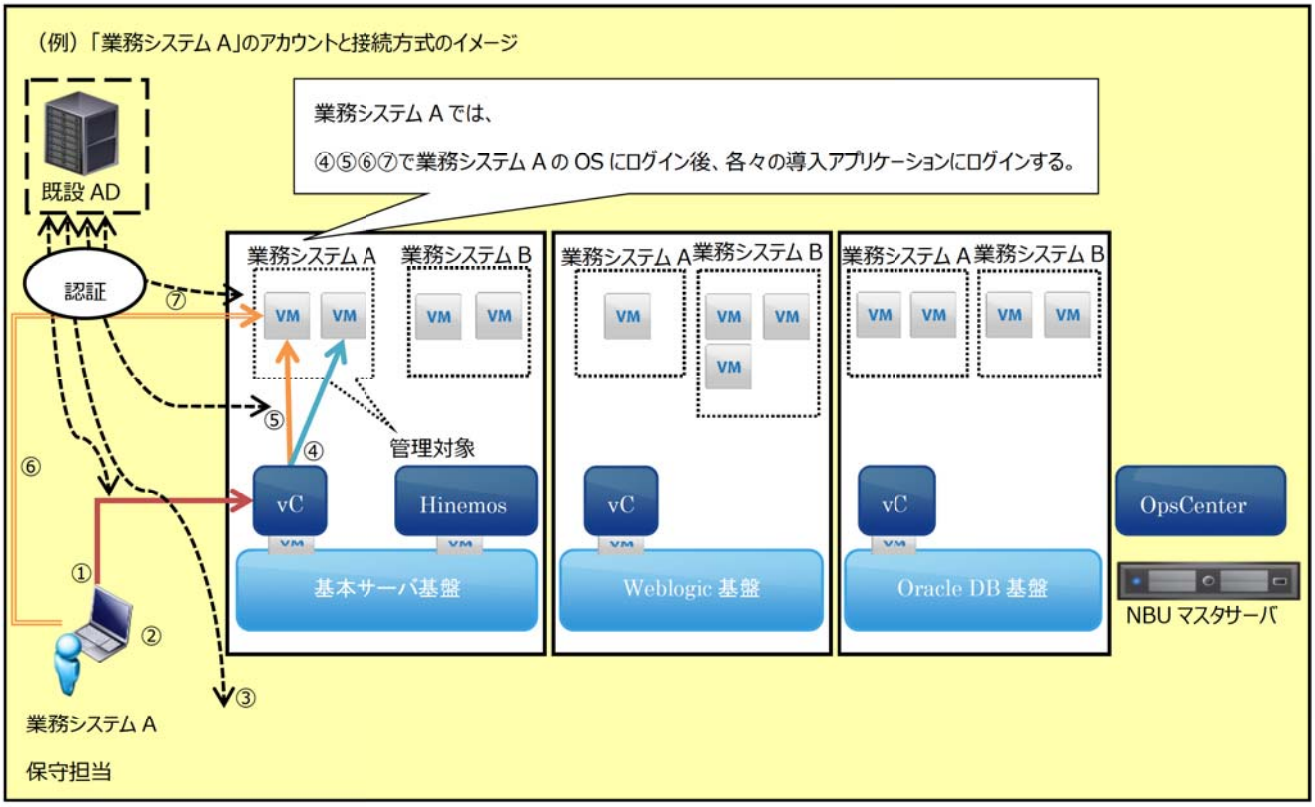
以下の図に、仮想基盤のリソース監視のイメージについて示します。



・・・CPU、メモリ、ディスク領域などの割り当てリソースのイメージ
リソースの使用状況に応じて、割り当てを小さく ⇒ したり、大きく ⇒ します。

5.3. 仮想マシンへの接続方式と使用アカウント

仮想基盤における仮想マシンおよび各ミドルウェア機能への接続方式について、以下の図に示します。
業務システム事業者にて用意する保守作業用の PC から、それぞれの用途のアカウントで、目的の接続先へ接続します。



① <vSphere Client>　AD アカウントで vCenter にログイン
② <Web ブラウザ>　Hinemos 専用ユーザで Hinemos マネージャにログイン
③ <Web ブラウザ>　AD アカウントで OpsCenter にログイン
④ <vSphere コンソール> 業務システム A の VM(Winows/Linux)に OS ローカルユーザでログオン
⑤ <vSphere コンソール>　業務システム A の Windows サーバに AD アカウントでログオン（必要に応じて）
⑥ <RDP,SSH,VNC>　業務システム A の VM(Winows/Linux)に OS ローカルユーザでログオン
⑦ <RDP,SSH,VNC>　業務システム A の Windows サーバに AD アカウントでログオン　（必要に応じて）

次の一覧表に、アカウントの詳細と権限、接続方式について示します。サーバ OS で使用する AD アカウントについては、通常運用では使用しない想定です。必要となる場合は、基盤システム所管部門へご相談ください。

アカウント権限

No	アカウント				接続方式	アカウントに付与する権限、想定する用途の概要など
	区分	種別	権限	提供方法・提供者		
1	OS	ローカル管理者（デフォルト）	管理者	仮想基盤事業者	④、⑥	OS ローカル管理者
2	OS	ローカル管理者（デフォルト以外）	管理者	業務システム事業者(任意作成)	④、⑥	業務システムの任意で付与
3	OS	ローカル一般アカウント	一般ユーザ	業務システム事業者(任意作成)	④、⑥	業務システムの任意で付与
4	OS	AD アカウント	管理者	基盤システム事業者	⑤、⑦	通常運用では使用しない想定。管理者権限の場合でもアクセス範囲は自システム内に限定する（他の AD 環境の操作不可）。
5	OS	AD アカウント	一般ユーザ	基盤システム事業者	⑤、⑦	
6	vCenter	AD アカウント	一般ユーザ	基盤システム事業者／仮想基盤事業者	①	電源 OFF/ON、端末コンソール操作
7	OpsCenter	AD アカウント	一般ユーザ	基盤システム事業者／仮想基盤事業者	③(※1)	NBU バックアップジョブ設定、NBU バックアップ取得・リストア操作
8	Hinemos	製品個別	一般ユーザ	仮想基盤事業者	②	ジョブ定義の設定

(※1) OpsCenter 接続に使用する Web ブラウザについては、「Mozilla Firefox バージョン 15.0」以上を使用してください。

アカウント使用者

No	アカウント		
	区分	種別	アカウント使用者
1	OS	ローカル管理者（デフォルト）	業務システム事業者
2	OS	ローカル管理者（デフォルト以外）	業務システム事業者
3	OS	ローカル一般アカウント	業務システム事業者
4	OS	AD アカウント	業務システム事業者
5	OS	AD アカウント	業務システム事業者
6	vCenter	AD アカウント	業務システム事業者
7	OpsCenter	AD アカウント	業務システム事業者
8	Hinemos	製品個別	業務システム事業者

6. その他制限事項・注意事項

- 仮想マシンテンプレートを用いた仮想マシン提供時において、デフォルト設定値となっている HDD（100GB）に対するパーティション分割はサービスの対象外となります。
- ハイパーバイザ（ESXi）側にてNICの冗長化を実現しているため、OS側での冗長化（Bonding、Teaming）については設定不要です。
- Oracle Database をインストールした後に、情報共有基盤システムにて提供している McAfee（アンチウイルスソフト）をインストールすると Oracle DB の動作が不安定となる事例が報告されています。したがって、仮想マシンに対して Oracle Database をインストールする際には、事前に McAfee のインストールを完了させておくことを推奨します。
- 業務システムにて管理するアカウントのパスワードの変更については、その影響範囲を事前に調査して問題がないことを確認してください。
- 仮想マシン引き渡し後のバックアップは、各業務システム事業者にて確実に実施してください。
- ネットワーク提供サービスにて業務システム側に提供する仮想 LB についてはセッションタイムアウト間隔:300 秒、パーシステンスタイムアウトが 3,600 秒となります。業務システム事業者はこの点を考慮してシステム方式設計を行ってください。
- OS および各ミドルウェアに関する問合せは各業務システム事業者から直接行ってください。その際に使用するサポート ID 等の情報は住民情報システム課に確認してください。

以上

【仮想基盤（仮想マシン）の利用可否の条件・仕様について】

・Oracle データベースを使用する場合にはライセンス制約により、現状の仮想基盤上での実現が不可になります。
・現状の仮想基盤の払い出し可能なリソース(CPU/メモリ)を超える場合には原則不可です。（※１）
・仮想基盤利用ガイドライン及び基盤概要説明書等に記載されている要件を満たさない場合は原則不可です。
・上記以外に特殊な要件や構成を求める場合は、協議の上不可となる可能性があります。

※１　下記、払出し可能なリソースになります。
　　CPU　：計 15 コア　（※２）
　　メモリ：計 100 GB
　　ディスク：計 10 TB

上記リソース情報については、2/6 時点での値となります。
今後の仮想マシン払い出し状況により、変動いたします。

●横浜市情報セキュリティ管理要綱

制定　平成 17 年３月 31 日　総Ｉ第 1148 号（局長決裁）
一部改正　平成 30 年３月 15 日　総行第 2034 号（局長決裁）

第１章　総則

（目的）

第１条　この要綱は、横浜市情報セキュリティ管理規程（平成 17 年３月横浜市達第２号）（以下「規程」という。）に基づき情報セキュリティ対策に関し必要な事項を定め、情報セキュリティの確保を図ることを目的とする。

（定義）

第２条　この要綱において、次の各号に掲げる用語の意義は、規程第２条に定めるもののほか、当該各号に定めるところによる。

(1)　非開示情報　横浜市の保有する情報の公開に関する条例（平成 12 年２月横浜市条例第１号）第７条第２項に規定する非開示情報をいう。

(2)　基本ソフトウェア　ハードウェアを正常に動作させるために必要なソフトウェア及び情報セキュリティのためのソフトウェアをいう。オペレーティングシステム、ハードウェアの設定を行うためのソフトウェア、ウイルス対策用ソフトウェアなどをさす。

(3)　業務ソフトウェア　業務を行うためのソフトウェアをいう。文書作成用ソフトウェア、表計算ソフトウェア及びサーバ等から提供されたデータを表示するためのソフトウェアなどをさす。

(4)　その他のソフトウェア　基本ソフトウェア及び業務ソフトウェア以外のソフトウェアをいう。

(5)　サーバ等　通信回線で接続された電子計算機に対して、データベース管理や、電子メールの送信などの機能の提供を主に行う電子計算機（付属する入力・出力・記憶装置及び機能維持のための機器を含む。）をいう。ホストコンピュータ、サーバなど（仮想化技術を用いて構築されたものを含む。）をさす。

(6)　端末機等　サーバ等及び通信機器等を除く電子計算機（付属する入力・出力・記憶装置を含む。）をいう。単独で事務に使用する電子計算機、ホストコンピュータの端末機、サーバの機能提供を受ける電子計算機、ハードディスク装置を搭載した複写機など記憶装置とソフトウェアを持つ事務機器など（仮想化技術を用いて構築されたものを含む。）をさす。

(7)　通信機器等　サーバ等及び端末機等を相互に接続するための機器及び情報セキュリティ対策のための機器、ネットワーク制御を行う機器、ネットワークを維持及び管理するための情報セキュリティ機器などをいう。ハブ、ルータ、モデム、通信ケーブルなど（仮想化技術を用いて構築されたものを含む。）をさす。

(8)　記録媒体等　情報資産のうち、記録媒体（仮想化技術を用いて構築されたものを含む。）及び紙を媒体とする行政文書をいう。

(9)　情報機器等　第２号から第８号を総称したものをいう。

(10) 携帯端末機　端末機等のうち、サーバ等や他の端末機から通信回線や記録媒体を用いてデータを取り入れ、持ち運んで利用する機器をいう。
(11) 特定用途機器　他の情報機器等と通信を行う端末機等のうち、特定の用途に用いるために機能が限定されており、業務ソフトウェアの追加など、情報資産管理者による機能拡張が想定されていない機器をいう。複合機・デジタルサイネージ・監視カメラ・センサーなどの IoT 機器、キオスク端末及び空調・プラントなどの制御・操作機器などをさす。
(12) 情報セキュリティインシデント　情報セキュリティ事故又は情報セキュリティ事故につながるおそれのある事象をいう。

第２章　職員の責務

（職員の責務）
第３条　職員は、規程第５条各項に基づき情報資産を適切に取り扱うにあたり、規程第 11 条及び第 12 条に基づく、情報セキュリティ担当者及び情報資産管理者の指導及び監督に従わなければならない。
２　職員は、著作権、著作権その他の権利に配慮し、プログラムの不正使用や無断改造等を行ってはならない。また、本市の保有する著作権、著作権その他の権利が侵害されないよう努めなければならない。
３　職員は､業務以外の目的で情報資産の外部への持ち出し､情報システムへのアクセス、電子メールアドレスの使用及びウェブの閲覧等、インターネットへのアクセスを行ってはならない。
４　職員は、情報セキュリティ運用管理者の許可なくパソコンや携帯端末機をネットワークに接続してはならない。
５　職員は、情報機器等のセキュリティ機能の設定を当該情報機器等に係る全ての情報資産管理者の許可なく変更してはならない。
６　職員は、外部からデータ又はソフトウェアを取り入れる場合は、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
７　職員は、差出人が不明又は不自然なファイルが添付された電子メールを受信した場合は、不用意に開封してはならない。
８　職員は、端末機等がコンピュータウイルス等の不正プログラムに感染した又は感染が疑われる場合は、通信ケーブルの即時取り外しを行わなければならない。
９　職員は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ担当者に報告しなければならない。

第３章　情報資産の分類及び管理

（情報資産の分類及び管理者）
第４条　規程第 13 条に基づく情報資産の分類及び当該分類された情報資産に対応する情報資産管理者は別表のとおりとする。

２　情報資産管理者は、情報資産を機密性、完全性及び可用性により次により分類し、必要に応じ取扱制限を行うものとする。

(1)　機密性による分類　直ちに一般に公表することを前提としていない情報資産

(2)　完全性による分類　改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障を及ぼすおそれがある情報資産

(3)　可用性による分類　滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障を及ぼすおそれがある情報資産

（情報資産管理者の責務）

第５条　情報資産管理者は、前条の分類に応じ主管する情報資産について、作成又は入手、利用、保管及び廃棄等の局面に応じ、適正に維持及び管理する責任及び運用する権限を有する。

２　情報資産管理者は、他の情報資産管理者が主管する情報資産を利用する場合、当該情報資産管理者に対して適正に維持及び管理する義務を負い、その指示に従わなければならない。

３　情報資産管理者は、主管する情報資産を横浜市以外のものに提供する場合、提供を受ける者がデータ利用時に利用者の認証を行っているか、情報セキュリティに関する研修を実施しているかなど、提供を受ける者が十分な情報セキュリティ対策を行っていることをあらかじめ確認しなければならない。

（情報資産の持ち出し制限）

第５条の２　職員は、すべての情報資産を、情報資産管理者の許可なく、庁外等、情報資産管理者が定めた保管及び利用場所以外に持ち出すことができない。

２　職員は、電子メール等により情報資産を送信する場合、必要に応じ暗号化又はパスワード設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

３　職員は、車両等により情報資産を庁外等に運搬する場合、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（情報資産の保管）

第５条の３　情報資産管理者は、利用頻度が低い記録媒体や情報システムのバックアップで取得したデータを記録する記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

２　情報資産管理者は、特に重要な情報を記録した記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

（情報資産の廃棄）

第５条の４　情報資産管理者は、記録媒体等が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄しなければならない。

第４章　物理的な情報セキュリティ対策

（物理的な情報セキュリティ対策）

第６条　情報セキュリティ運用管理者は、情報資産を設置する建物や設備に関する情報セキュリティの確保を図るため、次の各号に掲げる事項について区局に共通する物理的な情報セキュリティ対策を規定しなければならない。

(1)　サーバ等の設置及び管理

(2)　端末機等の設置及び管理

(3)　通信機器等の設置及び管理

(4)　記録媒体等の管理

（サーバ等設置箇所の管理）

第７条　情報資産管理者は、サーバ等を火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

２　情報資産管理者は、サーバ等の設置箇所について、情報資産の重要さに応じて次のような対策をとらなければならない。

(1)　すべての出入口に施錠設備を備えた部屋に設置すること。

(2)　サーバ等の設置場所であるようなことを示す表示をしないこと。

(3)　入退室管理を行うこと。

（サーバ等の管理）

第８条　情報資産管理者は、サーバ等を安全に運用するよう管理しなければならない。

２　情報資産管理者は､非開示情報を含むデータを保有するサーバ等の運用管理について、情報資産の重要さに応じて次のような対策をとらなければならない。

(1)　利用権限を持たない者が利用できないようにすること。

(2)　保守の記録を残すこと。

(3)　あらかじめ障害発生時の代替機器を用意しておくこと。

３　情報資産管理者は、ウェブサーバ等、インターネットを経由して不特定多数からアクセスが可能な状態にある情報機器等について、インターネットを経由したサイバー攻撃のリスクに対して、適切なセキュリティ対策を実施しなければならない。

（端末機等の管理）

第９条　情報資産管理者は、端末機等を安全に運用するよう管理しなければならない。

２　情報資産管理者は、非開示情報を含むデータを閲覧可能な端末機等の運用管理について、情報資産の重要さに応じて次のような対策をとらなければならない。

(1)　盗難防止対策を行うこと。

(2)　利用権限を持たない者が利用できないようにすること。

(3)　ソフトウェアは、業務に必要なもののみを導入すること。

(4)　外部への持ち出し制限対策又は外部でのデータ利用制限対策を行うこと。

3　情報資産管理者は、携帯端末機を導入する場合、セキュリティ確保のために必要な措置を講じなければならない。

（記録媒体等の管理）

第 10 条　情報資産管理者は、滅失又はき損した場合にその復元が困難であると認められるデータを記録した記録媒体について、安全に保管するとともに、複写など復元のための対策をとるものとする。

2　情報資産管理者は、非開示情報を含む記録媒体等のうち容易に持ち運べるものについて、利用しないときには施錠して保管する等の盗難防止対策を行わなければならない。

3　情報資産管理者は、非開示情報を含む記録媒体等について、廃棄時には復元できないよう対策をとらなければならない。記録媒体の場合にはデータを消去するか物理的に破壊する、紙媒体の場合には粉砕処理や溶解処理など、適正な対策を行うものとする。

（特定個人情報を取り扱う区域の管理）

第 10 条の２　情報資産管理者は、特定個人情報を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確化し、取扱区域の外で特定個人情報を取り扱うことがないよう運用するとともに、特定個人情報が取扱区域の外に持ち出されることのないよう対策をとらなければならない。

（通信回線等の管理）

第 10 条の３　情報セキュリティ総括管理者は、規程第３条に基づき、ネットワークを総合行政ネットワーク（以下「LGWAN」という。）接続系とインターネット接続系に分割する。

2　情報セキュリティ運用管理者は、行政系のネットワークを LGWAN 接続系に集約するように努めなければならない。

3　情報セキュリティ運用管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

4　情報セキュリティ運用管理者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続の防御を義務付けなければならない。

第５章　人的な情報セキュリティ対策

（人的な情報セキュリティ対策）

第 11 条　情報セキュリティ運用管理者は、過誤、盗難、不正行為又は設備の誤用など「人」に関わる情報セキュリティの確保を図るため、次の各号に掲げる事項について人的な情報セキュリティ対策を実施しなければならない。

(1)　職員に対する、情報セキュリティの重要性や規程等の内容を理解させるための研修・訓練等の実施

(2)　情報システムの開発、保守又は運用等の業務を外部事業者に委託する場合の、外部

事業者が守るべき事項の規定

２　区局情報セキュリティ総括責任者及び情報セキュリティ担当者は、所管する職員に対し、情報セキュリティの重要性や規程等の内容を理解させるための教育・訓練等を実施しなければならない。

（ＩＤ及びパスワードの管理）

第 11 条の２　職員は付与されたＩＤを次のとおり取り扱うものとする。

(1)　情報システムを利用する際は、原則として情報資産管理者から付与されたＩＤのみを利用すること。

(2)　情報資産管理者から付与されたＩＤを他人に使わせないこと。

２　利用者認証にあたりパスワードまたは認証用カードを利用する場合は、その管理を次のとおり行うものとする。

(1)　パスワード、認証用カード等が第三者に渡ることのないようにすること。

(2)　パスワードを設定する場合､他人に類推されやすいパスワードの利用は避けること。

(3)　パスワード、認証用カード等が第三者に渡ったおそれがあるときには、速やかに利用停止の手続き等を行うこと。

（私用の情報機器等の業務利用）

第 11 条の３　職員は、私用の情報機器等を原則業務に利用してはならない。ただし、業務上必要な場合は、情報セキュリティ担当者の許可を得て利用することができる。

第６章　技術的な情報セキュリティ対策

（技術的なセキュリティ対策）

第 12 条　情報セキュリティ運用管理者は、不正アクセスやコンピュータウイルス等からの情報資産の保護など情報システムの技術的処理方法に関わる情報セキュリティの確保及びインターネットリスクに関わる情報セキュリティの確保のため、次の各号に掲げる事項について区局に共通する技術的な情報セキュリティ対策を規定しなければならない。

(1)　情報資産をコンピュータウイルスから保護するために遵守しなければならない事項

(2)　情報資産を権限のない第三者による侵害から保護するために遵守しなければならない事項

（データの管理）

第 13 条　情報資産管理者は、データの管理について、次のとおり行うものとする。

(1)　必要最小限の職員に対して、必要最小限の範囲でのみ利用を認めること。

(2)　必要に応じて利用者の認証に関する管理を行うこと。

２　職員は、非開示情報を含むデータを取り扱うにあたって、情報の特性に応じて次のとおり扱わなければならない。

(1)　特定個人情報を含むデータ

特定個人情報に関する次の法令、ガイドラインに従って取り扱うこと。

ア　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）

イ　横浜市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の施行に関する条例（平成27年9月横浜市条例第52号）

ウ　「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」など、個人情報保護委員会が定める特定個人情報保護に関する文書

(2)　個人情報を含むデータ

横浜市個人情報の保護に関する条例（平成17年2月横浜市条例第6号）に従って取り扱うこと。

(3)　特定個人情報及び個人情報を含まないデータ

当該データについて守秘を定めた法令、規程等がある場合、当該法令、規程等に従って取り扱うこと。

3　情報資産管理者は、記録媒体について、必要に応じて定期的にバックアップを実施しなければならない。

（情報システムの管理）

第14条　情報資産管理者は、情報システムの管理について、次のとおり行うものとする。

(1)　情報システム開発の管理

ア　情報システム管理記録の作成及び管理

非開示情報を扱う情報システムについて、当該情報システムに関する開発中の変更等の作業履歴を記録・管理し、保管すること。

イ　情報システム開発環境の管理

非開示情報を扱う情報システムの開発の際には、必ず開発用の環境を用意し、本番環境とは切り離して管理すること。

ウ　テスト用のデータが実データに混入しないようにするなど、テスト用のデータと実データを分離すること。

(2)　ソフトウェアの管理

ア　ソフトウェア及びライセンスを適切に管理すること。

イ　非開示情報を扱う情報システムについて、当該情報システムの変更等の履歴を管理すること。

ウ　非開示情報を扱う情報システムについて、当該情報システムの仕様書及び手順書を最新の状態で管理し、必要とする職員がすみやかに閲覧できる状況の維持に努めるとともに、閲覧する権限のない者が閲覧することのないようにしなければならない。

（特定用途機器のセキュリティ管理）

第14条の2　情報資産管理者は、特定用途機器を導入する場合、当該機器が備える機能、設置環境並びに取り扱う情報資産に応じ、適切なセキュリティ対策を実施しなければならない。

（無線 LAN のセキュリティ管理）

第 14 条の３　情報資産管理者は、無線 LAN を導入する場合、当該機器が備える機能、設置環境並びに取り扱う情報資産に応じ、解読が困難な暗号化及び認証技術の使用等、適切なセキュリティ対策を実施しなければならない。

（コンピュータウイルス等対策）

第 15 条　本市のコンピュータウイルス等対策は、次のとおり実施するものとする。

(1)　本市のコンピュータウイルス等対策の責任者は、情報セキュリティ運用管理者とする。

(2)　情報セキュリティ運用管理者は、情報システムに大きな被害を及ぼす恐れのあるウイルス等が発見された場合、職員に周知しなければならない。

(3)　情報セキュリティ運用管理者は、ウイルス等対策の啓発を行い、ウイルス被害の情報収集のためにウイルス対策等窓口を設置しなければならない。

(4)　職員は、ウイルス等によって引き起こされる情報漏えいやシステム破壊の被害を未然に防ぐよう努めなければならない。

(5)　情報セキュリティ担当者は、ウイルス等による被害が発生した場合には、すみやかにウイルス対策等窓口あて報告しなければならない。

（利用者の認証）

第 16 条　非開示情報を含むデータを保有する情報システムの情報資産管理者は、利用者の認証について次のとおり実施するものとする。

(1)　利用の際に利用者を特定する機能を持たせること。

(2)　利用者によってデータを利用する権限が異なる場合、利用者ごとに閲覧・操作可能なデータの範囲を設定すること。

(3)　権限を持たない者がデータを利用することを防ぐこと。特に、利用者を特定するためのデータの管理は厳重にすること。

(4)　毎年度及び必要に応じてＩＤ発行、更新、停止を行うこと。

(5)　毎年度及び必要に応じて適切なＩＤ管理のための研修を行うこと。

(6)　毎年度及び必要に応じてＩＤ管理の自己点検を行うこと。

（電子計算機結合）

第 17 条　区局情報セキュリティ総括責任者は、横浜市の情報システムを横浜市以外のものと通信回線で結合する場合、不正アクセスや傍受への対策など、十分な情報セキュリティ対策を講じなければならない。

２　前項の結合を行う場合には、区局情報セキュリティ総括責任者は、必要に応じて、結合を行おうとする情報システムを所有する者とデータの適正な取扱いに関する書面を取り交わすものとする。

３　区局情報セキュリティ総括責任者は、非開示情報を含むデータを保有する情報システムを、横浜市以外のものと通信回線で結合する場合、情報セキュリティ対策の内容について、あらかじめ情報セキュリティ運用管理者と協議しなければならない。

（使用状況の監視）

第 18 条　情報資産管理者は、個人情報等の重要なデータについて、端末機等によるデータの更新、検索等の操作の記録を保存する等、システムの使用状況を監視するために必要な措置を講ずるものとする。

第７章　情報セキュリティ事故対策

（情報セキュリティ事故対策）

第 19 条　情報セキュリティ運用管理者は、次の各号に掲げる状況のほか発生し得る情報セキュリティ事故の状況を想定して、区局に共通する対応を定めなければならない。

(1)　情報システムのハードウェア上の問題による情報システムの停止等

(2)　情報システムのソフトウェア上の問題による情報システムの停止等

(3)　横浜市が管理する個人情報等の漏えい又は破壊等

２　区局情報セキュリティ総括責任者は、所管する区局の情報セキュリティ事故について、必要に応じて対策を定めなければならない。

３　情報セキュリティ担当者は、所管する情報資産に関する情報セキュリティ事故について、必要に応じて対策を定めなければならない。

第８章　その他

（セキュリティ対策実施手順）

第 20 条　情報セキュリティ運用管理者は、規程及びこの要綱の規定に基づく情報セキュリティ対策について、それらの具体的な取組や実施方法等を記載した「情報セキュリティ対策共通実施手順」（以下「共通実施手順」という。）を定めなければならない。

２　区局情報セキュリティ総括責任者は、所管する区局の情報セキュリティ対策について、共通実施手順に加え、必要に応じて情報セキュリティ対策を定めなければならない。

３　情報セキュリティ担当者は、自課内で実施する情報セキュリティ対策について、共通実施手順に加え、必要に応じて情報セキュリティ対策を定めなければならない。

４　情報資産管理者は、主管する情報資産の情報セキュリティ対策について、共通実施手順に加え、必要に応じて情報セキュリティ対策を定めなければならない。

５　区局情報セキュリティ総括責任者、情報セキュリティ担当者及び情報資産管理者は、情報セキュリティ対策を実施するにあたり、業務への影響及び事象発生の可能性を考慮し、共通実施手順によることなくリスクに対応できると判断した場合、共通実施手順で定める手順の一部を省略することができる。この場合、代替となる物理的及び技術的対策を定めるとともに、その内容について情報セキュリティ運用管理者の承認を得なければならない。

（議長等からの届出等）

第 21 条　情報セキュリティ運用管理者は、議長、公営企業管理者、教育委員会、選挙管理

委員会、人事委員会、監査委員、農業委員会及び固定資産評価審査委員会（以下「議長等」という。）に対し、情報セキュリティ確保のため必要があると認めるときは、情報セキュリティ対策の実施を求めることができる。

2　情報セキュリティ運用管理者は、議長等が情報セキュリティ対策に関して、それぞれの規程に基づき、届出、通知若しくは報告をし、又は協議、協力を求めてきたときは、この要綱の例により、届出等に応じなければならない。

3　情報セキュリティ運用管理者は、情報セキュリティ確保のため必要があると認めるときは、議長等に対し、調査を行うことについて協力を求めることができる。

（外部サービスの利用）

第22条　情報資産管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

2　情報資産管理者は、独自に外部へのネットワーク接続が必要な場合は、事前に、情報セキュリティ運用管理者の許可を得なければならない。

3　情報資産管理者は、情報資産を庁外で保管又は利用する場合、情報の機密性に応じた適切なセキュリティ対策が実施されている施設又はサービスを選定し、情報セキュリティ対策に関する事項を含めた運用手順を定め、事前に、情報セキュリティ運用管理者の許可を得なければならない。

附　則

（施行期日）

1　この要綱は、平成17年4月1日から施行する。

（横浜市電子計算機処理に係るシステム及びデータ保護管理要綱の廃止）

2　横浜市電子計算機処理に係るシステム及びデータ保護管理要綱（平成12年6月30日総情第83号）は、廃止する。

（施行期日）

1　この要綱は、平成19年9月14日から施行する。

（施行期日）

1　この要綱は、平成26年3月27日から施行する。

（施行期日）

1　この要綱は、平成27年10月15日から施行する。

（施行期日）

この要綱は、平成30年3月15日から施行する。

別表

分類区分			情報資産管理者	
大分類	中分類	小分類		
ハードウェア	サーバ等		横浜市が直接管理・運用を行うサーバ等	当該機器を主管する課等の長又は担当課長
			外部に委託して管理・運用を行うサーバ等、又は派遣契約により派遣された者が管理運用を行うサーバ等	当該外部委託又は派遣契約を行う課等の長又は担当課長
	端末機等		横浜市が直接管理・運用を行う端末機等	当該機器を主管する課等の長又は担当課長
			外部に委託して管理・運用を行う端末機等及び派遣契約により派遣された者に管理運用を行わせる端末機等	当該外部委託又は派遣契約を行う課等の長又は担当課長
	通信機器等及び記録媒体等		当該機器を主管する課等の長又は担当課長	
ソフトウェア	基本ソフトウェア		当該ソフトウェアを主管する課等の長又は担当課長	
	業務ソフトウェア		当該ソフトウェアを主管する課等の長又は担当課長	
	その他のソフトウェア		当該ソフトウェアを主管する課等の長又は担当課長	
データ	非開示情報を含むデータ	特定個人情報を含むデータ	当該データを利用する業務を主管する課等の長又は担当課長	
		個人情報を含むデータ	当該データを利用する業務を主管する課等の長又は担当課長	
		特定個人情報・個人情報を含まないデータ	当該データを利用する業務を主管する課等の長又は担当課長	
	非開示情報を含まないデータ	非開示情報を含まないデータ	当該データを利用する業務を主管する課等の長又は担当課長	
行政文書	特定個人情報を含む行政文書		当該行政文書を利用する業務を主管する課等の長又は担当課長	
	個人情報を含む行政文書		当該行政文書を利用する業務を主管する課等の長又は担当課長	
	システム関連文書		当該行政文書を利用する業務を主管する課等の長又は担当課長	
	データとなる情報を記した行政文書及びデータを印刷した行政文書		当該行政文書を利用する業務を主管する課等の長又は担当課長	

別紙7

住民情報系ネットワーク　セキュリティ管理ガイドライン

平成29年4月25日制定

第1章　はじめに

（目的）

第1条　本ガイドラインは、横浜市情報セキュリティ管理規程（平成17年3月達第2号。以下「規程」という。）及び横浜市情報セキュリティ管理要綱（以下「要綱」という。）に基づき、住民情報系ネットワークに係る情報資産の安全かつ適切な運用を実現するために必要な事項を定め、情報セキュリティの確保を図ることを目的とする。

（定義）

第2条　本ガイドラインにおいて、次の各号に掲げる用語の意義は、規程第2条及び要綱第2条に定めるもののほか、当該各号に定めるところによる。

(1) 基幹系システム　住民記録、新国民健康保険、介護保険、後期高齢者医療、税務等の業務システムをいう。

(2) 基盤系システム　情報共有基盤システム及び同基盤上で稼働する福祉保健、母子保健、生活保護等の業務システムをいう。

(3) 個別業務システム　住民情報系ネットワーク上で稼働する業務システムのうち、基幹系システム、基盤系システムのいずれにも該当しないものをいう。

(4) 基幹ネットワーク　横浜市（以下「本市」という。）の基幹系システムにおいて利用されているネットワークをいう。

(5) 基盤ネットワーク　本市の基盤系システムにおいて利用されているネットワークをいう。

(6) 住民情報系ネットワーク　本市の基幹ネットワーク及び基盤ネットワークの総称。基幹系システム、基盤系システム、個別業務システムに分類される業務システムが稼働している。通信回線、サーバー等、通信機器等と、これらに接続して使用する端末機等から構成される。

(7) データセンター　住民情報系ネットワークを構成する主要な通信機器等及びサーバー等の機器を設置し、自然災害や火災、盗難などの物理的な脅威から保護するために住民情報系ネットワーク統括責任者が借り上げた施設をいう。

(8) 端末統制基盤　住民情報系ネットワークに接続する端末機等に対し、セキュリティ設定等を統一的に提供する仕組みをいう。

(9) 拠点ネットワーク　住民情報系ネットワークとの通信を目的として、市庁舎、民間ビル及び事務所・事業所等の建物内に配線されたネットワークをいう。ただし、データセンター内のネットワークを除く。

(10) 情報システム　ある目的を達成するためのハードウェア、ソフトウェア、ネットワーク等により構成される電子計算機処理の機構をいう。

(11) データ　情報システムで扱う電磁的記録（電子的方式、磁気的方式、その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）をいう。

(12)業務システム　特定の業務での利用を目的とする情報システムをいう。住民情報系ネットワーク内で稼働するものと、他のネットワークで稼働するもので住民情報系ネットワークを介して利用するものがある。

(13)業務端末　住民情報系ネットワークに接続する端末機等をいう。

（適用範囲）

第３条　本ガイドラインは住民情報系ネットワークに接続するすべての情報資産に適用する。

第２章　管理体制

（住民情報系ネットワーク統括責任者等の設置）

第４条　本ガイドラインの目的を達成するため、以下の管理者を置く。

(1) 住民情報系ネットワーク統括責任者

(2) 業務システム管理責任者

(3) 業務端末管理責任者

(4) データ管理責任者

２　住民情報系ネットワーク統括責任者には、横浜市事務分掌条例（昭和26年10月横浜市条例第44号）において、基幹情報システムの管理及び運用を所管する課の長をあてる。

３　業務システム管理責任者には、以下に該当する課の長をもって充てる。

(1) 基幹系システムにあっては、基幹情報システムの管理及び運用を所管する課

(2) 基盤系システムにあっては、当該業務システムを利用する業務を所管する課（ただし、情報共有基盤システムについては、基幹情報システムの管理及び運用を所管する課）

(3) 個別業務システムにあっては、当該個別業務システムを利用する業務を所管する課

４　業務端末管理責任者には、以下に該当する課の長をもって充てる。

(1) 基幹系業務端末にあっては、基幹情報システムの管理及び運用を所管する課

(2) 基盤系業務端末にあっては、基幹情報システムの管理及び運用を所管する課又は当該端末を利用する業務を所管する課

(3) 個別業務システム用業務端末にあっては、当該端末を利用する業務を所管する課

５　データ管理責任者には、当該データを利用する業務を所管する課の長をもって充てる。

（住民情報系ネットワーク統括責任者の責務）

第５条　住民情報系ネットワーク統括責任者は、業務システム管理責任者及び業務端末管理責任者を統括するとともに、住民情報系ネットワークの運用及び管理を総合的に行うため、次に掲げる事項を実施するものとする。

(1) 住民情報系ネットワークの整備に関する事項

(2) 住民情報系ネットワーク全体に係る情報セキュリティ対策に関する事項

(3) データセンター内ネットワークの運用及び管理に関する事項

(4) 拠点ネットワークのうち幹線となるネットワーク（以下「拠点内幹線ネットワーク」という。）の運用及び管理に関する事項

(5) 住民情報系ネットワークに接続する業務システム及び業務端末の監督に関する事項
(6) 端末統制基盤の運用及び管理に関する事項
(7) 住民情報系ネットワークに係る関係部署及び関係機関との連絡調整に関する事項
(8) 住民情報系ネットワーク以外のネットワーク（外部ネットワーク）との接続に関する事項
(9) その他必要な事項

（業務システム管理責任者の責務）

第６条　業務システム管理責任者は、住民情報系ネットワーク統括責任者及び業務端末管理責任者と連携し、業務システムの運用及び管理を行うため、次に掲げる事項を実施するものとする。
(1) 所管業務システムにかかる業務アプリケーションの開発、運用及び管理に関する事項
(2) 所管業務システムにかかるサーバー等の整備、運用及び管理に関する事項
(3) 所管業務システムにかかる業務アプリケーション及びサーバー等の情報セキュリティ対策に関する事項
(4) 所管業務システムを利用する職員等（以下「業務システム利用者」という。）の管理に関する事項
(5) その他必要な事項

2　業務システム管理責任者は、所管業務システムを利用する課等の長に対し、情報セキュリティ対策に係る指示及び指導を行うものとする。

3　業務システム管理責任者は、第 1 項第 4 号に掲げる事項について、所管業務システムを利用する課等の長に一部を委任することができるものとする。

（業務端末管理責任者の責務）

第７条　業務端末管理責任者は、住民情報系ネットワーク統括責任者及び業務システム管理責任者と連携し、業務端末の運用及び管理を行うため、次に掲げる事項を実施するものとする。
(1) 所管業務端末（基本ソフトウェア及び端末に導入して使用するソフトウェアを含む。以下同じ）の運用及び管理に関する事項
(2) 拠点ネットワークのうち、拠点内幹線ネットワーク以外のネットワーク（以下「拠点内非幹線ネットワーク」という。）の運用及び管理に関する事項
(3) 所管業務端末で利用する外部記憶媒体の運用及び管理に関する事項
(4) 所管業務端末、拠点内非幹線ネットワーク及び外部記憶媒体に係る情報セキュリティ対策に関する事項
(5) 所管業務端末及び外部記憶媒体を利用する職員等（以下「業務端末等利用者」という。）の管理に関する事項
(6) その他必要な事項

2　業務端末管理責任者は、所管業務端末を設置する課等の長に対し、業務端末の電源の確保、業務端末及び外部記憶媒体の適切な利用及び安全な保管等について、必要な指示、調整を行うものとする。

3　業務端末管理責任者は、第 1 項に掲げる事項について、所管業務端末を設置する課等の長に一部を委任することができるものとする。

（データ管理責任者の責務）

第８条　データ管理責任者は、所管するデータを適正に維持及び管理するため、次に掲げる事項を実施するものとする。

(1) 所管データの管理（収集、保存、利用、廃棄）に関する事項

(2) 所管データに係る情報セキュリティ対策に関する事項

(3) 所管データの提供及び提供先の監督に関する事項

(4) 住民情報系ネットワークからの所管データ持出し及び持出し先での利用に関する事項

(5) その他必要な事項

（住民情報系ネットワークの利用）

第９条　業務システム管理責任者及び端末管理責任者は、住民情報系ネットワークの利用を開始、変更又は終了する場合、事前に住民情報系ネットワーク統括責任者と協議するものとする。

２　業務システム管理責任者は、業務システム利用者を特定し、所管業務システムにおいて業務システム利用者が利用可能な業務範囲及び利用権限（以下「利用可能領域」という。）を定め、その管理を行う。

３　業務端末管理責任者は、業務端末等利用者を特定し、所管業務端末において業務端末等利用者の利用可能領域を定め、その管理を行う。

（利用者の責務）

第 10 条　業務システム利用者及び業務端末等利用者（以下「利用者」という。）は、住民情報系ネットワークを利用するに当たり、次に掲げる内容を遵守するものとする。

(1) 関係法令等を遵守すること。

(2) 定められた利用可能領域を遵守し、利用に必要な情報を適切に管理すること。

(3) 住民情報系ネットワーク、業務システム及び業務端末の正常な運用を妨げる行為をしないこと。

(4) 他の利用者の正常な利用を妨げる行為をしないこと。

(5) その他住民情報系ネットワーク統括責任者、業務システム管理責任者、業務端末管理責任者又はデータ管理責任者が不適切と認めることを行わないこと。

第３章　基本原則

（利用の原則）

第 11 条　住民情報系ネットワークの利用にあたっては、次の各号に定める原則を遵守するものとする。

(1) 個人情報保護の原則　住民情報系ネットワーク上の業務システム及び業務端末で取り扱う個人情報及び特定個人情報については、横浜市個人情報の保護に関する条例（平成 12 年２月条例第１号）及び横浜市特定個人情報の安全管理に関する基本方針（平成 27 年 10 月）等に基づいて取り扱い、データ管理責任者の許可なく住民情報系ネットワーク外に持ち出してはならない。

(2) セキュリティ確保の原則　住民情報系ネットワーク統括責任者、業務システム管理責任者及び業務端末管理責任者（以下「全ての管理責任者」という。）は、住民情報系ネットワークの安全な運用を確保するために必要な措置を講じなければならない。また、利用者は、規程、要綱及び横浜市情報セキュリティ対策共通実施手順（以下「共通実施手順」という。）を遵守するとともに、全ての管理責任者のいずれかが講じた情報セキュリティ対策を改変してはならない。

(3) 管理機器使用の原則　住民情報系ネットワークを利用するときは、全ての管理責任者のいずれかが設置又は管理する機器、通信回線を使用しなければならない。

(4) 職務目的外利用の禁止の原則　利用者は、住民情報系ネットワークを職務目的以外に利用してはならない。

(5) 相互協調の原則　利用者は、住民情報系ネットワークの適正な利用を促進するため、運用上必要な連絡、緊急時の対処等について相互に協力し、対応に当たらなければならない。

第４章　情報セキュリティ対策

（基本情報セキュリティ対策）

第 12 条　住民情報系ネットワーク統括責任者は、住民情報系ネットワークの情報セキュリティ対策について、規程、要綱及びその他関連規定に基づき行うものとし、適時見直しを行い、情報技術の進展等に対応した適切な措置を講ずるものとする。

２　住民情報系ネットワーク統括責任者は、業務システム管理責任者及び業務端末管理責任者が所管する業務システム及び業務端末について情報セキュリティ対策を行うよう求めることができる。

３　業務システム管理責任者及び業務端末管理責任者は、住民情報系ネットワーク統括責任者が第１項の規定に基づき行った対策に準じて、所管する業務システム及び業務端末に関して適切な措置を講ずるものとする。

４　要綱第４条に基づく情報資産管理者は別表に定めるとおりとする。

（ネットワークの情報セキュリティ対策）

第 13 条　住民情報系ネットワーク統括責任者は、第５条第１項第２号に規定する情報セキュリティ対策として、前条及び共通実施手順で規定する対策に併せ、必要に応じて次の各号に掲げる事項を行い、安全で安定したネットワーク運用の確保を図るものとする。

(1) 不正アクセスの防止を目的とする機器の設置及び必要な措置

(2) 不正なプログラム等の侵入及び拡散を検知し、及び防止し、並びに不正なプログラム等を駆除するための適切な措置

(3) 通信機器等及び通信回線の二重化

(4) ネットワークの監視

(5) ネットワーク構成情報の管理

(6) 接続機器の安全対策

(7) 機器の不正接続を防止するための適切な措置

(8) その他必要な情報セキュリティ対策

（業務システムの情報セキュリティ対策）

第 14 条　業務システム管理責任者は、所管する業務システムについて、第６条第１項第３号に規定する情報セキュリティ対策として、第 12 条及び共通実施手順で規定する対策に併せて、特に次の各号に掲げる事項を行うものとする。

(1) サーバー等への不正アクセスを防止するために必要な措置

(2) サーバー等の稼働状況の監視
(3) システム構成情報の管理
(4) サーバー等に導入されている基本ソフトウェア、ミドルウェア及び業務アプリケーションを安全かつ正常に動作するよう保つための適切な措置
(5) サーバー等へのウイルス対策ソフトウェアの導入及び最新のウイルス定義ファイルを適用するための適切な措置
(6) サーバー等における必要な設定及び適切なデータ管理
(7) その他必要な情報セキュリティ対策

（業務端末の情報セキュリティ対策）

第15条　業務端末管理責任者は、所管する業務端末について、第7条第1項第4号に規定する情報セキュリティ対策として、第12条及び共通実施手順で規定する対策に併せて、特に次の各号に掲げる事項を行うものとする。
(1) 業務端末に導入されている基本ソフトウェア、ミドルウェア及び業務アプリケーションを安全かつ正常に動作するよう保つための適切な措置
(2) 業務端末へのウイルス対策ソフトウェアの導入及び最新のウイルス定義ファイルを適用するための適切な措置
(3) 業務端末及び外部記憶媒体における必要な設定及び適切なデータ管理
(4) 業務端末及び外部記憶媒体の取扱いに関して必要な規定の整備
(5) その他必要な情報セキュリティ対策

（データの情報セキュリティ対策）

第16条　データ管理責任者は、所管するデータについて、第8条第1項第2号に規定する情報セキュリティ対策として共通実施手順で規定する対策に併せて、特に次の各号に掲げる事項を行うものとする。
(1) データの取扱いに関する規定の整備
(2) その他必要な情報セキュリティ対策

（ネットワーク等の障害時の対応）

第17条　住民情報系ネットワーク統括責任者は、住民情報系ネットワーク等の障害時の連絡体制を整備するものとする。
2　業務システム管理責任者及び業務端末管理責任者は、業務システムや業務端末等の利用に関して発生した障害が、住民情報系ネットワークの運用に影響を与える恐れがあると判断した場合は、必要な対策を行うとともに、速やかに住民情報系ネットワーク統括責任者に連絡するものとする。
3　業務システム管理責任者及び業務端末管理責任者は、住民情報系ネットワークにおいて何らかの障害を検知した場合には、必要な対策を行うとともに、速やかに住民情報系ネットワーク統括責任者に連絡するものとする。
4　前2項の連絡を受けた住民情報系ネットワーク統括責任者は、業務システム管理責任者又は業務端末管理責任者とともに障害等の状況を把握し、必要な対策を行うとともに、速やかに必要な措置及び情報提供等の対応を行うものとする。

5　住民情報系ネットワーク統括責任者は、障害等の再発防止措置を行うとともに、必要に応じ業務システム管理責任者又は業務端末管理責任者に速やかに改善措置を取るよう求めることができる。

第5章　その他

（調査等）

第18条　住民情報系ネットワーク統括責任者は、住民情報系ネットワークについて運用上又は管理上必要があると認める場合は、業務システム又は業務端末の住民情報系ネットワークの利用状況及び管理状況の調査を行うことができる。

2　業務システム管理責任者及び業務端末管理責任者は、前項の調査に当たり、住民情報系ネットワーク統括責任者から依頼を受けた場合は、協力して調査に当たるものとする。

3　業務システム管理責任者及び業務端末管理責任者は、所管する業務システム又は業務端末の運用上又は管理上必要と認める場合は、住民情報系ネットワーク統括責任者に第1項に定める調査を依頼することができる。

4　住民情報系ネットワーク統括責任者は、第1項の調査により住民情報系ネットワークの運用上又は管理上の問題を確認した場合は、当該業務システム又は業務端末の利用を制限し、又は停止するとともに、必要な措置を講ずることができる。

5　データ管理責任者は、データ提供先におけるデータ利用状況及び管理状況について調査を行うことができる。

6　業務システム管理責任者及び業務端末管理責任者は、前項の調査に当たり、データ管理責任者から依頼を受けた場合は、協力して調査に当たるものとする。

（委任）

第19条　このガイドラインの施行に関し必要な事項は住民情報系ネットワーク統括責任者が定める。

附則

このガイドラインは平成29年4月25日から施行する。

別表

分類区分			情報資産管理者
大分類	中分類	小分類	
ハードウェア	サーバー等		業務システム管理責任者
	端末機等		業務端末管理責任者
	通信機器等	データセンター内ネットワークに係る機器	住民情報系ネットワーク統括責任者
		拠点内幹線ネットワークに係る機器	住民情報系ネットワーク統括責任者
		拠点内非幹線ネットワークに係る機器	業務端末管理責任者
ソフトウェア	サーバー等		業務システム管理責任者
	端末機等		業務端末管理責任者
データ			データ管理責任者

●個人情報を記録したシステムにおける端末機によるデータの更新、検索等の操作の記録に関する要綱

制定　平成 15 年８月 25 日　総Ｉ第 120 号（局長決裁）
一部改正　平成 30 年３月 15 日　総行第 2035 号（局長決裁）

（目的）

第１条　この要綱は、横浜市情報セキュリティ管理要綱（平成 17 年３月 31 日総行Ｉ第 1148 号）第 18 条に基づき、横浜市の個人情報を記録したシステムにおける端末機によるデータの更新、検索等の操作の記録（アクセスログ）を保存する等、システムの使用状況を監視するための必要な事項を定めることにより、電子計算機における個人情報の管理運営の適正化を図ることを目的とする。

（用語の意義）

第２条　この要綱において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　個人情報　横浜市個人情報の保護に関する条例（平成 17 年２月横浜市条例第６号）第２条第３項に規定する個人情報をいう。

(2)　システム　ある目的を達成するためのソフトウェア、ハードウェア、ネットワーク等を連携して構築する電子計算機処理の環境をいう。

(3)　ホストコンピュータ等　システムにおいて、プログラム、データ等が保存され、端末機からアクセスを受けるコンピュータをいう。

(4)　端末機　システムにおいて、ホストコンピュータ等にアクセスし、入出力を行う機器をいう。

(5)　アクセスログ　端末機を使用して行われる情報の更新、検索等の操作について記録した情報をいう。

(6)　操作者　システムの端末機から個人情報について更新、検索等の操作を行う者をいう。

(7)　アクセスログ蓄積対象情報　個人識別コード等、更新、検索等の対象となる個人を特定できる情報をいう。

(8)　区局等　横浜市事務分掌条例（昭和 26 年 10 月横浜市条例第 44 号）第１条に掲げる統括本部及び局並びに横浜市消防本部及び消防署の設置等に関する条例(昭和 38 年 10 月横浜市条例第 34 号）第２条第２項に規定する消防局（以下「消防局」という。)、横浜市会計室規則（平成 19 年３月 30 日規則第 36 号）第１条に規定する会計室（以下「会計室」という。）及び横浜市区役所事務分掌条例（平成 28 年２月条例第２号）第１条に規定する区役所（以下「区役所」という。）をいう。

（アクセスログ管理責任者の設置）

第３条　この要綱の目的を達成するため、電子計算機処理にかかる業務を主管する課の長をアクセスログ管理責任者に充てる。

２　アクセスログ管理責任者は、アクセスログの収集、保存、処理、廃棄に係る業務（以

下、「アクセスログに係る業務」という。）を管理する。

（アクセスログの収集）

第４条　アクセスログ管理責任者は、データの重要度に応じ、区局等が運用するシステムのうち、個人情報を扱い、端末機から、ホストコンピュータ等のファイル、データベース等に記録されている個人情報について更新、検索等の操作を行う場合にアクセスログを収集するものとする。

２　アクセスログの収集にあたっては、次の各号を識別できる項目を収集する。

(1)　操作年月日

(2)　操作時刻

(3)　操作者

(4)　アクセスログ蓄積対象情報

(5)　利用部署、端末機名、処理内容その他必要な項目

（アクセスログの管理）

第５条　アクセスログ管理責任者は、収集したアクセスログを次の各号に定めるとおり、適正に管理しなければならない。

(1)　アクセスログは他の法令等に定めがある場合を除き原則として３年保存とする。また、磁気テープ等の外部記録媒体で保存する場合は施錠できる金庫等に保管する。

(2)　廃棄年限を超えたアクセスログは、速やかかつ確実に消去する。

２　アクセスログ管理責任者は、収集したアクセスログについて、必要に応じて確認を行うものとする。

（アクセスログの開示）

第６条　横浜市個人情報の保護に関する条例（平成 17 年２月横浜市条例第６号）第 20 条の規定に基づき、アクセスログの本人開示請求があった場合、当該システムのアクセスログ管理責任者は、当該請求に係る情報（システムのセキュリティに影響のあるものを除く。）を開示する。

２　開示する情報は、紙へ印字し、又は電子媒体へ複写して提供する。

（アクセスログの収集の開始及び終了の報告）

第７条　アクセスログ管理責任者は、アクセスログの収集を開始し、又は終了するときは、別記様式により総務局長へ報告しなければならない。

（委任）

第８条　この要綱に定めるもののほか、アクセスログに係る必要な事項は、総務局行政・情報マネジメント課長が定める。

附　則

（施行期日）

この要綱は、平成 15 年９月１日から施行する。

附　則

（施行期日）

この要綱は、平成 17 年５月 30 日から施行する。

附　則

（施行期日）

この要綱は、平成 18 年４月１日から施行する。

附　則

（施行期日）

この要綱は、平成 19 年４月１日から施行する。

附　則

（施行期日）

この要綱は、平成 22 年４月１日から施行する。

附　則

（施行期日）

この要綱は、平成 27 年４月１日から施行する。

附　則

（施行期日）

この要綱は、平成 30 年３月 15 日から施行する。

別記様式（第７条）

個人情報を記録したシステムにおける端末機によるデータの更新、検索等の操作の記録（アクセスログ）収集開始・終了報告書

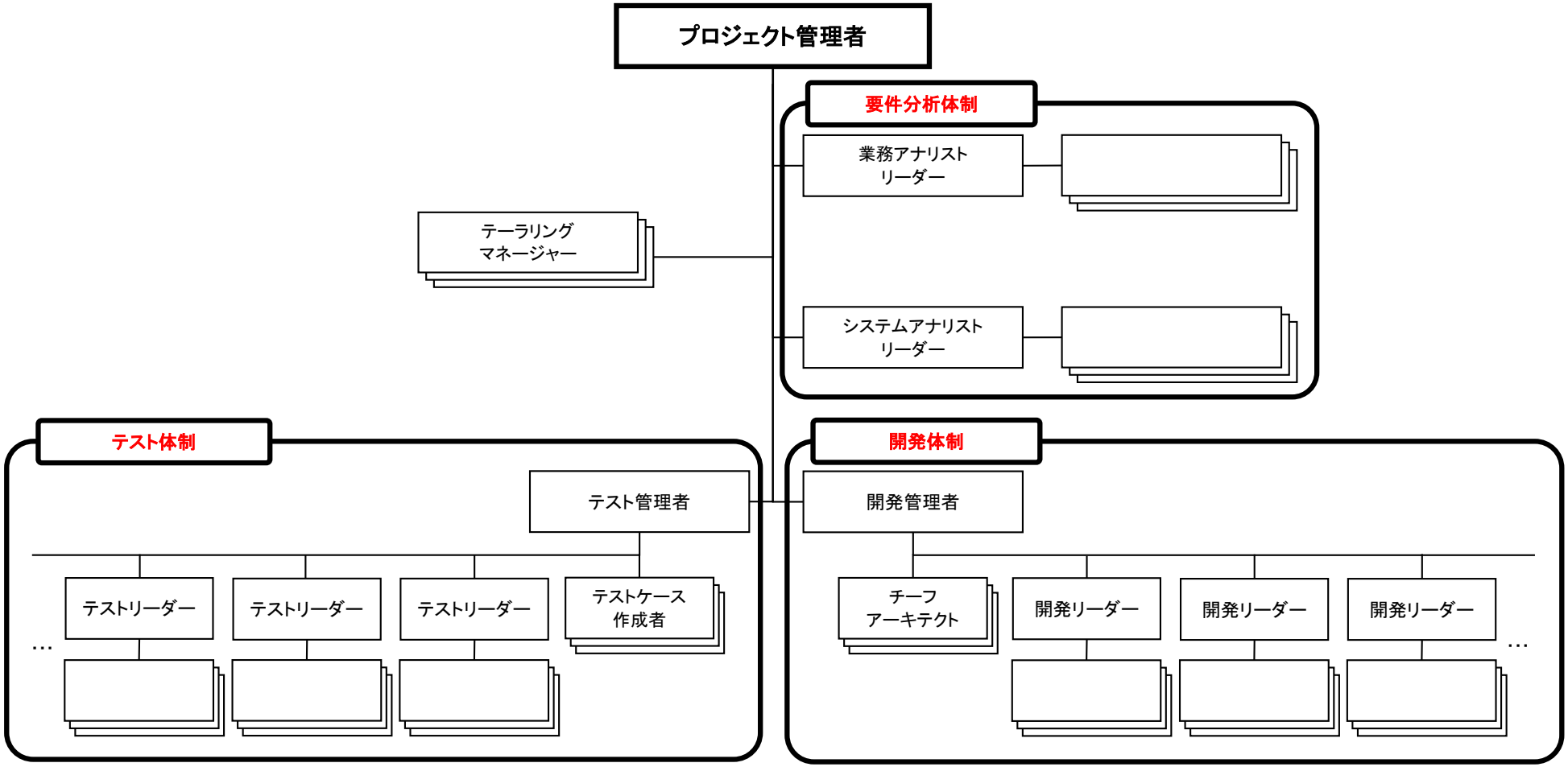
年　　月　　日

総務局長

長

個人情報を記録したシステムにおける端末機によるデータの更新、検索等の操作の記録に関する要綱第７条の規定により、次のとおり報告します。

事務の名称（システム名）	
担当課等	局　　課 担当 ＴＥＬ
開始・終了 年　　月　　日	年　　月　　日　開始　・　終了
備考	


プロジェクト管理者
要件分析体制
業務アナリスト
リーダー
テーラリング
マネージャー
システムアナリスト
リーダー
テスト体制
開発体制
テスト管理者
開発管理者
テストリーダー
テストリーダー
テストリーダー
テストケース
作成者
チーフ
アーキテクト
開発リーダー
開発リーダー
開発リーダー
…
…